Guide de l'utilisateur

AWS Support

Version de l'API 2013-04-15

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

AWS Support: Guide de l'utilisateur

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

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

Table of Contents

Démarrer avec AWS Support

AWS Support propose un large choix de formules qui vous permettent d'accéder aux outils et aux compétences nécessaires pour garantir la réussite et la santé opérationnelle de vos solutions AWS. Tous les plans de support offrent un accès en permanence au service client, à de la documentation sur AWS, des publications techniques et des forums de support. Pour accéder au support technique et à d'autres ressources qui vous aideront à planifier, déployer et améliorer votre environnement AWS, vous pouvez sélectionner un plan de support pour votre utilisation d'AWS.

Remarques

- Pour créer un cas dans la AWS Management Console, consultez Création d'un dossier de support.
- Pour plus d'informations sur les divers plans AWS Support, consultez Comparer les plans AWS Support (français non garanti) et Modifier les AWS Support plans.
- Les plans de support proposent différents temps de réponse pour vos demandes d'assistance. Consultez Choix du niveau de gravité et Temps de réponse.

Rubriques

Création de cas de support et de gestion de cas

Dans le AWS Management Console, vous pouvez créer trois types de dossiers clients dans AWS Support :

- Les cas de support de compte et de facturation sont disponibles pour tous les clients AWS. Vous pouvez obtenir de l'aide avec vos questions de facturation et de compte.

- Les requêtes d'augmentation de limite de service sont également disponibles pour tous les clients AWS. Pour de plus amples informations sur les quotas de service par défaut, anciennement appelés limites, veuillez consulter Quotas de service AWS dans la Références générales AWS.
- Les cas de support technique vous mettent en relation avec le support technique pour obtenir de l'aide pour des questions techniques liées au service et, dans certains cas, des applications tierces. Si vous avez un plan de support Basic, vous ne pouvez pas créer de cas de support technique.

> **Remarques**
>
> - Pour modifier votre plan de support, consultez Modifier les AWS Support plans.
> - Pour fermer votre compte, consultez Clôture d'un compte dans le Guide de l'utilisateur AWS Billing.
> - Pour consulter les rubriques de résolution des problèmes les plus courantes pour Services AWS, consultez Ressources de dépannage.
> - Si vous êtes client d'un AWS Partner qui fait partie de l'AWS Partner Network, et que vous utilisez le Support de revente, contactez directement votre AWS Partner pour tout problème lié à la facturation. AWS Support ne peut pas vous aider pour les questions non techniques du Support de revente, telles que la facturation et la gestion des comptes. Pour plus d'informations, consultez les rubriques suivantes :
>   - Comment les partenaires AWS peuvent déterminer les plans AWS Support dans une organisation
>   - AWS Partner-Support dirigé

Création d'un dossier de support

Vous pouvez créer un cas de support dans le Centre de support de la AWS Management Console.

> **Remarques**
>
> - Vous pouvez vous connecter au Centre de support en tant qu'utilisateur racine de votre compte AWS ou en tant qu'utilisateur AWS Identity and Access Management (IAM). Pour de plus amples informations, veuillez consulter Gérer l'accès au AWS Support centre.

- Si vous ne parvenez pas à vous connecter au Centre de support et à créer un cas de support, vous pouvez utiliser la page Contactez-nous à la place. Vous pouvez utiliser cette page pour obtenir de l'aide sur les problèmes de facturation et de compte.

Pour créer une demande de support

1. Connectez-vous à AWS Support Center Console.

   > **Tip**
   >
   > Dans la AWS Management Console, vous pouvez également choisir l'icône du point d'interrogation
   > (),
   > puis Support Center (Centre de support).

2. Choisissez Create case (Créer une demande).
3. Choisissez l'une des options suivantes :

   - Account and billing (Compte et facturation)
   - Technical (Technique)
   - Pour obtenir des augmentations des quotas de service, choisissez Looking for service limit increases? (Vous recherchez des augmentations de la limite de service ?) puis suivez les instructions pour Création d'augmentation de quota de service.

4. Choisissez le Service, la Category (Catégorie), et la Severity (Sévérité).

   > **Tip**
   >
   > Vous pouvez utiliser les solutions recommandées qui apparaissent pour les questions les plus fréquemment posées.

5. Choisissez Next step: Additional information (Étape suivante : informations supplémentaires)
6. Sur la page Additional information (Informations supplémentaires), pour Subject (Sujet), saisissez un titre concernant votre problème.
7. Pour la Description, suivez les invites pour décrire votre cas, comme par exemple les suivantes :

   - Messages d'erreur que vous avez reçus

- Étapes de dépannage que vous avez suivies
- La façon dont vous accédez au service :
  - AWS Management Console
  - AWS Command Line Interface (AWS CLI)
  - Opérations d'API

8. (Facultatif) Choisissez Attach files (Joindre des fichiers) pour ajouter des fichiers pertinents à votre cas, tels que des journaux d'erreurs ou des captures d'écran. Vous pouvez attacher jusqu'à 3 fichiers. La taille de chaque fichier peut aller jusqu'à 5 Mo.
9. Choisissez Next step: Solve now or contact us (Étape suivante : résolvez maintenant ou contactez-nous).
10. Sur la page Contact us (Contactez-nous), choisissez votre langue préférée.
11. Choisissez votre méthode de contact préférée. Vous pouvez choisir l'une des options suivantes :

    a. Web : recevoir une réponse dans le Centre de support.

    b. Conversation instantanée : initier un chat en direct avec un agent de support. Si vous ne parvenez pas à vous connecter à un chat, consultez Résolution des problèmes.

    c. Téléphone : recevoir un appel téléphonique d'un agent de support. Si vous choisissez cette option, saisissez les informations suivantes :

    - Country or region (Pays ou région)
    - Phone number (Numéro de téléphone)
    - (Optional) Extension (Extension [facultatif])

    > **Remarques**
    >
    > - Les options de contact qui apparaissent dépendent du type de cas et de votre plan d'assistance.
    > - Vous pouvez choisir Discard draft (Ignorer le brouillon) pour effacer le brouillon de votre dossier de support.

12. (Facultatif) Si vous possédez un plan de support Business, Enterprise On-Ramp ou Enterprise, les Additional contacts (Autres contacts) s'affichent. Indiquez les adresses e-mail des personnes à informer lorsque l'état du cas change. Si vous êtes connecté en tant qu'utilisateur IAM, incluez

votre propre adresse e-mail. Si vous êtes connecté avec l'adresse e-mail et le mot de passe de votre compte racine, vous n'avez pas besoin d'inclure votre e-mail

> **Note**
>
> Si vous avez souscrit au plan de support Basic, l'option Additional contacts (Autres contacts) n'est pas disponible. Le contact Opérationnel indiqué dans la section Autres contacts de la page Mon compte reçoit toutefois une copie des messages relatifs aux demandes de support, mais uniquement pour les cas spécifiques de type compte, facturation et technique.

13. Vérifiez les détails de votre cas et choisissez Submit (Envoyer). Votre numéro d'ID de dossier et votre résumé apparaissent.

Description de votre problème

Votre description doit être aussi détaillée que possible. Incluez des informations pertinentes sur les ressources, ainsi que tout autre élément susceptible de nous aider à comprendre votre demande. Par exemple, pour la résolution de problèmes liés aux performances, incluez des horodatages et des journaux. Pour des demandes de fonctionnalités ou des questions d'ordre général, incluez une description de votre environnement et votre objectif. Dans tous les cas, suivez les conseils pour la description qui s'affichent sur votre formulaire de soumission de demande.

En fournissant le plus de détails possible, vous augmentez les chances de résolution rapide de votre problème.

Choix du niveau de gravité

Vous pourriez être enclin à toujours créer une demande de support de la gravité la plus élevée que votre plan de support autorise. Cependant, nous vous recommandons de choisir les gravités les plus élevées pour les demandes qui ne peuvent pas être contournées ou qui affectent directement les applications de production. Pour plus d'informations sur le développement de vos services afin que la perte de ressources uniques n'affecte pas vos applications, consultez la documentation technique Building Fault-Tolerant Applications on AWS (Création d'applications tolérantes aux pannes sur AWS).

Le tableau suivant répertorie les niveaux de gravité, les temps de réponse et des exemples de problème.

Remarques

- Vous ne pouvez pas modifier le code de gravité d'une demande de support après sa création. Si la situation évolue, travaillez avec l'agent AWS Support pour votre cas de support.
- Pour plus d'informations sur le niveau de gravité, consultez la Référence d'API AWS Support.

Sévérité	Code de niveau de sévérité	Temps de réponse initial	Description et plan de support
General guidance	`low`	24 heures	Vous avez une question générale concernant le développement ou vous souhaitez obtenir une fonctionnalité. (*Plan de support Developer, Business, Enterprise On-Ramp ou Enterprise)
System impaired	`normal`	12 heures	Des fonctionnalités non critiques de votre application se comportent anormalement, ou vous avez une question de développement prioritaire. (*Plan de support Developer, Business, Enterprise On-Ramp ou Enterprise)
Production system impaired	`high`	4 heures	Des fonctions importantes de votre application sont défaillantes ou dégradées. (Plan de support Business, Enterprise On-Ramp ou Enterprise)
Production system down	`urgent`	1 heure	L'impact sur votre activité est considérable. Les fonctions importantes de votre application ne sont pas disponibles. (Plan de support Business, Enterprise On-Ramp ou Enterprise)
Business-critical system down	`critical`	15 minutes	Votre activité est en danger. Les fonctions critiques de votre application ne sont pas

Sévérité	Code de niveau de sévérité	Temps de réponse initial	Description et plan de support
			disponibles (plan de support Enterprise). Notez que cela dure 30 minutes pour le plan de support Enterprise On-Ramp.

Temps de réponse

Nous mettons tout en œuvre pour répondre à votre demande initiale dans le délai indiqué. Pour obtenir plus d'informations sur le niveau de support offert par chaque plan AWS Support, veuillez consulter Fonctionnalités de AWS Support.

Si vous possédez un plan de support Business, Enterprise On-Ramp ou Entreprise, vous possédez un service de support technique 24 h/24, 7 j/7. *Pour le plan de support Developer, le temps de réponse cible des cas de support est calculé en heures d'ouverture. Les heures d'ouverture sont généralement définies comme suit : de 8h00 à 18h00 dans le pays du client, à l'exception des jours fériés et des week-ends. Ces temps de réponse peuvent varier dans les pays couverts par plusieurs fuseaux horaires. Les informations du pays du client apparaissent dans la section Informations sur le contact de la page Mon compte dans AWS Management Console.

> **Note**
>
> Si vous choisissez le japonais comme langue de contact préférée pour les demandes de support, le support en japonais peut être disponible comme suit :
>
> - Si vous avez besoin d'un service client pour des demandes de support non techniques, ou si vous disposez d'un plan Developer Support et que vous avez besoin d'un support technique, le support en japonais est disponible pendant les heures ouvrables au Japon, de 9 h 00 à 18 h 00, Japan Standard Time (GMT+9), à l'exception des jours fériés et des week-ends.
> - Si vous possédez un plan de support Business, Enterprise On-Ramp ou Entreprise, les services de support technique en japonais sont disponibles 24 h/24, 7 j/7.

Si vous choisissez le chinois comme langue de contact préférée pour les demandes de support, le support en chinois peut être disponible comme suit :

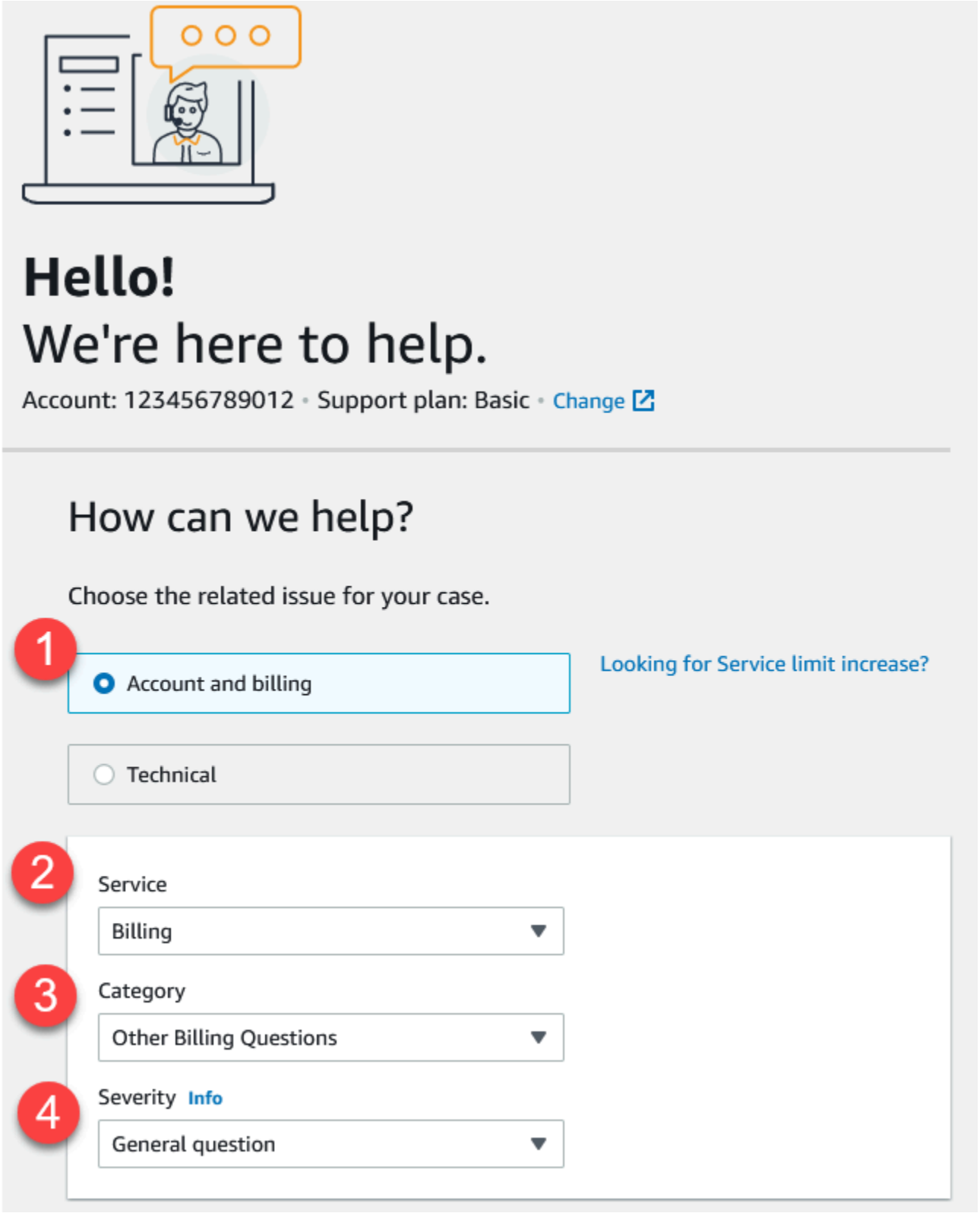
- Si vous avez besoin d'un service client pour des demandes de support non techniques, le support en chinois est disponible de 9 h 00 à 18 h 00 (GMT+8), à l'exception des jours fériés et des week-ends.
- Si vous disposez d'un plan Developer Support, le support technique en chinois est disponible pendant les heures ouvrables, généralement de 8 h 00 à 18 h 00 dans votre pays, comme indiqué dans la section Mon compte, à l'exception des jours fériés et des week-ends. Ces horaires peuvent varier dans les pays couverts par plusieurs fuseaux horaires.
- Si vous disposez d'un plan de support Business, Enterprise On-Ramp ou Entreprise, le support technique en chinois est disponibles 24 h/24, 7 j/7.

Si vous choisissez le coréen comme langue de contact préférée pour les demandes de support, le support en coréen peut être disponible comme suit :

- Si vous avez besoin d'un service client pour des demandes de support non techniques, le support en coréen est disponible pendant les heures ouvrables en Corée, de 9 h 00 à 18 h 00, Korean Standard Time (GMT+9), à l'exception des jours fériés et des week-ends.
- Si vous disposez d'un plan Developer Support, le support technique en coréen est disponible pendant les heures ouvrables, généralement de 8 h 00 à 18 h 00 dans votre pays, comme indiqué dans la section Mon compte, à l'exception des jours fériés et des week-ends. Ces horaires peuvent varier dans les pays couverts par plusieurs fuseaux horaires.
- Si vous disposez d'un plan de support Business, Enterprise On-Ramp ou Entreprise, le support technique en coréen est disponible 24 h/24, 7 j/7.

Exemple : créer un cas de support pour le compte et la facturation

L'exemple suivant est un cas de support pour un problème de facturation et de compte.



1. Créer un cas : choisissez le type de cas à créer. Dans cet exemple, le type de cas est Account and billing (Compte et facturation).

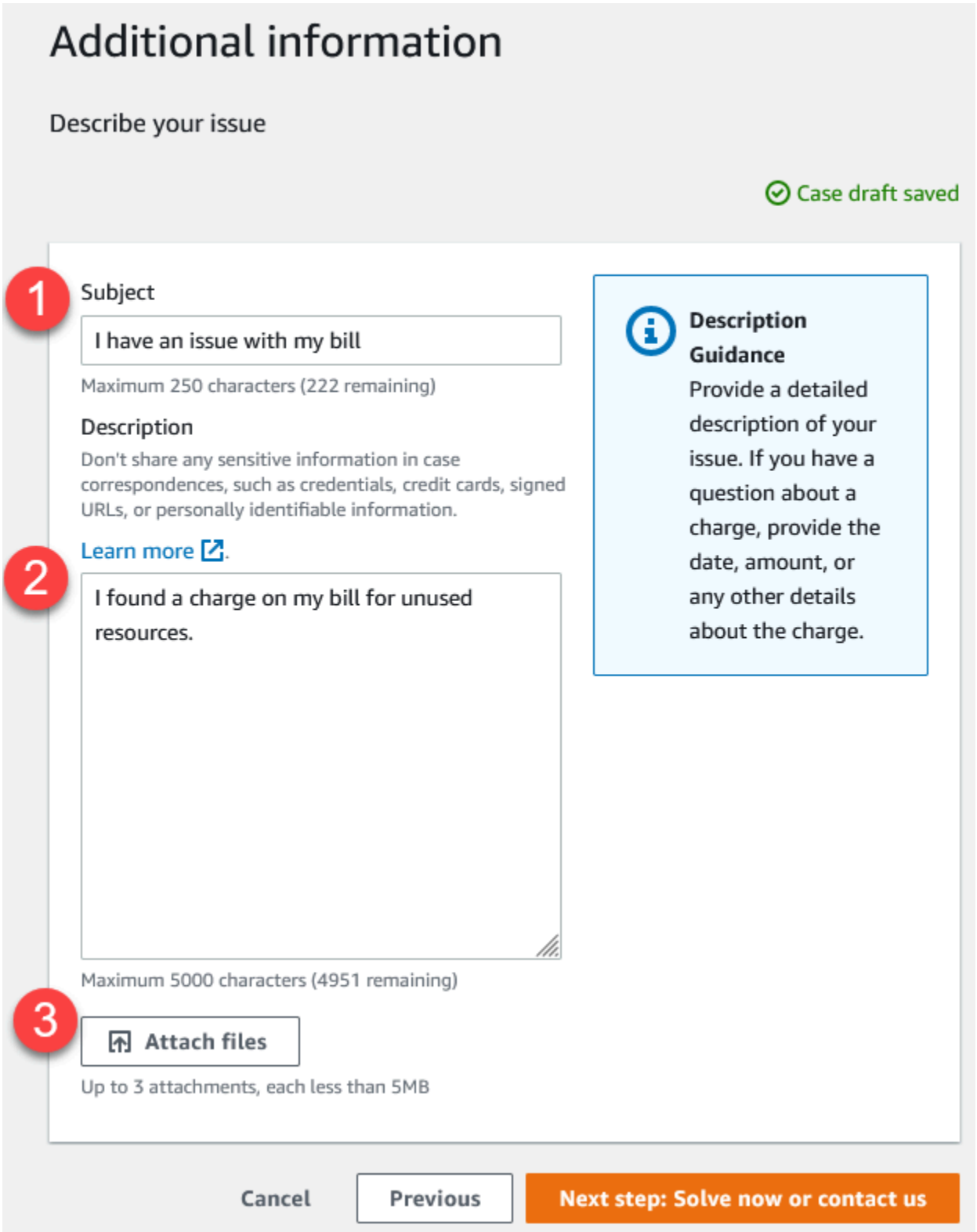
> **Note**
>
> Si vous avez souscrit au plan de support Basic, vous ne pouvez pas créer de cas de support technique.

2. Service : si votre question concerne plusieurs services, choisissez le service le plus approprié.
3. Catégorie : choisissez la catégorie qui convient le mieux à votre cas d'utilisation. Lorsque vous choisissez une catégorie, des liens vers des informations susceptibles de résoudre votre problème apparaissent en-dessous.
4. Sévérité : les clients ayant un plan de support payant peuvent choisir le niveau de gravité General guidance (Recommandations générales) (temps de réponse d'un jour) ou System impaired (Système dégradé) (temps de réponse de 12 heures). Les clients avec un plan de support Business peuvent également choisir le niveau Production system impaired (Système de production dégradé) (temps de réponse de 4 heures) ou Production system down (Système de production défaillant) (temps de réponse d'une heure). Les clients disposant d'un plan de support Enterprise On-Ramp ou Enterprise peuvent choisir Business-critical system down (Système stratégique défaillant) (réponse en 15 minutes pour le support Enterprise et réponse en 30 minutes pour Enterprise On-Ramp).

   Les délais de réponse se rapportent à la première réponse fournie par AWS Support. Ils ne s'appliquent pas aux réponses ultérieures. Pour les problèmes se rapportant à des applications tierces, les temps de réponse peuvent être plus longs, en fonction de la disponibilité de personnel qualifié. Pour en savoir plus, consultez Choix du niveau de gravité.

   > **Note**
   >
   > En fonction de la catégorie choisie, des informations supplémentaires peuvent vous être demandées.

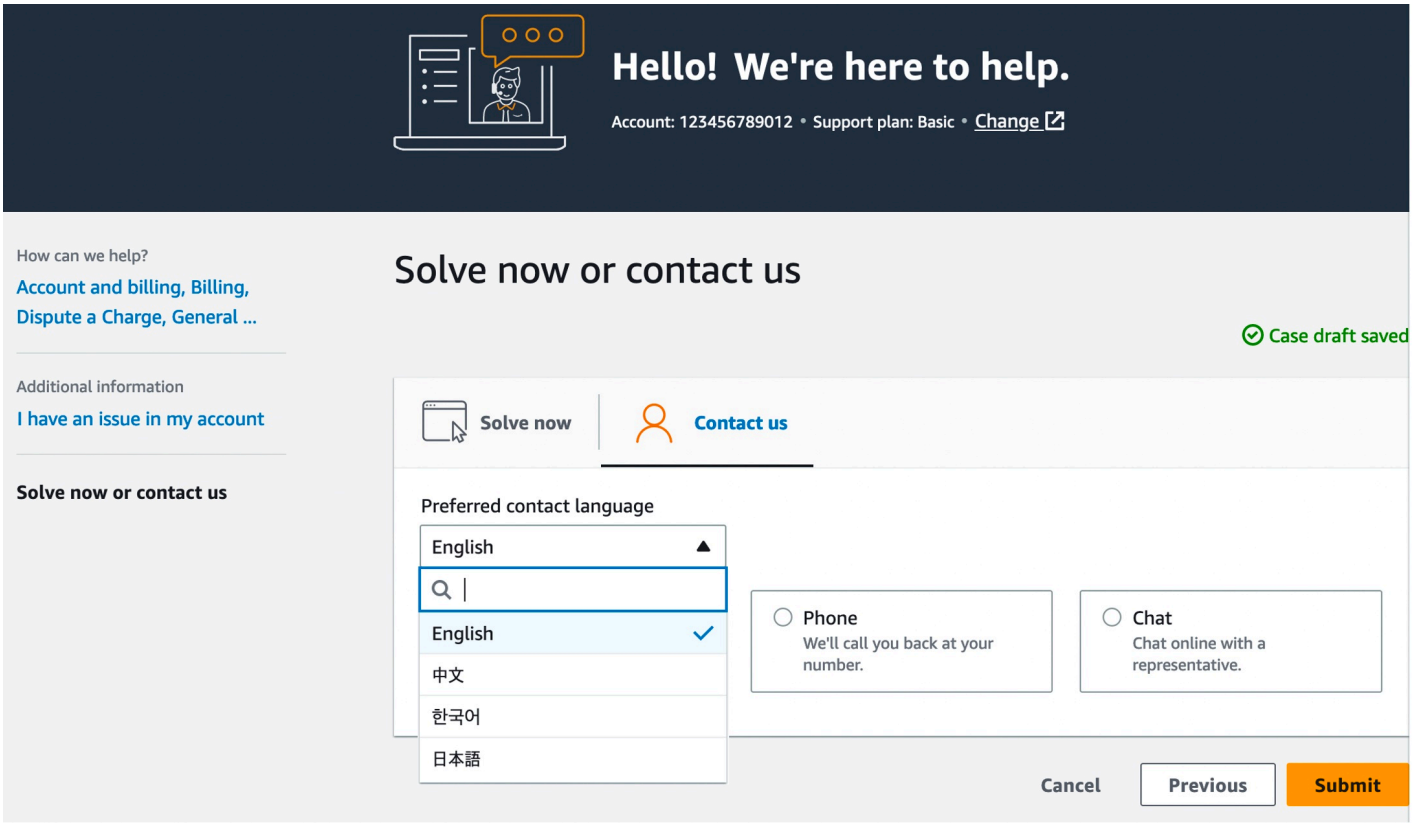
Après avoir spécifié le type de demande et sa catégorie, vous pouvez spécifier la description et la façon dont vous souhaitez être contacté.



1. Objet : entrez un titre qui décrit brièvement votre problème.

2. Description : décrivez votre cas de support. Il s'agit de l'information la plus importante fournie à AWS Support. Pour certaines combinaisons de services et de catégories, une invite apparaît avec des informations connexes. Utilisez ces liens pour vous aider à résoudre votre problème. Pour en savoir plus, consultez Description de votre problème.
3. Pièces jointes : joignez des captures d'écran et d'autres fichiers qui peuvent aider les agents de support à résoudre votre cas plus rapidement. Vous pouvez attacher jusqu'à 3 fichiers. La taille de chaque fichier peut aller jusqu'à 5 Mo.

Après avoir ajouté les détails de votre cas, vous pouvez choisir la méthode par laquelle vous souhaitez être contacté.



1. Langue de contact préférée : choisissez votre langue préférée. Actuellement, vous pouvez choisir l'anglais, le chinois, le coréen ou le japonais. Les options de contact personnalisées dans votre langue préférée s'afficheront dans votre plan de support.
2. Choisissez une méthode de contact. Les options de contact qui apparaissent dépendent du type de cas et de votre plan d'assistance.
   - Si vous choisissez Web, vous pouvez consulter et suivre la progression du cas dans le Centre de support.

- Choisissez Chat (Conversation instantanée) ou Phone (Téléphone). Si vous sélectionnez Téléphone, vous êtes invité à indiquer votre numéro de téléphone.

3. Cliquez sur le bouton Soumettre une fois que vous avez entré toutes les informations et que vous êtes prêt à créer la demande.

> **Note**
>
> Si vous choisissez le japonais comme langue de contact préférée pour les demandes de support, le support en japonais peut être disponible comme suit :
>
> - Si vous avez besoin d'un service client pour des demandes de support non techniques, ou si vous disposez d'un plan Developer Support et que vous avez besoin d'un support technique, le support en japonais est disponible pendant les heures ouvrables au Japon, de 9 h 00 à 18 h 00, Japan Standard Time (GMT+9), à l'exception des jours fériés et des week-ends.
> - Si vous possédez un plan de support Business, Enterprise On-Ramp ou Entreprise, les services de support technique en japonais sont disponibles 24 h/24, 7 j/7.
>
> Si vous choisissez le chinois comme langue de contact préférée pour les demandes de support, le support en chinois peut être disponible comme suit :
>
> - Si vous avez besoin d'un service client pour des demandes de support non techniques, le support en chinois est disponible de 9 h 00 à 18 h 00 (GMT+8), à l'exception des jours fériés et des week-ends.
> - Si vous disposez d'un plan Developer Support, le support technique en chinois est disponible pendant les heures ouvrables, généralement de 8 h 00 à 18 h 00 dans votre pays, comme indiqué dans la section Mon compte, à l'exception des jours fériés et des week-ends. Ces horaires peuvent varier dans les pays couverts par plusieurs fuseaux horaires.
> - Si vous disposez d'un plan de support Business, Enterprise On-Ramp ou Entreprise, le support technique en chinois est disponibles 24 h/24, 7 j/7.
>
> Si vous choisissez le coréen comme langue de contact préférée pour les demandes de support, le support en coréen peut être disponible comme suit :

- Si vous avez besoin d'un service client pour des demandes de support non techniques, le support en coréen est disponible pendant les heures ouvrables en Corée, de 9 h 00 à 18 h 00, Korean Standard Time (GMT+9), à l'exception des jours fériés et des week-ends.
- Si vous disposez d'un plan Developer Support, le support technique en coréen est disponible pendant les heures ouvrables, généralement de 8 h 00 à 18 h 00 dans votre pays, comme indiqué dans la section Mon compte, à l'exception des jours fériés et des week-ends. Ces horaires peuvent varier dans les pays couverts par plusieurs fuseaux horaires.
- Si vous disposez d'un plan de support Business, Enterprise On-Ramp ou Entreprise, le support technique en coréen est disponible 24 h/24, 7 j/7.

Création d'augmentation de quota de service

Pour améliorer les performances de votre service, demandez des augmentations de quota de service (anciennement désignés sous le nom de limites).

> **Note**
>
> Vous pouvez également utiliser le service Service Quotas pour demander des augmentations directement pour vos services. Actuellement, Service Quotas ne prend pas en charge les quotas de service pour tous les services. Pour plus d'informations, veuillez consulter la rubrique Qu'est-ce que Service Quotas ? dans le Guide de l'utilisateur Service Quotas.

Créez un cas de support pour demander une augmentation de quota de service

1. Connectez-vous à AWS Support Center Console.

   > **Tip**
   >
   > Dans la AWS Management Console, vous pouvez également choisir l'icône du point d'interrogation
   > (),
   > puis Support Center (Centre de support).

2. Choisissez Create case (Créer une demande).

3. Choisissez Looking for service limit increases? (Vous recherchez des augmentations de la limite de service ?)
4. Pour demander une augmentation, suivez les instructions. Les options possibles sont les suivantes :
   - Type de limite
   - Sévérité

   > **Note**
   >
   > En fonction de la catégorie choisie, des invites peuvent demander plus d'informations.
5. Pour Requests (Requêtes), choisissez la Region (Région).
6. Pour Limit (Limite), choisissez le type de limite de service.
7. Pour New limit value (Nouvelle valeur limite), saisissez la valeur que vous désirez.
8. Pour demander une augmentation de quota pour une autre région , choisissez Add another request (Ajouter une autre demande).
9. Pour Case description (Description du cas), décrivez votre cas de support.
10. Pour la page Contact options (Options de contact), choisissez votre langue préférée et la méthode par laquelle vous souhaitez être contacté. Vous pouvez choisir l'une des options suivantes :
    - Web : recevoir une réponse dans le Centre de support.
    - Conversation instantanée : initier un chat en direct avec un agent de support. Si vous ne parvenez pas à vous connecter à un chat, consultez Résolution des problèmes.
    - Téléphone : recevoir un appel téléphonique d'un agent de support. Si vous choisissez cette option, saisissez les informations suivantes :
      - Country/Region (Pays/Région)
      - Phone number (Numéro de téléphone)
      - (Optional) Extension (Extension [facultatif])
11. Sélectionnez Submit (Envoyer). Votre numéro d'ID de dossier et votre résumé apparaissent.

Mise à jour, surveillance, résolution et réouverture de votre cas

Après avoir créé votre cas de support, vous pouvez contrôler l'état de votre cas dans le Centre de support. L'état initial d'un nouveau cas est Unassigned. Lorsqu'un agent de support commence à traiter un cas, son état devient Work in Progress (Traitement en cours). L'agent de support répond à votre cas, soit en demandant plus d'informations (Pending Customer Action (Action client en attente)), soit en vous informant que la demande est en cours de vérification (Pending Amazon Action (Action Amazon en attente)).

Lorsque votre cas est mis à jour, vous recevez un e-mail avec la correspondance relative au cas et un lien vers le cas dans le Centre de support. Utilisez le lien contenu dans le message électronique pour accéder au cas de support. Vous ne pouvez pas répondre à la correspondance relative au cas par e-mail.

Remarques

- Vous devez vous connecter au Compte AWS qui a soumis le cas de support. Si vous vous connectez en tant qu'utilisateur AWS Identity and Access Management (IAM), vous devez disposer des autorisations requises pour afficher les cas de support. Pour de plus amples informations, veuillez consulter Gérer l'accès au AWS Support centre.
- Si vous ne répondez pas au cas dans un délai de quelques jours, AWS Support résout automatiquement le cas.
- Les cas de support qui ont été résolus depuis plus de 14 jours ne peuvent pas être rouverts. Si vous rencontrez un problème similaire lié au cas résolu, vous pouvez créer un cas connexe. Pour de plus amples informations, veuillez consulter Création d'un cas connexe.

Rubriques

Mise à jour d'un cas de support existant

Vous pouvez mettre à jour votre cas pour fournir plus d'informations à l'agent de support. Par exemple, vous pouvez répondre à des correspondances, démarrer un autre chat en direct, ajouter des destinataires, etc. Cependant, vous ne pouvez pas mettre à jour la gravité d'un cas une fois que vous l'avez créé. Pour de plus amples informations, veuillez consulter Choix du niveau de gravité.

Pour mettre à jour un cas de support existant

1. Connectez-vous à AWS Support Center Console.

   > **Tip**
   >
   > Dans la AWS Management Console, vous pouvez également choisir l'icône du point d'interrogation
   > (),
   > puis Support Center (Centre de support).

2. Sous Open support cases (Cas de support ouverts), choisissez Subject (Objet) du cas de support.
3. Choisissez Reply (Répondre). Dans Correspondence (Correspondance), vous pouvez également effectuer une ou plusieurs des modifications suivantes :
   - Fournir les informations demandées par l'agent de support
   - Charger des pièces jointes
   - Changer votre méthode de contact préférée
   - Ajouter des adresses e-mail pour recevoir des mises à jour sur le cas
4. Sélectionnez Submit (Envoyer).

> **Tip**
>
> Si vous avez fermé la fenêtre de chat et que vous souhaitez lancer un autre chat en direct, ajoutez une Reply (Réponse) à votre cas de support, choisissez Chat, puis Submit (Envoyer). Une nouvelle fenêtre de chat contextuelle s'ouvre.

Résoudre un cas de support

Lorsque vous êtes satisfait de la réponse ou que votre problème est résolu, vous pouvez résoudre le cas dans le Centre de support.

Pour résoudre un cas de support

1. Connectez-vous à AWS Support Center Console.

   > **Tip**
   >
   > Dans la AWS Management Console, vous pouvez également choisir l'icône du point d'interrogation
   > ( ),
   > puis Support Center (Centre de support).

2. Sous Open support cases (Cas de support ouverts), choisissez Subject (Objet) du cas de support que vous souhaitez résoudre.
3. (Facultatif) Choisissez Reply (Répondre) et dans la section Correspondence (Correspondance), entrez la raison pour laquelle vous résolvez le cas, puis choisissez Submit (Envoyer). Par exemple, vous pouvez entrer des informations sur la façon dont vous avez résolu le problème vous-même au cas où vous auriez besoin de ces informations pour une référence ultérieure.
4. Choisissez Resolve case (Résoudre le cas).
5. Dans la boîte de dialogue, choisissez OK pour résoudre le cas.

> **Note**
>
> Si AWS Support a résolu votre cas pour vous, vous pouvez utiliser le lien d'envoi de commentaires pour fournir plus d'informations sur votre expérience avec AWS Support.

Example : Liens d'envoi de commentaires

La capture d'écran suivante montre les liens de rétroaction dans la correspondance d'un cas dans le Centre de support.

Please let us know if we helped resolve your issue:

If YES, click here:
https://console.aws.amazon.com/support/feedback?eventId=1234567890&language=en&questionnaireId=Support-HMD-Yes

If NO, click here:
https://console.aws.amazon.com/support/feedback?eventId=1234567890&language=en&questionnaireId=Support-HMD-No

rouverte d'un cas résolu

Si vous rencontrez à nouveau le même problème, vous pouvez rouvrir le cas d'origine. Fournissez des détails sur la date à laquelle le problème s'est reproduit et les étapes de dépannage que vous avez essayées. Inclure tous les numéros de cas associés afin que l'agent de support puisse se référer aux correspondances précédentes.

Remarques

- Vous pouvez rouvrir votre cas de support jusqu'à 14 jours à compter de la résolution de votre problème. Toutefois, vous ne pouvez pas rouvrir un cas inactif depuis plus de 14 jours. Vous pouvez créer un nouveau cas ou un cas connexe. Pour de plus amples informations, veuillez consulter Création d'un cas connexe.
- Si vous rouvrez un cas existant qui contient des informations différentes de celles de votre problème actuel, l'agent de support peut vous demander de créer un nouveau cas.

Pour rouvrir un cas résolu

1. Connectez-vous à AWS Support Center Console.

   Tip

   Dans la AWS Management Console, vous pouvez également choisir l'icône du point d'interrogation
   ( ),
   puis Support Center (Centre de support).

2. Choisissez View all cases (Afficher tous les cas), puis sélectionnez Subject (Sujet) ou Case ID (ID de cas) du cas de support que vous souhaitez rouvrir.
3. Choisissez Reopen case (Rouvrir le cas).
4. Sous Correspondence (Correspondance), pour Reply (Répondre), entrez les détails du cas.
5. (Facultatif) Choisissez Choose files (Choisir les fichiers) pour joindre des fichiers à votre cas. Vous pouvez attacher jusqu'à 3 fichiers.
6. Pour Contact methods (Moyens de contact), choisissez l'une des options suivantes :
   - Web : recevez une notification par e-mail et par le Centre de support.
   - Conversation instantanée : chat en ligne avec un agent de support.
   - Téléphone : recevoir un appel téléphonique d'un agent de support.
7. (Facultatif) Pour Additional contacts (Autres contacts), entrez les adresses e-mail des autres personnes devant recevoir les correspondances sur les cas.
8. Vérifiez les détails de votre cas de support et choisissez Submit (Envoyer).

Création d'un cas connexe

Après 14 jours d'inactivité, vous ne pouvez pas rouvrir un cas résolu. Si vous rencontrez un problème similaire lié au cas résolu, vous pouvez créer un cas connexe. Ce cas connexe inclura un lien vers le cas précédemment résolu, afin que l'agent de support puisse examiner les détails et les correspondances du cas précédent. Si vous rencontrez un autre problème, nous vous recommandons de créer un nouveau cas.

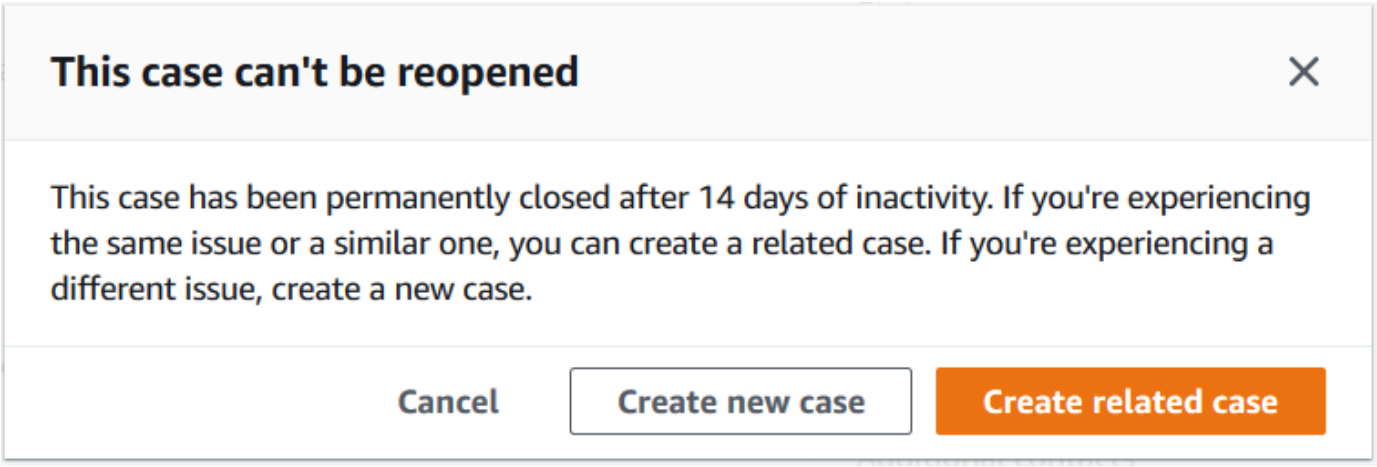
Pour créer un cas connexe

1. Connectez-vous à AWS Support Center Console.

   > **Tip**
   >
   > Dans la AWS Management Console, vous pouvez également choisir l'icône du point d'interrogation
   > (),
   > puis Support Center (Centre de support).

2. Choisissez View all cases (Afficher tous les cas), puis sélectionnez Subject (Sujet) ou Case ID (ID de cas) du cas de support que vous souhaitez rouvrir.

3. Choisissez Reopen case (Rouvrir le cas).
4. Dans la boîte de dialogue, choisissez Create related cas (Créer un cas connexe). Les informations relatives au cas précédent seront automatiquement ajoutées à votre cas connexe. Si vous avez un autre problème, choisissez Create a new case (Créer un nouveau cas).

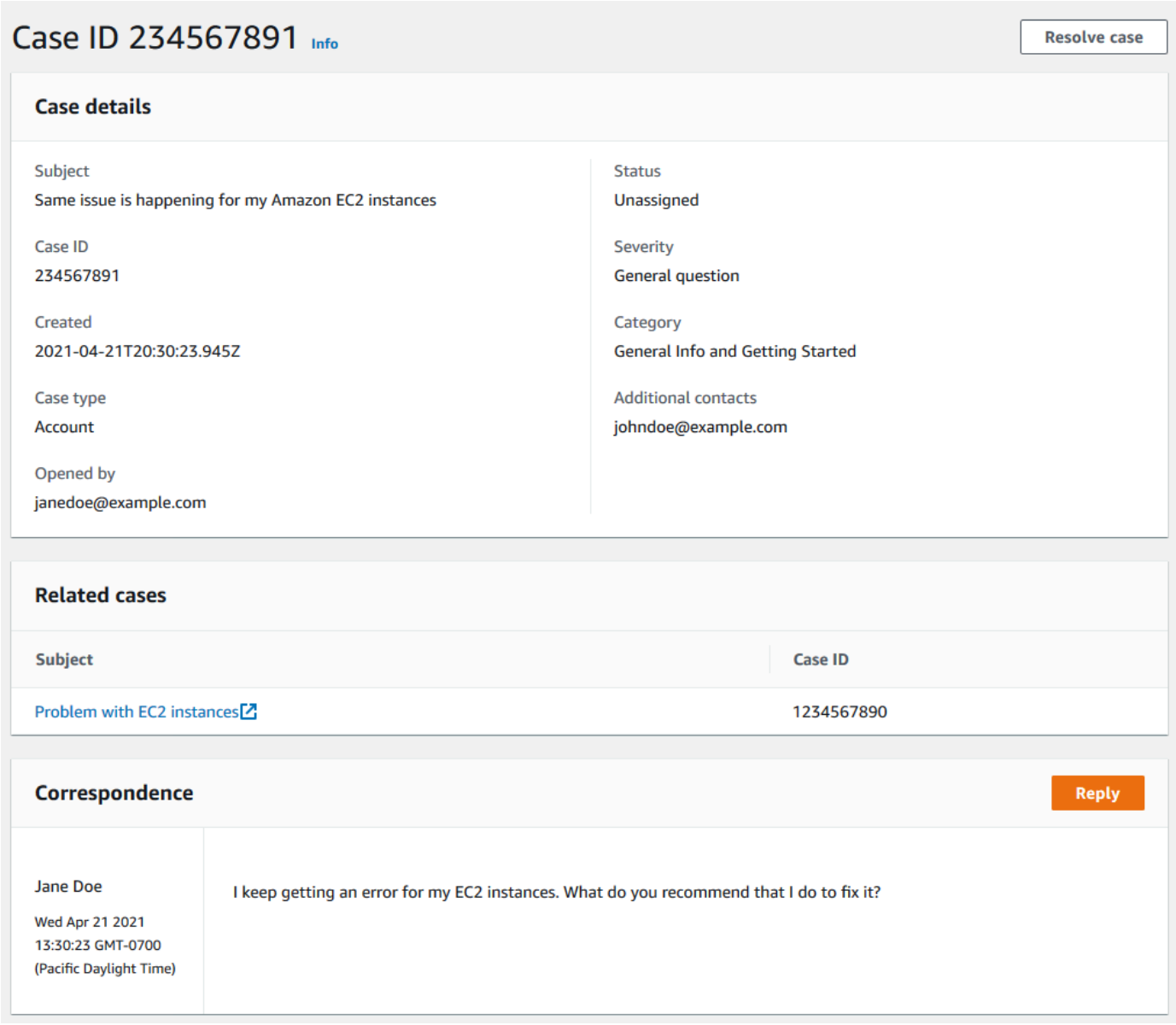


5. Suivez les étapes ci-après pour créer votre cas. Consultez Création d'un dossier de support.

> **Note**
>
> Par défaut, votre cas associé a les mêmes valeurs pour Type, Category (Catégorie) et Severity (Sévérité) que celles du cas précédent. Vous pouvez mettre à jour les détails du cas si nécessaire.

6. Vérifiez les détails de votre cas de support et choisissez Submit (Envoyer).

Une fois que vous avez créé votre cas, le cas précédent apparaît dans la fenêtreRelated cases (Cas connexes), comme dans l'exemple suivant.



Historique des demandes de support

Vous pouvez afficher les informations relatives à l'historique des demandes jusqu'à 24 mois après la création d'une demande.

Résolution des problèmes

Si vous rencontrez des problèmes lors de la création ou de la gestion de votre cas de support, consultez les informations de dépannage suivantes.

Je souhaite rouvrir un chat en direct pour mon cas

Vous pouvez répondre à votre cas de support existant pour ouvrir une autre fenêtre de chat. Pour en savoir plus, consultez Mise à jour d'un cas de support existant.

Je ne parviens pas à me connecter à un chat en direct

Si vous avez choisi l'option Chat, mais que vous ne parvenez pas à vous connecter à la fenêtre de chat, effectuez d'abord les vérifications suivantes :

- Assurez-vous d'avoir configuré votre navigateur pour autoriser les fenêtres contextuelles dans le Centre de support.

  > **Note**
  >
  > Vérifiez les paramètres de votre navigateur. Pour plus d'informations, consultez les sites web d'aide Chrome et d'assistance Firefox.

- Assurez-vous d'avoir configuré votre réseau de manière à pouvoir utiliser AWS Support :
  - Votre réseau a accès au point de terminaison `*.connect.us-east-1.amazonaws.com`.

    > **Note**
    >
    > Pour AWS GovCloud (US), le point de terminaison est `*.connect-fips.us-east-1.amazonaws.com`.

  - Votre pare-feu prend en charge les connexions socket web.

Si vous ne parvenez toujours pas à vous connecter à la fenêtre de chat, contactez AWS Support par e-mail ou par téléphone.

Utilisation de AWS Support avec un kit SDK AWS.

Les kits de développement (SDK) AWS sont disponibles pour de nombreux langages de programmation populaires. Chaque kit SDK fournit une API, des exemples de code et de la documentation qui facilitent la création d'applications par les développeurs dans leur langage préféré.

Documentation des kits SDK	Exemples de code
AWS SDK for C++	Exemples de code AWS SDK for C++
AWS SDK for Go	Exemples de code AWS SDK for Go
AWS SDK for Java	Exemples de code AWS SDK for Java
AWS SDK for JavaScript	Exemples de code AWS SDK for JavaScript
Kit AWS SDK pour Kotlin	Exemples de code Kit AWS SDK pour Kotlin
AWS SDK for .NET	Exemples de code AWS SDK for .NET
AWS SDK for PHP	Exemples de code AWS SDK for PHP
AWS SDK for Python (Boto3)	Exemples de code AWS SDK for Python (Boto3)
AWS SDK for Ruby	Exemples de code AWS SDK for Ruby
Kit AWS SDK pour Rust	Exemples de code Kit AWS SDK pour Rust
AWS SDK pour SAP ABAP	Exemples de code AWS SDK pour SAP ABAP
Kit AWS SDK pour Swift	Exemples de code Kit AWS SDK pour Swift

Exemple de disponibilité

Vous n'avez pas trouvé ce dont vous avez besoin ? Demandez un exemple de code en utilisant le lien Provide feedback (Fournir un commentaire) en bas de cette page.

À propos de l'API AWS Support

L'API AWS Support permet d'accéder à quelques-unes des fonctions du Centre de support AWS.

Actuellement, le service offre deux groupes d'opérations différents :

- Les opérations Gestion des demandes de support pour gérer l'ensemble du cycle de vie de vos demandes de support AWS, depuis la création d'une demande jusqu'à sa résolution.
- Opérations AWS Trusted Advisor d'accès aux vérifications AWS Trusted Advisor

> **Note**
>
> Vous devez posséder un plan de support Business, Enterprise On-Ramp ou Enterprise pour utiliser l'API AWS Support. Pour plus d'informations, consultez AWS Support.

Pour obtenir plus d'informations sur les opérations et les types de données fournis par AWS Support, consultez la référence à l'API AWS Support.

Rubriques

- Gestion des demandes de support
- AWS Trusted Advisor
- Points de terminaison
- Support dans les kits SDK AWS

Gestion des demandes de support

Vous pouvez utiliser l'API pour effectuer les tâches suivantes :

- Soumettre une demande de support.
- Obtenir une liste de vos demandes de support récentes et des informations détaillées sur celles-ci.
- Filtrer votre recherche de demandes de support en fonction de leurs dates et identificateurs, y compris les demandes résolues.

- Ajoutez des communications et des pièces jointes à vos demandes de support, et ajoutez les adresses e-mail des destinataires pour la correspondance relative aux demandes de support. Vous pouvez attacher jusqu'à 3 fichiers. La taille maximale de chaque fichier est de 5 Mo.
- Résoudre vos demandes de support.

L'AWS SupportAPI prend en charge la CloudTrail journalisation pour les opérations de gestion des dossiers d'assistance. Pour en savoir plus, consultez Journalisation des appels d'API AWS Support avec AWS CloudTrail.

Pour obtenir des exemples de code illustrant comment gérer l'ensemble du cycle de vie d'un dossier de support, consultez Exemples de code AWS Support à l'aide des AWS SDK (français non garanti).

AWS Trusted Advisor

Vous pouvez utiliser les opérations Trusted Advisor pour effectuer les tâches suivantes :

- Obtenir les noms et les identificateurs pour les vérifications Trusted Advisor.
- Demander l'exécution d'une vérification Trusted Advisor sur votre compte et vos ressources AWS.
- Obtenir des résumés et des informations détaillées pour vos vérifications Trusted Advisor.
- Actualiser vos vérifications Trusted Advisor
- Obtenir l'état de chaque vérification Trusted Advisor

L'AWS SupportAPI prend en charge la CloudTrail journalisation des Trusted Advisor opérations. Pour en savoir plus, consultez Informations AWS Trusted Advisor dans la consignation CloudTrail.

Vous pouvez utiliser Amazon CloudWatch Events pour surveiller les modifications apportées aux résultats de vos vérificationsTrusted Advisor. Pour en savoir plus, consultez Surveillance des résultats des AWS Trusted Advisor contrôles avec Amazon EventBridge.

Pour un exemple de code Java qui explique comment utiliser les opérations Trusted Advisor, consultez Utilisation de Trusted Advisor en tant que service web.

Points de terminaison

AWS Support est un service global. Cela signifie que tout point de terminaison que vous utilisez mettra à jour vos dossiers de support dans la Support Center Console.

Par exemple, si vous utilisez le point de terminaison USA Est (Virginie du Nord) pour créer un dossier, vous pouvez utiliser le point de terminaison USA Ouest (Oregon) ou Europe (Irlande) pour ajouter une correspondance au même dossier.

Vous pouvez utiliser les points de terminaison suivants pour accéder à l'API AWS Support :

- USA Est (Virginie du Nord) – https://support.us-east-1.amazonaws.com
- USA Ouest (Oregon) – https://support.us-west-2.amazonaws.com
- Europe (Irlande) – https://support.eu-west-1.amazonaws.com

> **Important**
>
> - Si vous appelez l'CreateCaseopération pour créer des demandes de support relatives aux tests, nous vous recommandons d'inclure une ligne d'objet, telle que TEST CASE-please ignore. Une fois que vous avez terminé le test de votre demande d'assistance, appelez l'ResolveCaseopération pour la résoudre.
> - Pour appeler les opérations AWS Trusted Advisor dans l'API AWS Support, vous devez utiliser le point de terminaison USA Est (Virginie du Nord). Actuellement, les points de terminaison USA Ouest (Oregon) et Europe (Irlande), ne prennent pas en charge les opérations Trusted Advisor.

Pour de plus amples informations sur les points de terminaison AWS, veuillez consulter Points de terminaison et quotas AWS Support dans le Référence générale d'Amazon Web Services.

Support dans les kits SDK AWS

Le AWS Command Line Interface (AWS CLI) et le kit SDK AWS incluent le support pour l'API AWS Support.

Pour obtenir la liste des langues compatibles avec l'AWS SupportAPI, choisissez un nom d'opération, par exemple CreateCase, et dans la section Voir aussi, choisissez votre langue préférée.

AWS Support Plans

Vous pouvez modifier AWS Support les forfaits de votre compte en fonction des besoins de votre entreprise.

Rubriques

Caractéristiques des AWS Support plans

AWS Support propose cinq plans de support :

- Base
- Developer
- Entreprise
- Enterprise On-Ramp
- Enterprise

Le plan Basic offre un support pour les questions relatives aux comptes, à la facturation et aux augmentations de quota du service. Les autres plans proposent un certain nombre de cas de support technique assortis de pay-by-the-month tarifs et sans contrats à long terme.

Tous les AWS clients ont automatiquement accès 24 h/24 et 7 j/7 aux fonctionnalités suivantes du Support de base :

- O ne-on-one réponses aux questions relatives au compte et à la facturation
- Forums de support
- Vérifications de l'état du service
- Documentation, publications techniques et guides des bonnes pratiques

Les clients disposant d'un plan de support Developer ont accès aux fonctionnalités supplémentaires suivantes :

- Assistance concernant les bonnes pratiques
- Outils de diagnostic client
- Support de l'architecture modulaire : conseils sur la façon d'utiliser les AWS produits, les fonctionnalités et les services ensemble
- Prend en charge un nombre illimité de demandes d'assistance qui peuvent être ouvertes par n'importe quel utilisateur autorisé.

En outre, les clients possédant un plan de support Business, Enterprise On-Ramp ou Enterprise ont accès aux fonctionnalités suivantes :

- Conseils d'utilisation : quels AWS produits, fonctionnalités et services utiliser pour répondre au mieux à vos besoins spécifiques.
- AWS Trusted Advisor— Une fonctionnalité de AWS Support, qui inspecte les environnements des clients et identifie les opportunités d'économiser de l'argent, de combler les failles de sécurité et d'améliorer la fiabilité et les performances du système. Vous pouvez accéder à tous les Trusted Advisor chèques.
- L' AWS Support API pour interagir avec le Support Center et Trusted Advisor. Vous pouvez utiliser l'API AWS Support pour automatiser la gestion des cas de support et les opérations Trusted Advisor .
- Prise en charge de logiciels tiers : assistance pour les systèmes d'exploitation d'instance Amazon Elastic Compute Cloud (Amazon EC2) et configuration. Aidez également à améliorer les performances des composants logiciels tiers les plus populaires sur AWS. Le support logiciel tiers n'est pas disponible pour les clients ayant des plans de support Basic ou Developer.
- Prend en charge un nombre illimité d'utilisateurs AWS Identity and Access Management (IAM) qui peuvent ouvrir des dossiers de support technique.

En outre, les clients possédant un plan de support Enterprise On-Ramp ou Enterprise ont accès aux fonctionnalités suivantes :

- Conseils du support d'architecture des applications : des directives concernant la façon dont les services s'accordent pour satisfaire votre cas d'utilisation, votre charge de travail ou votre application spécifiques.
- Gestion des événements de l'infrastructure : engagement à court terme avec AWS Support pour avoir une compréhension approfondie de votre cas d'utilisation. Après analyse, fournissez des conseils d'architecture et de mise à l'échelle pour un événement.

- Responsable de compte technique : collaborez avec un gestionnaire de compte technique (TAM) pour vos cas d'utilisation et applications spécifiques.
- Traitement sur mesure des cas
- Suivi des activités de gestion.

Pour plus d'informations sur les fonctionnalités et les tarifs de chaque plan de support, consultez AWS Supportet comparez les AWS Support plans. Certaines fonctionnalités, telles que la prise en charge par téléphone et par chat 24 h/24, 7 j/7, ne sont pas disponibles dans toutes les langues.

Modifier les AWS Support plans

Vous pouvez utiliser la console AWS Support Plans pour modifier votre plan de support pour votre Compte AWS. Pour modifier votre plan de support, vous devez disposer des autorisations AWS Identity and Access Management (IAM) ou vous connecter à votre compte en tant qu'utilisateur root. Pour plus d'informations, consultez Gérez l'accès aux AWS Support plans et AWS politiques gérées pour les AWS Support plans.

Pour modifier votre plan d'assistance

1. Connectez-vous à la console AWS Support Plans à l'adresse https://console.aws.amazon.com/support/plans/home.
2. (Facultatif) Sur la page AWS Support Plans, comparez les plans de support. Pour plus d'informations sur la tarification, visitez la page de détails sur la tarification.
3. (Facultatif) Sous AWS Support pricing example (Exemple de tarification), sélectionnez See examples (Voir les exemples), puis choisissez l'une des options de plan de support pour voir le coût estimé.
4. Lorsque vous choisissez un plan, sélectionnez Review downgrade (Examiner le déclassement) ou Review upgrade (Examiner la mise à niveau) pour le plan que vous voulez.

> **Remarques**
>
> - Si vous vous inscrivez à un plan de support payant, vous êtes responsable d'un abonnement d'un mois minimum d' AWS Support. Pour plus d'informations, consultez la FAQ AWS Support.

- Si vous disposez d'un plan Enterprise On-Ramp ou Enterprise Support, dans la boîte de dialogue Change plan confirmation (Confirmation de la modification du plan), contactez AWS Support pour modifier votre plan de support.

5. Dans la boîte de dialogue Change plan confirmation (Confirmation de la modification du plan), vous pouvez développer les éléments de support pour voir les fonctionnalités que vous voulez ajouter ou supprimer de votre compte.

   Sous Pricing (Tarification), vous pouvez voir les frais uniques prévus pour le nouveau plan de support.
6. Cliquez sur Accept and agree (Accepter et convenir).

Informations connexes

Pour plus d'informations sur AWS Support les forfaits, consultez les AWS Support FAQ. Vous pouvez également choisir Contact us (Contactez-nous) dans la console Support Plans.

Pour fermer votre compte, consultez Clôture d'un compte dans le Guide de l'utilisateur AWS Billing .

AWS Trusted Advisor

Trusted Advisor s'appuie sur les meilleures pratiques apprises en servant des centaines de milliers de AWS clients. Trusted Advisor inspecte votre AWS environnement, puis émet des recommandations lorsque des opportunités se présentent pour économiser de l'argent, améliorer la disponibilité et les performances du système ou contribuer à combler les failles de sécurité.

Si vous disposez d'un plan Basic ou d'un plan Support pour les développeurs, vous pouvez utiliser la Trusted Advisor console pour accéder à tous les contrôles de la catégorie Limites de service et à six contrôles de la catégorie Sécurité.

Si vous avez un plan Business, Enterprise On-Ramp ou Enterprise Support, vous pouvez utiliser la Trusted Advisor console et l'AWS Trusted Advisor API pour accéder à toutes les Trusted Advisor vérifications. Vous pouvez également utiliser Amazon CloudWatch Events pour surveiller le statut des Trusted Advisor chèques. Pour plus d'informations, consultez Surveillance des résultats des AWS Trusted Advisor contrôles avec Amazon EventBridge.

Vous pouvez accéder Trusted Advisor dans le AWS Management Console. Pour plus d'informations sur le contrôle de l'accès à la Trusted Advisor console, consultezGérez l'accès à AWS Trusted Advisor.

Pour plus d'informations, voir Trusted Advisor.

Rubriques

- Démarrer avec Trusted Advisor Recommendations
- Commencez avec l'Trusted AdvisorAPI
- Utilisation de Trusted Advisor en tant que service web
- Vue organisationnelle pour AWS Trusted Advisor
- Afficher les contrôles AWS Trusted Advisor optimisés par AWS Config
- Affichage des contrôles AWS Security Hub dans AWS Trusted Advisor
- Inscription à AWS Compute Optimizer pour les vérifications de Trusted Advisor
- Démarrer avec AWS Trusted Advisor Priority
- Commencer avec AWS Trusted Advisor Engage (version préliminaire)
- Référence de la vérification AWS Trusted Advisor
- Journal des modifications pour AWS Trusted Advisor

Démarrer avec Trusted Advisor Recommendations

Vous pouvez utiliser la page Trusted Advisor Recommendations de la console Trusted Advisor pour consulter les résultats de vérification de votre Compte AWS, puis suivre les étapes recommandées pour résoudre les problèmes. Par exemple, Trusted Advisor peut vous recommander de supprimer des ressources inutilisées pour réduire votre facture mensuelle, telles qu'une instance Amazon Elastic Compute Cloud (Amazon EC2).

Vous pouvez également utiliser l'API AWS Trusted Advisor pour effectuer des opérations sur vos vérifications Trusted Advisor. Pour plus d'informations, consultez le Guide de référence des AWS Trusted Advisor API

Rubriques

Connectez-vous à la console Trusted Advisor.

Vous pouvez afficher les vérifications et l'état de chaque vérification dans la console Trusted Advisor.

> **Note**
>
> Pour accéder à la console Trusted Advisor, vous devez disposer d'un ensemble minimum d'autorisations AWS Identity and Access Management (IAM). Pour plus d'informations, consultez Gérez l'accès à AWS Trusted Advisor.

Pour se connecter à la console Trusted Advisor

1. Accédez à la console Trusted Advisor sur https://console.aws.amazon.com/trustedadvisor/home.

2. Dans la page Trusted Advisor Recommendations, affichez le résumé de chaque catégorie de vérification :

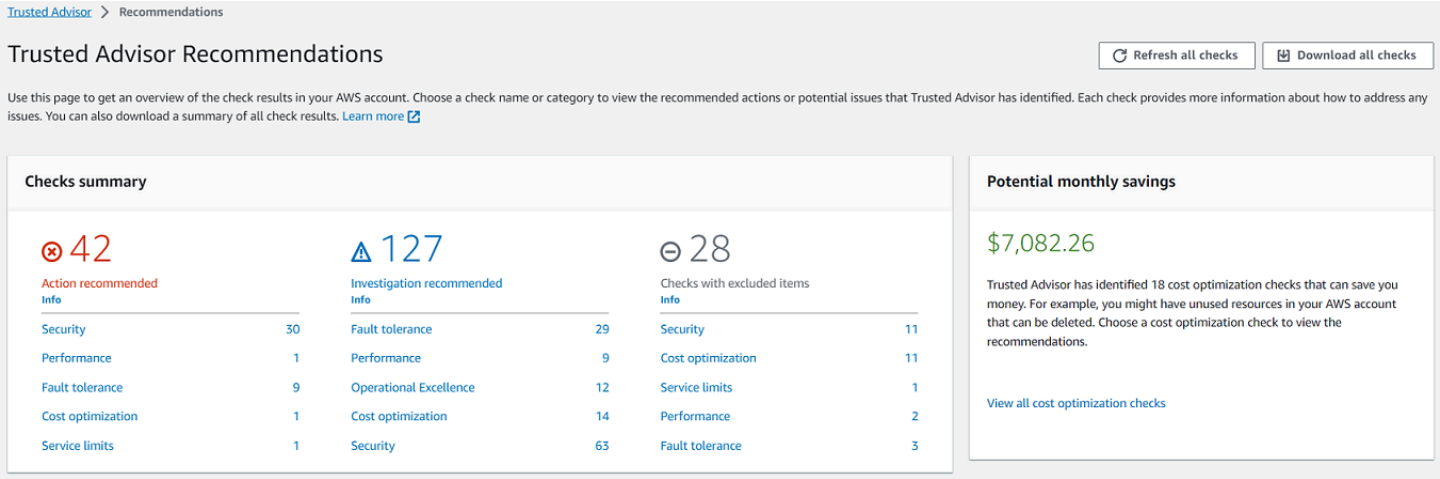
   - Action recommandée (rouge) : Trusted Advisor recommande une action pour la vérification. Par exemple, une vérification qui détecte un problème de sécurité pour vos ressources IAM peut recommander des étapes urgentes.
   - Investigation recommandée (jaune) : Trusted Advisor détecte un problème possible pour la vérification. Par exemple, une vérification qui atteint un quota pour une ressource peut recommander des moyens de supprimer des ressources inutilisées.
   - Vérifications avec des éléments exclus (gris) : nombre de vérifications qui ont exclu des éléments, tels que les ressources que vous souhaitez ignorer. Par exemple, il peut s'agir d'instances Amazon EC2 que vous ne souhaitez pas que la vérification évalue.

3. Sur la page Trusted Advisor Recommendations, vous pouvez effectuer les opérations suivantes :

   - Pour actualiser tous les vérifications de votre compte, choisissez Refresh all checks (Actualiser toutes les vérifications).
   - Pour créer un fichier .xls qui inclut tous les résultats de vérification, choisissez Download all checks (Télécharger toutes les vérifications).
   - Sous Checks Summary (Résumé des vérifications), choisissez une catégorie de vérification, telle que Security (Sécurité), pour afficher les résultats.
   - Sous Potential Monthly Savings (Économies mensuelles potentielles), vous pouvez voir combien vous pouvez économiser pour votre compte et les vérifications d'optimisation des coûts pour les recommandations.
   - Sous Recent changes (Changements récents), vous pouvez afficher les modifications des états des vérifications au cours des 30 derniers jours. Choisissez un nom de vérification pour afficher les derniers résultats de cette vérification ou choisissez l'icône de flèche pour afficher la page suivante.

Example : Trusted Advisor Recommendations

L'exemple suivant montre le résumé des résultats de la vérification d'un Compte AWS.



Afficher les catégories de vérifications

Vous pouvez afficher les descriptions et les résultats des vérifications pour les catégories de vérifications suivantes :

- Cost Optimization (Optimisation des coûts) : des recommandations qui peuvent potentiellement vous faire économiser de l'argent. Ces vérifications mettent en évidence les ressources inutilisées et les possibilités de réduire votre facture.
- Performances : des recommandations qui peuvent améliorer la rapidité et la réactivité de vos applications.
- Sécurité : des recommandations pour les paramètres de sécurité qui peuvent rendre votre solution AWS plus sécurisée.
- Tolérance aux pannes : des recommandations qui aident à augmenter la résilience de votre solution AWS. Ces vérifications mettent en évidence les lacunes en matière de redondance et la surutilisation des ressources.
- Service Limits : vérifie l'utilisation de votre compte et si votre compte approche ou dépasse la limite (également appelée quotas) pour les services et ressources AWS.
- Excellence opérationnelle : recommandations pour vous aider à exploiter votre environnement AWS de manière efficace et à grande échelle.

Pour afficher les catégories de vérifications

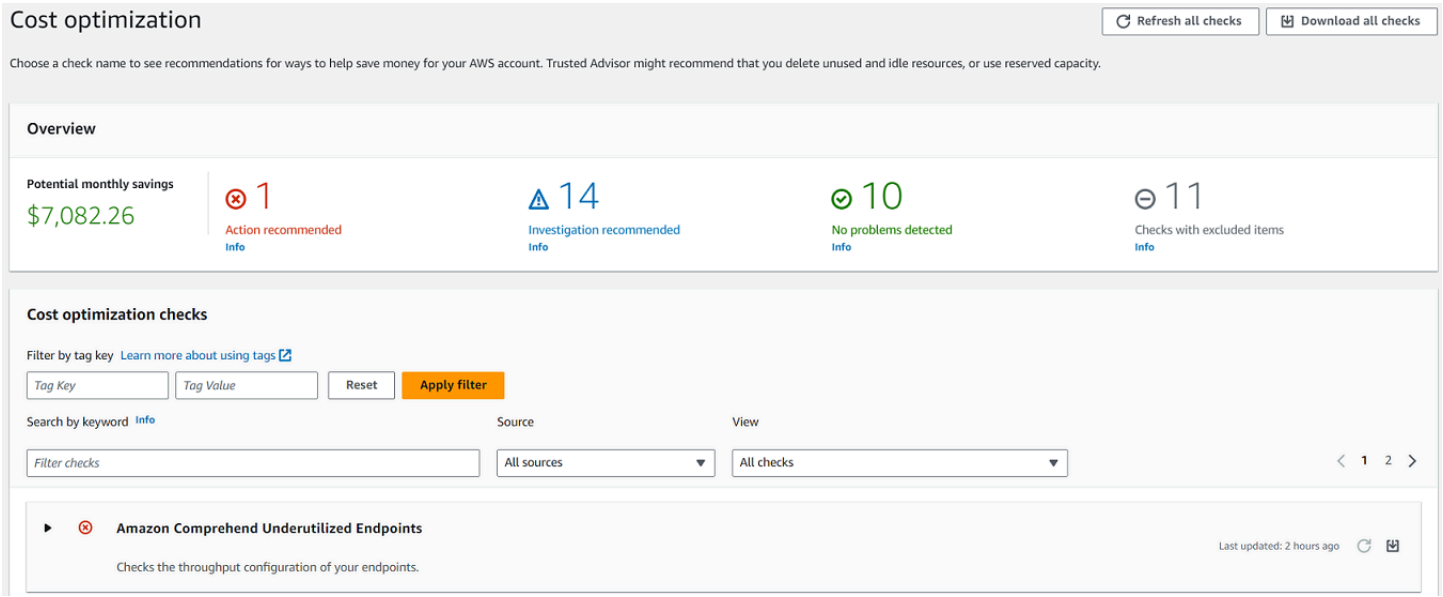
1. Accédez à la console Trusted Advisor sur https://console.aws.amazon.com/trustedadvisor/home.
2. Dans le panneau de navigation, choisissez la catégorie des vérifications.
3. Dans la page des catégories, affichez le résumé de chaque catégorie de vérification :

- Action recommandée (rouge) :Trusted Advisor recommande une action pour la vérification.
- Investigation recommandée (jaune) : Trusted Advisor détecte un problème possible pour la vérification.
- Aucun problème détecté (vert) : Trusted Advisor ne détecte pas de problème pour la vérification.
- Éléments exclus (gris) : nombre de vérifications qui ont exclu des éléments, tels que les ressources que vous souhaitez ignorer.

4. Pour chaque vérification, choisissez l'icône Actualiser
   ( )
   pour actualiser cette vérification.
5. Choisissez l'icône de téléchargement
   ( )
   pour créer un fichier .xls qui inclut les résultats de cette vérification.

Example : catégorie Cost Optimization (Optimisation des coûts)

L'exemple suivant montre 16 vérifications (vertes) qui n'ont aucun problème.



Afficher des vérifications spécifiques

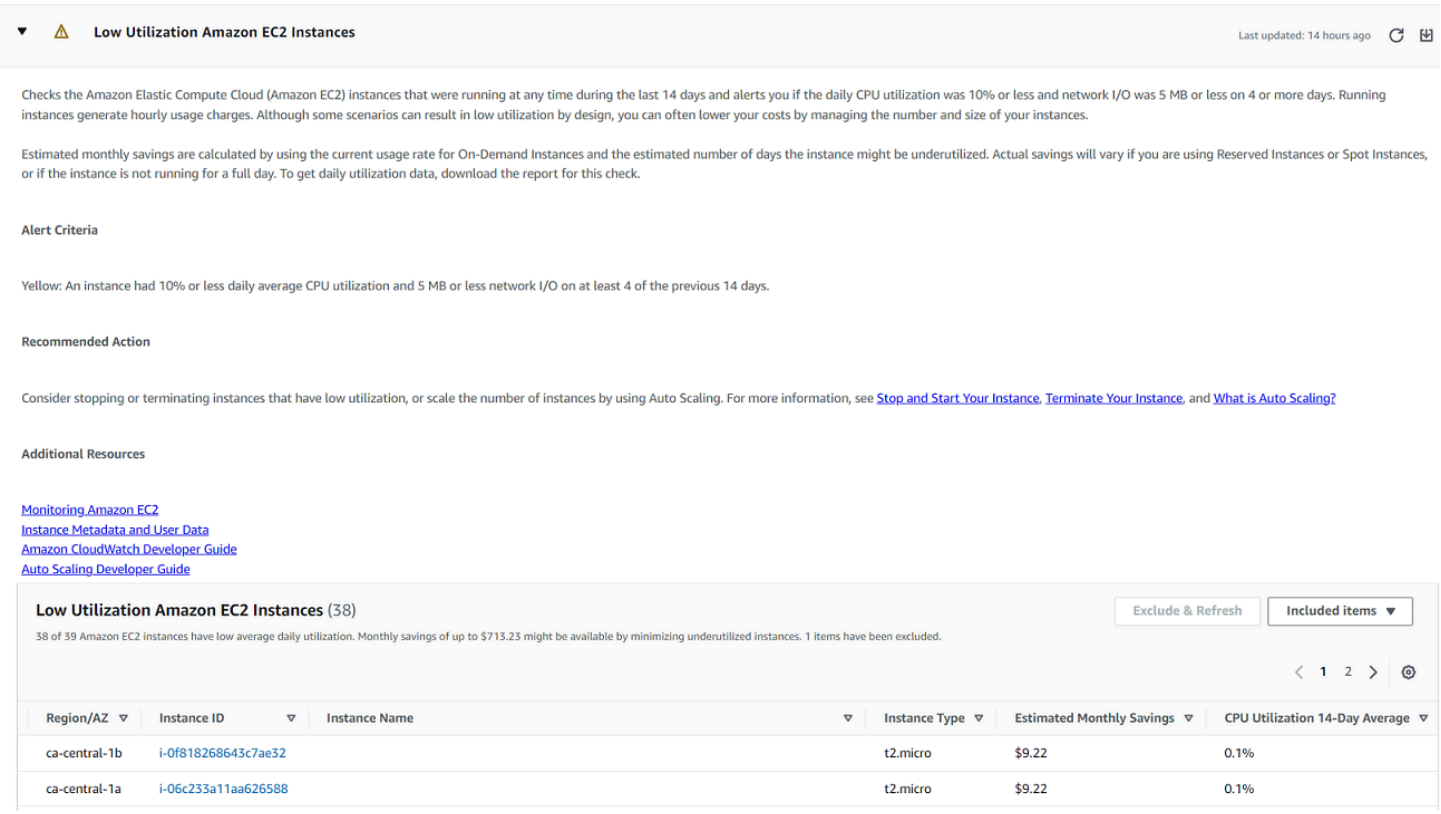
Développez une vérification pour afficher la description complète de la vérification, les ressources affectées, les étapes recommandées et les liens vers plus d'informations.

Pour afficher une vérification spécifique

1. Accédez à la console Trusted Advisor sur https://console.aws.amazon.com/trustedadvisor/home.
2. Dans le panneau de navigation, choisissez une catégorie de vérification.
3. Choisissez le nom de la vérification pour afficher la description et les détails suivants :
   - Alert Criteria (Critères d'alerte) : décrit le seuil à partir duquel une vérification va changer d'état.
   - Recommended Action (Action recommandée) : décrit les actions recommandées pour cette vérification.
   - Additional Resources (Ressources supplémentaires) : Listes relatives à la documentation AWS.
   - Tableau qui répertorie les éléments concernés de votre compte. Vous pouvez inclure ou exclure ces éléments des résultats de vérification.
4. (Facultatif) Pour exclure les éléments afin qu'ils n'apparaissent pas dans les résultats de vérification :
   a. Sélectionnez un élément et choisissez Exclude & Refresh (Exclure et actualiser).
   b. Pour afficher tous les éléments exclus, choisissez Excluded items (Éléments exclus).
5. (Facultatif) Pour inclure des éléments afin que la vérification les évalue à nouveau :
   a. Choisissez Excluded items (Éléments exclus), sélectionnez un élément, puis choisissez Include & Refresh (Inclure et actualiser).
   b. Pour afficher tous les éléments inclus, choisissez Included items (Éléments inclus).
6. Choisissez l'icône de paramètres ().
   Dans la boîte de dialogue Preferences (Préférences), vous pouvez spécifier le nombre d'éléments ou les propriétés à afficher, puis choisir ensuite Confirm (Confirmer).

Example : vérification de Cost Optimization (Optimisation des coûts)

La vérification Low Utilization Amazon EC2 Instances (Instances Amazon EC2 sous-exploitées) suivante répertorie les instances concernées dans le compte. Cette vérification identifie 38 instances Amazon EC2 dont l'utilisation est faible et vous recommande d'arrêter ou de terminer les ressources.



Filtrer vos vérifications

Dans les pages des catégories de vérification, vous pouvez spécifier les résultats de vérification que vous souhaitez afficher. Par exemple, vous pouvez filtrer par vérifications qui ont détecté des erreurs dans votre compte, afin que vous puissiez d'abord examiner les problèmes urgents.

Si vous avez des vérifications qui évaluent les éléments de votre compte, tels que les ressources AWS, vous pouvez utiliser des filtres de balises pour afficher uniquement les éléments qui ont la balise spécifiée.

Pour filtrer vos vérifications

1. Accédez à la console Trusted Advisor sur https://console.aws.amazon.com/trustedadvisor/home.
2. Dans le volet de navigation ou la page Trusted Advisor Recommendations, choisissez la catégorie de vérification.
3. Pour Search by keyword (Recherche par mot-clé), saisissez un mot-clé à partir du nom de la vérification ou de la description pour filtrer les résultats.
4. Pour la liste View (Afficher), spécifiez les vérifications à afficher :

    - All checks (Toutes les vérifications) : répertorie toutes les vérifications pour cette catégorie

- Action recommended (Action recommandée) : liste les vérifications qui vous recommandent de prendre des mesures. Ces vérifications sont mises en évidence en rouge.
- Investigation recommended (Investigation recommandée) : liste les vérifications qui vous recommandent de prendre de possibles mesures. Ces vérifications sont mises en évidence en jaune.
- No problems detected (Aucun problème détecté) : liste les vérifications qui n'ont aucun problème. Ces vérifications sont mises en évidence en vert.
- Checks with excluded items (Vérifications avec les éléments exclus) : répertorie les vérifications que vous avez spécifiées pour exclure les éléments des résultats de vérification.

5. Si vous avez ajouté des balises à vos ressources AWS, telles que les instances Amazon EC2 ou AWS CloudTrail, vous pouvez filtrer vos résultats de sorte que les vérifications n'affichent que les éléments qui ont la balise spécifiée.

   Pour Filter by tag (Filtrer par balise), entrez une clé de balise et une valeur de balise, puis choisissez Apply filter (Appliquer le filtre).
6. Dans le tableau de la vérification, les résultats de la vérification affichent uniquement les éléments qui ont la clé et la valeur spécifiées.
7. Pour effacer le filtre par balises, choisissez Reset (Réinitialiser).

Informations connexes

Pour plus d'informations sur le balisage d'objets pour Trusted Advisor, consultez les rubriques suivantes :

- AWS Support active les fonctionnalités de balisage pour Trusted Advisor
- Balisage des ressources AWS dans le Références générales AWS

Actualiser les résultats de vérifications

Vous pouvez actualiser les vérifications afin d'obtenir les derniers résultats pour votre compte. Si vous possédez un plan de support Developer ou Basic, vous pouvez vous connecter à la console de Trusted Advisor pour actualiser les vérifications. Si vous possédez un plan de support Business, Enterprise On-Ramp ou Enterprise, Trusted Advisor actualise automatiquement les vérifications de votre compte de manière hebdomadaire.

Pour actualiser les vérifications Trusted Advisor

1. Accédez à la console AWS Trusted Advisor sur https://console.aws.amazon.com/trustedadvisor.
2. Sur la page Trusted Advisor Recommendations ou sur une page de catégorie de vérification, choisissez Refresh all checks (Actualiser toutes les vérifications).

Vous pouvez aussi actualiser des vérifications spécifiques des manières suivantes :

- Choisissez l'icône d'actualisation () pour une vérification individuelle.
- Utilisez l'opération d'API RefreshTrustedAdvisorCheck.

> Remarques
>
> - Trusted Advisor actualise automatiquement certaines vérifications plusieurs fois par jour, comme la vérification des problèmes à haut risque pour la fiabilité AWS Well-Architected. Les modifications peuvent prendre quelques heures pour s'afficher dans votre compte. Pour ces vérifications automatiquement actualisées, vous ne pouvez pas choisir l'icône d'actualisation () pour actualiser manuellement les résultats.
> - Si vous avez activé AWS Security Hub pour votre compte, vous ne pouvez pas utiliser la console Trusted Advisor pour actualiser les vérifications de Security Hub. Pour en savoir plus, consultez Actualiser les résultats de Security Hub.

Télécharger les résultats des vérifications

Vous pouvez télécharger les résultats de vérification pour obtenir un aperçu de Trusted Advisordans votre compte. Vous pouvez télécharger les résultats pour toutes les vérifications ou une vérification spécifique.

Pour télécharger les résultats de la vérification depuis Trusted Advisor Recommendations

1. Accédez à la console AWS Trusted Advisor sur https://console.aws.amazon.com/trustedadvisor.

- Pour télécharger tous les résultats de la vérification, sur la page Trusted Advisor Recommendations ou sur une page de catégorie de vérification, choisissez Download all checks (Télécharger toutes les vérifications).
- Pour télécharger un résultat de vérification pour une vérification spécifique, choisissez le nom de la vérification, puis choisissez l'icône de téléchargement ( )

2. Enregistrez ou ouvrez le fichier .xls. Le fichier contient les mêmes informations de résumé provenant de la console Trusted Advisor, telles que le nom de vérification, la description, l'état, les ressources affectées, etc.

Vue organisationnelle

Vous pouvez utiliser la vue organisationnelle pour créer un rapport pour tous les comptes des membres de votre organisation AWS. Pour plus d'informations, consultez Vue organisationnelle pour AWS Trusted Advisor.

Préférences

Sur la page Gérer Trusted Advisor, vous pouvez désactiver Trusted Advisor.

Sur la page Notifications, vous pouvez configurer vos e-mails hebdomadaires pour le résumé des vérifications. Consultez Configuration des préférences de notification.

Sur la page Votre organisation, vous pouvez activer ou désactiver l'accès sécurisé avec AWS Organizations. Ceci est requis pour la fonctionnalité Vue organisationnelle pour AWS Trusted Advisor, pour Trusted Advisor Priority et pour Trusted Advisor Engage.

Configuration des préférences de notification

Spécifiez qui peut recevoir les messages électroniques Trusted Advisor hebdomadaires pour les résultats de vérification et la langue. Vous recevez une notification par e-mail sur votre résumé de vérification pour Trusted Advisor Recommendations une fois par semaine.

Les notifications par e-mail pour Trusted Advisor Recommendations n'incluent pas les résultats pour Trusted Advisor Priority. Pour en savoir plus, consultez Gestion des notifications de Trusted Advisor Priority.

Pour configurer des préférences de notification

1. Accédez à la console Trusted Advisor sur https://console.aws.amazon.com/trustedadvisor/home.
2. Dans le panneau de navigation, sous Preferences (Préférences), choisissez Notifications.
3. Dans Recommendations (Recommandations), sélectionnez qui doit être prévenu de vos résultats de vérification. Vous pouvez ajouter et supprimer des contacts dans la page Account Settings (Paramètres de compte) dans la console AWS Billing and Cost Management.
4. Pour Language (Langue), choisissez la langue du message électronique.
5. Choisissez Save your preferences (Enregistrer vos préférences).

Configurer la vue organisationnelle

Si vous configurez votre compte avec AWS Organizations, vous pouvez créer des rapports pour tous les comptes membres de votre organisation. Pour plus d'informations, consultez Vue organisationnelle pour AWS Trusted Advisor.

Désactiver Trusted Advisor

Lorsque vous désactivez ce service, Trusted Advisor n'effectuera aucune vérification sur votre compte. Toute personne qui essaie d'accéder à la console Trusted Advisor ou utiliser les opérations API recevra un message d'erreur d'accès refusé.

Pour désactiver Trusted Advisor

1. Accédez à la console Trusted Advisor sur https://console.aws.amazon.com/trustedadvisor/home.
2. Dans le panneau de navigation, sous Preferences (Préférences), choisissez Manage Trusted Advisor (Gérer).
3. Sous Trusted Advisor, désactivez Enabled (Activé). Cette action désactive Trusted Advisor pour toutes les vérifications de votre compte.
4. Vous pouvez ensuite supprimer manuellement le de votre compte. Pour en savoir plus, consultez Suppression d'un rôle lié à un service pour Trusted Advisor.

Informations connexes

Pour plus d'informations sur Trusted Advisor, consultez les rubriques suivantes :

- Comment commencer à utiliser Trusted Advisor ?

- Référence de la vérification AWS Trusted Advisor

Commencez avec l'Trusted AdvisorAPI

La référence AWS Trusted Advisor d'API est destinée aux programmeurs qui ont besoin d'informations détaillées sur les opérations d'Trusted AdvisorAPI et les types de données. Cette API permet d'accéder aux Trusted Advisor recommandations pour votre compte ou pour tous les comptes de votre AWS organisation. L'Trusted AdvisorAPI utilise des méthodes HTTP qui renvoient les résultats au format JSON.

> **Note**
>
> - Vous devez disposer d'un plan Business, Enterprise On-Ramp ou Enterprise Support pour utiliser l'API Trusted Advisor
> - Si vous appelez l'AWS Trusted AdvisorAPI depuis un compte qui n'a pas de plan Business, Enterprise On-Ramp ou Enterprise Support, vous recevez une exception de refus d'accès. Pour plus d'informations sur la modification de votre plan de support, consultez AWS Support.

Vous pouvez utiliser l'AWS Trusted AdvisorAPI pour obtenir une liste des vérifications et leurs descriptions, des recommandations et des ressources pour les recommandations. Vous pouvez également mettre à jour le cycle de vie des recommandations. Pour gérer les recommandations, utilisez les opérations d'API suivantes :

- Utilisez les opérations ListChecksListRecommendations, GetRecommendation, et ListRecommendationResourcesAPI pour afficher les recommandations ainsi que les comptes et ressources correspondants.
- Utilisez l'opération UpdateRecommendationLifecycleAPI pour mettre à jour le cycle de vie d'une recommandation gérée par Trusted Advisor Priority.
- Les appels ListOrganizationRecommendationsGetOrganizationRecommendation, ListOrganizationRecommendationResources, ListOrganizationRecommendationAccounts, et UpdateOrganizationRecommendationLifecycleAPI ne prennent en charge que les recommandations gérées par Trusted Advisor Priority. Ces recommandations sont également appelées recommandations prioritaires. Vous pouvez consulter et gérer vos recommandations prioritaires à partir d'un compte de gestion ou d'administrateur délégué si vous avez activé Trusted

Advisor Priority. Si la priorité n'est pas activée, vous recevez une exception d'accès refusé lorsque vous faites des demandes.

Pour plus d'informations, consultez AWS Trusted Advisor le Guide de l'utilisateur du AWS Support.

Pour l'authentification des demandes, consultez le processus de signature Signature version 4.

Utilisation de Trusted Advisor en tant que service web

> **Note**
>
> Trusted Advisorles opérations ne seront pas prises en charge par l'API Support en 2024. Utilisez la nouvelle AWS Trusted AdvisorAPI pour accéder par programmation aux vérifications et aux recommandations relatives aux meilleures pratiques

Le service AWS Support vous permet d'écrire des applications qui interagissent avec AWS Trusted Advisor. Cette rubrique vous montre comment obtenir une liste des contrôles Trusted Advisor, actualiser l'un de ces contrôles, puis obtenir les résultats détaillés pour le contrôle. Ces tâches sont décrites dans Java. Pour plus d'informations sur la prise en charge d'autres langages, consultez Outils pour Amazon Web Services.

Rubriques

Obtenir la liste des contrôles Trusted Advisor disponibles

L'extrait de code Java suivant crée une instance de client AWS Support que vous pouvez utiliser pour appeler l'ensemble des opérations d'API Trusted Advisor. Ensuite, le code obtient la liste des Trusted Advisor vérifications et leurs `CheckId` valeurs correspondantes en appelant l'opération DescribeTrustedAdvisorChecksAPI. Vous pouvez utiliser ces informations pour créer des interfaces

utilisateur qui permettent aux utilisateurs de sélectionner le contrôle qu'ils veulent exécuter ou actualiser.

```
private static AWSSupport createClient()
{
    return AWSSupportClientBuilder.defaultClient();
}
// Get the List of Available Trusted Advisor Checks
public static void getTAChecks() {
    // Possible language parameters: "en" (English), "ja" (Japanese), "fr" (French),
 "zh" (Chinese)
    DescribeTrustedAdvisorChecksRequest request = new
 DescribeTrustedAdvisorChecksRequest().withLanguage("en");
    DescribeTrustedAdvisorChecksResult result =
 createClient().describeTrustedAdvisorChecks(request);
    for (TrustedAdvisorCheckDescription description : result.getChecks()) {
        // Do something with check description.
        System.out.println(description.getId());
        System.out.println(description.getName());
    }
}
```

Actualiser la liste des contrôles Trusted Advisor disponibles

L'extrait de code Java suivant crée une instance de client AWS Support que vous pouvez utiliser pour actualiser les données Trusted Advisor.

```
// Refresh a Trusted Advisor Check
// Note: Some checks are refreshed automatically, and they cannot be refreshed by using
 this operation.
// Specifying the check ID of a check that is automatically refreshed causes an
 InvalidParameterValue error.
public static void refreshTACheck(final String checkId) {
    RefreshTrustedAdvisorCheckRequest request = new
 RefreshTrustedAdvisorCheckRequest().withCheckId(checkId);
    RefreshTrustedAdvisorCheckResult result =
 createClient().refreshTrustedAdvisorCheck(request);
    System.out.println("CheckId: " + result.getStatus().getCheckId());
    System.out.println("Milliseconds until refreshable: " +
 result.getStatus().getMillisUntilNextRefreshable());
    System.out.println("Refresh Status: " + result.getStatus().getStatus());
}
```

Interroger un contrôle Trusted Advisor pour vérifier les changements d'état

Après avoir soumis la demande d'exécution d'une Trusted Advisor vérification afin de générer les dernières données d'état, vous utilisez l'opération DescribeTrustedAdvisorCheckRefreshStatusesAPI pour demander la progression de l'exécution de la vérification et savoir quand de nouvelles données sont prêtes pour la vérification.

L'extrait de code Java suivant obtient l'état du contrôle demandé dans la section suivante, à l'aide de la valeur correspondante dans la variable `CheckId`. En outre, le code illustre plusieurs autres utilisations du service Trusted Advisor :

1. Vous pouvez appeler `getMillisUntilNextRefreshable` en parcourant les objets contenus dans l'instance `DescribeTrustedAdvisorCheckRefreshStatusesResult`. Vous pouvez utiliser la valeur renvoyée pour tester si votre code doit continuer à actualiser le contrôle.
2. Si la valeur de `timeUntilRefreshable` est égale à zéro, vous pouvez demander une actualisation du contrôle.
3. A l'aide de l'état renvoyé, vous pouvez continuer l'interrogation afin d'identifier les modifications d'état ; l'extrait de code définit l'intervalle d'interrogation sur le délai recommandé, à savoir dix secondes. Si l'état est `enqueued` ou `in_progress`, la boucle revient au point de départ et redemande un autre état. Si l'appel renvoie `successful`, la boucle se termine.
4. Enfin, le code renvoie une instance d'un type de données `DescribeTrustedAdvisorCheckResultResult` que vous pouvez utiliser pour parcourir les informations générées par le contrôle.

Remarque : utilisez une seule requête d'actualisation avant d'interroger le statut de la requête.

```
// Retrieves TA refresh statuses. Multiple checkId's can be submitted.
public static List<TrustedAdvisorCheckRefreshStatus> getTARefreshStatus(final String...
 checkIds) {
    DescribeTrustedAdvisorCheckRefreshStatusesRequest request =
            new
 DescribeTrustedAdvisorCheckRefreshStatusesRequest().withCheckIds(checkIds);
    DescribeTrustedAdvisorCheckRefreshStatusesResult result =
            createClient().describeTrustedAdvisorCheckRefreshStatuses(request);
    return result.getStatuses();
}
// Retrieves a TA check status, and checks to see if it has finished processing.
public static boolean isTACheckStatusInTerminalState(final String checkId) {
```

```
    // Since we only submitted one checkId to getTARefreshStatus, just retrieve the
 only element in the list.
    TrustedAdvisorCheckRefreshStatus status = getTARefreshStatus(checkId).get(0);
    // Valid statuses are:
    // 1. "none", the check has never been refreshed before.
    // 2. "enqueued", the check is waiting to be processed.
    // 3. "processing", the check is in the midst of being processed.
    // 4. "success", the check has succeeded and finished processing - refresh data is
 available.
    // 5. "abandoned", the check has failed to process.
    return status.getStatus().equals("abandoned") ||
 status.getStatus().equals("success");
}
// Enqueues a Trusted Advisor check refresh. Periodically polls the check refresh
 status for completion.
public static TrustedAdvisorCheckResult getFreshTACheckResult(final String checkId)
 throws InterruptedException {
    refreshTACheck(checkId);
    while(!isTACheckStatusInTerminalState(checkId)) {
        Thread.sleep(10000);
    }
    return getTACheckResult(checkId);
}
// Retrieves fresh TA check data whenever possible.
// Note: Some checks are refreshed automatically, and they cannot be refreshed by using
 this operation. This method
// is only functional for checks that can be refreshed using the
 RefreshTrustedAdvisorCheck operation.
public static void pollForTACheckResultChanges(final String checkId) throws
 InterruptedException {
    String checkResultStatus = null;
    do {
        TrustedAdvisorCheckResult result = getFreshTACheckResult(checkId);
        if (checkResultStatus != null && !checkResultStatus.equals(result.getStatus()))
 {
            break;
        }
        checkResultStatus = result.getStatus();
        // The rule refresh has completed, but due to throttling rules the checks may
 not be refreshed again
        // for a short period of time.
        // Since we only submitted one checkId to getTARefreshStatus, just retrieve the
 only element in the list.
```

```
        TrustedAdvisorCheckRefreshStatus refreshStatus =
 getTARefreshStatus(checkId).get(0);
        Thread.sleep(refreshStatus.getMillisUntilNextRefreshable());
    } while(true);
    // Signal that a TA check has changed check result status here.
}
```

Demander un résultat de contrôle Trusted Advisor

Après avoir sélectionné la vérification des résultats détaillés que vous souhaitez, vous soumettez une demande à l'aide de l'opération DescribeTrustedAdvisorCheckResultAPI.

> **Tip**
>
> Les noms et les descriptions des vérifications Trusted Advisor sont susceptibles d'être modifiées. Nous vous recommandons de spécifier l'ID de vérification dans votre code pour identifier de manière unique une vérification. Vous pouvez utiliser l'opération DescribeTrustedAdvisorChecksAPI pour obtenir l'ID du chèque.

L'extrait de code Java suivant utilise l'instance `DescribeTrustedAdvisorChecksResult` référencée par la variable `result`, obtenue dans l'extrait de code précédent. Plutôt que de définir un contrôle de manière interactive via une interface utilisateur, une fois que vous avez soumis une demande d'exécution, l'extrait de code soumet une demande d'exécution du premier contrôle dans la liste en spécifiant une valeur d'index 0 dans chaque appel `result.getChecks().get(0)`. Ensuite, le code définit une instance de `DescribeTrustedAdvisorCheckResultRequest` qu'il transmet à une instance de `DescribeTrustedAdvisorCheckResultResult` appelée `checkResult`. Vous pouvez utiliser les structures membres de ce type de données pour afficher les résultats du contrôle.

```
// Request a Trusted Advisor Check Result
public static TrustedAdvisorCheckResult getTACheckResult(final String checkId) {
    DescribeTrustedAdvisorCheckResultRequest request = new
 DescribeTrustedAdvisorCheckResultRequest()
            // Possible language parameters: "en" (English), "ja" (Japanese),
 "fr" (French), "zh" (Chinese)
            .withLanguage("en")
            .withCheckId(checkId);
    DescribeTrustedAdvisorCheckResultResult requestResult =
 createClient().describeTrustedAdvisorCheckResult(request);
```

```
    return requestResult.getResult();
}
```

Remarque : demander un résultat de contrôle Trusted Advisor ne génère pas de données de résultats mises à jour.

Imprimer les détails d'un contrôle Trusted Advisor

L'extrait de code Java suivant itère sur l'instance `DescribeTrustedAdvisorCheckResultResult` renvoyée dans la section précédente afin d'obtenir la liste des ressources signalées par le contrôle Trusted Advisor.

```
// Print ResourceIds for flagged resources.
for (TrustedAdvisorResourceDetail flaggedResource :
    result1.getResult().getFlaggedResources())
{
    System.out.println(
        "The resource for this ResourceID has been flagged: " +
        flaggedResource.getResourceId());
}
```

Vue organisationnelle pour AWS Trusted Advisor

La vue organisationnelle vous permet d'afficher les vérifications Trusted Advisor pour tous les comptes de votre AWS Organizations. Après avoir activé cette fonctionnalité, vous pouvez créer des rapports pour agréger les résultats de vérification de tous les comptes de membres de votre organisation. Le rapport comprend un résumé des résultats des vérifications et des informations sur les ressources affectées pour chaque compte. Par exemple, vous pouvez utiliser les rapports pour identifier les comptes de votre organisation qui utilisent AWS Identity and Access Management (IAM) avec la vérification d'utilisation IAM ou si vous avez recommandé des actions pour les compartiments Amazon Simple Storage Service (Amazon S3) avec la vérification des autorisations de compartiment Amazon S3.

Rubriques

- Prérequis
- Activer la vue organisationnelle
- Actualiser les vérifications Trusted Advisor

- Créer des rapports de vue organisationnelle
- Consulter le résumé du rapport
- Télécharger un rapport de vue organisationnelle
- Désactiver la vue organisationnelle
- Utilisation des politiques IAM pour autoriser l'accès à la vue organisationnelle
- Utilisation d'autres services AWS pour afficher les rapports Trusted Advisor

Prérequis

Vous devez respecter les exigences suivantes pour activer l'affichage organisationnel :

- Vos comptes doivent être membres de votre organisation AWS.
- Toutes les fonctions de votre organisation doivent être activées pour Organisations. Pour de plus amples informations, consultez Activation de toutes les fonctionnalités de l'organisation dans le Guide de l'utilisateur AWS Organizations.
- Le compte de gestion de votre organisation doit posséder un plan de support Business, Enterprise On-Ramp ou Enterprise. Vous pouvez trouver votre plan d'assistance à partir du Centre AWS Support ou à partir de la page Plans de support. Voir Comparer les plans AWS Support.
- Vous devez être connecté en tant qu'utilisateur dans le compte de gestion (ou un rôle équivalent supposé). Que vous vous connectiez en tant qu'utilisateur IAM ou en tant que rôle IAM, vous devez disposer d'une politique avec les autorisations requises. Consultez Utilisation des politiques IAM pour autoriser l'accès à la vue organisationnelle.

Activer la vue organisationnelle

Une fois les prérequis respectés, procédez comme suit pour activer l'affichage organisationnel. Une fois que vous avez activé cette fonctionnalité, voici ce qui se produit :

- Trusted Advisor est activé en tant que service approuvé dans votre organisation. Pour de plus amples informations, consultez Activation de l'accès approuvé avec d'autres services AWS dans le Guide de l'utilisateur AWS Organizations.
- Le rôle lié au service `AWSServiceRoleForTrustedAdvisorReporting` est créé pour vous dans le compte de gestion de votre organisation. Ce rôle inclut les autorisations nécessaires à Trusted Advisor pour appeler Organizations en votre nom. Ce rôle lié au service est verrouillé et

vous ne pouvez pas le supprimer manuellement. Pour plus d'informations, consultez Utilisation des rôles liés aux services pour Trusted Advisor.

Vous activez la vue organisationnelle à partir de la console Trusted Advisor.

Pour activer la vue organisationnelle

1. Connectez-vous en tant qu'administrateur dans le compte de gestion de l'organisation et ouvrez la console AWS Trusted Advisor sur https://console.aws.amazon.com/trustedadvisor.
2. Dans le panneau de navigation, sous Preferences (Préférences), choisissez Your organization (Votre organisation).
3. Sous Enable trusted access with AWS Organizations (Activer l'accès de confiance avec), activez Enabled (Activé).

> **Note**
>
> L'activation de la vue organisationnelle pour le compte de gestion ne fournit pas les mêmes vérifications pour tous les comptes membres. Par exemple, si vos comptes membres bénéficient tous d'un support basique, ces comptes n'auront pas les mêmes vérifications disponibles que votre compte de gestion. Le plan AWS Support détermine les vérifications Trusted Advisor disponibles pour un compte.

Actualiser les vérifications Trusted Advisor

Avant de créer un rapport pour votre organisation, nous vous recommandons d'actualiser les statuts de vos vérifications Trusted Advisor. Vous pouvez télécharger un rapport sans actualiser vos vérifications Trusted Advisor, mais il se peut que votre rapport ne dispose pas des informations les plus récentes.

Si vous possédez un plan de support Business, Enterprise On-Ramp ou Enterprise, Trusted Advisor actualise automatiquement les vérifications de votre compte de manière hebdomadaire.

> **Note**
>
> Si vous avez des comptes dans votre organisation qui disposent d'un plan de support Developer ou Basic, un utilisateur de ces comptes doit se connecter à la console Trusted

Advisor pour actualiser les vérifications. Vous ne pouvez pas actualiser les vérifications pour tous les comptes à partir du compte de gestion de l'organisation.

Pour actualiser les vérifications Trusted Advisor

1. Accédez à la console AWS Trusted Advisor sur https://console.aws.amazon.com/trustedadvisor.
2. Sur la page Trusted Advisor Recommendations, choisissez l'option Refresh all checks (Actualiser toutes les vérifications). Cette opération actualise toutes les vérifications de votre compte.

Vous pouvez aussi actualiser des vérifications spécifiques des manières suivantes :

- Utilisez l'opération d'API RefreshTrustedAdvisorCheck.
- Choisissez l'icône d'actualisation
  ()
  pour une vérification individuelle.

Créer des rapports de vue organisationnelle

Une fois que vous avez activé la vue organisationnelle, vous pouvez créer des rapports afin de pouvoir afficher les résultats des vérifications Trusted Advisor de votre organisation.

Vous pouvez créer jusqu'à 50 rapports. Si vous créez des rapports au-delà de ce quota, Trusted Advisor supprime le rapport le plus ancien. Il n'est pas possible de récupérer les rapports supprimés.

Pour créer des rapports de vue organisationnelle

1. Connectez-vous au compte de gestion de l'organisation et ouvrez la console AWS Trusted Advisor sur https://console.aws.amazon.com/trustedadvisor.
2. Dans le volet de navigation, choisissez Organizational View (Vue organisationnelle).
3. Choisissez Créer un rapport.
4. Par défaut, le rapport inclut l'ensemble des régions AWS, des catégories de vérification, des vérifications et des statuts des ressources. Dans la page Create report (Créer un rapport), vous pouvez utiliser les options de filtre pour personnaliser votre rapport. Par exemple, vous pouvez

désélectionner l'option All (Tout) pour Region (Région), puis spécifiez les régions individuelles à inclure dans le rapport.

a. Entrez un nom pour le rapport.

b. Sous Format, choisissez JSON ou CSV.

c. Pour Region (Région), spécifiez la région AWS ou choisissez All (Tout).

d. Pour Check category (Catégorie de vérification), choisissez la catégorie de vérification ou choisissez All (Tout).

e. Pour Checks (Vérifications), choisissez les vérifications spécifiques pour cette catégorie ou choisissez All (Tout).

> **Note**
>
> Le filtre Check category (Catégorie de vérification) remplace le filtre Check (Vérification). Par exemple, si vous choisissez la catégorie Security (Sécurité), puis choisissez un nom de vérification spécifique, votre rapport inclut tous les résultats de vérification pour cette catégorie. Pour créer un rapport pour des vérifications spécifiques uniquement, conservez la valeur par défaut All (Tout) pour Check category (Catégorie de vérification), puis choisissez vos noms de vérification.

f. Pour Resource status (Statut de la ressource), choisissez le statut pour filtrer, tel que Warning (Avertissement) ou choisissez All (Tout).

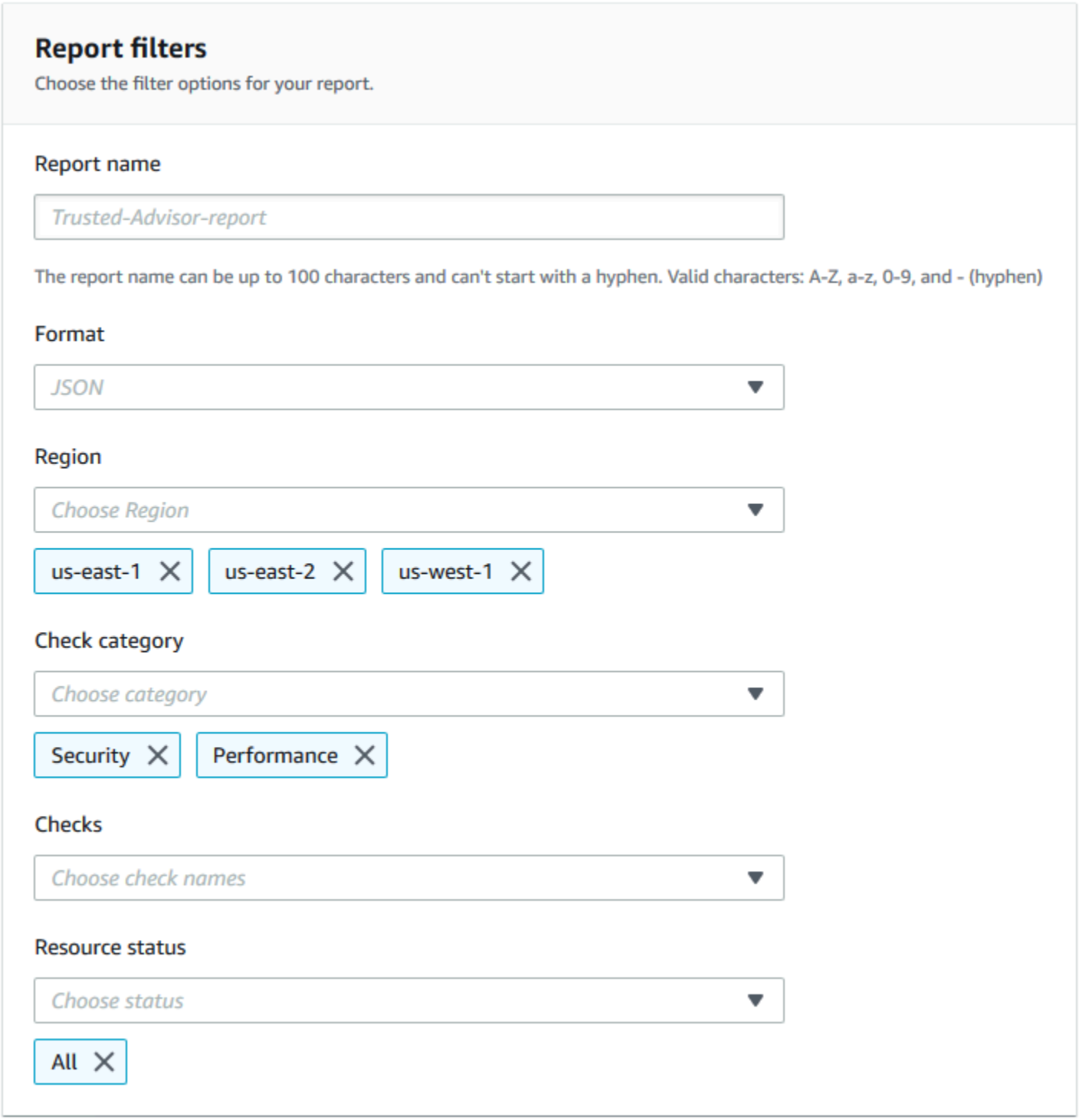
5. Pour AWS Organization (Organisation AWS), sélectionnez les unités organisationnelles (UO) à inclure dans votre rapport. Pour plus d'informations sur les UO, consultez Gestion des unités d'organisation dans le Guide de l'utilisateur AWS Organizations.

6. Choisissez Créer un rapport.

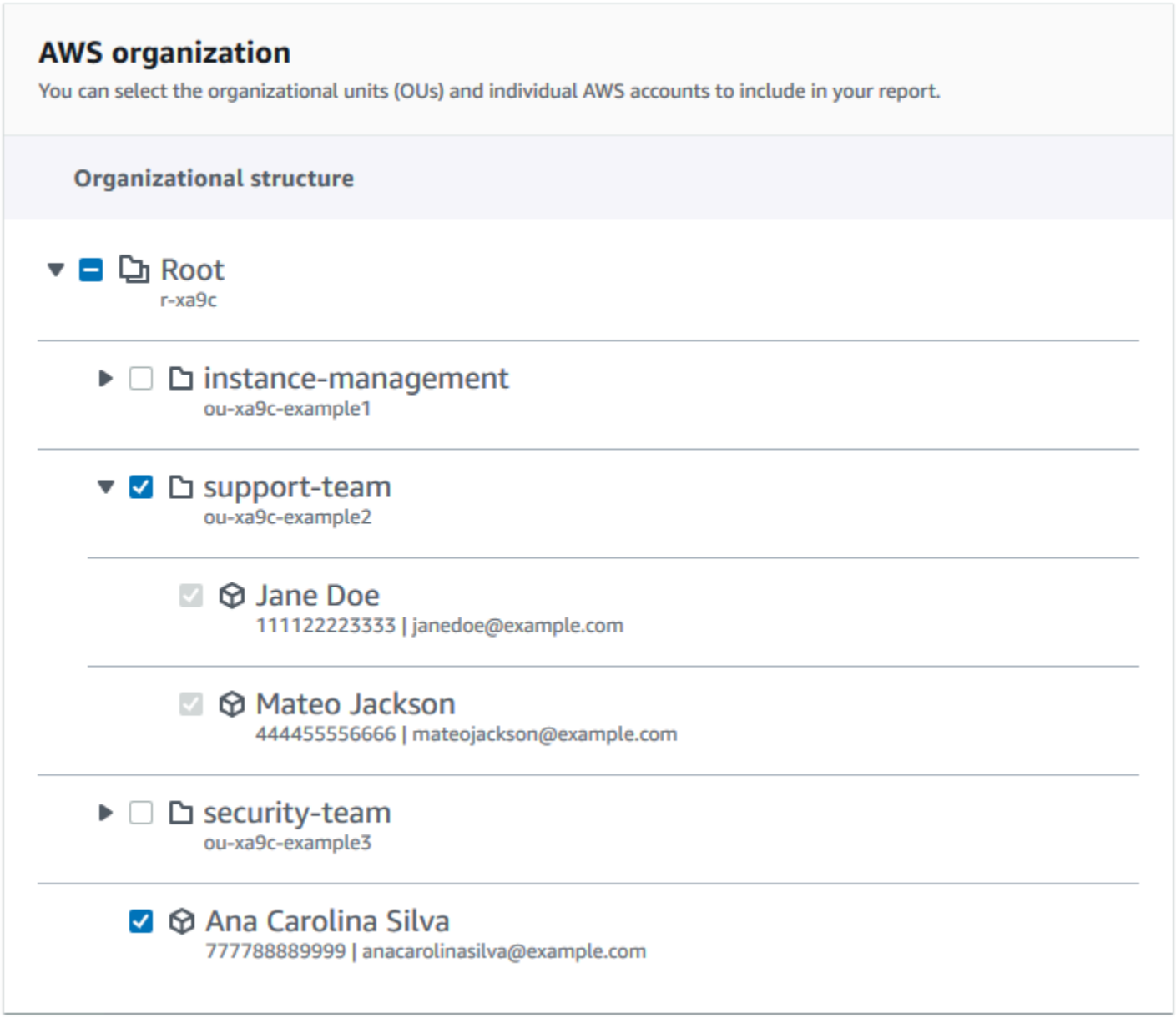
Example : Créer des options de filtre de rapport

L'exemple suivant crée un rapport JSON pour les éléments suivants :

- Trois régions AWS
- Toutes les vérifications Security (Sécurité) et Performance



Dans l'exemple suivant, le rapport inclut l'UO support-team et un compte AWS qui font partie de l'organisation.



Remarques

- Le temps nécessaire à la création du rapport dépend du nombre de comptes dans l'organisation et du nombre de ressources dans chaque compte.
- Vous ne pouvez pas créer plus d'un rapport à la fois à moins que le rapport actuel ne soit exécuté depuis plus de six heures.
- Actualisez la page si le rapport ne s'affiche pas sur la page.

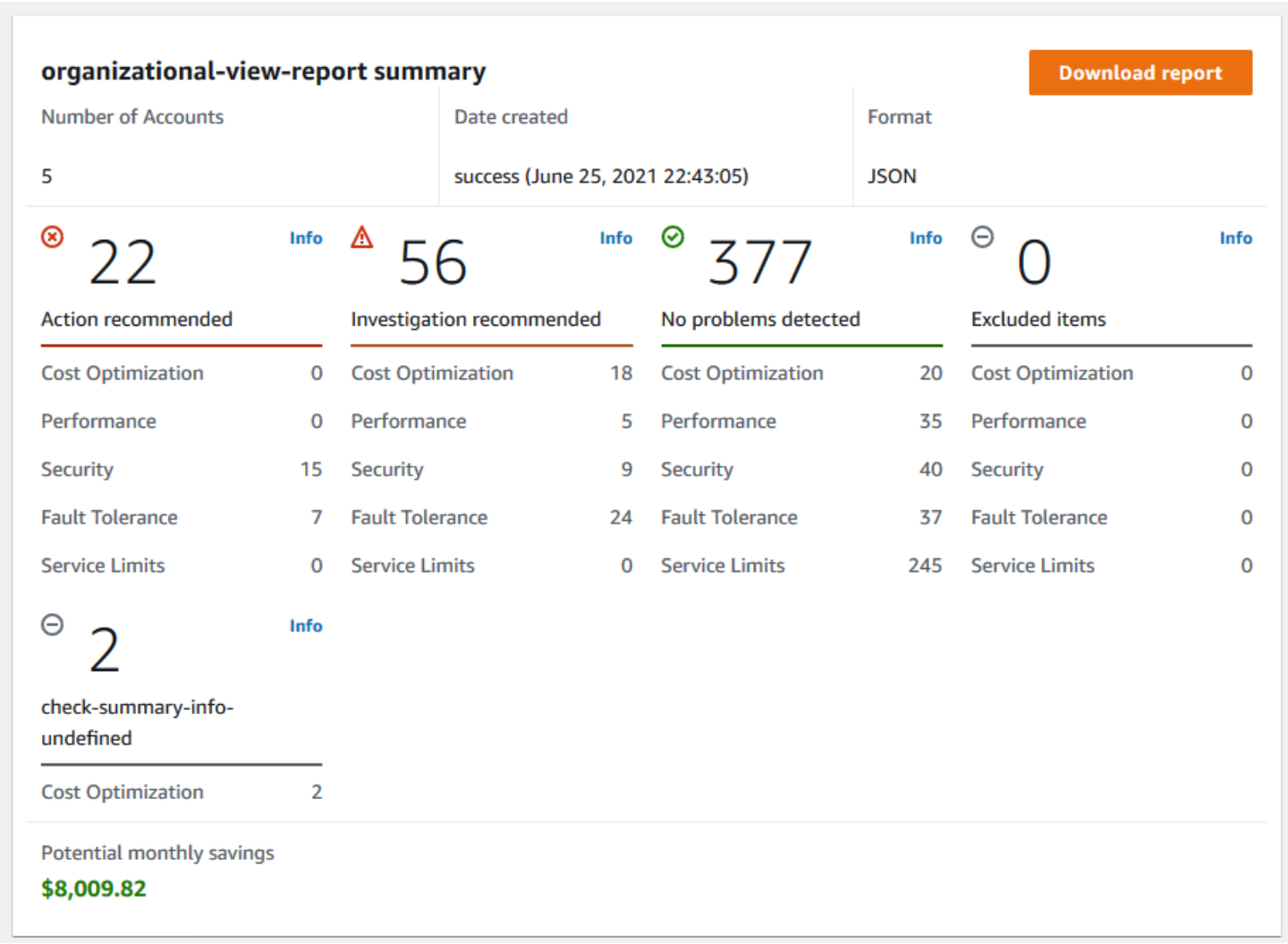
Consulter le résumé du rapport

Une fois le rapport prêt, vous pouvez afficher le résumé du rapport à partir de la console Trusted Advisor. Cela vous permet d'afficher rapidement le résumé des résultats de vos vérifications dans l'ensemble de votre organisation.

Pour afficher le résumé du rapport

1. Connectez-vous au compte de gestion de l'organisation et ouvrez la console AWS Trusted Advisor à l'adresse suivante : https://console.aws.amazon.com/trustedadvisor.
2. Dans le volet de navigation, choisissez Organizational View (Vue organisationnelle).
3. Choisissez le nom du rapport.
4. Dans la page Summary (Résumé), affichez les statuts de vérification de chaque catégorie. Vous pouvez également sélectionner Download report (Téléchargement du rapport).

Example : Synthèse du rapport pour une organisation



Télécharger un rapport de vue organisationnelle

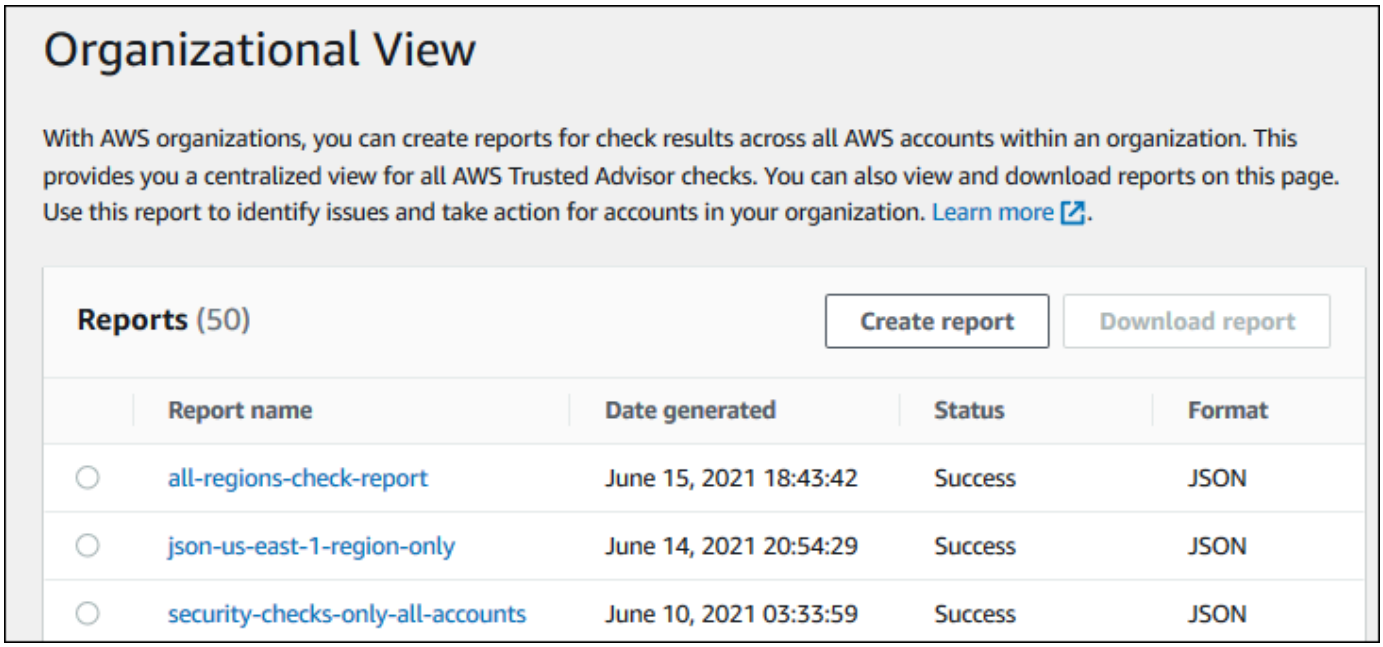
Une fois que votre rapport est prêt, téléchargez-le à partir de la console Trusted Advisor. Le rapport est un fichier .zip reprenant trois fichiers :

- `summary.json` : contient un résumé des résultats de la vérification pour chaque catégorie de contrôle.
- `schema.json` : contient le schéma des vérifications spécifiées dans le rapport.
- Fichier de ressources (.json ou .csv) : contient des informations détaillées sur les statuts de vérification des ressources de votre organisation.

Pour télécharger un rapport de vue organisationnelle

1. Connectez-vous au compte de gestion de l'organisation et ouvrez la console AWS Trusted Advisor à l'adresse suivante : https://console.aws.amazon.com/trustedadvisor.
2. Dans le volet de navigation, choisissez Organizational View (Vue organisationnelle).

   La page Organizational View (Vue organisationnelle) affiche les rapports disponibles à télécharger.
3. Sélectionnez un rapport, choisissez Download report (Télécharger le rapport), puis enregistrez le fichier. Vous ne pouvez télécharger qu'un seul rapport à la fois.



4. Décompressez le fichier.
5. Utilisez un éditeur de texte pour ouvrir le fichier `.json` ou une application de feuille de calcul pour ouvrir le fichier `.csv`.

> **Note**
>
> Vous pouvez recevoir plusieurs fichiers si la taille de votre rapport est égale à 5 Mo ou plus.

Example : fichier summary.json

Le fichier `summary.json` indique le nombre de comptes dans l'organisation et les statuts des vérifications dans chaque catégorie.

Trusted Advisor utilise le code couleur suivant pour les résultats de vérification :

- `Green` : Trusted Advisor ne détecte pas de problème pour la vérification.
- `Yellow` : Trusted Advisor détecte un problème possible pour la vérification.
- `Red` : Trusted Advisor détecte une erreur et recommande une action pour la vérification.
- `Blue` : Trusted Advisor ne peut pas déterminer le statut de la vérification.

Dans l'exemple suivant, deux vérifications sont `Red`, l'une est `Green` et l'une est `Yellow`.


```
{
    "numAccounts": 3,
    "filtersApplied": {
        "accountIds": ["123456789012","111122223333","111111111111"],
        "checkIds": "All",
        "categories": [
            "security",
            "performance"
        ],
        "statuses": "All",
        "regions": [
            "us-west-1",
            "us-west-2",
            "us-east-1"
        ],
        "organizationalUnitIds": [
            "ou-xa9c-EXAMPLE1",
            "ou-xa9c-EXAMPLE2"
        ]
    },
    "categoryStatusMap": {
        "security": {
            "statusMap": {
                "ERROR": {
                    "name": "Red",
                    "count": 2
                },
                "OK": {
```

```
                    "name": "Green",
                    "count": 1
                },
                "WARN": {
                    "name": "Yellow",
                    "count": 1
                }
            },
            "name": "Security"
        }
    },
    "accountStatusMap": {
        "123456789012": {
            "security": {
                "statusMap": {
                    "ERROR": {
                        "name": "Red",
                        "count": 2
                    },
                    "OK": {
                        "name": "Green",
                        "count": 1
                    },
                    "WARN": {
                        "name": "Yellow",
                        "count": 1
                    }
                },
                "name": "Security"
            }
        }
    }
}
```

Example : fichier schema.json

Le fichier `schema.json` inclut le schéma des vérifications dans le rapport. L'exemple suivant inclut les ID et les propriétés des vérifications de la politique de mot de passe IAM (Yw2K9puPzl) et la rotation des clés IAM (DqdJqYeRm5).

```
{
    "Yw2K9puPzl": [
        "Password Policy",
```

```
        "Uppercase",
        "Lowercase",
        "Number",
        "Non-alphanumeric",
        "Status",
        "Reason"
    ],
    "DqdJqYeRm5": [
        "Status",
        "IAM User",
        "Access Key",
        "Key Last Rotated",
        "Reason"
    ],
    ...
}
```

Example : fichier resources.csv

Le fichier `resources.csv` contient des informations sur les ressources de l'organisation. Cet exemple montre certaines des colonnes de données qui apparaissent dans le rapport, telles que les suivantes :

- ID de compte du compte affecté
- L'ID de la vérification Trusted Advisor
- L'ID de la ressource
- Horodatage du rapport
- Le nom complet de la vérification Trusted Advisor
- La catégorie de vérification Trusted Advisor
- ID de compte de l'unité organisationnelle ou racine parent

AccountId	CheckId	ResourceId	TimeStamp	CheckName	Category
1.11122E+11	Qch7DwouX1	LnW14f1M40NMjmMLvY5	1.58983E+12	Low Utilization Amazon EC2 Instances	Cost Optimizing
1.11122E+11	HCP4007jGY	dJrQZXw36ZdswBeo9WUl	1.58983E+12	Security Groups - Specific Ports Unrestricted	Security
1.11122E+11	HCP4007jGY	1hzakmTbWd5UmAM_a0L	1.58983E+12	Security Groups - Specific Ports Unrestricted	Security
4.44456E+11	1iG5NDGVre	dJrQZXw36ZdswBeo9WUl	1.58983E+12	Security Groups - Unrestricted Access	Security
4.44456E+11	1iG5NDGVre	1hzakmTbWd5UmAM_a0L	1.58983E+12	Security Groups - Unrestricted Access	Security
4.44456E+11	Pfx0RwqBli	vioZmlba45kf2JWIe_W0j5	1.58983E+12	Amazon S3 Bucket Permissions	Security
4.44456E+11	Pfx0RwqBli	wAvASS3YOwy6WWxIBHf	1.58983E+12	Amazon S3 Bucket Permissions	Security
1.23457E+11	Pfx0RwqBli	LIc4zRaUSiIGRSlmqaMa5V	1.58983E+12	Amazon S3 Bucket Permissions	Security
1.23457E+11	Pfx0RwqBli	gWB27TMXof2evYzMSYBg	1.58983E+12	Amazon S3 Bucket Permissions	Security
7.77789E+11	Pfx0RwqBli	M3LBsF0e15Cl9Mxppapcx	1.58983E+12	Amazon S3 Bucket Permissions	Security
7.77789E+11	Yw2K9puPzl	47DEQpj8HBSa-_TImW-5J	1.58983E+12	IAM Password Policy	Security
7.77789E+11	H7IgTzjTYb	1xHQ5ovV8bS0H1Z-t7Kbib	1.58983E+12	Amazon EBS Snapshots	Fault Tolerance
7.77789E+11	wuy7G1zxql	10F6p6VAF0F-MuL6Dc-dl1	1.58983E+12	Amazon EC2 Availability Zone Balance	Fault Tolerance

Le fichier de ressources ne contient des entrées que si un résultat de vérification existe au niveau de la ressource. Il est possible que vous ne voyiez pas les vérifications dans le rapport pour les raisons suivantes :

- Certaines vérifications, telles que MFA on Root Account (MFA sur le compte racine), n'ont pas de ressources et n'apparaîtront pas dans le rapport. Les vérifications sans ressources apparaissent dans le fichier `summary.json` à la place.
- Certaines vérifications ne montrent que les ressources si elles sont `Red` ou `Yellow`. Si toutes les ressources sont `Green`, elles peuvent ne pas apparaître dans votre rapport.
- Si un compte n'est pas activé pour un service nécessitant la vérification, la vérification peut ne pas apparaître dans le rapport. Par exemple, si vous n'utilisez pas les instances réservées Amazon Elastic Compute Cloud dans votre organisation, la vérification Amazon EC2 Reserved Instance Lease Expiration n'apparaît pas dans votre rapport.
- Le compte n'a pas actualisé les résultats de la vérification. Cela peut se produire lorsque les utilisateurs disposant d'un plan de support Basic ou Developer se connectent à la console Trusted Advisor pour la première fois. Si vous possédez un plan de support Business, Enterprise On-Ramp ou Enterprise, il faudra peut-être une semaine maximum à compter de l'inscription d'un compte pour que les utilisateurs puissent voir les résultats de la vérification. Pour de plus amples informations, veuillez consulter Actualiser les vérifications Trusted Advisor.
- Si seul le compte de gestion de l'organisation a activé les recommandations pour les contrôles, l'état n'inclut pas de ressources pour les autres comptes de l'organisation.

Pour le fichier resources, vous pouvez utiliser un logiciel commun tel que Microsoft Excel pour ouvrir le format de fichier .csv. Vous pouvez utiliser le fichier .csv pour une analyse unique de toutes les

vérifications entre tous les comptes de votre organisation. Si vous souhaitez utiliser votre rapport avec une application, vous pouvez le télécharger en tant que fichier .json à la place.

Le format de fichier .json offre plus de flexibilité que le format de fichier .csv pour les cas d'utilisation avancés tels que l'agrégation et l'analyse avancée avec plusieurs jeux de données. Par exemple, vous pouvez utiliser une interface SQL avec un service AWS tel qu'Amazon Athena pour exécuter des requêtes sur vos rapports. Vous pouvez également utiliser Amazon QuickSight pour créer des tableaux de bord et visualiser vos données. Pour plus d'informations, consultez Utilisation d'autres services AWS pour afficher les rapports Trusted Advisor.

Désactiver la vue organisationnelle

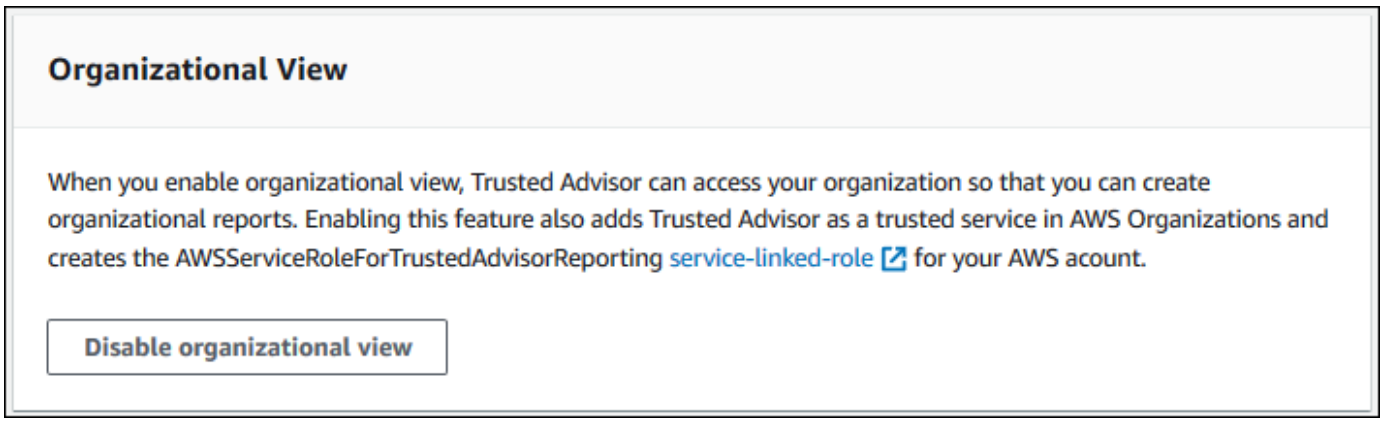
Suivez cette procédure pour désactiver la vue organisationnelle. Vous devez vous connecter au compte de gestion de l'organisation ou assumer un rôle avec les autorisations requises pour désactiver cette fonction. Vous ne pouvez pas désactiver cette fonctionnalité à partir d'un autre compte de l'organisation.

Une fois que vous avez désactivé cette fonctionnalité, voici ce qui se produit :

- Trusted Advisor est supprimé en tant que service approuvé dans Organizations.
- Le rôle lié à un service `AWSServiceRoleForTrustedAdvisorReporting` est déverrouillé dans le compte de gestion de l'organisation. Cela signifie que vous pouvez le supprimer manuellement, si nécessaire.
- Vous ne pouvez pas créer, afficher ou télécharger des rapports pour votre organisation. Pour accéder aux rapports créés précédemment, vous devez réactiver la vue organisationnelle à partir de la console Trusted Advisor. Consultez Activer la vue organisationnelle.

Pour désactiver la vue organisationnelle pour Trusted Advisor

1. Connectez-vous au compte de gestion de l'organisation et ouvrez la console AWS Trusted Advisor à l'adresse suivante : https://console.aws.amazon.com/trustedadvisor.
2. Dans le panneau de navigation, sélectionnez Préférences.
3. Sous Organizational View (Vue organisationnelle), choisissez Disable organizational view (Désactiver la vue organisationnelle).



Après avoir désactivé la vue organisationnelle, Trusted Advisor n'agrège plus les vérifications d'autres comptes AWS de votre organisation. Cependant, le rôle lié à un service `AWSServiceRoleForTrustedAdvisorReporting` reste sur le compte de gestion de l'organisation jusqu'à ce que vous le supprimiez via la console IAM, l'API IAM ou AWS Command Line Interface (AWS CLI). Pour plus d'informations, veuillez consulter Suppression d'un rôle lié à un service dans le Guide de l'utilisateur IAM.

> **Note**
>
> Vous pouvez utiliser d'autres services AWS pour interroger et visualiser vos données pour les rapports de vue organisationnelle. Pour plus d'informations, consultez les ressources suivantes :
>
> - Afficher les recommandations AWS Trusted Advisor à grande échelle avec AWS Organizations dans le Blog Gestion & Gouvernance AWS (en anglais)
> - Utilisation d'autres services AWS pour afficher les rapports Trusted Advisor

Utilisation des politiques IAM pour autoriser l'accès à la vue organisationnelle

Vous pouvez utiliser les politiques AWS Identity and Access Management (IAM) pour autoriser les utilisateurs ou les rôles de votre accès au compte à la vue organisationnelle dans AWS Trusted Advisor.

Example : Accès complet à la vue organisationnelle

La politique suivante accorde un accès complet à la fonction de vue organisationnelle. Un utilisateur avec ces autorisations peut effectuer les opérations suivantes :

- Activation et désactivation de la vue organisationnelle
- Création, affichage, et téléchargement des rapports

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "ReadStatement",
            "Effect": "Allow",
            "Action": [
                "organizations:ListAccountsForParent",
                "organizations:ListAccounts",
                "organizations:ListRoots",
                "organizations:DescribeOrganization",
                "organizations:ListOrganizationalUnitsForParent",
                "organizations:ListAWSServiceAccessForOrganization",
                "trustedadvisor:DescribeAccount",
                "trustedadvisor:DescribeChecks",
                "trustedadvisor:DescribeCheckSummaries",
                "trustedadvisor:DescribeAccountAccess",
                "trustedadvisor:DescribeOrganization",
                "trustedadvisor:DescribeReports",
                "trustedadvisor:DescribeServiceMetadata",
                "trustedadvisor:DescribeOrganizationAccounts",
                "trustedadvisor:ListAccountsForParent",
                "trustedadvisor:ListRoots",
                "trustedadvisor:ListOrganizationalUnitsForParent"
            ],
            "Resource": "*"
        },
        {
            "Sid": "CreateReportStatement",
            "Effect": "Allow",
            "Action": [
                "trustedadvisor:GenerateReport"
            ],
            "Resource": "*"
```

```
        },
        {
            "Sid": "ManageOrganizationalViewStatement",
            "Effect": "Allow",
            "Action": [
                "organizations:EnableAWSServiceAccess",
                "organizations:DisableAWSServiceAccess",
                "trustedadvisor:SetOrganizationAccess"
            ],
            "Resource": "*"
        },
        {
            "Sid": "CreateServiceLinkedRoleStatement",
            "Effect": "Allow",
            "Action": "iam:CreateServiceLinkedRole",
            "Resource": "arn:aws:iam::*:role/aws-service-role/
reporting.trustedadvisor.amazonaws.com/AWSServiceRoleForTrustedAdvisorReporting"
        }
    ]
}
```

Example : Accès en lecture à la vue organisationnelle

La politique suivante accorde un accès en lecture uniquement à la vue organisationnelle pour Trusted Advisor. Un utilisateur disposant de ces autorisations ne peut afficher et télécharger que les rapports existants.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "ReadStatement",
            "Effect": "Allow",
            "Action": [
                "organizations:ListAccountsForParent",
                "organizations:ListAccounts",
                "organizations:ListRoots",
                "organizations:DescribeOrganization",
                "organizations:ListOrganizationalUnitsForParent",
                "organizations:ListAWSServiceAccessForOrganization",
                "trustedadvisor:DescribeAccount",
                "trustedadvisor:DescribeChecks",
                "trustedadvisor:DescribeCheckSummaries",
```

```
                "trustedadvisor:DescribeAccountAccess",
                "trustedadvisor:DescribeOrganization",
                "trustedadvisor:DescribeReports",
                "trustedadvisor:ListAccountsForParent",
                "trustedadvisor:ListRoots",
                "trustedadvisor:ListOrganizationalUnitsForParent"
            ],
            "Resource": "*"
        }
    ]
}
```

Vous pouvez également créer votre propre politique IAM. Pour plus d'informations, consultez Création de politiques IAM dans le Guide de l'utilisateur IAM.

> **Note**
>
> Si vous avez activé AWS CloudTrail dans votre compte, les rôles suivants peuvent apparaître dans vos entrées de journal :
>
> - `AWSServiceRoleForTrustedAdvisorReporting` : le rôle lié à un service que Trusted Advisor utilise pour accéder aux comptes de votre organisation.
> - `AWSServiceRoleForTrustedAdvisor` : le rôle lié à un service que Trusted Advisor utilise pour accéder aux services de votre organisation.
>
> Pour plus d'informations sur les rôles liés à un service, consultez Utilisation des rôles liés aux services pour Trusted Advisor.

Utilisation d'autres services AWS pour afficher les rapports Trusted Advisor

Suivez ce didacticiel pour télécharger et afficher vos données à l'aide d'autres services AWS. Dans cette rubrique, vous créez un compartiment Amazon Simple Storage Service (Amazon S3) pour stocker votre rapport et un modèle AWS CloudFormation pour créer des ressources dans votre compte. Ensuite, vous pouvez utiliser Amazon Athena pour analyser ou exécuter des requêtes pour votre rapport ou Amazon QuickSight pour visualiser ces données dans un tableau de bord.

Pour plus d'informations et des exemples sur la visualisation des données de votre rapport, consultez Afficher les recommandations AWS Trusted Advisor à grande échelle avec AWS Organizations dans le Blog Gestion & Gouvernance AWS.

Prérequis

Avant de commencer ce didacticiel, vous devez respecter les conditions requises suivantes :

- Connectez-vous en tant qu'utilisateur AWS Identity and Access Management (IAM) disposant d'autorisations d'administrateur.
- Utilisation de la région AWS USA Est (Virginie du Nord) pour configurer rapidement vos services et ressources AWS.
- Créez un compte Amazon QuickSight. Pour de plus amples informations, consultez Mise en route avec les analyses de données dans Amazon QuickSight dans le Guide de l'utilisateur Amazon QuickSight.

Télécharger le rapport sur Amazon S3

Après avoir téléchargé votre rapport `resources.json`, téléchargez le fichier sur Amazon S3. Vous devez utiliser un compartiment dans la région USA Est (Virginie du Nord).

Pour télécharger le rapport dans un compartiment Amazon S3

1. Connectez-vous à AWS Management Console via https://console.aws.amazon.com/.
2. Utilisez le sélecteur de région et choisissez la région US East (N. Virginia) (USA Est (Virginie du Nord)).
3. Ouvrez la console Amazon S3 sur https://console.aws.amazon.com/s3/.
4. Dans la liste de compartiments, choisissez un compartiment S3, puis copiez le nom. Vous utilisez le nom dans la procédure suivante.
5. Dans la page *`bucket-name`*, choisissez Create Folder (Créer un dossier), entrez le nom **`folder1`**, puis Save (Enregistrer).
6. Choisissez folder1.
7. Dans folder1 (dossier1), choisissez Upload (Charger) et choisissez le fichier `resources.json`.
8. Choisissez Next (Suivant), conservez les options par défaut et choisissez ensuite Upload (Charger).

> **Note**
>
> Si vous téléchargez un nouveau rapport dans ce compartiment, renommez les fichiers `.json` chaque fois que vous les téléchargez afin de ne pas remplacer les rapports existants. Par exemple, vous pouvez ajouter l'horodatage à chaque fichier, tel que `resources-timestamp.json`, `resources-timestamp2.json`, etc.

Créer vos ressources à l'aide de AWS CloudFormation

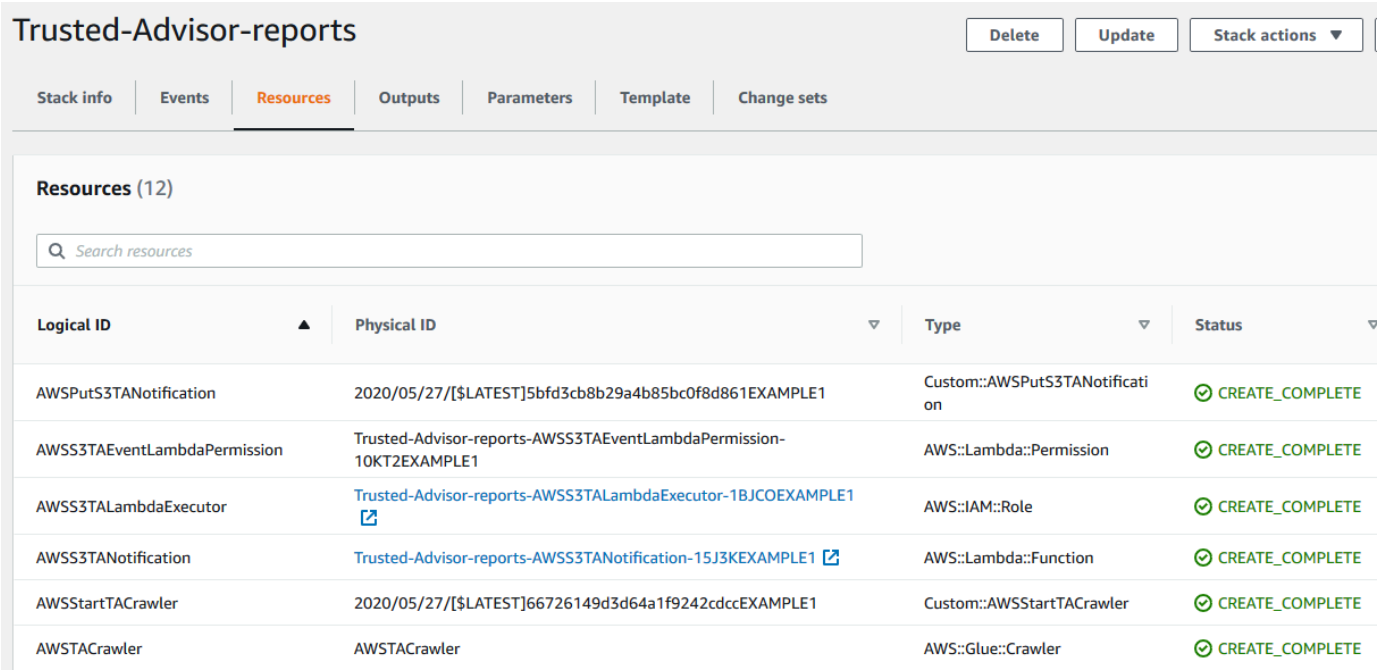
Après avoir chargé votre rapport sur Amazon S3, téléchargez le modèle YAML suivant sur AWS CloudFormation. Ce modèle indique AWS CloudFormation les ressources à créer pour votre compte afin que d'autres services puissent utiliser les données du rapport dans le compartiment S3. Le modèle crée des ressources pour IAM, AWS Lambda et AWS Glue.

Pour créer vos ressources avec AWS CloudFormation

1. Téléchargez le fichier trusted-advisor-reports-template.zip.
2. Décompressez le fichier.
3. Ouvrez votre fichier de modèle dans un éditeur de texte.
4. Pour les paramètres `BucketName` et `FolderName`, remplacez les valeurs pour *`your-bucket-name-here`* et *`folder1`* avec le nom du compartiment et le nom du dossier dans votre compte.
5. Sauvegardez le fichier.
6. Ouvrez la console AWS CloudFormation à l'adresse https://console.aws.amazon.com/cloudformation.
7. Si vous ne l'avez pas déjà fait, dans le sélecteur de région, choisissez la région US East (N. Virginia) (USA Est (Virginie du Nord)).
8. Dans le volet de navigation, choisissez Stack (Piles).
9. Choisissez Créer une pile et choisissez Avec de nouvelles ressources (standard).
10. Dans le page Create stack (Créer une pile), sous Specify template (Spécifier le modèle), choisissez Upload a template file (Charger un fichier modèle), puis choisissez Choose file (Choisir le fichier).
11. Choisissez votre fichier YAML, puis choisissez Next (Suivant).
12. Sur la page Specify stack details (Spécifier les détails de la pile), saisissez un nom pour la pile, tel que **`Organizational-view-Trusted-Advisor-reports`** et choisissez Next (Suivant).

13. Dans la page Configure stack options (Configuration des options des piles), conservez les options par défaut et choisissez Next (Suivant).
14. Sur la page Vérification de **`Organizational-view-Trusted-Advisor-reports`**, vérifiez vos choix. Au bas de la page, activez la case à cocher indiquant I acknowledge that AWS CloudFormation might create IAM resources (Je reconnais que CFN pourrait créer des ressources IAM).
15. Sélectionnez Create stack (Créer une pile).

    La création de la pile prend environ 5 minutes.
16. Une fois que la pile a été correctement créée, l'onglet Resources (Ressources) apparaît comme suit.



Interroger les données dans Amazon Athena

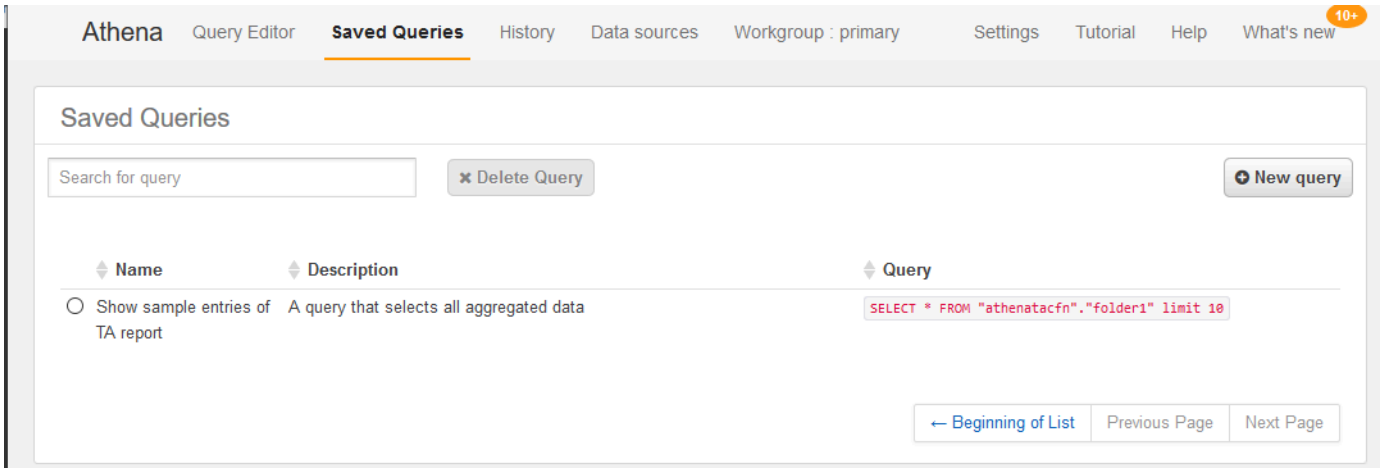
Une fois que vous avez vos ressources, vous pouvez afficher les données dans Athena. Utilisez Athena pour créer des requêtes et analyser les résultats du rapport, tels que la recherche de résultats de vérification spécifiques pour les comptes de l'organisation.

> **Remarques**
>
> - Choisissez la région US East (N. Virginia) (USA Est (Virginie du Nord)..

- Si vous êtes nouveau dans Athena, vous devez spécifier un emplacement de résultat de requête avant de pouvoir exécuter une requête pour votre rapport. Nous vous recommandons de spécifier un compartiment S3 différent pour cet emplacement. Pour de plus amples informations, veuillez consulter Spécification d'un emplacement de résultats de requête dans le Guide de l'utilisateur Amazon Athena.

Interroger les données dans Athena

1. Ouvrez la console Athena à l'adresse https://console.aws.amazon.com/athena/.
2. Si vous ne l'avez pas déjà fait, dans le sélecteur de région, choisissez la région US East (N. Virginia) (USA Est (Virginie du Nord)).
3. Choisissez Saved Queries (Requêtes enregistrées) dans le champ de recherche, entrez **`Show sample`**.
4. Choisissez la requête qui s'affiche, telle que Show sample entries of TA report (Afficher des exemples d'entrées de rapport TA).



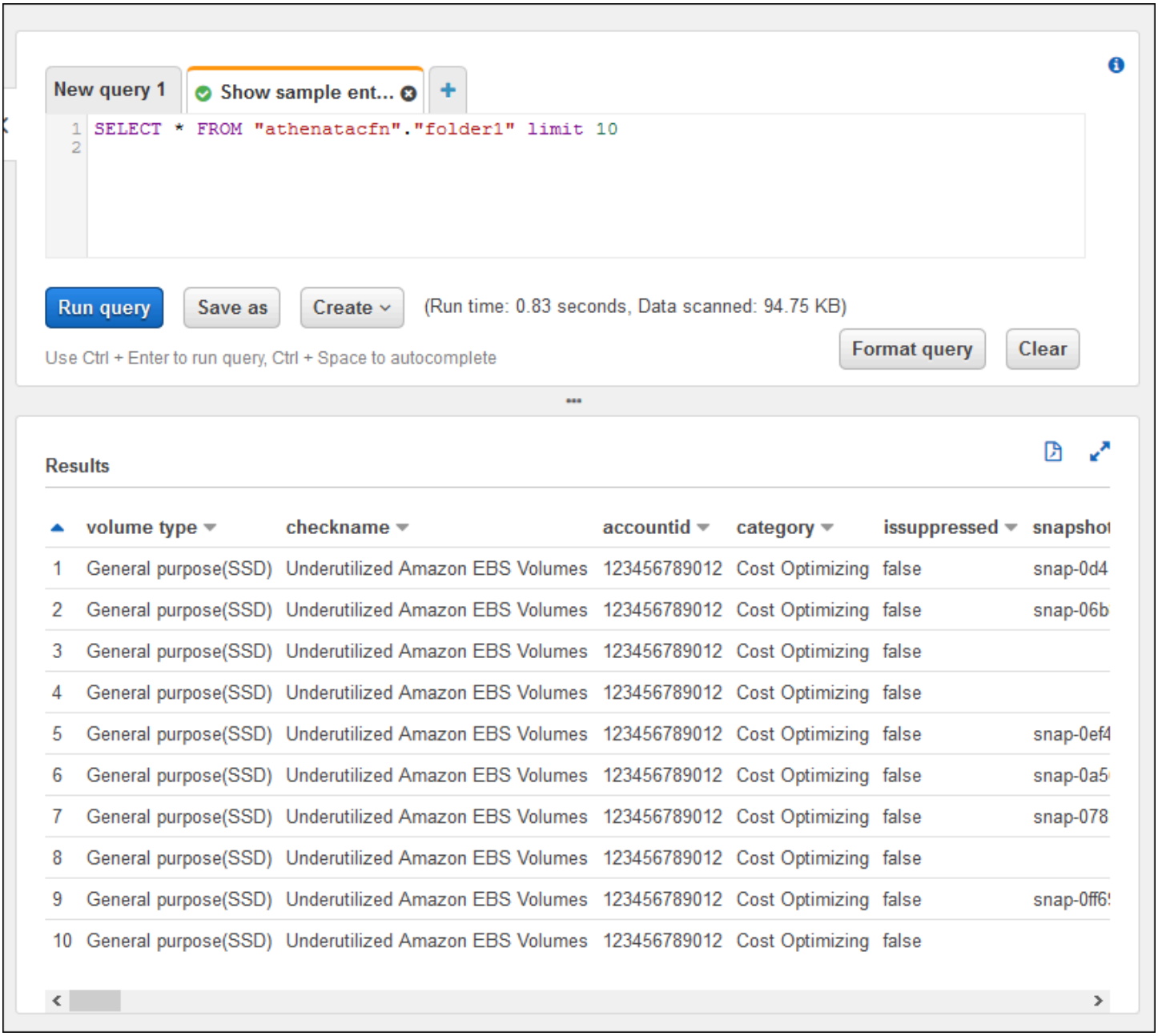
   La requête doit ressembler à ce qui suit.

```
SELECT * FROM "athenatacfn"."folder1" limit 10
```

5. Choisissez Run Query (Exécuter la requête). Les résultats de votre requête s'affichent.

Example : requête Athena

L'exemple suivant montre 10 exemples d'entrées du rapport.



Pour de plus amples informations, consultez Exécution de requêtes SQL à l'aide d'Amazon Athena dans le Guide de l'utilisateur Amazon Athena.

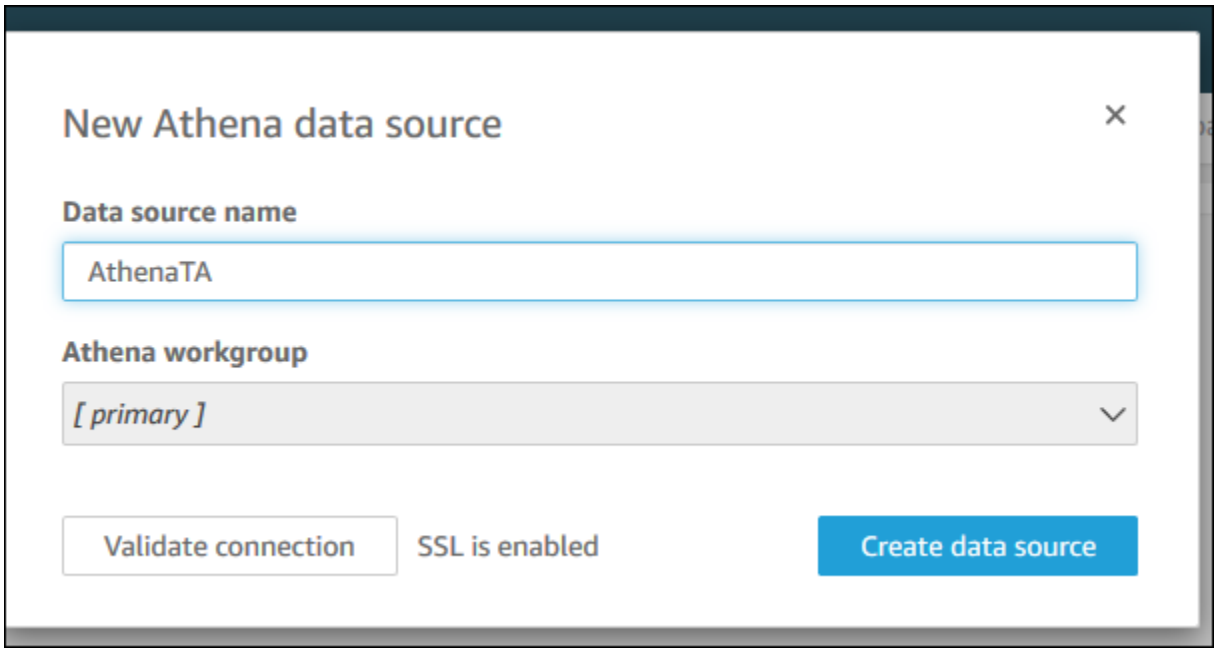
Créer un tableau de bord dans Amazon QuickSight

Vous pouvez également configurer Amazon QuickSight afin que vous puissiez afficher vos données dans un tableau de bord et visualiser les informations de votre rapport.

