aws

Guide de l’utilisateur

Le DevOps gourou d'Amazon

Copyright © 2026 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

Le DevOps gourou d'Amazon: Guide de l’utilisateur

Copyright © 2026 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

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

Table of Contents

Qu'est-ce qu'Amazon DevOps Guru ? ... 1
Comment fonctionne DevOps Guru ? ... 1
Flux de travail DevOps Guru de haut niveau ... 2
Flux de travail détaillé de DevOps Guru ... 4
Comment puis-je commencer ? ... 5
Comment puis-je arrêter de payer des frais DevOps Guru ? ... 5
Concepts ... 6
Anomalie ... 6
Informations ... 6
Métriques et événements opérationnels ... 7
Groupes de journaux et anomalies du journal ... 7
Recommandations ... 8
Couverture ... 8
Liste de couverture des services ... 10
Configuration ... 12
Inscrivez-vous pour AWS ... 12
Inscrivez-vous pour Compte AWS ... 12
Déterminer la couverture pour DevOps Guru ... 13
Identifiez le sujet de vos notifications ... 14
Autorisations ajoutées à votre sujet ... 14
Estimation de vos coûts ... 16
Prise en main ... 19
Étape 1 : Configuration ... 19
Étape 2 : Activez DevOps Guru ... 19
Surveillez les comptes au sein de votre organisation ... 19
Surveillez votre compte courant ... 21
Étape 3 : Spécifiez la couverture de vos ressources DevOps Guru ... 22
AWS Services habilitants pour l'analyse DevOps Guru ... 25
Travailler avec des informations ... 26
Visualisation des informations ... 26
Comprendre les informations contenues dans la console DevOps Guru ... 28
Comprendre comment les comportements anormaux sont regroupés en informations ... 31
Comprendre la sévérité des informations ... 31
Surveillance des bases de données ... 33

Bases de données relationnelles 33
Surveillance des opérations de base de données dans Amazon RDS 33
Surveillance des opérations de base de données dans Amazon Redshift 36
Gestion des anomalies dans DevOps Guru for RDS 37
Bases de données non relationnelles 58
Surveillance des opérations de base de données dans Amazon DynamoDB 59
Surveillance des opérations de base de données dans Amazon ElastiCache 59
Intégration avec CodeGuru Profiler 61
Définition des applications à l'aide de AWS ressources 62
Utiliser des balises pour identifier les ressources de vos applications 63
Qu'est-ce qu'un tag ? 64
Définition d'une application à l'aide d'une balise 64
Utiliser des tags avec DevOps Guru 65
Ajout de balises à des ressources 66
Utiliser des piles pour identifier les ressources dans vos applications DevOps Guru 67
Choisir les piles à analyser 68
Travailler avec EventBridge 70
Événements pour DevOps Guru 70
DevOps Événement ouvert Guru New Insight 70
Exemple de modèle d'événement personnalisé pour une gravité élevée | new Insight 72
Mise à jour des paramètres 73
Mettre à jour votre compte de gestion 73
Mise à jour de votre couverture AWS d'analyse 73
Mettre à jour vos notifications 74
Accédez aux paramètres de notification dans la console DevOps Guru 75
Ajouter des sujets de notification Amazon SNS 75
Supprimer les sujets de notification Amazon SNS 76
Mise à jour des configurations de notification Amazon SNS 76
Autorisations ajoutées à votre sujet 77
Filtrer vos notifications 78
Filtrer les notifications à l'aide d'une politique de filtrage des abonnements Amazon SNS 78
Exemple de notification Amazon SNS filtrée 79
Mettre à jour l'intégration de Systems Manager 80
Mise à jour de la détection des anomalies dans le journal 81
Mettre à jour le chiffrement 81
Affichage des notifications 83

Nouveau point de vue ... 83
Aperçu fermé ... 84
Nouvelle association ... 86
Nouvelle recommandation ... 87
Sévérité améliorée ... 88
Échec de validation des ressources ... 89
Afficher les ressources analysées ... 91
Mise à jour de votre couverture AWS d'analyse ... 91
Suppression de la vue des ressources analysées pour les utilisateurs ... 93
Bonnes pratiques ... 95
Sécurité ... 96
Protection des données ... 97
Chiffrement des données ... 98
Comment DevOps Guru utilise les subventions dans AWS KMS ... 99
Surveillance de vos clés de chiffrement dans DevOps Guru ... 100
Création d'une clé gérée par le client ... 100
Confidentialité du trafic ... 102
Gestion de l'identité et des accès ... 102
Public ciblé ... 103
Authentification par des identités ... 103
Gestion de l'accès à l'aide de politiques ... 105
Mises à jour des politiques ... 107
Comment Amazon DevOps Guru fonctionne avec IAM ... 112
Identity-based politiques ... 118
Utilisation des rôles liés à un service ... 129
DevOpsRéférence des autorisations Guru ... 135
Autorisations pour les rubriques Amazon SNS ... 140
Autorisations pour les rubriques Amazon SNS cryptées ... 144
Résolution des problèmes ... 144
DevOpsGourou de la surveillance ... 149
Surveillance avec CloudWatch ... 149
Enregistrement des appels d'API DevOps Guru avec AWS CloudTrail ... 152
Points de terminaison de VPC (AWS PrivateLink) ... 155
Considérations relatives aux points de DevOps terminaison Guru VPC ... 156
Création d'un point de terminaison VPC d'interface pour Guru DevOps ... 156
Création d'une politique de point de terminaison VPC pour Guru DevOps ... 156

Sécurité de l'infrastructure 157
Résilience 158
Quotas et limites 159
Notifications 159
CloudFormation piles 159
DevOpsLimites de surveillance des ressources Guru 159
DevOpsQuotas Guru pour la création, le déploiement et la gestion d'une API 160
Historique de la documentation 161
AWS Glossaire 169
..... clxx

Qu'est-ce qu'Amazon DevOps Guru ?

Bienvenue dans le guide de l'utilisateur d'Amazon DevOps Guru.

DevOpsGuru est un service d'exploitation entièrement géré qui permet aux développeurs et aux opérateurs d'améliorer facilement les performances et la disponibilité de leurs applications. DevOpsGuru vous permet de vous décharger des tâches administratives associées à l'identification des problèmes opérationnels afin que vous puissiez rapidement mettre en œuvre des recommandations pour améliorer votre application. DevOpsGuru crée des informations réactives que vous pouvez utiliser pour améliorer votre application dès maintenant. Il crée également des informations proactives pour vous aider à éviter les problèmes opérationnels susceptibles d'affecter votre application à l'avenir.

DevOpsGuru applique l'apprentissage automatique pour analyser vos données opérationnelles ainsi que les indicateurs et événements de votre application afin d'identifier les comportements qui s'écartent des modèles de fonctionnement normaux. Vous êtes averti lorsque DevOps Guru détecte un problème ou un risque opérationnel. Pour chaque problème, DevOps Guru présente des recommandations intelligentes pour résoudre les problèmes opérationnels actuels et futurs.

Consultez Comment démarrer avec DevOps Guru ? pour démarrer

Comment fonctionne DevOps Guru ?

Le flux de travail DevOps Guru commence lorsque vous configurez sa couverture et ses notifications. Une fois que vous avez configuré DevOps Guru, celui-ci commence à analyser vos données opérationnelles. Lorsqu'il détecte un comportement anormal, il crée un aperçu contenant des recommandations et des listes de mesures, de groupes de journaux et d'événements liés au problème. Pour chaque idée, DevOps Guru vous en informe. Si vous l'avez activé AWS Systems Manager OpsCenter, un OpsItem est créé afin que vous puissiez utiliser Systems Manager OpsCenter pour suivre et gérer le traitement de vos informations. Chaque aperçu contient des recommandations, des mesures, des groupes de journaux et des événements liés à un comportement anormal. Utilisez les informations pour vous aider à comprendre le comportement anormal et à y remédier.

Voir Flux de travail DevOps Guru de haut niveau pour plus de détails sur les trois étapes de haut niveau du flux de travail. Consultez Flux de travail détaillé de DevOps Guru pour en savoir plus sur le flux de travail plus détaillé de DevOps Guru, notamment sur la manière dont il interagit avec les autres AWS services.

Rubriques

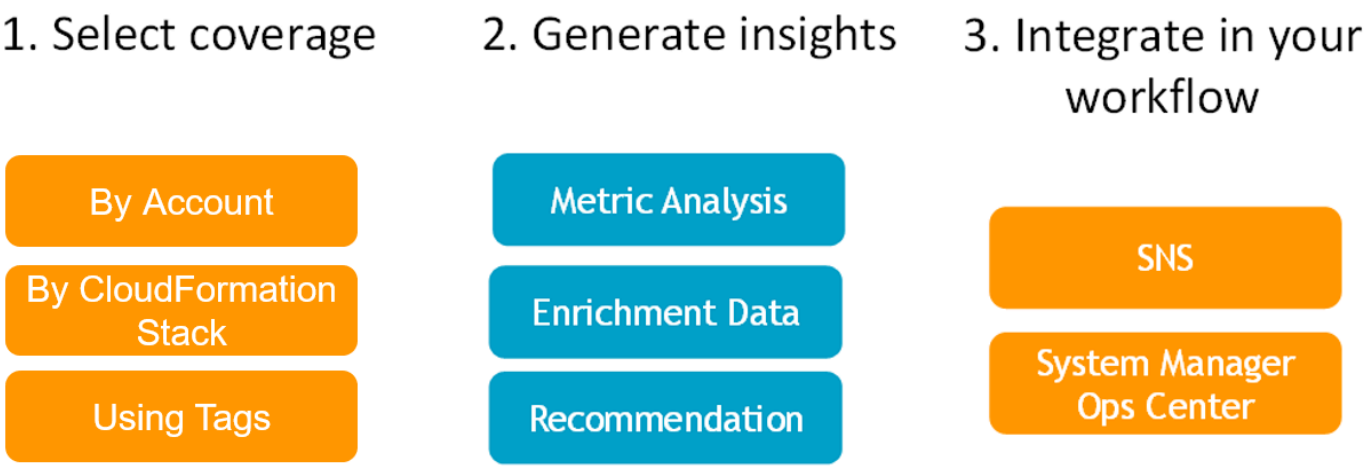
- Flux de travail DevOps Guru de haut niveau
- Flux de travail détaillé de DevOps Guru

Flux de travail DevOps Guru de haut niveau

Le flux de travail Amazon DevOps Guru peut être décomposé en trois étapes de haut niveau.

1. Spécifiez la couverture de DevOps Guru en lui indiquant les AWS ressources de votre AWS compte que vous souhaitez qu'il analyse.
2. DevOpsGuru commence à analyser CloudWatch les métriques d'Amazon et d'autres données opérationnelles afin d'identifier les problèmes que vous pouvez résoudre afin d'améliorer vos opérations. AWS CloudTrail
3. DevOpsGuru s'assure que vous êtes au courant des idées et des informations importantes en vous envoyant une notification pour chaque événement important du DevOps Guru.

Vous pouvez également configurer DevOps Guru pour créer un identifiant OpsItem AWS Systems Manager OpsCenter afin de vous aider à suivre vos informations. Le schéma suivant illustre ce flux de travail de haut niveau.



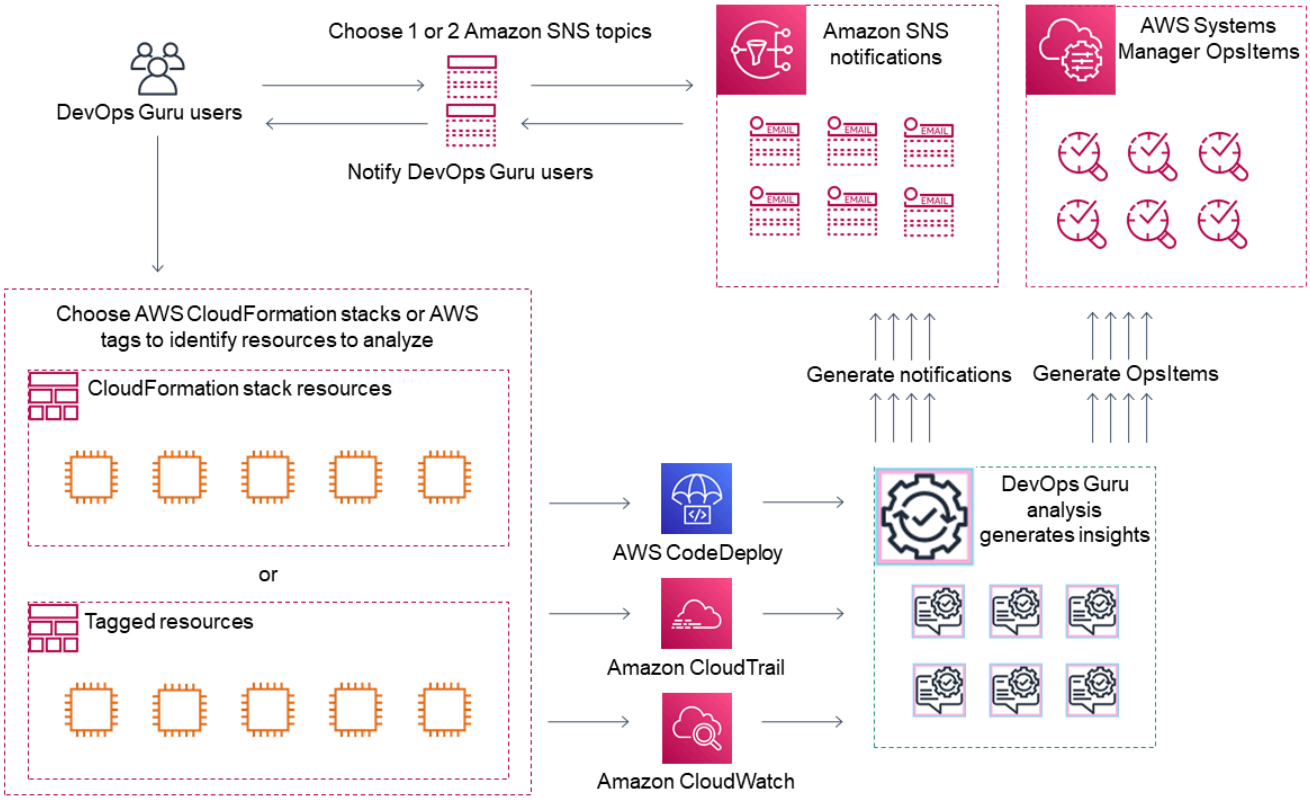
1. Dans un premier temps, vous choisissez votre couverture en spécifiant les AWS ressources de votre AWS compte qui sont analysées. DevOpsGuru peut couvrir ou analyser toutes les ressources d'un AWS compte, ou vous pouvez utiliser des AWS CloudFormation piles ou des AWS balises pour spécifier un sous-ensemble des ressources de votre compte à analyser. Assurez-vous que les ressources que vous spécifiez constituent les applications critiques, les

charges de travail et les microservices de votre entreprise. Pour plus d'informations sur les services et ressources pris en charge, consultez les tarifs Amazon DevOps Guru.

2. Dans un deuxième temps, DevOps Guru analyse les ressources pour générer des informations. Il s'agit d'un processus continu. Vous pouvez consulter les informations, les recommandations et les informations connexes qu'elles contiennent dans la console DevOps Guru. DevOps Guru analyse les données suivantes pour identifier les problèmes et obtenir des informations.
   - CloudWatch Mesures Amazon individuelles émises par vos AWS ressources. Lorsqu'un problème est identifié, DevOps Guru collecte ces indicateurs ensemble.
   - Enregistrez les anomalies depuis les groupes de CloudWatch journaux Amazon. Si vous activez la détection des anomalies de journal, DevOps Guru affiche les anomalies de journal associées en cas de problème.
   - DevOpsGuru extrait les données d'enrichissement AWS CloudTrail des journaux de gestion pour trouver les événements liés aux métriques collectées. Les événements peuvent être des événements de déploiement de ressources et des modifications de configuration.
   - Si vous en utilisez AWS CodeDeploy, DevOps Guru analyse les événements de déploiement pour générer des informations. Les événements relatifs à tous les types de CodeDeploy déploiements (serveur sur site, serveur Amazon EC2, Lambda ou Amazon EC2) sont analysés.
   - Lorsque DevOps Guru trouve un modèle spécifique, il génère une ou plusieurs recommandations pour aider à atténuer ou à résoudre le problème identifié. Les recommandations sont rassemblées en un seul aperçu. L'aperçu contient également une liste des mesures et des événements liés au problème. Vous utilisez les données d'analyse pour résoudre et comprendre le problème identifié.
3. Dans la troisième étape, DevOps Guru intègre des notifications informatives dans votre flux de travail pour vous aider à gérer les problèmes et à les résoudre rapidement.
   - Les informations générées sur votre AWS compte sont publiées sur la rubrique Amazon Simple Notification Service (Amazon SNS) choisie DevOps lors de la configuration de Guru. C'est ainsi que vous êtes averti dès qu'un aperçu est créé. Pour de plus amples informations, veuillez consulter Mettre à jour vos notifications dans DevOps Guru.
   - Si vous l'avez activé AWS Systems Manager lors de la configuration de DevOps Guru, chaque information crée une correspondance OpsItem pour vous aider à suivre et à gérer les problèmes découverts. Pour de plus amples informations, veuillez consulter Mettre à jour AWS Systems Manager l'intégration dans DevOps Guru.

Flux de travail détaillé de DevOps Guru

Le flux de travail DevOps Guru s'intègre à plusieurs AWS services CloudWatch, notamment Amazon AWS CloudTrail, Amazon Simple Notification Service et AWS Systems Manager. Le schéma suivant montre un flux de travail détaillé qui inclut son fonctionnement avec d'autres AWS services.



Ce diagramme montre un scénario dans lequel la couverture de DevOps Guru est spécifiée par les AWS ressources définies dans des AWS CloudFormation piles ou à l'aide de AWS balises. Si aucune pile ou étiquette n'est choisie, DevOps Guru coverage analyse toutes les AWS ressources de votre compte. Pour plus d'informations, consultez Définition des applications à l'aide de AWS ressources et Déterminer la couverture pour DevOps Guru.

1. Lors de la configuration, vous spécifiez une ou deux rubriques Amazon SNS utilisées pour vous informer des événements importants du DevOps Guru, tels que la création d'un aperçu. Ensuite, vous pouvez spécifier des AWS CloudFormation piles qui définissent les ressources que vous souhaitez analyser. Vous pouvez également permettre à Systems Manager de générer une information OpsItem pour chaque information afin de vous aider à gérer vos informations.
2. Une fois que DevOps Guru est configuré, il commence à analyser les CloudWatch métriques, les groupes de journaux et les événements émis par vos ressources et les AWS CloudTrail données

liées aux CloudWatch métriques. Si vos opérations incluent des CodeDeploy déploiements, DevOps Guru analyse également les événements de déploiement.

DevOpsGuru crée des informations lorsqu'il identifie un comportement inhabituel et anormal dans les données analysées. Chaque aperçu contient une ou plusieurs recommandations, une liste des mesures utilisées pour générer l'aperçu, une liste des groupes de journaux associés et une liste des événements utilisés pour générer l'aperçu. Utilisez ces informations pour résoudre le problème identifié.

3. Une fois chaque aperçu créé, DevOps Guru envoie une notification en utilisant le ou les sujets Amazon SNS spécifiés lors de la configuration de DevOps Guru. Si vous avez autorisé DevOps Guru à générer un OpsItem dans Systems Manager OpsCenter, chaque information déclenche également un nouveau Systems ManagerOpsItem. Vous pouvez utiliser Systems Manager pour gérer vos informations OpsItems.

Comment démarrer avec DevOps Guru ?

Nous vous recommandons d'effectuer les étapes suivantes :

1. Apprenez-en plus sur DevOps Guru en lisant les informations dansDevOpsLes concepts du gourou.
2. Configurez votre AWS compte, le AWS CLI, et un utilisateur administratif en suivant les étapes décrites dansConfiguration d'Amazon DevOps Guru.
3. Utilisez DevOps Guru en suivant les instructions deDébuter avec DevOps Guru.

Comment puis-je arrêter de payer des frais DevOps Guru ?

Pour désactiver Amazon DevOps Guru afin qu'il cesse d'encourir des frais liés à l'analyse des ressources de votre AWS compte et de votre région, mettez à jour vos paramètres de couverture afin qu'il n'analyse pas les ressources. Pour ce faire, suivez les étapes décrites Mettre à jour votre couverture AWS d'analyse dans DevOps Guru et choisissez Aucun à l'étape 4. Vous devez le faire pour chaque AWS compte et région dans lesquels DevOps Guru analyse les ressources.

> **Note**
>
> Si vous mettez à jour votre couverture pour arrêter d'analyser les ressources, vous pourriez continuer à encourir des frais mineurs si vous consultez les informations existantes générées

par DevOps Guru dans le passé. Ces frais sont associés aux appels d'API utilisés pour récupérer et afficher des informations d'aperçu. Pour plus d'informations, consultez les tarifs Amazon DevOps Guru.

DevOpsLes concepts du gourou

Les concepts suivants sont importants pour comprendre le fonctionnement d'Amazon DevOps Guru.

Rubriques

- Anomalie
- Informations
- Métriques et événements opérationnels
- Groupes de journaux et anomalies du journal
- Recommandations

Anomalie

Une anomalie représente une ou plusieurs mesures connexes détectées par DevOps Guru qui sont inattendues ou inhabituelles. DevOpsGuru génère des anomalies en utilisant l'apprentissage automatique pour analyser les métriques et les données opérationnelles liées à vos AWS ressources. Vous spécifiez les AWS ressources que vous souhaitez analyser lorsque vous configurez Amazon DevOps Guru. Pour de plus amples informations, veuillez consulter Configuration d'Amazon DevOps Guru.

Informations

Un aperçu est un ensemble d'anomalies créées lors de l'analyse des AWS ressources que vous spécifiez lors de la configuration de DevOps Guru. Chaque aperçu contient des observations, des recommandations et des données analytiques que vous pouvez utiliser pour améliorer vos performances opérationnelles. Il existe deux types d'informations :

- Réactif : un aperçu réactif permet d'identifier les comportements anormaux au fur et à mesure qu'ils se produisent. Il contient des anomalies avec des recommandations, des indicateurs connexes et des événements pour vous aider à comprendre et à résoudre les problèmes dès maintenant.

- Proactivité : un aperçu proactif vous permet de détecter les comportements anormaux avant qu'ils ne se produisent. Il contient des anomalies et des recommandations pour vous aider à résoudre les problèmes avant qu'ils ne se produisent.

Métriques et événements opérationnels

Les anomalies qui constituent un aperçu sont générées en analysant les métriques renvoyées par Amazon CloudWatch et les événements opérationnels émis par vos AWS ressources. Vous pouvez consulter les indicateurs et les événements opérationnels qui fournissent des informations qui vous aideront à mieux comprendre les problèmes de votre application.

Groupes de journaux et anomalies du journal

Lorsque vous activez la détection des anomalies dans les journaux, les groupes de journaux pertinents sont affichés sur les pages d'aperçu de DevOps Guru dans la console DevOps Guru. Un groupe de journaux vous permet de connaître les informations de diagnostic critiques concernant les performances et l'accès à une ressource.

Une anomalie de journal représente un groupe d'événements de journal anormaux similaires trouvés au sein d'un groupe de journaux. Des exemples d'événements de journal anormaux qui peuvent être affichés dans DevOps Guru incluent les anomalies de mots clés, les anomalies de format, les anomalies de code HTTP, etc.

Vous pouvez utiliser les anomalies du journal pour diagnostiquer la cause première d'un problème de fonctionnement. DevOpsGuru fait également référence aux lignes de journal dans ses recommandations afin de fournir plus de contexte aux solutions recommandées.

> **Note**
>
> DevOpsGuru travaille avec Amazon CloudWatch pour permettre la détection des anomalies dans les journaux. Lorsque vous activez la détection des anomalies dans les journaux, DevOps Guru ajoute des balises à vos groupes de CloudWatch journaux. Lorsque vous désactivez la détection des anomalies dans les journaux, DevOps Guru supprime les balises de vos groupes de CloudWatch journaux.
> En outre, les administrateurs doivent s'assurer que seuls les utilisateurs autorisés à consulter les CloudWatch journaux sont autorisés à consulter les CloudWatch journaux anormaux. Nous vous recommandons d'utiliser des politiques IAM pour autoriser ou refuser l'accès à

l'`ListAnomalousLogs`opération. Pour plus d'informations, consultez Identity and Access Management for DevOps Guru.

Recommandations

Chaque information fournit des recommandations et des suggestions pour vous aider à améliorer les performances de votre application. La recommandation inclut les éléments suivants :

- Description des actions de recommandation pour corriger les anomalies qui constituent l'aperçu.
- Une liste des indicateurs analysés dans lesquels DevOps Guru a détecté un comportement anormal. Chaque métrique inclut le nom de la CloudFormation pile qui a généré la ressource associée aux métriques, le nom de la ressource et le nom du AWS service associé à la ressource.
- Liste des événements liés aux mesures anormales associées à l'aperçu. Chaque événement associé contient le nom de la CloudFormation pile qui a généré la ressource associée à l'événement, le nom de la ressource qui a généré l'événement et le nom du AWS service associé à l'événement.
- Liste des groupes de journaux liés au comportement anormal associé à l'aperçu. Chaque groupe de journaux contient un exemple de message de journal, des informations sur les types d'anomalies de journal signalées, l'heure à laquelle les anomalies sont survenues et un lien permettant de consulter les lignes de journal CloudWatch.

DevOpsCouverture Guru

DevOpsGuru aborde et crée des informations pour un certain nombre de AWS services différents. Pour chaque service pour lequel DevOps Guru crée des informations, DevOps Guru affiche une variété de mesures analysées et d'informations générées.

Exemple de cas d'utilisation pour des informations réactives :

Service Name	Cas d'utilisation	Exemples	Métriques
AWS Lambda	Détectez les anomalies de latence ou de durée des fonctions Lambda	Déploiement du code : la Amazon API Gateway latence est affectée par une	Duration Throttles

Service Name	Cas d’utilisation	Exemples	Métriques
	causées par diverses causes fondament ales telles que les démarrages à froid, l'augmentation des demandes, la limitatio n en aval ou les déploiements de code. Recommandez des moyens d'atténue r rapidement les effets.	augmentation de la latence Lambda après un récent déploiement de code Lambda. Régulatio n en aval : l'opérate ur a réduit la capacité des unités de lecture pour DynamoDB, ce qui a entraîné une augmentation du nombre de tentative s. Cela entraîne un étranglement. Démarrage à froid : la fonction Lambda étant sous-provisionnée, Lambda prend plus de temps lorsque des demandes sont effectuées.	

Exemple de cas d'utilisation pour des informations proactives :

Service Name	Cas d’utilisation	Métriques
Amazon DynamoDB	La capacité consommée de lecture des tables DynamoDB risque d'atteindre la limite de la table. Action recommand ée : si vous utilisez le mode capacité provisionnée, utilisez le dimensionnement automatiq ue pour gérer activement la	ConsumedReadCapacityUnits

Service Name	Cas d'utilisation	Métriques
	capacité de débit des tables ou achetez de la capacité réservée à l'avance pour les tables. Passez en mode capacité à la demande pour payer par demande de lecture, en ne payant que pour ce qui est utilisé. Durée de détection : 6 jours	

Liste de couverture des services

Pour certains services, DevOps Guru crée des informations réactives. Un insight réactif identifie un comportement anormal lorsqu'il se produit. Il contient des anomalies avec des recommandations, des indicateurs connexes et des événements pour vous aider à comprendre et à résoudre les problèmes dès maintenant.

Pour certains services, DevOps Guru crée des informations proactives. Un aperçu proactif vous permet de détecter les comportements anormaux avant qu'ils ne se produisent. Il contient des anomalies et des recommandations pour vous aider à résoudre les problèmes avant qu'ils ne se produisent.

DevOpsGuru crée des informations réactives pour des services tels que les suivants :

- Amazon API Gateway
- Amazon CloudFront
- Amazon DynamoDB
- Amazon EC2

> **Note**
>
> DevOpsLa supervision de Guru se fait au niveau du groupe Auto Scaling, et non au niveau d'une seule instance.

- Amazon ECS

- Amazon EKS
- AWS Elastic Beanstalk
- Elastic Load Balancing
- Amazon Kinesis
- AWS Lambda
- Amazon OpenSearch Service
- Amazon RDS
- Amazon Redshift
- Amazon Route 53
- Amazon S3
- Amazon SageMaker AI
- AWS Step Functions
- Amazon SNS
- Amazon SQS
- Amazon SWF
- Amazon VPC

DevOpsGuru crée des informations proactives pour des services tels que les suivants :

- Amazon DynamoDB
- Amazon Kinesis
- AWS Lambda
- Amazon RDS
- Amazon SQS

Configuration d'Amazon DevOps Guru

Effectuez les tâches décrites dans cette section pour configurer Amazon DevOps Guru pour la première fois. Si vous possédez déjà un AWS compte, si vous savez quel AWS compte ou quels comptes vous souhaitez analyser et si vous avez une rubrique Amazon Simple Notification Service à utiliser pour les notifications d'analyse, vous pouvez passer directement àDébuter avec DevOps Guru.

Vous pouvez éventuellement utiliser Quick Setup, une fonctionnalité de AWS Systems Manager, pour configurer DevOps Guru et configurer rapidement ses options. Vous pouvez utiliser la configuration rapide pour configurer DevOps Guru pour un compte autonome ou pour une organisation. Pour utiliser la configuration rapide dans Systems Manager afin de configurer DevOps Guru pour une organisation, vous devez disposer des prérequis suivants :

- Une organisation avec AWS Organizations. Pour plus d'informations, consultez AWS Organizations la terminologie et les concepts du Guide de AWS Organizations l'utilisateur.
- Deux unités organisationnelles (UO) ou plus.
- Un ou plusieurs AWS comptes cibles dans chaque unité d'organisation.
- Un compte administrateur doté des privilèges nécessaires pour gérer les comptes cibles.

Pour savoir comment configurer DevOps Guru à l'aide de la configuration rapide, voir Configurer DevOps Guru avec Quick Setup dans le Guide de AWS Systems Manager l'utilisateur.

Suivez les étapes ci-dessous pour configurer DevOps Guru sans configuration rapide.

- Étape 1 — Inscrivez-vous AWS
- Étape 2 — Déterminer la couverture pour DevOps Guru
- Étape 3 — Identifiez le sujet de vos notifications Amazon SNS

Étape 1 — Inscrivez-vous AWS

Inscrivez-vous pour Compte AWS

Pour commencer AWS, vous avez besoin d'un Compte AWS. Pour plus d'informations sur la création d'un Compte AWS, consultez la section Démarrage avec un Compte AWS dans le Guide de Gestion de compte AWS référence.

Étape 2 — Déterminer la couverture pour DevOps Guru

Votre couverture des limites détermine les AWS ressources qui sont analysées par Amazon DevOps Guru pour détecter tout comportement anormal. Nous vous recommandons de regrouper vos ressources dans vos applications opérationnelles. Toutes les ressources situées dans votre limite de ressources doivent comprendre une ou plusieurs de vos applications. Si vous disposez d'une solution opérationnelle, votre limite de couverture doit inclure toutes ses ressources. Si vous avez plusieurs applications, choisissez les ressources qui constituent chaque solution et regroupez-les à l'aide de CloudFormation piles ou de AWS balises. Toutes les ressources combinées que vous spécifiez, qu'elles définissent une ou plusieurs applications, sont analysées par DevOps Guru et constituent sa limite de couverture.

Utilisez l'une des méthodes suivantes pour spécifier les ressources de vos solutions opérationnelles.

- Choisissez que votre AWS région et votre compte définissent votre limite de couverture. Avec cette option, DevOps Guru analyse toutes les ressources de votre compte et de votre région. C'est une bonne option à choisir si vous n'utilisez votre compte que pour une seule application.
- Utilisez CloudFormation des piles pour définir les ressources de votre application opérationnelle. CloudFormation les modèles définissent et génèrent vos ressources pour vous. Spécifiez les piles qui créent les ressources de votre application lorsque vous configurez DevOps Guru. Vous pouvez mettre à jour vos piles à tout moment. Toutes les ressources des piles que vous choisissez définissent votre couverture limite. Pour de plus amples informations, veuillez consulter Utiliser des CloudFormation piles pour identifier les ressources dans vos applications DevOps Guru.
- Utilisez des AWS balises pour spécifier AWS les ressources de vos applications. DevOpsGuru analyse uniquement les ressources qui contiennent les balises que vous choisissez. Ces ressources constituent vos limites.

  Un AWS tag se compose d'une clé de tag et d'une valeur de tag. Vous pouvez spécifier une clé de balise et spécifier une ou plusieurs valeurs avec cette clé. Utilisez une valeur unique pour toutes les ressources de l'une de vos applications. Si vous avez plusieurs applications, utilisez une balise avec la même clé pour chacune d'entre elles et regroupez les ressources dans vos applications à l'aide des valeurs des balises. Toutes les ressources avec les balises que vous choisissez constituent la limite de couverture de DevOps Guru. Pour de plus amples informations, veuillez consulter Utiliser des balises pour identifier les ressources dans vos applications DevOps Guru.

Si votre couverture limite inclut des ressources qui constituent plusieurs applications, vous pouvez utiliser des balises pour filtrer vos informations afin de les afficher par application à la fois. Pour plus d'informations, reportez-vous à l'étape 4 deConsulter les informations de DevOps Guru.

Pour de plus amples informations, veuillez consulter Définition des applications à l'aide de AWS ressources. Pour plus d'informations sur les services et ressources pris en charge, consultez la rubrique Tarification d'Amazon DevOps Guru.

Étape 3 — Identifiez le sujet de vos notifications Amazon SNS

Vous utilisez une ou deux rubriques Amazon SNS pour générer des notifications concernant des événements DevOps Guru importants, tels que la création d'un aperçu. Cela vous permet de connaître les problèmes détectés par DevOps Guru le plus rapidement possible. Préparez vos sujets lorsque vous configurez DevOps Guru. Lorsque vous utilisez la console DevOps Guru pour configurer DevOps Guru, vous spécifiez une rubrique de notification en utilisant son nom ou son Amazon Resource Name (ARN). Pour plus d'informations, voir Activer DevOps Guru. Vous pouvez utiliser la console Amazon SNS pour afficher le nom et l'ARN de chacune de vos rubriques. Si vous n'avez pas de sujet, vous pouvez en créer un lorsque vous activez DevOps Guru à l'aide de la console DevOps Guru. Pour plus d'informations, consultez la section Création d'une rubrique dans le guide du développeur Amazon Simple Notification Service.

Autorisations ajoutées à votre rubrique Amazon SNS

Une rubrique Amazon SNS est une ressource qui contient une politique de ressources Gestion des identités et des accès AWS (IAM). Lorsque vous spécifiez un sujet ici, DevOps Guru ajoute les autorisations suivantes à sa politique de ressources.

```
{
    "Sid": "DevOpsGuru-added-SNS-topic-permissions",
    "Effect": "Allow",
    "Principal": {
        "Service": "region-id.devops-guru.amazonaws.com"
    },
    "Action": "sns:Publish",
    "Resource": "arn:aws:sns:region-id:topic-owner-account-id:my-topic-name",
    "Condition" : {
      "StringEquals" : {
        "AWS:SourceArn": "arn:aws:devops-guru:region-id:topic-owner-account-
id:channel/devops-guru-channel-id",
        "AWS:SourceAccount": "topic-owner-account-id"
```

```
    }
  }
}
```

Ces autorisations sont requises pour que DevOps Guru puisse publier des notifications à l'aide d'un sujet. Si vous préférez ne pas disposer de ces autorisations sur le sujet, vous pouvez les supprimer en toute sécurité et le sujet continuera à fonctionner comme avant que vous ne le choisissiez. Toutefois, si ces autorisations ajoutées sont supprimées, DevOps Guru ne peut pas utiliser la rubrique pour générer des notifications.

