Guida all'implementazione

Rilevamento dei carichi di lavoro su AWS

Rilevamento dei carichi di lavoro su AWS: Guida all'implementazione

Table of Contents

Implementa uno strumento di visualizzazione che genera automaticamente diagrammi di architettura dei carichi di lavoro nel cloud AWS

Il monitoraggio dei carichi di lavoro nel cloud di Amazon Web Services (AWS) è fondamentale per mantenere la salute e l'efficienza operative. Tuttavia, tenere traccia delle risorse AWS e delle relazioni tra di esse può essere una sfida. Workload Discovery on AWS è uno strumento di visualizzazione che genera automaticamente diagrammi di architettura del carico di lavoro su AWS. Puoi utilizzare questa soluzione per creare, personalizzare e condividere visualizzazioni dettagliate del carico di lavoro basate su dati in tempo reale di AWS.

Questa soluzione funziona mantenendo un inventario delle risorse AWS tra gli account e le regioni, mappando le relazioni tra di essi e visualizzandole in un'interfaccia utente Web (interfaccia utente Web). Quando apporti modifiche a una risorsa, Workload Discovery on AWS ti fa risparmiare tempo fornendo un collegamento alla risorsa nella Console di gestione AWS.

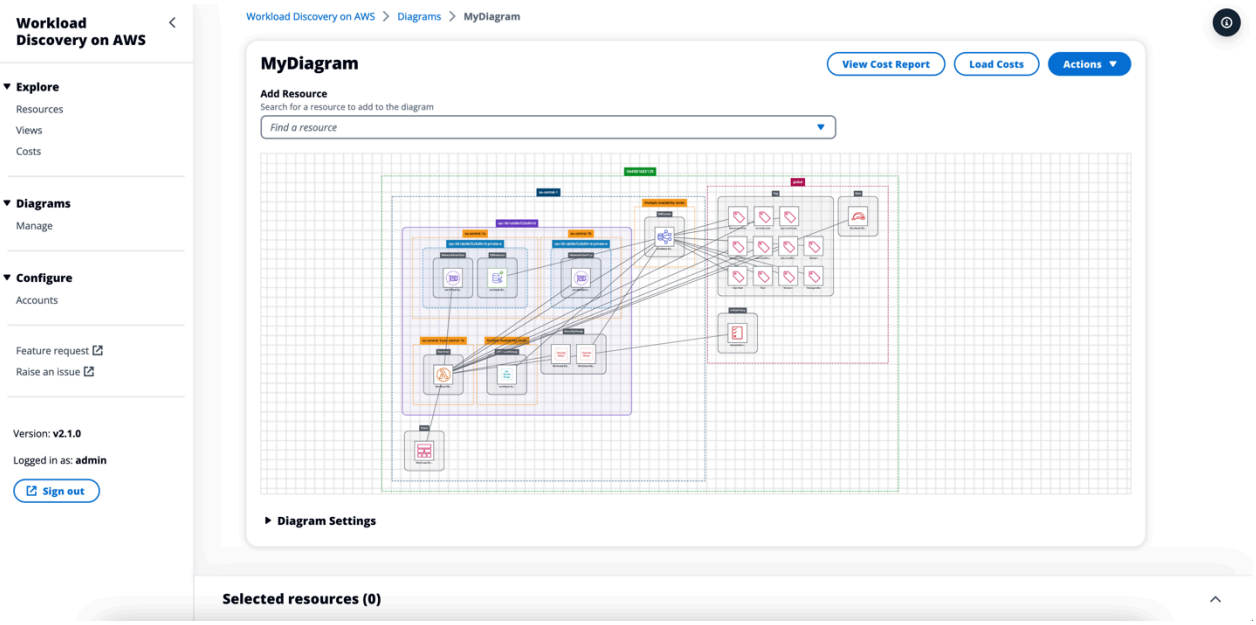


Diagramma di architettura di esempio generato da Workload Discovery su AWS

Questa guida all'implementazione descrive considerazioni architettoniche e passaggi di configurazione per la distribuzione di Workload Discovery su AWS nel cloud AWS. Include collegamenti a un CloudFormation modello AWS che avvia e configura i servizi AWS necessari per distribuire questa soluzione utilizzando le best practice di AWS per la sicurezza e la disponibilità.

Il pubblico previsto per l'implementazione della soluzione Workload Discovery on AWS nel proprio ambiente include architetti di soluzioni, decisori aziendali, DevOps ingegneri, data scientist e professionisti del cloud.

Utilizza questa tabella di navigazione per trovare rapidamente le risposte a queste domande:

Se vuoi.	Leggi..
Conosci il costo di esecuzione di questa soluzione. Il costo stimato per l'esecuzione di questa soluzione nella regione Stati Uniti orientali (Virginia settentrionale) è di 425,19 USD al mese.	Costo
Comprendi le considerazioni sulla sicurezza relative a questa soluzione.	Sicurezza
Scopri come pianificare le quote per questa soluzione.	Quote
Scopri quali regioni AWS supportano questa soluzione.	Regioni AWS supportate
Visualizza o scarica il CloudFormation modello AWS incluso in questa soluzione per distribuire automaticamente le risorse dell'infrastruttura (lo «stack») per questa soluzione.	CloudFormation Modello AWS
Accedi al codice sorgente.	GitHub repository

Funzionalità e vantaggi

Workload Discovery on AWS offre le seguenti funzionalità:

Crea diagrammi di architettura utilizzando dati quasi in tempo reale

Workload Discovery on AWS analizza i tuoi account ogni 15 minuti per garantire che i diagrammi che crei rappresentino una rappresentazione accurata e aggiornata dei tuoi carichi di lavoro.

Visualizza le risorse di più account e regioni in un unico posto

La soluzione mantiene un inventario delle risorse AWS tra gli account e le regioni AWS in un database grafico centralizzato, consentendoti di esplorare più account e regioni e le loro relazioni reciproche in un'unica interfaccia utente.

Integrazione con AWS Organizations

Quando distribuisci la soluzione con AWS Organizations, Workload Discovery on AWS scoprirà automaticamente tutte le risorse supportate nella tua organizzazione. In questa configurazione, non è necessario gestire direttamente la distribuzione di CloudFormation modelli specifici di account per renderli disponibili alla scoperta.

Raccogli i dati sui costi tra i tuoi carichi di lavoro

Se abilitata, la funzione relativa ai costi ti consente di cercare le risorse nel tuo account in base al costo e di aggiungere le risorse che trovi a un diagramma. Puoi anche aggiungere dati sui costi a diagrammi già esistenti.

Esporta su diagrams.net (precedentemente draw.io)

Workload Discovery on AWS può esportare i tuoi diagrammi in modo da poterli annotare ulteriormente utilizzando questo software di disegno di terze parti.

Integrazione con AWS Service Catalog AppRegistry e Application Manager, una funzionalità di AWS Systems Manager

Questa soluzione include una AppRegistry risorsa Service Catalog per registrare il CloudFormation modello della soluzione e le relative risorse sottostanti come applicazione sia in Service Catalog AppRegistry che in Application Manager. Con questa integrazione, è possibile gestire centralmente le risorse della soluzione e abilitare le azioni di ricerca, reporting e gestione delle applicazioni.

Casi d'uso

Revisioni del design e della sicurezza

Utilizzate questa soluzione per generare diagrammi di architettura per verificare che l'implementazione di un carico di lavoro corrisponda al progetto proposto.

Esplora e documenta i carichi di lavoro esistenti

Crea diagrammi di architettura per esplorare i carichi di lavoro in cui esiste poca documentazione o che sono stati implementati manualmente senza infrastruttura come codice.

Visualizza i costi

Genera un rapporto sui costi per i tuoi diagrammi di architettura che contenga una panoramica del costo stimato.

Concetti e definizioni

Questa sezione descrive i concetti chiave e definisce la terminologia specifica di questa soluzione:

risorsa

Una risorsa AWS, come un bucket Amazon Simple Storage Service (Amazon S3) o una funzione AWS Lambda.

relazione

Un collegamento tra due risorse, ad esempio un ruolo AWS Identity and Access Management (IAM) e una funzione AWS Lambda associata.

tipo di risorsa

La categoria di classificazione di una risorsa. Segue sempre la convenzione CloudFormation di denominazione, ad esempio`AWS::Lambda::Function`.

scoperta

Il processo avviato dalla soluzione per mappare le risorse e le loro relazioni negli account e nelle regioni AWS.

modalità di scoperta dell'account

Il metodo per scoprire gli account e aggiungerli alla soluzione: gestito autonomamente tramite l'interfaccia utente di Workload Discovery on AWS o delegato ad AWS Organizations.

> **Note**
>
> Per un riferimento generale ai termini di AWS, consulta il Glossario AWS.

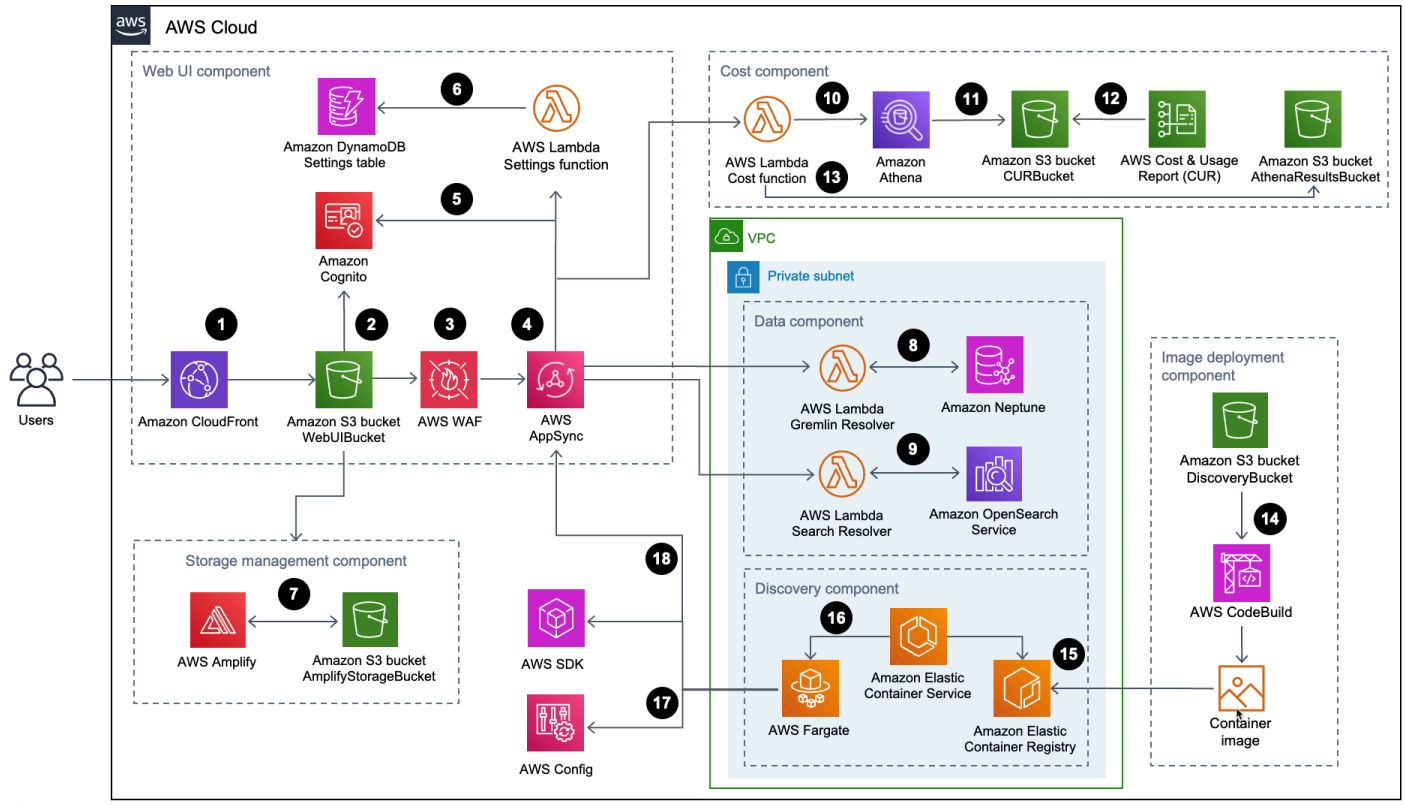
Panoramica dell'architettura

Questa sezione fornisce un diagramma dell'architettura di implementazione di riferimento per i componenti distribuiti con questa soluzione.

Diagramma architetturale

La distribuzione di questa soluzione con i parametri predefiniti crea il seguente ambiente nel cloud AWS.

Workload Discovery sull'architettura AWS



Il flusso di processo di alto livello per i componenti della soluzione distribuiti con il CloudFormation modello AWS è il seguente:

1. HTTP Strict-Transport-Security (HSTS) aggiunge intestazioni di sicurezza a ogni risposta della distribuzione Amazon CloudFront.
2. Un bucket Amazon Simple Storage Service (Amazon S3) ospita l'interfaccia utente Web, distribuita con Amazon. CloudFront Amazon Cognito autentica l'accesso degli utenti all'interfaccia utente Web.

