aws

Guide de l’utilisateur

Amazon DevOps Guru

Amazon DevOps Guru: Guide de l’utilisateur

Table of Contents

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.

Pour commencer, voir Comment démarrer avec DevOps Guru ?

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.

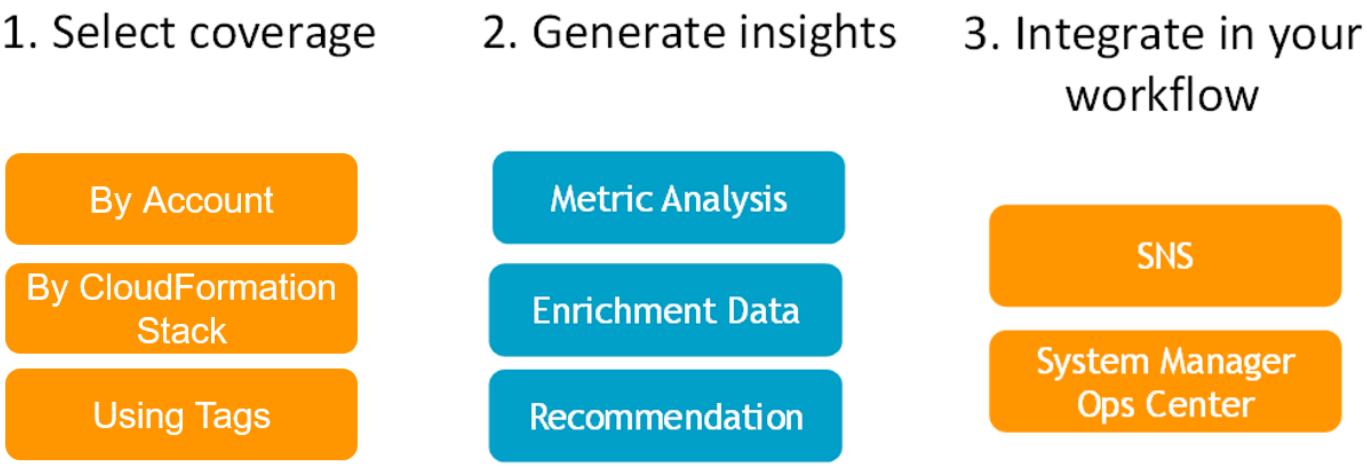
Rubriques

Flux de travail DevOps Guru de haut niveau

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.



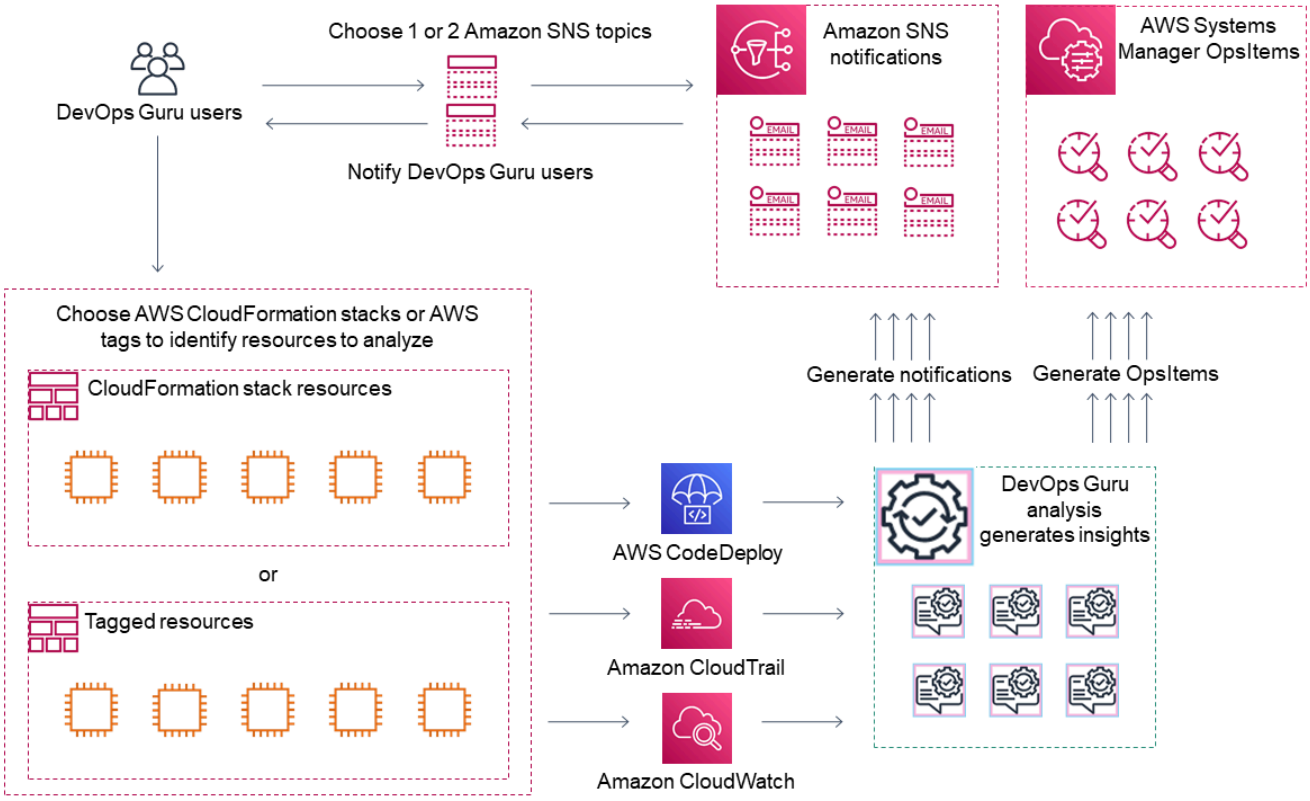
1. Dans un premier temps, vous choisissez votre couverture en spécifiant les AWS ressources de votre AWS compte qui sont analysées. DevOpsGuru peut couvrir ou analyser toutes les ressources d'un AWS compte, ou vous pouvez utiliser des AWS CloudFormation piles ou des AWS balises pour spécifier un sous-ensemble 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. DevOpsGuru 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 plus d'informations, consultez Mettre à jour vos notifications dans DevOpsGourou.
   - 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 plus d'informations, consultez Mise à jourAWS Systems Managerintégration dansDevOpsGourou.

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 en utilisantAWSressources 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 dans DevOpsConcepts 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 votreAWScouverture de l'analyse dans DevOpsGourou 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.

DevOpsConcepts du gourou

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

Rubriques

- Anomalie
- Informations
- Métriques et événements opérationnels
- Groupes de journaux et anomalies de 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 vosAWS ressources. Vous spécifiez lesAWS ressources que vous souhaitez analyser lorsque vous configurez Amazon DevOps Guru. Pour plus d'informations, veuillez consulter Configuration d'Amazon DevOps Guru.

Informations

Un aperçu est un ensemble d'anomalies créées lors de l'analyse desAWS 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 un comportement anormal au fur et à mesure qu'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.
- Proactif : un aperçu proactif vous permet d'être au courant des 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 indicateurs renvoyés par Amazon CloudWatch et les événements opérationnels émis par vosAWS ressources. Vous pouvez consulter les indicateurs et les événements opérationnels qui vous permettront de mieux comprendre les problèmes de votre application.

Groupes de journaux et anomalies de journal

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

Une anomalie de journal représente un groupe d'événements anormaux similaires détectés dans un groupe de journaux. Parmi les événements de journal anormaux qui peuvent être affichés dans DevOps Guru, citons les anomalies de mots clés, les anomalies de format, les anomalies de code HTTP, etc.

Vous pouvez utiliser les anomalies des journaux pour diagnostiquer la cause première d'un problème opérationnel. DevOpsGuru fait également référence aux lignes de journal dans ses recommandations d'informations 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 CloudWatch les journaux sont autorisés à consulter les CloudWatch journaux anormaux. Nous vous recommandons d'utiliser des politiques IAM pour autoriser ou refuser l'accès`ListAnomalousLogs` IAM. Pour de plus amples informations, veuillez consulter Identity and Access Management pour DevOps Guru.

Recommandations

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

- Une description des mesures recommandées pour corriger les anomalies qui constituent l'information.
- Une liste des indicateurs analysés dans lesquels DevOps Guru a découvert un comportement anormal. Chaque métrique inclut le nom de laAWS CloudFormation pile qui a généré la ressource associée aux métriques, le nom de la ressource et le nom duAWS service associé à la ressource.
- Liste des événements liés aux indicateurs anormaux associés à l'aperçu. Chaque événement associé contient le nom de laAWS CloudFormation pile qui a généré la ressource associée à l'événement, le nom de la ressource qui a généré l'événement et le nom duAWS 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 se sont produites et un lien permettant d'afficher 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 causées par diverses causes fondament ales telles que les	Déploiement du code : la Amazon API Gateway latence est affectée par une augmentation de la latence Lambda après un récent	Durée Throttles

Service Name	Cas d’utilisation	Exemples	Métriques
	démarrages à froid, l'augmentation des demandes, la limitation en aval ou les déploiements de code. Recommandez des moyens d'atténuer rapidement les effets.	déploiement de code Lambda. Régulation en aval : l'opérateur a réduit la capacité des unités de lecture pour DynamoDB, ce qui a entraîné une augmentation du nombre de tentatives. 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 recommandée : si vous utilisez le mode capacité provisionnée, utilisez le dimensionnement automatique pour gérer activement la capacité de débit des tables ou achetez de la capacité réservée à l'avance pour	ConsumedReadCapacityUnits

Service Name	Cas d'utilisation	Métriques
	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
- 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 avez déjà un AWS compte, que vous savez quel AWS compte ou quels comptes vous souhaitez analyser et que vous avez une rubrique Amazon Simple Notification Service à utiliser pour les notifications analytiques, vous pouvez passer 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 Quick Setup dans Systems Manager afin de configurer DevOps Guru pour une organisation, vous devez remplir les conditions préalables suivantes :

- 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 la configuration rapide dans le guide de AWS Systems Manager l'utilisateur.

Suivez les étapes ci-dessous pour configurer DevOps Guru sans Quick Setup.

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

Étape 1 — Inscrivez-vous à AWS

Inscrivez-vous pour un Compte AWS

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

Pour vous inscrire à un Compte AWS

1. Ouvrez https://portal.aws.amazon.com/billing/signup.

2. Suivez les instructions en ligne.

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

   Lorsque vous vous inscrivez à un Compte AWS, un Utilisateur racine d'un compte AWSest créé. Par défaut, seul l'utilisateur racine a accès à l'ensemble des Services AWS et des ressources de ce compte. Pour des raisons de sécurité, attribuez un accès administratif à un utilisateur et utilisez uniquement l'utilisateur root pour effectuer les tâches nécessitant un accès utilisateur root.

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

Création d'un utilisateur doté d'un accès administratif

Après vous être inscrit à un Compte AWS, sécurisez Utilisateur racine d'un compte AWS AWS IAM Identity Center, activez et créez un utilisateur administratif afin de ne pas utiliser l'utilisateur root pour les tâches quotidiennes.

Sécurisez votre Utilisateur racine d'un compte AWS

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

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

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

Création d'un utilisateur doté d'un accès administratif

1. Activez IAM Identity Center.

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

2. Dans IAM Identity Center, accordez un accès administratif à un utilisateur.

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

Connectez-vous en tant qu'utilisateur disposant d'un accès administratif

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

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

Attribuer l'accès à des utilisateurs supplémentaires

1. Dans IAM Identity Center, créez un ensemble d'autorisations conforme aux meilleures pratiques en matière d'application des autorisations du moindre privilège.

   Pour obtenir des instructions, voir Création d'un ensemble d'autorisations dans le guide de AWS IAM Identity Center l'utilisateur.

2. Affectez des utilisateurs à un groupe, puis attribuez un accès d'authentification unique au groupe.

   Pour obtenir des instructions, consultez la section Ajouter des groupes dans le guide de AWS IAM Identity Center l'utilisateur.

Étape 2 — Déterminer la couverture pour DevOps Guru

Votre couverture limite détermine les AWS ressources analysées par Amazon DevOps Guru pour détecter tout comportement anormal. Nous vous recommandons de regrouper vos ressources dans vos applications opérationnelles. Toutes les ressources comprises 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 composent chaque solution et regroupez-les à l'aide de AWS 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 de laisser votre AWS région et votre compte définir les limites de votre 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 des AWS CloudFormation piles pour définir les ressources de votre application opérationnelle. AWS 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 stacks à tout moment. Toutes les ressources des piles que vous choisissez définissent la couverture de vos limites. Pour plus d'informations, consultez A l'aide deAWS CloudFormationdes piles pour identifier les ressources de votre DevOpsApplications Guru.
- Utilisez des AWS balises pour spécifier AWS les ressources de vos applications. DevOpsGuru analyse uniquement les ressources qui contiennent les balises que vous avez choisies. Ces ressources constituent votre limite.

  Une AWS balise se compose d'une clé de balise et d'une valeur de balise. Vous pouvez spécifier une clé de balise et vous pouvez 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 toutes et regroupez les ressources dans vos applications à l'aide des valeurs des balises. Toutes les ressources associées aux balises que vous avez choisies constituent la limite de couverture de DevOps Guru. Pour plus d'informations, consultez Utilisation de 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 dansAffichageDevOpsInformations sur le gourou.

Pour plus d'informations, consultez Définition des applications en utilisantAWSressources. Pour plus d'informations sur les services et ressources pris en charge, consultez les tarifs 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 les événements importants du DevOps Guru, tels que la création d'un aperçu. Cela vous permet de connaître les problèmes découverts 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 un sujet de notification en utilisant son nom ou son Amazon Resource Name (ARN). Pour plus d'informations, consultez Enable DevOps Guru. Vous pouvez utiliser la console Amazon SNS pour consulter le nom et l'ARN de chacun de vos sujets. 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 AWS Identity and Access Management (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 comme 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.

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, l'exécution peut prendre de 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 AWS 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 De cette façon, DevOps Guru dispose 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 AWS 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 AWS 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'AWS CloudFormationutilisateur.
     3. (Facultatif) Si vous utilisez une AWS 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 AWScompte 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

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 AWS CloudFormation l'utilisateur, Étape 2 — Déterminer la couverture pour DevOps Guru et. etA l'aide deAWS CloudFormationdes piles pour identifier les ressources de votre DevOpsApplications 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.

Command	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 votreAWScouverture de l'analyse dans DevOpsGourou.

   DevOpsGuru peut analyser toute 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 plus d'informations, consultez 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 AWS CloudFormation piles de votre AWS compte qui créent les ressources que vous souhaitez analyser. Une AWS 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'AWS CloudFormation utilisateur, Déterminer la couverture pour DevOps Guru et. etA l'aide deAWS CloudFormationdes piles pour identifier les ressources de votre DevOpsApplications 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 plus d'informations, consultez A l'aide deAWS CloudFormationdes piles pour identifier les ressources de votre DevOpsApplications 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.