Estimation des coûts d'analyse des ressources Amazon DevOps Guru

Vous pouvez estimer le coût mensuel de l'analyse de vos ressources AWS par Amazon DevOps Guru. Vous payez le nombre d'heures analysées pour chaque ressource AWS active comprise dans la couverture de ressources que vous avez spécifiée. Une ressource est active si elle produit des métriques, des événements ou des journaux en moins d'une heure.

DevOps Guru analyse les ressources que vous avez sélectionnées pour créer une estimation des coûts mensuels. Vous pouvez consulter les ressources, leur prix horaire facturable et leurs frais mensuels estimés. L'estimateur de coûts suppose par défaut que les ressources actives analysées sont utilisées 100 % du temps. Vous pouvez modifier ce pourcentage pour chaque service analysé en fonction de votre utilisation estimée afin de créer une estimation des coûts mensuels actualisée. L'estimation concerne le coût d'analyse de vos ressources et n'inclut pas les coûts associés aux appels d'API DevOps Guru.

Vous pouvez créer une estimation des coûts à la fois. Le temps nécessaire pour générer une estimation des coûts dépend du nombre de ressources que vous spécifiez lors de la création de l'estimation des coûts. Lorsque vous spécifiez quelques ressources, cela peut prendre 1 à 2 heures. Lorsque vous spécifiez un grand nombre de ressources, l'exécution peut prendre jusqu'à 4 heures. Vos coûts réels varient et dépendent du pourcentage de temps pendant lequel les ressources actives analysées sont utilisées.

> **Note**
>
> Pour une estimation des coûts, vous ne pouvez spécifier qu'une seule CloudFormation pile. Pour votre limite de couverture réelle, vous pouvez spécifier jusqu'à 1 000 piles.

Pour créer une estimation des coûts d'analyse des ressources mensuelle

1. Ouvrez la console Amazon DevOps Guru à l'adresse https://console.aws.amazon.com/devops-guru/.
2. Choisissez Cost estimator dans le volet de navigation.
3. Si vous n'avez pas activé DevOps Guru, vous devez créer un rôle IAM. Dans la fenêtre contextuelle Créer un rôle IAM pour DevOps Guru qui apparaît, choisissez Agree pour créer un

rôle IAM. Cela permet à DevOps Guru de créer pour vous un rôle lié au service IAM lorsque vous choisissez de commencer l'analyse d'estimation des coûts ou de commencer à utiliser Guru. DevOps DevOpsGuru dispose ainsi des autorisations nécessaires pour créer l'estimation des coûts. Si vous avez déjà activé DevOps Guru, le rôle a déjà été créé et cette option n'apparaît pas.

4. Choisissez les ressources que vous souhaitez utiliser pour créer votre estimation.

   - Si vous souhaitez estimer le coût pour DevOps Guru d'analyser les ressources définies par une CloudFormation pile, procédez comme suit.
     1. Choisissez CloudFormation une pile dans la région actuelle.
     2. Dans Choisir une CloudFormation pile, choisissez le nom d'une CloudFormation pile dans votre AWS compte. Vous pouvez également saisir le nom d'une pile pour la retrouver rapidement. Pour plus d'informations sur l'utilisation et l'affichage de vos piles, consultez la section Utilisation des piles dans le guide de l'CloudFormation utilisateur.
     3. (Facultatif) Si vous utilisez une CloudFormation pile que vous n'analysez pas actuellement, choisissez Activer l'analyse des ressources pour permettre à DevOps Guru de commencer à analyser ses ressources. Cette option n'est pas disponible si vous n'avez pas activé DevOps Guru ou si vous analysez déjà les ressources de la pile.
   - Si vous souhaitez estimer le coût d'analyse des ressources par DevOps Guru à l'aide d'une balise, procédez comme suit.
     1. Choisissez des tags sur AWS les ressources de la région actuelle
     2. Dans Tag key, choisissez la clé de votre tag
     3. Dans Valeur du tag, choisissez (toutes les valeurs) ou choisissez une valeur.
   - Si vous souhaitez estimer le coût pour que DevOps Guru analyse la ressource de votre AWS compte et de votre région, choisissez un AWS compte dans la région actuelle.
5. Choisissez Estimer le coût mensuel.
6. (Facultatif) Dans la colonne % d'utilisation active des ressources, entrez une valeur de pourcentage actualisée pour un ou plusieurs services AWS. Le % d'utilisation des ressources actives par défaut est de 100 %. Cela signifie que DevOps Guru génère l'estimation du service AWS en calculant le coût d'une heure d'analyse de ses ressources, puis en extrapolant ce montant sur 30 jours pour un total de 720 heures. Si un service est actif moins de 100 % du temps, vous pouvez mettre à jour le pourcentage en fonction de votre utilisation estimée pour une estimation plus précise. Par exemple, si vous actualisez le taux d'utilisation des ressources actives d'un service à 75 %, le coût d'une heure d'analyse de ses ressources est extrapolé sur (720 x 0,75) heures, soit 540 heures.

Si votre estimation est de zéro dollar, les ressources que vous avez choisies n'incluent probablement pas les ressources prises en charge par DevOps Guru. Pour plus d'informations sur les services et ressources pris en charge, consultez les tarifs Amazon DevOps Guru.

Débuter avec DevOps Guru

Dans cette section, vous découvrirez comment démarrer avec Amazon DevOps Guru afin qu'il puisse analyser les données opérationnelles et les indicateurs de votre application afin de générer des informations.

Rubriques

- Étape 1 : Configuration
- Étape 2 : Activez DevOps Guru
- Étape 3 : Spécifiez la couverture de vos ressources DevOps Guru

Étape 1 : Configuration

Avant de commencer, préparez-vous en suivant les étapes décrites dansConfiguration d'Amazon DevOps Guru.

Étape 2 : Activez DevOps Guru

Pour configurer Amazon DevOps Guru afin de l'utiliser pour la première fois, vous devez choisir la manière dont vous souhaitez configurer DevOps Guru. Vous pouvez soit surveiller les applications au sein de votre organisation, soit surveiller les applications de votre compte courant.

Vous pouvez soit surveiller vos applications au sein de votre organisation, soit activer DevOps Guru exclusivement pour le compte courant. Les procédures suivantes décrivent les différentes manières de configurer DevOps Guru en fonction de vos besoins.

Surveillez les comptes au sein de votre organisation

Si vous choisissez de surveiller les applications au sein de votre organisation, connectez-vous au compte de gestion de votre organisation. Vous pouvez éventuellement configurer un compte de membre de l'organisation en tant qu'administrateur délégué. Vous ne pouvez avoir qu'un seul administrateur délégué à la fois et vous pouvez modifier les paramètres de l'administrateur ultérieurement. Le compte de gestion et le compte d'administrateur délégué que vous configurez ont tous deux accès à toutes les informations relatives à tous les comptes de votre organisation.

Vous pouvez soit ajouter une prise en charge multicompte pour votre organisation à l'aide de la console, soit à l'aide de la AWS CLI.

Intégrez la console DevOps Guru

Vous pouvez utiliser la console pour ajouter la prise en charge des comptes au sein de votre organisation.

Utilisez la console pour permettre à DevOps Guru de consulter des informations agrégées

1. Ouvrez la console Amazon DevOps Guru à l'adresse https://console.aws.amazon.com/devops-guru/.
2. Choisissez Surveiller les applications de vos organisations comme type de configuration.
3. Choisissez le compte que vous souhaitez utiliser en tant qu'administrateur délégué. Choisissez ensuite Enregistrer un administrateur délégué. Cela donne accès à une vue consolidée pour tout compte sur lequel DevOps Guru est activé. L'administrateur délégué dispose d'une vue consolidée de toutes les informations et statistiques de DevOps Guru au sein de votre organisation. Vous pouvez activer d'autres comptes à l'aide de la configuration rapide ou des ensembles de AWS CloudFormation piles SSM. Pour en savoir plus sur la configuration rapide, consultez Configurer DevOps Guru avec la configuration rapide. Pour en savoir plus sur la configuration avec des ensembles de piles, voir Utilisation des piles dans le Guide de CloudFormation l'utilisateur, Étape 2 — Déterminer la couverture pour DevOps Guru et. etUtiliser des CloudFormation piles pour identifier les ressources dans vos applications DevOps Guru.

Intégrer avec la AWS CLI

Vous pouvez utiliser la AWS CLI pour permettre à DevOps Guru de consulter des informations agrégées. Exécutez les commandes suivantes.

```
aws iam create-service-linked-role --aws-service-name devops-guru.amazonaws.com --
description "My service-linked role to support DevOps Guru"

aws organizations enable-aws-service-access --service-principal devops-
guru.amazonaws.com

aws organizations register-delegated-administrator --account-id >ACCOUNT_ID< --service-
principal devops-guru.amazonaws.com
```

Le tableau suivant décrit les commandes.

Commande	Description

Commande	Description
`create-service-linked-role`	Permet à DevOps Guru de recueillir des informations sur votre organisation. Ne poursuivez pas si cette étape échoue.
`enable-aws-service-access`	Intégrez votre organisation à DevOps Guru.
`register-delegated-administrator`	Donne accès au compte du membre pour consulter les informations.

Surveillez votre compte courant

Si vous choisissez de surveiller les applications de votre AWS compte courant, choisissez les AWS ressources de votre compte et de votre région qui sont couvertes ou analysées et spécifiez un ou deux sujets Amazon Simple Notification Service qui sont utilisés pour vous avertir lorsqu'un aperçu est créé. Vous pouvez mettre à jour ces paramètres ultérieurement si nécessaire.

Permettez à DevOps Guru de surveiller les applications de votre AWS compte courant

1. Ouvrez la console Amazon DevOps Guru à l'adresse https://console.aws.amazon.com/devops-guru/.
2. Choisissez Surveiller les applications du AWS compte courant comme type de configuration.
3. Dans la couverture de l'analyse DevOps Guru, choisissez l'une des options suivantes.

   - Analysez toutes les AWS ressources du AWS compte courant : DevOps Guru analyse toutes les AWS ressources de votre compte.
   - Choisissez les ressources AWS à analyser ultérieurement : vous choisissez votre limite d'analyse ultérieurement. Pour plus d’informations, consultez Déterminer la couverture pour DevOps Guru et Mettre à jour votre couverture AWS d'analyse dans DevOps Guru.

   DevOpsGuru peut analyser n'importe quelle ressource associée au AWS compte qu'il prend en charge. Pour plus d'informations sur les services et ressources pris en charge, consultez les tarifs Amazon DevOps Guru.

4. Vous pouvez ajouter jusqu'à deux sujets. DevOpsGuru utilise le ou les sujets pour vous informer des événements importants du DevOps Guru, tels que la création d'un nouvel aperçu. Si vous ne spécifiez pas de sujet pour le moment, vous pouvez en ajouter un ultérieurement en choisissant Paramètres dans le volet de navigation.

   a. Dans Spécifier une rubrique Amazon SNS, choisissez une rubrique à utiliser.

   b. Pour ajouter une rubrique Amazon SNS, effectuez l'une des opérations suivantes.

      - Choisissez Générer une nouvelle rubrique SNS par e-mail. Ensuite, dans Spécifiez l'adresse e-mail, entrez l'adresse e-mail à laquelle vous souhaitez recevoir des notifications. Pour saisir des adresses e-mail supplémentaires, choisissez Ajouter une nouvelle adresse e-mail.
      - Choisissez Utiliser une rubrique SNS existante. Ensuite, dans Choisissez un sujet dans votre AWS compte, sélectionnez le sujet que vous souhaitez utiliser.
      - Choisissez Utiliser l'ARN d'une rubrique SNS existante pour spécifier une rubrique existante provenant d'un autre compte. Ensuite, dans Entrez un ARN pour un sujet, entrez l'ARN du sujet. L'ARN est le nom de la ressource Amazon du sujet. Vous pouvez définir un sujet dans un autre compte. Si vous utilisez un sujet dans un autre compte, vous devez y ajouter une politique de ressources. Pour de plus amples informations, veuillez consulter Autorisations pour les rubriques Amazon SNS.

5. Sélectionnez Activer.

Pour configurer Amazon DevOps Guru afin de l'utiliser pour la première fois, vous devez choisir les AWS ressources de votre compte et de votre région qui sont couvertes ou analysées, et spécifier une ou deux rubriques Amazon Simple Notification Service qui sont utilisées pour vous avertir lorsqu'un aperçu est créé. Vous pouvez mettre à jour ces paramètres ultérieurement si nécessaire.

Étape 3 : Spécifiez la couverture de vos ressources DevOps Guru

Si vous avez choisi de spécifier les AWS ressources ultérieurement lorsque vous avez activé DevOps Guru, vous devez choisir les CloudFormation piles de votre AWS compte qui créent les ressources que vous souhaitez analyser. Une CloudFormation pile est un ensemble de AWS ressources que vous gérez comme une seule unité. Vous pouvez utiliser une ou plusieurs piles pour inclure toutes les ressources nécessaires à l'exécution de vos applications opérationnelles, puis les spécifier afin qu'elles soient analysées par DevOps Guru. Si vous ne spécifiez pas de piles, DevOps Guru analyse toutes les AWS ressources de votre compte. Pour plus d'informations, voir Utilisation des piles dans

le Guide de l'CloudFormation utilisateur, Déterminer la couverture pour DevOps Guru et. etUtiliser des CloudFormation piles pour identifier les ressources dans vos applications DevOps Guru.

> **Note**
>
> Pour plus d'informations sur les services et ressources pris en charge, consultez les tarifs Amazon DevOps Guru.

Spécifier la couverture des ressources DevOps Guru

1. Ouvrez la console Amazon DevOps Guru à l'adresse https://console.aws.amazon.com/devops-guru/.
2. Développez les paramètres dans le volet de navigation.
3. Dans Ressources analysées, choisissez Modifier les ressources analysées.
4. Choisissez l'une des options de couverture suivantes.

   - Choisissez Toutes les ressources du compte si vous souhaitez que DevOps Guru analyse toutes les ressources prises en charge dans votre AWS compte et dans votre région. Si vous choisissez cette option, votre AWS compte est la limite de couverture de votre analyse des ressources. Toutes les ressources de chaque pile de votre compte sont regroupées dans leur propre application. Toutes les ressources restantes qui ne figurent pas dans une pile sont regroupées dans leur propre application.
   - Choisissez les CloudFormation piles si vous souhaitez que DevOps Guru analyse les ressources qui se trouvent dans les piles de votre choix, puis choisissez l'une des options suivantes.
     - Toutes les ressources : toutes les ressources accumulées sur votre compte sont analysées. Les ressources de chaque pile sont regroupées dans leur propre application. Les ressources de votre compte qui ne figurent pas dans une pile ne sont pas analysées.
     - Sélectionnez les piles — Sélectionnez les piles que vous souhaitez que DevOps Guru analyse. Les ressources de chaque pile que vous sélectionnez sont regroupées dans leur propre application. Vous pouvez saisir le nom d'une pile dans Rechercher des piles pour localiser rapidement une pile spécifique. Vous pouvez sélectionner jusqu'à 1 000 piles.

   Pour de plus amples informations, veuillez consulter Utiliser des CloudFormation piles pour identifier les ressources dans vos applications DevOps Guru.

- Choisissez Tags si vous souhaitez que DevOps Guru analyse toutes les ressources contenant les tags que vous avez choisis. Choisissez une clé, puis l'une des options suivantes.
  - Toutes les ressources du compte : analysez toutes les ressources AWS de la région et du compte actuels. Les ressources dont la clé de balise est sélectionnée sont regroupées par valeur de balise, le cas échéant. Les ressources dépourvues de cette clé de balise sont regroupées et analysées séparément.
  - Choisissez des valeurs de balise spécifiques : toutes les ressources contenant une balise avec la clé que vous avez choisie sont analysées. DevOpsGuru regroupe vos ressources dans des applications en fonction des valeurs de votre tag.

  Pour de plus amples informations, veuillez consulter Utiliser des balises pour identifier les ressources dans vos applications DevOps Guru.
- Choisissez Aucune si vous ne voulez pas que DevOps Guru analyse les ressources. Cette option désactive DevOps Guru afin que vous arrêtiez de payer des frais liés à l'analyse des ressources.

5. Choisissez Enregistrer.

AWS Services habilitants pour l'analyse DevOps Guru

Amazon DevOps Guru peut analyser les performances de toutes les AWS ressources qu'il prend en charge. Lorsqu'il détecte un comportement anormal, il génère un aperçu détaillé du comportement et de la manière d'y remédier. Pour plus d'informations sur les services et ressources pris en charge, consultez les tarifs Amazon DevOps Guru.

DevOpsGuru utilise CloudWatch les métriques, les AWS CloudTrail événements et bien plus encore d'Amazon pour analyser les ressources. La plupart des ressources qu'il prend en charge génèrent automatiquement les métriques requises pour l'analyse DevOps Guru. Cependant, certains AWS services nécessitent des actions supplémentaires pour générer les métriques requises. Pour certains services, l'activation de ces indicateurs fournit une analyse supplémentaire de la couverture DevOps Guru existante. Pour d'autres, l'analyse n'est pas possible tant que vous n'activez pas ces mesures. Pour plus d'informations, consultez Déterminer la couverture pour DevOps Guru et Mettre à jour votre couverture AWS d'analyse dans DevOps Guru.

Services nécessitant une action pour l'analyse de DevOps Guru

- Amazon Elastic Container Service — Pour générer des indicateurs supplémentaires qui améliorent la couverture de ses ressources par DevOps Guru, suivez les étapes décrites dans Configuration des informations sur les conteneurs sur Amazon ECS. Cela peut entraîner des CloudWatch frais Amazon.
- Amazon Elastic Kubernetes Service : DevOps pour générer des métriques à analyser par Guru, suivez les étapes décrites dans Configuration des informations sur les conteneurs sur Amazon EKS et Kubernetes. DevOpsGuru n'analyse aucune ressource Amazon EKS tant que la génération de ces métriques n'est pas configurée. Cela peut entraîner des CloudWatch frais Amazon.
- Amazon Simple Storage Service — Pour générer des métriques à analyser par DevOps Guru, vous devez activer les métriques de demande. Suivez les étapes décrites dans Création d'une configuration de CloudWatch métriques pour tous les objets de votre compartiment. DevOps Guru n'analyse aucune ressource Amazon S3 tant que la génération de ces métriques n'est pas configurée. Cela peut entraîner des frais CloudWatch pour Amazon S3.

Pour plus d'informations, consultez les CloudWatch tarifs Amazon.

Travailler avec des informations dans DevOps Guru

Amazon DevOps Guru génère des informations lorsqu'il détecte un comportement anormal dans vos applications opérationnelles. DevOpsGuru analyse les métriques, les événements et plus encore dans les AWS ressources que vous avez spécifiées lors de la configuration de DevOps Guru. Chaque analyse contient une ou plusieurs recommandations que vous pouvez appliquer pour atténuer le problème. Il contient également une liste des métriques, une liste des groupes de journaux et une liste des événements utilisés pour identifier le comportement inhabituel.

Il existe deux types d'informations.

- Reactive Insights contient des recommandations que vous pouvez appliquer pour résoudre les problèmes actuels.
- Proactive Insights contient des recommandations qui résolvent les problèmes qui, selon DevOps Guru, se produiront dans le futur.

Rubriques

- Consulter les informations de DevOps Guru
- Comprendre les informations contenues dans la console DevOps Guru
- Comprendre comment les comportements anormaux sont regroupés en informations
- Comprendre la sévérité des informations

Consulter les informations de DevOps Guru

Vous pouvez consulter vos informations à l'aide du Console de gestion AWS.

Consultez les informations de votre DevOps gourou

1. Ouvrez la console Amazon DevOps Guru à l'adresse https://console.aws.amazon.com/devops-guru/.
2. Ouvrez le volet de navigation, puis choisissez Insights.
3. Dans l'onglet Réactif, vous pouvez voir une liste d'informations réactives. Dans l'onglet Proactive, vous pouvez voir une liste d'informations proactives.
4. (Facultatif) Utilisez un ou plusieurs des filtres suivants pour trouver les informations que vous recherchez.

- Choisissez l'onglet Réactif ou Proactif, selon le type d'information que vous recherchez.
- Choisissez Filtrer les informations, puis choisissez une option pour spécifier un filtre. Vous pouvez ajouter une combinaison de filtres de statut, de gravité, de ressources et de balises. Utilisez un filtre de AWS balises pour afficher les informations générées uniquement par les ressources dotées de balises spécifiques. Pour en savoir plus, veuillez consulter la section Utiliser des balises pour identifier les ressources dans vos applications DevOps Guru.

> **Note**
>
> DevOpsGuru peut analyser les ressources suivantes, mais ne peut pas filtrer leurs informations à l'aide de balises.
>
> - Chemins et itinéraires Amazon API Gateway
> - Amazon DynamoDB Streams
> - Instances de groupe Amazon EC2 Auto Scaling
> - AWS Elastic Beanstalk environnements
> - Nœuds Amazon Redshift

- Choisissez ou spécifiez une plage de temps à filtrer en fonction de l'heure de création de l'aperçu.
  - 12h affiche les informations créées au cours des 12 dernières heures.
  - 1d affiche les informations créées au cours de la dernière journée.
  - 1w montre les informations créées au cours de la semaine écoulée.
  - 1m montre les informations créées au cours du mois dernier.
  - L'option Personnaliser vous permet de définir une autre plage horaire. La période maximale que vous pouvez utiliser pour filtrer les informations est de 180 jours.

5. Pour afficher les détails d'un aperçu, choisissez son nom.

Comprendre les informations contenues dans la console DevOps Guru

Utilisez la console Amazon DevOps Guru pour consulter des informations utiles dans vos analyses afin de vous aider à diagnostiquer et à traiter les comportements anormaux. Lorsque DevOps Guru analyse vos ressources et trouve CloudWatch des métriques, des AWS CloudTrail événements et des données opérationnelles Amazon connexes qui indiquent un comportement inhabituel, il crée un aperçu contenant des recommandations pour résoudre le problème et des informations sur les mesures et événements associés. Utilisez les données d'information Les meilleures pratiques dans DevOps Guru pour résoudre les problèmes opérationnels détectés par DevOps Guru.

Pour consulter un aperçu, suivez les étapes décrites Visualisation des informations pour en trouver un, puis choisissez son nom. La page d'aperçu contient les informations suivantes.

Aperçu d'Insight

Utilisez cette section pour obtenir un aperçu de haut niveau des informations. Vous pouvez voir le statut de l'aperçu (en cours ou fermé), le nombre de CloudFormation piles concernées, la date de début, de fin et de dernière mise à jour de l'aperçu, ainsi que l'élément des opérations associé le cas échéant.

Si un aperçu est regroupé au niveau de la pile, vous pouvez choisir le nombre de piles concernées pour voir leur nom. Le comportement anormal à l'origine de l'information s'est produit dans les ressources créées par les piles concernées. Si un aperçu est regroupé au niveau du compte, le chiffre est nul ou n'apparaît pas.

Pour de plus amples informations, veuillez consulter Comprendre comment les comportements anormaux sont regroupés en informations.

Nom de l'aperçu

Le nom d'un aperçu varie selon qu'il est regroupé au niveau de la pile ou au niveau du compte.

- Les noms d'informations au niveau de la pile incluent le nom de la pile qui contient la ressource au comportement anormal.
- Les noms d'aperçu au niveau du compte n'incluent pas de nom de pile.

Pour de plus amples informations, veuillez consulter Comprendre comment les comportements anormaux sont regroupés en informations.

Métriques agrégées

Choisissez l'onglet Mesures agrégées pour afficher les mesures liées aux informations. Dans le tableau, chaque ligne représente une métrique. Vous pouvez voir quelle CloudFormation pile a créé la ressource qui a émis la métrique, le nom de la ressource et son type. Les métriques ne sont pas toutes associées à une CloudFormation pile ou n'ont pas de nom.

Lorsque plusieurs ressources présentent des anomalies en même temps, la vue chronologique regroupe les ressources et présente leurs indicateurs anormaux dans une chronologie unique pour faciliter l'analyse. Les lignes rouges sur une chronologie indiquent les périodes pendant lesquelles une métrique a émis des valeurs inhabituelles. Pour zoomer, utilisez votre souris pour sélectionner une plage de temps spécifique. Vous pouvez également utiliser les icônes en forme de loupe pour zoomer ou dézoomer.

Choisissez une ligne rouge dans la chronologie pour afficher des informations détaillées. Dans la fenêtre qui s'ouvre, vous pouvez :

- Choisissez Afficher dans CloudWatch pour voir à quoi ressemble la métrique dans la CloudWatch console. Pour plus d'informations, consultez la section Statistiques et dimensions du guide de CloudWatch l'utilisateur Amazon.
- Passez la souris sur le graphique pour afficher les détails des données métriques anormales et le moment où elles se sont produites.
- Cochez la case avec la flèche vers le bas pour télécharger une image PNG du graphique.

Anomalies représentées graphiquement

Choisissez l'onglet Anomalies graphiques pour afficher des graphiques détaillés pour chacune des anomalies de l'aperçu. Une vignette apparaît pour chaque anomalie avec des détails sur les comportements inhabituels détectés dans les métriques associées. Vous pouvez étudier et examiner une anomalie au niveau des ressources et par statistique. Les graphiques sont regroupés par nom de métrique. Dans chaque vignette, vous pouvez choisir une plage de temps spécifique dans la chronologie pour zoomer. Vous pouvez également utiliser les icônes en forme de loupe pour zoomer ou dézoomer, ou choisir une durée prédéfinie en heures, jours ou semaines (1H, 3H, 12H, 1D, 3D, 1W ou 2W).

Choisissez Afficher toutes les statistiques et les dimensions pour voir les détails de l'anomalie. Dans la fenêtre qui s'ouvre, vous pouvez :

- Choisissez Afficher dans CloudWatch pour voir à quoi ressemble la métrique dans la CloudWatch console.

- Passez la souris sur le graphique pour afficher les détails des données métriques anormales et le moment où elles se sont produites.
- Choisissez Statistiques ou Dimension pour personnaliser l'affichage du graphique. Pour plus d'informations, consultez la section Statistiques et dimensions du guide de CloudWatch l'utilisateur Amazon.

Groupes de journaux

Lorsque vous activez la détection des anomalies dans les journaux, DevOps Guru balise vos groupes de CloudWatch journaux afin que vous puissiez consulter les groupes de journaux liés à vos informations. Dans la section Groupes de journaux de la page de détails des informations, chaque ligne du tableau représente un groupe de journaux et répertorie la ressource associée.

Lorsqu'il existe plusieurs groupes de journaux anormaux en même temps, la vue chronologique les regroupe et les présente dans une chronologie unique pour faciliter l'analyse. Les lignes violettes sur une chronologie indiquent les périodes pendant lesquelles un groupe de logs a connu des anomalies logarithmiques.

Choisissez une ligne violette dans la chronologie pour afficher un échantillon d'informations sur les anomalies du journal, telles que les exceptions aux mots clés et les écarts numériques. Choisissez Afficher les détails du groupe de journaux pour afficher les anomalies du journal. Dans la fenêtre qui s'ouvre, vous pouvez :

- Affichez un graphique des anomalies du journal et des événements pertinents.
- Passez la souris sur le graphique pour afficher les détails des données du journal anormal et la date à laquelle elles se sont produites.
- Visualisez les anomalies du journal en détail avec des exemples de messages, la fréquence des événements, les recommandations associées et l'heure de leur survenue.
- Cliquez sur Afficher les détails CloudWatch pour afficher les lignes de journal d'une anomalie du journal.

Évènements connexes

Dans Événements connexes, consultez les AWS CloudTrail événements liés à vos informations. Utilisez ces événements pour comprendre, diagnostiquer et traiter la cause sous-jacente du comportement anormal.

Recommandations

Dans Recommandations, vous pouvez consulter les suggestions susceptibles de vous aider à résoudre le problème sous-jacent. Lorsque DevOps Guru détecte un comportement anormal,

il tente de créer des recommandations. Un aperçu peut contenir une, plusieurs ou aucune recommandation.

Comprendre comment les comportements anormaux sont regroupés en informations

Un aperçu est regroupé au niveau de la pile ou au niveau du compte. Si un aperçu est généré pour une ressource figurant dans une AWS CloudFormation pile, il s'agit d'un aperçu au niveau de la pile. Dans le cas contraire, il s'agit d'un aperçu au niveau du compte.

La manière dont une pile est regroupée peut dépendre de la façon dont vous avez configuré votre couverture d'analyse des ressources dans Amazon DevOps Guru.

Si votre couverture est définie par des CloudFormation cumuls

Toutes les ressources contenues dans les piles que vous choisissez sont analysées et toutes les informations détectées sont regroupées au niveau de la pile.

Si votre couverture concerne votre AWS compte courant et votre région

Toutes les ressources de votre compte et de votre région sont analysées, et il existe trois scénarios de regroupement possibles pour les informations détectées.

- Les informations générées à partir d'une ressource qui ne fait pas partie d'une pile sont regroupées au niveau du compte.
- Les informations générées à partir d'une ressource figurant dans l'une des 10 000 premières piles analysées sont regroupées au niveau de la pile.
- Les informations générées à partir d'une ressource qui ne figure pas dans l'une des 10 000 premières piles analysées sont regroupées au niveau du compte. Par exemple, un aperçu généré pour une ressource de la 10 001e pile analysée est regroupé au niveau du compte.

Pour de plus amples informations, veuillez consulter Déterminer la couverture pour DevOps Guru.

Comprendre la sévérité des informations

Un aperçu peut avoir l'une des trois sévérités suivantes : élevée, moyenne ou faible. Amazon DevOps Guru crée un aperçu après avoir détecté les anomalies associées et attribué une gravité à chaque anomalie. DevOpsGuru attribue à une anomalie une gravité élevée, moyenne ou faible en

s'appuyant sur des connaissances du domaine et des années d'expérience collective. La gravité d'un aperçu est déterminée par l'anomalie la plus grave qui a contribué à la création de l'aperçu.

- Si la gravité de toutes les anomalies qui ont généré l'aperçu est faible, alors la gravité de l'aperçu est faible.
- Si la gravité la plus élevée de toutes les anomalies qui ont généré l'aperçu est moyenne, alors la gravité de l'aperçu est moyenne. La gravité de certaines des anomalies à l'origine de l'information peut être faible.
- Si la gravité la plus élevée de toutes les anomalies qui ont généré l'aperçu est élevée, alors la gravité de l'aperçu est élevée. La gravité de certaines des anomalies à l'origine de l'information peut être faible ou moyenne.

Surveillance des bases de données avec DevOps Guru

DevOpsGuru apporte une valeur significative pour l'exploitation de bases de données sur AWS. En tirant parti de ses algorithmes d'apprentissage automatique, DevOps Guru peut aider à optimiser les performances des bases de données, à améliorer la fiabilité et à réduire les frais opérationnels. Cette section du guide de l'utilisateur fournit une présentation détaillée de ces fonctionnalités de base de données, y compris des cas d'utilisation spécifiques de DevOps Guru pour différents services AWS de base de données.

DevOpsGuru peut fournir des informations pour les bases de données relationnelles telles qu'Amazon RDS et. Amazon Redshift Il peut également fournir des informations pour les bases de données non relationnelles ou NoSQL telles que et. Amazon DynamoDB Amazon ElastiCache

Rubriques

- Surveillance des bases de données relationnelles à l'aide de Guru DevOps
- Surveillance de bases de données non relationnelles à l'aide de Guru DevOps

Surveillance des bases de données relationnelles à l'aide de Guru DevOps

DevOpsGuru s'appuie sur deux sources de données principales pour rechercher des informations et des anomalies dans les bases de données relationnelles. Pour Amazon RDS et Amazon Amazon Redshift, les métriques CloudWatch vendues sont analysées pour tous les types d'instances. Pour Amazon RDS, les données Performance Insights sont également ingérées pour les types de moteurs suivants : RDS pour PostgreSQL, Aurora PostgreSQL et Aurora MySQL.

Surveillance des opérations de base de données dans Amazon RDS

Cette section inclut des informations spécifiques sur les cas d'utilisation et les métriques surveillés dans DevOps Guru for RDS, y compris les données issues des métriques vendues et CloudWatch des Performances Insights. Pour plus d'informations sur DevOps Guru for RDS, notamment sur les concepts clés, les configurations et les avantages, consultezthe section called “Gestion des anomalies dans DevOps Guru for RDS”.

Surveillance du RDS à l'aide des données issues des métriques CloudWatch vendues

DevOpsGuru est capable de surveiller tous les types d'instances RDS en ingérant des CloudWatch métriques par défaut, telles que l'utilisation du processeur et la latence des opérations de lecture et d'écriture. Comme ces métriques sont fournies par défaut, lorsque vous surveillez vos instances RDS avec DevOps Guru, aucune autre configuration n'est requise pour obtenir des informations. DevOpsGuru établit automatiquement une base de référence pour ces indicateurs sur la base de modèles historiques et les compare aux données en temps réel afin de détecter les anomalies et les problèmes potentiels dans votre base de données.

Le tableau suivant présente une liste d'informations réactives potentielles pour Amazon RDS à partir de métriques CloudWatch vendues.

AWS ressource surveillée par DevOps Guru	Scénario identifié par DevOps Guru	CloudWatch métriques surveillées
Amazon RDS (tous les types d'instances)	Le processeur ou la mémoire atteignent leurs limites	DBLoad, DBLoad processeur
RDS pour PostgreSQL	Retard élevé entre les emplacements de réplication	OldestReplicationSlotLag

Mesures supplémentaires CloudWatch vendues à partir d'instances Amazon RDS surveillées par DevOps Guru :

- CPUUtilization
- DatabaseConnections
- DiskQueueDepth
- Échoué SQLServer AgentJobsCount
- ReadLatency
- ReadThroughput
- ReplicaLag
- WriteLatency

Surveillance du RDS à l'aide des données de Performance Insights

Pour certains types d'instances Amazon RDS, tels qu'Aurora PostgreSQL, Aurora MySQL et RDS pour PostgreSQL, vous pouvez tirer davantage parti de la surveillance DevOps Guru en vous assurant que Performance Insights est activé sur ces instances.