3. AWS WAF protegge l' AppSync API da exploit e bot comuni che possono influire sulla disponibilità, compromettere la sicurezza o consumare risorse eccessive.
4. Gli AppSync endpoint AWS consentono al componente dell'interfaccia utente Web di richiedere dati sulle relazioni tra le risorse, eseguire query sui costi, importare nuove regioni AWS e aggiornare le preferenze. AWS consente AppSync inoltre al componente discovery di archiviare dati persistenti nei database della soluzione.
5. AWS AppSync utilizza JSON Web Tokens (JWTs) forniti da Amazon Cognito per autenticare ogni richiesta.
6. La funzione `Settings`AWS Lambda mantiene le regioni importate e altre configurazioni in Amazon DynamoDB.
7. La soluzione implementa AWS Amplify e un bucket Amazon S3 come componente di gestione dello storage per archiviare le preferenze degli utenti e i diagrammi di architettura salvati.
8. Il componente dati utilizza la funzione `Gremlin Resolver` AWS Lambda per interrogare e restituire dati da un database Amazon Neptune.
9. Il componente dati utilizza la funzione `Search Resolver` Lambda per interrogare e rendere persistenti i dati delle risorse in un dominio Amazon OpenSearch Service.
10. La funzione `Cost` Lambda utilizza Amazon Athena per interrogare AWS Cost and Usage Reports (AWS CUR) per fornire dati sui costi stimati all'interfaccia utente Web.
11. Amazon Athena esegue query su AWS CUR.
12. AWS CUR invia i report al bucket `CostAndUsageReportBucket` Amazon S3.
13. La funzione `Cost` Lambda memorizza i risultati di Amazon Athena nel bucket Amazon `AthenaResultsBucket` S3.
14. AWS CodeBuild crea l'immagine del contenitore del componente di rilevamento nel componente di distribuzione dell'immagine.
15. Amazon Elastic Container Registry (Amazon ECR) contiene un'immagine Docker fornita dal componente di distribuzione dell'immagine.
16. Amazon Elastic Container Service (Amazon ECS) gestisce il task AWS Fargate e fornisce la configurazione necessaria per eseguirlo. AWS Fargate esegue un'attività di container ogni 15 minuti per aggiornare i dati di inventario e risorse.
17. Le chiamate AWS Config e AWS SDK aiutano il componente discovery a mantenere un inventario dei dati delle risorse dalle regioni importate, quindi a memorizzarne i risultati nel componente dati.

18. Il task AWS Fargate mantiene i risultati delle chiamate AWS Config e AWS SDK in un database Amazon Neptune e in un dominio Amazon Service con chiamate API all'API. OpenSearch AppSync

Considerazioni sulla progettazione di AWS Well-Architected

Questa soluzione utilizza le best practice di AWS Well-Architected Framework che aiutano i clienti a progettare e gestire carichi di lavoro affidabili, sicuri, efficienti ed economici nel cloud.

Questa sezione descrive in che modo i principi di progettazione e le migliori pratiche di Well-Architected Framework favoriscono questa soluzione.

Eccellenza operativa

Abbiamo progettato questa soluzione utilizzando i principi e le migliori pratiche del pilastro dell'eccellenza operativa a vantaggio di questa soluzione.

- Risorse definite come infrastruttura come utilizzo di codice. CloudFormation
- La soluzione invia i parametri CloudWatch ad Amazon per fornire osservabilità nell'infrastruttura, nelle funzioni Lambda, nelle attività di Amazon ECS, nei bucket AWS S3 e nel resto dei componenti della soluzione.

Sicurezza

Abbiamo progettato questa soluzione utilizzando i principi e le migliori pratiche del pilastro della sicurezza a vantaggio di questa soluzione.

- Amazon Cognito autentica e autorizza gli utenti delle app per l'interfaccia utente Web.
- Tutti i ruoli utilizzati dalla soluzione prevedono l'accesso con privilegi minimi. In altre parole, contengono solo le autorizzazioni minime necessarie per il corretto funzionamento del servizio.
- I dati inattivi e in transito vengono crittografati utilizzando chiavi archiviate in AWS Key Management Service (AWS KMS), un archivio di gestione delle chiavi dedicato.
- Le credenziali hanno una scadenza breve e seguono una politica di password sicura.
- Le direttive GraphQL di AppSync sicurezza di AWS offrono un controllo granulare su quali operazioni possono essere richiamate dal frontend e dal backend.
- La registrazione, il tracciamento e il controllo delle versioni sono attivati laddove applicabile.

- L'applicazione automatica di patch (versione secondaria) e la creazione di istantanee sono attivate laddove applicabile.
- L'accesso alla rete è privato per impostazione predefinita e gli endpoint Amazon Virtual Private Cloud (Amazon VPC) vengono attivati laddove disponibili.

Affidabilità

Abbiamo progettato questa soluzione utilizzando i principi e le migliori pratiche del pilastro dell'affidabilità a vantaggio di questa soluzione.

- La soluzione utilizza i servizi serverless AWS laddove possibile per garantire un'elevata disponibilità e il ripristino in caso di guasto del servizio.
- Tutte le elaborazioni di calcolo utilizzano funzioni Lambda o Amazon ECS su AWS Fargate.
- Tutto il codice personalizzato utilizza l'SDK AWS e le richieste vengono limitate sul lato client per impedire il raggiungimento delle quote di velocità API.

Efficienza delle prestazioni

Abbiamo progettato questa soluzione utilizzando i principi e le migliori pratiche del pilastro dell'efficienza delle prestazioni a vantaggio di questa soluzione.

- La soluzione utilizza l'architettura serverless AWS ove possibile. Ciò elimina l'onere operativo della gestione dei server fisici.
- La soluzione può essere lanciata in qualsiasi regione che supporti i servizi AWS utilizzati in questa soluzione, ad esempio: AWS Lambda, Amazon Neptune, AWS, AppSync Amazon S3 e Amazon Cognito.
- Nelle regioni supportate, Amazon Neptune serverless consente di eseguire e scalare istantaneamente carichi di lavoro grafici, senza la necessità di gestire e ottimizzare la capacità del database.
- La soluzione utilizza dappertutto servizi gestiti per ridurre l'onere operativo legato all'approvvigionamento e alla gestione delle risorse.

Ottimizzazione dei costi

Abbiamo progettato questa soluzione utilizzando i principi e le migliori pratiche del pilastro dell'ottimizzazione dei costi a vantaggio di questa soluzione.

- AWS ECS su AWS Fargate utilizza le funzioni Lambda esclusivamente per il calcolo e addebita solo tariffe basate sull'uso.
- Amazon DynamoDB ridimensiona la capacità su richiesta, quindi paghi solo per la capacità utilizzata.

Sostenibilità

Abbiamo progettato questa soluzione utilizzando i principi e le migliori pratiche del pilastro della sostenibilità a vantaggio di questa soluzione.

- La soluzione utilizza servizi gestiti e serverless, ove possibile, per ridurre al minimo l'impatto ambientale dei servizi di backend.

Dettagli architettonici

Questa sezione descrive i componenti e i servizi AWS che compongono questa soluzione e i dettagli dell'architettura su come questi componenti interagiscono.

Meccanismo di autenticazione

Workload Discovery on AWS utilizza un pool di utenti Amazon Cognito sia per l'interfaccia utente che per l'autenticazione AWS AppSync . Una volta autenticato, Amazon Cognito fornisce un token Web JSON (JWT) all'interfaccia utente Web che verrà fornito con tutte le richieste API successive. Se non viene fornito un JWT valido, la richiesta API avrà esito negativo e restituirà una risposta HTTP 403 Forbidden.

Risorse supportate

Per un elenco dei tipi di risorse AWS che Workload Discovery on AWS può scoprire all'interno dei tuoi account e regioni, consulta Risorse supportate.

Workload Discovery sulla gestione dei diagrammi dell'architettura AWS

Puoi salvare i diagrammi di architettura Workload Discovery on AWS utilizzando l'interfaccia utente Web in cui è possibile eseguire operazioni di creazione, lettura, aggiornamento ed eliminazione (CRUD). L'API di storage AWS Amplify consente a Workload Discovery su AWS di archiviare diagrammi di architettura in un bucket Amazon S3. Sono disponibili due livelli di autorizzazioni:

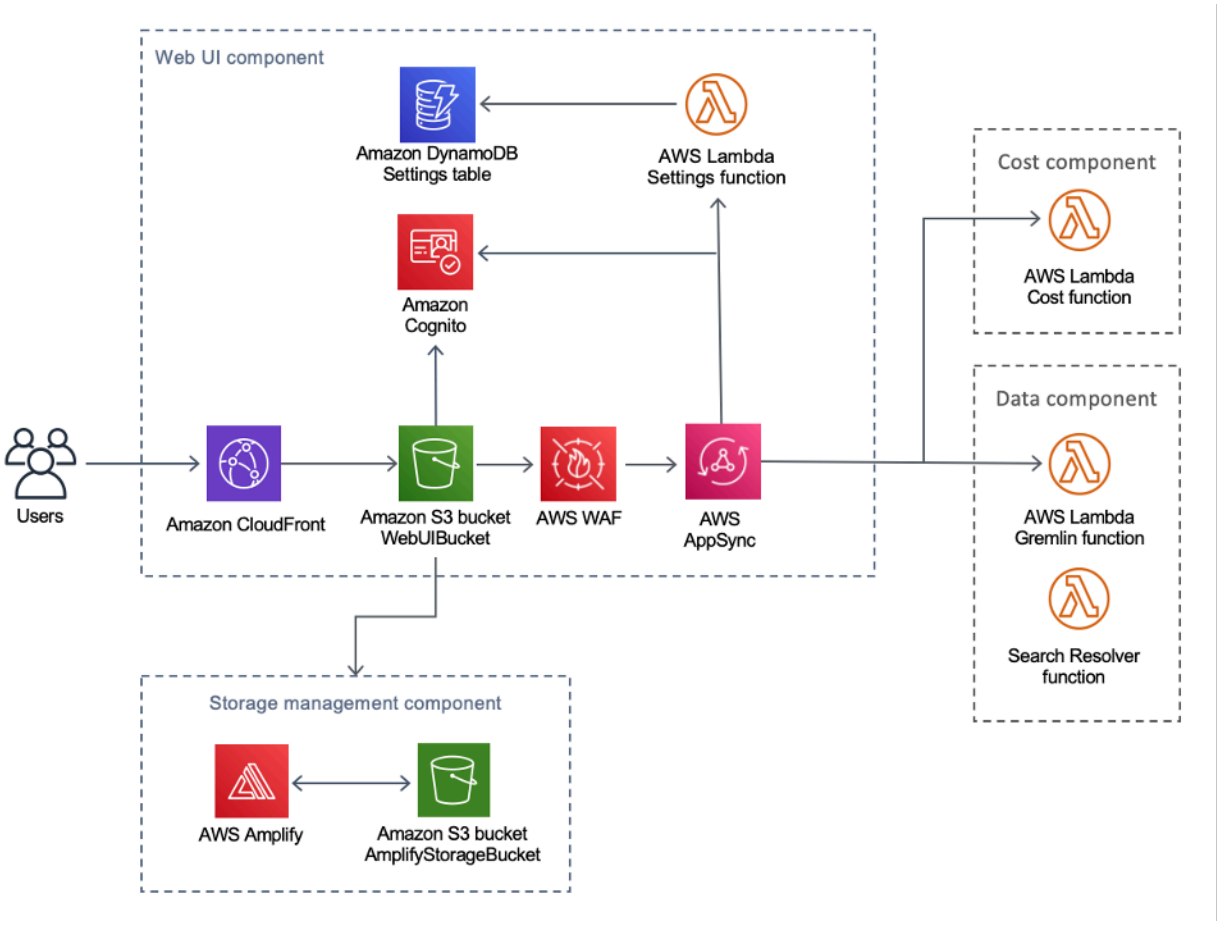
- Tutti gli utenti: consente ai diagrammi dell'architettura di Workload Discovery on AWS di essere visibili agli utenti di Workload Discovery on AWS durante la distribuzione. Gli utenti possono scaricare e modificare questi diagrammi.
- Tu: consente ai diagrammi di architettura di Workload Discovery on AWS di essere visibili solo al creatore. Gli altri utenti non saranno in grado di visualizzarli.

Interfaccia utente Web e gestione dello storage

Abbiamo sviluppato l'interfaccia utente web utilizzando React. L'interfaccia utente Web fornisce una console frontend per consentire agli utenti di interagire con Workload Discovery on AWS.

Amazon CloudFront è configurato per aggiungere intestazioni sicure a ogni richiesta HTTP all'interfaccia utente Web. Ciò fornisce un ulteriore livello di sicurezza, proteggendo da attacchi come il cross-site scripting (XSS).

Workload Discovery sull'interfaccia utente Web AWS e componenti di gestione dello storage

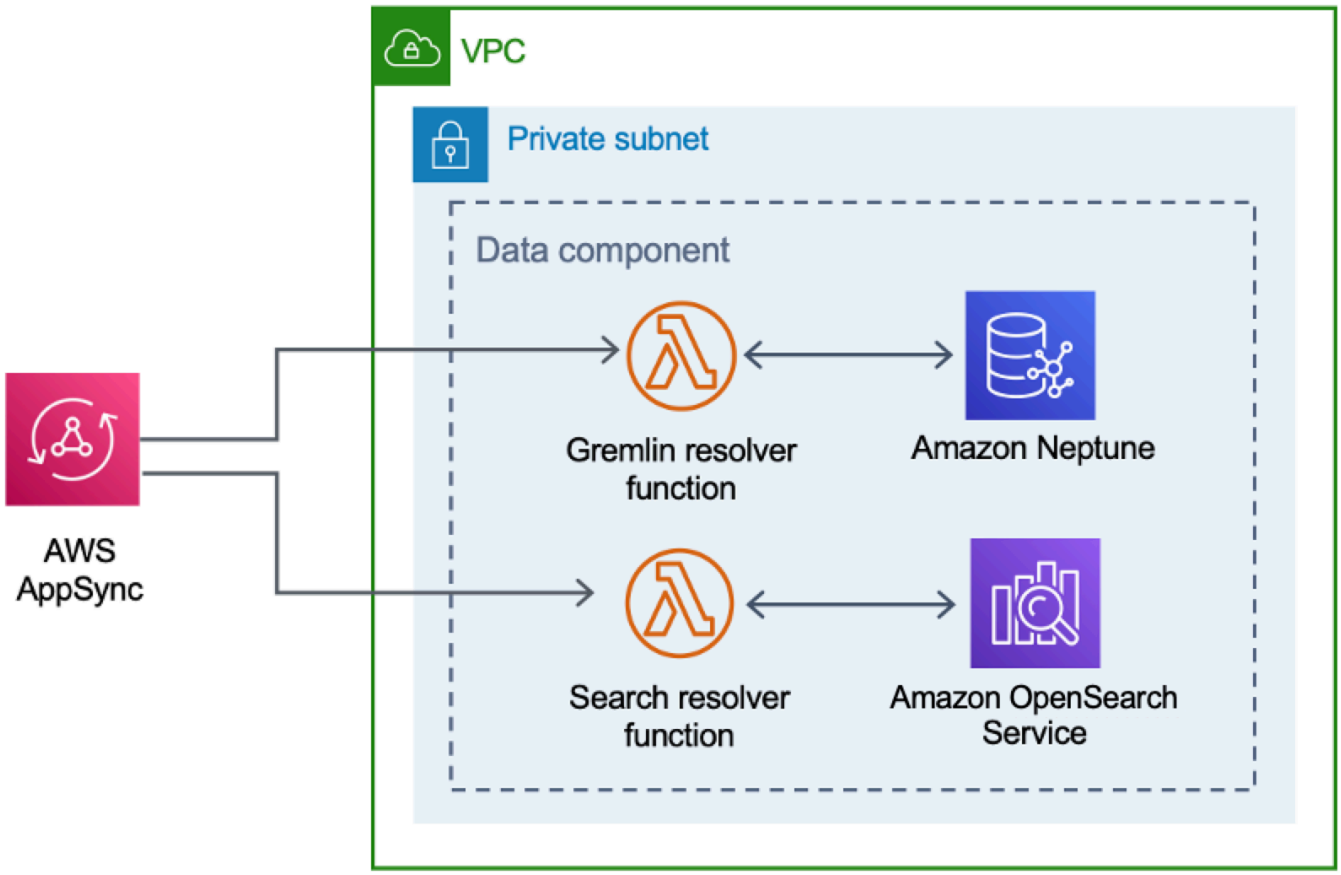


Le risorse dell'interfaccia utente Web sono ospitate nel bucket `WebUIBucket` Amazon S3 e distribuite da Amazon. CloudFront AWS Amplify fornisce un livello di astrazione per semplificare le integrazioni con AWS e Amazon S3. AppSync

Questa soluzione utilizza AWS AppSync per facilitare l'interazione con varie configurazioni disponibili per Workload Discovery on AWS, inclusa la gestione delle regioni importate. AWS AppSync utilizza la funzione `Settings` AWS Lambda per gestire richieste come l'importazione di un nuovo account o regione.