  La clé de la balise doit commencer par le préfixe`devops-guru-`. Ce préfixe ne distingue pas les majuscules et minuscules. Par exemple, une clé valide est`DevOps-Guru-Production-Applications`. Pour plus d'informations, consultez Utilisation de 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.

AWSServices habilitants pour l'analyse de 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 des informations détaillées sur le comportement et la manière d'y remédier. Pour plus d'informations sur les services et ressources pris en charge, consultez la tarification d'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 de DevOps Guru. Toutefois, certains AWS services nécessitent des actions supplémentaires pour générer les mesures requises. Pour certains services, l'activation de ces mesures 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 votreAWScouverture de l'analyse dans DevOpsGourou.

Services nécessitant une action pour l'analyse de DevOps Guru

- Amazon Elastic Container Service : pour générer des mesures supplémentaires qui améliorent la couverture de ses ressources par DevOps Guru, suivez les étapes décrites dans la section Configuration des informations sur les conteneurs sur Amazon ECS. Cela peut entraîner des CloudWatch frais Amazon.
- Amazon Elastic Kubernetes Service : pour générer des métriques à analyser par DevOps Guru, suivez les étapes décrites dans la section 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 la section Création d'une configuration de CloudWatch métriques pour tous les objets de votre bucket. DevOpsGuru n'analyse aucune ressource Amazon S3 tant que la génération de ces métriques n'est pas configurée. Cela peut entraîner CloudWatch des frais Amazon S3.

Pour plus d'informations, consultez les CloudWatchtarifs d'Amazon.

Utilisation d'informations dansDevOpsGuru

AmazonDevOpsGuru génère unaperçulorsqu'il détecte un comportement anormal dans vos applications opérationnelles. DevOpsGuru analyse les indicateurs, les événements et bien plus encore dansAWSressources que vous avez spécifiées lors de la configurationDevOpsGourou. Chaque aperçu contient une ou plusieurs recommandations que vous pouvez suivre pour atténuer le problème. Il contient également une liste des mesures, une liste des groupes de journaux et une liste des événements qui ont été utilisés pour identifier le comportement inhabituel.

Il existe deux types d'informations.

- RéactifInsights contient des recommandations que vous pouvez suivre pour résoudre les problèmes qui se posent actuellement.
- Proactifles analyses contiennent des recommandations qui abordent des problèmes quiDevOpsGuru prédit que cela se produira dans le futur.

Rubriques

AffichageDevOpsInformations sur le gourou

Vous pouvez consulter vos informations à l'aide duAWS Management Console.

Afficher votreDevOpsInformations sur le gourou

1. Ouvrez l'AmazonDevOpsConsole Guru àhttps://console.aws.amazon.com/devops-guru/.
2. Ouvrez le volet de navigation, puis choisissezPerspectives.
3. Sur leRéactifonglet, vous pouvez voir une liste d'informations réactives. Sur leProactifonglet, 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 leRéactifouProactifonglet, en fonction du type d'aperçu que vous recherchez.
- ChoisissezFiltrer les informations, puis choisissez une option pour spécifier un filtre. Vous pouvez ajouter une combinaison de filtres d'état, de gravité, de ressources et de balises. Utilisez unAWSfiltre de balises pour afficher les informations générées uniquement par les ressources avec des balises spécifiques. Pour en savoir plus, consultez Utilisation de 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
> - Streams Amazon DynamoDB
> - Instances de groupe Amazon EC2 Auto Scaling
> - Environnements AWS Elastic Beanstalk
> - Nœuds Amazon Redshift

- Choisissez ou spécifiez une plage de temps à filtrer en fonction de l'heure de création des informations.
  - 12haffiche les informations créées au cours des 12 dernières heures.
  - 1daffiche les informations créées au cours de la dernière journée.
  - 1 waffiche les informations créées la semaine dernière.
  - 1 maffiche les informations créées le mois dernier.
  - Personnalisévous permet de spécifier un autre intervalle de temps. 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 dansDevOpsConsole Guru

Utilisez AmazonDevOpsConsole Guru qui permet d'afficher des informations utiles dans vos analyses afin de vous aider à diagnostiquer et à corriger les comportements anormaux. QuandDevOpsGuru

analyse vos ressources et trouve des sites Amazon connexesCloudWatchmétriques,AWS CloudTrailles événements et les données opérationnelles indiquant un comportement inhabituel, il crée un aperçu contenant des recommandations pour résoudre le problème et des informations sur les indicateurs et les événements associés. Utilisez des données d'analyse avecMeilleures pratiques en DevOps Gurupour résoudre les problèmes opérationnels détectés parDevOpsGourou.

Pour obtenir un aperçu, suivez les étapes décrites dansAffichage des informationspour en trouver un, puis choisissez son nom. La page d'aperçu contient les informations suivantes.

Présentation d'Insight

Utilisez cette section pour obtenir une vue d'ensemble de haut niveau des informations. Vous pouvez voir l'état de l'aperçu (En coursouFermé), combienAWS CloudFormationles piles sont affectées, à la date à laquelle l'aperçu a commencé, s'est terminé et a été mis à jour pour la dernière fois, ainsi que l'élément d'opérations associé s'il en existe un.

Si un aperçu est regroupé dansniveau de la pile, puis vous pouvez choisir le nombre de piles concernées pour voir leurs noms. Le comportement anormal à l'origine de l'aperçu s'est produit dans les ressources créées par les piles concernées. Si un aperçu est regroupé dansniveau du compte, alors le nombre est égal à zéro ou n'apparaît pas.

Pour plus d'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 dansniveau de la pileou leniveau du compte.

- Niveau de pileLes noms des insights incluent le nom de la pile qui contient la ressource avec son comportement anormal.
- Niveau du compteles noms des aperçus n'incluent pas de nom de pile.

Pour plus d'informations, veuillez consulter Comprendre comment les comportements anormaux sont regroupés en informations.

Métriques agrégées

Choisissez leMétriques agrégéesonglet pour afficher les mesures liées à l'aperçu.
Dans le tableau, chaque ligne représente une métrique. Vous pouvez voir lequelAWS CloudFormationstack a créé la ressource qui a émis la métrique, le nom de la ressource et son type. Toutes les métriques ne sont pas associées àAWS CloudFormationempilez ou attribuez un nom.

Lorsque plusieurs ressources présentent des anomalies en même temps, la vue chronologique regroupe les ressources et présente leurs mesures anormales 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 un intervalle de temps spécifique. Vous pouvez également utiliser les icônes de loupe pour zoomer et dézoomer.

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

- ChoisissezAfficher dansCloudWatchpour voir à quoi ressemble la métrique dansCloudWatchconsole. Pour plus d'informations, voirStatistiquesetDimensionsdans leAmazonCloudWatchGuide de l'utilisateur.
- Passez la souris sur le graphique pour afficher des détails sur les données métriques anormales et la date à laquelle elles se sont produites.
- Cochez la case avec la flèche vers le bas pour télécharger une image PNG du graphique.

Anomalies représentées graphiquement

Choisissez leAnomalies représentées graphiquementonglet 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 période spécifique dans la chronologie pour zoomer. Vous pouvez également utiliser les icônes de loupe pour zoomer et dézoomer, ou choisir une durée prédéfinie en heures, jours ou semaines (1H,3H,12H,1D,3D,1 W, ou2 W).

ChoisissezAfficher toutes les statistiques et dimensionspour voir les détails de l'anomalie. Dans la fenêtre qui s'ouvre, vous pouvez :

- ChoisissezAfficher dansCloudWatchpour voir à quoi ressemble la métrique dansCloudWatchconsole.
- Passez la souris sur le graphique pour afficher des détails sur les données métriques anormales et la date à laquelle elles se sont produites.
- ChoisissezStatistiquesouDimensionpour personnaliser l'affichage du graphique. Pour plus d'informations, voirStatistiquesetDimensionsdans leAmazonCloudWatchGuide de l'utilisateur.

Groupes de journaux

Lorsque vous activez la détection des anomalies dans les journaux,DevOpsGuru tague votreCloudWatchgroupes de journaux afin que vous puissiez consulter les groupes de journaux liés à vos informations. Dans leGroupes de journauxsection 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 journaux a connu des anomalies de journalisation.

Choisissez une ligne violette dans la chronologie pour afficher un exemple d'informations sur les anomalies enregistrées, telles que les exceptions relatives aux mots clés et les écarts numériques. ChoisissezAfficher les détails du groupe de journauxpour consulter 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 des détails sur les données de journal anormales et la date à laquelle elles se sont produites.
- Affichez les anomalies du journal en détail à l'aide d'exemples de messages, de la fréquence des occurrences, des recommandations associées et de l'heure de survenue.
- Cliquez surAfficher les détails dansCloudWatchpour afficher les lignes du journal correspondant à une anomalie du journal.

Évènements connexes

DansÉvènements connexes, afficherAWS CloudTrailles événements qui sont liés à vos connaissances. Utilisez ces événements pour comprendre, diagnostiquer et traiter la cause sous-jacente du comportement anormal.

Recommandations

DansRecommandations, vous pouvez consulter des suggestions susceptibles de vous aider à résoudre le problème sous-jacent. QuandDevOpsGuru détecte les comportements anormaux et 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 dansniveau de la pileou leniveau du compte. Si un aperçu est généré pour une ressource qui se trouve dans unAWS CloudFormationpile, alors c'est unniveau de la pileaperçu. Dans le cas contraire, il s'agit d'unniveau du compteaperçu.

La façon dont une pile est regroupée peut dépendre de la manière dont vous avez configuré la couverture de votre analyse des ressources dans AmazonDevOpsGourou.

Si votre couverture est définie parAWS CloudFormationpiles

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

Si votre couverture est votre couverture actuelleAWScompte et 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.

- Un aperçu généré à partir d'une ressource ne faisant pas partie d'une pile est regroupé dansniveau du compte.
- Un aperçu généré à partir d'une ressource figurant dans l'une des 10 000 premières piles analysées est regroupé dansniveau de la pile.
- Un aperçu généré à partir d'une ressource ne figurant pas dans l'une des 10 000 premières piles analysées est regroupé dansniveau du compte. Par exemple, un aperçu généré pour une ressource de la 10 001e pile analysée est regroupé dansniveau du compte.

Pour plus d'informations, veuillez consulter Déterminer la couverture pour DevOps Guru.

Comprendre la gravité des informations

Un aperçu peut avoir l'une des trois degrés de gravité suivants :haute,moyen, oubas. Un aperçu est créé par AmazonDevOpsGuru détecte ensuite les anomalies associées et attribue à chaque anomalie une gravité. DevOpsGuru attribue à une anomalie une gravité dehaute,moyen, oubasen utilisant les 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 estbas, alors la gravité de l'aperçu estbas.
- Si la gravité la plus élevée de toutes les anomalies qui ont généré l'aperçu estmoyen, alors la gravité de l'aperçu estmoyen. La gravité de certaines des anomalies qui ont généré les informations peut êtrebas.
- Si la gravité la plus élevée de toutes les anomalies qui ont généré l'aperçu esthaute, alors la gravité de l'aperçu esthaute. La gravité de certaines des anomalies qui ont généré les informations peut êtrebasoumoyen.

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

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, DBLoadCPU
RDS for 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
- SQL défaillant ServerAgentJobsCount
- 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
- WLM QueueLength
- WLM QueueWaitTime
- WLM QueryDuration
- 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

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, voir DevOpsConcepts du gourou.

Rubriques

- Moteurs de base de données compatibles

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. DevOpsGuru 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. DevOpsGuru 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. DevOpsGuru 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 régulièrement un seuil spécifié sur une période donnée. 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 performances de base 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 les identifiants SQL *`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 effectuent des opérations de mémoire excessives, telles que le tri en mémoire ou les jointures volumineuses.
- Étudiez l'utilisation intensive des E/S pour les ID SQL suivants : *`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. DevOpsGuru 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 compatibles

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.

Paramètres

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 gérée par AWS `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 compteCompte AWS, y compris Région AWS les bases de données Amazon RDS.
- Spécifiez AWS CloudFormation les piles pour DevOps Guru for RDS.

  Pour plus d'informations, consultez A l'aide deAWS CloudFormationdes piles pour identifier les ressources de votre DevOpsApplications 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 plus d'informations, consultez Utilisation de 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 Activer 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 "Utilisation de 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 plus d'informations, consultez 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 plus d'informations, consultez 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

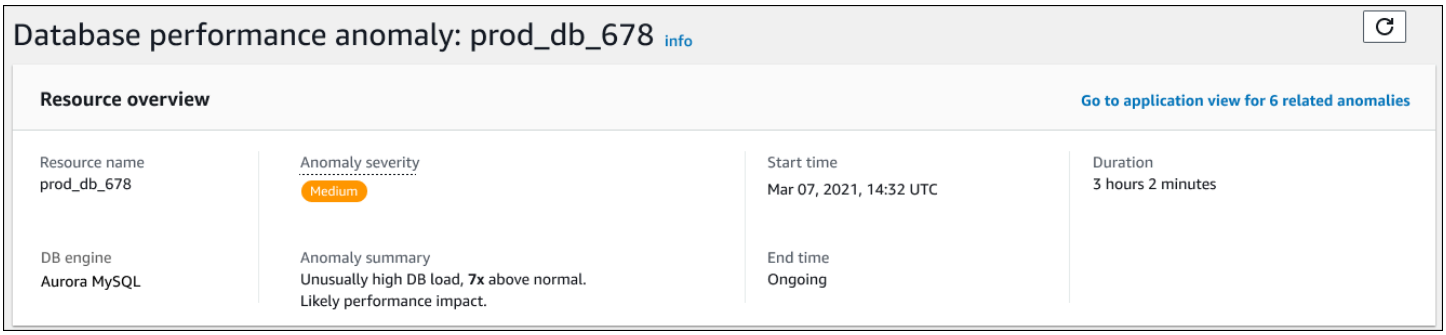
1. Sur la page d'aperçu, recherchez une métrique agrégée avec le type de ressource AWS/RDS.
2. Sélectionnez Afficher les détails.

   La page de détails de l'anomalie apparaît. Le titre commence par « Anomalie des performances de la base de données » et nomme la ressource « Afficher ». 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.

Vue d'ensemble 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.