DevOpsGuru fournit des informations réactives pour diverses situations, notamment les scénarios suivants :

Scénario que DevOps Guru identifie pour générer un aperçu réactif
Problème de contention lié au verrouillage
Index manquant
Mauvaise configuration du pool d'applications
Valeurs JDBC par défaut sous-optimales

DevOpsGuru fournit des informations proactives pour diverses situations, notamment les scénarios suivants :

AWS ressource surveillée par DevOps Guru	Scénario que DevOps Guru identifie pour générer un aperçu proactif
Aurora MySQL	La liste d'historique d'InnoDB devient trop longue, ce qui peut entraîner une dégradation des performances, telle qu'un long délai d'arrêt de la base de données
Aurora MySQL	Augmentation du nombre de tables temporair es créées sur le disque qui peut avoir un impact sur les performances de la base de données
RDS pour PostgreSQL, Aurora PostgreSQL	Connexion inactive pendant une transacti on trop longue, impact potentiel du maintien des verrous, du blocage d'autres requêtes et de l'impossibilité pour le système Vacuum (y

AWS ressource surveillée par DevOps Guru	Scénario que DevOps Guru identifie pour générer un aperçu proactif
	compris Autovacuum) de nettoyer les lignes mortes

Surveillance des opérations de base de données dans Amazon Redshift

DevOpsGuru est capable de surveiller vos Amazon Redshift ressources en ingérant des CloudWatch métriques par défaut, notamment l'utilisation du processeur et le pourcentage d'espace disque utilisé. Comme ces métriques sont fournies par défaut, aucune autre configuration n'est requise pour que DevOps Guru surveille automatiquement vos Amazon Redshift ressources. DevOpsGuru établit une base de référence pour ces indicateurs sur la base de modèles historiques et les compare aux données en temps réel afin de détecter les anomalies.

Scénario identifié par DevOps Guru	CloudWatch métriques surveillées
Détectez l'utilisation élevée du processeur d'une Amazon Redshift instance due à des facteurs tels que la charge de travail du cluster, les données asymétriques et non triées ou les tâches du nœud principal	CPUUtilization
Détectez lorsqu'une Amazon Redshift instance manque d'espace disque en raison de problèmes liés au traitement des requêtes, à la distribution et à la clé de tri, aux opérations de maintenance ou aux blocs de pierre angulaire	PercentageDiskSpaceUsed

Mesures supplémentaires CloudWatch vendues à partir d' Amazon Redshift instances surveillées par DevOps Guru :

- DatabaseConnections
- HealthStatus
- MaintenanceMode
- NumExceededSchemaQuotas

- PercentageQuotaUsed
- QueryDuration
- QueryRuntimeBreakdown
- ReadIOPS
- ReadLatency
- WLMQueueLongueur
- WLMQueueWaitTime
- WLMQueryDurée
- WriteLatency

Gestion des anomalies dans DevOps Guru for RDS

DevOpsGuru détecte, analyse et fournit des recommandations pour les AWS ressources prises en charge, notamment les moteurs Amazon RDS. Pour les instances de base de données Amazon Aurora et RDS pour PostgreSQL sur lesquelles Performance Insights est activé DevOps, Guru for RDS fournit des analyses détaillées et spécifiques à la base de données des problèmes de performance et recommande des mesures correctives.

Rubriques

- Présentation de DevOps Guru for RDS
- Enabling DevOps Guru pour RDS
- Analyse des anomalies dans Amazon RDS

Présentation de DevOps Guru for RDS

Vous trouverez ci-dessous un résumé des principaux avantages et fonctionnalités de DevOps Guru for RDS. Pour plus d'informations sur les informations et les anomalies, voirDevOpsLes concepts du gourou.

Rubriques

- Avantages de DevOps Guru for RDS
- Concepts clés pour le réglage des performances des bases de données
- Concepts clés de DevOps Guru for RDS
- Comment fonctionne DevOps Guru for RDS

- Moteurs de base de données pris en charge

Avantages de DevOps Guru for RDS

Si vous êtes responsable d'une base de données Amazon RDS, vous ne savez peut-être pas qu'un événement ou une régression affectant cette base de données est en train de se produire. Lorsque vous prenez connaissance de ce problème, vous ne savez pas toujours pourquoi il se produit ni comment y remédier. Plutôt que de vous adresser à un administrateur de base de données (DBA) pour obtenir de l'aide ou de vous fier à des outils tiers, vous pouvez suivre les recommandations de DevOps Guru for RDS.

L'analyse détaillée de DevOps Guru for RDS vous apporte les avantages suivants :

Diagnostic rapide

DevOpsGuru for RDS surveille et analyse en permanence la télémétrie des bases de données. Performance Insights, Enhanced Monitoring et Amazon CloudWatch collectent des données de télémétrie pour vos instances de base de données. DevOpsGuru for RDS utilise des techniques statistiques et d'apprentissage automatique pour exploiter ces données et détecter les anomalies. Pour en savoir plus sur les données de télémétrie pour les bases de données Amazon Aurora, consultez les sections Surveillance de la charge de base de données avec Performance Insights sur Amazon Aurora et Surveillance du système d'exploitation à l'aide de la surveillance améliorée dans le guide de l'utilisateur Amazon Aurora. Pour en savoir plus sur les données de télémétrie d'autres bases de données Amazon RDS, consultez les sections Surveillance de la charge de base de données avec Performance Insights on Amazon Relational Database Service et Surveillance des métriques du système d'exploitation avec surveillance améliorée dans le guide de l'utilisateur Amazon RDS.

Résolution rapide

Chaque anomalie identifie le problème de performances et suggère des pistes d’enquête ou des actions correctives. Par exemple, DevOps Guru for RDS peut vous recommander d'étudier des événements d'attente spécifiques. Il peut également vous recommander de régler les paramètres de votre groupe d’applications afin de limiter le nombre de connexions à la base de données. Sur la base de ces recommandations, vous pouvez résoudre les problèmes de performances plus rapidement qu’en effectuant un dépannage manuel.

Insights proactifs

DevOpsGuru for RDS utilise les indicateurs de vos ressources pour détecter les comportements potentiellement problématiques avant qu'ils ne s'aggravent. Par exemple, il peut détecter les cas où les sessions connectées à la base de données n'effectuent pas de travail actif et peuvent bloquer les ressources de la base de données. DevOps Guru fournit ensuite des recommandations pour vous aider à résoudre les problèmes avant qu'ils ne s'aggravent.

Connaissance approfondie des ingénieurs Amazon et du machine learning

Pour détecter les problèmes de performance et vous aider à résoudre les goulots d'étranglement, DevOps Guru for RDS s'appuie sur l'apprentissage automatique (ML) et sur des analyses statistiques avancées. Les ingénieurs de base de données Amazon ont contribué au développement des résultats de DevOps Guru for RDS, qui résument de nombreuses années de gestion de centaines de milliers de bases de données. En s'appuyant sur ces connaissances collectives, DevOps Guru for RDS peut vous enseigner les meilleures pratiques.

Concepts clés pour le réglage des performances des bases de données

DevOpsGuru for RDS part du principe que vous connaissez quelques concepts de performance clés. Pour en savoir plus sur ces concepts, consultez Overview of Performance Insights dans le guide de l'utilisateur Amazon Aurora ou Overview of Performance Insights dans le guide de l'utilisateur Amazon RDS.

Rubriques

- Métriques
- Détection des problèmes
- Charge de la base de données
- Événements d’attente

Métriques

Une métrique représente un ensemble de points de données ordonnés dans le temps. Envisagez une métrique comme une variable à surveiller et les points de données comme les valeurs de cette variable au fil du temps. Amazon RDS fournit des métriques en temps réel pour la base de données et pour le système d'exploitation (OS) sur lequel votre instance de base de données s'exécute. Vous pouvez consulter toutes les métriques du système et les informations de processus pour

vos instances de base de données Amazon RDS sur la console Amazon RDS. DevOps Guru for RDS surveille et fournit des informations sur certaines de ces métriques. Pour plus d'informations, consultez Surveillance des métriques dans un cluster Amazon Aurora ou Surveillance des métriques dans une instance Amazon Relational Database Service.

Détection des problèmes

DevOpsGuru for RDS utilise des métriques de base de données et de système d'exploitation (OS) pour détecter les problèmes critiques de performance des bases de données, qu'ils soient imminents ou permanents. La détection des problèmes par DevOps Guru for RDS fonctionne principalement de deux manières :

- Utilisation de seuils
- Utilisation des anomalies

Détecter les problèmes liés aux seuils

Les seuils sont les valeurs limites par rapport auxquelles les mesures surveillées sont évaluées. Vous pouvez considérer un seuil comme une ligne horizontale sur un graphique métrique qui sépare un comportement normal d'un comportement potentiellement problématique. DevOps Guru for RDS surveille des métriques spécifiques et crée des seuils en analysant les niveaux considérés comme potentiellement problématiques pour une ressource spécifique. DevOpsGuru for RDS crée ensuite des informations dans la console DevOps Guru lorsque de nouvelles valeurs métriques franchissent un seuil spécifié sur une période donnée de manière cohérente. Les informations contiennent des recommandations visant à éviter tout impact futur sur les performances des bases de données.

Par exemple, DevOps Guru for RDS peut surveiller le nombre de tables temporaires utilisant le disque sur une période de 15 minutes et créer un aperçu lorsque le taux de tables temporaires utilisant le disque par seconde est anormalement élevé. L'augmentation des niveaux d'utilisation des tables temporaires sur disque peut avoir un impact sur les performances de la base de données. En exposant cette situation avant qu'elle ne devienne critique, DevOps Guru for RDS vous aide à prendre des mesures correctives pour éviter les problèmes.

Détecter les problèmes liés aux anomalies

Bien que les seuils constituent un moyen simple et efficace de détecter les problèmes de base de données, ils ne sont pas suffisants dans certains cas. Imaginons le cas où les valeurs métriques augmentent et se transforment régulièrement en comportements potentiellement problématiques en raison d'un processus connu, tel qu'un travail de reporting quotidien. Étant donné que de tels

pics sont attendus, la création d'informations et de notifications pour chacun d'entre eux serait contreproductive et conduirait probablement à une lassitude face aux alertes.

Cependant, il est toujours nécessaire de détecter les pics très inhabituels, car des métriques beaucoup plus élevées que les autres ou qui durent beaucoup plus longtemps peuvent représenter de véritables problèmes de performance des bases de données. Pour répondre à ce problème, DevOps Guru for RDS surveille certaines métriques afin de détecter les cas où le comportement d'une métrique devient très inhabituel ou anormal. DevOpsGuru rapporte ensuite ces anomalies dans Insights.

Par exemple, DevOps Guru for RDS peut créer un aperçu lorsque la charge de base de données est non seulement élevée, mais qu'elle s'écarte également de manière significative de son comportement habituel, ce qui indique un ralentissement inattendu majeur des opérations de base de données. En reconnaissant uniquement les pics de charge anormaux dans les bases de données, DevOps Guru for RDS vous permet de vous concentrer sur les problèmes réellement importants.

Charge de la base de données

Le concept clé pour le réglage des bases de données est la métrique de charge de base de données (charge de base de données). La charge de base de données représente le niveau d'activité de votre base de données à un moment donné. Une augmentation de la charge de base de données signifie une augmentation de l'activité de la base de données.

Une session de base de données représente le dialogue d'une application avec une base de données relationnelle. Une session active est une session en cours d'exécution d'une demande de base de données. Une session est active lorsqu'elle s'exécute sur le processeur (CPU) ou attend qu'une ressource devienne disponible pour pouvoir continuer. Par exemple, une session active peut attendre qu'une page soit lue en mémoire avant d'utiliser le processeur pendant la lecture des données de la page.

La `DBLoad` métrique de Performance Insights est mesurée en nombre moyen de sessions actives (AAS). Pour calculer l'AAS, Performance Insights échantillonne le nombre de sessions actives chaque seconde. Pour une période donnée, l'AAS est le nombre total de sessions actives divisé par le nombre total d'échantillons. Une valeur AAS de 2 signifie qu'en moyenne, 2 sessions étaient actives dans les demandes à un moment donné.

L'activité au sein d'un entrepôt représente une bonne analogie avec la charge de base de données. Supposons qu'un entrepôt emploie 100 employés. Lorsqu'une commande est réceptionnée, elle traitée par un employés et les autres sont inactifs. Si 100 commandes ou plus arrivent, les 100

travailleurs exécutent les commandes simultanément. Si vous échantillonnez périodiquement le nombre d'employés actifs sur une période donnée, vous pouvez calculer le nombre moyen d'employés actifs. Le calcul montre qu'en moyenne, N employés sont occupés à traiter des commandes à un moment donné. Si la moyenne était de 50 employés hier et qu'elle est aujourd'hui de 75 employés, cela indique le niveau d'activité dans l'entrepôt a augmenté. De la même manière, la charge de la base de données augmente à mesure que l'activité de la session augmente.

Pour en savoir plus, consultez la section Chargement de base de données dans le guide de l'utilisateur Amazon Aurora ou Chargement de base de données dans le guide de l'utilisateur Amazon RDS.

Événements d’attente

Un événement d'attente est un type d'instrumentation de base de données qui vous indique la ressource qu'une session de base de données attend pour pouvoir continuer. Lorsque Performance Insights compte les sessions actives pour calculer la charge de la base de données, il enregistre également les événements d'attente à l'origine de l'attente des sessions actives. Cette technique permet à Performance Insights de vous montrer quels événements d'attente contribuent à la charge de la base de données.

Chaque session active est soit en cours d’exécution au niveau du processeur soit en attente. Par exemple, les sessions consomment du processeur lorsqu'elles recherchent de la mémoire, effectuent un calcul ou exécutent du code procédural. Lorsque les sessions ne consomment pas de CPU, elles peuvent attendre la lecture d'un fichier de données ou l'écriture d'un journal. Le temps que passe une session à attendre des ressources est autant de temps en moins qu’elle passe à s’exécuter au niveau du processeur.

Lorsque vous réglez une base de données, vous essayez souvent de trouver les ressources que les sessions attendent. Par exemple, deux ou trois événements d'attente peuvent représenter 90 % de la charge de base de données. Cette mesure signifie qu’en moyenne, les sessions actives passent la majeure partie de leur temps à attendre un petit nombre de ressources. Si vous pouvez découvrir la cause de ces attentes, vous pouvez essayer de remédier au problème.

Considérez l'analogie avec un magasinier. Une commande de livre est réceptionnée. L'employé peut être retardé dans le traitement de la commande. Par exemple, il se peut qu'un autre travailleur réapprovisionne actuellement les étagères ou qu'un chariot ne soit pas disponible. ou le système servant à saisir l'état des commandes se montre très lent. Plus le travailleur attend, plus la commande met du temps à être exécutée. L'attente fait naturellement partie du flux de travail de l'entrepôt, mais si le temps d'attente devient excessif, la productivité diminue. De la même manière,

les attentes longues ou répétées d'une session peuvent dégrader les performances de la base de données.

Pour plus d'informations sur les événements d'attente dans Amazon Aurora, consultez les sections Tuning with wait events for Aurora PostgreSQL et Tuning with wait events for Aurora MySQL dans le guide de l'utilisateur Amazon Aurora.

Pour plus d'informations sur les événements d'attente dans d'autres bases de données Amazon RDS, consultez la section Tuning with wait events for RDS for PostgreSQL dans le guide de l'utilisateur Amazon RDS.

Concepts clés de DevOps Guru for RDS

Un aperçu est généré par DevOps Guru lorsqu'il détecte un comportement anormal ou problématique dans vos applications opérationnelles. Un aperçu contient des anomalies pour une ou plusieurs ressources. Une anomalie représente une ou plusieurs mesures connexes détectées par DevOps Guru qui sont inattendues ou inhabituelles.

La sévérité d'un aperçu est élevée, moyenne ou faible. La gravité de l'aperçu est déterminée par l'anomalie la plus grave qui a contribué à la création de l'aperçu. Par exemple, si l'aperçu AWS-ECS_ MemoryUtilization _and_others inclut une anomalie de faible gravité et une autre de gravité élevée, la gravité globale de l'aperçu est élevée.

Si les instances de base de données Amazon RDS ont activé Performance Insights, DevOps Guru for RDS fournit une analyse détaillée et des recommandations concernant les anomalies associées à ces instances. Pour identifier une anomalie, DevOps Guru for RDS développe une base de référence pour les valeurs métriques de base de données. DevOpsGuru for RDS compare ensuite les valeurs métriques actuelles à la base de référence historique.

Rubriques

- Insights proactifs
- Insights réactifs
- Recommandations

Insights proactifs

Un insight proactif vous permet de connaître un comportement problématique avant qu'il se produise. Il contient des anomalies avec des recommandations et des mesures connexes pour vous aider à résoudre les problèmes avant qu'ils ne s'aggravent.

Chaque page d'information proactive fournit des informations détaillées sur une anomalie.

Insights réactifs

Un insight réactif identifie un comportement anormal lorsqu’il se produit. Il contient des anomalies avec des recommandations, des indicateurs connexes et des événements pour vous aider à comprendre et à résoudre les problèmes dès maintenant.

Anomalies causales

Une anomalie causale est une anomalie de premier niveau au sein d’un insight réactif. Elle est affichée en tant que métrique principale sur la page de détails des anomalies de la console DevOps Guru. Le chargement de la base de données (charge de base de données) est l'anomalie causale de DevOps Guru for RDS. Par exemple, l'aperçu AWS-ECS_ MemoryUtilization _and_others peut présenter plusieurs anomalies métriques, dont l'une est le chargement de base de données (charge de base de données) pour la ressource AWS/RDS.

D'après un aperçu, l'anomalie de charge de la base de données (charge de base de données) peut se produire pour plusieurs instances de base de données Amazon RDS. La gravité de l'anomalie peut être différente pour chaque instance de base de données. Par exemple, la gravité d'une instance de base de données peut être élevée alors que la gravité des autres est faible. La console détecte par défaut l'anomalie la plus grave.

Anomalies contextuelles

Une anomalie contextuelle est un résultat dans la charge de base de données qui est associé à un insight réactif. Il est affiché dans la section Métriques associées de la page de détails des anomalies de la console DevOps Guru. Chaque anomalie contextuelle décrit un problème de performance Amazon RDS spécifique qui nécessite une enquête. Par exemple, une anomalie causale peut inclure les anomalies contextuelles suivantes :

- Capacité du processeur dépassée : la file d'attente ou l'utilisation du processeur sont supérieures à la normale.
- Mémoire insuffisante dans la base de données : les processus ne disposent pas de suffisamment de mémoire.
- Nombre élevé de connexions à la base de données : le nombre de connexions à la base de données est supérieur à la normale.

Recommandations

Chaque aperçu comporte au moins une action suggérée. Les exemples suivants sont des recommandations générées par DevOps Guru for RDS :

- Réglez le SQL IDs *`list_of_IDs`* pour réduire l'utilisation du processeur ou mettez à niveau le type d'instance pour augmenter la capacité du processeur.
- Passez en revue le pic associé de connexions actuelles à la base de données. Envisagez de régler les paramètres du pool d'applications pour éviter l'allocation dynamique fréquente de nouvelles connexions à la base de données.
- Recherchez les instructions SQL qui exécutent des opérations de mémoire excessives, telles que le tri en mémoire ou les jointures volumineuses.
- Étudiez l' I/O utilisation intensive du code SQL suivant IDs :*`list_of_IDs`*.
- Vérifiez les instructions qui créent de grandes quantités de données temporaires, par exemple celles qui effectuent des tris importants ou utilisent de grandes tables temporaires.
- Vérifiez les applications pour déterminer la cause de l'augmentation de la charge de travail de la base de données.
- Envisagez d'activer le schéma de performance MySQL.
- Vérifiez les transactions de longue durée et terminez-les par un commit ou un rollback.
- Configurez le paramètre idle_in_transaction_session_timeout pour mettre fin à toute session restée dans l'état « inactive en cours de transaction » pendant plus longtemps que la durée spécifiée.

Comment fonctionne DevOps Guru for RDS

DevOpsGuru for RDS collecte des données métriques, les analyse, puis publie les anomalies dans le tableau de bord.

Rubriques

- Collecte et analyse de données
- Publication d'anomalies

Collecte et analyse de données

DevOpsGuru for RDS collecte des données sur vos bases de données Amazon RDS à partir d'Amazon RDS Performance Insights. Cette fonctionnalité surveille les instances de base de données Amazon RDS, collecte les métriques et vous permet d'explorer les métriques dans un graphique.

L'indicateur de performance le plus important est`DBLoad`. DevOpsGuru for RDS utilise les métriques Performance Insights et les analyse pour détecter les anomalies. Pour plus d'informations sur Performance Insights, consultez Surveillance de la charge de base de données avec Performance Insights sur Amazon Aurora dans le guide de l'utilisateur Amazon Aurora ou Surveillance de la charge de base de données avec Performance Insights sur Amazon RDS dans le guide de l'utilisateur Amazon RDS.

DevOpsGuru for RDS utilise l'apprentissage automatique et l'analyse statistique avancée pour analyser les données collectées à partir de Performance Insights. Si DevOps Guru for RDS détecte des problèmes de performances, il passe à l'étape suivante.

Publication d'anomalies

Un problème de performance de base de données, tel qu'une charge de base de données élevée, peut dégrader la qualité de service de votre base de données. Lorsque DevOps Guru détecte un problème dans une base de données RDS, il publie un aperçu dans le tableau de bord. L'aperçu contient une anomalie pour la ressource AWS/RDS.

Si Performance Insights est activé pour vos instances, l'anomalie contient une analyse détaillée du problème. DevOps Guru for RDS vous recommande également de mener une enquête ou de prendre des mesures correctives spécifiques. Par exemple, il peut être recommandé d'étudier une instruction SQL spécifique à forte charge, d'envisager d'augmenter la capacité du processeur ou de fermer idle-in-transaction des sessions.

Moteurs de base de données pris en charge

DevOpsGuru for RDS est compatible avec les moteurs de base de données suivants :

Amazon Aurora avec compatibilité MySQL

Pour en savoir plus sur ce moteur, consultez la section Utilisation d'Amazon Aurora MySQL dans le guide de l'utilisateur Amazon Aurora.

Amazon Aurora avec compatibilité PostgreSQL

Pour en savoir plus sur ce moteur, consultez la section Utilisation d'Amazon Aurora PostgreSQL dans le guide de l'utilisateur Amazon Aurora.

Compatibilité avec Amazon RDS for PostgreSQL

Pour en savoir plus sur ce moteur, consultez Amazon RDS for PostgreSQLle guide de l'utilisateur Amazon RDS.

DevOpsGuru signale les anomalies et fournit des analyses de base pour les autres moteurs de base de données. DevOpsGuru for RDS fournit des analyses détaillées et des recommandations uniquement pour les instances Amazon Aurora et RDS pour PostgreSQL.

Enabling DevOps Guru pour RDS

Lorsque vous activez DevOps Guru pour RDS, vous permettez à DevOps Guru d'analyser les anomalies dans les ressources telles que les instances de base de données. Amazon RDS permet de découvrir et d'activer facilement les fonctionnalités recommandées pour une instance de base de données ou un cluster de base de données RDS. Pour ce faire, RDS effectue des appels d'API vers d'autres services, tels qu'Amazon EC2 DevOps, Guru et IAM. Lorsque la console RDS effectue ces appels d'API, elle les AWS CloudTrail enregistre à des fins de visibilité.

Pour permettre à DevOps Guru de publier des informations pour une base de données Amazon RDS, effectuez les tâches décrites dans les sections suivantes.

Rubriques

- Activer Performance Insights pour vos instances de base de données Amazon RDS
- Configuration des politiques d'accès pour DevOps Guru for RDS
- Ajouter des instances de base de données Amazon RDS à votre couverture DevOps Guru

Activer Performance Insights pour vos instances de base de données Amazon RDS

Pour que DevOps Guru for RDS puisse analyser les anomalies sur une instance de base de données, assurez-vous que Performance Insights est activé. Si Performance Insights n'est pas activé pour une instance de base de données, DevOps Guru for RDS vous en informe aux endroits suivants :

Tableau de bord

Si vous consultez les informations par type de ressource, la vignette RDS vous avertit que Performance Insights n'est pas activé. Cliquez sur le lien pour activer Performance Insights dans la console Amazon RDS.

Informations

Dans la section Recommandations au bas de la page, choisissez Enable Amazon RDS Performance Insights.

Settings

Dans la section Service : Amazon RDS, choisissez le lien pour activer Performance Insights dans la console Amazon RDS.

Pour plus d'informations, consultez Turning Performance Insights dans le guide de l'utilisateur Amazon Aurora ou Turning Performance Insights dans le guide de l'utilisateur Amazon RDS.

Configuration des politiques d'accès pour DevOps Guru for RDS

Pour qu'un utilisateur puisse accéder à DevOps Guru for RDS, il doit être autorisé par l'une des politiques suivantes :

- La politique AWS gérée `AmazonRDSFullAccess`
- Politique gérée par le client permettant les actions suivantes :
  - `pi:GetResourceMetrics`
  - `pi:DescribeDimensionKeys`
  - `pi:GetDimensionKeyDetails`

Pour plus d'informations, consultez Configuration des politiques d'accès pour Performance Insights dans le guide de l'utilisateur Amazon Aurora ou Configuration des politiques d'accès pour Performance Insights dans le guide de l'utilisateur Amazon RDS.

Ajouter des instances de base de données Amazon RDS à votre couverture DevOps Guru

Vous pouvez configurer DevOps Guru pour surveiller vos bases de données Amazon RDS soit dans la console DevOps Guru, soit dans la console Amazon RDS.

Dans la console DevOps Guru, vous disposez des options suivantes :

- Activez DevOps Guru au niveau du compte. Il s'agit de l'option par défaut. Lorsque vous choisissez cette option, DevOps Guru analyse toutes les AWS ressources prises en charge dans votre compte Compte AWS, y compris Région AWS les bases de données Amazon RDS.
- Spécifiez AWS CloudFormation les piles pour DevOps Guru for RDS.

  Pour de plus amples informations, veuillez consulter Utiliser des CloudFormation piles pour identifier les ressources dans vos applications DevOps Guru.
- Marquez vos ressources Amazon RDS.

Une balise est une étiquette d'attribut personnalisée que vous attribuez à une AWS ressource. Utilisez des balises pour identifier les AWS ressources qui constituent votre application. Vous pouvez ensuite filtrer vos informations par balise pour n'afficher que celles créées par votre application. Pour afficher uniquement les informations générées par les ressources Amazon RDS de votre application, ajoutez une valeur, par exemple `Devops-guru-rds` à vos balises de ressources Amazon RDS. Pour de plus amples informations, veuillez consulter Utiliser des balises pour identifier les ressources dans vos applications DevOps Guru.

> **Note**
>
> Lorsque vous balisez des ressources Amazon RDS, vous devez baliser l'instance de base de données et non le cluster.

Pour activer la surveillance de DevOps Guru depuis la console Amazon RDS, consultez la section Activation de DevOps Guru dans la console RDS. Notez que pour activer DevOps Guru depuis la console Amazon RDS, vous devez utiliser des balises. Pour en savoir plus sur les identifications, consultez the section called “Utiliser des balises pour identifier les ressources de vos applications”.

Analyse des anomalies dans Amazon RDS

Lorsque DevOps Guru for RDS publie une anomalie de performance dans le tableau de bord, vous effectuez généralement les étapes suivantes :

1. Consultez les informations dans le tableau de bord DevOps Guru. DevOpsGuru for RDS fournit des informations à la fois réactives et proactives.

   Pour de plus amples informations, veuillez consulter Visualisation des informations.
2. Afficher les anomalies relatives aux ressources AWS/RDS.

   Pour plus d’informations, consultez Visualisation des anomalies réactives et Visualisation proactive des anomalies.
3. Répondez aux recommandations de DevOps Guru pour obtenir des recommandations RDS.

   Pour de plus amples informations, veuillez consulter Réponse aux recommandations.
4. Surveillez l'état de vos instances de base de données pour vous assurer que les problèmes de performances résolus ne se reproduisent pas.

Pour plus d'informations, consultez les sections Surveillance des métriques dans un cluster de base de données Amazon Aurora dans le guide de l'utilisateur Amazon Aurora et Surveillance des métriques dans une instance Amazon RDS dans le guide de l'utilisateur Amazon RDS.

Visualisation des informations

Accédez à la page Insights de la console DevOps Guru pour trouver des informations réactives et proactives. À partir de là, vous pouvez choisir un aperçu dans la liste pour afficher une page détaillée contenant des statistiques, des recommandations et plus d'informations sur cet aperçu.

Pour consulter un aperçu

1. Ouvrez la console Amazon DevOps Guru à l'adresse https://console.aws.amazon.com/devops-guru/.
2. Ouvrez le volet de navigation, puis choisissez Insights.
3. Choisissez l'onglet Réactif pour consulter les informations réactives, ou choisissez Proactive pour afficher les informations proactives.
4. Choisissez le nom d'un aperçu, en le hiérarchisant par statut et par gravité.

   La page d'aperçu détaillé apparaît.

Visualisation des anomalies réactives

Dans un aperçu, vous pouvez visualiser les anomalies relatives aux ressources Amazon RDS. Sur une page d'analyse réactive, dans la section Mesures agrégées, vous pouvez consulter une liste des anomalies avec les chronologies correspondantes. Certaines sections affichent également des informations sur les groupes de journaux et les événements liés aux anomalies. Dans un aperçu réactif, les anomalies causales ont chacune une page correspondante contenant des détails sur l'anomalie.

Visualisation de l'analyse détaillée d'une anomalie réactive du RDS

À ce stade, analysez l'anomalie pour obtenir une analyse détaillée et des recommandations pour vos instances de base de données Amazon RDS.

L'analyse détaillée n'est disponible que pour les instances de base de données Amazon RDS sur lesquelles Performance Insights est activé.

Pour accéder à la page de détails des anomalies

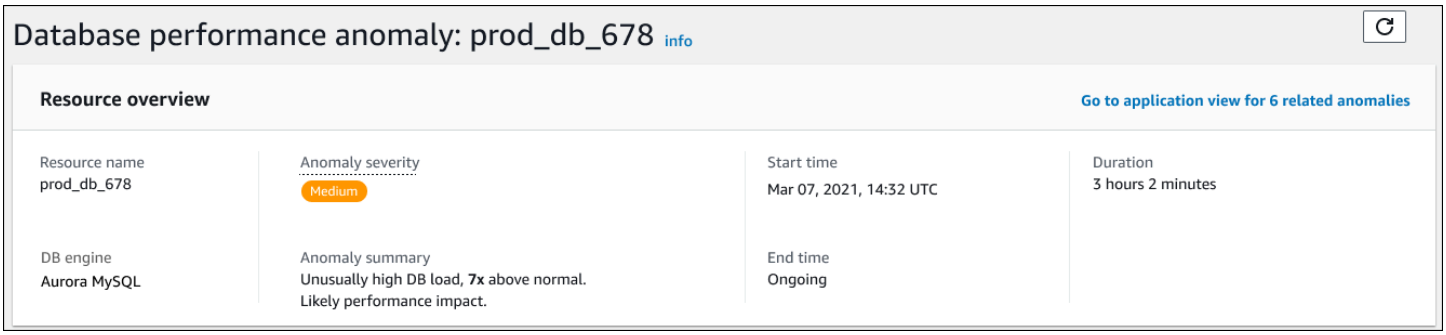
1. Sur la page d'aperçu, recherchez une métrique agrégée avec le type de ressource AWS/RDS.
2. Sélectionnez Afficher les détails.

   La page de détails de l'anomalie apparaît. Le titre commence par Anomalie des performances de la base de données et nomme la ressource affichée. La console détecte par défaut l'anomalie la plus grave, quel que soit le moment où l'anomalie s'est produite.
3. (Facultatif) Si plusieurs ressources sont concernées, choisissez-en une autre dans la liste en haut de la page.

Vous trouverez ci-dessous les descriptions des composants de la page de détails.

Aperçu des ressources

La section supérieure de la page de détails est la vue d'ensemble des ressources. Cette section résume l'anomalie de performance rencontrée par votre instance de base de données Amazon RDS.



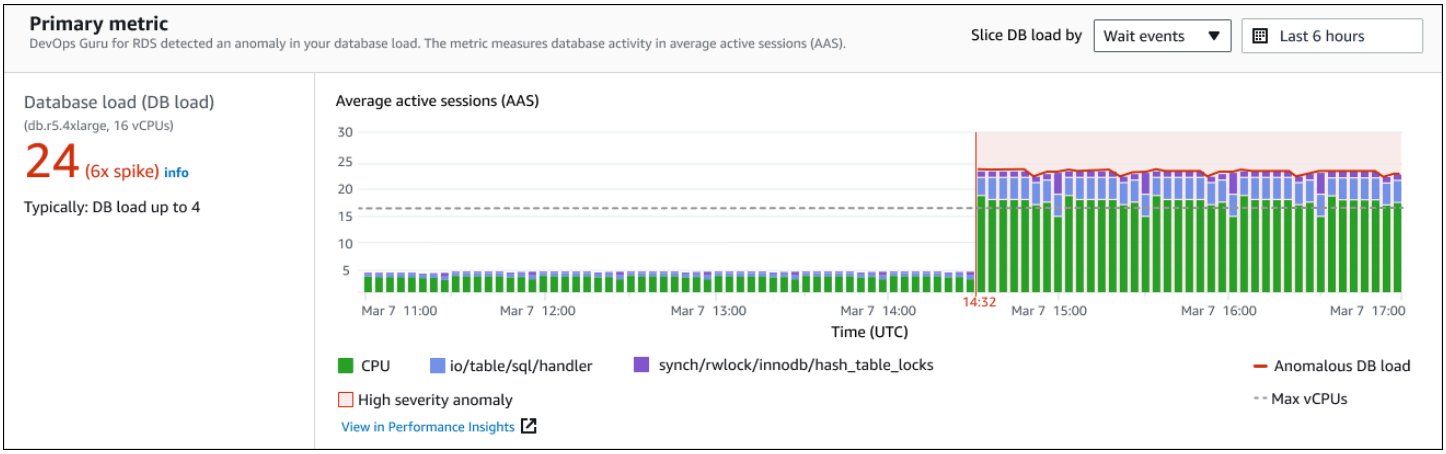
Cette section contient les champs suivants :

- Nom de la ressource : nom de l'instance de base de données qui présente l'anomalie. Dans cet exemple, la ressource s'appelle prod_db_678.
- Moteur de base de données : nom de l'instance de base de données présentant l'anomalie. Dans cet exemple, le moteur est Aurora MySQL.
- Gravité de l'anomalie : mesure de l'impact négatif de l'anomalie sur votre instance. Les sévérités possibles sont élevées, moyennes et faibles.
- Résumé de l'anomalie : bref résumé du problème. Un résumé typique est une charge de base de données anormalement élevée.
- Heure de début et heure de fin : heure de début et de fin de l'anomalie. Si l'heure de fin est en cours, l'anomalie persiste.

- Durée : durée du comportement anormal. Dans cet exemple, l'anomalie est permanente et se produit depuis 3 heures et 2 minutes.

Métrique principale

La section Métrique principale résume l'anomalie occasionnelle, qui est l'anomalie de premier niveau de l'aperçu. Vous pouvez considérer l'anomalie causale comme le problème général rencontré par votre instance de base de données.



Le panneau de gauche fournit plus de détails sur le problème. Dans cet exemple, le résumé inclut les informations suivantes :

- Charge de base de données (charge de base de données) : catégorisation de l'anomalie en tant que problème de chargement de base de données. La métrique correspondante dans Performance Insights est`DBLoad`. Cette statistique est également publiée sur Amazon CloudWatch.
- db.r5.4xlarge — La classe d'instance de base de données. Le nombre de vCPUs, 16 dans cet exemple, correspond à la ligne pointillée du graphique Average active sessions (AAS).
- 24 (6x pic) — La charge de base de données, mesurée en nombre moyen de sessions actives (AAS) pendant l'intervalle de temps indiqué dans l'aperçu. Ainsi, à tout moment pendant la période de l'anomalie, 24 sessions en moyenne étaient actives sur la base de données. La charge de base de données est 6 fois supérieure à la charge de base de données normale pour cette instance.
- Généralement : charge de base de données jusqu'à 4 : valeur de référence de la charge de base de données, mesurée en AAS, pendant une charge de travail typique. La valeur 4 signifie que, pendant les opérations normales, en moyenne 4 sessions ou moins sont actives sur la base de données à un moment donné.