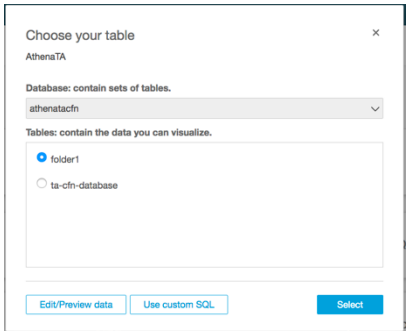
> **Note**
>
> Vous devez utiliser la région US East (N. Virginia) (USA Est (Virginie du Nord)..

Pour créer un tableau de bord dans Amazon QuickSight

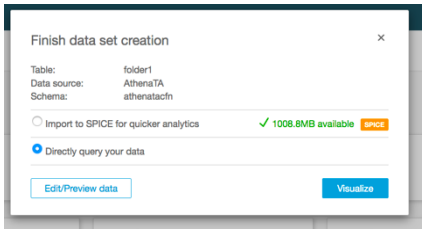
1. Accédez à la console Amazon QuickSight et connectez-vous à votre compte.
2. Choisissez New analysis (Nouvelle analyse), New dataset (Nouvel ensemble de données), puis.Athena.
3. Dans la boîte de dialogue New Athena data source (Nouvelle source de données Athena), indiquez un nom de source de données tel que AthenaTA, puis choisissez Create data source (Création de source de données).



4. Dans la boîte de dialogue Choose your table (Choisir votre table), choisissez la table athenatacfn, puis folder1, et enfin Select (Sélectionner).



5. Dans la boîte de dialogue Finish data set creation (Terminer la création d'un ensemble de données), choisissez Directly query your data (Interroger directement vos données, puis Visualize (Visualiser).

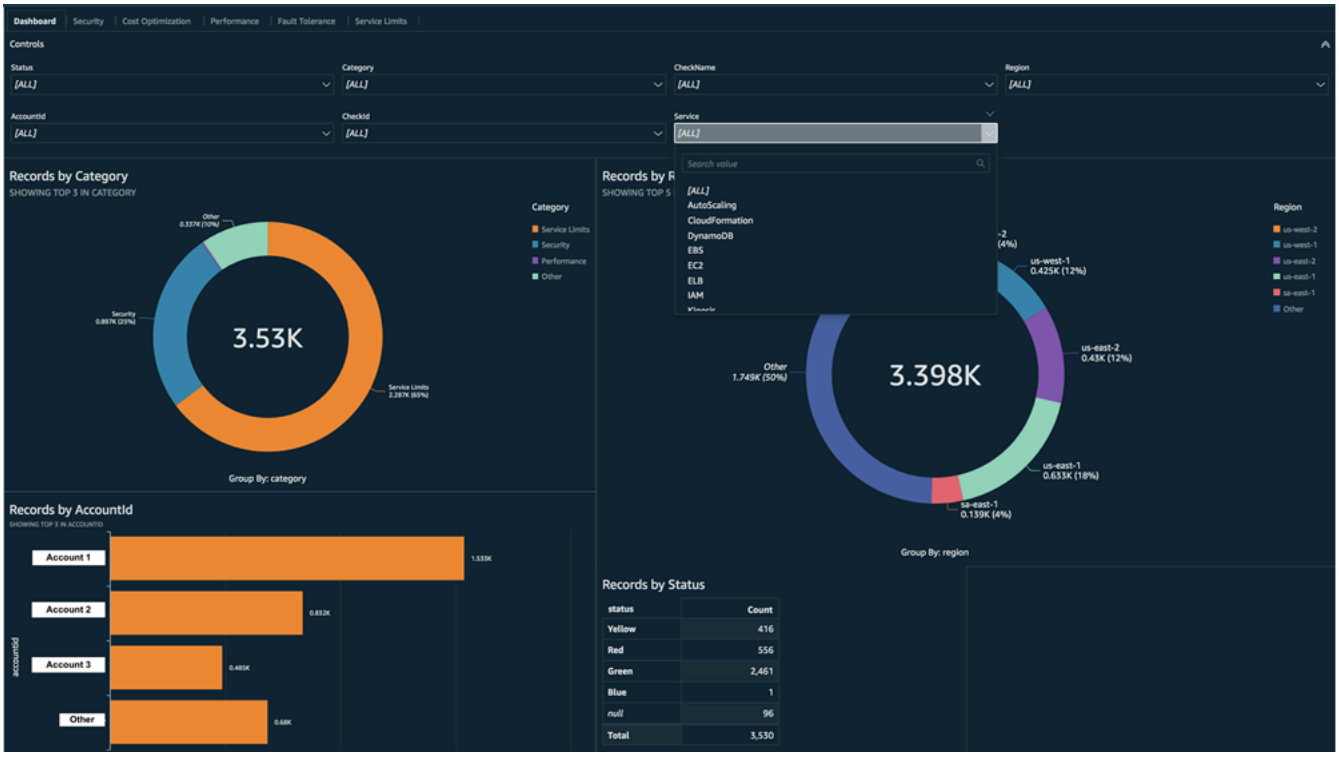


Vous pouvez maintenant créer un tableau de bord dans Amazon QuickSight Pour de plus amples informations, consultez Utilisation de tableaux de bord dans le Guide de l'utilisateur Amazon QuickSight.

Example : tableau de bord Amazon QuickSight

Le tableau de bord suivant en exemple présente des informations sur les vérifications Trusted Advisor, telles que les suivantes :

- ID de compte affectés
- Résumé par régions AWS
- Catégories de vérification
- Statuts de vérification
- Nombre d'entrées dans le rapport pour chaque compte



> **Note**
>
> Si vous rencontrez des erreurs d'autorisation lors de la création de votre tableau de bord, assurez-vous qu'Amazon QuickSight peut utiliser Athena. Pour plus d'informations, consultez Je ne parviens pas à me connecter à Amazon Athena dans le Guide de l'utilisateur Amazon QuickSight.

Pour plus d'informations et des exemples sur la visualisation des données de votre rapport, consultez Afficher les recommandations AWS Trusted Advisor à grande échelle avec AWS Organizations dans le Blog Gestion & Gouvernance AWS.

Résolution des problèmes

Si vous rencontrez des problèmes avec ce didacticiel, consultez les conseils de dépannage suivants.

Je ne vois pas les dernières données dans mon rapport

Lorsque vous créez un rapport, la fonctionnalité de vue organisationnelle n'actualise pas automatiquement les vérifications Trusted Advisor dans votre organisation. Pour obtenir les derniers résultats de vérification, actualisez les vérifications du compte de gestion et de chaque compte

de membre de l'organisation. Pour de plus amples informations, veuillez consulter Actualiser les vérifications Trusted Advisor.

J'ai des colonnes en double dans le rapport

La console Athena peut afficher l'erreur suivante dans votre tableau si votre rapport comporte des colonnes en double.

```
HIVE_INVALID_METADATA: Hive metadata for table folder1 is invalid: Table descriptor contains duplicate columns
```

Par exemple, si vous avez ajouté une colonne dans votre rapport qui existe déjà, cela peut provoquer des problèmes lorsque vous essayez d'afficher les données du rapport dans la console Athena. Vous pouvez suivre ces étapes pour résoudre ce problème.

Recherche de colonnes en double

Vous pouvez utiliser la console AWS Glue pour afficher le schéma et identifier rapidement si vous avez des colonnes en double dans votre rapport.

Pour rechercher des colonnes en double

1. Ouvrez la console AWS Glue, à l'adresse https://console.aws.amazon.com/glue/.
2. Si vous ne l'avez pas déjà fait, dans le sélecteur de région, choisissez la région US East (N. Virginia) (USA Est (Virginie du Nord)).
3. Dans le volet de navigation, choisissez Tables.
4. Choisissez le nom de votre dossier, tel que ***folder1***, puis sous Schema, affichez les valeurs de Column name (Nom de la colonne).

   Si vous disposez d'une colonne en double, vous devez charger un nouveau rapport dans votre compartiment Amazon S3. Examinez la section Télécharger un nouveau rapport suivante.

Télécharger un nouveau rapport

Une fois la colonne en double identifiée, nous vous recommandons de remplacer le rapport existant par un nouveau. Cela garantit que les ressources créées à partir de ce didacticiel utilisent les données de rapport les plus récentes de votre organisation.

Pour télécharger un nouveau rapport

1. Si vous ne l'avez pas déjà fait, actualisez vos vérifications Trusted Advisor pour les comptes de votre organisation. Consultez Actualiser les vérifications Trusted Advisor.
2. Créez et téléchargez un autre rapport JSON dans la console Trusted Advisor. Consultez Créer des rapports de vue organisationnelle. Vous devez utiliser un fichier JSON pour ce didacticiel.
3. Connectez-vous à la AWS Management Console et ouvrez la console Amazon S3 à l'adresse https://console.aws.amazon.com/s3/.
4. Choisissez votre compartiment Amazon S3 et choisissez le dossier *folder1*.
5. Sélectionnez les rapports *resources*.json précédents et choisissez Delete (Supprimer).
6. Dans la page Delete objects (Suppression d'objets), sous Permanently delete objects? (Supprimer définitivement des objets ?), entrez **permanently delete**, puis choisissez Delete objects (Supprimer les objets).
7. Dans votre compartiment S3, choisissez Upload (Télécharger), puis spécifiez le nouveau rapport. Cette action met automatiquement à jour votre table Athena et les ressources d'analyseur AWS Glue avec les données de rapport les plus récentes. La mise à jour de vos ressources peut prendre quelques minutes.
8. Entrez une nouvelle requête dans la console Athena. Consultez Interroger les données dans Amazon Athena.

> **Note**
>
> Si vous rencontrez toujours des problèmes avec ce didacticiel, vous pouvez créer une demande d'assistance technique dans le Centre AWS Support.

Afficher les contrôles AWS Trusted Advisor optimisés par AWS Config

AWS Config est un service qui évalue et audite en permanence vos configurations de ressources en fonction des paramètres souhaités. AWS Config fournit des règles gérées prédéfinies et des contrôles de conformité personnalisables que AWS Config utilise pour évaluer la conformité de vos ressources AWS avec les bonnes pratiques courantes.

La console AWS Config vous guide à travers le processus de configuration et d'activation des règles gérées. Vous pouvez également utiliser la AWS Command Line Interface (AWS CLI) ou l'API AWS Config pour transmettre le code JSON qui définit votre configuration d'une règle gérée. Vous pouvez personnaliser le comportement d'une règle gérée en fonction de vos besoins. Vous pouvez personnaliser les paramètres d'une règle pour définir les attributs dont vos ressources doivent disposer pour être conformes à la règle. Pour en savoir plus sur l'activation de AWS Config, voir le Guide du développeur AWS Config.

Les règles gérées AWS Config permettent la mise en œuvre d'un ensemble de contrôles Trusted Advisor dans toutes les catégories. Lorsque vous activez certaines règles gérées, les contrôles Trusted Advisor correspondants sont automatiquement activés. Pour savoir quels contrôles Trusted Advisor sont optimisés par des règles gérées AWS Config spécifiques, voir Référence de la vérification AWS Trusted Advisor.

Les contrôles optimisés par AWS Config sont disponibles pour les clients disposant de plans AWS Business Support, AWS Enterprise On-Ramp et AWS Enterprise Support. Si vous activez AWS Config et que vous disposez de l'un de ces plans de support AWS, des recommandations basées sur les règles gérées AWS Config déployées correspondantes s'afficheront automatiquement.

> **Note**
>
> Les résultats de ces contrôles sont actualisés automatiquement lorsque les règles gérées AWS Config sont mises à jour. Les demandes d'actualisation ne sont pas autorisées. Actuellement, vous ne pouvez pas exclure des ressources de cette vérification.

Résolution des problèmes

Si vous rencontrez des problèmes avec cette intégration, consultez les informations de dépannage suivantes.

Table des matières

J'ai activé l'enregistrement et les règles gérées pour AWS Config, mais aucun contrôle Trusted Advisor correspondant ne s'affiche.

Une fois que la règle AWS Config a généré les résultats de l'évaluation, vous pouvez afficher ces derniers dans Trusted Advisor en temps quasi réel. Si vous rencontrez toujours des problèmes avec cette fonctionnalité, vous pouvez créer une demande de support technique dans le Centre AWS Support.

J'ai déployé deux fois la même règle gérée AWS Config. Que vais-je voir dans Trusted Advisor ?

Les résultats de contrôle Trusted Advisor contiennent des entrées distinctes pour chaque règle gérée que vous configurez.

J'ai désactivé l'enregistrement pour AWS Config dans une région AWS. Que vais-je voir dans Trusted Advisor ?

Si vous avez désactivé l'enregistrement des ressources pour AWS Config dans une région AWS, Trusted Advisor ne recevra plus de données pour les règles gérées et les contrôles correspondants dans cette région. Les résultats existants des règles gérées restent actifs dans AWS Config et Trusted Advisor jusqu'à l'expiration de AWS Config, conformément à la politique de conservation des enregistreurs. La suppression d'une règle gérée entraîne généralement la suppression des données de contrôle Trusted Advisor en temps quasi réel.

Affichage des contrôles AWS Security Hub dans AWS Trusted Advisor

Une fois que vous avez activé AWS Security Hub pour le Compte AWS, vous pouvez consulter les contrôles de sécurité et leurs résultats dans la console de Trusted Advisor. Vous pouvez utiliser les contrôles de Security Hub pour identifier les vulnérabilités de sécurité de votre compte de la même manière que vous pouvez utiliser les vérifications Trusted Advisor. Vous pouvez afficher l'état de la vérification, la liste des ressources affectées, puis suivre les recommandations de Security Hub pour résoudre les problèmes de sécurité. Vous pouvez utiliser cette fonction pour trouver des recommandations de sécurité à partir de Trusted Advisor et Security Hub dans un emplacement pratique.

Remarques

- À partir de Trusted Advisor, vous pouvez afficher les contrôles de la norme de sécurité Bonnes pratiques de sécurité de base AWS, sauf pour les contrôles dotés de Category: Recover > Resilience (Catégorie : Récupérer > Résilience). Pour obtenir la liste des contrôles pris en charge, consultez les contrôles des Bonnes pratiques de sécurité de base de AWS dans le Guide de l'utilisateur de AWS Security Hub.

  Pour plus d'informations sur les catégories de Security Hub, consultez Catégories de contrôle.
- Actuellement, lorsque Security Hub ajoute de nouveaux contrôles de la norme de sécurité Bonnes pratiques de sécurité de base AWS, il peut y avoir un délai de deux à quatre semaines avant de pouvoir les consulter dans Trusted Advisor. Ce délai est réduit au minimum, mais n'est pas garanti.

Rubriques

Prérequis

Vous devez respecter les conditions requises suivantes pour activer l'intégration de Security Hub avec Trusted Advisor :

- Vous devez posséder un plan de support Business, Enterprise On-Ramp ou Enterprise pour utiliser cette fonction. Vous pouvez trouver un plan de support à partir du Centre AWS Support ou à partir de la page Plans de support. Pour plus d'informations, consultez Comparer les plans de AWS Support.
- Vous devez activer l'enregistrement de ressource dans AWS Config pour les Régions AWS souhaitées pour les contrôles de Security Hub. Pour plus d'informations, consultez Activation et configuration de AWS Config.

- Vous devez activer Security Hub et sélectionner la norme de sécurité Bonnes pratiques de sécurité de base v1.0.0 de AWS. Si vous ne l'avez pas encore fait, consultez Configuration de AWS Security Hub dans le Guide de l'utilisateur de AWS Security Hub.

> **Note**
>
> Si vous avez déjà complété ces conditions préalables, vous pouvez passer directement à Afficher les résultats de Security Hub.

À propos des comptes AWS Organizations

Si vous avez déjà complété les conditions préalables pour un compte de gestion, cette intégration est automatiquement activée pour tous les comptes membres de votre organisation. Les comptes membres individuels n'ont pas besoin de contacter AWS Support pour activer cette fonction. Toutefois, les comptes membres de votre organisation doivent activer Security Hub s'ils veulent consulter leurs résultats dans Trusted Advisor.

Si vous souhaitez désactiver cette intégration pour un compte membre spécifique, consultez Désactiver cette fonction pour les comptes AWS Organizations.

Afficher les résultats de Security Hub

Après avoir activé Security Hub pour votre compte, l'affichage des résultats de Security Hub peut prendre jusqu'à 24 heures pour s'afficher dans la page Security (Sécurité) de la console de Trusted Advisor.

Afficher les résultats de Security Hub dans Trusted Advisor

1. Accédez à la console de Trusted Advisor, puis choisissez la catégorie Security (Sécurité).
2. Dans le champ de la Search by keyword (Recherche par mot-clé), saisissez le nom ou la description du contrôle.

> **Tip**
>
> Pour la Source, vous pouvez choisir AWS Security Hub pour filtrer les contrôles de Security Hub.

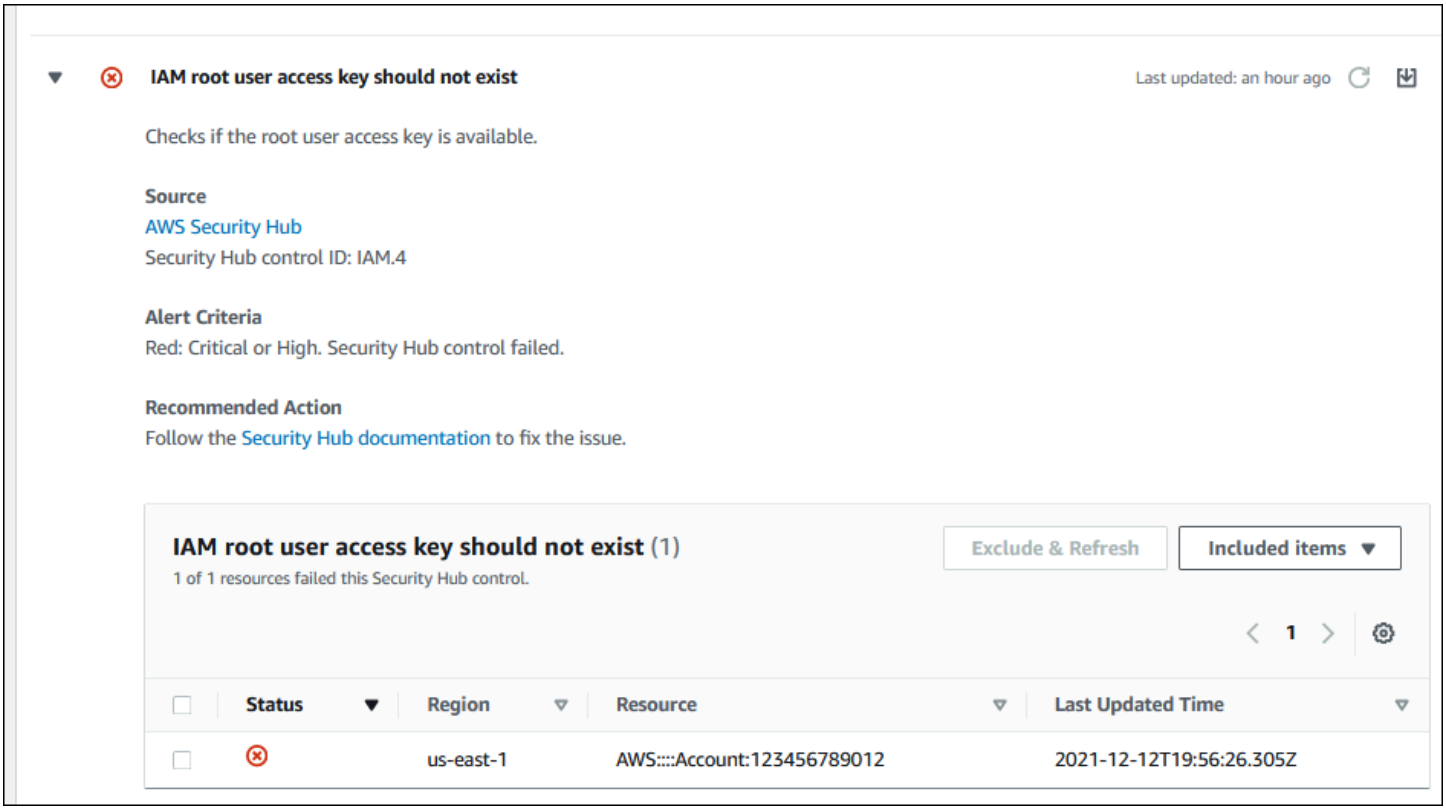
3. Choisissez le nom du contrôle de Security Hub pour afficher les informations suivantes :

   - Description : décrit comment ce contrôle vérifie les vulnérabilités de sécurité de votre compte.
   - Source : indique si la vérification provient de AWS Trusted Advisor ou AWS Security Hub. Pour les contrôles de Security Hub, vous pouvez trouver l'ID du contrôle.
   - Alert Criteria (Critères d'alerte) : l'état du contrôle. Par exemple, si Security Hub détecte un problème important, le statut peut être Red: Critical or High (Rouge : Critique ou Élevé).
   - Recommended Action (Action recommandée) : utilisez le lien de la documentation de Security Hub pour trouver les étapes recommandées et résoudre le problème.
   - Security Hub resources (Ressources de Security Hub) : vous pouvez trouver les ressources de votre compte où Security Hub a détecté un problème.

> **Remarques**
>
> - Vous devez utiliser Security Hub pour exclure des ressources des résultats. Actuellement, vous ne pouvez pas utiliser la console de Trusted Advisor pour exclure des éléments des contrôles de Security Hub. Pour plus d'informations, consultez Paramètres de l'état du flux de travail pour les résultats.
> - La fonction de vue organisationnelle prend en charge cette intégration avec Security Hub. Vous pouvez afficher les résultats des contrôles de Security Hub dans l'ensemble de votre organisation, puis créer et télécharger des rapports. Pour plus d'informations, consultez Vue organisationnelle pour AWS Trusted Advisor.

Example Exemple : le contrôle de Security Hub pour la clé d'accès utilisateur IAM ne devrait pas exister

Voici un exemple de résultat pour un contrôle de Security Hub dans la console de Trusted Advisor.



Actualiser les résultats de Security Hub

Après avoir activé une norme de sécurité, Security Hub peut prendre jusqu'à deux heures pour vous fournir des résultats des ressources. Les données peuvent prendre jusqu'à 24 heurs pour s'afficher dans la console de Trusted Advisor. Si vous avez récemment activé la norme de sécurité AWS Bonnes pratiques de sécurité de base v1.0.0, vérifiez la console de Trusted Advisor plus tard.

> **Note**
>
> - La planification d'actualisation de chaque contrôle de Security Hub est périodique ou déclenchée par des modifications. Actuellement, vous ne pouvez pas utiliser la console de Trusted Advisor ou l'API AWS Support pour actualiser les contrôles de Security Hub. Pour plus d'informations, consultez Planification de l'exécution des vérifications de sécurité.
> - Vous devez utiliser Security Hub pour exclure des ressources de vos résultats. Actuellement, vous ne pouvez pas utiliser la console de Trusted Advisor pour exclure des éléments des contrôles de Security Hub. Pour plus d'informations, consultez Paramètres de l'état du flux de travail pour les résultats.

Désactiver Security Hub de Trusted Advisor

Suivez cette procédure si vous ne souhaitez pas que les informations de Security Hub s'affichent dans la console de Trusted Advisor. Cette procédure désactive uniquement l'intégration de Security Hub avec Trusted Advisor. Elle n'affectera pas vos configurations de Security Hub. Vous pouvez continuer à utiliser la console de Security Hub pour afficher vos contrôles de sécurité, vos ressources, et vos recommandations.

Pour désactiver l'intégration de Security Hub

1. Contactez AWS Support et demandez la désactivation de l'intégration de Security Hub avec Trusted Advisor.

   Une fois que AWS Support désactive cette fonction, Security Hub n'envoie plus de données à Trusted Advisor. Vos données de Security Hub seront supprimées de Trusted Advisor.
2. Si vous souhaitez activer à nouveau cette intégration, contactez AWS Support.

Désactiver cette fonction pour les comptes AWS Organizations

Si vous avez déjà complété la procédure précédente pour un compte de gestion, l'intégration de Security Hub est automatiquement supprimée de tous les comptes membres de votre organisation. Les comptes membres individuels de votre organisation n'ont pas besoin de contacter AWS Support séparément.

Si vous êtes un compte membre au sein d'une organisation, vous pouvez contacter AWS Support pour supprimer cette fonction de votre compte uniquement.

Résolution des problèmes

Si vous rencontrez des problèmes avec cette intégration, consultez les informations de dépannage suivantes.

Table des matières

- Je souhaite activer ou désactiver cette fonction pour un compte membre appartenant à une organisation AWS
- Je vois plusieurs Régions AWS pour la même ressource affectée pour une vérification Security Hub
- J'ai désactivé Security Hub ou AWS Config dans une région
- Mon contrôle est archivé dans Security Hub, mais je vois toujours les résultats dans Trusted Advisor
- Je n'arrive toujours pas à visualiser les résultats de mon Security Hub

Je ne vois pas les résultats de Security Hub dans la console de Trusted Advisor

Vérifiez si vous avez complété les étapes suivantes :

- Vous devez avoir un plan de support Business, Enterprise On-Ramp ou Enterprise.
- Vous avez activé l'enregistrement de ressource dans AWS Config au sein de la même région de Security Hub.
- Vous avez activé Security Hub et sélectionné la norme de sécurité AWS Bonnes pratiques de sécurité de base v1.0.0.
- Les nouveaux contrôles provenant de Security Hub sont ajoutés en tant que vérifications dans Trusted Advisor dans un délai de deux à quatre semaines. Consultez la note.

Pour plus d'informations, consultez le Prérequis.

J'ai configuré Security Hub et AWS Config correctement, mais les résultats ne s'affichent toujours pas

Security Hub peut prendre jusqu'à deux heures pour obtenir des résultats des ressources. Les données peuvent prendre jusqu'à 24 heurs pour s'afficher dans la console de Trusted Advisor. Vérifiez la console de Trusted Advisor plus tard.

> **Remarques**
>
> - Seuls les résultats pour vos contrôles dans la norme de sécurité AWS Bonnes pratiques de sécurité de base s'afficheront dans Trusted Advisor, sauf pour les contrôles dotés de Category: Recover > Resilience (Catégorie : Récupérer > Résilience).

- S'il y a un problème de service avec Security Hub ou si Security Hub n'est pas disponible, les résultats peuvent prendre jusqu'à 24 heures pour s'afficher dans Trusted Advisor. Vérifiez la console de Trusted Advisor plus tard.

Je souhaite désactiver des contrôles spécifiques de Security Hub

Security Hub envoie vos données à Trusted Advisor automatiquement. Si vous désactivez un contrôle de Security Hub ou si vous ne disposez plus de ressources pour ce contrôle, les résultats ne s'afficheront pas dans Trusted Advisor.

Vous pouvez vous connecter à la console de Security Hub et vérifier si le contrôle est activé ou désactivé.

Si vous désactivez un contrôle de Security Hub ou tous les contrôles de la norme de sécurité Bonnes pratiques de sécurité de base AWS, vos résultats seront archivés dans les cinq jours suivants. Cette période d'archivage de 5 jours est approximative et n'est pas garantie. Lorsque vos résultats sont archivés, ils sont supprimés de Trusted Advisor.

Pour plus d'informations, consultez les rubriques suivantes :

- Désactivation et activation des contrôles individuels
- Désactivation ou activation d'une norme de sécurité

Je souhaite trouver mes ressources de Security Hub exclues

À partir de la console de Trusted Advisor, vous pouvez choisir le nom de contrôle de votre Security Hub, puis choisir l'option Excluded items (Éléments exclus). Cette option affiche toutes les ressources supprimées dans Security Hub.

Si l'état du flux de travail d'une ressource est défini sur `SUPPRESSED`, cette ressource est alors un élément exclu dans Trusted Advisor. Vous ne pouvez pas supprimer les ressources de Security Hub à partir de la console de Trusted Advisor. Pour ce faire, utilisez la console de Security Hub. Pour plus d'informations, consultez Paramètres de l'état du flux de travail pour les résultats.

Je souhaite activer ou désactiver cette fonction pour un compte membre appartenant à une organisation AWS

Par défaut, les comptes membres héritent de la fonction du compte de gestion pour AWS Organizations. Si le compte de gestion a activé la fonction, alors tous les comptes de l'organisation disposeront également de cette fonction. Si vous possédez un compte membre et souhaitez apporter des modifications spécifiques au compte, vous devez contacter AWS Support.

Je vois plusieurs Régions AWS pour la même ressource affectée pour une vérification Security Hub

Certains Services AWS sont globaux et ne sont pas spécifiques à une région, comme IAM et Amazon CloudFront. Par défaut, les ressources globales telles que les compartiments Amazon S3 apparaissent dans la région USA Est (Virginie du Nord).

Pour les vérifications Security Hub qui évaluent les ressources pour les services globaux, vous pouvez voir plus d'un élément pour les ressources affectées. Par exemple, si l'option `Hardware MFA should be enabled for the root user` identifie que votre compte n'a pas activé cette fonction, vous verrez plusieurs régions dans le tableau pour la même ressource.

Vous pouvez configurer Security Hub et AWS Config pour que plusieurs régions n'apparaissent pas pour la même ressource. Pour plus d'informations, consultez Contrôles des bonnes pratiques de base AWS que vous pourriez vouloir désactiver.

J'ai désactivé Security Hub ou AWS Config dans une région

Si vous arrêtez l'enregistrement des ressources avec AWS Config ou que vous désactivez Security Hub dans une Région AWS, Trusted Advisor ne reçoit plus de données pour aucun contrôle dans cette région. Trusted Advisor supprime vos résultats de dans les 7 à 9 jours. Ce délai est réduit au minimum, mais n'est pas garanti. Pour de plus amples informations, veuillez consulter Disabling Security Hub (Désactiver Security Hub).

Pour désactiver cette fonction pour votre compte, consultez Désactiver Security Hub de Trusted Advisor.

Mon contrôle est archivé dans Security Hub, mais je vois toujours les résultats dans Trusted Advisor

Lorsque le statut `RecordState` passe à `ARCHIVED` pour un résultat, Trusted Advisor supprime le résultat pour ce contrôle Security Hub de votre compte. Il se peut que le résultat soit encore

visible dans Trusted Advisor pendant 7 à 9 jours avant qu'il ne soit supprimé. Ce délai est réduit au minimum, mais n'est pas garanti.

Je n'arrive toujours pas à visualiser les résultats de mon Security Hub

Si vous rencontrez toujours des problèmes avec cette fonction, vous pouvez créer une demande de support technique dans le Centre AWS Support.

Inscription à AWS Compute Optimizer pour les vérifications de Trusted Advisor

Compute Optimizer est un service qui analyse la configuration et les métriques d'utilisation de vos ressources AWS. Ce service indique si vos ressources sont correctement configurées pour assurer leur efficacité et leur fiabilité. Il suggère également des améliorations que vous pouvez implémenter pour améliorer les performances de la charge de travail. Avec Compute Optimizer, vous voyez les mêmes recommandations dans vos vérifications de Trusted Advisor.

Vous pouvez inscrire soit uniquement votre Compte AWS, ou tous les comptes membres qui font partie d'une organisation dans AWS Organizations. Pour plus d'informations, consultez Démarrer dans le Guide de l'utilisateur AWS Compute Optimizer.

Une fois que vous vous êtes inscrit à Compute Optimizer, les contrôles suivants reçoivent des données provenant de vos fonctions Lambda et de vos volumes Amazon EBS. La génération des résultats et des recommandations d'optimisation peut prendre jusqu'à 12 heures. L'affichage de vos résultats peut prendre jusqu'à 48 heures dans Trusted Advisor pour les vérifications suivantes :

Optimisation des coûts

- Volumes Amazon EBS surprovisionnés
- Fonctions AWS Lambda surprovisionnées pour la taille de la mémoire

Performances

- Volumes Amazon EBS sous-provisionnés
- Fonctions AWS Lambda sous-provisionnées pour la taille de la mémoire

Remarques

- Les résultats de ces contrôles sont actualisés automatiquement plusieurs fois par jour. Les demandes d'actualisation ne sont pas autorisées. Plusieurs heures peuvent encore être nécessaires pour que les modifications apparaissent. Actuellement, vous ne pouvez pas exclure des ressources de cette vérification.
- Trusted Advisor a déjà les vérifications de volumes Amazon EBS sous-utilisés et de volumes magnétiques Amazon EBS surutilisés.

  Une fois que vous vous êtes inscrit à Compute Optimizer, nous vous recommandons d'utiliser plutôt les nouveaux contrôles des volumes surprovisionnés Amazon EBS et des volumes sous-provisionnés Amazon EBS.

Informations connexes

Pour plus d'informations, consultez les rubriques suivantes :

- Affichage des recommandations de volume Amazon EBS dans le Guide de l'utilisateur AWS Compute Optimizer
- Affichage des recommandations de fonction Lambda dans le Guide de l'utilisateur AWS Compute Optimizer
- Configuration de la mémoire de fonction Lambda dans le Guide du développeur AWS Lambda
- Demander des modifications pour vos volumes Amazon EBS dans le Guide de l'utilisateur Amazon EC2 pour les instances Linux

Démarrer avec AWS Trusted Advisor Priority

Trusted Advisor Priority vous aide à sécuriser et à optimiser votre Compte AWS pour mieux respecter les bonnes pratiques AWS. Avec Trusted Advisor Priority, votre équipe Compte AWS peut surveiller votre compte de manière proactive et créer des recommandations prioritaires lorsqu'elle identifie des opportunités pour vous.

Par exemple, votre équipe de compte peut voir que l'utilisateur root de votre compte AWS ne dispose d'aucune authentification multifactorielle (MFA). Votre équipe de compte peut créer une recommandation pour que vous preniez des mesures immédiates en cas de vérification, par exemple

`MFA on Root Account`. La recommandation apparaît comme une recommandation prioritaire active sur la page Trusted Advisor Priority de la console Trusted Advisor. Vous suivez ensuite les recommandations pour le résoudre.

Les recommandations de Trusted Advisor Priority peuvent provenir des deux sources suivantes :

- Services AWS : des services tels que Trusted Advisor, AWS Security Hub et AWS Well-Architected créent automatiquement des recommandations. Votre équipe de compte partage ces recommandations avec vous pour qu'elles apparaissent dans Trusted Advisor Priority.
- Votre équipe de compte : votre équipe de compte peut créer des recommandations manuelles.

Trusted Advisor Priority vous aide à vous concentrer sur les recommandations les plus importantes. Vous et votre équipe de compte pouvez suivre le cycle de vie de la recommandation, depuis le moment où votre équipe de compte a partagé la recommandation, jusqu'au moment où vous l'acceptez, la résolvez ou la rejetez. Vous pouvez utiliser Trusted Advisor Priority pour trouver des recommandations pour tous les comptes membres de votre organisation.

Rubriques

Prérequis

Vous devez remplir les conditions suivantes pour utiliser Trusted Advisor Priority :

- Vous devez disposer d'un plan de support Enterprise.
- Votre compte doit faire partie d'une organisation ayant activé toutes les fonctionnalités dans AWS Organizations. Pour de plus amples informations, consultez Activation de toutes les fonctionnalités de l'organisation dans le Guide de l'utilisateur AWS Organizations.
- Votre organisation doit avoir activé l'accès sécurisé à Trusted Advisor. Pour activer l'accès approuvé, connectez-vous avec un compte de gestion. Ouvrez la page Votre organisation dans la console Trusted Advisor.
- Vous devez être connecté à votre compte AWS pour afficher les recommandations de Trusted Advisor Priority pour votre compte.
- Vous devez être connecté au compte de gestion de l'organisation ou à un compte d'administrateur délégué pour afficher les recommandations agrégées pour l'ensemble de votre organisation. Pour obtenir des instructions sur la façon d'enregistrer des comptes d'administrateurs délégués, voir Enregistrer des administrateurs délégués.
- Vous devez disposer des autorisations AWS Identity and Access Management (IAM) pour accéder à Trusted Advisor Priority. Pour plus d'informations sur la manière de contrôler l'accès à Trusted Advisor Priority, voir Gérez l'accès à AWS Trusted Advisor et AWS politiques gérées pour AWS Trusted Advisor.

Activer Trusted Advisor Priority

Demandez à votre équipe de compte d'activer cette fonctionnalité pour vous. Vous devez disposer d'un plan Enterprise Support et être le propriétaire du compte de gestion de votre organisation. Si la page Trusted Advisor Priority de la console indique que vous avez besoin d'un accès sécurisé avec AWS Organizations, choisissez Activer l'accès de confiance avec AWS Organizations. Pour plus d'informations, consultez la section Prérequis.

Voir les recommandations hiérarchisées

Après que votre équipe de compte a activé Trusted Advisor Priority pour vous, vous pouvez afficher les dernières recommandations pour votre compte AWS.

Pour visualiser les recommandations hiérarchisées

1. Accédez à la console Trusted Advisor sur https://console.aws.amazon.com/trustedadvisor/home.
2. La page Trusted Advisor Priority affiche les éléments suivants :

Si vous utilisez un compte de gestion ou un compte d'administrateur délégué AWS Organizations, passez à l'onglet Mon compte.

- Actions needed (Actions nécessaires) : le nombre de recommandations en attente d'une réponse ou en cours de traitement.
- Overview (Présentation) : les informations suivantes :
  - Recommandations rejetées au cours des 90 derniers jours
  - Recommandations résolues au cours des 90 derniers jours
  - Recommandations sans mise à jour depuis plus de 30 jours
  - Le temps moyen de résolution des recommandations

3. Sous l'onglet Actif, la section Recommandations priorisées actives affiche les recommandations que votre équipe de compte a priorisées pour vous. L'onglet Fermé affiche les recommandations résolues ou rejetées.

   - Pour filtrer vos résultats, utilisez les options suivantes :
     - Recommendation (Recommandation) : saisissez des mots-clés pour rechercher par nom. Il peut s'agir d'un nom de vérification ou d'un nom personnalisé créé par votre équipe de compte.
     - Status (État) : indique si la recommandation est en attente de réponse, en cours, rejetée ou résolue.
     - Source (Source) : origine d'une recommandation hiérarchisée. La recommandation peut provenir de Services AWS, de votre équipe Compte AWS ou d'un événement de service planifié.
     - Category (Catégorie) : la catégorie de recommandation, telle que la sécurité ou l'optimisation des coûts.
     - Age (Âge) : quand votre équipe de compte a partagé la recommandation avec vous.

4. Choisissez une recommandation pour en savoir plus et afficher les ressources et les actions recommandées. Vous pouvez ensuite accuser réception ou rejeter la recommandation.

Pour afficher les recommandations priorisées pour tous les comptes de votre organisation AWS

Le compte de gestion et les administrateurs délégués Trusted Advisor Priority peuvent afficher les recommandations agrégées pour l'ensemble de votre organisation.

> **Note**
>
> Les comptes membres n'ont pas accès aux recommandations agrégées.

1. Accédez à la console Trusted Advisor à l'adresse https://console.aws.amazon.com/trustedadvisor/home.
2. Sur la page Trusted Advisor Priority, assurez-vous que vous êtes sur l'onglet Mon organisation.
3. Pour afficher les recommandations relatives à un compte, sélectionnez le compte en question dans la liste déroulante Sélectionnez un compte dans votre organisation. Vous pouvez également afficher les recommandations pour l'ensemble de vos comptes.

   L'onglet Mon organisation affiche les éléments suivants :

   - Actions nécessaires : nombre de recommandations en attente d'une réponse ou en cours de traitement pour l'ensemble de votre organisation.
   - Vue d'ensemble : affiche les éléments suivants :

     - Recommandations ignorées au cours des 90 derniers jours

     - Recommandations résolues au cours des 90 derniers jours

     - Recommandations sans mise à jour depuis plus de 30 jours

     - Temps moyen de résolution des recommandations
4. Sous l'onglet Actif, la section Recommandations priorisées actives affiche les recommandations que votre équipe de compte a priorisées pour vous. L'onglet Fermé affiche les recommandations résolues ou rejetées.

   Pour filtrer vos résultats, utilisez les options suivantes :

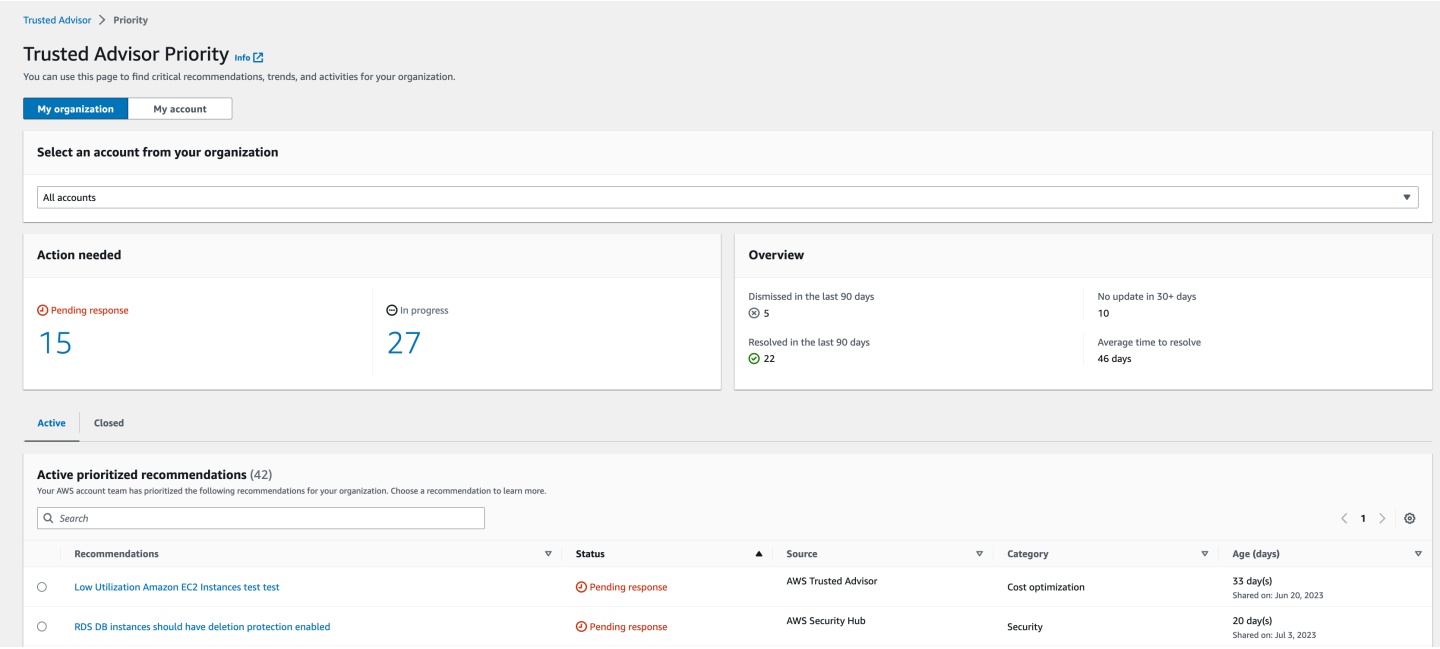
   - Recommendation (Recommandation) : saisissez des mots-clés pour rechercher par nom. Il peut s'agir d'un nom de vérification ou d'un nom personnalisé créé par votre équipe de compte.
   - Status (État) : indique si la recommandation est en attente de réponse, en cours, rejetée ou résolue.

- Source (Source) : origine d'une recommandation hiérarchisée. La recommandation peut provenir de Services AWS, de votre équipe Compte AWS ou d'un événement de service planifié.
- Category (Catégorie) : la catégorie de recommandation, telle que la sécurité ou l'optimisation des coûts.
- Age (Âge) : quand votre équipe de compte a partagé la recommandation avec vous.

5. Choisissez une recommandation pour en savoir plus et pour afficher les comptes et ressources concernés et les actions recommandées. Vous pouvez ensuite accuser réception ou rejeter la recommandation.

Example : recommandations de Trusted Advisor Priority

L'exemple suivant montre 15 recommandations en attente de réponse et 27 recommandations en cours dans la section Action requise. L'image suivante montre deux des recommandations en attente de réponse dans l'onglet Recommandations priorisées actives.



Reconnaître une recommandation

Dans l'onglet Active (Actif), vous pouvez en savoir plus sur la recommandation, puis décider si vous voulez l'accepter.

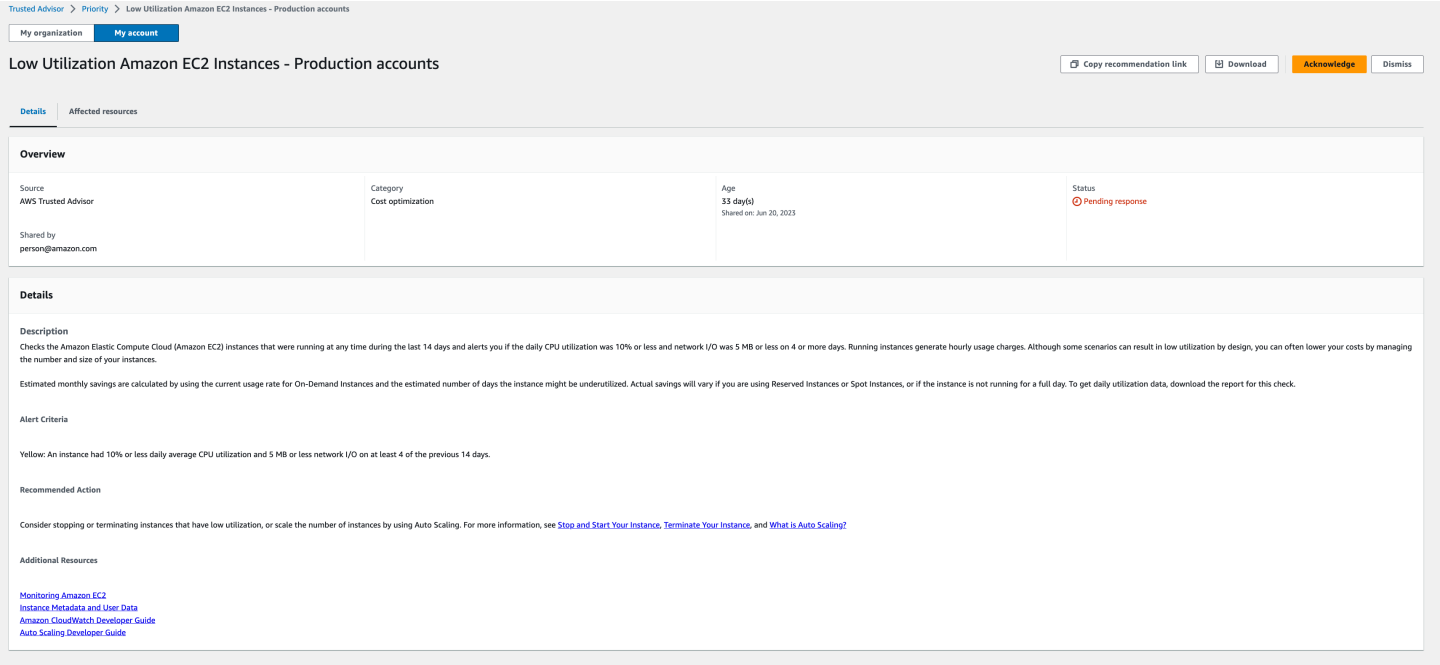
Pour accuser réception d'une recommandation

1. Accédez à la console Trusted Advisor à l'adresse https://console.aws.amazon.com/trustedadvisor/home.
2. Si vous utilisez un compte de gestion ou un compte d'administrateur délégué AWS Organizations, passez à l'onglet Mon compte.
3. Sur la page Trusted Advisor Priority, sous l'onglet Active (Active), choisissez un nom de recommandation.
4. Dans la section Détails, vous pouvez passer en revue les actions recommandées pour résoudre la recommandation.
5. Dans la section Ressources concernées, vous pouvez passer en revue les ressources concernées et les filtrer par état.
6. Sélectionnez I acknowledge (Je confirme).
7. Dans la boîte de dialogue Accuser réception de la recommandation, choisissez Accuser réception.

   L'état de la recommandation passe à In progress (En cours). Les recommandations en cours ou en attente d'une réponse apparaissent dans l'onglet Active (Actif) de la page Trusted Advisor Priority.
8. Suivez les actions recommandées pour résoudre la recommandation. Pour en savoir plus, consultez Résoudre une recommandation.

Example : recommandation manuelle de Trusted Advisor Priority

L'image suivante montre la recommandation Instances EC2 sous-exploitées qui est en attente d'une réponse.



Pour accuser réception d'une recommandation pour tous les comptes de votre organisation AWS

Le compte de gestion ou les administrateurs délégués de Trusted Advisor peuvent accuser réception d'une recommandation pour tous les comptes concernés.

> **Note**
>
> Les comptes membres n'ont pas accès aux recommandations agrégées.

1. Accédez à la console Trusted Advisor à l'adresse https://console.aws.amazon.com/trustedadvisor/home.
2. Sur la page Trusted Advisor Priority, assurez-vous que vous êtes sur l'onglet Mon organisation.
3. Dans l'onglet Actif, sélectionnez le nom d'une recommandation.
4. Sélectionnez I acknowledge (Je confirme).
5. Dans la boîte de dialogue Accuser réception de la recommandation, choisissez Accuser réception.

   L'état de la recommandation passe à In progress (En cours).
6. Suivez les actions recommandées pour résoudre la recommandation. Pour en savoir plus, consultez Résoudre une recommandation.

7. Pour afficher les détails de la recommandation, choisissez le nom de la recommandation.

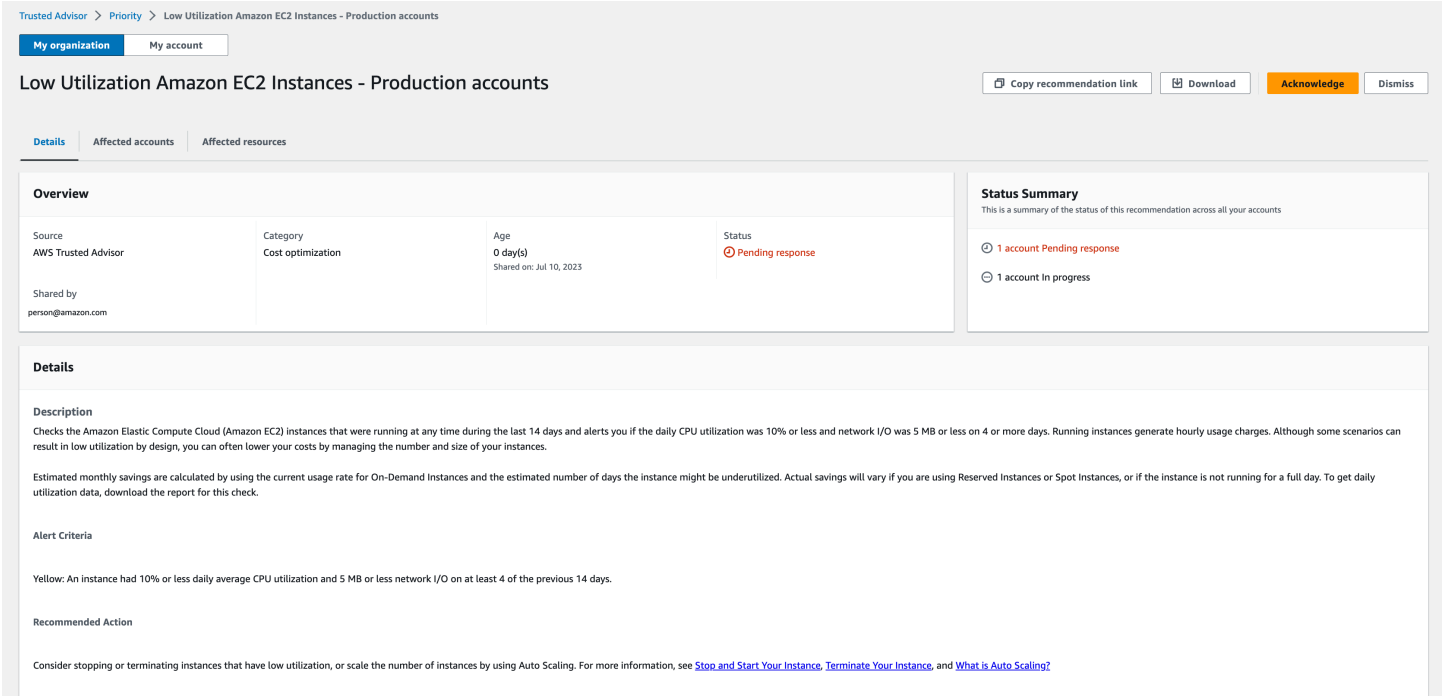
   Dans la section Détails, vous pouvez consulter les informations suivantes concernant la recommandation :

   - Une présentation de la recommandation et une section Détails décrivant les actions recommandées à effectuer.

     Un récapitulatif de statut qui présente les recommandations pour tous les comptes concernés.
   - Dans la section Comptes affectés, vous pouvez passer en revue les ressources concernées pour tous vos comptes. Vous pouvez filtrer par numéro de compte et par statut.
   - Dans la section Ressources affectées, vous pouvez passer en revue les ressources concernées pour tous vos comptes. Vous pouvez filtrer par numéro de compte et par statut.

Example : recommandation manuelle de Trusted Advisor Priority

L'image suivante montre la recommandation Instances Amazon EC2 sous-exploitées qui est en attente d'une réponse. L'un des comptes concernés a accusé réception de la recommandation. Un autre compte est en attente de réponse, la recommandation affiche donc le statut Réponse en attente.



Rejeter une recommandation

Vous pouvez également rejeter une recommandation. Cela signifie que vous accusez réception de la recommandation, mais que vous ne voulez pas y donner suite. Vous pouvez rejeter une recommandation si elle n'est pas pertinente pour votre compte. Par exemple, si vous avez l'intention Compte AWS de supprimer un test, vous n'avez pas besoin de suivre les actions recommandées.

Rejeter une recommandation

1. Accédez à la console Trusted Advisor à l'adresse https://console.aws.amazon.com/trustedadvisor/home.
2. Si vous utilisez un compte de gestion ou un compte d'administrateur délégué AWS Organizations, passez à l'onglet Mon compte.
3. Sur la page Trusted Advisor Priority, sous l'onglet Active (Active), choisissez un nom de recommandation.
4. Sur la page de détails de la recommandation, passez en revue les informations sur les ressources concernées.
5. Si cette recommandation ne s'applique pas à votre compte, choisissez Ignorer.
6. Dans la boîte de dialogue Rejeter une recommandation, sélectionnez une raison pour laquelle vous ne traiterez pas la recommandation.
7. (Facultatif) Saisissez une remarque indiquant la raison pour laquelle vous ignorez la recommandation. Si vous choisissez Autre, vous devez saisir une description dans la section Note.
8. Choisissez Ignorer. Le statut de la recommandation devient Rejected (Rejetée) et apparaît dans l'onglet Closed (Fermée) de la page Trusted Advisor Priority.

Pour ignorer une recommandation pour l'ensemble des comptes de votre organisation AWS

Le compte de gestion ou l'administrateur délégué de Trusted Advisor Priority peut ignorer une recommandation pour l'ensemble de ses comptes.

1. Accédez à la console Trusted Advisor à l'adresse https://console.aws.amazon.com/trustedadvisor/home.
2. Sur la page Trusted Advisor Priority, assurez-vous que vous êtes sur l'onglet Mon organisation.
3. Dans l'onglet Actif, sélectionnez le nom d'une recommandation.

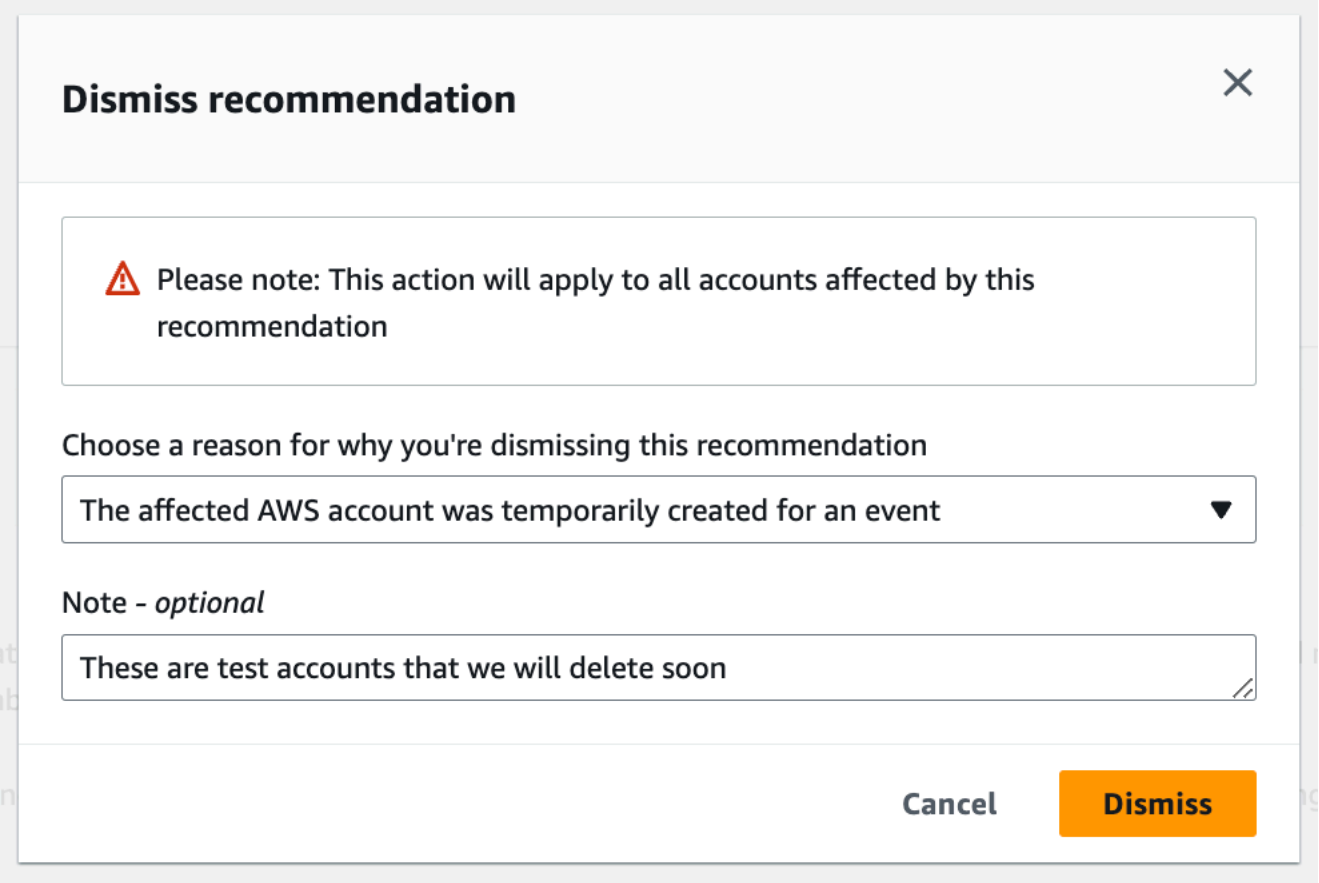
4. Si cette recommandation ne s'applique pas à votre compte, choisissez Ignorer.
5. Dans la boîte de dialogue Rejeter une recommandation, sélectionnez une raison pour laquelle vous ne traiterez pas la recommandation.
6. (Facultatif) Saisissez une remarque indiquant la raison pour laquelle vous ignorez la recommandation. Si vous choisissez Autre, vous devez saisir une justification dans la section Remarque.
7. Choisissez Ignorer. L'état de la recommandation passe à Rejeté. L'état de la recommandation est affiché dans l'onglet Fermé de la page Trusted Advisor Priority.

> **Note**
>
> Vous pouvez choisir le nom de la recommandation et choisir Afficher la note pour trouver le motif du licenciement. Si l'équipe chargée de votre compte a rejeté la recommandation à votre place, son adresse e-mail apparaît à côté de la note.

Trusted Advisor Priority notifie également votre équipe de compte que vous avez rejeté la recommandation.

Example : rejeter une recommandation de Trusted Advisor Priority

L'exemple suivant montre comment rejeter une recommandation.



Résoudre une recommandation

Après avoir accusé réception de la recommandation et effectué les actions recommandées, vous pouvez résoudre la recommandation.

> **Tip**
>
> Après avoir résolu une recommandation, vous ne pouvez pas la rouvrir. Si vous souhaitez revoir la recommandation ultérieurement, consultez Rejeter une recommandation.

Pour résoudre une recommandation

1. Accédez à la console Trusted Advisor sur https://console.aws.amazon.com/trustedadvisor/home.
2. Sur la page Trusted Advisor Priority, assurez-vous que vous êtes sur l'onglet Mon organisation.
3. Sur la pageTrusted Advisor Priority, sélectionnez la recommandation, puis choisissez Resolve (Résoudre).

4. Dans la boîte de dialogue Résoudre les recommandations, choisissez Résoudre. Les recommandations résolues apparaissent sous l'onglet Closed (Fermée) sur la page Trusted Advisor Priority. Trusted Advisor Priority notifie à votre équipe de compte que vous avez résolu la recommandation.

Pour résoudre une recommandation pour l'ensemble des comptes de votre organisation AWS

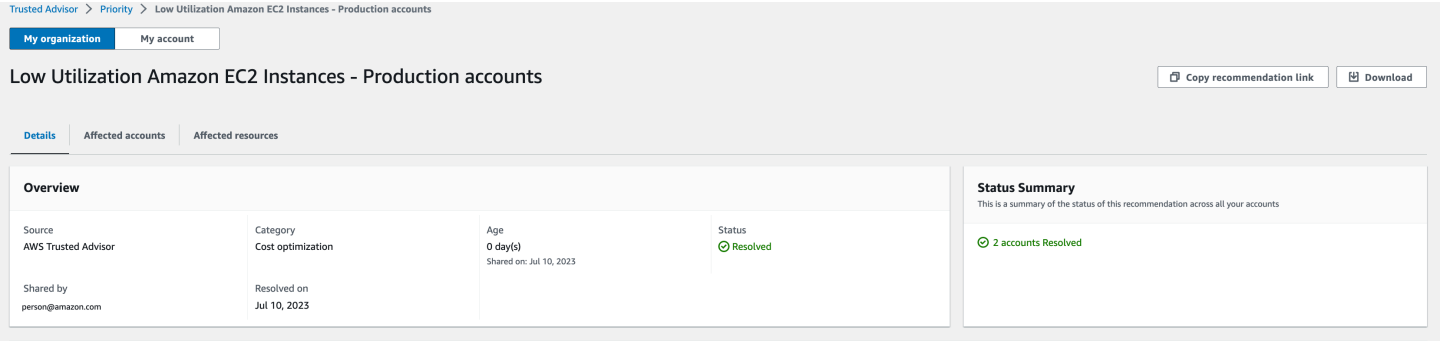
Le compte de gestion ou l'administrateur délégué de Trusted Advisor Priority peut résoudre une recommandation pour l'ensemble de ses comptes.

> **Note**
>
> Les comptes membres n'ont pas accès aux recommandations agrégées.

1. Accédez à la console Trusted Advisor à l'adresse https://console.aws.amazon.com/trustedadvisor/home.
2. Si vous utilisez un compte de gestion ou un compte d'administrateur délégué AWS Organizations, passez à l'onglet Mon compte.
3. Dans l'onglet Actif, sélectionnez le nom d'une recommandation.
4. Si la recommandation ne s'applique pas à votre compte, choisissez Résoudre.
5. Dans la boîte de dialogue Résoudre les recommandations, choisissez Résoudre. Les recommandations résolues apparaissent sous l'onglet Closed (Fermée) sur la page Trusted Advisor Priority. Trusted Advisor Priority notifie à votre équipe de compte que vous avez résolu la recommandation.

Example : recommandation manuelle de Trusted Advisor Priority

L'exemple suivant montre une recommandation Instances Amazon EC2 sous-exploitées résolue.



Rouvrir une recommandation

Après avoir rejeté une recommandation, vous ou votre équipe de compte pouvez rouvrir la recommandation.

Pour rouvrir une recommandation

1. Accédez à la console Trusted Advisor à l'adresse https://console.aws.amazon.com/trustedadvisor/home.
2. Si vous utilisez un compte de gestion ou un compte d'administrateur délégué AWS Organizations, passez à l'onglet Mon compte.
3. Sur la page Trusted Advisor Priority, choisissez l'onglet Closed (Fermée).
4. Sous Closed recommendations (Recommandations fermées), sélectionnez la recommandation qui est Dismissed (Supprimée), puis cliquez sur Reopen (Rouvrir).
5. Dans la boîte de dialogue Rouvrir la recommandation, décrivez pourquoi vous rouvrez la recommandation.
6. Sélectionnez Reopen (Rouvrir). Le statut de la recommandation passe à In progress (En cours) et apparaît sous l'onglet Active (Actif).

   > **Tip**
   >
   > Vous pouvez choisir le nom de la recommandation et choisir Afficher la note pour connaître la raison de la réouverture. Si l'équipe chargée de votre compte a rouvert la recommandation pour vous, son nom apparaît à côté de la note.

7. Suivez les étapes indiquées dans les détails de la recommandation.

Pour rouvrir une recommandation pour l'ensemble des comptes de votre organisation AWS

Le compte de gestion ou l'administrateur délégué de Trusted Advisor Priority peut rouvrir une recommandation pour l'ensemble de ses comptes.

> **Note**
>
> Les comptes membres n'ont pas accès aux recommandations agrégées.

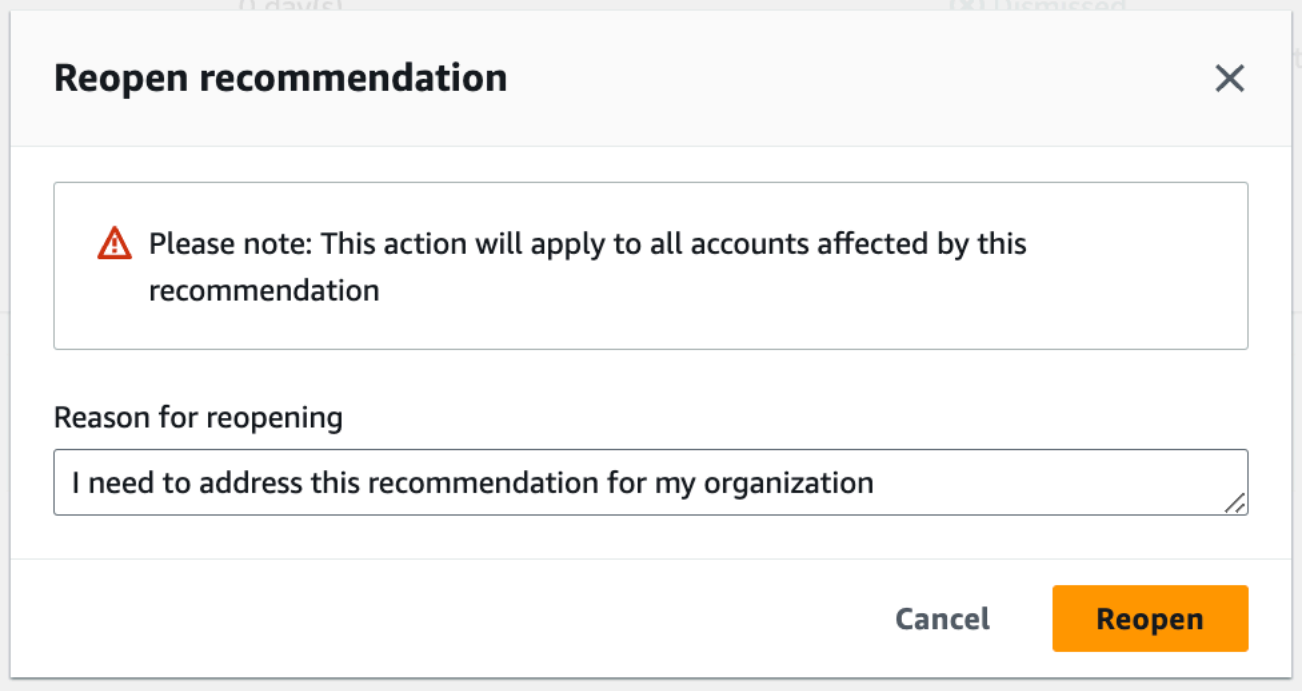
1. Accédez à la console Trusted Advisor à l'adresse https://console.aws.amazon.com/trustedadvisor/home.
2. Sur la page Trusted Advisor Priority, assurez-vous que vous êtes sur l'onglet Mon organisation.
3. Sous Closed recommendations (Recommandations fermées), sélectionnez la recommandation qui est Dismissed (Supprimée), puis cliquez sur Reopen (Rouvrir).
4. Dans la boîte de dialogue Rouvrir la recommandation, décrivez pourquoi vous rouvrez la recommandation.
5. Sélectionnez Reopen (Rouvrir). Le statut de la recommandation passe à In progress (En cours) et apparaît sous l'onglet Active (Actif).

> **Tip**
>
> Vous pouvez choisir le nom de la recommandation et choisir Afficher la note pour connaître la raison de la réouverture. Si l'équipe chargée de votre compte a rouvert la recommandation pour vous, son nom apparaît à côté de la note.

6. Suivez les étapes indiquées dans les détails de la recommandation.

Example : rouvrir une recommandation de Trusted Advisor Priority

L'exemple suivant montre une recommandation que vous voulez rouvrir.



Télécharger les détails des recommandations

Vous pouvez également télécharger les résultats d'une recommandation hiérarchisée depuis Trusted Advisor Priority.

> **Note**
>
> Actuellement, vous ne pouvez télécharger qu'une seule recommandation à la fois.

Téléchargement d'une recommandation

1. Accédez à la console Trusted Advisor sur https://console.aws.amazon.com/trustedadvisor/home.
2. Sur la page Trusted Advisor Priority, sélectionnez la recommandation, puis choisissez Download (Télécharger).
3. Ouvrez le fichier pour afficher les détails de la recommandation.

Enregistrer des administrateurs délégués

Vous pouvez ajouter des comptes membres qui font partie de votre organisation en tant qu'administrateurs délégués. Les comptes d'administrateurs délégués peuvent examiner, accepter, résoudre, rejeter et rouvrir des recommandations dans Trusted Advisor Priority.

Après avoir enregistré un compte, vous devez accorder à l'administrateur délégué les autorisations AWS Identity and Access Management requises pour accéder à Trusted Advisor Priority. Pour plus d'informations, consultez Gérez l'accès à AWS Trusted Advisor et AWS politiques gérées pour AWS Trusted Advisor.

Vous pouvez enregistrer jusqu'à cinq comptes membres. Seul le compte de gestion peut ajouter des administrateurs délégués pour l'organisation. Vous devez être connecté au compte de gestion de l'organisation pour enregistrer ou annuler l'enregistrement d'un administrateur délégué.

Pour enregistrer un administrateur délégué

1. Accédez à la console Trusted Advisor en vous connectant au compte de gestion à l'adresse https://console.aws.amazon.com/trustedadvisor/home.
2. Dans le panneau de navigation, sous Preferences (Préférences), choisissez Your organization (Votre organisation).

3. Sous Delegated administrator (Administrateur délégué), sélectionnez Register new account (Enregistrer un nouveau compte).
4. Dans la boîte de dialogue, saisissez l'ID de compte membre, puis cliquez sur Register (Enregistrer).
5. (Facultatif) Pour annuler l'enregistrement d'un compte, sélectionnez un compte et cliquez sur Deregister (Annuler l'enregistrement). Dans la boîte de dialogue, sélectionnez à nouveau Deregister (Annuler l'enregistrement).

Annulation de l'enregistrement des administrateurs délégués

Lorsque vous annulez l'enregistrement d'un compte membre, ce compte n'a plus le même accès à Trusted Advisor Priority que le compte de gestion. Les comptes qui ne sont plus des administrateurs délégués ne recevront pas de notifications par e-mail de Trusted Advisor Priority.

Pour annuler l'enregistrement d'un administrateur délégué

1. Accédez à la console Trusted Advisor en vous connectant au compte de gestion à l'adresse https://console.aws.amazon.com/trustedadvisor/home.
2. Dans le panneau de navigation, sous Preferences (Préférences), choisissez Your organization (Votre organisation).
3. Sous Administrateur délégué, sélectionnez un compte et choisissez Annuler l'enregistrement.
4. Dans la boîte de dialogue, sélectionnez Deregister (Annuler l'enregistrement).

Gestion des notifications de Trusted Advisor Priority

Trusted Advisor Priority envoie des notifications par e-mail. Cet e-mail de notification comprend un résumé des recommandations que votre équipe de compte a classées par ordre de priorité pour vous. Vous pouvez spécifier la fréquence à laquelle vous recevez les mises à jour de Trusted Advisor Priority.

Si vous avez enregistré des comptes de membres en tant qu'administrateurs délégués, ils peuvent également configurer leurs comptes pour recevoir des notifications par e-mail de Trusted Advisor Priority.

Les notifications par e-mail d'Trusted Advisor Priority ne comprennent pas les résultats des vérifications pour les comptes individuels et sont distinctes de la notification hebdomadaire d'Trusted

Advisor Recommendations. Pour en savoir plus, consultez Configuration des préférences de notification.

> **Note**
>
> Seuls le compte de gestion ou l'administrateur délégué peuvent configurer les notifications Trusted Advisor prioritaires par e-mail.

Pour gérer vos notifications de Trusted Advisor Priority

1. Accédez à la console Trusted Advisor en vous connectant à un compte de gestion ou à un compte d'administrateur délégué à l'adresse https://console.aws.amazon.com/trustedadvisor/home.
2. Dans le panneau de navigation, sous Preferences (Préférences), choisissez Notifications.
3. Sous Priority, vous pouvez sélectionner les options suivantes.
   a. Daily (Quotidien) : recevez une notification par e-mail tous les jours.
   b. Weekly (Hebdomadaire) : recevez une notification par e-mail une fois par semaine.
   c. Choisissez les notifications à recevoir :
      - Résumé des recommandations classées par ordre de priorité
      - Dates de résolution
4. Pour Destinataires, sélectionnez d'autres contacts auxquels les e-mails de notification doivent être envoyés. Vous pouvez ajouter et supprimer des contacts dans la page Account Settings (Paramètres de compte) dans la console AWS Billing and Cost Management.
5. Pour Language (Langue), choisissez la langue l'e-mail de notification.
6. Choisissez Save your preferences (Enregistrer vos préférences).

> **Note**
>
> Trusted Advisor Priority envoie des e-mails de notification à partir de l'adresse noreply@notifications.trustedadvisor.us-west-2.amazonaws.com. Vous devrez peut-être vérifier que votre client e-mail n'identifie pas ces e-mails comme des spams.

Désactiver Trusted Advisor Priority

Contactez votre équipe de compte et demandez-lui de désactiver cette fonction pour vous. Une fois cette fonctionnalité désactivée, les recommandations prioritaires ne s'affichent plus dans votre console Trusted Advisor.

Si vous désactivez Trusted Advisor Priority et que vous l'activez à nouveau ultérieurement, vous pouvez toujours visualiser les recommandations que votre équipe de compte a envoyées avant que vous ne désactiviez Trusted Advisor Priority.

Commencer avec AWS Trusted Advisor Engage (version préliminaire)

> **Note**
>
> AWS Trusted Advisor Engage est actuellement disponible en version préliminaire et susceptible d'être modifié. Vous pouvez consulter les conditions de service de la version préliminaire à l'adresse https://aws.amazon.com/service-terms/.

Tirez le meilleur parti de vos plans AWS Support en utilisant AWS Trusted Advisor Engage pour consulter, demander et suivre facilement tous vos engagements actifs, et pour communiquer avec votre équipe Compte AWS au sujet des engagements en cours.

Par exemple, vous pouvez demander un « suivi des activités de gestion » à votre équipe Compte AWS en accédant à la page Engage de la console AWS Trusted Advisor. Un expert AWS sera alors affecté à votre demande et suivra l'intégralité de l'engagement.

Rubriques

- Modification de l'état d'un engagement
- Distinction entre les engagements recommandés et les engagements demandés
- Recherche d'engagements

Prérequis

Vous devez prendre les mesures nécessaires pour satisfaire aux exigences suivantes afin d'utiliser Trusted Advisor Engage :

- Vous devez disposer d'un plan de support Enterprise On-Ramp.
- Votre compte doit faire partie d'une organisation ayant activé toutes les fonctionnalités dans AWS Organizations. Pour de plus amples informations, consultez Activation de toutes les fonctionnalités de l'organisation dans le Guide de l'utilisateur AWS Organizations.
- Votre organisation doit avoir activé l'accès sécurisé à Trusted Advisor. Vous pouvez activer l'accès sécurisé en vous connectant en tant que compte de gestion et en accédant à la page Votre organisation dans la Trusted Advisor console.
- Vous devez disposer d'autorisations AWS Identity and Access Management (IAM) pour accéder à Trusted Advisor Engage. Pour plus d'informations sur la manière de contrôler l'accès à Trusted Advisor Engage, voir Gérez l'accès à AWS Trusted Advisor.

> **Note**
>
> N'importe quel compte au sein d'une organisation AWS peut créer une demande d'engagement. Si un compte titulaire d'un engagement est transféré vers une autre organisation AWS, l'engagement ne sera accessible qu'au compte en question. Pour limiter les contrôles, voir Exemples de politiques de contrôle des services pour AWS Trusted Advisor.

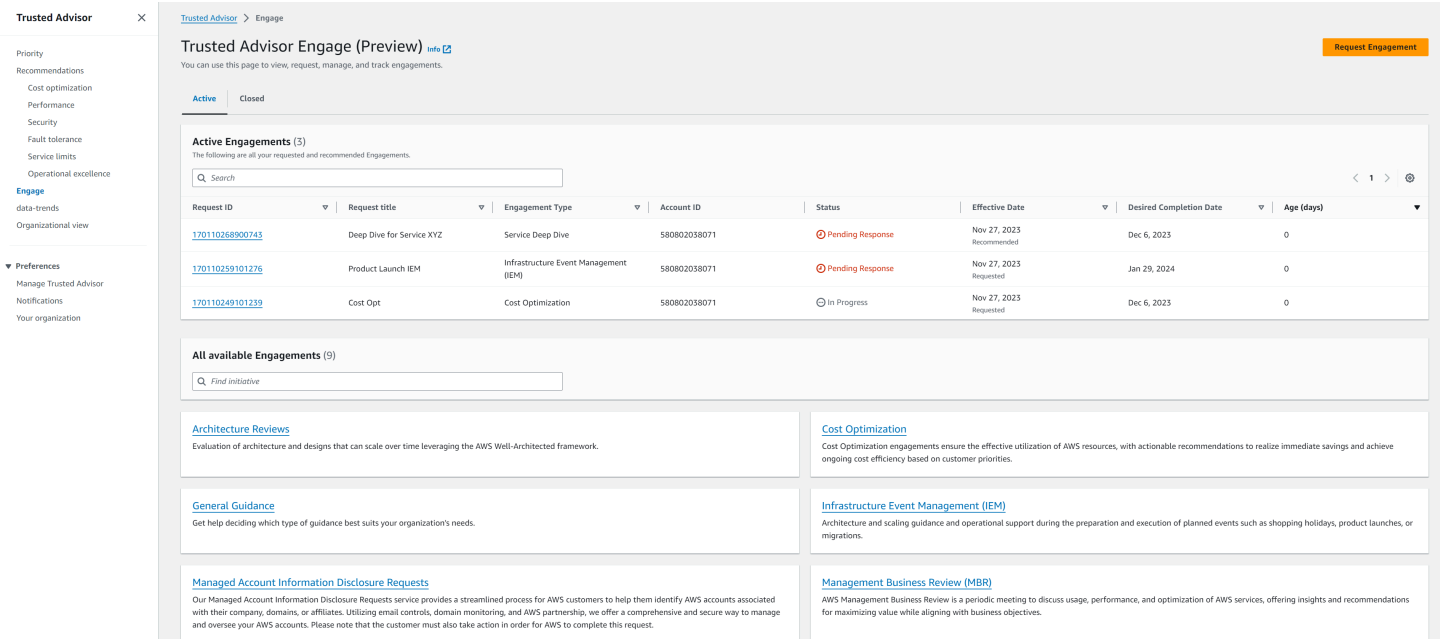
Affichage du tableau de bord des engagements

Une fois que vous avez obtenu les droits d'accès, vous pouvez accéder à la page Trusted Advisor Engage de la console Trusted Advisor pour afficher un tableau de bord à partir duquel vous pouvez gérer les engagements avec votre équipe Compte AWS.

Pour gérer vos engagements :

1. Accédez à la console Trusted Advisor à l'adresse https://console.aws.amazon.com/trustedadvisor/home.
2. La page Trusted Advisor Engage comprend les éléments suivants :
   - Bouton Demandez un engagement
   - Tableau des engagements actifs
   - Tableau des engagements clôturés
   - Catalogue de tous les engagements disponibles

Example : tableau de bord des engagements



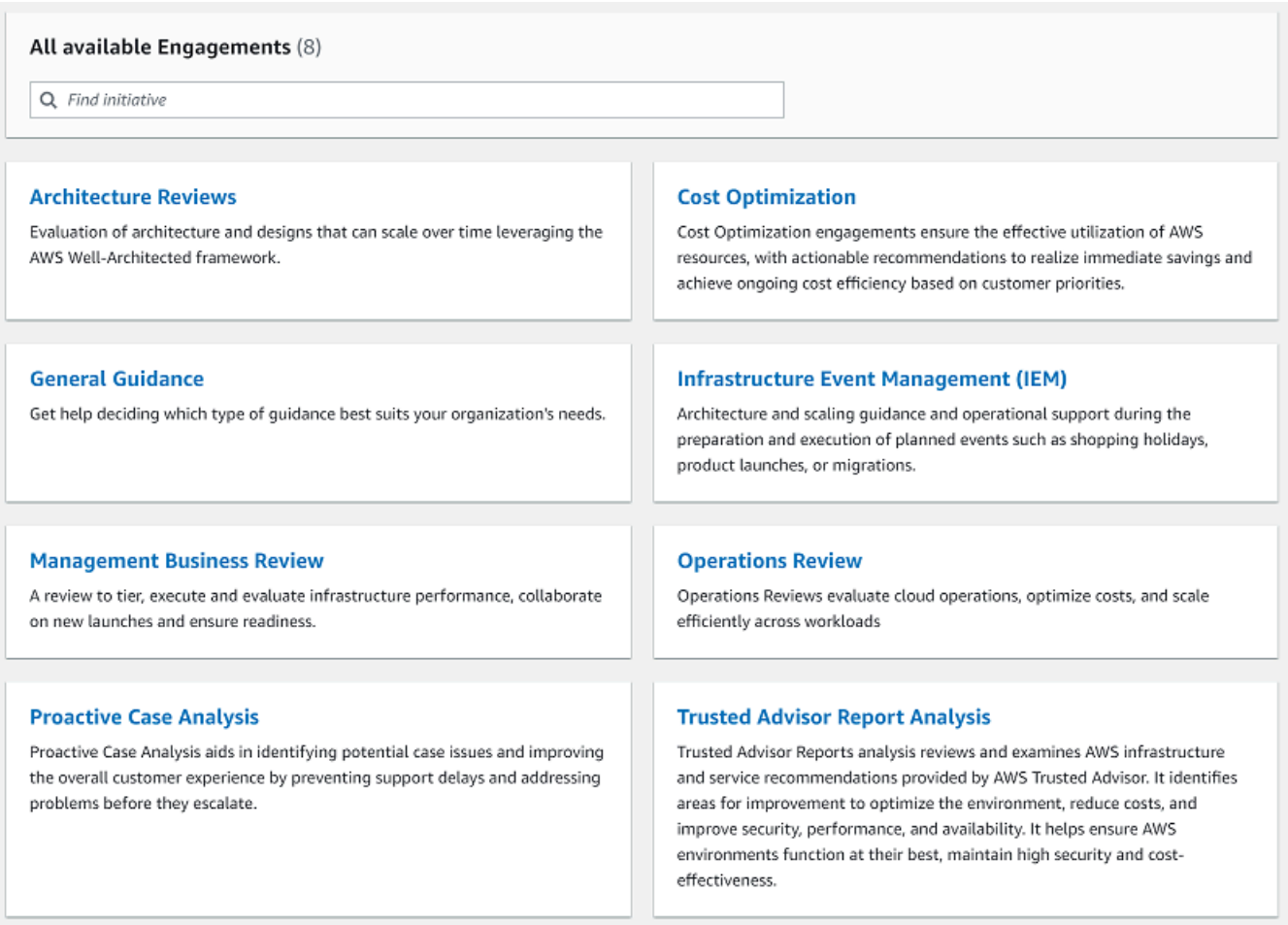
Affichage du catalogue des types d'engagements

Vous pouvez afficher le catalogue des types d'engagements pour trouver les derniers types d'engagements que vous pouvez demander à votre équipe Compte AWS.

Pour afficher le catalogue des types d'engagements :

1. Accédez à la console Trusted Advisor à l'adresse https://console.aws.amazon.com/trustedadvisor/home.
2. Le catalogue des types d'engagements est accessible depuis la page Trusted Advisor Engage.

Example : catalogue des types d'engagements



Demande d'engagement

Vous pouvez demander des engagements à votre équipe Compte AWS en fonction des types d'engagements inclus dans votre plan de support AWS.

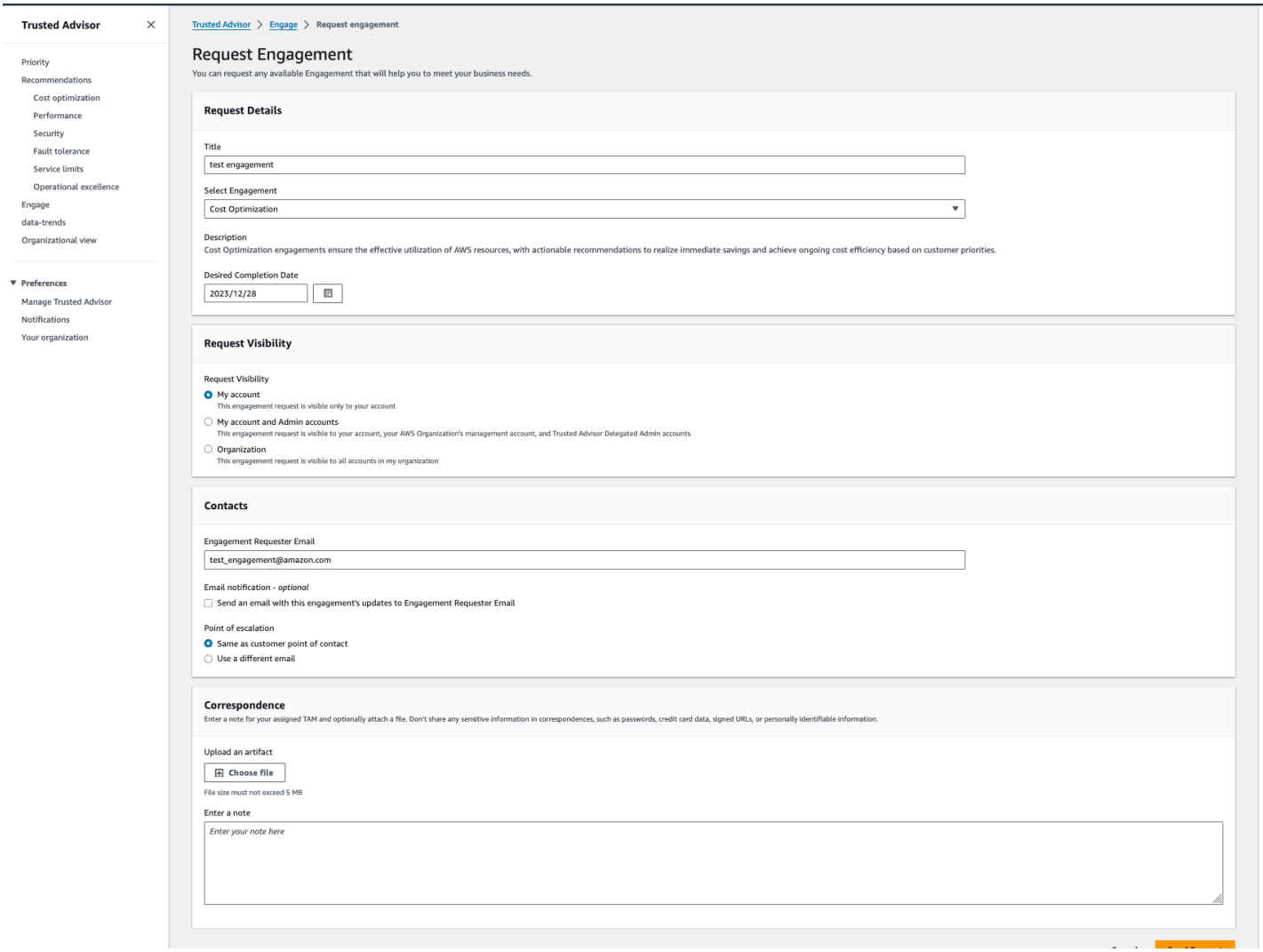
Pour demander un engagement :

1. Accédez à la console Trusted Advisor à l'adresse https://console.aws.amazon.com/trustedadvisor/home.
2. Sur la page Trusted Advisor Engage, choisissez Demandez un engagement.
3. Renseignez les champs suivants :
   - Titre
   - Sélectionner un engagement : type d'engagement que vous souhaitez demander.

- Date d'achèvement souhaitée : date de fin souhaitée de l'engagement. Le délai varie selon le type d'engagement et est calculé en fonction de la date d'achèvement minimale souhaitée.
- Visibilité des demandes :
  - Mon compte : cette demande d'engagement n'est visible que pour votre compte.
  - Mon compte et comptes d'administrateurs : cette demande d'engagement est visible pour votre compte, ainsi que pour le compte de gestion et pour tous les comptes d'administrateur délégué de votre organisation AWS.
  - Organisation : cette demande d'engagement est visible pour tous les comptes de votre organisation AWS.
- Adresse e-mail du demandeur d'engagement : adresse e-mail qui AWS sera utilisée comme point de contact principal pour cet engagement.
- Paramètres de notification par e-mail : choisissez si l'e-mail du demandeur d'engagement recevra des notifications par e-mail concernant l'engagement.
- Point d'escalade : adresse e-mail qui sera utilisée par AWS lorsqu'une escalade est requise pour cet engagement.
- Correspondance : remarque et pièce jointe facultative qui vous permettent de fournir plus d'informations sur cet engagement.

4. Choisissez Envoyer une demande.

Example : demande d'engagement



Modification d'un engagement

Vous pouvez modifier les détails de votre demande d'engagement.

Pour modifier un engagement :

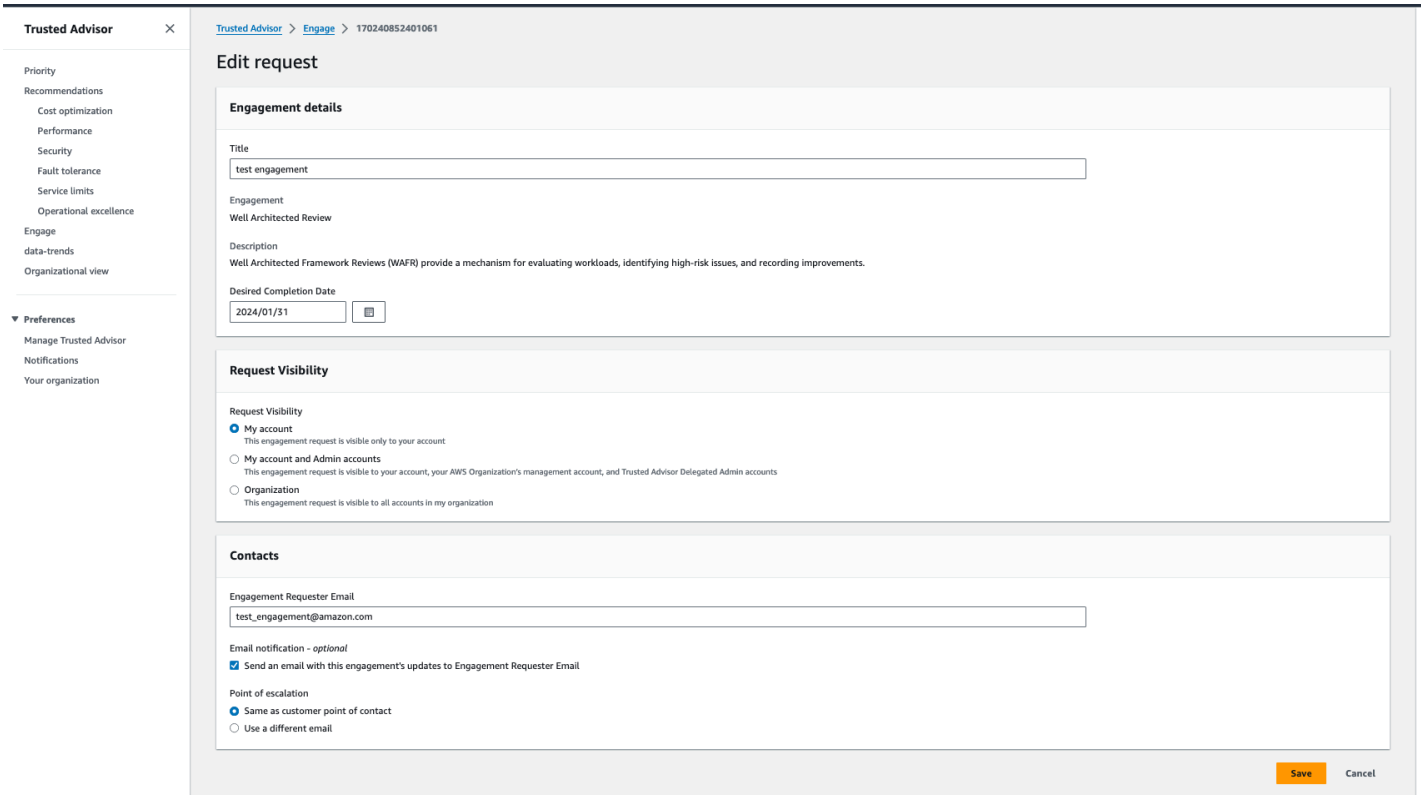
1. Accédez à la console Trusted Advisor à l'adresse https://console.aws.amazon.com/trustedadvisor/home.
2. Sur la page Trusted Advisor Engage, sélectionnez un engagement existant.
3. Tâche de sélection Modifier.
4. Vous pouvez modifier les informations suivantes :

    - Titre

- Date d'achèvement souhaitée : date de fin souhaitée de l'engagement. Le délai varie selon le type d'engagement et est calculé en fonction de la date d'achèvement minimale souhaitée.
- Visibilité des demandes :
  - Mon compte : cette demande d'engagement n'est visible que pour votre compte.
  - Mon compte et comptes d'administrateurs : cette demande d'engagement est visible pour votre compte, ainsi que pour le compte de gestion et pour tous les comptes d'administrateur délégué de votre organisation AWS.
  - Organisation : cette demande d'engagement est visible pour tous les comptes de votre organisation AWS.
- Adresse e-mail du demandeur d'engagement : adresse e-mail qui AWS sera utilisée comme point de contact principal pour cet engagement.
- Paramètres de notification par e-mail : choisissez si l'e-mail du demandeur d'engagement recevra des notifications par e-mail concernant l'engagement.
- Point d'escalade : adresse e-mail qui sera utilisée par AWS lorsqu'une escalade est requise pour cet engagement.

5. Choisissez Enregistrer.

Example : modification d'un engagement



Envoi de pièces jointes et de remarques

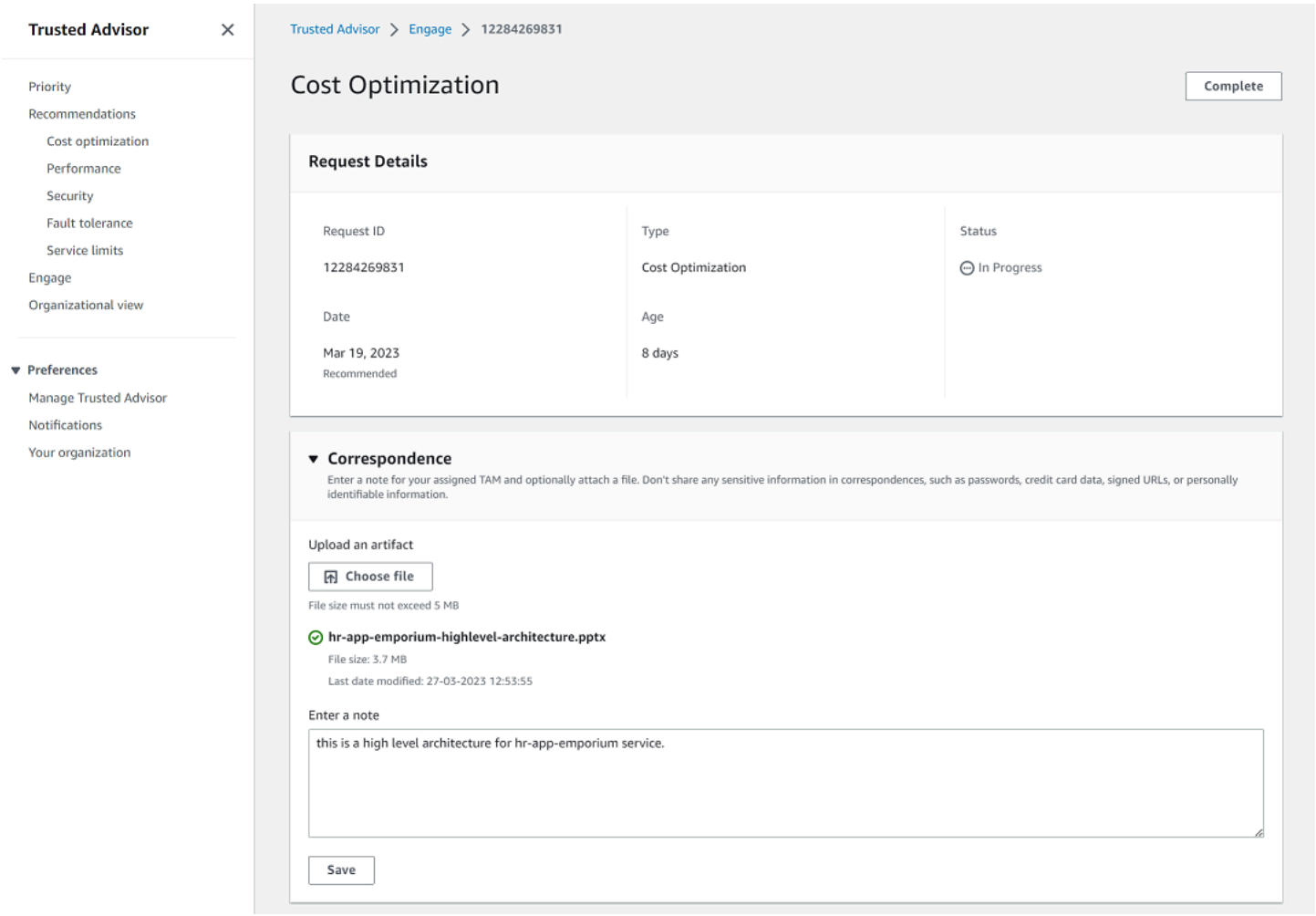
Communiquez avec votre équipe Compte AWS au sujet d'engagements spécifiques en envoyant des remarques et des pièces jointes pour appuyer votre demande d'engagement. Vous pouvez inclure une seule pièce jointe et une seule remarque par communication. Vous ne pouvez joindre des fichiers à un engagement qu'avec le Compte AWS utilisé pour la demande d'engagement, et vous ne pouvez pas supprimer de pièces jointes ou de remarques après l'envoi d'une communication.

Pour joindre des fichiers ou ajouter des remarques à une demande d'engagement actif :

1. Accédez à la console Trusted Advisor à l'adresse https://console.aws.amazon.com/trustedadvisor/home.
2. Sur la page Trusted Advisor Engage, choisissez l'ID de l'engagement actif auquel vous souhaitez joindre des fichiers ou ajouter des remarques.
3. Choisissez Correspondance pour développer le formulaire.
4. Entrez une remarque pour le TAM qui vous a été attribué et joignez éventuellement un fichier. Ne partagez aucune information sensible dans les correspondances, telles que des mots de passe, des données de carte de crédit, des URL signées ou des informations personnelles identifiables.

5. Choisissez Enregistrer.

Example : ajout d'une remarque et d'un fichier à un engagement



Modification de l'état d'un engagement

Vous pouvez modifier l'état des engagements pour annuler les engagements en attente de réponse, terminer les engagements en cours et rouvrir les engagements marqués comme annulés ou clôturés.

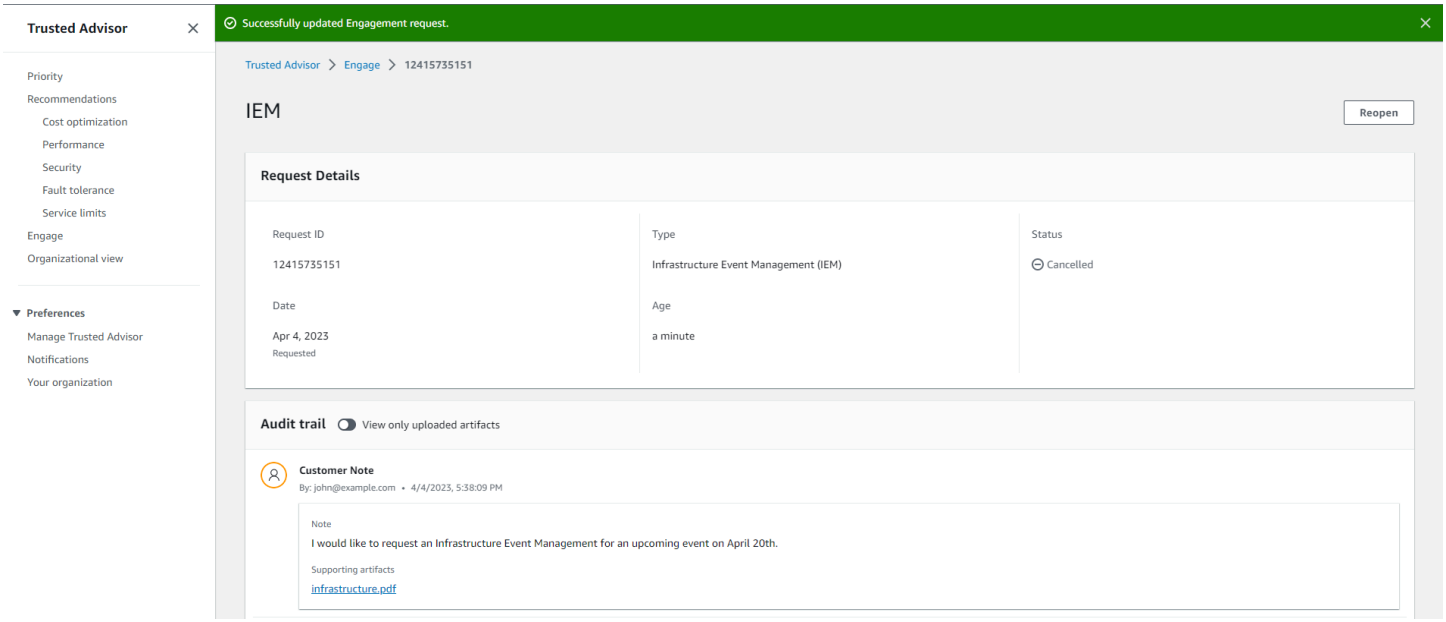
Pour modifier l'état d'un engagement :

1. Accédez à la console Trusted Advisor à l'adresse https://console.aws.amazon.com/trustedadvisor/home.
2. Sur la page Trusted Advisor Engage, choisissez l'ID de l'engagement actif dont vous souhaitez modifier l'état.

3. Sur la page des détails de l'engagement, vous pouvez modifier l'état en Annulé ou Terminé.

   - Vous pouvez sélectionner Annuler lorsque l'état de l'engagement est Réponse en attente.
   - Vous pouvez sélectionner Terminé lorsque l'état de l'engagement est En cours.
   - Vous pouvez sélectionner Rouvrir pour les engagements clôturés. L'état des engagements annulés passe à Réponse en attente, tandis que celui des engagements terminés passe à En cours.

Example : modification de l'état d'un engagement



Distinction entre les engagements recommandés et les engagements demandés

Vous pouvez identifier la source des engagements pour savoir si un engagement a été demandé par vous ou recommandé par votre équipe Compte AWS.

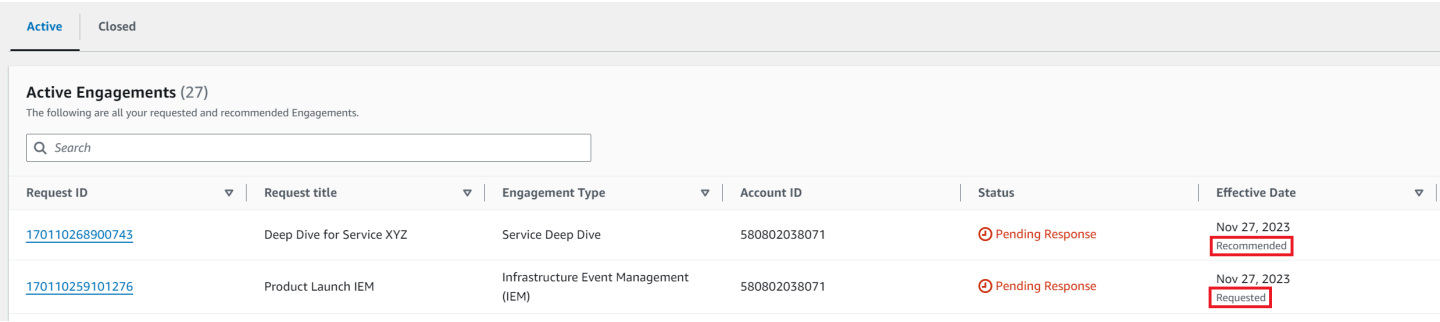
Pour afficher les différentes sources des engagements actifs :

1. Accédez à la console Trusted Advisor à l'adresse https://console.aws.amazon.com/trustedadvisor/home.
2. Sur la page Trusted AdvisorEngage, consultez la colonne Date d'entrée en vigueur pour faire la distinction entre les engagements recommandés et demandés :

   - Recommandé : demande d'engagement créée par vos équipes Compte AWS.

- Demandé : demande d'engagement créée par l'utilisateur.

Example : distinction entre les engagements recommandés et les engagements demandés



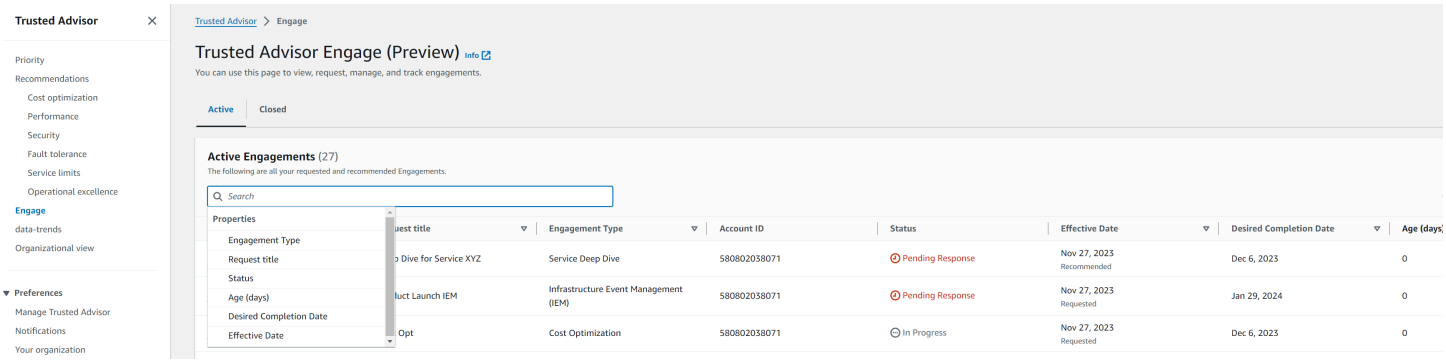
Recherche d'engagements

Vous pouvez rechercher vos engagements actifs et clôturés à l'aide de filtres.

Pour rechercher des engagements :

1. Accédez à la console Trusted Advisor à l'adresse https://console.aws.amazon.com/trustedadvisor/home.
2. Sur la page Trusted Advisor Engage, vous pouvez sélectionner l'un des filtres suivants :
   - Âge (jours)
   - Type d'engagement
   - Titre de la demande
   - Statut
   - Date d'achèvement souhaitée
   - Date d'effet

Example : recherche d'engagements



Référence de la vérification AWS Trusted Advisor

Vous pouvez afficher tous les noms de vérification Trusted Advisor, les descriptions et les ID dans la référence suivante. Vous pouvez également vous connecter à la console Trusted Advisor pour afficher plus d'informations sur les vérifications, les actions recommandées et leurs statuts.

Si vous possédez un plan de support Business, Enterprise On-Ramp ou Enterprise, vous pouvez utiliser l'API AWS Trusted Advisor et AWS Command Line Interface (AWS CLI) pour accéder à vos vérifications. Pour plus d'informations, consultez les rubriques suivantes :

- Commencez avec l'Trusted AdvisorAPI
- Référence API AWS Trusted Advisor

> **Note**
>
> Si vous possédez un plan de support de base et de support aux développeurs, vous pouvez utiliser la console Trusted Advisor pour accéder à toutes les vérifications dans la catégorie Service Limits et les vérifications suivantes dans la catégorie de sécurité :
>
> - Instantanés publics Amazon EBS
> - Instantanés publics Amazon RDS
> - Autorisations pour le compartiment Amazon S3
> - Utilisation d'IAM
> - MFA sur le compte racine
> - Groupes de sécurité — Ports spécifiques non restreints

Catégories de vérification

- Optimisation des coûts
- Performance
- Sécurité
- Tolérance aux pannes
- Service Limits
- Excellence opérationnelle

Optimisation des coûts

Vous pouvez utiliser les vérifications suivantes pour la catégorie d'optimisation des coûts.

Noms des vérifications

- Le compte AWS ne fait pas partie d'AWS Organizations
- Points de terminaison sous-utilisés d'Amazon Comprehend
- Volumes Amazon EBS surprovisionnés
- Consolidation des instances Amazon EC2 pour Microsoft SQL Server
- Instances Amazon EC2 trop approvisionnées pour Microsoft SQL Server
- Instances Amazon EC2 arrêtées
- Amazon EC2 Reserved Instance Lease Expiration
- Optimisation des instances réservées Amazon EC2
- Référentiel Amazon ECR sans politique de cycle de vie configurée
- Optimisation des nœuds ElastiCache réservés Amazon
- Optimisation des instances réservées Amazon OpenSearch Service
- Instances de base de données Amazon RDS inactives
- Optimisation des nœuds réservés Amazon Redshift
- Optimisation des instances réservées Amazon Relational Database Service (RDS)
- Jeux d'enregistrements de ressource de latence Amazon Route 53.
- Politique de cycle de vie de compartiment Amazon S3 configurée
- Configuration incomplète de l'interruption du téléchargement en plusieurs parties sur Amazon S3

- Compartiments Amazon S3 compatibles avec la gestion des versions, sans politiques de cycle de vie configurées
- Fonctions AWS Lambda avec des délais excessifs
- Fonctions AWS Lambda avec taux élevé d'erreurs
- Fonctions AWS Lambda surprovisionnées pour la taille de la mémoire
- Problèmes à risque élevé AWS Well-Architected pour l'optimisation des coûts
- Équilibreurs de charge inactifs
- Instances Amazon EC2 sous-exploitées
- Savings Plan
- Adresses IP Elastic non associées
- Volumes Amazon EBS sous-utilisés
- Underutilized Amazon Redshift Clusters

Le compte AWS ne fait pas partie d'AWS Organizations

Description

Vérifie si un compte AWS fait partie de AWS Organizations sous le compte de gestion approprié.

AWS Organizations est un service de gestion de comptes permettant de consolider plusieurs comptes AWS au sein d'une organisation gérée de manière centralisée. Cela vous permet de structurer les comptes de manière centralisée pour la consolidation de la facturation et de mettre en œuvre des politiques de propriété et de sécurité à mesure que vos charges de travail augmentent sur AWS.

Vous pouvez spécifier l'identifiant du compte de gestion à l'aide du MasterAccountIdparamètre des AWS Config règles.

Pour en savoir plus, voir Qu'est-ce qu'AWS Organizations ?

> **Note**
>
> Les résultats de cette vérification sont automatiquement actualisés plusieurs fois par jour et les demandes d'actualisation ne sont pas autorisées. Plusieurs heures peuvent encore être nécessaires pour que les modifications apparaissent. Actuellement, vous ne pouvez pas exclure des ressources de cette vérification.

ID de la vérification

`c18d2gz127`

Source

`AWS Config Managed Rule: account-part-of-organizations`

Critères d'alerte

Jaune : ce compte AWS ne fait pas partie de AWS Organizations.

Action recommandée

Ajoutez ce compte AWS à AWS Organizations.

Pour plus d'informations, voir Didacticiel : Création et configuration d'une organisation.

Colonnes du rapport

- Statut
- Région
- Ressource
- Règle AWS Config
- Paramètres d'entrée
- Heure de la dernière modification

Points de terminaison sous-utilisés d'Amazon Comprehend

Description

Vérifie la configuration du débit de vos points de terminaison. Cette vérification vous avertit lorsque les points de terminaison ne sont pas activement utilisés pour les demandes d'inférence en temps réel. Un point de terminaison qui n'est pas utilisé pendant plus de 15 jours consécutifs est considéré comme sous-utilisé. Tous les points de terminaison accumulent des frais basés à la fois sur le débit fixé et sur la durée d'activité du point de terminaison.

> **Note**
>
> Cette vérification est automatiquement actualisée une fois par jour. Actuellement, vous ne pouvez pas exclure des ressources de cette vérification.

ID de la vérification

`Cm24dfsM12`

Critères d'alerte

Jaune : le point de terminaison est actif, mais n'a pas été utilisé pour les demandes d'inférence en temps réel au cours des 15 derniers jours.

Action recommandée

Si le point de terminaison n'a pas été utilisé au cours des 15 derniers jours, nous vous recommandons de définir une politique de mise à l'échelle pour la ressource en utilisant Application Autoscaling.

Si une politique de mise à l'échelle est définie pour le point de terminaison et que ce dernier n'a pas été utilisé au cours des 30 derniers jours, envisagez de le supprimer et d'utiliser l'inférence asynchrone. Pour de plus amples informations, veuillez consulter Suppression d'un point de terminaison avec Amazon Comprehend.

Colonnes du rapport

- Statut
- Région
- ARN du point de terminaison
- Unité d'inférence provisionnée
- AutoScaling État
- Raison
- Heure de la dernière modification

Volumes Amazon EBS surprovisionnés

Description

Vérifie les volumes Amazon Elastic Block Store (Amazon EBS) qui étaient en cours d'exécution à tout moment pendant la période de recherche. Cette vérification vous avertit si des volumes EBS ont été surprovisionnés pour vos charges de travail. Lorsque vous avez des volumes surprovisionnés, vous payez pour les ressources inutilisées. Bien que certains scénarios puissent entraîner une faible optimisation par conception, vous pouvez souvent réduire vos coûts en

modifiant la configuration de vos volumes EBS. Les économies mensuelles estimées sont calculées en utilisant le taux d'utilisation actuel des volumes EBS. Les économies réelles varient si le volume n'est pas présent pendant un mois complet.

> **Note**
>
> Les résultats de cette vérification sont automatiquement actualisés plusieurs fois par jour et les demandes d'actualisation ne sont pas autorisées. Plusieurs heures peuvent encore être nécessaires pour que les modifications apparaissent. Actuellement, vous ne pouvez pas exclure des ressources de cette vérification.

ID de la vérification

`C0r6dfpM03`

Critères d'alerte

Jaune : volume EBS surprovisionné pendant la période de recherche. Pour déterminer si un volume est surprovisionné, nous prenons en compte toutes les CloudWatch mesures par défaut (y compris les IOPS et le débit). L'algorithme utilisé pour identifier les volumes EBS surprovisionnés suit les bonnes pratiques AWS. L'algorithme est mis à jour lorsqu'un nouveau modèle a été identifié.

Action recommandée

Envisagez de diminuer la taille des volumes peu utilisés.

Pour plus d’informations, consultez Inscription à AWS Compute Optimizer pour les vérifications de Trusted Advisor.

Colonnes du rapport

- Statut
- Région
- ID du volume
- Type de volume
- Taille du volume (Go)
- IOPS de référence du volume
- IOPS de rafale du volume

- Débit de rafale du volume
- Type de volume recommandé
- Taille de volume recommandée (Go)
- IOPS de référence de volume recommandées
- IOPS de rafale de volume recommandées
- Débit de référence de volume recommandé
- Débit de rafale de volume recommandé
- Période de recherche (jours)
- Opportunité d'économies (%)
- Économies mensuelles estimées
- Devise des économies mensuelles estimées
- Heure de la dernière modification

Consolidation des instances Amazon EC2 pour Microsoft SQL Server

Description

Vérifie vos instances Amazon Elastic Compute Cloud (Amazon EC2) qui exécutent SQL Server au cours des dernières 24 heures. Cette vérification vous avertit si l'instance dispose d'une valeur inférieure au nombre minimal de licences SQL Server. Dans le Guide des licences Microsoft SQL Server, vous payez 4 licences de vCPU même si une instance ne possède que 1 ou 2 vCPU. Vous pouvez consolider des instances SQL Server plus petites afin de réduire les coûts.

> **Note**
>
> Les résultats de cette vérification sont automatiquement actualisés plusieurs fois par jour et les demandes d'actualisation ne sont pas autorisées. Plusieurs heures peuvent encore être nécessaires pour que les modifications apparaissent. Actuellement, vous ne pouvez pas exclure des ressources de cette vérification.

ID de la vérification

`Qsdfp3A4L2`

Critères d'alerte

Jaune : une instance avec SQL Server possède moins de 4 vCPU.

Action recommandée

Envisagez de consolider les charges de travail SQL Server plus petites dans des instances dotées d'au moins 4 vCPU.

Ressources supplémentaires

- Microsoft SQL Server sur AWS
- Licences Microsoft sur AWS
- Guide des licences Microsoft SQL Server

Colonnes du rapport

- Statut
- Région
- ID d’instance
- Type d'instance
- vCPU
- vCPU minimum
- Edition SQL Server
- Heure de la dernière modification

Instances Amazon EC2 trop approvisionnées pour Microsoft SQL Server

Description

Vérifie vos instances Amazon Elastic Compute Cloud (Amazon EC2) qui exécutent SQL Server au cours des dernières 24 heures. La capacité de calcul d'une base de données SQL Server est limitée pour chaque instance. Une instance avec SQL Server Standard Edition peut utiliser jusqu'à 48 vCPU. Une instance avec SQL Server Web peut utiliser jusqu'à 32 vCPU. Cette vérification vous avertit si une instance dépasse cette limite de vCPU.

Si votre instance est trop approvisionnée, vous payez le prix total sans améliorer la performance. Afin de réduire les coûts, vous pouvez gérer le nombre et la taille de vos instances.

Les économies mensuelles estimées sont calculées en utilisant la même famille d'instance avec le nombre maximal de vCPU qu'une instance SQL Server peut utiliser et la tarification à la demande. Les économies réelles varient si vous utilisez des instances réservées (RI, Reserved Instances), ou si l'instance ne s'exécute pas pendant une journée complète.

> **Note**
>
> Les résultats de cette vérification sont automatiquement actualisés plusieurs fois par jour et les demandes d'actualisation ne sont pas autorisées. Plusieurs heures peuvent encore être nécessaires pour que les modifications apparaissent. Actuellement, vous ne pouvez pas exclure des ressources de cette vérification.

ID de la vérification

`Qsdfp3A4L1`

Critères d'alerte

- Rouge : une instance avec SQL Server Standard Edition possède plus de 48 vCPU.
- Rouge : une instance avec SQL Server Web Edition possède plus de 32 vCPU.

Action recommandée

Pour SQL Server Standard Edition, envisagez de passer à une instance de la même famille d'instances avec 48 vCPU. Pour SQL Server Web Edition, envisagez de passer à une instance de la même famille d'instances avec 32 vCPU. Si elle consomme beaucoup de mémoire, envisagez de passer à des instances R5 optimisées pour la mémoire. Pour de plus amples informations, veuillez consulter Bonnes pratiques relatives au déploiement de Microsoft SQL Server sur Amazon EC2.

Ressources supplémentaires

- Microsoft SQL Server sur AWS
- Vous pouvez utiliser Launch Wizard pour simplifier le déploiement de SQL Server sur EC2.

Colonnes du rapport

- Statut
- Région
- ID d’instance
- Type d'instance

- vCPU
- Edition SQL Server
- vCPU maximum
- Type d'instance recommandé
- Économies mensuelles estimées
- Heure de la dernière modification

Instances Amazon EC2 arrêtées

Description

Vérifie si certaines instances Amazon EC2 ont été arrêtées pendant plus de 30 jours.

Vous pouvez spécifier la valeur du nombre de jours autorisés dans les AWS Config paramètres AllowedDaysof.

Pour plus d'informations, voir Pourquoi suis-je facturé pour Amazon EC2 alors que toutes mes instances ont été terminées ?.

> **Note**
>
> Les résultats de cette vérification sont automatiquement actualisés plusieurs fois par jour et les demandes d'actualisation ne sont pas autorisées. Plusieurs heures peuvent encore être nécessaires pour que les modifications apparaissent. Actuellement, vous ne pouvez pas exclure des ressources de cette vérification.

ID de la vérification

`c18d2gz150`

Source

`AWS Config Managed Rule: ec2-stopped-instance`

Critères d'alerte

- Jaune : vérifie si certaines instances Amazon EC2 ont été arrêtées plus longtemps que le nombre de jours autorisé.

Action recommandée

Passez en revue les instances Amazon EC2 qui ont été arrêtées pendant au moins 30 jours. Pour éviter des coûts inutiles, terminez toutes les instances dont vous n'avez plus besoin.

Pour plus d'informations, voir Terminaison de votre instance.

Ressources supplémentaires

- Tarification d'Amazon EC2 à la demande

Colonnes du rapport

- Statut
- Région
- Ressource
- Règle AWS Config
- Paramètres d'entrée
- Heure de la dernière modification

Amazon EC2 Reserved Instance Lease Expiration

Description

Recherche les instances réservées Amazon EC2 dont l'expiration est prévue dans les 30 prochains jours, ou ont expiré au cours des 30 derniers jours.

Les instances réservées ne sont pas renouvelées automatiquement. Vous pouvez continuer à utiliser une instance Amazon EC2 couverte par la réservation sans interruption, mais elle sera facturée aux tarifs à la demande. Les nouvelles instances réservées peuvent avoir les mêmes paramètres que les instances expirées, ou vous pouvez acheter des instances réservées avec des paramètres différents.

Les économies mensuelles estimées correspondent à la différence entre les tarifs des instances à la demande et ceux des instances réservées pour le même type d'instance.

ID de la vérification

```
1e93e4c0b5
```

Critères d'alerte

- Jaune : le bail de l'instance réservée expire dans moins de 30 jours.

- Jaune : le bail de l'instance réservée a expiré au cours des 30 derniers jours.

Action recommandée

Envisagez d'acheter une nouvelle instance réservée pour remplacer celle dont la fin de durée de vie approche. Pour de plus amples informations, veuillez consulter Comment acheter des instances réservées et Acheter des instances réservées.

Ressources supplémentaires

- Instances réservées
- Types d'instances

Colonnes du rapport

- Statut
- disponibilité
- Type d'instance
- Plateforme
- Nombre d'instances
- Coût mensuel actuel
- Économies mensuelles estimées
- Date d'expiration
- ID Instance réservée
- Raison

Optimisation des instances réservées Amazon EC2

Description

Une grande partie de l'utilisation d'AWS implique de trouver l'équilibre entre vos achats d'instances réservées (RI) et votre utilisation d'instances à la demande. Cette vérification fournit des recommandations sur les instances réservées qui permettent de diminuer les coûts relatifs à l'utilisation d'instances à la demande.

Nous créons ces recommandations en analysant votre utilisation à la demande au cours des 30 derniers jours. Nous classons ensuite l'utilisation en catégories éligibles pour les réservations. Nous simulons chaque combinaison de réservations dans la catégorie d'utilisation générée pour identifier le nombre recommandé de chaque type d'instance réservée à acheter. Ce processus de simulation et d'optimisation nous permet de réaliser le plus d'économies sur les coûts. Cette

vérification couvre les recommandations basées sur les instances réservées standard avec l'option de paiement initial partiel.

Cette vérification n'est pas disponible pour les comptes liés à la facturation consolidée. Les recommandations pour cette vérification ne sont disponibles que pour le compte de règlement.

ID de la vérification

`cX3c2R1chu`

Critères d'alerte

Jaune : l'optimisation de l'utilisation des instances réservées initiales partielles peut contribuer à réduire les coûts.

Action recommandée

Consultez la page de l'Explorateur de coûts pour des recommandations plus détaillées et personnalisées. Consultez également le guide d'achat pour comprendre comment acheter des instances réservées et connaître les options disponibles.

Ressources supplémentaires

- Vous trouverez des informations sur les instances réservées et sur la façon dont elles peuvent vous faire économiser de l'argent ici.
- Pour plus d'informations sur cette recommandation, consultez Vérification de l'optimisation des instances réservées dans la FAQ Trusted Advisor.

Colonnes du rapport

- Région
- Type d'instance
- Plateforme
- Nombre recommandé d'instances réservées à acheter
- Utilisation moyenne attendue des instances réservées
- Économies estimées avec les recommandations (mensuelles)
- Coût initial des instances réservées
- Coûts estimés des instances réservés (mensuels)
- Coût à la demande estimé après l'achat recommandé de l'instance réservée (mensuel)
- Rentabilité estimée (mois)
- Période de recherche (jours)

- Durée (années)

Référentiel Amazon ECR sans politique de cycle de vie configurée

Description

Vérifie si au moins une politique de cycle de vie est configurée dans un référentiel privé Amazon ECR. Les politiques de cycle de vie vous permettent de définir un ensemble de règles pour nettoyer automatiquement les images de conteneur anciennes ou inutilisées. Cela vous permet de contrôler la gestion du cycle de vie des images, de mieux organiser les référentiels Amazon ECR et de réduire les coûts de stockage globaux.

Pour plus d'informations, voir Politiques de cycle de vie.

ID de la vérification

```
c18d2gz128
```

Source

```
AWS Config Managed Rule: ecr-private-lifecycle-policy-configured
```

Critères d'alerte

Jaune : aucune politique de cycle de vie n'est configurée pour un référentiel privé Amazon ECR.

Action recommandée

Créez au moins une politique de cycle de vie pour votre référentiel privé Amazon ECR.

Pour plus d'informations, voir Création d'une politique de cycle de vie.

Ressources supplémentaires

- Politiques de cycle de vie
- Création d'une politique de cycle de vie
- Exemples de politiques de cycle de vie

Colonnes du rapport

- Statut
- Région
- Ressource
- Règle AWS Config
- Paramètres d'entrée

- Heure de la dernière modification

Optimisation des nœuds ElastiCache réservés Amazon

Description

Vérifie votre utilisation des nœuds réservés ElastiCache et fournit des recommandations pour leur achat. Ces recommandations visent à réduire les coûts liés à l'utilisation de ElastiCache On-Demand. Nous créons ces recommandations en analysant votre utilisation à la demande au cours des 30 derniers jours.

Nous utilisons cette analyse pour simuler chaque combinaison de réservations dans la catégorie d'utilisation générée. Cela nous permet de recommander le nombre de chaque type de nœud réservé à acheter pour réaliser le plus d'économies. Cette vérification couvre les recommandations basées sur l'option de paiement initial partiel avec un engagement d'un an ou de trois ans.

Cette vérification n'est pas disponible pour les comptes liés à la facturation consolidée. Les recommandations pour cette vérification ne sont disponibles que pour le compte de règlement.

ID de la vérification

`h3L1otH3re`

Critères d'alerte

Jaune : l'optimisation de l'achat de nœuds ElastiCache réservés peut contribuer à réduire les coûts.

Action recommandée

Consultez la page Cost Explorer pour obtenir des recommandations plus détaillées, des options de personnalisation (par exemple, période rétrospective, option de paiement, etc.) et pour acheter ElastiCache des nœuds réservés.

Ressources supplémentaires

- Vous trouverez ici des informations sur les nœuds ElastiCache réservés et sur la manière dont ils peuvent vous faire économiser de l'argent.
- Pour plus d'informations sur cette recommandation, consultez Vérification de l'optimisation des instances réservées dans la FAQ Trusted Advisor.
- Pour une description plus détaillée des champs, voir la documentation de l'Explorateur de coûts

Colonnes du rapport

- Région
- Famille
- Type de nœud
- Description du produit
- Nombre recommandé de nœuds réservés à acheter
- Utilisation moyenne attendue des nœuds réservés
- Économies estimées avec les recommandations (mensuelles)
- Coût initial des nœuds réservés
- Coût estimé des nœuds réservés (mensuel)
- Coût à la demande estimé après achat des nœuds réservés recommandés (mensuel)
- Rentabilité estimée (mois)
- Période de recherche (jours)
- Durée (années)

Optimisation des instances réservées Amazon OpenSearch Service

Description

Vérifie votre utilisation d'Amazon OpenSearch Service et fournit des recommandations sur l'achat d'instances réservées. Ces recommandations visent à réduire les coûts liés à l'utilisation de OpenSearch On-Demand. Nous créons ces recommandations en analysant votre utilisation à la demande au cours des 30 derniers jours.

Nous utilisons cette analyse pour simuler chaque combinaison de réservations dans la catégorie d'utilisation générée. Cela nous permet de recommander le nombre de chaque type d'instance réservée à acheter pour réaliser le plus d'économies. Cette vérification couvre les recommandations basées sur l'option de paiement initial partiel avec un engagement d'un an ou de trois ans.

Cette vérification n'est pas disponible pour les comptes liés à la facturation consolidée. Les recommandations pour cette vérification ne sont disponibles que pour le compte de règlement.

ID de la vérification

`7ujm6yhn5t`

Critères d'alerte

Jaune : l'optimisation de l'achat d'instances réservées Amazon OpenSearch Service peut contribuer à réduire les coûts.

Action recommandée

Consultez la page Cost Explorer pour obtenir des recommandations plus détaillées, des options de personnalisation (par exemple, période rétrospective, option de paiement, etc.) et pour acheter des instances réservées Amazon OpenSearch Service.

Ressources supplémentaires

- Vous trouverez ici des informations sur les instances réservées Amazon OpenSearch Service et sur la manière dont elles peuvent vous faire économiser de l'argent.
- Pour plus d'informations sur cette recommandation, consultez Vérification de l'optimisation des instances réservées dans la FAQ Trusted Advisor.
- Pour une description plus détaillée des champs, voir la documentation de l'Explorateur de coûts

Colonnes du rapport

- Région
- Classe d'instance
- Taille d’instance
- Nombre recommandé d'instances réservées à acheter
- Utilisation moyenne attendue des instances réservées
- Économies estimées avec les recommandations (mensuelles)
- Coût initial des instances réservées
- Coût estimé des instances réservées (mensuel)
- Coût à la demande estimé après achat des instances réservées recommandées (mensuel)
- Rentabilité estimée (mois)
- Période de recherche (jours)
- Durée (années)

Instances de base de données Amazon RDS inactives

Description

Vérifie la configuration de votre Amazon Relational Database Service (Amazon RDS) pour toutes les instances de base de données qui semblent inactives.

Si une instance de base de données n'a pas fait l'objet d'une connexion pendant une période prolongée, vous pouvez supprimer l'instance pour réduire les coûts. Une instance de base de données est considérée comme inactive si l'instance n'a pas fait l'objet d'une connexion au cours des 7 derniers jours. Si un stockage permanent est nécessaire pour les données de l'instance, vous pouvez utiliser des options moins coûteuses telles que la prise d'un instantané de bases de données et sa conservation. Les instantanés de bases de données créés manuellement sont conservés jusqu'à ce que vous les supprimiez.

ID de la vérification

`Ti39halfu8`

Critères d'alerte

Jaune : une instance de base de données active n'a pas fait l'objet d'une connexion au cours des 7 derniers jours.

Action recommandée

Envisagez de prendre un instantané de l'instance de base de données inactive, puis de l'arrêter ou de la supprimer. L'arrêt de l'instance de base de données supprime certains coûts, mais ne supprime pas les coûts de stockage. Une instance arrêtée conserve toutes les sauvegardes automatisées en fonction de la période de conservation configurée. L'arrêt d'une instance de base de données entraîne généralement des coûts supplémentaires par rapport à la suppression de l'instance et à la conservation de l'instantané final uniquement. Voir Arrêt temporaire d'une instance de bases de données Amazon RDS et Deleting a DB Instance with a Final Snapshot (Suppression d'une instance de base de données avec un instantané final).

Ressources supplémentaires

Sauvegarde et restauration

Colonnes du rapport

- Région
- Nom de l'instance de base de données

- Multi-AZ
- Type d'instance
- Stockage provisionné (Go)
- Nombre de jours depuis la dernière connexion
- Économies mensuelles estimées (à la demande)

Optimisation des nœuds réservés Amazon Redshift

Description

Vérifie votre utilisation d'Amazon Redshift et fournit des recommandations sur l'achat de nœuds réservés afin de réduire les coûts relatifs à l'utilisation d'Amazon Redshift à la demande.

Nous générons ces recommandations en analysant votre utilisation à la demande au cours des 30 derniers jours. Nous utilisons cette analyse pour simuler chaque combinaison de réservations dans la catégorie d'utilisation générée. Cela nous permet de déterminer le meilleur nombre de chaque type de nœuds réservés à acheter pour réaliser le plus d'économies. Cette vérification couvre les recommandations basées sur l'option de paiement initial partiel avec un engagement d'un an ou de trois ans.

Cette vérification n'est pas disponible pour les comptes liés à la facturation consolidée. Les recommandations pour cette vérification ne sont disponibles que pour le compte de règlement.

ID de la vérification

`1qw23er45t`

Critères d'alerte

Jaune : l'optimisation de l'achat de nœuds réservés Amazon Redshift peut contribuer à réduire les coûts.

Action recommandée

Consultez la page de l'Explorateur de coûts pour des recommandations plus détaillées, des options de personnalisation (par exemple, période de recherche, option de paiement, etc.) et pour acheter des nœuds réservés Amazon Redshift.

Ressources supplémentaires

- Vous trouverez des informations sur les nœuds réservés Amazon Redshift et sur la façon dont ils peuvent vous faire économiser de l'argent ici.

- Pour plus d'informations sur cette recommandation, consultez Vérification de l'optimisation des instances réservées dans la FAQ Trusted Advisor.
- Pour une description plus détaillée des champs, voir la documentation de l'Explorateur de coûts

Colonnes du rapport

- Région
- Famille
- Type de nœud
- Nombre recommandé de nœuds réservés à acheter
- Utilisation moyenne attendue des nœuds réservés
- Économies estimées avec les recommandations (mensuelles)
- UpFront Coût des nœuds réservés
- Coût estimé des nœuds réservés (mensuel)
- Coût à la demande estimé après achat des nœuds réservés recommandés (mensuel)
- Rentabilité estimée (mois)
- Période de recherche (jours)
- Durée (années)

Optimisation des instances réservées Amazon Relational Database Service (RDS)

Description

Vérifie votre utilisation de RDS et fournit des recommandations sur l'achat d'instances réservées afin de réduire les coûts relatifs à l'utilisation de RDS à la demande.

Nous générons ces recommandations en analysant votre utilisation à la demande au cours des 30 derniers jours. Nous utilisons cette analyse pour simuler chaque combinaison de réservations dans la catégorie d'utilisation générée. Cela nous permet de déterminer le meilleur nombre de chaque type d'instance réservée à acheter pour réaliser le plus d'économies. Cette vérification couvre les recommandations basées sur l'option de paiement initial partiel avec un engagement d'un an ou de trois ans.

Cette vérification n'est pas disponible pour les comptes liés à la facturation consolidée. Les recommandations pour cette vérification ne sont disponibles que pour le compte de règlement.

ID de la vérification

`1qazXsw23e`

Critères d'alerte

Jaune : l'optimisation de l'achat d'instances réservées Amazon RDS peut contribuer à réduire les coûts.

Action recommandée

Consultez la page de l'Explorateur de coûts pour des recommandations plus détaillées, des options de personnalisation (par exemple, période de recherche, option de paiement, etc.) et pour acheter des instances réservées Amazon RDS.

Ressources supplémentaires

- Vous trouverez des informations sur les instances réservées Amazon RDS et sur la façon dont elles peuvent vous faire économiser de l'argent ici.
- Pour plus d'informations sur cette recommandation, consultez Vérification de l'optimisation des instances réservées dans la FAQ Trusted Advisor.
- Pour une description plus détaillée des champs, voir la documentation de l'Explorateur de coûts

Colonnes du rapport

- Région
- Famille
- Type d'instance
- Modèle de licence
- Édition de base de données
- Moteur de base de données
- Option de déploiement
- Nombre recommandé d'instances réservées à acheter
- Utilisation moyenne attendue des instances réservées
- Économies estimées avec les recommandations (mensuelles)
- Coût initial des instances réservées
- Coût estimé des instances réservées (mensuel)
- Coût à la demande estimé après achat des instances réservées recommandées (mensuel)
- Rentabilité estimée (mois)

- Période de recherche (jours)
- Durée (années)

Jeux d'enregistrements de ressource de latence Amazon Route 53.

Description

Vérifie les jeux d'enregistrements de latence Amazon Route 53 qui ne sont pas configurés de manière efficace.

Pour autoriser Amazon Route 53 à acheminer les requêtes vers la Région AWS avec la latence réseau la plus faible, vous devez créer des jeux d'enregistrements de ressource de latence pour un nom de domaine particulier (par exemple exemple.com) dans différentes régions. Si vous créez un seul jeu d'enregistrements de ressource de latence pour un nom de domaine, toutes les requêtes sont acheminées vers une région et vous payez des frais supplémentaires pour un routage basé sur la latence sans bénéficier des avantages.

Les zones hébergées créées par les services AWS n'apparaîtront pas dans vos résultats de vérification.

ID de la vérification

`51fC20e7I2`

Critères d'alerte

Jaune : un seul ensemble d'enregistrements de ressources de latence est configuré pour un nom de domaine particulier.

Action recommandée

Si vous avez des ressources dans plusieurs régions, veillez à définir un ensemble d'enregistrements de ressources de latence pour chaque région. Voir Routage basé sur la latence.

Si vous avez des ressources dans une seule Région AWS, envisagez de créer des ressources dans plus d'une Région AWS et définissez des ensembles d'enregistrements de ressources de latence pour chacune d'entre elles. Voir Routage basé sur la latence.

Si vous ne souhaitez pas utiliser plusieurs Régions AWS, vous devez utiliser un ensemble d'enregistrements de ressources simple. Voir Working with Resource Record Sets (Utilisation des ensembles d'enregistrements de ressources).

Ressources supplémentaires

- Guide du développeur Amazon Route 53
- Tarification Amazon Route 53

Colonnes du rapport

- Nom de la zone hébergée
- ID de la zone hébergée
- Nom de l'ensemble d'enregistrements de ressources
- Type d'ensemble d'enregistrements de ressources

Politique de cycle de vie de compartiment Amazon S3 configurée

Description

Vérifie si une politique de cycle de vie est configurée pour un compartiment Amazon S3. Une politique de cycle de vie Amazon S3 assure que les objets Amazon S3 du compartiment sont stockés à moindre coût tout au long de leur cycle de vie. Cela est important pour répondre aux exigences réglementaires en matière de conservation et de stockage des données. La configuration de la politique est un ensemble de règles qui définit des actions que le service Amazon S3 applique à un groupe d'objets. Une politique de cycle de vie vous permet d'automatiser le transfert des objets vers des classes de stockage moins coûteuses ou de supprimer les objets en fonction de leur ancienneté. Par exemple, vous pouvez transférer un objet vers le stockage Amazon S3 Standard-IA 30 jours après sa création, ou vers Amazon S3 Glacier après 1 an.

Vous pouvez également définir l'expiration de l'objet afin qu'Amazon S3 supprime l'objet pour vous après un certain temps.

Vous pouvez ajuster la configuration de la vérification à l'aide des paramètres de vos règles AWS Config.

Pour plus d'informations, voir Gestion du cycle de vie de votre stockage.

> **Note**
>
> Les résultats de cette vérification sont automatiquement actualisés plusieurs fois par jour et les demandes d'actualisation ne sont pas autorisées. Plusieurs heures peuvent encore

être nécessaires pour que les modifications apparaissent. Actuellement, vous ne pouvez pas exclure des ressources de cette vérification.

ID de la vérification

`c18d2gz100`

Source

`AWS Config Managed Rule: s3-lifecycle-policy-check`

Critères d'alerte

Jaune : aucune politique de cycle de vie n'est configurée pour le compartiment Amazon S3.

Action recommandée

Assurez-vous qu'une politique de cycle de vie est configurée dans votre compartiment Amazon S3.

Si votre organisation n'a pas mis en place de politique de conservation, utilisez Amazon S3 Intelligent-Tiering pour optimiser les coûts.

Pour plus d'informations sur la façon de définir votre politique de cycle de vie Amazon S3, voir Définition d'une configuration de cycle de vie sur un compartiment.

Pour plus d'informations sur Amazon S3 Intelligent-Tiering, voir Classe de stockage Amazon S3 Intelligent-Tiering.

Ressources supplémentaires

Définition d'une configuration de cycle de vie sur un compartiment

Exemples de configurations de cycle de vie S3

Colonnes du rapport

- Statut
- Région
- Ressource
- Règle AWS Config
- Paramètres d'entrée

Configuration incomplète de l'interruption du téléchargement en plusieurs parties sur Amazon S3

Description

Vérifie que chaque compartiment Amazon S3 est configuré avec une règle de cycle de vie afin d'annuler les téléchargements partitionnés qui restent incomplets après 7 jours. Il est recommandé d'utiliser une règle de cycle de vie pour annuler ces téléchargements incomplets et supprimer le stockage associé.

> **Note**
>
> Les résultats de cette vérification sont automatiquement actualisés une ou plusieurs fois par jour, et les demandes d'actualisation ne sont pas autorisées. Plusieurs heures peuvent encore être nécessaires pour que les modifications apparaissent. Actuellement, vous ne pouvez pas exclure des ressources de cette vérification.

ID de la vérification

`c1cj39rr6v`

Critères d'alerte

Jaune : le compartiment de configuration du cycle de vie ne contient pas de règle de cycle de vie permettant d'annuler tous les téléchargements partitionnés qui restent incomplets après 7 jours.

Action recommandée

Passez en revue la configuration du cycle de vie des buckets sans établir de règle de cycle de vie qui permettrait de nettoyer tous les téléchargements partitionnés incomplets. Il est peu probable que les téléchargements qui ne sont pas terminés après 24 heures soient terminés. Cliquez ici pour suivre les instructions de création d'une règle de cycle de vie. Il est recommandé de l'appliquer à tous les objets de votre compartiment. Si vous devez appliquer d'autres actions du cycle de vie à des objets sélectionnés dans votre compartiment, vous pouvez avoir plusieurs règles avec différents filtres. Consultez le tableau de bord des lentilles de stockage ou appelez l' ListMultipartUpload API pour plus d'informations.

Ressources supplémentaires

Création d'une configuration du cycle de vie

Découverte et suppression des téléchargements partitionnés incomplets pour réduire les coûts liés à Amazon S3

Chargement et copie d'objets à l'aide du téléchargement partitionné

Éléments de configuration du cycle de vie

Éléments pour décrire les actions du cycle de vie

Configuration du cycle de vie pour annuler les téléchargements partitionnés

Colonnes du rapport

- Statut
- Région
- Nom du compartiment
- ARN de compartiment
- Règle de cycle de vie pour supprimer un MPU incomplet
- Jours après l'initiation
- Heure de la dernière modification

Compartiments Amazon S3 compatibles avec la gestion des versions, sans politiques de cycle de vie configurées

Description

Vérifie si une politique de cycle de vie est configurée pour les compartiments Amazon S3 compatibles avec la gestion des versions.

Pour plus d'informations, voir Gestion du cycle de vie de votre stockage.

Vous pouvez spécifier les noms des compartiments à vérifier l'aide du paramètre bucketNames de vos règles AWS Config.

> **Note**
>
> Les résultats de cette vérification sont automatiquement actualisés plusieurs fois par jour et les demandes d'actualisation ne sont pas autorisées. Plusieurs heures peuvent encore

être nécessaires pour que les modifications apparaissent. Actuellement, vous ne pouvez pas exclure des ressources de cette vérification.

ID de la vérification

`c18d2gz171`

Source

`AWS Config Managed Rule: s3-version-lifecycle-policy-check`

Critères d'alerte

Jaune : aucune politique de cycle de vie n'est configurée pour un compartiment Amazon S3 compatible avec la gestion des versions.

Action recommandée

Configurez des politiques de cycle de vie pour vos compartiments Amazon S3 pour gérer vos objets afin qu'ils soient stockés de manière rentable tout au long de leur cycle de vie.

Pour en savoir plus, consultez Définition d'une configuration de cycle de vie sur un compartiment.

Ressources supplémentaires

Gestion du cycle de vie de votre stockage

Définition d'une configuration de cycle de vie sur un compartiment

Colonnes du rapport

- Statut
- Région
- Ressource
- Règle AWS Config
- Paramètres d'entrée
- Heure de la dernière modification

Fonctions AWS Lambda avec des délais excessifs

Description

Vérifie les fonctions Lambda avec des taux élevés de délais pouvant entraîner des coûts élevés.

Frais Lambda basés sur le temps d'exécution et le nombre de demandes pour votre fonction. Les délais d'expiration des fonctions entraînent des erreurs qui peuvent provoquer de nouvelles tentatives. Retenter des fonctions entraîne des frais supplémentaires relatifs à la demande et l'exécution.

> **Note**
>
> Les résultats de cette vérification sont automatiquement actualisés plusieurs fois par jour, et les requêtes d'actualisation ne sont pas autorisées. Plusieurs heures peuvent encore être nécessaires pour que les modifications apparaissent. Actuellement, vous ne pouvez pas exclure des ressources de cette vérification.

ID de la vérification

`L4dfs2Q3C3`

Critères d'alerte

Jaune : fonctions dans lesquelles plus de 10 % des appels se terminent par une erreur en raison d'un délai d'expiration un jour donné au cours des 7 derniers jours.

Action recommandée

Inspectez la journalisation des fonctions et les suivis X-Ray pour déterminer le participant à la durée élevée de la fonction. Implémentez la journalisation dans votre code aux parties pertinentes, comme avant ou après les appels d'API ou les connexions à la base de données. Par défaut, les délais d'expiration des clients des kits SDK AWS peuvent être plus longs que la durée de la fonction configurée. Ajustez les clients de connexions d'API et de kits SDK pour réessayer ou échouer dans le délai d'expiration de la fonction. Si la durée attendue est supérieure au délai d'expiration configuré, vous pouvez augmenter le paramètre de délai d'expiration pour la fonction. Pour de plus amples informations, veuillez consulter Surveillance et dépannage d'applications Lambda.

Ressources supplémentaires

- Surveillance et dépannage d'applications Lambda
- Nouvelles tentatives et délai d'expiration d'une fonction Lambda à l'aide d'un kit SDK
- Utilisation de AWS Lambda avec AWS X-Ray
- Accès aux CloudWatch journaux Amazon pour AWS Lambda
- Exemple d'application du processeur d'erreurs pour AWS Lambda

Colonnes du rapport

- Statut
- Région
- ARN de la fonction
- Taux de délai d'expiration quotidien maximal
- Date du taux de délai d'expiration quotidien maximal
- Taux d'expiration quotidien moyen
- Paramètres du délai d'expiration des fonctions (millisecondes)
- Coût de calcul quotidien perdu
- Invocations quotidiennes moyennes
- Invocations du jour actuel
- Taux d'expiration du jour actuel
- Heure de la dernière modification

Fonctions AWS Lambda avec taux élevé d'erreurs

Description

Vérifie les fonctions Lambda avec des taux élevés d'erreurs pouvant augmenter les coûts.

Les frais Lambda sont basés sur le nombre de demandes et le temps d'exécution agrégé de votre fonction. Les erreurs de fonction peuvent entraîner des nouvelles tentatives impliquant des frais supplémentaires.

> **Note**
>
> Les résultats de cette vérification sont automatiquement actualisés plusieurs fois par jour, et les requêtes d'actualisation ne sont pas autorisées. Plusieurs heures peuvent encore être nécessaires pour que les modifications apparaissent. Actuellement, vous ne pouvez pas exclure des ressources de cette vérification.

ID de la vérification

`L4dfs2Q3C2`

Critères d'alerte

Jaune : fonctions dans lesquelles plus de 10 % des invocations se terminent par une erreur un jour donné au cours des 7 derniers jours.

Action recommandée

Envisagez les mesures suivantes pour réduire les erreurs. Les erreurs de fonction comprennent des erreurs renvoyées par le code de la fonction et des erreurs renvoyées par l'environnement d'exécution de la fonction.

Pour vous aider à résoudre les erreurs Lambda, Lambda s'intègre à des services tels qu'Amazon et. CloudWatch AWS X-Ray Vous pouvez utiliser une combinaison de journaux, de mesures, d'alarmes et de suivis X-Ray pour détecter rapidement et identifier les problèmes dans le code de votre fonction, de l'API ou d'autres ressources qui prennent en charge votre application. Pour de plus amples informations, veuillez consulter Surveillance et dépannage d'applications Lambda.

Pour plus d'informations sur la gestion des erreurs avec des environnements d'exécution spécifiques, consultez Gestion des erreurs et tentatives automatiques dans AWS Lambda.

Pour aller plus loin dans la résolution, consultez Résolution des problèmes dans Lambda.

Vous pouvez également choisir parmi un écosystème d'outils de surveillance et d'observabilité fournis par les partenaires AWS Lambda. Pour plus d'informations, consultez Partenaires AWS Lambda.

Ressources supplémentaires

- Gestion des erreurs et tentatives automatiques dans AWS Lambda
- Surveillance et dépannage d'applications Lambda
- Nouvelles tentatives et délai d'expiration d'une fonction Lambda à l'aide d'un kit SDK
- Résolution des problèmes dans Lambda
- Erreurs d'invocation d'API
- Exemple d'application du processeur d'erreurs pour AWS Lambda

Colonnes du rapport

- Statut
- Région
- ARN de la fonction

- Taux d'erreurs quotidien maximal
- Date du taux d'erreurs quotidien maximal
- Taux d'erreurs quotidien moyen
- Coût de calcul quotidien perdu
- Invocations quotidiennes moyennes
- Invocations du jour actuel

  Taux d'erreurs du jour actuel
- Heure de la dernière modification

Fonctions AWS Lambda surprovisionnées pour la taille de la mémoire

Description

Vérifie les fonctions AWS Lambda qui ont été invoquées au moins une fois pendant la période de recherche. Cette vérification vous avertit si l'une de vos fonctions Lambda a été surprovisionnée pour la taille de la mémoire. Lorsque des fonctions Lambda sont surprovisionnée pour les tailles de mémoire, vous payez pour les ressources inutilisées. Bien que certains scénarios puissent entraîner une faible utilisation par conception, vous pouvez souvent réduire vos coûts en modifiant la configuration de la mémoire de vos fonctions Lambda. Les économies mensuelles estimées sont calculées en utilisant le taux d'utilisation actuel des fonctions Lambda.

> **Note**
>
> Les résultats de cette vérification sont automatiquement actualisés plusieurs fois par jour et les demandes d'actualisation ne sont pas autorisées. Plusieurs heures peuvent encore être nécessaires pour que les modifications apparaissent. Actuellement, vous ne pouvez pas exclure des ressources de cette vérification.

ID de la vérification

`C0r6dfpM05`

Critères d'alerte

Jaune : fonction Lambda surprovisionnée pour la taille de la mémoire pendant la période de recherche. Pour déterminer si une fonction Lambda est surprovisionnée, nous prenons en compte

toutes les CloudWatch mesures par défaut pour cette fonction. L'algorithme utilisé pour identifier les fonctions Lambda surprovisionnées pour la taille de la mémoire suit les bonnes pratiques AWS. L'algorithme est mis à jour lorsqu'un nouveau modèle a été identifié.

Action recommandée

Pensez à réduire la taille de la mémoire de vos fonctions Lambda.

Pour plus d'informations, consultez Inscription à AWS Compute Optimizer pour les vérifications de Trusted Advisor.

Colonnes du rapport

- Statut
- Région
- Nom de la fonction
- Version de fonction
- Taille de la mémoire (Mo)
- Taille de mémoire recommandée (Mo)
- Période de recherche (jours)
- Opportunité d'économies (%)
- Économies mensuelles estimées
- Devise des économies mensuelles estimées
- Heure de la dernière modification

Problèmes à risque élevé AWS Well-Architected pour l'optimisation des coûts

Description

Vérifiez les éventuels problèmes à risque élevé (HRI, high risk issues) pour vos charges de travail dans le pilier de l'optimisation des coûts. Cette vérification est basée sur vos commentaires AWS-Well Architected. Les résultats de la vérification varient selon que vous avez terminé ou non l'évaluation de la charge de travail avec AWS Well-Architected.

> **Note**
>
> Les résultats de cette vérification sont automatiquement actualisés plusieurs fois par jour et les demandes d'actualisation ne sont pas autorisées. Plusieurs heures peuvent encore

être nécessaires pour que les modifications apparaissent. Actuellement, vous ne pouvez pas exclure des ressources de cette vérification.

ID de la vérification

`Wxdfp4B1L1`

Critères d'alerte

- Rouge : au moins un problème à risque élevé actif a été identifié dans le pilier Optimisation des coûts du Cadre AWS Well-Architected.
- Vert : aucun problème à risque élevé actif n'a été détecté dans le pilier Optimisation des coûts du Cadre AWS Well-Architected.

