Guide de mise en œuvre

Découverte de la charge de travail sur AWS

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

Découverte de la charge de travail sur AWS: Guide de mise en œuvre

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

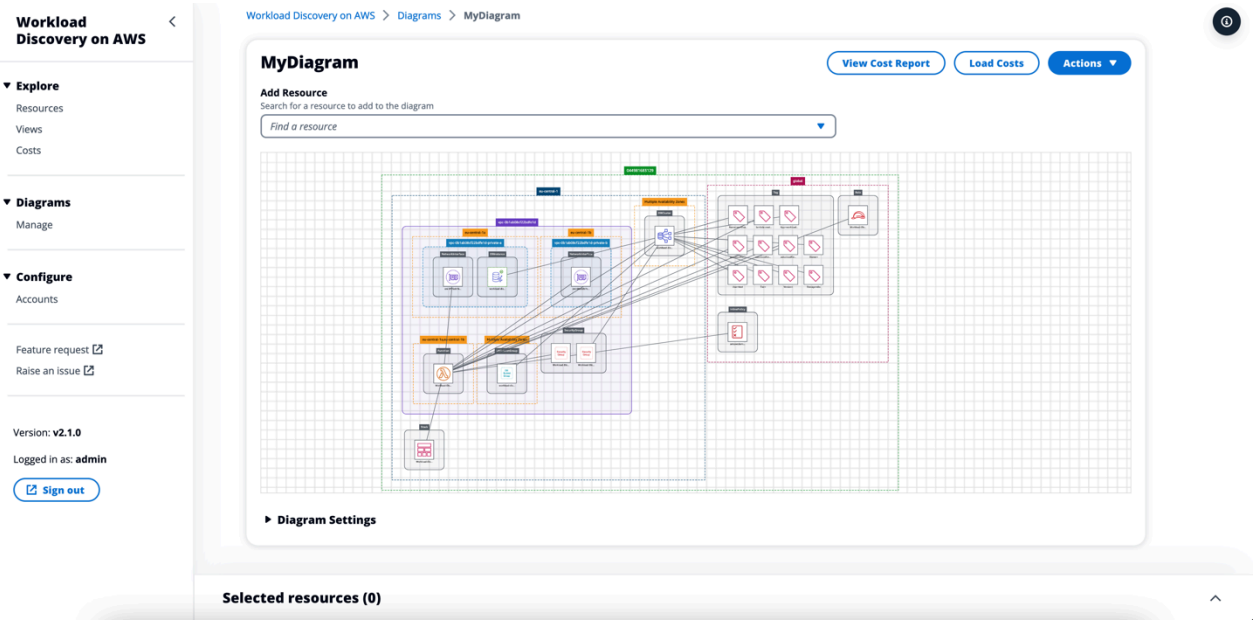
Les marques commerciales et la présentation commerciale d’Amazon ne peuvent pas être utilisées en relation avec un produit ou un service extérieur à Amazon, d’une manière susceptible d’entraîner une confusion chez les clients, ou d’une manière qui dénigre ou discrédite Amazon. Toutes les autres marques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

Table of Contents

Déployez un outil de visualisation qui génère automatiquement des diagrammes d'architecture des charges de travail du cloud AWS

La surveillance de vos charges de travail dans le cloud Amazon Web Services (AWS) est essentielle au maintien de la santé et de l'efficacité opérationnelles. Cependant, le suivi des ressources AWS et des relations entre elles peut s'avérer difficile. Workload Discovery sur AWS est un outil de visualisation qui génère automatiquement des diagrammes d'architecture de votre charge de travail sur AWS. Vous pouvez utiliser cette solution pour créer, personnaliser et partager des visualisations détaillées de la charge de travail basées sur les données en direct d'AWS.

Cette solution fonctionne en tenant à jour un inventaire des ressources AWS sur l'ensemble de vos comptes et de vos régions, en cartographiant les relations entre elles et en les affichant dans une interface utilisateur Web (interface utilisateur Web). Lorsque vous modifiez une ressource, Workload Discovery sur AWS vous fait gagner du temps en fournissant un lien vers la ressource dans l'AWS Management Console.



Exemple de schéma d'architecture généré par Workload Discovery sur AWS

Ce guide de mise en œuvre décrit les considérations architecturales et les étapes de configuration pour déployer Workload Discovery sur AWS dans le cloud AWS. Il inclut des liens vers un CloudFormation modèle AWS qui lance et configure les services AWS nécessaires au déploiement de cette solution en utilisant les meilleures pratiques d'AWS en matière de sécurité et de disponibilité.

Le public visé par la mise en œuvre de la solution Workload Discovery sur AWS dans leur environnement comprend les architectes de solutions, les décideurs commerciaux, les DevOps ingénieurs, les scientifiques des données et les professionnels du cloud.

Utilisez ce tableau de navigation pour trouver rapidement les réponses aux questions suivantes :

Si tu veux...	Lisez.
Connaissez le coût de fonctionnement de cette solution. Le coût d'exécution de cette solution dans la région de l'est des États-Unis (Virginie du Nord) est estimé à 425,19 dollars américains par mois.	Coût
Comprenez les considérations de sécurité liées à cette solution.	Sécurité
Sachez comment planifier les quotas pour cette solution.	Quotas
Découvrez quelles régions AWS prennent en charge cette solution.	Régions AWS prises en charge
Consultez ou téléchargez le CloudFormation modèle AWS inclus dans cette solution pour déployer automatiquement les ressources d'infrastructure (la « pile ») de cette solution.	CloudFormation Modèle AWS
Accédez au code source.	GitHub référentiel

Fonctionnalités et avantages

Workload Discovery sur AWS fournit les fonctionnalités suivantes :

Créez des diagrammes d'architecture à l'aide de données en temps quasi réel

Workload Discovery sur AWS analyse vos comptes toutes les 15 minutes pour s'assurer que les diagrammes que vous créez sont une représentation précise et actuelle de vos charges de travail.

Afficher les ressources de plusieurs comptes et régions en un seul endroit

La solution gère un inventaire des ressources AWS de vos comptes et régions AWS dans une base de données graphique centralisée, ce qui vous permet d'explorer plusieurs comptes et régions ainsi que leurs relations entre eux dans une seule interface utilisateur.

Intégration avec AWS Organizations

Lors du déploiement de la solution avec AWS Organizations, Workload Discovery on AWS découvre automatiquement toutes les ressources prises en charge dans votre organisation. Dans cette configuration, il n'est pas nécessaire de gérer directement le déploiement de CloudFormation modèles spécifiques aux comptes pour rendre ces comptes disponibles à des fins de découverte.

Collectez les données sur les coûts pour l'ensemble de vos charges de travail

Lorsqu'elle est activée, la fonction de coût vous permet de rechercher les ressources de votre compte par coût et d'ajouter les ressources que vous trouvez à un diagramme. Vous pouvez également ajouter des données de coûts à des diagrammes déjà existants.

Exporter vers diagrams.net (anciennement draw.io)

Workload Discovery sur AWS peut exporter vos diagrammes afin que vous puissiez les annoter davantage à l'aide de ce logiciel de dessin tiers.

Intégration avec AWS Service Catalog AppRegistry et Application Manager, une fonctionnalité d'AWS Systems Manager

Cette solution inclut une AppRegistry ressource Service Catalog pour enregistrer le CloudFormation modèle de la solution et ses ressources sous-jacentes en tant qu'application dans Service Catalog AppRegistry et Application Manager. Grâce à cette intégration, vous pouvez gérer de manière centralisée les ressources de la solution et activer les actions de recherche, de reporting et de gestion des applications.

Cas d’utilisation

Examens de conception et de sécurité

Utilisez cette solution pour générer des diagrammes d'architecture afin de valider que la mise en œuvre d'une charge de travail correspond à la conception proposée.

Explorez et documentez les charges de travail existantes

Créez des diagrammes d'architecture pour explorer les charges de travail pour lesquelles il existe peu de documentation ou qui ont été déployées manuellement sans infrastructure sous forme de code.

Visualisez les coûts

Générez un rapport de coûts pour vos diagrammes d'architecture contenant une vue d'ensemble du coût estimé.

Concepts et définitions

Cette section décrit les concepts clés et définit la terminologie spécifique à cette solution :

ressource

Une ressource AWS, telle qu'un bucket Amazon Simple Storage Service (Amazon S3) ou une fonction AWS Lambda.

relation

Lien entre deux ressources, telles qu'un rôle AWS Identity and Access Management (IAM) et une fonction AWS Lambda associée.

type de ressource

Catégorie de classification d'une ressource. Respecte toujours la convention de CloudFormation dénomination, telle que`AWS::Lambda::Function`.

découverte

Processus lancé par la solution pour cartographier les ressources et leurs relations dans vos comptes et régions AWS.

mode de découverte de compte

Méthode permettant de découvrir les comptes et de les ajouter à la solution : soit autogérée via l'interface utilisateur Workload Discovery on AWS, soit déléguée à AWS Organizations.

> **Note**
>
> Pour une référence générale des termes AWS, consultez le glossaire AWS.

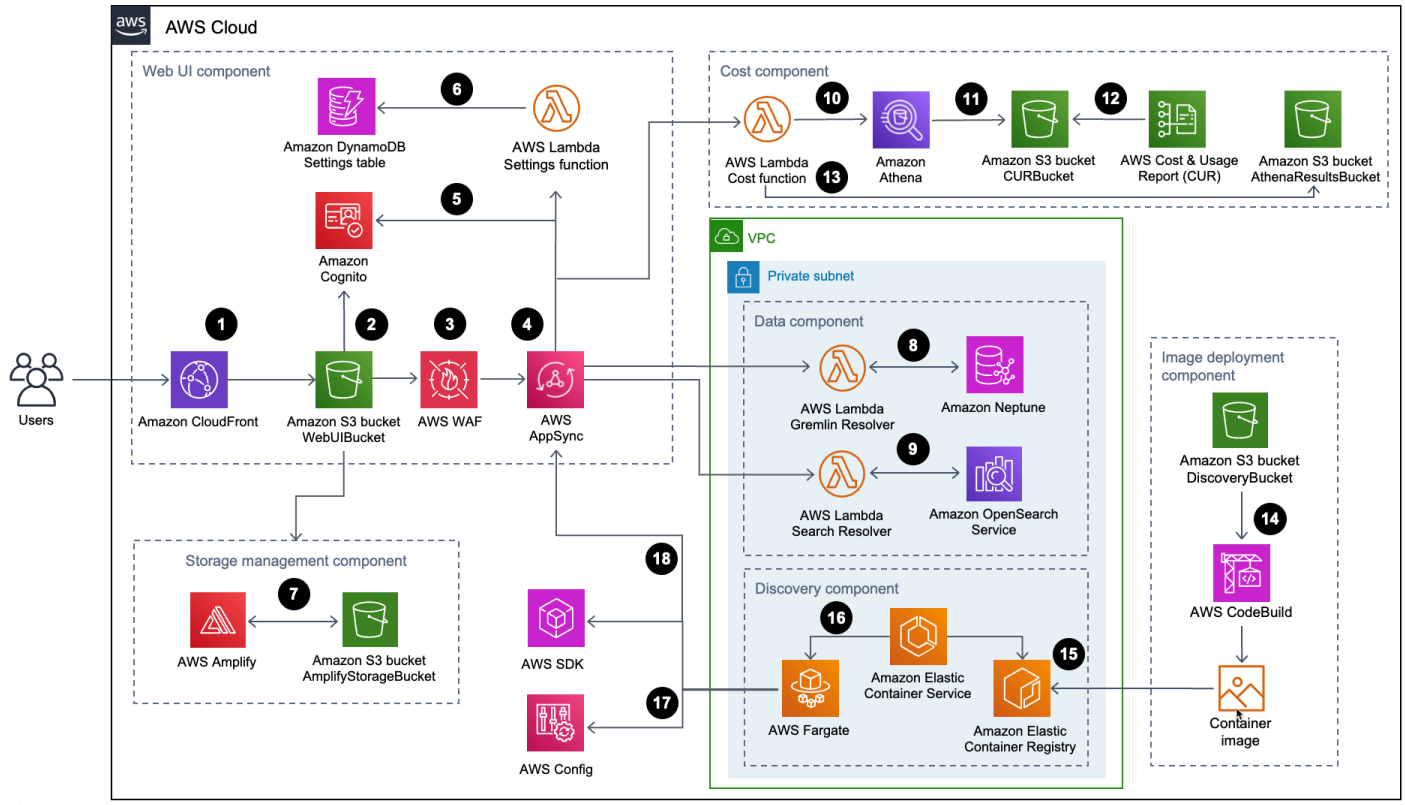
Présentation de l’architecture

Cette section fournit un schéma d'architecture d'implémentation de référence pour les composants déployés avec cette solution.

Diagramme d'architecture

Le déploiement de cette solution avec les paramètres par défaut permet de créer l'environnement suivant dans le cloud AWS.

Découverte de la charge de travail sur l'architecture AWS



Le flux de processus de haut niveau pour les composants de solution déployés avec le CloudFormation modèle AWS est le suivant :

1. Le protocole HTTP Strict-Transport-Security (HSTS) ajoute des en-têtes de sécurité à chaque réponse de la distribution Amazon CloudFront.
2. Un compartiment Amazon Simple Storage Service (Amazon S3) héberge l'interface utilisateur Web, qui est distribuée avec Amazon CloudFront. Amazon Cognito authentifie l'accès des utilisateurs à l'interface utilisateur Web.

3. AWS WAF protège l' AppSync API contre les exploits et les robots courants susceptibles d'affecter la disponibilité, de compromettre la sécurité ou de consommer des ressources excessives.
4. Les AppSync points de terminaison AWS permettent au composant de l'interface utilisateur Web de demander des données sur les relations entre les ressources, de demander les coûts, d'importer de nouvelles régions AWS et de mettre à jour les préférences. AWS permet AppSync également au composant de découverte de stocker des données persistantes dans les bases de données de la solution.
5. AWS AppSync utilise des jetons Web JSON (JWTs) fournis par Amazon Cognito pour authentifier chaque demande.
6. La fonction `Settings` AWS Lambda conserve les régions importées et les autres configurations dans Amazon DynamoDB.
7. La solution déploie AWS Amplify et un compartiment Amazon S3 en tant que composant de gestion du stockage pour stocker les préférences des utilisateurs et les diagrammes d'architecture enregistrés.
8. Le composant de données utilise la fonction `Gremlin Resolver` AWS Lambda pour interroger et renvoyer des données depuis une base de données Amazon Neptune.
9. Le composant de données utilise la fonction `Search Resolver` Lambda pour interroger et conserver les données de ressources dans un domaine Amazon OpenSearch Service.
10. La fonction `Cost` Lambda utilise Amazon Athena pour interroger les rapports sur les coûts et l'utilisation d'AWS (AWS CUR) afin de fournir des données de coûts estimées à l'interface utilisateur Web.
11. Amazon Athena exécute des requêtes sur AWS CUR.
12. AWS CUR envoie les rapports au compartiment `CostAndUsageReportBucket` Amazon S3.
13. La fonction `Cost` Lambda stocke les résultats Amazon Athena dans le `AthenaResultsBucket` compartiment Amazon S3.
14. AWS CodeBuild crée l'image du conteneur du composant de découverte dans le composant de déploiement d'images.
15. Amazon Elastic Container Registry (Amazon ECR) contient une image Docker fournie par le composant de déploiement d'images.
16. Amazon Elastic Container Service (Amazon ECS) gère la tâche AWS Fargate et fournit la configuration requise pour exécuter la tâche. AWS Fargate exécute une tâche de conteneur toutes les 15 minutes pour actualiser les données d'inventaire et de ressources.

