aws

ユーザーガイド

Amazon DataZone

Amazon DataZone: ユーザーガイド

Table of Contents

Amazon とは DataZone 1
..... 1
Amazon が他の DataZone をサポートおよび統合する方法 AWS サービス？ 2
Amazon にアクセスするにはどうすればよいですか DataZone？ 2
用語と概念 4
Amazon DataZone コンポーネント 4
Amazon DataZone ドメインとは 5
Amazon DataZone のプロジェクトと環境とは 5
Amazon DataZone ブループリントとは 6
Amazon DataZone インベントリと発行ワークフローとは 8
プロジェクトインベントリアセットの作成 8
Amazon DataZone カタログへのプロジェクトインベントリアセットの発行 9
Amazon DataZone サブスクリプションおよびフルフィルメントワークフローとは 10
Amazon のユーザーペルソナ DataZone 11
Amazon DataZone の用語 12
新しいものは何ですか？ 19
2024 19
Amazon がドメインユニットと承認ポリシー DataZone を起動する 19
Amazon がデータ製品 DataZone を起動 19
Amazon がきめ細かなアクセスコントロール機能 DataZone を起動 19
Amazon がデータ系統機能 DataZone を起動 20
Amazon がカスタム DataZone を起動 AWS サービスの設計図 20
データソース作成フローの強化 21
Amazon が Amazon との統合 DataZone を開始 SageMaker 21
Amazon が との統合 DataZone を開始 AWS Lake Formation ハイブリッドアクセスモード 21
Amazon が との統合 DataZone を開始 AWS Glue データ品質 21
Amazon での説明に関する AI レコメンデーションの一般提供リリース DataZone 22
Amazon が Amazon Redshift 統合の機能強化 DataZone を開始 23
AWS Amazon の Cloud Formation サポート DataZone 24
Amazon DataZone プロジェクトのメンバーとしてプリンIAMシパルを直接追加する 24
データポータルからのカスタムアセットタイプのサポート 24
2023 25
ドメインの削除 25

ハイブリッドモード ... 25
HIPAA 適格性 ... 25
Amazon DataZone での説明に関する AI レコメンデーション (プレビュー) ... 25
DefaultDataLake ブループリントの強化 ... 26
設定 ... 27
にサインアップする AWS アカウント ... 27
マネジメントコンソールを使用するために必要なIAMアクセス許可を設定する ... 28
管理コンソールにアクセスするためのユーザー、グループ、またはロールに必須およびオプションのポリシーをアタッチする ... 28
管理サービスコンソールのロール作成を簡素化するIAMアクセス許可のカスタムポリシーを作成する ... 29
ドメインに関連付けられたアカウントを管理するアクセス許可のカスタムポリシーを作成する ... 31
(オプション) のカスタムポリシーを作成する AWS ドメインへのSSOユーザーおよびSSOグループのアクセスを追加および削除する Identity Center のアクセス許可 ... 33
(オプション) プリンIAMシパルをキーユーザーとして追加し、 のカスタマーマネージドキーを使用してドメインを作成します。 AWS KMS ... 35
データポータルを使用するために必要なIAMアクセス許可を設定する ... 35
データポータルへのアクセスに必要なポリシーをユーザー、グループ、またはロールにアタッチする ... 36
カタログアクセスに必要なポリシーをユーザー、グループ、またはロールにアタッチする ... 37
ドメインが のカスタマーマネージドキーで暗号化されている場合、データポータルまたはカタログアクセス用のユーザー、グループ、またはロールにオプションのポリシーをアタッチする AWS KMS ... 38
設定 AWS IAM Amazon 用 Identity Center DataZone ... 39
使用開始 ... 41
サンプルを含むクイックスタートガイド AWS Glue データ ... 41
ステップ 1 - Amazon DataZone ドメインとデータポータルを作成する ... 42
ステップ 2 - 公開プロジェクトを作成する ... 44
ステップ 3 - 環境を作成する ... 44
ステップ 4 - 公開用のデータを生成する ... 45
ステップ 5 - からメタデータを収集する AWS 接着語 ... 46
ステップ 6 - データアセットをキュレートして公開する ... 46
ステップ 7 - データ分析用のプロジェクトを作成する ... 46
ステップ 8 - データ分析用の環境を作成する ... 47

ステップ 9 - データカタログを検索してデータをサブスクライブする 47
ステップ 10 - サブスクリプションリクエストを承認する 48
ステップ 11 - Amazon Athena でクエリを構築し、データを分析する 48
サンプル Amazon Redshift データを使用したクイックスタートガイド 48
ステップ 1 - Amazon DataZone ドメインとデータポータルを作成する 49
ステップ 2 - 公開プロジェクトを作成する 51
ステップ 3 - 環境を作成する 51
ステップ 4 - 公開用のデータを生成する 52
ステップ 5 - Amazon Redshift からメタデータを収集する 53
ステップ 6 - データアセットをキュレートして公開する 53
ステップ 7 - データ分析用のプロジェクトを作成する 53
ステップ 8 - データ分析用の環境を作成する 54
ステップ 9 - データカタログを検索してデータをサブスクライブする 55
ステップ 10 - サブスクリプションリクエストを承認する 55
ステップ 11 - Amazon Redshift でクエリを構築し、データを分析する 55
一般的なタスクのサンプルスクリプト 56
Amazon DataZone ドメインとデータポータルを作成する 56
公開プロジェクトを作成する 57
環境プロファイルを作成する 57
環境の作成 59
からメタデータを収集する AWS 接着語 60
データアセットをキュレートして公開する 63
データカタログを検索してデータをサブスクライブする 66
その他の便利なサンプルスクリプト 68
ドメインとユーザーアクセス 70
ドメインの作成 70
ドメインの編集 72
ドメインの削除 73
Amazon の IAM Identity Center を有効にする DataZone 74
Identity Center for Amazon IAM を無効にする DataZone 75
Amazon DataZone コンソールでユーザーを管理する 77
IAM ロールとユーザーの管理 77
SSO ユーザーを管理する 78
SSO グループの管理 80
データポータルでユーザーアクセス許可を管理する 81
ドメインユニットと承認ポリシー 82

ドメイン単位の作成 84
ドメイン単位の編集 84
ドメイン単位の削除 85
ドメイン単位の所有者を管理する 85
ドメイン単位内のユーザーとグループに承認ポリシーを割り当てる 86
ドメイン単位の階層におけるプロジェクトメンバーシップポリシー 87
ドメイン単位内のプロジェクトに承認ポリシーを割り当てる 93
設計図設定内に承認ポリシーを割り当てる 94
組み込みブループリント 96
で組み込みブループリントを有効にする AWS Amazon DataZone ドメインを所有する アカウント 96
で Amazon を信頼されたサービス SageMaker として追加する AWS Amazon DataZone ドメインを所有する アカウント 102
カスタム AWS サービスの設計図 103
カスタムを有効にする AWS サービス設計図 103
カスタム を使用して環境を作成する AWS サービス設計図 104
カスタムでアクションを作成する AWS サービス環境 105
カスタムにプロジェクトメンバーを追加する AWS サービス環境 106
でデータソースを設定する AWS サービス環境 106
でサブスクリプションターゲットを設定する AWS サービス環境 107
関連付けられたアカウント 109
他の との関連付けをリクエストする AWS アカウント 109
カスタマーマネージドKMSキーへのアカウントアクセスを提供する 110
Amazon DataZone ドメインからのアカウント関連付けリクエストを受け入れ、環境ブループリントを有効にする 111
関連付けられた で環境ブループリントを有効にする AWS アカウント 112
関連付けられた に Amazon を信頼されたサービス SageMaker として追加する AWS アカウント 117
Amazon DataZone ドメインからアカウント関連付けリクエストを拒否する 118
関連付けられたアカウントを削除する 118
データカタログ 120
ビジネス用語集を作成する 121
ビジネス用語集を編集する 122
ビジネス用語集を削除する 123
用語集に用語を作成する 123
用語集の用語を編集する 124

用語集の用語を削除する 125
メタデータフォームを作成する 126
メタデータフォームを編集する 127
メタデータフォームを削除する 127
メタデータ形式でフィールドを作成する 128
メタデータフォームのフィールドを編集する 129
メタデータフォームのフィールドを削除する 130
プロジェクトと環境 131
環境プロファイルを作成する 132
環境プロファイルを編集する 134
環境プロファイルを削除する 136
新しい環境を作成する 136
環境を編集する 137
環境を削除する 138
の新規プロジェクトの作成 138
プロジェクトの編集 139
プロジェクトの削除 140
プロジェクトを離れる 141
プロジェクトにメンバーを追加する 142
プロジェクトからメンバーを削除する 143
データインベントリと公開 144
Amazon の Lake Formation アクセス許可を設定する DataZone 145
Amazon と DataZone の統合 AWS Lake Formation ハイブリッドモード 146
カスタムアセットタイプを作成する 149
のデータソースを作成して実行する AWS Glue Data Catalog 154
Amazon Redshift のデータソースを作成して実行する 156
データソースを編集する 159
データソースの削除 160
プロジェクトインベントリからカタログにアセットを発行する 161
アセットを公開する 162
インベントリの管理とアセットのキュレート 162
追加のメタデータフォームをアセットにアタッチする 164
キュレーション後にカタログにアセットを発行する 164
アセットを手動で作成する 165
カタログからアセットを公開解除する 166
アセットを削除する 166

データソースの実行を手動で開始する 167
アセットのバージョニング 168
Amazon のデータ品質 DataZone 169
のデータ品質の有効化 AWS Glue アセット 169
カスタムアセットタイプのデータ品質の有効化 170
機械学習と生成 AI の使用 172
Amazon のデータ系統 DataZone （プレビュー） 174
Amazon の系統ノードのタイプ DataZone 176
系統ノードの主要な属性 176
データ系統の視覚化 177
Amazon でのデータ系統認証 DataZone 178
Amazon でのデータ系統のサンプルエクスペリエンス DataZone 178
Amazon DataZone データ系統をプログラムで使用する 179
データ製品 180
新しいデータ製品を作成する 180
データ製品の公開 181
データ製品を編集する 182
データ製品の公開解除 183
データ製品を削除する 184
データ製品をサブスクライブする 185
サブスクリプションリクエストを確認し、データ製品にサブスクリプションを付与する 185
データ製品を再発行する 186
データ検出、サブスクリプション、消費 188
カタログでアセットを検索して表示する 189
アセットへのサブスクリプションをリクエストする 190
サブスクリプションリクエストを承認または拒否する 191
既存のサブスクリプションを取り消す 192
サブスクリプションリクエストをキャンセルする 193
アセットのサブスクリプションを解除する 194
既存のIAMロールを使用して Amazon DataZone サブスクリプションを満たす 194
マネージド へのアクセスを許可する AWS Glue Data Catalog アセット 197
マネージド Amazon Redshift アセットへのアクセスを許可する 198
承認済みサブスクリプションのアクセスをアンマネージドアセットに許可する 200
Amazon Athena または Amazon Redshift でデータをクエリする 200
Amazon Athena を使用してデータをクエリする 201
Amazon Redshift を使用してデータをクエリする 204

データへのきめ細かなアクセスコントロール 206
行フィルターの作成 207
列フィルターの作成 208
行または列フィルターの削除 209
行または列フィルターの編集 209
フィルターを使用したアクセス許可の付与 210
AWS Glue テーブル 210
Amazon Redshift 211
イベントと通知 212
Amazon DataZone データポータルの専用受信トレイ経由のイベント 212
Amazon EventBridge デフォルトバス経由のイベント 218
セキュリティ 222
データ保護 223
データ暗号化 224
転送中の暗号化 224
ネットワーク間トラフィックのプライバシー 224
Amazon の保管中のデータ暗号化 DataZone 225
Amazon のインターフェイスVPCエンドポイントの使用 DataZone 233
Amazon での認可 DataZone 233
Amazon DataZone コンソールでの承認 234
Amazon DataZone ポータルでの承認 234
Amazon DataZone プロファイルとロール 235
アクセスの制御 235
AWS 管理ポリシー 236
IAM Amazon の ロール DataZone 330
一時認証情報 339
プリンシパル権限 340
コンプライアンス検証 340
セキュリティのベストプラクティス 341
最小特権アクセスの実装 342
IAM ロールを使用する 342
依存リソースでのサーバー側の暗号化の実装 342
CloudTrail を使用してAPI通話をモニタリングする 342
耐障害性 343
データソースの耐障害性 343
アセットレジリエンス 344

アセットタイプとメタデータフォームの耐障害性 344
用語集の耐障害性 344
グローバル検索の耐障害性 344
サブスクリプションの耐障害性 345
環境レジリエンス 345
環境設計図の耐障害性 345
プロジェクトの耐障害性 345
RAM レジリエンス 345
ユーザープロファイル管理の耐障害性 346
ドメインレジリエンス 346
Amazon のインフラストラクチャセキュリティ DataZone 346
Amazon でのサービス間の混乱した代理の防止 DataZone 346
for Amazon での設定と脆弱性の分析 DataZone 347
許可リストに追加するドメイン 347
モニタリング 348
イベントのモニタリング 348
CloudTrail ログ 349
の Amazon DataZone 情報 CloudTrail 349
トラブルシューティング 351
Amazon の AWS Lake Formation 許可のトラブルシューティング DataZone 351
アップストリームデータセットとの Amazon DataZone 系統アセットリンクのトラブルシューティング 354
SourceIdentifier 系統ノード上の 355
Amazon は OpenLineage イベント sourceIdentifier から をどのように DataZone 構築しますか？ 354
代替アプローチ 360
アセット系統ノードのアップストリームの欠如のトラブルシューティング 361
クォータ 365
ドキュメント履歴 367
..... cccxcix

Amazon とは DataZone

Amazon DataZone は、 に保存されているデータのカタログ化、検出、共有、管理を迅速かつ簡単に行うことができるデータ管理サービスです。 AWS、オンプレミス、およびサードパーティーのソース。Amazon を使用すると DataZone、組織のデータアセットを監督する管理者は、きめ細かなコントロールを使用してデータへのアクセスを管理および管理できます。これらのコントロールは、適切なレベルの権限とコンテキストでアクセスを確保するのに役立ちます。Amazon DataZone を使用すると、エンジニア、データサイエンティスト、プロダクトマネージャー、アナリスト、ビジネスユーザーは、組織全体でデータを簡単に共有してアクセスできるため、データ主導型のインサイトを発見、使用、コラボレーションして取得できます。

Amazon DataZone は、Amazon Redshift、Amazon Athena、Amazon などのデータ管理サービスを統合することで、エンドユーザーに直接データを配信し、アーキテクチャを簡素化するのに役立ちます。 QuickSight AWS Glue、 AWS Lake Formation、オンプレミスソース、サードパーティーソースなど。

トピック

- Amazon で何ができますか DataZone？
- Amazon が他の DataZone をサポートおよび統合する方法 AWS サービス？
- Amazon にアクセスするにはどうすればよいですか DataZone？

Amazon で何ができますか DataZone？

Amazon では DataZone、次のことを実行できます。

- 組織の境界を越えてデータアクセスを管理します。Amazon を使用すると DataZone、個々の認証情報に頼ることなく、組織のセキュリティ規制に従って、適切なユーザーが適切な目的で適切なデータにアクセスできるようになります。また、データアセットの使用状況の透明性を提供し、管理されたワークフローでデータサブスクリプションを承認することもできます。使用状況監査機能を使用して、プロジェクト全体のデータアセットをモニタリングすることもできます。
- 共有データとツールを使用してデータワーカーを接続し、ビジネスインサイトを促進します。Amazon を使用すると DataZone、チーム間でシームレスにコラボレーションし、データと分析ツールへのセルフサービスアクセスを提供することで、ビジネスチームの効率を高めることができます。ビジネス用語を使用して、 に保存されているカタログ化されたデータを検索、共有、およびアクセスできます。 AWS、オンプレミス、またはサードパーティープロバイダー。また、Amazon DataZone ビジネス用語集を使用して、使用するデータの詳細を確認できます。

- 機械学習を使用してデータ検出とカタログ化を自動化します。Amazon を使用すると DataZone、ビジネスデータカタログへのデータ属性の手動入力にかかる時間を短縮できます。データカタログの Richer データにより、検索エクスペリエンスも向上します。

Amazon が他の DataZone をサポートおよび統合する方法 AWS サービス？

Amazon DataZone は、他の と 3 種類の統合をサポートしています。 AWS サービス :

- プロデューサーデータソース - に保存されているデータから Amazon DataZone カタログにデータアセットを発行できます。 AWS Glue Data Catalog と Amazon Redshift のテーブルとビュー。Amazon Simple Storage Service (S3) から Amazon DataZone カタログにオブジェクトを手動で発行することもできます。
- コンシューマーツール - Amazon Athena または Amazon Redshift クエリエディタを使用して、データアセットにアクセスして分析できます。
- アクセスコントロールとフルフィルメント - Amazon DataZone は へのアクセスの付与をサポートしています AWS Lake Formation マネージド AWS Glue テーブルと Amazon Redshift テーブルとビュー。他のすべてのデータアセットについては、Amazon はアクション (サブスクリプションリクエストに対する承認など) に関連する標準イベントを Amazon に DataZone 発行します EventBridge。これらの標準イベントを使用して、他の と統合できます。 AWS カスタム統合用のサービスまたはサードパーティーソリューション。

Amazon にアクセスするにはどうすればよいですか DataZone？

Amazon には、次のいずれかの DataZone 方法でアクセスできます。

- Amazon DataZone コンソール

  Amazon DataZone マネジメントコンソールを使用して、Amazon DataZone ドメイン、ブループリント、およびユーザーにアクセスして設定できます。詳細については、https://console.aws.amazon.com「/datazone」を参照してください。Amazon DataZone マネジメントコンソールは、Amazon DataZone データポータルの作成にも使用されます。
- Amazon DataZone データポータル

  Amazon DataZone データポータルは、セルフサービス方式でデータをカタログ化、検出、管理、共有、分析できるブラウザベースのウェブアプリケーションです。データポータルは、 を通じ

て ID プロバイダーの認証情報を使用してユーザーを認証できます。 AWS IAM Identity Center (後継 へ AWS SSO) 、または IAM認証情報を使用します。データポータルを取得するには、https://console.aws.amazon.com/datazone の Amazon DataZone コンソールURLにアクセスします。

- Amazon DataZone HTTPS API

  Amazon を使用して DataZone プログラムで Amazon DataZone HTTPS にアクセスできます。これによりAPI、サービスにHTTPSリクエストを直接発行できます。詳細については、「Amazon DataZone API リファレンス」を参照してください。

Amazon DataZone の用語と概念

Amazon DataZone は、 に保存されているデータのカタログ化、検出、共有、管理を迅速かつ簡単に行うことができるデータ管理サービスです。 AWS、オンプレミス、およびサードパーティーのソース。Amazon を使用すると DataZone、組織のデータアセットを監督する管理者とデータスチュワードは、きめ細かな制御を使用してデータへのアクセスを管理および管理できます。これらのコントロールは、適切なレベルの権限とコンテキストでアクセスを確保するように設計されています。Amazon DataZone では、エンジニア、データサイエンティスト、プロダクトマネージャー、アナリスト、ビジネスユーザーが組織全体のデータに簡単にアクセスできるため、データ主導型のインサイトを発見、使用、コラボレーションできます。

Amazon の使用を開始するときは DataZone、その主要な概念、用語、コンポーネントを理解することが重要です。

トピック

- Amazon DataZone コンポーネント
- Amazon DataZone ドメインとは
- Amazon DataZone のプロジェクトと環境とは
- Amazon DataZone ブループリントとは
- Amazon DataZone インベントリと発行ワークフローとは
- Amazon DataZone サブスクリプションおよびフルフィルメントワークフローとは
- Amazon のユーザーペルソナ DataZone
- Amazon DataZone の用語

Amazon DataZone コンポーネント

Amazon DataZone には、次の 4 つの主要コンポーネントが含まれています。

- ビジネスデータカタログ - このコンポーネントを使用して、組織全体のデータをビジネスコンテキストでカタログ化できるため、組織内のすべてのユーザーがデータをすばやく見つけて理解できます。
- ワークフローの公開とサブスクライブ - これらの自動ワークフローを使用して、プロデューサーとコンシューマー間のデータをセルフサービス方式で保護し、組織内のすべてのユーザーが適切な目的で適切なデータにアクセスできるようにすることができます。
- プロジェクトと環境

- Amazon DataZone プロジェクトでは、人、アセット (データ) 、ツールをビジネスユースケースに基づいてグループ化し、 へのアクセスを簡素化します。 AWS 分析。プロジェクトは、プロジェクトメンバーが共同作業、データ交換、アセットの共有ができる分野を提供します。デフォルトでは、プロジェクトは、プロジェクトに明示的に追加されたユーザーのみが、その中のデータと分析ツールにアクセスできるように設定されています。プロジェクトは、データコンシューマーがアクセスするためのプロジェクトポリシーに従って生成されたアセットの所有権を管理します。
- Amazon DataZone プロジェクト内では、環境は設定済みのリソース (Amazon S3 バケット、AWS Glue データベース、または Amazon Athena ワークグループ) で、特定のIAMプリンシパルのセット (例えば、寄稿者のアクセス許可を持つユーザー) を操作できます。

- データポータル (AWS マネジメントコンソール) - これはブラウザベースのウェブアプリケーションであり、さまざまなユーザーがセルフサービス方式でデータのカタログ化、検出、管理、共有、分析を行うことができます。データポータルは、 を介して ID プロバイダーからのIAM認証情報または既存の認証情報を使用してユーザーを認証します。 AWS IAM Identity Center.

Amazon DataZone ドメインとは

Amazon DataZone ドメインを使用して、アセット、ユーザー、およびプロジェクトを整理できます。追加の を関連付ける AWS Amazon DataZone ドメインの アカウントでは、データソースをまとめることができます。その後、メタデータフォームと用語集を使用して、これらのデータソースからドメインのカタログにアセットを発行し、メタデータの完全性と品質を向上させることができます。これらのアセットを検索して参照し、ドメインで公開されているデータを確認することもできます。さらに、プロジェクトに参加して他のユーザーとコラボレーションしたり、アセットをサブスクライブしたり、プロジェクト環境を使用して Amazon Athena や Amazon Redshift などの分析ツールにアクセスしたりできます。Amazon DataZone ドメインを使用すると、エンタープライズ用に単一の Amazon ドメインを作成する場合でも、 DataZone 異なるビジネスユニット用に複数の Amazon DataZone ドメインを作成する場合でも、組織構造のデータと分析のニーズを柔軟に反映できます。

Amazon DataZone のプロジェクトと環境とは

Amazon DataZone では、チームや分析ユーザーが、チーム、ツール、データのユースケースベースのグループを作成して、プロジェクトでコラボレーションできます。

- Amazon では DataZone、プロジェクトにより、Amazon DataZone カタログ内のデータの公開、検出、サブスクライブ、消費など、さまざまなビジネスユースケースでユーザーのグループがコラボレーションできるようになります。プロジェクトメンバーは Amazon DataZone カタログのア

セットを消費し、1 つ以上の分析ワークフローを使用して新しいアセットを生成します。プロジェクトは、データポータル内の以下のアクティビティをサポートします。

- プロジェクト所有者は、所有者と寄稿者のアクセス許可を持つメンバーを追加できます
- プロジェクトメンバーは、SSOユーザー、SSOグループ、IAMユーザーです
- プロジェクトメンバーがデータカタログ内のアセットへのサブスクリプションをリクエストできる

  サブスクリプションの承認がプロジェクトに提供される

- Amazon DataZone プロジェクトでは、環境は設定済みのリソース (Amazon S3、 AWS Glue データベース、または Amazon Athena ワークグループ) 。これらのリソースを操作できる特定のプリンIAMシパルのセット。環境は、環境を作成するための再利用可能なテンプレートを提供する事前設定されたリソースとブループリントのセットである環境プロファイルを使用して作成されます。環境プロファイルは、 などの設定を定義します。 AWS アカウント 環境がデプロイされている またはリージョン。

Amazon DataZone ブループリントとは

環境が作成されるブループリントは、何を定義しますか AWS ツールとサービス (例： AWS Glue または Amazon Redshift) 環境が属するプロジェクトのメンバーは、Amazon DataZone カタログ内のアセットを操作するときに を使用できます。

Amazon の現在のリリースでは DataZone、以下のデフォルトのブループリントがサポートされています。

設計図名	説明	作成されたリソース
Data Lake の設計図	Amazon DataZone プロジェクトメンバーが 環境内で Data Lake プロデューサーおよびコンシューマーサービスを起動できるようにします。 コンシューマー として、Amazon DataZone プロジェクトメンバーは、Amazon Athena および Lake Formation	Amazon Athena を使用して Lake Formation テーブルを作成およびクエリする機能をユーザーに提供します。Amazon Athena ワークグループ、 AWS Glue 「読み取り専用」Lake Formation 許可、「読み取り専用IAM」許可、およびプロジェクトによって管理される Amazon S3

設計図名	説明	作成されたリソース
	がサポートする他のクエリエンジンで、Lake Formation が管理するアセットの「読み取り専用」コピーに直接アクセスできます。 プロデューサー として、Amazon DataZone プロジェクトメンバーは Amazon Athena を使用して新しい LakeFormationマネージドテーブルを作成し、Amazon DataZone カタログに公開できます。	へのアクセスを持つ データベース。 AWS Glue 「作成」と「付与」の Lake Formation 許可、「読み取り」と「書き込みIAM」許可を持つ データベース、 AWS Glue ETL タグ付けによる (抽出、変換、ロード) 。
データウェアハウスの設計図	コンシューマー として、このブループリントにより、Amazon DataZone プロジェクトメンバーは独自の Amazon Redshift クラスターに接続してリモートデータストアをクエリし、新しいデータセットを作成して保存できます。 プロデューサー として、このブループリントにより、Amazon DataZone プロジェクトメンバーは独自の Amazon Redshift クラスターに接続して、リモートデータストアをクエリし、新しいデータセットを作成し、Amazon DataZone カタログに公開できます。	Amazon Redshift クエリエディタへのアクセス、Amazon DataZone カタログからサブスクライブされたデータソースへの「読み取り」アクセス、設定された Amazon Redshift クラスターにローカルアセットを作成する機能。Amazon Redshift クエリエディタへのアクセス、Amazon DataZone カタログからサブスクライブされたデータソースへの「読み取り」アクセス、設定された Amazon Redshift クラスターからアセットを作成および発行する機能。

設計図名	説明	作成されたリソース
Amazon Sagemaker の設計図	このブループリントは、データプロデューサーとコンシューマーがシームレスに Amazon に切り替え SageMaker て機械学習 (ML) プロジェクトで共同作業を行い、データや ML アセットへのアクセスガバナンスを実施するのに役立ちます。Amazon DataZone と Amazon の新しい組み込み統合により SageMaker、データコンシューマーとプロデューサーは、インフラストラクチャのセットアップ全体の ML ガバナンスを合理化し、ビジネスイニシアチブに共同作業を行い、データと ML アセットを簡単に管理できます。	Amazon でデータおよび ML アセットを検索、サブスクライブ、公開できる Amazon SageMaker ドメインを作成できます DataZone。をサブスクライブして に発行することもできます。 AWS Glue データベースと設定されたレイクフォーメーション。

Amazon DataZone インベントリと発行ワークフローとは

プロジェクトインベントリアセットの作成

Amazon を使用してデータを DataZone カタログ化するには、まずデータ (アセット) を Amazon のプロジェクトのインベントリとして持ち込む必要があります DataZone。プロジェクトのインベントリを作成すると、そのプロジェクトのメンバーのみがアセットを検出できるようになります。プロジェクトインベントリアセットは、明示的に公開されていない限り、検索/閲覧のすべてのドメインユーザーが利用できるわけではありません。Amazon の現在のリリースでは DataZone、次の方法でプロジェクトインベントリにアセットを追加できます。

- データポータルまたは Amazon を使用してデータソースを作成して実行します DataZone APIs。Amazon の現在のリリースでは DataZone、 のデータソースを作成して実行できます。AWS Glue と Amazon Redshift。を作成して実行する AWS Glue または Amazon Redshift データ

ソースでは、選択したプロジェクトインベントリにアセットを作成し、その技術メタデータをソースデータベーステーブルまたはデータウェアハウスからインベントリとして Amazon にインポートします DataZone。

- を使用してAPIs、使用可能なシステムアセットタイプ (AWS Glue、Amazon Redshift、Amazon S3 オブジェクト) 、またはカスタムアセットタイプから。
  - Amazon を使用して、プロジェクトインベントリにカスタムアセットタイプを作成します DataZone APIs。カスタムアセットタイプには、ML モデル、ダッシュボード、オンプレミステーブルなどが含まれます。
  - Amazon を使用して、これらのカスタムアセットタイプからアセットを作成します DataZone APIs。
- Amazon DataZone データポータルを使用して、S3 オブジェクトのアセットを手動で作成します。

プロジェクトインベントリアセットのキュレーション - プロジェクトインベントリを作成した後、データ所有者は、ビジネス名 (アセットとスキーマ) 、説明 (アセットとスキーマ) 、読み上げ、用語集用語 (アセットとスキーマ) 、メタデータフォームを追加または更新することで、必要なビジネスメタデータでインベントリアセットをキュレートできます。これは、データポータルまたは Amazon を使用して実行できます DataZone APIs。アセットを編集するたびに、新しいインベントリバージョンが作成されます。

Amazon DataZone カタログへのプロジェクトインベントリアセットの発行

Amazon を使用してデータを DataZone カタログ化する次のステップは、プロジェクトのインベントリアセットをドメインユーザーが検出できるようにすることです。これを行うには、インベントリアセットを Amazon DataZone カタログに発行します。インベントリアセットの最新バージョンのみをカタログに公開でき、最新の公開バージョンのみが検出カタログでアクティブになります。インベントリアセットが Amazon DataZone カタログに公開された後に更新された場合は、最新バージョンが検出カタログに含まれるように、インベントリアセットを再度明示的に公開する必要があります。Amazon の現在のリリースでは DataZone、次の方法でプロジェクトインベントリアセットを Amazon DataZone カタログに公開できます。

- データポータルまたは Amazon を使用して、プロジェクトインベントリアセットを Amazon DataZone カタログに手動で公開します DataZone APIs。
- データソースの作成または編集の一環として、オプションの「 の発行」を有効にします。 AWS アセットをカタログに Glue するか、Amazon Redshift アセットをカタログ設定に公開して、スケジュールされたデータソースまたは自動化されたデータソースの実行中に使用します。この設定を

有効にすると、データソースの実行によってプロジェクトのインベントリにアセットが追加され、インベントリアセットも Amazon DataZone カタログに発行されます。直接公開すると、アセットにビジネスメタデータがない可能性があり、すべてのドメインユーザーが直接検出できるようになります。この設定は、データポータルまたは Amazon を使用してデータソースで使用できます DataZone APIs。

Amazon DataZone サブスクリプションおよびフルフィルメントワークフローとは

アセットが Amazon DataZone カタログに公開されると、ドメインユーザーはこれらのアセットを検出し、これらのアセットをリクエストしてアクセスし、引き続き Amazon を使用してこれらのアセット DataZone を管理、共有、分析できます。

ユーザーは、プロジェクトに代わってそのアセットにサブスクライブすることで、アセットへのアクセスをリクエストします。サブスクリプションリクエストが作成されると、アセットの所有者は通知を受け取り、サブスクリプションリクエストを確認して、承認または拒否するかどうかを決定できます。サブスクリプションリクエストがデータ所有者によって承認されると、サブスクライブするプロジェクトにそのアセットへのアクセス権が付与されます。

サブスクリプションリクエストが承認されると、Amazon はサブスクリプションフルフィルメントワークフロー DataZone を開始し、必要な許可を で作成して、プロジェクト内のすべての該当する環境にアセットを自動的に追加します。 AWS Lake Formation または Amazon Redshift。これにより、サブスクライブしているプロジェクトメンバーは、環境内のクエリツール (Amazon Athena または Amazon Redshift クエリエディタ) のいずれかを使用してアセットをクエリできます。

Amazon はこの自動フルフィルメントロジックをマネージドアセットに対してのみトリガー DataZone できます (これには、 AWS Glue テーブルと Amazon Redshift テーブルとビュー) 。他のすべてのアセットタイプ (アンマネージドアセット) の場合、Amazon DataZone は自動的にフルフィルメントをトリガーすることはできませんが、代わりにイベントペイロードに必要なすべての詳細を含むイベントを Amazon Eventbridge に発行して、Amazon の外部で必要な許可を作成できるようにします DataZone。また、Amazon は、サブスクリプションが Amazon の外部で受理された後にサブスクリプションのステータスを更新して、Amazon がプロジェクトメンバー DataZone にアセットの使用を開始 DataZone できることを通知する`updateSubscriptionStatus`APIことができる DataZone も提供します。

Amazon のユーザーペルソナ DataZone

Amazon DataZone ユーザーの主なペルソナは次のとおりです。

- Amazon を組織の分析プラットフォーム DataZone として設定するドメイン管理者。

  Amazon のコンテキストでは DataZone、ドメイン管理者は に Amazon をインストール DataZone します。 AWS アカウント、Amazon DataZone ドメインの作成、設定 AWS アカウントの関連付けと ID プロバイダーの Amazon DataZone ドメインとの関連付け。ドメイン管理者は他の も使用します。 AWS などの サービスコンソール AWS Amazon を設定するための Organization と Service Catalog DataZone。
- 分析および機械学習タスクの Amazon DataZone （ アセットパブリッシャーおよびサブスクライバー) の主なユーザーであるデータユーザー。

  データユーザーには、データアセットを生成して使用するデータ分析ワーカー、データサイエンティスト、システムユーザーが含まれます。Amazon のコンテキストでは DataZone、データユーザーはプロジェクトと環境を作成および結合し、事前設定された分析または機械学習ツールを使用してデータアセットをサブスクライブおよび消費し、出力データアセットを Amazon DataZone ドメインカタログに公開して他のユーザーと共有します。
- カスタムインフラストラクチャテンプレートを構築し、Amazon DataZone を内部カタログまたは本番システムと統合するシステムデベロッパー。

  Amazon のコンテキストでは DataZone、システムデベロッパーは環境設計図 (インフラストラクチャテンプレート) または Infrastructure-As-Code CI/CD パイプラインを環境プロバイダーとして構築します。データパイプラインは、環境間でデータアセットを昇格させます。カタログ同期およびサブスクリプション許可フルフィルメントアダプターは、内部カタログと統合します。必要に応じて、Amazon DataZone APIs と内部ユーザーインターフェイスまたは本番システムの統合を行います。
- 組織のセキュリティ、プライバシー、その他のコンプライアンスポリシーの定義とリスクを所有し、組織 DataZone 内での Amazon の使用がこれらの定義に準拠していることを確認するデータガバナンス責任者。

Amazon DataZone の用語

[ドメイン]

Amazon DataZone ドメインは、アセット、ユーザー、およびそれらのプロジェクトを連結するための組織エンティティです。Amazon DataZone ドメインを使用すると、エンタープライズ用の単一の Amazon ドメインを作成するか、複数のデータゾーンを作成するか、異なるビジネスユニットやチーム用のドメインを作成する DataZoneかにかかわらず、組織構造のデータと分析のニーズを柔軟に反映できます。

ドメイン単位

ドメインユニットを使用すると、アセットやその他のドメインエンティティを特定のビジネスユニットやチームで簡単に整理できます。組織のビジネスユニット間で安全かつ効率的なデータ共有を設定するには、Amazon 内でドメインユニットを作成し、各ビジネスユニット内の選択したユーザーがカタログにログインしてアセットを共有 DataZone できるようにします。ドメインユニットを使用して、 などのリソース所有者を有効にすることもできます。 AWS アカウント所有者は、リソースに Amazon DataZone 認証アクセス許可を設定します。ドメインユニットは、アカウント所有者からドメインユニット所有者に委任された権限を提供し、アカウント所有者に代わって環境プロファイル (設計図設定を使用して作成された) に認証権限を設定できます。詳細については、「Amazon のドメインユニットと承認ポリシー DataZone」を参照してください。