Action recommandée

AWS Well-Architected a détecté des problèmes à risque élevé pendant l'évaluation de votre charge de travail. Ces problèmes offrent la possibilité de réduire les risques et d'économiser de l'argent. Connectez-vous à l'outil AWS Well-Architected afin de passer en revue vos réponses et d'intervenir pour résoudre vos problèmes actifs.

Colonnes du rapport

- Statut
- Région
- ARN de la charge de travail
- Nom de la charge de travail
- Nom de l'évaluateur
- Type de charge de travail
- Date de début de la charge de travail
- Date de la dernière modification de la charge de travail
- Nombre de problèmes à haut risque identifiés pour l'Optimisation des coûts
- Nombre de problèmes à haut risque résolus pour l'Optimisation des coûts
- Nombre de questions ayant reçu une réponse pour l'Optimisation des coûts
- Nombre total de questions dans le pilier Optimisation des coûts
- Heure de la dernière modification

Équilibreurs de charge inactifs

Description

Vérifie la configuration Elastic Load Balancing pour les équilibreurs de charge qui sont inactifs.

Tout équilibreur de charge configuré entraîne des frais. Si un équilibreur de charge n'a aucune instance back-end associée, ou si le trafic réseau est sévèrement limité, l'équilibreur de charge n'est pas utilisé efficacement. Cette vérification vérifie actuellement uniquement le type de Classic Load Balancer dans le service ELB. Elle n'inclut pas d'autres types ELB (Application Load Balancer, Network Load Balancer).

ID de la vérification

`hjLMh88uM8`

Critères d'alerte

- Jaune : un équilibreur de charge ne possède aucune instance principale active.
- Jaune : un équilibreur de charge ne possède aucune instance principale saine active.
- Jaune : un équilibreur de charge a reçu moins de 100 demandes par jour au cours des 7 derniers jours.

Action recommandée

Si votre équilibreur de charge ne possède aucune instance principale active, envisagez d'enregistrer des instances ou de supprimer votre équilibreur de charge. Voir Enregistrement ou annulation de l'enregistrement de vos instances Amazon EC2 pour votre Classic Load Balancer ou Suppression de votre équilibreur de charge.

Si votre équilibreur de charge ne possède aucune instance principale saine, consultez Résoudre les problèmes liés à un Classic Load Balancer : configuration de la surveillance de l'état.

Si votre équilibreur de charge a reçu un faible nombre de demandes, envisagez de le supprimer. Voir Suppression de votre équilibreur de charge.

Ressources supplémentaires

- Gestion des équilibreurs de charge
- Résoudre les problèmes liés à votre Classic Load Balancer

Colonnes du rapport

- Région
- Nom de l'équilibreur de charge

- Raison
- Économies mensuelles estimées

Instances Amazon EC2 sous-exploitées

Description

Vérifie les instances Amazon Elastic Compute Cloud (Amazon EC2) exécutées à tout moment au cours des 14 derniers jours. Cette vérification vous avertit si l'utilisation quotidienne du processeur était de 10 % ou moins et si les I/O réseau étaient de 5 Mo ou moins pendant au moins 4 jours.

Les instances en cours d'exécution génèrent des coûts d'utilisation horaires. Bien que certains scénarios puissent entraîner une faible utilisation par conception, vous pouvez souvent réduire vos coûts en gérant le nombre et la taille de vos instances.

Les économies mensuelles estimées sont calculées en utilisant le taux d'utilisation actuel des instances à la demande et le nombre estimé de jours pendant lesquels l'instance peut être sous-utilisée. Les économies réelles varient si vous utilisez des instances réservées ou des instances Spot, ou si l'instance n'est pas en cours d'exécution pendant une journée complète. Pour obtenir des données d'utilisation quotidienne, téléchargez le rapport pour cette vérification.

ID de la vérification

`Qch7DwouX1`

Critères d'alerte

Jaune : une instance affichait 10 % ou moins d'utilisation moyenne du processeur par jour et 5 Mo ou moins d'E/S réseau pendant au moins 4 des 14 derniers jours.

Action recommandée

Envisagez d'arrêter ou de résilier les instances peu utilisées, ou augmentez le nombre d'instances à l'aide d'Auto Scaling. Pour de plus amples informations, veuillez consulter Arrêt et démarrage de votre instance, Résilier une instance et Qu'est-ce qu'Amazon EC2 Auto Scaling ?.

Ressources supplémentaires

- Surveiller Amazon EC2
- Métadonnées d'instance et données utilisateur
- Guide de CloudWatch l'utilisateur Amazon
- Guide du développeur Auto Scaling

Colonnes du rapport

- Région/zone de disponibilité
- ID d’instance
- Nom de l'instance
- Type d'instance
- Économies mensuelles estimées
- Utilisation moyenne du processeur sur 14 jours
- E/S réseau moyennes sur 14 jours
- Nombre de jours d'utilisation faible

Savings Plan

Description

Vérifie votre utilisation d'Amazon EC2, de Fargate et de Lambda au cours des 30 derniers jours et fournit des recommandations d'achat de Savings Plan. Ces recommandations vous permettent de vous engager à un montant d'utilisation uniforme mesuré en dollars par heure pour une période d'un ou trois ans en échange de tarifs réduits.

Ceux-ci proviennent de AWS Cost Explorer, qui peut obtenir des informations plus détaillées sur les recommandations. Vous pouvez également acheter un Savings Plan via Cost Explorer. Ces recommandations devraient être considérées comme une alternative à vos recommandations sur les instances réservées. Nous vous suggérons de ne suivre qu'à une seule série de recommandations. Prendre les deux en considération peut conduire à un engagement excessif.

Cette vérification n'est pas disponible pour les comptes liés dans la facturation consolidée. Les recommandations pour cette vérification ne sont disponibles que pour le compte de règlement.

ID de la vérification

`vZ2c2W1srf`

Critères d'alerte

Jaune : l'optimisation de l'achat de Savings Plans peut contribuer à réduire les coûts.

Action recommandée

Consultez la page de l'Explorateur de coûts pour des recommandations personnalisées et pour acheter des Savings Plans.

Ressources supplémentaires

- Guide de l'utilisateur Savings Plans
- FAQ Savings Plans

Colonnes du rapport

- Type de Savings Plan
- Option de paiement
- Coût initial
- Engagement d'achat horaire
- Utilisation moyenne estimée
- Économies mensuelles estimées
- Pourcentage d'économies estimé
- Durée (années)
- Période de recherche (jours)

Adresses IP Elastic non associées

Description

Recherche les adresses IP Elastic (EIP) qui ne sont pas associées à une instance Amazon Elastic Compute Cloud (Amazon EC2) en cours d'exécution.

Les EIP sont des adresses IP statiques conçues pour le cloud computing dynamique. Contrairement aux adresses IP statiques traditionnelles, les EIP masquent l'échec d'une instance ou d'une zone de disponibilité en remappant une adresse IP publique à une autre instance de votre compte. Des frais nominaux sont appliqués pour un EIP qui n'est pas associé à une instance en cours d'exécution.

ID de la vérification

`Z4AUBRNSmz`

Critères d'alerte

Jaune : une adresse IP Elastic (EIP) allouée n'est pas associée à une instance Amazon EC2 en cours d'exécution.

Action recommandée

Associez l'EIP à une instance active en cours d'exécution ou libérez l'adresse IP non associée. Pour de plus amples informations, veuillez consulter Associating an Elastic IP Address with a Different Running Instance (Associer une adresse IP Elastic à une autre instance en cours d'exécution) et Releasing an Elastic IP Address (Libérer une adresse IP Elastic).

Ressources supplémentaires

Adresses IP Elastic

Colonnes du rapport

- Région
- Adresse IP

Volumes Amazon EBS sous-utilisés

Description

Vérifie les configurations de volumes Amazon Elastic Block Store (Amazon EBS) et avertit lorsque les volumes semblent sous-utilisés.

Les frais sont calculés dès qu'un volume est créé. Si un volume reste non attaché ou a une activité d'écriture très faible (à l'exclusion des volumes de démarrage) pendant un certain temps, le volume est sous-utilisé. Nous vous recommandons de supprimer les volumes sous-utilisés pour réduire les coûts.

ID de la vérification

`DAvU99Dc4C`

Critères d'alerte

Jaune : un volume est détaché ou a enregistré moins d'une IOPS par jour au cours des 7 derniers jours.

Action recommandée

Envisagez de créer un instantané et de supprimer le volume pour réduire les coûts. Pour de plus amples informations, veuillez consulter Créer des instantanés Amazon EBS et Supprimer un volume Amazon EBS.

Ressources supplémentaires

- Amazon Elastic Block Store (Amazon EBS)

- Surveillance du statut de vos volumes

Colonnes du rapport

- Région
- ID du volume
- Nom du volume
- Type de volume
- Taille du volume
- Coût de stockage mensuel
- ID de l'instantané
- Nom de l'instantané
- Âge de l'instantané

> **Note**
>
> Si vous avez inscrit votre compte à AWS Compute Optimizer, nous vous recommandons d'utiliser plutôt le contrôle des volumes surprovisionnés Amazon EBS. Pour plus d'informations, consultez Inscription à AWS Compute Optimizer pour les vérifications de Trusted Advisor.

Underutilized Amazon Redshift Clusters

Description

Vérifie la présence de clusters qui semblent sous-utilisés dans votre configuration Amazon Redshift.

Si un cluster Amazon Redshift n'a pas fait l'objet d'une connexion depuis longtemps ou utilise une faible quantité du processeur, vous avez d'autres possibilités telles que la réduction de la taille du cluster ou l'arrêt du cluster et la prise d'un instantané final. Les instantanés finaux sont conservés même après la suppression de votre cluster.

ID de la vérification

`G31sQ1E9U`

Critères d'alerte

- Jaune : aucun cluster en cours d'exécution n'a fait l'objet d'une connexion au cours des 7 derniers jours.
- Jaune : un cluster en cours d'exécution a affiché moins de 5 % d'utilisation moyenne du processeur au niveau du cluster pendant 99 % du temps sur les 7 derniers jours.

Action recommandée

Envisagez d'arrêter le cluster et de prendre un instantané final, ou de réduire la taille du cluster. Voir Shutting Down and Deleting (Arrêt et suppression de clusters) et Redimensionnement des clusters.

Ressources supplémentaires

Guide de CloudWatch l'utilisateur Amazon

Colonnes du rapport

- Statut
- Région
- Cluster
- Type d'instance
- Raison
- Économies mensuelles estimées

Performance

Améliorez les performances de votre service en vérifiant vos Service Quotas (anciennement appelés limites), afin que vous puissiez profiter du débit provisionné, contrôler les instances surutilisées et détecter les ressources inutilisées.

Vous pouvez utiliser les vérifications suivantes pour la catégorie de performances.

Noms des vérifications

- Le cluster de base de données Amazon Aurora est sous-provisionné pour la charge de travail de lecture
- Amazon DynamoDB Auto Scaling non activé
- Optimisation Amazon EBS non activée
- Configuration des pièces jointes de volumes d'IOPS provisionnés Amazon EBS (SSD)

- Volumes Amazon EBS sous-provisionnés
- Le groupe Amazon EC2 Auto Scaling n'est associé à aucun modèle de lancement
- Optimisation du débit Amazon EC2 vers EBS
- La virtualisation EC2 est de type paravirtuel
- Limite stricte de mémoire Amazon ECS
- Optimisation du mode de débit Amazon EFS
- Le paramètre d'autovacuum d'Amazon RDS est désactivé
- Les clusters de base de données Amazon RDS ne prennent en charge que des volumes allant jusqu'à 64 TiB
- Instances de base de données Amazon RDS dans les clusters avec des classes d'instances hétérogènes
- Instances de base de données Amazon RDS dans les clusters avec des tailles d'instance hétérogènes
- Les paramètres de mémoire de la base de données Amazon RDS divergent des paramètres par défaut
- Le paramètre enable_indexonlyscan d'Amazon RDS est désactivé
- Le paramètre enable_indexscan d'Amazon RDS est désactivé
- Le paramètre general_logging d'Amazon RDS est activé
- Paramètre Amazon RDS InnoDB_CHANGE_BUFFERING utilisant une valeur inférieure à la valeur optimale
- Le paramètre innodb_open_files d'Amazon RDS est faible
- Le paramètre innodb_stats_persistent d'Amazon RDS est désactivé
- Instance Amazon RDS sous-provisionnée pour la capacité du système
- Le volume magnétique Amazon RDS est en cours d'utilisation
- Les groupes de paramètres Amazon RDS n'utilisent pas de pages volumineuses
- Le paramètre de cache de requêtes Amazon RDS est activé
- La mise à jour de la classe d'instance des ressources Amazon RDS est requise
- La mise à jour des versions majeures des ressources Amazon RDS est requise
- Ressources Amazon RDS utilisant l'édition du moteur de fin de support sous licence incluse
- Jeux d'enregistrements de ressource d'alias dans Amazon Route 53.
- Fonctions AWS Lambda sous-provisionnées pour la taille de la mémoire

- Fonctions AWS Lambda configurées sans limite de simultanéité
- Problèmes à risque élevé AWS Well-Architected pour la performance
- CloudFront Noms de domaine alternatifs
- CloudFront Optimisation de la diffusion de contenu
- CloudFront Transfert d'en-têtes et taux de réussite du cache
- Instances Amazon EC2 surexploitées
- Grand nombre de règles de groupe de sécurité EC2 appliquées à une instance
- Grand nombre de règles dans un groupe de sécurité EC2
- Volumes magnétiques Amazon EBS surutilisés

Le cluster de base de données Amazon Aurora est sous-provisionné pour la charge de travail de lecture

Description

Vérifie si le cluster de base de données Amazon Aurora dispose des ressources nécessaires pour prendre en charge une charge de travail de lecture.

ID de la vérification

`c1qf5bt038`

Critères d'alerte

Jaune :

Augmentation du nombre de lectures de base de données : la charge de base de données était élevée et la base de données lisait plus de lignes qu'elle n'écrivait ou ne mettait à jour les lignes.

Action recommandée

Nous vous recommandons de régler vos requêtes pour réduire la charge de la base de données ou d'ajouter une instance de base de données de lecture à votre cluster de bases de données avec la même classe et la même taille que l'instance de base de données d'écriture du cluster. La configuration actuelle comporte au moins une instance de base de données dont la charge de base de données est constamment élevée, principalement en raison d'opérations de lecture. Répartissez ces opérations en ajoutant une autre instance de base de données au cluster et en dirigeant la charge de travail de lecture vers le point de terminaison en lecture seule du cluster de base de données.

Ressources supplémentaires

Un cluster de base de données Aurora possède un point de terminaison de lecteur pour les connexions en lecture seule. Ce point de terminaison utilise l'équilibrage de charge pour gérer les requêtes qui contribuent le plus à la charge de la base de données dans votre cluster de bases de données. Le point de terminaison du lecteur dirige ces instructions vers les répliques Aurora Read et réduit la charge sur l'instance principale. Le point de terminaison du lecteur adapte également la capacité à gérer des requêtes SELECT simultanées en fonction du nombre de répliques Aurora Read dans le cluster.

Pour plus d'informations, consultez les sections Ajout de répliques Aurora à un cluster de base de données et Gestion des performances et du dimensionnement des clusters de bases de données Aurora.

Colonnes du rapport

- Statut
- Région
- Ressource
- Augmentation du nombre de lectures de base de données (nombre)
- Dernière période de détection
- Heure de la dernière modification

Amazon DynamoDB Auto Scaling non activé

Description

Vérifie si l'autoscaling ou la mise à l'échelle à la demande sont activés sur pour vos tables Amazon DynamoDB et vos index secondaires globaux.

L'autoscaling d'Amazon DynamoDB utilise le service d'autoscaling d'application pour ajuster de manière dynamique la capacité de débit provisionnée en votre nom en réponse aux schémas de trafic réels. Cela permet à une table ou à un index secondaire global d'augmenter sa capacité de lecture et d'écriture approvisionnée afin de gérer les hausses soudaines de trafic sans limitation. Lorsque la charge de travail diminue, la scalabilité automatique d'application réduit le débit de sorte que vous ne payez pas pour une capacité approvisionnée non utilisée.

Vous pouvez ajuster la configuration de la vérification à l'aide des paramètres de vos règles AWS Config.

Pour plus d'informations, voir Gestion automatique de la capacité de débit avec l'autoscaling de DynamoDB.

> **Note**
>
> Les résultats de cette vérification sont automatiquement actualisés plusieurs fois par jour et les demandes d'actualisation ne sont pas autorisées. Plusieurs heures peuvent encore être nécessaires pour que les modifications apparaissent. Actuellement, vous ne pouvez pas exclure des ressources de cette vérification.

ID de la vérification

`c18d2gz136`

Source

AWS ConfigRègle gérée : dynamodb-autoscaling-enabled

Critères d'alerte

Jaune : l'autoscaling n'est pas activé pour vos tables DynamoDB et/ou vos index secondaires globaux.

Action recommandée

Activez l'autoscaling pour vos tables Amazon DynamoDB, à moins que vous ne disposiez déjà d'un mécanisme permettant de mettre à l'échelle automatiquement le débit provisionné de votre table DynamoDB et/ou de vos index secondaires globaux en fonction de vos exigences en matière de charge de travail.

Pour plus d'informations, voir Utilisation de la console de gestion AWS avec l'autoscaling de DynamoDB.

Ressources supplémentaires

Gestion automatique de la capacité de débit avec l'autoscaling de DynamoDB

Colonnes du rapport

- Statut
- Région
- Ressource
- Règle AWS Config

- Paramètres d'entrée
- Heure de la dernière modification

Optimisation Amazon EBS non activée

Description

Vérifie si l'optimisation Amazon EBS est activée pour vos instances Amazon EC2.

Une instance optimisée pour Amazon EBS utilise une pile de configuration optimisée et fournit une capacité supplémentaire dédiée aux E/S Amazon EBS. Cette optimisation offre les meilleures performances pour vos volumes EBS en limitant les conflits entre les E/S Amazon EBS et le trafic restant de votre instance.

Pour plus d'informations, voir Instances optimisées pour Amazon EBS.

> **Note**
>
> Les résultats de cette vérification sont automatiquement actualisés plusieurs fois par jour et les demandes d'actualisation ne sont pas autorisées. Plusieurs heures peuvent encore être nécessaires pour que les modifications apparaissent. Actuellement, vous ne pouvez pas exclure des ressources de cette vérification.

ID de la vérification

`c18d2gz142`

Source

AWS ConfigRègle gérée : ebs-optimized-instance

Critères d'alerte

Jaune : l'optimisation Amazon EBS n'est pas activée sur les instances Amazon EC2 prises en charge.

Action recommandée

Activez l'optimisation Amazon EBS sur les instances prises en charge.

Pour plus d'informations, voir Activation de l'optimisation EBS au lancement.

Ressources supplémentaires

Instances optimisées pour Amazon EBS

Colonnes du rapport

- Statut
- Région
- Ressource
- Règle AWS Config
- Paramètres d'entrée
- Heure de la dernière modification

Configuration des pièces jointes de volumes d'IOPS provisionnés Amazon EBS (SSD)

Description

Vérifie les volumes d'IOPS provisionnés (SSD) attachés à une instance Amazon Elastic Compute Cloud (Amazon EC2) pouvant être optimisée pour Amazon EBS qui n'est pas optimisée pour EBS.

Les volumes IOPS provisionnés (SSD) dans Amazon Elastic Block Store (Amazon EBS) sont conçus pour fournir les performances attendues uniquement lorsqu'ils sont attachés à une instance optimisée pour EBS.

ID de la vérification

`PPkZrjsH2q`

Critères d'alerte

Jaune : une instance Amazon EC2 qui peut être optimisée pour EBS possède un volume d'IOPS provisionnés (SSD) attaché, mais l'instance n'est pas optimisée pour EBS.

Action recommandée

Créez une nouvelle instance optimisée pour EBS, détachez le volume et rattachez-le à votre nouvelle instance. Pour plus d'informations, consultez Instances optimisées pour Amazon EBS et Attacher un volume Amazon EBS à une instance.

Ressources supplémentaires

- Types de volumes Amazon EBS

- Performance des volumes Amazon EBS sur les instances Linux

Colonnes du rapport

- Statut
- Région/zone de disponibilité
- ID du volume
- Nom du volume
- Attachement du volume
- ID d'instance
- Type d'instance
- Optimisée pour EBS

Volumes Amazon EBS sous-provisionnés

Description

Vérifie les volumes Amazon Elastic Block Store (Amazon EBS) qui étaient en cours d'exécution à tout moment pendant la période de recherche. Cette vérification vous avertit si des volumes EBS ont été sous-provisionnés pour vos charges de travail. Une utilisation élevée constante peut indiquer des performances optimisées et stables, mais peut également indiquer qu'une application ne dispose pas de ressources suffisantes.

> **Note**
>
> Les résultats de cette vérification sont automatiquement actualisés plusieurs fois par jour et les demandes d'actualisation ne sont pas autorisées. Plusieurs heures peuvent encore être nécessaires pour que les modifications apparaissent. Actuellement, vous ne pouvez pas exclure des ressources de cette vérification.

ID de la vérification

`C0r6dfpM04`

Critères d'alerte

Jaune : volume EBS sous-provisionné pendant la période de recherche. Pour déterminer si un volume est sous-provisionné, nous prenons en compte toutes les CloudWatch mesures par

défaut (y compris les IOPS et le débit). L'algorithme utilisé pour identifier les volumes EBS sous-provisionnés suit les bonnes pratiques AWS. L'algorithme est mis à jour lorsqu'un nouveau modèle a été identifié.

Action recommandée

Pensez à augmenter les volumes d'utilisation élevée.

Pour plus d'informations, consultez Inscription à AWS Compute Optimizer pour les vérifications de Trusted Advisor.

Colonnes du rapport

- Statut
- Région
- ID du volume
- Type de volume
- Taille du volume (Go)
- IOPS de référence du volume
- IOPS de rafale du volume
- Débit de rafale du volume
- Type de volume recommandé
- Taille de volume recommandée (Go)
- IOPS de référence de volume recommandées
- IOPS de rafale de volume recommandées
- Débit de référence de volume recommandé
- Débit de rafale de volume recommandé
- Période de recherche (jours)
- Risques liés aux performances
- Heure de la dernière modification

Le groupe Amazon EC2 Auto Scaling n'est associé à aucun modèle de lancement

Description

Vérifie si un groupe Amazon EC2 Auto Scaling est créé à partir d'un modèle de lancement Amazon EC2.

Utilisez un modèle de lancement pour créer vos groupes Amazon EC2 Auto Scaling afin d'assurer l'accès aux dernières fonctionnalités et améliorations des groupes Auto Scaling, notamment la gestion des versions et les types d'instances multiples.

Pour plus d'informations, voir Modèles de lancement.

> **Note**
>
> Les résultats de cette vérification sont automatiquement actualisés plusieurs fois par jour et les demandes d'actualisation ne sont pas autorisées. Plusieurs heures peuvent encore être nécessaires pour que les modifications apparaissent. Actuellement, vous ne pouvez pas exclure des ressources de cette vérification.

ID de la vérification

`c18d2gz102`

Source

AWS ConfigRègle gérée : autoscaling-launch-template

Critères d'alerte

Le groupe Amazon EC2 Auto Scaling n'est associé à aucun modèle de lancement valide.

Action recommandée

Utilisez un modèle de lancement Amazon EC2 pour créer vos groupes Amazon EC2 Auto Scaling.

Pour plus d'informations, voir Création d'un modèle de lancement pour un groupe Auto Scaling.

Ressources supplémentaires

- Modèles de lancement
- Création d'un modèle de lancement

Colonnes du rapport

- Statut
- Région
- Ressource
- Règle AWS Config

- Paramètres d'entrée
- Heure de la dernière modification

Optimisation du débit Amazon EC2 vers EBS

Description

Vérifie les volumes Amazon EBS dont les performances peuvent être affectées par la capacité de débit maximum de l'instance Amazon EC2 à laquelle ils sont attachés.

Pour optimiser les performances, vous devez vous assurer que le débit maximum d'une instance Amazon EC2 est supérieur au débit maximum agrégé des volumes EBS attachés. Cette vérification calcule le débit total du volume EBS pour chaque période de cinq minutes du jour précédent (basé sur l'heure universelle coordonnée (UTC)) pour chaque instance optimisée pour EBS et vous avertit si l'utilisation au cours de plus de la moitié de ces périodes est supérieure à 95 % du débit maximum de l'instance EC2.

ID de la vérification

`Bh2xRR2FGH`

Critères d'alerte

Jaune : la veille (UTC), le débit agrégé (mégaoctets/s) des volumes EBS attachés à l'instance EC2 dépassait 95 % du débit publié entre l'instance et les volumes EBS plus de 50 % du temps.

Action recommandée

Comparez le débit maximal de vos volumes Amazon EBS (voir Types de volume Amazon EBS) avec le débit maximum de l'instance Amazon EC2 à laquelle ils sont attachés. Voir les types d'instances qui prennent en charge l'optimisation EBS.

Envisagez d'associer vos volumes à une instance qui prend en charge un débit plus élevé vers Amazon EBS pour des performances optimales.

Ressources supplémentaires

- Types de volumes Amazon EBS
- Instances optimisées pour Amazon EBS
- Surveillance du statut de vos volumes
- Attacher un volume Amazon EBS à une instance

- Détacher un volume Amazon EBS d'une instance
- Supprimer un volume Amazon EBS

Colonnes du rapport

- Statut
- Région
- ID d’instance
- Type d'instance
- Heure quasi maximum

La virtualisation EC2 est de type paravirtuel

Description

Vérifie si la virtualisation d'une instance Amazon EC2 est de type paravirtuel.

Il est recommandé d'utiliser des instances de machines virtuelles matérielles (HVM) plutôt que des instances paravirtuelles, dans la mesure du possible. Cela est dû aux améliorations de la virtualisation HVM et à la disponibilité de pilotes de paravirtualisation (PV) pour les AMI HVM, qui ont permis de combler l'écart de performance qui existait traditionnellement entre les invités PV et HVM. Il est important de noter que les types d'instances de la génération actuelle ne prennent pas en charge les AMI PV. Par conséquent, le choix d'un type d'instance HVM offre les meilleures performances et la meilleure compatibilité avec le matériel moderne.

Pour plus d'informations, consultez Types de virtualisations AMI Linux.

> **Note**
>
> Les résultats de cette vérification sont automatiquement actualisés plusieurs fois par jour et les demandes d'actualisation ne sont pas autorisées. Plusieurs heures peuvent encore être nécessaires pour que les modifications apparaissent. Actuellement, vous ne pouvez pas exclure des ressources de cette vérification.

ID de la vérification

`c18d2gz148`

Source

AWS ConfigRègle gérée : ec2- paravirtual-instance-check

Critères d'alerte

Jaune : la virtualisation des instances Amazon EC2 est de type paravirtuel.

Action recommandée

Utilisez la virtualisation HVM pour vos instances Amazon EC2 et utilisez un type d'instance compatible.

Pour plus d'informations sur le choix du type de virtualisation approprié, voir Compatibilité pour modifier le type d'instance.

Ressources supplémentaires

Compatibilité pour modifier le type d'instance

Colonnes du rapport

- Statut
- Région
- Ressource
- Règle AWS Config
- Paramètres d'entrée
- Heure de la dernière modification

Limite stricte de mémoire Amazon ECS

Description

Vérifie si les définitions des tâches Amazon ECS ont une limite de mémoire définie pour leurs définitions de conteneurs. La quantité totale de mémoire réservée pour tous les conteneurs d'une tâche doit être inférieure à la valeur Mémoire de la tâche.

Pour plus d'informations, voir Définitions de conteneur.

> **Note**
>
> Les résultats de cette vérification sont automatiquement actualisés plusieurs fois par jour et les demandes d'actualisation ne sont pas autorisées. Plusieurs heures peuvent encore

être nécessaires pour que les modifications apparaissent. Actuellement, vous ne pouvez pas exclure des ressources de cette vérification.

ID de la vérification

`c18d2gz176`

Source

AWS ConfigRègle gérée : ecs-task-definition-memory -hard-limit

Critères d'alerte

Jaune : aucune limite stricte de mémoire Amazon ECS n'est définie.

Action recommandée

Allouez de la mémoire à vos tâches Amazon ECS afin d'éviter de manquer de mémoire. Si votre conteneur tente de dépasser la mémoire spécifiée, il est terminé.

Pour plus d'informations, voir Comment allouer de la mémoire à des tâches dans Amazon ECS ?.

Ressources supplémentaires

Réservation de cluster

Colonnes du rapport

- Statut
- Région
- Ressource
- Règle AWS Config
- Paramètres d'entrée
- Heure de la dernière modification

Optimisation du mode de débit Amazon EFS

Description

Vérifie si le système de fichiers Amazon EFS du client est actuellement configuré pour utiliser le mode de débit en rafales.

Les systèmes de fichiers en mode de débit en rafales d'EFS [1] fournissent un niveau de débit de référence constant (50 Ko/s par Go de données dans le stockage standard EFS) et utilisent un modèle de crédit pour fournir des niveaux supérieurs de performance de « débit de transmission de débordement » lorsque des « crédits de transmission en rafales » sont disponibles. Lorsque vous épuisez vos crédits, les performances de votre système de fichiers sont limitées à ce niveau de référence inférieur, ce qui peut entraîner des ralentissements, des délais d'attente ou d'autres formes d'impact sur les performances pour vos utilisateurs finaux ou vos applications.

ID de la vérification

`c1dfprch02`

Critères d'alerte

- Jaune : le système de fichiers utilise le mode de débit en rafale.

Action recommandée

Nous vous recommandons de mettre à jour la configuration de votre système de fichiers en mode de débit élastique [2] pour permettre à vos utilisateurs et à vos applications d'atteindre le débit souhaité. En mode de débit élastique, votre système de fichiers peut atteindre jusqu'à 10 Go/s de débit de lecture ou 3 Go/s de débit d'écriture, en fonction de la région AWS [3], et vous ne payez que pour le débit que vous utilisez. Notez que vous pouvez mettre à jour la configuration de votre système de fichiers pour basculer à la demande entre les modes de débit élastique et en rafales, et que les systèmes de fichiers en mode de débit élastique peuvent occasionner des frais supplémentaires pour le transfert de données [4].

Ressources supplémentaires

- [1] Performances d'Amazon EFS – Modes de débit
- [2] Performances d'Amazon EFS – Mode de débit élastique
- [3] Quotas et limites Amazon EFS
- [4] Tarification d'Amazon EFS

Colonnes du rapport

- Statut
- Région
- Identifiant de système de fichiers EFS
- Mode de débit
- Heure de la dernière modification

Le paramètre d'autovacuum d'Amazon RDS est désactivé

Description

Le paramètre autovacuum est désactivé pour vos instances de base de données. La désactivation de l'aspirateur automatique augmente le gonflement de la table et de l'index et a un impact sur les performances.

Nous vous recommandons d'activer l'autovacuum dans vos groupes de paramètres de base de données.

> **Note**
>
> Les résultats de cette vérification sont automatiquement actualisés plusieurs fois par jour et les demandes d'actualisation ne sont pas autorisées. Plusieurs heures peuvent encore être nécessaires pour que les modifications apparaissent. Actuellement, vous ne pouvez pas exclure des ressources de cette vérification.

> **Note**
>
> Lorsqu'une instance ou un cluster de bases de données est arrêté, vous pouvez consulter les recommandations Amazon RDS Trusted Advisor pendant 3 à 5 jours. Après cinq jours, les recommandations ne sont plus disponibles dansTrusted Advisor. Pour consulter les recommandations, ouvrez la console Amazon RDS, puis choisissez Recommendations. Si vous supprimez une instance ou un cluster de bases de données, les recommandations associées à ces instances ou clusters ne sont pas disponibles dans Trusted Advisor ou dans la console de gestion Amazon RDS.

ID de la vérification

`c1qf5bt025`

Critères d'alerte

Jaune : l'autovacuum est désactivé pour les groupes de paramètres de base de données.

Action recommandée

Activez le paramètre autovacuum dans vos groupes de paramètres de base de données.

Ressources supplémentaires

La base de données PostgreSQL nécessite une maintenance périodique connue sous le nom de mise sous vide. Autovacuum dans PostgreSQL automatise l'exécution des commandes VACCUUM et ANALYZE. Ce processus rassemble les statistiques du tableau et supprime les lignes mortes. Lorsque l'autovacuum est désactivé, l'augmentation de la table, le gonflement de l'index et les statistiques périmées ont un impact sur les performances de la base de données.

Pour plus d'informations, consultez Comprendre l'autovacuum dans les environnements Amazon RDS for PostgreSQL.

Colonnes du rapport

- Statut
- Région
- Ressource
- Nom du paramètre
- Valeur recommandée
- Heure de la dernière modification

Les clusters de base de données Amazon RDS ne prennent en charge que des volumes allant jusqu'à 64 TiB

Description

Vos clusters de base de données prennent en charge des volumes allant jusqu'à 64 TiB. Les dernières versions du moteur prennent en charge des volumes allant jusqu'à 128 TiB. Nous vous recommandons de mettre à niveau la version du moteur de votre cluster de base de données vers les dernières versions afin de prendre en charge des volumes allant jusqu'à 128 TiB.

> **Note**
>
> Les résultats de cette vérification sont automatiquement actualisés plusieurs fois par jour et les demandes d'actualisation ne sont pas autorisées. Plusieurs heures peuvent encore être nécessaires pour que les modifications apparaissent. Actuellement, vous ne pouvez pas exclure des ressources de cette vérification.

> **Note**
>
> Lorsqu'une instance ou un cluster de bases de données est arrêté, vous pouvez consulter les recommandations Amazon RDS Trusted Advisor pendant 3 à 5 jours. Après cinq jours, les recommandations ne sont plus disponibles dansTrusted Advisor. Pour consulter les recommandations, ouvrez la console Amazon RDS, puis choisissez Recommendations. Si vous supprimez une instance ou un cluster de bases de données, les recommandations associées à ces instances ou clusters ne sont pas disponibles dans Trusted Advisor ou dans la console de gestion Amazon RDS.

ID de la vérification

`c1qf5bt017`

Critères d'alerte

Jaune : les clusters de base de données ne prennent en charge que les volumes jusqu'à 64 TiB.

Action recommandée

Mettez à niveau la version du moteur de vos clusters de base de données pour prendre en charge des volumes allant jusqu'à 128 TiB.

Ressources supplémentaires

Lorsque vous augmentez votre application sur un seul cluster de base de données Amazon Aurora, vous risquez de ne pas atteindre la limite si la limite de stockage est de 128 TiB. L'augmentation de la limite de stockage permet d'éviter de supprimer les données ou de diviser la base de données sur plusieurs instances.

Pour plus d'informations, consultez les limites de taille d'Amazon Aurora.

Colonnes du rapport

- Statut
- Région
- Ressource
- Nom du moteur
- Version actuelle du moteur
- Valeur recommandée
- Heure de la dernière modification

Instances de base de données Amazon RDS dans les clusters avec des classes d'instances hétérogènes

Description

Nous vous recommandons d'utiliser la même classe et la même taille d'instance de base de données pour toutes les instances de base de données de votre cluster de base de données.

> **Note**
>
> Les résultats de cette vérification sont automatiquement actualisés plusieurs fois par jour et les demandes d'actualisation ne sont pas autorisées. Plusieurs heures peuvent encore être nécessaires pour que les modifications apparaissent. Actuellement, vous ne pouvez pas exclure des ressources de cette vérification.

> **Note**
>
> Lorsqu'une instance ou un cluster de bases de données est arrêté, vous pouvez consulter les recommandations Amazon RDS Trusted Advisor pendant 3 à 5 jours. Après cinq jours, les recommandations ne sont plus disponibles dansTrusted Advisor. Pour consulter les recommandations, ouvrez la console Amazon RDS, puis choisissez Recommendations. Si vous supprimez une instance ou un cluster de bases de données, les recommandations associées à ces instances ou clusters ne sont pas disponibles dans Trusted Advisor ou dans la console de gestion Amazon RDS.

ID de la vérification

`c1qf5bt009`

Critères d'alerte

Rouge : les clusters de base de données contiennent des instances de base de données avec des classes d'instances hétérogènes.

Action recommandée

Utilisez la même classe et la même taille d'instance pour toutes les instances de base de données de votre cluster de base de données.

Ressources supplémentaires

Lorsque les instances de base de données de votre cluster de base de données utilisent différentes classes ou tailles d'instances de base de données, il peut y avoir un déséquilibre dans la charge de travail des instances de base de données. Lors d'un basculement, l'une des instances de base de données du lecteur devient une instance de base de données du rédacteur. Si les instances de base de données utilisent la même classe et la même taille d'instance de base de données, la charge de travail peut être équilibrée pour les instances de base de données de votre cluster de base de données.

Pour plus d'informations, consultez la section Répliques d'Aurora.

Colonnes du rapport

- Statut
- Région
- Ressource
- Valeur recommandée
- Nom du moteur
- Heure de la dernière modification

Instances de base de données Amazon RDS dans les clusters avec des tailles d'instance hétérogènes

Description

Nous vous recommandons d'utiliser la même classe et la même taille d'instance de base de données pour toutes les instances de base de données de votre cluster de base de données.

> **Note**
>
> Les résultats de cette vérification sont automatiquement actualisés plusieurs fois par jour et les demandes d'actualisation ne sont pas autorisées. Plusieurs heures peuvent encore être nécessaires pour que les modifications apparaissent. Actuellement, vous ne pouvez pas exclure des ressources de cette vérification.

> **Note**
>
> Lorsqu'une instance ou un cluster de bases de données est arrêté, vous pouvez consulter les recommandations Amazon RDS Trusted Advisor pendant 3 à 5 jours. Après cinq jours, les recommandations ne sont plus disponibles dansTrusted Advisor. Pour consulter les recommandations, ouvrez la console Amazon RDS, puis choisissez Recommendations. Si vous supprimez une instance ou un cluster de bases de données, les recommandations associées à ces instances ou clusters ne sont pas disponibles dans Trusted Advisor ou dans la console de gestion Amazon RDS.

ID de la vérification

`c1qf5bt008`

Critères d'alerte

Rouge : les clusters de base de données contiennent des instances de base de données de tailles d'instance hétérogènes.

Action recommandée

Utilisez la même classe et la même taille d'instance pour toutes les instances de base de données de votre cluster de base de données.

Ressources supplémentaires

Lorsque les instances de base de données de votre cluster de base de données utilisent différentes classes ou tailles d'instances de base de données, il peut y avoir un déséquilibre dans la charge de travail des instances de base de données. Lors d'un basculement, l'une des instances de base de données du lecteur devient une instance de base de données du rédacteur. Si les instances de base de données utilisent la même classe et la même taille d'instance de base de données, la charge de travail peut être équilibrée pour les instances de base de données de votre cluster de base de données.

Pour plus d'informations, consultez la section Répliques d'Aurora.

Colonnes du rapport

- Statut
- Région
- Ressource

- Valeur recommandée
- Nom du moteur
- Heure de la dernière modification

Les paramètres de mémoire de la base de données Amazon RDS divergent des paramètres par défaut

Description

Les paramètres de mémoire des instances de base de données sont significativement différents des valeurs par défaut. Ces paramètres peuvent avoir un impact sur les performances et provoquer des erreurs.

Nous vous recommandons de réinitialiser les paramètres de mémoire personnalisés de l'instance de base de données à leurs valeurs par défaut dans le groupe de paramètres de base de données.

> **Note**
>
> Les résultats de cette vérification sont automatiquement actualisés plusieurs fois par jour et les demandes d'actualisation ne sont pas autorisées. Plusieurs heures peuvent encore être nécessaires pour que les modifications apparaissent. Actuellement, vous ne pouvez pas exclure des ressources de cette vérification.

> **Note**
>
> Lorsqu'une instance ou un cluster de bases de données est arrêté, vous pouvez consulter les recommandations Amazon RDS Trusted Advisor pendant 3 à 5 jours. Après cinq jours, les recommandations ne sont plus disponibles dansTrusted Advisor. Pour consulter les recommandations, ouvrez la console Amazon RDS, puis choisissez Recommendations. Si vous supprimez une instance ou un cluster de bases de données, les recommandations associées à ces instances ou clusters ne sont pas disponibles dans Trusted Advisor ou dans la console de gestion Amazon RDS.

ID de la vérification

`c1qf5bt020`

Critères d'alerte

Jaune : les groupes de paramètres de base de données ont des paramètres de mémoire qui divergent considérablement par rapport aux valeurs par défaut.

Action recommandée

Réinitialisez les paramètres de mémoire à leurs valeurs par défaut.

Ressources supplémentaires

Pour plus d'informations, consultez Bonnes pratiques de configuration des paramètres pour Amazon RDS for MySQL, partie 1 : Paramètres liés aux performances.

Colonnes du rapport

- Statut
- Région
- Ressource
- Nom du paramètre
- Valeur recommandée
- Heure de la dernière modification

Le paramètre enable_indexonlyscan d'Amazon RDS est désactivé

Description

Le planificateur ou l'optimiseur de requêtes ne peut pas utiliser le type de plan de scan indexé uniquement lorsqu'il est désactivé.

Nous vous recommandons de définir la valeur du paramètre enable_indexonlyscan sur 1.

> **Note**
>
> Les résultats de cette vérification sont automatiquement actualisés plusieurs fois par jour et les demandes d'actualisation ne sont pas autorisées. Plusieurs heures peuvent encore être nécessaires pour que les modifications apparaissent. Actuellement, vous ne pouvez pas exclure des ressources de cette vérification.

> **Note**
>
> Lorsqu'une instance ou un cluster de bases de données est arrêté, vous pouvez consulter les recommandations Amazon RDS Trusted Advisor pendant 3 à 5 jours. Après cinq jours, les recommandations ne sont plus disponibles dansTrusted Advisor. Pour consulter les recommandations, ouvrez la console Amazon RDS, puis choisissez Recommendations. Si vous supprimez une instance ou un cluster de bases de données, les recommandations associées à ces instances ou clusters ne sont pas disponibles dans Trusted Advisor ou dans la console de gestion Amazon RDS.

ID de la vérification

`c1qf5bt028`

Critères d'alerte

Jaune : le paramètre enable_indexonlyscan est désactivé pour les groupes de paramètres de base de données.

Action recommandée

Définissez le paramètre enable_indexonlyscan sur 1.

Ressources supplémentaires

Lorsque vous désactivez le paramètre enable_indexonlyscan, il empêche le planificateur de requêtes de sélectionner un plan d'exécution optimal. Le planificateur de requêtes utilise un autre type de plan, tel que le scan d'index, qui peut augmenter le coût des requêtes et le temps d'exécution. Le type de plan de numérisation à index uniquement permet de récupérer les données sans accéder aux données de la table.

Pour plus d'informations, consultez enable_indexonlyscan (boolean) sur le site Web de documentation de PostgreSQL.

Colonnes du rapport

- Statut
- Région
- Ressource
- Nom du paramètre

- Valeur recommandée
- Heure de la dernière modification

Le paramètre enable_indexscan d'Amazon RDS est désactivé

Description

Le planificateur ou l'optimiseur de requêtes ne peut pas utiliser le type de plan d'analyse d'index lorsqu'il est désactivé.

Nous vous recommandons de définir la valeur du paramètre enable_indexscan sur 1.

> **Note**
>
> Les résultats de cette vérification sont automatiquement actualisés plusieurs fois par jour et les demandes d'actualisation ne sont pas autorisées. Plusieurs heures peuvent encore être nécessaires pour que les modifications apparaissent. Actuellement, vous ne pouvez pas exclure des ressources de cette vérification.

> **Note**
>
> Lorsqu'une instance ou un cluster de bases de données est arrêté, vous pouvez consulter les recommandations Amazon RDS Trusted Advisor pendant 3 à 5 jours. Après cinq jours, les recommandations ne sont plus disponibles dansTrusted Advisor. Pour consulter les recommandations, ouvrez la console Amazon RDS, puis choisissez Recommendations. Si vous supprimez une instance ou un cluster de bases de données, les recommandations associées à ces instances ou clusters ne sont pas disponibles dans Trusted Advisor ou dans la console de gestion Amazon RDS.

ID de la vérification

`c1qf5bt029`

Critères d'alerte

Jaune : le paramètre enable_indexscan est désactivé pour les groupes de paramètres de base de données.

Action recommandée

Définissez le paramètre enable_indexscan sur 1.

Ressources supplémentaires

Lorsque vous désactivez le paramètre enable_indexscan, il empêche le planificateur de requêtes de sélectionner un plan d'exécution optimal. Le planificateur de requêtes utilise un autre type de plan, tel que le scan d'index, qui peut augmenter le coût des requêtes et le temps d'exécution.

Pour plus d'informations, consultez enable_indexscan (boolean) sur le site Web de documentation de PostgreSQL.

Colonnes du rapport

- Statut
- Région
- Ressource
- Nom du paramètre
- Valeur recommandée
- Heure de la dernière modification

Le paramètre general_logging d'Amazon RDS est activé

Description

La journalisation générale est activée pour votre instance de base de données. Ce paramètre est utile pour résoudre les problèmes liés à la base de données. Cependant, l'activation de la journalisation générale augmente le nombre d'opérations d'E/S et l'espace de stockage alloué, ce qui peut entraîner des conflits et une dégradation des performances.

Vérifiez vos exigences en matière d'utilisation générale de la journalisation. Nous vous recommandons de définir la valeur du paramètre general_logging sur 0.

> **Note**
>
> Les résultats de cette vérification sont automatiquement actualisés plusieurs fois par jour et les demandes d'actualisation ne sont pas autorisées. Plusieurs heures peuvent encore être nécessaires pour que les modifications apparaissent. Actuellement, vous ne pouvez pas exclure des ressources de cette vérification.

> **Note**
>
> Lorsqu'une instance ou un cluster de bases de données est arrêté, vous pouvez consulter les recommandations Amazon RDS Trusted Advisor pendant 3 à 5 jours. Après cinq jours, les recommandations ne sont plus disponibles dansTrusted Advisor. Pour consulter les recommandations, ouvrez la console Amazon RDS, puis choisissez Recommendations. Si vous supprimez une instance ou un cluster de bases de données, les recommandations associées à ces instances ou clusters ne sont pas disponibles dans Trusted Advisor ou dans la console de gestion Amazon RDS.

ID de la vérification

`c1qf5bt037`

Critères d'alerte

Jaune : general_logging est activé pour les groupes de paramètres de base de données.

Action recommandée

Vérifiez vos exigences en matière d'utilisation générale de la journalisation. Si ce n'est pas obligatoire, nous vous recommandons de définir la valeur du paramètre general_logging sur 0.

Ressources supplémentaires

Le journal général des requêtes est activé lorsque la valeur du paramètre general_logging est 1. Le journal général des requêtes contient les enregistrements des opérations du serveur de base de données. Le serveur écrit des informations dans ce journal lorsque les clients se connectent ou se déconnectent et les journaux contiennent chaque instruction SQL reçue des clients. Le journal général des requêtes est utile lorsque vous suspectez une erreur chez un client et que vous souhaitez trouver les informations que le client doit envoyer au serveur de base de données.

Pour plus d'informations, consultez Présentation des journaux de base de données RDS pour MySQL.

Colonnes du rapport

- Statut
- Région
- Ressource
- Nom du paramètre

- Valeur recommandée
- Heure de la dernière modification

Paramètre Amazon RDS InnoDB_CHANGE_BUFFERING utilisant une valeur inférieure à la valeur optimale

Description

La mise en mémoire tampon des modifications permet à une instance de base de données MySQL de différer quelques écritures, qui sont nécessaires pour maintenir les index secondaires. Cette fonctionnalité était utile dans les environnements où les disques étaient lents. La modification de la configuration de la mise en mémoire tampon a légèrement amélioré les performances de la base de données, mais a retardé la reprise après incident et a prolongé les temps d'arrêt pendant la mise à niveau.

Nous vous recommandons de définir la valeur du paramètre innodb_change_buffering sur NONE.

> **Note**
>
> Les résultats de cette vérification sont automatiquement actualisés plusieurs fois par jour et les demandes d'actualisation ne sont pas autorisées. Plusieurs heures peuvent encore être nécessaires pour que les modifications apparaissent. Actuellement, vous ne pouvez pas exclure des ressources de cette vérification.

> **Note**
>
> Lorsqu'une instance ou un cluster de bases de données est arrêté, vous pouvez consulter les recommandations Amazon RDS Trusted Advisor pendant 3 à 5 jours. Après cinq jours, les recommandations ne sont plus disponibles dansTrusted Advisor. Pour consulter les recommandations, ouvrez la console Amazon RDS, puis choisissez Recommendations. Si vous supprimez une instance ou un cluster de bases de données, les recommandations associées à ces instances ou clusters ne sont pas disponibles dans Trusted Advisor ou dans la console de gestion Amazon RDS.

ID de la vérification

`c1qf5bt021`

Critères d'alerte

Jaune : le paramètre innodb_change_buffering est défini sur une valeur optimale basse pour les groupes de paramètres de base de données.

Action recommandée

Définissez la valeur du paramètre innodb_change_buffering sur NONE dans vos groupes de paramètres de base de données.

Ressources supplémentaires

Pour plus d'informations, consultez Bonnes pratiques de configuration des paramètres pour Amazon RDS for MySQL, partie 1 : Paramètres liés aux performances.

Colonnes du rapport

- Statut
- Région
- Ressource
- Nom du paramètre
- Valeur recommandée
- Heure de la dernière modification

Le paramètre innodb_open_files d'Amazon RDS est faible

Description

Le paramètre innodb_open_files contrôle le nombre de fichiers qu'InnoDB peut ouvrir en même temps. InnoDB ouvre tous les fichiers log et tablespace système lorsque mysqld est en cours d'exécution.

Votre instance de base de données a une faible valeur pour le nombre maximal de fichiers qu'InnoDB peut ouvrir en même temps. Nous vous recommandons de définir le paramètre innodb_open_files sur une valeur minimale de 65.

> **Note**
>
> Les résultats de cette vérification sont automatiquement actualisés plusieurs fois par jour et les demandes d'actualisation ne sont pas autorisées. Plusieurs heures peuvent encore être nécessaires pour que les modifications apparaissent. Actuellement, vous ne pouvez pas exclure des ressources de cette vérification.

> **Note**
>
> Lorsqu'une instance ou un cluster de bases de données est arrêté, vous pouvez consulter les recommandations Amazon RDS Trusted Advisor pendant 3 à 5 jours. Après cinq jours, les recommandations ne sont plus disponibles dansTrusted Advisor. Pour consulter les recommandations, ouvrez la console Amazon RDS, puis choisissez Recommendations. Si vous supprimez une instance ou un cluster de bases de données, les recommandations associées à ces instances ou clusters ne sont pas disponibles dans Trusted Advisor ou dans la console de gestion Amazon RDS.

ID de la vérification

`c1qf5bt033`

Critères d'alerte

Jaune : le paramètre des fichiers ouverts d'InnoDB est mal configuré pour les groupes de paramètres de base de données.

Action recommandée

Définissez le paramètre innodb_open_files sur une valeur minimale de 65.

Ressources supplémentaires

Le paramètre innodb_open_files contrôle le nombre de fichiers qu'InnoDB peut ouvrir en même temps. InnoDB garde tous les fichiers journaux et les fichiers d'espace disque logique du système ouverts lorsque mysqld est en cours d'exécution. InnoDB doit également ouvrir quelques fichiers .ibd, si le modèle de file-per-table stockage est utilisé. Lorsque le paramètre innodb_open_files est faible, cela a un impact sur les performances de la base de données et le serveur peut ne pas démarrer.

Pour plus d'informations, consultez Options de démarrage et variables système d'InnoDB - innodb_open_files sur le site Web de documentation. MySql

Colonnes du rapport

- Statut
- Région
- Ressource
- Nom du paramètre
- Valeur recommandée
- Heure de la dernière modification

Le paramètre innodb_stats_persistent d'Amazon RDS est désactivé

Description

Votre instance de base de données n'est pas configurée pour conserver les statistiques InnoDB sur le disque. Lorsque les statistiques ne sont pas stockées, elles sont recalculées à chaque redémarrage de l'instance et à chaque accès à la table. Cela entraîne des variations dans le plan d'exécution des requêtes. Vous pouvez modifier la valeur de ce paramètre global au niveau de la table.

Nous vous recommandons de définir la valeur du paramètre innodb_stats_persistent sur ON.

> **Note**
>
> Les résultats de cette vérification sont automatiquement actualisés plusieurs fois par jour et les demandes d'actualisation ne sont pas autorisées. Plusieurs heures peuvent encore être nécessaires pour que les modifications apparaissent. Actuellement, vous ne pouvez pas exclure des ressources de cette vérification.

> **Note**
>
> Lorsqu'une instance ou un cluster de bases de données est arrêté, vous pouvez consulter les recommandations Amazon RDS Trusted Advisor pendant 3 à 5 jours. Après cinq jours, les recommandations ne sont plus disponibles dansTrusted Advisor. Pour consulter les recommandations, ouvrez la console Amazon RDS, puis choisissez Recommendations.

Si vous supprimez une instance ou un cluster de bases de données, les recommandations associées à ces instances ou clusters ne sont pas disponibles dans Trusted Advisor ou dans la console de gestion Amazon RDS.

ID de la vérification

`c1qf5bt032`

Critères d'alerte

Jaune : les groupes de paramètres de base de données ont des statistiques d'optimisation qui ne sont pas conservées sur le disque.

Action recommandée

Définissez la valeur du paramètre innodb_stats_persistent sur ON.

Ressources supplémentaires

Si le paramètre innodb_stats_persistent est défini sur ON, les statistiques de l'optimiseur sont conservées au redémarrage de l'instance. Cela améliore la stabilité du plan d'exécution et la cohérence des performances des requêtes. Vous pouvez modifier la persistance des statistiques globales au niveau de la table en utilisant la clause STATS_PERSISTENT lorsque vous créez ou modifiez une table.

Pour plus d'informations, consultez Bonnes pratiques de configuration des paramètres pour Amazon RDS for MySQL, partie 1 : Paramètres liés aux performances.

Colonnes du rapport

- Statut
- Région
- Ressource
- Nom du paramètre
- Valeur recommandée
- Heure de la dernière modification

Instance Amazon RDS sous-provisionnée pour la capacité du système

Description

Vérifie si l'instance Amazon RDS ou l'instance de base de données Amazon Aurora possède la capacité système requise pour fonctionner.

ID de la vérification

`c1qf5bt039`

Critères d'alerte

Jaune :

O ut-of-memory kills : lorsqu'un processus est arrêté sur l'hôte de la base de données en raison d'une réduction de la mémoire au niveau du système d'exploitation, le compteur de pertes en mémoire insuffisante (OOM) augmente.

Échange excessif : les valeurs des métriques os.memory.swap.in et os.memory.swap.out étaient élevées.

Action recommandée

Nous vous recommandons de régler vos requêtes de manière à utiliser moins de mémoire ou d'utiliser un type d'instance de base de données avec une plus grande quantité de mémoire allouée. Lorsque la mémoire de l'instance est insuffisante, cela a un impact sur les performances de la base de données.

Ressources supplémentaires

Aucun ut-of-memory kill n'a été détecté : le noyau Linux invoque le logiciel Out of Memory (OOM) Killer lorsque les processus exécutés sur l'hôte nécessitent plus que la mémoire physiquement disponible sur le système d'exploitation. Dans ce cas, l'OOM Killer passe en revue tous les processus en cours d'exécution et arrête un ou plusieurs processus afin de libérer de la mémoire système et de maintenir le système en marche.

Un échange est détecté : lorsque la mémoire n'est pas suffisante sur l'hôte de base de données, le système d'exploitation envoie quelques pages utilisées au minimum sur le disque dans l'espace de swap. Ce processus de déchargement a un impact sur les performances de la base de données.

Pour plus d'informations, consultez Types d'instances Amazon RDS et Mise à l'échelle de votre instance Amazon RDS.

Colonnes du rapport

- Statut
- Région
- Ressource
- O ut-of-memory victimes (en nombre)
- Interrogations excessives (nombre)
- Dernière période de détection
- Heure de la dernière modification

Le volume magnétique Amazon RDS est en cours d'utilisation

Description

Vos instances de base de données utilisent le stockage magnétique. Le stockage magnétique n'est pas recommandé pour la plupart des instances de base de données. Choisissez un autre type de stockage : General Purpose (SSD) ou Provisioned IOPS.

> **Note**
>
> Les résultats de cette vérification sont automatiquement actualisés plusieurs fois par jour et les demandes d'actualisation ne sont pas autorisées. Plusieurs heures peuvent encore être nécessaires pour que les modifications apparaissent. Actuellement, vous ne pouvez pas exclure des ressources de cette vérification.

> **Note**
>
> Lorsqu'une instance ou un cluster de bases de données est arrêté, vous pouvez consulter les recommandations Amazon RDS Trusted Advisor pendant 3 à 5 jours. Après cinq jours, les recommandations ne sont plus disponibles dansTrusted Advisor. Pour consulter les recommandations, ouvrez la console Amazon RDS, puis choisissez Recommendations. Si vous supprimez une instance ou un cluster de bases de données, les recommandations associées à ces instances ou clusters ne sont pas disponibles dans Trusted Advisor ou dans la console de gestion Amazon RDS.

ID de la vérification

`c1qf5bt000`

Critères d'alerte

Jaune : les ressources Amazon RDS utilisent le stockage magnétique.

Action recommandée

Choisissez un autre type de stockage : General Purpose (SSD) ou Provisioned IOPS.

Ressources supplémentaires

Le stockage magnétique est un type de stockage de génération antérieure. Le type de stockage à usage général (SSD) ou IOPS provisionné est le type de stockage recommandé pour les nouvelles exigences de stockage. Ces types de stockage offrent des performances supérieures et constantes, ainsi que des options de taille de stockage améliorées.

Pour plus d'informations, consultez la section Volumes des générations précédentes.

Colonnes du rapport

- Statut
- Région
- Ressource
- Valeur recommandée
- Nom du moteur
- Heure de la dernière modification

Les groupes de paramètres Amazon RDS n'utilisent pas de pages volumineuses

Description

Les grandes pages peuvent augmenter l'évolutivité de la base de données, mais votre instance de base de données n'utilise pas de grandes pages. Nous vous recommandons de définir la valeur du paramètre use_large_pages sur UNIQUEMENT dans le groupe de paramètres de base de données de votre instance de base de données.

> **Note**
>
> Les résultats de cette vérification sont automatiquement actualisés plusieurs fois par jour et les demandes d'actualisation ne sont pas autorisées. Plusieurs heures peuvent encore

être nécessaires pour que les modifications apparaissent. Actuellement, vous ne pouvez pas exclure des ressources de cette vérification.

> **Note**
>
> Lorsqu'une instance ou un cluster de bases de données est arrêté, vous pouvez consulter les recommandations Amazon RDS Trusted Advisor pendant 3 à 5 jours. Après cinq jours, les recommandations ne sont plus disponibles dansTrusted Advisor. Pour consulter les recommandations, ouvrez la console Amazon RDS, puis choisissez Recommendations. Si vous supprimez une instance ou un cluster de bases de données, les recommandations associées à ces instances ou clusters ne sont pas disponibles dans Trusted Advisor ou dans la console de gestion Amazon RDS.

ID de la vérification

`c1qf5bt024`

Critères d'alerte

Jaune : les groupes de paramètres de base de données n'utilisent pas de grandes pages.

Action recommandée

Définissez la valeur du paramètre use_large_pages sur UNIQUEMENT dans vos groupes de paramètres de base de données.

Ressources supplémentaires

Pour plus d'informations, voir Activation HugePages d'une instance RDS pour Oracle.

Colonnes du rapport

- Statut
- Région
- Ressource
- Nom du paramètre
- Valeur recommandée
- Heure de la dernière modification

Le paramètre de cache de requêtes Amazon RDS est activé

Description

Lorsque les modifications nécessitent la purge de votre cache de requêtes, votre instance de base de données semble bloquée. La plupart des charges de travail ne bénéficient pas d'un cache de requête. Le cache de requête a été supprimé de MySQL version 8.0. Nous vous recommandons de définir le paramètre query_cache_type sur 0.

> **Note**
>
> Les résultats de cette vérification sont automatiquement actualisés plusieurs fois par jour et les demandes d'actualisation ne sont pas autorisées. Plusieurs heures peuvent encore être nécessaires pour que les modifications apparaissent. Actuellement, vous ne pouvez pas exclure des ressources de cette vérification.

> **Note**
>
> Lorsqu'une instance ou un cluster de bases de données est arrêté, vous pouvez consulter les recommandations Amazon RDS Trusted Advisor pendant 3 à 5 jours. Après cinq jours, les recommandations ne sont plus disponibles dansTrusted Advisor. Pour consulter les recommandations, ouvrez la console Amazon RDS, puis choisissez Recommendations. Si vous supprimez une instance ou un cluster de bases de données, les recommandations associées à ces instances ou clusters ne sont pas disponibles dans Trusted Advisor ou dans la console de gestion Amazon RDS.

ID de la vérification

`c1qf5bt022`

Critères d'alerte

Jaune : le cache de requêtes est activé pour les groupes de paramètres de base de données.

Action recommandée

Définissez la valeur du paramètre query_cache_type sur 0 dans vos groupes de paramètres de base de données.

Ressources supplémentaires

Pour plus d'informations, consultez Bonnes pratiques de configuration des paramètres pour Amazon RDS for MySQL, partie 1 : Paramètres liés aux performances.

Colonnes du rapport

- Statut
- Région
- Ressource
- Nom du paramètre
- Valeur recommandée
- Heure de la dernière modification

La mise à jour de la classe d'instance des ressources Amazon RDS est requise

Description

Votre base de données exécute une classe d'instance de base de données de génération précédente. Nous avons remplacé les classes d'instance de base de données d'une génération précédente par des classes d'instance de base de données offrant un meilleur coût, de meilleures performances, ou les deux. Nous vous recommandons d'exécuter votre instance de base de données avec une classe d'instance de base de données de nouvelle génération.

> **Note**
>
> Les résultats de cette vérification sont automatiquement actualisés plusieurs fois par jour et les demandes d'actualisation ne sont pas autorisées. Plusieurs heures peuvent encore être nécessaires pour que les modifications apparaissent. Actuellement, vous ne pouvez pas exclure des ressources de cette vérification.

> **Note**
>
> Lorsqu'une instance ou un cluster de bases de données est arrêté, vous pouvez consulter les recommandations Amazon RDS Trusted Advisor pendant 3 à 5 jours. Après cinq jours, les recommandations ne sont plus disponibles dansTrusted Advisor. Pour consulter les recommandations, ouvrez la console Amazon RDS, puis choisissez Recommendations.

Si vous supprimez une instance ou un cluster de bases de données, les recommandations associées à ces instances ou clusters ne sont pas disponibles dans Trusted Advisor ou dans la console de gestion Amazon RDS.

ID de la vérification

`c1qf5bt015`

Critères d'alerte

Rouge : les instances de base de données utilisent une classe d'instance de base de données de fin de support.

Action recommandée

Effectuez une mise à niveau vers la dernière classe d'instance DB.

Ressources supplémentaires

Pour plus d'informations, consultez Moteurs de base de données pris en charge pour les classes d'instances de base de données.

Colonnes du rapport

- Statut
- Région
- Ressource
- Classe d'instance de base de données
- Valeur recommandée
- Nom du moteur
- Heure de la dernière modification

La mise à jour des versions majeures des ressources Amazon RDS est requise

Description

Les bases de données dotées de la version majeure actuelle du moteur de base de données ne seront pas prises en charge. Nous vous recommandons de passer à la dernière version majeure qui inclut de nouvelles fonctionnalités et améliorations.

> **Note**
>
> Les résultats de cette vérification sont automatiquement actualisés plusieurs fois par jour et les demandes d'actualisation ne sont pas autorisées. Plusieurs heures peuvent encore être nécessaires pour que les modifications apparaissent. Actuellement, vous ne pouvez pas exclure des ressources de cette vérification.

> **Note**
>
> Lorsqu'une instance ou un cluster de bases de données est arrêté, vous pouvez consulter les recommandations Amazon RDS Trusted Advisor pendant 3 à 5 jours. Après cinq jours, les recommandations ne sont plus disponibles dansTrusted Advisor. Pour consulter les recommandations, ouvrez la console Amazon RDS, puis choisissez Recommendations. Si vous supprimez une instance ou un cluster de bases de données, les recommandations associées à ces instances ou clusters ne sont pas disponibles dans Trusted Advisor ou dans la console de gestion Amazon RDS.

ID de la vérification

`c1qf5bt014`

Critères d'alerte

Rouge : les ressources RDS utilisent des versions majeures en fin de support.

Action recommandée

Effectuez une mise à niveau vers la dernière version majeure du moteur de base de données.

Ressources supplémentaires

Amazon RDS publie de nouvelles versions pour les moteurs de base de données pris en charge afin de maintenir vos bases de données avec la dernière version. Les nouvelles versions publiées peuvent inclure des corrections de bogues, des améliorations de sécurité et d'autres améliorations du moteur de base de données. Vous pouvez minimiser le temps d'arrêt requis pour la mise à niveau de l'instance de base de données en utilisant un déploiement bleu/vert.

Pour plus d’informations, consultez les ressources suivantes :

- Mettre à niveau une version du moteur d'instance de base de données
- Mises à jour d'Amazon Aurora
- Utilisation des déploiements bleu/vert d'Amazon RDS pour les mises à jour de bases de données

Colonnes du rapport

- Statut
- Région
- Ressource
- Nom du moteur
- Version actuelle du moteur
- Valeur recommandée
- Heure de la dernière modification

Ressources Amazon RDS utilisant l'édition du moteur de fin de support sous licence incluse

Description

Nous vous recommandons de mettre à niveau la version majeure vers la dernière version du moteur prise en charge par Amazon RDS afin de continuer à bénéficier du support de licence actuel. La version du moteur de votre base de données ne sera pas prise en charge avec la licence actuelle.

> **Note**
>
> Les résultats de cette vérification sont automatiquement actualisés plusieurs fois par jour et les demandes d'actualisation ne sont pas autorisées. Plusieurs heures peuvent encore être nécessaires pour que les modifications apparaissent. Actuellement, vous ne pouvez pas exclure des ressources de cette vérification.

> **Note**
>
> Lorsqu'une instance ou un cluster de bases de données est arrêté, vous pouvez consulter les recommandations Amazon RDS Trusted Advisor pendant 3 à 5 jours. Après cinq jours,

les recommandations ne sont plus disponibles dansTrusted Advisor. Pour consulter les recommandations, ouvrez la console Amazon RDS, puis choisissez Recommendations. Si vous supprimez une instance ou un cluster de bases de données, les recommandations associées à ces instances ou clusters ne sont pas disponibles dans Trusted Advisor ou dans la console de gestion Amazon RDS.

ID de la vérification

`c1qf5bt016`

Critères d'alerte

Rouge : les ressources Amazon RDS utilisent l'édition du moteur de fin de support dans le cadre d'un modèle avec licence incluse.

Action recommandée

Nous vous recommandons de mettre à niveau votre base de données vers la dernière version prise en charge par Amazon RDS afin de continuer à utiliser le modèle sous licence.

Ressources supplémentaires

Pour plus d'informations, consultez la section Mises à niveau des versions majeures d'Oracle.

Colonnes du rapport

- Statut
- Région
- Ressource
- Nom du moteur
- Version actuelle du moteur
- Valeur recommandée
- Nom du moteur
- Heure de la dernière modification

Jeux d'enregistrements de ressource d'alias dans Amazon Route 53.

Description

Vérifie les jeux d'enregistrements de ressource qui peuvent être modifiés en jeux d'enregistrements de ressource d'alias afin d'améliorer les performances et de faire des économies.

Un jeu d'enregistrements de ressource d'alias achemine les requêtes DNS vers une ressource AWS (par exemple, un équilibreur de charge Elastic Load Balancing ou un compartiment Amazon S3) ou à un autre jeu d'enregistrements de ressource Route 53. Lorsque vous utilisez des jeux d'enregistrements de ressource d'alias, Route 53 achemine vos requêtes DNS vers des ressources AWS gratuitement.

Les zones hébergées créées par les services AWS n'apparaîtront pas dans vos résultats de vérification.

ID de la vérification

`B913Ef6fb4`

Critères d'alerte

- Jaune : un ensemble d'enregistrements de ressources est un CNAME vers un site web Amazon S3.
- Jaune : un ensemble d'enregistrements de ressources est le CNAME d'une CloudFront distribution Amazon.
- Jaune : un ensemble d'enregistrements de ressources est un CNAME vers un équilibreur de charge Elastic Load Balancing.

Action recommandée

Remplacez les ensembles d'enregistrements de ressources CNAME répertoriés par des ensembles d'enregistrements de ressources alias. Voir Choix entre des enregistrements avec ou sans alias.

Vous devez également modifier le type d'enregistrement CNAME en A ou AAAA, en fonction de la ressource AWS. Voir Valeurs à spécifier lorsque vous créez ou modifiez des enregistrements Amazon Route 53.

Ressources supplémentaires

Acheminement des requêtes vers des ressources AWS

Colonnes du rapport

- Statut
- Nom de la zone hébergée
- ID de la zone hébergée
- Nom de l'ensemble d'enregistrements de ressources
- Type d'ensemble d'enregistrements de ressources
- Identifiant d'un ensemble d'enregistrements de ressources
- Cible d'alias

Fonctions AWS Lambda sous-provisionnées pour la taille de la mémoire

Description

Vérifie les fonctions AWS Lambda qui ont été invoquées au moins une fois pendant la période de recherche. Cette vérification vous avertit si l'une de vos fonctions Lambda a été sous-provisionnée pour la taille de la mémoire. Lorsque des fonctions Lambda sont sous-provisionnées pour la taille de la mémoire, ces fonctions mettent plus de temps à se terminer.

> **Note**
>
> Les résultats de cette vérification sont automatiquement actualisés plusieurs fois par jour et les demandes d'actualisation ne sont pas autorisées. Plusieurs heures peuvent encore être nécessaires pour que les modifications apparaissent. Actuellement, vous ne pouvez pas exclure des ressources de cette vérification.

ID de la vérification

`COr6dfpM06`

Critères d'alerte

Jaune : fonction Lambda sous-provisionnée pour la taille de la mémoire pendant la période de recherche. Pour déterminer si une fonction Lambda est sous-provisionnée, nous prenons en compte toutes les CloudWatch métriques par défaut pour cette fonction. L'algorithme utilisé pour identifier les fonctions Lambda sous-provisionnées pour la taille de la mémoire suit les bonnes pratiques AWS. L'algorithme est mis à jour lorsqu'un nouveau modèle a été identifié.

Action recommandée

Pensez à augmenter la taille de la mémoire de vos fonctions Lambda.

Pour plus d'informations, consultez Inscription à AWS Compute Optimizer pour les vérifications de Trusted Advisor.

Colonnes du rapport

- Statut
- Région
- Nom de la fonction
- Version de fonction
- Taille de la mémoire (Mo)
- Taille de mémoire recommandée (Mo)
- Période de recherche (jours)
- Risques liés aux performances
- Heure de la dernière modification

Fonctions AWS Lambda configurées sans limite de simultanéité

Description

Vérifie si les fonctions AWS Lambda sont configurées avec une limite d'exécution simultanée au niveau de la fonction.

La simultanéité correspond au nombre de demandes en cours que votre fonction AWS Lambda traite en même temps. Pour chaque demande simultanée, Lambda fournit une instance distincte de votre environnement d'exécution.

Vous pouvez définir les limites de simultanéité minimale et maximale à l'aide des ConcurrencyLimitHighparamètres concurrencyLimitLowet de vos AWS Config règles.

Pour plus d'informations, consultez Capacité de mise à l'échelle d'une fonction Lambda.

> **Note**
>
> Les résultats de cette vérification sont automatiquement actualisés plusieurs fois par jour et les demandes d'actualisation ne sont pas autorisées. Plusieurs heures peuvent encore

être nécessaires pour que les modifications apparaissent. Actuellement, vous ne pouvez pas exclure des ressources de cette vérification.

ID de la vérification

`c18d2gz181`

Source

AWS ConfigRègle gérée : lambda-concurrency-check

Critères d'alerte

Jaune : aucune limite de simultanéité n'est configurée pour la fonction Lambda.

Action recommandée

Assurez-vous que la simultanéité est configurée pour vos fonctions Lambda. La configuration d'une limite de simultanéité pour vos fonctions Lambda permet de garantir que celles-ci traitent les demandes de manière fiable et prévisible. Une limite de simultanéité réduit le risque que votre fonction soit débordée en raison d'une augmentation soudaine du trafic.

Pour plus d'informations, voir Configuration de la simultanéité réservée.

Ressources supplémentaires

- Mise à l'échelle de fonction Lambda
- Configuration de la simultanéité réservée

Colonnes du rapport

- Statut
- Région
- Ressource
- Règle AWS Config
- Paramètres d'entrée
- Heure de la dernière modification

Problèmes à risque élevé AWS Well-Architected pour la performance

Description

Vérifiez les éventuels problèmes à risque élevé (HRI) pour vos charges de travail dans le pilier de performance. Cette vérification est basée sur vos commentaires AWS-Well Architected. Les résultats de la vérification varient selon que vous avez terminé ou non l'évaluation de la charge de travail avec AWS Well-Architected.

> **Note**
>
> Les résultats de cette vérification sont automatiquement actualisés plusieurs fois par jour et les demandes d'actualisation ne sont pas autorisées. Plusieurs heures peuvent encore être nécessaires pour que les modifications apparaissent. Actuellement, vous ne pouvez pas exclure des ressources de cette vérification.

ID de la vérification

`Wxdfp4B1L2`

Critères d'alerte

- Rouge : au moins un problème à risque élevé actif a été identifié dans le pilier Efficacité des performances du Cadre AWS Well-Architected.
- Vert : aucun problème à risque élevé actif n'a été détecté dans le pilier Efficacité des performances du Cadre AWS Well-Architected.

Action recommandée

AWS Well-Architected a détecté des problèmes à risque élevé pendant l'évaluation de votre charge de travail. Ces problèmes offrent la possibilité de réduire les risques et d'économiser de l'argent. Connectez-vous à l'outil AWS Well-Architected afin de passer en revue vos réponses et d'intervenir pour résoudre vos problèmes actifs.

Colonnes du rapport

- Statut
- Région
- ARN de la charge de travail
- Nom de la charge de travail

- Nom de l'évaluateur
- Type de charge de travail
- Date de début de la charge de travail
- Date de la dernière modification de la charge de travail
- Nombre de problèmes à haut risque identifiés pour l'Efficacité des performances
- Nombre de problèmes à haut risque résolus pour l'Efficacité des performances
- Nombre de questions ayant reçu une réponse pour l'Efficacité des performances
- Nombre total de questions dans le pilier Efficacité des performances
- Heure de la dernière modification

CloudFront Noms de domaine alternatifs

Description

Vérifie les CloudFront distributions Amazon pour détecter les noms de domaine alternatifs (CNAMES) dont les paramètres DNS sont mal configurés.

Si une CloudFront distribution inclut des noms de domaine alternatifs, la configuration DNS des domaines doit acheminer les requêtes DNS vers cette distribution.

> **Note**
>
> Cette vérification suppose que le DNS d'Amazon Route 53 et CloudFront la distribution Amazon sont configurés de la même manièreCompte AWS. En tant que telle, la liste d'alertes peut inclure des ressources qui peuvent aussi fonctionner comme prévu en raison de la configuration DNS en dehors de ce Compte AWS.

ID de la vérification

`N420c450f2`

Critères d'alerte

- Jaune : une CloudFront distribution inclut des noms de domaine alternatifs, mais la configuration DNS n'est pas correctement configurée avec un enregistrement CNAME ou un enregistrement de ressource d'alias Amazon Route 53.

- Jaune : une CloudFront distribution inclut des noms de domaine alternatifs, mais n'a pas Trusted Advisor pu évaluer la configuration DNS en raison du trop grand nombre de redirections.
- Jaune : une CloudFront distribution inclut des noms de domaine alternatifs, mais n'Trusted Advisora pas pu évaluer la configuration DNS pour une autre raison, probablement en raison d'un délai d'attente.

Action recommandée

Mettez à jour la configuration DNS pour acheminer les requêtes DNS vers la distribution CloudFront. Voir Utilisation de noms de domaines alternatifs (CNAME).

Si vous utilisez Amazon Route 53 comme service DNS, consultez Routage du trafic vers une distribution CloudFront Web Amazon à l'aide de votre nom de domaine. Si le délai de vérification a expiré, essayez d'actualiser la vérification.

Ressources supplémentaires

Guide CloudFront du développeur Amazon

Colonnes du rapport

- Statut
- ID de distribution
- Nom du domaine de distribution
- Nom du domaine alternatif
- Raison

CloudFront Optimisation de la diffusion de contenu

Description

Vérifie les cas dans lesquels le transfert de données depuis les compartiments Amazon Simple Storage Service (Amazon S3) pourrait être accéléré en utilisant CloudFront Amazon, AWS le service mondial de diffusion de contenu.

Lorsque vous configurez CloudFront la diffusion de votre contenu, les demandes relatives à votre contenu sont automatiquement acheminées vers l'emplacement périphérique le plus proche où le contenu est mis en cache. Ce routage permet de diffuser du contenu à vos utilisateurs avec les meilleures performances possibles. Un ratio élevé de données transférées par rapport aux

données stockées dans le compartiment indique que vous pourriez bénéficier de l'utilisation d'Amazon CloudFront pour fournir les données.

ID de la vérification

`796d6f3D83`

Critères d'alerte

- Jaune : la quantité de données transférées hors du compartiment à vos utilisateurs par les requêtes GET au cours des 30 jours précédant la vérification est au moins 25 fois supérieure à la quantité moyenne de données stockées dans le compartiment.
- Rouge : la quantité de données transférées hors du compartiment à vos utilisateurs par les requêtes GET au cours des 30 jours précédant la vérification atteint au moins 10 To et est au moins 25 fois supérieure à la quantité moyenne de données stockées dans le compartiment.

Action recommandée

Envisagez de l'utiliser CloudFront pour de meilleures performances. Consultez les détails CloudFront du produit Amazon.

Si les données transférées sont supérieures ou égales à 10 To par mois, consultez CloudFront les tarifs Amazon pour découvrir les économies possibles.

Ressources supplémentaires

- Guide CloudFront du développeur Amazon
- Étude de cas AWS : PBS

Colonnes du rapport

- Statut
- Région
- Nom du compartiment
- Stockage S3 (Go)
- Transfert de données en sortie (Go)
- Rapport entre transfert et stockage

CloudFront Transfert d'en-têtes et taux de réussite du cache

Description

Vérifie les en-têtes de requête HTTP CloudFront actuellement reçus du client et les transmet à votre serveur d'origine.

Certains en-têtes, tels que date ou user-agent, réduisent considérablement le taux de réussite du cache (la proportion de demandes traitées à partir d'un cache CloudFront périphérique). Cela augmente la charge sur votre origine et réduit les performances, car vous CloudFront devez transmettre davantage de demandes à votre origine.

ID de la vérification

`N415c450f2`

Critères d'alerte

Jaune : un ou plusieurs en-têtes de requête renvoyés CloudFront vers votre source peuvent réduire considérablement le taux de réussite de votre cache.

Action recommandée

Déterminez si les en-têtes de requête offrent suffisamment d'avantages pour justifier l'impact négatif sur le taux d'accès au cache. Si votre origine renvoie le même objet quelle que soit la valeur d'un en-tête donné, nous vous recommandons de ne pas configurer CloudFront pour transférer cet en-tête vers l'origine. Pour plus d'informations, consultez la section Configuration de la mise CloudFront en cache des objets en fonction des en-têtes de demande.

Ressources supplémentaires

- Augmenter la proportion de demandes servies à partir des caches périphériques CloudFront
- CloudFront Rapports de statistiques sur le cache
- En-têtes et CloudFront comportement des requêtes HTTP

Colonnes du rapport

- ID de distribution
- Nom du domaine de distribution
- Modèle de chemin de comportement du cache
- En-têtes

Instances Amazon EC2 surexploitées

Description

Vérifie les instances Amazon Elastic Compute Cloud (Amazon EC2) exécutées à tout moment au cours des 14 derniers jours. Une alerte est envoyée si l'utilisation quotidienne du processeur était supérieure à 90 % sur quatre jours ou plus.

Une utilisation élevée et constante peut indiquer des performances optimisées et stables. Cependant, il peut également indiquer qu'une application ne dispose pas de ressources suffisantes. Pour obtenir les données d'utilisation quotidienne du processeur, téléchargez le rapport pour cette vérification.

ID de la vérification

`ZRxQlPsb6c`

Critères d'alerte

Jaune : une instance a affiché plus de 90 % d'utilisation moyenne quotidienne du processeur pendant au moins 4 jours au cours des 14 derniers jours.

Action recommandée

Pensez à ajouter d'autres instances. Pour plus d'informations sur la mise à l'échelle du nombre d'instances en fonction de la demande, consultez Qu'est-ce qu'Amazon EC2 Auto Scaling ?

Ressources supplémentaires

- Surveiller Amazon EC2
- Métadonnées d'instance et données utilisateur
- Guide de CloudWatch l'utilisateur Amazon
- Guide de l'utilisateur Amazon EC2 Auto Scaling

Colonnes du rapport

- Région/zone de disponibilité
- ID d’instance
- Type d'instance
- Nom de l'instance
- Utilisation moyenne du processeur sur 14 jours
- Nombre de jours d'utilisation du processeur supérieure à 90 %

Grand nombre de règles de groupe de sécurité EC2 appliquées à une instance

Description

Vérifie les instances Amazon Elastic Compute Cloud (Amazon EC2) comportant un grand nombre de règles de groupe de sécurité. Les performances peuvent être dégradées si une instance a un grand nombre de règles.

ID de la vérification

`j3DFqYTe29`

Critères d'alerte

- Jaune : une instance Amazon EC2-VPC possède plus de 50 règles de groupe de sécurité.
- Jaune : une instance Amazon EC2-Classic possède plus de 100 règles de groupe de sécurité.

Action recommandée

Réduisez le nombre de règles associées à une instance en supprimant les règles inutiles ou qui se chevauchent. Pour de plus amples informations, veuillez consulter Supprimer des règles d'un groupe de sécurité.

Ressources supplémentaires

Groupes de sécurité Amazon EC2

Colonnes du rapport

- Région
- ID d’instance
- Nom de l'instance
- ID du VPC
- Règles entrantes totales
- Règles sortantes totales

Grand nombre de règles dans un groupe de sécurité EC2

Description

Vérifie les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2) avec un grand nombre de règles de groupe de sécurité.

Si un groupe de sécurité a un grand nombre de règles, les performances peuvent être dégradées.

ID de la vérification

`tfg86AVHAZ`

Critères d'alerte

- Jaune : un groupe de sécurité Amazon EC2-VPC possède plus de 50 règles.
- Jaune : un groupe de sécurité Amazon EC2-Classic possède plus de 100 règles.

Action recommandée

Réduisez le nombre de règles dans un groupe de sécurité en supprimant les règles inutiles ou qui se chevauchent. Pour de plus amples informations, veuillez consulter Supprimer des règles d'un groupe de sécurité.

Ressources supplémentaires

Groupes de sécurité Amazon EC2

Colonnes du rapport

- Région
- Nom du groupe de sécurité
- ID du groupe
- Description
- Nombre d'instances
- ID du VPC
- Règles entrantes totales
- Règles sortantes totales

Volumes magnétiques Amazon EBS surutilisés

Description

Vérifie les volumes magnétiques Amazon Elastic Block Store (Amazon EBS) qui sont potentiellement surutilisés et qui pourraient bénéficier d'une configuration plus efficace.

Un volume magnétique est conçu pour les applications avec des exigences d'entrée/sortie (E/S) modérées ou en rafale et le taux d'IOPS n'est pas garanti. Il fournit environ 100 IOPS en moyenne, avec la possibilité d'atteindre plusieurs centaines d'IOPS. Pour des IOPS plus élevées

plus régulièrement, vous pouvez utiliser un volume d'IOPS provisionnés (SSD). Pour les IOPS en paquets, vous pouvez utiliser un volume polyvalent (SSD). Pour de plus amples informations, veuillez consulter Types de volume Amazon EBS.

Pour obtenir la liste des types d'instances qui prennent en charge un comportement optimisé pour EBS, consultez Instances optimisées pour Amazon EBS.

Pour obtenir des métriques d'utilisation quotidienne, téléchargez le rapport pour cette vérification. Le rapport détaillé contient une colonne pour chacun des 14 derniers jours. S'il n'y a aucun volume EBS actif, la cellule est vide. Si les données sont insuffisantes pour effectuer une mesure fiable, la cellule contient `N/A`. Si les données sont suffisantes, la cellule contient la médiane quotidienne et le pourcentage de la variance par rapport à la médiane (par exemple, `256 / 20%`).

ID de la vérification

`k3J2hns32g`

Critères d'alerte

Jaune : un volume Amazon EBS Magnetic est attaché à une instance qui peut être optimisée pour EBS ou qui fait partie d'un réseau de calcul de cluster avec une médiane quotidienne de plus de 95 IOPS, et varie de moins de 10 % de la valeur médiane pendant au moins 7 des 14 derniers jours.

Action recommandée

Pour des IOPS plus élevées plus régulièrement, vous pouvez utiliser un volume d'IOPS provisionnés (SSD). Pour les IOPS en paquets, vous pouvez utiliser un volume polyvalent (SSD). Pour de plus amples informations, veuillez consulter Types de volume Amazon EBS.

Ressources supplémentaires

Amazon Elastic Block Store (Amazon EBS)

Colonnes du rapport

- Statut
- Région
- ID du volume
- Nom du volume
- Nombre de jours écoulés
- Médiane quotidienne maximale

> **Note**
>
> Si vous avez inscrit votre compte à AWS Compute Optimizer, nous vous recommandons d'utiliser plutôt le contrôle des volumes sous-provisionnés Amazon EBS. Pour plus d'informations, consultez Inscription à AWS Compute Optimizer pour les vérifications de Trusted Advisor.

Sécurité

Vous pouvez utiliser les vérifications suivantes pour la catégorie de sécurité.

> **Note**
>
> Si vous avez activé Security Hub pour votre Compte AWS, vous pouvez consulter vos résultats dans la Trusted Advisor console. Pour plus d'informations, consultez Affichage des contrôles AWS Security Hub dans AWS Trusted Advisor.
> Vous pouvez consulter tous les contrôles dans la norme de sécurité AWS Foundational Security Best Practices, à l'exception des contrôles dont la catégorie est : Restaurer > Résilience. Pour obtenir la liste des contrôles pris en charge, consultez les contrôles des Bonnes pratiques de sécurité de base de AWS dans le Guide de l'utilisateur de AWS Security Hub .

Noms des vérifications

- Période de conservation d'Amazon CloudWatch Log Group
- Instances Amazon EC2 avec fin de support de Microsoft SQL Server
- Instances Amazon EC2 avec fin de support de Microsoft Windows Server
- Fin de la prise en charge standard des instances Amazon EC2 avec Ubuntu LTS
- Les clients Amazon EFS n'utilisent pas data-in-transit le chiffrement
- Instantanés publics Amazon EBS
- Le chiffrement du stockage Amazon RDS Aurora est désactivé
- La mise à niveau de la version mineure du moteur Amazon RDS est requise
- Instantanés publics Amazon RDS
- Risque lié à l'accès aux groupes de sécurité Amazon RDS

- Le chiffrement du stockage Amazon RDS est désactivé
- Amazon Route 53 : enregistrements CNAME non concordants pointant directement vers des compartiments S3
- Jeux d'enregistrements de ressource MX Amazon Route 53 et cadre de politique de l'expéditeur
- Autorisations pour le compartiment Amazon S3
- Connexions d'appairage Amazon VPC avec résolution DNS désactivée
- AWS Backup Vault sans politique basée sur les ressources pour empêcher la suppression de points de restauration
- AWS CloudTrail Journalisation
- AWS Lambda Fonctions utilisant des environnements d'exécution obsolètes
- Problèmes à risque élevé AWS Well-Architected pour la sécurité
- CloudFrontCertificats SSL personnalisés dans le magasin de certificats IAM
- CloudFront Certificat SSL sur le serveur d'origine
- Sécurité des écouteurs ELB
- Groupes de sécurité ELB
- Exposed Access Keys
- Rotation des clés d'accès IAM
- Politique de mot de passe IAM
- Utilisation d'IAM
- MFA sur le compte racine
- Groupes de sécurité — Ports spécifiques non restreints
- Groupes de sécurité — Accès illimité

Période de conservation d'Amazon CloudWatch Log Group

Description

Vérifie si la période de conservation des groupes de CloudWatch journaux Amazon est définie sur 365 jours ou sur un autre nombre spécifié.

Par défaut, les journaux sont conservés indéfiniment et n'expirent jamais. Cependant, vous pouvez ajuster la politique de conservation pour chaque groupe de journaux afin de vous conformer aux réglementations du secteur ou aux exigences légales pour une période spécifique.

Vous pouvez spécifier la durée de rétention minimale et les noms des groupes de journaux à l'aide LogGroupNamesdes MinRetentionTimeparamètres et de vos AWS Config règles.

> **Note**
>
> Les résultats de cette vérification sont automatiquement actualisés plusieurs fois par jour et les demandes d'actualisation ne sont pas autorisées. Plusieurs heures peuvent encore être nécessaires pour que les modifications apparaissent. Actuellement, vous ne pouvez pas exclure des ressources de cette vérification.

ID de la vérification

`c18d2gz186`

Source

`AWS Config Managed Rule: cw-loggroup-retention-period-check`

Critères d'alerte

Jaune : la durée de conservation d'un groupe de CloudWatch logs Amazon est inférieure au nombre minimum de jours souhaité.

Action recommandée

Configurez une période de conservation de plus de 365 jours pour vos données de journal stockées dans Amazon CloudWatch Logs afin de répondre aux exigences de conformité.

Pour plus d'informations, voir Conservation des données du journal des modifications dans CloudWatch les journaux.

Ressources supplémentaires

Modification de la conservation des CloudWatch journaux

Colonnes du rapport

- Statut
- Région
- Ressource
- AWS Config Règle
- Paramètres d'entrée

- Heure de la dernière modification

Instances Amazon EC2 avec fin de support de Microsoft SQL Server

Description

Vérifiez les versions de SQL Server pour les instances Amazon Elastic Compute Cloud (Amazon EC2) exécutées au cours des dernières 24 heures. Cette vérification vous avertit si les versions sont proches de la fin de support ou l'ont atteint. Chaque version de SQL Server offre 10 ans de support, dont 5 ans de support standard et 5 ans de support étendu. À la fin du support, la version de SQL Server ne recevra plus de mises à jour de sécurité régulières. L'exécution d'applications à l'aide de versions de SQL Server non prises en charge peut entraîner des risques de sécurité ou de conformité.

> **Note**
>
> Les résultats de cette vérification sont automatiquement actualisés plusieurs fois par jour et les demandes d'actualisation ne sont pas autorisées. Plusieurs heures peuvent encore être nécessaires pour que les modifications apparaissent. Actuellement, vous ne pouvez pas exclure des ressources de cette vérification.

ID de la vérification

`Qsdfp3A4L3`

Critères d'alerte

- Rouge : une instance EC2 possède une version SQL Server qui n'est plus prise en charge.
- Jaune : une instance EC2 possède une version SQL Server qui ne sera plus prise en charge dans 12 mois.

Action recommandée

Pour moderniser vos charges de travail SQL Server, envisagez de refactoriser vers des bases de données AWS Cloud natives comme Amazon Aurora. Pour plus d'informations, voir Moderniser les charges de travail Windows avec AWS.

Pour passer à une base de données entièrement gérée, envisagez de passer à Amazon Relational Database Service (Amazon RDS). Pour plus d'informations, consultez Amazon RDS for SQL Server.

Pour mettre à niveau votre SQL Server sur Amazon EC2, pensez à utiliser le Runbook Automation afin de simplifier votre mise à niveau. Pour en savoir plus, consultez la documentation AWS Systems Manager.

Si vous ne pouvez pas mettre à niveau votre SQL Server sur Amazon EC2, pensez au Programme de migration pour fin du support dédié à Windows Server. Pour plus d'informations, consultez le site web EMP.

Ressources supplémentaires

- Préparez-vous à la fin du support de SQL Server avec AWS
- Microsoft SQL Server sur AWS

Colonnes du rapport

- Statut
- Région
- ID d’instance
- SQL Server Version
- Cycle de prise en charge
- Fin de la prise en charge
- Heure de la dernière modification

Instances Amazon EC2 avec fin de support de Microsoft Windows Server

Description

Cette vérification vous avertit si les versions sont proches de la fin de support ou l'ont atteint. Chaque version de Windows Server offre 10 ans de support. Cela comprend 5 ans de support standard et 5 ans de support étendu. À la fin du support, la version de Windows Server ne recevra plus de mises à jour de sécurité régulières. Si vous exécutez des applications avec des versions de Windows Server non prises en charge, vous risquez de compromettre la sécurité ou la conformité de ces applications.

> **Note**
>
> Les résultats de cette vérification sont automatiquement actualisés plusieurs fois par jour et les demandes d'actualisation ne sont pas autorisées. Plusieurs heures peuvent encore

être nécessaires pour que les modifications apparaissent. Actuellement, vous ne pouvez pas exclure des ressources de cette vérification.

ID de la vérification

`Qsdfp3A4L4`

Critères d'alerte

- Rouge : une instance EC2 a une version de Windows Server qui a atteint la fin du support (Windows Server 2003, 2003 R2, 2008 et 2008 R2).
- Jaune : une instance EC2 a une version de Windows Server qui atteindra la fin de son support dans moins de 18 mois (Windows Server 2012 et 2012 R2).

Action recommandée

Pour moderniser vos charges de travail Windows Server, considérez les différentes options disponibles sur Moderniser les charges de travail Windows avec. AWS

Pour mettre à niveau vos charges de travail Windows Server afin qu'elles s'exécutent sur des versions plus récentes de Windows Server, vous pouvez utiliser un runbook d'automatisation. Pour plus d'informations, consultez la documentation d'AWS Systems Manager.

Veuillez suivre les étapes ci-dessous :

- a. Mettre à niveau la version de Windows Server
- b. Arrêt et démarrage difficiles lors de la mise à niveau
- c. Si vous utilisez EC2Config, veuillez migrer vers EC2Launch

Colonnes du rapport

- Statut
- Région
- ID d’instance
- Version de Windows Server
- Cycle de prise en charge
- Fin de la prise en charge
- Heure de la dernière modification

Fin de la prise en charge standard des instances Amazon EC2 avec Ubuntu LTS

Description

Cette vérification vous avertit si les versions sont proches ou ont atteint la fin du support standard. Il est important de passer à l'action, soit en migrant vers le prochain LTS, soit en passant à Ubuntu Pro. Après la fin du support, vos machines 18.04 LTS ne recevront aucune mise à jour de sécurité. Avec un abonnement Ubuntu Pro, votre déploiement Ubuntu 18.04 LTS peut bénéficier d'une maintenance de sécurité étendue (ESM) jusqu'en 2028. Les failles de sécurité non corrigées exposent vos systèmes aux pirates informatiques et à la possibilité d'une violation majeure.

ID de la vérification

`c1dfprch15`

Critères d'alerte

Rouge : une instance Amazon EC2 possède une version d'Ubuntu qui a atteint la fin du support standard (Ubuntu 18.04 LTS, 18.04.1 LTS, 18.04.2 LTS, 18.04.3 LTS, 18.04.4 LTS, 18.04.5 LTS et 18.04.6 LTS).

Jaune : une instance Amazon EC2 possède une version Ubuntu dont le support standard expirera dans moins de 6 mois (Ubuntu 20.04 LTS, 20.04.1 LTS, 20.04.2 LTS, 20.04.3 LTS, 20.04.4 LTS, 20.04.5 LTS et 20.04.6 LTS).

Vert : toutes les instances Amazon EC2 sont conformes.

Action recommandée

Pour mettre à niveau les instances d'Ubuntu 18.04 LTS vers une version LTS prise en charge, veuillez suivre les étapes mentionnées dans cet article. Pour mettre à niveau les instances d'Ubuntu 18.04 LTS vers Ubuntu Pro, rendez-vous sur AWS License Manager la console et suivez les étapes indiquées dans le guide de l'AWS License Manager utilisateur. Vous pouvez également consulter le blog Ubuntu présentant une démonstration étape par étape de la mise à niveau d'instances Ubuntu vers Ubuntu Pro.

Ressources supplémentaires

Pour plus d'informations sur les prix, contactez AWS Support.

Colonnes du rapport

- Statut

- Région
- Version Ubuntu Lts
- Date de fin de support prévue
- ID d’instance
- Cycle de prise en charge
- Heure de la dernière modification

Les clients Amazon EFS n'utilisent pas data-in-transit le chiffrement

Description

Vérifie si le système de fichiers Amazon EFS est monté par data-in-transit chiffrement. AWS recommande aux clients d'utiliser data-in-transit le chiffrement pour tous les flux de données afin de protéger les données contre toute exposition accidentelle ou tout accès non autorisé. Amazon EFS recommande aux clients d'utiliser le paramètre de montage « -o tls » à l'aide de l'assistant de montage Amazon EFS pour chiffrer les données en transit à l'aide du protocole TLS v1.2.

ID de la vérification

`c1dfpnchv1`

Critères d'alerte

Jaune : un ou plusieurs clients NFS de votre système de fichiers Amazon EFS n'utilisent pas les paramètres de montage recommandés pour le data-in-transit chiffrement.

Vert : tous les clients NFS de votre système de fichiers Amazon EFS utilisent les paramètres de montage recommandés pour le data-in-transit chiffrement.

Action recommandée

Pour tirer parti de la fonctionnalité de data-in-transit chiffrement d'Amazon EFS, nous vous recommandons de remonter votre système de fichiers à l'aide de l'assistant de montage Amazon EFS et des paramètres de montage recommandés.

> **Note**
>
> Certaines distributions de Linux n'incluent pas de version de Stunnel prenant en charge les fonctionnalités TLS par défaut. Si vous utilisez une distribution Linux non prise en

charge (voir les distributions prises en charge ici), nous vous recommandons de la mettre à niveau avant le remontage avec le paramètre de montage recommandé.

Ressources supplémentaires

- Chiffrement des données en transit

Colonnes du rapport

- Statut
- Région
- Identifiant de système de fichiers EFS
- AS avec connexions non chiffrées
- Heure de la dernière modification

Instantanés publics Amazon EBS

Description

Vérifie les paramètres d'autorisation pour les instantanés de vos volumes Amazon Elastic Block Store (Amazon EBS) et vous avertit si des instantanés sont accessibles au public.

Lorsque vous publiez un instantané, vous permettez à tous Comptes AWS et aux utilisateurs d'accéder à toutes les données qu'il contient. Si vous souhaitez partager un instantané uniquement avec des utilisateurs ou des comptes spécifiques, marquez l'instantané comme privé. Ensuite, spécifiez l'utilisateur ou les comptes avec lesquels vous souhaitez partager les données d'instantané. Notez que si vous avez activé l'option Bloquer l'accès public en mode « bloquer tout partage », vos instantanés publics ne seront pas accessibles au public et n'apparaîtront pas dans les résultats de cette vérification.

> **Note**
>
> Les résultats de cette vérification sont automatiquement actualisés plusieurs fois par jour et les demandes d'actualisation ne sont pas autorisées. Plusieurs heures peuvent encore être nécessaires pour que les modifications apparaissent.

ID de la vérification

`ePs02jT06w`

Critères d'alerte

Rouge : l'instantané du volume EBS est accessible au public.

Action recommandée

À moins que vous ne soyez certain de vouloir partager toutes les données de l'instantané avec tous Comptes AWS les utilisateurs, modifiez les autorisations : marquez l'instantané comme privé, puis spécifiez les comptes auxquels vous souhaitez accorder des autorisations. Pour plus d'informations, consultez Partager un instantané Amazon EBS. Utilisez Bloquer l'accès public pour les instantanés EBS afin de contrôler les paramètres qui autorisent l'accès public à vos données. Cette vérification ne peut pas être exclue de la vue dans la Trusted Advisor console.

Pour modifier directement les autorisations associées à vos instantanés, vous pouvez utiliser un runbook dans la AWS Systems Manager console. Pour plus d'informations, consultez `AWSSupport-ModifyEBSSnapshotPermission`.

Ressources supplémentaires

Instantanés Amazon EBS

Colonnes du rapport

- Statut
- Région
- ID du volume
- ID de l'instantané
- Description

Le chiffrement du stockage Amazon RDS Aurora est désactivé

Description

Amazon RDS prend en charge le chiffrement au repos pour tous les moteurs de base de données à l'aide des clés que vous gérez. AWS Key Management Service Sur une instance de base de données active avec chiffrement Amazon RDS, les données stockées au repos dans le stockage sont chiffrées, comme dans le cas des sauvegardes automatisées, des répliques de lecture et des instantanés.

Si le chiffrement n'est pas activé lors de la création d'un cluster de base de données Aurora, vous devez restaurer un instantané déchiffré sur un cluster de base de données chiffré.

> **Note**
>
> Les résultats de cette vérification sont automatiquement actualisés plusieurs fois par jour et les demandes d'actualisation ne sont pas autorisées. Plusieurs heures peuvent encore être nécessaires pour que les modifications apparaissent. Actuellement, vous ne pouvez pas exclure des ressources de cette vérification.

> **Note**
>
> Lorsqu'une instance ou un cluster de bases de données est arrêté, vous pouvez consulter les recommandations Amazon RDS Trusted Advisor pendant 3 à 5 jours. Après cinq jours, les recommandations ne sont plus disponibles dans Trusted Advisor. Pour consulter les recommandations, ouvrez la console Amazon RDS, puis choisissez Recommendations. Si vous supprimez une instance ou un cluster de bases de données, les recommandations associées à ces instances ou clusters ne sont pas disponibles dans Trusted Advisor ou dans la console de gestion Amazon RDS.

ID de la vérification

`c1qf5bt005`

Critères d'alerte

Rouge : le chiffrement n'est pas activé sur les ressources Amazon RDS Aurora.

Action recommandée

Activez le chiffrement des données au repos pour votre cluster de bases de données.

Ressources supplémentaires

Vous pouvez activer le chiffrement lors de la création d'une instance de base de données ou utiliser une solution de contournement pour activer le chiffrement sur une instance de base de données active. Vous ne pouvez pas modifier un cluster de base de données déchiffré en cluster de base de données chiffré. Toutefois, vous pouvez restaurer un instantané déchiffré

sur un cluster de base de données chiffré. Lorsque vous effectuez une restauration à partir de l'instantané déchiffré, vous devez spécifier une clé. AWS KMS

Pour plus d'informations, consultez Chiffrer des ressources Amazon Aurora.

Colonnes du rapport

- Statut
- Région
- Ressource
- Nom du moteur
- Heure de la dernière modification

La mise à niveau de la version mineure du moteur Amazon RDS est requise

Description

Les ressources de votre base de données n'exécutent pas la dernière version mineure du moteur de base de données. La dernière version mineure contient les derniers correctifs de sécurité et d'autres améliorations.

> **Note**
>
> Les résultats de cette vérification sont automatiquement actualisés plusieurs fois par jour et les demandes d'actualisation ne sont pas autorisées. Plusieurs heures peuvent encore être nécessaires pour que les modifications apparaissent. Actuellement, vous ne pouvez pas exclure des ressources de cette vérification.

> **Note**
>
> Lorsqu'une instance ou un cluster de bases de données est arrêté, vous pouvez consulter les recommandations Amazon RDS Trusted Advisor pendant 3 à 5 jours. Après cinq jours, les recommandations ne sont plus disponibles dans Trusted Advisor. Pour consulter les recommandations, ouvrez la console Amazon RDS, puis choisissez Recommendations. Si vous supprimez une instance ou un cluster de bases de données, les recommandations associées à ces instances ou clusters ne sont pas disponibles dans Trusted Advisor ou dans la console de gestion Amazon RDS.

ID de la vérification

`c1qf5bt003`

Critères d'alerte

Rouge : les ressources Amazon RDS n'exécutent pas la dernière version mineure du moteur de base de données.

Action recommandée

Effectuez une mise à niveau vers la dernière version du moteur.

Ressources supplémentaires

Nous vous recommandons de maintenir votre base de données avec la dernière version mineure du moteur de base de données, car cette version inclut les derniers correctifs de sécurité et de fonctionnalité. Les mises à niveau des versions mineures du moteur de base de données contiennent uniquement les modifications rétrocompatibles avec les versions mineures antérieures de la même version majeure du moteur de base de données.

Pour plus d'informations, voir Mise à niveau de la version d'un moteur d'instance de base de données.

Colonnes du rapport

- Statut
- Région
- Ressource
- Nom du moteur
- Version actuelle du moteur
- Valeur recommandée
- Heure de la dernière modification

Instantanés publics Amazon RDS

Description

Vérifie les paramètres d'autorisation pour vos instantanés de base de données Amazon Relational Database Service (Amazon RDS) et vous avertit si des instantanés sont marqués comme publics.

Lorsque vous publiez un instantané, vous permettez à tous Comptes AWS et aux utilisateurs d'accéder à toutes les données qu'il contient. Si vous souhaitez partager un instantané uniquement avec des utilisateurs ou des comptes spécifiques, marquez l'instantané comme privé. Ensuite, spécifiez l'utilisateur ou les comptes avec lesquels vous souhaitez partager les données d'instantané.

> **Note**
>
> Les résultats de cette vérification sont automatiquement actualisés plusieurs fois par jour, et les requêtes d'actualisation ne sont pas autorisées. Plusieurs heures peuvent encore être nécessaires pour que les modifications apparaissent.

ID de la vérification

`rSs93HQwa1`

Critères d'alerte

Rouge : l'instantané Amazon RDS est marqué comme public.

Action recommandée

À moins que vous ne soyez certain de vouloir partager toutes les données de l'instantané avec tous Comptes AWS les utilisateurs, modifiez les autorisations : marquez l'instantané comme privé, puis spécifiez les comptes auxquels vous souhaitez accorder des autorisations. Pour plus d'informations, consultez Sharing a DB Snapshot or DB Cluster Snapshot (Partager un instantané de base de données ou un instantané de cluster de base de données). Cette vérification ne peut pas être exclue de la vue dans la Trusted Advisor console.

Pour modifier directement les autorisations associées à vos instantanés, vous pouvez utiliser un runbook dans la AWS Systems Manager console. Pour plus d'informations, consultez `AWSSupport-ModifyRDSSnapshotPermission`.

Ressources supplémentaires

Sauvegarde et restauration d'une instance de base de données Amazon RDS

Colonnes du rapport

- Statut
- Région
- ID de l'instance ou ID du cluster

- ID de l'instantané

Risque lié à l'accès aux groupes de sécurité Amazon RDS

Description

Vérifie les configurations des groupes de sécurité pour Amazon Relational Database Service (Amazon RDS) et avertit lorsqu'une règle de groupe de sécurité accorde un accès trop permissif à votre base de données. La configuration recommandée pour une règle de groupe de sécurité consiste à autoriser l'accès uniquement à partir de groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2) spécifiques ou à partir d'une adresse IP spécifique.

ID de la vérification

`nNauJisYIT`

Critères d'alerte

- Jaune : une règle de groupe de sécurité de base de données fait référence à un groupe de sécurité Amazon EC2 qui accorde un accès global sur l'un de ces ports : 20, 21, 22, 1433, 1434, 3306, 3389, 4333, 5432, 5500.
- Jaune : une règle de groupe de sécurité de base de données autorise l'accès à plusieurs adresses IP (le suffixe de la règle CIDR n'est pas /0 ou /32).
- Rouge : une règle de groupe de sécurité de base de données accorde un accès global (le suffixe de la règle CIDR est /0).

Action recommandée

Vérifiez les règles de votre groupe de sécurité et limitez l'accès aux adresses IP ou aux plages d'adresses IP autorisées. Pour modifier un groupe de sécurité, utilisez l'SecurityGroupIngressAPI AuthorizeDB ou le. AWS Management Console Pour plus d'informations, consultez Utilisation des groupes de sécurité DB.

Ressources supplémentaires

- Groupes de sécurité Amazon RDS
- Classless Inter-Domain Routing
- Liste des numéros de ports TCP et UDP

Colonnes du rapport

- Statut
- Région

- Nom du groupe de sécurité RDS
- Règle d'entrée
- Raison

Le chiffrement du stockage Amazon RDS est désactivé

Description

Amazon RDS prend en charge le chiffrement au repos pour tous les moteurs de base de données à l'aide des clés que vous gérez. AWS Key Management Service Sur une instance de base de données active avec chiffrement Amazon RDS, les données stockées au repos dans le stockage sont chiffrées, comme dans le cas des sauvegardes automatisées, des répliques de lecture et des instantanés.

Si le chiffrement n'est pas activé lors de la création d'une instance de base de données, vous devez restaurer une copie chiffrée de l'instantané déchiffré avant d'activer le chiffrement.

> **Note**
>
> Les résultats de cette vérification sont automatiquement actualisés plusieurs fois par jour et les demandes d'actualisation ne sont pas autorisées. Plusieurs heures peuvent encore être nécessaires pour que les modifications apparaissent. Actuellement, vous ne pouvez pas exclure des ressources de cette vérification.

> **Note**
>
> Lorsqu'une instance ou un cluster de bases de données est arrêté, vous pouvez consulter les recommandations Amazon RDS Trusted Advisor pendant 3 à 5 jours. Après cinq jours, les recommandations ne sont plus disponibles dans Trusted Advisor. Pour consulter les recommandations, ouvrez la console Amazon RDS, puis choisissez Recommendations. Si vous supprimez une instance ou un cluster de bases de données, les recommandations associées à ces instances ou clusters ne sont pas disponibles dans Trusted Advisor ou dans la console de gestion Amazon RDS.

ID de la vérification

`c1qf5bt006`

Critères d'alerte

Rouge : le chiffrement n'est pas activé sur les ressources Amazon RDS.

Action recommandée

Activez le chiffrement des données au repos pour votre instance de base de données.

Ressources supplémentaires

Vous pouvez chiffrer une instance de base de données uniquement lorsque vous créez l'instance de base de données. Pour chiffrer une instance de base de données active existante :

Créez une copie chiffrée de l'instance de base de données d'origine

1. Créez un instantané de votre instance de base de données.
2. Créez une copie cryptée de l'instantané créé à l'étape 1.
3. Restaurez une instance de base de données à partir du snapshot chiffré.

Pour plus d’informations, consultez les ressources suivantes :

- Chiffrement des ressources Amazon RDS
- Copier un instantané de base de données

Colonnes du rapport

- Statut
- Région
- Ressource
- Nom du moteur
- Heure de la dernière modification

Amazon Route 53 : enregistrements CNAME non concordants pointant directement vers des compartiments S3

Description

Vérifie les zones hébergées Amazon Route 53 avec des enregistrements CNAME pointant directement vers les noms d'hôtes des compartiments Amazon S3 et émet des alertes si votre CNAME ne correspond pas au nom de votre compartiment S3.

ID de la vérification

`c1ng44jvbm`

Critères d'alerte

Rouge : la zone hébergée Amazon Route 53 contient des enregistrements CNAME indiquant que les noms d'hôte des compartiments S3 ne correspondent pas.

Vert : aucun enregistrement CNAME non concordant n'a été trouvé dans votre zone hébergée Amazon Route 53.

Action recommandée

Lorsque vous pointez des enregistrements CNAME vers les noms d'hôte des compartiments S3, vous devez vous assurer qu'un compartiment correspondant existe pour tout enregistrement CNAME ou alias que vous configurez. Ce faisant, vous évitez le risque que vos enregistrements CNAME soient falsifiés. Vous empêchez également tout AWS utilisateur non autorisé d'héberger du contenu Web défectueux ou malveillant sur votre domaine.

Pour éviter de faire pointer les enregistrements CNAME directement vers les noms d'hôte des compartiments S3, pensez à utiliser le contrôle d'accès à l'origine (OAC) pour accéder aux ressources Web de vos compartiments S3 via Amazon. CloudFront

Pour plus d'informations sur l'association du CNAME au nom d'hôte d'un compartiment Amazon S3, consultez Personnalisation des URL Amazon S3 avec des enregistrements CNAME.

Ressources supplémentaires

- Comment associer un nom d'hôte à un compartiment Amazon S3
- Restreindre l'accès à une origine Amazon S3 avec CloudFront

Colonnes du rapport

- Statut

- ID de la zone hébergée
- Zone hébergée (ARN)
- Enregistrements CNAME correspondants
- Enregistrements CNAME non concordants
- Heure de la dernière modification

Jeux d'enregistrements de ressource MX Amazon Route 53 et cadre de politique de l'expéditeur

Description

Pour chaque jeu d'enregistrements de ressource MX, vérifie que le jeu d'enregistrements de ressource TXT ou SPF contient un enregistrement SPF valide. Le registre doit commencer par « `v=spf1` ». L'enregistrement SPF spécifie les serveurs autorisés à envoyer des e-mails pour votre domaine, ce qui permet de détecter et d'arrêter l'usurpation d'adresse e-mail et de diminuer le volume de courrier indésirable. Route 53 recommande d'utiliser un enregistrement TXT au lieu d'un enregistrement SPF. Trusted Advisor signale cette vérification en vert tant que chaque ensemble d'enregistrements de ressources MX contient au moins un enregistrement SPF ou TXT.

ID de la vérification

`c9D319e7sG`

Critères d'alerte

Jaune : un ensemble d'enregistrements de ressources MX ne possède pas d'enregistrement de ressources TXT ou SPF contenant une valeur SPF valide.

Action recommandée

Pour chaque ensemble d'enregistrements de ressources MX, créez un ensemble d'enregistrements de ressources TXT qui contient une valeur SPF valide. Pour de plus amples informations, veuillez consulter Sender Policy Framework: SPF Record Syntax (Sender Policy Framework : syntaxe de l'enregistrement SPF) et Création d'enregistrements à l'aide de la console Amazon Route 53.

Ressources supplémentaires

- Sender Policy Framework
- Enregistrement Mail eXchanger

Colonnes du rapport

- Nom de la zone hébergée
- ID de la zone hébergée
- Nom de l'ensemble d'enregistrements de ressources
- Statut

Autorisations pour le compartiment Amazon S3

Description

Vérifie les compartiments d'Amazon Simple Storage Service (Amazon S3) dotés d'autorisations d'accès ouvert ou autorisant l'accès à n'importe quel utilisateur authentifié. AWS

Cette vérification examine les autorisations de compartiment explicites, ainsi que les politiques de compartiment susceptibles de remplacer ces autorisations. L'octroi d'autorisations d'accès à la liste à tous les utilisateurs pour un compartiment Amazon S3 n'est pas recommandé. Ces autorisations peuvent mener des utilisateurs à répertorier des objets dans le compartiment à une fréquence élevée qui n'était pas prévue, pouvant alors entraîner des frais plus élevés qu'au départ. Les autorisations qui accordent l'accès au téléchargement et à la suppression à tout le monde peuvent générer des vulnérabilités de sécurité dans votre compartiment.

ID de la vérification

`Pfx0RwqBli`

Critères d'alerte

- Jaune : la liste ACL du compartiment autorise l'accès à la liste pour Tout le monde ou Tout utilisateur AWS authentifié.
- Jaune : une politique de compartiment autorise tout type d'accès ouvert.
- Jaune : la politique de compartiment contient des déclarations qui accordent un accès public. Le paramètre Block public and cross-account access to buckets that have public policies (Bloquer l'accès public et intercompte aux compartiments dotés de politiques publiques) est activé et limite l'accès aux seuls utilisateurs autorisés de ce compte jusqu'à ce que les déclarations d'accès public soient supprimées.
- Jaune : Trusted Advisor n'est pas autorisé à vérifier la politique, ou la politique n'a pas pu être évaluée pour d'autres raisons.

- Rouge : la liste ACL du compartiment autorise le chargement et la suppression pour Tout le monde ou Tout utilisateur AWS authentifié.

Action recommandée

Si un compartiment autorise l'accès ouvert, déterminez si ce dernier est réellement nécessaire. Si ce n'est pas le cas, mettez à jour les autorisations du compartiment pour limiter l'accès au propriétaire ou à des utilisateurs spécifiques. Utilisez le blocage de l'accès public Amazon S3 pour contrôler les paramètres qui autorisent l'accès public à vos données. Voir Setting Bucket and Object Access Permissions (Définition des autorisations d'accès aux compartiments et aux objets).

Ressources supplémentaires

Gestion des autorisations d'accès à vos ressources Amazon S3

Colonnes du rapport

- Statut
- Nom de la région
- Paramètres d'API de région
- Nom du compartiment
- Liste des autorisations ACL
- Autorisations de téléchargement/suppression ACL
- Accès aux autorisations de politique

Connexions d'appairage Amazon VPC avec résolution DNS désactivée

Description

Vérifie si la résolution DNS de vos connexions d'appairage de VPC est activée à la fois pour les VPC accepteurs et demandeurs.

La résolution DNS pour une connexion d'appairage de VPC permet la résolution des noms d'hôte DNS publics en adresses IPv4 privées lors de l'interrogation de votre VPC. Cela permet d'utiliser des noms DNS pour la communication entre les ressources dans les VPC appairés. La résolution DNS de vos connexions d'appairage de VPC simplifie le développement et la gestion des applications et réduit les risques d'erreur. Elle assure également la communication privée entre les ressources via la connexion d'appairage de VPC.

Vous pouvez spécifier les identifiants VPC à l'aide des paramètres vpCIDs de vos règles. AWS Config

Pour plus d'informations, consultez Activation de la résolution DNS pour une connexion d'appairage de VPC.

> **Note**
>
> Les résultats de cette vérification sont automatiquement actualisés plusieurs fois par jour et les demandes d'actualisation ne sont pas autorisées. Plusieurs heures peuvent encore être nécessaires pour que les modifications apparaissent. Actuellement, vous ne pouvez pas exclure des ressources de cette vérification.

ID de la vérification

`c18d2gz124`

Source

`AWS Config Managed Rule: vpc-peering-dns-resolution-check`

Critères d'alerte

Jaune : la résolution DNS n'est pas activée pour les VPC accepteurs et demandeurs dans le cadre d'une connexion d'appairage de VPC.

Action recommandée

Activez la résolution DNS pour vos connexions d'appairage de VPC.

Ressources supplémentaires

- Modification des options de connexion d'appairage de VPC
- Attributs DNS dans votre VPC

Colonnes du rapport

- Statut
- Région
- Ressource
- AWS Config Règle
- Paramètres d'entrée

- Heure de la dernière modification

AWS Backup Vault sans politique basée sur les ressources pour empêcher la suppression de points de restauration

Description

Vérifie si les AWS Backup coffres-forts sont associés à une politique basée sur les ressources qui empêche la suppression des points de récupération.

La politique basée sur les ressources empêche la suppression inattendue de points de reprise, ce qui vous permet d'appliquer le contrôle d'accès selon le principe du moindre privilège à vos données de sauvegarde.

Vous pouvez spécifier les AWS Identity and Access Management ARN que vous ne souhaitez pas que la règle consigne dans le principalArnListparamètre de vos AWS Config règles.

> **Note**
>
> Les résultats de cette vérification sont automatiquement actualisés plusieurs fois par jour et les demandes d'actualisation ne sont pas autorisées. Plusieurs heures peuvent encore être nécessaires pour que les modifications apparaissent. Actuellement, vous ne pouvez pas exclure des ressources de cette vérification.

ID de la vérification

`c18d2gz152`

Source

`AWS Config Managed Rule: backup-recovery-point-manual-deletion-disabled`

Critères d'alerte

Jaune : certains AWS Backup coffres-forts ne disposent pas d'une politique basée sur les ressources pour empêcher la suppression des points de récupération.

Action recommandée

Créez des politiques basées sur les ressources pour vos AWS Backup coffres-forts afin d'empêcher la suppression inattendue de points de récupération.

La politique doit inclure une déclaration « Deny » avec les PutBackupVaultAccessPolicy autorisations backup :UpdateRecoveryPointLifecycle, backup : et backup :. DeleteRecoveryPoint

Pour plus d'informations, voir Définition de politiques d'accès pour les coffres-forts de sauvegarde.

Colonnes du rapport

- Statut
- Région
- Ressource
- AWS Config Règle
- Paramètres d'entrée
- Heure de la dernière modification

AWS CloudTrail Journalisation

Description

Vérifie votre utilisation de AWS CloudTrail. CloudTrail fournit une visibilité accrue sur l'activité de votre compte en Compte AWS enregistrant des informations sur les appels d' AWS API effectués sur le compte. Vous pouvez utiliser ces journaux pour déterminer, par exemple, quelles actions un utilisateur particulier a effectuées au cours d'une période spécifiée ou quels utilisateurs ont effectué des actions sur une ressource particulière au cours d'une période spécifiée.

Étant donné CloudTrail que les fichiers journaux sont fournis à un compartiment Amazon Simple Storage Service (Amazon S3) CloudTrail , vous devez disposer d'autorisations d'écriture pour le compartiment. Si un journal d'activité s'applique à toutes les régions (valeur par défaut lors de la création d'un journal d'activité), le journal d'activité apparaît plusieurs fois dans le rapport Trusted Advisor .

ID de la vérification

`vjafUGJ9H0`

Critères d'alerte

- Jaune : CloudTrail signale les erreurs de livraison d'un journal pour un parcours.
- Rouge : aucun suivi n'a été créé pour une région, ou la journalisation est désactivée pour un suivi.

Action recommandée

Pour créer un suivi et démarrer la journalisation à partir de la console, accédez à la console AWS CloudTrail.

Pour démarrer la journalisation, veuillez consulter Stopping and Starting Logging for a Trail (Arrêter et démarrer la journalisation d'un suivi).

Si vous recevez des erreurs de livraison de journaux, assurez-vous que le compartiment existe et que la politique nécessaire y est attachée. Voir Politique de compartiment Amazon S3.

Ressources supplémentaires

- AWS CloudTrail Guide de l'utilisateur
- Régions prises en charge
- Services pris en charge

Colonnes du rapport

- Statut
- Région
- Nom du suivi
- Statut de la journalisation
- Nom du compartiment
- Date de la dernière livraison

AWS Lambda Fonctions utilisant des environnements d'exécution obsolètes

Description

Vérifie les fonctions Lambda dont la version $LATEST est configurée pour utiliser un environnement d'exécution proche de la dépréciation, ou qui est obsolète. Les environnements d'exécution obsolètes ne sont pas éligibles aux mises à jour de sécurité ou au support technique

> **Note**
>
> Les résultats de cette vérification sont automatiquement actualisés plusieurs fois par jour et les demandes d'actualisation ne sont pas autorisées. Plusieurs heures peuvent encore être nécessaires pour que les modifications apparaissent. Actuellement, vous ne pouvez pas exclure des ressources de cette vérification.

Les versions des fonctions Lambda publiées sont immuables, ce qui signifie qu'elles peuvent être invoquées, mais qu'elles ne peuvent pas être mises à jour. Seule la version `$LATEST` d'une fonction Lambda peut être mise à jour. Pour plus d'informations, consultez Versions de fonctions Lambda.

ID de la vérification

`L4dfs2Q4C5`

Critères d'alerte

- Rouge : La version $LATEST de la fonction est configurée pour utiliser un environnement d'exécution déjà obsolète.
- Jaune : La version $LATEST de la fonction s'exécute sur un environnement d'exécution qui sera obsolète dans les 180 jours.

Action recommandée

Si certaines fonctions s'exécutent sur un environnement d'exécution qui est sur le point de devenir obsolète, vous devez préparer la migration vers un environnement d'exécution pris en charge. Pour de plus amples informations, veuillez consulter Runtime support policy (Stratégie de prise en charge de l'environnement d'exécution).

Nous vous recommandons de supprimer les versions de fonctions antérieures que vous n'utilisez plus.

Ressources supplémentaires

Environnements d'exécution (runtimes) Lambda

Colonnes du rapport

- Statut
- Région
- ARN de la fonction
- Environnement d'exécution
- Jours avant l'obsolescence
- Date d'obsolescence
- Invocations quotidiennes moyennes
- Heure de la dernière modification

Problèmes à risque élevé AWS Well-Architected pour la sécurité

Description

Vérifiez les éventuels problèmes à risque élevé (HRI) pour vos charges de travail dans le pilier de sécurité. Cette vérification est basée sur vos commentaires AWS-Well Architected. Les résultats de la vérification varient selon que vous avez terminé ou non l'évaluation de la charge de travail avec AWS Well-Architected.

> **Note**
>
> Les résultats de cette vérification sont automatiquement actualisés plusieurs fois par jour et les demandes d'actualisation ne sont pas autorisées. Plusieurs heures peuvent encore être nécessaires pour que les modifications apparaissent. Actuellement, vous ne pouvez pas exclure des ressources de cette vérification.

ID de la vérification

`Wxdfp4B1L3`

Critères d'alerte

- Rouge : Au moins un problème actif à haut risque a été identifié dans le pilier de sécurité de AWS Well-Architected.
- Vert : aucun problème actif à haut risque n'a été détecté dans le pilier de sécurité de AWS Well-Architected.

Action recommandée

AWS Well-Architected a détecté des problèmes à haut risque lors de l'évaluation de votre charge de travail. Ces problèmes offrent la possibilité de réduire les risques et d'économiser de l'argent. Connectez-vous à l'outil AWS Well-Architected afin de passer en revue vos réponses et d'intervenir pour résoudre vos problèmes actifs.

Colonnes du rapport

- Statut
- Région
- ARN de la charge de travail
- Nom de la charge de travail

- Nom de l'évaluateur
- Type de charge de travail
- Date de début de la charge de travail
- Date de la dernière modification de la charge de travail
- Nombre de problèmes à haut rique identifiés pour la Sécurité
- Nombre de problèmes à haut risque résolus pour la Sécurité
- Nombre de questions de Sécurité
- Nombre total de questions dans le pilier Sécurité
- Heure de la dernière modification

CloudFrontCertificats SSL personnalisés dans le magasin de certificats IAM

Description

Vérifie les certificats SSL pour les noms de domaine CloudFront alternatifs dans le magasin de certificats IAM. Cette vérification vous avertit si un certificat a expiré, expirera bientôt, utilise un chiffrement obsolète ou n'est pas configuré correctement pour la distribution.

Lorsqu'un certificat personnalisé pour un autre nom de domaine expire, les navigateurs qui affichent votre CloudFront contenu peuvent afficher un message d'avertissement concernant la sécurité de votre site Web. Les certificats chiffrés à l'aide de l'algorithme de hachage SHA-1 sont obsolètes par les navigateurs web tels que Chrome et Firefox.

Un certificat doit contenir un nom de domaine correspondant au nom de domaine d'origine ou au nom de domaine dans l'en-tête hôte de la demande d'un utilisateur. S'il ne correspond pas, CloudFront renvoie un code d'état HTTP 502 (mauvaise passerelle) à l'utilisateur. Pour de plus amples informations, veuillez consulter Utilisation de noms de domaines alternatifs et de HTTPS.

ID de la vérification

`N425c450f2`

Critères d'alerte

- Rouge : un certificat SSL personnalisé a expiré.
- Jaune : un certificat SSL personnalisé expire dans les 7 prochains jours.
- Jaune : un certificat SSL personnalisé a été chiffré à l'aide de l'algorithme de hachage SHA-1.

- Jaune : un ou plusieurs noms de domaines alternatifs de la distribution n'apparaissent ni dans le champ Comme Name (Nom commun), ni dans le champ Subject Alternative Name (Nom Subject Alternative) du certificat SSL personnalisé.

Action recommandée

Renouvelez un certificat expiré ou sur le point d'expirer.

Remplacez un certificat qui a été chiffré à l'aide de l'algorithme de hachage SHA-1 par un certificat chiffré à l'aide de l'algorithme de hachage SHA-256.

Remplacez le certificat par un certificat qui contient les valeurs applicables dans les champs Common Name (Nom commun) ou Subject Alternative Domain Names (Noms Subject Alternative Domain).

Ressources supplémentaires

Utiliser une connexion HTTPS pour accéder à vos objets

Colonnes du rapport

- Statut
- ID de distribution
- Nom du domaine de distribution
- Nom du certificat
- Raison

CloudFront Certificat SSL sur le serveur d'origine

Description

Vérifie votre serveur d'origine pour les certificats SSL qui sont arrivés à expiration, sur le point d'expirer, manquants ou qui utilisent un chiffrement obsolète. Si un certificat présente l'un de ces problèmes, il CloudFront répond aux demandes concernant votre contenu avec le code d'état HTTP 502, Bad Gateway.

Les certificats chiffrés à l'aide de l'algorithme de hachage SHA-1 sont obsolètes dans des navigateurs web tels que Chrome et Firefox. En fonction du nombre de certificats SSL que vous avez associés à vos CloudFront distributions, ce chèque peut ajouter quelques centimes par mois à votre facture auprès de votre fournisseur d'hébergement Web, par exemple, AWS si vous utilisez Amazon EC2 ou Elastic Load Balancing comme origine de votre CloudFront

distribution. Cette vérification ne concerne pas votre chaîne de certificats d'origine ni les autorités de certification. Vous pouvez les vérifier dans votre CloudFront configuration.

ID de la vérification

N430c450f2

Critères d'alerte

- Rouge : un certificat SSL sur votre origine a expiré ou est manquant.
- Jaune : un certificat SSL sur votre origine expire dans les 30 prochains jours.
- Jaune : un certificat SSL sur votre origine a été chiffré à l'aide de l'algorithme de hachage SHA-1.
- Jaune : aucun certificat SSL sur votre origine n'a pu être localisé. La connexion a peut-être échoué en raison d'une expiration de délai ou d'autres problèmes de connexion HTTPS.

Action recommandée

Renouvelez le certificat de votre origine s'il a expiré ou est sur le point d'expirer.

Ajoutez un certificat s'il n'en existe pas.

Remplacez un certificat qui a été chiffré à l'aide de l'algorithme de hachage SHA-1 par un certificat chiffré à l'aide de l'algorithme de hachage SHA-256.

Ressources supplémentaires

Utiliser des noms de domaines alternatifs et HTTPS

Colonnes du rapport

- Statut
- ID de distribution
- Nom du domaine de distribution
- Origin
- Raison

Sécurité des écouteurs ELB

Description

Vérifie la présence d'équilibreurs de charge dotés d'écouteurs qui n'utilisent pas les configurations de sécurité recommandées pour les communications chiffrées. AWS recommande d'utiliser

un protocole sécurisé (HTTPS ou SSL), des politiques de up-to-date sécurité, ainsi que des chiffrements et des protocoles sécurisés.

Lorsque vous utilisez un protocole sécurisé pour une connexion frontale (client à équilibreur de charge), les demandes sont chiffrées entre vos clients et l'équilibreur de charge, créant ainsi un environnement plus sécurisé. Elastic Load Balancing fournit des politiques de sécurité prédéfinies avec des chiffrements et des protocoles conformes aux meilleures pratiques AWS de sécurité. De nouvelles versions de politiques prédéfinies sont publiées à mesure que de nouvelles configurations deviennent disponibles.

ID de la vérification

`a2sEc6ILx`

Critères d'alerte

- Jaune : un équilibreur de charge n'a aucun écouteur qui utilise un protocole sécurisé (HTTPS ou SSL).
- Jaune : un écouteur d'équilibreur de charge utilise une politique de sécurité SSL prédéfinie obsolète.
- Jaune : un écouteur d'équilibreur de charge utilise un chiffrement ou un protocole qui n'est pas recommandé.
- Rouge : un écouteur d'équilibreur de charge utilise un chiffrement ou un protocole non sécurisé.

Action recommandée

Si le trafic vers votre équilibreur de charge doit être sécurisé, utilisez le protocole HTTPS ou SSL pour la connexion frontale.

Mettez à niveau votre équilibreur de charge vers la dernière version de la politique de sécurité SSL prédéfinie.

Utilisez uniquement les chiffrements et protocoles recommandés.

Pour de plus amples informations, veuillez consulter Écouteurs de votre Classic Load Balancer.

Ressources supplémentaires

- Référence rapide des configurations d'écouteur
- Mettre à jour la configuration de négociation SSL de votre Classic Load Balancer
- Configurations de négociation SSL pour Classic Load Balancers
- Table des politiques de sécurité SSL

Colonnes du rapport

- Statut
- Région
- Nom de l'équilibreur de charge
- Port de l'équilibreur de charge
- Raison

Groupes de sécurité ELB

Description

Vérifie les équilibreurs de charge configurés avec un groupe de sécurité manquant ou un groupe de sécurité qui autorise l'accès aux ports non configurés pour l'équilibreur de charge.

Si un groupe de sécurité associé à un équilibreur de charge est supprimé, l'équilibreur de charge ne fonctionnera pas comme prévu. Si un groupe de sécurité autorise l'accès à des ports non configurés pour l'équilibreur de charge, le risque de perte de données ou d'attaques malveillantes augmente.

ID de la vérification

`xSqX82fQu`

Critères d'alerte

- Jaune : les règles entrantes d'un groupe de sécurité Amazon VPC associé à un équilibreur de charge autorisent l'accès à des ports qui ne sont pas définis dans la configuration de l'écouteur de l'équilibreur de charge.
- Rouge : aucun groupe de sécurité associé à un équilibreur de charge n'existe.

Action recommandée

Configurez les règles du groupe de sécurité pour limiter l'accès uniquement aux ports et protocoles définis dans la configuration de l'écouteur de l'équilibreur de charge, ainsi que le protocole ICMP pour prendre en charge la détection de la MTU du chemin. Voir Écouteurs de votre Classic Load Balancer et Groupes de sécurité pour les équilibreurs de charge dans un VPC.

Si un groupe de sécurité est manquant, appliquez-en un nouveau à l'équilibreur de charge. Créez des règles de groupe de sécurité qui limitent l'accès uniquement aux ports et protocoles définis dans la configuration de l'écouteur de l'équilibreur de charge. Voir Groupes de sécurité pour les équilibreurs de charge dans un VPC.

Ressources supplémentaires

- Guide de l'utilisateur Elastic Load Balancing
- Configurer votre Classic Load Balancer

Colonnes du rapport

- Statut
- Région
- Nom de l'équilibreur de charge
- ID de groupe de sécurité
- Raison

Exposed Access Keys

Description

Vérifie les référentiels de code populaires pour les clés d'accès ayant été exposées au public et pour l'utilisation irrégulière d'Amazon Elastic Compute Cloud (Amazon EC2) qui pourrait être le résultat d'une clé d'accès compromise.

La clé d'accès comprend un ID de clé d'accès et une clé d'accès secrète). Les clés d'accès exposées présentent un risque pour la sécurité de votre compte et d'autres utilisateurs, peuvent entraîner des frais excessifs relatifs aux activités non autorisées ou à des abus, et enfreindre le contrat du client AWS.

Si votre clé d'accès est exposée, prenez immédiatement des mesures pour sécuriser votre compte. Pour protéger votre compte contre les frais excessifs, AWS limitez temporairement votre capacité à créer certaines AWS ressources. Cela ne sécurise pas votre compte. Cette action ne limite que partiellement l'utilisation non autorisée susceptible d'être facturée.

> **Note**
>
> Cette vérification ne garantit pas l'identification des clés d'accès exposées ou des instances EC2 compromises. Vous êtes responsable en dernier ressort de la sûreté et de la sécurité de vos clés d'accès et de vos AWS ressources.
> Les résultats de cette vérification sont automatiquement actualisés, et les demandes d'actualisation ne sont pas autorisées. Actuellement, vous ne pouvez pas exclure des ressources de cette vérification.

Si une date limite est indiquée pour une clé d'accès, vous AWS pouvez la suspendre Compte AWS si l'utilisation non autorisée n'est pas arrêtée à cette date. Si vous pensez qu'il s'agit d'une erreur, contactez AWS Support.

Les informations affichées ne reflètent Trusted Advisor peut-être pas l'état le plus récent de votre compte. Aucune clé d'accès exposée n'est marquée comme résolue tant que toutes les clés d'accès exposées du compte n'ont pas été résolues. Cette synchronisation des données peut prendre jusqu'à une semaine.

ID de la vérification

`12Fnkpl8Y5`

Critères d'alerte

- Rouge : potentiellement compromis : AWS a identifié un identifiant de clé d'accès et une clé d'accès secrète correspondante qui ont été exposés sur Internet et pourraient avoir été compromis (utilisés).
- Rouge : exposé : AWS a identifié un identifiant de clé d'accès et la clé d'accès secrète correspondante qui ont été exposés sur Internet.
- Rouge : suspect – L'utilisation irrégulière d'Amazon EC2 indique qu'une clé d'accès a peut-être été compromise, mais qu'elle n'a pas été identifiée comme étant exposée sur Internet.

Action recommandée

Supprimez dès que possible la clé d'accès concernée. Si la clé est associée à un utilisateur IAM, consultez Gestion des clés d'accès pour les utilisateurs IAM.

Vérifiez si votre compte est utilisé sans autorisation. Connectez-vous à la AWS Management Console et vérifiez la présence de ressources suspectes dans chaque console de service. Portez une attention particulière à l'exécution des instances Amazon EC2, aux demandes d'instance Spot, aux clés d'accès et aux utilisateurs IAM. Vous pouvez également vérifier l'utilisation globale sur la console Billing and Cost Management.

Ressources supplémentaires

- Meilleures pratiques en matière de gestion des clés AWS d'accès
- AWS Directives relatives aux audits de sécurité

Colonnes du rapport

- ID de clé d'accès
- Nom d'utilisateur (IAM ou racine)

- Type de fraude
- ID du dossier
- Heure de mise à jour
- Emplacement
- Date limite
- Utilisation (USD par jour)

Rotation des clés d'accès IAM

Description

Vérifie les clés d'accès IAM actives qui n'ont pas fait l'objet d'une rotation au cours des 90 derniers jours.

Lorsque vous faites tourner régulièrement vos clés d'accès, vous réduisez les risques qu'une clé compromise puisse être utilisée à votre insu pour accéder aux ressources. Aux fins de cette vérification, la date et l'heure de la dernière rotation correspondent à la date à laquelle la clé d'accès a été créée ou activée pour la dernière fois. Le numéro et la date de la clé d'accès proviennent des informations sur `access_key_1_last_rotated` et `access_key_2_last_rotated`du rapport d'informations d'identification IAM le plus récent.

La fréquence de régénération d'un rapport d'informations d'identification étant limitée, l'actualisation de cette vérification peut ne pas refléter les modifications récentes. Pour plus d'informations, consultez Obtenir les rapports d'informations d'identification de votre Compte AWS.

Pour créer des clès d'accès et en effectuer une rotation, un utilisateur doit disposer des autorisations appropriées. Pour plus d'informations, consultez Allow Users to Manage Their Own Passwords, Access Keys, and SSH Keys (Autoriser les utilisateurs à gérer leurs propres mots de passe, clés d'accès et clés SSH).

ID de la vérification

`DqdJqYeRm5`

Critères d'alerte

- Vert : la clé d'accès est active et a fait l'objet d'une rotation au cours des 90 derniers jours.
- Jaune : la clé d'accès est active et a fait l'objet d'une rotation au cours des 2 dernières années, mais il y a plus de 90 jours.

- Rouge : la clé d'accès est active et a fait l'objet d'une rotation au cours des 2 dernières années.

Action recommandée

Effectuez une rotation des clés d'accès régulièrement. Voir Rotation des clés d'accès et Gestion des clés d'accès pour les utilisateurs IAM.

Ressources supplémentaires

- Bonnes pratiques IAM
- How to Rotate Access Keys for IAM Users (Comment effectuer une rotation des clés d'accès pour les utilisateurs IAM)

Colonnes du rapport

- Statut
- Utilisateur IAM
- Clé d'accès
- Dernière rotation de clé
- Raison

Politique de mot de passe IAM

Description

Vérifie la politique de mot de passe de votre compte et vous avertit lorsqu'une politique de mot de passe n'est pas activée ou si les exigences relatives au contenu du mot de passe n'ont pas été activées.

Les exigences en matière de contenu de mot de passe augmentent la sécurité globale de AWS en imposant la création de mots de passe utilisateur forts. Lorsque vous créez ou modifiez une politique de mot de passe, la modification est immédiatement appliquée aux nouveaux utilisateurs, mais n'oblige pas les utilisateurs existants à modifier leurs mots de passe.

ID de la vérification

`Yw2K9puPzl`

Critères d'alerte

- Jaune : une politique de mot de passe est activée, mais au moins une exigence de contenu n'est pas activée.
- Rouge : aucune politique de mot de passe n'est activée.

Action recommandée

Si certaines exigences de contenu ne sont pas activées, envisagez de les activer. Si aucune politique de mot de passe n'est activée, créez-en une et configurez-la. Voir Définition d'une politique de mot de passe du compte pour les utilisateurs IAM.

Ressources supplémentaires

Gestion des mots de passe

Colonnes du rapport

- Politique relative aux mots de passe
- Majuscule
- Minuscule
- Nombre
- Non alphanumérique

Utilisation d'IAM

Description

Vérifie votre utilisation d'IAM. Vous pouvez utiliser IAM pour créer des utilisateurs, des groupes et des rôles dans AWS. Vous pouvez également utiliser des autorisations pour contrôler l'accès aux ressources AWS . Cette vérification vise à décourager l'utilisation de l'accès à la racine en vérifiant l'existence d'au moins un utilisateur IAM. Vous pouvez ignorer l'alerte si vous suivez les bonnes pratiques de centralisation des identités et de configuration des utilisateurs dans un fournisseur d'identité externe ou AWS IAM Identity Center.

ID de la vérification

`zXCkfM1nI3`

Critères d'alerte

Jaune : aucun utilisateur IAM n'a été créé pour ce compte.

Action recommandée

Créez un utilisateur IAM ou utilisez-le AWS IAM Identity Center pour créer des utilisateurs supplémentaires dont les autorisations sont limitées pour effectuer des tâches spécifiques dans votre AWS environnement.

Ressources supplémentaires

- Qu'est-ce que c'est AWS IAM Identity Center ?
- En quoi consiste IAM ?

MFA sur le compte racine

Description

Vérifie le compte racine et avertit si l'authentification multi-facteur (MFA) n'est pas activée.

Pour une sécurité accrue, nous vous recommandons de protéger votre compte en utilisant l'authentification MFA, qui oblige l'utilisateur à saisir un code d'authentification unique provenant de son matériel MFA ou de son appareil virtuel lorsqu'il interagit avec les AWS Management Console sites Web associés.

ID de la vérification

`7DAFEmoDos`

Critères d'alerte

Rouge : l'authentification MFA n'est pas activée sur le compte racine.

Action recommandée

Connectez-vous à votre compte racine et activez un dispositif MFA. Voir Vérification du statut de l'authentification MFA et Activation des dispositifs MFA.

Ressources supplémentaires

Utilisation de dispositifs d'authentification multifactorielle (MFA) avec AWS

Groupes de sécurité — Ports spécifiques non restreints

Description

Vérifie les groupes de sécurité pour les règles qui autorisent l'accès illimité (0.0.0.0/0) à des ports spécifiques.

L'accès illimité augmente les risques d'activités malveillantes (piratage, denial-of-service attaques, perte de données). Les ports présentant le risque le plus élevé sont signalés en rouge, et ceux qui présentent moins de risques sont signalés en jaune. Les ports indiqués en vert sont généralement utilisés par les applications nécessitant un accès illimité, telles que HTTP et SMTP.

Si vous avez délibérément configuré vos groupes de sécurité de cette manière, nous vous recommandons d'utiliser des mesures de sécurité supplémentaires pour sécuriser votre infrastructure (telles que les tables IP).

> **Note**
>
> Cette vérification évalue uniquement les groupes de sécurité que vous créez et leurs règles entrantes pour les adresses IPv4. Les groupes de sécurité créés par AWS Directory Service sont indiqués en rouge ou jaune, mais ils ne présentent pas de risque de sécurité et peuvent être ignorés en toute sécurité ou exclus. Pour en savoir plus, consultez le FAQ Trusted Advisor.

> **Note**
>
> Cette vérification n'inclut pas le cas d'utilisation lorsqu'une liste de préfixes gérée par le client accorde l'accès à 0.0.0.0/0 et est utilisée comme source avec un groupe de sécurité.

ID de la vérification

`HCP4007jGY`

Critères d'alerte

- Vert : l'accès au port 80, 25, 443 ou 465 n'est pas restreint.
- Rouge : l'accès au port 20, 21, 1433, 1434, 3306, 3389, 4333, 5432 ou 5500 n'est pas restreint.
- Jaune : l'accès à tout autre port n'est pas restreint.

Action recommandée

Limitez l'accès uniquement aux adresses IP qui en ont besoin. Pour limiter l'accès à une adresse IP spécifique, définissez le suffixe sur /32 (par exemple, 192.0.2.10/32). Assurez-vous de supprimer les règles trop permissives après avoir créé des règles plus restrictives.

Ressources supplémentaires

- Groupes de sécurité Amazon EC2

  Liste des numéros de ports TCP et UDP
- Classless Inter-Domain Routing

Colonnes du rapport

- Statut
- Région
- Nom du groupe de sécurité
- ID du groupe de sécurité
- Protocole
- Port d'origine
- Port de destination

Groupes de sécurité — Accès illimité

Description

Vérifie les groupes de sécurité pour les règles qui autorisent un accès illimité à une ressource.

L'accès illimité augmente les risques d'activités malveillantes (piratage, denial-of-service attaques, perte de données).

> **Note**
>
> Cette vérification évalue uniquement les groupes de sécurité que vous créez et leurs règles entrantes pour les adresses IPv4. Les groupes de sécurité créés par AWS Directory Service sont indiqués en rouge ou jaune, mais ils ne présentent pas de risque de sécurité et peuvent être ignorés en toute sécurité ou exclus. Pour en savoir plus, consultez le FAQ Trusted Advisor.

> **Note**
>
> Cette vérification n'inclut pas le cas d'utilisation lorsqu'une liste de préfixes gérée par le client accorde l'accès à 0.0.0.0/0 et est utilisée comme source avec un groupe de sécurité.

ID de la vérification

`1iG5NDGVre`

Critères d'alerte

Rouge : une règle de groupe de sécurité possède une adresse IP source avec un suffixe /0 pour les ports autres que 25, 80 ou 443.

Action recommandée

Limitez l'accès uniquement aux adresses IP qui en ont besoin. Pour limiter l'accès à une adresse IP spécifique, définissez le suffixe sur /32 (par exemple, 192.0.2.10/32). Assurez-vous de supprimer les règles trop permissives après avoir créé des règles plus restrictives.

Ressources supplémentaires

- Groupes de sécurité Amazon EC2
- Classless Inter-Domain Routing

Colonnes du rapport

- Statut
- Région
- Nom du groupe de sécurité
- ID du groupe de sécurité
- Protocole
- Port d'origine
- Port de destination
- Plage IP

Tolérance aux pannes

Vous pouvez utiliser les vérifications suivantes pour la catégorie de tolérance aux pannes.

Noms des vérifications

- ALB Multi-AZ
- Le retour sur trace du cluster Amazon Aurora MySQL n'est pas activé
- Accessibilité de l'instance de base de données Amazon Aurora
- Amazon CloudFront Origin Failover
- Risque d'accès aux points de terminaison Amazon Comprehend
- Clusters AZ uniques Amazon DocumentDB

- Restauration d'Amazon oint-in-time DynamoDB P
- La table Amazon DynamoDB n'est pas incluse dans le plan de sauvegarde
- Amazon EBS n'est pas inclus dans le forfait AWS Backup
- Instantanés Amazon EBS
- La surveillance de l'état ELB n'est pas activée pour Amazon EC2 Auto Scaling
- Le rééquilibrage de capacité est activé pour le groupe Amazon EC2 Auto Scaling
- Amazon EC2 Auto Scaling n'est pas déployé dans plusieurs zones de disponibilité ou le nombre minimal de zones de disponibilité n'est pas atteint
- Équilibre des zones de disponibilité Amazon EC2
- La surveillance détaillée Amazon EC2 n'est pas activée
- Pilote Amazon ECS AWS Logs en mode blocage
- Service Amazon ECS utilisant une seule AZ
- Stratégie de placement Amazon ECS Multi-AZ
- Redondance d'aucune cible de montage Amazon EFS
- Amazon EFS n'est pas inclus dans le AWS Backup plan
- Clusters ElastiCache multi-AZ Amazon
- Sauvegarde automatique des clusters Amazon ElastiCache Redis
- Clusters Amazon MemoryDB multi-AZ
- Les agents Amazon MSK hébergent un trop grand nombre de partitions
- Domaines Amazon OpenSearch Service avec moins de trois nœuds de données
- Sauvegardes Amazon RDS
- Les clusters de base de données Amazon RDS possèdent une instance de base de données
- Clusters de base de données Amazon RDS avec toutes les instances dans la même zone de disponibilité
- Clusters de base de données Amazon RDS avec toutes les instances de lecteur dans la même zone de disponibilité
- La surveillance améliorée des instances de base de données Amazon RDS n'est pas activée
- La mise à l'échelle automatique du stockage est désactivée sur les instances de base de données Amazon RDS
- Les instances de base de données Amazon RDS n'utilisent pas le déploiement multi-AZ
- Amazon RDS DiskQueueDepth

- Amazon RDS FreeStorageSpace
- Le paramètre log_output d'Amazon RDS est défini sur table
- Le réglage du paramètre innodb_default_row_format d'Amazon RDS n'est pas sûr
- Le paramètre Amazon RDS innodb_flush_log_at_trx_commit n'est pas 1
- Le paramètre max_user_connections d'Amazon RDS est faible
- Amazon RDS Multi-AZ
- Amazon RDS n'est pas inclus dans le plan AWS Backup
- Les répliques Amazon RDS Read sont ouvertes en mode inscriptible
- Les sauvegardes automatisées des ressources Amazon RDS sont désactivées
- Le paramètre sync_binlog d'Amazon RDS est désactivé
- Aucune réplication multi-AZ n'est activée pour le cluster de base de données RDS
- Instance de secours RDS Multi-AZ non activée
- Amazon RDS ReplicaLag
- Le paramètre synchronous_commit d'Amazon RDS est désactivé
- Instantanés automatisés du cluster Amazon Redshift
- Surveillances des états supprimées Amazon Route 53
- Jeux d'enregistrements de ressource de basculement dans Amazon Route 53.
- Jeux d'enregistrements de ressource ayant une durée de vie élevée Amazon Route 53
- Délégations du serveur de noms Amazon Route 53
- Amazon Route 53 Resolver Redondance de la zone de disponibilité des terminaux
- Journalisation des compartiments Amazon S3
- La réplication de compartiment Amazon S3 n'est pas activée
- Amazon S3 Bucket Versioning
- Les Application Load Balancers, Network Load Balancers et Gateway Load Balancers ne sont pas répartis sur plusieurs zones de disponibilités
- Auto Scaling des adresses IP disponibles dans les sous-réseaux
- Surveillances de l'état du groupe Auto Scaling
- Ressources du groupe Auto Scaling
- Clusters AWS CloudHSM exécutant des instances HSM dans une mono-AZ
- AWS Direct Connect Redondance de connexion
- AWS Direct Connect Redondance des lieux

- AWS Direct Connect Résilience de localisation
- AWS Direct Connect Redondance de l'interface virtuelle
- AWS Lambda fonctions sans configuration d'une file d'attente de lettres mortes
- AWS Lambda Destinations des événements en cas de défaillance
- Fonctions compatibles VPC AWS Lambda sans redondance Multi-AZ
- AWS Resilience Hub Vérification des composants de l'application
- AWS Resilience Hub politique violée
- AWS Resilience Hub scores de résilience
- AWS Resilience Hub âge d'évaluation
- AWS Site-to-Site VPN possède au moins un tunnel à l'état DOWN
- Problèmes à risque élevé AWS Well-Architected pour la fiabilité
- Le Classic Load Balancer n'a pas plusieurs zones de disponibilité configurés
- Connection Draining ELB
- Équilibrage de charge entre zones ELB
- Optimisation des programmes Elastic Load Balancer
- Indépendance de la zone de disponibilité des passerelles NAT
- Équilibrage de charge entre zones sur les Network Load Balancers
- NLB - Ressource connectée à Internet dans un sous-réseau privé
- NLB Multi-AZ
- Nombre de Régions AWS dans un ensemble de réplication Incident Manager
- Vérification des applications sur une seule zone de disponibilité
- Interface VPC : interfaces réseau de point de terminaison dans plusieurs zones de disponibilité
- Redondance des tunnels VPN
- Redondance de zone de disponibilité pour ActiveMQ
- Redondance de zone de disponibilité pour RabbitMQ

ALB Multi-AZ

Description

Vérifie si vos équilibreurs de charge d'application sont configurés pour utiliser plusieurs zones de disponibilité (AZ). Une zone de disponibilité est un emplacement distinct isolé des défaillances

dans d'autres zones. Configurez votre équilibreur de charge dans plusieurs AZ de la même région pour améliorer la disponibilité de votre charge de travail.

> **Note**
>
> Les résultats de cette vérification sont automatiquement actualisés plusieurs fois par jour et les demandes d'actualisation ne sont pas autorisées. Plusieurs heures peuvent encore être nécessaires pour que les modifications apparaissent. Actuellement, vous ne pouvez pas exclure des ressources de cette vérification.

ID de la vérification

`c1dfprch08`

Critères d'alerte

Jaune : ALB est dans un seul AZ.

Vert : ALB possède au moins deux AZ.

Action recommandée

Assurez-vous que votre équilibreur de charge est configuré avec au moins deux zones de disponibilité.

Pour plus d'informations, consultez Zones de disponibilité pour votre Application Load Balancer.

Ressources supplémentaires

Pour plus d’informations, consultez la documentation de suivante :

- Comment fonctionne Elastic Load Balancing
- Régions, zones de disponibilité et zones locales

Colonnes du rapport

- Statut
- Région
- Nom ALB
- Règle ALB
- ARN DE LABORATOIRE
- Nombre de zones de disponibilité

- Heure de la dernière modification

Le retour sur trace du cluster Amazon Aurora MySQL n'est pas activé

Description

Vérifie si le retour sur trace est activé sur un cluster Amazon Aurora MySQL.

Le retour sur trace de cluster Amazon Aurora MySQL est une fonctionnalité qui vous permet de restaurer un cluster de base de données Aurora à un point antérieur sans créer de nouveau cluster. Cela vous permet de restaurer votre base de données à un point donné au cours d'une période de conservation, sans utiliser d'instantané.

Vous pouvez ajuster la fenêtre temporelle de retour en arrière (heures) dans le BacktrackWindowInHoursparamètre des AWS Config règles.

Pour plus d'informations, consultez Retour en arrière d'un cluster de base de données Amazon Aurora.

> **Note**
>
> Les résultats de cette vérification sont automatiquement actualisés plusieurs fois par jour et les demandes d'actualisation ne sont pas autorisées. Plusieurs heures peuvent encore être nécessaires pour que les modifications apparaissent. Actuellement, vous ne pouvez pas exclure des ressources de cette vérification.

ID de la vérification

`c18d2gz131`

Source

`AWS Config Managed Rule: aurora-mysql-backtracking-enabled`

Critères d'alerte

Jaune : le retour sur trace de clusters Amazon Aurora MySQL n'est pas activé.

Action recommandée

Activez le retour sur trace pour votre cluster Amazon Aurora MySQL.

Pour plus d'informations, consultez Retour en arrière d'un cluster de base de données Amazon Aurora.

