Guía de implementación

Descubrimiento de cargas de trabajo en AWS

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

Descubrimiento de cargas de trabajo en AWS: Guía de implementación

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

Las marcas comerciales y la imagen comercial de Amazon no se pueden utilizar en relación con ningún producto o servicio que no sea de Amazon, de ninguna manera que pueda causar confusión entre los clientes y que menosprecie o desacredite a Amazon. Todas las demás marcas registradas que no son propiedad de Amazon son propiedad de sus respectivos propietarios, que pueden o no estar afiliados, conectados o patrocinados por Amazon.

Table of Contents

Información general de la solución 1
Características y ventajas 2
Casos de uso 3
Conceptos y definiciones 4
Información general de la arquitectura 5
Diagrama de arquitectura 5
Consideraciones sobre el diseño de AWS Well-Architected 7
Excelencia operativa 7
Seguridad 7
Fiabilidad 8
Eficiencia del rendimiento 8
Optimización de costos 9
Sostenibilidad 9
Detalles de la arquitectura 10
Mecanismo de autenticación 10
Recursos admitidos 10
Descubrimiento de cargas de trabajo en la administración de diagramas de arquitectura de AWS 10
Interfaz de usuario web y administración del almacenamiento 10
Componente de datos 12
Componente de despliegue de imágenes 13
Componente de descubrimiento 13
Componente de costo 14
Los servicios de AWS en esta solución 15
Planificación de la implementación 18
Regiones de AWS admitidas 18
Costo 19
Ejemplos de tablas de costos 19
Seguridad 21
Acceso a recursos 21
Acceso a la red 22
Configuración de aplicaciones 22
Cuotas 23
Cuotas para los servicios de AWS en esta solución 23

CloudFormation Cuotas de AWS 24
Cuotas de AWS Lambda 24
Cuotas de Amazon VPC 24
Elegir la cuenta de despliegue 25
Implementación de la solución 26
Información general del proceso de implementación 26
Requisitos previos 26
Recopile detalles de los parámetros de implementación 26
CloudFormation Plantilla de AWS 29
Lanzar la pila 29
Tareas de configuración posteriores al despliegue 39
Activar la seguridad avanzada en Amazon Cognito 39
Crear usuarios de Amazon Cognito 39
Para crear usuarios adicionales: 39
Inicie sesión en Workload Discovery en AWS 41
Importa una región 41
Importar una región 42
Implemente las CloudFormation plantillas de AWS 44
Se utiliza CloudFormation StackSets para aprovisionar recursos globales en todas las cuentas 44
Se utiliza CloudFormation StackSets para aprovisionar recursos regionales 45
Implemente la pila para aprovisionar los recursos globales mediante CloudFormation 47
Implemente la pila para aprovisionar los recursos regionales mediante CloudFormation 48
Compruebe que la región se haya importado correctamente 49
Configure la función de coste 50
Cree el informe de costo y uso de AWS en la cuenta de implementación 50
Crear el informe de costos y uso de AWS en una cuenta externa 51
Configure la replicación 52
Edite las políticas del ciclo de vida de los cubos 54
Supervisión de la solución 55
myApplications 55
CloudWatch AppInsights 55
Actualización de la solución 57
Solución de problemas 58
Resolución de problemas conocidos 58
Error de Config Delivery Channel 58

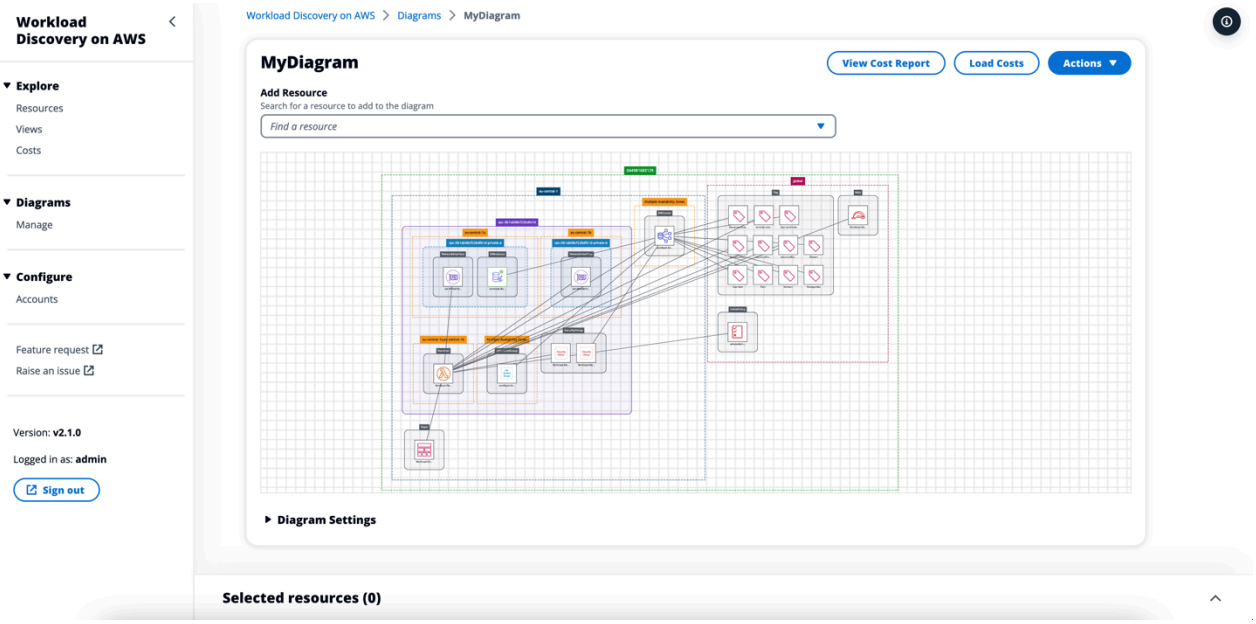
Se agota el tiempo de espera para la implementación de Search Resolver Stack cuando se implementa en una VPC existente ... 59
Los recursos no se descubren después de importar la cuenta ... 59
Solo se descubren recursos que no son de AWS Config en cuentas específicas ... 60
Póngase en contacto con AWS Support. ... 61
Cree un caso ... 61
¿Cómo podemos ayudar? ... 61
Información adicional ... 62
Ayúdenos a resolver su caso más rápido ... 62
Resuelva ahora o póngase en contacto con nosotros ... 62
Desinstalar la solución ... 63
Uso de Consola de administración de AWS ... 63
Uso de la interfaz de línea de comandos de AWS ... 63
Guía para desarrolladores ... 64
Código fuente ... 64
Localizar los recursos de implementación ... 64
Recursos admitidos ... 64
Modo de descubrimiento de cuentas de AWS Organizations ... 65
Acciones de la función de replicación de Amazon S3 ... 66
Política de bucket de S3 ... 67
AWS APIs ... 68
API Gateway ... 68
Cognito ... 69
Config ... 69
DynamoDB Streams ... 69
Amazon EC2 ... 69
Amazon Elastic Load Balancer ... 69
Amazon Elastic Kubernetes Service ... 69
IAM ... 70
Lambda ... 70
OpenSearch Servicio ... 70
Organizations ... 70
Amazon Simple Notification Service ... 70
Amazon Security Token Service ... 70
Referencia ... 71
Recopilación de datos anonimizados ... 71

Colaboradores 72
Revisiones 73
Avisos 74
..... lxxv

Implemente una herramienta de visualización que genere automáticamente diagramas de arquitectura de las cargas de trabajo en la nube de AWS

La supervisión de las cargas de trabajo en la nube de Amazon Web Services (AWS) es fundamental para mantener el buen estado y la eficiencia de las operaciones. Sin embargo, hacer un seguimiento de los recursos de AWS y de las relaciones entre ellos puede ser un desafío. Workload Discovery en AWS es una herramienta de visualización que genera automáticamente diagramas de arquitectura de la carga de trabajo en AWS. Puede usar esta solución para crear, personalizar y compartir visualizaciones detalladas de las cargas de trabajo basadas en datos en tiempo real de AWS.

Esta solución funciona manteniendo un inventario de los recursos de AWS en sus cuentas y regiones, mapeando las relaciones entre ellas y mostrándolas en una interfaz de usuario web (interfaz de usuario web). Al realizar cambios en un recurso, Workload Discovery on AWS le ahorra tiempo al proporcionar un enlace al recurso en la consola de administración de AWS.



Ejemplo de diagrama de arquitectura generado por Workload Discovery en AWS

Esta guía de implementación describe las consideraciones arquitectónicas y los pasos de configuración para implementar Workload Discovery en AWS en la nube de AWS. Incluye enlaces a una CloudFormation plantilla de AWS que lanza y configura los servicios de AWS necesarios para implementar esta solución utilizando las prácticas recomendadas de AWS en materia de seguridad y disponibilidad.

El público objetivo para implementar la solución Workload Discovery on AWS en su entorno incluye arquitectos de soluciones, responsables de la toma de decisiones empresariales, DevOps ingenieros, científicos de datos y profesionales de la nube.

Utilice esta tabla de navegación para encontrar rápidamente las respuestas a estas preguntas:

Si quiere…	Lea…
Conocer el costo de ejecutar esta solución. El costo estimado de ejecutar esta solución en la región de EE. UU. Este (Virginia del Norte) es de 425,19 USD al mes.	Costo
Comprender las consideraciones de seguridad de esta solución.	Seguridad
Saber cómo planificar las cuotas de esta solución.	Cuotas
Conozca qué regiones de AWS admiten esta solución.	Regiones de AWS admitidas
Consulte o descargue la CloudFormation plantilla de AWS incluida en esta solución para implementar automáticamente los recursos de infraestructura (la «pila») de esta solución.	CloudFormation Plantilla de AWS
Acceda al código fuente.	GitHub repositorio

Características y ventajas

Workload Discovery en AWS ofrece las siguientes funciones:

Cree diagramas de arquitectura con datos prácticamente en tiempo real

Workload Discovery on AWS escanea sus cuentas cada 15 minutos para garantizar que los diagramas que cree sean una representación precisa y actualizada de sus cargas de trabajo.

Vea los recursos de varias cuentas y regiones en un solo lugar

La solución mantiene un inventario de los recursos de AWS en todas sus cuentas y regiones de AWS en una base de datos gráfica centralizada, lo que le permite explorar varias cuentas y regiones y sus relaciones entre sí en una única interfaz de usuario.

Integración de AWS Organizations

Al implementar la solución con AWS Organizations, Workload Discovery en AWS descubrirá automáticamente todos los recursos compatibles de su organización. En esta configuración, no es necesario administrar directamente la implementación de CloudFormation plantillas específicas de cuentas para que estas estén disponibles para su detección.

Recopile los datos de costes de sus cargas de trabajo

Cuando está habilitada, la función de costo le permite buscar recursos en su cuenta por costo y agregar los recursos que encuentre a un diagrama. También puede agregar datos de costos a los diagramas ya existentes.

Exporta a diagrams.net (anteriormente draw.io)

Workload Discovery en AWS puede exportar sus diagramas para que pueda anotarlos con más detalle con este software de dibujo de terceros.

Integración con AWS Service Catalog AppRegistry y Application Manager, una funcionalidad de AWS Systems Manager

Esta solución incluye un AppRegistry recurso de Service Catalog para registrar la CloudFormation plantilla de la solución y sus recursos subyacentes como una aplicación tanto en Service Catalog AppRegistry como en Application Manager. Con esta integración, puede administrar de forma centralizada los recursos de la solución y habilitar las acciones de búsqueda, generación de informes y administración de aplicaciones.

Casos de uso

Revisiones de diseño y seguridad

Utilice esta solución para generar diagramas de arquitectura que validen que la implementación de una carga de trabajo coincide con el diseño propuesto.

Explore y documente las cargas de trabajo existentes

Cree diagramas de arquitectura para explorar las cargas de trabajo en las que existe poca documentación o que se implementaron manualmente sin infraestructura como código.

Visualice los costos

Genere un informe de costos para sus diagramas de arquitectura que contenga una visión general del costo estimado.

Conceptos y definiciones

En esta sección se describen los conceptos clave y se define la terminología específica de esta solución:

recurso

Un recurso de AWS, como un bucket de Amazon Simple Storage Service (Amazon S3) o una función de AWS Lambda.

relación

Un enlace entre dos recursos, como un rol de AWS Identity and Access Management (IAM) y una función de AWS Lambda asociada.

tipo de recurso

La categoría de clasificación de un recurso. Sigue siempre la convención de CloudFormation nomenclatura, por ejemplo`AWS::Lambda::Function`.

discovery

El proceso que inicia la solución para mapear los recursos y sus relaciones en sus cuentas y regiones de AWS.

modo de descubrimiento de cuentas

El método para detectar cuentas y añadirlas a la solución: autogestionadas mediante la interfaz de usuario de Workload Discovery en AWS o delegadas a AWS Organizations.

> **Note**
>
> Para obtener una referencia general de los términos de AWS, consulte el glosario de AWS.