Componente dati

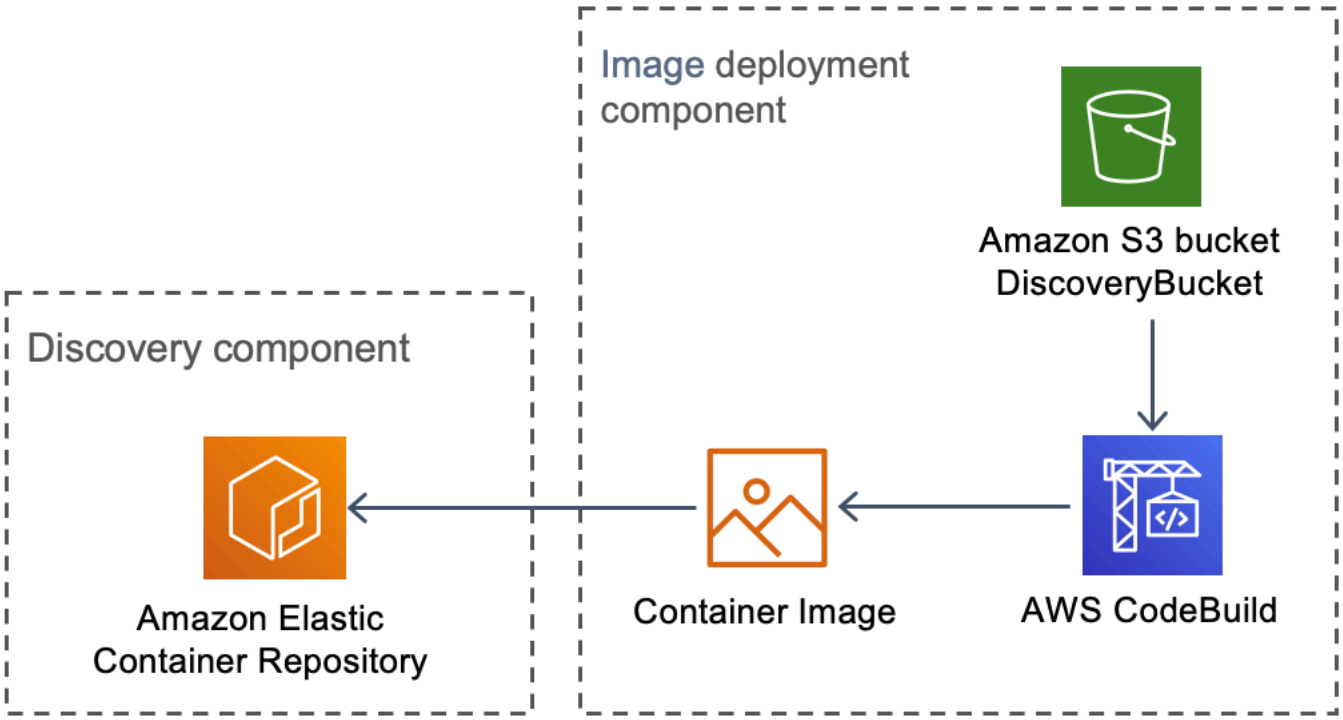
Workload Discovery sul componente dati AWS



L'interfaccia utente Web invia le richieste all' AppSync API, che richiama le funzioni o `Gremlin Resolver` LambdaSearch `Resolver`. Queste funzioni elaborano le richieste e interrogano Amazon Neptune OpenSearch o Service per recuperare dati sulle risorse fornite. AWS supporta AppSync anche le richieste di dati sui costi stimati provenienti da AWS CUR.

Il componente discovery invia richieste all' AppSync API per la lettura e la persistenza dei dati nei database di Amazon OpenSearch Neptune e Service. L'API riceve le richieste dal task AWS Fargate nel componente discovery. L'API viene quindi autenticata utilizzando un ruolo IAM che fornisce l'accesso ai database.

Componente di distribuzione delle immagini



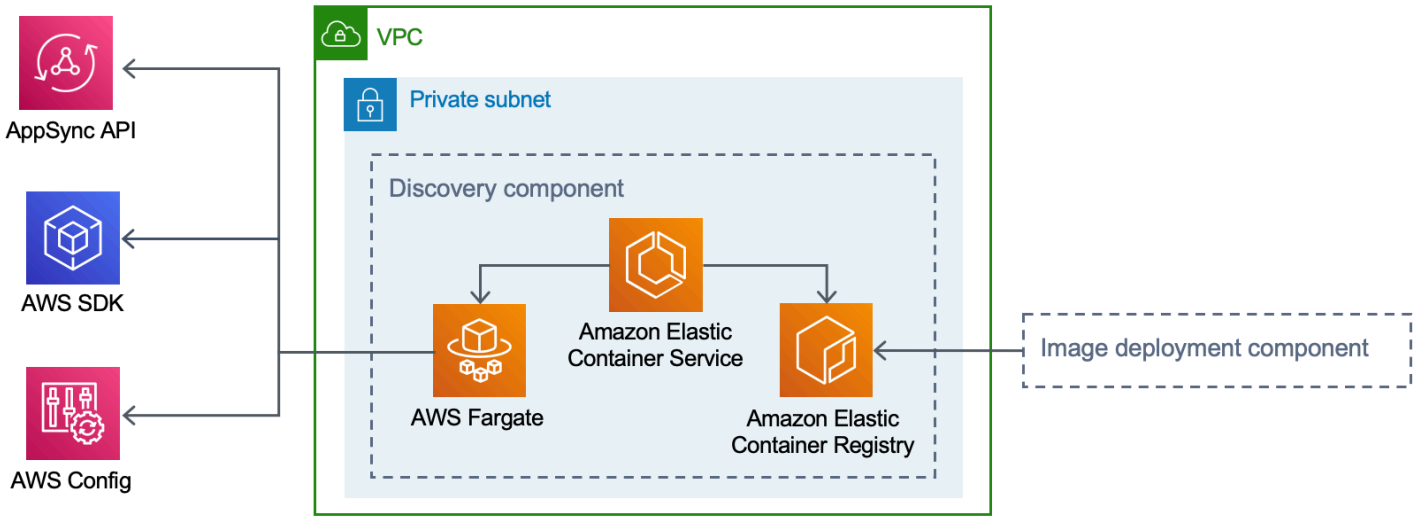
Workload Discovery sul componente di distribuzione delle immagini AWS

Il componente di distribuzione delle immagini crea l'immagine del contenitore utilizzata dal componente discovery. Il bucket `DiscoveryBucket` e Amazon S3 ospitano il codice che può essere scaricato al momento della distribuzione da un CodeBuild processo AWS che crea l'immagine del contenitore e la carica su Amazon ECR.

Componente Discovery

Il componente discovery è il principale elemento di raccolta dati dell'architettura Workload Discovery on AWS. È responsabile di interrogare AWS Config e descrivere le chiamate API per mantenere l'inventario delle risorse e le loro relazioni reciproche.

Workload Discovery sul componente AWS Discovery



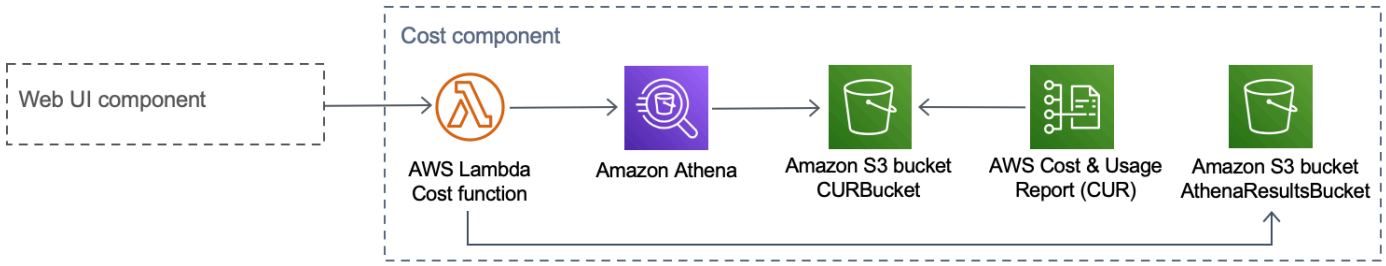
Questa soluzione configura Amazon ECS per eseguire un'attività AWS Fargate utilizzando l'immagine del contenitore scaricata da Amazon ECR. L'esecuzione del task AWS Fargate è pianificata a intervalli di 15 minuti. I dati sulle relazioni tra le risorse raccolti vengono inseriti in un database grafico Amazon Neptune e in Amazon Service. OpenSearch

Il flusso di lavoro dei componenti di scoperta prevede i seguenti tre passaggi:

1. Amazon ECS richiama un'attività AWS Fargate a intervalli di 15 minuti.
2. Il task Fargate raccoglie dati sulle risorse da AWS Config, dalle chiamate di descrizione delle API AWS e dal database Amazon Neptune.
3. Il task Fargate calcola la differenza tra ciò che è presente nel database Amazon Neptune e ciò che ha ricevuto da AWS Config e le chiamate di descrizione.
4. L'attività Fargate invia richieste all' AppSync API per rendere permanenti le modifiche alle risorse e alle relazioni scoperte in Amazon Neptune e Amazon Service. OpenSearch

Componente di costo

Componente di costo di Workload Discovery on AWS



Puoi creare un AWS CUR in AWS Billing and Cost Management and Cost Management. Questo pubblica un file in formato Parquet nel bucket Amazon `CostAndUsageReportBucket` S3. L'interfaccia utente Web invia richieste all' AppSync endpoint AWS che richiama la funzione Cost Lambda. La funzione invia query predefinite ad Amazon Athena che restituiscono informazioni sui costi stimati da AWS CUR.

A causa delle dimensioni di AWS CUR, le risposte di Amazon Athena possono essere molto grandi. La soluzione archivia i risultati nel bucket `AthenaResultsBucket` Amazon S3 e li impagina nuovamente nell'interfaccia utente Web. La politica del ciclo di vita configurata su questo bucket rimuove gli elementi che hanno più di sette giorni.

Servizi AWS in questa soluzione

Servizio AWS	Descrizione
AWS AppSync	Core. Questa soluzione fornisce un'API GraphQL serverless utilizzata AppSync dall'interfaccia utente Web.
Amazon CloudFront	Nucleo. Questa soluzione utilizza CloudFront un bucket Amazon S3 come origine. Ciò limita l'accesso al bucket Amazon S3 in modo che non sia accessibile al pubblico e impedisce l'accesso diretto dal bucket.
AWS Config	Nucleo. La soluzione utilizza AWS Config come fonte di dati principale per le risorse e le relazioni rilevate dalla soluzione.

Servizio AWS	Descrizione
OpenSearch Servizio Amazon	Nucleo. La soluzione utilizza Amazon OpenSearch Service per il monitoraggio delle applicazioni, l'analisi dei log e l'osservabilità.
Amazon DynamoDB	Nucleo. Questa soluzione utilizza DynamoDB per archiviare i dati di configurazione per la soluzione.
Amazon Elastic Container Service (ECS)	Nucleo. Questa soluzione utilizza Amazon ECS per orchestrare l'esecuzione dell'attività che rileva risorse e relazioni nei tuoi account AWS.
AWS Fargate	Nucleo. Questa soluzione utilizza AWS Fargate su Amazon ECS come livello di calcolo per l'attività di scoperta.
AWS Lambda	Nucleo. Questa soluzione utilizza funzioni Lambda serverless, con runtime Node.js e Python, per gestire le chiamate API.
Amazon Neptune	Nucleo. Questa soluzione utilizza Neptune come datastore principale per le risorse e le relazioni rilevate dalla soluzione.
Amazon Simple Storage Service	Nucleo. Questa soluzione utilizza Amazon S3 per scopi di storage frontend e backend.
Amazon CloudWatch	Supporto. Questa soluzione consente CloudWatch di raccogliere e visualizzare registri, metriche e dati sugli eventi in tempo reale in casi automatizzati. Inoltre, è possibile monitorare l'utilizzo delle risorse e i problemi di prestazioni della soluzione implementata.