Ressources supplémentaires

Retour sur trace d'un cluster de base de données Aurora

Colonnes du rapport

- Statut
- Région
- Ressource
- AWS Config Règle
- Paramètres d'entrée
- Heure de la dernière modification

Accessibilité de l'instance de base de données Amazon Aurora

Description

Vérifie les cas dans lesquels un cluster de base de données Amazon Aurora possède des instances privées et publiques.

En d'autres termes, si l'instance principale est défaillante, un réplica peut être promu comme l'instance principale. Si ce réplica est privé, les utilisateurs qui n'ont qu'un accès public ne pourront plus se connecter à la base de données après le basculement. Nous recommandons que toutes les instances de base de données d'un cluster aient la même accessibilité.

ID de la vérification

`xuy7H1avtl`

Critères d'alerte

Jaune : les instances d'un cluster de base de données Aurora n'ont pas la même accessibilité (combinaison de public et de privé).

Action recommandée

Modifiez le paramètre `Publicly Accessible` des instances du cluster de la base de données afin qu'elles soient toutes soit publiques soit privées. Pour plus de détails, consultez

les instructions pour les instances MySQL sur Modification d'une instance de base de données exécutant le moteur de base de données MySQL.

Ressources supplémentaires

Fault Tolerance for an Aurora DB Cluster (Tolérance aux pannes pour un cluster de base de données Aurora)

Colonnes du rapport

- Statut
- Région
- Cluster
- Instances de base de données publiques
- Instances de base de données privées
- Raison

Amazon CloudFront Origin Failover

Description

Vérifie qu'un groupe d'origine est configuré pour les distributions qui incluent deux origines sur Amazon CloudFront.

Pour plus d'informations, consultez Optimisation de la haute disponibilité avec le basculement CloudFront d'origine.

> **Note**
>
> Les résultats de cette vérification sont automatiquement actualisés plusieurs fois par jour et les demandes d'actualisation ne sont pas autorisées. Plusieurs heures peuvent encore être nécessaires pour que les modifications apparaissent. Actuellement, vous ne pouvez pas exclure des ressources de cette vérification.

ID de la vérification

`c18d2gz112`

Source

```
AWS Config Managed Rule: cloudfront-origin-failover-enabled
```

Critères d'alerte

Jaune : le basculement CloudFront d'Amazon Origin n'est pas activé.

Action recommandée

Assurez-vous d'activer la fonctionnalité de basculement d'origine pour vos CloudFront distributions afin de garantir la haute disponibilité de votre contenu aux utilisateurs finaux. Lorsque vous activez cette fonctionnalité, le trafic est automatiquement acheminé vers le serveur d'origine de secours si le serveur d'origine principal n'est pas disponible. Cela permet de limiter les temps d'arrêt potentiels et d'assurer la disponibilité continue de votre contenu.

Colonnes du rapport

- Statut
- Région
- Ressource
- AWS Config Règle
- Paramètres d'entrée
- Heure de la dernière modification

Risque d'accès aux points de terminaison Amazon Comprehend

Description

Vérifie les autorisations de clé AWS Key Management Service (AWS KMS) pour un point de terminaison où le modèle sous-jacent a été chiffré à l'aide de clés gérées par le client. Si la clé gérée par le client est désactivée, ou si la politique de clé a été modifiée pour changer les autorisations autorisées pour Amazon Comprehend, la disponibilité du point de terminaison peut être affectée.

> **Note**
>
> Les résultats de cette vérification sont automatiquement actualisés plusieurs fois par jour et les demandes d'actualisation ne sont pas autorisées. Plusieurs heures peuvent encore

être nécessaires pour que les modifications apparaissent. Actuellement, vous ne pouvez pas exclure des ressources de cette vérification.

ID de la vérification

`Cm24dfsM13`

Critères d'alerte

Rouge : la clé gérée par le client est désactivée, ou la politique de clé a été modifiée pour changer les autorisations autorisées pour l'accès à Amazon Comprehend.

Action recommandée

Si la clé gérée par le client a été désactivée, nous vous recommandons de l'activer. Pour plus d'informations, consultez Activation des clés. Si la politique clé a été modifiée et que vous souhaitez continuer à utiliser le point de terminaison, nous vous recommandons de mettre à jour la politique AWS KMS clé. Consultez Modification d'une stratégie de clé pour de plus amples informations.

Ressources supplémentaires

AWS KMS Autorisations

Colonnes du rapport

- Statut
- Région
- ARN du point de terminaison
- ARN du modèle
- KMS KeyId
- Heure de la dernière modification

Clusters AZ uniques Amazon DocumentDB

Description

Vérifie s'il existe des clusters Amazon DocumentDB configurés en mode mono-AZ.

L'exécution des charges de travail Amazon DocumentDB dans une architecture mono-AZ n'est pas suffisante pour les charges de travail très critiques et la restauration en cas de

défaillance d'un composant peut prendre jusqu'à 10 minutes. Les clients doivent déployer des instances de réplication dans des zones de disponibilité supplémentaires afin de garantir la disponibilité pendant la maintenance, les pannes d'instance, les défaillances de composants ou les défaillances de zones de disponibilité.

> **Note**
>
> Les résultats de cette vérification sont automatiquement actualisés une ou plusieurs fois par jour, et les demandes d'actualisation ne sont pas autorisées. Plusieurs heures peuvent encore être nécessaires pour que les modifications apparaissent. Actuellement, vous ne pouvez pas exclure des ressources de cette vérification.

ID de la vérification

`c15vnddn2x`

Critères d'alerte

Jaune : le cluster Amazon DocumentDB possède des instances dans moins de trois zones de disponibilité.

Vert : le cluster Amazon DocumentDB possède des instances réparties dans trois zones de disponibilité.

Action recommandée

Si votre application nécessite une haute disponibilité, modifiez votre instance de base de données pour activer le mode multi-AZ à l'aide d'instances de réplication. Voir Amazon DocumentDB High Availability and Replication

Ressources supplémentaires

Comprendre la tolérance aux pannes du cluster Amazon DocumentDB

Régions et zones de disponibilité

Colonnes du rapport

- Statut
- Région
- Zone de disponibilité

- Identificateur du cluster DB
- ARN du cluster de base de données
- Heure de la dernière modification

Restauration d'Amazon oint-in-time DynamoDB P

Description

Vérifie si la restauration à un instant dans le passe est activée pour vos tables Amazon DynamoDB.

La restauration à un instant dans le passé permet de protéger vos tables DynamoDB contre les opérations d'écriture ou de suppression accidentelles. Grâce à la restauration à un instant dans le passé, vous n'avez plus à vous soucier de la création, de la gestion ou de la planification des sauvegardes à la demande. Grâce à la restauration à un instant dans le passé, vous pouvez restaurer des tables à n'importe quel instant dans le passé au cours des 35 derniers jours. DynamoDB conserve des sauvegardes incrémentielles de votre table.

Pour plus d'informations, consultez la section oint-in-time Restauration de P pour DynamoDB.

> **Note**
>
> Les résultats de cette vérification sont automatiquement actualisés plusieurs fois par jour et les demandes d'actualisation ne sont pas autorisées. Plusieurs heures peuvent encore être nécessaires pour que les modifications apparaissent. Actuellement, vous ne pouvez pas exclure des ressources de cette vérification.

ID de la vérification

```
c18d2gz138
```

Source

```
AWS Config Managed Rule: dynamodb-pitr-enabled
```

Critères d'alerte

Jaune : la oint-in-time restauration P n'est pas activée pour vos tables DynamoDB.

Action recommandée

Activez la point-in-time restauration dans Amazon DynamoDB pour sauvegarder en permanence les données de vos tables.

Pour plus d'informations, consultez P oint-in-time recovery : How it works.

Ressources supplémentaires

oint-in-time Restauration IP pour DynamoDB

Colonnes du rapport

- Statut
- Région
- Ressource
- AWS Config Règle
- Paramètres d'entrée
- Heure de la dernière modification

La table Amazon DynamoDB n'est pas incluse dans le plan de sauvegarde

Description

Vérifie si les tables Amazon DynamoDB font partie d'un plan. AWS Backup

AWS Backup fournit des sauvegardes incrémentielles pour les tables DynamoDB qui capturent les modifications apportées depuis la dernière sauvegarde. L'inclusion de tables DynamoDB dans AWS Backup un plan permet de protéger vos données contre les scénarios de perte de données accidentelle et d'automatiser le processus de sauvegarde. Cela fournit une solution de sauvegarde fiable et évolutive pour vos tables DynamoDB, assurant ainsi la protection de vos précieuses données et leur restauration selon les besoins.

Pour plus d'informations, voir Création de sauvegardes de tables DynamoDB avec AWS Backup

> **Note**
>
> Les résultats de cette vérification sont automatiquement actualisés plusieurs fois par jour et les demandes d'actualisation ne sont pas autorisées. Plusieurs heures peuvent encore

être nécessaires pour que les modifications apparaissent. Actuellement, vous ne pouvez pas exclure des ressources de cette vérification.

ID de la vérification

`c18d2gz107`

Source

`AWS Config Managed Rule: dynamodb-in-backup-plan`

Critères d'alerte

Jaune : la table Amazon DynamoDB n'est pas incluse dans le forfait. AWS Backup

Action recommandée

Assurez-vous que vos tables Amazon DynamoDB font partie d'un plan. AWS Backup

Ressources supplémentaires

Sauvegardes planifiées

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

Création de plans de sauvegarde à l'aide de la console AWS Backup

Colonnes du rapport

- Statut
- Région
- Ressource
- AWS Config Règle
- Paramètres d'entrée
- Heure de la dernière modification

Amazon EBS n'est pas inclus dans le forfait AWS Backup

Description

Vérifie si des volumes Amazon EBS sont présents dans les plans de sauvegarde pour AWS Backup.

Incluez les volumes Amazon EBS dans un AWS Backup plan visant à automatiser les sauvegardes régulières des données stockées sur ces volumes. Cela vous protège contre les pertes de données, facilite la gestion des données et permet leur restauration en cas de besoin. Un plan de sauvegarde permet d'assurer la sécurité de vos données et de respecter les objectifs de délai et de point de reprise (RTO/RPO) pour votre application et vos services.

Pour plus d'informations, voir Création d'un plan de sauvegarde.

> **Note**
>
> Les résultats de cette vérification sont automatiquement actualisés plusieurs fois par jour et les demandes d'actualisation ne sont pas autorisées. Plusieurs heures peuvent encore être nécessaires pour que les modifications apparaissent. Actuellement, vous ne pouvez pas exclure des ressources de cette vérification.

ID de la vérification

`c18d2gz106`

Source

`AWS Config Managed Rule: ebs-in-backup-plan`

Critères d'alerte

Jaune : le volume Amazon EBS n'est pas inclus dans le AWS Backup forfait.

Action recommandée

Assurez-vous que vos volumes Amazon EBS font partie d'un AWS Backup plan.

Ressources supplémentaires

Création de plans de sauvegarde à l'aide de la AWS Backup console

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

Mise en route 3 : création d'une sauvegarde planifiée

Colonnes du rapport

- Statut
- Région

- Ressource
- AWS Config Règle
- Paramètres d'entrée
- Heure de la dernière modification

Instantanés Amazon EBS

Description

Vérifie l'ancienneté des instantanés pour vos volumes Amazon Elastic Block Store (Amazon EBS) (disponibles ou en cours d'utilisation).

Même si les volumes Amazon EBS sont répliqués, des échecs peuvent se produire. Les instantanés sont conservés dans Amazon Simple Storage Service (Amazon S3) pour un stockage et une restauration durables. point-in-time

ID de la vérification

`H7IgTzjTYb`

Critères d'alerte

- Jaune : l'instantané de volume le plus récent date de 7 à 30 jours.
- Rouge : l'instantané de volume le plus récent date de plus de 30 jours.
- Rouge : le volume ne possède pas d'instantané.

Action recommandée

Créez des instantanés hebdomadaires ou mensuels de vos volumes. Pour plus d'informations, consultez Creating an Amazon EBS Snapshot (Création d'un instantané Amazon EBS).

Ressources supplémentaires

Amazon Elastic Block Store (Amazon EBS)

Colonnes du rapport

- Statut
- Région
- ID du volume
- Nom du volume
- ID de l'instantané

- Nom de l'instantané
- Âge de l'instantané
- Attachement du volume
- Raison

La surveillance de l'état ELB n'est pas activée pour Amazon EC2 Auto Scaling

Description

Vérifie si vos groupes Amazon EC2 Auto Scaling associés à un Classic Load Balancer utilisent la surveillance de l'état Elastic Load Balancing. La surveillance de l'état par défaut d'un groupe Auto Scaling correspond uniquement à la surveillance de l'état Amazon EC2. Si une instance échoue lors de ces contrôles d'état, elle est marquée comme défectueuse et terminée. Dans ce cas, Amazon EC2 Auto Scaling lance une instance de remplacement. La surveillance de l'état Elastic Load Balancing surveille régulièrement les instances Amazon EC2 afin de détecter et de terminer les instances défectueuses, puis de lancer de nouvelles instances.

Pour plus d'informations, consultez Add Elastic Load Balancing health checks.

> **Note**
>
> Les résultats de cette vérification sont automatiquement actualisés plusieurs fois par jour et les demandes d'actualisation ne sont pas autorisées. Plusieurs heures peuvent encore être nécessaires pour que les modifications apparaissent. Actuellement, vous ne pouvez pas exclure des ressources de cette vérification.

ID de la vérification

```
c18d2gz104
```

Source

```
AWS Config Managed Rule: autoscaling-group-elb-healthcheck-required
```

Critères d'alerte

Jaune : la surveillance de l'état Elastic Load Balancing n'est pas activée pour le groupe Amazon EC2 Auto Scaling attaché au Classic Load Balancer.

Action recommandée

Assurez-vous que vos groupes Auto Scaling associés à un Classic Load Balancer utilisent la surveillance de l'état Elastic Load Balancing.

La surveillance de l'état Elastic Load Balancing indique si l'équilibreur de charge est sain et disponible pour traiter les demandes. Cela assure une haute disponibilité pour votre application.

Pour plus d'informations, voir Ajout de la surveillance d'état Elastic Load Balancing à un groupe Auto Scaling.

Colonnes du rapport

- Statut
- Région
- Ressource
- AWS Config Règle
- Paramètres d'entrée
- Heure de la dernière modification

Le rééquilibrage de capacité est activé pour le groupe Amazon EC2 Auto Scaling

Description

Vérifie si le rééquilibrage de capacité est activé pour les groupes Amazon EC2 Auto Scaling qui utilisent plusieurs types d'instances.

La configuration des groupes Amazon EC2 Auto Scaling avec le rééquilibrage de capacité permet de s'assurer que les instances Amazon EC2 sont réparties uniformément entre les zones de disponibilité, quels que soient le type d'instance et les options d'achat. Elle utilise une politique de suivi des cibles associée au groupe, telle que l'utilisation de l'UC ou le trafic réseau.

Pour plus d'informations, voir Groupes Auto Scaling avec plusieurs types d'instances et d'options d'achat.

> **Note**
>
> Les résultats de cette vérification sont automatiquement actualisés plusieurs fois par jour et les demandes d'actualisation ne sont pas autorisées. Plusieurs heures peuvent encore

être nécessaires pour que les modifications apparaissent. Actuellement, vous ne pouvez pas exclure des ressources de cette vérification.

ID de la vérification

`AWS Config c18d2gz103`

Source

AWS Config Règle gérée : autoscaling-capacity-rebalancing

Critères d'alerte

Le rééquilibrage de capacité n'est pas activé pour le groupe Amazon EC2 Auto Scaling.

Action recommandée

Assurez-vous que le rééquilibrage de capacité est activé pour vos groupes Amazon EC2 Auto Scaling qui utilisent plusieurs types d'instances.

Pour plus d'informations, voir Activation du rééquilibrage de capacité (console).

Colonnes du rapport

- Statut
- Région
- Ressource
- AWS Config Règle
- Paramètres d'entrée
- Heure de la dernière modification

Amazon EC2 Auto Scaling n'est pas déployé dans plusieurs zones de disponibilité ou le nombre minimal de zones de disponibilité n'est pas atteint

Description

Vérifie si le groupe Amazon EC2 Auto Scaling est déployé dans plusieurs zones de disponibilité ou si le nombre minimal de zones de disponibilité est spécifié. Déployez des instances Amazon EC2 dans plusieurs zones de disponibilité pour assurer une haute disponibilité.

Vous pouvez ajuster le nombre minimum de zones de disponibilité à l'aide du minAvailibilityZonesparamètre de vos AWS Config règles.

Pour plus d'informations, voir Groupes Auto Scaling avec plusieurs types d'instances et d'options d'achat.

ID de la vérification

`c18d2gz101`

Source

`AWS Config Managed Rule: autoscaling-multiple-az`

Critères d'alerte

Rouge : plusieurs zones de disponibilité ne sont pas configurées pour le groupe Amazon EC2 Auto Scaling ou le nombre minimal de zones de disponibilité spécifié n'est pas atteint.

Action recommandée

Assurez-vous que plusieurs zones de disponibilité sont configurées pour votre groupe Amazon EC2 Auto Scaling. Déployez des instances Amazon EC2 dans plusieurs zones de disponibilité pour assurer une haute disponibilité.

Ressources supplémentaires

Création d'un groupe Auto Scaling à l'aide d'un modèle de lancement

Création d'un groupe Auto Scaling à l'aide d'une configuration de lancement

Colonnes du rapport

- Statut
- Région
- Ressource
- AWS Config Règle
- Paramètres d'entrée
- Heure de la dernière modification

Équilibre des zones de disponibilité Amazon EC2

Description

Vérifie la distribution des instances Amazon Elastic Compute Cloud (Amazon EC2) dans les zones de disponibilité d'une région.

Les zones de disponibilité sont des emplacements distincts dans une région, isolés des échecs dans d'autres zones de disponibilité. Cela permet d'avoir une connectivité réseau économique à faible latence entre les zones de disponibilité de la même région. En lançant des instances dans plusieurs zones de disponibilité d'une même région, vous pouvez protéger vos applications contre l'échec d'une zone.

ID de la vérification

`wuy7G1zxql`

Critères d'alerte

- Jaune : la région possède des instances dans plusieurs zones, mais la distribution est inégale (la différence entre le nombre d'instances le plus élevé et le plus faible dans les zones de disponibilité utilisées est supérieure à 20 %).
- Rouge : la région ne possède des instances que dans une seule zone de disponibilité.

Action recommandée

Équilibrez uniformément vos instances Amazon EC2 sur plusieurs zones de disponibilité. Vous pouvez le faire en lançant des instances manuellement ou en utilisant Auto Scaling pour le faire automatiquement. Pour de plus amples informations, veuillez consulter Launch Your Instance (Lancer votre instance) et Load Balance Your Auto Scaling group (Répartir la charge de votre groupe Auto Scaling).

Ressources supplémentaires

Guide de l'utilisateur Amazon EC2 Auto Scaling

Colonnes du rapport

- Statut
- Région
- Instances de zone a
- Instances de zone b
- Instances de zone c

- Instances de zone e
- Instances de zone f
- Raison

La surveillance détaillée Amazon EC2 n'est pas activée

Description

Vérifie si la surveillance détaillée est activée pour vos instances EC2.

Par exemple, la surveillance détaillée pour Amazon EC2 fournit des métriques plus fréquentes, publiées à intervalles d'une minute, contre cinq minutes pour la surveillance basique pour Amazon EC2. L'utilisation de la surveillance détaillée pour Amazon EC2 vous aide à mieux gérer vos ressources Amazon EC2, de sorte que vous puissiez identifier les tendances et agir plus rapidement.

Pour plus d'informations, voir Surveillance basique et surveillance détaillée.

> **Note**
>
> Les résultats de cette vérification sont automatiquement actualisés plusieurs fois par jour et les demandes d'actualisation ne sont pas autorisées. Plusieurs heures peuvent encore être nécessaires pour que les modifications apparaissent. Actuellement, vous ne pouvez pas exclure des ressources de cette vérification.

ID de la vérification

`AWS Config c18d2gz144`

Source

AWS Config Règle gérée : ec2- instance-detailed-monitoring-enabled

Critères d'alerte

Jaune : la surveillance détaillée n'est pas activée pour les instances Amazon EC2.

Action recommandée

Activez la surveillance détaillée de vos instances Amazon EC2 afin d'augmenter la fréquence à laquelle les données métriques Amazon EC2 sont publiées sur CloudWatch Amazon (de 5 à 1 minute d'intervalle).

Colonnes du rapport

- Statut
- Région
- Ressource
- AWS Config Règle
- Paramètres d'entrée
- Heure de la dernière modification

Pilote Amazon ECS AWS Logs en mode blocage

Description

Vérifie les définitions de tâches Amazon ECS configurées avec le pilote de journalisation AWS des journaux en mode blocage. Un pilote configuré en mode blocage met en danger la disponibilité du système.

> **Note**
>
> Les résultats de cette vérification sont automatiquement actualisés une ou plusieurs fois par jour, et les demandes d'actualisation ne sont pas autorisées. Plusieurs heures peuvent encore être nécessaires pour que les modifications apparaissent. Actuellement, vous ne pouvez pas exclure des ressources de cette vérification.

ID de la vérification

`c1dvkm4z6b`

Critères d'alerte

Jaune : le mode des paramètres de configuration de journalisation du pilote awslogs est défini sur blocage ou absent. Un paramètre de mode manquant indique une configuration de blocage par défaut.

Vert : la définition des tâches Amazon ECS n'utilise pas le pilote awslogs ou le pilote awslogs est configuré en mode non bloquant.

Action recommandée

Pour atténuer le risque de disponibilité, envisagez de modifier la définition de la tâche. La configuration du pilote AWS Logs passe du mode bloquant au mode non bloquant. En mode non bloquant, vous devrez définir une valeur pour le max-buffer-size paramètre. Pour plus d'informations et de conseils sur les paramètres de configuration, consultez. Voir Prévention de la perte de journaux grâce au mode non bloquant dans le pilote de journal du conteneur AWS Logs

Ressources supplémentaires

Utilisation du pilote AWS Logs Log

Choix des options d'enregistrement des conteneurs pour éviter la contre-pression

Prévention de la perte de journaux grâce au mode non bloquant dans le pilote de journal du conteneur AWS Logs

Colonnes du rapport

- Statut
- Région
- ARN de définition des tâches
- Noms de définition des conteneurs
- Heure de la dernière modification

Service Amazon ECS utilisant une seule AZ

Description

Vérifie que la configuration de votre service utilise une seule zone de disponibilité (AZ).

Une zone de disponibilité est un emplacement distinct isolé des défaillances dans d'autres zones. Cela permet d'avoir une connectivité réseau économique à faible latence entre les zones de disponibilité d'une même Région AWS. En lançant des instances dans plusieurs zones de disponibilité d'une même région, vous pouvez protéger vos applications contre un point unique de défaillance.

> **Note**
>
> Les résultats de cette vérification sont automatiquement actualisés plusieurs fois par jour et les demandes d'actualisation ne sont pas autorisées. Plusieurs heures peuvent encore être nécessaires pour que les modifications apparaissent. Actuellement, vous ne pouvez pas exclure des ressources de cette vérification.

ID de la vérification

`c1z7dfpz01`

Critères d'alerte

- Jaune : un service Amazon ECS exécute toutes les tâches dans une seule zone de disponibilité.
- Vert : un service Amazon ECS exécute des tâches dans au moins deux zones de disponibilité différentes.

Action recommandée

Créez au moins une tâche supplémentaire pour le service dans une zone de disponibilité différente.

Ressources supplémentaires

Capacité et disponibilité d'Amazon ECS

Colonnes du rapport

- Statut
- Région
- Nom du cluster/service ECS
- Nombre de zones de disponibilité
- Heure de la dernière modification

Stratégie de placement Amazon ECS Multi-AZ

Description

Vérifie que votre service Amazon ECS utilise la stratégie de placement par répartition basée sur la zone de disponibilité (AZ). Cette stratégie répartit les tâches entre les zones de disponibilité de

manière identique Région AWS et peut contribuer à protéger vos applications contre un point de défaillance unique.

Pour les tâches exécutées dans le cadre d'un service Amazon ECS, la répartition constitue la stratégie de placement des tâches par défaut.

Ce contrôle permet également de vérifier que la répartition est la première ou la seule stratégie dans votre liste de stratégies de placement actives.

> **Note**
>
> Les résultats de cette vérification sont automatiquement actualisés plusieurs fois par jour et les demandes d'actualisation ne sont pas autorisées. Plusieurs heures peuvent encore être nécessaires pour que les modifications apparaissent. Actuellement, vous ne pouvez pas exclure des ressources de cette vérification.

ID de la vérification

`c1z7dfpz02`

Critères d'alerte

- Jaune : la répartition par zone de disponibilité est désactivée ou n'est pas la première stratégie de votre liste de stratégies de placement actives pour votre service Amazon ECS.
- Vert : la répartition par zone de disponibilité est la première stratégie dans votre liste de stratégies de placement actives ou la seule stratégie de placement active pour votre service Amazon ECS.

Action recommandée

Activez la stratégie de répartition des tâches pour répartir les tâches entre plusieurs zones de disponibilité. Vérifiez que la répartition par zone de disponibilité est la première ou la seule stratégie de placement de tâches active utilisée. Si vous choisissez de gérer le placement dans les zones de disponibilité, vous pouvez utiliser un service de mise en miroir dans une autre zone de disponibilité pour limiter ces risques.

Ressources supplémentaires

Stratégies de placement des tâches Amazon ECS

Colonnes du rapport

- Statut

- Région
- Nom du cluster/service ECS
- Stratégie de placement des tâches par répartition activée et appliquée correctement
- Heure de la dernière modification

Redondance d'aucune cible de montage Amazon EFS

Description

Vérifie si des cibles de montage existent dans plusieurs zones de disponibilité d'un système de fichiers Amazon EFS.

Une zone de disponibilité est un emplacement distinct isolé des défaillances dans d'autres zones. La création de cibles de montage dans plusieurs zones de disponibilité géographiquement séparées au sein d'une même région AWS vous permet d'obtenir une disponibilité et une durabilité supérieures pour vos systèmes de fichiers Amazon EFS.

> **Note**
>
> Les résultats de cette vérification sont automatiquement actualisés plusieurs fois par jour et les demandes d'actualisation ne sont pas autorisées. Plusieurs heures peuvent encore être nécessaires pour que les modifications apparaissent. Actuellement, vous ne pouvez pas exclure des ressources de cette vérification.

ID de la vérification

`c1dfprch01`

Critères d'alerte

- Jaune : une cible de montage a été créée dans une zone de disponibilité pour le système de fichiers.

  Vert : au moins deux cibles de montage ont été créées dans plusieurs zones de disponibilité pour le système de fichiers.

Action recommandée

Pour les systèmes de fichiers EFS utilisant des classes de stockage unizones, nous vous recommandons de créer de nouveaux systèmes de fichiers utilisant des classes de stockage

standard en restaurant une sauvegarde sur un nouveau système de fichiers. Créez ensuite des cibles de montage dans plusieurs zones de disponibilité.

Pour les systèmes de fichiers EFS utilisant des classes de stockage standard, nous vous recommandons de créer des cibles de montage dans plusieurs zones de disponibilité.

Ressources supplémentaires

- Gestion des cibles de montage à l'aide de la console Amazon EFS
- Quotas et limites Amazon EFS

Colonnes du rapport

- Statut
- Région
- Identifiant de système de fichiers EFS
- Nombre de cibles de montage
- Nombre de zones de disponibilité
- Heure de la dernière modification

Amazon EFS n'est pas inclus dans le AWS Backup plan

Description

Vérifie si les systèmes de fichiers Amazon EFS sont inclus dans les plans de sauvegarde avec AWS Backup.

AWS Backup est un service de sauvegarde unifié conçu pour simplifier la création, la migration, la restauration et la suppression des sauvegardes, tout en fournissant des rapports et des audits améliorés.

Pour plus d'informations, consultez Backing up your Amazon EFS file systems (Sauvegarde de vos systèmes de fichiers Amazon EFS).

ID de la vérification

```
c18d2gz117
```

Source

```
AWS Config Managed Rule: EFS_IN_BACKUP_PLAN
```

Critères d'alerte

Rouge : Amazon EFS n'est pas inclus dans le AWS Backup forfait.

Action recommandée

Assurez-vous que vos systèmes de fichiers Amazon EFS sont inclus dans votre AWS Backup plan afin de vous protéger contre la perte ou la corruption de données accidentelles.

Ressources supplémentaires

Sauvegarde de vos systèmes de fichiers Amazon EFS

Amazon EFS Backup and Restore à l'aide de AWS Backup.

Colonnes du rapport

- Statut
- Région
- Ressource
- AWS Config Règle
- Paramètres d'entrée
- Heure de la dernière modification

Clusters ElastiCache multi-AZ Amazon

Description

Vérifie les ElastiCache clusters déployés dans une seule zone de disponibilité (AZ). Ce contrôle vous avertit si Multi-AZ est inactif dans un cluster.

Les déploiements dans plusieurs zones de zone améliorent la disponibilité des ElastiCache clusters en effectuant une réplication asynchrone vers des répliques en lecture seule dans une zone de zone différente. Lorsqu'une maintenance planifiée du cluster a lieu ou qu'un nœud principal n'est pas disponible, une réplique est ElastiCache automatiquement convertie en nœud principal. Ce basculement permet de reprendre les opérations d'écriture du cluster et ne nécessite pas l'intervention d'un administrateur.

> **Note**
>
> Les résultats de cette vérification sont automatiquement actualisés plusieurs fois par jour et les demandes d'actualisation ne sont pas autorisées. Plusieurs heures peuvent encore

être nécessaires pour que les modifications apparaissent. Actuellement, vous ne pouvez pas exclure des ressources de cette vérification.

ID de la vérification

`ECHdfsQ402`

Critères d'alerte

- Vert : Multi-AZ est actif dans le cluster.
- Jaune : Multi-AZ est inactif dans le cluster.

Action recommandée

Créez au moins un réplica par partition, dans une zone de disponibilité différente de la principale.

Ressources supplémentaires

Pour plus d'informations, consultez Minimiser les temps d'arrêt ElastiCache pour Redis avec Multi-AZ.

Colonnes du rapport

- Statut
- Région
- Nom du cluster
- Heure de la dernière modification

Sauvegarde automatique des clusters Amazon ElastiCache Redis

Description

Vérifie si la sauvegarde automatique est activée sur les clusters Amazon ElastiCache pour Redis et si la période de conservation des instantanés est supérieure à la limite par défaut spécifiée ou à 15 jours. Lorsque les sauvegardes automatiques sont activées, ElastiCache crée une sauvegarde quotidienne du cluster.

Vous pouvez définir la limite de conservation des instantanés souhaitée à l'aide des snapshotRetentionPeriodparamètres de vos AWS Config règles.

Pour plus d'informations, consultez Backup and restore ElastiCache for Redis.

> **Note**
>
> Les résultats de cette vérification sont automatiquement actualisés plusieurs fois par jour et les demandes d'actualisation ne sont pas autorisées. Plusieurs heures peuvent encore être nécessaires pour que les modifications apparaissent. Actuellement, vous ne pouvez pas exclure des ressources de cette vérification.

ID de la vérification

`c18d2gz178`

Source

`AWS Config Managed Rule: elasticache-redis-cluster-automatic-backup-check`

Critères d'alerte

Rouge : la sauvegarde automatique n'est pas activée sur les clusters Amazon ElastiCache pour Redis ou la durée de conservation des instantanés est inférieure à la limite.

Action recommandée

Assurez-vous que la sauvegarde automatique est activée sur les clusters Amazon ElastiCache pour Redis et que la période de conservation des instantanés est supérieure à la limite par défaut spécifiée ou à 15 jours. Les sauvegardes automatiques peuvent constituer une protection contre la perte de données. En prévision d'une éventuelle défaillance, vous pouvez créer un cluster et restaurer vos données à partir de la sauvegarde la plus récente.

Pour plus d'informations, consultez Backup and restore ElastiCache for Redis.

Ressources supplémentaires

Pour plus d'informations, voir Planification des sauvegardes automatiques.

Colonnes du rapport

- Statut
- Région
- Nom du cluster
- Heure de la dernière modification

Clusters Amazon MemoryDB multi-AZ

Description

Vérifie les clusters MemoryDB déployés dans une zone de disponibilité (AZ). Ce contrôle vous avertit si Multi-AZ est inactif dans un cluster.

Les déploiements dans plusieurs AZ améliorent la disponibilité des clusters MemoryDB en répliquant de manière asynchrone vers des réplicas en lecture seule dans une autre AZ. Lorsqu'une maintenance planifiée du cluster a lieu ou qu'un nœud primaire n'est pas disponible, MemoryDB convertit automatiquement un réplica en nœud primaire. Ce basculement permet de reprendre les opérations d'écriture du cluster et ne nécessite pas l'intervention d'un administrateur.

> **Note**
>
> Les résultats de cette vérification sont automatiquement actualisés plusieurs fois par jour et les demandes d'actualisation ne sont pas autorisées. Plusieurs heures peuvent encore être nécessaires pour que les modifications apparaissent. Actuellement, vous ne pouvez pas exclure des ressources de cette vérification.

ID de la vérification

`MDBdfsQ401`

Critères d'alerte

- Vert : Multi-AZ est actif dans le cluster.
- Jaune : Multi-AZ est inactif dans le cluster.

Action recommandée

Créez au moins un réplica par partition, dans une zone de disponibilité différente de la principale.

Ressources supplémentaires

Pour de plus amples informations, veuillez consulter Réduction des temps d'arrêt avec Multi-AZ (français non garanti).

Colonnes du rapport

- Statut

- Région
- Nom du cluster
- Heure de la dernière modification

Les agents Amazon MSK hébergent un trop grand nombre de partitions

Description

Vérifie que le nombre de partitions attribuées aux agents d'un cluster Managed Streaming for Kafka (MSK) respecte la limite recommandée.

ID de la vérification

`Cmsvnj8vf1`

Critères d'alerte

- Rouge : le nombre de partitions attribuées à l'agent de votre cluster MSK a atteint ou dépassé le nombre maximal de partitions recommandé.
- Jaune : le nombre de partitions attribuées à l'agent de votre cluster MSK a atteint ou dépassé 80 % du nombre maximal de partitions recommandé.

Action recommandée

Suivez les bonnes pratiques recommandées en matière de MSK pour mettre à l'échelle votre cluster MSK ou supprimer les partitions inutilisées.

Ressources supplémentaires

- Dimensionnement correct de votre cluster

Colonnes du rapport

- Statut
- Région
- ARN de cluster
- Identifiant de l'agent
- Nombre de partitions

Domaines Amazon OpenSearch Service avec moins de trois nœuds de données

Description

Vérifie si les domaines Amazon OpenSearch Service sont configurés avec au moins trois nœuds de données et si ZoneAwarenessEnabled c'est vrai. ZoneAwarenessEnabled Lorsque cette option est activée, Amazon OpenSearch Service garantit que chaque partition principale et sa réplique correspondante sont allouées dans différentes zones de disponibilité.

Pour plus d'informations, consultez Configuration d'un domaine multi-AZ dans Amazon OpenSearch Service.

> **Note**
>
> Les résultats de cette vérification sont automatiquement actualisés plusieurs fois par jour et les demandes d'actualisation ne sont pas autorisées. Plusieurs heures peuvent encore être nécessaires pour que les modifications apparaissent. Actuellement, vous ne pouvez pas exclure des ressources de cette vérification.

ID de la vérification

`c18d2gz183`

Source

`AWS Config Managed Rule: opensearch-data-node-fault-tolerance`

Critères d'alerte

Jaune : les domaines Amazon OpenSearch Service sont configurés avec moins de trois nœuds de données.

Action recommandée

Assurez-vous que les domaines Amazon OpenSearch Service sont configurés avec au moins trois nœuds de données. Configurez un domaine multi-AZ pour améliorer la disponibilité du cluster Amazon OpenSearch Service en allouant des nœuds et en répliquant les données sur trois zones de disponibilité au sein de la même région. Cela évite la perte de données et limite les temps d'arrêt en cas de défaillance d'un nœud ou du centre de données (AZ).

Pour plus d'informations, consultez Augmenter la disponibilité d'Amazon OpenSearch Service en le déployant dans trois zones de disponibilité.

Ressources supplémentaires

- Améliorez la disponibilité d'Amazon OpenSearch Service en le déployant dans trois zones de disponibilité

Colonnes du rapport

- Statut
- Région
- Ressource
- AWS Config Règle
- Paramètres d'entrée
- Heure de la dernière modification

Sauvegardes Amazon RDS

Description

Vérifie les sauvegardes automatiques des instances de base de données Amazon RDS.

Par défaut, les sauvegardes sont activées avec une période de rétention d'un jour. Les sauvegardes réduisent le risque de perte de données imprévue et permettent la point-in-time restauration.

ID de la vérification

`opQPADkZvH`

Critères d'alerte

Rouge : la période de conservation des sauvegardes d'une instance de base de données est définie sur 0 jours.

Action recommandée

Définissez la période de conservation des sauvegardes automatisées de l'instance de base de données sur 1 à 35 jours, en fonction des exigences de votre application. Consultez Working With Automated Backups (Utilisation des sauvegardes automatiques).

Ressources supplémentaires

Getting Started with Amazon RDS (Démarrer avec Amazon RDS)

Colonnes du rapport

- Statut
- Région/zone de disponibilité
- instance de base de données
- ID du VPC
- Période de conservation de la sauvegarde

Les clusters de base de données Amazon RDS possèdent une instance de base de données

Description

Ajoutez au moins une autre instance de base de données au cluster de base de données pour améliorer la disponibilité et les performances.

> **Note**
>
> Les résultats de cette vérification sont automatiquement actualisés plusieurs fois par jour et les demandes d'actualisation ne sont pas autorisées. Plusieurs heures peuvent encore être nécessaires pour que les modifications apparaissent. Actuellement, vous ne pouvez pas exclure des ressources de cette vérification.

> **Note**
>
> Lorsqu'une instance ou un cluster de bases de données est arrêté, vous pouvez consulter les recommandations Amazon RDS Trusted Advisor pendant 3 à 5 jours. Après cinq jours, les recommandations ne sont plus disponibles dans Trusted Advisor. Pour consulter les recommandations, ouvrez la console Amazon RDS, puis choisissez Recommendations. Si vous supprimez une instance ou un cluster de bases de données, les recommandations associées à ces instances ou clusters ne sont pas disponibles dans Trusted Advisor ou dans la console de gestion Amazon RDS.

ID de la vérification

```
c1qf5bt011
```

Critères d'alerte

Jaune : les clusters de base de données ne possèdent qu'une seule instance de base de données.

Action recommandée

Ajoutez une instance de base de données de lecteur au cluster de base de données.

Ressources supplémentaires

Dans la configuration actuelle, une instance de base de données est utilisée pour les opérations de lecture et d'écriture. Vous pouvez ajouter une autre instance de base de données pour autoriser la redistribution des lectures et une option de basculement.

Pour plus d'informations, consultez la section Haute disponibilité pour Amazon Aurora.

Colonnes du rapport

- Statut
- Région
- Ressource
- Nom du moteur
- Classe d'instance de base de données
- Heure de la dernière modification

Clusters de base de données Amazon RDS avec toutes les instances dans la même zone de disponibilité

Description

Les clusters de base de données se trouvent actuellement dans une seule zone de disponibilité. Utilisez plusieurs zones de disponibilité pour améliorer la disponibilité.

> **Note**
>
> Les résultats de cette vérification sont automatiquement actualisés plusieurs fois par jour et les demandes d'actualisation ne sont pas autorisées. Plusieurs heures peuvent encore être nécessaires pour que les modifications apparaissent. Actuellement, vous ne pouvez pas exclure des ressources de cette vérification.

> **Note**
>
> Lorsqu'une instance ou un cluster de bases de données est arrêté, vous pouvez consulter les recommandations Amazon RDS Trusted Advisor pendant 3 à 5 jours. Après cinq jours, les recommandations ne sont plus disponibles dans Trusted Advisor. Pour consulter les recommandations, ouvrez la console Amazon RDS, puis choisissez Recommendations. Si vous supprimez une instance ou un cluster de bases de données, les recommandations associées à ces instances ou clusters ne sont pas disponibles dans Trusted Advisor ou dans la console de gestion Amazon RDS.

ID de la vérification

`c1qf5bt007`

Critères d'alerte

Jaune : les clusters de base de données ont toutes les instances dans la même zone de disponibilité.

Action recommandée

Ajoutez les instances de base de données à plusieurs zones de disponibilité de votre cluster de base de données.

Ressources supplémentaires

Nous vous recommandons d'ajouter les instances de base de données à plusieurs zones de disponibilité dans un cluster de base de données. L'ajout d'instances de base de données à plusieurs zones de disponibilité améliore la disponibilité de votre cluster de bases de données.

Pour plus d'informations, consultez la section Haute disponibilité pour Amazon Aurora.

Colonnes du rapport

- Statut
- Région
- Ressource
- Nom du moteur
- Heure de la dernière modification

Clusters de base de données Amazon RDS avec toutes les instances de lecteur dans la même zone de disponibilité

Description

Votre cluster de base de données a toutes les instances de lecteur dans la même zone de disponibilité. Nous vous recommandons de répartir les instances de Reader sur plusieurs zones de disponibilité de votre cluster de base de données.

La distribution augmente la disponibilité de la base de données et améliore le temps de réponse en réduisant la latence du réseau entre les clients et la base de données.

> **Note**
>
> Les résultats de cette vérification sont automatiquement actualisés plusieurs fois par jour et les demandes d'actualisation ne sont pas autorisées. Plusieurs heures peuvent encore être nécessaires pour que les modifications apparaissent. Actuellement, vous ne pouvez pas exclure des ressources de cette vérification.

> **Note**
>
> Lorsqu'une instance ou un cluster de bases de données est arrêté, vous pouvez consulter les recommandations Amazon RDS Trusted Advisor pendant 3 à 5 jours. Après cinq jours, les recommandations ne sont plus disponibles dans Trusted Advisor. Pour consulter les recommandations, ouvrez la console Amazon RDS, puis choisissez Recommendations. Si vous supprimez une instance ou un cluster de bases de données, les recommandations associées à ces instances ou clusters ne sont pas disponibles dans Trusted Advisor ou dans la console de gestion Amazon RDS.

ID de la vérification

`c1qf5bt018`

Critères d'alerte

Rouge : les clusters de base de données ont les instances de lecteur dans la même zone de disponibilité.

Action recommandée

Répartissez les instances du lecteur sur plusieurs zones de disponibilité.

Ressources supplémentaires

Les zones de disponibilité (AZ) sont des emplacements distincts les uns des autres afin de garantir l'isolation en cas de panne dans chaque AWS région. Nous vous recommandons de répartir l'instance principale et les instances de lecteur de votre cluster de base de données sur plusieurs zones de disponibilité afin d'améliorer la disponibilité de votre cluster de base de données. Vous pouvez créer un cluster multi-AZ à l'aide de l'API AWS Management Console AWS CLI, ou Amazon RDS lorsque vous créez le cluster. Vous pouvez modifier le cluster Aurora existant en cluster multi-AZ en ajoutant une nouvelle instance de lecteur et en spécifiant une autre AZ.

Pour plus d'informations, consultez la section Haute disponibilité pour Amazon Aurora.

Colonnes du rapport

- Statut
- Région
- Ressource
- Nom du moteur
- Heure de la dernière modification

La surveillance améliorée des instances de base de données Amazon RDS n'est pas activée

Description

Vérifie si la surveillance améliorée est activée pour vos instances de base de données Amazon RDS.

La surveillance améliorée d'Amazon RDS fournit des métriques en temps réel pour le système d'exploitation sur lequel votre instance de base de données s'exécute. Vous pouvez afficher toutes les métriques système et les informations de processus pour vos instances de base de données Amazon RDS sur la console Amazon RDS. Vous pouvez également personnaliser le tableau de bord. Grâce à la surveillance améliorée, vous avez une visibilité sur l'état de fonctionnement de votre instance Amazon RDS en temps quasi réel, ce qui vous permet de répondre aux problèmes opérationnels plus rapidement.

Vous pouvez spécifier l'intervalle de surveillance souhaité à l'aide du paramètre MonitoringInterval de vos règles. AWS Config

Pour plus d'informations, voir Vue d'ensemble de la surveillance améliorée et Métriques du système d'exploitation dans la surveillance améliorée.

> **Note**
>
> Les résultats de cette vérification sont automatiquement actualisés plusieurs fois par jour et les demandes d'actualisation ne sont pas autorisées. Plusieurs heures peuvent encore être nécessaires pour que les modifications apparaissent. Actuellement, vous ne pouvez pas exclure des ressources de cette vérification.

ID de la vérification

`c18d2gz158`

Source

`AWS Config Managed Rule: rds-enhanced-monitoring-enabled`

Critères d'alerte

Jaune : la surveillance améliorée n'est pas activée ou l'intervalle souhaité n'est pas configuré pour vos instances de base de données Amazon RDS.

Action recommandée

Activez la surveillance améliorée pour vos instances de base de données Amazon RDS afin d'améliorer la visibilité sur l'état de fonctionnement de vos instances Amazon RDS.

Pour plus d'informations, voir Surveillance des métriques du système d'exploitation à l'aide de la surveillance améliorée.

Ressources supplémentaires

Métriques du système d'exploitation dans la surveillance améliorée

Colonnes du rapport

- Statut
- Région

- Ressource
- AWS Config Règle
- Paramètres d'entrée
- Heure de la dernière modification

La mise à l'échelle automatique du stockage est désactivée sur les instances de base de données Amazon RDS

Description

Le dimensionnement automatique du stockage Amazon RDS n'est pas activé pour votre instance de base de données. En cas d'augmentation de la charge de travail de la base de données, le scalage automatique de RDS Storage adapte automatiquement la capacité de stockage sans interruption de service.

> **Note**
>
> Les résultats de cette vérification sont automatiquement actualisés plusieurs fois par jour et les demandes d'actualisation ne sont pas autorisées. Plusieurs heures peuvent encore être nécessaires pour que les modifications apparaissent. Actuellement, vous ne pouvez pas exclure des ressources de cette vérification.

> **Note**
>
> Lorsqu'une instance ou un cluster de bases de données est arrêté, vous pouvez consulter les recommandations Amazon RDS Trusted Advisor pendant 3 à 5 jours. Après cinq jours, les recommandations ne sont plus disponibles dans Trusted Advisor. Pour consulter les recommandations, ouvrez la console Amazon RDS, puis choisissez Recommendations. Si vous supprimez une instance ou un cluster de bases de données, les recommandations associées à ces instances ou clusters ne sont pas disponibles dans Trusted Advisor ou dans la console de gestion Amazon RDS.

ID de la vérification

`c1qf5bt013`

Critères d'alerte

Rouge : le dimensionnement automatique du stockage n'est pas activé sur les instances de base de données.

Action recommandée

Activez le dimensionnement automatique du stockage Amazon RDS avec un seuil de stockage maximal spécifié.

Ressources supplémentaires

Le dimensionnement automatique du stockage Amazon RDS adapte automatiquement la capacité de stockage sans interruption lorsque la charge de travail de la base de données augmente. L'autoscaling du stockage surveille l'utilisation du stockage et augmente automatiquement la capacité lorsque l'utilisation est proche de la capacité de stockage provisionnée. Vous pouvez définir une limite maximale de stockage qu'Amazon RDS peut allouer à l'instance de base de données. La mise à l'échelle automatique du stockage n'entraîne aucun coût supplémentaire. Vous ne payez que pour les ressources Amazon RDS allouées à votre instance de base de données. Nous vous recommandons d'activer le dimensionnement automatique du stockage Amazon RDS.

Pour plus d'informations, consultez Gestion automatique de la capacité avec la scalabilité automatique du stockage Amazon RDS.

Colonnes du rapport

- Statut
- Région
- Ressource
- Valeur recommandée
- Nom du moteur
- Heure de la dernière modification

Les instances de base de données Amazon RDS n'utilisent pas le déploiement multi-AZ

Description

Nous vous recommandons d'utiliser un déploiement multi-AZ. Les déploiements multi-AZ améliorent la disponibilité et la durabilité de l'instance de base de données.

> **Note**
>
> Les résultats de cette vérification sont automatiquement actualisés plusieurs fois par jour et les demandes d'actualisation ne sont pas autorisées. Plusieurs heures peuvent encore être nécessaires pour que les modifications apparaissent. Actuellement, vous ne pouvez pas exclure des ressources de cette vérification.

> **Note**
>
> Lorsqu'une instance ou un cluster de bases de données est arrêté, vous pouvez consulter les recommandations Amazon RDS Trusted Advisor pendant 3 à 5 jours. Après cinq jours, les recommandations ne sont plus disponibles dans Trusted Advisor. Pour consulter les recommandations, ouvrez la console Amazon RDS, puis choisissez Recommendations. Si vous supprimez une instance ou un cluster de bases de données, les recommandations associées à ces instances ou clusters ne sont pas disponibles dans Trusted Advisor ou dans la console de gestion Amazon RDS.

ID de la vérification

`c1qf5bt019`

Critères d'alerte

Jaune : les instances de base de données n'utilisent pas le déploiement multi-AZ.

Action recommandée

Configurez Multi-AZ pour les instances de base de données concernées.

Ressources supplémentaires

Dans un déploiement Amazon RDS Multi-AZ, Amazon RDS crée automatiquement une instance de base de données principale et réplique les données sur une instance située dans une autre zone de disponibilité. Lorsqu'il détecte une panne, Amazon RDS bascule automatiquement vers une instance de secours sans intervention manuelle.

Pour plus d’informations, consultez Tarification d’.

Colonnes du rapport

- Statut

- Région
- Ressource
- Nom du moteur
- Heure de la dernière modification

Amazon RDS DiskQueueDepth

Description

Vérifie si la CloudWatch métrique DiskQueueDepth indique que le nombre d'écritures en file d'attente dans le stockage de la base de données de l'instance RDS a atteint un niveau tel qu'une enquête opérationnelle doit être suggérée.

ID de la vérification

`Cmsvnj8db3`

Critères d'alerte

- Rouge : la DiskQueueDepth CloudWatch métrique a dépassé 10
- Jaune : la DiskQueueDepth CloudWatch métrique est supérieure à 5 mais inférieure ou égale à 10
- Vert : la DiskQueueDepth CloudWatch métrique est inférieure ou égale à 5

Action recommandée

Passez à des instances et à des volumes de stockage compatibles avec les caractéristiques de lecture/écriture.

Colonnes du rapport

- Statut
- Région
- ARN d'instance de base de données
- DiskQueueDepth Métrique

Amazon RDS FreeStorageSpace

Description

Vérifie si la FreeStorageSpace CloudWatch métrique d'une instance de base de données RDS a dépassé un seuil raisonnable du point de vue opérationnel.

ID de la vérification

`Cmsvnj8db2`

Critères d'alerte

- Rouge : FreeStorageSpace a atteint/dépassé 90 % de la capacité totale
- Jaune : FreeStorageSpace entre 80 % et 90 % de la capacité totale
- Vert : FreeStorageSpace représente moins de 80 % de la capacité totale

Action recommandée

Augmentez l'espace de stockage pour l'instance de base de données RDS qui manque de stockage disponible à l'aide de la console de gestion Amazon RDS, de l'API Amazon RDS ou de l'interface de ligne de commande AWS.

Colonnes du rapport

- Statut
- Région
- ARN d'instance de base de données
- FreeStorageSpace Métrique (Mo)
- Stockage alloué à l'instance de base de données (Mo)
- Pourcentage d'utilisation du stockage de l'instance de base de données

Le paramètre log_output d'Amazon RDS est défini sur table

Description

Lorsque log_output est défini sur TABLE, plus d'espace de stockage est utilisé que lorsque log_output est défini sur FILE. Nous vous recommandons de définir le paramètre sur FILE, afin d'éviter d'atteindre la limite de taille de stockage.

> **Note**
>
> Les résultats de cette vérification sont automatiquement actualisés plusieurs fois par jour et les demandes d'actualisation ne sont pas autorisées. Plusieurs heures peuvent encore être nécessaires pour que les modifications apparaissent. Actuellement, vous ne pouvez pas exclure des ressources de cette vérification.

> **Note**
>
> Lorsqu'une instance ou un cluster de bases de données est arrêté, vous pouvez consulter les recommandations Amazon RDS Trusted Advisor pendant 3 à 5 jours. Après cinq jours, les recommandations ne sont plus disponibles dans Trusted Advisor. Pour consulter les recommandations, ouvrez la console Amazon RDS, puis choisissez Recommendations. Si vous supprimez une instance ou un cluster de bases de données, les recommandations associées à ces instances ou clusters ne sont pas disponibles dans Trusted Advisor ou dans la console de gestion Amazon RDS.

ID de la vérification

`c1qf5bt023`

Critères d'alerte

Jaune : le paramètre log_output est défini sur TABLE pour les groupes de paramètres de base de données.

Action recommandée

Définissez la valeur du paramètre log_output sur FILE dans vos groupes de paramètres de base de données.

Ressources supplémentaires

Pour plus d'informations, consultez les fichiers journaux de base de données MySQL.

Colonnes du rapport

- Statut
- Région
- Ressource

- Nom du paramètre
- Valeur recommandée
- Heure de la dernière modification

Le réglage du paramètre innodb_default_row_format d'Amazon RDS n'est pas sûr

Description

Votre instance de base de données rencontre un problème connu : une table créée dans une version de MySQL inférieure à 8.0.26 avec le paramètre row_format défini sur COMPACT ou REDONDANT est inaccessible et irrécupérable lorsque l'index dépasse 767 octets.

Nous vous recommandons de définir la valeur du paramètre innodb_default_row_format sur DYNAMIC.

> **Note**
>
> Les résultats de cette vérification sont automatiquement actualisés plusieurs fois par jour et les demandes d'actualisation ne sont pas autorisées. Plusieurs heures peuvent encore être nécessaires pour que les modifications apparaissent. Actuellement, vous ne pouvez pas exclure des ressources de cette vérification.

> **Note**
>
> Lorsqu'une instance ou un cluster de bases de données est arrêté, vous pouvez consulter les recommandations Amazon RDS Trusted Advisor pendant 3 à 5 jours. Après cinq jours, les recommandations ne sont plus disponibles dans Trusted Advisor. Pour consulter les recommandations, ouvrez la console Amazon RDS, puis choisissez Recommendations. Si vous supprimez une instance ou un cluster de bases de données, les recommandations associées à ces instances ou clusters ne sont pas disponibles dans Trusted Advisor ou dans la console de gestion Amazon RDS.

ID de la vérification

`c1qf5bt036`

Critères d'alerte

Rouge : les groupes de paramètres de base de données ont un paramètre non sécurisé pour le paramètre innodb_default_row_format.

Action recommandée

Définissez le paramètre innodb_default_row_format sur DYNAMIC.

Ressources supplémentaires

Lorsqu'une table est créée avec une version de MySQL inférieure à 8.0.26 avec row_format défini sur COMPACT ou REDONDANT, la création d'index avec un préfixe de clé inférieur à 767 octets n'est pas obligatoire. Après le redémarrage de la base de données, il est impossible d'accéder à ces tables ni de les récupérer.

Pour plus d'informations, consultez Modifications apportées à MySQL 8.0.26 (20/07/2021, disponibilité générale) n sur le site Web de documentation MySQL.

Colonnes du rapport

- Statut
- Région
- Ressource
- Nom du paramètre
- Valeur recommandée
- Heure de la dernière modification

Le paramètre Amazon RDS innodb_flush_log_at_trx_commit n'est pas 1

Description

La valeur du paramètre innodb_flush_log_at_trx_commit de votre instance de base de données n'est pas une valeur sûre. Ce paramètre contrôle la persistance des opérations de validation sur le disque.

Nous vous recommandons de définir le paramètre innodb_flush_log_at_trx_commit sur 1.

> **Note**
>
> Les résultats de cette vérification sont automatiquement actualisés plusieurs fois par jour et les demandes d'actualisation ne sont pas autorisées. Plusieurs heures peuvent encore

être nécessaires pour que les modifications apparaissent. Actuellement, vous ne pouvez pas exclure des ressources de cette vérification.

> **Note**
>
> Lorsqu'une instance ou un cluster de bases de données est arrêté, vous pouvez consulter les recommandations Amazon RDS Trusted Advisor pendant 3 à 5 jours. Après cinq jours, les recommandations ne sont plus disponibles dans Trusted Advisor. Pour consulter les recommandations, ouvrez la console Amazon RDS, puis choisissez Recommendations. Si vous supprimez une instance ou un cluster de bases de données, les recommandations associées à ces instances ou clusters ne sont pas disponibles dans Trusted Advisor ou dans la console de gestion Amazon RDS.

ID de la vérification

`c1qf5bt030`

Critères d'alerte

Jaune : innodb_flush_log_at_trx_commit est défini sur une valeur différente de 1 pour les groupes de paramètres de base de données.

Action recommandée

Définissez la valeur du paramètre innodb_flush_log_at_trx_commit sur 1

Ressources supplémentaires

La transaction de base de données est durable lorsque la mémoire tampon est enregistrée dans le stockage durable. Cependant, l'enregistrement sur le disque a un impact sur les performances. En fonction de la valeur définie pour le paramètre innodb_flush_log_at_trx_commit, le comportement de la manière dont les journaux sont écrits et enregistrés sur le disque peut varier.

- Lorsque la valeur du paramètre est 1, les journaux sont écrits et enregistrés sur le disque après chaque transaction validée.
- Lorsque la valeur du paramètre est 0, les journaux sont écrits et enregistrés sur le disque une fois par seconde.

- Lorsque la valeur du paramètre est 2, les journaux sont écrits après la validation de chaque transaction et enregistrés sur le disque une fois par seconde. Les données sont transférées de la mémoire tampon InnoDB vers le cache du système d'exploitation qui se trouve également dans la mémoire.

> **Note**
>
> Lorsque la valeur du paramètre n'est pas 1, InnoDB ne garantit pas les propriétés ACID. Les transactions récentes de la dernière seconde peuvent être perdues en cas de panne de la base de données.

Pour plus d'informations, consultez Bonnes pratiques de configuration des paramètres pour Amazon RDS for MySQL, partie 1 : Paramètres liés aux performances.

Colonnes du rapport

- Statut
- Région
- Ressource
- Nom du paramètre
- Valeur recommandée
- Heure de la dernière modification

Le paramètre max_user_connections d'Amazon RDS est faible

Description

Votre instance de base de données a une valeur faible pour le nombre maximal de connexions simultanées pour chaque compte de base de données.

Nous recommandons de définir le paramètre max_user_connections sur un nombre supérieur à 5.

> **Note**
>
> Les résultats de cette vérification sont automatiquement actualisés plusieurs fois par jour et les demandes d'actualisation ne sont pas autorisées. Plusieurs heures peuvent encore

être nécessaires pour que les modifications apparaissent. Actuellement, vous ne pouvez pas exclure des ressources de cette vérification.

> **Note**
>
> Lorsqu'une instance ou un cluster de bases de données est arrêté, vous pouvez consulter les recommandations Amazon RDS Trusted Advisor pendant 3 à 5 jours. Après cinq jours, les recommandations ne sont plus disponibles dans Trusted Advisor. Pour consulter les recommandations, ouvrez la console Amazon RDS, puis choisissez Recommendations. Si vous supprimez une instance ou un cluster de bases de données, les recommandations associées à ces instances ou clusters ne sont pas disponibles dans Trusted Advisor ou dans la console de gestion Amazon RDS.

ID de la vérification

`c1qf5bt034`

Critères d'alerte

Jaune : max_user_connections est mal configuré pour les groupes de paramètres de base de données.

Action recommandée

Augmentez la valeur du paramètre max_user_connections à un nombre supérieur à 5.

Ressources supplémentaires

Le paramètre max_user_connections contrôle le nombre maximum de connexions simultanées autorisées pour un compte utilisateur MySQL. L'atteinte de cette limite de connexion entraîne des échecs dans les opérations d'administration des instances Amazon RDS, telles que la sauvegarde, l'application de correctifs et les modifications de paramètres.

Pour plus d'informations, consultez la section Définition des limites de ressources du compte sur le site Web de documentation MySQL.

Colonnes du rapport

- Statut
- Région
- Ressource

- Nom du paramètre
- Valeur recommandée
- Heure de la dernière modification

Amazon RDS Multi-AZ

Description

Vérifie les instances de base de données déployées dans une seule zone de disponibilité (AZ).

Les déploiements multi-AZ améliorent la disponibilité de la base de données en effectuant une réplication synchrone vers une instance de secours dans une zone de disponibilité différente. Au cours de la maintenance planifiée de la base de données ou en cas d'échec d'une instance de base de données ou d'une zone de disponibilité, Amazon RDS passe automatiquement à l'instance de secours. Ce basculement permet de reprendre rapidement les opérations de base de données sans intervention administrative. Étant donné qu'Amazon RDS ne prend pas en charge le déploiement multi-AZ pour Microsoft SQL Server, cette vérification n'examine pas les instances SQL Server.

ID de la vérification

`f2iK5R6Dep`

Critères d'alerte

Jaune : une instance de base de données est déployée dans une seule zone de disponibilité.

Action recommandée

Si votre application nécessite une disponibilité élevée, modifiez votre instance de base de données pour activer le déploiement multi-AZ. Consultez High Availability (Multi-AZ) (Haute disponibilité (Multi-AZ)).

Ressources supplémentaires

Régions et zones de disponibilité

Colonnes du rapport

- Statut
- Région/zone de disponibilité
- instance de base de données
- ID du VPC

- Multi-AZ

Amazon RDS n'est pas inclus dans le plan AWS Backup

Description

Vérifie si vos instances de base de données Amazon RDS sont incluses dans un plan de sauvegarde dans AWS Backup.

AWS Backup est un service de sauvegarde entièrement géré qui facilite la centralisation et l'automatisation de la sauvegarde des données entre les AWS services.

L'ajout de votre instance de base de données Amazon RDS à un plan de sauvegarde est important au regard des obligations de conformité réglementaire, de la reprise après sinistre, des politiques de l'entreprise en matière de protection des données et des objectifs de continuité des activités.

Pour plus d'informations, voir Qu'est-ce que AWS Backup ?.

> **Note**
>
> Les résultats de cette vérification sont automatiquement actualisés plusieurs fois par jour et les demandes d'actualisation ne sont pas autorisées. Plusieurs heures peuvent encore être nécessaires pour que les modifications apparaissent. Actuellement, vous ne pouvez pas exclure des ressources de cette vérification.

ID de la vérification

```
c18d2gz159
```

Source

```
AWS Config Managed Rule: rds-in-backup-plan
```

Critères d'alerte

Jaune : une instance de base de données Amazon RDS n'est pas incluse dans un plan de sauvegarde avec AWS Backup.

Action recommandée

Incluez vos instances de base de données Amazon RDS dans un plan de sauvegarde avec AWS Backup.

Pour plus d'informations, voir Sauvegarde et restauration d'Amazon RDS à l'aide d'AWS Backup.

Ressources supplémentaires

Affectation de ressources à un plan de sauvegarde

Colonnes du rapport

- Statut
- Région
- Ressource
- AWS Config Règle
- Paramètres d'entrée
- Heure de la dernière modification

Les répliques Amazon RDS Read sont ouvertes en mode inscriptible

Description

Votre instance de base de données possède une réplique en lecture en mode inscriptible, qui permet les mises à jour par les clients.

Nous vous recommandons de définir le paramètre read_only sur TrueIfReplicaafin que les répliques en lecture ne soient pas en mode inscriptible.

> **Note**
>
> Les résultats de cette vérification sont automatiquement actualisés plusieurs fois par jour et les demandes d'actualisation ne sont pas autorisées. Plusieurs heures peuvent encore être nécessaires pour que les modifications apparaissent. Actuellement, vous ne pouvez pas exclure des ressources de cette vérification.

> **Note**
>
> Lorsqu'une instance ou un cluster de bases de données est arrêté, vous pouvez consulter les recommandations Amazon RDS Trusted Advisor pendant 3 à 5 jours. Après cinq jours, les recommandations ne sont plus disponibles dans Trusted Advisor. Pour consulter les recommandations, ouvrez la console Amazon RDS, puis choisissez Recommendations. Si vous supprimez une instance ou un cluster de bases de données, les recommandations associées à ces instances ou clusters ne sont pas disponibles dans Trusted Advisor ou dans la console de gestion Amazon RDS.

ID de la vérification

`c1qf5bt035`

Critères d'alerte

Jaune : les groupes de paramètres de base de données activent le mode inscriptible pour les répliques lues.

Action recommandée

Définissez la valeur du paramètre read_only sur. TrueIfReplica

Ressources supplémentaires

Le paramètre read_only contrôle l'autorisation d'écriture accordée par les clients à une instance de base de données. La valeur par défaut de ce paramètre est TrueIfReplica. Pour une instance de réplique, TrueIfReplicadéfinit la valeur read_only sur ON (1) et désactive toute activité d'écriture provenant des clients. Pour une instance maître/scripteur, TrueIfReplicadéfinit la valeur sur OFF (0) et active l'activité d'écriture des clients pour l'instance. Lorsque la réplique en lecture est ouverte en mode inscriptible, les données stockées dans cette instance peuvent diverger de celles de l'instance principale, ce qui entraîne des erreurs de réplication.

Pour plus d'informations, consultez la section Meilleures pratiques de configuration des paramètres pour Amazon RDS for MySQL, partie 2 : Paramètres liés à la réplication sur le site Web de documentation MySQL.

Colonnes du rapport

- Statut
- Région

- Ressource
- Nom du paramètre
- Valeur recommandée
- Heure de la dernière modification

Les sauvegardes automatisées des ressources Amazon RDS sont désactivées

Description

Les sauvegardes automatisées sont désactivées sur vos ressources de base de données. Les sauvegardes automatisées permettent de point-in-time restaurer votre instance de base de données.

> **Note**
>
> Les résultats de cette vérification sont automatiquement actualisés plusieurs fois par jour et les demandes d'actualisation ne sont pas autorisées. Plusieurs heures peuvent encore être nécessaires pour que les modifications apparaissent. Actuellement, vous ne pouvez pas exclure des ressources de cette vérification.

> **Note**
>
> Lorsqu'une instance ou un cluster de bases de données est arrêté, vous pouvez consulter les recommandations Amazon RDS Trusted Advisor pendant 3 à 5 jours. Après cinq jours, les recommandations ne sont plus disponibles dans Trusted Advisor. Pour consulter les recommandations, ouvrez la console Amazon RDS, puis choisissez Recommendations. Si vous supprimez une instance ou un cluster de bases de données, les recommandations associées à ces instances ou clusters ne sont pas disponibles dans Trusted Advisor ou dans la console de gestion Amazon RDS.

ID de la vérification

`c1qf5bt001`

Critères d'alerte

Rouge : les sauvegardes automatiques ne sont pas activées sur les ressources Amazon RDS

Action recommandée

Activez les sauvegardes automatisées avec une période de conservation allant jusqu'à 14 jours.

Ressources supplémentaires

Les sauvegardes automatisées permettent de point-in-time restaurer vos instances de base de données. Nous vous recommandons d'activer les sauvegardes automatisées. Lorsque vous activez les sauvegardes automatisées pour une instance de base de données, Amazon RDS effectue automatiquement une sauvegarde complète de vos données quotidiennement pendant la fenêtre de sauvegarde de votre choix. La sauvegarde capture les journaux de transactions lorsque votre instance de base de données est mise à jour. Vous bénéficiez d'un stockage de sauvegarde jusqu'à la taille de stockage de votre instance de base de données sans frais supplémentaires.

Pour plus d’informations, consultez les ressources suivantes :

- Activation des sauvegardes automatisées
- Démystifier les coûts de stockage des sauvegardes Amazon RDS

Colonnes du rapport

- Statut
- Région
- Ressource
- Valeur recommandée
- Nom du moteur
- Heure de la dernière modification

Le paramètre sync_binlog d'Amazon RDS est désactivé

Description

La synchronisation du journal binaire avec le disque n'est pas appliquée avant que les validations des transactions ne soient reconnues dans votre instance de base de données.

Nous vous recommandons de définir la valeur du paramètre sync_binlog sur 1.

> **Note**
>
> Les résultats de cette vérification sont automatiquement actualisés plusieurs fois par jour et les demandes d'actualisation ne sont pas autorisées. Plusieurs heures peuvent encore être nécessaires pour que les modifications apparaissent. Actuellement, vous ne pouvez pas exclure des ressources de cette vérification.

> **Note**
>
> Lorsqu'une instance ou un cluster de bases de données est arrêté, vous pouvez consulter les recommandations Amazon RDS Trusted Advisor pendant 3 à 5 jours. Après cinq jours, les recommandations ne sont plus disponibles dans Trusted Advisor. Pour consulter les recommandations, ouvrez la console Amazon RDS, puis choisissez Recommendations. Si vous supprimez une instance ou un cluster de bases de données, les recommandations associées à ces instances ou clusters ne sont pas disponibles dans Trusted Advisor ou dans la console de gestion Amazon RDS.

ID de la vérification

`c1qf5bt031`

Critères d'alerte

Jaune : la journalisation binaire synchrone des groupes de paramètres de base de données est désactivée.

Action recommandée

Définissez le paramètre sync_binlog sur 1.

Ressources supplémentaires

Le paramètre sync_binlog contrôle la façon dont MySQL envoie le journal binaire sur le disque. Lorsque la valeur de ce paramètre est définie sur 1, il active la synchronisation du journal binaire avec le disque avant que les transactions ne soient validées. Lorsque la valeur de ce paramètre est définie sur 0, la synchronisation du journal binaire avec le disque est désactivée. Généralement, le serveur MySQL dépend du système d'exploitation pour transférer régulièrement le journal binaire sur le disque, comme c'est le cas pour les autres fichiers. La valeur du paramètre sync_binlog définie sur 0 peut améliorer les performances. Cependant, lors d'une

panne de courant ou d'un crash du système d'exploitation, le serveur perd toutes les transactions validées qui n'ont pas été synchronisées avec les journaux binaires.

Pour plus d'informations, consultez Bonnes pratiques de configuration des paramètres pour Amazon RDS for MySQL, partie 2 : Paramètres liés à la réplication.

Colonnes du rapport

- Statut
- Région
- Ressource
- Nom du paramètre
- Valeur recommandée
- Heure de la dernière modification

Aucune réplication multi-AZ n'est activée pour le cluster de base de données RDS

Description

Vérifie si la réplication multi-AZ est activée pour vos clusters de base de données Amazon RDS.

Un cluster de base de données multi-AZ compte une instance de base de données d'écriture et deux instances de base de données de lecture dans trois zones de disponibilité distinctes. Les clusters de base de données multi-AZ offrent une haute disponibilité, une capacité accrue pour les charges de travail en lecture et une moindre latence par rapport aux déploiements multi-AZ.

Pour plus d'informations, voir Création d'un cluster de base de données multi-AZ.

> **Note**
>
> Les résultats de cette vérification sont automatiquement actualisés plusieurs fois par jour et les demandes d'actualisation ne sont pas autorisées. Plusieurs heures peuvent encore être nécessaires pour que les modifications apparaissent. Actuellement, vous ne pouvez pas exclure des ressources de cette vérification.

ID de la vérification

`c18d2gz161`

Source

```
AWS Config Managed Rule: rds-cluster-multi-az-enabled
```

Critères d'alerte

Jaune : la réplication multi-AZ n'est pas configurée pour votre cluster de base de données Amazon RDS.

Action recommandée

Activez le déploiement de cluster de bases de données multi-AZ lorsque vous créez un cluster de bases de données Amazon RDS.

Pour plus d'informations, voir Création d'un cluster de base de données multi-AZ.

Ressources supplémentaires

Déploiements de clusters de base de données multi-AZ

Colonnes du rapport

- Statut
- Région
- Ressource
- AWS Config Règle
- Paramètres d'entrée
- Heure de la dernière modification

Instance de secours RDS Multi-AZ non activée

Description

Vérifie si un réplica de secours multi-AZ est configuré sur vos instances de base de données Amazon RDS.

Amazon RDS Multi-AZ permet une disponibilité et une durabilité élevées des instances de base de données en répliquant les données sur un réplica de secours dans une zone de disponibilité différente. Cela permet un basculement automatique et améliore les performances et la durabilité des données. Dans un déploiement d'instance de base de données multi-AZ, Amazon RDS alloue et maintient automatiquement un réplica de secours synchrone dans une zone de disponibilité

différente. L'instance de base de données primaire est répliquée de manière synchrone dans les zones de disponibilité sur un réplica de secours afin d'assurer une redondance des données et de limiter les pics de latence lors des sauvegardes système. L'exécution d'une instance de base de données haute disponibilité peut améliorer la disponibilité lors de la maintenance planifiée du système. Elle peut également contribuer à protéger vos bases de données contre la défaillance d'une instance de base de données et la perturbation d'une zone de disponibilité.

Pour plus d'informations, voir Déploiements d'instances de bases de données multi-AZ.

> **Note**
>
> Les résultats de cette vérification sont automatiquement actualisés plusieurs fois par jour et les demandes d'actualisation ne sont pas autorisées. Plusieurs heures peuvent encore être nécessaires pour que les modifications apparaissent. Actuellement, vous ne pouvez pas exclure des ressources de cette vérification.

ID de la vérification

`c18d2gz156`

Source

`AWS Config Managed Rule: rds-multi-az-support`

Critères d'alerte

Jaune : aucun réplica multi-AZ n'est configuré pour une instance de base de données Amazon RDS.

Action recommandée

Activez le déploiement multi-AZ lorsque vous créez une instance de bases de données Amazon RDS.

Cette vérification ne peut pas être exclue de la vue dans la Trusted Advisor console.

Ressources supplémentaires

Déploiements d'instances de base de données multi-AZ

Colonnes du rapport

- Statut

- Région
- Ressource
- AWS Config Règle
- Paramètres d'entrée
- Heure de la dernière modification

Amazon RDS ReplicaLag

Description

Vérifie si la ReplicaLag CloudWatch métrique d'une instance de base de données RDS a dépassé un seuil raisonnable du point de vue opérationnel au cours de la semaine écoulée.

ReplicaLag métrique mesure le nombre de secondes pendant lesquelles une réplique en lecture se trouve derrière l'instance principale. Le délai de réplication se produit lorsque le réplica en lecture ne peut pas être mis à jour au même rythme que l'instance de base de données principale. En cas de défaillance de l'instance principale, des données peuvent être absentes de la réplique lue si le seuil ReplicaLag est supérieur à un seuil raisonnable du point de vue opérationnel.

ID de la vérification

`Cmsvnj8db1`

Critères d'alerte

- Rouge : la ReplicaLag métrique a dépassé 60 secondes au moins une fois par semaine.
- Jaune : la ReplicaLag métrique a dépassé 10 secondes au moins une fois par semaine.
- Vert : ReplicaLag durée inférieure à 10 secondes.

Action recommandée

Plusieurs causes peuvent expliquer cette augmentation au-delà ReplicaLag des niveaux sûrs sur le plan opérationnel. Par exemple, cela peut être dû à des instances de réplicas récemment remplacées/lancées à partir d'anciennes sauvegardes, car ces réplicas mettent souvent un certain temps à se « resynchroniser » avec l'instance de base de données principale et les transactions en direct. Cela ReplicaLag peut diminuer au fil du temps à mesure que le rattrapage se produit. Autre exemple, la vitesse de transaction pouvant être atteinte sur l'instance de base de données principale est supérieure à celle du processus de réplication ou à celle de l'infrastructure de réplica. Ce chiffre ReplicaLag peut augmenter au fil du temps, car la réplication ne parvient pas à suivre le rythme des performances de la base de données principale. Enfin, la charge de travail

peut être excessive à différentes périodes de la journée/du mois/etc., ce qui entraîne parfois des retards. ReplicaLag Votre équipe doit déterminer quelle cause première possible a contribué au niveau élevé ReplicaLag de la base de données, et éventuellement modifier le type d'instance de base de données ou d'autres caractéristiques de la charge de travail afin de garantir que la continuité des données sur la réplique répond à vos besoins.

Ressources supplémentaires

- Utilisation de réplicas en lecture pour Amazon RDS for PostgreSQL
- Utilisation de la réplication MySQL dans Amazon RDS
- Utilisation de réplicas en lecture MySQL

Colonnes du rapport

- Statut
- Région
- ARN d'instance de base de données
- ReplicaLag Métrique

Le paramètre synchronous_commit d'Amazon RDS est désactivé

Description

Lorsque le paramètre synchronous_commit est désactivé, des données peuvent être perdues en cas de panne de base de données. La durabilité de la base de données est menacée.

Nous vous recommandons d'activer le paramètre synchronous_commit.

> **Note**
>
> Les résultats de cette vérification sont automatiquement actualisés plusieurs fois par jour et les demandes d'actualisation ne sont pas autorisées. Plusieurs heures peuvent encore être nécessaires pour que les modifications apparaissent. Actuellement, vous ne pouvez pas exclure des ressources de cette vérification.

> **Note**
>
> Lorsqu'une instance ou un cluster de bases de données est arrêté, vous pouvez consulter les recommandations Amazon RDS Trusted Advisor pendant 3 à 5 jours. Après cinq jours,

les recommandations ne sont plus disponibles dans Trusted Advisor. Pour consulter les recommandations, ouvrez la console Amazon RDS, puis choisissez Recommendations. Si vous supprimez une instance ou un cluster de bases de données, les recommandations associées à ces instances ou clusters ne sont pas disponibles dans Trusted Advisor ou dans la console de gestion Amazon RDS.

ID de la vérification

`c1qf5bt026`

Critères d'alerte

Rouge : le paramètre synchronous_commit est désactivé pour les groupes de paramètres de base de données.

Action recommandée

Activez le paramètre synchronous_commit dans vos groupes de paramètres de base de données.

Ressources supplémentaires

Le paramètre synchronous_commit définit l'achèvement du processus de journalisation par écriture anticipée (WAL) avant que le serveur de base de données n'envoie une notification de réussite au client. Ce commit est appelé commit asynchrone car le client accuse réception du commit avant que WAL n'enregistre la transaction sur le disque. Si le paramètre synchronous_commit est désactivé, les transactions peuvent être perdues, la durabilité de l'instance de base de données peut être compromise et des données peuvent être perdues en cas de panne d'une base de données.

Pour plus d'informations, consultez les fichiers journaux de base de données MySQL.

Colonnes du rapport

- Statut
- Région
- Ressource
- Nom du paramètre
- Valeur recommandée
- Heure de la dernière modification

Instantanés automatisés du cluster Amazon Redshift

Description

Vérifie si les instantanés automatisés sont activés pour vos clusters Amazon Redshift.

Amazon Redshift prend automatiquement des instantanés incrémentaux qui effectuent le suivi des modifications du cluster depuis l'instantané automatique précédent. Les instantanés automatiques conservent toutes les données requises pour restaurer un cluster à partir d'un instantané. Pour désactiver les instantanés automatiques, définissez la période de conservation sur zéro. Vous ne pouvez pas désactiver les instantanés automatisés pour les types de nœuds RA3.

Vous pouvez spécifier les périodes de conservation minimale et maximale souhaitées à l'aide du MaxRetentionPeriodparamètre MinRetentionPeriodet de vos AWS Config règles.

Instantanés et sauvegardes Amazon Redshift

> **Note**
>
> Les résultats de cette vérification sont automatiquement actualisés plusieurs fois par jour et les demandes d'actualisation ne sont pas autorisées. Plusieurs heures peuvent encore être nécessaires pour que les modifications apparaissent. Actuellement, vous ne pouvez pas exclure des ressources de cette vérification.

ID de la vérification

`c18d2gz135`

Source

`AWS Config Managed Rule: redshift-backup-enabled`

Critères d'alerte

Rouge : les instantanés automatisés ne sont pas configurés sur la période de conservation souhaitée pour Amazon Redshift.

Action recommandée

Assurez-vous que les instantanés automatisés sont activés pour vos clusters Amazon Redshift.

Pour plus d'informations, consultez Gestion des instantanés à l'aide de la console.

Ressources supplémentaires

Instantanés et sauvegardes Amazon Redshift

Pour plus d'informations, consultez la page Utilisation des sauvegardes.

Colonnes du rapport

- Statut
- Région
- Ressource
- AWS Config Règle
- Paramètres d'entrée
- Heure de la dernière modification

Surveillances des états supprimées Amazon Route 53

Description

Vérifie les jeux d'enregistrements de ressource associés à des surveillances de l'état ayant été supprimées.

Route 53 ne vous empêche pas de supprimer une surveillance de l'état, même si elle est associée à un ou plusieurs enregistrements de ressource. Si vous supprimez une surveillance de l'état sans mettre à jour les jeux d'enregistrements de ressource associés, le routage des requêtes DNS pour votre configuration de basculement DNS ne fonctionnera pas comme prévu.

Les zones hébergées créées par AWS les services n'apparaîtront pas dans les résultats de votre vérification.

ID de la vérification

`Cb877eB72b`

Critères d'alerte

Jaune : un ensemble d'enregistrements de ressources est associé à une surveillance de l'état qui a été supprimée.

Action recommandée

Créez une nouvelle surveillance de l'état et associez-la à l'ensemble d'enregistrements de ressources. Consultez Création, mise à jour et suppression des surveillances de l'état et Adding

Health Checks to Resource Record Sets (Ajout de surveillances de l'état à des ensembles d'enregistrements de ressources).

Ressources supplémentaires

- Surveillances de l'état Amazon Route 53 et basculement DNS
- Fonctionnement des surveillance de l'état dans les configurations Amazon Route 53 simples

Colonnes du rapport

- Nom de la zone hébergée
- ID de la zone hébergée
- Nom de l'ensemble d'enregistrements de ressources
- Type d'ensemble d'enregistrements de ressources
- Identifiant d'un ensemble d'enregistrements de ressources

Jeux d'enregistrements de ressource de basculement dans Amazon Route 53.

Description

Vérifie les jeux d'enregistrements de ressource de basculement Amazon Route 53 mal configurés.

Lorsque les surveillances de l'état Amazon Route 53 déterminent que la ressource principale n'est pas intègre, Amazon Route 53 répond aux requêtes avec un jeu d'enregistrements de ressource de sauvegarde secondaire. Vous devez créer des jeux d'enregistrements de ressource principaux et secondaires correctement configurés pour que le basculement fonctionne.

Les zones hébergées créées par AWS les services n'apparaîtront pas dans les résultats de votre vérification.

ID de la vérification

`b73EEdD790`

Critères d'alerte

- Jaune : un ensemble d'enregistrements de ressources de basculement principal ne possède pas d'ensemble d'enregistrements de ressources secondaire correspondant.
- Jaune : un ensemble d'enregistrements de ressources de basculement secondaire ne possède pas d'ensemble d'enregistrements de ressources principal correspondant.
- Jaune : les ensembles d'enregistrements de ressources principaux et secondaires qui ont le même nom sont associés à la même surveillance de l'état.

Action recommandée

S'il manque un ensemble de ressources de basculement, créez l'ensemble d'enregistrements de ressources correspondant. Voir Creating Failover Resource Record Sets (Création d'ensembles d'enregistrements de ressources de basculement).

Si vos ensembles d'enregistrements de ressources sont associés à la même surveillance de l'état, créez des surveillances de l'état distincts pour chacun d'eux. Voir Création, mise à jour et suppression de surveillance de l'état.

Ressources supplémentaires

Surveillances de l'état Amazon Route 53 et basculement DNS

Colonnes du rapport

- Nom de la zone hébergée
- ID de la zone hébergée
- Nom de l'ensemble d'enregistrements de ressources
- Type d'ensemble d'enregistrements de ressources
- Raison

Jeux d'enregistrements de ressource ayant une durée de vie élevée Amazon Route 53

Description

Vérifie les ensembles d'enregistrements de ressources qui peuvent bénéficier d'une valeur inférieure time-to-live (TTL).

TTL représente le nombre de secondes pendant lesquelles un jeu d'enregistrements de ressource est mis en cache par les résolveurs DNS. Lorsque vous spécifiez une longue durée de vie, les résolveurs DNS prennent plus de temps pour demander des enregistrements DNS mis à jour, ce qui peut entraîner un retard inutile dans le réacheminement du trafic. Par exemple, une longue durée de vie crée un délai entre le moment où le basculement DNS détecte un échec du point de terminaison et le moment où il réagit en réacheminant le trafic.

Les zones hébergées créées par AWS les services n'apparaîtront pas dans les résultats de votre vérification.

ID de la vérification

`C056F80cR3`

Critères d'alerte

- Jaune : un ensemble d'enregistrements de ressources dont la politique de routage est Basculement a une durée de vie supérieure à 60 secondes.
- Jaune : un ensemble d'enregistrements de ressources avec une surveillance de l'état associée a une durée de vie supérieure à 60 secondes.

Action recommandée

Saisissez une valeur de durée de vie de 60 secondes pour les ensembles d'enregistrements de ressources répertoriés. Pour plus d'informations, consultez Working with Resource Record Sets (Utilisation d'ensembles d'enregistrements de ressources).

Ressources supplémentaires

Surveillances de l'état Amazon Route 53 et basculement DNS

Colonnes du rapport

- Statut
- Nom de la zone hébergée
- ID de la zone hébergée
- Nom de l'ensemble d'enregistrements de ressources
- Type d'ensemble d'enregistrements de ressources
- ID de l'ensemble d'enregistrements de ressources
- TTL

Délégations du serveur de noms Amazon Route 53

Description

Vérifie les zones hébergées Amazon Route 53 pour lesquelles votre registre de domaine ou DNS n'utilise pas les bons serveurs de noms Route 53.

Lorsque vous créez une zone hébergée, Route 53 attribue un ensemble de quatre serveurs de noms. Les noms de ces serveurs sont ns-###.awsdns-##.com, .net, .org et .co.uk, où ### et ## représentent généralement des nombres différents. Avant que Route 53 puisse acheminer des requêtes DNS pour votre domaine, vous devez mettre à jour la configuration du serveur de noms de votre bureau d'enregistrement afin de supprimer les serveurs de noms affectés par ce dernier. Ensuite, vous devez ajouter les quatre serveurs de noms dans l'ensemble de délégations Route 53. Pour une disponibilité maximale, vous devez ajouter les quatre serveurs de noms Route 53.

Les zones hébergées créées par AWS les services n'apparaîtront pas dans les résultats de votre vérification.

ID de la vérification

`cF171Db240`

Critères d'alerte

Jaune : zone hébergée pour laquelle le bureau d'enregistrement de votre domaine n'utilise pas les quatre serveurs de noms Route 53 de l'ensemble de délégations.

Action recommandée

Ajoutez ou mettez à jour les enregistrements de serveurs de noms avec votre bureau d'enregistrement ou le service DNS actuel de votre domaine afin d'inclure les quatre serveurs de noms dans votre ensemble de délégations Route 53. Pour trouver ces valeurs, consultez Obtention de la liste des serveurs de noms d'une zone hébergée publique. Pour plus d'informations sur l'ajout ou la mise à jour d'enregistrements de serveurs, consultez Création et migration de domaines et de sous-domaines vers Amazon Route 53.

Ressources supplémentaires

Utilisation de zones hébergées

Colonnes du rapport

- Nom de la zone hébergée
- ID de la zone hébergée
- Nombre de délégations de serveurs de noms utilisées

Amazon Route 53 Resolver Redondance de la zone de disponibilité des terminaux

Description

Vérifie si la configuration de votre service comporte des adresses IP spécifiées dans au moins deux zones de disponibilité pour la redondance. Une zone de disponibilité est un emplacement distinct isolé des défaillances dans d'autres zones. En spécifiant des adresses IP dans plusieurs zones de disponibilité d'une même région, vous pouvez protéger vos applications contre un point unique de défaillance.

ID de la vérification

`Chrv231ch1`

Critères d'alerte

- Jaune : les adresses IP ne sont spécifiées que dans une zone de disponibilité.
- Vert : les adresses IP sont spécifiées dans au moins deux zones de disponibilité.

Action recommandée

Spécifiez les adresses IP dans au moins deux zones de disponibilité pour la redondance.

Ressources supplémentaires

- Si vous avez besoin que plus d'un point de terminaison d'Interface réseau Elastic soit disponible à tout moment, nous vous recommandons de créer au moins une interface réseau de plus que nécessaire, afin de vous assurer que vous disposez d'une capacité supplémentaire pour gérer d'éventuelles surtensions de trafic. L'interface réseau supplémentaire assure également la disponibilité pendant les opérations de service, telles que la maintenance ou les mises à niveau.
- Haute disponibilité pour les points de terminaison Resolver

Colonnes du rapport

- Statut
- Région
- ARN des ressources
- Nombre de zones de disponibilité

Journalisation des compartiments Amazon S3

Description

Vérifie la configuration de journalisation des compartiments Amazon Simple Storage Service (Amazon S3).

Lorsque la journalisation des accès au serveur est activée, les journaux d'accès détaillés sont remis toutes les heures dans un compartiment que vous choisissez. Un enregistrement du journal d'accès contient des détails sur la requête, tels que son type, les ressources qui y sont spécifiées, ainsi que l'heure et la date auxquelles elle a été traitée. Par défaut, la journalisation du compartiment n'est pas activée. Vous devez activer la journalisation si vous souhaitez effectuer des audits de sécurité ou en savoir plus sur les utilisateurs et les modèles d'utilisation.

Lorsque la journalisation est initialement activée, la configuration est automatiquement validée. Toutefois, les modifications futures peuvent entraîner des échecs de journalisation. Cette vérification examine les autorisations de compartiment Amazon S3 explicites, mais elle n'examine

pas les politiques de compartiment associées qui pourraient remplacer les autorisations de compartiment.

ID de la vérification

`BueAdJ7NrP`

Critères d'alerte

- Jaune : la journalisation des accès au serveur du compartiment n'est pas activée.
- Jaune : les autorisations du compartiment cible n'incluent pas le compte root, il est donc Trusted Advisor impossible de le vérifier.
- Rouge : le compartiment cible n'existe pas.
- Rouge : le compartiment cible et le compartiment source n'ont pas les mêmes propriétaires.
- Rouge : le livreur de journal ne dispose pas d'autorisations d'écriture pour le compartiment cible.

Action recommandée

Activez la journalisation des compartiments pour la plupart des compartiments. Consultez Enabling Logging Using the Console (Activation de la journalisation à l'aide de la console) et Enabling Logging Programmatically (Activation de la journalisation par programmation).

Si les autorisations du bucket cible n'incluent pas le compte root et que vous Trusted Advisor souhaitez vérifier l'état de journalisation, ajoutez le compte root en tant que bénéficiaire. Voir Editing Bucket Permissions (Modification des autorisations de compartiment).

Si le compartiment cible n'existe pas, sélectionnez un compartiment existant en tant que cible ou créez-en un nouveau et sélectionnez-le. Voir Managing Bucket Logging (Gestion de la journalisation des compartiments).

Si la cible et la source n'ont pas les mêmes propriétaires, remplacez le compartiment cible par un compartiment ayant le même propriétaire que le compartiment source. Voir Managing Bucket Logging (Gestion de la journalisation des compartiments).

Si le livreur de journaux ne dispose pas d'autorisations d'écriture pour la cible (écriture non activée), accordez les autorisations de téléchargement/suppression au groupe de livraison des journaux. Voir Editing Bucket Permissions (Modification des autorisations de compartiment).

Ressources supplémentaires

- Utilisation des compartiments

- Journalisation des accès au serveur
- Format des journaux d'accès au serveur
- Suppression des fichiers journaux

Colonnes du rapport

- Statut
- Région
- Nom du compartiment
- Nom de la cible
- La cible existe
- Même propriétaire
- Écriture activée
- Raison

La réplication de compartiment Amazon S3 n'est pas activée

Description

Vérifie si les règles de réplication de vos compartiments Amazon S3 sont activées pour la réplication entre régions, la réplication dans une même région ou les deux.

La réplication est la copie automatique et asynchrone d'objets entre des compartiments situés dans la même région ou dans des régions différentes. AWS Elle réplique les objets nouvellement créés et les mises à jour d'objets d'un compartiment source vers un ou plusieurs compartiments de destination. Utilisez la réplication de compartiment Amazon S3 pour améliorer la résilience et la conformité de vos applications et de votre stockage de données.

Pour plus d'informations, voir Réplication d'objets.

> **Note**
>
> Les résultats de cette vérification sont automatiquement actualisés plusieurs fois par jour et les demandes d'actualisation ne sont pas autorisées. Plusieurs heures peuvent encore être nécessaires pour que les modifications apparaissent. Actuellement, vous ne pouvez pas exclure des ressources de cette vérification.

ID de la vérification

```
c18d2gz119
```

Source

```
AWS Config Managed Rule: s3-bucket-replication-enabled
```

Critères d'alerte

Jaune : les règles de réplication de vos compartiments Amazon S3 ne sont pas activées pour la réplication entre régions, la réplication dans une même région ou les deux.

Action recommandée

Activez la réplication de compartiment Amazon S3 pour améliorer la résilience et la conformité de vos applications et de votre stockage de données.

Pour plus d'informations, voir Affichage de vos tâches de sauvegarde et de vos points de restauration et Configuration de la réplication.

Ressources supplémentaires

Procédures : exemples de configurations de réplication

Colonnes du rapport

- Statut
- Région
- Ressource
- AWS Config Règle
- Paramètres d'entrée
- Heure de la dernière modification

Amazon S3 Bucket Versioning

Description

Vérifie les compartiments Amazon Simple Storage pour lesquels la gestion des versions est désactivée ou suspendue.

Lorsque la gestion des versions est activée, vous pouvez facilement récupérer les données en cas d'actions involontaires des utilisateurs ou d'échecs des applications. Vous pouvez utiliser

la gestion des versions pour préserver, récupérer et restaurer chaque version de chaque objet stocké dans votre compartiment . Vous pouvez utiliser des règles de cycle de vie pour gérer toutes les versions de vos objets, ainsi que leurs coûts associés, en archivant automatiquement les objets dans la classe de stockage Glacier. Les règles peuvent également être configurées pour supprimer des versions de vos objets après un temps spécifié. Vous pouvez également exiger l'authentification multi-facteur (MFA) pour toute suppression d'objets ou modification de la configuration de vos compartiments.

La gestion des versions ne peut pas être désactivée une fois qu'elle a été activée. Cependant, elle peut être suspendue, ce qui empêche la création de nouvelles versions d'objets. L'utilisation de la gestion des versions peut augmenter vos coûts pour Amazon S3, car vous payez pour le stockage de plusieurs versions d'un même objet.

ID de la vérification

`R365s2Qddf`

Critères d'alerte

- Vert : la gestion des versions est activée pour le compartiment.
- Jaune : la gestion des versions n'est pas activée pour le compartiment.
- Jaune : la gestion des versions est suspendue pour le compartiment.

Action recommandée

Activez la gestion des versions sur la plupart des compartiments afin d'éviter la suppression ou l'écrasement accidentels. Voir Utilisation de la gestion des versions et Enabling Versioning Programmatically (Activation de la gestion des versions par programmation).

Si la gestion des versions du compartiment est suspendue, pensez à la réactiver. Pour plus d'informations sur l'utilisation des objets dans un compartiment dont la gestion des versions est interrompue, consultez Managing Objects in a Versioning-Suspended Bucket (Gestion des objets dans un compartiment dont la gestion des versions est suspendue).

Lorsque la gestion des versions est activée ou suspendue, vous pouvez définir des règles de configuration du cycle de vie pour marquer certaines versions d'objets comme ayant expiré ou pour supprimer définitivement les versions d'objets inutiles. Pour de plus amples informations, veuillez consulter Gestion du cycle de vie des objets.

MFA Delete nécessite une authentification supplémentaire lorsque le statut de gestion des versions du compartiment est modifié ou lorsque des versions d'un objet sont supprimées. L'utilisateur doit saisir des informations d'identification et un code provenant d'un périphérique

d'authentification approuvé. Pour de plus amples informations, veuillez consulter Fonction Supprimer MFA.

Ressources supplémentaires

Utilisation des compartiments

Colonnes du rapport

- Statut
- Région
- Nom du compartiment
- Gestion des versions
- Fonction Supprimer MFA activée

Les Application Load Balancers, Network Load Balancers et Gateway Load Balancers ne sont pas répartis sur plusieurs zones de disponibilités

Description

Vérifie si vos Application Load Balancers, Network Load Balancers et Gateway Load Balancers sont configurés avec des sous-réseaux répartis sur plusieurs zones de disponibilité.

Vous pouvez spécifier les zones de disponibilité minimales souhaitées dans les minAvailabilityZonesparamètres de vos AWS Config règles.

Pour plus d'informations, voir Zones de disponibilité pour votre Application Load Balancer, Zones de disponibilité – Network Load Balancers et Création d'un Gateway Load Balancer.

> **Note**
>
> Les résultats de cette vérification sont automatiquement actualisés plusieurs fois par jour et les demandes d'actualisation ne sont pas autorisées. Plusieurs heures peuvent encore être nécessaires pour que les modifications apparaissent. Actuellement, vous ne pouvez pas exclure des ressources de cette vérification.

ID de la vérification

`c18d2gz169`

Source

AWS Config Managed Rule: elbv2-multiple-az

Critères d'alerte

Jaune : les Application Load Balancers, Network Load Balancers et Gateway Load Balancers sont configurés avec des sous-réseaux dans moins de deux zones de disponibilité.

Action recommandée

Configurez vos Application Load Balancers, Network Load Balancers et Gateway Load Balancers avec des sous-réseaux répartis sur plusieurs zones de disponibilité.

Ressources supplémentaires

Zones de disponibilité pour votre Application Load Balancer

Zones de disponibilité (Elastic Load Balancing)

Création d'un Gateway Load Balancer

Colonnes du rapport

- Statut
- Région
- Ressource
- AWS Config Règle
- Paramètres d'entrée
- Heure de la dernière modification

Auto Scaling des adresses IP disponibles dans les sous-réseaux

Description

Vérifie qu'il reste suffisamment d'adresses IP disponibles dans les sous-réseaux ciblés. Il peut être utile de disposer de suffisamment d'adresses IP lorsqu'un groupe Auto Scaling atteint sa taille maximale et doit lancer des instances supplémentaires.

ID de la vérification

Cjxm268ch1

Critères d'alerte

- Rouge : le nombre maximal d'instances et d'adresses IP pouvant être créées par un groupe Auto Scaling dépasse le nombre d'adresses IP restantes dans les sous-réseaux configurés.
- Vert : il y a suffisamment d'adresses IP disponibles pour l'échelle restante possible dans le groupe Auto Scaling.

Action recommandée

Augmentation du nombre d'adresses IP disponibles

Colonnes du rapport

- Statut
- Région
- ARN des ressources
- Nombre maximal d'instances pouvant être créées
- Nombre d'instances disponibles

Surveillances de l'état du groupe Auto Scaling

Description

Examine la configuration de la surveillance de l'état des groupes Auto Scaling.

Si Elastic Load Balancing est utilisé pour un groupe Auto Scaling, la configuration recommandée est d'activer une surveillance de l'état Elastic Load Balancing. Si aucune surveillance de l'état Elastic Load Balancing n'est utilisé, Auto Scaling ne peut agir que sur l'état de l'instance Amazon Elastic Compute Cloud (Amazon EC2). Auto Scaling n'agira pas sur l'application exécutée sur l'instance.

ID de la vérification

`CL0G40CD08`

Critères d'alerte

- Jaune : un groupe Auto Scaling a un équilibreur de charge associé, mais la surveillance de l'état Elastic Load Balancing n'est pas activée.
- Jaune : un groupe Auto Scaling n'a pas d'équilibreur de charge associé, mais la surveillance de l'état Elastic Load Balancing est activée.

Action recommandée

Si le groupe Auto Scaling a un équilibreur de charge associé, mais que la surveillance de l'état Elastic Load Balancing n'est pas activée, consultez Add an Elastic Load Balancing Health Check (Ajouter une surveillance de l'état Elastic Load Balancing à votre groupe Auto Scaling).

Si la surveillance de l'état Elastic Load Balancing est activée, mais qu'aucun équilibreur de charge n'est associé au groupe Auto Scaling, consultez Set Up an Auto-Scaled and Load-Balanced Application (Configurer une application redimensionnée et à charge équilibrée).

Ressources supplémentaires

Guide de l'utilisateur Amazon EC2 Auto Scaling

Colonnes du rapport

- Statut
- Région
- Nom du groupe Auto Scaling
- Équilibreur de charge associé
- Vérification de l'état

Ressources du groupe Auto Scaling

Description

Vérifie la disponibilité des ressources associées aux configurations du lancement et à vos groupes Auto Scaling.

Les groupes Auto Scaling qui pointent vers des ressources indisponibles ne peuvent pas lancer de nouvelles instances Amazon Elastic Compute Cloud (Amazon EC2). Lorsque Auto Scaling est correctement configuré, cela augmente de manière régulière le nombre d'instances Amazon EC2 lors des pics de demande et le diminue automatiquement lors de ralentissements des demandes. Les groupes Auto Scaling et les configurations du lancement qui pointent vers des ressources indisponibles ne fonctionnent pas comme prévu.

ID de la vérification

`8CNsSllI5v`

Critères d'alerte

- Rouge : un groupe Auto Scaling est associé à un équilibreur de charge supprimé.

- Rouge : une configuration de lancement est associée à une Amazon Machine Image (AMI) supprimée.

Action recommandée

Si l'équilibreur de charge a été supprimé, vous pouvez en créer un nouveau ou créer un nouveau groupe cible, puis l'associer au nouveau groupe Auto Scaling, ou créer un groupe Auto Scaling sans équilibreur de charge. Pour plus d'informations sur la création d'un groupe Auto Scaling avec un nouvel équilibreur de charge, consultez Set Up an Auto-Scaled and Load-Balanced Application (Configurer une application redimensionnée et à charge équilibrée). Pour plus d'informations sur la création d'un nouveau groupe Auto Scaling sans équilibreur de charge, consultez Create Auto Scaling Group (Créer un groupe Auto Scaling) dans Getting Started With Auto Scaling Using the Console (Démarrer avec Auto Scaling à l'aide de la console).

Si l'AMI a été supprimée, créez un nouveau modèle de lancement ou une nouvelle version de modèle de lancement à l'aide d'une AMI, et associez-y un groupe Auto Scaling. Voir Create Launch Configuration (Créer une configuration de lancement) dans Getting Started With Auto Scaling Using the Console (Débuter avec Auto Scaling à l'aide de la console).

Ressources supplémentaires

- Résolution d'Auto Scaling : AMI Amazon EC2
- Résolution d'Auto Scaling : configuration de l'équilibreur de charge
- Guide de l'utilisateur Amazon EC2 Auto Scaling

Colonnes du rapport

- Statut
- Région
- Nom du groupe Auto Scaling
- Type de lancement
- Type de ressource
- Nom de la ressource

Clusters AWS CloudHSM exécutant des instances HSM dans une mono-AZ

Description

Surveille vos clusters qui exécutent des instances HSM dans une zone de disponibilité (AZ) mono-AZ. Ce contrôle vous avertit si vos clusters risquent de ne pas disposer de la sauvegarde la plus récente.

> **Note**
>
> Les résultats de cette vérification sont automatiquement actualisés plusieurs fois par jour et les demandes d'actualisation ne sont pas autorisées. Plusieurs heures peuvent encore être nécessaires pour que les modifications apparaissent. Actuellement, vous ne pouvez pas exclure des ressources de cette vérification.

ID de la vérification

`hc0dfs7601`

Critères d'alerte

- Jaune : un cluster CloudHSM exécute toutes les instances HSM dans une zone de disponibilité (AZ) mono-AZ pendant plus d'une heure.
- Vert : un cluster CloudHSM exécute toutes les instances HSM dans au moins deux zones de disponibilité différentes.

Action recommandée

Créez au moins une instance supplémentaire pour le cluster dans une autre zone de disponibilité.

Ressources supplémentaires

Les meilleures pratiques pour AWS CloudHSM

Colonnes du rapport

- Statut
- Région
- ID du cluster
- Nombre d'instances HSM
- Heure de la dernière modification

AWS Direct Connect Redondance de connexion

Description

Les chèques pour Régions AWS cela n'ont qu'une seule AWS Direct Connect connexion. La connectivité à vos AWS ressources doit être configurée à tout moment par deux connexions Direct Connect afin d'assurer la redondance en cas d'indisponibilité d'un appareil.

> **Note**
>
> Les résultats de cette vérification sont automatiquement actualisés plusieurs fois par jour et les demandes d'actualisation ne sont pas autorisées. Plusieurs heures peuvent encore être nécessaires pour que les modifications apparaissent.

ID de la vérification

`0t121N1Ty3`

Critères d'alerte

Jaune : Région AWS Il n'y a qu'une seule AWS Direct Connect connexion.

Action recommandée

Configurez une connexion Direct Connect supplémentaire pour vous Région AWS protéger contre l'indisponibilité de l'appareil. Pour en savoir plus, consultez Configuration de connexions redondantes avec AWS Direct Connect (français non garanti). Pour vous protéger contre l'indisponibilité du site et ajouter une redondance d'emplacement, configurez la connexion Direct Connect supplémentaire à un autre emplacement Direct Connect.

Ressources supplémentaires

- Mise en route avec AWS Direct Connect
- Questions fréquentes AWS Direct Connect (FAQ)

Colonnes du rapport

- Statut
- Région
- Horodatage
- Emplacement
- ID de connexion

AWS Direct Connect Redondance des lieux

Description

Vérifie la présence Régions AWS d'une ou de plusieurs AWS Direct Connect connexions et d'un seul AWS Direct Connect emplacement. La connectivité à vos AWS ressources doit comporter des connexions Direct Connect configurées vers différents emplacements Direct Connect afin de garantir la redondance en cas d'indisponibilité d'un site.

> **Note**
>
> Les résultats de cette vérification sont automatiquement actualisés plusieurs fois par jour et les demandes d'actualisation ne sont pas autorisées. Plusieurs heures peuvent encore être nécessaires pour que les modifications apparaissent.

ID de la vérification

`8M012Ph3U5`

Critères d'alerte

Jaune : Les connexions Direct Connect du ne Région AWS sont pas configurées vers des emplacements différents.

Action recommandée

Configurez une connexion Direct Connect qui utilise un autre emplacement Direct Connect pour vous protéger contre l'indisponibilité de l'emplacement. Pour plus d'informations, consultez Getting Started with AWS Direct Connect.

Ressources supplémentaires

- Mise en route avec AWS Direct Connect
- Questions fréquentes AWS Direct Connect (FAQ)

Colonnes du rapport

- Statut
- Région
- Horodatage
- Emplacement

- Informations de connexion

AWS Direct Connect Résilience de localisation

Description

Vérifie la résilience de AWS Direct Connect localisation associée à chacune de vos passerelles privées virtuelles ou passerelles de transit.

Cette vérification vous avertit si l'une de vos passerelles privées virtuelles ou passerelles Direct Connect n'est pas configurée pour utiliser au moins deux emplacements Direct Connect. Le manque de résilience de l'emplacement peut entraîner des temps d'arrêt inattendus et une mauvaise expérience de connectivité.

> **Note**
>
> Les résultats de cette vérification sont automatiquement actualisés plusieurs fois par jour et les demandes d'actualisation ne sont pas autorisées. Plusieurs heures peuvent encore être nécessaires pour que les modifications apparaissent.

ID de la vérification

`c1dfpnchv2`

Critères d'alerte

Rouge : la passerelle privée virtuelle ou la passerelle Direct Connect ne possède pas d'interfaces virtuelles configurées pour se connecter à des appareils situés sur plusieurs sites Direct Connect.

Jaune : la passerelle privée virtuelle ou passerelle Direct Connect est configurée avec plusieurs interfaces virtuelles pour se connecter à différents appareils au sein du même emplacement Direct Connect. Mais il n'est pas configuré pour se connecter à des appareils situés sur plusieurs sites Direct Connect.

Vert : La passerelle privée virtuelle ou passerelle Direct Connect est configurée pour utiliser au moins deux emplacements Direct Connect.

Action recommandée

Pour renforcer la résilience des sites Direct Connect, vous pouvez configurer la passerelle privée virtuelle ou la passerelle Direct Connect pour qu'elle se connecte à au moins deux emplacements

Direct Connect distincts. Pour plus d'informations, consultez AWS Direct Connect la section Recommandation de résilience.

Ressources supplémentaires

AWS Direct Connect Recommandations en matière de résilience

AWS Direct Connect Test de basculement

Colonnes du rapport

- Statut
- Région
- Heure de la dernière modification
- État de résilience
- Emplacement
- ID de connexion
- ID de la passerelle

AWS Direct Connect Redondance de l'interface virtuelle

Description

Vérifie les passerelles privées virtuelles dotées d'interfaces AWS Direct Connect virtuelles (VIF) qui ne sont pas configurées sur au moins deux AWS Direct Connect connexions. La connectivité à votre passerelle réseau privé virtuel doit avoir plusieurs interfaces virtuelles configurées sur plusieurs connexions et emplacements Direct Connect. Cela fournit une redondance si un périphérique ou un emplacement n'est pas disponible.

> **Note**
>
> Les résultats de cette vérification sont automatiquement actualisés plusieurs fois par jour, et les requêtes d'actualisation ne sont pas autorisées. Plusieurs heures peuvent encore être nécessaires pour que les modifications apparaissent.

ID de la vérification

`4g3Nt5M1Th`

Critères d'alerte

Jaune : une passerelle privée virtuelle possède moins de deux interfaces virtuelles, ou les interfaces ne sont pas configurées pour plusieurs connexions Direct Connect.

Action recommandée

Configurez au moins deux interfaces virtuelles pour deux connexions Direct Connect afin de vous protéger contre l'indisponibilité du périphérique ou de l'emplacement. Voir Créer une interface virtuelle.

Ressources supplémentaires

- Mise en route avec AWS Direct Connect
- Questions fréquentes AWS Direct Connect (FAQ)
- Utilisation d'interfaces AWS Direct Connect virtuelles

Colonnes du rapport

- Statut
- Région
- Horodatage
- ID de la passerelle
- Emplacement du VIF
- ID de connexion du VIF

AWS Lambda fonctions sans configuration d'une file d'attente de lettres mortes

Description

Vérifie si une AWS Lambda fonction est configurée avec une file d'attente de lettres mortes.

Une file d'attente de lettres mortes est une fonctionnalité AWS Lambda qui vous permet de capturer et d'analyser les événements ayant échoué, afin de gérer ces événements en conséquence. Votre code peut déclencher une exception, expirer ou manquer de mémoire, ce qui peut entraîner l'échec des exécutions asynchrones de votre fonction Lambda. Une file d'attente de lettres mortes stocke les messages provenant d'invocations ayant échoué, ce qui permet de gérer les messages et de résoudre les problèmes.

Vous pouvez spécifier la ressource de file d'attente contenant des lettres mortes que vous souhaitez vérifier à l'aide du paramètre DLQarns de vos règles. AWS Config

Pour plus d’informations, consultez Files d’attente de lettres mortes.

> **Note**
>
> Les résultats de cette vérification sont automatiquement actualisés plusieurs fois par jour et les demandes d'actualisation ne sont pas autorisées. Plusieurs heures peuvent encore être nécessaires pour que les modifications apparaissent. Actuellement, vous ne pouvez pas exclure des ressources de cette vérification.

ID de la vérification

`c18d2gz182`

Source

`AWS Config Managed Rule: lambda-dlq-check`

Critères d'alerte

Jaune : aucune file d'attente de lettres mortes n'est configurée pour la AWS Lambda fonction.

Action recommandée

Assurez-vous que vos AWS Lambda fonctions disposent d'une file d'attente de lettres mortes configurée pour contrôler la gestion des messages pour tous les appels asynchrones ayant échoué.

Pour plus d’informations, consultez Files d’attente de lettres mortes.

Ressources supplémentaires

- Conception d'application sans serveur robuste avec les files d'attente de lettres mortes AWS Lambda

Colonnes du rapport

- Statut
- Région
- Ressource
- AWS Config Règle
- Paramètres d'entrée
- Heure de la dernière modification

AWS Lambda Destinations des événements en cas de défaillance

Description

Vérifie qu'une destination d'événement en cas d'échec ou une file d'attente de lettres morte est configurée pour les fonctions Lambda de votre compte pour les invocations asynchrones, afin que les enregistrements des invocations ayant échoué puissent être stockés pour être analysés ou traités ultérieurement.

> **Note**
>
> Les résultats de cette vérification sont automatiquement actualisés plusieurs fois par jour et les demandes d'actualisation ne sont pas autorisées. Plusieurs heures peuvent encore être nécessaires pour que les modifications apparaissent. Actuellement, vous ne pouvez pas exclure des ressources de cette vérification.

ID de la vérification

`c1dfprch05`

Critères d'alerte

- Jaune : aucune destination d'événement en cas d'échec ou aucune file d'attente de lettres mortes n'est configurée pour la fonction.

Action recommandée

Configurez une destination d'événement en cas d'échec ou une file d'attente de lettres mortes pour que vos fonctions Lambda envoient les invocations ayant échoué ainsi que d'autres informations à l'un des services AWS de destination disponibles pour un débogage ou un traitement ultérieur.

Ressources supplémentaires

- Invocation asynchrone
- AWS Lambda Destinations des événements en cas de défaillance

Colonnes du rapport

- Statut
- Région
- La fonction dont la version est signalée.

- Pourcentage de demandes asynchrones abandonnées pour la date du jour
- Demandes asynchrones pour la date du jour
- Pourcentage moyen de demandes asynchrones quotidiennes abandonnées
- Invocations asynchrones quotidiennes moyennes
- Heure de la dernière modification

Fonctions compatibles VPC AWS Lambda sans redondance Multi-AZ

Description

Vérifie la version $LATEST des fonctions Lambda compatibles VPC qui sont vulnérables aux interruptions de service dans une seule zone de disponibilité. Il est recommandé que les fonctions compatibles VPC soient connectées à plusieurs zones de disponibilité pour garantir une haute disponibilité.

> **Note**
>
> Les résultats de cette vérification sont automatiquement actualisés plusieurs fois par jour et les demandes d'actualisation ne sont pas autorisées. Plusieurs heures peuvent encore être nécessaires pour que les modifications apparaissent. Actuellement, vous ne pouvez pas exclure des ressources de cette vérification.

ID de la vérification

`L4dfs2Q4C6`

Critères d'alerte

Jaune : La version $LATEST d'une fonction Lambda compatible VPC est connectée à des sous-réseaux dans une seule zone de disponibilité.

Action recommandée

Lors de la configuration des fonctions d'accès à votre VPC, choisissez des sous-réseaux dans plusieurs zones de disponibilité afin d'assurer une haute disponibilité.

Ressources supplémentaires

- Configuration d'une fonction Lambda pour accéder aux ressources d'un VPC

- Résilience dans AWS Lambda

Colonnes du rapport

- Statut
- Région
- ARN de la fonction
- ID du VPC
- Invocations quotidiennes moyennes
- Heure de la dernière modification

AWS Resilience Hub Vérification des composants de l'application

Description

Vérifie si un composant d'application (AppComponent) de votre application est irrécupérable. En cas AppComponent d'impossibilité de restauration en cas d'interruption, vous risquez de subir une perte de données inconnue et une interruption du système.

> **Note**
>
> Les résultats de cette vérification sont automatiquement actualisés plusieurs fois par jour et les demandes d'actualisation ne sont pas autorisées. Plusieurs heures peuvent encore être nécessaires pour que les modifications apparaissent.

ID de la vérification

`RH23stmM04`

Critères d'alerte

Rouge : AppComponent irrécupérable.

Action recommandée

Pour vous assurer que vous AppComponent êtes récupérable, passez en revue et mettez en œuvre les recommandations de résilience, puis effectuez une nouvelle évaluation. Pour plus d'informations sur la révision des recommandations de résilience, consultez Ressources supplémentaires.

Ressources supplémentaires

Révision des recommandations en matière de résilience

Concepts de AWS Resilience Hub

AWS Resilience Hub Guide de l'utilisateur

Colonnes du rapport

- Statut
- Région
- Nom de l'application
- AppComponent Nom
- Heure de la dernière modification

AWS Resilience Hub politique violée

Description

Vérifie Resilience Hub pour les applications qui ne répondent pas à l'objectif de délai de reprise (RTO) et à l'objectif de point de reprise (RPO) définis par la politique. La vérification vous alerte si votre application ne répond pas aux objectifs RTO et RPO que vous avez définis pour une application dans Resilience Hub.

> **Note**
>
> Les résultats de cette vérification sont automatiquement actualisés, et les demandes d'actualisation ne sont pas autorisées. Actuellement, vous ne pouvez pas exclure des ressources de cette vérification.

ID de la vérification

`RH23stmM02`

Critères d'alerte

- Vert : l'application dispose d'une politique et répond aux objectifs RTO et RPO.
- Jaune : la demande n'a pas encore été évaluée.

- Rouge : l'application dispose d'une politique mais ne répond pas aux objectifs RTO et RPO.

Action recommandée

Connectez-vous à la console Resilience Hub et passez en revue les recommandations afin que votre application réponde aux objectifs RTO et RPO.

Ressources supplémentaires

Concepts du Resilience Hub

Colonnes du rapport

- Statut
- Région
- Nom de l'application
- Heure de la dernière modification

AWS Resilience Hub scores de résilience

Description

Vérifie si vous avez effectué une évaluation pour vos applications dans Resilience Hub. Cette vérification vous avertit si vos scores de résilience sont inférieurs à une valeur spécifique.

> **Note**
>
> Les résultats de cette vérification sont automatiquement actualisés, et les demandes d'actualisation ne sont pas autorisées. Actuellement, vous ne pouvez pas exclure des ressources de cette vérification.

ID de la vérification

`RH23stmM01`

Critères d'alerte

- Vert : votre application a un score de résilience supérieur ou égal à 70.
- Jaune : votre application a un score de résilience compris entre 40 et 69.
- Jaune : la demande n'a pas encore été évaluée.

- Rouge : votre application a un score de résilience inférieur à 40.

Action recommandée

Connectez-vous à la console Resilience Hub et exécutez une évaluation pour votre application. Passez en revue les recommandations pour améliorer le score de résilience.

Ressources supplémentaires

Concepts du Resilience Hub

Colonnes du rapport

- Statut
- Région
- Nom de l'application
- Score de résilience des applications
- Heure de la dernière modification

AWS Resilience Hub âge d'évaluation

Description

Vérifie le temps écoulé depuis la dernière évaluation d'application. Cette vérification vous avertit si vous n'avez pas effectué d'évaluation de candidature depuis un certain nombre de jours.

> **Note**
>
> Les résultats de cette vérification sont automatiquement actualisés plusieurs fois par jour et les demandes d'actualisation ne sont pas autorisées. Plusieurs heures peuvent encore être nécessaires pour que les modifications apparaissent. Actuellement, vous ne pouvez pas exclure des ressources de cette vérification.

ID de la vérification

`RH23stmM03`

Critères d'alerte

- Vert : votre évaluation d'application a été exécutée au cours des 30 derniers jours.
- Jaune : votre évaluation d'application n'a pas été exécutée au cours des 30 derniers jours.

Action recommandée

Connectez-vous à la console Resilience Hub et exécutez une évaluation pour votre application.

Ressources supplémentaires

Concepts du Resilience Hub

Colonnes du rapport

- Statut
- Région
- Nom de l'application
- Nombre de jours écoulés depuis la dernière évaluation
- Durée d'exécution de la dernière évaluation
- Heure de la dernière modification

AWS Site-to-Site VPN possède au moins un tunnel à l'état DOWN

Description

Vérifie le nombre de tunnels actifs pour chacun de vos AWS Site-to-Site VPN.

Un VPN doit avoir deux tunnels configurés en permanence. Cela permet une redondance en cas de panne ou de maintenance planifiée des périphériques au point de terminaison AWS. Pour certains matériels, un seul tunnel est actif à la fois. Si un VPN n'a aucun tunnel actif, des frais pour le VPN peuvent quand même s'appliquer.

Pour plus d'informations, voir Qu'est-ce qu'AWS Site-to-Site VPN ?

> **Note**
>
> Les résultats de cette vérification sont automatiquement actualisés plusieurs fois par jour et les demandes d'actualisation ne sont pas autorisées. Plusieurs heures peuvent encore être nécessaires pour que les modifications apparaissent. Actuellement, vous ne pouvez pas exclure des ressources de cette vérification.

ID de la vérification

`c18d2gz123`

Source

```
AWS Config Managed Rule: vpc-vpn-2-tunnels-up
```

Critères d'alerte

Jaune : au moins un tunnel d'un VPN Site-to-Site affiche l'état DOWN.

Action recommandée

Assurez-vous que deux tunnels sont configurés pour les connexions VPN. Et, si votre configuration matérielle le permet, assurez-vous que les deux tunnels sont actifs. Si vous n'avez plus besoin d'une connexion VPN, supprimez-la pour éviter des frais.

Pour plus d'informations, voir Votre périphérique de passerelle client et le contenu disponible dans le Centre de connaissances AWS.

Ressources supplémentaires

- AWS Site-to-Site VPN Guide de l'utilisateur
- Ajout d'une passerelle privée virtuelle à votre VPC

Colonnes du rapport

- Statut
- Région
- Ressource
- AWS Config Règle
- Paramètres d'entrée
- Heure de la dernière modification

Problèmes à risque élevé AWS Well-Architected pour la fiabilité

Description

Vérifiez les éventuels problèmes à risque élevé (HRI) pour vos charges de travail dans le pilier de fiabilité. Cette vérification est basée sur vos commentaires AWS-Well Architected. Les résultats de la vérification varient selon que vous avez terminé ou non l'évaluation de la charge de travail avec AWS Well-Architected.

> **Note**
>
> Les résultats de cette vérification sont automatiquement actualisés plusieurs fois par jour et les demandes d'actualisation ne sont pas autorisées. Plusieurs heures peuvent encore être nécessaires pour que les modifications apparaissent. Actuellement, vous ne pouvez pas exclure des ressources de cette vérification.

ID de la vérification

`Wxdfp4B1L4`

Critères d'alerte

- Rouge : Au moins un problème actif à haut risque a été identifié dans le pilier de fiabilité de AWS Well-Architected.
- Vert : aucun problème actif à haut risque n'a été détecté dans le pilier de fiabilité de AWS Well-Architected.

Action recommandée

AWS Well-Architected a détecté des problèmes à haut risque lors de l'évaluation de votre charge de travail. Ces problèmes offrent la possibilité de réduire les risques et d'économiser de l'argent. Connectez-vous à l'outil AWS Well-Architected afin de passer en revue vos réponses et d'intervenir pour résoudre vos problèmes actifs.

Colonnes du rapport

- Statut
- Région
- ARN de la charge de travail
- Nom de la charge de travail
- Nom de l'évaluateur
- Type de charge de travail
- Date de début de la charge de travail
- Date de la dernière modification de la charge de travail
- Nombre de problèmes à haut risque identifiés pour la Fiabilité
- Nombre de problèmes à haut risque résolus pour la Fiabilité
- Nombre de questions ayant reçu une réponse pour la Fiabilité

- Nombre total de questions dans le pilier Fiabilité
- Heure de la dernière modification

Le Classic Load Balancer n'a pas plusieurs zones de disponibilité configurés

Description

Vérifie si un Classic Load Balancer est réparti sur plusieurs zones de disponibilité.

Un équilibreur de charge distribue le trafic applicatif entrant sur plusieurs instances Amazon EC2 réparties sur plusieurs zones de disponibilité. Par défaut, l'équilibreur de charge répartit le trafic uniformément entre les zones de disponibilité qui vous activez pour votre équilibreur de charge. En cas de panne d'une zone de disponibilité, les nœuds de l'équilibreur de charge transfèrent automatiquement les demandes aux instances enregistrées saines dans une ou plusieurs zones de disponibilité.

Vous pouvez ajuster le nombre minimum de zones de disponibilité à l'aide du minAvailabilityZonesparamètre de vos AWS Config règles

Pour plus d'informations, voir Qu'est-ce qu'un Classic Load Balancer ?.

> **Note**
>
> Les résultats de cette vérification sont automatiquement actualisés plusieurs fois par jour et les demandes d'actualisation ne sont pas autorisées. Plusieurs heures peuvent encore être nécessaires pour que les modifications apparaissent. Actuellement, vous ne pouvez pas exclure des ressources de cette vérification.

ID de la vérification

```
c18d2gz154
```

Source

```
AWS Config Managed Rule: clb-multiple-az
```

Critères d'alerte

Jaune : le Classic Load Balancer n'est pas configuré sur plusieurs zones de disponibilités ou ne respecte pas le nombre minimal de zones de disponibilité spécifié.

Action recommandée

Assurez-vous que plusieurs zones de disponibilité sont configurées sur vos Classic Load Balancers. Répartissez votre équilibreur de charge sur plusieurs zones de disponibilité pour garantir la haute disponibilité de votre application.

Pour plus d'informations, voir Didacticiel : Création d'un Classic Load Balancer.

Colonnes du rapport

- Statut
- Région
- Ressource
- AWS Config Règle
- Paramètres d'entrée
- Heure de la dernière modification

Connection Draining ELB

Description

Vérifie les équilibreurs de charge pour lesquels Connection Draining n'est pas activé.

Lorsque Connection Draining n'est pas activé et que vous annulez l'enregistrement d'une instance Amazon EC2 à un équilibreur de charge, l'équilibreur de charge arrête le routage du trafic vers cette instance et ferme la connexion. Lorsque Connection Draining est activé, l'équilibreur de charge cesse d'envoyer de nouvelles requêtes à l'instance qui n'est plus enregistrée, mais maintient la connexion ouverte pour servir les requêtes actives.

ID de la vérification

`7qGXsKIUw`

Critères d'alerte

Jaune : le drainage de la connexion n'est pas activé pour un équilibreur de charge.

Action recommandée

Activez le drainage de la connexion pour l'équilibreur de charge. Pour plus d'informations, consultez Connexion draining et Enable or Disable Connection Draining for Your Load Balancer (Activer ou désactiver le drainage de la connexion pour votre équilibreur de charge).

Ressources supplémentaires

Concepts Elastic Load Balancer

Colonnes du rapport

- Statut
- Région
- Nom de l'équilibreur de charge
- Raison

Équilibrage de charge entre zones ELB

Description

Lorsque l'équilibrage de charge entre zones est désactivé, le service peut être indisponible suite à une distribution inégale du trafic ou une surcharge du backend. Ce problème peut se produire lorsque les clients ne mettent pas correctement en cache les informations DNS. Le problème peut également se produire lorsque le nombre d'instances dans chaque zone de disponibilité est inégal (par exemple, si vous avez supprimé certaines instances pour la maintenance).

ID de la vérification

`xdeXZKIUy`

Critères d'alerte

Jaune : l'équilibrage de charge entre zones n'est pas activé pour un équilibreur de charge.

Action recommandée

Vérifiez que les instances Amazon EC2 enregistrées auprès de l'équilibreur de charge sont lancées dans plusieurs zones de disponibilité, puis activez l'équilibrage de charge entre zones pour l'équilibreur de charge. Pour de plus amples informations, consultez Availability Zones and Regions (Zones de disponibilité et régions) et Enable or Disable Cross-Zone Load Balancing for Your Load Balancer (Activation ou désactivation de l'équilibrage de charge entre zones pour votre équilibreur de charge).

Ressources supplémentaires

- Demande de routage
- Concepts Elastic Load Balancer

Colonnes du rapport

- Statut
- Région
- Nom de l'équilibreur de charge
- Raison

Optimisation des programmes Elastic Load Balancer

Description

Vérifie la configuration de votre équilibreur de charge.

Pour augmenter le niveau de tolérance aux pannes dans Amazon Elastic Compute Cloud (Amazon EC2) lors de l'utilisation d'Elastic Load Balancing, nous vous recommandons d'exécuter un nombre égal d'instances sur plusieurs zones de disponibilité dans une région. Un équilibreur de charge configuré augmente les frais, donc il s'agit également d'une vérification d'optimisation des coûts.

ID de la vérification

`iqdCTZKCUp`

Critères d'alerte

- Jaune : un équilibreur de charge est activé pour une seule zone de disponibilité.
- Jaune : un équilibreur de charge est activé pour une zone de disponibilité qui ne possède aucune instance active.
- Jaune : les instances Amazon EC2 enregistrées avec un équilibreur de charge sont réparties de manière inégale entre les zones de disponibilité. (La différence entre le nombre d'instances le plus élevé et le plus faible dans les zones de disponibilité utilisées est supérieure à 1, et la différence est supérieure à 20 % du nombre le plus élevé.)

Action recommandée

Assurez-vous que l'équilibreur de charge pointe vers des instances actives et saines dans au moins deux zones de disponibilité. Pour plus d'informations, consultez Ajouter des zones de disponibilité.

Si votre équilibreur de charge est configuré pour une zone de disponibilité sans instances saines, ou en cas de déséquilibre des instances entre les zones de disponibilité, déterminez si

toutes les zones de disponibilité sont nécessaires. Omettez les zones de disponibilité inutiles et assurez-vous que les instances sont réparties de manière équilibrée entre les zones de disponibilité restantes. Pour de plus amples informations, veuillez consulter Remove Availability Zone (Supprimer une zone de disponibilité).

Ressources supplémentaires

- Régions et zones de disponibilité
- Gestion des équilibreurs de charge
- Bonnes pratiques d'évaluation d'Elastic Load Balancing

Colonnes du rapport

- Statut
- Région
- Nom de l'équilibreur de charge
- Nombre de zones
- Instances de zone a
- Instances de zone b
- Instances de zone c
- Instances de zone d
- Instances de zone e
- Instances de zone f
- Raison

Indépendance de la zone de disponibilité des passerelles NAT

Description

Vérifie si l'indépendance des zones de disponibilité (AZ) est configurée pour vos passerelles NAT.

Une passerelle NAT permet aux ressources de votre sous-réseau privé de se connecter en toute sécurité à des services en dehors du sous-réseau à l'aide des adresses IP de la passerelle NAT et supprime tout trafic entrant non sollicité. Chaque passerelle NAT fonctionne dans une zone de disponibilité (AZ) désignée et est conçue de manière redondante uniquement dans cette zone. Par conséquent, vos ressources dans une zone de disponibilité donnée doivent utiliser une passerelle NAT dans la même zone de disponibilité, de sorte que toute panne potentielle d'une

passerelle NAT ou de sa zone de disponibilité n'ait aucun impact sur vos ressources dans une autre zone de disponibilité.

> **Note**
>
> Les résultats de cette vérification sont automatiquement actualisés plusieurs fois par jour et les demandes d'actualisation ne sont pas autorisées. Plusieurs heures peuvent encore être nécessaires pour que les modifications apparaissent. Actuellement, vous ne pouvez pas exclure des ressources de cette vérification.

ID de la vérification

`c1dfptbg10`

Critères d'alerte

- Rouge : le trafic provenant de votre sous-réseau dans une zone de disponibilité est acheminé via une passerelle NAT dans une autre zone de disponibilité.
- Vert : le trafic provenant de votre sous-réseau dans une zone de disponibilité est acheminé via une passerelle NAT dans la même zone de disponibilité.

Action recommandée

Vérifiez la zone de disponibilité de votre sous-réseau et acheminez le trafic via une passerelle NAT dans la même zone de disponibilité.

S'il n'existe aucune passerelle NAT dans la zone de disponibilité, créez-en une et utilisez-la pour acheminer le trafic de votre sous-réseau.

Si la même table de routage est associée à des sous-réseaux dans différentes zones de disponibilité, conservez cette table de routage associée aux sous-réseaux résidant dans la même zone de disponibilité que la passerelle NAT. Pour les sous-réseaux dans l'autre zone de disponibilité, associez une table de routage distincte à un routage vers une passerelle NAT dans cette autre zone de disponibilité.

Nous vous recommandons de choisir une fenêtre de maintenance pour les modifications d'architecture de votre VPC Amazon.

Ressources supplémentaires

- Création d'une passerelle NAT

- Configuration de routages pour différents cas d'utilisation de passerelle NAT

Colonnes du rapport

- Statut
- Région
- Zone de disponibilité de la passerelle NAT
- Identifiant de la passerelle NAT
- Zone de disponibilité du sous-réseau
- ID de sous-réseau (subnet)
- Identifiant de la table de routage
- ARN de la passerelle NAT
- Heure de la dernière modification

Équilibrage de charge entre zones sur les Network Load Balancers

Description

Vérifie si l'équilibrage de charge entre zones est activé sur les Network Load Balancers.

L'équilibrage de charge entre zones permet de maintenir une répartition uniforme du trafic entrant entre les instances des différentes zones de disponibilité. Cela empêche l'équilibreur de charge d'acheminer tout le trafic vers des instances situées dans la même zone de disponibilité, ce qui peut entraîner une répartition inégale du trafic et une surcharge. Cette fonctionnalité renforce également la fiabilité des applications en acheminant automatiquement le trafic vers des instances saines situées dans d'autres zones de disponibilité en cas de défaillance d'une zone de disponibilité.

Pour plus d'informations, voir Équilibrage de charge entre zones.

> **Note**
>
> Les résultats de cette vérification sont automatiquement actualisés plusieurs fois par jour et les demandes d'actualisation ne sont pas autorisées. Plusieurs heures peuvent encore être nécessaires pour que les modifications apparaissent. Actuellement, vous ne pouvez pas exclure des ressources de cette vérification.

ID de la vérification

`c18d2gz105`

Source

`AWS Config Managed Rule: nlb-cross-zone-load-balancing-enabled`

Critères d'alerte

- Jaune : l'équilibrage de charge entre zones n'est pas activé sur le Network Load Balancer.

Action recommandée

Assurez-vous que l'équilibrage de charge entre zones est activé sur les Network Load Balancers.

Ressources supplémentaires

Équilibrage de charge entre zones (Network Load Balancers)

Colonnes du rapport

- Statut
- Région
- Ressource
- AWS Config Règle
- Paramètres d'entrée
- Heure de la dernière modification

NLB - Ressource connectée à Internet dans un sous-réseau privé

Description

Vérifie si un Network Load Balancer (NLB) connecté à Internet est configuré avec un sous-réseau privé. Un Network Load Balancer (NLB) connecté à Internet doit être configuré dans les sous-réseaux publics pour recevoir du trafic. Un sous-réseau public est défini comme un sous-réseau doté d'une route directe vers une passerelle Internet. Si le sous-réseau est configuré comme privé, sa zone de disponibilité (AZ) ne reçoit pas de trafic, ce qui peut entraîner des problèmes de disponibilité.

> **Note**
>
> Les résultats de cette vérification sont automatiquement actualisés plusieurs fois par jour et les demandes d'actualisation ne sont pas autorisées. Plusieurs heures peuvent encore

être nécessaires pour que les modifications apparaissent. Actuellement, vous ne pouvez pas exclure des ressources de cette vérification.

ID de la vérification

`c1dfpnchv4`

Critères d'alerte

Rouge : NLB est configuré avec un ou plusieurs sous-réseaux privés

Vert : aucun sous-réseau privé n'est configuré pour le NLB connecté à Internet

Action recommandée

Vérifiez que les sous-réseaux configurés dans un équilibreur de charge connecté à Internet sont publics. Un sous-réseau public est défini comme un sous-réseau doté d'une route directe vers une passerelle Internet. Utilisez l'une des options suivantes :

- Créez un nouvel équilibreur de charge et sélectionnez un autre sous-réseau avec une route directe vers une passerelle Internet.
- Modifiez le sous-réseau actuellement attaché à l'équilibreur de charge de privé à public. Pour cela, modifiez sa table de routage et associez une passerelle Internet.

Ressources supplémentaires

- Configuration d'un équilibreur de charge et d'un écouteur
- Sous-réseaux pour votre VPC
- Associer une passerelle à une table de routage

Colonnes du rapport

- Statut
- Région
- Bras NLB
- Nom NLB
- ID de sous-réseau (subnet)
- Schéma NLB
- Type de sous-réseau

- Heure de la dernière modification

NLB Multi-AZ

Description

Vérifie si vos équilibreurs de charge réseau sont configurés pour utiliser plusieurs zones de disponibilité (AZ). Une zone de disponibilité est un emplacement distinct isolé des défaillances dans d'autres zones. Configurez votre équilibreur de charge dans plusieurs AZ de la même région pour améliorer la disponibilité de votre charge de travail.

> **Note**
>
> Les résultats de cette vérification sont automatiquement actualisés plusieurs fois par jour et les demandes d'actualisation ne sont pas autorisées. Plusieurs heures peuvent encore être nécessaires pour que les modifications apparaissent. Actuellement, vous ne pouvez pas exclure des ressources de cette vérification.

ID de la vérification

`c1dfprch09`

Critères d'alerte

Jaune : NLB se trouve dans un seul AZ.

Vert : NLB possède au moins deux AZ.

Action recommandée

Assurez-vous que votre équilibreur de charge est configuré avec au moins deux zones de disponibilité.

Ressources supplémentaires

Pour plus d’informations, consultez la documentation de suivante :

- Zones de disponibilité
- AWS Well-Architected - Déployez la charge de travail sur plusieurs sites
- Régions et zones de disponibilité

Colonnes du rapport

- Statut
- Région
- Nombre de zones de disponibilité
- NLB ARN
- Nom NLB
- Heure de la dernière modification

Nombre de Régions AWS dans un ensemble de réplication Incident Manager

Description

Vérifie que la configuration d'un ensemble de réplication Incident Manager en utilise plusieurs Région AWS pour prendre en charge le basculement et la réponse régionaux. Pour les incidents créés par des CloudWatch alarmes ou EventBridge des événements, Incident Manager crée un incident au même Région AWS titre que la règle d'alarme ou d'événement. Si la gestion des incidents est temporairement indisponible dans cette région, le système tente de créer un incident dans une autre région de l'ensemble de réplications. Si l'ensemble de réplications ne comprend qu'une seule région, le système ne pourra pas créer d'enregistrement d'incident tant que la gestion des incidents est indisponible.

> **Note**
>
> Les résultats de cette vérification sont automatiquement actualisés plusieurs fois par jour et les demandes d'actualisation ne sont pas autorisées. Plusieurs heures peuvent encore être nécessaires pour que les modifications apparaissent. Actuellement, vous ne pouvez pas exclure des ressources de cette vérification.

ID de la vérification

`cIdfp1js9r`

Critères d'alerte

- Vert : l'ensemble de réplications comprend plusieurs régions.
- Jaune : l'ensemble de réplications comprend une région.

Action recommandée

Ajoutez au moins une région supplémentaire à l'ensemble de réplications.

Ressources supplémentaires

Pour plus d'informations, voir Gestion des incidents entre régions.

Colonnes du rapport

- Statut
- Ensemble de réplication
- multirégional
- Heure de la dernière modification

Vérification des applications sur une seule zone de disponibilité

Description

Vérifie à l'aide de modèles de réseau si votre trafic réseau sortant est acheminé via une seule zone de disponibilité (AZ).

Une zone de disponibilité est un emplacement distinct isolé de tout impact dans d'autres zones. En répartissant votre service sur plusieurs zones de disponibilité, vous limitez le rayon d'impact d'une panne de zone de disponibilité.

> **Note**
>
> Les résultats de cette vérification sont automatiquement actualisés plusieurs fois par jour et les demandes d'actualisation ne sont pas autorisées. Plusieurs heures peuvent encore être nécessaires pour que les modifications apparaissent. Actuellement, vous ne pouvez pas exclure des ressources de cette vérification.

ID de la vérification

`c1dfptbg11`

Critères d'alerte

- Jaune : votre application ne peut être déployée que dans une seule zone de disponibilité d'après les modèles de trafic réseau sortant observés. Si cela est vrai et qu'une haute

disponibilité est nécessaire pour votre application, nous vous recommandons de provisionner les ressources de votre application et de configurer vos flux réseau de manière à utiliser plusieurs zones de disponibilité.

Action recommandée

Si votre application nécessite une haute disponibilité, mettez en œuvre une architecture multi-AZ.

Colonnes du rapport

- Statut
- Région
- ID du VPC
- Heure de la dernière modification

Interface VPC : interfaces réseau de point de terminaison dans plusieurs zones de disponibilité

Description

Vérifie si les points de terminaison de votre interface AWS PrivateLink VPC sont configurés pour utiliser plusieurs zones de disponibilité (AZ). Une zone de disponibilité est un emplacement distinct isolé des défaillances dans d'autres zones. Cela permet une connectivité réseau peu coûteuse et à faible latence entre les zones de disponibilité d'une même AWS région. Sélectionnez des sous-réseaux dans plusieurs zones de disponibilité lorsque vous créez des points de terminaison d'interface afin de protéger vos applications contre un point de défaillance unique.

> **Note**
>
> Cette vérification inclut actuellement uniquement les points de terminaison de l'interface.

> **Note**
>
> Les résultats de cette vérification sont automatiquement actualisés plusieurs fois par jour et les demandes d'actualisation ne sont pas autorisées. Plusieurs heures peuvent encore être nécessaires pour que les modifications apparaissent. Actuellement, vous ne pouvez pas exclure des ressources de cette vérification.

ID de la vérification

`c1dfprch10`

Critères d'alerte

Jaune : le point de terminaison VPC se trouve dans une seule zone AZ.

Vert : le point de terminaison du VPC se trouve dans au moins deux AZ.

Action recommandée

Assurez-vous que le point de terminaison de votre interface VPC est configuré avec au moins deux zones de disponibilité.

Ressources supplémentaires

Pour plus d'informations, consultez la documentation de suivante :

- Accédez à un AWS service à l'aide d'un point de terminaison VPC d'interface
- Adresse IP privée de l'interface réseau du terminal
- AWS PrivateLink concepts
- Régions et zones de disponibilité

Colonnes du rapport

- Statut
- Région
- ID de point de terminaison VPC
- Est Multi AZ
- Heure de la dernière modification

Redondance des tunnels VPN

Description

Vérifie le nombre de tunnels actifs pour chacun de vos VPN.

Un VPN doit avoir deux tunnels configurés en permanence. Cela fournit une redondance en cas de panne ou de maintenance planifiée des périphériques au point de terminaison AWS . Pour certains matériels, un seul tunnel est actif à la fois. Si un VPN n'a aucun tunnel actif, des frais

pour le VPN peuvent quand même s'appliquer. Pour plus d'informations, consultez le Guide d'administration AWS Client VPN.

ID de la vérification

`S45wrEXrLz`

Critères d'alerte

- Jaune : un VPN possède un tunnel actif (ce qui est normal pour certains matériels).
- Jaune : un VPN n'a aucun tunnel actif.

Action recommandée

Assurez-vous que deux tunnels sont configurés pour votre connexion VPN et qu'ils sont tous deux actifs si votre matériel le prend en charge. Si vous n'avez plus besoin d'une connexion VPN, vous pouvez la supprimer pour éviter des frais. Pour de plus amples informations, consultez Your Customer Gateway (Votre passerelle client) ou Deleting a VPN connection (Suppression d'une connexion VPN).

Ressources supplémentaires

- AWS Guide de l'utilisateur du VPN de site à site
- Ajout d'une passerelle réseau privé virtuel Hardware à votre VPC

Colonnes du rapport

- Statut
- Région
- ID d'VPN
- VPC
- Passerelle réseau privé virtuel
- Passerelle client
- Tunnels actifs
- Raison

Redondance de zone de disponibilité pour ActiveMQ

Description

Vérifie que les agents Amazon MQ pour ActiveMQ sont configurés pour une haute disponibilité avec un agent actif/de secours dans plusieurs zones de disponibilité.

> **Note**
>
> Les résultats de cette vérification sont automatiquement actualisés plusieurs fois par jour et les demandes d'actualisation ne sont pas autorisées. Plusieurs heures peuvent encore être nécessaires pour que les modifications apparaissent. Actuellement, vous ne pouvez pas exclure des ressources de cette vérification.

ID de la vérification

`c1t3k8mqv1`

Critères d'alerte

- Jaune : un agent Amazon MQ pour ActiveMQ est configuré dans une seule zone de disponibilité.

  Vert : un agent Amazon MQ pour ActiveMQ est configuré dans au moins deux zones de disponibilité.

Action recommandée

Créez un nouveau courtier avec un mode de déploiement actif/de secours.

Ressources supplémentaires

- Création d'un agent ActiveMQ

Colonnes du rapport

- Statut
- Région
- Identifiant de l'agent ActiveMQ
- Type de moteur d'agent
- Mode de déploiement
- Heure de la dernière modification

Redondance de zone de disponibilité pour RabbitMQ

Description

Vérifie que les agents Amazon MQ pour RabbitMQ sont configurés pour une haute disponibilité avec des instances de cluster dans plusieurs zones de disponibilité.

> **Note**
>
> Les résultats de cette vérification sont automatiquement actualisés plusieurs fois par jour et les demandes d'actualisation ne sont pas autorisées. Plusieurs heures peuvent encore être nécessaires pour que les modifications apparaissent. Actuellement, vous ne pouvez pas exclure des ressources de cette vérification.

ID de la vérification

`c1t3k8mqv2`

Critères d'alerte

- Jaune : un agent Amazon MQ pour RabbitMQ est configuré dans une seule zone de disponibilité.

  Vert : un agent Amazon MQ pour RabbitMQ est configuré dans plusieurs zones de disponibilité.

Action recommandée

Créez un nouvel agent avec le mode de déploiement de cluster.

Ressources supplémentaires

- Création d'un agent RabbitMQ

Colonnes du rapport

- Statut
- Région
- Identifiant de l'agent RabbitMQ
- Type de moteur d'agent
- Mode de déploiement
- Heure de la dernière modification

Service Limits

Consultez les vérifications suivantes pour la catégorie Service Limits (également appelées quotas).

Toutes les vérifications de cette catégorie ont les descriptions suivantes :

Critères d'alerte

- Jaune : 80 % de la limite atteinte.
- Rouge : 100 % de la limite atteinte.
- Bleu : Trusted Advisor n'a pas pu récupérer l'utilisation ou les limites d'une ou de plusieurs Régions AWS.

Action recommandée

Si vous pensez dépasser une limite de service, demandez une augmentation directement à partir de la console Service Quotas. Si Service Quotas ne prend pas encore en charge votre service, vous pouvez créer un cas de support dans le Centre de support.

Colonnes du rapport

- Statut
- Service
- Région
- Volume limite
- Utilisation actuelle

> **Note**
>
> - Les valeurs sont basées sur un instantané, de sorte que votre utilisation actuelle peut différer. Les données sur les quotas et l'utilisation peuvent prendre jusqu'à 24 heures pour être reflétés dans les modifications. Dans les cas où les quotas ont été récemment augmentés, il se peut que l'utilisation dépasse temporairement le quota.

Noms des vérifications

- Groupes Auto Scaling
- Configuration du lancement d'Auto Scaling
- CloudFormation Piles
- Capacité de lecture DynamoDB
- Capacité d'écriture DynamoDB
- Instantané actifs EBS
- Stockage des volumes EBS à froid HDD (sc1)

- Stockage de volumes EBS polyvalent SSD (gp2)
- Stockage de volumes EBS polyvalent SSD (gp3)
- Stockage de volumes magnétique EBS (standard)
- IOPS d'agrégation des volumes d'IOPS provisionnés (SSD) EBS
- Stockage de volume d'IOPS provisionnés SSD EBS (io1)
- Stockage de volume d'IOPS provisionnés SSD EBS (io2)
- Stockage de volumes HDD à débit optimisé EBS (st1)
- Instances à la demande EC2
- Baux d'instance réservée EC2
- Adresses IP Elastic EC2-Classic
- Adresse IP Elastic EC2-VPC
- ELB Application Load Balancers
- ELB Application Load Balancers
- Dispositifs d'équilibrage de charge de réseau ELB
- Groupe IAM
- Profils d'instance IAM
- Politiques IAM
- Rôles IAM
- Certificats de serveur IAM
- Utilisateurs IAM
- Partitions de Kinesis par région
- Utilisation du stockage de code Lambda
- Groupes de paramètres de cluster RDS
- Rôles de cluster RDS
- Clusters RDS
- Instances de base de données RDS
- Instantanés manuels de base de données RDS
- Groupes de paramètres de base de données RDS
- Groupes de sécurité de base de données RDS
- Abonnements aux événements RDS

- Autorisations RDS maximum par groupe de sécurité
- Groupes d'options RDS
- Réplicas en lecture par master RDS
- Instances réservées RDS
- Groupe de sous-réseaux RDS
- Sous-réseaux RDS par groupe de sous-réseaux
- Quota total de stockage RDS
- Zones hébergées Route 53
- Surveillances de l'état maximum Route 53
- Ensembles de délégations réutilisables Route 53
- Politiques de trafic Route 53
- Instances de politique de trafic Route 53
- Quota d'envoi quotidien SES
- VPC
- Passerelles Internet VPC

Groupes Auto Scaling

Description

Vérifie l'utilisation qui représente plus de 80 % du quota des groupes Auto Scaling.

ID de la vérification

`fW7HH0l7J9`

Ressources supplémentaires

Quotas Auto Scaling

Configuration du lancement d'Auto Scaling

Description

Vérifie l'utilisation qui représente plus de 80 % du quota de configurations du lancement d'Auto Scaling.

ID de la vérification

`aW7HH0l7J9`

Ressources supplémentaires

- Quotas Auto Scaling

CloudFormation Piles

Description

Vérifie si l'utilisation est supérieure à 80 % du quota de CloudFormation piles.

ID de la vérification

`gW7HH0l7J9`

Ressources supplémentaires

- Quotas AWS CloudFormation

Capacité de lecture DynamoDB

Description

Vérifie l'utilisation qui représente plus de 80 % de la limite de débit provisionné DynamoDB pour les lectures par Compte AWS.

ID de la vérification

`6gtQddfEw6`

Ressources supplémentaires

- Quotas DynamoDB

Capacité d'écriture DynamoDB

Description

Vérifie l'utilisation qui représente plus de 80 % de la limite de débit provisionné DynamoDB pour les écritures par Compte AWS.

ID de la vérification

`c5ftjdfkMr`

Ressources supplémentaires

Quotas DynamoDB

Instantané actifs EBS

Description

Vérifie l'utilisation qui représente plus de 80 % du quota d'instantanés actifs EBS.

ID de la vérification

`eI7KK0l7J9`

Ressources supplémentaires

Limites Amazon EBS

Stockage des volumes EBS à froid HDD (sc1)

Description

Vérifie l'utilisation qui représente plus de 80 % du quota de stockage de volumes EBS à froid HDD (sc1).

ID de la vérification

`gH5CC0e3J9`

Ressources supplémentaires

Limites Amazon EBS

Stockage de volumes EBS polyvalent SSD (gp2)

Description

Vérifie l'utilisation qui représente plus de 80 % du quota de stockage de volumes EBS polyvalent SDD (gp2).

ID de la vérification

dH7RR0l6J9

Ressources supplémentaires

Limites Amazon EBS

Stockage de volumes EBS polyvalent SSD (gp3)

Description

Vérifie l'utilisation qui représente plus de 80 % du quota de stockage de volumes EBS polyvalent SDD (gp3).

ID de la vérification

dH7RR0l6J3

Ressources supplémentaires

Limites Amazon EBS

Stockage de volumes magnétique EBS (standard)

Description

Vérifie l'utilisation qui représente plus de 80 % du quota de stockage de volumes magnétiques EBS (standard).

ID de la vérification

cG7HH0l7J9

Ressources supplémentaires

Limites Amazon EBS

IOPS d'agrégation des volumes d'IOPS provisionnés (SSD) EBS

Description

Vérifie l'utilisation qui représente plus de 80 % du quota d'IOPS d'agrégation de volumes d'IOPS provisionnés (SSD) EBS.

ID de la vérification

`tV7YY0l7J9`

Ressources supplémentaires

Limites Amazon EBS

Stockage de volume d'IOPS provisionnés SSD EBS (io1)

Description

Vérifie l'utilisation qui représente plus de 80 % du quota de stockage de volumes d'IOPS provisionnés SSD EBS (io1).

ID de la vérification

`gI7MM0l7J9`

Ressources supplémentaires

Limites Amazon EBS

Stockage de volume d'IOPS provisionnés SSD EBS (io2)

Description

Vérifie l'utilisation qui représente plus de 80 % du quota de stockage de volumes d'IOPS provisionnés SSD EBS (io2).

ID de la vérification

`gI7MM0l7J2`

Ressources supplémentaires

Limites Amazon EBS

Stockage de volumes HDD à débit optimisé EBS (st1)

Description

Vérifie l'utilisation qui représente plus de 80 % du quota de stockage de volumes HDD à débit optimisé EBS (st1).

ID de la vérification

`wH7DD0l3J9`

Ressources supplémentaires

Limites Amazon EBS

Instances à la demande EC2

Description

Vérifie l'utilisation qui représente plus de 80 % du quota d'instances à la demande EC2.

ID de la vérification

`0Xc6LMYG8P`

Ressources supplémentaires

Quotas Amazon EC2

Baux d'instance réservée EC2

Description

Vérifie l'utilisation qui représente plus de 80 % du quota de baux d'instance réservée EC2.

ID de la vérification

`iH7PP0l7J9`

Ressources supplémentaires

Quotas Amazon EC2

Adresses IP Elastic EC2-Classic

Description

Vérifie l'utilisation qui représente plus de 80 % du quota d'adresses IP Elastic EC2-Classic.

ID de la vérification

`aW9HH0l8J6`

Ressources supplémentaires

Quotas Amazon EC2

Adresse IP Elastic EC2-VPC

Description

Vérifie l'utilisation qui représente plus de 80 % du quota d'adresses IP Elastic EC2-VPC.

ID de la vérification

`lN7RR0l7J9`

Ressources supplémentaires

Quotas d'adresses IP Elastic de VPC

ELB Application Load Balancers

Description

Vérifie l'utilisation qui représente plus de 80 % du quota d'ELB Application Load Balancers.

ID de la vérification

`EM8b3yLRTr`

Ressources supplémentaires

Quotas Elastic Load Balancing

ELB Application Load Balancers

Description

Vérifie l'utilisation qui représente plus de 80 % du quota d'ELB Application Load Balancers.

ID de la vérification

`iK700l7J9`

Ressources supplémentaires

Quotas Elastic Load Balancing

Dispositifs d'équilibrage de charge de réseau ELB

Description

Vérifie l'utilisation qui représente plus de 80 % du quota de dispositifs d'équilibrage de charge de réseau ELB

ID de la vérification

`8wIqYSt25K`

Ressources supplémentaires

Quotas Elastic Load Balancing

Groupe IAM

Description

Vérifie l'utilisation qui représente plus de 80 % du quota de groupe IAM.

ID de la vérification

`sU7XX0l7J9`

Ressources supplémentaires

Quotas IAM

Profils d'instance IAM

Description

Vérifie l'utilisation qui représente plus de 80 % du quota de profils d'instance IAM.

ID de la vérification

`n07SS0l7J9`

Ressources supplémentaires

Quotas IAM

Politiques IAM

Description

Vérifie l'utilisation qui représente plus de 80 % du quota de politiques IAM.

ID de la vérification

`pR7UU0l7J9`

Ressources supplémentaires

Quotas IAM

Rôles IAM

Description

Vérifie l'utilisation qui représente plus de 80 % du quota de rôles IAM.

ID de la vérification

`oQ7TT0l7J9`

Ressources supplémentaires

Quotas IAM

Certificats de serveur IAM

Description

Vérifie l'utilisation qui représente plus de 80 % du quota de certificats de serveur IAM.

ID de la vérification

`rT7WW0l7J9`

Ressources supplémentaires

Quotas IAM

Utilisateurs IAM

Description

Vérifie l'utilisation qui représente plus de 80 % du quota d'utilisateurs IAM.

ID de la vérification

`qS7VV0l7J9`

Ressources supplémentaires

Quotas IAM

Partitions de Kinesis par région

Description

Vérifie l'utilisation de plus de 80 % des partitions Kinesis par quota de région.