承認ポリシー

Amazon DataZone 認証ポリシーは、プロジェクト、ブループリント、環境、用語集、メタデータフォームなどのエンティティ DataZone に適用される Amazon 内の一連のコントロールです。これらのポリシーは、Amazon DataZone ポータルでこれらのエンティティを作成し、そのライフサイクルを管理できるユーザーを定義します。

Amazon DataZone ドメインユニット内で、ユーザーとグループに次の承認ポリシーを割り当てて、ユーザーに特定のアクセス許可を付与できます。

- ドメイン単位作成ポリシー
- プロジェクト作成ポリシー
- プロジェクトメンバーシップポリシー
- ドメイン単位の所有権の引き受けポリシー
- プロジェクト所有権の引き受けポリシー

詳細については、「Amazon DataZone ドメイン単位内のユーザーとグループに承認ポリシーを割り当てる」を参照してください。

Amazon DataZone ドメインユニット内で、次の承認ポリシーをプロジェクトに割り当てて、特定のアクセス許可を付与できます。

- 用語集作成ポリシー
- メタデータフォーム作成ポリシー
- カスタムアセットタイプ作成ポリシー

詳細については、「Amazon DataZone ドメイン単位内のプロジェクトに承認ポリシーを割り当てる」を参照してください。

特定のブループリント設定内で、プロジェクトとドメイン単位の所有者に次の承認ポリシーを割り当てることができます。

- このブループリントを使用して環境プロファイルを作成する - このポリシーは Amazon DataZone プロジェクトに割り当てることができ、このブループリントを使用して環境プロファイルを作成することを承認します。
- このブループリントを使用して環境プロファイルを作成するアクセス許可を付与する - このポリシーはドメイン単位の所有者に割り当てることができ、このブループリントを使用して環境プロファイルを作成するアクセス許可をプロジェクトに付与することを承認します。

詳細については、「Amazon DataZone ブループリント設定内で承認ポリシーを割り当てる」を参照してください。

関連付けられたアカウント

の関連付け AWS Amazon DataZone ドメインを持つ アカウントでは、これらの からのデータを発行できます。 AWS アカウントを Amazon DataZone カタログに追加し、複数の にまたがるデータを操作するための Amazon DataZone プロジェクトを作成します。 AWS アカウント。アカウント関連付けリクエストは、 でのみ開始できます。 AWS Amazon DataZone ドメインを所有する アカウント。アカウント関連付けリクエストは、招待された の管理ユーザーのみが受け入れることができます。 AWS アカウント。の 1 回 AWS アカウントは Amazon DataZone ドメインに関連付けられており、 などのデータソースを登録できます。 AWS このアカウントの Glue カタログと Amazon Redshift をこのドメインに。関連付けられると、 も有効になります。 AWS Amazon DataZone プロジェクトと環境を作成するための アカウント。

An AWS アカウント は、1 つ以上の Amazon DataZone ドメインに関連付けることができます。

データソース

Amazon では DataZone、データソースを使用して、ソースデータベースまたはデータウェアハウスから Amazon にアセット (データ) の技術メタデータをインポートできます DataZone。Amazon の現在のリリースでは DataZone、 のデータソースを作成して実行できま

す。 AWS Glue と Amazon Redshift。データソースを作成することで、Amazon DataZone とソース (AWS Glue Data Catalog または Amazon Redshift ウェアハウス) を使用して、テーブル名、列名、データ型などの技術的なメタデータを読み取ることができます。データソースを作成することで、Amazon で新しいアセットを作成または既存のアセットを更新する最初のデータソース実行も開始します DataZone。データソースの作成中またはデータソースが正常に作成された後に、データソースの実行スケジュールを指定するオプションもあります。

データソースの実行

Amazon では DataZone、データソースの実行は、プロジェクトインベントリにアセットを作成し、オプションでプロジェクトインベントリアセットを Amazon DataZone カタログに発行するために Amazon が DataZone 実行するタスクです。データソースの実行は、自動 (データソースが最初に作成されたときに開始) でも、スケジュールまたは手動でもかまいません。データ選択基準を使用すると、プロジェクトインベントリまたは Amazon DataZone カタログに取り込む既存および将来のデータセットと、それらのインベントリまたはカタログアセットへのメタデータ更新の頻度を微調整できます。

サブスクリプションターゲット

Amazon では DataZone、サブスクリプションターゲットを使用すると、プロジェクトでサブスクライブしたデータにアクセスできます。サブスクリプションターゲットは、Amazon がソースデータとの接続を確立し、Amazon DataZone プロジェクトのメンバーがサブスクライブしたデータのクエリを開始できるように、必要な許可を作成するために DataZone 使用できる場所 (データベースやスキーマなど) と必要なアクセス許可 (IAMロールなど) を指定します。

サブスクリプションリクエスト

Amazon では DataZone、サブスクリプションリクエストは、Amazon DataZone プロジェクトが特定のアセットへのアクセスを許可するために従う必要があるプロセスです。サブスクリプションリクエストは、承認、拒否、取り消し、または付与できます。

[アセット]

Amazon では DataZone、アセットは、単一の物理データオブジェクト (テーブル、ダッシュボード、ファイルなど) または仮想データオブジェクト (ビューなど) を表示するエンティティです。

アセットタイプ

アセットタイプは、Amazon DataZone カタログでのアセットの表現方法を定義します。アセットタイプは、特定のタイプのアセットのスキーマを定義します。アセットが作成されると、アセットタイプ (デフォルトでは最新バージョン) で定義されたスキーマに対して検証されます。アセットの更新が発生すると、Amazon DataZone は新しいアセットバージョンを作成し、Amazon DataZone ユーザーがすべてのアセットバージョンを操作できるようにします。

ビジネス用語集

Amazon では DataZone、ビジネス用語集は、アセットに関連する可能性のあるビジネス用語のコレクションです。ビジネス用語集は、さまざまなデータ分析タスクを通じて組織全体で同じ用語と定義が使用されるようにするのに役立ちます。

ビジネス用語集の用語をアセットや列に追加して、検索中にそれらの属性を分類または識別を強化できます。用語集は、アセットに関連付けられているメタデータフォームのフィールドの値タイプとして選択できます。アセットのメタデータフォームフィールドの値として特定の用語を選択すると、ユーザーはビジネス用語集の用語を検索し、関連するアセットを検索できます。

メタデータフォームタイプ

メタデータフォームタイプは、アセットがインベントリとして作成されたとき、または Amazon DataZone ドメインで公開されたときに収集および保存されるメタデータを定義するテンプレートです。メタデータフォームタイプは、データアセットに関連付けることができます。メタデータフォームタイプは、ドメイン管理者がコンプライアンス情報、規制情報、分類など、そのドメインに必要なメタデータフォームを定義するのに役立ちます。これにより、ドメイン管理者はアセットの追加メタデータをカスタマイズできます。Amazon DataZone には、 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-type、 object-collection-form-type subscription-terms-form-typeなどのシステムメタデータフォームタイプがあります suggestion-form-type。

メタデータフォーム

Amazon では DataZone、メタデータフォームは、アセットがインベントリとして作成されたとき、または Amazon DataZone ドメインで公開されたときに収集および保存されるメタデータを定義します。メタデータフォーム定義は、ドメイン管理者がカタログドメインに作成します。メタデータフォーム定義は 1 つ以上のフィールド定義で構成され、ブール値、日付、10 進数、整数、文字列、ビジネス用語集フィールド値データ型がサポートされています。

ドメイン管理者は、ドメインにメタデータフォームを追加して、ドメイン内のアセットにメタデータフォームを適用します。アセットパブリッシャーは、メタデータフォームにオプションおよび必須のフィールド値を提供します。

プロジェクト

Amazon では DataZone、プロジェクトでは、プロジェクトインベントリにアセットを作成してすべてのプロジェクトメンバーが検出できるようにし、Amazon DataZone カタログでアセットを公開、検出、サブスクライブ、消費することを含むさまざまなビジネスユースケースでユー

ザーのグループがコラボレーションできます。プロジェクトメンバーは Amazon DataZone カタログのアセットを消費し、1 つ以上の分析ワークフローを使用して新しいアセットを生成します。プロジェクトメンバーは、所有者または寄稿者です。プロジェクト所有者は、他のユーザーを所有者または寄稿者として追加または削除したり、プロジェクトを変更または削除したりできます。寄稿者に対するその他の制限は、 ポリシーで定義できます。ユーザーがプロジェクトを作成すると、そのプロジェクトの最初の所有者になります。

環境

環境は、設定されたリソース (Amazon S3 バケット、 AWS Glue データベース、または Amazon Athena ワークグループ) 。これらのリソースを操作できる特定のIAMプリンシパルのセット (寄稿者アクセス許可が付与されている) 。各環境には、 リソースへのアクセスと、サブスクリプションとフルフィルメントを介してデータへのアクセスを許可されたユーザープリンシパルがいる場合もあります。環境は、実用的なリンクを に保存できるように設計されています。AWS サービス、外部 IDEsおよびコンソール。プロジェクトのメンバーは、 環境内で設定されたディープリンクを介して、Amazon Athena コンソールなどのサービスにアクセスできます。SSO ユーザーとプロジェクトのIAMユーザーは、特定の環境を使用/アクセスするようにさらに絞り込むことができます。

環境プロファイル

Amazon では DataZone、環境プロファイルは環境の作成に使用できるテンプレートです。環境プロファイルは、ブループリントを使用して作成されます。

環境プロファイルを使用すると、ドメイン管理者は設計図を事前設定されたパラメータでラップでき、データワーカーは既存の環境プロファイルを選択し、新しい環境の名前を指定することで、任意の数の新しい環境をすばやく作成できます。これにより、データワーカーは、ドメイン管理者によって適用されるデータガバナンスポリシーを確実に満たすと同時に、プロジェクトと環境を効率的に管理できます。

ブループリント

環境が作成されるブループリントは、何を定義しますか AWS ツールとサービス (例： AWS Glue または Amazon Redshift) 環境が属するプロジェクトのメンバーは、Amazon DataZone カタログ内のアセットを操作するときに を使用できます。

Amazon の現在のリリースでは DataZone 、以下のデフォルトのブループリントがサポートされています。

- データレイクの設計図
- データウェアハウスの設計図

- Amazon Sagemaker の設計図

ユーザープロファイル

ユーザープロファイルは Amazon DataZone ユーザーを表します。Amazon DataZone は、さまざまな目的で Amazon SSO DataZone マネジメントコンソールとデータポータルとやり取りするためのIAMロールと ID の両方をサポートしています。ドメイン管理者は、IAMロールを使用して、新しい Amazon ドメインの作成、メタデータフォームタイプの設定、ポリシーの実装など、Amazon DataZone マネジメントコンソールで最初の管理 DataZone ドメイン関連の作業を実行します。データワーカーは Identity Center 経由でSSO企業 ID を使用して Amazon DataZone Data Portal にログインし、メンバーシップがあるプロジェクトにアクセスします。

グループプロファイル

グループプロファイルは、Amazon DataZone ユーザーのグループを表します。グループは手動で作成することも、エンタープライズ顧客の Active Directory グループにマッピングすることもできます。Amazon では DataZone、グループは 2 つの目的を果たします。まず、グループは組織図のユーザーのチームにマッピングできるため、チームに加わったり退出したりする新しい従業員がいる場合の Amazon DataZone プロジェクト所有者の管理作業を減らすことができます。次に、企業管理者は Active Directory グループを使用してユーザーステータスを管理および更新するため、Amazon DataZone ドメイン管理者はこれらのグループメンバーシップを使用して Amazon DataZone ドメインポリシーを実装できます。

ドメイン管理者

Amazon では DataZone、Amazon DataZone ドメインを作成するIAMプリンシパルが、そのドメインのデフォルトのドメイン管理者です。Amazon のドメイン管理者は、ドメインの作成、他のドメイン管理者の割り当て、データソースとサブスクリプションターゲットの追加、プロジェクトと環境の作成、プロジェクト所有者の割り当てなど、ドメインの主要な機能 DataZone を実行します。

パブリッシャー

Amazon では DataZone、パブリッシャーは Amazon DataZone カタログにアセットを発行し、パブリッシュするアセットのメタデータを編集できます。この権限が付与されると、パブリッシャーは Amazon DataZone カタログで公開したアセットへのサブスクリプションリクエストを承認または拒否できます。

サブスクライバー

Amazon では DataZone、サブスクライバーは Amazon DataZone カタログ内のアセットを検索、アクセス、消費したい Amazon DataZone プロジェクトです。

AWS アカウント owner (オーナー)

Amazon では DataZone、 AWS アカウント 所有者は、 でロール、ポリシー、アクセス許可を作成します。 AWS アカウント これらの を有効にする AWS アカウント Amazon DataZone ドメインに関連付けられる 。

Amazon の新機能 DataZone

このセクションでは、Amazon の新機能と改善点をリリース日 DataZone 別に説明します。

トピック

- 2024
- 2023

2024

Amazon がドメインユニットと承認ポリシー DataZone を起動する

08/12/2024 にリリース

Amazon では、お客様がビジネスユニット/チームレベルの組織を作成し、ビジネスニーズに応じてポリシーを管理できるようにする、ドメイン単位と承認ポリシーと呼ばれる一連の新しいデータガバナンス機能 DataZone が導入されています。ドメインユニットを追加すると、ユーザーはビジネスユニットやチームに関連するデータアセットやプロジェクトを整理、作成、検索、検索できます。承認ポリシーを使用すると、これらのドメイン単位ユーザーは、Amazon 内でプロジェクト、用語集、およびコンピューティングリソースを使用するためのアクセスポリシーを設定できます DataZone。詳細については、「Amazon のドメインユニットと承認ポリシー DataZone」を参照してください。

Amazon がデータ製品 DataZone を起動

08/05/2024 にリリース

Amazon はデータ製品 DataZone を導入し、データアセットを特定のビジネスユースケースに合わせた明確に定義された自己完結型のパッケージにグループ化できるようにします。例えば、マーケティング分析データ製品は、マーケティングキャンペーンデータ、パイプラインデータ、顧客データなど、さまざまなデータアセットをバンドルできます。データ製品を使用すると、お客様は検出プロセスとサブスクリプションプロセスを簡素化し、ビジネス目標に合わせて調整し、個々のアセットの処理の冗長性を軽減できます。詳細については、「Amazon DataZone データ製品 」を参照してください。

Amazon がきめ細かなアクセスコントロール機能 DataZone を起動

07/02/2024 にリリース

Amazon DataZone はきめ細かなアクセスコントロールを導入し、データレイクとデータウェアハウス全体で Amazon のビジネスデータカタログのデータアセット DataZoneをきめ細かく制御できるようになりました。新機能により、データ所有者は、データアセット全体へのアクセス権を付与するのではなく、行レベルと列レベルで特定のデータレコードへのアクセスを制限できるようになりました。例えば、データに個人を特定できる情報 (PII) などの機密情報を含む列が含まれている場合、必要な列のみへのアクセスを制限して、機密情報を保護しながら、機密性の高いデータへのアクセスを許可できます。同様に、行レベルでアクセスを制御できるため、ユーザーは自分のロールまたはタスクに関連するレコードのみを表示できます。詳細については、「Amazon のデータへのきめ細かなアクセスコントロール DataZone」を参照してください

Amazon がデータ系統機能 DataZone を起動

06/27/2024 にリリース

Amazon はプレビューでデータ系統 DataZone を起動し、 対応システムから、または OpenLineage を介して系統イベントを視覚化APIし、ソースから消費へのデータ移動を追跡するのに役立ちます。Amazon DataZoneの OpenLineageと互換性のある を使用するとAPIs、ドメイン管理者とデータプロデューサーは、Amazon S3 での変換など DataZone、Amazon で利用できるものを超える系統イベントをキャプチャして保存できます。 AWS Glue およびその他の サービス。さらに、Amazon DataZone バージョンは各イベントに系統付けられており、ユーザーは任意の時点で系統を視覚化したり、アセットまたはジョブの履歴全体の変換を比較したりできます。この過去の系統は、データアセットの整合性のトラブルシューティング、監査、検証に不可欠な、データがどのように進化したかをより深く理解するのに役立ちます。詳細については、「Amazon のデータ系統 DataZone （プレビュー）」を参照してください

Amazon がカスタム DataZone を起動 AWS サービスの設計図

06/17/2024 にリリース

カスタム を使用する AWS 既存の がある場合は、 サービスのブループリント AWS IAM ロール、データレイク、データメッシュ、Amazon S3 バケット、Amazon Redshift クラスターなどの リソースでは、独自のカスタムIAMロールを使用してこれらの既存のリソースへのアクセス許可を指定できるようになりました。これにより、Amazon DataZone ユーザーはパブリケーションとサブスクリプションを活用してこれらのリソースを共有および管理できます。カスタム を使用する AWS サービスブループリント、Amazon DataZone 管理者は を設定できます AWS 独自のカスタムロールを使用する サービス環境。これらの のアクションリンクを設定できます。 AWS サービス環境により、既存の へのフェデレーションアクセスが提供されます。 AWS リソースの使用料金を見積もることができます。これらのカスタム でサブスクリプションターゲットとデータソースを設定することもで

きます。 AWS サービス環境。管理者は を設定できます AWS 独自の Amazon DataZone ドメイン アカウント、またはデータを発行、サブスクライブ、検出、管理したい関連アカウントの サービス環境。詳細については、「Amazon DataZone カスタム AWS サービスの設計図 」を参照してください。

データソース作成フローの強化

06/10/2024 にリリース

Amazon DataZone は、データソース作成フローの機能強化を追加し、データプロデューサーのアクセス管理を簡素化しました。これらの更新により、データプロデューサーが を公開するためのデータソースを作成するとき AWS Glue および Amazon Redshift アセットでは、Amazon はプロジェクトメンバーに読み取り専用アクセス許可 DataZone を付与します。を作成する場合 AWS Glue データソース、Amazon はデータソースの作成に使用される環境のIAMロールに「読み取り専用」アクセス許可 DataZone を自動的に付与し、関連付けられた 内のすべてのテーブルへのアクセスを許可します。 AWS Glue データベース。同様に、Amazon Redshift データソースの場合、Amazon はデータソースで使用される Amazon Redshift スキーマ内のすべてのテーブルへの読み取り専用アクセス DataZone を許可します。詳細については、「の Amazon DataZone データソースを作成して実行する AWS Glue Data Catalog」および「Amazon Redshift の Amazon DataZone データソースを作成して実行する」を参照してください。

Amazon が Amazon との統合 DataZone を開始 SageMaker

05/06/2024 にリリース

Amazon は Amazon SageMaker との統合 DataZone を開始して、データプロデューサーとコンシューマーが Amazon にシームレスに切り替え SageMaker て機械学習 (ML) プロジェクトで共同作業を行い、データおよび ML アセットへのアクセスガバナンスを強制できるようにします。Amazon DataZone と Amazon の新しい組み込み統合により SageMaker、データコンシューマーとプロデューサーは、インフラストラクチャのセットアップ全体の ML ガバナンスを合理化し、ビジネスイニシアチブに共同作業し、データと ML アセットを簡単に管理できます。詳細については、「Amazon DataZone 組み込みブループリント」および「Amazon の関連アカウント DataZone」を参照してください。

Amazon が との統合 DataZone を開始 AWS Lake Formation ハイブリッドアクセスモード

04/03/2024 にリリース

Amazon DataZone は との統合を導入しました AWS Lake Formation ハイブリッドアクセスモード。この統合により、 を簡単に公開および共有できます。 AWS で登録しなくても DataZone、Amazon を介してテーブルを Glue で登録できます。 AWS Lake Formation を最初に使用します。開始するには、管理者は Amazon DataZone コンソールの`DefaultDataLake`ブループリントでデータロケーション登録設定を有効にします。次に、データコンシューマーが にサブスクライブすると、 AWS アクセスIAM許可によって管理される Glue テーブル。Amazon は DataZone まずこのテーブルの Amazon S3 ロケーションをハイブリッドモードで登録し、 を介してテーブルに対するアクセス許可を管理することでデータコンシューマーへのアクセスを許可します。 AWS Lake Formation。これにより、新しく付与された でテーブルに対するIAMアクセス許可が引き続き存在するようになります。 AWS 既存のワークフローを中断することなく、Lake Formation のアクセス許可。詳細については、「Amazon と DataZone の統合 AWS Lake Formation ハイブリッドモード 」を参照してください。

Amazon が との統合 DataZone を開始 AWS Glue データ品質

04/03/2024 にリリース

Amazon が との統合 DataZone を開始 AWS Glue Data Quality と はAPIs、サードパーティーのデータ品質ソリューションのデータ品質メトリクスを統合するための を提供しています。新しい統合により、 を自動発行できます。 AWS Data Quality スコアを Amazon DataZone ビジネスデータカタログにまとめます。Amazon DataZone APIs は、サードパーティーのソースから品質メトリクスを取り込むために使用できます。公開されると、データコンシューマーはデータアセットを簡単に検索し、きめ細かな品質メトリクスを表示し、失敗したチェックとルールを特定できるため、ビジネス上の意思決定に役立ちます。詳細については、「Amazon のデータ品質 DataZone」を参照してください。

Amazon での説明に関する AI レコメンデーションの一般提供リリース DataZone

03/27/2024 にリリース

Amazon は、ビジネスデータカタログを強化することで、データ検出、データ理解、データ使用量を向上させるための新しい生成 AI ベースの機能の一般提供リリース DataZone を発表しました。ワンクリックで、データプロデューサーは包括的なビジネスデータの説明とコンテキストを生成し、影響のある列を強調し、分析ユースケースに関するレコメンデーションを含めることができます。起動により、データプロデューサーAPIsがアセットの説明をプログラムで生成するために使用できる のサポートが追加されました。詳細については、「機械学習と生成 AI の使用」を参照してください。

Amazon が Amazon Redshift 統合の機能強化 DataZone を開始

03/21/2024 にリリース

Amazon DataZone では、Amazon Redshift の統合にいくつかの機能強化が導入され、Amazon Redshift テーブルとビューの公開とサブスクライブのプロセスが簡素化されました。これらの更新により、データプロデューサーとコンシューマーの両方のエクスペリエンスが効率化され、Amazon DataZone 管理者が提供する事前設定された認証情報と接続パラメータを使用してデータウェアハウス環境をすばやく作成できます。さらに、これらの機能強化により、管理者は自分の 内のリソースを使用できるユーザーをより詳細に制御できます。 AWS アカウントと Amazon Redshift クラスター、および目的。

- ブループリント設定 : `DefaultDataWarehouseBlueprint`ブループリントを有効にすると、有効な`DefaultDataWarehouseBlueprint`ブループリントに管理プロジェクトを割り当てることで、アカウントでブループリントを使用して環境プロファイルを作成できるプロジェクトを制御できます。クラスター、データベース、 などのパラメータを指定`DefaultDataWarehouseBlueprint`して、 の上にパラメータセットを作成することもできます。 AWS シークレット。また、 AWS Amazon DataZone コンソール内からのシークレット。
- 環境プロファイル : 環境プロファイルを作成するときに、独自の Amazon Redshift パラメータを指定するか、設計図設定からパラメータセットのいずれかを使用できます。設計図設定で作成されたパラメータセットを使用する場合は、 AWS シークレットには`AmazonDataZoneDomain`タグのみが必要です (`AmazonDataZoneProject`タグは、環境プロファイルで独自のパラメータセットを指定する場合にのみ必要です) 。環境プロファイルでは、承認されたプロジェクトのリストを指定できます。この環境プロファイルを使用してデータウェアハウス環境を作成できるのは、承認されたプロジェクトのみです。どのデータ認可プロジェクトを公開できるかを指定することもできます。現在、次のオプションのいずれかを選択できます。1) 任意のスキーマから発行する、2) デフォルトの環境スキーマから発行する、3) 発行を許可しない。
- 環境 : データプロデューサーまたはコンシューマーは、 を含む独自の Amazon Redshift パラメータを指定しなくても、環境を作成するための環境プロファイルを選択できるようになりました。AWS シークレット、クラスター、ワークグループ、データベース。これらのパラメータは、環境プロファイルから環境に移行されます。環境の作成に加えて、Amazon は環境のデフォルトスキーマも作成する DataZone ようになりました。プロジェクトのメンバーは、このスキーマへの読み取りおよび書き込みアクセス権を持ち、環境作成の一部として作成されたデフォルトのデータソースを実行することで、このスキーマで作成されたテーブルをカタログに簡単に発行できます。環境の作成に使用される Amazon Redshift パラメータは、新しいデータソースの作成にも使用できます (データソースの作成時に独自のパラメータを提供するためのデータプロデューサーの代わりに) 。

AWS Amazon の Cloud Formation サポート DataZone

01/18/2024 にリリース

Amazon のユーザーが DataZone を利用できるようになりました AWS CloudFormation Amazon DataZone リソースのスイートを効果的にモデル化および管理するための 。このアプローチにより、リソースの一貫したプロビジョニングが容易になり、コードプラクティスとしてのインフラストラクチャによるライフサイクル管理も可能になります。カスタムテンプレートを使用すると、必要なリソースとその相互依存関係を正確に定義できます。詳細については、「Amazon DataZone リソースタイプのリファレンス」を参照してください。

Amazon DataZone プロジェクトのメンバーとしてプリンIAMシパルを直接追加する

01/05/2024 にリリース

プリンIAMシパルがまだ Amazon にログインしていない場合でも DataZone （ 以前の要件 ）、プリンIAMシパルをプロジェクトメンバーとして追加できるようになりました。ドメイン管理者または IT 管理者がドメインのドメイン実行ロール`iam:GetRole`に `iam:GetUser`と を追加した後、プロジェクト所有者はIAM、ロールまたはIAMユーザーの Amazon リソース名 (ARN) を指定するだけで、プリンIAMシパルをメンバーとして追加できます。IAM プリンシパルには、Amazon へのアクセスに必要なアクセスIAM許可が引き続き必要です。アクセス許可は DataZone 、IAMコンソールで設定できます。詳細については、「プロジェクトにメンバーを追加する」を参照してください。

データポータルからのカスタムアセットタイプのサポート

01/05/2024 にリリース

カスタムアセットのサポートにより、Amazon DataZone はデータポータルを介してダッシュボード、クエリ、モデルなどの非構造化データ用にアセットをカタログ化できるため、以前に利用可能なAPIサポートとともに、カスタムアセットをデータポータルに直接追加することが容易になります。Amazon でカスタムアセットを作成、更新、公開する機能により DataZone、あらゆる種類のアセットを共有、検索、サブスクライブし、それらのアセットのガバナンスを提供するビジネスワークフローを構築できます。詳細については、「カスタムアセットタイプを作成する」を参照してください。

2023

ドメインの削除

12/27/2023 にリリース

これは、ドメインをより簡単に削除できる機能です。これで、ドメインが空でなくても (にプロジェクト、環境、アセット、データソースなどが含まれているように) 、ドメインの削除を続行できます。詳細については、「Amazon DataZone ドメインを削除する」を参照してください。

ハイブリッドモード

12/22/2023 にリリース

Amazon DataZone が のサポートを追加 AWS Lake Formation ハイブリッドモード。このサポートにより、 を公開する場合 AWS Glue テーブルを DataZone で Amazon に AWS ハイブリッドモードで Lake Formation に登録された S3 ロケーション。Amazon はこのテーブルをマネージドアセットとして DataZone 扱い、このテーブルへのサブスクリプション許可を管理できます。この機能リリース以前 DataZone は、Amazon はこのテーブルをアンマネージドアセットとして扱い DataZone ます。つまり、Amazon はこのテーブルにサブスクリプションを付与できません。詳細については、「Amazon の Lake Formation アクセス許可を設定する DataZone」を参照してください。

HIPAA 適格性

12/14/2023 にリリース

Amazon DataZone は、1996 年米国健康保険の相互運用性と説明責任に関する法律 (HIPAA) に準拠するようになりました。のリストを表示するには AWS HIPAA コンプライアンスを備えた のサービスについては、https://aws.amazon.com/compliance/hipaa-eligible-services-reference「/」を参照してください。

Amazon DataZone での説明に関する AI レコメンデーション (プレビュー)

11/28/2023 にリリース

AWS は、Amazon で新しい生成 AI ベースの機能の DataZoneプレビューを発表しました。これにより、ビジネスデータカタログを強化することで、データ検出、データ理解、データ使用量が向上します。ワンクリックで、データプロデューサーは包括的なビジネスデータの説明とコンテキストを生成し、影響のある列を強調し、分析ユースケースに関するレコメンデーションを含めることが

できます。Amazon での説明に関する AI レコメンデーションを使用すると DataZone、データコンシューマーは分析に必要なデータテーブルと列を識別できるため、データ検出性が向上し、データプロデューサーとの back-and-forth 通信が削減されます。プレビューは、次でプロビジョニングされた Amazon DataZone ドメインで利用できます。 AWS リージョン: 米国東部 (バージニア北部) 、米国西部 (オレゴン) 。詳細については、「機械学習と生成 AI の使用」を参照してください。

DefaultDataLake ブループリントの強化

11/20/2023 にリリース

Amazon DataZone は、 からどのデータを公開できるかをより適切に制御できる機能強化を DefaultDataLake ブループリントに追加しました。 AWS アカウント。この機能の起動に伴って導入された主な変更点が 2 つあります。

- コンソールでブルー DefaultDataLake プリントを有効にすると、有効な DefaultDataLake ブループリントに管理プロジェクトを割り当てることで、アカウントのブループリントを使用して環境プロファイルを作成できるプロジェクトを制御できます。
- 2 番目の変更は、 ポータルで行われます。 DefaultDataLake 設計図を使用して環境プロファイルを作成する場合は、環境プロファイルを使用して環境を作成することを許可されているプロジェクトを選択することもできます。デフォルトでは、すべてのプロジェクトでデータレイク環境プロファイルを使用できますが、環境プロファイルを特定のプロジェクトに制限したり、プロファイルで作成された環境を使用して公開できるデータを制御したりできます。

詳細については、「環境プロファイルを作成する」を参照してください。

Amazon のセットアップ DataZone

Amazon をセットアップするには DataZone、 が必要です AWS アカウントを作成し、Amazon に必要なIAMポリシーとアクセス許可を設定します DataZone。

Amazon アクセス DataZone 許可を設定したら、「開始方法」セクションのステップを完了することをお勧めします。このステップでは、Amazon ??? DataZone ドメインの作成、データポータル の取得URL、およびデータプロデューサーとデータコンシューマー向けの基本的な Amazon DataZone ワークフローについて説明します。

トピック

- にサインアップする AWS アカウント
- Amazon DataZone マネジメントコンソールを使用するために必要なIAMアクセス許可を設定する
- Amazon DataZone データポータルを使用するために必要なIAMアクセス許可を設定する
- 設定 AWS IAM Amazon 用 Identity Center DataZone

にサインアップする AWS アカウント

をお持ちでない場合 AWS アカウントを作成するには、次のステップを実行します。

をお持ちの場合 AWS organization、アカウントを作成します。

1. にサインインする AWS マネジメントコンソール で Organizations コンソールを開きますhttps://console.aws.amazon.com/organizations/。
2. ナビゲーションペインで、 を選択します。 AWS アカウント 。
3. の追加 を選択します。 AWS アカウント 。
4. の作成 を選択します。 AWS アカウントを作成し、リクエストされた詳細を入力します。作成 を選択します。 AWS アカウント 。

にサインアップするには AWS アカウント

1. https://portal.aws.amazon.com/billing/サインアップを開く
2. オンラインの手順に従います。

   サインアップ手順の一環として、通話呼び出しを受け取り、電話キーパッドで検証コードを入力するように求められます。

にサインアップするとき AWS アカウント、 AWS アカウントルートユーザーが作成されます。ルートユーザーはすべての にアクセスできます AWS アカウントの サービスとリソース。セキュリティのベストプラクティスとして、管理ユーザーに管理アクセスを割り当て、ルートユーザーアクセスが必要なタスクを実行する場合にのみ、ルートユーザーを使用してください。

Amazon DataZone マネジメントコンソールを使用するために必要なIAMアクセス許可を設定する

Amazon DataZone ドメイン、ブループリント、ユーザーにアクセスして設定し、Amazon DataZone データポータルを作成するには、Amazon DataZone マネジメントコンソールを使用する必要があります。

Amazon DataZone マネジメントコンソールの使用を希望するユーザー、グループ、またはロールに必要なアクセス許可やオプションのアクセス許可を設定するには、以下の手順を完了する必要があります。

マネジメントコンソールを使用するためのIAMアクセス許可を設定する手順

- Amazon DataZone コンソールにアクセスするためのユーザー、グループ、またはロールに必須およびオプションのポリシーをアタッチする
- Amazon DataZone サービスコンソールのロール作成を簡素化するIAMアクセス許可のカスタムポリシーを作成する
- Amazon DataZone ドメインに関連付けられたアカウントを管理するアクセス許可のカスタムポリシーを作成する
- （オプション）のカスタムポリシーを作成する AWS Amazon DataZone ドメインへのSSOユーザーおよびSSOグループアクセスを追加および削除する Identity Center のアクセス許可
- （オプション）プリンIAMシパルをキーユーザーとして追加し、 のカスタマーマネージドキーを使用して Amazon DataZone ドメインを作成します。 AWS Key Management Service (KMS)

Amazon DataZone コンソールにアクセスするためのユーザー、グループ、またはロールに必須およびオプションのポリシーをアタッチする

ユーザー、グループ、またはロールに必須およびオプションのカスタムポリシーをアタッチするには、以下の手順を実行します。詳細については、「AWS Amazon の マネージドポリシー DataZone」を参照してください。

1. にサインインする AWS マネジメントコンソール でIAMコンソールを開きますhttps://console.aws.amazon.com/iam/。
2. ナビゲーションペインで、ポリシー を選択します。
3. ユーザー、グループ、またはロールにアタッチする次のポリシーを選択します。

   - ポリシーのリストで、 の横にあるチェックボックスをオンにしますAmazonDataZoneFullAccess。[Filter (フィルター)] メニューと検索ボックスを使用して、ポリシーのリストをフィルタリングできます。詳細については、「AWS マネージドポリシー：AmazonDataZoneFullAccess」を参照してください。
   - (オプション) Amazon DataZone サービスコンソールのロール作成を簡素化するIAMアクセス許可のカスタムポリシーを作成します。
   - (オプション) のカスタムポリシーを作成する AWS Amazon DataZone ドメインへのSSOユーザーおよびSSOグループアクセスを追加および削除する Identity Center のアクセス許可。
4. [Actions (アクション)] を選択し、[Attach (アタッチ)] を選択します。
5. ポリシーをアタッチするユーザー、グループ、またはロールを選択します。[Filter] メニューと検索ボックスを使用して、プリンシパルエンティティのリストをフィルタリングできます。ユーザー、グループ、またはロールを選択したら、ポリシーのアタッチ を選択します。

Amazon DataZone サービスコンソールのロール作成を簡素化するIAMアクセス許可のカスタムポリシーを作成する

Amazon が で必要なロールを作成するために必要なアクセス許可を持つカスタムインラインポリシー DataZone を作成するには、以下の手順を実行します。 AWS ユーザーに代わって マネジメントコンソール。

1. にサインインする AWS マネジメントコンソール でIAMコンソールを開きますhttps://console.aws.amazon.com/iam/。
2. ナビゲーションペインで、[Users] (ユーザー) または [User groups] (ユーザーグループ) を選択します。
3. 一覧から、ポリシーを埋め込むユーザーまたはグループの名前を選択します。
4. [Permissions (アクセス許可)] タブを選択して、必要であれば [Permissions policies (アクセス許可ポリシー)] セクションを展開します。
5. アクセス許可の追加 とインラインポリシーリンクの作成 を選択します。