Servizio AWS	Descrizione
AWS CodeBuild	Supporto. Questa soluzione consente CodeBuild di creare il contenitore Docker che contiene il codice per l'attività di rilevamen to e di distribuire le risorse per il frontend su Amazon S3.
Amazon Cognito	Supporto. Questa soluzione utilizza i pool di utenti di Cognito per autenticare e autorizzare gli utenti ad accedere all'interfaccia utente web della soluzione.
AWS Systems Manager	Supporto. Questa soluzione utilizza AWS Systems Manager per fornire il monitorag gio delle risorse a livello di applicazione e la visualizzazione delle operazioni delle risorse e dei dati sui costi.
Amazon Virtual Private Cloud	Supporto. Questa soluzione utilizza un VPC per avviare Neptune e i database. OpenSearch
AWS WAF	Supporto. Questa soluzione utilizza AWS WAF per proteggere l' AppSync API da exploit e bot comuni che possono influire sulla disponibi lità, compromettere la sicurezza o consumare risorse eccessive.
Amazon Athena	Facoltativo. Questa soluzione utilizza Athena per interrogare i report sui costi e sull'utilizzo se la funzionalità relativa ai costi è abilitata.

Pianifica la tua implementazione

Questa sezione descrive la regione, i costi, la sicurezza e altre considerazioni prima di implementare la soluzione.

Regioni AWS supportate

Questa soluzione utilizza il servizio Amazon Cognito, che attualmente non è disponibile in tutte le regioni AWS. Per la disponibilità più aggiornata dei servizi AWS per regione, consulta l'AWS Regional Services List.

Workload Discovery on AWS è disponibile nelle seguenti regioni AWS:

Nome della regione	
Stati Uniti orientali (Virginia settentrionale)	Canada (Centrale)
Stati Uniti orientali (Ohio)	Europa (Londra)
US West (Oregon)	Europa (Francoforte)
Asia Pacifico (Mumbai)	Europa (Irlanda)
Asia Pacifico (Seoul)	Europa (Parigi)
Asia Pacifico (Singapore)	Europa (Stoccolma)
Asia Pacifico (Sydney)	Sud America (San Paolo)
Asia Pacifico (Tokyo)	

Workload Discovery on AWS non è disponibile nelle seguenti regioni AWS:

Nome della regione	Servizio non disponibile
AWS GovCloud (Stati Uniti orientali)	AWS AppSync
AWS GovCloud (Stati Uniti occidentali)	AWS AppSync

Nome della regione	Servizio non disponibile
Cina (Pechino)	Amazon Cognito
Cina (Ningxia)	Amazon Cognito

Costo

Sei responsabile del costo dei servizi AWS forniti durante l'esecuzione di questa soluzione. A partire da questa revisione, il costo per l'esecuzione di questa soluzione utilizzando l'opzione di distribuzione a istanza singola nella regione Stati Uniti orientali (Virginia settentrionale) è di circa 0,58 USD all'ora o 425,19 USD al mese.

> **Note**
>
> Il costo per l'esecuzione di Workload Discovery on AWS nel cloud AWS dipende dalla configurazione di distribuzione scelta. Gli esempi seguenti forniscono una ripartizione dei costi per le configurazioni di distribuzione a istanza singola e multipla nella regione Stati Uniti orientali (Virginia settentrionale). I servizi AWS elencati nelle tabelle di esempio riportate di seguito vengono fatturati su base mensile.

Ti consigliamo di creare un budget tramite AWS Cost Explorer per gestire i costi. I prezzi sono soggetti a modifiche. Per tutti i dettagli, consulta la pagina web dei prezzi per ogni servizio AWS utilizzato in questa soluzione.

Tabelle dei costi di esempio

Opzione 1: distribuzione a istanza singola (impostazione predefinita)

Quando si distribuisce questa soluzione utilizzando un CloudFormation modello AWS, si modifica il OpensearchMultiAzparametro per `No` distribuire una singola istanza per il dominio OpenSearch Service e si modifica il CreateNeptuneReplicaparametro per `No` distribuire una singola istanza per il data store Neptune. L'opzione di distribuzione a istanza singola comporta un costo inferiore, ma riduce la disponibilità di Workload Discovery su AWS in caso di guasto di una zona di disponibilità.

Servizio AWS	Tipo di istanza	Costo orario [USD]	Costo mensile [USD]
Amazon Neptune	`db.r5.large`	0,348 USD	$254,04
OpenSearch Servizio Amazon	`m6g.large .search`	0,128$	$93,44
Amazon VPC (gateway NAT)	N/D	0,090 USD	65,7$
AWS Config	N/D	0,003 USD per risorsa	0,003 USD per risorsa
Amazon ECS (attività AWS Fargate)	N/D	0,02 USD	$12,01
Totale		$0,586	425,19$

Opzione 2: implementazione su più istanze

Quando si distribuisce questa soluzione utilizzando un CloudFormation modello AWS, si modifica il OpensearchMultiAzparametro per `Yes` distribuire due istanze in due zone di disponibilità per il dominio del OpenSearch servizio e si modifica il CreateNeptuneReplicaparametro per `Yes` distribuire due istanze in due zone di disponibilità per il data store Neptune. L'opzione di distribuzione a più istanze avrà un costo di esecuzione maggiore, ma aumenta la disponibilità di Workload Discovery su AWS in caso di guasto della zona di disponibilità.

Servizio AWS	Tipo di istanza	Costo orario	Costo mensile [USD]
Amazon Neptune	`db.r5.large`	0,696 USD	$508,08
OpenSearch Servizio Amazon	`m6g.large .search`	0,256$	$186,88
Amazon VPC (gateway NAT)	N/D	0,090 USD	65,7$
AWS Config	N/D	0,003 USD per risorsa	0,003 USD per risorsa

Servizio AWS	Tipo di istanza	Costo orario	Costo mensile [USD]
Amazon ECS (attività AWS Fargate)	N/D	0,02 USD	$12,01
Totale		$1,062	$772,67

- Il costo finale dipende dal numero di risorse rilevate da AWS Config. Oltre all'importo indicato nella tabella, verranno addebitati 0,003 USD per elemento di risorsa registrato.

> **Important**
>
> Il costo di Amazon Neptune e OpenSearch Amazon Service varia a seconda del tipo di istanza selezionato.

Sicurezza

Quando crei sistemi sull'infrastruttura AWS, le responsabilità di sicurezza vengono condivise tra te e AWS. Questo modello di responsabilità condivisa riduce il carico operativo perché AWS gestisce, gestisce e controlla i componenti, tra cui il sistema operativo host, il livello di virtualizzazione e la sicurezza fisica delle strutture in cui operano i servizi. Per ulteriori informazioni sulla sicurezza di AWS, visita il Centro di sicurezza AWS.

Accesso alle risorse

Ruoli IAM

I ruoli IAM consentono ai clienti di assegnare policy di accesso e autorizzazioni granulari a servizi e utenti sul cloud AWS. Sono necessari più ruoli per eseguire Workload Discovery su AWS e scoprire risorse negli account AWS.

Amazon Cognito

Amazon Cognito viene utilizzato per autenticare l'accesso con credenziali forti e di breve durata che garantiscono l'accesso ai componenti necessari a Workload Discovery su AWS.

Accesso alla rete

Amazon VPC

Workload Discovery on AWS è distribuito all'interno di un Amazon VPC e configurato secondo le migliori pratiche per offrire sicurezza e alta disponibilità. Per ulteriori dettagli, consulta le best practice di sicurezza per il tuo VPC. Gli endpoint VPC consentono il transito non Internet tra i servizi e sono configurati laddove disponibili.

I gruppi di sicurezza vengono utilizzati per controllare e isolare il traffico di rete tra i componenti necessari per eseguire Workload Discovery su AWS.

Ti consigliamo di esaminare i gruppi di sicurezza e di limitare ulteriormente l'accesso, se necessario, una volta che la distribuzione è attiva e funzionante.

Amazon CloudFront

Questa soluzione implementa un'interfaccia utente per console Web ospitata in un bucket Amazon S3 distribuito da Amazon. CloudFront Utilizzando la funzionalità Origin Access Identity, i contenuti di questo bucket Amazon S3 sono accessibili solo tramite. CloudFront Per ulteriori informazioni, consulta la sezione Limitazione dell'accesso a un'origine Amazon S3 nella CloudFront Amazon Developer Guide.

CloudFront attiva ulteriori mitigazioni di sicurezza per aggiungere intestazioni di sicurezza HTTP a ciascuna risposta del visualizzatore. Per ulteriori dettagli, consulta Aggiungere o rimuovere intestazioni HTTP nelle risposte. CloudFront

Questa soluzione utilizza il CloudFront certificato predefinito che ha un protocollo di sicurezza minimo supportato di TLS v1.0. Per imporre l'uso di TLS v1.2 o TLS v1.3, è necessario utilizzare un certificato SSL personalizzato anziché il certificato predefinito. CloudFront Per ulteriori informazioni, consulta Come posso configurare la mia CloudFront distribuzione per utilizzare un certificato SSL/TLS.

Configurazione dell'applicazione

AWS AppSync

Workload Discovery su AWS APIs GraphQL prevede la convalida delle richieste fornita da AppSync AWS secondo le specifiche GraphQL. Inoltre, l'autenticazione e l'autorizzazione vengono implementate utilizzando IAM e Amazon Cognito, che utilizzano il JWT fornito da Amazon Cognito quando un utente si autentica correttamente nell'interfaccia utente Web.

AWS Lambda

Per impostazione predefinita, le funzioni Lambda sono configurate con la versione stabile più recente del runtime del linguaggio. Non vengono registrati dati o segreti sensibili. Le interazioni di servizio vengono eseguite con il privilegio minimo richiesto. I ruoli che definiscono questi privilegi non sono condivisi tra le funzioni.

OpenSearch Servizio Amazon

I domini Amazon OpenSearch Service sono configurati con una politica di accesso che limita l'accesso per bloccare qualsiasi richiesta non firmata effettuata al OpenSearch cluster di servizi. Questo è limitato a una singola funzione Lambda.

Il cluster OpenSearch di servizi è costruito con node-to-node la crittografia attivata per aggiungere un ulteriore livello di protezione dei dati oltre alle funzionalità di sicurezza del OpenSearch servizio esistenti.

Quote

Le quote di servizio, anche denominate limiti, rappresentano il numero massimo di risorse di servizio o operazioni per l'account AWS.

Quote per i servizi AWS in questa soluzione

Assicurati di disporre di una quota sufficiente per ciascuno dei servizi implementati in questa soluzione. Per ulteriori informazioni, consulta Quote di servizio AWS.

Utilizza i seguenti collegamenti per accedere alla pagina relativa al servizio. Per visualizzare le quote di servizio per tutti i servizi AWS nella documentazione senza cambiare pagina, visualizza invece le informazioni nella pagina Endpoint e quote del servizio nel PDF.

Amplify	Amazon ECR
Athena	Lambda
CloudFront	OpenSearch Servizio
Cognito*	Neptune
Config	Amazon S3

Amazon ECS	

CloudFormation Quote AWS

Il tuo account AWS ha CloudFormation quote AWS di cui dovresti essere a conoscenza quando avvii lo stack di questa soluzione. Comprendendo queste quote, puoi evitare errori di limitazione che potrebbero impedirti di implementare questa soluzione con successo. Per ulteriori informazioni, consulta le CloudFormation quote AWS nella AWS CloudFormation User's Guide.

Quote AWS Lambda

Il tuo account ha una quota di esecuzione simultanea di AWS Lambda pari a 1000. Se la soluzione viene utilizzata in un account in cui sono presenti altri carichi di lavoro in esecuzione e che utilizzano Lambda, imposta questa quota su un valore appropriato. Questo valore è regolabile; per ulteriori informazioni, consulta le quote di AWS Lambda nella AWS Lambda User's Guide.

> **Note**
>
> Questa soluzione richiede 150 esecuzioni dalla quota di esecuzione simultanea per essere disponibile nell'account in cui viene distribuita la soluzione. Se in quell'account sono disponibili meno di 150 esecuzioni, la CloudFormation distribuzione avrà esito negativo.

Quote Amazon VPC

Il tuo account AWS può contenere cinque VPCs e due Elastic IPs (EIPs). Se la soluzione viene utilizzata in un account con un altro VPCs o EIPs, ciò potrebbe impedire la corretta implementazione della soluzione. Se corri il rischio di raggiungere questa quota, puoi fornire il tuo VPC per la distribuzione fornendolo quando segui i passaggi nella sezione Launch the Stack. Per ulteriori informazioni, consulta le quote di Amazon VPC nella Amazon VPC User's Guide.

Scelta dell'account di distribuzione

Se stai distribuendo Workload Discovery su AWS su un'organizzazione AWS, la soluzione deve essere installata in un account amministratore delegato in cui siano state abilitate StackSetsle funzionalità AWS Config multiregione.

Se non utilizzi AWS Organizations, ti consigliamo di distribuire Workload Discovery on AWS in un account AWS dedicato creato appositamente per questa soluzione. Questo approccio significa che Workload Discovery on AWS è isolato dai carichi di lavoro esistenti e fornisce un'unica posizione per la configurazione della soluzione, ad esempio l'aggiunta di utenti e l'importazione di nuove regioni. Inoltre, è più facile tenere traccia dei costi sostenuti durante l'esecuzione della soluzione.

Dopo aver distribuito Workload Discovery on AWS, puoi importare le regioni da qualsiasi account di cui hai già effettuato il provisioning.

Implementa la soluzione

Questa soluzione utilizza CloudFormation modelli e stack AWS per automatizzarne l'implementazione. Il CloudFormation modello specifica le risorse AWS incluse in questa soluzione e le relative proprietà. Lo CloudFormation stack fornisce le risorse descritte nel modello.

Panoramica del processo di distribuzione

> **Note**
>
> Se in precedenza hai distribuito Workload Discovery su AWS e desideri eseguire l'aggiornamento alla versione più recente, consulta Aggiornare la soluzione.

Segui le step-by-step istruzioni in questa sezione per configurare e distribuire la soluzione nel tuo account.

Tempo di implementazione: circa 30 minuti

Prima di avviare la soluzione, esaminate i costi, l'architettura, la sicurezza di rete e altre considerazioni discusse in questa guida.

> **Important**
>
> Questa soluzione include un'opzione per inviare metriche operative anonime ad AWS. Utilizziamo questi dati per comprendere meglio come i clienti utilizzano questa soluzione e i servizi e i prodotti correlati. AWS è proprietaria dei dati raccolti tramite questo sondaggio. La raccolta dei dati è soggetta all'Informativa sulla privacy di AWS.