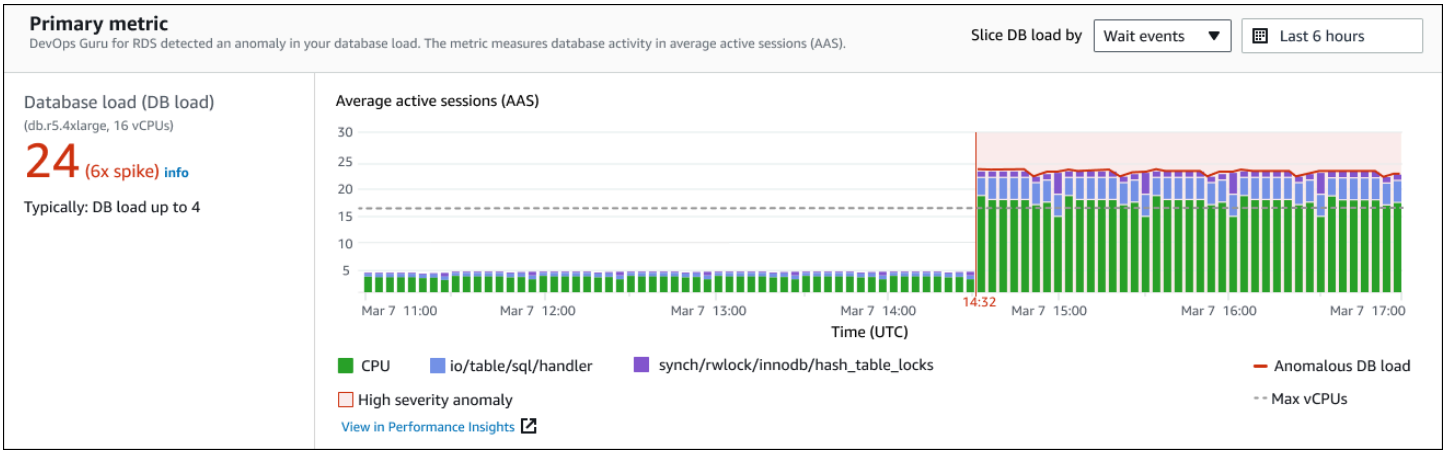
Cette section contient les champs suivants :

- 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 niveaux de sévérité possibles sont élevés, moyens 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 vCPU, 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.

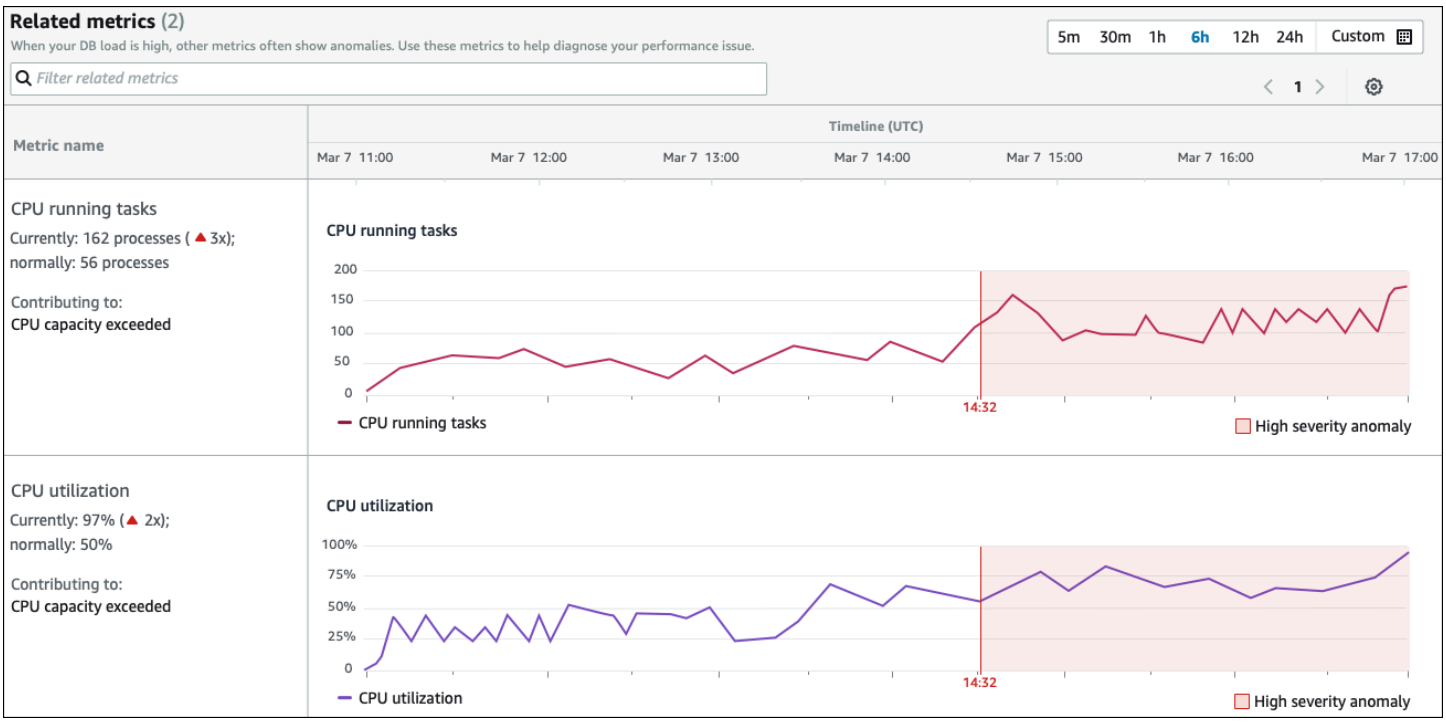
Par défaut, le graphique de charge est découpé en fonction des événements d'attente. Cela signifie que pour chaque barre du graphique, la plus grande zone colorée représente l'événement d'attente qui contribue le plus à la charge totale de la base de données. Le graphique indique l'heure (en rouge) à 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 :

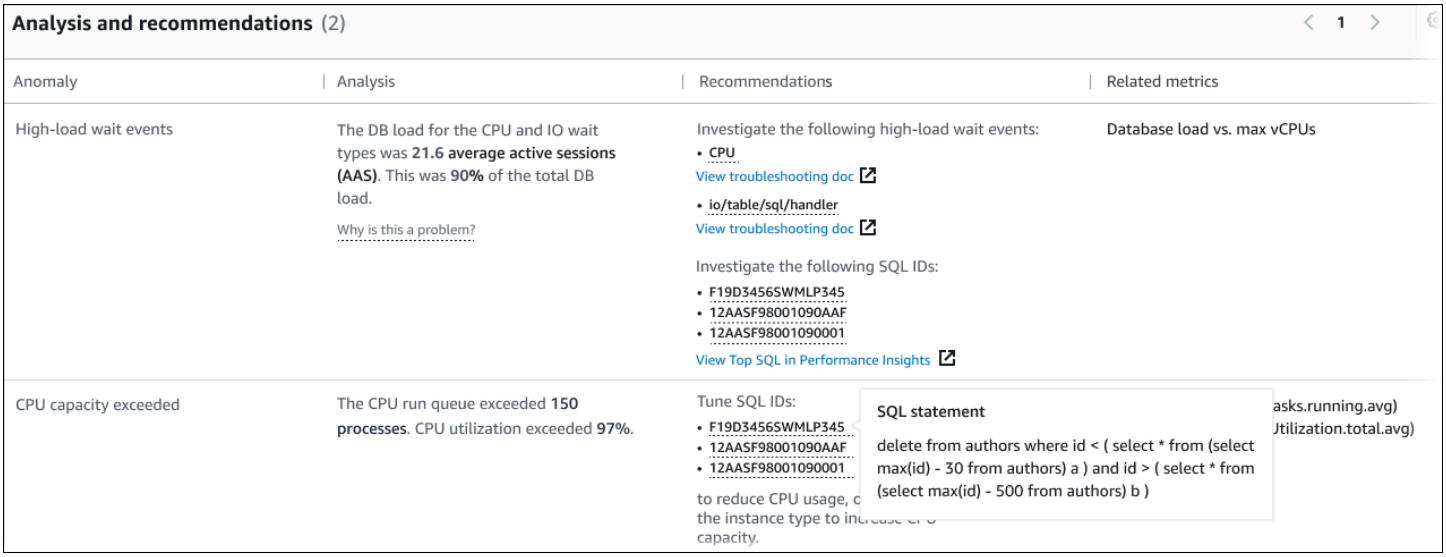
- ***Nom*** : nom de la métrique. La première ligne identifie la métrique en tant que tâches exécutées par le processeur.
- Actuellement : valeur actuelle de la métrique. Dans la première ligne, la valeur actuelle est 162 processus (3x).
- Normalement : référence de cette métrique pour cette base de 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 cpu et io/table/sql/handler dans le 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 AWS CloudFormation l'agrégation. Les anomalies peuvent impliquer plusieurs ressources qui sont toutes affectées par la même solution. DevOpsGuru 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	Utilisation du processeur, utilisation du processeur du moteur, 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 présente la façon dont Amazon DevOps Guru s'intègre à Amazon. CodeGuru Profiler. Vous pouvez consulter les recommandations à partir de CodeGuru Profiler comme informations dans la console DevOps Guru.

Amazon DevOps Guru s'intègre à Amazon CodeGuru Profiler avec un EventBridge règle 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 de CodeGuru Profiler est un rapport d'anomalie proactif. Pour de plus amples informations, veuillez consulterUtilisation d'EventBridge avec CodeGuru Profiler.

DevOps Guru 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 portent CodeGuru Informations de recommandation de profiler ainsi que des métadonnées pour vos ressources de calcul. Pour plus d'informations sur le cycle de vie d'un événement, voirAmazon EventBridge Events (Événements).

Lorsque vous configurez DevOps Guru, DevOps Guru crée le EventBridge Règle gérée de votre compte qui achemine les événements depuis un autre service. Cette règle est acheminée vers DevOps Guru. Les notifications sont envoyées en cas d'événement entrant.

Un bus d'événements reçoit des événements provenant d'une source telle que DevOps Guru et les achemine vers les règles associées à ce bus d'événements. Pour de plus amples informations sur les bus d'événements, veuillez consulterBus d'événements.

Pour de plus amples informations sur certains des paramètres, veuillez consulterÉvénements Amazon EventBridge.

À recevoir CodeGuru Les informations relatives aux profileurs dans DevOps Guru, vous devez avoir ce qui suit.

- CodeGuru Profiler doit être activé. Pour plus d'informations sur l'activation CodeGuru Profiler, voirConfiguration d' CodeGuru Profiler.
- DevOps Guru doit être activé. Pour plus d'informations sur l'activation de DevOps Guru, voirActiver DevOps Guru.
- Les mêmes ressources doivent être surveillées dans la même région dans les deux CodeGuru Profiler et DevOps Guru.

Définition des applications en utilisantAWSressources

Amazon DevOpsGuru regroupe les ressources qui se trouvent dans la limite de couverture qui spécifie les ressources qu'il analyse pour obtenir des informations opérationnelles. Les ressources sont regroupées par ressources dansAWS CloudFormationpiles ou par ressources à l'aide de balises. Vous choisissez les piles ou les tags lors de la configuration DevOpsGuru. 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, vous pouvez disposer de toutes les ressources que vous utilisez pour une application de surveillance 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 ressourcesDevOpsAnalyses 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 de plus amples informations sur les services et ressources pris en charge, veuillez consulterAmazon DevOpsTarification Guru.

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

- Spécifiez que tous les supportsAWSressources de votreAWScompte et région. Cela fait de votre compte et de votre région votre limite de ressources. Avec cette option, DevOpsGuru analyse toutes les ressources prises en charge sur votre compte et votre région. Toutes les ressources d'une pile sont regroupées dans une application. Toutes les ressources qui ne se trouvent pas dans une pile sont regroupées dans leur propre application.
- UtiliserAWS CloudFormationdes piles pour spécifier les ressources de vos applications. Une pile contient des ressources générées à l'aide deAWS CloudFormation. Dans DevOpsGuru, tu peux choisir des piles sur ton compte. Les ressources que vous trouvez dans chaque stack que vous choisissez sont regroupées dans une application. Toutes les ressources des piles sont analysées par DevOpsLe gourou des informations.
- UtiliserAWSdes balises pour spécifier les ressources de vos applications. UnAWSla balise contient uncléet unvaleur. Dans DevOpsGuru, choisissez un tagcléet choisissez éventuellement une ou plusieursvaleursqui sont associés à çaclé. Vous pouvez utiliser le pluginvaleurspour regrouper vos ressources dans des applications.

Pour plus d'informations, consultez Mettre à jour votreAWScouverture de l'analyse dans DevOpsGourou.

Rubriques

Utilisation de 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 les ressources à regrouper 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 tag spécifique qui commence par « devops-guru ». 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 des valeurs de balise afin de spécifier les ressources que DevOps Guru doit analyser, sélectionnez Choisir des valeurs de balise spécifiques.

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

Vous utilisez la clé d'une balise pour identifier les ressources, puis vous utilisez des valeurs associées à cette clé pour regrouper les ressources dans vos applications. Par exemple, vous pouvez étiqueter 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 du tag `devops-guru-applications/database`devops-guru-applications/cicd, et `devops-guru-applications/monitoring` pour identifier trois applications dans votre compte. Chaque application est composée de ressources connexes 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 plus d'informations, consultez Ajouter des AWS balises aux AWS ressources.

Après avoir ajouté une balise aux ressources de votre application, vous pouvez filtrer vos informations en fonction des balises associées aux ressources qui les ont générées.

Pour plus d'informations sur la façon de filtrer vos informations à l'aide d'une balise, consultezAffichageDevOpsInformations sur le gourou.

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

Rubriques

- Qu'est-ce qu'un AWS tag ?
- Définition d'une application DevOps Guru à l'aide d'une balise
- Utiliser des tags avec DevOps Guru
- Ajouter des AWS balises aux AWS ressources

Qu'est-ce qu'un AWS tag ?

Les balises vous aident à identifier et organiser vos ressources AWS. De nombreux services AWS prennent en charge le balisage. Vous pouvez donc attribuer la même balise à des ressources à partir 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 fonction AWS Lambda. Pour de plus amples informations sur l'utilisation de balises, veuillez consulter le livre blanc sur les bonnes pratiques de balisage.

Chaque balise AWS se compose de 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, ajoutez cette balise aux AWS ressources de votre compte qui constituent votre application. Votre balise contient une clé et une valeur. Nous vous recommandons d'ajouter une balise 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 `containers`, `database`, et `monitoring` pour trois applications. Pour plus d'informations, consultez Mettre à jour votreAWScouverture de l'analyse dans DevOpsGourou.

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

> **Important**
>
> La chaîne employée pour une clé dans une balise que vous utilisez pour définir votre couverture de ressources doit commencer par le préfixe `Devops-guru-`. La clé de balise peut être `DevOps-Guru-deployment-application` ou `devops-guru-rds-application`. 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 les valeurs des 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 les paramètres.

3. Dans Ressources analysées, choisissez Modifier.
4. 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 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 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.

   La clé de la balise doit commencer par le préfixe`devops-guru-`. Ce préfixe ne distingue pas les majuscules et minuscules. Par exemple, une clé valide est`DevOps-Guru-Production-Applications`.
5. Choisissez Enregistrer.

