aws

Guida per l'utente

Amazon DataZone

Amazon DataZone: Guida per l'utente

Table of Contents

Che cos'è Amazon DataZone?

Amazon DataZone è un servizio di gestione dei dati che semplifica e velocizza la catalogazione, la scoperta, la condivisione e la gestione dei dati archiviati su AWS fonti locali e di terze parti. Con Amazon DataZone, gli amministratori che supervisionano gli asset di dati dell'organizzazione possono gestire e governare l'accesso ai dati utilizzando controlli granulari. Questi controlli aiutano a garantire l'accesso con il giusto livello di privilegi e contesto. Amazon DataZone consente a ingegneri, data scientist, product manager, analisti e utenti aziendali di condividere e accedere ai dati all'interno dell'organizzazione in modo che possano scoprirli, utilizzarli e collaborare per ricavare informazioni basate sui dati.

Amazon ti DataZone aiuta a fornire dati direttamente agli utenti finali e semplifica la tua architettura integrando servizi di gestione dei dati, tra cui Amazon Redshift, Amazon Athena, Amazon, QuickSight Glue, Lake AWS Formation AWS , fonti locali, fonti di terze parti e altro ancora.

Argomenti

Cosa posso fare con Amazon DataZone?

Con Amazon DataZone, puoi fare quanto segue:

- Gestisci l'accesso ai dati oltre i confini dell'organizzazione. Con Amazon DataZone, puoi contribuire a garantire che l'utente giusto acceda ai dati giusti per lo scopo giusto, in conformità con le norme di sicurezza della tua organizzazione, senza fare affidamento su credenziali individuali. Puoi anche fornire trasparenza sull'utilizzo degli asset di dati e approvare gli abbonamenti ai dati con un flusso di lavoro regolato. Puoi anche monitorare le risorse di dati tra i progetti tramite funzionalità di controllo dell'utilizzo.
- Connect i data worker tramite dati e strumenti condivisi per ottenere informazioni aziendali approfondite. Con Amazon DataZone, puoi aumentare l'efficienza dei team aziendali collaborando senza problemi tra i team e fornendo accesso self-service a dati e strumenti di analisi. Puoi utilizzare termini commerciali per cercare, condividere e accedere ai dati catalogati archiviati in locale o con AWS fornitori di terze parti. E puoi saperne di più sui dati che desideri utilizzare utilizzando i DataZone glossari aziendali di Amazon.

- Automatizza la scoperta e la catalogazione dei dati con l'apprendimento automatico. Con Amazon DataZone, puoi ridurre il tempo impiegato per l'inserimento manuale degli attributi dei dati nel catalogo dei dati aziendali. Una maggiore quantità di dati nel catalogo dati migliora anche l'esperienza di ricerca.

In che modo Amazon DataZone supporta e si integra con altri AWS servizi?

Amazon DataZone supporta tre tipi di integrazioni con altri AWS servizi:

- Fonti di dati dei produttori: puoi pubblicare asset di dati nel DataZone catalogo Amazon dai dati archiviati nelle tabelle e nelle AWS viste di Glue Data Catalog e Amazon Redshift. Puoi anche pubblicare manualmente oggetti da Amazon Simple Storage Service (S3) nel catalogo Amazon. DataZone
- Strumenti per i consumatori: puoi utilizzare gli editor di query di Amazon Athena o Amazon Redshift per accedere e analizzare le tue risorse di dati.
- Controllo e adempimento degli accessi: Amazon DataZone supporta la concessione dell'accesso alle tabelle AWS Glue gestite da AWS Lake Formation e alle tabelle e viste di Amazon Redshift. Per tutte le altre risorse di dati, Amazon DataZone pubblica eventi standard relativi alle tue azioni (ad esempio, l'approvazione data a una richiesta di abbonamento) su Amazon EventBridge. Puoi utilizzare questi eventi standard per l'integrazione con altri AWS servizi o soluzioni di terze parti per integrazioni personalizzate.

Come posso accedere ad Amazon DataZone?

Puoi accedere ad Amazon DataZone in uno dei seguenti modi:

- DataZone Console Amazon

  Puoi utilizzare la console di DataZone gestione Amazon per accedere e configurare i tuoi DataZone domini, blueprint e utenti Amazon. Per ulteriori informazioni, consulta https://console.aws.amazon.com/datazone. La console DataZone di gestione Amazon viene utilizzata anche per creare il portale DataZone dati Amazon.
- Portale DataZone dati Amazon

Il portale DataZone dati Amazon è un'applicazione Web basata su browser in cui è possibile catalogare, scoprire, gestire, condividere e analizzare i dati in modalità self-service. Il portale dati può autenticarti con le credenziali del tuo provider di identità tramite AWS IAM Identity Center (successore di AWS SSO) o con le tue credenziali IAM. Puoi ottenere l'URL del portale dati accedendo alla DataZone console Amazon all'indirizzo https://console.aws.amazon.com/datazone.

- API Amazon DataZone HTTPS

  Puoi accedere ad Amazon in modo DataZone programmatico utilizzando l'API Amazon DataZone HTTPS, che ti consente di inviare richieste HTTPS direttamente al servizio. Per ulteriori informazioni, consulta Amazon DataZone API Reference.

DataZone Terminologia e concetti di Amazon

Quando inizi a usare Amazon DataZone, è importante comprenderne i concetti chiave, la terminologia e i componenti.

Argomenti

DataZone Componenti Amazon

Amazon DataZone include i seguenti quattro componenti principali:

- Catalogo dei dati aziendali: puoi utilizzare questo componente per catalogare i dati di tutta l'organizzazione in base al contesto aziendale e consentire così a tutti i membri dell'organizzazione di trovare e comprendere rapidamente i dati.
- Flussi di lavoro di pubblicazione e sottoscrizione: puoi utilizzare questi flussi di lavoro automatizzati per proteggere i dati tra produttori e consumatori in modalità self-service e per garantire che tutti i membri dell'organizzazione abbiano accesso ai dati giusti per lo scopo giusto.
- Progetti e ambienti
  - In Amazon, DataZone i progetti sono raggruppamenti di persone, risorse (dati) e strumenti basati su casi d'uso aziendale utilizzati per semplificare l'accesso alle analisi. AWS I progetti forniscono aree in cui i membri del progetto possono collaborare, scambiare dati e condividere risorse. Per impostazione predefinita, i progetti sono configurati in modo che solo coloro che vengono aggiunti esplicitamente al progetto possano accedere ai dati e agli strumenti di analisi al loro interno. I progetti gestiscono la proprietà delle risorse prodotte in conformità alle politiche di progetto a cui possono accedere i consumatori di dati.

  - All'interno dei DataZone progetti Amazon, gli ambienti sono raccolte di zero o più risorse configurate (ad esempio, un bucket Amazon S3, un AWS Glue database o un gruppo di lavoro Amazon Athena) su cui può operare un determinato set di principi IAM (ad esempio, utenti con autorizzazioni di contributore).
- Portale dati (esterno alla console di AWS gestione): si tratta di un'applicazione Web basata su browser in cui diversi utenti possono catalogare, scoprire, governare, condividere e analizzare i dati in modalità self-service. Il portale dati autentica gli utenti con credenziali IAM o credenziali esistenti fornite dal provider di identità tramite. AWS IAM Identity Center

Cosa sono i DataZone domini Amazon?

Puoi utilizzare i DataZone domini Amazon per organizzare le tue risorse, gli utenti e i loro progetti. Associando AWS account aggiuntivi ai tuoi DataZone domini Amazon, puoi riunire le tue fonti di dati. Puoi quindi pubblicare le risorse provenienti da queste fonti di dati nel catalogo del tuo dominio, con moduli di metadati e glossari che migliorano la completezza e la qualità dei metadati. Puoi anche cercare e sfogliare queste risorse per vedere quali dati sono pubblicati nel dominio. Inoltre, puoi partecipare a progetti per collaborare con altri utenti, sottoscrivere risorse e utilizzare ambienti di progetto per accedere a strumenti di analisi, tra cui Amazon Athena e Amazon Redshift. DataZone I domini Amazon ti offrono la flessibilità necessaria per riflettere le esigenze di dati e analisi della tua struttura organizzativa, sia che si tratti di creare un singolo DataZone dominio Amazon per la tua azienda o più DataZone domini Amazon per diverse unità aziendali.

Cosa sono i DataZone progetti e gli ambienti Amazon?

Amazon DataZone consente ai team e agli utenti di analisi di collaborare ai progetti creando raggruppamenti di team, strumenti e dati basati su casi d'uso.

- In Amazon DataZone, i progetti consentono a un gruppo di utenti di collaborare su vari casi d'uso aziendali che coinvolgono la pubblicazione, la scoperta, la sottoscrizione e l'utilizzo dei dati nel catalogo Amazon DataZone . I membri del progetto utilizzano risorse dal DataZone catalogo Amazon e producono nuove risorse utilizzando uno o più flussi di lavoro analitici. I progetti supportano le seguenti attività all'interno del portale dati:
  - I proprietari del progetto possono aggiungere membri con autorizzazioni di proprietario e collaboratore
  - I membri del progetto possono essere utenti SSO, gruppi SSO e utenti IAM
  - I membri del progetto possono richiedere l'abbonamento alle risorse nel catalogo dati

Le approvazioni degli abbonamenti vengono fornite ai progetti

- In un DataZone progetto Amazon, gli ambienti sono raccolte di zero o più risorse configurate (ad esempio, un Amazon S3, un AWS Glue database o un gruppo di lavoro Amazon Athena), con un determinato set di principi IAM che possono operare su tali risorse. Gli ambienti vengono creati utilizzando profili di ambiente, che sono set di risorse e progetti preconfigurati che forniscono modelli riutilizzabili per la creazione di ambienti. I profili di ambiente definiscono impostazioni come la regione Account AWS o la regione in cui vengono distribuiti gli ambienti.

Cosa sono i DataZone progetti Amazon?

Un blueprint con cui viene creato l'ambiente definisce quali AWS strumenti e servizi (ad esempio Amazon Redshift) i membri del progetto a cui appartiene l'ambiente possono utilizzare mentre lavorano con le risorse nel catalogo Amazon DataZone . AWS Glue

Nella versione corrente di Amazon DataZone, sono supportati i seguenti blueprint predefiniti:

Nome del progetto	Descrizione	Risorse create
Progetto Data Lake	Consente ai membri DataZone del progetto Amazon di lanciare servizi Data Lake per produttori e consumatori all'interno dell'ambiente. In qualità di consumatore, consente ai membri DataZone del progetto Amazon di accedere a una copia «di sola lettura» degli asset gestiti da Lake Formation direttamente in Amazon Athena e in altri motori di query supportati da Lake Formation. In qualità di produttore, consente ai membri DataZone del progetto Amazon di creare	Fornisce agli utenti la possibili tà di creare e interrogare tabelle Lake Formation utilizzando Amazon Athena. Gruppo di lavoro Amazon Athena, AWS Glue database con autorizzazioni Lake Formation «sola lettura», autorizzazioni IAM «sola lettura» e accesso ad Amazon S3 gestito dal progetto. AWS Glue database con autorizzazioni di «creazion e» e «concessione» di Lake Formation, autorizzazioni IAM di «lettura» e «scrittura», AWS Glue ETL (estrazione,

Nome del progetto	Descrizione	Risorse create
	nuove tabelle LakeFormation gestite utilizzando Amazon Athena e di pubblicarle nel catalogo Amazon DataZone.	trasformazione e caricamento) con tag.
Progetto Data Warehouse	In qualità di consumatore, questo modello consente ai membri DataZone del progetto Amazon di connettersi ai propri cluster Amazon Redshift per interrogare archivi dati remoti e creare e archiviare nuovi set di dati. In qualità di produttore, questo modello consente ai membri DataZone del progetto Amazon di connettersi ai propri cluster Amazon Redshift per interrogare archivi di dati remoti, creare nuovi set di dati e pubblicarli nel catalogo Amazon. DataZone	Accesso all'editor di query di Amazon Redshift, accesso in «lettura» alle fonti di dati sottoscritte dal DataZone catalogo Amazon, possibili tà di creare risorse locali nel cluster Amazon Redshift configurato. Accesso all'edito r di query di Amazon Redshift, accesso in «lettura» alle fonti di dati sottoscritte dal DataZone catalogo Amazon, possibilità di creare e pubblicare risorse dal cluster Amazon Redshift configurato.

Nome del progetto	Descrizione	Risorse create
Progetto Amazon Sagemaker	Questo modello aiuta i produttori di dati e i consumatori a passare senza problemi SageMaker ad Amazon per collaborare su progetti di machine learning (ML), rafforzando al contempo la governance dell'accesso ai dati e alle risorse ML. Con la nuova integrazione integrata tra Amazon DataZone e Amazon SageMaker, i consumatori e i produttori di dati possono semplificare la governance del machine learning in tutta la configurazione dell'infrastruttura, collaborare a iniziative aziendali e gestire facilmente dati e risorse ML.	Puoi creare un SageMaker dominio Amazon in grado di cercare, sottoscrivere e pubblicare dati e risorse ML in Amazon DataZone. Inoltre, puoi iscriverti e pubblicare sui database AWS Glue e sulla formazione di laghi come configurato.

Cosa sono i flussi di lavoro di DataZone inventario e pubblicazione di Amazon?

Creazione di risorse di inventario del progetto

Per utilizzare Amazon per DataZone catalogare i tuoi dati, devi prima importare i tuoi dati (asset) come inventario del tuo progetto in Amazon DataZone. La creazione di un inventario per un progetto rende le risorse individuabili solo dai membri di quel progetto. Le risorse dell'inventario del progetto non sono disponibili per tutti gli utenti del dominio in search/browse a meno che non vengano pubblicate in modo esplicito. Nell'attuale versione di Amazon DataZone, puoi aggiungere risorse all'inventario del progetto nei seguenti modi:

- Crea ed esegui fonti di dati tramite il portale dati o utilizzando le DataZone API di Amazon. Nell'attuale versione di Amazon DataZone, puoi creare ed eseguire fonti di dati per AWS Glue e Amazon Redshift. Creando ed eseguendo sorgenti dati AWS Glue o Amazon Redshift, crei risorse nell'inventario di un progetto scelto e ne importi i metadati tecnici dalle tabelle del database di origine o dai data warehouse come inventario in Amazon. DataZone
- Utilizzando le API, puoi creare risorse dai tipi di asset di sistema disponibili (AWS Glue, Amazon Redshift, oggetti Amazon S3) o dai tuoi tipi di asset personalizzati.
  - Crea tipi di asset personalizzati nell'inventario di un progetto utilizzando le DataZone API di Amazon. I tipi di risorse personalizzati possono includere modelli ML, dashboard, tabelle locali, ecc.
  - Crea risorse da questi tipi di risorse personalizzate utilizzando le DataZone API di Amazon.
- Crea manualmente risorse per oggetti S3 utilizzando il portale DataZone dati Amazon.

Gestione delle risorse di inventario del progetto: dopo aver creato un inventario del progetto, i proprietari dei dati possono curare le proprie risorse di inventario con i metadati aziendali richiesti aggiungendo o aggiornando nomi aziendali (asset e schema), descrizioni (asset e schema), readme, termini del glossario (asset e schema) e moduli di metadati. Puoi farlo tramite il portale dati o utilizzando le DataZone API di Amazon. Ogni modifica alla tua risorsa crea una nuova versione dell'inventario.

Pubblicazione delle risorse di inventario del progetto nel DataZone catalogo Amazon

Il passaggio successivo dell'utilizzo di Amazon DataZone per catalogare i dati consiste nel rendere le risorse di inventario del progetto individuabili dagli utenti del dominio. Puoi farlo pubblicando le risorse di inventario nel DataZone catalogo Amazon. Solo la versione più recente della risorsa di inventario può essere pubblicata nel catalogo e solo l'ultima versione pubblicata è attiva nel catalogo Discovery. Se una risorsa di inventario viene aggiornata dopo la sua pubblicazione nel DataZone catalogo Amazon, devi pubblicarla nuovamente in modo esplicito affinché la versione più recente sia presente nel catalogo Discovery. Nell'attuale versione di Amazon DataZone, puoi pubblicare le risorse di inventario dei tuoi progetti nel DataZone catalogo Amazon nei seguenti modi:

- Pubblica manualmente le risorse dell'inventario del progetto nel DataZone catalogo Amazon tramite il portale dati o utilizzando le DataZone API di Amazon.
- Come parte della creazione o della modifica delle fonti di dati, abilita le impostazioni opzionali Publish your AWS Glue sul catalogo o Pubblica le tue risorse Amazon Redshift nel catalogo

da utilizzare durante le esecuzioni pianificate o automatizzate delle origini dati. Quando questa impostazione è abilitata, l'esecuzione di un'origine dati aggiunge risorse all'inventario del progetto e quindi pubblica anche le risorse di inventario nel DataZone catalogo Amazon. Tieni presente che se pubblichi direttamente, le risorse potrebbero non contenere metadati aziendali e saranno rese direttamente individuabili da tutti gli utenti del dominio. Puoi utilizzare questa impostazione sulle tue fonti di dati tramite il portale dati o utilizzando le DataZone API di Amazon.

Cosa sono i flussi di lavoro relativi agli DataZone abbonamenti e agli adempimenti di Amazon?

Una volta pubblicate le tue risorse nel DataZone catalogo Amazon, gli utenti del tuo dominio possono scoprirle, richiederle e accedervi e continuare a utilizzare Amazon DataZone per governare, condividere e analizzare queste risorse.

Gli utenti richiedono l'accesso a una risorsa sottoscrivendo tale risorsa per conto di un progetto. Una volta creata una richiesta di abbonamento, i proprietari della risorsa ricevono una notifica e possono esaminarla e decidere se approvarla o rifiutarla. Se la richiesta di sottoscrizione viene approvata dal proprietario dei dati, al progetto sottoscrittore viene concesso l'accesso a tale risorsa.

Una volta approvata una richiesta di abbonamento, Amazon DataZone avvia un flusso di lavoro di evasione dell'abbonamento che aggiunge automaticamente la risorsa a tutti gli ambienti applicabili all'interno del progetto creando le sovvenzioni necessarie in AWS Lake Formation o Amazon Redshift. Ciò consente ai membri del progetto abbonati di interrogare la risorsa utilizzando uno degli strumenti di query (Amazon Athena o Amazon Redshift query editor) nei propri ambienti.

Amazon DataZone può attivare questa logica di evasione automatica solo per le risorse gestite (incluse le tabelle AWS Glue e le tabelle e viste di Amazon Redshift). Per tutti gli altri tipi di risorse (risorse non gestite), Amazon non DataZone può attivare automaticamente l'adempimento, ma pubblica invece un evento in Amazon Eventbridge con tutti i dettagli necessari nel payload dell'evento in modo che tu possa creare le sovvenzioni necessarie al di fuori di Amazon. DataZone Amazon fornisce DataZone anche l'`updateSubscriptionStatus`API che consente di aggiornare lo stato dell'abbonamento una volta completato al di fuori di Amazon, in DataZone modo che Amazon DataZone possa notificare ai membri del progetto che possono iniziare a utilizzare la risorsa.

I personaggi utente di Amazon DataZone

Di seguito sono riportati i principali DataZone utenti di Amazon:

- Amministratori di dominio proprietari della configurazione di Amazon DataZone come piattaforma di analisi per la propria organizzazione.

  Nel contesto di Amazon DataZone, gli amministratori di dominio installano Amazon DataZone negli AWS account, creano DataZone domini Amazon e configurano associazioni di AWS account e associazioni di provider di identità con i domini Amazon DataZone . Gli amministratori di dominio utilizzano anche altre console di AWS servizio come AWS Organization e Service Catalog per configurare Amazon. DataZone
- Utenti di dati che sono i principali utenti di Amazon DataZone (editori di asset e abbonati) per le loro attività di analisi e apprendimento automatico.

  Gli utenti dei dati includono addetti all'analisi dei dati, data scientist e utenti di sistema che producono e consumano risorse di dati. Nel contesto di Amazon DataZone, gli utenti di dati creano e partecipano a progetti e ambienti, sottoscrivono e utilizzano asset di dati con strumenti di analisi o machine learning preconfigurati e pubblicano gli asset di dati di output nel catalogo di DataZone domini Amazon per condividerli con altri.
- Sviluppatori di sistema che creano modelli di infrastruttura personalizzati e integrano Amazon DataZone con cataloghi o sistemi di produzione interni.

  Nel contesto di Amazon DataZone, gli sviluppatori di sistemi creano progetti di ambiente (modelli di infrastruttura) o pipeline CI/CD Infrastructure-As-Code come provider di ambiente, pipeline di dati per promuovere le risorse di dati tra gli ambienti, adattatori di sincronizzazione dei cataloghi e di evasione delle sovvenzioni per l'integrazione con i cataloghi interni o integrazioni tra le API di Amazon e le interfacce utente interne o i sistemi di produzione, se necessario. DataZone
- Responsabili della governance dei dati che possiedono le definizioni e i rischi della sicurezza organizzativa, della privacy e di altre politiche di conformità e che si assicurano che l'utilizzo di Amazon DataZone nelle loro organizzazioni sia conforme a tali definizioni.

DataZone Terminologia Amazon

Domain

Un DataZone dominio Amazon è l'entità organizzativa per connettere le tue risorse, gli utenti e i loro progetti. Con DataZone i domini Amazon, hai la flessibilità necessaria per riflettere le esigenze di dati e analisi della tua struttura organizzativa, che si tratti di creare un singolo DataZone dominio Amazon per la tua azienda o più zone dati; domini per diverse unità aziendali o team.

Account associato

L'associazione AWS dei tuoi account ai DataZone domini Amazon ti consente di pubblicare i dati di questi AWS account nel DataZone catalogo Amazon e di creare DataZone progetti Amazon per utilizzare i tuoi dati su più AWS account. Le richieste di associazione di account possono essere avviate solo in AWS account che possiedono un DataZone dominio Amazon. Le richieste di associazione di account possono essere accettate solo dagli utenti amministrativi degli AWS account invitati. Una volta che un AWS account è associato a un DataZone dominio Amazon, puoi registrare le tue fonti di dati come AWS Glue catalog e Amazon Redshift in questo account su questo dominio. L'associazione consente inoltre a un AWS account di creare DataZone progetti e ambienti Amazon.

An Account AWS può essere associato a uno o più DataZone domini Amazon.

Origine dati

In Amazon DataZone, puoi utilizzare le fonti di dati per importare i metadati tecnici degli asset (dati) dai database di origine o dai data warehouse in Amazon. DataZone Nell'attuale versione di Amazon DataZone, puoi creare ed eseguire fonti di dati per AWS Glue e Amazon Redshift. Creando un'origine dati, stabilisci una connessione tra Amazon DataZone e la fonte (AWS Glue Data Catalog o Amazon Redshift Warehouse) che ti consente di leggere i metadati tecnici, inclusi nomi di tabelle, nomi di colonne e tipi di dati. Creando un'origine dati, dai anche il via all'esecuzione iniziale dell'origine dati che crea nuove risorse o aggiorna quelle esistenti in Amazon DataZone. Durante la creazione di un'origine dati o dopo che l'origine dati è stata creata correttamente, hai anche la possibilità di specificare una pianificazione per l'esecuzione dell'origine dati.

Esecuzione dell'origine dati

In Amazon DataZone, l'esecuzione di un'origine dati è un'attività che Amazon DataZone esegue per creare risorse negli inventari dei progetti e, facoltativamente, anche per pubblicare risorse di inventario del progetto nel catalogo Amazon DataZone . Le esecuzioni delle sorgenti dati possono essere automatizzate (avviate quando una fonte di dati viene inizialmente creata) o pianificata o manuale. I criteri di selezione dei dati consentono di ottimizzare i set di dati esistenti e futuri da inserire negli inventari dei progetti o nel catalogo DataZone Amazon e la frequenza degli aggiornamenti dei metadati di tali risorse di inventario o catalogo.

Obiettivo dell'abbonamento

In Amazon DataZone, gli obiettivi di abbonamento ti consentono di accedere ai dati a cui ti sei iscritto nei tuoi progetti. Un obiettivo di sottoscrizione specifica la posizione (ad esempio, un

database o uno schema) e le autorizzazioni richieste (ad esempio, un ruolo IAM) che Amazon DataZone può utilizzare per stabilire una connessione con i dati di origine e per creare le concessioni necessarie in modo che i membri del DataZone progetto Amazon possano iniziare a interrogare i dati a cui si sono abbonati.

Richiesta di abbonamento

In Amazon DataZone, una richiesta di abbonamento è un processo che un DataZone progetto Amazon deve seguire per ottenere l'accesso a una risorsa specifica. Le richieste di abbonamento possono essere approvate, rifiutate, revocate o concesse.

Asset

In Amazon DataZone, una risorsa è un'entità che presenta un singolo oggetto di dati fisico (ad esempio, una tabella, un dashboard, un file) o un oggetto di dati virtuale (ad esempio, una vista).

Asset type (Tipo asset)

I tipi di asset definiscono il modo in cui gli asset vengono rappresentati nel DataZone catalogo Amazon. Un tipo di risorsa definisce lo schema per un tipo specifico di risorsa. Quando le risorse vengono create, vengono convalidate in base allo schema definito dal tipo di risorsa (per impostazione predefinita, la versione più recente). Quando si verifica un aggiornamento degli asset, Amazon DataZone crea una nuova versione dell'asset e consente DataZone agli utenti Amazon di operare su tutte le versioni degli asset.

Glossario aziendale

In Amazon DataZone, un glossario aziendale è una raccolta di termini commerciali che possono essere associati agli asset. Un glossario aziendale aiuta a garantire che gli stessi termini e le stesse definizioni vengano utilizzati in un'organizzazione in tutte le sue varie attività di analisi dei dati.

I termini di un glossario aziendale possono essere aggiunti alle risorse e alle colonne per classificare o migliorare l'identificazione di tali attributi durante la ricerca. Il glossario può essere selezionato come tipo di valore per un campo in un modulo di metadati associato a una risorsa. Quando un termine particolare viene selezionato come valore per il campo del modulo di metadati di una risorsa, gli utenti possono cercare il termine del glossario aziendale e trovare le risorse associate.

Tipo di modulo per metadati

Un tipo di modulo di metadati è un modello che definisce i metadati che vengono raccolti e salvati quando le risorse vengono create come inventario o pubblicate in un dominio Amazon

DataZone . I tipi di modulo di metadati possono essere associati a una risorsa di dati. I tipi di modulo di metadati aiutano gli amministratori di dominio a definire i moduli di metadati necessari per quel dominio, ad esempio informazioni sulla conformità, informazioni sulle normative o classificazioni. Consente agli amministratori di dominio di personalizzare metadati aggiuntivi per le proprie risorse. Amazon DataZone dispone di tipi di moduli di metadati di sistema come asset-common-details-form -type, column-business-metadata-form -type,, glue-table-form-type,, glue-view-form-type redshift-table-form-type, s3- redshift-view-form-typeobject-collection-form-type, e. subscription-terms-form-type suggestion-form-type

Modulo per i metadati

In Amazon DataZone, i moduli di metadati definiscono i metadati che vengono raccolti e salvati quando le risorse vengono create come inventario o pubblicate in un dominio Amazon DataZone . Le definizioni dei moduli di metadati vengono create nel dominio del catalogo da un amministratore di dominio. La definizione di un modulo di metadati è composta da una o più definizioni di campo, con supporto per i tipi di dati booleani, date, decimali, numeri interi, stringhe e valori dei campi del glossario aziendale.

Un amministratore di dominio applica un modulo di metadati alle risorse del proprio dominio aggiungendo il modulo di metadati al proprio dominio. Gli editori di risorse forniscono quindi tutti i valori di campo facoltativi e obbligatori nel modulo di metadati.

Progetto

In Amazon DataZone, i progetti consentono a un gruppo di utenti di collaborare su vari casi d'uso aziendali che prevedono la creazione di risorse negli inventari dei progetti e quindi la loro individuazione da parte di tutti i membri del progetto, quindi la pubblicazione, la scoperta, la sottoscrizione e il consumo di risorse nel catalogo Amazon. DataZone I membri del progetto utilizzano risorse dal DataZone catalogo Amazon e producono nuove risorse utilizzando uno o più flussi di lavoro analitici. I membri del progetto possono essere proprietari o collaboratori. I proprietari dei progetti possono aggiungere o rimuovere altri utenti come proprietari o collaboratori e possono modificare o eliminare i progetti. Altre restrizioni relative ai contributori possono essere definite mediante politiche. Quando un utente crea un progetto, diventa il primo proprietario di quel progetto.

Ambiente

Un ambiente è una raccolta di risorse configurate (ad esempio, un bucket Amazon S3, un AWS Glue database o un gruppo di lavoro Amazon Athena), con un determinato set di principali IAM (con autorizzazioni di collaboratore assegnate) che possono operare su tali risorse. Ogni

ambiente può inoltre avere utenti principali autorizzati ad accedere alle risorse e ai dati tramite sottoscrizione e adempimento. Gli ambienti sono progettati per archiviare collegamenti utilizzabili verso AWS servizi, IDE e console esterni. I membri del progetto possono accedere a servizi come la console Amazon Athena e altro ancora tramite deep link configurati all'interno di un ambiente. Gli utenti SSO e gli utenti IAM del progetto possono essere ulteriormente ridotti per utilizzare/accedere ad ambienti specifici.

Profilo ambientale

In Amazon DataZone, un profilo di ambiente è un modello che puoi utilizzare per creare ambienti. I profili di ambiente vengono creati utilizzando i blueprint.

Con i profili di ambiente, gli amministratori di dominio possono creare blueprint con parametri preconfigurati, quindi i data worker possono creare rapidamente un numero qualsiasi di nuovi ambienti selezionando i profili di ambiente esistenti e specificando i nomi per i nuovi ambienti. Ciò consente ai data worker di gestire in modo efficiente i propri progetti e ambienti, garantendo al contempo che soddisfino le politiche di governance dei dati applicate dagli amministratori di dominio.

Piano

Un blueprint con cui viene creato l'ambiente definisce quali AWS strumenti e servizi (ad esempio Amazon Redshift) i membri del progetto a cui appartiene l'ambiente possono utilizzare mentre lavorano con le risorse nel catalogo Amazon DataZone . AWS Glue

Nella versione corrente di Amazon sono supportati DataZone i seguenti blueprint predefiniti:

- Blueprint Data Lake
- Progetto di data warehouse
- Progetto Amazon Sagemaker

Profilo utente

Un profilo utente rappresenta DataZone gli utenti Amazon. Amazon DataZone supporta sia i ruoli IAM che le identità SSO per interagire con la Console di DataZone gestione Amazon e il portale dati per scopi diversi. Gli amministratori di dominio utilizzano i ruoli IAM per eseguire il lavoro amministrativo iniziale relativo al dominio nella Console di DataZone gestione Amazon, tra cui la creazione di nuovi DataZone domini Amazon, la configurazione dei tipi di modulo di metadati e l'implementazione di politiche. I data worker utilizzano le loro identità aziendali SSO tramite Identity Center per accedere ad Amazon DataZone Data Portal e accedere ai progetti a cui sono iscritti.

Profilo del gruppo

I profili di gruppo rappresentano gruppi di DataZone utenti Amazon. I gruppi possono essere creati manualmente o mappati su gruppi di clienti aziendali di Active Directory. In Amazon DataZone, i gruppi hanno due scopi. Innanzitutto, un gruppo può associarsi a un team di utenti nell'organigramma e quindi ridurre il lavoro amministrativo del proprietario di un DataZone progetto Amazon quando ci sono nuovi dipendenti che entrano o escono da un team. In secondo luogo, gli amministratori aziendali utilizzano i gruppi di Active Directory per gestire e aggiornare gli stati degli utenti e quindi gli amministratori di DataZone dominio Amazon possono utilizzare queste appartenenze ai gruppi per implementare le politiche di dominio Amazon. DataZone

Amministratore di dominio

In Amazon DataZone, un principale IAM che crea un DataZone dominio Amazon è l'amministratore di dominio predefinito di quel dominio. Gli amministratori di dominio in Amazon DataZone eseguono funzionalità chiave per il dominio, tra cui la creazione di domini, l'assegnazione di altri amministratori di dominio, l'aggiunta di fonti di dati e obiettivi di abbonamento, la creazione di progetti e ambienti e l'assegnazione dei proprietari dei progetti.

Editore

In Amazon DataZone, gli editori pubblicano le risorse nel DataZone catalogo Amazon e possono modificare i metadati delle risorse che pubblicano. Se viene concessa questa autorità, gli editori possono approvare o rifiutare le richieste di abbonamento alle risorse che hanno pubblicato nel catalogo Amazon. DataZone

Sottoscrittore

In Amazon DataZone, un abbonato è un DataZone progetto Amazon che desidera trovare, accedere e utilizzare risorse nel catalogo Amazon DataZone .

Account AWS owner

In Amazon DataZone, Account AWS i proprietari creano ruoli, politiche e autorizzazioni Account AWS che consentono di associarli Account AWS ai DataZone domini Amazon.

Cosa c'è di nuovo in Amazon DataZone?

Questa sezione descrive le nuove funzionalità e i miglioramenti di Amazon in DataZone base alla data di rilascio.

Argomenti

2024

Amazon DataZone lancia l'integrazione con Amazon SageMaker

Rilasciato il 05/06/2024

Amazon DataZone lancia l'integrazione con Amazon SageMaker per aiutare i produttori di dati e i consumatori a passare senza problemi SageMaker ad Amazon per collaborare su progetti di machine learning (ML), rafforzando al contempo la governance dell'accesso ai dati e alle risorse ML. Con la nuova integrazione integrata tra Amazon DataZone e Amazon SageMaker, i consumatori e i produttori di dati possono semplificare la governance del machine learning in tutta la configurazione dell'infrastruttura, collaborare a iniziative aziendali e gestire facilmente dati e risorse ML. Per ulteriori informazioni, consulta Lavorare con i blueprint DataZone integrati di Amazon e Utilizzo degli account associati per pubblicare e utilizzare dati.

Amazon DataZone lancia l'integrazione con la modalità di accesso ibrida AWS Lake Formation

Rilasciato il 04/03/2024

Amazon DataZone ha introdotto un'integrazione con la modalità di accesso ibrida AWS Lake Formation. Questa integrazione ti consente di pubblicare e condividere facilmente le tue tabelle AWS Glue tramite Amazon DataZone, senza la necessità di registrarle prima in AWS Lake Formation. Per iniziare, gli amministratori abilitano l'impostazione di registrazione della posizione dei dati nel `DefaultDataLake` blueprint nella console Amazon DataZone . Quindi, quando un consumatore di dati si iscrive a una tabella AWS Glue gestita tramite autorizzazioni IAM, Amazon registra DataZone prima le posizioni Amazon S3 di questa tabella in modalità ibrida, quindi concede l'accesso al consumatore di dati gestendo le autorizzazioni sulla tabella tramite Lake Formation. AWS Ciò

garantisce che le autorizzazioni IAM sulla tabella continuino a esistere con le autorizzazioni AWS Lake Formation appena concesse, senza interrompere i flussi di lavoro esistenti. Per ulteriori informazioni, consulta DataZone Integrazione di Amazon con la modalità ibrida AWS Lake Formation .

Amazon DataZone lancia l'integrazione con AWS Glue Data Quality

Rilasciato il 04/03/2024

Amazon DataZone lancia l'integrazione con AWS Glue Data Quality e offre API per integrare metriche di qualità dei dati da soluzioni di qualità dei dati di terze parti. La nuova integrazione consente di pubblicare automaticamente i punteggi AWS Glue Data Quality nel catalogo di dati DataZone aziendali di Amazon. DataZone Le API di Amazon possono essere utilizzate per acquisire metriche di qualità da fonti di terze parti. Una volta pubblicati, i consumatori di dati possono facilmente cercare asset di dati, visualizzare metriche di qualità granulari e identificare controlli e regole non riusciti, rafforzando così le decisioni aziendali. Per ulteriori informazioni, consulta Qualità dei dati in Amazon DataZone.

Versione di disponibilità generale dei consigli di intelligenza artificiale per le descrizioni in Amazon DataZone

Rilasciato il 27/03/2024

Amazon DataZone ha annunciato la versione per la disponibilità generale della nuova funzionalità generativa basata sull'intelligenza artificiale per migliorare il rilevamento, la comprensione e l'utilizzo dei dati arricchendo il catalogo dei dati aziendali. Con un solo clic, i produttori di dati possono generare descrizioni e contesto completi dei dati aziendali, evidenziare le colonne di impatto e includere consigli sui casi d'uso analitici. Il lancio aggiunge il supporto per le API che i produttori di dati possono utilizzare per generare descrizioni per le risorse in modo programmatico. Per ulteriori informazioni, consulta Utilizzo dell'apprendimento automatico e dell'intelligenza artificiale generativa.

Amazon DataZone lancia miglioramenti all'integrazione con Amazon Redshift

Rilasciato il 21/03/2024

Amazon DataZone ha introdotto diversi miglioramenti all'integrazione con Amazon Redshift, semplificando il processo di pubblicazione e sottoscrizione alle tabelle e alle visualizzazioni di Amazon Redshift. Questi aggiornamenti semplificano l'esperienza sia per i produttori di dati che

per i consumatori, consentendo loro di creare rapidamente ambienti di data warehouse utilizzando credenziali e parametri di connessione preconfigurati forniti dai loro amministratori Amazon. DataZone Inoltre, questi miglioramenti garantiscono agli amministratori un maggiore controllo su chi può utilizzare le risorse all'interno dei propri AWS account e dei cluster Amazon Redshift e per quale scopo.

- Configurazione del blueprint: una volta abilitato il `DefaultDataWarehouseBlueprint` blueprint, puoi controllare quali progetti possono utilizzare il `DefaultDataWarehouseBlueprint` blueprint nel tuo account per creare profili ambientali assegnando la gestione dei progetti al blueprint abilitato. È inoltre possibile creare set di parametri `DefaultDataWarehouseBlueprint` fornendo parametri come cluster, database e un Secret. AWS Puoi anche creare AWS Secrets direttamente dalla DataZone console Amazon.
- Profilo ambientale: quando crei un profilo di ambiente, puoi scegliere di fornire i tuoi parametri Amazon Redshift o utilizzare uno dei set di parametri dalla configurazione del blueprint. Se scegli di utilizzare il set di parametri creato nella configurazione del blueprint, il AWS segreto richiede solo il `AmazonDataZoneDomain` tag (il `AmazonDataZoneProject` tag è richiesto solo se scegli di fornire i tuoi set di parametri nel profilo ambientale). Nel profilo dell'ambiente, è possibile specificare un elenco di progetti autorizzati. Solo i progetti autorizzati possono utilizzare questo profilo di ambiente per creare ambienti di data warehouse. È inoltre possibile specificare quali dati i progetti autorizzati possono pubblicare. Attualmente puoi scegliere una delle seguenti opzioni: 1) Pubblica da qualsiasi schema, 2) Pubblica dallo schema di ambiente predefinito, 3) Non consentire la pubblicazione.
- Ambiente: i produttori o i consumatori di dati possono ora selezionare un profilo di ambiente per creare ambienti, senza la necessità di fornire i propri parametri Amazon Redshift, tra cui AWS Secret, cluster, workgroup e database. Questi parametri vengono trasferiti nell'ambiente dal profilo ambientale. Oltre alla creazione dell'ambiente, Amazon DataZone ora crea anche uno schema predefinito per l'ambiente. I membri del progetto hanno accesso in lettura e scrittura a questo schema e possono pubblicare facilmente qualsiasi tabella creata in questo schema nel catalogo eseguendo l'origine dati predefinita creata come parte della creazione dell'ambiente. I parametri di Amazon Redshift utilizzati per creare l'ambiente possono essere utilizzati anche per creare nuove fonti di dati (anziché che il produttore di dati fornisca i propri parametri nella creazione dell'origine dati).

AWS Supporto per la formazione del cloud per Amazon DataZone

Rilasciato il 18/01/2024

Gli utenti di Amazon DataZone possono ora sfruttare AWS CloudFormation per modellare e gestire in modo efficace una suite di DataZone risorse Amazon. Questo approccio facilita l'approvvigionamento coerente delle risorse, consentendo al contempo la gestione del ciclo di vita attraverso l'infrastruttura come codice. Con i modelli personalizzati, puoi definire con precisione le risorse richieste e le loro interdipendenze. Per ulteriori informazioni, consulta il riferimento ai tipi di DataZone risorse Amazon.

Aggiungi i responsabili IAM direttamente come membri dei progetti Amazon DataZone

Rilasciato il 01/05/2024

Ora puoi aggiungere i principali IAM come membri del progetto, anche se tali responsabili IAM non hanno ancora effettuato l'accesso ad Amazon DataZone (requisito precedente). Dopo che un amministratore di dominio o un amministratore IT ha aggiunto `iam:GetUser` il ruolo di esecuzione del dominio, i proprietari del progetto possono aggiungere i principali IAM come membri semplicemente fornendo l'Amazon Resouce Name (ARN) del ruolo IAM o dell'utente IAM. `iam:GetRole` Il principale IAM deve comunque disporre delle autorizzazioni IAM necessarie per accedere ad Amazon DataZone e queste possono essere configurate nella console IAM. Per ulteriori informazioni, consulta Aggiungi membri a un progetto.

Support per tipi di asset personalizzati dal Data Portal

Rilasciato il 01/05/2024

Il supporto per risorse personalizzate consente DataZone ad Amazon di catalogare le risorse tramite il Data Portal per i dati non strutturati, inclusi dashboard, query e modelli, semplificando l'aggiunta di risorse personalizzate direttamente nel portale dati insieme al supporto API precedentemente disponibile. La possibilità di creare, aggiornare e pubblicare risorse personalizzate in Amazon ti consente di condividere DataZone, trovare, sottoscrivere qualsiasi tipo di risorsa e creare un flusso di lavoro aziendale che fornisca la governance di tali risorse. Per ulteriori informazioni, consulta Crea tipi di asset personalizzati.

2023

Eliminare il dominio

Rilasciato il 27/12/2023

Questa è una funzionalità che ti consente di eliminare più facilmente i tuoi domini. Ora puoi procedere con l'eliminazione del dominio anche se non è vuoto (ad esempio contiene progetti, ambienti, risorse, fonti di dati, ecc.). Per ulteriori informazioni, consulta Elimina i domini.

Modalità ibrida

Rilasciato il 22/12/2023

Amazon DataZone ha aggiunto il supporto per la modalità ibrida AWS Lake Formation. Con questo supporto, se pubblichi una tabella AWS Glue su Amazon DataZone con la sua sede AWS S3 registrata in Lake Formation in modalità ibrida, Amazon DataZone considera questa tabella come una risorsa gestita e può gestire le concessioni di abbonamento a questa tabella. Prima di questa versione di funzionalità, Amazon DataZone considerava questa tabella come una risorsa non gestita, ovvero Amazon non DataZone sarebbe stata in grado di concedere abbonamenti a questa tabella. Per ulteriori informazioni, consulta Configura le autorizzazioni di Lake Formation per Amazon DataZone.

Conformità HIPAA

Rilasciato il 14/12/2023

Amazon DataZone è ora conforme all'U.S. Health Insurance Portability and Accountability Act del 1996 (HIPAA). Per visualizzare l'elenco dei AWS servizi conformi alla normativa HIPAA, consulta https://aws.amazon.com/compliance//. hipaa-eligible-services-reference

Consigli di intelligenza artificiale per le descrizioni in Amazon DataZone (anteprima)

Rilasciato il 28/11/2023

AWS annuncia l'anteprima di una nuova funzionalità generativa basata sull'intelligenza artificiale in Amazon DataZone per migliorare il rilevamento, la comprensione e l'utilizzo dei dati arricchendo il catalogo dei dati aziendali. Con un solo clic, i produttori di dati possono generare descrizioni e contesto completi dei dati aziendali, evidenziare le colonne di impatto e includere consigli sui casi d'uso analitici. Grazie ai consigli di intelligenza artificiale per le descrizioni in Amazon DataZone, i consumatori di dati possono identificare le tabelle e le colonne di dati necessarie per l'analisi, il che migliora la reperibilità dei dati e riduce le back-and-forth comunicazioni con i produttori di dati. L'anteprima è disponibile nei DataZone domini Amazon distribuiti AWS nelle seguenti regioni: Stati

Uniti orientali (Virginia settentrionale), Stati Uniti occidentali (Oregon). Per ulteriori informazioni, consulta Utilizzo dell'apprendimento automatico e dell'intelligenza artificiale generativa.

DefaultDataLake miglioramento del progetto

Rilasciato il 20/11/2023

Amazon DataZone ha aggiunto un miglioramento al DefaultDataLake modello che ti offre un migliore controllo su chi può pubblicare quali dati dal tuo account. AWS Sono state introdotte due modifiche chiave con il lancio di questa funzionalità.

- Nella console, una volta abilitato il DefaultDataLake blueprint, puoi controllare quali progetti possono utilizzare il DefaultDataLake blueprint nel tuo account per creare profili di ambiente assegnando la gestione dei progetti al blueprint abilitato.
- La seconda modifica riguarda il portale. Se si crea un profilo di ambiente utilizzando il DefaultDataLake blueprint, è anche possibile selezionare i progetti autorizzati a utilizzare il profilo di ambiente per la creazione di ambienti. Per impostazione predefinita, tutti i progetti possono utilizzare il profilo di ambiente data lake, ma è possibile limitare il profilo di ambiente a progetti specifici e controllare anche quali dati possono essere pubblicati utilizzando gli ambienti creati con il profilo.

Per ulteriori informazioni, consulta Crea un profilo ambientale.

Configurazione

Per configurare Amazon DataZone, devi disporre di un AWS account e configurare le politiche e le autorizzazioni IAM richieste per Amazon DataZone.

Dopo aver configurato DataZone le autorizzazioni Amazon, ti consigliamo di completare i passaggi nella sezione Guida introduttiva che illustra come creare il DataZone dominio Amazon, ottenere l'URL del portale dati e i DataZone flussi di lavoro Amazon di base per produttori e consumatori di dati.

Argomenti

Registrati per creare un account AWS

Se non disponi di un AWS account, completa i seguenti passaggi per crearne uno.

Se hai un' AWS organizzazione, crea un account:

1. Accedere alla AWS Management Console e aprire la console Organizations all'indirizzo https://console.aws.amazon.com/organizations/.
2. Nel riquadro di navigazione, scegli AWS account.
3. Scegli Aggiungi un AWS account.
4. Scegli Crea un AWS account e fornisci i dettagli richiesti. Scegli Crea AWS account.

Per creare un AWS account

1. Apri https://portal.aws.amazon.com/billing/signup
2. Segui le istruzioni online.

   Nel corso della procedura di registrazione riceverai una telefonata, durante la quale sarà necessario inserire un codice di verifica attraverso la tastiera del telefono.

Quando si registra un AWS account, viene creato un utente root dell'AWS account. L'utente root ha accesso a tutti i AWS servizi e le risorse dell'account. Come best practice di sicurezza, assegna l'accesso amministrativo a un utente amministrativo e utilizza solo l'utente root per eseguire attività che richiedono l'accesso di un utente root.

Configura le autorizzazioni IAM necessarie per utilizzare la console di DataZone gestione Amazon

Qualsiasi utente, gruppo o ruolo che desideri utilizzare la console di DataZone gestione Amazon deve disporre delle autorizzazioni richieste.

Argomenti

- Allega policy obbligatorie e facoltative a un utente, gruppo o ruolo per l'accesso alla DataZone console Amazon
- Crea una policy personalizzata per le autorizzazioni IAM per abilitare la creazione semplificata di ruoli da parte della console di DataZone servizio Amazon
- Crea una politica personalizzata per le autorizzazioni per gestire un account associato a un dominio Amazon DataZone
- (Facoltativo) Crea una politica personalizzata per le autorizzazioni di AWS Identity Center per abilitare il Single Sign-On (SSO) per il tuo dominio
- (Facoltativo) Crea una policy personalizzata per le autorizzazioni di AWS Identity Center per aggiungere e rimuovere l'accesso di utenti e gruppi SSO al tuo dominio Amazon. DataZone
- (Facoltativo) Aggiungi il tuo responsabile IAM come utente chiave per creare il tuo DataZone dominio Amazon con una chiave gestita dal cliente fornita da AWS Key Management Service (KMS)

Allega policy obbligatorie e facoltative a un utente, gruppo o ruolo per l'accesso alla DataZone console Amazon

Completa la seguente procedura per allegare le politiche personalizzate obbligatorie e facoltative a un utente, gruppo o ruolo. Per ulteriori informazioni, consulta AWS politiche gestite per Amazon DataZone.

1. Accedi alla console di AWS gestione e apri la console IAM all'indirizzo https://console.aws.amazon.com/iam/.
2. Nel riquadro di navigazione, seleziona Policy.
3. Scegli le seguenti politiche da associare al tuo utente, gruppo o ruolo.

   - Nell'elenco delle politiche, seleziona la casella di controllo accanto a AmazonDataZoneFullAccess. Puoi utilizzare il menu Filtro e la casella di ricerca per filtrare l'elenco di policy. Per ulteriori informazioni, consulta AWS politica gestita: AmazonDataZoneFullAccess.
   - (Facoltativo) Crea una policy personalizzata per le autorizzazioni IAM per abilitare la creazione semplificata di ruoli tramite la console di DataZone servizio Amazon.
   - (Facoltativo) Crea una policy personalizzata per le autorizzazioni di AWS Identity Center per abilitare il Single Sign-On (SSO) per il tuo dominio.
   - (Facoltativo) Crea una policy personalizzata per le autorizzazioni di AWS Identity Center per aggiungere e rimuovere l'accesso di utenti e gruppi SSO al tuo dominio Amazon. DataZone
4. Scegli Operazioni e seleziona Collega.
5. Scegli l'utente, il gruppo o il ruolo a cui desideri allegare la policy. Puoi usare il menu Filtro e la casella di ricerca per filtrare l'elenco delle entità principali. Dopo aver scelto l'utente, il gruppo o il ruolo, scegli Allega politica.

Crea una policy personalizzata per le autorizzazioni IAM per abilitare la creazione semplificata di ruoli da parte della console di DataZone servizio Amazon

Completa la seguente procedura per creare una policy in linea personalizzata e disporre delle autorizzazioni necessarie per consentire DataZone ad Amazon di creare i ruoli necessari nella console di AWS gestione per tuo conto.

1. Accedi alla console di AWS gestione e apri la console IAM all'indirizzo https://console.aws.amazon.com/iam/.
2. Nel pannello di navigazione, scegli Utenti o Gruppi di utenti.
3. Nell'elenco, scegli il nome dell'utente o del gruppo in cui integrare una policy.
4. Scegliere la scheda Permissions (Autorizzazioni) e, se necessario, espandere la sezione Permissions policies (Policy autorizzazioni).

5. Scegli il link Aggiungi autorizzazioni e Crea policy in linea.
6. Nella schermata Crea politica, nella sezione Editor delle politiche, scegli JSON.

   Crea un documento di policy con le seguenti istruzioni JSON, quindi scegli Avanti.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "iam:CreatePolicy",
                "iam:CreateRole"
            ],
            "Resource": [
                "arn:aws:iam::*:policy/service-role/AmazonDataZone*",
                "arn:aws:iam::*:role/service-role/AmazonDataZone*"
            ]
        },
        {
            "Effect": "Allow",
            "Action": "iam:AttachRolePolicy",
            "Resource": "arn:aws:iam::*:role/service-role/AmazonDataZone*",
            "Condition": {
                "ArnLike": {
                    "iam:PolicyARN": [
                        "arn:aws:iam::aws:policy/AmazonDataZone*",
                        "arn:aws:iam::*:policy/service-role/AmazonDataZone*"
                    ]
                }
            }
        }
    ]
}
```

7. Nella schermata Revisione della politica, inserisci un nome per la politica. Al termine, scegliere Create policy (Crea policy). Assicurati che non siano presenti errori in una casella rossa nella parte superiore dello schermo. Correggi gli eventuali errori segnalati.

Crea una politica personalizzata per le autorizzazioni per gestire un account associato a un dominio Amazon DataZone

Completa la seguente procedura per creare una politica in linea personalizzata e disporre delle autorizzazioni necessarie in un AWS account associato per elencare, accettare e rifiutare le condivisioni di risorse di un dominio, quindi abilitare, configurare e disabilitare i blueprint di ambiente nell'account associato. È inoltre necessario abilitare la creazione semplificata di ruoli della console di DataZone servizio Amazon opzionale disponibile durante la configurazione del blueprint. Crea una policy personalizzata per le autorizzazioni IAM per abilitare la creazione semplificata di ruoli da parte della console di DataZone servizio Amazon

1. Accedi alla console di AWS gestione e apri la console IAM all'indirizzo https://console.aws.amazon.com/iam/.
2. Nel pannello di navigazione, scegli Utenti o Gruppi di utenti.
3. Nell'elenco, scegli il nome dell'utente o del gruppo in cui integrare una policy.
4. Scegliere la scheda Permissions (Autorizzazioni) e, se necessario, espandere la sezione Permissions policies (Policy autorizzazioni).
5. Scegli il link Aggiungi autorizzazioni e Crea policy in linea.
6. Nella schermata Crea politica, nella sezione Editor delle politiche, scegli JSON. Crea un documento di policy con le seguenti istruzioni JSON, quindi scegli Avanti.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "datazone:ListEnvironmentBlueprintConfigurations",
                "datazone:PutEnvironmentBlueprintConfiguration",
                "datazone:GetDomain",
                "datazone:ListDomains",
                "datazone:GetEnvironmentBlueprintConfiguration",
                "datazone:ListEnvironmentBlueprints",
                "datazone:GetEnvironmentBlueprint",
                "datazone:ListAccountEnvironments",
                "datazone:DeleteEnvironmentBlueprintConfiguration"
            ],
            "Resource": "*"
```

```
        },
        {
            "Effect": "Allow",
            "Action": "iam:PassRole",
            "Resource": [
                "arn:aws:iam::*:role/AmazonDataZone",
                "arn:aws:iam::*:role/service-role/AmazonDataZone*"
            ],
            "Condition": {
                "StringEquals": {
                    "iam:passedToService": "datazone.amazonaws.com"
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": "iam:AttachRolePolicy",
            "Resource": "arn:aws:iam::*:role/service-role/AmazonDataZone*",
            "Condition": {
                "ArnLike": {
                    "iam:PolicyARN": [
                        "arn:aws:iam::aws:policy/AmazonDataZone*",
                        "arn:aws:iam::*:policy/service-role/AmazonDataZone*"
                    ]
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": "iam:ListRoles",
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "iam:CreatePolicy",
                "iam:CreateRole"
            ],
            "Resource": [
                "arn:aws:iam::*:policy/service-role/AmazonDataZone*",
                "arn:aws:iam::*:role/service-role/AmazonDataZone*"
            ]
        },
        {
```

```
            "Effect": "Allow",
            "Action": [
                "ram:AcceptResourceShareInvitation",
                "ram:RejectResourceShareInvitation",
                "ram:GetResourceShareInvitations"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "s3:ListAllMyBuckets",
                "s3:ListBucket",
                "s3:GetBucketLocation"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": "s3:CreateBucket",
            "Resource": "arn:aws:s3:::amazon-datazone*"
        }
    ]
}
```

7. Nella schermata Revisione della politica, inserisci un nome per la politica. Al termine, scegliere Create policy (Crea policy). Assicurati che non siano presenti errori in una casella rossa nella parte superiore dello schermo. Correggi gli eventuali errori segnalati.

(Facoltativo) Crea una politica personalizzata per le autorizzazioni di AWS Identity Center per abilitare il Single Sign-On (SSO) per il tuo dominio

Completa la seguente procedura per creare una policy in linea personalizzata con le autorizzazioni necessarie per abilitare il single sign-on (SSO) utilizzando IAM AWS Identity Center in Amazon. DataZone

1. Accedi alla console di AWS gestione e apri la console IAM all'indirizzo https://console.aws.amazon.com/iam/.
2. Nel pannello di navigazione, scegli Utenti o Gruppi di utenti.

3. Nell'elenco, scegli il nome dell'utente o del gruppo in cui integrare una policy.
4. Scegliere la scheda Permissions (Autorizzazioni) e, se necessario, espandere la sezione Permissions policies (Policy autorizzazioni).
5. Scegli Aggiungi autorizzazioni e Crea policy in linea.
6. Nella schermata Crea policy, nella sezione Editor di policy, scegli JSON.

   Crea un documento di policy con le seguenti istruzioni JSON, quindi scegli Avanti.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "sso:DeleteManagedApplicationInstance",
                "sso:CreateManagedApplicationInstance",
                "sso:PutApplicationAssignmentConfiguration"
            ],
            "Resource": "*"
        }
    ]
}
```

7. Nella schermata Revisione della politica, inserisci un nome per la politica. Al termine, scegliere Create policy (Crea policy). Assicurati che non siano presenti errori in una casella rossa nella parte superiore dello schermo. Correggi gli eventuali errori segnalati.

(Facoltativo) Crea una policy personalizzata per le autorizzazioni di AWS Identity Center per aggiungere e rimuovere l'accesso di utenti e gruppi SSO al tuo dominio Amazon. DataZone

Completa la seguente procedura per creare una politica in linea personalizzata con le autorizzazioni necessarie per aggiungere e rimuovere l'accesso di utenti e gruppi SSO al tuo dominio Amazon. DataZone

1. Accedi alla console di AWS gestione e apri la console IAM all'indirizzo https://console.aws.amazon.com/iam/.

2. Nel pannello di navigazione, scegli Utenti o Gruppi di utenti.
3. Nell'elenco, scegli il nome dell'utente o del gruppo in cui integrare una policy.
4. Scegliere la scheda Permissions (Autorizzazioni) e, se necessario, espandere la sezione Permissions policies (Policy autorizzazioni).
5. Scegli Aggiungi autorizzazioni e Crea policy in linea.
6. Nella schermata Crea policy, nella sezione Editor di policy, scegli JSON.

   Crea un documento di policy con le seguenti istruzioni JSON, quindi scegli Avanti.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "sso:GetManagedApplicationInstance",
        "sso:ListProfiles",
        "sso:GetProfiles",
        "sso:AssociateProfile",
        "sso:DisassociateProfile",
        "sso:GetProfile"
      ],
      "Resource": "*"
    }
  ]
}
```

7. Nella schermata Revisione della politica, inserisci un nome per la politica. Al termine, scegliere Create policy (Crea policy). Assicurati che non siano presenti errori in una casella rossa nella parte superiore dello schermo. Correggi gli eventuali errori segnalati.

(Facoltativo) Aggiungi il tuo responsabile IAM come utente chiave per creare il tuo DataZone dominio Amazon con una chiave gestita dal cliente fornita da AWS Key Management Service (KMS)

Prima di poter creare facoltativamente il tuo DataZone dominio Amazon con una chiave gestita dal cliente (CMK) del AWS Key Management Service (KMS), completa la seguente procedura per rendere il tuo responsabile IAM un utente della tua chiave KMS.

1. Accedi alla console di AWS gestione e apri la console KMS all'indirizzo https://console.aws.amazon.com/kms/.
2. Per visualizzare le chiavi nell'account creato e gestito dall'utente, nel riquadro di navigazione, seleziona Chiavi gestite dal cliente.
3. Nell'elenco di chiavi KMS, scegliere l'alias o l'ID chiave della chiave KMS che si intende esaminare.
4. Per aggiungere o rimuovere utenti chiave e consentire o impedire agli AWS account esterni di utilizzare la chiave KMS, utilizza i controlli nella sezione Utenti chiave della pagina. Gli utenti della chiave possono utilizzare la chiave KMS nelle operazioni di crittografia, ad esempio crittografia, decrittografia, ricrittografia e generazione di chiavi di dati.

Configura le autorizzazioni IAM necessarie per utilizzare il portale DataZone dati Amazon

Qualsiasi utente, gruppo o ruolo che desideri utilizzare il portale DataZone dati o il catalogo Amazon deve disporre delle autorizzazioni richieste.

Argomenti

- Allega la policy richiesta a un utente, gruppo o ruolo per l'accesso al portale DataZone dati Amazon
- Allega la policy richiesta a un utente, gruppo o ruolo per l'accesso al DataZone catalogo Amazon
- Allega una policy opzionale a un utente, gruppo o ruolo per l'accesso al portale DataZone dati o al catalogo Amazon se il tuo dominio è crittografato con una chiave gestita dal cliente fornita da Key Management Service (AWS KMS)

Allega la policy richiesta a un utente, gruppo o ruolo per l'accesso al portale DataZone dati Amazon

Puoi accedere al portale DataZone dati di Amazon utilizzando le tue credenziali o AWS le tue credenziali Single Sign-On (SSO). Segui le istruzioni nella sezione seguente per configurare le autorizzazioni necessarie per accedere al portale dati con le tue credenziali. AWS Per ulteriori informazioni sull'utilizzo di Amazon DataZone con SSO, consultaConfigurazione di AWS IAM Identity Center per Amazon DataZone.

> **Note**
>
> Solo i responsabili IAM presenti nell' AWS account del tuo dominio possono accedere al portale dati del dominio. I responsabili IAM di altri AWS account non possono accedere al portale dati del dominio.

Completa la procedura seguente per allegare la policy richiesta a un utente, gruppo o ruolo. Per ulteriori informazioni, consulta AWS politiche gestite per Amazon DataZone.

1. Accedi alla console di AWS gestione e apri la console IAM all'indirizzo https://console.aws.amazon.com/iam/.
2. Nel riquadro di navigazione, scegli Utenti, Gruppi di utenti o Ruoli.
3. Nell'elenco, scegli il nome dell'utente, del gruppo o del ruolo in cui incorporare una politica.
4. Scegliere la scheda Permissions (Autorizzazioni) e, se necessario, espandere la sezione Permissions policies (Policy autorizzazioni).
5. Scegli il link Aggiungi autorizzazioni e Crea policy in linea.
6. Nella schermata Crea politica, nella sezione Editor delle politiche, scegli JSON. Crea un documento di policy con le seguenti istruzioni JSON, quindi scegli Avanti.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "datazone:GetIamPortalLoginUrl"
```

```
            ],
            "Resource": [
                "*"
            ]
        }
    ]
}
```

7. Nella schermata Revisione della politica, inserisci un nome per la politica. Al termine, scegliere Create policy (Crea policy). Assicurati che non siano presenti errori in una casella rossa nella parte superiore dello schermo. Correggi gli eventuali errori segnalati.

Allega la policy richiesta a un utente, gruppo o ruolo per l'accesso al DataZone catalogo Amazon

> **Note**
>
> Solo i responsabili IAM presenti nell' AWS account del tuo dominio possono accedere al catalogo del dominio. I principali IAM di altri AWS account non possono accedere al catalogo del dominio.

Puoi concedere alle tue identità IAM l'accesso al catalogo del tuo DataZone dominio Amazon tramite API e SDK con la seguente procedura. Se desideri che queste identità IAM abbiano accesso anche al portale DataZone dati Amazon, segui inoltre la procedura sopra riportata perAllega la policy richiesta a un utente, gruppo o ruolo per l'accesso al portale DataZone dati Amazon. Per ulteriori informazioni, consulta AWS politiche gestite per Amazon DataZone.

1. Accedi alla console di AWS gestione e apri la console IAM all'indirizzo https://console.aws.amazon.com/iam/.
2. Nel riquadro di navigazione, seleziona Policy.
3. Nell'elenco delle politiche, seleziona il pulsante di opzione accanto alla AmazonDataZoneFullUserAccesspolitica. Puoi utilizzare il menu Filtro e la casella di ricerca per filtrare l'elenco di policy. Per ulteriori informazioni, consulta AWS politica gestita: AmazonDataZoneFullUserAccess
4. Scegli Operazioni e seleziona Collega.

5. Scegli l'utente, il gruppo o il ruolo a cui desideri allegare la politica selezionando la casella di controllo accanto a ciascun principale. Puoi usare il menu Filtro e la casella di ricerca per filtrare l'elenco delle entità principali. Dopo aver scelto l'utente, il gruppo o il ruolo, scegli Allega politica.

Allega una policy opzionale a un utente, gruppo o ruolo per l'accesso al portale DataZone dati o al catalogo Amazon se il tuo dominio è crittografato con una chiave gestita dal cliente fornita da Key Management Service (AWS KMS)

Se crei il tuo DataZone dominio Amazon con la tua chiave KMS per la crittografia dei dati, devi anche creare una policy in linea con le seguenti autorizzazioni e collegarla ai tuoi principali IAM in modo che possano accedere al portale o al catalogo DataZone dati Amazon.

1. Accedi alla console di AWS gestione e apri la console IAM all'indirizzo https://console.aws.amazon.com/iam/.
2. Nel riquadro di navigazione, scegli Utenti, Gruppi di utenti o Ruoli.
3. Nell'elenco, scegli il nome dell'utente, del gruppo o del ruolo in cui incorporare una politica.
4. Scegliere la scheda Permissions (Autorizzazioni) e, se necessario, espandere la sezione Permissions policies (Policy autorizzazioni).
5. Scegli il link Aggiungi autorizzazioni e Crea policy in linea.
6. Nella schermata Crea politica, nella sezione Editor delle politiche, scegli JSON. Crea un documento di policy con le seguenti istruzioni JSON, quindi scegli Avanti.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "kms:Decrypt",
                "kms:GenerateDataKey",
                "kms:DescribeKey"
            ],
            "Resource": "*"
        }
    ]
```

```
}
```

7. Nella schermata Revisione della politica, inserisci un nome per la politica. Al termine, scegliere Create policy (Crea policy). Assicurati che non siano presenti errori in una casella rossa nella parte superiore dello schermo. Correggi gli eventuali errori segnalati.

Configurazione di AWS IAM Identity Center per Amazon DataZone

> **Note**
>
> AWS Identity Center deve essere abilitato nella stessa AWS regione del tuo DataZone dominio Amazon. Attualmente, AWS Identity Center può essere abilitato solo in una singola AWS regione.

Puoi accedere al portale DataZone dati di Amazon utilizzando le tue credenziali o credenziali Single Sign-On (SSO). AWS Segui le istruzioni in questa sezione per configurare AWS IAM Identity Center for Amazon DataZone. Per ulteriori informazioni sull'utilizzo di Amazon DataZone con AWS le tue credenziali, consultaConfigura le autorizzazioni IAM necessarie per utilizzare la console di DataZone gestione Amazon.

Puoi saltare le procedure in questa sezione se hai già abilitato e configurato AWS IAM Identity Center (successore di AWS Single Sign-On) nella stessa AWS regione in cui desideri creare il tuo dominio Amazon. DataZone

Completa la seguente procedura per abilitare AWS IAM Identity Center (successore di Single Sign-On). AWS

1. Per abilitare AWS IAM Identity Center, devi accedere alla console di AWS gestione utilizzando le credenziali del tuo account di gestione AWS Organizations. Non puoi abilitare IAM Identity Center dopo aver effettuato l'accesso con le credenziali di un account membro AWS Organizations. Per ulteriori informazioni, consulta Creare e gestire un'organizzazione nella AWS Organizations User Guide.
2. Apri la console AWS IAM Identity Center (successore di AWS Single Sign-On) e utilizza il selettore di regione nella barra di navigazione in alto per scegliere la AWS regione in cui desideri creare il tuo dominio Amazon. DataZone
3. Scegli Abilita .

4. Scegli la fonte della tua identità.

   Per impostazione predefinita, hai a disposizione uno store IAM Identity Center per una gestione degli utenti semplice e veloce. Facoltativamente, puoi invece connettere un provider di identità esterno. In questa procedura, utilizziamo l'archivio IAM Identity Center predefinito.

   Per ulteriori informazioni, consulta Scegli la tua fonte di identità.
5. Nel riquadro di navigazione di IAM Identity Center, scegli Gruppi e scegli Crea gruppo. Inserisci il nome del gruppo e scegli Crea.
6. Nel riquadro di navigazione di IAM Identity Center, scegli Utenti.
7. Nella schermata Aggiungi utente, inserisci le informazioni richieste e scegli Invia un'e-mail all'utente con le istruzioni per la configurazione della password. L'utente dovrebbe ricevere un'e-mail con i passaggi di configurazione successivi.
8. Scegli Avanti: Gruppi, scegli il gruppo che desideri e scegli Aggiungi utente. Gli utenti dovrebbero ricevere un'e-mail che li invita a utilizzare l'SSO. In questa e-mail, devono scegliere Accetta invito e impostare la password.

Dopo aver creato il tuo DataZone dominio Amazon, puoi abilitare AWS Identity Center for Amazon DataZone e fornire l'accesso ai tuoi utenti e gruppi SSO. Per ulteriori informazioni, consulta Abilita IAM Identity Center per Amazon DataZone.

Nozioni di base

Le informazioni contenute in questa sezione ti aiutano a iniziare a usare Amazon DataZone. Se non conosci Amazon DataZone, inizia acquisendo familiarità con i concetti e la terminologia presentati in DataZone Terminologia e concetti di Amazon.

Questa sezione introduttiva illustra i seguenti flussi di lavoro Amazon DataZone quickstart:

Argomenti

- Amazon DataZone quickstart con i dati di AWS Glue
- Amazon DataZone quickstart con i dati di Amazon Redshift
- Amazon DataZone quickstart con script di esempio

> **Important**
>
> Prima di iniziare i passaggi di uno di questi flussi di lavoro di avvio rapido, devi completare le procedure descritte nella sezione Configurazione di questa guida. Se utilizzi un AWS account nuovo di zecca, devi configurare le autorizzazioni necessarie per utilizzare la console di DataZone gestione Amazon. Se utilizzi un AWS account con oggetti AWS Glue Data Catalog esistenti, devi anche configurare le autorizzazioni Lake Formation per Amazon DataZone.