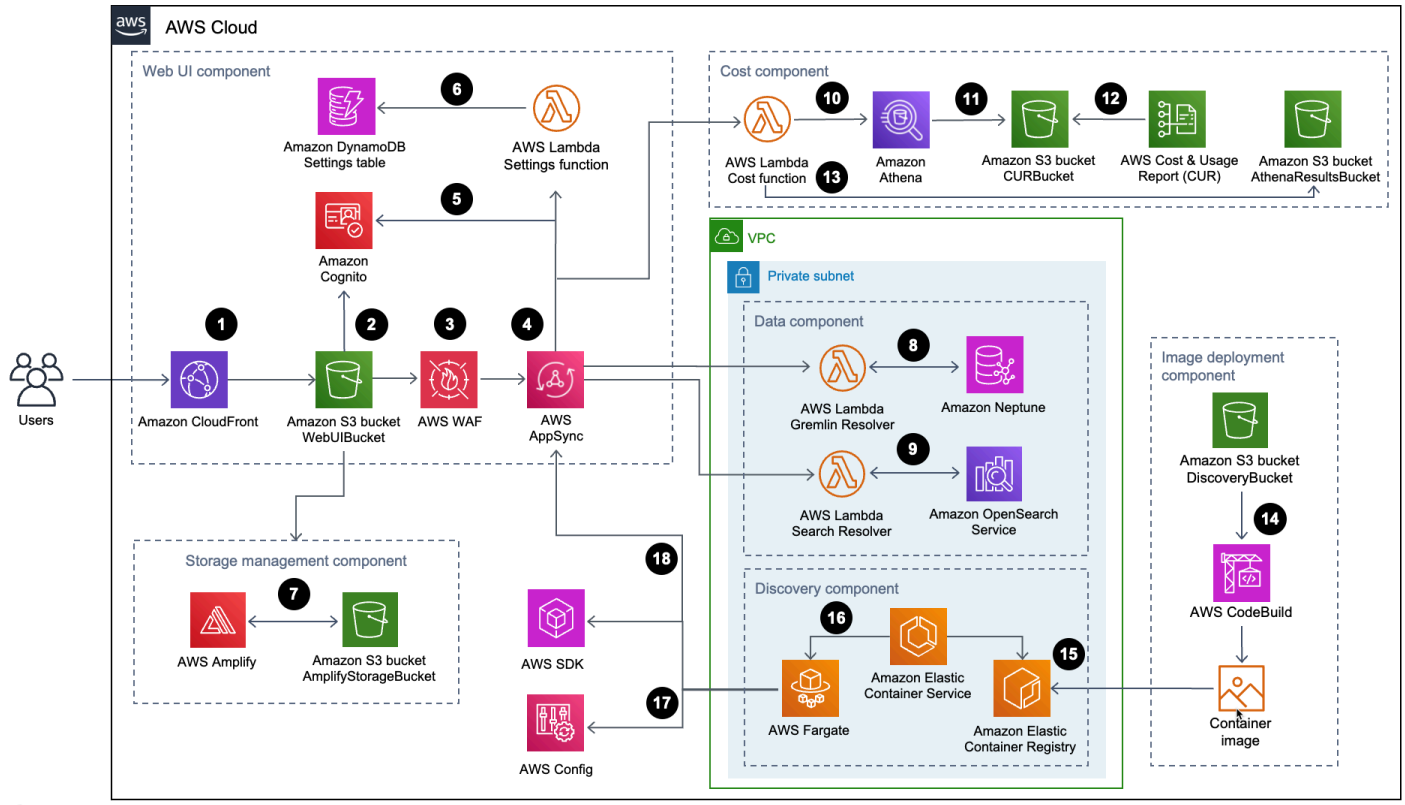
Información general de la arquitectura

En esta sección se proporciona un diagrama de arquitectura de implementación de referencia para los componentes implementados con esta solución.

Diagrama de arquitectura

Al implementar esta solución con los parámetros predeterminados, se crea el siguiente entorno en la nube de AWS.

Descubrimiento de cargas de trabajo en la arquitectura de AWS



El flujo de proceso de alto nivel para los componentes de la solución implementados con la CloudFormation plantilla de AWS es el siguiente:

1. HTTP Strict-Transport-Security (HSTS) añade encabezados de seguridad a cada respuesta de la distribución de Amazon CloudFront.
2. Un bucket de Amazon Simple Storage Service (Amazon S3) aloja la interfaz de usuario web, que se distribuye con Amazon CloudFront. Amazon Cognito autentica el acceso de los usuarios a la interfaz de usuario web.

3. AWS WAF protege la AppSync API de vulnerabilidades y bots comunes que pueden afectar a la disponibilidad, comprometer la seguridad o consumir recursos excesivos.
4. AppSyncLos puntos de enlace de AWS permiten que el componente de la interfaz de usuario web solicite datos de relaciones entre recursos, consulte los costos, importe nuevas regiones de AWS y actualice las preferencias. AWS AppSync también permite que el componente de descubrimiento almacene datos persistentes en las bases de datos de la solución.
5. AWS AppSync utiliza los JSON Web Tokens (JWTs) aprovisionados por Amazon Cognito para autenticar cada solicitud.
6. La función `Settings` AWS Lambda conserva las regiones importadas y otras configuraciones en Amazon DynamoDB.
7. La solución implementa AWS Amplify y un bucket de Amazon S3 como componente de administración del almacenamiento para almacenar las preferencias de los usuarios y los diagramas de arquitectura guardados.
8. El componente de datos utiliza la función `Gremlin Resolver` AWS Lambda para consultar y devolver datos de una base de datos de Amazon Neptune.
9. El componente de datos utiliza la función `Search Resolver` Lambda para consultar y conservar los datos de los recursos en un dominio de Amazon OpenSearch Service.
10. La función `Cost` Lambda usa Amazon Athena para consultar los informes de costo y uso de AWS (AWS CUR) a fin de proporcionar datos de costos estimados a la interfaz de usuario web.
11. Amazon Athena ejecuta consultas en AWS CUR.
12. AWS CUR entrega los informes al bucket de `CostAndUsageReportBucket` Amazon S3.
13. La función `Cost` Lambda almacena los resultados de Amazon Athena en el bucket de Amazon `AthenaResultsBucket` S3.
14. AWS CodeBuild crea la imagen del contenedor del componente de descubrimiento en el componente de implementación de la imagen.
15. Amazon Elastic Container Registry (Amazon ECR) contiene una imagen de Docker proporcionada por el componente de despliegue de imágenes.
16. Amazon Elastic Container Service (Amazon ECS) administra la tarea de AWS Fargate y proporciona la configuración necesaria para ejecutarla. AWS Fargate ejecuta una tarea de contenedor cada 15 minutos para actualizar los datos de inventario y recursos.
17. Las llamadas a AWS Config y AWS SDK ayudan al componente de descubrimiento a mantener un inventario de los datos de recursos de las regiones importadas y, a continuación, a almacenar sus resultados en el componente de datos.

18La tarea de AWS Fargate conserva los resultados de las llamadas a AWS Config y al SDK de AWS en una base de datos de Amazon Neptune y en un dominio de OpenSearch Amazon Service con las llamadas a la API. AppSync

Consideraciones sobre el diseño de AWS Well-Architected

Esta solución utiliza las mejores prácticas del AWS Well-Architected Framework, que ayuda a los clientes a diseñar y operar cargas de trabajo confiables, seguras, eficientes y rentables en la nube.

En esta sección se describe cómo los principios de diseño y las prácticas recomendadas de Well-Architected Framework benefician a esta solución.

Excelencia operativa

Diseñamos esta solución utilizando los principios y las mejores prácticas del pilar de la excelencia operativa en beneficio de esta solución.

- Los recursos definidos como infraestructura son como el uso CloudFormation de código.
- La solución envía las métricas CloudWatch a Amazon para proporcionar observabilidad en la infraestructura, las funciones de Lambda, las tareas de Amazon ECS, los buckets de AWS S3 y el resto de los componentes de la solución.

Seguridad

Diseñamos la arquitectura de esta solución utilizando los principios y las mejores prácticas del pilar de la seguridad en beneficio de esta solución.

- Amazon Cognito autentica y autoriza a los usuarios de la aplicación de interfaz de usuario web.
- Todas las funciones que utiliza la solución se basan en el acceso con el mínimo privilegio. En otras palabras, solo contienen los permisos mínimos necesarios para que el servicio pueda funcionar correctamente.
- Los datos en reposo y en tránsito se cifran mediante claves almacenadas en AWS Key Management Service (AWS KMS), un almacén dedicado a la administración de claves.
- Las credenciales tienen una caducidad breve y siguen una política de contraseñas segura.
- Las directivas GraphQL de AppSync seguridad de AWS proporcionan un control detallado sobre las operaciones que pueden invocar el frontend y el backend.

- El registro, el rastreo y el control de versiones están activados cuando corresponde.
- La aplicación automática de parches (versión secundaria) y la creación de instantáneas están activadas cuando corresponde.
- El acceso a la red es privado de forma predeterminada y los puntos de conexión de Amazon Virtual Private Cloud (Amazon VPC) están activados cuando están disponibles.

Fiabilidad

Diseñamos esta solución utilizando los principios y las mejores prácticas del pilar de la confiabilidad para aprovechar esta solución.

- La solución utiliza los servicios sin servidor de AWS siempre que es posible para garantizar la alta disponibilidad y la recuperación en caso de fallo del servicio.
- Todo el procesamiento informático utiliza funciones de Lambda o Amazon ECS en AWS Fargate.
- Todo el código personalizado utiliza el SDK de AWS y las solicitudes se limitan por parte del cliente para evitar que se alcancen las cuotas de velocidad de la API.

Eficiencia del rendimiento

Diseñamos esta solución utilizando los principios y las mejores prácticas del pilar de la eficiencia del rendimiento en beneficio de esta solución.

- La solución utiliza la arquitectura sin servidor de AWS siempre que es posible. Esto elimina la carga operativa que supone la administración de servidores físicos.
- La solución se puede lanzar en cualquier región que admita los servicios de AWS utilizados en esta solución, como AWS Lambda, Amazon Neptune, AppSync AWS, Amazon S3 y Amazon Cognito.
- En las regiones compatibles, Amazon Neptune sin servidor le permite ejecutar y escalar al instante cargas de trabajo de gráficos, sin necesidad de administrar ni optimizar la capacidad de la base de datos.
- La solución utiliza servicios gestionados en todo momento para reducir la carga operativa que supone el aprovisionamiento y la administración de los recursos.

Optimización de costos

Diseñamos esta solución utilizando los principios y las mejores prácticas del pilar de la optimización de costes en beneficio de esta solución.

- AWS ECS en AWS Fargate utiliza funciones de Lambda exclusivamente para el procesamiento y solo cobra en función del uso.
- Amazon DynamoDB escala la capacidad a pedido, de modo que solo paga por la capacidad que utilice.

Sostenibilidad

Diseñamos esta solución utilizando los principios y las mejores prácticas del pilar de la sostenibilidad en beneficio de esta solución.

- La solución utiliza servicios gestionados y sin servidor siempre que es posible para minimizar el impacto ambiental de los servicios de backend.

Detalles de la arquitectura

En esta sección se describen los componentes y los servicios de AWS que componen esta solución y los detalles de la arquitectura sobre cómo funcionan juntos estos componentes.

Mecanismo de autenticación

Workload Discovery en AWS utiliza un grupo de usuarios de Amazon Cognito tanto para la interfaz de usuario como para la autenticación de AWS AppSync . Una vez autenticado, Amazon Cognito proporciona un token web JSON (JWT) a la interfaz de usuario web que se proporcionará con todas las solicitudes de API posteriores. Si no se proporciona un JWT válido, la solicitud de API fallará y devolverá una respuesta HTTP 403 Forbidden.

Recursos admitidos

Para obtener una lista de los tipos de recursos de AWS que Workload Discovery on AWS puede encontrar en sus cuentas y regiones, consulte Recursos compatibles.

Descubrimiento de cargas de trabajo en la administración de diagramas de arquitectura de AWS

Puede guardar Workload Discovery en los diagramas de arquitectura de AWS mediante la interfaz de usuario web, donde se pueden realizar operaciones de creación, lectura, actualización y eliminación (CRUD). La API de almacenamiento AWS Amplify permite a Workload Discovery en AWS almacenar diagramas de arquitectura en un bucket de Amazon S3. Hay dos niveles de permisos disponibles:

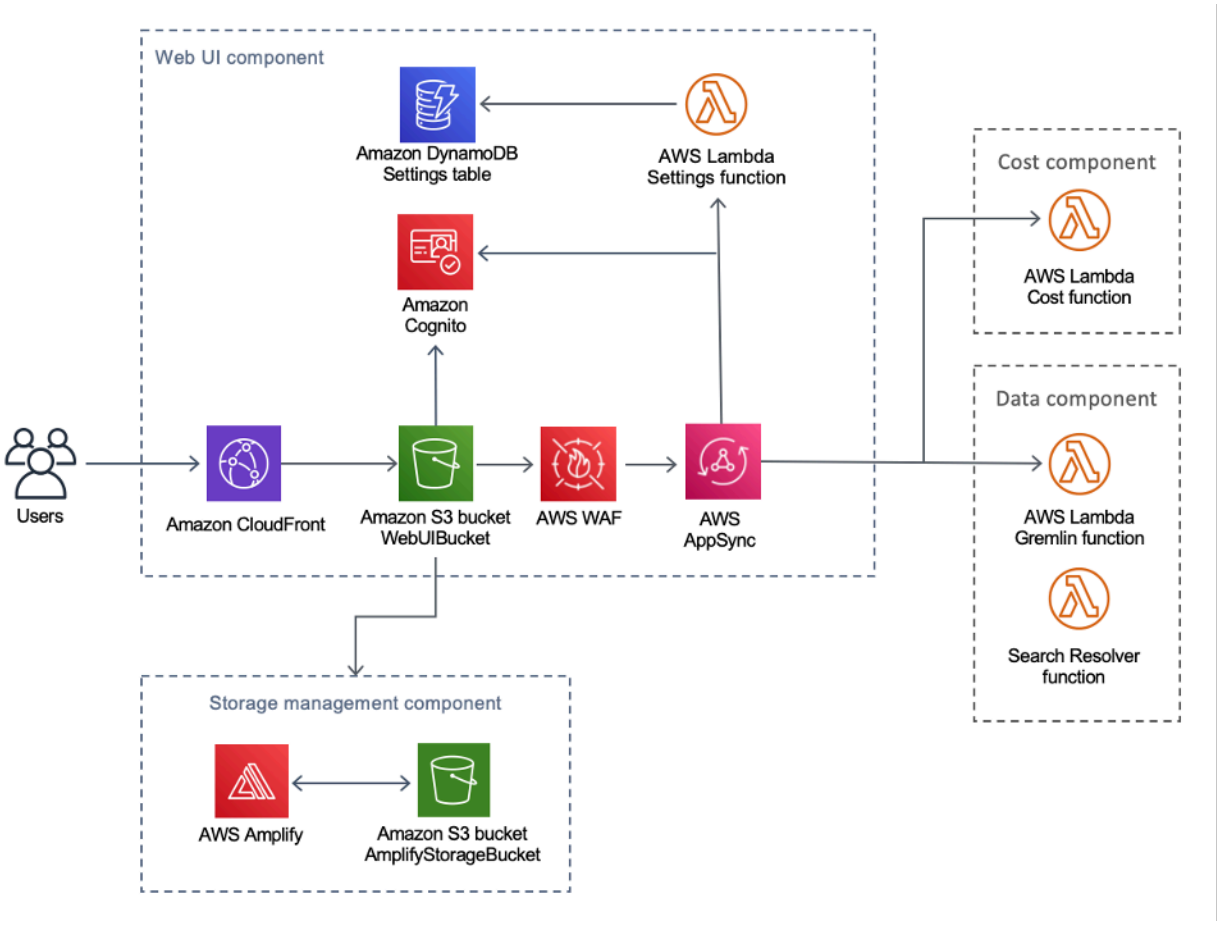
- Todos los usuarios: permite que los usuarios de Workload Discovery on AWS puedan ver los diagramas de arquitectura de Workload Discovery on AWS de su implementación. Los usuarios pueden descargar y editar estos diagramas.
- Tú: permite que Workload Discovery en los diagramas de arquitectura de AWS solo sea visible para el creador. Los demás usuarios no podrán verlos.