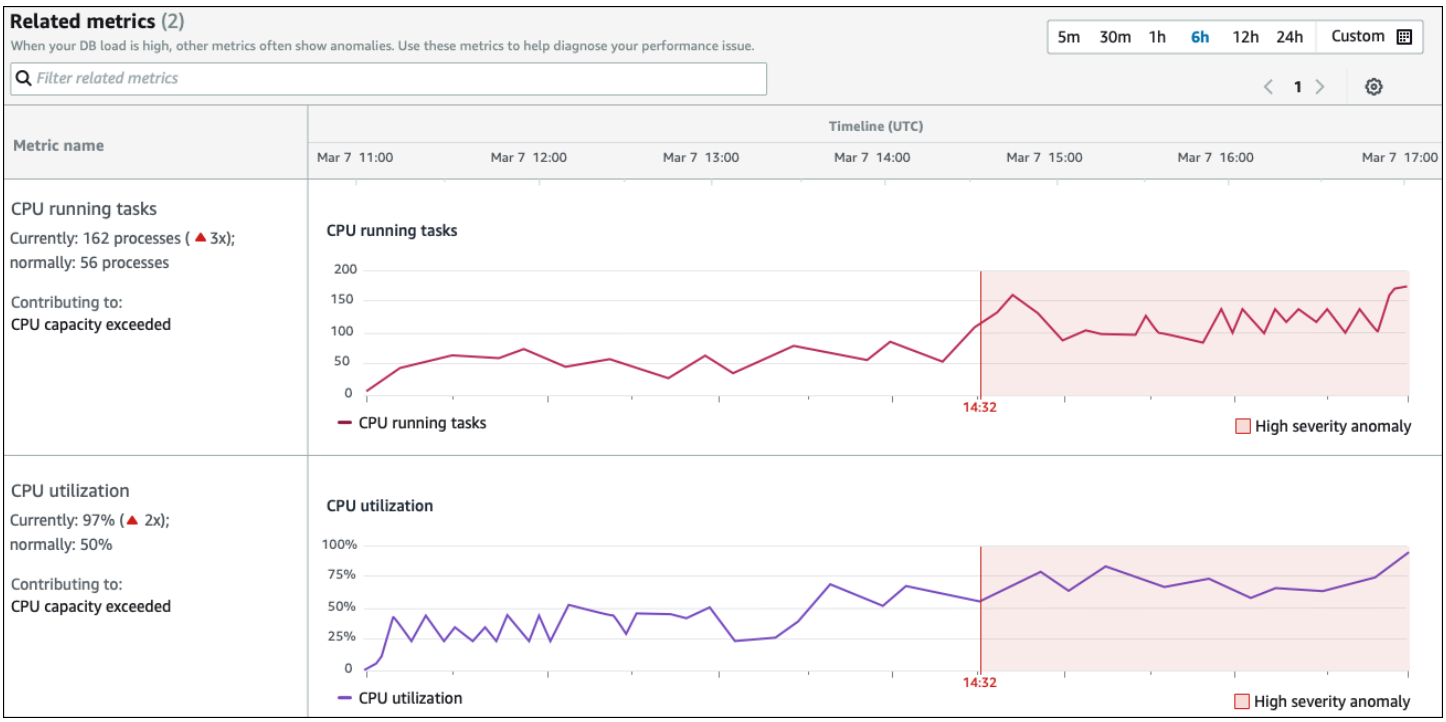
Par défaut, le graphique de charge est découpé en fonction des événements d'attente. Cela signifie que pour chaque barre du graphique, la plus grande zone colorée représente l'événement d'attente qui contribue le plus à la charge totale de la base de données. Le graphique indique l'heure (en rouge) à laquelle le problème a commencé. Concentrez votre attention sur les événements d'attente qui occupent le plus d'espace dans la barre :

- `CPU`
- `IO:wait/io/sql/table/handler`

Les événements d'attente précédents apparaissent plus que d'habitude pour cette base de données Aurora MySQL. Pour savoir comment optimiser les performances à l'aide d'événements d'attente dans Amazon Aurora, consultez les sections Tuning with wait events for Aurora MySQL et Tuning with wait events for Aurora PostgreSQL dans le guide de l'utilisateur Amazon Aurora. Pour savoir comment optimiser les performances à l'aide d'événements d'attente dans RDS pour PostgreSQL, consultez la section Optimisation avec des événements d'attente pour RDS pour PostgreSQL dans le guide de l'utilisateur Amazon RDS.

Métriques associées

La section Paramètres connexes répertorie les anomalies contextuelles, qui sont des constatations spécifiques au sein de l'anomalie causale. Ces résultats fournissent des informations supplémentaires sur les problèmes de performance.



Le tableau des mesures associées comporte deux colonnes : nom des mesures et chronologie (UTC). Chaque ligne du tableau correspond à une métrique spécifique.

La première colonne de chaque ligne contient les informations suivantes :

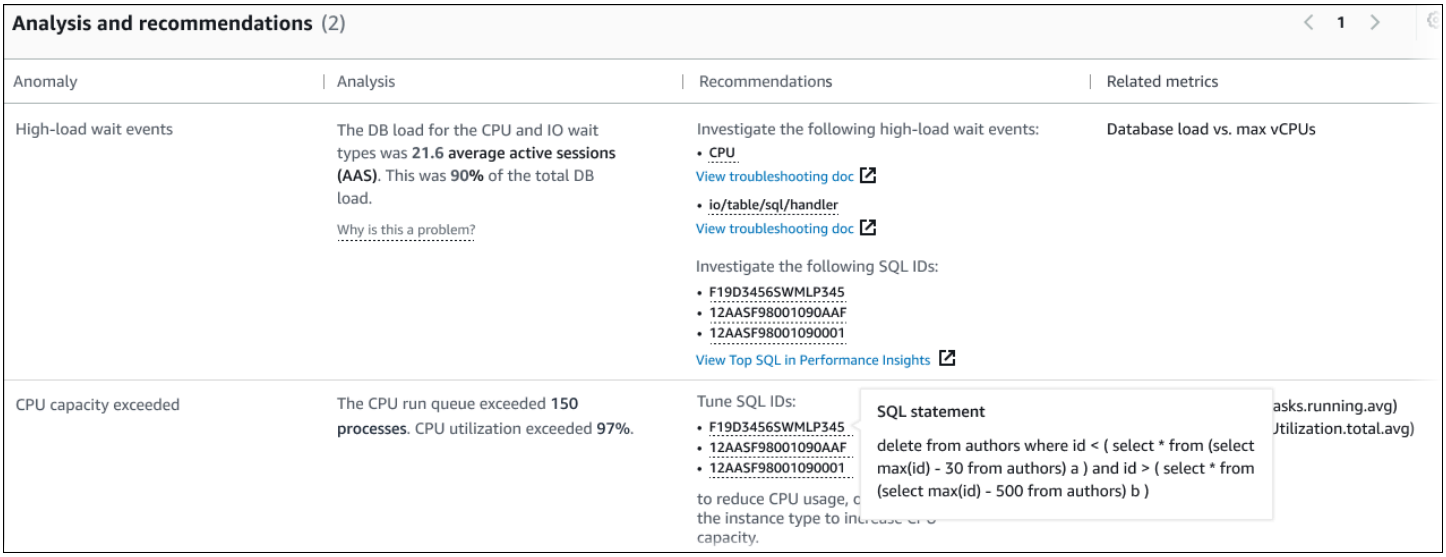
- ***Name***— Le nom de la métrique. La première ligne identifie la métrique en tant que tâches exécutées par le processeur.
- Actuellement : valeur actuelle de la métrique. Dans la première ligne, la valeur actuelle est de 162 processus (3x).
- Normalement : base de référence de cette métrique pour cette base de données lorsqu'elle fonctionne normalement. DevOpsGuru for RDS calcule la base de référence comme étant la valeur du 95e percentile sur une semaine d'historique. La première ligne indique que 56 processus sont généralement exécutés sur le processeur.
- Contribution à — Le résultat associé à cette métrique. Dans la première ligne, la métrique des tâches exécutées par le processeur est associée à l'anomalie de dépassement de la capacité du processeur.

La colonne Chronologie affiche un graphique linéaire pour la métrique. La zone ombrée indique l'intervalle de temps pendant DevOps lequel Guru for RDS a qualifié le résultat de grave.

Analyse et recommandations

Alors que l'anomalie causale décrit le problème global, une anomalie contextuelle décrit une constatation spécifique qui nécessite une enquête. Chaque résultat correspond à un ensemble de mesures connexes.

Dans l'exemple suivant de section Analyse et recommandations, l'anomalie de charge de base de données élevée a deux résultats.



Cette table possède les colonnes suivantes :

- Anomalie — Description générale de cette anomalie contextuelle. Dans cet exemple, la première anomalie concerne les événements d'attente liés à une charge élevée, et la seconde, le dépassement de la capacité du processeur.
- Analyse — Explication détaillée de l'anomalie.

  Dans la première anomalie, trois types d'attente contribuent à 90 % de la charge de base de données. Dans la deuxième anomalie, la file d'attente d'exécution du processeur dépassait 150, ce qui signifie qu'à tout moment, plus de 150 sessions attendaient le temps du processeur. L'utilisation du processeur était supérieure à 97 %, ce qui signifie que pendant la durée du problème, le processeur était occupé 97 % du temps. Ainsi, le processeur était occupé presque continuellement alors qu'en moyenne 150 sessions attendaient de s'exécuter sur le processeur.
- Recommandations — La réponse suggérée par l'utilisateur à l'anomalie.

  Dans la première anomalie, DevOps Guru for RDS vous recommande d'étudier les événements `cpu` d'attente et. `io/table/sql/handler` Pour savoir comment optimiser les performances de votre base de données en fonction de ces événements, consultez la section cpu et io/table/sql/handlerle guide de l'utilisateur Amazon Aurora.

  Dans le cas de la deuxième anomalie, DevOps Guru for RDS recommande de réduire la consommation du processeur en ajustant trois instructions SQL. Vous pouvez survoler les liens pour voir le texte SQL.
- Métriques associées : mesures qui vous fournissent des mesures spécifiques pour l'anomalie. Pour plus d'informations sur ces métriques, consultez la référence des métriques pour Amazon Aurora

dans le guide de l'utilisateur Amazon Aurora ou la référence des métriques pour Amazon RDS dans le guide de l'utilisateur Amazon RDS.

Dans le cas de la première anomalie, DevOps Guru for RDS recommande de comparer la charge de base de données au processeur maximal de votre instance. Dans la deuxième anomalie, il est recommandé de prendre en compte la file d'attente d'exécution du processeur, l'utilisation du processeur et le taux d'exécution SQL.

Visualisation proactive des anomalies

Dans Insights, vous pouvez consulter les anomalies relatives aux ressources Amazon RDS. Chaque information proactive fournit des détails sur une anomalie proactive. Sur une page d'analyse proactive, vous pouvez consulter un aperçu des informations, des mesures détaillées concernant l'anomalie et des recommandations pour éviter de futurs problèmes. Pour visualiser une anomalie proactive, rendez-vous sur la page Proactive Insight.

Aperçu d'Insight

La section de présentation d'Insight fournit des détails sur les raisons pour lesquelles l'aperçu a été créé. Il affiche la gravité de l'information ainsi qu'une description de l'anomalie et un calendrier indiquant le moment où l'anomalie s'est produite. Il répertorie également le nombre de services et d'applications concernés détectés par DevOps Guru.

Métriques

La section Métriques fournit des graphiques de l'anomalie. Chaque graphique affiche un seuil déterminé par le comportement de base de la ressource, ainsi que les données de la métrique rapportée au moment de l'anomalie.

Recommandations pour les ressources agrégées

Cette section suggère des mesures que vous pouvez prendre pour atténuer les problèmes signalés avant qu'ils ne s'aggravent. Les actions que vous pouvez effectuer sont présentées dans la colonne Modification personnalisée recommandée. La justification des recommandations est présentée dans la section Pourquoi DevOps Guru recommande-t-il cela ? colonne. Pour plus d'informations sur la manière de répondre aux recommandations, consultezthe section called “Réponse aux recommandations”.

Réponse aux recommandations

Les recommandations constituent la partie la plus importante de l'information. À ce stade de l'analyse, vous agissez pour résoudre le problème de performance. En général, vous devez suivre les étapes suivantes :

1. Décidez si le problème de performance signalé indique un problème réel.

   Dans certains cas, un problème peut être prévisible et bénin. Par exemple, si vous soumettez une base de données de test à une charge de base de données extrême, DevOps Guru for RDS signale cette charge comme une anomalie de performance. Cependant, il n'est pas nécessaire de remédier à cette anomalie, car il s'agit d'un résultat attendu de vos tests.

   Si vous déterminez que le problème nécessite une réponse, passez à l'étape suivante.
2. Décidez s'il convient de mettre en œuvre la recommandation.

   Dans le tableau des recommandations, une colonne indique les actions recommandées. Pour des informations réactives, il s'agit de la colonne Ce que nous recommandons sur la page détaillée d'une anomalie réactive. Pour obtenir des informations proactives, il s'agit de la colonne des modifications personnalisées recommandées sur une page d'informations proactives.

   DevOpsGuru for RDS propose une liste de recommandations qui couvrent plusieurs scénarios problématiques potentiels. Après avoir examiné cette liste, déterminez quelle recommandation correspond le mieux à votre situation actuelle et envisagez de l'appliquer. Si une recommandation convient à votre situation, passez à l'étape suivante. Si ce n'est pas le cas, ignorez l'étape restante et résolvez le problème à l'aide de techniques manuelles.
3. Effectuez les actions recommandées.

   DevOpsGuru for RDS vous recommande d'effectuer l'une des opérations suivantes :

   - Effectuez une action corrective spécifique.

     Par exemple, DevOps Guru for RDS peut vous recommander d'augmenter la capacité du processeur, de régler les paramètres du pool d'applications ou d'activer le schéma de performance.
   - Recherchez la cause du problème.

     DevOpsGuru for RDS vous recommande généralement d'étudier des instructions SQL ou des événements d'attente spécifiques. Par exemple, il peut être recommandé d'étudier l'événement d'attente`io/table/sql/handler`. Recherchez l'événement d'attente répertorié dans Tuning

with wait events for Aurora PostgreSQL ou Tuning with wait events for Aurora MySQL dans le guide de l'utilisateur Amazon Aurora, ou dans Tuning with wait events for RDS for PostgreSQL dans le guide de l'utilisateur Amazon RDS. Effectuez ensuite les actions recommandées.

> **Important**
>
> Nous vous recommandons de tester toutes les modifications apportées à une instance test avant de modifier une instance de production. Vous pouvez ainsi mieux appréhender l'impact d'une modification.

Surveillance de bases de données non relationnelles à l'aide de Guru DevOps

DevOpsGuru est capable de générer des informations pour vos bases de données non relationnelles ou NoSQL qui vous aident à configurer vos ressources conformément aux meilleures pratiques. Par exemple, DevOps Guru peut vous aider à rester au fait de la planification des capacités en prévoyant les besoins futurs en fonction du trafic existant. DevOpsGuru peut déterminer si vous utilisez moins de ressources que celles que vous avez configurées et fournir des recommandations pour améliorer la disponibilité des applications en fonction de votre historique d'utilisation. Cela peut vous aider à réduire les coûts inutiles.

Au-delà de la planification des capacités, DevOps Guru détecte et vous aide à résoudre les problèmes opérationnels tels que le ralentissement, les conflits de transactions, les échecs des contrôles conditionnels et les domaines à améliorer dans les paramètres du SDK. Les bases de données sont généralement connectées à plusieurs services et ressources, et DevOps Guru peut corréler la structure de votre application à des fins d'analyse à l'aide de groupes basés sur le balisage ou CloudFormation l'agrégation. Les anomalies peuvent impliquer plusieurs ressources qui sont toutes affectées par la même solution. DevOps Guru est capable de corréler différents indicateurs de ressources, configurations, journaux et événements. Par exemple, DevOps Guru peut analyser et relier les données d'une fonction Lambda qui peut lire ou écrire des données à partir d'une Amazon DynamoDB table. DevOpsGuru surveille ainsi plusieurs ressources connexes afin de détecter les anomalies et de fournir des informations utiles pour vos solutions de base de données.

Surveillance des opérations de base de données dans Amazon DynamoDB

Le tableau ci-dessous présente des exemples de scénarios et des informations que DevOps Guru surveille Amazon DynamoDB.

Amazon DynamoDB cas d'utilisation	Exemples	Métriques
Détecte lorsqu'un pourcentage élevé de AccountProvisioned ReadCapacityUtilization et AccountProvisionedWriteCapacityUtilization est utilisé, en raison d'un grand nombre de demandes de lecture et d'écriture.	Amazon DynamoDB les capacités de consommation des tables pour les demandes de lecture ou d'écriture atteignent leurs limites au niveau des tables.	AccountProvisioned ReadCapacityUtilization, AccountProvisionedWriteCapacityUtilization
Détectez les échecs de contrôle conditionnel dans les Amazon DynamoDB demandes provoqués par une expression de condition fournie ne correspondant pas à ce qui est attendu dans la base de données.	Les échecs des vérifications conditionnelles sont dus à des données erronées dans votre tableau, à une expression de condition stricte ou à des conditions de course.	ConditionalCheckFailedRequests

Surveillance des opérations de base de données dans Amazon ElastiCache

Le tableau ci-dessous présente des exemples de scénarios et des informations que DevOps Guru surveille Amazon ElastiCache.

Scénario identifié par DevOps Guru	CloudWatch métriques surveillées
Détectez lorsqu'un Amazon ElastiCache cluster atteint sa limite de calcul pour Redis	CPUUtilization, MoteurCPUUtilization, Expulsions

Scénario identifié par DevOps Guru	CloudWatch métriques surveillées
ou Memcached en raison de l'évolution des demandes de vos clusters.	

Intégration avec CodeGuru Profiler

Cette section fournit un aperçu de la manière dont Amazon DevOps Guru s'intègre à Amazon CodeGuru Profiler. Vous pouvez consulter les recommandations du CodeGuru profileur sous forme d'informations dans la console DevOps Guru.

Amazon DevOps Guru s'intègre à Amazon CodeGuru Profiler grâce à une règle EventBridge gérée. CodeGuru Profiler envoie des événements à. EventBridge La règle gérée achemine les événements envoyés avec le bus d'événements par défaut. Chaque événement entrant provenant de CodeGuru Profiler est un rapport d'anomalie proactif. Pour plus d'informations, consultez la section Utilisation EventBridge du CodeGuru profileur.

DevOpsGuru prend en charge les événements entrants avec EventBridge. Un événement indique un changement dans une recommandation identifiée par DevOps Guru. CodeGuru Profiler envoie un événement de battement de cœur toutes les 24 heures pour montrer la continuité de l'événement. Les événements contiennent des informations de recommandation du CodeGuru Profiler ainsi que des métadonnées relatives à vos ressources informatiques. Pour plus d'informations sur le cycle de vie d'un événement, consultez Amazon EventBridge Events.

Lorsque vous configurez DevOps Guru, DevOps Guru crée la règle EventBridge gérée dans votre compte qui achemine les événements depuis un autre service. Cette règle mène à DevOps Guru. Des notifications sont envoyées en cas d'événement entrant.

Un bus d'événements reçoit des événements d'une source telle que DevOps Guru et les achemine vers les règles associées à ce bus d'événements. Pour plus d'informations sur les bus d'événements, consultez la section Bus d'événements.

Pour plus d'informations sur certains paramètres, consultez Amazon EventBridge events.

Pour recevoir des informations sur CodeGuru Profiler dans DevOps Guru, vous devez disposer des éléments suivants.

- CodeGuru Le profileur doit être activé. Pour plus d'informations sur l'activation du CodeGuru profileur, voir Configuration du CodeGuru profileur.
- DevOpsGuru doit être activé. Pour plus d'informations sur l'activation de DevOps Guru, consultez la section Activer DevOps Guru.
- Les mêmes ressources doivent être surveillées dans la même région à la fois dans CodeGuru Profiler et DevOps Guru.

Définition des applications à l'aide de AWS ressources

Amazon DevOps Guru regroupe les ressources situées dans la limite de couverture qui spécifie les ressources qu'il analyse pour obtenir des informations opérationnelles. Les ressources sont regroupées par ressources CloudFormation empilées ou par ressources dotées de balises. Vous choisissez les piles ou les tags lorsque vous configurez DevOps Guru. Vous pouvez également mettre à jour les piles ou les balises ultérieurement. Nous vous recommandons de considérer vos groupes de ressources comme des applications. Par exemple, toutes les ressources que vous utilisez pour une application de surveillance peuvent être définies dans une pile. Vous pouvez également ajouter la même balise à toutes les ressources que vous utilisez dans une application de base de données. La limite qui définit les ressources analysées par DevOps Guru. Toutes les ressources de la collection se trouvent à l'intérieur de cette limite. Toutes les ressources de votre compte qui ne figurent pas dans votre collection de ressources se trouvent en dehors des limites et ne sont pas analysées. Pour plus d'informations sur les services et ressources pris en charge, consultez les tarifs Amazon DevOps Guru.

Vous pouvez définir votre limite de couverture qui contient les ressources de vos applications de trois manières.

- Spécifiez toutes les AWS ressources prises en charge dans votre AWS compte et dans votre région. Cela fait de votre compte et de votre région votre limite de ressources. Avec cette option, DevOps Guru analyse toutes les ressources prises en charge dans votre compte et dans votre région. Toutes les ressources qui se trouvent dans une pile sont regroupées dans une application. Toutes les ressources qui ne figurent pas dans une pile sont regroupées dans leur propre application.
- Utilisez des CloudFormation piles pour spécifier les ressources de vos applications. Une pile contient des ressources générées à l'aide de CloudFormation. Dans DevOps Guru, vous choisissez les piles dans votre compte. Dans chaque pile que vous choisissez, les ressources que vous choisissez sont regroupées dans une application. Toutes les ressources des piles sont analysées par DevOps Guru pour obtenir des informations.
- Utilisez des AWS balises pour définir les ressources de vos applications. Une AWS balise contient une clé et une valeur. Dans DevOps Guru, choisissez une clé de balise et choisissez éventuellement une ou plusieurs valeurs associées à cette clé. Vous pouvez utiliser les valeurs pour regrouper vos ressources dans des applications.

Pour de plus amples informations, veuillez consulter Mettre à jour votre couverture AWS d'analyse dans DevOps Guru.

Rubriques

- Utiliser des balises pour identifier les ressources dans vos applications DevOps Guru
- Utiliser des CloudFormation piles pour identifier les ressources dans vos applications DevOps Guru

Utiliser des balises pour identifier les ressources dans vos applications DevOps Guru

Vous pouvez utiliser des balises pour identifier les AWS ressources analysées par Amazon DevOps Guru et pour spécifier quelles ressources sont regroupées à des fins de surveillance à l'aide de la clé de balise et des valeurs de balise sélectionnées. Vous pouvez modifier ces configurations lorsque vous configurez DevOps Guru ou lorsque vous choisissez Modifier les ressources analysées sur la page Ressources analysées. Après avoir sélectionné Tags, vous choisissez une clé de balise spécifique que vous souhaitez qu'Amazon DevOps Guru surveille. Pour analyser toutes les ressources du compte et utiliser des valeurs de balise pour regrouper les ressources, sélectionnez Toutes les ressources du compte. Pour utiliser les valeurs de balises afin de spécifier les ressources que DevOps Guru doit analyser, sélectionnez Choisir des valeurs de balises spécifiques.

> **Note**
>
> Lorsque Toutes les ressources du compte est sélectionnée et qu'aucune valeur de balise n'existe, les ressources sans clé de balise sont regroupées et analysées séparément.

Vous utilisez la clé d'une balise pour identifier les ressources, puis vous utilisez les valeurs associées à cette clé pour regrouper les ressources dans vos applications. Par exemple, vous pouvez baliser vos ressources avec la clé `devops-guru-applications`, puis utiliser cette clé avec une valeur différente pour chacune de vos applications. Vous pouvez utiliser les paires clé-valeur de balise `devops-guru-applications/databasedevops-guru-applications/cicd`, et `devops-guru-applications/monitoring` pour identifier trois applications de votre compte. Chaque application est composée de ressources associées qui contiennent la même paire clé-valeur de balise. Vous ajoutez des balises à vos ressources en utilisant le AWS service auquel elles appartiennent. Pour de plus amples informations, veuillez consulter Ajouter AWS tags pour AWS resources.

Après avoir ajouté une balise aux ressources de votre application, vous pouvez filtrer vos informations en fonction des balises des ressources qui les ont générées. Pour plus d'informations sur la façon de filtrer vos informations à l'aide d'une balise, consultezConsulter les informations de DevOps Guru.

Pour plus d'informations sur les services et ressources pris en charge, consultez la rubrique Tarification d'Amazon DevOps Guru.

Rubriques

- Qu'est-ce qu'un AWS étiquette ?
- Définition d'une application DevOps Guru à l'aide d'une balise
- Utiliser des tags avec DevOps Guru
- Ajouter AWS tags pour AWS resources

Qu'est-ce qu'un AWS étiquette ?

Les balises vous aident à identifier et à organiser vos AWS ressources. De nombreux AWS services prennent en charge le balisage. Vous pouvez donc attribuer le même tag à des ressources provenant de différents services pour indiquer que les ressources sont liées. Par exemple, vous pouvez attribuer la même balise à une ressource de table Amazon DynamoDB que vous affectez à une AWS Lambda fonction. Pour de plus amples informations sur l'utilisation de balises, veuillez consulter le livre blanc sur les bonnes pratiques de balisage.

Chaque AWS étiquette comporte deux parties.

- Une clé de balise (par exemple, `CostCenter`, `Environment`, `Project` ou `Secret`). Les clés de balises sont sensibles à la casse.
- Un champ facultatif appelé valeur de balise (par exemple, `111122223333`, `Production` ou le nom d'une équipe). Omettre la valeur de balise équivaut à l'utilisation d'une chaîne vide. Tout comme les clés de balises, les valeurs de balises sont sensibles à la casse.

Ensemble, ces éléments sont connus sous le nom de paires clé-valeur.

Définition d'une application DevOps Guru à l'aide d'une balise

Pour définir votre application Amazon DevOps Guru à l'aide d'une balise, AWS ajoutez-la aux ressources de votre compte qui constituent votre application. Votre tag contient une clé et une

valeur. Nous vous recommandons d'ajouter une étiquette à chacune de vos AWS ressources analysées par DevOps Guru qui possède la même clé. Utilisez une valeur différente dans la balise pour regrouper les ressources dans vos applications. Par exemple, vous pouvez attribuer des balises avec la clé `devops-guru-analysis-boundary` à toutes les AWS ressources de votre limite de couverture. Utilisez différentes valeurs avec cette clé pour identifier les applications de votre compte. Vous pouvez utiliser les valeurs `containersdatabase`, et `monitoring` pour trois applications. Pour de plus amples informations, veuillez consulter Mettre à jour votre couverture AWS d'analyse dans DevOps Guru.

Si vous utilisez des AWS balises pour spécifier les ressources à analyser, vous ne pouvez utiliser des balises qu'avec une seule clé. Vous pouvez associer la clé de vos tags à n'importe quelle valeur. Utilisez cette valeur pour regrouper les ressources contenant votre clé dans vos applications opérationnelles.

> **Important**
>
> Lorsque vous créez une clé, la casse des caractères de la clé peut être celle de votre choix. Une fois que vous avez créé une clé, elle est sensible à la casse. Par exemple, DevOps Guru travaille avec une clé nommée `devops-guru-rds` et une clé nomméeDevOps-Guru-RDS, qui agissent comme deux clés différentes. Les paires clé/valeur possibles dans votre application peuvent être `Devops-Guru-production-application/RDS` ou `Devops-Guru-production-application/containers`.

Utiliser des tags avec DevOps Guru

Spécifiez les AWS balises qui identifient les AWS ressources que vous souhaitez qu'Amazon DevOps Guru analyse, ou spécifiez des valeurs de balises qui identifient les ressources qui seront regroupées. Ces ressources constituent la limite de couverture de vos ressources. Vous pouvez choisir une clé et zéro ou plusieurs valeurs.

Pour choisir vos tags

1. Ouvrez la console Amazon DevOps Guru à l'adresse https://console.aws.amazon.com/devops-guru/.
2. Ouvrez le volet de navigation, puis développez Paramètres.
3. Dans Ressources analysées, choisissez Modifier.

4. Choisissez Tags si vous souhaitez que DevOps Guru analyse toutes les ressources qui contiennent les balises de votre choix. Choisissez une touche, puis choisissez l'une des options suivantes.

   - Toutes les ressources du compte : analysez toutes les AWS ressources de la région et du compte actuels. Les ressources dont la clé de balise est sélectionnée sont regroupées par valeur de balise, le cas échéant. Les ressources dépourvues de cette clé de balise sont regroupées et analysées séparément.
   - Choisissez des valeurs de balises spécifiques — Toutes les ressources contenant une étiquette avec la clé que vous avez choisie sont analysées. DevOpsGuru regroupe vos ressources dans des applications en fonction des valeurs de votre tag.

5. Choisissez Enregistrer.

Ajouter AWS tags pour AWS resources

Lorsque vous spécifiez les AWS balises qui identifient les AWS ressources que vous souhaitez que DevOps Guru analyse, choisissez les balises auxquelles des ressources sont associées. Vous pouvez ajouter des balises à vos ressources à l'aide du AWS service auquel appartient chaque ressource ou à l'aide de l'éditeur de AWS balises.

- Pour gérer les balises à l'aide du service de vos ressources, utilisez la console ou le SDK du service auquel appartient une ressource. AWS Command Line Interface Par exemple, vous pouvez baliser une ressource de flux Amazon Kinesis ou une ressource de CloudFront distribution Amazon. Voici deux exemples de services dont les ressources peuvent être étiquetées. La plupart des ressources sur lesquelles DevOps Guru peut analyser les balises de support. Pour plus d'informations, consultez les sections Marquer vos streams dans le Guide du développeur Amazon Kinesis et Marquer une distribution dans le Guide du développeur Amazon CloudFront . Pour savoir comment ajouter des balises à d'autres types de ressources, consultez le guide de l'utilisateur ou le guide du développeur du AWS service auquel elles appartiennent.

> **Note**
>
> Lorsque vous balisez des ressources Amazon RDS, vous devez baliser l'instance de base de données et non le cluster.

- Vous pouvez utiliser l'éditeur de AWS balises pour gérer les balises par ressources de votre région et par ressources de AWS services spécifiques. Pour plus d'informations, consultez la section Éditeur de balises dans le Guide de l'utilisateur AWS des groupes de ressources et des balises.

Lorsque vous ajoutez une balise à une ressource, vous pouvez ajouter la clé uniquement ou la clé et une valeur. Par exemple, vous pouvez créer un tag avec la clé `devops-guru-` pour toutes les ressources qui font partie de votre DevOps application. Vous pouvez également ajouter une balise contenant la clé `devops-guru-` et la valeur `RDS`, puis ajouter cette paire clé-valeur uniquement aux ressources Amazon RDS de votre application. Cela est utile si vous souhaitez afficher dans la console des informations générées uniquement à partir des ressources Amazon RDS de votre application.

Utiliser des CloudFormation piles pour identifier les ressources dans vos applications DevOps Guru

Vous pouvez utiliser des AWS CloudFormation piles pour spécifier les AWS ressources que DevOps Guru doit analyser. Une pile est un ensemble de AWS ressources gérées comme une seule unité. Les ressources des piles que vous choisissez constituent la limite de couverture de votre DevOps Guru. Pour chaque pile que vous choisissez, les données opérationnelles des ressources prises en charge sont analysées pour détecter tout comportement anormal. Ces problèmes sont ensuite regroupés en anomalies connexes afin de créer des informations. Chaque information inclut une ou plusieurs recommandations pour vous aider à y répondre. Le nombre maximum de piles que vous pouvez spécifier est de 1 000. Pour plus d'informations, consultez les sections Utilisation des piles dans le guide de l'AWS CloudFormation utilisateur etMettre à jour votre couverture AWS d'analyse dans DevOps Guru.

Une fois que vous avez choisi une pile, DevOps Guru commence immédiatement à analyser toutes les ressources que vous y ajoutez. Si vous supprimez une ressource d'une pile, elle n'est plus analysée.

Si vous choisissez de demander à DevOps Guru d'analyser toutes les ressources prises en charge sur votre compte (cela signifie que votre AWS compte et votre région constituent la limite de couverture de votre compte DevOps Guru), DevOps Guru analyse et crée des informations pour chaque ressource prise en charge de votre compte, y compris celles cumulées. Les informations créées à partir d'anomalies dans une ressource qui ne figure pas dans une pile sont regroupées au niveau du compte. Si un aperçu est créé à partir d'anomalies dans une ressource figurant dans

une pile, il est regroupé au niveau de la pile. Pour de plus amples informations, veuillez consulter Comprendre comment les comportements anormaux sont regroupés en informations.

Choisir des piles à analyser par DevOps Guru

Spécifiez les ressources que vous souhaitez qu'Amazon DevOps Guru analyse en choisissant les CloudFormation piles qui les créent. Vous pouvez le faire à l'aide du Console de gestion AWS ou du SDK.

Rubriques

- Choix des piles à analyser par DevOps Guru (console)
- Choisir les piles à analyser par DevOps Guru (SDK DevOps Guru)

Choix des piles à analyser par DevOps Guru (console)

Vous pouvez ajouter des AWS CloudFormation piles à l'aide de la console.

Pour choisir les piles contenant les ressources à analyser

1. Ouvrez la console Amazon DevOps Guru à l'adresse https://console.aws.amazon.com/devops-guru/.
2. Ouvrez le volet de navigation, puis sélectionnez Paramètres.
3. Dans la couverture de l'analyse DevOps Guru, choisissez Gérer.
4. Choisissez les CloudFormation piles si vous souhaitez que DevOps Guru analyse les ressources qui se trouvent dans les piles de votre choix, puis choisissez l'une des options suivantes.
   - Toutes les ressources : toutes les ressources accumulées sur votre compte sont analysées. Les ressources de chaque pile sont regroupées dans leur propre application. Les ressources de votre compte qui ne figurent pas dans une pile ne sont pas analysées.
   - Sélectionnez les piles — Sélectionnez les piles que vous souhaitez que DevOps Guru analyse. Les ressources de chaque pile que vous sélectionnez sont regroupées dans leur propre application. Vous pouvez saisir le nom d'une pile dans Rechercher des piles pour localiser rapidement une pile spécifique. Vous pouvez sélectionner jusqu'à 1 000 piles.
5. Choisissez Enregistrer.

Choisir les piles à analyser par DevOps Guru (SDK DevOps Guru)

Pour spécifier des CloudFormation piles à l'aide du SDK Amazon DevOps Guru, utilisez la `UpdateResourceCollection` méthode. Pour plus d'informations, consultez UpdateResourceCollectionle manuel Amazon DevOps Guru API Reference.