ID de la vérification

`bW7HH0l7J9`

Ressources supplémentaires

Quotas Kinesis

Utilisation du stockage de code Lambda

Description

Détecte toute utilisation du stockage de code supérieure à 80 % de la limite du compte.

> **Note**
>
> Les résultats de cette vérification sont automatiquement actualisés plusieurs fois par jour et les demandes d'actualisation ne sont pas autorisées. Plusieurs heures peuvent encore être nécessaires pour que les modifications apparaissent. Actuellement, vous ne pouvez pas exclure des ressources de cette vérification.

ID de la vérification

`c1dfprch07`

Critères d'alerte

- Jaune : 80 % de la limite atteinte.

Action recommandée

Identifiez les fonctions ou versions Lambda inutilisées et supprimez-les afin de libérer de l'espace dans le stockage de code pour votre compte dans la région. Si vous avez besoin de stockage supplémentaire, créez une demande de support dans le Centre de support. Si vous pensez dépasser une limite de service, demandez une augmentation directement à partir de la console Service Quotas. Si Service Quotas ne prend pas encore en charge votre service, vous pouvez créer un cas de support dans le Centre de support.

Ressources supplémentaires

- Utilisation du stockage de code Lambda

Colonnes du rapport

- Statut
- Région
- ARN de fonction qualifié pour cette ressource
- L'utilisation du stockage du code de fonction est MegaBytes de 2 décimales.
- Nombre de versions de la fonction
- Heure de la dernière modification

Groupes de paramètres de cluster RDS

Description

Vérifie l'utilisation qui représente plus de 80 % du quota de groupes de paramètres de cluster RDS.

ID de la vérification

`jtlIMO3qZM`

Ressources supplémentaires

Quotas Amazon RDS

Rôles de cluster RDS

Description

Vérifie l'utilisation qui représente plus de 80 % du quota de rôles de cluster RDS.

ID de la vérification

`7fuccf1Mx7`

Ressources supplémentaires

Quotas Amazon RDS

Clusters RDS

Description

Vérifie l'utilisation qui représente plus de 80 % du quota de cluster RDS.

ID de la vérification

`gjqMBn6pjz`

Ressources supplémentaires

Quotas Amazon RDS

Instances de base de données RDS

Description

Vérifie l'utilisation qui représente plus de 80 % du quota d'instances de base de données RDS.

ID de la vérification

`XG0aXHpIEt`

Ressources supplémentaires

Quotas Amazon RDS

Instantanés manuels de base de données RDS

Description

Vérifie l'utilisation qui représente plus de 80 % du quota d'instantanés manuels de base de données RDS.

ID de la vérification

`dV84wpqRUs`

Ressources supplémentaires

Quotas Amazon RDS

Groupes de paramètres de base de données RDS

Description

Vérifie l'utilisation qui représente plus de 80 % du quota de groupes de paramètres de base de données RDS.

ID de la vérification

`jEECYg2YVU`

Ressources supplémentaires

Quotas Amazon RDS

Groupes de sécurité de base de données RDS

Description

Vérifie l'utilisation qui représente plus de 80 % du quota de groupes de sécurité de base de données RDS.

ID de la vérification

`gfZAn3W7wl`

Ressources supplémentaires

Quotas Amazon RDS

Abonnements aux événements RDS

Description

Vérifie l'utilisation qui représente plus de 80 % du quota d'abonnements aux événements RDS.

ID de la vérification

`keAhfbH5yb`

Ressources supplémentaires

Quotas Amazon RDS

Autorisations RDS maximum par groupe de sécurité

Description

Vérifie l'utilisation supérieure à 80 % des quotas d'autorisations RDS maximum par groupe de sécurité.

ID de la vérification

`dBkuNCvqn5`

Ressources supplémentaires

Quotas Amazon RDS

Groupes d'options RDS

Description

Vérifie l'utilisation qui représente plus de 80 % du quota de groupes d'options RDS.

ID de la vérification

`3Njm0DJQO9`

Ressources supplémentaires

Quotas Amazon RDS

Réplicas en lecture par master RDS

Description

Vérifie l'utilisation qui représente plus de 80 % du quota de réplicas en lecture RDS par master.

ID de la vérification

`pYW8UkYz2w`

Ressources supplémentaires

Quotas Amazon RDS

Instances réservées RDS

Description

Vérifie l'utilisation qui représente plus de 80 % du quota d'instances réservées RDS.

ID de la vérification

`UUDv0a5r34`

Ressources supplémentaires

Quotas Amazon RDS

Groupe de sous-réseaux RDS

Description

Vérifie l'utilisation qui représente plus de 80 % du quota de groupes de sous-réseaux RDS.

ID de la vérification

`dYWBaXaaMM`

Ressources supplémentaires

Quotas Amazon RDS

Sous-réseaux RDS par groupe de sous-réseaux

Description

Vérifie l'utilisation qui représente plus de 80 % du quota de sous-réseaux RDS par groupes de sous-réseaux.

ID de la vérification

`jEhCtdJK0Y`

Ressources supplémentaires

Quotas Amazon RDS

Quota total de stockage RDS

Description

Vérifie l'utilisation qui représente plus de 80 % du quota total de stockage RDS.

ID de la vérification

`P1jhKWEmLa`

Ressources supplémentaires

Quotas Amazon RDS

Zones hébergées Route 53

Description

Vérifie l'utilisation qui représente plus de 80 % du quota de zones hébergées Route 53 par compte.

ID de la vérification

`dx3xfcdfMr`

Ressources supplémentaires

Quotas Route 53

Surveillances de l'état maximum Route 53

Description

Vérifie l'utilisation qui représente plus de 80 % du quota de surveillances de l'état Route 53 par compte.

ID de la vérification

`ru4xfcdfMr`

Ressources supplémentaires

Quotas Route 53

Ensembles de délégations réutilisables Route 53

Description

Vérifie l'utilisation qui représente plus de 80 % du quota d'ensembles de délégation réutilisable Route 53 par compte.

ID de la vérification

`ty3xfcdfMr`

Ressources supplémentaires

Quotas Route 53

Politiques de trafic Route 53

Description

Vérifie l'utilisation qui représente plus de 80 % du quota de politiques de trafic Route 53 par compte.

ID de la vérification

`dx3xfbjfMr`

Ressources supplémentaires

Quotas Route 53

Instances de politique de trafic Route 53

Description

Vérifie l'utilisation qui représente plus de 80 % du quota d'instances de politique de trafic Route 53 par compte.

ID de la vérification

`dx8afcdfMr`

Ressources supplémentaires

Quotas Route 53

Quota d'envoi quotidien SES

Description

Vérifie l'utilisation qui représente plus de 80 % du quota d'envoi quotidien Amazon SES.

ID de la vérification

`hJ7NN0l7J9`

Ressources supplémentaires

Quotas Amazon SES

VPC

Description

Vérifie l'utilisation qui représente plus de 80 % du quota de VPC.

ID de la vérification

`jL7PP0l7J9`

Ressources supplémentaires

Quotas VPC

Passerelles Internet VPC

Description

Vérifie l'utilisation qui représente plus de 80 % du quota de passerelles Internet VPC.

ID de la vérification

`kM7QQ0l7J9`

Ressources supplémentaires

Quotas VPC

Excellence opérationnelle

Vous pouvez utiliser les vérifications suivantes pour la catégorie Excellence opérationnelle.

Noms des vérifications

- Amazon API Gateway ne consigne pas les journaux d'exécution
- API REST Amazon API Gateway sans suivi X-Ray
- Amazon CloudFront Access Log configuré
- Amazon CloudWatch Alarm Action est désactivée
- Instance Amazon EC2 non gérée par AWS Systems Manager
- Référentiel Amazon ECR avec immuabilité des balises désactivée
- Container Insights est désactivé sur les clusters Amazon ECS
- Journalisation des tâches Amazon ECS non activée
- La journalisation OpenSearch d'Amazon Service CloudWatch n'est pas configurée
- Instances de base de données Amazon RDS dans les clusters avec des groupes de paramètres hétérogènes
- La surveillance améliorée d'Amazon RDS est désactivée
- Amazon RDS Performance Insights est désactivé
- Le paramètre track_counts d'Amazon RDS est désactivé
- Journalisation des audits du cluster Amazon Redshift
- Les notifications d'événements ne sont pas activées dans Amazon S3

- Les rubriques Amazon SNS ne consignent pas l'état de distribution des messages
- Amazon VPC sans journaux de flux
- La journalisation d'accès est désactivée pour les Application Load Balancers et les Classic Load Balancers
- Notification de pile AWS CloudFormation
- Journalisation des événements de données AWS CloudTrail pour les objets d'un compartiment S3
- Journalisation des projets AWS CodeBuild
- Restauration et surveillance automatiques activées pour AWS CodeDeploy
- AWS CodeDeployLambda utilise all-at-once la configuration de déploiement
- Les rapports d'intégrité améliorés AWS Elastic Beanstalk ne sont pas configurés
- AWS Elastic Beanstalk avec les mises à jour de plateforme gérées désactivées
- La version de plateforme AWS Fargate n'est pas la plus récente
- L'association du gestionnaire d'états AWS Systems Manager n'est pas conforme
- CloudTrail les sentiers ne sont pas configurés avec Amazon CloudWatch Logs
- La protection contre la suppression d'Elastic Load Balancing n'est pas activée pour les équilibreurs de charge
- Vérification de la protection contre la suppression du cluster de base de données RDS
- Vérification de la mise à niveau automatique de version mineure de l'instance de base de données RDS

Amazon API Gateway ne consigne pas les journaux d'exécution

Description

Vérifie si les CloudWatch journaux sont activés sur Amazon API Gateway au niveau de journalisation souhaité.

Activez la CloudWatch journalisation pour les méthodes d'API WebSocket REST ou les routes d'API dans Amazon API Gateway afin de collecter les journaux d'exécution dans les CloudWatch journaux pour les demandes reçues par vos API. Les informations contenues dans les journaux d'exécution permettent d'identifier et de résoudre les problèmes liés à votre API.

Vous pouvez spécifier l'identifiant de niveau de journalisation (ERROR, INFO) dans le paramètre loggingLevel des règles AWS Config.

Reportez-vous à l'API REST ou à la documentation de l' WebSocket API pour plus d'informations sur la CloudWatch connexion à Amazon API Gateway.

> **Note**
>
> Les résultats de cette vérification sont automatiquement actualisés plusieurs fois par jour et les demandes d'actualisation ne sont pas autorisées. Plusieurs heures peuvent encore être nécessaires pour que les modifications apparaissent. Actuellement, vous ne pouvez pas exclure des ressources de cette vérification.

ID de la vérification

`c18d2gz125`

Source

`AWS Config Managed Rule: api-gw-execution-logging-enabled`

Critères d'alerte

Jaune : le paramètre de CloudWatch journalisation pour la collecte des journaux d'exécution n'est pas activé au niveau de journalisation souhaité pour un Amazon API Gateway.

Action recommandée

Activez la CloudWatch journalisation pour les journaux d'exécution de vos API REST Amazon API Gateway ou de vos WebSocket API avec le niveau de journalisation approprié (ERROR, INFO).

Pour plus d'informations, voir Création d'un journal de flux.

Ressources supplémentaires

- Configuration de la CloudWatch journalisation pour une API REST dans API Gateway
- Configuration de la journalisation pour une WebSocket API

Colonnes du rapport

- Statut
- Région
- Ressource
- Règle AWS Config
- Paramètres d'entrée
- Heure de la dernière modification

API REST Amazon API Gateway sans suivi X-Ray

Description

Vérifie si le suivi AWS X-Ray est activé pour les API REST Amazon API Gateway.

Activez le suivi X-Ray pour vos API REST afin de permettre à API Gateway de créer des exemples de demandes d'invocation d'API avec des informations de suivi. Vous pouvez ainsi tirer profit de AWS X-Ray pour suivre et analyser les demandes lorsqu'elles transitent par vos API REST API Gateway vers les services en aval.

Pour plus d'informations, voir Suivi des demandes utilisateur vers les API REST à l'aide de X-Ray.

> **Note**
>
> Les résultats de cette vérification sont automatiquement actualisés plusieurs fois par jour et les demandes d'actualisation ne sont pas autorisées. Plusieurs heures peuvent encore être nécessaires pour que les modifications apparaissent. Actuellement, vous ne pouvez pas exclure des ressources de cette vérification.

ID de la vérification

`c18d2gz126`

Source

`AWS Config Managed Rule: api-gw-xray-enabled`

Critères d'alerte

Jaune : le suivi X-Ray n'est pas activé pour une API REST API Gateway.

Action recommandée

Activez le suivi X-Ray pour vos API REST API Gateway.

Pour plus d'informations, voir Configuration de AWS X-Ray avec les API REST API Gateway.

Ressources supplémentaires

- Suivi des demandes utilisateur vers les API REST à l'aide de X-Ray
- Présentation de AWS X-Ray

Colonnes du rapport

- Statut
- Région
- Ressource
- Règle AWS Config
- Paramètres d'entrée
- Heure de la dernière modification

Amazon CloudFront Access Log configuré

Description

Vérifie si les CloudFront distributions Amazon sont configurées pour capturer des informations à partir des journaux d'accès au serveur Amazon S3. Les journaux d'accès au serveur Amazon S3 contiennent des informations détaillées sur chaque demande d'utilisateur CloudFront reçue.

Vous pouvez ajuster le nom du compartiment Amazon S3 pour stocker les journaux d'accès au serveur, en utilisant le BucketName paramètre S3 dans vos AWS Config règles.

Pour plus d'informations, voir Configuration et utilisation des journaux standard (journaux d'accès).

> **Note**
>
> Les résultats de cette vérification sont automatiquement actualisés plusieurs fois par jour et les demandes d'actualisation ne sont pas autorisées. Plusieurs heures peuvent encore être nécessaires pour que les modifications apparaissent. Actuellement, vous ne pouvez pas exclure des ressources de cette vérification.

ID de la vérification

```
c18d2gz110
```

Source

```
AWS Config Managed Rule: cloudfront-accesslogs-enabled
```

Critères d'alerte

Jaune : la journalisation des CloudFront accès à Amazon n'est pas activée

Action recommandée

Assurez-vous d'activer la journalisation des CloudFront accès pour recueillir des informations détaillées sur chaque demande d'utilisateur CloudFront reçue.

Vous pouvez activer les journaux standard lorsque vous créez ou mettez à jour une distribution.

Pour plus d'informations, voir Valeurs que vous spécifiez lorsque vous créez ou mettez à jour une distribution.

Ressources supplémentaires

- Valeurs que vous spécifiez lorsque vous créez ou mettez à jour une distribution
- Configuration et utilisation des journaux standard (journaux d'accès)

Colonnes du rapport

- Statut
- Région
- Ressource
- Règle AWS Config
- Paramètres d'entrée
- Heure de la dernière modification

Amazon CloudWatch Alarm Action est désactivée

Description

Vérifie si votre action d' CloudWatch alarme Amazon est désactivée.

Vous pouvez utiliser la AWS CLI pour activer ou désactiver la fonctionnalité d'action de votre alarme. Vous pouvez également activer ou désactiver la fonctionnalité d'action à l'aide du AWS SDK. Lorsque la fonction d'action d'alarme est désactivée, CloudWatch elle n'exécute aucune action définie dans aucun état (OK, INSUFFIENT_DATA, ALARM).

> **Note**
>
> Les résultats de cette vérification sont automatiquement actualisés plusieurs fois par jour et les demandes d'actualisation ne sont pas autorisées. Plusieurs heures peuvent encore

être nécessaires pour que les modifications apparaissent. Actuellement, vous ne pouvez pas exclure des ressources de cette vérification.

ID de la vérification

`c18d2gz109`

Source

`AWS Config Managed Rule: cloudwatch-alarm-action-enabled-check`

Critères d'alerte

Jaune : l'action CloudWatch d'alarme Amazon n'est pas activée. Aucune action n'est effectuée, quel que soit l'état d'alarme.

Action recommandée

Activez les actions dans vos CloudWatch alarmes, sauf si vous avez une raison valable de les désactiver, par exemple à des fins de test.

Si l' CloudWatch alarme n'est plus nécessaire, supprimez-la pour éviter des coûts inutiles.

Pour plus d'informations, reportez-vous enable-alarm-actionsà la section AWS CLI Command Reference et à func (*CloudWatch) EnableAlarmActions à la référence de l'AWSAPI SDK for Go.

Colonnes du rapport

- Statut
- Région
- Ressource
- Règle AWS Config
- Paramètres d'entrée
- Heure de la dernière modification

Instance Amazon EC2 non gérée par AWS Systems Manager

Description

Vérifie si les instances Amazon EC2 de votre compte sont gérées par AWS Systems Manager.

Systems Manager vous aide à comprendre et à contrôler l'état actuel de votre instance Amazon EC2 et de vos configurations de système d'exploitation. Avec Systems Manager, vous pouvez collecter des informations de configuration logicielle et d'inventaire concernant votre flotte d'instances, y compris les logiciels installés sur celles-ci. Cela vous permet de suivre de très près la configuration système, les niveaux de correctifs du système d'exploitation, les configurations des applications et d'obtenir d'autres informations concernant votre déploiement.

Pour plus d'informations, voir Configuration de Systems Manager pour les instances EC2.

> **Note**
>
> Les résultats de cette vérification sont automatiquement actualisés plusieurs fois par jour et les demandes d'actualisation ne sont pas autorisées. Plusieurs heures peuvent encore être nécessaires pour que les modifications apparaissent. Actuellement, vous ne pouvez pas exclure des ressources de cette vérification.

ID de la vérification

`c18d2gz145`

Source

`AWS Config Managed Rule: ec2-instance-managed-by-systems-manager`

Critères d'alerte

Jaune : les instances Amazon EC2 ne sont pas gérées par Systems Manager.

Action recommandée

Configurez votre instance Amazon EC2 de sorte qu'elle soit gérée par Systems Manager.

Cette vérification ne peut pas être exclue de la vue dans la console Trusted Advisor.

Pour plus d'informations, voir Pourquoi mon instance EC2 ne s'affiche-t-elle pas en tant que nœud géré ou affiche-t-elle l'état « Perte de connexion » dans Systems Manager ?.

Ressources supplémentaires

Configuration de Systems Manager pour les instances EC2

Colonnes du rapport

- Statut

- Région
- Ressource
- Règle AWS Config
- Paramètres d'entrée
- Heure de la dernière modification

Référentiel Amazon ECR avec immuabilité des balises désactivée

Description

Vérifie si l'immuabilité des balises d'image est activée dans un référentiel Amazon ECR privé.

Activez l'immuabilité des balises d'image pour un référentiel Amazon ECR privé afin d'empêcher l'écrasement des balises d'image. Cela vous permet de vous appuyer sur les balises descriptives en tant que mécanisme fiable pour suivre et identifier des images de manière unique. Par exemple, si l'immuabilité des balises d'image est activée, les utilisateurs peuvent utiliser une balise d'image de manière fiable pour corréler une version d'image déployée avec le générateur qui a produit cette image.

Pour plus d'informations, voir Mutabilité des balises d'image.

> **Note**
>
> Les résultats de cette vérification sont automatiquement actualisés plusieurs fois par jour et les demandes d'actualisation ne sont pas autorisées. Plusieurs heures peuvent encore être nécessaires pour que les modifications apparaissent. Actuellement, vous ne pouvez pas exclure des ressources de cette vérification.

ID de la vérification

`c18d2gz129`

Source

`AWS Config Managed Rule: ecr-private-tag-immutability-enabled`

Critères d'alerte

Jaune : l'immuabilité des balises n'est pas activée pour un référentiel privé Amazon ECR.

Action recommandée

Activez l'immuabilité des balises d'image pour vos référentiels privés Amazon ECR.

Pour plus d'informations, voir Mutabilité des balises d'image.

Colonnes du rapport

- Statut
- Région
- Ressource
- Règle AWS Config
- Paramètres d'entrée
- Heure de la dernière modification

Container Insights est désactivé sur les clusters Amazon ECS

Description

Vérifie si Amazon CloudWatch Container Insights est activé pour vos clusters Amazon ECS.

CloudWatch Container Insights collecte, agrège et résume les métriques et les journaux de vos applications conteneurisées et de vos microservices. Les métriques incluent l'utilisation des ressources telles que l'UC, la mémoire, le disque et le réseau.

Pour plus d'informations, consultez Amazon ECS CloudWatch Container Insights.

> **Note**
>
> Les résultats de cette vérification sont automatiquement actualisés plusieurs fois par jour et les demandes d'actualisation ne sont pas autorisées. Plusieurs heures peuvent encore être nécessaires pour que les modifications apparaissent. Actuellement, vous ne pouvez pas exclure des ressources de cette vérification.

ID de la vérification

`c18d2gz173`

Source

`AWS Config Managed Rule: ecs-container-insights-enabled`

Critères d'alerte

Jaune : Container Insights n'est pas activé pour les clusters Amazon ECS.

Action recommandée

Activez CloudWatch Container Insights sur vos clusters Amazon ECS.

Pour plus d'informations, voir Utilisation de Container Insights.

Ressources supplémentaires

Informations sur les CloudWatch conteneurs Amazon ECS

Colonnes du rapport

- Statut
- Région
- Ressource
- Règle AWS Config
- Paramètres d'entrée
- Heure de la dernière modification

Journalisation des tâches Amazon ECS non activée

Description

Vérifie si la configuration de la journalisation est active dans les définitions de tâches Amazon ECS.

La vérification de la configuration de la journalisation dans vos définitions de tâches Amazon ECS garantit que les journaux générés par les conteneurs sont correctement configurés et stockés. Cela permet d'identifier et de résoudre les problèmes plus rapidement, d'optimiser les performances et de répondre aux exigences de conformité.

Par défaut, les journaux qui sont capturés affichent la sortie de commande qui s'affiche normalement dans un terminal interactif si vous exécutez le conteneur localement. Le pilote awslogs transmet ces journaux de Docker à Amazon Logs. CloudWatch

Pour plus d'informations, voir Utilisation du pilote de journalisation awslogs.

> **Note**
>
> Les résultats de cette vérification sont automatiquement actualisés plusieurs fois par jour et les demandes d'actualisation ne sont pas autorisées. Plusieurs heures peuvent encore être nécessaires pour que les modifications apparaissent. Actuellement, vous ne pouvez pas exclure des ressources de cette vérification.

ID de la vérification

`c18d2gz175`

Source

`AWS Config Managed Rule: ecs-task-definition-log-configuration`

Critères d'alerte

Jaune : la définition de tâche Amazon ECS ne comprend aucune configuration de journalisation.

Action recommandée

Envisagez de spécifier la configuration du pilote de journal dans la définition du conteneur pour envoyer les informations de journal à CloudWatch Logs ou à un autre pilote de journalisation.

Pour plus d'informations, consultez LogConfiguration.

Ressources supplémentaires

Envisagez de spécifier la configuration du pilote de journal dans la définition du conteneur pour envoyer les informations de journal à CloudWatch Logs ou à un autre pilote de journalisation.

Pour plus d'informations, voir Exemples de définitions de tâches.

Colonnes du rapport

- Statut
- Région
- Ressource
- Règle AWS Config
- Paramètres d'entrée

- Heure de la dernière modification

La journalisation OpenSearch d'Amazon Service CloudWatch n'est pas configurée

Description

Vérifie si les domaines Amazon OpenSearch Service sont configurés pour envoyer des journaux à Amazon CloudWatch Logs.

La surveillance des journaux est essentielle pour maintenir la fiabilité, la disponibilité et les performances du OpenSearch Service.

Les journaux lents de recherche, les journaux lents d'indexation et les journaux d'erreurs permettent de résoudre les problèmes de performances et de stabilité de votre charge de travail. Ces journaux doivent être activés pour permettre la capture de données.

Vous pouvez spécifier les types de journaux à filtrer (journaux d'erreur, de recherche ou d'indexation) à l'aide du paramètre logTypes de vos règles AWS Config.

Pour plus d'informations, consultez la section Surveillance des domaines Amazon OpenSearch Service.

> **Note**
>
> Les résultats de cette vérification sont automatiquement actualisés plusieurs fois par jour et les demandes d'actualisation ne sont pas autorisées. Plusieurs heures peuvent encore être nécessaires pour que les modifications apparaissent. Actuellement, vous ne pouvez pas exclure des ressources de cette vérification.

ID de la vérification

`c18d2gz184`

Source

`AWS Config Managed Rule: opensearch-logs-to-cloudwatch`

Critères d'alerte

Jaune : Amazon OpenSearch Service n'a pas de configuration de journalisation avec Amazon CloudWatch Logs

Action recommandée

Configurez les domaines de OpenSearch service pour publier les CloudWatch journaux dans Logs.

Pour plus d'informations, voir Activation de la publication des journaux (console).

Ressources supplémentaires

- Surveillance des métriques du cluster OpenSearch Service avec Amazon CloudWatch

Colonnes du rapport

- Statut
- Région
- Ressource
- Règle AWS Config
- Paramètres d'entrée
- Heure de la dernière modification

Instances de base de données Amazon RDS dans les clusters avec des groupes de paramètres hétérogènes

Description

Nous recommandons que toutes les instances de base de données du cluster de base de données utilisent le même groupe de paramètres de base de données.

> **Note**
>
> Les résultats de cette vérification sont automatiquement actualisés plusieurs fois par jour et les demandes d'actualisation ne sont pas autorisées. Plusieurs heures peuvent encore être nécessaires pour que les modifications apparaissent. Actuellement, vous ne pouvez pas exclure des ressources de cette vérification.

> **Note**
>
> Lorsqu'une instance ou un cluster de bases de données est arrêté, vous pouvez consulter les recommandations Amazon RDS Trusted Advisor pendant 3 à 5 jours. Après cinq jours,

les recommandations ne sont plus disponibles dansTrusted Advisor. Pour consulter les recommandations, ouvrez la console Amazon RDS, puis choisissez Recommendations. Si vous supprimez une instance ou un cluster de bases de données, les recommandations associées à ces instances ou clusters ne sont pas disponibles dans Trusted Advisor ou dans la console de gestion Amazon RDS.

ID de la vérification

`c1qf5bt010`

Critères d'alerte

Jaune : les clusters de base de données contiennent des instances de base de données avec des groupes de paramètres hétérogènes.

Action recommandée

Associez l'instance de base de données au groupe de paramètres de base de données associé à l'instance d'écriture dans votre cluster de base de données.

Ressources supplémentaires

Lorsque les instances de base de données de votre cluster de base de données utilisent différents groupes de paramètres de base de données, il peut y avoir un comportement incohérent lors d'un basculement ou des problèmes de compatibilité entre les instances de base de données de votre cluster de base de données.

Pour plus d'informations, veuillez consulter Utilisation des groupes de paramètres.

Colonnes du rapport

- Statut
- Région
- Ressource
- Valeur recommandée
- Nom du moteur
- Heure de la dernière modification

La surveillance améliorée d'Amazon RDS est désactivée

Description

La surveillance améliorée n'est pas activée sur les ressources de votre base de données. La surveillance améliorée fournit des métriques de système d'exploitation en temps réel pour la surveillance et le dépannage.

> **Note**
>
> Les résultats de cette vérification sont automatiquement actualisés plusieurs fois par jour et les demandes d'actualisation ne sont pas autorisées. Plusieurs heures peuvent encore être nécessaires pour que les modifications apparaissent. Actuellement, vous ne pouvez pas exclure des ressources de cette vérification.

> **Note**
>
> Lorsqu'une instance ou un cluster de bases de données est arrêté, vous pouvez consulter les recommandations Amazon RDS Trusted Advisor pendant 3 à 5 jours. Après cinq jours, les recommandations ne sont plus disponibles dansTrusted Advisor. Pour consulter les recommandations, ouvrez la console Amazon RDS, puis choisissez Recommendations. Si vous supprimez une instance ou un cluster de bases de données, les recommandations associées à ces instances ou clusters ne sont pas disponibles dans Trusted Advisor ou dans la console de gestion Amazon RDS.

ID de la vérification

`c1qf5bt004`

Critères d'alerte

Jaune : la surveillance améliorée n'est pas activée sur les ressources Amazon RDS.

Action recommandée

Activez la surveillance améliorée.

Ressources supplémentaires

La surveillance améliorée pour Amazon RDS fournit une visibilité supplémentaire sur l'état de vos instances de base de données. Nous vous recommandons d'activer la surveillance améliorée. Lorsque l'option Enhanced Monitoring est activée pour votre instance de base de données, elle collecte des métriques vitales du système d'exploitation et des informations de processus.

Pour plus d'informations, voir Surveillance des métriques du système d'exploitation à l'aide de la surveillance améliorée.

Colonnes du rapport

- Statut
- Région
- Ressource
- Valeur recommandée
- Nom du moteur
- Heure de la dernière modification

Amazon RDS Performance Insights est désactivé

Description

Amazon RDS Performance Insights surveille la charge de votre instance de base de données pour vous aider à analyser et à résoudre les problèmes de performance des bases de données. Nous vous recommandons d'activer Performance Insights.

> **Note**
>
> Les résultats de cette vérification sont automatiquement actualisés plusieurs fois par jour et les demandes d'actualisation ne sont pas autorisées. Plusieurs heures peuvent encore être nécessaires pour que les modifications apparaissent. Actuellement, vous ne pouvez pas exclure des ressources de cette vérification.

> **Note**
>
> Lorsqu'une instance ou un cluster de bases de données est arrêté, vous pouvez consulter les recommandations Amazon RDS Trusted Advisor pendant 3 à 5 jours. Après cinq jours,

les recommandations ne sont plus disponibles dansTrusted Advisor. Pour consulter les recommandations, ouvrez la console Amazon RDS, puis choisissez Recommendations. Si vous supprimez une instance ou un cluster de bases de données, les recommandations associées à ces instances ou clusters ne sont pas disponibles dans Trusted Advisor ou dans la console de gestion Amazon RDS.

ID de la vérification

`c1qf5bt012`

Critères d'alerte

Jaune : Performance Insights n'est pas activé sur les ressources Amazon RDS.

Action recommandée

Activer l'option Performance Insights.

Ressources supplémentaires

Performance Insights utilise une méthode de collecte de données légère qui n'a aucun impact sur les performances de vos applications. Performance Insights vous aide à évaluer rapidement la charge de la base de données.

Pour plus d'informations, consultez la section Surveillance de la charge de base de données avec Performance Insights sur Amazon RDS.

Colonnes du rapport

- Statut
- Région
- Ressource
- Valeur recommandée
- Nom du moteur
- Heure de la dernière modification

Le paramètre track_counts d'Amazon RDS est désactivé

Description

Lorsque le paramètre track_counts est désactivé, la base de données ne collecte pas les statistiques d'activité de la base de données. Autovacuum a besoin de ces statistiques pour fonctionner correctement.

Nous vous recommandons de définir le paramètre track_counts sur 1

> **Note**
>
> Les résultats de cette vérification sont automatiquement actualisés plusieurs fois par jour et les demandes d'actualisation ne sont pas autorisées. Plusieurs heures peuvent encore être nécessaires pour que les modifications apparaissent. Actuellement, vous ne pouvez pas exclure des ressources de cette vérification.

> **Note**
>
> Lorsqu'une instance ou un cluster de bases de données est arrêté, vous pouvez consulter les recommandations Amazon RDS Trusted Advisor pendant 3 à 5 jours. Après cinq jours, les recommandations ne sont plus disponibles dansTrusted Advisor. Pour consulter les recommandations, ouvrez la console Amazon RDS, puis choisissez Recommendations. Si vous supprimez une instance ou un cluster de bases de données, les recommandations associées à ces instances ou clusters ne sont pas disponibles dans Trusted Advisor ou dans la console de gestion Amazon RDS.

ID de la vérification

`c1qf5bt027`

Critères d'alerte

Jaune : le paramètre track_counts est désactivé pour les groupes de paramètres de base de données.

Action recommandée

Définissez le paramètre track_counts sur 1

Ressources supplémentaires

Lorsque le paramètre track_counts est désactivé, il désactive la collecte des statistiques d'activité de la base de données. Le démon autovacuum a besoin des statistiques collectées pour identifier les tables pour autovacuum et autoanalysis.

Pour plus d'informations, consultez la section Statistiques d'exécution pour PostgreSQL sur le site Web de documentation de PostgreSQL.

Colonnes du rapport

- Statut
- Région
- Ressource
- Valeur de paramètre
- Valeur recommandée
- Heure de la dernière modification

Journalisation des audits du cluster Amazon Redshift

Description

Vérifie si la journalisation des audits de base de données est activée sur vos clusters Amazon Redshift. Amazon Redshift consigne dans un journal les informations sur les connexions et les activités de l'utilisateur dans votre base de données.

Vous pouvez spécifier le nom de compartiment Amazon S3 de journalisation de votre choix dans le paramètre bucketNames de vos règles AWS Config.

Pour plus d'informations, voir Journalisation des audits de base de données.

> **Note**
>
> Les résultats de cette vérification sont automatiquement actualisés plusieurs fois par jour et les demandes d'actualisation ne sont pas autorisées. Plusieurs heures peuvent encore être nécessaires pour que les modifications apparaissent. Actuellement, vous ne pouvez pas exclure des ressources de cette vérification.

ID de la vérification

`c18d2gz134`

Source

`AWS Config Managed Rule: redshift-audit-logging-enabled`

Critères d'alerte

Jaune : la journalisation des audits de base de données est désactivée dans un cluster Amazon Redshift.

Action recommandée

Activez la journalisation et la surveillance pour vos clusters Amazon Redshift.

Pour plus d'informations, voir Configuration des audits à l'aide de la console.

Ressources supplémentaires

Journalisation et surveillance dans Amazon Redshift

Colonnes du rapport

- Statut
- Région
- Ressource
- Règle AWS Config
- Paramètres d'entrée
- Heure de la dernière modification

Les notifications d'événements ne sont pas activées dans Amazon S3

Description

Vérifie si les notifications d'événements Amazon S3 sont activées ou correctement configurées avec la destination ou les types souhaités.

Vous pouvez utiliser la fonctionnalité Notifications d'événements Amazon S3 pour recevoir des notifications lorsque certains événements se produisent dans votre compartiment Amazon S3. Amazon S3 peut envoyer des notifications aux files d'attente Amazon SQS, aux rubriques SNS et aux fonctions AWS Lambda.

Vous pouvez spécifier la destination et les types d'événements souhaités à l'aide des paramètres destinationArn et eventTypes de vos règles AWS Config.

Pour plus d'informations, voir Notifications d'événements Amazon S3.

> **Note**
>
> Les résultats de cette vérification sont automatiquement actualisés plusieurs fois par jour et les demandes d'actualisation ne sont pas autorisées. Plusieurs heures peuvent encore être nécessaires pour que les modifications apparaissent. Actuellement, vous ne pouvez pas exclure des ressources de cette vérification.

ID de la vérification

`c18d2gz163`

Source

`AWS Config Managed Rule: s3-event-notifications-enabled`

Critères d'alerte

Jaune : les notifications d'événements ne sont pas activées ou ne sont pas configurées avec la destination ou les types souhaités dans Amazon S3.

Action recommandée

Configurez les notifications d'événements Amazon S3 pour les événements liés aux objets et aux compartiments.

Pour plus d'informations, voir Activation et configuration des notifications d'événements à l'aide de la console Amazon S3.

Colonnes du rapport

- Statut
- Région
- Ressource
- Règle AWS Config
- Paramètres d'entrée
- Heure de la dernière modification

Les rubriques Amazon SNS ne consignent pas l'état de distribution des messages

Description

Vérifie si la journalisation de l'état de distribution des messages est activée dans les rubriques Amazon SNS.

Configurez les rubriques Amazon SNS pour consigner l'état de distribution des messages afin de fournir de meilleures informations opérationnelles. Par exemple, la journalisation de la distribution des messages vérifie si un message a été distribué à un point de terminaison Amazon SNS spécifique. Elle permet également d'identifier la réponse envoyée par le point de terminaison.

Pour plus d'informations, voir État de distribution des messages Amazon SNS.

> **Note**
>
> Les résultats de cette vérification sont automatiquement actualisés plusieurs fois par jour et les demandes d'actualisation ne sont pas autorisées. Plusieurs heures peuvent encore être nécessaires pour que les modifications apparaissent. Actuellement, vous ne pouvez pas exclure des ressources de cette vérification.

ID de la vérification

`c18d2gz121`

Source

`AWS Config Managed Rule: sns-topic-message-delivery-notification-enabled`

Critères d'alerte

Jaune : la journalisation de l'état de distribution des messages n'est pas activée pour une rubrique Amazon SNS.

Action recommandée

Activez la journalisation de l'état de distribution des messages pour vos rubriques SNS.

Pour plus d'informations, voir Configuration de la journalisation de l'état de distribution à l'aide de la console de gestion AWS.

Colonnes du rapport

- Statut

- Région
- Ressource
- Règle AWS Config
- Paramètres d'entrée
- Heure de la dernière modification

Amazon VPC sans journaux de flux

Description

Vérifie si des journaux de flux Amazon Virtual Private Cloud sont créés pour un VPC.

Vous pouvez spécifier le type de trafic à l'aide du paramètre trafficType de vos règles AWS Config.

Pour plus d'informations, voir Journalisation du trafic IP à l'aide des journaux de flux VPC.

> **Note**
>
> Les résultats de cette vérification sont automatiquement actualisés plusieurs fois par jour et les demandes d'actualisation ne sont pas autorisées. Plusieurs heures peuvent encore être nécessaires pour que les modifications apparaissent. Actuellement, vous ne pouvez pas exclure des ressources de cette vérification.

ID de la vérification

`c18d2gz122`

Source

`AWS Config Managed Rule: vpc-flow-logs-enabled`

Critères d'alerte

Jaune : les VPC ne disposent pas de journaux de flux Amazon VPC.

Action recommandée

Créez des journaux de flux VPC pour chacun de vos VPC.

Pour plus d'informations, voir Création d'un journal de flux.

Colonnes du rapport

- Statut
- Région
- Ressource
- Règle AWS Config
- Paramètres d'entrée
- Heure de la dernière modification

La journalisation d'accès est désactivée pour les Application Load Balancers et les Classic Load Balancers

Description

Vérifie si la journalisation d'accès est activée pour les Application Load Balancers et les Classic Load Balancers.

Elastic Load Balancing fournit des journaux d'accès qui capturent des informations détaillées sur les demandes envoyées à votre équilibreur de charge. Chaque journal contient des informations comme l'heure à laquelle la demande a été reçue, l'adresse IP du client, les latences, les chemins de demande et les réponses du serveur. Vous pouvez utiliser ces journaux d'accès pour analyser les modèles de trafic et résoudre des problèmes.

Les journaux d'accès sont une fonctionnalité facultative d'Elastic Load Balancing qui est désactivée par défaut. Une fois que vous avez activé les journaux d'accès pour votre équilibreur de charge, Elastic Load Balancing capture les journaux et les stocke dans le compartiment Amazon S3 que vous spécifiez.

Vous pouvez spécifier le paquet Amazon S3 du journal d'accès que vous souhaitez vérifier à l'aide du BucketNames paramètre s3 de vos AWS Config règles.

Pour plus d'informations, voir Journalisation d'accès pour votre Application Load Balancer ou Journalisation d'accès pour votre Classic Load Balancer.

> **Note**
>
> Les résultats de cette vérification sont automatiquement actualisés plusieurs fois par jour et les demandes d'actualisation ne sont pas autorisées. Plusieurs heures peuvent encore

être nécessaires pour que les modifications apparaissent. Actuellement, vous ne pouvez pas exclure des ressources de cette vérification.

ID de la vérification

`c18d2gz167`

Source

`AWS Config Managed Rule: elb-logging-enabled`

Critères d'alerte

Jaune : la fonctionnalité de journalisation d'accès n'est pas activée pour un Application Load Balancer ou un Classic Load Balancer.

Action recommandée

Activez la journalisation d'accès pour les Application Load Balancers et les Classic Load Balancers.

Pour plus d'informations, voir Activation de la journalisation d'accès pour votre Application Load Balancer ou Activation de la journalisation d'accès pour votre Classic Load Balancer.

Colonnes du rapport

- Statut
- Région
- Ressource
- Règle AWS Config
- Paramètres d'entrée
- Heure de la dernière modification

Notification de pile AWS CloudFormation

Description

Vérifie si toutes vos piles AWS CloudFormation utilisent Amazon SNS pour recevoir des notifications lorsqu'un événement se produit.

Vous pouvez configurer cette vérification pour rechercher des ARN de rubrique Amazon SNS spécifiques à l'aide des paramètres de vos règles AWS Config.

Pour plus d'informations, voir Définition des options de pile AWS CloudFormation.

> **Note**
>
> Les résultats de cette vérification sont automatiquement actualisés plusieurs fois par jour et les demandes d'actualisation ne sont pas autorisées. Plusieurs heures peuvent encore être nécessaires pour que les modifications apparaissent. Actuellement, vous ne pouvez pas exclure des ressources de cette vérification.

ID de la vérification

`c18d2gz111`

Source

`AWS Config Managed Rule: cloudformation-stack-notification-check`

Critères d'alerte

Jaune : les notifications d'événements Amazon SNS pour vos piles AWS CloudFormation ne sont pas activées.

Action recommandée

Vérifiez que toutes vos piles AWS CloudFormation utilisent Amazon SNS pour recevoir des notifications lorsqu'un événement se produit.

La surveillance des événements de pile vous permet de réagir rapidement en cas d'actions non autorisées susceptibles de modifier votre environnement AWS.

Ressources supplémentaires

Comment puis-je recevoir une alerte par e-mail lorsque ma CloudFormation pile AWS passe au statut ROLLBACK_IN_PROGRESS ?

Colonnes du rapport

- Statut
- Région
- Ressource
- Règle AWS Config
- Paramètres d'entrée
- Heure de la dernière modification

Journalisation des événements de données AWS CloudTrail pour les objets d'un compartiment S3

Description

Vérifie si au moins un suivi AWS CloudTrail enregistre les événements de données Amazon S3 pour tous vos compartiments Amazon S3.

Pour plus d'informations, voir Journalisation des appels d'API Amazon S3 à l'aide de AWS CloudTrail.

> **Note**
>
> Les résultats de cette vérification sont automatiquement actualisés plusieurs fois par jour et les demandes d'actualisation ne sont pas autorisées. Plusieurs heures peuvent encore être nécessaires pour que les modifications apparaissent. Actuellement, vous ne pouvez pas exclure des ressources de cette vérification.

ID de la vérification

`c18d2gz166`

Source

`AWS Config Managed Rule: cloudtrail-s3-dataevents-enabled`

Critères d'alerte

Jaune : la journalisation des événements AWS CloudTrail pour les compartiments Amazon S3 n'est pas configurée.

Action recommandée

Activez la journalisation des CloudTrail événements pour les compartiments et les objets Amazon S3 afin de suivre les demandes d'accès au compartiment cible.

Pour plus d'informations, consultez Activation de la journalisation des CloudTrail événements pour les compartiments et objets S3.

Colonnes du rapport

- Statut
- Région

- Ressource
- Règle AWS Config
- Paramètres d'entrée
- Heure de la dernière modification

Journalisation des projets AWS CodeBuild

Description

Vérifie si l'environnement de projet AWS CodeBuild utilise la journalisation. Les options de journalisation peuvent être des CloudWatch journaux dans Amazon Logs, des journaux intégrés à un compartiment Amazon S3 spécifique, ou les deux. L'activation de la connexion à un CodeBuild projet peut apporter plusieurs avantages, tels que le débogage et l'audit.

Vous pouvez spécifier le nom du bucket ou du groupe CloudWatch Logs Amazon S33 pour stocker les journaux, en utilisant le paramètre s3 BucketNames ou cloudWatchGroupNames dans vos AWS Config règles.

Pour de plus amples informations, veuillez consulter la section relative à la surveillance AWS CodeBuild.

> **Note**
>
> Les résultats de cette vérification sont automatiquement actualisés plusieurs fois par jour et les demandes d'actualisation ne sont pas autorisées. Plusieurs heures peuvent encore être nécessaires pour que les modifications apparaissent. Actuellement, vous ne pouvez pas exclure des ressources de cette vérification.

ID de la vérification

```
c18d2gz113
```

Source

```
AWS Config Managed Rule: codebuild-project-logging-enabled
```

Critères d'alerte

Jaune : la journalisation des projets AWS CodeBuild n'est pas activée.

Action recommandée

Assurez-vous que la journalisation est activée dans votre projet AWS CodeBuild. Cette vérification ne peut pas être exclue de la vue dans la console AWS Trusted Advisor.

Pour plus d'informations, voir Journalisation et surveillance dans AWS CodeBuild.

Colonnes du rapport

- Statut
- Région
- Ressource
- Règle AWS Config
- Paramètres d'entrée
- Heure de la dernière modification

Restauration et surveillance automatiques activées pour AWS CodeDeploy

Description

Vérifie si la restauration et la surveillance automatiques du déploiement avec les alarmes attachées sont activées pour le groupe de déploiement. En cas de problème lors d'un déploiement, celui-ci est automatiquement restauré et votre application reste dans un état stable.

Pour plus d'informations, consultez Redéployer et annuler un déploiement avec CodeDeploy.

> **Note**
>
> Les résultats de cette vérification sont automatiquement actualisés plusieurs fois par jour et les demandes d'actualisation ne sont pas autorisées. Plusieurs heures peuvent encore être nécessaires pour que les modifications apparaissent. Actuellement, vous ne pouvez pas exclure des ressources de cette vérification.

ID de la vérification

```
c18d2gz114
```

Source

```
AWS Config Managed Rule: codedeploy-auto-rollback-monitor-enabled
```

Critères d'alerte

Jaune : la restauration et la surveillance automatiques du déploiement AWS CodeDeploy ne sont pas activées.

Action recommandée

Configurez un groupe de déploiement ou un déploiement pour être annulés automatiquement lorsqu'un déploiement échoue, ou lorsqu'une limite de surveillance que vous spécifiez est atteinte.

Configurez une alarme pour surveiller différentes métriques, comme l'utilisation de l'UC, de la mémoire ou le trafic réseau pendant le processus de déploiement. Si l'une de ces métriques dépasse certaines limites, les alarmes se déclenchent et le déploiement est arrêté ou annulé.

Pour plus d'informations sur la configuration des annulations automatiques et des alarmes pour vos groupes de déploiement, voir Configuration des options avancées pour un groupe de déploiement.

Ressources supplémentaires

Qu'est-ce que c'est CodeDeploy ?

Colonnes du rapport

- Statut
- Région
- Ressource
- Règle AWS Config
- Paramètres d'entrée
- Heure de la dernière modification

AWS CodeDeployLambda utilise all-at-once la configuration de déploiement

Description

Vérifie si le groupe AWS CodeDeploy de déploiement de la plate-forme de AWS Lambda calcul utilise la configuration de all-at-once déploiement.

Pour réduire le risque d'échec du déploiement de vos fonctions Lambda dans CodeDeploy, il est recommandé d'utiliser la configuration de déploiement Canary ou linéaire au lieu de l'option par défaut selon laquelle tout le trafic est transféré de la fonction Lambda d'origine vers la fonction mise à jour en une fois.

Pour plus d'informations, voir Versions des fonctions Lambda et Configuration du déploiement.

> **Note**
>
> Les résultats de cette vérification sont automatiquement actualisés plusieurs fois par jour et les demandes d'actualisation ne sont pas autorisées. Plusieurs heures peuvent encore être nécessaires pour que les modifications apparaissent. Actuellement, vous ne pouvez pas exclure des ressources de cette vérification.

ID de la vérification

`c18d2gz115`

Source

`AWS Config Managed Rule: codedeploy-lambda-allatonce-traffic-shift-disabled`

Critères d'alerte

Jaune : le déploiement AWS CodeDeploy Lambda utilise la configuration de all-at-once déploiement pour transférer simultanément tout le trafic vers les fonctions Lambda mises à jour.

Action recommandée

Utilisez la configuration de déploiement Canary ou Linear du groupe de CodeDeploy déploiement pour la plate-forme de calcul Lambda.

Ressources supplémentaires

Configuration de déploiement

Colonnes du rapport

- Statut
- Région
- Ressource
- Règle AWS Config
- Paramètres d'entrée
- Heure de la dernière modification

Les rapports d'intégrité améliorés AWS Elastic Beanstalk ne sont pas configurés

Description

Vérifie si des rapports d'intégrité améliorés sont configurés dans un environnement AWS Elastic Beanstalk.

Les rapports d'intégrité améliorés Elastic Beanstalk fournissent des indicateurs de performance détaillés, comme l'utilisation de l'UC, de la mémoire, le trafic réseau, et des informations sur l'intégrité de l'infrastructure, comme le nombre d'instances et l'état de l'équilibreur de charge.

Pour plus d'informations, voir Rapports d'intégrité améliorés et surveillance.

> **Note**
>
> Les résultats de cette vérification sont automatiquement actualisés plusieurs fois par jour et les demandes d'actualisation ne sont pas autorisées. Plusieurs heures peuvent encore être nécessaires pour que les modifications apparaissent. Actuellement, vous ne pouvez pas exclure des ressources de cette vérification.

ID de la vérification

`c18d2gz108`

Source

`AWS Config Managed Rule: beanstalk-enhanced-health-reporting-enabled`

Critères d'alerte

Jaune : les rapports d'intégrité améliorés ne sont pas configurés dans l'environnement Elastic Beanstalk.

Action recommandée

Vérifiez que des rapports d'intégrité améliorés sont configurés dans un environnement Elastic Beanstalk.

Pour plus d'informations, voir Activation des rapports d'intégrité améliorés à l'aide de la console Elastic Beanstalk.

Ressources supplémentaires

- Activation des rapports d'intégrité améliorés Elastic Beanstalk

- Rapports d'intégrité améliorés et surveillance

Colonnes du rapport

- Statut
- Région
- Ressource
- Règle AWS Config
- Paramètres d'entrée
- Heure de la dernière modification

AWS Elastic Beanstalk avec les mises à jour de plateforme gérées désactivées

Description

Vérifie si les mises à jour de plateforme gérées dans les environnements Elastic Beanstalk et les modèles de configuration sont activées.

AWS Elastic Beanstalk publie régulièrement des mises à jour de plateforme pour fournir des correctifs, des mises à jour logicielles et de nouvelles fonctionnalités. Grâce aux mises à jour de plateforme gérées, Elastic Beanstalk peut automatiquement mettre à jour la plateforme lorsque de nouvelles versions de correctifs ou de nouvelles versions mineures sont disponibles.

Vous pouvez spécifier le niveau de mise à jour souhaité dans les UpdateLevelparamètres de vos AWS Config règles.

Pour plus d'informations, voir Mise à jour de la version de la plateforme de votre environnement Elastic Beanstalk.

> **Note**
>
> Les résultats de cette vérification sont automatiquement actualisés plusieurs fois par jour et les demandes d'actualisation ne sont pas autorisées. Plusieurs heures peuvent encore être nécessaires pour que les modifications apparaissent. Actuellement, vous ne pouvez pas exclure des ressources de cette vérification.

ID de la vérification

`c18d2gz177`

Source

`AWS Config Managed Rule: elastic-beanstalk-managed-updates-enabled`

Critères d'alerte

Jaune : les mises à jour de plateforme gérées par AWS Elastic Beanstalk ne sont pas du tout configurées, qu'il s'agisse des mises à jour de version mineure ou de version corrective.

Action recommandée

Activez les mises à jour de plateforme gérées dans vos environnements Elastic Beanstalk ou configurez les mises à jour de version mineure ou de version corrective.

Pour plus d'informations, voir Mises à jour de plateforme gérées.

Ressources supplémentaires

- Activation des rapports d'intégrité améliorés Elastic Beanstalk
- Rapports d'intégrité améliorés et surveillance

Colonnes du rapport

- Statut
- Région
- Ressource
- Règle AWS Config
- Paramètres d'entrée
- Heure de la dernière modification

La version de plateforme AWS Fargate n'est pas la plus récente

Description

Vérifie si Amazon ECS exécute la dernière version de la plateforme AWS Fargate. Les versions de plateforme Fargate font référence à un environnement d'exécution spécifique pour l'infrastructure de tâche Fargate. Il s'agit d'une combinaison de la version du noyau et de la version d'exécution du conteneur. De nouvelles versions de plateforme sont publiées au fur et à mesure de l'évolution de l'environnement d'exécution, par exemple, si des mises à jour, de nouvelles fonctionnalités, des corrections de bugs ou des mises à jour de sécurité sont apportées au noyau ou au système d'exploitation.

Pour plus d'informations, voir Maintenance des tâches Fargate.

> **Note**
>
> Les résultats de cette vérification sont automatiquement actualisés plusieurs fois par jour et les demandes d'actualisation ne sont pas autorisées. Plusieurs heures peuvent encore être nécessaires pour que les modifications apparaissent. Actuellement, vous ne pouvez pas exclure des ressources de cette vérification.

ID de la vérification

`c18d2gz174`

Source

`AWS Config Managed Rule: ecs-fargate-latest-platform-version`

Critères d'alerte

Jaune : Amazon ECS ne s'exécute pas sur la dernière version de la plateforme Fargate.

Action recommandée

Effectuez une mise à jour vers la dernière version de la plateforme Fargate.

Pour plus d'informations, voir Maintenance des tâches Fargate.

Colonnes du rapport

- Statut
- Région
- Ressource
- Règle AWS Config
- Paramètres d'entrée
- Heure de la dernière modification

L'association du gestionnaire d'états AWS Systems Manager n'est pas conforme

Description

Vérifie si l'association AWS Systems Manager affiche l'état COMPLIANT ou NON_COMPLIANT après l'exécution de l'association sur l'instance.

Le gestionnaire d'états, une fonctionnalité de AWS Systems Manager, est un service de gestion de configuration sécurisé et évolutif qui automatise le processus de maintien de vos nœuds gérés et autres ressources AWS dans un état que vous définissez. Une association du gestionnaire d'états est une configuration que vous affectez à vos ressources AWS. La configuration définit l'état que vous souhaitez maintenir sur vos ressources, par exemple, afin d'éviter les incohérences de configuration entre vos instances Amazon EC2.

Pour plus d'informations, voir Gestionnaire d'états AWS Systems Manager.

> **Note**
>
> Les résultats de cette vérification sont automatiquement actualisés plusieurs fois par jour et les demandes d'actualisation ne sont pas autorisées. Plusieurs heures peuvent encore être nécessaires pour que les modifications apparaissent. Actuellement, vous ne pouvez pas exclure des ressources de cette vérification.

ID de la vérification

`c18d2gz147`

Source

`AWS Config Managed Rule: ec2-managedinstance-association-compliance-status-check`

Critères d'alerte

Jaune : l'association AWS Systems Manager affiche l'état de conformité NON_COMPLIANT.

Action recommandée

Validez l'état des associations du gestionnaire d'états et prenez les mesures nécessaires pour revenir à l'état COMPLIANT.

Pour plus d'informations, voir À propos du gestionnaire d'états.

Ressources supplémentaires

Gestionnaire d'états AWS Systems Manager

Colonnes du rapport

- Statut
- Région

- Ressource
- Règle AWS Config
- Paramètres d'entrée
- Heure de la dernière modification

CloudTrail les sentiers ne sont pas configurés avec Amazon CloudWatch Logs

Description

Vérifie si les AWS CloudTrail sentiers sont configurés pour envoyer des CloudWatch journaux à Logs.

Surveillez les fichiers CloudTrail CloudWatch journaux à l'aide des journaux pour déclencher une réponse automatique lorsque des événements critiques sont capturésAWS CloudTrail.

Pour plus d'informations, consultez la section Surveillance des fichiers CloudTrail journaux à l'aide de CloudWatch journaux.

> **Note**
>
> Les résultats de cette vérification sont automatiquement actualisés plusieurs fois par jour et les demandes d'actualisation ne sont pas autorisées. Plusieurs heures peuvent encore être nécessaires pour que les modifications apparaissent. Actuellement, vous ne pouvez pas exclure des ressources de cette vérification.

ID de la vérification

`c18d2gz164`

Source

`AWS Config Managed Rule: cloud-trail-cloud-watch-logs-enabled`

Critères d'alerte

Jaune : n'AWS CloudTrailest pas configuré avec l'intégration CloudWatch des journaux.

Action recommandée

Configurez les CloudTrail traces pour envoyer les événements du journal à CloudWatch Logs.

Pour plus d'informations, voir Création d' CloudWatch alarmes pour CloudTrail des événements : exemples.

Colonnes du rapport

- Statut
- Région
- Ressource
- Règle AWS Config
- Paramètres d'entrée
- Heure de la dernière modification

La protection contre la suppression d'Elastic Load Balancing n'est pas activée pour les équilibreurs de charge

Description

Vérifie si la protection contre les suppressions est activée pour vos équilibreurs de charge.

Elastic Load Balancing prend en charge la protection contre la suppression pour vos Application Load Balancers, Network Load Balancers et Gateway Load Balancers. Activez la protection contre la suppression pour protéger votre équilibreur de charge contre toute suppression accidentelle. La protection contre la suppression est désactivée par défaut lorsque vous créez un équilibreur de charge. Si vos équilibreurs de charge font partie d'un environnement de production, activez la protection contre la suppression.

Les journaux d'accès sont une fonctionnalité facultative d'Elastic Load Balancing qui est désactivée par défaut. Une fois que vous avez activé les journaux d'accès pour votre équilibreur de charge, Elastic Load Balancing capture les journaux et les stocke dans le compartiment Amazon S3 que vous spécifiez.

Pour plus d'informations, voir Protection des Application Load Balancers contre la suppression, Protection des Network Load Balancers contre la suppression ou Protection des Gateway Load Balancers contre la suppression.

> **Note**
>
> Les résultats de cette vérification sont automatiquement actualisés plusieurs fois par jour et les demandes d'actualisation ne sont pas autorisées. Plusieurs heures peuvent encore

être nécessaires pour que les modifications apparaissent. Actuellement, vous ne pouvez pas exclure des ressources de cette vérification.

ID de la vérification

`c18d2gz168`

Source

`AWS Config Managed Rule: elb-deletion-protection-enabled`

Critères d'alerte

Jaune : la protection contre la suppression n'est pas activée pour un équilibreur de charge.

Action recommandée

Activez la protection contre la suppression pour vos Application Load Balancers, Network Load Balancers et Gateway Load Balancers.

Pour plus d'informations, voir Protection des Application Load Balancers contre la suppression, Protection des Network Load Balancers contre la suppression ou Protection des Gateway Load Balancers contre la suppression.

Colonnes du rapport

- Statut
- Région
- Ressource
- Règle AWS Config
- Paramètres d'entrée
- Heure de la dernière modification

Vérification de la protection contre la suppression du cluster de base de données RDS

Description

Vérifie si la protection contre la suppression est activée pour vos clusters de base de données Amazon RDS.

Lorsque la protection contre la suppression est configurée pour un cluster, la base de données ne peut être supprimée par aucun utilisateur.

La protection contre la suppression est disponible pour les instances de base de données Amazon Aurora et RDS for MySQL, RDS for MariaDB, RDS for Oracle, RDS for PostgreSQL et RDS for SQL Server dans toutes les régions AWS.

Pour plus d'informations, voir Protection des clusters Aurora contre la suppression.

ID de la vérification

`c18d2gz160`

Source

`AWS Config Managed Rule: rds-cluster-deletion-protection-enabled`

Critères d'alerte

Jaune : la protection contre la suppression n'est pas activée pour certains de vos clusters de base de données Amazon RDS.

Action recommandée

Activez la protection contre la suppression lorsque vous créez un cluster de base de données Amazon RDS.

Vous pouvez uniquement supprimer les clusters pour lesquels la protection contre la suppression est désactivée. L'activation de la protection contre la suppression ajoute une couche de protection supplémentaire et évite les pertes de données dues à une suppression accidentelle ou non accidentelle d'une instance de base de données. La protection contre la suppression permet également de répondre aux exigences de conformité réglementaire et d'assurer la continuité des activités.

Pour plus d'informations, voir Protection des clusters Aurora contre la suppression.

> **Note**
>
> Les résultats de cette vérification sont automatiquement actualisés plusieurs fois par jour et les demandes d'actualisation ne sont pas autorisées. Plusieurs heures peuvent encore être nécessaires pour que les modifications apparaissent. Actuellement, vous ne pouvez pas exclure des ressources de cette vérification.

Ressources supplémentaires

Protection des clusters Aurora contre la suppression

Colonnes du rapport

- Statut
- Région
- Ressource
- Règle AWS Config
- Paramètres d'entrée
- Heure de la dernière modification

Vérification de la mise à niveau automatique de version mineure de l'instance de base de données RDS

Description

Vérifie si les mises à niveau automatiques de version mineure sont configurées pour les instances de base de données Amazon RDS.

Activez les mises à niveau automatiques de version mineure pour une instance Amazon RDS pour vous assurer que la base de données exécute toujours la dernière version sûre et stable. Les mises à niveau mineures fournissent des mises à jour de sécurité, des corrections de bogues, des améliorations des performances et garantissent la compatibilité avec les applications existantes.

Pour plus d'informations, voir Mise à niveau de la version d'un moteur d'instance de base de données.

> **Note**
>
> Les résultats de cette vérification sont automatiquement actualisés plusieurs fois par jour et les demandes d'actualisation ne sont pas autorisées. Plusieurs heures peuvent encore être nécessaires pour que les modifications apparaissent. Actuellement, vous ne pouvez pas exclure des ressources de cette vérification.

ID de la vérification

`c18d2gz155`

Source

`AWS Config Managed Rule: rds-automatic-minor-version-upgrade-enabled`

Critères d'alerte

Jaune : les mises à niveau automatiques de version mineure ne sont pas activées pour l'instance de base de données RDS.

Action recommandée

Activez les mises à niveau automatiques de version mineure lorsque vous créez une instance de base de données Amazon RDS.

Lorsque vous activez la mise à niveau de version mineure, la version de la base de données est automatiquement mise à niveau si elle exécute une version mineure du moteur de base de données antérieure à la version de mise à niveau manuelle du moteur.

Colonnes du rapport

- Statut
- Région
- Ressource
- Règle AWS Config
- Paramètres d'entrée
- Heure de la dernière modification

Journal des modifications pour AWS Trusted Advisor

Consultez la rubrique suivante pour connaître les modifications récentes apportées aux Trusted Advisor contrôles.

> **Note**
>
> Si vous utilisez la Trusted Advisor console ou l' AWS Support API, les vérifications supprimées n'apparaîtront pas dans les résultats des vérifications. Si vous utilisez l'un des contrôles supprimés, tels que la spécification de l'ID du contrôle dans une opération d' AWS Support API ou dans votre code, vous devez supprimer ces contrôles pour éviter les erreurs d'appel d'API.

Pour de plus amples informations sur les vérifications disponibles, consultez Référence de la vérification AWS Trusted Advisor.

Nouvelle vérification de tolérance aux pannes

Trusted Advisor a ajouté 1 contrôle de tolérance aux pannes le 29 février 2024 :

- NLB - Ressource connectée à Internet dans un sous-réseau privé

Pour plus d'informations, consultez le Référence de la vérification AWS Trusted Advisor.

Tolérance aux pannes et contrôles de sécurité mis à jour

Trusted Advisor a ajouté 1 nouveau contrôle de tolérance aux pannes et modifié 1 tolérance aux pannes existante et 1 contrôle de sécurité le 28 mars 2024 :

- Vérification des composants de AWS Resilience Hub l'application ajoutée
- Fonctions AWS Lambda compatibles VPC mises à jour sans redondance multi-AZ
- AWS Lambda Fonctions mises à jour à l'aide d'environnements d'exécution obsolètes

Pour plus d'informations, consultez le Référence de la vérification AWS Trusted Advisor.

Nouvelle vérification de tolérance aux pannes

Trusted Advisor a ajouté 1 contrôle de tolérance aux pannes le 31 janvier 2024 :

- AWS Direct Connect Résilience de localisation

Pour plus d'informations, consultez le Référence de la vérification AWS Trusted Advisor.

Contrôle de tolérance aux pannes mis à jour

Trusted Advisor a modifié 1 contrôle de tolérance aux pannes le 8 janvier 2024 :

- Le paramètre Amazon RDS innodb_flush_log_at_trx_commit n'est pas 1

Pour plus d'informations, consultez le Référence de la vérification AWS Trusted Advisor.

Contrôle de sécurité mis à jour

Trusted Advisor modifié 1 Contrôle de sécurité le 21 décembre 2023 :

- AWS Lambda Fonctions utilisant des environnements d'exécution obsolètes

Pour plus d’informations, consultez le Référence de la vérification AWS Trusted Advisor.

Nouveaux contrôles de sécurité et de performance

Trusted Advisor a ajouté 2 nouveaux contrôles de sécurité et 2 nouveaux contrôles de performance le 20 décembre 2023 :

- Les clients Amazon EFS n'utilisent pas data-in-transit le chiffrement
- Le cluster de base de données Amazon Aurora est sous-provisionné pour la charge de travail de lecture
- Instance Amazon RDS sous-provisionnée pour la capacité du système
- Fin de la prise en charge standard des instances Amazon EC2 avec Ubuntu LTS

Pour plus d’informations, consultez le Référence de la vérification AWS Trusted Advisor.

Nouveau contrôle de sécurité

Trusted Advisor a ajouté 1 nouveau contrôle de sécurité le 15 décembre 2023 :

- Amazon Route 53 : enregistrements CNAME non concordants pointant directement vers des compartiments S3

Pour plus d’informations, consultez le Référence de la vérification AWS Trusted Advisor.

Nouveaux contrôles de tolérance aux pannes et d'optimisation des coûts

Trusted Advisor a ajouté 2 nouveaux contrôles de tolérance aux pannes et 1 nouveau contrôle d'optimisation des coûts le 7 décembre 2023 :

- Clusters mono-AZ Amazon DocumentDB
- Configuration incomplète de l'interruption du téléchargement en plusieurs parties sur Amazon S3
- Pilote Amazon ECS AWS Logs en mode blocage

Pour plus d'informations, consultez le Référence de la vérification AWS Trusted Advisor.

Nouvelles vérifications de tolérance aux pannes

Trusted Advisor a ajouté 3 nouveaux contrôles de tolérance aux pannes le 17 novembre 2023 :

- ALB Multi-AZ
- NLB Multi-AZ
- Interface VPC : interfaces réseau de point de terminaison dans plusieurs zones de disponibilité

Pour plus d'informations, consultez le Référence de la vérification AWS Trusted Advisor.

Nouveaux chèques pour Amazon RDS

Trusted Advisor a ajouté 37 nouveaux chèques pour Amazon RDS le 15 novembre 2023.

Pour plus d'informations, consultez le Référence de la vérification AWS Trusted Advisor.

Nouvelle AWS Trusted Advisor API

AWS Trusted Advisor introduit de nouvelles API pour vous permettre d'accéder par programmation aux vérifications des meilleures pratiques, aux recommandations et aux recommandations hiérarchisées de Trusted Advisor. Trusted Advisor Les API vous permettent d'intégrer par programmation votre outil opérationnel préféré afin Trusted Advisor d'automatiser et d'optimiser vos charges de travail à grande échelle. Disponibles pour les clients Business, Enterprise On-Ramp ou Enterprise Support, les nouvelles API permettent d'accéder aux Trusted Advisor recommandations pour votre compte ou pour tous les comptes associés au sein d'un compte payeur. Les clients du support aux entreprises ayant accès à des comptes de gestion ou à des comptes d'administrateur délégué peuvent également récupérer des recommandations hiérarchisées par ordre de priorité au sein de leur organisation.

Les nouvelles Trusted Advisor API remplaceront les 3 fonctionnalités précédemment proposées par le biais de l'API AWS Support (SAPI). SAPI continuera à fournir des informations sur les dossiers et d'autres informations d'assistance.

Trusted Advisor Les API sont généralement disponibles dans les régions USA Est (Ohio), USA Est (Virginie du Nord), USA Ouest (Oregon), Asie-Pacifique (Séoul), Asie-Pacifique (Sydney) et Europe (Irlande).

Pour en savoir plus, rendez-vous sur la page de AWS Trusted Advisor l'API.

Trusted Advisor retrait de chèques

Trusted Advisor a supprimé les vérifications suivantes le 9 novembre 2023.

Nom de la vérification	Catégorie de la vérification	ID de la vérification
Les volumes EBS doivent être attachés aux instances EC2	Sécurité	`Hs4Ma3G119`
Le chiffrement côté serveur doit être activé dans les compartiments S3	Sécurité	`Hs4Ma3G167`
CloudFront l'identité d'accès à l'origine doit être activée pour les distributions	Sécurité	`Hs4Ma3G195`

Intégration des AWS Config chèques dans Trusted Advisor

Trusted Advisor a ajouté 64 nouveaux chèques effectués AWS Config le 30 octobre 2023.

Pour plus d'informations, consultez le Afficher les contrôles AWS Trusted Advisor optimisés par AWS Config.

Nouvelles vérifications de tolérance aux pannes

Trusted Advisor a ajouté les vérifications suivantes le 12 octobre 2023.

- Amazon RDS ReplicaLag
- Amazon RDS FreeStorageSpace
- Amazon RDS DiskQueueDepth
- Amazon Route 53 Resolver Redondance de la zone de disponibilité des terminaux
- Adresses IP disponibles dans les sous-réseaux pour l'autoscaling
- Les agents Amazon MSK hébergent un trop grand nombre de partitions

Pour plus d'informations, consultez la catégorie Tolérance aux pannes.

Nouvelle vérification des limites de service

Trusted Advisor a ajouté le contrôle suivant le 17 août 2023.

- Utilisation du stockage de code Lambda

Pour plus d'informations, consultez la catégorie Service Limits.

Nouvelle vérification de tolérance aux pannes

Trusted Advisor a ajouté le contrôle suivant le 3 août 2023.

- AWS Lambda Destinations des événements en cas de défaillance

Pour plus d'informations, consultez la catégorie Tolérance aux pannes.

Nouvelles vérifications de tolérance aux pannes et de performance

Trusted Advisor a ajouté les vérifications suivantes le 1er juin 2023.

- Redondance de cible sans montage Amazon EFS
- Optimisation du mode de débit Amazon EFS
- Redondance de zone de disponibilité pour ActiveMQ
- Redondance de zone de disponibilité pour RabbitMQ

Pour plus d'informations, voir les catégories Tolérance aux pannes et Performance.

Nouvelles vérifications de tolérance aux pannes

Trusted Advisor a ajouté les vérifications suivantes le 16 mai 2023.

- Indépendance de la zone de disponibilité des passerelles NAT
- Vérification des applications sur une seule zone de disponibilité

Pour plus d'informations, consultez la catégorie Tolérance aux pannes.

Nouvelles vérifications de tolérance aux pannes

Trusted Advisor a ajouté les vérifications suivantes le 27 avril 2023.

- Nombre de Régions AWS dans un ensemble de réplication Incident Manager
- AWS Resilience Hub âge d'évaluation

Pour plus d'informations, consultez la catégorie Tolérance aux pannes.

Extension régionale des vérifications de tolérance aux pannes pour Amazon ECS

Trusted Advisor a étendu les contrôles suivants à d'autres régions le 27 avril 2023. Trusted Advisor les chèques pour Amazon ECS sont désormais disponibles dans toutes les régions où Amazon ECS est généralement disponible.

- Service Amazon ECS utilisant une seule AZ
- Stratégie de placement multi-AZ pour Amazon ECS

Les régions ajoutées sont les suivantes : Afrique (Le Cap), Asie-Pacifique (Hong Kong), Asie-Pacifique (Hyderabad), Asie-Pacifique (Jakarta), Asie Pacifique (Melbourne), Europe (Milan), Europe (Espagne), Europe (Zurich), Moyen-Orient (Bahreïn) et Moyen-Orient (EAU).

Nouvelles vérifications de tolérance aux pannes

Trusted Advisor a ajouté les vérifications suivantes le 30 mars 2023.

- Service Amazon ECS utilisant une seule AZ
- Stratégie de placement Amazon ECS Multi-AZ

Pour plus d'informations, consultez la catégorie Tolérance aux pannes.

Nouvelles vérifications de tolérance aux pannes

Trusted Advisor a ajouté les vérifications suivantes le 15 décembre 2022.

- AWS CloudHSM clusters exécutant des instances HSM dans un seul AZ

- Clusters ElastiCache multi-AZ Amazon
- Clusters Amazon MemoryDB multi-AZ

Pour recevoir des résultats Trusted Advisor pour vos clusters AWS CloudHSM, ElastiCache, et MemoryDB, vous devez avoir des clusters dans vos zones de disponibilité. Pour plus d'informations, consultez la documentation de suivante :

- AWS CloudHSM Guide de l'utilisateur
- Guide du développeur Amazon MemoryDB for Redis (français non garanti)
- Guide de l'utilisateur ElastiCache d'Amazon pour Redis

Trusted Advisor a mis à jour les informations de vérification suivantes le 15 décembre 2022.

- AWS Resilience Hub politique violée — Le nom de l'application a été remplacé par le nom de l'application
- AWS Resilience Hub scores de résilience — Le nom de l'application et le score de résilience des applications ont été mis à jour en tant que nom de l'application et score de résilience des applications

Pour plus d'informations, consultez la catégorie Tolérance aux pannes.

Mises à jour de Trusted Advisor l'intégration avec AWS Security Hub

Trusted Advisor a effectué la mise à jour suivante le 17 novembre 2022.

Si vous désactivez Security Hub ou si vous AWS Config le souhaitez Région AWS, vous Trusted Advisor supprimez désormais vos résultats de contrôle dans un Région AWS délai de 7 à 9 jours. Auparavant, le délai de suppression de vos données Security Hub Trusted Advisor était de 90 jours.

Pour de plus amples informations, veuillez consulter les sections suivantes dans la rubrique Résolution des problèmes :

- J'ai désactivé Security Hub ou AWS Config dans une région
- Mon contrôle est archivé dans Security Hub, mais je vois toujours les résultats dans Trusted Advisor

Nouvelles vérifications de la tolérance aux pannes pour AWS Resilience Hub

Trusted Advisor a ajouté les vérifications suivantes le 17 novembre 2022.

- AWS Resilience Hub politique violée
- AWS Resilience Hub scores de résilience

Vous pouvez utiliser ces vérifications pour consulter le dernier état de la politique de résilience et le score de résilience de vos applications. Resilience Hub vous permet de définir, suivre et gérer la résilience et la disponibilité de vos applications de manière centralisée.

Pour obtenir des résultats Trusted Advisor pour vos applications Resilience Hub, vous devez déployer une AWS application et utiliser Resilience Hub pour suivre le niveau de résilience de l'application. Pour plus d'informations, consultez le Guide de l'utilisateur AWS Resilience Hub.

Pour recevoir des résultats Trusted Advisor pour vos clusters ElastiCache et MemoryDB, vous devez disposer de clusters dans vos zones de disponibilité. Pour plus d'informations, consultez la documentation de suivante :

- Guide du développeur Amazon MemoryDB for Redis (français non garanti)
- Guide de l'utilisateur ElastiCache d'Amazon pour Redis

Pour plus d'informations, consultez la catégorie Tolérance aux pannes.

Mise à jour de la Trusted Advisor console

Trusted Advisor a ajouté la modification suivante le 16 novembre 2022.

Le Trusted Advisor tableau de bord de la console s'intitule désormais Trusted Advisor Recommandations. La page Trusted Advisor Recommendations affiche toujours les résultats des vérifications et les vérifications disponibles pour chaque catégorie de votre Compte AWS.

Ce changement de nom met uniquement à jour la Trusted Advisor console. Vous pouvez continuer à utiliser la Trusted Advisor console et les Trusted Advisor opérations de l' AWS Support API comme d'habitude.

Pour plus d'informations, consultez Démarrer avec Trusted Advisor Recommendations.

Nouvelles vérifications pour Amazon EC2

Trusted Advisor a ajouté la vérification suivante le 1 septembre 2022.

- Instances Amazon EC2 avec fin de support de Microsoft Windows Server

Pour plus d'informations, consultez la catégorie Sécurité.

Ajout de vérifications Security Hub à Trusted Advisor

À compter du 23 juin 2022, Trusted Advisor ne prend en charge que les contrôles Security Hub disponibles jusqu'au 7 avril 2022. Cette version prend en charge tous les contrôles de la norme de sécurité AWS Foundational Security Best Practices, à l'exception des contrôles de la catégorie : Restaurer > Résilience. Pour plus d'informations, consultez Affichage des contrôles AWS Security Hub dans AWS Trusted Advisor.

Pour obtenir la liste des contrôles pris en charge, consultez les contrôles des Bonnes pratiques de sécurité de base de AWS dans le Guide de l'utilisateur de AWS Security Hub .

Chèques ajoutés de AWS Compute Optimizer

Trusted Advisor a ajouté les vérifications suivantes le 4 mai 2022.

Nom de la vérification	Catégorie de la vérification	ID de la vérification
Volumes Amazon EBS surprovisionnés	Optimisation des coûts	`COr6dfpM03`
Volumes Amazon EBS sous-provisionnés	Performance	`COr6dfpM04`
AWS Lambda fonctions surdimensionnées pour la taille de la mémoire	Optimisation des coûts	`COr6dfpM05`
AWS Lambda fonctions sous-provisionnées pour la taille de la mémoire	Performance	`COr6dfpM06`

Vous devez opter Compte AWS pour Compute Optimizer afin que ces contrôles puissent recevoir des données de vos ressources Lambda et Amazon EBS. Pour plus d'informations, consultez Inscription à AWS Compute Optimizer pour les vérifications de Trusted Advisor.

Mises à jour de la vérification des clés d'accès exposées

Trusted Advisor a mis à jour la vérification suivante le 25 avril 2022.

Nom de la vérification	Catégorie de la vérification	ID de la vérification
Exposed Access Keys	Sécurité	`12Fnkpl8Y5`

Trusted Advisor actualise désormais automatiquement cette vérification pour vous. Cette vérification ne peut pas être actualisée manuellement à partir de la Trusted Advisor console ou de l' AWS Support API. Si votre application ou votre code actualise cette vérification pour vous Compte AWS, nous vous recommandons de la mettre à jour pour ne plus l'actualiser. Dans le cas contraire, vous recevrez une erreur `InvalidParameterValue`.

Toutes les clés d'accès que vous avez exclues avant cette mise à jour ne seront plus exclues et apparaîtront en tant que ressources affectées. Vous ne pouvez pas exclure les clés d'accès des résultats de vos vérifications. Pour plus d'informations, consultez Exposed Access Keys.

> **Note**
>
> Si vous avez créé votre clé Compte AWS après le 25 avril 2022, les résultats de vérification pour les clés d'accès exposées affichent initialement l'icône grise ( ), même pour les clés d'accès non exposées. Cela signifie que Trusted Advisor n'a identifié aucune modification apportée à la vérification.
> S'il Trusted Advisor identifie une ressource à risque, le statut passe à l'icône de l'action recommandée ( ).
> Une fois que vous avez corrigé ou supprimé la ressource, le résultat de la vérification affiche l'icône de coche ( ).

Vérifications mises à jour pour AWS Direct Connect

Trusted Advisor a mis à jour les vérifications suivantes le 29 mars 2022.

Nom de la vérification	Catégorie de la vérification	ID de la vérification
AWS Direct Connect Redondance de connexion	Tolérance aux pannes	`0t121N1Ty3`
AWS Direct Connect Redondance des lieux	Tolérance aux pannes	`8M012Ph3U5`
AWS Direct Connect Redondance de l'interface virtuelle	Tolérance aux pannes	`4g3Nt5M1Th`

- La valeur de la colonne Region (Région) affiche désormais le code de la Région AWS au lieu du nom complet. Par exemple, les ressources de la région USA Est (Virginie du Nord) auront désormais la valeur `us-east-1`.
- La valeur de la colonne Time Stamp (Horodatage) apparaît désormais dans le format RFC 3339, comme `2022-03-30T01:02:27.000Z`.
- Les ressources qui ne présentent aucun problème détecté apparaissent désormais dans le tableau à cocher. Ces ressources comportent une icône de coche ( ) à côté d'elles.

  Auparavant, seules les ressources qui vous Trusted Advisor recommandaient d'effectuer des recherches apparaissaient dans le tableau. Ces ressources comportent une icône d'avertissement ( ) à côté d'elles.

AWS Security Hub commandes ajoutées à la AWS Trusted Advisor console

AWS Trusted Advisor a ajouté 111 contrôles Security Hub à la catégorie Sécurité le 18 janvier 2022.

Vous pouvez consulter les résultats relatifs aux contrôles du Security Hub à partir de la norme de sécurité AWS Foundational Security Best Practices. Cette intégration n'inclut pas les contrôles dotés de Category: Recover > Resilience (Catégorie : Récupérer > Résilience).

Pour en savoir plus sur cette fonction, consultez Affichage des contrôles AWS Security Hub dans AWS Trusted Advisor.

Nouvelles vérifications pour Amazon EC2 et Well-Architected AWS

Trusted Advisor a ajouté les vérifications suivantes le 20 décembre 2021.

- Consolidation des instances Amazon EC2 pour Microsoft SQL Server
- Instances Amazon EC2 trop approvisionnées pour Microsoft SQL Server
- Instances Amazon EC2 avec fin de support de Microsoft SQL Server
- AWS Well-ArchitectedProblèmes à risque élevé pour l'optimisation des coûts
- Problèmes à risque élevé AWS Well-Architected pour la performance
- Problèmes à risque élevé AWS Well-Architected pour la sécurité
- Problèmes à risque élevé AWS Well-Architected pour la fiabilité

Pour plus d'informations, consultez la Référence des vérifications de AWS Trusted Advisor.

Nom du chèque mis à jour pour Amazon OpenSearch Service

Trusted Advisor a mis à jour le nom du Amazon OpenSearch Service Reserved Instance Optimization chèque le 8 septembre 2021.

Les recommandations de vérification, la catégorie et l'ID sont les mêmes.

Nom de la vérification	Catégorie de la vérification	ID de la vérification
Optimisation des instances réservées Amazon OpenSearch Service	Optimisation des coûts	`7ujm6yhn5t`

> **Note**
>
> Si vous utilisez Trusted Advisor pour les CloudWatch métriques Amazon, le nom de la métrique pour cette vérification est également mis à jour. Pour plus d'informations, consultez Création d'alarmes Amazon CloudWatch pour contrôler les métriques AWS Trusted Advisor.

Vérifications ajoutées pour le stockage des volumes Amazon Elastic Block Store

Trusted Advisor a ajouté les vérifications suivantes le 8 juin 2021.

Nom de la vérification	Catégorie de la vérification	ID de la vérification
Stockage en volume SSD polyvalent EBS (gp3)	Service Limits	`dH7RR0l6J3`
Stockage en volume SSD d'IOPS provisionnés EBS (io2)	Service Limits	`gI7MM0l7J2`

Contrôles ajoutés pour AWS Lambda

Trusted Advisor a ajouté les vérifications suivantes le 8 mars 2021.

Nom de la vérification	Catégorie de la vérification	ID de la vérification
AWS Lambda Fonctions présentant des délais d'attente excessifs	Optimisation des coûts	`L4dfs2Q3C3`
AWS Lambda Fonctions présentant un taux d'erreur élevé	Optimisation des coûts	`L4dfs2Q3C2`
AWS Lambda Fonctions utilisant des environnements d'exécution obsolètes	Sécurité	`L4dfs2Q4C5`

Nom de la vérification	Catégorie de la vérification	ID de la vérification
AWS Lambda Fonctions compatibles VPC sans redondance multi-AZ	Tolérance aux pannes	`L4dfs2Q4C6`

Pour plus d'informations sur l'utilisation de ces vérifications avec Lambda, consultez Exemple de AWS Trusted Advisor flux de travail pour consulter les recommandations du Guide du AWS Lambda développeur.

Trusted Advisor retrait de chèques

Trusted Advisor a retiré le chèque suivant pour AWS GovCloud (US) Region le 8 mars 2021.

Nom de la vérification	Catégorie de la vérification	ID de la vérification
Adresses IP Elastic EC2	Service Limits	`aW9HH0l8J6`

Mise à jour de vérifications pour Amazon Elastic Block Store

Trusted Advisor a mis à jour l'unité du volume Amazon EBS de gibioctet (GiB) à tebioctet (TiB) pour les vérifications suivantes le 5 mars 2021.

> **Note**
>
> Si vous utilisez Trusted Advisor des CloudWatch métriques pour Amazon, les noms des métriques pour ces cinq vérifications sont également mis à jour. Pour plus d'informations, consultez Création d'alarmes Amazon CloudWatch pour contrôler les métriques AWS Trusted Advisor.

Nom de la vérification	Catégorie de la vérification	ID de la vérification	CloudWatch Métrique mise à jour pour ServiceLimit
Stockage en volume HDD EBS à froid (sc1)	Service Limits	`gH5CC0e3J9`	Stockage en volume HDD à froid (Tio) (sc1)
Stockage en volume SSD polyvalent EBS (gp2)	Service Limits	`dH7RR0l6J9`	Stockage de volume SSD polyvalent (gp2) (Tio)
Stockage en volume (standard) magnétiqu e EBS	Service Limits	`cG7HH0l7J9`	Stockage de volume (standard) magnétiqu e (Tio)
Stockage en volume SSD d'IOPS provision nés EBS (io1)	Service Limits	`gI7MM0l7J9`	Stockage (SSD) d'IOPS provisionnés (Tio)
Stockage de volume HDD optimisé pour le débit EBS (st1)	Service Limits	`wH7DD0l3J9`	Stockage de volumes HDD optimisé pour le débit (st1) (Tio)

Trusted Advisor retrait de chèques

> **Note**
>
> Trusted Advisor a supprimé les vérifications suivantes le 18 novembre 2020.

Contrôles supprimés le 18 novembre 2020	Catégorie de la vérification	ID de la vérification
Service EC2Config pour les instances Windows EC2	Tolérance aux pannes	`V77i0LlBqz`

Contrôles supprimés le 18 novembre 2020	Catégorie de la vérification	ID de la vérification
Version du pilote ENA pour les instances Windows EC2	Tolérance aux pannes	TyfdMXG69d
Version du pilote NVMe pour les instances Windows EC2	Tolérance aux pannes	yHAGQJV9K5
Version du pilote PV pour les instances Windows EC2	Tolérance aux pannes	Wnwm9Il5bG
Volumes actifs EBS	Service Limits	fH7LL0l7J9

Amazon Elastic Block Store n'est plus limité en ce qui concerne le nombre de volumes que vous pouvez allouer.

Vous pouvez surveiller vos instances Amazon EC2 et vérifier qu'elles sont à jour en utilisant AWS Systems Manager Distributor, d'autres outils tiers, ou écrivez vos propres scripts pour renvoyer des informations de pilote pour Windows Management Instrumentation (WMI).

Trusted Advisor retrait de chèques

Trusted Advisor a retiré le contrôle suivant le 18 février 2020.

Nom de la vérification	Catégorie de la vérification	ID de la vérification
Service Limits	Performance	eW7HH0l7J9

Application AWS Support dans Slack

Vous pouvez utiliser l'application AWS Support pour gérer vos cas de support AWS dans Slack. Vous pouvez inviter les membres de votre équipe à des canaux de discussion, répondre aux mises à jour des cas et discuter directement avec les agents de support. L'application AWS Support vous aide à gérer les cas de support rapidement et directement dans Slack.

Par exemple, vous pouvez utiliser l'application AWS Support pour que exécute les opérations suivantes :

- Créer, mettre à jour, rechercher et résoudre des cas de support dans les canaux Slack
- Joindre des fichiers aux cas de support
- Demander des augmentations de quotas à partir de Service Quotas
- Partager les détails d'un cas de support avec votre équipe sans quitter le canal Slack
- Démarrer une session de chat en direct avec des agents de support

Lorsque vous créez, mettez à jour ou résolvez un dossier de support dans l'application AWS Support, le dossier est également mis à jour dans l'application AWS Support Center Console. Vous n'avez pas besoin de vous connecter à la console du centre de support pour gérer vos cas de support séparément.

> **Remarques**
>
> - Les temps de réponse pour les cas de support sont les mêmes, que vous ayez créé le cas depuis Slack ou depuis la console du centre de support.
> - Vous pouvez créer un cas de support pour le support de compte et de facturation, l'augmentation des quotas de service et le support technique.

Rubriques

- Réponse aux cas de support dans Slack
- Rejoindre une session de chat en direct avec AWS Support
- Recherche de cas de support dans Slack
- Résolution d'un cas de support dans Slack
- Réouverture d'un cas de support dans Slack
- Demande d'augmentations de quota de service
- Suppression d'une configuration de canal Slack à partir de l'application AWS Support
- Suppression d'une configuration d'espace de travail Slack à partir de l'application AWS Support
- Application AWS Support dans les commandes Slack
- Afficher les correspondances de l'application AWS Support dans la AWS Support Center Console
- Création d'une application AWS Support dans les ressources Slack avec AWS CloudFormation

Prérequis

Vous devez remplir les conditions suivantes pour utiliser l'application AWS Support dans Slack :

- Vous devez avoir un plan de support Business, Enterprise On-Ramp ou Enterprise. Vous pouvez trouver votre plan de support à partir de la AWS Support Center Console ou de la page Support plans (Plans de support). Pour plus d'informations, consultez Comparer les plans de AWS Support.
- Vous avez un espace de travail et un canal Slack pour votre organisation. Vous devez être un administrateur de l'espace de travail Slack ou avoir l'autorisation d'ajouter des applications à cet espace de travail Slack. Pour plus d'informations, consultez le Centre d'aide de Slack (français non garanti).
- Vous vous connectez au Compte AWS en tant qu'utilisateur ou rôle AWS Identity and Access Management (IAM) avec les autorisations requises. Pour de plus amples informations, veuillez consulter Gestion de l'accès au widget de l'application AWS Support.
- Vous devez créer un rôle IAM qui dispose des autorisations requises pour effectuer des actions à votre place. L'application AWS Support utilise ce rôle pour effectuer des appels d'API auprès de différents services. Pour de plus amples informations, veuillez consulter Gestion de l'accès à l'application AWS Support.

Rubriques

- Gestion de l'accès au widget de l'application AWS Support

- Gestion de l'accès à l'application AWS Support

Gestion de l'accès au widget de l'application AWS Support

Vous pouvez associer une politique AWS Identity and Access Management (IAM) pour accorder à un utilisateur IAM l'autorisation de configurer le widget de l'application AWS Support dans la AWS Support Center Console.

Pour plus d'informations sur l'ajout d'une politique à une entité IAM, consultez Ajout d'autorisations d'identité IAM (console) dans le Guide de l'utilisateur IAM.

> **Note**
>
> Vous pouvez également vous connecter en tant qu'utilisateur root dans votre Compte AWS, mais nous ne vous le recommandons pas. Pour plus d'informations sur l'accès de l'utilisateur root, consultez Safeguard your root user credentials and don't use them for everyday tasks in the IAM User Guide (Protection des informations d'identification de l'utilisateur root et ne pas les utiliser pour des tâches quotidiennes) dans le Guide de l'utilisateur IAM.

Exemple de politique IAM

Vous pouvez associer la politique suivante à une entité, telle qu'un utilisateur ou un groupe IAM. Cette politique permet à un utilisateur d'autoriser un espace de travail Slack et de configurer des canaux Slack dans la console du centre de support.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "supportapp:GetSlackOauthParameters",
                "supportapp:RedeemSlackOauthCode",
                "supportapp:DescribeSlackChannels",
                "supportapp:ListSlackWorkspaceConfigurations",
                "supportapp:ListSlackChannelConfigurations",
                "supportapp:CreateSlackChannelConfiguration",
                "supportapp:DeleteSlackChannelConfiguration",
                "supportapp:DeleteSlackWorkspaceConfiguration",
```

```
                "supportapp:GetAccountAlias",
                "supportapp:PutAccountAlias",
                "supportapp:DeleteAccountAlias",
                "supportapp:UpdateSlackChannelConfiguration",
                "iam:ListRoles"
            ],
            "Resource": "*"
        }
    ]
}
```

Autorisations requises pour connecter l'application AWS Support à Slack

L'application AWS Support inclut des actions avec autorisations uniquement qui ne correspondent pas directement à une opération d'API. Ces actions sont indiquées dans la référence d'autorisation de service avec [permission only].

L'application AWS Support utilise les actions d'API suivantes pour se connecter à Slack, puis répertorie vos chaînes Slack publiques dans l' AWS Support Center Console :

- `supportapp:GetSlackOauthParameters`
- `supportapp:RedeemSlackOauthCode`
- `supportapp:DescribeSlackChannels`

Ces actions d'API ne sont pas conçues pour être appelées par votre code. Elles ne sont donc pas incluses dans l'interface AWS CLI et les kits SDK AWS.

Gestion de l'accès à l'application AWS Support

Après avoir obtenu les autorisations pour le widget de l'application AWS Support, vous devez également créer un rôle AWS Identity and Access Management (IAM). Ce rôle exécute des actions d'autres Services AWS pour vous, comme l'API AWS Support et Service Quotas.

Vous associez ensuite une politique IAM à ce rôle afin qu'il dispose des autorisations nécessaires pour effectuer ces actions. Vous choisissez ce rôle lorsque vous créez la configuration de votre canal Slack dans la console du centre de support.

Les utilisateurs de votre canal Slack ont les mêmes autorisations que celles que vous accordez au rôle IAM. Par exemple, si vous spécifiez un accès en lecture seule à vos cas de support, les

utilisateurs de votre canal Slack peuvent voir vos cas de support, mais ne peuvent pas les mettre à jour.

> **Important**
>
> Lorsque vous demandez un chat en direct avec un agent de support et que vous choisissez un nouveau canal privé comme canal de chat en direct préféré, l'application AWS Support crée un canal Slack distinct. Ce canal Slack a les mêmes autorisations que le canal où vous avez créé le cas ou initié le chat.
> Si vous modifiez le rôle IAM ou la politique IAM, vos modifications s'appliquent au canal Slack que vous avez configuré et à tout nouveau canal Slack de chat en direct que l'application AWS Support crée pour vous.

Suivez ces procédures pour créer votre rôle et votre politique IAM.

Rubriques

- Utiliser une politique gérée par AWS ou créer une politique gérée par le client
- Créer un rôle IAM
- Résolution des problèmes

Utiliser une politique gérée par AWS ou créer une politique gérée par le client

Pour accorder des autorisations à votre rôle, vous pouvez utiliser une politique gérée par AWS ou une politique gérée par le client.

> **Tip**
>
> Si vous ne voulez pas créer une politique manuellement, nous vous conseillons d'utiliser une politique gérée par AWS à la place et d'ignorer cette procédure. Les politiques gérées disposent automatiquement des autorisations requises pour l'application AWS Support. Vous n'avez pas besoin de mettre à jour les politiques manuellement. Pour de plus amples informations, veuillez consulter AWS politiques gérées pour les AWS Support applications dans Slack.

Suivez cette procédure pour créer une politique gérée par le client pour votre rôle. Cette procédure utilise l'éditeur de politique JSON dans la console IAM.

Pour créer une politique gérée par le client pour l'application AWS Support

1. Connectez-vous à la AWS Management Console et ouvrez la console IAM à l'adresse https://console.aws.amazon.com/iam/.
2. Dans le panneau de navigation, choisissez Policies (Politiques).
3. Sélectionnez Créer une politique.
4. Choisissez l'onglet JSON.
5. Saisissez votre JSON, puis remplacez le JSON par défaut dans l'éditeur. Vous pouvez utiliser l'exemple de politique.
6. Choisissez Next: Tags (Suivant : Balises).
7. (Facultatif) Vous pouvez utiliser des balises comme paires clé-valeur pour ajouter des métadonnées à la politique.
8. Choisissez Next: Review (Suivant : Vérification).
9. Dans la page Review policy (Vérifier la politique), saisissez un Name (Nom), tel que *AWSSupportAppRolePolicy*, et une Description (facultatif).
10. Examinez la page Summary (Résumé) pour voir les autorisations que la politique autorise, puis cliquez sur Create policy (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.

Exemple de politique IAM

Vous pouvez associer l'exemple de politique suivant à votre rôle IAM. Cette politique permet au rôle d'avoir des autorisations complètes pour toutes les actions requises pour l'application AWS Support. Après avoir configuré un canal Slack avec le rôle, tout utilisateur dans votre canal a les mêmes autorisations.

> **Note**
>
> Pour une liste des politiques gérées par AWS, consultez AWS politiques gérées pour les AWS Support applications dans Slack.

Vous pouvez mettre à jour la politique pour supprimer une autorisation de l'application AWS Support.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "servicequotas:GetRequestedServiceQuotaChange",
                "servicequotas:GetServiceQuota",
                "servicequotas:RequestServiceQuotaIncrease",
                "support:AddAttachmentsToSet",
                "support:AddCommunicationToCase",
                "support:CreateCase",
                "support:DescribeCases",
                "support:DescribeCommunications",
                "support:DescribeSeverityLevels",
                "support:InitiateChatForCase",
                "support:ResolveCase"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": "iam:CreateServiceLinkedRole",
            "Resource": "*",
            "Condition": {
                "StringEquals": {"iam:AWSServiceName": "servicequotas.amazonaws.com"}
            }
        }
    ]
}
```

Pour obtenir des descriptions de chaque action, consultez les rubriques suivantes dans la référence de l'autorisation de service :

- Actions, ressources et clés de condition pour AWS Support
- Actions, ressources et clés de condition pour Service Quotas
- Actions, ressources et clés de condition pour AWS Identity and Access Management

Créer un rôle IAM

Après avoir créé la politique, vous devez créer un rôle IAM, puis associer la politique à ce rôle. Vous choisissez ce rôle lorsque vous créez une configuration de canal Slack dans la console du centre de support.

Pour créer un rôle pour l'application AWS Support

1. Connectez-vous à l'outil AWS Management Console, puis ouvrez la console IAM à l'adresse https://console.aws.amazon.com/iam/.
2. Dans le volet de navigation, sélectionnez Rôles, puis Créer un rôle.
3. Pour Select trusted entity (Sélectionner une entité de confiance), choisissez Service AWS.
4. Choisissez Application AWS Support.
5. Sélectionnez Next: Permissions (Étape suivante : autorisations).
6. Saisissez le nom de la politique. Vous pouvez choisir la politique gérée par AWS ou sélectionner une politique gérée par le client que vous avez créée, telle que *AWSSupportAppRolePolicy*. Ensuite, cochez la case à côté de la politique.
7. Choisissez Next: Tags (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 Role name (Nom du rôle), saisissez un nom, tel que *AWSSupportAppRole*.
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. Vous pouvez maintenant choisir ce rôle lorsque vous configurez un canal Slack dans la console du centre de support. Consultez Configuration d'un canal Slack.

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

Résolution des problèmes

Consultez les rubriques suivantes pour gérer l'accès à l'application AWS Support.

Table des matières

- Je veux interdire des actions spécifiques à certains utilisateurs de mon canal Slack
- Lorsque je configure un canal Slack, je ne vois pas le rôle IAM que j'ai créé
- Il manque une autorisation à mon rôle IAM
- Une erreur Slack indique que mon rôle IAM n'est pas valide
- L'application AWS Support indique qu'il me manque un rôle IAM pour Service Quotas

Je veux interdire des actions spécifiques à certains utilisateurs de mon canal Slack

Par défaut, les utilisateurs de votre canal Slack ont les mêmes autorisations que celles spécifiées dans la politique IAM que vous associez au rôle IAM que vous créez. Cela signifie que toute personne dans le canal a un accès en lecture ou en écriture à vos cas de support, qu'elle ait ou non un Compte AWS ou un utilisateur IAM.

Nous recommandons les bonnes pratiques suivantes :

- Configurez des canaux Slack privés avec l'application AWS Support
- N'invitez à votre canal que les utilisateurs qui ont besoin d'accéder à vos cas de support
- Utilisez une politique IAM qui dispose des autorisations minimales requises pour l'application AWS Support. Consultez AWS politiques gérées pour les AWS Support applications dans Slack.

Lorsque je configure un canal Slack, je ne vois pas le rôle IAM que j'ai créé

Si votre rôle IAM n'apparaît pas dans la liste des rôles IAM pour l'application AWS Support, cela signifie que le rôle n'a pas l'application AWS Support comme entité de confiance, ou que le rôle a été supprimé. Vous pouvez mettre à jour le rôle existant ou en créer un autre. Consultez Créer un rôle IAM.

Il manque une autorisation à mon rôle IAM

Le rôle IAM que vous créez pour votre canal Slack a besoin d'autorisations pour effectuer les actions que vous voulez. Par exemple, si vous voulez que vos utilisateurs dans Slack créent des cas de support, le rôle doit avoir l'autorisation `support:CreateCase`. L'application AWS Support assume ce rôle pour exécuter ces actions à votre place.

Si vous recevez une erreur concernant une autorisation manquante de la part de l'application AWS Support, vérifiez que la politique associée à votre rôle possède l'autorisation requise.

Voir le Exemple de politique IAM précédent.

Une erreur Slack indique que mon rôle IAM n'est pas valide

Vérifiez que vous avez choisi le rôle correct pour votre configuration de canal.

Pour vérifier votre rôle

1. Connectez-vous à la AWS Support Center Console sur la page https://console.aws.amazon.com/support/app#/config.
2. Choisissez le canal que vous avez configuré avec l'application AWS Support.
3. Dans la section Permissions (Autorisations), trouvez le nom du rôle IAM que vous avez choisi.
   - Pour modifier le rôle, sélectionnez Edit (Modifier), choisissez un autre rôle, puis sélectionnez Save (Enregistrer).
   - Pour mettre à jour le rôle ou la politique associée au rôle, connectez-vous à la console IAM.

L'application AWS Support indique qu'il me manque un rôle IAM pour Service Quotas

Vous devez avoir le rôle `AWSServiceRoleForServiceQuotas` dans votre compte pour demander des augmentations de quota à Service Quotas. Si vous recevez une erreur concernant une ressource manquante, effectuez l'une des étapes suivantes :

- Utilisez la console Service Quotas pour demander une augmentation de quota. Après avoir effectué une demande réussie, Service Quotas crée automatiquement ce rôle pour vous. Ensuite, vous pouvez utiliser l'application AWS Support pour demander des augmentations de quotas dans Slack. Pour plus d'informations, consultez Demande d'augmentation de quota.
- Mettez à jour la politique IAM associée à votre rôle. Ceci accorde au rôle l'autorisation pour Service Quotas. La section suivante dans le Exemple de politique IAM permet à l'application AWS Support de créer le rôle Service Quotas pour vous.

```
{
    "Effect": "Allow",
    "Action": "iam:CreateServiceLinkedRole",
    "Resource": "*",
    "Condition": {
        "StringEquals": {"iam:AWSServiceName": "servicequotas.amazonaws.com"}
     }
}
```

Si vous supprimez le rôle IAM que vous configurez pour votre canal, vous devez créer manuellement le rôle ou mettre à jour la politique IAM pour permettre à l'application AWS Support d'en créer un pour vous.

Autorisation d'un espace de travail Slack

Après avoir autorisé votre espace de travail et donné à l'application AWS Support l'autorisation d'y accéder, vous avez besoin d'un rôle AWS Identity and Access Management (IAM) pour votre Compte AWS. L'application AWS Support utilise ce rôle pour appeler les opérations d'API depuis AWS Support et Service Quotas pour vous. Par exemple, l'application AWS Support utilise ce rôle pour appeler l'opération `CreateCase` afin de créer un cas de support pour vous dans Slack.

Remarques

- Le canal Slack hérite des autorisations du rôle IAM. Cela signifie que tout utilisateur dans le canal Slack a les mêmes autorisations que celles spécifiées dans la politique IAM qui est attachée au rôle.

  Par exemple, si votre politique IAM autorise le rôle à avoir des autorisations complètes de lecture et d'écriture pour vos cas de support, toute personne dans votre canal Slack peut créer, mettre à jour et résoudre vos cas de support. Si votre politique IAM autorise le rôle à avoir des autorisations en lecture seule, les utilisateurs de votre canal Slack n'ont que des autorisations de lecture pour vos cas de support.
- Nous vous recommandons d'ajouter les espaces de travail et les canaux Slack dont vous avez besoin pour gérer vos opérations de support. Nous vous recommandons de configurer des canaux privés et d'inviter uniquement les utilisateurs requis.

Vous devez autoriser chaque espace de travail Slack que vous voulez utiliser pour votre Compte AWS. Si vous avez plusieurs Comptes AWS, vous devez vous connecter à chaque compte et répéter la procédure suivante pour autoriser l'espace de travail. Si votre compte appartient à une organisation dans AWS Organizations et que vous voulez autoriser plusieurs comptes, passez à Autorisation de plusieurs comptes.

Pour autoriser l'espace de travail Slack pour votre Compte AWS

1. Connectez-vous à la AWS Support Center Console et sélectionnez Slack configuration (Configuration de Slack).

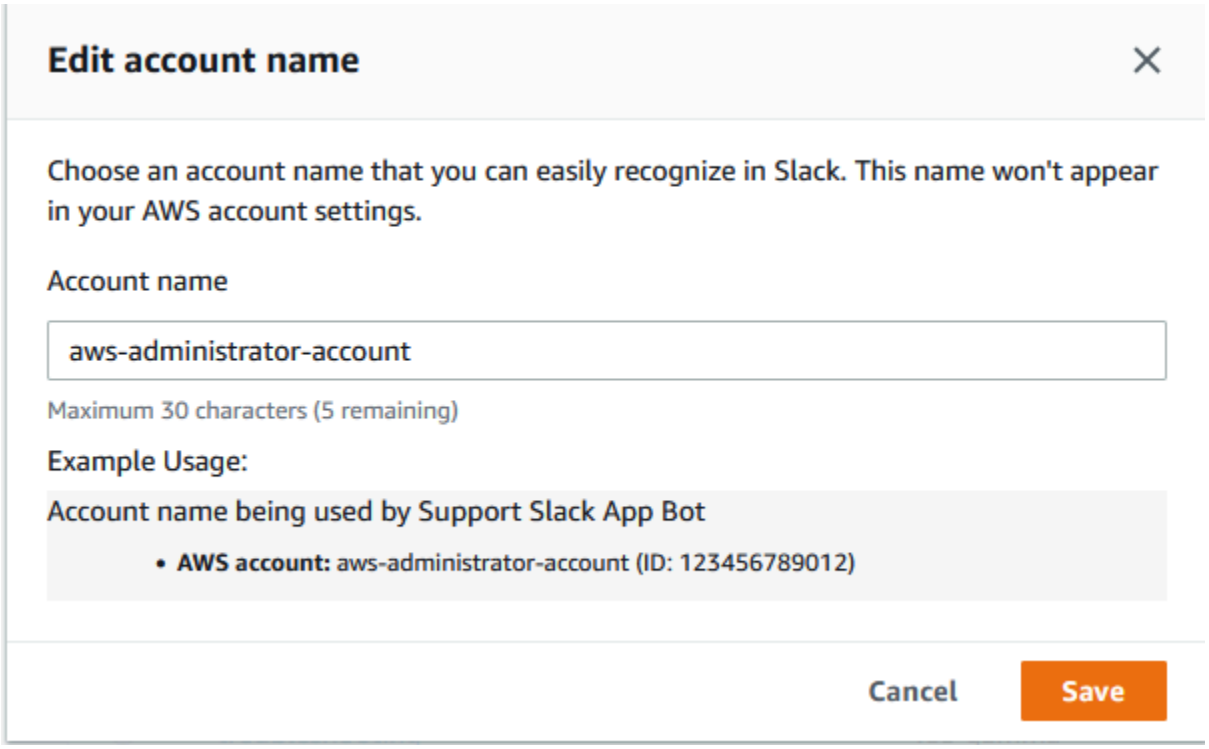
2. Sur la page Getting started (Mise en route), sélectionnez Authorize workspace (Autoriser l'espace de travail).
3. Si vous n'êtes pas déjà connecté à Slack, sur la page Sign in to your workspace (Connexion à votre espace de travail), saisissez le nom de votre espace de travail, puis sélectionnez Continue (Continuer).
4. Sur la page AWS Support is requesting permission to access the your-workspace-name Slack (demande l'autorisation d'accéder à your-workspace-name Slack), sélectionnez Allow (Autoriser).

> **Note**
>
> Si vous ne pouvez pas autoriser Slack à accéder à votre espace de travail, assurez-vous que vous avez les autorisations de votre administrateur Slack pour ajouter l'application AWS Support à l'espace de travail. Consultez Prérequis.

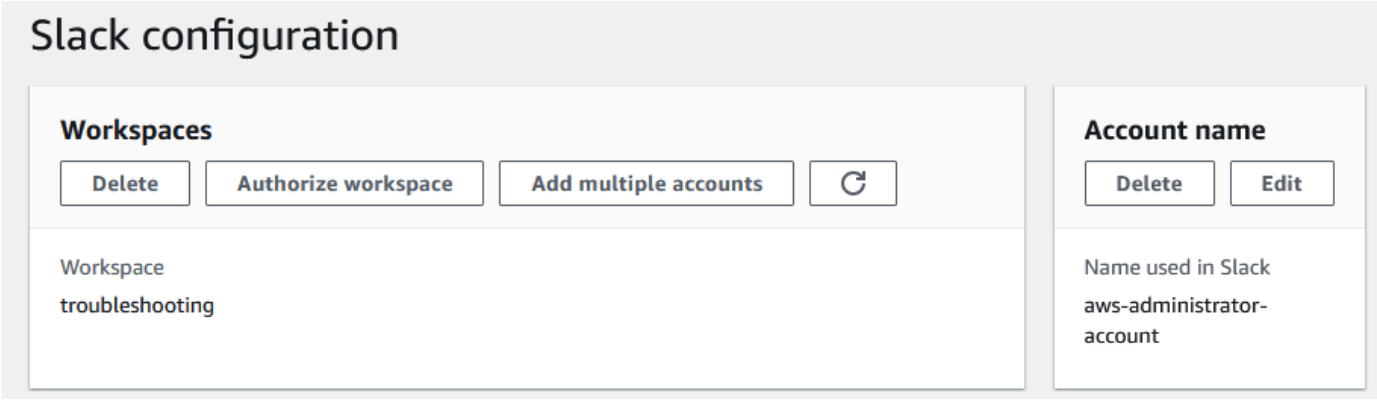
Sur la page Slack configuration (Configuration de Slack), le nom de votre espace de travail apparaît sous Workspaces (Espaces de travail).

5. (Facultatif) Pour ajouter d'autres espaces de travail, sélectionnez Authorize workspace (Autoriser l'espace de travail) et répétez les étapes 3 et 4. Vous pouvez ajouter jusqu'à cinq espaces de travail à votre compte.
6. (Facultatif) Par défaut, le numéro d'identification de votre Compte AWS apparaît comme nom de compte dans votre canal Slack. Pour modifier cette valeur, sous Account name (Nom de compte), sélectionnez Edit (Modifier), saisissez le nom de votre compte, puis sélectionnez Save (Enregistrer).

> **Tip**
>
> Utilisez un nom que vous et votre équipe pouvez facilement reconnaître. L'application AWS Support utilise ce nom pour identifier votre compte dans le canal Slack. Vous pouvez mettre à jour ce nom à tout moment.



Votre espace de travail et votre nom de compte apparaissent sur la page Slack configuration (Configuration de Slack).



Autorisation de plusieurs comptes

Pour autoriser plusieurs Comptes AWS à utiliser les espaces de travail Slack, vous pouvez utiliser AWS CloudFormation ou Terraform pour créer vos ressources de l'application AWS Support.

Configuration d'un canal Slack

Après avoir autorisé votre espace de travail Slack, vous pouvez configurer vos canaux Slack pour utiliser l'application AWS Support.

Le canal dans lequel vous invitez et ajoutez l'application AWS Support est celui dans lequel vous pouvez créer et rechercher des cas, et recevoir des notifications de cas. Ce canal affiche les mises à jour des cas, comme les cas nouvellement créés ou résolus, les correspondances ajoutées et les détails des cas partagés.

Le canal Slack hérite des autorisations du rôle IAM. Cela signifie que tout utilisateur dans le canal Slack a les mêmes autorisations que celles spécifiées dans la politique IAM qui est attachée au rôle.

Par exemple, si votre politique IAM autorise le rôle à avoir des autorisations complètes de lecture et d'écriture pour vos cas de support, toute personne dans votre canal Slack peut créer, mettre à jour et résoudre vos cas de support. Si votre politique IAM autorise le rôle à avoir des autorisations en lecture seule, les utilisateurs de votre canal Slack n'ont que des autorisations de lecture pour vos cas de support.

Vous pouvez ajouter jusqu'à 20 canaux pour un compte. Un canal Slack peut avoir jusqu'à 100 Comptes AWS. Cela signifie que seuls 100 comptes peuvent ajouter le même canal Slack à l'application AWS Support. Nous vous recommandons d'ajouter uniquement les comptes dont vous avez besoin pour gérer les cas de support de votre organisation. Cela peut réduire le nombre de notifications que vous recevez dans le canal afin que vous et votre équipe ayez moins de distractions.

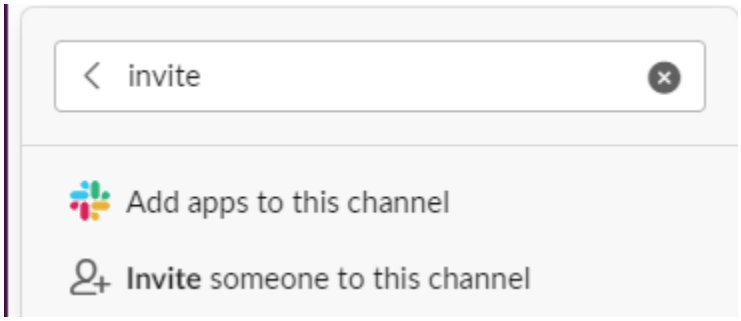
Chaque Compte AWS doit configurer un canal Slack séparément dans l'application AWS Support. De cette façon, l'application AWS Support peut accéder aux cas de support dans ce Compte AWS. Si un autre Compte AWS de votre organisation a déjà invité l'application AWS Support à ce canal Slack, passez à l'étape 3.

> **Note**
>
> Vous pouvez configurer des canaux faisant partie de Slack Connect et des canaux partagées avec plusieurs espaces de travail. Toutefois, seul le premier espace de travail qui a configuré le canal partagé pour un Compte AWS peut utiliser l'application AWS Support. L'application AWS Support renvoie un message d'erreur si vous essayez de configurer le même canal Slack pour un autre espace de travail.

Pour configurer un canal Slack

1. Depuis votre application Slack, choisissez le canal Slack que vous voulez utiliser avec l'application AWS Support.
2. Effectuez les étapes suivantes pour inviter l'application AWS Support à votre canal :

   a. Choisissez l'icône + et saisissez `invite`, puis, lorsque vous y êtes invité, choisissez Add apps to this channel (Ajouter des applications à ce canal).

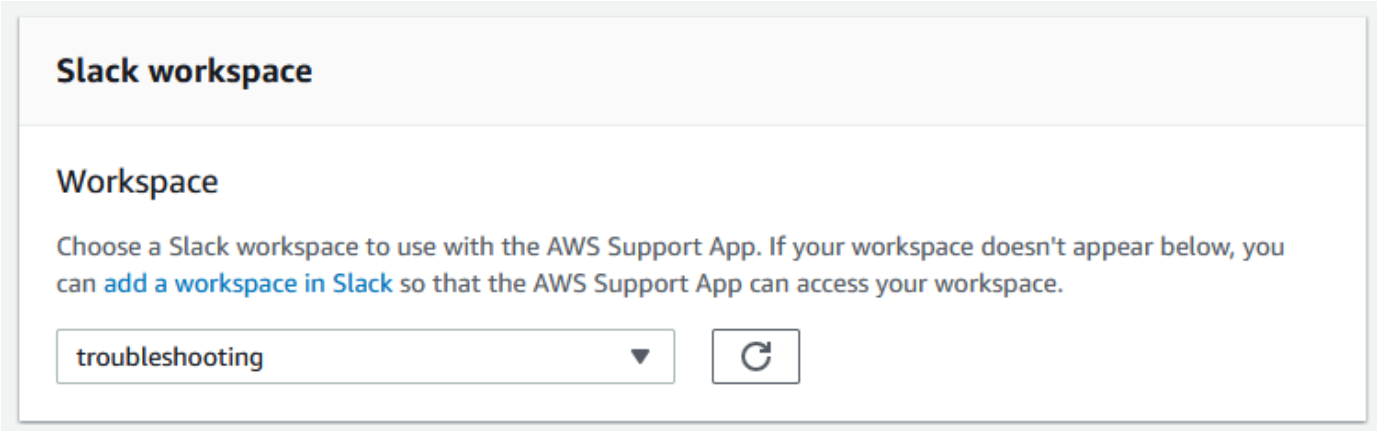
   

   b. Pour rechercher l'application, sous Add apps to channelName (Ajouter des applications à channelName), saisissez AWS SupportApp (Application).

   c. Sélectionnez Add (Ajouter) à côté de AWS SupportApp (Application).

3. Connectez-vous à Support Center Console (Console du centre de support) et choisissez Slack configuration (Configuration de Slack).
4. Choisissez Add channel (Ajouter un canal).
5. Sur la page Add channel (Ajouter un canal), sous Workspace (Espace de travail), sélectionnez le nom de l'espace de travail que vous avez précédemment autorisé. Vous pouvez choisir l'icône d'actualisation si le nom de l'espace de travail n'apparaît pas dans la liste.



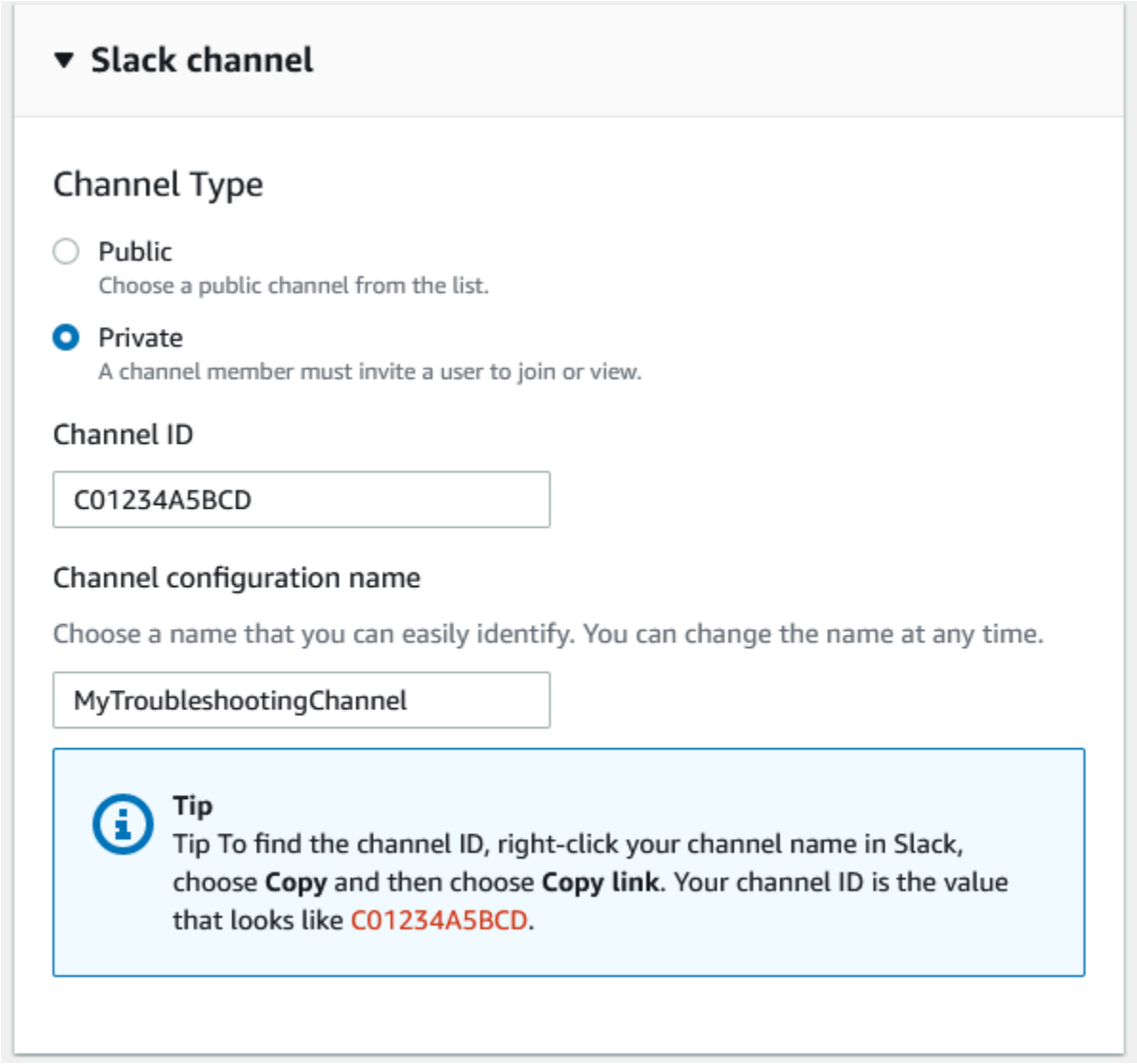
6. Sous Slack channel (Canal Slack), pour Channel type (Type de canal), sélectionnez l'une des options suivantes :

   - Public : sous Public channel (Canal public), choisissez le canal Slack auquel vous avez invité l'application AWS Support (étape 2). Si votre canal n'apparaît pas dans la liste, choisissez l'icône d'actualisation et réessayez.
   - Private (Privé) : sous Channel ID (ID du canal), saisissez l'ID ou l'URL du canal Slack auquel vous avez invité l'application AWS Support.

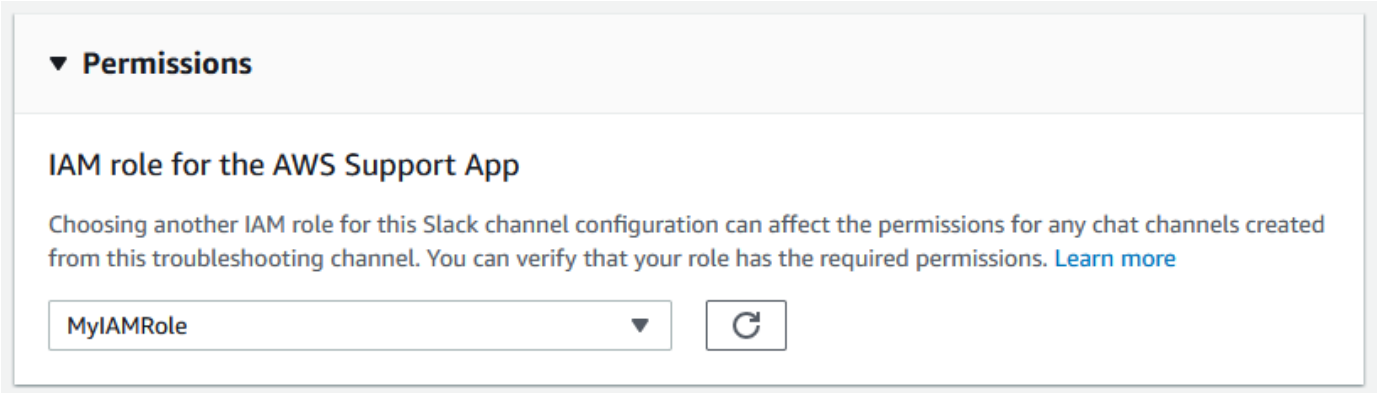
   > **Tip**
   >
   > Pour trouver l'ID du canal, ouvrez le menu contextuel (clic droit) pour le nom du canal dans Slack, puis choisissez Copy (Copier), et enfin Copy link (Copier le lien). L'ID de votre canal est la valeur qui ressemble à *C01234A5BCD*.

7. Sous Channel configuration name (Nom de la configuration du canal), saisissez un nom qui identifie facilement votre configuration de canal Slack pour l'application AWS Support. Ce nom apparaît uniquement dans votre Compte AWS et n'apparaît pas dans Slack. Vous pouvez renommer la configuration de votre canal plus tard.

   Le type de votre canal Slack peut ressembler à l'exemple suivant.



8. Sous Permissions (Autorisations), pour IAM role for the AWS Support App in Slack (Rôle IAM pour l'application dans Slack), sélectionnez un rôle que vous avez créé pour l'application AWS Support. Seuls les rôles qui ont l'application AWS Support comme entité de confiance apparaissent dans la liste.



> **Note**
>
> Si vous n'avez pas créé de rôle ou si vous ne voyez pas votre rôle dans la liste, consultez Gestion de l'accès à l'application AWS Support.

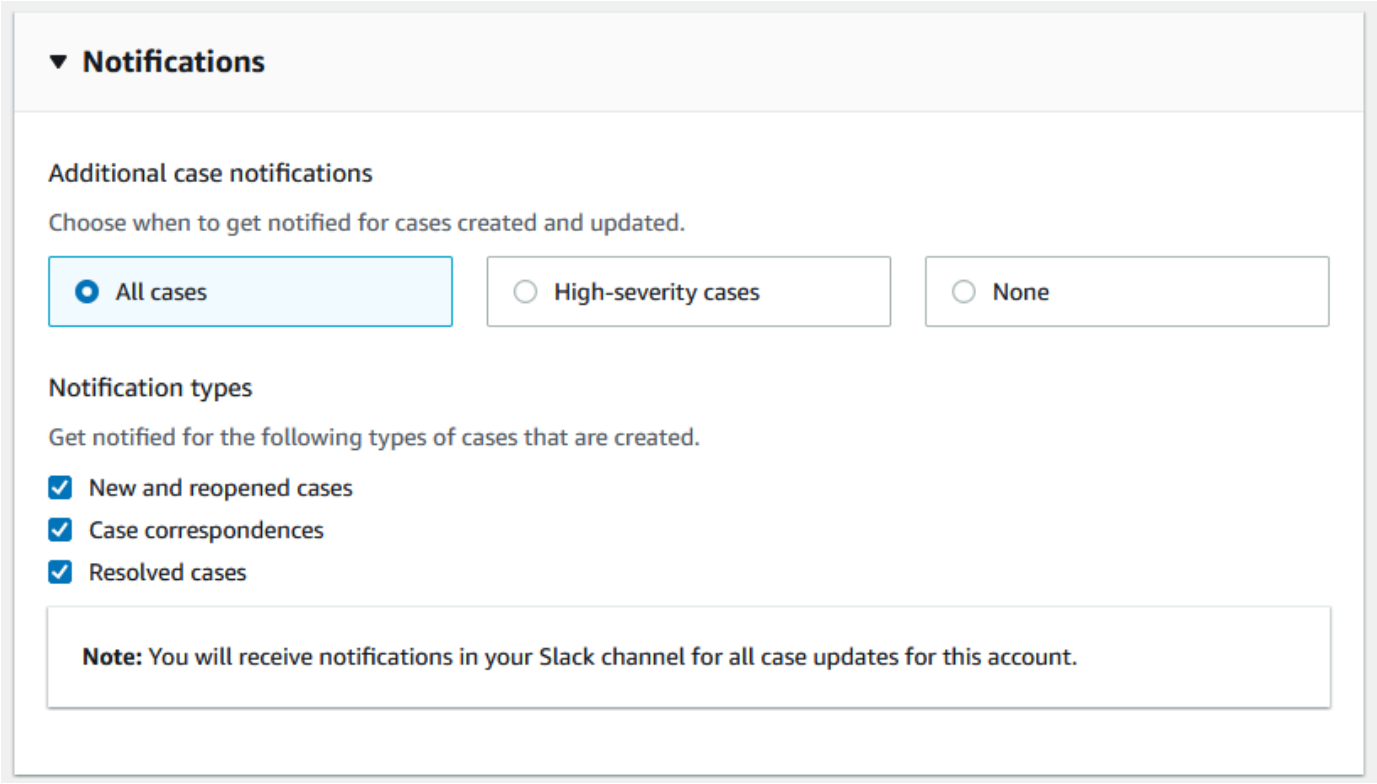
9. Sous Notifications, indiquez comment être notifié pour les cas.

   - All cases (Tous les cas) : recevez une notification pour toutes les mises à jour de cas.
   - High-severity cases (Cas de gravité élevée) : recevez une notification uniquement pour les cas qui affectent un système de production ou de niveau plus élevé. Pour de plus amples informations, veuillez consulter Choix du niveau de gravité.
   - None (Aucun) : ne pas être notifié des mises à jour de cas.

10. (Facultatif) Si vous choisissez All cases (Tous les cas) ou High-severity cases (Cas de gravité élevée), vous devez sélectionner au moins une des options suivantes :

    - New and reopened cases (Cas nouveaux et réouverts)
    - Case correspondences (Correspondances de cas)
    - Resolved cases (Cas résolus)

    Le canal suivant reçoit les notifications de cas pour toutes les mises à jour de cas dans Slack.



11. Vérifiez votre configuration et choisissez Add channel (Ajouter un canal). Votre canal apparaît dans la page Slack configuration (Configuration de Slack).

Mise à jour de la configuration de votre canal Slack

Après avoir configuré votre canal Slack, vous pouvez le mettre à jour ultérieurement pour modifier le rôle IAM ou la notification de cas.

Pour mettre à jour la configuration de votre canal Slack

1. Connectez-vous à Support Center Console (Console du centre de support) et choisissez Slack configuration (Configuration de Slack).
2. Sous Channels (Canaux), sélectionnez la configuration de canal que vous voulez.
3. Sur la page ***channelName***, vous pouvez effectuer les tâches suivantes :
   - Sélectionnez Rename (Renommer) pour mettre à jour le nom de la configuration de votre canal. Ce nom n'apparaît que dans votre Compte AWS et n'apparaîtra pas dans Slack.
   - Sélectionnez Delete (Supprimer) pour supprimer la configuration de canal à partir de l'application AWS Support. Consultez Suppression d'une configuration de canal Slack à partir de l'application AWS Support.

- Sélectionnez Open in Slack (Ouvrir dans Slack) pour ouvrir le canal Slack dans votre navigateur.
- Sélectionnez Edit (Modifier) pour modifier le rôle IAM ou les notifications.

Création de cas de support dans un canal Slack

Après avoir autorisé votre espace de travail Slack et ajouté votre canal Slack, vous pouvez créer un cas de support dans votre canal Slack.

Pour créer un cas de support dans Slack

1. Dans votre canal Slack, saisissez la commande suivante :

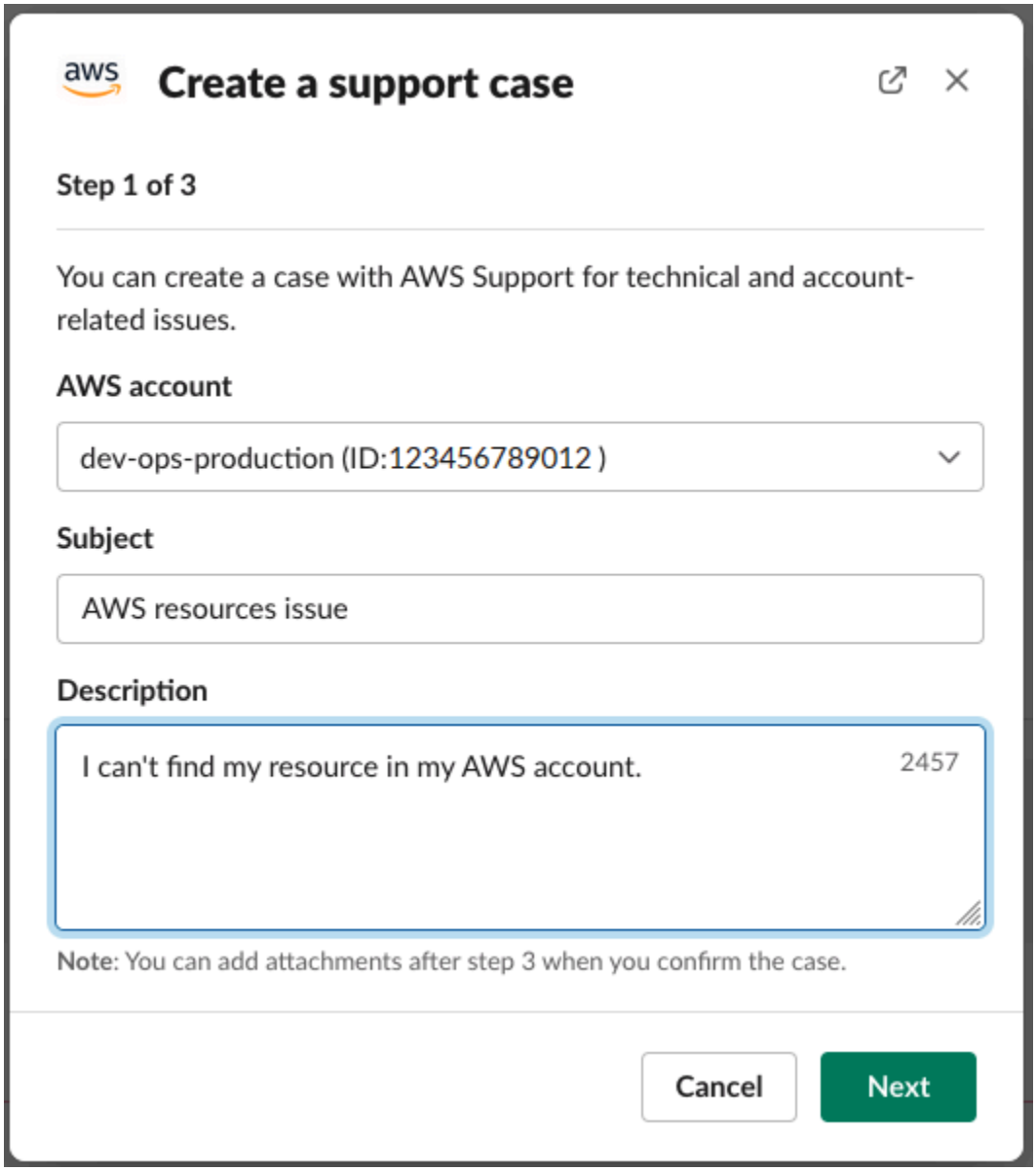
   ```
   /awssupport create
   ```

2. Dans la boîte de dialogue Create a support case (Créer un cas de support), suivez les étapes suivantes :

   a. Si vous avez configuré plus d'un compte pour ce canal Slack, pour Compte AWS, sélectionnez l'ID de compte. Si vous avez créé un nom de compte, cette valeur apparaît à côté de l'ID de compte. Pour de plus amples informations, veuillez consulter Autorisation d'un espace de travail Slack.

   b. Pour Subject (Sujet), saisissez un titre pour le cas de support.

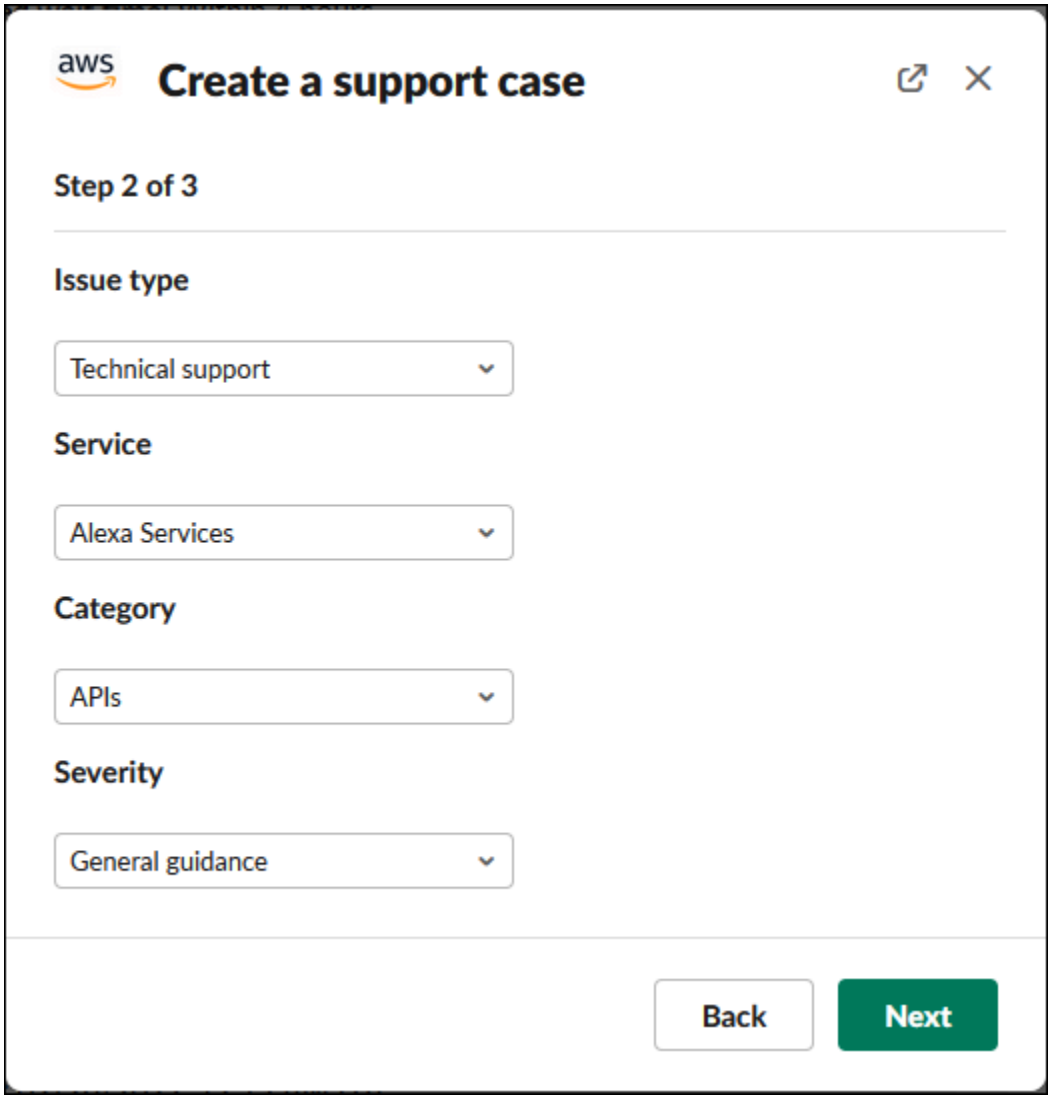
   c. Pour Description, décrivez le cas de support. Fournissez des détails, tels que la façon dont vous utilisez un Service AWS et les étapes de dépannage que vous avez essayées.



3. Choisissez Next (Suivant).
4. Dans la boîte de dialogue Create a support case (Créer un cas de support), spécifiez les options suivantes :

   a. Sélectionnez le Issue type (Type de problème).
   b. Sélectionnez le Service.
   c. Sélectionnez la Category (Catégorie).
   d. Sélectionnez la Severity (Gravité).
   e. Vérifiez les détails de votre cas et sélectionnez Next (Suivant).

      L'exemple suivant montre un dossier de support technique pour les Services Alexa.

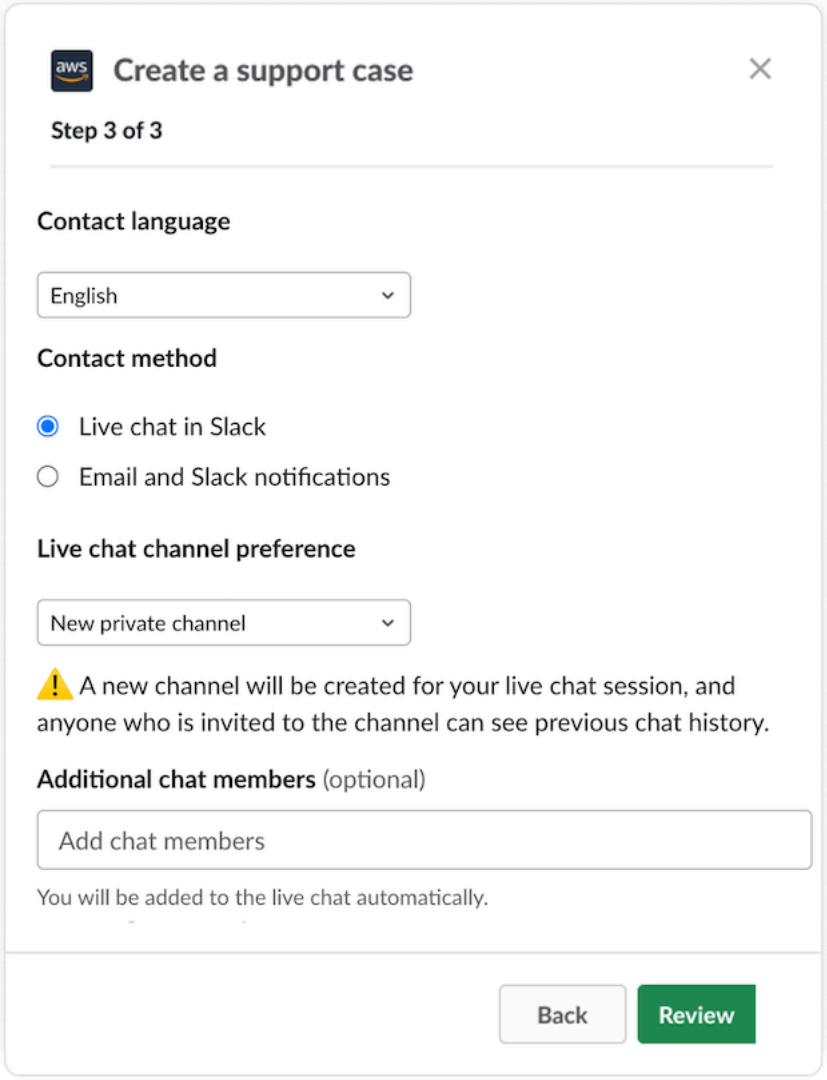


5. Pour Contact language (Langue de contact), choisissez votre langue préférée pour le cas de support.

> **Note**
>
> L'assistance en japonais n'est pas disponible pour le chat en direct dans Slack pour les cas de support pour le compte et la facturation.

6. Pour Contact method (Méthode de contact), choisissez Email and Slack notifications (Notifications par e-mail et Slack) ou Live chat in Slack (Chat en direct dans Slack).

   L'exemple suivant montre comment choisir un chat en direct dans Slack.



a. Si vous choisissez Live chat in Slack (Chat en direct dans Slack), choisissez New private channel (Nouveau canal privé) ou Current channel (Canal actuel) dans Live chat channel preference (Préférences de canal de chat en direct). Si vous choisissez New private channel (Nouveau canal privé), un canal privé distinct sera créé pour vous permettre de discuter avec l'agent AWS Support. Si vous choisissez Current channel (Canal actuel), un fil de discussion du canal actuel sera utilisé pour le chat avec l'agent AWS Support.

b. (Facultatif) Si vous choisissez Live chat in Slack (Chat en direct dans Slack), vous pouvez saisir les noms d'autres membres de Slack. Si vous choisissez New private channel (Nouveau canal privé), l'application AWS Support vous ajoutera automatiquement, ainsi que les membres sélectionnés, au nouveau canal. Si vous choisissez Current channel (Canal actuel), l'application AWS Support vous mentionnera automatiquement, ainsi que les membres sélectionnés, dans le fil de discussion lorsque l'agent AWS Support le rejoindra.

> **Important**
>
> - Nous vous recommandons de n'ajouter que les membres du chat auxquels vous souhaitez donner accès à votre demande de support et à l'historique de chat.
> - Si vous lancez une nouvelle session de chat en direct pour une demande de support existante, l'application AWS Support utilise le même canal de chat que celui utilisé pour un précédent chat en direct. L'application AWS Support utilise également les mêmes préférences de canal de chat en direct que celles utilisées précédemment.
> - L'option Current channel (Canal actuel) n'est disponible que si le chat est demandé depuis un canal privé. Nous vous recommandons de n'utiliser cette option que si vous souhaitez que tous les membres du chat aient accès à votre demande de support.

7. (Facultatif) Pour Additional contacts to notify (Contacts supplémentaires à notifier), saisissez les adresses e-mail qui recevront également les mises à jour concernant ce cas de support. Vous pouvez ajouter jusqu'à 10 adresses e-mail.
8. Choisissez Examiner.
9. Dans le canal Slack, consultez les détails du cas. Vous pouvez effectuer les actions suivantes :
   - Choisissez Edit (Modifier) pour modifier les détails du cas.
   - Ajoutez un fichier à votre cas. Pour ce faire, procédez comme suit :
     a. Choisissez Attach file (Joindre un fichier), puis l'icône + dans Slack, et choisissez Your computer (Votre ordinateur).
     b. Accédez à votre fichier et choisissez-le.
     c. Dans la boîte de dialogue Upload a file (Charger un fichier), saisissez `@awssupport` et appuyez sur l'icône d'envoi de message  .

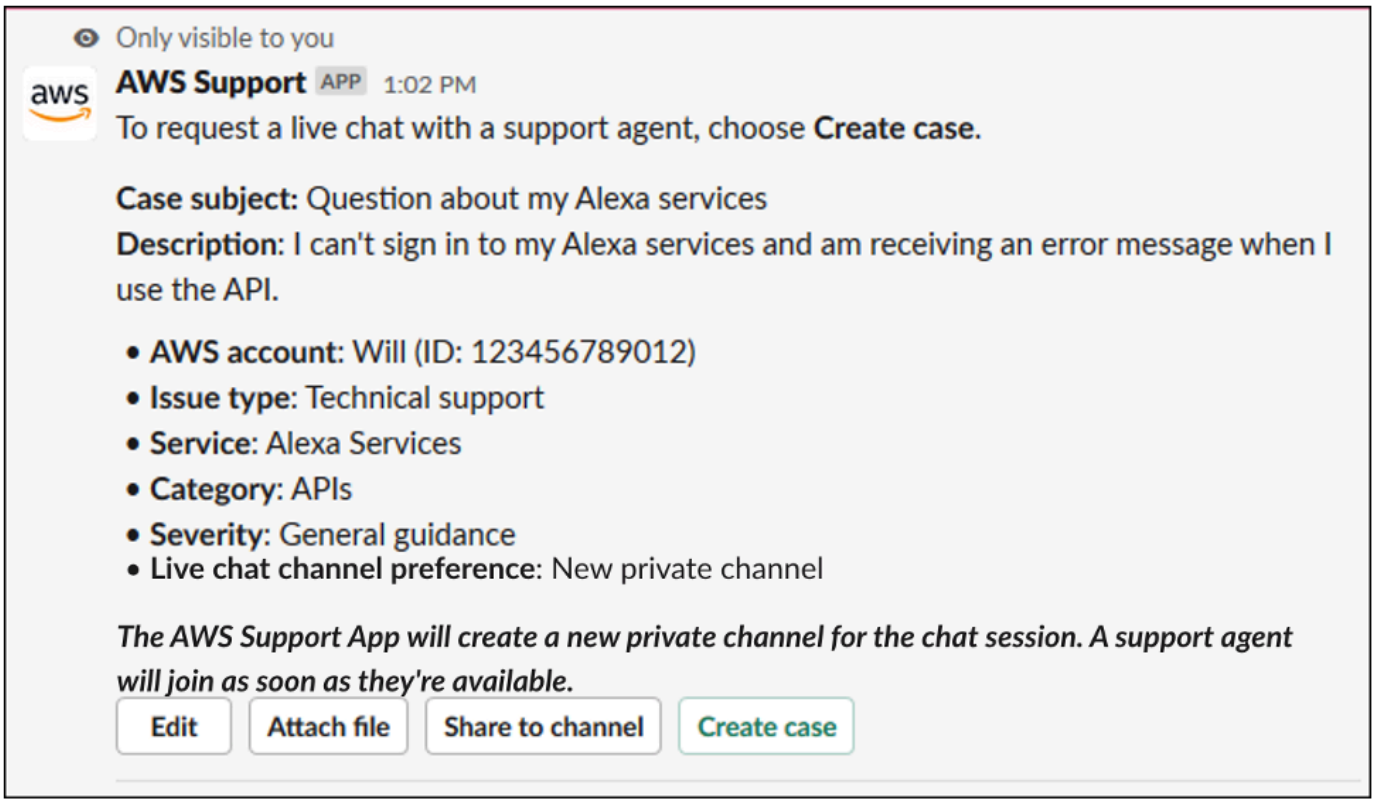
> **Remarques**
>
> - Vous pouvez attacher jusqu'à 3 fichiers. La taille de chaque fichier peut aller jusqu'à 5 Mo.

- Si vous joignez un fichier à votre cas de support, vous devez envoyer votre cas dans un délai d'une heure. Si vous ne le faites pas, vous devez ajouter les fichiers à nouveau.

- Choisissez Share to channel (Partager sur le canal) pour partager les détails du cas avec d'autres personnes dans le canal Slack. Vous pouvez utiliser cette option pour partager les détails du cas avec votre équipe avant de créer le cas.

10. Vérifiez les détails de votre cas, puis sélectionnez Create case (Créer le cas).

    L'exemple suivant montre un dossier de support technique pour les Services Alexa.



    Après avoir créé un cas de support, il peut s'écouler quelques minutes avant que les détails de votre cas n'apparaissent.

11. Lorsque votre cas de support est mis à jour, vous pouvez choisir See details (Voir les détails) pour afficher les informations relatives à votre cas. Vous pouvez alors effectuer ce qui suit :

    - Choisissez Share to channel (Partager sur le canal) pour partager les détails du cas avec d'autres personnes dans le canal Slack.
    - Choisissez Reply (Répondre) pour ajouter une correspondance.
    - Choisissez Resolve case (Résoudre le cas).

> **Note**
>
> Si vous n'avez pas choisi de recevoir des mises à jour automatiques des cas dans Slack, vous pouvez rechercher le cas de support pour trouver l'option See details (Voir les détails).

Réponse aux cas de support dans Slack

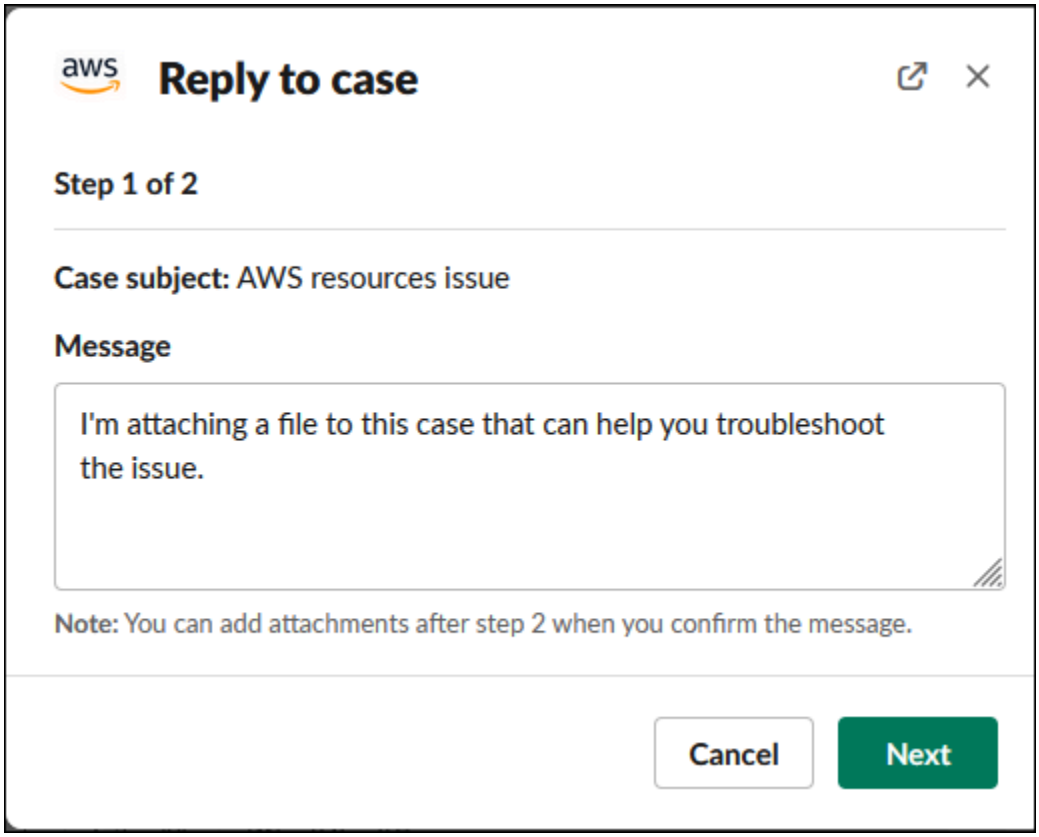
Vous pouvez ajouter des mises à jour à votre dossier, comme les détails du dossier et les pièces jointes, et répondre aux réponses de l'agent d'assistance.

> **Note**
>
> - Vous pouvez également utiliser le AWS Support Center Console pour répondre aux agents de support. Pour de plus amples informations, veuillez consulter Mise à jour, surveillance, résolution et réouverture de votre cas.
> - Vous ne pouvez pas ajouter de correspondance à des demandes provenant de canaux de chat créés par l'application AWS Support. Les canaux de chat en direct n'envoient des messages aux agents que pendant le chat en direct.

Pour répondre à un cas de support dans Slack

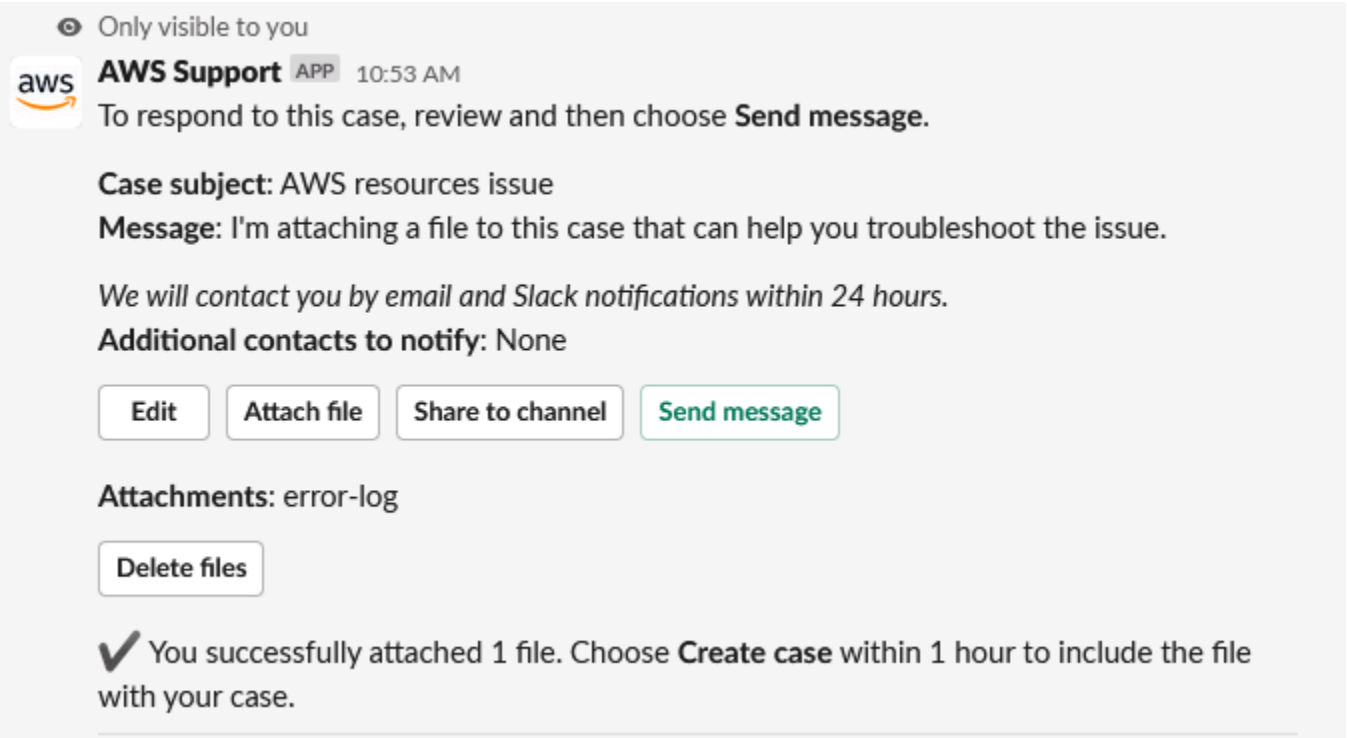
1. Dans votre canal Slack, choisissez le cas auquel vous voulez répondre. Vous pouvez saisir `/awssupport search` pour trouver votre cas de support.
2. Sélectionnez See details (Voir les détails) à côté du cas que vous voulez.
3. En bas des détails du cas, sélectionnez Reply (Répondre).