Interfaz de usuario web y administración del almacenamiento

Desarrollamos la interfaz de usuario web usando React. La interfaz de usuario web proporciona una consola frontend que permite a los usuarios interactuar con Workload Discovery en AWS.

Amazon CloudFront está configurado para añadir encabezados seguros a todas las solicitudes HTTP de la interfaz de usuario web. Esto proporciona un nivel de seguridad adicional que lo protege contra ataques como el cross-site scripting (XSS).

Descubrimiento de cargas de trabajo en la interfaz de usuario web de AWS y componentes de administración del almacenamiento

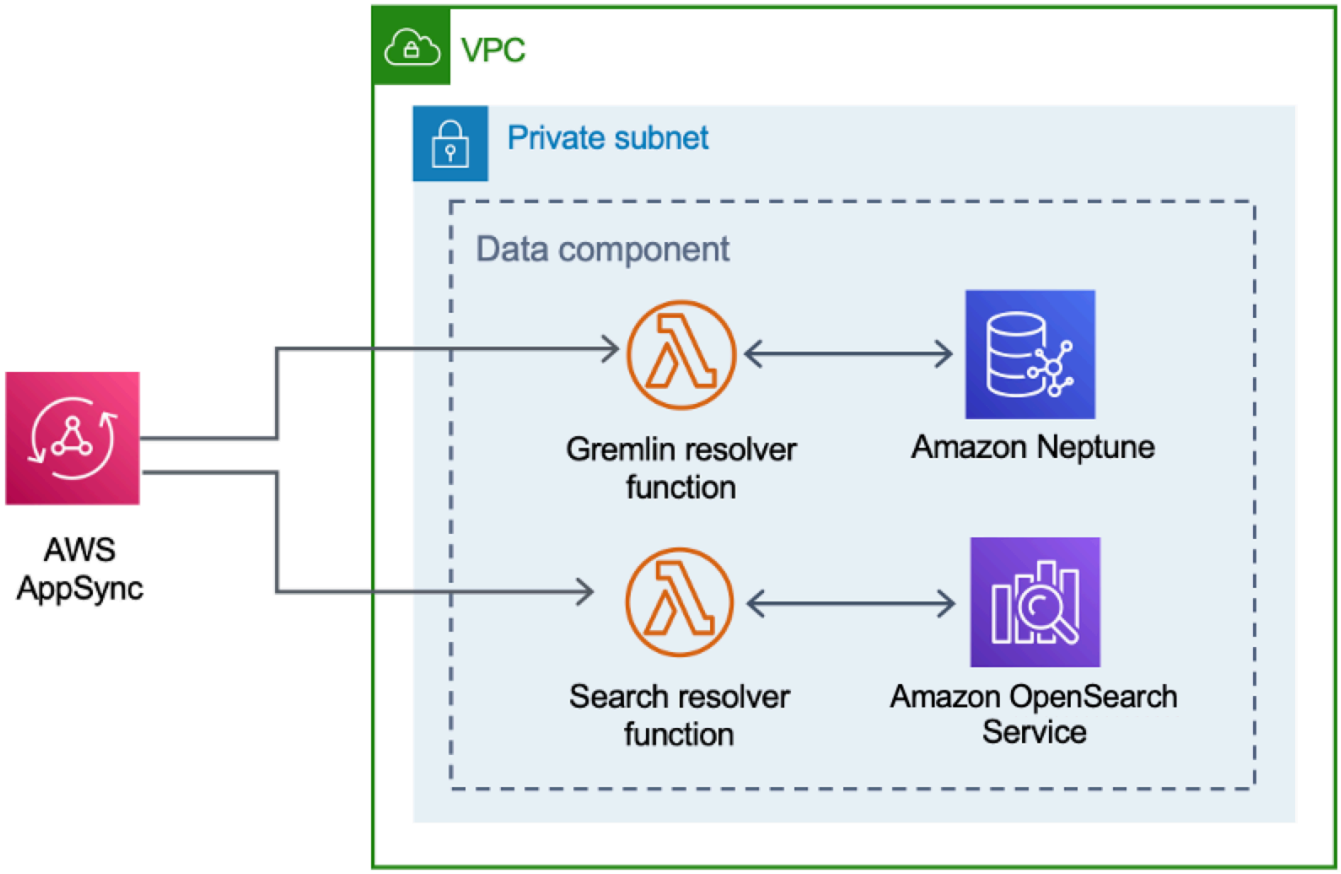


Los recursos de la interfaz de usuario web se alojan en el bucket de `WebUIBucket` Amazon S3 y Amazon los distribuye CloudFront. AWS Amplify proporciona una capa de abstracción para simplificar las integraciones con AWS y AppSync Amazon S3.

Esta solución utiliza AWS AppSync para facilitar la interacción con las diversas configuraciones disponibles para Workload Discovery en AWS, incluida la administración de regiones importadas. AWS AppSync utiliza la función `Settings` AWS Lambda para gestionar solicitudes como la importación de una nueva cuenta o región.

Componente de datos

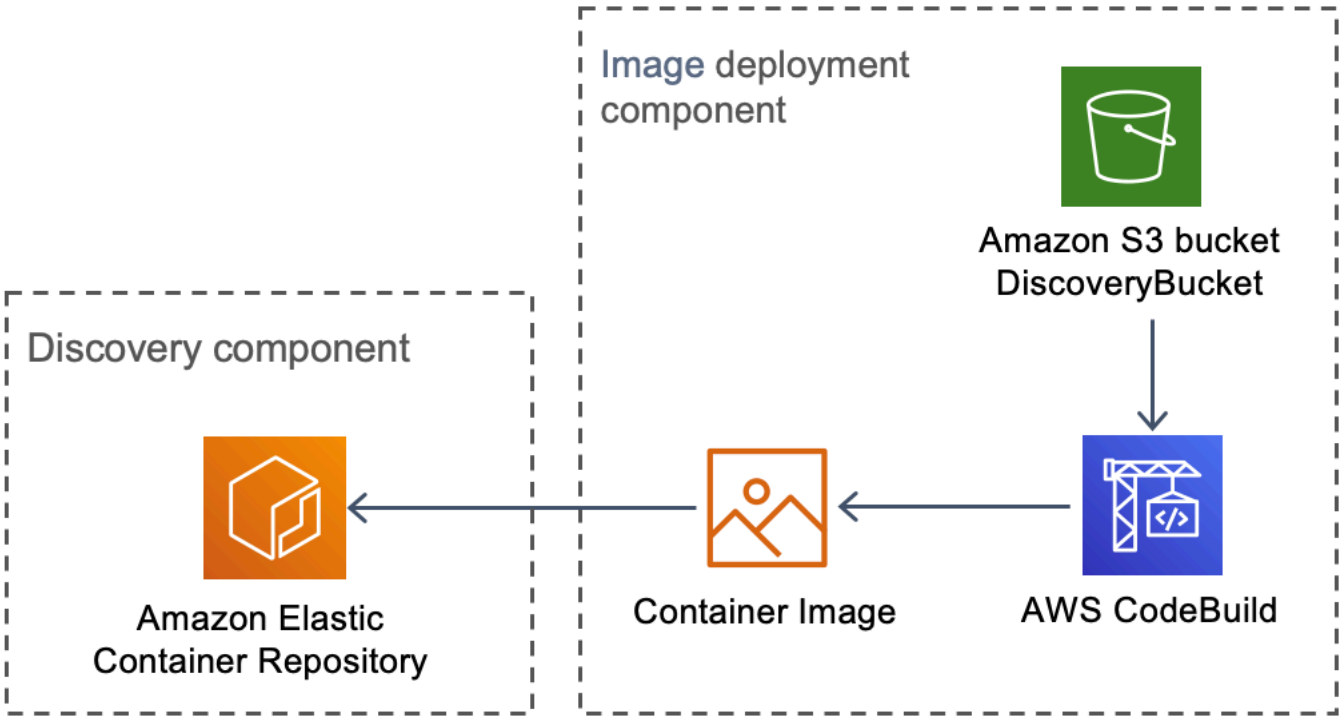
Descubrimiento de cargas de trabajo en el componente de datos de AWS



La interfaz de usuario web envía solicitudes a la AppSync API, que invoca las funciones `Gremlin Resolver` o las de `Search Resolver` Lambda. Estas funciones procesan las solicitudes y consultan a Amazon Neptune o OpenSearch Service para recuperar datos sobre los recursos proporcionados. AWS AppSync también admite las solicitudes de datos de costos estimados del CUR de AWS.

El componente de descubrimiento envía solicitudes a la AppSync API para leer y conservar datos en las bases de datos de Amazon Neptune y OpenSearch Service. La API recibe solicitudes de la tarea de AWS Fargate en el componente de descubrimiento. A continuación, la API se autentica mediante una función de IAM que proporciona acceso a las bases de datos.

Componente de despliegue de imágenes



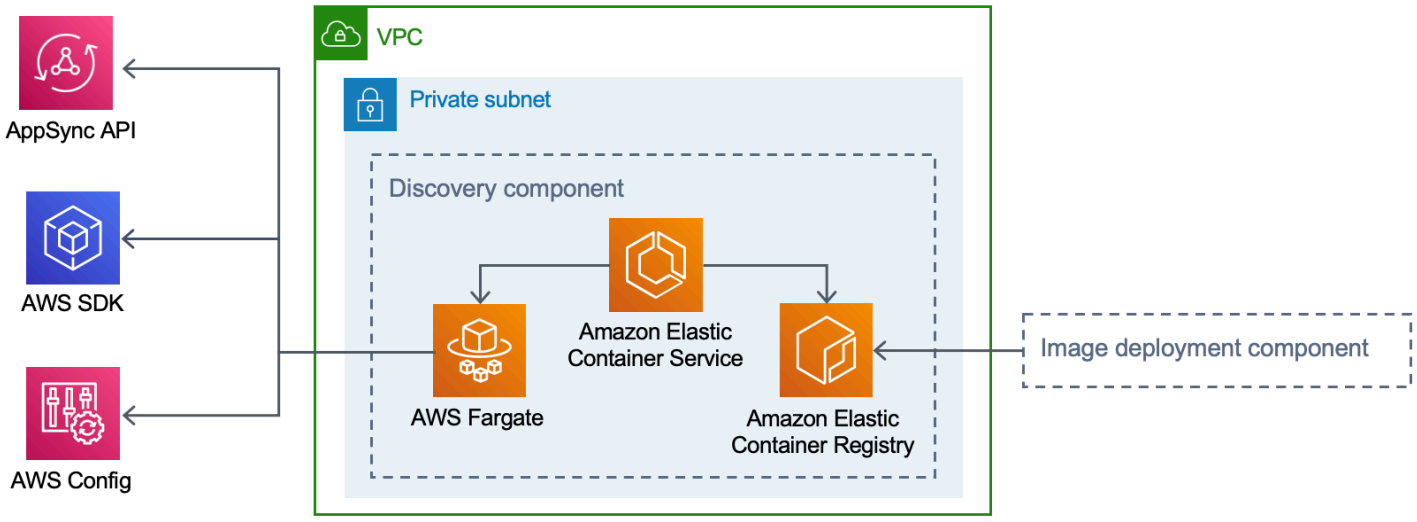
Componente de despliegue de imágenes de Workload Discovery en AWS

El componente de despliegue de imágenes crea la imagen de contenedor que utiliza el componente de descubrimiento. El bucket `DiscoveryBucket` y Amazon S3 alojan el código, que puede descargarse en el momento de la implementación mediante un CodeBuild trabajo de AWS que crea la imagen del contenedor y la carga en Amazon ECR.

Componente de descubrimiento

El componente de descubrimiento es el principal elemento de recopilación de datos de la arquitectura Workload Discovery on AWS. Es responsable de consultar AWS Config y de describir las llamadas a la API para mantener el inventario de los recursos y sus relaciones entre sí.

Componente de descubrimiento de cargas de trabajo en AWS



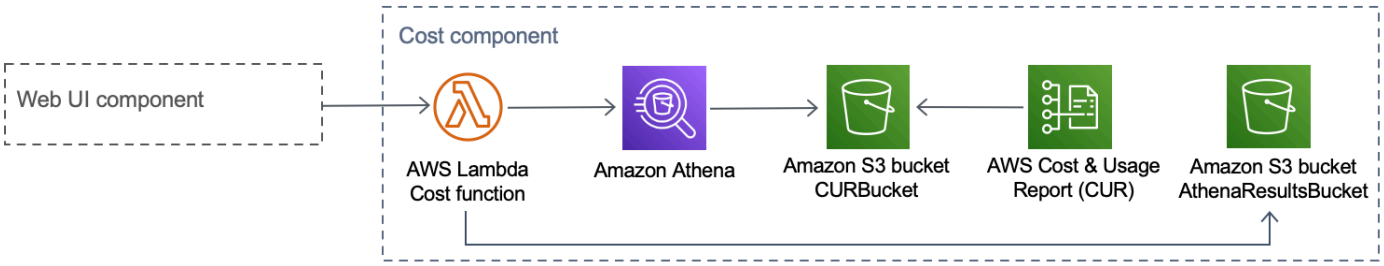
Esta solución configura Amazon ECS para ejecutar una tarea de AWS Fargate con la imagen del contenedor descargada de Amazon ECR. La tarea de AWS Fargate está programada para ejecutarse en intervalos de 15 minutos. Los datos de relación de recursos que se recopilan se insertan en una base de datos de gráficos de Amazon Neptune y en Amazon OpenSearch Service.

El flujo de trabajo del componente de descubrimiento consta de los tres pasos siguientes:

1. Amazon ECS invoca una tarea de AWS Fargate en intervalos de 15 minutos.
2. La tarea Fargate recopila datos de recursos de AWS Config, de las llamadas que describen las API de AWS y de la base de datos de Amazon Neptune.
3. La tarea Fargate calcula la diferencia entre lo que está presente en la base de datos de Amazon Neptune y lo que ha recibido de AWS Config y las llamadas de descripción.
4. La tarea Fargate envía solicitudes a la AppSync API para que persistan los cambios en los recursos y las relaciones descubiertos en Amazon Neptune y OpenSearch Amazon Service.

Componente de costo

Componente de costo de descubrimiento de cargas de trabajo en AWS



Puede crear un CUR de AWS en AWS Billing and Cost Management y Cost Management. Esto publica un archivo con formato Parquet en el bucket de `CostAndUsageReportBucket` Amazon S3. La interfaz de usuario web realiza solicitudes al AppSync punto de enlace de AWS que invoca la función Cost Lambda. La función envía consultas predefinidas a Amazon Athena que devuelven información sobre los costos estimados de AWS CUR.