17 Les appels AWS Config et AWS SDK aident le composant de découverte à maintenir un inventaire des données de ressources provenant des régions importées, puis à stocker ses résultats dans le composant de données.

18 La tâche AWS Fargate conserve les résultats des appels AWS Config et AWS SDK dans une base de données Amazon Neptune et un domaine OpenSearch Amazon Service avec des appels d'API vers l'API. AppSync

Considérations relatives à la conception d'AWS Well-Architected

Cette solution utilise les meilleures pratiques de l'AWS Well-Architected Framework, qui aide les clients à concevoir et à exploiter des charges de travail fiables, sécurisées, efficaces et rentables dans le cloud.

Cette section décrit comment les principes de conception et les meilleures pratiques du Well-Architected Framework profitent à cette solution.

Excellence opérationnelle

Nous avons conçu cette solution en utilisant les principes et les meilleures pratiques du pilier de l'excellence opérationnelle au profit de cette solution.

- Ressources définies comme une infrastructure utilisant du code CloudFormation.
- La solution transmet des métriques à Amazon CloudWatch afin de garantir l'observabilité de l'infrastructure, des fonctions Lambda, des tâches Amazon ECS, des compartiments AWS S3 et des autres composants de la solution.

Sécurité

Nous avons conçu cette solution en utilisant les principes et les meilleures pratiques du pilier de sécurité au profit de cette solution.

- Amazon Cognito authentifie et autorise les utilisateurs de l'application d'interface utilisateur Web.
- Tous les rôles utilisés par la solution suivent le principe du moindre privilège d'accès. En d'autres termes, ils ne contiennent que les autorisations minimales requises pour que le service puisse fonctionner correctement.
- Les données au repos et en transit sont chiffrées à l'aide de clés stockées dans AWS Key Management Service (AWS KMS), un magasin de gestion de clés dédié.

- Les identifiants ont une courte durée d'expiration et sont soumis à une politique de mot de passe fort.
- Les directives GraphQL de AppSync sécurité d'AWS permettent de contrôler avec précision les opérations pouvant être invoquées par le frontend et le backend.
- La journalisation, le suivi et le versionnement sont activés le cas échéant.
- L'application automatique de correctifs (version mineure) et la création d'instantanés sont activées le cas échéant.
- L'accès au réseau est privé par défaut, les points de terminaison Amazon Virtual Private Cloud (Amazon VPC) étant activés lorsqu'ils sont disponibles.

Fiabilité

Nous avons conçu cette solution en utilisant les principes et les meilleures pratiques du pilier de fiabilité pour en tirer parti.

- La solution utilise les services sans serveur AWS dans la mesure du possible pour garantir une haute disponibilité et une restauration en cas de panne de service.
- Tous les traitements informatiques utilisent les fonctions Lambda ou Amazon ECS sur AWS Fargate.
- Tout le code personnalisé utilise le SDK AWS et les demandes sont limitées côté client pour éviter d'atteindre les quotas de débit d'API.

Efficacité des performances

Nous avons conçu cette solution en utilisant les principes et les meilleures pratiques du pilier de l'efficacité des performances pour tirer parti de cette solution.

- La solution utilise l'architecture sans serveur AWS dans la mesure du possible. Cela élimine la charge opérationnelle liée à la gestion des serveurs physiques.
- La solution peut être lancée dans n'importe quelle région prenant en charge les services AWS utilisés dans cette solution, tels que : AWS Lambda, Amazon Neptune, AppSync AWS, Amazon S3 et Amazon Cognito.
- Dans les régions prises en charge, Amazon Neptune sans serveur vous permet d'exécuter et de redimensionner instantanément les charges de travail graphiques, sans avoir à gérer ni à optimiser la capacité de la base de données.

- La solution utilise des services gérés dans l'ensemble afin de réduire la charge opérationnelle liée au provisionnement et à la gestion des ressources.

Optimisation des coûts

Nous avons conçu cette solution en utilisant les principes et les meilleures pratiques du pilier de l'optimisation des coûts pour tirer parti de cette solution.

- AWS ECS sur AWS Fargate utilise les fonctions Lambda exclusivement pour le calcul et facture uniquement en fonction de l'utilisation.
- Amazon DynamoDB adapte la capacité à la demande, de sorte que vous ne payez que pour la capacité que vous utilisez.

Durabilité

Nous avons conçu cette solution en utilisant les principes et les meilleures pratiques du pilier du développement durable au profit de cette solution.

- La solution utilise des services gérés et sans serveur dans la mesure du possible afin de minimiser l'impact environnemental des services principaux.

Détails de l'architecture

Cette section décrit les composants et les services AWS qui constituent cette solution ainsi que les détails de l'architecture sur la manière dont ces composants fonctionnent ensemble.

Mécanisme d’authentification

Workload Discovery sur AWS utilise un groupe d'utilisateurs Amazon Cognito pour l'interface utilisateur et l'authentification AWS AppSync . Une fois authentifié, Amazon Cognito fournit un jeton Web JSON (JWT) à l'interface utilisateur Web qui sera fourni avec toutes les demandes d'API suivantes. Si aucun JWT valide n'est fourni, la demande d'API échouera et renverra une réponse HTTP 403 Forbidden.

Ressources prises en charge

Pour obtenir la liste des types de ressources AWS que Workload Discovery sur AWS peut découvrir au sein de vos comptes et de vos régions, consultez la section Ressources prises en charge.

Découverte de la charge de travail sur la gestion des diagrammes d'architecture AWS

Vous pouvez enregistrer les diagrammes d'architecture Workload Discovery sur AWS à l'aide de l'interface utilisateur Web dans laquelle les opérations de création, de lecture, de mise à jour et de suppression (CRUD) peuvent être effectuées. L'API de stockage AWS Amplify permet à Workload Discovery sur AWS de stocker des diagrammes d'architecture dans un compartiment Amazon S3. Deux niveaux d'autorisations sont disponibles :

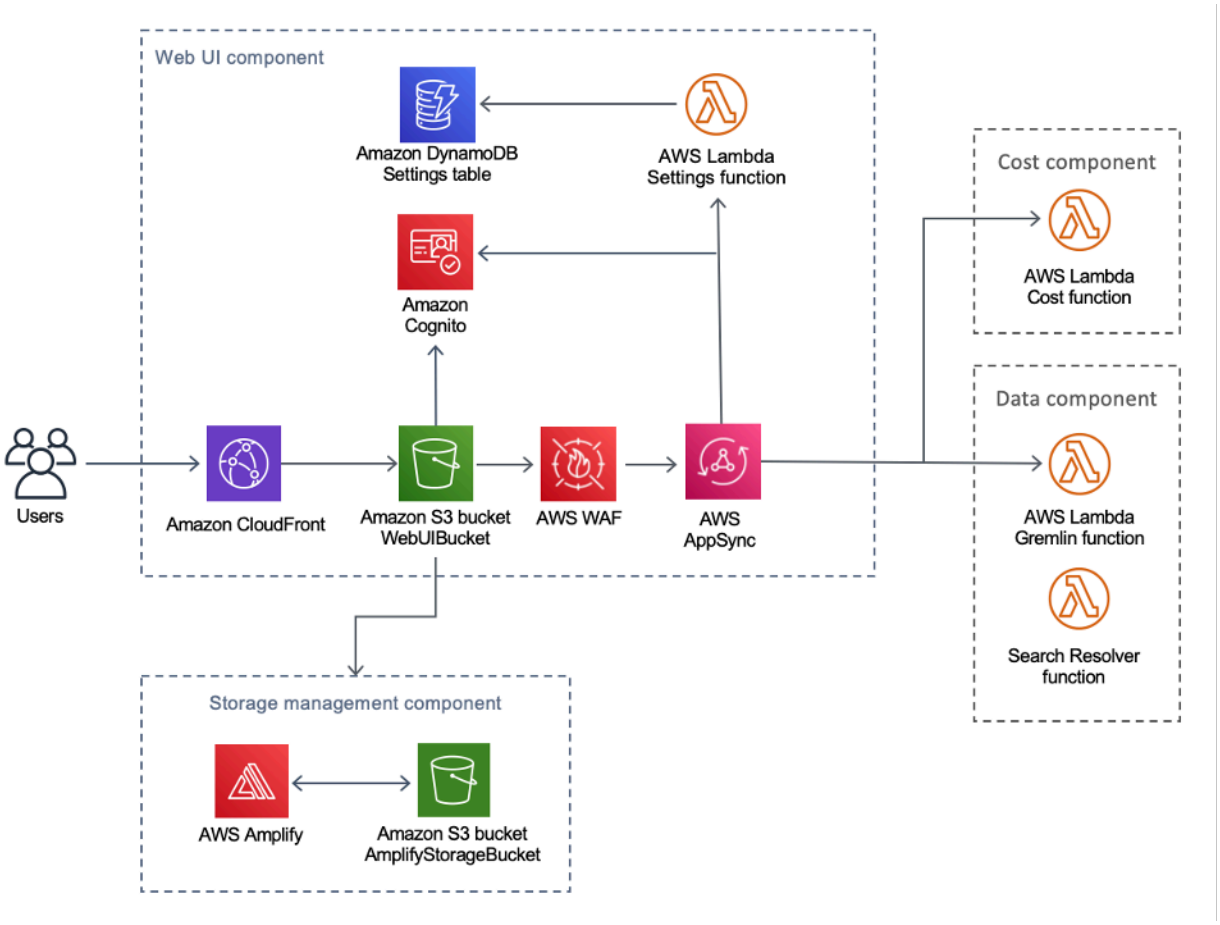
- Tous les utilisateurs : permet aux utilisateurs de Workload Discovery on AWS de voir les diagrammes d'architecture Workload Discovery on AWS dans le cadre de votre déploiement. Les utilisateurs peuvent télécharger et modifier ces diagrammes.
- Vous : permet à la découverte de la charge de travail sur les diagrammes d'architecture AWS d'être visible uniquement par le créateur. Les autres utilisateurs ne pourront pas les consulter.

Interface utilisateur Web et gestion du stockage

Nous avons développé l'interface utilisateur Web à l'aide de React. L'interface utilisateur Web fournit une console frontale permettant aux utilisateurs d'interagir avec Workload Discovery sur AWS.

Amazon CloudFront est configuré pour ajouter des en-têtes sécurisés à chaque requête HTTP envoyée à l'interface utilisateur Web. Cela fournit une couche de sécurité supplémentaire, protégeant contre les attaques telles que le cross-site scripting (XSS).

Découverte de la charge de travail sur l'interface utilisateur Web AWS et composants de gestion du stockage



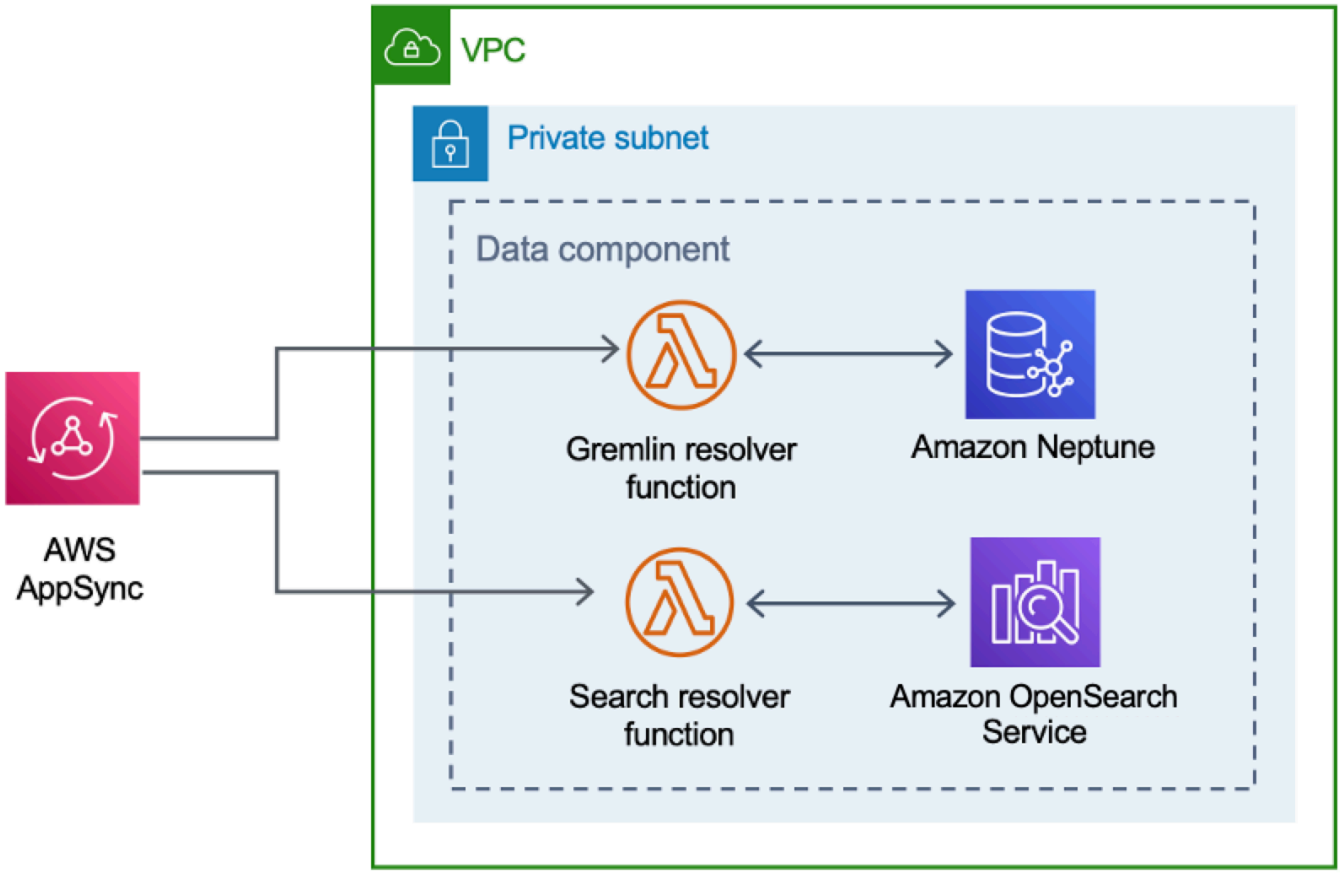
Les ressources de l'interface utilisateur Web sont hébergées dans le compartiment `WebUIBucket` Amazon S3 et distribuées par Amazon CloudFront. AWS Amplify fournit une couche d'abstraction pour simplifier les intégrations à AWS et AppSync Amazon S3.

Cette solution utilise AWS AppSync pour faciliter l'interaction avec les différentes configurations disponibles pour Workload Discovery sur AWS, notamment la gestion des régions importées. AWS

AppSync utilise la fonction `Settings` AWS Lambda pour traiter les demandes telles que l'importation d'un nouveau compte ou d'une nouvelle région.