Ajouter des AWS balises aux AWS ressources

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 que DevOps Guru peut analyser sont des balises de support. Pour plus d'informations, consultez les sections Marquage de vos flux dans le manuel Amazon Kinesis Developer Guide et Marquage d'une distribution dans le manuel Amazon CloudFront Developer Guide. 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 dans votre région et par ressources dans des 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 uniquement ajouter la clé ou la clé et une valeur. Par exemple, vous pouvez créer une balise contenant la clé `devops-guru-` de 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.

A l'aide deAWS CloudFormationdes piles pour identifier les ressources de votre DevOpsApplications Guru

Vous pouvez utiliserAWS CloudFormationpiles pour spécifier lesquellesAWSles ressources que vous souhaitez DevOpsUn gourou à analyser. Une pile est une collection deAWSdes ressources qui sont gérées comme une seule unité. Les ressources des piles que vous choisissez constituent votre DevOpsLimite de couverture Guru. Pour chaque stack 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 aperçu 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, veuillez consulter la rubriqueUtilisation des pilesdans leAWS CloudFormationGuide de l'utilisateuretMettre à jour votreAWScouverture de l'analyse dans DevOpsGourou.

Après avoir choisi une pile, DevOpsGuru commence immédiatement à analyser toute ressource que vous y ajoutez. Si vous supprimez une ressource d'une pile, elle n'est plus analysée.

Si vous choisissez d'avoir DevOpsGuru analyse toutes les ressources prises en charge sur votre compte (cela signifie que votreAWScompte et région sont votre DevOpsGuru (limite de couverture), puis DevOpsGuru analyse et crée des informations pour chaque ressource prise en charge sur votre compte, y compris celles qui se trouvent dans des piles. Un aperçu créé à partir d'anomalies dans une ressource qui ne se trouve pas dans une pile est regroupé dansniveau du compte. Si un aperçu est créé à partir d'anomalies dans une ressource qui se trouve dans une pile, il est regroupé dansLevel de pile. Pour plus d'informations, consultez Comprendre comment les comportements anormaux sont regroupés en informations.

Choisir des piles pour DevOpsAmazon Guru

Spécifiez les ressources qui vous intéresse Amazon DevOpsGuru à analyser en choisissantAWS CloudFormationdes piles qui les créent. Pour ce faire, vous pouvez utiliser le pluginAWS Management Consoleou le kit SDK.

Rubriques

- Choisir des piles pour DevOpsGuru à analyser (console)
- Choisir des piles pour DevOpsGuru à analyser (DevOpsGuru

Choisir des piles pour DevOpsGuru à analyser (console)

Vous pouvez ajouterAWS CloudFormationse pile via la console.

Pour choisir les piles qui contiennent les ressources à analyser

1. Ouvrez Amazon DevOpsGuruhttps://console.aws.amazon.com/devops-guru/.
2. Ouvrez le volet de navigation, puis choisissezParamètres.
3. DansDevOpsCouverture Guru, choisissezGérer.
4. ChoisissezCloudFormation pilessi tu veux DevOpsGuru pour analyser les ressources qui se trouvent dans les piles de votre choix, puis choisissez l'une des options suivantes.

   - Toutes les ressources— Toutes les ressources empilées sur votre compte sont analysées. Les ressources de chaque pile sont regroupées dans leur propre application. Toutes les ressources de votre compte qui ne figurent pas dans une pile ne sont pas analysées.
   - Sélectionnez des piles— Sélectionnez les piles qui vous intéresse DevOpsUn gourou à analyser. Les ressources de chaque stack que vous sélectionnez sont regroupées dans

leur propre application. Vous pouvez saisir le nom d'une pile dansRecherchez des pilespour localiser rapidement une pile spécifique. Vous pouvez sélectionner jusqu'à 1 000 piles.

5. Choisissez Save (Enregistrer).

Choisir des piles pour DevOpsGuru à analyser (DevOpsGuru

SpécifiezAWS CloudFormationpiles utilisant Amazon DevOpsGuru SDK, utilisez le`UpdateResourceCollection`Méthode. Pour plus d'informations, veuillez consulter la rubriqueUpdateResourceCollectiondans leAmazon DevOpsRéférence Guru.

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.

DevOpsGuruÉvénement New Insight Open

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"
         ]
  }
}
```

Mise à jour DevOpsRéglages Guru

Vous pouvez mettre à jour le Amazon suivant DevOpsParamètres du gourou :

- Votre DevOpsCouverture 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 d'informations importantes DevOpsÉvénements Guru.
- Des fonctionnalités pour des informations améliorées. Cela inclut la détection des anomalies du journal, le chiffrement et votreAWS Systems Managerparamètres d'intégration. Cela détermine si DevOpsGuru affiche les données du journal, indique si vous utilisez des clés de sécurité supplémentaires et si un OpsItem est créé dans Systems Manager OpsCenter pour chaque nouvel aperçu.

Rubriques

Mettre à jour les paramètres de votre compte de gestion

Vous pouvez configurer DevOpsLe gourou des comptes au sein de votre organisation. Si vous n'avez pas enregistré d'administrateur délégué, vous pouvez le faire en choisissantEnregistrer un administrateur délégué. Pour plus d'informations sur l'enregistrement d'un administrateur délégué, voirActiverDevOpsGourou.

Mettre à jour votreAWScouverture de l'analyse dans DevOpsGourou

Vous pouvez mettre à jour lequelAWSressources de votre compte DevOpsGuru analyse. Pour ce faire, accédez auRessources analyséespage dans la console, puis choisissezModifier. Pour plus d'informations, veuillez consulter Affichage des ressources analysées.

Mettre à jour vos notifications dans DevOpsGourou

Configurez les rubriques Amazon Simple Notification Service qui sont utilisées pour vous informer des informations importantes concernant Amazon DevOpsÉvénements Guru. Vous pouvez choisir parmi une liste de noms de sujets qui existent déjà dans votreAWScompte, entrez le nom d'un nouveau sujet qui DevOpsGuru crée dans votre compte ou saisissez le nom de ressource Amazon (ARN) d'un sujet existant dans n'importe quelAWScompte dans votre région. Si vous spécifiez l'ARN d'un sujet qui ne figure pas dans votre compte, vous devez autoriserDevOpsGuru pour accéder à ce sujet en y ajoutant une politique IAM. Pour plus d'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 améliorée à partir de`Low`ou`Medium`pour`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 unAWS CloudFormationla clé de pile ou de balise n'est pas valide lorsque vous essayez d'ajouter des ressources à votre DevOpsCompte 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 DevOpsConsole 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 Amazon DevOpsConsole Guru àhttps://console.aws.amazon.com/devops-guru/.
2. Choisissez Settings (Paramètres) dans le volet de navigation.

   La page Paramètres inclutNotificationssection, avec des informations sur les rubriques Amazon SNS configurées.

Ajout de sujets de notification Amazon SNS dans DevOpsConsole Guru

Pour ajouter une rubrique de notification Amazon SNS dans DevOpsConsole Guru

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

   - ChoisissezGénérer une nouvelle rubrique SNS par e-mail. Puis, à partir deSpécifiez l'adresse e-mail, entrez l'adresse e-mail à laquelle vous souhaitez recevoir des notifications. Pour saisir des adresses e-mail supplémentaires, sélectionnezAjouter un nouvel e-mail.
   - ChoisissezUtiliser une rubrique SNS existante. Puis, à partir deChoisissez un sujet dans votreAWScompte, choisissez le sujet que vous souhaitez utiliser.
   - ChoisissezUtiliser l'ARN d'une rubrique SNS existante pour spécifier une rubrique existante provenant d'un autre compte. Puis, dansEntrez un ARN pour un sujet, entrez le sujet ARN. 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 plus d'informations, veuillez consulter Autorisations pour les rubriques Amazon SNS.

4. Choisissez Enregistrer.

Suppression des rubriques de notification Amazon SNS dans DevOpsConsole Guru

Pour supprimer des rubriques Amazon SNS dans DevOpsConsole Guru

1. the section called "Accédez aux paramètres de notification dans DevOpsConsole Guru".
2. ChoisissezSélectionnez un sujet existant.
3. Dans le menu déroulant, sélectionnez le sujet que vous souhaitez supprimer.
4. Choisissez Remove (Supprimer).
5. Choisissez Save (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 DevOpsGourou. Vous pouvez choisir de recevoir des notifications de tous les niveaux de gravité ou uniquement des notifications avecÉlevéetMoyenniveaux de gravité. 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, 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 améliorée à partir de`Low`ou`Medium`pour`High`.
- Le statut d'un aperçu passe de « en cours » à « résolu ».
- Une recommandation pour un aperçu est identifiée.

Par défaut, vous ne recevez queÉlevéetMoyennotifications de niveau de gravité, 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 DevOpsConsole Guru".
2. ChoisissezSélectionnez un sujet existant.
3. Dans le menu déroulant, sélectionnez le sujet que vous souhaitez modifier.
4. ChoisissezTous les niveaux de gravitépour recevoir des notifications présentant des niveaux de gravité élevés, moyens et faibles, ou choisissezHaut et moyen uniquementpour recevoir des notifications présentant des niveaux de gravité élevés et moyens.
5. ChoisissezAvertissez-moi de toutes les mises à jour de l'aperçu, ou choisissezM'avertir lorsqu'un aperçu est ouvert ou fermé, ou lorsque le niveau de gravité passe de faible ou moyen à élevé.
6. Choisissez Save (Enregistrer).

Autorisations ajoutées à votre rubrique Amazon SNS

Une rubrique Amazon SNS est une ressource qui contient unAWS Identity and Access Managementpolitique de ressources (IAM). Lorsque vous spécifiez un sujet ici, DevOpsGuru 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 DevOpsGuru pour 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, DevOpsGuru ne peut pas utiliser le sujet pour générer des notifications.

Filtrer votre DevOpsNotifications du guru

Vous pouvez filtrer votre DevOpsNotifications du gourou parthe 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 avec une politique de filtrage des abonnements Amazon SNS
- Exemple de notification Amazon SNS filtrée pour Amazon DevOpsGourou

Filtrer les notifications avec 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 DevOpsGourou.

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 des abonnements Amazon SNS, consultezPolitiques de filtrage des abonnements Amazon SNSdans leGuide du développeur

d'Amazon Simple Notification Service. Dans votre politique de filtrage, vous spécifiez l'un des mots clés avec la politique`MessageType`. Par exemple, ce qui suit apparaîtrait 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 DevOpsGourou

Voici un exemple de notification Amazon Simple Notification Service (Amazon SNS) provenant d'une rubrique Amazon SNS avec une politique de filtrage. C'est`MessageType`est défini sur`NEW_ASSOCIATION`, il envoie donc 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"
         ]
        }
      }
}
```

Mise à jourAWS Systems Managerintégration dansDevOpsGourou

Vous pouvez activer la création d'un OpsItem pour chaque nouvel aperçu deAWS Systems Manager OpsCenter. OpsCenter est un système centralisé dans lequel vous pouvez visualiser, étudier et examiner les éléments de travail opérationnels (OpsItems). Le OpsItems car vos informations peuvent 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, voirAWS Systems Manager OpsCenteretTravailler avec OpsItemdans leAWS Systems ManagerGuide de l'utilisateur.

> **Note**
>
> Si vous modifiez la clé ou la valeur du champ de balise d'un OpsItem, puis DevOpsGuru n'est pas en mesure de le mettre à jour OpsItem. Par exemple, si vous modifiez le tag d'un OpsItem à partir de`"aws:RequestTag/DevOps-GuruInsightSsmOpsItemRelated": "true"`à autre chose, alors DevOpsGuru ne peut pas le mettre à jour OpsItem.

Pour gérer votre intégration à Systems Manager

1. Ouvrez Amazon DevOpsConsole Guru àhttps://console.aws.amazon.com/devops-guru/.
2. Choisissez Settings (Paramètres) dans le volet de navigation.
3. DansAWS Systems Managerintégration, sélectionnezActiver DevOpsGuru pour créer unAWS OpstItem dans OpsCenter pour chaque aperçupour avoir un OpsItem créé pour chaque nouvel aperçu. Désélectionnez-le pour ne plus avoir OpsItemcréé pour chaque nouvel aperçu.

Vous êtes facturé pour OpsItems créé dans votre compte. Pour en savoir plus, consultez PricingAWS Systems Manager (Tarification).

Mise à jour de la détection des anomalies du journal dansDevOpsGourou

Pour gérer les paramètres de détection des anomalies du journal

1. Ouvrez Amazon DevOpsConsole Guru àhttps://console.aws.amazon.com/devops-guru/.
2. Choisissez Settings (Paramètres) dans le volet de navigation.
3. DansDétection des anomalies du journal, sélectionnezActivez la détection des anomalies du journal en accordant DevOpsAutorisations du gourou pour afficher les données du journal associées à un aperçu.avoirDevOpsGuru affiche les données du journal relatives aux informations.

Mise à jour des paramètres de chiffrement dansDevOpsGourou

Vous pouvez mettre à jour les paramètres de chiffrement pour utiliserAWSclés possédées ouAWS KMSclés gérées par le client. Lorsque vous passez à un nouveau client géréAWS KMSclé gérée par un client existantAWS KMSclé, DevOpsGuru commence automatiquement à chiffrer les métadonnées nouvellement ingérées à l'aide de la nouvelle clé. Les données historiques resteront cryptées avec la configuration précédente gérée par le clientAWS KMSclé.

> **Note**
>
> Si vous révoquez la subvention, désactivez ou supprimez la précédenteAWS KMSclé, DevOpsGuru ne pourra accéder à aucune des données cryptées par cette clé et vous verrez peut-être le`AccessDeniedException`lors d'une opération de lecture.

Pour gérer vos paramètres de chiffrement

1. Ouvrez Amazon DevOpsConsole Guru àhttps://console.aws.amazon.com/devops-guru/.
2. Choisissez Settings (Paramètres) dans le volet de navigation.
3. Dans leChiffrementsection, choisissezModifier le chiffrement.
4. Sélectionnez le type de cryptage que vous souhaitez utiliser pour protéger vos données. Vous pouvez utiliser une valeur par défautAWSclé détenue, choisissez une clé gérée par le client existante ou créez une nouvelle clé gérée par le clientAWS KMSclé.
5. Choisissez Save (Enregistrer).

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

Affichage des notifications

Il existe différents types de notifications dans DevOps Guru.