Prerequisiti

Raccogli i dettagli dei parametri di distribuzione

Prima di distribuire Workload Discovery su AWS, esamina i dettagli di configurazione per il ruolo collegato ai servizi Amazon OpenSearch Service e AWS Config.

Verifica se hai un ruolo AWSService RoleForAmazonOpenSearchService

L'implementazione crea un cluster Amazon OpenSearch Service all'interno di un Amazon Virtual Private Cloud (Amazon VPC). Il modello utilizza un ruolo collegato al servizio per creare il OpenSearch cluster di servizi. Tuttavia, se hai già creato il ruolo nel tuo account, usa il ruolo esistente.

Per verificare se hai già questo ruolo:

1. Accedi alla console Identity and Access Management (IAM) per l'account su cui intendi implementare questa soluzione.
2. Nella casella Search (Cerca) immettere `AWSServiceRoleForAmazonOpenSearchService`.
3. Se la ricerca restituisce un ruolo, No selezionalo come CreateOpensearchServiceRoleparametro all'avvio dello stack.

Verifica che AWS Config sia configurato

Workload Discovery on AWS utilizza AWS Config per raccogliere la maggior parte delle configurazioni di risorse. Quando distribuisci la soluzione o importi una nuova regione, devi confermare se AWS Config è già configurato e funziona come previsto. Il AlreadyHaveConfigSetup CloudFormation parametro indica a Workload Discovery on AWS se configurare AWS Config.

Il seguente frammento è tratto da AWS CLI Command Reference. Esegui il comando nella regione in cui intendi distribuire Workload Discovery su AWS o importalo in Workload Discovery on AWS.

Immetti il comando seguente:

```
aws configservice get-status
```

Se ricevi una risposta simile all'output, in quella regione sono in esecuzione un Configuration Recorder e un Delivery Channel. Seleziona `Yes` per il AlreadyHaveConfigSetup CloudFormation parametro.

Output:

```
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
```

Se stai configurando AWS CloudFormation StackSets, devi includere questa regione nel batch di regioni in cui AWS Config è già configurato.

Verifica i dettagli di AWS Config nel tuo account

La distribuzione tenterà di configurare AWS Config. Se utilizzi già AWS Config nell'account che intendi distribuire o rendere rilevabile tramite Workload Discovery su AWS, seleziona i parametri pertinenti quando distribuisci questa soluzione. Inoltre, per una corretta implementazione, assicurati di non aver limitato le risorse scansionate da AWS Config.

Per verificare la configurazione corrente di AWS Config:

1. Accedi alla console AWS Config.
2. Scegli Impostazioni e assicurati che le caselle Registra tutte le risorse supportate in questa regione e Includi risorse globali siano selezionate.

Verifica la configurazione VPC

Se esegui la distribuzione su un VPC esistente, verifica che le sottoreti private possano indirizzare le richieste ai servizi AWS.

Se scegli l'opzione per implementare la soluzione in un VPC esistente, devi assicurarti che le funzioni di Workload Discovery on AWS Lambda e le attività Amazon ECS in esecuzione nelle sottoreti private del tuo VPC possano connettersi ad altri servizi AWS. Il modo standard per abilitarlo è con i gateway NAT. Puoi elencare i gateway NAT presenti nel tuo account come mostrato nel seguente esempio di codice.

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

Output:

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

> **Note**
>
> Se restituiscono meno di due risultati, le sottoreti non hanno il numero corretto di gateway NAT.

Se il tuo VPC non dispone di gateway NAT, devi eseguirne il provisioning o assicurarti di disporre di endpoint VPC per tutti i servizi AWS elencati nella sezione AWS. APIs

CloudFormation Modello AWS

Questa soluzione utilizza AWS CloudFormation per automatizzare la distribuzione di Workload Discovery su AWS nel cloud AWS. Include il seguente CloudFormation modello, che puoi scaricare prima della distribuzione:

View template

workload-discovery-on-aws.template: utilizza questo modello per avviare la soluzione e tutti i componenti associati. La configurazione predefinita implementa le soluzioni principali e di supporto disponibili nei servizi AWS in questa sezione delle soluzioni, ma puoi personalizzare il modello per soddisfare le tue esigenze specifiche.

> **Note**
>
> Puoi personalizzare il modello per soddisfare le tue esigenze specifiche; tuttavia, eventuali modifiche apportate potrebbero influire sul processo di aggiornamento.

Avvio dello stack

Questo CloudFormation modello AWS automatizzato distribuisce Workload Discovery su AWS nel cloud AWS. È necessario raccogliere i dettagli dei parametri di distribuzione prima di avviare lo stack. Per i dettagli, consulta Prerequisiti.

Tempo di implementazione: circa 30 minuti

1. Accedi alla Console di gestione AWS e seleziona il pulsante per avviare il CloudFormation modello `workload-discovery-on-aws.template` AWS.

2. Per impostazione predefinita, il modello viene avviato nella regione Stati Uniti orientali (Virginia settentrionale). Per avviare la soluzione in un'altra regione AWS, utilizza il selettore della regione nella barra di navigazione della console.

> **Note**
>
> Questa soluzione utilizza servizi che non sono disponibili in tutte le regioni AWS. Per un elenco delle regioni AWS supportate, consulta la sezione Regioni AWS supportate.

3. Nella pagina Create stack, verifica che l'URL del modello corretto sia nella casella di testo URL Amazon S3 e scegli Avanti.
4. Nella pagina Specificare i dettagli dello stack, assegna un nome allo stack di soluzioni. Per informazioni sulle limitazioni dei caratteri di denominazione, consulta le quote IAM e AWS STS nella AWS Identity and Access Management User Guide.
5. In Parametri, esamina i parametri per questo modello di soluzione e modificali se necessario. Questa soluzione utilizza i seguenti valori predefiniti.

Parametro	Predefinito	Descrizione
AdminUserEmailAddress	*<Requires input>*	Un indirizzo e-mail per creare il primo utente. Le credenziali temporanee verranno inviate a questo indirizzo e-mail.

Parametro	Predefinito	Descrizione
AlreadyHaveConfigSetup	`No`	Conferma del fatto che AWS Config sia già configurato o meno nell'account di distribuzione. Per i dettagli, consulta Prerequisiti.
AthenaWorkgroup	`primary`	Il gruppo di lavoro che verrà utilizzato per inviare la query Athena quando la funzionalità Costo è abilitata.
ApiAllowListedRanges	`0.0.0.0/1,128.0.0.0/1`	Elenco separato da virgole CIDRs per gestire l'accesso all'API AppSync GraphQL. Per consentire l'intero accesso a Internet, usa 0.0.0.0/1,128.0.0.0/1. Se si limita l'accesso a elementi specifici CIDRs, è necessario includere anche gli indirizzi IP (e una subnet mask di /32) dei gateway NAT che consentono all'attività ECS del processo di rilevamento in esecuzione nella relativa sottorete privata di accedere a Internet. NOTA: questo elenco di autorizzazioni non regola l'accesso alla WebUI, ma solo all'API GraphQL.

Parametro	Predefinito	Descrizione
CreateNeptuneReplica	No	Scegli se creare una replica di lettura per Neptune in una zona di disponibilità separata. La scelta Yes migliora la resilienza ma aumenta il costo di questa soluzione.
CreateOpenSearchServiceRole	Yes	Conferma del fatto che tu abbia già o meno un ruolo collegato al servizio per Amazon OpenSearch Service. Per i dettagli, consulta Prerequisiti.
NeptuneInstanceClass	db.r5.large	Il tipo di istanza utilizzato per ospitare il database Amazon Neptune. Ciò che selezioni qui influisce sul costo di esecuzione di questa soluzione.
OpensearchInstanceType	m6g.large.search	Il tipo di istanza utilizzato per i nodi dati del OpenSearch servizio. La selezione effettuata influisce sul costo di esecuzione della soluzione.
OpensearchMultiAz	No	Scegli se creare un cluster di OpenSearch servizi che si estenda su più zone di disponibilità. La scelta Yes migliora la resilienza ma aumenta il costo di questa soluzione.

Parametro	Predefinito	Descrizione
CrossAccountDiscovery	`SELF_MANAGED`	Scegli se Workload Discovery on AWS o AWS Organizations gestisca l'importazione degli account. Il valore può essere `SELF_MANAGED` o `AWS_ORGANIZATIONS` .
OrganizationUnitId	<Optional input>	L'ID dell'unità organizzativa principale. Questo parametro viene utilizzato solo quando CrossAccountDiscoveryè impostato su`AWS_ORGANIZATIONS` .
AccountType	`DELEGATED_ADMIN`	Il tipo di account AWS Organizations in cui installare Workload Discovery on AWS. Questo parametro viene utilizzato solo quando CrossAccountDiscoveryè impostato su. `AWS_ORGANIZATIONS` Per i dettagli, consulta Scelta dell'account di distribuzione.

Parametro	Predefinito	Descrizione
ConfigAggregatorName	<Optional input>	L'aggregatore Config a livello di organizzazione AWS da utilizzare. È necessario installare la soluzione nello stesso account e nella stessa regione di questo aggregato re. Se lasci vuoto questo parametro, verrà creato un nuovo aggregatore. Questo parametro viene utilizzat o solo quando CrossAcco untDiscoveryè impostato su. `AWS;_ORGANIZATIONS`
CpuUnits	`1 vCPU`	Il numero di elementi CPUs da allocare per l'attività Fargate in cui viene eseguito il processo di scoperta.
Memoria	`2048`	La quantità di memoria da allocare per l'attività Fargate in cui viene eseguito il processo di rilevamento.
DiscoveryTaskFrequency	`15mins`	L'intervallo di tempo tra ogni esecuzione dell'attività ECS del processo di scoperta.

Parametro	Predefinito	Descrizione
MinNCUs	1	Unità di capacità minima di Neptune NCUs () da impostare sul cluster Neptune (deve essere inferiore o uguale a Max). NCUs Obbligatorio se il tipo è. DBInstance `db.serverless`
MaxNCUs	128	Massimo NCUs da impostare sul cluster Neptune (deve essere maggiore o uguale a Min). NCUs Obbligatorio se il DBInstance tipo è. `db.serverless`
VpcId	<Optional input>	L'ID di un VPC esistente per la soluzione da utilizzare. Se lasci vuoto questo parametro , verrà eseguito il provisioning di un nuovo VPC.
VpcCidrBlock	<Optional input>	Il blocco VPC CIDR del VPC a cui fa riferimento il parametro. VpcId Questo parametro viene utilizzato solo se il VpcIdparametro è impostato.
PrivateSubnet0	<Optional input>	La sottorete privata che desideri utilizzare. Questo parametro viene utilizzato solo se il VpcIdparametro è impostato.

Parametro	Predefinito	Descrizione
PrivateSubnet1	<Optional input>	La sottorete privata che desideri utilizzare. Questo parametro viene utilizzato solo se il VpcIdparametro è impostato.
UsesCustomIdentity	No	Conferma se intendi utilizzare o meno un provider di identità personalizzato, come SAML o OIDC.
CognitoCustomDomain	<Optional input>	Il prefisso di dominio per il dominio personalizzato Amazon Cognito che ospita le pagine di registrazione e accesso per la tua applicazione. Lascia vuoto se non utilizzi un IdP personalizzato, altrimenti devi includere solo lettere minuscole, numeri e trattini.
CognitoAttributeMapping	<Optional input>	La mappatura degli attributi IdP agli attributi del pool di utenti Cognito standard e personalizzati. Lascia vuoto se non stai utilizzando un IdP personalizzato, altrimenti deve essere una stringa JSON valida.
IdentityType	<Optional input>	Il tipo di Identity Provider da utilizzare (`GoogleSAML`, `oOIDC`). Lascia vuoto se non utilizzi un IdP personalizzato.

Parametro	Predefinito	Descrizione
ProviderName	<Optional input>	Nome dell'Identity Provider. Lascia vuoto se non utilizzi un IdP personalizzato.
GoogleClientId	<Optional input>	L'ID client di Google da utilizzare. Parametro utilizzato solo quando IdentityTypeè impostato su`Google`.
GoogleClientSecret	<Optional input>	Il segreto del client Google da utilizzare. Parametro utilizzato solo quando IdentityTypeè impostato su`Google`.
SAMLMetadataURL	<Optional input>	L'URL dei metadati per il provider di identità SAML. Parametro utilizzato solo quando IdentityTypeè impostato su SAML.
OIDCClientId	<Optional input>	L'ID client OIDC da utilizzare. Parametro utilizzato solo quando IdentityTypeè impostato su. `OIDC`
OIDCClientSecret	<Optional input>	Il segreto del client OIDC da usare. Parametro utilizzato solo quando IdentityTypeè impostato su. `OIDC`
OIDCIssuerURL	<Optional input>	L'URL dell'emittente OIDC da utilizzare. Parametro utilizzato solo quando IdentityTypeè impostato su. `OIDC`

Parametro	Predefinito	Descrizione
OIDCAttributeRequestMethod	`GET`	Il metodo di richiesta degli attributi OIDC da utilizzare. Deve essere `GET` o `POST` (fare riferimento al provider OIDC o utilizzare il valore predefinito). Parametro utilizzato solo quando IdentityTypeè impostato su. `OIDC`

6. Scegli Next (Successivo).
7. Nella pagina Configure stack options (Configura opzioni pila), scegliere Next (Successivo).
8. Nella pagina Rivedi e crea, rivedi e conferma le impostazioni. Seleziona le caselle che riconoscono che il modello crea risorse IAM e richiede determinate funzionalità.
9. Scegli Invia per distribuire lo stack.

   Puoi visualizzare lo stato dello stack nella CloudFormation console AWS nella colonna Status. Dovresti ricevere lo status CREATE_COMPLETE in circa 30 minuti.

> **Note**
>
> Se eliminato, questo stack rimuove tutte le risorse. Se lo stack viene aggiornato, mantiene il pool di utenti di Amazon Cognito per garantire che gli utenti configurati non vadano persi.

Attività di configurazione successive all'implementazione

Dopo che Workload Discovery on AWS è stato distribuito correttamente, completa le seguenti attività di configurazione post-implementazione.

Attiva la sicurezza avanzata in Amazon Cognito

Per attivare le funzionalità di sicurezza avanzate per Amazon Cognito, segui le istruzioni su Aggiungere sicurezza avanzata a un pool di utenti nella Amazon Cognito Developer Guide.