Composant de données

Composant de données de découverte de la charge de travail sur AWS

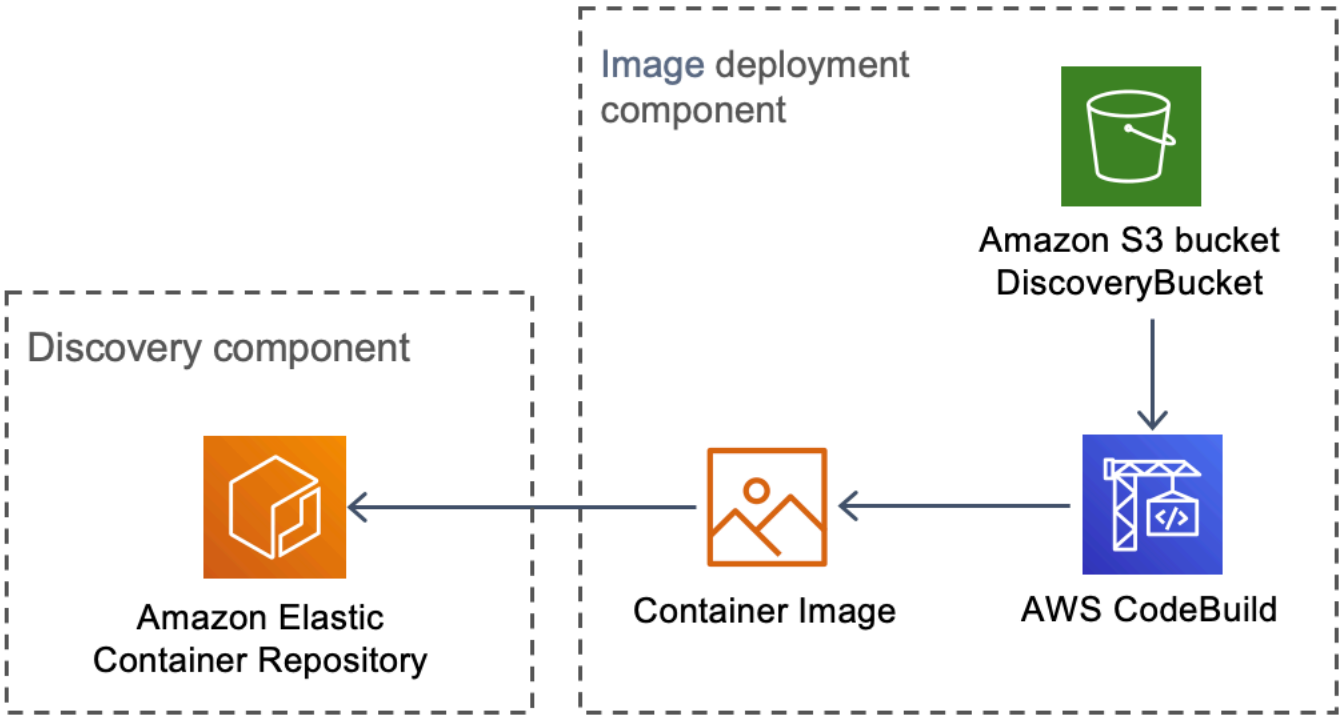


L'interface utilisateur Web envoie des requêtes à l' AppSync API, qui invoque les fonctions `Search Resolver` Lambda `Gremlin Resolver` ou les fonctions Lambda. Ces fonctions traitent les demandes et interrogent Amazon Neptune ou OpenSearch Service pour récupérer des données sur les ressources fournies. AWS prend AppSync également en charge les demandes de données relatives aux coûts estimés provenant du CUR AWS.

Le composant de découverte envoie des demandes à l' AppSync API pour lire et conserver les données dans les bases de données Amazon Neptune et OpenSearch Service. L'API reçoit les

demandes de la tâche AWS Fargate dans le composant de découverte. L'API est ensuite authentifiée à l'aide d'un rôle IAM qui donne accès aux bases de données.

Composant de déploiement d'images



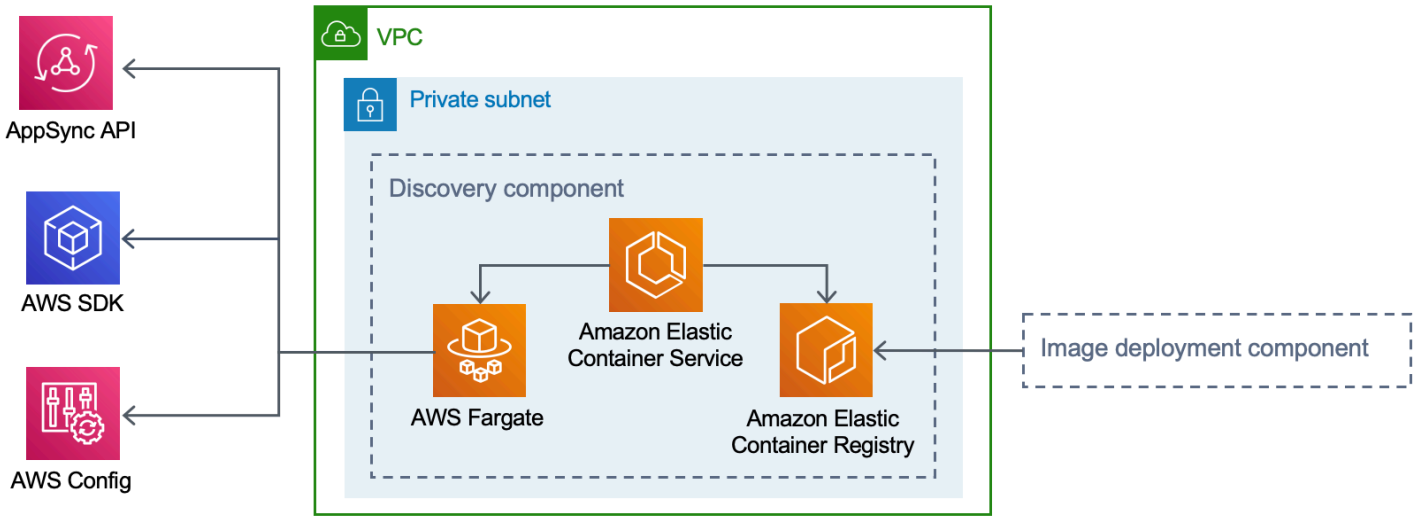
Composant de déploiement d'images Workload Discovery sur AWS

Le composant de déploiement d'image crée l'image de conteneur utilisée par le composant de découverte. Le `DiscoveryBucket` compartiment Amazon S3 héberge le code qui peut être téléchargé au moment du déploiement par une CodeBuild tâche AWS qui crée l'image du conteneur et la télécharge sur Amazon ECR.

Composant Discovery

Le composant de découverte est le principal élément de collecte de données de l'architecture Workload Discovery sur AWS. Il est chargé d'interroger AWS Config et d'effectuer des appels d'API de description afin de maintenir l'inventaire des ressources et leurs relations entre elles.

Composant de découverte de la charge de travail sur AWS



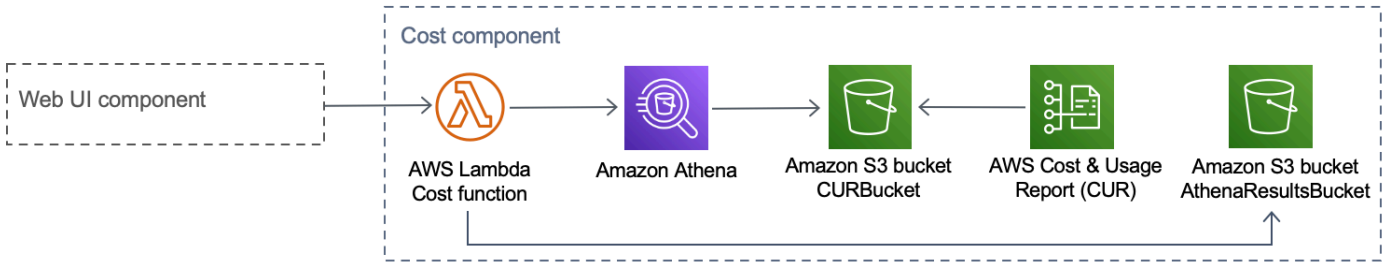
Cette solution configure Amazon ECS pour exécuter une tâche AWS Fargate à l'aide de l'image du conteneur téléchargée depuis Amazon ECR. La tâche AWS Fargate est planifiée pour être exécutée à intervalles de 15 minutes. Les données relatives aux relations entre les ressources collectées sont insérées dans une base de données de graphes Amazon Neptune et dans Amazon OpenSearch Service.

Le flux de travail du composant de découverte comprend les trois étapes suivantes :

1. Amazon ECS invoque une tâche AWS Fargate à intervalles de 15 minutes.
2. La tâche Fargate collecte des données sur les ressources à partir d'AWS Config, des appels de description d'API AWS et de la base de données Amazon Neptune.
3. La tâche Fargate calcule la différence entre le contenu de la base de données Amazon Neptune et ce qu'elle a reçu d'AWS Config et des appels de description.
4. La tâche Fargate envoie des demandes à AppSync l'API pour conserver les modifications apportées aux ressources et aux relations découvertes dans Amazon Neptune et Amazon Service. OpenSearch

Composante des coûts

Composant de coût relatif à la découverte de la charge de travail sur AWS



Vous pouvez créer un CUR AWS dans AWS Billing and Cost Management and Cost Management. Cela publie un fichier au format Parquet dans le compartiment `CostAndUsageReportBucket` Amazon S3. L'interface utilisateur Web envoie des requêtes au point de AppSync terminaison AWS qui invoque la fonction Cost Lambda. La fonction envoie des requêtes prédéfinies à Amazon Athena qui renvoient des informations sur les coûts estimés à partir d'AWS CUR.

En raison de la taille du CUR AWS, les réponses d'Amazon Athena peuvent être très importantes. La solution stocke les résultats dans le compartiment `AthenaResultsBucket` Amazon S3 et les pagine vers l'interface utilisateur Web. La politique de cycle de vie configurée pour ce compartiment supprime les éléments vieux de plus de sept jours.

Services AWS inclus dans cette solution

Service AWS	Description
AWS AppSync	Noyau. Cette solution permet AppSync de fournir une API GraphQL sans serveur que l'interface utilisateur Web consomme.
Amazon CloudFront	Noyau. Cette solution utilise CloudFront un compartiment Amazon S3 comme origine. Cela restreint l'accès au compartiment Amazon S3 afin qu'il ne soit pas accessible au public et empêche l'accès direct depuis le compartiment.
AWS Config	Noyau. La solution utilise AWS Config comme source de données principale pour les ressources et les relations qu'elle découvre.

Service AWS	Description
Amazon OpenSearch Service	Noyau. La solution utilise Amazon OpenSearch Service pour la surveillance des applications, l'analyse des journaux et l'observabilité.
Amazon DynamoDB	Noyau. Cette solution utilise DynamoDB pour stocker les données de configuration de la solution.
Amazon Elastic Container Service (ECS)	Noyau. Cette solution utilise Amazon ECS pour orchestrer l'exécution de la tâche qui découvre les ressources et les relations dans vos comptes AWS.
AWS Fargate	Noyau. Cette solution utilise AWS Fargate sur Amazon ECS comme couche de calcul pour la tâche de découverte.
AWS Lambda	Noyau. Cette solution utilise des fonctions Lambda sans serveur, avec des environnements d'exécution Node.js et Python, pour gérer les appels d'API.
Amazon Neptune	Noyau. Cette solution utilise Neptune comme banque de données principale pour les ressources et les relations découvertes par la solution.
Amazon Simple Storage Service	Noyau. Cette solution utilise Amazon S3 à des fins de stockage frontal et principal.

Service AWS	Description
Amazon CloudWatch	Soutenir. Cette solution permet CloudWatc h de collecter et de visualiser des journaux, des métriques et des données d'événements en temps réel dans des cas automatisés. En outre, vous pouvez surveiller l'utilisation des ressources et les problèmes de performance de la solution déployée.
AWS CodeBuild	Soutenir. Cette solution permet CodeBuild de créer le conteneur Docker qui contient le code de la tâche de découverte et de déployer les ressources du frontend sur Amazon S3.
Amazon Cognito	Soutenir. Cette solution utilise les groupes d'utilisateurs de Cognito pour authentifier et autoriser les utilisateurs à accéder à l'interface utilisateur Web de la solution.
AWS Systems Manager	Soutenir. Cette solution utilise AWS Systems Manager pour fournir une surveillance des ressources au niveau de l'application et une visualisation des opérations sur les ressources et des données de coûts.
Amazon Virtual Private Cloud	Soutenir. Cette solution utilise un VPC pour lancer Neptune et ses bases de données. OpenSearch
AWS WAF	Soutenir. Cette solution utilise AWS WAF pour protéger l' AppSync API contre les exploits courants et les robots susceptibles d'affecter la disponibilité, de compromettre la sécurité ou de consommer des ressources excessives.

Service AWS	Description
Amazon Athena	Facultatif. Cette solution utilise Athena pour interroger les rapports de coûts et d'utilisation si la fonctionnalité de coût est activée.

Planifiez votre déploiement

Cette section décrit la région, le coût, la sécurité et d'autres considérations avant le déploiement de la solution.

Régions AWS prises en charge

Cette solution utilise le service Amazon Cognito, qui n'est actuellement pas disponible dans toutes les régions AWS. Pour connaître la disponibilité la plus récente des services AWS par région, consultez la liste des services régionaux AWS.

Workload Discovery sur AWS est disponible dans les régions AWS suivantes :

Nom de la région	
USA Est (Virginie du Nord)	Canada (Centre)
USA Est (Ohio)	Europe (Londres)
USA Ouest (Oregon)	Europe (Francfort)
Asie-Pacifique (Mumbai)	Europe (Irlande)
Asie-Pacifique (Séoul)	Europe (Paris)
Asie-Pacifique (Singapour)	Europe (Stockholm)
Asie-Pacifique (Sydney)	Amérique du Sud (São Paulo)
Asie-Pacifique (Tokyo)	

La découverte de la charge de travail sur AWS n'est pas disponible dans les régions AWS suivantes :

Nom de la région	Service non disponible
AWS GovCloud (USA Est)	AWS AppSync
AWS GovCloud (ouest des États-Unis)	AWS AppSync

Nom de la région	Service non disponible
Chine (Beijing)	Amazon Cognito
Chine (Ningxia)	Amazon Cognito

Coût

Vous êtes responsable du coût des services AWS fournis lors de l'exécution de cette solution. À compter de cette révision, le coût d'exécution de cette solution à l'aide de l'option de déploiement à instance unique dans la région de l'est des États-Unis (Virginie du Nord) est d'environ 0,58 USD par heure ou 425,19 USD par mois.

> **Note**
>
> Le coût d'exécution de Workload Discovery sur AWS dans le cloud AWS dépend de la configuration de déploiement que vous choisissez. Les exemples suivants fournissent une ventilation des coûts pour les configurations de déploiement à instance unique et à instances multiples dans la région de l'est des États-Unis (Virginie du Nord). Les services AWS répertoriés dans les exemples de tableaux ci-dessous sont facturés sur une base mensuelle.