Amazon DataZone quickstart con i dati di AWS Glue

Argomenti

- Fase 1: creare il DataZone dominio Amazon e il portale dati
- Fase 2 - Creare il progetto di pubblicazione
- Fase 3 - Creare l'ambiente
- Fase 4 - Produrre dati per la pubblicazione
- Fase 5 - Raccogli i metadati da AWS Glue
- Passaggio 6: cura e pubblica la risorsa di dati
- Fase 7 - Creazione del progetto per l'analisi dei dati
- Fase 8 - Creare un ambiente per l'analisi dei dati
- Passaggio 9: cerca nel catalogo dati e iscriviti ai dati

- Passaggio 10: approva la richiesta di abbonamento
- Passaggio 11: creare una query e analizzare i dati in Amazon Athena

Fase 1: creare il DataZone dominio Amazon e il portale dati

Questa sezione descrive i passaggi per creare un DataZone dominio Amazon e un portale dati per questo flusso di lavoro.

Completa la seguente procedura per creare un DataZone dominio Amazon. Per ulteriori informazioni sui DataZone domini Amazon, consulta DataZone Terminologia e concetti di Amazon.

1. Accedi alla DataZone console Amazon all'indirizzo https://console.aws.amazon.com/datazone, accedi e scegli Crea dominio.

   > **Note**
   >
   > Se desideri utilizzare un DataZone dominio Amazon esistente per questo flusso di lavoro, scegli Visualizza domini, quindi scegli il dominio che desideri utilizzare e quindi procedi alla Fase 2 della creazione di un progetto di pubblicazione.

2. Nella pagina Crea dominio, fornisci i valori per i seguenti campi:

   - Nome: specifica un nome per il tuo dominio. Ai fini di questo flusso di lavoro, puoi chiamare questo dominio Marketing.
   - Descrizione: specifica una descrizione del dominio opzionale.
   - Crittografia dei dati: per impostazione predefinita, i dati vengono crittografati con una chiave che AWS possiede e gestisce per te. In questo caso d'uso, puoi lasciare le impostazioni di crittografia dei dati predefinite.

     Per ulteriori informazioni sull'utilizzo delle chiavi gestite dai clienti, consultaCrittografia dei dati a riposo per Amazon DataZone. Se utilizzi la tua chiave KMS per la crittografia dei dati, devi includere la seguente dichiarazione come predefinitaAmazonDataZoneDomainExecutionRole.

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

```
      "Action": [
        "kms:Decrypt",
        "kms:GenerateDataKey"
      ],
      "Resource": "*"
    }
  ]
}
```

- Accesso al servizio: lascia invariata l'opzione Usa un ruolo predefinito selezionata per impostazione predefinita.

> **Note**
>
> Se utilizzi un DataZone dominio Amazon esistente per questo flusso di lavoro, puoi scegliere l'opzione Usa un ruolo di servizio esistente e quindi scegliere un ruolo esistente dal menu a discesa.

- In Configurazione rapida, scegli Configura questo account per il consumo e la pubblicazione dei dati. Questa opzione abilita i DataZone blueprint Amazon integrati di Data lake e Data warehouse e configura le autorizzazioni, le risorse, un progetto predefinito e i profili di ambiente data lake e data warehouse predefiniti per questo account. Per ulteriori informazioni sui DataZone blueprint di Amazon, consulta DataZone Terminologia e concetti di Amazon.
- Mantieni invariati i campi rimanenti sotto i dettagli delle autorizzazioni.

> **Note**
>
> Se disponi di un DataZone dominio Amazon esistente, puoi scegliere l'opzione Usa un ruolo di servizio esistente e quindi scegliere un ruolo esistente dal menu a discesa per il ruolo Glue Manage Access, il ruolo Redshift Manage Access e il ruolo Provisioning.

- Mantieni invariati i campi sotto i tag.
- Scegli Crea dominio.

3. Una volta creato correttamente il dominio, scegli questo dominio e nella pagina di riepilogo del dominio, annota l'URL del portale dati per questo dominio. Puoi utilizzare questo URL per accedere al tuo portale DataZone dati Amazon e completare il resto dei passaggi di questo flusso di lavoro. Puoi anche accedere al portale dati scegliendo Open data portal.

> **Note**
>
> Nell'attuale versione di Amazon DataZone, una volta creato il dominio, l'URL generato per il portale dati non può essere modificato.

Il completamento della creazione del dominio può richiedere diversi minuti. Attendi che lo stato del dominio sia Disponibile prima di procedere al passaggio successivo.

Fase 2 - Creare il progetto di pubblicazione

Questa sezione descrive i passaggi necessari per creare il progetto di pubblicazione per questo flusso di lavoro.

1. Dopo aver completato il passaggio 1 precedente e aver creato un dominio, vedrai il messaggio Benvenuto su Amazon DataZone! finestra. In questa finestra, scegli Crea progetto.
2. Specificate il nome del progetto, ad esempio, per questo flusso di lavoro, potete assegnargli un nome SalesDataPublishingProject, quindi lasciare invariati gli altri campi e quindi scegliere Crea.

Fase 3 - Creare l'ambiente

Questa sezione descrive i passaggi necessari per creare un ambiente per questo flusso di lavoro.

1. Una volta completato il passaggio 2 precedente e aver creato il progetto, verrà visualizzata la finestra Il progetto è pronto per l'uso. In questa finestra, scegli Crea ambiente.
2. Nella pagina Crea ambiente, specifica quanto segue e quindi scegli Crea ambiente.
3. Specificate i valori per quanto segue:
   - Nome: specifica il nome dell'ambiente. Per questa procedura dettagliata, puoi chiamarla. `Default data lake environment`
   - Descrizione: specifica una descrizione per l'ambiente.
   - Profilo ambientale: scegli il profilo DataLakeProfiledell'ambiente. Ciò ti consente di utilizzare Amazon DataZone in questo flusso di lavoro per lavorare con i dati in Amazon S3, AWS Glue Catalog e Amazon Athena.
   - Per questa procedura dettagliata, mantieni invariati gli altri campi.
4. Seleziona Create environment (Crea ambiente).

Fase 4 - Produrre dati per la pubblicazione

Questa sezione descrive i passaggi necessari per produrre dati da pubblicare in questo flusso di lavoro.

1. Una volta completato il passaggio 3 precedente, nel `SalesDataPublishingProject` progetto, nel pannello di destra, in Strumenti di analisi, scegli Amazon Athena. Questo apre l'editor di query Athena utilizzando le credenziali del progetto per l'autenticazione. Assicurati che il tuo ambiente di pubblicazione sia selezionato nel menu a discesa DataZone dell'ambiente Amazon e che il `<environment_name>%_pub_db` database sia selezionato come nell'editor di query.
2. Per questa procedura dettagliata, stai utilizzando lo script di query Create Table as Select (CTAS) per creare una nuova tabella da pubblicare su Amazon. DataZone Nel tuo editor di query, esegui questo script CTAS per creare una `mkt_sls_table` tabella da pubblicare e rendere disponibile per la ricerca e l'abbonamento.

```
CREATE TABLE mkt_sls_table AS
SELECT 146776932 AS ord_num, 23 AS sales_qty_sld, 23.4 AS wholesale_cost, 45.0 as
 lst_pr, 43.0 as sell_pr, 2.0 as disnt, 12 as ship_mode,13 as warehouse_id, 23 as
 item_id, 34 as ctlg_page, 232 as ship_cust_id, 4556 as bill_cust_id
UNION ALL SELECT 46776931, 24, 24.4, 46, 44, 1, 14, 15, 24, 35, 222, 4551
UNION ALL SELECT 46777394, 42, 43.4, 60, 50, 10, 30, 20, 27, 43, 241, 4565
UNION ALL SELECT 46777831, 33, 40.4, 51, 46, 15, 16, 26, 33, 40, 234, 4563
UNION ALL SELECT 46779160, 29, 26.4, 50, 61, 8, 31, 15, 36, 40, 242, 4562
UNION ALL SELECT 46778595, 43, 28.4, 49, 47, 7, 28, 22, 27, 43, 224, 4555
UNION ALL SELECT 46779482, 34, 33.4, 64, 44, 10, 17, 27, 43, 52, 222, 4556
UNION ALL SELECT 46779650, 39, 37.4, 51, 62, 13, 31, 25, 31, 52, 224, 4551
UNION ALL SELECT 46780524, 33, 40.4, 60, 53, 18, 32, 31, 31, 39, 232, 4563
UNION ALL SELECT 46780634, 39, 35.4, 46, 44, 16, 33, 19, 31, 52, 242, 4557
UNION ALL SELECT 46781887, 24, 30.4, 54, 62, 13, 18, 29, 24, 52, 223, 4561
```

   Assicurati che la tabella mkt_sls_table sia stata creata correttamente nella sezione Tabelle e viste sul lato sinistro. Ora hai una risorsa di dati che può essere pubblicata nel DataZone catalogo Amazon.

Fase 5 - Raccogli i metadati da AWS Glue

Questa sezione descrive la fase di raccolta dei metadati da AWS Glue per questo flusso di lavoro.

1. Una volta completato il passaggio 4 precedente, nel portale DataZone dati Amazon, scegli il `SalesDataPublishingProject` progetto, quindi scegli la scheda Dati e quindi scegli Origini dati nel pannello a sinistra.
2. Scegli la fonte che è stata creata come parte del processo di creazione dell'ambiente.
3. Scegli Esegui accanto al menu a discesa Azione, quindi scegli il pulsante Aggiorna. Una volta completata l'esecuzione dell'origine dati, le risorse vengono aggiunte all' DataZone inventario Amazon.

Passaggio 6: cura e pubblica la risorsa di dati

Questa sezione descrive le fasi di cura e pubblicazione della risorsa di dati in questo flusso di lavoro.

1. Una volta completato il passaggio 5 precedente, nel portale DataZone dati di Amazon, scegli il `SalesDataPublishingProject` progetto che hai creato nel passaggio precedente, scegli la scheda Dati, scegli Dati di inventario nel pannello a sinistra e individua la `mkt_sls_table` tabella.
2. Apri la pagina dei dettagli dell'`mkt_sls_table`asset per visualizzare i nomi aziendali generati automaticamente. Scegliete l'icona Metadati generati automaticamente per visualizzare i nomi generati automaticamente per le risorse e le colonne. Puoi accettare o rifiutare ogni nome singolarmente o scegliere Accetta tutto per applicare i nomi generati. Facoltativamente, puoi anche aggiungere il modulo di metadati disponibile alla tua risorsa e selezionare i termini del glossario per classificare i dati.
3. Scegliete Pubblica risorsa per pubblicare la risorsa. `mkt_sls_table`

Fase 7 - Creazione del progetto per l'analisi dei dati

Questa sezione descrive le fasi di creazione del progetto per l'analisi dei dati. Questo è l'inizio delle fasi relative al consumo di dati di questo flusso di lavoro.

1. Una volta completato il passaggio 6 precedente, nel portale DataZone dati Amazon, scegli Crea progetto dal menu a discesa Progetto.

2. Nella pagina Crea progetto, specifica il nome del progetto, ad esempio, per questo flusso di lavoro, puoi assegnargli un nome MarketingDataAnalysisProject, quindi lascia invariati gli altri campi e quindi scegli Crea.

Fase 8 - Creare un ambiente per l'analisi dei dati

Questa sezione descrive le fasi di creazione di un ambiente per l'analisi dei dati.

1. Una volta completato il passaggio 7 precedente, nel portale DataZone dati Amazon, scegli il `MarketingDataAnalysisProject` progetto, quindi scegli la scheda Ambienti e quindi scegli Crea ambiente.
2. Nella pagina Crea ambiente, specifica quanto segue e quindi scegli Crea ambiente.
   - Nome: specifica il nome dell'ambiente. Per questa procedura dettagliata, puoi chiamarla. `Default data lake environment`
   - Descrizione: specifica una descrizione per l'ambiente.
   - Profilo ambientale: scegli il profilo DataLakeProfileambientale integrato.
   - Per questa procedura dettagliata, mantieni invariato il resto dei campi.

Passaggio 9: cerca nel catalogo dati e iscriviti ai dati

Questa sezione descrive i passaggi della ricerca nel catalogo dati e della sottoscrizione ai dati.

1. Una volta completato il passaggio 8 precedente, nel portale DataZone dati di Amazon, scegli l' DataZoneicona Amazon e, nel campo Amazon DataZone Search, cerca gli asset di dati utilizzando parole chiave (ad esempio, «catalogo» o «vendite») nella barra di ricerca del portale dati.

   Se necessario, applica filtri o ordinamenti e, una volta individuato l'asset Product Sales Data, puoi sceglierlo per aprire la pagina dei dettagli della risorsa.
2. Nella pagina dei dettagli della risorsa Catalog Sales Data, scegliete Iscriviti.
3. Nella finestra di dialogo Iscriviti, scegli il tuo progetto MarketingDataAnalysisProjectconsumer dal menu a discesa, quindi specifica il motivo della richiesta di abbonamento e quindi scegli Iscriviti.

Passaggio 10: approva la richiesta di abbonamento

Questa sezione descrive i passaggi per l'approvazione della richiesta di abbonamento.

1. Una volta completato il passaggio 9 precedente, nel portale DataZone dati di Amazon, scegli il SalesDataPublishingProjectprogetto con cui hai pubblicato la tua risorsa.
2. Scegli la scheda Dati, quindi Dati pubblicati, quindi scegli Richieste in arrivo.
3. Ora puoi vedere la riga relativa alla nuova richiesta che richiede un'approvazione. Scegli Visualizza richiesta. Fornisci un motivo per l'approvazione e scegli Approva.

Passaggio 11: creare una query e analizzare i dati in Amazon Athena

Ora che hai pubblicato con successo una risorsa nel DataZone catalogo Amazon e ti sei abbonato, puoi analizzarla.

1. Nel portale DataZone dati di Amazon, scegli il tuo progetto MarketingDataAnalysisProjectconsumer e poi, dal pannello di destra, in Strumenti di analisi, scegli il link Query data with Amazon Athena. Questo apre l'editor di query di Amazon Athena utilizzando le credenziali del progetto per l'autenticazione. Scegli l'ambiente MarketingDataAnalysisProjectconsumer dal menu a discesa Amazon DataZone Environment nell'editor di query, quindi scegli il tuo progetto `<environment_name>%sub_db` dal menu a discesa del database.
2. Ora puoi eseguire interrogazioni sulla tabella degli abbonati. È possibile scegliere la tabella tra Tabelle e viste, quindi scegliere Anteprima per visualizzare l'istruzione select nella schermata dell'editor. Esegui la query per vedere i risultati.

Amazon DataZone quickstart con i dati di Amazon Redshift

Argomenti

- Fase 1: creare il DataZone dominio Amazon e il portale dati
- Fase 2 - Creare il progetto di pubblicazione
- Fase 3 - Creare l'ambiente
- Fase 4 - Produrre dati per la pubblicazione
- Fase 5 - Raccolta di metadati da Amazon Redshift
- Passaggio 6: cura e pubblica la risorsa di dati

- Fase 7 - Creazione del progetto per l'analisi dei dati
- Fase 8 - Creare un ambiente per l'analisi dei dati
- Passaggio 9: cerca nel catalogo dati e iscriviti ai dati
- Passaggio 10: approva la richiesta di abbonamento
- Fase 11: creare una query e analizzare i dati in Amazon Redshift

Fase 1: creare il DataZone dominio Amazon e il portale dati

Completa la seguente procedura per creare un DataZone dominio Amazon. Per ulteriori informazioni sui DataZone domini Amazon, consulta DataZone Terminologia e concetti di Amazon.

1. Accedi alla DataZone console Amazon all'indirizzo https://console.aws.amazon.com/datazone, accedi e scegli Crea dominio.

   > **Note**
   >
   > Se desideri utilizzare un DataZone dominio Amazon esistente per questo flusso di lavoro, scegli Visualizza domini, quindi scegli il dominio che desideri utilizzare e quindi procedi alla Fase 2 della creazione di un progetto di pubblicazione.

2. Nella pagina Crea dominio, fornisci i valori per i seguenti campi:

   - Nome: specifica un nome per il tuo dominio. Ai fini di questo flusso di lavoro, puoi chiamare questo dominio`Marketing`.
   - Descrizione: specifica una descrizione del dominio opzionale.
   - Crittografia dei dati: per impostazione predefinita, i dati vengono crittografati con una chiave che AWS possiede e gestisce per te. Per questa procedura dettagliata, puoi lasciare le impostazioni di crittografia dei dati predefinite.

     Per ulteriori informazioni sull'utilizzo delle chiavi gestite dai clienti, consulta. Crittografia dei dati a riposo per Amazon DataZone Se utilizzi la tua chiave KMS per la crittografia dei dati, devi includere la seguente dichiarazione come predefinitaAmazonDataZoneDomainExecutionRole.

     ```
     {
       "Version": "2012-10-17",
       "Statement": [
     ```

```
    {
      "Effect": "Allow",
      "Action": [
        "kms:Decrypt",
        "kms:GenerateDataKey"
      ],
      "Resource": "*"
    }
  ]
}
```

- Accesso al servizio: scegli l'opzione Usa un ruolo di servizio personalizzato, quindi scegli l'opzione AmazonDataZoneDomainExecutionRoledal menu a discesa.
- In Configurazione rapida, scegli Configura questo account per il consumo e la pubblicazione dei dati. Questa opzione abilita i DataZone blueprint Amazon integrati di Data lake e Data warehouse e configura le autorizzazioni e le risorse necessarie per completare il resto dei passaggi di questo flusso di lavoro. Per ulteriori informazioni sui DataZone blueprint di Amazon, consulta DataZone Terminologia e concetti di Amazon.
- Mantieni invariati i campi rimanenti in Informazioni sulle autorizzazioni e Tag, quindi scegli Crea dominio.

3. Una volta creato correttamente il dominio, scegli questo dominio e, nella pagina di riepilogo del dominio, annota l'URL del portale dati relativo a questo dominio. Puoi utilizzare questo URL per accedere al tuo portale DataZone dati Amazon e completare il resto dei passaggi di questo flusso di lavoro.

> **Note**
>
> Nell'attuale versione di Amazon DataZone, una volta creato il dominio, l'URL generato per il portale dati non può essere modificato.

Il completamento della creazione del dominio può richiedere diversi minuti. Attendi che lo stato del dominio sia Disponibile prima di procedere al passaggio successivo.

Fase 2 - Creare il progetto di pubblicazione

La sezione seguente descrive le fasi di creazione del progetto di pubblicazione in questo flusso di lavoro.

1. Una volta completato il passaggio 1, accedi al portale DataZone dati Amazon utilizzando l'URL del portale dati e accedi utilizzando le tue credenziali Single Sign-On (SSO) o AWS IAM.
2. Scegli Crea progetto, specifica il nome del progetto, ad esempio, per questo flusso di lavoro, puoi assegnargli un nome SalesDataPublishingProject, quindi lascia invariati gli altri campi e quindi scegli Crea.

Fase 3 - Creare l'ambiente

La sezione seguente descrive i passaggi per creare un ambiente in questo flusso di lavoro.

1. Una volta completato il passaggio 2, nel portale DataZone dati Amazon, scegli il `SalesDataPublishingProject` progetto creato nel passaggio precedente, quindi scegli la scheda Ambienti e quindi scegli Crea ambiente.
2. Nella pagina Crea ambiente, specifica quanto segue e poi scegli Crea ambiente.

   - Nome: specifica il nome dell'ambiente. Per questa procedura dettagliata, puoi chiamarla. `Default data warehouse environment`
   - Descrizione: specifica una descrizione per l'ambiente.
   - Profilo ambientale: scegli il profilo DataWarehouseProfiledell'ambiente.
   - Fornisci il nome del cluster Amazon Redshift, il nome del database e l'ARN segreto per il cluster Amazon Redshift in cui sono archiviati i dati.

   > **Note**
   >
   > Assicurati che il tuo segreto in AWS Secrets Manager includa i seguenti tag (chiave/valore):
   >
   > - Per il cluster Amazon Redshift - datazone.rs.cluster: <cluster_name:database name>
   >
   >   Per il gruppo di lavoro Serverless Amazon Redshift - datazone.rs.workgroup: <workgroup_name:database_name>
   > - AmazonDataZoneProject: <projectID>

- AmazonDataZoneDomain: <domainID>

Per ulteriori informazioni, vedere Memorizzazione delle credenziali del database in AWS Secrets Manager.

L'utente del database fornito in AWS Secrets Manager deve disporre delle autorizzazioni di super utente.

Fase 4 - Produrre dati per la pubblicazione

La sezione seguente descrive le fasi di produzione dei dati da pubblicare in questo flusso di lavoro.

1. Una volta completato il passaggio 3, nel portale DataZone dati di Amazon, scegli il `SalesDataPublishingProject` progetto, quindi, nel pannello di destra, in Strumenti di analisi, scegli Amazon Redshift. Questo apre l'editor di query di Amazon Redshift utilizzando le credenziali del progetto per l'autenticazione.
2. Per questa procedura dettagliata, stai utilizzando lo script di query Create Table as Select (CTAS) per creare una nuova tabella da pubblicare su Amazon. DataZone Nel tuo editor di query, esegui questo script CTAS per creare una `mkt_sls_table` tabella da pubblicare e rendere disponibile per la ricerca e l'abbonamento.

```
CREATE TABLE mkt_sls_table AS
SELECT 146776932 AS ord_num, 23 AS sales_qty_sld, 23.4 AS wholesale_cost, 45.0 as
 lst_pr, 43.0 as sell_pr, 2.0 as disnt, 12 as ship_mode,13 as warehouse_id, 23 as
 item_id, 34 as ctlg_page, 232 as ship_cust_id, 4556 as bill_cust_id
UNION ALL SELECT 46776931, 24, 24.4, 46, 44, 1, 14, 15, 24, 35, 222, 4551
UNION ALL SELECT 46777394, 42, 43.4, 60, 50, 10, 30, 20, 27, 43, 241, 4565
UNION ALL SELECT 46777831, 33, 40.4, 51, 46, 15, 16, 26, 33, 40, 234, 4563
UNION ALL SELECT 46779160, 29, 26.4, 50, 61, 8, 31, 15, 36, 40, 242, 4562
UNION ALL SELECT 46778595, 43, 28.4, 49, 47, 7, 28, 22, 27, 43, 224, 4555
UNION ALL SELECT 46779482, 34, 33.4, 64, 44, 10, 17, 27, 43, 52, 222, 4556
UNION ALL SELECT 46779650, 39, 37.4, 51, 62, 13, 31, 25, 31, 52, 224, 4551
UNION ALL SELECT 46780524, 33, 40.4, 60, 53, 18, 32, 31, 31, 39, 232, 4563
UNION ALL SELECT 46780634, 39, 35.4, 46, 44, 16, 33, 19, 31, 52, 242, 4557
UNION ALL SELECT 46781887, 24, 30.4, 54, 62, 13, 18, 29, 24, 52, 223, 4561
```

Assicurati che la tabella mkt_sls_table sia stata creata correttamente. Ora hai una risorsa di dati che può essere pubblicata nel DataZone catalogo Amazon.

Fase 5 - Raccolta di metadati da Amazon Redshift

La sezione seguente descrive le fasi di raccolta dei metadati da Amazon Redshift.

1. Una volta completato il passaggio 4, nel portale DataZone dati Amazon, scegli il `SalesDataPublishingProject` progetto, quindi scegli la scheda Dati e quindi scegli Origini dati.
2. Scegli la fonte che è stata creata come parte del processo di creazione dell'ambiente.
3. Scegli Esegui accanto al menu a discesa Azione, quindi scegli il pulsante Aggiorna. Una volta completata l'esecuzione dell'origine dati, le risorse vengono aggiunte all' DataZone inventario Amazon.

Passaggio 6: cura e pubblica la risorsa di dati

La sezione seguente descrive le fasi di cura e pubblicazione della risorsa di dati in questo flusso di lavoro.

1. Una volta completato il passaggio 5, nel portale DataZone dati di Amazon, scegli il `SalesDataPublishingProject` progetto, quindi scegli la scheda Dati, scegli Dati di inventario e individua la `mkt_sls_table` tabella.
2. Apri la pagina dei dettagli dell'`mkt_sls_table`asset per visualizzare i nomi aziendali generati automaticamente. Scegliete l'icona Metadati generati automaticamente per visualizzare i nomi generati automaticamente per le risorse e le colonne. Puoi accettare o rifiutare ogni nome singolarmente o scegliere Accetta tutto per applicare i nomi generati. Facoltativamente, puoi anche aggiungere il modulo di metadati disponibile alla tua risorsa e selezionare i termini del glossario per classificare i dati.
3. Scegliete Pubblica per pubblicare la risorsa. `mkt_sls_table`

Fase 7 - Creazione del progetto per l'analisi dei dati

La sezione seguente descrive le fasi di creazione del progetto per l'analisi dei dati in questo flusso di lavoro.

1. Una volta completato il passaggio 6, nel portale DataZone dati Amazon, scegli Crea progetto.

2. Nella pagina Crea progetto, specifica il nome del progetto, ad esempio, per questo flusso di lavoro, puoi assegnargli un nome MarketingDataAnalysisProject, quindi lasciare invariato il resto dei campi e quindi scegli Crea.

Fase 8 - Creare un ambiente per l'analisi dei dati

La sezione seguente descrive le fasi di creazione di un ambiente per l'analisi dei dati in questo flusso di lavoro.

1. Una volta completato il passaggio 7, nel portale DataZone dati Amazon, scegli il `MarketingDataAnalysisProject` progetto creato nel passaggio precedente, quindi scegli la scheda Ambienti e quindi scegli Aggiungi ambiente.
2. Nella pagina Crea ambiente, specifica quanto segue e poi scegli Crea ambiente.

   - Nome: specifica il nome dell'ambiente. Per questa procedura dettagliata, puoi chiamarla. `Default data warehouse environment`
   - Descrizione: specifica una descrizione per l'ambiente.
   - Profilo ambientale: scegli il profilo DataWarehouseProfiledell'ambiente.
   - Fornisci il nome del cluster Amazon Redshift, il nome del database e l'ARN segreto per il cluster Amazon Redshift in cui sono archiviati i dati.

   > **Note**
   >
   > Assicurati che il tuo segreto in AWS Secrets Manager includa i seguenti tag (chiave/valore):
   >
   > - Per il cluster Amazon Redshift - datazone.rs.cluster: <cluster_name:database name>
   >
   >   Per il gruppo di lavoro Serverless Amazon Redshift - datazone.rs.workgroup: <workgroup_name:database_name>
   > - AmazonDataZoneProject: <projectID>
   > - AmazonDataZoneDomain: <domainID>
   >
   > Per ulteriori informazioni, vedere Memorizzazione delle credenziali del database in AWS Secrets Manager.
   > L'utente del database fornito in AWS Secrets Manager deve disporre delle autorizzazioni di super utente.

- Per questa procedura dettagliata, mantieni invariati gli altri campi.

Passaggio 9: cerca nel catalogo dati e iscriviti ai dati

La sezione seguente descrive i passaggi per la ricerca nel catalogo dati e la sottoscrizione ai dati.

1. Una volta completato il passaggio 8, nel portale DataZone dati di Amazon, cerca gli asset di dati utilizzando parole chiave (ad esempio, «catalogo» o «vendite») nella barra di ricerca del portale dati.

   Se necessario, applica filtri o ordinamenti e, una volta individuato l'asset Product Sales Data, puoi sceglierlo per aprire la pagina dei dettagli della risorsa.
2. Nella pagina dei dettagli della risorsa Product Sales Data, scegli Iscriviti.
3. Nella finestra di dialogo, scegli il tuo progetto consumer dal menu a discesa, fornisci il motivo della richiesta di accesso, quindi scegli Abbonati.

Passaggio 10: approva la richiesta di abbonamento

La sezione seguente descrive i passaggi di approvazione della richiesta di abbonamento in questo flusso di lavoro.

1. Una volta completato il passaggio 9, nel portale DataZone dati di Amazon, scegli il SalesDataPublishingProjectprogetto con cui hai pubblicato la tua risorsa.
2. Scegli la scheda Dati, quindi Dati pubblicati e infine Richieste in arrivo.
3. Scegli il link di richiesta di visualizzazione, quindi scegli Approva.

Fase 11: creare una query e analizzare i dati in Amazon Redshift

Ora che hai pubblicato con successo una risorsa nel DataZone catalogo Amazon e ti sei abbonato, puoi analizzarla.

1. Nel portale DataZone dati di Amazon, nel pannello di destra, fai clic sul link Amazon Redshift. Questo apre l'editor di query di Amazon Redshift utilizzando le credenziali del progetto per l'autenticazione.

2. Ora puoi eseguire una query (select statement) sulla tabella sottoscritta. È possibile fare clic sulla tabella (three-vertical-dots opzione) e scegliere l'anteprima per visualizzare l'istruzione select nella schermata dell'editor. Esegui la query per vedere i risultati.

Amazon DataZone quickstart con script di esempio

La sezione seguente descrive script di esempio che richiamano varie DataZone API Amazon che puoi utilizzare per completare le seguenti attività:

Argomenti

Crea un DataZone dominio Amazon e un portale dati

Puoi utilizzare il seguente script di esempio per creare un DataZone dominio Amazon. Per ulteriori informazioni sui DataZone domini Amazon, consulta DataZone Terminologia e concetti di Amazon.

```
import sys
import boto3

// Initialize datazone client
region = 'us-east-1'
dzclient = boto3.client(service_name='datazone', region_name='us-east-1')

// Create DataZone domain
def create_domain(name):
    return dzclient.create_domain(
        name = name,
        description = "this is a description",
```

```
        domainExecutionRole = "arn:aws:iam::<account>:role/
AmazonDataZoneDomainExecutionRole",
    )
```

Crea un progetto di pubblicazione

Puoi utilizzare il seguente script di esempio per creare un progetto di pubblicazione in Amazon DataZone.

```
// Create Project
def create_project(domainId):
    return dzclient.create_project(
        domainIdentifier = domainId,
        name = "sample-project"
    )
```

Crea un profilo ambientale

Puoi utilizzare i seguenti script di esempio per creare un profilo di ambiente in Amazon DataZone.

Questo payload di esempio viene utilizzato quando viene richiamata l'`CreateEnvironmentProfile`API:

```
Sample Payload
{
    "Content":{
        "project_name": "Admin_project",
        "domain_name": "Drug-Research-and-Development",
        "blueprint_account_region": [
            {
                "blueprint_name": "DefaultDataLake",
                "account_id": ["066535990535",
                "413878397724",
                "676266385322",
                "747721550195",
                "755347404384"
                ],
                "region": ["us-west-2", "us-east-1"]
            },
```

```
            {
                "blueprint_name": "DefaultDataWarehouse",
                "account_id": ["066535990535",
                "413878397724",
                "676266385322",
                "747721550195",
                "755347404384"
                ],
                "region":["us-west-2", "us-east-1"]
            }
        ]
    }
}
```

Questo script di esempio richiama l'API: `CreateEnvironmentProfile`

```
def create_environment_profile(domain_id, project_id, env_blueprints)
        try:
            response = dz.list_environment_blueprints(
                domainIdentifier=domain_id,
                managed=True
            )
            env_blueprints = response.get("items")
            env_blueprints_map = {}
            for i in env_blueprints:
                env_blueprints_map[i["name"]] = i['id']

            print("Environment Blueprint map", env_blueprints_map)
            for i in blueprint_account_region:
                print(i)
                for j in i["account_id"]:
                    for k in i["region"]:
                        print("The env blueprint name is", i['blueprint_name'])
                        dz.create_environment_profile(
                            description='This is a test environment profile created via
 lambda function',
                            domainIdentifier=domain_id,
                            awsAccountId=j,
                            awsAccountRegion=k,

 environmentBlueprintIdentifier=env_blueprints_map.get(i["blueprint_name"]),
```

```
                            name=i["blueprint_name"] + j + k + "_profile",
                            projectIdentifier=project_id
                        )
        except Exception as e:
            print("Failed to created Environment Profile")
            raise e
```

Questo è il payload di output di esempio una volta richiamata l'`CreateEnvironmentProfile`API:

```
{
    "Content":{
        "project_name": "Admin_project",
        "domain_name": "Drug-Research-and-Development",
        "blueprint_account_region": [
            {
                "blueprint_name": "DefaultDataWarehouse",
                "account_id": ["111111111111"],
                "region":["us-west-2"],
                "user_parameters":[
                    {
                        "name": "dataAccessSecretsArn",
                        "value": ""
                    }
                ]
            }
        ]
    }
}
```

Creazione di un ambiente

Puoi utilizzare il seguente script di esempio per creare un ambiente in Amazon DataZone.

```
def create_environment(domain_id, project_id,blueprint_account_region ):
         try:
            #refer to get_domain_id and get_project_id for fetching ids using names.
            sts_client = boto3.client("sts")
            # Get the current account ID
```

```
            account_id = sts_client.get_caller_identity()["Account"]
            print("Fetching environment profile ids")
            env_profile_map = get_env_profile_map(domain_id, project_id)

            for i in blueprint_account_region:
                for j in i["account_id"]:
                    for k in i["region"]:
                        print(" env blueprint name", i['blueprint_name'])
                        profile_name = i["blueprint_name"] + j + k + "_profile"
                        env_name = i["blueprint_name"] + j + k + "_env"
                        description = f'This is environment is created for
{profile_name}, Account {account_id} and region {i["region"]}'
                        try:
                            dz.create_environment(
                                description=description,
                                domainIdentifier=domain_id,

environmentProfileIdentifier=env_profile_map.get(profile_name),
                                name=env_name,
                                projectIdentifier=project_id
                            )
                            print(f"Environment created - {env_name}")
                        except:
                            dz.create_environment(
                                description=description,
                                domainIdentifier=domain_id,

environmentProfileIdentifier=env_profile_map.get(profile_name),
                                name=env_name,
                                projectIdentifier=project_id,
                                userParameters= i["user_parameters"]
                            )
                            print(f"Environment created - {env_name}")
        except Exception as e:
            print("Failed to created Environment")
            raise e
```

Raccogli metadati da AWS Glue

Puoi usare questo script di esempio per raccogliere metadati da AWS Glue. Questo script viene eseguito secondo una pianificazione standard. È possibile recuperare i parametri dallo script di esempio e renderli globali. Recupera il progetto, l'ambiente e l'ID del dominio utilizzando funzioni

standard. L'origine dati AWS Glue viene creata ed eseguita a un'ora standard che può essere aggiornata nella sezione cron dello script.

```
def crcreate_data_source(domain_id, project_id,data_source_name)
        print("Creating Data Source")
        data_source_creation = dz.create_data_source(
            # Define data source : Customize the data source to which you'd like to
 connect
            # define the name of the Data source to create, example: name
 ='TestGlueDataSource'
            name=data_source_name,
            # give a description for the datasource (optional), example:
 description='This is a dorra test for creation on DZ datasources'
            description=data_source_description,
            # insert the domain identifier corresponding to the domain to which the
 datasource will belong, example: domainIdentifier= 'dzd_6f3gst5jjmrrmv'
            domainIdentifier=domain_id,
            # give environment identifier , example: environmentIdentifier=
 '3weyt6hhn8qcvb'
            environmentIdentifier=environment_id,
            # give corresponding project identifier, example: projectIdentifier=
 '6tl4csoyrg16ef',
            projectIdentifier=project_id,
            enableSetting="ENABLED",
            # publishOnImport used to select whether assets are added to the inventory
 and/or discovery catalog .
            # publishOnImport = True : Assets will be added to project's inventory as
 well as published to the discovery catalog
            # publishOnImport = False : Assets will only be added to project's
 inventory.
            # You can later curate the metadata of the assets and choose subscription
 terms to publish them from the inventory to the discovery catalog.
            publishOnImport=False,
            # Automated business name generation : Use AI to automatically generate
 metadata for assets as they are published or updated by this data source run.
            # Automatically generated metadata can be be approved, rejected, or edited
 by data publishers.
            # Automatically generated metadata is badged with a small icon next to the
 corresponding metadata field.
            recommendation={"enableBusinessNameGeneration": True},
            type="GLUE",
            configuration={
```

```
                "glueRunConfiguration": {
                    "dataAccessRole": "arn:aws:iam::"
                    + account_id
                    + ":role/service-role/AmazonDataZoneGlueAccess-"
                    + current_region
                    + "-"
                    + domain_id
                    + "",
                    "relationalFilterConfigurations": [
                        {
                            #
                            "databaseName": glue_database_name,
                            "filterExpressions": [
                                {"expression": "*", "type": "INCLUDE"},
                            ],
                            #    "schemaName": "TestSchemaName",
                        },
                    ],
                },
            },
            # Add metadata forms to the data source (OPTIONAL).
            # Metadata forms will be automatically applied to any assets that are
 created by the data source.
            # assetFormsInput=[
            #     {
            #         "content": "string",
            #         "formName": "string",
            #         "typeIdentifier": "string",
            #         "typeRevision": "string",
            #     },
            # ],
            schedule={
                "schedule": "cron(5 20 * * ? *)",
                "timezone": "UTC",
            },
        )
        # This is a suggested syntax to return values
        #       return_values["data_source_creation"] = data_source_creation["items"]
        print("Data Source Created")


//This is the sample response payload after the CreateDataSource API is invoked:

{
```

```
    "Content":{
        "project_name": "Admin",
        "domain_name": "Drug-Research-and-Development",
        "env_name": "GlueEnvironment",
        "glue_database_name": "test",
        "data_source_name" : "test",
        "data_source_description" : "This is a test data source"
    }
}
```

Cura e pubblica una risorsa di dati

Puoi utilizzare i seguenti script di esempio per curare e pubblicare asset di dati in Amazon. DataZone

Puoi utilizzare il seguente script per creare tipi di modulo personalizzati:

```
def create_form_type(domainId, projectId):
    return dzclient.create_form_type(
        domainIdentifier = domainId,
        name = "customForm",
        model = {
            "smithy": "structure customForm { simple: String }"
        },
        owningProjectIdentifier = projectId,
        status = "ENABLED"
    )
```

È possibile utilizzare il seguente script di esempio per creare tipi di risorse personalizzati:

```
def create_custom_asset_type(domainId, projectId):
    return dzclient.create_asset_type(
        domainIdentifier = domainId,
        name = "userCustomAssetType",
        formsInput = {
            "Model": {
                "typeIdentifier": "customForm",
                "typeRevision": "1",
                "required": False
```

```
            }
        },
        owningProjectIdentifier = projectId,
    )
```

È possibile utilizzare il seguente script di esempio per creare risorse personalizzate:

```
def create_custom_asset(domainId, projectId):
    return dzclient.create_asset(
        domainIdentifier = domainId,
        name = 'custom asset',
        description = "custom asset",
        owningProjectIdentifier = projectId,
        typeIdentifier = "userCustomAssetType",
        formsInput = [
            {
                "formName": "UserCustomForm",
                "typeIdentifier": "customForm",
                "content": "{\"simple\":\"sample-catalogId\"}"
            }
        ]
    )
```

È possibile utilizzare il seguente script di esempio per creare un glossario:

```
def create_glossary(domainId, projectId):
    return dzclient.create_glossary(
        domainIdentifier = domainId,
        name = "test7",
        description = "this is a test glossary",
        owningProjectIdentifier = projectId
    )
```

È possibile utilizzare il seguente script di esempio per creare un termine di glossario:

```
def create_glossary_term(domainId, glossaryId):
```

```
    return dzclient.create_glossary_term(
        domainIdentifier = domainId,
        name = "soccer",
        shortDescription = "this is a test glossary",
        glossaryIdentifier = glossaryId,
    )
```

È possibile utilizzare il seguente script di esempio per creare una risorsa utilizzando un tipo di risorsa definito dal sistema:

```
def create_asset(domainId, projectId):
    return dzclient.create_asset(
        domainIdentifier = domainId,
        name = 'sample asset name',
        description = "this is a glue table asset",
        owningProjectIdentifier = projectId,
        typeIdentifier = "amazon.datazone.GlueTableAssetType",
        formsInput = [
            {
                "formName": "GlueTableForm",
                "content": "{\"catalogId\":\"sample-catalogId\",\"columns\":
[{\"columnDescription\":\"sample-columnDescription\",\"columnName\":\"sample-
columnName\",\"dataType\":\"sample-dataType\",\"lakeFormationTags\":{\"sample-
key1\":\"sample-value1\",\"sample-key2\":\"sample-value2\"}}],\"compressionType\":
\"sample-compressionType\",\"lakeFormationDetails\":{\"lakeFormationManagedTable
\":false,\"lakeFormationTags\":{\"sample-key1\":\"sample-value1\",\"sample-key2\":
\"sample-value2\"}},\"primaryKeys\":[\"sample-Key1\",\"sample-Key2\"],\"region\":
\"us-east-1\",\"sortKeys\":[\"sample-sortKey1\"],\"sourceClassification\":\"sample-
sourceClassification\",\"sourceLocation\":\"sample-sourceLocation\",\"tableArn\":
\"sample-tableArn\",\"tableDescription\":\"sample-tableDescription\",\"tableName\":
\"sample-tableName\"}"
            }
        ]
    )
```

Potete utilizzare il seguente script di esempio per creare una revisione di una risorsa e allegare un termine di glossario:

```
def create_asset_revision(domainId, assetId):
    return dzclient.create_asset_revision(
        domainIdentifier = domainId,
        identifier = assetId,
        name = 'glue table asset 7',
        description = "glue table asset description update",
        formsInput = [
            {
                "formName": "GlueTableForm",
                "content": "{\"catalogId\":\"sample-catalogId\",\"columns\":
[{\"columnDescription\":\"sample-columnDescription\",\"columnName\":\"sample-
columnName\",\"dataType\":\"sample-dataType\",\"lakeFormationTags\":{\"sample-
key1\":\"sample-value1\",\"sample-key2\":\"sample-value2\"}}],\"compressionType\":
\"sample-compressionType\",\"lakeFormationDetails\":{\"lakeFormationManagedTable
\":false,\"lakeFormationTags\":{\"sample-key1\":\"sample-value1\",\"sample-key2\":
\"sample-value2\"}},\"primaryKeys\":[\"sample-Key1\",\"sample-Key2\"],\"region\":
\"us-east-1\",\"sortKeys\":[\"sample-sortKey1\"],\"sourceClassification\":\"sample-
sourceClassification\",\"sourceLocation\":\"sample-sourceLocation\",\"tableArn\":
\"sample-tableArn\",\"tableDescription\":\"sample-tableDescription\",\"tableName\":
\"sample-tableName\"}"
            }
        ],
        glossaryTerms = ["<glossaryTermId:>"]
    )
```

È possibile utilizzare il seguente script di esempio per pubblicare una risorsa:

```
def publish_asset(domainId, assetId):
    return dzclient.create_listing_change_set(
        domainIdentifier = domainId,
        entityIdentifier = assetId,
        entityType = "ASSET",
        action = "PUBLISH",
    )
```

Cerca nel catalogo dati e sottoscrivi i dati

È possibile utilizzare i seguenti script di esempio per effettuare ricerche nel catalogo dati e sottoscrivere i dati:

```
def search_asset(domainId, projectId, text):
    return dzclient.search(
        domainIdentifier = domainId,
        owningProjectIdentifier = projectId,
        searchScope = "ASSET",
        searchText = text,
    )
```

Puoi utilizzare il seguente script di esempio per ottenere l'ID dell'inserzione per la risorsa:

```
def search_listings(domainId, assetName, assetId):
    listings = dzclient.search_listings(
        domainIdentifier=domainId,
        searchText=assetName,
        additionalAttributes=["FORMS"]
    )

    assetListing = None
    for listing in listings['items']:
        if listing['assetListing']['entityId'] == assetId:
            assetListing = listing

    return listing['assetListing']['listingId']
```

Puoi utilizzare i seguenti script di esempio per creare una richiesta di abbonamento utilizzando l'ID dell'inserzione:

```
create_subscription_response = def create_subscription_request(domainId, projectId,
 listingId):
    return dzclient.create_subscription_request(
        subscribedPrincipals=[{
            "project": {
                "identifier": projectId
            }
        }],
        subscribedListings=[{
            "identifier": listingId
```

```
        }],
        requestReason="Give request reason here."
    )
```

Utilizzando `create_subscription_response` quanto sopra, ottieni e poi accetta/approva l' `subscription_request_id`abbonamento utilizzando il seguente script di esempio:

```
subscription_request_id = create_subscription_response["id"]

def accept_subscription_request(domainId, subscriptionRequestId):
    return dzclient.accept_subscription_request(
        domainIdentifier=domainId,
        identifier=subscriptionRequestId
    )
```

Altri script di esempio utili

Puoi utilizzare i seguenti script di esempio per completare varie attività mentre lavori con i tuoi dati in Amazon DataZone.

Usa il seguente script di esempio per elencare i DataZone domini Amazon esistenti:

```
def list_domains():
    datazone = boto3.client('datazone')
    response = datazone.list_domains(status='AVAILABLE')
    [print("%12s | %16s | %12s | %52s" % (item['id'], item['name'],
 item['managedAccountId'], item['portalUrl'])) for item in response['items']]
    return
```

Usa il seguente script di esempio per elencare i DataZone progetti Amazon esistenti:

```
def list_projects(domain_id):
    datazone = boto3.client('datazone')
    response = datazone.list_projects(domainIdentifier=domain_id)
    [print("%12s | %16s " % (item['id'], item['name'])) for item in response['items']]
```

```
    return
```

Utilizza il seguente script di esempio per elencare i moduli di DataZone metadati Amazon esistenti:

```
def list_metadata_forms(domain_id):
    datazone = boto3.client('datazone')
    response = datazone.search_types(domainIdentifier=domain_id,
        managed=False,
        searchScope='FORM_TYPE')
    [print("%16s | %16s | %3s | %8s" % (item['formTypeItem']['name'],
 item['formTypeItem']['owningProjectId'],item['formTypeItem']['revision'],
 item['formTypeItem']['status'])) for item in response['items']]
    return
```

Gestione dei DataZone domini Amazon e dell'accesso degli utenti

Argomenti

Crea domini

> **Note**
>
> Se utilizzi Amazon DataZone con AWS Identity Center per fornire l'accesso a utenti e gruppi SSO, attualmente il tuo DataZone dominio Amazon deve trovarsi nella stessa AWS regione dell'istanza di AWS Identity Center.

Amazon DataZone, un dominio è un'entità organizzativa per connettere tra loro risorse, utenti e i loro progetti. Per ulteriori informazioni, consulta DataZone Terminologia e concetti di Amazon.

Per creare un DataZone dominio Amazon, devi assumere un ruolo IAM nell'account con autorizzazioni amministrative. Configura le autorizzazioni IAM necessarie per utilizzare la console di DataZone gestione Amazonper ottenere le autorizzazioni minime necessarie per creare un dominio.

Amazon ha bisogno di ruoli IAM aggiuntivi DataZone per eseguire azioni per conto degli utenti del dominio con una configurazione predefinita. Puoi creare questi ruoli IAM in anticipo o chiedere ad Amazon di DataZone crearli per te. Se desideri che Amazon DataZone crei questi ruoli IAM per te durante il processo di creazione del dominio, per la creazione del dominio devi assumere un ruolo IAM con autorizzazioni per la creazione di ruoli. Per informazioni,

consulta Crea una policy personalizzata per le autorizzazioni IAM per abilitare la creazione semplificata di ruoli da parte della console di DataZone servizio Amazon . A seconda delle tue scelte di creazione del dominio, Amazon DataZone creerà per te fino a quattro nuovi ruoli IAM: AmazonDataZoneDomainExecutionRoleAmazonDataZoneGlueManageAccessRole, AmazonDataZoneRedshiftManageAccessRole, e AmazonDataZoneProvisioningRole.

Completa la seguente procedura per creare un DataZone dominio Amazon.

1. Accedi alla DataZone console Amazon all'indirizzo https://console.aws.amazon.com/datazone e utilizza il selettore della regione nella barra di navigazione in alto per scegliere la AWS regione appropriata.
2. Scegli Crea dominio e fornisci i valori per i seguenti campi:

   - Nome: specifica un nome descrittivo per il dominio. Una volta creato il dominio, questo nome non può essere modificato.
   - Descrizione: (opzionale) specifica una descrizione del dominio.
   - Crittografia dei dati: il DataZone dominio Amazon, i metadati e i dati di reporting vengono crittografati dal AWS Key Management Service (KMS) utilizzando una chiave specifica per Amazon. DataZone Utilizza questo campo per specificare se desideri utilizzare una chiave di AWS proprietà o scegliere una chiave AWS KMS diversa.

     Per ulteriori informazioni sull'utilizzo delle chiavi gestite dai clienti, consultaCrittografia dei dati a riposo per Amazon DataZone. Se utilizzi la tua chiave KMS per la crittografia dei dati, devi includere la seguente dichiarazione come predefinitaAmazonDataZoneDomainExecutionRole.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "Statement1",
      "Effect": "Allow",
      "Action": [
        "kms:Decrypt",
        "kms:DescribeKey",
        "kms:GenerateDataKey"
      ],
      "Resource": [
        "*"
      ]
```