Debido al tamaño del CUR de AWS, las respuestas de Amazon Athena pueden ser muy numerosas. La solución almacena los resultados en el bucket de `AthenaResultsBucket` Amazon S3 y los vuelve a paginar en la interfaz de usuario web. La política de ciclo de vida configurada en este depósito elimina los elementos que tienen más de siete días de antigüedad.

Los servicios de AWS en esta solución

Servicio de AWS	Descripción
AWS AppSync	Principal. Esta solución se utiliza AppSync para proporcionar una API GraphQL sin servidor que consume la interfaz de usuario web.
Amazon CloudFront	Principal. Esta solución utiliza CloudFront un bucket de Amazon S3 como origen. Esto restringe el acceso al depósito de Amazon S3 para que no sea de acceso público e impide el acceso directo desde el depósito.
AWS Config	Principal. La solución utiliza AWS Config como fuente de datos principal para los recursos y las relaciones que descubre la solución.

Servicio de AWS	Descripción
OpenSearch Servicio Amazon	Principal. La solución utiliza Amazon OpenSearch Service para la supervisión de aplicaciones, el análisis de registros y la observabilidad.
Amazon DynamoDB	Principal. Esta solución usa DynamoDB para almacenar los datos de configuración de la solución.
Amazon Elastic Container Service (ECS)	Principal. Esta solución utiliza Amazon ECS para organizar la ejecución de la tarea que descubre los recursos y las relaciones en sus cuentas de AWS.
AWS Fargate	Principal. Esta solución utiliza AWS Fargate en Amazon ECS como capa de procesamiento para la tarea de descubrimiento.
AWS Lambda	Principal. Esta solución utiliza funciones Lambda sin servidor, con tiempos de ejecución de Node.js y Python, para gestionar las llamadas a la API.
Amazon Neptune	Principal. Esta solución usa Neptune como el almacén de datos principal para los recursos y las relaciones que descubre la solución.
Amazon Simple Storage Service	Principal. Esta solución utiliza Amazon S3 con fines de almacenamiento frontend y backend.
Amazon CloudWatch	Admite. Esta solución se utiliza CloudWatch para recopilar y visualizar registros, métricas y datos de eventos en tiempo real en casos automatizados. Además, puede supervisa r el uso de los recursos y los problemas de rendimiento de la solución implementada.

Servicio de AWS	Descripción
AWS CodeBuild	Admite. Esta solución se utiliza CodeBuild para crear el contenedor de Docker que contiene el código para la tarea de descubrimiento y para implementar los activos de la interfaz en Amazon S3.
Amazon Cognito	Admite. Esta solución utiliza grupos de usuarios de Cognito para autenticar y autorizar a los usuarios a acceder a la interfaz de usuario web de la solución.
AWS Systems Manager	Admite. Esta solución usa AWS Systems Manager para proporcionar monitoreo de recursos a nivel de aplicación y visualización de datos de costos y operaciones de recursos.
Amazon Virtual Private Cloud	Admite. Esta solución utiliza una VPC para lanzar Neptune y sus bases de datos. OpenSearch
AWS WAF	Admite. Esta solución utiliza AWS WAF para proteger la AppSync API de las vulnerabi lidades y los bots más comunes que pueden afectar a la disponibilidad, comprometer la seguridad o consumir recursos excesivos.
Amazon Athena	Opcional. Esta solución usa Athena para consultar los informes de costos y uso si la función de costo está habilitada.

Planificación de la implementación

En esta sección se describen la región, el costo, la seguridad y otras consideraciones antes de implementar la solución.

Regiones de AWS admitidas

Esta solución utiliza el servicio Amazon Cognito, que actualmente no está disponible en todas las regiones de AWS. Para obtener la disponibilidad más reciente de los servicios de AWS por región, consulte la lista de servicios regionales de AWS.

La detección de cargas de trabajo en AWS está disponible en las siguientes regiones de AWS:

Nombre de la región	
Este de EE. UU. (Norte de Virginia)	Canadá (centro)
Este de EE. UU. (Ohio)	Europa (Londres)
Oeste de EE. UU. (Oregón)	Europa (Fráncfort)
Asia-Pacífico (Bombay)	Europa (Irlanda)
Asia-Pacífico (Seúl)	Europa (París)
Asia-Pacífico (Singapur)	Europa (Estocolmo)
Asia-Pacífico (Sídney)	América del Sur (São Paulo)
Asia-Pacífico (Tokio)	

La detección de cargas de trabajo en AWS no está disponible en las siguientes regiones de AWS:

Nombre de la región	Servicio no disponible
AWS GovCloud (EE. UU. Este)	AWS AppSync
AWS GovCloud (EE. UU. Oeste)	AWS AppSync

Nombre de la región	Servicio no disponible
China (Pekín)	Amazon Cognito
China (Ningxia)	Amazon Cognito

Costo

Usted es responsable del coste de los servicios de AWS aprovisionados durante la ejecución de esta solución. A partir de esta revisión, el coste de ejecutar esta solución mediante la opción de implementación de una sola instancia en la región de EE. UU. del Este (Virginia del Norte) es de aproximadamente 0,58$ por hora o 425,19 $ al mes.

> **Note**
>
> El costo de ejecutar Workload Discovery en AWS en la nube de AWS depende de la configuración de implementación que elija. Los siguientes ejemplos proporcionan un desglose de los costos de las configuraciones de implementación de una o varias instancias en la región EE.UU. Este (Virginia del Norte). Los servicios de AWS que se muestran en las tablas de ejemplo siguientes se facturan mensualmente.

Recomendamos crear un presupuesto a través de AWS Cost Explorer para ayudar a administrar los costos. Los precios están sujetos a cambios. Para obtener más información, consulte la página web de precios de cada servicio de AWS utilizado en esta solución.

Ejemplos de tablas de costos

Opción 1: implementación en una sola instancia (predeterminada)

Al implementar esta solución mediante una CloudFormation plantilla de AWS, se modifica el OpensearchMultiAzparámetro para No implementar una sola instancia para el dominio de OpenSearch servicio y se modifica el CreateNeptuneReplicaparámetro para No implementar una sola instancia para el almacén de datos de Neptune. La opción de implementación en una sola instancia tiene un costo menor, pero reduce la disponibilidad de Workload Discovery en AWS en caso de que se produzca un error en la zona de disponibilidad.

Servicio de AWS	Tipo de instancia	Coste por hora [USD]	Coste mensual [USD]
Amazon Neptune	`db.r5.large`	0,348$	254,04 DÓLARES
OpenSearch Servicio Amazon	`m6g.large.search`	0,128$	93,44 DÓLARES
Amazon VPC (puerta de enlace NAT)	N/A	0,090 USD	65,7 DÓLARES
AWS Config	N/A	0,003$ por recurso	0,003$ por recurso
Amazon ECS (tarea de AWS Fargate)	N/A	0,02$	12,01 DÓLARES
Total		0,586$	425,19 DÓLARES

Opción 2: implementación en varias instancias

Al implementar esta solución mediante una CloudFormation plantilla de AWS, modifique el OpensearchMultiAzparámetro para implementar `Yes` dos instancias en dos zonas de disponibilidad para el dominio de OpenSearch servicio y modifique el CreateNeptuneReplicaparámetro para `Yes` implementar dos instancias en dos zonas de disponibilidad para el almacén de datos de Neptune. La opción de implementación en varias instancias costará más, pero aumentará la disponibilidad de Workload Discovery en AWS en caso de que se produzca un error en la zona de disponibilidad.

Servicio de AWS	Tipo de instancia	Coste por hora	Coste mensual [USD]
Amazon Neptune	`db.r5.large`	0,696$	508,08 DÓLARES
OpenSearch Servicio Amazon	`m6g.large.search`	0,256$	186,88 DÓLARES
Amazon VPC (puerta de enlace NAT)	N/A	0,090 USD	65,7 DÓLARES
AWS Config	N/A	0,003$ por recurso	0,003$ por recurso

Servicio de AWS	Tipo de instancia	Coste por hora	Coste mensual [USD]
Amazon ECS (tarea de AWS Fargate)	N/A	0,02$	12,01 DÓLARES
Total		1,062 DÓLARES	772,67 DÓLARES

- El costo final depende de la cantidad de recursos que AWS Config detecte. Se incurrirá en 0,003 USD por elemento de recurso registrado, además del importe indicado en la tabla.

> **Important**
>
> El coste de Amazon Neptune y Amazon OpenSearch Service varía en función del tipo de instancia que seleccione.

Seguridad

Cuando crea sistemas en la infraestructura de AWS, las responsabilidades de seguridad se comparten entre usted y AWS. Este modelo de responsabilidad compartida reduce la carga operativa, ya que AWS opera, administra y controla los componentes, incluidos el sistema operativo anfitrión, la capa de virtualización y la seguridad física de las instalaciones en las que operan los servicios. Para obtener más información sobre la seguridad de AWS, visite el Centro de seguridad de AWS.

Acceso a recursos

Roles de IAM

Las funciones de IAM permiten a los clientes asignar políticas y permisos de acceso detallados a los servicios y usuarios de la nube de AWS. Se requieren varios roles para ejecutar Workload Discovery en AWS y descubrir recursos en las cuentas de AWS.

Amazon Cognito

Amazon Cognito se utiliza para autenticar el acceso con credenciales sólidas y de corta duración que permiten el acceso a los componentes que Workload Discovery necesita en AWS.

Acceso a la red

Amazon VPC

Workload Discovery en AWS se implementa en una VPC de Amazon y se configura de acuerdo con las prácticas recomendadas para ofrecer seguridad y alta disponibilidad. Para obtener más información, consulte las prácticas recomendadas de seguridad para su VPC. Los puntos finales de VPC permiten el tránsito entre los servicios sin conexión a Internet y se configuran cuando están disponibles.

Los grupos de seguridad se utilizan para controlar y aislar el tráfico de red entre los componentes necesarios para ejecutar Workload Discovery en AWS.

Le recomendamos que revise los grupos de seguridad y restrinja aún más el acceso según sea necesario una vez que la implementación esté en marcha.

Amazon CloudFront

Esta solución implementa una interfaz de usuario de consola web alojada en un bucket de Amazon S3 distribuido por Amazon CloudFront. Al utilizar la función de identidad de acceso de origen, solo se puede acceder al contenido de este bucket de Amazon S3 a través de CloudFront. Para obtener más información, consulte Restringir el acceso a un origen de Amazon S3 en la Guía para CloudFront desarrolladores de Amazon.

CloudFront activa medidas de seguridad adicionales para añadir encabezados de seguridad HTTP a cada respuesta del espectador. Para obtener más información, consulta Añadir o eliminar encabezados HTTP en las respuestas. CloudFront

Esta solución usa el CloudFront certificado predeterminado, que tiene un protocolo de seguridad mínimo admitido de TLS v1.0. Para imponer el uso de TLS v1.2 o TLS v1.3, debe usar un certificado SSL personalizado en lugar del certificado predeterminado. CloudFront Para obtener más información, consulte Cómo configuro mi CloudFront distribución para usar un certificado SSL/TLS.

Configuración de aplicaciones

AWS AppSync

Workload Discovery on AWS GraphQL APIs solicita la validación proporcionada por AWS de AppSync acuerdo con la especificación de GraphQL. Además, la autenticación y la autorización

se implementan mediante IAM y Amazon Cognito, que utilizan el JWT proporcionado por Amazon Cognito cuando un usuario se autentica correctamente en la interfaz de usuario web.

AWS Lambda

De forma predeterminada, las funciones de Lambda se configuran con la versión estable más reciente del motor de ejecución del lenguaje. No se registran datos confidenciales ni secretos. Las interacciones de servicio se llevan a cabo con el mínimo de privilegios requerido. Los roles que definen estos privilegios no se comparten entre funciones.

OpenSearch Servicio Amazon

Los dominios OpenSearch de Amazon Service están configurados con una política de acceso que restringe el acceso para detener cualquier solicitud no firmada realizada al clúster de OpenSearch servicios. Esto está restringido a una sola función Lambda.

El clúster de OpenSearch servicios está creado con el node-to-node cifrado activado para añadir una capa adicional de protección de datos a las funciones de seguridad del OpenSearch servicio existentes.

Cuotas

Las cuotas de servicio (que también se denominan límites) establecen el número máximo de recursos u operaciones de servicio para su cuenta de AWS.

Cuotas para los servicios de AWS en esta solución

Asegúrese de tener una cuota suficiente para cada uno de los servicios implementados en esta solución. Para obtener más información, consulte Service Quotas de AWS.

Utilice los siguientes enlaces para ir a la página de ese servicio. Para ver las cuotas de servicio de todos los servicios de AWS en la documentación sin cambiar de página, consulte la información en la página de puntos finales y cuotas del servicio en el PDF.

Amplify	Amazon ECR
Athena	Lambda

CloudFront	OpenSearch Servicio
Cognito	Neptune
Config	Amazon S3
Amazon ECS	

CloudFormation Cuotas de AWS

Su cuenta de AWS tiene CloudFormation cuotas de AWS que debe tener en cuenta al lanzar la pila de esta solución. Si comprende estas cuotas, puede evitar errores de limitación que le impidan implementar esta solución correctamente. Para obtener más información, consulte CloudFormation las cuotas de AWS en la Guía del CloudFormation usuario de AWS.

Cuotas de AWS Lambda

Su cuenta tiene una cuota de 1000 ejecuciones simultáneas de AWS Lambda. Si la solución se usa en una cuenta en la que hay otras cargas de trabajo en ejecución y que utilizan Lambda, establezca esta cuota en un valor adecuado. Este valor se puede ajustar; para obtener más información, consulte las cuotas de AWS Lambda en la Guía del usuario de AWS Lambda.

> **Note**
>
> Esta solución requiere 150 ejecuciones de la cuota de ejecución simultánea para que esté disponible en la cuenta en la que se va a implementar la solución. Si hay menos de 150 ejecuciones disponibles en esa cuenta, la CloudFormation implementación fallará.

Cuotas de Amazon VPC

Su cuenta de AWS puede contener cinco VPCs y dos Elastic IPs (EIPs). Si la solución se usa en una cuenta con otro VPCs o EIPs, esto podría impedirle implementar la solución correctamente. Si corre el riesgo de alcanzar esta cuota, puede proporcionar su propia VPC para la implementación si la proporciona al seguir los pasos de la sección Launch the Stack. Para obtener más información, consulte las cuotas de Amazon VPC en la Guía del usuario de Amazon VPC.