Nous vous recommandons de créer un budget via AWS Cost Explorer pour vous aider à gérer les coûts. Les prix sont susceptibles d'être modifiés. Pour plus de détails, consultez la page Web de tarification de chaque service AWS utilisé dans cette solution.

Exemples de tableaux de coûts

Option 1 : déploiement d'une instance unique (par défaut)

Lors du déploiement de cette solution à l'aide d'un CloudFormation modèle AWS, la modification du OpensearchMultiAzparamètre pour No déployer une seule instance pour le domaine OpenSearch Service et la modification du CreateNeptuneReplicaparamètre pour No déployer une instance unique pour le magasin de données Neptune. L'option de déploiement à instance unique est moins coûteuse, mais elle réduit la disponibilité de Workload Discovery sur AWS en cas de défaillance d'une zone de disponibilité.

Service AWS	Type d'instance	Coût horaire [USD]	Coût mensuel [USD]
Amazon Neptune	`db.r5.large`	0,348$	254,04$
Amazon OpenSearch Service	`m6g.large .search`	0,128$	93,44$
Amazon VPC (passerelle NAT)	N/A	$0.090	65,7$
AWS Config	N/A	0,003$ par ressource	0,003$ par ressource
Amazon ECS (tâche AWS Fargate)	N/A	0,02$	12,01$
Total		0,586$	425,19$

Option 2 : déploiement de plusieurs instances

Lorsque vous déployez cette solution à l'aide d'un CloudFormation modèle AWS, modifiez le OpensearchMultiAzparamètre pour `Yes` déployer deux instances dans deux zones de disponibilité pour le domaine OpenSearch Service, et modifiez le CreateNeptuneReplicaparamètre pour `Yes` déployer deux instances dans deux zones de disponibilité pour le magasin de données Neptune. L'option de déploiement d'instances multiples coûtera plus cher à exécuter, mais elle augmente la disponibilité de Workload Discovery sur AWS en cas de défaillance d'une zone de disponibilité.

Service AWS	Type d'instance	Coût horaire	Coût mensuel [USD]
Amazon Neptune	`db.r5.large`	0,696$	508,08$
Amazon OpenSearch Service	`m6g.large .search`	0,256$	186,88$
Amazon VPC (passerelle NAT)	N/A	$0.090	65,7$
AWS Config	N/A	0,003$ par ressource	0,003$ par ressource

Service AWS	Type d'instance	Coût horaire	Coût mensuel [USD]
Amazon ECS (tâche AWS Fargate)	N/A	0,02$	12,01$
Total		1,062$	772,67$

- Votre coût final dépend du nombre de ressources détectées par AWS Config. 0,003 USD par élément de ressource enregistré seront engagés en plus du montant indiqué dans le tableau.

> **Important**
>
> Le coût d'Amazon Neptune et d'Amazon OpenSearch Service varie en fonction du type d'instance que vous sélectionnez.

Sécurité

Lorsque vous créez des systèmes sur l'infrastructure AWS, les responsabilités en matière de sécurité sont partagées entre vous et AWS. Ce modèle de responsabilité partagée réduit votre charge opérationnelle car AWS exploite, gère et contrôle les composants, notamment le système d'exploitation hôte, la couche de virtualisation et la sécurité physique des installations dans lesquelles les services fonctionnent. Pour plus d'informations sur la sécurité AWS, consultez le centre de sécurité AWS.

Accès aux ressources

Rôles IAM

Les rôles IAM permettent aux clients d'attribuer des politiques d'accès et des autorisations détaillées aux services et aux utilisateurs sur le cloud AWS. Plusieurs rôles sont nécessaires pour exécuter Workload Discovery sur AWS et découvrir des ressources dans des comptes AWS.

Amazon Cognito

Amazon Cognito est utilisé pour authentifier l'accès à l'aide d'informations d'identification fiables et de courte durée donnant accès aux composants nécessaires à Workload Discovery sur AWS.

Accès réseau

Amazon VPC

Workload Discovery sur AWS est déployé au sein d'un Amazon VPC et configuré conformément aux meilleures pratiques pour garantir sécurité et haute disponibilité. Pour plus de détails, reportez-vous aux meilleures pratiques de sécurité pour votre VPC. Les points de terminaison VPC permettent le transit hors Internet entre les services et sont configurés lorsqu'ils sont disponibles.

Les groupes de sécurité sont utilisés pour contrôler et isoler le trafic réseau entre les composants nécessaires à l'exécution de Workload Discovery sur AWS.

Nous vous recommandons de passer en revue les groupes de sécurité et de restreindre davantage l'accès, le cas échéant, une fois le déploiement terminé.

Amazon CloudFront

Cette solution déploie une interface utilisateur de console Web hébergée dans un compartiment Amazon S3 distribué par Amazon CloudFront. En utilisant la fonctionnalité d'identité d'accès à l'origine, le contenu de ce compartiment Amazon S3 n'est accessible que via CloudFront. Pour plus d'informations, reportez-vous à la section Restreindre l'accès à une origine Amazon S3 dans le manuel Amazon CloudFront Developer Guide.

CloudFront active des mesures de sécurité supplémentaires pour ajouter des en-têtes de sécurité HTTP à chaque réponse du spectateur. Pour plus de détails, reportez-vous à la section Ajout ou suppression d'en-têtes HTTP dans les CloudFront réponses.

Cette solution utilise le CloudFront certificat par défaut dont le protocole de sécurité minimum pris en charge est TLS v1.0. Pour imposer l'utilisation de TLS v1.2 ou TLS v1.3, vous devez utiliser un certificat SSL personnalisé au lieu du certificat par défaut. CloudFront Pour plus d'informations, reportez-vous à Comment configurer ma CloudFront distribution pour utiliser un certificat SSL/TLS.

Configuration de l'application

AWS AppSync

Workload Discovery sur AWS GraphQL APIs dispose d'une validation des demandes fournie par AWS AppSync conformément à la spécification GraphQL. En outre, l'authentification et l'autorisation sont mises en œuvre à l'aide d'IAM et d'Amazon Cognito, qui utilisent le JWT fourni par Amazon Cognito lorsqu'un utilisateur s'authentifie avec succès dans l'interface utilisateur Web.

AWS Lambda

Par défaut, les fonctions Lambda sont configurées avec la version stable la plus récente du moteur d'exécution du langage. Aucune donnée sensible ou aucun secret n'est enregistré. Les interactions de service sont effectuées avec le moins de privilèges requis. Les rôles qui définissent ces privilèges ne sont pas partagés entre les fonctions.

Amazon OpenSearch Service

Les domaines Amazon OpenSearch Service sont configurés avec une politique d'accès qui restreint l'accès afin d'arrêter toute demande non signée envoyée au cluster de OpenSearch services. Ceci est limité à une seule fonction Lambda.

Le cluster de OpenSearch services est conçu avec node-to-node le chiffrement activé pour ajouter une couche supplémentaire de protection des données en plus des fonctionnalités de sécurité du OpenSearch service existantes.

Quotas

Les quotas de service, également appelés limites, représentent le nombre maximal de ressources ou d'opérations de service pour votre compte AWS.

Quotas pour les services AWS dans cette solution

Assurez-vous de disposer d'un quota suffisant pour chacun des services mis en œuvre dans cette solution. Pour de plus amples informations, veuillez consulter Quotas de service AWS.

Utilisez les liens suivants pour accéder à la page de ce service. Pour consulter les quotas de service pour tous les services AWS dans la documentation sans changer de page, consultez plutôt les informations de la page Points de terminaison et quotas du service dans le PDF.

Amplifier	Amazon ECR
Athéna	Lambda
CloudFront	OpenSearch Service
Cognito	Neptune
Config	Amazon S3

Amazon ECS	

CloudFormation Quotas AWS

Votre compte AWS comporte CloudFormation des quotas AWS dont vous devez tenir compte lorsque vous lancez la pile dans cette solution. En comprenant ces quotas, vous pouvez éviter les erreurs de limitation qui vous empêcheraient de déployer correctement cette solution. Pour plus d'informations, consultez CloudFormation les quotas AWS dans le guide de CloudFormation l'utilisateur AWS.

Quotas AWS Lambda

Votre compte dispose d'un quota d'exécution simultanée AWS Lambda de 1 000. Si la solution est utilisée dans un compte sur lequel d'autres charges de travail sont exécutées et utilisent Lambda, définissez ce quota sur une valeur appropriée. Cette valeur est ajustable ; pour plus d'informations, consultez les quotas AWS Lambda dans le guide de l'utilisateur AWS Lambda.

> **Note**
>
> Cette solution nécessite que 150 exécutions par rapport au quota d'exécutions simultanées soient disponibles sur le compte sur lequel la solution est déployée. Si moins de 150 exécutions sont disponibles sur ce compte, le CloudFormation déploiement échouera.

Quotas Amazon VPC

Votre compte AWS peut contenir cinq VPCs et deux Elastic IPs (EIPs). Si la solution est utilisée dans un compte auprès VPCs d'un autre EIPs opérateur, cela pourrait vous empêcher de déployer correctement cette solution. Si vous risquez d'atteindre ce quota, vous pouvez fournir votre propre VPC pour le déploiement en le fournissant lorsque vous suivez les étapes de la section Launch the Stack. Pour plus d'informations, consultez les quotas Amazon VPC dans le guide de l'utilisateur Amazon VPC.

Choix du compte de déploiement

Si vous déployez Workload Discovery sur AWS au sein d'une organisation AWS, la solution doit être installée sur un compte d'administrateur délégué sur lequel StackSetsles fonctionnalités AWS Config multirégionales ont été activées.

Si vous n'utilisez pas AWS Organizations, nous vous recommandons de déployer Workload Discovery sur AWS sur un compte AWS dédié créé spécifiquement pour cette solution. Cette approche signifie que Workload Discovery sur AWS est isolée de vos charges de travail existantes et fournit un emplacement unique pour configurer la solution, par exemple pour ajouter des utilisateurs et importer de nouvelles régions. Il est également plus facile de suivre les coûts engagés lors de l'exécution de la solution.

Une fois Workload Discovery sur AWS déployé, vous pouvez importer des régions à partir de tous les comptes que vous avez déjà provisionnés.

Déployez la solution

Cette solution utilise des CloudFormation modèles et des piles AWS pour automatiser son déploiement. Le CloudFormation modèle indique les ressources AWS incluses dans cette solution et leurs propriétés. La CloudFormation pile fournit les ressources décrites dans le modèle.

Vue d'ensemble du processus de déploiement

> **Note**
>
> Si vous avez déjà déployé Workload Discovery sur AWS et que vous souhaitez passer à la dernière version, reportez-vous à la section Mettre à jour la solution.

Suivez les step-by-step instructions de cette section pour configurer et déployer la solution dans votre compte.

Temps de déploiement : environ 30 minutes

Avant de lancer la solution, examinez le coût, l'architecture, la sécurité du réseau et les autres considérations abordées dans ce guide.

> **Important**
>
> Cette solution inclut une option permettant d'envoyer des métriques opérationnelles anonymisées à AWS. Nous utilisons ces données pour mieux comprendre la façon dont les clients utilisent cette solution et les services et produits associés. AWS est propriétaire des données recueillies dans le cadre de cette enquête. La collecte de données est soumise à l'avis de confidentialité d'AWS.

Prérequis

Collectez les détails des paramètres de déploiement

Avant de déployer Workload Discovery sur AWS, passez en revue les détails de configuration du rôle lié au OpenSearch service Amazon Service et d'AWS Config.

Vérifiez si vous avez un AWSService RoleForAmazonOpenSearchService rôle

Le déploiement crée un cluster Amazon OpenSearch Service au sein d'un Amazon Virtual Private Cloud (Amazon VPC). Le modèle utilise un rôle lié à un service pour créer le cluster de OpenSearch services. Toutefois, si le rôle est déjà créé dans votre compte, utilisez le rôle existant.

Pour vérifier si vous possédez déjà ce rôle, procédez comme suit :

1. Connectez-vous à la console Identity and Access Management (IAM) du compte sur lequel vous comptez déployer cette solution.
2. Dans la zone Rechercher, entrez `AWSServiceRoleForAmazonOpenSearchService`.
3. Si votre recherche renvoie un rôle, sélectionnez `No` le CreateOpensearchServiceRoleparamètre lorsque vous lancez la pile.

Vérifiez qu'AWS Config est configuré

Workload Discovery sur AWS utilise AWS Config pour rassembler la majorité des configurations de ressources. Lors du déploiement de la solution ou de l'importation d'une nouvelle région, vous devez vérifier si AWS Config est déjà configuré et fonctionne comme prévu. Le AlreadyHaveConfigSetup CloudFormation paramètre indique à Workload Discovery sur AWS s'il convient de configurer AWS Config.

L'extrait suivant est extrait de la référence de commande de l'AWS CLI. Exécutez la commande dans la région dans laquelle vous souhaitez déployer Workload Discovery sur AWS ou importer dans Workload Discovery sur AWS.

Entrez la commande suivante :

```
aws configservice get-status
```

Si vous recevez une réponse similaire à la sortie, cela signifie qu'un enregistreur de configuration et un canal de diffusion sont en cours d'exécution dans cette région. Sélectionnez `Yes` le AlreadyHaveConfigSetup CloudFormation paramètre.

Sortie :

```
Configuration Recorders:

name: default
```

```
recorder: ON
last status: SUCCESS

Delivery Channels:

name: default
last stream delivery status: SUCCESS
last history delivery status: SUCCESS
last snapshot delivery status: SUCCESS
```

Si vous configurez AWS CloudFormation StackSets, vous devez inclure cette région dans le lot de régions pour lesquelles AWS Config est déjà configuré.

Vérifiez les informations de votre AWS Config dans votre compte

Le déploiement tentera de configurer AWS Config. Si vous utilisez déjà AWS Config dans le compte sur lequel vous prévoyez de déployer ou de rendre détectable par Workload Discovery sur AWS, sélectionnez les paramètres appropriés lorsque vous déployez cette solution. En outre, pour un déploiement réussi, assurez-vous de ne pas avoir restreint les ressources analysées par AWS Config.

Pour vérifier votre configuration AWS Config actuelle :

1. Connectez-vous à la console AWS Config.
2. Choisissez Paramètres et assurez-vous que les cases Enregistrer toutes les ressources prises en charge dans cette région et Inclure les ressources globales sont sélectionnées.

Vérification de votre configuration VPC

En cas de déploiement sur un VPC existant, vérifiez que vos sous-réseaux privés peuvent acheminer les demandes vers les services AWS.

Si vous choisissez de déployer la solution dans un VPC existant, vous devez vous assurer que les fonctions Workload Discovery on AWS Lambda et les tâches Amazon ECS exécutées dans les sous-réseaux privés de votre VPC peuvent se connecter à d'autres services AWS. La méthode standard pour l'activer consiste à utiliser des passerelles NAT. Vous pouvez répertorier les passerelles NAT de votre compte comme indiqué dans l'exemple de code suivant.

```
aws ec2 describe-route-tables --filters Name=association.subnet-id,Values=<private-
subnet-id1>,<private-subnet-id2> --query 'RouteTables[].Routes[].NatGatewayId'
```

Sortie :

```
[
    "nat-1111111111111111",
    "nat-2222222222222222"
]
```

> **Note**
>
> Si moins de deux résultats sont renvoyés, les sous-réseaux ne disposent pas du nombre correct de passerelles NAT.