Rubriques

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 AWS 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"
}
```

Affichage des ressources analysées parDevOpsGuru

DevOpsGuru fournit une liste des noms de ressources et de leurs limites d'application en cours d'analyse à l'aide du`ListMonitoredResources`action. Ces informations sont collectées auprès d'AmazonCloudWatch,AWS CloudTrail, et d'autresAWSservices utilisant leDevOpsRôle lié au service Guru.

Notez que même si un utilisateur ne dispose pas de l'autorisation explicite d'accéder aux API d'un autre service tel queAWS Lambdaou Amazon RDS,DevOpsGuru fournit toujours une liste de ressources provenant de ce service tant que`ListMonitoredResources`l'action est autorisée.

Rubriques

- Mettre à jour votreAWScouverture de l'analyse dansDevOpsGuru
- Suppression de la vue des ressources analysées pour les utilisateurs

Mettre à jour votreAWScouverture de l'analyse dansDevOpsGuru

Vous pouvez mettre à jour quelsAWSressources de votre compteDevOpsDes analyses de gourou. Les ressources analysées constituent votreDevOpsLimite de couverture de Guru. Lorsque vous définissez votre limite, vos ressources sont regroupées dans des applications. Vous disposez de quatre options de couverture des limites.

- Choisissez d'avoirDevOpsGuru analyse 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 votre compte comporte plusieurs piles, les ressources de chaque pile constituent leur propre application. Si certaines ressources de votre compte ne figurent pas dans une pile, elles sont regroupées dans leur propre application.
- Spécifiez les ressources en choisissantAWS CloudFormationdes piles qui définissent ces ressources. Si tu fais ça,DevOpsGuru analyse chaque ressource spécifiée dans les piles que vous choisissez. Si une ressource de votre compte n'est pas définie par une pile de votre choix, elle n'est pas analysée. Pour plus d'informations, voirUtilisation de pilesdans leAWS CloudFormationGuide de l'utilisateuretDéterminer la couverture pour DevOps Guru.
- Spécifiez les ressources en utilisantAWSbalises. 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 plus d'informations, veuillez consulter Utilisation de 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, des frais mineurs peuvent continuer à vous être facturés si vous passez en revue les informations existantes générées parDevOpsGuru dans le passé. Ces frais sont associés aux appels d'API utilisés pour récupérer et afficher des informations analytiques. Pour plus d'informations, voirAmazonDevOpsTarifs 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, voirAmazonDevOpsTarifs Guru.

Pour gérer votreDevOpsCouverture de l'analyse de Guru

1. Ouvrez l'AmazonDevOpsConsole Guru àhttps://console.aws.amazon.com/devops-guru/.
2. ÉlargirRessources analyséesdans le volet de navigation.
3. Choisissez Edit (Modifier).
4. Choisissez l'une des options de couverture suivantes.

   - ChoisissezToutes les ressources du comptesi tu veuxDevOpsGuru pour analyser toutes les ressources prises en charge dans votreAWScompte et région. Si vous choisissez cette option, votreAWSle 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.
   - ChoisissezCloudFormationpilessi tu veuxDevOpsGuru pour analyser les ressources qui se trouvent dans les piles de votre choix, puis choisissez l'une des options suivantes.
     - Toutes les ressources— Toutes les ressources présentes dans les piles de 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 souhaitezDevOpsUn gourou de l'analyse. Les ressources de chaque pile que vous sélectionnez sont regroupées dans leur propre application. Vous pouvez saisir le nom d'une pile dansTrouvez des pilespour localiser rapidement une pile spécifique. Vous pouvez sélectionner jusqu'à 1 000 piles.

Pour plus d'informations, veuillez consulter A l'aide deAWS CloudFormationdes piles pour identifier les ressources de votre DevOpsApplications Guru.

- ChoisissezÉtiquettessi tu veuxDevOpsGuru pour analyser toutes les ressources contenant les balises que vous avez choisies. Choisissez unclé, puis choisissez l'une des options suivantes.
  - Toutes les ressources du compte—Analysez toutes les ressources AWS de la région et du compte actuels. Les ressources associées à la clé de balise sélectionnée sont regroupées par valeur de balise, s'il en existe une. Les ressources sans cette clé de balise sont regroupées et analysées séparément.
  - Choisissez des valeurs de balise spécifiques— Toutes les ressources qui contiennent un tag avec leclévous avez choisi sont analysés. DevOpsGuru regroupe vos ressources en applications en fonction de vos balisesvaleurs.

  Le tagclédoit commencer par le préfixe`devops-guru-`. Ce préfixe ne fait pas la distinction entre majuscules et minuscules. Par exemple, uncléest`DevOps-Guru-Production-Applications`. Pour plus d'informations, veuillez consulter Utilisation de balises pour identifier les ressources dans vos applications DevOps Guru.
- ChoisissezAucunsi tu ne veux pasDevOpsGuru pour analyser toutes les ressources. Cette option désactiveDevOpsGuru pour que vous n'entriez plus de 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 ne dispose pas d'une autorisation explicite pour accéder aux API d'un autre service tel que Lambda ou Amazon RDS,DevOpsGuru fournit toujours une liste de ressources provenant de ce service tant que`ListMonitoredResources`l'action est autorisée. Pour modifier ce comportement, vous pouvez mettre à jour votreAWSPolitique de l'IAM consistant à refuser cette action.

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

Meilleures pratiques en DevOps Guru

Les meilleures pratiques suivantes peuvent vous aider à comprendre, diagnostiquer et corriger les comportements anormaux détectés par Amazon DevOps Guru. Bonnes pratiques avecComprendre les informations contenues dansDevOpsConsole Gurupour résoudre les problèmes opérationnels détectés par DevOps Guru.

- Dans la vue chronologique d'un aperçu, examinez d'abord les mesures mises en surbrillance. Ils sont souvent des indicateurs clés du problème.
- Utilisez Amazon CloudWatch pour afficher les mesures qui se sont produites immédiatement avant la première mesure mise en surbrillance dans un aperçu afin de déterminer quand et comment le comportement a changé. Cela peut vous aider à diagnostiquer et à corriger le problème.
- Pour les ressources Amazon RDS, consultez les mesures Performance Insights. En corrélant les mesures de compteur avec la charge de base de données, vous pouvez obtenir des informations détaillées sur les problèmes de performances. Pour de plus amples informations, veuillez consulterAnalyse des anomalies de performances avec DevOps Gurufor Amazon RDS.
- Les dimensions multiples d'une même mesure peuvent souvent être anormales. Examinez les dimensions de la vue graphique pour mieux comprendre le problème.
- Consultez la section Événements d'un aperçu des événements de déploiement ou d'infrastructure survenus au moment de la création de l'information. 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 les tickets de votre système d'exploitation qui se sont produits à peu près au même moment pour trouver des indices.
- Dans un aperçu, lisez les recommandations et visitez les liens des recommandations. Ces derniers comportent souvent des étapes de dépannage qui peuvent vous aider à diagnostiquer et à résoudre rapidement les problèmes.
- N'ignorez pas les informations résolues à moins d'avoir déjà résolu le problème. Une fois par jour, regardez de nouvelles informations, même si elles ont été résolues. Essayez de comprendre la cause première derrière le plus grand nombre de connaissances possible. Recherchez un modèle qui pourrait être le signe d'un problème systémique. Si un problème systémique n'est pas résolu, il pourrait causer des problèmes plus graves à l'avenir. La résolution des problèmes transitoires peut maintenant aider à prévenir les incidents futurs et plus graves.

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 entreprises les plus sensibles en matière de sécurité.

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

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

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

Rubriques

Protection des données dans Amazon DevOps Guru

Le modèle de responsabilité AWS partagée s'applique à la protection des données dans Amazon DevOps Guru. Comme décrit dans ce modèle, AWS est chargé de protéger l'infrastructure mondiale qui gère tous les AWS Cloud. La gestion du contrôle de votre contenu hébergé sur cette infrastructure relève de votre responsabilité. Vous êtes également responsable des tâches de configuration et de gestion de la sécurité des Services AWS que vous utilisez. Pour plus d'informations sur la confidentialité des données, consultez Questions fréquentes (FAQ) sur la confidentialité des données. Pour en savoir plus sur la protection des données en Europe, consultez le billet de blog Modèle de responsabilité partagée AWS et RGPD (Règlement général sur la protection des données) sur le Blog de sécuritéAWS .

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

- Utilisez l'authentification multifactorielle (MFA) avec chaque compte.
- Utilisez le protocole SSL/TLS pour communiquer avec les ressources. AWS Nous exigeons TLS 1.2 et recommandons TLS 1.3.
- Configurez l'API et la journalisation de l'activité des utilisateurs avec AWS CloudTrail.
- Utilisez des solutions de AWS chiffrement, ainsi que tous les contrôles de sécurité par défaut qu'ils contiennent Services AWS.
- Utilisez des services de sécurité gérés avancés tels qu'Amazon Macie, qui contribuent à la découverte et à la sécurisation des données sensibles stockées dans Amazon S3.
- Si vous avez besoin de modules cryptographiques validés par la norme FIPS 140-2 pour accéder AWS via une interface de ligne de commande ou une API, utilisez un point de terminaison FIPS. Pour plus d'informations sur les points de terminaison FIPS (Federal Information Processing Standard) disponibles, consultez Federal Information Processing Standard (FIPS) 140-2 (Normes de traitement de l'information fédérale).

Nous vous recommandons fortement de ne jamais placer d'informations confidentielles ou sensibles, telles que les adresses e-mail de vos clients, dans des balises ou des champs de texte libre tels que le champ Name (Nom). Cela inclut lorsque vous travaillez avec DevOps Guru ou une autre personne Services AWS à l'aide de la console, de l'API ou AWS des SDK. 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 intervention de votre part. Vous pouvez configurer d'autres types de chiffrement, par exemple pour les données au repos, lorsque vous créez votre projet ou votre build.

- 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 par le protocole TLS et authentifiées à l'aide du processus de signature Signature version 4. Tous les points de terminaison DevOps Guru utilisent des certificats gérés par AWS Private Certificate Authority. 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 à l'aide d'Amazon S3, Amazon DynamoDB et Amazon Kinesis. Si AWS CloudFormation des piles sont utilisées pour définir les ressources analysées, les données des piles sont également collectées. DevOpsGuru applique les politiques de conservation des données d'Amazon S3, DynamoDB et Kinesis. Les données stockées dans Kinesis peuvent être conservées jusqu'à un an, selon les politiques définies. Les données stockées dans Amazon S3 et DynamoDB sont stockées pendant un an.

  Les données stockées sont chiffrées à l'aide des fonctionnalités de data-at-rest chiffrement d'Amazon S3, DynamoDB et Kinesis.

  Clés gérées par le client : DevOps Guru prend en charge le chiffrement du contenu client et des métadonnées sensibles telles que les anomalies de journal générées à partir des CloudWatch journaux à l'aide de 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 les paramètres de votre 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. Toutefois, AWS KMS des frais s'appliquent pour l'utilisation d'une clé gérée par le client. Pour plus d'informations sur les tarifs, consultez les AWS Key Management Service tarifs.

Comment DevOps Guru utilise les subventions dans AWS KMS

DevOpsGuru a besoin d'une autorisation 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 donner à DevOps Guru l'accès à une AWS KMS clé dans un compte client.

DevOpsGuru a besoin de l'autorisation d'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 symétrique géré par le client saisi lors de la création d'un tracker ou d'une collection de géofences est valide.

- Envoyez GenerateDataKey des demandes AWS KMS à pour générer des clés de données chiffrées par votre clé gérée par le client.
- Envoyez des demandes de déchiffrement AWS KMS à pour déchiffrer les clés de données chiffrées afin qu'elles puissent être utilisées pour chiffrer 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 essayez 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 les ressources de votre 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 AWS Management Console ou des AWS KMS API.

Pour créer une clé symétrique gérée par le client, reportez-vous à la section Création de clés KMS de chiffrement symétriques.

Stratégie de clé

Les politiques de clés 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 les ressources de votre DevOps Guru, les opérations d'API suivantes doivent être autorisées dans la politique des clés :

- `kms:CreateGrant` : ajoute une attribution à une clé gérée par le client. Accorde un accès de contrôle à une AWS KMS clé spécifiée, ce qui permet d'accéder aux opérations d'octroi 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 de faire ce qui suit :

- Appelez GenerateDataKey pour générer une clé de données cryptée 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.
- Configurez un directeur partant à la retraite pour permettre au service de RetireGrant.
- Utilisez kms : DescribeKey pour fournir les informations relatives aux clés gérées 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 votre analyse des ressources et de la génération d'informations en configurant DevOps Guru pour qu'il utilise un point de terminaison VPC d'interface. 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 plus d'informations, consultez DevOpsPoints de terminaison VPC Guru et interface ()AWS PrivateLink. Pour plus d'informations sur PrivateLink les points de terminaison VPC, consultez et AWS PrivateLinkAccès aux services AWS via. PrivateLink

Identity and Access Management pour Amazon DevOps Guru

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

Rubriques

- Public ciblé

- Authentification par des identités
- Gestion des accès à l'aide de politiques
- DevOpsMises à jour de Guru AWS concernant les politiques gérées et le rôle lié au service
- Comment Amazon DevOps Guru travaille avec IAM
- Politiques basées sur l'identité pour Amazon Guru DevOps
- Utilisation de rôles liés à un service pour Guru DevOps
- Référence des autorisations Amazon DevOps Guru
- Autorisations pour les rubriques Amazon SNS
- Autorisations pour les AWS KMS rubriques Amazon SNS chiffrées
- Résolution des problèmes d'identité et d'accès à Amazon DevOps Guru

Public ciblé

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

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

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

Administrateur IAM — Si vous êtes administrateur IAM, vous souhaiterez peut-être en savoir plus sur la manière dont vous pouvez rédiger des politiques pour gérer l'accès à DevOps Guru. Pour consulter des exemples de politiques basées sur l'identité DevOps Guru que vous pouvez utiliser dans IAM, consultez. Politiques basées sur l'identité pour Amazon Guru DevOps

Authentification par des identités

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

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

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

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

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

Compte AWS utilisateur root

Lorsque vous créez un Compte AWS, vous commencez par une identité de connexion unique qui donne un accès complet à toutes Services AWS les ressources du compte. Cette identité est appelée utilisateur Compte AWS root et est accessible en vous connectant avec l'adresse e-mail et le mot de passe que vous avez utilisés pour créer le compte. Il est vivement recommandé de ne pas

utiliser l'utilisateur racine pour vos tâches quotidiennes. Protégez vos informations d'identification d'utilisateur racine et utilisez-les pour effectuer les tâches que seul l'utilisateur racine peut effectuer. Pour obtenir la liste complète des tâches qui vous imposent de vous connecter en tant qu'utilisateur root, consultez Tâches nécessitant des informations d'identification d'utilisateur root dans le Guide de l'utilisateur IAM.

Identité fédérée

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

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

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

Utilisateurs et groupes IAM

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

Un groupe IAM est une identité qui concerne un ensemble d'utilisateurs IAM. Vous ne pouvez pas vous connecter en tant que groupe. Vous pouvez utiliser les groupes pour spécifier des autorisations pour plusieurs utilisateurs à la fois. Les groupes permettent de gérer plus facilement les autorisations

pour de grands ensembles d'utilisateurs. Par exemple, vous pouvez avoir un groupe nommé IAMAdmins et accorder à ce groupe les autorisations d'administrer des ressources IAM.

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

Rôles IAM

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

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

- Accès utilisateur fédéré – Pour attribuer des autorisations à une identité fédérée, vous créez un rôle et définissez des autorisations pour le rôle. Quand une identité externe s'authentifie, l'identité est associée au rôle et reçoit les autorisations qui sont définies par celui-ci. Pour obtenir des informations sur les rôles pour la fédération, consultez Création d'un rôle pour un fournisseur d'identité tiers (fédération) dans le Guide de l'utilisateur IAM. Si vous utilisez IAM Identity Center, vous configurez un jeu d'autorisations. IAM Identity Center met en corrélation le jeu d'autorisations avec un rôle dans IAM afin de contrôler à quoi vos identités peuvent accéder après leur authentification. Pour plus d'informations sur les jeux d'autorisations, consultez la rubrique Jeux d'autorisations dans le Guide de l'utilisateur AWS IAM Identity Center .
- Autorisations d'utilisateur IAM temporaires : un rôle ou un utilisateur IAM peut endosser un rôle IAM pour profiter temporairement d'autorisations différentes pour une tâche spécifique.
- Accès intercompte : vous pouvez utiliser un rôle IAM pour permettre à un utilisateur (principal de confiance) d'un compte différent d'accéder aux ressources de votre compte. Les rôles constituent le principal moyen d'accorder l'accès intercompte. Toutefois, dans certains Services AWS cas, vous pouvez associer une politique directement à une ressource (au lieu d'utiliser un rôle comme proxy). Pour en savoir plus sur la différence entre les rôles et les politiques basées sur les ressources pour l'accès intercompte, consultez Différence entre les rôles IAM et les politiques basées sur les ressources dans le Guide de l'utilisateur IAM.

- Accès multiservices — Certains Services AWS utilisent des fonctionnalités dans d'autres Services AWS. Par exemple, lorsque vous effectuez un appel dans un service, il est courant que ce service exécute des applications dans Amazon EC2 ou stocke des objets dans Amazon S3. Un service peut le faire en utilisant les autorisations d'appel du principal, un rôle de service ou un rôle lié au service.