Elegir la cuenta de despliegue

Si va a implementar Workload Discovery en AWS en una organización de AWS, la solución debe estar instalada en una cuenta de administrador delegado en la que estén StackSetshabilitadas las capacidades multirregionales de AWS Config.

Si no utiliza AWS Organizations, le recomendamos que implemente Workload Discovery on AWS en una cuenta de AWS dedicada creada específicamente para esta solución. Este enfoque significa que Workload Discovery en AWS está aislado de sus cargas de trabajo existentes y proporciona una ubicación única para configurar la solución, por ejemplo, añadir usuarios e importar nuevas regiones. También es más fácil realizar un seguimiento de los costes incurridos al ejecutar la solución.

Después de implementar Workload Discovery en AWS, podrá importar regiones de cualquier cuenta que ya haya aprovisionado.

Implementación de la solución

Esta solución utiliza CloudFormation plantillas y pilas de AWS para automatizar su implementación. La CloudFormation plantilla especifica los recursos de AWS incluidos en esta solución y sus propiedades. La CloudFormation pila aprovisiona los recursos que se describen en la plantilla.

Información general del proceso de implementación

> **Note**
>
> Si ya implementó Workload Discovery en AWS y desea actualizar a la versión más reciente, consulte Actualizar la solución.

Siga las step-by-step instrucciones de esta sección para configurar e implementar la solución en su cuenta.

Tiempo de implementación: aproximadamente 30 minutos

Antes de lanzar la solución, revise el costo, la arquitectura, la seguridad de la red y otras consideraciones que se describen en esta guía.

> **Important**
>
> Esta solución incluye una opción para enviar métricas operativas anonimizadas a AWS. Utilizamos estos datos para comprender mejor cómo utilizan los clientes esta solución, así como los servicios y productos relacionados. AWS es propietario de los datos recopilados a través de esta encuesta. La recopilación de datos está sujeta al Aviso de privacidad de AWS.

Requisitos previos

Recopile detalles de los parámetros de implementación

Antes de implementar Workload Discovery en AWS, revise los detalles de configuración del rol vinculado al OpenSearch servicio de Amazon Service y de AWS Config.

Compruebe si tiene un rol AWSService RoleForAmazonOpenSearchService

La implementación crea un clúster de Amazon OpenSearch Service dentro de una Amazon Virtual Private Cloud (Amazon VPC). La plantilla utiliza un rol vinculado al servicio para crear el OpenSearch clúster de servicios. Sin embargo, si ya ha creado el rol en su cuenta, utilice el rol existente.

Para comprobar si ya tienes este rol:

1. Inicie sesión en la consola de Identity and Access Management (IAM) de la cuenta en la que planea implementar esta solución.
2. En el cuadro Search (Buscar), introduzca `AWSServiceRoleForAmazonOpenSearchService`.
3. Si la búsqueda arroja un rol, CreateOpensearchServiceRoleselecciónelo `No` cuando lance la pila.

Compruebe que AWS Config esté configurado

Workload Discovery en AWS utiliza AWS Config para recopilar la mayoría de las configuraciones de recursos. Al implementar la solución o importar una nueva región, debe confirmar si AWS Config ya está configurado y funciona según lo previsto. El AlreadyHaveConfigSetup CloudFormation parámetro informa a Workload Discovery on AWS de si se debe configurar AWS Config.

El siguiente fragmento está tomado de la AWS CLI Command Reference. Ejecute el comando en la región en la que desee implementar Workload Discovery en AWS o importarlo a Workload Discovery en AWS.

Escriba el siguiente comando:

```
aws configservice get-status
```

Si recibe una respuesta similar a la salida, significa que hay un grabador de configuración y un canal de entrega en ejecución en esa región. Seleccione `Yes` este AlreadyHaveConfigSetup CloudFormation parámetro.

Salida:

```
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 está configurando AWS CloudFormation StackSets, debe incluir esta región en el lote de regiones que ya tienen AWS Config configurado.

Verifique los detalles de AWS Config en su cuenta

La implementación intentará configurar AWS Config. Si ya utiliza AWS Config en la cuenta en la que planea implementar o hacer que Workload Discovery pueda detectarla en AWS, seleccione los parámetros pertinentes al implementar esta solución. Además, para una implementación exitosa, asegúrese de no haber restringido los recursos que escanea AWS Config.

Para comprobar la configuración actual de AWS Config:

1. Inicie sesión en la consola de AWS Config.
2. Elija Configuración y asegúrese de que las casillas Registrar todos los recursos admitidos en esta región e Incluir recursos globales estén seleccionadas.

Verificación de la configuración VPC

Si se implementa en una VPC existente, compruebe que sus subredes privadas puedan enrutar las solicitudes a los servicios de AWS.

Si elige la opción de implementar la solución en una VPC existente, debe asegurarse de que las funciones de detección de cargas de trabajo en AWS Lambda y las tareas de Amazon ECS que se ejecutan en las subredes privadas de su VPC puedan conectarse a otros servicios de AWS. La forma estándar de habilitarlo es mediante pasarelas NAT. Puede enumerar las pasarelas NAT de su cuenta, como se muestra en el siguiente ejemplo de código.

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

Salida:

```
[
```

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

> **Note**
>
> Si se obtienen menos de dos resultados, las subredes no tienen el número correcto de puertas de enlace NAT.

Si su VPC no tiene puertas de enlace NAT, debe aprovisionarlas o asegurarse de tener puntos de enlace de VPC para todos los servicios de AWS que se enumeran en la sección AWS. APIs

CloudFormation Plantilla de AWS

Esta solución utiliza AWS CloudFormation para automatizar la implementación de Workload Discovery en AWS en la nube de AWS. Incluye la siguiente CloudFormation plantilla, que puede descargar antes de la implementación:

View template

workload-discovery-on-aws.template: utilice esta plantilla para lanzar la solución y todos los componentes asociados. La configuración predeterminada implementa las soluciones principales y de soporte que se encuentran en los servicios de AWS en esta sección de soluciones, pero puede personalizar la plantilla para adaptarla a sus necesidades específicas.

> **Note**
>
> Puede personalizar la plantilla para adaptarla a sus necesidades específicas; sin embargo, cualquier cambio que realice podría afectar al proceso de actualización.

Lanzar la pila

Esta CloudFormation plantilla de AWS automatizada implementa Workload Discovery en AWS en la nube de AWS. Debe recopilar los detalles de los parámetros de implementación antes de lanzar la pila. Para obtener más información, consulte los requisitos previos.

Tiempo de despliegue: aproximadamente 30 minutos

1. Inicie sesión en la consola de administración de AWS y seleccione el botón para lanzar la CloudFormation plantilla de `workload-discovery-on-aws.template` AWS.

2. La plantilla se lanza en la región Este de EE. UU. (Norte de Virginia) de forma predeterminada. Para lanzar la solución en otra región de AWS, utilice el selector de regiones de la barra de navegación de la consola.

> **Note**
>
> Esta solución utiliza servicios que no están disponibles en todas las regiones de AWS. Consulte las regiones de AWS compatibles para obtener una lista de las regiones de AWS compatibles.

3. En la página Crear pila, compruebe que la URL de la plantilla correcta esté en el cuadro de texto URL de Amazon S3 y seleccione Siguiente.
4. En la página Especificar los detalles de la pila, especifique un nombre para la pila. Para obtener información sobre las limitaciones de caracteres en los nombres, consulte las cuotas de IAM y AWS STS en la Guía del usuario de AWS Identity and Access Management.
5. En Parámetros, revise los parámetros de esta plantilla de solución y modifíquelos según sea necesario. Esta solución utiliza los siguientes valores predeterminados.

Parámetro	Predeterminado/a	Descripción
AdminUserEmailAddress	*<Requires input>*	Una dirección de correo electrónico para crear el primer usuario. Las credencia les temporales se enviarán a esta dirección de correo electrónico.
AlreadyHaveConfigSetup	No	Confirmación de si ya tiene AWS Config configurado o no en la cuenta de implement

Parámetro	Predeterminado/a	Descripción
		ación. Para obtener más información, consulte los requisitos previos.
AthenaWorkgroup	`primary`	El grupo de trabajo que se utilizará para emitir la consulta de Athena cuando la función Coste esté habilitada.
ApiAllowListedRanges	`0.0.0.0/1,128.0.0.0/1`	Lista separada por comas de CIDRs para gestionar el acceso a la API AppSync GraphQL. Para permitir todo el acceso a Internet, usa 0.0.0.0/1,128.0.0.0/1. Si restringe el acceso a determinadas áreas CIDRs, también debe incluir las direcciones IP (y una máscara de subred de /32) de las puertas de enlace NAT que permiten que la tarea ECS del proceso de descubrimiento se ejecute en su subred privada para acceder a Internet. NOTA: Esta lista de permisos no regula el acceso a la WeBui, solo a la API GraphQL.

Parámetro	Predeterminado/a	Descripción
CreateNeptuneReplica	No	Elija si desea crear una réplica de lectura de Neptune en una zona de disponibilidad independiente. La elección Yes mejora la resiliencia, pero aumenta el costo de esta solución.
CreateOpenSearchServiceRole	Yes	Confirmación de si ya tienes o no un rol vinculado a un servicio para Amazon OpenSearch Service. Para obtener más información, consulta los requisitos previos.
NeptuneInstanceClass	db.r5.large	El tipo de instancia utilizado para alojar la base de datos de Amazon Neptune. Lo que seleccione aquí afecta al costo de ejecutar esta solución.
OpensearchInstanceType	m6g.large.search	El tipo de instancia utilizado para los nodos OpenSearch de datos de su servicio. Su selección afecta al coste de funcionamiento de la solución.

Parámetro	Predeterminado/a	Descripción
OpensearchMultiAz	No	Elija si desea crear un clúster OpenSearch de servicios que abarque varias zonas de disponibilidad. La elección `Yes` mejora la resiliencia, pero aumenta el costo de esta solución.
CrossAccountDiscovery	`SELF_MANAGED`	Elija si Workload Discovery on AWS o AWS Organizat ions gestiona la importación de cuentas. El valor puede ser `SELF_MANAGED` o `AWS_ORGANIZATIONS` .
OrganizationUnitId	<Optional input>	El identificador de la unidad organizativa raíz. Este parámetro solo se usa cuando CrossAcco untDiscoveryestá establecido en`AWS_ORGANIZATIONS` .
AccountType	`DELEGATED_ADMIN`	El tipo de cuenta de AWS Organizations en la que se va a instalar Workload Discovery en AWS. Este parámetro solo se usa cuando CrossAcco untDiscoveryestá establecido en`AWS_ORGANIZATIONS` . Para obtener más informaci ón, consulte Elegir la cuenta de despliegue.

Parámetro	Predeterminado/a	Descripción
ConfigAggregatorName	<Optional input>	El agregador de AWS Organization-wide Config que se debe utilizar. Debe instalar la solución en la misma cuenta y región que este agregador. Si deja este parámetro en blanco, se creará un nuevo agregador. Este parámetro solo se usa cuando CrossAccountDiscoveryestá establecido en. `AWS;_ORGANIZATIONS`
CpuUnits	`1 vCPU`	El número de CPUs que se va a asignar a la tarea de Fargate en la que se ejecuta el proceso de descubrimiento.
Memoria	`2048`	La cantidad de memoria que se debe asignar a la tarea de Fargate en la que se ejecuta el proceso de descubrimiento.
DiscoveryTaskFrequency	`15mins`	El intervalo de tiempo entre cada ejecución de la tarea ECS del proceso de descubrimiento.

Parámetro	Predeterminado/a	Descripción
Mín (Mínimo)NCUs	1	Unidades de capacidad mínima de Neptuno (NCUs) que se establecerán en el cúmulo de Neptuno (deben ser menores o iguales a Max). NCUs Obligatorio si el DBInstance tipo es. `db.serverless`
Max (Máximo)NCUs	128	El máximo NCUs debe establecerse en el cúmulo de Neptuno (debe ser mayor o igual a Min NCUs). Obligator io si el DBInstance tipo es`db.serverless` .
VpcId	<Optional input>	El ID de una VPC existente que debe utilizar la solución. Si deja este parámetro en blanco, se aprovisionará una nueva VPC.
VpcCidrBlock	<Optional input>	El bloque CIDR de VPC de la VPC al que hace referenci a el parámetro. VpcId Este parámetro solo se usa si el VpcIdparámetro está establecido.
PrivateSubnet0	<Optional input>	La subred privada que desea usar. Este parámetro solo se usa si el VpcIdparámetro está establecido.

Parámetro	Predeterminado/a	Descripción
PrivateSubnet1	<Optional input>	La subred privada que desea usar. Este parámetro solo se usa si el VpcIdparámetro está establecido.
UsesCustomIdentity	No	Confirmación de si utilizará o no un proveedor de identidad personalizado, como SAML u OIDC.
CognitoCustomDomain	<Optional input>	El prefijo de dominio del dominio personalizado de Amazon Cognito que aloja las páginas de registro e inicio de sesión de su aplicación. Déjelo en blanco si no utiliza un IdP personalizado; de lo contrario, debe incluir solo letras minúsculas, números y guiones.
CognitoAttributeMapping	<Optional input>	La asignación de los atributos del IdP a los atributos del grupo de usuarios de Cognito estándar y personalizado. Déjelo en blanco si no utiliza un IdP personalizado; de lo contrario, debe ser una cadena JSON válida.
IdentityType	<Optional input>	El tipo de proveedor de identidad que se va a utilizar (`GoogleSAML`, o`OIDC`). Déjelo en blanco si no utiliza un IdP personalizado.

Parámetro	Predeterminado/a	Descripción
ProviderName	<Optional input>	Nombre del proveedor de identidad. Déjelo en blanco si no utiliza un IdP personalizado.
GoogleClientId	<Optional input>	El ID de cliente de Google que se va a utilizar. El parámetro solo se usa cuando IdentityTypeestá establecido en`Google`.
GoogleClientSecret	<Optional input>	El secreto del cliente de Google que se va a utilizar. El parámetro solo se usa cuando IdentityTypeestá establecido en`Google`.
SAMLMetadataURL	<Optional input>	La URL de metadatos del proveedor de identidad SAML. El parámetro solo se usa cuando IdentityTypeestá configurado en SAML.
OIDCClientId	<Optional input>	El ID de cliente OIDC que se va a utilizar. El parámetro solo se usa cuando IdentityTypeestá establecido en. `OIDC`
OIDCClientSecret	<Optional input>	El secreto del cliente OIDC que se va a utilizar. El parámetro solo se usa cuando IdentityTypeestá establecido en. `OIDC`

Parámetro	Predeterminado/a	Descripción
OIDCIssuerURL	<Optional input>	La URL del emisor del OIDC que se va a utilizar. El parámetro solo se usa cuando IdentityTypeestá establecido en. `OIDC`
OIDCAttributeRequestMethod	`GET`	El método de solicitud de atributos del OIDC que se va a utilizar. Debe ser uno `GET` de los dos `POST` (consulte al proveedor del OIDC o utilice el valor predeterminado). El parámetro solo se usa cuando IdentityTypeestá establecido en. `OIDC`

6. Elija Siguiente.
7. En la página Configurar opciones de pila, elija Siguiente.
8. En la página Revisar y crear, revise y confirme la configuración. Seleccione las casillas para confirmar que la plantilla crea recursos de IAM y requiere determinadas funciones.
9. Elija Crear para implementar la pila.

   Puede ver el estado de la pila en la CloudFormation consola de AWS en la columna Estado. Debería recibir el estado CREATE_COMPLETE en aproximadamente 30 minutos.

> **Note**
>
> Si se elimina, esta pila elimina todos los recursos. Si la pila se actualiza, conserva el grupo de usuarios de Amazon Cognito para garantizar que no se pierdan los usuarios configurados.

Tareas de configuración posteriores al despliegue

Una vez que Workload Discovery on AWS se haya implementado correctamente, complete las siguientes tareas de configuración posteriores a la implementación.

Activar la seguridad avanzada en Amazon Cognito

Para activar las funciones de seguridad avanzadas de Amazon Cognito, siga las instrucciones sobre cómo añadir seguridad avanzada a un grupo de usuarios en la Guía para desarrolladores de Amazon Cognito.

> **Note**
>
> La activación de la seguridad avanzada en Amazon Cognito conlleva un coste adicional.

Crear usuarios de Amazon Cognito

Workload Discovery en AWS utiliza Amazon Cognito para gestionar todos los usuarios y la autenticación. Crea un usuario para usted durante la implementación y envía un correo electrónico a la dirección proporcionada en el AdminUserEmailAddress parámetro con credenciales temporales.

Para crear usuarios adicionales:

1. Inicie sesión en la consola de AWS Cognito.
2. Elija Administrar grupos de usuarios.
3. Elija WDCognitoUserPool-*<ID-string>*.
4. En el panel de navegación, en Configuración general, elija Usuarios y grupos.
5. En la pestaña Usuarios, elija Crear usuario.
6. En el cuadro Crear usuario, introduzca los valores de todos los campos obligatorios.

Campo de formulario	¿Obligatorio?	Descripción
Nombre de usuario	Sí	El nombre de usuario que utilizará para iniciar sesión en Workload Discovery en AWS.

Campo de formulario	¿Obligatorio?	Descripción
Envíe una invitación	Sí (solo correo electrónico)	Cuando se selecciona, envía una notificación como recordatorio de la contraseña temporal. Selecciona Solo correo electrónico. Si seleccionas SMS (predeterminado), aparece un mensaje de error, pero el usuario sigue creado.
Contraseña temporal	Sí	Introduzca una contraseña temporal. El usuario se ve obligado a cambiar esta situación cuando inicia sesión en Workload Discovery en AWS por primera vez.
Número de teléfono	No	Introduzca un número de teléfono en formato internacional, por ejemplo,\+44. Asegúrese de marcar el número de teléfono como verificado. la casilla está seleccionada.
Correo electrónico	Sí	Introduzca una dirección de correo electrónico válida. Asegúrese de marcar el correo electrónico como verificado. la casilla está seleccionada.

7. Seleccione la opción Crear un usuario.

Repita este proceso para crear tantos usuarios como necesite.

> **Note**
>
> Todos los usuarios tendrán el mismo nivel de acceso a los recursos descubiertos. Recomendamos aprovisionar una implementación independiente de Workload Discovery en AWS para las cuentas que contienen cargas de trabajo o datos confidenciales. Esto le permite restringir el acceso solo a los usuarios que lo necesiten.

Inicie sesión en Workload Discovery en AWS

Una vez que la solución se haya implementado correctamente, determine la URL de la CloudFront distribución de Amazon que sirve a la interfaz de usuario web de la solución.

1. Inicie sesión en la CloudFormation consola de AWS.
2. Seleccione Ver anidado para mostrar las pilas anidadas que componen la implementación. Según sus preferencias, es posible que ya se muestren las pilas anidadas.
3. Seleccione la pila principal de Workload Discovery on AWS.
4. Seleccione la pestaña Salidas y elija la URL en la columna Valor asociada a la WebUiUrlclave.
5. En la pantalla de inicio de sesión, introduce las credenciales de inicio de sesión que recibiste por correo electrónico. A continuación, realice las siguientes acciones:
   a. Sigue las instrucciones para cambiar la contraseña.
   b. Usa el código de verificación enviado a tu correo electrónico para completar la recuperación de la cuenta.

Importa una región

> **Note**
>
> La siguiente sección solo se aplica cuando el modo de detección de cuentas de la solución es autogestionado. Para obtener información sobre cómo funciona la detección de cuentas en el modo AWS Organizations, consulte la sección Modo de detección de cuentas de AWS Organizations.

La importación de una región requiere el despliegue de cierta infraestructura. Esta infraestructura consta de recursos globales y regionales:

Globales: recursos que se implementan una vez en una cuenta y se reutilizan en cada región importada.

- Un rol de IAM () WorkloadDiscoveryRole

Regional: se importan los recursos que se implementan en cada región.

- Un canal de entrega de AWS Config
- Un bucket de Amazon S3 para AWS Config
- Un rol de IAM () ConfigRole

Existen dos opciones para implementar esta infraestructura:

- AWS CloudFormation StackSets (recomendado)
- AWS CloudFormation

Importar una región

Estos pasos le guiarán a través de la importación de una región y la implementación de las CloudFormation plantillas de AWS.

1. Inicie sesión en Workload Discovery en AWS. Consulte Iniciar sesión en Workload Discovery en AWS para ver la URL.
2. En el menú de navegación, seleccione Cuentas.
3. Seleccione Importar.
4. Selecciona el método de importación:
   a. Agregue cuentas y regiones mediante un archivo CSV.
   b. Agregue cuentas y regiones mediante un formulario.

archivo CSV

Proporcione un archivo de valores separados por comas (CSV) que contenga las regiones que se van a importar en el siguiente formato.