Si votre VPC ne possède pas de passerelles NAT, vous devez soit les configurer, soit vous assurer que vous disposez de points de terminaison VPC pour tous les services AWS répertoriés dans la section AWS. APIs

CloudFormation Modèle AWS

Cette solution utilise AWS CloudFormation pour automatiser le déploiement de Workload Discovery sur AWS dans le cloud AWS. Il inclut le CloudFormation modèle suivant, que vous pouvez télécharger avant le déploiement :

workload-discovery-on-aws.template - Utilisez ce modèle pour lancer la solution et tous les composants associés. La configuration par défaut déploie les solutions de base et de support figurant dans les services AWS de cette section de solutions, mais vous pouvez personnaliser le modèle en fonction de vos besoins spécifiques.

> **Note**
>
> Vous pouvez personnaliser le modèle pour répondre à vos besoins spécifiques ; toutefois, toute modification que vous apportez peut affecter le processus de mise à niveau.

Lancement de la pile

Ce CloudFormation modèle AWS automatisé déploie Workload Discovery sur AWS dans le cloud AWS. Vous devez recueillir les détails des paramètres de déploiement avant de lancer la pile. Pour plus de détails, reportez-vous à la section Conditions préalables.

Temps de déploiement : environ 30 minutes

1. Connectez-vous à l'AWS Management Console et sélectionnez le bouton pour lancer le CloudFormation modèle `workload-discovery-on-aws.template` AWS.

2. Le modèle est lancé par défaut dans la région USA Est (Virginie du Nord). Pour lancer la solution dans une autre région AWS, utilisez le sélecteur de région dans la barre de navigation de la console.

> **Note**
>
> Cette solution utilise des services qui ne sont pas disponibles dans toutes les régions AWS. Reportez-vous à la section Régions AWS prises en charge pour obtenir la liste des régions AWS prises en charge.

3. Sur la page Create stack, vérifiez que l'URL du modèle est correcte dans la zone de texte URL Amazon S3, puis choisissez Next.
4. Sur la page Spécifier les détails de la pile, attribuez un nom à votre pile de solutions. Pour plus d'informations sur les limites relatives aux caractères de dénomination, reportez-vous aux quotas IAM et AWS STS dans le guide de l'utilisateur d'AWS Identity and Access Management.
5. Sous Paramètres, passez en revue les paramètres de ce modèle de solution et modifiez-les si nécessaire. Cette solution utilise les valeurs par défaut suivantes.

Paramètre	Par défaut	Description
AdminUserEmailAddress	*<Requires input>*	Adresse e-mail pour créer le premier utilisateur. Les informations d'identification

Paramètre	Par défaut	Description
		temporaires seront envoyées à cette adresse e-mail.
AlreadyHaveConfigSetup	`No`	Confirmation indiquant si AWS Config est déjà configuré dans le compte de déploiement. Pour plus de détails, reportez-vous à la section Conditions préalables.
AthenaWorkgroup	`primary`	Le groupe de travail qui sera utilisé pour émettre la requête Athena lorsque la fonctionnalité Coût sera activée.

Paramètre	Par défaut	Description
ApiAllowListedRanges	`0.0.0.0/1,128.0.0.0/1`	Liste séparée par des virgules CIDRs pour gérer l'accès à l'API AppSync GraphQL. Pour autoriser l'accès à Internet dans son intégralité, utilisez 0.0.0.0/1 ,128.0.0.0/1. Si vous limitez l'accès à des données spécifiques CIDRs, vous devez également inclure les adresses IP (et un masque de sous-réseau /32) des passerelles NAT qui permettent à la tâche ECS du processus de découvert e exécutée dans son sous-réseau privé d'accéder à Internet. REMARQUE : Cette liste d'autorisations ne régit pas l'accès à la WebUI, mais uniquement à l'API GraphQL.
CreateNeptuneReplica	No	Choisissez si vous souhaitez créer une réplique en lecture pour Neptune dans une zone de disponibilité distincte. Le choix `Yes` améliore la résilience mais augmente le coût de cette solution.

Paramètre	Par défaut	Description
CreateOpenSearchServiceRole	`Yes`	Confirmation indiquant si vous possédez déjà un rôle lié à un service pour Amazon OpenSearch Service. Pour plus de détails, reportez-vous à la section Conditions préalables.
NeptuneInstanceClass	`db.r5.large`	Type d'instance utilisé pour héberger la base de données Amazon Neptune. Ce que vous sélectionnez ici influe sur le coût d'exécution de cette solution.
OpensearchInstanceType	`m6g.large.search`	Type d'instance utilisé pour vos nœuds OpenSearch de données de service. Votre sélection influe sur le coût de fonctionnement de la solution.
OpensearchMultiAz	`No`	Choisissez si vous souhaitez créer un cluster de OpenSearch services couvrant plusieurs zones de disponibilité. Le choix `Yes` améliore la résilience mais augmente le coût de cette solution.

Paramètre	Par défaut	Description
CrossAccountDiscovery	`SELF_MANAGED`	Choisissez si Workload Discovery on AWS ou AWS Organizations gère l'importation des comptes. La valeur peut être `SELF_MANAGED` ou `AWS_ORGANIZATIONS` .
OrganizationUnitId	<Optional input>	ID de l'unité organisationnelle racine. Ce paramètre n'est utilisé que lorsqu'il CrossAccountDiscoveryest défini sur`AWS_ORGANIZATIONS` .
AccountType	`DELEGATED_ADMIN`	Type de compte AWS Organizations dans lequel installer Workload Discovery sur AWS. Ce paramètre n'est utilisé que lorsqu'il CrossAccountDiscoveryest défini sur`AWS_ORGANIZATIONS` . Pour plus de détails, reportez-vous à la section Choix du compte de déploiement.

Paramètre	Par défaut	Description
ConfigAggregatorName	<Optional input>	L'agrégateur de configuration à l'échelle de l'organisation AWS à utiliser. Vous devez installer la solution dans le même compte et dans la même région que cet agrégateur. Si vous laissez ce paramètre vide, un nouvel agrégateur sera créé. Ce paramètre n'est utilisé que lorsqu'il CrossAccountDiscoveryest défini surAWS;_ORGANIZATIONS .
CpuUnits	1 vCPU	Le nombre de CPUs à allouer à la tâche Fargate dans laquelle s'exécute le processus de découverte.
Mémoire	2048	Quantité de mémoire à allouer à la tâche Fargate dans laquelle s'exécute le processus de découverte.
DiscoveryTaskFrequency	15mins	Intervalle de temps entre chaque exécution de la tâche ECS du processus de découverte.

Paramètre	Par défaut	Description
MinNCUs	1	Unités de capacité Neptune minimales (NCUs) à définir sur le cluster Neptune (elles doivent être inférieures ou égales à Max). NCUs Obligatoire si DBInstance le type estdb.serverless .
MaxNCUs	128	Maximum NCUs à définir sur le cluster Neptune (doit être supérieur ou égal à Min NCUs). Obligatoi re si DBInstance le type estdb.serverless .
VpcId	<Optional input>	L'ID d'un VPC existant pour la solution à utiliser. Si vous laissez ce paramètre vide, un nouveau VPC sera provision né.
VpcCidrBlock	<Optional input>	Le bloc CIDR VPC du VPC référencé par le paramètre . VpcId Ce paramètre n'est utilisé que s'VpcIdil est défini.
PrivateSubnet0	<Optional input>	Le sous-réseau privé que vous souhaitez utiliser. Ce paramètre n'est utilisé que s'VpcIdil est défini.
PrivateSubnet1	<Optional input>	Le sous-réseau privé que vous souhaitez utiliser. Ce paramètre n'est utilisé que s'VpcIdil est défini.

Paramètre	Par défaut	Description
UsesCustomIdentity	No	Confirmation indiquant si vous utiliserez ou non un fournisseur d'identité personnalisé, tel que SAML ou OIDC.
CognitoCustomDomain	<Optional input>	Préfixe de domaine du domaine personnalisé Amazon Cognito qui héberge les pages d'inscription et de connexion de votre applicati on. Laissez ce champ vide si vous n'utilisez pas d'IdP personnalisé, sinon vous ne devez inclure que des lettres minuscules, des chiffres et des traits d'union.
CognitoAttributeMapping	<Optional input>	Le mappage des attributs IdP avec les attributs standard et personnalisés du groupe d'utilisateurs de Cognito. Laissez ce champ vide si vous n'utilisez pas d'IdP personnalisé, sinon il doit s'agir d'une chaîne JSON valide.
IdentityType	<Optional input>	Type de fournisseur d'identit é à utiliser (`GoogleSAML`, ou`OIDC`). Laissez ce champ vide si vous n'utilisez pas d'IdP personnalisé.

Paramètre	Par défaut	Description
ProviderName	<Optional input>	Nom du fournisseur d'identité. Laissez ce champ vide si vous n'utilisez pas d'IdP personnalisé.
GoogleClientId	<Optional input>	L'identifiant client Google à utiliser. Paramètre utilisé uniquement lorsqu'il IdentityTypeest défini sur`Google`.
GoogleClientSecret	<Optional input>	Le secret du client Google à utiliser. Paramètre utilisé uniquement lorsqu'il IdentityTypeest défini sur`Google`.
SAMLMetadataURL	<Optional input>	URL des métadonnées du fournisseur d'identité SAML. Paramètre utilisé uniquement lorsqu'il IdentityTypeest défini sur SAML.
OIDCClientId	<Optional input>	L'ID du client OIDC à utiliser. Paramètre utilisé uniquement lorsqu'il IdentityTypeest défini sur`OIDC`.
OIDCClientSecret	<Optional input>	Le secret du client OIDC à utiliser. Paramètre utilisé uniquement lorsqu'il IdentityTypeest défini sur`OIDC`.
OIDCIssuerURL	<Optional input>	URL de l'émetteur OIDC à utiliser. Paramètre utilisé uniquement lorsqu'il IdentityTypeest défini sur`OIDC`.

Paramètre	Par défaut	Description
OIDCAttributeRequestMethod	`GET`	Méthode de demande d'attribut OIDC à utiliser. Doit être l'`GET`un ou l'autre `POST` (reportez-vous au fournisse ur OIDC ou utilisez la valeur par défaut). Paramètre utilisé uniquement lorsqu'il IdentityT ypeest défini sur`OIDC`.

6. Choisissez Next (Suivant).
7. Sur la page Configurer les options de pile, choisissez Suivant.
8. Sur la page Réviser et créer, vérifiez et confirmez les paramètres. Cochez les cases indiquant que le modèle crée des ressources IAM et nécessite certaines fonctionnalités.
9. Choisissez Submit pour déployer la pile.

   Vous pouvez consulter l'état de la pile dans la CloudFormation console AWS dans la colonne Status. Vous devriez recevoir le statut CREATE_COMPLETE dans environ 30 minutes.

> **Note**
>
> Si elle est supprimée, cette pile supprime toutes les ressources. Si la pile est mise à jour, elle conserve le groupe d'utilisateurs Amazon Cognito afin de garantir que les utilisateurs configurés ne soient pas perdus.

Tâches de configuration après le déploiement

Après le déploiement réussi de Workload Discovery sur AWS, effectuez les tâches de configuration post-déploiement suivantes.

Activer la sécurité avancée dans Amazon Cognito

Pour activer les fonctionnalités de sécurité avancées pour Amazon Cognito, suivez les instructions relatives à l'ajout d'une sécurité avancée à un groupe d'utilisateurs dans le guide du développeur Amazon Cognito.

> **Note**
>
> L'activation de la sécurité avancée dans Amazon Cognito entraîne un coût supplémentaire.

Création d'utilisateurs Amazon Cognito

Workload Discovery sur AWS utilise Amazon Cognito pour gérer tous les utilisateurs et l'authentification. Il crée un utilisateur pour vous lors du déploiement et envoie un e-mail à l'adresse fournie dans le AdminUserEmailAddress paramètre avec des informations d'identification temporaires.

Pour créer des utilisateurs supplémentaires, procédez comme suit :

1. Connectez-vous à la console AWS Cognito.
2. Sélectionnez Gérer les groupes d’utilisateurs.
3. Choisissez WDCognitoUserPool-*<ID-string>*.
4. Dans le volet de navigation, sous Paramètres généraux, sélectionnez Utilisateurs et groupes.
5. Dans l'onglet Utilisateurs, choisissez Créer un utilisateur.
6. Dans le champ Créer un utilisateur, entrez des valeurs pour tous les champs obligatoires.

Champ du formulaire	Obligatoire ?	Description
Nom d’utilisateur	Oui	Le nom d'utilisateur que vous utiliserez pour vous connecter

Champ du formulaire	Obligatoire ?	Description
		à Workload Discovery sur AWS.
Envoyer une invitation	Oui (e-mail uniquement)	Lorsque cette option est sélectionnée, envoie une notification pour rappeler le mot de passe temporair e. Sélectionnez E-mail uniquement. Si vous sélection nez SMS (par défaut), un message d'erreur s'affiche, mais l'utilisateur est toujours créé.
Mot de passe temporaire	Oui	Entrez un mot de passe temporaire. L'utilisateur est obligé de modifier cela lorsqu'il se connecte à Workload Discovery sur AWS pour la première fois.
Numéro de téléphone	Non	Entrez un numéro de téléphone au format internati onal, par exemple,\+44. Assurez-vous que le numéro de téléphone Mark est vérifié ? la case est sélection née.
E-mails	Oui	Entrez une adresse e-mail valide. Assurez-vous que l'e-mail Marquer comme vérifié ? la case est sélectionnée.

7. Choisissez Create user (Créer un utilisateur).

Répétez ce processus pour créer autant d'utilisateurs que nécessaire.

> **Note**
>
> Chaque utilisateur aura le même niveau d'accès aux ressources découvertes. Nous recommandons de configurer un déploiement distinct de Workload Discovery sur AWS pour les comptes contenant des charges de travail ou des données sensibles. Cela vous permet de restreindre l'accès aux seuls utilisateurs qui en ont besoin.

Connectez-vous à Workload Discovery sur AWS

Une fois la solution déployée avec succès, déterminez l'URL de la CloudFront distribution Amazon qui fournit l'interface utilisateur Web de la solution.

1. Connectez-vous à la CloudFormation console AWS.
2. Choisissez Afficher imbriqué pour afficher les piles imbriquées qui constituent le déploiement. Selon vos préférences, les piles imbriquées sont peut-être déjà affichées.
3. Sélectionnez la pile principale de découverte de la charge de travail sur AWS.
4. Sélectionnez l'onglet Sorties et choisissez l'URL dans la colonne Valeur associée à la WebUiUrlclé.
5. Sur l'écran de connexion, entrez les informations de connexion que vous avez reçues par e-mail. Effectuez ensuite les actions suivantes :
   a. Suivez les instructions pour modifier votre mot de passe.
   b. Utilisez le code de vérification envoyé à votre adresse e-mail pour terminer la restauration du compte.