Travailler avec Amazon EventBridge

Amazon DevOps Guru s'intègre EventBridge à Amazon pour vous informer de certains événements liés aux informations et des mises à jour correspondantes. Les événements AWS liés aux services sont diffusés EventBridge en temps quasi réel. Vous pouvez écrire des règles simples pour préciser les événements qui vous intéressent et les actions automatisées à effectuer quand un événement correspond à une règle. Les actions qui peuvent être initiées automatiquement incluent les exemples suivants :

- Invoquer une fonction AWS Lambda
- Invocation d'une commande d'exécution Amazon Elastic Compute Cloud
- Relais de l'événement à Amazon Kinesis Data Streams
- Activation d'une machine à états Step Functions
- Notifier un Amazon SNS ou un Amazon SQS

Vous pouvez sélectionner l'un des modèles prédéfinis suivants pour filtrer les événements ou créer une règle de modèle personnalisée pour lancer des actions dans une AWS ressource prise en charge.

- DevOps Guru New Insight est ouvert
- DevOps Association Guru New Anomaly
- DevOps Guru Insight Severity amélioré
- DevOps Guru : nouvelle recommandation créée
- DevOps Guru Insight Fermé

Événements pour DevOps Guru

Voici des exemples d'événements de DevOps Guru. Les événements sont générés sur la base du meilleur effort. Pour en savoir plus sur les modèles d'événements, consultez Getting started with Amazon EventBridge ou Amazon EventBridge Event patterns.

DevOps Événement ouvert Guru New Insight

Lorsque DevOps Guru ouvre un nouvel aperçu, il envoie l'événement suivant.

```
{
    "version" : "0",
    "id" : "08108845-ef90-00b8-1ad6-2ee5570ac6c4",
    "detail-type" : "DevOps Guru New Insight Open",
    "source" : "aws.devops-guru",
    "account" : "123456789012",
    "time" : "2021-11-01T17:06:10Z",
    "region" : "us-east-1",
    "resources" : [ ],
    "detail" : {
      "insightSeverity" : "high",
      "insightDescription" : "ApiGateway 5XXError Anomalous In Stack TestStack",
      "insightType" : "REACTIVE",
      "anomalies" : [
        {
          "startTime" : "1635786000000",
          "id" : "AL41JDFFQPYlZlXD8cpREkAAAAF83HGGgC9TmTr9lbfJ7sCiISlWMeFCbHY_XXXX",
          "sourceDetails" : [
            {
              "dataSource" : "CW_METRICS",
              "dataIdentifiers" : {
                "period" : "60",
                "stat" : "Average",
                "unit" : "None",
                "name" : "5XXError",
                "namespace" : "AWS/ApiGateway",
                "dimensions" : [
                  {
                    "name" : "ApiName",
                    "value" : "Test API Service"
                  },
                  {
                    "name" : "Stage",
                    "value" : "prod"
                  }
                ]
              }
            }
          ]
        }
      ],
      "accountId" : "123456789012",
      "messageType" : "NEW_INSIGHT",
```

```
      "insightUrl" : "https://us-east-1.console.aws.amazon.com/devops-guru/#/insight/
reactive/AIYH6JxdbgkcG0xJmypiL4MAAAAAAAAAL0SLEjkxiNProXWcsTJbLU07EZ7XXXX",
      "startTime" : "1635786120000",
      "insightId" : "AIYH6JxdbgkcG0xJmypiL4MAAAAAAAAAL0SLEjkxiNProXWcsTJbLU07EZ7XXXX",
      "region" : "us-east-1"
    }
  },
```

Exemple de modèle d'événement personnalisé pour une gravité élevée | new Insight

Les règles utilisent des modèles d'événements pour sélectionner des événements et les acheminer vers des cibles. Voici un exemple de modèle d'événement DevOps Guru.

```
{
  "source": [
    "aws.devops-guru"
  ],
  "detail-type": [
    "DevOps Guru New Insight Open"
  ],
  "detail": {
    "insightSeverity": [
         "high"
         ]
  }
}
```

Mettre à jour les paramètres DevOps Guru

Vous pouvez mettre à jour les paramètres Amazon DevOps Guru suivants :

- Votre couverture DevOps Guru. Cela permet de déterminer quelles ressources de votre compte sont analysées.
- Vos notifications. Cela permet de déterminer quels sujets Amazon Simple Notification Service sont utilisés pour vous informer des événements importants du DevOps Guru.
- Des fonctionnalités pour des informations améliorées. Cela inclut la détection des anomalies du journal, le chiffrement et vos paramètres AWS Systems Manager d'intégration. Cela détermine si DevOps Guru affiche les données du journal, si vous utilisez des clés de sécurité supplémentaires et si une clé OpsItem est créée dans Systems Manager OpsCenter pour chaque nouvel aperçu.

Rubriques

- Mettre à jour les paramètres de votre compte de gestion
- Mettre à jour votre couverture AWS d'analyse dans DevOps Guru
- Mettre à jour vos notifications dans DevOps Guru
- Filtrer les notifications de votre DevOps Guru
- Mettre à jour AWS Systems Manager l'intégration dans DevOps Guru
- Mise à jour de la détection des anomalies du journal dans Guru DevOps
- Mettre à jour les paramètres de chiffrement dans DevOps Guru

Mettre à jour les paramètres de votre compte de gestion

Vous pouvez configurer DevOps Guru pour les comptes de votre organisation. Si vous n'avez pas enregistré d'administrateur délégué, vous pouvez le faire en choisissant Enregistrer un administrateur délégué. Pour plus d'informations sur l'enregistrement d'un administrateur délégué, consultez Enable DevOps Guru.

Mettre à jour votre couverture AWS d'analyse dans DevOps Guru

Vous pouvez mettre à jour les AWS ressources de votre compte analysées par DevOps Guru. Pour ce faire, accédez à la page Ressources analysées dans la console, puis choisissez Modifier. Pour de plus amples informations, veuillez consulter Afficher les ressources analysées.

Mettre à jour vos notifications dans DevOps Guru

Configurez les rubriques Amazon Simple Notification Service qui sont utilisées pour vous informer des événements Amazon DevOps Guru importants. Vous pouvez choisir parmi une liste de noms de sujets qui existent déjà dans votre AWS compte, saisir le nom d'un nouveau sujet créé par DevOps Guru sur votre compte ou saisir le nom de ressource Amazon (ARN) d'un sujet existant dans n'importe quel AWS compte de votre région. Si vous spécifiez l'ARN d'un sujet qui ne figure pas dans votre compte, vous devez autoriser DevOps Guru à accéder à ce sujet en y ajoutant une politique IAM. Pour de plus amples informations, veuillez consulter Autorisations pour les rubriques Amazon SNS. Vous pouvez définir jusqu'à deux sujets.

DevOpsGuru envoie des notifications pour les mises à jour suivantes :

- Un nouvel aperçu est créé.
- Une nouvelle anomalie est ajoutée à un aperçu.
- La sévérité d'un aperçu est augmentée de `Low` ou `Medium` vers`High`.
- Le statut d'un aperçu passe de « en cours » à « résolu ».
- Une recommandation pour un aperçu est identifiée.

DevOpsGuru envoie également des notifications si une clé de CloudFormation pile ou de tag sélectionnée n'est pas valide lorsque vous essayez d'ajouter des ressources à votre compte DevOps Guru.

Vous pouvez choisir de recevoir des notifications Amazon SNS pour toutes sortes de mises à jour relatives à un problème ou de recevoir des notifications Amazon SNS uniquement lorsque le problème est ouvert, fermé ou présente un changement de gravité. Par défaut, vous recevez des notifications pour toutes les mises à jour.

Pour mettre à jour vos notifications, accédez d'abord à la page des notifications, puis choisissez d'ajouter, de supprimer ou de mettre à jour les configurations pour les sujets de notification Amazon SNS.

Rubriques

- Accédez aux paramètres de notification dans la console DevOps Guru
- Ajout de sujets de notification Amazon SNS dans la console Guru DevOps
- Supprimer les sujets de notification Amazon SNS dans la console Guru DevOps

- Mise à jour des configurations de notification Amazon SNS
- Autorisations ajoutées à votre rubrique Amazon SNS

Accédez aux paramètres de notification dans la console DevOps Guru

Pour mettre à jour les notifications, vous devez d'abord accéder à la section des paramètres de notification.

Pour accéder à la section des paramètres de notification

1. Ouvrez la console Amazon DevOps Guru à l'adresse https://console.aws.amazon.com/devops-guru/.
2. Choisissez Settings (Paramètres) dans le volet de navigation.

   La page Paramètres inclut la section Notifications, qui contient des informations sur les rubriques Amazon SNS configurées.

Ajout de sujets de notification Amazon SNS dans la console Guru DevOps

Pour ajouter un sujet de notification Amazon SNS dans la DevOps console Guru

1. the section called “Accédez aux paramètres de notification dans la console DevOps Guru”.
2. Sélectionnez Ajouter une notification.
3. Pour ajouter une rubrique Amazon SNS, effectuez l'une des opérations suivantes.

   - Choisissez Générer une nouvelle rubrique SNS par e-mail. Ensuite, dans Spécifiez l'adresse e-mail, entrez l'adresse e-mail à laquelle vous souhaitez recevoir des notifications. Pour saisir des adresses e-mail supplémentaires, choisissez Ajouter une nouvelle adresse e-mail.
   - Choisissez Utiliser une rubrique SNS existante. Ensuite, dans Choisissez un sujet dans votre AWS compte, sélectionnez le sujet que vous souhaitez utiliser.
   - Choisissez Utiliser l'ARN d'une rubrique SNS existante pour spécifier une rubrique existante provenant d'un autre compte. Ensuite, dans Entrez un ARN pour un sujet, entrez l'ARN du sujet. L'ARN est le nom de la ressource Amazon du sujet. Vous pouvez définir un sujet dans un autre compte. Si vous utilisez un sujet dans un autre compte, vous devez y ajouter une politique de ressources. Pour de plus amples informations, veuillez consulter Autorisations pour les rubriques Amazon SNS.

4. Choisissez Enregistrer.

Supprimer les sujets de notification Amazon SNS dans la console Guru DevOps

Pour supprimer des rubriques Amazon SNS dans la console Guru DevOps

1. the section called “Accédez aux paramètres de notification dans la console DevOps Guru”.
2. Choisissez Sélectionner un sujet existant.
3. Dans le menu déroulant, sélectionnez le sujet que vous souhaitez supprimer.
4. Cliquez sur Supprimer.
5. Choisissez Enregistrer.

Mise à jour des configurations de notification Amazon SNS

Il existe deux types de configurations de notification pour les sujets de notification Amazon SNS dans DevOps Guru. Vous pouvez choisir de recevoir des notifications de tous les niveaux de gravité ou uniquement des notifications de niveaux de gravité élevé ou moyen. Vous pouvez également choisir de recevoir des notifications pour tous les types de mises à jour ou uniquement pour certains types de mises à jour.

Lorsque vous choisissez de recevoir des notifications Amazon SNS pour toutes sortes de mises à jour relatives au problème, DevOps Guru envoie des notifications pour les mises à jour suivantes :

- Un nouvel aperçu est créé.
- Une nouvelle anomalie est ajoutée à un aperçu.
- La sévérité d'un aperçu est augmentée de `Low` ou `Medium` vers`High`.
- Le statut d'un aperçu passe de « en cours » à « résolu ».
- Une recommandation pour un aperçu est identifiée.

Par défaut, vous ne recevez que des notifications de niveau de gravité élevé et moyen, et vous recevez des notifications pour toutes sortes de mises à jour.

Pour mettre à jour les configurations de notification pour les rubriques de notification Amazon SNS

1. the section called “Accédez aux paramètres de notification dans la console DevOps Guru”.
2. Choisissez Sélectionner un sujet existant.
3. Dans le menu déroulant, sélectionnez le sujet que vous souhaitez modifier.
4. Choisissez Tous les niveaux de gravité pour recevoir des notifications avec des niveaux de gravité élevés, moyens et faibles, ou choisissez uniquement des niveaux élevés et moyens pour recevoir des notifications avec des niveaux de gravité élevés et moyens.
5. Choisissez M'avertir de toutes les mises à jour de l'information, ou choisissez M'avertir lorsqu'une information est ouverte ou fermée, ou lorsque le niveau de gravité passe de faible ou moyen à élevé.
6. Choisissez Enregistrer.

Autorisations ajoutées à votre rubrique Amazon SNS

Une rubrique Amazon SNS est une ressource qui contient une politique de ressources Gestion des identités et des accès AWS (IAM). Lorsque vous spécifiez un sujet ici, DevOps Guru ajoute les autorisations suivantes à sa politique de ressources.

```
{
    "Sid": "DevOpsGuru-added-SNS-topic-permissions",
    "Effect": "Allow",
    "Principal": {
        "Service": "region-id.devops-guru.amazonaws.com"
    },
    "Action": "sns:Publish",
    "Resource": "arn:aws:sns:region-id:topic-owner-account-id:my-topic-name",
    "Condition" : {
      "StringEquals" : {
        "AWS:SourceArn": "arn:aws:devops-guru:region-id:topic-owner-account-
id:channel/devops-guru-channel-id",
        "AWS:SourceAccount": "topic-owner-account-id"
    }
  }
}
```

Ces autorisations sont requises pour que DevOps Guru puisse publier des notifications en utilisant un sujet. Si vous préférez ne pas avoir ces autorisations sur le sujet, vous pouvez les supprimer en toute

sécurité et le sujet continuera de fonctionner tel qu'il était avant que vous ne le choisissiez. Toutefois, si ces autorisations ajoutées sont supprimées, DevOps Guru ne peut pas utiliser le sujet pour générer des notifications.

Filtrer les notifications de votre DevOps Guru

Vous pouvez filtrer vos notifications DevOps Guru par the section called “Mise à jour des configurations de notification Amazon SNS” ou en utilisant une politique de filtrage des abonnements Amazon SNS.

Rubriques

- Filtrer les notifications à l'aide d'une politique de filtrage des abonnements Amazon SNS
- Exemple de notification Amazon SNS filtrée pour Amazon Guru DevOps

Filtrer les notifications à l'aide d'une politique de filtrage des abonnements Amazon SNS

Vous pouvez créer une politique de filtrage des abonnements Amazon Simple Notification Service (Amazon SNS) afin de réduire le nombre de notifications que vous recevez d'Amazon Guru. DevOps

Utilisez une politique de filtrage pour spécifier les types de notifications que vous recevez. Vous pouvez filtrer vos messages Amazon SNS à l'aide des mots clés suivants.

- `NEW_INSIGHT`— Recevez une notification lorsqu'un nouvel aperçu est créé.
- `CLOSED_INSIGHT`— Recevez une notification lorsqu'un aperçu existant est fermé.
- `NEW_RECOMMENDATION`— Recevez une notification lorsqu'une nouvelle recommandation est créée à partir d'un aperçu.
- `NEW_ASSOCIATION`— Recevez une notification lorsqu'une nouvelle anomalie est détectée à partir d'un aperçu.
- `CLOSED_ASSOCIATION`— Recevez une notification lorsqu'une anomalie existante est corrigée.
- `SEVERITY_UPGRADED`— Recevez une notification lorsque la gravité d'un aperçu est améliorée

Pour plus d'informations sur la création d'une politique de filtrage d'abonnement Amazon SNS, consultez les politiques de filtrage d'abonnement Amazon SNS dans le guide du développeur

Amazon Simple Notification Service. Dans votre politique de filtrage, vous spécifiez l'un des mots clés avec la politique`MessageType`. Par exemple, les informations suivantes apparaîtront dans un filtre qui indique que la rubrique Amazon SNS envoie des notifications uniquement lorsqu'une nouvelle anomalie est détectée à partir d'un aperçu.

```
{
  "MessageType":["NEW_ ASSOCIATION"]
}
```

Exemple de notification Amazon SNS filtrée pour Amazon Guru DevOps

Voici un exemple de notification Amazon Simple Notification Service (Amazon SNS) provenant d'une rubrique Amazon SNS avec une politique de filtrage. Il `MessageType` est réglé sur`NEW_ASSOCIATION`, de sorte qu'il envoie des notifications uniquement lorsqu'une nouvelle anomalie est détectée à partir d'un aperçu.

```
{
      "accountId": "123456789012",
      "region": "us-east-1",
      "messageType": "NEW_ASSOCIATION",
      "insightId": "ADyf4FvaVNDzu9MA2-IgFDkAAAAAAAAAEGpJd5sjicgauU2wmAlnWUyyI2hiO5it",
      "insightName": "Repeated Insight: Anomalous increase in Lambda
 ApigwLambdaDdbStack-22-Function duration due to increased number of invocations",
      "insightUrl": "https://us-east-1.console.aws.amazon.com/devops-guru/insight/
reactive/ADyf4FvaVNDzu9MA2-IgFDkAAAAAAAAAEGpJd5sjicgauU2wmAlnWUyyI2hiO5it",
      "insightType": "REACTIVE",
      "insightDescription": "At March 29, 2023 22:02 GMT, Lambda function
 ApigwLambdaDdbStack-22-Function had\n an increased duration anomaly possibly caused by
 the Lambda function invocation increase. DevOps Guru has detected this is a repeated
 insight. DevOps Guru treats repeated insights as 'Low Severity'.",
      "startTime": 1628767500000,
      "startTimeISO": "2023-03-29T22:00:00Z",
      "anomalies": [
        {
          "id": "AG2n8ljW74BoI1CHu-m_oAgAAAF7Ohu24N4Yro69ZSdUtn_alzPH7VTpaL30JXiF",
          "startTime": 1628767500000,
          "startTimeISO": "2023-03-29T22:00:00Z",
          "openTime": 1680127740000,
          "openTimeISO": "2023-03-29T22:09:00Z",
          "sourceDetails": [
            {
```

```
              "dataSource": "CW_METRICS",
              "dataIdentifiers": {
                "namespace": "AWS/SQS",
                "name": "ApproximateAgeOfOldestMessage",
                "stat": "Maximum",
                "unit": "None",
                "period": "60",
                "dimensions": "{\"QueueName\":\"FindingNotificationsDLQ\"}"
              }
            }
          ],
          "associatedResourceArns":[
           "arn:aws:sns:us-east-1:123456789012:DevOpsGuru-insights-sns"
          ]
        }
      ],
      "resourceCollection":{
      "cloudFormation":{
         "stackNames":[
            "CapstoneNotificationPublisherEcsApplicationInfrastructure"
          ]
        }
      }
}
```

Mettre à jour AWS Systems Manager l'intégration dans DevOps Guru

Vous pouvez activer la création d'un OpsItem pour chaque nouvel aperçu dans AWS Systems Manager OpsCenter. OpsCenter est un système centralisé dans lequel vous pouvez visualiser, étudier et examiner les éléments de travail opérationnels (OpsItems). L' OpsItems outil for your insights peut vous aider à gérer le travail visant à remédier au comportement anormal à l'origine de la création de chaque information. Pour plus d'informations, reportez-vous AWS Systems Manager OpsCenterà la section « Travailler avec » OpsItem dans le guide de AWS Systems Manager l'utilisateur.

> **Note**
>
> Si vous modifiez la clé ou la valeur du champ de balise d'un OpsItem, DevOps Guru n'est pas en mesure de le mettre à jour OpsItem. Par exemple, si vous remplacez le tag d'un form par

un OpsItem autre, DevOps Guru ne peut pas le mettre à jour OpsItem. `"aws:RequestTag/DevOps-GuruInsightSsmOpsItemRelated": "true"`

Pour gérer votre intégration à Systems Manager

1. Ouvrez la console Amazon DevOps Guru à l'adresse https://console.aws.amazon.com/devops-guru/.
2. Choisissez Settings (Paramètres) dans le volet de navigation.
3. Lors de AWS Systems Manager l'intégration, sélectionnez Enable DevOps Guru pour créer un OpsCenter identifiant pour chaque aperçu afin d' AWS OpstItem en OpsItem créer un pour chaque nouvel aperçu. Désélectionnez-le pour ne plus en avoir OpsItem créé pour chaque nouvel aperçu.

La OpsItems création sur votre compte vous est facturée. Pour en savoir plus, consultez Pricing AWS Systems Manager (Tarification).

Mise à jour de la détection des anomalies du journal dans Guru DevOps

Pour gérer les paramètres de détection des anomalies du journal

1. Ouvrez la console Amazon DevOps Guru à l'adresse https://console.aws.amazon.com/devops-guru/.
2. Choisissez Settings (Paramètres) dans le volet de navigation.
3. Dans Détection des anomalies du journal, sélectionnez Activer la détection des anomalies du journal en accordant à DevOps Guru l'autorisation d'afficher les données du journal associées à un aperçu. pour que DevOps Guru affiche les données du journal relatives aux informations.

Mettre à jour les paramètres de chiffrement dans DevOps Guru

Vous pouvez mettre à jour les paramètres de chiffrement pour utiliser des clés AWS détenues ou des clés gérées par le AWS KMS client. Lorsque vous passez d'une AWS KMS clé gérée par le client à une nouvelle AWS KMS clé gérée par le client existante, DevOps Guru commence automatiquement

à chiffrer les métadonnées nouvellement ingérées à l'aide de la nouvelle clé. Les données historiques resteront cryptées à l'aide de la AWS KMS clé gérée par le client précédemment configurée.

> **Note**
>
> Si vous révoquez l'autorisation, désactivez ou supprimez la AWS KMS clé précédente, DevOps Guru ne pourra accéder à aucune des données cryptées par cette clé et vous pourriez le voir `AccessDeniedException` lorsque vous effectuez une opération de lecture.

Pour gérer vos paramètres de chiffrement

1. Ouvrez la console Amazon DevOps Guru à l'adresse https://console.aws.amazon.com/devops-guru/.
2. Choisissez Settings (Paramètres) dans le volet de navigation.
3. Dans la section Chiffrement, choisissez Modifier le chiffrement.
4. Sélectionnez le type de cryptage que vous souhaitez utiliser pour protéger vos données. Vous pouvez utiliser une clé AWS détenue par défaut, choisir une clé gérée par le client existante ou créer une nouvelle AWS KMS clé gérée par le client.
5. Choisissez Enregistrer.

Le chiffrement est un élément important de la sécurité de DevOps Guru. Pour de plus amples informations, veuillez consulter the section called “Protection des données”.

Affichage des notifications

Il existe différents types de notifications dans DevOps Guru.

Rubriques

- Nouveau point de vue
- Aperçu fermé
- Nouvelle association
- Nouvelle recommandation
- Sévérité améliorée
- Échec de validation des ressources

Les sections de cette page présentent des exemples de chaque type de notification.

Nouveau point de vue

Les notifications relatives aux nouvelles informations contiennent les informations suivantes :


```
{
   "accountId":"123456789101",
   "region":"eu-west-1",
   "messageType":"NEW_INSIGHT",
   "insightId":"a1b2c3d4-5678-90ab-cdef-EXAMPLE22222",
   "insightName": "Repeated Insight: ApiGateway 5XXError Anomalous In Application
 CanaryCommonResources-123456789101-LogAnomaly-4",
   "insightUrl":"https://eu-west-1.console.aws.amazon.com/devops-guru/insight/reactive/
a1b2c3d4-5678-90ab-cdef-EXAMPLE22222",
   "insightType":"REACTIVE",
   "insightDescription":"DevOps Guru has detected this is a repeated insight. DevOps
 Guru treats repeated insights as 'Low Severity'.",
   "insightSeverity":"medium",
   "startTime": 1680148920000,
   "startTimeISO": "2023-03-30T04:02:00Z",
   "anomalies":[
      {
         "id":"a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
         "startTime": 1680148800000,
         "startTimeISO": "2023-03-30T04:00:00Z",
```

```
         "openTime": 1680148920000,
         "openTimeISO": "2023-03-30T04:02:00Z",
         "sourceDetails":[
            {
               "dataSource":"CW_METRICS",
               "dataIdentifiers":{
                  "name":"ApproximateAgeOfOldestMessage",
                  "namespace":"AWS/SQS",
                  "period":"60",
                  "stat":"Maximum",
                  "unit":"None",
                  "dimensions":"{\"QueueName\":\"SampleQueue\"}"
               }
            }
         ],
         "associatedResourceArns":[
            "arn:aws:sqs:eu-west-1:123456789101:SampleQueue"
         ]
      }
   ],
   "resourceCollection":{
        "cloudFormation":{
            "stackNames":[
                "SampleApplication"
            ]
        },
   }
}
```

Aperçu fermé

Les notifications relatives à des informations fermées contiennent les informations suivantes :

```
{
"accountId":"123456789101",
   "region":"us-east-1",
   "messageType":"CLOSED_INSIGHT",
   "insightId":"a1b2c3d4-5678-90ab-cdef-EXAMPLE33333",
   "insightName": "DynamoDB table writes are under utilized in mock-stack",
   "insightUrl":"https://us-east-1.console.aws.amazon.com/devops-guru/insight/
proactive/a1b2c3d4-5678-90ab-cdef-EXAMPLE33333",
   "insightType":"PROACTIVE",
   "insightDescription":"DynamoDB table writes are under utilized",
```

```
    "insightSeverity":"medium",
    "startTime": 1670612400000,
    "startTimeISO": "2022-12-09T19:00:00Z",
    "endTime": 1679994000000,
    "endTimeISO": "2023-03-28T09:00:00Z",
    "anomalies":[
       {
          "id":"a1b2c3d4-5678-90ab-cdef-EXAMPLEaaaaa",
          "startTime": 1665428400000,
          "startTimeISO": "2022-10-10T19:00:00Z",
          "endTime": 1679986800000,
          "endTimeISO": "2023-03-28T07:00:00Z",
          "openTime": 1670612400000,
          "openTimeISO": "2022-12-09T19:00:00Z",
          "closeTime": 1679994000000,
          "closeTimeISO": "2023-03-28T09:00:00Z",
          "description":"Empty receives while messages are available",
          "anomalyResources":[
             {
                "type":"AWS::SQS::Queue",
                "name":"SampleQueue"
             }
          ],
          "sourceDetails":[
             {
                "dataSource":"CW_METRICS",
                "dataIdentifiers":{
                "name":"NumberOfEmptyReceives",
                   "namespace":"AWS/SQS",
                   "period":"60",
                   "stat":"Sum",
                   "unit":"COUNT",
                   "dimensions":"{\"QueueName\":\"SampleQueue\"}"
                }
             }
           ],
         "associatedResourceArn": [
             "arn:aws:sqs:us-east-1:123456789101:SampleQueue"
         ]
       }
    ],
    "resourceCollection":{
         "cloudFormation":{
             "stackNames":[
```

```
                "SampleApplication"
            ]
        }
    }
}
```

Nouvelle association

Les notifications relatives aux nouvelles associations contiennent les informations suivantes :

```
{
"accountId":"123456789101",
   "region":"eu-west-1",
   "messageType":"NEW_ASSOCIATION",
   "insightId":"a1b2c3d4-5678-90ab-cdef-EXAMPLE22222",
   "insightName": "Repeated Insight: Anomalous increase in Lambda
 ApigwLambdaDdbStack-22-GetOneFunction duration due to increased number of
 invocations",
   "insightUrl":"https://eu-west-1.console.aws.amazon.com/devops-guru/insight/reactive/
a1b2c3d4-5678-90ab-cdef-EXAMPLE22222",
   "insightType":"REACTIVE",
   "insightDescription":"At March 29, 2023 22:02 GMT, Lambda function
 ApigwLambdaDdbStack-22-GetOneFunction had\nan increased duration anomaly possibly
 caused by the Lambda function invocation increase. DevOps Guru has detected this is a
 repeated insight. DevOps Guru treats repeated insights as 'Low Severity'.",
   "insightSeverity":"medium",
   "startTime": 1680127200000,
   "startTimeISO": "2023-03-29T22:00:00Z",
   "anomalies":[
      {
         "id":"a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
         "startTime":1672945500000,
         "startTimeISO": "2023-03-29T22:00:00Z",
         "openTime": 1680127740000,
         "openTimeISO": "2023-03-29T22:09:00Z",
         "sourceDetails":[
            {
               "dataSource":"CW_METRICS",
               "dataIdentifiers":{
               "namespace":"AWS/SQS",
                  "name":"ApproximateAgeOfOldestMessage",
                  "stat":"Maximum",
                  "unit":"None",
```

```
                  "period":"60",
                  "dimensions":"{\"QueueName\":\"SampleQueue\"}"
               }
            }
         ],
         "associatedResourceArns":[
            "arn:aws:sqs:eu-west-1:123456789101:SampleQueue"
         ]
      }
   ],
   "resourceCollection":{
        "cloudFormation":{
            "stackNames":[
                "SampleApplication"
            ]
        }
   }
}
```

Nouvelle recommandation

Les notifications relatives aux nouvelles recommandations contiennent les informations suivantes :

```
{
   "accountId":"123456789101",
   "region":"us-east-1",
   "messageType":"NEW_RECOMMENDATION",
   "insightId":"a1b2c3d4-5678-90ab-cdef-EXAMPLE33333",
   "insightName": "Recreation of AWS SDK Service Clients",
   "insightUrl":"https://us-east-1.console.aws.amazon.com/devops-guru/insight/
proactive/a1b2c3d4-5678-90ab-cdef-EXAMPLE33333",
   "insightType":"PROACTIVE",
   "insightDescription": "Usually for a given service you can create one [AWS SDK
 service client](https://docs.aws.amazon.com/sdk-for-java/v1/developer-guide/creating-
clients.html) and reuse that client across your entire service.\n\nWhen instead you
 create a new AWS SDK service client for each call (e.g. for DynamoDB) it\u0027s
 generally a waste of CPU time.",
   "insightSeverity":"medium",
   "startTime": 1680125893576,
   "startTimeISO": "2023-03-29T21:38:13.576Z",
   "recommendations":[
      {
         "name":"Tune Availability Zones of your Lambda Function",
```

```
        "description":"Based on your configurations, we recommend that you set
 SampleFunction to be deployed in at least 3 Availability Zones to maintain Multi
 Availability Zone Redundancy.",
        "reason":"Lambda Function SampleFunction is currently only deployed to 2
 unique Availability zones in a region with 7 total Availability zones.",
        "link":"https://docs.aws.amazon.com/lambda/latest/dg/configuration-vpc.html",
        "relatedAnomalies":[
           {
              "sourceDetails":{
                   "cloudWatchMetrics":null
              },
              "resources":[
                 {
                    "name":"SampleFunction",
                    "type":"AWS::Lambda::Function"
                 }
              ],
              "associatedResourceArns": [
                 "arn:aws:lambda:arn:123456789101:SampleFunction"
              ]
           }
        ]
     }
  ],
  "resourceCollection": {
       "cloudFormation": {
       "stackNames":[
           "SampleApplication"
        ]
     }
  }
}
```


Sévérité améliorée

Les notifications relatives aux mises à niveau de gravité contiennent les informations suivantes :


```
{
"accountId":"123456789101",
   "region":"eu-west-1",
   "messageType":"SEVERITY_UPGRADED",
   "insightId":"a1b2c3d4-5678-90ab-cdef-EXAMPLEbbbbb",
```

```
   "insightName": "Repeated Insight: ApiGateway 5XXError Anomalous In Application
 CanaryCommonResources-123456789101-LogAnomaly-11",
   "insightUrl":"https://eu-west-1.console.aws.amazon.com/devops-guru/insight/reactive/
a1b2c3d4-5678-90ab-cdef-EXAMPLEbbbbb",
   "insightType":"REACTIVE",
   "insightDescription": "DevOps Guru has detected this is a repeated insight. DevOps
 Guru will treat future occurrences of this insight as 'Low Severity' for the next 7
 days.",
   "insightSeverity":"high",
   "startTime": 1680127320000,
   "startTimeISO": "2023-03-29T22:02:00Z",
   "resourceCollection":{
        "cloudFormation":{
            "stackNames":[
                "SampleApplication"
            ]
        }
   }
}
```

Échec de validation des ressources

Vous pouvez utiliser des CloudFormation piles et des AWS balises pour filtrer et identifier les AWS ressources que vous souhaitez que DevOps Guru analyse. Lorsque vous choisissez une pile ou un tag non valide pour que DevOps Guru identifie les ressources, DevOps Guru crée une `SELECTED_RESOURCE_FILTER_VALIDATION_FAILURE` notification. Cela peut se produire lorsque le nom de balise ou de pile que vous spécifiez n'est pas associé à des ressources. Pour tirer le meilleur parti des méthodes de filtrage DevOps Guru, choisissez des piles et des tags auxquels des ressources sont associées.

```
{
    "accountId":"123456789101",
    "region":"eu-west-1",
    "messageType":"SELECTED_RESOURCE_FILTER_VALIDATION_FAILURE",
    "ResourceFilterType": "Tags",
    "InvalidResourceNames": [
         "Devops-Guru-tag-key-tag-value"
    ],
    "awsInsightSource": "aws.devopsguru"
}
```

Afficher les ressources analysées par DevOps Guru

DevOpsGuru fournit une liste des noms de ressources et de leurs limites d'application en cours d'analyse à l'aide de l'`ListMonitoredResources`action. Ces informations sont collectées auprès d'Amazon CloudWatch et d'autres AWS services à l'aide du rôle lié au service DevOps Guru. AWS CloudTrail

Notez que même si un utilisateur n'a pas l'autorisation explicite d'accéder APIs à un autre service tel qu' AWS Lambda Amazon RDS, DevOps Guru fournit toujours une liste des ressources de ce service tant que l'`ListMonitoredResources`action est autorisée.

Rubriques

- Mettre à jour votre couverture AWS d'analyse dans DevOps Guru
- Suppression de la vue des ressources analysées pour les utilisateurs

Mettre à jour votre couverture AWS d'analyse dans DevOps Guru

Vous pouvez mettre à jour les AWS ressources de votre compte analysées par DevOps Guru. Les ressources analysées constituent la limite de couverture de votre DevOps Guru. Lorsque vous définissez vos limites, vos ressources sont regroupées dans des applications. Vous avez quatre options de couverture des limites.

- Choisissez de demander à DevOps Guru d'analyser toutes les ressources prises en charge sur votre compte. Toutes les ressources de votre compte qui se trouvent dans une pile sont regroupées dans une application. Si vous avez plusieurs piles dans votre compte, les ressources de chaque pile constituent leur propre application. Si des ressources de votre compte ne figurent pas dans une pile, elles sont regroupées dans leur propre application.
- Spécifiez les ressources en choisissant AWS CloudFormation des piles qui définissent ces ressources. Dans ce cas, DevOps Guru analyse chaque ressource spécifiée dans les piles que vous choisissez. Si une ressource de votre compte n'est pas définie par une pile que vous choisissez, elle n'est pas analysée. Pour plus d'informations, consultez les sections Utilisation des piles dans le guide de l'CloudFormation utilisateur etDéterminer la couverture pour DevOps Guru.
- Spécifiez les ressources à l'aide de AWS balises. DevOpsGuru analyse soit toutes les ressources de votre compte et de votre région, soit toutes les ressources contenant la clé de balise que vous avez choisie. Les ressources sont regroupées en fonction des valeurs de balises sélectionnées.

Pour de plus amples informations, veuillez consulter Utiliser des balises pour identifier les ressources dans vos applications DevOps Guru.

- Spécifiez qu'aucune ressource n'est analysée afin de ne plus encourir de frais liés à l'analyse des ressources.