```
"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. Selecciona Cargar un CSV.
2. Busca y abre tu archivo CSV.
3. Revisa la tabla de regiones y selecciona Importar.
4. En el cuadro de diálogo modal, descargue la plantilla de recursos globales y la plantilla de recursos regionales.
5. Implemente las CloudFormation plantillas en las cuentas correspondientes (consulte la sección Implementación de CloudFormation plantillas de AWS).
6. Una vez implementadas las plantillas de recursos globales y regionales, seleccione ambas casillas para confirmar que la instalación se ha completado y elija Importar.

Formulario

Indique las regiones que desea importar mediante el formulario:

1. Para el ID de cuenta, introduzca un ID de cuenta de 12 dígitos o seleccione un ID de cuenta existente.
2. En Nombre de cuenta, introduce un nombre de cuenta o utiliza un valor rellenado previamente al seleccionar un ID de cuenta existente.
3. Seleccione las regiones que desee importar.
4. Seleccione Añadir para rellenar las regiones de la tabla de regiones que aparece a continuación.
5. Revisa la tabla de regiones y, a continuación, selecciona Importar.
6. En el cuadro de diálogo modal, descargue la plantilla de recursos globales y la plantilla de recursos regionales.
7. Implemente las CloudFormation plantillas en las cuentas correspondientes (consulte la sección Implementación de CloudFormation plantillas de AWS).
8. Una vez implementadas las plantillas de recursos globales y regionales, seleccione ambas casillas para confirmar que la instalación se ha completado y elija Importar.

Implemente las CloudFormation plantillas de AWS

Los recursos globales se deben implementar una vez por cuenta. No implemente esta plantilla al importar una región desde una cuenta que contenga una región que ya se haya importado a Workload Discovery en AWS. Si la región ya se ha importado, siga las instrucciones de Implementar la pila para aprovisionar los recursos regionales.

Se utiliza CloudFormation StackSets para aprovisionar recursos globales en todas las cuentas

> **Important**
>
> En primer lugar, complete los requisitos previos para que las operaciones del conjunto de pilas se StackSets activen en las cuentas de destino.

1. En la cuenta de administrador, inicie sesión en la CloudFormation consola de AWS.
2. En el menú de navegación, seleccione StackSets.
3. Seleccione Crear StackSet.
4. En la página Elegir una plantilla, en Permisos:
   a. Si utiliza AWS Organizations, elija permisos gestionados por servicio o permisos de autoservicio. Para obtener más información, consulte Uso StackSets en una organización de AWS.
   b. Si no utiliza AWS Organizations, introduzca el nombre del rol de ejecución de IAM utilizado al seguir los pasos StackSets previos. Para obtener más información, consulte Otorgar permisos autogestionados.
5. En Especificar plantilla, selecciona Cargar un archivo de plantilla. Elige el `global-resources.template` archivo (que descargaste anteriormente al importar una región mediante un archivo CSV o un formulario) y selecciona Siguiente.
6. En la página Especificar StackSet detalles, asigne un nombre a su StackSet. Para obtener información sobre las limitaciones de caracteres en los nombres, consulte las cuotas de IAM y AWS STS en la Guía del usuario de AWS Identity and Access Management.
7. En Parámetros, revise los parámetros de esta plantilla de solución y modifíquelos según sea necesario. Esta solución utiliza los siguientes valores predeterminados.

Nombre del campo	Predeterminado/a	Descripción
AccountId	El ID de la cuenta de despliegue	El ID de cuenta de la cuenta de despliegue original. Debe dejar este valor como predeterminado.

1. Elija Siguiente.
2. En la página Configurar StackSet opciones, seleccione Siguiente.
3. En la página Definir opciones de despliegue, en Cuentas, introduzca la cuenta IDs para implementar el rol de cuenta en el cuadro Números de cuenta.
4. En Especificar regiones, seleccione una región para instalar la pila.
5. En Opciones de implementación, seleccione Paralelo y, a continuación, elija Siguiente.
6. En la página de revisión, marque la casilla para confirmar que AWS CloudFormation podría crear recursos de IAM con nombres personalizados.
7. Seleccione Enviar.

Se utiliza CloudFormation StackSets para aprovisionar recursos regionales

> **Important**
>
> En primer lugar, complete los requisitos previos para que las operaciones del conjunto de pilas se StackSets activen en las cuentas de destino.
> Si tiene algunas regiones con AWS Config instalado y otras sin él, debe realizar dos StackSet operaciones, una para las regiones con AWS Config instalado y otra para las que no lo tienen.

1. En la cuenta de administrador, inicie sesión en la CloudFormation consola de AWS.
2. En el menú de navegación, seleccione StackSets.
3. Seleccione Crear StackSet.
4. En la página Elegir una plantilla, en Permisos:

a. Si utiliza AWS Organizations, elija permisos gestionados por servicio o permisos de autoservicio. Para obtener más información, consulte Uso StackSets en una organización de AWS.

b. Si no utiliza AWS Organizations, introduzca el nombre del rol de ejecución de IAM utilizado al seguir los pasos StackSets previos. Para obtener más información, consulte Otorgar permisos autogestionados.

5. En Especificar plantilla, selecciona Cargar un archivo de plantilla. Elige el `regional-resources.template` archivo (que descargaste anteriormente al importar una región mediante un archivo CSV o un formulario) y selecciona Siguiente.
6. En la página Especificar StackSet detalles, asigne un nombre a su StackSet. Para obtener información sobre las limitaciones de caracteres en los nombres, consulte las cuotas de IAM y AWS STS en la Guía del usuario de AWS Identity and Access Management.
7. En Parámetros, revise los parámetros de esta plantilla de solución y modifíquelos según sea necesario. Esta solución utiliza los siguientes valores predeterminados.

Nombre del campo	Predeterminado/a	Descripción
AccountId	El ID de la cuenta de despliegue	El ID de cuenta de la cuenta de despliegue original. Debe dejar este valor como predeterminado.
AggregationRegion	La región de despliegue	La región en la que se desplegó originalmente. Debe dejar este valor como predeterminado.
AlreadyHaveConfigSetup	`No`	Confirmación de si la región ya tiene AWS Config instalado . Establézcalo en Sí si AWS Config ya está instalado en esta región.

1. Elija Siguiente.
2. En la página de StackSet opciones de configuración, seleccione Siguiente.

3. En la página Definir opciones de despliegue, en Cuentas, introduzca la cuenta en la IDs que desea implementar el rol de cuenta en el cuadro Números de cuenta.
4. En Especificar regiones, seleccione una región para instalar la pila. Esto instala la pila en estas regiones en todas las cuentas ingresadas en el paso 6.
5. En Opciones de despliegue, selecciona Paralelo y, a continuación, Siguiente.
6. En la página de revisión, marque la casilla para confirmar que AWS CloudFormation podría crear recursos de IAM con nombres personalizados.
7. Seleccione Enviar.

Implemente la pila para aprovisionar los recursos globales mediante CloudFormation

Los recursos globales se deben implementar una vez por cuenta. No implemente esta plantilla al importar una región desde una cuenta que contenga una región que ya se haya importado a Workload Discovery en AWS.

1. Inicie sesión en la CloudFormation consola de AWS.
2. Elija Crear pila y, a continuación, seleccione Con nuevos recursos (estándar).
3. En la página Crear pila, en la sección Especificar plantilla, selecciona Cargar un archivo de plantilla.
4. Seleccione Elegir archivo y seleccione el `global-resources.template` archivo que se descargó anteriormente al importar una región mediante un archivo CSV o un formulario) y, a continuación, elija Siguiente.
5. En la página Especificar los detalles de la pila, especifique un nombre para la pila. Para obtener información sobre las limitaciones de caracteres en los nombres, consulte las cuotas de IAM y AWS STS en la _Guía del usuario de AWS Identity and Access Management.
6. En Parámetros, revise los parámetros de esta plantilla de solución y modifíquelos según sea necesario. Esta solución utiliza los siguientes valores predeterminados.

Nombre del campo	Predeterminado/a	Descripción
Nombre de pila	`workload-discovery`	El nombre de esta CloudFormation pila de AWS.

Nombre del campo	Predeterminado/a	Descripción
AccountId	ID de cuenta de implement ación	El ID de cuenta de la cuenta de despliegue original. Debe dejar este valor como predeterminado.