Importer une région

> **Note**
>
> La section suivante s'applique uniquement lorsque le mode de découverte des comptes de la solution est autogéré. Pour plus d'informations sur le fonctionnement de la découverte de comptes en mode AWS Organizations, consultez la section Mode de découverte de comptes AWS Organizations.

L'importation d'une région nécessite le déploiement de certaines infrastructures. Cette infrastructure comprend des ressources mondiales et régionales :

Global : ressources déployées une fois dans un compte et réutilisées pour chaque région importée.

- Un rôle IAM () WorkloadDiscoveryRole

Régional — Les ressources déployées dans chaque région sont importées.

- Un canal de diffusion AWS Config
- Un compartiment Amazon S3 pour AWS Config
- Un rôle IAM () ConfigRole

Il existe deux options pour déployer cette infrastructure :

- AWS CloudFormation StackSets (recommandé)
- AWS CloudFormation

Importer une région

Ces étapes vous guident dans l'importation d'une région et le déploiement des CloudFormation modèles AWS.

1. Connectez-vous à Workload Discovery sur AWS. Reportez-vous à la section Connexion à Workload Discovery sur AWS pour obtenir l'URL.
2. Dans le menu de navigation, sélectionnez Comptes.
3. Choisissez Importer.
4. Sélectionnez la méthode d'importation :
   a. Ajoutez des comptes et des régions à l'aide d'un fichier CSV.
   b. Ajoutez des comptes et des régions à l'aide d'un formulaire.

Fichier CSV

Fournissez un fichier CSV (valeurs séparées par des virgules) contenant les régions à importer au format suivant.

```
"accountId","accountName","region"
123456789012,"test-account-1",eu-west-2
123456789013,"test-account-2",eu-west-1
123456789013,"test-account-2",eu-west-2
123456789014,"test-account-3",eu-west-3
```

1. Sélectionnez Charger un fichier CSV.
2. Localisez et ouvrez votre fichier CSV.
3. Consultez le tableau des régions, puis sélectionnez Importer.
4. Dans la boîte de dialogue modale, téléchargez le modèle de ressources globales et le modèle de ressources régionales.
5. Déployez les CloudFormation modèles dans les comptes concernés (reportez-vous à la section Déployer les CloudFormation modèles AWS).
6. Une fois que les modèles de ressources mondiaux et régionaux ont été déployés, cochez les deux cases pour confirmer que l'installation est terminée et choisissez Importer.

Formulaire

Indiquez les régions à importer à l'aide du formulaire :

1. Pour ID de compte, entrez un identifiant de compte à 12 chiffres ou sélectionnez un identifiant de compte existant.
2. Pour Nom du compte, entrez un nom de compte ou utilisez une valeur préremplie lors de la sélection d'un identifiant de compte existant.
3. Sélectionnez les régions à importer.
4. Sélectionnez Ajouter pour renseigner les régions dans le tableau des régions ci-dessous.
5. Consultez le tableau des régions, puis sélectionnez Importer.
6. Dans la boîte de dialogue modale, téléchargez le modèle de ressources globales et le modèle de ressources régionales.
7. Déployez les CloudFormation modèles dans les comptes concernés (reportez-vous à la section Déployer les CloudFormation modèles AWS).
8. Une fois que les modèles de ressources mondiaux et régionaux ont été déployés, cochez les deux cases pour confirmer que l'installation est terminée et choisissez Importer.

Déployez les CloudFormation modèles AWS

Les ressources globales doivent être déployées une fois par compte. Ne déployez pas ce modèle lorsque vous importez une région depuis un compte contenant une région déjà importée dans Workload Discovery sur AWS. Si la région a déjà été importée, suivez les instructions de la section Déployer la pile pour approvisionner les ressources régionales.

CloudFormation StackSets À utiliser pour provisionner des ressources globales sur plusieurs comptes

> **Important**
>
> Tout d'abord, remplissez les conditions préalables pour que les opérations de stack set soient activées StackSets dans vos comptes cibles.

1. Dans le compte administrateur, connectez-vous à la CloudFormation console AWS.
2. Dans le menu de navigation, sélectionnez StackSets.
3. Choisissez Créer StackSet.
4. Sur la page Choisir un modèle, sous Autorisations :
   a. Si vous utilisez AWS Organizations, choisissez soit les autorisations gérées par le service, soit les autorisations en libre-service. Pour plus de détails, consultez la section Utilisation StackSets dans une organisation AWS.
   b. Si vous n'utilisez pas AWS Organizations, entrez le nom du rôle d'exécution IAM utilisé lorsque vous suivez les étapes StackSets préalables. Pour plus de détails, reportez-vous à la section Accorder des autorisations autogérées.
5. Sous Spécifier le modèle, sélectionnez Télécharger un fichier modèle. Choisissez le `global-resources.template` fichier (téléchargé plus tôt lorsque vous avez importé une région par fichier CSV ou par formulaire), puis cliquez sur Suivant.
6. Sur la page Spécifier StackSet les détails, attribuez un nom à votre StackSet. Pour plus d'informations sur les limites relatives aux caractères de dénomination, reportez-vous aux quotas IAM et AWS STS dans le guide de l'utilisateur d'AWS Identity and Access Management.
7. Sous Paramètres, passez en revue les paramètres de ce modèle de solution et modifiez-les si nécessaire. Cette solution utilise les valeurs par défaut suivantes.

Nom de champ	Par défaut	Description
AccountId	L'ID du compte de déploiement	ID de compte du compte de déploiement d'origine. Vous devez laisser cette valeur par défaut.

1. Choisissez Suivant.
2. Sur la page des StackSet options de configuration, choisissez Next.
3. Sur la page Définir les options de déploiement, sous Comptes, entrez le compte IDs pour déployer le rôle de compte dans le champ Numéros de compte.
4. Sous Spécifier les régions, sélectionnez une région pour installer la pile.
5. Sous Options de déploiement, sélectionnez Parallèle, puis Next.
6. Sur la page de révision, cochez la case reconnaissant qu'AWS CloudFormation peut créer des ressources IAM avec des noms personnalisés.
7. Sélectionnez Envoyer.

Utilisation CloudFormation StackSets pour fournir des ressources régionales

> **Important**
>
> Tout d'abord, remplissez les conditions préalables pour que les opérations de stack set soient activées StackSets dans vos comptes cibles.
> Si vous avez installé AWS Config dans certaines régions et d'autres non, vous devez effectuer deux StackSet opérations, l'une pour les régions où AWS Config est installé et l'autre pour celles qui n'en ont pas.

1. Dans le compte administrateur, connectez-vous à la CloudFormation console AWS.
2. Dans le menu de navigation, sélectionnez StackSets.
3. Choisissez Créer StackSet.
4. Sur la page Choisir un modèle, sous Autorisations :

a. Si vous utilisez AWS Organizations, choisissez soit les autorisations gérées par le service, soit les autorisations en libre-service. Pour plus de détails, consultez la section Utilisation StackSets dans une organisation AWS.

b. Si vous n'utilisez pas AWS Organizations, entrez le nom du rôle d'exécution IAM utilisé lorsque vous suivez les étapes StackSets préalables. Pour plus de détails, reportez-vous à la section Accorder des autorisations autogérées.

5. Sous Spécifier le modèle, sélectionnez Télécharger un fichier modèle. Choisissez le `regional-resources.template` fichier (téléchargé plus tôt lorsque vous avez importé une région par fichier CSV ou par formulaire), puis cliquez sur Suivant.
6. Sur la page Spécifier StackSet les détails, attribuez un nom à votre StackSet. Pour plus d'informations sur les limites relatives aux caractères de dénomination, reportez-vous aux quotas IAM et AWS STS dans le guide de l'utilisateur d'AWS Identity and Access Management.
7. Sous Paramètres, passez en revue les paramètres de ce modèle de solution et modifiez-les si nécessaire. Cette solution utilise les valeurs par défaut suivantes.

Nom de champ	Par défaut	Description
AccountId	L'ID du compte de déploiement	ID de compte du compte de déploiement d'origine. Vous devez laisser cette valeur par défaut.
AggregationRegion	La région de déploiement	La région dans laquelle le déploiement a été initialement effectué. Vous devez laisser cette valeur par défaut.
AlreadyHaveConfigSetup	`No`	Confirmation indiquant si AWS Config est déjà installé dans la région. Définissez ce paramètre sur Oui si AWS Config est déjà installé dans cette région.

1. Choisissez Suivant.

2. Sur la page des StackSet options de configuration, choisissez Next.
3. Sur la page Définir les options de déploiement, sous Comptes, entrez le compte IDs vers lequel déployer le rôle de compte dans le champ Numéros de compte.
4. Sous Spécifier les régions, sélectionnez une région pour installer la pile. Cela installe la pile dans ces régions dans tous les comptes saisis à l'étape 6.
5. Sous Options de déploiement, sélectionnez Parallèle, puis Next.
6. Sur la page de révision, cochez la case reconnaissant qu'AWS CloudFormation peut créer des ressources IAM avec des noms personnalisés.
7. Sélectionnez Envoyer.

Déployez la pile pour approvisionner les ressources globales en utilisant CloudFormation

Les ressources globales doivent être déployées une fois par compte. Ne déployez pas ce modèle lorsque vous importez une région depuis un compte contenant une région déjà importée dans Workload Discovery sur AWS.

1. Connectez-vous à la CloudFormation console AWS.
2. Choisissez Créer une pile, puis sélectionnez Avec de nouvelles ressources (standard).
3. Sur la page Créer une pile, dans la section Spécifier un modèle, sélectionnez Télécharger un fichier modèle.
4. Choisissez Choisir un fichier et sélectionnez le `global-resources.template` fichier qui (téléchargé précédemment lorsque vous avez importé une région par fichier CSV ou par formulaire), puis cliquez sur Suivant.
5. Sur la page Spécifier les détails de la pile, attribuez un nom à votre pile de solutions. Pour plus d'informations sur les limites relatives aux caractères de dénomination, reportez-vous aux quotas IAM et AWS STS dans le _AWS Identity and Access Management _User Guide.
6. Sous Paramètres, passez en revue les paramètres de ce modèle de solution et modifiez-les si nécessaire. Cette solution utilise les valeurs par défaut suivantes.

Nom de champ	Par défaut	Description
Nom de la pile	`workload-discovery`	Le nom de cette CloudFormation pile AWS.
AccountId	ID du compte de déploiement	ID de compte du compte de déploiement d'origine. Vous devez laisser cette valeur par défaut.

1. Choisissez Suivant.
2. Cochez la case reconnaissant qu'AWS CloudFormation peut créer des ressources IAM avec des noms personnalisés.
3. Sélectionnez Créer la pile.

Les nouvelles régions seront scannées lors du prochain processus de découverte, qui se déroule à intervalles de 15 minutes, par exemple : 15 h 00, 15 h 15, 15 h 30, 15 h 45.

Déployez la pile pour approvisionner les ressources régionales en utilisant CloudFormation

1. Connectez-vous à la CloudFormation console AWS.
2. Choisissez Créer une pile, puis sélectionnez Avec de nouvelles ressources (standard).
3. Sur la page Créer une pile, dans la section Spécifier un modèle, sélectionnez Télécharger un fichier modèle.
4. Choisissez Choisir un fichier et sélectionnez le `regional-resources.template` fichier (téléchargé précédemment lorsque vous avez importé une région par fichier CSV ou par formulaire), puis cliquez sur Suivant.
5. Sur la page Spécifier les détails de la pile, attribuez un nom à votre pile de solutions. Pour plus d'informations sur les limites relatives aux caractères de dénomination, reportez-vous aux quotas IAM et AWS STS dans le guide de l'utilisateur d'AWS Identity and Access Management.
6. Sous Paramètres, passez en revue les paramètres de ce modèle de solution et modifiez-les si nécessaire. Cette solution utilise les valeurs par défaut suivantes.

Nom de champ	Par défaut	Description
AccountId	ID du compte de déploiement de la solution	ID de compte du compte de déploiement d'origine. Doit être laissé par défaut.
AggregationRegion	Région de déploiement de la solution	La région dans laquelle le déploiement a été initialement effectué. Doit être laissé par défaut.
AlreadyHaveConfigSetup	`No`	Confirmation indiquant si AWS Config est déjà installé dans la région. Défini sur `Yes` si AWS Config est déjà installé dans cette région.

1. Choisissez Suivant.
2. Cochez la case reconnaissant qu'AWS CloudFormation peut créer des ressources IAM avec des noms personnalisés.
3. Sélectionnez Créer la pile.

Les nouvelles régions seront scannées lors du prochain processus de découverte, qui se déroule à intervalles de 15 minutes, par exemple à 15h00, 15h15, 15h30, 15h45.

Vérifiez que la région a été importée correctement

1. Connectez-vous à l'interface utilisateur Web de la solution (ou actualisez la page si elle est déjà chargée). Reportez-vous à la section Connexion à Workload Discovery sur AWS pour obtenir l'URL.
2. Dans le panneau de navigation de gauche, sous Paramètres, sélectionnez Régions importées.

La région, le nom et l'identifiant du compte apparaissent dans le tableau. La colonne Dernière analyse indique les dernières ressources découvertes dans cette région.

> **Note**
>
> Si la colonne Dernière analyse reste vide pendant plus de 30 minutes, reportez-vous à la section Débogage du composant de découverte.

Configuration de la fonction de coût

La fonctionnalité de coût nécessite la configuration manuelle des rapports sur les coûts et l'utilisation (CUR) d'AWS. En suivant les instructions ci-dessous, vous pourrez :

1. Configurez un CUR planifié.
2. Configurer la réplication Amazon S3 (lorsque vous CURs êtes en dehors du compte de déploiement)

Créez le rapport sur les coûts et l'utilisation d'AWS dans le compte de déploiement

1. Connectez-vous à la console de facturation du compte à partir duquel vous souhaitez collecter les données de coûts.
2. Dans le menu de navigation, sous Facturation, sélectionnez Rapports sur les coûts et l'utilisation.
3. Choisissez Créer un rapport.
4. Utiliser `workload-discovery-cost-and-usage-` *`<your-workload-discovery-deployment-account-ID>`* comme nom du rapport.

   > **Note**
   >
   > Vous devez suivre cette convention de dénomination car une petite quantité d'infrastructure sera déployée pour faciliter l'interrogation du CURs.

5. Sélectionnez la IDs case Inclure la ressource.

> **Note**
>
> Vous devez sélectionner la IDs case Inclure la ressource pour afficher les données de coûts. Cet identifiant doit correspondre aux ressources découvertes par Workload Discovery sur AWS.

6. Choisissez Suivant.
7. Sur la page Options de livraison, choisissez Configurer 0
8. Sélectionnez le compartiment *<stack-name>* `-s3buc-costandusagereportbucket-` *<ID-string>* Amazon S3 pour stocker le CUR. Choisissez Suivant.
9. Passez en revue la politique, sélectionnez la case de confirmation, puis cliquez sur Enregistrer.
10. Définissez le chemin du préfixe du rapport sur. `aws-perspective`
11. Sélectionnez Quotidien pour la granularité temporelle.
12. Sous Activer l'intégration des données de rapport pour, sélectionnez Amazon Athena.
13. Choisissez Suivant.
14. Choisissez Réviser et terminer.