> **Note**
>
> È previsto un costo aggiuntivo per l'attivazione della sicurezza avanzata in Amazon Cognito.

Crea utenti Amazon Cognito

Workload Discovery on AWS utilizza Amazon Cognito per gestire tutti gli utenti e l'autenticazione. Crea un utente per te durante la distribuzione e invia un'e-mail all'indirizzo fornito nel AdminUserEmailAddress parametro con credenziali temporanee.

Per creare utenti aggiuntivi:

1. Accedi alla console AWS Cognito.
2. Scegli Manage User Pools (Gestisci pool di utenti).
3. Scegli WDCognitoUserPool-*<ID-string>*.
4. Nel riquadro di navigazione, in Impostazioni generali, scegli Utenti e gruppi.
5. Nella scheda Utenti, scegli Crea utente.
6. Nella casella Crea utente, inserisci i valori per tutti i campi obbligatori.

Campo del modulo	Obbligatorio?	Descrizione
Username	Sì	Il nome utente che utilizzer ai per accedere a Workload Discovery on AWS.

Campo del modulo	Obbligatorio?	Descrizione
Invia un invito	Sì (solo e-mail)	Se selezionata, invia una notifica come promemoria della password temporane a. Seleziona Solo e-mail. Se selezioni SMS (impostazione predefinita), viene visualizz ato un messaggio di errore, ma l'utente viene comunque creato.
Password temporanea	Sì	Inserisci una password temporanea. L'utente è obbligato a modificarlo quando accede a Workload Discovery on AWS per la prima volta.
Numero di telefono	No	Inserisci un numero di telefono in formato internazi onale, `\+44` ad esempio. Assicurati che il numero di telefono di Mark sia verificat o? la casella è selezionata.
E-mail	Sì	Inserisci un indirizzo email valido. Assicurati che l'email Contrassegna come verificat a? la casella è selezionata.

7. Selezionare Create user (Crea utente).

Ripeti questo processo per creare tutti gli utenti di cui hai bisogno.

> **Note**
>
> Ogni utente avrà lo stesso livello di accesso alle risorse scoperte. Consigliamo di effettuare il provisioning di una distribuzione separata di Workload Discovery on AWS per gli account che contengono carichi di lavoro o dati sensibili. Ciò consente di limitare l'accesso solo agli utenti che ne hanno bisogno.

Accedi a Workload Discovery su AWS

Dopo che la soluzione è stata implementata correttamente, determina l'URL per la CloudFront distribuzione Amazon che serve l'interfaccia utente Web della soluzione.

1. Accedi alla CloudFormation console AWS.
2. Scegli View nested per visualizzare gli stack nidificati che compongono la distribuzione. A seconda delle preferenze, gli stack nidificati potrebbero già essere visualizzati.
3. Seleziona lo stack principale di Workload Discovery on AWS.
4. Seleziona la scheda Output e scegli l'URL nella colonna Valore associata alla chiave. WebUiUrl
5. Nella schermata Accedi a, inserisci le credenziali di accesso che hai ricevuto via e-mail. Quindi intraprendi le seguenti azioni:
   a. Segui le istruzioni per modificare la password.
   b. Utilizza il codice di verifica inviato alla tua email per completare il ripristino dell'account.

Importa una regione

> **Note**
>
> La sezione seguente si applica solo quando la modalità di individuazione degli account della soluzione è gestita automaticamente. Per informazioni su come funziona l'individuazione degli account in modalità AWS Organizations, consulta la sezione AWS Organizations Account Discovery Mode.

L'importazione di una regione richiede l'implementazione di una determinata infrastruttura. Questa infrastruttura è costituita da risorse globali e regionali:

Globale: risorse che vengono distribuite una sola volta in un account e riutilizzate per ogni regione importata.

- Un ruolo IAM () WorkloadDiscoveryRole

Regionale: risorse distribuite in ogni regione importate.

- Un canale di distribuzione AWS Config
- Un bucket Amazon S3 per AWS Config
- Un ruolo IAM () ConfigRole

Esistono due opzioni per implementare questa infrastruttura:

- AWS CloudFormation StackSets (consigliato)
- AWS CloudFormation

Importa una regione

Questi passaggi ti guidano nell'importazione di una regione e nella distribuzione dei modelli CloudFormation AWS.

1. Accedi a Workload Discovery su AWS. Per l'URL, consulta Accedi a Workload Discovery on AWS.
2. Nel menu di navigazione, seleziona Account.
3. Seleziona Importa.
4. Seleziona il metodo di importazione:
   a. Aggiungi account e regioni utilizzando un file CSV.
   b. Aggiungi account e regioni utilizzando un modulo.

File CSV

Fornisci un file CSV (Comma Separated Value) che contenga le regioni da importare nel seguente 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. Seleziona Carica un file CSV.
2. Individua e apri il tuo file CSV.
3. Controlla la tabella Regioni, quindi seleziona Importa.
4. Nella finestra di dialogo modale, scarica il modello Risorse globali e il modello Risorse regionali.
5. Distribuisci i CloudFormation modelli negli account pertinenti (consulta la sezione Distribuisci i CloudFormation modelli AWS).
6. Una volta distribuiti i modelli di risorse globali e regionali, seleziona entrambe le caselle per confermare che l'installazione è completa e scegli Importa.

Modulo

Fornisci le regioni da importare utilizzando il modulo:

1. Per Account ID, inserisci un ID account a 12 cifre o seleziona un ID account esistente.
2. Per Nome account, inserisci un nome di account o utilizza un valore precompilato quando selezioni un ID account esistente.
3. Seleziona le regioni da importare.
4. Seleziona Aggiungi per compilare le Regioni nella tabella Regioni riportata di seguito.
5. Esamina la tabella Regioni, quindi seleziona Importa.
6. Nella finestra di dialogo modale, scarica il modello Risorse globali e il modello Risorse regionali.
7. Distribuisci i CloudFormation modelli negli account pertinenti (consulta la sezione Distribuisci i CloudFormation modelli AWS).
8. Una volta distribuiti i modelli di risorse globali e regionali, seleziona entrambe le caselle per confermare che l'installazione è completa e scegli Importa.

Implementa i modelli AWS CloudFormation

Le risorse globali devono essere distribuite una volta per account. Non distribuire questo modello quando si importa una regione da un account che contiene una regione già importata in Workload

Discovery on AWS. Se la regione è già stata importata, segui le istruzioni in Distribuisci lo stack per fornire le risorse regionali.

CloudFormation StackSets Da utilizzare per fornire risorse globali tra più account

> **Important**
>
> Innanzitutto, completa i prerequisiti per l'attivazione delle operazioni di stack set StackSets negli account di destinazione.

1. Nell'account amministratore, accedi alla CloudFormation console AWS.
2. Dal menu di navigazione, seleziona StackSets.
3. Scegli Create StackSet (Crea).
4. Nella pagina Scegli un modello, sotto Autorizzazioni:
   a. Se utilizzi AWS Organizations, scegli tra le autorizzazioni gestite dal servizio o le autorizzazioni self-service. Per i dettagli, consulta Using StackSets in an AWS Organization.
   b. Se non utilizzi AWS Organizations, inserisci il nome del ruolo di esecuzione IAM utilizzato quando segui i passaggi dei StackSets prerequisiti. Per i dettagli, consulta Concedi autorizzazioni autogestite.
5. In Specificare il modello, seleziona Carica un file modello. Scegli il `global-resources.template` file (scaricato in precedenza quando hai importato una regione tramite file CSV o modulo) e scegli Avanti.
6. Nella pagina Specificare StackSet i dettagli, assegna un nome al tuo. StackSet Per informazioni sulle limitazioni dei caratteri di denominazione, consulta le quote IAM e AWS STS nella AWS Identity and Access Management User Guide.
7. In Parametri, esamina i parametri per questo modello di soluzione e modificali se necessario. Questa soluzione utilizza i seguenti valori predefiniti.

Nome campo	Predefinito	Descrizione
AccountId	L'ID dell'account di distribuzione	L'ID dell'account di distribuzione originale. È necessario

Nome campo	Predefinito	Descrizione
		lasciare questo valore come predefinito.

1. Scegli Next (Successivo).
2. Nella pagina Configura StackSet opzioni, scegli Avanti.
3. Nella pagina Imposta opzioni di distribuzione, in Account, inserisci l'account IDs per la distribuzione del ruolo dell'account nella casella Numeri di account.
4. In Specificare le regioni, seleziona una regione per installare lo stack.
5. In Opzioni di distribuzione, seleziona Parallelo, quindi scegli Avanti.
6. Nella pagina di revisione, seleziona la casella per confermare che AWS CloudFormation potrebbe creare risorse IAM con nomi personalizzati.
7. Scegli Invia.

CloudFormation StackSets Da utilizzare per fornire risorse regionali

> **Important**
>
> Innanzitutto, completa i prerequisiti per l'attivazione delle operazioni di stack set StackSets negli account di destinazione.
> Se hai alcune regioni con AWS Config installato e altre senza, devi eseguire due StackSet operazioni, una per le regioni con AWS Config installato e una per quelle senza.

1. Nell'account amministratore, accedi alla CloudFormation console AWS.
2. Dal menu di navigazione, seleziona StackSets.
3. Scegli Create StackSet (Crea).
4. Nella pagina Scegli un modello, sotto Autorizzazioni:
   a. Se utilizzi AWS Organizations, scegli tra le autorizzazioni gestite dal servizio o le autorizzazioni self-service. Per i dettagli, consulta Using StackSets in an AWS Organization.
   b. Se non utilizzi AWS Organizations, inserisci il nome del ruolo di esecuzione IAM utilizzato quando segui i passaggi dei StackSets prerequisiti. Per i dettagli, consulta Concedi autorizzazioni autogestite.

5. In Specificare il modello, seleziona Carica un file modello. Scegli il `regional-resources.template` file (scaricato in precedenza quando hai importato una regione tramite file CSV o modulo) e scegli Avanti.
6. Nella pagina Specificare StackSet i dettagli, assegna un nome al tuo. StackSet Per informazioni sulle limitazioni dei caratteri di denominazione, consulta le quote IAM e AWS STS nella AWS Identity and Access Management User Guide.
7. In Parametri, esamina i parametri per questo modello di soluzione e modificali se necessario. Questa soluzione utilizza i seguenti valori predefiniti.

Nome campo	Predefinito	Descrizione
AccountId	L'ID dell'account di distribuzione	L'ID dell'account di distribuzione originale. È necessario lasciare questo valore come predefinito.
AggregationRegion	La regione di distribuzione	La regione in cui era stato originariamente schierato. È necessario lasciare questo valore come predefinito.
AlreadyHaveConfigSetup	`No`	Verifica se nella regione è già installato AWS Config. Imposta su Sì se AWS Config è già installato in questa regione.

1. Scegli Next (Successivo).
2. Nella pagina delle StackSet opzioni di configurazione, scegli Avanti.
3. Nella pagina Imposta opzioni di distribuzione, in Account, inserisci l'account IDs a cui distribuire il ruolo dell'account nella casella Numeri di account.
4. In Specificare le regioni, seleziona una regione per installare lo stack. Questo installa lo stack in queste regioni in tutti gli account inseriti nel passaggio 6.
5. In Opzioni di distribuzione, seleziona Parallelo, quindi scegli Avanti.

6. Nella pagina di revisione, seleziona la casella per confermare che AWS CloudFormation potrebbe creare risorse IAM con nomi personalizzati.
7. Scegli Invia.

Implementa lo stack per fornire le risorse globali utilizzando CloudFormation

Le risorse globali devono essere distribuite una volta per account. Non distribuire questo modello quando si importa una regione da un account che contiene una regione già importata in Workload Discovery on AWS.

1. Accedi alla CloudFormation console AWS.
2. Scegli Create stack, quindi seleziona Con nuove risorse (standard).
3. Nella pagina Crea stack, nella sezione Specificare il modello, seleziona Carica un file modello.
4. Scegli file e seleziona il **`global-resources.template`** file (scaricato in precedenza quando importavi una regione tramite file CSV o modulo), quindi scegli Avanti.
5. Nella pagina Specificare i dettagli dello stack, assegna un nome allo stack di soluzioni. Per informazioni sulle limitazioni dei caratteri di denominazione, consulta le quote IAM e AWS STS nella _AWS Identity and Access Management _User Guide.
6. In Parametri, esamina i parametri per questo modello di soluzione e modificali se necessario. Questa soluzione utilizza i seguenti valori predefiniti.

Nome campo	Predefinito	Descrizione
Stack name (Nome stack)	`workload-discovery`	Il nome di questo CloudFormation stack AWS.
AccountId	ID dell'account di distribuzione	L'ID dell'account di distribuzione originale. È necessario lasciare questo valore come predefinito.

1. Scegli Next (Successivo).
2. Seleziona la casella riconoscendo che AWS CloudFormation potrebbe creare risorse IAM con nomi personalizzati.

3. Seleziona Crea stack.

Le nuove regioni verranno scansionate durante il successivo processo di scoperta, che viene eseguito a intervalli di 15 minuti, ad esempio: 15:00, 15:15, 15:30, 15:45.

Implementa lo stack per fornire le risorse regionali utilizzando CloudFormation

1. Accedi alla CloudFormation console AWS.
2. Scegli Create stack, quindi seleziona Con nuove risorse (standard).
3. Nella pagina Crea stack, nella sezione Specificare il modello, seleziona Carica un file modello.
4. Scegli file e seleziona il **`regional-resources.template`** file (scaricato in precedenza quando importavi una regione tramite file CSV o modulo), quindi scegli Avanti.
5. Nella pagina Specificare i dettagli dello stack, assegna un nome allo stack di soluzioni. Per informazioni sulle limitazioni dei caratteri di denominazione, consulta le quote IAM e AWS STS nella AWS Identity and Access Management User Guide.
6. In Parametri, esamina i parametri per questo modello di soluzione e modificali se necessario. Questa soluzione utilizza i seguenti valori predefiniti.

Nome campo	Predefinito	Descrizione
AccountId	ID dell'account di distribuzione della soluzione	L'ID dell'account di distribuzione originale. Deve essere lasciato come predefinito.
AggregationRegion	Regione di distribuzione della soluzione	La regione in cui è stata originariamente distribuita. Deve essere lasciato come predefinito.
AlreadyHaveConfigSetup	`No`	Verifica se nella regione è già installato AWS Config. Imposta `Yes` se AWS Config è già installato in questa regione.