```
    }
  ]
}
```

- Accesso al servizio: scegli se consentire ad Amazon di DataZone crearne e utilizzarne uno nuovo DomainExecutionRoleper te o scegli un ruolo IAM esistente.
- Configurazione rapida: (opzionale) seleziona questa casella per iniziare più rapidamente facendo DataZone configurare ad Amazon il tuo account per il consumo e la pubblicazione dei dati. Amazon DataZone creerà tre ruoli IAM per il provisioning, l'acquisizione e la gestione dell'accesso alle risorse AWS Glue e Amazon Redshift, creerà un nuovo bucket Amazon S3, creerà un DataZone progetto Amazon amministrativo e creerà profili di ambiente per i blueprint predefiniti del data lake e del data warehouse.
- Tag: (facoltativo) specifica i AWS tag (coppie di chiavi e valori) per il dominio.
- Una volta creato correttamente il dominio, il browser dovrebbe essere aggiornato per visualizzare la pagina dei dettagli del nuovo DataZone dominio Amazon.

Modifica i domini

In Amazon DataZone, un dominio è un'entità organizzativa per connettere tra loro risorse, utenti e i loro progetti. Per ulteriori informazioni, consulta DataZone Terminologia e concetti di Amazon.

Dopo aver creato un DataZone dominio Amazon, puoi successivamente modificare il dominio per: modificare la descrizione, abilitare IAM Identity Center e aggiungere, modificare o rimuovere le chiavi dei tag e i relativi valori. Per modificare un DataZone dominio Amazon, devi assumere un ruolo IAM nell'account con autorizzazioni amministrative. Configura le autorizzazioni IAM necessarie per utilizzare la console di DataZone gestione Amazonper ottenere le autorizzazioni minime necessarie per modificare un dominio.

Per modificare un dominio, completa i seguenti passaggi:

1. Accedi alla Console di AWS gestione e apri la DataZone console Amazon all'indirizzo https://console.aws.amazon.com/datazone.
2. Scegli Visualizza domini e scegli il nome del dominio dall'elenco. Il nome è un collegamento ipertestuale.
3. Nella pagina dei dettagli del dominio, scegli Modifica.
4. • Modifica la descrizione.

- Imposta le impostazioni di IAM Identity Center. Scopri di più su queste impostazioni in[Configurazione di AWS IAM Identity Center per Amazon DataZone](#).
- Aggiungi, modifica o rimuovi le chiavi Tag e i relativi valori.

5. Dopo aver apportato le modifiche, scegli Aggiorna dominio.

Elimina i domini

In Amazon DataZone, un dominio è un'entità organizzativa per connettere tra loro risorse, utenti e i loro progetti. Per ulteriori informazioni, consulta [DataZone Terminologia e concetti di Amazon](#).

L'operazione di eliminazione di un dominio è definitiva. L'eliminazione rimuove irrevocabilmente ogni DataZone entità Amazon, incluse fonti di dati, progetti, ambienti, risorse, glossari e moduli di metadati. L'eliminazione non elimina DataZone AWS le risorse non Amazon che Amazon DataZone potrebbe averti aiutato a creare, come ruoli IAM, bucket S3, database AWS Glue e concessioni di abbonamento tramite o Redshift. LakeFormation Se non hai più bisogno di queste risorse, eliminale nel rispettivo servizio. AWS

Per impedire a qualcuno di eliminare un dominio in modo dannoso, l'eliminazione di un dominio richiede autorizzazioni amministrative IAM per Amazon DataZone, che puoi configurare con IAM. Per evitare che qualcuno elimini accidentalmente un dominio, l'eliminazione di un dominio richiede una parola di conferma (nella console Amazon DataZone).

Per eliminare un dominio, completa i seguenti passaggi:

1. Accedi alla Console di AWS gestione e apri la DataZone console Amazon all'[indirizzo https://console.aws.amazon.com/datazone](#).
2. Scegli Visualizza domini e scegli il nome del dominio dall'elenco. Il nome è un collegamento ipertestuale.
3. Scegliete Elimina e controllate gli avvisi informativi.
4. Digita il testo richiesto per confermare di aver compreso questi avvisi. Scegli Elimina.

> **Important**
>
> L'eliminazione del dominio è un'azione irrevocabile che non può essere annullata né da te né da parte tua. AWS

> **Note**
>
> Quando tu o gli utenti del tuo dominio create un ambiente in un progetto, Amazon DataZone crea AWS risorse nel tuo dominio o negli account associati per fornire funzionalità a te e agli utenti del dominio. Di seguito è riportato l'elenco delle AWS risorse che Amazon DataZone può creare per i progetti nel tuo dominio, insieme al nome predefinito. L'eliminazione di un dominio non elimina nessuna di queste AWS risorse dai tuoi AWS account.
>
> - <environmentId>Ruoli IAM: datazone_usr_.
> - <environmentName>Database Glue: (1) <environmentName>_pub_db-*, (2) _sub_db-*. Se esisteva già un database con questo nome, Amazon DataZone aggiungerà l'ID dell'ambiente.
> - <environmentName>Gruppi di lavoro Athena: -*. Se esisteva già un gruppo di lavoro con questo nome, Amazon DataZone aggiungerà l'ID dell'ambiente.
> - CloudWatch gruppo di log: datazone_ <environmentId>

Abilita IAM Identity Center per Amazon DataZone

> **Note**
>
> Per completare questa procedura, devi avere AWS IAM Identity Center abilitato nella stessa AWS regione del tuo DataZone dominio Amazon.

Puoi fornire a utenti e gruppi SSO l'accesso al tuo portale DataZone dati Amazon utilizzando AWS IAM Identity Center. Al termineConfigurazione di AWS IAM Identity Center per Amazon DataZone, puoi consentire ai tuoi utenti e gruppi SSO di accedere al portale dati del tuo DataZone dominio Amazon.

Per abilitare AWS IAM Identity Center per l'uso con il tuo DataZone dominio Amazon, devi assumere un ruolo IAM nell'account con autorizzazioni amministrative. Configura le autorizzazioni IAM necessarie per utilizzare la console di DataZone gestione Amazone Crea una policy personalizzata per le autorizzazioni IAM per abilitare la creazione semplificata di ruoli da parte della console di DataZone servizio Amazon per ottenere le autorizzazioni minime necessarie per abilitare IAM Identity Center per l'utilizzo con Amazon DataZone.

Completa la seguente procedura per abilitare AWS IAM Identity Center for Amazon DataZone.

1. Accedi alla console di AWS gestione e apri la DataZone console all'indirizzo https://console.aws.amazon.com/datazone.
2. Seleziona Visualizza domini e scegli il nome del dominio dall'elenco. Il nome è un collegamento ipertestuale.
3. Nella pagina dei dettagli del dominio, scegli Modifica.
   - Seleziona la casella di controllo Abilita gli utenti in IAM Identity Center.
   - Scegli tra le due modalità di assegnazione degli utenti. Una volta che il dominio è stato aggiornato con la selezione, non può essere modificato in seguito.
     - Con l'assegnazione implicita degli utenti, qualsiasi utente aggiunto alla tua directory IAM Identity Center può accedere al tuo dominio Amazon DataZone .
     - Con l'assegnazione esplicita degli utenti, aggiungerai utenti o gruppi specifici dalla tua directory IAM Identity Center per fornire loro l'accesso al tuo dominio Amazon DataZone . Aggiungerai e rimuoverai questi utenti e gruppi in un secondo momento nella DataZone Console Amazon.
4. Una volta che sei soddisfatto della selezione, scegli Aggiorna dominio.

Disattiva IAM Identity Center per Amazon DataZone

La disabilitazione di AWS IAM Identity Center per un DataZone dominio Amazon rimuoverà l'accesso per tutti gli utenti SSO.

> **Note**
>
> La disabilitazione di IAM Identity Center non interromperà la fatturazione per gli utenti SSO. Per interrompere la fatturazione degli utenti SSO, devi disattivarli nel tuo dominio. La fatturazione continua fino alla fine del mese in cui un utente viene disattivato. Per disattivare gli utenti, consulta. Gestisci gli utenti nella DataZone console Amazon

Puoi fornire a utenti e gruppi SSO l'accesso al tuo portale DataZone dati Amazon utilizzando AWS IAM Identity Center. Se hai abilitato AWS IAM Identity Center for Amazon DataZone, puoi successivamente disabilitare l'accesso per tutti gli utenti.

Per disabilitare AWS IAM Identity Center per l'utilizzo con il tuo DataZone dominio Amazon, devi assumere un ruolo IAM nell'account con autorizzazioni amministrative. Configura le autorizzazioni IAM necessarie per utilizzare la console di DataZone gestione Amazone Crea una policy personalizzata per le autorizzazioni IAM per abilitare la creazione semplificata di ruoli da parte della console di DataZone servizio Amazon per ottenere le autorizzazioni minime necessarie per disabilitare l'uso di IAM Identity Center con Amazon DataZone.

Completa la seguente procedura per disabilitare AWS IAM Identity Center for Amazon DataZone.

1. Accedi alla console di AWS gestione e apri la DataZone console all'indirizzo https://console.aws.amazon.com/datazone.
2. Seleziona Visualizza domini e scegli il nome del dominio dall'elenco. Il nome è un collegamento ipertestuale.
3. <regionName><accountId><domainName>Copia l'Amazon Resource Name (ARN) per il tuo dominio, che inizia con arn:aws:datazone: ::domain/.
4. Apri la console IAM Identity Center all'indirizzo https://console.aws.amazon.com/singlesignon/.
5. Selezionare Applications (Applicazioni).
6. Scegli il dominio per il quale desideri disabilitare AWS IAM Identity Center, che di conseguenza rimuoverà l'accesso al portale dati del dominio per tutti gli utenti SSO. Puoi utilizzare il menu Filtro e la casella di ricerca per filtrare l'elenco delle applicazioni.
7. Dal menu Azioni, scegli Disabilita.
8. Gli utenti SSO perderanno l'accesso al DataZone dominio Amazon.
9. Per riattivare AWS IAM Identity Center per il DataZone dominio Amazon, scegli il dominio per il quale desideri riattivare AWS IAM Identity Center e, dal menu Azioni, scegli Abilita.

Gestisci gli utenti nella DataZone console Amazon

I tuoi utenti possono accedere al portale DataZone dati di Amazon utilizzando AWS le proprie credenziali o credenziali Single Sign-On (SSO). Per gestire gli utenti nella DataZone console Amazon per un DataZone dominio Amazon, devi assumere un ruolo IAM nell'account con autorizzazioni amministrative. Configura le autorizzazioni IAM necessarie per utilizzare la console di DataZone gestione Amazonper ottenere le autorizzazioni minime necessarie per gestire gli utenti nella DataZone console Amazon.

Argomenti

- Gestisci i ruoli e gli utenti IAM
- Gestisci gli utenti SSO
- Gestisci i gruppi SSO

Gestisci i ruoli e gli utenti IAM

I ruoli e gli utenti IAM vengono creati utilizzando AWS Identity and Access Management (IAM) e ottengono l'accesso ai tuoi domini DataZone Amazon tramite le autorizzazioni ad essi associate tramite policy. Per ulteriori informazioni, consulta Configura le autorizzazioni IAM necessarie per utilizzare il portale DataZone dati Amazon. Puoi visualizzare l'elenco dei ruoli e degli utenti IAM che hanno attivato l'abbonamento al DataZone dominio Amazon, disattivare il loro accesso e attivare il loro accesso se precedentemente disattivato.

1. Accedi alla console di AWS gestione e apri la DataZone console all'indirizzo https://console.aws.amazon.com/datazone.
2. Seleziona Visualizza domini e scegli il nome del dominio dall'elenco. Il nome è un collegamento ipertestuale.
3. Nella pagina dei dettagli del dominio, scegli Gestione utenti.
4. Per il tipo di utente, seleziona Utenti IAM per visualizzare l'elenco corrente di utenti e ruoli IAM attivati e disattivati.
    - La colonna Name mostra l'arn dell'utente o del ruolo IAM.
    - La colonna Status mostra lo stato corrente dell'utente o del ruolo IAM nel dominio.
        - Attivato significa che l'utente o il ruolo IAM ha chiamato un'API, emesso un comando (tramite Command Line Interface) o ha effettuato l'accesso DataZone al portale Amazon per il tuo dominio e ti viene addebitato l'abbonamento dell'utente.
        - Disattivato significa che l'accesso dell'utente o del ruolo IAM al tuo DataZone dominio Amazon è bloccato.
5. Per disattivare un utente o un ruolo IAM attualmente attivato, seleziona la casella accanto all'utente e seleziona Disattiva dal menu Azioni. L'utente perderà l'accesso al DataZone dominio Amazon. La fatturazione per l'utente terminerà alla fine del mese solare corrente.
6. Per attivare un utente o un ruolo IAM attualmente disattivato, seleziona la casella accanto all'utente e seleziona Attiva dal menu Azioni. L'utente avrà accesso al DataZone dominio Amazon se l'utente o il ruolo IAM dispone delle autorizzazioni appropriate. La fatturazione per l'utente ricomincerà.

Gestisci gli utenti SSO

Gli utenti SSO vengono creati o sincronizzati con il tuo provider di identità in AWS IAM Identity Center. Per ulteriori informazioni, consulta Configurazione di AWS IAM Identity Center per Amazon DataZone e Abilita IAM Identity Center per Amazon DataZone per abilitare e configurare AWS IAM Identity Center for Amazon DataZone. Puoi visualizzare l'elenco degli utenti SSO assegnati al dominio, aggiungere utenti SSO e rimuovere utenti SSO.

1. Accedi alla console di AWS gestione e apri la DataZone console all'indirizzo https://console.aws.amazon.com/datazone.
2. Seleziona Visualizza domini e scegli il nome del dominio dall'elenco. Il nome è un collegamento ipertestuale.
3. Nella pagina dei dettagli del dominio, scorri verso il basso e scegli Gestione utenti.
4. Per tipo di utente, seleziona Utenti SSO per visualizzare l'elenco corrente degli utenti SSO.
   - La colonna Nome mostra il nome dell'utente SSO.
   - La colonna Status mostra lo stato corrente dell'utente SSO nel dominio.
     - Assegnato significa che l'utente SSO è stato assegnato in modo esplicito al dominio. Di conseguenza, l'utente ha accesso ad Amazon DataZone. Questo stato viene utilizzato solo quando la modalità provider di identità del dominio è impostata sull'assegnazione esplicita.
     - Attivato significa che l'utente SSO ha effettuato l'accesso DataZone al portale Amazon per il dominio e ti viene addebitato l'abbonamento dell'utente. L'attivazione avviene automaticamente.
     - Disattivato significa che l'accesso dell'utente SSO è bloccato al portale dati del dominio. La fatturazione per l'utente è terminata alla fine del mese in cui l'accesso era stato disattivato.
     - Rimosso significa che l'utente SSO era stato precedentemente assegnato al dominio, ma rimosso prima dell'accesso.
5. Aggiungi utenti SSO selezionando Aggiungi e aggiungi utenti. Questa opzione non è disponibile se il dominio è impostato sull'assegnazione implicita degli utenti, il che significa che tutti gli utenti del pool di identità hanno accesso al dominio Amazon DataZone .
   - Nella pagina Aggiungi utenti, cerca gli alias degli utenti che desideri aggiungere. Sotto la casella di ricerca verrà visualizzato un elenco con potenziali corrispondenze.
   - Scegli l'utente che desideri aggiungere. Il loro alias apparirà sotto forma di chip sotto la casella di ricerca.

- Quando sei soddisfatto dell'elenco di utenti che desideri aggiungere, scegli Aggiungi utente/i.
- Gli utenti vengono assegnati al DataZone dominio Amazon con lo stato Assegnato.
- Quando l'utente accede per la prima volta al portale dati del dominio, lo stato cambierà automaticamente in Attivato e inizierai a ricevere la fatturazione dell'abbonamento dell'utente.

6. Rimuovi un utente SSO assegnato selezionando l'utente e scegliendo Disabilita dal menu Azioni. Di conseguenza, l'utente perderà l'accesso al DataZone dominio Amazon. Lo stato dell'utente verrà visualizzato come Rimosso. Questa opzione non è disponibile se il dominio è impostato sull'assegnazione implicita dell'utente.
7. Disattiva un utente SSO attivato selezionando l'utente e scegliendo Disattiva dal menu Azioni. Di conseguenza, l'accesso dell'utente al DataZone dominio Amazon verrà perso e bloccato. La fatturazione dell'abbonamento dell'utente continuerà fino alla fine del mese. Lo stato dell'utente verrà visualizzato come Disattivato.
8. Attiva un utente SSO disattivato selezionando l'utente e scegliendo Attiva dal menu Azioni. Di conseguenza, l'utente riotterrà l'accesso al DataZone dominio Amazon. La fatturazione verrà avviata immediatamente. Quello dell'utente verrà visualizzato come Attivato.

Gestisci i gruppi SSO

I gruppi SSO vengono creati o sincronizzati con il tuo provider di identità in AWS IAM Identity Center. Per ulteriori informazioni, consulta Configurazione di AWS IAM Identity Center per Amazon DataZone e Abilita IAM Identity Center per Amazon DataZone per abilitare e configurare AWS IAM Identity Center for Amazon DataZone. Puoi visualizzare l'elenco dei gruppi SSO assegnati al dominio, aggiungere gruppi SSO e rimuovere gruppi SSO.

1. Accedi alla console di AWS gestione e apri la DataZone console all'indirizzo https://console.aws.amazon.com/datazone.
2. Seleziona Visualizza domini e scegli il nome del dominio dall'elenco. Il nome è un collegamento ipertestuale.
3. Nella pagina dei dettagli del dominio, scorri verso il basso e scegli Gestione utenti.
4. Per il tipo di utente, seleziona Gruppi SSO per visualizzare l'elenco corrente dei gruppi SSO.

- La colonna Nome mostra il nome del gruppo SSO.
- La colonna Status mostra lo stato attuale del gruppo SSO nel dominio.

- Assegnato significa che il gruppo SSO è stato assegnato in modo esplicito al dominio. Di conseguenza, tutti gli utenti del gruppo hanno accesso al portale dati del dominio (a meno che l'utente non sia disattivato).
- Non assegnato significa che il gruppo SSO è stato rimosso dal dominio. Gli utenti del gruppo non hanno accesso al portale dati del dominio tramite la loro appartenenza a questo gruppo.

5. Aggiungi gruppi SSO selezionando Aggiungi e Aggiungi gruppi. Questa opzione non è disponibile se il dominio è impostato sull'assegnazione implicita degli utenti, il che significa che tutti gli utenti del pool di identità hanno accesso al DataZone dominio Amazon indipendentemente dall'appartenenza al gruppo.

   - Nella pagina Aggiungi gruppi, cerca gli alias dei gruppi che desideri aggiungere. Sotto la casella di ricerca verrà visualizzato un elenco con potenziali corrispondenze.
   - Scegli il gruppo che desideri aggiungere. Il loro alias apparirà sotto forma di chip sotto la casella di ricerca.
   - Quando sei soddisfatto dell'elenco dei gruppi che desideri aggiungere, scegli Aggiungi gruppo/i.
   - I gruppi vengono assegnati al DataZone dominio Amazon con lo stato Assegnato.
   - Quando un membro del gruppo accede al portale dati del dominio, lo stato cambierà automaticamente in Attivato e inizierai a ricevere la fatturazione dell'abbonamento dell'utente.

6. Rimuovi un gruppo SSO assegnato selezionando il gruppo e scegliendo Annulla assegnazione dal menu Azioni. Di conseguenza, il gruppo perderà l'accesso al DataZone dominio Amazon. Lo stato del gruppo verrà visualizzato come Non assegnato. Gli utenti che hanno ottenuto l'accesso ad Amazon DataZone tramite l'iscrizione a questo gruppo perderanno l'accesso. Questa opzione non è disponibile se il dominio è impostato sull'assegnazione implicita dell'utente. Per interrompere la fatturazione degli utenti il cui accesso viene rimosso annullando l'assegnazione del gruppo, dovrai quindi selezionare e disattivare manualmente i relativi profili utente.

Gestione delle autorizzazioni degli utenti nel portale DataZone dati Amazon

Nell'attuale versione di Amazon DataZone, il meccanismo di autorizzazione predefinito consente a tutti gli utenti autenticati (IAM e SSO) dei DataZone domini Amazon di creare progetti, creare entità all'interno dei progetti e condurre ricerche. I membri del progetto devono comunque rispettare le

autorizzazioni loro concesse in base ai ruoli designati di proprietario del progetto o collaboratore del progetto.

Lavorare con i blueprint DataZone integrati di Amazon

Un modello con cui viene creato un ambiente definisce quali strumenti e servizi i membri del progetto a cui appartiene l'ambiente possono utilizzare mentre lavorano con le risorse nel DataZone catalogo Amazon. Nell'attuale versione di Amazon DataZone, sono presenti i seguenti progetti integrati:

- Blueprint Data Lake
- Progetto di data warehouse
- SageMaker Progetto Amazon

Argomenti

Abilita i blueprint integrati nell' AWS account che possiede il dominio Amazon DataZone

Un modello con cui viene creato un ambiente definisce quali strumenti e servizi i membri del progetto a cui appartiene l'ambiente possono utilizzare mentre lavorano con le risorse nel DataZone catalogo Amazon.

Nell'attuale versione di Amazon DataZone, ci sono diversi blueprint integrati: data lake blueprint, data warehouse blueprint e Amazon blueprint. SageMaker

- Il modello Data Lake contiene la definizione per il lancio e la configurazione di un set di servizi (AWS Glue, AWS Lake Formation, Amazon Athena) per pubblicare e utilizzare le risorse del data lake nel catalogo Amazon. DataZone
- Il modello di data warehouse contiene la definizione per il lancio e la configurazione di un set di servizi (Amazon Redshift) per pubblicare e utilizzare le risorse Amazon Redshift nel catalogo Amazon. DataZone
- Amazon SageMaker blueprint contiene la definizione per il lancio e la configurazione di un set di servizi (Amazon SageMaker Studio) per pubblicare e utilizzare le SageMaker risorse Amazon nel catalogo Amazon. DataZone

Per ulteriori informazioni, consulta DataZone Terminologia e concetti di Amazon.

Durante la creazione di un DataZone dominio Amazon, hai la possibilità di scegliere la configurazione rapida che abilita automaticamente il data lake predefinito e i blueprint predefiniti integrati nel data warehouse come parte del processo di creazione del dominio. La configurazione rapida crea anche profili di ambiente e ambienti predefiniti per te utilizzando questi blueprint integrati.

Se non scegli la configurazione rapida come parte della creazione del tuo DataZone dominio Amazon, puoi utilizzare la procedura seguente per abilitare i blueprint integrati disponibili nell' AWS account che ospita questo DataZone dominio Amazon. È necessario abilitare questi blueprint integrati prima di poterli utilizzare per creare profili e ambienti ambientali in questo dominio.

Per abilitare i blueprint integrati in un DataZone dominio Amazon tramite la console di DataZone gestione Amazon, devi assumere un ruolo IAM nell'account con autorizzazioni amministrative. Configura le autorizzazioni IAM necessarie per utilizzare la console di DataZone gestione Amazonper ottenere le autorizzazioni minime.

Abilita i blueprint integrati in un dominio Amazon DataZone

1. Accedi alla DataZone console Amazon all'indirizzo https://console.aws.amazon.com/datazone e accedi con le credenziali del tuo account.
2. Scegli Visualizza domini e scegli il dominio in cui desideri abilitare uno o più blueprint integrati.
3. Nella pagina dei dettagli del dominio, vai alla scheda Blueprints.
4. Dall'elenco Blueprints, scegli il DefaultDataLakeo il o DefaultDataWarehouseil SageMaker blueprint Amazon.
5. Nella pagina dei dettagli del progetto scelto, scegli Abilita in questo account.
6. Nella pagina Autorizzazioni e risorse, specifica quanto segue:

   - Se stai abilitando il DefaultDataLakeblueprint, per il ruolo Glue Manage Access, specifica un ruolo di servizio nuovo o esistente che conceda ad Amazon DataZone l'autorizzazione a importare e gestire l'accesso alle tabelle in AWS Glue and Lake Formation AWS .
   - Se stai abilitando il DefaultDataWarehouseblueprint, per il ruolo Redshift Manage Access, specifica un ruolo di servizio nuovo o esistente che conceda ad DataZone Amazon l'autorizzazione a importare e gestire l'accesso a condivisioni di dati, tabelle e viste in Amazon Redshift.
   - Se stai abilitando il SageMaker blueprint Amazon, per il ruolo SageMaker Manage Access, specifica un ruolo di servizio nuovo o esistente che conceda ad Amazon DataZone le

autorizzazioni per pubblicare SageMaker i dati Amazon nel catalogo. Fornisce inoltre ad Amazon DataZone le autorizzazioni per concedere l'accesso o revocare l'accesso alle risorse SageMaker pubblicate da Amazon nel catalogo.

> **Important**
>
> Quando abiliti il SageMaker blueprint Amazon, Amazon DataZone verifica se i seguenti ruoli IAM per Amazon DataZone esistono nell'account e nella regione correnti. Se questi ruoli non esistono, Amazon li crea DataZone automaticamente.
>
> - AmazonDataZoneGlueAccess- <region>- <domainId>
> - AmazonDataZoneRedshiftAccess- <region>- <domainId>

- Per il ruolo Provisioning, specifica un ruolo di servizio nuovo o esistente che conceda ad Amazon DataZone l'autorizzazione a creare e configurare risorse ambientali utilizzando AWS CloudFormation l'account e la regione dell'ambiente.
- Se stai abilitando il SageMaker blueprint Amazon, per il bucket Amazon S3 SageMaker per l'origine dati -Glue, specifica un bucket Amazon S3 che deve essere utilizzato da tutti gli ambienti dell'account. SageMaker AWS Il prefisso del bucket che specifichi deve essere uno dei seguenti:
  - amazon-datazone*
  - datazone-sagemaker*
  - sagemaker-datazone*
  - DataZone-Salviettore*
  - Salviettiere- * DataZone
  - DataZone-SageMaker*
  - SageMaker-DataZone*

7. Scegli Abilita blueprint.

Una volta abilitati i blueprint scelti, puoi controllare quali progetti possono utilizzare i blueprint del tuo account per creare profili ambientali. È possibile farlo assegnando la gestione dei progetti alla configurazione del blueprint.

Specificare la gestione dei progetti sui blueprint abilitati

1. Accedi alla DataZone console Amazon all'indirizzo https://console.aws.amazon.com/datazone e accedi con le credenziali del tuo account.
2. Scegli Visualizza domini, quindi scegli il dominio in cui desideri aggiungere i progetti di gestione per i progetti scelti.
3. Scegli la scheda Blueprint, quindi scegli il blueprint con cui vuoi lavorare.
4. Per impostazione predefinita, tutti i progetti all'interno del DefaultDataLake dominio possono utilizzare SageMaker i blueprint or o Amazon nell'account per creare profili di ambiente. DefaultDataWareshouse Tuttavia, puoi limitare questo problema assegnando la gestione dei progetti ai blueprint. Per aggiungere progetti in gestione, scegli Seleziona progetto di gestione, quindi scegli i progetti che desideri aggiungere come progetti di gestione dal menu a discesa, quindi scegli Seleziona progetti di gestione.

Dopo aver abilitato il DefaultDataWarehouse blueprint nel tuo AWS account, puoi aggiungere set di parametri alla configurazione del blueprint. Un set di parametri è un gruppo di chiavi e valori, necessario DataZone ad Amazon per stabilire una connessione al cluster Amazon Redshift e viene utilizzato per creare ambienti di data warehouse. Questi parametri includono il nome del cluster Amazon Redshift, il database e il AWS segreto che contiene le credenziali del cluster.

Aggiungere set di parametri al blueprint DefaultDataWarehouse

1. Accedi alla DataZone console Amazon all'indirizzo https://console.aws.amazon.com/datazone e accedi con le credenziali del tuo account.
2. Scegli Visualizza domini, quindi scegli il dominio in cui desideri aggiungere il set di parametri.
3. Scegli la scheda Blueprint, quindi scegli il DefaultDataWareshouse blueprint per aprire la pagina dei dettagli del blueprint.
4. Nella scheda Set di parametri nella pagina dei dettagli del blueprint, scegli Crea set di parametri.
   - Fornisci un nome per il set di parametri.
   - Facoltativamente, fornite una descrizione per il set di parametri.
   - Seleziona una regione
   - Seleziona un cluster Amazon Redshift o Amazon Redshift Serverless.
   - Seleziona l'ARN AWS segreto che contiene le credenziali per il cluster Amazon Redshift selezionato o il gruppo di lavoro Amazon Redshift Serverless. Il AWS segreto deve essere

etichettato con il `AmazonDataZoneDomain : [Domain_ID]` tag per essere idoneo all'uso all'interno di un set di parametri.

- Se non disponi di un AWS segreto esistente, puoi anche crearne uno nuovo scegliendo Crea nuovo AWS segreto. Si apre una finestra di dialogo in cui è possibile fornire il nome del segreto, il nome utente e la password. Dopo aver scelto Create New AWS Secret, Amazon DataZone crea un nuovo segreto nel servizio AWS Secrets Manager e assicura che il segreto sia etichettato con il dominio in cui stai tentando di creare il set di parametri.

- Se hai scelto il cluster Amazon Redshift nel passaggio precedente, ora scegli un cluster dal menu a discesa. Se hai scelto il gruppo di lavoro Amazon Redshift nel passaggio precedente, ora scegli un gruppo di lavoro dal menu a discesa.
- Inserisci il nome del database all'interno del cluster Amazon Redshift o del gruppo di lavoro Amazon Redshift Serverless selezionato.
- Scegli Crea set di parametri.

Dopo aver abilitato il SageMaker blueprint Amazon nel tuo AWS account, puoi aggiungere set di parametri alla configurazione del blueprint. Un set di parametri è un gruppo di chiavi e valori, necessario DataZone ad Amazon per stabilire una connessione con Amazon SageMaker e viene utilizzato per creare ambienti sagemaker.

Aggiungere set di parametri al SageMaker blueprint Amazon

1. Accedi alla DataZone console Amazon all'indirizzo https://console.aws.amazon.com/datazone e accedi con le credenziali del tuo account.
2. Scegli Visualizza domini, quindi scegli il dominio che contiene il blueprint abilitato a cui desideri aggiungere il set di parametri.
3. Scegli la scheda Blueprints, quindi scegli il SageMaker blueprint Amazon per aprire la pagina dei dettagli del progetto.
4. Nella scheda Set di parametri nella pagina dei dettagli del blueprint, scegli Crea set di parametri, quindi specifica quanto segue:

   - Fornisci un nome per il set di parametri.
   - Facoltativamente, fornite una descrizione per il set di parametri.
   - Specificare il tipo di autenticazione del SageMaker dominio Amazon. Puoi scegliere IAM o IAM Identity Center (SSO).
   - Specificare una AWS regione.

- Specificare una chiave AWS KMS per la crittografia dei dati. Puoi scegliere una chiave esistente o crearne una nuova.
- In Parametri di ambiente, specificate quanto segue:
  - ID VPC: l'ID che stai utilizzando per il VPC dell'ambiente Amazon. SageMaker Puoi specificare un VPC esistente o crearne uno nuovo.
  - Sottoreti: uno o più ID per un intervallo di indirizzi IP per risorse specifiche all'interno del tuo VPC.
  - Accesso alla rete: scegli solo VPC o Solo Internet pubblico.
  - Gruppo di sicurezza: il gruppo di sicurezza da utilizzare per la configurazione di VPC e sottoreti.
- In Parametri dell'origine dati, scegli una delle seguenti opzioni:
  - AWS Solo colla
  - AWS Glue+ Amazon Redshift Serverless. Se scegli questa opzione, specifica quanto segue:
    - Specificare l'ARN AWS segreto che contiene le credenziali per il cluster Amazon Redshift selezionato. Il AWS segreto deve essere etichettato con il `AmazonDataZoneDomain : [Domain_ID]` tag per essere idoneo all'uso all'interno di un set di parametri.

      Se non disponi di un AWS segreto esistente, puoi anche crearne uno nuovo scegliendo Crea nuovo AWS segreto. Si apre una finestra di dialogo in cui è possibile fornire il nome del segreto, il nome utente e la password. Dopo aver scelto Create New AWS Secret, Amazon DataZone crea un nuovo segreto nel servizio AWS Secrets Manager e assicura che il segreto sia etichettato con il dominio in cui stai tentando di creare il set di parametri.
    - Specificate il gruppo di lavoro Amazon Redshift che desiderate utilizzare per la creazione degli ambienti.
    - Specificate il nome del database (all'interno del gruppo di lavoro che avete scelto) che desiderate utilizzare durante la creazione degli ambienti.
  - AWS Solo Glue+ Amazon Redshift Cluster
    - Specificare l'ARN AWS segreto che contiene le credenziali per il cluster Amazon Redshift selezionato. Il AWS segreto deve essere etichettato con il `AmazonDataZoneDomain : [Domain_ID]` tag per essere idoneo all'uso all'interno di un set di parametri.

      Se non disponi di un AWS segreto esistente, puoi anche crearne uno nuovo scegliendo Crea nuovo AWS segreto. Si apre una finestra di dialogo in cui è possibile fornire il nome del segreto, il nome utente e la password. Dopo aver scelto Create New AWS Secret,

Amazon DataZone crea un nuovo segreto nel servizio AWS Secrets Manager e assicura che il segreto sia etichettato con il dominio in cui stai tentando di creare il set di parametri.

- Specificate il cluster Amazon Redshift che desiderate utilizzare per la creazione degli ambienti.
- Specificate il nome del database (all'interno del cluster che avete scelto) che desiderate utilizzare per creare ambienti.

5. Scegliete Crea set di parametri.

Aggiungi Amazon SageMaker come servizio affidabile nell' AWS account che possiede il DataZone dominio Amazon

Se hai abilitato il SageMaker blueprint Amazon, devi aggiungerlo anche SageMaker come uno dei servizi affidabili all'interno di Amazon DataZone. A tale scopo, completa la seguente procedura:

1. Accedi alla DataZone console Amazon all'indirizzo https://console.aws.amazon.com/datazone e accedi con le credenziali del tuo account.
2. Scegli Visualizza domini, quindi scegli il dominio che contiene il blueprint abilitato SageMaker .
3. Scegli i servizi affidabili, quindi scegli Amazon SageMaker e quindi scegli Abilita.

Utilizzo degli account associati per pubblicare e utilizzare dati

L'associazione AWS dei tuoi account al tuo DataZone dominio Amazon consente agli utenti del dominio di pubblicare e utilizzare i dati di questi AWS account. Esistono tre passaggi per configurare un'associazione di account.

- Innanzitutto, condividi il dominio con l' AWS account desiderato richiedendo l'associazione. Amazon DataZone utilizza AWS Resource Access Manager (RAM) se l' AWS account è diverso dall' AWS account del dominio. Un'associazione di account può essere avviata solo dal DataZone dominio Amazon.
- In secondo luogo, chiedi al proprietario dell'account di accettare la richiesta di associazione.
- In terzo luogo, chiedi al proprietario dell'account di abilitare i progetti di ambiente desiderati. Abilitando un blueprint, il proprietario dell'account fornisce agli utenti del dominio i ruoli IAM e le configurazioni delle risorse necessarie per creare e accedere alle risorse nel proprio account, come i database AWS Glue e i cluster Amazon Redshift.

Argomenti

Richiedi l'associazione con altri account AWS

> **Note**
>
> Inviando una richiesta di associazione a un altro AWS account, condividi il tuo dominio con l'altro AWS account tramite AWS Resource Access Manager (RAM). Assicurati di controllare l'accuratezza dell'ID dell'account che inserisci.

Per richiedere l'associazione con altri AWS account nella DataZone console Amazon per un DataZone dominio Amazon, devi assumere un ruolo IAM nell'account con autorizzazioni amministrative. Configura le autorizzazioni IAM necessarie per utilizzare la console di DataZone gestione Amazonper ottenere le autorizzazioni minime necessarie per richiedere l'associazione di un account.

Completa la seguente procedura per richiedere l'associazione con altri AWS account.

1. Accedi alla console di AWS gestione e apri la console di DataZone gestione Amazon all'indirizzo https://console.aws.amazon.com/datazone.
2. Scegli Visualizza domini e scegli il nome del dominio dall'elenco. Il nome è un collegamento ipertestuale.
3. Scorri verso il basso fino alla scheda Account associati e scegli Richiedi associazione.
4. Inserisci gli ID degli account per i quali desideri richiedere l'associazione. Quando sei soddisfatto dell'elenco degli ID degli account, scegli Richiedi associazione.
5. Amazon DataZone crea una condivisione di risorse nel AWS Resource Access Manager per conto del tuo account, con gli ID account inseriti come principali.
6. Devi avvisare il proprietario degli altri AWS account per accettare la tua richiesta. Gli inviti scadono dopo sette (7) giorni.

Fornisci l'accesso all'account alla tua chiave KMS gestita dal cliente

DataZone I domini Amazon e i relativi metadati sono crittografati (per impostazione predefinita) utilizzando una chiave detenuta da AWS o (facoltativamente) una chiave gestita dal AWS cliente del Key Management Service (KMS) di tua proprietà e fornita durante la creazione del dominio. Se il tuo dominio è crittografato con una chiave gestita dal cliente, segui la procedura seguente per autorizzare l'account associato a utilizzare la chiave KMS.

1. Accedi alla console di AWS gestione e apri la console KMS all'indirizzo https://console.aws.amazon.com/kms/.
2. Per visualizzare le chiavi nell'account creato e gestito dall'utente, nel riquadro di navigazione, seleziona Chiavi gestite dal cliente.
3. Per visualizzare le chiavi nell'account creato e gestito dall'utente, nel riquadro di navigazione, seleziona Chiavi gestite dal cliente.
4. Nell'elenco di chiavi KMS, scegliere l'alias o l'ID chiave della chiave KMS che si intende esaminare.

5. Per consentire o impedire agli AWS account esterni di utilizzare la chiave KMS, utilizza i controlli nella sezione Altri AWS account della pagina. I responsabili IAM di questi account (dotati anch'essi delle autorizzazioni KMS appropriate) possono utilizzare la chiave KMS in operazioni crittografiche, come la crittografia, la decrittografia, la ricrittografia e la generazione di chiavi di dati.

Accetta una richiesta di associazione di account da un DataZone dominio Amazon e abilita un blueprint di ambiente

Per accettare l'associazione nella console di DataZone gestione Amazon con un DataZone dominio Amazon, devi assumere un ruolo IAM nell'account con autorizzazioni amministrative. Configura le autorizzazioni IAM necessarie per utilizzare la console di DataZone gestione Amazonper ottenere le autorizzazioni minime.

Completa quanto segue per accettare l'associazione con un DataZone dominio Amazon.

1. Accedi alla console di AWS gestione e apri la console di DataZone gestione Amazon all'indirizzo https://console.aws.amazon.com/datazone.
2. Scegli Visualizza richieste e seleziona il dominio invitante dall'elenco. Lo stato dell'invito deve essere Richiesto. Scegli Richiesta di revisione.
3. Scegli se abilitare i blueprint predefiniti del data lake e/o dell'ambiente di data warehouse selezionando nessuna delle caselle, entrambe o una delle caselle. Puoi farlo più tardi.

   - Il modello di ambiente data lake consente agli utenti del dominio di creare e gestire risorse AWS Glue, Amazon S3 e Amazon Athena da pubblicare e utilizzare da un data lake.
   - Il blueprint dell'ambiente di data warehouse consente agli utenti del dominio di creare e gestire risorse Amazon Redshift da pubblicare e utilizzare da un data warehouse.
4. Se scegli di selezionare uno o entrambi i blueprint di ambiente predefiniti, configura le seguenti autorizzazioni e risorse.

   - Il ruolo IAM Manage access fornisce le autorizzazioni ad Amazon per consentire DataZone agli utenti del dominio di importare e gestire l'accesso alle tabelle, come AWS Glue e Amazon Redshift. Puoi scegliere di fare in modo che Amazon DataZone crei e utilizzi un nuovo ruolo IAM oppure puoi scegliere da un elenco di ruoli IAM esistenti.
   - Il ruolo Provisioning IAM fornisce le autorizzazioni DataZone ad Amazon per consentire agli utenti del dominio di creare e configurare risorse ambientali, come i database AWS Glue. Puoi

scegliere di fare in modo che Amazon DataZone crei e utilizzi un nuovo ruolo IAM oppure puoi scegliere da un elenco di ruoli IAM esistenti.

- Il bucket Amazon S3 per Data Lake è il bucket o il percorso che Amazon DataZone utilizzerà quando gli utenti del dominio archiviano i dati del data lake. Puoi utilizzare il bucket predefinito selezionato da Amazon DataZone o scegliere il tuo percorso Amazon S3 esistente inserendo la relativa stringa di percorso. Se selezioni il tuo percorso Amazon S3, dovrai aggiornare le policy IAM per fornire ad Amazon DataZone le autorizzazioni per utilizzarlo.

5. Quando sei soddisfatto delle tue configurazioni, scegli Accept e configura l'associazione.

Rifiuta una richiesta di associazione di account da un dominio Amazon DataZone

Per rifiutare una richiesta di associazione nella console di DataZone gestione Amazon da un DataZone dominio Amazon, devi assumere un ruolo IAM nell'account con autorizzazioni amministrative. Configura le autorizzazioni IAM necessarie per utilizzare la console di DataZone gestione Amazonper ottenere le autorizzazioni minime.

Completa quanto segue per rifiutare una richiesta di associazione da un DataZone dominio Amazon.

1. Accedi alla console di AWS gestione e apri la console di DataZone gestione Amazon all'indirizzo https://console.aws.amazon.com/datazone.
2. Scegli Visualizza richieste e seleziona il dominio invitante dall'elenco. Lo stato dell'invito deve essere Richiesto. Scegli Rifiuta l'associazione. Conferma la tua scelta scegliendo Rifiuta associazione.

Abilita un blueprint di ambiente in un account associato AWS

Per abilitare un blueprint di ambiente nella console di DataZone gestione Amazon, devi assumere un ruolo IAM nell'account con autorizzazioni amministrative. Configura le autorizzazioni IAM necessarie per utilizzare la console di DataZone gestione Amazonper ottenere le autorizzazioni minime.

Completa quanto segue per abilitare un blueprint in un dominio associato.

1. Accedi alla console di AWS gestione e apri la console di DataZone gestione Amazon all'indirizzo https://console.aws.amazon.com/datazone.
2. Apri il pannello di navigazione a sinistra e scegli Domini associati.

3. Scegli il dominio per il quale desideri abilitare un blueprint di ambiente.
4. Dall'elenco Blueprint, scegli il DefaultDataLakeo il DefaultDataWarehouse SageMakerprogetto Amazon.
5. Nella pagina dei dettagli del progetto scelto, scegli Abilita in questo account.
6. Nella pagina Autorizzazioni e risorse, specifica quanto segue:

   - Se stai abilitando il DefaultDataLakeblueprint, per il ruolo Glue Manage Access, specifica un ruolo di servizio nuovo o esistente che conceda ad Amazon DataZone l'autorizzazione a importare e gestire l'accesso alle tabelle in AWS Glue and Lake Formation AWS .
   - Se stai abilitando il DefaultDataWarehouseblueprint, per il ruolo Redshift Manage Access, specifica un ruolo di servizio nuovo o esistente che conceda ad DataZone Amazon l'autorizzazione a importare e gestire l'accesso a condivisioni di dati, tabelle e viste in Amazon Redshift.
   - Se stai abilitando il SageMaker blueprint Amazon, per il ruolo SageMaker Manage Access, specifica un ruolo di servizio nuovo o esistente che conceda ad Amazon DataZone le autorizzazioni per pubblicare SageMaker i dati Amazon nel catalogo. Fornisce inoltre ad Amazon DataZone le autorizzazioni per concedere l'accesso o revocare l'accesso alle risorse SageMaker pubblicate da Amazon nel catalogo.

     > **Important**
     >
     > Quando abiliti il SageMaker blueprint Amazon, Amazon DataZone verifica se i seguenti ruoli IAM per Amazon DataZone esistono nell'account e nella regione correnti. Se questi ruoli non esistono, Amazon li crea DataZone automaticamente.
     >
     > - AmazonDataZoneGlueAccess- <region>- <domainId>
     > - AmazonDataZoneRedshiftAccess- <region>- <domainId>

   - Per il ruolo Provisioning, specifica un ruolo di servizio nuovo o esistente che conceda ad Amazon DataZone l'autorizzazione a creare e configurare risorse ambientali utilizzando AWS CloudFormation l'account e la regione dell'ambiente.
   - Se stai abilitando il SageMaker blueprint Amazon, per il bucket Amazon S3 SageMaker per l'origine dati -Glue, specifica un bucket Amazon S3 che deve essere utilizzato da tutti gli ambienti dell'account. SageMaker AWS Il prefisso del bucket che specifichi deve essere uno dei seguenti:

     - amazon-datazone*

- datazone-sagemaker*
- sagemaker-datazone*
- DataZone-Sagemaker *
- Salviettiere- * DataZone
- DataZone-SageMaker*
- SageMaker-DataZone*

7. Scegli Abilita blueprint.

Una volta abilitati i blueprint scelti, puoi controllare quali progetti possono utilizzare i blueprint del tuo account per creare profili ambientali. Puoi farlo assegnando la gestione dei progetti alla configurazione del blueprint.

Specificare la gestione dei progetti su Enabled DefaultDataLake o Blueprint DefaultDataWarehouse

1. Accedi alla DataZone console Amazon all'indirizzo https://console.aws.amazon.com/datazone e accedi con le credenziali del tuo account.
2. Apri il pannello di navigazione a sinistra e scegli Domini associati, quindi scegli il dominio a cui desideri aggiungere i progetti di gestione.
3. Scegli la scheda Blueprint, quindi scegli DefaultDataLake o DefaultDataWareshouse blueprint.
4. Per impostazione predefinita, tutti i progetti all'interno del dominio possono utilizzare il DefaultDataWareshouse blueprint DefaultDataLake o nell'account per creare profili ambientali. Tuttavia, è possibile limitare questo problema assegnando la gestione dei progetti al blueprint. Per aggiungere progetti in gestione, scegli Seleziona progetto di gestione, quindi scegli i progetti che desideri aggiungere come progetti di gestione dal menu a discesa, quindi scegli Seleziona progetti di gestione.

Dopo aver abilitato il DefaultDataWarehouse blueprint nel tuo AWS account, puoi aggiungere set di parametri alla configurazione del blueprint. Un set di parametri è un gruppo di chiavi e valori, necessario DataZone ad Amazon per stabilire una connessione al cluster Amazon Redshift e viene utilizzato per creare ambienti di data warehouse. Questi parametri includono il nome del cluster Amazon Redshift, il database e il AWS segreto che contiene le credenziali del cluster.

Aggiungere set di parametri al blueprint DefaultDataWarehouse

1. Accedi alla DataZone console Amazon all'indirizzo https://console.aws.amazon.com/datazone e accedi con le credenziali del tuo account.
2. Apri il pannello di navigazione a sinistra e scegli Domini associati, quindi scegli il dominio a cui desideri aggiungere i set di parametri.
3. Scegli la scheda Blueprint, quindi scegli il DefaultDataWareshouse blueprint per aprire la pagina dei dettagli del blueprint.
4. Nella scheda Set di parametri nella pagina dei dettagli del blueprint, scegli Crea set di parametri.
   - Fornisci un nome per il set di parametri.
   - Facoltativamente, fornite una descrizione per il set di parametri.
   - Seleziona una regione
   - Seleziona un cluster Amazon Redshift o Amazon Redshift Serverless.
   - Seleziona l'ARN AWS segreto che contiene le credenziali del cluster Amazon Redshift selezionato o del gruppo di lavoro Amazon Redshift Serverless. Il AWS segreto deve essere etichettato con il `AmazonDataZoneDomain : [Domain_ID]` tag per essere idoneo all'uso all'interno di un set di parametri.
     - Se non disponi di un AWS segreto esistente, puoi anche crearne uno nuovo scegliendo Crea nuovo AWS segreto. Si apre una finestra di dialogo in cui è possibile fornire il nome del segreto, il nome utente e la password. Dopo aver scelto Create New AWS Secret, Amazon DataZone crea un nuovo segreto nel servizio AWS Secrets Manager e assicura che il segreto sia etichettato con il dominio in cui stai tentando di creare il set di parametri.
   - Seleziona il cluster Amazon Redshift o il gruppo di lavoro Serverless Amazon Redshift.
   - Inserisci il nome del database all'interno del cluster Amazon Redshift o del gruppo di lavoro Amazon Redshift Serverless selezionato.
   - Scegli Crea set di parametri.

Dopo aver abilitato il SageMaker blueprint Amazon nel tuo AWS account, puoi aggiungere set di parametri alla configurazione del blueprint. Un set di parametri è un gruppo di chiavi e valori, necessario DataZone ad Amazon per stabilire una connessione con Amazon SageMaker e viene utilizzato per creare ambienti sagemaker.

Aggiungere set di parametri al SageMaker blueprint Amazon

1. Accedi alla DataZone console Amazon all'indirizzo https://console.aws.amazon.com/datazone e accedi con le credenziali del tuo account.
2. Scegli Visualizza domini, quindi scegli il dominio che contiene il blueprint abilitato a cui desideri aggiungere il set di parametri.
3. Scegli la scheda Blueprints, quindi scegli il SageMaker blueprint Amazon per aprire la pagina dei dettagli del progetto.
4. Nella scheda Set di parametri nella pagina dei dettagli del blueprint, scegli Crea set di parametri, quindi specifica quanto segue:
   - Fornisci un nome per il set di parametri.
   - Facoltativamente, fornite una descrizione per il set di parametri.
   - Specificare il tipo di autenticazione del SageMaker dominio Amazon. Puoi scegliere IAM o IAM Identity Center (SSO).
   - Specificare una AWS regione.
   - Specificare una chiave AWS KMS per la crittografia dei dati. Puoi scegliere una chiave esistente o crearne una nuova.
   - In Parametri di ambiente, specificate quanto segue:
     - ID VPC: l'ID che stai utilizzando per il VPC dell'ambiente Amazon. SageMaker Puoi specificare un VPC esistente o crearne uno nuovo.
     - Sottoreti: uno o più ID per un intervallo di indirizzi IP per risorse specifiche all'interno del tuo VPC.
     - Accesso alla rete: scegli solo VPC o Solo Internet pubblico.
     - Gruppo di sicurezza: il gruppo di sicurezza da utilizzare per la configurazione di VPC e sottoreti.
   - In Parametri dell'origine dati, scegli una delle seguenti opzioni:
     - AWS Solo colla
     - AWS Glue+ Amazon Redshift Serverless. Se scegli questa opzione, specifica quanto segue:
       - Specificare l'ARN AWS segreto che contiene le credenziali del cluster Amazon Redshift selezionato. Il AWS segreto deve essere etichettato con il `AmazonDataZoneDomain : [Domain_ID]` tag per essere idoneo all'uso all'interno di un set di parametri.

Se non disponi di un AWS segreto esistente, puoi anche crearne uno nuovo scegliendo Crea nuovo AWS segreto. Si apre una finestra di dialogo in cui è possibile fornire il nome del segreto, il nome utente e la password. Dopo aver scelto Create New AWS Secret, Amazon DataZone crea un nuovo segreto nel servizio AWS Secrets Manager e assicura che il segreto sia etichettato con il dominio in cui stai tentando di creare il set di parametri.

- Specificate il gruppo di lavoro Amazon Redshift che desiderate utilizzare per la creazione degli ambienti.
- Specificate il nome del database (all'interno del gruppo di lavoro che avete scelto) che desiderate utilizzare durante la creazione degli ambienti.

- AWS Solo Glue+ Amazon Redshift Cluster
  - Specificare l'ARN AWS segreto che contiene le credenziali del cluster Amazon Redshift selezionato. Il AWS segreto deve essere etichettato con il `AmazonDataZoneDomain : [Domain_ID]` tag per essere idoneo all'uso all'interno di un set di parametri.

    Se non disponi di un AWS segreto esistente, puoi anche crearne uno nuovo scegliendo Crea nuovo AWS segreto. Si apre una finestra di dialogo in cui è possibile fornire il nome del segreto, il nome utente e la password. Dopo aver scelto Create New AWS Secret, Amazon DataZone crea un nuovo segreto nel servizio AWS Secrets Manager e assicura che il segreto sia etichettato con il dominio in cui stai tentando di creare il set di parametri.
  - Specificate il cluster Amazon Redshift che desiderate utilizzare per la creazione degli ambienti.
  - Specificate il nome del database (all'interno del cluster che avete scelto) che desiderate utilizzare per creare ambienti.

5. Scegli Crea set di parametri.

Aggiungi Amazon SageMaker come servizio affidabile nell' AWS account associato

Se hai abilitato il SageMaker blueprint Amazon, devi aggiungerlo anche SageMaker come uno dei servizi affidabili di Amazon DataZone. A tale scopo, completa la seguente procedura:

1. Accedi alla DataZone console Amazon all'indirizzo https://console.aws.amazon.com/datazone e accedi con le credenziali del tuo account.
2. Scegli Visualizza domini, quindi scegli il dominio che contiene il blueprint abilitato SageMaker .

3. Scegli i servizi affidabili, quindi scegli Amazon SageMaker e quindi scegli Abilita.

Rimuovi un account associato

Per rimuovere un AWS account associato nella console di DataZone gestione Amazon, devi assumere un ruolo IAM nell'account con autorizzazioni amministrative. Configura le autorizzazioni IAM necessarie per utilizzare la console di DataZone gestione Amazonper ottenere le autorizzazioni minime.

Completa la seguente procedura per rimuovere un account associato dal tuo dominio.

1. Accedi alla console di AWS gestione e apri la console di DataZone gestione Amazon all'indirizzo https://console.aws.amazon.com/datazone.
2. Scegli Visualizza domini e scegli il nome del dominio dall'elenco. Il nome è un collegamento ipertestuale.
3. Scorri verso il basso fino alla scheda Account associati. Scegli l'ID dell' AWS account che desideri rimuovere.
4. Scegli Dissocia. Conferma la tua scelta inserendo dissocia nel campo e scegliendo Dissocia.
5. L'account è ora rimosso dal tuo dominio e non può essere utilizzato dagli utenti del dominio per pubblicare e consumare dati.

Lavorare con il catalogo DataZone dati di Amazon

Puoi utilizzare il catalogo di dati DataZone aziendali di Amazon per catalogare i dati in tutta l'organizzazione in base al contesto aziendale e consentire così a tutti i membri dell'organizzazione di trovare e comprendere rapidamente i dati. Per ulteriori informazioni, consulta DataZone Terminologia e concetti di Amazon.

Argomenti

Crea, modifica o elimina un glossario aziendale

In Amazon DataZone, un glossario aziendale è una raccolta di termini commerciali (parole) che possono essere associati a risorse (dati). Fornisce vocabolari appropriati con un elenco di termini commerciali e le relative definizioni per consentire agli utenti aziendali di utilizzare le stesse definizioni in tutta l'organizzazione durante l'analisi dei dati. I glossari aziendali vengono creati nel dominio del catalogo e possono essere applicati a risorse e colonne per aiutare a comprendere le caratteristiche chiave di quella risorsa o colonna. È possibile applicare uno o più termini del glossario. Un glossario aziendale può essere un semplice elenco di termini in cui qualsiasi termine del glossario aziendale può essere associato a un sottoelenco di altri termini. Per ulteriori informazioni, consulta DataZone Terminologia e concetti di Amazon. Per creare, modificare o eliminare un glossario nel tuo DataZone dominio Amazon, devi essere il membro del progetto proprietario con le autorizzazioni corrette per quel dominio.

Per creare un glossario, completa i seguenti passaggi:

1. Accedi al portale DataZone dati di Amazon utilizzando l'URL del portale dati e accedi utilizzando il tuo SSO o AWS le tue credenziali. Se sei un DataZone amministratore Amazon, puoi ottenere l'URL del portale dati accedendo alla DataZone console Amazon all'indirizzo https://console.aws.amazon.com/datazone nell' AWS account in cui è stato creato il DataZone dominio Amazon.
2. Vai al menu Catalogo nella barra di navigazione in alto accanto a Cerca.

3. In Amazon DataZone Data Portal, scegli Glossari, quindi scegli Crea glossario.
4. Specificate un nome, una descrizione e un proprietario per il glossario, quindi scegliete Crea glossario.
5. Abilita il nuovo glossario scegliendo l'interruttore Abilitato.
6. Nella pagina dei dettagli del glossario, puoi scegliere Crea readme per aggiungere alcune informazioni aggiuntive su questo glossario.

Per disabilitare o abilitare un glossario aziendale, completa i seguenti passaggi:

1. Accedi al portale DataZone dati di Amazon utilizzando l'URL del portale dati e accedi utilizzando il tuo SSO o AWS le tue credenziali. Se sei un DataZone amministratore Amazon, puoi ottenere l'URL del portale dati accedendo alla DataZone console Amazon all'indirizzo https://console.aws.amazon.com/datazone nell' AWS account in cui è stato creato il DataZone dominio Amazon.
2. Vai al menu Catalogo nella barra di navigazione in alto accanto a Cerca.
3. In Amazon DataZone Data Portal, scegli Glossari e individua il glossario aziendale che desideri disabilitare/abilitare.
4. Nella pagina dei dettagli del glossario, individua l'interruttore Abilita/Disabilita e usalo per abilitare o disabilitare il glossario selezionato.

> **Note**
>
> La disabilitazione di un glossario disabilita anche tutti i termini in esso contenuti.

Per modificare un glossario aziendale, completa i seguenti passaggi:

1. Accedi al portale DataZone dati di Amazon utilizzando l'URL del portale dati e accedi utilizzando il tuo SSO o AWS le tue credenziali. Se sei un DataZone amministratore Amazon, puoi ottenere l'URL del portale dati accedendo alla DataZone console Amazon all'indirizzo https://console.aws.amazon.com/datazone nell' AWS account in cui è stato creato il DataZone dominio Amazon.
2. Vai al menu Catalogo nella barra di navigazione in alto accanto a Cerca.
3. In Amazon DataZone Data Portal, scegli Glossari e individua il glossario aziendale che desideri modificare.

4. Nella pagina dei dettagli del glossario, espandi Azioni, quindi scegli Modifica per modificare il glossario.
5. Aggiorna il nome, la descrizione, quindi scegli Salva.

Per eliminare un glossario aziendale, completa i seguenti passaggi:

1. Accedi al portale DataZone dati di Amazon utilizzando l'URL del portale dati e accedi utilizzando il tuo SSO o AWS le tue credenziali. Se sei un DataZone amministratore Amazon, puoi ottenere l'URL del portale dati accedendo alla DataZone console Amazon all'indirizzo https://console.aws.amazon.com/datazone nell' AWS account in cui è stato creato il DataZone dominio Amazon.
2. Vai al menu Catalogo nella barra di navigazione in alto accanto a Cerca.
3. In Amazon DataZone Data Portal, scegli Glossari e individua il glossario aziendale che desideri eliminare.
4. Nella pagina dei dettagli del glossario, espandi Azioni, quindi scegli Elimina per eliminare il glossario.

> **Note**
>
> È necessario eliminare tutti i termini esistenti nel glossario prima di poter eliminare il glossario.

5. Conferma l'eliminazione del glossario scegliendo Elimina.

Crea, modifica o elimina un termine in un glossario

In Amazon DataZone, un glossario aziendale è una raccolta di termini commerciali che possono essere associati agli asset (dati). Per ulteriori informazioni, consulta DataZone Terminologia e concetti di Amazon. Per creare, modificare o eliminare termini in un glossario del tuo DataZone dominio Amazon, devi essere il membro del progetto proprietario con le autorizzazioni corrette per quel dominio.

In Amazon DataZone, i termini del glossario aziendale possono avere descrizioni dettagliate. Per impostare il contesto di un termine particolare, puoi specificare le relazioni tra i termini. Quando si definisce una relazione per un termine, questa viene aggiunta automaticamente alla definizione del

termine correlato. Le relazioni terminologiche del glossario disponibili in Amazon DataZone includono quanto segue:

- È un tipo di: indica che il termine corrente è un tipo del termine identificato. Indica che il termine identificato è un capostipite del termine corrente.
- Ha tipi: indica che il termine corrente è un termine generico per il termine o i termini specifici indicati. Questa relazione può indicare termini secondari rispetto al termine generico.

Per creare un nuovo termine, completa i seguenti passaggi:

1. Accedi al portale DataZone dati di Amazon utilizzando l'URL del portale dati e accedi utilizzando il tuo SSO o AWS le tue credenziali. Se sei un DataZone amministratore Amazon, puoi ottenere l'URL del portale dati accedendo alla DataZone console Amazon all'indirizzo https://console.aws.amazon.com/datazone nell' AWS account in cui è stato creato il DataZone dominio Amazon.
2. Vai al menu Catalogo nella barra di navigazione in alto accanto a Cerca.
3. In Amazon DataZone Data Portal, scegli Glossari, quindi scegli il glossario in cui desideri creare il nuovo termine.
4. Specificate un nome, una descrizione e un proprietario per il termine, quindi scegliete Crea termine.
5. Abilita il nuovo termine scegliendo l'interruttore Abilitato.
6. Per aggiungere Readme, vai alla pagina dei dettagli del termine, quindi puoi scegliere Crea readme per aggiungere alcune informazioni aggiuntive su questo glossario.
7. Per aggiungere relazioni, vai alla pagina dei dettagli del termine, scegli la sezione Relazioni tra termini, quindi scegli Aggiungi termini del glossario. Nella finestra di dialogo, scegli la relazione e i termini che desideri correlare, quindi scegli Chiudi per aggiungere un termine al tipo di relazione appropriato. Questa relazione viene inoltre aggiunta a tutti i termini che avete reso correlati.

Per modificare un termine in un glossario, completa i seguenti passaggi:

1. Accedi al portale DataZone dati di Amazon utilizzando l'URL del portale dati e accedi utilizzando il tuo SSO o AWS le tue credenziali. Se sei un DataZone amministratore Amazon, puoi ottenere l'URL del portale dati accedendo alla DataZone console Amazon all'indirizzo https://console.aws.amazon.com/datazone nell' AWS account in cui è stato creato il DataZone dominio Amazon.

2. Vai al menu Catalogo nella barra di navigazione in alto accanto a Cerca.
3. In Amazon DataZone Data Portal, scegli Glossari, individua il glossario che contiene il termine che desideri modificare, quindi scegli quel termine.
4. Nella pagina dei dettagli del termine, espandi Azioni, quindi scegli Modifica per modificare il termine.
5. Aggiorna il nome e la descrizione, quindi scegli Salva.

Per eliminare un termine in un glossario, completa i seguenti passaggi:

1. Accedi al portale DataZone dati di Amazon utilizzando l'URL del portale dati e accedi utilizzando il tuo SSO o AWS le tue credenziali. Se sei un DataZone amministratore Amazon, puoi ottenere l'URL del portale dati accedendo alla DataZone console Amazon all'indirizzo https://console.aws.amazon.com/datazone nell' AWS account in cui è stato creato il DataZone dominio Amazon.
2. Vai al menu Catalogo nella barra di navigazione in alto accanto a Cerca.
3. In Amazon DataZone Data Portal, scegli Glossari, individua il glossario che contiene il termine che desideri eliminare, quindi scegli quel termine.
4. Nella pagina dei dettagli del glossario, espandi Azioni, quindi scegli Elimina per eliminare il termine.
5. Conferma l'eliminazione del termine scegliendo Elimina.

Crea, modifica o elimina moduli di metadati

In Amazon DataZone, i moduli di metadati sono moduli semplici per aggiungere un contesto aziendale aggiuntivo ai metadati delle risorse nel catalogo. Funge da meccanismo estensibile che consente ai proprietari di dati di arricchire la risorsa con informazioni che possono aiutare gli utenti a cercare e trovare tali dati. I moduli di metadati possono anche fungere da meccanismo per imporre la coerenza a tutte le risorse pubblicate nel catalogo Amazon DataZone .

La definizione di un modulo di metadati è composta da una o più definizioni di campo, con supporto per i tipi di dati booleani, date, decimali, interi, stringhe e valori dei campi del glossario aziendale. Per ulteriori informazioni, consulta DataZone Terminologia e concetti di Amazon. Per creare, modificare o eliminare moduli di metadati nel tuo DataZone dominio Amazon, devi essere un membro del progetto proprietario con le credenziali corrette.

Per creare un modulo di metadati, completa i seguenti passaggi:

1. Accedi al portale DataZone dati di Amazon utilizzando l'URL del portale dati e accedi utilizzando il tuo SSO o AWS le tue credenziali. Se sei un DataZone amministratore Amazon, puoi ottenere l'URL del portale dati accedendo alla DataZone console Amazon all'indirizzo https://console.aws.amazon.com/datazone nell' AWS account in cui è stato creato il DataZone dominio Amazon.
2. Vai al menu Catalogo nella barra di navigazione in alto accanto a Cerca.
3. In Amazon DataZone Data Portal, scegli Moduli di metadati, quindi scegli Crea modulo.
4. Specificate il nome, la descrizione e il proprietario del modulo di metadati, quindi scegliete Crea modulo.

Per modificare un modulo di metadati, completa i seguenti passaggi:

1. Accedi al portale DataZone dati di Amazon utilizzando l'URL del portale dati e accedi utilizzando il tuo SSO o AWS le tue credenziali. Se sei un DataZone amministratore Amazon, puoi ottenere l'URL del portale dati accedendo alla DataZone console Amazon all'indirizzo https://console.aws.amazon.com/datazone nell' AWS account in cui è stato creato il DataZone dominio Amazon.
2. Vai al menu Catalogo nella barra di navigazione in alto accanto a Cerca.
3. In Amazon DataZone Data Portal, scegli Moduli di metadati, quindi individua il modulo di metadati che desideri modificare.
4. Nella pagina dei dettagli del modulo di metadati, espandi Azioni, quindi scegli Modifica.
5. Aggiorna il nome, la descrizione, i campi del proprietario, quindi scegli Aggiorna modulo.

Per eliminare un modulo di metadati, completa i seguenti passaggi:

> **Note**
>
> Prima di poter eliminare un modulo di metadati, è necessario rimuoverlo da tutti i tipi di risorse o risorse a cui è applicato.

1. Accedi al portale DataZone dati di Amazon utilizzando l'URL del portale dati e accedi utilizzando il tuo SSO o AWS le tue credenziali. Se sei un DataZone amministratore Amazon, puoi ottenere l'URL del portale dati accedendo alla DataZone console Amazon all'indirizzo https://

console.aws.amazon.com/datazone nell' AWS account in cui è stato creato il DataZone dominio Amazon.

2. Vai al menu Catalogo nella barra di navigazione in alto accanto a Cerca.
3. In Amazon DataZone Data Portal, scegli Moduli di metadati, quindi individua il modulo di metadati che desideri eliminare.
4. Se il modulo di metadati che desideri eliminare è abilitato, disabilita il modulo di metadati selezionando l'interruttore Abilitato.
5. Nella pagina dei dettagli del modulo di metadati, espandi Azioni, quindi scegli Elimina.
6. Conferma l'eliminazione scegliendo Elimina.

Crea, modifica o elimina i campi nei moduli di metadati

In Amazon DataZone, i moduli di metadati sono moduli semplici per aggiungere un contesto aziendale aggiuntivo ai metadati delle risorse nel catalogo. Funge da meccanismo estensibile che consente ai proprietari di dati di arricchire la risorsa con informazioni che possono aiutare gli utenti a cercare e trovare tali dati. I moduli di metadati possono anche fungere da meccanismo per imporre la coerenza a tutte le risorse pubblicate nel catalogo Amazon DataZone .

La definizione di un modulo di metadati è composta da una o più definizioni di campo, con supporto per i tipi di dati booleani, date, decimali, interi, stringhe e valori dei campi del glossario aziendale. Per ulteriori informazioni, consulta DataZone Terminologia e concetti di Amazon. Per creare, modificare o eliminare campi nei moduli di metadati nel tuo DataZone dominio Amazon, devi essere un membro del progetto proprietario con le credenziali corrette.

Per creare un campo in un modulo di metadati, completa i seguenti passaggi:

1. Accedi al portale DataZone dati di Amazon utilizzando l'URL del portale dati e accedi utilizzando il tuo SSO o AWS le tue credenziali. Se sei un DataZone amministratore Amazon, puoi ottenere l'URL del portale dati accedendo alla DataZone console Amazon all'indirizzo https://console.aws.amazon.com/datazone nell' AWS account in cui è stato creato il DataZone dominio Amazon.
2. Vai al menu Catalogo nella barra di navigazione in alto accanto a Cerca.
3. In Amazon DataZone Data Portal, scegli Moduli di metadati, quindi scegli il modulo di metadati in cui desideri creare i campi.
4. Nella pagina dei dettagli del modulo, scegli Crea campo.

5. Specificate il nome, la descrizione, il tipo e se si tratta di un campo obbligatorio, quindi scegliete Crea campo.

Per modificare un campo in un modulo di metadati, completa i seguenti passaggi:

1. Accedi al portale DataZone dati di Amazon utilizzando l'URL del portale dati e accedi utilizzando il tuo SSO o AWS le tue credenziali. Se sei un DataZone amministratore Amazon, puoi ottenere l'URL del portale dati accedendo alla DataZone console Amazon all'indirizzo https://console.aws.amazon.com/datazone nell' AWS account in cui è stato creato il DataZone dominio Amazon.
2. Vai al menu Catalogo nella barra di navigazione in alto accanto a Cerca.
3. In Amazon DataZone Data Portal, scegli Moduli di metadati, quindi scegli il modulo di metadati in cui desideri modificare i campi.
4. Nella pagina dei dettagli del modulo, scegli il campo che desideri modificare, quindi espandi Azioni e scegli Modifica.
5. Aggiorna il nome, la descrizione, il tipo di campo e indica se si tratta di un campo obbligatorio, quindi scegli Aggiorna campo.

Per eliminare un campo in un modulo di metadati, completa i seguenti passaggi:

1. Accedi al portale DataZone dati di Amazon utilizzando l'URL del portale dati e accedi utilizzando il tuo SSO o AWS le tue credenziali. Se sei un DataZone amministratore Amazon, puoi ottenere l'URL del portale dati accedendo alla DataZone console Amazon all'indirizzo https://console.aws.amazon.com/datazone nell' AWS account in cui è stato creato il DataZone dominio Amazon.
2. Vai al menu Catalogo nella barra di navigazione in alto accanto a Cerca.
3. In Amazon DataZone Data Portal, scegli Moduli di metadati, quindi scegli il modulo di metadati in cui desideri eliminare i campi.
4. Nella pagina dei dettagli del modulo, scegli il campo che desideri eliminare, quindi espandi Azioni e scegli Elimina.
5. Conferma l'eliminazione scegliendo Elimina.

Lavorare con progetti e ambienti in Amazon DataZone

In Amazon DataZone, i progetti consentono a un gruppo di utenti di collaborare su vari casi d'uso aziendali che prevedono la pubblicazione, la scoperta, la sottoscrizione e il consumo di risorse di dati nel catalogo Amazon DataZone . Ogni DataZone progetto Amazon ha una serie di controlli di accesso applicati in modo che solo le persone, i gruppi e i ruoli autorizzati possano accedere al progetto e alle risorse di dati a cui il progetto è abbonato e possano utilizzare solo gli strumenti definiti dalle autorizzazioni del progetto. I progetti agiscono come un principio di identità che riceve concessioni di accesso alle risorse sottostanti, consentendo DataZone ad Amazon di operare all'interno dell'infrastruttura di un'organizzazione senza fare affidamento sulle credenziali dei singoli utenti. Per ulteriori informazioni, consulta DataZone Terminologia e concetti di Amazon

Argomenti

Crea un profilo ambientale

In Amazon DataZone, un profilo di ambiente è un modello che puoi utilizzare per creare ambienti. Lo scopo di un profilo ambientale è semplificare la creazione dell'ambiente incorporando informazioni di posizionamento come AWS account e regione all'interno dei profili. Per ulteriori informazioni, consulta DataZone Terminologia e concetti di Amazon. Per creare profili di ambiente in un DataZone

dominio Amazon, devi appartenere a un DataZone progetto Amazon. Tutti i profili di ambiente sono di proprietà dei progetti e possono essere utilizzati da tutti gli utenti autorizzati, di qualsiasi progetto, per creare nuovi ambienti.

Per creare un profilo ambientale

1. Accedi al portale DataZone dati di Amazon utilizzando l'URL del portale dati e accedi utilizzando il tuo SSO o AWS le tue credenziali. Se sei un DataZone amministratore Amazon, puoi ottenere l'URL del portale dati accedendo alla DataZone console Amazon all'indirizzo https://console.aws.amazon.com/datazone nell' AWS account in cui è stato creato il DataZone dominio Amazon.
2. All'interno del portale dati, scegli Sfoglia progetti e seleziona il progetto in cui desideri creare il profilo ambientale.
3. Vai alla scheda Ambienti all'interno del progetto, quindi scegli Crea profilo ambientale.
4. Configura i campi seguenti:

   - Nome: il nome del tuo profilo ambientale.
   - Descrizione: (Facoltativo) Una descrizione del profilo di ambiente.
   - Progetto proprietario: il progetto in cui viene creato il profilo è selezionato per impostazione predefinita in questo campo.
   - Blueprint: il blueprint per il quale viene creato questo profilo. Puoi scegliere uno dei DataZone blueprint Amazon predefiniti (Data Lake o Data Warehouse).

     Se hai specificato il blueprint Data Warehouse, procedi come segue:

     - Fornire un set di parametri. Per selezionare un set di parametri esistente, scegliete l'opzione Scegli un set di parametri. Se desideri inserire i tuoi parametri, scegli Inserisci i miei.
     - Se scegli di selezionare un parametro esistente, procedi come segue:
       - Seleziona un AWS account dal menu a discesa.
       - Seleziona un set di parametri dal menu a discesa.
     - Se scegli di inserire i tuoi parametri, procedi come segue:
       - Fornisci i AWS parametri selezionando AWS Account e Regione dal menu a discesa.
       - Fornisci i parametri di Redshift Data Wareshoue:
         - Seleziona un cluster Amazon Redshift o Amazon Redshift Serverless
         - Inserisci l'ARN AWS segreto che contiene le credenziali del cluster Amazon Redshift o del gruppo di lavoro Amazon Redshift Serverless selezionato. Il AWS segreto deve

essere contrassegnato con l'ID del dominio e l'ID del progetto in cui si sta creando il profilo di ambiente.

- `AmazonDataZoneDomain: [Domain_ID]`
- `AmazonDataZoneProject: [Project_ID]`

- Inserisci il nome del cluster Amazon Redshift o del gruppo di lavoro Amazon Redshift Serverless.
- Inserisci il nome del database all'interno del cluster Amazon Redshift o del gruppo di lavoro Amazon Redshift Serverless selezionato.

- Nella sezione Progetti autorizzati, specifica i progetti che possono utilizzare il profilo ambientale per creare ambienti. Per impostazione predefinita, tutti i progetti all'interno del dominio possono utilizzare i profili di ambiente dell'account per creare ambienti. Per mantenere questa impostazione predefinita, scegli Tutti i progetti. Tuttavia, puoi limitare questo problema assegnando progetti autorizzati all'ambiente. A tale scopo, scegli Solo progetti autorizzati e quindi specifica i progetti che possono utilizzare questo profilo di progetto per creare ambienti.
- Nella sezione Pubblicazione, scegli una delle seguenti opzioni:
  - Pubblica da qualsiasi schema: se scegli questa opzione, gli ambienti creati utilizzando questo profilo di ambiente possono essere utilizzati per pubblicare da qualsiasi schema all'interno del database selezionato nei parametri Redshift forniti sopra. Gli utenti dell'ambiente creato utilizzando questi profili di ambiente possono anche fornire i propri parametri Amazon Redshift da pubblicare da qualsiasi schema all'interno dell' AWS account e della regione selezionati nel profilo di ambiente.
  - Pubblica solo dallo schema di ambiente predefinito: se scegli questa opzione, gli ambienti creati utilizzando questa possono essere utilizzati per pubblicare solo dallo schema predefinito creato da Amazon DataZone per quell'ambiente. Gli utenti dell'ambiente creato utilizzando questi profili di ambiente non possono fornire i propri parametri Amazon Redshift.
  - Non consentire la pubblicazione: se scegli questa opzione, gli ambienti creati utilizzando questo profilo di ambiente possono essere utilizzati solo per la sottoscrizione e il consumo di dati. Gli ambienti non possono essere utilizzati affatto per pubblicare dati.

Se hai specificato il blueprint Data Lake, procedi come segue:

- Nella sezione dei parametri AWS dell'account, specifica il numero di AWS account e la regione AWS dell'account in cui verranno creati i potenziali ambienti.

- Nella sezione Progetti autorizzati, specifica i progetti che possono utilizzare il profilo di ambiente con il profilo di ambiente Data Lake integrato per la creazione di ambienti. Per impostazione predefinita, tutti i progetti all'interno del dominio possono utilizzare il blueprint data lake nell'account per creare profili ambientali. Per mantenere questa impostazione predefinita, scegli Tutti i progetti. Tuttavia, puoi limitare questo problema assegnando progetti al blueprint. A tale scopo, scegli Solo progetti autorizzati e quindi specifica i progetti che possono utilizzare questo profilo di progetto per creare ambienti.
- Nella sezione Database, scegli Qualsiasi database per abilitare la pubblicazione da qualsiasi database all'interno dell' AWS account e della regione in cui è stato creato l'ambiente oppure scegli Solo database predefinito per abilitare la pubblicazione solo dal database di pubblicazione predefinito creato con l'ambiente.

5. Scegli Crea profilo di ambiente.

Modifica un profilo ambientale

In Amazon DataZone, un profilo di ambiente è un modello che puoi utilizzare per creare ambienti. Per ulteriori informazioni, consulta DataZone Terminologia e concetti di Amazon. Per modificare i profili di ambiente esistenti in un DataZone dominio Amazon, devi appartenere a un DataZone progetto Amazon.

Per modificare un profilo ambientale

1. Vai all'URL del portale DataZone dati di Amazon e accedi utilizzando Single Sign-On (SSO) o le tue credenziali. AWS Se sei un DataZone amministratore Amazon, puoi accedere alla DataZone console Amazon all'indirizzo https://console.aws.amazon.com/datazone e accedere con il Account AWS luogo in cui è stato creato il dominio, quindi scegliere Open data portal.
2. All'interno del portale dati, scegli Sfoglia progetti e seleziona il progetto in cui desideri modificare il profilo dell'ambiente.
3. Passa alla scheda Ambienti all'interno del progetto, quindi scegli Profili ambientali e quindi scegli il profilo di ambiente che desideri modificare.

   Se stai modificando un profilo di ambiente Data Warehouse, puoi modificare solo il nome e la descrizione di un profilo di ambiente esistente.

Se stai modificando un profilo di ambiente Data Lake, puoi modificare il nome e la descrizione del profilo e puoi anche modificare i progetti autorizzati a utilizzare questo profilo per creare ambienti e modificare database. Per modificare queste impostazioni, procedi come segue:

- Nella sezione Progetti autorizzati, specifica i progetti che possono utilizzare il profilo di ambiente con il profilo di ambiente Data Lake integrato per creare ambienti. Per impostazione predefinita, tutti i progetti all'interno del dominio possono utilizzare il blueprint data lake nell'account per creare profili ambientali. Per mantenere questa impostazione predefinita, scegli Tutti i progetti. Tuttavia, puoi limitare questo problema assegnando progetti al blueprint. A tale scopo, scegli Solo progetti autorizzati e quindi specifica i progetti che possono utilizzare questo profilo di progetto per creare ambienti.
- Nella sezione Database, scegli Qualsiasi database per abilitare la pubblicazione da qualsiasi database all'interno dell' AWS account e della regione in cui è stato creato l'ambiente oppure scegli Solo database predefinito per abilitare la pubblicazione solo dal database di pubblicazione predefinito creato con l'ambiente.

Una volta completate le modifiche, scegli Modifica profilo di ambiente.

Elimina un profilo ambientale

In Amazon DataZone, un profilo di ambiente è un modello che puoi utilizzare per creare ambienti. Lo scopo di un profilo ambientale è semplificare la creazione dell'ambiente incorporando informazioni di posizionamento come AWS account e regione all'interno dei profili. Per ulteriori informazioni, consulta DataZone Terminologia e concetti di Amazon. Per eliminare i profili di ambiente in un DataZone dominio Amazon, devi appartenere a un DataZone progetto Amazon.

> **Note**
>
> Quando elimini un profilo di ambiente, non puoi creare altri ambienti utilizzando questo profilo.

Per eliminare un profilo di ambiente

1. Vai all'URL del portale DataZone dati di Amazon e accedi utilizzando Single Sign-On (SSO) o le tue credenziali. AWS Se sei un DataZone amministratore Amazon, puoi accedere alla

DataZone console Amazon all'indirizzo https://console.aws.amazon.com/datazone e accedere con il Account AWS luogo in cui è stato creato il dominio, quindi scegliere Open data portal.

2. All'interno del portale dati, scegli Sfoglia progetti e seleziona il progetto in cui desideri eliminare il profilo ambientale.
3. Passa alla scheda Ambienti all'interno del progetto, quindi scegli Profili ambientali e quindi scegli il profilo di ambiente che desideri eliminare.
4. Seleziona il profilo ambientale che desideri eliminare, quindi scegli Azioni, Elimina e conferma l'eliminazione.

Creazione di un nuovo ambiente

Nei DataZone progetti Amazon, gli ambienti sono raccolte di risorse configurate (ad esempio, un bucket Amazon S3, un database AWS Glue o un gruppo di lavoro Amazon Athena), con un determinato set di principi IAM (ruoli utente ambientali) con autorizzazioni di proprietario o collaboratore assegnate che possono operare su tali risorse. Per ulteriori informazioni, consulta DataZone Terminologia e concetti di Amazon.

Qualsiasi DataZone utente Amazon con le autorizzazioni necessarie per accedere al portale dati può creare un DataZone ambiente Amazon all'interno di un progetto.

Per creare un nuovo ambiente, completa i seguenti passaggi.

1. Vai all'URL del portale DataZone dati di Amazon e accedi utilizzando Single Sign-On (SSO) o le tue credenziali. AWS Se sei un DataZone amministratore Amazon, puoi accedere alla DataZone console Amazon all'indirizzo https://console.aws.amazon.com/datazone e accedere con il Account AWS luogo in cui è stato creato il dominio, quindi scegliere Open data portal.
2. Scegli Sfoglia tutti i progetti e seleziona il progetto in cui desideri creare un nuovo ambiente.
3. Scegli Crea ambiente, specifica i valori per i seguenti campi, quindi scegli Crea ambiente:

   - Nome: il nome dell'ambiente
   - Descrizione: una descrizione dell'ambiente
   - Profilo ambientale: scegli un profilo di ambiente esistente o creane uno nuovo. Un profilo di ambiente è un modello che è possibile utilizzare per creare ambienti. Per ulteriori informazioni, consulta DataZone Terminologia e concetti di Amazon.

     Dopo aver selezionato il profilo di ambiente, nella sezione Parametri, specificate i valori per i campi che fanno parte di questo profilo di ambiente.

Modifica un ambiente

Nei DataZone progetti Amazon, gli ambienti sono raccolte di risorse configurate (ad esempio, un bucket Amazon S3, un database AWS Glue o un gruppo di lavoro Amazon Athena), con un determinato set di principali IAM (con autorizzazioni di collaborazione assegnate) che possono operare su tali risorse. Per ulteriori informazioni, consulta DataZone Terminologia e concetti di Amazon.

Qualsiasi DataZone utente Amazon con le autorizzazioni necessarie per accedere al portale dati può modificare un DataZone ambiente Amazon all'interno di un progetto.

Per modificare un ambiente esistente, completa i seguenti passaggi.

1. Vai all'URL del portale DataZone dati di Amazon e accedi utilizzando Single Sign-On (SSO) o le tue credenziali. AWS Se sei un DataZone amministratore Amazon, puoi accedere alla DataZone console Amazon all'indirizzo https://console.aws.amazon.com/datazone e accedere con il Account AWS luogo in cui è stato creato il dominio, quindi scegliere Open data portal.
2. Scegli Sfoglia progetti dal pannello di navigazione in alto e seleziona il progetto che contiene l'ambiente che desideri modificare.
3. Individua e scegli l'ambiente per aprirne la pagina dei dettagli. Quindi espandi Azioni e scegli Modifica ambiente.
4. Apporta le modifiche al nome e alla descrizione dell'ambiente, quindi scegli Salva modifiche.

Elimina un ambiente

Nei DataZone progetti Amazon, gli ambienti sono raccolte di risorse configurate (ad esempio, un bucket Amazon S3, un database AWS Glue o un gruppo di lavoro Amazon Athena), con un determinato set di principali IAM (con autorizzazioni di collaborazione assegnate) che possono operare su tali risorse. Per ulteriori informazioni, consulta DataZone Terminologia e concetti di Amazon.

Qualsiasi DataZone utente Amazon con le autorizzazioni necessarie per accedere al portale dati può eliminare un DataZone ambiente Amazon all'interno di un progetto.

Per eliminare un ambiente esistente, completa i seguenti passaggi.

1. Vai all'URL del portale DataZone dati di Amazon e accedi utilizzando Single Sign-On (SSO) o le tue credenziali. AWS Se sei un DataZone amministratore Amazon, puoi accedere alla

DataZone console Amazon all'indirizzo https://console.aws.amazon.com/datazone e accedere con il Account AWS luogo in cui è stato creato il dominio, quindi scegliere Open data portal.

2. Scegli Sfoglia progetto dal pannello di navigazione in alto e seleziona il progetto che contiene l'ambiente che desideri eliminare.
3. Individua e scegli l'ambiente per aprirne la pagina dei dettagli, quindi espandi Azioni e scegli Elimina ambiente.
4. Nella finestra pop-up Elimina ambiente, conferma l'eliminazione digitando `Delete` nel campo e quindi scegli Elimina ambiente.

   È possibile eliminare con successo un ambiente solo dopo che tutte le entità con una dipendenza da questo ambiente sono state eliminate. Per eliminare un ambiente, devi prima eliminare tutte le fonti di dati e gli obiettivi di sottoscrizione associati.

Crea un nuovo progetto

In Amazon DataZone, i progetti consentono a un gruppo di utenti di collaborare su vari casi d'uso aziendali che prevedono la pubblicazione, la scoperta, la sottoscrizione e il consumo di risorse di dati nel catalogo Amazon DataZone . Per ulteriori informazioni, consulta DataZone Terminologia e concetti di Amazon.

Qualsiasi DataZone utente Amazon con le autorizzazioni necessarie per accedere al portale dati può creare un DataZone progetto Amazon.

Per creare un nuovo progetto, completa i seguenti passaggi.

1. Vai all'URL del portale DataZone dati di Amazon e accedi utilizzando Single Sign-On (SSO) o le tue credenziali. AWS Se sei un DataZone amministratore Amazon, puoi accedere alla DataZone console Amazon all'indirizzo https://console.aws.amazon.com/datazone e accedere con il Account AWS luogo in cui è stato creato il dominio, quindi scegliere Open data portal.
2. Nel portale DataZone dati Amazon, scegli Crea progetto.
3. Specificate i valori per i seguenti campi, quindi scegliete Crea progetto:

   - Nome: il nome del progetto.
   - Descrizione: una descrizione del progetto.

Modifica progetto

In Amazon DataZone, i progetti consentono a un gruppo di utenti di collaborare su vari casi d'uso aziendali che prevedono la pubblicazione, la scoperta, la sottoscrizione e il consumo di risorse di dati nel catalogo Amazon DataZone . Per ulteriori informazioni, consulta DataZone Terminologia e concetti di Amazon. Per modificare un DataZone progetto Amazon, devi essere il proprietario di quel progetto o l'amministratore di dominio del dominio che contiene questo progetto.

Per modificare un progetto esistente, completa i seguenti passaggi.

1. Vai all'URL del portale DataZone dati di Amazon e accedi utilizzando Single Sign-On (SSO) o le tue credenziali. AWS Se sei un DataZone amministratore Amazon, puoi accedere alla DataZone console Amazon all'indirizzo https://console.aws.amazon.com/datazone e accedere con il Account AWS luogo in cui è stato creato il dominio, quindi scegliere Open data portal.
2. Scegli Sfoglia progetti.
3. Scegli il progetto che desideri modificare. Se non lo vedi subito nell'elenco dei progetti, puoi cercarlo specificando il nome del progetto nel campo Trova progetto.
4. Espandi Azioni e scegli Modifica progetto.
5. Aggiorna il nome e la descrizione del progetto, quindi scegli Salva.

Eliminare il progetto

In Amazon DataZone, i progetti consentono a un gruppo di utenti di collaborare su vari casi d'uso aziendali che prevedono la pubblicazione, la scoperta, la sottoscrizione e/o il consumo di risorse di dati nel catalogo Amazon DataZone . Per ulteriori informazioni, consulta DataZone Terminologia e concetti di Amazon.

L'operazione di eliminazione di un progetto è definitiva. L'eliminazione elimina irrevocabilmente i contenuti del progetto, comprese le fonti di dati, gli ambienti, le risorse, i glossari e i moduli di metadati. Amazon DataZone revoca le sovvenzioni che DataZone Amazon ha concesso agli asset gestiti tramite Lake Formation e Amazon Redshift. L'eliminazione di un progetto non elimina DataZone AWS le risorse non Amazon che Amazon DataZone potrebbe averti aiutato a creare. Se non ti servono più queste AWS risorse, eliminale nei rispettivi AWS servizi e account.

Per eliminare un DataZone progetto Amazon, devi essere il proprietario del progetto.

Per eliminare un progetto esistente, completa i seguenti passaggi.

1. Vai all'URL del portale DataZone dati di Amazon e accedi utilizzando Single Sign-On (SSO) o le tue credenziali. AWS Un responsabile IAM può accedere alla DataZone console Amazon all'indirizzo https://console.aws.amazon.com/datazone e accedere con il Account AWS luogo in cui è stato creato il dominio, quindi scegliere Open data portal.
2. Scegli Sfoglia progetti dal pannello di navigazione in alto.
3. Scegli il progetto che desideri eliminare. Se non lo vedi nell'elenco dei progetti, puoi cercarlo specificando il nome del progetto nel campo Trova progetto.
4. Espandi Azioni e scegli Elimina progetto.

   Consulta gli avvisi informativi sul potenziale impatto dell'eliminazione del progetto.
5. Se accetti gli avvisi, digita il testo di conferma e scegli Elimina.

> **Important**
>
> L'eliminazione di un progetto è un'azione irrevocabile che non può essere annullata né da te né da. AWS

> **Note**
>
> Quando tu o gli utenti del tuo dominio create un ambiente in un progetto, Amazon DataZone crea AWS risorse nel tuo dominio o negli account associati per fornire funzionalità a te e agli utenti del dominio. Di seguito è riportato l'elenco delle AWS risorse che Amazon DataZone può creare per un progetto, insieme al nome predefinito. L'eliminazione di un progetto non elimina nessuna di queste AWS risorse dai tuoi AWS account.
>
> - <environmentId>Ruoli IAM: datazone_usr_.
> - <environmentName>Database Glue: (1) <environmentName>_pub_db-*, (2) _sub_db-*. Se esisteva già un database con questo nome, Amazon DataZone aggiungerà l'ID dell'ambiente.
> - <environmentName>Gruppi di lavoro Athena: -*. Se esisteva già un gruppo di lavoro con questo nome, Amazon DataZone aggiungerà l'ID dell'ambiente.
> - CloudWatch gruppo di log: datazone_ <environmentId>

Abbandona il progetto

In Amazon DataZone, i progetti consentono a un gruppo di utenti di collaborare su vari casi d'uso aziendali che prevedono la pubblicazione, la scoperta, la sottoscrizione e il consumo di risorse di dati nel catalogo Amazon DataZone . Per ulteriori informazioni, consulta DataZone Terminologia e concetti di Amazon.

Per abbandonare un progetto esistente, completa i seguenti passaggi.

1. Vai all'URL del portale DataZone dati di Amazon e accedi utilizzando Single Sign-On (SSO) o le tue credenziali. AWS Se sei un DataZone amministratore Amazon, puoi accedere alla DataZone console Amazon all'indirizzo https://console.aws.amazon.com/datazone e accedere con il Account AWS luogo in cui è stato creato il dominio, quindi scegliere Open data portal.
2. Scegli Seleziona progetto dal pannello di navigazione in alto e seleziona il progetto.
3. Scegli il progetto che vuoi abbandonare. Se non lo vedi subito nell'elenco dei progetti, puoi cercarlo specificando il nome del progetto nel campo Trova progetto.
4. Espandi Azioni e scegli Abbandona progetto.

Aggiungi membri a un progetto

In Amazon DataZone, i progetti consentono a un gruppo di utenti di collaborare su vari casi d'uso aziendali che prevedono la pubblicazione, la scoperta, la sottoscrizione e il consumo di risorse di dati nel catalogo Amazon DataZone . Per ulteriori informazioni, consulta DataZone Terminologia e concetti di Amazon.

Devi essere il proprietario o il collaboratore del progetto per aggiungere membri a un progetto. Puoi aggiungere gruppi SSO, utenti SSO o responsabili IAM (ruoli o utenti) come membri del progetto.

Per aggiungere membri a un progetto esistente, completa i passaggi seguenti.

1. Vai all'URL del portale DataZone dati di Amazon e accedi utilizzando Single Sign-On (SSO) o le tue credenziali. AWS Se sei un DataZone amministratore Amazon, puoi accedere alla DataZone console Amazon all'indirizzo https://console.aws.amazon.com/datazone e accedere con il Account AWS luogo in cui è stato creato il dominio, quindi scegliere Open data portal.
2. Scegli Seleziona progetto dal pannello di navigazione in alto e seleziona il progetto.
3. Scegli il progetto a cui vuoi aggiungere membri. Se non lo vedi subito nell'elenco dei progetti, puoi cercarlo specificando il nome del progetto nel campo Trova progetto.

4. Nella pagina dei dettagli del progetto, seleziona la scheda Membri e scegli il nodo Tutti i membri.
5. Nella scheda Membri del progetto, scegli Aggiungi membri.
6. Nella finestra pop-up Aggiungi membri al progetto, specifica gli utenti che desideri aggiungere e specifica il loro ruolo all'interno del progetto (proprietario o collaboratore), quindi scegli Aggiungi membri.

> **Note**
>
> Puoi aggiungere un responsabile IAM come membro del progetto se tale responsabile ha già un profilo DataZone utente Amazon nel dominio. Amazon crea DataZone automaticamente un profilo utente per un principale IAM quando interagisce con successo con il dominio tramite il portale, l'API o la CLI. Non puoi creare un profilo utente per un principale IAM. Per aggiungere i principali IAM come membri del progetto nel caso in cui il principale IAM non disponga di un profilo DataZone utente Amazon esistente nel dominio, chiedi al tuo amministratore di aggiungere le seguenti due autorizzazioni IAM a quelle del tuo dominio AmazonDataZoneDomainExecutionRolenella console IAM: `iam:GetUser` e. `iam:GetRole` Separatamente, per eseguire azioni nel dominio, il responsabile IAM deve disporre delle autorizzazioni IAM corrispondenti per tali azioni.

Rimuovere membri da un progetto

In Amazon DataZone, i progetti consentono a un gruppo di utenti di collaborare su vari casi d'uso aziendali che prevedono la pubblicazione, la scoperta, la sottoscrizione e il consumo di risorse di dati nel catalogo Amazon DataZone . Per ulteriori informazioni, consulta DataZone Terminologia e concetti di Amazon. Devi essere il proprietario del progetto per rimuovere membri da un progetto.

Per rimuovere membri da un progetto esistente, completa i seguenti passaggi.

1. Accedi al portale DataZone dati di Amazon utilizzando l'URL del portale dati e accedi utilizzando il tuo SSO o AWS le tue credenziali. Se sei un DataZone amministratore Amazon, puoi ottenere l'URL del portale dati accedendo alla DataZone console Amazon all'indirizzo https://console.aws.amazon.com/datazone nell' AWS account in cui è stato creato il DataZone dominio Amazon.
2. Scegli Seleziona progetto dal pannello di navigazione in alto e seleziona il progetto.

3. Scegli il progetto in cui desideri rimuovere i membri. Se non lo vedi subito nell'elenco dei progetti, puoi cercarlo specificando il nome del progetto nel campo Trova progetto.
4. Nella pagina dei dettagli del progetto, seleziona la scheda Membri e scegli il nodo Tutti i membri.
5. Nella scheda Membri del progetto, scegli i membri che desideri rimuovere dal progetto, quindi scegli Rimuovi.
6. Nella finestra pop-up Rimuovi membri, conferma la rimozione scegliendo Rimuovi membri.

Creazione di inventario e pubblicazione di dati in Amazon DataZone

Questa sezione descrive le attività e le procedure che desideri eseguire per creare un inventario dei tuoi dati in Amazon DataZone e pubblicare i tuoi dati su Amazon DataZone.

Per utilizzare Amazon per DataZone catalogare i tuoi dati, devi prima importare i tuoi dati (asset) come inventario del tuo progetto in Amazon DataZone. La creazione di un inventario per un particolare progetto rende le risorse individuabili solo dai membri di quel progetto. Le risorse dell'inventario del progetto non sono disponibili per tutti gli utenti del dominio in search/browse a meno che non vengano pubblicate esplicitamente. Dopo aver creato un inventario del progetto, i proprietari dei dati possono curare le proprie risorse di inventario con i metadati aziendali richiesti aggiungendo o aggiornando nomi aziendali (asset e schema), descrizioni (asset e schema), readme, termini del glossario (risorsa e schema) e moduli di metadati.

Il passaggio successivo dell'utilizzo di Amazon DataZone per catalogare i dati consiste nel rendere le risorse di inventario del progetto individuabili dagli utenti del dominio. Puoi farlo pubblicando le risorse di inventario nel DataZone catalogo Amazon. Solo la versione più recente della risorsa di inventario può essere pubblicata nel catalogo e solo l'ultima versione pubblicata è attiva nel catalogo Discovery. Se una risorsa di inventario viene aggiornata dopo la sua pubblicazione nel DataZone catalogo Amazon, devi pubblicarla nuovamente in modo esplicito affinché la versione più recente sia presente nel catalogo Discovery.

Argomenti

- Avvia manualmente un'origine dati eseguita in Amazon DataZone
- Revisioni degli asset in Amazon DataZone
- Qualità dei dati in Amazon DataZone
- Utilizzo dell'apprendimento automatico e dell'intelligenza artificiale generativa

Configura le autorizzazioni di Lake Formation per Amazon DataZone

Quando crei un ambiente utilizzando il data lake blueprint integrato (DefaultDataLake), viene aggiunto un database AWS Glue in Amazon DataZone come parte del processo di creazione di questo ambiente. Se desideri pubblicare risorse da questo database AWS Glue, non sono necessarie autorizzazioni aggiuntive.

Tuttavia, se desideri pubblicare risorse e sottoscrivere risorse da un database AWS Glue che esiste al di fuori del tuo DataZone ambiente Amazon, devi fornire esplicitamente ad Amazon DataZone le autorizzazioni per accedere alle tabelle in questo database AWS Glue esterno. A tale scopo, è necessario completare le seguenti impostazioni in AWS Lake Formation e allegare le autorizzazioni necessarie per Lake Formation a. AmazonDataZoneGlueAccess- <region>- <domainId>

- Configura la posizione Amazon S3 per il tuo data lake in AWS Lake Formation con la modalità di autorizzazione Lake Formation o la modalità di accesso ibrida. Per ulteriori informazioni, consulta https://docs.aws.amazon.com/lake-formation/latest/dg/ register-data-lake .html.
- Rimuovi l'`IAMAllowedPrincipals`autorizzazione dalle tabelle di Amazon Lake Formation per le quali Amazon DataZone gestisce le autorizzazioni. Per ulteriori informazioni, consulta https://docs.aws.amazon.com/lake-formation/latest/dg/ upgrade-glue-lake-formation -background.html.
- Allega le seguenti autorizzazioni AWS Lake Formation a: AmazonDataZoneGlueAccess- <region>- <domainId>
  - `Describe`e `Describe grantable` autorizzazioni sul database in cui esistono le tabelle
  - `Describe`,`Select`,`Describe Grantable`, `Select Grantable` autorizzazioni su tutte le tabelle del database di cui sopra a cui desideri gestire l'accesso DataZone per tuo conto.

> **Note**
>
> Amazon DataZone supporta la modalità AWS Lake Formation Hybrid. La modalità ibrida Lake Formation ti consente di iniziare a gestire le autorizzazioni sui tuoi database e tabelle

AWS Glue tramite Lake Formation, continuando al contempo a mantenere le autorizzazioni IAM esistenti su queste tabelle e database. Per ulteriori informazioni, consulta DataZone Integrazione di Amazon con la modalità ibrida AWS Lake Formation

Per ulteriori informazioni, consulta Risoluzione dei problemi relativi alle autorizzazioni di AWS Lake Formation per Amazon DataZone.

DataZone Integrazione di Amazon con la modalità ibrida AWS Lake Formation

Amazon DataZone è integrato con la modalità ibrida AWS Lake Formation. Questa integrazione ti consente di pubblicare e condividere facilmente le tue tabelle AWS Glue tramite Amazon DataZone senza la necessità di registrarle prima in AWS Lake Formation. La modalità ibrida ti consente di iniziare a gestire le autorizzazioni sulle tue tabelle AWS Glue tramite AWS Lake Formation continuando a mantenere le autorizzazioni IAM esistenti su queste tabelle.

Per iniziare, puoi abilitare l'impostazione di registrazione della posizione dei dati nel DefaultDataLakeblueprint nella console di DataZone gestione Amazon.

Abilita l'integrazione con la modalità ibrida AWS Lake Formation

1. Accedi alla DataZone console Amazon all'indirizzo https://console.aws.amazon.com/datazone e accedi con le credenziali del tuo account.
2. Scegli Visualizza domini e scegli il dominio in cui desideri abilitare l'integrazione con la modalità ibrida AWS Lake Formation.
3. Nella pagina dei dettagli del dominio, vai alla scheda Blueprints.
4. Dall'elenco Blueprint, scegli il DefaultDataLakeblueprint.
5. Assicurati che il DefaultDataLake blueprint sia abilitato. Se non è abilitato, segui i passaggi indicati Abilita i blueprint integrati nell' AWS account che possiede il dominio Amazon DataZone per abilitarlo nel tuo AWS account.
6. Nella pagina dei DefaultDataLake dettagli, apri la scheda Provisioning e scegli il pulsante Modifica nell'angolo in alto a destra della pagina.
7. In Registrazione della posizione dei dati, seleziona la casella per abilitare la registrazione della posizione dei dati.
8. Per il ruolo di gestione della posizione dei dati, puoi creare un nuovo ruolo IAM o selezionare un ruolo IAM esistente. Amazon DataZone utilizza questo ruolo per gestire l'accesso in lettura/

scrittura ai bucket Amazon S3 scelti per Data Lake utilizzando la modalità di accesso ibrida Lake AWS Formation. Per ulteriori informazioni, consulta AmazonDataZone<region>Gestione S3- - <domainId>.

9. Facoltativamente, puoi scegliere di escludere determinate sedi Amazon S3 se non desideri che DataZone Amazon le registri automaticamente in modalità ibrida. A tal fine, completa i seguenti passaggi:

   - Scegli il pulsante di attivazione/disattivazione per escludere località Amazon S3 specificate.
   - Fornisci l'URI del bucket Amazon S3 che desideri escludere.
   - Per aggiungere altri bucket, scegli Aggiungi posizione S3.

   > **Note**
   >
   > Amazon consente DataZone solo l'esclusione di una posizione S3 root. Qualsiasi posizione S3 all'interno del percorso di una posizione S3 principale verrà automaticamente esclusa dalla registrazione.

   - Seleziona Salvataggio delle modifiche.

Dopo aver abilitato l'impostazione di registrazione della posizione dei dati nel tuo AWS account, quando un consumatore di dati si iscrive a una tabella AWS Glue gestita tramite le autorizzazioni IAM, Amazon DataZone registra prima le posizioni Amazon S3 di questa tabella in modalità ibrida, quindi concede l'accesso al consumatore di dati gestendo le autorizzazioni sulla tabella tramite Lake Formation. AWS Ciò garantisce che le autorizzazioni IAM sulla tabella continuino a esistere con le autorizzazioni AWS Lake Formation appena concesse, senza interrompere i flussi di lavoro esistenti.

Come gestire le posizioni crittografate di Amazon S3 quando si abilita l'integrazione in modalità ibrida AWS Lake Formation in Amazon DataZone

Se utilizzi una posizione Amazon S3 crittografata con una chiave KMS gestita dal cliente o AWS gestita dal cliente, il ruolo AmazonDataZoneS3Manage deve avere l'autorizzazione a crittografare e decrittografare i dati con la chiave KMS oppure la politica della chiave KMS deve concedere le autorizzazioni sulla chiave per il ruolo.

Se la tua posizione Amazon S3 è crittografata con una chiave AWS gestita, aggiungi la seguente policy in linea al ruolo: AmazonDataZoneDataLocationManagement