Pour vérifier que le rapport est correctement configuré, recherchez le fichier de test dans le compartiment Amazon S3.

> **Note**
>
> Le chargement des rapports dans votre bucket peut prendre jusqu'à 24 heures.

Création du rapport sur les coûts et l'utilisation d'AWS dans un compte externe

1. Connectez-vous à la console de facturation du compte à partir duquel vous souhaitez collecter les données de coûts.
2. Dans le menu de navigation, sous Gestion des coûts, sélectionnez Rapports sur les coûts et l'utilisation.
3. Choisissez Créer un rapport.

4. Utiliser `workload-discovery-cost-and-usage-` *`<your-external-account-ID>`* comme nom du rapport.

> **Note**
>
> Vous devez suivre cette convention de dénomination car une petite quantité d'infrastructure sera déployée pour faciliter l'interrogation du CURs.

5. Cochez la IDs case Inclure la ressource.

> **Note**
>
> Vous devez sélectionner la IDs case Inclure la ressource pour afficher les données de coûts. Cet identifiant est nécessaire pour correspondre aux ressources découvertes par Workload Discovery sur AWS.

6. Choisissez Suivant.
7. Sur la page Options de livraison, choisissez Configurer 0
8. Créez un nouveau compartiment Amazon S3 pour stocker le CURs.
9. Passez en revue la politique, sélectionnez la case de confirmation, puis cliquez sur Enregistrer.
10. Définissez le chemin du préfixe du rapport sur. `aws-perspective`
11. Sélectionnez Quotidien pour la granularité temporelle.
12. Sous Activer l'intégration des données de rapport pour, sélectionnez Amazon Athena.
13. Choisissez Suivant.
14. Choisissez Réviser et terminer. Pour vérifier que le rapport est correctement configuré, recherchez le fichier de test dans le compartiment Amazon S3.

> **Note**
>
> Le chargement des rapports dans votre bucket peut prendre jusqu'à 24 heures.

Configurez ensuite la réplication sur le compte de déploiement.

Configuration de la réplication

Configurez la réplication dans le compartiment Amazon S3 créé lors du déploiement. Le compartiment Amazon S3 suit le format suivant : `<stack-name>-s3buc-costandusagereportbucket-<ID-string>`. Cela permet à la solution d'interroger le compartiment avec Amazon Athena.

1. Connectez-vous au compte AWS dans la console Amazon S3 qui contient le CUR créé qui doit être répliqué.
2. Sélectionnez le compartiment Amazon S3 créé lors de la configuration de votre CUR. Pour plus d'informations, consultez l'étape 8 de la section Création et planification du rapport sur les coûts et l'utilisation d'AWS.
3. Choisissez l'onglet Gestion.
4. Sous Règles de réplication, sélectionnez Créer une règle de réplication.
5. Sous Configuration des règles de réplication, dans le champ Nom de la règle de réplication, entrez un ID de règle descriptif.
6. Sous Compartiment source, sélectionnez Appliquer à tous les objets du compartiment pour configurer l'étendue de la règle.
7. Sous Destination, configurez les éléments suivants :
   a. Sélectionnez Spécifier un compartiment dans un autre compte.
   b. Entrez l'identifiant du compte.
   c. Entrez une valeur pour le nom du compartiment créé lors du déploiement de Workload Discovery sur AWS. Vous pouvez le trouver en suivant les instructions de la section Localisation des ressources de déploiement, en utilisant l'ID logique `CostAndUsageReportBucket` et le nom de pile que vous avez spécifiés lors du premier déploiement de Workload Discovery sur AWS.
   d. Cochez la case Changer la propriété de l'objet en propriétaire du compartiment de destination.
8. Sous Rôle IAM, sélectionnez Créer un nouveau rôle.

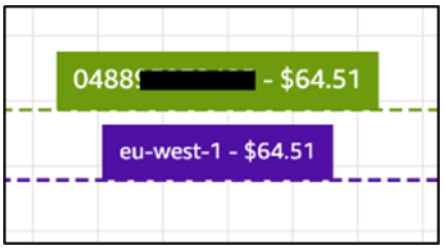
> **Note**
>
> Il se peut qu'un rôle de réplication existe déjà. Vous pouvez le sélectionner et vous assurer qu'il possède les actions de rôle de réplication S3 requises.

9. Choisissez Enregistrer.

10. Connectez-vous à la console de gestion AWS où le CUR est installé, accédez à la page du service S3 et sélectionnez le compartiment `CostAndUsageReportBucket` S3. Pour plus de détails, reportez-vous à la section Localisation des ressources de déploiement.
11. Sélectionnez l'onglet Gestion.
12. Sous Règles de réplication, dans le menu déroulant Actions, sélectionnez Recevoir des objets répliqués.
13. Sous Paramètres du compte Source bucket :
    a. Entrez l'ID du compte du compartiment source.
    b. Choisissez Générer des politiques.
    c. Sous Politiques, sélectionnez Afficher la politique du bucket.
    d. Sélectionnez Inclure l'autorisation pour changer la propriété de l'objet en propriétaire du compartiment de destination.
    e. Choisissez Appliquer les paramètres. Cela lui permet d'y copier des objets. Reportez-vous à la politique de réplication de Cost Bucket pour un exemple de politique de compartiment S3.

> **Note**
>
> Lors de la réplication CURs à partir de plusieurs comptes AWS. Vous devez vous assurer que la politique de compartiment du compartiment de destination (dans le compte Workload Discovery on AWS) contient l'ARN de chaque rôle IAM que vous utilisez pour chaque compte. Reportez-vous à la politique de réplication de Cost Bucket pour plus de détails.

Lorsque les rapports sont enregistrés dans le compte, les données relatives aux coûts apparaissent dans les cases de sélection et sur les ressources individuelles.



Modifier les politiques de cycle de vie des compartiments S3

Au cours du déploiement, la solution configure les politiques de cycle de vie sur deux compartiments :

- `CostAndUsageReportBucket`
- `AccessLogsBucket`

> **Important**
>
> Ces politiques de cycle de vie suppriment les données de ces compartiments après 90 jours. Vous pouvez modifier le cycle de vie pour l'adapter à toutes vos politiques internes.

Surveillance de la solution

Cette solution utilise MyApplications et vous CloudWatch AppInsightspermet de surveiller votre déploiement de Workload Discovery sur AWS.

Mes candidatures

MyApplications est une extension de Console Home qui vous permet de gérer et de surveiller le coût, l'intégrité, le niveau de sécurité et les performances de vos applications sur AWS. Vous pouvez accéder à toutes les applications de votre compte, aux indicateurs clés de toutes les applications, ainsi qu'à une vue d'ensemble des indicateurs de coûts, de sécurité et d'exploitation et aux informations provenant de plusieurs consoles de service depuis une seule vue dans l'AWS Management Console.

Pour consulter le tableau de bord MyApplications pour Workload Discovery sur AWS :

1. Connectez-vous à l'AWS Management Console.
2. Dans la barre latérale gauche, choisissez myApplications.
3. Tapez `workload-discovery` dans la barre de recherche pour trouver l'application.
4. Sélectionnez l'application.

CloudWatch AppInsights

CloudWatch Application Insights vous aide à surveiller vos applications en identifiant et en configurant des indicateurs, des journaux et des alarmes clés pour l'ensemble de vos ressources applicatives et de votre infrastructure technologique. Il surveille en permanence les métriques et les journaux afin de détecter et de corréler les anomalies et les erreurs. Afin de faciliter le dépannage, elle crée des tableaux de bord automatisés pour les problèmes détectés, qui incluent les anomalies de métriques corrélées, les erreurs de journalisation, ainsi que des informations supplémentaires vous indiquant la cause racine potentielle.

Pour consulter le CloudWatch AppInsights tableau de bord de Workload Discovery sur AWS :

1. Connectez-vous à la console CloudWatch .
2. Dans la barre latérale gauche, choisissez Insights, Application Insights.
3. Sélectionnez l'onglet Applications.

4. Tapez `workload-discovery` dans la barre de recherche pour trouver le tableau de bord.
5. Sélectionnez le tableau de bord.
6. Sélectionnez l'application.

Mettre à jour la solution

Important

La mise à jour de la version v1.x.x vers la version 2.x.x de Workload Discovery sur AWS n'est pas prise en charge. Nous vous recommandons de désinstaller la version v1.x.x de cette solution avant d'installer la version 2.x.x.

Pour effectuer une mise à jour à partir d'un déploiement 2.x.x, procédez comme suit.

1. Téléchargez le CloudFormation modèle AWS de la solution.
2. Connectez-vous à la CloudFormation console AWS.
3. Sélectionnez la pile portant le nom fourni lors du déploiement et choisissez Mettre à jour.
4. Sur la page Mettre à jour la pile, sélectionnez Remplacer le modèle actuel, puis sélectionnez Télécharger un fichier modèle, puis téléchargez le fichier téléchargé à l'étape 1.
5. Choisissez Suivant.
6. Sur la page de détail de la pile, sous Paramètres, passez en revue les paramètres et modifiez-les si nécessaire.
7. Choisissez Suivant.
8. Sur la page Configurer les options de pile, sous Options d'échec de pile, assurez-vous que le bouton radio Comportement en cas d'échec du provisionnement est réglé sur Annuler toutes les ressources de la pile.
9. choisissez Next.
10. Sur la page Vérification, vérifiez et confirmez les paramètres. Cochez les cases indiquant que le modèle crée des ressources IAM et nécessite certaines fonctionnalités.
11. Choisissez Mettre à jour la pile pour déployer la pile.

Note

Si vous avez déployé la solution en mode de découverte de comptes autogéré, vous devez mettre à jour les ressources globales que vous avez déployées en suivant les étapes de la section Importer une région.

Résolution des problèmes

La résolution des problèmes connus fournit des instructions pour atténuer les erreurs connues. Si ces instructions ne répondent pas à votre problème, consultez la section Contacter le support AWS pour savoir comment ouvrir un dossier de support AWS pour cette solution.

Résolution des problèmes connus

Pendant le déploiement de Workload Discovery sur AWS et pendant la phase de post-déploiement, plusieurs erreurs de configuration courantes peuvent survenir :

> **Note**
>
> Pour faciliter le dépannage, nous vous recommandons de désactiver la fonctionnalité de restauration en cas d'échec dans le modèle AWS. CloudFormation Vous pouvez également trouver une aide supplémentaire pour résoudre les problèmes dans la documentation de configuration post-déploiement de Workload Discovery sur AWS.

Erreur du canal de distribution Config

Problème : L'erreur suivante se produit lors du déploiement du CloudFormation modèle AWS principal :

```
Failed to put delivery channel '<stack-name>-DiscoveryImport-<ID-string>-
DeliveryChannel-<ID-string>' because the maximum number of delivery channels:
 1 is reached. (Service: AmazonConfig; Status Code: 400; Error Code:
 MaxNumberOfDeliveryChannelsExceededException; Request ID: 4edc54bc-8c85-4925-
b99d-7ef9c73215b3; Proxy: null)
```

Raison : La solution est déployée dans une région dans laquelle AWS Config est déjà activé.

Résolution : suivez les instructions de la section des prérequis et déployez la solution avec le CloudFormation paramètre AlreadyHaveConfigSetupdéfini sur. `Yes`

Le délai de déploiement de Search Resolver Stack expire lors du déploiement sur un VPC existant

Problème : la pile imbriquée qui fournit une ressource personnalisée pour créer un index dans le OpenSearch cluster expire avec l'erreur suivante :

```
Embedded stack arn:aws:cloudformation:<region>::stack/<stack-name>-
SearchResolversStack-<ID-string>/<guid> was not successfullycreated: Stack creation
 time exceeded the specified timeout
```

Raison : Les sous-réseaux privés fournis en tant que CloudFormation paramètres ne peuvent pas être routés vers S3 (les ressources personnalisées doivent écrire le résultat de leur exécution dans un compartiment S3 à l'aide d'une URL présignée). Il y a généralement deux raisons à cela :

1. Les sous-réseaux privés ne sont pas associés à des passerelles NAT, il n'y a donc pas d'accès à Internet.
2. Le sous-réseau privé utilise des points de terminaison VPC au lieu d'une passerelle NAT et le point de terminaison de la passerelle S3 n'est pas configuré correctement.

Résolution :

1. Provisionnez des passerelles NAT dans le VPC pour permettre aux tâches exécutées dans des sous-réseaux privés d'accéder à Internet, soit à l'aide de l'interface de ligne de commande AWS, CloudFormation soit à l'aide de la CLI AWS, conformément à la documentation.
2. Assurez-vous que les tables de routage des sous-réseaux ont été mises à jour pour le point de terminaison VPC S3 conformément à la documentation.

Ressources non découvertes après l'importation du compte

Problème : les comptes ont été importés via l'interface utilisateur Web, mais aucune ressource ne semble avoir été découverte une fois le processus de découverte exécuté.

Motif : Les raisons les plus probables sont les suivantes,

1. Lorsque le CrossAccountDiscovery CloudFormation paramètre est défini sur`SELF_MANAGED`, le CloudFormation modèle de ressources globales n'a pas été déployé.

2. Lorsque le CrossAccountDiscovery CloudFormation paramètre est défini sur `AWS_ORGANIZATIONS` : un ou plusieurs comptes ne sont pas découverts et la colonne État du rôle contient des entrées Non déployées. Cela signifie qu'il y a eu un problème avec le déploiement automatique du modèle de ressources globales à l'aide de StackSets.
3. La tâche ECS du processus de découverte est à court de mémoire. Cela se produit lors de l'importation d'un grand nombre de comptes ou de ressources. La colonne Dernière découverte de l'interface utilisateur aura une valeur supérieure à celle spécifiée dans le DiscoveryTaskFrequency CloudFormation paramètre (la valeur par défaut est de 15 minutes) et une erreur de mémoire insuffisante se produira dans la console ECS.

Résolution :

1. Déployez le modèle de ressources globales dans les comptes requis, conformément à la documentation.
2. Accédez à la région WdGlobalResources StackSet dans laquelle Workload Discovery a été déployé et vérifiez les erreurs dans les instances de stack qui n'ont pas pu être déployées.
3. Mettez à jour le CloudFormation paramètre Memory à une valeur plus élevée : commencez par le double et augmentez jusqu'à ce que l'erreur cesse.

> **Note**
>
> Seules certaines combinaisons d'unités de processeur et de valeurs de mémoire sont valides, il se peut donc que vous deviez également mettre à jour le CpuUnits CloudFormation paramètre. La liste complète des combinaisons est répertoriée dans la documentation ECS.

Seules des ressources de configuration autres qu'AWS sont découvertes dans des comptes spécifiques

Problème : Les seuls types de ressources découverts par la solution sont ceux répertoriés dans le tableau de la section Ressources prises en charge.