1. Scegli Next (Successivo).
2. Seleziona la casella riconoscendo che AWS CloudFormation potrebbe creare risorse IAM con nomi personalizzati.
3. Seleziona Crea stack.

Le nuove regioni verranno scansionate durante il successivo processo di scoperta, che viene eseguito a intervalli di 15 minuti, ad esempio alle 15:00, 15:15, 15:30, 15:45.

Verifica che la regione sia stata importata correttamente

1. Accedi all'interfaccia utente web della soluzione (o aggiorna la pagina se è già caricata). Per l'URL, consulta Accedi a Workload Discovery on AWS.
2. Dal pannello di navigazione a sinistra, in Impostazioni, seleziona Regioni importate.

La regione, il nome dell'account e l'ID dell'account vengono visualizzati nella tabella. La colonna Ultima scansione mostra le ultime risorse scoperte in quella regione.

> **Note**
>
> Se la colonna Ultima scansione rimane vuota per più di 30 minuti, consulta Debugging the discovery component.

Imposta la funzionalità relativa ai costi

La funzionalità relativa ai costi richiede la configurazione manuale dei report AWS Cost and Usage (CUR). Seguendo le istruzioni riportate di seguito potrai:

1. Configurare un CUR pianificato.
2. Configura la replica di Amazon S3 (quando non CURs sei all'account di distribuzione)

Crea il report sui costi e l'utilizzo di AWS nell'account di distribuzione

1. Accedi alla console di fatturazione dell'account da cui desideri raccogliere i dati sui costi.
2. Nel menu di navigazione, in Fatturazione, seleziona Rapporti su costi e utilizzo.
3. Scegli Crea rapporto.

4. Usa `workload-discovery-cost-and-usage-` *<your-workload-discovery-deployment-account-ID>* come nome del rapporto.

> **Note**
>
> È necessario seguire questa convenzione di denominazione perché verrà implementata una piccola quantità di infrastruttura per facilitare l'interrogazione di. CURs

5. Seleziona la casella Includi risorsa. IDs

> **Note**
>
> È necessario selezionare la IDs casella Includi risorsa per visualizzare i dati sui costi. Questo ID deve corrispondere alle risorse scoperte da Workload Discovery on AWS.

6. Scegli Next (Successivo).
7. Nella pagina Opzioni di consegna, scegli Configura 0
8. Seleziona il bucket *<stack-name>* `-s3buc-costandusagereportbucket-` *<ID-string>* Amazon S3 per archiviare il CUR. Scegli Next (Successivo).
9. Controlla la politica, seleziona la casella di conferma e scegli Salva.
10. Imposta il percorso del prefisso del rapporto su`aws-perspective`.
11. Seleziona Giornaliero per la granularità temporale.
12. In Abilita l'integrazione dei dati dei report per, seleziona Amazon Athena.
13. Scegli Next (Successivo).
14. Scegli Rivedi e completa.

Per verificare che il report sia configurato correttamente, controlla il file di test nel bucket Amazon S3.

> **Note**
>
> Il caricamento dei report nel tuo bucket può richiedere fino a 24 ore.

Crea il report sui costi e l'utilizzo di AWS in un account esterno

1. Accedi alla console di fatturazione dell'account da cui desideri raccogliere i dati sui costi.

2. Nel menu di navigazione, sotto Gestione dei costi, seleziona Rapporti su costi e utilizzo.
3. Scegli Crea rapporto.
4. Usa `workload-discovery-cost-and-usage-` *`<your-external-account-ID>`* come nome del rapporto.

> **Note**
>
> È necessario seguire questa convenzione di denominazione perché verrà implementata una piccola quantità di infrastruttura per facilitare l'interrogazione di. CURs

5. Seleziona la casella Includi risorsa. IDs

> **Note**
>
> È necessario selezionare la IDs casella Includi risorsa per visualizzare i dati sui costi. Questo ID è necessario per corrispondere alle risorse scoperte da Workload Discovery on AWS.

6. Scegli Next (Successivo).
7. Nella pagina Opzioni di consegna, scegli Configura 0
8. Crea un nuovo bucket Amazon S3 per archiviare. CURs
9. Controlla la politica, seleziona la casella di conferma e scegli Salva.
10. Imposta il percorso del prefisso del rapporto su `aws-perspective`.
11. Seleziona Giornaliero per la granularità temporale.
12. In Abilita l'integrazione dei dati dei report per, seleziona Amazon Athena.
13. Scegli Next (Successivo).
14. Scegli Rivedi e completa. Per verificare che il report sia configurato correttamente, controlla il file di test nel bucket Amazon S3.

> **Note**
>
> Il caricamento dei report nel tuo bucket può richiedere fino a 24 ore.

Quindi, configura la replica sull'account di distribuzione.

Configurare la replica

Configura la replica nel bucket Amazon S3 creato durante la distribuzione. Il bucket Amazon S3 segue il seguente formato:. *<stack-name>* `-s3buc-costandusagereportbucket-` *<ID-string>* Ciò consente alla soluzione di interrogare il bucket con Amazon Athena.

1. Accedi all'account AWS nella console Amazon S3 che contiene il CUR creato che deve essere replicato.
2. Seleziona il bucket Amazon S3 creato durante la configurazione del tuo CUR. Per ulteriori informazioni, consulta la fase 8 di Creazione e pianificazione del report sui costi e sull'utilizzo di AWS.
3. Scegliere la scheda Management (Gestione),
4. In Regole di replica, scegli Crea regola di replica.
5. In Configurazione delle regole di replica, nella casella Nome regola di replica, inserisci un ID descrittivo della regola.
6. In Source bucket, seleziona Applica a tutti gli oggetti nel bucket per configurare l'ambito della regola.
7. In Destinazione, configura quanto segue:
   a. Seleziona Specificare un bucket in un altro account.
   b. Inserisci l'ID dell'account.
   c. Inserisci un valore per il nome Bucket che è stato creato durante la distribuzione di Workload Discovery su AWS. Puoi trovarlo seguendo le istruzioni in Localizzazione delle risorse di distribuzione, utilizzando l'ID logico `CostAndUsageReportBucket` e il nome dello stack che hai specificato durante la prima distribuzione di Workload Discovery su AWS.
   d. Seleziona la casella Cambia la proprietà dell'oggetto con il proprietario del bucket di destinazione.
8. In Ruolo IAM, scegli Crea nuovo ruolo.

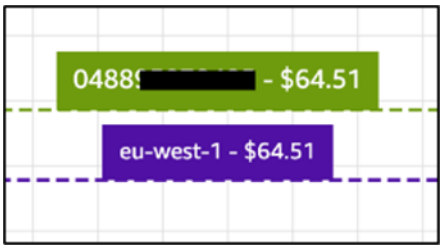
> **Note**
>
> Potrebbe già esistere un ruolo di replica. È possibile selezionarlo e assicurarsi che disponga delle azioni del ruolo di replica S3 richieste.

9. Scegli Save (Salva).

10. Accedi alla Console di gestione AWS in cui è installato CUR, vai alla pagina del servizio S3 e seleziona il bucket `CostAndUsageReportBucket` S3. Per i dettagli, consulta Localizzazione delle risorse di distribuzione.
11. Seleziona la scheda Gestione.
12. In Regole di replica, dal menu a discesa Azioni, seleziona Ricevi oggetti replicati.
13. In Impostazioni dell'account Source Bucket:
    a. Inserisci l'ID dell'account bucket di origine.
    b. Scegli Genera politiche.
    c. In Politiche, seleziona Visualizza la politica del bucket.
    d. Seleziona Includi l'autorizzazione a modificare la proprietà dell'oggetto in proprietario del bucket di destinazione.
    e. Scegli Applica impostazioni. Questo gli dà accesso per copiare oggetti su di esso. Fai riferimento alla policy di replica di Cost Bucket per un esempio di policy del bucket S3.

> **Note**
>
> Durante la replica CURs da più account AWS. Devi assicurarti che la policy del bucket sul bucket di destinazione (all'interno dell'account Workload Discovery on AWS) contenga l'ARN di ogni ruolo IAM che utilizzi per ogni account. Per maggiori dettagli, consulta la politica di replica di Cost Bucket.

Quando i report sono presenti nell'account, i dati sui costi vengono visualizzati nei riquadri di selezione e nelle singole risorse.



Modifica le politiche relative al ciclo di vita dei bucket S3

Durante l'implementazione, la soluzione configura le politiche del ciclo di vita su due bucket:

- `CostAndUsageReportBucket`

- `AccessLogsBucket`

> **Important**
>
> Queste politiche del ciclo di vita eliminano i dati da questi bucket dopo 90 giorni. Puoi modificare il ciclo di vita per adattarlo a qualsiasi politica interna in uso.

Monitoraggio della soluzione

Questa soluzione utilizza MyApplications e ti consente di CloudWatch AppInsightsmonitorare la tua distribuzione Workload Discovery su AWS.

Le mie applicazioni

MyApplications è un'estensione di Console Home che ti aiuta a gestire e monitorare costi, integrità, sicurezza e prestazioni delle tue applicazioni su AWS. Puoi accedere a tutte le applicazioni del tuo account, ai parametri chiave di tutte le applicazioni e a una panoramica dei parametri e degli approfondimenti su costi, sicurezza e operazioni da più console di servizio da un'unica visualizzazione nella Console di gestione AWS.

Per visualizzare la dashboard MyApplications per Workload Discovery su AWS:

1. Accedi alla Console di gestione AWS.
2. Nella barra laterale sinistra, scegli myApplications.
3. Digita `workload-discovery` nella barra di ricerca per trovare l'applicazione.
4. Seleziona l'applicazione.

CloudWatch AppInsights

CloudWatch Application Insights ti aiuta a monitorare le tue applicazioni identificando e configurando metriche chiave, log e allarmi tra le risorse applicative e lo stack tecnologico. Monitora continuamente metriche e log per rilevare e correlare anomalie ed errori. Per assistere nella risoluzione dei problemi, crea pannelli di controllo automatizzati per i problemi rilevati, che includono anomalie parametri ed errori di log correlati, insieme ad altri approfondimenti per indirizzarti verso la causa principale potenziale.

Per visualizzare la CloudWatch AppInsights dashboard per Workload Discovery on AWS:

1. Accedi alla CloudWatch console .
2. Nella barra laterale sinistra, scegli Insights, Application Insights.
3. Seleziona la scheda Applicazioni.
4. Digita `workload-discovery` nella barra di ricerca per trovare la dashboard.

5. Seleziona la dashboard.
6. Seleziona l'applicazione.

Aggiorna la soluzione

> **Important**
>
> L'aggiornamento dalla v1.x.x alla v2.x.x di Workload Discovery on AWS non è supportato. Ti consigliamo di disinstallare la versione 1.x.x di questa soluzione prima di installare la v2.x.x.

Per eseguire l'aggiornamento da una distribuzione 2.x.x, segui questi passaggi.

1. Scarica il CloudFormation modello AWS della soluzione.
2. Accedi alla CloudFormation console AWS.
3. Seleziona lo stack con il nome fornito durante la distribuzione e scegli Aggiorna.
4. Nella pagina Update stack, seleziona Sostituisci il modello corrente, quindi seleziona Carica un file modello e carica il file scaricato nel passaggio 1.
5. Scegli Next (Successivo).
6. Nella pagina Specificare i dettagli dello stack, in Parametri, rivedi i parametri e modificali se necessario.
7. Scegli Next (Successivo).
8. Nella pagina Configura le opzioni dello stack, in Opzioni di errore dello stack, assicurati che il pulsante di opzione Behavior on provisioning failure sia impostato su Ripristina tutte le risorse dello stack.
9. scegli Avanti.
10. Nella pagina Rivedi, verifica e conferma le impostazioni. Seleziona le caselle riconoscendo che il modello crea risorse IAM e richiede determinate funzionalità.
11. Scegli Update stack per distribuire lo stack.

> **Note**
>
> Se hai distribuito la soluzione in modalità di individuazione degli account autogestiti, devi aggiornare le risorse globali distribuite seguendo i passaggi nella sezione Importa una regione.

Risoluzione dei problemi

La risoluzione dei problemi noti fornisce istruzioni per mitigare gli errori noti. Se queste istruzioni non risolvono il problema, consulta la sezione Contatta AWS Support per istruzioni su come aprire un caso AWS Support per questa soluzione.

Risoluzione di problemi noti

Durante la distribuzione di Workload Discovery su AWS e nella fase successiva alla distribuzione, possono verificarsi diversi errori di configurazione comuni:

> **Note**
>
> Per semplificare la risoluzione dei problemi, consigliamo di disabilitare la funzionalità di rollback on failure nel modello AWS. CloudFormation Puoi anche trovare ulteriore assistenza per la risoluzione dei problemi nella documentazione di configurazione post-implementazione di Workload Discovery on AWS.