  - Sessions d'accès direct (FAS) : lorsque vous utilisez un utilisateur ou un rôle IAM pour effectuer des actions AWS, vous êtes considéré comme un mandant. Lorsque vous utilisez certains services, vous pouvez effectuer une action qui initie une autre action dans un autre service. FAS utilise les autorisations du principal appelant et Service AWS, associées Service AWS à la demande, pour adresser des demandes aux services en aval. Les demandes FAS ne sont effectuées que lorsqu'un service reçoit une demande qui nécessite des interactions avec d'autres personnes Services AWS ou des ressources pour être traitée. Dans ce cas, vous devez disposer d'autorisations nécessaires pour effectuer les deux actions. Pour plus de détails sur la politique relative à la transmission de demandes FAS, consultez Sessions de transmission d'accès.
  - Rôle de service : il s'agit d'un rôle IAM attribué à un service afin de réaliser des actions en votre nom. Un administrateur IAM peut créer, modifier et supprimer une fonction du service à partir d'IAM. Pour plus d'informations, consultez Création d'un rôle pour la délégation d'autorisations à un Service AWS dans le Guide de l'utilisateur IAM.
  - Rôle lié à un service — Un rôle lié à un service est un type de rôle de service lié à un. Service AWS Le service peut endosser le rôle afin d'effectuer une action en votre nom. Les rôles liés à un service apparaissent dans votre Compte AWS répertoire et appartiennent au service. Un administrateur IAM peut consulter, mais ne peut pas modifier, les autorisations concernant les rôles liés à un service.
- Applications exécutées sur Amazon EC2 : vous pouvez utiliser un rôle IAM pour gérer les informations d'identification temporaires pour les applications qui s'exécutent sur une instance EC2 et qui envoient des demandes d'API. AWS CLI AWS Cette solution est préférable au stockage des clés d'accès au sein de l'instance EC2. Pour attribuer un AWS rôle à une instance EC2 et le mettre à la disposition de toutes ses applications, vous devez créer un profil d'instance attaché à l'instance. Un profil d'instance contient le rôle et permet aux programmes qui s'exécutent sur l'instance EC2 d'obtenir des informations d'identification temporaires. Pour plus d'informations, consultez Utilisation d'un rôle IAM pour accorder des autorisations à des applications s'exécutant sur des instances Amazon EC2 dans le Guide de l'utilisateur IAM.

Pour savoir dans quel cas utiliser des rôles ou des utilisateurs IAM, consultez Quand créer un rôle IAM (au lieu d'un utilisateur) dans le Guide de l'utilisateur IAM.

Gestion des accès à l'aide de politiques

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

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

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

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

Politiques basées sur l'identité

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

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

une politique gérée et une politique en ligne, consultez Choix entre les politiques gérées et les politiques en ligne dans le Guide de l'utilisateur IAM.

politiques basées sur les ressources

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

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

Listes de contrôle d'accès (ACL)

Les listes de contrôle d'accès (ACL) vérifie quels principals (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.

Amazon S3 et Amazon VPC sont des exemples de services qui prennent en charge les ACL. AWS WAF Pour en savoir plus sur les listes de contrôle d'accès, consultez Vue d'ensemble des listes de contrôle d'accès (ACL) dans le Guide du développeur Amazon Simple Storage Service.

Autres types de politique

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

- Limite d'autorisations : une limite d'autorisations est une fonctionnalité avancée dans laquelle vous définissez le nombre maximal d'autorisations qu'une politique basée sur l'identité peut accorder à une entité IAM (utilisateur ou rôle IAM). Vous pouvez définir une limite d'autorisations pour une entité. Les autorisations en résultant représentent la combinaison des politiques basées sur

l'identité d'une entité et de ses limites d'autorisation. Les politiques basées sur les ressources qui spécifient l'utilisateur ou le rôle dans le champ `Principal` ne sont pas limitées par les limites d'autorisations. Un refus explicite dans l'une de ces politiques remplace l'autorisation. Pour plus d'informations sur les limites d'autorisations, consultez Limites d'autorisations pour des entités IAM dans le Guide de l'utilisateur IAM.

- Politiques de contrôle des services (SCP) — Les SCP sont des politiques JSON qui spécifient les autorisations maximales pour une organisation ou une unité organisationnelle (UO) dans. AWS Organizations AWS Organizations est un service permettant de regrouper et de gérer de manière centralisée Comptes AWS les multiples propriétés de votre entreprise. Si vous activez toutes les fonctionnalités d'une organisation, vous pouvez appliquer les politiques de contrôle des services (SCP) à l'un ou à l'ensemble de vos comptes. Le SCP limite les autorisations pour les entités figurant dans les comptes des membres, y compris chacune Utilisateur racine d'un compte AWS d'entre elles. Pour plus d'informations sur les organisations et les SCP, consultez Fonctionnement des SCP dans le Guide de l'utilisateur AWS Organizations .
- Politiques de séance : les politiques de séance sont des politiques avancées que vous utilisez en tant que paramètre lorsque vous créez par programmation une séance temporaire pour un rôle ou un utilisateur fédéré. Les autorisations de séance en résultant sont une combinaison des politiques basées sur l'identité de l'utilisateur ou du rôle et des politiques de séance. Les autorisations peuvent également provenir d'une politique basée sur les ressources. Un refus explicite dans l'une de ces politiques annule l'autorisation. Pour plus d'informations, consultez politiques de séance 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 concernant les politiques gérées et le rôle lié au service

Consultez les détails des mises à jour des politiques AWS gérées et du rôle lié au service 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 flux RSS du DevOps GuruAmazonDevOpsHistorique du document Guru.

Modification	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'abonnement Amazon SNS.	9 août 2023
AmazonDevOpsGuruServiceRolePolicy - Mettre à jour vers une politique existante.	Le rôle `AWSServiceRoleForDevOpsGuru` lié au 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
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

Modification	Description	Date
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 au service prend désormais en charge les actions de CloudWatch journalisation `FilterLogEvents` `DescribeLogGroups` , et. `DescribeLogStreams`	12 juillet 2022
Politiques basées sur l'identité pour DevOps Guru — Nouvelle politique gérée.	La `AmazonDevOpsGuruConsoleFullAccess` politique a été ajoutée.	16 décembre 2021

Modification	Description	Date
AmazonDevOpsGuruServiceRolePolicy - Mettre à jour vers une politique existante.	Le rôle `AWSServiceRoleForDevOpsGuru` lié au service prend désormais en charge les actions Performance Insights `DescribeMetricsKeys` et Amazon `DescribeDBInstances` RDS.	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 `DescribeDBInstances` RDS.	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

Modification	Description	Date
Politiques basées sur l'identité pour Amazon Guru DevOps— Ajout d'une nouvelle politique.	Le rôle `AWSServiceRoleForDevOpsGuru` lié au service prend désormais en charge l'accès aux actions Amazon RDS et Performance `DescribeDBInstances` Insights. `GetResourceMetrics` La politique `AmazonDevOpsGuruOrganizationsAccess` gérée donne accès à DevOps Guru au sein d'une organisation.	16 novembre 2021
AmazonDevOpsGuruServiceRolePolicy - Mettre à jour vers une politique existante.	Le rôle `AWSServiceRoleForDevOpsGuru` lié à un service est désormais compatible avec AWS Organizations.	4 novembre 2021
AmazonDevOpsGuruServiceRolePolicy - Mettre à jour vers une politique existante.	Le rôle `AWSServiceRoleForDevOpsGuru` lié au service contient désormais de nouvelles conditions sur les actions `ssm:CreateOpsItem`et`ssm:AddTagsToResource` .	11 octobre 2021

Modification	Description	Date
Autorisations de rôle liées au service pour Guru DevOps - Mettre à jour vers une politique existante.	Le rôle `AWSServiceRoleForDevOpsGuru` lié au 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 AWS Identity and Access Management `GetRole` et au 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
AmazonDevOpsGuruServiceRolePolicy - Mettre à jour vers une politique existante.	Le `AWSServiceRoleForDevOpsGuru` rôle permet désormais d'accéder aux actions AWS Systems Manager `AddTagsToResource` et à Amazon EC2 Auto Scaling `DescribeAutoScalingGroups`.	27 avril 2021

Modification	Description	Date
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 travaille 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

Fonction IAM	DevOpsAssistance aux gourous
Politiques basées sur l'identité	Oui
Politiques basées sur les ressources	Non
Actions de politique	Oui
Ressources de politique	Oui
Clés de condition d'une politique	Oui
ACL	Non
ABAC (étiquettes dans les politiques)	Non
Informations d'identification temporaires	Oui
Autorisations de principal	Oui
Fonctions du service	Non
Rôles liés à un service	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 compatibles avec IAM dans le Guide de l'utilisateur IAM.

Politiques basées sur l'identité pour Guru DevOps

Prend en charge les politiques basées sur l'identité	Oui

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

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

Exemples de politiques basées sur l'identité pour Guru DevOps

Pour consulter des exemples de politiques basées sur l'identité de DevOps Guru, consultez. Politiques basées sur l'identité pour Amazon Guru DevOps

Politiques basées sur les ressources au sein de Guru DevOps

Prend en charge les politiques basées sur les ressources	Non

Les politiques basées sur les ressources sont des documents de politique JSON que vous attachez à une ressource. Des politiques basées sur les ressources sont, par exemple, les politiques de confiance de rôle IAM et des politiques de compartiment. Dans les services qui sont compatibles avec les politiques basées sur les ressources, les administrateurs de service peuvent les utiliser pour

contrôler l'accès à une ressource spécifique. Pour la ressource dans laquelle se trouve la politique, cette dernière définit quel type d'actions un principal spécifié peut effectuer sur cette ressource et dans quelles conditions. Vous devez spécifier un principal dans une politique basée sur les ressources. Les principaux peuvent inclure des comptes, des utilisateurs, des rôles, des utilisateurs fédérés ou. Services AWS

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

Actions politiques pour DevOps Guru

Prend en charge les actions de politique	Oui

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

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

Intégration d'actions dans une stratégie 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 politiques 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. Politiques basées sur l'identité pour Amazon Guru DevOps

Ressources sur les politiques pour DevOps Guru

Prend en charge les ressources de politique	Oui

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

L'élément de politique JSON `Resource` indique le ou les objets auxquels l'action s'applique. Les instructions doivent inclure un élément `Resource` ou `NotResource`. Il est recommandé de définir une ressource à l'aide de son Amazon Resource Name (ARN). Vous pouvez le faire pour des actions qui prennent en charge un type de ressource spécifique, connu sous la dénomination autorisations de niveau ressource.

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

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

Pour consulter la liste des types de ressources DevOps Guru et leurs ARN, consultez la section Ressources définies par Amazon DevOps Guru dans le Service Authorization Reference. Pour savoir

avec quelles actions vous pouvez spécifier l'ARN de chaque ressource, consultez Actions définies par Amazon DevOps Guru.

Pour consulter des exemples de politiques basées sur l'identité de DevOps Guru, consultez. Politiques basées sur l'identité pour Amazon Guru DevOps

Clés de conditions de politique pour DevOps Guru

Prend en charge les clés de condition de politique spécifiques au service	Oui

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

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

Si vous spécifiez plusieurs éléments `Condition` dans une instruction, ou plusieurs clés dans un seul élément `Condition`, AWS les évalue à l'aide d'une opération `AND` logique. Si vous spécifiez plusieurs valeurs pour une seule clé de condition, AWS évalue la condition à l'aide d'une `OR` opération logique. Toutes les conditions doivent être remplies avant que les autorisations associées à l'instruction ne soient accordées.

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

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

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 ressources vous pouvez utiliser une clé de condition, consultez Actions définies par Amazon DevOps Guru.

Pour consulter des exemples de politiques basées sur l'identité de DevOps Guru, consultez. Politiques basées sur l'identité pour Amazon Guru DevOps

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

Prend en charge les listes ACL	Non

Les listes de contrôle d'accès (ACL) vérifient 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.

Contrôle d'accès basé sur les attributs (ABAC) avec Guru DevOps

Prise en charge d'ABAC (identifications dans les politiques)	Non

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

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

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

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

Pour plus d'informations sur l'ABAC, consultez Qu'est-ce que le contrôle d'accès basé sur les attributs (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

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

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

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

Autorisations principales interservices pour Guru DevOps

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

Lorsque vous utilisez un utilisateur ou un rôle IAM pour effectuer des actions AWS, vous êtes considéré comme un mandant. Lorsque vous utilisez certains services, vous pouvez effectuer une

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

Rôles de service pour DevOps Guru

Prend en charge les fonctions de service	Non

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

> **Warning**
>
> La modification des autorisations associées à un rôle de service peut perturber les fonctionnalités de DevOps Guru. Modifiez les rôles de service uniquement lorsque DevOps Guru fournit des conseils à cet effet.

Rôles liés aux services pour Guru DevOps

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

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 Rôle lié à un service. Choisissez le lien Oui pour consulter la documentation du rôle lié à ce service.

Politiques basées sur l'identité pour Amazon Guru DevOps

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

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

Pour plus de détails 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

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

- Commencez AWS par les politiques gérées et passez aux autorisations du moindre privilège : pour commencer à accorder des autorisations à vos utilisateurs et à vos charges de travail, utilisez les politiques AWS gérées qui accordent des autorisations pour de nombreux cas d'utilisation courants. Ils sont disponibles dans votre Compte AWS. Nous vous recommandons de réduire

davantage les autorisations en définissant des politiques gérées par les AWS clients spécifiques à vos cas d'utilisation. Pour plus d'informations, consultez politiques gérées par AWS ou politiques gérées par AWS pour les activités professionnelles dans le Guide de l'utilisateur IAM.

- Accorder 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 de IAM pour appliquer des autorisations, consultez politiques et autorisations dans IAM dans le Guide de l'utilisateur IAM.
- Utiliser des conditions dans les politiques IAM pour restreindre davantage l'accès : vous pouvez ajouter une condition à vos politiques afin de limiter l'accès aux actions et aux ressources. Par exemple, vous pouvez écrire une condition de politique pour spécifier que toutes les demandes doivent être envoyées via SSL. Vous pouvez également utiliser des conditions pour accorder l'accès aux actions de service si elles sont utilisées par le biais d'un service spécifique Service AWS, tel que AWS CloudFormation. Pour plus d'informations, consultez Conditions pour éléments de politique JSON IAM dans le Guide de l'utilisateur IAM.
- Utilisez IAM Access Analyzer pour valider vos politiques IAM afin de garantir des autorisations sécurisées et fonctionnelles : IAM Access Analyzer 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 politique IAM Access Analyzer dans le Guide de l'utilisateur IAM.
- Exiger l'authentification multifactorielle (MFA) : si vous avez un scénario qui nécessite des utilisateurs IAM ou un utilisateur root, activez l'authentification MFA pour une sécurité accrue. Compte AWS Pour exiger le MFA lorsque des opérations d'API sont appelées, ajoutez des conditions MFA à vos politiques. Pour plus d'informations, consultez Configuration de l'accès aux API protégé par 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 minimal d'autorisations. Ces autorisations doivent vous permettre de répertorier et de consulter les détails des

ressources DevOps Guru de votre Compte AWS. Si vous créez une stratégie 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 stratégie.

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

Pour garantir que les utilisateurs et les rôles peuvent toujours utiliser la console DevOps Guru, associez également le DevOps Guru `AmazonDevOpsGuruReadOnlyAccess` ou la politique `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 les autorisations permettant d'effectuer cette action sur la console ou par programmation à l'aide de l'API AWS CLI or AWS .

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "ViewOwnUserInfo",
            "Effect": "Allow",
            "Action": [
                "iam:GetUserPolicy",
                "iam:ListGroupsForUser",
                "iam:ListAttachedUserPolicies",
                "iam:ListUserPolicies",
                "iam:GetUser"
            ],
            "Resource": ["arn:aws:iam::*:user/${aws:username}"]
        },
        {
            "Sid": "NavigateInConsole",
            "Effect": "Allow",
            "Action": [
                "iam:GetGroupPolicy",
                "iam:GetPolicyVersion",
                "iam:GetPolicy",
```

```
                "iam:ListAttachedGroupPolicies",
                "iam:ListGroupPolicies",
                "iam:ListPolicyVersions",
                "iam:ListPolicies",
                "iam:ListUsers"
            ],
            "Resource": "*"
        }
    ]
}
```