Raison : Les causes les plus courantes de ce problème sont les suivantes :

1. Lorsque le CrossAccountDiscovery CloudFormation paramètre est défini sur`SELF_MANAGED`, le CloudFormation modèle de ressources régionales n'a pas été déployé dans les régions de chaque compte à découvrir.
2. Lorsque le CrossAccountDiscovery CloudFormation paramètre est défini sur`SELF_MANAGED`, le CloudFormation modèle de ressources régionales a été déployé dans les régions d'un certain nombre de comptes pour lesquels Config n'était pas activé, mais le CloudFormation paramètre AlreadyHaveConfigSetupétait défini par erreur sur. `Yes`
3. Lorsque le CrossAccountDiscovery CloudFormation paramètre est défini sur`AWS_ORGANIZATIONS`, AWS Config n'est pas activé dans les régions de chaque compte à découvrir. En `AWS_ORGANIZATIONS` mode, vous êtes responsable de l'activation de Config conformément aux politiques de votre organisation.

Résolution :

1. Déployez les modèles de ressources régionales dans les comptes requis, conformément à la documentation.
2. Supprimez la pile de ressources régionales précédemment déployée (dans le cas contraire, AWS Config sera dans un état incohérent) et redéployez-la avec le CloudFormation paramètre AlreadyHaveConfigSetupdéfini sur. `No`
3. Activez AWS Config dans les régions de chaque compte à découvrir.

Contacter AWS Support

Si vous bénéficiez d'AWS Developer Support, d'AWS Business Support ou d'AWS Enterprise Support, vous pouvez utiliser le Centre de support pour obtenir l'assistance d'experts concernant cette solution. Les sections suivantes fournissent des instructions.

Créer un dossier

1. Connectez-vous au Centre de Support.
2. Choisissez Create case (Créer une demande).

Comment pouvons-nous vous aider ?

1. Choisissez Technique.

2. Dans le champ Service, sélectionnez Solutions.
3. Dans Catégorie, sélectionnez Autres solutions.
4. Pour Severity, sélectionnez l'option qui correspond le mieux à votre cas d'utilisation.
5. Lorsque vous entrez le service, la catégorie et la gravité, l'interface contient des liens vers des questions de dépannage courantes. Si vous ne parvenez pas à résoudre votre question à l'aide de ces liens, sélectionnez Étape suivante : Informations supplémentaires.

Informations supplémentaires

1. Dans le champ Objet, saisissez un texte résumant votre question ou problème.
2. Dans le champ Description, décrivez le problème en détail.
3. Choisissez Joindre des fichiers.
4. Joignez les informations dont AWS Support a besoin pour traiter la demande.

Aidez-nous à résoudre votre cas plus rapidement

1. Entrez les informations demandées.
2. Choisissez Next step: Solve now or contact us (Étape suivante : résolvez maintenant ou contactez-nous).

Résolvez maintenant ou contactez-nous

1. Passez en revue les solutions Solve now.
2. Si vous ne parvenez pas à résoudre votre problème avec ces solutions, choisissez Contactez-nous, entrez les informations demandées, puis cliquez sur Soumettre.

Désinstallez la solution

Pour désinstaller la solution, utilisez l'AWS Management Console ou l'AWS Command Line Interface (AWS CLI). Tout d'abord, arrêtez toutes les tâches en cours d'exécution depuis le cluster Amazon ECS. Dans le cas contraire, la suppression de la pile risque d'échouer.

Utilisation de la AWS Management Console

1. Connectez-vous à la CloudFormation console AWS.
2. Sélectionnez la pile portant le nom fourni lors du déploiement.
3. Choisissez Supprimer la pile.

Utilisation de l'interface de ligne de commande AWS

Déterminez si l'AWS CLI est disponible dans votre environnement. Pour les instructions d'installation, reportez-vous à la section Qu'est-ce que l'interface de ligne de commande AWS dans le guide de l'utilisateur de l'AWS CLI.

Après avoir confirmé que l'AWS CLI est disponible, exécutez la commande suivante :

```
$ aws cloudformation delete-stack --stack-name <customer-defined-stack-name>
```

Manuel du développeur

Cette section fournit le code source de la solution ainsi que des personnalisations supplémentaires.

Code source

Consultez le GitHub référentiel Workload Discovery sur AWS pour télécharger les modèles et les scripts de cette solution et pour partager vos personnalisations avec d'autres utilisateurs.

Localisation des ressources de déploiement

Suivez ces étapes pour localiser les ressources déployées sur votre compte.

1. Connectez-vous à la CloudFormation console AWS.
2. Sélectionnez la région dans laquelle vous avez déployé la solution.

   En fonction de l'utilisation de ce compte, il peut contenir plusieurs piles pour différentes charges de travail. Il y aura une pile principale avec le nom fourni lors du déploiement et plusieurs piles imbriquées en dessous.
3. Sélectionnez chaque pile pour accéder aux ressources déployées à l'aide de ce modèle.
4. Sélectionnez l'onglet Ressources et cliquez sur le lien d'identification physique de la ressource concernée pour afficher la ressource dans sa console de service respective.

   Si vous connaissez l'ID logique d'une ressource, vous pouvez également effectuer une recherche à l'aide de la barre de recherche située au-dessus du tableau.

Ressources prises en charge

La solution prend en charge tous les types de ressources pris en charge par AWS Config, comme indiqué ici. Le tableau suivant contient les ressources prises en charge découvertes par Workload Discovery sur AWS et qui ne sont pas prises en charge par AWS Config. Les détails sont fournis dans la liste de documentation AWS correspondante.

Type de ressource	Source	Description
AWS::APIGateway::Authorizer	SDK	Obtenir des autorisateurs

Type de ressource	Source	Description
AWS::ApiGateway::Resource	SDK	Obtenir une ressource
AWS::ApiGateway::Method	SDK	Méthode Get
AWS::Cognito::UserPool	SDK	describeUserPool
AWS::ECS::Task	SDK	décrire les tâches
AWS::EKS::Nodegroup	SDK	Décrire le groupe de nœuds
AWS::DynamoDB::Stream	SDK	Décrivez Stream
Politique AWS : :IAM : : AWSManaged	SDK	getAccountAuthorizationDétails
AWS::ElasticLoadBalancingV2::TargetGroup	SDK	describeTargetGroups
AWS::EC2::Spot	SDK	describeSpotInstanceRequêtes
AWS::EC2::SpotFleet	SDK	describeSpotFleetRequêtes

Mode de découverte des comptes AWS Organizations

Lorsque Workload Discovery sur AWS est déployée dans une organisation AWS, la découverte des comptes n'est plus gérée via l'interface utilisateur Web de la solution. Dans ce cas, il n'est pas nécessaire de gérer le déploiement de CloudFormation modèles pour découvrir des comptes.

La solution utilise plutôt un agrégateur AWS Config à l'échelle de l'organisation AWS pour découvrir les ressources de tous les comptes de l'organisation sur lesquels AWS Config est activé.

Pour les types de ressources qui ne sont pas pris en charge par AWS Config, la solution déploie automatiquement un rôle IAM dans chaque compte de l'organisation utilisant AWS. CloudFormation StackSets Ce rôle permet au processus de découverte d'effectuer des appels au SDK dans tous les comptes de l'organisation pour découvrir ces ressources supplémentaires.

Ceci StackSet est configuré pour déployer automatiquement le rôle dans tous les nouveaux comptes ajoutés à l'organisation et supprimer le rôle de tous les comptes supprimés de l'organisation.

> **Note**
>
> Il n'est pas possible StackSet pour une instance de stack de déployer sur le compte de gestion. Si vous souhaitez que Workload Discovery découvre ce compte, vous devez déployer le modèle de ressources globales en utilisant la méthode de CloudFormation déploiement standard d'AWS décrite dans la CloudFormation section Déployer la pile pour provisionner les ressources globales à l'aide.

Actions du rôle de réplication Amazon S3

Le rôle IAM utilisé pour effectuer la réplication doit comporter les actions suivantes :

s3 : ReplicateObject
s3 : ReplicateDelete
s3 : ReplicateTags
s3 : ObjectOwnerOverrideToBucketOwner
s3 : ListBucket
s3 : GetReplicationConfiguration
s3 : GetObjectVersionForReplication
s3 : GetObjectVersionAcl
s3 : GetObjectVersionTagging
s3 : GetObjectRetention
s3 : GetObjectLegalHold

Pour vérifier que le rôle possède le rôle de réplication, procédez comme suit :

1. Copiez le nom du rôle dans l'assistant de réplication S3.
2. Connectez-vous à la console IAM depuis le compte dans lequel vous configurez la réplication.
3. Collez le nom du rôle dans le champ Search IAM.
4. Sélectionnez le premier élément dans la liste. Il s'agit du rôle IAM qui sera utilisé.
5. Sous Politiques d'autorisations, développez la politique gérée.
6. Assurez-vous que la politique comporte les actions détaillées dans le tableau précédent.

Politique de compartiment S3

Vous trouverez ci-dessous un exemple de politique de compartiment S3 qui CURs autorisera le téléchargement dans le compartiment, ainsi que des autorisations permettant aux comptes externes d'y répliquer des objets. Vous devez ajouter le rôle IAM de chaque compte AWS externe à cette politique pour accorder les autorisations nécessaires à la réplication.

```
   {
      "Version":"2012-10-17",
      "Id":"",
      "Statement":[
          {
            "Sid":"Set permissions for objects"
            "Effect":"Allow",
            "Principal":{
                "AWS":"arn-of-role-selected-in-replication-setup-in-source-account"
          },
      "Action":["s3:ReplicateObject",
      "s3:ReplicateDelete"],
"s3:ObjectOwnerOverrideToBucketOwner",
        "Resource":"arn:aws:s3:::destination-bucket-name/*"
      },
      {
          "Sid":"Set permissions on bucket",
          "Effect":"Allow",
          "Principal":{
                "AWS":"arn-of-role-selected-in-replication-setup-in-source-account"
      },

      "Action":["s3:GetBucketVersioning",
"s3:PutBucketVersioning"],
        "Resource":"arn:aws:s3:::destination-bucket-name "
```

```
      },
      {
          "Sid": "Stmt1335892150622",
          "Effect": "Allow",
          "Principal": {
              "Service": "billingreports.amazonaws.com"
          },
          "Action": [
              "s3:GetBucketAcl",
              "s3:GetBucketPolicy"
           ],
          "Resource": "arn:aws:s3:::destination-bucket-name"
      },
      {

          "Sid": "Stmt1335892526596",
          "Effect": "Allow",
          "Principal": {
              "Service": "billingreports.amazonaws.com"
          },
          "Action": "s3:PutObject",
          "Resource": "arn:aws:s3:::destination-bucket-name/*"

        }
    ]
  }
```

AWS APIs

Comme indiqué dans les conditions préalables, si vous déployez la solution sur un VPC existant, les services suivants doivent être accessibles depuis vos sous-réseaux privés.

API Gateway

- GetAuthorizers
- GetIntegration
- GetMethod
- GetResources
- GetRestApis

Cognito

- DescribeUserPool

Config

- BatchGetAggregateResourceConfig
- DescribeConfigurationAggregators
- ListAggregateDiscoveredResources
- SelectAggregateResourceConfig

DynamoDB Streams

- DescribeStream

Amazon EC2

- DescribeInstances
- DescribeSpotFleetRequests
- DescribeSpotInstanceRequests
- DescribeTransitGatewayAttachments

Amazon Elastic Load Balancer

- DescribeLoadBalancers
- DescribeListeners
- DescribeTargetGroups
- DescribeTargetHealth

Amazon Elastic Kubernetes Service

- DescribeNodegroup
- ListNodegroups

IAM

- GetAccountAuthorizationDetails
- ListPolicies

Lambda

- GetFunction
- GetFunctionConfiguration
- ListEventSourceMappings

OpenSearch Service

- DescribeDomains
- ListDomainNames

Organizations

- ListAccounts
- ListAccountsForParent
- ListOrganizationalUnitsForParent
- ListRoots

Amazon Simple Notification Service

- ListSubscriptions

Service de jetons de sécurité Amazon

- AssumeRole

Référence

Cette section inclut des informations sur une fonctionnalité facultative permettant de collecter des métriques uniques pour cette solution, ainsi qu'une liste des créateurs qui ont contribué à cette solution.

Collecte de données anonymisée

Cette solution inclut une option permettant d'envoyer des métriques opérationnelles anonymisées à AWS. Nous utilisons ces données pour mieux comprendre la façon dont les clients utilisent cette solution et les services et produits associés. Une fois activé, les informations suivantes sont collectées et envoyées à AWS :

- ID de solution : identifiant de solution AWS
- ID unique (UUID) : identifiant unique généré aléatoirement pour chaque déploiement
- Horodatage - Horodatage de la collecte de données
- Fonction de coût activée - Informations indiquant si l'utilisateur utilise la fonctionnalité de coût
- Nombre de comptes : nombre de comptes que l'utilisateur a intégrés lors de son déploiement
- Nombre de diagrammes : nombre de diagrammes créés dans chaque déploiement
- Nombre de ressources : nombre de ressources découvertes dans tous les comptes intégrés

AWS est propriétaire des données collectées dans le cadre de cette enquête. La collecte de données est soumise à l'avis de confidentialité. Pour désactiver cette fonctionnalité, suivez les étapes ci-dessous avant de lancer le CloudFormation modèle AWS.

1. Téléchargez le CloudFormation modèle AWS sur votre disque dur local.
2. Ouvrez le CloudFormation modèle AWS dans un éditeur de texte.
3. Modifiez la section de mappage des CloudFormation modèles AWS à partir de :

```
Mappings:
  Solution:
    Metrics:
      CollectAnonymizedUsageMetrics: 'true'
```

par :

```
Mappings:
  Solution:
    Metrics:
      CollectAnonymizedUsageMetrics: 'false'
```

1. Connectez-vous à la CloudFormation console AWS.
2. Sélectionnez Créer une pile.
3. Sur la page Créer une pile, section Spécifier le modèle, sélectionnez Télécharger un fichier modèle.
4. Sous Télécharger un fichier modèle, choisissez Choisir un fichier et sélectionnez le modèle modifié sur votre disque local.
5. Choisissez Next et suivez les étapes décrites dans Lancer la pile.

Collaborateurs

- Mohsan Jaffery
- Matthieu Ball
- Stefano Vozza
- Connor Kirkpatrick
- Chris Deigan
- Nick Lee
- Tim Mekari

Révisions

Date de publication : septembre 2020. Pour les mises à jour, reportez-vous au fichier ChangeLog.md dans le référentiel. GitHub

Reportez-vous au fichier ChangeLog.md dans le référentiel. GitHub

Avis

Il incombe aux clients de procéder à une évaluation indépendante des informations contenues dans le présent document. Ce document : (a) est fourni à titre informatif uniquement, (b) représente les offres de produits et les pratiques actuelles d'AWS, qui sont susceptibles d'être modifiées sans préavis, et (c) ne crée aucun engagement ni aucune garantie de la part d'AWS et de ses filiales, fournisseurs ou concédants de licence. Les produits ou services AWS sont fournis « tels quels » sans garanties, déclarations ou conditions d'aucune sorte, qu'elles soient explicites ou implicites. Les responsabilités et obligations d'AWS vis-à-vis de ses clients sont régies par les contrats AWS. Le présent document ne fait partie d'aucun, et ne modifie aucun, contrat entre AWS et ses clients.

La solution est concédée sous licence selon les termes de la licence Apache, version 2.0.

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.