6. 「ポリシーの作成」画面の「ポリシーエディタ」セクションで、「」を選択しますJSON。

   次のJSONステートメントを使用してポリシードキュメントを作成し、次へ を選択します。

```
{
    "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. ポリシーの確認 画面で、ポリシーの名前を入力します。ポリシーが完成したら、[Create policy (ポリシーの作成)] を選択します。画面上部の赤いボックスにエラーが表示されていないことを確認します。報告されたエラーがあれば、修正します。

Amazon DataZone ドメインに関連付けられたアカウントを管理するアクセス許可のカスタムポリシーを作成する

で必要なアクセス許可を関連付けるカスタムインラインポリシーを作成するには、次の手順を実行します。 AWS アカウントは、ドメインのリソース共有を一覧表示、承認、拒否し、関連付けられたアカウントで環境ブループリントを有効、設定、および無効にします。ブループリント設定時に使用可能なオプションの Amazon DataZone サービスコンソールの簡易ロール作成を有効にするには、 も必要ですAmazon DataZone サービスコンソールのロール作成を簡素化するIAMアクセス許可のカスタムポリシーを作成する 。

1. にサインインする AWS マネジメントコンソール でIAMコンソールを開きますhttps://console.aws.amazon.com/iam/。
2. ナビゲーションペインで、[Users] (ユーザー) または [User groups] (ユーザーグループ) を選択します。
3. 一覧から、ポリシーを埋め込むユーザーまたはグループの名前を選択します。
4. [Permissions (アクセス許可)] タブを選択して、必要であれば [Permissions policies (アクセス許可ポリシー)] セクションを展開します。
5. アクセス許可の追加 とインラインポリシーリンクの作成 を選択します。
6. 「ポリシーの作成」画面の「ポリシーエディタ」セクションで、「」を選択しますJSON。次のJSONステートメントを使用してポリシードキュメントを作成し、次へ を選択します。

```
{
    "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. ポリシーの確認 画面で、ポリシーの名前を入力します。ポリシーが完成したら、[Create policy (ポリシーの作成)] を選択します。画面上部の赤いボックスにエラーが表示されていないことを確認します。報告されたエラーがあれば、修正します。

(オプション) のカスタムポリシーを作成する AWS Amazon DataZone ドメインへのSSOユーザーおよびSSOグループアクセスを追加および削除する Identity Center のアクセス許可

Amazon DataZone ドメインへのSSOユーザーおよびSSOグループアクセスを追加および削除するのに必要なアクセス許可を持つカスタムインラインポリシーを作成するには、以下の手順を実行します。

1. にサインインする AWS マネジメントコンソール でIAMコンソールを開きますhttps://console.aws.amazon.com/iam/。

2. ナビゲーションペインで、[Users] (ユーザー) または [User groups] (ユーザーグループ) を選択します。
3. 一覧から、ポリシーを埋め込むユーザーまたはグループの名前を選択します。
4. [Permissions (アクセス許可)] タブを選択して、必要であれば [Permissions policies (アクセス許可ポリシー)] セクションを展開します。
5. アクセス許可の追加 とインラインポリシーの作成 を選択します。
6. 「ポリシーの作成」画面の「ポリシーエディタ」セクションで、「」を選択しますJSON。

   次のJSONステートメントを使用してポリシードキュメントを作成し、次へ を選択します。

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

7. ポリシーの確認 画面で、ポリシーの名前を入力します。ポリシーが完成したら、[Create policy (ポリシーの作成)] を選択します。画面上部の赤いボックスにエラーが表示されていないことを確認します。報告されたエラーがあれば、修正します。

(オプション) プリンIAMシパルをキーユーザーとして追加し、 のカスタマーマネージドキーを使用して Amazon DataZone ドメインを作成します。 AWS Key Management Service (KMS)

オプションで、 からカスタマーマネージドキー (CMK) を使用して Amazon DataZone ドメインを作成する前に AWS Key Management Service (KMS) で次の手順を実行して、IAMプリンシパルをKMSキーのユーザーにします。

1. にサインインする AWS マネジメントコンソール でKMSコンソールを開きますhttps://console.aws.amazon.com/kms/。
2. ユーザーが作成および管理するアカウント内のキーを表示するには、ナビゲーションペインで [Customer managed keys] (カスタマーマネージドキー) を選択します。
3. KMS キーのリストで、確認するキーのエイリアスまたはKMSキー ID を選択します。
4. キーユーザーを追加または削除し、外部ユーザーを許可または禁止するには AWS アカウントでKMSキーを使用するには、ページの「キーユーザー」セクションのコントロールを使用します。キーユーザーは、データKMSキーの暗号化、復号、再暗号化、生成などの暗号化オペレーションで キーを使用できます。

Amazon DataZone データポータルを使用するために必要なIAMアクセス許可を設定する

Amazon DataZone データポータル (AWS マネジメントコンソール外) は、ユーザーがセルフサービス方式でデータをカタログ化、検出、管理、共有、分析できるブラウザベースのウェブアプリケーションです。データポータルは、 を通じて ID プロバイダーからのIAM認証情報または既存の認証情報を使用してユーザーを認証します。 AWS IAM Identity Center。

Amazon DataZone データポータルまたはカタログを使用するユーザー、グループ、またはロールに必要なアクセス許可を設定するには、以下の手順を完了する必要があります。

データポータルを使用するためのIAMアクセス許可を設定する手順

- Amazon DataZone データポータルへのアクセスに必要なポリシーをユーザー、グループ、またはロールにアタッチする
- Amazon DataZone カタログアクセスに必要なポリシーをユーザー、グループ、またはロールにアタッチする

- ドメインが のカスタマーマネージドキーで暗号化されている場合、Amazon DataZone データポータルまたはカタログアクセス用のユーザー、グループ、またはロールにオプションのポリシーをアタッチする AWS Key Management Service (KMS)

Amazon DataZone データポータルへのアクセスに必要なポリシーをユーザー、グループ、またはロールにアタッチする

Amazon DataZone データポータルにアクセスするには、 のいずれかを使用します。 AWS 認証情報またはシングルサインオン (SSO) 認証情報。以下のセクションの指示に従って、 でデータポータルにアクセスするために必要なアクセス許可を設定します。 AWS 認証情報。 DataZone での Amazon の使用の詳細については、SSO「」を参照してください設定 AWS IAM Amazon 用 Identity Center DataZone。

> **Note**
>
> ドメインの のIAMプリンシパルのみ AWS アカウントは、ドメインのデータポータルにアクセスできます。IAM 他の からのプリンシパル AWS アカウントはドメインのデータポータルにアクセスできません。

ユーザー、グループ、またはロールに必要なポリシーをアタッチするには、次の手順を実行します。詳細については、「AWS Amazon の マネージドポリシー DataZone」を参照してください。

1. にサインインする AWS マネジメントコンソール でIAMコンソールを開きますhttps://console.aws.amazon.com/iam/。
2. ナビゲーションペインで、ユーザー、ユーザーグループ、またはロール を選択します。
3. リストで、ポリシーを埋め込むユーザー、グループ、またはロールの名前を選択します。
4. [Permissions (アクセス許可)] タブを選択して、必要であれば [Permissions policies (アクセス許可ポリシー)] セクションを展開します。
5. アクセス許可を追加 とインラインポリシーリンクの作成 を選択します。
6. 「ポリシーの作成」画面の「ポリシーエディタ」セクションで、「」を選択しますJSON。次のJSONステートメントを使用してポリシードキュメントを作成し、次へ を選択します。

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

```
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "datazone:GetIamPortalLoginUrl"
            ],
            "Resource": [
                "*"
            ]
        }
    ]
}
```

7. ポリシーの確認 画面で、ポリシーの名前を入力します。ポリシーが完成したら、[Create policy (ポリシーの作成)] を選択します。画面上部の赤いボックスにエラーが表示されていないことを確認します。報告されたエラーがあれば、修正します。

Amazon DataZone カタログアクセスに必要なポリシーをユーザー、グループ、またはロールにアタッチする

> **Note**
>
> ドメインの のIAMプリンシパルのみ AWS アカウントはドメインのカタログにアクセスできます。IAM 他の からのプリンシパル AWS アカウントはドメインのカタログにアクセスできません。

以下の手順でIAM、 APIおよび を使用して、Amazon DataZone ドメインのカタログへのアクセス権を ID SDK に付与できます。これらの IAM ID が Amazon DataZone データポータルにもアクセスできるようにするには、上記の手順に加えて に従いますAmazon DataZone データポータルへのアクセスに必要なポリシーをユーザー、グループ、またはロールにアタッチする。詳細については、「AWS Amazon の マネージドポリシー DataZone」を参照してください。

1. にサインインする AWS マネジメントコンソール でIAMコンソールを開きますhttps://console.aws.amazon.com/iam/。
2. ナビゲーションペインで、ポリシー を選択します。
3. ポリシーのリストで、AmazonDataZoneFullUserAccessポリシーの横にあるラジオボタンを選択します。[Filter (フィルター)] メニューと検索ボックスを使用して、ポリシー

のリストをフィルタリングできます。詳細については、「AWS マネージドポリシー：AmazonDataZoneFullUserAccess」を参照してください

4. [Actions (アクション)] を選択し、[Attach (アタッチ)] を選択します。
5. 各プリンシパルの横にあるチェックボックスをオンにして、ポリシーをアタッチするユーザー、グループ、またはロールを選択します。[Filter] メニューと検索ボックスを使用して、プリンシパルエンティティのリストをフィルタリングできます。ユーザー、グループ、またはロールを選択したら、ポリシーのアタッチ を選択します。

ドメインが のカスタマーマネージドキーで暗号化されている場合、Amazon DataZone データポータルまたはカタログアクセス用のユーザー、グループ、またはロールにオプションのポリシーをアタッチする AWS Key Management Service (KMS)

データ暗号化用の独自のKMSキーを使用して Amazon DataZone ドメインを作成する場合は、以下のアクセス許可を持つインラインポリシーも作成し、プリンIAMシパルが Amazon DataZone データポータルまたはカタログにアクセスできるようにプリンシパルにアタッチする必要があります。

1. にサインインする AWS マネジメントコンソール でIAMコンソールを開きますhttps://console.aws.amazon.com/iam/。
2. ナビゲーションペインで、ユーザー、ユーザーグループ、またはロール を選択します。
3. リストで、ポリシーを埋め込むユーザー、グループ、またはロールの名前を選択します。
4. [Permissions (アクセス許可)] タブを選択して、必要であれば [Permissions policies (アクセス許可ポリシー)] セクションを展開します。
5. アクセス許可の追加 とインラインポリシーリンクの作成 を選択します。
6. 「ポリシーの作成」画面の「ポリシーエディタ」セクションで、「」を選択しますJSON。次のJSONステートメントを使用してポリシードキュメントを作成し、次へ を選択します。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "kms:Decrypt",
                "kms:GenerateDataKey",
```

```
                "kms:DescribeKey"
            ],
            "Resource": "*"
        }
    ]
}
```

7. ポリシーの確認 画面で、ポリシーの名前を入力します。ポリシーが完成したら、[Create policy (ポリシーの作成)] を選択します。画面上部の赤いボックスにエラーが表示されていないことを確認します。報告されたエラーがあれば、修正します。

設定 AWS IAM Amazon 用 Identity Center DataZone

> **Note**
>
> AWS Identity Center は同じ で有効にする必要があります AWS Amazon DataZone ドメインとしての リージョン。現在、 AWS Identity Center は 1 つの でのみ有効にできます AWS リージョン。

Amazon DataZone データポータルにアクセスするには、シングルサインオン (SSO) 認証情報または AWS 認証情報。このセクションの指示に従って を設定します。 AWS IAM Amazon の Identity Center DataZone。 DataZone で Amazon を使用する方法の詳細については、 AWS 認証情報については、「」を参照してくださいAmazon DataZone マネジメントコンソールを使用するために必要なIAMアクセス許可を設定する。

既に がある場合は、このセクションの手順をスキップできます。 AWS IAM アイデンティティセンター (の後継サービス AWS Single Sign-On) は同じ で有効および設定されている AWS Amazon DataZone ドメインを作成するリージョン。

を有効にするには、次の手順を実行します。 AWS IAM アイデンティティセンター (の後継サービス AWS シングルサインオン) 。

1. を有効にするには AWS IAM Identity Center、 にサインインする必要があります AWS の認証情報を使用した マネジメントコンソール AWS Organizations 管理アカウント。の認証情報を使用してサインインしているときに IAM Identity Center を有効にすることはできません AWS Organizations メンバーアカウント。詳細については、「」の「組織の作成と管理」を参照してください。 AWS Organizations ユーザーガイド。

2. を開きますAWS IAM アイデンティティセンター (の後継サービス AWS Single Sign-On) コンソールで、上部のナビゲーションバーのリージョンセレクターを使用して を選択します。 AWS Amazon DataZone ドメインを作成するリージョン。
3. [Enable (有効化)] を選択します。
4. ID ソースを選択します。

   デフォルトでは、IAMIdentity Center ストアを使用して、迅速かつ簡単にユーザーを管理できます。オプションで、代わりに外部 ID プロバイダーに接続できます。この手順では、デフォルトの IAM Identity Center ストアを使用します。

   詳細については、「ID ソースの選択」を参照してください。
5. IAM Identity Center ナビゲーションペインで、グループ を選択し、グループの作成 を選択します。グループ名を入力し、 の作成を選択します。
6. IAM Identity Center ナビゲーションペインで、ユーザー を選択します。
7. ユーザーの追加 画面で必要な情報を入力し、パスワード設定手順 を使用してユーザーに E メールを送信 を選択します。ユーザーは、次のセットアップ手順に関する E メールを受信する必要があります。
8. 次へ: グループ を選択し、目的のグループを選択し、ユーザーの追加 を選択します。ユーザーは、 を使用するように招待する E メールを受信する必要がありますSSO。この E メールでは、招待を受け入れるを選択し、パスワードを設定する必要があります。

Amazon DataZone ドメインを作成したら、 を有効にできます。 AWS Identity Center for Amazon DataZone と は、SSOユーザーとSSOグループへのアクセスを提供します。詳細については、「Amazon の IAM Identity Center を有効にする DataZone」を参照してください。

Amazon の開始方法 DataZone

このセクションの情報は、Amazon の使用を開始するのに役立ちます DataZone。Amazon を初めて使用する場合は DataZone、まず「」で説明されている概念と用語を理解してくださいAmazon DataZone の用語と概念。

これらのクイックスタートワークフローのいずれかのステップを開始する前に、このガイドの「セットアップ」セクションで説明されている手順を完了する必要があります。新しい を使用している場合 AWS アカウント、Amazon DataZone マネジメントコンソール を使用するために必要なアクセス許可を設定する必要があります。を使用している場合 AWS 既存の を持つ アカウント AWS Glue Data Catalog オブジェクトでは、Amazon への Lake Formation アクセス許可も設定 DataZoneする必要があります。

この入門セクションでは、以下の Amazon DataZone クイックスタートワークフローについて説明します。

トピック

- を使用した Amazon DataZone クイックスタート AWS Glue データ
- Amazon Redshift データを使用した Amazon DataZone クイックスタート
- サンプルスクリプトを使用した Amazon DataZone クイックスタート

を使用した Amazon DataZone クイックスタート AWS Glue データ

以下のクイックスタートステップを完了して、Amazon で完全なデータプロデューサーとデータコンシューマーのワークフローをサンプル DataZone で実行します。 AWS Glue データ。

クイックスタートステップ

- ステップ 1 - Amazon DataZone ドメインとデータポータルを作成する
- ステップ 2 - 公開プロジェクトを作成する
- ステップ 3 - 環境を作成する
- ステップ 4 - 公開用のデータを生成する
- ステップ 5 - からメタデータを収集する AWS 接着語
- ステップ 6 - データアセットをキュレートして公開する
- ステップ 7 - データ分析用のプロジェクトを作成する

- ステップ 8 - データ分析用の環境を作成する
- ステップ 9 - データカタログを検索してデータをサブスクライブする
- ステップ 10 - サブスクリプションリクエストを承認する
- ステップ 11 - Amazon Athena でクエリを構築し、データを分析する

ステップ 1 - Amazon DataZone ドメインとデータポータルを作成する

このセクションでは、このワークフロー用の Amazon DataZone ドメインとデータポータルを作成する手順について説明します。

Amazon DataZone ドメインを作成するには、次の手順を実行します。Amazon DataZone ドメインの詳細については、「」を参照してくださいAmazon DataZone の用語と概念。

1. https://console.aws.amazon.com/datazone で Amazon DataZone コンソールに移動し、サインインして、ドメインの作成 を選択します。

   > **Note**
   >
   > このワークフローに既存の Amazon DataZone ドメインを使用する場合は、ドメインの表示 を選択し、使用するドメインを選択してから、公開プロジェクトの作成のステップ 2 に進みます。

2. ドメインの作成ページで、次のフィールドに値を指定します。

   - 名前 - ドメインの名前を指定します。このワークフローでは、このドメインのマーケティングを呼び出すことができます。
   - 説明 - オプションのドメインの説明を指定します。
   - データ暗号化 - データは、デフォルトで次のキーで暗号化されます。 AWS はお客様に代わって を所有および管理します。このユースケースでは、デフォルトのデータ暗号化設定のままにしておくことができます。

     カスタマーマネージドキーの使用の詳細については、「」を参照してくださいAmazon の保管中のデータ暗号化 DataZone。データ暗号化に独自のKMSキーを使用する場合は、デフォルトの に次のステートメントを含める必要がありますAmazonDataZoneDomainExecutionRole。

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

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

- サービスアクセス - デフォルトでは、 を選択したままにします。デフォルトのロールオプションは変更されません。

> **Note**
>
> このワークフローに既存の Amazon DataZone ドメインを使用している場合は、既存のサービスロールを使用するオプションを選択し、ドロップダウンメニューから既存のロールを選択できます。

- 「クイックセットアップ」で、データ消費と の公開のためにこのアカウントを設定するを選択します。このオプションは、データレイクとデータウェアハウス の組み込み Amazon DataZone ブループリントを有効にし、このアカウントに必要なアクセス許可、リソース、デフォルトのプロジェクト、デフォルトのデータレイクとデータウェアハウス環境プロファイルを設定します。Amazon DataZone ブループリントの詳細については、「」を参照してくださいAmazon DataZone の用語と概念。
- アクセス許可の詳細の残りのフィールドは変更しないでください。

> **Note**
>
> 既存の Amazon DataZone ドメインがある場合は、既存のサービスロールを使用するオプションを選択し、 Glue 管理アクセスロール 、Redshift 管理アクセスロール 、およびプロビジョニングロールのドロップダウンメニューから既存のロールを選択できます。

- タグの下のフィールドは変更しないでください。
- [ドメインの作成] をクリックします。

3. ドメインが正常に作成されたら、このドメインを選択し、ドメインの概要ページで、このドメインのデータポータルURLを書き留めます。これを使用して Amazon DataZone データポータルURLにアクセスし、このワークフローの残りのステップを完了できます。Open data portal を選択して、データポータルに移動することもできます。

> **Note**
>
> Amazon の現在のリリースでは DataZone、ドメインが作成されると、データポータル用にURL生成された を変更することはできません。

ドメインの作成が完了するまでに数分かかる場合があります。次のステップに進む前に、ドメインのステータスが Available になるまで待ちます。

ステップ 2 - 公開プロジェクトを作成する

このセクションでは、このワークフローの発行プロジェクトを作成するために必要な手順について説明します。

1. 上記のステップ 1 を完了してドメインを作成すると、Amazon DataZone! へようこそウィンドウが表示されます。このウィンドウで、プロジェクトの作成 を選択します。
2. プロジェクト名を指定します。例えば、このワークフローでは、 という名前を付けSalesDataPublishingProject、残りのフィールドは変更せずにおき、 の作成 を選択します。

ステップ 3 - 環境を作成する

このセクションでは、このワークフローの環境を作成するために必要な手順について説明します。

1. 上記のステップ 2 を完了してプロジェクトを作成すると、プロジェクトを使用する準備ができたウィンドウが表示されます。このウィンドウで、環境の作成 を選択します。
2. 「環境の作成」ページで以下を指定し、「環境の作成」を選択します。
3. 以下の値を指定します。

   - 名前 - 環境の名前を指定します。このチュートリアルでは、 と呼びますDefault data lake environment。
   - 説明 - 環境の説明を指定します。

- 環境プロファイル - DataLakeProfile環境プロファイルを選択します。これにより、このワークフロー DataZone で Amazon を使用して Amazon S3 内のデータを操作できます。 AWS Glue Catalog、および Amazon Athena
- このチュートリアルでは、残りのフィールドは変更しないでください。

4. [Create environment (環境の作成)] を選択します。

ステップ 4 - 公開用のデータを生成する

このセクションでは、このワークフローで公開するためのデータを生成するために必要な手順について説明します。

1. 上記のステップ 3 を完了したら、SalesDataPublishingProjectプロジェクトで右側のパネルの分析ツール で Amazon Athenaを選択します。これにより、認証にプロジェクトの認証情報を使用して Athena クエリエディタが開きます。公開環境が Amazon DataZone 環境ドロップダウンで選択され、<environment_name>%_pub_dbデータベースがクエリエディタで として選択されていることを確認します。
2. このチュートリアルでは、Create Table as Select (CTAS) クエリスクリプトを使用して、Amazon に発行する新しいテーブルを作成します DataZone。クエリエディタで、このCTASスクリプトを実行して、公開して検索とサブスクリプションに使用できるmkt_sls_tableテーブルを作成します。

```
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
```

左側の「テーブルとビュー」セクションに m""_sls_table テーブルが正常に作成されていることを確認します。これで、Amazon DataZone カタログに公開できるデータアセットができました。

ステップ 5 - からメタデータを収集する AWS 接着語

このセクションでは、 からメタデータを収集するステップについて説明します。 AWS このワークフローの Glue。

1. 上記のステップ 4 を完了したら、Amazon DataZone データポータルでSalesDataPublishingProjectプロジェクトを選択し、データタブを選択し、左側のパネルでデータソースを選択します。
2. 環境作成プロセスの一部として作成されたソースを選択します。
3. アクションドロップダウンメニューの横にある実行 を選択し、更新ボタンを選択します。データソースの実行が完了すると、アセットが Amazon DataZone インベントリに追加されます。

ステップ 6 - データアセットをキュレートして公開する

このセクションでは、このワークフローでデータアセットをキュレートして公開する手順について説明します。

1. 上記のステップ 5 を完了したら、Amazon DataZone データポータルで、前のステップで作成したSalesDataPublishingProjectプロジェクトを選択し、データタブを選択し、左側のパネルでインベントリデータを選択し、mkt_sls_tableテーブルを見つけます。
2. mkt_sls_table アセットの詳細ページを開いて、自動的に生成されたビジネス名を表示します。自動生成されたメタデータアイコンを選択すると、アセットと列の自動生成された名前が表示されます。各名前を個別に承諾または拒否するか、すべて承諾を選択して生成された名前を適用できます。必要に応じて、使用可能なメタデータフォームをアセットに追加し、用語集の用語を選択してデータを分類することもできます。
3. アセットを発行を選択してアセットを発行しますmkt_sls_table。

ステップ 7 - データ分析用のプロジェクトを作成する

このセクションでは、データ分析用のプロジェクトを作成する手順について説明します。これは、このワークフローのデータコンシューマーステップの始まりです。

1. 上記のステップ 6 を完了したら、Amazon DataZone データポータルで、プロジェクトドロップダウンメニューからプロジェクトの作成を選択します。
2. 「プロジェクトの作成」ページでプロジェクト名を指定します。例えば、このワークフローでは、名前を にしMarketingDataAnalysisProject、残りのフィールドは変更せずにおき、「作成」を選択します。

ステップ 8 - データ分析用の環境を作成する

このセクションでは、データ分析用の環境を作成する手順について説明します。

1. 上記のステップ 7 を完了したら、Amazon DataZone データポータルでMarketingDataAnalysisProjectプロジェクトを選択し、環境 タブを選択し、環境の作成 を選択します。
2. 「環境の作成」ページで以下を指定し、「環境の作成」を選択します。

   - 名前 - 環境の名前を指定します。このチュートリアルでは、 と呼びますDefault data lake environment。
   - 説明 - 環境の説明を指定します。
   - 環境プロファイル - 組み込みDataLakeProfile環境プロファイルを選択します。
   - このチュートリアルでは、残りのフィールドは変更しないでください。

ステップ 9 - データカタログを検索してデータをサブスクライブする

このセクションでは、データカタログを検索し、データをサブスクライブする手順について説明します。

1. 上記のステップ 8 を完了したら、Amazon DataZone データポータルで Amazon DataZone アイコンを選択し、Amazon DataZone Search フィールドで、データポータルの検索バーでキーワード (「カタログ」や「売上」など) を使用してデータアセットを検索します。

   必要に応じて、フィルターまたはソートを適用し、製品販売データアセットを見つけたら、それを選択してアセットの詳細ページを開くことができます。
2. カタログ販売データアセットの詳細ページで、サブスクライブ を選択します。
3. Subscribe ダイアログで、ドロップダウンからMarketingDataAnalysisProjectコンシューマープロジェクトを選択し、サブスクリプションリクエストの理由を指定し、Subscribe を選択します。

ステップ 10 - サブスクリプションリクエストを承認する

このセクションでは、サブスクリプションリクエストを承認する手順について説明します。

1. 上記のステップ 9 を完了したら、Amazon DataZone データポータルで、アセットを公開したSalesDataPublishingProjectプロジェクトを選択します。
2. データ タブを選択し、次に公開されたデータ を選択し、受信リクエスト を選択します。
3. これで、承認が必要な新しいリクエストの行が表示されます。リクエストの表示 を選択します。承認の理由を入力し、承認 を選択します。

ステップ 11 - Amazon Athena でクエリを構築し、データを分析する

アセットを Amazon DataZone カタログに正常に公開し、サブスクライブしたので、分析できます。

1. Amazon DataZone データポータルでコンシューマーMarketingDataAnalysisProjectプロジェクトを選択し、右側のパネルの分析ツール で Amazon Athena とのクエリデータリンクを選択します。これにより、プロジェクトの認証情報を使用して認証用の Amazon Athena クエリエディタが開きます。クエリエディタの Amazon DataZone Environment ドロップダウンからMarketingDataAnalysisProjectコンシューマー環境を選択し、データベースドロップダウン`<environment_name>%sub_db`からプロジェクトの を選択します。
2. サブスクライブされたテーブルでクエリを実行できるようになりました。テーブルとビュー からテーブルを選択し、プレビュー を選択してエディタ画面で Select ステートメントを表示できます。クエリを実行して結果を表示します。

Amazon Redshift データを使用した Amazon DataZone クイックスタート

以下のクイックスタートステップを実行して、Amazon Redshift データのサンプル DataZone を使用して、Amazon で完全なデータプロデューサーおよびデータコンシューマーワークフローを実行します。

クイックスタートステップ

- ステップ 1 - Amazon DataZone ドメインとデータポータルを作成する
- ステップ 2 - 公開プロジェクトを作成する
- ステップ 3 - 環境を作成する

- ステップ 4 - 公開用のデータを生成する
- ステップ 5 - Amazon Redshift からメタデータを収集する
- ステップ 6 - データアセットをキュレートして公開する
- ステップ 7 - データ分析用のプロジェクトを作成する
- ステップ 8 - データ分析用の環境を作成する
- ステップ 9 - データカタログを検索してデータをサブスクライブする
- ステップ 10 - サブスクリプションリクエストを承認する
- ステップ 11 - Amazon Redshift でクエリを構築し、データを分析する

ステップ 1 - Amazon DataZone ドメインとデータポータルを作成する

Amazon DataZone ドメインを作成するには、次の手順を実行します。Amazon DataZone ドメインの詳細については、「」を参照してくださいAmazon DataZone の用語と概念。

1. https://console.aws.amazon.com/datazone の Amazon DataZone コンソールに移動し、サインインして、ドメインの作成 を選択します。

   > **Note**
   >
   > このワークフローに既存の Amazon DataZone ドメインを使用する場合は、ドメインの表示 を選択し、使用するドメインを選択してから、公開プロジェクトの作成のステップ 2 に進みます。

2. ドメインの作成ページで、次のフィールドに値を指定します。

   - 名前 - ドメインの名前を指定します。このワークフローでは、このドメイン を呼び出すことができます`Marketing`。
   - 説明 - オプションのドメインの説明を指定します。
   - データ暗号化 - データは、デフォルトで次のキーで暗号化されます。 AWS はお客様に代わって を所有および管理します。このチュートリアルでは、デフォルトのデータ暗号化設定のままにしておくことができます。

     カスタマーマネージドキーの使用の詳細については、「」を参照してくださいAmazon の保管中のデータ暗号化 DataZone。データ暗号化に独自のKMSキーを使用する場合は、デフォルトの に次のステートメントを含める必要がありますAmazonDataZoneDomainExecutionRole。

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

- サービスアクセス - カスタムサービスロールの使用 オプションを選択し、ドロップダウンメニューAmazonDataZoneDomainExecutionRoleから を選択します。
- 「クイックセットアップ」で、データ消費と の公開のためにこのアカウントを設定するを選択します。このオプションは、データレイクとデータウェアハウスの組み込み Amazon DataZone ブループリントを有効にし、このワークフローの残りのステップを完了するために必要なアクセス許可とリソースを設定します。Amazon DataZone ブループリントの詳細については、「」を参照してくださいAmazon DataZone の用語と概念。
- アクセス許可の詳細とタグの残りのフィールドを変更せずに、ドメインの作成 を選択します。

3. ドメインが正常に作成されたら、このドメインを選択し、ドメインの概要ページで、このドメインのデータポータルURLを書き留めます。これを使用して Amazon DataZone データポータルURLにアクセスし、このワークフローの残りのステップを完了できます。

> **Note**
>
> Amazon の現在のリリースでは DataZone、ドメインが作成されると、データポータル用にURL生成された を変更することはできません。

ドメインの作成が完了するまでに数分かかる場合があります。次のステップに進む前に、ドメインのステータスが Available になるまで待ちます。

ステップ 2 - 公開プロジェクトを作成する

次のセクションでは、このワークフローで公開プロジェクトを作成する手順について説明します。

1. ステップ 1 を完了したら、 DataZone データポータルを使用して Amazon データポータルに移動URLし、シングルサインオン (SSO) または を使用してログインします。 AWS IAM 認証情報。
2. 「プロジェクトの作成」を選択し、プロジェクト名を指定します。例えば、このワークフローでは、名前を にしSalesDataPublishingProject、残りのフィールドは変更せずにおき、「作成」を選択します。

ステップ 3 - 環境を作成する

次のセクションでは、このワークフローで環境を作成する手順について説明します。

1. ステップ 2 を完了したら、Amazon DataZone データポータルで、前のステップで作成したSalesDataPublishingProjectプロジェクトを選択し、環境 タブを選択し、環境の作成を選択します。
2. 「環境の作成」ページで以下を指定し、「環境の作成」を選択します。

   - 名前 - 環境の名前を指定します。このチュートリアルでは、 と呼びますDefault data warehouse environment。
   - 説明 - 環境の説明を指定します。
   - 環境プロファイル - DataWarehouseProfile環境プロファイルを選択します。
   - Amazon Redshift クラスターの名前、データベース名、およびデータが保存されている Amazon Redshift クラスターARNのシークレットを指定します。

     > **Note**
     >
     > のシークレットを確認します。 AWS Secrets Manager には、次のタグ (キー/値) が含まれています。
     >
     > - Amazon Redshift クラスターの場合 - datazone.rs.cluster: <cluster_name:database name>
     >
     >   Amazon Redshift Serverless ワークグループの場合 - datazone.rs.workgroup: <workgroup_name:database_name>
     > - AmazonDataZoneProject: <projectID >

- AmazonDataZoneDomain: <domainID >

詳細については、「 でのデータベース認証情報の保存」を参照してください。 AWS Secrets Manager 。
で指定したデータベースユーザー AWS Secrets Manager にはスーパーユーザーアクセス許可が必要です。

ステップ 4 - 公開用のデータを生成する

次のセクションでは、このワークフローで公開するデータを生成する手順について説明します。

1. ステップ 3 を完了したら、Amazon DataZone データポータル でSalesDataPublishingProjectプロジェクトを選択し、右側のパネルの分析ツール で Amazon Redshift を選択します。これにより、プロジェクトの認証情報を使用して認証用の Amazon Redshift クエリエディタが開きます。
2. このチュートリアルでは、Create Table as Select (CTAS) クエリスクリプトを使用して、Amazon に発行する新しいテーブルを作成します DataZone。クエリエディタで、このCTASスクリプトを実行して、公開して検索とサブスクリプションに使用できるmkt_sls_tableテーブルを作成します。

```
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
```

m""_sls_table テーブルが正常に作成されたことを確認します。これで、Amazon DataZone カタログに公開できるデータアセットができました。

ステップ 5 - Amazon Redshift からメタデータを収集する

次のセクションでは、Amazon Redshift からメタデータを収集する手順について説明します。

1. ステップ 4 を完了したら、Amazon DataZone データポータルでSalesDataPublishingProjectプロジェクトを選択し、データタブを選択し、データソース を選択します。
2. 環境作成プロセスの一部として作成されたソースを選択します。
3. アクションドロップダウンメニューの横にある実行 を選択し、更新ボタンを選択します。データソースの実行が完了すると、アセットが Amazon DataZone インベントリに追加されます。

ステップ 6 - データアセットをキュレートして公開する

次のセクションでは、このワークフローでデータアセットをキュレートして公開する手順について説明します。

1. ステップ 5 を完了したら、Amazon DataZone データポータルでSalesDataPublishingProjectプロジェクトを選択し、データタブを選択し、インベントリデータ を選択し、mkt_sls_tableテーブルを見つけます。
2. mkt_sls_table アセットの詳細ページを開いて、自動的に生成されたビジネス名を表示します。自動生成されたメタデータアイコンを選択して、アセットと列の自動生成された名前を表示します。各名前を個別に承諾または拒否するか、すべて承諾を選択して生成された名前を適用できます。オプションで、使用可能なメタデータフォームをアセットに追加し、用語集の用語を選択してデータを分類することもできます。
3. Publish を選択してmkt_sls_tableアセットを公開します。

ステップ 7 - データ分析用のプロジェクトを作成する

次のセクションでは、このワークフローでデータ分析用の te プロジェクトを作成する手順について説明します。

1. ステップ 6 を完了したら、Amazon DataZone データポータルでプロジェクトの作成 を選択します。
2. 「プロジェクトの作成」ページでプロジェクト名を指定します。例えば、このワークフローでは、名前を にしMarketingDataAnalysisProject、残りのフィールドは変更せずにおき、「作成」を選択します。

ステップ 8 - データ分析用の環境を作成する

次のセクションでは、このワークフローでデータ分析用の環境を作成する手順について説明します。

1. ステップ 7 を完了したら、Amazon DataZone データポータルで、前のステップで作成したMarketingDataAnalysisProjectプロジェクトを選択し、環境タブを選択し、環境の追加を選択します。
2. 「環境の作成」ページで以下を指定し、「環境の作成」を選択します。

   - 名前 - 環境の名前を指定します。このチュートリアルでは、 と呼びますDefault data warehouse environment。
   - 説明 - 環境の説明を指定します。
   - 環境プロファイル - DataWarehouseProfile環境プロファイルを選択します。
   - Amazon Redshift クラスターの名前、データベース名、およびデータが保存されているAmazon Redshift クラスターARNのシークレットを指定します。

     > **Note**
     >
     > のシークレットを確認します。 AWS Secrets Manager には、次のタグ (キー/値) が含まれます。
     >
     > - Amazon Redshift クラスターの場合 - datazone.rs.cluster: <cluster_name:database name>
     >
     >   Amazon Redshift Serverless ワークグループの場合 - datazone.rs.workgroup: <workgroup_name:database_name>
     > - AmazonDataZoneProject: <projectID >
     > - AmazonDataZoneDomain: <domainID >
     >
     > 詳細については、「 でのデータベース認証情報の保存」を参照してください。 AWS Secrets Manager 。
     > で指定したデータベースユーザー AWS Secrets Manager にはスーパーユーザーアクセス許可が必要です。

   - このチュートリアルでは、残りのフィールドは変更しないでください。

ステップ 9 - データカタログを検索してデータをサブスクライブする

次のセクションでは、データカタログを検索し、データをサブスクライブする手順について説明します。

1. ステップ 8 を完了したら、Amazon DataZone データポータルで、データポータルの検索バーでキーワード (「カタログ」や「売上」など) を使用してデータアセットを検索します。

   必要に応じて、フィルターまたはソートを適用し、製品販売データアセットを見つけたら、アセットの詳細ページを開くように選択できます。
2. 製品販売データアセットの詳細ページで、「サブスクライブ」を選択します。
3. ダイアログで、ドロップダウンからコンシューマープロジェクトを選択し、アクセスリクエストの理由を入力し、「サブスクライブ」を選択します。

ステップ 10 - サブスクリプションリクエストを承認する

次のセクションでは、このワークフローでサブスクリプションリクエストを承認する手順について説明します。

1. ステップ 9 を完了したら、Amazon DataZone データポータルで、アセットを公開したSalesDataPublishingProjectプロジェクトを選択します。
2. データタブを選択し、次に公開されたデータ を選択し、次に着信リクエスト を選択します。
3. ビューリクエストリンクを選択し、承認 を選択します。

ステップ 11 - Amazon Redshift でクエリを構築し、データを分析する

アセットを Amazon DataZone カタログに正常に公開し、サブスクライブしたので、分析できます。

1. Amazon DataZone データポータルの右側のパネルで、Amazon Redshift リンクをクリックします。これにより、認証にプロジェクトの認証情報を使用して Amazon Redshift クエリエディタが開きます。
2. サブスクライブされたテーブルでクエリ (select ステートメント) を実行できるようになりました。テーブル (three-vertical-dots オプション) をクリックし、プレビューを選択すると、エディタ画面で select ステートメントが表示されます。クエリを実行して結果を表示します。

サンプルスクリプトを使用した Amazon DataZone クイックスタート

Amazon には、管理ポータルまたは Amazon DataZone データポータル DataZone 経由で、または Amazon DataZone HTTPS を使用してプログラムでアクセスできます。これによりAPI、サービスに直接HTTPSリクエストを発行できます。このセクションには、以下の一般的なタスクを完了するために使用できる Amazon DataZone APIs を呼び出すサンプルスクリプトが含まれています。

サンプルスクリプト

- Amazon DataZone ドメインとデータポータルを作成する
- 公開プロジェクトを作成する
- 環境プロファイルを作成する
- 環境の作成
- からメタデータを収集する AWS 接着語
- データアセットをキュレートして公開する
- データカタログを検索してデータをサブスクライブする
- その他の便利なサンプルスクリプト

Amazon DataZone ドメインとデータポータルを作成する

次のサンプルスクリプトを使用して Amazon DataZone ドメインを作成できます。Amazon DataZone ドメインの詳細については、「」を参照してくださいAmazon DataZone の用語と概念。