```
 {
"Version": "2012-10-17",
"Statement": [
  {
    "Effect": "Allow",
    "Action": [
      "kms:Encrypt",
      "kms:Decrypt",
      "kms:ReEncrypt*",
      "kms:GenerateDataKey*",
      "kms:DescribeKey"
    ],
    "Resource": "<AWS managed key ARN>"
  }
]
```

Se la tua posizione Amazon S3 è crittografata con una chiave gestita dal cliente, procedi come segue:

1. Apri la console AWS KMS all'indirizzo https://console.aws.amazon.com/kms e accedi come utente amministrativo di AWS Identity and Access Management (IAM) o come utente che può modificare la politica chiave della chiave KMS utilizzata per crittografare la posizione.
2. Nel riquadro di navigazione, scegli Customer managed keys, quindi scegli il nome della chiave KMS desiderata.
3. Nella pagina dei dettagli della chiave KMS, scegli la scheda Politica chiave, quindi esegui una delle seguenti operazioni per aggiungere il tuo ruolo personalizzato o il ruolo collegato al servizio Lake Formation come utente chiave KMS:

   - Se viene visualizzata la visualizzazione predefinita (con le sezioni Amministratori chiave, Eliminazione delle chiavi, Utenti chiave e Altri AWS account), nella sezione Utenti chiave, aggiungi il ruolo. AmazonDataZoneDataLocationManagement
   - Se viene visualizzata la politica chiave (JSON), modifica la politica per aggiungere il AmazonDataZoneDataLocationManagementruolo all'oggetto «Consenti l'uso della chiave», come mostrato nell'esempio seguente

     ```
     ...
             {
                 "Sid": "Allow use of the key",
     ```

```
            "Effect": "Allow",
            "Principal": {
                "AWS": [
                    "arn:aws:iam::111122223333:role/service-role/
AmazonDataZoneDataLocationManage-<region>-<domain-id>",
                    "arn:aws:iam::111122223333:user/keyuser"
                ]
            },
            "Action": [
                "kms:Encrypt",
                "kms:Decrypt",
                "kms:ReEncrypt*",
                "kms:GenerateDataKey*",
                "kms:DescribeKey"
            ],
            "Resource": "*"
        },
        ...
```

> **Note**
>
> Se la chiave KMS o la posizione Amazon S3 non si trovano AWS nello stesso account del catalogo dati, segui le istruzioni in Registrazione di una posizione Amazon S3 crittografata tra gli account. AWS

Crea tipi di asset personalizzati

In Amazon DataZone, gli asset rappresentano tipi specifici di risorse di dati come tabelle di database, dashboard o modelli di machine learning. Per garantire coerenza e standardizzazione nella descrizione degli asset del catalogo, un DataZone dominio Amazon deve disporre di una serie di tipi di asset che definiscono il modo in cui gli asset sono rappresentati nel catalogo. Un tipo di risorsa definisce lo schema per un tipo specifico di risorsa. Un tipo di risorsa ha una serie di tipi di modulo di metadati nominabili obbligatori e facoltativi (ad esempio, GovForm o). GovernanceFormType I tipi di asset in Amazon DataZone sono suddivisi in versioni. Quando le risorse vengono create, vengono convalidate in base allo schema definito dal tipo di risorsa (in genere la versione più recente) e, se viene specificata una struttura non valida, la creazione delle risorse fallisce.

Tipi di asset di sistema: Amazon DataZone fornisce tipi di asset di sistema di proprietà del servizio (inclusi GlueTableAssetType GlueViewAssetType, RedshiftTableAssetType RedshiftViewAssetType, e S3ObjectCollectionAssetType) e tipi di moduli di sistema (tra cui DataSourceReferenceFormType AssetCommonDetailsFormType, e). SubscriptionTermsFormType I tipi di risorse di sistema non possono essere modificati.

Tipi di risorse personalizzati: per creare tipi di risorse personalizzati, iniziate creando i tipi di modulo di metadati e i glossari richiesti da utilizzare nei tipi di modulo. È quindi possibile creare tipi di risorse personalizzati specificando il nome, la descrizione e i moduli di metadati associati, che possono essere obbligatori o facoltativi.

Per i tipi di risorse con dati strutturati, per rappresentare lo schema a colonne nel portale dati, puoi utilizzare il `RelationalTableFormType` per aggiungere i metadati tecnici alle colonne (inclusi nomi di colonne, descrizioni e tipi di dati) e `ColumnBusinessMetadataForm` per aggiungere le descrizioni aziendali delle colonne, inclusi nomi aziendali, termini del glossario e coppie di valori chiave personalizzate.

Per creare un tipo di risorsa personalizzato tramite il portale Data, completa i seguenti passaggi:

1. Vai all'URL del portale DataZone dati di Amazon e accedi utilizzando Single Sign-On (SSO) o le tue credenziali. AWS Se sei un DataZone amministratore Amazon, puoi accedere alla DataZone console Amazon all'indirizzo https://console.aws.amazon.com/datazone e accedere con il Account AWS luogo in cui è stato creato il dominio, quindi scegliere Open data portal.
2. Scegli Seleziona progetto dal pannello di navigazione in alto e seleziona il progetto in cui desideri creare un tipo di risorsa personalizzato.
3. Vai alla scheda Dati per il progetto.
4. Scegli Tipi di risorse dal riquadro di navigazione a sinistra, quindi scegli Crea tipo di risorsa.
5. Specificate quanto segue e quindi scegliete Crea.
   - Nome: il nome del tipo di risorsa personalizzato
   - Descrizione: la descrizione del tipo di risorsa personalizzata.
   - Scegliete Aggiungi moduli di metadati per aggiungere moduli di metadati a questo tipo di risorsa personalizzato.
6. Una volta creato il tipo di risorsa personalizzato, puoi utilizzarlo per creare risorse.

Per creare un tipo di risorsa personalizzato tramite le API, completa i seguenti passaggi:

1. Crea un tipo di modulo di metadati richiamando l'`CreateFormType`eazione API.

   Di seguito è riportato un SageMaker esempio di Amazon:

```
m_model = "

structure SageMakerModelFormType {
   @required
   @amazon.datazone#searchable
   modelName: String

   @required
   modelArn: String

   @required
   creationTime: String
}
"

CreateFormType(
    domainIdentifier="my-dz-domain",
    owningProjectIdentifier="d4bywm0cja1dbb",
    name="SageMakerModelFormType",
    model=m_model
    status="ENABLED"
    )
```

2. Successivamente, puoi creare un tipo di risorsa richiamando l'azione `CreateAssetType` API. Puoi creare tipi di asset solo tramite le DataZone API di Amazon utilizzando i tipi di modulo di sistema disponibili (`SubscriptionTermsFormType`nell'esempio seguente) o i tipi di modulo personalizzati. Per i tipi di modulo di sistema, il nome del tipo deve iniziare con`amazon.datazone`.

```
CreateAssetType(
    domainIdentifier="my-dz-domain",
    owningProjectIdentifier="d4bywm0cja1dbb",
    name="SageMakerModelAssetType",
    formsInput={
        "ModelMetadata": {
```

```
            "typeIdentifier": "SageMakerModelMetadataFormType",
            "typeRevision": 7,
            "required": True,
        },
        "SubscriptionTerms": {
            "typeIdentifier": "amazon.datazone.SubscriptionTermsFormType",
            "typeRevision": 1,
            "required": False,
        },
    },
)
```

Di seguito è riportato un esempio di creazione di un tipo di risorsa per dati strutturati:

```
CreateAssetType(
    domainIdentifier="my-dz-domain",
    owningProjectIdentifier="d4bywm0cja1dbb",
    name="OnPremMySQLAssetType",
    formsInput={
        "OnpremMySQLForm": {
            "typeIdentifier": "OnpremMySQLFormType",
            "typeRevision": 5,
            "required": True,
        },
        "RelationalTableForm": {
            "typeIdentifier": "RelationalTableFormType",
            "typeRevision": 1,
            "required": True,
        },
        "ColumnBusinessMetadataForm": {
            "typeIdentifier": "ColumnBusinessMetadataForm",
            "typeRevision": 1,
            "required": False,
        },
        "SubscriptionTerms": {
            "typeIdentifier": "SubscriptionTermsFormType",
            "typeRevision": 1,
            "required": False,
        },
    },
```

```
)
```

3. E ora puoi creare una risorsa utilizzando i tipi di risorse personalizzati che hai creato nei passaggi precedenti.

```
CreateAsset(
   domainIdentifier="my-dz-domain",
   owningProjectIdentifier="d4bywm0cja1dbb",
   owningProjectIdentifier="my-project",
   name="MyModelAsset",
   glossaryTerms="xxx",
   formsInput=[{
        "formName": "SageMakerModelForm",
        "typeIdentifier": "SageMakerModelForm",
        "typeRevision": "5",
        "content": "{\n \"ModelName\" : \"sample-ModelName\",\n \"ModelArn\" :
 \"999999911111\"\n}"
        }
        ]
)
```

E in questo esempio stai creando una risorsa di dati strutturati:

```
CreateAsset(
   domainIdentifier="my-dz-domain",
   owningProjectIdentifier="d4bywm0cja1dbb",
   name="MyModelAsset",
   glossaryTerms="xxx",
   formsInput=[{
        "formName": "RelationalTableForm",
        "typeIdentifier": "amazon.datazone.RelationalTableForm",
        "typeRevision": "1",
        "content": ".."
        },
        {
        "formName": "mySQLTableForm",
        "typeIdentifier": "mySQLTableForm",
        "typeRevision": "6",
```

```
        "content": ".."
        },
        {
        "formName": "mySQLTableForm",
        "typeIdentifier": "mySQLTableForm",
        "typeRevision": "1",
        "content": ".."
        },
        .....
        ]
)
```

Crea ed esegui un'origine DataZone dati Amazon per AWS Glue Data Catalog

In Amazon DataZone, puoi creare un'origine AWS Glue Data Catalog dati da cui importare i metadati tecnici delle tabelle del database. AWS Glue Per aggiungere una fonte di dati per AWS Glue Data Catalog, il database di origine deve già esistere in AWS Glue.

Quando crei ed AWS Glue esegui un'origine dati, aggiungi risorse dal AWS Glue database di origine all'inventario del tuo DataZone progetto Amazon. Puoi eseguire le tue fonti di AWS Glue dati secondo una pianificazione prestabilita o su richiesta per creare o aggiornare i metadati tecnici delle tue risorse. Durante l'esecuzione dell'origine dati, puoi facoltativamente scegliere di pubblicare le tue risorse nel DataZone catalogo Amazon e renderle così rilevabili da tutti gli utenti del dominio. Puoi anche pubblicare le risorse di inventario del progetto dopo aver modificato i relativi metadati aziendali. Gli utenti del dominio possono cercare e scoprire le risorse pubblicate e richiedere abbonamenti a tali risorse.

Per aggiungere una fonte di AWS Glue dati

1. Vai all'URL del portale DataZone dati di Amazon e accedi utilizzando Single Sign-On (SSO) o le tue credenziali. AWS Se sei un DataZone amministratore Amazon, puoi accedere alla DataZone console Amazon all'indirizzo https://console.aws.amazon.com/datazone e accedere con il Account AWS luogo in cui è stato creato il dominio, quindi scegliere Open data portal.
2. Scegli Seleziona progetto dal pannello di navigazione in alto e seleziona il progetto a cui desideri aggiungere la fonte di dati.
3. Vai alla scheda Dati per il progetto.

4. Scegli Origini dati dal riquadro di navigazione a sinistra, quindi scegli Crea origine dati.
5. Configura i campi seguenti:

   - Nome: il nome dell'origine dati.
   - Descrizione: la descrizione dell'origine dati.
6. In Tipo di origine dati, scegli AWS Glue.
7. In Seleziona un ambiente, specifica un ambiente in cui pubblicare le AWS Glue tabelle.
8. In Selezione dei dati, fornisci un AWS Glue database e inserisci i criteri di selezione della tabella. Ad esempio, se scegliete Includi e immettete`*corporate`, il database includerà tutte le tabelle di origine che terminano con la parola`corporate`.

   Puoi scegliere un AWS Glue database dal menu a discesa o digitare un nome per il database. Il menu a discesa include due database: il database di pubblicazione e il database di sottoscrizione dell'ambiente. Se desideri importare risorse da un database non creato dall'ambiente, devi digitare il nome del database invece di selezionarlo dal menu a discesa.

   Puoi aggiungere più regole di inclusione ed esclusione per le tabelle all'interno di un singolo database. È inoltre possibile aggiungere più database utilizzando il pulsante Aggiungi un altro database.

9. In Qualità dei dati, puoi scegliere di Abilita la qualità dei dati per questa fonte di dati. Se lo fai, Amazon DataZone importa l'output di qualità dei dati AWS Glue esistente nel tuo DataZone catalogo Amazon. Per impostazione predefinita, Amazon DataZone importa da AWS Glue gli ultimi 100 report di qualità esistenti senza data di scadenza.

   Le metriche sulla qualità dei dati in Amazon ti DataZone aiutano a comprendere la completezza e l'accuratezza delle tue fonti di dati. Amazon DataZone estrae queste metriche sulla qualità dei dati da AWS Glue per fornire un contesto in un determinato momento, ad esempio durante una ricerca nel catalogo di dati aziendali. Gli utenti dei dati possono vedere come i parametri di qualità dei dati cambiano nel tempo per gli asset sottoscritti. I produttori di dati possono acquisire i punteggi di qualità dei dati di AWS Glue in base a una pianificazione. Il catalogo di dati DataZone aziendali di Amazon può anche visualizzare metriche sulla qualità dei dati provenienti da sistemi di terze parti tramite API per la qualità dei dati. Per ulteriori informazioni, consulta Qualità dei dati in Amazon DataZone
10. Seleziona Successivo.
11. Per le impostazioni di pubblicazione, scegli se le risorse sono immediatamente individuabili nel catalogo dei dati aziendali. Se le aggiungi solo all'inventario, puoi scegliere le condizioni di

abbonamento in un secondo momento e pubblicarle nel catalogo dei dati aziendali. Per ulteriori informazioni, consulta the section called “Gestisci le fonti di dati esistenti”.

12. Per la generazione automatizzata dei nomi aziendali, scegli se generare automaticamente i metadati per le risorse man mano che vengono importate dalla fonte.
13. (Facoltativo) Per i moduli di metadati, aggiungi moduli per definire i metadati che vengono raccolti e salvati quando le risorse vengono importate in Amazon. DataZone Per ulteriori informazioni, consulta the section called “Crea, modifica o elimina moduli di metadati”.
14. Per la preferenza Esegui, scegli quando eseguire la fonte di dati.
    - Esegui in base a una pianificazione: specifica le date e l'ora in cui eseguire l'origine dati.
    - Esegui su richiesta: puoi avviare manualmente le esecuzioni delle sorgenti dati.
15. Seleziona Successivo.
16. Controlla la configurazione dell'origine dati e scegli Crea.

Crea ed esegui un'origine DataZone dati Amazon per Amazon Redshift

In Amazon DataZone, puoi creare un'origine dati Amazon Redshift per importare metadati tecnici di tabelle e viste di database dal data warehouse Amazon Redshift. Per aggiungere un'origine DataZone dati Amazon per Amazon Redshift, il data warehouse di origine deve già esistere in Amazon Redshift.

Quando crei ed esegui un'origine dati Amazon Redshift, aggiungi risorse dal data warehouse Amazon Redshift di origine all'inventario del tuo progetto DataZone Amazon. Puoi eseguire le tue fonti di dati Amazon Redshift secondo una pianificazione prestabilita o su richiesta per creare o aggiornare i metadati tecnici delle tue risorse. Durante l'esecuzione dell'origine dati, puoi facoltativamente scegliere di pubblicare le risorse di inventario del progetto nel DataZone catalogo Amazon e renderle così individuabili da tutti gli utenti del dominio. Puoi anche pubblicare le tue risorse di inventario dopo aver modificato i relativi metadati aziendali. Gli utenti del dominio possono cercare e scoprire le risorse pubblicate e richiedere abbonamenti a tali risorse.

Per aggiungere un'origine dati Amazon Redshift

1. Vai all'URL del portale DataZone dati di Amazon e accedi utilizzando Single Sign-On (SSO) o le tue credenziali. AWS Se sei un DataZone amministratore Amazon, puoi accedere alla

DataZone console Amazon all'indirizzo https://console.aws.amazon.com/datazone e accedere con il Account AWS luogo in cui è stato creato il dominio, quindi scegliere Open data portal.

2. Scegli Seleziona progetto dal pannello di navigazione in alto e seleziona il progetto a cui desideri aggiungere la fonte di dati.
3. Vai alla scheda Dati per il progetto.
4. Scegli Origini dati dal riquadro di navigazione a sinistra, quindi scegli Crea origine dati.
5. Configura i campi seguenti:

   - Nome: il nome dell'origine dati.
   - Descrizione: la descrizione dell'origine dati.
6. In Tipo di origine dati, scegli Amazon Redshift.
7. In Seleziona un ambiente, specifica un ambiente in cui pubblicare le tabelle Amazon Redshift.
8. A seconda dell'ambiente selezionato, Amazon DataZone applicherà automaticamente le credenziali di Amazon Redshift e altri parametri direttamente dall'ambiente o ti darà la possibilità di sceglierne uno personalizzato.

   - Se hai selezionato un ambiente che consente la pubblicazione solo dallo schema Amazon Redshift predefinito dell'ambiente, Amazon DataZone applicherà automaticamente le credenziali Amazon Redshift e altri parametri, tra cui il nome del cluster o del gruppo di lavoro Amazon Redshift, il segreto AWS , il nome del database e il nome dello schema. Non è possibile modificare questi parametri compilati automaticamente.
   - Se si seleziona un ambiente che non consente la pubblicazione di dati, non sarà possibile procedere con la creazione dell'origine dati.
   - Se selezioni un ambiente che consente la pubblicazione di dati da qualsiasi schema, vedrai la possibilità di utilizzare le credenziali e altri parametri di Amazon Redshift dall'ambiente o di inserire le tue credenziali/parametri.
9. Se scegli di utilizzare le tue credenziali per creare l'origine dati, fornisci i seguenti dettagli:

   - Nella sezione Fornisci credenziali Amazon Redshift, scegli se utilizzare un cluster Amazon Redshift fornito o uno spazio di lavoro Serverless Amazon Redshift come origine dati.
   - A seconda della selezione effettuata nel passaggio precedente, scegli il cluster o lo spazio di lavoro Amazon Redshift dal menu a discesa, quindi scegli il segreto in Secrets Manager AWS da utilizzare per l'autenticazione. Puoi scegliere un segreto esistente o crearne uno nuovo.
   - Affinché il segreto esistente appaia nel menu a discesa, assicurati che il segreto in AWS Secrets Manager includa i seguenti tag (chiave/valore):

- AmazonDataZoneProject: <projectID>
- AmazonDataZoneDomain: <domainID>

Se scegli di creare un nuovo segreto, il segreto viene automaticamente etichettato con i tag di cui sopra e non sono necessari passaggi aggiuntivi. Per ulteriori informazioni, vedere Memorizzazione delle credenziali del database in. AWS Secrets Manager

Gli utenti di Amazon Redshift che possiedono il AWS segreto fornito per la creazione dell'origine dati devono disporre `SELECT` delle autorizzazioni per le tabelle che devono essere pubblicate. Se desideri che Amazon DataZone gestisca anche gli abbonamenti (accesso) per tuo conto, gli utenti del database in AWS segreto devono disporre anche delle seguenti autorizzazioni:

- `CREATE DATASHARE`
- `ALTER DATASHARE`
- `DROP DATASHARE`

10. In Selezione dei dati, fornisci un database Amazon Redshift, uno schema e inserisci la tabella o visualizza i criteri di selezione. Ad esempio, se scegli Includi e inserisci`*corporate`, la risorsa includerà tutte le tabelle di origine che terminano con la parola`corporate`.

    Potete aggiungere più regole di inclusione per le tabelle all'interno di un singolo database. È inoltre possibile aggiungere più database utilizzando il pulsante Aggiungi un altro database.
11. Seleziona Successivo.
12. Per le impostazioni di pubblicazione, scegliete se le risorse sono immediatamente individuabili nel catalogo dati. Se le aggiungi solo all'inventario, puoi scegliere le condizioni di abbonamento in un secondo momento e pubblicarle nel catalogo dei dati aziendali. Per ulteriori informazioni, consulta the section called “Gestisci le fonti di dati esistenti”.
13. Per la generazione automatizzata dei nomi aziendali, scegli se generare automaticamente i metadati per le risorse man mano che vengono pubblicate e aggiornate dalla fonte.
14. (Facoltativo) Per i moduli di metadati, aggiungi moduli per definire i metadati che vengono raccolti e salvati quando le risorse vengono importate in Amazon. DataZone Per ulteriori informazioni, consulta the section called “Crea, modifica o elimina moduli di metadati”.
15. Per la preferenza Esegui, scegli quando eseguire la fonte di dati.

    - Esegui in base a una pianificazione: specifica le date e l'ora in cui eseguire l'origine dati.
    - Esegui su richiesta: puoi avviare manualmente le esecuzioni delle sorgenti dati.

16. Seleziona Successivo.
17. Controlla la configurazione dell'origine dati e scegli Crea.

Gestisci le fonti di DataZone dati Amazon esistenti

Dopo aver creato un'origine DataZone dati Amazon, puoi modificarla in qualsiasi momento per modificare i dettagli dell'origine o i criteri di selezione dei dati. Quando non hai più bisogno di un'origine dati, puoi eliminarla.

Per completare questi passaggi, devi avere la policy AmazonDataZoneFullAccess AWS gestita allegata. Per ulteriori informazioni, consulta the section called “AWS politiche gestite”.

Argomenti

- Modifica una fonte di dati
- Eliminazione di un'origine dati

Modifica una fonte di dati

Puoi modificare un'origine DataZone dati Amazon per modificarne le impostazioni di selezione dei dati, inclusa l'aggiunta, la rimozione o la modifica dei criteri di selezione della tabella. Puoi anche aggiungere e rimuovere database. Non puoi modificare il tipo di origine dati o l'ambiente in cui viene pubblicata un'origine dati.

Per modificare un'origine dati

1. Vai all'URL del portale DataZone dati di Amazon e accedi utilizzando Single Sign-On (SSO) o le tue credenziali. AWS Se sei un DataZone amministratore Amazon, puoi accedere alla DataZone console Amazon all'indirizzo https://console.aws.amazon.com/datazone e accedere con il Account AWS luogo in cui è stato creato il dominio, quindi scegliere Open data portal.
2. Scegli Seleziona progetto dal pannello di navigazione in alto e seleziona il progetto a cui appartiene la fonte di dati.
3. Vai alla scheda Dati per il progetto.
4. Scegli Origini dati dal riquadro di navigazione a sinistra, quindi scegli l'origine dati che desideri modificare.
5. Vai alla scheda Definizione dell'origine dati e scegli Modifica.

6. Apporta le modifiche alla definizione dell'origine dati. È possibile aggiornare i dettagli dell'origine dati e apportare modifiche ai criteri di selezione dei dati.
7. Una volta completate le modifiche, scegli Save (Salva).

Eliminazione di un'origine dati

Quando non hai più bisogno di un'origine DataZone dati Amazon, puoi rimuoverla definitivamente. Dopo aver eliminato una fonte di dati, tutte le risorse che hanno avuto origine da tale fonte di dati sono ancora disponibili nel catalogo e gli utenti possono ancora abbonarsi. Tuttavia, le risorse smetteranno di ricevere aggiornamenti dalla fonte. Ti consigliamo di spostare le risorse dipendenti in un'altra fonte di dati prima di eliminarle.

> **Note**
>
> Devi rimuovere tutti gli adempimenti dall'origine dati prima di poterla eliminare. Per ulteriori informazioni, consulta Scoperta, sottoscrizione e utilizzo dei dati in Amazon DataZone.

Per eliminare un'origine dati

1. Nella scheda Dati del progetto, scegli Origini dati dal riquadro di navigazione a sinistra.
2. Scegli la fonte di dati che desideri eliminare.
3. Scegli Azioni, Elimina origine dati e conferma l'eliminazione.

Pubblica risorse nel DataZone catalogo Amazon dall'inventario del progetto

Puoi pubblicare le DataZone risorse Amazon e i relativi metadati dagli inventari dei progetti nel catalogo Amazon DataZone . Puoi pubblicare solo la versione più recente di una risorsa nel catalogo.

Quando pubblicate risorse nel catalogo, tenete presente quanto segue:

- Per pubblicare una risorsa nel catalogo, devi essere il proprietario o il collaboratore di quel progetto.
- Per gli asset Amazon Redshift, assicurati che i cluster Amazon Redshift associati ai cluster di editori e abbonati soddisfino tutti i requisiti per la condivisione dei dati di Amazon Redshift, in modo

che Amazon possa gestire l'accesso alle tabelle e DataZone alle viste di Redshift. Vedi Concetti di condivisione dei dati per Amazon Redshift.

- Amazon supporta DataZone solo la gestione degli accessi per le risorse pubblicate da AWS Glue Data Catalog e Amazon Redshift. Per tutte le altre risorse, come gli oggetti Amazon S3, Amazon DataZone non gestisce l'accesso per gli abbonati approvati. Se ti iscrivi a queste risorse non gestite, riceverai una notifica con il seguente messaggio:

  ```
  Subscription approval does not provide access to data. Subscription
  grants on this asset are not managed by Amazon DataZone. For more
  information or help, reach out to your administrator.
  ```

Pubblica una risorsa

Se non avete scelto di rendere le risorse immediatamente individuabili nel catalogo dati quando avete creato un'origine dati, effettuate le seguenti operazioni per pubblicarle in un secondo momento.

Per pubblicare una risorsa

1. Vai all'URL del portale DataZone dati di Amazon e accedi utilizzando Single Sign-On (SSO) o le tue credenziali. AWS Se sei un DataZone amministratore Amazon, puoi accedere alla DataZone console Amazon all'indirizzo https://console.aws.amazon.com/datazone e accedere con il Account AWS luogo in cui è stato creato il dominio, quindi scegliere Open data portal.
2. Scegli Seleziona progetto dal pannello di navigazione in alto e seleziona il progetto a cui appartiene la risorsa.
3. Vai alla scheda Dati per il progetto.
4. Scegli Dati di inventario dal riquadro di navigazione a sinistra, quindi seleziona la risorsa che desideri pubblicare.

> **Note**
>
> Per impostazione predefinita, tutte le risorse richiedono l'approvazione della sottoscrizione, il che significa che il proprietario dei dati deve approvare tutte le richieste di sottoscrizione alla risorsa. Se desideri modificare questa impostazione prima di pubblicare la risorsa, apri i dettagli della risorsa e scegli Modifica accanto ad Approvazione della sottoscrizione. Puoi modificare questa impostazione in un secondo momento modificando e ripubblicando la risorsa.

5. Scegliete Pubblica risorsa. La risorsa viene pubblicata direttamente nel catalogo.

   Se apporti modifiche alla risorsa, ad esempio modificandone i requisiti di approvazione, puoi scegliere Ripubblica per pubblicare gli aggiornamenti nel catalogo.

Gestisci l'inventario e cura le risorse

Per utilizzare Amazon per DataZone catalogare i tuoi dati, devi prima importare i tuoi dati (asset) come inventario del tuo progetto in Amazon DataZone. La creazione di un inventario per un particolare progetto rende le risorse individuabili solo dai membri di quel progetto.

Una volta create le risorse nell'inventario del progetto, i relativi metadati possono essere curati. Ad esempio, puoi modificare il nome, la descrizione della risorsa o leggermi. Ogni modifica alla risorsa crea una nuova versione della risorsa. Puoi utilizzare la scheda Cronologia nella pagina dei dettagli della risorsa per visualizzare tutte le versioni della risorsa.

Puoi modificare la sezione Leggimi e aggiungere descrizioni dettagliate per la risorsa. La sezione Read Me supporta il markdown, che consente quindi di formattare le descrizioni come richiesto e di descrivere le informazioni chiave su una risorsa ai consumatori.

I termini del glossario possono essere aggiunti a livello di risorsa compilando i moduli disponibili.

Per curare lo schema, puoi rivedere le colonne, aggiungere nomi commerciali, descrizioni e aggiungere termini del glossario a livello di colonna.

Se la generazione automatica di metadati è abilitata al momento della creazione dell'origine dati, i nomi commerciali delle risorse e delle colonne possono essere esaminati e accettati o rifiutati singolarmente o tutti insieme.

Puoi anche modificare i termini di abbonamento per specificare se l'approvazione per la risorsa è richiesta o meno.

I moduli di metadati in Amazon DataZone consentono di estendere il modello di metadati di un asset di dati aggiungendo attributi personalizzati (ad esempio, regione di vendita, anno di vendita e trimestre di vendita). I moduli di metadati allegati a un tipo di risorsa vengono applicati a tutte le risorse create da quel tipo di risorsa. Puoi anche aggiungere moduli di metadati aggiuntivi a singole risorse come parte dell'esecuzione dell'origine dati o dopo la sua creazione. Per creare nuovi moduli, consultathe section called “Crea, modifica o elimina moduli di metadati”.

Per aggiornare i metadati di una risorsa, devi essere il proprietario o il collaboratore del progetto a cui appartiene la risorsa.

Per aggiornare i metadati di una risorsa

1. Vai all'URL del portale DataZone dati di Amazon e accedi utilizzando Single Sign-On (SSO) o le tue credenziali. AWS Se sei un DataZone amministratore Amazon, puoi accedere alla DataZone console Amazon all'indirizzo https://console.aws.amazon.com/datazone e accedere con il Account AWS luogo in cui è stato creato il dominio, quindi scegliere Open data portal.
2. Scegli Seleziona progetto dal pannello di navigazione in alto e seleziona il progetto che contiene la risorsa di cui desideri aggiornare i metadati.
3. Vai alla scheda Dati per il progetto.
4. Scegli Dati di inventario dal riquadro di navigazione a sinistra, quindi scegli il nome della risorsa di cui desideri aggiornare i metadati.
5. Nella pagina dei dettagli della risorsa, in Moduli di metadati, scegli Modifica e modifica i moduli esistenti secondo necessità. Puoi anche allegare moduli di metadati aggiuntivi alla risorsa. Per ulteriori informazioni, consulta the section called “Allega moduli di metadati aggiuntivi alle risorse”.
6. Quando hai finito di apportare gli aggiornamenti, scegli Salva modulo.

   Quando salvi il modulo, Amazon DataZone genera una nuova versione di inventario della risorsa. Per pubblicare la versione aggiornata nel catalogo, scegli Ripubblica risorsa.

Allega moduli di metadati aggiuntivi alle risorse

Per impostazione predefinita, i moduli di metadati allegati a un dominio sono allegati a tutte le risorse pubblicate in quel dominio. Gli editori di dati possono associare moduli di metadati aggiuntivi a singole risorse per fornire un contesto aggiuntivo.

Per allegare moduli di metadati aggiuntivi a una risorsa

1. Vai all'URL del portale DataZone dati di Amazon e accedi utilizzando Single Sign-On (SSO) o le tue credenziali. AWS Se sei un DataZone amministratore Amazon, puoi accedere alla DataZone console Amazon all'indirizzo https://console.aws.amazon.com/datazone e accedere con il Account AWS luogo in cui è stato creato il dominio, quindi scegliere Open data portal.
2. Scegli Seleziona progetto dal pannello di navigazione in alto e seleziona il progetto che contiene la risorsa a cui desideri aggiungere i metadati.

3. Vai alla scheda Dati per il progetto.
4. Scegli Dati di inventario dal riquadro di navigazione a sinistra, quindi scegli il nome della risorsa a cui desideri aggiungere i metadati.
5. Nella pagina dei dettagli della risorsa, in Moduli di metadati, scegli Aggiungi moduli.
6. Seleziona i moduli da aggiungere alla risorsa, quindi scegli Aggiungi moduli.
7. Inserisci i valori per ogni campo di metadati, quindi scegli Salva modulo.

   Quando salvi il modulo, Amazon DataZone genera una nuova versione di inventario della risorsa. Per pubblicare la versione aggiornata nel catalogo, scegli Ripubblica risorsa.

Pubblica la risorsa nel catalogo dopo la curatela

Una volta soddisfatto della cura delle risorse, il proprietario dei dati può pubblicare una versione della risorsa nel DataZone catalogo Amazon e renderla così individuabile da tutti gli utenti del dominio. La risorsa mostra la versione dell'inventario e la versione pubblicata. Nel Discovery Catalog, viene visualizzata solo l'ultima versione pubblicata. Se i metadati vengono aggiornati dopo la pubblicazione, sarà disponibile una nuova versione di inventario da pubblicare nel catalogo.

Crea manualmente una risorsa

In Amazon DataZone, una risorsa è un'entità che presenta un singolo oggetto di dati fisico (ad esempio una tabella, una dashboard, un file) o un oggetto di dati virtuale (ad esempio una vista). Per ulteriori informazioni, consulta DataZone Terminologia e concetti di Amazon. La pubblicazione manuale di una risorsa è un'operazione unica. Non specificate una pianificazione di esecuzione per la risorsa, quindi questa non viene aggiornata automaticamente se la sua fonte cambia.

Per creare manualmente una risorsa tramite un progetto, devi essere il proprietario o il collaboratore di quel progetto.

Per creare una risorsa manualmente

1. Vai all'URL del portale DataZone dati di Amazon e accedi utilizzando Single Sign-On (SSO) o le tue credenziali. AWS Se sei un DataZone amministratore Amazon, puoi accedere alla DataZone console Amazon all'indirizzo https://console.aws.amazon.com/datazone e accedere con il Account AWS luogo in cui è stato creato il dominio, quindi scegliere Open data portal.
2. Scegli Seleziona progetto dal pannello di navigazione in alto e seleziona il progetto in cui creare la risorsa.

3. Vai alla scheda Dati per il progetto.
4. Scegli Origini dati dal riquadro di navigazione a sinistra, quindi scegli Crea risorsa di dati.
5. Per i dettagli sulla risorsa, configura le seguenti impostazioni:
   - Tipo di risorsa: il tipo di risorsa.
   - Nome: il nome della risorsa.
   - Descrizione: una descrizione della risorsa.
6. Per la posizione S3, inserisci l'Amazon Resource Name (ARN) del bucket S3 di origine.

   Facoltativamente, inserisci un punto di accesso S3. Per ulteriori informazioni, consulta Gestione dell'accesso ai dati con access point Amazon S3.
7. Per le impostazioni di pubblicazione, scegliete se le risorse sono immediatamente individuabili nel catalogo. Se le aggiungi solo all'inventario, puoi scegliere le condizioni di abbonamento in un secondo momento per pubblicarle nel catalogo.
8. Scegli Crea.

   Una volta creata, la risorsa verrà pubblicata direttamente come risorsa attiva nel catalogo o verrà archiviata nell'inventario fino a quando non deciderai di pubblicarla.

Annullare la pubblicazione di una risorsa dal catalogo Amazon DataZone

Quando annulli la pubblicazione di una DataZone risorsa Amazon dal catalogo, questa non viene più visualizzata nei risultati di ricerca globali. I nuovi utenti non saranno in grado di trovare o abbonarsi all'elenco delle risorse nel catalogo, ma tutti gli abbonamenti esistenti rimarranno gli stessi.

Per annullare la pubblicazione di una risorsa, devi essere il proprietario o il collaboratore del progetto a cui appartiene la risorsa:

Per annullare la pubblicazione di una risorsa

1. Vai all'URL del portale DataZone dati di Amazon e accedi utilizzando Single Sign-On (SSO) o le tue credenziali. AWS Se sei un DataZone amministratore Amazon, puoi accedere alla DataZone console Amazon all'indirizzo https://console.aws.amazon.com/datazone e accedere con il Account AWS luogo in cui è stato creato il dominio, quindi scegliere Open data portal.

2. Scegli Seleziona progetto dal pannello di navigazione in alto e seleziona il progetto a cui appartiene la risorsa.
3. Vai alla scheda Dati per il progetto.
4. Scegli Dati pubblicati dal riquadro di navigazione a sinistra.
5. Individua la risorsa dall'elenco delle risorse pubblicate, quindi scegli Annulla pubblicazione.

   La risorsa viene rimossa dal catalogo. Puoi ripubblicare la risorsa in qualsiasi momento scegliendo Pubblica.

Eliminare una DataZone risorsa Amazon

Quando non hai più bisogno di una risorsa in Amazon DataZone, puoi eliminarla definitivamente. L'eliminazione di una risorsa è diversa dall'annullamento della pubblicazione di una risorsa dal catalogo. Puoi eliminare una risorsa e il relativo elenco nel catalogo in modo che non sia visibile nei risultati di ricerca. Per eliminare l'elenco delle risorse, devi prima revocare tutte le relative sottoscrizioni.

Per eliminare una risorsa, devi essere il proprietario o il collaboratore del progetto a cui appartiene la risorsa:

> **Note**
>
> Per eliminare un elenco di risorse, devi prima revocare tutte le sottoscrizioni esistenti alla risorsa. Non puoi eliminare un elenco di risorse con abbonati esistenti.

Per eliminare una risorsa

1. Vai all'URL del portale DataZone dati di Amazon e accedi utilizzando Single Sign-On (SSO) o le tue credenziali. AWS Se sei un DataZone amministratore Amazon, puoi accedere alla DataZone console Amazon all'indirizzo https://console.aws.amazon.com/datazone e accedere con il Account AWS luogo in cui è stato creato il dominio, quindi scegliere Open data portal.
2. Scegli Seleziona progetto dal pannello di navigazione in alto e seleziona il progetto che contiene la risorsa che desideri eliminare.
3. Vai alla scheda Dati per il progetto.
4. Scegli Dati pubblicati dal riquadro di navigazione a sinistra, quindi individua e scegli la risorsa che desideri eliminare. Si apre la pagina dei dettagli della risorsa.

5. Scegliete Azioni, Elimina e confermate l'eliminazione.

   Una volta eliminata, la risorsa non è più disponibile per la visualizzazione e gli utenti non possono abbonarsi.

Avvia manualmente un'origine dati eseguita in Amazon DataZone

Quando gestisci un'origine dati, Amazon DataZone estrae tutti i metadati nuovi o modificati dalla fonte e aggiorna gli asset associati nell'inventario. Quando aggiungi un'origine dati ad Amazon DataZone, specifichi la preferenza di esecuzione della fonte, che definisce se la fonte viene eseguita in base a una pianificazione o su richiesta. Se la tua origine viene eseguita su richiesta, devi avviare un'origine dati eseguita manualmente.

Anche se l'origine viene eseguita secondo una pianificazione, puoi comunque eseguirla manualmente in qualsiasi momento. Dopo aver aggiunto i metadati aziendali alle risorse, puoi selezionare le risorse e pubblicarle nel DataZone catalogo Amazon in modo che queste risorse siano individuabili da tutti gli utenti del dominio. Solo le risorse pubblicate possono essere ricercate da altri utenti del dominio.

Per eseguire manualmente una fonte di dati

1. Vai all'URL del portale DataZone dati di Amazon e accedi utilizzando Single Sign-On (SSO) o le tue credenziali. AWS Se sei un DataZone amministratore Amazon, puoi accedere alla DataZone console Amazon all'indirizzo https://console.aws.amazon.com/datazone e accedere con il Account AWS luogo in cui è stato creato il dominio, quindi scegliere Open data portal.
2. Scegli Seleziona progetto dal pannello di navigazione in alto e seleziona il progetto a cui appartiene la fonte di dati.
3. Vai alla scheda Dati per il progetto.
4. Scegli Origini dati dal riquadro di navigazione a sinistra, quindi individua e scegli l'origine dati che desideri eseguire. Si apre la pagina dei dettagli dell'origine dati.
5. Scegli Esegui su richiesta.

   Lo stato dell'origine dati cambia `Running` man mano che Amazon DataZone aggiorna i metadati degli asset con i dati più recenti provenienti dalla fonte. Puoi monitorare lo stato dell'esecuzione nella scheda Data source run.

Revisioni degli asset in Amazon DataZone

Amazon DataZone incrementa la revisione di una risorsa quando ne modifichi i metadati aziendali o tecnici. Queste modifiche includono la modifica del nome della risorsa, della descrizione, dei termini del glossario, dei nomi delle colonne, dei moduli di metadati e dei valori dei campi del modulo di metadati. Queste modifiche possono derivare da modifiche manuali, dall'esecuzione di processi all'origine dei dati o da operazioni API. Amazon genera DataZone automaticamente una nuova revisione delle risorse ogni volta che apporti una modifica alla risorsa.

Dopo aver aggiornato una risorsa ed essere stata generata una nuova revisione, devi pubblicare la nuova revisione nel catalogo affinché sia aggiornata e disponibile per gli abbonati. Per ulteriori informazioni, consulta the section called “Pubblica le risorse nel catalogo dall'inventario del progetto”. Puoi pubblicare solo la versione più recente di una risorsa nel catalogo.

Per visualizzare le revisioni precedenti di una risorsa

1. Vai all'URL del portale DataZone dati di Amazon e accedi utilizzando Single Sign-On (SSO) o le tue credenziali. AWS Se sei un DataZone amministratore Amazon, puoi accedere alla DataZone console Amazon all'indirizzo https://console.aws.amazon.com/datazone e accedere con il Account AWS luogo in cui è stato creato il dominio, quindi scegliere Open data portal.
2. Scegli Seleziona progetto dal pannello di navigazione in alto e seleziona il progetto che contiene la risorsa.
3. Vai alla scheda Dati del progetto, quindi individua e scegli la risorsa. Si apre la pagina dei dettagli della risorsa.
4. Vai alla scheda Cronologia, che mostra un elenco delle revisioni precedenti della risorsa.

Qualità dei dati in Amazon DataZone

Le metriche sulla qualità dei dati in Amazon ti DataZone aiutano a comprendere i diversi parametri di qualità come la completezza, la tempestività e l'accuratezza delle tue fonti di dati. Amazon DataZone si integra con AWS Glue Data Quality e offre API per integrare metriche di qualità dei dati da soluzioni di qualità dei dati di terze parti. Gli utenti dei dati possono vedere come le metriche sulla qualità dei dati cambiano nel tempo per gli asset sottoscritti. Per creare ed eseguire le regole sulla qualità dei dati, puoi utilizzare il tuo strumento di qualità dei dati preferito, come AWS Glue data quality. Con le metriche sulla qualità dei dati di Amazon DataZone, i consumatori di dati possono visualizzare i punteggi di qualità dei dati per gli asset e le colonne, contribuendo a creare fiducia nei dati che utilizzano per le decisioni.

Prerequisiti e modifiche ai ruoli IAM

Se utilizzi le policy AWS gestite DataZone di Amazon, non ci sono passaggi di configurazione aggiuntivi e queste policy gestite vengono aggiornate automaticamente per supportare la qualità dei dati. Se utilizzi le tue politiche per i ruoli che concedono ad Amazon DataZone le autorizzazioni necessarie per interagire con i servizi supportati, devi aggiornare le politiche allegate a questi ruoli per abilitare il supporto per la lettura delle informazioni sulla qualità dei dati di AWS Glue in AWS politica gestita: AmazonDataZoneGlueManageAccessRolePolicy e abilitare il supporto per le API delle serie temporali in and. AWS politica gestita: AmazonDataZoneDomainExecutionRolePolicy AWS politica gestita: AmazonDataZoneFullUserAccess

Abilitare la qualità dei dati per le risorse AWS Glue

Amazon DataZone estrae le metriche sulla qualità dei dati da AWS Glue per fornire un contesto in un determinato momento, ad esempio durante una ricerca nel catalogo di dati aziendali. Gli utenti dei dati possono vedere come i parametri di qualità dei dati cambiano nel tempo per gli asset sottoscritti. I produttori di dati possono acquisire i punteggi di qualità dei dati di AWS Glue in base a una pianificazione. Il catalogo di dati DataZone aziendali di Amazon può anche visualizzare metriche sulla qualità dei dati provenienti da sistemi di terze parti tramite API per la qualità dei dati. Per ulteriori informazioni, consulta AWS Glue Data Quality e Guida introduttiva a AWS Glue Data Quality for the Data Catalog.

Puoi abilitare i parametri di qualità dei dati per i tuoi DataZone asset Amazon nei seguenti modi:

- Utilizza il Data Portal o le DataZone API di Amazon per abilitare la qualità dei dati per la tua sorgente dati AWS Glue tramite il portale dati Amazon durante la creazione di una nuova fonte di DataZone dati Glue o la modifica di un'origine dati AWS Glue esistente.

  Per ulteriori informazioni sull'abilitazione della qualità dei dati per una fonte di dati tramite il portale, consulta Crea ed esegui un'origine DataZone dati Amazon per AWS Glue Data Catalog eGestisci le fonti di DataZone dati Amazon esistenti.

  > **Note**
  >
  > Puoi utilizzare il Data Portal per abilitare la qualità dei dati solo per le tue risorse di inventario AWS Glue. In questa versione di Amazon, l' DataZone abilitazione della qualità dei dati per Amazon Redshift o per asset di tipo personalizzato tramite il portale dati non è supportata.

Puoi anche utilizzare le API per abilitare la qualità dei dati per le tue fonti di dati nuove o esistenti. Puoi farlo richiamando CreateDataSourceo UpdateDataSourcee impostando il `autoImportDataQualityResult` parametro su «True».

Dopo aver abilitato la qualità dei dati, puoi eseguire l'origine dati su richiesta o in base alla pianificazione. Ogni esecuzione può includere fino a 100 parametri per risorsa. Non è necessario creare moduli o aggiungere metriche manualmente quando si utilizza una fonte di dati per la qualità dei dati. Quando la risorsa viene pubblicata, gli aggiornamenti apportati al modulo sulla qualità dei dati (fino a 30 punti dati per regola storica) si riflettono nell'elenco destinato ai consumatori. Successivamente, ogni nuova aggiunta di metriche alla risorsa viene aggiunta automaticamente all'elenco. Non è necessario ripubblicare la risorsa per rendere disponibili ai consumatori gli ultimi punteggi.

Abilitazione della qualità dei dati per tipi di asset personalizzati

Puoi utilizzare le DataZone API di Amazon per abilitare la qualità dei dati per qualsiasi tuo asset di tipo personalizzato. Per ulteriori informazioni, consulta gli argomenti seguenti:

- PostTimeSeriesDataPoints
- ListTimeSeriesDataPoints
- GetTimeSeriesDataPoint
- DeleteTimeSeriesDataPoints

I passaggi seguenti forniscono un esempio di utilizzo di API o CLI per importare parametri di terze parti per i tuoi asset in Amazon: DataZone

1. Richiama l'API come seguePostTimeSeriesDataPoints:

```
aws datazone post-time-series-data-points  \
--cli-input-json file://createTimeSeriesPayload.json \
```

con il seguente payload:

```
{
"domainIdentifier": "dzd_bqqlk3nz21zp2f",
"entityIdentifier": "4nwl5ew0dsu27b",
"entityType": "ASSET",
"forms": [
{
"content": "{\n \"evaluationsCount\" : 11,\n \"evaluations\" : [ {\n \"description
\" : \"IsComplete \\\"Id\\\"\",\n \"details\" : {\n \"STATISTIC_NAME\" :
 \"Completeness\",\n \"COLUMN_NAME\" : \"Id\"\n },\n \"status\" : \"PASS\"\n },
 {\n \"description\" : \"Uniqueness \\\"Id\\\" > 0.95\",\n \"details\" : {\n
 \"STATISTIC_NAME\" : \"Uniqueness\",\n \"COLUMN_NAME\" : \"Id\"\n },\n \"status
\" : \"PASS\"\n }, {\n \"description\" : \"ColumnLength \\\"Id\\\" = 18\",\n
 \"details\" : {\n \"STATISTIC_NAME\" : \"MinimumLength,MaximumLength\",\n
 \"COLUMN_NAME\" : \"Id,Id\"\n },\n \"status\" : \"PASS\"\n }, {\n \"description
\" : \"IsComplete \\\"IsDeleted\\\"\",\n \"details\" : {\n \"STATISTIC_NAME\" :
 \"Completeness\",\n \"COLUMN_NAME\" : \"IsDeleted\"\n },\n \"status\" : \"PASS
\"\n }, {\n \"description\" : \"Completeness \\\"Type\\\" >= 0.59\",\n \"details
\" : {\n \"STATISTIC_NAME\" : \"Completeness\",\n \"COLUMN_NAME\" : \"Type\"\n },
\n \"status\" : \"PASS\"\n }, {\n \"description\" : \"ColumnValues \\\"Type\
\\" in [\\\"Customer - Direct\\\",\\\"Customer - Channel\\\"] with threshold
 >= 0.8\",\n \"details\" : {\n \"STATISTIC_NAME\" : \"\",\n \"COLUMN_NAME\" :
 \"\"\n },\n \"status\" : \"PASS\"\n }, {\n \"description\" : \"ColumnLength \\
\"Type\\\" <= 18\",\n \"details\" : {\n \"STATISTIC_NAME\" : \"MaximumLength\",\n
 \"COLUMN_NAME\" : \"Type\"\n },\n \"status\" : \"PASS\"\n }, {\n \"description
\" : \"ColumnLength \\\"ParentId\\\" <= 18\",\n \"details\" : {\n \"STATISTIC_NAME
\" : \"MaximumLength\",\n \"COLUMN_NAME\" : \"ParentId\"\n },\n \"status\" :
 \"PASS\"\n }, {\n \"description\" : \"Completeness \\\"AnnualRevenue\\\" >=
 0.28\",\n \"details\" : {\n \"STATISTIC_NAME\" : \"Completeness\",\n \"COLUMN_NAME
\" : \"AnnualRevenue\"\n },\n \"status\" : \"PASS\"\n }, {\n \"description
\" : \"StandardDeviation \\\"AnnualRevenue\\\" between 1658483123.39 and
 1833060294.28\",\n \"details\" : {\n \"STATISTIC_NAME\" : \"StandardDeviation
\",\n \"COLUMN_NAME\" : \"AnnualRevenue\"\n },\n \"status\" : \"PASS\"\n }, {\n
 \"description\" : \"ColumnValues \\\"AnnualRevenue\\\" between 29999999 and
 5600000001\",\n \"details\" : {\n \"STATISTIC_NAME\" : \"Minimum,Maximum\",\n
 \"COLUMN_NAME\" : \"AnnualRevenue,AnnualRevenue\"\n },\n \"status\" : \"PASS
\"\n } ],\n \"passingPercentage\" : 1.0\n}",
"formName": "GREAT_EXPECTATION_NEW",
"typeIdentifier": "amazon.datazone.DataQualityResultFormType",
"timestamp": 1608969556
}
]
}
```

2. Richiama l'`DeleteTimeSeriesDataPoints`API come segue:

```
aws datazone delete-time-series-data-points\
--domain-identifier dzd_bqqlk3nz21zp2f \
--entity-identifier dzd_bqqlk3nz21zp2f \
--entity-type ASSET \
--form-name rulesET1 \
```

Utilizzo dell'apprendimento automatico e dell'intelligenza artificiale generativa

> **Note**
>
> Realizzato da Amazon Bedrock: AWS implementa il rilevamento automatico degli abusi. Poiché la funzionalità dei consigli di intelligenza artificiale per le descrizioni in Amazon DataZone è basata su Amazon Bedrock, gli utenti ereditano i controlli implementati in Amazon Bedrock per rafforzare la sicurezza e l'uso responsabile dell'intelligenza artificiale.

Nell'attuale versione di Amazon DataZone, puoi utilizzare la funzionalità di descrizione dei consigli di intelligenza artificiale per automatizzare l'individuazione e la catalogazione dei dati. Il supporto per l'intelligenza artificiale generativa e l'apprendimento automatico in Amazon DataZone crea descrizioni per risorse e colonne. Puoi utilizzare queste descrizioni per aggiungere un contesto aziendale ai tuoi dati e consigliare analisi per i set di dati, che possono contribuire a migliorare i risultati della scoperta dei dati.

Basati sui grandi modelli linguistici di Amazon Bedrock, i consigli di intelligenza artificiale per la descrizione degli asset di dati in Amazon ti DataZone aiutano a garantire che i tuoi dati siano comprensibili e facilmente individuabili. Le raccomandazioni sull'intelligenza artificiale suggeriscono anche le applicazioni analitiche più pertinenti per i set di dati. Riducendo le attività di documentazione manuale e fornendo consigli sull'uso appropriato dei dati, le descrizioni generate automaticamente possono aiutarti a migliorare l'affidabilità dei tuoi dati e ridurre al minimo la trascuratezza dei dati preziosi per accelerare il processo decisionale informato.

> **Important**
>
> Nell'attuale DataZone versione di Amazon, la funzionalità AI Recommendations for Descriptions è supportata solo nelle seguenti regioni:
>
> - Stati Uniti orientali (Virginia settentrionale)
> - US West (Oregon)
> - Europa (Francoforte)
> - Asia Pacifico (Tokyo)

La procedura seguente descrive come generare consigli di intelligenza artificiale per le descrizioni in Amazon DataZone:

1. Vai all'URL del portale DataZone dati di Amazon, quindi accedi utilizzando Single Sign-On (SSO) o le tue credenziali. AWS Se sei un DataZone amministratore Amazon, accedi alla DataZone console Amazon all'indirizzo https://console.aws.amazon.com/datazone e accedi con il Account AWS luogo in cui è stato creato il dominio, quindi scegli Open data portal.
2. Nel riquadro di navigazione in alto, scegli Seleziona progetto, quindi scegli il progetto che contiene la risorsa per la quale desideri generare consigli di intelligenza artificiale per le descrizioni.
3. Vai alla scheda Dati per il progetto.
4. Nel riquadro di navigazione a sinistra, scegli Dati di inventario, quindi scegli il nome della risorsa per la quale desideri generare consigli di intelligenza artificiale per le descrizioni della risorsa.
5. Nella pagina dei dettagli della risorsa, nella scheda Metadati aziendali, scegli Genera descrizioni.
6. Una volta generate le descrizioni, puoi modificarle, accettarle o rifiutarle. Le icone verdi vengono visualizzate accanto a ciascuna descrizione dei metadati generata automaticamente per la risorsa di dati. Nella scheda Metadati aziendali, puoi scegliere l'icona verde accanto al riepilogo generato automaticamente, quindi scegliere Modifica, Accetta o Rifiuta per indirizzare la descrizione generata. Puoi anche scegliere Accetta tutto o Rifiuta tutte le opzioni visualizzate nella parte superiore della pagina quando è selezionata la scheda Metadati aziendali, ed eseguire così l'azione selezionata su tutte le descrizioni generate automaticamente.

   Oppure puoi scegliere la scheda Schema e quindi indirizzare individualmente le descrizioni generate automaticamente scegliendo l'icona verde per la descrizione di una colonna alla volta e quindi scegliendo Accetta o Rifiuta. Nella scheda Schema, puoi anche scegliere Accetta

tutto o Rifiuta tutto ed eseguire così l'azione selezionata su tutte le descrizioni generate automaticamente.

7. Per pubblicare la risorsa nel catalogo con le descrizioni generate, scegliete Pubblica risorsa, quindi confermate questa azione scegliendo nuovamente Pubblica risorsa nella finestra pop-up Pubblica risorsa.

> **Note**
>
> Se non accettate o rifiutate le descrizioni generate per una risorsa e poi pubblicate questa risorsa, questi metadati generati automaticamente non revisionati non vengono inclusi nella risorsa di dati pubblicata.

Scoperta, sottoscrizione e utilizzo dei dati in Amazon DataZone

In Amazon DataZone, una volta pubblicata una risorsa su un dominio, gli abbonati possono scoprire e richiedere un abbonamento a questa risorsa. Il processo di sottoscrizione inizia con la ricerca e l'esplorazione del catalogo da parte di un abbonato per trovare la risorsa desiderata. Dal DataZone portale Amazon, scelgono di abbonarsi alla risorsa inviando una richiesta di abbonamento che include la giustificazione e il motivo della richiesta. L'approvatore dell'abbonamento, come definito nel contratto di pubblicazione, esamina quindi la richiesta di accesso. Può approvare o rifiutare la richiesta.

Dopo la concessione di un abbonamento, inizia un processo di adempimento per facilitare l'accesso alla risorsa per l'abbonato. Esistono due modalità principali di controllo e adempimento degli accessi alle risorse: quelle per le risorse DataZone gestite da Amazon e quelle per le risorse che non sono gestite da Amazon. DataZone

- Risorse gestite: Amazon DataZone può gestire l'adempimento e le autorizzazioni per le risorse gestite, come AWS Glue tabelle e tabelle e viste di Amazon Redshift.
- Risorse non gestite: Amazon DataZone pubblica eventi standard relativi alle tue azioni (ad esempio, l'approvazione data a una richiesta di abbonamento) su Amazon. EventBridge Puoi utilizzare questi eventi standard per l'integrazione con altri AWS servizi o soluzioni di terze parti per integrazioni personalizzate.

Argomenti

Alla scoperta dei dati

Le seguenti attività descrivono vari modi per scoprire dati in Amazon DataZone.

Argomenti

Cerca e visualizza le risorse nel catalogo

Amazon DataZone offre un modo semplificato per la ricerca di dati. Qualsiasi DataZone utente Amazon con le autorizzazioni per accedere al portale dati può cercare risorse nel DataZone catalogo Amazon e visualizzare i nomi delle risorse e i metadati loro assegnati. Puoi dare un'occhiata più da vicino a una risorsa esaminando la sua pagina dei dettagli.

> **Note**
>
> Per visualizzare i dati effettivi contenuti in una risorsa, devi prima sottoscrivere la risorsa, approvare la richiesta di abbonamento e concedere l'accesso. Per ulteriori informazioni, consulta Iscrizione ai dati.

Per cercare risorse nel catalogo

1. Vai all'URL del portale DataZone dati di Amazon e accedi utilizzando Single Sign-On (SSO) o le tue credenziali. AWS Se sei un DataZone amministratore Amazon, puoi accedere alla DataZone console Amazon all'indirizzo https://console.aws.amazon.com/datazone e accedere con il Account AWS luogo in cui è stato creato il dominio, quindi scegliere Open data portal.
2. Puoi digitare il nome della risorsa che stai cercando nella barra di ricerca sulla home page del portale dati.
3. Per sfogliare i namespace, scegliete Catalog in alto a destra della pagina per aprire il catalogo. Il catalogo offre un'esperienza di ricerca sfaccettata che consente di trovare le risorse in base a criteri quali proprietario dei dati e termini del glossario.
4. Inserisci il termine di ricerca in una delle caselle di ricerca. Dopo aver eseguito una ricerca, puoi applicare vari filtri per restringere i risultati. I filtri includono il tipo di risorsa, l'account di origine e il tipo Regione AWS a cui appartiene la risorsa.
5. Per visualizzare i dettagli su una risorsa specifica, scegliete la risorsa per aprire la relativa pagina dei dettagli. La pagina dei dettagli include le seguenti informazioni:

   - Il nome della risorsa, l'origine dei dati (AWS Glue Amazon Redshift o Amazon S3), il tipo (tabella, vista o oggetto S3), il numero di colonne e la dimensione.
   - Una descrizione dell'asset.

- La revisione attualmente pubblicata della risorsa, il proprietario, l'eventuale necessità di approvazione per gli abbonamenti, il namepace e la cronologia degli aggiornamenti.
- Una scheda Panoramica che include i termini del glossario e i moduli di metadati.
- Una scheda Schema che mostra lo schema della risorsa, inclusi i nomi delle colonne commerciali e tecniche, i tipi di dati e le descrizioni aziendali delle colonne. La scheda dello schema è visibile solo per le tabelle e le viste (non per gli oggetti Amazon S3).
- Una scheda Abbonamenti che include un elenco di abbonati al dominio.
- Una scheda Cronologia che include un elenco delle revisioni precedenti della risorsa.

Iscrizione ai dati

Le seguenti attività forniscono dettagli sulla sottoscrizione agli asset in Amazon DataZone.

Argomenti

Richiedi l'abbonamento agli asset

Amazon ti DataZone consente di trovare, accedere e utilizzare le risorse nel DataZone catalogo Amazon. Quando trovi una risorsa nel catalogo a cui desideri accedere, devi abbonarti alla risorsa, il che crea una richiesta di abbonamento. Un approvatore può quindi approvare o richiedere la tua richiesta.

Devi essere un membro di un progetto per richiedere l'abbonamento a una risorsa all'interno di quel progetto.

Per sottoscrivere una risorsa

1. Vai all'URL del portale DataZone dati di Amazon e accedi utilizzando Single Sign-On (SSO) o le tue credenziali. AWS Se sei un DataZone amministratore Amazon, puoi accedere alla

DataZone console Amazon all'indirizzo https://console.aws.amazon.com/datazone e accedere con il Account AWS luogo in cui è stato creato il dominio, quindi scegliere Open data portal.

2. Usa la barra di ricerca per cercare e scegliere la risorsa a cui desideri abbonarti, quindi scegli Abbonati.
3. Nella finestra pop-up Iscriviti, fornisci le seguenti informazioni:
   - Il progetto a cui desideri sottoscrivere la risorsa.
   - Una breve giustificazione per la tua richiesta di abbonamento.
4. Scegliere Subscribe (Effettua sottoscrizione).

   Riceverai una notifica nel portale dati quando l'editore approva la tua richiesta.

Per visualizzare lo stato della richiesta di abbonamento, individuate e scegliete il progetto con cui avete sottoscritto la risorsa. Vai alla scheda Dati del progetto, quindi scegli Dati richiesti dal riquadro di navigazione a sinistra. Questa pagina elenca le risorse a cui il progetto ha richiesto l'accesso. È possibile filtrare l'elenco in base allo stato della richiesta.

Approva o rifiuta una richiesta di abbonamento

Amazon ti DataZone consente di trovare, accedere e utilizzare le risorse nel DataZone catalogo Amazon. Quando trovi una risorsa nel catalogo a cui desideri accedere, devi abbonarti alla risorsa, il che crea una richiesta di abbonamento. Un approvatore può quindi approvare o rifiutare la richiesta.

Devi essere un membro del progetto proprietario (il progetto che ha pubblicato la risorsa) per approvare o rifiutare una richiesta di abbonamento.

Per approvare o rifiutare una richiesta di abbonamento

1. Vai all'URL del portale DataZone dati di Amazon e accedi utilizzando Single Sign-On (SSO) o le tue credenziali. AWS Se sei un DataZone amministratore Amazon, puoi accedere alla DataZone console Amazon all'indirizzo https://console.aws.amazon.com/datazone e accedere con il Account AWS luogo in cui è stato creato il dominio, quindi scegliere Open data portal.
2. Nel portale dati, scegli Sfoglia l'elenco dei progetti e seleziona il progetto che contiene la risorsa con la richiesta di abbonamento.
3. Vai alla scheda Dati, quindi scegli Richieste in arrivo dal riquadro di navigazione a sinistra.
4. Individua la richiesta e scegli Visualizza richiesta. Puoi filtrare per In sospeso per visualizzare solo le richieste ancora aperte.

5. Controlla la richiesta di iscrizione e il motivo dell'accesso e decidi se approvarla o rifiutarla.
6. (Facoltativo) Inserisci una risposta che spieghi il motivo per cui accetti o rifiuti la richiesta.
7. Scegli Approva o Rifiuta.

In qualità di proprietario del progetto, puoi revocare l'abbonamento in qualsiasi momento. Per ulteriori informazioni, consulta the section called “Revoca un abbonamento esistente”.

Per visualizzare tutte le richieste di abbonamento, consulta. Utilizzo DataZone degli eventi e delle notifiche di Amazon

Revoca un abbonamento esistente

Amazon ti DataZone consente di trovare, accedere e utilizzare le risorse nel DataZone catalogo Amazon. Quando trovi una risorsa nel catalogo a cui desideri accedere, devi abbonarti alla risorsa, il che crea una richiesta di abbonamento. Un approvatore può quindi approvare o richiedere la tua richiesta. Potrebbe essere necessario revocare un abbonamento dopo averlo approvato, o perché l'approvazione è stata un errore o perché l'abbonato non ha più bisogno di accedere alla risorsa.

Devi essere un membro del progetto proprietario (il progetto che ha pubblicato la risorsa) per revocare un abbonamento.

Per revocare un abbonamento

1. Vai all'URL del portale DataZone dati di Amazon e accedi utilizzando Single Sign-On (SSO) o le tue credenziali. AWS Se sei un DataZone amministratore Amazon, puoi accedere alla DataZone console Amazon all'indirizzo https://console.aws.amazon.com/datazone e accedere con il Account AWS luogo in cui è stato creato il dominio, quindi scegliere Open data portal.
2. Scegli Seleziona progetto dal pannello di navigazione in alto e seleziona il progetto che contiene l'abbonamento che desideri revocare.
3. Vai alla scheda Dati, quindi scegli Richieste in arrivo dal riquadro di navigazione a sinistra.
4. Individua l'abbonamento che desideri revocare e scegli Visualizza abbonamento.
5. (Facoltativo) Attiva la casella di controllo per consentire al sottoscrittore di mantenere la risorsa tra gli obiettivi di sottoscrizione del progetto. Un obiettivo di sottoscrizione è un riferimento a un insieme di risorse in cui i dati sottoscritti possono essere resi disponibili all'interno di un ambiente.

Se desideri revocare l'accesso alla risorsa dalla destinazione dell'abbonamento in un secondo momento, devi farlo in. AWS Lake Formation

6. Scegli l'abbonamento Revoke.

Non puoi riapprovare un abbonamento dopo averlo revocato. Il sottoscrittore deve sottoscrivere nuovamente la risorsa per consentirti di approvarla.

Annullare una richiesta di abbonamento

Amazon ti DataZone consente di trovare, accedere e utilizzare le risorse nel DataZone catalogo Amazon. Quando trovi una risorsa nel catalogo a cui desideri accedere, devi abbonarti alla risorsa, il che crea una richiesta di abbonamento. Un approvatore può quindi approvare o richiedere la tua richiesta. Potresti dover annullare una richiesta di abbonamento in sospeso, perché l'hai inviata per errore o perché non hai più bisogno dell'accesso in lettura alla risorsa.

Per annullare una richiesta di abbonamento, devi essere il proprietario del progetto o il collaboratore.

Per annullare una richiesta di abbonamento

1. Vai all'URL del portale DataZone dati di Amazon e accedi utilizzando Single Sign-On (SSO) o le tue credenziali. AWS Se sei un DataZone amministratore Amazon, puoi accedere alla DataZone console Amazon all'indirizzo https://console.aws.amazon.com/datazone e accedere con il Account AWS luogo in cui è stato creato il dominio, quindi scegliere Open data portal.
2. Scegli Seleziona progetto dal pannello di navigazione in alto e seleziona il progetto che contiene la richiesta di abbonamento.
3. Vai alla scheda Dati per il progetto, quindi scegli Dati richiesti dal riquadro di navigazione a sinistra. Questa pagina elenca le risorse a cui il progetto ha richiesto l'accesso.
4. Filtra per Richiesto per visualizzare solo le richieste ancora in sospeso. Individua la richiesta e scegli Visualizza richiesta.
5. Controlla la richiesta di abbonamento e scegli Annulla richiesta.

Se desideri sottoscrivere nuovamente la risorsa (o una risorsa diversa), consultathe section called “Richiedi l'abbonamento agli asset”.

Annullare l'iscrizione a una risorsa

Amazon ti DataZone consente di trovare, accedere e utilizzare le risorse nel DataZone catalogo Amazon. Quando trovi una risorsa nel catalogo a cui desideri accedere, devi abbonarti alla risorsa, il che crea una richiesta di abbonamento. Un approvatore può quindi approvare o richiedere la tua richiesta. Potresti dover annullare l'iscrizione a una risorsa, o perché ti sei iscritto per errore e sei stato approvato, o perché non hai più bisogno dell'accesso in lettura alla risorsa.

Devi essere membro di un progetto per annullare l'iscrizione a una delle sue risorse.

Per annullare l'iscrizione a una risorsa

1. Vai all'URL del portale DataZone dati di Amazon e accedi utilizzando Single Sign-On (SSO) o le tue credenziali. AWS Se sei un DataZone amministratore Amazon, puoi accedere alla DataZone console Amazon all'indirizzo https://console.aws.amazon.com/datazone e accedere con il Account AWS luogo in cui è stato creato il dominio, quindi scegliere Open data portal.
2. Scegli Seleziona progetto dal pannello di navigazione in alto e seleziona il progetto che contiene la risorsa a cui desideri annullare l'iscrizione.
3. Vai alla scheda Dati del progetto, quindi scegli Dati richiesti dal riquadro di navigazione a sinistra. Questa pagina elenca le risorse a cui il progetto ha richiesto l'accesso.
4. Filtra per Approvato per visualizzare solo le richieste che sono state approvate. Individua la richiesta e scegli Visualizza abbonamento.
5. Controlla l'abbonamento e scegli Annulla iscrizione.

Se desideri sottoscrivere nuovamente la risorsa (o una risorsa diversa), consulta. the section called “Richiedi l'abbonamento agli asset”

Utilizzo dei ruoli IAM esistenti per soddisfare DataZone gli abbonamenti Amazon

Nella versione corrente, Amazon ti DataZone supporta nell'utilizzo dei ruoli IAM esistenti per accedere ai dati. A tal fine, puoi creare un obiettivo di abbonamento nell' DataZone ambiente Amazon che stai utilizzando per completare l'abbonamento. Per creare un obiettivo di sottoscrizione per un ambiente in uno degli AWS account associati, puoi utilizzare i seguenti passaggi:

Passaggio 1: assicurati che il tuo DataZone dominio Amazon utilizzi la versione 2 o successiva della politica RAM

1. Vai alla pagina Shared by me: Resource shares nella console AWS RAM.
2. Poiché le condivisioni di risorse AWS RAM esistono in AWS regioni specifiche, scegli la AWS regione appropriata dall'elenco a discesa nell'angolo in alto a destra della console.
3. Seleziona la condivisione di risorse corrispondente al tuo DataZone dominio Amazon, quindi scegli Modifica. Puoi identificare la condivisione RAM per il DataZone dominio Amazon utilizzando il nome o l'ID del dominio poiché la condivisione RAM viene creata con il nome:`DataZone-<domain-name>-<domain-id>`.
4. Scegli Avanti per procedere al passaggio successivo in cui puoi controllare la versione della politica RAM e modificarla.
5. Assicurati che la versione della politica RAM sia la versione 2 o successiva. In caso contrario, utilizza il menu a discesa per selezionare la versione 2 o successiva.
6. Scegli Vai al passaggio 4: Rivedi e aggiorna.
7. Scegli Aggiorna condivisione risorse.

Passaggio 2: crea un obiettivo di abbonamento da un account associato

- Nella versione corrente, Amazon DataZone supporta la creazione di obiettivi di abbonamento utilizzando solo le API. Di seguito sono riportati alcuni esempi del payload che puoi utilizzare per creare un obiettivo di abbonamento per soddisfare gli abbonamenti alle tue tabelle AWS Glue e alle tabelle o viste di Amazon Redshift. Per ulteriori informazioni, consulta. CreateSubscriptionTarget

  Esempio di obiettivo di abbonamento per AWS Glue

```
{
        "domainIdentifier": "<DOMAIN_ID>",
        "environmentIdentifier": "<ENVIRONMENT_ID>",
        "name": "<SUBSCRIPTION_TARGET_NAME>",
        "type": "GlueSubscriptionTargetType",
        "authorizedPrincipals" : ["IAM_ROLE_ARN"],
        "subscriptionTargetConfig" : [{"content": "{\"databaseName\":
 \"<DATABASE_NAME>\"}", "formName": "GlueSubscriptionTargetConfigForm"}],
        "manageAccessRole": "<GLUE_DATA_ACCESS_ROLE_IN_ASSOCIATED_ACCOUNT_ARN>",
        "applicableAssetTypes" : ["GlueTableAssetType"],
```

```
        "provider": "Amazon DataZone"
}
```

Esempio di obiettivo di sottoscrizione per Amazon Redshift:

```
{
        "domainIdentifier": "<DOMAIN_ID>",
        "environmentIdentifier": "<ENVIRONMENT_ID>",
        "name": "<SUBSCRIPTION_TARGET_NAME>",
        "type": "RedshiftSubscriptionTargetType",
        "authorizedPrincipals" : ["REDSHIFT_DATABASE_ROLE_NAME"],
        "subscriptionTargetConfig" : [{"content": "{\"databaseName\":
 \"<DATABASE_NAME>\", \"secretManagerArn\": \"<SECRET_MANAGER_ARN>
\",\"clusterIdentifier\": \"<CLUSTER_IDENTIFIER>\"}", "formName":
 "RedshiftSubscriptionTargetConfigForm"}],
        "manageAccessRole":
 "<REDSHIFT_DATA_ACCESS_ROLE_IN_ASSOCIATED_ACCOUNT_ARN>",
        "applicableAssetTypes" : ["RedshiftViewAssetType",
 "RedshiftTableAssetType"],
        "provider": "Amazon DataZone"
}
```

Important

- L'EnvironmentIdentifier che usi nella chiamata API precedente dovrebbe esistere nello stesso account associato da cui stai effettuando la chiamata API. In caso contrario, la chiamata API non avrà esito positivo.
- L'ARN del ruolo IAM che usi in «AuthorizedPrincipal» è il ruolo a cui Amazon DataZone concederà l'accesso dopo l'aggiunta di una risorsa sottoscritta all'obiettivo dell'abbonamento. Questi principali autorizzati devono appartenere allo stesso account dell'ambiente in cui viene creato il target di sottoscrizione.
- Il valore per il campo provider deve essere «Amazon DataZone» per consentire DataZone ad Amazon di completare l'adempimento dell'abbonamento.
- Il nome del database fornito subscriptionTargetConfig dovrebbe già esistere nell'account in cui viene creata la destinazione. Amazon non DataZone creerà

questo database. Assicurati inoltre che il ruolo di gestione dell'accesso disponga dell'autorizzazione CREATE TABLE su questo database.

- Assicurati inoltre che i ruoli (ruolo IAM per AWS Glue e ruolo database per Amazon Redshift) forniti come principali autorizzati esistano già nell'account di ambiente. Per gli obiettivi di abbonamento ad Amazon Redshift, sono necessari aggiornamenti aggiuntivi per il ruolo assunto durante la connessione al cluster. Questo ruolo deve avere un RedshiftDbRoles tag associato al ruolo. Il valore del tag può essere un elenco separato da virgole. Il valore deve essere il ruolo del database fornito come principale autorizzato durante la creazione dell'obiettivo di sottoscrizione.

Fase 3: Abbonarsi a una nuova tabella e completare la sottoscrizione al nuovo obiettivo

- Dopo aver creato l'obiettivo di abbonamento, puoi iscriverti a una nuova tabella e Amazon DataZone soddisferà l'obiettivo sopra indicato. Per ulteriori informazioni, consulta Iscrizione ai dati.

Concessione dell'accesso ai dati

Le seguenti attività forniscono dettagli sulla concessione dell'accesso agli abbonamenti approvati agli asset in Amazon. DataZone

In Amazon DataZone, le richieste di abbonamento e gli abbonamenti approvati o concessi per l'accesso in lettura agli asset vengono gestiti dagli approvatori delle sottoscrizioni. L'approvazione dell'abbonamento a una risorsa è determinata dal contratto di pubblicazione con cui tale risorsa è stata pubblicata nel DataZone catalogo Amazon.

Argomenti

- Concedi l'accesso agli asset gestiti AWS Glue Data Catalog
- Concedi l'accesso agli asset gestiti di Amazon Redshift
- Concedi l'accesso agli abbonamenti approvati agli asset non gestiti

Concedi l'accesso agli asset gestiti AWS Glue Data Catalog

> **Note**
>
> La gestione degli accessi agli AWS Glue Data Catalog asset mediante il metodo AWS Lake Formation LF-TBAC non è supportata.
> Il supporto per la condivisione di risorse tra regioni non AWS Glue Data Catalog è supportato.

Una volta approvata una richiesta di abbonamento agli AWS Glue Data Catalog asset gestiti, Amazon aggiunge DataZone automaticamente questi asset a tutti gli ambienti data lake esistenti nel progetto. Amazon DataZone quindi concede e gestisce l'accesso alle AWS Glue Data Catalog tabelle approvate per tuo conto tramite AWS Lake Formation. Per il progetto destinato agli abbonati, le risorse concesse vengono visualizzate nelle risorse AWS Glue Data Catalog come del tuo account. Puoi quindi utilizzare Amazon Athena per interrogare le tabelle.

> **Note**
>
> Se viene aggiunto un nuovo ambiente data lake al progetto dopo che gli AWS Glue Data Catalog asset sottoscritti sono stati aggiunti automaticamente agli ambienti data lake esistenti, è necessario aggiungere manualmente gli AWS Glue Data Catalog asset sottoscritti a questo nuovo ambiente data lake. Puoi farlo scegliendo l'opzione Aggiungi sovvenzione nella scheda Dati della pagina di panoramica del progetto nel portale DataZone dati Amazon.

Affinché Amazon DataZone possa concedere l'accesso alle tabelle di AWS Glue Data Catalog, devono essere soddisfatte le seguenti condizioni.

- La tabella AWS Glue deve essere gestita da Lake Formation poiché Amazon DataZone concede l'accesso gestendo le autorizzazioni di Lake Formation.
- Il ruolo Manage access per l'ambiente data lake utilizzato per pubblicare la tabella AWS Glue Data Catalog deve avere le seguenti autorizzazioni Lake Formation:
  - `DESCRIBE`e `DESCRIBE GRANTABLE` autorizzazioni sul database AWS Glue che contiene la tabella pubblicata.
  - `DESCRIBE`,`SELECT`,`DESCRIBE GRANTABLE`, `SELECT GRANTABLE` permessi in Lake Formation sulla tabella pubblicata stessa.

Per ulteriori informazioni, consulta Concessione e revoca delle autorizzazioni sulle risorse del catalogo nella Guida per gli sviluppatori.AWS Lake Formation

Concedi l'accesso agli asset gestiti di Amazon Redshift

Quando viene approvato un abbonamento a una tabella o vista di Amazon Redshift, Amazon DataZone può aggiungere automaticamente la risorsa sottoscritta a tutti gli ambienti di data warehouse all'interno del progetto, in modo che i membri del progetto possano interrogare i dati utilizzando il link Amazon Redshift Query Editor all'interno dei propri ambienti. Sotto il cofano DataZone, Amazon crea le concessioni e le condivisioni di dati necessarie tra l'origine e il target dell'abbonamento.

Il processo di concessione dell'accesso varia a seconda di dove si trovano il database di origine (editore) e il database di destinazione (sottoscrittore).

- Stesso cluster, stesso database: se i dati devono essere condivisi all'interno dello stesso database, Amazon DataZone concede le autorizzazioni direttamente sulla tabella di origine.
- Stesso cluster, database diverso: se i dati devono essere condivisi tra due database all'interno dello stesso cluster, Amazon DataZone crea una vista nel database di destinazione e vengono concesse le autorizzazioni per la vista creata.
- Cluster diverso dello stesso account: Amazon DataZone crea un datashare tra il cluster di origine e quello di destinazione e crea una vista sulla parte superiore della tabella condivisa. Le autorizzazioni sono concesse per la visualizzazione.
- Cross-account: come sopra, ma è necessario un passaggio aggiuntivo per autorizzare la condivisione dei dati tra account sul lato del cluster di produttori e un altro passaggio per associare la condivisione dei dati sul lato del cluster di consumatori.

> **Note**
>
> Se viene aggiunto un nuovo ambiente di data warehouse al progetto dopo che gli asset Amazon Redshift sottoscritti sono stati aggiunti automaticamente agli ambienti di data warehouse esistenti, devi aggiungere manualmente gli asset Amazon Redshift sottoscritti a questo nuovo ambiente di data warehouse. Puoi farlo scegliendo l'opzione Aggiungi sovvenzione nella scheda Dati della pagina di panoramica del progetto nel portale DataZone dati Amazon.

Assicurati che i cluster Amazon Redshift di pubblicazione e sottoscrizione soddisfino tutti i requisiti per le condivisioni di dati Amazon Redshift. Per ulteriori informazioni, consulta la Amazon Redshift Developer Guide.

> **Note**
>
> Amazon DataZone supporta la concessione automatica di abbonamenti agli asset Amazon Redshift Cluster e Amazon Redshift Serverless.
> La condivisione di dati tra regioni tramite Amazon Redshift non è supportata.

> **Note**
>
> Nella versione attuale, Amazon DataZone può gestire l'accesso alle tabelle e alle viste di Amazon Redshift solo se i cluster o i gruppi di lavoro Amazon Redshift di origine e destinazione si trovano negli account che appartengono AWS alla stessa organizzazione. AWS

Concedi l'accesso agli abbonamenti approvati agli asset non gestiti

Amazon DataZone consente agli utenti di pubblicare qualsiasi tipo di risorsa nel catalogo di dati aziendali. Per alcune di queste risorse, Amazon DataZone può gestire automaticamente le concessioni di accesso. Queste risorse sono chiamate risorse gestite e includono tabelle AWS Glue Data Catalog gestite da Lake Formation e tabelle e viste di Amazon Redshift. Tutte le altre risorse a cui Amazon non DataZone può concedere automaticamente abbonamenti vengono chiamate non gestite.

Amazon ti DataZone offre un percorso per gestire le concessioni di accesso per le tue risorse non gestite. Quando un abbonamento a una risorsa nel catalogo dei dati aziendali viene approvato dal proprietario dei dati, Amazon DataZone pubblica un evento su Amazon EventBridge nel tuo account insieme a tutte le informazioni necessarie nel payload che ti consentono di creare le concessioni di accesso tra l'origine e la destinazione. Quando ricevi questo evento, puoi attivare un gestore personalizzato che può utilizzare le informazioni relative all'evento per creare le concessioni o le autorizzazioni necessarie. Una volta concesso l'accesso, puoi segnalare e aggiornare lo stato dell'abbonamento in Amazon in DataZone modo che possa notificare agli utenti abbonati all'asset che possono iniziare a utilizzare l'asset. Per ulteriori informazioni, consulta Utilizzo DataZone degli eventi e delle notifiche di Amazon.

Consumo di dati

Le seguenti attività forniscono dettagli sul consumo dei dati a cui ti sei abbonato su Amazon DataZone.

Argomenti

Interroga i dati in Amazon Athena o Amazon Redshift

In Amazon DataZone, una volta che un abbonato ha accesso a una risorsa nel catalogo, può utilizzarla (eseguire query e analizzare) utilizzando Amazon Athena o Amazon Redshift query editor v2. Devi essere il proprietario o il collaboratore del progetto per completare questa attività. A seconda dei blueprint abilitati nel progetto, Amazon DataZone fornisce collegamenti ad Amazon Athena e/o all'editor di query Amazon Redshift v2 nel riquadro a destra della pagina del progetto nel portale dati.

1. Vai all'URL del portale DataZone dati di Amazon e accedi utilizzando Single Sign-On (SSO) o le tue credenziali. AWS Se sei un DataZone amministratore Amazon, puoi accedere alla DataZone console Amazon all'indirizzo https://console.aws.amazon.com/datazone e accedere con il Account AWS luogo in cui è stato creato il dominio, quindi scegliere Open data portal.
2. Nel portale DataZone dati di Amazon, scegli Browse Projects List, quindi trova e scegli il progetto in cui hai i dati che desideri analizzare.
3. Se il blueprint Data Lake è abilitato su questo progetto, viene visualizzato un collegamento ad Amazon Athena nel pannello a destra della home page del progetto.

   Se il blueprint Data Warehouse è abilitato su questo progetto, nel pannello a destra della home page del progetto viene visualizzato un collegamento all'editor di query.

   > **Note**
   >
   > I blueprint sono definiti nel profilo di ambiente con cui viene creato un progetto.

Argomenti

Interroga i dati con Amazon Athena

Scegli il link Amazon Athena per aprire l'editor di query Amazon Athena in una nuova scheda del browser utilizzando le credenziali del progetto per l'autenticazione. Il DataZone progetto Amazon a cui stai lavorando viene selezionato automaticamente come gruppo di lavoro corrente nell'editor di query.

Nell'editor di query di Amazon Athena, scrivi ed esegui le tue query. Alcune attività comuni includono:

- Interroga e analizza gli asset sottoscritti
- Crea nuove tabelle
- Crea una tabella dai risultati delle query (CTAS) da un bucket S3 esterno

Interroga e analizza gli asset sottoscritti

Se l'accesso alle risorse a cui è sottoscritto il tuo progetto non viene concesso automaticamente da Amazon DataZone, devi essere autorizzato ad accedere ai dati sottostanti. Per ulteriori informazioni su come concedere l'accesso a queste risorse, consultaConcedi l'accesso agli abbonamenti approvati agli asset non gestiti.

Se l'accesso alle risorse a cui è sottoscritto il tuo progetto viene concesso automaticamente da Amazon DataZone, puoi eseguire query SQL sulle tabelle e vedere i risultati in Amazon Athena. Per ulteriori informazioni sull'uso di SQL in Amazon Athena, consulta il riferimento SQL per Athena.

Quando accedi all'editor di query di Amazon Athena dopo aver scelto il link Amazon Athena nel pannello a destra della home page del progetto, viene visualizzato un menu a discesa Progetto nell'angolo in alto a destra dell'editor di query di Amazon Athena e il contesto del progetto viene selezionato automaticamente.

Puoi visualizzare i seguenti database nel menu a discesa Database:

- Un database di pubblicazione (*{environmentname}*_pub_db). Lo scopo di questo database è fornirti un ambiente in cui puoi produrre nuovi dati nel contesto del tuo progetto e quindi essere in grado di pubblicare questi dati nel DataZone catalogo Amazon. I proprietari e i collaboratori del progetto hanno accesso in lettura e scrittura a questo database. I visualizzatori del progetto hanno accesso solo in lettura a questo database.
- Un database di sottoscrizioni (*{environmentname}*_sub_db). Lo scopo di questo database è condividere con te i dati a cui ti sei iscritto come membro del progetto nel DataZone catalogo Amazon e consentirti di interrogare tali dati.

Crea nuove tabelle

Se ti sei connesso a un bucket S3 esterno, puoi utilizzare Amazon Athena per interrogare e analizzare gli asset da un bucket Amazon S3 esterno. In questo scenario, Amazon DataZone non dispone delle autorizzazioni per concedere l'accesso diretto ai dati sottostanti nel bucket Amazon S3 esterno e i dati Amazon S3 esterni creati all'esterno del progetto non vengono gestiti automaticamente in Lake Formation e non possono essere gestiti da Amazon. DataZone Un'alternativa consiste nel copiare i dati dal bucket Amazon S3 esterno in una nuova tabella all'interno del bucket Amazon S3 del progetto utilizzando un'istruzione in Amazon Athena. `CREATE TABLE` Quando esegui una `CREATE TABLE` query in Amazon Athena, registri la tua tabella con. AWS Glue Data Catalog

Puoi specificare il percorso dei dati in Amazon S3, utilizzare la proprietà `LOCATION`, come illustrato nel seguente breve esempio:

```
CREATE EXTERNAL TABLE 'test_table'(
...
)
ROW FORMAT ...
STORED AS INPUTFORMAT ...
OUTPUTFORMAT ...
LOCATION 's3://bucketname/folder/'
```

Per ulteriori informazioni, consulta Table location in Amazon S3.

Crea una tabella dai risultati delle query (CTAS) da un bucket S3 esterno

Quando sottoscrivi una risorsa, l'accesso ai dati sottostanti è di sola lettura. Puoi usare Amazon Athena per creare una copia della tabella. In Amazon Athena, la `A CREATE TABLE AS SELECT (CTAS)` query crea una nuova tabella in Amazon Athena dai risultati di `SELECT` un'istruzione di un'altra query. Per informazioni sulla sintassi CTAS, consulta CREATE TABLE AS.

L'esempio seguente crea una tabella copiando tutte le colonne di una tabella:

```
CREATE TABLE new_table AS
SELECT *
FROM old_table;
```

Nella seguente variazione dello stesso esempio, l'istruzione `SELECT` comprende anche una clausola `WHERE`. In questo caso, la query seleziona solo le righe dalla tabella che soddisfano la clausola `WHERE`:

```
CREATE TABLE new_table AS
SELECT *
FROM old_table WHERE condition;
```

L'esempio seguente crea una nuova query che viene eseguita su un set di colonne da un'altra tabella:

```
CREATE TABLE new_table AS
SELECT column_1, column_2, ... column_n
FROM old_table;
```

Questa variazione dello stesso esempio crea una nuova tabella in base a colonne specifiche di più tabelle:

```
CREATE TABLE new_table AS
SELECT column_1, column_2, ... column_n
FROM old_table_1, old_table_2, ... old_table_n;
```

Queste tabelle appena create fanno ora parte del AWS Glue database dei tuoi progetti e possono essere rese individuabili da altri e condivise con altri DataZone progetti Amazon pubblicando i dati come risorsa nel catalogo Amazon DataZone.

Interroga i dati con Amazon Redshift

Nel portale DataZone dati di Amazon, apri un ambiente che utilizza il modello di data warehouse. Scegli il link Amazon Redshift nel pannello a destra nella pagina dell'ambiente. Si apre una finestra di dialogo di conferma con i dettagli necessari per aiutarti a stabilire una connessione al cluster Amazon Redshift o al gruppo di lavoro Amazon Redshift Serverless del tuo ambiente nell'editor di query

Amazon Redshift v2.0. Dopo aver identificato i dettagli necessari per stabilire la connessione, scegli il pulsante Apri Amazon Redshift. Questo apre l'editor di query Amazon Redshift v2.0 in una nuova scheda del browser utilizzando credenziali temporanee dell'ambiente Amazon. DataZone

Nell'editor di query, segui i passaggi seguenti a seconda che il tuo ambiente utilizzi un gruppo di lavoro Serverless Amazon Redshift o un cluster Amazon Redshift.

Per un gruppo di lavoro Serverless Amazon Redshift

1. Nell'editor di query, identifica il gruppo di lavoro Amazon Redshift Serverless del tuo DataZone ambiente Amazon, fai clic con il pulsante destro del mouse e scegli Crea una connessione.
2. Scegli Federated User per l'autenticazione.
3. Fornisci il nome del database DataZone dell'ambiente Amazon.
4. Scegli Crea connessione.

Per un cluster Amazon Redshift:

1. Nell'editor di query, identifica il cluster Amazon Redshift del tuo DataZone ambiente Amazon, fai clic con il pulsante destro del mouse e scegli Crea una connessione.
2. Seleziona Credenziali temporanee utilizzando la tua identità IAM per l'autenticazione.
3. Se il metodo di autenticazione sopra indicato non è disponibile, apri le impostazioni dell'account selezionando il pulsante a forma di ingranaggio nell'angolo in basso a sinistra, scegli Autentica con credenziali IAM e salva. Questa è un' one-time-onlyimpostazione.
4. Fornisci il nome del database DataZone dell'ambiente Amazon per creare la connessione.
5. Scegli Crea connessione.

Ora puoi iniziare a eseguire query sulle tabelle e sulle viste all'interno del cluster Amazon Redshift o del gruppo di lavoro Amazon Redshift Serverless configurato per il tuo ambiente Amazon. DataZone

Tutte le tabelle o le viste di Amazon Redshift a cui ti sei abbonato sono collegate al cluster Amazon Redshift o al gruppo di lavoro Amazon Redshift Serverless configurato per l'ambiente. Puoi iscriverti alle tabelle e alle viste e pubblicare nuove tabelle e viste che crei nel cluster o nel database del tuo ambiente.

Ad esempio, prendiamo uno scenario in cui un ambiente è collegato a un cluster Amazon Redshift chiamato `redshift-cluster-1` e a un database chiamato `dev` in quel cluster. Utilizzando il portale DataZone dati Amazon, puoi interrogare le tabelle e le viste che vengono aggiunte al tuo ambiente.

Nella `Analytics tools` sezione nel riquadro a destra del portale dati, puoi scegliere il link Amazon Redshift per questo ambiente, che apre l'editor di query. Puoi quindi fare clic con il pulsante destro del mouse sul `redshift-cluster-1` cluster e creare una connessione utilizzando credenziali temporanee utilizzando la tua identità IAM. Una volta stabilita la connessione, puoi vedere tutte le tabelle e le viste a cui il tuo ambiente ha accesso nel database di sviluppo.

Utilizzo DataZone degli eventi e delle notifiche di Amazon

Amazon ti DataZone tiene informato sulle attività importanti all'interno del tuo portale dati, come richieste di abbonamento, aggiornamenti, commenti ed eventi di sistema. Amazon ti DataZone fornisce queste informazioni recapitando i messaggi nella casella di posta dedicata nel portale dati o tramite il bus EventBridge predefinito di Amazon.

Argomenti

Lavorare con gli eventi tramite la casella di posta dedicata nel portale DataZone dati di Amazon

Amazon DataZone fornisce una casella di posta dedicata nel portale dati in cui puoi visualizzare e agire sui tuoi messaggi. I messaggi recenti appaiono anche nella home page, nella pagina del progetto e nella pagina del catalogo. Ad esempio, se un utente richiede l'accesso a una risorsa di dati, i proprietari e i collaboratori del progetto di pubblicazione di tale risorsa visualizzano la richiesta nel portale dati e, una volta intrapresa un'azione, i membri del progetto sottoscrittore relativo a questa richiesta visualizzano la notifica nel portale dati. Esistono due tipi di messaggi:

- Attività: questi messaggi informano il destinatario che è necessaria un'azione da qualche parte. Hanno un campo di stato opzionale che puoi usare per il tracciamento.
- Eventi: questi messaggi sono informativi e non hanno uno stato assegnato. Gli eventi forniscono una traccia di controllo degli aggiornamenti recenti.

In Amazon DataZone, i messaggi vengono generati per i seguenti tipi di eventi:

Categoria dell'evento	Nome evento	Descrizione dell'evento	Tipo di evento
Subscription	Richiesta di abbonamento creata	L'evento viene generato quando viene creata	Attività

Categoria dell'evento	Nome evento	Descrizione dell'evento	Tipo di evento
		una richiesta di abbonamento	
Subscription	Richiesta di iscrizione accettata	L'evento viene generato quando viene accettata una richiesta di abbonamento	Evento
Subscription	Richiesta di iscrizione rifiutata	L'evento viene generato quando una richiesta di abbonamento viene rifiutata	Evento
Subscription	Richiesta di iscrizione eliminata	L'evento viene generato quando viene eliminata una richiesta di iscrizione	Evento
Progetto	Creazione del progetto riuscita	L'evento viene generato quando la creazione del progetto ha esito positivo	Evento
Appartenenza al progetto	L'aggiunta di un membro al progetto è avvenuta con successo	L'evento viene generato quando un nuovo membro viene aggiunto a un progetto	Evento

Categoria dell'evento	Nome evento	Descrizione dell'evento	Tipo di evento
Appartenenza al progetto	Rimozione dei membri del progetto avvenuta con successo	L'evento viene generato quando un membro viene rimosso da un progetto	Evento
Appartenenza al progetto	La modifica del ruolo di membro del progetto è avvenuta con successo	L'evento è stato generato il ruolo di un membro nel progetto è cambiato	Evento
Ambiente	La distribuzione dell'ambiente è iniziata	L'evento viene generato quando viene avviata la distribuzione di un ambiente	Evento
Ambiente	Implementazione dell'ambiente completata	L'evento viene generato quando l'implementazione di un ambiente viene completata correttamente	Evento
Ambiente	Installazione dell'ambiente non riuscita	L'evento viene generato quando l'implementazione di un ambiente fallisce	Evento
Ambiente	È stato avviato un flusso di lavoro personalizzato per la distribuzione dell'ambiente	L'evento viene generato quando viene avviato un ambiente con flusso di lavoro personalizzato	Evento

Categoria dell'evento	Nome evento	Descrizione dell'evento	Tipo di evento
Asset di dati	Risorsa aggiunta all'inventario	L'evento viene generato quando una nuova risorsa di dati viene aggiunta all'inventario, ad esempio aggiunta al catalogo in stato di bozza	Evento
Asset di dati	Risorsa pubblicata	L'evento viene generato quando viene pubblicata una nuova risorsa di dati, ovvero è disponibile per l'abbonamento	Evento
Asset di dati	Lo schema degli asset è stato modificato	L'evento viene generato quando lo schema di un asset è cambiato rispetto al precedente processo di inserimento	Evento
Sottoscrizione in corso	Abbonamento creato	L'evento viene generato quando qualcuno richiede di iscriversi a una risorsa di dati	Attività

Categoria dell'evento	Nome evento	Descrizione dell'evento	Tipo di evento
Sottoscrizione in corso	Abbonamento approvato	L'evento viene generato quando un abbonamento viene approvato dal proprietario o dal collaboratore del progetto di pubblicazione	Evento
Sottoscrizione in corso	Abbonamento rifiutato	L'evento viene generato quando un abbonamento viene rifiutato dal proprietario o dal collaboratore del progetto di pubblicazione	Evento
Sottoscrizione in corso	Abbonamento eliminato	L'evento viene generato quando un abbonamento viene annullato dall'abbonato	Evento
Sottoscrizione in corso	È richiesta la concessione dell'abbonamento	L'evento viene generato quando qualcuno richiede l'accesso a una risorsa	Evento

Categoria dell'evento	Nome evento	Descrizione dell'evento	Tipo di evento
Sottoscrizione in corso	Concessione dell'abbonamento completata	L'evento viene generato quando a un abbonamento viene concesso l'accesso alla risorsa dal proprietario o dal collaboratore del progetto editoriale	Evento
Sottoscrizione in corso	Concessione dell'abbonamento non riuscita	L'evento viene generato quando la concessione di una sottoscrizione fallisce	Evento
Sottoscrizione in corso	È richiesta la revoca della concessione dell'abbonamento	L'evento viene generato quando una concessione di abbonamento revocata viene avviata dal proprietario o dal collaboratore del progetto editoriale	Evento
Sottoscrizione in corso	La revoca della concessione dell'abbonamento è stata completata	L'evento viene generato quando viene completata la revoca della concessione di un abbonamento	Evento

Categoria dell'evento	Nome evento	Descrizione dell'evento	Tipo di evento
Sottoscrizione in corso	La revoca della concessione dell'abbonamento non è riuscita	L'evento viene generato quando la revoca della concessione di un abbonamento fallisce	Evento
Generazione automatizzata di nomi aziendali	Nome aziendale generato con successo	L'evento viene generato quando il processo automatizzato generato dal nome aziendale viene completato correttamente	Evento
Generazione automatizzata di nomi aziendali	Generazione del nome aziendale non riuscita	L'evento viene generato quando il processo automatizzato generato dal nome aziendale ha esito negativo	Evento
Esecuzione dell'origine dati	Fonte di dati creata	L'evento viene generato quando viene creata una nuova fonte di dati	Evento
Origine dati eseguita	Fonte dati aggiornata	L'evento viene generato quando viene aggiornata un'origine dati esistente	Evento

Categoria dell'evento	Nome evento	Descrizione dell'evento	Tipo di evento
Origine dati eseguita	L'esecuzione della fonte di dati è stata attivata	L'evento viene generato quando viene avviata l'esecuzione di un'origine dati	Evento
Esecuzione della fonte di dati	Esecuzione dell'origine dati riuscita	L'evento viene generato quando l'esecuzione di un'origine dati ha esito positivo	Evento
Esecuzione dell'origine dati	Esecuzione dell'origine dati non riuscita	L'evento viene generato quando l'esecuzione di un'origine dati non riesce	Evento

Per visualizzare le attività nella posta in arrivo del portale dati, completa i seguenti passaggi:

1. Accedi al portale DataZone dati di Amazon utilizzando l'URL del portale dati e accedi utilizzando il tuo SSO o AWS le tue credenziali. Se sei un DataZone amministratore Amazon, puoi ottenere l'URL del portale dati accedendo alla DataZone console Amazon all'indirizzo https://console.aws.amazon.com/datazone nell' AWS account in cui è stato creato il DataZone dominio Amazon.
2. Nel portale dati, per visualizzare un pop-up con la serie di attività recenti, seleziona l'icona a forma di campana accanto alla barra di ricerca.
3. Seleziona Visualizza tutto per visualizzare tutte le attività. Puoi modificare le visualizzazioni e visualizzare tutti gli eventi selezionando la scheda Eventi.
4. Puoi filtrare la ricerca in base all'oggetto dell'evento, allo stato attivo o inattivo o all'intervallo di date.
5. Scegli una singola attività per accedere alla posizione in cui puoi rispondere all'attività.

Per visualizzare gli eventi nella posta in arrivo del portale dati, completa i seguenti passaggi:

1. Accedi al portale DataZone dati di Amazon utilizzando l'URL del portale dati e accedi utilizzando il tuo SSO o AWS le tue credenziali. Se sei un DataZone amministratore Amazon, puoi ottenere l'URL del portale dati accedendo alla DataZone console Amazon all'indirizzo https://console.aws.amazon.com/datazone nell' AWS account in cui è stato creato il dominio DataZone radice Amazon.
2. Nel portale dati, per visualizzare il popup relativo alla serie recente di eventi, seleziona l'icona a forma di campana accanto alla barra di ricerca.
3. Seleziona Visualizza tutto per visualizzare tutti gli eventi. È possibile modificare le visualizzazioni e visualizzare tutte le attività selezionando la scheda Attività.
4. Filtra la ricerca per oggetto dell'evento o intervallo di date.
5. Scegli un singolo evento per accedere al luogo in cui puoi visualizzare i dettagli su quell'evento.

Lavorare con gli eventi tramite il bus EventBridge predefinito di Amazon

Oltre a inviare messaggi alla tua casella di posta dedicata nel portale dati, invia DataZone anche questi messaggi al tuo bus eventi EventBridge predefinito di Amazon nello stesso AWS account in cui è ospitato il tuo dominio DataZone root Amazon. Ciò consente l'automazione basata sugli eventi, come l'adempimento degli abbonamenti o le integrazioni personalizzate con altri strumenti. Puoi creare regole che corrispondano EventBridge agli eventi Amazon in arrivo e inviarle alle EventBridge destinazioni Amazon per l'elaborazione. Una singola regola può inviare un evento a più destinazioni, che possono quindi essere eseguite in parallelo.

Ecco un esempio di evento:

```
{
  "version": "0",
  "id": "bd3d6239-2877-f464-0572-b1d76760e085",
  "detail-type": "Subscription Request Created",
  "source": "aws.datazone",
  "account": "111111111111",
  "time": "2023-11-13T17:57:00Z",
  "region": "us-east-1",
  "resources": [],
  "detail": {
    "version": "655",
```

```
    "metadata": {
      "domain": "dzd_bc8e1ez8r2a6xz",
      "user": "44f864b8-50a1-70cc-736f-c1f763934ab7",
      "id": "5jbc0lie0sr99j",
      "version": "1",
      "typeName": "SubscriptionRequestEntityType",
      "owningProjectId": "6oy92hwk937pgn",
      "awsAccountId": "111111111111",
      "clientToken": "e781b7b5-78c5-4608-961e-3792a6c3ff0d"
    },
    "data": {
      "autoApproved": true,
      "requesterId": "44f864b8-50a1-70cc-736f-c1f763934ab7",
      "status": "PENDING",
      "subscribedListings": [
        {
          "id": "ayzstznnx4dxyf",
          "ownerProjectId": "5a3se66qm88947",
          "version": "12"
        }
      ],
      "subscribedPrincipals": [
        {
          "id": "6oy92hwk937pgn",
          "type": "PROJECT"
        }
      ]
    }
  }
}
```

L'elenco completo dei tipi di dettagli supportati da Amazon DataZone include:

- Richiesta di abbonamento creata
- Richiesta di iscrizione accettata
- Richiesta di abbonamento rifiutata
- Richiesta di iscrizione eliminata
- Concessione di abbonamento richiesta
- Concessione di abbonamento completata
- Concessione dell'abbonamento non riuscita

- Richiesta di revoca della concessione dell'abbonamento
- Revoca della concessione dell'abbonamento completata
- Revoca della concessione dell'abbonamento non riuscita
- Risorsa aggiunta all'inventario
- Risorsa aggiunta al catalogo
- Schema degli asset modificato
- Modifica dello stato dell'origine dati
- Fonte di dati creata
- Fonte dati aggiornata
- Fonte dati Run Triggered
- Esecuzione dell'origine dati riuscita
- Esecuzione dell'origine dati non riuscita
- Creazione del dominio riuscita
- Creazione del dominio non riuscita
- Eliminazione del dominio riuscita
- Eliminazione del dominio non riuscita
- Distribuzione dell'ambiente iniziata
- Implementazione dell'ambiente completata
- Installazione dell'ambiente non riuscita
- Eliminazione dell'ambiente iniziata
- Eliminazione dell'ambiente completata
- Eliminazione dell'ambiente non riuscita
- Creazione del progetto riuscita
- Aggiunta di un membro del progetto avvenuta con successo
- Rimozione del membro del progetto avvenuta con successo
- Cambio di ruolo del membro del progetto riuscito
- Avvio del flusso di lavoro del cliente per l'implementazione dell'ambiente
- Generazione del nome aziendale riuscita
- Generazione del nome aziendale non riuscita

Per ulteriori informazioni, consulta Amazon EventBridge.

Sicurezza in Amazon DataZone

La sicurezza del cloud AWS è la massima priorità. In qualità di AWS cliente, puoi beneficiare di data center e architetture di rete progettati per soddisfare i requisiti delle organizzazioni più sensibili alla sicurezza.

La sicurezza è una responsabilità condivisa tra te e te. AWS Il modello di responsabilità condivisa descrive questo aspetto come sicurezza del cloud e sicurezza nel cloud:

- Sicurezza del cloud: AWS è responsabile della protezione dell'infrastruttura che gestisce AWS i servizi in Cloud AWS. AWS fornisce inoltre servizi che è possibile utilizzare in modo sicuro. I revisori esterni testano e verificano regolarmente l'efficacia della nostra sicurezza nell'ambito dei AWS Programmi di AWS conformità dei Programmi di conformità dei di . Per maggiori informazioni sui programmi di conformità applicabili ad Amazon DataZone, consulta AWS Services in Scope by Compliance Program AWS .
- Sicurezza nel cloud: la tua responsabilità è determinata dal AWS servizio che utilizzi. Sei anche responsabile di altri fattori, tra cui la riservatezza dei dati, i requisiti della tua azienda e le leggi e normative vigenti.

Questa documentazione ti aiuta a capire come applicare il modello di responsabilità condivisa quando usi Amazon DataZone. I seguenti argomenti mostrano come configurare Amazon per DataZone soddisfare i tuoi obiettivi di sicurezza e conformità. Scopri anche come utilizzare altri AWS servizi che ti aiutano a monitorare e proteggere le tue DataZone risorse Amazon.

Argomenti

Protezione dei dati in Amazon DataZone

Il modello di responsabilità AWS condivisa Modello di si applica alla protezione dei dati in Amazon DataZone. Come descritto in questo modello, AWS è responsabile della protezione dell'infrastruttura globale che gestisce tutti i Cloud AWS. L'utente è responsabile del controllo dei contenuti ospitati su questa infrastruttura. L'utente è inoltre responsabile della configurazione della protezione e delle attività di gestione per i Servizi AWS utilizzati. Per ulteriori informazioni sulla privacy dei dati, vedi le Domande frequenti sulla privacy dei dati. Per informazioni sulla protezione dei dati in Europa, consulta il post del blog relativo al Modello di responsabilità condivisa AWS e GDPR nel Blog sulla sicurezza AWS .

Ai fini della protezione dei dati, consigliamo di proteggere Account AWS le credenziali e configurare i singoli utenti con AWS IAM Identity Center or AWS Identity and Access Management (IAM). In tal modo, a ogni utente verranno assegnate solo le autorizzazioni necessarie per svolgere i suoi compiti. Ti suggeriamo, inoltre, di proteggere i dati nei seguenti modi:

- Utilizza l'autenticazione a più fattori (MFA) con ogni account.
- Usa SSL/TLS per comunicare con le risorse. AWS È richiesto TLS 1.2 ed è consigliato TLS 1.3.
- Configura l'API e la registrazione delle attività degli utenti con. AWS CloudTrail
- Utilizza soluzioni di AWS crittografia, insieme a tutti i controlli di sicurezza predefiniti all'interno Servizi AWS.
- Utilizza i servizi di sicurezza gestiti avanzati, come Amazon Macie, che aiutano a individuare e proteggere i dati sensibili archiviati in Amazon S3.
- Se hai bisogno di moduli crittografici convalidati FIPS 140-2 per l'accesso AWS tramite un'interfaccia a riga di comando o un'API, utilizza un endpoint FIPS. Per ulteriori informazioni sugli endpoint FIPS disponibili, consulta il Federal Information Processing Standard (FIPS) 140-2.

Ti consigliamo vivamente di non inserire mai informazioni riservate o sensibili, ad esempio gli indirizzi e-mail dei clienti, nei tag o nei campi di testo in formato libero, ad esempio nel campo Nome. Ciò include quando lavori con Amazon DataZone o altri utenti Servizi AWS utilizzando la console, l'API o AWS gli SDK. AWS CLI I dati inseriti nei tag o nei campi di testo in formato libero utilizzati per i nomi possono essere utilizzati per i la fatturazione o i log di diagnostica. Quando fornisci un URL a un server esterno, ti suggeriamo vivamente di non includere informazioni sulle credenziali nell'URL per convalidare la tua richiesta al server.

Crittografia dei dati

Quando concedi le autorizzazioni, sei tu a decidere chi ottiene quali autorizzazioni per quali risorse Amazon. DataZone Si possono abilitare le operazioni specifiche che desideri consentire su tali risorse. Pertanto è necessario concedere solo le autorizzazioni necessarie per eseguire un'attività. L'applicazione dell'accesso con privilegio minimo è fondamentale per ridurre i rischi di sicurezza e l'impatto risultante da errori o intenzioni dannose.

Crittografia a riposo

Amazon DataZone crittografa tutti i tuoi dati per impostazione predefinita con una AWS chiave Key Management Service (AWS KMS) che AWS possiede e gestisce per te. Puoi anche crittografare i dati archiviati nel DataZone catalogo Amazon utilizzando le chiavi gestite con AWS KMS.

Quando crei un dominio in Amazon DataZone, puoi fornire impostazioni di crittografia selezionando la casella di controllo accanto a Personalizza le impostazioni di crittografia (avanzate) in Crittografia dei dati e fornendo una chiave KMS.

Crittografia in transito

Amazon DataZone utilizza Transport Layer Security (TLS) e la crittografia lato client per la crittografia in transito. La comunicazione con Amazon DataZone avviene sempre tramite HTTPS, quindi i dati sono sempre crittografati in transito.

Riservatezza del traffico Internet

Per proteggere le connessioni tra gli account, Amazon DataZone utilizza i ruoli di servizio e i ruoli IAM per connettersi in modo sicuro agli account dei clienti ed eseguire operazioni per conto del cliente.

Argomenti

- Crittografia dei dati a riposo per Amazon DataZone
- Utilizzo degli endpoint VPC di interfaccia per Amazon DataZone

Crittografia dei dati a riposo per Amazon DataZone

La crittografia predefinita dei dati a riposo aiuta a ridurre il sovraccarico operativo e la complessità associati alla protezione dei dati sensibili. Allo stesso tempo, consente di creare applicazioni sicure che soddisfano i rigorosi requisiti normativi e di conformità alla crittografia.

Amazon DataZone utilizza chiavi AWS di proprietà predefinite per crittografare automaticamente i dati inattivi. Non puoi visualizzare, gestire o controllare l'uso delle chiavi di AWS proprietà. Per ulteriori informazioni, consulta chiavi AWS possedute.

Sebbene non sia possibile disabilitare questo livello di crittografia o selezionare un tipo di crittografia alternativo, puoi aggiungere un secondo livello di crittografia alle chiavi di crittografia di AWS proprietà esistenti scegliendo una chiave gestita dal cliente quando crei i tuoi domini Amazon. DataZone Amazon DataZone supporta l'uso di chiavi simmetriche gestite dal cliente che puoi creare, possedere e gestire per aggiungere un secondo livello di crittografia alla crittografia di AWS proprietà esistente. Poiché hai il pieno controllo di questo livello di crittografia, in esso puoi eseguire le seguenti attività:

- Stabilire e mantenere le politiche chiave
- Stabilisci e mantieni le politiche e le sovvenzioni IAM
- Abilita e disabilita le politiche chiave
- Ruota il materiale crittografico chiave
- Aggiunta di tag
- Crea alias chiave
- Pianifica l'eliminazione delle chiavi

Per ulteriori informazioni, consulta Customer managed keys.

> **Note**
>
> Amazon abilita DataZone automaticamente la crittografia a riposo utilizzando chiavi AWS di proprietà per proteggere gratuitamente i dati dei clienti.
> AWS Per l'utilizzo di chiavi gestite dal cliente si applicano le tariffe KMS. Per ulteriori informazioni sui prezzi, consulta la sezione Prezzi del servizio di gestione delle AWS chiavi.

In che modo Amazon DataZone utilizza le sovvenzioni in KMS AWS

Amazon DataZone richiede tre sovvenzioni per utilizzare la chiave gestita dai clienti. Quando crei un DataZone dominio Amazon crittografato con una chiave gestita dal cliente, Amazon DataZone crea sovvenzioni e sotto-sovvenzioni per tuo conto inviando CreateGrantrichieste a KMS. AWS Le sovvenzioni in AWS KMS vengono utilizzate per consentire ad Amazon di DataZone accedere a una

chiave KMS nel tuo account. Amazon DataZone crea le seguenti sovvenzioni per utilizzare la chiave gestita dai clienti per le seguenti operazioni interne:

Una concessione per la crittografia dei dati inattivi per le seguenti operazioni:

- Invia DescribeKeyrichieste a AWS KMS per verificare che l'ID della chiave KMS simmetrica gestita dal cliente inserito durante la creazione di una raccolta di DataZone domini Amazon sia valido.
- Invia GenerateDataKeyrequestsa AWS KMS per generare chiavi dati crittografate dalla chiave gestita dal cliente.
- Invia le richieste Decrypt a AWS KMS per decrittografare le chiavi dati crittografate in modo che possano essere utilizzate per crittografare i tuoi dati.
- RetireGrantper ritirare la concessione quando il dominio viene eliminato.

Due sovvenzioni per la ricerca e l'individuazione dei dati:

- Sovvenzione 2:
  - DescribeKey
  - GenerateDataKey
  - Crittografa, decrittografa, ReEncrypt
  - CreateGrantper creare borse di studio per bambini per i AWS servizi utilizzati internamente da. DataZone
  - RetireGrant
- Sovvenzione 3:
  - GenerateDataKey
  - Decrypt
  - RetireGrant

Puoi revocare l'accesso alla concessione o rimuovere l'accesso del servizio alla chiave gestita dal cliente in qualsiasi momento. In tal caso, Amazon DataZone non sarà in grado di accedere a nessuno dei dati crittografati dalla chiave gestita dal cliente, il che influirà sulle operazioni che dipendono da tali dati. Ad esempio, se tenti di ottenere dettagli sugli asset di dati a cui Amazon non DataZone può accedere, l'operazione restituirà un `AccessDeniedException` errore.

Creazione di una chiave gestita dal cliente

Puoi creare una chiave simmetrica gestita dal cliente utilizzando la console di AWS gestione o le API AWS KMS.

Per creare una chiave simmetrica gestita dal cliente, segui i passaggi per la creazione di una chiave gestita dal cliente simmetrica nella Key Management Service Developer Guide. AWS

Politica chiave: le politiche chiave controllano l'accesso alla chiave gestita dal cliente. Ogni chiave gestita dal cliente deve avere esattamente una policy della chiave, che contiene istruzioni che determinano chi può usare la chiave e come la possono usare. Quando crei la chiave gestita dal cliente, puoi specificare una policy della chiave. Per ulteriori informazioni, consulta Gestire l'accesso alle chiavi gestite dal cliente nella AWS Key Management Service Developer Guide.

Per utilizzare la chiave gestita dai clienti con le tue DataZone risorse Amazon, nella policy chiave devono essere consentite le seguenti operazioni API:

- kms: CreateGrant — aggiunge una concessione a una chiave gestita dal cliente. Concede l'accesso di controllo a una chiave KMS specificata, che consente l'accesso alle operazioni di concessione richieste da Amazon DataZone . Per ulteriori informazioni sull'utilizzo di Grants, consulta la AWS Key Management Service Developer Guide.
- kms: DescribeKey — fornisce i dettagli chiave gestiti dal cliente per consentire ad Amazon di DataZone convalidare la chiave.
- kms: GenerateDataKey — restituisce una chiave dati simmetrica unica da utilizzare al di fuori di KMS. AWS
- KMS:Decrypt — decrittografa il testo cifrato che è stato crittografato da una chiave KMS.

Di seguito sono riportati alcuni esempi di policy policy che puoi aggiungere per Amazon DataZone:

```
"Statement" : [
    {
      "Sid" : "Allow access to principals authorized to manage Amazon DataZone",
      "Effect" : "Allow",
      "Principal" : {
        "AWS" : "arn:aws:iam::<account_id>:root"
      },
      "Action" : [
        "kms:DescribeKey",
```

```
        "kms:CreateGrant",
        "kms:GenerateDataKey",
        "kms:Decrypt"
      ],
      "Resource" : "arn:aws:kms:region:<account_id>:key/key_ID",
    }
  ]
```

> **Note**
>
> La politica di negazione del KMS non viene applicata alle risorse a cui si accede tramite il portale DataZone dati di Amazon.

Per ulteriori informazioni sulla specificazione delle autorizzazioni in una policy, consulta la AWS Key Management Service Developer Guide.

Per ulteriori informazioni sulla risoluzione dei problemi di accesso tramite chiave, consulta la AWS Key Management Service Developer Guide.

Specificare una chiave gestita dal cliente per Amazon DataZone

Contesto DataZone di crittografia Amazon

Un contesto di crittografia è un set facoltativo di coppie chiave-valore che contengono ulteriori informazioni contestuali sui dati.

AWS KMS utilizza il contesto di crittografia come dati autenticati aggiuntivi per supportare la crittografia autenticata. Quando includi un contesto di crittografia in una richiesta di crittografia dei dati, AWS KMS associa il contesto di crittografia ai dati crittografati. Per decrittografare i dati, nella richiesta deve essere incluso lo stesso contesto di crittografia.

Amazon DataZone utilizza il seguente contesto di crittografia:

```
"encryptionContextSubset": {
    "aws:datazone:domainId": "{root-domain-uuid}"
}
```

Utilizzo del contesto di crittografia per il monitoraggio: quando utilizzi una chiave simmetrica gestita dal cliente per crittografare DataZone Amazon, puoi anche utilizzare il contesto di crittografia nei record e nei log di controllo per identificare come viene utilizzata la chiave gestita dal cliente. Il contesto di crittografia appare anche nei log generati da AWS CloudTrail o Amazon CloudWatch Logs.

Utilizzo del contesto di crittografia per controllare l'accesso alla chiave gestita dal cliente: puoi utilizzare il contesto di crittografia nelle politiche chiave e nelle politiche IAM come condizioni per controllare l'accesso alla tua chiave simmetrica gestita dal cliente. È possibile utilizzare i vincoli del contesto di crittografia in una concessione.

Amazon DataZone utilizza un vincolo di contesto di crittografia nelle concessioni per controllare l'accesso alla chiave gestita dal cliente nel tuo account o nella tua regione. Il vincolo della concessione richiede che le operazioni consentite dalla concessione utilizzino il contesto di crittografia specificato.

Di seguito sono riportati alcuni esempi di istruzioni delle policy delle chiavi per concedere l'accesso a una chiave gestita dal cliente per un contesto di crittografia specifico. Questa istruzione della policy impone come condizione che le concessioni abbiano un vincolo che specifica il contesto di crittografia.

```
{
    "Sid": "Enable DescribeKey",
    "Effect": "Allow",
    "Principal": {
        "AWS": "arn:aws:iam::111122223333:role/ExampleReadOnlyRole"
     },
     "Action": "kms:DescribeKey",
     "Resource": "*"
},{
    "Sid": "Enable Decrypt, GenerateDataKey",
     "Effect": "Allow",
     "Principal": {
        "AWS": "arn:aws:iam::111122223333:role/ExampleReadOnlyRole"
     },
     "Action": [
        "kms:Decrypt",
        "kms:GenerateDataKey"
     ],
     "Resource": "*",
```

```
     "Condition": {
        "StringEquals": {
            "kms:EncryptionContext:aws:datazone:domainId": "{root-domain-uuid}"
        }
    }
}
```

Monitoraggio delle chiavi di crittografia per Amazon DataZone

Quando utilizzi una chiave gestita dal cliente AWS KMS con le tue DataZone risorse Amazon, puoi utilizzarla AWS CloudTrailper tenere traccia delle richieste che Amazon DataZone invia a AWS KMS. Gli esempi seguenti sono AWS CloudTrail eventi per `CreateGrant` `GenerateDataKeyDecrypt`, e per `DescribeKey` monitorare le operazioni KMS chiamate da Amazon DataZone per accedere ai dati crittografati dalla chiave gestita dal cliente. Quando utilizzi una chiave gestita dal cliente AWS KMS per crittografare il tuo DataZone dominio Amazon, Amazon DataZone invia una `CreateGrant` richiesta per tuo conto per accedere alla chiave KMS nel tuo account. AWS Le sovvenzioni DataZone create da Amazon sono specifiche per la risorsa associata alla chiave gestita dai clienti AWS KMS. Inoltre, Amazon DataZone utilizza l'`RetireGrant`operazione per rimuovere una concessione quando elimini un dominio. L'evento di esempio seguente registra l'operazione `CreateGrant`:

```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "AssumedRole",
        "principalId": "AROAIGDTESTANDEXAMPLE:Sampleuser01",
        "arn": "arn:aws:sts::111122223333:assumed-role/Admin/Sampleuser01",
        "accountId": "111122223333",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE3",
        "sessionContext": {
            "sessionIssuer": {
                "type": "Role",
                "principalId": "AROAIGDTESTANDEXAMPLE:Sampleuser01",
                "arn": "arn:aws:sts::111122223333:assumed-role/Admin/Sampleuser01",
                "accountId": "111122223333",
                "userName": "Admin"
            },
            "webIdFederationData": {},
            "attributes": {
                "mfaAuthenticated": "false",
```

```
                "creationDate": "2021-04-22T17:02:00Z"
            }
        },
        "invokedBy": "datazone.amazonaws.com"
    },
    "eventTime": "2021-04-22T17:07:02Z",
    "eventSource": "kms.amazonaws.com",
    "eventName": "CreateGrant",
    "awsRegion": "us-west-2",
    "sourceIPAddress": "172.12.34.56",
    "userAgent": "ExampleDesktop/1.0 (V1; OS)",
    "requestParameters": {
        "constraints": {
            "encryptionContextSubset": {
                "aws:datazone:domainId": "SAMPLE-root-domain-uuid"
            }
        },
        "keyId": "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-123456SAMPLE",
        "operations": [
            "Decrypt",
            "GenerateDataKey",
            "RetireGrant",
            "DescribeKey"
        ],
        "granteePrincipal": "datazone.us-west-2.amazonaws.com"
    },
    "responseElements": {
        "grantId":
 "0ab0ac0d0b000f00ea00cc0a0e00fc00bce000c000f0000000c0bc0a0000aaafSAMPLE",
        "keyId": "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-123456SAMPLE"
    },
    "requestID": "ff000af-00eb-00ce-0e00-ea000fb0fba0SAMPLE",
    "eventID": "ff000af-00eb-00ce-0e00-ea000fb0fba0SAMPLE",
    "readOnly": false,
    "resources": [
        {
            "accountId": "111122223333",
            "type": "AWS::KMS::Key",
            "ARN": "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-123456SAMPLE"
        }
    ],
```

```
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "eventCategory": "Management",
    "recipientAccountId": "111122223333"
}
```

Creazione di ambienti Data Lake che coinvolgono cataloghi AWS Glue crittografati

Nei casi d'uso avanzati, quando lavori con un catalogo AWS Glue crittografato, devi concedere l'accesso al DataZone servizio Amazon per utilizzare la tua chiave KMS gestita dal cliente. Puoi farlo aggiornando la tua politica KMS personalizzata e aggiungendo un tag alla chiave. Per concedere l'accesso al DataZone servizio Amazon per lavorare con i dati in un catalogo AWS Glue crittografato, completa quanto segue:

- Aggiungi la seguente politica alla tua chiave KMS personalizzata. Per ulteriori informazioni, vedere Modifica di una policy delle chiavi.