1. Elija Siguiente.
2. Seleccione la casilla para confirmar que AWS CloudFormation podría crear recursos de IAM con nombres personalizados.
3. Seleccione Creación de pila.

Las nuevas regiones se escanearán durante el siguiente proceso de descubrimiento, que se llevará a cabo en intervalos de 15 minutos, por ejemplo: 15:00, 15:15, 15:30, 15:45.

Implemente la pila para aprovisionar los recursos regionales mediante CloudFormation

1. Inicie sesión en la CloudFormation consola de AWS.
2. Elija Crear pila y, a continuación, seleccione Con nuevos recursos (estándar).
3. En la página Crear pila, en la sección Especificar plantilla, selecciona Cargar un archivo de plantilla.
4. Seleccione Elegir archivo y seleccione el `regional-resources.template` archivo (se descargó anteriormente al importar una región mediante un archivo CSV o un formulario) y, a continuación, elija Siguiente.
5. En la página Especificar los detalles de la pila, especifique un nombre para la pila. Para obtener información sobre las limitaciones de caracteres en los nombres, consulte las cuotas de IAM y AWS STS en la Guía del usuario de AWS Identity and Access Management.
6. En Parámetros, revise los parámetros de esta plantilla de solución y modifíquelos según sea necesario. Esta solución utiliza los siguientes valores predeterminados.

Nombre del campo	Predeterminado/a	Descripción
AccountId	ID de cuenta de implement ación de la solución	El ID de cuenta de la cuenta de despliegue original. Debe dejarse como predeterminado.
AggregationRegion	Región de despliegue de la solución	La región en la que se implementó originalmente. Debe dejarse como predeterm inado.
AlreadyHaveConfigSetup	`No`	Confirmación de si la región ya tiene AWS Config instalado . Se establece en `Yes` si AWS Config ya está instalado en esta región.

1. Elija Siguiente.
2. Seleccione la casilla para confirmar que AWS CloudFormation podría crear recursos de IAM con nombres personalizados.
3. Seleccione Creación de pila.

Las nuevas regiones se escanearán durante el siguiente proceso de descubrimiento, que se llevará a cabo en intervalos de 15 minutos, por ejemplo, a las 15:00, 15:15, 15:30, 15:45.

Compruebe que la región se haya importado correctamente

1. Inicie sesión en la interfaz de usuario web de la solución (o actualice la página si ya está cargada). Consulte Iniciar sesión en Workload Discovery en AWS para ver la URL.
2. En el panel de navegación izquierdo, en Configuración, seleccione Regiones importadas.

La región, el nombre de la cuenta y el ID de la cuenta aparecen en la tabla. La columna Último escaneado muestra los últimos recursos descubiertos en esa región.

> **Note**
>
> Si la columna Último escaneado permanece en blanco durante más de 30 minutos, consulte Depuración del componente de descubrimiento.

Configure la función de coste

La función de costes requiere la configuración manual de los informes de coste y uso (CUR) de AWS. Siguiendo las instrucciones que aparecen a continuación, podrá:

1. Configure un CUR programado.
2. Configure la replicación de Amazon S3 (cuando CURs esté fuera de la cuenta de implementación)

Cree el informe de costo y uso de AWS en la cuenta de implementación

1. Inicie sesión en la consola de facturación de la cuenta de la que desee recopilar los datos de costes.
2. En el menú de navegación, en Facturación, selecciona Informes de coste y uso.
3. Selecciona Crear informe.
4. `workload-discovery-cost-and-usage-`*`<your-workload-discovery-deployment-account-ID>`*Utilícelo como nombre del informe.

   > **Note**
   >
   > Debe seguir esta convención de nomenclatura porque se implementará una pequeña cantidad de infraestructura para facilitar la consulta del CURs.

5. Seleccione la IDs casilla Incluir recursos.

   > **Note**
   >
   > Debe seleccionar la IDs casilla Incluir recursos para ver los datos de costos. Este ID debe coincidir con los recursos descubiertos por Workload Discovery en AWS.

6. Elija Siguiente.

7. En la página de opciones de entrega, elija Configurar 0
8. Seleccione el bucket de *<stack-name>* `-s3buc-costandusagereportbucket-` *<ID-string>* Amazon S3 para almacenar el CUR. Elija Siguiente.
9. Revise la política, seleccione la casilla de confirmación y elija Guardar.
10. Defina la ruta del prefijo del informe en `aws-perspective`.
11. Seleccione Diariamente para ver la granularidad del tiempo.
12. En Habilitar la integración de datos de informes para, seleccione Amazon Athena.
13. Elija Siguiente.
14. Elija Revisar y completar.

Para comprobar que el informe está configurado correctamente, busque el archivo de prueba en el bucket de Amazon S3.

> **Note**
>
> Los informes pueden tardar hasta 24 horas en cargarse en su depósito.

Crear el informe de costos y uso de AWS en una cuenta externa

1. Inicie sesión en la consola de facturación de la cuenta de la que desee recopilar los datos de costes.
2. En el menú de navegación, en la sección Gestión de costes, selecciona Informes de costes y uso.
3. Seleccione Crear informe.
4. `workload-discovery-cost-and-usage-`*<your-external-account-ID>*Utilícelo como nombre del informe.

   > **Note**
   >
   > Debe seguir esta convención de nomenclatura porque se implementará una pequeña cantidad de infraestructura para facilitar la consulta del CURs.

5. Marque la IDs casilla Incluir recurso.

> **Note**
>
> Debe seleccionar la IDs casilla Incluir recurso para ver los datos de costos. Este ID es necesario para que coincida con los recursos descubiertos por Workload Discovery en AWS.

6. Elija Siguiente.
7. En la página de opciones de entrega, elija Configurar 0
8. Cree un nuevo bucket de Amazon S3 para almacenar el CURs.
9. Revisa la política, selecciona la casilla de confirmación y selecciona Guardar.
10. Defina la ruta del prefijo del informe en`aws-perspective`.
11. Seleccione Diariamente para ver la granularidad del tiempo.
12. En Habilitar la integración de datos de informes para, seleccione Amazon Athena.
13. Elija Siguiente.
14. Elija Revisar y completar. Para comprobar que el informe está configurado correctamente, busque el archivo de prueba en el bucket de Amazon S3.

> **Note**
>
> Los informes pueden tardar hasta 24 horas en cargarse en su depósito.

A continuación, configure la replicación en la cuenta de implementación.

Configure la replicación

Configure la replicación en el bucket de Amazon S3 creado durante la implementación. El bucket de Amazon S3 tiene el siguiente formato: *<stack-name>* `-s3buc-costandusagereportbucket-`*<ID-string>*. Esto permite que la solución consulte el depósito con Amazon Athena.

1. Inicie sesión en la cuenta de AWS en la consola de Amazon S3 que contiene el CUR creado que debe replicarse.
2. Seleccione el bucket de Amazon S3 creado al configurar su CUR. Para obtener más información, consulte el paso 8 de Crear y programar el informe de costo y uso de AWS.

3. Seleccione la pestaña Administración.
4. En Reglas de replicación, elija Crear regla de replicación.
5. En Configuración de reglas de replicación, en el cuadro Nombre de la regla de replicación, introduzca un ID de regla descriptivo.
6. En el depósito de origen, seleccione Aplicar a todos los objetos del depósito para configurar el ámbito de la regla.
7. En Destino, configura lo siguiente:
   a. Seleccione Especificar un depósito en otra cuenta.
   b. Introduce el ID de la cuenta.
   c. Introduzca un valor para el nombre del bucket que se creó durante la implementación de Workload Discovery en AWS. Para encontrarlo, siga las instrucciones de Localizar los recursos de implementación, utilizando el ID lógico `CostAndUsageReportBucket` y el nombre de la pila que especificó al implementar Workload Discovery por primera vez en AWS.
   d. Seleccione la casilla Cambiar la propiedad del objeto por el propietario del bucket de destino.
8. En Función de IAM, selecciona Crear nueva función.

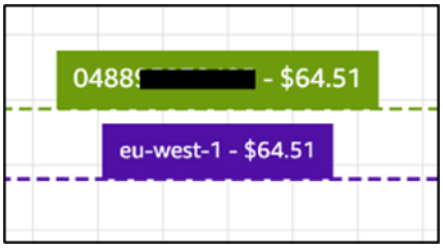
> **Note**
>
> Es posible que ya exista un rol de replicación. Puede seleccionarlo y asegurarse de que tiene las acciones de rol de replicación de S3 requeridas.

9. Seleccione Save.
10. Inicie sesión en la consola de administración de AWS donde está instalado el CUR, vaya a la página de servicios de S3 y seleccione el bucket de `CostAndUsageReportBucket` S3. Para obtener más información, consulte Cómo localizar los recursos de implementación.
11. Seleccione la pestaña Administración.
12. En Reglas de replicación, en el menú desplegable Acciones, seleccione Recibir objetos replicados.
13. En la configuración de la cuenta de bucket de origen:
    a. Introduce el ID de la cuenta del bucket de origen.
    b. Selecciona Generar políticas.
    c. En Políticas, selecciona ver política de bucket.
    d. Selecciona Incluir permiso para cambiar la propiedad del objeto por la del propietario del bucket de destino.

e. Selecciona Aplicar configuración. Esto le da acceso para copiar objetos en él. Consulte la política de replicación de cubos de costes para ver un ejemplo de política de cubos de S3.

> **Note**
>
> Al replicar CURs desde varias cuentas de AWS. Debe asegurarse de que la política de bucket del bucket de destino (dentro de la cuenta Workload Discovery on AWS) contenga el ARN de cada rol de IAM que utilice en cada cuenta. Consulte la política de replicación de Cost Bucket para obtener más información.

Cuando los informes están en la cuenta, los datos de costos aparecen en los recuadros delimitadores y en los recursos individuales.



Edite las políticas del ciclo de vida de los cubos

Durante la implementación, la solución configura las políticas del ciclo de vida en dos cubos:

- `CostAndUsageReportBucket`
- `AccessLogsBucket`

> **Important**
>
> Estas políticas de ciclo de vida eliminan los datos de estos depósitos después de 90 días. Puede editar el ciclo de vida para adaptarlo a cualquier política interna que tenga.

Supervisión de la solución

Esta solución usa MyApplications y CloudWatch AppInsightsle permite monitorear su implementación de Workload Discovery en AWS.

myApplications

MyApplications es una extensión de Console Home que le ayuda a gestionar y supervisar el coste, el estado, la seguridad y el rendimiento de sus aplicaciones en AWS. Puede acceder a todas las aplicaciones de su cuenta, a las métricas clave de todas las aplicaciones y a una visión general de las métricas e información sobre costos, seguridad y operaciones de varias consolas de servicio desde una sola vista en la consola de administración de AWS.

Para ver el panel de MyApplications para Workload Discovery en AWS:

1. Inicie sesión en la Consola de administración de AWS.
2. En la barra lateral izquierda, elija myApplications.
3. Escriba `workload-discovery` en la barra de búsqueda para encontrar la aplicación.
4. Selecciona la aplicación.

CloudWatch AppInsights

CloudWatch Application Insights le ayuda a supervisar sus aplicaciones al identificar y configurar las métricas, los registros y las alarmas clave en todos los recursos de aplicaciones y en el conjunto de tecnologías. Supervisa continuamente las métricas y los registros para detectar y correlacionar las anomalías y los errores. Para ayudar con la solución de problemas, crea paneles automatizados para los problemas detectados, que incluyen anomalías de métricas y errores de registro relacionados, además de información adicional que indica la posible causa raíz.

Para ver el CloudWatch AppInsights panel de control de Workload Discovery en AWS:

1. Inicie sesión en la consola de CloudWatch .
2. En la barra lateral izquierda, selecciona Insights, Application Insights.
3. Seleccione la pestaña Aplicaciones.
4. Escribe `workload-discovery` en la barra de búsqueda para encontrar el panel de control.

5. Selecciona el panel de control.
6. Seleccione la aplicación.

Actualización de la solución

> **Important**
>
> No se admite la actualización de Workload Discovery en AWS de la versión 1.x.x a la versión 2.x.x. Se recomienda desinstalar la versión 1.x.x de esta solución antes de instalar la versión 2.x.x.

Para actualizar desde una implementación 2.x.x, siga estos pasos.

1. Descargue la CloudFormation plantilla de AWS de la solución.
2. Inicie sesión en la CloudFormation consola de AWS.
3. Seleccione la pila con el nombre proporcionado durante la implementación y elija Actualizar.
4. En la página Actualizar pila, selecciona Reemplazar la plantilla actual y, a continuación, selecciona Cargar un archivo de plantilla y carga el archivo descargado en el paso 1.
5. Elija Siguiente.
6. En la página Especificar detalles de la pila, en Parámetros, revise los parámetros y modifíquelos según sea necesario.
7. Elija Siguiente.
8. En la página Configurar opciones de pila, en Opciones de error de pila, asegúrese de que el botón de opción Comportamiento en caso de fallo de aprovisionamiento esté configurado en Revertir todos los recursos de la pila.
9. seleccione Siguiente.
10. En la página Revisar, revise y confirme la configuración. Seleccione las casillas para confirmar que la plantilla crea recursos de IAM y requiere determinadas funciones.
11. Seleccione Crear pila para implementar la pila.

> **Note**
>
> Si implementó la solución en el modo de detección de cuentas autogestionada, debe actualizar los recursos globales que implementó siguiendo los pasos de la sección Importar una región.

Solución de problemas

La resolución de problemas conocidos proporciona instrucciones para mitigar los errores conocidos. Si estas instrucciones no resuelven el problema, consulte la sección Póngase en contacto con AWS Support para obtener instrucciones sobre cómo abrir un caso de AWS Support para esta solución.

Resolución de problemas conocidos

Durante la implementación de Workload Discovery en AWS y en la fase posterior a la implementación, pueden producirse varios errores de configuración comunes:

> **Note**
>
> Para facilitar la solución de problemas, recomendamos deshabilitar la función de reversión en caso de error en la plantilla de AWS. CloudFormation También puede encontrar ayuda adicional para la solución de problemas en la documentación de configuración posterior a la implementación de Workload Discovery on AWS.

Error de Config Delivery Channel

Problema: se produce el siguiente error al implementar la CloudFormation plantilla principal de AWS:

```
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)
```

Motivo: la solución se está implementando en una región que ya tiene AWS Config activado.