```
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",
    )
```

公開プロジェクトを作成する

次のサンプルスクリプトを使用して、Amazon で公開プロジェクトを作成できます DataZone。

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

環境プロファイルを作成する

次のサンプルスクリプトを使用して、Amazon で環境プロファイルを作成できます DataZone。

このサンプルペイロードは、 `CreateEnvironmentProfile` API が呼び出されるときに使用されます。

```
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"]
            }
        ]
    }
}
```

このサンプルスクリプトはCreateEnvironmentProfile、 を呼び出しますAPI。

```
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
```

これは、 が呼び出された後のサンプル出力ペイロードCreateEnvironmentProfileAPIです。

```
{
    "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": ""
                    }
                ]
            }
        ]
    }
}
```

環境の作成

次のサンプルスクリプトを使用して、Amazon で環境を作成できます 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
```

からメタデータを収集する AWS 接着語

このサンプルスクリプトを使用して、 からメタデータを収集できます。 AWS Glue。このスクリプトは標準スケジュールで実行されます。サンプルスクリプトからパラメータを取得し、グローバルにすることができます。標準関数を使用してプロジェクト、環境、ドメイン ID を取得します。- AWS

Glue データソースは、スクリプトの cron セクションで更新できる標準時刻に作成および実行されます。

```
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"
    }
}
```

データアセットをキュレートして公開する

次のサンプルスクリプトを使用して、Amazon でデータアセットをキュレートして公開できます DataZone。

次のスクリプトを使用してカスタムフォームタイプを作成できます。

```
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"
    )
```

次のサンプルスクリプトを使用して、カスタムアセットタイプを作成できます。

```
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,
    )
```

次のサンプルスクリプトを使用して、カスタムアセットを作成できます。

```
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\"}"
            }
        ]
    )
```

次のサンプルスクリプトを使用して用語集を作成できます。

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

次のサンプルスクリプトを使用して用語集の用語を作成できます。

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

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

次のサンプルスクリプトを使用して、システム定義のアセットタイプを使用してアセットを作成できます。

```
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\"}"
            }
        ]
    )
```

次のサンプルスクリプトを使用してアセットリビジョンを作成し、用語集の用語をアタッチできます。

```
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:>"]
    )
```

次のサンプルスクリプトを使用してアセットを発行できます。

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

データカタログを検索してデータをサブスクライブする

次のサンプルスクリプトを使用して、データカタログを検索し、データをサブスクライブできます。

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

次のサンプルスクリプトを使用して、アセットのリスト ID を取得できます。

```
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']
```

次のサンプルスクリプトを使用して、リスト ID を使用してサブスクリプションリクエストを作成できます。

```
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."
```

```
    )
```

create_subscription_response 上記を使用して を取得し subscription_request_id、次のサンプルスクリプトを使用してサブスクリプションを承諾/承認します。

```
subscription_request_id = create_subscription_response["id"]

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

その他の便利なサンプルスクリプト

次のサンプルスクリプトを使用して、Amazon でデータを操作するときにさまざまなタスクを完了できます DataZone。

次のサンプルスクリプトを使用して、既存の Amazon DataZone ドメインを一覧表示します。

```
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
```

次のサンプルスクリプトを使用して、既存の Amazon DataZone プロジェクトを一覧表示します。

```
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
```

次のサンプルスクリプトを使用して、既存の Amazon DataZone メタデータフォームを一覧表示します。