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 les autorisations nécessaires. Pour de plus amples informations, veuillez consulter Stratégies gérées par AWS dans le Guide de l'utilisateur IAM.

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

Vous pouvez également créer vos propres politiques IAM personnalisées pour autoriser les actions et les ressources du 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 les autorisations pour créer des sujets Amazon SNS, accéder aux CloudWatch métriques Amazon

et accéder aux piles d'accès AWS CloudFormation . Ne l'appliquez qu'aux utilisateurs de niveau administratif auxquels vous souhaitez accorder un contrôle total sur Guru. DevOps

La `AmazonDevOpsGuruFullAccess` politique contient la déclaration suivante.

```
{
    "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 les autorisations pour créer des sujets Amazon SNS, accéder aux CloudWatch métriques Amazon et accéder aux piles d'accès AWS CloudFormation . Cette politique comporte des autorisations supplémentaires relatives aux informations sur les performances afin que vous puissiez consulter les analyses détaillées relatives aux instances de base de données Amazon RDS Aurora anormales dans la console. Ne l'appliquez qu'aux utilisateurs de niveau administratif auxquels vous souhaitez accorder un contrôle total sur Guru. DevOps

La `AmazonDevOpsGuruConsoleFullAccess` politique contient la déclaration suivante.

```
{
    "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`— Accorde 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 les informations, mais pas de mettre à jour la limite de couverture des analyses de DevOps Guru, les rubriques Amazon SNS ou l'intégration de Systems Manager OpsCenter.

La `AmazonDevOpsGuruReadOnlyAccess` politique contient la déclaration suivante.

```
{
"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 DevOps Guru de votre organisation. Vous pouvez appliquer `AmazonDevOpsGuruReadOnlyAccess` ou compléter `AmazonDevOpsGuruFullAccess` cette politique pour fournir un accès complet ou en lecture seule à DevOps Guru.

La `AmazonDevOpsGuruOrganizationsAccess` politique contient la déclaration suivante.

```
{
 "Version": "2012-10-17",
 "Statement": [
  {
   "Sid": "AmazonDevOpsGuruOrganizationsAccess",
   "Effect": "Allow",
   "Action": [
    "devops-guru:DescribeOrganizationHealth",
    "devops-guru:DescribeOrganizationResourceCollectionHealth",
    "devops-guru:DescribeOrganizationOverview",
    "devops-guru:ListOrganizationInsights",
    "devops-guru:SearchOrganizationInsights"
   ],
   "Resource": "*"
  },
  {
   "Sid": "OrganizationsDataAccess",
   "Effect": "Allow",
```

```
    "Action": [
     "organizations:DescribeAccount",
     "organizations:DescribeOrganization",
     "organizations:ListAWSServiceAccessForOrganization",
     "organizations:ListAccounts",
     "organizations:ListChildren",
     "organizations:ListOrganizationalUnitsForParent",
     "organizations:ListRoots"
    ],
    "Resource": "arn:aws:organizations::*:"
   },
   {
    "Sid": "OrganizationsAdminDataAccess",
    "Effect": "Allow",
    "Action": [
     "organizations:DeregisterDelegatedAdministrator",
     "organizations:RegisterDelegatedAdministrator",
     "organizations:ListDelegatedAdministrators",
     "organizations:EnableAWSServiceAccess",
     "organizations:DisableAWSServiceAccess"
    ],
    "Resource": "*",
    "Condition": {
     "StringEquals": {
      "organizations:ServicePrincipal": [
       "devops-guru.amazonaws.com"
      ]
     }
    }
   }
  ]
}
```

Utilisation de rôles liés à un service pour Guru DevOps

Amazon DevOps Guru utilise des AWS Identity and Access Management rôles liés à un service (IAM). Un rôle lié à un service est un type unique de rôle IAM directement lié à Guru. DevOps Les rôles liés au service sont prédéfinis par DevOps Guru et incluent toutes les autorisations dont le service a besoin pour appeler AWS CloudTrail Amazon CloudWatch et AWS Organizations en votre nom. AWS CodeDeploy AWS X-Ray

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 associées à ses rôles liés aux services et, sauf indication contraire, seul DevOps Guru peut assumer ses rôles. Les autorisations définies comprennent la politique d'approbation et la politique d'autorisation. De plus, cette politique d'autorisation ne peut pas être attachée à une autre entité IAM.

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

Autorisations de rôle liées au service pour Guru DevOps

DevOpsGuru utilise le rôle lié au service nommé. `AWSServiceRoleForDevOpsGuru` Il s'agit d'une politique AWS gérée avec des autorisations limitées 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.

```
{
 "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 le AWS Management Console, le ou l' 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

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

DevOpsGuru ne vous autorise pas à modifier le rôle `AWSServiceRoleForDevOpsGuru` lié au service. Une fois que vous avez créé un rôle lié à un service, vous ne pouvez pas changer le nom du rôle, car plusieurs entités peuvent faire référence à ce rôle. Néanmoins, vous pouvez modifier la

description du rôle à l'aide d'IAM. Pour plus d'informations, consultez Modification d'un rôle lié à un service dans le Guide de l'utilisateur IAM.

Supprimer un rôle lié à un service pour 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. Toutefois, 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 risque d'échouer. Si cela se produit, patientez quelques minutes et réessayez.

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

Utilisez la console IAM, le AWS CLI, ou l' AWS API pour supprimer le rôle lié au `AWSServiceRoleForDevOpsGuru` service. Pour plus d'informations, consultez Suppression d'un rôle lié à un service dans le Guide de l'utilisateur IAM.

Référence des autorisations Amazon DevOps Guru

Vous pouvez utiliser des clés AWS de condition larges dans les politiques de votre DevOps Guru pour exprimer des conditions. Pour obtenir une liste, reportez-vous à la section Référence des éléments de politique IAM JSON 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 gourou et `devops-guru:List*` spécifie toutes les actions du DevOps gourou qui commencent par le mot`List`. L'exemple suivant fait référence à tous les insights dotés d'un identifiant unique universel (UUID) commençant 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'autorisation 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`

Nécessaire pour renvoyer une 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 AWS CloudFormation piles utilisées pour spécifier les AWS ressources de votre compte 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`

Nécessaire pour renvoyer la liste des AWS CloudFormation piles utilisées pour spécifier les AWS ressources de votre compte 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`

Nécessaire pour renvoyer une liste d'informations dans votre AWS compte. Vous pouvez spécifier les informations 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`

Nécessaire pour renvoyer une liste d'informations dans votre AWS compte. Vous pouvez spécifier les informations 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 détails d'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 les événements renvoyés.

Ressource : *

`ListRecommendations`

Action : `devops-guru:ListRecommendations`

Obligatoire pour renvoyer une liste des recommandations d'un aperçu spécifié. Chaque recommandation inclut 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 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 AWS 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 aperçu OpsItem pour chaque information générée.

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 aperçu OpsItem pour chaque information générée.

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 aux sujets Amazon SNS appartenant à un autre AWS compte.

Pour que DevOps Guru envoie des notifications à une rubrique Amazon SNS appartenant à un autre compte, vous devez associer à cette rubrique Amazon SNS une politique autorisant Guru à DevOps lui envoyer des notifications. Si vous configurez DevOps Guru pour envoyer des notifications aux sujets Amazon SNS détenus par le même compte que celui 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 Guru. DevOps Vous pouvez également mettre à jour votre politique Amazon SNS à l'aide d'un canal de notification afin de la sécuriser davantage.

> **Note**
>
> DevOpsGuru ne prend actuellement en charge que l'accès entre comptes 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 lorsque vous

utilisez 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'identifiant de compte du propriétaire du sujet, *`topic-sender-account-id`*de l'identifiant de compte de l'utilisateur qui a configuré DevOps Guru et *`devops-guru-role`*du rôle IAM de l'utilisateur individuel concerné. Vous devez remplacer les valeurs appropriées par *`region-id`* (par exemple,`us-west-2`), et. *`my-topic-name`*

```
{
    "Version": "2012-10-17",
    "Statement": [{
            "Sid": "EnableDevOpsGuruServicePrincipal",
            "Action": "sns:Publish",
            "Effect": "Allow",
            "Resource": "arn:aws:sns:region-id:topic-owner-account-id:my-topic-name",
            "Principal": {
                "Service": "region-id.devops-guru.amazonaws.com"
            },
            "Condition": {
                "StringEquals": {
                    "AWS:SourceAccount": "topic-sender-account-id"
                }
            }
        },
        {
            "Sid": "EnableAccountPrincipal",
            "Action": "sns:Publish",
            "Effect": "Allow",
            "Resource": "arn:aws:sns:region-id:topic-owner-account-id:my-topic-name",
            "Principal": {
                "AWS": ["arn:aws:iam::topic-sender-account-id:role/devops-guru-role"]
            }
        }
```

```
    ]
}
```

Ajouter des autorisations en tant qu'utilisateur IAM

Pour utiliser une rubrique Amazon SNS depuis 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'identifiant de compte du propriétaire du sujet, *`topic-sender-account-id`*de l'identifiant 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 tels que les 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.

```
{
    "Version": "2012-10-17",
    "Statement": [{
            "Sid": "EnableDevOpsGuruServicePrincipal",
            "Action": "sns:Publish",
            "Effect": "Allow",
            "Resource": "arn:aws:sns:region-id:topic-owner-account-id:my-topic-name",
            "Principal": {
                "Service": "region-id.devops-guru.amazonaws.com"
            },
            "Condition": {
                "StringEquals": {
                    "AWS:SourceAccount": "topic-sender-account-id"
                }
            }
        },
        {
            "Sid": "EnableAccountPrincipal",
```

```
            "Action": "sns:Publish",
            "Effect": "Allow",
            "Resource": "arn:aws:sns:region-id:topic-owner-account-id:my-topic-name",
            "Principal": {
                "AWS": ["arn:aws:iam::topic-sender-account-id:user/devops-guru-user-
name"]
            }
        }
    ]
}
```

Ajouter une rubrique Amazon SNS depuis un autre compte

Après avoir configuré les autorisations pour un sujet Amazon SNS dans un autre compte, vous pouvez ajouter ce sujet Amazon SNS à DevOps vos paramètres de notification 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 d'un autre compte.
- Lorsque vous utilisez l' AWS CLI opération add-notification-channel, vous devez spécifier l'`TopicArn`intérieur de l'`NotificationChannelConfig`objet.

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 sélectionnez 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 attachant 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 dans le compte à partir duquel 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 du canal 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 en utilisant l'identifiant du propriétaire du sujet 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'identifiant de chaîne 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.

```
{
     "Version": "2012-10-17",
     "Statement": [{
           "Sid": "DevOpsGuruTopicPermissions",
           "Effect": "Allow",
           "Action": [
                 "sns:CreateTopic",
                 "sns:GetTopicAttributes",
                 "sns:SetTopicAttributes",
                 "sns:Publish"
           ],
           "Resource": "arn:aws:sns:region-id:account-id:my-topic-name"
     }]
}
```

Autorisations pour les AWS KMS rubriques Amazon SNS chiffrées

La rubrique Amazon SNS que vous spécifiez est peut-être chiffrée par. AWS Key Management Service Pour permettre à DevOps Guru de travailler avec des sujets chiffrés, vous devez d'abord créer une, AWS KMS key puis ajouter l'instruction suivante à la politique de la clé KMS. Pour plus

d'informations, consultez les sections Chiffrement des messages publiés sur Amazon SNS avec AWS KMS, Identifiants clés KeyId () dans AWS KMS le guide de l'utilisateur et chiffrement des données dans le guide du développeur Amazon Simple Notification Service.

```
{
  "Version": "2012-10-17",
  "Id": "your-kms-key-policy",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "region-id.devops-guru.amazonaws.com"
      },
      "Action": [
        "kms:GenerateDataKey*",
        "kms:Decrypt"
      ],
      "Resource": "*"
    }
  ]
}
```

> **Note**
>
> DevOpsGuru prend actuellement en charge les sujets cryptés à utiliser dans 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 à accéder aux ressources de mon DevOps Guru

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

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

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 AWS l'extérieur du AWS Management Console. La manière d'accorder un accès programmatique dépend du type d'utilisateur qui y accède AWS.