Solución: siga las instrucciones de la sección de requisitos previos e implemente la solución con el CloudFormation parámetro AlreadyHaveConfigSetupestablecido en. `Yes`

Se agota el tiempo de espera para la implementación de Search Resolver Stack cuando se implementa en una VPC existente

Problema: se agota el tiempo de espera de una pila anidada que aprovisiona un recurso personalizado para crear un índice en el OpenSearch clúster y se produce el siguiente error:

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

Motivo: las subredes privadas que se proporcionan como CloudFormation parámetros no pueden enrutarse a S3 (los recursos personalizados deben escribir el resultado de su ejecución en un bucket de S3 mediante una URL prefirmada). Por lo general, esto se debe a dos motivos:

1. Las subredes privadas no tienen pasarelas NAT asociadas, por lo que no hay acceso a Internet.
2. La subred privada utiliza puntos de enlace de VPC en lugar de una puerta de enlace de NAT y el punto de enlace de puerta de enlace S3 no está configurado correctamente.

Solución

1. Aprovisione puertas de enlace NAT en la VPC para permitir que las tareas que se ejecutan en subredes privadas accedan a Internet, ya sea CloudFormation mediante la AWS CLI, según se indica en la documentación.
2. Asegúrese de que las tablas de enrutamiento de las subredes se hayan actualizado para el punto final de la VPC de S3 según la documentación.

Los recursos no se descubren después de importar la cuenta

Problema: las cuentas se han importado a través de la interfaz de usuario web, pero parece que no se ha descubierto ningún recurso una vez finalizado el proceso de descubrimiento.

Motivo: los motivos más probables son los siguientes:

1. Si el CrossAccountDiscovery CloudFormation parámetro se establece en`SELF_MANAGED`, la CloudFormation plantilla de recursos globales no se ha implementado.
2. Cuando el CrossAccountDiscovery CloudFormation parámetro está establecido en`AWS_ORGANIZATIONS`: no se detectan una o más cuentas y la columna Estado del rol contiene

entradas No desplegadas. Esto significa que se ha producido un problema con el despliegue automatizado de la plantilla de recursos globales que utiliza StackSets.

3. La tarea ECS del proceso de descubrimiento se está quedando sin memoria. Esto ocurre cuando se importa una gran cantidad de cuentas o recursos. La columna Última vez descubierta de la interfaz de usuario tendrá un valor superior al especificado en el DiscoveryTaskFrequency CloudFormation parámetro (el valor predeterminado es 15 minutos) y habrá un error de memoria insuficiente en la consola ECS.

Solución

1. Implemente la plantilla de recursos globales en las cuentas requeridas, según se indica en la documentación.
2. Ve a la región WdGlobalResources StackSet en la que se ha implementado Workload Discovery y comprueba los errores en las instancias de la pila que no se han podido implementar.
3. Actualice el CloudFormation parámetro de memoria a un valor mayor: comience con el doble y siga aumentando hasta que se detenga el error.

> **Note**
>
> Solo determinadas combinaciones de unidades de CPU y valores de memoria son válidas, por lo que puede que también tenga que actualizar el CpuUnits CloudFormation parámetro. La lista completa de combinaciones se encuentra en la documentación del ECS.

Solo se descubren recursos que no son de AWS Config en cuentas específicas

Problema: Los únicos tipos de recursos que descubre la solución son los que aparecen en la tabla de la sección Recursos compatibles.

Motivo: las causas más comunes de este problema son:

1. Si el CrossAccountDiscovery CloudFormation parámetro se establece en`SELF_MANAGED`, la CloudFormation plantilla de recursos regionales no se ha implementado en las regiones de cada cuenta que se va a descubrir.

2. Cuando el CrossAccountDiscovery CloudFormation parámetro se establece en`SELF_MANAGED`, la CloudFormation plantilla de recursos regionales se ha implementado en las regiones de varias cuentas que no tenían la opción Config habilitada, pero el CloudFormation parámetro AlreadyHaveConfigSetupse estableció erróneamente. `Yes`
3. Si el CrossAccountDiscovery CloudFormation parámetro se establece en`AWS_ORGANIZATIONS`, AWS Config no se habilita en las regiones de cada cuenta que se va a descubrir. En `AWS_ORGANIZATIONS` el modo, eres responsable de habilitar Config según las políticas de tu organización.

Solución

1. Implemente las plantillas de recursos regionales en las cuentas requeridas, según se indica en la documentación.
2. Elimine la pila de recursos regionales implementada anteriormente (de lo contrario, AWS Config estará en un estado incoherente) y vuelva a implementarla con el CloudFormation parámetro AlreadyHaveConfigSetupestablecido en. `No`
3. Active AWS Config en las regiones de cada cuenta que desee detectar.

Póngase en contacto con AWS Support.

Si cuenta con AWS Developer Support, AWS Business Support o AWS Enterprise Support, puede utilizar el Centro de soporte para obtener asistencia de expertos con esta solución. En las siguientes secciones, encontrará instrucciones.

Cree un caso

1. Inicie sesión en Support Center.
2. Seleccione Crear caso.

¿Cómo podemos ayudar?

1. Elija Técnico.
2. Para el servicio, seleccione Soluciones.
3. Para la categoría, seleccione Otras soluciones.
4. En Gravedad, seleccione la opción que mejor se adapte a su caso de uso.

5. Al introducir el servicio, la categoría y la gravedad, la interfaz rellena los enlaces a las preguntas de solución de problemas más frecuentes. Si no puede resolver su pregunta con estos enlaces, seleccione Siguiente paso: información adicional.

Información adicional

1. En Asunto, introduce un texto que resuma tu pregunta o problema.
2. En Descripción, describe el problema en detalle.
3. Selecciona Adjuntar archivos.
4. Adjunte la información que AWS Support necesita para procesar la solicitud.

Ayúdenos a resolver su caso más rápido

1. Introduzca la información solicitada.
2. Elija Siguiente paso: Resuelva ahora o póngase en contacto con nosotros.

Resuelva ahora o póngase en contacto con nosotros

1. Revise las soluciones Solve now.
2. Si no puede resolver su problema con estas soluciones, elija Contactar con nosotros, introduzca la información solicitada y pulse Enviar.

Desinstalar la solución

Para desinstalar la solución, utilice la consola de administración de AWS o la interfaz de línea de comandos de AWS (AWS CLI). En primer lugar, detenga todas las tareas en ejecución desde el clúster de Amazon ECS. De lo contrario, la eliminación de la pila puede fallar.

Uso de Consola de administración de AWS

1. Inicie sesión en la CloudFormation consola de AWS.
2. Seleccione la pila con el nombre proporcionado durante la implementación.
3. Elija Eliminar pila.

Uso de la interfaz de línea de comandos de AWS

Determine si la AWS CLI está disponible en su entorno. Para obtener instrucciones de instalación, consulte Qué es la interfaz de línea de comandos de AWS en la Guía del usuario de la CLI de AWS.

Tras confirmar que la AWS CLI está disponible, ejecute el siguiente comando:

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

Guía para desarrolladores

En esta sección se proporciona el código fuente de la solución y otras personalizaciones.

Código fuente

Visite el GitHub repositorio Workload Discovery en AWS para descargar las plantillas y los scripts de esta solución y compartir sus personalizaciones con otras personas.

Localizar los recursos de implementación

Siga estos pasos para localizar los recursos que se han desplegado en su cuenta.

1. Inicie sesión en la CloudFormation consola de AWS.
2. Seleccione la región en la que implementó la solución.

   Según el uso de esta cuenta, es posible que contenga varias pilas para diferentes cargas de trabajo. Habrá una pila principal con el nombre que se proporcionó durante la implementación y varias pilas anidadas debajo.
3. Seleccione cada pila para acceder a los recursos implementados con esa plantilla.
4. Seleccione la pestaña Recursos y elija el enlace de identificación física del recurso correspondiente para ver el recurso en su consola de servicio correspondiente.

   Si conoce el ID lógico de un recurso, también puede buscarlo en la barra de búsqueda situada encima de la tabla.

Recursos admitidos

La solución admite todos los tipos de recursos compatibles con AWS Config, tal y como se indica aquí. La siguiente tabla contiene los recursos compatibles que Workload Discovery on AWS descubre y que no son compatibles con AWS Config. Los detalles se proporcionan en la lista de documentación de AWS correspondiente.

Tipo de recurso	Origen	Descripción
AWS::APIGateway::Authorizer	SDK	Obtenga Authorizers

Tipo de recurso	Origen	Descripción
AWS::ApiGateway::Resource	SDK	Obtenga un recurso
AWS::ApiGateway::Method	SDK	Método Get
AWS::Cognito::UserPool	SDK	describeUserPool
AWS::ECS::Task	SDK	describe-tasks
AWS::EKS::Nodegroup	SDK	Describa un grupo de nodos
AWS::DynamoDB::Stream	SDK	Describa Stream
Política de AWS: :IAM: AWSManaged	SDK	getAccountAuthorizationDetalles
AWS::ElasticLoadBalancingV2::TargetGroup	SDK	describeTargetGroups
AWS::EC2::Spot	SDK	describeSpotInstanceSolicitudes
AWS::EC2::SpotFleet	SDK	describeSpotFleetSolicitudes

Modo de descubrimiento de cuentas de AWS Organizations

Cuando Workload Discovery on AWS se implementa en una organización de AWS, la detección de cuentas ya no se gestiona a través de la interfaz de usuario web de la solución. En este caso, no necesita gestionar la implementación de CloudFormation plantillas para detectar cuentas.

En su lugar, la solución utiliza un agregador de AWS Config para toda la organización para detectar los recursos de todas las cuentas de la organización que tienen habilitado AWS Config.

Para los tipos de recursos que AWS Config no admite, la solución implementa automáticamente un rol de IAM en cada cuenta de la organización que utiliza AWS. CloudFormation StackSets Esta función permite al proceso de descubrimiento realizar llamadas al SDK en todas las cuentas de la organización para descubrir estos recursos adicionales.

StackSet Está configurado para implementar automáticamente el rol en cualquier cuenta nueva que se añada a la organización y eliminar el rol de cualquier cuenta eliminada de la organización.

> **Note**
>
> No es posible implementar una instancia StackSet de pila en la cuenta de administración. Si desea que Workload Discovery descubra esta cuenta, debe implementar la plantilla de recursos globales mediante el método de CloudFormation implementación estándar de AWS descrito en la CloudFormation sección Implementar la pila para aprovisionar los recursos globales mediante.

Acciones de la función de replicación de Amazon S3

La función de IAM utilizada para realizar la replicación debe incluir las siguientes acciones:

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

Para comprobar que el rol tiene las acciones del rol de replicación:

1. Copie el nombre del rol en el asistente de replicación de S3.
2. Inicie sesión en la consola de IAM desde la cuenta en la que está configurando la replicación.
3. Pegue el nombre del rol en el cuadro Buscar en IAM.
4. Seleccione el elemento principal de la lista. Esta es la función de IAM que se utilizará.
5. En Políticas de permisos, amplíe la Política gestionada.
6. Asegúrese de que la política incluya las acciones que se detallan en la tabla anterior.

Política de bucket de S3

A continuación, se muestra un ejemplo de una política de bucket de S3 CURs que permitirá cargarla en el bucket junto con permisos que permitirán a las cuentas externas replicar objetos en él. Debe añadir el rol de IAM de cada cuenta externa de AWS a esta política para conceder permisos para que se lleve a cabo la replicación.

```
   {
      "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

Como se detalla en los requisitos previos, si va a implementar la solución en una VPC existente, debe poder acceder a los siguientes servicios desde sus subredes privadas.

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 Servicio

- DescribeDomains
- ListDomainNames

Organizations

- ListAccounts
- ListAccountsForParent
- ListOrganizationalUnitsForParent
- ListRoots

Amazon Simple Notification Service

- ListSubscriptions

Amazon Security Token Service

- AssumeRole

Referencia

Esta sección incluye información sobre una función opcional para recopilar métricas únicas para esta solución y una lista de los desarrolladores que han contribuido a esta solución.

Recopilación de datos anonimizados

Esta solución incluye una opción para enviar métricas operativas anonimizadas a AWS. Utilizamos estos datos para comprender mejor cómo utilizan los clientes esta solución, así como los servicios y productos relacionados. Cuando se activa, se recopila la siguiente información y se envía a AWS:

- ID de solución: el identificador de la solución de AWS
- ID único (UUID): identificador único generado aleatoriamente para cada implementación
- Marca de tiempo: marca de tiempo de recopilación de datos
- Función de coste activada: información sobre si el usuario está utilizando la función de coste
- Número de cuentas: número de cuentas que el usuario ha incorporado en su despliegue
- Número de diagramas: número de diagramas creados en cada implementación
- Número de recursos: número de recursos descubiertos en todas las cuentas integradas

AWS es propietario de los datos recopilados a través de esta encuesta. La recopilación de datos está sujeta al Aviso de privacidad. Para excluirse de esta función, complete los siguientes pasos antes de lanzar la CloudFormation plantilla de AWS.

1. Descargue la CloudFormation plantilla de AWS en su disco duro local.
2. Abra la CloudFormation plantilla de AWS con un editor de texto.
3. Modifique la sección de mapeo de CloudFormation plantillas de AWS desde:

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

a:

```
Mappings:
```

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

1. Inicie sesión en la CloudFormation consola de AWS.
2. Elija Crear pila.
3. En la página Crear pila, en la sección Especificar plantilla, seleccione Cargar un archivo de plantilla.
4. En Cargar un archivo de plantilla, seleccione Elegir archivo y después seleccione la plantilla editada de su unidad local.
5. Seleccione Siguiente y siga los pasos que se indican en Lanzar la pila.

Colaboradores

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

Revisiones

Fecha de publicación: septiembre de 2020. Para obtener actualizaciones, consulte el archivo ChangeLog.md del repositorio. GitHub

Consulte el archivo ChangeLog.md del repositorio. GitHub

Avisos

Es responsabilidad de los clientes realizar su propia evaluación independiente de la información que contiene este documento. Este documento: (a) tiene únicamente fines informativos, (b) representa las ofertas y prácticas actuales de los productos de AWS, que están sujetas a cambios sin previo aviso, y (c) no crea ningún compromiso ni garantía por parte de AWS y sus filiales, proveedores o licenciantes. Los productos o servicios de AWS se proporcionan «tal cual» sin garantías, declaraciones ni condiciones de ningún tipo, ya sean expresas o implícitas. Las responsabilidades y obligaciones de AWS con respecto a sus clientes se controlan mediante los acuerdos de AWS y este documento no forma parte ni modifica ningún acuerdo entre AWS y sus clientes.

La licencia de la solución está sujeta a los términos de la licencia Apache, versión 2.0.

Las traducciones son generadas a través de traducción automática. En caso de conflicto entre la traducción y la version original de inglés, prevalecerá la version en inglés.