```
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
```

Amazon でのドメインとユーザーアクセス DataZone

このセクションでは、Amazon でドメインとユーザーアクセスを作成および管理する方法を説明します DataZone。

Amazon DataZone ドメインは、アセット、ユーザー、およびプロジェクトを連結するための組織エンティティです。Amazon DataZone ドメインを使用すると、エンタープライズ DataZone 用の単一の Amazon ドメインを作成するか、複数のデータゾーンを作成するか、異なるビジネスユニットやチーム用のドメインを作成するかにかかわらず、組織構造のデータと分析のニーズを柔軟に反映できます。

このセクションでは、Amazon DataZone コンソールと Amazon DataZone ポータルへのユーザーアクセスの管理についても説明します。

詳細については、「Amazon DataZone の用語と概念」を参照してください。

トピック

- Amazon DataZone ドメインを作成する
- Amazon DataZone ドメインを編集する
- Amazon DataZone ドメインを削除する
- Amazon の IAM Identity Center を有効にする DataZone
- Identity Center for Amazon IAM を無効にする DataZone
- Amazon DataZone コンソールでユーザーを管理する
- Amazon DataZone データポータルでユーザーアクセス許可を管理する

Amazon DataZone ドメインを作成する

> **Note**
>
> DataZone で Amazon を使用している場合 AWS SSO ユーザーとグループへのアクセスを提供する Identity Center では、現在 Amazon DataZone ドメインが同じ に存在する必要があります。 AWS としてのリージョン AWS Identity Center インスタンス。

Amazon DataZone、ドメインは、アセット、ユーザー、およびそれらのプロジェクトを連結するための組織エンティティです。詳細については、「Amazon DataZone の用語と概念」を参照してください。

Amazon DataZone ドメインを作成するには、管理アクセス許可を持つアカウントで IAMロールを引き受ける必要があります。 Amazon DataZone マネジメントコンソールを使用するために必要なIAMアクセス許可を設定するは、ドメインの作成に必要な最小限のアクセス許可を取得する必要があります。

デフォルト設定のドメインユーザーに代わってアクションを実行 DataZone するには、Amazon によって追加のIAMロールが必要です。これらのIAMロールは、事前に作成することも、Amazon に DataZone 作成させることもできます。ドメイン作成プロセス中に Amazon DataZone がこれらのIAMロールを作成する場合は、ドメイン作成時にIAMロール作成権限を持つ ロールを引き受ける必要があります。「Amazon DataZone サービスコンソールのロール作成を簡素化するIAMアクセス許可のカスタムポリシーを作成する 」を参照してください。ドメイン作成の選択に応じて、Amazon DataZone は 、AmazonDataZoneDomainExecutionRole、、 の 4 つの新しいIAMロールを作成しますAmazonDataZoneGlueManageAccessRoleAmazonDataZoneRedshiftManageAccessRoleAmazonDataZon

Amazon DataZone ドメインを作成するには、次の手順を実行します。

1. https://console.aws.amazon.com/datazone の Amazon DataZone コンソールに移動し、上部のナビゲーションバーのリージョンセレクターを使用して適切な を選択します。 AWS リージョン。
2. ドメインの作成を選択し、次のフィールドに値を指定します。

   - 名前 - ドメインのフレンドリ名を指定します。ドメインが作成されると、この名前を変更することはできません。
   - 説明 - (オプション) ドメインの説明を指定します。
   - データ暗号化 - Amazon DataZone ドメイン、メタデータ、レポートデータは によって暗号化されます。 AWS Amazon に固有のキーを使用する Key Management Service (KMS) DataZone。このフィールドを使用して、 を使用するかどうかを指定します。 AWS 所有キー、または別のキーを選択する AWS KMS キー。

     カスタマーマネージドキーの使用の詳細については、「」を参照してくださいAmazon の保管中のデータ暗号化 DataZone。データ暗号化に独自のKMSキーを使用する場合は、デフォルトの に次のステートメントを含める必要がありますAmazonDataZoneDomainExecutionRole。

     ```
     {
     ```

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

- サービスアクセス - Amazon に新しい DataZone を作成して使用するかDomainExecutionRole、既存のIAMロールを選択するかを選択します。
- クイックセットアップ - (オプション) このチェックボックスをオンにすると、Amazon がデータ消費と公開のためにアカウントを DataZone セットアップすることで、より迅速に開始できます。Amazon DataZone は、 へのアクセスをプロビジョニング、取り込み、管理するための 3 つのIAMロールを作成します。 AWS Glue と Amazon Redshift のリソース、新しい Amazon S3 バケットの作成、管理用 Amazon DataZone プロジェクトの作成、データレイクとデータウェアハウスのデフォルト設計図の環境プロファイルの作成を行います。
- タグ - (オプション) 指定 AWS ドメインの タグ (キーと値のペア) 。
- ドメインが正常に作成されると、ブラウザが更新され、新しい Amazon DataZone ドメインの詳細ページが表示されます。

Amazon DataZone ドメインを編集する

Amazon では DataZone、ドメインはアセット、ユーザー、およびそれらのプロジェクトを連結するための組織エンティティです。詳細については、「Amazon DataZone の用語と概念」を参照してください。

Amazon DataZone ドメインを作成したら、後でドメインを編集して、説明の変更、IAMIdentity Center の有効化、タグキーとその値の追加、編集、削除を行うことができます。Amazon DataZone ドメインを編集するには、管理アクセス許可を持つアカウントで IAMロールを引き受ける必要があ

ります。 Amazon DataZone マネジメントコンソールを使用するために必要なIAMアクセス許可を設定するは、ドメインの編集に必要な最小限のアクセス許可を取得する必要があります。

ドメインを編集するには、次のステップを実行します。

1. にサインインする AWS マネジメントコンソール を開き、/datazone で Amazon DataZone コンソールを開きます。 https://console.aws.amazon.com
2. ドメインを表示を選択し、リストからドメイン名を選択します。名前はハイパーリンクです。
3. ドメインの詳細ページで、編集 を選択します。
4. • 説明 を編集します。
   • IAM Identity Center 設定 を設定します。これらの設定の詳細については、「」を参照してください設定 AWS IAM Amazon 用 Identity Center DataZone。
   • タグキーとその値を追加、編集、または削除します。
5. 編集が完了したら、ドメインの更新 を選択します。

Amazon DataZone ドメインを削除する

Amazon では DataZone、ドメインはアセット、ユーザー、およびそれらのプロジェクトを連結するための組織エンティティです。詳細については、「Amazon DataZone の用語と概念」を参照してください。

ドメインを削除する行為は最終的なものです。削除により、データソース、プロジェクト、環境、アセット、用語集、メタデータフォームなど、すべての Amazon DataZone エンティティが取り消し不能で削除されます。削除しても Amazon 以外の は削除されません DataZone AWS IAM ロール DataZone 、S3 バケット、 AWS Glue データベース、 LakeFormation または Redshift を介したサブスクリプション付与。これらのリソースが不要になった場合は、それぞれの で削除します。 AWS サービス。

誰かがドメインを悪意を持って削除しないようにするには、ドメインを削除するには Amazon の管理IAMアクセス許可が必要です。これは DataZone、 で設定できますIAM。誰かがドメインを誤って削除しないようにするには、ドメインを削除するには、確認ワード (Amazon DataZone コンソール内) が必要です。

ドメインを削除するには、次のステップを実行します。

1. にサインインする AWS マネジメントコンソール を開き、/datazone で Amazon DataZone コンソールを開きます。 https://console.aws.amazon.com

2. ドメインを表示を選択し、リストからドメイン名を選択します。名前はハイパーリンクです。
3. 削除を選択し、情報警告を確認します。
4. リクエストされたテキストを入力して、これらの警告を理解したことを確認します。[削除] を選択します。

> **Important**
>
> ドメインの削除は取り消し不可能なアクションであり、ユーザーまたは によって元に戻すことはできません。 AWS.

> **Note**
>
> ユーザーまたはドメインユーザーがプロジェクトに環境を作成すると、Amazon DataZone は を作成します。 AWS ドメインまたは関連するアカウントの リソース。ユーザーおよびドメインユーザーに機能を提供します。以下は のリストです。 AWS Amazon がドメイン内のプロジェクト用に作成 DataZone できる リソースとデフォルト名。ドメインを削除しても、これらのいずれも削除されません。 AWS の リソース AWS アカウント。
>
> - IAM roles: datazone_usr_<environmentId > 。
> - Glue データベース: (1) <environmentName>_pub_db-*、(2) <environmentName>_sub_db-*。この名前の既存のデータベースがすでにある場合、Amazon DataZone は環境 ID を追加します。
> - Athena ワークグループ: <environmentName>-*。この名前の既存のワークグループがすでに存在する場合、Amazon DataZone は環境 ID を追加します。
> - CloudWatch ロググループ: datazone_<environmentId >

Amazon の IAM Identity Center を有効にする DataZone

> **Note**
>
> この手順を完了するには、 AWS IAM 同じ で有効になっている Identity Center AWS Amazon DataZone ドメインとしての リージョン。

を使用して、Amazon DataZone データポータルへのアクセスをSSOユーザーとグループに許可できます。 AWS IAM Identity Center。を完了すると設定 AWS IAM Amazon 用 Identity Center DataZone、SSOユーザーとグループが Amazon DataZone ドメインデータポータルにアクセスできるようになります。

を有効にするには AWS IAM Amazon DataZone ドメインで使用する Identity Center では、管理アクセス許可を持つアカウントで IAMロールを引き受ける必要があります。 Amazon DataZone マネジメントコンソールを使用するために必要なIAMアクセス許可を設定するおよび Amazon DataZone サービスコンソールのロール作成を簡素化するIAMアクセス許可のカスタムポリシーを作成する は、IAMIdentity Center を Amazon で使用するために必要な最小限のアクセス許可を取得する必要があります DataZone。

を有効にするには、次の手順を実行します。 AWS IAM Amazon の Identity Center DataZone。

1. にサインインする AWS マネジメントコンソール を開き、https://console.aws.amazon.com/datazone で DataZone コンソールを開きます。
2. ドメインを表示を選択し、リストからドメイン名を選択します。名前はハイパーリンクです。
3. ドメインの詳細ページで、編集 を選択します。
   - IAM Identity Center でユーザーを有効にする のチェックボックスをオンにします。
   - 2 つのユーザー割り当てモードから選択します。選択内容でドメインが更新されると、後で変更することはできません。
     - 暗黙的なユーザー割り当て を使用すると、IAMIdentity Center ディレクトリに追加されたすべてのユーザーが Amazon DataZone ドメインにアクセスできます。
     - 明示的なユーザー割り当て では、IAMIdentity Center ディレクトリから特定のユーザーまたはグループを追加して、Amazon DataZone ドメインへのアクセスを許可します。これらのユーザーとグループは、後で Amazon DataZone コンソールで追加および削除します。
4. 選択内容に問題がなければ、ドメインの更新 を選択します。

Identity Center for Amazon IAM を無効にする DataZone

無効化 AWS IAM Amazon DataZone ドメインの Identity Center は、すべてのSSOユーザーのアクセスを削除します。

> **Note**
>
> IAM Identity Center を無効にしても、SSOユーザーの請求は停止されません。SSO ユーザーの請求を停止するには、ドメインでユーザーを非アクティブ化する必要があります。請求は、ユーザーが非アクティブ化された月末まで継続されます。ユーザーを非アクティブ化するには、「」を参照してくださいAmazon DataZone コンソールでユーザーを管理する。

を使用して、Amazon DataZone データポータルへのアクセスをSSOユーザーとグループに許可できます。 AWS IAM Identity Center。を有効にしている場合 AWS IAM Identity Center for Amazon では DataZone、後ですべてのユーザーのアクセスを無効にすることができます。

を無効にするには AWS IAM Amazon DataZone ドメインで使用する Identity Center では、管理アクセス許可を持つ アカウントの IAM ロールを引き受ける必要があります。 Amazon DataZone マネジメントコンソールを使用するために必要なIAMアクセス許可を設定するおよび Amazon DataZone サービスコンソールのロール作成を簡素化するIAMアクセス許可のカスタムポリシーを作成する は、IAMIdentity Center を Amazon で使用できなくなるために必要な最小限のアクセス許可を取得する必要があります DataZone。

を無効にするには、次の手順を実行します。 AWS IAM Amazon の Identity Center DataZone。

1. にサインインする AWS マネジメントコンソール を開き、https://console.aws.amazon.com/datazone で DataZone コンソールを開きます。
2. ドメインを表示を選択し、リストからドメイン名を選択します。名前はハイパーリンクです。
3. ドメインの Amazon リソースネーム (ARN) をコピーします。これは、arn:aws:datazone:<regionName>:<accountId>:domain/<domainName> で始まります。
4. で IAM Identity Center コンソールを開きますhttps://console.aws.amazon.com/singlesignon/。
5. [Applications] (アプリケーション) を選択します。
6. 無効にするドメインを選択する AWS IAM Identity Center は、その結果、すべてのSSOユーザーのドメインのデータポータルへのアクセスを削除します。フィルターメニューと検索ボックスを使用して、アプリケーションのリストをフィルタリングできます。
7. アクションメニューから、 の無効化を選択します。
8. SSO ユーザーは Amazon DataZone ドメインにアクセスできなくなります。
9. を再度有効にするには AWS IAM Amazon DataZone ドメインの Identity Center で、再度有効にするドメインを選択します。 AWS IAM Identity Center で、アクションメニューから を有効にする を選択します。

Amazon DataZone コンソールでユーザーを管理する

ユーザーは、 のいずれかを使用して Amazon DataZone データポータルにアクセスできます。AWS 認証情報またはシングルサインオン (SSO) 認証情報。Amazon DataZone ドメインの Amazon DataZone コンソールでユーザーを管理するには、管理アクセス許可を持つアカウントの IAMロールを引き受ける必要があります。 Amazon DataZone マネジメントコンソールを使用するために必要なIAMアクセス許可を設定するは、Amazon DataZone コンソールでユーザーを管理するために必要な最小限のアクセス許可を取得する必要があります。

トピック

- IAM ロールとユーザーの管理
- SSO ユーザーを管理する
- SSO グループの管理

IAM ロールとユーザーの管理

IAM ロールとユーザーは、 を使用して作成されます。 AWS Identity and Access Management (IAM) と は、ポリシーを介してアタッチされたアクセス許可を通じて Amazon DataZone ドメインにアクセスできます。詳細については、「Amazon DataZone データポータルを使用するために必要なIAMアクセス許可を設定する」を参照してください。Amazon の現在のリリースでは DataZone、Amazon DataZone ドメイン所有者アカウントの管理者は、自分のアカウントまたは関連付けられたアカウントのユーザーのユーザーIAMプロファイルを作成できます。Amazon DataZone ドメイン所有者アカウントの管理者は、既存のユーザーのステータスを割り当て済みまたは未割り当て (Amazon を使用するための割り当て済みまたは未割り当て DataZone) に設定したり、既存のユーザーをアクティブ化または非アクティブ化したりすることもできます。

1. にサインインする AWS マネジメントコンソール を開き、https://console.aws.amazon.com/datazone で DataZone コンソールを開きます。
2. ドメインを表示を選択し、リストからドメイン名を選択します。名前はハイパーリンクです。
3. ドメインの詳細ページで、ユーザー管理 を選択します。
4. Amazon DataZone ドメイン所有者アカウントまたは関連付けられたアカウントにIAMユーザーを追加するには、追加 を選択し、IAMユーザーの追加 を選択します。
5. ユーザーの追加ページで、現在のアカウントまたは関連アカウント を選択し、ユーザーまたはロールの検索と追加 フィールドを使用して追加するユーザーを検索し、ユーザーの追加 を選択します。

6. 既存のIAMユーザーのステータスを表示するには、ユーザー管理ページで、IAMユーザータイプのドロップダウンメニューでユーザーを選択します。

   - Name 列には、IAMユーザーまたはロールARNの が表示されます。
   - ステータス列には、ドメイン内のIAMユーザーまたはロールの現在のステータスが表示されます。
     - 割り当てられた は、IAMユーザーが Amazon を使用するように割り当てられたことを意味します DataZone。
     - 未割り当てとは、IAMユーザーが Amazon を使用するように未割り当てであることを意味します DataZone。
     - アクティブ化とは、IAMユーザーまたはロールが を呼び出したかAPI、コマンドを発行したか (コマンドラインインターフェイスを使用) 、ドメインの Amazon DataZone ポータルにアクセスし、ユーザーのサブスクリプションに対して課金されることを意味します。
     - 非アクティブ化は、IAMユーザーまたはロールが Amazon DataZone ドメインへのアクセスをブロックしていることを意味します。
7. 現在アクティブ化されているIAMユーザーまたはロールを非アクティブ化するには、ユーザーの横にあるチェックボックスをオンにし、アクションメニューから非アクティブ化を選択します。ユーザーは Amazon DataZone ドメインにアクセスできなくなります。ユーザーの請求は、現在の暦月末に終了します。
8. 現在非アクティブ化されているIAMユーザーまたはロールをアクティブ化するには、ユーザーの横にあるチェックボックスをオンにし、アクションメニューからアクティブ化を選択します。ユーザーまたはロールに適切なアクセス許可がある場合、IAMユーザーは Amazon DataZone ドメインにアクセスできます。ユーザーの請求が再開されます。

SSO ユーザーを管理する

SSO ユーザーが で作成または ID プロバイダーと同期される AWS IAM Identity Center。詳細については、設定 AWS IAM Amazon 用 Identity Center DataZone「」およびAmazon の IAM Identity Center を有効にする DataZone「」を参照して、 を有効にして設定します。 AWS IAM Amazon の Identity Center DataZone。ドメインに割り当てられたSSOユーザーのリストを表示したり、SSO ユーザーを追加したり、SSOユーザーを削除したりできます。

1. にサインインする AWS マネジメントコンソール を開き、https://console.aws.amazon.com/datazone で DataZone コンソールを開きます。
2. ドメインを表示を選択し、リストからドメイン名を選択します。名前はハイパーリンクです。

3. ドメインの詳細ページで、下にスクロールし、ユーザー管理 を選択します。
4. ユーザータイプで、SSOユーザーを選択して現在のSSOユーザーのリストを表示します。

   - Name 列には、SSOユーザー名が表示されます。
   - ステータス列には、ドメイン内のSSOユーザーの現在のステータスが表示されます。
     - 割り当てられた は、SSOユーザーがドメインに明示的に割り当てられていることを意味します。その結果、ユーザーは Amazon にアクセスできます DataZone。このステータスは、ドメインの ID プロバイダーモードが明示的な割り当てに設定されている場合にのみ使用されます。
     - アクティブ化とは、SSOユーザーがドメインの Amazon DataZone ポータルにアクセスし、ユーザーのサブスクリプションに対して課金されることを意味します。アクティベーションは自動的に行われます。
     - 非アクティブ化は、SSOユーザーのアクセスがドメインのデータポータルにブロックされることを意味します。ユーザーの請求は、アクセスが非アクティブ化された月の月末に終了しました。
     - 削除された は、SSOユーザーが以前にドメインに割り当てられたが、アクセスする前に削除されたことを意味します。
5. ユーザーの追加 と SSO ユーザーの追加 を選択してユーザーを追加します。このオプションは、ドメインが暗黙的なユーザー割り当てに設定されている場合は使用できません。つまり、ID プール内のすべてのユーザーが Amazon DataZone ドメインにアクセスできます。

   - ユーザーの追加ページで、追加するユーザーのエイリアスを検索します。検索ボックスの下に、一致する可能性のあるリストが表示されます。
   - 追加するユーザーを選択します。エイリアスは検索ボックスの下にチップとして表示されます。
   - 追加するユーザーのリストに問題がなければ、ユーザーを追加 (複数可) を選択します。
   - ユーザーには、ステータスが割り当てられた の Amazon DataZone ドメインが割り当てられます。
   - ユーザーがドメインのデータポータルに初めてアクセスすると、ステータスは自動的にアクティブ化された に変わり、ユーザーのサブスクリプションに対する請求が開始されます。
6. ユーザーSSOを選択し、アクションメニューから無効化を選択して、割り当てられたユーザーを削除します。その結果、ユーザーは Amazon DataZone ドメインにアクセスできなくなります。ユーザーのステータスは 削除済み と表示されます。このオプションは、ドメインが暗黙的なユーザー割り当てに設定されている場合は使用できません。

7. ユーザーSSOを選択し、アクションメニューから非アクティブ化を選択して、アクティブ化されたユーザーを非アクティブ化します。 その結果、Amazon DataZone ドメインへのユーザーのアクセスは失われ、ブロックされます。ユーザーのサブスクリプションに対する請求は、月末まで継続されます。ユーザーのステータスは非アクティブ化済み と表示されます。
8. ユーザーを選択し、アクションメニューからアクティブ化を選択して、非アクティブ化SSOされたユーザーをアクティブ化します。その結果、ユーザーは Amazon DataZone ドメインへのアクセスを回復します。請求はすぐに開始されます。ユーザーの はアクティブ化された と表示されます。

SSO グループの管理

SSO グループが で作成または ID プロバイダーと同期される AWS IAM Identity Center。詳細については、設定 AWS IAM Amazon 用 Identity Center DataZone「」およびAmazon の IAM Identity Center を有効にする DataZone「」を参照して、 を有効にして設定します。 AWS IAM Amazon の Identity Center DataZone。ドメインに割り当てられたSSOグループのリストを表示したり、SSOグループを追加したり、SSOグループを削除したりできます。

1. にサインインする AWS マネジメントコンソール を開き、https://console.aws.amazon.com/datazone で DataZone コンソールを開きます。
2. ドメインを表示を選択し、リストからドメイン名を選択します。名前はハイパーリンクです。
3. ドメインの詳細ページで、下にスクロールし、ユーザー管理 を選択します。
4. ユーザータイプで、SSOグループを選択して、グループの現在のリストを表示しますSSO。

   - Name 列には、SSOグループの名前が表示されます。
   - ステータス列には、ドメイン内のSSOグループの現在のステータスが表示されます。
     - 割り当てられた は、SSOグループがドメインに明示的に割り当てられていることを意味します。その結果、グループ内のすべてのユーザーがドメインのデータポータルにアクセスできます (ユーザーが非アクティブ化されている場合を除く) 。
     - 未割り当て は、SSOグループがドメインから削除されたことを意味します。グループのユーザーは、このグループのメンバーシップを介してドメインのデータポータルにアクセスできません。
5. SSO グループを追加 と グループを追加 を選択してグループを追加します。このオプションは、ドメインが暗黙的なユーザー割り当てに設定されている場合は使用できません。つまり、ID プール内のすべてのユーザーがグループメンバーシップに関係なく Amazon DataZone ドメインにアクセスできます。

- グループの追加ページで、追加するグループのエイリアスを検索します。検索ボックスの下に、一致する可能性のあるリストが表示されます。
- 追加するグループを選択します。エイリアスは検索ボックスの下にチップとして表示されます。
- 追加するグループのリストに問題がなければ、グループを追加 (複数可) を選択します。
- グループは Amazon DataZone ドメインに割り当てられ、ステータスは割り当て済み です。
- グループのメンバーからドメインのデータポータルにアクセスすると、ステータスは自動的にアクティブ化された に変わり、ユーザーのサブスクリプションに対する請求が開始されます。

6. 割り当てられたSSOグループを削除するには、グループを選択し、アクションメニューから割り当て解除を選択します。その結果、グループは Amazon DataZone ドメインにアクセスできなくなります。グループのステータスは未割り当て と表示されます。このグループのメンバーシップ DataZone を通じて Amazon にアクセスしたユーザーはアクセスできなくなります。このオプションは、ドメインが暗黙的なユーザー割り当てに設定されている場合は使用できません。グループの割り当てを解除してアクセスが削除されたユーザーの請求を停止するには、次にユーザープロファイルを手動で選択して非アクティブ化する必要があります。

Amazon DataZone データポータルでユーザーアクセス許可を管理する

Amazon の現在のリリースでは DataZone、デフォルトの認証メカニズムにより、Amazon DataZone ドメインのすべての認証済みユーザー (IAM および SSO) がプロジェクトの作成、プロジェクト内のエンティティの作成、検索を実行できます。プロジェクトメンバーは、指定されたプロジェクト所有者またはプロジェクト寄稿者ロールごとに付与されたアクセス許可に従う必要があります。

Amazon のドメインユニットと承認ポリシー DataZone

ドメインユニットを使用すると、アセットやその他のドメインエンティティを特定のビジネスユニットやチームで簡単に整理できます。組織のビジネスユニット間で安全かつ効率的なデータ共有を設定するには、Amazon DataZone 内でドメインユニットを作成し、各ビジネスユニット内の選択したユーザーがカタログにログインしてアセットを共有できるようにします。企業内のどこからでも、ユーザーはそれらのビジネスユニットのアセットを簡単に検索し、それらのアセットへのアクセスをリクエストできます。ドメインユニットを使用して、 などのリソース所有者を有効にすることもできます。 AWS アカウント所有者は、リソースに Amazon DataZone 認証アクセス許可を設定します。ドメインユニットは、アカウント所有者からドメインユニット所有者に委任された権限を提供し、アカウント所有者に代わって環境プロファイル (設計図設定を使用して作成された) に認証権限を設定できます。これにより、属するビジネスユニットに応じて、どの環境プロファイルを作成および使用できるユーザーを簡単に制限できます。Amazon DataZone 認証アクセス許可を使用してメタデータ標準を適用し、選択したプロジェクトのみがメタデータフォームと用語集を作成できるようにすることもできます。これにより、一貫性のある高品質のメタデータを維持できます。詳細については、「Amazon DataZone の用語と概念」を参照してください。

Amazon DataZone ドメインユニット内で、ユーザーとグループに次の承認ポリシーを割り当てて、ユーザーに特定のアクセス許可を付与できます。

- ドメイン単位作成ポリシー
- プロジェクト作成ポリシー
- プロジェクトメンバーシップポリシー
- ドメイン単位の所有権の引き受けポリシー
- プロジェクト所有権の引き受けポリシー

詳細については、「Amazon DataZone ドメイン単位内のユーザーとグループに承認ポリシーを割り当てる」を参照してください。

Amazon DataZone ドメインユニット内で、次の承認ポリシーをプロジェクトに割り当てて、特定のアクセス許可を付与できます。

- 用語集作成ポリシー
- メタデータフォーム作成ポリシー
- カスタムアセットタイプ作成ポリシー

詳細については、「Amazon DataZone ドメイン単位内のプロジェクトに承認ポリシーを割り当てる」を参照してください。

Amazon で認証メカニズムを使用するもう 1 つの方法は DataZone 、Amazon DataZone ブループリント設定内のプロジェクトとドメイン単位の所有者に認証ポリシーを適用することです。

Amazon DataZone ブループリント設定は、ユーザーワークフローの公開とサブスクライブに使用されるリソースの作成と設定に必要な情報をカプセル化するエンティティです。この情報には以下が含まれます。 AWS アカウント番号とリージョン、CFNテンプレート、 VPCs やサブネットなどのアカウントレベルのパラメータ、データベース接続情報と認証情報を含めることもできます。コストを管理し、セキュリティを向上させるために、データプラットフォームのユーザーには、これらのブループリントを使用できるユーザーを制御し、環境を作成できる機能が必要です。

特定のブループリント設定内で、プロジェクトとドメイン単位の所有者に次の承認ポリシーを割り当てることができます。

- このブループリントを使用して環境プロファイルを作成する - このポリシーは Amazon DataZone プロジェクトに割り当てることができ、このブループリントを使用して環境プロファイルを作成することを承認します。
- このブループリントを使用して環境プロファイルを作成するアクセス許可を付与する - このポリシーはドメイン単位の所有者に割り当てることができ、このブループリントを使用して環境プロファイルを作成するアクセス許可をプロジェクトに付与することを承認します。

詳細については、「Amazon DataZone ブループリント設定内で承認ポリシーを割り当てる」を参照してください。

トピック

- Amazon でドメインユニットを作成する DataZone
- Amazon でドメインユニットを編集する DataZone
- Amazon でドメインユニットを削除する DataZone
- Amazon でドメイン単位の所有者を管理する DataZone
- Amazon DataZone ドメイン単位内のユーザーとグループに承認ポリシーを割り当てる
- Amazon DataZone ドメイン単位内のプロジェクトに承認ポリシーを割り当てる
- Amazon DataZone ブループリント設定内で承認ポリシーを割り当てる

Amazon でドメインユニットを作成する DataZone

Amazon では DataZone、ドメインユニットを使用すると、アセットやその他のドメインエンティティを特定のビジネスユニットやチームで整理できます。詳細については、「Amazon DataZone の用語と概念」を参照してください。

ドメイン単位を作成するには

1. データポータルを使用して Amazon DataZone データポータルに移動URLし、 SSOまたは を使用してログインします。 AWS 認証情報。Amazon DataZone 管理者の場合は、 の https://console.aws.amazon.com/datazone にある Amazon DataZone コンソールURLにアクセスしてデータポータルを取得できます。 AWS Amazon DataZone ドメインが作成された アカウント。
2. ドメインを表示を選択し、ドメイン単位を作成するドメインを選択します。
3. ドメインの詳細ページで、ドメイン単位タブに移動します。
4. ドメイン単位の作成 を選択します。
5. 以下を指定し、ドメイン単位の作成 を選択します。
   - ドメイン単位の詳細 で、名前 にドメイン単位名を指定します。
   - ドメイン単位の詳細 で、説明 にドメイン単位の説明を指定します。
   - ドメイン単位の親 - 新しいドメイン単位を追加する親ドメイン単位を選択します。
   - ドメイン単位所有者 - このドメイン単位を編集できるドメイン単位所有者を指定します。

Amazon でドメインユニットを編集する DataZone

Amazon では DataZone、ドメインユニットを使用すると、アセットやその他のドメインエンティティを特定のビジネスユニットやチームで整理できます。詳細については、「Amazon DataZone の用語と概念」を参照してください。

ドメイン単位を編集するには

1. データポータルを使用して Amazon DataZone データポータルに移動URLし、 SSOまたは を使用してログインします。 AWS 認証情報。Amazon DataZone 管理者の場合は、 の https://console.aws.amazon.com/datazone にある Amazon DataZone コンソールURLにアクセスしてデータポータルを取得できます。 AWS Amazon DataZone ドメインが作成された アカウント。
2. ドメインを表示を選択し、ドメイン単位を編集するドメインを選択します。
3. ドメインの詳細ページで、ドメイン単位タブに移動し、編集するドメイン単位を選択します。

4. アクションを展開し、ドメイン単位の編集 を選択します。
5. ドメイン名と説明を変更し、変更を保存 を選択します。

Amazon でドメインユニットを削除する DataZone

Amazon では DataZone、ドメインユニットを使用すると、アセットやその他のドメインエンティティを特定のビジネスユニットやチームで整理できます。詳細については、「Amazon DataZone の用語と概念」を参照してください。

ドメイン単位を編集するには

1. データポータルを使用して Amazon DataZone データポータルに移動URLし、 SSOまたは を使用してログインします。 AWS 認証情報。Amazon DataZone 管理者の場合は、 の https://console.aws.amazon.com/datazone にある Amazon DataZone コンソールURLにアクセスしてデータポータルを取得できます。 AWS Amazon DataZone ドメインが作成された アカウント。
2. ドメインを表示を選択し、ドメイン単位を削除するドメインを選択します。
3. ドメインの詳細ページで、ドメイン単位タブに移動し、削除するドメイン単位を選択します。
4. アクション を展開し、ドメイン単位の削除 を選択します。
5. 「ドメイン単位の削除」ポップアップウィンドウで、「ドメイン単位の削除」を選択して削除を確認します。

Amazon でドメイン単位の所有者を管理する DataZone

Amazon では DataZone、ドメインユニットを使用すると、アセットやその他のドメインエンティティを特定のビジネスユニットやチームで整理できます。詳細については、「Amazon DataZone の用語と概念」を参照してください。

Amazon DataZone マネジメントコンソールを使用して最上位ドメインユニットに所有者を追加するには、次のステップを実行します。

1. https://console.aws.amazon.com/datazone の Amazon DataZone コンソールに移動し、アカウントの認証情報を使用してサインインします。
2. ドメインを表示を選択し、 DataZone ドメイン単位の所有者を追加する Amazon ドメインを選択します。
3. ドメインの詳細ページで、ドメインルート所有者タブに移動します。

4. 「追加」を選択し、「ドメイン単位所有者の追加」ポップアップウィンドウで、ドメイン単位所有者にするユーザーを指定します。「所有者の追加」を選択します。

Amazon DataZone Data Portal を介してドメイン単位の所有者を追加するには、次の手順を実行します。

1. データポータルを使用して Amazon DataZone データポータルに移動URLし、 SSOまたは を使用してログインします。 AWS 認証情報。Amazon DataZone 管理者の場合は、 の https://console.aws.amazon.com/datazone にある Amazon DataZone コンソールURLにアクセスしてデータポータルを取得できます。 AWS Amazon DataZone ドメインが作成された アカウント。
2. ドメインを表示を選択し、ドメインとドメイン単位所有者を追加するドメイン単位を選択します。
3. ドメイン単位の詳細ページで、所有者タブを選択し、所有者の追加を選択します。
4. 「ドメイン単位所有者の追加」ポップアップウィンドウで、ドメイン単位所有者にするユーザーを指定し、「所有者の追加」を選択します。

Amazon DataZone ドメイン単位内のユーザーとグループに承認ポリシーを割り当てる

Amazon では DataZone、ドメインユニットを使用すると、アセットやその他のドメインエンティティを特定のビジネスユニットやチームで整理できます。詳細については、「Amazon DataZone の用語と概念」を参照してください。

Amazon DataZone ドメインユニットでは、次の承認ポリシーをユーザーとグループに割り当てて、このドメインユニット内のさまざまな承認許可を付与できます。

- ドメイン単位作成ポリシー
- プロジェクト作成ポリシー
- プロジェクトメンバーシップポリシー
- ドメイン単位の所有権の引き受けポリシー
- プロジェクト所有権の引き受けポリシー

ドメイン単位内のユーザーとグループに承認ポリシーを割り当てるには、次の手順を実行します。

1. Amazon DataZone データポータルに移動URLし、シングルサインオン (SSO) または を使用してサインインします。 AWS 認証情報。Amazon DataZone 管理者の場合は、https://console.aws.amazon.com/datazone で Amazon DataZone コンソールに移動し、 でサインインできます。 AWS アカウント ドメインが作成された場所で、Open data portal を選択します。
2. ドメインを表示を選択し、承認ポリシーを割り当てるドメインとドメイン単位を選択します。
3. ドメイン単位の詳細ページで、ユーザー/グループに割り当てる承認ポリシーを選択し、ユーザーの追加 を選択します。
4. ユーザーの追加ポップアップウィンドウで、次のいずれかを実行します。
   - 選択したユーザーとグループ を選択し、選択した承認ポリシーを割り当てるユーザーとグループを指定し、ユーザーの追加 を選択します。
   - 「すべてのユーザー」を選択し、「ユーザーを追加」を選択します。
   - すべてのグループ を選択し、ユーザーの追加 を選択します。
5. 選択したユーザーの選択した承認ポリシーのカスケードアクセス許可を有効または無効にすることもできます。これを行うには、カスケードアクセス許可を有効にするユーザー (複数可) を選択し、アクション を展開して、カスケードアクセス許可を true に設定 を選択します。選択したユーザーには、このポリシーによってこのドメイン単位のすべての子ドメイン単位に付与されたアクセス許可があります。または、カスケードアクセス許可を無効にするユーザー (複数可) を選択し、アクション を展開して、カスケードアクセス許可を false に設定することもできます。

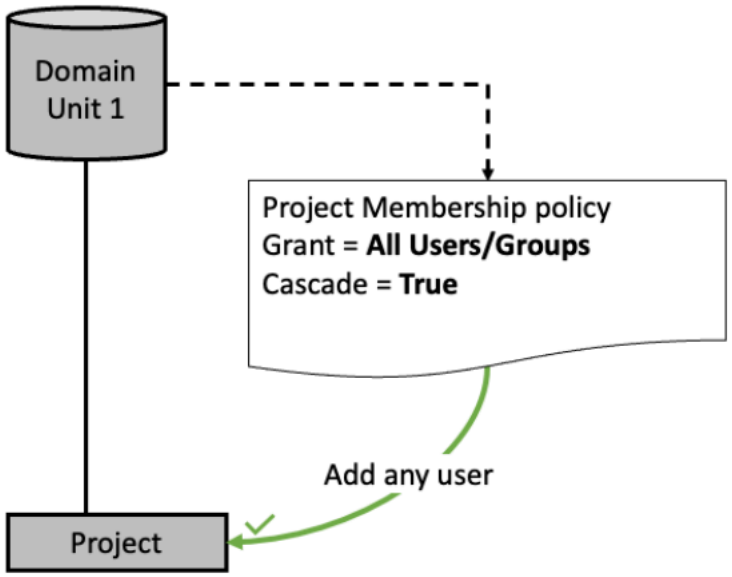
ドメイン単位の階層におけるプロジェクトメンバーシップポリシー

プロジェクトメンバーシップポリシーは、ドメイン単位内のプロジェクトにメンバーとして追加できる個人またはグループを定義します。このトピックでは、階層構造の個々のドメイン単位とドメイン単位に関連するポリシーの影響のシナリオについて説明します。

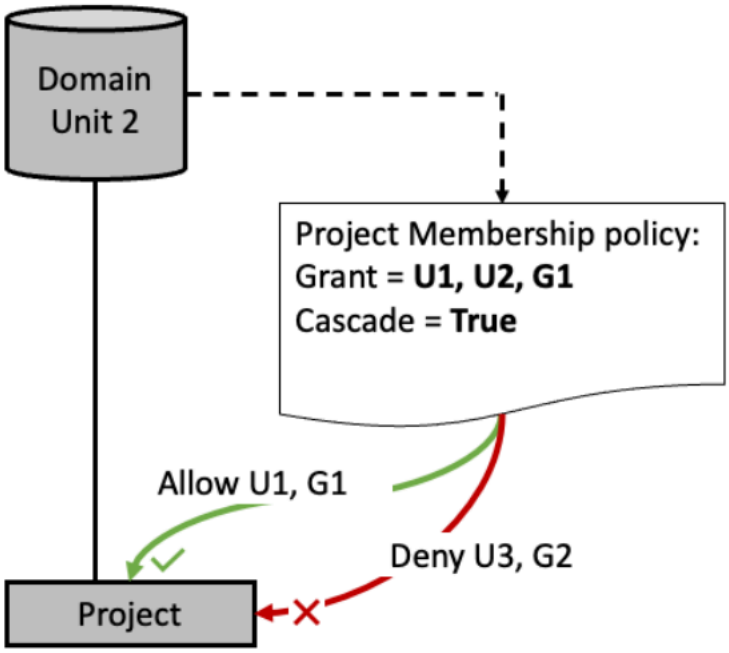
このトピックで使用されるいくつかの概念に注意することが重要です。

- メンバーシッププール - プロジェクトメンバーシップポリシーを通じてアクセス権が付与されたプリンシパル (ユーザーまたはグループ) は、プロジェクトメンバーシッププールの一部と見なされます。例えば、ドメイン単位のポリシーDU1がユーザー U1 と U2、および Single Sign-On (SSO) グループ G1 に付与されている場合、 のプロジェクトメンバーシッププールは {U1、U2, G1} DU1 で構成されます。
- カスケード - ドメイン単位階層を介して接続されているすべての子ドメイン単位に許可を渡す機能。
- grant - ユーザーまたはグループがアクションを実行するためのアクセス許可。

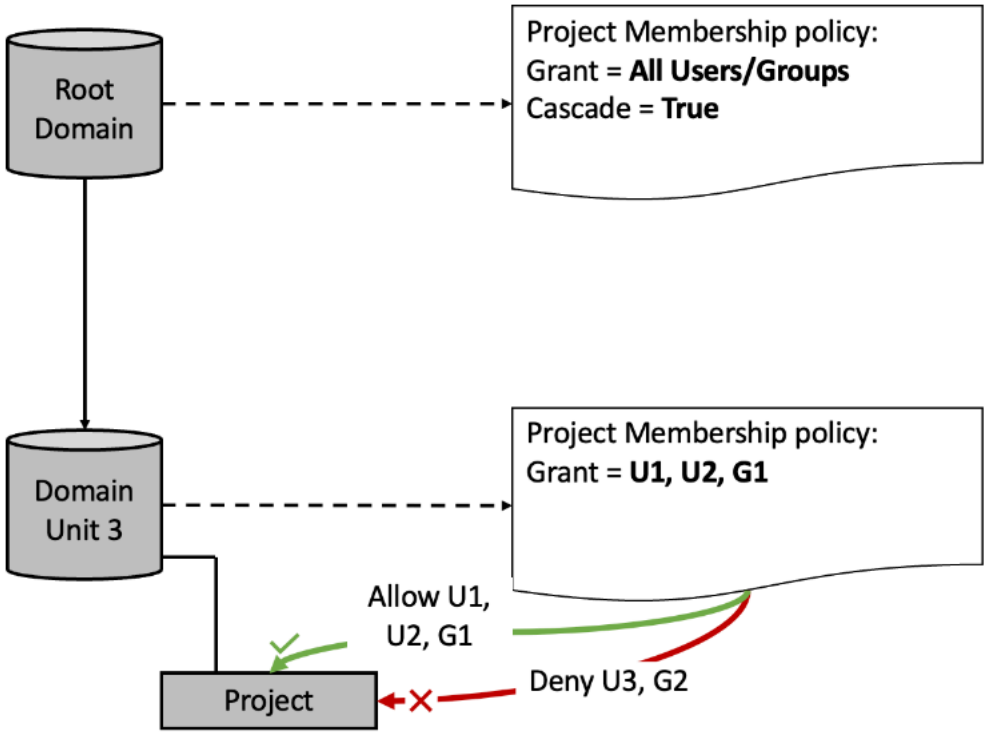
シナリオ 1 - メンバーシッププールが {すべてのユーザー/グループ} で構成されているため、ドメインユニット 1 のプロジェクトに任意のユーザーまたはグループを追加できます。



シナリオ 2 - ユーザー {U1, G1} はドメインユニット 2 のメンバーシッププールの一部であるため、ドメインユニット 2 のプロジェクトに追加できます。ユーザー {U3, G2} はメンバーシッププールに含まれていないため、プロジェクトに追加できません。

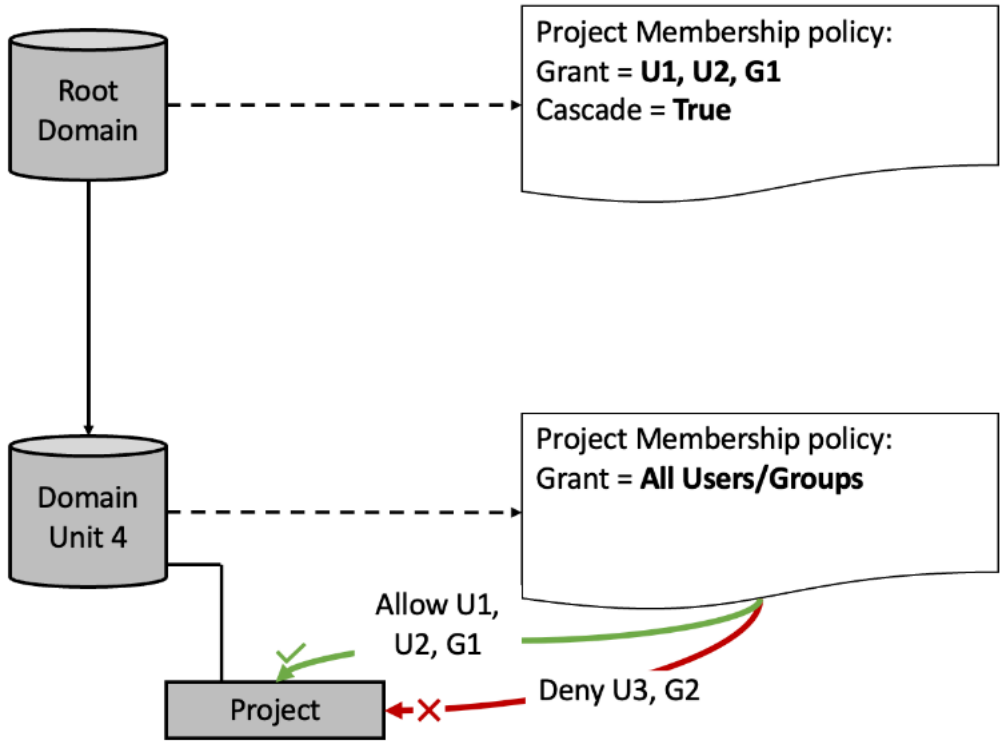


シナリオ 3 - メンバーシッププールの交差: 異なるドメイン単位階層レベルにメンバーシッププールがある場合、すべてのメンバーシッププールにあるユーザーとグループのみをプロジェクトに追加できます。



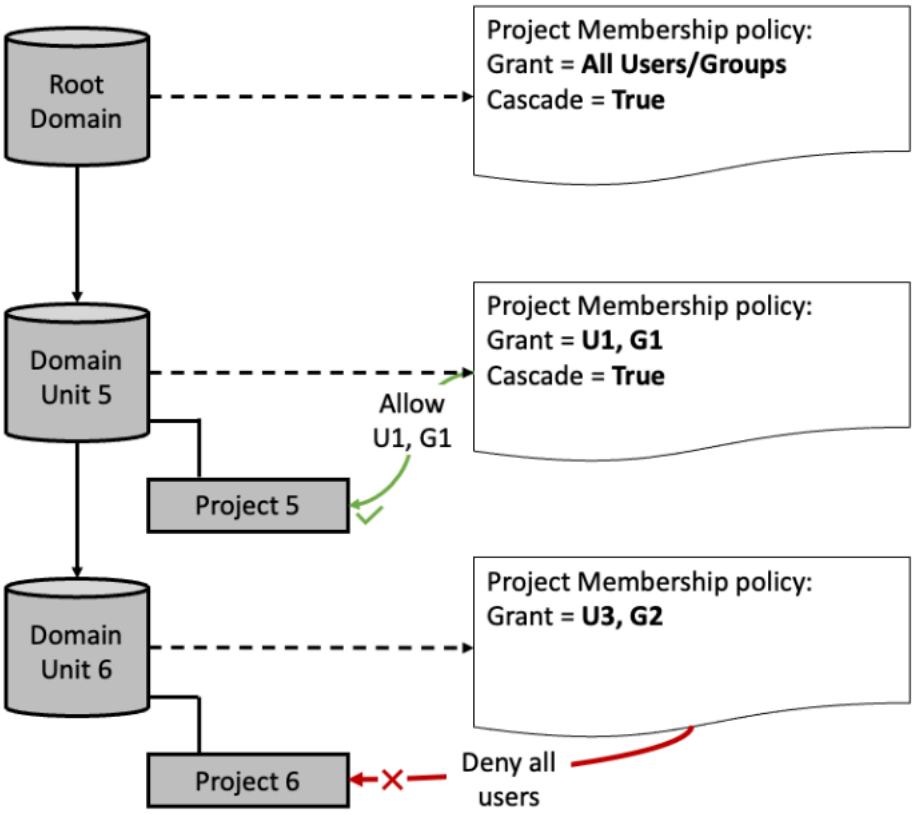
- 両方のメンバーシッププールにまたがるユーザーの共通部分は {U1, U2, G1} です。
- ユーザー {U1、U2, G1} はドメインユニット 3 のプロジェクトに追加できます。
- ユーザー {U3, G2} は、すべてのユーザーとすべてのグループがルートドメインユニットレベルのメンバーシッププールにある場合でも、ドメインユニット 3 のプロジェクトに追加できません。

シナリオ 4 - メンバーシッププールの交差: 異なるドメイン単位階層レベルにメンバーシッププールがある場合、すべてのメンバーシッププールにあるユーザーとグループのみをプロジェクトに追加できます。

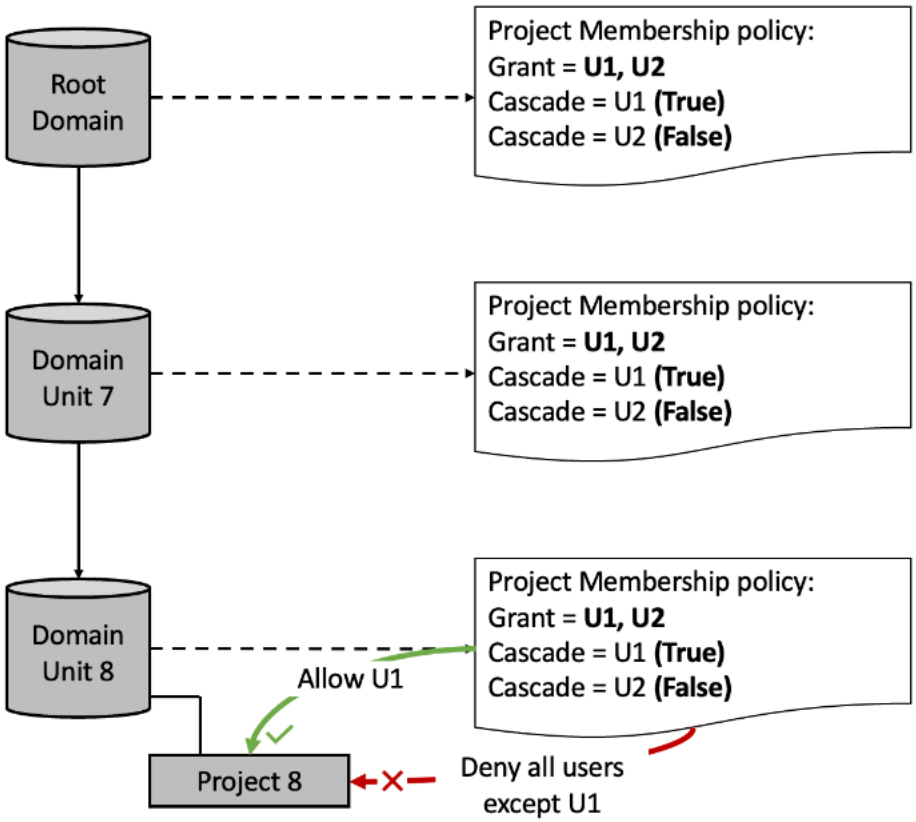


- 両方のメンバーシッププールにまたがるユーザーの共通部分は {U1, U2, G1} です。
- ドメインユニット 4 のメンバーシッププールは {All Users / Groups} ですが、メンバーシッププールはルートドメイン {U1、U2, G1} のメンバーシッププールを超えて拡張することはできません。
- ユーザー {U3, G2} は、すべてのユーザーとすべてのグループがドメインユニット 4 のメンバーシッププールにある場合でも、ドメインユニット 4 のプロジェクトに追加できません。

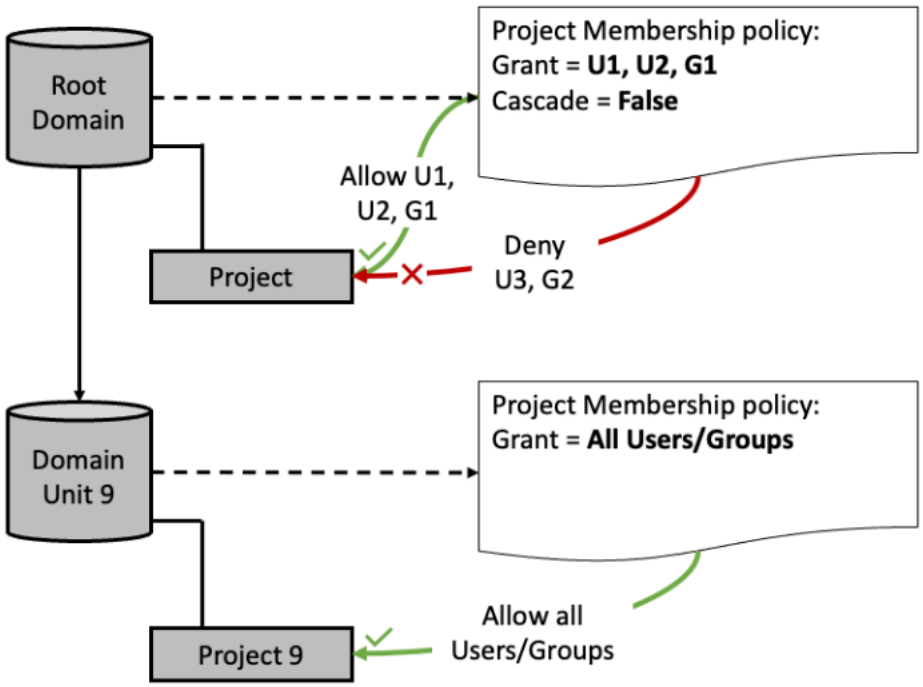
シナリオ 5 - ユーザー {U1, G1} は、ルートドメインとドメインユニット 5 の間のメンバーシッププールの共通部分の一部としてプロジェクト 5 に追加できます。3 つのメンバーシッププールの共通部分が空であるため、プロジェクト 6 にユーザー/グループを追加することはできません。



シナリオ 6 - 3 つのメンバーシッププールすべてにまたがる交差は、ユーザー {U1} のみをプロジェクト 8 に追加できることを意味します。ドメインユニット 8 の の交差プールは {U1}、{U1}、{U1、U2} - 3 つの間で共通するのは {U1} のみです。



シナリオ 7 - ユーザー {U1, U2, G1} は、ルートドメインからメンバーシッププールの一部としてルートドメインのプロジェクトに追加できます。ドメインユニット 9 の下のプロジェクトにユーザーまたはグループを追加できます。これは、カスケードがルートドメインの上位で false に設定されているため、メンバーシッププールが {すべてのユーザー/グループ} で構成されているためです。



Amazon DataZone ドメイン単位内のプロジェクトに承認ポリシーを割り当てる

Amazon では DataZone、ドメインユニットを使用すると、アセットやその他のドメインエンティティを特定のビジネスユニットやチームで整理できます。詳細については、「Amazon DataZone の用語と概念」を参照してください。

Amazon DataZone ドメインユニットでは、次の承認ポリシーをプロジェクトに割り当てて、このドメインユニット内のさまざまな承認許可をこれらのエンティティに付与できます。

- 用語集作成ポリシー
- メタデータフォーム作成ポリシー
- カスタムアセットタイプ作成ポリシー

ドメイン単位内のプロジェクトに承認ポリシーを割り当てるには、次の手順を実行します。

1. Amazon DataZone データポータルに移動URLし、シングルサインオン (SSO) または を使用してサインインします。 AWS 認証情報。Amazon DataZone 管理者の場合は、https://console.aws.amazon.com/datazone で Amazon DataZone コンソールに移動し、 でサインイン

できます。 AWS アカウント ドメインが作成された場所で、データポータルを開く を選択します。

2. ドメインを表示を選択し、承認ポリシーを割り当てるドメインとドメイン単位を選択します。
3. ドメイン単位の詳細ページで、プロジェクトに割り当てる承認ポリシーを選択し、プロジェクトの追加 を選択します。
4. 「プロジェクトの追加」ポップアップウィンドウで、次のいずれかを実行します。

   - ドメイン単位 で選択したプロジェクト を選択し、選択した承認ポリシーを割り当てるプロジェクトを指定し、プロジェクトの追加 を選択します。
   - 「ドメイン単位内のすべてのプロジェクト」を選択し、「プロジェクトを追加」を選択します。

Amazon DataZone ブループリント設定内で承認ポリシーを割り当てる

Amazon で認証メカニズムを使用するもう 1 つの方法は DataZone 、Amazon DataZone ブループリント設定内のプロジェクトとドメイン単位の所有者に認証ポリシーを適用することです。

Amazon DataZone ブループリント設定は、ユーザーワークフローの公開とサブスクライブに使用されるリソースの作成と設定に必要な情報をカプセル化するエンティティです。この情報には以下が含まれます。 AWS アカウント番号とリージョン、CFNテンプレート、 VPCs やサブネットなどのアカウントレベルのパラメータ、データベース接続情報と認証情報を含めることもできます。コストを管理し、セキュリティを向上させるために、データプラットフォームのユーザーには、これらのブループリントを使用できるユーザーを制御し、環境を作成できる機能が必要です。

特定のブループリント設定内で、プロジェクトとドメイン単位の所有者に次の承認ポリシーを割り当てることができます。

- このブループリントを使用して環境プロファイルを作成する - このポリシーは Amazon DataZone プロジェクトに割り当てることができ、このブループリントを使用して環境プロファイルを作成することを承認します。
- このブループリントを使用して環境プロファイルを作成するアクセス許可を付与する - このポリシーはドメイン単位の所有者に割り当てることができ、このブループリントを使用して環境プロファイルを作成するアクセス許可をプロジェクトに付与することを承認します。

この設計図承認ポリシーを使用して環境プロファイルの作成を、Amazon DataZone データポータル経由で設計図設定からプロジェクトに割り当てる

1. Amazon DataZone データポータルに移動URLし、シングルサインオン (SSO) または を使用してサインインします。 AWS 認証情報。Amazon DataZone 管理者の場合は、https://console.aws.amazon.com/datazone で Amazon DataZone コンソールに移動し、 でサインインできます。 AWS アカウント ドメインが作成された場所で、データポータルを開く を選択します。
2. データポータルで、使用するブループリントが有効になっているドメインを選択し、ブループリント設定タブに移動します。
3. ブループリント設定タブで、作業する有効なブループリントを選択し、このブループリントの詳細ページで承認ポリシータブに移動し、このブループリント承認ポリシーを使用して環境プロファイルを作成するを選択します。
4. この設計図承認ポリシーの詳細ページを使用して環境プロファイルを作成する で、アクションを展開し、プロジェクトの追加 を選択します。
5. 「プロジェクトの追加」ポップアップウィンドウで、次のいずれかを実行できます。

   - ドメイン単位内のすべてのプロジェクト オプションを選択し、このブループリントで環境プロファイルの作成を承認するプロジェクトを含むドメイン単位を検索して指定し、プロジェクトの追加 を選択します。
   - ドメイン単位オプションで選択したプロジェクトを選択し、このポリシーを割り当てるプロジェクトを含むドメイン単位を検索して指定し、このポリシーを割り当てるプロジェクトを検索して選択し、プロジェクトの追加 を選択します。

Amazon DataZone マネジメントコンソールを使用して、設計図設定からドメイン単位の所有者に、この設計図承認ポリシーを使用して環境プロファイルを作成する許可を付与する

1. https://console.aws.amazon.com/datazone の Amazon DataZone コンソールに移動し、アカウントの認証情報を使用してサインインします。
2. Amazon DataZone コンソールで、使用するブループリントが有効になっているドメインを選択し、ブループリントタブに移動します。
3. ブループリントタブで、作業する有効なブループリントを選択し、ブループリントの詳細ページで、委任されたアクセス許可タブに移動します。
4. 委任されたアクセス許可 タブで、このブループリントポリシーを使用して環境プロファイルを作成するアクセス許可を付与する所有者にドメインユニットを検索して選択し、委任されたアクセス許可を追加 を選択します。

Amazon DataZone 組み込みブループリント

環境が作成されるブループリントは、環境が属するプロジェクトのメンバーは、Amazon DataZone カタログ内のアセットを操作するときにどのツールやサービスを使用できるかを定義します。Amazon の現在のリリースでは DataZone、以下の組み込みブループリントがあります。

- データレイクの設計図
- データウェアハウスの設計図
- Amazon SageMaker ブループリント

Amazon でデフォルトのブループリントを有効にするには、以下の手順を実行します DataZone。

- で組み込みブループリントを有効にする AWS Amazon DataZone ドメインを所有する アカウント
- で Amazon を信頼されたサービス SageMaker として追加する AWS Amazon DataZone ドメインを所有する アカウント

で組み込みブループリントを有効にする AWS Amazon DataZone ドメインを所有する アカウント

環境が作成されるブループリントは、環境が属するプロジェクトのメンバーは、Amazon DataZone カタログ内のアセットを操作するときにどのツールやサービスを使用できるかを定義します。

Amazon の現在のリリースでは DataZone、データレイクブループリント、データウェアハウスブループリント、Amazon ブループリントのいくつかのブルー SageMaker プリントが組み込まれています。

- データレイクの設計図には、一連のサービス (AWS Glue、 AWS Lake Formation、Amazon Athena) は、Amazon DataZone カタログでデータレイクアセットを公開して使用します。
- データウェアハウスの設計図には、Amazon DataZone カタログで Amazon Redshift アセットを公開および使用するための一連の サービス (Amazon Redshift) を起動および設定するための定義が含まれています。
- Amazon SageMaker ブループリントには、Amazon DataZone カタログで Amazon SageMaker アセットを公開および使用するための一連の サービス (Amazon SageMaker Studio) を起動および設定するための定義が含まれています。

詳細については、「Amazon DataZone の用語と概念」を参照してください。

Amazon DataZone ドメインの作成中に、ドメイン作成プロセスの一環として、デフォルトのデータレイクとデフォルトのデータウェアハウス組み込みブループリントを自動的に有効にするクイックセットアップを選択することもできます。クイックセットアップでは、これらの組み込みブループリントを使用して、デフォルトの環境プロファイルとデフォルトの環境も作成されます。

Amazon DataZone ドメインの作成の一環としてクイックセットアップを選択しない場合は、以下の手順に従って、 で使用可能な組み込みブループリントを有効にできます。 AWS この Amazon DataZone ドメインを格納する アカウント。これらの組み込みブループリントを使用して、このドメインで環境プロファイルと環境を作成する前に、これらの組み込みブループリントを有効にする必要があります。

Amazon DataZone マネジメントコンソールを介して Amazon DataZone ドメインで組み込みブループリントを有効にするには、管理アクセス許可を持つアカウントの IAMロールを引き受ける必要があります。 は、最小限のアクセス許可Amazon DataZone マネジメントコンソールを使用するために必要なIAMアクセス許可を設定するを取得します。

Amazon DataZone ドメインで組み込みブループリントを有効にする

1. https://console.aws.amazon.com/datazone の Amazon DataZone コンソールに移動し、アカウントの認証情報を使用してサインインします。
2. ドメインを表示を選択し、1 つ以上の組み込みブループリントを有効にするドメインを選択します。
3. ドメインの詳細ページで、ブループリントタブに移動します。
4. ブループリントリストから、 DefaultDataLakeまたは DefaultDataWarehouse、または Amazon SageMaker ブループリントを選択します。
5. 選択したブループリントの詳細ページで、このアカウント で有効化 を選択します。
6. アクセス許可とリソースページで、以下を指定します。

   - DefaultDataLake ブループリントを有効にする場合は、 Glue のアクセス管理ロール で、 のテーブルへのアクセスを取り込んで管理する DataZone 権限を Amazon に付与する新規または既存のサービスロールを指定します。 AWS Glue と AWS Lake Formation。
   - DefaultDataWarehouse ブループリントを有効にする場合は、Redshift のアクセス管理ロールで、Amazon Redshift のデータ共有、テーブル、ビューへのアクセスを取り込み、管理する DataZone 権限を Amazon に付与する新規または既存のサービスロールを指定します。

- Amazon SageMaker ブループリントを有効にする場合は、SageMaker アクセス管理ロールで、Amazon SageMaker データをカタログに発行するアクセス許可を Amazon DataZone に付与する新規または既存のサービスロールを指定します。また、カタログ内の Amazon が SageMaker 公開したアセットへのアクセスを許可または取り消すアクセス DataZone 許可も Amazon に付与します。

  > **Important**
  >
  > Amazon SageMaker ブループリントを有効にすると、Amazon は Amazon の次のIAM ロールが現在のアカウントとリージョン DataZone に存在する DataZone かどうかを確認します。これらのロールが存在しない場合、Amazon DataZone によって自動的に作成されます。
  >
  > - AmazonDataZoneGlueAccess-<region>-<domainId >
  > - AmazonDataZoneRedshiftAccess-<region>-<domainId >

- プロビジョニングロール で、 を使用して環境リソースを作成および設定する権限を Amazon DataZone に付与する新規または既存のサービスロールを指定します。 AWS CloudFormation 環境アカウントとリージョンの 。
- Amazon SageMaker ブループリントを有効にする場合は、 SageMaker-Glue データソース の Amazon S3 バケット に、 内のすべての SageMaker 環境で使用される Amazon S3 バケットを指定します。 AWS アカウント。指定するバケットプレフィックスは、次のいずれかである必要があります。
  - Amazon データゾーン*
  - datazone-sagemaker*
  - sagemaker-datazone*
  - DataZone-Sagemaker*
  - Sagemaker-DataZone*
  - DataZone-SageMaker*
  - SageMaker-DataZone*

7. ブループリントを有効にする を選択します。

選択したブループリントを有効にすると、アカウントでブループリント (複数可) を使用して環境プロファイルを作成できるプロジェクトを制御できます。これを行うには、プロジェクトの管理をブループリントの設定に割り当てます。

> **Important**
>
> デフォルトでは、環境ブループリントの管理プロジェクトは指定されません。つまり、Amazon DataZone ユーザーは環境ブループリントのプロファイルを作成できます。したがって、ガバナンスを強化するために、環境ブループリントのプロジェクト管理を常に指定することを強くお勧めします。

有効なブループリントでプロジェクトの管理を指定する

1. https://console.aws.amazon.com/datazone の Amazon DataZone コンソールに移動し、アカウントの認証情報を使用してサインインします。
2. ドメインを表示 (View Domains) を選択し、選択した設計図の管理プロジェクトを追加するドメインを選択します。
3. ブループリント タブを選択し、使用するブループリントを選択します。
4. デフォルトでは、ドメイン内のすべてのプロジェクトは、 DefaultDataLake または DefaultDataWareshouse、またはアカウント内の Amazon SageMaker ブループリントを使用して環境プロファイルを作成できます。ただし、プロジェクト管理をブループリントに割り当てることで、これを制限できます。管理プロジェクトを追加するには、「管理プロジェクトを選択」を選択し、ドロップダウンメニューから管理プロジェクトとして追加するプロジェクトを選択し、「管理プロジェクトを選択」(複数可) を選択します。

で DefaultDataWarehouse ブループリントを有効にしたら AWS アカウントでは、設計図設定にパラメータセットを追加できます。パラメータセットはキーと値のグループであり、Amazon Redshift クラスターへの接続を確立 DataZone するために Amazon が必要とするもので、データウェアハウス環境の作成に使用されます。これらのパラメータには、Amazon Redshift クラスター、データベース、および の名前が含まれます。 AWS クラスターの認証情報を保持する シークレット。

DefaultDataWarehouse 設計図へのパラメータセットの追加

1. https://console.aws.amazon.com/datazone の Amazon DataZone コンソールに移動し、アカウントの認証情報を使用してサインインします。
2. ドメインを表示を選択し、パラメータセットを追加するドメインを選択します。
3. ブループリントタブを選択し、 DefaultDataWareshouse ブループリントを選択してブループリントの詳細ページを開きます。
4. 設計図の詳細ページのパラメータセットタブで、パラメータセットの作成 を選択します。

- パラメータセットの名前を指定します。
- 必要に応じて、パラメータセットの説明を入力します。
- リージョンの選択
- Amazon Redshift クラスターまたは Amazon Redshift Serverless を選択します。
- を選択する AWS 選択した Amazon Redshift クラスターまたは Amazon Redshift Serverless ワークグループの認証情報ARNを保持する シークレット。- AWS シークレットをパラメータセット内で使用できるようにするには、 タグで`AmazonDataZoneDomain : [Domain_ID]`タグ付けする必要があります。
  - 既存の がない場合 AWS シークレット、新規作成 を選択して新しいシークレットを作成することもできます。 AWS シークレット 。これにより、シークレットの名前、ユーザー名、パスワードを指定できるダイアログボックスが開きます。新規作成を選択したら AWS シークレット 、Amazon DataZone は に新しいシークレットを作成します。 AWS Secrets Manager サービスと は、シークレットにパラメータセットを作成しようとしているドメインがタグ付けされていることを確認します。
- 上記のステップで Amazon Redshift クラスターを選択した場合は、ドロップダウンからクラスターを選択します。上記のステップで Amazon Redshift ワークグループを選択した場合は、ドロップダウンからワークグループを選択します。
- 選択した Amazon Redshift クラスターまたは Amazon Redshift Serverless ワークグループ内のデータベースの名前を入力します。
- パラメータセットの作成 を選択します。

> **Note**
>
> 設計図に追加できるパラメータセットは最大 10 DefaultDataWarehouse個までです。

で Amazon SageMaker ブループリントを有効にしたら AWS アカウントでは、設計図設定にパラメータセットを追加できます。パラメータセットはキーと値のグループであり、Amazon が Amazon への接続を確立 DataZone するために必要 SageMaker であり、sagemaker 環境の作成に使用されます。

Amazon SageMaker ブループリントへのパラメータセットの追加

1. https://console.aws.amazon.com/datazone の Amazon DataZone コンソールに移動し、アカウントの認証情報を使用してサインインします。

2. ドメインを表示を選択し、パラメータセットを追加する有効なブループリントを含むドメインを選択します。
3. ブループリントタブを選択し、Amazon SageMaker ブループリントを選択してブループリントの詳細ページを開きます。
4. 設計図の詳細ページのパラメータ設定タブで、パラメータセットの作成 を選択し、以下を指定します。

   - パラメータセットの名前を指定します。
   - 必要に応じて、パラメータセットの説明を指定します。
   - Amazon SageMaker ドメイン認証タイプを指定します。IAM または IAM Identity Center () のいずれかを選択できますSSO。
   - を指定する AWS リージョン。
   - を指定する AWS KMS データ暗号化用の キー。既存のキーを選択するか、新しいキーを作成できます。
   - 環境パラメータ で、以下を指定します。
     - VPC ID - Amazon SageMaker 環境VPCの に使用している ID。既存の を指定するか、新しい を作成できますVPC。
     - サブネット - 内の特定のリソースの IP アドレスIDs範囲の 1 つ以上の VPC。
     - ネットワークアクセス - VPCのみまたはパブリックインターネットのみを選択します。
     - セキュリティグループ - VPCおよび サブネットを設定するときに使用するセキュリティグループ。
   - データソースパラメータで、次のいずれかを選択します。
     - AWS Glue のみ
     - AWS Glue + Amazon Redshift Serverless。このオプションを選択した場合は、以下を指定します。
       - を指定する AWS 選択した Amazon Redshift クラスターの認証情報ARNを保持する シークレット。- AWS シークレットをパラメータセット内で使用できるようにするには、 タグで`AmazonDataZoneDomain : [Domain_ID]`タグ付けする必要があります。

         既存の がない場合 AWS シークレット、新規作成 を選択して新しいシークレットを作成することもできます。 AWS シークレット 。これにより、シークレットの名前、ユーザー名、パスワードを指定できるダイアログボックスが開きます。新規作成を選択したら AWS シークレット 、Amazon DataZone は に新しいシークレットを作成します。 AWS

Secrets Manager サービスと は、シークレットにパラメータセットを作成しようとしているドメインがタグ付けされていることを確認します。

- 環境の作成時に使用する Amazon Redshift ワークグループを指定します。
- 環境の作成時に使用するデータベースの名前 (選択したワークグループ内) を指定します。

- AWS Glue のみ + Amazon Redshift クラスター
  - を指定する AWS 選択した Amazon Redshift クラスターの認証情報ARNを保持する シークレット。- AWS シークレットをパラメータセット内で使用できるようにするには、 タグで`AmazonDataZoneDomain : [Domain_ID]`タグ付けする必要があります。

    既存の がない場合 AWS シークレット、新規作成 を選択して新しいシークレットを作成することもできます。 AWS シークレット 。これにより、シークレットの名前、ユーザー名、パスワードを指定できるダイアログボックスが開きます。新規作成を選択したら AWS シークレット 、Amazon DataZone は に新しいシークレットを作成します。 AWS Secrets Manager サービスと は、シークレットにパラメータセットを作成しようとしているドメインがタグ付けされていることを確認します。
  - 環境の作成時に使用する Amazon Redshift クラスターを指定します。
  - 環境の作成時に使用するデータベースの名前 (選択したクラスター内) を指定します。

5. パラメータセットの作成 を選択します。

で Amazon を信頼されたサービス SageMaker として追加する AWS Amazon DataZone ドメインを所有する アカウント

Amazon SageMaker ブループリントを有効にしている場合は、Amazon 内の信頼できるサービスの 1 つ SageMaker として も追加する必要があります DataZone。これを行うには、次の手順を実行します。

1. https://console.aws.amazon.com/datazone の Amazon DataZone コンソールに移動し、アカウントの認証情報を使用してサインインします。
2. ドメインを表示 を選択し、有効な SageMaker ブループリントを含むドメインを選択します。
3. Trusted services を選択し、Amazon SageMakerを選択し、Enable を選択します。

Amazon DataZone カスタム AWS サービスの設計図

Amazon では DataZone、カスタム AWS サービスブループリントでは、Amazon が独自の既存の を使用する DataZone ように設定することで、リソースの使用状況とコストを最適化できます。 AWS Identity and Access Management (IAM) ロールと AWS 組織で既にセットアップしている のサービス。

Amazon DataZone 環境が作成されるブループリントは、環境が属するプロジェクトのメンバーは、Amazon DataZone カタログ内のアセットを操作するときにどのツールやサービスを使用できるかを定義します。Amazon の現在のリリースでは DataZone、以下の組み込みブループリントがあります。

- データレイクの設計図
- データウェアハウスの設計図
- Amazon SageMaker ブループリント

Amazon Custom DataZone の使用 AWS サービスブループリントでは、任意の にカスタマイズされた環境とプロジェクトを作成できます。 AWS 組織で現在使用している のサービス。カスタムブループリントを使用すると、 DataZone 既存のIAMロールを使用してインフラストラクチャのセットアップ全体のガバナンスを強化し、ビジネスイニシアチブでコラボレーションするように設定することで、既存のデータパイプラインに Amazon を含めることができます。

トピック

- カスタムを有効にする AWS サービス設計図
- カスタム を使用して環境を作成する AWS サービス設計図
- カスタムでアクションを作成する AWS サービス環境
- カスタムにプロジェクトメンバーを追加する AWS サービス環境
- でデータソースを設定する AWS サービス環境
- でサブスクリプションターゲットを設定する AWS サービス環境

カスタムを有効にする AWS サービス設計図

カスタム を有効にするには、次の手順を実行します。 AWS ドメイン内の サービスブループリント。

1. にサインインする AWS マネジメントコンソール を開き、/datazone で Amazon DataZone マネジメントコンソールを開きます。 https://console.aws.amazon.com
2. ドメインを表示を選択し、カスタムを有効にするドメインを選択します。 AWS サービス設計図。
3. ブループリントタブを選択し、 AWS 使用可能なブループリントのリストから サービスブループリントを選択し、 を有効にするを選択します。

カスタム を使用して環境を作成する AWS サービス設計図

カスタム を使用して環境を作成するには、次の手順を実行します。 AWS サービス設計図。

1. にサインインする AWS マネジメントコンソール を開き、/datazone で Amazon DataZone マネジメントコンソールを開きます。 https://console.aws.amazon.com
2. ドメインを表示を選択し、カスタムのドメインを選択します。 AWS サービスブループリントが有効になっています。
3. ブループリント タブを選択し、有効になっている を選択します。 AWS サービスブループリントを選択し、環境の作成 を選択します。
4. 「環境の作成」ページで以下を指定し、「環境の作成」を選択します。

   - 名前 - 環境の名前を指定します。
   - 説明 - 環境の説明を指定します。
   - プロジェクト - 環境に新規または既存の所有プロジェクトを指定します。プロジェクトを使用すると、ユーザーのグループは Amazon のアセットを検出、公開、サブスクライブ、消費できます DataZone。この環境は、指定されたプロジェクトのメンバー全員が使用できます。すべての環境は、ユーザーが環境にアクセスできるプロジェクトによって所有されます。
   - 環境ロール - 既存の DataZone へのアクセスを Amazon に許可する既存のIAMロールを指定します。 AWS Amazon S3 や などの サービスとリソース AWS この環境の Glue。

   > **Note**
   >
   > Amazon DataZone はこのロールをプロビジョニングしません。既存の へのアクセス許可を持つ既存の IAM ロールが必要です AWS この環境で有効にする サービスとリソース。
   > このIAMロールに最低限必要なアクセス許可があることを確認します。つまり、 へのアクセスのみを提供するようにスコープダウンします。 AWS この環境で有効にするサービスとリソース。

を使用できます。 AWS Policy Generator は、要件に合ったポリシーを構築し、使用するカスタムIAMロールにアタッチします。
ルールに従ってAmazonDataZone口ールが で始まることを確認します。これは必須ではありませんが、推奨されます。IAM 管理者がAmazonDataZoneFullAccessポリシーを使用している場合は、パスロールチェックの検証があるため、この規則に従う必要があります。
カスタムロールを作成するときは、信頼ポリシーdatazone.amazonaws.comで が信頼していることを確認してください。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "Service": [
                    "datazone.amazonaws.com"
                ]
            },
            "Action": [
                "sts:AssumeRole",
                "sts:TagSession"
            ]
        }
    ]
}
```