4. Dans la boîte de dialogue Reply to case (Répondre au cas), saisissez une brève description du problème dans le champ Message. Sélectionnez ensuite Next (Suivant).



5. Choisissez votre méthode de contact. Les méthodes de contact disponibles dépendent du type de cas et du plan de support.
6. (Facultatif) Pour Additional contacts to notify (Contacts supplémentaires à notifier), saisissez les adresses e-mail supplémentaires dont vous voulez qu'elles reçoivent des mises à jour sur ce cas de support. Vous pouvez ajouter jusqu'à 10 adresses e-mail.
7. Choisissez Examiner. Vous pouvez ensuite choisir si vous voulez modifier votre réponse, joindre des fichiers ou partager sur le canal.
8. Lorsque vous êtes prêt à répondre, sélectionnez Send message (Envoyer le message).
9. (Facultatif) Pour afficher la correspondance précédente pour votre cas, sélectionnez Previous correspondence (Correspondance précédente). Pour afficher des messages abrégés, sélectionnez Show full message (Afficher le message complet).

Example : Répondre à un cas dans Slack



Rejoindre une session de chat en direct avec AWS Support

Lorsque vous demandez un chat en direct pour votre demande, vous avez le choix d'utiliser soit un nouveau canal de chat, soit un fil de discussion pour vous et l'agent AWS Support dans le canal actuel. Utilisez ce canal de chat ou ce fil de discussion pour communiquer avec l'agent de support et toute autre personne que vous avez invitée au chat en direct.

> **Important**
>
> Toute personne qui rejoint un canal comprenant un chat en direct peut afficher les détails de la demande de support en question et l'historique de chat. Nous vous recommandons de n'ajouter que les utilisateurs qui ont besoin d'accéder à vos cas de support. Tous les membres d'un canal de chat ou d'un fil de discussion peuvent également participer à un chat actif.

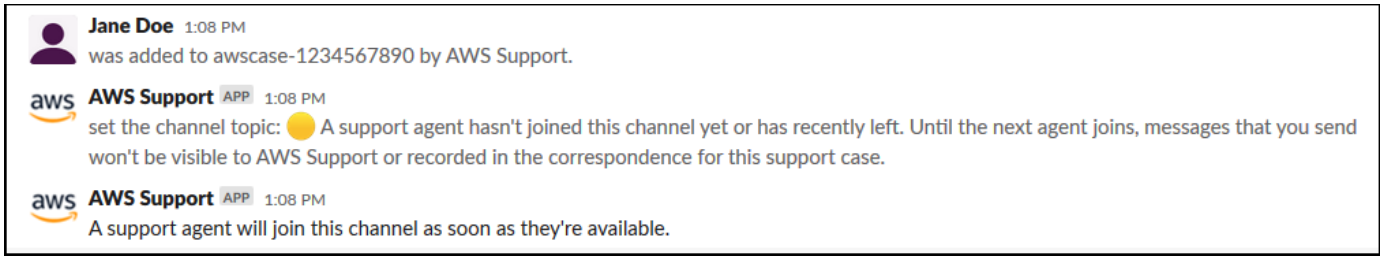
> **Note**
>
> Des notifications s'afficheront également dans les canaux de chat en direct et les fils de discussion si une correspondance est ajoutée à la demande en dehors de la session de chat en direct. Cela se produira avant, pendant et après une session de chat. Vous pouvez donc utiliser un canal de chat ou un fil de discussion pour suivre toutes les mises à jour relatives à une demande. Si vous choisissez d'utiliser un nouveau canal de chat, utilisez le canal de configuration sur lequel vous avez invité l'application AWS Support pour répondre à ces correspondances.

Pour rejoindre une session de chat en direct avec AWS Support dans un nouveau canal

1. Dans l'application Slack, accédez au canal que l'application AWS Support crée pour vous. Le nom du canal comprend l'ID de votre cas de support, tel que *awscase-1234567890*.

   > **Note**
   >
   > L'application AWS Support ajoute un message épinglé au canal de chat en direct qui contient des détails sur votre cas de support. À partir du message épinglé, vous pouvez mettre fin au chat ou résoudre le cas. Vous pouvez trouver tous les messages épinglés dans ce canal sous le nom du canal.

2. Lorsque l'agent de support rejoint le canal, vous pouvez discuter de votre cas de support. Tant qu'un agent de support n'a pas rejoint le canal, l'agent ne verra pas les messages de ce chat, et les messages n'apparaîtront pas dans la correspondance de votre cas.

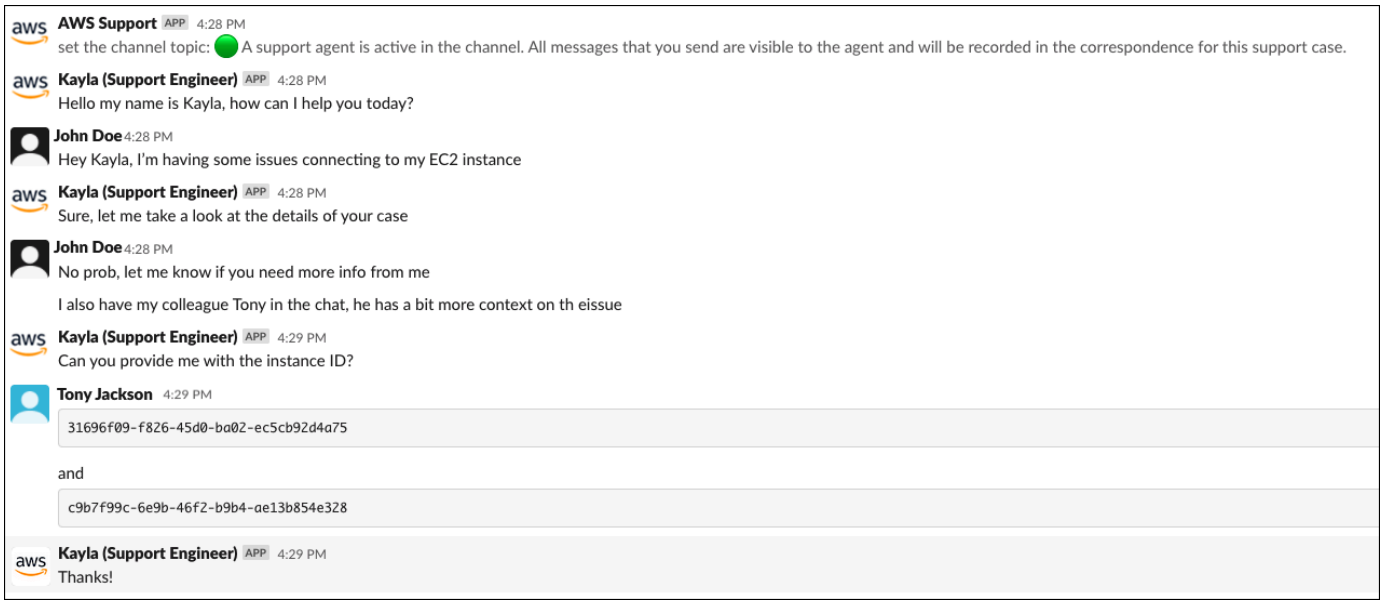
3. (Facultatif) Ajoutez d'autres membres au canal de chat. Par défaut, les canaux de chat sont privés.
4. Une fois que l'agent de support a rejoint le chat, le canal de chat est actif et l'application AWS Support enregistre le chat.

Vous pouvez discuter avec l'agent de votre cas de support et charger toute pièce jointe sur le canal. L'application AWS Support enregistre automatiquement vos fichiers et le journal du chat dans la correspondance de votre cas.

> **Note**
>
> Lorsque vous discutez avec un agent de support, notez les différences suivantes dans Slack pour l'application AWS Support :
>
> - Les agents de support ne peuvent pas voir les messages ou fils de discussion partagés. Pour partager le texte d'un message ou d'un fil de discussion, saisissez le texte dans un nouveau message.
> - Si vous modifiez ou supprimez un message, l'agent voit toujours le message original. Vous devez saisir à nouveau votre nouveau message pour afficher la révision.

Example : Session de chat en direct

Voici un exemple de session de chat en direct avec un agent de support pour résoudre un problème de connectivité pour deux instances Amazon Elastic Compute Cloud (Amazon EC2).

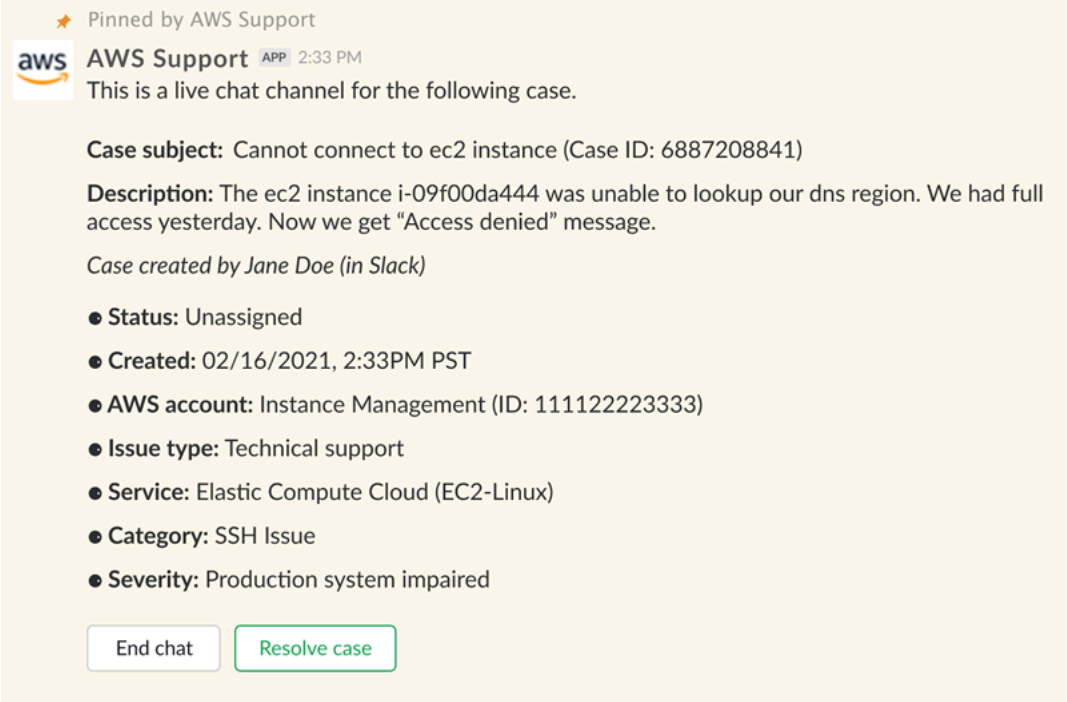


5. (Facultatif) Pour arrêter le chat en direct, cliquez sur End chat (Terminer le chat). L'agent de support quitte le canal et l'application AWS Support arrête d'enregistrer le chat en direct. Vous pouvez trouver l'historique du chat attaché à la correspondance de ce cas de support.

6. Si le problème est résolu, vous pouvez choisir Resolve case (Résoudre le cas) à partir du message épinglé ou saisir `/awssupport resolve`.

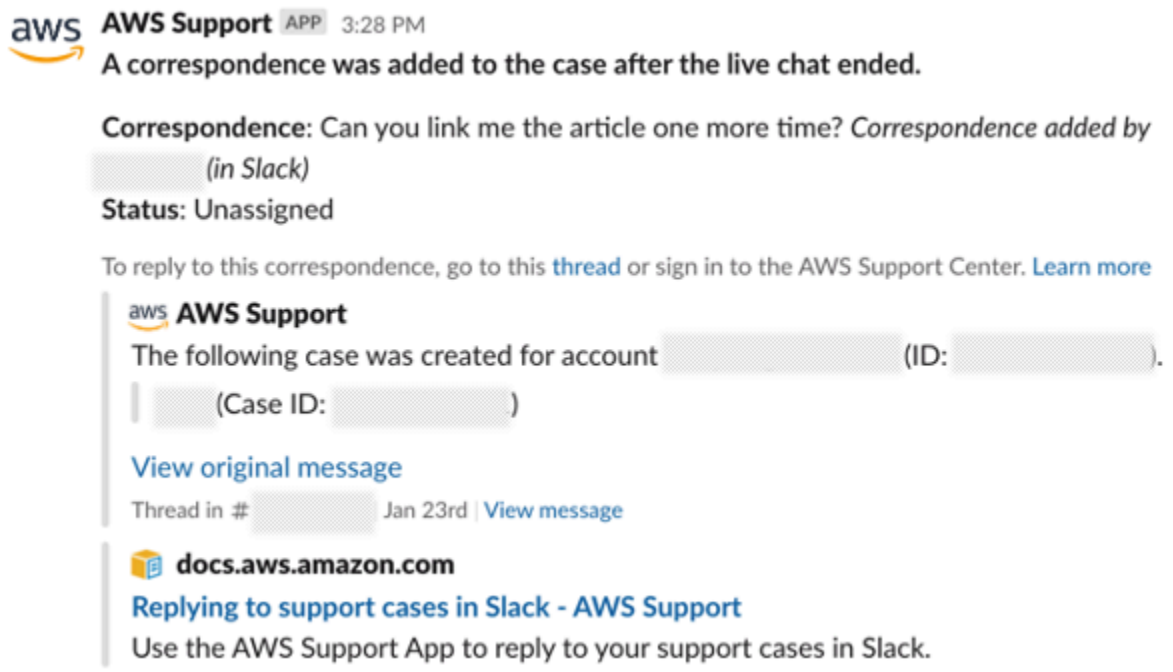
   Example : Terminer un chat en direct

   Le message épinglé suivant montre les détails du cas concernant une instance Amazon EC2. Vous pouvez trouver les messages épinglés sous le nom du canal Slack.



   Example : notification de correspondance dans le canal de discussion

   Voici un exemple de canal de chat en direct recevant une notification lorsqu'un autre collaborateur ajoute une mise à jour une fois le chat terminé.

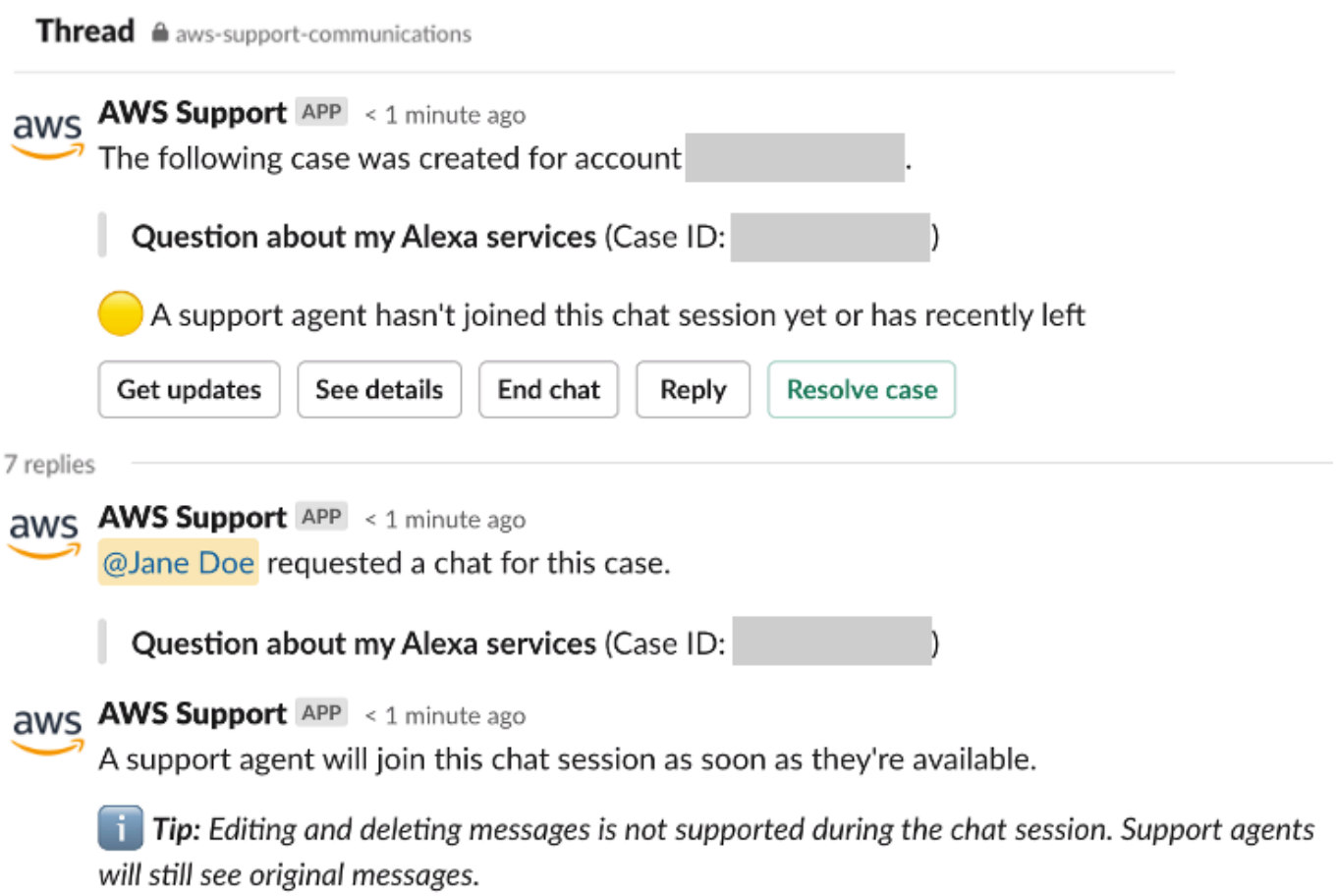


La notification indiquera l'état du chat (demandé, en cours ou terminé) et si la correspondance a été ajoutée par un agent ou par un autre collaborateur. L'application Support tentera également d'établir un lien vers le fil ou le canal Slack d'origine sur lequel cette discussion a été demandée. Vous pouvez répondre à cette affaire à partir de ce canal ou de tout autre canal ayant accès à cette affaire.

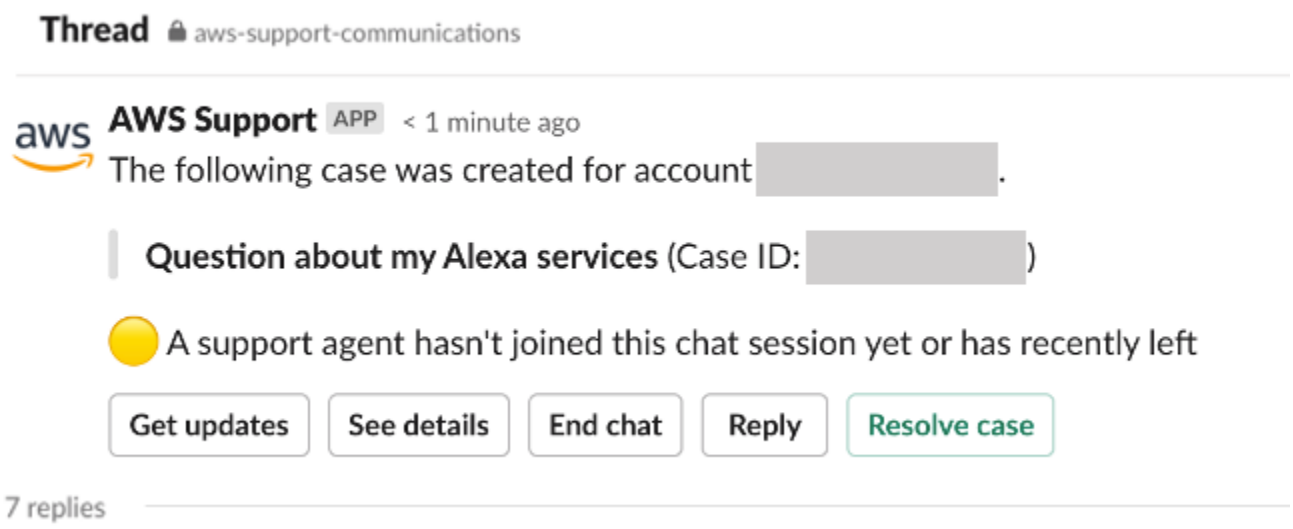
Pour rejoindre une session de chat en direct avec AWS Support dans le canal actuel

1. Dans l'application Slack, accédez au fil de discussion du canal actuel que l'application AWS Support utilise pour le chat. Dans la plupart des cas, il s'agit du fil de discussion créé lors de la création de la demande.
2. Lorsque l'agent de support rejoint le fil de discussion, vous pouvez discuter de votre demande de support. Tant qu'il n'aura pas rejoint le fil de discussion, l'agent ne verra pas les messages qu'il contient, et les messages ne s'afficheront pas dans la correspondance liée à votre demande lorsque le chat prendra fin.

> **Note**
>
> Les messages envoyés dans ce canal en dehors du fil de discussion ne sont jamais vus par AWS Support, même lorsqu'un chat est actif.



3. (Facultatif) Mentionnez les autres membres du canal pour les notifier dans le fil de discussion.
4. Une fois que l'agent de support a rejoint le chat, le fil de discussion est actif et l'application AWS Support enregistre le chat. Comme pour l'option utilisant un nouveau canal, vous pouvez discuter avec l'agent de votre demande de support et charger des pièces jointes sur le canal. L'application AWS Support enregistre automatiquement vos fichiers et le journal du chat dans la correspondance de votre cas.
5. (Facultatif) Pour arrêter le chat en direct, cliquez sur End chat (Terminer le chat) au niveau du premier message du fil de discussion. L'agent de support quitte le fil de discussion et l'application AWS Support arrête d'enregistrer le chat en direct. Vous pouvez trouver l'historique du chat attaché à la correspondance de ce cas de support.
6. Si le problème est résolu, choisissez Résoudre le cas au niveau du premier message du fil de discussion.



Recherche de cas de support dans Slack

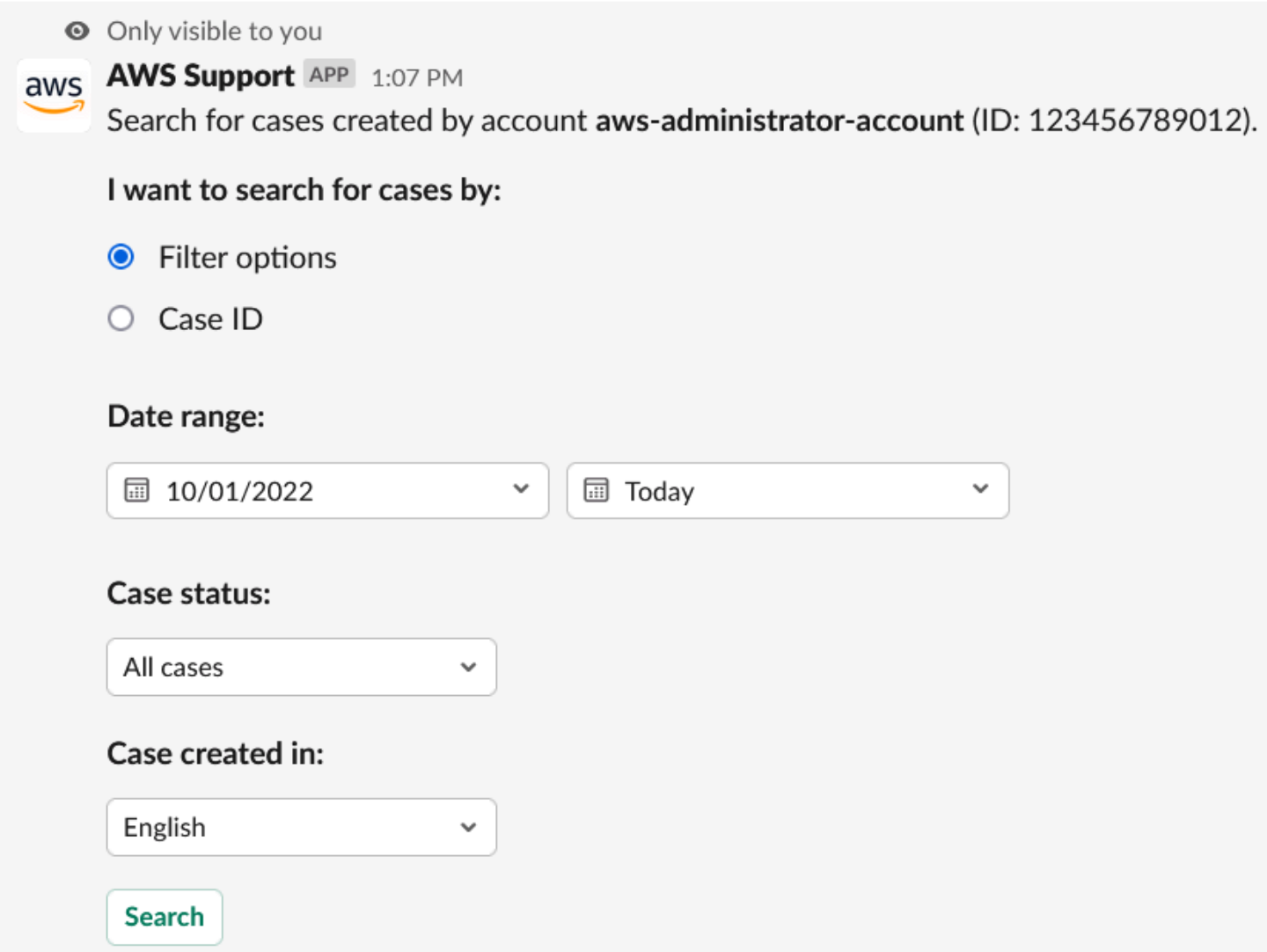
Depuis votre canal Slack, vous pouvez rechercher des dossiers de support depuis votre Compte AWS et depuis d'autres comptes qui ont configuré le même canal et le même espace de travail. Par exemple, si votre compte (123456789012) et celui de votre collègue (111122223333) ont configuré le même espace de travail et les mêmes canaux dans la AWS Support Center Console, vous pouvez utiliser l'application AWS Support pour rechercher les dossiers de support de chacun.

Pour filtrer vos résultats, utilisez les options suivantes :

- ID de compte
- ID du dossier
- Statut du dossier
- Langue du contact
- Plage de dates

Example : recherche de cas dans Slack

L'exemple suivant montre comment effectuer une recherche par Filter options (Options de filtre) pour un seul compte en spécifiant la plage de dates, l'état du cas et la langue du contact.



Pour rechercher un dossier de support dans Slack

1. Dans le canal Slack, saisissez la commande suivante :

   ```
   /awssupport search
   ```

2. Pour l'option I want to search for cases by: (Je souhaite rechercher des dossiers par :), choisissez l'une des options suivantes :

   A. Filter options (Options de filtre) : vous pouvez filtrer les dossiers à l'aide des options suivantes :

   - Compte AWS : cette liste n'apparaît que si vous avez plusieurs comptes dans ce canal.
   - Date range (Plage de dates) : date à laquelle le dossier a été créé.

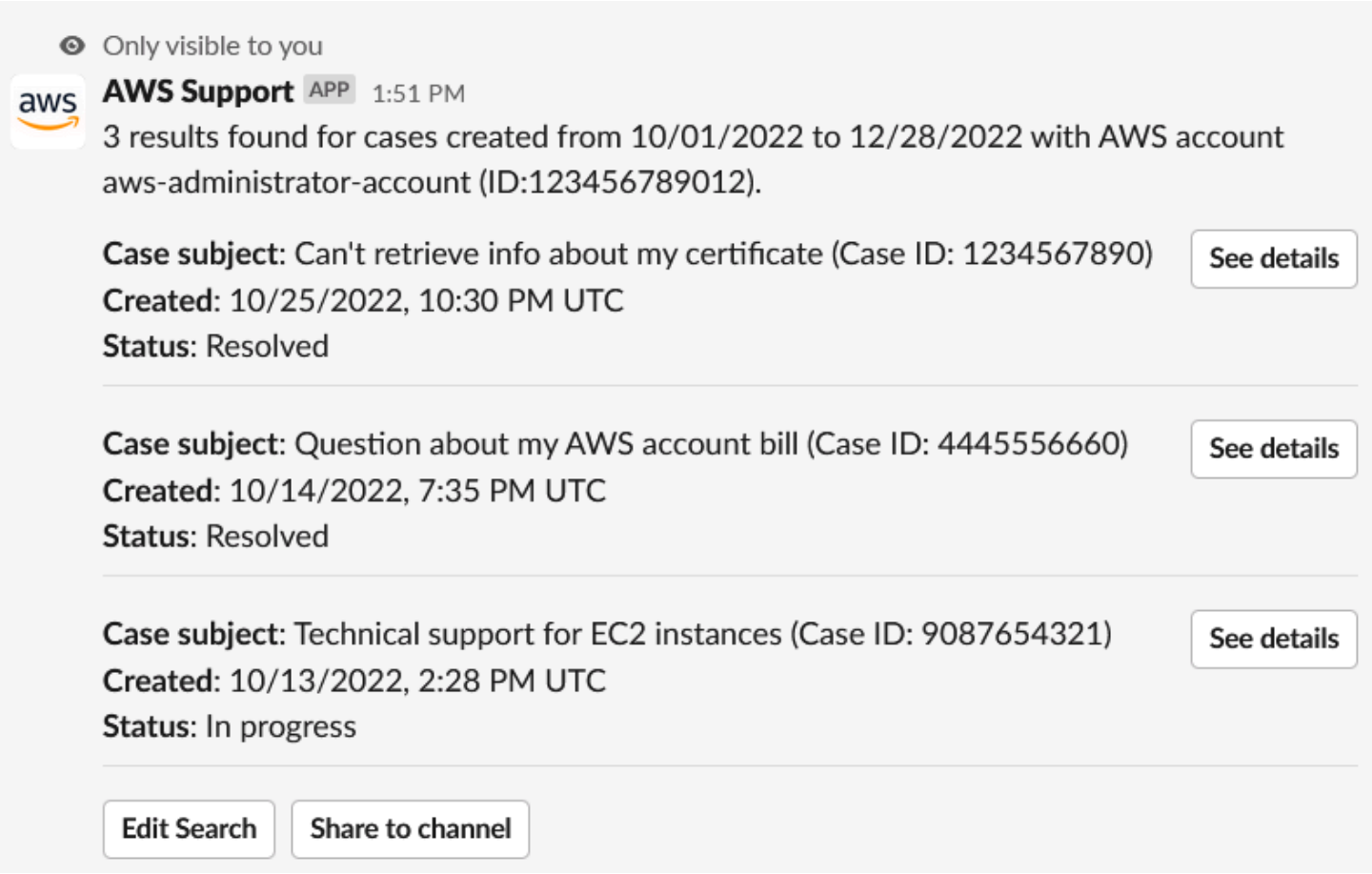
- Case status (Statut du dossier) : choisissez l'état du dossier, tel que All open cases (Tous les dossiers ouverts) ou Resolved (Résolus).
- Case created in (Dossier créé dans) : la langue de contact pour le dossier.

B. Case ID (ID du dossier) : entrez l'ID du dossier. Vous ne pouvez saisir qu'un seul dossier à la fois. Si vous avez plusieurs comptes sur la chaîne, choisissez le Compte AWS pour rechercher le dossier.

3. Choisissez Search (Rechercher). Les résultats de votre recherche apparaissent dans Slack.

Utilisez les résultats de votre recherche

L'exemple suivant renvoie trois dossiers de support résolus à partir d'un Compte AWS.



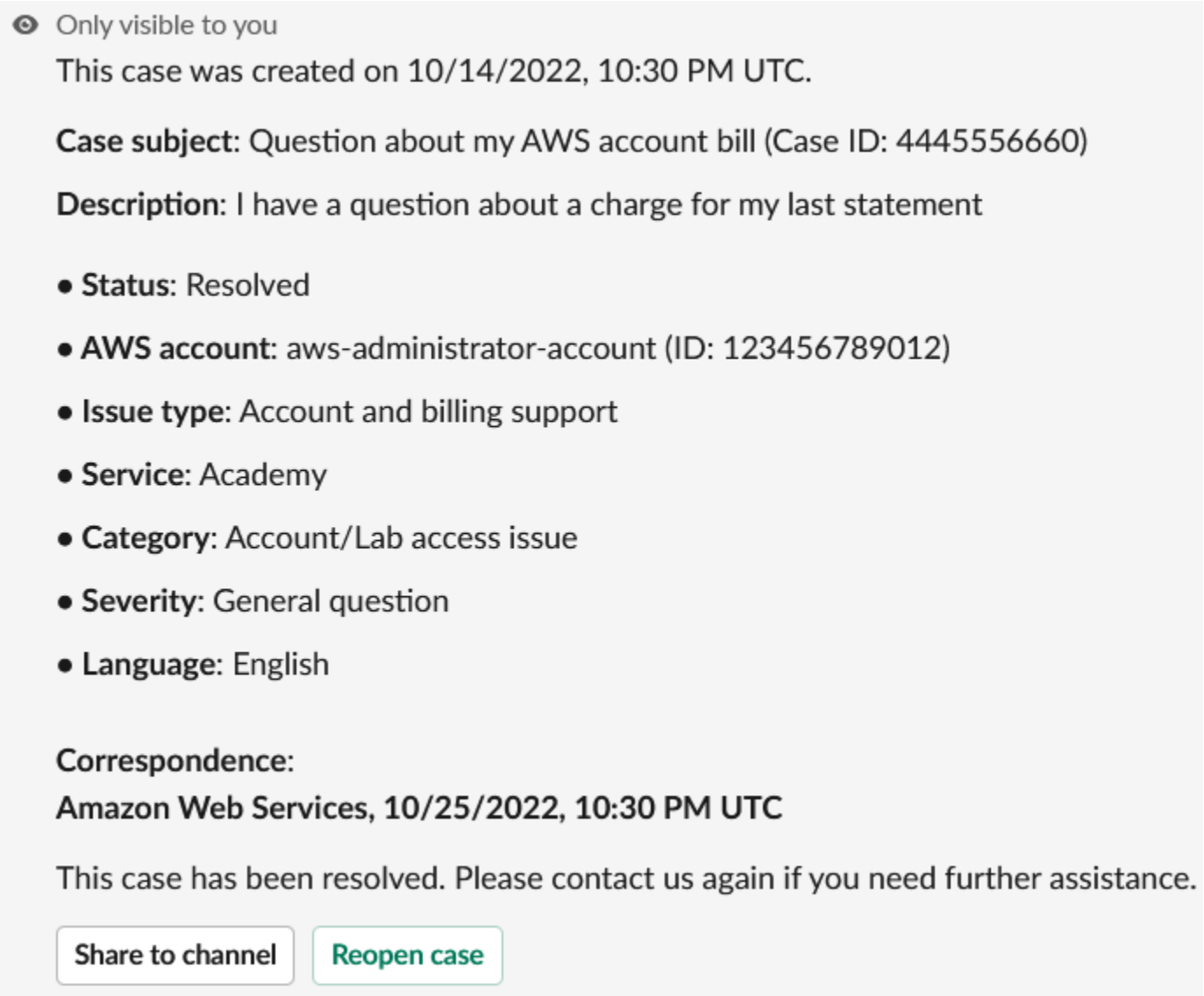
Une fois que vous recevez les résultats de votre recherche, procédez comme suit :

Pour utiliser les résultats de votre recherche

1. Choisissez Edit Search (Modifier la recherche) pour modifier vos options de filtre ou votre ID de dossier précédent.
2. Choisissez Share to channel (Partager sur le canal) pour partager les résultats de la recherche avec le canal.
3. Choisissez See details (Voir les détails) pour avoir plus d'informations sur un dossier. Vous pouvez choisir Show full message (Afficher le message complet) pour voir le reste de la dernière correspondance.
4. Si vous avez effectué une recherche à l'aide des options de filtre, les résultats de recherche peuvent renvoyer plusieurs dossiers. Choisissez Next 5 results (Les 5 résultats suivants) ou Previous 5 results (Les 5 résultats précédents) pour afficher les 5 dossiers suivants ou précédents.

Example : résoudre un dossier de support

L'exemple suivant montre un dossier d'assistance résolu concernant un problème de compte et de facturation après avoir sélectionné Afficher les détails.



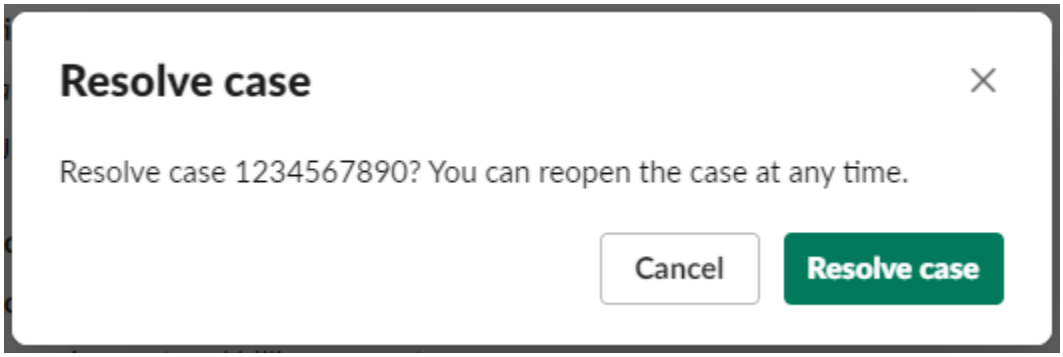
Résolution d'un cas de support dans Slack

Si vous n'avez plus besoin de votre cas de support, ou si vous avez résolu le problème, vous pouvez résoudre un cas de support directement dans Slack. Cela résout également le cas dans l'application AWS Support Center Console. Après avoir résolu un cas, vous pouvez le rouvrir plus tard.

Pour résoudre un cas de support dans Slack

1. Dans votre canal Slack, accédez au cas de support. Consultez Recherche de cas de support dans Slack.
2. Sélectionnez See details (Voir les détails) pour le cas.
3. Choisissez Resolve case (Résoudre le cas).

4. Dans la boîte de dialogue Resolve case (Résoudre le cas), choisissez Resolve case (Résoudre le cas). Vous pouvez rouvrir un cas dans le canal Slack ou à partir de la console du centre de support.

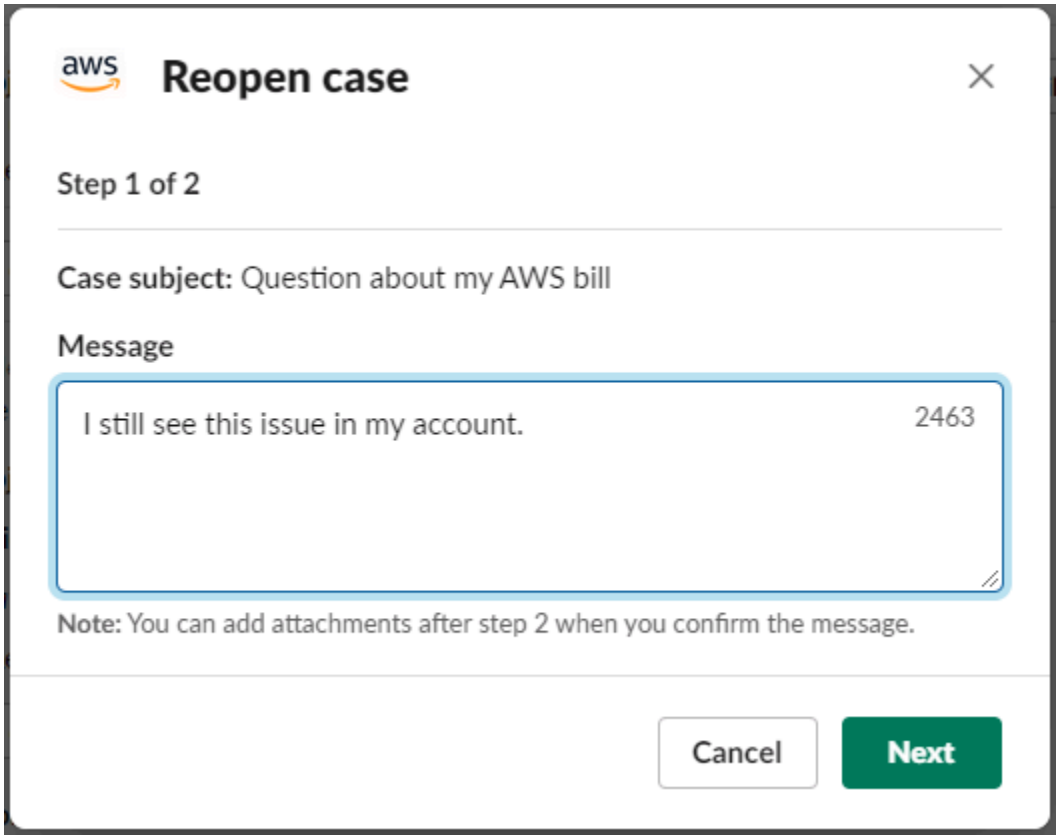


Réouverture d'un cas de support dans Slack

Après avoir résolu un cas de support, vous pouvez rouvrir le cas depuis Slack.

Pour rouvrir un cas de support dans Slack

1. Trouvez le cas de support à rouvrir dans Slack. Consultez Recherche de cas de support dans Slack.
2. Sélectionnez See details (Voir les détails).
3. Choisissez Reopen case (Rouvrir le cas).
4. Dans la boîte de dialogue Reopen case (Rouvrir le cas), saisissez une brève description du problème dans le champ Message.
5. Choisissez Next (Suivant).



6. (Facultatif) Saisissez des contacts supplémentaires.
7. Choisissez Examiner.
8. Vérifiez les détails de votre cas, puis cliquez sur Send message (Envoyer le message). Votre cas est rouvert. Si vous avez demandé un nouveau chat en direct avec un agent de support, Slack utilise le même canal de chat ou fil de discussion que celui utilisé pour précédent chat en direct. S'il s'agit de la première fois que vous demandez un chat en direct dans un nouveau canal, un nouveau canal de chat s'ouvre. S'il s'agit de la première fois que vous demandez un chat en direct dans le canal actuel, un fil de discussion dans le canal actuel est utilisé.

Demande d'augmentations de quota de service

Vous pouvez demander des augmentations de quota de service pour votre compte depuis votre canal Slack.

Pour demander des augmentations de quota de service

1. Dans le canal Slack, saisissez la commande suivante :

   ```
   /awssupport quota
   ```

2. Dans la boîte de dialogue Increase service quota (Augmenter le quota de service), saisissez les informations suivantes :

   a. Cliquez sur le bouton Compte AWS.

   b. Cliquez sur le bouton Région AWS.

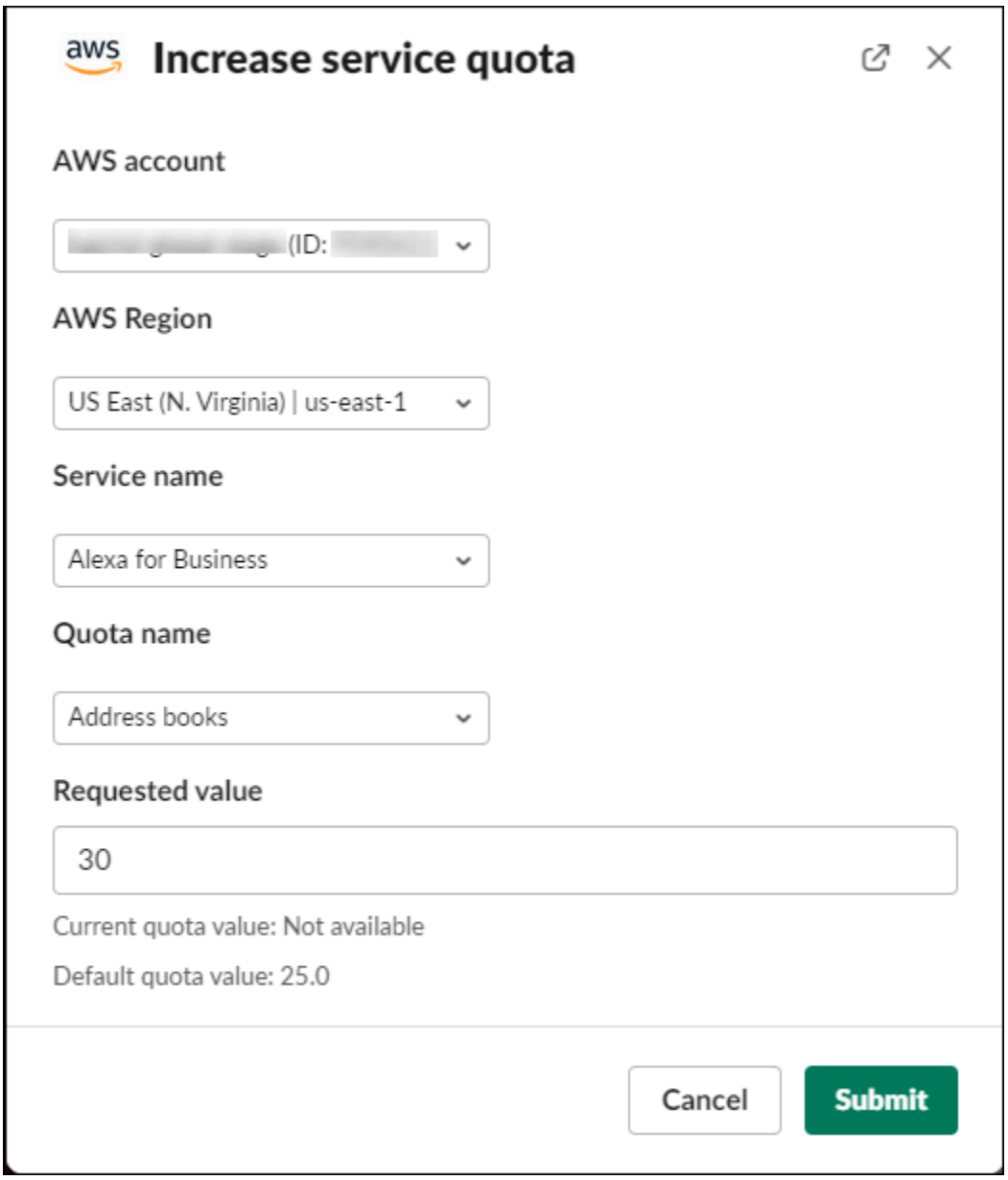
   c. Choisissez le Service name (Nom du service).

   d. Choisissez le Quota name (Nom du quota).

   e. Saisissez la Requested value (Valeur demandée) pour l'augmentation du quota. Vous devez saisir une valeur supérieure au quota par défaut.

3. Sélectionnez Submit (Envoyer).

Example : Augmentation du quota pour Alexa for Business



Vous pouvez également consulter vos demandes à partir de la console Service Quotas. Pour de plus amples informations, veuillez consulter Demande d'augmentation de quota dans le Guide de l'utilisateur Service Quotas.

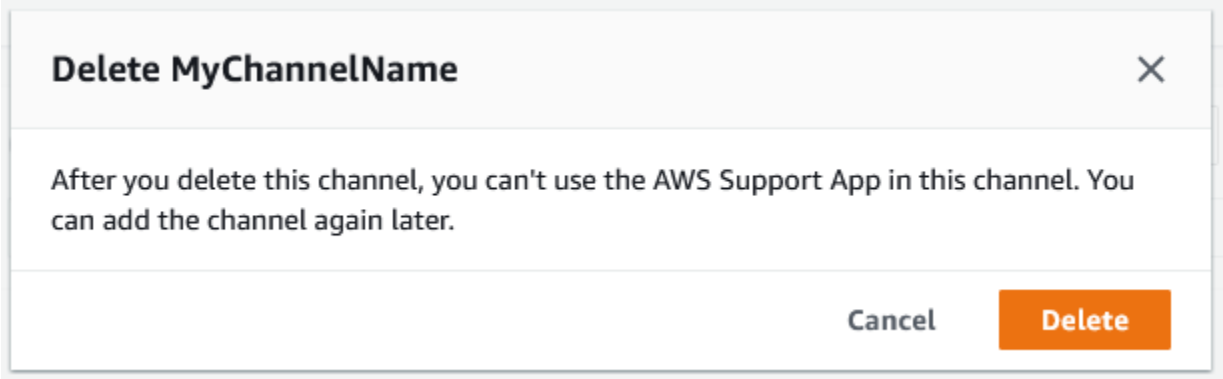
Suppression d'une configuration de canal Slack à partir de l'application AWS Support

Vous pouvez supprimer une configuration de canal à partir de l'application AWS Support si vous n'en avez pas besoin. Cette action supprime uniquement le canal à partir de l'application AWS Support et de la AWS Support Center Console. Votre canal n'est pas supprimé à partir de Slack.

Vous pouvez ajouter jusqu'à 20 canaux pour votre Compte AWS. Si vous avez déjà atteint ce quota, vous devez supprimer un canal avant de pouvoir en ajouter un autre.

Pour supprimer la configuration d'un canal Slack

1. Connectez-vous à Support Center Console (Console du centre de support) et choisissez Slack configuration (Configuration de Slack).
2. Sur la page Slack configuration (Configuration de Slack), sous Channels (Canaux), sélectionnez le nom du canal, puis Delete (Supprimer).
3. Dans la boîte de dialogue Delete channel name (Supprimer le nom du canal), cliquez sur Delete (Supprimer). Vous pouvez ajouter à nouveau ce canal à l'application AWS Support plus tard.



Suppression d'une configuration d'espace de travail Slack à partir de l'application AWS Support

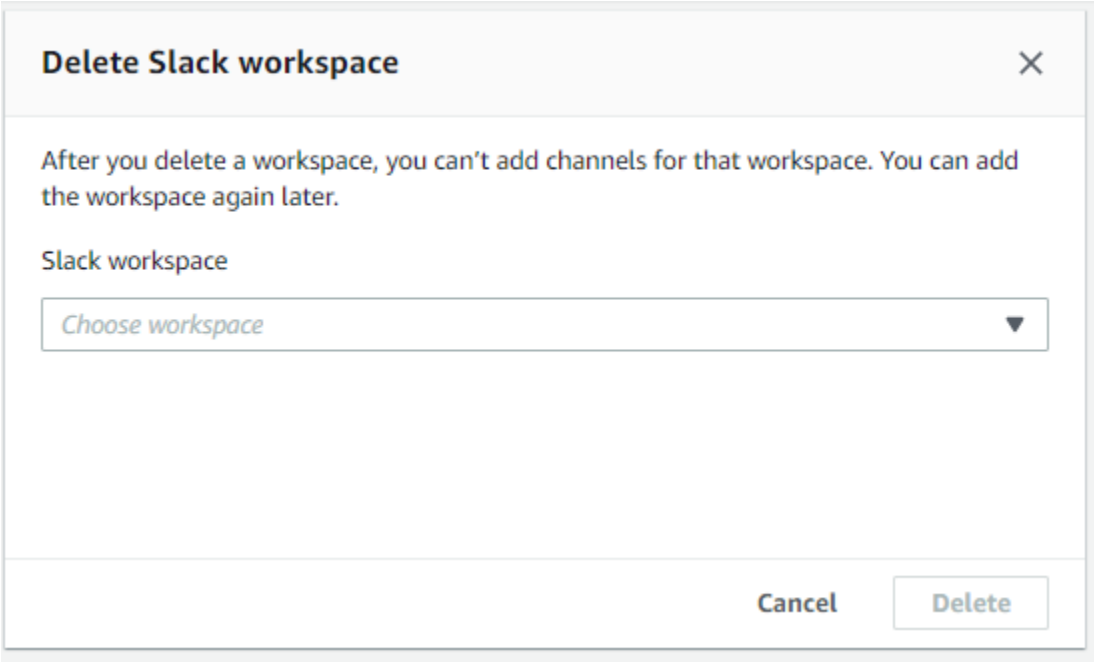
Vous pouvez supprimer une configuration d'espace de travail à partir de l'application AWS Support si vous n'en avez pas besoin. Cette action supprime uniquement l'espace de travail à partir de l'application AWS Support et de la AWS Support Center Console. Votre espace de travail n'est pas supprimé à partir de Slack.

Vous pouvez ajouter jusqu'à 5 espaces de travail pour votre Compte AWS. Si vous avez déjà atteint ce quota, vous devez supprimer un espace de travail Slack avant de pouvoir en ajouter un autre.

> **Note**
>
> Si vous avez ajouté des canaux de cet espace de travail à l'application AWS Support, vous devez d'abord supprimer ces canaux avant de pouvoir supprimer l'espace de travail. Consultez Suppression d'une configuration de canal Slack à partir de l'application AWS Support.

Pour supprimer la configuration d'un espace de travail Slack

1. Connectez-vous à la AWS Support Center Console et sélectionnez Slack configuration (Configuration de Slack).
2. Sur la page Slack configuration (Configuration de Slack), sous Slack workspaces (Espaces de travail Slack), sélectionnez Delete a workspace (Supprimer un espace de travail).
3. Dans la boîte de dialogue Delete Slack workspace (Supprimer l'espace de travail Slack), sélectionnez le nom de l'espace de travail Slack, puis cliquez sur Delete (Supprimer). Vous pouvez ajouter à nouveau l'espace de travail à votre Compte AWS plus tard.



Application AWS Support dans les commandes Slack

Commandes du canal Slack

Vous pouvez saisir les commandes suivantes dans le canal Slack où vous avez invité l'application AWS Support. Ce nom de canal Slack apparaît également comme un canal configuré dans l'application AWS Support Center Console.

`/awssupport create` ou `/awssupport create-case`

Créez un cas de support.

`/awssupport search` ou `/awssupport search-case`

Recherchez des cas. Vous pouvez rechercher des cas de support pour le Comptes AWS qui a configuré l'application AWS Support pour le même canal Slack.

`/awssupport quota` ou `/awssupport service-quota-increase`

Demandez une augmentation du quota de service.

Commandes du canal de chat en direct

Vous pouvez saisir les commandes suivantes dans le canal de chat en direct. Il s'agit du canal que l'application AWS Support crée pour vous lorsque vous choisissez un nouveau canal pour discuter avec AWS Support. Les canaux de chat incluent l'ID de votre cas de support, tel que *`awscase-1234567890`*.

> **Note**
>
> Les commandes suivantes ne sont pas disponibles lorsque vous utilisez un fil de discussion dans le canal actuel pour un chat en direct. Utilisez plutôt les boutons attachés au message du fil de discussion initial pour mettre fin à un chat, inviter un nouvel agent ou résoudre la demande de support.

`/awssupport endchat`

Supprimez l'agent de support et mettez fin à la session de chat en direct.

`/awssupport invite`

Invitez un nouvel agent de support à ce canal.

`/awssupport resolve`

Résolvez ce cas de support.

Afficher les correspondances de l'application AWS Support dans la AWS Support Center Console

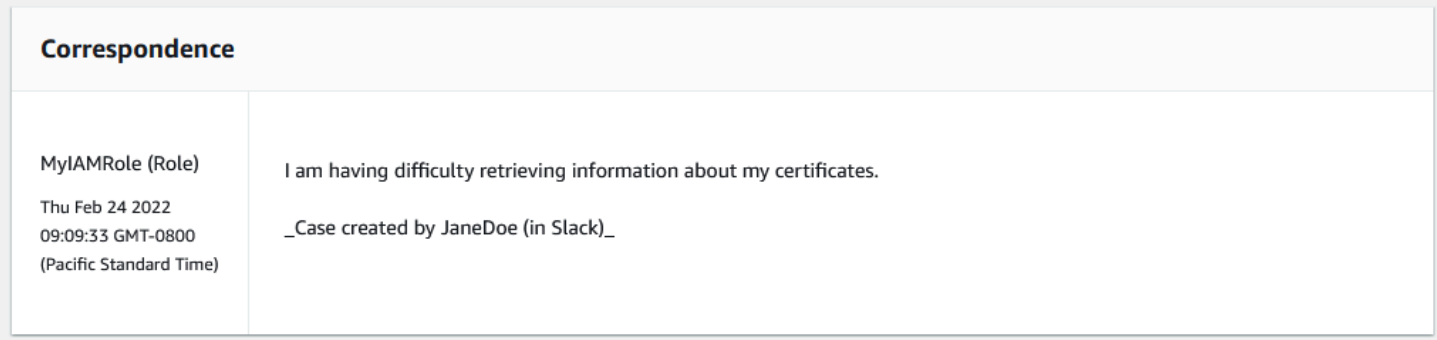
Lorsque vous créez, mettez à jour ou résolvez des cas de support pour votre compte dans le canal Slack, vous pouvez également vous connecter à la console du centre de support pour afficher vos cas. Vous pouvez afficher les correspondances du cas pour déterminer si le cas a été mis à jour dans le canal Slack, afficher l'historique du chat avec un agent de support et trouver toutes les pièces jointes que vous avez chargées depuis Slack.

Pour afficher les correspondances de cas à partir de Slack

1. Connectez-vous à la AWS Support Center Console de votre compte.
2. Sélectionnez votre cas de support.
3. Dans Correspondence (Correspondance), vous pouvez voir si le cas a été créé et mis à jour depuis le canal Slack.

Example : Cas de support

Dans la capture d'écran suivante, Jane Doe a rouvert un cas de support dans Slack. Cette correspondance apparaît pour le cas de support dans la console du centre de support.



Création d'une application AWS Support dans les ressources Slack avec AWS CloudFormation

L'application AWS Support dans Slack est intégrée à AWS CloudFormation, un service qui vous aide à modéliser et à configurer vos ressources AWS afin que vous puissiez consacrer moins de temps à la création et à la gestion de vos ressources et de votre infrastructure. Vous créez un modèle qui décrit toutes les ressources AWS que vous voulez (comme votre AccountAlias et SlackChannelConfiguration), et AWS CloudFormation fournit et configure ces ressources pour vous.

Lorsque vous utilisez AWS CloudFormation, vous pouvez réutiliser votre modèle pour configurer vos ressources de l'application AWS Support de manière cohérente et répétée. Décrivez vos ressources une seule fois, puis allouez-les autant de fois que vous le souhaitez dans plusieurs Comptes AWS et régions.

Application AWS Support et modèles AWS CloudFormation

Pour provisionner et configurer des ressources pour l'application AWS Support et les services associés, vous devez maîtriser les modèles AWS CloudFormation. Les modèles sont des fichiers texte formatés en JSON ou YAML. Ces modèles décrivent les ressources que vous souhaitez allouer dans vos piles AWS CloudFormation. Si JSON ou YAML ne vous est pas familier, vous pouvez utiliser AWS CloudFormation Designer pour vous aider à démarrer avec des modèles AWS CloudFormation. Pour plus d'informations, consultez Qu'est-ce que AWS CloudFormation Designer ? dans le AWS CloudFormationGuide de l'utilisateur.

L'application AWS Support prend en charge la création de votre AccountAlias et SlackChannelConfiguration dans AWS CloudFormation. Pour plus d'informations, y compris des exemples de modèles JSON et YAML pour les ressources AccountAlias et SlackChannelConfiguration, consultez la Référence du type de ressource de l'application AWS Support dans le Guide de l'utilisateur AWS CloudFormation.

Créez des ressources de configuration Slack pour votre organisation

Vous pouvez utiliser des modèles CloudFormation pour créer les ressources dont vous avez besoin pour l'application AWS Support. Si vous êtes en charge du compte de gestion pour votre organisation, vous pouvez utiliser les modèles pour créer ces ressources pour vos comptes membres dans AWS Organizations.

Par exemple, vous pouvez utiliser un modèle pour créer la même configuration d'espace de travail Slack pour tous les comptes de l'organisation, puis utiliser des modèles distincts pour créer

différentes configurations de canaux Slack pour des Comptes AWS ou des unités d'organisation (OU) spécifiques. Vous pouvez également utiliser un modèle pour créer une configuration d'espace de travail Slack afin que les comptes membres puissent ensuite configurer les canaux Slack qu'ils souhaitent pour leurs comptes Comptes AWS.

Vous pouvez choisir d'utiliser des modèles CloudFormation ou non. Si vous n'utilisez pas de modèles CloudFormation, vous pouvez effectuer les étapes manuelles suivantes à la place :

- Créez les ressources pour l'application AWS Support dans la AWS Support Center Console.
- Créez un dossier de support avec AWS Support pour autoriser plusieurs comptes à utiliser l'application AWS Support.
- Vous pouvez utiliser l'opération API RegisterSlackWorkspaceForOrganization pour enregistrer un espace de travail Slack pour votre compte. La pile CloudFormation appelle cette opération d'API pour vous.

Suivez ces procédures pour charger le modèle CloudFormation dans votre organisation. Vous pouvez utiliser les exemples de modèles de la page Référence des types de ressources d'application AWS Support (français non garanti).

Les modèles disent à CloudFormation de créer les ressources suivantes :

- Une configuration de canal Slack.
- Une configuration d'espace de travail Slack.
- Un rôle IAM portant le nom `AWSSupportSlackAppCFNRole`. La politique gérée par AWSSupportAppFullAccess AWS est attachée au rôle.

Table des matières

Mettre à jour vos modèles CloudFormation pour Slack

Pour commencer, utilisez les modèles suivants pour créer votre pile. Vous devez remplacer les modèles par des valeurs valides pour votre espace de travail et votre canal Slack.

> **Note**
>
> Nous ne recommandons pas l'utilisation du modèle pour créer une ressource AccountAlias pour votre organisation. La ressource AccountAlias identifie de manière unique un Compte AWS dans l'application AWS Support. Vos comptes membres peuvent saisir un nom de compte dans la Support Center Console. Pour de plus amples informations, veuillez consulter Autorisation d'un espace de travail Slack.

Pour mettre à jour vos modèles CloudFormation pour Slack

1. Si vous êtes en charge du compte de gestion pour une organisation, vous devez autoriser manuellement un espace de travail Slack pour votre compte avant que vos comptes membres puissent utiliser CloudFormation pour créer les ressources. Si vous ne l'avez pas déjà fait, consultez Autorisation d'un espace de travail Slack.
2. Sur la page Référence des types de ressources d'application AWS Support (français non garanti), copiez le modèle JSON ou YAML pour la ressource que vous souhaitez.
3. Dans un éditeur de texte, collez le modèle dans un nouveau fichier.
4. Dans le modèle, spécifiez les paramètres souhaités. Au minimum, remplacez les valeurs dans les champs suivants :

   - `TeamId` par votre ID d'espace de travail Slack
   - `ChannelId` par l'ID de canal Slack
   - `ChannelName` par un nom pour identifier la configuration du canal Slack

   > **Tip**
   >
   > Pour trouver les ID de l'espace de travail et du canal, ouvrez votre canal Slack dans un navigateur. Dans l'URL, l'ID de votre espace de travail est le premier identifiant et l'ID du canal est le second. Par exemple, dans https://app.slack.com/client/T012ABCDEFG/C01234A5BCD, T012ABCDEFG est l'ID de l'espace de travail et C01234A5BCD est l'ID du canal.

5. Enregistrez le fichier JSON ou YAML.

Créer une pile pour le compte de gestion

Ensuite, vous devez créer une pile pour le compte de gestion de l'organisation. Cette étape appelle l'opération d'API RegisterSlackWorkspaceForOrganization pour vous et autorise l'espace de travail avec Slack.

> **Note**
>
> Nous vous recommandons de charger le modèle de configuration de l'espace de travail Slack que vous avez mis à jour lors de la procédure précédente pour le compte de gestion. Vous n'avez pas besoin de charger le modèle de configuration de canal Slack, sauf si vous configurez également le compte de gestion pour utiliser l'application AWS Support.

Pour créer une pile pour le compte de gestion

1. Connectez-vous à la AWS Management Console en utilisant le compte de gestion de votre organisation.
2. Ouvrez la console AWS CloudFormation à l'adresse https://console.aws.amazon.com/cloudformation.
3. Si vous ne l'avez pas déjà fait, dans le sélecteur de région, choisissez l'une des Régions AWS suivantes :
   - Europe (Francfort)
   - Europe (Irlande)
   - Europe (Londres)
   - USA Est (Virginie du Nord)
   - USA Est (Ohio)
   - US West (Oregon)
   - Asie-Pacifique (Singapour)
   - Asie Pacifique (Tokyo)
   - Canada (Centre)
4. Suivez la procédure ci-dessous pour créer une pile: Pour de plus amples informations, consultez Création d'une pile sur la console AWS CloudFormation.

Une fois que CloudFormation crée la pile avec succès, vous pouvez utiliser le même modèle pour créer une pile pour votre organisation.

Créer un ensemble de piles pour votre organisation

Ensuite, utilisez le même modèle pour la configuration de l'espace de travail Slack afin de créer un ensemble de piles avec des autorisations `service-managed`. Vous pouvez utiliser des ensembles de piles pour créer la pile pour toute votre organisation ou spécifier les unités d'organisation souhaitées. Pour plus d'informations, consultez Créer un ensemble de piles.

Cette procédure appelle également l'opération d'API RegisterSlackWorkspaceForOrganization pour vous. Cette opération d'API autorise l'espace de travail avec Slack pour les comptes membres.

Pour créer un ensemble de piles pour votre organisation

1. Connectez-vous à la AWS Management Console en utilisant le compte de gestion de votre organisation.
2. Ouvrez la console AWS CloudFormation à l'adresse https://console.aws.amazon.com/cloudformation.
3. Si vous ne l'avez pas déjà fait, dans le sélecteur de région, choisissez la même Région AWS que celle que vous avez utilisée dans la procédure précédente.
4. Choisissez StackSets dans le volet de navigation.
5. Choisissez Create StackSet (Créer un StackSet).
6. Sur la page Choose a template (Choisir un modèle), conservez les options par défaut pour les options suivantes :
   - Sous Permissions (Autorisations), conservez Service-managed permissions (Autorisations gérées par le service).
   - Pour Prerequisite - Prepare template (Conditions préalables – Préparer le modèle), conservez Template is ready (Le modèle est prêt).
7. Pour Specify template (Spécifier un modèle), choisissez Upload a template file (Télécharger un fichier de modèle), puis choisissez Choose file (Choisir un fichier).
8. Choisissez votre fichier YAML, puis sélectionnez Next (Suivant).
9. Sur la page Specify StackSet details (Spécifier les détails du StackSet), saisissez un nom pour la pile, tel que **`support-app-slack-workspace`** et choisissez Next (Suivant).

10. Dans la page Configure StackSet options (Configurer les options de StackSet), conservez les options par défaut et choisissez Next (Suivant).
11. Sur la page Set deployment options (Définir les options de déploiement), pour Add stacks to stack set (Ajouter des piles à l'ensemble de piles), conservez l'option par défaut Deploy new stacks (Déployer de nouvelles piles).
12. Pour les Deployment targets (Cibles de déploiement), choisissez si vous souhaitez créer la pile pour l'ensemble de l'organisation ou pour des unités d'organisation spécifiques. Si vous choisissez une unité d'organisation, entrez l'ID de l'OU.
13. Pour Specify regions (Spécifier les régions), saisissez uniquement l'une des valeurs suivantesRégions AWS :

    - Europe (Francfort)
    - Europe (Irlande)
    - Europe (Londres)
    - USA Est (Virginie du Nord)
    - USA Est (Ohio)
    - US West (Oregon)
    - Asie-Pacifique (Singapour)
    - Asie Pacifique (Tokyo)
    - Canada (Centre)

    > Remarques :
    >
    > - Pour rationaliser votre flux de travail, nous vous recommandons d'utiliser la même Région AWS que celle choisie à l'étape 3.
    > - Choisir plusieurs Région AWS peut entraîner des conflits lors de la création de votre pile.

14. Pour Deployment options (Options de déploiement), dans Failure tolerance - optional (Tolérance aux pannes - facultatif), entrez le nombre de comptes sur lesquels les piles peuvent échouer avant que CloudFormation n'arrête l'opération. Nous vous recommandons de saisir le nombre de comptes que vous souhaitez ajouter, moins un. Par exemple, si l'unité d'organisation que vous avez spécifiée a 10 comptes membres, entrez 9. Cela signifie que même si CloudFormation échoue 9 fois, au moins un compte réussira.

15. Choisissez Next (Suivant).
16. Sur la page Review (Vérification), vérifiez vos choix et choisissez Submit (Soumettre). Vous pouvez vérifier l'état de votre pile dans l'onglet Instances de pile.
17. (Facultatif) Répétez cette procédure pour charger un modèle de configuration de canal Slack. L'exemple de modèle crée également le rôle IAM et associe une politique gérée par AWS. Ce rôle possède les autorisations requises pour accéder à d'autres services pour vous. Pour de plus amples informations, veuillez consulter Gestion de l'accès à l'application AWS Support.

    Si vous ne créez pas d'ensemble de piles pour créer la configuration du canal Slack, vos comptes membres peuvent configurer manuellement le canal Slack. Pour de plus amples informations, veuillez consulter Configuration d'un canal Slack.

Une fois que CloudFormation crée les piles, chaque compte membre peut se connecter et accéder à la Support Center Console et trouver les espaces de travail et les canaux Slack qu'ils ont configurés. Ils peuvent ensuite utiliser l'application AWS Support pour leur Compte AWS. Consultez Création de cas de support dans un canal Slack.

> **Tip**
>
> Si vous devez charger un nouveau modèle, nous vous recommandons d'utiliser la même Région AWS que celle spécifiée précédemment.

En savoir plus sur CloudFormation

Pour en savoir plus sur AWS CloudFormation, consultez les ressources suivantes :

- AWS CloudFormation
- Guide de l'utilisateur AWS CloudFormation
- Référence API AWS CloudFormation
- Guide de l'utilisateur de l'interface de ligne de commande AWS CloudFormation

Créer des ressources de l'application AWS Support à l'aide de Terraform (français non garanti)

Vous pouvez également utiliser Terraform pour créer les ressources de l'application AWS Support pour votre Compte AWS. Terraform est un outil d'infrastructure en tant que code que vous pouvez utiliser pour vos applications cloud. Vous pouvez utiliser Terraform pour créer des ressources de l'application AWS Support au lieu de déployer une pile CloudFormation sur un compte.

Après avoir installé Terraform, vous pouvez spécifier les ressources de l'application AWS Support souhaitées. Terraform appelle l'opération d'API RegisterSlackWorkspaceForOrganization pour enregistrer un espace de travail Slack pour vous et créer vos ressources. Vous pouvez ensuite vous connecter à la Support Center Console et rechercher les espaces de travail et les canaux Slack que vous avez configurés.

Remarques

- Si vous êtes en charge du compte de gestion pour une organisation, vous devez autoriser manuellement un espace de travail Slack pour votre compte avant que vos comptes membres puissent utiliser Terraform pour créer les ressources. Si vous ne l'avez pas déjà fait, consultez Autorisation d'un espace de travail Slack.
- Contrairement aux ensembles de piles CloudFormation, vous ne pouvez pas utiliser Terraform pour créer les ressources de l'application AWS Support pour une unité d'organisation au sein de votre organisation.
- Vous pouvez également trouver l'historique des événements relatifs à ces mises à jour de Terraform dans AWS CloudTrail. Les `eventSource` pour ces événements seront `cloudcontrolapi.amazonaws.com` et `supportapp.amazonaws.com`. Pour de plus amples informations, veuillez consulter Journalisation des appels d'API de l'application AWS Support dans Slack à l'aide de AWS CloudTrail.

En savoir plus

Pour en savoir plus sur Terraform, consultez les rubriques suivantes :

- Installation de Terraform
- Tutoriel Terraform : Créez une infrastructure pour AWS
- `awscc_support_app_account_alias`

- awscc_supportapp_slack_workspace_configuration
- awscc_supportapp_slack_channel_configuration

Sécurité dans AWS Support

La sécurité du cloud AWS est la priorité absolue. En tant que AWS client, vous bénéficiez d'un centre de données et d'une architecture 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 AWS cadre des programmes de de). Pour en savoir plus sur les programmes de conformité applicables à AWS Support, consultez la section AWS Services concernés par programme de conformité .
- Sécurité dans le cloud — Votre responsabilité est déterminée par le AWS service que vous utilisez. Vous êtes également responsable d'autres facteurs, y compris de la sensibilité de vos données, des exigences de votre entreprise, ainsi que de la législation et de la réglementation applicables.

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

Rubriques

Protection des données dans AWS Support

Le modèle de responsabilité AWS partagée de s'applique à la protection des données dans AWS Support. Comme décrit dans ce modèle, AWS est chargé de protéger l'infrastructure mondiale qui gère tous les AWS Cloud. La gestion du contrôle de votre contenu hébergé sur cette infrastructure relève de votre responsabilité. Vous êtes également responsable des tâches de configuration et de gestion de la sécurité des Services AWS que vous utilisez. Pour en savoir plus sur la confidentialité des données, consultez Questions fréquentes (FAQ) sur la confidentialité des données. Pour en savoir plus sur la protection des données en Europe, consultez le billet de blog Modèle de responsabilité partagée AWS et RGPD (Règlement général sur la protection des données) sur le Blog de sécuritéAWS .

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

- Utilisez l’authentification multifactorielle (MFA) avec chaque compte.
- Utilisez le protocole SSL/TLS pour communiquer avec les ressources. AWS Nous exigeons TLS 1.2 et recommandons TLS 1.3.
- Configurez l'API et la journalisation de l'activité des utilisateurs avec AWS CloudTrail.
- 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 140-2 pour accéder AWS via une interface de ligne de commande ou une API, utilisez un point de terminaison FIPS. Pour en savoir plus sur les points de terminaison FIPS (Federal Information Processing Standard) disponibles, consultez Federal Information Processing Standard (FIPS) 140-2 (Normes de traitement de l’information fédérale).

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 Name (Nom). Cela inclut lorsque vous travaillez avec AWS Support ou d'autres Services AWS utilisateurs de la console, de l'API ou AWS des SDK. AWS CLI Toutes les données que vous

saisissez 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.

Sécurité pour vos AWS Support affaires

Lorsque vous créez un dossier d'assistance, vous êtes propriétaire des informations que vous incluez dans votre dossier d'assistance. AWS n'accède pas à vos Compte AWS données sans votre autorisation. AWS ne partage pas vos informations avec des tiers.

Lorsque vous créez un cas de support, notez ce qui suit :

- AWS Support utilise les autorisations définies dans le rôle `AWSServiceRoleForSupport` lié au service pour appeler d'autres personnes chargées de résoudre Services AWS les problèmes des clients à votre place. Pour plus d'informations, voir Utilisation de rôles liés à un service pour AWS Support et politique AWS gérée :. AWSSupportServiceRolePolicy
- Vous pouvez consulter les appels d'API AWS Support qui se sont produits dans votre Compte AWS. Par exemple, vous pouvez afficher les informations du journal lorsqu'une personne de votre compte crée ou résout un cas de support. Pour plus d'informations, consultez la section Journalisation des appels d' AWS Support API avec AWS CloudTrail.
- Vous pouvez utiliser l' AWS Support API pour appeler l'`DescribeCases`API. Cette API renvoie des informations sur les cas de support, telles que l'ID du cas, la date de création et de résolution, et les correspondances avec l'agent de support. Vous pouvez afficher les détails du cas jusqu'à 12 mois après sa création. Pour plus d'informations, consultez DescribeCasesla référence de AWS Support l'API.
- Vos cas de support suivent la validation de conformité pour AWS Support.
- Lorsque vous créez un dossier d'assistance, AWS il n'a pas accès à votre compte. Si nécessaire, les agents de support utilisent un outil de partage d'écran pour visualiser votre écran à distance et identifier et résoudre les problèmes. Cet outil est en mode visualisation seulement. AWS Support ne peut pas agir pour vous pendant la session de partage d'écran. Vous devez donner votre consentement pour partager un écran avec un agent de support. Pour plus d'informations, consultez la FAQ AWS Support.
- Vous pouvez modifier votre AWS Support forfait pour obtenir l'aide dont vous avez besoin pour votre compte. Pour plus d'informations, voir Comparer AWS Support les forfaits et Modifier votre AWS Support forfait.

Gestion des identités et des accès pour AWS Support

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 Support 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 Support

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

Administrateur du service — Si vous êtes responsable des AWS Support ressources de votre entreprise, vous avez probablement un accès complet à AWS Support. C'est à vous de déterminer les AWS Support 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 Support, voirComment AWS Support 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 Support. Pour consulter des exemples de politiques AWS Support basées sur l'identité que vous pouvez utiliser dans IAM, consultez. AWS Support 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 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 vous-même les demandes, consultez la section Signature des demandes AWS 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 en savoir plus, veuillez consulter Multi-factor authentication (Authentification multifactorielle) dans le Guide de l'utilisateur AWS IAM Identity Center et Utilisation de l'authentification multifactorielle (MFA) dans l'interface AWS 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 root, consultez Tâches nécessitant les informations d'identification de l'utilisateur root 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 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 tels que les 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 de faire pivoter les 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 avoir un groupe nommé IAMAdmins et accorder à ce groupe les autorisations d'administrer des 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 en savoir plus, consultez Quand créer un utilisateur IAM (au lieu d'un rôle) 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. Vous pouvez assumer temporairement un rôle IAM dans le en AWS Management Console changeant de rôle. 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 Utilisation de rôles IAM 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, veuillez consulter la rubrique 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 Différence entre les rôles IAM et les politiques basées sur les ressources 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, une fonction 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 la politique relative à la transmission de demandes FAS, consultez Sessions de transmission d'accès.
- Fonction du 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 une fonction du 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 instance EC2 et qui envoient des demandes d'API. AWS CLI AWS Cette solution est préférable au stockage des clés d'accès au sein de l'instance EC2. Pour attribuer un AWS rôle à une instance EC2 et le mettre à la disposition de 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 qui s'exécutent sur l'instance EC2 d'obtenir des informations d'identification temporaires. Pour plus d'informations, consultez Utilisation d'un rôle IAM pour accorder des autorisations à des applications s'exécutant sur des instances Amazon EC2 dans le Guide de l'utilisateur IAM.

Pour savoir dans quel cas utiliser des rôles ou des utilisateurs IAM, consultez Quand créer un rôle IAM (au lieu d'un utilisateur) 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 Présentation 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 Création de politiques IAM 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, veuillez consulter Choix entre les politiques gérées et les politiques en ligne dans le Guide de l'utilisateur IAM.

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 fonction 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 qui en résultent 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 remplace 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 (SCP) — Les SCP sont des 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 fonctions d'une organisation, vous pouvez appliquer les politiques de contrôle des services (SCP) 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 organisations et les SCP, consultez Fonctionnement des SCP dans le Guide de l'utilisateur AWS Organizations .
- Politiques de séance – Les politiques de séance sont des politiques avancées que vous passez en tant que paramètre lorsque vous programmez afin de créer une séance temporaire pour un rôle ou un utilisateur fédéré. Les autorisations de la séance obtenue 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 remplace l'autorisation. Pour plus d'informations, consultez Politiques de séance dans le Guide de l'utilisateur IAM.

Plusieurs types de politique

Lorsque plusieurs types de politiques s'appliquent à la requête, les autorisations obtenues 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 Support fonctionne avec IAM

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

Pour plus d'informations sur la façon de gérer l'accès à AWS Support l'aide d'IAM, voir Gérer l'accès pour AWS Support.

Rubriques

- Politiques basées sur l'identitéAWS Support
- AWS Support Rôles IAM

Politiques basées sur l'identitéAWS Support

Avec les politiques basées sur une 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 Support prend en charge des actions spécifiques. Pour en savoir plus sur les éléments que vous utilisez dans une politique JSON, veuillez consulter 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 stratégie afin d’accorder l’autorisation d’exécuter les opérations associées.

Les actions de politique en AWS Support cours utilisent le préfixe suivant avant l'action :`support:`. Par exemple, pour accorder à une personne l'autorisation d'exécuter une instance Amazon EC2 avec l'opération d'API `RunInstances` Amazon EC2, vous incluez l'action `ec2:RunInstances` dans sa politique. Les déclarations de politique doivent inclure un élément `Action` ou `NotAction`. AWS Support définit son propre ensemble d'actions qui décrivent les tâches que vous pouvez effectuer avec ce service.

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

```
"Action": [
      "ec2:action1",
      "ec2:action2"
```

Vous pouvez aussi spécifier 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": "ec2:Describe*"
```

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

Exemples

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

AWS Support Rôles IAM

Un rôle IAM est une entité de votre AWS compte qui possède des autorisations spécifiques.

Utilisation d'informations d'identification temporaires avec AWS Support

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 Support 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 Support prend en charge les rôles liés aux services. Pour plus de détails sur la création ou la gestion des rôles AWS Support liés à un service, consultez. Utilisation des rôles liés aux services pour AWS Support

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 fonctions du 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 Support prend en charge les rôles de service.

AWS Support 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 Support . 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 apprendre à créer une politique basée sur l'identité IAM à l'aide de ces exemples de documents de politique JSON, veuillez consulter Création de politiques dans l'onglet JSON dans le Guide de l'utilisateur IAM.

Rubriques

- Bonnes pratiques en matière de politiques
- Utilisation de la console AWS Support

- Autorisation accordée aux utilisateurs pour afficher leurs propres autorisations

Bonnes pratiques en matière de politiques

Les politiques basées sur l'identité sont très puissantes. Ils déterminent si quelqu'un peut créer, accéder ou supprimer AWS Support des ressources dans votre compte. Lorsque vous créez ou modifiez des politiques basées sur l'identité, suivez ces instructions et recommandations :

- Commencez à utiliser les politiques AWS gérées — Pour commencer à les utiliser AWS Support rapidement, utilisez des politiques AWS gérées pour donner à vos employés les autorisations dont ils ont besoin. Ces politiques sont déjà disponibles dans votre compte et sont gérées et mises à jour par AWS. Pour plus d'informations, voir Commencer à utiliser les autorisations avec les politiques AWS gérées dans le Guide de l'utilisateur IAM.
- Accorder le privilège le plus faible : Lorsque vous créez des politiques personnalisées, accordez uniquement les autorisations requises pour exécuter une seule tâche. Commencez avec un ensemble d'autorisations minimum et accordez-en d'autres si nécessaire. Cette méthode est plus sûre que de commencer avec des autorisations trop permissives et d'essayer de les restreindre plus tard. Pour plus d'informations, consultez Accorder le moindre privilège possible dans le Guide de l'utilisateur IAM.
- Activer MFA pour les opérations sensibles – Pour plus de sécurité, obligez les utilisateurs IAM à utiliser l'authentification multi-facteurs (MFA) pour accéder à des ressources ou à des opérations d'API sensibles. Pour plus d'informations, consultez Utilisation de l'authentification multifacteur (MFA) dans AWS dans le Guide de l'utilisateur IAM.
- Utiliser des conditions de politique pour une plus grande sécurité : tant que cela reste pratique pour vous, définissez les conditions dans lesquelles vos politiques basées sur l'identité autorisent l'accès à une ressource. Par exemple, vous pouvez rédiger les conditions pour spécifier une plage d'adresses IP autorisées d'où peut provenir une demande. Vous pouvez également écrire des conditions pour autoriser les requêtes uniquement à une date ou dans une plage de temps spécifiée, ou pour imposer l'utilisation de SSL ou de MFA. Pour plus d'informations, veuillez consulter Conditions pour éléments de politique JSON IAM dans le Guide de l'utilisateur IAM.

Utilisation de la console AWS Support

Pour accéder à la AWS Support console, vous devez disposer d'un ensemble minimal d'autorisations. Ces autorisations doivent vous permettre de répertorier et d'afficher les informations relatives AWS Support 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 vous assurer que ces entités peuvent toujours utiliser la AWS Support console, associez également la politique AWS gérée suivante aux entités. Pour plus d'informations, veuillez consulter Ajout d'autorisations à un utilisateur dans le Guide de l'utilisateur IAM.

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.

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": "*"
        }
    ]
}
```

Utilisation des rôles liés à un service

AWS Support et AWS Trusted Advisor utilisez des rôles AWS Identity and Access Management liés à un service (IAM). Un rôle lié à un service est un rôle IAM unique directement lié à et. AWS Support Trusted Advisor Dans chaque cas, le rôle lié à un service est un rôle prédéfini. Ce rôle inclut toutes les autorisations nécessaires AWS Support ou Trusted Advisor nécessaires pour appeler d'autres AWS services en votre nom. Les rubriques suivantes expliquent à quoi servent les rôles liés aux services et comment les utiliser dans AWS Support et. Trusted Advisor

Rubriques

- Utilisation des rôles liés aux services pour AWS Support
- Utilisation des rôles liés aux services pour Trusted Advisor

Utilisation des rôles liés aux services pour AWS Support

AWS Support les outils collectent des informations sur vos AWS ressources par le biais d'appels d'API pour fournir un service client et un support technique. Pour accroître la transparence et l'auditabilité des activités de support, AWS Support utilise un rôle lié au service AWS Identity and Access Management (IAM).

Le rôle `AWSServiceRoleForSupport` lié à un service est un rôle IAM unique directement lié à. AWS Support Ce rôle lié au service est prédéfini et inclut les autorisations nécessaires pour appeler AWS Support d'autres AWS services en votre nom.

Le rôle lié à un service `AWSServiceRoleForSupport` fait confiance au service `support.amazonaws.com` pour endosser le rôle.

Pour fournir ces services, les autorisations prédéfinies du rôle donnent AWS Support accès aux métadonnées des ressources, et non aux données des clients. Seuls AWS Support les outils peuvent assumer ce rôle, qui existe au sein de votre AWS compte.

Nous rédigeons des champs qui peuvent contenir des données des clients. Par exemple, les `Output` champs `Input` et de l'GetExecutionHistoryappel d' AWS Step Functions API ne sont pas visibles pour AWS Support. Nous utilisons AWS KMS keys pour chiffrer les champs sensibles. Ces champs sont expurgés dans la réponse de l'API et ne sont pas visibles pour les AWS Support agents.

> **Note**
>
> AWS Trusted Advisor utilise un rôle distinct lié au service IAM pour accéder aux AWS ressources de votre compte afin de fournir des recommandations et des vérifications relatives aux meilleures pratiques. Pour plus d'informations, consultez Utilisation des rôles liés aux services pour Trusted Advisor.

Le rôle `AWSServiceRoleForSupport` lié au service permet aux clients d'accéder à tous les appels d' AWS Support API. AWS CloudTrail Cela permet de répondre aux exigences de surveillance et d'audit, car cela fournit un moyen transparent de comprendre les actions AWS Support effectuées en votre nom. Pour plus d'informations CloudTrail, consultez le guide de AWS CloudTrail l'utilisateur.

Autorisations des rôles liés à un service pour AWS Support

Ce rôle utilise la politique `AWSSupportServiceRolePolicy` AWS gérée. Cette politique gérée est attachée au rôle et permet au rôle d'autoriser à effectuer des actions en votre nom.

Ces actions incluent ce qui suit :

- Facturation, administration, support et autres services clients : le service AWS client utilise les autorisations accordées par la politique gérée pour effectuer un certain nombre de services dans le cadre de votre plan de support. Il s'agit notamment d'étudier et de répondre aux questions relatives aux comptes et à la facturation, de fournir un support administratif pour votre compte, d'augmenter les quotas de service et d'offrir un service clientèle supplémentaire.
- Traitement des attributs de service et des données d'utilisation de votre AWS compte : les autorisations accordées par la politique gérée AWS Support peuvent être utilisées pour accéder aux attributs de service et aux données d'utilisation de votre AWS compte. Cette politique permet AWS Support de fournir un support technique, administratif et de facturation pour votre compte. Les attributs de service incluent les identificateurs de ressource de votre compte, les balises de métadonnées, les rôles et les autorisations. L'utilisation des données inclut des politiques d'utilisation ainsi que des statistiques et des analyses de l'utilisation.

- Maintien de la santé opérationnelle de votre compte et de ses ressources : AWS Support utilise des outils automatisés pour effectuer des actions liées au support opérationnel et technique.

Pour plus d'informations sur les services et les actions autorisés, consultez la politique AWSSupportServiceRolePolicy dans la console IAM.

> **Note**
>
> AWS Support met automatiquement à jour la `AWSSupportServiceRolePolicy` politique une fois par mois pour ajouter des autorisations pour de nouveaux AWS services et actions.

Pour plus d'informations, consultez AWS politiques gérées pour AWS Support.

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

Vous n'avez pas besoin de créer manuellement le rôle lié à un service `AWSServiceRoleForSupport`. Lorsque vous créez un AWS compte, ce rôle est automatiquement créé et configuré pour vous.

> **Important**
>
> Si vous l'avez utilisé AWS Support avant qu'il ne commence à prendre en charge les rôles liés à un service, vous avez AWS créé le `AWSServiceRoleForSupport` rôle dans votre compte. Pour plus d'informations, consultez Un nouveau rôle est apparu dans mon compte IAM.

Modification et suppression d'un rôle lié à un service pour AWS Support

Vous pouvez utiliser IAM pour modifier la description du rôle lié à un service `AWSServiceRoleForSupport`. Pour plus d'informations, consultez Modification d'un rôle lié à un service dans le Guide de l'utilisateur IAM.

Le `AWSServiceRoleForSupport` rôle est nécessaire AWS Support pour fournir un support administratif, opérationnel et technique pour votre compte. Par conséquent, ce rôle ne peut pas être supprimé via la console IAM, l'API ou AWS Command Line Interface (AWS CLI). Cela protège votre compte AWS , car vous ne pouvez pas supprimer par inadvertance les autorisations nécessaires à l'administration des services de support.

Pour plus d'informations sur le rôle `AWSServiceRoleForSupport` ou ses utilisations, contactez AWS Support.

Utilisation des rôles liés aux services pour Trusted Advisor

AWS Trusted Advisor utilise le rôle AWS Identity and Access Management lié au service (IAM). Un rôle lié à un service est un rôle IAM unique directement lié à. AWS Trusted Advisor Les rôles liés au service sont prédéfinis par Trusted Advisor et incluent toutes les autorisations dont le service a besoin pour appeler d'autres AWS services en votre nom. Trusted Advisor utilise ce rôle pour vérifier votre utilisation globale AWS et pour fournir des recommandations visant à améliorer votre AWS environnement. Par exemple, Trusted Advisor analyse l'utilisation de votre instance Amazon Elastic Compute Cloud (Amazon EC2) pour vous aider à réduire les coûts, à améliorer les performances, à tolérer les défaillances et à améliorer la sécurité.

> **Note**
>
> AWS Support utilise un rôle distinct lié au service IAM pour accéder aux ressources de votre compte afin de fournir des services de facturation, d'administration et de support. Pour plus d'informations, consultez Utilisation des rôles liés aux services pour AWS Support.

Pour obtenir des informations sur les autres services qui prennent en charge les rôles liés à un service, consultez Services AWS qui fonctionnent avec IAM. Recherchez les services qui comportent un Oui dans la colonne Rôle lié à un service. Choisissez un Oui ayant un lien pour consulter la documentation du rôle lié à un service, pour ce service.

Rubriques

- Autorisations des rôles liés à un service pour Trusted Advisor
- Gérer les autorisations de rôles liés à un service
- Création d'un rôle lié à un service pour Trusted Advisor
- Modification d'un rôle lié à un service pour Trusted Advisor
- Suppression d'un rôle lié à un service pour Trusted Advisor

Autorisations des rôles liés à un service pour Trusted Advisor

Trusted Advisor utilise deux rôles liés à un service :

- AWSServiceRoleForTrustedAdvisor— Ce rôle fait confiance au Trusted Advisor service pour assumer le rôle d'accéder aux AWS services en votre nom. La politique d'autorisation des rôles autorise l'accès Trusted Advisor en lecture seule à toutes AWS les ressources. Ce rôle simplifie la prise en main de votre AWS compte, car vous n'avez pas à ajouter les autorisations nécessaires pour Trusted Advisor. Lorsque vous ouvrez un AWS compte, Trusted Advisor crée ce rôle pour vous. Les autorisations définies comprennent la politique d'approbation et la politique d'autorisations. Vous ne pouvez pas attacher la politique d'autorisations à une autre entité IAM.

  Pour plus d'informations sur la politique ci-jointe, consultez AWSTrustedAdvisorServiceRolePolicy.
- AWSServiceRoleForTrustedAdvisorReporting : Ce rôle approuve le service Trusted Advisor pour assumer le rôle de la fonctionnalité de vue organisationnelle. Ce Trusted Advisor rôle constitue un service fiable au sein de votre AWS Organizations organisation. Trusted Advisor crée ce rôle pour vous lorsque vous activez la vue organisationnelle.

  Pour plus d'informations sur la politique attachée, consultez AWSTrustedAdvisorReportingServiceRolePolicy.

  Vous pouvez utiliser la vue organisationnelle pour créer des rapports contenant les résultats des Trusted Advisor vérifications pour tous les comptes de votre organisation. Pour en savoir plus sur cette fonction, consultez Vue organisationnelle pour AWS Trusted Advisor.

Gérer les autorisations de rôles liés à un service

Vous devez configurer les autorisations de manière à permettre à une entité IAM (comme un utilisateur, un groupe ou un rôle) de créer, modifier ou supprimer un rôle lié à un service. Les exemples suivants utilisent le rôle lié à un service `AWSServiceRoleForTrustedAdvisor`.

Example : Pour permettre à une entité IAM de créer le rôle lié à un service **`AWSServiceRoleForTrustedAdvisor`**

Cette étape n'est nécessaire que si le Trusted Advisor compte est désactivé, si le rôle lié au service est supprimé et si l'utilisateur doit recréer le rôle pour le réactiver. Trusted Advisor

Vous pouvez ajouter l'instruction suivante à la politique d'autorisations de l'entité IAM pour créer le rôle lié à un service.

```
{
    "Effect": "Allow",
    "Action": [
```

```
        "iam:CreateServiceLinkedRole",
        "iam:PutRolePolicy"
    ],
    "Resource": "arn:aws:iam::*:role/aws-service-role/trustedadvisor.amazonaws.com/
AWSServiceRoleForTrustedAdvisor*",
    "Condition": {"StringLike": {"iam:AWSServiceName": "trustedadvisor.amazonaws.com"}}
}
```

Example : Pour permettre à une entité IAM de modifier la description du rôle lié à un service **`AWSServiceRoleForTrustedAdvisor`**

Vous ne pouvez modifier que la description pour le rôle `AWSServiceRoleForTrustedAdvisor`. Vous pouvez ajouter l'instruction suivante à la politique d'autorisations de l'entité IAM pour modifier la description d'un rôle lié à un service.

```
{
    "Effect": "Allow",
    "Action": [
        "iam:UpdateRoleDescription"
    ],
    "Resource": "arn:aws:iam::*:role/aws-service-role/trustedadvisor.amazonaws.com/
AWSServiceRoleForTrustedAdvisor*",
    "Condition": {"StringLike": {"iam:AWSServiceName": "trustedadvisor.amazonaws.com"}}
}
```

Example : Pour permettre à une entité IAM de supprimer le rôle lié à un service **`AWSServiceRoleForTrustedAdvisor`**

Vous pouvez ajouter l'instruction suivante à la politique d'autorisations de l'entité IAM pour supprimer un rôle lié à un service.

```
{
    "Effect": "Allow",
    "Action": [
        "iam:DeleteServiceLinkedRole",
        "iam:GetServiceLinkedRoleDeletionStatus"
    ],
    "Resource": "arn:aws:iam::*:role/aws-service-role/trustedadvisor.amazonaws.com/
AWSServiceRoleForTrustedAdvisor*",
    "Condition": {"StringLike": {"iam:AWSServiceName": "trustedadvisor.amazonaws.com"}}
}
```

Vous pouvez également utiliser une politique AWS gérée, par exemple AdministratorAccesspour fournir un accès complet à Trusted Advisor.

Création d'un rôle lié à un service pour Trusted Advisor

Vous n'avez pas besoin de créer manuellement un rôle lié au service `AWSServiceRoleForTrustedAdvisor`. Lorsque vous ouvrez un AWS compte, il Trusted Advisor crée pour vous le rôle lié au service.

> **Important**
>
> Si vous utilisiez le Trusted Advisor service avant qu'il ne commence à prendre en charge les rôles liés au service, vous avez Trusted Advisor déjà créé le `AWSServiceRoleForTrustedAdvisor` rôle dans votre compte. Pour plus d'informations, consultez Un nouveau rôle est apparu dans mon compte IAM dans le Guide de l'utilisateur IAM.

Si votre compte ne comporte pas de rôle lié à un service `AWSServiceRoleForTrustedAdvisor`, alors Trusted Advisor ne fonctionnera pas comme prévu. Cela peut se produire si un utilisateur de votre compte a désactivé Trusted Advisor puis a supprimé le rôle lié au service. Dans ce cas, vous pouvez utiliser IAM pour créer le rôle lié à un service `AWSServiceRoleForTrustedAdvisor`, puis réactiver Trusted Advisor.

Pour activer Trusted Advisor (console)

1. Utilisez la console IAM ou l'API IAM pour créer un rôle lié à un service pour. AWS CLI Trusted Advisor Pour plus d'informations, consultez Création d'un rôle lié à un service.
2. Connectez-vous au AWS Management Console, puis accédez à la Trusted Advisor console à l'adressehttps://console.aws.amazon.com/trustedadvisor.

   La bannière d'état Disabled Trusted Advisor (Trusted Advisor désactivé) s'affiche dans la console.
3. Choisissez Activer Trusted Advisor le rôle dans la bannière d'état. Si le `AWSServiceRoleForTrustedAdvisor` obligatoire n'est pas détecté, la bannière d'état Disabled (Désactivé) reste affichée.

Modification d'un rôle lié à un service pour Trusted Advisor

Vous ne pouvez pas modifier le nom du rôle car diverses entités pourraient y faire référence. Vous pouvez toutefois utiliser la console IAM ou AWS CLI l'API IAM pour modifier la description du rôle. Pour en savoir plus, consultez Modification d’un rôle lié à un service dans le guide de l’utilisateur IAM.

Suppression d'un rôle lié à un service pour Trusted Advisor

Si vous n'avez pas besoin d'utiliser les fonctionnalités ou les services de Trusted Advisor, vous pouvez supprimer le `AWSServiceRoleForTrustedAdvisor` rôle. Vous devez le désactiver Trusted Advisor avant de pouvoir supprimer ce rôle lié à un service. Cela vous évite de supprimer des autorisations requises par les opérations Trusted Advisor . Lorsque vous le désactivez Trusted Advisor, vous désactivez toutes les fonctionnalités du service, y compris le traitement hors ligne et les notifications. De plus, si vous le désactivez Trusted Advisor pour un compte membre, le compte payeur distinct est également affecté, ce qui signifie que vous ne recevrez pas de Trusted Advisor chèques identifiant des moyens de réduire les coûts. Vous ne pouvez pas accéder à la console Trusted Advisor . Appels d'API pour Trusted Advisor renvoyer une erreur de refus d'accès.

Vous devez recréer le rôle lié au service `AWSServiceRoleForTrustedAdvisor` dans le compte avant de pouvoir réactiver Trusted Advisor.

Vous devez d'abord le désactiver Trusted Advisor dans la console avant de pouvoir supprimer le rôle `AWSServiceRoleForTrustedAdvisor` lié au service.

Pour désactiver Trusted Advisor

1. Connectez-vous à AWS Management Console et accédez à la Trusted Advisor console à l'adressehttps://console.aws.amazon.com/trustedadvisor.
2. Dans le volet de navigation, sélectionnez Préférences.
3. Dans la section Service Linked Role Permissions (Autorisations de rôles liés à un service), choisissez Désactiver Trusted Advisor.
4. Dans la boîte de dialogue de confirmation, choisissez OK pour confirmer la suppression de Trusted Advisor.

Après la désactivation Trusted Advisor, toutes les Trusted Advisor fonctionnalités sont désactivées et la Trusted Advisor console affiche uniquement la bannière d'état de désactivation.

Vous pouvez ensuite utiliser la console IAM AWS CLI, ou l'API IAM pour supprimer le rôle lié au Trusted Advisor service nommé. `AWSServiceRoleForTrustedAdvisor` Pour plus d'informations, consultez Suppression d'un rôle lié à un service dans le Guide de l'utilisateur IAM.

AWS politiques gérées pour AWS Support

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 Service AWS est lancée ou lorsque de nouvelles opérations d'API sont disponibles pour les services existants.

Pour plus d'informations, consultez la section Politiques gérées par AWS dans le Guide de l'utilisateur IAM.

Rubriques

AWS politiques gérées pour AWS Support

AWS Support possède les politiques gérées suivantes.

Table des matières

AWS politique gérée : AWSSupportServiceRolePolicy

AWS Support utilise la politique AWSSupportServiceRolePolicy AWS gérée. Cette politique gérée est attachée au rôle lié à un service `AWSServiceRoleForSupport`. La politique permet au rôle lié à un service d'exécuter des actions en votre nom. Vous ne pouvez pas attacher cette politique à vos entités IAM. Pour plus d'informations, consultez Autorisations des rôles liés à un service pour AWS Support.

Pour une liste des modifications apportées à la politique, consultez AWS Support mises à jour des politiques AWS gérées et Modifications des autorisations pour AWSSupportServiceRolePolicy.

AWS Support mises à jour des politiques AWS gérées

Consultez les détails des mises à jour des politiques AWS gérées AWS Support depuis que ces services ont 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.

Le tableau suivant décrit les mises à jour importantes apportées aux politiques AWS Support gérées depuis le 17 février 2022.

AWS Support

Modification	Description	Date
AWSSupportServiceRolePolicy – Mise à jour d'une stratégie existante	17 nouvelles autorisations ont été ajoutées aux services suivants pour effectuer des actions permettant de résoudre les problèmes des clients liés à la facturation, à	22 mars 2024

Modification	Description	Date
	l'administration et au support technique : • Amazon CloudWatch Network Monitor : pour résoudre les problèmes liés au service Network Monitor. • Amazon CloudWatch Logs — Pour résoudre les problèmes liés à Amazon CloudWatch Logs. • Amazon Managed Streaming for Apache Kafka — Pour résoudre les problèmes liés à Amazon Managed Streaming for Apache Kafka. • Amazon Managed Service for Prometheus : pour résoudre les problèmes liés au service géré Amazon pour Prometheus.	

Modification	Description	Date
AWSSupportServiceRolePolicy – Mise à jour d'une politique existante	63 nouvelles autorisations ont été ajoutées aux services suivants pour effectuer des actions permettant de résoudre les problèmes des clients liés à la facturation, à l'administration et au support technique : • AWS Salles blanches — Pour résoudre les problèmes liés aux salles AWS blanches. • CodeConnections — Pour résoudre les problèmes liés à. CodeConnections • Amazon EKS — Pour résoudre les problèmes liés à Amazon EKS. • Image Builder : pour résoudre les problèmes liés à Image Builder. • Amazon Inspector2 — Pour résoudre les problèmes liés à Amazon Inspector2. • Amazon Inspector Scan : pour résoudre les problèmes liés à Amazon Inspector Scan. • Amazon CloudWatch Logs — Pour résoudre les problèmes liés à Amazon CloudWatch Logs.	17 janvier 2024

Modification	Description	Date
	• AWS Outposts — Pour résoudre les problèmes liés au AWS Outposts. • Amazon RDS : pour déboguer les problèmes liés à Amazon RDS. • AWS IAM Identity Center — Pour résoudre les problèmes liés à. AWS IAM Identity Center • Amazon S3 Express : pour résoudre les problèmes liés à Amazon S3 Express. • AWS Trusted Advisor — Pour résoudre les problèmes liés à. AWS Trusted Advisor	

Modification	Description	Date
AWSSupportServiceRolePolicy – Mise à jour d'une politique existante	126 nouvelles autorisations ont été ajoutées aux services suivants pour effectuer des actions permettant de résoudre les problèmes des clients liés à la facturation, à l'administration et au support technique : • AWS Direct Connect — Pour résoudre les problèmes liés au AWS Direct Connect service. • Amazon SageMaker — Pour résoudre les problèmes liés au SageMaker service Amazon. • Amazon AppStream — Pour résoudre les problèmes liés à Amazon AppStream. • Explorateur de ressources AWS — Pour résoudre les problèmes liés au Explorateur de ressources AWS. • Amazon Redshift sans serveur : pour résoudre les problèmes liés à Amazon Redshift sans serveur. • Amazon ElastiCache — Pour résoudre les problèmes liés à Amazon ElastiCache.	6 déc. 2023

Modification	Description	Date
	• Amazon Comprehend : pour résoudre des problèmes liés à Amazon Comprehend. • Amazon EC2 — Pour résoudre les problèmes liés à Amazon EC2. • Amazon Elastic Kubernetes Service — Pour résoudre les problèmes liés à Amazon Elastic Kubernetes Service. • AWS Elastic Disaster Recovery — Pour résoudre les problèmes liés à. AWS Elastic Disaster Recovery • AWS AppSync — Pour résoudre les problèmes liés à. AWS AppSync • Amazon CloudWatch Logs — Pour résoudre les problèmes liés à Amazon CloudWatch Logs. • AWS Health — Pour résoudre les problèmes liés au AWS Health Service. • Amazon Connect — Pour résoudre les problèmes liés à Amazon Connect. • AWS Snowball — Pour résoudre les problèmes liés à. AWS Snowball	

Modification	Description	Date
	• AWS Health Imagerie : pour résoudre les problèmes liés à l' AWS Health imagerie.	

Modification	Description	Date
AWSSupportServiceRolePolicy – Mise à jour d'une politique existante	Ajout de 163 nouvelles autorisations aux services suivants pour effectuer des actions permettant de résoudre les problèmes des clients liés à la facturation, à l'administration et au support technique : • Amazon CloudFront — Pour résoudre les problèmes liés au CloudFront service. • Amazon EC2 : pour résoudre les problèmes liés au service Amazon EC2. • Amazon AppStream — Pour résoudre les problèmes liés à Amazon AppStream. • AWS WAF — Pour résoudre les problèmes liés au AWS Web Application Firewall. • Amazon Connect : pour résoudre les problèmes liés à Amazon Connect. • AWS IoT — Pour résoudre les problèmes liés au AWS IoT. • Amazon Route 53 : pour résoudre les problèmes liés à Amazon Route 53. • AWS Accès vérifié : pour résoudre les problèmes liés	27 octobre 2023

Modification	Description	Date
	au service d'accès AWS vérifié. • Amazon Simple Email Service : pour résoudre les problèmes liés à Amazon Simple Email Service. • AWS Elastic Beanstalk — Pour résoudre les problèmes liés à. AWS Elastic Beanstalk • Amazon DynamoDB : pour déboguer les problèmes liés à Amazon DynamoDB. • AWS EC2 Image Builder : pour résoudre les problèmes liés AWS à EC2 Image Builder. • AWS Outposts — Pour résoudre les problèmes liés au AWS Outposts Service. • AWS Glue — Pour résoudre les problèmes liés au AWS Glue. • AWS Directory Service — Pour résoudre les problèmes liés à. AWS Directory Service • AWS Elastic Disaster Recovery — Pour résoudre les problèmes liés à. AWS Elastic Disaster Recovery • AWS Step Functions — Pour résoudre les	

Modification	Description	Date
	problèmes liés à. AWS Step Functions • Amazon EMR : pour résoudre les problèmes liés à Amazon EMR. • Amazon Relational Database Service : pour résoudre les problèmes liés à Amazon Relational Database Service. • Amazon EC2 Systems Manager : pour déboguer les problèmes liés à Amazon EC2 Systems Manager.	

Modification	Description	Date
AWSSupportServiceRolePolicy – Mise à jour d'une politique existante	Ajout de 176 nouvelles autorisations aux services suivants pour effectuer des actions qui permettent de résoudre les problèmes des clients liés à la facturation, à l'administration et au support technique : • AWS Glue — Pour résoudre les problèmes liés au service AWS Glue • Amazon EMR : pour résoudre les problèmes liés au service Amazon EMR. • Amazon Security Lake : pour déboguer les problèmes liés à Amazon Security Lake. • AWS Systems Manager — Pour résoudre les problèmes liés au service Systems Manager. • Amazon Verified Permissions : pour résoudre les problèmes liés à Amazon Verified Permissions. • AWS Analyseur d'accès IAM : pour résoudre les problèmes liés au service IAM Access Analyzer. • AWS Backup — Pour résoudre les problèmes liés à. AWS Backup	28 août 2023

Modification	Description	Date
	• AWS Database Migration Service — Pour résoudre les problèmes liés au service DMS. • Amazon DynamoDB : pour déboguer les problèmes liés à DynamoDB. • Amazon Elastic Container Registry (Amazon ECR) : pour résoudre des problèmes liés à Amazon Elastic Container Registry (Amazon ECR). • Amazon Elastic Container Service : pour déboguer les problèmes liés à Amazon Elastic Container Service. • Amazon Elastic Kubernetes Service : pour résoudre les problèmes liés à Amazon Elastic Kubernetes Service. • Amazon EMR sans serveur : pour déboguer les problèmes liés au service Amazon EMR sans serveur. • AWS Identity and Access Management — Pour résoudre les problèmes liés à. AWS Identity and Access Management • AWS Network Firewall : pour résoudre les	

Modification	Description	Date
	problèmes liés au AWS Network Firewall. • AWS HealthOmics — Pour résoudre les problèmes liés à. AWS HealthOmics • Amazon QuickSight — Pour résoudre les problèmes liés à Amazon QuickSight. • Amazon Relational Database Service : pour résoudre les problèmes liés à Amazon Relational Database Service. • Amazon Redshift : pour résoudre les problèmes liés à Amazon Redshift. • Amazon Redshift sans serveur : pour déboguer les problèmes liés au service Amazon Redshift sans serveur. • Amazon SageMaker — Pour résoudre les problèmes liés à Amazon SageMaker.	

Modification	Description	Date
AWSSupportServiceRolePolicy – Mise à jour d'une politique existante	Ajout de 141 nouvelles autorisations aux services suivants pour effectuer des actions qui permettent de résoudre les problèmes des clients liés à la facturation, à l'administration et au support technique : • Lambda : pour résoudre les problèmes liés au service Lambda. • Amazon Lex : pour résoudre les problèmes liés au service Amazon Lex. • AWS Transfert — Pour résoudre les problèmes liés au service de transfert. • AWS Amplify — Pour résoudre les problèmes liés au service Amplify. • Amazon EventBridge Pipes — Pour résoudre les problèmes d'autorisation et de facturation liés à Pipes. • Amazon EventBridge — Pour résoudre les problèmes liés à Amazon EventBridge • Amazon CloudWatch Logs — Pour résoudre les problèmes liés à Amazon CloudWatch Logs.	26 juin 2023

Modification	Description	Date
	• AWS Systems Manager — Pour résoudre les problèmes liés à Systems Manager. • Amazon CloudWatch — Pour résoudre les problèmes liés à. CloudWatch • Amazon ElastiCache — Pour résoudre les problèmes liés à Amazon ElastiCache. • Amazon Athena : pour déboguer les problèmes liés à Athena. • AWS Elastic Disaster Recovery — Pour résoudre les problèmes liés à Elastic Disaster Recovery. • Amazon CloudWatch — Pour résoudre les problèmes de configuration d'Amazon CloudWatch. • Amazon EC2 : pour résoudre les problèmes liés au service EC2. • AWS Certificate Manager — Pour résoudre les problèmes liés à Certificate Manager. • Amazon EventBridge Scheduler : pour résoudre	

Modification	Description	Date
	les problèmes liés au planificateur. EventBridge • Amazon OpenSearch Service — Pour résoudre les problèmes liés à OpenSearch. • Amazon EventBridge Schemas — Pour résoudre les problèmes liés aux EventBridge schémas. • AWS Notifications utilisate ur — Pour résoudre les problèmes liés aux notificat ions utilisateur. • Amazon CloudWatch Application Insights : pour résoudre les problèmes liés à CloudWatch Application Insights. • Amazon DynamoDB : pour déboguer les problèmes liés à DynamoDB. • Clusters élastiques Amazon DocumentDB : pour résoudre les problèmes liés aux clusters élastiques DocumentDB.	

Modification	Description	Date
AWSSupportServiceRolePolicy – Mise à jour d'une politique existante	Ajout de 53 nouvelles autorisations aux services suivants pour effectuer des actions qui permettent de résoudre les problèmes des clients liés à la facturation, à l'administration et au support technique : • Autoscaling : pour résoudre les problèmes liés au service d'autoscaling. • Amazon CloudWatch — Pour résoudre les problèmes liés à Amazon CloudWatch. • AWS Compute Optimizer — Pour résoudre les problèmes liés à Compute Optimizer. • Amazon CloudWatch Evidently — Pour résoudre les problèmes liés à Evidently. • EC2 Image Builder : pour résoudre les problèmes liés au service Image Builder. • AWS IoT TwinMaker — Pour résoudre les problèmes liés à. AWS IoT TwinMaker • Amazon CloudWatch Logs — Pour résoudre les problèmes liés à Amazon CloudWatch Logs.	2 mai 2023

Modification	Description	Date
	• Amazon Pinpoint : pour résoudre des problèmes liés à Amazon Pinpoint. • AWS Lien OAM — Pour résoudre les problèmes liés aux ressources OAM. • AWS Outposts — Pour résoudre les problèmes liés à. AWS Outposts • Amazon RDS : pour déboguer les problèmes liés à Amazon RDS. • Explorateur de ressources AWS — Pour résoudre les problèmes liés à Resource Explorer. • Amazon CloudWatch RUM — Pour résoudre les problèmes de configuration des ressources du service RUM. • Amazon SNS : pour résoudre les problèmes liés à Amazon SNS. • Amazon CloudWatch Synthetics — Pour résoudre les problèmes liés aux Synthetics. CloudWatch	

Modification	Description	Date
AWSSupportServiceRolePolicy – Mise à jour d'une politique existante	Ajout de 52 nouvelles autorisations aux services suivants pour effectuer des actions qui permettent de résoudre les problèmes des clients liés à la facturation, à l'administration et au support technique : • AWS Backup gateway — Pour résoudre les problèmes liés à la passerelle Backup. • Amazon S3 : pour déboguer les problèmes liés à Amazon S3. • AWS Application Migration Service — Pour résoudre les problèmes liés au service de migration d'applications. • AWS Salles propres — Pour résoudre les problèmes liés aux salles AWS blanches ; • AWS Systems Manager pour SAP — Pour résoudre les problèmes liés AWS Systems Manager à SAP. • Amazon VPC Lattice : pour déboguer les problèmes liés à Amazon VPC Lattice.	16 mars 2023

Modification	Description	Date
AWSSupportServiceRolePolicy – Mise à jour d'une politique existante	Ajout de 220 nouvelles autorisations aux services suivants pour effectuer des actions qui aident à résoudre les problèmes des clients liés à la facturation, à l'administration et au support technique : • Amazon Athena — Permettre de AWS Support développer des outils pouvant être utilisés pour aider les clients à répondre à leurs questions concernant Athena. • Amazon Chime : pour résoudre des problèmes liés à Amazon Chime. • Amazon CloudWatch Internet Monitor — Pour résoudre les problèmes liés à Internet Monitor. • Amazon Comprehend : pour résoudre des problèmes liés à Amazon Comprehend. • Amazon Elastic Compute Cloud : pour déboguer des problèmes liés à Transit Gateway Connect et aux fonctionnalités de multicast. • Amazon EventBridge Pipes — Pour résoudre les	10 janvier 2023

Modification	Description	Date
	problèmes liés à EventBridge Pipes. • Amazon Interactive Video Service — Pour AWS Support permettre d'interroger les ressources Amazon IVS afin de résoudre les problèmes des clients. • Amazon FSx — Permettre de développer des outils permettant AWS Support de prendre en charge l'importation et l'exportation pour un référentiel de données Amazon FSx. • Amazon GameLift — Pour résoudre les problèmes liés à Amazon GameLift. • AWS Glue : pour résoudre des problèmes liés à AWS Glue Data Quality. • Amazon Kinesis Video Streams : pour résoudre des problèmes liés à Kinesis Video Streams. • Amazon Managed Service for Prometheus : pour résoudre des problèmes liés à Amazon Managed Service for Prometheus. • Amazon Managed Streaming for Apache Kafka : pour résoudre des	

Modification	Description	Date
	problèmes liés à Amazon MSK Connect. • AWS Network Manager — Pour résoudre les problèmes liés à Network Manager. • Amazon Nimble Studio : pour déboguer des problèmes liés à Nimble Studio. • Amazon Personalize : pour déboguer des problèmes liés à Amazon Personalize. • Amazon Pinpoint : pour résoudre des problèmes liés à Amazon Pinpoint. • AWS HealthOmics — Pour résoudre les problèmes liés à. HealthOmics • Amazon Transcribe : pour déboguer des problèmes liés à Amazon Transcribe.	

Modification	Description	Date
AWSSupportServiceRolePolicy – Mise à jour d'une politique existante	Ajout de 47 nouvelles autorisations aux services suivants pour effectuer des actions qui aident à résoudre les problèmes des clients liés à la facturation, à l'administration et au support technique : • AWS Application Migration Service — Pour résoudre les problèmes de réplication et de lancement. • AWS CloudFormation crochets — Pour permettre de AWS Support développer des outils d'automatisation qui peuvent aider à résoudre les problèmes. • Amazon Elastic Kubernetes Service : pour résoudre les problèmes liés à Amazon EKS. • AWS IoT FleetWise : pour résoudre les problèmes liés à AWS IoT FleetWise. • AWS Mainframe Modernization — Pour résoudre les problèmes liés à la modernisation du mainframe. • AWS Outposts — Pour aider à AWS Support obtenir une liste d'hôtes et d'actifs dédiés.	4 octobre 2022

Modification	Description	Date
	• AWS Private 5G : pour résoudre les problèmes liés à Private 5G. • AWS Tiros : pour déboguer les problèmes liés à Tiros.	

Modification	Description	Date
AWSSupportServiceRolePolicy – Mise à jour d'une politique existante	Ajout de 46 nouvelles autorisations aux services suivants pour effectuer des actions qui aident à résoudre les problèmes des clients liés à la facturation, à l'administration et au support technique : • Amazon Managed Streaming for Apache Kafka : pour résoudre les problèmes liés à Amazon MSK. • AWS DataSync — Pour résoudre les problèmes liés à. DataSync • AWS Elastic Disaster Recovery — Pour résoudre les problèmes de réplication et de lancement. • Amazon GameSparks — Pour résoudre les problèmes liés à. GameSparks • AWS IoT TwinMaker — Pour résoudre les problèmes liés à. AWS IoT TwinMaker • AWS Lambda — Pour consulter la configuration de l'URL d'une fonction afin de résoudre les problèmes. • Amazon Lookout for Equipment : pour résoudre	17 août 2022

Modification	Description	Date
	les problèmes liés à Lookout for Equipment. • Amazon Route 53 et Amazon Route 53 Resolver : pour obtenir des configurations de résolveur AWS Support afin de vérifier le comportem ent de résolution DNS d'un VPC.	

Modification	Description	Date
AWSSupportServiceRolePolicy – Mise à jour d'une politique existante	Ajout de nouvelles autorisations aux services suivants pour effectuer des actions qui aident à résoudre les problèmes des clients liés à la facturation, à l'administration et au support technique : • Amazon CloudWatch Logs — Pour aider à résoudre les problèmes liés aux CloudWatch journaux. • Amazon Interactive Video Service : pour vous aider à AWS Support consulter les ressources Amazon IVS existantes pour les cas d'assistance concernant des cas de fraude ou de compromission de comptes. • Amazon Inspector – Pour résoudre les problèmes liés à Amazon Inspector. Autorisations supprimées pour les services, tels qu'Amazon WorkLink. Amazon WorkLink est devenu obsolète le 19 avril 2022.	23 juin 2022

Modification	Description	Date
AWSSupportServiceRolePolicy – Mise à jour d'une politique existante	Ajout de 25 nouvelles autorisations aux services suivants pour effectuer des actions qui aident à résoudre les problèmes des clients liés à la facturation, à l'administration et au support technique : • AWS Amplify UI Builder : pour résoudre les problèmes liés à la génération de composants et de thèmes. • Amazon AppStream — Pour résoudre les problèmes en récupérant les ressources relatives aux fonctionnalités récemment lancées. • AWS Backup — Pour résoudre les problèmes liés aux tâches de sauvegarde. • AWS CloudFormation — Pour effectuer des diagnostics sur des problèmes liés à l'IAM, à l'extension et au versionnement. • Amazon Kinesis : pour résoudre les problèmes liés à Kinesis. • AWS Transfer Family — Pour résoudre les problèmes liés à Transfer Family.	27 avril 2022

Modification	Description	Date

AWSSupportServiceRolePolicy : mise à jour d'une politique existante	Ajout de 54 nouvelles autorisations aux services suivants pour effectuer des actions qui aident à résoudre les problèmes des clients liés à la facturation, à l'administration et au support technique :
	• Amazon Elastic Compute Cloud
	  • Pour résoudre les problèmes liés aux listes des clients et préfixées gérées par AWS.
	  • Pour résoudre les problèmes liés à Amazon VPC IP Address Manager (IPAM).
	• AWS Gestionnaire de réseau : pour résoudre les problèmes liés au gestionnaire de réseau.
	• Savings Plans : pour obtenir des métadonnées sur les engagements du Savings Plan en cours.
	• AWS Serverless Application Repository — Améliorer et soutenir les actions de réponse dans le cadre de la recherche et de la résolution des cas de soutien.
	• Amazon WorkSpaces Web — Pour déboguer et
		14 mars 2022

Modification	Description	Date
	résoudre les problèmes liés aux services WorkSpaces Web.	

Modification	Description	Date
AWSSupportServiceRolePolicy – Mise à jour d'une politique existante	Ajout de 74 nouvelles autorisations aux services suivants pour effectuer des actions qui aident à résoudre les problèmes des clients liés à la facturation, à l'administration et au support technique : • AWS Application Migration Service — Pour prendre en charge la réplication sans agent dans le service de migration des applications. • AWS CloudFormation — Pour effectuer des diagnostics sur les problèmes liés à l'IAM, aux extensions et au versionnement. • Amazon CloudWatch Logs — Pour valider les politiques relatives aux ressources. • Corbeille Amazon EC2 : pour obtenir des métadonnées sur les règles de rétention de la corbeille. • AWS Elastic Disaster Recovery — Pour résoudre les problèmes de réplication et de lancement dans les comptes clients. • Amazon FSx : pour afficher la description des instantanés Amazon FSx.	17 février 2022

Modification	Description	Date
	• Amazon Lightsail : pour afficher les métadonnées et les détails des configurations des compartiments Lightsail. • Amazon Macie : pour afficher les configurations de Macie, telles que les tâches de classification, les identificateurs de données personnalisés, les expressions régulières et les résultats . • Amazon S3 : pour collecter des métadonnées et des configurations pour les compartiments Amazon S3. • AWS Storage Gateway — Pour consulter les métadonnées relatives aux politiques de création automatique de bandes des clients. • Elastic Load Balancing : pour afficher la description des limites de ressources lors de l'utilisation de la console Service Quotas. Pour plus d'informations, consultez Modifications des autorisations pour	

Modification	Description	Date
	AWSSupportServiceRolePolicy.	
Journal des modifications publié	Journal des modifications pour les politiques AWS Support gérées.	17 février 2022

Modifications des autorisations pour AWSSupportServiceRolePolicy

La plupart des autorisations ont été ajoutées AWS Support pour `AWSSupportServiceRolePolicy` permettre d'appeler une opération d'API portant le même nom. Toutefois, certaines opérations d'API nécessitent des autorisations portant un nom différent.

Le tableau suivant répertorie uniquement les opérations d'API qui nécessitent des autorisations portant un nom différent. Ce tableau décrit ces différences à compter du 17 février 2022.

Date	Nom de l'opération d'API	Autorisation de politique requise
Autorisations ajoutées le 17 février 2022	`s3.GetBucketAnalyticsConfiguration` `s3.ListBucketAnalyticsConfiguration`	`s3:GetAnalyticsConfiguration`
	`s3.GetBucketNotificationConfiguration`	`s3:GetBucketNotification`
	`s3.GetBucketEncryption`	`s3:GetEncryptionConfiguration`
	`s3.GetBucketIntelligentTieringConfiguration`	`s3:GetIntelligentTieringConfiguration`

Date	Nom de l'opération d'API	Autorisation de politique requise
	s3.ListBucketIntelligentTieringConfiguration	
	s3.GetBucketInventoryConfiguration s3.ListBucketInventoryConfiguration	s3:GetInventoryConfiguration
	s3.GetBucketLifecycleConfiguration	s3:GetLifecycleConfiguration
	s3.GetBucketMetricsConfiguration s3.ListBucketMetricsConfiguration	s3:GetMetricsConfiguration
	s3.GetBucketReplication	s3:GetReplicationConfiguration
	s3.HeadBucket s3.ListObjects	s3:ListBucket
	s3.ListBuckets	s3:ListAllMyBuckets
	s3.ListMultipartUploads	s3:ListBucketMultipartUploads
	s3.ListObjectVersions	s3:ListBucketVersions
	s3.ListParts	s3:ListMultipartUploadParts

AWS politiques gérées pour les AWS Support applications dans Slack

> **Note**
>
> Pour accéder aux demandes d'assistance et les consulter dans le AWS Support Center Console, voirGérer l'accès au AWS Support centre.

AWS Support L'application dispose des politiques gérées suivantes.

Table des matières

AWS politique gérée : AWSSupportAppFullAccess

Vous pouvez utiliser la politique gérée AWSSupportAppFullAccess pour accorder au rôle IAM les autorisations pour les configurations de votre canal Slack. Vous pouvez également associer la politique AWSSupportAppFullAccess à vos entités IAM.

Pour plus d’informations, consultez Application AWS Support dans Slack.

Cette politique accorde des autorisations permettant à l'entité d'effectuer AWS Support des actions Service Quotas et IAM pour l' AWS Support application.

Détails de l’autorisation

Cette politique inclut les autorisations suivantes :

- `servicequotas` : décrit vos quotas de service et demandes existants, et crée des augmentations de quota de service pour votre compte.
- `support` : crée, met à jour et résout vos cas de support. Met à jour et décrit les informations sur vos cas, comme les pièces jointes, les correspondances et les niveaux de gravité. Initie des sessions de chat en direct avec un agent de support.

- `iam` : crée un rôle lié à un service pour Service Quotas.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "servicequotas:GetRequestedServiceQuotaChange",
                "servicequotas:GetServiceQuota",
                "servicequotas:RequestServiceQuotaIncrease",
                "support:AddAttachmentsToSet",
                "support:AddCommunicationToCase",
                "support:CreateCase",
                "support:DescribeCases",
                "support:DescribeCommunications",
                "support:DescribeSeverityLevels",
                "support:InitiateChatForCase",
                "support:ResolveCase"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": "iam:CreateServiceLinkedRole",
            "Resource": "*",
            "Condition": {
                "StringEquals": {"iam:AWSServiceName": "servicequotas.amazonaws.com"}
            }
        }
    ]
}
```

Pour plus d’informations, consultez Gestion de l'accès à l'application AWS Support.

AWS politique gérée : AWSSupportAppReadOnlyAccess

La AWSSupportAppReadOnlyAccesspolitique accorde des autorisations qui permettent à l'entité d'effectuer des actions d' AWS Support application en lecture seule. Pour plus d’informations, consultez Application AWS Support dans Slack.

Détails de l’autorisation

Cette politique inclut les autorisations suivantes :

- `support` : décrit les détails des cas de support et les communications ajoutées aux cas de support.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "support:DescribeCases",
                "support:DescribeCommunications"
            ],
            "Resource": "*"
        }
    ]
}
```

AWS Support Mises à jour des politiques AWS gérées par les applications

Consultez les détails des mises à jour des politiques AWS gérées pour AWS Support l'application 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.

Le tableau suivant décrit les mises à jour importantes apportées aux politiques gérées par l' AWS Support application depuis le 17 août 2022.

AWS Support Appli

Modification	Description	Date
AWSSupportAppFullAccessetAWSSupportAppReadOnlyAccess Nouvelles politiques AWS gérées pour l' AWS Support application	Vous pouvez utiliser ces politiques pour le rôle IAM que vous configurez pour votre configuration de canal Slack. Pour plus d'informations, consultez Gestion de l'accès à l'application AWS Support.	19 août 2022
Journal des modifications publié	Journal des modifications pour les politiques gérées par l' AWS Support application.	19 août 2022

AWS politiques gérées pour AWS Trusted Advisor

Trusted Advisor possède les politiques AWS gérées suivantes.

Table des matières

AWS politique gérée : AWSTrustedAdvisorPriorityFullAccess

La AWSTrustedAdvisorPriorityFullAccesspolitique accorde un accès complet à Trusted Advisor Priority. Cette politique permet également à l'utilisateur d'ajouter Trusted Advisor en tant que service de confiance AWS Organizations et de spécifier les comptes d'administrateur délégué pour Trusted Advisor Priority.

Détails de l'autorisation

Dans la première instruction, la politique inclut les autorisations suivantes pour `trustedadvisor` :

- Décrit votre compte et votre organisation.
- Décrit les risques identifiés par Trusted Advisor Priority. Les autorisations vous permettent de télécharger et de mettre à jour le statut du risque.
- Décrit vos configurations pour les notifications par e-mail Trusted Advisor prioritaires. Les autorisations vous permettent de configurer les e-mails de notification et de les désactiver pour vos administrateurs délégués.
- Configure de Trusted Advisor telle sorte que votre compte puisse être activé AWS Organizations.

Dans la deuxième instruction, la politique inclut les autorisations suivantes pour `organizations` :

- Décrit votre Trusted Advisor compte et votre organisation.
- Répertorie les Organisations Services AWS que vous avez autorisées à utiliser.

Dans la troisième instruction, la politique inclut les autorisations suivantes pour `organizations` :

- Répertorie les administrateurs délégués pour Trusted Advisor Priority.
- Active et désactive l'accès sécurisé aux Organizations.

Dans la quatrième instruction, la politique inclut les autorisations suivantes pour `iam` :

- Crée le rôle lié à un service `AWSServiceRoleForTrustedAdvisorReporting`.

Dans la cinquième instruction, la politique inclut les autorisations suivantes pour `organizations` :

- Permet d'enregistrer et d'annuler l'enregistrement des administrateurs délégués pour Trusted Advisor Priority.

```
{
 "Version": "2012-10-17",
 "Statement": [
  {
   "Sid": "AWSTrustedAdvisorPriorityFullAccess",
   "Effect": "Allow",
   "Action": [
    "trustedadvisor:DescribeAccount*",
    "trustedadvisor:DescribeOrganization",
```

```
    "trustedadvisor:DescribeRisk*",
    "trustedadvisor:DownloadRisk",
    "trustedadvisor:UpdateRiskStatus",
    "trustedadvisor:DescribeNotificationConfigurations",
    "trustedadvisor:UpdateNotificationConfigurations",
    "trustedadvisor:DeleteNotificationConfigurationForDelegatedAdmin",
    "trustedadvisor:SetOrganizationAccess"
   ],
   "Resource": "*"
  },
  {
   "Sid": "AllowAccessForOrganization",
   "Effect": "Allow",
   "Action": [
    "organizations:DescribeAccount",
    "organizations:DescribeOrganization",
    "organizations:ListAWSServiceAccessForOrganization"
   ],
   "Resource": "*"
  },
  {
   "Sid": "AllowListDelegatedAdministrators",
   "Effect": "Allow",
   "Action": [
    "organizations:ListDelegatedAdministrators",
    "organizations:EnableAWSServiceAccess",
    "organizations:DisableAWSServiceAccess"
   ],
   "Resource": "*",
   "Condition": {
    "StringEquals": {
     "organizations:ServicePrincipal": [
      "reporting.trustedadvisor.amazonaws.com"
     ]
    }
   }
  },
  {
   "Sid": "AllowCreateServiceLinkedRole",
   "Effect": "Allow",
   "Action": "iam:CreateServiceLinkedRole",
   "Resource": "arn:aws:iam::*:role/aws-service-role/
reporting.trustedadvisor.amazonaws.com/AWSServiceRoleForTrustedAdvisorReporting",
   "Condition": {
```

```
    "StringLike": {
     "iam:AWSServiceName": "reporting.trustedadvisor.amazonaws.com"
    }
   }
  },
  {
   "Sid": "AllowRegisterDelegatedAdministrators",
   "Effect": "Allow",
   "Action": [
    "organizations:RegisterDelegatedAdministrator",
    "organizations:DeregisterDelegatedAdministrator"
   ],
   "Resource": "arn:aws:organizations::*:*",
   "Condition": {
    "StringEquals": {
     "organizations:ServicePrincipal": [
      "reporting.trustedadvisor.amazonaws.com"
     ]
    }
   }
  }
 ]
}
```

AWS politique gérée : AWSTrustedAdvisorPriorityReadOnlyAccess

La AWSTrustedAdvisorPriorityReadOnlyAccesspolitique accorde des autorisations en lecture seule à Trusted Advisor Priority, y compris l'autorisation de consulter les comptes d'administrateurs délégués.

Détails de l’autorisation

Dans la première instruction, la politique inclut les autorisations suivantes pour `trustedadvisor` :

- Décrit votre Trusted Advisor compte et votre organisation.
- Décrit les risques identifiés par Trusted Advisor Priority et vous permet de les télécharger.
- Décrit les configurations des notifications par e-mail Trusted Advisor prioritaires.

Dans la deuxième et troisième instruction, la politique inclut les autorisations suivantes pour `organizations` :

- Décrit votre organisation à l'aide d'Organizations.

- Répertorie les Organisations Services AWS que vous avez autorisées à utiliser.
- Répertorie les administrateurs délégués pour Trusted Advisor Priority

```
{
 "Version": "2012-10-17",
 "Statement": [
  {
   "Sid": "AWSTrustedAdvisorPriorityReadOnlyAccess",
   "Effect": "Allow",
   "Action": [
    "trustedadvisor:DescribeAccount*",
    "trustedadvisor:DescribeOrganization",
    "trustedadvisor:DescribeRisk*",
    "trustedadvisor:DownloadRisk",
    "trustedadvisor:DescribeNotificationConfigurations"
   ],
   "Resource": "*"
  },
  {
   "Sid": "AllowAccessForOrganization",
   "Effect": "Allow",
   "Action": [
    "organizations:DescribeOrganization",
    "organizations:ListAWSServiceAccessForOrganization"
   ],
   "Resource": "*"
  },
  {
   "Sid": "AllowListDelegatedAdministrators",
   "Effect": "Allow",
   "Action": [
    "organizations:ListDelegatedAdministrators"
   ],
   "Resource": "*",
   "Condition": {
    "StringEquals": {
     "organizations:ServicePrincipal": [
      "reporting.trustedadvisor.amazonaws.com"
     ]
    }
   }
  }
```

```
 ]
}
```

Politique gérée par AWS : AWSTrustedAdvisorServiceRolePolicy

Cette politique est attachée au rôle lié à un service `AWSServiceRoleForTrustedAdvisor`. Elle permet au rôle lié à un service d'exécuter des actions pour vous. Vous ne pouvez pas associer la politique AWSTrustedAdvisorServiceRolePolicy à vos entités AWS Identity and Access Management (IAM). Pour plus d'informations, consultez Utilisation des rôles liés aux services pour Trusted Advisor.

Cette politique accorde des autorisations administratives qui permettent au rôle lié au service d'accéder aux Services AWS. Ces autorisations permettent aux vérifications Trusted Advisor d'évaluer votre compte.

Détails de l'autorisation

Cette politique inclut les autorisations suivantes.

- `Auto Scaling` : Décrit les quotas et les ressources de compte Amazon EC2 Auto Scaling
- `cloudformation`— Décrit AWS CloudFormation (CloudFormation) les quotas et les piles de comptes
- `cloudfront`— Décrit les CloudFront distributions Amazon
- `cloudtrail`— Décrit AWS CloudTrail (CloudTrail) les sentiers
- `dynamodb` : Décrit les quotas et les ressources de compte Amazon DynamoDB
- `ec2` : Décrit les quotas et les ressources de compte Amazon Elastic Compute Cloud (Amazon EC2)
- `elasticloadbalancing` : décrit les ressources et quotas de compte Elastic Load Balancing (ELB)
- `iam` : Récupère les ressources IAM, telles que les informations d'identification, la politique de mot de passe et les certificats
- `kinesis` : Décrit les quotas de compte Amazon Kinesis (Kinesis)
- `rds` : Décrit les ressources Amazon Relational Database Service (Amazon RDS)
- `redshift` : Décrit les ressources Amazon Redshift
- `route53` : Décrit les quotas et les ressources de compte Amazon Route 53

- `s3` : Décrit les ressources Amazon Simple Storage Service (Amazon S3)
- `ses` : Récupère les quotas d'envoi Amazon Simple Email Service (Amazon SES)
- `sqs` : Répertorie les files d'attente Amazon Simple Queue Service (Amazon SQS)
- `cloudwatch`— Obtient les statistiques métriques d'Amazon CloudWatch CloudWatch Events (Events)
- `ce` : Récupère les recommandations du service Cost Explorer (Cost Explorer)
- `route53resolver`— Obtient les points de terminaison et les ressources du Amazon Route 53 Resolver résolveur
- `kafka` : pour obtenir les ressources Amazon Managed Streaming for Apache Kafka.
- `ecs`— Récupère les ressources Amazon ECS
- `outposts`— Obtient AWS Outposts des ressources

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "autoscaling:DescribeAccountLimits",
                "autoscaling:DescribeAutoScalingGroups",
                "autoscaling:DescribeLaunchConfigurations",
                "ce:GetReservationPurchaseRecommendation",
                "ce:GetSavingsPlansPurchaseRecommendation",
                "cloudformation:DescribeAccountLimits",
                "cloudformation:DescribeStacks",
                "cloudformation:ListStacks",
                "cloudfront:ListDistributions",
                "cloudtrail:DescribeTrails",
                "cloudtrail:GetTrailStatus",
                "cloudtrail:GetTrail",
                "cloudtrail:ListTrails",
                "cloudtrail:GetEventSelectors",
                "cloudwatch:GetMetricStatistics",
                "dynamodb:DescribeLimits",
                "dynamodb:DescribeTable",
                "dynamodb:ListTables",
                "ec2:DescribeAddresses",
                "ec2:DescribeReservedInstances",
```

```
                "ec2:DescribeInstances",
                "ec2:DescribeVpcs",
                "ec2:DescribeInternetGateways",
                "ec2:DescribeImages",
                "ec2:DescribeVolumes",
                "ec2:DescribeSecurityGroups",
                "ec2:DescribeSubnets",
                "ec2:DescribeRegions",
                "ec2:DescribeReservedInstancesOfferings",
                "ec2:DescribeSnapshots",
                "ec2:DescribeVpnConnections",
                "ec2:DescribeVpnGateways",
                "ec2:DescribeLaunchTemplateVersions",
                "ecs:DescribeTaskDefinition",
                "ecs:ListTaskDefinitions"
                "elasticloadbalancing:DescribeAccountLimits",
                "elasticloadbalancing:DescribeInstanceHealth",
                "elasticloadbalancing:DescribeLoadBalancerAttributes",
                "elasticloadbalancing:DescribeLoadBalancerPolicies",
                "elasticloadbalancing:DescribeLoadBalancerPolicyTypes",
                "elasticloadbalancing:DescribeLoadBalancers",
                "elasticloadbalancing:DescribeTargetGroups",
                "iam:GenerateCredentialReport",
                "iam:GetAccountPasswordPolicy",
                "iam:GetAccountSummary",
                "iam:GetCredentialReport",
                "iam:GetServerCertificate",
                "iam:ListServerCertificates",
                "kinesis:DescribeLimits",
                "kafka:ListClustersV2",
                "kafka:ListNodes",
                "outposts:GetOutpost",
                "outposts:ListAssets",
                "outposts:ListOutposts",
                "rds:DescribeAccountAttributes",
                "rds:DescribeDBClusters",
                "rds:DescribeDBEngineVersions",
                "rds:DescribeDBInstances",
                "rds:DescribeDBParameterGroups",
                "rds:DescribeDBParameters",
                "rds:DescribeDBSecurityGroups",
                "rds:DescribeDBSnapshots",
                "rds:DescribeDBSubnetGroups",
                "rds:DescribeEngineDefaultParameters",
```

```
                "rds:DescribeEvents",
                "rds:DescribeOptionGroupOptions",
                "rds:DescribeOptionGroups",
                "rds:DescribeOrderableDBInstanceOptions",
                "rds:DescribeReservedDBInstances",
                "rds:DescribeReservedDBInstancesOfferings",
                "rds:ListTagsForResource",
                "redshift:DescribeClusters",
                "redshift:DescribeReservedNodeOfferings",
                "redshift:DescribeReservedNodes",
                "route53:GetAccountLimit",
                "route53:GetHealthCheck",
                "route53:GetHostedZone",
                "route53:ListHealthChecks",
                "route53:ListHostedZones",
                "route53:ListHostedZonesByName",
                "route53:ListResourceRecordSets",
                "route53resolver:ListResolverEndpoints",
                "route53resolver:ListResolverEndpointIpAddresses",
                "s3:GetAccountPublicAccessBlock",
                "s3:GetBucketAcl",
                "s3:GetBucketPolicy",
                "s3:GetBucketPolicyStatus",
                "s3:GetBucketLocation",
                "s3:GetBucketLogging",
                "s3:GetBucketVersioning",
                "s3:GetBucketPublicAccessBlock",
                "s3:GetLifecycleConfiguration",
                "s3:ListBucket",
                "s3:ListAllMyBuckets",
                "ses:GetSendQuota",
                "sqs:ListQueues"
            ],
            "Resource": "*"
        }
    ]
}
```

AWS politique gérée : AWSTrustedAdvisorReportingServiceRolePolicy

Cette politique est attachée au rôle `AWSServiceRoleForTrustedAdvisorReporting` lié au service qui permet Trusted Advisor d'effectuer des actions pour la fonctionnalité d'affichage

organisationnel. Vous ne pouvez pas attacher AWSTrustedAdvisorReportingServiceRolePolicy à vos entités IAM. Pour plus d'informations, consultez Utilisation des rôles liés aux services pour Trusted Advisor.

Cette politique accorde des autorisations administratives qui permettent au rôle lié au service d'effectuer des AWS Organizations actions.

Détails de l'autorisation

Cette politique inclut les autorisations suivantes.

- `organizations` : Décrit votre organisation et répertorie l'accès au service, les comptes, les parents, les enfants et les unités organisationnelles

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

Trusted Advisor mises à jour des politiques AWS gérées

Consultez les détails des mises à jour des politiques AWS gérées pour AWS Support et Trusted Advisor depuis que ces services ont 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.

Le tableau suivant décrit les mises à jour importantes apportées aux politiques Trusted Advisor gérées depuis le 10 août 2021.

Trusted Advisor

Modification	Description	Date
AWSTrustedAdvisorServiceRolePolicy Mise à jour d'une politique existante.	Trusted Advisor a ajouté de nouvelles actions pour accorder `cloudtrail:GetTrail` `cloudtrail:ListTrails` `cloudtrail:GetEventSelectors` `outposts:GetOutpost` les `outposts:ListOutposts` autorisations `outposts:ListAssets` et.	18 janvier 2024
AWSTrustedAdvisorPriorityFullAccess Mise à jour d'une politique existante.	Trusted Advisor a mis à jour la politique `AWSTrustedAdvisorPriorityFullAccess` AWS gérée pour inclure les identifiants des relevés.	6 décembre 2023
AWSTrustedAdvisorPriorityReadOnlyAccess Mise à jour d'une politique existante.	Trusted Advisor a mis à jour la politique `AWSTrustedAdvisorPriorityReadOnlyAccess` AWS	6 décembre 2023

Modification	Description	Date
	gérée pour inclure les identifiants des relevés.	
AWSTrustedAdvisorServiceRolePolicy – Mise à jour d'une politique existante	Trusted Advisor a ajouté de nouvelles actions pour accorder les `ecs:ListTaskDefinitions` autorisations `ec2:DescribeRegions` `s3:GetLifecycleConfiguration` `ecs:DescribeTaskDefinition` et.	9 novembre 2023
AWSTrustedAdvisorServiceRolePolicy – Mise à jour d'une politique existante	Trusted Advisor a ajouté de nouvelles actions IAM`route53resolver:ListResolverEndpoints` , `route53resolver:ListResolverEndpointIpAddresses` `ec2:DescribeSubnets` , `kafka:ListClustersV2` et `kafka:ListNodes` pour intégrer de nouveaux contrôles de résilience.	14 septembre 2023

Modification	Description	Date
AWSTrustedAdvisorReportingServiceRolePolicy V2 de la politique gérée attachée au rôle lié au Trusted Advisor `AWSServiceRoleForTrustedAdvisorReporting` service	Mettez à niveau la politique AWS gérée vers la version V2 pour le Trusted Advisor `AWSServiceRoleForTrustedAdvisorReporting` rôle lié au service. La V2 ajoutera une action IAM supplémentaire : `organizations:ListDelegatedAdministrators`	28 février 2023
AWSTrustedAdvisorPriorityFullAccess et AWSTrustedAdvisorPriorityReadOnlyAccess Nouvelles politiques AWS gérées pour Trusted Advisor	Trusted Advisor a ajouté deux nouvelles politiques gérées que vous pouvez utiliser pour contrôler l'accès à Trusted Advisor Priority.	17 août 2022

Modification	Description	Date
AWSTrustedAdvisorServiceRolePolicy – Mise à jour d'une politique existante	Trusted Advisor a ajouté de nouvelles actions pour accorder les `GetAccountPublicAccessBlock` autorisations `DescribeTargetGroups` et. L'autorisation `DescribeTargetGroup` est requise pour que la surveillance de l'état du groupe Auto Scaling récupère les équilibreurs de charge non Classic attachés à un groupe Auto Scaling. L'autorisation `GetAccountPublicAccessBlock` est requise pour la vérification des autorisations relatives aux compartiments Amazon S3 afin de récupérer les paramètres d'accès public aux blocs pour un Compte AWS.	10 août 2021
Journal des modifications publié	Trusted Advisor a commencé à suivre les modifications apportées AWS à ses politiques gérées.	10 août 2021

AWS politiques gérées pour les AWS Support plans

AWS Support Plans applique les politiques gérées suivantes.

Table des matières

- AWS politique gérée : AWSSupportPlansReadOnlyAccess
- AWS Support Planifie les mises à jour des politiques AWS gérées

AWS politique gérée : AWSSupportPlansFullAccess

AWS Support Plans utilise la politique AWSSupportPlansFullAccess AWS gérée. L'entité IAM utilise cette politique pour effectuer les actions Support Plans suivantes pour vous :

- Consultez votre plan de support pour votre Compte AWS
- Afficher les détails sur le statut d'une demande de modification de votre plan de support
- Modifiez le plan de support pour votre Compte AWS
- Créez des plannings de plans d'assistance pour votre Compte AWS

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "supportplans:GetSupportPlan",
                "supportplans:GetSupportPlanUpdateStatus",
                "supportplans:StartSupportPlanUpdate",
                "supportplans:CreateSupportPlanSchedule"
            ],
            "Resource": "*"
        }
    ]
}
```

Pour une liste des modifications apportées aux politiques, consultez AWS Support Planifie les mises à jour des politiques AWS gérées.

AWS politique gérée : AWSSupportPlansReadOnlyAccess

AWS Support Plans utilise la politique AWSSupportPlansReadOnlyAccess AWS gérée. L'entité IAM utilise cette politique pour effectuer les actions Support Plans en lecture seule suivantes pour vous :

- Consultez votre plan de support pour votre Compte AWS
- Afficher les détails sur le statut d'une demande de modification de votre plan de support

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "supportplans:GetSupportPlan",
                "supportplans:GetSupportPlanUpdateStatus"
            ],
            "Resource": "*"
        }
    ]
}
```

Pour une liste des modifications apportées aux politiques, consultez AWS Support Planifie les mises à jour des politiques AWS gérées.

AWS Support Planifie les mises à jour des politiques AWS gérées

Consultez les informations relatives aux mises à jour des politiques AWS gérées pour les plans de support depuis que ces services ont 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.

Le tableau suivant décrit les mises à jour importantes apportées aux politiques gérées de Support Plans depuis le 29 septembre 2022.

AWS Support

Modification	Description	Date
AWSSupportPlansFullAccess : mise à jour d'une stratégie existante	Ajout de l'action `CreateSupportPlanSchedule` à la politique gérée `AWSSupportPlansFullAccess` .	8 mai 2023
Journal des modifications publié	Journal des modifications pour les politiques gérées de Support Plans.	29 septembre 2022

Gérer l'accès au AWS Support centre

Vous devez disposer d'autorisations pour accéder au Centre de support et créer une demande de support.

Vous pouvez utiliser l'une des options suivantes pour accéder au Centre de support :

- Utilisez l'adresse e-mail et le mot de passe associés à votre AWS compte. Cette identité est appelée utilisateur root du AWS compte.
- Utiliser AWS Identity and Access Management (IAM).

Si vous avez un plan Business, Enterprise On-Ramp ou Enterprise Support, vous pouvez également utiliser l'AWS Support API pour accéder AWS Support et effectuer Trusted Advisor des opérations par programmation. Pour plus d'informations, consultez la référence d'API AWS Support.

> **Note**
>
> Si vous ne parvenez pas à vous connecter au Centre de support, vous pouvez utiliser la page Contactez-nous. Vous pouvez utiliser cette page pour obtenir de l'aide sur les problèmes de facturation et de compte.

AWS compte

Vous pouvez vous connecter au Centre de Support AWS Management Console et y accéder en utilisant l'adresse e-mail et le mot de passe de votre AWS compte. Cette identité est appelée utilisateur root du AWS compte. Toutefois, il est vivement recommandé de ne pas utiliser l'utilisateur racine pour vos tâches quotidiennes, y compris pour les tâches administratives. Nous vous recommandons plutôt d'utiliser IAM, ce qui vous permet de contrôler qui peut effectuer certaines tâches dans votre compte.

AWS actions de soutien

Vous pouvez effectuer les AWS Support actions suivantes dans la console. Vous pouvez également spécifier ces AWS Support actions dans une politique IAM pour autoriser ou refuser des actions spécifiques.

> **Note**
>
> Le refus de l'une des actions ci-dessous dans vos politiques IAM peut entraîner un comportement involontaire dans le Centre de support lors de la création ou de l'interaction avec une demande de support.

Action	Description
`DescribeSupportLevel`	Accorde l'autorisation de renvoyer le niveau de support pour un identificateur de compte AWS . Ceci est utilisé en interne par AWS Support Center pour identifier votre niveau de support.
`InitiateCallForCase`	Accorde l'autorisation de lancer un appel au AWS Support Centre. Il est utilisé en interne par AWS Support Center pour démarrer un appel en votre nom.
`InitiateChatForCase`	Accorde l'autorisation de lancer un appel au centre AWS Support . Ceci est utilisé en interne par AWS Support Center pour démarrer une discussion en votre nom.
`RateCaseCommunication`	Accorde l'autorisation d'évaluer une communica tion AWS Support relative à un dossier.
`DescribeCaseAttributes`	Accorde l'autorisation aux services secondaires de lire des demandes AWS Support . Ceci est utilisé en interne par AWS Support Center pour étiqueter les attributs sur votre dossier.
`DescribeIssueTypes`	Accorde l'autorisation de renvoyer les types de problèmes pour les demandes AWS Support . Il est utilisé en interne par AWS Support Center pour obtenir les types de problèmes disponibles pour votre compte.

Action	Description
`SearchForCases`	Accorde l'autorisation de renvoyer une liste de AWS Support cas correspondant aux entrées données. Ceci est utilisé en interne par le AWS Support Centre pour trouver les cas recherché s.
`PutCaseAttributes`	Accorde l'autorisation d'autoriser les services secondaires à associer des attributs aux AWS Support dossiers. Ceci est utilisé en interne par AWS Support Center pour ajouter des balises opérationnelles à vos AWS Support dossiers.

IAM

Par défaut, les utilisateurs IAM ne peuvent pas accéder au Centre de support. Vous pouvez utiliser IAM pour créer des utilisateurs ou des groupes individuels. Vous associez ensuite des politiques IAM à ces entités, afin qu'elles soient autorisées à effectuer des actions et à accéder aux ressources, par exemple pour ouvrir des dossiers du Support Center et utiliser l' AWS Support API.

Après avoir créé des utilisateurs IAM, vous pouvez leur attribuer des mots de passe individuels et une page de connexion spécifique au compte. Ils peuvent ensuite se connecter à votre AWS compte et travailler dans le Centre de Support. Les utilisateurs IAM qui y ont AWS Support accès peuvent voir tous les dossiers créés pour le compte.

Pour plus d'informations, consultez la section Comment les utilisateurs d'IAM se connectent à votre AWS compte dans le guide de l'utilisateur d'IAM.

Le moyen le plus simple d'accorder des autorisations consiste à associer la politique AWS gérée AWSSupportAccessà l'utilisateur, au groupe ou au rôle. AWS Support autorise des autorisations au niveau de l'action pour contrôler l'accès à des opérations spécifiques AWS Support . AWS Support ne fournit pas d'accès au niveau des ressources, de sorte que l'`Resource`élément est toujours défini sur. * Vous ne pouvez pas autoriser ou refuser l'accès à des demandes de support spécifiques.

Example : Autoriser l'accès à toutes les AWS Support actions

La politique AWS gérée AWSSupportAccessaccorde à un utilisateur IAM l'accès à AWS Support. Un utilisateur IAM doté de cette politique peut accéder à toutes les AWS Support opérations et ressources.

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

Pour plus d'informations sur la façon d'attacher la politique `AWSSupportAccess` à vos entités, consultez Ajout d'autorisations d'identité IAM (console) dans le Guide de l'utilisateur IAM.

Example : autorise l'accès à toutes les actions sauf à l' ResolveCase action

Vous pouvez également créer des politiques gérées par le client dans IAM pour spécifier quelles actions autoriser ou refuser. La déclaration de politique suivante permet à un utilisateur IAM d'effectuer toutes les actions AWS Support sauf de résoudre un dossier.

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

Pour plus d'informations sur la création d'une politique IAM gérée par le client, consultez Création de politiques IAM (console) dans le Guide de l'utilisateur IAM.

Si l'utilisateur ou le groupe dispose déjà d'une politique, vous pouvez ajouter la déclaration de politique AWS Support spécifique à cette stratégie.

> **Important**
>
> - Si vous ne pouvez pas afficher les demandes dans le Centre de support, assurez-vous que vous disposez des autorisations requises. Vous devrez peut-être contacter votre administrateur IAM. Pour plus d'informations, consultez Gestion des identités et des accès pour AWS Support.

Accès à AWS Trusted Advisor

Dans le AWS Management Console, un espace de noms `trustedadvisor` IAM distinct contrôle l'accès à. Trusted Advisor Dans l' AWS Support API, l'espace de noms `support` IAM contrôle l'accès à. Trusted Advisor Pour plus d'informations, consultez Gérez l'accès à AWS Trusted Advisor.

Gérez l'accès aux AWS Support plans

Rubriques

- Autorisations pour la console Support Plans
- Actions Support Plans
- Exemples de politiques IAM pour Support Plans
- Résolution des problèmes

Autorisations pour la console Support Plans

Pour accéder à la console Support Plans, un utilisateur doit disposer d'un ensemble minimum d'autorisations. Ces autorisations doivent permettre à l'utilisateur de répertorier et de visualiser les informations relatives aux ressources Support Plans du Compte AWS.

Vous pouvez créer une politique AWS Identity and Access Management (IAM) avec l'espace de `supportplans` noms. Vous pouvez utiliser cette politique pour préciser des autorisations pour des actions et des ressources.

Lorsque vous créez une politique, vous pouvez spécifier l'espace de noms du service pour autoriser ou refuser une action. L'espace de nom pour Support Plans est `supportplans`.

Vous pouvez utiliser des politiques AWS gérées et les associer à vos entités IAM. Pour plus d'informations, consultez AWS politiques gérées pour les AWS Support plans.

Actions Support Plans

Vous pouvez effectuer les actions Support Plans suivantes dans la console. Vous pouvez également spécifier ces actions Support Plans dans une politique IAM pour autoriser ou refuser des actions spécifiques.

Action	Description
`GetSupportPlan`	Accorde l'autorisation d'afficher des détails sur le plan de support en cours pour ce Compte AWS.
`GetSupportPlanUpdateStatus`	Accorde l'autorisation d'afficher des détails sur l'état d'une demande de mise à jour d'un plan de support.
`StartSupportPlanUpdate`	Accorde l'autorisation de lancer la demande de mise à jour du plan de support pour ce Compte AWS
`CreateSupportPlanSchedule`	Accorde l'autorisation de créer des calendriers de plans de support pour ce Compte AWS.

Exemples de politiques IAM pour Support Plans

Vous pouvez utiliser les exemples de politiques suivants pour gérer l'accès à Support Plans.

Accès complet à Support Plans

La politique suivante autorise un accès complet des utilisateurs à Support Plans.