> **Note**
>
> Si vous mettez à jour votre couverture pour arrêter d'analyser les ressources, vous pourriez continuer à encourir des frais mineurs si vous consultez les informations existantes générées par DevOps Guru dans le passé. Ces frais sont associés aux appels d'API utilisés pour récupérer et afficher des informations d'aperçu. Pour plus d'informations, consultez les tarifs d'Amazon DevOps Guru.

DevOpsGuru prend en charge toutes les ressources associées aux services pris en charge. Pour plus d'informations sur les services et ressources pris en charge, consultez les tarifs Amazon DevOps Guru.

Pour gérer votre couverture d'analyse DevOps Guru

1. Ouvrez la console Amazon DevOps Guru à l'adresse https://console.aws.amazon.com/devops-guru/.
2. Développez les ressources analysées dans le volet de navigation.
3. Choisissez Modifier.
4. Choisissez l'une des options de couverture suivantes.

    - Choisissez Toutes les ressources du compte si vous souhaitez que DevOps Guru analyse toutes les ressources prises en charge dans votre AWS compte et dans votre région. Si vous choisissez cette option, votre AWS compte est la limite de couverture de votre analyse des ressources. Toutes les ressources de chaque pile de votre compte sont regroupées dans leur propre application. Toutes les ressources restantes qui ne figurent pas dans une pile sont regroupées dans leur propre application.
    - Choisissez les CloudFormation piles si vous souhaitez que DevOps Guru analyse les ressources qui se trouvent dans les piles de votre choix, puis choisissez l'une des options suivantes.

- Toutes les ressources : toutes les ressources accumulées sur votre compte sont analysées. Les ressources de chaque pile sont regroupées dans leur propre application. Les ressources de votre compte qui ne figurent pas dans une pile ne sont pas analysées.
- Sélectionnez les piles — Sélectionnez les piles que vous souhaitez que DevOps Guru analyse. Les ressources de chaque pile que vous sélectionnez sont regroupées dans leur propre application. Vous pouvez saisir le nom d'une pile dans Rechercher des piles pour localiser rapidement une pile spécifique. Vous pouvez sélectionner jusqu'à 1 000 piles.

Pour de plus amples informations, veuillez consulter Utiliser des CloudFormation piles pour identifier les ressources dans vos applications DevOps Guru.

- Choisissez Tags si vous souhaitez que DevOps Guru analyse toutes les ressources contenant les tags que vous avez choisis. Choisissez une clé, puis l'une des options suivantes.
  - Toutes les ressources du compte : analysez toutes les ressources AWS de la région et du compte actuels. Les ressources dont la clé de balise est sélectionnée sont regroupées par valeur de balise, le cas échéant. Les ressources sans cette clé de balise sont regroupées et analysées séparément.
  - Choisissez des valeurs de balise spécifiques : toutes les ressources contenant une balise avec la clé que vous avez choisie sont analysées. DevOpsGuru regroupe vos ressources dans des applications en fonction des valeurs de votre tag.

  Pour de plus amples informations, veuillez consulter Utiliser des balises pour identifier les ressources dans vos applications DevOps Guru.
- Choisissez Aucune si vous ne voulez pas que DevOps Guru analyse les ressources. Cette option désactive DevOps Guru afin que vous arrêtiez de payer des frais liés à l'analyse des ressources.

5. Choisissez Save (Enregistrer).

Suppression de la vue des ressources analysées pour les utilisateurs

Même si un utilisateur n'a pas l'autorisation explicite d'accéder APIs à un autre service tel que Lambda ou Amazon RDS, DevOps Guru fournit toujours une liste des ressources de ce service tant que l'`ListMonitoredResources`action est autorisée. Pour modifier ce comportement, vous pouvez mettre à jour votre politique AWS IAM afin de refuser cette action.

```
{
            "Sid": "DenyListMonitoredResources",
            "Effect": "Deny",
            "Action": [
                "devops-guru:ListMonitoredResources"
            ]
}
```

Les meilleures pratiques dans DevOps Guru

Les bonnes pratiques suivantes peuvent vous aider à comprendre, diagnostiquer et corriger les comportements anormaux détectés par Amazon DevOps Guru. Utilisez les meilleures pratiques Comprendre les informations contenues dans la console DevOps Guru pour résoudre les problèmes opérationnels détectés par DevOps Guru.

- Dans la vue chronologique d'un aperçu, examinez d'abord les indicateurs mis en évidence. Ce sont souvent des indicateurs clés du problème.
- Utilisez Amazon CloudWatch pour consulter les indicateurs survenus juste avant le premier indicateur mis en évidence afin de déterminer quand et comment le comportement a changé. Cela peut vous aider à diagnostiquer et à résoudre le problème.
- Pour les ressources Amazon RDS, consultez les métriques Performance Insights. En corrélant les contre-métriques avec le chargement de la base de données, vous pouvez obtenir des informations détaillées sur les problèmes de performances. Pour plus d'informations, consultez Analyser les anomalies de performances avec DevOps Gurufor Amazon RDS.
- Plusieurs dimensions d'une même métrique peuvent souvent être anormales. Examinez les dimensions dans la vue graphique pour mieux comprendre le problème.
- Consultez la section des événements d'un aperçu pour connaître les événements de déploiement ou d'infrastructure survenus au moment où l'aperçu a été créé. Le fait de savoir quels événements se sont produits lorsque le comportement anormal d'un aperçu s'est produit peut vous aider à comprendre et à diagnostiquer le problème.
- Recherchez dans votre système d'exploitation les tickets survenus à peu près au même moment pour obtenir des indices.
- Pour en savoir plus, lisez les recommandations et consultez les liens figurant dans les recommandations. Ils comportent souvent des étapes de dépannage qui peuvent vous aider à diagnostiquer et à résoudre les problèmes rapidement.
- N'ignorez pas les informations résolues, sauf si vous avez déjà résolu le problème. Une fois par jour, examinez les nouvelles informations, même si elles ont été résolues. Essayez de comprendre la cause première du plus grand nombre possible d'informations. Recherchez un schéma qui pourrait être le signe d'un problème systémique. Si un problème systémique n'est pas résolu, il pourrait entraîner des problèmes plus graves à l'avenir. La résolution des problèmes transitoires dès maintenant peut aider à prévenir de futurs incidents plus graves.

La sécurité dans Amazon DevOps Guru

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

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

- Sécurité du cloud : elle AWS est chargée de protéger l'infrastructure qui exécute AWS les services dans le AWS cloud. AWS vous fournit également des services que vous pouvez utiliser en toute sécurité. Third-party les auditeurs testent et vérifient régulièrement l'efficacité de notre sécurité dans le AWS cadre des programmes de . Pour en savoir plus sur les programmes de conformité qui s'appliquent à Amazon DevOps Guru, consultez la section Services .
- Sécurité dans le cloud — Votre responsabilité est déterminée par le AWS service que vous utilisez. Vous êtes également responsable d'autres facteurs, y compris de la sensibilité de vos données, des exigences de votre entreprise, ainsi que de la législation et de la réglementation applicables.

Cette documentation vous aide à comprendre comment appliquer le modèle de responsabilité partagée lors de l'utilisation de DevOps Guru. Les rubriques suivantes vous montrent comment configurer DevOps Guru pour atteindre vos objectifs de sécurité et de conformité. Vous apprendrez également à utiliser d'autres services AWS qui vous aident à surveiller et à sécuriser vos ressources DevOps Guru.

Rubriques

- Protection des données dans Amazon DevOps Guru
- Gestion des identités et des accès pour Amazon DevOps Guru
- DevOpsGuru de journalisation et de surveillance
- DevOpsPoints de terminaison VPC Guru et interface (AWS PrivateLink)
- Sécurité des infrastructures à DevOps Guru
- La résilience dans Amazon DevOps Guru

Protection des données dans Amazon DevOps Guru

Le modèle de responsabilité AWS https://aws.amazon.com/compliance/shared-responsibility-model/ s'applique à la protection des données dans Amazon DevOps Guru. Comme décrit dans ce modèle, AWS est responsable de la protection de l'infrastructure mondiale qui gère l'ensemble des AWS Cloud. La gestion du contrôle de votre contenu hébergé sur cette infrastructure relève de votre responsabilité. Vous êtes également responsable des tâches de configuration et de gestion de la sécurité des Services AWS que vous utilisez. Pour plus d'informations sur la confidentialité des données, consultez la FAQ sur la confidentialité des données et les conditions légales de la région . Pour plus d'informations sur la protection des données en Europe, consultez le Centre du règlement général sur la protection des données (RGPD).

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 Gestion des identités et des accès AWS (IAM). Ainsi, chaque utilisateur se voit attribuer uniquement les autorisations nécessaires pour exécuter ses tâches. Nous vous recommandons également de sécuriser vos données comme indiqué ci-dessous :

- Utilisez l'authentification multifactorielle (MFA) avec chaque compte.
- SSL/TLS À utiliser pour communiquer avec AWS les ressources. Nous exigeons TLS 1.2 et recommandons TLS 1.3.
- Configurez l'API et la journalisation des activités des utilisateurs avec AWS CloudTrail. Pour plus d'informations sur l'utilisation des CloudTrail sentiers pour enregistrer AWS des activités, consultez la section Utilisation des CloudTrail sentiers dans le Guide de AWS CloudTrail l'utilisateur.
- Utilisez des solutions de AWS cryptage, ainsi que tous les contrôles de sécurité par défaut qui s'y trouvent Services AWS.
- Utilisez des services de sécurité gérés avancés tels qu'Amazon Macie, qui contribuent à la découverte et à la sécurisation des données sensibles stockées dans Amazon S3.
- Si vous avez besoin de modules cryptographiques validés par la norme FIPS 140-3 pour accéder AWS via une interface de ligne de commande ou une API, utilisez un point de terminaison FIPS. Pour plus d'informations sur les points de terminaison FIPS disponibles, consultez Norme FIPS (Federal Information Processing Standard) 140-3.

Nous vous recommandons fortement de ne jamais placer d'informations confidentielles ou sensibles, telles que les adresses e-mail de vos clients, dans des balises ou des champs de texte libre tels que le champ Nom. Cela inclut lorsque vous travaillez avec DevOps Guru ou autre à Services AWS l'aide

de la console, de l'API ou des AWS kits de développement logiciel. AWS CLI Toutes les données que vous entrez dans des balises ou des champs de texte de forme libre utilisés pour les noms peuvent être utilisées à des fins de facturation ou dans les journaux de diagnostic. Si vous fournissez une adresse URL à un serveur externe, nous vous recommandons fortement de ne pas inclure d'informations d'identification dans l'adresse URL permettant de valider votre demande adressée à ce serveur.

Chiffrement des données dans DevOps Guru

Le chiffrement est un élément important de la sécurité de DevOps Guru. Certains chiffrements, par exemple pour les données en transit, sont fournis par défaut et ne nécessitent aucune action de votre part. Vous pouvez configurer d'autres types de chiffrement, par exemple pour les données au repos, lors de la création ou de la compilation de votre projet.

- Chiffrement des données en transit : toutes les communications entre les clients et DevOps Guru et entre DevOps Guru et ses dépendances en aval sont protégées à l'aide du protocole TLS et authentifiées à l'aide du processus de signature Signature Version 4. Tous les terminaux DevOps Guru utilisent des certificats gérés par Autorité de certification privée AWS. Pour de plus amples informations, veuillez consulter Processus de signature Signature Version 4 et Présentation d'ACM PCA.
- Chiffrement des données au repos : pour toutes les AWS ressources analysées par DevOps Guru, les CloudWatch métriques et données Amazon, les identifiants de ressources et les AWS CloudTrail événements sont stockés via Amazon S3, Amazon DynamoDB et Amazon Kinesis. Si CloudFormation des piles sont utilisées pour définir les ressources analysées, les données des piles sont également collectées. DevOpsGuru utilise les politiques de conservation des données d'Amazon S3, DynamoDB et Kinesis. Les données stockées dans Kinesis peuvent être conservées jusqu'à un an, en fonction des politiques définies. Les données stockées dans Amazon S3 et DynamoDB sont conservées pendant un an.

  Les données stockées sont chiffrées à l'aide des fonctionnalités de chiffrement des données au repos d'Amazon S3, DynamoDB et Kinesis.

  Clés gérées par le client : DevOps Guru prend en charge le cryptage du contenu client et des métadonnées sensibles telles que les anomalies de journal générées à partir CloudWatch des journaux avec des clés gérées par le client. Cette fonctionnalité vous permet d'ajouter une couche de sécurité autogérée pour vous aider à répondre aux exigences réglementaires et de conformité de votre organisation. Pour plus d'informations sur l'activation des clés gérées par le client dans vos paramètres DevOps Guru, consultezthe section called “Mettre à jour le chiffrement”.

Étant donné que vous avez le contrôle total de cette couche de chiffrement, vous pouvez effectuer les tâches suivantes :

- Établissement et gestion des stratégies de clé
- Établissement et gestion des politiques IAM et des octrois
- Activation et désactivation des stratégies de clé
- Rotation des matériaux de chiffrement de clé
- Ajout de balises
- Création d'alias de clé
- Planification des clés pour la suppression

Pour plus d'informations, consultez la section Clés gérées par le client dans le Guide du AWS Key Management Service développeur.

> **Note**
>
> DevOpsGuru active automatiquement le chiffrement au repos à l'aide de clés AWS détenues pour protéger gratuitement les métadonnées sensibles. L'utilisation d'une clé gérée par le client entraîne toutefois des AWS KMS frais. Pour plus d'informations sur la tarification, consultez la rubrique AWS Key Management Service Tarification.

Comment DevOps Guru utilise les subventions dans AWS KMS

DevOpsGuru a besoin d'une subvention pour utiliser votre clé gérée par le client.

Lorsque vous choisissez d'activer le chiffrement à l'aide d'une clé gérée par le client, DevOps Guru crée une subvention en votre nom en envoyant une CreateGrant demande à AWS KMS. Les subventions AWS KMS sont utilisées pour permettre à DevOps Guru d'accéder à une AWS KMS clé d'un compte client.

DevOpsGuru a besoin de cette autorisation pour utiliser votre clé gérée par le client pour les opérations internes suivantes :

- Envoyez DescribeKey des demandes AWS KMS à pour vérifier que l'ID de clé KMS géré par le client symétrique saisi lors de la création d'un tracker ou d'une collection de géofence est valide.

- Envoyez GenerateDataKey des demandes AWS KMS à pour générer des clés de données chiffrées par la clé gérée par votre client.
- Envoyez des demandes de déchiffrement AWS KMS à pour déchiffrer les clés de données cryptées afin qu'elles puissent être utilisées pour crypter vos données.

Vous pouvez révoquer l'accès à l'octroi ou supprimer l'accès du service à la clé gérée par le client à tout moment. Si vous le faites, DevOps Guru ne pourra accéder à aucune des données chiffrées par la clé gérée par le client, ce qui affectera les opérations qui dépendent de ces données. Par exemple, si vous tentez d'obtenir des informations chiffrées sur les anomalies du journal auxquelles DevOps Guru ne peut pas accéder, l'opération renverra une AccessDeniedException erreur.

Surveillance de vos clés de chiffrement dans DevOps Guru

Lorsque vous utilisez une clé gérée par le AWS KMS client avec vos ressources DevOps Guru, vous pouvez utiliser AWS CloudTrail ou CloudWatch Logs pour suivre les demandes que DevOps Guru envoie AWS KMS.

Création d'une clé gérée par le client

Vous pouvez créer une clé symétrique gérée par le client à l'aide des API Console de gestion AWS ou des AWS KMS API.

Pour créer une clé gérée par le client symétrique, voir Création de clés KMS de chiffrement symétrique.

Stratégie de clé

Les stratégies de clé contrôlent l'accès à votre clé gérée par le client. Chaque clé gérée par le client doit avoir exactement une stratégie de clé, qui contient des instructions qui déterminent les personnes pouvant utiliser la clé et comment elles peuvent l'utiliser. Lorsque vous créez votre clé gérée par le client, vous pouvez spécifier une stratégie de clé. Pour plus d'informations, consultez la section Authentification et contrôle d'accès AWS KMS dans le Guide du AWS Key Management Service développeur.

Pour utiliser votre clé gérée par le client avec vos ressources DevOps Guru, les opérations d'API suivantes doivent être autorisées dans la politique de clé :

- `kms:CreateGrant` : ajoute une attribution à une clé gérée par le client. Les autorisations contrôlent l'accès à une AWS KMS clé spécifiée, ce qui permet d'accéder aux opérations de

subvention requises par DevOps Guru. Pour plus d'informations sur l'utilisation des subventions, consultez le Guide du AWS Key Management Service développeur.

Cela permet à DevOps Guru d'effectuer les opérations suivantes :

- Appelez GenerateDataKey pour générer une clé de données chiffrée et la stocker, car la clé de données n'est pas immédiatement utilisée pour chiffrer.
- Appelez Decrypt pour utiliser la clé de données cryptée stockée afin d'accéder aux données cryptées.
- Configurer un principal sortant pour permettre au service de RetireGrant.
- Utilisez kms : DescribeKey pour fournir les détails de la clé gérée par le client afin de permettre à DevOps Guru de valider la clé.

La déclaration suivante inclut des exemples de déclarations de politique que vous pouvez ajouter pour DevOps Guru :

```
"Statement" : [
  {
    "Sid" : "Allow access to principals authorized to use DevOps Guru",
    "Effect" : "Allow",
    "Principal" : {
      "AWS" : "*"
    },
    "Action" : [
      "kms:DescribeKey",
      "kms:CreateGrant"
    ],
    "Resource" : "*",
    "Condition" : {
      "StringEquals" : {
        "kms:ViaService" : "devops-guru.Region.amazonaws.com",
        "kms:CallerAccount" : "111122223333"
      }
  },
  {
    "Sid": "Allow access for key administrators",
    "Effect": "Allow",
    "Principal": {
      "AWS": "arn:aws:iam::111122223333:root"
     },
```

```
      "Action" : [
        "kms:*"
       ],
      "Resource": "arn:aws:kms:region:111122223333:key/key_ID"
    },
    {
      "Sid" : "Allow read-only access to key metadata to the account",
      "Effect" : "Allow",
      "Principal" : {
        "AWS" : "arn:aws:iam::111122223333:root"
      },
      "Action" : [
        "kms:Describe*",
        "kms:Get*",
        "kms:List*"
      ],
      "Resource" : "*"
    }
  ]
```

Confidentialité du trafic

Vous pouvez améliorer la sécurité de l'analyse de vos ressources et de la génération d'informations en configurant DevOps Guru pour qu'il utilise une interface VPC endpoint. Pour ce faire, vous n'avez pas besoin d'une passerelle Internet, d'un périphérique NAT ni d'une passerelle privée virtuelle. Il n'est pas non plus nécessaire de le configurer PrivateLink, bien que cela soit recommandé. Pour de plus amples informations, veuillez consulter DevOpsPoints de terminaison VPC Guru et interface (AWS PrivateLink). Pour plus d'informations sur PrivateLink les points de terminaison VPC, consultez la section Accès AWS PrivateLink aux services AWS via. PrivateLink

Gestion des identités et des accès pour Amazon DevOps Guru

Gestion des identités et des accès AWS (IAM) permet à un Service AWS administrateur de contrôler en toute sécurité l'accès aux AWS ressources. Les administrateurs IAM contrôlent qui peut être authentifié (connecté) et autorisé (possède des autorisations) à utiliser les ressources DevOps Guru. IAM est un Service AWS outil que vous pouvez utiliser sans frais supplémentaires.

Rubriques

- Public ciblé

- Authentification par des identités
- Gestion de l'accès à l'aide de politiques
- DevOpsMises à jour de Guru AWS politiques gérées et rôle lié aux services
- Comment Amazon DevOps Guru fonctionne avec IAM
- Identity-based politiques relatives à Amazon DevOps Guru
- Utilisation de rôles liés à des services pour Guru DevOps
- Référence des autorisations Amazon DevOps Guru
- Autorisations pour les rubriques Amazon SNS
- Autorisations pour AWS KMS—rubriques Amazon SNS cryptées
- Résolution des problèmes d'identité et d'accès à Amazon DevOps Guru

Public ciblé

La façon dont vous utilisez Gestion des identités et des accès AWS (IAM) varie en fonction de votre rôle :

- Utilisateur du service : demandez des autorisations à votre administrateur si vous ne pouvez pas accéder aux fonctionnalités (voir Résolution des problèmes d'identité et d'accès à Amazon DevOps Guru)
- Administrateur du service : déterminez l'accès des utilisateurs et soumettez les demandes d'autorisation (voir Comment Amazon DevOps Guru fonctionne avec IAM)
- Administrateur IAM : rédigez des politiques pour gérer l'accès (voir Identity-based politiques relatives à Amazon DevOps Guru)

Authentification par des identités

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

Vous pouvez vous connecter en tant qu'identité fédérée à l'aide d'informations d'identification provenant d'une source d'identité telle que AWS IAM Identity Center (IAM Identity Center), de l'authentification unique ou d'informations d'identification. Google/Facebook Pour plus d'informations

sur la connexion, consultez Connexion à votre Compte AWS dans le Guide de l'utilisateur Connexion à AWS .

Pour l'accès par programmation, AWS fournit un SDK et une interface de ligne de commande pour signer les demandes de manière cryptographique. Pour plus d'informations, consultez Signature AWS Version 4 pour les demandes d'API dans le Guide de l'utilisateur IAM.

Compte AWS utilisateur root

Lorsque vous créez un Compte AWS, vous commencez avec une seule identité de connexion appelée utilisateur Compte AWS root qui dispose d'un accès complet à toutes Services AWS les ressources. Il est vivement déconseillé d'utiliser l'utilisateur racine pour vos tâches quotidiennes. Pour les tâches qui requièrent des informations d'identification de l'utilisateur racine, consultez Tâches qui requièrent les informations d'identification de l'utilisateur racine dans le Guide de l'utilisateur IAM.

Identité fédérée

Il est recommandé d'obliger les utilisateurs humains à utiliser la fédération avec un fournisseur d'identité pour accéder à l' Services AWS aide d'informations d'identification temporaires.

Une identité fédérée est un utilisateur de votre annuaire d'entreprise, de votre fournisseur d'identité Web ou Directory Service qui accède à l' Services AWS aide d'informations d'identification provenant d'une source d'identité. Les identités fédérées assument des rôles qui fournissent des informations d'identification temporaires.

Pour une gestion des accès centralisée, nous vous recommandons d'utiliser AWS IAM Identity Center. Pour plus d'informations, consultez Qu'est-ce que IAM Identity Center ? dans le Guide de l'utilisateur AWS IAM Identity Center .

Utilisateurs et groupes IAM

Un utilisateur IAM est une identité qui dispose d'autorisations spécifiques pour une seule personne ou application. Nous vous recommandons d'utiliser ces informations d'identification temporaires au lieu des utilisateurs IAM avec des informations d'identification à long terme. Pour plus d'informations, voir Exiger des utilisateurs humains qu'ils utilisent la fédération avec un fournisseur d'identité pour accéder à AWS l'aide d'informations d'identification temporaires dans le Guide de l'utilisateur IAM.

Les groupes IAM spécifient une collection d'utilisateurs IAM et permettent de gérer plus facilement les autorisations pour de grands ensembles d'utilisateurs. Pour plus d'informations, consultez Cas d'utilisation pour les utilisateurs IAM dans le Guide de l'utilisateur IAM.

Rôles IAM

Un rôle IAM est une identité dotée d'autorisations spécifiques qui fournit des informations d'identification temporaires. Vous pouvez assumer un rôle en passant d'un rôle utilisateur à un rôle IAM (console) ou en appelant une opération AWS CLI ou AWS API. Pour plus d'informations, consultez Méthodes pour endosser un rôle dans le Guide de l'utilisateur IAM.

Les rôles IAM sont utiles pour l'accès des utilisateurs fédérés, les autorisations temporaires des utilisateurs IAM, les accès intercompte, les accès entre services et les applications exécutées sur Amazon EC2. Pour plus d'informations, consultez Accès intercompte aux ressources dans IAM dans le Guide de l'utilisateur IAM.

Gestion de l'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 définit les autorisations lorsqu'elles sont associées à une identité ou à une ressource. AWS évalue ces politiques lorsqu'un directeur fait une demande. La plupart des politiques sont stockées AWS sous forme de documents JSON. Pour plus d'informations les documents de politique JSON, consultez Vue d'ensemble des politiques JSON dans le Guide de l'utilisateur IAM.

À l'aide de politiques, les administrateurs précisent qui a accès à quoi en définissant 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. Un administrateur IAM crée des politiques IAM et les ajoute aux rôles, que les utilisateurs peuvent ensuite assumer. Les politiques IAM définissent les autorisations quelle que soit la méthode que vous utilisez pour exécuter l'opération.

Identity-based politiques

Identity-based les politiques sont des documents de politique d'autorisations JSON que vous associez à une identité (utilisateur, groupe ou rôle). Ces politiques contrôlent les actions que peuvent exécuter ces identités, sur quelles ressources et dans quelles conditions. Pour découvrir comment créer une politique basée sur l'identité, consultez Définition d'autorisations IAM personnalisées avec des politiques gérées par le client dans le Guide de l'utilisateur IAM.

Identity-based les politiques peuvent être des politiques en ligne (intégrées directement dans une identité unique) ou des politiques gérées (politiques autonomes associées à plusieurs identités).

Pour découvrir comment choisir entre des politiques gérées et en ligne, consultez Choix entre les politiques gérées et les politiques en ligne dans le Guide de l'utilisateur IAM.

Resource-based politiques

Resource-based les politiques sont des documents de stratégie JSON que vous joignez à une ressource. Les exemples incluent les politiques de confiance de rôle IAM et les stratégies de compartiment Amazon S3. Dans les services qui sont compatibles avec les politiques basées sur les ressources, les administrateurs de service peuvent les utiliser pour contrôler l'accès à une ressource spécifique. Vous devez spécifier un principal dans une politique basée sur les ressources.

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

Autres types de politique

AWS prend en charge des types de politiques supplémentaires qui peuvent définir les autorisations maximales accordées par les types de politiques les plus courants :

- Limites d'autorisations : une limite des autorisations définit le nombre maximum d'autorisations qu'une politique basée sur l'identité peut accorder à une entité IAM. Pour plus d'informations, consultez Limites d'autorisations pour des entités IAM dans le Guide de l'utilisateur IAM.
- Politiques de contrôle des services (SCP) : spécifient les autorisations maximales pour une organisation ou une unité organisationnelle dans AWS Organizations. Pour plus d'informations, consultez Politiques de contrôle de service dans le Guide de l'utilisateur AWS Organizations .
- Politiques de contrôle des ressources (RCP) : définissent les autorisations maximales disponibles pour les ressources de votre organisation. Pour plus d'informations, consultez Politiques de contrôle des ressources (RCP) dans le Guide de l'utilisateur AWS Organizations .
- Politiques de session : politiques avancées que vous passez en tant que paramètre lorsque vous créez par programmation une session temporaire pour un rôle ou un utilisateur fédéré. Pour plus d'informations, consultez Politiques de session dans le Guide de l'utilisateur IAM.

Plusieurs types de politique

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

DevOpsMises à jour de Guru AWS politiques gérées et rôle lié aux services

Consultez les détails des mises à jour apportées aux politiques AWS gérées et au rôle lié aux services pour DevOps Guru depuis que ce service a commencé à suivre ces modifications. Pour recevoir des alertes automatiques concernant les modifications apportées à cette page, abonnez-vous au fil RSS du DevOps GuruHistorique du document Amazon DevOps Guru.

Modifier	Description	Date
AmazonDevOpsGuruConsoleFullAccess - Mettre à jour vers une politique existante.	La politique `AmazonDevOpsGuruFullAccess` gérée prend désormais en charge les abonnements Amazon SNS.	9 août 2023
AmazonDevOpsGuruReadOnlyAccess : mise à jour d'une politique existante	La politique `AmazonDevOpsGuruReadOnlyAccess` gérée prend désormais en charge l'accès en lecture seule aux listes d'abonnements Amazon SNS.	9 août 2023
AmazonDevOpsGuruServiceRolePolicy - Mettre à jour vers une politique existante.	Le rôle `AWSServiceRoleForDevOpsGuru` lié à un service prend désormais en charge l'accès aux actions GET d'API Gateway sur les API REST.	11 janvier 2023
AmazonDevOpsGuruServiceRolePolicy - Mettre à jour vers une politique existante.	Le rôle `AWSServiceRoleForDevOpsGuru` lié à un service prend désormais en charge plusieurs actions Amazon Simple Storage Service et Service Quotas.	19 octobre 2022

Modifier	Description	Date
AmazonDevOpsGuruFullAccess : mise à jour d'une politique existante	La politique gérée `AmazonDevOpsGuruFullAccess` prend désormais en charge l'accès à l' CloudWatch `FilterLogEvents` action.	30 août 2022
AmazonDevOpsGuruConsoleFullAccess : mise à jour d'une politique existante	La politique `AmazonDevOpsGuruConsoleFullAccess` gérée prend désormais en charge l'accès à l' CloudWatch`FilterLogEvents` action.	30 août 2022
AmazonDevOpsGuruReadOnlyAccess : mise à jour d'une politique existante	La politique `AmazonDevOpsGuruReadOnlyAccess` gérée prend désormais en charge l'accès en lecture seule à l' CloudWatch `FilterLogEvents` action.	30 août 2022
AmazonDevOpsGuruServiceRolePolicy - Mettre à jour vers une politique existante.	Le rôle `AWSServiceRoleForDevOpsGuru` lié à un service prend désormais en charge les CloudWatch journaux, les actions `FilterLogEvents` `DescribeLogGroups` , et. `DescribeLogStreams`	12 juillet 2022
Identity-based politiques pour DevOps Guru — Nouvelle politique gérée.	La `AmazonDevOpsGuruConsoleFullAccess` politique a été ajoutée.	16 décembre 2021

Modifier	Description	Date
AmazonDevOpsGuruServiceRolePolicy - Mettre à jour vers une politique existante.	Le rôle `AWSServiceRoleForDevOpsGuru` lié à un service prend désormais en charge Performance Insights et `DescribeMetricsKeys` les actions Amazon RDS`DescribeDBInstances` .	1er décembre 2021
AmazonDevOpsGuruReadOnlyAccess : mise à jour d'une politique existante	La politique `AmazonDevOpsGuruReadOnlyAccess` gérée prend désormais en charge l'accès en lecture seule aux actions Amazon RDS`DescribeDBInstances` .	1er décembre 2021
AmazonDevOpsGuruFullAccess : mise à jour d'une politique existante	La politique `AmazonDevOpsGuruFullAccess` gérée prend désormais en charge l'accès aux `DescribeDBInstances` actions Amazon RDS.	1er décembre 2021

Modifier	Description	Date
Identity-based politiques relatives à Amazon DevOps Guru— Une nouvelle politique a été ajoutée.	Le rôle `AWSServiceRoleForDevOpsGuru` lié à un service permet désormais d'accéder aux actions Amazon RDS `DescribeDBInstances` et Performance Insights`GetResourceMetrics` . La politique `AmazonDevOpsGuruOrganizationsAccess` gérée permet d'accéder à DevOps Guru au sein d'une organisation.	16 novembre 2021
AmazonDevOpsGuruServiceRolePolicy - Mettre à jour vers une politique existante.	Le rôle `AWSServiceRoleForDevOpsGuru` lié aux services prend désormais en charge les organisations AWS.	4 novembre 2021
AmazonDevOpsGuruServiceRolePolicy - Mettre à jour vers une politique existante.	Le rôle `AWSServiceRoleForDevOpsGuru` lié à un service contient désormais de nouvelles conditions sur les actions `ssm:CreateOpsItem` et`ssm:AddTagsToResource` .	11 octobre 2021

Modifier	Description	Date
Service-linked autorisations de rôle pour DevOps Guru - Mettre à jour vers une politique existante.	Le rôle `AWSServiceRoleForDevOpsGuru` lié à un service contient désormais de nouvelles conditions sur les actions `ssm:CreateOpsItem` et `ssm:AddTagsToResource`.	14 juin 2021
AmazonDevOpsGuruReadOnlyAccess : mise à jour d'une politique existante	La politique `AmazonDevOpsGuruReadOnlyAccess` gérée permet désormais un accès en lecture seule aux actions Gestion des identités et des accès AWS `GetRole` et aux actions DevOps Guru `DescribeFeedback`.	14 juin 2021
AmazonDevOpsGuruReadOnlyAccess : mise à jour d'une politique existante	La politique `AmazonDevOpsGuruReadOnlyAccess` gérée permet désormais un accès en lecture seule au DevOps Guru `GetCostEstimation` et `StartCostEstimation` aux actions.	27 avril 2021

Modifier	Description	Date
AmazonDevOpsGuruServiceRolePolicy - Mettre à jour vers une politique existante.	Le `AWSServiceRoleForDevOpsGuru` rôle permet désormais d'accéder aux `DescribeAutoScalingGroups` actions Amazon EC2 Auto Scaling AWS Systems Manager `AddTagsToResource` et à Amazon EC2.	27 avril 2021
DevOpsGuru a commencé à suivre les modifications	DevOpsGuru a commencé à suivre les modifications apportées AWS à ses politiques gérées.	10 décembre 2020

Comment Amazon DevOps Guru fonctionne avec IAM

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

Fonctionnalités IAM que vous pouvez utiliser avec Amazon Guru DevOps

Fonctionnalité IAM	DevOpsAssistance Guru
Identity-based politiques	Oui
Resource-based politiques	Non
Actions de politique	Oui
Ressources de politique	Oui
Clés de condition de politique	Oui
ACL	Non

Fonctionnalité IAM	DevOpsAssistance Guru
ABAC (étiquettes dans les politiques)	Non
Informations d'identification temporaires	Oui
Autorisations de principal	Oui
Rôles du service	Non
Service-linked rôles	Oui

Pour obtenir une vue d'ensemble de la façon dont DevOps Guru et les autres AWS services fonctionnent avec la plupart des fonctionnalités IAM, consultez la section AWS Services qui fonctionnent avec IAM dans le Guide de l'utilisateur IAM.

Identity-based politiques pour DevOps Guru

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

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

Avec les politiques IAM basées sur l'identité, vous pouvez spécifier des actions et ressources autorisées ou refusées, ainsi que les conditions dans lesquelles les actions sont autorisées ou refusées. Pour découvrir tous les éléments que vous utilisez dans une politique JSON, consultez Références des éléments de politique JSON IAM dans le Guide de l'utilisateur IAM.

Identity-based exemples de politiques pour DevOps Guru

Pour consulter des exemples de politiques basées sur l'identité de DevOps Guru, consultez. Identity-based politiques relatives à Amazon DevOps Guru

Resource-based politiques au sein de DevOps Guru

Prend en charge les politiques basées sur les ressources : non

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

Pour permettre un accès intercompte, vous pouvez spécifier un compte entier ou des entités IAM dans un autre compte en tant que principal dans une politique basée sur les ressources. Pour plus d'informations, consultez Accès intercompte aux ressources dans IAM dans le Guide de l'utilisateur IAM.

Actions politiques pour DevOps Guru

Prend en charge les actions de politique : oui

Les administrateurs peuvent utiliser des 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. Intégration d'actions dans une politique afin d'accorder l'autorisation d'exécuter les opérations associées.

Pour consulter la liste des actions de DevOps Guru, consultez la section Actions définies par Amazon DevOps Guru dans la référence d'autorisation de service.