- AWS region - を指定します AWS この環境を作成するリージョン。

カスタムでアクションを作成する AWS サービス環境

カスタムでアクションを作成するには、次の手順を実行します。 AWS サービス環境。カスタムでアクションを作成する AWS サービス環境では、Amazon DataZone データポータルへのディープリンクを、この環境で利用可能な分析ツールに追加します。

1. にサインインする AWS マネジメントコンソール を開き、/datazone で Amazon DataZone マネジメントコンソールを開きます。 https://console.aws.amazon.com

2. ドメインを表示を選択し、カスタムのドメインを選択します。 AWS サービスブループリントが有効になっています。
3. ブループリントタブを選択し、有効になっている を選択します。 AWS サービス bluepint を選択し、 AWS アクションを追加する サービス環境。
4. で AWS コンソールリンクページ、人気 からリンク (アクション) を選択します。 AWS リンクまたはカスタム AWS リンクセクションを使用して、Amazon S3 バケット、Amazon Athena ワークグループ、 AWS Glue ジョブ、またはその他のカスタム AWS Amazon DataZone データポータル経由でこの環境の コンソールリソース。
5. この環境の 概要セクションにあるデータポータルリンクを使用してデータポータルでこの環境に移動すると、分析ツールセクションに追加したディープリンクが表示されます。

カスタムにプロジェクトメンバーを追加する AWS サービス環境

プロジェクトメンバーを に追加するには、次の手順を実行します。 AWS サービス環境。

1. にサインインする AWS マネジメントコンソール を開き、/datazone で Amazon DataZone マネジメントコンソールを開きます。 https://console.aws.amazon.com
2. プロジェクト タブを選択し、 内のプロジェクトを選択します。 AWS メンバーを追加する サービス環境。
3. 追加 を選択し、メンバーの追加 ページで、IAMユーザー 、ユーザー 、SSOまたはグループ からメンバーを検索して追加します。 SSO 所有者 または寄稿者 のいずれかに割り当てられたプロジェクトロールを指定します。メンバーの検索と追加が完了したら、メンバーの追加 を選択します。

でデータソースを設定する AWS サービス環境

でデータソースを設定するには、次の手順を実行します。 AWS サービス環境。

1. にサインインする AWS マネジメントコンソール を開き、/datazone で Amazon DataZone マネジメントコンソールを開きます。 https://console.aws.amazon.com
2. ブループリント タブを選択し、カスタム を選択します。 AWS サービス設計図。
3. 作成済み環境 で、 AWS データソースを設定する サービス環境。
4. データソースタブを選択し、「追加」を選択し、以下を指定して、「追加」を選択します。

    - 名前 - データソース名。

- リソース - どちらかを選択します AWS Glue または Amazon Redshift。
  - [AWS Glue で、リソースデータベースを指定します。
  - Amazon Redshift では、クラスターまたはサーバーレス を選択し、新規または既存の を含む Redshift 認証情報 を指定します。 AWS シークレット、環境の作成時に使用するクラスターまたはサーバーレスワークグループ、環境の作成時に使用するデータベース、および指定されたデータベース内のスキーマ。
- アクセス許可 - Amazon に DataZone のテーブルへのアクセスの取り込みと管理を許可する管理アクセスロールを指定します。 AWS Lake Formation (用 AWS Glue) または で、Amazon Redshift DataZone のテーブルへのアクセスを取り込み、管理する権限を Amazon に付与します。
- データを消費するために使用します。Amazon では DataZone、プロジェクトメンバーはサブスクリプションターゲットを介してデータを消費できます。Amazon DataZone はこれを使用して、プロジェクトでサブスクライブしたデータにアクセスできます。このデータソースをサブスクリプションターゲットとして追加するかどうかを指定します。

でサブスクリプションターゲットを設定する AWS サービス環境

でサブスクリプションターゲットを設定するには、次の手順を実行します。 AWS サービス環境。

1. にサインインする AWS マネジメントコンソール を開き、/datazone で Amazon DataZone マネジメントコンソールを開きます。 https://console.aws.amazon.com
2. ブループリントタブを選択し、 AWS サービス設計図。
3. 作成済み環境 で、 AWS サブスクリプションターゲットを設定する サービス環境。
4. サブスクリプションターゲットタブを選択し、「追加」を選択し、以下を指定して、「追加」を選択します。

   - 名前 - サブスクリプションターゲット名。
   - リソース - どちらかを選択します AWS Glue または Amazon Redshift。
     - [AWS Glue で、リソースデータベースを指定します。
     - Amazon Redshift では、クラスターまたはサーバーレス を選択し、新規または既存の を含む Redshift 認証情報 を指定します。 AWS シークレット、環境の作成時に使用するクラスターまたはサーバーレスワークグループ、環境の作成時に使用するデータベース、および指定されたデータベース内のスキーマ。

- アクセス許可 - Amazon に のテーブルへのアクセスの取り込みと管理 DataZone を許可する管理アクセスロールを指定します。 AWS Lake Formation (用 AWS Glue) または で、Amazon Redshift DataZone のテーブルへのアクセスを取り込み、管理する権限を Amazon に付与します。
- データを消費するために使用します。Amazon では DataZone、メタデータの取り込みを可能にするデータソースを介してデータカタログにデータを公開できます。このサブスクリプションターゲットをデータソースとして追加するかどうかを指定します。

Amazon の関連アカウント DataZone

の関連付け AWS Amazon DataZone ドメインを持つ アカウントを使用すると、ドメインユーザーはこれらの からのデータを公開および使用できます。 AWS アカウント。アカウントの関連付けを設定するには、3 つのステップがあります。

- まず、目的の とドメインを共有します。 AWS 関連付けをリクエストして アカウント。Amazon DataZone が を使用する AWS の場合、Resource Access Manager (RAM) AWS アカウントがドメインの と異なる AWS アカウント。アカウントの関連付けは、Amazon DataZone ドメインによってのみ開始できます。
- 次に、アカウント所有者に関連付けリクエストを受け入れさせます。
- 3 つ目は、アカウント所有者が目的の環境ブループリントを有効にすることです。ブループリントを有効にすることで、アカウント所有者は、ドメイン内のユーザーに、 などのアカウント内のリソースの作成とアクセスに必要なIAMロールとリソース設定を提供します。 AWS Glue データベースと Amazon Redshift クラスター。

アカウントを Amazon に関連付けるには、次のステップを実行します DataZone。

- ステップ 1 - 他の との関連付けをリクエストする AWS アカウント
- ステップ 2 - Amazon DataZone ドメインからのアカウント関連付けリクエストを受け入れ、環境ブループリントを有効にする
- ステップ 3 - 関連付けられた で環境ブループリントを有効にする AWS アカウント

他の との関連付けをリクエストする AWS アカウント

> **Note**
>
> 関連付けリクエストを別の に送信する AWS アカウント、ドメインを他の アカウントと共有している AWS アカウント AWS Resource Access Manager (RAM) 。入力するアカウント ID の精度を必ず確認してください。

他の との関連付けをリクエストするには AWS Amazon DataZone ドメインの Amazon DataZone コンソールの アカウントでは、管理アクセス許可を持つアカウントの IAMロールを引き受ける必要があります。 Amazon DataZone マネジメントコンソールを使用するために必要なIAMアクセス許可を

設定する は、アカウントの関連付けをリクエストするために必要な最小限のアクセス許可を取得します。

次の手順を実行して、他の との関連付けをリクエストします。 AWS アカウント。

1. にサインインする AWS マネジメントコンソール を開き、/datazone で Amazon DataZone マネジメントコンソールを開きます。 https://console.aws.amazon.com
2. ドメインを表示を選択し、リストからドメイン名を選択します。名前はハイパーリンクです。
3. 関連アカウントタブまでスクロールし、関連付けのリクエスト を選択します。
4. 関連付けをリクエストするIDsアカウントの を入力します。アカウント のリストに問題がなければIDs、関連付けのリクエスト を選択します。
5. RAM ポリシーで、アカウントの関連付けのRAMポリシーを指定します。関連付けられているアカウントAWSRAMPermissionDataZonePortalReadWriteが Amazon DataZone APIs を実行してデータポータルにアクセスできるようにするか、 を選択するかを選択できます。関連付けられているアカウントが Amazon DataZone APIs のみを実行することを許可しAWSRAMPermissionDataZoneDefault、データポータルへのアクセスを提供しません。 DataZone 次に、Amazon は にリソース共有を作成します。 AWS アカウントに代わって Resource Access Manager (入力されたアカウント ID) をプリンシパルとします。
6. 他の の所有者に通知する必要があります AWS account (s) リクエストを承諾します。招待は 7 (7) 日後に期限切れになります。

カスタマーマネージドKMSキーへのアカウントアクセスを提供する

Amazon DataZone ドメインとそのメタデータは、 によって保持されるキーを使用して (デフォルトで) 暗号化されます。 AWS、または (オプションで) のカスタマーマネージドキー AWS ドメインの作成時に所有および提供する Key Management Service (KMS) 。ドメインがカスタマーマネージドキーで暗号化されている場合は、以下の手順に従って、関連付けられたアカウントにKMSキーを使用するアクセス許可を付与します。

1. にサインインする AWS マネジメントコンソール でKMSコンソールを開きますhttps://console.aws.amazon.com/kms/。
2. ユーザーが作成および管理するアカウント内のキーを表示するには、ナビゲーションペインで [Customer managed keys] (カスタマーマネージドキー) を選択します。
3. ユーザーが作成および管理するアカウント内のキーを表示するには、ナビゲーションペインで [Customer managed keys] (カスタマーマネージドキー) を選択します。
4. KMS キーのリストで、確認するキーのエイリアスまたはKMSキー ID を選択します。

5. 外部 を許可または禁止するには AWS アカウントでKMSキーを使用し、その他の のコントロールを使用する AWS ページの accounts セクション。IAM これらのアカウントのプリンシパル (適切なKMSアクセス許可を持つもの) は、データKMSキーの暗号化、復号、再暗号化、生成などの暗号化オペレーションで キーを使用できます。

Amazon DataZone ドメインからのアカウント関連付けリクエストを受け入れ、環境ブループリントを有効にする

Amazon DataZone マネジメントコンソールで Amazon DataZone ドメインとの関連付けを受け入れるには、管理アクセス許可を持つ アカウントの IAM ロールを引き受ける必要があります。 は、最小限のアクセス許可Amazon DataZone マネジメントコンソールを使用するために必要なIAMアクセス許可を設定するを取得します。

Amazon DataZone ドメインとの関連付けを受け入れるには、以下を完了します。

1. にサインインする AWS マネジメントコンソール を開き、/datazone で Amazon DataZone マネジメントコンソールを開きます。 https://console.aws.amazon.com
2. リクエストを表示を選択し、リストから招待するドメインを選択します。招待の状態は、リクエスト済み である必要があります。リクエストの確認 を選択します。
3. どちらも、両方、またはいずれかのボックスを選択して、デフォルトのデータレイクやデータウェアハウス環境の設計図を有効にするかどうかを選択します。これは後で実行できます。

   - データレイク環境の設計図により、ドメインユーザーは を作成および管理できます。 AWS データレイクから発行および消費する Glue、Amazon S3、および Amazon Athena リソース。
   - データウェアハウス環境の設計図により、ドメインユーザーは Amazon Redshift リソースを作成して管理し、データウェアハウスから発行して使用できます。
4. デフォルトの環境設計図の 1 つまたは両方を選択する場合は、次のアクセス許可とリソースを設定します。

   - アクセス管理IAMロールは、ドメインユーザーが などのテーブルへのアクセスを取り込んで管理できるようにするアクセス許可を Amazon DataZone に提供します。 AWS Glue と Amazon Redshift。Amazon に新しいIAMロール DataZone を作成して使用させるか、既存のIAMロールのリストから選択できます。
   - プロビジョニングIAMロールは、ドメインユーザーが などの環境リソースを作成および設定できるようにするアクセス許可を Amazon DataZone に提供します。 AWS Glue データベー

ス。Amazon に新しいIAMロール DataZone を作成して使用させるか、既存のIAMロールのリストから選択できます。

- Data Lake の Amazon S3 バケットは、ドメインユーザーがデータレイクデータを保存するときに Amazon が使用するバケットまたはパス DataZone です。Amazon で選択したデフォルトのバケットを使用する DataZone か、パス文字列を入力して既存の Amazon S3 パスを選択できます。独自の Amazon S3 パスを選択した場合は、IAMポリシーを更新して、そのパスを使用するアクセス許可を Amazon DataZone に付与する必要があります。

5. 設定に満足したら、「関連付けを受け入れて設定する」を選択します。

関連付けられた で環境ブループリントを有効にする AWS アカウント

Amazon DataZone マネジメントコンソールで環境ブループリントを有効にするには、管理アクセス許可を持つアカウントで IAMロールを引き受ける必要があります。最小限のアクセス許可を取得するAmazon DataZone マネジメントコンソールを使用するために必要なIAMアクセス許可を設定するには。

関連付けられているドメインでブループリントを有効にするには、以下を実行します。

1. にサインインする AWS マネジメントコンソール を開き、/datazone で Amazon DataZone マネジメントコンソールを開きます。 https://console.aws.amazon.com
2. 左側のナビゲーションパネルを開き、関連付けられたドメイン を選択します。
3. 環境ブループリントを有効にするドメインを選択します。
4. ブループリントリストから、 DefaultDataLakeまたは 、Amazon SageMakerDefaultDataWarehouse、またはカスタム のいずれかを選択します。 AWS サービス設計図。

> **Note**
>
> カスタム を有効にする場合 AWS サービス設計図では、アクセスロールの管理を指定する必要はありません。カスタム のアクセス許可と承認メカニズム AWS サービスブループリントは、このブループリントを使用して環境を作成するときに処理されます。詳細については、「カスタム を使用して環境を作成する AWS サービス設計図」を参照してください。

5. 選択したブループリントの詳細ページで、このアカウント で有効化 を選択します。

6. アクセス許可とリソースページで、以下を指定します。

- DefaultDataLake ブループリントを有効にする場合は、 Glue のアクセス管理ロール で、 のテーブルへのアクセスを取り込んで管理する DataZone 権限を Amazon に付与する新規または既存のサービスロールを指定します。 AWS Glue と AWS Lake Formation。
- DefaultDataWarehouse ブループリントを有効にする場合は、Redshift のアクセス管理ロールで、Amazon Redshift のデータ共有、テーブル、ビューへのアクセスを取り込み、管理する DataZone 権限を Amazon に付与する新規または既存のサービスロールを指定します。
- Amazon SageMaker ブループリントを有効にする場合は、SageMaker アクセス管理ロールに、Amazon SageMaker データをカタログに発行するアクセス DataZone 許可を Amazon に付与する新規または既存のサービスロールを指定します。また、カタログ内の Amazon が SageMaker 公開したアセットへのアクセスを許可または取り消すアクセス DataZone 許可も Amazon に付与します。

> **Important**
>
> Amazon SageMaker ブループリントを有効にすると、Amazon は Amazon の次のIAM ロールが現在のアカウントとリージョン DataZone に存在する DataZone かどうかを確認します。これらのロールが存在しない場合、Amazon DataZone は自動的に作成します。
>
> - AmazonDataZoneGlueAccess-<region>-<domainId >
> - AmazonDataZoneRedshiftAccess-<region>-<domainId >

- プロビジョニングロール で、 を使用して環境リソースを作成および設定する権限を Amazon DataZone に付与する新規または既存のサービスロールを指定します。 AWS CloudFormation 環境アカウントとリージョンの 。
- Amazon SageMaker ブループリントを有効にする場合は、 SageMaker-Glue データソース の Amazon S3 バケット に、 内のすべての SageMaker 環境で使用される Amazon S3 バケットを指定します。 AWS アカウント。指定するバケットプレフィックスは、次のいずれかである必要があります。
  - Amazon データゾーン*
  - datazone-sagemaker*
  - sagemaker-datazone*
  - DataZone-Sagemaker*
  - Sagemaker-DataZone*

- DataZone-SageMaker*
- SageMaker-DataZone*

7. ブループリントを有効にする を選択します。

選択したブループリント (複数可) を有効にすると、アカウントでブループリントを使用して環境プロファイルを作成できるプロジェクトを制御できます。これを行うには、プロジェクトの管理をブループリントの設定に割り当てます。

有効 DefaultDataLake または DefaultDataWarehouse 設計図でプロジェクトの管理を指定する

1. https://console.aws.amazon.com/datazone の Amazon DataZone コンソールに移動し、アカウントの認証情報を使用してサインインします。
2. 左側のナビゲーションパネルを開き、関連ドメインを選択し、管理プロジェクトを追加するドメインを選択します。
3. ブループリント タブを選択し、 DefaultDataLake または DefaultDataWareshouse ブループリントを選択します。
4. デフォルトでは、ドメイン内のすべてのプロジェクトは、アカウントの DefaultDataLake または DefaultDataWareshouse ブループリントを使用して環境プロファイルを作成できます。ただし、管理プロジェクトをブループリントに割り当てることで、これを制限できます。管理プロジェクトを追加するには、「管理プロジェクトを選択」を選択し、ドロップダウンメニューから管理プロジェクトとして追加するプロジェクトを選択し、「管理プロジェクトを選択」(複数可) を選択します。

で DefaultDataWarehouse ブループリントを有効にしたら AWS アカウントでは、設計図設定にパラメータセットを追加できます。パラメータセットはキーと値のグループであり、Amazon Redshift クラスターへの接続を確立 DataZone するために Amazon が必要とするもので、データウェアハウス環境の作成に使用されます。これらのパラメータには、Amazon Redshift クラスター、データベース、および の名前が含まれます。 AWS クラスターの認証情報を保持する シークレット。

> **Important**
>
> デフォルトでは、環境ブループリントの管理プロジェクトは指定されません。つまり、Amazon DataZone ユーザーは環境ブループリントのプロファイルを作成できます。したがって、ガバナンスを強化するために、環境ブループリントの管理プロジェクトを常に指定することを強くお勧めします。

設計図への DefaultDataWarehouseパラメータセットの追加

1. https://console.aws.amazon.com/datazone の Amazon DataZone コンソールに移動し、アカウントの認証情報を使用してサインインします。
2. 左側のナビゲーションパネルを開き、関連付けられたドメインを選択し、パラメータセットを追加するドメインを選択します。
3. ブループリントタブを選択し、 DefaultDataWareshouse ブループリントを選択してブループリントの詳細ページを開きます。
4. 設計図の詳細ページのパラメータセットタブで、パラメータセットの作成 を選択します。
   - パラメータセットの名前を指定します。
   - 必要に応じて、パラメータセットの説明を入力します。
   - リージョンの選択
   - Amazon Redshift クラスターまたは Amazon Redshift Serverless のいずれかを選択します。
   - を選択する AWS 選択した Amazon Redshift クラスターまたは Amazon Redshift Serverless ワークグループの認証情報ARNを保持する シークレット。- AWS シークレットをパラメータセット内で使用できるようにするには、 `AmazonDataZoneDomain : [Domain_ID]` タグでタグ付けする必要があります。
     - 既存の がない場合 AWS シークレット。新規作成を選択して新しいシークレットを作成することもできます。 AWS シークレット 。これにより、シークレットの名前、ユーザー名、パスワードを指定できるダイアログボックスが開きます。新規作成を選択したら AWS シークレット 、Amazon DataZone は に新しいシークレットを作成します。 AWS Secrets Manager サービスと は、パラメータセットを作成しようとしているドメインでシークレットがタグ付けされていることを確認します。
   - Amazon Redshift クラスターまたは Amazon Redshift Serverless ワークグループを選択します。
   - 選択した Amazon Redshift クラスターまたは Amazon Redshift Serverless ワークグループ内のデータベースの名前を入力します。
   - パラメータセットの作成 を選択します。

> **Note**
>
> DefaultDataWarehouse 設計図に追加できるパラメータセットは最大 10 個までです。

で Amazon SageMaker ブループリントを有効にしたら AWS アカウントでは、設計図設定にパラメータセットを追加できます。パラメータセットはキーと値のグループであり、Amazon が Amazon への接続を確立 DataZone するために必要 SageMaker であり、sagemaker 環境の作成に使用されます。

Amazon SageMaker ブループリントへのパラメータセットの追加

1. https://console.aws.amazon.com/datazone の Amazon DataZone コンソールに移動し、アカウントの認証情報を使用してサインインします。
2. ドメインを表示を選択し、パラメータセットを追加する有効なブループリントを含むドメインを選択します。
3. ブループリントタブを選択し、Amazon SageMaker ブループリントを選択してブループリントの詳細ページを開きます。
4. 設計図の詳細ページのパラメータセットタブで、パラメータセットの作成 を選択し、以下を指定します。

   - パラメータセットの名前を指定します。
   - 必要に応じて、パラメータセットの説明を指定します。
   - Amazon SageMaker ドメイン認証タイプを指定します。IAM または IAM Identity Center () のいずれかを選択できますSSO。
   - を指定する AWS リージョン。
   - を指定する AWS KMS データ暗号化用の キー。既存のキーを選択するか、新しいキーを作成できます。
   - 環境パラメータ で、以下を指定します。
     - VPC ID - Amazon SageMaker 環境VPCの に使用している ID。既存の を指定するか、新しい を作成できますVPC。
     - サブネット - 内の特定のリソースの IP アドレスIDs範囲の 1 つ以上の VPC。
     - ネットワークアクセス - VPCのみまたはパブリックインターネットのみを選択します。
     - セキュリティグループ - VPCおよび サブネットを設定するときに使用するセキュリティグループ。
   - データソースパラメータで、次のいずれかを選択します。
     - AWS Glue のみ
     - AWS Glue + Amazon Redshift Serverless。このオプションを選択した場合は、以下を指定します。

- を指定する AWS 選択した Amazon Redshift クラスターの認証情報ARNを保持する シークレット。- AWS シークレットをパラメータセット内で使用できるようにするには、`AmazonDataZoneDomain : [Domain_ID]` タグでタグ付けする必要があります。

  既存の がない場合 AWS シークレット。新規作成を選択して新しいシークレットを作成することもできます。 AWS シークレット 。これにより、シークレットの名前、ユーザー名、パスワードを指定できるダイアログボックスが開きます。新規作成を選択したら AWS シークレット 、Amazon DataZone は に新しいシークレットを作成します。 AWS Secrets Manager サービスと は、パラメータセットを作成しようとしているドメインでシークレットがタグ付けされていることを確認します。
- 環境の作成時に使用する Amazon Redshift ワークグループを指定します。
- 環境の作成時に使用するデータベースの名前 (選択したワークグループ内) を指定します。

- AWS Glue のみ + Amazon Redshift クラスター
  - を指定する AWS 選択した Amazon Redshift クラスターの認証情報ARNを保持する シークレット。- AWS シークレットをパラメータセット内で使用できるようにするには、`AmazonDataZoneDomain : [Domain_ID]` タグでタグ付けする必要があります。

    既存の がない場合 AWS シークレット。新規作成を選択して新しいシークレットを作成することもできます。 AWS シークレット 。これにより、シークレットの名前、ユーザー名、パスワードを指定できるダイアログボックスが開きます。新規作成を選択したら AWS シークレット 、Amazon DataZone は に新しいシークレットを作成します。 AWS Secrets Manager サービスと は、パラメータセットを作成しようとしているドメインでシークレットがタグ付けされていることを確認します。
  - 環境の作成時に使用する Amazon Redshift クラスターを指定します。
  - 環境の作成時に使用するデータベースの名前 (選択したクラスター内) を指定します。

5. パラメータセットの作成 を選択します。

関連付けられた に Amazon を信頼されたサービス SageMaker として追加する AWS アカウント

Amazon SageMaker ブループリントを有効にしている場合は、Amazon 内の信頼できるサービスの 1 つ SageMaker として も追加する必要があります DataZone。これを行うには、次の手順を実行します。

1. https://console.aws.amazon.com/datazone の Amazon DataZone コンソールに移動し、アカウントの認証情報を使用してサインインします。
2. ドメインを表示を選択し、有効な SageMaker ブループリントを含むドメインを選択します。
3. Trusted services を選択し、Amazon SageMakerを選択し、Enable を選択します。

Amazon DataZone ドメインからアカウント関連付けリクエストを拒否する

Amazon DataZone ドメインから Amazon DataZone マネジメントコンソールの関連付けリクエストを拒否するには、管理アクセス許可を持つアカウントの IAMロールを引き受ける必要があります。は、最小限のアクセス許可Amazon DataZone マネジメントコンソールを使用するために必要なIAMアクセス許可を設定するを取得します。

Amazon DataZone ドメインからの関連付けリクエストを拒否するには、以下を実行します。

1. にサインインする AWS マネジメントコンソール を開き、/datazone で Amazon DataZone マネジメントコンソールを開きます。 https://console.aws.amazon.com
2. リクエストを表示を選択し、リストから招待するドメインを選択します。招待の状態は、リクエスト済み である必要があります。関連付けの拒否 を選択します。関連付けの拒否 を選択して、選択を確認します。

関連付けられたアカウントを削除する

関連付けられた を削除するには AWS Amazon DataZone マネジメントコンソールの アカウントでは、管理アクセス許可を持つアカウントの IAMロールを引き受ける必要があります。最小限のアクセス許可を取得するAmazon DataZone マネジメントコンソールを使用するために必要なIAMアクセス許可を設定するには。

ドメインから関連付けられたアカウントを削除するには、次の手順を実行します。

1. にサインインする AWS マネジメントコンソール を開き、/datazone で Amazon DataZone マネジメントコンソールを開きます。 https://console.aws.amazon.com
2. ドメインを表示を選択し、リストからドメイン名を選択します。名前はハイパーリンクです。
3. 下にスクロールして、関連アカウントタブに移動します。のアカウント ID を選択する AWS 削除する アカウント。