```
{
    "Version": "2012-10-17",
```

```
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "supportplans:*",
            "Resource": "*"
        }
    ]
}
```

Accès en lecture seule à Support Plans

La politique suivante autorise l'accès en lecture seule à Support Plans.

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

Refuser l'accès à Support Plans

La politique suivante interdit aux utilisateurs l'accès à Support Plans.

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

Résolution des problèmes

Consultez les rubriques suivantes pour gérer l'accès à Support Plans.

Lorsque j'essaie de consulter ou de modifier mon plan de support, la console Support Plans indique que je n'ai pas l'autorisation **`GetSupportPlan`**

Les utilisateurs IAM doivent disposer des autorisations requises pour accéder à la console Support Plans. Vous pouvez mettre à jour votre politique IAM pour inclure l'autorisation manquante ou utiliser une politique gérée par AWS , telle que AWSSupportPlansFullAccess ou AWSSupportPlansReadOnlyAccess. Pour plus d'informations, consultez AWS politiques gérées pour les AWS Support plans.

Si vous n'avez pas accès à la mise à jour de vos politiques IAM, contactez votre administrateur de Compte AWS .

Informations connexes

Pour plus d'informations, consultez les rubriques suivantes dans le Guide de l'utilisateur IAM :

- Test des politiques IAM avec le simulateur de politiques IAM
- Résolution des problèmes liés aux messages d'erreur d'accès rejeté

J'ai les bonnes autorisations Support Plans, mais j'obtiens toujours la même erreur

Si vous Compte AWS êtes membre et que vous en faites partie AWS Organizations, il se peut que la politique de contrôle des services (SCP) doive être mise à jour. Les SCP sont un type de politique qui gère les autorisations dans une organisation.

Comme Support Plans est un service mondial, les politiques qui restreignent les Régions AWS peuvent empêcher les comptes des membres de consulter ou de modifier leur plan de support. Pour autoriser les services mondiaux au sein de votre organisation, tels que IAM et Support Plans, vous devez ajouter le service à la liste d'exclusion de tout SCP applicable. Cela signifie que les comptes de l'organisation peuvent accéder à ces services, même si le SCP refuse un service spécifié Région AWS.

Pour ajouter Support Plans comme exception, entrez `"supportplans:*"` dans la liste `"NotAction"` du SCP.

```
"supportplans:*",
```

Votre SCP peut apparaître sous la forme de l'extrait de politique suivant.

Example : SCP qui autorise l'accès à Support Plans au sein d'une organisation

```
{ "Version":  "2012-10-17",
   "Statement": [
     { "Sid":  "GRREGIONDENY",
       "Effect":  "Deny",
       "NotAction": [
         "aws-portal:*",
         "budgets:*",
         "chime:*"
         "iam:*",
         "supportplans:*",
         ....
```

Si vous possédez un compte membre et que vous ne parvenez pas à mettre à jour le SCP, contactez votre administrateur Compte AWS . Le compte de gestion a peut-être besoin de mettre à jour le SCP afin que tous les comptes membres puissent accéder à Support Plans.

Remarques pour AWS Control Tower

- Si votre organisation utilise un SCP avec AWS Control Tower, vous pouvez mettre à jour le paramètre Refuser l'accès en AWS fonction du Région AWS contrôle demandé (communément appelé contrôle de refus régional).
- Si vous mettez à jour le SCP AWS Control Tower pour autoriser`supportplans`, la réparation de la dérive supprimera votre mise à jour du SCP. Pour plus d'informations, consultez la section Détecter et résoudre le phénomène de dérive AWS Control Tower.

Informations connexes

Pour plus d’informations, consultez les rubriques suivantes :

- Politiques de contrôle des services (SCP) dans le Guide de l'utilisateur AWS Organizations .
- Configurer le contrôle du rejet des régions dans le Guide de l'utilisateur AWS Control Tower
- Refuser l'accès à la AWS base de ce qui est demandé Région AWS dans le guide de AWS Control Tower l'utilisateur

Gérez l'accès à AWS Trusted Advisor

Vous pouvez y accéder AWS Trusted Advisor depuis le AWS Management Console. Tous Comptes AWS ont accès à certains Trusted Advisor contrôles de base. Si vous possédez un plan de support Business, Enterprise On-Ramp ou Enterprise, vous pouvez accéder à toutes les vérifications. Pour plus d'informations, consultez Référence de la vérification AWS Trusted Advisor.

Vous pouvez utiliser AWS Identity and Access Management (IAM) pour contrôler l'accès à Trusted Advisor.

Rubriques

Autorisations pour la console Trusted Advisor

Pour accéder à la Trusted Advisor console, un utilisateur doit disposer d'un ensemble minimal d'autorisations. Ces autorisations doivent permettre à l'utilisateur de répertorier et d'afficher les détails Trusted Advisor des ressources de votre Compte AWS.

Vous pouvez utiliser les options suivantes pour contrôler l'accès à Trusted Advisor:

- Utilisez la fonction de filtre de balises de la Trusted Advisor console. L'utilisateur ou le rôle doit disposer d'autorisations associées aux balises.

  Vous pouvez utiliser des politiques AWS gérées ou des politiques personnalisées pour attribuer des autorisations par balises. Pour plus d'informations, consultez Contrôle de l'accès aux et pour les utilisateurs et rôles IAM à l'aide d'identifications.
- Créez une politique IAM avec l'espace de noms `trustedadvisor`. Vous pouvez utiliser cette politique pour préciser des autorisations pour des actions et des ressources.

Lorsque vous créez une politique, vous pouvez spécifier l'espace de noms du service pour autoriser ou refuser une action. L'espace de noms pour Trusted Advisor est`trustedadvisor`. Toutefois, vous ne pouvez pas utiliser l'espace de `trustedadvisor` noms pour autoriser ou refuser des opérations

Trusted Advisor d'API dans l' AWS Support API. Vous devez utiliser l'espace de noms `support` pour AWS Support , à la place.

> **Note**
>
> Si vous êtes autorisé à accéder à l'AWS SupportAPI, le Trusted Advisor widget qui s'y AWS Management Console trouve affiche une vue récapitulative de vos Trusted Advisor résultats. Pour afficher vos résultats dans la Trusted Advisor console, vous devez être autorisé à accéder à l'espace de `trustedadvisor` noms.

Trusted Advisor actions

Vous pouvez effectuer les Trusted Advisor actions suivantes dans la console. Vous pouvez également spécifier ces Trusted Advisor actions dans une politique IAM pour autoriser ou refuser des actions spécifiques.

Action	Description
`DescribeAccount`	Accorde l'autorisation de consulter le AWS Support plan et les différentes Trusted Advisor préférences.
`DescribeAccountAccess`	Accorde l'autorisation de voir Compte AWS s'il est activé ou désactivé Trusted Advisor.
`DescribeCheckItems`	Octroie l'autorisation d'afficher les détails des éléments de vérification.
`DescribeCheckRefreshStatuses`	Octroie l'autorisation d'afficher les états d'actualisation pour les vérifications Trusted Advisor .
`DescribeCheckSummaries`	Accorde l'autorisation de Trusted Advisor consulter les résumés des chèques.
`DescribeChecks`	Accorde l'autorisation de consulter les détails des Trusted Advisor chèques.

Action	Description
`DescribeNotificationPreferences`	Octroie l'autorisation d'afficher les préférences de notification pour le compte AWS
`ExcludeCheckItems`	Octroie l'autorisation d'exclure des recommandations pour les vérifications Trusted Advisor .
`IncludeCheckItems`	Octroie l'autorisation d'inclure des recommandations pour les vérifications Trusted Advisor .
`RefreshCheck`	Accorde l'autorisation d'actualiser un Trusted Advisor chèque.
`SetAccountAccess`	Accorde l'autorisation d'activer ou Trusted Advisor de désactiver le compte.
`UpdateNotificationPreferences`	Octroie l'autorisation de mettre à jour les préférences de notification pour Trusted Advisor.
`DescribeCheckStatusHistoryChanges`	Octroie l'autorisation d'afficher les résultats et les états modifiés pour les vérifications effectuées au cours des 30 derniers jours.

Trusted Advisor actions pour une vue organisationnelle

Les Trusted Advisor actions suivantes concernent la fonctionnalité d'affichage organisationnel. Pour plus d'informations, consultez Vue organisationnelle pour AWS Trusted Advisor.

Action	Description
`DescribeOrganization`	Accorde l'autorisation de voir s'il Compte AWS répond aux exigences pour activer la fonctionnalité d'affichage organisationnel.

Action	Description
`DescribeOrganizationAccounts`	Accorde l'autorisation de consulter les AWS comptes associés qui se trouvent dans l'organisation.
`DescribeReports`	Octroie l'autorisation d'afficher les détails des rapports de vue organisationnelle, tels que le nom, l'exécution, la date de création, l'état et le format du rapport
`DescribeServiceMetadata`	Accorde l'autorisation de consulter les informations relatives aux rapports d'affichage organisationnels, telles que les Régions AWS catégories de vérifications, les noms des vérifications et les statuts des ressources.
`GenerateReport`	Accorde l'autorisation de créer un rapport pour Trusted Advisor les contrôles dans votre organisation.
`ListAccountsForParent`	Accorde l'autorisation d'afficher, dans la Trusted Advisor console, tous les comptes d'une AWS organisation qui sont contenus par une racine ou une unité organisationnelle (UO).
`ListOrganizationalUnitsForParent`	Accorde l'autorisation d'afficher, dans la Trusted Advisor console, toutes les unités organisationnelles (UO) d'une unité organisationnelle parent ou racine.
`ListRoots`	Accorde l'autorisation d'afficher, dans la Trusted Advisor console, toutes les racines définies dans une AWS organisation.
`SetOrganizationAccess`	Accorde l'autorisation d'activer la fonctionnalité d'affichage organisationnel pour Trusted Advisor.

Trusted Advisor Actions prioritaires

Si la Trusted Advisor priorité est activée pour votre compte, vous pouvez effectuer les Trusted Advisor actions suivantes dans la console. Vous pouvez également ajouter ces actions Trusted Advisor dans une politique IAM pour autoriser ou refuser des actions spécifiques. Pour plus d'informations, consultez Exemples de politique IAM pour Trusted Advisor Priority..

> **Note**
>
> Les risques qui apparaissent dans Trusted Advisor Priority sont des recommandations que votre responsable technique de compte (TAM) a identifiées pour votre compte. Les recommandations d'un service, telles qu'un Trusted Advisor chèque, sont créées automatiquement pour vous. Les recommandations du TAM sont créées manuellement pour vous. Ensuite, votre TAM envoie ces recommandations afin qu'elles apparaissent dans Trusted Advisor Priority pour votre compte.

Pour plus d'informations, consultez Démarrer avec AWS Trusted Advisor Priority.

Action	Description
`DescribeRisks`	Autorise l'affichage des risques dans Trusted Advisor Priority.
`DescribeRisk`	Accorde l'autorisation de consulter les détails des risques dans Trusted Advisor Priority.
`DescribeRiskResources`	Accorde l'autorisation de visualiser les ressources affectées pour un risque dans Trusted Advisor Priority.
`DownloadRisk`	Accorde l'autorisation de télécharger un fichier contenant des informations détaillées sur le risque dans Trusted Advisor Priority.
`UpdateRiskStatus`	Accorde l'autorisation de mettre à jour l'état de risque dans Trusted Advisor Priority.

Action	Description
`DescribeNotificationConfigurations`	Accorde l'autorisation d'obtenir vos préférences de notification par e-mail pour Trusted Advisor Priority.
`UpdateNotificationConfigurations`	Accorde l'autorisation de créer ou mettre à jour vos préférences de notification par e-mail pour Trusted Advisor Priority.
`DeleteNotificationConfigurationForDelegatedAdmin`	Autorise le compte de gestion de l'organisation à supprimer les préférences de notification par e-mail d'un compte d'administrateur délégué pour Trusted Advisor Priority.

Trusted Advisor Engagez des actions

Si Trusted Advisor Engage est activé pour votre compte, vous pouvez effectuer les Trusted Advisor actions suivantes dans la console. Vous pouvez également ajouter ces Trusted Advisor actions dans une politique IAM pour autoriser ou refuser des actions spécifiques. Pour plus d'informations, consultez Exemples de politiques IAM pour Trusted Advisor Engage.

Pour plus d'informations, consultez Commencer avec AWS Trusted Advisor Engage (version préliminaire).

Action	Description
`CreateEngagement`	Accorde l'autorisation de créer un engagement dans Trusted Advisor Engage.
`CreateEngagementAttachment`	Accorde l'autorisation de créer une pièce jointe d'engagement dans Trusted Advisor Engage.
`CreateEngagementCommunication`	Accorde l'autorisation de créer une communication d'engagement dans Trusted Advisor Engage.

Action	Description
`GetEngagement`	Accorde l'autorisation de consulter un engagement dans Trusted Advisor Engage.
`GetEngagementAttachment`	Autorise l'affichage d'une pièce jointe à un engagement dans Trusted Advisor Engage.
`GetEngagementType`	Accorde l'autorisation de consulter un type d'engagement spécifique dans Trusted Advisor Engage.
`ListEngagementCommunications`	Accorde l'autorisation d'afficher toutes les communications d'un engagement dans Trusted Advisor Engage.
`ListEngagements`	Accorde l'autorisation de consulter tous les engagements dans Trusted Advisor Engage.
`ListEngagementTypes`	Accorde l'autorisation d'afficher tous les types d'engagement dans Trusted Advisor Engage.
`UpdateEngagement`	Accorde l'autorisation de mettre à jour les détails d'un engagement dans Trusted Advisor Engage.
`UpdateEngagementStatus`	Accorde l'autorisation de mettre à jour le statut d'un engagement dans Trusted Advisor Engage.

Exemples de politique IAM

Les politiques suivantes vous montrent comment autoriser et refuser l'accès à Trusted Advisor. Vous pouvez utiliser l'une des politiques suivantes pour créer une politique gérée par le client sur la console IAM. Par exemple, vous pouvez copier un exemple de politique, puis la coller dans l'onglet JSON de la console IAM. Vous pouvez ensuite attacher la politique à un utilisateur, un groupe ou un rôle IAM.

Pour de plus amples informations sur la création d'une politique IAM, veuillez consulter Création de politiques IAM (console) dans le Guide de l'utilisateur IAM.

Exemples

- Accès complet à Trusted Advisor
- Accès en lecture seule à Trusted Advisor
- Refuser l'accès à Trusted Advisor
- Autoriser et refuser des actions spécifiques
- Contrôlez l'accès aux opérations de AWS Support l'API pour Trusted Advisor
- Exemples de politique IAM pour Trusted Advisor Priority.
- Exemples de politiques IAM pour Trusted Advisor Engage

Accès complet à Trusted Advisor

La politique suivante permet aux utilisateurs de consulter et de prendre toutes les mesures nécessaires pour toutes les Trusted Advisor vérifications dans la Trusted Advisor console.

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

Accès en lecture seule à Trusted Advisor

La politique suivante autorise les utilisateurs à accéder à la console en lecture seule. Trusted Advisor Les utilisateurs ne peuvent pas apporter de modifications, telles que l'actualisation des contrôles ou les préférences de notification des modifications.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
```

```
            "Action": [
                "trustedadvisor:Describe*",
                "trustedadvisor:Get*",
                "trustedadvisor:List*"
            ],
            "Resource": "*"
        }
    ]
}
```

Refuser l'accès à Trusted Advisor

La politique suivante n'autorise pas les utilisateurs à consulter ou à effectuer des actions pour les Trusted Advisor vérifications dans la Trusted Advisor console.

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

Autoriser et refuser des actions spécifiques

La politique suivante permet aux utilisateurs d'afficher toutes les Trusted Advisor vérifications dans la Trusted Advisor console, mais ne leur permet pas d'actualiser les vérifications.

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

```
        }
    ]
}
```

Contrôlez l'accès aux opérations de AWS Support l'API pour Trusted Advisor

Dans le AWS Management Console, un espace de noms `trustedadvisor` IAM distinct contrôle l'accès à. Trusted Advisor Vous ne pouvez pas utiliser l'espace de `trustedadvisor` noms pour autoriser ou refuser des opérations Trusted Advisor d'API dans l' AWS Support API. Au lieu de cela, vous utilisez l'espace de noms `support`. Vous devez être autorisé à accéder à l' AWS Support API pour effectuer des appels Trusted Advisor par programmation.

Par exemple, si vous souhaitez appeler l'RefreshTrustedAdvisorCheckopération, vous devez disposer des autorisations nécessaires pour cette action dans la politique.

Example : Autoriser uniquement les opérations d' Trusted Advisor API

La politique suivante autorise les utilisateurs à accéder aux opérations d' AWS Support API pour Trusted Advisor, mais pas au reste des opérations d' AWS Support API. Par exemple, les utilisateurs peuvent utiliser l'API pour afficher et actualiser les vérifications. Ils ne peuvent pas créer, consulter, mettre à jour ou résoudre AWS Support des dossiers.

Vous pouvez utiliser cette politique pour appeler les opérations d' Trusted Advisor API par programmation, mais vous ne pouvez pas l'utiliser pour afficher ou actualiser les vérifications dans la Trusted Advisor console.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "support:DescribeTrustedAdvisorCheckRefreshStatuses",
                "support:DescribeTrustedAdvisorCheckResult",
                "support:DescribeTrustedAdvisorChecks",
                "support:DescribeTrustedAdvisorCheckSummaries",
                "support:RefreshTrustedAdvisorCheck",
                "trustedadvisor:Describe*"
            ],
            "Resource": "*"
        },
        {
```

```
            "Effect": "Deny",
            "Action": [
                "support:AddAttachmentsToSet",
                "support:AddCommunicationToCase",
                "support:CreateCase",
                "support:DescribeAttachment",
                "support:DescribeCases",
                "support:DescribeCommunications",
                "support:DescribeServices",
                "support:DescribeSeverityLevels",
                "support:ResolveCase"
            ],
            "Resource": "*"
        }
    ]
}
```

Pour plus d'informations sur le fonctionnement d'IAM avec AWS Support et Trusted Advisor, consultezActions.

Exemples de politique IAM pour Trusted Advisor Priority.

Vous pouvez utiliser les politiques AWS gérées suivantes pour contrôler l'accès à Trusted Advisor Priority. Pour plus d’informations, consultez AWS politiques gérées pour AWS Trusted Advisor et Démarrer avec AWS Trusted Advisor Priority.

Exemples de politiques IAM pour Trusted Advisor Engage

> **Note**
>
> Trusted Advisor Engage est en version préliminaire et ne dispose actuellement d'aucune politique AWS gérée. Vous pouvez utiliser l'une des politiques suivantes pour créer une politique gérée par le client sur la console IAM.

Voici un exemple de politique qui accorde un accès en lecture et en écriture dans Trusted Advisor Engage :

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
```

```
            "Effect": "Allow",
            "Action": [
                "trustedadvisor:CreateEngagement*",
                "trustedadvisor:DescribeAccount*",
                "trustedadvisor:GetEngagement*",
                "trustedadvisor:ListEngagement*",
                "trustedadvisor:UpdateEngagement*"
            ],
            "Resource": "*"
        }
    ]
}
```

Voici un exemple de politique qui accorde un accès en lecture seule dans Trusted Advisor Engage :

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "trustedadvisor:DescribeAccount*",
                "trustedadvisor:GetEngagement*",
                "trustedadvisor:ListEngagement*"
            ],
            "Resource": "*"
        }
    ]
}
```

Exemple de politique qui accorde un accès en lecture et en écriture dans Trusted Advisor Engage et la possibilité de permettre un accès fiable pour Trusted Advisor :

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "organizations:DescribeOrganization",
                "organizations:ListAWSServiceAccessForOrganization",
                "trustedadvisor:CreateEngagement*",
                "trustedadvisor:DescribeAccount*",
```

```
                "trustedadvisor:DescribeOrganization",
                "trustedadvisor:GetEngagement*",
                "trustedadvisor:ListEngagement*",
                "trustedadvisor:SetOrganizationAccess",
                "trustedadvisor:UpdateEngagement*"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "organizations:EnableAWSServiceAccess",
                "organizations:DisableAWSServiceAccess"
            ],
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "organizations:ServicePrincipal": [
                        "reporting.trustedadvisor.amazonaws.com"
                    ]
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": "iam:CreateServiceLinkedRole",
            "Resource": "arn:aws:iam::*:role/aws-service-role/
reporting.trustedadvisor.amazonaws.com/AWSServiceRoleForTrustedAdvisorReporting",
            "Condition": {
                "StringLike": {
                    "iam:AWSServiceName": "reporting.trustedadvisor.amazonaws.com"
                }
            }
        }
    ]
}
```

Consultez aussi

Pour plus d'informations sur Trusted Advisor les autorisations, consultez les ressources suivantes :

- Actions définies par AWS Trusted Advisor dans le Guide de l'utilisateur IAM.
- Contrôle de l'accès à la console Trusted Advisor

Exemples de politiques de contrôle des services pour AWS Trusted Advisor

AWS Trusted Advisor prend en charge les politiques de contrôle des services (SCP). Les SCP sont des politiques que vous attachez aux éléments d'une organisation pour gérer les autorisations au sein de cette organisation. Un SCP s'applique à tous les AWS comptes relevant de l'élément auquel vous attachez le SCP. Les politiques de contrôle des services (SCP) offrent un contrôle central sur les autorisations maximales disponibles pour tous les comptes de votre organisation. Ils peuvent vous aider à garantir que vos AWS comptes respectent les directives de contrôle d'accès de votre organisation. Pour plus d'informations, veuillez consulter Politiques de contrôle de service du Guide de l'utilisateur AWS Organizations .

Rubriques

Prérequis

Procédez comme suit pour utiliser les SCP :

- Activez toutes les fonctions de votre organisation. Pour de plus amples informations, consultez Activation de toutes les fonctionnalités de l'organisation dans le Guide de l'utilisateur AWS Organizations .
- Activez les SCP au sein de votre organisation. Pour plus d'informations, voir la rubrique Activation et désactivation des types des politiques du Guide de l'utilisateur AWS Organizations .
- Créez les SCP dont vous avez besoin. Pour plus d'informations sur la création de SCP, voir la rubrique Création, mise à jour et suppression de politiques de contrôle des services du Guide de l'utilisateur AWS Organizations .

Exemples de politiques de contrôle des services

Les exemples suivants montrent comment contrôler les différents aspects liés au partage des ressources dans une organisation.

Example : Empêcher les utilisateurs de créer ou de modifier des engagements dans Trusted Advisor Engage

La SCP suivante empêche les utilisateurs de créer de nouveaux engagements ou de modifier des engagements existants.

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

Example : refus d' Trusted Advisor engagement et accès Trusted Advisor prioritaire

Le SCP suivant empêche les utilisateurs d'accéder ou d'effectuer des actions dans Trusted Advisor Engage et Trusted Advisor Priority.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Deny",
      "Action": [
        "trustedadvisor:ListEngagement*",
        "trustedadvisor:GetEngagement*",
        "trustedadvisor:CreateEngagement*",
        "trustedadvisor:UpdateEngagement*",
        "trustedadvisor:DescribeRisk*",
        "trustedadvisor:UpdateRisk*",
        "trustedadvisor:DownloadRisk"
      ],
      "Resource": [
        "*"
```

```
      ]
    }
  ]
}
```

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

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

Rubriques

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

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 Support.

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 Support. 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 stratégies 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 Support

Pour autoriser d'autres personnes à accéder AWS Support, vous devez créer une entité IAM (utilisateur ou rôle) pour la personne ou l'application qui a besoin d'un accès. Ils utiliseront les informations d'identification de cette entité pour accéder à AWS. Vous devez ensuite associer une politique à l'entité qui leur accorde les autorisations appropriées dans AWS Support.

Pour démarrer immédiatement, veuillez consulter Création de votre premier groupe et utilisateur délégué IAM dans le Guide de l'utilisateur IAM.

Je souhaite autoriser des personnes extérieures à mon AWS compte à accéder à mes AWS Support 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 (ACL), vous pouvez utiliser ces politiques pour donner l'accès à vos ressources.

Pour en savoir plus, consultez les éléments suivants :

- Pour savoir si ces fonctionnalités sont prises AWS Support en charge, consultezComment AWS Support 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 découvrir quelle est la différence entre l'utilisation des rôles et l'utilisation des politiques basées sur les ressources pour l'accès comptes multiples, veuillez consulter Différence entre les rôles IAM et les politiques basées sur les ressources dans le Guide de l'utilisateur IAM.

Réponse aux incidents

La réponse aux incidents AWS Support est une AWS responsabilité. AWS dispose d'une politique et d'un programme formels et documentés qui régissent la réponse aux incidents. Pour plus d'informations, consultez le livre blanc « Présentation de la réponse aux incidents de AWS sécurité ».

Utilisez les options suivantes pour vous informer sur les problèmes opérationnels :

- Consultez les problèmes AWS opérationnels ayant un large impact sur le AWS Service Health Dashboard. Par exemple, les événements qui affectent un service ou une région qui n'est pas spécifique à votre compte.

- Affichez les problèmes opérationnels pour les comptes individuels dans le AWS Health Dashboard. Par exemple, les événements qui affectent des services ou des ressources de votre compte. Pour plus d'informations, consultez Mise en route avec le AWS Health Dashboard dans le AWS Health Guide de l'utilisateur.

Connexion et surveillance AWS Support et AWS Trusted Advisor

La surveillance joue un rôle important dans le maintien de la fiabilité, de la disponibilité et des performances de AWS Support AWS Trusted Advisor et de vos autres AWS solutions. AWS fournit les outils de surveillance suivants pour surveiller AWS Support et AWS Trusted Advisor 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 flux d'événements système en temps quasi réel qui décrivent les modifications apportées aux AWS ressources. EventBridge permet une informatique automatisée axée sur les événements, car vous pouvez écrire des règles qui surveillent certains événements et déclenchent des actions automatisées dans d'autres AWS services lorsque ces événements se produisent. Pour plus d'informations, consultez le guide de EventBridge l'utilisateur Amazon.
- 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 plus d'informations, consultez le Guide de l'utilisateur AWS CloudTrail.

Pour plus d'informations, consultez Surveillance et journalisation pour AWS Support et Surveillance et journalisation pour AWS Trusted Advisor.

Validation de conformité pour AWS Support

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 :

- Guides de démarrage rapide sur la sécurité et la conformité : ces guides de déploiement abordent les considérations architecturales et indiquent les étapes à suivre pour déployer des environnements de base axés sur AWS la sécurité et la conformité.
- Architecture axée sur la sécurité et la conformité HIPAA sur Amazon Web Services : ce livre blanc décrit comment les entreprises peuvent créer des applications AWS conformes à la loi HIPAA.

  > **Note**
  >
  > Tous ne Services AWS sont pas éligibles à la loi HIPAA. Pour plus d'informations, consultez le HIPAA Eligible Services Reference.

- 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 plusieurs 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.
- 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 Support

L'infrastructure AWS mondiale est construite autour des AWS régions et des zones de disponibilité. AWS Les régions fournissent plusieurs zones de disponibilité physiquement séparées et isolées, connectées par un réseau à faible latence, à haut débit et hautement redondant. Avec les zones de disponibilité, vous pouvez concevoir et exploiter des applications et des bases de données qui basculent automatiquement d'une zone à l'autre sans interruption. Les zones de disponibilité sont davantage disponibles, tolérantes aux pannes et ont une plus grande capacité de mise à l'échelle que les infrastructures traditionnelles à un ou plusieurs centres de données.

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

Sécurité de l'infrastructure dans AWS Support

En tant que service géré, AWS Support 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 Support 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 Support

Pour AWS Trusted Advisor, AWS gère les tâches de sécurité de base telles que l'application de correctifs au système d'exploitation client (OS) et aux bases de données, la configuration du pare-feu et la reprise après sinistre.

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.

Exemples de code pour AWS Support l'utilisation des AWS SDK

Les exemples de code suivants montrent comment utiliser AWS Support un kit de développement AWS logiciel (SDK).

Les actions sont des extraits de code de programmes plus larges et doivent être exécutées dans leur contexte. Alors que les actions vous indiquent comment appeler des fonctions de service individuelles, vous pouvez les voir en contexte dans leurs scénarios associés et dans des exemples interservices.

Les Scénarios sont des exemples de code qui vous montrent comment accomplir une tâche spécifique en appelant plusieurs fonctions au sein d'un même service.

Pour obtenir la liste complète des guides de développement du AWS SDK et des exemples de code, consultezUtilisation de AWS Support avec un kit SDK AWS.. Cette rubrique comprend également des informations sur le démarrage et sur les versions précédentes de SDK.

Mise en route

Bonjour AWS Support

Les exemples de code suivants montrent comment démarrer avec AWS Support.

.NET

AWS SDK for .NET

> **Note**
>
> Il y en a plus à ce sujet GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples de code AWS.

```
using Amazon.AWSSupport;
using Microsoft.Extensions.DependencyInjection;
using Microsoft.Extensions.Hosting;

public static class HelloSupport
```

```
{
    static async Task Main(string[] args)
    {
        // Use the AWS .NET Core Setup package to set up dependency injection for
 the AWS Support service.
        // Use your AWS profile name, or leave it blank to use the default
 profile.
        // You must have one of the following AWS Support plans: Business,
 Enterprise On-Ramp, or Enterprise. Otherwise, an exception will be thrown.
        using var host = Host.CreateDefaultBuilder(args)
            .ConfigureServices((_, services) =>
                services.AddAWSService<IAmazonAWSSupport>()
            ).Build();

        // Now the client is available for injection.
        var supportClient =
 host.Services.GetRequiredService<IAmazonAWSSupport>();

        // You can use await and any of the async methods to get a response.
        var response = await supportClient.DescribeServicesAsync();
        Console.WriteLine($"\tHello AWS Support! There are
 {response.Services.Count} services available.");
    }
}
```

- Pour plus de détails sur l'API, reportez-vous DescribeServicesà la section Référence des AWS SDK for .NET API.

Java

SDK pour Java 2.x

> **Note**
>
> Il y en a plus à ce sujet GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples de code AWS.

```
import software.amazon.awssdk.regions.Region;
import software.amazon.awssdk.services.support.SupportClient;
```

```
import software.amazon.awssdk.services.support.model.Category;
import software.amazon.awssdk.services.support.model.DescribeServicesRequest;
import software.amazon.awssdk.services.support.model.DescribeServicesResponse;
import software.amazon.awssdk.services.support.model.Service;
import software.amazon.awssdk.services.support.model.SupportException;
import java.util.ArrayList;
import java.util.List;

/**
 * Before running this Java (v2) code example, set up your development
 * environment, including your credentials.
 *
 * For more information, see the following documentation topic:
 *
 * https://docs.aws.amazon.com/sdk-for-java/latest/developer-guide/get-
started.html
 *
 * In addition, you must have the AWS Business Support Plan to use the AWS
 * Support Java API. For more information, see:
 *
 * https://aws.amazon.com/premiumsupport/plans/
 *
 * This Java example performs the following task:
 *
 * 1. Gets and displays available services.
 *
 *
 * NOTE: To see multiple operations, see SupportScenario.
 */

public class HelloSupport {
    public static void main(String[] args) {
        Region region = Region.US_WEST_2;
        SupportClient supportClient = SupportClient.builder()
                .region(region)
                .build();

        System.out.println("***** Step 1. Get and display available services.");
        displayServices(supportClient);
    }

    // Return a List that contains a Service name and Category name.
    public static void displayServices(SupportClient supportClient) {
        try {
```

```
            DescribeServicesRequest servicesRequest =
 DescribeServicesRequest.builder()
                    .language("en")
                    .build();

            DescribeServicesResponse response =
 supportClient.describeServices(servicesRequest);
            List<Service> services = response.services();

            System.out.println("Get the first 10 services");
            int index = 1;
            for (Service service : services) {
                if (index == 11)
                    break;

                System.out.println("The Service name is: " + service.name());

                // Display the Categories for this service.
                List<Category> categories = service.categories();
                for (Category cat : categories) {
                    System.out.println("The category name is: " + cat.name());
                }
                index++;
            }

        } catch (SupportException e) {
            System.out.println(e.getLocalizedMessage());
            System.exit(1);
        }
    }
}
```

- Pour plus de détails sur l'API, reportez-vous DescribeServicesà la section Référence des AWS SDK for Java 2.x API.

JavaScript

SDK pour JavaScript (v3)

> **Note**
>
> Il y en a plus à ce sujet GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples de code AWS.

Appelez « main() » pour exécuter l'exemple.

```
import {
  DescribeServicesCommand,
  SupportClient,
} from "@aws-sdk/client-support";

// Change the value of 'region' to your preferred AWS Region.
const client = new SupportClient({ region: "us-east-1" });

const getServiceCount = async () => {
  try {
    const { services } = await client.send(new DescribeServicesCommand({}));
    return services.length;
  } catch (err) {
    if (err.name === "SubscriptionRequiredException") {
      throw new Error(
        "You must be subscribed to the AWS Support plan to use this feature.",
      );
    } else {
      throw err;
    }
  }
};

export const main = async () => {
  try {
    const count = await getServiceCount();
    console.log(`Hello, AWS Support! There are ${count} services available.`);
  } catch (err) {
    console.error("Failed to get service count: ", err.message);
  }
};
```

- Pour plus de détails sur l'API, reportez-vous DescribeServicesà la section Référence des AWS SDK for JavaScript API.

Kotlin

SDK pour Kotlin

> **Note**
>
> Il y en a plus à ce sujet GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples de code AWS.

```
/**
Before running this Kotlin code example, set up your development environment,
including your credentials.

For more information, see the following documentation topic:
https://docs.aws.amazon.com/sdk-for-kotlin/latest/developer-guide/setup.html

In addition, you must have the AWS Business Support Plan to use the AWS Support
 Java API. For more information, see:

https://aws.amazon.com/premiumsupport/plans/

This Kotlin example performs the following task:

1. Gets and displays available services.
 */

suspend fun main() {
    displaySomeServices()
}

// Return a List that contains a Service name and Category name.
suspend fun displaySomeServices() {
    val servicesRequest = DescribeServicesRequest {
        language = "en"
    }
```

```
    SupportClient { region = "us-west-2" }.use { supportClient ->
        val response = supportClient.describeServices(servicesRequest)
        println("Get the first 10 services")
        var index = 1

        response.services?.forEach { service ->
            if (index == 11) {
                return@forEach
            }

            println("The Service name is: " + service.name)

            // Get the categories for this service.
            service.categories?.forEach { cat ->
                println("The category name is ${cat.name}")
                index++
            }
        }
    }
}
```

- Pour plus de détails sur l'API, reportez-vous DescribeServicesà la section AWS SDK pour la référence de l'API Kotlin.

Python

SDK pour Python (Boto3)

> **Note**
>
> Il y en a plus à ce sujet GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples de code AWS.

```
import logging
import boto3
from botocore.exceptions import ClientError
```

```
logger = logging.getLogger(__name__)


def hello_support(support_client):
    """
    Use the AWS SDK for Python (Boto3) to create an AWS Support client and count
    the available services in your account.
    This example uses the default settings specified in your shared credentials
    and config files.

    :param support_client: A Boto3 Support Client object.
    """
    try:
        print("Hello, AWS Support! Let's count the available Support services:")
        response = support_client.describe_services()
        print(f"There are {len(response['services'])} services available.")
    except ClientError as err:
        if err.response["Error"]["Code"] == "SubscriptionRequiredException":
            logger.info(
                "You must have a Business, Enterprise On-Ramp, or Enterprise
 Support "
                "plan to use the AWS Support API. \n\tPlease upgrade your
 subscription to run these "
                "examples."
            )
        else:
            logger.error(
                "Couldn't count services. Here's why: %s: %s",
                err.response["Error"]["Code"],
                err.response["Error"]["Message"],
            )
            raise


if __name__ == "__main__":
    hello_support(boto3.client("support"))
```

- Pour plus de détails sur l'API, consultez DescribeServicesle AWS manuel de référence de l'API SDK for Python (Boto3).

Exemples de code

Actions relatives à AWS Support l'utilisation des AWS SDK

Les exemples de code suivants montrent comment effectuer des AWS Support actions individuelles avec AWS les SDK. Ces extraits appellent l' AWS Support API et sont des extraits de code de programmes plus volumineux qui doivent être exécutés en contexte. Chaque exemple inclut un lien vers GitHub, où vous pouvez trouver des instructions pour configurer et exécuter le code.

Les exemples suivants incluent uniquement les actions les plus couramment utilisées. Pour obtenir la liste complète, veuillez consulter la AWS Support Référence d'API.

Exemples

- Utilisation AddCommunicationToCase avec un AWS SDK ou un outil de ligne de commande
- Utilisation CreateCase avec un AWS SDK ou un outil de ligne de commande
- Utilisation DescribeAttachment avec un AWS SDK ou un outil de ligne de commande
- Utilisation DescribeCases avec un AWS SDK ou un outil de ligne de commande
- Utilisation DescribeCommunications avec un AWS SDK ou un outil de ligne de commande
- Utilisation DescribeServices avec un AWS SDK ou un outil de ligne de commande
- Utilisation DescribeSeverityLevels avec un AWS SDK ou un outil de ligne de commande
- Utilisation DescribeTrustedAdvisorCheckRefreshStatuses avec un AWS SDK ou un outil de ligne de commande
- Utilisation DescribeTrustedAdvisorCheckResult avec un AWS SDK ou un outil de ligne de commande
- Utilisation DescribeTrustedAdvisorCheckSummaries avec un AWS SDK ou un outil de ligne de commande
- Utilisation DescribeTrustedAdvisorChecks avec un AWS SDK ou un outil de ligne de commande
- Utilisation RefreshTrustedAdvisorCheck avec un AWS SDK ou un outil de ligne de commande
- Utilisation ResolveCase avec un AWS SDK ou un outil de ligne de commande

Utilisation **`AddAttachmentsToSet`** avec un AWS SDK ou un outil de ligne de commande

Les exemples de code suivants montrent comment utiliser`AddAttachmentsToSet`.

Les exemples d'actions sont des extraits de code de programmes de plus grande envergure et doivent être exécutés en contexte. Vous pouvez voir cette action en contexte dans l'exemple de code suivant :

- Démarrer avec les dossiers

.NET

AWS SDK for .NET

> **Note**
>
> Il y en a plus à ce sujet GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples de code AWS.

```
   /// <summary>
   /// Add an attachment to a set, or create a new attachment set if one does
not exist.
   /// </summary>
   /// <param name="data">The data for the attachment.</param>
   /// <param name="fileName">The file name for the attachment.</param>
   /// <param name="attachmentSetId">Optional setId for the attachment. Creates
a new attachment set if empty.</param>
   /// <returns>The setId of the attachment.</returns>
   public async Task<string> AddAttachmentToSet(MemoryStream data, string
fileName, string? attachmentSetId = null)
   {
       var response = await _amazonSupport.AddAttachmentsToSetAsync(
           new AddAttachmentsToSetRequest
           {
               AttachmentSetId = attachmentSetId,
               Attachments = new List<Attachment>
               {
                   new Attachment
                   {
                       Data = data,
                       FileName = fileName
                   }
               }
           });
       return response.AttachmentSetId;
   }
```

- Pour plus de détails sur l'API, reportez-vous AddAttachmentsToSetà la section Référence des AWS SDK for .NET API.

Java

SDK pour Java 2.x

> **Note**
>
> Il y en a plus à ce sujet GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples de code AWS.

```
   public static String addAttachment(SupportClient supportClient, String
fileAttachment) {
       try {
           File myFile = new File(fileAttachment);
           InputStream sourceStream = new FileInputStream(myFile);
           SdkBytes sourceBytes = SdkBytes.fromInputStream(sourceStream);

           Attachment attachment = Attachment.builder()
                   .fileName(myFile.getName())
                   .data(sourceBytes)
                   .build();

           AddAttachmentsToSetRequest setRequest =
AddAttachmentsToSetRequest.builder()
                   .attachments(attachment)
                   .build();

           AddAttachmentsToSetResponse response =
supportClient.addAttachmentsToSet(setRequest);
           return response.attachmentSetId();

       } catch (SupportException | FileNotFoundException e) {
           System.out.println(e.getLocalizedMessage());
           System.exit(1);
       }
       return "";
   }
```

- Pour plus de détails sur l'API, reportez-vous AddAttachmentsToSetà la section Référence des AWS SDK for Java 2.x API.

JavaScript

SDK pour JavaScript (v3)

> **Note**
>
> Il y en a plus à ce sujet GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples de code AWS.

```
import { AddAttachmentsToSetCommand } from "@aws-sdk/client-support";

import { client } from "../libs/client.js";

export const main = async () => {
  try {
    // Create a new attachment set or add attachments to an existing set.
    // Provide an 'attachmentSetId' value to add attachments to an existing set.
    // Use AddCommunicationToCase or CreateCase to associate an attachment set
 with a support case.
    const response = await client.send(
      new AddAttachmentsToSetCommand({
        // You can add up to three attachments per set. The size limit is 5 MB
 per attachment.
        attachments: [
          {
            fileName: "example.txt",
            data: new TextEncoder().encode("some example text"),
          },
        ],
      }),
    );
    // Use this ID in AddCommunicationToCase or CreateCase.
    console.log(response.attachmentSetId);
    return response;
  } catch (err) {
    console.error(err);
  }
```

```
};
```

- Pour plus de détails sur l'API, reportez-vous AddAttachmentsToSetà la section Référence des AWS SDK for JavaScript API.

Kotlin

SDK pour Kotlin

> **Note**
>
> Il y en a plus à ce sujet GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples de code AWS.

```
suspend fun addAttachment(fileAttachment: String): String? {
    val myFile = File(fileAttachment)
    val sourceBytes = (File(fileAttachment).readBytes())
    val attachmentVal = Attachment {
        fileName = myFile.name
        data = sourceBytes
    }

    val setRequest = AddAttachmentsToSetRequest {
        attachments = listOf(attachmentVal)
    }

    SupportClient { region = "us-west-2" }.use { supportClient ->
        val response = supportClient.addAttachmentsToSet(setRequest)
        return response.attachmentSetId
    }
}
```

- Pour plus de détails sur l'API, reportez-vous AddAttachmentsToSetà la section AWS SDK pour la référence de l'API Kotlin.

Python

SDK pour Python (Boto3)

> **Note**
>
> Il y en a plus à ce sujet GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples de code AWS.

```
class SupportWrapper:
    """Encapsulates Support actions."""

    def __init__(self, support_client):
        """
        :param support_client: A Boto3 Support client.
        """
        self.support_client = support_client

    @classmethod
    def from_client(cls):
        """
        Instantiates this class from a Boto3 client.
        """
        support_client = boto3.client("support")
        return cls(support_client)


    def add_attachment_to_set(self):
        """
        Add an attachment to a set, or create a new attachment set if one does
 not exist.

        :return: The attachment set ID.
        """
        try:
            response = self.support_client.add_attachments_to_set(
                attachments=[
                    {
                        "fileName": "attachment_file.txt",
                        "data": b"This is a sample file for attachment to a
 support case.",
```

```
                    }
                ]
            )
            new_set_id = response["attachmentSetId"]
        except ClientError as err:
            if err.response["Error"]["Code"] == "SubscriptionRequiredException":
                logger.info(
                    "You must have a Business, Enterprise On-Ramp, or Enterprise
Support "
                    "plan to use the AWS Support API. \n\tPlease upgrade your
subscription to run these "
                    "examples."
                )
            else:
                logger.error(
                    "Couldn't add attachment. Here's why: %s: %s",
                    err.response["Error"]["Code"],
                    err.response["Error"]["Message"],
                )
                raise
        else:
            return new_set_id
```

- Pour plus de détails sur l'API, consultez AddAttachmentsToSetle AWS manuel de référence de l'API SDK for Python (Boto3).

Pour obtenir la liste complète des guides de développement du AWS SDK et des exemples de code, consultezUtilisation de AWS Support avec un kit SDK AWS.. Cette rubrique comprend également des informations sur le démarrage et sur les versions précédentes de SDK.

Utilisation **`AddCommunicationToCase`** avec un AWS SDK ou un outil de ligne de commande

Les exemples de code suivants montrent comment utiliser`AddCommunicationToCase`.

Les exemples d’actions sont des extraits de code de programmes de plus grande envergure et doivent être exécutés en contexte. Vous pouvez voir cette action en contexte dans l’exemple de code suivant :

- Démarrer avec les dossiers

.NET

AWS SDK for .NET

> **Note**
>
> Il y en a plus à ce sujet GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples de code AWS.

```
    /// <summary>
    /// Add communication to a case, including optional attachment set ID and CC
 email addresses.
    /// </summary>
    /// <param name="caseId">Id for the support case.</param>
    /// <param name="body">Body text of the communication.</param>
    /// <param name="attachmentSetId">Optional Id for an attachment set.</param>
    /// <param name="ccEmailAddresses">Optional list of CC email addresses.</
param>
    /// <returns>True if successful.</returns>
    public async Task<bool> AddCommunicationToCase(string caseId, string body,
        string? attachmentSetId = null, List<string>? ccEmailAddresses = null)
    {
        var response = await _amazonSupport.AddCommunicationToCaseAsync(
            new AddCommunicationToCaseRequest()
            {
                CaseId = caseId,
                CommunicationBody = body,
                AttachmentSetId = attachmentSetId,
                CcEmailAddresses = ccEmailAddresses
            });
        return response.Result;
    }
```

- Pour plus de détails sur l'API, reportez-vous AddCommunicationToCaseà la section Référence des AWS SDK for .NET API.

Java

SDK pour Java 2.x

> **Note**
>
> Il y en a plus à ce sujet GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples de code AWS.

```
   public static void addAttachSupportCase(SupportClient supportClient, String
caseId, String attachmentSetId) {
       try {
           AddCommunicationToCaseRequest caseRequest =
AddCommunicationToCaseRequest.builder()
                   .caseId(caseId)
                   .attachmentSetId(attachmentSetId)
                   .communicationBody("Please refer to attachment for details.")
                   .build();

           AddCommunicationToCaseResponse response =
supportClient.addCommunicationToCase(caseRequest);
           if (response.result())
               System.out.println("You have successfully added a communication
to an AWS Support case");
           else
               System.out.println("There was an error adding the communication
to an AWS Support case");

       } catch (SupportException e) {
           System.out.println(e.getLocalizedMessage());
           System.exit(1);
       }
   }
```

- Pour plus de détails sur l'API, reportez-vous AddCommunicationToCaseà la section Référence des AWS SDK for Java 2.x API.

JavaScript

SDK pour JavaScript (v3)

> **Note**
>
> Il y en a plus à ce sujet GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples de code AWS.

```
import { AddCommunicationToCaseCommand } from "@aws-sdk/client-support";

import { client } from "../libs/client.js";

export const main = async () => {
  let attachmentSetId;

  try {
    // Add a communication to a case.
    const response = await client.send(
      new AddCommunicationToCaseCommand({
        communicationBody: "Adding an attachment.",
        // Set value to an existing support case id.
        caseId: "CASE_ID",
        // Optional. Set value to an existing attachment set id to add
 attachments to the case.
        attachmentSetId,
      }),
    );
    console.log(response);
    return response;
  } catch (err) {
    console.error(err);
  }
};
```

- Pour plus de détails sur l'API, reportez-vous AddCommunicationToCaseà la section Référence des AWS SDK for JavaScript API.

Kotlin

SDK pour Kotlin

> **Note**
>
> Il y en a plus à ce sujet GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples de code AWS.

```
suspend fun addAttachSupportCase(caseIdVal: String?, attachmentSetIdVal: String?)
 {
    val caseRequest = AddCommunicationToCaseRequest {
        caseId = caseIdVal
        attachmentSetId = attachmentSetIdVal
        communicationBody = "Please refer to attachment for details."
    }

    SupportClient { region = "us-west-2" }.use { supportClient ->
        val response = supportClient.addCommunicationToCase(caseRequest)
        if (response.result) {
            println("You have successfully added a communication to an AWS
 Support case")
        } else {
            println("There was an error adding the communication to an AWS
 Support case")
        }
    }
}
```

- Pour plus de détails sur l'API, reportez-vous AddCommunicationToCaseà la section AWS SDK pour la référence de l'API Kotlin.

Python

SDK pour Python (Boto3)

> **Note**
>
> Il y en a plus à ce sujet GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples de code AWS.

```
class SupportWrapper:
    """Encapsulates Support actions."""

    def __init__(self, support_client):
        """
        :param support_client: A Boto3 Support client.
        """
        self.support_client = support_client

    @classmethod
    def from_client(cls):
        """
        Instantiates this class from a Boto3 client.
        """
        support_client = boto3.client("support")
        return cls(support_client)


    def add_communication_to_case(self, attachment_set_id, case_id):
        """
        Add a communication and an attachment set to a case.

        :param attachment_set_id: The ID of an existing attachment set.
        :param case_id: The ID of the case.
        """
        try:
            self.support_client.add_communication_to_case(
                caseId=case_id,
                communicationBody="This is an example communication added to a
 support case.",
                attachmentSetId=attachment_set_id,
            )
```

```
        except ClientError as err:
            if err.response["Error"]["Code"] == "SubscriptionRequiredException":
                logger.info(
                    "You must have a Business, Enterprise On-Ramp, or Enterprise
Support "
                    "plan to use the AWS Support API. \n\tPlease upgrade your
subscription to run these "
                    "examples."
                )
            else:
                logger.error(
                    "Couldn't add communication. Here's why: %s: %s",
                    err.response["Error"]["Code"],
                    err.response["Error"]["Message"],
                )
                raise
```

- Pour plus de détails sur l'API, consultez AddCommunicationToCasele AWS manuel de référence de l'API SDK for Python (Boto3).

Pour obtenir la liste complète des guides de développement du AWS SDK et des exemples de code, consultezUtilisation de AWS Support avec un kit SDK AWS.. Cette rubrique comprend également des informations sur le démarrage et sur les versions précédentes de SDK.

Utilisation **`CreateCase`** avec un AWS SDK ou un outil de ligne de commande

Les exemples de code suivants montrent comment utiliser`CreateCase`.

Les exemples d'actions sont des extraits de code de programmes de plus grande envergure et doivent être exécutés en contexte. Vous pouvez voir cette action en contexte dans l'exemple de code suivant :

- Démarrer avec les dossiers

.NET

AWS SDK for .NET

> **Note**
>
> Il y en a plus à ce sujet GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples de code AWS.

```
   /// <summary>
   /// Create a new support case.
   /// </summary>
   /// <param name="serviceCode">Service code for the new case.</param>
   /// <param name="categoryCode">Category for the new case.</param>
   /// <param name="severityCode">Severity code for the new case.</param>
   /// <param name="subject">Subject of the new case.</param>
   /// <param name="body">Body text of the new case.</param>
   /// <param name="language">Optional language support for your case.
   /// Currently Chinese (“zh”), English ("en"), Japanese ("ja") and Korean
(“ko”) are supported.</param>
   /// <param name="attachmentSetId">Optional Id for an attachment set for the
new case.</param>
   /// <param name="issueType">Optional issue type for the new case. Options are
"customer-service" or "technical".</param>
   /// <returns>The caseId of the new support case.</returns>
   public async Task<string> CreateCase(string serviceCode, string categoryCode,
string severityCode, string subject,
       string body, string language = "en", string? attachmentSetId = null,
string issueType = "customer-service")
   {
       var response = await _amazonSupport.CreateCaseAsync(
           new CreateCaseRequest()
           {
               ServiceCode = serviceCode,
               CategoryCode = categoryCode,
               SeverityCode = severityCode,
               Subject = subject,
               Language = language,
               AttachmentSetId = attachmentSetId,
               IssueType = issueType,
```

```
                CommunicationBody = body
            });
        return response.CaseId;
    }
```

- Pour plus de détails sur l'API, reportez-vous CreateCaseà la section Référence des AWS SDK for .NET API.

CLI

AWS CLI

Pour créer un dossier

L'`create-case`exemple suivant crée une demande d'assistance pour votre AWS compte.

```
aws support create-case \
    --category-code "using-aws" \
    --cc-email-addresses "myemail@example.com" \
    --communication-body "I want to learn more about an AWS service." \
    --issue-type "technical" \
    --language "en" \
    --service-code "general-info" \
    --severity-code "low" \
    --subject "Question about my account"
```

Sortie :

```
{
    "caseId": "case-12345678910-2013-c4c1d2bf33c5cf47"
}
```

Pour plus d'informations, consultez la section Gestion des dossiers dans le Guide de l'utilisateur du AWS Support.

- Pour plus de détails sur l'API, reportez-vous CreateCaseà la section Référence des AWS CLI commandes.

Java

SDK pour Java 2.x

> **Note**
>
> Il y en a plus à ce sujet GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples de code AWS.

```
   public static String createSupportCase(SupportClient supportClient,
List<String> sevCatList, String sevLevel) {
       try {
           String serviceCode = sevCatList.get(0);
           String caseCat = sevCatList.get(1);
           CreateCaseRequest caseRequest = CreateCaseRequest.builder()
                   .categoryCode(caseCat.toLowerCase())
                   .serviceCode(serviceCode.toLowerCase())
                   .severityCode(sevLevel.toLowerCase())
                   .communicationBody("Test issue with " +
serviceCode.toLowerCase())
                   .subject("Test case, please ignore")
                   .language("en")
                   .issueType("technical")
                   .build();

           CreateCaseResponse response = supportClient.createCase(caseRequest);
           return response.caseId();

       } catch (SupportException e) {
           System.out.println(e.getLocalizedMessage());
           System.exit(1);
       }
       return "";
   }
```

- Pour plus de détails sur l'API, reportez-vous CreateCaseà la section Référence des AWS SDK for Java 2.x API.

JavaScript

SDK pour JavaScript (v3)

> **Note**
>
> Il y en a plus à ce sujet GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples de code AWS.

```
import { CreateCaseCommand } from "@aws-sdk/client-support";

import { client } from "../libs/client.js";

export const main = async () => {
  try {
    // Create a new case and log the case id.
    // Important: This creates a real support case in your account.
    const response = await client.send(
      new CreateCaseCommand({
        // The subject line of the case.
        subject: "IGNORE: Test case",
        // Use DescribeServices to find available service codes for each service.
        serviceCode: "service-quicksight-end-user",
        // Use DescribeSecurityLevels to find available severity codes for your
 support plan.
        severityCode: "low",
        // Use DescribeServices to find available category codes for each
 service.
        categoryCode: "end-user-support",
        // The main description of the support case.
        communicationBody: "This is a test. Please ignore.",
      }),
    );
    console.log(response.caseId);
    return response;
  } catch (err) {
    console.error(err);
  }
};
```

- Pour plus de détails sur l'API, reportez-vous CreateCaseà la section Référence des AWS SDK for JavaScript API.

Kotlin

SDK pour Kotlin

> **Note**
>
> Il y en a plus à ce sujet GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples de code AWS.

```
suspend fun createSupportCase(sevCatListVal: List<String>, sevLevelVal: String):
 String? {
    val serCode = sevCatListVal[0]
    val caseCategory = sevCatListVal[1]
    val caseRequest = CreateCaseRequest {
        categoryCode = caseCategory.lowercase(Locale.getDefault())
        serviceCode = serCode.lowercase(Locale.getDefault())
        severityCode = sevLevelVal.lowercase(Locale.getDefault())
        communicationBody = "Test issue with
 ${serCode.lowercase(Locale.getDefault())}"
        subject = "Test case, please ignore"
        language = "en"
        issueType = "technical"
    }

    SupportClient { region = "us-west-2" }.use { supportClient ->
        val response = supportClient.createCase(caseRequest)
        return response.caseId
    }
}
```

- Pour plus de détails sur l'API, reportez-vous CreateCaseà la section AWS SDK pour la référence de l'API Kotlin.

PowerShell

Outils pour PowerShell

Exemple 1 : crée un nouveau dossier dans le AWS Support Center. Les valeurs des CategoryCode paramètres - ServiceCode et - peuvent être obtenues à l'aide de l'applet de commande Get-AsaService. La valeur du SeverityCode paramètre - peut être obtenue à l'aide de l'applet de commande Get-ASASeverityLevel . La valeur du IssueType paramètre - peut être « service client » ou « technique ». En cas de succès, le numéro de dossier de AWS support est affiché. Par défaut, le dossier sera traité en anglais. Pour utiliser le japonais, ajoutez le paramètre -Language « ja ». Les CommunicationBody paramètres -ServiceCode, -CategoryCode, -Subject et - sont obligatoires.

```
New-ASACase -ServiceCode "amazon-cloudfront" -CategoryCode "APIs" -SeverityCode
 "low" -Subject "subject text" -CommunicationBody "description of the case" -
CcEmailAddress @("email1@domain.com", "email2@domain.com") -IssueType "technical"
```

- Pour plus de détails sur l'API, reportez-vous CreateCaseà la section Référence des AWS Tools for PowerShell applets de commande.

Python

SDK pour Python (Boto3)

> **Note**
>
> Il y en a plus à ce sujet GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples de code AWS.

```
class SupportWrapper:
    """Encapsulates Support actions."""

    def __init__(self, support_client):
        """
        :param support_client: A Boto3 Support client.
        """
        self.support_client = support_client

    @classmethod
```

```
    def from_client(cls):
        """
        Instantiates this class from a Boto3 client.
        """
        support_client = boto3.client("support")
        return cls(support_client)


    def create_case(self, service, category, severity):
        """
        Create a new support case.

        :param service: The service to use for the new case.
        :param category: The category to use for the new case.
        :param severity: The severity to use for the new case.
        :return: The caseId of the new case.
        """
        try:
            response = self.support_client.create_case(
                subject="Example case for testing, ignore.",
                serviceCode=service["code"],
                severityCode=severity["code"],
                categoryCode=category["code"],
                communicationBody="Example support case body.",
                language="en",
                issueType="customer-service",
            )
            case_id = response["caseId"]
        except ClientError as err:
            if err.response["Error"]["Code"] == "SubscriptionRequiredException":
                logger.info(
                    "You must have a Business, Enterprise On-Ramp, or Enterprise
Support "
                    "plan to use the AWS Support API. \n\tPlease upgrade your
subscription to run these "
                    "examples."
                )
            else:
                logger.error(
                    "Couldn't create case. Here's why: %s: %s",
                    err.response["Error"]["Code"],
                    err.response["Error"]["Message"],
                )
                raise
```

```
        else:
            return case_id
```

- Pour plus de détails sur l'API, consultez CreateCasele AWS manuel de référence de l'API SDK for Python (Boto3).

Pour obtenir la liste complète des guides de développement du AWS SDK et des exemples de code, consultezUtilisation de AWS Support avec un kit SDK AWS.. Cette rubrique comprend également des informations sur le démarrage et sur les versions précédentes de SDK.

Utilisation **`DescribeAttachment`** avec un AWS SDK ou un outil de ligne de commande

Les exemples de code suivants montrent comment utiliser`DescribeAttachment`.

Les exemples d'actions sont des extraits de code de programmes de plus grande envergure et doivent être exécutés en contexte. Vous pouvez voir cette action en contexte dans l'exemple de code suivant :

- Démarrer avec les dossiers

.NET

AWS SDK for .NET

> **Note**
>
> Il y en a plus à ce sujet GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples de code AWS.

```
    /// <summary>
    /// Get description of a specific attachment.
    /// </summary>
    /// <param name="attachmentId">Id of the attachment, usually fetched by
describing the communications of a case.</param>
```

```
    /// <returns>The attachment object.</returns>
    public async Task<Attachment> DescribeAttachment(string attachmentId)
    {
        var response = await _amazonSupport.DescribeAttachmentAsync(
            new DescribeAttachmentRequest()
            {
                AttachmentId = attachmentId
            });
        return response.Attachment;
    }
```

- Pour plus de détails sur l'API, reportez-vous DescribeAttachmentà la section Référence des AWS SDK for .NET API.

CLI

AWS CLI

Pour décrire une pièce jointe

L'`describe-attachment`exemple suivant renvoie des informations sur la pièce jointe avec l'ID spécifié.

```
aws support describe-attachment \
    --attachment-id "attachment-KBnjRNrePd9D6Jx0-Mm00xZuDEaL2JAj_0-
gJv9qqDooTipsz3V1Nb19rCfkZneeQeDPgp8X1iVJyHH7UuhZDdNeqGoduZsPrAhyMakqlc60-
iJjL5HqyYGiT1FG8EXAMPLE"
```

Sortie :

```
{
    "attachment": {
        "fileName": "troubleshoot-screenshot.png",
        "data": "base64-blob"
    }
}
```

Pour plus d'informations, consultez la section Gestion des dossiers dans le Guide de l'utilisateur du AWS Support.

- Pour plus de détails sur l'API, reportez-vous DescribeAttachmentà la section Référence des AWS CLI commandes.

Java

SDK pour Java 2.x

> **Note**
>
> Il y en a plus à ce sujet GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples de code AWS.

```
   public static void describeAttachment(SupportClient supportClient, String
attachId) {
       try {
           DescribeAttachmentRequest attachmentRequest =
DescribeAttachmentRequest.builder()
                   .attachmentId(attachId)
                   .build();

           DescribeAttachmentResponse response =
supportClient.describeAttachment(attachmentRequest);
           System.out.println("The name of the file is " +
response.attachment().fileName());

       } catch (SupportException e) {
           System.out.println(e.getLocalizedMessage());
           System.exit(1);
       }
   }
```

- Pour plus de détails sur l'API, reportez-vous DescribeAttachmentà la section Référence des AWS SDK for Java 2.x API.

JavaScript

SDK pour JavaScript (v3)

> **Note**
>
> Il y en a plus à ce sujet GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples de code AWS.

```
import { DescribeAttachmentCommand } from "@aws-sdk/client-support";

import { client } from "../libs/client.js";

export const main = async () => {
  try {
    // Get the metadata and content of an attachment.
    const response = await client.send(
      new DescribeAttachmentCommand({
        // Set value to an existing attachment id.
        // Use DescribeCommunications or DescribeCases to find an attachment id.
        attachmentId: "ATTACHMENT_ID",
      }),
    );
    console.log(response.attachment?.fileName);
    return response;
  } catch (err) {
    console.error(err);
  }
};
```

- Pour plus de détails sur l'API, reportez-vous DescribeAttachmentà la section Référence des AWS SDK for JavaScript API.

Kotlin

SDK pour Kotlin

> **Note**
>
> Il y en a plus à ce sujet GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples de code AWS.

```
suspend fun describeAttachment(attachId: String?) {
    val attachmentRequest = DescribeAttachmentRequest {
        attachmentId = attachId
    }

    SupportClient { region = "us-west-2" }.use { supportClient ->
        val response = supportClient.describeAttachment(attachmentRequest)
        println("The name of the file is ${response.attachment?.fileName}")
    }
}
```

- Pour plus de détails sur l'API, reportez-vous DescribeAttachmentà la section AWS SDK pour la référence de l'API Kotlin.

Python

SDK pour Python (Boto3)

> **Note**
>
> Il y en a plus à ce sujet GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples de code AWS.

```
class SupportWrapper:
    """Encapsulates Support actions."""

    def __init__(self, support_client):
        """
```

```
        :param support_client: A Boto3 Support client.
        """
        self.support_client = support_client

    @classmethod
    def from_client(cls):
        """
        Instantiates this class from a Boto3 client.
        """
        support_client = boto3.client("support")
        return cls(support_client)


    def describe_attachment(self, attachment_id):
        """
        Get information about an attachment by its attachmentID.

        :param attachment_id: The ID of the attachment.
        :return: The name of the attached file.
        """
        try:
            response = self.support_client.describe_attachment(
                attachmentId=attachment_id
            )
            attached_file = response["attachment"]["fileName"]
        except ClientError as err:
            if err.response["Error"]["Code"] == "SubscriptionRequiredException":
                logger.info(
                    "You must have a Business, Enterprise On-Ramp, or Enterprise
Support "
                    "plan to use the AWS Support API. \n\tPlease upgrade your
subscription to run these "
                    "examples."
                )
            else:
                logger.error(
                    "Couldn't get attachment description. Here's why: %s: %s",
                    err.response["Error"]["Code"],
                    err.response["Error"]["Message"],
                )
                raise
        else:
            return attached_file
```

- Pour plus de détails sur l'API, consultez DescribeAttachmentle AWS manuel de référence de l'API SDK for Python (Boto3).

Pour obtenir la liste complète des guides de développement du AWS SDK et des exemples de code, consultezUtilisation de AWS Support avec un kit SDK AWS.. Cette rubrique comprend également des informations sur le démarrage et sur les versions précédentes de SDK.

Utilisation **`DescribeCases`** avec un AWS SDK ou un outil de ligne de commande

Les exemples de code suivants montrent comment utiliser`DescribeCases`.

Les exemples d'actions sont des extraits de code de programmes de plus grande envergure et doivent être exécutés en contexte. Vous pouvez voir cette action en contexte dans l'exemple de code suivant :

- Démarrer avec les dossiers

.NET

AWS SDK for .NET

> **Note**
>
> Il y en a plus sur GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples de code AWS.

```
    /// <summary>
    /// Get case details for a list of case ids, optionally with date filters.
    /// </summary>
    /// <param name="caseIds">The list of case IDs.</param>
    /// <param name="displayId">Optional display ID.</param>
    /// <param name="includeCommunication">True to include communication.
Defaults to true.</param>
```

```
    /// <param name="includeResolvedCases">True to include resolved cases.
 Defaults to false.</param>
    /// <param name="afterTime">The optional start date for a filtered search.</
param>
    /// <param name="beforeTime">The optional end date for a filtered search.</
param>
    /// <param name="language">Optional language support for your case.
    /// Currently Chinese (“zh”), English ("en"), Japanese ("ja") and Korean
 (“ko”) are supported.</param>
    /// <returns>A list of CaseDetails.</returns>
    public async Task<List<CaseDetails>> DescribeCases(List<string> caseIds,
 string? displayId = null, bool includeCommunication = true,
        bool includeResolvedCases = false, DateTime? afterTime = null, DateTime?
 beforeTime = null,
        string language = "en")
    {
        var results = new List<CaseDetails>();
        var paginateCases = _amazonSupport.Paginators.DescribeCases(
            new DescribeCasesRequest()
            {
                CaseIdList = caseIds,
                DisplayId = displayId,
                IncludeCommunications = includeCommunication,
                IncludeResolvedCases = includeResolvedCases,
                AfterTime = afterTime?.ToString("s"),
                BeforeTime = beforeTime?.ToString("s"),
                Language = language
            });
        // Get the entire list using the paginator.
        await foreach (var cases in paginateCases.Cases)
        {
            results.Add(cases);
        }
        return results;
    }
```

- Pour plus de détails sur l'API, reportez-vous DescribeCasesà la section Référence des AWS SDK for .NET API.

CLI

AWS CLI

Pour décrire un cas

L'`describe-cases`exemple suivant renvoie des informations sur le dossier d'assistance spécifié dans votre AWS compte.

```
aws support describe-cases \
    --display-id "1234567890" \
    --after-time "2020-03-23T21:31:47.774Z" \
    --include-resolved-cases \
    --language "en" \
    --no-include-communications \
    --max-item 1
```

Sortie :

```
{
    "cases": [
        {
            "status": "resolved",
            "ccEmailAddresses": [],
            "timeCreated": "2020-03-23T21:31:47.774Z",
            "caseId": "case-12345678910-2013-c4c1d2bf33c5cf47",
            "severityCode": "low",
            "language": "en",
            "categoryCode": "using-aws",
            "serviceCode": "general-info",
            "submittedBy": "myemail@example.com",
            "displayId": "1234567890",
            "subject": "Question about my account"
        }
    ]
}
```

Pour plus d'informations, consultez la section Gestion des dossiers dans le Guide de l'utilisateur du AWS Support.

- Pour plus de détails sur l'API, reportez-vous DescribeCasesà la section Référence des AWS CLI commandes.

Java

SDK pour Java 2.x

> **Note**
>
> Il y en a plus sur GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples de code AWS.

```
   public static void getOpenCase(SupportClient supportClient) {
       try {
           // Specify the start and end time.
           Instant now = Instant.now();
           java.time.LocalDate.now();
           Instant yesterday = now.minus(1, ChronoUnit.DAYS);

           DescribeCasesRequest describeCasesRequest =
DescribeCasesRequest.builder()
                   .maxResults(20)
                   .afterTime(yesterday.toString())
                   .beforeTime(now.toString())
                   .build();

           DescribeCasesResponse response =
supportClient.describeCases(describeCasesRequest);
           List<CaseDetails> cases = response.cases();
           for (CaseDetails sinCase : cases) {
               System.out.println("The case status is " + sinCase.status());
               System.out.println("The case Id is " + sinCase.caseId());
               System.out.println("The case subject is " + sinCase.subject());
           }

       } catch (SupportException e) {
           System.out.println(e.getLocalizedMessage());
           System.exit(1);
       }
   }
```

- Pour plus de détails sur l'API, reportez-vous DescribeCasesà la section Référence des AWS SDK for Java 2.x API.

JavaScript

SDK pour JavaScript (v3)

> **Note**
>
> Il y en a plus sur GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples de code AWS.

```
import { DescribeCasesCommand } from "@aws-sdk/client-support";

import { client } from "../libs/client.js";

export const main = async () => {
  try {
    // Get all of the unresolved cases in your account.
    // Filter or expand results by providing parameters to the
 DescribeCasesCommand. Refer
    // to the TypeScript definition and the API doc for more information on
 possible parameters.
    // https://docs.aws.amazon.com/AWSJavaScriptSDK/v3/latest/clients/client-
support/interfaces/describecasescommandinput.html
    const response = await client.send(new DescribeCasesCommand({}));
    const caseIds = response.cases.map((supportCase) => supportCase.caseId);
    console.log(caseIds);
    return response;
  } catch (err) {
    console.error(err);
  }
};
```

- Pour plus de détails sur l'API, reportez-vous DescribeCasesà la section Référence des AWS SDK for JavaScript API.

Kotlin

SDK pour Kotlin

> **Note**
>
> Il y en a plus sur GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples de code AWS.

```
suspend fun getOpenCase() {
    // Specify the start and end time.
    val now = Instant.now()
    LocalDate.now()
    val yesterday = now.minus(1, ChronoUnit.DAYS)
    val describeCasesRequest = DescribeCasesRequest {
        maxResults = 20
        afterTime = yesterday.toString()
        beforeTime = now.toString()
    }

    SupportClient { region = "us-west-2" }.use { supportClient ->
        val response = supportClient.describeCases(describeCasesRequest)
        response.cases?.forEach { sinCase ->
            println("The case status is ${sinCase.status}")
            println("The case Id is ${sinCase.caseId}")
            println("The case subject is ${sinCase.subject}")
        }
    }
}
```

- Pour plus de détails sur l'API, reportez-vous DescribeCasesà la section AWS SDK pour la référence de l'API Kotlin.

PowerShell

Outils pour PowerShell

Exemple 1 : renvoie les détails de tous les dossiers de support.

```
Get-ASACase
```

Exemple 2 : renvoie les détails de tous les dossiers de support depuis la date et l'heure spécifiées.

```
Get-ASACase -AfterTime "2013-09-10T03:06Z"
```

Exemple 3 : renvoie les détails des 10 premiers cas de support, y compris ceux qui ont été résolus.

```
Get-ASACase -MaxResult 10 -IncludeResolvedCases $true
```

Exemple 4 : renvoie les détails de l'unique dossier de support spécifié.

```
Get-ASACase -CaseIdList "case-12345678910-2013-c4c1d2bf33c5cf47"
```

Exemple 5 : renvoie les détails des demandes de support spécifiées.

```
Get-ASACase -CaseIdList @("case-12345678910-2013-c4c1d2bf33c5cf47",
 "case-18929034710-2011-c4fdeabf33c5cf47")
```

Exemple 6 : renvoie tous les dossiers de support à l'aide de la pagination manuelle. Les étuis sont récupérés par lots de 20.

```
$nextToken = $null
do {
  Get-ASACase -NextToken $nextToken -MaxResult 20
  $nextToken = $AWSHistory.LastServiceResponse.NextToken
} while ($nextToken -ne $null)
```

- Pour plus de détails sur l'API, reportez-vous DescribeCasesà la section Référence des AWS Tools for PowerShell applets de commande.

Python

SDK pour Python (Boto3)

> **Note**
>
> Il y en a plus sur GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples de code AWS.

```
class SupportWrapper:
    """Encapsulates Support actions."""

    def __init__(self, support_client):
        """
        :param support_client: A Boto3 Support client.
        """
        self.support_client = support_client

    @classmethod
    def from_client(cls):
        """
        Instantiates this class from a Boto3 client.
        """
        support_client = boto3.client("support")
        return cls(support_client)


    def describe_cases(self, after_time, before_time, resolved):
        """
        Describe support cases over a period of time, optionally filtering
        by status.

        :param after_time: The start time to include for cases.
        :param before_time: The end time to include for cases.
        :param resolved: True to include resolved cases in the results,
            otherwise results are open cases.
        :return: The final status of the case.
        """
        try:
            cases = []
            paginator = self.support_client.get_paginator("describe_cases")
```

```
            for page in paginator.paginate(
                afterTime=after_time,
                beforeTime=before_time,
                includeResolvedCases=resolved,
                language="en",
            ):
                cases += page["cases"]
        except ClientError as err:
            if err.response["Error"]["Code"] == "SubscriptionRequiredException":
                logger.info(
                    "You must have a Business, Enterprise On-Ramp, or Enterprise
Support "
                    "plan to use the AWS Support API. \n\tPlease upgrade your
subscription to run these "
                    "examples."
                )
            else:
                logger.error(
                    "Couldn't describe cases. Here's why: %s: %s",
                    err.response["Error"]["Code"],
                    err.response["Error"]["Message"],
                )
                raise
        else:
            if resolved:
                cases = filter(lambda case: case["status"] == "resolved", cases)
            return cases
```

- Pour plus de détails sur l'API, consultez DescribeCasesle AWS manuel de référence de l'API SDK for Python (Boto3).

Pour obtenir la liste complète des guides de développement du AWS SDK et des exemples de code, consultezUtilisation de AWS Support avec un kit SDK AWS.. Cette rubrique comprend également des informations sur le démarrage et sur les versions précédentes de SDK.

Utilisation **`DescribeCommunications`** avec un AWS SDK ou un outil de ligne de commande

Les exemples de code suivants montrent comment utiliser`DescribeCommunications`.

Les exemples d'actions sont des extraits de code de programmes de plus grande envergure et doivent être exécutés en contexte. Vous pouvez voir cette action en contexte dans l'exemple de code suivant :

- Démarrer avec les dossiers

.NET

AWS SDK for .NET

> **Note**
>
> Il y en a plus sur GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples de code AWS.

```
    /// <summary>
    /// Describe the communications for a case, optionally with a date filter.
    /// </summary>
    /// <param name="caseId">The ID of the support case.</param>
    /// <param name="afterTime">The optional start date for a filtered search.</
param>
    /// <param name="beforeTime">The optional end date for a filtered search.</
param>
    /// <returns>The list of communications for the case.</returns>
    public async Task<List<Communication>> DescribeCommunications(string caseId,
 DateTime? afterTime = null, DateTime? beforeTime = null)
    {
        var results = new List<Communication>();
        var paginateCommunications =
 _amazonSupport.Paginators.DescribeCommunications(
            new DescribeCommunicationsRequest()
            {
                CaseId = caseId,
                AfterTime = afterTime?.ToString("s"),
                BeforeTime = beforeTime?.ToString("s")
            });
        // Get the entire list using the paginator.
        await foreach (var communications in
 paginateCommunications.Communications)
```

```
        {
            results.Add(communications);
        }
        return results;
    }
```

- Pour plus de détails sur l'API, reportez-vous DescribeCommunicationsà la section Référence des AWS SDK for .NET API.

CLI

AWS CLI

Pour décrire la dernière communication concernant un dossier

L'`describe-communications`exemple suivant renvoie la dernière communication concernant le dossier d'assistance spécifié dans votre AWS compte.

```
aws support describe-communications \
    --case-id "case-12345678910-2013-c4c1d2bf33c5cf47" \
    --after-time "2020-03-23T21:31:47.774Z" \
    --max-item 1
```

Sortie :

```
{
    "communications": [
        {
            "body": "I want to learn more about an AWS service.",
            "attachmentSet": [],
            "caseId": "case-12345678910-2013-c4c1d2bf33c5cf47",
            "timeCreated": "2020-05-12T23:12:35.000Z",
            "submittedBy": "Amazon Web Services"
        }
    ],
    "NextToken":
 "eyJuZXh0VG9rZW4iOiBudWxsLCAiYm90b190cnVuY2F0ZV9hbW91bnQEXAMPLE=="
}
```

Pour plus d'informations, consultez la section Gestion des dossiers dans le Guide de l'utilisateur du AWS Support.

- Pour plus de détails sur l'API, reportez-vous DescribeCommunicationsà la section Référence des AWS CLI commandes.

Java

SDK pour Java 2.x

> **Note**
>
> Il y en a plus sur GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples de code AWS.

```
   public static String listCommunications(SupportClient supportClient, String
caseId) {
       try {
           String attachId = null;
           DescribeCommunicationsRequest communicationsRequest =
DescribeCommunicationsRequest.builder()
                   .caseId(caseId)
                   .maxResults(10)
                   .build();

           DescribeCommunicationsResponse response =
supportClient.describeCommunications(communicationsRequest);
           List<Communication> communications = response.communications();
           for (Communication comm : communications) {
               System.out.println("the body is: " + comm.body());

               // Get the attachment id value.
               List<AttachmentDetails> attachments = comm.attachmentSet();
               for (AttachmentDetails detail : attachments) {
                   attachId = detail.attachmentId();
               }
           }
           return attachId;

       } catch (SupportException e) {
           System.out.println(e.getLocalizedMessage());
```

```
            System.exit(1);
        }
        return "";
    }
```

- Pour plus de détails sur l'API, reportez-vous DescribeCommunicationsà la section Référence des AWS SDK for Java 2.x API.

JavaScript

SDK pour JavaScript (v3)

> **Note**
>
> Il y en a plus sur GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples de code AWS.

```
import { DescribeCommunicationsCommand } from "@aws-sdk/client-support";

import { client } from "../libs/client.js";

export const main = async () => {
  try {
    // Get all communications for the support case.
    // Filter results by providing parameters to the
 DescribeCommunicationsCommand. Refer
    // to the TypeScript definition and the API doc for more information on
 possible parameters.
    // https://docs.aws.amazon.com/AWSJavaScriptSDK/v3/latest/clients/client-
support/interfaces/describecommunicationscommandinput.html
    const response = await client.send(
      new DescribeCommunicationsCommand({
        // Set value to an existing case id.
        caseId: "CASE_ID",
      }),
    );
    const text = response.communications.map((item) => item.body).join("\n");
    console.log(text);
    return response;
```

```
  } catch (err) {
    console.error(err);
  }
};
```

- Pour plus de détails sur l'API, reportez-vous DescribeCommunicationsà la section Référence des AWS SDK for JavaScript API.

Kotlin

SDK pour Kotlin

> **Note**
>
> Il y en a plus sur GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples de code AWS.

```
suspend fun listCommunications(caseIdVal: String?): String? {
    val communicationsRequest = DescribeCommunicationsRequest {
        caseId = caseIdVal
        maxResults = 10
    }

    SupportClient { region = "us-west-2" }.use { supportClient ->
        val response =
 supportClient.describeCommunications(communicationsRequest)
        response.communications?.forEach { comm ->
            println("the body is: " + comm.body)
            comm.attachmentSet?.forEach { detail ->
                return detail.attachmentId
            }
        }
    }
    return ""
}
```

- Pour plus de détails sur l'API, reportez-vous DescribeCommunicationsà la section AWS SDK pour la référence de l'API Kotlin.

PowerShell

Outils pour PowerShell

Exemple 1 : renvoie toutes les communications pour le cas spécifié.

```
Get-ASACommunication -CaseId "case-12345678910-2013-c4c1d2bf33c5cf47"
```

Exemple 2 : renvoie toutes les communications depuis minuit UTC le 1er janvier 2012 pour le cas spécifié.

```
Get-ASACommunication -CaseId "case-12345678910-2013-c4c1d2bf33c5cf47" -AfterTime
 "2012-01-10T00:00Z"
```

Exemple 3 : renvoie toutes les communications depuis minuit UTC le 1er janvier 2012 pour le cas spécifié, en utilisant la pagination manuelle. Les communications sont récupérées par lots de 20.

```
$nextToken = $null
do {
  Get-ASACommunication -CaseId "case-12345678910-2013-c4c1d2bf33c5cf47" -
NextToken $nextToken -MaxResult 20
  $nextToken = $AWSHistory.LastServiceResponse.NextToken
} while ($nextToken -ne $null)
```

- Pour plus de détails sur l'API, reportez-vous DescribeCommunicationsà la section Référence des AWS Tools for PowerShell applets de commande.

Python

SDK pour Python (Boto3)

> **Note**
>
> Il y en a plus sur GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples de code AWS.

```
class SupportWrapper:
    """Encapsulates Support actions."""
```

```
    def __init__(self, support_client):
        """
        :param support_client: A Boto3 Support client.
        """
        self.support_client = support_client

    @classmethod
    def from_client(cls):
        """
        Instantiates this class from a Boto3 client.
        """
        support_client = boto3.client("support")
        return cls(support_client)


    def describe_all_case_communications(self, case_id):
        """
        Describe all the communications for a case using a paginator.

        :param case_id: The ID of the case.
        :return: The communications for the case.
        """
        try:
            communications = []
            paginator =
self.support_client.get_paginator("describe_communications")
            for page in paginator.paginate(caseId=case_id):
                communications += page["communications"]
        except ClientError as err:
            if err.response["Error"]["Code"] == "SubscriptionRequiredException":
                logger.info(
                    "You must have a Business, Enterprise On-Ramp, or Enterprise
Support "
                    "plan to use the AWS Support API. \n\tPlease upgrade your
subscription to run these "
                    "examples."
                )
            else:
                logger.error(
                    "Couldn't describe communications. Here's why: %s: %s",
                    err.response["Error"]["Code"],
                    err.response["Error"]["Message"],
                )
```

```
                raise
        else:
            return communications
```

- Pour plus de détails sur l'API, consultez DescribeCommunicationsle AWS manuel de référence de l'API SDK for Python (Boto3).

Pour obtenir la liste complète des guides de développement du AWS SDK et des exemples de code, consultezUtilisation de AWS Support avec un kit SDK AWS.. Cette rubrique comprend également des informations sur le démarrage et sur les versions précédentes de SDK.

Utilisation **`DescribeServices`** avec un AWS SDK ou un outil de ligne de commande

Les exemples de code suivants montrent comment utiliser`DescribeServices`.

Les exemples d'actions sont des extraits de code de programmes de plus grande envergure et doivent être exécutés en contexte. Vous pouvez voir cette action en contexte dans l'exemple de code suivant :

- Démarrer avec les dossiers

.NET

AWS SDK for .NET

> **Note**
>
> Il y en a plus sur GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples de code AWS.

```
/// <summary>
/// Get the descriptions of AWS services.
/// </summary>
```

```
    /// <param name="name">Optional language for services.
    /// Currently Chinese (“zh”), English ("en"), Japanese ("ja") and Korean
 (“ko”) are supported.</param>
    /// <returns>The list of AWS service descriptions.</returns>
    public async Task<List<Service>> DescribeServices(string language = "en")
    {
        var response = await _amazonSupport.DescribeServicesAsync(
            new DescribeServicesRequest()
            {
                Language = language
            });
        return response.Services;
    }
```

- Pour plus de détails sur l'API, reportez-vous DescribeServicesà la section Référence des AWS SDK for .NET API.

CLI

AWS CLI

Pour répertorier AWS les services et les catégories de services

L'`describe-services`exemple suivant répertorie les catégories de services disponibles pour demander des informations générales.

```
aws support describe-services \
    --service-code-list "general-info"
```

Sortie :

```
{
    "services": [
        {
            "code": "general-info",
            "name": "General Info and Getting Started",
            "categories": [
                {
                    "code": "charges",
```

```
                    "name": "How Will I Be Charged?"
                },
                {
                    "code": "gdpr-queries",
                    "name": "Data Privacy Query"
                },
                {
                    "code": "reserved-instances",
                    "name": "Reserved Instances"
                },
                {
                    "code": "resource",
                    "name": "Where is my Resource?"
                },
                {
                    "code": "using-aws",
                    "name": "Using AWS & Services"
                },
                {
                    "code": "free-tier",
                    "name": "Free Tier"
                },
                {
                    "code": "security-and-compliance",
                    "name": "Security & Compliance"
                },
                {
                    "code": "account-structure",
                    "name": "Account Structure"
                }
            ]
        }
    ]
}
```


Pour plus d'informations, consultez la section Gestion des dossiers dans le Guide de l'utilisateur du AWS Support.

- Pour plus de détails sur l'API, reportez-vous DescribeServicesà la section Référence des AWS CLI commandes.

Java

SDK pour Java 2.x

> **Note**
>
> Il y en a plus sur GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples de code AWS.

```
   // Return a List that contains a Service name and Category name.
   public static List<String> displayServices(SupportClient supportClient) {
       try {
           DescribeServicesRequest servicesRequest =
DescribeServicesRequest.builder()
                   .language("en")
                   .build();

           DescribeServicesResponse response =
supportClient.describeServices(servicesRequest);
           String serviceCode = null;
           String catName = null;
           List<String> sevCatList = new ArrayList<>();
           List<Service> services = response.services();

           System.out.println("Get the first 10 services");
           int index = 1;
           for (Service service : services) {
               if (index == 11)
                   break;

               System.out.println("The Service name is: " + service.name());
               if (service.name().compareTo("Account") == 0)
                   serviceCode = service.code();

               // Get the Categories for this service.
               List<Category> categories = service.categories();
               for (Category cat : categories) {
                   System.out.println("The category name is: " + cat.name());
                   if (cat.name().compareTo("Security") == 0)
                       catName = cat.name();
               }
```

```
                index++;
            }

            // Push the two values to the list.
            sevCatList.add(serviceCode);
            sevCatList.add(catName);
            return sevCatList;

        } catch (SupportException e) {
            System.out.println(e.getLocalizedMessage());
            System.exit(1);
        }
        return null;
    }
```

- Pour plus de détails sur l'API, reportez-vous DescribeServicesà la section Référence des AWS SDK for Java 2.x API.

Kotlin

SDK pour Kotlin

> **Note**
>
> Il y en a plus sur GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples de code AWS.

```
// Return a List that contains a Service name and Category name.
suspend fun displayServices(): List<String> {
    var serviceCode = ""
    var catName = ""
    val sevCatList = mutableListOf<String>()
    val servicesRequest = DescribeServicesRequest {
        language = "en"
    }

    SupportClient { region = "us-west-2" }.use { supportClient ->
        val response = supportClient.describeServices(servicesRequest)
        println("Get the first 10 services")
```

```
        var index = 1

        response.services?.forEach { service ->
            if (index == 11) {
                return@forEach
            }

            println("The Service name is ${service.name}")
            if (service.name == "Account") {
                serviceCode = service.code.toString()
            }

            // Get the categories for this service.
            service.categories?.forEach { cat ->
                println("The category name is ${cat.name}")
                if (cat.name == "Security") {
                    catName = cat.name!!
                }
            }
            index++
        }
    }

    // Push the two values to the list.
    serviceCode.let { sevCatList.add(it) }
    catName.let { sevCatList.add(it) }
    return sevCatList
}
```

- Pour plus de détails sur l'API, reportez-vous DescribeServicesà la section AWS SDK pour la référence de l'API Kotlin.

PowerShell

Outils pour PowerShell

Exemple 1 : renvoie tous les codes de service, noms et catégories disponibles.

```
Get-ASAService
```

Exemple 2 : renvoie le nom et les catégories du service avec le code spécifié.

```
Get-ASAService -ServiceCodeList "amazon-cloudfront"
```

Exemple 3 : renvoie le nom et les catégories des codes de service spécifiés.

```
Get-ASAService -ServiceCodeList @("amazon-cloudfront", "amazon-cloudwatch")
```

Exemple 4 : renvoie le nom et les catégories (en japonais) des codes de service spécifiés. Les codes de langue anglais (« en ») et japonais (« ja ») sont actuellement pris en charge.

```
Get-ASAService -ServiceCodeList @("amazon-cloudfront", "amazon-cloudwatch") -
Language "ja"
```

- Pour plus de détails sur l'API, reportez-vous DescribeServicesà la section Référence des AWS Tools for PowerShell applets de commande.

Python

SDK pour Python (Boto3)

> **Note**
>
> Il y en a plus sur GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples de code AWS.

```
class SupportWrapper:
    """Encapsulates Support actions."""

    def __init__(self, support_client):
        """
        :param support_client: A Boto3 Support client.
        """
        self.support_client = support_client

    @classmethod
    def from_client(cls):
        """
        Instantiates this class from a Boto3 client.
        """
```

```
        support_client = boto3.client("support")
        return cls(support_client)


    def describe_services(self, language):
        """
        Get the descriptions of AWS services available for support for a
language.

        :param language: The language for support services.
        Currently, only "en" (English) and "ja" (Japanese) are supported.
        :return: The list of AWS service descriptions.
        """
        try:
            response = self.support_client.describe_services(language=language)
            services = response["services"]
        except ClientError as err:
            if err.response["Error"]["Code"] == "SubscriptionRequiredException":
                logger.info(
                    "You must have a Business, Enterprise On-Ramp, or Enterprise
Support "
                    "plan to use the AWS Support API. \n\tPlease upgrade your
subscription to run these "
                    "examples."
                )
            else:
                logger.error(
                    "Couldn't get Support services for language %s. Here's why:
%s: %s",
                    language,
                    err.response["Error"]["Code"],
                    err.response["Error"]["Message"],
                )
                raise
        else:
            return services
```

- Pour plus de détails sur l'API, consultez DescribeServicesle AWS manuel de référence de l'API SDK for Python (Boto3).

Pour obtenir la liste complète des guides de développement du AWS SDK et des exemples de code, consultezUtilisation de AWS Support avec un kit SDK AWS.. Cette rubrique comprend également des informations sur le démarrage et sur les versions précédentes de SDK.

Utilisation **`DescribeSeverityLevels`** avec un AWS SDK ou un outil de ligne de commande

Les exemples de code suivants montrent comment utiliser`DescribeSeverityLevels`.

Les exemples d'actions sont des extraits de code de programmes de plus grande envergure et doivent être exécutés en contexte. Vous pouvez voir cette action en contexte dans l'exemple de code suivant :

- Démarrer avec les dossiers

.NET

AWS SDK for .NET

> **Note**
>
> Il y en a plus sur GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples de code AWS.

```
   /// <summary>
   /// Get the descriptions of support severity levels.
   /// </summary>
   /// <param name="name">Optional language for severity levels.
   /// Currently Chinese (“zh”), English ("en"), Japanese ("ja") and Korean
(“ko”) are supported.</param>
   /// <returns>The list of support severity levels.</returns>
   public async Task<List<SeverityLevel>> DescribeSeverityLevels(string language
= "en")
   {
       var response = await _amazonSupport.DescribeSeverityLevelsAsync(
           new DescribeSeverityLevelsRequest()
           {
               Language = language
```

```
            });
        return response.SeverityLevels;
    }
```

- Pour plus de détails sur l'API, reportez-vous DescribeSeverityLevelsà la section Référence des AWS SDK for .NET API.

CLI

AWS CLI

Pour répertorier les niveaux de gravité disponibles

L'`describe-severity-levels`exemple suivant répertorie les niveaux de gravité disponibles pour un dossier de support.

```
aws support describe-severity-levels
```

Sortie :

```
{
    "severityLevels": [
        {
            "code": "low",
            "name": "Low"
        },
        {
            "code": "normal",
            "name": "Normal"
        },
        {
            "code": "high",
            "name": "High"
        },
        {
            "code": "urgent",
            "name": "Urgent"
        },
        {
```

```
            "code": "critical",
            "name": "Critical"
        }
    ]
}
```

Pour plus d'informations, consultez la section Choix d'une sévérité dans le Guide de l'utilisateur du AWS Support.

- Pour plus de détails sur l'API, reportez-vous DescribeSeverityLevelsà la section Référence des AWS CLI commandes.

Java

SDK pour Java 2.x

> **Note**
>
> Il y en a plus sur GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples de code AWS.

```
   public static String displaySevLevels(SupportClient supportClient) {
       try {
           DescribeSeverityLevelsRequest severityLevelsRequest =
DescribeSeverityLevelsRequest.builder()
                   .language("en")
                   .build();

           DescribeSeverityLevelsResponse response =
supportClient.describeSeverityLevels(severityLevelsRequest);
           List<SeverityLevel> severityLevels = response.severityLevels();
           String levelName = null;
           for (SeverityLevel sevLevel : severityLevels) {
               System.out.println("The severity level name is: " +
sevLevel.name());
               if (sevLevel.name().compareTo("High") == 0)
                   levelName = sevLevel.name();
           }
           return levelName;
```

```
        } catch (SupportException e) {
            System.out.println(e.getLocalizedMessage());
            System.exit(1);
        }
        return "";
    }
```

- Pour plus de détails sur l'API, reportez-vous DescribeSeverityLevelsà la section Référence des AWS SDK for Java 2.x API.

JavaScript

SDK pour JavaScript (v3)

> **Note**
>
> Il y en a plus sur GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples de code AWS.

```
import { DescribeSeverityLevelsCommand } from "@aws-sdk/client-support";

import { client } from "../libs/client.js";

export const main = async () => {
  try {
    // Get the list of severity levels.
    // The available values depend on the support plan for the account.
    const response = await client.send(new DescribeSeverityLevelsCommand({}));
    console.log(response.severityLevels);
    return response;
  } catch (err) {
    console.error(err);
  }
};
```

- Pour plus de détails sur l'API, reportez-vous DescribeSeverityLevelsà la section Référence des AWS SDK for JavaScript API.

Kotlin

SDK pour Kotlin

> **Note**
>
> Il y en a plus sur GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples de code AWS.

```
suspend fun displaySevLevels(): String {
    var levelName = ""
    val severityLevelsRequest = DescribeSeverityLevelsRequest {
        language = "en"
    }

    SupportClient { region = "us-west-2" }.use { supportClient ->
        val response =
 supportClient.describeSeverityLevels(severityLevelsRequest)
        response.severityLevels?.forEach { sevLevel ->
            println("The severity level name is: ${sevLevel.name}")
            if (sevLevel.name == "High") {
                levelName = sevLevel.name!!
            }
        }
        return levelName
    }
}
```

- Pour plus de détails sur l'API, reportez-vous DescribeSeverityLevelsà la section AWS SDK pour la référence de l'API Kotlin.

PowerShell

Outils pour PowerShell

Exemple 1 : renvoie la liste des niveaux de gravité qui peuvent être attribués à un dossier AWS Support.

```
Get-ASASeverityLevel
```

Exemple 2 : renvoie la liste des niveaux de gravité qui peuvent être attribués à un dossier AWS Support. Les noms des niveaux sont renvoyés en japonais.

```
Get-ASASeverityLevel -Language "ja"
```

- Pour plus de détails sur l'API, reportez-vous DescribeSeverityLevelsà la section Référence des AWS Tools for PowerShell applets de commande.

Python

SDK pour Python (Boto3)

> **Note**
>
> Il y en a plus sur GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples de code AWS.

```
class SupportWrapper:
    """Encapsulates Support actions."""

    def __init__(self, support_client):
        """
        :param support_client: A Boto3 Support client.
        """
        self.support_client = support_client

    @classmethod
    def from_client(cls):
        """
        Instantiates this class from a Boto3 client.
        """
        support_client = boto3.client("support")
        return cls(support_client)


    def describe_severity_levels(self, language):
        """
```

```
        Get the descriptions of available severity levels for support cases for a
language.

        :param language: The language for support severity levels.
        Currently, only "en" (English) and "ja" (Japanese) are supported.
        :return: The list of severity levels.
        """
        try:
            response =
self.support_client.describe_severity_levels(language=language)
            severity_levels = response["severityLevels"]
        except ClientError as err:
            if err.response["Error"]["Code"] == "SubscriptionRequiredException":
                logger.info(
                    "You must have a Business, Enterprise On-Ramp, or Enterprise
Support "
                    "plan to use the AWS Support API. \n\tPlease upgrade your
subscription to run these "
                    "examples."
                )
            else:
                logger.error(
                    "Couldn't get severity levels for language %s. Here's why:
%s: %s",
                    language,
                    err.response["Error"]["Code"],
                    err.response["Error"]["Message"],
                )
                raise
        else:
            return severity_levels
```

- Pour plus de détails sur l'API, consultez DescribeSeverityLevelsle AWS manuel de référence de l'API SDK for Python (Boto3).

Pour obtenir la liste complète des guides de développement du AWS SDK et des exemples de code, consultezUtilisation de AWS Support avec un kit SDK AWS.. Cette rubrique comprend également des informations sur le démarrage et sur les versions précédentes de SDK.

Utilisation **DescribeTrustedAdvisorCheckRefreshStatuses** avec un AWS SDK ou un outil de ligne de commande

Les exemples de code suivants montrent comment utiliser`DescribeTrustedAdvisorCheckRefreshStatuses`.

CLI

AWS CLI

Pour répertorier les statuts d'actualisation des chèques AWS Trusted Advisor

L'`describe-trusted-advisor-check-refresh-statuses`exemple suivant répertorie les statuts d'actualisation de deux contrôles Trusted Advisor : Amazon S3 Bucket Permissions et IAM Use.

```
aws support describe-trusted-advisor-check-refresh-statuses \
    --check-id "Pfx0RwqBli" "zXCkfM1nI3"
```

Sortie :

```
{
    "statuses": [
        {
            "checkId": "Pfx0RwqBli",
            "status": "none",
            "millisUntilNextRefreshable": 0
        },
        {
            "checkId": "zXCkfM1nI3",
            "status": "none",
            "millisUntilNextRefreshable": 0
        }
    ]
}
```

Pour plus d'informations, consultez AWS Trusted Advisor dans le Guide de l'utilisateur du AWS Support.

- Pour plus de détails sur l'API, reportez-vous DescribeTrustedAdvisorCheckRefreshStatusesà la section Référence des AWS CLI commandes.

PowerShell

Outils pour PowerShell

Exemple 1 : renvoie l'état actuel des demandes d'actualisation pour les vérifications spécifiées. Request-ASA TrustedAdvisorCheckRefresh peut être utilisé pour demander que les informations d'état des chèques soient actualisées.

```
Get-ASATrustedAdvisorCheckRefreshStatus -CheckId @("checkid1", "checkid2")
```

- Pour plus de détails sur l'API, reportez-vous DescribeTrustedAdvisorCheckRefreshStatusesà la section Référence des AWS Tools for PowerShell applets de commande.

Pour obtenir la liste complète des guides de développement du AWS SDK et des exemples de code, consultezUtilisation de AWS Support avec un kit SDK AWS.. Cette rubrique comprend également des informations sur le démarrage et sur les versions précédentes de SDK.

Utilisation **`DescribeTrustedAdvisorCheckResult`** avec un AWS SDK ou un outil de ligne de commande

Les exemples de code suivants montrent comment utiliser`DescribeTrustedAdvisorCheckResult`.

CLI

AWS CLI

Pour répertorier les résultats d'un check effectué par AWS Trusted Advisor

L'`describe-trusted-advisor-check-result`exemple suivant répertorie les résultats du contrôle d'utilisation IAM.

```
aws support describe-trusted-advisor-check-result \
    --check-id "zXCkfM1nI3"
```

Sortie :

```
{
    "result": {
```

```
        "checkId": "zXCkfM1nI3",
        "timestamp": "2020-05-13T21:38:05Z",
        "status": "ok",
        "resourcesSummary": {
            "resourcesProcessed": 1,
            "resourcesFlagged": 0,
            "resourcesIgnored": 0,
            "resourcesSuppressed": 0
        },
        "categorySpecificSummary": {
            "costOptimizing": {
                "estimatedMonthlySavings": 0.0,
                "estimatedPercentMonthlySavings": 0.0
            }
        },
        "flaggedResources": [
            {
                "status": "ok",
                "resourceId": "47DEQpj8HBSa-_TImW-5JCeuQeRkm5NMpJWZEXAMPLE",
                "isSuppressed": false
            }
        ]
    }
}
```

Pour plus d'informations, consultez AWS Trusted Advisor dans le Guide de l'utilisateur du AWS Support.

- Pour plus de détails sur l'API, reportez-vous DescribeTrustedAdvisorCheckResultà la section Référence des AWS CLI commandes.

PowerShell

Outils pour PowerShell

Exemple 1 : renvoie les résultats d'un check Trusted Advisor. La liste des chèques Trusted Advisor disponibles peut être obtenue à l'aide de TrustedAdvisorChecks Get-ASA. Le résultat est l'état général de la vérification, l'horodatage auquel la vérification a été exécutée pour la dernière fois et l'identifiant de contrôle unique pour la vérification spécifique. Pour que les résultats soient affichés en japonais, ajoutez le paramètre -Language « ja ».

```
Get-ASATrustedAdvisorCheckResult -CheckId "checkid1"
```

- Pour plus de détails sur l'API, reportez-vous DescribeTrustedAdvisorCheckResultà la section Référence des AWS Tools for PowerShell applets de commande.

Pour obtenir la liste complète des guides de développement du AWS SDK et des exemples de code, consultezUtilisation de AWS Support avec un kit SDK AWS.. Cette rubrique comprend également des informations sur le démarrage et sur les versions précédentes de SDK.

Utilisation **`DescribeTrustedAdvisorCheckSummaries`** avec un AWS SDK ou un outil de ligne de commande

Les exemples de code suivants montrent comment utiliser`DescribeTrustedAdvisorCheckSummaries`.

CLI

AWS CLI

Pour répertorier les résumés des contrôles effectués par AWS Trusted Advisor

L'`describe-trusted-advisor-check-summaries`exemple suivant répertorie les résultats de deux contrôles effectués par Trusted Advisor : Amazon S3 Bucket Permissions et IAM Use.

```
aws support describe-trusted-advisor-check-summaries \
    --check-ids "Pfx0RwqBli" "zXCkfM1nI3"
```

Sortie :

```
{
    "summaries": [
        {
            "checkId": "Pfx0RwqBli",
            "timestamp": "2020-05-13T21:38:12Z",
            "status": "ok",
            "hasFlaggedResources": true,
            "resourcesSummary": {
                "resourcesProcessed": 44,
                "resourcesFlagged": 0,
                "resourcesIgnored": 0,
                "resourcesSuppressed": 0
            },
```

```
            "categorySpecificSummary": {
                "costOptimizing": {
                    "estimatedMonthlySavings": 0.0,
                    "estimatedPercentMonthlySavings": 0.0
                }
            }
        },
        {
            "checkId": "zXCkfM1nI3",
            "timestamp": "2020-05-13T21:38:05Z",
            "status": "ok",
            "hasFlaggedResources": true,
            "resourcesSummary": {
                "resourcesProcessed": 1,
                "resourcesFlagged": 0,
                "resourcesIgnored": 0,
                "resourcesSuppressed": 0
            },
            "categorySpecificSummary": {
                "costOptimizing": {
                    "estimatedMonthlySavings": 0.0,
                    "estimatedPercentMonthlySavings": 0.0
                }
            }
        }
    ]
}
```

Pour plus d'informations, consultez AWS Trusted Advisor dans le Guide de l'utilisateur du AWS Support.

- Pour plus de détails sur l'API, reportez-vous DescribeTrustedAdvisorCheckSummariesà la section Référence des AWS CLI commandes.

PowerShell

Outils pour PowerShell

Exemple 1 : Renvoie le dernier résumé du check Trusted Advisor spécifié.

```
Get-ASATrustedAdvisorCheckSummary -CheckId "checkid1"
```

Exemple 2 : renvoie les derniers résumés des contrôles Trusted Advisor spécifiés.

```
Get-ASATrustedAdvisorCheckSummary -CheckId @("checkid1", "checkid2")
```

- Pour plus de détails sur l'API, reportez-vous DescribeTrustedAdvisorCheckSummariesà la section Référence des AWS Tools for PowerShell applets de commande.

Pour obtenir la liste complète des guides de développement du AWS SDK et des exemples de code, consultezUtilisation de AWS Support avec un kit SDK AWS.. Cette rubrique comprend également des informations sur le démarrage et sur les versions précédentes de SDK.

Utilisation **`DescribeTrustedAdvisorChecks`** avec un AWS SDK ou un outil de ligne de commande

Les exemples de code suivants montrent comment utiliser`DescribeTrustedAdvisorChecks`.

CLI

AWS CLI

Pour répertorier les chèques AWS Trusted Advisor disponibles

L'`describe-trusted-advisor-checks`exemple suivant répertorie les chèques Trusted Advisor disponibles sur votre AWS compte. Ces informations incluent le nom, l'identifiant, la description, la catégorie et les métadonnées du chèque. Notez que la sortie est raccourcie pour des raisons de lisibilité.

```
aws support describe-trusted-advisor-checks \
    --language "en"
```

Sortie :

```
{
    "checks": [
        {
            "id": "zXCkfM1nI3",
            "name": "IAM Use",
            "description": "Checks for your use of AWS Identity and Access
 Management (IAM). You can use IAM to create users, groups, and roles in
 AWS, and you can use permissions to control access to AWS resources. \n<br>
\n<br>\n<b>Alert Criteria</b><br>\nYellow: No IAM users have been created
 for this account.\n<br>\n<br>\n<b>Recommended Action</b><br>\nCreate one or
```

```
 more IAM users and groups in your account. You can then create additional
 users whose permissions are limited to perform specific tasks in your AWS
 environment. For more information, see <a href=\"https://docs.aws.amazon.com/
IAM/latest/UserGuide/IAMGettingStarted.html\" target=\"_blank\">Getting
 Started</a>. \n<br><br>\n<b>Additional Resources</b><br>\n<a href=\"https://
docs.aws.amazon.com/IAM/latest/UserGuide/IAM_Introduction.html\" target=\"_blank
\">What Is IAM?</a>",
            "category": "security",
            "metadata": []
        }
    ]
}
```

Pour plus d'informations, consultez AWS Trusted Advisor dans le Guide de l'utilisateur du AWS Support.

- Pour plus de détails sur l'API, reportez-vous DescribeTrustedAdvisorChecksà la section Référence des AWS CLI commandes.

PowerShell

Outils pour PowerShell

Exemple 1 : Renvoie la collection de chèques Trusted Advisor. Vous devez spécifier le paramètre Language qui peut accepter soit « en » pour la sortie en anglais, soit « ja » pour la sortie japonaise.

```
Get-ASATrustedAdvisorCheck -Language "en"
```

- Pour plus de détails sur l'API, reportez-vous DescribeTrustedAdvisorChecksà la section Référence des AWS Tools for PowerShell applets de commande.

Pour obtenir la liste complète des guides de développement du AWS SDK et des exemples de code, consultezUtilisation de AWS Support avec un kit SDK AWS.. Cette rubrique comprend également des informations sur le démarrage et sur les versions précédentes de SDK.

Utilisation **`RefreshTrustedAdvisorCheck`** avec un AWS SDK ou un outil de ligne de commande

Les exemples de code suivants montrent comment utiliser`RefreshTrustedAdvisorCheck`.

CLI

AWS CLI

Pour actualiser un check AWS Trusted Advisor

L'`refresh-trusted-advisor-check`exemple suivant actualise le check Amazon S3 Bucket Permissions Trusted Advisor dans votre AWS compte.

```
aws support refresh-trusted-advisor-check \
    --check-id "Pfx0RwqBli"
```

Sortie :

```
{
    "status": {
        "checkId": "Pfx0RwqBli",
        "status": "enqueued",
        "millisUntilNextRefreshable": 3599992
    }
}
```

Pour plus d'informations, consultez AWS Trusted Advisor dans le Guide de l'utilisateur du AWS Support.

- Pour plus de détails sur l'API, reportez-vous RefreshTrustedAdvisorCheckà la section Référence des AWS CLI commandes.

PowerShell

Outils pour PowerShell

Exemple 1 : Demande une actualisation pour le check Trusted Advisor spécifié.

```
Request-ASATrustedAdvisorCheckRefresh -CheckId "checkid1"
```

- Pour plus de détails sur l'API, reportez-vous RefreshTrustedAdvisorCheckà la section Référence des AWS Tools for PowerShell applets de commande.

Pour obtenir la liste complète des guides de développement du AWS SDK et des exemples de code, consultezUtilisation de AWS Support avec un kit SDK AWS.. Cette rubrique comprend également des informations sur le démarrage et sur les versions précédentes de SDK.

Utilisation **`ResolveCase`** avec un AWS SDK ou un outil de ligne de commande

Les exemples de code suivants montrent comment utiliser`ResolveCase`.

Les exemples d'actions sont des extraits de code de programmes de plus grande envergure et doivent être exécutés en contexte. Vous pouvez voir cette action en contexte dans l'exemple de code suivant :

- Démarrer avec les dossiers

.NET

AWS SDK for .NET

> **Note**
>
> Il y en a plus sur GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples de code AWS.

```
/// <summary>
/// Resolve a support case by caseId.
/// </summary>
/// <param name="caseId">Id for the support case.</param>
/// <returns>The final status of the case after resolving.</returns>
public async Task<string> ResolveCase(string caseId)
{
    var response = await _amazonSupport.ResolveCaseAsync(
        new ResolveCaseRequest()
        {
            CaseId = caseId
        });
    return response.FinalCaseStatus;
}
```

```
```

- Pour plus de détails sur l'API, reportez-vous ResolveCaseà la section Référence des AWS SDK for .NET API.

CLI

AWS CLI

Pour résoudre un dossier d'assistance

L'`resolve-case`exemple suivant résout une demande d'assistance dans votre AWS compte.

```
aws support resolve-case \
    --case-id "case-12345678910-2013-c4c1d2bf33c5cf47"
```

Sortie :

```
{
    "finalCaseStatus": "resolved",
    "initialCaseStatus": "work-in-progress"
}
```

Pour plus d'informations, consultez la section Gestion des dossiers dans le Guide de l'utilisateur du AWS Support.

- Pour plus de détails sur l'API, reportez-vous ResolveCaseà la section Référence des AWS CLI commandes.

Java

SDK pour Java 2.x

> **Note**
>
> Il y en a plus sur GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples de code AWS.

```
   public static void resolveSupportCase(SupportClient supportClient, String
caseId) {
       try {
           ResolveCaseRequest caseRequest = ResolveCaseRequest.builder()
                   .caseId(caseId)
                   .build();

           ResolveCaseResponse response =
supportClient.resolveCase(caseRequest);
           System.out.println("The status of case " + caseId + " is " +
response.finalCaseStatus());

       } catch (SupportException e) {
           System.out.println(e.getLocalizedMessage());
           System.exit(1);
       }
   }
```

- Pour plus de détails sur l'API, reportez-vous ResolveCaseà la section Référence des AWS SDK for Java 2.x API.

JavaScript

SDK pour JavaScript (v3)

> **Note**
>
> Il y en a plus sur GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples de code AWS.

```
import { ResolveCaseCommand } from "@aws-sdk/client-support";

import { client } from "../libs/client.js";

const main = async () => {
  try {
    const response = await client.send(
      new ResolveCaseCommand({
        caseId: "CASE_ID",
```

```
      }),
    );

    console.log(response.finalCaseStatus);
    return response;
  } catch (err) {
    console.error(err);
  }
};
```

- Pour plus de détails sur l'API, reportez-vous ResolveCaseà la section Référence des AWS SDK for JavaScript API.

Kotlin

SDK pour Kotlin

> **Note**
>
> Il y en a plus sur GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples de code AWS.

```
suspend fun resolveSupportCase(caseIdVal: String) {
    val caseRequest = ResolveCaseRequest {
        caseId = caseIdVal
    }
    SupportClient { region = "us-west-2" }.use { supportClient ->
        val response = supportClient.resolveCase(caseRequest)
        println("The status of case $caseIdVal is ${response.finalCaseStatus}")
    }
}
```

- Pour plus de détails sur l'API, reportez-vous ResolveCaseà la section AWS SDK pour la référence de l'API Kotlin.

PowerShell

Outils pour PowerShell

Exemple 1 : renvoie l'état initial du cas spécifié et l'état actuel une fois l'appel pour le résoudre terminé.

```
Resolve-ASACase -CaseId "case-12345678910-2013-c4c1d2bf33c5cf47"
```

- Pour plus de détails sur l'API, reportez-vous ResolveCaseà la section Référence des AWS Tools for PowerShell applets de commande.

Python

SDK pour Python (Boto3)

> **Note**
>
> Il y en a plus sur GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples de code AWS.

```
class SupportWrapper:
    """Encapsulates Support actions."""

    def __init__(self, support_client):
        """
        :param support_client: A Boto3 Support client.
        """
        self.support_client = support_client

    @classmethod
    def from_client(cls):
        """
        Instantiates this class from a Boto3 client.
        """
        support_client = boto3.client("support")
        return cls(support_client)


    def resolve_case(self, case_id):
```

```
        """
        Resolve a support case by its caseId.

        :param case_id: The ID of the case to resolve.
        :return: The final status of the case.
        """
        try:
            response = self.support_client.resolve_case(caseId=case_id)
            final_status = response["finalCaseStatus"]
        except ClientError as err:
            if err.response["Error"]["Code"] == "SubscriptionRequiredException":
                logger.info(
                    "You must have a Business, Enterprise On-Ramp, or Enterprise
Support "
                    "plan to use the AWS Support API. \n\tPlease upgrade your
subscription to run these "
                    "examples."
                )
            else:
                logger.error(
                    "Couldn't resolve case. Here's why: %s: %s",
                    err.response["Error"]["Code"],
                    err.response["Error"]["Message"],
                )
                raise
        else:
            return final_status
```

- Pour plus de détails sur l'API, consultez ResolveCasele AWS manuel de référence de l'API SDK for Python (Boto3).

Pour obtenir la liste complète des guides de développement du AWS SDK et des exemples de code, consultezUtilisation de AWS Support avec un kit SDK AWS.. Cette rubrique comprend également des informations sur le démarrage et sur les versions précédentes de SDK.

Scénarios d' AWS Support utilisation des AWS SDK

Les exemples de code suivants vous montrent comment implémenter des scénarios courants AWS Support avec AWS les SDK. Ces scénarios vous montrent comment accomplir des tâches

spécifiques en appelant plusieurs fonctions AWS Support. Chaque scénario inclut un lien vers GitHub, où vous pouvez trouver des instructions sur la façon de configurer et d'exécuter le code.

Exemples

- Commencez à traiter les AWS Support dossiers à l'aide d'un AWS SDK

Commencez à traiter les AWS Support dossiers à l'aide d'un AWS SDK

Les exemples de code suivants montrent comment :

- Obtenez et affichez les services disponibles et les niveaux de gravité des dossiers.
- Créez un dossier de support en utilisant un service, une catégorie et un niveau de gravité sélectionnés.
- Obtenez et affichez une liste des dossiers ouverts pour la journée en cours.
- Ajoutez un ensemble de pièces jointes et une communication au nouveau dossier.
- Décrivez la nouvelle pièce jointe et la nouvelle communication relatives au dossier.
- Résolvez le dossier.
- Obtenez et affichez la liste des dossiers ouverts pour la journée en cours.

.NET

AWS SDK for .NET

> **Note**
>
> Il y en a plus sur GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples de code AWS.

Exécutez un scénario interactif à une invite de commande.

```
/// <summary>
/// Hello AWS Support example.
/// </summary>
public static class SupportCaseScenario
{
```

```
   /*
   Before running this .NET code example, set up your development environment,
including your credentials.
   To use the AWS Support API, you must have one of the following AWS Support
plans: Business, Enterprise On-Ramp, or Enterprise.

   This .NET example performs the following tasks:
   1.  Get and display services. Select a service from the list.
   2.  Select a category from the selected service.
   3.  Get and display severity levels and select a severity level from the
list.
   4.  Create a support case using the selected service, category, and severity
level.
   5.  Get and display a list of open support cases for the current day.
   6.  Create an attachment set with a sample text file to add to the case.
   7.  Add a communication with the attachment to the support case.
   8.  List the communications of the support case.
   9.  Describe the attachment set.
   10. Resolve the support case.
   11. Get a list of resolved cases for the current day.
  */

   private static SupportWrapper _supportWrapper = null!;

   static async Task Main(string[] args)
   {
       // Set up dependency injection for the AWS Support service.
       // Use your AWS profile name, or leave it blank to use the default
profile.
       using var host = Host.CreateDefaultBuilder(args)
           .ConfigureLogging(logging =>
               logging.AddFilter("System", LogLevel.Debug)
                   .AddFilter<DebugLoggerProvider>("Microsoft",
LogLevel.Information)
                   .AddFilter<ConsoleLoggerProvider>("Microsoft",
LogLevel.Trace))
           .ConfigureServices((_, services) =>
               services.AddAWSService<IAmazonAWSSupport>(new AWSOptions()
{ Profile = "default" })
                   .AddTransient<SupportWrapper>()
           )
           .Build();

       var logger = LoggerFactory.Create(builder =>
```

```
        {
            builder.AddConsole();
        }).CreateLogger(typeof(SupportCaseScenario));

        _supportWrapper = host.Services.GetRequiredService<SupportWrapper>();

        Console.WriteLine(new string('-', 80));
        Console.WriteLine("Welcome to the AWS Support case example scenario.");
        Console.WriteLine(new string('-', 80));

        try
        {
            var apiSupported = await _supportWrapper.VerifySubscription();
            if (!apiSupported)
            {
                logger.LogError("You must have a Business, Enterprise On-Ramp, or
Enterprise Support " +
                                "plan to use the AWS Support API. \n\tPlease
upgrade your subscription to run these examples.");
                return;
            }

            var service = await DisplayAndSelectServices();

            var category = DisplayAndSelectCategories(service);

            var severityLevel = await DisplayAndSelectSeverity();

            var caseId = await CreateSupportCase(service, category,
severityLevel);

            await DescribeTodayOpenCases();

            var attachmentSetId = await CreateAttachmentSet();

            await AddCommunicationToCase(attachmentSetId, caseId);

            var attachmentId = await ListCommunicationsForCase(caseId);

            await DescribeCaseAttachment(attachmentId);

            await ResolveCase(caseId);

            await DescribeTodayResolvedCases();
```

```
            Console.WriteLine(new string('-', 80));
            Console.WriteLine("AWS Support case example scenario complete.");
            Console.WriteLine(new string('-', 80));
        }
        catch (Exception ex)
        {
            logger.LogError(ex, "There was a problem executing the scenario.");
        }
    }

    /// <summary>
    /// List some available services from AWS Support, and select a service for
the example.
    /// </summary>
    /// <returns>The selected service.</returns>
    private static async Task<Service> DisplayAndSelectServices()
    {
        Console.WriteLine(new string('-', 80));
        var services = await _supportWrapper.DescribeServices();
        Console.WriteLine($"AWS Support client returned {services.Count}
services.");

        Console.WriteLine($"1. Displaying first 10 services:");
        for (int i = 0; i < 10 && i < services.Count; i++)
        {
            Console.WriteLine($"\t{i + 1}. {services[i].Name}");
        }

        var choiceNumber = 0;
        while (choiceNumber < 1 || choiceNumber > services.Count)
        {
            Console.WriteLine(
                "Select an example support service by entering a number from the
preceding list:");
            var choice = Console.ReadLine();
            Int32.TryParse(choice, out choiceNumber);
        }
        Console.WriteLine(new string('-', 80));

        return services[choiceNumber - 1];
    }

    /// <summary>
```

```
    /// List the available categories for a service and select a category for the
example.
    /// </summary>
    /// <param name="service">Service to use for displaying categories.</param>
    /// <returns>The selected category.</returns>
    private static Category DisplayAndSelectCategories(Service service)
    {
        Console.WriteLine(new string('-', 80));

        Console.WriteLine($"2. Available support categories for Service
\"{service.Name}\":");
        for (int i = 0; i < service.Categories.Count; i++)
        {
            Console.WriteLine($"\t{i + 1}. {service.Categories[i].Name}");
        }

        var choiceNumber = 0;
        while (choiceNumber < 1 || choiceNumber > service.Categories.Count)
        {
            Console.WriteLine(
                "Select an example support category by entering a number from the
preceding list:");
            var choice = Console.ReadLine();
            Int32.TryParse(choice, out choiceNumber);
        }

        Console.WriteLine(new string('-', 80));

        return service.Categories[choiceNumber - 1];
    }

    /// <summary>
    /// List available severity levels from AWS Support, and select a level for
the example.
    /// </summary>
    /// <returns>The selected severity level.</returns>
    private static async Task<SeverityLevel> DisplayAndSelectSeverity()
    {
        Console.WriteLine(new string('-', 80));
        var severityLevels = await _supportWrapper.DescribeSeverityLevels();

        Console.WriteLine($"3. Get and display available severity levels:");
        for (int i = 0; i < 10 && i < severityLevels.Count; i++)
        {
```

```
            Console.WriteLine($"\t{i + 1}. {severityLevels[i].Name}");
        }

        var choiceNumber = 0;
        while (choiceNumber < 1 || choiceNumber > severityLevels.Count)
        {
            Console.WriteLine(
                "Select an example severity level by entering a number from the
preceding list:");
            var choice = Console.ReadLine();
            Int32.TryParse(choice, out choiceNumber);
        }
        Console.WriteLine(new string('-', 80));

        return severityLevels[choiceNumber - 1];
    }

    /// <summary>
    /// Create an example support case.
    /// </summary>
    /// <param name="service">Service to use for the new case.</param>
    /// <param name="category">Category to use for the new case.</param>
    /// <param name="severity">Severity to use for the new case.</param>
    /// <returns>The caseId of the new support case.</returns>
    private static async Task<string> CreateSupportCase(Service service,
        Category category, SeverityLevel severity)
    {
        Console.WriteLine(new string('-', 80));
        Console.WriteLine($"4. Create an example support case" +
                          $" with the following settings:" +
                          $" \n\tService: {service.Name}, Category:
{category.Name} " +
                          $"and Severity Level: {severity.Name}.");
        var caseId = await _supportWrapper.CreateCase(service.Code,
category.Code, severity.Code,
            "Example case for testing, ignore.", "This is my example support
case.");

        Console.WriteLine($"\tNew case created with ID {caseId}");

        Console.WriteLine(new string('-', 80));

        return caseId;
    }
```

```
    /// <summary>
    /// List open cases for the current day.
    /// </summary>
    /// <returns>Async task.</returns>
    private static async Task DescribeTodayOpenCases()
    {
        Console.WriteLine($"5. List the open support cases for the current
day.");
        // Describe the cases. If it is empty, try again and allow time for the
new case to appear.
        List<CaseDetails> currentOpenCases = null!;
        while (currentOpenCases == null || currentOpenCases.Count == 0)
        {
            Thread.Sleep(1000);
            currentOpenCases = await _supportWrapper.DescribeCases(
                new List<string>(),
                null,
                false,
                false,
                DateTime.UtcNow.Date,
                DateTime.UtcNow);
        }

        foreach (var openCase in currentOpenCases)
        {
            Console.WriteLine($"\tCase: {openCase.CaseId} created
{openCase.TimeCreated}");
        }

        Console.WriteLine(new string('-', 80));
    }

    /// <summary>
    /// Create an attachment set for a support case.
    /// </summary>
    /// <returns>The attachment set id.</returns>
    private static async Task<string> CreateAttachmentSet()
    {
        Console.WriteLine(new string('-', 80));
        Console.WriteLine($"6. Create an attachment set for a support case.");
        var fileName = "example_attachment.txt";

        // Create the file if it does not already exist.
```

```
        if (!File.Exists(fileName))
        {
            await using StreamWriter sw = File.CreateText(fileName);
            await sw.WriteLineAsync(
                "This is a sample file for attachment to a support case.");
        }

        await using var ms = new MemoryStream(await
 File.ReadAllBytesAsync(fileName));

        var attachmentSetId = await _supportWrapper.AddAttachmentToSet(
            ms,
            fileName);

        Console.WriteLine($"\tNew attachment set created with id: \n
\t{attachmentSetId.Substring(0, 65)}...");

        Console.WriteLine(new string('-', 80));

        return attachmentSetId;
    }

    /// <summary>
    /// Add an attachment set and communication to a case.
    /// </summary>
    /// <param name="attachmentSetId">Id of the attachment set.</param>
    /// <param name="caseId">Id of the case to receive the attachment set.</
param>
    /// <returns>Async task.</returns>
    private static async Task AddCommunicationToCase(string attachmentSetId,
 string caseId)
    {
        Console.WriteLine(new string('-', 80));
        Console.WriteLine($"7. Add attachment set and communication to
 {caseId}.");

        await _supportWrapper.AddCommunicationToCase(
            caseId,
            "This is an example communication added to a support case.",
            attachmentSetId);

        Console.WriteLine($"\tNew attachment set and communication added to
 {caseId}");
```

```
        Console.WriteLine(new string('-', 80));
    }

    /// <summary>
    /// List the communications for a case.
    /// </summary>
    /// <param name="caseId">Id of the case to describe.</param>
    /// <returns>An attachment id.</returns>
    private static async Task<string> ListCommunicationsForCase(string caseId)
    {
        Console.WriteLine(new string('-', 80));
        Console.WriteLine($"8. List communications for case {caseId}.");

        var communications = await
_supportWrapper.DescribeCommunications(caseId);
        var attachmentId = "";
        foreach (var communication in communications)
        {
            Console.WriteLine(
                $"\tCommunication created on: {communication.TimeCreated} has
{communication.AttachmentSet.Count} attachments.");
            if (communication.AttachmentSet.Any())
            {
                attachmentId = communication.AttachmentSet.First().AttachmentId;
            }
        }

        Console.WriteLine(new string('-', 80));
        return attachmentId;
    }

    /// <summary>
    /// Describe an attachment by id.
    /// </summary>
    /// <param name="attachmentId">Id of the attachment to describe.</param>
    /// <returns>Async task.</returns>
    private static async Task DescribeCaseAttachment(string attachmentId)
    {
        Console.WriteLine(new string('-', 80));
        Console.WriteLine($"9. Describe the attachment set.");

        var attachment = await _supportWrapper.DescribeAttachment(attachmentId);
        var data = Encoding.ASCII.GetString(attachment.Data.ToArray());
```

```
        Console.WriteLine($"\tAttachment includes {attachment.FileName} with
data: \n\t{data}");

        Console.WriteLine(new string('-', 80));
    }

    /// <summary>
    /// Resolve the support case.
    /// </summary>
    /// <param name="caseId">Id of the case to resolve.</param>
    /// <returns>Async task.</returns>
    private static async Task ResolveCase(string caseId)
    {
        Console.WriteLine(new string('-', 80));
        Console.WriteLine($"10. Resolve case {caseId}.");

        var status = await _supportWrapper.ResolveCase(caseId);
        Console.WriteLine($"\tCase {caseId} has final status {status}");

        Console.WriteLine(new string('-', 80));
    }

    /// <summary>
    /// List resolved cases for the current day.
    /// </summary>
    /// <returns>Async Task.</returns>
    private static async Task DescribeTodayResolvedCases()
    {
        Console.WriteLine(new string('-', 80));
        Console.WriteLine($"11. List the resolved support cases for the current
day.");
        var currentCases = await _supportWrapper.DescribeCases(
            new List<string>(),
            null,
            false,
            true,
            DateTime.UtcNow.Date,
            DateTime.UtcNow);

        foreach (var currentCase in currentCases)
        {
            if (currentCase.Status == "resolved")
            {
                Console.WriteLine(
```

```
                    $"\tCase: {currentCase.CaseId}: status
 {currentCase.Status}");
            }
        }

        Console.WriteLine(new string('-', 80));
    }
}
```

Méthodes d'encapsulation utilisées par le scénario pour les AWS Support actions.

```
/// <summary>
/// Wrapper methods to use AWS Support for working with support cases.
/// </summary>
public class SupportWrapper
{
    private readonly IAmazonAWSSupport _amazonSupport;
    public SupportWrapper(IAmazonAWSSupport amazonSupport)
    {
        _amazonSupport = amazonSupport;
    }


    /// <summary>
    /// Get the descriptions of AWS services.
    /// </summary>
    /// <param name="name">Optional language for services.
    /// Currently Chinese (“zh”), English ("en"), Japanese ("ja") and Korean
 (“ko”) are supported.</param>
    /// <returns>The list of AWS service descriptions.</returns>
    public async Task<List<Service>> DescribeServices(string language = "en")
    {
        var response = await _amazonSupport.DescribeServicesAsync(
            new DescribeServicesRequest()
            {
                Language = language
            });
        return response.Services;
    }
```

```
   /// <summary>
   /// Get the descriptions of support severity levels.
   /// </summary>
   /// <param name="name">Optional language for severity levels.
   /// Currently Chinese (“zh”), English ("en"), Japanese ("ja") and Korean
(“ko”) are supported.</param>
   /// <returns>The list of support severity levels.</returns>
   public async Task<List<SeverityLevel>> DescribeSeverityLevels(string language
= "en")
   {
       var response = await _amazonSupport.DescribeSeverityLevelsAsync(
           new DescribeSeverityLevelsRequest()
           {
               Language = language
           });
       return response.SeverityLevels;
   }



   /// <summary>
   /// Create a new support case.
   /// </summary>
   /// <param name="serviceCode">Service code for the new case.</param>
   /// <param name="categoryCode">Category for the new case.</param>
   /// <param name="severityCode">Severity code for the new case.</param>
   /// <param name="subject">Subject of the new case.</param>
   /// <param name="body">Body text of the new case.</param>
   /// <param name="language">Optional language support for your case.
   /// Currently Chinese (“zh”), English ("en"), Japanese ("ja") and Korean
(“ko”) are supported.</param>
   /// <param name="attachmentSetId">Optional Id for an attachment set for the
new case.</param>
   /// <param name="issueType">Optional issue type for the new case. Options are
"customer-service" or "technical".</param>
   /// <returns>The caseId of the new support case.</returns>
   public async Task<string> CreateCase(string serviceCode, string categoryCode,
string severityCode, string subject,
       string body, string language = "en", string? attachmentSetId = null,
string issueType = "customer-service")
   {
       var response = await _amazonSupport.CreateCaseAsync(
           new CreateCaseRequest()
```

```
            {
                ServiceCode = serviceCode,
                CategoryCode = categoryCode,
                SeverityCode = severityCode,
                Subject = subject,
                Language = language,
                AttachmentSetId = attachmentSetId,
                IssueType = issueType,
                CommunicationBody = body
            });
        return response.CaseId;
    }



    /// <summary>
    /// Add an attachment to a set, or create a new attachment set if one does
not exist.
    /// </summary>
    /// <param name="data">The data for the attachment.</param>
    /// <param name="fileName">The file name for the attachment.</param>
    /// <param name="attachmentSetId">Optional setId for the attachment. Creates
a new attachment set if empty.</param>
    /// <returns>The setId of the attachment.</returns>
    public async Task<string> AddAttachmentToSet(MemoryStream data, string
fileName, string? attachmentSetId = null)
    {
        var response = await _amazonSupport.AddAttachmentsToSetAsync(
            new AddAttachmentsToSetRequest
            {
                AttachmentSetId = attachmentSetId,
                Attachments = new List<Attachment>
                {
                    new Attachment
                    {
                        Data = data,
                        FileName = fileName
                    }
                }
            });
        return response.AttachmentSetId;
    }
```

```
    /// <summary>
    /// Get description of a specific attachment.
    /// </summary>
    /// <param name="attachmentId">Id of the attachment, usually fetched by
 describing the communications of a case.</param>
    /// <returns>The attachment object.</returns>
    public async Task<Attachment> DescribeAttachment(string attachmentId)
    {
        var response = await _amazonSupport.DescribeAttachmentAsync(
            new DescribeAttachmentRequest()
            {
                AttachmentId = attachmentId
            });
        return response.Attachment;
    }



    /// <summary>
    /// Add communication to a case, including optional attachment set ID and CC
 email addresses.
    /// </summary>
    /// <param name="caseId">Id for the support case.</param>
    /// <param name="body">Body text of the communication.</param>
    /// <param name="attachmentSetId">Optional Id for an attachment set.</param>
    /// <param name="ccEmailAddresses">Optional list of CC email addresses.</
param>
    /// <returns>True if successful.</returns>
    public async Task<bool> AddCommunicationToCase(string caseId, string body,
        string? attachmentSetId = null, List<string>? ccEmailAddresses = null)
    {
        var response = await _amazonSupport.AddCommunicationToCaseAsync(
            new AddCommunicationToCaseRequest()
            {
                CaseId = caseId,
                CommunicationBody = body,
                AttachmentSetId = attachmentSetId,
                CcEmailAddresses = ccEmailAddresses
            });
        return response.Result;
    }
```

```
    /// <summary>
    /// Describe the communications for a case, optionally with a date filter.
    /// </summary>
    /// <param name="caseId">The ID of the support case.</param>
    /// <param name="afterTime">The optional start date for a filtered search.</
param>
    /// <param name="beforeTime">The optional end date for a filtered search.</
param>
    /// <returns>The list of communications for the case.</returns>
    public async Task<List<Communication>> DescribeCommunications(string caseId,
 DateTime? afterTime = null, DateTime? beforeTime = null)
    {
        var results = new List<Communication>();
        var paginateCommunications =
 _amazonSupport.Paginators.DescribeCommunications(
            new DescribeCommunicationsRequest()
            {
                CaseId = caseId,
                AfterTime = afterTime?.ToString("s"),
                BeforeTime = beforeTime?.ToString("s")
            });
        // Get the entire list using the paginator.
        await foreach (var communications in
 paginateCommunications.Communications)
        {
            results.Add(communications);
        }
        return results;
    }



    /// <summary>
    /// Get case details for a list of case ids, optionally with date filters.
    /// </summary>
    /// <param name="caseIds">The list of case IDs.</param>
    /// <param name="displayId">Optional display ID.</param>
    /// <param name="includeCommunication">True to include communication.
 Defaults to true.</param>
    /// <param name="includeResolvedCases">True to include resolved cases.
 Defaults to false.</param>
    /// <param name="afterTime">The optional start date for a filtered search.</
param>
```

```
    /// <param name="beforeTime">The optional end date for a filtered search.</
param>
    /// <param name="language">Optional language support for your case.
    /// Currently Chinese (“zh”), English ("en"), Japanese ("ja") and Korean
 (“ko”) are supported.</param>
    /// <returns>A list of CaseDetails.</returns>
    public async Task<List<CaseDetails>> DescribeCases(List<string> caseIds,
 string? displayId = null, bool includeCommunication = true,
        bool includeResolvedCases = false, DateTime? afterTime = null, DateTime?
 beforeTime = null,
        string language = "en")
    {
        var results = new List<CaseDetails>();
        var paginateCases = _amazonSupport.Paginators.DescribeCases(
            new DescribeCasesRequest()
            {
                CaseIdList = caseIds,
                DisplayId = displayId,
                IncludeCommunications = includeCommunication,
                IncludeResolvedCases = includeResolvedCases,
                AfterTime = afterTime?.ToString("s"),
                BeforeTime = beforeTime?.ToString("s"),
                Language = language
            });
        // Get the entire list using the paginator.
        await foreach (var cases in paginateCases.Cases)
        {
            results.Add(cases);
        }
        return results;
    }



    /// <summary>
    /// Resolve a support case by caseId.
    /// </summary>
    /// <param name="caseId">Id for the support case.</param>
    /// <returns>The final status of the case after resolving.</returns>
    public async Task<string> ResolveCase(string caseId)
    {
        var response = await _amazonSupport.ResolveCaseAsync(
            new ResolveCaseRequest()
            {
```

```
                CaseId = caseId
            });
        return response.FinalCaseStatus;
    }


    /// <summary>
    /// Verify the support level for AWS Support API access.
    /// </summary>
    /// <returns>True if the subscription level supports API access.</returns>
    public async Task<bool> VerifySubscription()
    {
        try
        {
            var response = await _amazonSupport.DescribeServicesAsync(
                new DescribeServicesRequest()
                {
                    Language = "en"
                });
            return response.HttpStatusCode == HttpStatusCode.OK;
        }
        catch (Amazon.AWSSupport.AmazonAWSSupportException ex)
        {
            if (ex.ErrorCode == "SubscriptionRequiredException")
            {
                return false;
            }
            else throw;
        }
    }
}
```

- Pour plus d'informations sur l'API consultez les rubriques suivantes dans la référence de l'API AWS SDK for .NET .
  - AddAttachmentsToSet
  - AddCommunicationToCase
  - CreateCase
  - DescribeAttachment
  - DescribeCases
  - DescribeCommunications

- DescribeServices
- DescribeSeverityLevels
- ResolveCase

Java

SDK pour Java 2.x

> **Note**
>
> Il y en a plus sur GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples de code AWS.

Exécutez diverses AWS Support opérations.

```
import software.amazon.awssdk.core.SdkBytes;
import software.amazon.awssdk.regions.Region;
import software.amazon.awssdk.services.support.SupportClient;
import software.amazon.awssdk.services.support.model.AddAttachmentsToSetResponse;
import
 software.amazon.awssdk.services.support.model.AddCommunicationToCaseRequest;
import
 software.amazon.awssdk.services.support.model.AddCommunicationToCaseResponse;
import software.amazon.awssdk.services.support.model.Attachment;
import software.amazon.awssdk.services.support.model.AttachmentDetails;
import software.amazon.awssdk.services.support.model.CaseDetails;
import software.amazon.awssdk.services.support.model.Category;
import software.amazon.awssdk.services.support.model.Communication;
import software.amazon.awssdk.services.support.model.CreateCaseRequest;
import software.amazon.awssdk.services.support.model.CreateCaseResponse;
import software.amazon.awssdk.services.support.model.DescribeAttachmentRequest;
import software.amazon.awssdk.services.support.model.DescribeAttachmentResponse;
import software.amazon.awssdk.services.support.model.DescribeCasesRequest;
import software.amazon.awssdk.services.support.model.DescribeCasesResponse;
import
 software.amazon.awssdk.services.support.model.DescribeCommunicationsRequest;
import
 software.amazon.awssdk.services.support.model.DescribeCommunicationsResponse;
import software.amazon.awssdk.services.support.model.DescribeServicesRequest;
import software.amazon.awssdk.services.support.model.DescribeServicesResponse;
```

```
import
 software.amazon.awssdk.services.support.model.DescribeSeverityLevelsRequest;
import
 software.amazon.awssdk.services.support.model.DescribeSeverityLevelsResponse;
import software.amazon.awssdk.services.support.model.ResolveCaseRequest;
import software.amazon.awssdk.services.support.model.ResolveCaseResponse;
import software.amazon.awssdk.services.support.model.Service;
import software.amazon.awssdk.services.support.model.SeverityLevel;
import software.amazon.awssdk.services.support.model.SupportException;
import software.amazon.awssdk.services.support.model.AddAttachmentsToSetRequest;
import java.io.File;
import java.io.FileInputStream;
import java.io.FileNotFoundException;
import java.io.InputStream;
import java.time.Instant;
import java.time.temporal.ChronoUnit;
import java.util.ArrayList;
import java.util.List;

/**
 * Before running this Java (v2) code example, set up your development
 * environment, including your credentials.
 *
 * For more information, see the following documentation topic:
 *
 * https://docs.aws.amazon.com/sdk-for-java/latest/developer-guide/get-
started.html
 *
 * In addition, you must have the AWS Business Support Plan to use the AWS
 * Support Java API. For more information, see:
 *
 * https://aws.amazon.com/premiumsupport/plans/
 *
 * This Java example performs the following tasks:
 *
 * 1. Gets and displays available services.
 * 2. Gets and displays severity levels.
 * 3. Creates a support case by using the selected service, category, and
 * severity level.
 * 4. Gets a list of open cases for the current day.
 * 5. Creates an attachment set with a generated file.
 * 6. Adds a communication with the attachment to the support case.
 * 7. Lists the communications of the support case.
 * 8. Describes the attachment set included with the communication.
```

```
 * 9. Resolves the support case.
 * 10. Gets a list of resolved cases for the current day.
 */
public class SupportScenario {

   public static final String DASHES = new String(new char[80]).replace("\0",
 "-");

   public static void main(String[] args) {
       final String usage = """

               Usage:
                   <fileAttachment>Where:
                   fileAttachment - The file can be a simple saved .txt file to
 use as an email attachment.\s
               """;

       if (args.length != 1) {
           System.out.println(usage);
           System.exit(1);
       }

       String fileAttachment = args[0];
       Region region = Region.US_WEST_2;
       SupportClient supportClient = SupportClient.builder()
               .region(region)
               .build();

       System.out.println(DASHES);
       System.out.println("***** Welcome to the AWS Support case example
 scenario.");
       System.out.println(DASHES);

       System.out.println(DASHES);
       System.out.println("1. Get and display available services.");
       List<String> sevCatList = displayServices(supportClient);
       System.out.println(DASHES);

       System.out.println(DASHES);
       System.out.println("2. Get and display Support severity levels.");
       String sevLevel = displaySevLevels(supportClient);
       System.out.println(DASHES);

       System.out.println(DASHES);
```

```
        System.out.println("3. Create a support case using the selected service,
category, and severity level.");
        String caseId = createSupportCase(supportClient, sevCatList, sevLevel);
        if (caseId.compareTo("") == 0) {
            System.out.println("A support case was not successfully created!");
            System.exit(1);
        } else
            System.out.println("Support case " + caseId + " was successfully
created!");
        System.out.println(DASHES);

        System.out.println(DASHES);
        System.out.println("4. Get open support cases.");
        getOpenCase(supportClient);
        System.out.println(DASHES);

        System.out.println(DASHES);
        System.out.println("5. Create an attachment set with a generated file to
add to the case.");
        String attachmentSetId = addAttachment(supportClient, fileAttachment);
        System.out.println("The Attachment Set id value is" + attachmentSetId);
        System.out.println(DASHES);

        System.out.println(DASHES);
        System.out.println("6. Add communication with the attachment to the
support case.");
        addAttachSupportCase(supportClient, caseId, attachmentSetId);
        System.out.println(DASHES);

        System.out.println(DASHES);
        System.out.println("7. List the communications of the support case.");
        String attachId = listCommunications(supportClient, caseId);
        System.out.println("The Attachment id value is" + attachId);
        System.out.println(DASHES);

        System.out.println(DASHES);
        System.out.println("8. Describe the attachment set included with the
communication.");
        describeAttachment(supportClient, attachId);
        System.out.println(DASHES);

        System.out.println(DASHES);
        System.out.println("9. Resolve the support case.");
        resolveSupportCase(supportClient, caseId);
```

```
        System.out.println(DASHES);

        System.out.println(DASHES);
        System.out.println("10. Get a list of resolved cases for the current
day.");
        getResolvedCase(supportClient);
        System.out.println(DASHES);

        System.out.println(DASHES);
        System.out.println("***** This Scenario has successfully completed");
        System.out.println(DASHES);
    }

    public static void getResolvedCase(SupportClient supportClient) {
        try {
            // Specify the start and end time.
            Instant now = Instant.now();
            java.time.LocalDate.now();
            Instant yesterday = now.minus(1, ChronoUnit.DAYS);

            DescribeCasesRequest describeCasesRequest =
DescribeCasesRequest.builder()
                    .maxResults(30)
                    .afterTime(yesterday.toString())
                    .beforeTime(now.toString())
                    .includeResolvedCases(true)
                    .build();

            DescribeCasesResponse response =
supportClient.describeCases(describeCasesRequest);
            List<CaseDetails> cases = response.cases();
            for (CaseDetails sinCase : cases) {
                if (sinCase.status().compareTo("resolved") == 0)
                    System.out.println("The case status is " + sinCase.status());
            }

        } catch (SupportException e) {
            System.out.println(e.getLocalizedMessage());
            System.exit(1);
        }
    }

    public static void resolveSupportCase(SupportClient supportClient, String
caseId) {
```

```
        try {
            ResolveCaseRequest caseRequest = ResolveCaseRequest.builder()
                    .caseId(caseId)
                    .build();

            ResolveCaseResponse response =
supportClient.resolveCase(caseRequest);
            System.out.println("The status of case " + caseId + " is " +
response.finalCaseStatus());

        } catch (SupportException e) {
            System.out.println(e.getLocalizedMessage());
            System.exit(1);
        }
    }

    public static void describeAttachment(SupportClient supportClient, String
attachId) {
        try {
            DescribeAttachmentRequest attachmentRequest =
DescribeAttachmentRequest.builder()
                    .attachmentId(attachId)
                    .build();

            DescribeAttachmentResponse response =
supportClient.describeAttachment(attachmentRequest);
            System.out.println("The name of the file is " +
response.attachment().fileName());

        } catch (SupportException e) {
            System.out.println(e.getLocalizedMessage());
            System.exit(1);
        }
    }

    public static String listCommunications(SupportClient supportClient, String
caseId) {
        try {
            String attachId = null;
            DescribeCommunicationsRequest communicationsRequest =
DescribeCommunicationsRequest.builder()
                    .caseId(caseId)
                    .maxResults(10)
                    .build();
```

```
            DescribeCommunicationsResponse response =
supportClient.describeCommunications(communicationsRequest);
            List<Communication> communications = response.communications();
            for (Communication comm : communications) {
                System.out.println("the body is: " + comm.body());

                // Get the attachment id value.
                List<AttachmentDetails> attachments = comm.attachmentSet();
                for (AttachmentDetails detail : attachments) {
                    attachId = detail.attachmentId();
                }
            }
            return attachId;

        } catch (SupportException e) {
            System.out.println(e.getLocalizedMessage());
            System.exit(1);
        }
        return "";
    }

    public static void addAttachSupportCase(SupportClient supportClient, String
caseId, String attachmentSetId) {
        try {
            AddCommunicationToCaseRequest caseRequest =
AddCommunicationToCaseRequest.builder()
                    .caseId(caseId)
                    .attachmentSetId(attachmentSetId)
                    .communicationBody("Please refer to attachment for details.")
                    .build();

            AddCommunicationToCaseResponse response =
supportClient.addCommunicationToCase(caseRequest);
            if (response.result())
                System.out.println("You have successfully added a communication
to an AWS Support case");
            else
                System.out.println("There was an error adding the communication
to an AWS Support case");

        } catch (SupportException e) {
            System.out.println(e.getLocalizedMessage());
            System.exit(1);
```

```
        }
    }

    public static String addAttachment(SupportClient supportClient, String
fileAttachment) {
        try {
            File myFile = new File(fileAttachment);
            InputStream sourceStream = new FileInputStream(myFile);
            SdkBytes sourceBytes = SdkBytes.fromInputStream(sourceStream);

            Attachment attachment = Attachment.builder()
                    .fileName(myFile.getName())
                    .data(sourceBytes)
                    .build();

            AddAttachmentsToSetRequest setRequest =
AddAttachmentsToSetRequest.builder()
                    .attachments(attachment)
                    .build();

            AddAttachmentsToSetResponse response =
supportClient.addAttachmentsToSet(setRequest);
            return response.attachmentSetId();

        } catch (SupportException | FileNotFoundException e) {
            System.out.println(e.getLocalizedMessage());
            System.exit(1);
        }
        return "";
    }

    public static void getOpenCase(SupportClient supportClient) {
        try {
            // Specify the start and end time.
            Instant now = Instant.now();
            java.time.LocalDate.now();
            Instant yesterday = now.minus(1, ChronoUnit.DAYS);

            DescribeCasesRequest describeCasesRequest =
DescribeCasesRequest.builder()
                    .maxResults(20)
                    .afterTime(yesterday.toString())
                    .beforeTime(now.toString())
                    .build();
```

```
            DescribeCasesResponse response =
supportClient.describeCases(describeCasesRequest);
            List<CaseDetails> cases = response.cases();
            for (CaseDetails sinCase : cases) {
                System.out.println("The case status is " + sinCase.status());
                System.out.println("The case Id is " + sinCase.caseId());
                System.out.println("The case subject is " + sinCase.subject());
            }

        } catch (SupportException e) {
            System.out.println(e.getLocalizedMessage());
            System.exit(1);
        }
    }

    public static String createSupportCase(SupportClient supportClient,
List<String> sevCatList, String sevLevel) {
        try {
            String serviceCode = sevCatList.get(0);
            String caseCat = sevCatList.get(1);
            CreateCaseRequest caseRequest = CreateCaseRequest.builder()
                    .categoryCode(caseCat.toLowerCase())
                    .serviceCode(serviceCode.toLowerCase())
                    .severityCode(sevLevel.toLowerCase())
                    .communicationBody("Test issue with " +
serviceCode.toLowerCase())
                    .subject("Test case, please ignore")
                    .language("en")
                    .issueType("technical")
                    .build();

            CreateCaseResponse response = supportClient.createCase(caseRequest);
            return response.caseId();

        } catch (SupportException e) {
            System.out.println(e.getLocalizedMessage());
            System.exit(1);
        }
        return "";
    }

    public static String displaySevLevels(SupportClient supportClient) {
        try {
```

```
            DescribeSeverityLevelsRequest severityLevelsRequest =
DescribeSeverityLevelsRequest.builder()
                    .language("en")
                    .build();

            DescribeSeverityLevelsResponse response =
supportClient.describeSeverityLevels(severityLevelsRequest);
            List<SeverityLevel> severityLevels = response.severityLevels();
            String levelName = null;
            for (SeverityLevel sevLevel : severityLevels) {
                System.out.println("The severity level name is: " +
sevLevel.name());
                if (sevLevel.name().compareTo("High") == 0)
                    levelName = sevLevel.name();
            }
            return levelName;

        } catch (SupportException e) {
            System.out.println(e.getLocalizedMessage());
            System.exit(1);
        }
        return "";
    }

    // Return a List that contains a Service name and Category name.
    public static List<String> displayServices(SupportClient supportClient) {
        try {
            DescribeServicesRequest servicesRequest =
DescribeServicesRequest.builder()
                    .language("en")
                    .build();

            DescribeServicesResponse response =
supportClient.describeServices(servicesRequest);
            String serviceCode = null;
            String catName = null;
            List<String> sevCatList = new ArrayList<>();
            List<Service> services = response.services();

            System.out.println("Get the first 10 services");
            int index = 1;
            for (Service service : services) {
                if (index == 11)
                    break;
```

```
                System.out.println("The Service name is: " + service.name());
                if (service.name().compareTo("Account") == 0)
                    serviceCode = service.code();

                // Get the Categories for this service.
                List<Category> categories = service.categories();
                for (Category cat : categories) {
                    System.out.println("The category name is: " + cat.name());
                    if (cat.name().compareTo("Security") == 0)
                        catName = cat.name();
                }
                index++;
            }

            // Push the two values to the list.
            sevCatList.add(serviceCode);
            sevCatList.add(catName);
            return sevCatList;

        } catch (SupportException e) {
            System.out.println(e.getLocalizedMessage());
            System.exit(1);
        }
        return null;
    }
}
```

- Pour plus d'informations sur l'API consultez les rubriques suivantes dans la référence de l'API AWS SDK for Java 2.x .
  - AddAttachmentsToSet
  - AddCommunicationToCase
  - CreateCase
  - DescribeAttachment
  - DescribeCases
  - DescribeCommunications
  - DescribeServices
  - DescribeSeverityLevels

- ResolveCase

JavaScript

SDK pour JavaScript (v3)

> **Note**
>
> Il y en a plus sur GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples de code AWS.

Exécutez un scénario interactif dans le terminal.