Errore Config Delivery Channel

Problema: durante la distribuzione del CloudFormation modello AWS principale si verifica il seguente errore:

```
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 soluzione viene distribuita in una regione in cui AWS Config è già abilitato.

Risoluzione: segui le istruzioni nella sezione dei prerequisiti e distribuisci la soluzione con il parametro impostato su. CloudFormation AlreadyHaveConfigSetup`Yes`

Tempi di implementazione di Search Resolver Stack durante la distribuzione su un VPC esistente

Problema: stack annidato che fornisce una risorsa personalizzata per creare un indice nel timeout del OpenSearch cluster con il seguente errore:

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

Motivo: le sottoreti private fornite come CloudFormation parametri non possono essere instradate verso S3 (le risorse personalizzate devono scrivere il risultato della loro esecuzione in un bucket S3 utilizzando un URL predefinito). I motivi di ciò sono generalmente due:

1. Alle sottoreti private non sono associati gateway NAT, quindi non è possibile accedere a Internet.
2. La sottorete privata utilizza endpoint VPC anziché un gateway NAT e l'endpoint del gateway S3 non è configurato correttamente.

Risoluzione:

1. Effettua il provisioning dei gateway NAT nel VPC per consentire alle attività in esecuzione in sottoreti private di accedere a Internet, utilizzando o la CLI CloudFormation AWS come indicato nella documentazione.
2. Assicurati che le tabelle di routing per le sottoreti siano state aggiornate per l'endpoint VPC S3 secondo la documentazione.

Risorse non rilevate dopo l'importazione dell'account

Problema: gli account sono stati importati tramite l'interfaccia utente Web ma sembra che non sia stata rilevata alcuna risorsa dopo l'esecuzione del processo di individuazione.

Motivo: i motivi più probabili sono i seguenti,

1. Quando il CrossAccountDiscovery CloudFormation parametro è impostato su`SELF_MANAGED`, il CloudFormation modello di risorse globali non è stato distribuito.
2. Quando il CrossAccountDiscovery CloudFormation parametro è impostato su`AWS_ORGANIZATIONS`: uno o più account non vengono rilevati e la colonna Role Status

contiene voci Not Deployed. Ciò significa che si è verificato un problema con la distribuzione automatica del modello di risorse globali utilizzando StackSets.

3. L'attività ECS del processo di rilevamento sta esaurendo la memoria. Ciò si verifica quando si importa un numero elevato di account o risorse. La colonna Last Discovered nell'interfaccia utente avrà un valore maggiore di quello specificato nel DiscoveryTaskFrequency CloudFormation parametro (il valore predefinito è 15 minuti) e si verificherà un errore di esaurimento della memoria nella console ECS.

Risoluzione:

1. Implementa il modello di risorse globali negli account richiesti, come indicato nella documentazione.
2. Vai alla regione WdGlobalResources StackSet in cui è stato distribuito Workload Discovery e controlla gli errori nelle istanze dello stack che non sono state distribuite.
3. Aggiorna il CloudFormation parametro Memory a un valore maggiore: inizia con double e continua ad aumentare fino a quando l'errore non si interrompe.

> **Note**
>
> Solo alcune combinazioni di unità CPU e valori di memoria sono valide, quindi potrebbe essere necessario aggiornare anche il CpuUnits CloudFormation parametro. L'elenco completo delle combinazioni è riportato nella documentazione ECS.

In account specifici vengono scoperte solo risorse non AWS Config

Problema: gli unici tipi di risorse rilevati dalla soluzione sono quelli elencati nella tabella della sezione Risorse supportate.

Motivo: le cause più comuni di questo problema sono,

1. Quando il CrossAccountDiscovery CloudFormation parametro è impostato su`SELF_MANAGED`, il CloudFormation modello di risorse regionali non è stato distribuito nelle regioni di ciascun account da scoprire.
2. Quando il CrossAccountDiscovery CloudFormation parametro è impostato su`SELF_MANAGED`, il CloudFormation modello di risorse regionali è stato distribuito nelle aree di diversi account

in cui Config non era abilitato, ma CloudFormation il AlreadyHaveConfigSetupparametro era erroneamente impostato su. `Yes`

3. Quando il CrossAccountDiscovery CloudFormation parametro è impostato su`AWS_ORGANIZATIONS`, AWS Config non è abilitato nelle regioni di ciascun account da scoprire. In `AWS_ORGANIZATIONS` modalità, sei responsabile dell'abilitazione di Config secondo le politiche della tua organizzazione.

Risoluzione:

1. Implementa i modelli di risorse regionali negli account richiesti, come indicato nella documentazione.
2. Elimina lo stack di risorse regionali precedentemente distribuito (in caso contrario AWS Config si troverebbe in uno stato incoerente) e riesegui la distribuzione con il parametro impostato su. CloudFormation AlreadyHaveConfigSetupNo
3. Abilita AWS Config nelle regioni di ogni account da scoprire.

Contattare AWS Support

Se disponi di AWS Developer Support, AWS Business Support o AWS Enterprise Support, puoi utilizzare il Support Center per ottenere l'assistenza di esperti su questa soluzione. Le istruzioni per eseguire tali operazioni sono fornite nelle sezioni seguenti.

Crea un caso

1. Accedi al Support Center.
2. Scegli Crea caso.

Come possiamo aiutarti?

1. Scegli Tecnico.
2. Per Assistenza, seleziona Soluzioni.
3. Per Categoria, seleziona Altre soluzioni.
4. Per Severità, seleziona l'opzione più adatta al tuo caso d'uso.

5. Quando si inseriscono i campi Servizio, Categoria e Severità, l'interfaccia compila i collegamenti alle domande più comuni per la risoluzione dei problemi. Se non riesci a risolvere la tua domanda con questi link, scegli Passaggio successivo: Informazioni aggiuntive.

Informazioni aggiuntive

1. In Oggetto, inserisci il testo che riassume la domanda o il problema.
2. Per Descrizione, descrivi il problema in dettaglio.
3. Scegli Allega file.
4. Allega le informazioni di cui AWS Support ha bisogno per elaborare la richiesta.

Aiutaci a risolvere il tuo caso più velocemente

1. Inserisci le informazioni richieste.
2. Scegli Passaggio successivo: risolvi ora o contattaci.

Risolvi subito o contattaci

1. Rivedi le soluzioni Solve now.
2. Se non riesci a risolvere il problema con queste soluzioni, scegli Contattaci, inserisci le informazioni richieste e scegli Invia.

Disinstalla la soluzione

Per disinstallare la soluzione, utilizza la Console di gestione AWS o l'AWS Command Line Interface (AWS CLI). Innanzitutto, interrompi tutte le attività in esecuzione dal cluster Amazon ECS. In caso contrario, l'eliminazione dello stack potrebbe fallire.

Utilizzando la Console di gestione AWS

1. Accedi alla CloudFormation console AWS.
2. Seleziona lo stack con il nome fornito durante la distribuzione.
3. Scegli Elimina stack.

Utilizzo dell'interfaccia a riga di comando AWS

Determina se la CLI AWS è disponibile nel tuo ambiente. Per istruzioni di installazione, consulta What Is the AWS Command Line Interface nella AWS CLI User Guide.

Dopo aver verificato che la CLI di AWS è disponibile, esegui il seguente comando:

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

Guida per sviluppatori

Questa sezione fornisce il codice sorgente della soluzione e personalizzazioni aggiuntive.

Codice sorgente

Visita il GitHub repository Workload Discovery on AWS per scaricare i modelli e gli script per questa soluzione e condividere le tue personalizzazioni con altri.

Individuazione delle risorse di distribuzione

Segui questi passaggi per individuare le risorse distribuite nel tuo account.

1. Accedi alla CloudFormation console AWS.
2. Seleziona la regione in cui hai distribuito la soluzione.

   A seconda dell'utilizzo di questo account, può contenere più stack per carichi di lavoro diversi. Ci sarà uno stack principale con il nome fornito durante la distribuzione e più stack annidati al di sotto di esso.
3. Seleziona ogni stack per accedere alle risorse distribuite utilizzando quel modello.
4. Seleziona la scheda Risorse e scegli il link Physical ID per la risorsa pertinente per visualizzare la risorsa nella rispettiva console di servizio.

   Se conosci l'ID logico di una risorsa, puoi anche effettuare la ricerca utilizzando la barra di ricerca sopra la tabella.

Risorse supportate

La soluzione supporta tutti i tipi di risorse supportati da AWS Config, elencati qui. La tabella seguente contiene le risorse supportate che Workload Discovery on AWS rileva e che non sono supportate da AWS Config. I dettagli sono forniti nell'elenco della documentazione AWS corrispondente.

Tipo di risorsa	Origine	Descrizione
AWS::APIGateway::Authorizer	SDK	GetAuthorizers

Tipo di risorsa	Origine	Descrizione
AWS::ApiGateway::Resource	SDK	Ottieni risorse
AWS::ApiGateway::Method	SDK	Metodo Get
AWS::Cognito::UserPool	SDK	describeUserPool
AWS::ECS::Task	SDK	descrizione-task
AWS::EKS::Nodegroup	SDK	Descrivi il gruppo di nodi
AWS::DynamoDB::Stream	SDK	Descrivi Stream
AWS: :IAM:: Politica AWSManaged	SDK	getAccountAuthorizationDettagli
AWS::ElasticLoadBalancingV2::TargetGroup	SDK	describeTargetGroups
AWS::EC2::Spot	SDK	describeSpotInstanceRichieste
AWS::EC2::SpotFleet	SDK	describeSpotFleetRichieste

Modalità di individuazione degli account AWS Organizations

Quando Workload Discovery on AWS viene distribuito in un'organizzazione AWS, la scoperta degli account non viene più gestita tramite l'interfaccia utente Web della soluzione. In questo caso, non è necessario gestire la distribuzione di CloudFormation modelli per scoprire gli account.

La soluzione utilizza invece un aggregatore AWS Config a livello di organizzazione AWS per scoprire le risorse in tutti gli account dell'organizzazione che hanno AWS Config abilitato.

Per i tipi di risorse che non sono supportati da AWS Config, la soluzione distribuisce automaticamente un ruolo IAM in ogni account dell'organizzazione utilizzando AWS. CloudFormation StackSets Questo ruolo consente al processo di scoperta di effettuare chiamate SDK in tutti gli account dell'organizzazione per scoprire queste risorse supplementari.

Questo StackSet è configurato per distribuire automaticamente il ruolo in tutti i nuovi account aggiunti all'organizzazione ed eliminare il ruolo da tutti gli account rimossi dall'organizzazione.

> **Note**
>
> Non è possibile distribuire un' StackSet istanza dello stack sull'account di gestione. Se desideri che Workload Discovery scopra questo account, devi distribuire il modello di risorse globali utilizzando il metodo di CloudFormation distribuzione AWS standard descritto nella sezione Deploy the stack to provisioning the Global resources using. CloudFormation

Azioni relative ai ruoli di replica di Amazon S3

Il ruolo IAM utilizzato per eseguire la replica deve avere le seguenti azioni:

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

Per verificare che il ruolo abbia le azioni del ruolo di replica:

1. Copia il nome del ruolo nella procedura guidata di replica S3.

2. Accedi alla console IAM con l'account in cui stai configurando la replica.
3. Incolla il nome del ruolo nella casella Cerca in IAM.
4. Seleziona l'elemento principale dall'elenco. Questo è il ruolo IAM che verrà utilizzato.
5. In Politiche di autorizzazione, espandi la politica gestita.
6. Assicurati che la policy contenga le azioni descritte nella tabella precedente.

Policy del bucket S3

Di seguito è riportato un esempio di policy sui bucket S3 che consentirà CURs il caricamento nel bucket insieme alle autorizzazioni per consentire agli account esterni di replicare oggetti al suo interno. È necessario aggiungere il ruolo IAM di ogni account AWS esterno a questa policy per concedere le autorizzazioni per la replica.

```
   {
      "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

Come dettagliato nei prerequisiti, se si implementa la soluzione su un VPC esistente, i seguenti servizi devono essere accessibili dalle sottoreti private.

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 Servizio

- DescribeDomains
- ListDomainNames

Organizations

- ListAccounts
- ListAccountsForParent
- ListOrganizationalUnitsForParent
- ListRoots

Amazon Simple Notification Service

- ListSubscriptions

Servizio Amazon Security Token

- AssumeRole

Riferimento

Questa sezione include informazioni su una funzionalità opzionale per la raccolta di metriche uniche per questa soluzione e un elenco di costruttori che hanno contribuito a questa soluzione.

Raccolta di dati in forma anonima

Questa soluzione include un'opzione per inviare metriche operative anonime ad AWS. Utilizziamo questi dati per comprendere meglio come i clienti utilizzano questa soluzione e i servizi e i prodotti correlati. Una volta attivata, le seguenti informazioni vengono raccolte e inviate ad AWS:

- ID della soluzione: l'identificatore della soluzione AWS
- ID univoco (UUID): identificatore univoco generato casualmente per ogni implementazione
- Timestamp: timestamp di raccolta dati
- Funzione di costo abilitata: informazioni sul fatto che l'utente stia utilizzando la funzione di costo
- Numero di account: numero di account integrati dall'utente durante la distribuzione
- Numero di diagrammi: numero di diagrammi creati in ogni distribuzione
- Numero di risorse: numero di risorse scoperte in tutti gli account registrati

AWS possiede i dati raccolti attraverso questo sondaggio. La raccolta dei dati è soggetta all'Informativa sulla privacy. Per disattivare questa funzionalità, completa i seguenti passaggi prima di avviare il CloudFormation modello AWS.

1. Scarica il CloudFormation modello AWS sul tuo disco rigido locale.
2. Apri il CloudFormation modello AWS con un editor di testo.
3. Modifica la sezione di mappatura dei CloudFormation modelli AWS da:

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

to:

```
Mappings:
```

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

1. Accedi alla CloudFormation console AWS.
2. Seleziona Crea stack.
3. Nella pagina Crea stack, sezione Specificare il modello, seleziona Carica un file modello.
4. In Carica un file modello, scegli Scegli file e seleziona il modello modificato dall'unità locale.
5. Scegli Avanti e segui i passaggi indicati in Avvia lo stack.

Collaboratori

- Mohsan Jaffery
- Matteo Ball
- Stefano Vozza
- Connor Kirkpatrick
- Chris Deigan
- Nicholas Lee
- Tim Mekari

Revisioni

Data di pubblicazione: settembre 2020. Per gli aggiornamenti, fare riferimento al file ChangeLog.md nel repository. GitHub

Fate riferimento al file ChangeLog.md nel repository. GitHub

Note

I clienti sono responsabili della propria valutazione indipendente delle informazioni contenute nel presente documento. Questo documento: (a) è solo a scopo informativo, (b) rappresenta le attuali offerte e pratiche di prodotti AWS, che sono soggette a modifiche senza preavviso, e (c) non crea alcun impegno o garanzia da parte di AWS e delle sue affiliate, fornitori o licenzianti. I prodotti o i servizi AWS sono forniti «così come sono» senza garanzie, dichiarazioni o condizioni di alcun tipo, esplicite o implicite. Le responsabilità di AWS nei confronti dei propri clienti sono definite dai contratti AWS e il presente documento non costituisce parte né modifica qualsivoglia contratto tra AWS e i suoi clienti.

Le traduzioni sono generate tramite traduzione automatica. In caso di conflitto tra il contenuto di una traduzione e la versione originale in Inglese, quest'ultima prevarrà.