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

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

Quel utilisateur a besoin d'un accès programmatique ?	Pour	Par
		Authentification IAM Identity Center dans le Guide de référence AWS des SDK 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 d'informations d'identification temporaires avec AWS les ressources du Guide de l'utilisateur IAM.
IAM	(Non recommandé) Utilisez des informations d'identification à long terme 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 le AWS CLI, voir Authentification à l'aide des informations d'identification utilisateur IAM dans le Guide de l'AWS Command Line Interface utilisateur. • Pour les AWS SDK et les outils, voir Authentifier à l'aide d'informations d'identification à long terme dans le Guide de AWS référence des SDK 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, un utilisateur doit disposer des autorisations nécessaires pour transmettre le rôle au service.

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

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

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

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

Je souhaite autoriser des personnes extérieures à mon AWS compte à accéder aux ressources de mon 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 en savoir plus, consultez les éléments suivants :

- Pour savoir si DevOps Guru prend en charge ces fonctionnalités, consultezComment Amazon DevOps Guru travaille avec IAM.
- Pour savoir comment fournir l'accès à vos ressources sur celles Comptes AWS que vous possédez, consultez la section Fournir l'accès à un utilisateur IAM dans un autre utilisateur Compte AWS que vous possédez dans le Guide de l'utilisateur IAM.

- Pour savoir comment fournir l'accès à vos ressources à des tiers Comptes AWS, consultez la section Fournir un accès à des ressources Comptes AWS détenues par des tiers dans le guide de l'utilisateur IAM.
- Pour savoir comment fournir un accès par le biais de la fédération d'identité, consultez Fournir un accès à des utilisateurs authentifiés en externe (fédération d'identité) dans le Guide de l'utilisateur IAM.
- Pour découvrir quelle est la différence entre l'utilisation des rôles et l'utilisation des politiques basées sur les ressources pour l'accès entre comptes, consultez Différence entre les rôles IAM et les politiques basées sur les ressources dans le Guide de l'utilisateur IAM.

DevOpsGuru de l'enregistrement et de la 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 un problème et prendre des mesures automatiques le cas échéant :

- Amazon CloudWatch surveille vos AWS ressources et les applications que vous utilisez AWS en temps réel. Vous pouvez collecter et suivre les métriques, créer des tableaux de bord personnalisés, et définir des alarmes qui vous informent ou prennent des mesures lorsqu'une métrique spécifique atteint un seuil que vous spécifiez. Par exemple, vous pouvez CloudWatch suivre l'utilisation du processeur ou d'autres indicateurs de vos instances Amazon EC2 et lancer automatiquement de nouvelles instances en cas de besoin. 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 compte de votre AWS compte et envoie les fichiers journaux dans un compartiment Amazon S3 que vous spécifiez. Vous pouvez identifier les utilisateurs et les comptes 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 l'utilisation de DevOps Guru CloudWatch, qui collecte les données brutes et les traite en métriques 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 indicateurs pour obtenir des informations et les indicateurs relatifs à votre utilisation de DevOps Guru. Vous pouvez être attentif à la création d'un grand nombre de solutions `Insights` pour vous aider à déterminer si vos solutions opérationnelles présentent un comportement anormal. Vous pouvez également surveiller votre utilisation de DevOps Guru pour vous aider à suivre vos coûts.

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

Rubriques

- Métriques Insight
- DevOpsStatistiques d'utilisation de Guru

Métriques Insight

Vous pouvez l'utiliser CloudWatch pour suivre une métrique afin de savoir combien d'informations sont 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`

Métrique	Description
	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` •

Métrique	Description
	SearchInsights • DescribeInsight • DescribeAnomaly Dimensions valides : ServiceClass,Type, Resource Statistiques valides : nombre d'échantillons, somme Unités : nombre

Les dimensions suivantes sont prises en charge pour les métriques 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 estDevOps-Guru .
Class	Il s'agit de la classe de la ressource qui est suivie. DevOpsGuru utilise cette dimension avec la valeurNone.
Type	Il s'agit du type de ressource qui est suivi. DevOpsGuru utilise cette dimension avec la valeurAPI.
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 des appels depuis la console DevOps Guru et des appels de code vers les opérations de l'API DevOps Guru. Si vous créez un suivi, 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 dans la CloudTrail console dans Historique des événements. À l'aide des informations collectées par CloudTrail, vous pouvez déterminer la demande qui a été faite 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 le gourou 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 dans votre AWS compte. Pour plus d'informations, consultez la section Affichage des événements avec l'historique des CloudTrail événements.

Pour un enregistrement continu des événements de votre AWS compte, y compris ceux de DevOps Guru, créez un parcours. Un suivi permet CloudTrail de fournir 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 détail les données d'événements collectées dans les CloudTrail journaux et agir en conséquence. Pour plus d'informations, consultez les ressources suivantes :

- Présentation de la création d'un 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 l'enregistrement de toutes ses actions sous forme d'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 plus d'informations, consultez l'élément CloudTrail UserIdentity.

Comprendre les entrées du fichier journal DevOps Guru

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

L'exemple suivant montre une entrée de CloudTrail journal illustrant l'`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 Actions dans le manuel Amazon DevOps Guru API Reference.

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 PrivateLinkune technologie qui vous permet d'accéder en privé aux API DevOps Guru sans passerelle Internet, appareil 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 la section Interface VPC endpoints (AWS PrivateLink) dans le guide de l'utilisateur Amazon VPC.

Considérations relatives aux points de DevOps terminaison VPC Guru

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 permet d'appeler 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-guru

Si vous activez le DNS privé pour le point de terminaison, vous pouvez envoyer des demandes 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 Guru DevOps

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

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

Sécurité de l'infrastructure dans 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 sur la manière dont AWS l'infrastructure est protégée, consultez la section Sécurité du AWS cloud. Pour concevoir votre AWS environnement en utilisant les meilleures pratiques en matière de sécurité de l'infrastructure, consultez la section Protection de l'infrastructure dans le cadre AWS bien architecturé du pilier de sécurité.

Vous utilisez des appels d'API AWS publiés pour accéder à 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.
- Ses suites de chiffrement PFS (Perfect Forward Secrecy) comme DHE (Ephemeral Diffie-Hellman) ou ECDHE (Elliptic Curve Ephemeral Diffie-Hellman). La plupart des systèmes modernes tels que Java 7 et les versions ultérieures prennent en charge ces modes.

En outre, les demandes doivent être signées à l'aide d'un ID de clé d'accès et d'une clé d'accès secrète associée à un principal IAM. Vous pouvez également utiliser AWS Security Token Service (AWS STS) pour générer des informations d'identification de sécurité temporaires et signer les demandes.

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

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

Quotas et limites pour AmazonDevOpsGuru

Le tableau suivant répertorie le quota actuel sur AmazonDevOpsGourou. Ce quota est pour chaque personne prise en chargeAWSRégion pour chaqueAWScompte.

Notifications

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

Piles AWS CloudFormation

Nombre maximum deAWS CloudFormationpiles que vous pouvez spécifier	1 000

DevOpsLimites de surveillance des ressources de 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 le neufDevOpsComptes Guru créés le 29 juin 2023 ou après cette date, et pour les comptes existants actifs à la même date et comportant moins de 100 files d'attente Amazon SQS.

**Pour demander une modification de cette limite, contactezAWS Supportàhttps://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 de 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 dansDevOpsGuru, à l'aide duAWS CLI, la console API Gateway ou l'API REST d'API Gateway et ses kits de développement logiciel.

Pour une liste de tousDevOpsAPI Guru, voirAmazonDevOpsActions du gourou.

Quota par défaut	Peut être augmenté	
20 requêtes par seconde par compte	Oui	

AmazonDevOpsHistorique du document Guru

Le tableau suivant décrit la documentation de cette version deDevOpsGourou.

- 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 à la liste des abonnements ont été ajoutés au`AmazonDevOpsGuruConsoleFullAccess` politique. L'accès à la liste des abonnements a également été ajouté au`AmazonDevOpsGuruReadOnlyAccess` politique. Pour plus d'informations, voirPolitiques basées sur l'identité pour AmazonDevOpsGuru.	9 août 2023
Clés de chiffrement gérées par le client	DevOpsGuru prend désormais en charge le chiffrement avec des clés gérées par le client à l'aide deAWS KMS. Pour plus d'informations, voirProtection des données dansDevOpsGuru.	5 juillet 2023
DevOpsGuru pour RDS est compatible avec RDS PostgreSQL	DevOpsGuru for RDS peut détecter les problèmes de performance et d'autres informations dans les bases	30 mars 2023

	de données PostgreSQL. Pour plus d'informations, voirLes avantages deDevOpsGuru pour RDS.	
DevOpsGuru pour RDS permet d'obtenir des informations proactives	DevOpsGuru for RDS publie des informations proactives avec 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, voirTravailler avec des anomalies dansDevOpsGuru pour RDS.	28 février 2023
Page de ressources analysées	Une nouvelle page dansDevOpsLa console Guru répertorie les ressources de votre compte qui sont analysées parDevOpsGourou. Pour plus d'informations, voirAffichage des ressources analysées parDevOpsGuru.	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 sévérité et certains événements. Pour plus d'informations, voirMise à jour des configurations de notification Amazon Amazon SNS.	30 septembre 2022

Ajout de l'analyse des anomalies aux politiques gérées	AWSpolitiques gérées pourDevOpsGuru a été mis à jour dans la console IAM pour permettre l'accès auCloudWatchaction`FilterLogEvents` . Pour plus d'informations, voirDevOpsMises à jour de GuruAWSpolitiques gérées et rôle lié à un service.	30 août 2022
Analyse des anomalies du journal ajoutée	Vous pouvez consulter des informations détaillées sur les groupes de journaux liés aux informations dansDevOpsConsole Guru. Un rôle étendu lié aux services est également disponible pour décrireCloudWatchjournaux et flux. Pour plus d'informations, voirComprendre les informations contenues dans leDevOpsConsole GuruetDevOpsMises à jour de GuruAWSpolitiques gérées et rôle lié à un service.	12 juillet 2022
CodeGuruIntégration de profileurs	DevOpsGuru s'intègre désormais à AmazonCodeGuruProfileur avecEventBridgerègle gérée. Chaque événement entrant provenant deCodeGuruProfiler est un rapport d'anomalie proactif. Pour plus d'informations, voirIntégration avecCodeGuruProfileur.	7 mars 2022

Mises à jour des rôles liés au service et des politiques gérées	Politiques étendues disponibles dans la console IAM. Les modifications permettent tDevOpsGuru va favoriser une intégration améliorée avec Amazon Relational Database Service (Amazon RDS). Pour plus d'informations, voirUtilisation de rôles liés à un serviceetAWSpolitiques gérées (prédéfinies) pourDevOpsGuru.	21 décembre 2021
Nouvelle politique gérée ajoutée	Le`AmazonDevOpsGuruConsoleFullAccess` une politique a été ajoutée. Pour plus d'informations, voirPolitiques basées sur l'identité pour AmazonDevOpsGuru.	6 décembre 2021
Aide à la définition de votre application avecAWSbalises	Vous pouvez désormais utiliserAWSdes balises pour identifier les ressources que vous souhaitezDevOpsUn expert capable d'analyser, d'identifier les ressources de vos applications et de filtrer les informations dans la console. Pour plus d'informations, voirUtilisez des balises pour identifier les ressources dans vos applications.	1er décembre 2021

Mises à jour des rôles liés au service et des politiques gérées	Politiques étendues disponibles dans la console IAM. Les modifications permettent tDevOpsGuru va favoriser une intégration améliorée avec Amazon Relational Database Service (Amazon RDS). Pour plus d'informations, voirUtilisation de rôles liés à un serviceetAWSpolitiques gérées (prédéfinies) pourDevOpsGuru.	1er décembre 2021
Support d'Amazon RDS	DevOpsGuru fournit désormais des analyses et des informations complètes sur les ressources Amazon Relational Database Service (Amazon RDS) de votre application. Pour plus d'informations, voirTravailler avec des anomalies dansDevOpsGuru pour Amazon RDS.	1er décembre 2021
AmazonEventBridgeintégration	DevOpsGuru s'intègre désormais àEventBridgepour vous informer de certains événements relatifs à votreDevOpsDes idées de gourou. Pour plus d'informations, consultez Utilisation de EventBridge.	18 novembre 2021

AWSpolitique gérée ajoutée	NouveauAWSpolitique gérée ajoutée. Le`AmazonDevOpsGuruOrganizationsAccess` la politique permet d'accéder àDevOpsUn gourou au sein d'une organisation. Pour plus d'informations, voirpolitiques basées sur l'identité.	16 novembre 2021
Mise à jour de la politique des rôles liés à un service	Politique étendue disponible dans la console IAM. Le changement permetDevOpsGuru pour prendre en charge la vue multi-comptes. Pour plus d'informations, voirUtilisation de rôles liés à un service.	4 novembre 2021
Support multicompte	Vous pouvez désormais consulter les informations et les statistiques de plusieurs comptes de votre organisation. Pour plus d'informations, voirQu'est-ce qu'Amazon DevOpsGuru.	4 novembre 2021
Communiqué de disponibilité générale	AmazonDevOpsGuru est désormais disponible pour le grand public (GA).	4 mai 2021

Nouvelle rubrique	Vous pouvez désormais générer une estimation des coûts mensuels pourDevOps Un gourou pour analyser vos ressources. Pour plus d'informations, voirEstimez votre AmazonDevOpsCoûts du gourou.	27 avril 2021
Prise en charge des terminaux 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, voirDevOpsPoints de terminaison VPC Guru et interface (AWS PrivateLink).	15 avril 2021
Nouvelle rubrique	Un nouveau sujet sur la façon de surveillerDevOpsGuru avec AmazonCloudWatcha été ajouté. Pour plus d'informations, voirSurveillanceDevOps Guru avec AmazonCloudWatch.	11 décembre 2020
Version préliminaire	Il s'agit de la version préliminaire duAmazonDevOpsGuide de l'utilisateur de Guru.	1er décembre 2020

Glossaire AWS

Pour connaître la terminologie la plus récente d'AWS, consultez le Glossaire AWS dans la Référence Glossaire AWS.

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