```
import {
  AddAttachmentsToSetCommand,
  AddCommunicationToCaseCommand,
  CreateCaseCommand,
  DescribeAttachmentCommand,
  DescribeCasesCommand,
  DescribeCommunicationsCommand,
  DescribeServicesCommand,
  DescribeSeverityLevelsCommand,
  ResolveCaseCommand,
  SupportClient,
} from "@aws-sdk/client-support";
import inquirer from "inquirer";

// Retry an asynchronous function on failure.
const retry = async ({ intervalInMs = 500, maxRetries = 10 }, fn) => {
  try {
    return await fn();
  } catch (err) {
    console.log(`Function call failed. Retrying.`);
    console.error(err.message);
    if (maxRetries === 0) throw err;
    await new Promise((resolve) => setTimeout(resolve, intervalInMs));
    return retry({ intervalInMs, maxRetries: maxRetries - 1 }, fn);
  }
};

const wrapText = (text, char = "=") => {
```

```
  const rule = char.repeat(80);
  return `${rule}\n    ${text}\n${rule}\n`;
};

const client = new SupportClient({ region: "us-east-1" });

// Verify that the account has a Support plan.
export const verifyAccount = async () => {
  const command = new DescribeServicesCommand({});

  try {
    await client.send(command);
  } catch (err) {
    if (err.name === "SubscriptionRequiredException") {
      throw new Error(
        "You must be subscribed to the AWS Support plan to use this feature."
      );
    } else {
      throw err;
    }
  }
};

// Get the list of available services.
export const getService = async () => {
  const { services } = await client.send(new DescribeServicesCommand({}));
  const { selectedService } = await inquirer.prompt({
    name: "selectedService",
    type: "list",
    message:
      "Select a service. Your support case will be created for this service. The
 list of services is truncated for readability.",
    choices: services.slice(0, 10).map((s) => ({ name: s.name, value: s })),
  });
  return selectedService;
};

// Get the list of available support case categories for a service.
export const getCategory = async (service) => {
  const { selectedCategory } = await inquirer.prompt({
    name: "selectedCategory",
    type: "list",
    message: "Select a category.",
    choices: service.categories.map((c) => ({ name: c.name, value: c })),
```

```
  });
  return selectedCategory;
};

// Get the available severity levels for the account.
export const getSeverityLevel = async () => {
  const command = new DescribeSeverityLevelsCommand({});
  const { severityLevels } = await client.send(command);
  const { selectedSeverityLevel } = await inquirer.prompt({
    name: "selectedSeverityLevel",
    type: "list",
    message: "Select a severity level.",
    choices: severityLevels.map((s) => ({ name: s.name, value: s })),
  });
  return selectedSeverityLevel;
};

// Create a new support case and return the caseId.
export const createCase = async ({
  selectedService,
  selectedCategory,
  selectedSeverityLevel,
}) => {
  const command = new CreateCaseCommand({
    subject: "IGNORE: Test case",
    communicationBody: "This is a test. Please ignore.",
    serviceCode: selectedService.code,
    categoryCode: selectedCategory.code,
    severityCode: selectedSeverityLevel.code,
  });
  const { caseId } = await client.send(command);
  return caseId;
};

// Get a list of open support cases created today.
export const getTodaysOpenCases = async () => {
  const d = new Date();
  const startOfToday = new Date(d.getFullYear(), d.getMonth(), d.getDate());
  const command = new DescribeCasesCommand({
    includeCommunications: false,
    afterTime: startOfToday.toISOString(),
  });

  const { cases } = await client.send(command);
```

```
  if (cases.length === 0) {
    throw new Error(
      "Unexpected number of cases. Expected more than 0 open cases."
    );
  }
  return cases;
};

// Create an attachment set.
export const createAttachmentSet = async () => {
  const command = new AddAttachmentsToSetCommand({
    attachments: [
      {
        fileName: "example.txt",
        data: new TextEncoder().encode("some example text"),
      },
    ],
  });
  const { attachmentSetId } = await client.send(command);
  return attachmentSetId;
};

export const linkAttachmentSetToCase = async (attachmentSetId, caseId) => {
  const command = new AddCommunicationToCaseCommand({
    attachmentSetId,
    caseId,
    communicationBody: "Adding attachment set to case.",
  });
  await client.send(command);
};

// Get all communications for a support case.
export const getCommunications = async (caseId) => {
  const command = new DescribeCommunicationsCommand({
    caseId,
  });
  const { communications } = await client.send(command);
  return communications;
};

// Get an attachment set.
export const getFirstAttachment = (communications) => {
  const firstCommWithAttachment = communications.find(
```

```
    (c) => c.attachmentSet.length > 0
  );
  return firstCommWithAttachment?.attachmentSet[0].attachmentId;
};

// Get an attachment.
export const getAttachment = async (attachmentId) => {
  const command = new DescribeAttachmentCommand({
    attachmentId,
  });
  const { attachment } = await client.send(command);
  return attachment;
};

// Resolve the case matching the given case ID.
export const resolveCase = async (caseId) => {
  const { shouldResolve } = await inquirer.prompt({
    name: "shouldResolve",
    type: "confirm",
    message: `Do you want to resolve ${caseId}?`,
  });

  if (shouldResolve) {
    const command = new ResolveCaseCommand({
      caseId: caseId,
    });

    await client.send(command);
    return true;
  }
  return false;
};

// Find a specific case in the list of provided cases by case ID.
// If the case is not found, and the results are paginated, continue
// paging through the results.
export const findCase = async ({ caseId, cases, nextToken }) => {
  const foundCase = cases.find((c) => c.caseId === caseId);

  if (foundCase) {
    return foundCase;
  }

  if (nextToken) {
```

```
    const response = await client.send(
      new DescribeCasesCommand({
        nextToken,
        includeResolvedCases: true,
      })
    );
    return findCase({
      caseId,
      cases: response.cases,
      nextToken: response.nextToken,
    });
  }

  throw new Error(`${caseId} not found.`);
};

// Get all cases created today.
export const getTodaysResolvedCases = async (caseIdToWaitFor) => {
  const d = new Date("2023-01-18");
  const startOfToday = new Date(d.getFullYear(), d.getMonth(), d.getDate());
  const command = new DescribeCasesCommand({
    includeCommunications: false,
    afterTime: startOfToday.toISOString(),
    includeResolvedCases: true,
  });
  const { cases, nextToken } = await client.send(command);
  await findCase({ cases, caseId: caseIdToWaitFor, nextToken });
  return cases.filter((c) => c.status === "resolved");
};

const main = async () => {
  let caseId;
  try {
    console.log(wrapText("Welcome to the AWS Support basic usage scenario."));

    // Verify that the account is subscribed to support.
    await verifyAccount();

    // Provided a truncated list of services and prompt the user to select one.
    const selectedService = await getService();

    // Provided the categories for the selected service and prompt the user to
 select one.
    const selectedCategory = await getCategory(selectedService);
```

```
   // Provide the severity available severity levels for the account and prompt
the user to select one.
   const selectedSeverityLevel = await getSeverityLevel();

   // Create a support case.
   console.log("\nCreating a support case.");
   caseId = await createCase({
     selectedService,
     selectedCategory,
     selectedSeverityLevel,
   });
   console.log(`Support case created: ${caseId}`);

   // Display a list of open support cases created today.
   const todaysOpenCases = await retry(
     { intervalInMs: 1000, maxRetries: 15 },
     getTodaysOpenCases
   );
   console.log(
     `\nOpen support cases created today: ${todaysOpenCases.length}`
   );
   console.log(todaysOpenCases.map((c) => `${c.caseId}`).join("\n"));

   // Create an attachment set.
   console.log("\nCreating an attachment set.");
   const attachmentSetId = await createAttachmentSet();
   console.log(`Attachment set created: ${attachmentSetId}`);

   // Add the attachment set to the support case.
   console.log(`\nAdding attachment set to ${caseId}`);
   await linkAttachmentSetToCase(attachmentSetId, caseId);
   console.log(`Attachment set added to ${caseId}`);

   // List the communications for a support case.
   console.log(`\nListing communications for ${caseId}`);
   const communications = await getCommunications(caseId);
   console.log(
     communications
       .map(
         (c) =>
           `Communication created on ${c.timeCreated}. Has
${c.attachmentSet.length} attachments.`
       )
```

```
        .join("\n")
    );

    // Describe the first attachment.
    console.log(`\nDescribing attachment ${attachmentSetId}`);
    const attachmentId = getFirstAttachment(communications);
    const attachment = await getAttachment(attachmentId);
    console.log(
      `Attachment is the file '${
        attachment.fileName
      }' with data: \n${new TextDecoder().decode(attachment.data)}`
    );

    // Confirm that the support case should be resolved.
    const isResolved = await resolveCase(caseId);
    if (isResolved) {
      // List the resolved cases and include the one previously created.
      // Resolved cases can take a while to appear.
      console.log(
        "\nWaiting for case status to be marked as resolved. This can take some
 time."
      );
      const resolvedCases = await retry(
        { intervalInMs: 20000, maxRetries: 15 },
        () => getTodaysResolvedCases(caseId)
      );
      console.log("Resolved cases:");
      console.log(resolvedCases.map((c) => c.caseId).join("\n"));
    }
  } catch (err) {
    console.error(err);
  }
};
```

- Pour plus d'informations sur l'API consultez les rubriques suivantes dans la référence de l'API AWS SDK for JavaScript .
  - AddAttachmentsToSet
  - AddCommunicationToCase
  - CreateCase
  - DescribeAttachment

- DescribeCases
- DescribeCommunications
- DescribeServices
- DescribeSeverityLevels
- ResolveCase

Kotlin

SDK pour Kotlin

> **Note**
>
> Il y en a plus sur GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples de code AWS.

```
/**
Before running this Kotlin code example, set up your development environment,
including your credentials.

For more information, see the following documentation topic:

https://docs.aws.amazon.com/sdk-for-kotlin/latest/developer-guide/setup.html
In addition, you must have the AWS Business Support Plan to use the AWS Support
 Java API. For more information, see:

https://aws.amazon.com/premiumsupport/plans/

This Kotlin example performs the following tasks:
1. Gets and displays available services.
2. Gets and displays severity levels.
3. Creates a support case by using the selected service, category, and severity
 level.
4. Gets a list of open cases for the current day.
5. Creates an attachment set with a generated file.
6. Adds a communication with the attachment to the support case.
7. Lists the communications of the support case.
8. Describes the attachment set included with the communication.
9. Resolves the support case.
10. Gets a list of resolved cases for the current day.
```

```
*/

suspend fun main(args: Array<String>) {
    val usage = """
    Usage:
        <fileAttachment>
    Where:
         fileAttachment - The file can be a simple saved .txt file to use as an
 email attachment.
    """

    if (args.size != 1) {
        println(usage)
        exitProcess(0)
    }

    val fileAttachment = args[0]
    println("***** Welcome to the AWS Support case example scenario.")
    println("***** Step 1. Get and display available services.")
    val sevCatList = displayServices()

    println("***** Step 2. Get and display Support severity levels.")
    val sevLevel = displaySevLevels()

    println("***** Step 3. Create a support case using the selected service,
 category, and severity level.")
    val caseIdVal = createSupportCase(sevCatList, sevLevel)
    if (caseIdVal != null) {
        println("Support case $caseIdVal was successfully created!")
    } else {
        println("A support case was not successfully created!")
        exitProcess(1)
    }

    println("***** Step 4. Get open support cases.")
    getOpenCase()

    println("***** Step 5. Create an attachment set with a generated file to add
 to the case.")
    val attachmentSetId = addAttachment(fileAttachment)
    println("The Attachment Set id value is $attachmentSetId")

    println("***** Step 6. Add communication with the attachment to the support
 case.")
```

```
    addAttachSupportCase(caseIdVal, attachmentSetId)

    println("***** Step 7. List the communications of the support case.")
    val attachId = listCommunications(caseIdVal)
    println("The Attachment id value is $attachId")

    println("***** Step 8. Describe the attachment set included with the
 communication.")
    describeAttachment(attachId)

    println("***** Step 9. Resolve the support case.")
    resolveSupportCase(caseIdVal)

    println("***** Step 10. Get a list of resolved cases for the current day.")
    getResolvedCase()
    println("***** This Scenario has successfully completed")
}

suspend fun getResolvedCase() {
    // Specify the start and end time.
    val now = Instant.now()
    LocalDate.now()
    val yesterday = now.minus(1, ChronoUnit.DAYS)
    val describeCasesRequest = DescribeCasesRequest {
        maxResults = 30
        afterTime = yesterday.toString()
        beforeTime = now.toString()
        includeResolvedCases = true
    }

    SupportClient { region = "us-west-2" }.use { supportClient ->
        val response = supportClient.describeCases(describeCasesRequest)
        response.cases?.forEach { sinCase ->
            println("The case status is ${sinCase.status}")
            println("The case Id is ${sinCase.caseId}")
            println("The case subject is ${sinCase.subject}")
        }
    }
}

suspend fun resolveSupportCase(caseIdVal: String) {
    val caseRequest = ResolveCaseRequest {
        caseId = caseIdVal
    }
```

```
    SupportClient { region = "us-west-2" }.use { supportClient ->
        val response = supportClient.resolveCase(caseRequest)
        println("The status of case $caseIdVal is ${response.finalCaseStatus}")
    }
}

suspend fun describeAttachment(attachId: String?) {
    val attachmentRequest = DescribeAttachmentRequest {
        attachmentId = attachId
    }

    SupportClient { region = "us-west-2" }.use { supportClient ->
        val response = supportClient.describeAttachment(attachmentRequest)
        println("The name of the file is ${response.attachment?.fileName}")
    }
}

suspend fun listCommunications(caseIdVal: String?): String? {
    val communicationsRequest = DescribeCommunicationsRequest {
        caseId = caseIdVal
        maxResults = 10
    }

    SupportClient { region = "us-west-2" }.use { supportClient ->
        val response =
 supportClient.describeCommunications(communicationsRequest)
        response.communications?.forEach { comm ->
            println("the body is: " + comm.body)
            comm.attachmentSet?.forEach { detail ->
                return detail.attachmentId
            }
        }
    }
    return ""
}

suspend fun addAttachSupportCase(caseIdVal: String?, attachmentSetIdVal: String?)
 {
    val caseRequest = AddCommunicationToCaseRequest {
        caseId = caseIdVal
        attachmentSetId = attachmentSetIdVal
        communicationBody = "Please refer to attachment for details."
    }
```

```
    SupportClient { region = "us-west-2" }.use { supportClient ->
        val response = supportClient.addCommunicationToCase(caseRequest)
        if (response.result) {
            println("You have successfully added a communication to an AWS
 Support case")
        } else {
            println("There was an error adding the communication to an AWS
 Support case")
        }
    }
}

suspend fun addAttachment(fileAttachment: String): String? {
    val myFile = File(fileAttachment)
    val sourceBytes = (File(fileAttachment).readBytes())
    val attachmentVal = Attachment {
        fileName = myFile.name
        data = sourceBytes
    }

    val setRequest = AddAttachmentsToSetRequest {
        attachments = listOf(attachmentVal)
    }

    SupportClient { region = "us-west-2" }.use { supportClient ->
        val response = supportClient.addAttachmentsToSet(setRequest)
        return response.attachmentSetId
    }
}

suspend fun getOpenCase() {
    // Specify the start and end time.
    val now = Instant.now()
    LocalDate.now()
    val yesterday = now.minus(1, ChronoUnit.DAYS)
    val describeCasesRequest = DescribeCasesRequest {
        maxResults = 20
        afterTime = yesterday.toString()
        beforeTime = now.toString()
    }

    SupportClient { region = "us-west-2" }.use { supportClient ->
        val response = supportClient.describeCases(describeCasesRequest)
        response.cases?.forEach { sinCase ->
```

```
            println("The case status is ${sinCase.status}")
            println("The case Id is ${sinCase.caseId}")
            println("The case subject is ${sinCase.subject}")
        }
    }
}

suspend fun createSupportCase(sevCatListVal: List<String>, sevLevelVal: String):
 String? {
    val serCode = sevCatListVal[0]
    val caseCategory = sevCatListVal[1]
    val caseRequest = CreateCaseRequest {
        categoryCode = caseCategory.lowercase(Locale.getDefault())
        serviceCode = serCode.lowercase(Locale.getDefault())
        severityCode = sevLevelVal.lowercase(Locale.getDefault())
        communicationBody = "Test issue with
 ${serCode.lowercase(Locale.getDefault())}"
        subject = "Test case, please ignore"
        language = "en"
        issueType = "technical"
    }

    SupportClient { region = "us-west-2" }.use { supportClient ->
        val response = supportClient.createCase(caseRequest)
        return response.caseId
    }
}

suspend fun displaySevLevels(): String {
    var levelName = ""
    val severityLevelsRequest = DescribeSeverityLevelsRequest {
        language = "en"
    }

    SupportClient { region = "us-west-2" }.use { supportClient ->
        val response =
 supportClient.describeSeverityLevels(severityLevelsRequest)
        response.severityLevels?.forEach { sevLevel ->
            println("The severity level name is: ${sevLevel.name}")
            if (sevLevel.name == "High") {
                levelName = sevLevel.name!!
            }
        }
        return levelName
```

```
    }
}

// Return a List that contains a Service name and Category name.
suspend fun displayServices(): List<String> {
    var serviceCode = ""
    var catName = ""
    val sevCatList = mutableListOf<String>()
    val servicesRequest = DescribeServicesRequest {
        language = "en"
    }

    SupportClient { region = "us-west-2" }.use { supportClient ->
        val response = supportClient.describeServices(servicesRequest)
        println("Get the first 10 services")
        var index = 1

        response.services?.forEach { service ->
            if (index == 11) {
                return@forEach
            }

            println("The Service name is ${service.name}")
            if (service.name == "Account") {
                serviceCode = service.code.toString()
            }

            // Get the categories for this service.
            service.categories?.forEach { cat ->
                println("The category name is ${cat.name}")
                if (cat.name == "Security") {
                    catName = cat.name!!
                }
            }
            index++
        }
    }

    // Push the two values to the list.
    serviceCode.let { sevCatList.add(it) }
    catName.let { sevCatList.add(it) }
    return sevCatList
}
```

- Pour plus d'informations sur l'API, consultez les rubriques suivantes dans AWS SDK for Kotlin API reference.
  - AddAttachmentsToSet
  - AddCommunicationToCase
  - CreateCase
  - DescribeAttachment
  - DescribeCases
  - DescribeCommunications
  - DescribeServices
  - DescribeSeverityLevels
  - ResolveCase

Python

SDK pour Python (Boto3)

> **Note**
>
> Il y en a plus sur GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples de code AWS.

Exécutez un scénario interactif à une invite de commande.

```
class SupportCasesScenario:
    """Runs an interactive scenario that shows how to get started using AWS
 Support."""

    def __init__(self, support_wrapper):
        """
        :param support_wrapper: An object that wraps AWS Support actions.
        """
        self.support_wrapper = support_wrapper

    def display_and_select_service(self):
        """
```

```
        Lists support services and prompts the user to select one.

        :return: The support service selected by the user.
        """
        print("-" * 88)
        services_list = self.support_wrapper.describe_services("en")
        print(f"AWS Support client returned {len(services_list)} services.")
        print("Displaying first 10 services:")

        service_choices = [svc["name"] for svc in services_list[:10]]
        selected_index = q.choose(
            "Select an example support service by entering a number from the
preceding list:",
            service_choices,
        )
        selected_service = services_list[selected_index]
        print("-" * 88)
        return selected_service

    def display_and_select_category(self, service):
        """
        Lists categories for a support service and prompts the user to select
one.

        :param service: The service of the categories.
        :return: The selected category.
        """
        print("-" * 88)
        print(
            f"Available support categories for Service {service['name']}
{len(service['categories'])}:"
        )
        categories_choices = [category["name"] for category in
service["categories"]]
        selected_index = q.choose(
            "Select an example support category by entering a number from the
preceding list:",
            categories_choices,
        )
        selected_category = service["categories"][selected_index]
        print("-" * 88)
        return selected_category

    def display_and_select_severity(self):
```

```
        """
        Lists available severity levels and prompts the user to select one.

        :return: The selected severity level.
        """
        print("-" * 88)
        severity_levels_list =
self.support_wrapper.describe_severity_levels("en")
        print(f"Available severity levels:")
        severity_choices = [level["name"] for level in severity_levels_list]
        selected_index = q.choose(
            "Select an example severity level by entering a number from the
preceding list:",
            severity_choices,
        )
        selected_severity = severity_levels_list[selected_index]
        print("-" * 88)
        return selected_severity

    def create_example_case(self, service, category, severity_level):
        """
        Creates an example support case with the user's selections.

        :param service: The service for the new case.
        :param category: The category for the new case.
        :param severity_level: The severity level for the new case.
        :return: The caseId of the new support case.
        """
        print("-" * 88)
        print(f"Creating new case for service {service['name']}.")
        case_id = self.support_wrapper.create_case(service, category,
severity_level)
        print(f"\tNew case created with ID {case_id}.")
        print("-" * 88)
        return case_id

    def list_open_cases(self):
        """
        List the open cases for the current day.
        """
        print("-" * 88)
        print("Let's list the open cases for the current day.")
        start_time = str(datetime.utcnow().date())
        end_time = str(datetime.utcnow().date() + timedelta(days=1))
```

```
        open_cases = self.support_wrapper.describe_cases(start_time, end_time,
False)
        for case in open_cases:
            print(f"\tCase: {case['caseId']}: status {case['status']}.")
        print("-" * 88)

    def create_attachment_set(self):
        """
        Create an attachment set with a sample file.

        :return: The attachment set ID of the new attachment set.
        """
        print("-" * 88)
        print("Creating attachment set with a sample file.")
        attachment_set_id = self.support_wrapper.add_attachment_to_set()
        print(f"\tNew attachment set created with ID {attachment_set_id}.")
        print("-" * 88)
        return attachment_set_id

    def add_communication(self, case_id, attachment_set_id):
        """
        Add a communication with an attachment set to the case.

        :param case_id: The ID of the case for the communication.
        :param attachment_set_id: The ID of the attachment set to
        add to the communication.
        """
        print("-" * 88)
        print(f"Adding a communication and attachment set to the case.")
        self.support_wrapper.add_communication_to_case(attachment_set_id,
case_id)
        print(
            f"Added a communication and attachment set {attachment_set_id} to the
case {case_id}."
        )
        print("-" * 88)

    def list_communications(self, case_id):
        """
        List the communications associated with a case.

        :param case_id: The ID of the case.
        :return: The attachment ID of an attachment.
        """
```

```
        print("-" * 88)
        print("Let's list the communications for our case.")
        attachment_id = ""
        communications =
self.support_wrapper.describe_all_case_communications(case_id)
        for communication in communications:
            print(
                f"\tCommunication created on {communication['timeCreated']} "
                f"has {len(communication['attachmentSet'])} attachments."
            )
            if len(communication["attachmentSet"]) > 0:
                attachment_id = communication["attachmentSet"][0]["attachmentId"]
        print("-" * 88)
        return attachment_id

    def describe_case_attachment(self, attachment_id):
        """
        Describe an attachment associated with a case.

        :param attachment_id: The ID of the attachment.
        """
        print("-" * 88)
        print("Let's list the communications for our case.")
        attached_file = self.support_wrapper.describe_attachment(attachment_id)
        print(f"\tAttachment includes file {attached_file}.")
        print("-" * 88)

    def resolve_case(self, case_id):
        """
        Shows how to resolve an AWS Support case by its ID.

        :param case_id: The ID of the case to resolve.
        """
        print("-" * 88)
        print(f"Resolving case with ID {case_id}.")
        case_status = self.support_wrapper.resolve_case(case_id)
        print(f"\tFinal case status is {case_status}.")
        print("-" * 88)

    def list_resolved_cases(self):
        """
        List the resolved cases for the current day.
        """
        print("-" * 88)
```

```
        print("Let's list the resolved cases for the current day.")
        start_time = str(datetime.utcnow().date())
        end_time = str(datetime.utcnow().date() + timedelta(days=1))
        resolved_cases = self.support_wrapper.describe_cases(start_time,
 end_time, True)
        for case in resolved_cases:
            print(f"\tCase: {case['caseId']}: status {case['status']}.")
        print("-" * 88)

    def run_scenario(self):
        logging.basicConfig(level=logging.INFO, format="%(levelname)s:
 %(message)s")

        print("-" * 88)
        print("Welcome to the AWS Support get started with support cases demo.")
        print("-" * 88)

        selected_service = self.display_and_select_service()
        selected_category = self.display_and_select_category(selected_service)
        selected_severity = self.display_and_select_severity()
        new_case_id = self.create_example_case(
            selected_service, selected_category, selected_severity
        )
        wait(10)
        self.list_open_cases()
        new_attachment_set_id = self.create_attachment_set()
        self.add_communication(new_case_id, new_attachment_set_id)
        new_attachment_id = self.list_communications(new_case_id)
        self.describe_case_attachment(new_attachment_id)
        self.resolve_case(new_case_id)
        wait(10)
        self.list_resolved_cases()

        print("\nThanks for watching!")
        print("-" * 88)


if __name__ == "__main__":
    try:
        scenario = SupportCasesScenario(SupportWrapper.from_client())
        scenario.run_scenario()
    except Exception:
        logging.exception("Something went wrong with the demo.")
```

Définissez une classe qui englobe les actions du client.

```
class SupportWrapper:
    """Encapsulates Support actions."""

    def __init__(self, support_client):
        """
        :param support_client: A Boto3 Support client.
        """
        self.support_client = support_client

    @classmethod
    def from_client(cls):
        """
        Instantiates this class from a Boto3 client.
        """
        support_client = boto3.client("support")
        return cls(support_client)


    def describe_services(self, language):
        """
        Get the descriptions of AWS services available for support for a
 language.

        :param language: The language for support services.
        Currently, only "en" (English) and "ja" (Japanese) are supported.
        :return: The list of AWS service descriptions.
        """
        try:
            response = self.support_client.describe_services(language=language)
            services = response["services"]
        except ClientError as err:
            if err.response["Error"]["Code"] == "SubscriptionRequiredException":
                logger.info(
                    "You must have a Business, Enterprise On-Ramp, or Enterprise
 Support "
                    "plan to use the AWS Support API. \n\tPlease upgrade your
 subscription to run these "
                    "examples."
                )
```

```
            else:
                logger.error(
                    "Couldn't get Support services for language %s. Here's why:
%s: %s",
                    language,
                    err.response["Error"]["Code"],
                    err.response["Error"]["Message"],
                )
                raise
        else:
            return services


    def describe_severity_levels(self, language):
        """
        Get the descriptions of available severity levels for support cases for a
language.

        :param language: The language for support severity levels.
        Currently, only "en" (English) and "ja" (Japanese) are supported.
        :return: The list of severity levels.
        """
        try:
            response =
self.support_client.describe_severity_levels(language=language)
            severity_levels = response["severityLevels"]
        except ClientError as err:
            if err.response["Error"]["Code"] == "SubscriptionRequiredException":
                logger.info(
                    "You must have a Business, Enterprise On-Ramp, or Enterprise
Support "
                    "plan to use the AWS Support API. \n\tPlease upgrade your
subscription to run these "
                    "examples."
                )
            else:
                logger.error(
                    "Couldn't get severity levels for language %s. Here's why:
%s: %s",
                    language,
                    err.response["Error"]["Code"],
                    err.response["Error"]["Message"],
                )
                raise
```

```
        else:
            return severity_levels


    def create_case(self, service, category, severity):
        """
        Create a new support case.

        :param service: The service to use for the new case.
        :param category: The category to use for the new case.
        :param severity: The severity to use for the new case.
        :return: The caseId of the new case.
        """
        try:
            response = self.support_client.create_case(
                subject="Example case for testing, ignore.",
                serviceCode=service["code"],
                severityCode=severity["code"],
                categoryCode=category["code"],
                communicationBody="Example support case body.",
                language="en",
                issueType="customer-service",
            )
            case_id = response["caseId"]
        except ClientError as err:
            if err.response["Error"]["Code"] == "SubscriptionRequiredException":
                logger.info(
                    "You must have a Business, Enterprise On-Ramp, or Enterprise
Support "
                    "plan to use the AWS Support API. \n\tPlease upgrade your
subscription to run these "
                    "examples."
                )
            else:
                logger.error(
                    "Couldn't create case. Here's why: %s: %s",
                    err.response["Error"]["Code"],
                    err.response["Error"]["Message"],
                )
                raise
        else:
            return case_id
```

```
    def add_attachment_to_set(self):
        """
        Add an attachment to a set, or create a new attachment set if one does
not exist.

        :return: The attachment set ID.
        """
        try:
            response = self.support_client.add_attachments_to_set(
                attachments=[
                    {
                        "fileName": "attachment_file.txt",
                        "data": b"This is a sample file for attachment to a
support case.",
                    }
                ]
            )
            new_set_id = response["attachmentSetId"]
        except ClientError as err:
            if err.response["Error"]["Code"] == "SubscriptionRequiredException":
                logger.info(
                    "You must have a Business, Enterprise On-Ramp, or Enterprise
Support "
                    "plan to use the AWS Support API. \n\tPlease upgrade your
subscription to run these "
                    "examples."
                )
            else:
                logger.error(
                    "Couldn't add attachment. Here's why: %s: %s",
                    err.response["Error"]["Code"],
                    err.response["Error"]["Message"],
                )
                raise
        else:
            return new_set_id


    def add_communication_to_case(self, attachment_set_id, case_id):
        """
        Add a communication and an attachment set to a case.

        :param attachment_set_id: The ID of an existing attachment set.
        :param case_id: The ID of the case.
```

```
        """
        try:
            self.support_client.add_communication_to_case(
                caseId=case_id,
                communicationBody="This is an example communication added to a
support case.",
                attachmentSetId=attachment_set_id,
            )
        except ClientError as err:
            if err.response["Error"]["Code"] == "SubscriptionRequiredException":
                logger.info(
                    "You must have a Business, Enterprise On-Ramp, or Enterprise
Support "
                    "plan to use the AWS Support API. \n\tPlease upgrade your
subscription to run these "
                    "examples."
                )
            else:
                logger.error(
                    "Couldn't add communication. Here's why: %s: %s",
                    err.response["Error"]["Code"],
                    err.response["Error"]["Message"],
                )
                raise


    def describe_all_case_communications(self, case_id):
        """
        Describe all the communications for a case using a paginator.

        :param case_id: The ID of the case.
        :return: The communications for the case.
        """
        try:
            communications = []
            paginator =
self.support_client.get_paginator("describe_communications")
            for page in paginator.paginate(caseId=case_id):
                communications += page["communications"]
        except ClientError as err:
            if err.response["Error"]["Code"] == "SubscriptionRequiredException":
                logger.info(
                    "You must have a Business, Enterprise On-Ramp, or Enterprise
Support "
```

```
                    "plan to use the AWS Support API. \n\tPlease upgrade your
subscription to run these "
                    "examples."
                )
            else:
                logger.error(
                    "Couldn't describe communications. Here's why: %s: %s",
                    err.response["Error"]["Code"],
                    err.response["Error"]["Message"],
                )
                raise
        else:
            return communications


    def describe_attachment(self, attachment_id):
        """
        Get information about an attachment by its attachmentID.

        :param attachment_id: The ID of the attachment.
        :return: The name of the attached file.
        """
        try:
            response = self.support_client.describe_attachment(
                attachmentId=attachment_id
            )
            attached_file = response["attachment"]["fileName"]
        except ClientError as err:
            if err.response["Error"]["Code"] == "SubscriptionRequiredException":
                logger.info(
                    "You must have a Business, Enterprise On-Ramp, or Enterprise
Support "
                    "plan to use the AWS Support API. \n\tPlease upgrade your
subscription to run these "
                    "examples."
                )
            else:
                logger.error(
                    "Couldn't get attachment description. Here's why: %s: %s",
                    err.response["Error"]["Code"],
                    err.response["Error"]["Message"],
                )
                raise
        else:
```

```
            return attached_file


    def resolve_case(self, case_id):
        """
        Resolve a support case by its caseId.

        :param case_id: The ID of the case to resolve.
        :return: The final status of the case.
        """
        try:
            response = self.support_client.resolve_case(caseId=case_id)
            final_status = response["finalCaseStatus"]
        except ClientError as err:
            if err.response["Error"]["Code"] == "SubscriptionRequiredException":
                logger.info(
                    "You must have a Business, Enterprise On-Ramp, or Enterprise
Support "
                    "plan to use the AWS Support API. \n\tPlease upgrade your
subscription to run these "
                    "examples."
                )
            else:
                logger.error(
                    "Couldn't resolve case. Here's why: %s: %s",
                    err.response["Error"]["Code"],
                    err.response["Error"]["Message"],
                )
                raise
        else:
            return final_status


    def describe_cases(self, after_time, before_time, resolved):
        """
        Describe support cases over a period of time, optionally filtering
        by status.

        :param after_time: The start time to include for cases.
        :param before_time: The end time to include for cases.
        :param resolved: True to include resolved cases in the results,
            otherwise results are open cases.
        :return: The final status of the case.
        """
```

```
        try:
            cases = []
            paginator = self.support_client.get_paginator("describe_cases")
            for page in paginator.paginate(
                afterTime=after_time,
                beforeTime=before_time,
                includeResolvedCases=resolved,
                language="en",
            ):
                cases += page["cases"]
        except ClientError as err:
            if err.response["Error"]["Code"] == "SubscriptionRequiredException":
                logger.info(
                    "You must have a Business, Enterprise On-Ramp, or Enterprise
Support "
                    "plan to use the AWS Support API. \n\tPlease upgrade your
subscription to run these "
                    "examples."
                )
            else:
                logger.error(
                    "Couldn't describe cases. Here's why: %s: %s",
                    err.response["Error"]["Code"],
                    err.response["Error"]["Message"],
                )
                raise
        else:
            if resolved:
                cases = filter(lambda case: case["status"] == "resolved", cases)
            return cases
```

- Pour plus d'informations sur l'API, consultez les rubriques suivantes dans AWS SDK for Python (Boto3) API Reference.
  - AddAttachmentsToSet
  - AddCommunicationToCase
  - CreateCase
  - DescribeAttachment

- DescribeCases
- DescribeCommunications
- DescribeServices
- DescribeSeverityLevels
- ResolveCase

Pour obtenir la liste complète des guides de développement du AWS SDK et des exemples de code, consultezUtilisation de AWS Support avec un kit SDK AWS.. Cette rubrique comprend également des informations sur le démarrage et sur les versions précédentes de SDK.

Surveillance et journalisation pour AWS Support

La surveillance constitue une part importante de la gestion de la fiabilité, de la disponibilité et des performances d'AWS Support et de vos autres solutions AWS. AWS fournit les outils de surveillance suivants pour surveiller AWS Support, signaler les problèmes et prendre des mesures automatiques, le cas échéant :

- Amazon EventBridge fournit un flux d'événements système en temps quasi réel qui décrivent les modifications apportées aux ressources AWS. EventBridge permet d'effectuer des calculs automatisés pilotés par des événements, car vous pouvez écrire des règles pour surveiller certains événements et déclencher des actions automatisées dans d'autres services AWS lorsque ces événements se produisent. Pour plus d'informations, consultez le Guide de l'utilisateur Amazon EventBridge.
- AWS CloudTrail capture les appels d'API et les événements associés créés par votre compte AWS ou au nom de celui-ci et livre les fichiers journaux dans un compartiment Amazon S3 que vous spécifiez. Vous pouvez identifier les utilisateurs et les comptes qui ont appelé AWS, l'adresse IP source à partir de laquelle les appels ont été émis, ainsi que le moment où les appels ont eu lieu. Pour de plus amples informations, veuillez consulter le Guide de l'utilisateur AWS CloudTrail.

Rubriques

Suivi AWS Support des cas avec Amazon EventBridge

Vous pouvez utiliser Amazon EventBridge pour détecter les modifications apportées à vos AWS Support dossiers 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 l'événement, vous pouvez envoyer des notifications, capturer des informations sur l'événement, prendre des mesures correctives, déclencher des événements ou prendre d'autres

mesures. Par exemple, vous pouvez être notifié lorsque les actions suivantes se produisent dans votre compte :

- Créer une demande de support
- Ajouter une correspondance à un cas de support existant
- Résoudre une demande de support
- Réouvrir un cas de support

> **Note**
>
> AWS Support fournit des événements dans la mesure du possible. Les événements ne sont pas toujours garantis d'être fournis à EventBridge.

Création d'une règle EventBridge pour les cas AWS Support

Vous pouvez créer une EventBridge règle pour être informé des événements liés au AWS Support dossier. La règle surveillera les mises à jour des cas de support dans votre compte, y compris les actions que vous, vos utilisateurs IAM ou les agents de support effectuent. Avant de créer une règle pour les événements de cas AWS Support, 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.
- Créez la cible à utiliser dans votre règle d'événement. Par exemple, vous pouvez créer une rubrique Amazon Simple Notification Service (Amazon SNS) de sorte que chaque fois qu'un cas de support est mis à jour, vous recevrez un message texte ou un e-mail. Pour plus d'informations, consultez les cibles EventBridge.

> **Note**
>
> AWS Support est un service global. Pour recevoir des mises à jour concernant vos demandes de support, vous pouvez utiliser une des régions suivantes : USA Est (Virginie du Nord), USA Ouest (Oregon) ou Europe (Irlande).

Pour créer une EventBridge règle pour les événements liés à une AWS Support affaire

1. Ouvrez la EventBridge console Amazon à l'adresse https://console.aws.amazon.com/events/.
2. Si ce n'est pas déjà fait, utilisez Region selector (Sélecteur de région) dans l'angle supérieur droit de la page et choisissez USA Est (Virginie du Nord).
3. Dans le volet de navigation, choisissez Rules.
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 AWSévénements ou événements EventBridge partenaires.
8. Sous Event pattern (Modèle d'événement), conservez la valeur par défaut pour Services AWS.
9. Pour Service AWS, choisissez Support.
10. Pour Event type (Type d'événement), choisissez Support Case Update (Mise à jour du cas de support).
11. Choisissez Suivant.
12. Dans la section Select target(s) (Sélectionner la ou les cibles), choisissez la cible que vous avez créée pour cette règle, puis configurez toutes les options supplémentaires requises pour ce type. Par exemple, si vous choisissez Amazon SNS, assurez-vous que votre rubrique SNS est configurée correctement pour que vous soyez notifié par e-mail ou SMS.
13. Choisissez Suivant.
14. (Facultatif) Sur la page Configure tags (Configurer des étiquettes), ajoutez des étiquettes, puis choisissez Next (Suivant).
15. Sur la page Review and create (Vérifier et créer), examinez la configuration de votre règle et assurez-vous qu'elle répond à vos exigences en matière de surveillance d'événements.
16. Choisissez Créer une règle. Votre règle va maintenant surveiller les événements de cas AWS Support et les envoyer à la cible que vous avez spécifiée.

Remarques

- Lorsque vous recevez un événement, vous pouvez utiliser le paramètre `origin` pour déterminer si vous ou un agent AWS Support avez ajouté une correspondance à un cas de support. La valeur pour `origin` peut être `CUSTOMER` ou `AWS`.

  Actuellement, seuls les événements pour l'action `AddCommunicationToCase` auront cette valeur.
- Pour plus d'informations sur la création de modèles d'événements, consultez la section Modèles d'événements dans le guide de EventBridge l'utilisateur Amazon.
- Vous pouvez également créer une autre règle pour l'appel d'API AWS via le type d'événement CloudTrail. Cette règle surveillera les journaux AWS CloudTrail pour les appels d'API AWS Support dans votre compte.

Exemples d'événements AWS Support

Les événements suivants sont créés lorsque des actions de support se produisent dans votre compte.

Example : Créer un cas de support

L'événement suivant est créé lorsqu'un cas de support est créé.

```
{
    "version": "0",
    "id": "3433df007-9285-55a3-f6d1-536944be45d7",
    "detail-type": "Support Case Update",
    "source": "aws.support",
    "account": "111122223333",
    "time": "2022-02-21T15:51:19Z",
    "region": "us-east-1",
    "resources": [],
    "detail": {
        "case-id": "case-111122223333-muen-2022-7118885805350839",
        "display-id": "1234563851",
        "communication-id": "",
        "event-name": "CreateCase",
        "origin": ""
    }
```

```
}
```

Example : Mettre à jour un cas de support

L'événement suivant est créé lorsque AWS Support répond à un cas de support.

```
{
    "version": "0",
    "id": "f90cb8cb-32be-1c91-c0ba-d50b4ca5e51b",
    "detail-type": "Support Case Update",
    "source": "aws.support",
    "account": "111122223333",
    "time": "2022-02-21T15:51:31Z",
    "region": "us-east-1",
    "resources": [],
    "detail": {
        "case-id": "case-111122223333-muen-2022-7118885805350839",
        "display-id": "1234563851",
        "communication-id": "ekko:us-east-1:12345678-268a-424b-be08-54613cab84d2",
        "event-name": "AddCommunicationToCase",
        "origin": "AWS"
    }
}
```

Example : Résoudre un cas de support

L'événement suivant est créé lorsqu'un cas de support est résolu.

```
{
    "version": "0",
    "id": "1aa4458d-556f-732e-ddc1-4a5b2fbd14a5",
    "detail-type": "Support Case Update",
    "source": "aws.support",
    "account": "111122223333",
    "time": "2022-02-21T15:51:31Z",
    "region": "us-east-1",
    "resources": [],
    "detail": {
        "case-id": "case-111122223333-muen-2022-7118885805350839",
        "display-id": "1234563851",
        "communication-id": "",
        "event-name": "ResolveCase",
        "origin": ""
```

```
    }
}
```

Example : Réouvrir un cas de support

L'événement suivant est créé lorsqu'un cas de support est réouvert.

```
{
    "version": "0",
    "id": "3bb9d8fe-6089-ad27-9508-804209b233ad",
    "detail-type": "Support Case Update",
    "source": "aws.support",
    "account": "111122223333",
    "time": "2022-02-21T15:47:19Z",
    "region": "us-east-1",
    "resources": [],
    "detail": {
        "case-id": "case-111122223333-muen-2021-27f40618fe0303ea",
        "display-id": "1234563851",
        "communication-id": "",
        "event-name": "ReopenCase",
        "origin": ""
    }
}
```

Consulter aussi

Pour plus d'informations sur l'utilisation EventBridge avecAWS Support, consultez les ressources suivantes :

- Comment automatiser AWS Support l'API avec Amazon EventBridge
- AWS Supportnotificateur d'activité des cas sur GitHub

Journalisation des appels d'API AWS Support avec AWS CloudTrail

AWS Support est intégré à AWS CloudTrail, un service qui fournit une archive des actions effectuées par un utilisateur, un rôle ou un service AWS dans AWS Support. CloudTrail capture les appels d'API pour AWS Support en tant qu'événements. Les appels capturés incluent des appels de la console AWS Support et les appels de code vers les opérations d'API AWS Support.

Si vous créez un journal d'activité, vous pouvez activer la livraison continue des événements CloudTrail dans un compartiment Amazon Simple Storage Service (Amazon S3, y compris les événements pour AWS Support. Si vous ne configurez pas de journal d'activité, vous pouvez toujours afficher les événements les plus récents dans la console CloudTrail dans Historique des événements.

Avec les informations collectées par CloudTrail, vous pouvez déterminer la demande qui a été envoyée à AWS Support, l'adresse IP à partir de laquelle la demande a été effectuée, l'auteur et la date de la demande, ainsi que d'autres détails.

Pour en savoir plus sur CloudTrail, y compris la façon de le configurer et de l'activer, consultez le AWS CloudTrail Guide de l'utilisateur.

AWS Support Informations dans CloudTrail

CloudTrail est activé dans votre compte AWS lors de la création de ce dernier. Quand une activité d'événement prise en charge a lieu dans AWS Support, elle est enregistrée dans un événement CloudTrail avec d'autres événements de service AWS dans Event history (Historique des événements). Vous pouvez afficher, rechercher et télécharger les événements récents dans votre compte AWS. Pour de plus amples informations, veuillez consulter Affichage des événements avec l'historique des événements CloudTrail.

Pour un enregistrement continu des événements dans votre compte AWS, y compris les événements pour AWS Support, créez un journal de suivi. Un journal d'activité permet à CloudTrail de distribuer les fichiers journaux vers Amazon S3 bucket. Par défaut, lorsque vous créez un journal de suivi dans la console, il s'applique à toutes les régions AWS. Le journal de suivi consigne les événements de toutes les Régions dans la partition AWS et livre les fichiers journaux dans le compartiment Amazon S3 de votre choix. En outre, vous pouvez configurer d'autres services AWS pour analyser et agir sur les données d'événements collectées dans les journaux CloudTrail. Pour en savoir plus, consultez les ressources suivantes :

- Présentation de la création d'un journal d'activité
- Intégrations et services pris en charge par CloudTrail
- Configuration des notifications Amazon SNS pour CloudTrail
- Réception de fichiers journaux CloudTrail de plusieurs régions et Réception de fichiers journaux CloudTrail de plusieurs comptes

Toutes les opérations de l'API AWS Support sont consignées par CloudTrail et documentées dans la Référence des API AWS Support.

Par exemple, les appels aux opérations `CreateCase`, `DescribeCases` et `ResolveCase` génèrent des entrées dans les fichiers journaux CloudTrail.

Chaque événement ou entrée de journal contient des informations sur la personne ayant initié la demande. Les informations relatives à l'identité permettent de déterminer les éléments suivants :

- Si la demande a été effectuée avec les informations d'identification utilisateur racine ou AWS Identity and Access Management (IAM).
- Si la demande a été effectuée avec les informations d'identification de sécurité temporaires d'un rôle ou d'un utilisateur fédéré.
- Si la requête a été effectuée par un autre service AWS.

Pour plus d'informations, veuillez consulter l'élément userIdentity CloudTrail.

Vous pouvez également regrouper des fichiers journaux AWS Support provenant de plusieurs régions AWS et de plusieurs comptes AWS dans un seul compartiment Amazon S3.

Informations AWS Trusted Advisor dans la consignation CloudTrail

Trusted Advisor est un service AWS Support qui vous permet de vérifier votre compte AWS pour savoir comment réduire vos coûts, améliorer la sécurité et optimiser votre compte .

Toutes les opérations de l'API Trusted Advisor sont consignées par CloudTrail et documentées dans la Référence des API AWS Support.

Par exemple, les appels aux opérations `DescribeTrustedAdvisorCheckRefreshStatuses`, `DescribeTrustedAdvisorCheckResult` et `RefreshTrustedAdvisorCheck` génèrent des entrées dans les fichiers journaux CloudTrail.

> **Note**
>
> CloudTrail consigne aussi les actions de la console Trusted Advisor. Consultez Journalisation des actions de console AWS Trusted Advisor avec AWS CloudTrail.

Présentation des AWS Support entrées des fichiers journaux

Un journal d'activité est une configuration qui permet d'envoyer les événements dans des fichiers journaux à un compartiment Amazon S3 que vous spécifiez. Les fichiers journaux CloudTrail peuvent

contenir une ou plusieurs entrées de journal. Un événement représente une demande unique d'une source quelconque. Il comprend des informations sur l'opération demandée, la date et l'heure de l'opération, les paramètres de la requête, etc. Les fichiers journaux CloudTrail ne constituent pas une série ordonnée retraçant les appels d'API publics. Ils ne suivent aucun ordre précis.

Example : Entrée de journal pour CreateCase

L'exemple suivant montre une entrée de journal CloudTrail pour une opération CreateCluster.


```
{
   "Records": [
      {
         "eventVersion": "1.04",
         "userIdentity": {
            "type": "IAMUser",
            "principalId": "AIDACKCEVSQ6C2EXAMPLE",
            "arn": "arn:aws:iam::111122223333:user/janedoe",
            "accountId": "111122223333",
            "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
            "userName": "janedoe",
            "sessionContext": {
               "attributes": {
                  "mfaAuthenticated": "false",
                  "creationDate": "2016-04-13T17:51:37Z"
               }
            },
            "invokedBy": "signin.amazonaws.com"
         },
         "eventTime": "2016-04-13T18:05:53Z",
         "eventSource": "support.amazonaws.com",
         "eventName": "CreateCase",
         "awsRegion": "us-east-1",
         "sourceIPAddress": "198.51.100.15",
         "userAgent": "signin.amazonaws.com",
         "requestParameters": {
            "severityCode": "low",
            "categoryCode": "other",
            "language": "en",
            "serviceCode": "support-api",
            "issueType": "technical"
         },
         "responseElements": {
            "caseId": "case-111122223333-muen-2016-c3f2077e504940f2"
```

```
        },
        "requestID": "58c257ef-01a2-11e6-be2a-01c031063738",
        "eventID": "5aa34bfc-ad5b-4fb1-8a55-2277c86e746a",
        "eventType": "AwsApiCall",
        "recipientAccountId": "111122223333"
      }
   ],
   ...
}
```

Example : Entrée de journal pour RefreshTrustedAdvisorCheck

L'exemple suivant montre une entrée de journal CloudTrail pour une opération RefreshTrustedAdvisorCheck.

```
{
    "eventVersion": "1.05",
    "userIdentity": {
        "type": "IAMUser",
        "principalId": "AIDACKCEVSQ6C2EXAMPLE",
        "arn": "arn:aws:iam::111122223333:user/Admin",
        "accountId": "111122223333",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "userName": "Admin"
    },
    "eventTime": "2020-10-21T16:34:13Z",
    "eventSource": "support.amazonaws.com",
    "eventName": "RefreshTrustedAdvisorCheck",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "72.21.198.67",
    "userAgent": "signin.amazonaws.com",
    "requestParameters": {
        "checkId": "Pfx0RwqBli"
    },
    "responseElements": null,
    "requestID": "4c4d5fc8-c403-4f82-9544-41f820e0fa01",
    "eventID": "2f4630ac-5c27-4f0d-b93f-63742d6fc85e",
    "eventType": "AwsApiCall",
    "recipientAccountId": "111122223333"
}
```

Journalisation des appels d'API de l'application AWS Support dans Slack à l'aide de AWS CloudTrail

L'application AWS Support dans Slack est intégrée à AWS CloudTrail. CloudTrail fournit un enregistrement des actions réalisées par un utilisateur, un rôle ou un Service AWS dans l'application AWS Support. Pour créer cet enregistrement, CloudTrail capture tous les appels d'API publics pour l'application AWS Support en tant qu'événements. Ces appels capturés incluent les appels de la console de l'application AWS Support et les appels de code vers les opérations de l'API publique de l'application AWS Support. Si vous créez un journal d'activité, vous pouvez activer la livraison continue d'événements CloudTrail à un compartiment Amazon S3, y compris des événements pour Amazon S3. Ceux-ci incluent les événements pour l'application AWS Support. Si vous ne configurez pas de journal d'activité, vous pouvez toujours afficher les événements les plus récents dans la console CloudTrail dans Event history (Historique des événements). Vous pouvez utiliser les informations que CloudTrail collecte pour déterminer si la demande qui a été faite à l'application AWS Support. Vous pouvez également découvrir l'adresse IP d'où provient l'appel, qui a fait la demande, quand elle a été faite et d'autres détails.

Pour en savoir plus sur CloudTrail, consultez le AWS CloudTrailGuide de l'utilisateur .

Informations sur l'application AWS Support dans CloudTrail

Lorsque vous créez votre Compte AWS, cela active CloudTrail dans le compte. Lorsque l'activité de l'API publique se produit dans l'application AWS Support, cette activité est enregistrée dans un événement CloudTrail, avec d'autres événements de service AWS dans Event history (Historique des événements). Vous pouvez afficher, rechercher et télécharger les événements récents dans votre Compte AWS. Pour plus d'informations, consultez Affichage des événements avec l'historique des événements CloudTrail.

Pour obtenir un enregistrement continu des événements de votre Compte AWS, y compris les événements pour l'application AWS Support, créez un journal d'activité. Par défaut, lorsque vous créez un journal d'activité dans la console, il s'applique à toutes les régions Régions AWS. Le journal d'activité consigne les événements de toutes les Régions dans la partition AWS et livre les fichiers journaux dans le compartiment Simple Storage Service (Amazon S3) de votre choix. De plus, vous pouvez configurer d'autres Services AWS pour analyser plus en profondeur les données d'événement collectées dans les journaux CloudTrail et agir sur celles-ci. Pour en savoir plus, consultez les ressources suivantes :

- Présentation de la création d'un journal d'activité

- Intégrations et services pris en charge par CloudTrail
- Configuration des notifications Amazon SNS pour CloudTrail
- Réception de fichiers journaux CloudTrail de plusieurs régions et Réception de fichiers journaux CloudTrail de plusieurs comptes

CloudTrail journalise toutes les actions publiques de l'application AWS Support. Ces actions sont également documentées dans la Référence d'API de l'application AWS Support dans Slack. À titre d'exemple, les appels vers les actions `CreateSlackChannelConfiguration`, `GetAccountAlias` et `UpdateSlackChannelConfiguration` génèrent des entrées dans les fichiers journaux CloudTrail.

Chaque événement ou entrée de journal contient des informations sur la personne ayant initié la demande. Les informations relatives à l'identité permettent de déterminer les éléments suivants :

- Si la demande a été effectuée avec les informations d'identification utilisateur racine ou AWS Identity and Access Management (IAM).
- Si la demande a été effectuée avec les informations d'identification de sécurité temporaires d'un rôle ou d'un utilisateur fédéré.
- Si la requête a été effectuée par un autre Service AWS.

Pour plus d'informations, consultez l'élément userIdentity CloudTrail.

Comprendre les entrées du fichier journal de l'application AWS Support

Un journal d'activité est une configuration qui permet d'envoyer des événements sous forme de fichiers journaux à un compartiment Simple Storage Service (Amazon S3) que vous spécifiez. Les fichiers journaux CloudTrail peuvent contenir une ou plusieurs entrées. Un événement représente une demande unique provenant de n'importe quelle source et comprend des informations sur l'action demandée, la date et l'heure de l'action, les paramètres de la requête, etc. Les fichiers journaux CloudTrail ne constituent pas une série ordonnée retraçant les appels d'API publiques. Cela signifie que les journaux n'apparaissent pas dans un ordre spécifique.

Example : Exemple de journal pour **`CreateSlackChannelConfiguration`**

L'exemple suivant montre une entrée de journal CloudTrail pour l'opération CreateSlackChannelConfiguration.

```
{
```

```
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "AssumedRole",
        "principalId": "AIDACKCEVSQ6C2EXAMPLE:JaneDoe",
        "arn": "arn:aws:sts::111122223333:assumed-role/Administrator/JaneDoe",
        "accountId": "111122223333",
        "accessKeyId": "AKIAI44QH8DHBEXAMPLE",
        "sessionContext": {
            "sessionIssuer": {
                "type": "Role",
                "principalId": "AIDACKCEVSQ6C2EXAMPLE",
                "arn": "arn:aws:iam::111122223333:role/Administrator",
                "accountId": "111122223333",
                "userName": "Administrator"
            },
            "webIdFederationData": {},
            "attributes": {
                "creationDate": "2022-02-26T01:37:57Z",
                "mfaAuthenticated": "false"
            }
        }
    },
    "eventTime": "2022-02-26T01:48:20Z",
    "eventSource": "supportapp.amazonaws.com",
    "eventName": "CreateSlackChannelConfiguration",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "205.251.233.183",
    "userAgent": "aws-cli/1.3.23 Python/2.7.6 Linux/2.6.18-164.el5",
    "requestParameters": {
        "notifyOnCreateOrReopenCase": true,
        "teamId": "T012ABCDEFG",
        "notifyOnAddCorrespondenceToCase": true,
        "notifyOnCaseSeverity": "all",
        "channelName": "troubleshooting-channel",
        "notifyOnResolveCase": true,
        "channelId": "C01234A5BCD",
        "channelRoleArn": "arn:aws:iam::111122223333:role/AWSSupportAppRole"
    },
    "responseElements": null,
    "requestID": "d06df6ca-c233-4ffb-bbff-63470c5dc255",
    "eventID": "0898ce29-a396-444a-899d-b068f390c361",
    "readOnly": false,
    "eventType": "AwsApiCall",
    "managementEvent": true,
```

```
    "recipientAccountId": "111122223333",
    "eventCategory": "Management"
}
```

Example : Exemple de journal pour **`ListSlackChannelConfigurations`**

L'exemple suivant montre une entrée de journal CloudTrail pour l'opération ListSlackChannelConfigurations.

```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "AssumedRole",
        "principalId": "AIDACKCEVSQ6C2EXAMPLE:AWSSupportAppRole",
        "arn": "arn:aws:sts::111122223333:assumed-role/AWSSupportAppRole",
        "accountId": "111122223333",
        "accessKeyId": "AKIAI44QH8DHBEXAMPLE",
        "sessionContext": {
            "sessionIssuer": {
                "type": "Role",
                "principalId": "AIDACKCEVSQ6C2EXAMPLE",
                "arn": "arn:aws:iam::111122223333:role/AWSSupportAppRole",
                "accountId": "111122223333",
                "userName": "AWSSupportAppRole"
            },
            "webIdFederationData": {},
            "attributes": {
                "creationDate": "2022-03-01T20:06:32Z",
                "mfaAuthenticated": "false"
            }
        }
    },
    "eventTime": "2022-03-01T20:06:46Z",
    "eventSource": "supportapp.amazonaws.com",
    "eventName": "ListSlackChannelConfigurations",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "72.21.217.131",
    "userAgent": "aws-cli/1.3.23 Python/2.7.6 Linux/2.6.18-164.el5",
    "requestParameters": null,
    "responseElements": null,
    "requestID": "20f81d63-31c5-4351-bd02-9eda7f76e7b8",
    "eventID": "70acb7fe-3f84-47cd-8c28-cc148ad06d21",
    "readOnly": true,
```

```
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "111122223333",
    "eventCategory": "Management"
}
```

Example : Exemple de journal pour **`GetAccountAlias`**

L'exemple suivant montre une entrée de journal CloudTrail pour l'opération GetAccountAlias.

```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "AssumedRole",
        "principalId": "AIDACKCEVSQ6C2EXAMPLE:devdsk",
        "arn": "arn:aws:sts::111122223333:assumed-role/AWSSupportAppRole/devdsk",
        "accountId": "111122223333",
        "accessKeyId": "AKIAI44QH8DHBEXAMPLE",
        "sessionContext": {
            "sessionIssuer": {
                "type": "Role",
                "principalId": "AIDACKCEVSQ6C2EXAMPLE",
                "arn": "arn:aws:iam::111122223333:role/AWSSupportAppRole",
                "accountId": "111122223333",
                "userName": "AWSSupportAppRole"
            },
            "webIdFederationData": {},
            "attributes": {
                "creationDate": "2022-03-01T20:31:27Z",
                "mfaAuthenticated": "false"
            }
        }
    },
    "eventTime": "2022-03-01T20:31:47Z",
    "eventSource": "supportapp.amazonaws.com",
    "eventName": "GetAccountAlias",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "72.21.217.142",
    "userAgent": "aws-cli/1.3.23 Python/2.7.6 Linux/2.6.18-164.el5",
    "requestParameters": null,
    "responseElements": null,
    "requestID": "a225966c-0906-408b-b8dd-f246665e6758",
    "eventID": "79ebba8d-3285-4023-831a-64af7de8d4ad",
    "readOnly": true,
```

```
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "111122223333",
    "eventCategory": "Management"
}
```

Surveillance et journalisation pour AWS Support Plans

La surveillance constitue une part importante de la gestion de la fiabilité, de la disponibilité et des performances de Support Plans et de vos autres solutions AWS. AWS fournit les outils de surveillance suivants pour surveiller Support Plans, signaler les problèmes et prendre des mesures automatiques, le cas échéant :

- AWS CloudTrail capture les appels d'API et les événements associés créés par ou au nom de votre compte AWS et envoie les fichiers journaux à un compartiment Amazon S3 que vous spécifiez. Vous pouvez identifier les utilisateurs et les comptes qui ont appelé AWS, l'adresse IP source à partir de laquelle les appels ont été émis, ainsi que le moment où les appels ont eu lieu. Pour de plus amples informations, veuillez consulter le Guide de l'utilisateur AWS CloudTrail.

Rubriques

Journalisation des appels d'API d'AWS Support Plans avec AWS CloudTrail

AWS Support Plans est intégré avec AWS CloudTrail, un service qui fournit un registre des actions prises par un utilisateur, un rôle ou un Service AWS. CloudTrail capture les appels d'API pour AWS Support Plans en tant qu'événements. Les appels capturés incluent des appels de la console AWS Support Plans et les appels de code vers les opérations d'API AWS Support Plans.

Si vous créez un journal d'activité, vous pouvez activer la distribution continue des événements CloudTrail dans un compartiment Amazon Simple Storage Service (Amazon S3, y compris les événements pour AWS Support Plans. Si vous ne configurez pas de journal d'activité, vous pouvez toujours afficher les événements les plus récents dans la console CloudTrail dans Event history (Historique des événements).

En utilisant les informations collectées par CloudTrail, vous pouvez déterminer la demande qui a été envoyée à AWS Support Plans, l'adresse IP, l'auteur et la date de la demande, ainsi que d'autres détails.

Pour en savoir plus sur CloudTrail, y compris la façon de le configurer et de l'activer, consultez le AWS CloudTrail Guide de l'utilisateur.

Informations sur AWS Support Plans dans CloudTrail

CloudTrail est activé dans votre Compte AWS lors de la création de ce dernier. Quand une activité d'événement prise en charge a lieu dans AWS Support Plans, elle est enregistrée dans un événement CloudTrail avec d'autres événements de Service AWS dans Event history (Historique des événements). Vous pouvez afficher, rechercher et télécharger les événements récents dans votre compte . Pour plus d'informations, consultez Affichage des événements avec l'historique des événements CloudTrail.

Pour un enregistrement continu des événements de votre compte, y compris les événements relatifs à AWS Support Plans, créez un journal d'activité. Un journal d'activité permet à CloudTrail de distribuer les fichiers journaux vers Simple Storage Service (Amazon S3) bucket. Par défaut, lorsque vous créez un journal d'activité dans la console, il s'applique à toutes les régions Régions AWS. Le journal d'activité consigne les événements de toutes les Régions dans la partition AWS et livre les fichiers journaux dans le compartiment Simple Storage Service (Amazon S3) de votre choix. De plus, vous pouvez configurer d'autres Services AWS pour analyser plus en profondeur les données d'événement collectées dans les journaux CloudTrail et agir sur celles-ci. Pour en savoir plus, consultez les ressources suivantes :

- Présentation de la création d'un journal d'activité
- Intégrations et services pris en charge par CloudTrail
- Configuration des notifications Amazon SNS pour CloudTrail
- Réception de fichiers journaux CloudTrail de plusieurs régions et Réception de fichiers journaux CloudTrail de plusieurs comptes

Toutes les opérations d'API d'AWS Support Plans sont journalisées par CloudTrail. Chaque événement ou entrée de journal contient des informations sur la personne ayant initié la demande. Les informations relatives à l'identité permettent de déterminer les éléments suivants :

- Si la demande a été effectuée avec les informations d'identification utilisateur racine ou AWS Identity and Access Management (IAM).
- Si la demande a été effectuée avec les informations d'identification de sécurité temporaires d'un rôle ou d'un utilisateur fédéré.
- Si la requête a été effectuée par un autre Service AWS.

Pour plus d'informations, consultez l'élément userIdentity CloudTrail.

Vous pouvez également regrouper des fichiers journaux AWS Support Plans provenant de plusieurs Régions AWS et de plusieurs comptes dans un seul compartiment Amazon S3.

Comprendre les entrées du fichier journal d'AWS Support Plans

Un journal d'activité est une configuration qui permet d'envoyer des événements sous forme de fichiers journaux à un compartiment Simple Storage Service (Amazon S3) que vous spécifiez. Les fichiers journaux CloudTrail peuvent contenir une ou plusieurs entrées de journal. Un événement représente une demande unique d'une source quelconque. Il comprend des informations sur l'opération demandée, la date et l'heure de l'opération, les paramètres de la requête, etc. Les fichiers journaux CloudTrail ne constituent pas une série ordonnée retraçant les appels d'API publics. Ils ne suivent aucun ordre précis.

Example : Entrée de journal pour **`GetSupportPlan`**

L'exemple suivant montre une entrée de journal CloudTrail pour une opération `GetSupportPlan`.


```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "AssumedRole",
        "principalId": "AIDACKCEVSQ6C2EXAMPLE",
        "arn": "arn:aws:sts::111122223333:user/janedoe",
        "accountId": "111122223333",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "sessionContext": {
            "sessionIssuer": {
                "type": "Role",
                "principalId": "AIDACKCEVSQ6C2EXAMPLE",
                "arn": "arn:aws:iam::111122223333:role/Admin",
                "accountId": "111122223333",
                "userName": "Admin"
            },
            "webIdFederationData": {},
            "attributes": {
                "creationDate": "2022-06-29T16:30:04Z",
                "mfaAuthenticated": "false"
            }
        }
    },
    "eventTime": "2022-06-29T16:39:11Z",
    "eventSource": "supportplans.amazonaws.com",
```

```
    "eventName": "GetSupportPlan",
    "awsRegion": "us-west-2",
    "sourceIPAddress": "205.251.233.183",
    "userAgent": "Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:91.0) Gecko/20100101
 Firefox/91.0",
    "requestParameters": null,
    "responseElements": null,
    "requestID": "7665c39a-d6bf-4d0d-8010-2f59740b8ecb",
    "eventID": "b711bc30-16a5-4579-8f0d-9ada8fe6d1ce",
    "readOnly": true,
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "111122223333",
    "eventCategory": "Management"
}
```

Example : Entrée de journal pour **`GetSupportPlanUpdateStatus`**

L'exemple suivant montre une entrée de journal CloudTrail pour une opération `GetSupportPlanUpdateStatus`.

```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "AssumedRole",
        "principalId": "AIDACKCEVSQ6C2EXAMPLE",
        "arn": "arn:aws:sts::111122223333:user/janedoe",
        "accountId": "111122223333",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "sessionContext": {
            "sessionIssuer": {
                "type": "Role",
                "principalId": "AIDACKCEVSQ6C2EXAMPLE",
                "arn": "arn:aws:iam::111122223333:role/Admin",
                "accountId": "111122223333",
                "userName": "Admin"
            },
            "webIdFederationData": {},
            "attributes": {
                "creationDate": "2022-06-29T16:30:04Z",
                "mfaAuthenticated": "false"
            }
        }
```

```
    },
    "eventTime": "2022-06-29T16:39:02Z",
    "eventSource": "supportplans.amazonaws.com",
    "eventName": "GetSupportPlanUpdateStatus",
    "awsRegion": "us-west-2",
    "sourceIPAddress": "205.251.233.183",
    "userAgent": "Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:91.0) Gecko/20100101
 Firefox/91.0",
    "requestParameters": {
        "supportPlanUpdateArn":
 "arn:aws:supportplans::111122223333:supportplanupdate/7f03b7a233a0e87ebc79e56d4d2bcaf19e976c37
    },
    "responseElements": null,
    "requestID": "75e5c767-8703-4ed3-b01e-4dda28020322",
    "eventID": "28d1c0e3-ccb6-4fd1-8793-65be010114cc",
    "readOnly": true,
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "111122223333",
    "eventCategory": "Management"
}
```


Example : Entrée de journal pour **`StartSupportPlanUpdate`**

L'exemple suivant montre une entrée de journal CloudTrail pour une opération `StartSupportPlanUpdate`.


```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "AssumedRole",
        "principalId": "AIDACKCEVSQ6C2EXAMPLE",
        "arn": "arn:aws:sts::111122223333:user/janedoe",
        "accountId": "111122223333",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "sessionContext": {
            "sessionIssuer": {
                "type": "Role",
                "principalId": "AIDACKCEVSQ6C2EXAMPLE",
                "arn": "arn:aws:iam::111122223333:role/Admin",
                "accountId": "111122223333",
                "userName": "Admin"
            },
```

```
            "webIdFederationData": {},
            "attributes": {
                "creationDate": "2022-06-29T16:30:04Z",
                "mfaAuthenticated": "false"
            }
        }
    },
    "eventTime": "2022-06-29T16:38:55Z",
    "eventSource": "supportplans.amazonaws.com",
    "eventName": "StartSupportPlanUpdate",
    "awsRegion": "us-west-2",
    "sourceIPAddress": "205.251.233.183",
    "userAgent": "Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:91.0) Gecko/20100101
 Firefox/91.0",
    "requestParameters": {
        "clientToken": "98add111-dcc9-464d-8722-438d697fe242",
        "update": {
            "supportLevel": "BASIC"
        }
    },
    "responseElements": {
        "Access-Control-Expose-Headers": "x-amzn-RequestId,x-amzn-ErrorType,x-amzn-
ErrorMessage,Date",
        "supportPlanUpdateArn":
 "arn:aws:supportplans::111122223333:supportplanupdate/7f03b7a233a0e87ebc79e56d4d2bcaf19e976c37
    },
    "requestID": "e5ff9382-5fb8-4764-9993-0f33fb0b1e17",
    "eventID": "5dba89f8-2e5b-42b9-9b8f-395580c52962",
    "readOnly": false,
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "111122223333",
    "eventCategory": "Management"
}
```


Example : Entrée de journal pour **`CreateSupportPlanSchedule`**

L'exemple suivant montre une entrée de journal CloudTrail pour une opération `CreateSupportPlanSchedule`.


```
{
    "eventVersion": "1.08",
    "userIdentity": {
```

```
        "type": "AssumedRole",
        "principalId": "AIDACKCEVSQ6C2EXAMPLE",
        "arn": "arn:aws:sts::111122223333:user/janedoe",
        "accountId": "111122223333",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "sessionContext": {
            "sessionIssuer": {
                "type": "Role",
                "principalId": "AIDACKCEVSQ6C2EXAMPLE",
                "arn": "arn:aws:iam::111122223333:role/Admin",
                "accountId": "111122223333",
                "userName": "Admin"
            },
            "webIdFederationData": {},
            "attributes": {
                "creationDate": "2023-05-09T16:30:04Z",
                "mfaAuthenticated": "false"
            }
        }
    },
    "eventTime": "2023-05-09T16:30:04Z",
    "eventSource": "supportplans.amazonaws.com",
    "eventName": "CreateSupportPlanSchedule",
    "awsRegion": "us-west-2",
    "sourceIPAddress": "205.251.233.183",
    "userAgent": "Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:91.0) Gecko/20100101
 Firefox/91.0",
    "requestParameters": {
        "clientToken": "b998de5e-ad1c-4448-90db-2bf86d6d9e9a",
        "scheduleCreationDetails": {
            "startLevel": "BUSINESS",
            "startOffer": "TrialPlan7FB93B",
            "startTimestamp": "2023-06-03T17:23:56.109Z",
            "endLevel": "BUSINESS",
            "endOffer": "StandardPlan2074BB",
            "endTimestamp": "2023-09-03T17:23:55.109Z"
        }
    },
    "responseElements": {
        "Access-Control-Expose-Headers": "x-amzn-RequestId,x-amzn-ErrorType,x-amzn-
ErrorMessage,Date",
        "supportPlanUpdateArn":
 "arn:aws:supportplans::111122223333:supportplanschedule/
b9a9a4336a3974950a6e670f7dab79b77a4b104db548a0d57050ce4544721d4b"
```

```
    },
    "requestID": "150450b8-e61a-4b15-93a8-c3b557a1ca48",
    "eventID": "a2a1ba44-610d-4dc8-bf16-29f1635b57a9",
    "readOnly": false,
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "111122223333",
    "eventCategory": "Management"
}
```

Journalisation des modifications apportées à votre plan AWS Support

Important

À compter du 3 août 2022, les opérations suivantes sont obsolètes et n'apparaîtront plus dans vos nouveaux journaux CloudTrail. Pour une liste des opérations prises en charge, consultez Comprendre les entrées du fichier journal d'AWS Support Plans.

- `DescribeSupportLevelSummary` : Cette action s'affiche dans votre journal lorsque vous ouvrez la page Plans de support.
- `UpdateProbationAutoCancellation` : Une fois que vous vous êtes inscrit au plan de support Developer ou Business, puis que vous essayez d'annuler dans les 30 jours, votre plan sera automatiquement annulé à la fin de cette période. Cette action apparaît dans votre journal lorsque vous choisissez Opt-out of automatic cancellation (Abandonner l'annulation automatique) dans la bannière qui apparaît dans la page Formules AWS Support. Vous reprendrez votre plan de support Developer ou Business.
- `UpdateSupportLevel` : cette action s'affiche dans votre journal lorsque vous modifiez votre plan de support.

Note

Le champ `eventSource` a l'espace de nom `support-subscription.amazonaws.com` pour ces actions.

Example : Entrée de journal pour DescribeSupportLevelSummary

L'exemple suivant montre une entrée de journal CloudTrail pour l'action `DescribeSupportLevelSummary`.


```
{
  "eventVersion": "1.08",
  "userIdentity": {
    "type": "Root",
    "principalId": "111122223333",
    "arn": "arn:aws:iam::111122223333:root",
    "accountId": "111122223333",
    "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
    "sessionContext": {
      "sessionIssuer": {},
      "webIdFederationData": {},
      "attributes": {
        "mfaAuthenticated": "false",
        "creationDate": "2021-01-07T22:08:05Z"
      }
    }
  },
  "eventTime": "2021-01-07T22:08:07Z",
  "eventSource": "support-subscription.amazonaws.com",
  "eventName": "DescribeSupportLevelSummary",
  "awsRegion": "us-east-1",
  "sourceIPAddress": "100.127.8.67",
  "userAgent": "AWS-SupportPlansConsole, aws-internal/3",
  "requestParameters": {
    "lang": "en"
  },
  "responseElements": null,
  "requestID": "b423b84d-829b-4090-a239-2b639b123abc",
  "eventID": "e1eeda0e-d77c-487b-a7e5-4014f7123abc",
  "readOnly": true,
  "eventType": "AwsApiCall",
  "managementEvent": true,
  "eventCategory": "Management",
  "recipientAccountId": "111122223333"
}
```

Example : Entrée de journal pour UpdateProbationAutoCancellation

L'exemple suivant montre une entrée de journal CloudTrail pour l'action `UpdateProbationAutoCancellation`.


```
{
  "eventVersion": "1.08",
  "userIdentity": {
    "type": "Root",
    "principalId": "111122223333",
    "arn": "arn:aws:iam::111122223333:root",
    "accountId": "111122223333",
    "accessKeyId": "AKIAIOSFODNN7EXAMPLE"
  },
  "eventTime": "2021-01-07T23:28:43Z",
  "eventSource": "support-subscription.amazonaws.com",
  "eventName": "UpdateProbationAutoCancellation",
  "awsRegion": "us-east-1", "sourceIPAddress": "100.127.8.67",
  "userAgent": "AWS-SupportPlansConsole, aws-internal/3",
  "requestParameters": {
    "lang": "en"
  },
  "responseElements": null,
  "requestID": "5492206a-e200-4c33-9fcf-4162d4123abc",
  "eventID": "f4a58c09-0bb0-4ba2-a8d3-df6909123abc",
  "readOnly": false,
  "eventType": "AwsApiCall",
  "managementEvent": true,
  "eventCategory": "Management",
  "recipientAccountId": "111122223333"
}
```


Example : Entrée de journal pour UpdateSupportLevel

L'exemple suivant montre une entrée de journal CloudTrail pour l'action `UpdateSupportLevel` pour passer au support Developer.


```
{
  "eventVersion": "1.08",
  "userIdentity": {
    "type": "Root",
    "principalId": "111122223333",
    "arn": "arn:aws:iam::111122223333:root",
```

```
    "accountId": "111122223333",
    "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
    "sessionContext": {
      "sessionIssuer": {},
      "webIdFederationData": {},
      "attributes": {
        "mfaAuthenticated": "false",
        "creationDate": "2021-01-07T22:08:05Z"
      }
    }
  },
  "eventTime": "2021-01-07T22:08:43Z",
  "eventSource": "support-subscription.amazonaws.com",
  "eventName": "UpdateSupportLevel",
  "awsRegion": "us-east-1",
  "sourceIPAddress": "100.127.8.247",
  "userAgent": "AWS-SupportPlansConsole, aws-internal/3",
  "requestParameters": {
    "supportLevel": "new_developer"
  },
  "responseElements": {
    "aispl": false,
    "supportLevel": "new_developer"
  },
  "requestID": "5df3da3a-61cd-4a3c-8f41-e5276b123abc",
  "eventID": "c69fb149-c206-47ce-8766-8df6ec123abc",
  "readOnly": false,
  "eventType": "AwsApiCall",
  "managementEvent": true,
  "eventCategory": "Management",
  "recipientAccountId": "111122223333"
}
```

Surveillance et journalisation pour AWS Trusted Advisor

La surveillance constitue une part importante de la gestion de la fiabilité, de la disponibilité et des performances d'Trusted Advisor et de vos autres solutions AWS. AWS fournit les outils de surveillance suivants pour surveiller Trusted Advisor, signaler les problèmes et prendre des mesures automatiques, le cas échéant :

- Amazon EventBridge fournit un flux d'événements système en temps quasi réel qui décrivent les modifications apportées aux ressources AWS. EventBridge permet d'effectuer des calculs automatisés pilotés par des événements, car vous pouvez écrire des règles pour surveiller certains événements et déclencher des actions automatisées dans d'autres services AWS lorsque ces événements se produisent.

  Par exemple, Trusted Advisor fournit la vérification Autorisations relatives aux compartiments Amazon S3. Ce contrôle permet de déterminer si vous disposez de compartiments disposant d'autorisations d'accès ouvert ou autorisant l'accès à un utilisateur AWS authentifié. Si une autorisation de compartiment change, l'état change pour la vérification Trusted Advisor. EventBridge détecte cet événement, puis vous envoie une notification afin que vous puissiez agir. Pour plus d'informations, consultez le Guide de l'utilisateur Amazon EventBridge.
- AWS Trusted Advisor identifie les moyens de réduire vos coûts, d'augmenter les performances et d'améliorer la sécurité de votre compte AWS. Vous pouvez utiliser EventBridge pour surveiller le statut des vérifications Trusted Advisor. Vous pouvez ensuite utiliser Amazon CloudWatch pour créer des alarmes sur les métriques Trusted Advisor. Ces alarmes vous avertissent lorsque le statut d'un contrôle Trusted Advisor change, par exemple une ressource mise à jour ou un quota de service atteint.
- AWS CloudTrail capture les appels d'API et les événements associés créés par ou au nom de votre compte AWS et envoie les fichiers journaux à un compartiment Amazon S3 que vous spécifiez. Vous pouvez identifier les utilisateurs et les comptes qui ont appelé AWS, l'adresse IP source à partir de laquelle les appels ont été émis, ainsi que le moment où les appels ont eu lieu. Pour de plus amples informations, veuillez consulter le Guide de l'utilisateur AWS CloudTrail.

Rubriques

Surveillance des résultats des AWS Trusted Advisor contrôles avec Amazon EventBridge

Vous pouvez l'utiliser EventBridge pour détecter le moment où vous vérifiez l'état du Trusted Advisor changement. Ensuite, en fonction des règles que vous créez, EventBridge invoque une ou plusieurs actions cibles lorsque le statut passe à une valeur que vous spécifiez dans une règle.

En fonction du changement de statut, vous pouvez envoyer des notifications, capturer les informations de statut, prendre des mesures correctives, déclencher des événements ou prendre d'autres mesures. Par exemple, vous pouvez spécifier les types de cible suivants si une vérification change de statut, passant d'aucun problème détecté (vert) à action recommandée (rouge).

- Utiliser une fonction AWS Lambda pour transmettre une notification à un canal Slack.
- Envoyer les données relatives à la vérification à un flux Amazon Kinesis pour prendre en charge la surveillance complète et en temps réel du statut.
- Envoyer une rubrique Amazon Simple Notification Service à votre e-mail.
- Recevez une notification d'une action CloudWatch d'alarme Amazon.

Pour plus d'informations sur l'utilisation EventBridge des fonctions Lambda pour automatiser les réponsesTrusted Advisor, consultez les Trusted Advisoroutils dans. GitHub

> **Remarques**
>
> - Trusted Advisor fournit des événements dans la mesure du possible. Les événements ne sont pas toujours garantis d'être fournis à EventBridge.
> - Vous devez disposer d'un plan de AWS Support Business, Enterprise On-Ramp ou Enterprise pour créer une règle pour les contrôles Trusted Advisor. Pour en savoir plus, consultez Modifier les AWS Support plans.
> - Comme Trusted Advisor c'est le cas pour un service mondial, tous les événements sont diffusés EventBridge dans la région de l'est des États-Unis (Virginie du Nord).

Suivez cette procédure pour créer une EventBridge règle pourTrusted Advisor. Avant de créer des règles d'événement, effectuez les opérations suivantes :

- 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.
- Créez la cible que vous allez utiliser dans votre règle d'événement.

Pour créer une EventBridge règle pour Trusted Advisor

1. Ouvrez la EventBridge console Amazon à l'adresse https://console.aws.amazon.com/events/.
2. Pour changer de région, utilisez Region selector (Sélecteur de région) dans l'angle supérieur droit de la page et choisissez USA Est (Virginie du Nord).
3. Dans le volet de navigation, choisissez Rules.
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 AWSévénements ou événements EventBridge partenaires.
8. Sous Event pattern (Modèle d'événement), conservez la valeur par défaut pour Services AWS.
9. Pour Service AWS, choisissez Trusted Advisor.
10. Pour Event type (Type d'événement), choisissez Check Item Refresh Status (Statut d'actualisation d'un élément de vérification).
11. Choisissez l'une des options suivantes pour les statuts de vérification :
    - Choisissez Any status (Tout statut) pour créer une règle qui surveille toute modification de statut.
    - Choisissez Specific status(es) (Statuts spécifiques), puis choisissez les valeurs que vous voulez que votre règle surveille.
      - ERROR : Trusted Advisor recommande une action pour la vérification.
      - INFO : Trusted Advisor ne peut pas déterminer le statut de la vérification.
      - OK : Trusted Advisor ne détecte pas de problème pour la vérification.
      - WARN : Trusted Advisor détecte un problème possible pour la vérification et recommande une investigation.

12. Choisissez l'une des options suivantes pour vos vérifications :
    - Choisissez Any check (Toute vérification).
    - Choisissez Specific check(s) (Vérifications spécifiques), puis choisissez un ou plusieurs noms de vérifications dans la liste.
13. Choisissez l'une des options suivantes pour les ressources AWS :
    - Choisissez Any resource ID (Tout ID de ressource) pour créer une règle qui surveille toutes les ressources.
    - Choisissez Specific resource ID(s) by ARN (ID de ressource spécifiques par ARN), puis saisissez les Amazon Resource Names (ARN) que vous souhaitez.
14. Choisissez Suivant.
15. Sur la page Select target(s) (Sélectionner la(les) cible(s)), choisissez le type de cible que vous avez créé pour cette règle, puis configurez toutes 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.
16. Choisissez Suivant.
17. (Facultatif) Sur la page Configure tags (Configurer des étiquettes), ajoutez des étiquettes, puis choisissez Next (Suivant).
18. 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.
19. Choisissez Créer une règle. Votre règle va maintenant surveiller les vérifications Trusted Advisor et ensuite envoyer l'événement à la cible que vous avez spécifiée.

Création d'alarmes Amazon CloudWatch pour contrôler les métriques AWS Trusted Advisor

Quand AWS Trusted Advisor actualise vos vérifications, Trusted Advisor publie des métriques concernant les résultats de vos vérifications dans CloudWatch. Vous pouvez afficher les métriques dans CloudWatch. Vous pouvez également créer des alarmes pour détecter les modifications d'état et les vérifications Trusted Advisor pour les ressources, et l'utilisation des quotas de service (anciennement appelés limites). Par exemple, vous pouvez créer une alarme pour suivre les modifications d'état des contrôles dans la catégorie Services Limits. L'alarme vous avertira alors lorsque vous atteignez ou dépassez un quota de service pour votre compte AWS.

Suivez cette procédure pour créer une alarme CloudWatch pour une métrique Trusted Advisor spécifiques.

Rubriques

Prérequis

Avant de créer des alarmes CloudWatch pour les métriques Trusted Advisor, passez en revue les informations suivantes :

- Comprenez comment CloudWatch utilise les métriques et les alarmes. Pour de plus amples informations, veuillez consulter Fonctionnement de CloudWatch dans le Guide de l'utilisateur Amazon CloudWatch.
- Utilisez la console Trusted Advisor ou l'API AWS Support pour actualiser vos vérifications et obtenir les derniers résultats de vérification. Pour plus d'informations, consultez Actualiser les résultats de vérifications.

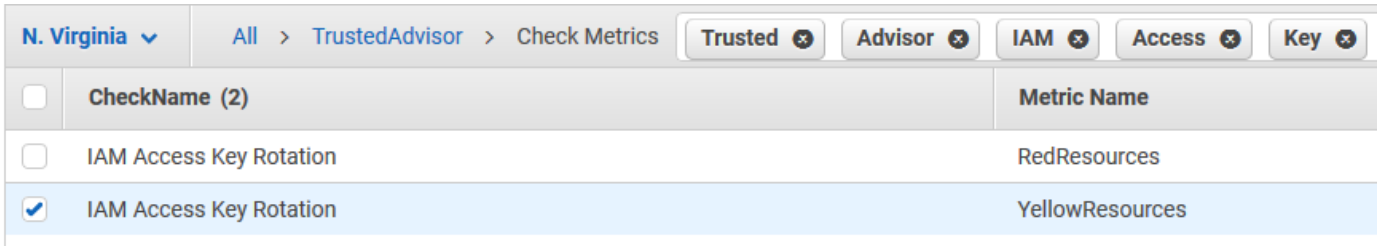
Pour créer une alarme CloudWatch pour des métriques Trusted Advisor

1. Ouvrez la console CloudWatch à l'adresse https://console.aws.amazon.com/cloudwatch/.
2. Utilisez le sélecteur de région et choisissez la région AWS US East (N. Virginia) (USA Est (Virginie du Nord)).
3. Dans le panneau de navigation, cliquez sur Alarms (Alarmes).
4. Choisissez Create alarm (Créer une alerte).
5. Choisissez Sélectionner une métrique.
6. Pour Metrics (Métriques), saisissez une ou plusieurs valeurs de dimension afin de filtrer la liste des métriques. Par exemple, vous pouvez entrer le nom de la métrique ServiceLimitUsageou la dimension, telle que le nom de vérification Trusted Advisor.

> **Tip**
>
> - Vous pouvez rechercher **`Trusted Advisor`** pour répertorier toutes les métriques du service.
> - Pour obtenir une liste des noms de métriques et de dimensions, consultez Trusted AdvisorMétriques et dimensions d'.

7. Dans la table des résultats, cochez la case pour la métrique.

   Dans l'exemple suivant, le nom de vérification est IAM Access Key Rotation (Rotation des clés d'accès IAM) et que le nom de métrique est YellowResources.



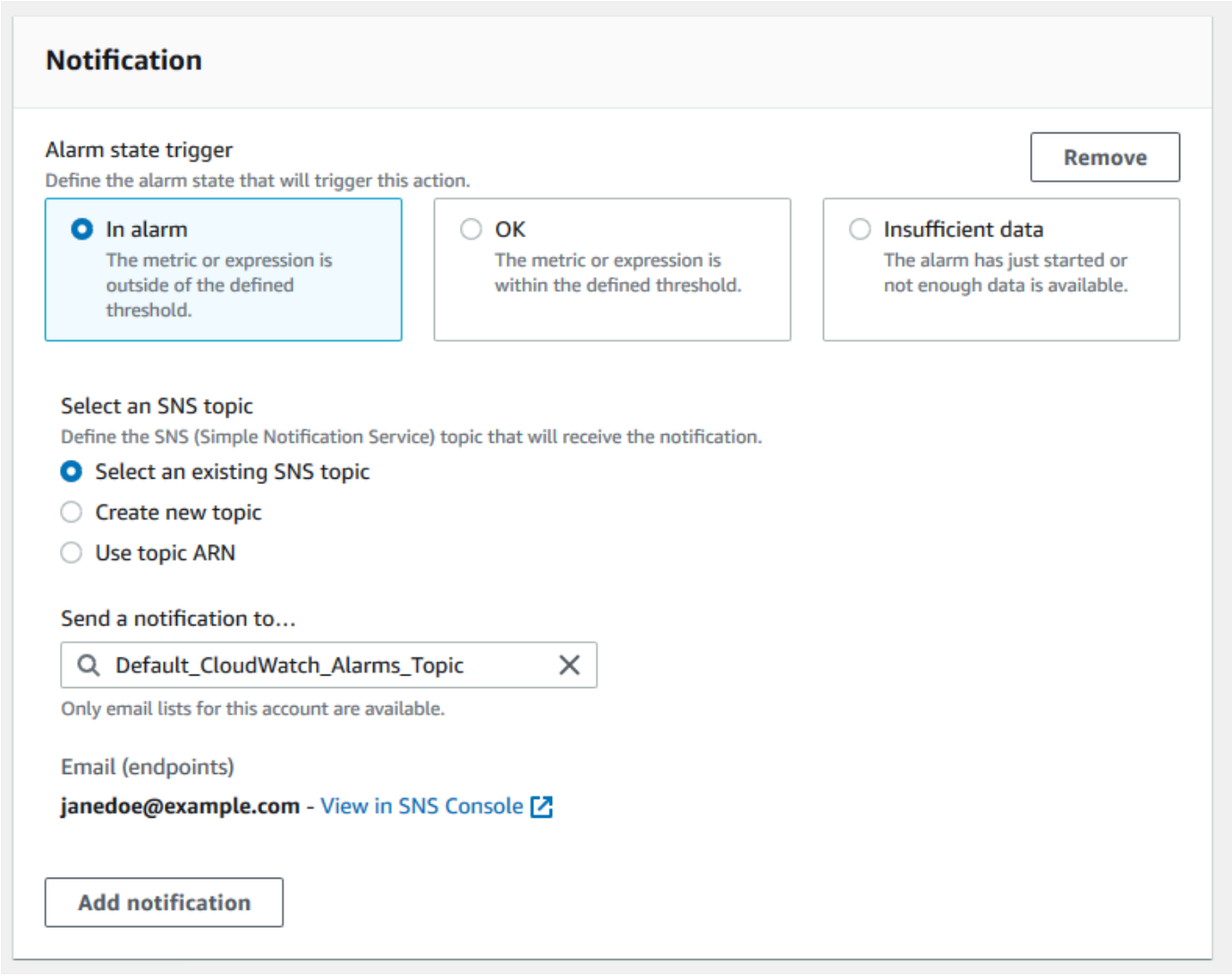
8. Choisissez Select metric (Sélectionner une métrique).
9. Dans la page Specify metric and conditions (Spécifier la métrique et les conditions), vérifiez que le nom de métrique et le nom de vérificationque vous avez choisi s'affichent sur la page.
10. Pour Period (Période), vous pouvez spécifier la période pendant laquelle vous souhaitez que l'alarme démarre lorsque l'état de la vérification change, par exemple 5 minutes.
11. Sous Conditions, choisissez Static (Statique), puis spécifiez la condition d'alarme pour le moment où l'alarme doit démarrer.

    Par exemple, si vous choisissez Greater/Equal >=threshold (Supérieur/égal >=seuil) et saisissez **1** pour la valeur seuil, cela signifie que l'alarme démarre lorsque Trusted Advisor détecte au moins une clé d'accès IAM n'ayant pas fait l'objet d'une rotation au cours des 90 derniers jours.

> **Remarques**
>
> - Pour les métriques GreenChecks, RedChecks, YellowChecks, RedResources et YellowResources, vous pouvez spécifier un seuil correspondant à n'importe quel nombre entier supérieur ou égal à zéro.

- Trusted Advisor n'envoie pas les métriques pour GreenResources, qui sont des ressources pour lesquelles Trusted Advisor n'a détecté aucun problème.

12. Choisissez Suivant.
13. Dans la page Configure actions (Configuration d'actions), pour Alarm state trigger (déclencheur d'état d'alarme), choisissez In alarm (avec alarme).
14. Pour Select an SNS topic (Sélectionner une rubrique SNS), choisissez une rubrique Amazon Simple Notification Service (Amazon SNS) existante ou créez-en une.



15. Choisissez Next (Suivant).
16. Pour Name and description (Nom et description), saisissez un nom et une description pour votre alarme.
17. Choisissez Next (Suivant).

18. Dans la page Preview and create (Aperçu et création), passez en revue les détails de votre alarme, puis choisissez Create alarm (Créer une alarme).

    Lorsque l'état de la vérification IAM Access Key Rotation (Rotation des clés d'accès IAM) change et est rouge pendant 5 minutes, votre alarme enverra une notification à votre rubrique SNS.

Example : Notification par e-mail pour une alarme CloudWatch

Le message électronique suivant indique qu'une alarme a détecté une modification dans la vérification IAM Access Key Rotation (Rotation des clés d'accès IAM).

```
You are receiving this email because your Amazon CloudWatch Alarm
 "IAMAcessKeyRotationCheckAlarm" in the US East (N. Virginia) region has entered the
 ALARM state,
because "Threshold Crossed: 1 out of the last 1 datapoints [9.0 (26/03/21 22:44:00)]
 was greater than or equal to the threshold (1.0) (minimum 1 datapoint for OK -> ALARM
 transition)." at "Friday 26 March, 2021 22:49:42 UTC".

View this alarm in the AWS Management Console:
https://us-east-1.console.aws.amazon.com/cloudwatch/home?region=us-
east-1#s=Alarms&alarm=IAMAcessKeyRotationCheckAlarm

Alarm Details:
- Name:                       IAMAcessKeyRotationCheckAlarm
- Description:                This alarm starts when one or more AWS access keys in my
 AWS account have not been rotated in the last 90 days.
- State Change:               INSUFFICIENT_DATA -> ALARM
- Reason for State Change:    Threshold Crossed: 1 out of the last 1 datapoints [9.0
 (26/03/21 22:44:00)] was greater than or equal to the threshold (1.0) (minimum 1
 datapoint for OK -> ALARM transition).
- Timestamp:                  Friday 26 March, 2021 22:49:42 UTC
- AWS Account:                123456789012
- Alarm Arn:                  arn:aws:cloudwatch:us-
east-1:123456789012:alarm:IAMAcessKeyRotationCheckAlarm

Threshold:
- The alarm is in the ALARM state when the metric is GreaterThanOrEqualToThreshold 1.0
 for 300 seconds.

Monitored Metric:
- MetricNamespace:                    AWS/TrustedAdvisor
- MetricName:                         RedResources
```

```
- Dimensions:                          [CheckName = IAM Access Key Rotation]
- Period:                              300 seconds
- Statistic:                           Average
- Unit:                                not specified
- TreatMissingData:                    missing


State Change Actions:
- OK:
- ALARM: [arn:aws:sns:us-east-1:123456789012:Default_CloudWatch_Alarms_Topic]
- INSUFFICIENT_DATA:
```

Métriques CloudWatch pour Trusted Advisor

Vous pouvez utiliser la console CloudWatch ou la AWS Command Line Interface (AWS CLI) pour trouver les métriques disponibles pour Trusted Advisor.

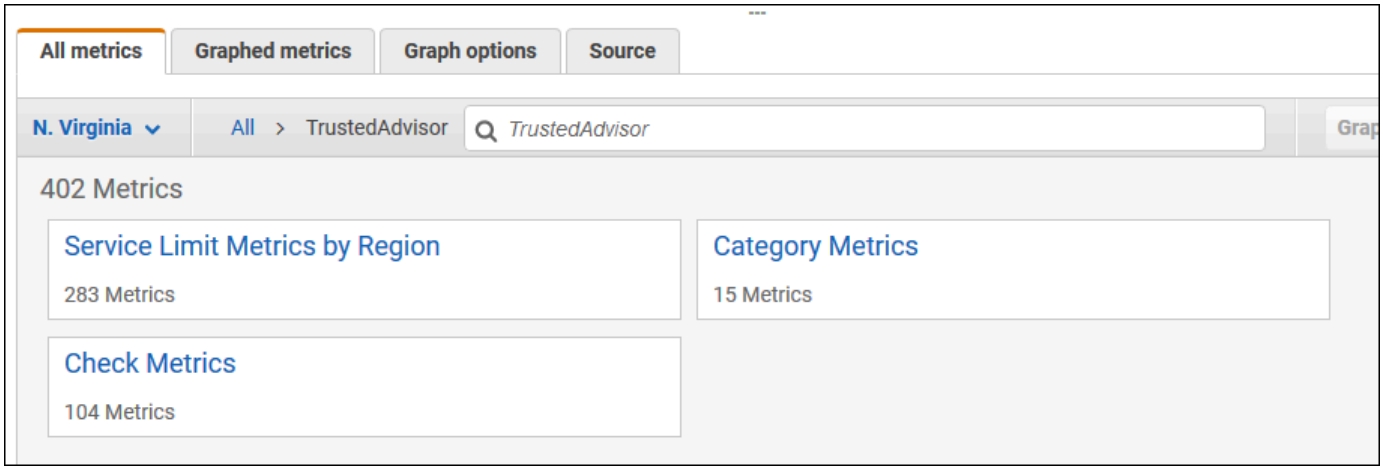
Pour obtenir la liste des espaces de noms, des métriques et des dimensions de tous les services qui publient des métriques, veuillez consulter Services AWS qui publient des métriques CloudWatch dans le Guide de l'utilisateur Amazon CloudWatch..

Afficher les métriques Trusted Advisor (console)

Vous pouvez utiliser la console CloudWatch et afficher les métriques disponibles pour Trusted Advisor.

Pour afficher les métriques Trusted Advisor disponibles (console)

1. Ouvrez la console CloudWatch à l'adresse https://console.aws.amazon.com/cloudwatch/.
2. Utilisez le sélecteur de région et choisissez la région AWS US East (N. Virginia) (USA Est (Virginie du Nord)).
3. Dans le volet de navigation, sélectionnez Metrics (Métriques).
4. Entrez un espace de noms de métrique, tel que **`TrustedAdvisor`**.
5. Sélectionnez une dimension de métrique, telle que Check Metrics (Métriques de vérification).



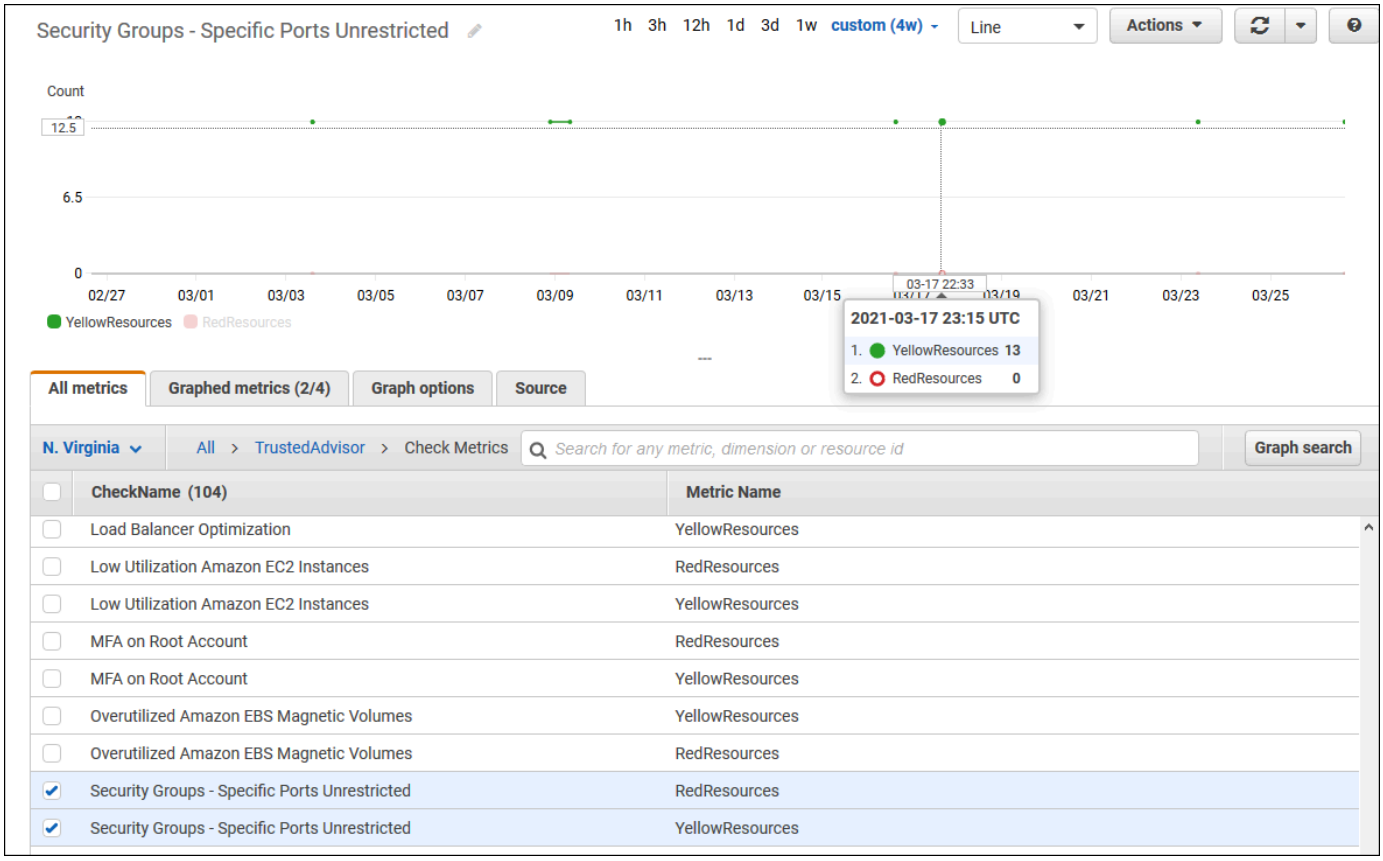
6. L'onglet All metrics (Toutes les métriques) affiche les métriques pour cette dimension dans l'espace de nom. Vous pouvez effectuer les actions suivantes :

   a. Pour trier le tableau, choisissez l'en-tête de colonne.

   b. Pour représenter graphiquement une métrique, cochez la case en regard de la métrique. Pour sélectionner toutes les métriques, cochez la case dans la ligne d'en-tête du tableau.

   c. Pour filtrer par métrique, choisissez le nom de la métrique, puis Ajouter à la recherche.

   L'exemple suivant illustre les résultats de la vérification Security Groups - Specific Ports Unrestricted (Groupes de sécurité :Ports spécifiques non restreints). La vérification identifie 13 ressources jaunes. Trusted Advisor vous recommande d'investiguer les vérifications en jaune.



7. (Facultatif) Pour ajouter ce graphique à un tableau de bord CloudWatch, choisissez Actions, puis choisissez Add to dashboard (Ajouter au tableau de bord).

   Pour plus d'informations sur la création d'un graphique pour afficher vos métriques, consultez Graphique d'une métrique dans le Guide de l'utilisateur Amazon CloudWatch..

Afficher les métriques Trusted Advisor (CLI)

Vous pouvez utiliser la commande AWS CLI, list-metrics pour afficher les métriques disponibles pour Trusted Advisor.

Example : répertorie toutes les mesures pour Trusted Advisor

L'exemple suivant spécifie l'espace de noms `AWS/TrustedAdvisor` pour afficher toutes les métriques pour Trusted Advisor.

```
aws cloudwatch list-metrics --namespace AWS/TrustedAdvisor
```

Le résultat peut être similaire à ce qui suit.

```
{
    "Metrics": [
        {
            "Namespace": "AWS/TrustedAdvisor",
            "Dimensions": [
                {
                    "Name": "ServiceName",
                    "Value": "EBS"
                },
                {
                    "Name": "ServiceLimit",
                    "Value": "Magnetic (standard) volume storage (TiB)"
                },
                {
                    "Name": "Region",
                    "Value": "ap-northeast-2"
                }
            ],
            "MetricName": "ServiceLimitUsage"
        },
        {
            "Namespace": "AWS/TrustedAdvisor",
            "Dimensions": [
                {
                    "Name": "CheckName",
                    "Value": "Overutilized Amazon EBS Magnetic Volumes"
                }
            ],
            "MetricName": "YellowResources"
        },
        {
            "Namespace": "AWS/TrustedAdvisor",
            "Dimensions": [
                {
                    "Name": "ServiceName",
                    "Value": "EBS"
                },
                {
                    "Name": "ServiceLimit",
                    "Value": "Provisioned IOPS"
                },
                {
                    "Name": "Region",
```

```
                    "Value": "eu-west-1"
                }
            ],
            "MetricName": "ServiceLimitUsage"
        },
        {
            "Namespace": "AWS/TrustedAdvisor",
            "Dimensions": [
                {
                    "Name": "ServiceName",
                    "Value": "EBS"
                },
                {
                    "Name": "ServiceLimit",
                    "Value": "Provisioned IOPS"
                },
                {
                    "Name": "Region",
                    "Value": "ap-south-1"
                }
            ],
            "MetricName": "ServiceLimitUsage"
        },
    ...
  ]
}
```

Example : liste de toutes les métriques pour une dimension

L'exemple suivant spécifie l'espace de nom `AWS/TrustedAdvisor` et la dimension `Region` afin d'afficher les métriques disponibles pour la région AWS spécifiée.

```
aws cloudwatch list-metrics --namespace AWS/TrustedAdvisor --dimensions
 Name=Region,Value=us-east-1
```

Le résultat peut être similaire à ce qui suit.

```
{
    "Metrics": [
        {
            "Namespace": "AWS/TrustedAdvisor",
            "Dimensions": [
                {
```

```
                    "Name": "ServiceName",
                    "Value": "SES"
                },
                {
                    "Name": "ServiceLimit",
                    "Value": "Daily sending quota"
                },
                {
                    "Name": "Region",
                    "Value": "us-east-1"
                }
            ],
            "MetricName": "ServiceLimitUsage"
        },
        {
            "Namespace": "AWS/TrustedAdvisor",
            "Dimensions": [
                {
                    "Name": "ServiceName",
                    "Value": "AutoScaling"
                },
                {
                    "Name": "ServiceLimit",
                    "Value": "Launch configurations"
                },
                {
                    "Name": "Region",
                    "Value": "us-east-1"
                }
            ],
            "MetricName": "ServiceLimitUsage"
        },
        {
            "Namespace": "AWS/TrustedAdvisor",
            "Dimensions": [
                {
                    "Name": "ServiceName",
                    "Value": "CloudFormation"
                },
                {
                    "Name": "ServiceLimit",
                    "Value": "Stacks"
                },
                {
```

```
                    "Name": "Region",
                    "Value": "us-east-1"
                }
            ],
            "MetricName": "ServiceLimitUsage"
        },
    ...
  ]
}
```

Example : liste les métriques d'un nom de métrique spécifique

L'exemple suivant spécifie l'espace de nom `AWS/TrustedAdvisor` et un nom de métrique `RedResources` pour afficher les résultats uniquement pour la métrique spécifiée.

```
aws cloudwatch list-metrics --namespace AWS/TrustedAdvisor --metric-name RedResources
```

Le résultat peut être similaire à ce qui suit.

```
{
    "Metrics": [
        {
            "Namespace": "AWS/TrustedAdvisor",
            "Dimensions": [
                {
                    "Name": "CheckName",
                    "Value": "Amazon RDS Security Group Access Risk"
                }
            ],
            "MetricName": "RedResources"
        },
        {
            "Namespace": "AWS/TrustedAdvisor",
            "Dimensions": [
                {
                    "Name": "CheckName",
                    "Value": "Exposed Access Keys"
                }
            ],
            "MetricName": "RedResources"
        },
        {
            "Namespace": "AWS/TrustedAdvisor",
```

```
            "Dimensions": [
                {
                    "Name": "CheckName",
                    "Value": "Large Number of Rules in an EC2 Security Group"
                }
            ],
            "MetricName": "RedResources"
        },
        {
            "Namespace": "AWS/TrustedAdvisor",
            "Dimensions": [
                {
                    "Name": "CheckName",
                    "Value": "Auto Scaling Group Health Check"
                }
            ],
            "MetricName": "RedResources"
        },
    ...
  ]
}
```

Trusted AdvisorMétriques et dimensions d'

Consultez les tableaux suivants pour en savoir plus sur les métriques et les dimensions Trusted Advisor que vous pouvez utiliser pour vos alarmes et vos graphiques CloudWatch.

Métriques de niveau de vérification Trusted Advisor

Vous pouvez utiliser les métriques suivantes pour les vérifications Trusted Advisor.

Métrique	Description
`RedResources`	Nombre de ressources à l'état rouge (action recommandée).
`YellowResources`	Nombre de ressources à l'état jaune (investigation recommandée).

Métriques de niveau de catégorie Trusted Advisor

Vous pouvez utiliser les métriques suivantes pour les catégories Trusted Advisor.

Métrique	Description
`GreenChecks`	Le nombre de vérifications Trusted Advisor à l'état vert (aucun problème détecté).
`RedChecks`	Le nombre de vérifications Trusted Advisor à l'état rouge (action recommandée).
`YellowChecks`	Le nombre de vérifications Trusted Advisor à l'état jaune (investigation recommandée).

Métriques au niveau du quota de service Trusted Advisor

Vous pouvez utiliser les métriques suivantes pour les quotas Service AWS.

Métrique	Description
`ServiceLimitUsage`	Pourcentage d'utilisation des ressources par rapport à un quota de service (anciennement appelé limites).

Dimensions pour les métriques de niveau de vérification

Vous pouvez utiliser les dimensions suivantes pour les vérifications Trusted Advisor.

Dimension	Description
`CheckName`	Nom d'une vérification Trusted Advisor. Vous pouvez trouver tous les noms des vérifications dans la console Trusted Advisor ou la Référence de la vérification AWS Trusted Advisor.

Dimensions pour les métriques de niveau de catégorie

Vous pouvez utiliser la dimension suivante pour les catégories de vérification Trusted Advisor.

Dimension	Description
`Category`	Nom d'une catégorie de contrôle Trusted Advisor. Vous trouverez toutes les catégories de vérification dans la console Trusted Advisor ou la page Afficher les catégories de vérifications.

Dimensions pour les métriques de quotas de service

Vous pouvez utiliser les métriques suivantes pour les métriques de quotas de service Trusted Advisor.

Dimension	Description
`Region`	L'Région AWS d'un quota de service.
`ServiceName`	Le nom de l'Service AWS.
`ServiceLimit`	Le nom du quota de service. Pour de plus amples informations sur les quotas de service, veuillez consulter Quotas Service AWS dans le Références générales AWS.

Journalisation des actions de console AWS Trusted Advisor avec AWS CloudTrail

Trusted Advisorest intégré à AWS CloudTrail un service qui fournit un enregistrement des actions entreprises par un utilisateur, un rôle ou un AWS service dansTrusted Advisor. CloudTrail capture les actions Trusted Advisor sous forme d'événements. Les appels capturés incluent les appels réalisés à partir de la console Trusted Advisor. Si vous créez un suivi, vous pouvez activer la diffusion continue des CloudTrail événements vers un bucket Amazon Simple Storage Service (Amazon S3), y compris les événements pour. Trusted Advisor 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 faiteTrusted Advisor, 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.

Trusted Advisorinformations dans CloudTrail

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

Pour enregistrer en continu les événements dans votre compte AWS, y compris les événements d'Trusted Advisor, créez un journal d'activité. Un suivi permet CloudTrail de fournir des fichiers journaux à un compartiment Amazon S3. Par défaut, lorsque vous créez un journal de suivi dans la console, il s'applique à toutes les régions AWS. 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 :

- Présentation de la création d'un parcours
- 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

Trusted Advisorprend en charge la journalisation d'un sous-ensemble des actions de la Trusted Advisor console sous forme d'événements dans des fichiers CloudTrail journaux. CloudTrail enregistre les actions suivantes :

- `CreateEngagement`
- `CreateEngagementAttachment`
- `CreateEngagementCommunication`

- CreateExcelReport
- DescribeAccount
- DescribeAccountAccess
- DescribeCheckItems
- DescribeCheckRefreshStatuses
- DescribeCheckSummaries
- DescribeChecks
- DescribeNotificationPreferences
- DescribeOrganization
- DescribeOrganizationAccounts
- DescribeReports
- DescribeServiceMetadata
- ExcludeCheckItems
- GenerateReport
- GetEngagement
- GetEngagementAttachment
- GetEngagementType
- GetExcelReport
- GetOrganizationRecommendation
- GetRecommendation
- IncludeCheckItems
- ListAccountsForParent
- ListChecks
- ListEngagementCommunications
- ListEngagementTypes
- ListEngagements
- ListOrganizationRecommendationAccounts
- ListOrganizationRecommendationResources
- ListOrganizationRecommendations

- `ListOrganizationalUnitsForParent`
- `ListRecommendationResources`
- `ListRecommendations`
- `ListRoots`
- `RefreshCheck`
- `SetAccountAccess`
- `SetOrganizationAccess`
- `UpdateEngagement`
- `UpdateEngagementStatus`
- `UpdateNotificationPreferences`
- `UpdateOrganizationRecommendationLifecycle`
- `UpdateRecommendationLifecycle`

Pour obtenir la liste complète des actions de la console Trusted Advisor, consultez Trusted Advisor actions.

> **Note**
>
> CloudTrail enregistre également les opérations Trusted Advisor d'API dans la référence AWS Support d'API. Pour plus d'informations, veuillez consulter Journalisation des appels d'API AWS Support avec AWS CloudTrail.

Chaque événement ou entrée de journal contient des informations sur la personne ayant initié la demande. Les informations relatives à l'identité permettent de déterminer les éléments suivants :

- Si la demande a été effectuée avec les informations d'identification utilisateur racine ou AWS Identity and Access Management (IAM).
- Si la demande a été effectuée avec les informations d'identification de sécurité temporaires d'un rôle ou d'un utilisateur fédéré.
- Si la demande a été effectuée par un autre service AWS.

Pour plus d'informations, consultez l'élément CloudTrail UserIdentity.

Exemple : Entrées de fichier journal Trusted Advisor

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.

Example : entrée de journal pour RefreshCheck

L'exemple suivant montre une entrée de CloudTrail journal qui illustre l'`RefreshCheck`action à effectuer pour le contrôle de version des compartiments Amazon S3 (IDR365s2Qddf).


```
{
        "eventVersion":"1.04",
        "userIdentity":{
        "type":"IAMUser",
        "principalId":"AIDACKCEVSQ6C2EXAMPLE",
        "arn":"arn:aws:iam::123456789012:user/janedoe",
        "accountId":"123456789012",
        "accessKeyId":"AKIAIOSFODNN7EXAMPLE",
        "userName":"janedoe",
        "sessionContext":{
        "attributes":{
        "mfaAuthenticated":"false",
        "creationDate":"2020-10-21T22:06:18Z"
        }
        }
        },
        "eventTime":"2020-10-21T22:06:33Z",
        "eventSource":"trustedadvisor.amazonaws.com",
        "eventName":"RefreshCheck",
        "awsRegion":"us-east-1",
        "sourceIPAddress":"100.127.34.136",
        "userAgent":"signin.amazonaws.com",
        "requestParameters":{
        "checkId":"R365s2Qddf"
        },
        "responseElements":{
        "status":{
```

```
        "checkId":"R365s2Qddf",
        "status":"enqueued",
        "millisUntilNextRefreshable":3599993
        }
        },
        "requestID":"d23ec729-8995-494c-8054-dedeaEXAMPLE",
        "eventID":"a49d5202-560f-4a4e-b38a-02f1cEXAMPLE",
        "eventType":"AwsApiCall",
        "recipientAccountId":"123456789012"
        }
```


Example : entrée de journal pour UpdateNotificationPreferences

L'exemple suivant montre une entrée de CloudTrail journal illustrant l'`UpdateNotificationPreferences`action.


```
{
        "eventVersion":"1.04",
        "userIdentity":{
        "type":"IAMUser",
        "principalId":"AIDACKCEVSQ6C2EXAMPLE",
        "arn":"arn:aws:iam::123456789012:user/janedoe",
        "accountId":"123456789012",
        "accessKeyId":"AKIAIOSFODNN7EXAMPLE",
        "userName":"janedoe",
        "sessionContext":{
        "attributes":{
        "mfaAuthenticated":"false",
        "creationDate":"2020-10-21T22:06:18Z"
        }
        }
        },
        "eventTime":"2020-10-21T22:09:49Z",
        "eventSource":"trustedadvisor.amazonaws.com",
        "eventName":"UpdateNotificationPreferences",
        "awsRegion":"us-east-1",
        "sourceIPAddress":"100.127.34.167",
        "userAgent":"signin.amazonaws.com",
        "requestParameters":{
        "contacts":[
        {
        "id":"billing",
```

```
        "type":"email",
        "active":false
        },
        {
        "id":"operational",
        "type":"email",
        "active":false
        },
        {
        "id":"security",
        "type":"email",
        "active":false
        }
        ],
        "language":"en"
        },
        "responseElements":null,
        "requestID":"695295f3-c81c-486e-9404-fa148EXAMPLE",
        "eventID":"5f923d8c-d210-4037-bd32-997c6EXAMPLE",
        "eventType":"AwsApiCall",
        "recipientAccountId":"123456789012"
        }
```

Example : entrée de journal pour GenerateReport

L'exemple suivant montre une entrée de CloudTrail journal illustrant l'`GenerateReport`action. Cette action crée un rapport pour votre organisation AWS.

```
{
        "eventVersion":"1.04",
        "userIdentity":{
        "type":"IAMUser",
        "principalId":"AIDACKCEVSQ6C2EXAMPLE",
        "arn":"arn:aws:iam::123456789012:user/janedoe",
        "accountId":"123456789012",
        "accessKeyId":"AKIAIOSFODNN7EXAMPLE",
        "userName":"janedoe",
        "sessionContext":{
        "attributes":{
        "mfaAuthenticated":"false",
        "creationDate":"2020-11-03T13:03:10Z"
        }
```

```
        }
        },
        "eventTime":"2020-11-03T13:04:29Z",
        "eventSource":"trustedadvisor.amazonaws.com",
        "eventName":"GenerateReport",
        "awsRegion":"us-east-1",
        "sourceIPAddress":"100.127.36.171",
        "userAgent":"signin.amazonaws.com",
        "requestParameters":{
        "refresh":false,
        "includeSuppressedResources":false,
        "language":"en",
        "format":"JSON",
        "name":"organizational-view-report",
        "preference":{
        "accounts":[

        ],
        "organizationalUnitIds":[
        "r-j134"
        ],
        "preferenceName":"organizational-view-report",
        "format":"json",
        "language":"en"
        }
        },
        "responseElements":{
        "status":"ENQUEUED"
        },
        "requestID":"bb866dc1-60af-47fd-a660-21498EXAMPLE",
        "eventID":"2606c89d-c107-47bd-a7c6-ec92fEXAMPLE",
        "eventType":"AwsApiCall",
        "recipientAccountId":"123456789012"
        }
```

Ressources de dépannage

Pour consulter les réponses aux questions de dépannage courantes, consultez le Centre de connaissances AWS Support.

Pour Windows, Amazon EC2 propose EC2Rescue, que les clients peuvent utiliser pour examiner leurs instances Windows afin d'identifier les problèmes courants, de collecter des fichiers journaux et de résoudre AWS Support vos problèmes. Vous pouvez également utiliser EC2Rescue pour analyser les volumes de démarrage à partir d'instances non fonctionnelles. Pour plus d'informations, consultez How can I use EC2Rescue to troubleshoot and fix common issues on my EC2 Windows instance?

Résolution de problèmes spécifiques aux services

La plupart de Service AWS la documentation contient des rubriques de résolution des problèmes qui peuvent vous aider à démarrer avant de contacter AWS Support. Le tableau suivant fournit des liens vers les rubriques de dépannage, répertoriées par service.

> **Note**
>
> Le tableau suivant fournit une liste des services les plus courants. Pour rechercher d'autres rubriques de résolution des problèmes, utilisez la zone de texte de recherche sur la Page d'accueil de la documentation AWS (français non garanti).

Service	Lien
Amazon Web Services	Résolution des erreurs liées à la version 4 de AWS Signature
Amazon API Gateway	Résolution des problèmes liés aux API HTTP
Amazon AppStream	Résoudre les problèmes liés à Amazon AppStream
Amazon Athena	Résolution des problèmes dans Athena
Amazon Aurora MySQL	Dépannage d'Amazon Aurora
Amazon Aurora PostgreSQL	Dépannage d'Amazon Aurora

Service	Lien
Amazon EC2 Auto Scaling	Dépannage d'Auto Scaling
AWS Certificate Manager (ACM)	Dépannage
AWS CloudFormation	Résolutions des problèmes liés à AWS CloudFormation
Amazon CloudFront	Dépannage | Dépannage des distributions RTMP
AWS CloudHSM	Dépannage
Amazon CloudSearch	Résolution des problèmes liés à Amazon CloudSearch
AWS CodeDeploy	Résolutions des problèmes liés à AWS CodeDeploy
Amazon CloudWatch	Résolutions des problèmes liés à
AWS Database Migration Service	Résolution des problèmes de migration dans AWS Database Migration Service
AWS Data Pipeline	Dépannage
AWS Direct Connect	Résolutions des problèmes liés à AWS Direct Connect
AWS Directory Service	Résolution des problèmes AWS Directory Service d'administration
Amazon DynamoDB	Résolution des problèmes | Résolution des problèmes d'établissement de connexion SSL/TLS
AWS Elastic Beanstalk	Dépannage
Amazon Elastic Compute Cloud (Amazon EC2)	Résolution des problèmes liés aux instances | Dépannage des problèmes liés aux instances Windows | Résolution des problèmes liés à VM Import/Export | Résolution des erreurs liées aux demandes d'API | Dépannage d' AWS Management Pack | Dépannage d' AWS Systems Manager pour Microsoft SCVMM | AWS Diagnostics pour Microsoft Windows Server

Service	Lien
Amazon Elastic Container Service (Amazon ECS)	Dépannage d'Amazon ECS
Amazon Elastic Kubernetes Service (Amazon EKS)	Dépannage d'Amazon EKS
Elastic Load Balancing	Résolution des problèmes de vos Application Load Balancers | Dépanner votre Classic Load Balancer
Amazon ElastiCache pour Memcached	Applications de dépannage
Amazon ElastiCache pour Redis	Applications de dépannage
Amazon EMR	Résolution des problèmes liés à un cluster
AWS Flow Framework	Conseils pour le dépannage et le débogage
AWS Glue	Dépannage AWS Glue
AWS Glue DataBrew	Résolution des problèmes d'identité et d'accès dans AWS Glue DataBrew
AWS GovCloud (US)	Dépannage
AWS Identity and Access Management (JE SUIS)	Dépannage IAM
Amazon Keyspaces (pour Apache Cassandra)	Dépannage d'Amazon Keyspaces (pour Apache Cassandra)
Amazon Kinesis Data Streams	Dépannage des problèmes liés aux applications producteur Amazon Kinesis Data Streams | Dépannage des problèmes liés aux applications consommateur Amazon Kinesis Data Streams

Service	Lien
Service géré Amazon pour Apache Flink	Résolution des problèmes de performances | Résolution des problèmes liés au Service géré Amazon pour Apache Flink pour les applications SQL
Amazon Data Firehose	Résolution des problèmes liés à Amazon Data Firehose
AWS Lambda	AWS Lambda Fonctions de dépannage et de surveillance avec CloudWatch
Amazon OpenSearch Service	Résolution des problèmes liés à Amazon OpenSearch Service
AWS OpsWorks	Guide de débogage et dépannage
Amazon Personalize	Dépannage
Amazon QLDB	Dépannage d'Amazon MQ
Amazon QuickSight	Résolution des problèmes liés à Amazon QuickSight | Résolution des erreurs de ligne ignorées
AWS Resource Access Manager (AWS RAM)	Résolution des problèmes liés à AWS RAM
Amazon Redshift	Résolution des problèmes de requêtes | Résolution des problèmes de chargement de données | Résolution des problèmes de connexion dans Amazon Redshift | Résolution des problèmes de journalisation d'audit dans Amazon Redshift | Résolution des problèmes liés aux requêtes dans Amazon Redshift Spectrum
Amazon Relational Database Service (Amazon RDS)	Résolution des problèmes | Résolution des problèmes liés aux applications sur Amazon RDS | Résolution des problèmes de base de données pour Amazon RDS Custom
Amazon Route 53	Dépannage d'Amazon Route 53
Amazon SageMaker	Résoudre les erreurs | Résolution des problèmes liés à Amazon Studio SageMaker

Service	Lien
Amazon Silk	Dépannage
Amazon Simple Email Service (Amazon SES)	Dépannage d'Amazon SES
Amazon Simple Storage Service (Amazon S3)	Résolutions des problèmes
Amazon Simple Workflow Service (Amazon SWF)	AWS framework flow pour Java : conseils de dépannage et de débogage | Framework AWS flow pour Ruby : workflows de résolution des problèmes et de débogage
AWS Storage Gateway	Résolution des problèmes de passerelle
AWS Systems Manager	Dépannage de SSM Agent
Amazon Virtual Private Cloud (Amazon VPC)	Dépannage
AWS Virtual Private Network (AWS VPN)	Dépannage de votre périphérique de passerelle client
AWS WAF	Tester et ajuster vos AWS WAF protections
Amazon WorkMail	Résolution des problèmes liés à l'application WorkMail Web Amazon
Amazon WorkSpaces	Résolution des WorkSpaces problèmes liés à Amazon | Résolution des problèmes liés aux WorkSpaces clients Amazon

Historique du document

Le tableau suivant décrit les modifications importantes apportées à la documentation depuis la dernière version du AWS Support service.

- AWS Support Version de l'API : 2013-04-15
- AWS Support Version de l'API de l'application : 20/08/2021

Le tableau suivant décrit les mises à jour importantes apportées à la AWS Trusted Advisor documentation AWS Support et à compter du 10 mai 2021. Vous pouvez vous abonner à un flux RSS pour recevoir les notifications sur les mises à jour.

Modification	Description	Date
Documentation mise à jour sur la tolérance aux pannes et les contrôles de sécurité	Ajout d'un nouveau contrôle de tolérance aux pannes. 1 tolérance aux pannes et 1 contrôle de sécurité mis à jour. Pour plus d'informations, voir Journal des modifications pour les AWS Trusted Advisor vérifications.	29 mars 2024
Documentation mise à jour pour `AWSSupportServiceRolePolicy`	Ajout de nouvelles autorisations pour fournir des services de facturation, d'administration et de support pour le rôle lié à un service. Pour plus d'informations, consultez Politique gérée par AWS : AWSSupportServiceRolePolicy.	22 mars 2024
Documentation mise à jour pour le AWS Support plan	Mises à jour des fonctionnalités des AWS Support forfaits. Pour plus d'informa	11 mars 2024

	tions, consultez la section AWS Support Plans.	
Documentation mise à jour pour Trusted Advisor	Ajout d'une vérification de tolérance aux pannes. Pour plus d'informations, voir Journal des modifications pour les AWS Trusted Advisor vérifications.	29 février 2024
Documentation mise à jour pour Trusted Advisor	Ajout d'une vérification de tolérance aux pannes. Pour plus d'informations, voir Journal des modifications pour les AWS Trusted Advisor vérifications.	31 janvier 2024
Documentation mise à jour pour `AWSTrustedAdvisorServiceRolePolicy`	Ajout de nouvelles actions IAM`cloudtrail:GetTrail` ,`cloudtrail:ListTrails` , `cloudtrail:GetEventSelectors` `outposts:GetOutpost` , `outposts:ListAssets` et `outposts:ListOutposts` pour intégrer de nouvelles vérifications. Pour plus d'informations, consultez Politique gérée par AWS : AWSTrustedAdvisorServiceRolePolicy.	18 janvier 2024

Documentation mise à jour pour `AWSSupportServiceRolePolicy`	Ajout de nouvelles autorisations pour fournir des services de facturation, d'administration et de support pour le rôle lié à un service. Pour plus d'informations, consultez Politique gérée par AWS : AWSSupportServiceRolePolicy.	17 janvier 2024
Documentation mise à jour pour Trusted Advisor	Mise à jour d'une vérification de tolérance aux pannes pour modifier le titre et la description. Pour plus d'informations, voir Journal des modifications pour les AWS Trusted Advisor vérifications.	8 janvier 2024
Documentation mise à jour pour Trusted Advisor	Mise à jour d'un contrôle de sécurité pour tenir compte de la modification de la période de dépréciation. Pour plus d'informations, voir Journal des modifications pour les AWS Trusted Advisor vérifications.	21 décembre 2023
Documentation mise à jour pour Trusted Advisor	Ajout de 2 contrôles de sécurité et de 2 contrôles de performance. Pour plus d'informations, voir Journal des modifications pour les AWS Trusted Advisor vérifications.	20 décembre 2023

Documentation mise à jour pour Trusted Advisor	Ajout d'un contrôle de sécurité. Pour plus d'informations, voir Journal des modifications pour les AWS Trusted Advisor vérifications.	15 décembre 2023
Documentation mise à jour pour Trusted Advisor Engage	Documentation Trusted Advisor Engage mise à jour avec modification de l'option de notification par e-mail.	14 décembre 2023
Documentation mise à jour pour Trusted Advisor Engage	Documentation Trusted Advisor Engage mise à jour avec les modifications apportées aux engagements planifiés.	11 décembre 2023
Documentation mise à jour pour Trusted Advisor	Ajout de 2 nouveaux contrôles de tolérance aux pannes et d'un contrôle d'optimisation des coûts. Pour plus d'informations, voir Journal des modifications pour les AWS Trusted Advisor vérifications.	7 décembre 2023
Documentation mise à jour pour `AWSSupportServiceRolePolicy`	Ajout de nouvelles autorisations pour fournir des services de facturation, d'administration et de support pour le rôle lié à un service. Pour plus d'informations, consultez Politique gérée par AWS : AWSSupportServiceRolePolicy.	6 décembre 2023

Politiques AWS gérées mises à jour pour Trusted Advisor	A mis à jour les politiques `AWSTrustedAdvisorPriorityFullAccess` et les politiques `AWSTrustedAdvisorPriorityReadOnlyAccess` AWS gérées pour inclure les identifiants des relevés. Pour plus d'informations, consultez Politiques gérées par AWS pour AWS Trusted Advisor.	6 décembre 2023
Documentation mise à jour pour Trusted Advisor	Ajout de 3 nouveaux contrôles de tolérance aux pannes. Pour plus d'informations, voir Journal des modifications pour les AWS Trusted Advisor vérifications.	17 novembre 2023
Documentation mise à jour pour Trusted Advisor	37 nouveaux chèques ont été ajoutés pour Amazon RDS. Pour plus d'informations, voir Journal des modifications pour les AWS Trusted Advisor vérifications.	15 novembre 2023

Documentation mise à jour pour `AWSTrustedAdvisorServiceRolePolicy`	Ajout de nouvelles actions `ec2:DescribeRegions` IAM `s3:GetLifecycleConfiguration` `ecs:DescribeTaskDefinition` et intégration `ecs:ListTaskDefinitions` de nouvelles vérifications. Pour plus d'informations, consultez Politique gérée par AWS : AWSTrustedAdvisorServiceRolePolicy.	9 novembre 2023
Documentation mise à jour pour `AWSSupportServiceRolePolicy`	Ajout de nouvelles autorisations pour fournir des services de facturation, d'administration et de support pour le rôle lié à un service. Pour plus d'informations, consultez Politique gérée par AWS : AWSSupportServiceRolePolicy.	27 octobre 2023
Documentation mise à jour pour Trusted Advisor	Ajout de 64 nouveaux chèques intégrés depuis AWS Config. Pour plus d'informations, consultez la section Journal des modifications pour les AWS Trusted Advisor vérifications.	26 octobre 2023
Documentation mise à jour pour Trusted Advisor	Ajout de six nouveaux contrôles de tolérance aux pannes Trusted Advisor. Pour plus d'informations, consultez le journal des modifications pour les AWS Trusted Advisor vérifications.	12 octobre 2023

Documentation mise à jour pour `AWSTrustedAdvisorServiceRolePolicy`	Ajout des actions IAM `route53resolver:ListResolverEndpoints` , `route53resolver:ListResolverEndpointIpAddresses` , `ec2:DescribeSubnets` , `kafka:ListClustersV2` et `kafka:ListNodes` pour intégrer de nouveaux contrôles de résilience. Pour plus d'informations, consultez Politique gérée par AWS : AWSTrustedAdvisorServiceRolePolicy.	14 septembre 2023
Documentation mise à jour pour `AWSSupportServiceRolePolicy`	Ajout de nouvelles autorisations pour fournir des services de facturation, d'administration et de support pour le rôle lié à un service. Pour plus d'informations, consultez Politique gérée par AWS : AWSSupportServiceRolePolicy.	28 août 2023
Documentation mise à jour pour Trusted Advisor	Ajout d'une nouvelle vérification des limites de service pour Lambda. Pour plus d'informations, consultez le journal des modifications pour les AWS Trusted Advisor vérifications.	17 août 2023

Documentation mise à jour pour Trusted Advisor	Ajout d'une nouvelle vérification de tolérance aux pannes pour Lambda. Pour plus d'informations, consultez le journal des modifications pour les AWS Trusted Advisor vérifications.	3 août 2023
Documentation mise à jour pour Trusted Advisor Engage	Mise à jour de la documentation Trusted Advisor Engage pour tenir compte des modifications apportées aux formulaires de création et de modification d'engagement. Ajout d'une page avec des exemples de politiques de contrôle des services pour AWS Trusted Advisor.	27 juillet 2023
Documentation mise à jour pour `AWSSupportServiceRolePolicy`	Ajout de nouvelles autorisations pour fournir des services de facturation, d'administration et de support pour le rôle lié à un service. Pour plus d'informations, consultez Politique gérée par AWS : AWSSupportServiceRolePolicy.	26 juin 2023

Documentation mise à jour pour Trusted Advisor	Ajout de deux nouvelles vérifications de tolérance aux pannes pour Amazon MQ. Ajout d'une nouvelle vérificat ion de tolérance aux pannes et d'une nouvelle vérification des performances pour Amazon Elastic File System. Pour plus d'informations, consultez le journal des modifications pour les AWS Trusted Advisor vérifications.	1er juin 2023
Documentation mise à jour pour Trusted Advisor	Ajout de deux nouvelles vérifications de tolérance aux pannes pour la passerell e NAT. Pour plus d'informa tions, consultez le journal des modifications pour les AWS Trusted Advisor vérifications.	16 mai 2023
Documentation mise à jour pour les AWS Support plans	Ajout d'une nouvelle autorisat ion et d'une nouvelle CloudTrai l documentation pour la création de calendriers de plans de support. Pour plus d'informations, consultez Gérer l'accès aux AWS Support plans, politiques AWS gérées pour les AWS Support plans et Journalisation AWS Support des appels d'API des plans avec AWS CloudTrail.	8 mai 2023

Documentation mise à jour pour `AWSSupportServiceRolePolicy`	Ajout de nouvelles autorisations pour fournir des services de facturation, d'administration et de support pour le rôle lié à un service. Pour plus d'informations, consultez Politique gérée par AWS : AWSSupportServiceRolePolicy.	2 mai 2023
Documentation mise à jour pour Trusted Advisor Engage et Trusted Advisor Priority	Prérequis clarifiés pour Trusted Advisor Engagement et Trusted Advisor Priority. Ajout d'un exemple de politique IAM avec la possibilité d'utiliser Trusted Advisor Engage et d'activer l'accès sécurisé à Trusted Advisor.	28 avril 2023
Documentation mise à jour pour Trusted Advisor	Ajout de deux nouveaux contrôles de tolérance aux pannes pour AWS Resilience Hub Incident Manager. Pour plus d'informations, consultez le journal des modifications pour les AWS Trusted Advisor vérifications.	27 avril 2023

Documentation ajoutée pour Trusted Advisor Engage	Vous pouvez utiliser AWS Trusted Advisor Engage pour tirer le meilleur parti de vos AWS Support plans en vous permettant de consulter, de demander et de suivre facilement tous vos engagements proactifs, et de communiquer avec votre Compte AWS équipe au sujet des engagements en cours. Pour plus d'informations, voir Démarrer avec AWS Trusted Advisor Engage.	6 avril 2023
Documentation mise à jour pour Trusted Advisor	Ajout de deux nouvelles vérifications de tolérance aux pannes pour Amazon ECS. Pour plus d'informations, consultez le journal des modifications pour les AWS Trusted Advisor vérifications.	30 mars 2023
Documentation mise à jour pour `AWSSupportServiceRolePolicy`	Ajout de nouvelles autorisations pour fournir des services de facturation, d'administration et de support pour le rôle lié à un service. Pour plus d'informations, consultez Politique gérée par AWS : AWSSupportServiceRolePolicy.	16 mars 2023

Documentation ajoutée pour Trusted Advisor Priority	Mise à jour de la console Trusted Advisor Priority : • Les boutons Accuser réception et Ignorer ont remplacé les boutons Accepter et Rejeter. • Vous n'avez pas besoin de saisir le titre ou le nom de votre poste pour accuser réception, résoudre, rejeter ou rouvrir des recommand ations. Pour plus d'informations, voir Commencer avec Trusted Advisor Priority.	16 février 2023
Exemples de code mis à jour pour AWS Support	Ajout d'exemples de code .NET, Java et Kotlin qui montrent comment utiliser AWS Support un kit de développement AWS logiciel (SDK). Pour plus d'informa tions, consultez la section Exemples de code pour AWS Support l'utilisation AWS des SDK.	16 janvier 2023

Documentation mise à jour pour `AWSSupportServiceRolePolicy`	Ajout de nouvelles autorisations pour fournir des services de facturation, d'administration et de support pour le rôle lié à un service. Pour plus d'informations, consultez Politique gérée par AWS : AWSSupportServiceRolePolicy.	10 janvier 2023
Documentation mise à jour pour AWS Support l'application	Vous pouvez rechercher des cas de support dans Slack en utilisant les options de filtre ou en recherchant par ID de dossier. Pour plus d'informations, consultez Recherche de cas de support dans Slack.	29 décembre 2022
Documentation mise à jour pour AWS Support l'application	Vous pouvez également utiliser Terraform pour créer vos ressources pour l' AWS Support application. Pour plus d'informations, consultez Créer des ressources d' AWS Support applications à l'aide de Terraform.	22 décembre 2022
Documentation mise à jour pour Trusted Advisor	Ajout de trois nouveaux contrôles de tolérance aux pannes pour Amazon MemoryDB ElastiCache, Amazon et. AWS CloudHSM Pour plus d'informations, consultez le journal des modifications pour les AWS Trusted Advisor vérifications.	15 décembre 2022

Documentation mise à jour pour l' AWS Support application dans Slack	Vous pouvez désormais demander une assistance par chat en direct pour les options suivantes : • Cas de support pour le compte et la facturation. • Support en japonais pour les cas de support technique. • Pour plus d'informations, consultez Création de cas de support dans un canal Slack.	14 décembre 2022
Documentation mise à jour pour AWS Support	Ajout de documentation sur les nouveaux points de terminaison pour l' AWS Support API. Pour plus d'informations sur l'API , consultez À propos de l'API AWS Support.	14 décembre 2022
Ajout de documentation pour les AWS CloudFormation modèles à utiliser pour l' AWS Support application dans Slack	Vous pouvez utiliser des CloudFormation modèles pour créer des espaces de travail et des canaux de configuration Slack à Comptes AWS utiliser. AWS Organizations Pour plus d'informations, consultez la section Création de ressources d' AWS Support applications avec AWS CloudFormation.	5 décembre 2022

Documentation mise à jour pour Trusted Advisor	Ajout de deux nouveaux contrôles de tolérance aux pannes pour AWS Resilienc e Hub. Pour plus d'informa tions, consultez le journal des modifications pour les AWS Trusted Advisor vérifications.	17 novembre 2022
Documentation ajoutée pour vos AWS Security Hub découvertes dans Trusted Advisor	Les résultats que vous avez obtenus grâce aux contrôles du Security Hub sont supprimés Trusted Advisor plus rapidement. Pour plus d'informations, consultez le journal des modifications pour les AWS Trusted Advisor vérifications.	17 novembre 2022
Documentation mise à jour pour AWS Trusted Advisor	Documentation ajoutée pour les Trusted Advisor recommandations. Pour plus d'informations, consultez le journal des modifications pour les AWS Trusted Advisor vérifications.	16 novembre 2022
Documentation mise à jour pour l' AWS Support applicati on dans Slack	Prise en charge ajoutée du japonais pour la documenta tion. Pour plus d'informations, consultez Création de cas de support dans un canal Slack.	11 novembre 2022

Documentation mise à jour pour les AWS Support plans	Ajout d'informations de dépannage pour autoriser l'accès de Support Plans au sein d'une organisation. Pour plus d'informations, consultez Dépannage.	9 novembre 2022
Documentation mise à jour pour l' AWS Support application dans Slack	Ajout de la documentation pour les autorisations `supportapp` . Pour plus d'informations, consultez la section Autorisations requises pour que l' AWS Support application se connecte à Slack.	1er novembre 2022
Documentation mise à jour pour l' AWS Support application dans Slack	Vous pouvez utiliser l'opération API `RegisterSlackWorkspaceForOrganization` pour enregistrer un espace de travail Slack pour votre Compte AWS. Pour appeler cette API, votre compte doit faire partie d'une organisation dans AWS Organizations. Pour plus d'informations, consultez l'AWS Support application dans la Référence API Slack.	19 octobre 2022

Documentation mise à jour pour `AWSSupportServiceRolePolicy`	Ajout de nouvelles autorisations pour fournir des services de facturation, d'administration et de support pour le rôle lié à un service. Pour plus d'informations, consultez Politique gérée par AWS : AWSSupportServiceRolePolicy.	4 octobre 2022
Documentation mise à jour pour Support Plans	Vous pouvez désormais utiliser AWS Identity and Access Management (IAM) pour gérer les autorisations permettant de modifier le plan de support de votre Compte AWS. Pour plus d'informations, consultez les rubriques suivantes : • Gestion de l'accès aux AWS Support plans • AWS politiques gérées pour les AWS Support plans • Modifier les AWS Support plans • Appels AWS Support d'API Logging Plans avec AWS CloudTrail	29 septembre 2022

Documentation mise à jour pour l' AWS Support application dans Slack	Ajout de documentation sur la façon de configure r une chaîne publique ou privée à utiliser avec l' AWS Support application. Pour plus d'informations, consultez Configuring a Slack channel (Configuration d'un canal Slack).	22 septembre 2022
Documentation mise à jour pour AWS Support	Ajout d'une nouvelle section sur la sécurité de vos cas de support. Pour plus d'informa tions, consultez la section Sécurité de vos AWS Support dossiers.	9 septembre 2022
Documentation mise à jour pour Trusted Advisor	Ajout d'un nouveau contrôle de sécurité pour Amazon EC2. Pour plus d'informa tions, consultez le journal des modifications pour les AWS Trusted Advisor vérifications.	1er septembre 2022

Documentation mise à jour pour l' AWS Support application dans Slack	Consultez les rubriques suivantes : Vous pouvez utiliser l' AWS Support application pour gérer vos demandes d'assistance, demander des augmentations de quotas de service et discuter avec des agents d'assistance directement sur vos canaux Slack. Pour plus d'informations, consultez la documentation sur l'application AWS Support dans Slack. Vous pouvez associer des politiques AWS gérées à vos rôles IAM pour utiliser l' AWS Support application. Pour plus d'informations, consultez la section Politiques AWS gérées pour les AWS Support applications dans Slack. Nouvelle référence d'API pour l' AWS Support application. Consultez la Référence d'API de l'application AWS Support.	24 août 2022
Documentation mise à jour pour `AWSSupportServiceRolePolicy`	Ajout de nouvelles autorisations pour fournir des services de facturation, d'administration et de support pour le rôle lié à un service. Pour plus d'informations, consultez Politique gérée par AWS : AWSSupportServiceRolePolicy.	17 août 2022

Documentation ajoutée pour Trusted Advisor Priority	Trusted Advisor Priority ajoute la prise en charge des fonctionnalités suivantes : • Administrateurs délégués • Notifications par e-mail quotidiennes et hebdomadaires pour les résumés des recommandations • Réouverture des recommandations résolues ou rejetées • AWS politiques gérées Pour plus d'informations, voir Commencer avec Trusted Advisor Priority.	17 août 2022
Documentation mise à jour pour Trusted Advisor	La page des préférences de la Trusted Advisor console a été mise à jour. Pour plus d'informations, consultez la section Mise en route avec AWS Trusted Advisor.	15 juillet 2022

Documentation mise à jour pour Trusted Advisor	Mise à jour des vérifications pour inclure les informations suivantes : • Critères d'alerte • Action recommandée • Ressources supplémentaires • Colonnes du rapport Pour plus d'informations, consultez la Référence des vérifications de AWS Trusted Advisor.	7 juillet 2022
Documentation mise à jour pour AWS Support	Ajout de documentation qui explique comment gérer vos cas de support. • Mise à jour d'un cas de support existant • Dépannage	28 juin 2022
Documentation mise à jour pour `AWSSupportServiceRolePolicy`	Ajout d'autorisations pour fournir des services de facturation, d'administration et de support pour le rôle lié à un service. Pour plus d'informations, consultez Politique gérée par AWS : AWSSupportServiceRolePolicy.	23 juin 2022

Documentation mise à jour pour Trusted Advisor	Trusted Advisor prend en charge des contrôles standard de sécurité supplémentaires issus des meilleures pratiques de sécurité AWS fondamentales provenant de AWS Security Hub. Pour plus d'informations, consultez le journal des modifications pour les AWS Trusted Advisor vérifications.	23 juin 2022
Documentation mise à jour pour Trusted Advisor	Ajout d'informations sur la demande d'augmentations de quotas de service. Pour plus d'informations, veuillez consulter Service Limits.	21 juin 2022
Documentation mise à jour pour AWS Support	L'expérience de création de cas a été mise à jour dans la console du Centre de support. Pour de plus amples informations, veuillez consulter Création de cas de support et de gestion de cas.	18 mai 2022
Documentation mise à jour pour Trusted Advisor	Ajout de quatre vérifications pour Amazon EBS et AWS Lambda. Pour plus d'informations, consultez la section S'inscrire AWS Compute Optimizer pour ajouter Trusted Advisor des chèques.	4 mai 2022

Documentation mise à jour pour `AWSSupportServiceRolePolicy`	Ajout de nouvelles autorisations pour fournir des services de facturation, d'administration et de support pour le rôle lié à un service. Pour plus d'informations, consultez Politique gérée par AWS : AWSSupportServiceRolePolicy.	27 avril 2022
Documentation mise à jour pour la vérification des clés d'accès exposées	Cette vérification est désormais automatiquement actualisée pour vous. Pour plus d'informations, consultez la section Journal des modifications pour les AWS Trusted Advisor vérifications.	25 avril 2022
Documentation mise à jour pour Trusted Advisor	Les AWS Direct Connect contrôles de la catégorie de tolérance aux pannes sont mis à jour. Pour plus d'informations, consultez la section Journal des modifications pour les AWS Trusted Advisor vérifications.	29 mars 2022
Documentation mise à jour pour `AWSSupportServiceRolePolicy`	Ajout de nouvelles autorisations pour fournir des services de facturation, d'administration et de support pour le rôle lié à un service. Pour plus d'informations, consultez Politique gérée par AWS : AWSSupportServiceRolePolicy.	14 mars 2022

Documentation ajoutée pour Trusted Advisor Priority	Vous pouvez utiliser Trusted Advisor Priority pour consulter la liste des recommandations prioritaires de votre responsable de compte technique (TAM). Pour plus d'informations, voir Commencer avec Trusted Advisor Priority.	28 février 2022
Documentation mise à jour pour l'utilisation d'Amazon EventBridge pour Trusted Advisor	Vous pouvez créer une EventBridge règle pour surveiller les modifications apportées à vos Trusted Advisor chèques. Pour plus d'informations, consultez la section Surveillance des AWS Trusted Advisor résultats de contrôle avec EventBridge.	21 février 2022
Nouvelle documentation sur l'utilisation d'Amazon EventBridge pour le suivi AWS Support des cas	Vous pouvez créer une EventBridge règle pour surveiller et recevoir des notifications concernant vos demandes d'assistance. Pour plus d'informations, consultez la section Surveillance AWS Support des cas avec EventBridge.	21 février 2022
Documentation mise à jour pour `AWSSupportServiceRolePolicy`	Ajout de nouvelles autorisations pour fournir des services de facturation, d'administration et de support pour le rôle lié à un service. Pour plus d'informations, consultez Politique gérée par AWS : AWSSupportServiceRolePolicy.	17 février 2022

Documentation ajoutée pour l'intégration avec AWS Security Hub	Dans la Trusted Advisor console, vous pouvez désormais consulter les résultats relatifs aux contrôles de votre Security Hub qui font partie de la norme de sécurité AWS Foundational Security Best Practices. Pour plus d'informations, consultez la section Affichage AWS Security Hub des commandes dans la AWS Trusted Advisor console.	18 janvier 2022
Documentation mise à jour pour Trusted Advisor	Trois nouvelles vérifications ont été ajoutées pour les instances Amazon EC2 qui exécutent Microsoft SQL Server. • Consolidation des instances Amazon EC2 pour Microsoft SQL Server • Instances Amazon EC2 trop approvisionnées pour Microsoft SQL Server • Instances Amazon EC2 avec fin de support de Microsoft SQL Server Pour plus d'informations, consultez la Référence des vérifications de AWS Trusted Advisor.	20 décembre 2021

Documentation mise à jour pour Trusted Advisor	Trusted Advisor a ajouté quatre nouvelles vérifications pour AWS Well-Architected • AWS Well-ArchitectedPr oblèmes à risque élevé pour l'optimisation des coûts • Problèmes à risque élevé AWS Well-Architected pour la performance • Problèmes à risque élevé AWS Well-Architected pour la sécurité • Problèmes à risque élevé AWS Well-Architected pour la fiabilité Pour plus d'informations, consultez la Référence des vérifications de AWS Trusted Advisor.	20 décembre 2021
Documentation mise à jour	Si vous avez un plan Enterprise On-Ramp Support, vous avez accès à tous les Trusted Advisor contrôles et à l' AWS Support API.	24 novembre 2021
Documentation mise à jour pour Trusted Advisor	Trusted Advisor a ajouté deux nouveaux chèques pour Amazon Comprehend. Pour plus d'informations, consultez la Référence des vérifications AWS Trusted Advisor.	29 septembre 2021

Documentation mise à jour pour Trusted Advisor	Le nom de la vérification pour Amazon OpenSearch Service Reserved Instance Optimization a été mis à jour. Pour plus d'informations, consultez la section Journal des modifications pour les AWS Trusted Advisor vérifications.	8 septembre 2021
Documentation mise à jour pour les Trusted Advisor contrôles	Ajout d'une rubrique de référence pour tous les Trusted Advisor contrôles. Pour plus d'informations, consultez Référence des vérifications AWS Trusted Advisor.	1er septembre 2021
Documentation mise à jour pour les politiques Trusted Advisor gérées	Documentation mise à jour pour les politiques Trusted Advisor gérées. Pour plus d'informations, consultez les politiques AWS gérées pour AWS Support et AWS Trusted Advisor.	10 août 2021
Documentation mise à jour pour Trusted Advisor	Documentation mise à jour pour la Trusted Advisor console. Pour plus d'informations, voir Commencer avec AWS Trusted Advisor.	16 juillet 2021

Documentation mise à jour pour la création de AWS Support dossiers	Ajout de documentation sur la création d'un cas de support connexe pour les cas définitivement fermés. Pour de plus amples informations, veuillez consulter Réouverture d'un cas clos et Création d'un cas connexe.	8 juin 2021
Documentation mise à jour pour Trusted Advisor	Trusted Advisor a ajouté deux nouveaux contrôles pour le stockage en volume d'Amazon Elastic Block Store (Amazon EBS). Pour plus d'informations, consultez la section Journal des modifications pour les AWS Trusted Advisor vérifications.	8 juin 2021
Documentation mise à jour	Les rubriques suivantes ont été mises à jour : • Procédures mises à jour et ajout de contenu à la rubrique Création d' CloudWatch alarmes Amazon pour surveiller AWS Trusted Advisor les métriques • Ajout de la section Quotas de service pour l' AWS Support API	12 mai 2021

Mises à jour antérieures

Modification	Description	Date
Documentation mise à jour pour Trusted Advisor	Ajout de la documentation pour filtrer, actualiser et télécharger les résultats de vérification. Pour plus d'informations, consultez les sections suivantes : • Filtrer vos vérifications • Actualiser les résultats de vérifications • Télécharger les résultats des vérifications	16 mars 2021
Documentation mise à jour sur les politiques AWS gérées	Ajout d'informations sur la politique `AWSSupportServiceRolePolicy` AWS gérée. Pour plus d'informations, consultez Utilisation des rôles liés aux services pour AWS Support.	16 mars 2021
Contrôles ajoutés pour AWS Lambda	Quatre AWS Trusted Advisor vérifications pour Lambda ont été ajoutées dans le. Journal des modifications pour AWS Trusted Advisor	8 mars 2021
Vérifications des limites de service mises à jour pour Amazon Elastic Block Store	Cinq AWS Trusted Advisor chèques pour Amazon EBS ont été mis à jour dans leJournal des modifications pour AWS Trusted Advisor.	5 mars 2021
Documentation mise à jour pour la CloudTrail journalisation	CloudTrail prend en charge la journalisation des actions de console lorsque vous modifiez votre AWS Support plan. Pour plus d'informations, consultez Journalisation des modifications apportées à votre plan AWS Support.	9 février 2021
Documentation mise à jour pour Trusted Advisor	Mise à jour de la rubrique Démarrer avec Trusted Advisor Recommendations.	29 janvier 2021

Modification	Description	Date
Documentation mise à jour pour les Trusted Advisor rapports	Ajout d'une Résolution des problèmes section pour l'utilisation Trusted Advisor des rapports avec d'autres AWS services.	4 décembre 2020
Ajout du AWS Trusted Advisor support pour la AWS CloudTrail journalisation	CloudTrail prend en charge la journalisation d'un sous-ensemble d'actions de Trusted Advisor console. Pour plus d'informations, consultez Journalisation des actions de console AWS Trusted Advisor avec AWS CloudTrail.	23 novembre 2020
Ajout d'une rubrique du journal des modifications	Consultez les modifications apportées aux AWS Trusted Advisor contrôles et aux catégories dans leJournal des modifications pour AWS Trusted Advisor.	18 novembre 2020
Ajout de support pour les unités organisat ionnelles	Vous pouvez désormais créer des rapports pour les Trusted Advisor vérifications des unités organisationnelles (UO). Pour plus d'informations, consultez Créer des rapports de vue organisationnelle.	17 novembre 2020
Mise à jour de la journalisation avec AWS CloudTrail le sujet	Ajout d'un exemple d'entrée de journal pour une opération d' Trusted Advisor API. veuillez consulter Informations AWS Trusted Advisor dans la consignation CloudTrail.	22 octobre 2020
AWS Support Quotas ajoutés	Ajout d'informations sur les quotas et restricti ons actuels pour AWS Support. Consultez les points de terminaison et les quotas AWS Support dans la Références générales AWS.	4 août 2020
Vue organisationnelle pour AWS Trusted Advisor	Vous pouvez désormais créer des rapports pour Trusted Advisor les chèques des comptes qui en font partie AWS Organizations. veuillez consulter Vue organisationnelle pour AWS Trusted Advisor.	17 juillet 2020

Modification	Description	Date
Sécurité et AWS Support	Actualisation des informations sur les aspects liés à la sécurité lors de l'utilisation de AWS Support et Trusted Advisor. Consultez Sécurité dans AWS Support	5 mai 2020
Sécurité et AWS Support	Ajout d'informations sur les considérations de sécurité lors de l'utilisation d' AWS Support.	10 janvier 2020
Utilisation en Trusted Advisor tant que service Web	Ajout d'instructions mises à jour pour actualise r Trusted Advisor les données après avoir obtenu la liste des Trusted Advisor vérifications.	1 novembre 2018
Utilisation des rôles liés à un service	Nouvelle section ajoutée.	11 juillet 2018
Mise en route : Résolution des problèmes	Ajout de liens relatifs à la résolution des problèmes pour Route 53 et AWS Certificate Manager.	1 septembre 2017
Exemple de gestion d'une demande de support : Création d'une demande de support	Ajout d'une remarque relative à la zone CC pour les utilisateurs ayant souscrit à un plan de support Basic.	1 août 2017
Surveillance des résultats des Trusted Advisor contrôles à l'aide d' CloudWatch événements	Nouvelle section ajoutée.	le 18 novembre 2016
Gestion des demandes	Noms des niveaux de gravité des demandes mis à jour.	27 octobre 2016
Enregistrement AWS Support des appels avec AWS CloudTrail	Nouvelle section ajoutée.	21 avril 2016

Modification	Description	Date
Mise en route : Résolution des problèmes	Ajout de liens supplémentaires vers des rubriques de dépannage.	19 mai 2015
Mise en route : Résolution des problèmes	Ajout de liens supplémentaires vers des rubriques de dépannage.	18 novembre 2014
Mise en route : Gestion des demandes de support	Mis à jour pour refléter le Service Catalog dans le AWS Management Console.	30 octobre 2014
Programmation de la durée de vie d'une AWS Support affaire	Ajout d'informations sur les nouveaux éléments d'API pour l'ajout de pièces jointes à des demandes de support et l'omission des communications relatives aux demandes lors de la récupération de l'historique des demandes.	16 juillet 2014
Accès AWS Support	Suppression des contacts de support nommés comme méthode d'accès.	28 mai 2014
Démarrage	Ajout de la section Mise en route.	13 décembre 2013
Publication initiale	Nouveau AWS Support service publié.	30 avril 2013

Glossaire AWS

Pour connaître la terminologie la plus récente d'AWS, consultez le Glossaire AWS dans la Référence Glossaire AWS.

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.