Les actions de stratégie dans DevOps Guru utilisent le préfixe suivant avant l'action :

```
aws
```

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

```
"Action": [
      "aws:action1",
```

```
      "aws:action2"
         ]
```

Pour consulter des exemples de politiques basées sur l'identité de DevOps Guru, consultez. Identity-based politiques relatives à Amazon DevOps Guru

Ressources politiques pour DevOps Guru

Prend en charge les ressources de politique : oui

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

L'élément de politique JSON `Resource` indique le ou les objets auxquels l'action s'applique. Il est recommandé de définir une ressource à l'aide de son Amazon Resource Name (ARN). Pour les actions qui ne sont pas compatibles avec les autorisations de niveau ressource, utilisez un caractère générique (*) afin d'indiquer que l'instruction s'applique à toutes les ressources.

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

Pour consulter la liste des types de ressources DevOps Guru et de leurs ARN, consultez la section Ressources définies par Amazon DevOps Guru dans la référence d'autorisation de service. Pour savoir quelles actions vous permettent de spécifier l'ARN de chaque ressource, consultez la section Actions définies par Amazon DevOps Guru.

Pour consulter des exemples de politiques basées sur l'identité de DevOps Guru, consultez. Identity-based politiques relatives à Amazon DevOps Guru

Clés de condition de politique pour DevOps Guru

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

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

L'élément `Condition` indique à quel moment les instructions s'exécutent en fonction de critères définis. Vous pouvez créer des expressions conditionnelles qui utilisent des opérateurs de condition, tels que les signes égal ou inférieur à, pour faire correspondre la condition de la politique aux valeurs de la demande. Pour voir toutes les clés de condition AWS globales, consultez les clés contextuelles de conditions AWS globales dans le guide de l'utilisateur IAM.

Pour consulter la liste des clés de condition DevOps Guru, consultez la section Clés de condition pour Amazon DevOps Guru dans la référence d'autorisation de service. Pour savoir avec quelles actions et quelles ressources vous pouvez utiliser une clé de condition, consultez la section Actions définies par Amazon DevOps Guru.

Pour consulter des exemples de politiques basées sur l'identité de DevOps Guru, consultez. Identity-based politiques relatives à Amazon DevOps Guru

Listes de contrôle d'accès (ACL) dans Guru DevOps

Prend en charge les ACL : non

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

Attribute-based contrôle d'accès (ABAC) avec Guru DevOps

Prise en charge d'ABAC (balises dans les politiques) : non

Attribute-based le contrôle d'accès (ABAC) est une stratégie d'autorisation qui définit les autorisations en fonction d'attributs appelés balises. Vous pouvez attacher des balises aux entités et AWS ressources IAM, puis concevoir des politiques ABAC pour autoriser les opérations lorsque la balise du principal correspond à celle de la ressource.

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

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

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

Utiliser des informations d'identification temporaires avec DevOps Guru

Prend en charge les informations d'identification temporaires : oui

Les informations d'identification temporaires fournissent un accès de courte durée aux AWS ressources et sont automatiquement créées lorsque vous utilisez la fédération ou que vous changez de rôle. AWS recommande de générer dynamiquement des informations d'identification temporaires au lieu d'utiliser des clés d'accès à long terme. Pour plus d'informations, consultez Informations d'identification de sécurité temporaires dans IAM et Services AWS compatibles avec IAM dans le Guide de l'utilisateur IAM.

Cross-service autorisations principales pour DevOps Guru

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

Les sessions d'accès direct (FAS) utilisent les autorisations du principal appelant et Service AWS, combinées Service AWS à la demande d'envoi de demandes aux services en aval. Pour plus de détails sur la politique relative à la transmission de demandes FAS, consultez la section Sessions de transmission d'accès.

Rôles de service pour DevOps Guru

Prend en charge les rôles de service : Non

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

> **Warning**
>
> La modification des autorisations pour un rôle de service peut interrompre les fonctionnalités de DevOps Guru. Modifiez les rôles de service uniquement lorsque DevOps Guru vous le conseille.

Service-linked rôles pour DevOps Guru

Prend en charge les rôles liés à un service : oui

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

Pour plus d'informations sur la création ou la gestion des rôles liés à un service, consultez Services AWS qui fonctionnent avec IAM. Recherchez un service dans le tableau qui inclut un `Yes` dans la colonne des Service-linked rôles. Choisissez le lien Oui pour consulter la documentation du rôle lié à ce service.

Identity-based politiques relatives à Amazon DevOps Guru

Par défaut, les utilisateurs et les rôles ne sont pas autorisés à créer ou à modifier les ressources DevOps Guru. 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.

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

Pour plus d'informations sur les actions et les types de ressources définis par DevOps Guru, y compris le format des ARN pour chacun des types de ressources, consultez la section Actions, ressources et clés de condition pour Amazon DevOps Guru dans la référence d'autorisation de service.

Rubriques

- Bonnes pratiques en matière de politiques
- Utilisation de la console DevOps Guru
- Autorisation accordée aux utilisateurs pour afficher leurs propres autorisations
- Politiques gérées (prédéfinies) par AWS pour DevOps Guru

Bonnes pratiques en matière de politiques

Identity-based les politiques déterminent si quelqu'un peut créer des ressources DevOps Guru sur votre compte, y accéder ou les supprimer. Ces actions peuvent entraîner des frais pour votre

Compte AWS. Lorsque vous créez ou modifiez des politiques basées sur l'identité, suivez ces instructions et recommandations :

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

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

Utilisation de la console DevOps Guru

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

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

Pour vous assurer que les utilisateurs et les rôles peuvent toujours utiliser la console DevOps Guru, associez également la politique DevOps Guru `AmazonDevOpsGuruReadOnlyAccess` ou `AmazonDevOpsGuruFullAccess` AWS gérée aux entités. Pour plus d'informations, consultez Ajout d'autorisations à un utilisateur dans le Guide de l'utilisateur IAM.

Autorisation accordée aux utilisateurs pour afficher leurs propres autorisations

Cet exemple montre comment créer une politique qui permet aux utilisateurs IAM d'afficher les politiques en ligne et gérées attachées à leur identité d'utilisateur. Cette politique inclut des autorisations pour 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": "*"
        }
    ]
}
```

Politiques gérées (prédéfinies) par AWS pour DevOps Guru

AWS répond à de nombreux cas d'utilisation courants en fournissant des politiques IAM autonomes créées et administrées par AWS. Ces politiques AWS gérées accordent les autorisations nécessaires pour les cas d'utilisation courants afin que vous n'ayez pas à rechercher quelles autorisations sont nécessaires. Pour de plus amples informations, veuillez consulter Stratégies gérées par AWS dans le Guide de l'utilisateur IAM.

Pour créer et gérer des rôles de service DevOps Guru, vous devez également joindre la politique AWS-managed nomméeIAMFullAccess.

Vous pouvez également créer vos propres politiques IAM personnalisées pour autoriser les actions et les ressources de DevOps Guru. Vous pouvez attacher ces stratégies personnalisées aux utilisateurs ou groupes qui nécessitent ces autorisations.

Les politiques AWS gérées suivantes, que vous pouvez associer aux utilisateurs de votre compte, sont spécifiques à DevOps Guru.

Rubriques

- AmazonDevOpsGuruFullAccess
- AmazonDevOpsGuruConsoleFullAccess
- AmazonDevOpsGuruReadOnlyAccess
- AmazonDevOpsGuruOrganizationsAccess

AmazonDevOpsGuruFullAccess

`AmazonDevOpsGuruFullAccess`— Fournit un accès complet à DevOps Guru, y compris des autorisations pour créer des rubriques Amazon SNS, accéder aux CloudWatch métriques Amazon et accéder aux AWS CloudFormation piles. Appliquez cette option uniquement aux utilisateurs de niveau administratif auxquels vous souhaitez accorder un contrôle total sur Guru. DevOps

La `AmazonDevOpsGuruFullAccess` politique contient la déclaration suivante.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "DevOpsGuruFullAccess",
            "Effect": "Allow",
            "Action": [
                "devops-guru:*"
            ],
            "Resource": "*"
        },
        {
            "Sid": "CloudFormationListStacksAccess",
            "Effect": "Allow",
            "Action": [
                "cloudformation:DescribeStacks",
                "cloudformation:ListStacks"
            ],
            "Resource": "*"
        },
        {
            "Sid": "CloudWatchGetMetricDataAccess",
            "Effect": "Allow",
            "Action": [
                "cloudwatch:GetMetricData"
            ],
            "Resource": "*"
        },
        {
            "Sid": "SnsListTopicsAccess",
            "Effect": "Allow",
```

```
            "Action": [
                "sns:ListTopics",
                "sns:ListSubscriptionsByTopic"
            ],
            "Resource": "*"
        },
        {
            "Sid": "SnsTopicOperations",
            "Effect": "Allow",
            "Action": [
                "sns:CreateTopic",
                "sns:GetTopicAttributes",
                "sns:SetTopicAttributes",
                "sns:Subscribe",
                "sns:Publish"
            ],
            "Resource": "arn:aws:sns:*:*:DevOps-Guru-*"
        },
        {
            "Sid": "DevOpsGuruSlrCreation",
            "Effect": "Allow",
            "Action": "iam:CreateServiceLinkedRole",
            "Resource": "arn:aws:iam::*:role/aws-service-role/devops-
guru.amazonaws.com/AWSServiceRoleForDevOpsGuru",
            "Condition": {
                "StringLike": {
                    "iam:AWSServiceName": "devops-guru.amazonaws.com"
                }
            }
        },
        {
            "Sid": "DevOpsGuruSlrDeletion",
            "Effect": "Allow",
            "Action": [
                "iam:DeleteServiceLinkedRole",
                "iam:GetServiceLinkedRoleDeletionStatus"
            ],
            "Resource": "arn:aws:iam::*:role/aws-service-role/devops-
guru.amazonaws.com/AWSServiceRoleForDevOpsGuru"
        },
        {
            "Sid": "RDSDescribeDBInstancesAccess",
            "Effect": "Allow",
            "Action": [
```

```
                "rds:DescribeDBInstances"
            ],
            "Resource": "*"
        },
        {
          "Sid": "CloudWatchLogsFilterLogEventsAccess",
          "Effect": "Allow",
          "Action": [
              "logs:FilterLogEvents"
          ],
          "Resource": "arn:aws:logs:*:*:log-group:*",
          "Condition": {
              "StringEquals": {
                  "aws:ResourceTag/DevOps-Guru-Analysis": "true"
              }
          }
        }
    ]
}
```

AmazonDevOpsGuruConsoleFullAccess

`AmazonDevOpsGuruConsoleFullAccess`— Fournit un accès complet à DevOps Guru, y compris des autorisations pour créer des rubriques Amazon SNS, accéder aux CloudWatch métriques Amazon et accéder aux AWS CloudFormation piles. Cette politique comporte des autorisations supplémentaires relatives aux informations sur les performances afin que vous puissiez consulter l'analyse détaillée relative aux instances de base de données Amazon RDS Aurora anormales dans la console. Appliquez cette option uniquement aux utilisateurs de niveau administratif auxquels vous souhaitez accorder un contrôle total sur Guru. DevOps

La `AmazonDevOpsGuruConsoleFullAccess` politique contient la déclaration suivante.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "DevOpsGuruFullAccess",
            "Effect": "Allow",
            "Action": [
```

```
                "devops-guru:*"
            ],
            "Resource": "*"
        },
        {
            "Sid": "CloudFormationListStacksAccess",
            "Effect": "Allow",
            "Action": [
                "cloudformation:DescribeStacks",
                "cloudformation:ListStacks"
            ],
            "Resource": "*"
        },
        {
            "Sid": "CloudWatchGetMetricDataAccess",
            "Effect": "Allow",
            "Action": [
                "cloudwatch:GetMetricData"
            ],
            "Resource": "*"
        },
        {
            "Sid": "SnsListTopicsAccess",
            "Effect": "Allow",
            "Action": [
                "sns:ListTopics",
                "sns:ListSubscriptionsByTopic"
            ],
            "Resource": "*"
        },
        {
            "Sid": "SnsTopicOperations",
            "Effect": "Allow",
            "Action": [
                "sns:CreateTopic",
                "sns:GetTopicAttributes",
                "sns:SetTopicAttributes",
                "sns:Subscribe",
                "sns:Publish"
            ],
            "Resource": "arn:aws:sns:*:*:DevOps-Guru-*"
        },
        {
            "Sid": "DevOpsGuruSlrCreation",
```

```
            "Effect": "Allow",
            "Action": "iam:CreateServiceLinkedRole",
            "Resource": "arn:aws:iam::*:role/aws-service-role/devops-
guru.amazonaws.com/AWSServiceRoleForDevOpsGuru",
            "Condition": {
                "StringLike": {
                    "iam:AWSServiceName": "devops-guru.amazonaws.com"
                }
            }
        },
        {
            "Sid": "DevOpsGuruSlrDeletion",
            "Effect": "Allow",
            "Action": [
                "iam:DeleteServiceLinkedRole",
                "iam:GetServiceLinkedRoleDeletionStatus"
            ],
            "Resource": "arn:aws:iam::*:role/aws-service-role/devops-
guru.amazonaws.com/AWSServiceRoleForDevOpsGuru"
        },
        {
            "Sid": "RDSDescribeDBInstancesAccess",
            "Effect": "Allow",
            "Action": [
                "rds:DescribeDBInstances"
            ],
            "Resource": "*"
        },
        {
            "Sid": "PerformanceInsightsMetricsDataAccess",
            "Effect": "Allow",
            "Action": [
                "pi:GetResourceMetrics",
                "pi:DescribeDimensionKeys"
            ],
            "Resource": "*"
        },
        {
          "Sid": "CloudWatchLogsFilterLogEventsAccess",
          "Effect": "Allow",
          "Action": [
              "logs:FilterLogEvents"
          ],
          "Resource": "arn:aws:logs:*:*:log-group:*",
```

```
            "Condition": {
                "StringEquals": {
                    "aws:ResourceTag/DevOps-Guru-Analysis": "true"
                }
            }
        }
    ]
}
```

AmazonDevOpsGuruReadOnlyAccess

`AmazonDevOpsGuruReadOnlyAccess`— Donne un accès en lecture seule à DevOps Guru et aux ressources associées dans d'autres AWS services. Appliquez cette politique aux utilisateurs auxquels vous souhaitez accorder la possibilité de consulter des informations, mais pas pour mettre à jour la limite de couverture des analyses de DevOps Guru, les rubriques Amazon SNS ou OpsCenter l'intégration de Systems Manager.

La `AmazonDevOpsGuruReadOnlyAccess` politique contient la déclaration suivante.

JSON

```
    {
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "DevOpsGuruReadOnlyAccess",
            "Effect": "Allow",
            "Action": [
                "devops-guru:DescribeAccountHealth",
                "devops-guru:DescribeAccountOverview",
                "devops-guru:DescribeAnomaly",
                "devops-guru:DescribeEventSourcesConfig",
                "devops-guru:DescribeFeedback",
                "devops-guru:DescribeInsight",
                "devops-guru:DescribeResourceCollectionHealth",
                "devops-guru:DescribeServiceIntegration",
                "devops-guru:GetCostEstimation",
                "devops-guru:GetResourceCollection",
                "devops-guru:ListAnomaliesForInsight",
                "devops-guru:ListEvents",
```

```
                "devops-guru:ListInsights",
                "devops-guru:ListAnomalousLogGroups",
                "devops-guru:ListMonitoredResources",
                "devops-guru:ListNotificationChannels",
                "devops-guru:ListRecommendations",
                "devops-guru:SearchInsights",
                "devops-guru:StartCostEstimation"
            ],
            "Resource": "*"
        },
        {
            "Sid": "CloudFormationListStacksAccess",
            "Effect": "Allow",
            "Action": [
                "cloudformation:DescribeStacks",
                "cloudformation:ListStacks"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "iam:GetRole"
            ],
            "Resource": "arn:aws:iam::*:role/aws-service-role/devops-
guru.amazonaws.com/AWSServiceRoleForDevOpsGuru"
        },
        {
            "Sid": "CloudWatchGetMetricDataAccess",
            "Effect": "Allow",
            "Action": [
                "cloudwatch:GetMetricData"
            ],
            "Resource": "*"
        },
        {
            "Sid": "RDSDescribeDBInstancesAccess",
            "Effect": "Allow",
            "Action": [
                "rds:DescribeDBInstances"
            ],
            "Resource": "*"
        },
        {
```

```
            "Sid": "SnsListTopicsAccess",
            "Effect": "Allow",
            "Action": [
                "sns:ListTopics",
                "sns:ListSubscriptionsByTopic"
            ],
            "Resource": "*"
        },
        {
          "Sid": "CloudWatchLogsFilterLogEventsAccess",
          "Effect": "Allow",
          "Action": [
              "logs:FilterLogEvents"
          ],
          "Resource": "arn:aws:logs:*:*:log-group:*",
          "Condition": {
              "StringEquals": {
                  "aws:ResourceTag/DevOps-Guru-Analysis": "true"
              }
          }
        }
    ]
}
```

AmazonDevOpsGuruOrganizationsAccess

`AmazonDevOpsGuruOrganizationsAccess`— Permet aux administrateurs des organisations d'accéder à la vue multi-comptes DevOps Guru au sein d'une organisation. Appliquez cette politique aux utilisateurs de niveau administrateur de votre organisation auxquels vous souhaitez accorder un accès complet à DevOps Guru au sein d'une organisation. Vous pouvez appliquer cette politique au compte de gestion et au compte d'administrateur délégué de votre organisation pour DevOps Guru. Vous pouvez appliquer `AmazonDevOpsGuruReadOnlyAccess` ou compléter `AmazonDevOpsGuruFullAccess` cette politique pour fournir un accès en lecture seule ou complet à DevOps Guru.

La `AmazonDevOpsGuruOrganizationsAccess` politique contient la déclaration suivante.

Utilisation de rôles liés à des services pour Guru DevOps

Amazon DevOps Guru utilise des Gestion des identités et des accès AWS rôles liés aux services (IAM). Un rôle lié à un service est un type unique de rôle IAM directement lié à Guru. DevOps

Service-linked les rôles sont prédéfinis par DevOps Guru et incluent toutes les autorisations dont le service a besoin pour appeler Amazon AWS CloudTrail CloudWatch AWS CodeDeploy AWS X-Ray, et AWS Organizations en votre nom.

Un rôle lié à un service facilite la configuration de DevOps Guru car vous n'avez pas à ajouter manuellement les autorisations nécessaires. DevOpsGuru définit les autorisations de ses rôles liés aux services et, sauf indication contraire, seul DevOps Guru peut assumer ses rôles. Les autorisations définies comprennent la politique de confiance et la politique d'autorisation. De plus, cette politique d'autorisation ne peut pas être attachée à une autre entité IAM.

Vous pouvez supprimer un rôle lié à un service uniquement après la suppression préalable de ses ressources connexes. Cela protège les ressources de votre DevOps Guru car vous ne pouvez pas supprimer par inadvertance l'autorisation d'accès aux ressources.

Service-linked autorisations de rôle pour DevOps Guru

DevOpsGuru utilise le rôle lié au service nommé. `AWSServiceRoleForDevOpsGuru` Il s'agit d'une politique AWS gérée avec des autorisations étendues dont DevOps Guru a besoin pour exécuter sur votre compte.

Le rôle lié à un service `AWSServiceRoleForDevOpsGuru` approuve le fait que le service suivant endosse le rôle :

- `devops-guru.amazonaws.com`

La politique d'autorisation des rôles `AmazonDevOpsGuruServiceRolePolicy` permet à DevOps Guru d'effectuer les actions suivantes sur les ressources spécifiées.

JSON

```
{
 "Version":"2012-10-17",
 "Statement": [
  {
   "Effect": "Allow",
   "Action": [
    "autoscaling:DescribeAutoScalingGroups",
    "cloudtrail:LookupEvents",
    "cloudwatch:GetMetricData",
    "cloudwatch:ListMetrics",
```

```
        "cloudwatch:DescribeAnomalyDetectors",
        "cloudwatch:DescribeAlarms",
        "cloudwatch:ListDashboards",
        "cloudwatch:GetDashboard",
        "cloudformation:GetTemplate",
        "cloudformation:ListStacks",
        "cloudformation:ListStackResources",
        "cloudformation:DescribeStacks",
        "cloudformation:ListImports",
        "codedeploy:BatchGetDeployments",
        "codedeploy:GetDeploymentGroup",
        "codedeploy:ListDeployments",
        "config:DescribeConfigurationRecorderStatus",
        "config:GetResourceConfigHistory",
        "events:ListRuleNamesByTarget",
        "xray:GetServiceGraph",
        "organizations:ListRoots",
        "organizations:ListChildren",
        "organizations:ListDelegatedAdministrators",
        "pi:GetResourceMetrics",
        "tag:GetResources",
        "lambda:GetFunction",
        "lambda:GetFunctionConcurrency",
        "lambda:GetAccountSettings",
        "lambda:ListProvisionedConcurrencyConfigs",
        "lambda:ListAliases",
        "lambda:ListEventSourceMappings",
        "lambda:GetPolicy",
        "ec2:DescribeSubnets",
        "application-autoscaling:DescribeScalableTargets",
        "application-autoscaling:DescribeScalingPolicies",
        "sqs:GetQueueAttributes",
        "kinesis:DescribeStream",
        "kinesis:DescribeLimits",
        "dynamodb:DescribeTable",
        "dynamodb:DescribeLimits",
        "dynamodb:DescribeContinuousBackups",
        "dynamodb:DescribeStream",
        "dynamodb:ListStreams",
        "elasticloadbalancing:DescribeLoadBalancers",
        "elasticloadbalancing:DescribeLoadBalancerAttributes",
        "rds:DescribeDBInstances",
        "rds:DescribeDBClusters",
        "rds:DescribeOptionGroups",
```

```
    "rds:DescribeDBClusterParameters",
    "rds:DescribeDBInstanceAutomatedBackups",
    "rds:DescribeAccountAttributes",
    "logs:DescribeLogGroups",
    "logs:DescribeLogStreams",
    "s3:GetBucketNotification",
    "s3:GetBucketPolicy",
    "s3:GetBucketPublicAccessBlock",
    "s3:GetBucketTagging",
    "s3:GetBucketWebsite",
    "s3:GetIntelligentTieringConfiguration",
    "s3:GetLifecycleConfiguration",
    "s3:GetReplicationConfiguration",
    "s3:ListAllMyBuckets",
    "s3:ListStorageLensConfigurations",
    "servicequotas:GetServiceQuota",
    "servicequotas:ListRequestedServiceQuotaChangeHistory",
    "servicequotas:ListServiceQuotas"
   ],
   "Resource": "*"
  },
  {
   "Sid": "AllowPutTargetsOnASpecificRule",
   "Effect": "Allow",
   "Action": [
    "events:PutTargets",
    "events:PutRule"
   ],
   "Resource": "arn:aws:events:*:*:rule/DevOps-Guru-managed-*"
  },
  {
   "Sid": "AllowCreateOpsItem",
   "Effect": "Allow",
   "Action": [
    "ssm:CreateOpsItem"
   ],
   "Resource": "*"
  },
  {
   "Sid": "AllowAddTagsToOpsItem",
   "Effect": "Allow",
   "Action": [
    "ssm:AddTagsToResource"
   ],
```

```
    "Resource": "arn:aws:ssm:*:*:opsitem/*"
   },
   {
    "Sid": "AllowAccessOpsItem",
    "Effect": "Allow",
    "Action": [
     "ssm:GetOpsItem",
     "ssm:UpdateOpsItem"
    ],
    "Resource": "*",
    "Condition": {
     "StringEquals": {
      "aws:ResourceTag/DevOps-GuruInsightSsmOpsItemRelated": "true"
     }
    }
   },
   {
    "Sid": "AllowCreateManagedRule",
    "Effect": "Allow",
    "Action": "events:PutRule",
    "Resource": "arn:aws:events:*:*:rule/DevOpsGuruManagedRule*"
   },
   {
    "Sid": "AllowAccessManagedRule",
    "Effect": "Allow",
    "Action": [
     "events:DescribeRule",
     "events:ListTargetsByRule"
    ],
    "Resource": "arn:aws:events:*:*:rule/DevOpsGuruManagedRule*"
   },
   {
    "Sid": "AllowOtherOperationsOnManagedRule",
    "Effect": "Allow",
    "Action": [
     "events:DeleteRule",
     "events:EnableRule",
     "events:DisableRule",
     "events:PutTargets",
     "events:RemoveTargets"
    ],
    "Resource": "arn:aws:events:*:*:rule/DevOpsGuruManagedRule*",
    "Condition": {
     "StringEquals": {
```

```
      "events:ManagedBy": "devops-guru.amazonaws.com"
     }
    }
   },
   {
    "Sid": "AllowTagBasedFilterLogEvents",
    "Effect": "Allow",
    "Action": [
     "logs:FilterLogEvents"
    ],
    "Resource": "arn:aws:logs:*:*:log-group:*",
    "Condition": {
     "StringEquals": {
      "aws:ResourceTag/DevOps-Guru-Analysis": "true"
     }
    }
   },
   {
    "Sid": "AllowAPIGatewayGetIntegrations",
    "Effect": "Allow",
    "Action": "apigateway:GET",
    "Resource": [
     "arn:aws:apigateway:*::/restapis/??????????",
     "arn:aws:apigateway:*::/restapis/*/resources",
     "arn:aws:apigateway:*::/restapis/*/resources/*/methods/*/integration"
    ]
   }
  ]
}
```

Création d'un rôle lié à un service pour Guru DevOps

Vous n’avez pas besoin de créer manuellement un rôle lié à un service. Lorsque vous créez un aperçu dans l' Console de gestion AWS AWS API AWS CLI, DevOps Guru crée le rôle lié au service pour vous.

> **Important**
>
> Ce rôle lié à un service peut apparaître dans votre compte si vous avez effectué une action dans un autre service utilisant les fonctionnalités prises en charge par ce rôle ; par exemple, il peut apparaître si vous avez ajouté DevOps Guru à un référentiel depuis. AWS CodeCommit

Modifier un rôle lié à un service pour Guru DevOps

DevOpsGuru ne vous permet pas de modifier le rôle `AWSServiceRoleForDevOpsGuru` lié au service. Après avoir créé un rôle lié à un service, vous ne pouvez pas changer le nom du rôle, car plusieurs entités peuvent faire référence à ce rôle. Néanmoins, vous pouvez modifier la description du rôle à l'aide d'IAM. Pour plus d'informations, consultez la section Modifier un Service-Linked rôle dans le guide de l'utilisateur IAM.

Supprimer un rôle lié à un service pour Guru DevOps

Si vous n'avez plus besoin d'utiliser une fonctionnalité ou un service qui nécessite un rôle lié à un service, nous vous recommandons de supprimer ce rôle. De cette façon, vous n'avez aucune entité inutilisée qui n'est pas surveillée ou gérée activement. Cependant, vous devez vous dissocier de tous les référentiels avant de pouvoir le supprimer manuellement.

> **Note**
>
> Si le service DevOps Guru utilise le rôle lorsque vous essayez de supprimer les ressources, la suppression peut échouer. Si cela se produit, patientez quelques minutes et réessayez.

Pour supprimer manuellement le rôle lié au service à l'aide d'IAM

Utilisez la console IAM AWS CLI, l'API ou l' AWS API pour supprimer le rôle lié au `AWSServiceRoleForDevOpsGuru` service. Pour plus d'informations, consultez la section Supprimer un Service-Linked rôle dans le guide de l'utilisateur IAM.

Référence des autorisations Amazon DevOps Guru

Vous pouvez utiliser des clés AWS de condition générales dans vos politiques DevOps Guru pour exprimer des conditions. Pour obtenir une liste, reportez-vous à la section Référence des éléments de politique JSON IAM dans le Guide de l'utilisateur IAM.

Vous spécifiez les actions dans le champ `Action` de la politique. Pour spécifier une action, utilisez le préfixe `devops-guru:` suivi du nom de l'opération d'API (par exemple, `devops-guru:SearchInsights` ou `devops-guru:ListAnomalies`). Pour spécifier plusieurs actions

dans une même instruction, séparez-les par une virgule (par exemple, `"Action": [ "devops-guru:SearchInsights", "devops-guru:ListAnomalies" ]`).

Utilisation de caractères génériques

Vous spécifiez un Amazon Resource Name (ARN), avec ou sans caractère générique (*), comme valeur de ressource dans le `Resource` champ de la politique. Vous pouvez utiliser un caractère générique pour spécifier plusieurs actions ou ressources. Par exemple, `devops-guru:*` spécifie toutes les actions du DevOps Guru et `devops-guru:List*` spécifie toutes les actions du DevOps Guru qui commencent par le mot`List`. L'exemple suivant fait référence à toutes les informations dont l'identifiant unique universel (UUID) commence par. `12345`

```
arn:aws:devops-guru:us-east-2:123456789012:insight:12345*
```

Vous pouvez utiliser le tableau suivant comme référence lorsque vous configurez Authentification par des identités et rédigez des politiques d'autorisations que vous pouvez associer à une identité IAM (politiques basées sur l'identité).

DevOpsOpérations de l'API Guru et autorisations requises pour les actions

`AddNotificationChannel`

Action : `devops-guru:AddNotificationChannel`

Nécessaire pour ajouter un canal de notification depuis DevOps Guru. Un canal de notification est utilisé pour vous avertir lorsque DevOps Guru génère un aperçu contenant des informations sur la manière d'améliorer vos opérations.

Ressource : *

`RemoveNotificationChannel`

`devops-guru:RemoveNotificationChannel`

Nécessaire pour supprimer un canal de notification de DevOps Guru. Un canal de notification est utilisé pour vous avertir lorsque DevOps Guru génère un aperçu contenant des informations sur la manière d'améliorer vos opérations.

Ressource : *

`ListNotificationChannels`

Action : `devops-guru:ListNotificationChannels`

Obligatoire pour renvoyer la liste des canaux de notification configurés pour DevOps Guru. Chaque canal de notification est utilisé pour vous avertir lorsque DevOps Guru génère un aperçu contenant des informations sur la manière d'améliorer vos opérations. Le seul type de notification pris en charge est Amazon Simple Notification Service.

Ressource : *

`UpdateResourceCollectionFilter`

Action : `devops-guru:UpdateResourceCollectionFilter`

Nécessaire pour mettre à jour la liste des CloudFormation piles utilisées pour spécifier les AWS ressources de votre compte qui sont analysées par DevOps Guru. L'analyse génère des informations qui incluent des recommandations, des mesures opérationnelles et des événements opérationnels que vous pouvez utiliser pour améliorer les performances de vos opérations. Cette méthode crée également les rôles IAM que vous devez utiliser CodeGuru OpsAdvisor.

Ressource : *

`GetResourceCollectionFilter`

Action : `devops-guru:GetResourceCollectionFilter`

Obligatoire pour renvoyer la liste des AWS CloudFormation piles utilisées pour spécifier les AWS ressources de votre compte qui sont analysées par DevOps Guru. L'analyse génère des informations qui incluent des recommandations, des mesures opérationnelles et des événements opérationnels que vous pouvez utiliser pour améliorer les performances de vos opérations.

Ressource : *

`ListInsights`

Action : `devops-guru:ListInsights`

Obligatoire pour renvoyer une liste d'informations sur votre AWS compte. Vous pouvez spécifier quelles informations sont renvoyées en fonction de leur heure de début, de leur statut (`ongoingouany`) et de leur type (`reactiveoupredictive`).

Ressource : *

`DescribeInsight`

Action : `devops-guru:DescribeInsight`

Obligatoire pour renvoyer les informations relatives à un aperçu que vous spécifiez à l'aide de son identifiant.

Ressource : *

`SearchInsights`

Action : `devops-guru:SearchInsights`

Obligatoire pour renvoyer une liste d'informations sur votre AWS compte. Vous pouvez spécifier quelles informations sont renvoyées en fonction de leur heure de début, de leurs filtres et de leur type (`reactiveoupredictive`).

Ressource : *

`ListAnomalies`

Action : `devops-guru:ListAnomalies`

Obligatoire pour renvoyer une liste des anomalies appartenant à un aperçu que vous spécifiez à l'aide de son ID.

Ressource : *

`DescribeAnomaly`

Action : `devops-guru:DescribeAnomaly`

Obligatoire pour renvoyer les informations relatives à une anomalie que vous spécifiez à l'aide de son identifiant.

Ressource : *

`ListEvents`

Action : `devops-guru:ListEvents`

Obligatoire pour renvoyer une liste des événements émis par les ressources évaluées par DevOps Guru. Vous pouvez utiliser des filtres pour spécifier quels événements sont renvoyés.

Ressource : *

`ListRecommendations`

Action : `devops-guru:ListRecommendations`

Obligatoire pour renvoyer une liste des recommandations d'un aperçu spécifié. Chaque recommandation comprend une liste de mesures et une liste d'événements liés aux recommandations.

Ressource : *

`DescribeAccountHealth`

Action : `devops-guru:DescribeAccountHealth`

Nécessaire pour renvoyer le nombre d'informations réactives ouvertes, le nombre d'informations prédictives ouvertes et le nombre de mesures analysées dans votre AWS compte. Utilisez ces chiffres pour évaluer l'état des opérations de votre AWS compte.

Ressource : *

`DescribeAccountOverview`

Action : `devops-guru:DescribeAccountOverview`

Nécessaire pour renvoyer les informations suivantes survenues au cours d'une période donnée : le nombre d'informations réactives ouvertes qui ont été créées, le nombre d'informations prédictives ouvertes créées et le temps moyen de restauration (MTTR) pour toutes les informations réactives fermées.

Ressource : *

`DescribeResourceCollectionHealthOverview`

Action : `devops-guru:DescribeResourceCollectionHealthOverview`

Nécessaire pour renvoyer le nombre d'informations prédictives ouvertes, d'informations réactives ouvertes et le temps moyen de restauration (MTTR) pour toutes les informations pour chaque CloudFormation pile spécifiée dans DevOps Guru.

Ressource : *

`DescribeIntegratedService`

Action : `devops-guru:DescribeIntegratedService`

Nécessaire pour renvoyer l'état d'intégration des services pouvant être intégrés à DevOps Guru. Le seul service qui peut être intégré à DevOps Guru est AWS Systems Manager celui qui peut être utilisé pour créer un OpsItem pour chaque aperçu généré.

Ressource : *

`UpdateIntegratedServiceConfig`

Action : `devops-guru:UpdateIntegratedServiceConfig`

Nécessaire pour activer ou désactiver l'intégration à un service pouvant être intégré à DevOps Guru. Le seul service qui peut être intégré à DevOps Guru est Systems Manager, qui peut être utilisé pour créer un OpsItem pour chaque aperçu généré.

Ressource : *

Autorisations pour les rubriques Amazon SNS

Utilisez les informations de cette rubrique uniquement si vous souhaitez configurer Amazon DevOps Guru pour envoyer des notifications sur les sujets Amazon SNS appartenant à un autre AWS compte.

Pour que DevOps Guru puisse envoyer des notifications à une rubrique Amazon SNS appartenant à un autre compte, vous devez associer une politique à la rubrique Amazon SNS qui autorise DevOps Guru à lui envoyer des notifications. Si vous configurez DevOps Guru pour envoyer des notifications aux sujets Amazon SNS appartenant au même compte que vous utilisez pour DevOps Guru, DevOps Guru ajoute une politique aux sujets pour vous.

Après avoir joint une politique pour configurer les autorisations pour une rubrique Amazon SNS dans un autre compte, vous pouvez ajouter la rubrique Amazon SNS dans DevOps Guru. Vous pouvez également mettre à jour votre politique Amazon SNS avec un canal de notification pour la rendre plus sécurisée.

> **Note**
>
> DevOpsGuru ne prend actuellement en charge que l'accès multicompte dans la même région.

Rubriques

- Configuration des autorisations pour une rubrique Amazon SNS dans un autre compte
- Ajouter une rubrique Amazon SNS depuis un autre compte
- Mettre à jour votre politique Amazon SNS avec un canal de notification (recommandé)

Configuration des autorisations pour une rubrique Amazon SNS dans un autre compte

Ajouter des autorisations en tant que rôle IAM

Pour utiliser une rubrique Amazon SNS depuis un autre compte après vous être connecté avec un rôle IAM, vous devez associer une politique à la rubrique Amazon SNS que vous souhaitez utiliser. Pour associer une politique à une rubrique Amazon SNS depuis un autre compte tout en utilisant un rôle IAM, vous devez disposer des autorisations suivantes pour cette ressource de compte dans le cadre de votre rôle IAM :

- SNS : CreateTopic
- SNS : GetTopicAttributes
- SNS : SetTopicAttributes
- sns:Publish

Joignez la politique suivante à la rubrique Amazon SNS que vous souhaitez utiliser. Pour la `Resource` clé, il *`topic-owner-account-id`* s'agit de l'ID de compte du propriétaire du sujet, *`topic-sender-account-id`* de l'ID de compte de l'utilisateur qui a configuré DevOps Guru et *`devops-guru-role`* du rôle IAM de l'utilisateur individuel impliqué. Vous devez remplacer les valeurs appropriées par *`region-id`* (par exemple,`us-west-2`) et*`my-topic-name`*.

Ajouter des autorisations en tant qu'utilisateur IAM

Pour utiliser une rubrique Amazon SNS provenant d'un autre compte en tant qu'utilisateur IAM, associez la politique suivante à la rubrique Amazon SNS que vous souhaitez utiliser. Pour la `Resource` clé, il *`topic-owner-account-id`* s'agit de l'ID de compte du propriétaire de la rubrique, *`topic-sender-account-id`* de l'ID de compte de l'utilisateur qui a configuré DevOps Guru et *`devops-guru-user-name`* de l'utilisateur IAM individuel impliqué. Vous devez remplacer les valeurs appropriées par *`region-id`* (par exemple,`us-west-2`) et*`my-topic-name`*.

> **Note**
>
> Dans la mesure du possible, nous vous recommandons de vous appuyer sur des informations d'identification temporaires plutôt que de créer des utilisateurs IAM ayant des informations d'identification à long terme telles que des mots de passe et des clés d'accès. Pour plus d'informations sur les bonnes pratiques dans IAM, consultez Bonnes pratiques de sécurité dans IAM dans le Guide de l'utilisateur IAM.

Ajouter une rubrique Amazon SNS depuis un autre compte

Après avoir configuré les autorisations pour une rubrique Amazon SNS dans un autre compte, vous pouvez ajouter cette rubrique Amazon SNS à vos paramètres de notification DevOps Guru. Vous pouvez ajouter la rubrique Amazon SNS à l'aide de la console AWS CLI ou de la console DevOps Guru.

- Lorsque vous utilisez la console, vous devez sélectionner l'option Utiliser un ARN de rubrique SNS pour spécifier une rubrique existante afin d'utiliser une rubrique provenant d'un autre compte.
- Lorsque vous utilisez l' AWS CLI opération add-notification-channel, vous devez spécifier le contenu de l'`TopicArn`objet. `NotificationChannelConfig`

Ajouter une rubrique Amazon SNS depuis un autre compte à l'aide de la console

1. Ouvrez la console Amazon DevOps Guru à l'adresse https://console.aws.amazon.com/devops-guru/.
2. Ouvrez le volet de navigation, puis choisissez Paramètres.
3. Accédez à la section Notifications et choisissez Modifier.
4. Choisissez Ajouter une rubrique SNS.
5. Choisissez Utiliser un ARN de rubrique SNS pour spécifier une rubrique existante.
6. Entrez l'ARN de la rubrique Amazon SNS que vous souhaitez utiliser. Vous devez déjà avoir configuré les autorisations pour cette rubrique en y joignant une politique.
7. (Facultatif) Choisissez Configuration des notifications pour modifier les paramètres de fréquence des notifications.
8. Choisissez Enregistrer.

Une fois que vous avez ajouté la rubrique Amazon SNS à vos paramètres de notification, DevOps Guru utilise cette rubrique pour vous informer des événements importants, tels que la création d'un nouvel aperçu.

Mettre à jour votre politique Amazon SNS avec un canal de notification (recommandé)

Après avoir ajouté un sujet, nous vous recommandons de renforcer la sécurité de votre politique en spécifiant des autorisations uniquement pour le canal de notification DevOps Guru qui contient votre sujet.

Mettez à jour votre politique thématique Amazon SNS avec un canal de notification (recommandé)

1. Exécutez la AWS CLI commande `list-notification-channels` DevOps Guru sur le compte depuis lequel vous souhaitez envoyer des notifications.