```
{
  "Sid": "Allow datazone environment roles to use the key",
  "Effect": "Allow",
  "Principal": {
    "AWS": "*"
  },
  "Action": [
    "kms:Decrypt",
    "kms:Describe*",
    "kms:Get*"
  ],
  "Resource": "*",
  "Condition": {
    "StringLike": {
      "aws:PrincipalArn": "arn:aws:iam::*:role/*datazone_usr*"
    }
  }
}
```

- Aggiungi il seguente tag alla tua chiave KMS personalizzata. Per ulteriori informazioni, consulta Usare i tag per controllare l'accesso alle chiavi KMS.

```
key: AmazonDataZoneEnvironment
value: all
```

Utilizzo degli endpoint VPC di interfaccia per Amazon DataZone

Se utilizzi Amazon Virtual Private Cloud (Amazon VPC) per ospitare AWS le tue risorse, puoi stabilire una connessione tra Amazon VPC e Amazon. DataZone Puoi utilizzare questa connessione con Amazon DataZone senza dover accedere alla rete Internet pubblica.

Amazon VPC ti consente di avviare AWS risorse in una rete virtuale personalizzata. Puoi utilizzare un VPC per controllare le impostazioni di rete, come l'intervallo di indirizzi IP, le sottoreti, le tabelle di routing e i gateway di rete. Per ulteriori informazioni sui VPC, consulta la Guida per l'utente di Amazon VPC.

Per connettere il tuo Amazon VPC ad Amazon DataZone, devi prima definire un endpoint VPC di interfaccia, che ti permetta di connettere il tuo VPC ad altri servizi. AWS L'endpoint offre una connettività scalabile e affidabile senza necessità di disporre di un gateway Internet, un'istanza NAT (Network Address Translation) o una connessione VPN. Per ulteriori informazioni e passaggi dettagliati su come creare un endpoint VPC, consulta Interface VPC Endpoints () nella Amazon VPC User AWS PrivateLink Guide.

> **Important**
>
> In VPC, una policy degli endpoint è una policy basata sulle risorse che puoi collegare a un endpoint VPC per controllare quali AWS principali principali possono utilizzare l'endpoint per accedere a un servizio. AWS
> Nell'attuale versione di Amazon DataZone, l'uso delle policy degli endpoint non è supportato per stabilire e utilizzare connessioni tra Amazon VPC e Amazon. DataZone La gestione degli DataZone accessi di Amazon si basa sulla configurazione della RAM e sulle principali policy IAM definite a livello di servizio.

Autorizzazione in Amazon DataZone

L'interfaccia DataZone di Amazon è costituita da una console di gestione interna AWS e da un'applicazione Web esterna alla console (portale dati).

La console di DataZone gestione Amazon può essere utilizzata dagli AWS amministratori per le top-level-resource API, inclusa la creazione e la gestione di domini, le associazioni di AWS account per questi domini e le fonti di dati per le quali desideri delegare la gestione degli accessi ad Amazon. DataZone Puoi utilizzare la console di DataZone gestione Amazon per gestire tutti i ruoli e la configurazione IAM necessari per delegare il controllo della gestione degli accessi al DataZone servizio Amazon per i relativi account configurati AWS in modo esplicito. Il portale DataZone dati Amazon è un'applicazione AWS Identity Center di prima parte per utenti SSO. Se abilitata, la console può essere utilizzata anche dai responsabili IAM autorizzati per la federazione nel portale dati anziché utilizzare un'identità SSO.

Il portale dati DataZone di Amazon è progettato per essere utilizzato principalmente dagli utenti autenticati da AWS IAM Identity Center per gestire l'accesso ai dati ed eseguire attività di pubblicazione, scoperta, sottoscrizione e analisi dei dati.

Autorizzazione nella DataZone console Amazon

Il modello di autorizzazione DataZone della console Amazon utilizza l'autorizzazione IAM. La console viene utilizzata dagli amministratori principalmente per la configurazione. Amazon DataZone utilizza il concetto di AWS account amministratore di dominio e AWS account membro e la console viene utilizzata da tutti questi account per creare relazioni di fiducia rispettando i confini AWS dell'organizzazione.

Autorizzazione nel DataZone portale Amazon

Il modello di autorizzazione del portale DataZone dati di Amazon è un ACL gerarchico con archetipi di ruolo statici (profili) che includono amministratori e visualizzatori. Ad esempio, gli utenti possono avere un profilo di amministratore o utente. A livello di dominio, possono avere come utente del dominio la designazione di proprietario dei dati. A livello di progetto, un utente può essere proprietario o collaboratore. Questi profili possono essere configurati in due tipi: utenti e gruppi. Questi profili vengono quindi associati a domini e progetti e lo stato di queste autorizzazioni viene memorizzato in una tabella di associazione.

All'interno di questo modello di autorizzazione, Amazon DataZone consente agli utenti di gestire le autorizzazioni di utenti e gruppi. Gli utenti gestiscono l'iscrizione ai progetti, richiedono

l'iscrizione ai progetti e approvano le iscrizioni. Gli utenti pubblicano dati, definiscono i responsabili dell'approvazione delle sottoscrizioni ai dati, si iscrivono ai dati e approvano le sottoscrizioni.

Gli utenti eseguono analisi dei dati in progetti specifici quando il loro client del portale dati richiede le credenziali di sessione IAM che Amazon DataZone genera in base al profilo effettivo dell'utente nel contesto specifico del progetto. Questa sessione riguarda sia le autorizzazioni dell'utente che le risorse specifiche del progetto. Gli utenti accedono quindi ad Athena o Redshift per interrogare i dati pertinenti e tutto il lavoro IAM sottostante viene completamente astratto.

DataZone Profili e ruoli Amazon

Una volta che un utente è autenticato, il contesto autenticato viene mappato a un ID del profilo utente. Questo profilo utente può avere più associazioni diverse (proprietario del progetto, amministratore di dominio, ecc.) che vengono utilizzate per autorizzare gli utenti. Ogni associazione (ad esempio, proprietario del progetto, amministratore di dominio, ecc.) dispone delle autorizzazioni per determinate attività in base al contesto. Ad esempio, un utente che dispone di un'associazione di amministratori di dominio può creare domini aggiuntivi, assegnare altri amministratori di dominio al dominio e creare modelli di progetto all'interno del proprio dominio. Il proprietario di un progetto può aggiungere o rimuovere membri del progetto, può creare accordi di pubblicazione con un dominio e pubblicare risorse in un dominio.

Controllo dell'accesso alle DataZone risorse Amazon tramite IAM

È necessario AWS Identity and Access Management (IAM) per completare le seguenti attività relative alla sicurezza:

- Crea utenti e gruppi con il tuo. Account AWS
- Assegna credenziali di sicurezza uniche a ciascun utente del tuo. Account AWS
- Controlla le autorizzazioni di ogni utente per eseguire attività con le risorse. AWS
- Consenti agli utenti di un altro utente Account AWS di condividere AWS le tue risorse.
- Crea ruoli per te Account AWS e definisci gli utenti o i servizi che possono assumerli.
- Utilizza le identità esistenti per la tua azienda per concedere le autorizzazioni per eseguire attività utilizzando le risorse AWS

Per ulteriori informazioni su IAM, consulta:

- AWS Identity and Access Management (IAM)

- Nozioni di base
- Guida per l'utente di IAM

Le seguenti sezioni descrivono le politiche e le autorizzazioni necessarie per configurare Amazon DataZone e i suoi componenti, come i domini (incluso il dominio), gli account associati, i progetti e le fonti di dati. Per ulteriori informazioni, consulta DataZone Terminologia e concetti di Amazon.

Indice

AWS politiche gestite per Amazon DataZone

Una politica AWS gestita è una politica autonoma creata e amministrata da AWS. AWS le politiche gestite sono progettate per fornire autorizzazioni per molti casi d'uso comuni, in modo da poter iniziare ad assegnare autorizzazioni a utenti, gruppi e ruoli.

Tieni presente che le policy AWS gestite potrebbero non concedere le autorizzazioni con il privilegio minimo per i tuoi casi d'uso specifici, poiché sono disponibili per tutti i clienti. AWS Consigliamo pertanto di ridurre ulteriormente le autorizzazioni definendo policy gestite dal cliente specifiche per i tuoi casi d'uso.

Non è possibile modificare le autorizzazioni definite nelle politiche gestite. AWS Se AWS aggiorna le autorizzazioni definite in una politica AWS gestita, l'aggiornamento ha effetto su tutte le identità principali (utenti, gruppi e ruoli) a cui è associata la politica. AWS è più probabile che aggiorni una policy AWS gestita quando ne Servizio AWS viene lanciata una nuova o quando diventano disponibili nuove operazioni API per i servizi esistenti.

Per ulteriori informazioni, consultare Policy gestite da AWSnella Guida per l'utente di IAM.

Indice

- AWS politica gestita: AmazonDataZoneCustomEnvironmentDeploymentPolicy
- AWS politica gestita: AmazonDataZoneEnvironmentRolePermissionsBoundary
- AWS politica gestita: AmazonDataZoneRedshiftGlueProvisioningPolicy
- AWS politica gestita: AmazonDataZoneGlueManageAccessRolePolicy
- AWS politica gestita: AmazonDataZoneRedshiftManageAccessRolePolicy
- AWS Policy gestita: AmazonDataZoneCrossAccountAdmin
- AWS politica gestita: AmazonDataZoneDomainExecutionRolePolicy
- AWS politica gestita: AmazonDataZoneSageMakerProvisioning
- AWS politica gestita: AmazonDataZoneSageMakerAccess
- AWS politica gestita: AmazonDataZoneSageMakerEnvironmentRolePermissionsBoundary
- DataZone Aggiornamenti Amazon alle politiche AWS gestite

AWS politica gestita: AmazonDataZoneFullAccess

È possibile allegare la policy `AmazonDataZoneFullAccess`alle identità IAM.

Questa politica fornisce l'accesso completo ad Amazon DataZone tramite AWS Management Console.

Dettagli dell'autorizzazione

Questa policy include le seguenti autorizzazioni:

- `datazone`— garantisce ai mandanti l'accesso completo ad Amazon DataZone tramite. AWS Management Console
- `kms`— Consente ai mandanti di elencare gli alias e descrivere le chiavi.
- `s3`— Consente ai responsabili di scegliere i bucket S3 esistenti o di creare nuovi per archiviare i dati Amazon. DataZone
- `ram`— Consente ai mandanti di condividere i DataZone domini Amazon tra. Account AWS
- `iam`— Consente ai dirigenti di elencare e assegnare ruoli e ottenere politiche.
- `sso`— Consente ai responsabili di ottenere le regioni in cui AWS IAM Identity Center è abilitato.

```
{
  "Version": "2012-10-17",
```

```
  "Statement": [
    {
      "Sid": "AmazonDataZoneStatement",
      "Effect": "Allow",
      "Action": [
        "datazone:*"
      ],
      "Resource": [
        "*"
      ]
    },
    {
      "Sid": "ReadOnlyStatement",
      "Effect": "Allow",
      "Action": [
        "kms:DescribeKey",
        "kms:ListAliases",
        "iam:ListRoles",
        "sso:DescribeRegisteredRegions",
        "s3:ListAllMyBuckets",
        "redshift:DescribeClusters",
        "redshift-serverless:ListWorkgroups",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "secretsmanager:ListSecrets"
      ],
      "Resource": [
        "*"
      ]
    },
    {
      "Sid": "BucketReadOnlyStatement",
      "Effect": "Allow",
      "Action": [
        "s3:ListBucket",
        "s3:GetBucketLocation"
      ],
      "Resource": "arn:aws:s3:::*"
    },
    {
      "Sid": "CreateBucketStatement",
      "Effect": "Allow",
      "Action": "s3:CreateBucket",
```

```
      "Resource": "arn:aws:s3:::amazon-datazone*"
    },
    {
      "Sid": "RamCreateResourceStatement",
      "Effect": "Allow",
      "Action": [
        "ram:CreateResourceShare"
      ],
      "Resource": "*",
      "Condition": {
        "StringEqualsIfExists": {
          "ram:RequestedResourceType": "datazone:Domain"
        }
      }
    },
    {
      "Sid": "RamResourceStatement",
      "Effect": "Allow",
      "Action": [
        "ram:DeleteResourceShare",
        "ram:AssociateResourceShare",
        "ram:DisassociateResourceShare",
        "ram:RejectResourceShareInvitation"
      ],
      "Resource": "*",
      "Condition": {
        "StringLike": {
          "ram:ResourceShareName": [
            "DataZone*"
          ]
        }
      }
    },
    {
      "Sid": "RamResourceReadOnlyStatement",
      "Effect": "Allow",
      "Action": [
        "ram:GetResourceShares",
        "ram:GetResourceShareInvitations",
        "ram:GetResourceShareAssociations"
      ],
      "Resource": "*"
    },
    {
```

```
      "Sid": "IAMPassRoleStatement",
      "Effect": "Allow",
      "Action": "iam:PassRole",
      "Resource": [
        "arn:aws:iam::*:role/AmazonDataZone*",
        "arn:aws:iam::*:role/service-role/AmazonDataZone*"
      ],
      "Condition": {
        "StringEquals": {
          "iam:passedToService": "datazone.amazonaws.com"
        }
      }
    },
    {
      "Sid": "IAMGetPolicyStatement",
      "Effect": "Allow",
      "Action": "iam:GetPolicy",
      "Resource": [
        "arn:aws:iam::*:policy/service-role/AmazonDataZoneRedshiftAccessPolicy*"
      ]
    },
    {
      "Sid": "DataZoneTagOnCreate",
      "Effect": "Allow",
      "Action": [
        "secretsmanager:TagResource"
      ],
      "Resource": "arn:aws:secretsmanager:*:*:secret:AmazonDataZone-*",
      "Condition": {
        "ForAllValues:StringEquals": {
          "aws:TagKeys": [
            "AmazonDataZoneDomain"
          ]
        },
        "StringLike": {
          "aws:RequestTag/AmazonDataZoneDomain": "dzd_*",
          "aws:ResourceTag/AmazonDataZoneDomain": "dzd_*"
        },
        "Null": {
          "aws:TagKeys": "false"
        }
      }
    },
    {
```

```
      "Sid": "CreateSecretStatement",
      "Effect": "Allow",
      "Action": [
        "secretsmanager:CreateSecret"
      ],
      "Resource": "arn:aws:secretsmanager:*:*:secret:AmazonDataZone-*",
      "Condition": {
        "StringLike": {
          "aws:RequestTag/AmazonDataZoneDomain": "dzd_*"
        }
      }
    }
  ]
}
```

Considerazioni e limitazioni relative alle politiche

Ci sono alcune funzionalità che la `AmazonDataZoneFullAccess` politica non copre.

- Se crei un DataZone dominio Amazon con la tua AWS KMS chiave, devi disporre delle autorizzazioni necessarie `kms:CreateGrant` affinché la creazione del dominio abbia successo e`kms:GenerateDataKey`, `kms:Decrypt` affinché quella chiave possa richiamare altre DataZone API Amazon come e. `listDataSources` `createDataSource` Inoltre, devi disporre delle autorizzazioni per`kms:CreateGrant`, `kms:Decrypt``kms:GenerateDataKey`, e `kms:DescribeKey` nella politica delle risorse di quella chiave.

  Se utilizzi la chiave KMS predefinita di proprietà del servizio, questa non è necessaria.

  Per ulteriori informazioni, consulta AWS Key Management Service.
- Se desideri utilizzare le funzionalità di creazione e aggiornamento dei ruoli all'interno della DataZone console Amazon, devi disporre dei privilegi di amministratore o disporre delle autorizzazioni IAM necessarie per creare ruoli IAM e creare/aggiornare le politiche. Le autorizzazioni richieste includono`iam:CreateRole`,, e autorizzazioni. `iam:CreatePolicy` `iam:CreatePolicyVersion` `iam:DeletePolicyVersion` `iam:AttachRolePolicy`
- Se crei un nuovo dominio in Amazon DataZone con l'accesso AWS IAM Identity Center degli utenti attivato o se lo attivi per un dominio esistente in Amazon DataZone, devi disporre delle autorizzazioni per quanto segue:`sso:CreateManagedApplicationInstance`,`sso:DeleteManagedApplicationInstance`, `esso:PutApplicationAssignmentConfiguration`.

- Per accettare una richiesta di associazione di AWS account su Amazon DataZone, devi disporre dell'`ram:AcceptResourceShareInvitation`autorizzazione.

AWS politica gestita: AmazonDataZoneFullUserAccess

Questa politica garantisce l'accesso completo ad Amazon DataZone, ma non consente la gestione di domini, utenti o account associati.

Dettagli dell'autorizzazione

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AmazonDataZoneUserOperations",
      "Effect": "Allow",
      "Action": [
        "datazone:GetDomain",
        "datazone:CreateFormType",
        "datazone:GetFormType",
        "datazone:GetIamPortalLoginUrl",
        "datazone:SearchUserProfiles",
        "datazone:SearchGroupProfiles",
        "datazone:GetUserProfile",
        "datazone:GetGroupProfile",
        "datazone:ListGroupsForUser",
        "datazone:DeleteFormType",
        "datazone:CreateAssetType",
        "datazone:GetAssetType",
        "datazone:DeleteAssetType",
        "datazone:CreateGlossary",
        "datazone:GetGlossary",
        "datazone:DeleteGlossary",
        "datazone:UpdateGlossary",
        "datazone:CreateGlossaryTerm",
        "datazone:GetGlossaryTerm",
        "datazone:DeleteGlossaryTerm",
        "datazone:UpdateGlossaryTerm",
        "datazone:CreateAsset",
        "datazone:GetAsset",
        "datazone:DeleteAsset",
```

```
        "datazone:CreateAssetRevision",
        "datazone:ListAssetRevisions",
        "datazone:AcceptPredictions",
        "datazone:RejectPredictions",
        "datazone:Search",
        "datazone:SearchTypes",
        "datazone:CreateListingChangeSet",
        "datazone:DeleteListing",
        "datazone:SearchListings",
        "datazone:GetListing",
        "datazone:CreateDataSource",
        "datazone:GetDataSource",
        "datazone:DeleteDataSource",
        "datazone:UpdateDataSource",
        "datazone:ListDataSources",
        "datazone:StartDataSourceRun",
        "datazone:GetDataSourceRun",
        "datazone:ListDataSourceRuns",
        "datazone:ListDataSourceRunActivities",
        "datazone:ListEnvironmentBlueprintConfigurations",
        "datazone:CreateEnvironmentBlueprint",
        "datazone:GetEnvironmentBlueprint",
        "datazone:DeleteEnvironmentBlueprint",
        "datazone:UpdateEnvironmentBlueprint",
        "datazone:ListEnvironmentBlueprints",
        "datazone:CreateProject",
        "datazone:UpdateProject",
        "datazone:GetProject",
        "datazone:DeleteProject",
        "datazone:ListProjects",
        "datazone:CreateProjectMembership",
        "datazone:DeleteProjectMembership",
        "datazone:ListProjectMemberships",
        "datazone:CreateEnvironmentProfile",
        "datazone:GetEnvironmentProfile",
        "datazone:UpdateEnvironmentProfile",
        "datazone:DeleteEnvironmentProfile",
        "datazone:ListEnvironmentProfiles",
        "datazone:CreateEnvironment",
        "datazone:GetEnvironment",
        "datazone:DeleteEnvironment",
        "datazone:UpdateEnvironment",
        "datazone:UpdateEnvironmentDeploymentStatus",
        "datazone:ListEnvironments",
```

```
        "datazone:ListAccountEnvironments",
        "datazone:GetEnvironmentActionLink",
        "datazone:GetEnvironmentCredentials",
        "datazone:GetSubscriptionTarget",
        "datazone:DeleteSubscriptionTarget",
        "datazone:ListSubscriptionTargets",
        "datazone:CreateSubscriptionRequest",
        "datazone:AcceptSubscriptionRequest",
        "datazone:UpdateSubscriptionRequest",
        "datazone:ListWarehouseMetadata",
        "datazone:RejectSubscriptionRequest",
        "datazone:GetSubscriptionRequestDetails",
        "datazone:ListSubscriptionRequests",
        "datazone:DeleteSubscriptionRequest",
        "datazone:GetSubscription",
        "datazone:CancelSubscription",
        "datazone:GetSubscriptionEligibility",
        "datazone:ListSubscriptions",
        "datazone:RevokeSubscription",
        "datazone:CreateSubscriptionGrant",
        "datazone:DeleteSubscriptionGrant",
        "datazone:GetSubscriptionGrant",
        "datazone:ListSubscriptionGrants",
        "datazone:UpdateSubscriptionGrantStatus",
        "datazone:ListNotifications",
        "datazone:StartMetadataGenerationRun",
        "datazone:GetMetadataGenerationRun",
        "datazone:CancelMetadataGenerationRun",
        "datazone:ListMetadataGenerationRuns"
      ],
      "Resource": "*"
    },
    {
      "Sid": "RAMResourceShareOperations",
      "Effect": "Allow",
      "Action": "ram:GetResourceShareAssociations",
      "Resource": "*"
    }
  ]
}
```

AWS politica gestita: AmazonDataZoneCustomEnvironmentDeploymentPolicy

È possibile utilizzare questa politica per aggiornare la configurazione degli ambienti creati utilizzando blueprint personalizzati. Questa politica può essere utilizzata anche per creare obiettivi di DataZone abbonamento Amazon e fonti di dati.

Dettagli dell'autorizzazione

```
{
 "Version": "2012-10-17",
 "Statement": [
  {
   "Sid": "AmazonDataZoneCustomEnvironment",
   "Effect": "Allow",
   "Action": [
    "datazone:ListAssociatedAccounts",
    "datazone:GetAccountAssociation",
    "datazone:GetEnvironment",
    "datazone:GetEnvironmentProfile",
    "datazone:GetEnvironmentBlueprint",
    "datazone:GetProject",
    "datazone:UpdateEnvironmentConfiguration",
    "datazone:UpdateEnvironmentDeploymentStatus",
    "datazone:CreateSubscriptionTarget",
    "datazone:CreateDataSource"
   ],
   "Resource": "*"
  }
 ]
}
```

AWS politica gestita: AmazonDataZoneEnvironmentRolePermissionsBoundary

> **Note**
>
> Questa politica è un limite di autorizzazioni. Un limite di autorizzazioni imposta le autorizzazioni massime che una policy basata sull'identità può concedere a un'entità IAM. Non devi utilizzare e allegare autonomamente le politiche limite DataZone relative alle autorizzazioni di Amazon. Le politiche sui limiti DataZone delle autorizzazioni di Amazon devono essere allegate solo ai ruoli DataZone gestiti da Amazon. Per ulteriori informazioni sui

limiti delle autorizzazioni, consulta Limiti delle autorizzazioni per le entità IAM nella Guida per l'utente IAM.

Quando crei un ambiente tramite il portale DataZone dati Amazon, Amazon DataZone applica questo limite di autorizzazioni ai ruoli IAM prodotti durante la creazione dell'ambiente. Il limite delle autorizzazioni limita l'ambito dei ruoli DataZone creati da Amazon e degli eventuali ruoli aggiunti.

Amazon DataZone utilizza la policy `AmazonDataZoneEnvironmentRolePermissionsBoundary` gestita per limitare il principale IAM fornito a cui è collegata. I responsabili potrebbero assumere la forma dei ruoli utente che Amazon DataZone può assumere per conto di utenti aziendali interattivi o di servizi di analisi (ad esempio)AWS Glue, e quindi condurre azioni per elaborare dati come la lettura e la scrittura da Amazon S3 o l'esecuzione. Crawler di AWS Glue

La `AmazonDataZoneEnvironmentRolePermissionsBoundary` policy concede l'accesso in lettura e scrittura per Amazon DataZone a servizi come Amazon S3 AWS Glue AWS Lake Formation, Amazon Redshift e Amazon Athena. La policy fornisce inoltre autorizzazioni di lettura e scrittura ad alcune risorse dell'infrastruttura necessarie per utilizzare questi servizi, come interfacce e chiavi di rete. AWS KMS

Amazon DataZone applica la policy `AmazonDataZoneEnvironmentRolePermissionsBoundary` AWS gestita come limite di autorizzazioni per tutti i ruoli DataZone dell'ambiente Amazon (proprietario e collaboratore). Questo limite di autorizzazioni limita questi ruoli per consentire l'accesso solo alle risorse e alle azioni richieste necessarie per un ambiente.

Il limite include le seguenti istruzioni JSON:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "CreateGlueConnection",
      "Effect": "Allow",
      "Action": [
        "ec2:CreateTags",
        "ec2:DeleteTags"
      ],
      "Resource": [
        "arn:aws:ec2:*:*:network-interface/*"
      ],
```

```
      "Condition": {
        "ForAllValues:StringEquals": {
          "aws:TagKeys": [
            "aws-glue-service-resource"
          ]
        }
      }
    },
    {
      "Sid": "GlueOperations",
      "Effect": "Allow",
      "Action": [
        "glue:*DataQuality*",
        "glue:BatchCreatePartition",
        "glue:BatchDeleteConnection",
        "glue:BatchDeletePartition",
        "glue:BatchDeleteTable",
        "glue:BatchDeleteTableVersion",
        "glue:BatchGetJobs",
        "glue:BatchGetWorkflows",
        "glue:BatchStopJobRun",
        "glue:BatchUpdatePartition",
        "glue:CreateBlueprint",
        "glue:CreateConnection",
        "glue:CreateCrawler",
        "glue:CreateDatabase",
        "glue:CreateJob",
        "glue:CreatePartition",
        "glue:CreatePartitionIndex",
        "glue:CreateTable",
        "glue:CreateWorkflow",
        "glue:DeleteBlueprint",
        "glue:DeleteColumnStatisticsForPartition",
        "glue:DeleteColumnStatisticsForTable",
        "glue:DeleteConnection",
        "glue:DeleteCrawler",
        "glue:DeleteJob",
        "glue:DeletePartition",
        "glue:DeletePartitionIndex",
        "glue:DeleteTable",
        "glue:DeleteTableVersion",
        "glue:DeleteWorkflow",
        "glue:GetColumnStatisticsForPartition",
        "glue:GetColumnStatisticsForTable",
```

```
        "glue:GetConnection",
        "glue:GetDatabase",
        "glue:GetDatabases",
        "glue:GetTable",
        "glue:GetTables",
        "glue:GetPartition",
        "glue:GetPartitions",
        "glue:ListSchemas",
        "glue:ListJobs",
        "glue:NotifyEvent",
        "glue:PutWorkflowRunProperties",
        "glue:ResetJobBookmark",
        "glue:ResumeWorkflowRun",
        "glue:SearchTables",
        "glue:StartBlueprintRun",
        "glue:StartCrawler",
        "glue:StartCrawlerSchedule",
        "glue:StartJobRun",
        "glue:StartWorkflowRun",
        "glue:StopCrawler",
        "glue:StopCrawlerSchedule",
        "glue:StopWorkflowRun",
        "glue:UpdateBlueprint",
        "glue:UpdateColumnStatisticsForPartition",
        "glue:UpdateColumnStatisticsForTable",
        "glue:UpdateConnection",
        "glue:UpdateCrawler",
        "glue:UpdateCrawlerSchedule",
        "glue:UpdateDatabase",
        "glue:UpdateJob",
        "glue:UpdatePartition",
        "glue:UpdateTable",
        "glue:UpdateWorkflow"
      ],
      "Resource": "*",
      "Condition": {
        "Null": {
          "aws:ResourceTag/AmazonDataZoneEnvironment": "false"
        }
      }
    },
    {
      "Sid": "PassRole",
      "Effect": "Allow",
```

```
      "Action": [
        "iam:PassRole"
      ],
      "Resource": [
        "arn:aws:iam::*:role/datazone*"
      ],
      "Condition": {
        "StringEquals": {
          "iam:PassedToService": "glue.amazonaws.com"
        }
      }
    },
    {
      "Sid": "SameAccountKmsOperations",
      "Effect": "Allow",
      "Action": [
        "kms:DescribeKey",
        "kms:Decrypt",
        "kms:ListKeys"
      ],
      "Resource": "*",
      "Condition": {
        "StringNotEquals": {
          "aws:ResourceAccount": "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid": "KmsOperationsWithResourceTag",
      "Effect": "Allow",
      "Action": [
        "kms:DescribeKey",
        "kms:Decrypt",
        "kms:ListKeys",
        "kms:Encrypt",
        "kms:GenerateDataKey",
        "kms:Verify",
        "kms:Sign"
      ],
      "Resource": "*",
      "Condition": {
        "Null": {
          "aws:ResourceTag/AmazonDataZoneEnvironment": "false"
        }
```

```
      }
    },
    {
      "Sid": "AnalyticsOperations",
      "Effect": "Allow",
      "Action": [
        "datazone:*",
        "sqlworkbench:*"
      ],
      "Resource": "*"
    },
    {
      "Sid": "QueryOperations",
      "Effect": "Allow",
      "Action": [
        "athena:BatchGetNamedQuery",
        "athena:BatchGetPreparedStatement",
        "athena:BatchGetQueryExecution",
        "athena:CreateNamedQuery",
        "athena:CreateNotebook",
        "athena:CreatePreparedStatement",
        "athena:CreatePresignedNotebookUrl",
        "athena:DeleteNamedQuery",
        "athena:DeleteNotebook",
        "athena:DeletePreparedStatement",
        "athena:ExportNotebook",
        "athena:GetDatabase",
        "athena:GetDataCatalog",
        "athena:GetNamedQuery",
        "athena:GetPreparedStatement",
        "athena:GetQueryExecution",
        "athena:GetQueryResults",
        "athena:GetQueryRuntimeStatistics",
        "athena:GetTableMetadata",
        "athena:GetWorkGroup",
        "athena:ImportNotebook",
        "athena:ListDatabases",
        "athena:ListDataCatalogs",
        "athena:ListEngineVersions",
        "athena:ListNamedQueries",
        "athena:ListPreparedStatements",
        "athena:ListQueryExecutions",
        "athena:ListTableMetadata",
        "athena:ListTagsForResource",
```

```
        "athena:ListWorkGroups",
        "athena:StartCalculationExecution",
        "athena:StartQueryExecution",
        "athena:StartSession",
        "athena:StopCalculationExecution",
        "athena:StopQueryExecution",
        "athena:TerminateSession",
        "athena:UpdateNamedQuery",
        "athena:UpdateNotebook",
        "athena:UpdateNotebookMetadata",
        "athena:UpdatePreparedStatement",
        "ec2:CreateNetworkInterface",
        "ec2:DeleteNetworkInterface",
        "ec2:Describe*",
        "glue:BatchCreatePartition",
        "glue:BatchDeletePartition",
        "glue:BatchDeleteTable",
        "glue:BatchDeleteTableVersion",
        "glue:BatchGetJobs",
        "glue:BatchGetPartition",
        "glue:BatchGetWorkflows",
        "glue:BatchUpdatePartition",
        "glue:CreateBlueprint",
        "glue:CreateConnection",
        "glue:CreateCrawler",
        "glue:CreateDatabase",
        "glue:CreateJob",
        "glue:CreatePartition",
        "glue:CreatePartitionIndex",
        "glue:CreateTable",
        "glue:CreateWorkflow",
        "glue:DeleteColumnStatisticsForPartition",
        "glue:DeleteColumnStatisticsForTable",
        "glue:DeletePartition",
        "glue:DeletePartitionIndex",
        "glue:DeleteTable",
        "glue:DeleteTableVersion",
        "glue:GetColumnStatisticsForPartition",
        "glue:GetColumnStatisticsForTable",
        "glue:GetConnection",
        "glue:GetDatabase",
        "glue:GetDatabases",
        "glue:GetTable",
        "glue:GetTables",
```

```
        "glue:GetPartition",
        "glue:GetPartitions",
        "glue:ListSchemas",
        "glue:ListJobs",
        "glue:NotifyEvent",
        "glue:SearchTables",
        "glue:UpdateColumnStatisticsForPartition",
        "glue:UpdateColumnStatisticsForTable",
        "glue:UpdateDatabase",
        "glue:UpdatePartition",
        "glue:UpdateTable",
        "iam:GetRole",
        "iam:GetRolePolicy",
        "iam:ListGroups",
        "iam:ListRolePolicies",
        "iam:ListRoles",
        "iam:ListUsers",
        "logs:DescribeLogGroups",
        "logs:DescribeLogStreams",
        "logs:DescribeMetricFilters",
        "logs:DescribeQueries",
        "logs:DescribeQueryDefinitions",
        "logs:DescribeMetricFilters",
        "logs:StartQuery",
        "logs:StopQuery",
        "logs:GetLogEvents",
        "logs:GetLogGroupFields",
        "logs:GetQueryResults",
        "logs:GetLogRecord",
        "logs:PutLogEvents",
        "logs:CreateLogStream",
        "logs:FilterLogEvents",
        "lakeformation:GetDataAccess",
        "lakeformation:GetDataLakeSettings",
        "lakeformation:GetResourceLFTags",
        "lakeformation:ListPermissions",
        "redshift-data:ListTables",
        "redshift-data:DescribeTable",
        "redshift-data:ListSchemas",
        "redshift-data:ListDatabases",
        "redshift-data:ExecuteStatement",
        "redshift-data:GetStatementResult",
        "redshift-data:DescribeStatement",
        "redshift:CreateClusterUser",
```

```
        "redshift:DescribeClusters",
        "redshift:DescribeDataShares",
        "redshift:GetClusterCredentials",
        "redshift:GetClusterCredentialsWithIAM",
        "redshift:JoinGroup",
        "redshift-serverless:ListNamespaces",
        "redshift-serverless:ListWorkgroups",
        "redshift-serverless:GetNamespace",
        "redshift-serverless:GetWorkgroup",
        "redshift-serverless:GetCredentials",
        "secretsmanager:ListSecrets",
        "tag:GetResources"
      ],
      "Resource": "*"
    },
    {
      "Sid": "QueryOperationsWithResourceTag",
      "Effect": "Allow",
      "Action": [
        "athena:GetQueryResultsStream"
      ],
      "Resource": "*",
      "Condition": {
        "Null": {
          "aws:ResourceTag/AmazonDataZoneEnvironment": "false"
        }
      }
    },
    {
      "Sid": "SecretsManagerOperationsWithTagKeys",
      "Effect": "Allow",
      "Action": [
        "secretsmanager:CreateSecret",
        "secretsmanager:TagResource"
      ],
      "Resource": "arn:aws:secretsmanager:*:*:secret:AmazonDataZone-*",
      "Condition": {
        "StringLike": {
          "aws:ResourceTag/AmazonDataZoneDomain": "*",
          "aws:ResourceTag/AmazonDataZoneProject": "*"
        },
        "Null": {
          "aws:TagKeys": "false"
        },
```

```
        "ForAllValues:StringEquals": {
          "aws:TagKeys": [
            "AmazonDataZoneDomain",
            "AmazonDataZoneProject"
          ]
        }
      }
    },
    {
      "Sid": "DataZoneS3Buckets",
      "Effect": "Allow",
      "Action": [
        "s3:AbortMultipartUpload",
        "s3:DeleteObject",
        "s3:DeleteObjectVersion",
        "s3:GetObject",
        "s3:PutObject",
        "s3:PutObjectRetention",
        "s3:ReplicateObject",
        "s3:RestoreObject"
      ],
      "Resource": [
        "arn:aws:s3:::*/datazone/*"
      ]
    },
    {
      "Sid": "DataZoneS3BucketLocation",
      "Effect": "Allow",
      "Action": [
        "s3:GetBucketLocation"
      ],
      "Resource": "*"
    },
    {
      "Sid": "ListDataZoneS3Bucket",
      "Effect": "Allow",
      "Action": [
        "s3:ListBucket"
      ],
      "Resource": [
        "*"
      ],
      "Condition": {
        "StringLike": {
```

```
          "s3:prefix": [
            "*/datazone/*",
            "datazone/*"
          ]
        }
      }
    },
    {
      "Sid": "NotDeniedOperations",
      "Effect": "Deny",
      "NotAction": [
        "datazone:*",
        "sqlworkbench:*",
        "athena:BatchGetNamedQuery",
        "athena:BatchGetPreparedStatement",
        "athena:BatchGetQueryExecution",
        "athena:CreateNamedQuery",
        "athena:CreateNotebook",
        "athena:CreatePreparedStatement",
        "athena:CreatePresignedNotebookUrl",
        "athena:DeleteNamedQuery",
        "athena:DeleteNotebook",
        "athena:DeletePreparedStatement",
        "athena:ExportNotebook",
        "athena:GetDatabase",
        "athena:GetDataCatalog",
        "athena:GetNamedQuery",
        "athena:GetPreparedStatement",
        "athena:GetQueryExecution",
        "athena:GetQueryResults",
        "athena:GetQueryResultsStream",
        "athena:GetQueryRuntimeStatistics",
        "athena:GetTableMetadata",
        "athena:GetWorkGroup",
        "athena:ImportNotebook",
        "athena:ListDatabases",
        "athena:ListDataCatalogs",
        "athena:ListEngineVersions",
        "athena:ListNamedQueries",
        "athena:ListPreparedStatements",
        "athena:ListQueryExecutions",
        "athena:ListTableMetadata",
        "athena:ListTagsForResource",
        "athena:ListWorkGroups",
```

```
        "athena:StartCalculationExecution",
        "athena:StartQueryExecution",
        "athena:StartSession",
        "athena:StopCalculationExecution",
        "athena:StopQueryExecution",
        "athena:TerminateSession",
        "athena:UpdateNamedQuery",
        "athena:UpdateNotebook",
        "athena:UpdateNotebookMetadata",
        "athena:UpdatePreparedStatement",
        "ec2:CreateNetworkInterface",
        "ec2:CreateTags",
        "ec2:DeleteNetworkInterface",
        "ec2:DeleteTags",
        "ec2:Describe*",
        "glue:*DataQuality*",
        "glue:BatchCreatePartition",
        "glue:BatchDeleteConnection",
        "glue:BatchDeletePartition",
        "glue:BatchDeleteTable",
        "glue:BatchDeleteTableVersion",
        "glue:BatchGetJobs",
        "glue:BatchGetPartition",
        "glue:BatchGetWorkflows",
        "glue:BatchStopJobRun",
        "glue:BatchUpdatePartition",
        "glue:CreateBlueprint",
        "glue:CreateConnection",
        "glue:CreateCrawler",
        "glue:CreateDatabase",
        "glue:CreateJob",
        "glue:CreatePartition",
        "glue:CreatePartitionIndex",
        "glue:CreateTable",
        "glue:CreateWorkflow",
        "glue:DeleteBlueprint",
        "glue:DeleteColumnStatisticsForPartition",
        "glue:DeleteColumnStatisticsForTable",
        "glue:DeleteConnection",
        "glue:DeleteCrawler",
        "glue:DeleteJob",
        "glue:DeletePartition",
        "glue:DeletePartitionIndex",
        "glue:DeleteTable",
```

```
        "glue:DeleteTableVersion",
        "glue:DeleteWorkflow",
        "glue:GetColumnStatisticsForPartition",
        "glue:GetColumnStatisticsForTable",
        "glue:GetConnection",
        "glue:GetDatabase",
        "glue:GetDatabases",
        "glue:GetTable",
        "glue:GetTables",
        "glue:GetPartition",
        "glue:GetPartitions",
        "glue:ListSchemas",
        "glue:ListJobs",
        "glue:NotifyEvent",
        "glue:PutWorkflowRunProperties",
        "glue:ResetJobBookmark",
        "glue:ResumeWorkflowRun",
        "glue:SearchTables",
        "glue:StartBlueprintRun",
        "glue:StartCrawler",
        "glue:StartCrawlerSchedule",
        "glue:StartJobRun",
        "glue:StartWorkflowRun",
        "glue:StopCrawler",
        "glue:StopCrawlerSchedule",
        "glue:StopWorkflowRun",
        "glue:UpdateBlueprint",
        "glue:UpdateColumnStatisticsForPartition",
        "glue:UpdateColumnStatisticsForTable",
        "glue:UpdateConnection",
        "glue:UpdateCrawler",
        "glue:UpdateCrawlerSchedule",
        "glue:UpdateDatabase",
        "glue:UpdateJob",
        "glue:UpdatePartition",
        "glue:UpdateTable",
        "glue:UpdateWorkflow",
        "iam:GetRole",
        "iam:GetRolePolicy",
        "iam:List*",
        "iam:PassRole",
        "kms:DescribeKey",
        "kms:Decrypt",
        "kms:Encrypt",
```

```
        "kms:GenerateDataKey",
        "kms:ListKeys",
        "kms:Verify",
        "kms:Sign",
        "logs:DescribeLogGroups",
        "logs:DescribeLogStreams",
        "logs:DescribeMetricFilters",
        "logs:DescribeQueries",
        "logs:DescribeQueryDefinitions",
        "logs:StartQuery",
        "logs:StopQuery",
        "logs:GetLogEvents",
        "logs:GetLogGroupFields",
        "logs:GetQueryResults",
        "logs:GetLogRecord",
        "logs:PutLogEvents",
        "logs:CreateLogStream",
        "logs:FilterLogEvents",
        "lakeformation:GetDataAccess",
        "lakeformation:GetDataLakeSettings",
        "lakeformation:GetResourceLFTags",
        "lakeformation:ListPermissions",
        "redshift-data:ListTables",
        "redshift-data:DescribeTable",
        "redshift-data:ListSchemas",
        "redshift-data:ListDatabases",
        "redshift-data:ExecuteStatement",
        "redshift-data:GetStatementResult",
        "redshift-data:DescribeStatement",
        "redshift:CreateClusterUser",
        "redshift:DescribeClusters",
        "redshift:DescribeDataShares",
        "redshift:GetClusterCredentials",
        "redshift:GetClusterCredentialsWithIAM",
        "redshift:JoinGroup",
        "redshift-serverless:ListNamespaces",
        "redshift-serverless:ListWorkgroups",
        "redshift-serverless:GetNamespace",
        "redshift-serverless:GetWorkgroup",
        "redshift-serverless:GetCredentials",
        "s3:AbortMultipartUpload",
        "s3:DeleteObject",
        "s3:DeleteObjectVersion",
        "s3:GetObject",
```

```
        "s3:GetBucketLocation",
        "s3:ListBucket",
        "s3:PutObject",
        "s3:PutObjectRetention",
        "s3:ReplicateObject",
        "s3:RestoreObject",
        "secretsmanager:CreateSecret",
        "secretsmanager:ListSecrets",
        "secretsmanager:TagResource",
        "tag:GetResources"
      ],
      "Resource": [
        "*"
      ]
    }
  ]
}
```

AWS politica gestita: AmazonDataZoneRedshiftGlueProvisioningPolicy

La AmazonDataZoneRedshiftGlueProvisioningPolicy policy concede ad Amazon DataZone le autorizzazioni necessarie per interagire con AWS Glue e Amazon Redshift.

```
{
 "Version": "2012-10-17",
 "Statement": [
  {
   "Sid": "AmazonDataZonePermissionsToCreateEnvironmentRole",
   "Effect": "Allow",
   "Action": [
    "iam:CreateRole",
    "iam:DetachRolePolicy",
    "iam:DeleteRolePolicy",
    "iam:AttachRolePolicy",
    "iam:PutRolePolicy"
   ],
   "Resource": "arn:aws:iam::*:role/datazone*",
   "Condition": {
    "StringEquals": {
```

```
     "iam:PermissionsBoundary": "arn:aws:iam::aws:policy/
AmazonDataZoneEnvironmentRolePermissionsBoundary",
     "aws:CalledViaFirst": [
      "cloudformation.amazonaws.com"
     ]
    }
   }
  },
  {
   "Sid": "IamPassRolePermissions",
   "Effect": "Allow",
   "Action": [
    "iam:PassRole"
   ],
   "Resource": [
    "arn:aws:iam::*:role/datazone*"
   ],
   "Condition": {
    "StringEquals": {
     "iam:PassedToService": [
      "glue.amazonaws.com",
      "lakeformation.amazonaws.com"
     ],
     "aws:CalledViaFirst": [
      "cloudformation.amazonaws.com"
     ]
    }
   }
  },
  {
   "Sid": "AmazonDataZonePermissionsToManageCreatedEnvironmentRole",
   "Effect": "Allow",
   "Action": [
    "iam:DeleteRole",
    "iam:GetRole"
   ],
   "Resource": "arn:aws:iam::*:role/datazone*",
   "Condition": {
    "StringEquals": {
     "aws:CalledViaFirst": [
      "cloudformation.amazonaws.com"
     ]
    }
   }
```

```
},
{
 "Sid": "AmazonDataZoneCFStackCreationForEnvironments",
 "Effect": "Allow",
 "Action": [
  "cloudformation:CreateStack",
  "cloudformation:TagResource"
 ],
 "Resource": [
  "arn:aws:cloudformation:*:*:stack/DataZone*"
 ],
 "Condition": {
  "ForAnyValue:StringLike": {
   "aws:TagKeys": "AmazonDataZoneEnvironment"
  },
  "Null": {
   "aws:ResourceTag/AmazonDataZoneEnvironment": "false"
  }
 }
},
{
 "Sid": "AmazonDataZoneCFStackManagementForEnvironments",
 "Effect": "Allow",
 "Action": [
  "cloudformation:DeleteStack",
  "cloudformation:DescribeStacks",
  "cloudformation:DescribeStackEvents"
 ],
 "Resource": [
  "arn:aws:cloudformation:*:*:stack/DataZone*"
 ]
},
{
 "Sid": "AmazonDataZoneEnvironmentParameterValidation",
 "Effect": "Allow",
 "Action": [
  "lakeformation:GetDataLakeSettings",
  "lakeformation:PutDataLakeSettings",
  "lakeformation:RevokePermissions",
  "lakeformation:ListPermissions",
  "glue:CreateDatabase",
  "glue:GetDatabase",
  "athena:GetWorkGroup",
  "logs:DescribeLogGroups",
```

```
    "redshift-serverless:GetNamespace",
    "redshift-serverless:GetWorkgroup",
    "redshift:DescribeClusters",
    "secretsmanager:ListSecrets"
   ],
   "Resource": "*"
  },
  {
   "Sid": "AmazonDataZoneEnvironmentLakeFormationPermissions",
   "Effect": "Allow",
   "Action": [
    "lakeformation:RegisterResource",
    "lakeformation:DeregisterResource",
    "lakeformation:GrantPermissions",
    "lakeformation:ListResources"
   ],
   "Resource": "*",
   "Condition": {
    "StringEquals": {
     "aws:CalledViaFirst": [
      "cloudformation.amazonaws.com"
     ]
    }
   }
  },
  {
   "Sid": "AmazonDataZoneEnvironmentGlueDeletePermissions",
   "Effect": "Allow",
   "Action": [
    "glue:DeleteDatabase"
   ],
   "Resource": "*",
   "Condition": {
    "StringEquals": {
     "aws:CalledViaFirst": [
      "cloudformation.amazonaws.com"
     ]
    }
   }
  },
  {
   "Sid": "AmazonDataZoneEnvironmentAthenaDeletePermissions",
   "Effect": "Allow",
   "Action": [
```

```
    "athena:DeleteWorkGroup"
   ],
   "Resource": "*",
   "Condition": {
    "StringEquals": {
     "aws:CalledViaFirst": [
      "cloudformation.amazonaws.com"
     ]
    }
   }
  },
  {
   "Sid": "AmazonDataZoneEnvironmentAthenaResourceCreation",
   "Effect": "Allow",
   "Action": [
    "athena:CreateWorkGroup",
    "athena:TagResource",
    "iam:TagRole",
    "iam:TagPolicy",
    "logs:TagLogGroup"
   ],
   "Resource": "*",
   "Condition": {
    "ForAnyValue:StringLike": {
     "aws:TagKeys": "AmazonDataZoneEnvironment"
    },
    "Null": {
     "aws:ResourceTag/AmazonDataZoneEnvironment": "false"
    },
    "StringEquals": {
     "aws:CalledViaFirst": [
      "cloudformation.amazonaws.com"
     ]
    }
   }
  },
  {
   "Sid": "AmazonDataZoneEnvironmentLogGroupCreation",
   "Effect": "Allow",
   "Action": [
    "logs:CreateLogGroup",
    "logs:DeleteLogGroup"
   ],
   "Resource": "arn:aws:logs:*:*:log-group:datazone-*",
```

```
    "Condition": {
     "ForAnyValue:StringLike": {
      "aws:TagKeys": "AmazonDataZoneEnvironment"
     },
     "Null": {
      "aws:ResourceTag/AmazonDataZoneEnvironment": "false"
     },
     "StringEquals": {
      "aws:CalledViaFirst": [
       "cloudformation.amazonaws.com"
      ]
     }
    }
   },
   {
    "Sid": "AmazonDataZoneEnvironmentLogGroupManagement",
    "Action": [
     "logs:PutRetentionPolicy"
    ],
    "Resource": "arn:aws:logs:*:*:log-group:datazone-*",
    "Effect": "Allow",
    "Condition": {
     "StringEquals": {
      "aws:CalledViaFirst": [
       "cloudformation.amazonaws.com"
      ]
     }
    }
   },
   {
    "Sid": "AmazonDataZoneEnvironmentIAMPolicyManagement",
    "Effect": "Allow",
    "Action": [
     "iam:DeletePolicy",
     "iam:CreatePolicy",
     "iam:GetPolicy",
     "iam:ListPolicyVersions"
    ],
    "Resource": [
     "arn:aws:iam::*:policy/datazone*"
    ],
    "Condition": {
     "StringEquals": {
      "aws:CalledViaFirst": [
```

```
      "cloudformation.amazonaws.com"
     ]
    }
   }
  },
  {
   "Sid": "AmazonDataZoneEnvironmentS3ValidationPermissions",
   "Effect": "Allow",
   "Action": [
    "s3:ListAllMyBuckets",
    "s3:ListBucket"
   ],
   "Resource": "arn:aws:s3:::*"
  },
  {
   "Sid": "AmazonDataZoneEnvironmentKMSDecryptPermissions",
   "Effect": "Allow",
   "Action": [
    "kms:GenerateDataKey",
    "kms:Decrypt"
   ],
   "Resource": "*",
   "Condition": {
    "Null": {
     "aws:ResourceTag/AmazonDataZoneEnvironment": "false"
    }
   }
  },
  {
   "Sid": "PermissionsToTagAmazonDataZoneEnvironmentGlueResources",
   "Effect": "Allow",
   "Action": [
    "glue:TagResource"
   ],
   "Resource": "*",
   "Condition": {
    "ForAnyValue:StringLike": {
     "aws:TagKeys": "AmazonDataZoneEnvironment"
    },
    "Null": {
     "aws:RequestTag/AmazonDataZoneEnvironment": "false"
    }
   }
  },
```

```
{
 "Sid": "PermissionsToGetAmazonDataZoneEnvironmentBlueprintTemplates",
 "Effect": "Allow",
 "Action": "s3:GetObject",
 "Resource": "*",
 "Condition": {
  "StringNotEquals": {
   "aws:ResourceAccount": "${aws:PrincipalAccount}"
  },
  "StringEquals": {
   "aws:CalledViaFirst": [
    "cloudformation.amazonaws.com"
   ]
  }
 }
},
{
 "Sid": "RedshiftDataPermissions",
 "Effect": "Allow",
 "Action": [
  "redshift-data:ListSchemas",
  "redshift-data:ExecuteStatement"
 ],
 "Resource": [
  "arn:aws:redshift-serverless:*:*:workgroup/*",
  "arn:aws:redshift:*:*:cluster:*"
 ]
},
{
 "Sid": "DescribeStatementPermissions",
 "Effect": "Allow",
 "Action": [
  "redshift-data:DescribeStatement"
 ],
 "Resource": "*"
},
{
 "Sid": "GetSecretValuePermissions",
 "Effect": "Allow",
 "Action": [
  "secretsmanager:GetSecretValue"
 ],
 "Resource": "*",
 "Condition": {
```

```
    "StringLike": {
     "secretsmanager:ResourceTag/AmazonDataZoneDomain": "dzd*"
    }
   }
  }
 ]
}
```

AWS politica gestita: AmazonDataZoneGlueManageAccessRolePolicy

Questa politica concede ad Amazon DataZone le autorizzazioni per pubblicare i dati di AWS Glue nel catalogo. Fornisce inoltre ad Amazon DataZone le autorizzazioni per concedere l'accesso o revocare l'accesso alle risorse pubblicate da AWS Glue nel catalogo.

```
{
 "Version": "2012-10-17",
 "Statement": [
  {
   "Sid": "GlueDataQualityPermissions",
   "Effect": "Allow",
   "Action": [
    "glue:ListDataQualityResults",
    "glue:GetDataQualityResult"
   ],
   "Resource": "arn:aws:glue:*:*:dataQualityRuleset/*",
   "Condition": {
    "StringEquals": {
     "aws:ResourceAccount": "${aws:PrincipalAccount}"
    }
   }
  },
  {
   "Sid": "GlueTableDatabasePermissions",
   "Effect": "Allow",
   "Action": [
    "glue:CreateTable",
    "glue:DeleteTable",
    "glue:GetDatabases",
    "glue:GetTables"
```

```
    ],
    "Resource": [
     "arn:aws:glue:*:*:catalog",
     "arn:aws:glue:*:*:database/*",
     "arn:aws:glue:*:*:table/*"
    ],
    "Condition": {
     "StringEquals": {
      "aws:ResourceAccount": "${aws:PrincipalAccount}"
     }
    }
   },
   {
    "Sid": "LakeformationResourceSharingPermissions",
    "Effect": "Allow",
    "Action": [
     "lakeformation:BatchGrantPermissions",
     "lakeformation:BatchRevokePermissions",
     "lakeformation:CreateLakeFormationOptIn",
     "lakeformation:DeleteLakeFormationOptIn",
     "lakeformation:GrantPermissions",
     "lakeformation:GetResourceLFTags",
     "lakeformation:ListLakeFormationOptIns",
     "lakeformation:ListPermissions",
     "lakeformation:RegisterResource",
     "lakeformation:RevokePermissions",
     "glue:GetDatabase",
     "glue:GetTable",
     "organizations:DescribeOrganization",
     "ram:GetResourceShareInvitations",
     "ram:ListResources"
    ],
    "Resource": "*"
   },
   {
    "Sid": "CrossAccountRAMResourceSharingPermissions",
    "Effect": "Allow",
    "Action": [
     "glue:DeleteResourcePolicy",
     "glue:PutResourcePolicy"
    ],
    "Resource": [
     "arn:aws:glue:*:*:catalog",
     "arn:aws:glue:*:*:database/*",
```

```
    "arn:aws:glue:*:*:table/*"
   ],
   "Condition": {
    "ForAnyValue:StringEquals": {
     "aws:CalledVia": [
      "ram.amazonaws.com"
     ]
    }
   }
  },
  {
   "Sid": "CrossAccountLakeFormationResourceSharingPermissions",
   "Effect": "Allow",
   "Action": [
    "ram:CreateResourceShare"
   ],
   "Resource": "*",
   "Condition": {
    "StringEqualsIfExists": {
     "ram:RequestedResourceType": [
      "glue:Table",
      "glue:Database",
      "glue:Catalog"
     ]
    },
    "ForAnyValue:StringEquals": {
     "aws:CalledVia": [
      "lakeformation.amazonaws.com"
     ]
    }
   }
  },
  {
   "Sid": "CrossAccountRAMResourceShareInvitationPermission",
   "Effect": "Allow",
   "Action": [
    "ram:AcceptResourceShareInvitation"
   ],
   "Resource": "arn:aws:ram:*:*:resource-share-invitation/*"
  },
  {
   "Sid": "CrossAccountRAMResourceSharingViaLakeFormationPermissions",
   "Effect": "Allow",
   "Action": [
```

```
    "ram:AssociateResourceShare",
    "ram:DeleteResourceShare",
    "ram:DisassociateResourceShare",
    "ram:GetResourceShares",
    "ram:ListResourceSharePermissions",
    "ram:UpdateResourceShare"
   ],
   "Resource": "*",
   "Condition": {
    "StringLike": {
     "ram:ResourceShareName": [
      "LakeFormation*"
     ]
    },
    "ForAnyValue:StringEquals": {
     "aws:CalledVia": [
      "lakeformation.amazonaws.com"
     ]
    }
   }
  },
  {
   "Sid": "CrossAccountRAMResourceSharingViaLakeFormationHybrid",
   "Effect": "Allow",
   "Action": "ram:AssociateResourceSharePermission",
   "Resource": "*",
   "Condition": {
    "StringLike": {
     "ram:PermissionArn": "arn:aws:ram::aws:permission/AWSRAMLFEnabled*"
    },
    "ForAnyValue:StringEquals": {
     "aws:CalledVia": [
      "lakeformation.amazonaws.com"
     ]
    }
   }
  },
  {
   "Sid": "KMSDecryptPermission",
   "Effect": "Allow",
   "Action": [
    "kms:Decrypt"
   ],
   "Resource": "*",
```

```
    "Condition": {
     "StringEquals": {
      "aws:ResourceTag/datazone:projectId": "proj-all"
     }
    }
   },
   {
    "Sid": "GetRoleForDataZone",
    "Effect": "Allow",
    "Action": [
     "iam:GetRole"
    ],
    "Resource": [
     "arn:aws:iam::*:role/AmazonDataZone*",
     "arn:aws:iam::*:role/service-role/AmazonDataZone*"
    ]
   },
   {
    "Sid": "PassRoleForDataLocationRegistration",
    "Effect": "Allow",
    "Action": [
     "iam:PassRole"
    ],
    "Resource": [
     "arn:aws:iam::*:role/AmazonDataZone*",
     "arn:aws:iam::*:role/service-role/AmazonDataZone*"
    ],
    "Condition": {
     "StringEquals": {
      "iam:PassedToService": [
       "lakeformation.amazonaws.com"
      ]
     }
    }
   }
  ]
}
```

AWS politica gestita: AmazonDataZoneRedshiftManageAccessRolePolicy

Questa politica concede ad Amazon DataZone le autorizzazioni per pubblicare i dati di Amazon Redshift nel catalogo. Fornisce inoltre ad Amazon DataZone le autorizzazioni per concedere o

revocare l'accesso agli asset pubblicati di Amazon Redshift o Amazon Redshift Serverless nel catalogo.

```
{
 "Version": "2012-10-17",
 "Statement": [
  {
   "Sid": "redshiftDataScopeDownPermissions",
   "Effect": "Allow",
   "Action": [
    "redshift-data:BatchExecuteStatement",
    "redshift-data:DescribeTable",
    "redshift-data:ExecuteStatement",
    "redshift-data:ListTables",
    "redshift-data:ListSchemas",
    "redshift-data:ListDatabases"
   ],
   "Resource": [
    "arn:aws:redshift-serverless:*:*:workgroup/*",
    "arn:aws:redshift:*:*:cluster:*"
   ],
   "Condition": {
    "StringEquals": {
     "aws:ResourceAccount": "${aws:PrincipalAccount}"
    }
   }
  },
  {
   "Sid": "listSecretsPermission",
   "Effect": "Allow",
   "Action": "secretsmanager:ListSecrets",
   "Resource": "*"
  },
  {
   "Sid": "getWorkgroupPermission",
   "Effect": "Allow",
   "Action": "redshift-serverless:GetWorkgroup",
   "Resource": [
    "arn:aws:redshift-serverless:*:*:workgroup/*"
   ],
   "Condition": {
    "StringEquals": {
```

```
      "aws:ResourceAccount": "${aws:PrincipalAccount}"
     }
    }
   },
   {
    "Sid": "getNamespacePermission",
    "Effect": "Allow",
    "Action": "redshift-serverless:GetNamespace",
    "Resource": [
     "arn:aws:redshift-serverless:*:*:namespace/*"
    ],
    "Condition": {
     "StringEquals": {
      "aws:ResourceAccount": "${aws:PrincipalAccount}"
     }
    }
   },
   {
    "Sid": "redshiftDataPermissions",
    "Effect": "Allow",
    "Action": [
     "redshift-data:DescribeStatement",
     "redshift-data:GetStatementResult",
     "redshift:DescribeClusters"
    ],
    "Resource": "*"
   },
   {
    "Sid": "dataSharesPermissions",
    "Effect": "Allow",
    "Action": [
     "redshift:AuthorizeDataShare",
     "redshift:DescribeDataShares"
    ],
    "Resource": [
     "arn:aws:redshift:*:*:datashare:*/datazone*"
    ],
    "Condition": {
     "StringEquals": {
      "aws:ResourceAccount": "${aws:PrincipalAccount}"
     }
    }
   },
   {
```

```
   "Sid": "associateDataShareConsumerPermission",
   "Effect": "Allow",
   "Action": "redshift:AssociateDataShareConsumer",
   "Resource": "arn:aws:redshift:*:*:datashare:*/datazone*"
  }
 ]
}
```

AWS Policy gestita: AmazonDataZoneCrossAccountAdmin

Puoi collegare la policy alle tue identità IAM AmazonDataZoneCrossAccountAdmin .

Questa politica consente agli utenti di lavorare con gli account DataZone associati ad Amazon.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "ram:UpdateResourceShare",
                "ram:DeleteResourceShare",
                "ram:AssociateResourceShare",
                "ram:DisassociateResourceShare",
                "ram:GetResourceShares"
            ],
            "Resource": "*",
            "Condition": {
                "StringLike": {
                    "ram:ResourceShareName": [
                        "DataZone*"
                    ]
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": [
                "datazone:PutEnvironmentBlueprintConfiguration",
                "datazone:GetEnvironmentBlueprintConfiguration",
                "datazone:DeleteEnvironmentBlueprintConfiguration",
                "datazone:ListEnvironmentBlueprintConfigurations",
```

```
                "datazone:ListDomains",
                "datazone:GetDomain",
                "datazone:GetEnvironmentBlueprint",
                "datazone:ListEnvironmentBlueprints",
                "datazone:ListEnvironments",
                "datazone:GetEnvironment",
                "ram:AcceptResourceShareInvitation",
                "ram:RejectResourceShareInvitation",
                "ram:Get*",
                "ram:List*"
            ],
            "Resource": "*"
        }
    ]
}
```

AWS politica gestita: AmazonDataZoneDomainExecutionRolePolicy

Questa è la politica predefinita per il ruolo DataZone `DomainExecutionRole` di servizio Amazon. Questo ruolo viene utilizzato da Amazon DataZone per catalogare, scoprire, gestire, condividere e analizzare i dati nel DataZone dominio Amazon.

Puoi allegare la AmazonDataZoneDomainExecutionRolePolicy politica al tuo`AmazonDataZoneDomainExecutionRole`.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "DomainExecutionRoleStatement",
      "Effect": "Allow",
      "Action": [
        "datazone:AcceptPredictions",
        "datazone:AcceptSubscriptionRequest",
        "datazone:CancelSubscription",
        "datazone:CreateAsset",
        "datazone:CreateAssetRevision",
        "datazone:CreateAssetType",
        "datazone:CreateDataSource",
        "datazone:CreateEnvironment",
        "datazone:CreateEnvironmentBlueprint",
```

```
        "datazone:CreateEnvironmentProfile",
        "datazone:CreateFormType",
        "datazone:CreateGlossary",
        "datazone:CreateGlossaryTerm",
        "datazone:CreateListingChangeSet",
        "datazone:CreateProject",
        "datazone:CreateProjectMembership",
        "datazone:CreateSubscriptionGrant",
        "datazone:CreateSubscriptionRequest",
        "datazone:DeleteAsset",
        "datazone:DeleteAssetType",
        "datazone:DeleteDataSource",
        "datazone:DeleteEnvironment",
        "datazone:DeleteEnvironmentBlueprint",
        "datazone:DeleteEnvironmentProfile",
        "datazone:DeleteFormType",
        "datazone:DeleteGlossary",
        "datazone:DeleteGlossaryTerm",
        "datazone:DeleteListing",
        "datazone:DeleteProject",
        "datazone:DeleteProjectMembership",
        "datazone:DeleteSubscriptionGrant",
        "datazone:DeleteSubscriptionRequest",
        "datazone:DeleteSubscriptionTarget",
        "datazone:GetAsset",
        "datazone:GetAssetType",
        "datazone:GetDataSource",
        "datazone:GetDataSourceRun",
        "datazone:GetDomain",
        "datazone:GetEnvironment",
        "datazone:GetEnvironmentActionLink",
        "datazone:GetEnvironmentBlueprint",
        "datazone:GetEnvironmentCredentials",
        "datazone:GetEnvironmentProfile",
        "datazone:GetFormType",
        "datazone:GetGlossary",
        "datazone:GetGlossaryTerm",
        "datazone:GetGroupProfile",
        "datazone:GetListing",
        "datazone:GetProject",
        "datazone:GetSubscription",
        "datazone:GetSubscriptionEligibility",
        "datazone:GetSubscriptionGrant",
        "datazone:GetSubscriptionRequestDetails",
```

```
        "datazone:GetSubscriptionTarget",
        "datazone:GetUserProfile",
        "datazone:ListAccountEnvironments",
        "datazone:ListAssetRevisions",
        "datazone:ListDataSourceRunActivities",
        "datazone:ListDataSourceRuns",
        "datazone:ListDataSources",
        "datazone:ListEnvironmentBlueprintConfigurations",
        "datazone:ListEnvironmentBlueprintConfigurationSummaries",
        "datazone:ListEnvironmentBlueprints",
        "datazone:ListEnvironmentProfiles",
        "datazone:ListEnvironments",
        "datazone:ListGroupsForUser",
        "datazone:ListNotifications",
        "datazone:ListProjectMemberships",
        "datazone:ListProjects",
        "datazone:ListSubscriptionGrants",
        "datazone:ListSubscriptionRequests",
        "datazone:ListSubscriptionTargets",
        "datazone:ListSubscriptions",
        "datazone:ListWarehouseMetadata",
        "datazone:RejectPredictions",
        "datazone:RejectSubscriptionRequest",
        "datazone:RevokeSubscription",
        "datazone:Search",
        "datazone:SearchGroupProfiles",
        "datazone:SearchListings",
        "datazone:SearchTypes",
        "datazone:SearchUserProfiles",
        "datazone:StartDataSourceRun",
        "datazone:UpdateDataSource",
        "datazone:UpdateEnvironment",
        "datazone:UpdateEnvironmentBlueprint",
        "datazone:UpdateEnvironmentDeploymentStatus",
        "datazone:UpdateEnvironmentProfile",
        "datazone:UpdateGlossary",
        "datazone:UpdateGlossaryTerm",
        "datazone:UpdateProject",
        "datazone:UpdateSubscriptionGrantStatus",
        "datazone:UpdateSubscriptionRequest",
        "datazone:StartMetadataGenerationRun",
        "datazone:GetMetadataGenerationRun",
        "datazone:CancelMetadataGenerationRun",
        "datazone:ListMetadataGenerationRuns"
```

```
      ],
      "Resource": "*"
    },
    {
      "Sid": "RAMResourceShareStatement",
      "Effect": "Allow",
      "Action": "ram:GetResourceShareAssociations",
      "Resource": "*"
    }
  ]
}
```

AWS politica gestita: AmazonDataZoneSageMakerProvisioning

La AmazonDataZoneSageMakerProvisioning politica concede ad Amazon DataZone le autorizzazioni necessarie per interagire con Amazon. SageMaker

```
{
 "Version": "2012-10-17",
 "Statement": [
  {
   "Sid": "CreateSageMakerStudio",
   "Effect": "Allow",
   "Action": [
    "sagemaker:CreateDomain"
   ],
   "Resource": [
    "*"
   ],
   "Condition": {
    "StringEquals": {
     "aws:CalledViaFirst": [
      "cloudformation.amazonaws.com"
     ]
    },
    "ForAnyValue:StringEquals": {
     "aws:TagKeys": [
      "AmazonDataZoneEnvironment"
     ]
    },
    "Null": {
     "aws:TagKeys": "false",
```

```
      "aws:ResourceTag/AmazonDataZoneEnvironment": "false",
      "aws:RequestTag/AmazonDataZoneEnvironment": "false"
     }
    }
   },
   {
    "Sid": "DeleteSageMakerStudio",
    "Effect": "Allow",
    "Action": [
     "sagemaker:DeleteDomain"
    ],
    "Resource": [
     "*"
    ],
    "Condition": {
     "StringEquals": {
      "aws:CalledViaFirst": [
       "cloudformation.amazonaws.com"
      ]
     },
     "ForAnyValue:StringLike": {
      "aws:TagKeys": [
       "AmazonDataZoneEnvironment"
      ]
     },
     "Null": {
      "aws:TagKeys": "false",
      "aws:ResourceTag/AmazonDataZoneEnvironment": "false"
     }
    }
   },
   {
    "Sid": "AmazonDataZoneEnvironmentSageMakerDescribePermissions",
    "Effect": "Allow",
    "Action": [
     "sagemaker:DescribeDomain"
    ],
    "Resource": "*",
    "Condition": {
     "StringEquals": {
      "aws:CalledViaFirst": [
       "cloudformation.amazonaws.com"
      ]
     }
```

```
    }
   },
   {
    "Sid": "IamPassRolePermissions",
    "Effect": "Allow",
    "Action": [
     "iam:PassRole"
    ],
    "Resource": [
     "arn:aws:iam::*:role/sm-provisioning/datazone_usr*"
    ],
    "Condition": {
     "StringEquals": {
      "iam:PassedToService": [
       "glue.amazonaws.com",
       "lakeformation.amazonaws.com",
       "sagemaker.amazonaws.com"
      ],
      "aws:CalledViaFirst": [
       "cloudformation.amazonaws.com"
      ]
     }
    }
   },
   {
    "Sid": "AmazonDataZonePermissionsToCreateEnvironmentRole",
    "Effect": "Allow",
    "Action": [
     "iam:CreateRole",
     "iam:DetachRolePolicy",
     "iam:DeleteRolePolicy",
     "iam:AttachRolePolicy",
     "iam:PutRolePolicy"
    ],
    "Resource": [
     "arn:aws:iam::*:role/sm-provisioning/datazone_usr*"
    ],
    "Condition": {
     "StringEquals": {
      "aws:CalledViaFirst": [
       "cloudformation.amazonaws.com"
      ],
      "iam:PermissionsBoundary": "arn:aws:iam::aws:policy/
AmazonDataZoneSageMakerEnvironmentRolePermissionsBoundary"
```

```
    }
   }
  },
  {
   "Sid": "AmazonDataZonePermissionsToManageEnvironmentRole",
   "Effect": "Allow",
   "Action": [
    "iam:GetRole",
    "iam:GetRolePolicy",
    "iam:DeleteRole"
   ],
   "Resource": [
    "arn:aws:iam::*:role/sm-provisioning/datazone_usr*"
   ],
   "Condition": {
    "StringEquals": {
     "aws:CalledViaFirst": [
      "cloudformation.amazonaws.com"
     ]
    }
   }
  },
  {
   "Sid": "AmazonDataZonePermissionsToCreateSageMakerServiceRole",
   "Effect": "Allow",
   "Action": [
    "iam:CreateServiceLinkedRole"
   ],
   "Resource": [
    "arn:aws:iam::*:role/aws-service-role/sagemaker.amazonaws.com/
AWSServiceRoleForAmazonSageMakerNotebooks"
   ],
   "Condition": {
    "StringEquals": {
     "aws:CalledViaFirst": [
      "cloudformation.amazonaws.com"
     ]
    }
   }
  },
  {
   "Sid": "AmazonDataZoneEnvironmentParameterValidation",
   "Effect": "Allow",
   "Action": [
```

```
    "ec2:DescribeVpcs",
    "ec2:DescribeSubnets",
    "sagemaker:ListDomains"
   ],
   "Resource": "*"
  },
  {
   "Sid": "AmazonDataZoneEnvironmentKMSKeyValidation",
   "Effect": "Allow",
   "Action": [
    "kms:DescribeKey"
   ],
   "Resource": "arn:aws:kms:*:*:key/*",
   "Condition": {
    "Null": {
     "aws:ResourceTag/AmazonDataZoneEnvironment": "false"
    }
   }
  },
  {
   "Sid": "AmazonDataZoneEnvironmentGluePermissions",
   "Effect": "Allow",
   "Action": [
    "glue:CreateConnection",
    "glue:DeleteConnection"
   ],
   "Resource": [
    "arn:aws:glue:*:*:connection/dz-sm-athena-glue-connection-*",
    "arn:aws:glue:*:*:connection/dz-sm-redshift-cluster-connection-*",
    "arn:aws:glue:*:*:connection/dz-sm-redshift-serverless-connection-*",
    "arn:aws:glue:*:*:catalog"
   ],
   "Condition": {
    "StringEquals": {
     "aws:CalledViaFirst": [
      "cloudformation.amazonaws.com"
     ]
    }
   }
  }
 ]
}
```

AWS politica gestita: AmazonDataZoneSageMakerAccess

Questa politica concede ad Amazon DataZone le autorizzazioni per pubblicare SageMaker risorse Amazon nel catalogo. Fornisce inoltre ad Amazon DataZone le autorizzazioni per concedere l'accesso o revocare l'accesso alle risorse SageMaker pubblicate da Amazon nel catalogo.

Questa policy include le autorizzazioni per eseguire le seguenti operazioni:

- cloudtrail: recupera informazioni sui sentieri. CloudTrail
- cloudwatch: recupera gli allarmi correnti. CloudWatch
- logs: recupera i filtri metrici per i log. CloudWatch
- sns: recupera l'elenco degli abbonamenti a un argomento SNS.
- config: recupera informazioni sui registratori di configurazione, sulle risorse e sulle regole di configurazione AWS . Consente inoltre al ruolo collegato al servizio di creare ed eliminare regole AWS Config e di eseguire valutazioni in base alle regole.
- iam: ottieni e genera report sulle credenziali per gli account.
- organizzazioni: recupera le informazioni sull'account e sull'unità organizzativa (OU) di un'organizzazione.
- securityhub: recupera informazioni su come sono configurati il servizio, gli standard e i controlli di Security Hub.
- tag: recupera informazioni sui tag delle risorse.