4. [Disassociate] (関連付け解除) を選択します。フィールドに関連付け解除と入力し、関連付け解除 を選択して、選択を確認します。
5. これで、アカウントはドメインから削除され、ドメインのユーザーがデータを発行して使用できなくなります。

Amazon DataZone データカタログ

Amazon DataZone ビジネスデータカタログを使用すると、組織全体のデータをビジネスコンテキストでカタログ化できるため、組織内のすべてのユーザーがデータをすばやく見つけて理解できます。

Amazon を使用してデータを DataZone カタログ化するには、まずデータ (アセット) を Amazon のプロジェクトのインベントリとして持ち込む必要があります DataZone。プロジェクトのインベントリを作成すると、そのプロジェクトのメンバーのみがアセットを検出できるようになります。プロジェクトインベントリアセットは、明示的に公開されていない限り、検索/閲覧のすべてのドメインユーザーが利用できるわけではありません。

プロジェクトインベントリを作成した後、データ所有者は、ビジネス名 (アセットとスキーマ) 、説明 (アセットとスキーマ) 、読み上げ、用語集用語 (アセットとスキーマ) 、メタデータフォームを追加または更新することで、必要なビジネスメタデータを使用してインベントリアセットをキュレートできます。

Amazon を使用してデータを DataZone カタログ化する次のステップは、プロジェクトのインベントリアセットをドメインユーザーが検出できるようにすることです。これを行うには、インベントリアセットを Amazon DataZone カタログに発行します。インベントリアセットの最新バージョンのみをカタログに公開でき、最新の公開バージョンのみが検出カタログでアクティブになります。インベントリアセットが Amazon DataZone カタログに公開された後に更新された場合は、最新バージョンが検出カタログに含まれるように、インベントリアセットを再度明示的に公開する必要があります。

詳細については、「Amazon DataZone の用語と概念」を参照してください。

トピック

- ビジネス用語集を作成する
- ビジネス用語集を編集する
- ビジネス用語集を削除する
- 用語集に用語を作成する
- 用語集の用語を編集する
- 用語集の用語を削除する
- メタデータフォームを作成する
- メタデータフォームを編集する
- メタデータフォームを削除する
- メタデータ形式でフィールドを作成する

- メタデータフォームのフィールドを編集する
- メタデータフォームのフィールドを削除する

ビジネス用語集を作成する

Amazon では DataZone、ビジネス用語集は、アセット (データ) に関連付ける可能性のあるビジネス用語 (単語) のコレクションです。データを分析するときに組織全体で同じ定義が使用されるように、ビジネス用語とその定義のリストを適切な語彙に提供します。ビジネス用語集はカタログドメインで作成され、アセットや列に適用して、そのアセットや列の主要な特性を理解するのに役立ちます。1 つ以上の用語集用語を適用できます。ビジネス用語集は、ビジネス用語集の任意の用語を他の用語のサブリストに関連付けることができる用語のフラットリストです。詳細については、「Amazon DataZone の用語と概念」を参照してください。Amazon DataZone ドメインで用語集を作成、編集、または削除するには、そのドメインに対する適切なアクセス許可を持つ所有プロジェクトのメンバーである必要があります。

用語集を作成するには、次のステップを実行します。

1. データポータルを使用して Amazon DataZone データポータルに移動URLし、 SSOまたは を使用してログインします。 AWS 認証情報。Amazon DataZone 管理者の場合は、 の https://console.aws.amazon.com/datazone にある Amazon DataZone コンソールURLにアクセスしてデータポータルを取得できます。 AWS Amazon DataZone ドメインが作成された アカウント。
2. 検索 の横にある上部ナビゲーションバーのカタログメニューに移動します。
3. Amazon DataZone Data Portal で、用語集 を選択し、用語集の作成 を選択します。
4. 用語集の名前、説明、所有者を指定し、用語集の作成 を選択します。
5. 有効トグルを選択して、新しい用語集を有効にします。
6. 用語集の詳細ページで readme の作成 を選択して、この用語集に関する追加情報を追加できます。

ビジネス用語集を無効または有効にするには、次のステップを実行します。

1. データポータルを使用して Amazon DataZone データポータルに移動URLし、 SSOまたは を使用してログインします。 AWS 認証情報。Amazon DataZone 管理者の場合は、 の https://console.aws.amazon.com/datazone にある Amazon DataZone コンソールURLにアクセスしてデータポータルを取得できます。 AWS Amazon DataZone ドメインが作成された アカウント。
2. 検索 の横にある上部ナビゲーションバーのカタログメニューに移動します。

3. Amazon DataZone Data Portal で用語集 を選択し、無効化/有効化するビジネス用語集を見つけます。
4. 用語集の詳細ページで、有効化/無効化トグルを見つけ、それを使用して選択した用語集を有効または無効にします。

> **Note**
>
> 用語集を無効にすると、用語集に含まれるすべての用語も無効になります。

ビジネス用語集を編集する

Amazon では DataZone、ビジネス用語集は、アセット (データ) に関連付ける可能性のあるビジネス用語 (単語) のコレクションです。データを分析するときに組織全体で同じ定義が使用されるように、ビジネス用語とその定義のリストを適切な語彙に提供します。ビジネス用語集はカタログドメインで作成され、アセットや列に適用して、そのアセットや列の主要な特性を理解するのに役立ちます。1 つ以上の用語集用語を適用できます。ビジネス用語集は、ビジネス用語集の任意の用語を他の用語のサブリストに関連付けることができる用語のフラットリストです。詳細については、「Amazon DataZone の用語と概念」を参照してください。Amazon DataZone ドメインで用語集を編集するには、そのドメインに対する適切なアクセス許可を持つ所有プロジェクトのメンバーである必要があります。

ビジネス用語集を編集するには、次のステップを実行します。

1. データポータルを使用して Amazon DataZone データポータルに移動URLし、 SSOまたは を使用してログインします。 AWS 認証情報。Amazon DataZone 管理者の場合は、 の https://console.aws.amazon.com/datazone にある Amazon DataZone コンソールURLにアクセスしてデータポータルを取得できます。 AWS Amazon DataZone ドメインが作成された アカウント。
2. 検索 の横にある上部ナビゲーションバーのカタログメニューに移動します。
3. Amazon DataZone Data Portal で用語集 を選択し、編集するビジネス用語集を見つけます。
4. 用語集の詳細ページで、アクション を展開し、編集 を選択して用語集を編集します。
5. 名前、説明を更新し、保存 を選択します。

ビジネス用語集を削除する

Amazon では DataZone、ビジネス用語集は、アセット (データ) に関連付ける可能性のあるビジネス用語 (単語) のコレクションです。データを分析するときに組織全体で同じ定義が使用されるように、ビジネス用語とその定義のリストを適切な語彙に提供します。ビジネス用語集はカタログドメインで作成され、アセットや列に適用して、そのアセットや列の主要な特性を理解するのに役立ちます。1 つ以上の用語集用語を適用できます。ビジネス用語集は、ビジネス用語集の任意の用語を他の用語のサブリストに関連付けることができる用語のフラットリストです。詳細については、「Amazon DataZone の用語と概念」を参照してください。Amazon DataZone ドメイン内の用語集を削除するには、そのドメインに対する適切なアクセス許可を持つ所有プロジェクトのメンバーである必要があります。

ビジネス用語集を削除するには、次のステップを実行します。

1. データポータルを使用して Amazon DataZone データポータルに移動URLし、 SSOまたは を使用してログインします。 AWS 認証情報。Amazon DataZone 管理者の場合は、 の https://console.aws.amazon.com/datazone にある Amazon DataZone コンソールURLにアクセスしてデータポータルを取得できます。 AWS Amazon DataZone ドメインが作成された アカウント。
2. 検索 の横にある上部ナビゲーションバーのカタログメニューに移動します。
3. Amazon DataZone Data Portal で用語集 を選択し、削除するビジネス用語集を見つけます。
4. 用語集の詳細ページで、アクションを展開し、削除を選択して用語集を削除します。

   > **Note**
   >
   > 用語集を削除する前に、用語集の既存の用語をすべて削除する必要があります。

5. 削除 を選択して、用語集の削除を確認します。

用語集に用語を作成する

Amazon では DataZone、ビジネス用語集は、アセット (データ) に関連付ける可能性のあるビジネス用語のコレクションです。詳細については、「Amazon DataZone の用語と概念」を参照してください。Amazon DataZone ドメインの用語集で用語を作成、編集、または削除するには、そのドメインに対する適切なアクセス許可を持つ所有プロジェクトのメンバーである必要があります。

Amazon では DataZone、ビジネス用語集に詳細な説明を含めることができます。特定の用語のコンテキストを設定するには、用語間の関係を指定できます。用語のリレーションシップを定義すると、

関連する用語の定義に自動的に追加されます。Amazon で使用できる用語集の用語の関係 DataZone には、次のものがあります。

- タイプ - 現在の用語が識別される用語のタイプであることを示します。識別された用語が現在の用語の親であることを示します。
- タイプあり - 現在の用語が、指定された特定の用語の一般的な用語であることを示します。この関係は、一般的な用語の子用語を表すことができます。

新しい用語を作成するには、次のステップを実行します。

1. データポータルを使用して Amazon DataZone データポータルに移動URLし、 SSOまたは を使用してログインします。 AWS 認証情報。Amazon DataZone 管理者の場合は、 の https://console.aws.amazon.com/datazone にある Amazon DataZone コンソールURLにアクセスしてデータポータルを取得できます。 AWS Amazon DataZone ドメインが作成された アカウント。
2. 検索 の横にある上部のナビゲーションバーのカタログメニューに移動します。
3. Amazon DataZone Data Portal で用語集 を選択し、新しい用語を作成する用語集を選択します。
4. 用語の名前、説明、所有者を指定し、用語の作成 を選択します。
5. 有効トグルを選択して、新しい用語を有効にします。
6. Readme を追加するには、用語の詳細ページに移動し、readme の作成を選択して、この用語集に関する追加情報を追加します。
7. 関係を追加するには、用語の詳細ページに移動し、用語関係セクションを選択し、用語集用語の追加を選択します。ダイアログで、関係と関連付ける用語を選択し、閉じる を選択して、適切な関係タイプに用語を追加します。この関係は、関連付けたすべての用語にも追加されます。

用語集の用語を編集する

Amazon では DataZone、ビジネス用語集は、アセット (データ) に関連付ける可能性のあるビジネス用語のコレクションです。詳細については、「Amazon DataZone の用語と概念」を参照してください。Amazon DataZone ドメインの用語集で用語を作成、編集、または削除するには、そのドメインに対する適切なアクセス許可を持つ所有プロジェクトのメンバーである必要があります。

Amazon では DataZone、ビジネス用語集に詳細な説明を含めることができます。特定の用語のコンテキストを設定するには、用語間の関係を指定できます。用語のリレーションシップを定義すると、関連する用語の定義に自動的に追加されます。Amazon で使用できる用語集の用語の関係 DataZone には、次のものがあります。

- タイプ - 現在の用語が識別された用語のタイプであることを示します。識別された用語が現在の用語の親であることを示します。
- タイプあり - 現在の用語が、指定された特定の用語の一般的な用語であることを示します。この関係は、一般的な用語の子用語を表すことができます。

用語集の用語を編集するには、次のステップを実行します。

1. データポータルを使用して Amazon DataZone データポータルに移動URLし、 SSOまたは を使用してログインします。 AWS 認証情報。Amazon DataZone 管理者の場合は、 の https://console.aws.amazon.com/datazone にある Amazon DataZone コンソールURLにアクセスしてデータポータルを取得できます。 AWS Amazon DataZone ドメインが作成された アカウント。
2. 検索 の横にある上部ナビゲーションバーのカタログメニューに移動します。
3. Amazon DataZone Data Portal で、用語集 を選択し、編集する用語を含む用語集を見つけ、その用語を選択します。
4. 用語の詳細ページで、アクション を展開し、編集 を選択して用語を編集します。
5. 名前、説明 を更新し、保存 を選択します。

用語集の用語を削除する

Amazon では DataZone、ビジネス用語集は、アセット (データ) に関連付ける可能性のあるビジネス用語のコレクションです。詳細については、「Amazon DataZone の用語と概念」を参照してください。Amazon DataZone ドメインの用語集で用語を作成、編集、または削除するには、そのドメインに対する適切なアクセス許可を持つ所有プロジェクトのメンバーである必要があります。

Amazon では DataZone、ビジネス用語集に詳細な説明を含めることができます。特定の用語のコンテキストを設定するには、用語間の関係を指定します。用語のリレーションシップを定義すると、関連する用語の定義に自動的に追加されます。Amazon で使用できる用語集の用語の関係 DataZone には、次のものがあります。

- タイプ - 現在の用語が識別された用語のタイプであることを示します。識別された用語が現在の用語の親であることを示します。
- タイプあり - 現在の用語が、指定された特定の用語の一般的な用語であることを示します。この関係は、一般的な用語の子用語を表すことができます。

用語集の用語を削除するには、次のステップを実行します。

1. データポータルを使用して Amazon DataZone データポータルに移動URLし、 SSOまたは を使用してログインします。 AWS 認証情報。Amazon DataZone 管理者の場合は、 の https://console.aws.amazon.com/datazone にある Amazon DataZone コンソールURLにアクセスしてデータポータルを取得できます。 AWS Amazon DataZone ドメインが作成された アカウント。
2. 検索 の横にある上部のナビゲーションバーのカタログメニューに移動します。
3. Amazon DataZone Data Portal で、用語集 を選択し、削除する用語を含む用語集を見つけ、その用語を選択します。
4. 用語集の詳細ページで、アクションを展開し、削除を選択して用語を削除します。
5. 削除 を選択して、用語の削除を確認します。

メタデータフォームを作成する

Amazon では DataZone、メタデータフォームは、カタログ内のアセットメタデータへのビジネスコンテキストを追加するためのシンプルな形式です。これは、データ所有者がデータを検索して見つけるときにデータユーザーに役立つ情報でアセットを充実させる拡張可能なメカニズムとして機能します。メタデータフォームは、Amazon DataZone カタログに公開されるすべてのアセットに一貫性を持たせるメカニズムとしても機能します。

メタデータフォーム定義は 1 つ以上のフィールド定義で構成され、ブール値、日付、10 進数、整数、文字列、ビジネス用語集フィールド値データ型がサポートされています。詳細については、「Amazon DataZone の用語と概念」を参照してください。Amazon DataZone ドメインでメタデータフォームを作成、編集、または削除するには、適切な認証情報を持つ所有プロジェクトのメンバーである必要があります。

メタデータフォームを作成するには、次のステップを実行します。

1. データポータルを使用して Amazon DataZone データポータルに移動URLし、 SSOまたは を使用してログインします。 AWS 認証情報。Amazon DataZone 管理者の場合は、 の https://console.aws.amazon.com/datazone にある Amazon DataZone コンソールURLにアクセスしてデータポータルを取得できます。 AWS Amazon DataZone ドメインが作成された アカウント。
2. 検索 の横にある上部ナビゲーションバーのカタログメニューに移動します。
3. Amazon DataZone Data Portal で、メタデータフォーム を選択し、フォームの作成 を選択します。
4. メタデータフォーム名、説明、所有者を指定し、フォームの作成 を選択します。

メタデータフォームを編集する

Amazon では DataZone、メタデータフォームは、カタログ内のアセットメタデータへのビジネスコンテキストを追加するためのシンプルな形式です。これは、データ所有者がデータを検索して見つけるときにデータユーザーに役立つ情報でアセットを充実させる拡張可能なメカニズムとして機能します。メタデータフォームは、Amazon DataZone カタログに公開されるすべてのアセットに一貫性を持たせるメカニズムとしても機能します。

メタデータフォーム定義は 1 つ以上のフィールド定義で構成され、ブール値、日付、10 進数、整数、文字列、ビジネス用語集フィールド値データ型がサポートされています。詳細については、「Amazon DataZone の用語と概念」を参照してください。Amazon DataZone ドメインでメタデータフォームを作成、編集、または削除するには、適切な認証情報を持つ所有プロジェクトのメンバーである必要があります。

メタデータフォームを編集するには、次のステップを実行します。

1. データポータルを使用して Amazon DataZone データポータルに移動URLし、 SSOまたは を使用してログインします。 AWS 認証情報。Amazon DataZone 管理者の場合は、 の https://console.aws.amazon.com/datazone にある Amazon DataZone コンソールURLにアクセスしてデータポータルを取得できます。 AWS Amazon DataZone ドメインが作成された アカウント。
2. 検索 の横にある上部ナビゲーションバーのカタログメニューに移動します。
3. Amazon DataZone Data Portal で、メタデータフォーム を選択し、編集するメタデータフォームを見つけます。
4. メタデータフォームの詳細ページで、アクション を展開し、編集 を選択します。
5. 名前、説明、所有者フィールドの更新を実行し、フォームの更新 を選択します。

メタデータフォームを削除する

Amazon では DataZone、メタデータフォームは、カタログ内のアセットメタデータへのビジネスコンテキストを追加するためのシンプルな形式です。これは、データ所有者がデータを検索して見つけるときにデータユーザーに役立つ情報でアセットを充実させる拡張可能なメカニズムとして機能します。メタデータフォームは、Amazon DataZone カタログに公開されるすべてのアセットに一貫性を持たせるメカニズムとしても機能します。

メタデータフォーム定義は 1 つ以上のフィールド定義で構成され、ブール値、日付、10 進数、整数、文字列、ビジネス用語集フィールド値データ型がサポートされています。詳細については、「Amazon DataZone の用語と概念」を参照してください。Amazon DataZone ドメインでメタデー

タフォームを作成、編集、または削除するには、適切な認証情報を持つ所有プロジェクトのメンバーである必要があります。

メタデータフォームを削除するには、次のステップを実行します。

> **Note**
>
> メタデータフォームを削除する前に、メタデータフォームが適用されるすべてのアセットタイプまたはアセットから削除する必要があります。

1. データポータルを使用して Amazon DataZone データポータルに移動URLし、 SSOまたは を使用してログインします。 AWS 認証情報。Amazon DataZone 管理者の場合は、 の https://console.aws.amazon.com/datazone にある Amazon DataZone コンソールURLにアクセスしてデータポータルを取得できます。 AWS Amazon DataZone ドメインが作成された アカウント。
2. 検索 の横にある上部のナビゲーションバーのカタログメニューに移動します。
3. Amazon DataZone Data Portal で、メタデータフォーム を選択し、削除するメタデータフォームを見つけます。
4. 削除するメタデータフォームが有効になっている場合は、有効トグルを選択してメタデータフォームを無効にします。
5. メタデータフォームの詳細ページで、アクション を展開し、削除 を選択します。
6. 削除 を選択して削除を確定します。

メタデータ形式でフィールドを作成する

Amazon では DataZone、メタデータフォームは、カタログ内のアセットメタデータへのビジネスコンテキストを追加するためのシンプルな形式です。これは、データ所有者がデータを検索して見つけるときにデータユーザーに役立つ情報でアセットを充実させる拡張可能なメカニズムとして機能します。メタデータフォームは、Amazon DataZone カタログに公開されるすべてのアセットに一貫性を持たせるメカニズムとしても機能します。

メタデータフォーム定義は 1 つ以上のフィールド定義で構成され、ブール値、日付、10 進数、整数、文字列、ビジネス用語集フィールド値データ型がサポートされています。詳細については、「Amazon DataZone の用語と概念」を参照してください。Amazon DataZone ドメインのメタデータフォームのフィールドを作成、編集、または削除するには、適切な認証情報を持つ所有プロジェクトのメンバーである必要があります。

メタデータフォームでフィールドを作成するには、次のステップを実行します。

1. データポータルを使用して Amazon DataZone データポータルに移動URLし、 SSOまたは を使用してログインします。 AWS 認証情報。Amazon DataZone 管理者の場合は、 の https://console.aws.amazon.com/datazone にある Amazon DataZone コンソールURLにアクセスしてデータポータルを取得できます。 AWS Amazon DataZone ドメインが作成された アカウント。
2. 検索 の横にある上部ナビゲーションバーのカタログメニューに移動します。
3. Amazon DataZone Data Portal で、メタデータフォームを選択し、フィールドを作成するメタデータフォームを選択します (複数可)。
4. フォームの詳細ページで、フィールドの作成 を選択します。
5. フィールド名、説明、タイプ、およびこれが必須フィールドかどうかを指定し、フィールドの作成 を選択します。

メタデータフォームのフィールドを編集する

Amazon では DataZone、メタデータフォームは、カタログ内のアセットメタデータへのビジネスコンテキストを追加するためのシンプルな形式です。これは、データ所有者がデータを検索して見つけるときにデータユーザーに役立つ情報でアセットを充実させる拡張可能なメカニズムとして機能します。メタデータフォームは、Amazon DataZone カタログに公開されるすべてのアセットに一貫性を持たせるメカニズムとしても機能します。

メタデータフォーム定義は 1 つ以上のフィールド定義で構成され、ブール値、日付、10 進数、整数、文字列、ビジネス用語集フィールド値データ型がサポートされています。詳細については、「Amazon DataZone の用語と概念」を参照してください。Amazon DataZone ドメインのメタデータフォームのフィールドを作成、編集、または削除するには、適切な認証情報を持つ所有プロジェクトのメンバーである必要があります。

メタデータフォームのフィールドを編集するには、次のステップを実行します。

1. データポータルを使用して Amazon DataZone データポータルに移動URLし、 SSOまたは を使用してログインします。 AWS 認証情報。Amazon DataZone 管理者の場合は、 の https://console.aws.amazon.com/datazone にある Amazon DataZone コンソールURLにアクセスしてデータポータルを取得できます。 AWS Amazon DataZone ドメインが作成された アカウント。
2. 検索 の横にある上部ナビゲーションバーのカタログメニューに移動します。
3. Amazon DataZone Data Portal で、メタデータフォームを選択し、フィールドを編集するメタデータフォームを選択します (複数可)。

4. フォームの詳細ページで、編集するフィールドを選択し、アクション を展開し、編集 を選択します。
5. フィールド名、説明、タイプ、およびこれが必須フィールドかどうかを更新し、フィールドの更新 を選択します。

メタデータフォームのフィールドを削除する

Amazon では DataZone、メタデータフォームは、カタログ内のアセットメタデータへのビジネスコンテキストを追加するためのシンプルな形式です。これは、データ所有者がデータを検索して見つけるときにデータユーザーに役立つ情報でアセットを充実させる拡張可能なメカニズムとして機能します。メタデータフォームは、Amazon DataZone カタログに公開されるすべてのアセットに一貫性を持たせるメカニズムとしても機能します。

メタデータフォーム定義は 1 つ以上のフィールド定義で構成され、ブール値、日付、10 進数、整数、文字列、ビジネス用語集フィールド値データ型がサポートされています。詳細については、「Amazon DataZone の用語と概念」を参照してください。Amazon DataZone ドメインのメタデータフォームのフィールドを作成、編集、または削除するには、適切な認証情報を持つ所有プロジェクトのメンバーである必要があります。

メタデータフォームのフィールドを削除するには、次のステップを実行します。

1. データポータルを使用して Amazon DataZone データポータルに移動URLし、 SSOまたは を使用してログインします。 AWS 認証情報。Amazon DataZone 管理者の場合は、 の https://console.aws.amazon.com/datazone にある Amazon DataZone コンソールURLにアクセスしてデータポータルを取得できます。 AWS Amazon DataZone ドメインが作成された アカウント。
2. 検索 の横にある上部ナビゲーションバーのカタログメニューに移動します。
3. Amazon DataZone Data Portal で、メタデータフォームを選択し、フィールドを削除するメタデータフォームを選択します (複数可) 。
4. フォームの詳細ページで、削除するフィールドを選択し、アクション を展開して、削除 を選択します。
5. 削除 を選択して削除を確認します。

Amazon DataZone プロジェクトと環境

Amazon では DataZone、プロジェクトにより、Amazon DataZone カタログ内のデータアセットの公開、検出、サブスクライブ、消費など、さまざまなビジネスユースケースでユーザーのグループがコラボレーションできるようになります。各 Amazon DataZone プロジェクトには一連のアクセスコントロールが適用されているため、承認された個人、グループ、ロールのみがこのプロジェクトがサブスクライブするプロジェクトとデータアセットにアクセスし、プロジェクトのアクセス許可で定義されたツールのみを使用できます。プロジェクトは、基盤となる リソースへのアクセス許可を受け取るアイデンティティプリンシパルとして機能し、個々のユーザーの認証情報に依存することなく、Amazon が組織のインフラストラクチャ内で DataZone 運用できるようにします。

Amazon では DataZone、環境は設定されたリソース (Amazon S3 バケット、 AWS Glue データベース、または Amazon Athena ワークグループ) 。これらのリソースを操作できる特定のIAMプリンシパルのセット (寄稿者アクセス許可が割り当てられている) を使用します。各環境には、リソースへのアクセスと、サブスクリプションとフルフィルメントを通じてデータへのアクセスを許可されたユーザープリンシパルもいる場合があります。環境は、実用的なリンクを に保存するように設計されています。 AWS サービス、外部 IDEsおよびコンソール。プロジェクトのメンバーは、 環境内で設定されたディープリンクを介して、Amazon Athena コンソールなどのサービスにアクセスできます。SSO ユーザーとプロジェクトのIAMユーザーは、特定の環境を使用/アクセスするようにさらに絞り込むことができます。

Amazon では DataZone、環境プロファイルと呼ばれるテンプレートを使用して環境を作成します。環境プロファイルは、組み込みの とカスタム を使用して作成されます。 AWS サービスの設計図。環境プロファイルを使用すると、ドメイン管理者は設計図を事前設定されたパラメータでラップでき、データワーカーは既存の環境プロファイルを選択し、新しい環境の名前を指定することで、任意の数の新しい環境をすばやく作成できます。これにより、データワーカーは、ドメイン管理者によって適用されるデータガバナンスポリシーを確実に満たすと同時に、プロジェクトと環境を効率的に管理できます。

詳細については、「Amazon DataZone の用語と概念」を参照してください

トピック

- 環境プロファイルを作成する
- 環境プロファイルを編集する
- 環境プロファイルを削除する
- 新しい環境を作成する

- 環境を編集する
- 環境を削除する
- の新規プロジェクトの作成
- プロジェクトの編集
- プロジェクトの削除
- プロジェクトを離れる
- プロジェクトにメンバーを追加する
- プロジェクトからメンバーを削除する

環境プロファイルを作成する

Amazon では DataZone、環境プロファイルは環境の作成に使用できるテンプレートです。環境プロファイルの目的は、 などの配置情報を埋め込むことで環境の作成を簡素化することです。 AWS プロファイル内の アカウントとリージョン。詳細については、「Amazon DataZone の用語と概念」を参照してください。Amazon DataZone ドメインに環境プロファイルを作成するには、Amazon DataZone プロジェクトに属している必要があります。すべての環境プロファイルはプロジェクトによって所有され、任意のプロジェクトのすべての認可されたユーザーが新しい環境を作成するために使用できます。

環境プロファイルを作成するには

1. データポータルを使用して Amazon DataZone データポータルに移動URLし、 SSOまたは を使用してログインします。 AWS 認証情報。Amazon DataZone 管理者の場合は、 の https://console.aws.amazon.com/datazone にある Amazon DataZone コンソールURLにアクセスしてデータポータルを取得できます。 AWS Amazon DataZone ドメインが作成された アカウント。
2. データポータル内で、プロジェクトを参照を選択し、環境プロファイルを作成するプロジェクトを選択します。
3. プロジェクト内の環境タブに移動し、環境プロファイルの作成 を選択します。
4. 次のフィールドを設定します。
    - 名前 – 環境プロファイルの名前。
    - 説明 – (オプション) 環境プロファイルの説明。
    - 所有者プロジェクト - このフィールドでは、プロファイルが作成されているプロジェクトがデフォルトで選択されます。

- ブループリント — このプロファイルが作成されるブループリント。デフォルトの Amazon DataZone ブループリント (データレイクまたはデータウェアハウス) のいずれかを選択できます。

  データウェアハウスの設計図を指定した場合は、次の操作を行います。

  - パラメータセットを指定します。既存のパラメータセットを選択するには、「パラメータセットの選択」を選択します。独自のパラメータを入力する場合は、「自分の を入力」を選択します。
  - 既存のパラメータを選択する場合は、次の操作を行います。
    - を選択する AWS ドロップダウンの アカウント。
    - ドロップダウンからパラメータセットを選択します。
  - 独自のパラメータを入力する場合は、次の手順を実行します。
    - を指定する AWS を選択して パラメータ AWS ドロップダウンのアカウントとリージョン。
    - Redshift データウェアハウスパラメータを指定します。
      - Amazon Redshift クラスターまたは Amazon Redshift Serverless のいずれかを選択する
      - を入力します。 AWS 選択した Amazon Redshift クラスターまたは Amazon Redshift Serverless ワークグループの認証情報ARNを保持するシークレット。- AWS シークレットは、環境プロファイルを作成するドメイン ID とプロジェクト ID でタグ付けする必要があります。
        - `AmazonDataZoneDomain: [Domain_ID]`
        - `AmazonDataZoneProject: [Project_ID]`
      - Amazon Redshift クラスターまたは Amazon Redshift Serverless ワークグループの名前を入力します。
      - 選択した Amazon Redshift クラスターまたは Amazon Redshift Serverless ワークグループ内のデータベースの名前を入力します。
  - 「承認済みプロジェクト」セクションで、環境プロファイルを使用して環境を作成できるプロジェクトを指定します。デフォルトでは、ドメイン内のすべてのプロジェクトがアカウントの環境プロファイルを使用して環境を作成できます。このデフォルト設定を維持するには、すべてのプロジェクト を選択します。ただし、承認されたプロジェクトを環境に割り当てて、これを制限できます。そのためには、承認済みプロジェクトのみを選択し、このプロジェクトプロファイルを使用して環境を作成できるプロジェクトを指定します。

- 公開セクションで、次のいずれかのオプションを選択します。
  - 任意のスキーマから発行: このオプションを選択すると、この環境プロファイルを使用して作成された環境を使用して、上記の Redshift パラメータで選択されたデータベース内の任意のスキーマから発行できます。この環境プロファイルを使用して作成された環境のユーザーは、独自の Amazon Redshift パラメータを指定して、 内の任意のスキーマから発行することもできます。 AWS 環境プロファイルで選択された アカウントとリージョン。
  - デフォルトの環境スキーマからのみ発行する: このオプションを選択すると、これを使用して作成された環境を使用して、Amazon がその環境 DataZone 用に作成したデフォルトのスキーマからのみ発行できます。この環境プロファイルを使用して作成された環境のユーザーは、独自の Amazon Redshift パラメータを指定できません。
  - の公開を許可しない: このオプションを選択した場合、この環境プロファイルを使用して作成された環境は、データのサブスクライブと使用にのみ使用できます。環境を使用してデータを公開することはできません。

Data Lake ブループリントを指定した場合は、次の操作を行います。

- AWS アカウントパラメータセクションで、 を指定します。 AWS アカウント番号と AWS 潜在的な環境が作成される アカウントリージョン。
- 「承認済みプロジェクト」セクションで、環境を作成するための組み込み Data Lake 環境プロファイルで環境プロファイルを使用できるプロジェクトを指定します。デフォルトでは、ドメイン内のすべてのプロジェクトは、アカウントのデータレイクブループリントを使用して環境プロファイルを作成できます。このデフォルト設定を維持するには、すべてのプロジェクト を選択します。ただし、設計図にプロジェクトを割り当てることで、これを制限できます。そのためには、承認済みプロジェクトのみを選択し、このプロジェクトプロファイルを使用して環境を作成できるプロジェクトを指定します。
- データベースセクションで、任意のデータベースを選択して、 内の任意のデータベースからの発行を有効にします。 AWS 環境が作成される アカウントとリージョン、または環境で作成されたデフォルトの公開データベースからの公開を有効にするデフォルトデータベースのみを選択します。

5. 環境プロファイルの作成 を選択します。

環境プロファイルを編集する

Amazon では DataZone、環境プロファイルは環境の作成に使用できるテンプレートです。詳細については、「Amazon DataZone の用語と概念」を参照してください。Amazon DataZone ドメイン内

の既存の環境プロファイルを編集するには、Amazon DataZone プロジェクトに属している必要があります。

環境プロファイルを編集するには

1. Amazon DataZone データポータルに移動URLし、シングルサインオン (SSO) または を使用してサインインします。 AWS 認証情報。Amazon DataZone 管理者の場合は、https://console.aws.amazon.com/datazone で Amazon DataZone コンソールに移動し、 でサインインできます。 AWS アカウント ドメインが作成された場所で、データポータルを開く を選択します。
2. データポータル内でプロジェクトを参照を選択し、環境プロファイルを編集するプロジェクトを選択します。
3. プロジェクト内の環境タブに移動し、環境プロファイル を選択し、編集する環境プロファイルを選択します。

   データウェアハウス環境プロファイルを編集する場合は、既存の環境プロファイルの名前と説明のみを編集できます。

   Data Lake 環境プロファイルを編集する場合は、プロファイルの名前と説明を編集できます。また、このプロファイルを使用して環境を作成することが許可されているプロジェクトを編集したり、データベースを編集したりできます。これらの設定を編集するには、次の手順を実行します。

   - 「承認済みプロジェクト」セクションで、環境を作成するための組み込み Data Lake 環境プロファイルで環境プロファイルを使用できるプロジェクトを指定します。デフォルトでは、ドメイン内のすべてのプロジェクトは、アカウントのデータレイクブループリントを使用して環境プロファイルを作成できます。このデフォルト設定を維持するには、すべてのプロジェクトを選択します。ただし、設計図にプロジェクトを割り当てることで、これを制限できます。そのためには、承認済みプロジェクトのみを選択し、このプロジェクトプロファイルを使用して環境を作成できるプロジェクトを指定します。
   - データベースセクションで、任意のデータベースを選択して、 内の任意のデータベースからの発行を有効にします。 AWS 環境が作成される アカウントとリージョン、または環境で作成されたデフォルトの公開データベースからの公開を有効にするデフォルトデータベースのみを選択します。

   編集が完了したら、環境プロファイルの編集 を選択します。

環境プロファイルを削除する

Amazon では DataZone、環境プロファイルは環境の作成に使用できるテンプレートです。環境プロファイルの目的は、 などの配置情報を埋め込むことで環境の作成を簡素化することです。 AWS プロファイル内の アカウントとリージョン。詳細については、「Amazon DataZone の用語と概念」を参照してください。Amazon DataZone ドメインの環境プロファイルを削除するには、Amazon DataZone プロジェクトに属している必要があります。

> **Note**
>
> 環境プロファイルを削除すると、このプロファイルを使用して環境を作成できなくなります。

環境プロファイルを削除するには

1. Amazon DataZone データポータルに移動URLし、シングルサインオン (SSO) または を使用してサインインします。 AWS 認証情報。Amazon DataZone 管理者の場合は、https://console.aws.amazon.com/datazone で Amazon DataZone コンソールに移動し、 でサインインできます。 AWS アカウント ドメインが作成された場所で、Open data portal を選択します。
2. データポータルで、プロジェクトを参照を選択し、環境プロファイルを削除するプロジェクトを選択します。
3. プロジェクト内の環境タブに移動し、環境プロファイル を選択し、削除する環境プロファイルを選択します。
4. 削除する環境プロファイルを選択し、アクション、削除、削除の確認を選択します。

新しい環境を作成する

Amazon DataZone プロジェクトでは、環境は設定されたリソース (Amazon S3 バケット、 AWS Glue データベース、または Amazon Athena ワークグループ) 。特定のIAMプリンシパル (環境ユーザーロール) セットには、これらのリソースを操作できる所有者または寄稿者のアクセス許可が割り当てられます。詳細については、「Amazon DataZone の用語と概念」を参照してください。

データポータルへのアクセスに必要な権限を持つ Amazon DataZone ユーザーは、プロジェクト内に Amazon DataZone 環境を作成できます。

新しい環境を作成するには、次のステップを実行します。

1. Amazon DataZone データポータルに移動URLし、シングルサインオン (SSO) または を使用してサインインします。 AWS 認証情報。Amazon DataZone 管理者の場合は、https://console.aws.amazon.com/datazone で Amazon DataZone コンソールに移動し、 でサインインできます。 AWS アカウント ドメインが作成された場所で、Open data portal を選択します。
2. すべてのプロジェクトを参照を選択し、新しい環境を作成するプロジェクトを選択します。
3. 環境の作成 を選択し、次のフィールドの値を指定してから、環境の作成 を選択します。