```
aws devops-guru list-notification-channels
```

2. Dans la `list-notification-channels` réponse, notez l'ID de chaîne qui contient l'ARN de votre rubrique Amazon SNS. L'identifiant de la chaîne est un guide.

   Par exemple, dans la réponse suivante, l'ID de canal pour le sujet avec l'ARN `arn:aws:sns:region-id:111122223333:topic-name` est *e89be5f7-989d-4c4c-b1fe-e7145037e531*

```
{
  "Channels": [
    {
      "Id": "e89be5f7-989d-4c4c-b1fe-e7145037e531",
      "Config": {
      "Sns": {
          "TopicArn": "arn:aws:sns:region-id:111122223333:topic-name"
        },
      "Filters": {
          "MessageTypes": ["CLOSED_INSIGHT", "NEW_INSIGHT", "SEVERITY_UPGRADED"],
          "Severities": ["HIGH", "MEDIUM"]
        }
      }
    }
  ]
}
```

3. Accédez à la politique que vous avez créée dans un autre compte à l'aide de l'ID du propriétaire de la rubrique dansthe section called “Configuration des autorisations pour une rubrique Amazon SNS dans un autre compte”. Dans l'`Condition`énoncé de la politique, ajoutez la ligne qui spécifie le`SourceArn`. L'ARN contient votre identifiant de région (par exemple`us-east-1`), le numéro de AWS compte de l'expéditeur du sujet et l'ID de canal que vous avez noté.

   Votre `Condition` relevé mis à jour ressemble à ce qui suit.

```
"Condition" : {
  "StringEquals" : {
```

```
    "AWS:SourceArn": "arn:aws:devops-guru:us-
east-1:111122223333:channel/e89be5f7-989d-4c4c-b1fe-e7145037e531",
    "AWS:SourceAccount": "111122223333"
   }
 }
```

Si vous `AddNotificationChannel` ne parvenez pas à ajouter votre rubrique SNS, vérifiez que votre politique IAM dispose des autorisations suivantes.

Autorisations pour AWS KMS—rubriques Amazon SNS cryptées

La rubrique Amazon SNS que vous spécifiez peut être chiffrée par AWS Key Management Service. Pour permettre à DevOps Guru de travailler sur des sujets chiffrés, vous devez d'abord créer une instruction, AWS KMS key puis ajouter l'instruction suivante à la politique de la clé KMS. Pour plus d'informations, consultez Chiffrement des messages publiés sur Amazon SNS avec AWS KMS, identificateurs de clé (KeyId) dans le Guide de l'AWS KMS utilisateur et Chiffrement des données dans le Guide du développeur Amazon Simple Notification Service.

> **Note**
>
> DevOpsGuru prend actuellement en charge les sujets cryptés à utiliser au sein d'un seul compte. L'utilisation d'un sujet chiffré sur plusieurs comptes n'est pas prise en charge pour le moment.

Résolution des problèmes d'identité et d'accès à Amazon DevOps Guru

Utilisez les informations suivantes pour vous aider à diagnostiquer et à résoudre les problèmes courants que vous pouvez rencontrer lorsque vous travaillez avec DevOps Guru et IAM.

Rubriques

- Je ne suis pas autorisé à effectuer une action dans DevOps Guru
- Je souhaite donner aux utilisateurs un accès programmatique
- Je ne suis pas autorisé à effectuer iam : PassRole
- Je souhaite autoriser des personnes extérieures à mon AWS compte pour accéder à mes ressources DevOps Guru

Je ne suis pas autorisé à effectuer une action dans DevOps Guru

Si cela vous Console de gestion AWS indique que vous n'êtes pas autorisé à effectuer une action, vous devez contacter votre administrateur pour obtenir de l'aide.

L'exemple d'erreur suivant se produit lorsque l'utilisateur `mateojackson` essaie d'utiliser la console pour afficher les détails d'une *`my-example-widget`* ressource fictive mais ne dispose pas des `aws:`*`GetWidget`* autorisations fictives.

```
User: arn:aws:iam::123456789012:user/mateojackson is not authorized to perform:
 aws:GetWidget on resource: my-example-widget
```

Dans ce cas, Mateo demande à son administrateur de mettre à jour ses politiques pour lui permettre d'accéder à la ressource *`my-example-widget`* à l'aide de l'action `aws:`*`GetWidget`*.

Je souhaite donner aux utilisateurs un accès programmatique

Les utilisateurs ont besoin d'un accès programmatique s'ils souhaitent interagir avec des AWS personnes extérieures au Console de gestion AWS. La manière d'accorder l'accès par programmation dépend du type d'utilisateur qui accède AWS.

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

Quel utilisateur a besoin d'un accès programmatique ?	À	Méthode
IAM	(Recommandé) Utilisez les informations d'identification de la console comme informations d'identification temporaires pour signer les AWS CLI demandes programmatiques adressées aux AWS SDK ou AWS aux API.	Suivez les instructions de l'interface que vous souhaitez utiliser. • Pour cela AWS CLI, consultez la section Connexion pour le développement AWS local dans le Guide de AWS Command Line Interface l'utilisateur. • Pour les AWS kits de développement, consultez la

Quel utilisateur a besoin d'un accès programmatique ?	À	Méthode
		section Connexion pour le développement AWS local dans le Guide de référence AWS des kits de développement logiciel et des outils.
Identité de la main-d'œuvre (Utilisateurs gérés dans IAM Identity Center)	Utilisez des informations d'identification temporaires pour signer les demandes programmatiques adressées aux AWS CLI AWS SDK ou AWS aux API.	Suivez les instructions de l'interface que vous souhaitez utiliser. • Pour cela AWS CLI, reportez-vous AWS CLI à la section Configuration de l'utilisation AWS IAM Identity Center dans le Guide de AWS Command Line Interface l'utilisateur. • Pour les AWS kits de développement logiciel, les outils et les AWS API, consultez la section Authentification IAM Identity Center dans le Guide de référence AWS des kits de développement logiciel et des outils.
IAM	Utilisez des informations d'identification temporaires pour signer les demandes programmatiques adressées aux AWS CLI AWS SDK ou AWS aux API.	Suivez les instructions de la section Utilisation des informations d'identification temporaires avec AWS les ressources du Guide de l'utilisateur IAM.

Quel utilisateur a besoin d'un accès programmatique ?	À	Méthode
IAM	(Non recommandé) Utilisez des informations d'identification à long terme pour signer des demandes programmatiques adressées aux AWS CLI AWS SDK ou AWS aux API.	Suivez les instructions de l'interface que vous souhaitez utiliser. • Pour cela AWS CLI, consultez la section Authentification à l'aide des informations d'identification utilisateur IAM dans le Guide de l'AWS Command Line Interface utilisateur. • Pour les AWS kits de développement logiciel et les outils, consultez la section Authentification à l'aide d'informations d'identification à long terme dans le Guide de référence AWS des kits de développement logiciel et des outils. • Pour les AWS API, consultez la section Gestion des clés d'accès pour les utilisateurs IAM dans le Guide de l'utilisateur IAM.

Je ne suis pas autorisé à effectuer iam : PassRole

Si vous recevez un message d'erreur indiquant que vous n'êtes pas autorisé à effectuer l'`iam:PassRole`action, vos politiques doivent être mises à jour pour vous permettre de transmettre un rôle à DevOps Guru.

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, vous devez disposer des autorisations nécessaires pour transmettre le rôle au service.

L'exemple d'erreur suivant se produit lorsqu'un utilisateur IAM nommé `marymajor` essaie d'utiliser la console pour effectuer une action dans DevOps Guru. Toutefois, l'action nécessite que le service ait des autorisations accordées par un rôle de service. Mary n'est pas autorisée à transmettre le rôle au service.

```
User: arn:aws:iam::123456789012:user/marymajor is not authorized to perform:
 iam:PassRole
```

Dans ce cas, les politiques de Mary doivent être mises à jour pour lui permettre d'exécuter l'action `iam:PassRole`.

Si vous avez besoin d'aide, contactez votre AWS administrateur. Votre administrateur vous a fourni vos informations d'identification de connexion.

Je souhaite autoriser des personnes extérieures à mon AWS compte pour accéder à mes ressources DevOps Guru

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 plus d'informations, consultez les éléments suivants :

- Pour savoir si DevOps Guru prend en charge ces fonctionnalités, consultezComment Amazon DevOps Guru fonctionne avec IAM.
- Pour savoir comment donner accès à vos ressources par l'intermédiaire de celles Comptes AWS que vous possédez, consultez la section Fournir l'accès à un utilisateur IAM dans un autre utilisateur Compte AWS qui vous appartient dans le Guide de l'utilisateur IAM.
- Pour savoir comment donner accès à vos ressources à des tiers Comptes AWS, consultez la section Fournir un accès à des ressources Comptes AWS détenues par des tiers dans le Guide de l'utilisateur IAM.

- Pour savoir comment fournir un accès par le biais de la fédération d'identité, consultez Fournir un accès à des utilisateurs authentifiés en externe (fédération d'identité) dans le Guide de l'utilisateur IAM.
- Pour en savoir plus sur la différence entre l'utilisation des rôles et des politiques basées sur les ressources pour l'accès intercompte, consultez Accès intercompte aux ressources dans IAM dans le Guide de l'utilisateur IAM.

DevOpsGuru de journalisation et de surveillance

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

- Amazon CloudWatch surveille vos AWS ressources et les applications que vous exécutez 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 EC2 et lancer automatiquement de nouvelles instances si nécessaire. Pour plus d'informations, consultez le guide de CloudWatch 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 au 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

- Supervision DevOps Guru avec Amazon CloudWatch
- Journalisation des appels d'API Amazon DevOps Guru avec AWS CloudTrail

Supervision DevOps Guru avec Amazon CloudWatch

Vous pouvez surveiller DevOps Guru à l'aide de CloudWatch, qui collecte des données brutes et les transforme en mesures lisibles en temps quasi réel. Ces statistiques sont enregistrées pour

une durée de 15 mois ; par conséquent, vous pouvez accéder aux informations historiques et acquérir un meilleur point de vue de la façon dont votre service ou application web s'exécute. Vous pouvez également définir des alarmes qui surveillent certains seuils et envoient des notifications ou prennent des mesures lorsque ces seuils sont atteints. Pour plus d'informations, consultez le guide de CloudWatch l'utilisateur Amazon.

Pour DevOps Guru, vous pouvez suivre les statistiques pour obtenir des informations et les mesures relatives à votre utilisation de DevOps Guru. Vous souhaiterez peut-être surveiller un grand nombre de créations pour vous aider `Insights` à déterminer si vos solutions opérationnelles présentent un comportement anormal. Vous pouvez également surveiller votre utilisation de DevOps Guru pour suivre vos coûts.

Le service DevOps Guru rapporte les métriques suivantes dans l'`AWS/DevOps-Guru`espace de noms.

Rubriques

- Métriques Insight
- DevOpsStatistiques d'utilisation de Guru

Métriques Insight

Vous pouvez utiliser CloudWatch pour suivre une métrique qui vous indique le nombre d'informations créées dans votre AWS compte. Vous pouvez spécifier la `Type` dimension à suivre `proactive` ou `reactive` les informations. Ne spécifiez pas de dimension si vous souhaitez suivre toutes les informations.

Métriques

Métrique	Description
`Insight`	Le nombre d'informations créées dans un AWS compte. Dimensions valides : `Type` Statistiques valides : nombre d'échantillons, somme Unités : nombre

La dimension suivante est prise en charge pour la `Insight` métrique DevOps Guru.

Dimensions

Dimension	Description
`Type`	C'est le type de perspicacité. Ne spécifiez pas de dimension pour la `Insights` métrique si vous souhaitez suivre toutes les informations. Les valeurs valides sont :`proactive` ,`reactive`.

DevOpsStatistiques d'utilisation de Guru

Vous pouvez l'utiliser CloudWatch pour suivre votre utilisation d'Amazon DevOps Guru.

Métriques

Métrique	Description
`CallCount`	Le nombre d'appels effectués par l'une des méthodes DevOps Guru suivantes. • `ListInsights` • `ListAnomaliesForInsight` • `ListRecommendations` • `ListEvents` • `SearchInsights` • `DescribeInsight` • `DescribeAnomaly` Dimensions valides :`Service`,`Class`,`Type`, `Resource`

Métrique	Description
	Statistiques valides : nombre d'échantillons, somme Unités : nombre

Les dimensions suivantes sont prises en charge pour les mesures d'utilisation de DevOps Guru.

Dimensions

Dimension	Description
`Service`	Il s'agit du nom du service AWS qui contient la ressource. Par exemple, pour DevOps Guru, cette valeur est`DevOps-Guru` .
`Class`	Il s'agit de la classe de la ressource qui est suivie. DevOpsGuru utilise cette dimension avec la valeur`None`.
`Type`	Il s'agit du type de ressource qui est suivi. DevOpsGuru utilise cette dimension avec la valeur`API`.
`Resource`	C'est le nom de l'opération DevOps Guru. Les valeurs valides sont les suivantes : `ListInsights` `ListAnomaliesForInsight` `ListRecommendations` ,`ListEvents` ,,`SearchInsights` ,`DescribeInsight` ,`DescribeAnomaly` .

Journalisation des appels d'API Amazon DevOps Guru avec AWS CloudTrail

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

vous ne configurez pas de suivi, vous pouvez toujours consulter les événements les plus récents sur la CloudTrail console dans l'historique des événements. À l'aide des informations collectées par CloudTrail, vous pouvez déterminer la demande qui a été faite à DevOps Guru, 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, consultez le Guide de AWS CloudTrail l'utilisateur.

DevOpsInformations sur les gourous dans CloudTrail

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

Pour un suivi permanent des événements de votre AWS compte, y compris des événements pour DevOps Guru, créez un historique. Un journal permet CloudTrail de transmettre des fichiers journaux à un compartiment Amazon S3. Par défaut, lorsque vous créez un journal d'activité dans la console, il s'applique à toutes les régions AWS. Le journal enregistre les événements de toutes les régions de la AWS partition et transmet les fichiers journaux au compartiment Amazon S3 que vous spécifiez. En outre, vous pouvez configurer d'autres AWS services pour analyser plus en profondeur les données d'événements collectées dans les CloudTrail journaux et y donner suite. Pour plus d'informations, consultez les ressources suivantes :

- Présentation de la création d'un journal de suivi
- 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

DevOpsGuru prend en charge la journalisation de toutes ses actions en tant qu'événements dans des fichiers CloudTrail journaux. Pour plus d'informations, consultez la section Actions dans la référence de l'API DevOps Guru.

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 .
- 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 faite par un autre AWS service.

Pour de plus amples informations, veuillez consulter l'élément userIdentity CloudTrail .

Comprendre les entrées du fichier journal DevOps Guru

Un journal 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 sont pas une pile ordonnée des appels d'API publics, ils n'apparaissent donc pas dans un ordre spécifique.

L'exemple suivant montre une entrée de CloudTrail journal qui illustre l'`UpdateResourceCollection`action.

```
{
  "eventVersion": "1.08",
  "userIdentity": {
    "type": "AssumedRole",
    "principalId": "AAAAAAAAAEXAMPLE:TestSession",
    "arn": "arn:aws:sts::123456789012:assumed-role/TestRole/TestSession",
    "accountId": "123456789012",
    "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
    "sessionContext": {
      "sessionIssuer": {
        "type": "Role",
        "principalId": "AIDACKCEVSQ6C2EXAMPLE",
        "arn": "arn:aws:iam::123456789012:role/TestRole",
        "accountId": "123456789012",
        "userName": "sample-user-name"
      },
      "webIdFederationData": {},
      "attributes": {
        "mfaAuthenticated": "false",
        "creationDate": "2020-12-03T15:29:51Z"
      }
    }
```

```
  },
  "eventTime": "2020-12-01T16:14:31Z",
  "eventSource": "devops-guru.amazonaws.com",
  "eventName": "UpdateResourceCollection",
  "awsRegion": "us-east-1",
  "sourceIPAddress": "sample-ip-address",
  "userAgent": "aws-internal/3 aws-sdk-java/1.11.901
 Linux/4.9.217-0.3.ac.206.84.332.metal1.x86_64 OpenJDK_64-Bit_Server_VM/25.275-b01
 java/1.8.0_275 vendor/Oracle_Corporation",
  "requestParameters": {
    "Action": "REMOVE",
    "ResourceCollection": {
      "CloudFormation": {
        "StackNames": [
          "*"
        ]
      }
    }
  },
  "responseElements": null,
  "requestID": " cb8c167e-EXAMPLE ",
  "eventID": " e3c6f4ce-EXAMPLE ",
  "readOnly": false,
  "eventType": "AwsApiCall",
  "managementEvent": true,
  "eventCategory": "Management",
  "recipientAccountId": "123456789012"
}
```


DevOpsPoints de terminaison VPC Guru et interface (AWS PrivateLink)

Vous pouvez utiliser des points de terminaison VPC lorsque vous appelez les API Amazon DevOps Guru. Lorsque vous utilisez des points de terminaison VPC, vos appels d'API sont plus sécurisés car ils sont contenus dans votre VPC et n'accèdent pas à Internet. Pour plus d'informations, consultez la section Actions dans la référence de l'API Amazon DevOps Guru.

Vous établissez une connexion privée entre votre VPC et DevOps Guru en créant un point de terminaison VPC d'interface. Les points de terminaison de l'interface sont alimentés par AWS PrivateLink une technologie qui vous permet d'accéder en privé aux API DevOps Guru sans passerelle Internet, périphérique NAT, connexion VPN ou connexion AWS Direct Connect. Les

instances de votre VPC n'ont pas besoin d'adresses IP publiques pour communiquer avec les API DevOps Guru. Le trafic entre votre VPC et DevOps Guru ne quitte pas le réseau Amazon.

Chaque point de terminaison d'interface est représenté par une ou plusieurs interfaces réseau Elastic dans vos sous-réseaux.

Pour plus d'informations, consultez Interface VPC endpoints (AWS PrivateLink) dans le guide de l'utilisateur Amazon VPC.

Considérations relatives aux points de DevOps terminaison Guru VPC

Avant de configurer un point de terminaison VPC d'interface pour DevOps Guru, assurez-vous de consulter les propriétés et les limites du point de terminaison d'interface dans le guide de l'utilisateur Amazon VPC.

DevOpsGuru prend en charge les appels vers toutes ses actions d'API depuis votre VPC.

Création d'un point de terminaison VPC d'interface pour Guru DevOps

Vous pouvez créer un point de terminaison VPC pour le service DevOps Guru à l'aide de la console Amazon VPC ou du AWS Command Line Interface ()AWS CLI. Pour plus d'informations, consultez Création d'un point de terminaison d'interface dans le Guide de l'utilisateur Amazon VPC.

Créez un point de terminaison VPC pour DevOps Guru en utilisant le nom de service suivant :

- com.amazonaws. *region*.devops-gourou

Si vous activez le DNS privé pour le terminal, vous pouvez envoyer des requêtes d'API à DevOps Guru en utilisant son nom DNS par défaut pour la région, par exemple`devops-guru.us-east-1.amazonaws.com`.

Pour plus d'informations, consultez Accès à un service via un point de terminaison d'interface dans le Guide de l'utilisateur Amazon VPC.

Création d'une politique de point de terminaison VPC pour Guru DevOps

Vous pouvez associer une politique de point de terminaison à votre point de terminaison VPC qui contrôle l'accès à DevOps Guru. La politique spécifie les informations suivantes :

- Le principal qui peut exécuter des actions.

- Les actions qui peuvent être effectuées.
- Les ressources sur lesquelles les actions peuvent être exécutées.

Pour plus d'informations, consultez Contrôle de l'accès aux services avec points de terminaison d'un VPC dans le Guide de l'utilisateur Amazon VPC.

Exemple : politique de point de terminaison VPC pour les actions DevOps Guru

Voici un exemple de politique de point de terminaison pour DevOps Guru. Lorsqu'elle est associée à un endpoint, cette politique donne accès aux actions DevOps Guru répertoriées pour tous les principaux sur toutes les ressources.

```
{
   "Statement":[
      {
         "Principal":"*",
         "Effect":"Allow",
         "Action":[
            "devops-guru:AddNotificationChannel",
            "devops-guru:ListInsights",
            "devops-guru:ListRecommendations"
         ],
         "Resource":"*"
      }
   ]
}
```

Sécurité des infrastructures à DevOps Guru

En tant que service géré, Amazon DevOps Guru est protégé par la sécurité du réseau AWS mondial. Pour plus d'informations sur les services AWS de sécurité et la manière de AWS protéger l'infrastructure, consultez AWS Cloud Security. Pour concevoir votre AWS environnement en utilisant les meilleures pratiques en matière de sécurité de l'infrastructure, consultez la section Protection de l'infrastructure dans Security Pillar AWS Well-Architected Framework.

Vous utilisez des appels d'API AWS publiés pour accéder à DevOps Guru via le réseau. Les clients doivent prendre en charge les éléments suivants :

- Protocole TLS (Transport Layer Security). Nous exigeons TLS 1.2 et recommandons TLS 1.3.

- Suites de chiffrement avec une confidentialité directe parfaite (PFS) telles que DHE (Ephemeral) ou ECDHE (Elliptic Curve Ephemeral Diffie-Hellman). Diffie-Hellman La plupart des systèmes modernes tels que Java 7 et les versions ultérieures prennent en charge ces modes.

La résilience dans Amazon DevOps Guru

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, qui sont connectées à un réseau à faible latence, haut débit et hautement redondant. DevOpsGuru opère dans plusieurs zones de disponibilité et stocke les données d'artefacts et les métadonnées dans Amazon S3 et Amazon DynamoDB. Vos données cryptées sont stockées de manière redondante sur plusieurs installations et sur plusieurs appareils au sein de chaque installation, ce qui les rend hautement disponibles et extrêmement durables.

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

Quotas et limites pour Amazon DevOps Guru

Le tableau suivant répertorie le quota actuel dans Amazon DevOps Guru. Ce quota s'applique à chaque AWS région prise en charge pour chaque AWS compte.

Notifications

Nombre maximum de sujets Amazon Simple Notification Service que vous pouvez spécifier simultanément	2

CloudFormation piles

Nombre maximum de AWS CloudFormation piles que vous pouvez spécifier	1 000

DevOpsLimites de surveillance des ressources Guru

Description de la ressource	Limite	Peut être augmenté
Limite par défaut pour la surveillance des files d'attente Amazon Simple Queue Service (Amazon SQS)	100*	Oui**

*Pour les nouveaux comptes DevOps Guru créés le 29 juin 2023 ou après cette date, et pour les comptes existants qui étaient actifs à la même date et comportant moins de 100 files d'attente Amazon SQS.

**Pour demander une modification de cette limite, contactez Support https://aws.amazon.com/contact-us. Vous pouvez demander une limite de surveillance des files d'attente Amazon SQS de 100, 500, 1 000, 5 000 ou 10 000.

DevOpsQuotas Guru pour la création, le déploiement et la gestion d'une API

Les quotas fixes suivants s'appliquent à la création, au déploiement et à la gestion d'une API dans DevOps Guru AWS CLI, à l'aide de la console API Gateway ou de l'API REST API Gateway et ses SDKs.

Pour obtenir la liste de tous les DevOps Guru APIs, consultez Amazon DevOps Guru Actions.

Quota par défaut	Peut être augmenté	
20 demandes toutes les 1 seconde par compte	Oui	

Historique du document Amazon DevOps Guru

Le tableau suivant décrit la documentation de cette version de DevOps Guru.

- Version de l'API : dernière en date
- Dernière mise à jour de la documentation : 9 août 2023

Modification	Description	Date
Mises à jour des politiques gérées	Les abonnements Amazon SNS et l'accès aux listes d'abonnements ont été ajoutés à la `AmazonDevOpsGuruConsoleFullAccess` politique. L'accès aux listes d'abonnement a également été ajouté à la `AmazonDevOpsGuruReadOnlyAccess` politique. Pour plus d'informations, consultez les politiques basées sur l'identité pour Amazon DevOps Guru.	9 août 2023
Clés de chiffrement gérées par le client	DevOpsGuru prend désormais en charge le chiffrement à l'aide de clés gérées par le client AWS KMS. Pour plus d'informations, consultez la section Protection des données dans DevOps Guru.	5 juillet 2023
DevOpsGuru for RDS prend en charge RDS PostgreSQL	DevOpsGuru for RDS peut détecter les problèmes de performance et d'autres informations dans les bases de données PostgreSQL.	30 mars 2023

	Pour plus d'informations, consultez la section Avantages de DevOps Guru pour RDS.	
DevOpsGuru for RDS soutient les informations proactives	DevOpsGuru for RDS publie des informations proactives contenant des recommandations pour vous aider à résoudre les problèmes liés à vos bases de données Aurora avant qu'ils ne s'aggravent. Pour plus d'informations, consultez la section Gestion des anomalies dans DevOps Guru for RDS.	28 février 2023
Page de ressources analysées	Une nouvelle page de la console DevOps Guru répertorie les ressources de votre compte qui sont analysées par DevOps Guru. Pour plus d'informations, consultez la section Affichage des ressources analysées par DevOps Guru.	20 octobre 2022
Nouveaux paramètres de configuration des notifications	Vous pouvez désormais choisir de recevoir toutes les notifications ou de ne recevoir que des notifications pour certaines sévérités et certains événements. Pour plus d'informations, consultez Mettre à jour les configurations de notification Amazon Amazon SNS.	30 septembre 2022

Ajout de l'analyse des anomalies du journal aux politiques gérées	AWS les politiques gérées pour DevOps Guru ont été mises à jour dans la console IAM afin de permettre l'accès à l' CloudWatch action. `FilterLogEvents` Pour plus d'informations, consultez les mises à jour DevOps apportées par Guru aux politiques AWS gérées et aux rôles liés aux services.	30 août 2022
Ajout de l'analyse des anomalies du journal	Vous pouvez consulter des informations détaillées sur les groupes de journaux liés à Insights dans la console DevOps Guru. Un rôle étendu lié à un service est également disponible pour décrire les CloudWatch journaux et les flux. Pour plus d'informations, consultez Comprendre les informations contenues dans la console DevOps Guru et les mises à jour de DevOps Guru concernant les politiques AWS gérées et les rôles liés aux services.	12 juillet 2022

CodeGuru Intégration du profileur	DevOpsGuru s'intègre désormais à Amazon CodeGuru Profiler grâce à une règle EventBridge gérée. Chaque événement entrant provenant de CodeGuru Profiler est un rapport d'anomalie proactif. Pour plus d'informations, consultez la section Intégration au CodeGuru profileur.	7 mars 2022
Mises à jour des rôles liés au service et des politiques gérées	Des politiques étendues sont disponibles dans la console IAM. Les modificat ions permettent à DevOps Guru de prendre en charge une intégration améliorée avec Amazon Relational Database Service (Amazon RDS). Pour plus d'informations, consultez Utilisation de rôles liés à un service et de politiques AWS gérées (prédéfinies) pour DevOps Guru.	21 décembre 2021
Ajout d'une nouvelle politique gérée	La `AmazonDevOpsGuruConsoleFullAccess` politique a été ajoutée. Pour plus d'informations, consultez les politiques basées sur l'identité pour Amazon DevOps Guru.	6 décembre 2021

Support pour définir votre application à l'aide de AWS balises	Vous pouvez désormais utiliser des AWS balises pour identifier les ressources que DevOps Guru doit analyser, identifier les ressources de vos applications et filtrer les informations dans la console. Pour plus d'informations, consultez la section Utiliser des balises pour identifier les ressources de vos applications.	1er décembre 2021
Mises à jour des rôles liés au service et des politiques gérées	Des politiques étendues sont disponibles dans la console IAM. Les modifications permettent à DevOps Guru de prendre en charge une intégration améliorée avec Amazon Relational Database Service (Amazon RDS). Pour plus d'informations, consultez Utilisation de rôles liés à un service et de politiques AWS gérées (prédéfinies) pour DevOps Guru.	1er décembre 2021

Assistance Amazon RDS	DevOpsGuru fournit désormais des analyses et des informations complètes sur les ressources Amazon Relationa l Database Service (Amazon RDS) de votre application. Pour plus d'informations, consultez Gérer les anomalies dans DevOps Guru pour Amazon RDS.	1er décembre 2021
EventBridge Intégration avec Amazon	DevOpsGuru s'intègre désormais EventBridge pour vous informer de certains événements liés à vos connaissances sur DevOps Guru. Pour plus d'informations, consultez la section Travailler avec EventBridge.	18 novembre 2021
AWS politique gérée ajoutée	Ajout d'une nouvelle politique AWS gérée. La `AmazonDev OpsGuruOrganizatio nsAccess` politique donne accès à DevOps Guru au sein d'une organisation. Pour plus d'informations, consultez la section Politiques basées sur l'identité.	16 novembre 2021

Mise à jour de la politique des rôles liés aux services	Politique étendue disponible dans la console IAM. Le changement permet à DevOps Guru de prendre en charge la vue multi-comptes. Pour plus d'informations, consultez la section Utilisation de rôles liés à un service.	4 novembre 2021
Support multi-comptes	Vous pouvez désormais consulter des informations et des statistiques sur plusieurs comptes de votre organisation. Pour plus d'informations, consultez Qu'est-ce qu'Amazon DevOps Guru ?	4 novembre 2021
Version de disponibilité générale	Amazon DevOps Guru est désormais disponible pour tous (GA).	4 mai 2021
Nouvelle rubrique	Vous pouvez désormais générer une estimation des coûts mensuels pour que DevOps Guru analyse vos ressources. Pour plus d'informations, consultez Estimez les coûts liés à votre Amazon DevOps Guru.	27 avril 2021

Support des points de terminaison VPC	Vous pouvez désormais utiliser les points de terminaison VPC pour améliorer la sécurité de votre analyse des ressources et de la génération d'informations. Pour plus d'informations, consultez DevOpsGuru et interface VPC endpoints ().AWS PrivateLink	15 avril 2021
Nouvelle rubrique	Un nouveau sujet expliquant comment surveiller DevOps Guru avec Amazon CloudWatch a été ajouté. Pour plus d'informations, consultez Monitoring DevOps Guru with Amazon CloudWatch.	11 décembre 2020
Version préliminaire	Il s'agit de la version préliminaire du guide de l'utilisateur Amazon DevOps Guru.	1er décembre 2020

AWS Glossaire

Pour la AWS terminologie la plus récente, consultez le AWS glossaire dans la Glossaire AWS référence.

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