```
{
 "Version": "2012-10-17",
 "Statement": [
  {
   "Sid": "AmazonSageMakerReadPermission",
   "Effect": "Allow",
   "Action": [
    "sagemaker:DescribeFeatureGroup",
    "sagemaker:ListModelPackages",
    "sagemaker:DescribeModelPackage",
    "sagemaker:DescribeModelPackageGroup",
    "sagemaker:DescribeAlgorithm",
    "sagemaker:ListTags",
    "sagemaker:DescribeDomain",
    "sagemaker:GetModelPackageGroupPolicy",
```

```
    "sagemaker:Search"
   ],
   "Resource": "*"
  },
  {
   "Sid": "AmazonSageMakerTaggingPermission",
   "Effect": "Allow",
   "Action": [
    "sagemaker:AddTags",
    "sagemaker:DeleteTags"
   ],
   "Resource": "*",
   "Condition": {
    "ForAnyValue:StringLike": {
     "aws:TagKeys": [
      "sagemaker:shared-with:*"
     ]
    }
   }
  },
  {
   "Sid": "AmazonSageMakerModelPackageGroupPolicyPermission",
   "Effect": "Allow",
   "Action": [
    "sagemaker:PutModelPackageGroupPolicy",
    "sagemaker:DeleteModelPackageGroupPolicy"
   ],
   "Resource": [
    "arn:*:sagemaker:*:*:model-package-group/*"
   ]
  },
  {
   "Sid": "AmazonSageMakerRAMPermission",
   "Effect": "Allow",
   "Action": [
    "ram:GetResourceShares",
    "ram:GetResourceShareInvitations",
    "ram:GetResourceShareAssociations"
   ],
   "Resource": "*"
  },
  {
   "Sid": "AmazonSageMakerRAMResourcePolicyPermission",
   "Effect": "Allow",
```

```
    "Action": [
     "sagemaker:PutResourcePolicy",
     "sagemaker:GetResourcePolicy",
     "sagemaker:DeleteResourcePolicy"
    ],
    "Resource": [
     "arn:*:sagemaker:*:*:feature-group/*"
    ]
   },
   {
    "Sid": "AmazonSageMakerRAMTagResourceSharePermission",
    "Effect": "Allow",
    "Action": [
     "ram:TagResource"
    ],
    "Resource": "arn:*:ram:*:*:resource-share/*",
    "Condition": {
     "Null": {
      "aws:RequestTag/AwsDataZoneDomainId": "false"
     }
    }
   },
   {
    "Sid": "AmazonSageMakerRAMDeleteResourceSharePermission",
    "Effect": "Allow",
    "Action": [
     "ram:DeleteResourceShare"
    ],
    "Resource": "arn:*:ram:*:*:resource-share/*",
    "Condition": {
     "Null": {
      "aws:ResourceTag/AwsDataZoneDomainId": "false"
     }
    }
   },
   {
    "Sid": "AmazonSageMakerRAMCreateResourceSharePermission",
    "Effect": "Allow",
    "Action": [
     "ram:CreateResourceShare"
    ],
    "Resource": "*",
    "Condition": {
     "StringLikeIfExists": {
```

```
     "ram:RequestedResourceType": [
      "sagemaker:*"
     ]
    },
    "Null": {
     "aws:RequestTag/AwsDataZoneDomainId": "false"
    }
   }
  },
  {
   "Sid": "AmazonSageMakerS3BucketPolicyPermission",
   "Effect": "Allow",
   "Action": [
    "s3:DeleteBucketPolicy",
    "s3:PutBucketPolicy",
    "s3:GetBucketPolicy"
   ],
   "Resource": [
    "arn:aws:s3:::sagemaker-datazone*",
    "arn:aws:s3:::SageMaker-DataZone*",
    "arn:aws:s3:::datazone-sagemaker*",
    "arn:aws:s3:::DataZone-SageMaker*",
    "arn:aws:s3:::amazon-datazone*"
   ]
  },
  {
   "Sid": "AmazonSageMakerS3Permission",
   "Effect": "Allow",
   "Action": [
    "s3:GetObject",
    "s3:ListBucket"
   ],
   "Resource": [
    "arn:aws:s3:::sagemaker-datazone*",
    "arn:aws:s3:::SageMaker-DataZone*",
    "arn:aws:s3:::datazone-sagemaker*",
    "arn:aws:s3:::DataZone-SageMaker*",
    "arn:aws:s3:::amazon-datazone*"
   ]
  },
  {
   "Sid": "AmazonSageMakerECRPermission",
   "Effect": "Allow",
   "Action": [
```

```
    "ecr:GetRepositoryPolicy",
    "ecr:SetRepositoryPolicy",
    "ecr:DeleteRepositoryPolicy"
   ],
   "Resource": "*",
   "Condition": {
    "Null": {
     "aws:ResourceTag/AmazonDataZoneEnvironment": "false"
    }
   }
  },
  {
   "Sid": "AmazonSageMakerKMSReadPermission",
   "Effect": "Allow",
   "Action": [
    "kms:DescribeKey"
   ],
   "Resource": "*",
   "Condition": {
    "ForAnyValue:StringEquals": {
     "aws:TagKeys": [
      "AmazonDataZoneEnvironment"
     ]
    }
   }
  },
  {
   "Sid": "AmazonSageMakerKMSGrantPermission",
   "Effect": "Allow",
   "Action": [
    "kms:CreateGrant"
   ],
   "Resource": "*",
   "Condition": {
    "ForAnyValue:StringEquals": {
     "aws:TagKeys": [
      "AmazonDataZoneEnvironment"
     ]
    },
    "ForAllValues:StringEquals": {
     "kms:GrantOperations": [
      "Decrypt"
     ]
    }
```

```
    }
   }
  ]
}
```

AWS politica gestita: AmazonDataZoneSageMakerEnvironmentRolePermissionsBoundary

> **Note**
>
> Questa politica è un limite di autorizzazioni. Un limite di autorizzazioni imposta le autorizzazioni massime che una policy basata sull'identità può concedere a un'entità IAM. Non devi utilizzare e allegare autonomamente le politiche limite DataZone relative alle autorizzazioni di Amazon. Le politiche sui limiti DataZone delle autorizzazioni di Amazon devono essere allegate solo ai ruoli DataZone gestiti da Amazon. Per ulteriori informazioni sui limiti delle autorizzazioni, consulta Limiti delle autorizzazioni per le entità IAM nella Guida per l'utente IAM.

Quando crei un SageMaker ambiente Amazon tramite il portale DataZone dati Amazon, Amazon DataZone applica questo limite di autorizzazioni ai ruoli IAM prodotti durante la creazione dell'ambiente. Il limite delle autorizzazioni limita l'ambito dei ruoli DataZone creati da Amazon e degli eventuali ruoli aggiunti.

Amazon DataZone utilizza la policy `AmazonDataZoneSageMakerEnvironmentRolePermissionsBoundary` gestita per limitare il principale IAM fornito a cui è collegata. I responsabili potrebbero assumere la forma dei ruoli utente che Amazon DataZone può assumere per conto di utenti aziendali interattivi o di servizi di analisi (ad esempio)AWS SageMaker, e quindi condurre azioni per elaborare dati come leggere e scrivere da Amazon S3 o Amazon Redshift o eseguire il crawler Glue. AWS

La `AmazonDataZoneSageMakerEnvironmentRolePermissionsBoundary` policy concede l'accesso in lettura e scrittura per Amazon DataZone a servizi come Amazon SageMaker, AWS Glue, Amazon S3, Lake AWS Formation, Amazon Redshift e Amazon Athena. La policy fornisce inoltre autorizzazioni di lettura e scrittura ad alcune risorse dell'infrastruttura necessarie per utilizzare questi servizi, come interfacce di rete, repository Amazon ECR e chiavi KMS. AWS Fornisce inoltre accesso ad SageMaker applicazioni Amazon come Amazon SageMaker Canvas.

Amazon DataZone applica la policy `AmazonDataZoneSageMakerEnvironmentRolePermissionsBoundary` gestita come limite di autorizzazioni per tutti i ruoli DataZone dell'ambiente Amazon (proprietario e collaboratore). Questo limite di autorizzazioni limita questi ruoli per consentire l'accesso solo alle risorse e alle azioni richieste necessarie per un ambiente.

```
       {
"Version": "2012-10-17",
"Statement": [
 {
  "Sid": "AllowAllNonAdminSageMakerActions",
  "Effect": "Allow",
  "Action": [
   "sagemaker:*",
   "sagemaker-geospatial:*"
  ],
  "NotResource": [
   "arn:aws:sagemaker:*:*:domain/*",
   "arn:aws:sagemaker:*:*:user-profile/*",
   "arn:aws:sagemaker:*:*:app/*",
   "arn:aws:sagemaker:*:*:space/*",
   "arn:aws:sagemaker:*:*:flow-definition/*"
  ]
 },
 {
  "Sid": "AllowSageMakerProfileManagement",
  "Effect": "Allow",
  "Action": [
   "sagemaker:CreateUserProfile",
   "sagemaker:DescribeUserProfile",
   "sagemaker:UpdateUserProfile",
   "sagemaker:CreatePresignedDomainUrl"
  ],
  "Resource": "arn:aws:sagemaker:*:*:*/*"
 },
 {
  "Sid": "AllowLakeFormation",
  "Effect": "Allow",
  "Action": [
   "lakeformation:GetDataAccess"
  ],
  "Resource": "*"
```

```
  },
  {
   "Sid": "AllowAddTagsForAppAndSpace",
   "Effect": "Allow",
   "Action": [
    "sagemaker:AddTags"
   ],
   "Resource": [
    "arn:aws:sagemaker:*:*:app/*",
    "arn:aws:sagemaker:*:*:space/*"
   ],
   "Condition": {
    "StringEquals": {
     "sagemaker:TaggingAction": [
      "CreateApp",
      "CreateSpace"
     ]
    }
   }
  },
  {
   "Sid": "AllowStudioActions",
   "Effect": "Allow",
   "Action": [
    "sagemaker:CreatePresignedDomainUrl",
    "sagemaker:DescribeApp",
    "sagemaker:DescribeDomain",
    "sagemaker:DescribeSpace",
    "sagemaker:DescribeUserProfile",
    "sagemaker:ListApps",
    "sagemaker:ListDomains",
    "sagemaker:ListSpaces",
    "sagemaker:ListUserProfiles"
   ],
   "Resource": "*"
  },
  {
   "Sid": "AllowAppActionsForUserProfile",
   "Effect": "Allow",
   "Action": [
    "sagemaker:CreateApp",
    "sagemaker:DeleteApp"
   ],
   "Resource": "arn:aws:sagemaker:*:*:app/*/*/*/*",
```

```
    "Condition": {
     "Null": {
      "sagemaker:OwnerUserProfileArn": "true"
     }
    }
   },
   {
    "Sid": "AllowAppActionsForSharedSpaces",
    "Effect": "Allow",
    "Action": [
     "sagemaker:CreateApp",
     "sagemaker:DeleteApp"
    ],
    "Resource": "arn:aws:sagemaker:*:*:app/${sagemaker:DomainId}/*/*/*",
    "Condition": {
     "StringEquals": {
      "sagemaker:SpaceSharingType": [
       "Shared"
      ]
     }
    }
   },
   {
    "Sid": "AllowMutatingActionsOnSharedSpacesWithoutOwner",
    "Effect": "Allow",
    "Action": [
     "sagemaker:CreateSpace",
     "sagemaker:DeleteSpace",
     "sagemaker:UpdateSpace"
    ],
    "Resource": "arn:aws:sagemaker:*:*:space/${sagemaker:DomainId}/*",
    "Condition": {
     "Null": {
      "sagemaker:OwnerUserProfileArn": "true"
     }
    }
   },
   {
    "Sid": "RestrictMutatingActionsOnSpacesToOwnerUserProfile",
    "Effect": "Allow",
    "Action": [
     "sagemaker:CreateSpace",
     "sagemaker:DeleteSpace",
     "sagemaker:UpdateSpace"
```

```
    ],
    "Resource": "arn:aws:sagemaker:*:*:space/${sagemaker:DomainId}/*",
    "Condition": {
     "ArnLike": {
      "sagemaker:OwnerUserProfileArn": "arn:aws:sagemaker:*:*:user-profile/
${sagemaker:DomainId}/${sagemaker:UserProfileName}"
     },
     "StringEquals": {
      "sagemaker:SpaceSharingType": [
       "Private",
       "Shared"
      ]
     }
    }
   },
   {
    "Sid": "RestrictMutatingActionsOnPrivateSpaceAppsToOwnerUserProfile",
    "Effect": "Allow",
    "Action": [
     "sagemaker:CreateApp",
     "sagemaker:DeleteApp"
    ],
    "Resource": "arn:aws:sagemaker:*:*:app/${sagemaker:DomainId}/*/*/*",
    "Condition": {
     "ArnLike": {
      "sagemaker:OwnerUserProfileArn": "arn:aws:sagemaker:*:*:user-profile/
${sagemaker:DomainId}/${sagemaker:UserProfileName}"
     },
     "StringEquals": {
      "sagemaker:SpaceSharingType": [
       "Private"
      ]
     }
    }
   },
   {
    "Sid": "AllowFlowDefinitionActions",
    "Effect": "Allow",
    "Action": "sagemaker:*",
    "Resource": [
     "arn:aws:sagemaker:*:*:flow-definition/*"
    ],
    "Condition": {
     "StringEqualsIfExists": {
```

```
     "sagemaker:WorkteamType": [
      "private-crowd",
      "vendor-crowd"
     ]
    }
   }
  },
  {
   "Sid": "AllowAWSServiceActions",
   "Effect": "Allow",
   "Action": [
    "sqlworkbench:*",
    "datazone:*",
    "application-autoscaling:DeleteScalingPolicy",
    "application-autoscaling:DeleteScheduledAction",
    "application-autoscaling:DeregisterScalableTarget",
    "application-autoscaling:DescribeScalableTargets",
    "application-autoscaling:DescribeScalingActivities",
    "application-autoscaling:DescribeScalingPolicies",
    "application-autoscaling:DescribeScheduledActions",
    "application-autoscaling:PutScalingPolicy",
    "application-autoscaling:PutScheduledAction",
    "application-autoscaling:RegisterScalableTarget",
    "aws-marketplace:ViewSubscriptions",
    "cloudformation:GetTemplateSummary",
    "cloudwatch:DeleteAlarms",
    "cloudwatch:DescribeAlarms",
    "cloudwatch:GetMetricData",
    "cloudwatch:GetMetricStatistics",
    "cloudwatch:ListMetrics",
    "cloudwatch:PutMetricAlarm",
    "cloudwatch:PutMetricData",
    "codecommit:BatchGetRepositories",
    "codecommit:CreateRepository",
    "codecommit:GetRepository",
    "codecommit:List*",
    "ec2:CreateNetworkInterface",
    "ec2:CreateNetworkInterfacePermission",
    "ec2:DeleteNetworkInterface",
    "ec2:DeleteNetworkInterfacePermission",
    "ec2:DescribeDhcpOptions",
    "ec2:DescribeNetworkInterfaces",
    "ec2:DescribeRouteTables",
    "ec2:DescribeSecurityGroups",
```

```
    "ec2:DescribeSubnets",
    "ec2:DescribeVpcEndpoints",
    "ec2:DescribeVpcEndpointServices",
    "ec2:DescribeVpcs",
    "ecr:BatchCheckLayerAvailability",
    "ecr:BatchGetImage",
    "ecr:Describe*",
    "ecr:GetAuthorizationToken",
    "ecr:GetDownloadUrlForLayer",
    "ecr:StartImageScan",
    "elastic-inference:Connect",
    "elasticfilesystem:DescribeFileSystems",
    "elasticfilesystem:DescribeMountTargets",
    "fsx:DescribeFileSystems",
    "groundtruthlabeling:*",
    "iam:GetRole",
    "iam:ListRoles",
    "kms:DescribeKey",
    "kms:ListAliases",
    "lambda:ListFunctions",
    "logs:CreateLogDelivery",
    "logs:CreateLogGroup",
    "logs:CreateLogStream",
    "logs:DeleteLogDelivery",
    "logs:DescribeLogGroups",
    "logs:DescribeLogStreams",
    "logs:GetLogDelivery",
    "logs:GetLogEvents",
    "logs:ListLogDeliveries",
    "logs:PutLogEvents",
    "logs:UpdateLogDelivery",
    "redshift-data:BatchExecuteStatement",
    "redshift-data:CancelStatement",
    "redshift-data:DescribeStatement",
    "redshift-data:DescribeTable",
    "redshift-data:ExecuteStatement",
    "redshift-data:GetStatementResult",
    "redshift-data:ListSchemas",
    "redshift-data:ListTables",
    "redshift-serverless:GetCredentials",
    "redshift-serverless:GetNamespace",
    "redshift-serverless:GetWorkgroup",
    "redshift-serverless:ListNamespaces",
    "redshift-serverless:ListWorkgroups",
```

```
    "secretsmanager:ListSecrets",
    "servicecatalog:Describe*",
    "servicecatalog:List*",
    "servicecatalog:ScanProvisionedProducts",
    "servicecatalog:SearchProducts",
    "servicecatalog:SearchProvisionedProducts",
    "sns:ListTopics",
    "tag:GetResources"
   ],
   "Resource": "*"
  },
  {
   "Sid": "AllowRAMInvitation",
   "Effect": "Allow",
   "Action": "ram:AcceptResourceShareInvitation",
   "Resource": "*",
   "Condition": {
    "StringLike": {
     "ram:ResourceShareName": "dzd_*"
    }
   }
  },
  {
   "Sid": "AllowECRActions",
   "Effect": "Allow",
   "Action": [
    "ecr:SetRepositoryPolicy",
    "ecr:CompleteLayerUpload",
    "ecr:CreateRepository",
    "ecr:BatchDeleteImage",
    "ecr:UploadLayerPart",
    "ecr:DeleteRepositoryPolicy",
    "ecr:InitiateLayerUpload",
    "ecr:DeleteRepository",
    "ecr:PutImage",
    "ecr:TagResource",
    "ecr:UntagResource"
   ],
   "Resource": [
    "arn:aws:ecr:*:*:repository/sagemaker*",
    "arn:aws:ecr:*:*:repository/datazone*"
   ]
  },
  {
```

```
    "Sid": "AllowCodeCommitActions",
    "Effect": "Allow",
    "Action": [
     "codecommit:GitPull",
     "codecommit:GitPush"
    ],
    "Resource": [
     "arn:aws:codecommit:*:*:*sagemaker*",
     "arn:aws:codecommit:*:*:*SageMaker*",
     "arn:aws:codecommit:*:*:*Sagemaker*"
    ]
   },
   {
    "Sid": "AllowCodeBuildActions",
    "Action": [
     "codebuild:BatchGetBuilds",
     "codebuild:StartBuild"
    ],
    "Resource": [
     "arn:aws:codebuild:*:*:project/sagemaker*",
     "arn:aws:codebuild:*:*:build/*"
    ],
    "Effect": "Allow"
   },
   {
    "Sid": "AllowStepFunctionsActions",
    "Action": [
     "states:DescribeExecution",
     "states:GetExecutionHistory",
     "states:StartExecution",
     "states:StopExecution",
     "states:UpdateStateMachine"
    ],
    "Resource": [
     "arn:aws:states:*:*:statemachine:*sagemaker*",
     "arn:aws:states:*:*:execution:*sagemaker*:*"
    ],
    "Effect": "Allow"
   },
   {
    "Sid": "AllowSecretManagerActions",
    "Effect": "Allow",
    "Action": [
     "secretsmanager:DescribeSecret",
```

```
    "secretsmanager:GetSecretValue",
    "secretsmanager:CreateSecret",
    "secretsmanager:PutResourcePolicy"
   ],
   "Resource": [
    "arn:aws:secretsmanager:*:*:secret:AmazonSageMaker-*"
   ]
  },
  {
   "Sid": "AllowServiceCatalogProvisionProduct",
   "Effect": "Allow",
   "Action": [
    "servicecatalog:ProvisionProduct"
   ],
   "Resource": "*"
  },
  {
   "Sid": "AllowServiceCatalogTerminateUpdateProvisionProduct",
   "Effect": "Allow",
   "Action": [
    "servicecatalog:TerminateProvisionedProduct",
    "servicecatalog:UpdateProvisionedProduct"
   ],
   "Resource": "*",
   "Condition": {
    "StringEquals": {
     "servicecatalog:userLevel": "self"
    }
   }
  },
  {
   "Sid": "AllowS3ObjectActions",
   "Effect": "Allow",
   "Action": [
    "s3:AbortMultipartUpload",
    "s3:DeleteObject",
    "s3:DeleteObjectVersion",
    "s3:GetObject",
    "s3:PutObject",
    "s3:PutObjectRetention",
    "s3:ReplicateObject",
    "s3:RestoreObject",
    "s3:GetBucketAcl",
    "s3:PutObjectAcl"
```

```
    ],
    "Resource": [
     "arn:aws:s3:::SageMaker-DataZone*",
     "arn:aws:s3:::DataZone-SageMaker*",
     "arn:aws:s3:::Sagemaker-DataZone*",
     "arn:aws:s3:::DataZone-Sagemaker*",
     "arn:aws:s3:::sagemaker-datazone*",
     "arn:aws:s3:::datazone-sagemaker*",
     "arn:aws:s3:::amazon-datazone*"
    ]
   },
   {
    "Sid": "AllowS3GetObjectWithSageMakerExistingObjectTag",
    "Effect": "Allow",
    "Action": [
     "s3:GetObject"
    ],
    "Resource": [
     "arn:aws:s3:::*"
    ],
    "Condition": {
     "StringEqualsIgnoreCase": {
      "s3:ExistingObjectTag/SageMaker": "true"
     }
    }
   },
   {
    "Sid": "AllowS3GetObjectWithServiceCatalogProvisioningExistingObjectTag",
    "Effect": "Allow",
    "Action": [
     "s3:GetObject"
    ],
    "Resource": [
     "arn:aws:s3:::*"
    ],
    "Condition": {
     "StringEquals": {
      "s3:ExistingObjectTag/servicecatalog:provisioning": "true"
     }
    }
   },
   {
    "Sid": "AllowS3BucketActions",
    "Effect": "Allow",
```

```
    "Action": [
     "s3:GetBucketLocation",
     "s3:ListBucket",
     "s3:ListAllMyBuckets",
     "s3:GetBucketCors",
     "s3:PutBucketCors"
    ],
    "Resource": [
     "arn:aws:s3:::SageMaker-DataZone*",
     "arn:aws:s3:::DataZone-SageMaker*",
     "arn:aws:s3:::Sagemaker-DataZone*",
     "arn:aws:s3:::DataZone-Sagemaker*",
     "arn:aws:s3:::sagemaker-datazone*",
     "arn:aws:s3:::datazone-sagemaker*",
     "arn:aws:s3:::amazon-datazone*"
    ]
   },
   {
    "Sid": "ReadSageMakerJumpstartArtifacts",
    "Effect": "Allow",
    "Action": "s3:GetObject",
    "Resource": [
     "arn:aws:s3:::jumpstart-cache-prod-us-west-2/*",
     "arn:aws:s3:::jumpstart-cache-prod-us-east-1/*",
     "arn:aws:s3:::jumpstart-cache-prod-us-east-2/*",
     "arn:aws:s3:::jumpstart-cache-prod-eu-west-1/*",
     "arn:aws:s3:::jumpstart-cache-prod-eu-central-1/*",
     "arn:aws:s3:::jumpstart-cache-prod-ap-south-1/*",
     "arn:aws:s3:::jumpstart-cache-prod-ap-northeast-2/*",
     "arn:aws:s3:::jumpstart-cache-prod-ap-northeast-1/*",
     "arn:aws:s3:::jumpstart-cache-prod-ap-southeast-1/*",
     "arn:aws:s3:::jumpstart-cache-prod-ap-southeast-2/*"
    ]
   },
   {
    "Sid": "AllowLambdaInvokeFunction",
    "Effect": "Allow",
    "Action": [
     "lambda:InvokeFunction"
    ],
    "Resource": [
     "arn:aws:lambda:*:*:function:*SageMaker*",
     "arn:aws:lambda:*:*:function:*sagemaker*",
     "arn:aws:lambda:*:*:function:*Sagemaker*",
```

```
     "arn:aws:lambda:*:*:function:*LabelingFunction*"
    ]
   },
   {
    "Sid": "AllowCreateServiceLinkedRoleForSageMakerApplicationAutoscaling",
    "Action": "iam:CreateServiceLinkedRole",
    "Effect": "Allow",
    "Resource": "arn:aws:iam::*:role/aws-service-role/sagemaker.application-
autoscaling.amazonaws.com/AWSServiceRoleForApplicationAutoScaling_SageMakerEndpoint",
    "Condition": {
     "StringLike": {
      "iam:AWSServiceName": "sagemaker.application-autoscaling.amazonaws.com"
     }
    }
   },
   {
    "Sid": "AllowSNSActions",
    "Effect": "Allow",
    "Action": [
     "sns:Subscribe",
     "sns:CreateTopic",
     "sns:Publish"
    ],
    "Resource": [
     "arn:aws:sns:*:*:*SageMaker*",
     "arn:aws:sns:*:*:*Sagemaker*",
     "arn:aws:sns:*:*:*sagemaker*"
    ]
   },
   {
    "Sid": "AllowPassRoleForSageMakerRoles",
    "Effect": "Allow",
    "Action": [
     "iam:PassRole"
    ],
    "Resource": [
     "arn:aws:iam::*:role/sm-provisioning/datazone_usr_sagemaker_execution_role_*"
    ],
    "Condition": {
     "StringEquals": {
      "iam:PassedToService": [
       "glue.amazonaws.com",
       "bedrock.amazonaws.com",
       "states.amazonaws.com",
```

```
      "lakeformation.amazonaws.com",
      "events.amazonaws.com",
      "sagemaker.amazonaws.com",
      "forecast.amazonaws.com"
     ]
    }
   }
  },
  {
   "Sid": "CrossAccountKmsOperations",
   "Effect": "Allow",
   "Action": [
    "kms:DescribeKey",
    "kms:Decrypt",
    "kms:ListKeys"
   ],
   "Resource": "*",
   "Condition": {
    "StringNotEquals": {
     "aws:ResourceAccount": "${aws:PrincipalAccount}"
    }
   }
  },
  {
   "Sid": "KmsOperationsWithResourceTag",
   "Effect": "Allow",
   "Action": [
    "kms:DescribeKey",
    "kms:Decrypt",
    "kms:ListKeys",
    "kms:Encrypt",
    "kms:GenerateDataKey",
    "kms:RetireGrant"
   ],
   "Resource": "*",
   "Condition": {
    "Null": {
     "aws:ResourceTag/AmazonDataZoneEnvironment": "false"
    }
   }
  },
  {
   "Sid": "AllowAthenaActions",
   "Effect": "Allow",
```

```
    "Action": [
     "athena:BatchGetNamedQuery",
     "athena:BatchGetPreparedStatement",
     "athena:BatchGetQueryExecution",
     "athena:CreateNamedQuery",
     "athena:CreateNotebook",
     "athena:CreatePreparedStatement",
     "athena:CreatePresignedNotebookUrl",
     "athena:DeleteNamedQuery",
     "athena:DeleteNotebook",
     "athena:DeletePreparedStatement",
     "athena:ExportNotebook",
     "athena:GetDatabase",
     "athena:GetDataCatalog",
     "athena:GetNamedQuery",
     "athena:GetPreparedStatement",
     "athena:GetQueryExecution",
     "athena:GetQueryResults",
     "athena:GetQueryResultsStream",
     "athena:GetQueryRuntimeStatistics",
     "athena:GetTableMetadata",
     "athena:GetWorkGroup",
     "athena:ImportNotebook",
     "athena:ListDatabases",
     "athena:ListDataCatalogs",
     "athena:ListEngineVersions",
     "athena:ListNamedQueries",
     "athena:ListPreparedStatements",
     "athena:ListQueryExecutions",
     "athena:ListTableMetadata",
     "athena:ListTagsForResource",
     "athena:ListWorkGroups",
     "athena:StartCalculationExecution",
     "athena:StartQueryExecution",
     "athena:StartSession",
     "athena:StopCalculationExecution",
     "athena:StopQueryExecution",
     "athena:TerminateSession",
     "athena:UpdateNamedQuery",
     "athena:UpdateNotebook",
     "athena:UpdateNotebookMetadata",
     "athena:UpdatePreparedStatement"
    ],
    "Resource": [
```

```
    "*"
   ]
  },
  {
   "Sid": "AllowGlueCreateDatabase",
   "Effect": "Allow",
   "Action": [
    "glue:CreateDatabase"
   ],
   "Resource": [
    "arn:aws:glue:*:*:catalog",
    "arn:aws:glue:*:*:database/default"
   ]
  },
  {
   "Sid": "AllowRedshiftGetClusterCredentials",
   "Effect": "Allow",
   "Action": [
    "redshift:GetClusterCredentials"
   ],
   "Resource": [
    "arn:aws:redshift:*:*:dbuser:*/sagemaker_access*",
    "arn:aws:redshift:*:*:dbname:*"
   ]
  },
  {
   "Sid": "AllowListTags",
   "Effect": "Allow",
   "Action": [
    "sagemaker:ListTags"
   ],
   "Resource": [
    "arn:aws:sagemaker:*:*:user-profile/*",
    "arn:aws:sagemaker:*:*:domain/*"
   ]
  },
  {
   "Sid": "AllowCloudformationListStackResources",
   "Effect": "Allow",
   "Action": [
    "cloudformation:ListStackResources"
   ],
   "Resource": "arn:aws:cloudformation:*:*:stack/SC-*"
  },
```

```
{
 "Sid": "AllowGlueActions",
 "Effect": "Allow",
 "Action": [
  "glue:GetColumnStatisticsForPartition",
  "glue:GetColumnStatisticsForTable",
  "glue:ListJobs",
  "glue:CreateSession",
  "glue:RunStatement",
  "glue:BatchCreatePartition",
  "glue:CreatePartitionIndex",
  "glue:CreateTable",
  "glue:BatchGetWorkflows",
  "glue:BatchUpdatePartition",
  "glue:BatchDeletePartition",
  "glue:GetPartition",
  "glue:GetPartitions",
  "glue:UpdateTable",
  "glue:DeleteTableVersion",
  "glue:DeleteTable",
  "glue:DeleteColumnStatisticsForPartition",
  "glue:DeleteColumnStatisticsForTable",
  "glue:DeletePartitionIndex",
  "glue:UpdateColumnStatisticsForPartition",
  "glue:UpdateColumnStatisticsForTable",
  "glue:BatchDeleteTableVersion",
  "glue:BatchDeleteTable",
  "glue:CreatePartition",
  "glue:DeletePartition",
  "glue:UpdatePartition",
  "glue:CreateBlueprint",
  "glue:CreateJob",
  "glue:CreateConnection",
  "glue:CreateCrawler",
  "glue:CreateDataQualityRuleset",
  "glue:CreateWorkflow",
  "glue:GetDatabases",
  "glue:GetTables",
  "glue:GetTable",
  "glue:SearchTables",
  "glue:NotifyEvent",
  "glue:ListSchemas",
  "glue:BatchGetJobs",
  "glue:GetConnection",
```

```
    "glue:GetDatabase"
   ],
   "Resource": [
    "*"
   ]
  },
  {
   "Sid": "AllowGlueActionsWithEnvironmentTag",
   "Effect": "Allow",
   "Action": [
    "glue:SearchTables",
    "glue:NotifyEvent",
    "glue:StartBlueprintRun",
    "glue:PutWorkflowRunProperties",
    "glue:StopCrawler",
    "glue:DeleteJob",
    "glue:DeleteWorkflow",
    "glue:UpdateCrawler",
    "glue:DeleteBlueprint",
    "glue:UpdateWorkflow",
    "glue:StartCrawler",
    "glue:ResetJobBookmark",
    "glue:UpdateJob",
    "glue:StartWorkflowRun",
    "glue:StopCrawlerSchedule",
    "glue:ResumeWorkflowRun",
    "glue:ListSchemas",
    "glue:DeleteCrawler",
    "glue:UpdateBlueprint",
    "glue:BatchStopJobRun",
    "glue:StopWorkflowRun",
    "glue:BatchGetJobs",
    "glue:BatchGetWorkflows",
    "glue:UpdateCrawlerSchedule",
    "glue:DeleteConnection",
    "glue:UpdateConnection",
    "glue:GetConnection",
    "glue:GetDatabase",
    "glue:GetTable",
    "glue:GetPartition",
    "glue:GetPartitions",
    "glue:BatchDeleteConnection",
    "glue:StartCrawlerSchedule",
    "glue:StartJobRun",
```

```
    "glue:CreateWorkflow",
    "glue:*DataQuality*"
   ],
   "Resource": "*",
   "Condition": {
    "Null": {
     "aws:ResourceTag/AmazonDataZoneEnvironment": "false"
    }
   }
  },
  {
   "Sid": "AllowGlueDefaultAccess",
   "Effect": "Allow",
   "Action": [
    "glue:BatchGet*",
    "glue:Get*",
    "glue:SearchTables",
    "glue:List*",
    "glue:RunStatement"
   ],
   "Resource": [
    "arn:aws:glue:*:*:catalog",
    "arn:aws:glue:*:*:database/default",
    "arn:aws:glue:*:*:connection/dz-sm-*",
    "arn:aws:glue:*:*:session/*"
   ]
  },
  {
   "Sid": "AllowRedshiftClusterActions",
   "Effect": "Allow",
   "Action": [
    "redshift:GetClusterCredentialsWithIAM",
    "redshift:DescribeClusters"
   ],
   "Resource": [
    "arn:aws:redshift:*:*:cluster:*",
    "arn:aws:redshift:*:*:dbname:*"
   ]
  },
  {
   "Sid": "AllowCreateClusterUser",
   "Effect": "Allow",
   "Action": [
    "redshift:CreateClusterUser"
```

```
    ],
    "Resource": [
     "arn:aws:redshift:*:*:dbuser:*"
    ]
   },
   {
    "Sid": "AllowCreateSecretActions",
    "Effect": "Allow",
    "Action": [
     "secretsmanager:CreateSecret",
     "secretsmanager:TagResource"
    ],
    "Resource": "arn:aws:secretsmanager:*:*:secret:AmazonDataZone-*",
    "Condition": {
     "StringLike": {
      "aws:ResourceTag/AmazonDataZoneDomain": "dzd_*",
      "aws:RequestTag/AmazonDataZoneDomain": "dzd_*"
     },
     "Null": {
      "aws:TagKeys": "false",
      "aws:ResourceTag/AmazonDataZoneProject": "false",
      "aws:ResourceTag/AmazonDataZoneDomain": "false",
      "aws:RequestTag/AmazonDataZoneDomain": "false",
      "aws:RequestTag/AmazonDataZoneProject": "false"
     },
     "ForAllValues:StringEquals": {
      "aws:TagKeys": [
       "AmazonDataZoneDomain",
       "AmazonDataZoneProject"
      ]
     }
    }
   },
   {
    "Sid": "ForecastOperations",
    "Effect": "Allow",
    "Action": [
     "forecast:CreateExplainabilityExport",
     "forecast:CreateExplainability",
     "forecast:CreateForecastEndpoint",
     "forecast:CreateAutoPredictor",
     "forecast:CreateDatasetImportJob",
     "forecast:CreateDatasetGroup",
     "forecast:CreateDataset",
```

```
    "forecast:CreateForecast",
    "forecast:CreateForecastExportJob",
    "forecast:CreatePredictorBacktestExportJob",
    "forecast:CreatePredictor",
    "forecast:DescribeExplainabilityExport",
    "forecast:DescribeExplainability",
    "forecast:DescribeAutoPredictor",
    "forecast:DescribeForecastEndpoint",
    "forecast:DescribeDatasetImportJob",
    "forecast:DescribeDataset",
    "forecast:DescribeForecast",
    "forecast:DescribeForecastExportJob",
    "forecast:DescribePredictorBacktestExportJob",
    "forecast:GetAccuracyMetrics",
    "forecast:InvokeForecastEndpoint",
    "forecast:GetRecentForecastContext",
    "forecast:DescribePredictor",
    "forecast:TagResource",
    "forecast:DeleteResourceTree"
   ],
   "Resource": [
    "arn:aws:forecast:*:*:*Canvas*"
   ]
  },
  {
   "Sid": "RDSOperation",
   "Effect": "Allow",
   "Action": "rds:DescribeDBInstances",
   "Resource": "*"
  },
  {
   "Sid": "AllowEventBridgeRule",
   "Effect": "Allow",
   "Action": [
    "events:PutRule"
   ],
   "Resource": "arn:aws:events:*:*:rule/*",
   "Condition": {
    "StringEquals": {
     "aws:RequestTag/sagemaker:is-canvas-data-prep-job": "true"
    }
   }
  },
  {
```

```
    "Sid": "EventBridgeOperations",
    "Effect": "Allow",
    "Action": [
     "events:DescribeRule",
     "events:PutTargets"
    ],
    "Resource": "arn:aws:events:*:*:rule/*",
    "Condition": {
     "StringEquals": {
      "aws:ResourceTag/sagemaker:is-canvas-data-prep-job": "true"
     }
    }
   },
   {
    "Sid": "EventBridgeTagBasedOperations",
    "Effect": "Allow",
    "Action": [
     "events:TagResource"
    ],
    "Resource": "arn:aws:events:*:*:rule/*",
    "Condition": {
     "StringEquals": {
      "aws:RequestTag/sagemaker:is-canvas-data-prep-job": "true",
      "aws:ResourceTag/sagemaker:is-canvas-data-prep-job": "true"
     }
    }
   },
   {
    "Sid": "EventBridgeListTagOperation",
    "Effect": "Allow",
    "Action": "events:ListTagsForResource",
    "Resource": "*"
   },
   {
    "Sid": "AllowEMR",
    "Effect": "Allow",
    "Action": [
     "elasticmapreduce:DescribeCluster",
     "elasticmapreduce:ListInstanceGroups",
     "elasticmapreduce:ListClusters"
    ],
    "Resource": "*"
   },
   {
```

```
    "Sid": "AllowSSOAction",
    "Effect": "Allow",
    "Action": [
     "sso:CreateApplicationAssignment",
     "sso:AssociateProfile"
    ],
    "Resource": "*"
   },
   {
    "Sid": "DenyNotAction",
    "Effect": "Deny",
    "NotAction": [
     "sagemaker:*",
     "sagemaker-geospatial:*",
     "sqlworkbench:*",
     "datazone:*",
     "forecast:*",
     "application-autoscaling:DeleteScalingPolicy",
     "application-autoscaling:DeleteScheduledAction",
     "application-autoscaling:DeregisterScalableTarget",
     "application-autoscaling:DescribeScalableTargets",
     "application-autoscaling:DescribeScalingActivities",
     "application-autoscaling:DescribeScalingPolicies",
     "application-autoscaling:DescribeScheduledActions",
     "application-autoscaling:PutScalingPolicy",
     "application-autoscaling:PutScheduledAction",
     "application-autoscaling:RegisterScalableTarget",
     "athena:BatchGetNamedQuery",
     "athena:BatchGetPreparedStatement",
     "athena:BatchGetQueryExecution",
     "athena:CreateNamedQuery",
     "athena:CreateNotebook",
     "athena:CreatePreparedStatement",
     "athena:CreatePresignedNotebookUrl",
     "athena:DeleteNamedQuery",
     "athena:DeleteNotebook",
     "athena:DeletePreparedStatement",
     "athena:ExportNotebook",
     "athena:GetDatabase",
     "athena:GetDataCatalog",
     "athena:GetNamedQuery",
     "athena:GetPreparedStatement",
     "athena:GetQueryExecution",
     "athena:GetQueryResults",
```

```
    "athena:GetQueryResultsStream",
    "athena:GetQueryRuntimeStatistics",
    "athena:GetTableMetadata",
    "athena:GetWorkGroup",
    "athena:ImportNotebook",
    "athena:ListDatabases",
    "athena:ListDataCatalogs",
    "athena:ListEngineVersions",
    "athena:ListNamedQueries",
    "athena:ListPreparedStatements",
    "athena:ListQueryExecutions",
    "athena:ListTableMetadata",
    "athena:ListTagsForResource",
    "athena:ListWorkGroups",
    "athena:StartCalculationExecution",
    "athena:StartQueryExecution",
    "athena:StartSession",
    "athena:StopCalculationExecution",
    "athena:StopQueryExecution",
    "athena:TerminateSession",
    "athena:UpdateNamedQuery",
    "athena:UpdateNotebook",
    "athena:UpdateNotebookMetadata",
    "athena:UpdatePreparedStatement",
    "aws-marketplace:ViewSubscriptions",
    "cloudformation:GetTemplateSummary",
    "cloudformation:ListStackResources",
    "cloudwatch:DeleteAlarms",
    "cloudwatch:DescribeAlarms",
    "cloudwatch:GetMetricData",
    "cloudwatch:GetMetricStatistics",
    "cloudwatch:ListMetrics",
    "cloudwatch:PutMetricAlarm",
    "cloudwatch:PutMetricData",
    "codebuild:BatchGetBuilds",
    "codebuild:StartBuild",
    "codecommit:BatchGetRepositories",
    "codecommit:CreateRepository",
    "codecommit:GetRepository",
    "codecommit:List*",
    "codecommit:GitPull",
    "codecommit:GitPush",
    "ec2:CreateNetworkInterface",
    "ec2:CreateNetworkInterfacePermission",
```

```
    "ec2:DeleteNetworkInterface",
    "ec2:DeleteNetworkInterfacePermission",
    "ec2:DescribeDhcpOptions",
    "ec2:DescribeNetworkInterfaces",
    "ec2:DescribeRouteTables",
    "ec2:DescribeSecurityGroups",
    "ec2:DescribeSubnets",
    "ec2:DescribeVpcEndpoints",
    "ec2:DescribeVpcEndpointServices",
    "ec2:DescribeVpcs",
    "ecr:BatchCheckLayerAvailability",
    "ecr:BatchGetImage",
    "ecr:CreateRepository",
    "ecr:Describe*",
    "ecr:GetAuthorizationToken",
    "ecr:GetDownloadUrlForLayer",
    "ecr:SetRepositoryPolicy",
    "ecr:CompleteLayerUpload",
    "ecr:BatchDeleteImage",
    "ecr:UploadLayerPart",
    "ecr:DeleteRepositoryPolicy",
    "ecr:InitiateLayerUpload",
    "ecr:DeleteRepository",
    "ecr:PutImage",
    "ecr:StartImageScan",
    "ecr:TagResource",
    "ecr:UntagResource",
    "elastic-inference:Connect",
    "elasticfilesystem:DescribeFileSystems",
    "elasticfilesystem:DescribeMountTargets",
    "elasticmapreduce:DescribeCluster",
    "elasticmapreduce:ListInstanceGroups",
    "elasticmapreduce:ListClusters",
    "events:PutRule",
    "events:DescribeRule",
    "events:PutTargets",
    "events:TagResource",
    "events:ListTagsForResource",
    "fsx:DescribeFileSystems",
    "glue:SearchTables",
    "glue:NotifyEvent",
    "glue:StartBlueprintRun",
    "glue:PutWorkflowRunProperties",
    "glue:StopCrawler",
```

```
    "glue:DeleteJob",
    "glue:DeleteWorkflow",
    "glue:UpdateCrawler",
    "glue:DeleteBlueprint",
    "glue:UpdateWorkflow",
    "glue:StartCrawler",
    "glue:ResetJobBookmark",
    "glue:UpdateJob",
    "glue:StartWorkflowRun",
    "glue:StopCrawlerSchedule",
    "glue:ResumeWorkflowRun",
    "glue:DeleteCrawler",
    "glue:UpdateBlueprint",
    "glue:BatchStopJobRun",
    "glue:StopWorkflowRun",
    "glue:BatchGet*",
    "glue:UpdateCrawlerSchedule",
    "glue:DeleteConnection",
    "glue:UpdateConnection",
    "glue:Get*",
    "glue:BatchDeleteConnection",
    "glue:StartCrawlerSchedule",
    "glue:StartJobRun",
    "glue:CreateWorkflow",
    "glue:*DataQuality*",
    "glue:List*",
    "glue:CreateSession",
    "glue:RunStatement",
    "glue:BatchCreatePartition",
    "glue:CreateDatabase",
    "glue:CreatePartitionIndex",
    "glue:CreateTable",
    "glue:BatchUpdatePartition",
    "glue:BatchDeletePartition",
    "glue:UpdateTable",
    "glue:DeleteTableVersion",
    "glue:DeleteTable",
    "glue:DeleteColumnStatisticsForPartition",
    "glue:DeleteColumnStatisticsForTable",
    "glue:DeletePartitionIndex",
    "glue:UpdateColumnStatisticsForPartition",
    "glue:UpdateColumnStatisticsForTable",
    "glue:BatchDeleteTableVersion",
    "glue:BatchDeleteTable",
```

```
    "glue:CreatePartition",
    "glue:DeletePartition",
    "glue:UpdatePartition",
    "glue:CreateBlueprint",
    "glue:CreateJob",
    "glue:CreateConnection",
    "glue:CreateCrawler",
    "groundtruthlabeling:*",
    "iam:CreateServiceLinkedRole",
    "iam:GetRole",
    "iam:ListRoles",
    "iam:PassRole",
    "kms:DescribeKey",
    "kms:ListAliases",
    "kms:Decrypt",
    "kms:ListKeys",
    "kms:Encrypt",
    "kms:GenerateDataKey",
    "kms:RetireGrant",
    "lakeformation:GetDataAccess",
    "lambda:ListFunctions",
    "lambda:InvokeFunction",
    "logs:CreateLogDelivery",
    "logs:CreateLogGroup",
    "logs:CreateLogStream",
    "logs:DeleteLogDelivery",
    "logs:Describe*",
    "logs:GetLogDelivery",
    "logs:GetLogEvents",
    "logs:ListLogDeliveries",
    "logs:PutLogEvents",
    "logs:UpdateLogDelivery",
    "ram:AcceptResourceShareInvitation",
    "rds:DescribeDBInstances",
    "redshift:CreateClusterUser",
    "redshift:GetClusterCredentials",
    "redshift:GetClusterCredentialsWithIAM",
    "redshift:DescribeClusters",
    "redshift-data:BatchExecuteStatement",
    "redshift-data:CancelStatement",
    "redshift-data:DescribeStatement",
    "redshift-data:DescribeTable",
    "redshift-data:ExecuteStatement",
    "redshift-data:GetStatementResult",
```

```
    "redshift-data:ListSchemas",
    "redshift-data:ListTables",
    "redshift-serverless:ListNamespaces",
    "redshift-serverless:ListWorkgroups",
    "redshift-serverless:GetNamespace",
    "redshift-serverless:GetWorkgroup",
    "redshift-serverless:GetCredentials",
    "s3:GetBucketAcl",
    "s3:PutObjectAcl",
    "s3:GetObject",
    "s3:PutObject",
    "s3:DeleteObject",
    "s3:AbortMultipartUpload",
    "s3:CreateBucket",
    "s3:GetBucketLocation",
    "s3:ListBucket",
    "s3:ListAllMyBuckets",
    "s3:GetBucketCors",
    "s3:PutBucketCors",
    "s3:DeleteObjectVersion",
    "s3:PutObjectRetention",
    "s3:ReplicateObject",
    "s3:RestoreObject",
    "secretsmanager:ListSecrets",
    "secretsmanager:DescribeSecret",
    "secretsmanager:GetSecretValue",
    "secretsmanager:CreateSecret",
    "secretsmanager:PutResourcePolicy",
    "secretsmanager:TagResource",
    "servicecatalog:Describe*",
    "servicecatalog:List*",
    "servicecatalog:ScanProvisionedProducts",
    "servicecatalog:SearchProducts",
    "servicecatalog:SearchProvisionedProducts",
    "servicecatalog:ProvisionProduct",
    "servicecatalog:TerminateProvisionedProduct",
    "servicecatalog:UpdateProvisionedProduct",
    "sns:ListTopics",
    "sns:Subscribe",
    "sns:CreateTopic",
    "sns:Publish",
    "states:DescribeExecution",
    "states:GetExecutionHistory",
    "states:StartExecution",
```

```
    "states:StopExecution",
    "states:UpdateStateMachine",
    "tag:GetResources",
    "sso:CreateApplicationAssignment",
    "sso:AssociateProfile"
   ],
   "Resource": "*"
  }
 ]
}
```

DataZone Aggiornamenti Amazon alle politiche AWS gestite

Visualizza i dettagli sugli aggiornamenti delle politiche AWS gestite per Amazon DataZone da quando questo servizio ha iniziato a tracciare queste modifiche. Per ricevere avvisi automatici sulle modifiche a questa pagina, iscriviti al feed RSS nella pagina della cronologia di Amazon DataZone Document.

Modifica	Descrizione	Data
AmazonDataZoneSageMakerEnvironmentRolePermissionsBoundary - nuovo limite di autorizzazioni	Nuovo limite di autorizzazioni chiamato. AmazonDataZoneSageMakerEnvironmentRolePermissionsBoundary Quando crei un SageMaker ambiente Amazon tramite il portale DataZone dati Amazon, Amazon DataZone applica questo limite di autorizzazioni ai ruoli IAM prodotti durante la creazione dell'ambiente. Il limite delle autorizzazioni limita l'ambito dei ruoli DataZone creati da Amazon e degli eventuali ruoli aggiunti.	30 aprile 2024
AmazonDataZoneSageMakerAccess - nuova politica	La nuova policy denominata AmazonDataZoneSage	30 aprile 2024

Modifica	Descrizione	Data
	MakerAccessconcede ad Amazon DataZone le autorizzazioni per pubblicare SageMaker risorse Amazon nel catalogo. Fornisce inoltre ad Amazon DataZone le autorizzazioni per concedere l'accesso o revocare l'accesso alle risorse SageMaker pubblicate da Amazon nel catalogo.	
AmazonDataZoneFullAccess - aggiornamento della politica	Un aggiornamento della AmazonDataZoneFull Accesspolitica che aggiunge l'accesso all'`DescribeSecurityGroups` azione per migliorare l'usabilità per gli amministratori degli account, configurando i blueprint nella console e `GetPolicy` un'azione per aiutare a recuperare informazioni sulla politica gestita specificata.	30 aprile 2024
AmazonDataZoneSageMakerProvisioning - nuova politica	Una nuova politica denominata AmazonDataZoneSageMakerProvisioningconcede ad Amazon DataZone le autorizzazioni necessarie per interagire con Amazon. SageMaker	30 aprile 2024

Modifica	Descrizione	Data
AmazonDataZone<region><domainId>S3Manage- - - nuovo ruolo	Nuovo ruolo chiamato AmazonDataZoneS3Manage-<region>, <domainId>utilizzato quando Amazon DataZone chiama AWS Lake Formation per registrare una sede Amazon Simple Storage Service (Amazon S3). AWS Lake Formation assume questo ruolo quando accede ai dati in quella posizione.	1 aprile 2024
AmazonDataZoneGlue ManageAccessRolePolicy - Aggiornamento della politica	È stato aggiornato il AmazonDataZoneGlue ManageAccessRolePolicysupporto per le autorizzazioni che consentono DataZone ad Amazon di abilitare la pubblicazione e le concessioni di accesso ai dati.	1 aprile 2024
AmazonDataZoneDomainExecutionRolePolicy e AmazonDataZoneFullUserAccess - Aggiornamento della politica	Aggiornato AmazonDataZoneDomainExecutionRolePolicye AmazonDataZoneFullUserAccessper abilitare il supporto per l'`CancelMetadataGenerationRun` API.	29 marzo 2024

Modifica	Descrizione	Data
AmazonDataZoneFullAccess - Aggiornamento della politica	È stato aggiornato `AmazonDataZoneFullAccess` per consentire agli utenti di scegliere i propri segreti, cluster, vpc e sottoreti nella console di DataZone gestione di Amazon anziché digitarli in una casella di testo.	13 marzo 2024
AmazonDataZoneDomainExecutionRolePolicy - Aggiornamento della politica	Aggiornato AmazonDataZoneDomainExecutionRolePolicyper abilitare il supporto per l'`ListEnvironmentBlueprintConfigurationSummaries` API necessaria per la creazione di profili di ambiente identificando quali blueprint sono abilitati in quale account e regione.	01 febbraio 2024
AmazonDataZoneGlueManageAccessRolePolicy - Aggiornamento della politica	Aggiornato il AmazonDataZoneGlueManageAccessRolePolicyper abilitare il supporto per la modalità ibrida AWS Lake Formation.	14 dicembre 2023

Modifica	Descrizione	Data
AmazonDataZoneFull UserAccess e AmazonDat aZoneDomainExecuti onRolePolicy - Aggiornamenti delle politiche	Sono state aggiornate le politiche AmazonDat aZoneFullUserAccesse le AmazonDataZoneDoma inExecutionRolePolicypolitiche per supportare la funzional ità generativa di descrizio ne dei dati basata sull'inte lligenza artificiale in Amazon. DataZone	28 novembre 2023
AmazonDataZoneEnvi ronmentRolePermiss ionsBoundary - Aggiornam ento della politica	Amazon DataZone ha apportato un aggiornam ento alla politica AmazonDat aZoneEnvironmentRo lePermissionsBoundarygestita che consiste in un'`athena:Ge tQueryResultsStrea m` autorizzazione aggiuntiva relativa alla `ResourceTag` condizione.	17 novembre 2023
AmazonDataZoneReds hiftManageAccessRolePolicy - Aggiornamento della politica	Amazon DataZone ha aggiornato il AmazonDat aZoneRedshiftManag eAccessRolePolicyfile rimuovendo l'ID dell'orga nizzazione di controllo per l'`redshift: AssociateDataShare Consumer` azione. Ciò consente di condividere le risorse tra AWS le organizza zioni.	16 novembre 2023

Modifica	Descrizione	Data
AmazonDataZoneFull UserAccess - Aggiornamento della politica	Amazon DataZone ha aggiornato la AmazonDat aZoneFullUserAccesspolitica che garantisce l'accesso completo ad Amazon DataZone, ma non consente la gestione di domini, utenti o account associati.	02 ottobre 2023
AmazonDataZonePort alFullAccessPolicy - politica obsoleta	Amazon ha DataZone reso obsoleto il. AmazonDat aZonePortalFullAccessPolicy	29 settembre 2023
AmazonDataZonePrev iewConsoleFullAccess - politica obsoleta	Amazon ha DataZone reso obsoleto il. AmazonDat aZonePreviewConsol eFullAccess	29 settembre 2023

Modifica	Descrizione	Data
AmazonDataZoneDomainExecutionRolePolicy - Nuova politica	Amazon DataZone ha aggiunto una nuova politica chiamata AmazonDataZoneDomainExecutionRolePolicy. Questa è la politica predefinita per il ruolo DataZone `AmazonDataZoneDomainExecutionRole` di servizio Amazon. Questo ruolo viene utilizzato da Amazon DataZone per catalogare, scoprire, gestire, condividere e analizzare i dati nel DataZone dominio Amazon. Puoi allegare la `AmazonDataZoneDomainExecutionRolePolicy` politica al tuo`AmazonDataZoneDomainExecutionRole` .	25 settembre 2023
AmazonDataZoneCrossAccountAdmin - Nuova politica	Amazon DataZone ha aggiunto una nuova politica chiamata AmazonDataZoneCrossAccountAdminche consente agli utenti di lavorare con Amazon DataZone e gli account associati.	19 settembre 2023

Modifica	Descrizione	Data
AmazonDataZoneFull UserAccess - Nuova politica	Amazon DataZone ha aggiunto una nuova politica chiamata AmazonDat aZoneFullUserAccessche garantisce l'accesso completo ad Amazon DataZone, ma non consente la gestione di domini, utenti o account associati.	12 settembre 2023
AmazonDataZoneReds hiftManageAccessRolePolicy - Nuova politica	Amazon DataZone ha aggiunto una nuova politica chiamata AmazonDat aZoneRedshiftManag eAccessRolePolicyche concede autorizzazioni per consentire ad Amazon di DataZone abilitare la pubblicazione e le concessioni di accesso ai dati.	12 settembre 2023
AmazonDataZoneGlue ManageAccessRolePolicy - Nuova politica	Amazon DataZone ha aggiunto una nuova politica chiamata AmazonDat aZoneGlueManageAcc essRolePolicyche concede ad Amazon DataZone le autorizzazioni per pubblicare i dati di AWS Glue nel catalogo. Fornisce inoltre ad Amazon DataZone le autorizzazioni per concedere l'accesso o revocare l'accesso alle risorse pubblicate da AWS Glue nel catalogo.	12 settembre 2023

Modifica	Descrizione	Data
AmazonDataZoneRedshiftGlueProvisioningPolicy - Nuova politica	Amazon DataZone ha aggiunto una nuova politica chiamata AmazonDataZoneRedshiftGlueProvisioningPolicyche concede ad Amazon DataZone le autorizzazioni necessarie per interagire con le fonti di dati supportate.	12 settembre 2023
AmazonDataZoneEnvironmentRolePermissionsBoundary - Nuova politica	Amazon DataZone ha aggiunto una nuova policy denominata AmazonDataZoneEnvironmentRolePermissionsBoundaryche limita il principale IAM fornito a cui è collegata.	12 settembre 2023
AmazonDataZoneFullAccess - Nuova politica	Amazon DataZone ha aggiunto una nuova politica chiamata AmazonDataZoneFullAccessche fornisce l'accesso completo ad Amazon DataZone tramite la console di AWS gestione.	12 settembre 2023
Aggiornamento della policy gestita	Aggiornamenti alla politica AmazonDataZonePreviewConsoleFullAccessgestita che consiste in `iam:GetPolicy` autorizzazioni aggiuntive.	13 giugno 2023

Modifica	Descrizione	Data
Amazon DataZone ha iniziato a tracciare le modifiche	Amazon DataZone ha iniziato a tracciare le modifiche alle sue politiche AWS gestite.	20 marzo 2023

Ruoli IAM per Amazon DataZone

Argomenti

- AmazonDataZoneProvisioningRole-<domainAccountId>
- AmazonDataZoneDomainExecutionRole
- AmazonDataZoneGlueAccess- <region>- <domainId>
- AmazonDataZoneRedshiftAccess- <region>- <domainId>
- AmazonDataZone<region>Gestione S3- - <domainId>
- AmazonDataZoneSageMakerManageAccessRole<region>- - <domainId>
- AmazonDataZoneSageMakerProvisioningRole-<domainAccountId>

AmazonDataZoneProvisioningRole-<domainAccountId>

`AmazonDataZoneProvisioningRole-<domainAccountId>`Ha l'`AmazonDataZoneRedshiftGlueProvisioningPolicy`allegato. Questo ruolo concede ad Amazon DataZone le autorizzazioni necessarie per interagire con AWS Glue e Amazon Redshift.

L'impostazione predefinita prevede la seguente politica di `AmazonDataZoneProvisioningRole-<domainAccountId>` attendibilità allegata:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "datazone.amazonaws.com"
      },
      "Action": "sts:AssumeRole",
      "Condition": {
```

```
        "StringEquals": {
            "aws:SourceAccount": "{{domain_account}}"
        }
      }
    }
  ]
}
```

AmazonDataZoneDomainExecutionRole

AmazonDataZoneDomainExecutionRoleHa la politica AWS gestita AmazonDataZoneDomainExecutionRolePolicyallegata. Amazon DataZone crea questo ruolo per te per tuo conto. Per determinate azioni nel portale dati, Amazon DataZone assume questo ruolo nell'account in cui viene creato il ruolo e verifica che questo ruolo sia autorizzato a eseguire l'azione.

Il AmazonDataZoneDomainExecutionRoleruolo è obbligatorio nell'area Account AWS che ospita il tuo DataZone dominio Amazon. Questo ruolo viene creato automaticamente per te quando crei il tuo DataZone dominio Amazon.

Il AmazonDataZoneDomainExecutionRoleruolo predefinito ha la seguente politica di fiducia.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "Service": "datazone.amazonaws.com"
            },
            "Action": [
                "sts:AssumeRole",
                "sts:TagSession"
            ],
            "Condition": {
                "StringEquals": {
                    "aws:SourceAccount": "{{source_account_id}}"
                },
                "ForAllValues:StringLike": {
                    "aws:TagKeys": [
                        "datazone*"
```

```
                    ]
                }
            }
        }
    ]
}
```

AmazonDataZoneGlueAccess- <region>- <domainId>

Il `AmazonDataZoneGlueAccess-<region>-<domainId>` ruolo ha l'`AmazonDataZoneGlueManageAccessRolePolicy`allegato. Questo ruolo concede ad Amazon DataZone le autorizzazioni per pubblicare i dati di AWS Glue nel catalogo. Fornisce inoltre ad Amazon DataZone le autorizzazioni per concedere l'accesso o revocare l'accesso alle risorse pubblicate da AWS Glue nel catalogo.

Al `AmazonDataZoneGlueAccess-<region>-<domainId>` ruolo predefinito è allegata la seguente politica di attendibilità:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "datazone.amazonaws.com"
      },
      "Action": "sts:AssumeRole",
      "Condition": {
            "StringEquals": {
                "aws:SourceAccount": "{{domain_account}}"
            },
            "ArnEquals": {
                "aws:SourceArn": "arn:aws:datazone:{{region}}:
{{domain_account}}:domain/{{root_domain_id}}"
            }
        }
    }
  ]
}
```

AmazonDataZoneRedshiftAccess- <region>- <domainId>

Il `AmazonDataZoneRedshiftAccess-<region>-<domainId>` ruolo ha l'`AmazonDataZoneRedshiftManageAccessRolePolicy`allegato. Questo ruolo concede ad Amazon DataZone le autorizzazioni per pubblicare i dati di Amazon Redshift nel catalogo. Fornisce inoltre ad Amazon DataZone le autorizzazioni per concedere o revocare l'accesso agli asset pubblicati di Amazon Redshift o Amazon Redshift Serverless nel catalogo.

Al `AmazonDataZoneRedshiftAccess-<region>-<domainId>` ruolo predefinito è allegata la seguente politica di autorizzazioni in linea:

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Sid": "RedshiftSecretStatement",
         "Effect":"Allow",
         "Action":"secretsmanager:GetSecretValue",
         "Resource":"*",
         "Condition":{
            "StringEquals":{
               "secretsmanager:ResourceTag/AmazonDataZoneDomain":"{{domainId}}"
            }
         }
      }
   ]
}
```

L'impostazione predefinita `AmazonDataZoneRedshiftManageAccessRole<timestamp>` prevede la seguente politica di attendibilità allegata:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "datazone.amazonaws.com"
```

```
      },
      "Action": "sts:AssumeRole",
      "Condition": {
            "StringEquals": {
                "aws:SourceAccount": "{{domain_account}}"
            },
            "ArnEquals": {
                "aws:SourceArn": "arn:aws:datazone:{{region}}:
{{domain_account}}:domain/{{root_domain_id}}"
            }
        }
    }
  ]
}
```

AmazonDataZone<region>Gestione S3- - <domainId>

AmazonDataZoneS3Manage- <region>- <domainId>viene utilizzato quando Amazon DataZone chiama AWS Lake Formation per registrare una sede Amazon Simple Storage Service (Amazon S3). AWS Lake Formation assume questo ruolo quando accede ai dati in quella posizione. Per ulteriori informazioni, consulta Requisiti per i ruoli utilizzati per registrare le sedi.

A questo ruolo è allegata la seguente politica di autorizzazioni in linea.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "LakeFormationDataAccessPermissionsForS3",
            "Effect": "Allow",
            "Action": [
                "s3:PutObject",
                "s3:GetObject",
                "s3:DeleteObject"
            ],
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "aws:ResourceAccount": "{{accountId}}"
                }
            }
```

```
        },
        {
            "Sid": "LakeFormationDataAccessPermissionsForS3ListBucket",
            "Effect": "Allow",
            "Action": [
                "s3:ListBucket"
            ],
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "aws:ResourceAccount": "{{accountId}}"
                }
            }
        },
        {
            "Sid": "LakeFormationDataAccessPermissionsForS3ListAllMyBuckets",
            "Effect": "Allow",
            "Action": [
                "s3:ListAllMyBuckets"
            ],
            "Resource": "arn:aws:s3:::*",
            "Condition": {
                "StringEquals": {
                    "aws:ResourceAccount": "{{accountId}}"
                }
            }
        },
        {
            "Sid": "LakeFormationExplicitDenyPermissionsForS3",
            "Effect": "Deny",
            "Action": [
                "s3:PutObject",
                "s3:GetObject",
                "s3:DeleteObject"
            ],
            "Resource": [
                "arn:aws:s3:::[[BucketNames]]/*"
            ],
            "Condition": {
                "StringEquals": {
                    "aws:ResourceAccount": "{{accountId}}"
                }
            }
        },
```

```
        {
            "Sid": "LakeFormationExplicitDenyPermissionsForS3ListBucket",
            "Effect": "Deny",
            "Action": [
                "s3:ListBucket"
            ],
            "Resource": [
                "arn:aws:s3:::[[BucketNames]]"
            ],
            "Condition": {
                "StringEquals": {
                    "aws:ResourceAccount": "{{accountId}}"
                }
            }
        }
    ]
}
```

A AmazonDataZone S3Manage- <region>- <domainId>è allegata la seguente politica di fiducia:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "TrustLakeFormationForDataLocationRegistration",
            "Effect": "Allow",
            "Principal": {
                "Service": "lakeformation.amazonaws.com"
            },
            "Action": "sts:AssumeRole",
            "Condition": {
                "StringEquals": {
                    "aws:SourceAccount": "{{source_account_id}}"
                }
            }
        }
    ]
}
```

AmazonDataZoneSageMakerManageAccessRole<region>- - <domainId>

Il `AmazonDataZoneSageMakerManageAccessRole` ruolo ha il `AmazonDataZoneSageMakerAccessAmazonDataZoneRedshiftManageAccessRolePolicy`, il e l'`AmazonDataZoneGlueManageAccessRolePolicy`allegato. Questo ruolo concede ad Amazon DataZone le autorizzazioni per pubblicare e gestire abbonamenti per data lake, data warehouse e asset Amazon Sagemaker.

Al `AmazonDataZoneSageMakerManageAccessRole` ruolo è allegata la seguente politica in linea:

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Sid": "RedshiftSecretStatement",
         "Effect":"Allow",
         "Action":"secretsmanager:GetSecretValue",
         "Resource":"*",
         "Condition":{
            "StringEquals":{
               "secretsmanager:ResourceTag/AmazonDataZoneDomain":"{{domainId}}"
            }
         }
      }
   ]
}
```

Al `AmazonDataZoneSageMakerManageAccessRole` ruolo è allegata la seguente politica di fiducia:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "DatazoneTrustPolicyStatement",
      "Effect": "Allow",
      "Principal": {
        "Service":  ["datazone.amazonaws.com",
                    "sagemaker.amazonaws.com"]
```

```
      },
      "Action": "sts:AssumeRole",
      "Condition": {
            "StringEquals": {
                "aws:SourceAccount": "{{domain_account}}"
            },
            "ArnEquals": {
                "aws:SourceArn": "arn:aws:datazone:{{region}}:
{{domain_account}}:domain/{{root_domain_id}}"
            }
        }
    }
]
}
```

AmazonDataZoneSageMakerProvisioningRole-<domainAccountId>

Al `AmazonDataZoneSageMakerProvisioningRole` ruolo è `AmazonDataZoneRedshiftGlueProvisioningPolicy` associata la `AmazonDataZoneSageMakerProvisioning` e la. Questo ruolo concede ad Amazon DataZone le autorizzazioni necessarie per interagire con AWS Glue, Amazon Redshift e Amazon Sagemaker.

Al `AmazonDataZoneSageMakerProvisioningRole` ruolo è allegata la seguente politica in linea:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "SageMakerStudioTagOnCreate",
            "Effect": "Allow",
            "Action": [
                "sagemaker:AddTags"
            ],
            "Resource": "arn:aws:sagemaker:*:{{AccountId}}:*/*",
            "Condition": {
                "Null": {
                    "sagemaker:TaggingAction": "false"
                }
            }
        }
    ]
```

```
}
```

Al `AmazonDataZoneSageMakerProvisioningRole` ruolo è allegata la seguente politica di fiducia:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "DataZoneTrustPolicyStatement",
      "Effect": "Allow",
      "Principal": {
        "Service": "datazone.amazonaws.com"
      },
      "Action": "sts:AssumeRole",
      "Condition": {
        "StringEquals": {
            "aws:SourceAccount": "{{domain_account}}"
        }
      }
    }
  ]
}
```

Ruoli basati sull'identità

Le policy basate su identità sono documenti di policy di autorizzazione JSON che è possibile allegare a un'identità (utente, gruppo di utenti o ruoli IAM). Tali policy definiscono le azioni che utenti e ruoli possono eseguire, su quali risorse e in quali condizioni. Per informazioni su come creare una policy basata su identità, consulta Creazione di policy IAM nella Guida per l'utente di IAM.

Con le policy basate su identità di IAM, è possibile specificare quali operazioni e risorse sono consentite o respinte, nonché le condizioni in base alle quali le operazioni sono consentite o respinte. Non è possibile specificare l'entità principale in una policy basata sull'identità perché si applica all'utente o al ruolo a cui è associato. Per informazioni su tutti gli elementi utilizzabili in una policy JSON, consulta Guida di riferimento agli elementi delle policy JSON IAM nella Guida per l'utente di IAM.

Quando crei un DataZone progetto Amazon, nel portale, vengono creati tre ruoli IAM per questo progetto, uno per ogni tipo di ruolo membro del progetto: proprietario e collaboratore. Le autorizzazioni associate a ciascun ruolo riguardano il ruolo del progetto e le politiche di autorizzazione associate dipendono dalle funzionalità con cui viene distribuito il progetto.

Per consentire DataZone ad Amazon di gestire le autorizzazioni e condividere le risorse con i progetti sottoscrittori, i ruoli utente del progetto sottoscrittore vengono aggiunti automaticamente come amministratore del data lake AWS Lake Formation nelle risorse di Account AWS pubblicazione.

Puoi visualizzare la maggior parte delle up-to-date versioni del ruolo nella console di gestione AWS IAM o esaminare le diverse autorizzazioni del ruolo nella tabella seguente.

Autorizzazioni del proprietario del progetto

Tipo di ambiente	Autorizzazioni IAM
Data Lake predefinito	Questa è la combinazione delle funzionalità Essential, Data Lake Producer e Data Lake Consumer.
Essential	{ "Version": "2012-10-17", "Statement": [{ "Effect": "Allow", "Action": ["s3:List*", "s3:Get*", "s3:Describe*", "s3:DeleteObjectVersion", "s3:RestoreObject", "s3:ReplicateObject", "s3:PutObject", "s3:AbortMultipartUpload",

Tipo di ambiente	Autorizzazioni IAM	

```
        "s3:PutOb
jectRetention",
        "s3:Delet
eObject"
      ],
      "Resource":
 ["s3BucketArn",
 "s3BucketArn/*"]
    },
    { "Action":
 ["s3:List*"],
 "Resource": "*",
 "Effect": "Allow" },
    {
      "Action": [
        "kms:List*",
        "kms:Get*",
        "kms:Desc
ribe*",
        "kms:Decrypt",
        "kms:Encrypt",
        "kms:ReEn
crypt*",
        "kms:Verify",
        "kms:Sign",
        "kms:Gene
rateDataKey"
      ],
      "Resource":
 "keyArn",
      "Effect": "Allow"
    },
    {
      "Action":
 ["kms:ListKeys",
 "kms:ListAliases"],
      "Resource": "*",
      "Effect": "Allow"
    },
    {
      "Action": [
```

Tipo di ambiente	Autorizzazioni IAM	

```
        "ec2:Desc
ribeSecurityGroups",
        "ec2:Desc
ribeSecurityGroupR
ules",
        "ec2:Desc
ribeTags"
      ],
      "Resource": "*",
      "Effect": "Allow"
    },
    {
      "Action": [
        "logs:Des
cribe*",
        "logs:Sta
rtQuery",
        "logs:Sto
pQuery",
        "logs:Get*",
        "logs:List*",
        "logs:Put
LogEvents",
        "logs:Cre
ateLogStream",
        "logs:Fil
terLogEvents"
      ],
      "Resource":
 "arn:aws:logs:regi
on:account-id:log-
group:log-group-na
me:*",
      "Effect": "Allow"
    },
    {
      "Effect": "Allow",
      "Action": [
        "s3:Get*",
        "s3:List*",
        "kms:List*",
        "kms:Get*",
```

Tipo di ambiente	Autorizzazioni IAM	

```
        "kms:Desc
ribe*",
        "kms:Decrypt"
      ],
      "Resource": "*",
      "Condition": {
        "StringNo
tEquals": {
          "aws:Reso
urceAccount":
 "project-account-id"
        }
      }
    }
  ]
}
```

Tipo di ambiente	Autorizzazioni IAM	
Produttore di Data Lake	{ "Version": "2012-10-17", "Statement": [{ "Effect": "Allow", "Action": ["glue:BatchGet*", "glue:Get*", "glue:SearchTables", "glue:List*", "glue:BatchCreateP artition", "glue:CreatePartit ionIndex", "glue:CreateTable", "glue:BatchUpdateP artition", "glue:BatchDeleteP artition", "glue:UpdateTable", "glue:DeleteTableV ersion", "glue:DeleteTable", "glue:DeleteColumn	

Tipo di ambiente	Autorizzazioni IAM	

```
StatisticsForParti
tion",

 "glue:DeleteColumn
StatisticsForTable",

 "glue:DeletePartit
ionIndex",

 "glue:UpdateColumn
StatisticsForParti
tion",

 "glue:UpdateColumn
StatisticsForTable",

 "glue:BatchDeleteT
ableVersion",

 "glue:BatchDeleteT
able",

 "glue:CreatePartit
ion",

 "glue:DeletePartit
ion",

 "glue:UpdatePartit
ion"
            ],
            "Resource":
 [

 "arn:aws:glue:regi
on:account:database/
dbName",

 "arn:aws:glue:regi
on:account:catalog",

 "arn:aws:glue:regi
```

Tipo di ambiente	Autorizzazioni IAM	

```
on:account:table/d
bName/*"
            ]
        },
        {
            "Sid":
 "VisualEditor0",
            "Effect":
 "Allow",
            "Action": [

 "glue:SearchTables",

 "glue:NotifyEvent",

 "glue:StartBluepri
ntRun",

 "glue:PutWorkflowR
unProperties",

 "glue:StopCrawler",

 "glue:DeleteJob",

 "glue:DeleteWorkfl
ow",

 "glue:UpdateCrawler",

 "glue:DeleteBluepr
int",

 "glue:UpdateWorkfl
ow",

 "glue:StartCrawler",

 "glue:ResetJobBook
mark",

 "glue:UpdateJob",
```

Tipo di ambiente	Autorizzazioni IAM	

```
 "glue:StartWorkflo
wRun",

 "glue:StopCrawlerS
chedule",

 "glue:ResumeWorkfl
owRun",

 "glue:List*",

 "glue:DeleteCrawler",

 "glue:UpdateBluepr
int",

 "glue:BatchStopJob
Run",

 "glue:StopWorkflow
Run",

 "glue:BatchGet*",

 "glue:UpdateCrawle
rSchedule",

 "glue:DeleteConnec
tion",

 "glue:UpdateConnec
tion",

 "glue:Get*",

 "glue:BatchDeleteC
onnection",

 "glue:StartCrawler
Schedule",
```

Tipo di ambiente	Autorizzazioni IAM	

```
 "glue:StartJobRun",

 "glue:CreateWorkfl
ow",

 "glue:PublishDataQ
uality",

 "glue:*DataQuality*"
           ],
           "Resource":
 "*",
           "Conditio
n": {

 "ForAnyValue:Strin
gEquals": {

 "aws:ResourceTag/n
oah-analytics:proj
ectId": "projectId"
               }
           }
       },
       {
           "Sid":
 "CreateGlueResourc
es",
           "Effect":
 "Allow",
           "Action": [

 "glue:CreateBluepr
int",

 "glue:CreateJob",

 "glue:CreateConnec
tion",

 "glue:CreateCrawler",
```

Tipo di ambiente	Autorizzazioni IAM	

```
 "glue:CreateDataQu
alityRuleset"
            ],
            "Resource":
 "*"
        },
        {
            "Sid":
 "VisualEditor0",
            "Effect":
 "Allow",
            "Action": [

 "iam:ListRoles",

 "iam:ListUsers",

 "iam:ListGroups",

 "iam:ListRolePolic
ies",

 "iam:GetRole",

 "iam:GetRolePolicy"
            ],
            "Resource":
 "*"
        }
    ]
}
```

Tipo di ambiente	Autorizzazioni IAM

Consumatore di Data Lake	{
	  "Version": "2012-10-17",
	  "Statement": [
	  {
	  "Effect": "Allow",
	  "Action": [
	  "athena:TerminateSession",
	  "athena:CreatePreparedStatement",
	  "athena:StopCalculationExecution",
	  "athena:StartQueryExecution",
	  "athena:UpdatePreparedStatement",
	  "athena:BatchGet*",
	  "athena:UpdateNotebook",
	  "athena:DeleteNotebook",
	  "athena:DeletePreparedStatement",
	  "athena:UpdateNotebookMetadata",
	  "athena:DeleteNamedQuery",
	  "athena:Get*",
	  "athena:UpdateNamedQuery",
	  "athena:CreateNamedQuery",

Tipo di ambiente	Autorizzazioni IAM	

```
        "athena:E
xportNotebook",
        "athena:S
topQueryExecution",
        "athena:S
tartCalculationExe
cution",
        "athena:S
tartSession",
        "athena:C
reatePresignedNote
bookUrl",
        "athena:C
reateNotebook",
        "athena:I
mportNotebook"
      ],
      "Resource": [
        "arn:aws:
athena:region:acco
unt-id:workgroup/w
orkGroupName",
        "arn:aws:
athena:region:acco
unt-id:datacatalog/
AwsDataCatalog"
      ]
    },
    {
      "Effect": "Allow",
      "Action": [
        "athena:L
istWorkGroups",
        "athena:L
istDataCatalogs",
        "athena:List*"
      ],
      "Resource": ["*"]
    },
    {
      "Effect": "Allow",
      "Action": [
```

Tipo di ambiente	Autorizzazioni IAM	

```
        "glue:Bat
chGet*",
        "glue:Get*",
        "glue:Sea
rchTables",
        "glue:List*"
      ],
      "Resource": [
        "arn:aws:
glue:region:account-
id:database/dbName",
        "arn:aws:
glue:region:account-
id:catalog",
        "arn:aws:
glue:region:account-
id:table/dbName/*"
      ]
    }
  ]
}
```

Tipo di ambiente	Autorizzazioni IAM	

Produttore di Data Warehouse	{
	"Version": "2012-10-17",
	"Statement": [
	{
	"Effect": "Allow",
	"Action": [
	"redshift:GetClusterCredentials",
	"redshift:JoinGroup",
	"redshift:CreateClusterUser",
	"redshift:DescribeClusters"
	],
	"Resource": "arn:aws:redshift:region:account:cluster:producerRedshiftCluster"
	},
	{
	"Effect": "Allow",
	"Action": [
	"redshift-data:DescribeStatement",
	"redshift-data:ExecuteStatement"
	],
	"Resource": "arn:aws:redshift:region:account:cluster:producerRedshiftCluster"
	}
	]
	}	

Tipo di ambiente	Autorizzazioni IAM	

Tipo di ambiente	Autorizzazioni IAM

Consumatore di data warehouse	{
	  "Version": "2012-10-17",
	  "Statement": [
	  {
	  "Effect": "Allow",
	  "Action": [
	  "redshift:GetClusterCredentials",
	  "redshift:JoinGroup",
	  "redshift:CreateClusterUser",
	  "redshift:DescribeClusters"
	  ],
	  "Resource": [
	  "arn:aws:redshift:region:account:dbuser:cluster-identifier/dbUser",
	  "arn:aws:redshift:region:account:dbgroup:cluster-identifier/project_owner@projectName",
	  "arn:aws:redshift:region:account:dbname:cluster-identifier/*"
	  ],
	  "Condition": {
	  "ForAnyValue:StringEquals": {
	  "aws:PrincipalTag/RedshiftDbUser": "dbUser"
	  }

Tipo di ambiente	Autorizzazioni IAM	

```
      }
    },
    {
      "Sid": "VisualEd
itor2",
      "Effect": "Allow",
      "Action": [
        "redshift-
data:DescribeStat
ement",
        "redshift-
data:ExecuteStatement"
      ],
      "Resource":
 "arn:aws:redshift:
region:account-id:
cluster:cluster-id
entifier"
    }
  ]
}
```

Tipo di ambiente	Autorizzazioni IAM

Editor di query v2 di Amazon Redshift	{
	  "Version": "2012-10-17",
	  "Statement": [
	    {
	      "Action": "redshift:DescribeClusters",
	      "Effect": "Allow",
	      "Resource": "arn:aws:redshift:region:account-id:cluster:*",
	      "Sid": "RedshiftPermissions"
	    },
	    {
	      "Action": "tag:GetResources",
	      "Condition": {
	        "StringEquals": { "aws:CalledViaLast": "sqlworkbench.amazonaws.com" }
	      },
	      "Effect": "Allow",
	      "Resource": "*",
	      "Sid": "ResourceGroupsTaggingPermissions"
	    },
	    {
	      "Action": [
	        "sqlworkbench:DriverExecute",
	        "sqlworkbench:GenerateSession",

Tipo di ambiente	Autorizzazioni IAM	

```
        "sqlworkb
ench:ListConnectio
ns",
        "sqlworkb
ench:ListDatabases",
        "sqlworkb
ench:ListFiles",
        "sqlworkb
ench:ListNotebooks",
        "sqlworkb
ench:ListQueryExec
utionHistory",
        "sqlworkb
ench:ListRedshiftC
lusters",
        "sqlworkb
ench:ListSampleDat
abases",
        "sqlworkb
ench:ListTabs",
        "sqlworkb
ench:ListTaggedRes
ources"
      ],
      "Effect": "Allow",
      "Resource": "*",
      "Sid": "AmazonRe
dshiftQueryEditorV
2PermissionsPart1"
    },
    {
      "Action":
 "sqlworkbench:*",
      "Effect": "Allow",
      "Resource": [
        "arn:aws:
sqlworkbench:regio
n:account-id:query/
*",
        "arn:aws:
sqlworkbench:regio
```

Tipo di ambiente	Autorizzazioni IAM
	n:account-id:noteb ook/*", "arn:aws: sqlworkbench:regio n:account-id:conne ction/*", "arn:aws: sqlworkbench:regio n:account-id:chart/ *", "arn:aws: sqlworkbench:regio n:account-id:/*"], "Sid": "AmazonRe dshiftQueryEditorV 2PermissionsPart2" }] }

Autorizzazioni per i collaboratori del progetto

Tipo di ambiente	Autorizzazioni IAM
Data Lake predefinito	Questa è la combinazione delle funzionalità Essential, Data Lake Producer e Data Lake Consumer.
Essential	{ "Version": "2012-10- 17", "Statement": [{ "Effect": "Allow",

Tipo di ambiente	Autorizzazioni IAM	

```
      "Action": [
        "s3:List*",
        "s3:Get*",
        "s3:Describe*",
        "s3:Delet
eObjectVersion",
        "s3:Resto
reObject",
        "s3:Repli
cateObject",
        "s3:PutObject",
        "s3:Abort
MultipartUpload",
        "s3:PutOb
jectRetention",
        "s3:Delet
eObject"
      ],
      "Resource":
 ["s3BucketArn",
 "s3BucketArn/*"]
    },
    { "Action":
 ["s3:List*"],
 "Resource": "*",
 "Effect": "Allow" },
    {
      "Action": [
        "kms:List*",
        "kms:Get*",
        "kms:Desc
ribe*",
        "kms:Decrypt",
        "kms:Encrypt",
        "kms:ReEn
crypt*",
        "kms:Verify",
        "kms:Sign",
        "kms:Gene
rateDataKey"
      ],
```

Tipo di ambiente	Autorizzazioni IAM	

```
      "Resource":
 "keyArn",
      "Effect": "Allow"
    },
    {
      "Action":
 ["kms:ListKeys",
 "kms:ListAliases"],
      "Resource": "*",
      "Effect": "Allow"
    },
    {
      "Action": [
        "ec2:Desc
ribeSecurityGroups",
        "ec2:Desc
ribeSecurityGroupR
ules",
        "ec2:Desc
ribeTags"
      ],
      "Resource": "*",
      "Effect": "Allow"
    },
    {
      "Action": [
        "logs:Des
cribe*",
        "logs:Sta
rtQuery",
        "logs:Sto
pQuery",
        "logs:Get*",
        "logs:List*",
        "logs:Put
LogEvents",
        "logs:Cre
ateLogStream",
        "logs:Fil
terLogEvents"
      ],
```

Tipo di ambiente	Autorizzazioni IAM	

```
      "Resource":
 "arn:aws:logs:regi
on:account-id:log-
group:log-group-na
me:*",
      "Effect": "Allow"
    },
    {
      "Effect": "Allow",
      "Action": [
        "s3:Get*",
        "s3:List*",
        "kms:List*",
        "kms:Get*",
        "kms:Desc
ribe*",
        "kms:Decrypt"
      ],
      "Resource": "*",
      "Condition": {
        "StringNo
tEquals": {
          "aws:Reso
urceAccount":
 "project-account-id"
        }
      }
    }
  ]
}
```

Tipo di ambiente	Autorizzazioni IAM

Produttore di Data Lake	{
	  "Version": "2012-10-17",
	  "Statement": [
	  {
	  "Effect": "Allow",
	  "Action": [
	  "glue:BatchGet*",
	  "glue:Get*",
	  "glue:SearchTables",
	  "glue:List*",
	  "glue:BatchCreatePartition",
	  "glue:CreatePartitionIndex",
	  "glue:CreateTable",
	  "glue:BatchUpdatePartition",
	  "glue:BatchDeletePartition",
	  "glue:UpdateTable",
	  "glue:DeleteTableVersion",
	  "glue:DeleteTable",
	  "glue:DeleteColumnStatisticsForPartition",
	  "glue:DeleteColumnStatisticsForTable",
	  "glue:DeletePartitionIndex",
	  "glue:UpdateColumnStatisticsForPartition",

Tipo di ambiente	Autorizzazioni IAM	

```
        "glue:Upd
ateColumnStatistic
sForTable",
        "glue:Bat
chDeleteTableVersi
on",
        "glue:Bat
chDeleteTable",
        "glue:Cre
atePartition",
        "glue:Del
etePartition",
        "glue:Upd
atePartition"
      ],
      "Resource": [
        "arn:aws:
glue:region:accoun
t:database/dbName",
        "arn:aws:
glue:region:accoun
t:catalog",
        "arn:aws:
glue:region:accoun
t:table/dbName/*"
      ]
    },
    {
      "Sid": "VisualEd
itor0",
      "Effect": "Allow",
      "Action": [
        "glue:Sea
rchTables",
        "glue:Not
ifyEvent",
        "glue:Sta
rtBlueprintRun",
        "glue:Put
WorkflowRunPropert
ies",
```

Tipo di ambiente	Autorizzazioni IAM	

```
        "glue:Sto
pCrawler",
        "glue:Del
eteJob",
        "glue:Del
eteWorkflow",
        "glue:Upd
ateCrawler",
        "glue:Del
eteBlueprint",
        "glue:Upd
ateWorkflow",
        "glue:Sta
rtCrawler",
        "glue:Res
etJobBookmark",
        "glue:Upd
ateJob",
        "glue:Sta
rtWorkflowRun",
        "glue:Sto
pCrawlerSchedule",
        "glue:Res
umeWorkflowRun",
        "glue:List*",
        "glue:Del
eteCrawler",
        "glue:Upd
ateBlueprint",
        "glue:Bat
chStopJobRun",
        "glue:Sto
pWorkflowRun",
        "glue:Bat
chGet*",
        "glue:Upd
ateCrawlerSchedule",
        "glue:Del
eteConnection",
        "glue:Upd
ateConnection",
        "glue:Get*",
```

Tipo di ambiente	Autorizzazioni IAM	

```
        "glue:Bat
chDeleteConnection",
        "glue:Sta
rtCrawlerSchedule",
        "glue:Sta
rtJobRun",
        "glue:Cre
ateWorkflow",
        "glue:Pub
lishDataQuality",
        "glue:*Da
taQuality*"
      ],
      "Resource": "*",
      "Condition": {
        "ForAnyVa
lue:StringEquals": {
          "aws:Reso
urceTag/noah-analy
tics:projectId":
 "projectId"
        }
      }
    },
    {
      "Sid": "CreateGl
ueResources",
      "Effect": "Allow",
      "Action": [
        "glue:Cre
ateBlueprint",
        "glue:Cre
ateJob",
        "glue:Cre
ateConnection",
        "glue:Cre
ateCrawler",
        "glue:Cre
ateDataQualityRule
set"
      ],
      "Resource": "*"
```

Tipo di ambiente	Autorizzazioni IAM	

```
    },
    {
      "Sid": "VisualEd
itor0",
      "Effect": "Allow",
      "Action": [
        "iam:List
Roles",
        "iam:List
Users",
        "iam:List
Groups",
        "iam:List
RolePolicies",
        "iam:GetRole",
        "iam:GetR
olePolicy"
      ],
      "Resource": "*"
    }
  ]
}
```

Tipo di ambiente	Autorizzazioni IAM

Consumatore di Data Lake	{
	  "Version": "2012-10-17",
	  "Statement": [
	  {
	  "Effect": "Allow",
	  "Action": [
	  "athena:TerminateSession",
	  "athena:CreatePreparedStatement",
	  "athena:StopCalculationExecution",
	  "athena:StartQueryExecution",
	  "athena:UpdatePreparedStatement",
	  "athena:BatchGet*",
	  "athena:UpdateNotebook",
	  "athena:DeleteNotebook",
	  "athena:DeletePreparedStatement",
	  "athena:UpdateNotebookMetadata",
	  "athena:DeleteNamedQuery",
	  "athena:Get*",
	  "athena:UpdateNamedQuery",
	  "athena:CreateNamedQuery",

Tipo di ambiente	Autorizzazioni IAM	

```
        "athena:E
xportNotebook",
        "athena:S
topQueryExecution",
        "athena:S
tartCalculationExe
cution",
        "athena:S
tartSession",
        "athena:C
reatePresignedNote
bookUrl",
        "athena:C
reateNotebook",
        "athena:I
mportNotebook"
      ],
      "Resource": [
        "arn:aws:
athena:region:acco
unt-id:workgroup/w
orkGroupName",
        "arn:aws:
athena:region:acco
unt-id:datacatalog/
AwsDataCatalog"
      ]
    },
    {
      "Effect": "Allow",
      "Action": [
        "athena:L
istWorkGroups",
        "athena:L
istDataCatalogs",
        "athena:List*"
      ],
      "Resource": ["*"]
    },
    {
      "Effect": "Allow",
      "Action": [
```

Tipo di ambiente	Autorizzazioni IAM	

```
        "glue:Bat
chGet*",
        "glue:Get*",
        "glue:Sea
rchTables",
        "glue:List*"
      ],
      "Resource": [
        "arn:aws:
glue:region:account-
id:database/dbName",
        "arn:aws:
glue:region:account-
id:catalog",
        "arn:aws:
glue:region:account-
id:table/dbName/*"
      ]
    }
  ]
}
```

Tipo di ambiente	Autorizzazioni IAM	

Produttore di Data Warehouse	{
	"Version": "2012-10-17",
	"Statement": [
	{
	"Effect": "Allow",
	"Action": [
	"redshift:GetClusterCredentials",
	"redshift:JoinGroup",
	"redshift:CreateClusterUser",
	"redshift:DescribeClusters"
	],
	"Resource": "arn:aws:redshift:region:account:cluster:producerRedshiftCluster"
	},
	{
	"Effect": "Allow",
	"Action": [
	"redshift-data:DescribeStatement",
	"redshift-data:ExecuteStatement"
	],
	"Resource": "arn:aws:redshift:region:account:cluster:producerRedshiftCluster"
	}
	]
	}	

Tipo di ambiente	Autorizzazioni IAM	

Tipo di ambiente	Autorizzazioni IAM

Consumatore di data warehouse	{
	"Version": "2012-10-17",
	"Statement": [
	{
	"Effect": "Allow",
	"Action": [
	"redshift:GetClusterCredentials",
	"redshift:JoinGroup",
	"redshift:CreateClusterUser",
	"redshift:DescribeClusters"
	],
	"Resource": [
	"arn:aws:redshift:region:account:dbuser:cluster-identifier/dbUser",
	"arn:aws:redshift:region:account:dbgroup:cluster-identifier/project_owner@projectName",
	"arn:aws:redshift:region:account:dbname:cluster-identifier/*"
	],
	"Condition": {
	"ForAnyValue:StringEquals": {
	"aws:PrincipalTag/RedshiftDbUser": "dbUser"
	}

Tipo di ambiente	Autorizzazioni IAM	

```
      }
    },
    {
      "Sid": "VisualEd
itor2",
      "Effect": "Allow",
      "Action": [
        "redshift-
data:DescribeStat
ement",
        "redshift-
data:ExecuteStatement"
      ],
      "Resource":
 "arn:aws:redshift:
region:account-id:
cluster:cluster-id
entifier"
    }
  ]
}
```

Tipo di ambiente	Autorizzazioni IAM	

Editor di query v2 di Amazon Redshift	{
	  "Version": "2012-10-17",
	  "Statement": [
	    {
	      "Action": "redshift:DescribeClusters",
	      "Effect": "Allow",
	      "Resource": "arn:aws:redshift:region:account-id:cluster:*",
	      "Sid": "RedshiftPermissions"
	    },
	    {
	      "Action": "tag:GetResources",
	      "Condition": {
	        "StringEquals": { "aws:CalledViaLast": "sqlworkbench.amazonaws.com" }
	      },
	      "Effect": "Allow",
	      "Resource": "*",
	      "Sid": "ResourceGroupsTaggingPermissions"
	    },
	    {
	      "Action": [
	        "sqlworkbench:DriverExecute",
	        "sqlworkbench:GenerateSession",	

Tipo di ambiente	Autorizzazioni IAM	

```
        "sqlworkb
ench:ListConnectio
ns",
        "sqlworkb
ench:ListDatabases",
        "sqlworkb
ench:ListFiles",
        "sqlworkb
ench:ListNotebooks",
        "sqlworkb
ench:ListQueryExec
utionHistory",
        "sqlworkb
ench:ListRedshiftC
lusters",
        "sqlworkb
ench:ListSampleDat
abases",
        "sqlworkb
ench:ListTabs",
        "sqlworkb
ench:ListTaggedRes
ources"
      ],
      "Effect": "Allow",
      "Resource": "*",
      "Sid": "AmazonRe
dshiftQueryEditorV
2PermissionsPart1"
    },
    {
      "Action":
 "sqlworkbench:*",
      "Effect": "Allow",
      "Resource": [
        "arn:aws:
sqlworkbench:regio
n:account-id:query/
*",
        "arn:aws:
sqlworkbench:regio
```

Tipo di ambiente	Autorizzazioni IAM

```
n:account-id:noteb
ook/*",
        "arn:aws:
sqlworkbench:regio
n:account-id:conne
ction/*",
        "arn:aws:
sqlworkbench:regio
n:account-id:chart/
*",
        "arn:aws:
sqlworkbench:regio
n:account-id:/*"
      ],
      "Sid": "AmazonRe
dshiftQueryEditorV
2PermissionsPart2"
    }
  ]
}
```

Credenziali temporanee

Alcuni AWS servizi non funzionano quando si accede utilizzando credenziali temporanee. Per ulteriori informazioni, inclusi AWS i servizi che funzionano con credenziali temporanee, consulta AWS i servizi che funzionano con IAM nella IAM User Guide.

Stai utilizzando credenziali temporanee se accedi AWS Management Console utilizzando qualsiasi metodo tranne nome utente e password. Ad esempio, quando accedi AWS utilizzando il link Single Sign-On (SSO) della tua azienda, tale processo crea automaticamente credenziali temporanee. Le credenziali temporanee vengono create in automatico anche quando accedi alla console come utente e poi cambi ruolo. Per ulteriori informazioni sullo scambio dei ruoli, consulta Cambio di un ruolo (console) nella Guida per l'utente di IAM.

È possibile creare manualmente credenziali temporanee utilizzando l'API or. AWS CLI AWS È quindi possibile utilizzare tali credenziali temporanee per accedere. AWS AWS consiglia di generare

dinamicamente credenziali temporanee anziché utilizzare chiavi di accesso a lungo termine. Per ulteriori informazioni, consulta Credenziali di sicurezza provvisorie in IAM.

Autorizzazioni del principale

Quando utilizzi un utente o un ruolo IAM per eseguire azioni AWS, sei considerato un principale. Le policy concedono autorizzazioni a un principale. Quando si utilizzano alcuni servizi, è possibile eseguire un'azione che attiva un'altra azione in un servizio diverso. In questo caso è necessario disporre delle autorizzazioni per eseguire entrambe le azioni. Per vedere se un'azione richiede azioni dipendenti aggiuntive in una policy, consulta Actions, Resources and Condition Keys for AWS Documentation Essentials nel Service Authorization Reference.

Convalida della conformità per Amazon DataZone

Per sapere se un Servizio AWS programma rientra nell'ambito di specifici programmi di conformità, consulta Servizi AWS la sezione Scope by Compliance Program Servizi AWS e scegli il programma di conformità che ti interessa. Per informazioni generali, consulta Programmi di AWS conformità Programmi di di .

È possibile scaricare report di audit di terze parti utilizzando AWS Artifact. Per ulteriori informazioni, consulta Scaricamento dei report in AWS Artifact .

La vostra responsabilità di conformità durante l'utilizzo Servizi AWS è determinata dalla sensibilità dei dati, dagli obiettivi di conformità dell'azienda e dalle leggi e dai regolamenti applicabili. AWS fornisce le seguenti risorse per contribuire alla conformità:

- Guide introduttive su sicurezza e conformità: queste guide all'implementazione illustrano considerazioni sull'architettura e forniscono passaggi per implementare ambienti di base incentrati sulla AWS sicurezza e la conformità.
- Progettazione per la sicurezza e la conformità HIPAA su Amazon Web Services: questo white paper descrive in che modo le aziende possono utilizzare AWS per creare applicazioni idonee all'HIPAA.

> **Note**
>
> Non Servizi AWS tutte sono idonee all'HIPAA. Per ulteriori informazioni, consulta la sezione Riferimenti sui servizi conformi ai requisiti HIPAA.

- AWS Risorse per la per la conformità: questa raccolta di cartelle di lavoro e guide potrebbe essere valida per il tuo settore e la tua località.
- AWS Guide alla conformità dei clienti: comprendi il modello di responsabilità condivisa attraverso la lente della conformità. Le guide riassumono le migliori pratiche per la protezione Servizi AWS e mappano le linee guida per i controlli di sicurezza su più framework (tra cui il National Institute of Standards and Technology (NIST), il Payment Card Industry Security Standards Council (PCI) e l'International Organization for Standardization (ISO)).
- Valutazione delle risorse con regole nella Guida per gli AWS Config sviluppatori: il AWS Config servizio valuta la conformità delle configurazioni delle risorse alle pratiche interne, alle linee guida e alle normative del settore.
- AWS Security Hub— Ciò Servizio AWS fornisce una visione completa dello stato di sicurezza interno. AWS La Centrale di sicurezza utilizza i controlli di sicurezza per valutare le risorse AWS e verificare la conformità agli standard e alle best practice del settore della sicurezza. Per un elenco dei servizi e dei controlli supportati, consulta la pagina Documentazione di riferimento sui controlli della Centrale di sicurezza.
- Amazon GuardDuty: Servizio AWS rileva potenziali minacce ai tuoi carichi di lavoro Account AWS, ai contenitori e ai dati monitorando l'ambiente alla ricerca di attività sospette e dannose. GuardDuty può aiutarti a soddisfare vari requisiti di conformità, come lo standard PCI DSS, soddisfacendo i requisiti di rilevamento delle intrusioni imposti da determinati framework di conformità.
- AWS Audit Manager— Ciò Servizio AWS consente di verificare continuamente l' AWS utilizzo per semplificare la gestione del rischio e la conformità alle normative e agli standard di settore.

Best practice di sicurezza per Amazon DataZone

Amazon DataZone offre una serie di funzionalità di sicurezza da prendere in considerazione durante lo sviluppo e l'implementazione delle proprie politiche di sicurezza. Le seguenti best practice sono linee guida generali e non rappresentano una soluzione di sicurezza completa. Poiché queste best practice potrebbero non essere appropriate o sufficienti per l'ambiente, gestiscile come considerazioni utili anziché prescrizioni.

Implementazione dell'accesso con privilegi minimi

Quando concedi le autorizzazioni, sei tu a decidere chi ottiene quali autorizzazioni per quali risorse Amazon. DataZone È possibile abilitare operazioni specifiche che si desidera consentire su tali risorse. Pertanto è necessario concedere solo le autorizzazioni necessarie per eseguire un'attività.

L'implementazione dell'accesso con privilegi minimi è fondamentale per ridurre i rischi di sicurezza e l'impatto risultante da errori o intenzioni dannose.

Uso di ruoli IAM

Le applicazioni Producer e Client devono disporre di credenziali valide per accedere alle DataZone risorse Amazon. Non è necessario archiviare AWS le credenziali direttamente in un'applicazione client o in un bucket Amazon S3. Si tratta di credenziali a lungo termine che non vengono automaticamente ruotate e potrebbero avere un impatto aziendale significativo se vengono compromesse.

Invece, dovresti utilizzare un ruolo IAM per gestire le credenziali temporanee per le tue applicazioni di produzione e client per accedere alle DataZone risorse Amazon. Quando utilizzi un ruolo, non devi necessariamente usare credenziali a lungo termine (ad esempio, nome utente e password o chiavi di accesso) per accedere ad altre risorse.

Per ulteriori informazioni, consulta gli argomenti seguenti nella Guida per l'utente IAM:

- Ruoli IAM
- Scenari comuni per ruoli: utenti, applicazioni e servizi

Implementazione della crittografia lato server in risorse dipendenti

I dati inattivi e i dati in transito possono essere crittografati in Amazon DataZone.

Utilizzalo CloudTrail per monitorare le chiamate API

Amazon DataZone è integrato con AWS CloudTrail, un servizio che fornisce un registro delle azioni intraprese da un utente, un ruolo o un AWS servizio in Amazon DataZone.

Utilizzando le informazioni raccolte da CloudTrail, puoi determinare la richiesta che è stata effettuata ad Amazon DataZone, l'indirizzo IP da cui è stata effettuata la richiesta, chi ha effettuato la richiesta, quando è stata effettuata e dettagli aggiuntivi.

Resilienza in Amazon DataZone

L'infrastruttura AWS globale è costruita attorno a Regioni AWS zone di disponibilità. Regioni AWS forniscono più zone di disponibilità fisicamente separate e isolate, collegate con reti a bassa latenza,

ad alto throughput e altamente ridondanti. Con le zone di disponibilità, puoi progettare e gestire applicazioni e database che eseguono automaticamente il failover tra zone di disponibilità senza interruzioni. Le zone di disponibilità sono più disponibili, tolleranti ai guasti e scalabili rispetto alle infrastrutture a data center singolo o multiplo tradizionali.

Per ulteriori informazioni sulle zone di disponibilità, vedere Global Regioni AWS Infrastructure.AWS

Oltre all'infrastruttura AWS globale, Amazon DataZone offre diverse funzionalità per aiutarti a supportare le tue esigenze di resilienza e backup dei dati.

Argomenti

- Resilienza delle fonti di dati
- Resilienza degli asset
- Resilienza del tipo di risorsa e del modulo dei metadati
- Glossario: resilienza
- Resilienza della ricerca globale
- Resilienza degli abbonamenti
- Resilienza dell'ambiente
- Resilienza del modello ambientale
- Resilienza del progetto
- Resilienza della RAM
- Resilienza nella gestione dei profili utente
- Resilienza del dominio

Resilienza delle fonti di dati

Durante un evento di DataZone disponibilità di Amazon, i `DataSource` lavori riproveranno periodicamente per un massimo di 24 ore. Se un processo fallisce a causa di un'errata configurazione, verrà `DataSourceRunFailed` emesso un evento. Se il DataZone dominio Amazon è configurato con una chiave KMS e AmazonDataZoneDomainExecutionRole perde l'accesso a questa chiave durante l'esecuzione di un processo, l'esecuzione terminerà nello `INACCESSIBLE` stato. Una volta ripristinato l'accesso KMS, il lavoro deve essere aggiornato manualmente per attivare la transizione verso uno stato utilizzabile.

Resilienza degli asset

In Amazon DataZone, le risorse sono suddivise in versioni. Se è necessario ripristinare una versione di una risorsa, puoi creare una nuova versione utilizzando il contenuto dell'ultima versione stabile. È possibile pubblicare una versione della risorsa. Una versione pubblicata di una risorsa non può essere modificata, se non pubblicando una nuova versione. È possibile sottoscrivere una risorsa pubblicata (nota anche come elenco). Per evitare nuove sottoscrizioni a una risorsa, questa può essere annullata dalla pubblicazione. L'annullamento della pubblicazione di una risorsa non ha alcun effetto sugli abbonamenti esistenti. L'eliminazione di una risorsa eliminerà tutte le versioni non pubblicate della risorsa. Le versioni pubblicate della risorsa devono essere eliminate separatamente. Una versione pubblicata di una risorsa può essere eliminata solo se non ci sono sottoscrizioni.

Resilienza del tipo di risorsa e del modulo dei metadati

In Amazon DataZone, i tipi di asset e i tipi di modulo di metadati sono versionati. Un tipo di risorsa non può essere eliminato se è utilizzato da una risorsa. Un tipo di modulo di metadati non può essere eliminato se è utilizzato da un tipo di risorsa o da una risorsa. Se non desideri che vengano utilizzati specifici metadata-form-type per la cura, puoi disabilitarli, senza che ciò influisca su quelli a cui sono già associati.

Glossario: resilienza

In Amazon DataZone, i glossari e i termini del glossario non possono essere eliminati se sono in uso. Se non desideri utilizzare un glossario o un termine di glossario specifico per la cura, puoi disabilitarli senza influire su quelli a cui sono già associati.

Resilienza della ricerca globale

In Amazon DataZone, le risorse pubblicate (note anche come inserzioni) possono essere scoperte tramite la ricerca globale. La pubblicazione di una risorsa può essere annullata annullando la pubblicazione della risorsa. L'annullamento della pubblicazione di una risorsa non influisce sugli abbonamenti esistenti. Una risorsa pubblicata può essere ripristinata a una versione particolare della risorsa ripubblicando quella versione. Ciò non influirà sugli abbonamenti esistenti.

Resilienza degli abbonamenti

In Amazon DataZone, SubscriptionGrant Fulfillment tenterà di ritirarsi due volte prima di fallire. Se fallisce, deve essere eliminato manualmente per riprovare. Se Amazon DataZone non è in grado di revocare le autorizzazioni per un abbonamento, l'eliminazione dell'abbonamento

potrebbe non riuscire. È necessario correggere l'errore sottostante oppure è possibile utilizzare il `retainPermissions` flag nell'operazione `DeleteSubscriptionGrant` API per forzare l'eliminazione della concessione da Amazon DataZone senza revocare le autorizzazioni.

Se il DataZone dominio Amazon è configurato con una chiave KMS e `AmazonDataZoneDomainExecutionRole` perde l'accesso a questa chiave durante il `SubscriptionGrant` flusso di lavoro, la concessione viene contrassegnata`INACCESSIBLE`. Una volta ripristinato l'accesso KMS, le `INACCESSIBLE` concessioni devono essere eliminate e ricreate.

Resilienza dell'ambiente

Se il DataZone dominio Amazon è configurato con una chiave KMS e `AmazonDataZoneDomainExecutionRole` perde l'accesso a questa chiave durante il flusso di lavoro dell'ambiente, l'ambiente verrà contrassegnato`INACCESSIBLE`. Una volta ripristinato l'accesso KMS, l'`INACCESSIBLE`ambiente deve essere eliminato e ricreato. La creazione dell'ambiente tenterà di ritirarsi due volte prima di fallire. Se fallisce, deve essere eliminato manualmente per riprovare. Se il flusso di lavoro dell'ambiente fallisce, l'ambiente entrerà in uno stato di errore. A questo punto, può solo essere eliminato e ricreato.

Resilienza del modello ambientale

In Amazon DataZone, un blueprint di ambiente non può essere eliminato se sono presenti profili di ambiente sottostanti.

Resilienza del progetto

In Amazon DataZone, un progetto non può essere eliminato se sono presenti ambienti contenuti.

Resilienza della RAM

Per informazioni sulla resilienza della RAM, vedere https://docs.aws.amazon.com/ram/latest/ userguide/ security-disaster-recovery-resiliency .html.

Resilienza nella gestione dei profili utente

Per informazioni sulla resilienza del profilo utente, consulta AWS Identity Center.

Resilienza del dominio

In Amazon DataZone, un dominio non può essere eliminato se contiene progetti o fonti di dati.

Sicurezza dell'infrastruttura in Amazon DataZone

In quanto servizio gestito, Amazon DataZone è protetto dalla sicurezza di rete AWS globale. Per informazioni sui servizi AWS di sicurezza e su come AWS protegge l'infrastruttura, consulta AWS Cloud Security. Per progettare il tuo AWS ambiente utilizzando le migliori pratiche per la sicurezza dell'infrastruttura, vedi Infrastructure Protection in Security Pillar AWS Well-Architected Framework.

Utilizzi chiamate API AWS pubblicate per accedere ad Amazon DataZone tramite la rete. I client devono supportare quanto segue:

- Transport Layer Security (TLS). È richiesto TLS 1.2 ed è consigliato TLS 1.3.
- Suite di cifratura con Perfect Forward Secrecy (PFS), ad esempio Ephemeral Diffie-Hellman (DHE) o Elliptic Curve Ephemeral Diffie-Hellman (ECDHE). La maggior parte dei sistemi moderni, come Java 7 e versioni successive, supporta tali modalità.

Inoltre, le richieste devono essere firmate utilizzando un ID chiave di accesso e una chiave di accesso segreta associata a un principale IAM. O puoi utilizzare AWS Security Token Service (AWS STS) per generare credenziali di sicurezza temporanee per sottoscrivere le richieste.

Prevenzione interservizio confusa su più servizi in Amazon DataZone

Con "confused deputy" si intende un problema di sicurezza in cui un'entità che non dispone dell'autorizzazione per eseguire una certa operazione può costringere un'entità con più privilegi a eseguire tale operazione. Nel AWS, l'impersonificazione tra servizi può portare al confuso problema del vicesceriffo. La rappresentazione tra servizi può verificarsi quando un servizio (il servizio chiamante) effettua una chiamata a un altro servizio (il servizio chiamato). Il servizio chiamante può essere manipolato per utilizzare le proprie autorizzazioni e agire sulle risorse di un altro cliente, a cui normalmente non avrebbe accesso. Per evitare che ciò accada, AWS mette a disposizione strumenti che consentono di proteggere i dati relativi a tutti i servizi con responsabili del servizio a cui è stato concesso l'accesso alle risorse del vostro account.

Ti consigliamo di utilizzare la chiave aws: SourceAccount global condition context nelle policy delle risorse per limitare le autorizzazioni che Amazon DataZone concede a un altro servizio alla risorsa. Usa aws: SourceAccount se desideri consentire l'associazione di qualsiasi risorsa in quell'account all'utilizzo tra servizi.

Analisi della configurazione e delle vulnerabilità per Amazon DataZone

AWS gestisce le attività di sicurezza di base come l'applicazione di patch al sistema operativo guest (OS) e al database, la configurazione del firewall e il disaster recovery. Queste procedure sono state riviste e certificate dalle terze parti appropriate. Per ulteriori informazioni, consulta il modello di responsabilità AWS condivisa.

Domini da aggiungere all'elenco dei domini consentiti

Affinché il portale DataZone dati Amazon possa accedere al DataZone servizio Amazon, devi aggiungere i seguenti domini all'elenco dei domini consentiti sulla rete da cui il portale dati sta tentando di accedere al servizio.

- `*.api.aws`
- `*.on.aws`

Monitoraggio Amazon DataZone

Il monitoraggio è una parte importante per mantenere l'affidabilità, la disponibilità e le prestazioni di Amazon DataZone e delle altre AWS soluzioni. AWS fornisce i seguenti strumenti di monitoraggio per monitorare Amazon DataZone, segnalare quando qualcosa non va e intraprendere azioni automatiche quando necessario:

- Amazon CloudWatch monitora AWS le tue risorse e le applicazioni su cui esegui AWS in tempo reale. Puoi raccogliere i parametri e tenerne traccia, creare pannelli di controllo personalizzati e impostare allarmi per inviare una notifica o intraprendere azioni quando un parametro specificato raggiunge una determinata soglia. Ad esempio, puoi tenere CloudWatch traccia dell'utilizzo della CPU o di altri parametri delle tue istanze Amazon EC2 e avviare automaticamente nuove istanze quando necessario. Per ulteriori informazioni, consulta la Amazon CloudWatch User Guide.
- Amazon CloudWatch Logs ti consente di monitorare, archiviare e accedere ai tuoi file di log da istanze Amazon EC2 e altre CloudTrail fonti. CloudWatch I log possono monitorare le informazioni nei file di registro e avvisarti quando vengono raggiunte determinate soglie. Puoi inoltre archiviare i dati del log in storage estremamente durevole. Per ulteriori informazioni, consulta la Amazon CloudWatch Logs User Guide.
- Amazon EventBridge può essere utilizzato per automatizzare i AWS servizi e rispondere automaticamente agli eventi di sistema, come problemi di disponibilità delle applicazioni o modifiche delle risorse. Gli eventi AWS relativi ai servizi vengono forniti quasi EventBridge in tempo reale. Puoi compilare regole semplici che indichino quali eventi sono considerati di interesse per te e quali operazioni automatizzate intraprendere quando un evento corrisponde a una regola. Per ulteriori informazioni, consulta Amazon EventBridge User Guide.
- AWS CloudTrailacquisisce le chiamate API e gli eventi correlati effettuati da o per conto del tuo AWS account e invia i file di log a un bucket Amazon S3 da te specificato. Puoi identificare quali utenti e account hanno chiamato AWS, l'indirizzo IP di origine da cui sono state effettuate le chiamate e quando sono avvenute le chiamate. Per ulteriori informazioni, consulta la Guida per l'utente AWS CloudTrail.

Monitoraggio di Amazon DataZone con Amazon CloudWatch

Puoi monitorare DataZone l'utilizzo di Amazon CloudWatch, che raccoglie dati grezzi e li elabora in metriche leggibili quasi in tempo reale. Queste statistiche vengono conservate per un periodo di 15 mesi, per permettere l'accesso alle informazioni storiche e offrire una prospettiva migliore sulle

prestazioni del servizio o dell'applicazione web. È anche possibile impostare allarmi che controllano determinate soglie e inviare notifiche o intraprendere azioni quando queste soglie vengono raggiunte. Per ulteriori informazioni, consulta la Amazon CloudWatch User Guide.

Il portale DataZone dati Amazon utilizza le API del piano DataZone dati di Amazon con autenticazione e autorizzazione JWT. Amazon DataZone assume il ruolo di servizio DataZone predefinito di Amazon e registra tutte le chiamate DataZone API Amazon effettuate tramite il portale DataZone dati Amazon in un gruppo di log denominato DataZoneDataPortal API. CallLogs

Monitoraggio DataZone degli eventi Amazon su Amazon EventBridge

Puoi monitorare DataZone gli eventi di Amazon in EventBridge, che fornisce un flusso di dati in tempo reale dalle tue applicazioni, applicazioni software-as-a-service (SaaS) e AWS servizi. EventBridgeindirizza tali dati verso obiettivi come Amazon AWS Lambda Simple Notification Service. Questi eventi sono gli stessi che compaiono in Amazon CloudWatch Events, che fornisce un flusso quasi in tempo reale di eventi di sistema che descrivono i cambiamenti nelle AWS risorse.

Per ulteriori informazioni, consulta Lavorare con gli eventi tramite il bus EventBridge predefinito di Amazon.

Registrazione delle chiamate DataZone API Amazon tramite AWS CloudTrail

Amazon DataZone è integrato con AWS CloudTrail, un servizio che fornisce un registro delle azioni intraprese da un utente, un ruolo o un AWS servizio in Amazon DataZone. CloudTrail acquisisce tutte le chiamate API per Amazon DataZone come eventi. Le chiamate acquisite includono chiamate dalla DataZone console Amazon e chiamate in codice alle operazioni dell' DataZone API Amazon. Se crei un trail, puoi abilitare la distribuzione continua di CloudTrail eventi a un bucket Amazon S3, inclusi gli eventi per Amazon. DataZone Se non configuri un percorso, puoi comunque visualizzare gli eventi più recenti nella CloudTrail console nella cronologia degli eventi. Utilizzando le informazioni raccolte da CloudTrail, puoi determinare la richiesta che è stata effettuata ad Amazon DataZone, l'indirizzo IP da cui è stata effettuata la richiesta, chi ha effettuato la richiesta, quando è stata effettuata e dettagli aggiuntivi.

Per ulteriori informazioni CloudTrail, consulta la Guida AWS CloudTrail per l'utente.

DataZone Informazioni su Amazon in CloudTrail

CloudTrail è abilitato sul tuo account al Account AWS momento della creazione dell'account. Quando si verifica un'attività nella console di DataZone gestione Amazon, tale attività viene registrata in un CloudTrail evento insieme ad altri eventi di AWS servizio nella cronologia degli eventi. Puoi visualizzare, cercare e scaricare gli eventi recenti nel tuo Account AWS. Per ulteriori informazioni, consulta Visualizzazione degli eventi con la cronologia degli CloudTrail eventi.

Per una registrazione continua degli eventi del tuo sito Account AWS, compresi gli eventi per Amazon DataZone, crea un percorso. Un trail consente di CloudTrail inviare file di log a un bucket Amazon S3. Per impostazione predefinita, quando si crea un percorso nella console, questo sarà valido in tutte le Regioni AWS. Il trail registra gli eventi di tutte le regioni della AWS partizione e consegna i file di log al bucket Amazon S3 specificato. Inoltre, puoi configurare altri AWS servizi per analizzare ulteriormente e agire in base ai dati sugli eventi raccolti nei log. CloudTrail Per ulteriori informazioni, consulta gli argomenti seguenti:

- Panoramica della creazione di un percorso
- CloudTrail servizi e integrazioni supportati
- Configurazione delle notifiche Amazon SNS per CloudTrail
- Ricezione di file di CloudTrail registro da più regioni e ricezione di file di CloudTrail registro da più account

Tutte le DataZone azioni di Amazon vengono registrate da CloudTrail.

Risoluzione dei problemi con Amazon DataZone

Se riscontri problemi di accesso negato o difficoltà simili quando lavori con Amazon, DataZone consulta gli argomenti di questa sezione.

Risoluzione dei problemi relativi alle autorizzazioni di AWS Lake Formation per Amazon DataZone

Questa sezione contiene istruzioni per la risoluzione dei problemi che potresti riscontrare quando lo faiConfigura le autorizzazioni di Lake Formation per Amazon DataZone.

Messaggio di errore nel Data Portal	Risoluzione
Impossibile assumere il ruolo di accesso ai dati.	Questo errore viene visualizzato quando Amazon non DataZone è in grado di presumere AmazonDataZoneGlueDataAccessRoleche tu abbia utilizzato per abilitarlo DefaultDa taLakeBlueprintnel tuo account. Per risolvere il problema, accedi alla console AWS IAM dell'account in cui si trova il tuo asset di dati e assicurati che AmazonDataZoneGlue DataAccessRoleabbia il giusto rapporto di fiducia con il responsabile del DataZone servizio Amazon. Per ulteriori informazioni, consulta AmazonDataZoneGlueAccess- <region>- <domainId>
Il ruolo di accesso ai dati non dispone delle autorizzazioni necessarie per leggere i metadati della risorsa a cui stai tentando di sottoscrivere.	Questo errore viene visualizzato quando Amazon assume DataZone correttamente il AmazonDataZoneGlueDataAccessRoleruolo, ma il ruolo non dispone delle autorizzazioni necessarie. Per risolvere il problema, accedi alla console AWS IAM dell'account in cui si trova il tuo asset di dati e assicurati che al ruolo sia AmazonDataZoneGlueManageAcc essRolePolicyassociato. Per ulteriori informazi

Messaggio di errore nel Data Portal	Risoluzione
	oni, consulta AmazonDataZoneGlueAccess-<region>- <domainId>.
L'asset è un collegamento a una risorsa. Amazon DataZone non supporta gli abbonamenti ai link alle risorse.	Questo errore viene visualizzato quando la risorsa che stai tentando di pubblicare su Amazon DataZone è un link di risorsa a una tabella AWS Glue.

Messaggio di errore nel Data Portal	Risoluzione
L'asset non è gestito da AWS Lake Formation.	Questo errore indica che le autorizzazioni di AWS Lake Formation non sono applicate alla risorsa che desideri pubblicare. Questo può accadere nei seguenti casi. • La posizione dell'asset in Amazon S3 non è registrata in AWS Lake Formation. Per risolvere il problema, accedi alla console di AWS Lake Formation nell'account in cui esiste la tabella e registra la sede Amazon S3 in modalità AWS Lake Formation o in modalità Hybrid. Per ulteriori informazioni, consulta la pagina Registrazione di una posizione Amazon S3. Esistono diversi scenari che richiedono ulteriori modifiche. Questi includono bucket AmazonS3 crittografati o un bucket S3 per più account e una configurazione Glue Catalog. AWS In questi casi, potrebbero essere necessarie modifiche alle impostazioni KMS e/o S3. Per ulteriori informazioni, consulta la pagina Registrazione di una posizione crittografata Amazon S3. • La posizione Amazon S3 è registrata in modalità AWS Lake Formation, ma IAM AllowedPrincipal viene aggiunto ai permessi della tabella. Per risolvere il problema, puoi rimuovere l'IAM AllowedPrincipal dalle autorizzazioni della tabella o registrare la posizione S3 in modalità ibrida. Per ulteriori informazioni, consulta Informazioni sull'aggiornamento al modello di autorizzazioni Lake Formation. Se la tua posizione S3 è crittografata o la posizione S3 si trova su un account diverso da quello della tabella AWS Glue,

Messaggio di errore nel Data Portal	Risoluzione
	segui le istruzioni in Registrazione di una posizione Amazon S3 crittografata.
Il ruolo Data Access non dispone delle autorizzazioni Lake Formation necessarie per concedere l'accesso a questa risorsa.	Questo errore indica che il file AmazonDataZoneGlueDataAccessRoleche stai utilizzando per abilitare il contenuto DefaultDataLakeBlueprintnel tuo account non dispone delle autorizzazioni necessarie DataZone ad Amazon per gestire le autorizzazioni sulla risorsa pubblicata. Puoi risolvere il problema aggiungendolo AmazonDataZoneGlueDataAccessRolecome amministratore di AWS Lake Formation o concedendo le seguenti autorizzazioni AmazonDataZoneGlueDataAccessRolealla risorsa che desideri pubblicare. • Descrivi e descrivi le autorizzazioni concedibili sul database in cui esiste la risorsa • Autorizzazioni Descrivi, Select, Descrivi Grantable, Select Grantable su tutte le risorse del database l'accesso a cui desideri che Amazon gestisca per tuo conto. DataZone

Quote per Amazon DataZone

Il tuo AWS account ha delle quote predefinite, precedentemente denominate limiti, per ogni servizio. AWS Salvo diversa indicazione, ogni quota è specifica per regione.

Amazon DataZone ha le seguenti quote e limiti.

Risorsa	Descrizione	Valore
Tipi di asset di dati	Il numero massimo di tipi di asset di dati che possono essere creati in un DataZone dominio	1000
Asset di dati	Il numero massimo di asset di dati che possono essere creati in un DataZone dominio Amazon	1 milione
Glossari	Il numero massimo di glossari aziendali che puoi creare in un dominio	1000
Termini del glossario aziendale	Il numero massimo di termini totali del glossario aziendale che puoi creare in un dominio	10000
Ambienti in un dominio	Il numero massimo di ambienti in un DataZone dominio Amazon	500

Cronologia dei documenti per l'Amazon DataZone User Guide

La tabella seguente descrive le versioni della documentazione per Amazon DataZone.

Modifica	Descrizione	Data
AmazonDataZoneSageMakerProvisioning - nuova politica	Una nuova politica denominata AmazonDataZoneSageMakerProvisioningconcede ad Amazon DataZone le autorizzazioni necessarie per interagire con Amazon. SageMaker Per ulteriori informazioni, consulta Amazon DataZone updates to AWS managed policy.	30 aprile 2024
AmazonDataZoneSageMakerEnvironmentRolePermissionsBoundary - nuovo limite di autorizzazioni	Nuovo limite di autorizzazioni chiamato. AmazonDataZoneSageMakerEnvironmentRolePermissionsBoundary Quando crei un SageMaker ambiente Amazon tramite il portale DataZone dati Amazon, Amazon DataZone applica questo limite di autorizzazioni ai ruoli IAM prodotti durante la creazione dell'ambiente. Il limite delle autorizzazioni limita l'ambito dei ruoli DataZone creati da Amazon e degli eventuali ruoli aggiunti. Per ulteriori informazioni, consulta	30 aprile 2024

	Amazon DataZone updates to AWS managed policy.	
AmazonDataZoneSageMakerAccess - nuova politica	Una nuova politica denominata AmazonDataZoneSageMakerAccessconcede ad Amazon DataZone le autorizzazioni necessarie per concedere agli utenti l'accesso a varie risorse nell'ambiente Amazon SageMaker. Per ulteriori informazioni, consulta Amazon DataZone updates to AWS managed policy.	30 aprile 2024
AmazonDataZoneFullAccess - aggiornamento della politica	Un aggiornamento della AmazonDataZoneFullAccesspolitica che aggiunge l'accesso all'`DescribeSecurityGroups` azione per migliorare l'usabilità per gli amministratori degli account, configurando i blueprint nella console e `GetPolicy` un'azione per aiutare a recuperare informazioni sulla politica gestita specificata. Per ulteriori informazioni, consulta Amazon DataZone updates to AWS managed policy.	30 aprile 2024

AmazonDataZoneS3Manage- - nuovo ruolo <region>< domainId>	Nuovo ruolo chiamato AmazonDataZoneS3Manage-<region>, <domainId>utilizzato quando Amazon DataZone chiama AWS Lake Formation per registrare una sede Amazon Simple Storage Service (Amazon S3). AWS Lake Formation assume questo ruolo quando accede ai dati in quella posizione. Per ulteriori informazioni, consulta Amazon DataZone updates to AWS managed policy.	1 aprile 2024
AmazonDataZoneGlue ManageAccessRolePolicy - Aggiornamento della politica	È stato aggiornato il AmazonDataZoneGlue ManageAccessRolePolicysupporto per le autorizzazioni che consentono DataZone ad Amazon di abilitare la pubblicazione e le concessioni di accesso ai dati. Per ulteriori informazioni, consulta Amazon DataZone updates to AWS managed policy.	1 aprile 2024

AmazonDataZoneDomainExecutionRolePolicy e AmazonDataZoneFullUserAccess - Aggiornamento della politica	Aggiornato AmazonDataZoneDomainExecutionRolePolicye AmazonDataZoneFullUserAccessper abilitare il supporto per l'`CancelMetadataGenerationRun` API. Per ulteriori informazioni, consulta Amazon DataZone updates to AWS managed policy.	29 marzo 2024
AmazonDataZoneFullAccess - Aggiornamento della politica	È stato aggiornato `AmazonDataZoneFullAccess` per consentire agli utenti di scegliere i propri segreti, cluster, vpc e sottoreti nella console di DataZone gestione di Amazon anziché digitarli in una casella di testo. Per ulteriori informazioni, consulta Amazon DataZone updates to AWS managed policy.	13 marzo 2024

AmazonDataZoneDomainExecutionRolePolicy - Aggiornamento della politica	Aggiornato AmazonDataZoneDomainExecutionRolePolicyper abilitare il supporto per l' ListEnvironmentBlueprintConfigurationSummaries API necessaria per la creazione di profili di ambiente identificando quali blueprint sono abilitati in quale account e regione. Per ulteriori informazioni, consulta Amazon DataZone updates to AWS managed policy.	1 febbraio 2024
AmazonDataZoneGlueManageAccessRolePolicy - Aggiornamento della politica	Aggiornato il AmazonDataZoneGlueManageAccessRolePolicyper abilitare il supporto per la modalità ibrida AWS Lake Formation. Per ulteriori informazioni, consulta Amazon DataZone updates to AWS managed policy.	14 dicembre 2023

AmazonDataZoneFullUserAccess e AmazonDataZoneDomainExecutionRolePolicy - Aggiornamenti delle politiche	Amazon DataZone ha aggiornato le politiche AmazonDataZoneFullUserAccesse le AmazonDataZoneDomainExecutionRolePolicypolitiche per supportare la funzionalità generativa di descrizione dei dati basata sull'intelligenza artificiale in Amazon. DataZone Per ulteriori informazioni, consulta Amazon DataZone updates to AWS managed policy.	28 novembre 2023
AmazonDataZoneEnvironmentRolePermissionsBoundary - Aggiornamento della politica	Amazon DataZone ha apportato un aggiornamento alla politica AmazonDataZoneEnvironmentRolePermissionsBoundarygestita che consiste in un'`athena:GetQueryResultsStream` autorizzazione aggiuntiva relativa alla `ResourceTag` condizione. Per ulteriori informazioni, consulta Amazon DataZone updates to AWS managed policy.	17 novembre 2023

AmazonDataZoneRedshiftManageAccessRolePolicy - Aggiornamento della politica	Amazon DataZone ha aggiornato la AmazonDataZoneRedshiftManageAccessRolePolicypolitica rimuovendo l'ID dell'organizzazione di controllo relativo all'`redshift:AssociateDataShareConsumer` azione. Ciò consente di condividere le risorse tra AWS le organizzazioni. Per ulteriori informazioni, consulta Amazon DataZone updates to AWS managed policy.	16 novembre 2023
AmazonDataZoneFullUserAccess - Aggiornamento della politica	Amazon DataZone ha aggiornato la AmazonDataZoneFullUserAccesspolitica che garantisce l'accesso completo ad Amazon DataZone, ma non consente la gestione di domini, utenti o account associati. Per ulteriori informazioni, consulta gli DataZone aggiornamenti di Amazon alle AWS politiche gestite.	2 ottobre 2023

AmazonDataZonePreviewConsoleFullAccess - politica obsoleta	Amazon ha DataZone reso obsoleto il AmazonDataZonePreviewConsoleFullAccess. Per ulteriori informazioni, consulta DataZone gli aggiornamenti di Amazon alle politiche gestite. AWS	29 settembre 2023
AmazonDataZonePortalFullAccessPolicy - politica obsoleta	Amazon ha DataZone reso obsoleto il AmazonDataZonePortalFullAccessPolicy. Per ulteriori informazioni, consulta DataZone gli aggiornamenti di Amazon alle politiche gestite. AWS	29 settembre 2023

AmazonDataZoneDomainExecutionRolePolicy - Nuova politica	Amazon DataZone ha aggiunto una nuova politica chiamata AmazonDataZoneDomainExecutionRolePolicy. Questa è la politica predefinita per il ruolo DataZone di servizio Amazon `AmazonDataZoneDomainExecutionRole`. Questo ruolo viene utilizzato da Amazon DataZone per catalogare, scoprire, gestire, condividere e analizzare i dati nel DataZone dominio Amazon. Puoi allegare la politica `AmazonDataZoneDomainExecutionRolePolicy` al tuo `AmazonDataZoneDomainExecutionRole`. Per ulteriori informazioni, consulta Amazon DataZone updates to AWS managed policy.	25 settembre 2023
AmazonDataZoneCrossAccountAdmin - Nuova politica	Amazon DataZone ha aggiunto una nuova politica chiamata AmazonDataZoneCrossAccountAdmin che consente agli utenti di lavorare con Amazon DataZone e gli account associati. Per ulteriori informazioni, consulta Amazon DataZone updates to AWS managed policy.	19 settembre 2023

AmazonDataZoneRedshiftManageAccessRolePolicy - Nuova politica	Amazon DataZone ha aggiunto una nuova politica chiamata AmazonDataZoneRedshiftManageAccessRolePolicyche concede autorizzazioni per consentire ad Amazon di DataZone abilitare la pubblicazione e le concessioni di accesso ai dati. Per ulteriori informazioni, consulta Amazon DataZone updates to AWS managed policy.	12 settembre 2023
AmazonDataZoneRedshiftGlueProvisioningPolicy - Nuova politica	Amazon DataZone ha aggiunto una nuova politica chiamata AmazonDataZoneRedshiftGlueProvisioningPolicyche concede ad Amazon DataZone le autorizzazioni necessarie per interagire con le fonti di dati supportate. Per ulteriori informazioni, consulta Amazon DataZone updates to AWS managed policy.	12 settembre 2023

AmazonDataZoneGlueManageAccessRolePolicy - Nuova politica	Amazon DataZone ha aggiunto una nuova politica chiamata AmazonDataZoneGlueManageAccessRolePolicyconcessione ad Amazon DataZone delle autorizzazioni per pubblicare i dati di AWS Glue nel catalogo. Fornisce inoltre ad Amazon DataZone le autorizzazioni per concedere l'accesso o revocare l'accesso alle risorse pubblicate da AWS Glue nel catalogo. Per ulteriori informazioni, consulta Amazon DataZone updates to AWS managed policy.	12 settembre 2023
AmazonDataZoneFullUserAccess - Nuova politica	Amazon DataZone ha aggiunto una nuova politica chiamata AmazonDataZoneFullUserAccessche garantisce l'accesso completo ad Amazon DataZone tramite il portale dati. Per ulteriori informazioni, consulta Amazon DataZone updates to AWS managed policy.	12 settembre 2023

AmazonDataZoneFullAccess - Nuova politica	Amazon DataZone ha aggiunto una nuova politica chiamata AmazonDataZoneFullAccessche fornisce l'accesso completo ad Amazon DataZone tramite la console di AWS gestione. Per ulteriori informazioni, consulta Amazon DataZone updates to AWS managed policy.	12 settembre 2023
AmazonDataZoneEnvironmentRolePermissionsBoundary - Nuova politica	Amazon DataZone ha aggiunto una nuova policy chiamata AmazonDataZoneEnvironmentRolePermissionsBoundaryche limita il principale IAM fornito a cui è collegata. Per ulteriori informazioni, consulta Amazon DataZone updates to AWS managed policy.	12 settembre 2023
Aggiornamento gestito delle politiche	Aggiornamenti alla politica AmazonDataZonePreviewConsoleFullAccess gestita. Per ulteriori informazioni, consulta Amazon DataZone updates to AWS managed policy.	13 giugno 2023
Aggiornamento gestito delle politiche	Aggiornamenti alla politica AmazonDataZoneProjectDeploymentPermissionsBoundary gestita. Per ulteriori informazioni, consulta Amazon DataZone updates to AWS managed policy.	3 aprile 2023

???	Versione iniziale della Amazon DataZone (Preview) User Guide.	29 marzo 2023

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.