   - 名前 – 環境名
   - 説明 – 環境の説明
   - 環境プロファイル – 既存の環境プロファイルを選択するか、新しい環境プロファイルを作成します。環境プロファイルは、環境の作成に使用できるテンプレートです。詳細については、「Amazon DataZone の用語と概念」を参照してください。

     環境プロファイルを選択したら、パラメータセクションで、この環境プロファイルの一部であるフィールドの値を指定します。

環境を編集する

Amazon DataZone プロジェクトでは、環境は設定されたリソース (Amazon S3 バケット、 AWS Glue データベース、または Amazon Athena ワークグループ) 。これらのリソースを操作できる特定のIAMプリンシパルのセット (寄稿者アクセス許可が割り当てられている) 。詳細については、「Amazon DataZone の用語と概念」を参照してください。

データポータルへのアクセスに必要な権限を持つ Amazon DataZone ユーザーは、プロジェクト内の Amazon DataZone 環境を編集できます。

既存の環境を編集するには、次のステップを実行します。

1. Amazon DataZone データポータルに移動URLし、シングルサインオン (SSO) または を使用してサインインします。 AWS 認証情報。Amazon DataZone 管理者の場合は、https://console.aws.amazon.com/datazone で Amazon DataZone コンソールに移動し、 でサインインできます。 AWS アカウント ドメインが作成された場所で、Open data portal を選択します。
2. 上部のナビゲーションペインからプロジェクトを参照を選択し、編集する環境を含むプロジェクトを選択します。
3. 環境を見つけて選択し、詳細ページを開きます。次に、アクション を展開し、環境の編集 を選択します。
4. 環境の名前と説明を編集し、変更を保存 を選択します。

環境を削除する

Amazon DataZone プロジェクトでは、環境は設定されたリソース (Amazon S3 バケット、 AWS Glue データベース、または Amazon Athena ワークグループ) 。これらのリソースを操作できる特定のIAMプリンシパルのセット (寄稿者アクセス許可が割り当てられている) 。詳細については、「Amazon DataZone の用語と概念」を参照してください。

データポータルへのアクセスに必要な権限を持つ Amazon DataZone ユーザーは、プロジェクト内の Amazon DataZone 環境を削除できます。

既存の環境を削除するには、次のステップを実行します。

1. Amazon DataZone データポータルに移動URLし、シングルサインオン (SSO) または を使用してサインインします。 AWS 認証情報。Amazon DataZone 管理者の場合は、https://console.aws.amazon.com/datazone で Amazon DataZone コンソールに移動し、 でサインインできます。 AWS アカウント ドメインが作成された場所で、データポータルを開く を選択します。
2. 上部のナビゲーションペインからプロジェクトを参照を選択し、削除する環境を含むプロジェクトを選択します。
3. 環境を見つけて選択し、詳細ページを開き、アクション を展開して環境の削除 を選択します。
4. 「環境の削除」ポップアップウィンドウで、`Delete`「」フィールドに入力して削除を確定し、「環境の削除」を選択します。

   この環境への依存関係を持つすべてのエンティティが削除された後にのみ、環境を正常に削除できます。環境を削除するには、まず、関連するすべてのデータソースとサブスクリプションターゲットを削除する必要があります。

の新規プロジェクトの作成

Amazon では DataZone、プロジェクトにより、Amazon DataZone カタログ内のデータアセットの公開、検出、サブスクライブ、消費など、さまざまなビジネスユースケースでユーザーのグループがコラボレーションできるようになります。詳細については、「Amazon DataZone の用語と概念」を参照してください。

データポータルへのアクセスに必要な権限を持つ Amazon DataZone ユーザーは、Amazon DataZone プロジェクトを作成できます。

新しいプロジェクトを作成するには、次のステップを実行します。

1. Amazon DataZone データポータルに移動URLし、シングルサインオン (SSO) または を使用してサインインします。 AWS 認証情報。Amazon DataZone 管理者の場合は、https://console.aws.amazon.com/datazone で Amazon DataZone コンソールに移動し、 でサインインできます。 AWS アカウント ドメインが作成された場所で、データポータルを開く を選択します。
2. Amazon DataZone データポータルで、プロジェクトの作成 を選択します。
3. 次のフィールドに値を指定し、プロジェクトの作成 を選択します。

   - 名前 – プロジェクト名。
   - 説明 – プロジェクトの説明。
   - ドメイン単位 – このプロジェクトを作成するドメイン単位。

プロジェクトの編集

Amazon では DataZone、プロジェクトにより、Amazon DataZone カタログ内のデータアセットの公開、検出、サブスクライブ、消費など、さまざまなビジネスユースケースでユーザーのグループがコラボレーションできるようになります。詳細については、「Amazon DataZone の用語と概念」を参照してください。Amazon DataZone プロジェクトを編集するには、そのプロジェクトの所有者であるか、このプロジェクトを含むドメインのドメイン管理者である必要があります。

既存のプロジェクトを編集するには、次のステップを実行します。

1. Amazon DataZone データポータルに移動URLし、シングルサインオン (SSO) または を使用してサインインします。 AWS 認証情報。Amazon DataZone 管理者の場合は、https://console.aws.amazon.com/datazone で Amazon DataZone コンソールに移動し、 でサインインできます。 AWS アカウント ドメインが作成された場所で、Open data portal を選択します。
2. プロジェクトを参照 を選択します。
3. 編集するプロジェクトを選択します。プロジェクトのリストにすぐに表示されない場合は、プロジェクトの検索フィールドにプロジェクト名を指定して検索できます。
4. アクションを展開し、プロジェクトの編集 を選択します。
5. プロジェクト名と説明を更新し、保存 を選択します。

プロジェクトの削除

Amazon では DataZone、プロジェクトにより、Amazon DataZone カタログ内のデータアセットの公開、検出、サブスクライブ、使用など、さまざまなビジネスユースケースでユーザーのグループがコラボレーションできるようになります。詳細については、「Amazon DataZone の用語と概念」を参照してください。

プロジェクトを削除する行為は最終的なものです。削除により、データソース、環境、アセット、用語集、メタデータフォームなど、プロジェクトのコンテンツが取り消し不能で削除されます。Amazon DataZone は、Lake Formation と Amazon Redshift を介して Amazon がマネージドアセットに付与した許可を DataZone 取り消します。プロジェクトを削除しても Amazon 以外の は削除されません DataZone AWS Amazon が作成した DataZone リソース。これらが不要になった場合 AWS リソース、それぞれの で削除 AWS サービスとアカウント。

Amazon DataZone プロジェクトを削除するには、プロジェクトの所有者である必要があります。

既存のプロジェクトを削除するには、次のステップを実行します。

1. Amazon DataZone データポータルに移動URLし、シングルサインオン (SSO) または を使用してサインインします。 AWS 認証情報。IAM プリンシパルは https://console.aws.amazon.com/datazone で Amazon DataZone コンソールに移動し、 でサインインできます。 AWS アカウント ドメインが作成された場所で、データポータルを開く を選択します。
2. 上部のナビゲーションペインからプロジェクトを参照を選択します。
3. 削除するプロジェクトを選択します。プロジェクトのリストに表示されない場合は、プロジェクトの検索フィールドにプロジェクト名を指定して検索できます。
4. アクション を展開し、プロジェクトの削除 を選択します。

   プロジェクトの削除による潜在的な影響に関する情報の警告を確認します。
5. 警告を受け入れる場合は、確認テキストを入力し、「削除」を選択します。

> **Important**
>
> プロジェクトの削除は、ユーザーまたは によって元に戻すことができない取り消し不可能なアクションです。 AWS.

> **Note**
>
> ユーザーまたはドメインユーザーがプロジェクトに環境を作成すると、Amazon DataZone は を作成します。 AWS ドメインまたは関連するアカウントの リソース。ユーザーおよびドメインユーザーに機能を提供します。以下は のリストです。 AWS Amazon がプロジェクト用に作成 DataZone できる リソースとデフォルト名。プロジェクトを削除しても、これらはいずれも削除されません。 AWS の リソース AWS アカウント。
>
> - IAM roles: datazone_usr_<environmentId > 。
> - Glue データベース: (1) <environmentName>_pub_db-*、(2) <environmentName>_sub_db-*。この名前の既存のデータベースがすでにある場合、Amazon DataZone は環境 ID を追加します。
> - Athena ワークグループ: <environmentName>-*。この名前の既存のワークグループがすでに存在する場合、Amazon DataZone は環境 ID を追加します。
> - CloudWatch ロググループ: datazone_<environmentId >

プロジェクトを離れる

Amazon では DataZone、プロジェクトにより、Amazon DataZone カタログ内のデータアセットの公開、検出、サブスクライブ、消費など、さまざまなビジネスユースケースでユーザーのグループがコラボレーションできるようになります。詳細については、「Amazon DataZone の用語と概念」を参照してください。

既存のプロジェクトを離れるには、次のステップを実行します。

1. Amazon DataZone データポータルに移動URLし、シングルサインオン (SSO) または を使用してサインインします。 AWS 認証情報。Amazon DataZone 管理者の場合は、https://console.aws.amazon.com/datazone で Amazon DataZone コンソールに移動し、 でサインインできます。 AWS アカウント ドメインが作成された場所で、データポータルを開く を選択します。
2. 上部のナビゲーションペインからプロジェクトの選択を選択し、プロジェクトを選択します。
3. 終了するプロジェクトを選択します。プロジェクトのリストにすぐに表示されない場合は、プロジェクトの検索フィールドにプロジェクト名を指定して検索できます。
4. アクション を展開し、プロジェクト を残す を選択します。

プロジェクトにメンバーを追加する

Amazon では DataZone、プロジェクトにより、Amazon DataZone カタログ内のデータアセットの公開、検出、サブスクライブ、消費など、さまざまなビジネスユースケースでユーザーのグループがコラボレーションできるようになります。詳細については、「Amazon DataZone の用語と概念」を参照してください。

プロジェクトにメンバーを追加するには、プロジェクト所有者または寄稿者である必要があります。SSO グループ、SSOユーザー、またはIAMプリンシパル (ロールまたはユーザー) をプロジェクトメンバーとして追加できます。

終了しているプロジェクトにメンバーを追加するには、次のステップを実行します。

1. Amazon DataZone データポータルに移動URLし、シングルサインオン (SSO) または を使用してサインインします。 AWS 認証情報。Amazon DataZone 管理者の場合は、https://console.aws.amazon.com/datazone で Amazon DataZone コンソールに移動し、 でサインインできます。 AWS アカウント ドメインが作成された場所で、データポータルを開く を選択します。
2. 上部のナビゲーションペインからプロジェクトの選択を選択し、プロジェクトを選択します。
3. memebr を追加するプロジェクトを選択します。プロジェクトのリストにすぐに表示されない場合は、プロジェクトの検索フィールドにプロジェクト名を指定して検索できます。
4. プロジェクトの詳細ページで、メンバー タブを選択し、「すべてのメンバー」ノードを選択します。
5. プロジェクトメンバー タブで、メンバーの追加 を選択します。
6. プロジェクトにメンバーを追加するポップアップウィンドウで、追加するユーザー (複数可) を指定し、プロジェクト内のロール (所有者または寄稿者) を指定し、メンバーを追加 を選択します。

> **Important**
>
> これらのユーザーは、このプロジェクトが存在するドメイン単位に設定されたプロジェクトメンバーシップ承認ポリシーによって、このプロジェクトのメンバーになることを許可されたプロジェクトメンバーとしてのみ追加できます。詳細については、「Amazon DataZone ドメイン単位内のユーザーとグループに承認ポリシーを割り当てる」を参照してください。

> **Note**
>
> IAM プリンシパルに既に Amazon DataZone ユーザープロファイルがドメインにある場合は、プリンシパルをプロジェクトメンバーとして追加できます。Amazon は、ポータル、、APIまたは を介してドメインと正常にやり取りすると、IAMプリンシパルのユーザープロファイル DataZone を自動的に作成しますCLI。IAM プリンシパルのユーザープロファイルを作成することはできません。IAM プリンシパルにドメインに既存の Amazon DataZone ユーザープロファイルがない場合にプリンIAMシパルをプロジェクトメンバーとして追加するには、 IAM コンソールAmazonDataZoneDomainExecutionRoleでドメインの に次の `iam:GetUser` 2 つのIAMアクセス許可を追加するように管理者に依頼しますiam:GetRole。これとは別に、ドメインでアクションを実行するには、IAMプリンシパルがそのようなアクションに対応するIAMアクセス許可を持っている必要があります。

プロジェクトからメンバーを削除する

Amazon では DataZone、プロジェクトにより、Amazon DataZone カタログ内のデータアセットの公開、検出、サブスクライブ、消費など、さまざまなビジネスユースケースでユーザーのグループがコラボレーションできるようになります。詳細については、「Amazon DataZone の用語と概念」を参照してください。プロジェクトからメンバーを削除するには、プロジェクト所有者である必要があります。

終了したプロジェクトからメンバーを削除するには、次のステップを実行します。

1. データポータルを使用して Amazon DataZone データポータルに移動URLし、 SSOまたは を使用してログインします。 AWS 認証情報。Amazon DataZone 管理者の場合は、 の https://console.aws.amazon.com/datazone にある Amazon DataZone コンソールURLにアクセスしてデータポータルを取得できます。 AWS Amazon DataZone ドメインが作成された アカウント。
2. 上部のナビゲーションペインからプロジェクトの選択を選択し、プロジェクトを選択します。
3. memebr を削除するプロジェクトを選択します。プロジェクトのリストにすぐに表示されない場合は、プロジェクトの検索フィールドにプロジェクト名を指定して検索できます。
4. プロジェクトの詳細ページで、メンバー タブを選択し、「すべてのメンバー」ノードを選択します。
5. プロジェクトメンバー タブで、プロジェクトから削除するメンバー (複数可) を選択し、 の削除を選択します。
6. メンバーの削除 ポップアップウィンドウで、メンバーの削除 を選択して削除を確認します。

Amazon でのデータインベントリと公開 DataZone

このセクションでは、Amazon でデータのインベントリを作成し、Amazon でデータを公開するために実行するタスク DataZone と手順について説明します DataZone。

Amazon を使用してデータを DataZone カタログ化するには、まずデータ (アセット) を Amazon のプロジェクトのインベントリとして持ち込む必要があります DataZone。特定のプロジェクトのインベントリを作成すると、そのプロジェクトのメンバーのみがアセットを検出できるようになります。プロジェクトインベントリアセットは、明示的に公開されていない限り、検索/閲覧のすべてのドメインユーザーが利用できるわけではありません。プロジェクトインベントリを作成した後、データ所有者は、ビジネス名 (アセットとスキーマ) 、説明 (アセットとスキーマ) 、読み上げ、用語集用語 (アセットとスキーマ) 、メタデータフォームを追加または更新することで、必要なビジネスメタデータを使用してインベントリアセットをキュレートできます。

Amazon を使用してデータを DataZone カタログ化する次のステップは、プロジェクトのインベントリアセットをドメインユーザーが検出できるようにすることです。これを行うには、インベントリアセットを Amazon DataZone カタログに発行します。インベントリアセットの最新バージョンのみをカタログに公開でき、最新の公開バージョンのみが検出カタログでアクティブになります。インベントリアセットが Amazon DataZone カタログに公開された後に更新された場合は、最新バージョンが検出カタログに含まれるように、インベントリアセットを再度明示的に公開する必要があります。

詳細については、「Amazon DataZone の用語と概念」を参照してください

トピック

- Amazon の Lake Formation アクセス許可を設定する DataZone
- カスタムアセットタイプを作成する
- の Amazon DataZone データソースを作成して実行する AWS Glue Data Catalog
- Amazon Redshift の Amazon DataZone データソースを作成して実行する
- データソースを編集する
- データソースの削除
- プロジェクトインベントリから Amazon DataZone カタログにアセットを発行する
- インベントリの管理とアセットのキュレート
- アセットを手動で作成する
- Amazon DataZone カタログからアセットを公開解除する
- Amazon DataZone アセットを削除する

- Amazon でデータソース実行を手動で開始する DataZone
- Amazon でのアセットリビジョン DataZone
- Amazon のデータ品質 DataZone
- 機械学習と生成 AI の使用
- Amazon のデータ系統 DataZone （ プレビュー ）

Amazon の Lake Formation アクセス許可を設定する DataZone

組み込みのデータレイク設計図 (DefaultDataLake) を使用して環境を作成する場合、 AWS Glue データベースは、この環境の作成プロセス DataZone の一環として Amazon に追加されます。この からアセットを発行する場合 AWS Glue データベース。追加のアクセス許可は必要ありません。

ただし、アセットを公開し、 からアセットをサブスクライブする場合は、 AWS Amazon DataZone 環境の外部に存在する Glue データベースでは、この外部 DataZone にあるテーブルにアクセスするためのアクセス許可を Amazon に明示的に提供する必要があります。 AWS Glue データベース。これを行うには、 で次の設定を完了する必要があります。 AWS Lake Formation を使用して、必要な Lake Formation 許可を AmazonDataZoneGlueAccess-<region>-<domainId > にアタッチします。

- でデータレイクの Amazon S3 の場所を設定する AWS Lake Formation 許可モード またはハイブリッドアクセスモード の Lake Formation。詳細については、https://docs.aws.amazon.com/lake-formation/「 latest/dg/register-data-lake.html」を参照してください。
- Amazon がIAMAllowedPrincipalsアクセス許可 DataZone を処理する Amazon Lake Formation テーブルからアクセス許可を削除します。詳細については、https://docs.aws.amazon.com/lake-formation/「 latest/dg/upgrade-glue-lake-formation-background.html」を参照してください。
- 以下をアタッチする AWS への Lake Formation 許可AmazonDataZoneGlueAccess-<region>-<domainId > ：
  - Describe テーブルが存在するデータベースに対する および アクセスDescribe grantable許可
  - Describeユーザーに代わってアクセスを管理する上記のデータベース内のすべてのテーブルに対する SelectDescribe Grantable、 DataZone 、、 のアクセスSelect Grantable許可。

> **Note**
>
> Amazon が DataZone をサポート AWS Lake Formation ハイブリッドモード。Lake Formation ハイブリッドモードでは、アクセス許可の管理を開始できます。 AWS Lake Formation を通じてデータベースとテーブルを Glue しながら、これらのテーブルとデータベースに対する既存のIAMアクセス許可は維持します。詳細については、「Amazon と DataZone の統合 AWS Lake Formation ハイブリッドモード」を参照してください

詳細については、「Amazon の AWS Lake Formation 許可のトラブルシューティング DataZone」を参照してください。

Amazon と DataZone の統合 AWS Lake Formation ハイブリッドモード

Amazon DataZone は と統合されています AWS Lake Formation ハイブリッドモード。この統合により、 を簡単に公開および共有できます。 AWS で登録しなくても Amazon DataZone 経由でテーブルを Glue する AWS Lake Formation を最初に使用します。ハイブリッドモードでは、 に対するアクセス許可の管理を開始できます。 AWS による Glue テーブル AWS Lake Formation は、これらのテーブルに対する既存のIAMアクセス許可を維持したままです。

開始するには、Amazon DataZone マネジメントコンソールのDefaultDataLakeブループリントでデータロケーション登録設定を有効にします。

との統合を有効にする AWS Lake Formation ハイブリッドモード

1. https://console.aws.amazon.com/datazone の Amazon DataZone コンソールに移動し、アカウントの認証情報を使用してサインインします。
2. ドメインを表示を選択し、統合を有効にするドメインを選択します。 AWS Lake Formation ハイブリッドモード。
3. ドメインの詳細ページで、ブループリントタブに移動します。
4. ブループリント リストから、DefaultDataLakeブループリントを選択します。
5. DefaultDataLake ブループリントが有効になっていることを確認します。有効になっていない場合は、「」の手順に従って、 でで組み込みブループリントを有効にする AWS Amazon DataZone ドメインを所有する アカウント有効にします。 AWS アカウント。
6. DefaultDataLake 詳細ページでプロビジョニングタブを開き、ページの右上隅にある編集ボタンを選択します。

7. 「データロケーション登録」で、データロケーション登録を有効にするチェックボックスをオンにします。
8. データロケーション管理ロールでは、新しいIAMロールを作成するか、既存のIAMロールを選択できます。Amazon DataZone は、このロールを使用して、Data Lake 用に選択した Amazon S3 バケットへの読み取り/書き込みアクセスを管理します (AWS Lake Formation ハイブリッドアクセスモード。詳細については、「AmazonDataZoneS3Manage-<region>-<domainId >」を参照してください。
9. オプションで、Amazon がハイブリッドモードで自動的に登録しないようにする場合は DataZone 、特定の Amazon S3 ロケーションを除外するように選択できます。そのためには、次のステップを実行します。

   - トグルボタンを選択して、指定された Amazon S3 の場所を除外します。
   - 除外する Amazon S3 バケットURIの を指定します。
   - バケットを追加するには、S3 ロケーションの追加を選択します。

   > **Note**
   >
   > Amazon DataZone では、ルート S3 の場所のみを除外できます。ルート S3 ロケーションのパス内の S3 ロケーションは、自動的に登録から除外されます。

   - [Save changes] (変更の保存) をクリックします。

でデータロケーション登録設定を有効にしたら、 AWS データコンシューマーが にサブスクライブするときの アカウント AWS アクセスIAM許可によって管理される Glue テーブルでは、Amazon DataZone はまずこのテーブルの Amazon S3 ロケーションをハイブリッドモードで登録し、次にを介してテーブルに対するアクセス許可を管理することでデータコンシューマーへのアクセスを許可します。 AWS Lake Formation。これにより、新しく付与された でテーブルに対するIAMアクセス許可が引き続き存在するようになります。 AWS 既存のワークフローを中断することなく、Lake Formation のアクセス許可。

を有効にするときに暗号化された Amazon S3 の場所を処理する方法 AWS Amazon での Lake Formation ハイブリッドモードの統合 DataZone

カスタマー管理の または で暗号化された Amazon S3 ロケーションを使用している場合 AWS マネージドKMSキー、AmazonDataZoneS3Manage ロールには、KMSキーを使用してデータを暗号化および復号するアクセス許可が必要です。または、KMSキーポリシーは、キーに対するアクセス許可をロールに付与する必要があります。

Amazon S3 の場所が で暗号化されている場合 AWS マネージドキーで、次のインラインポリシーをAmazonDataZoneDataLocationManagementロールに追加します。

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

Amazon S3 ロケーションがカスタマーマネージドキーで暗号化されている場合は、次の操作を行います。

1. を開く AWS KMS /https://console.aws.amazon.comkms のコンソールで としてログインする AWS Identity and Access Management (IAM) 管理ユーザー、または場所の暗号化に使用されるキーのKMSキーポリシーを変更できるユーザー。
2. ナビゲーションペインで、カスタマーマネージドキー を選択し、目的のKMSキーの名前を選択します。
3. KMS キーの詳細ページでキーポリシータブを選択し、次のいずれかを実行してカスタムロールまたは Lake Formation サービスにリンクされたロールをKMSキーユーザーとして追加します。

   - デフォルトビューが表示されている場合 (キー管理者、キー削除、キーユーザーなどを含む AWS アカウントセクション) – キーユーザーセクションで、AmazonDataZoneDataLocationManagementロールを追加します。
   - キーポリシー (JSON) が表示されている場合 – 次の例に示すように、ポリシーを編集して、オブジェクト「キーの使用を許可」にAmazonDataZoneDataLocationManagementロールを追加します。

```
...
        {
            "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**
>
> KMS キーまたは Amazon S3 の場所が同じでない場合 AWS アカウントをデータカタログとして、「 間で暗号化された Amazon S3 ロケーションを登録する」の手順に従います。Amazon S3 AWS アカウント 。

カスタムアセットタイプを作成する

Amazon では DataZone、アセットはデータベーステーブル、ダッシュボード、機械学習モデルなどの特定のタイプのデータリソースを表します。カタログアセットを記述する際に一貫性と標準化を実現するには、Amazon DataZone ドメインに、カタログでアセットがどのように表現されるかを定義するアセットタイプのセットが必要です。アセットタイプは、特定のタイプのアセットのスキーマを定義します。アセットタイプには、必須およびオプションの名前付きメタデータフォームタイプ (例: govForm または) のセットがあります GovernanceFormType。Amazon のアセットタイプ DataZone はバージョニングされています。アセットが作成されると、アセットタイプ (通常は最新バージョン)

で定義されたスキーマに対して検証され、無効な構造が指定されると、アセットの作成は失敗します。

システムアセットタイプ - Amazon DataZone は、サービス所有のシステムアセットタイプ (GlueTableAssetType GlueViewAssetType、 RedshiftTableAssetType RedshiftViewAssetType、および S3ObjectCollectionAssetType を含む) とシステムフォームタイプ (DataSourceReferenceFormType、 AssetCommonDetailsFormTypeおよび を含む) をプロビジョニングします SubscriptionTermsFormType。システムアセットタイプは編集できません。

カスタムアセットタイプ - カスタムアセットタイプを作成するために、まずフォームタイプで使用する必要なメタデータフォームタイプと用語集を作成します。その後、名前、説明、および関連するメタデータフォームを指定して、カスタムアセットタイプを作成できます。これは必須またはオプションです。

構造化データを持つアセットタイプの場合、データポータルの列スキーマを表すには、 を使用して列名、説明、データ型などの`RelationalTableFormType`技術メタデータを列に追加し、`ColumnBusinessMetadataForm`を使用して、ビジネス名、用語集、カスタムキーバリューペアなどの列のビジネス説明を追加できます。

データポータルを使用してカスタムアセットタイプを作成するには、次のステップを実行します。

1. Amazon DataZone データポータルに移動URLし、シングルサインオン (SSO) または を使用してサインインします。 AWS 認証情報。Amazon DataZone 管理者の場合は、https://console.aws.amazon.com/datazone で Amazon DataZone コンソールに移動し、 でサインインできます。 AWS アカウント ドメインが作成された場所で、Open data portal を選択します。
2. 上部のナビゲーションペインからプロジェクトの選択を選択し、カスタムアセットタイプを作成するプロジェクトを選択します。
3. プロジェクトのデータタブに移動します。
4. 左側のナビゲーションペインからアセットタイプを選択し、アセットタイプの作成を選択します。
5. 以下を指定し、 の作成を選択します。
   - Name - カスタムアセットタイプの名前
   - 説明 - カスタムアセットタイプの説明。
   - メタデータフォームの追加 を選択して、このカスタムアセットタイプにメタデータフォームを追加します。
6. カスタムアセットタイプを作成したら、それを使用してアセットを作成できます。

を使用してカスタムアセットタイプを作成するにはAPIs、次のステップを実行します。

1. CreateFormType API アクションを呼び出してメタデータフォームタイプを作成します。

   Amazon の例を次に示します SageMaker 。

```
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. 次に、 CreateAssetTypeAPIアクションを呼び出してアセットタイプを作成できます。アセットタイプは、使用可能なシステムフォームタイプ (SubscriptionTermsFormType以下の例の) またはカスタムフォームタイプを使用して Amazon DataZone APIs 経由でのみ作成できます。システムフォームタイプの場合、タイプ名は で始まる必要があります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,
        },
    },
)
```

以下は、構造化データのアセットタイプを作成する例です。

```
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. そして、上記のステップで作成したカスタムアセットタイプを使用してアセットを作成できるようになりました。

```
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}"
        }
        ]
)
```

この例では、構造化データアセットを作成します。

```
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": ".."
        },
        .....
        ]
)
```

の Amazon DataZone データソースを作成して実行する AWS Glue Data Catalog

Amazon では DataZone、 を作成できます。 AWS Glue Data Catalog データベーステーブルの技術メタデータを からインポートするための データソース AWS Glue。 のデータソースを追加するには AWS Glue Data Catalog、ソースデータベースは に既に存在している必要があります AWS Glue.

を作成して実行する場合 AWS Glue データソース、ソースからアセットを追加する AWS Glue データベースを Amazon DataZone プロジェクトのインベントリに。は で実行できます。 AWS Glue アセットの技術メタデータを作成または更新するための、設定されたスケジュールまたはオンデマンドでの データソース。データソースの実行中に、オプションでアセットを Amazon DataZone カタログに発行することを選択し、すべてのドメインユーザーがアセットを検出できるようにします。ビジネスメタデータを編集した後、プロジェクトインベントリアセットを公開することもできます。ドメインユーザーは、公開されたアセットを検索して検出し、これらのアセットへのサブスクリプションをリクエストできます。

を追加するには AWS Glue データソース

1. Amazon DataZone データポータルに移動URLし、シングルサインオン (SSO) または を使用してサインインします。 AWS 認証情報。Amazon DataZone 管理者の場合は、https://console.aws.amazon.com/datazone で Amazon DataZone コンソールに移動し、 でサインインできます。 AWS アカウント ドメインが作成された場所で、データポータルを開く を選択します。

2. 上部のナビゲーションペインからプロジェクトの選択を選択し、データソースを追加するプロジェクトを選択します。
3. プロジェクトのデータタブに移動します。
4. 左側のナビゲーションペインからデータソースを選択し、データソースの作成を選択します。
5. 次のフィールドを設定します。

   - 名前 – データソース名。
   - 説明 – データソースの説明。

6. データソースタイプ で、 を選択します。 AWS Glue.
7. 環境を選択 で、 を発行する環境を指定します。 AWS Glue テーブル。
8. データ選択 で、 を指定します。 AWS Glue データベースに を入力し、テーブルの選択基準を入力します。例えば、Include を選択して と入力すると`*corporate`、データベースには、 という単語で終わるすべてのソーステーブルが含まれます`corporate`。

   次のいずれかを選択できます。 AWS Glue データベースをドロップダウンにするか、データベース名を入力します。ドロップダウンには、環境の公開データベースとサブスクリプションデータベースの 2 つのデータベースが含まれます。環境によって作成されていないデータベースからアセットを取り込む場合は、ドロップダウンから選択するのではなく、データベースの名前を入力する必要があります。

   1 つのデータベース内のテーブルに複数の包含ルールと除外ルールを追加できます。別のデータベースを追加 ボタンを使用して、複数のデータベースを追加することもできます。

9. 「データ品質」で、このデータソース のデータ品質を有効にすることを選択できます。これを行うと、Amazon DataZone は既存の をインポートします。 AWS Amazon DataZone カタログへの Glue データ品質出力。デフォルトでは、Amazon は有効期限のない最新の既存の 100 品質レポートを から DataZone インポートします。 AWS Glue。

   Amazon のデータ品質メトリクス DataZone は、データソースの完全性と正確性を理解するのに役立ちます。Amazon は、 からこれらのデータ品質メトリクス DataZone を取得します。 AWS ビジネスデータカタログの検索など、特定の時点にコンテキストを提供するための Glue。データユーザーは、サブスクライブしたアセットのデータ品質メトリクスが時間の経過とともにどのように変化するかを確認できます。データプロデューサーが取り込むことができる AWS スケジュールに基づく Glue データ品質スコア。Amazon DataZone ビジネスデータカタログでは、データ品質 を通じてサードパーティーシステムからのデータ品質メトリクスを表示することもできますAPIs。詳細については、「Amazon のデータ品質 DataZone」を参照してください

10. [Next (次へ)] を選択します。
11. 公開設定 で、アセットがビジネスデータカタログですぐに検出可能かどうかを選択します。インベントリにのみ追加する場合は、後でサブスクリプション条件を選択し、ビジネスデータカタログに発行できます。
12. 自動ビジネス名生成 では、出典からインポートされたアセットのメタデータを自動的に生成するかどうかを選択します。
13. (オプション) メタデータフォーム には、アセットが Amazon にインポートされたときに収集および保存されるメタデータを定義するフォームを追加します DataZone。詳細については、「the section called “メタデータフォームを作成する”」を参照してください。
14. 実行設定 で、データソースを実行するタイミングを選択します。
    - スケジュールに従って実行する – データソースを実行する日時を指定します。
    - オンデマンドで実行 — データソースの実行を手動で開始できます。
15. [Next (次へ)] を選択します。
16. データソース設定を確認し、 の作成を選択します。

> **Note**
>
> の場合 AWS Glue データソースが作成され、Amazon は DataZone 、 内のすべてのテーブルにアクセスするためのデータソースの作成に使用される環境のIAMロールに対する Lake Formation の「読み取り専用」アクセス許可を作成します。 AWS データソースで使用される Glue データベース。これらの権限のステータスは、環境の詳細ページのデータソースでモニタリングできます。Amazon は以下 DataZone を追加します。 AWS へのタグ AWS 公開環境のIAMロールへのアクセス権を付与するときの Glue データベース: `DataZoneDiscoverable_${domainId}: true`
> Amazon の現在のリリースより前に作成された環境では DataZone、プロジェクトメンバーは Amazon Athena で付与されたテーブルを表示できません。

Amazon Redshift の Amazon DataZone データソースを作成して実行する

Amazon では DataZone、Amazon Redshift データウェアハウスからデータベーステーブルとビューのテクニカルメタデータをインポートするために、Amazon Redshift データソースを作成できま

す。Amazon Redshift の Amazon DataZone データソースを追加するには、ソースデータウェアハウスが Amazon Redshift に既に存在している必要があります。

Amazon Redshift データソースを作成して実行するときは、ソース Amazon Redshift データウェアハウスのアセットを Amazon DataZone プロジェクトのインベントリに追加します。Amazon Redshift データソースは、設定されたスケジュールまたはオンデマンドで実行して、アセットの技術メタデータを作成または更新できます。データソースの実行中に、オプションでプロジェクトインベントリアセットを Amazon DataZone カタログに公開し、すべてのドメインユーザーが検出できるようにすることができます。ビジネスメタデータを編集した後にインベントリアセットを発行することもできます。ドメインユーザーは、公開されたアセットを検索して検出し、これらのアセットへのサブスクリプションをリクエストできます。

Amazon Redshift データソースを追加するには

1. Amazon DataZone データポータルに移動URLし、シングルサインオン (SSO) または を使用してサインインします。 AWS 認証情報。Amazon DataZone 管理者の場合は、https://console.aws.amazon.com/datazone で Amazon DataZone コンソールに移動し、 でサインインできます。 AWS アカウント ドメインが作成された場所で、Open data portal を選択します。
2. 上部のナビゲーションペインからプロジェクトの選択を選択し、データソースを追加するプロジェクトを選択します。
3. プロジェクトのデータタブに移動します。
4. 左側のナビゲーションペインからデータソースを選択し、データソースの作成を選択します。
5. 次のフィールドを設定します。

   - 名前 – データソース名。
   - 説明 – データソースの説明。
6. データソースタイプ で、Amazon Redshift を選択します。
7. 環境を選択 で、Amazon Redshift テーブルを発行する環境を指定します。
8. 選択した環境に応じて、Amazon DataZone は環境から直接 Amazon Redshift 認証情報やその他のパラメータを自動的に適用するか、独自のパラメータを選択するオプションを提供します。

   - 環境のデフォルトの Amazon Redshift スキーマからの公開のみを許可する環境を選択した場合、Amazon DataZone は Amazon Redshift 認証情報と、Amazon Redshift クラスターやワークグループ名などの他のパラメータを自動的に適用します。 AWS シークレット、データベース名、スキーマ名。これらの自動入力パラメータは編集できません。
   - がデータを公開できない環境を選択すると、データソースの作成を続行できなくなります。

- 任意のスキーマからのデータの公開を許可する環境を選択すると、環境の認証情報やその他の Amazon Redshift パラメータを使用するか、独自の認証情報/パラメータを入力するオプションが表示されます。

9. 独自の認証情報を使用してデータソースを作成する場合は、次の詳細を指定します。

   - 「Amazon Redshift 認証情報の提供」で、プロビジョニングされた Amazon Redshift クラスターまたは Amazon Redshift Serverless ワークスペースをデータソースとして使用するかどうかを選択します。
   - 上記のステップで選択した内容に応じて、ドロップダウンメニューから Amazon Redshift クラスターまたはワークスペースを選択し、 でシークレットを選択します。 AWS 認証に使用する Secrets Manager。既存のシークレットを選択するか、新しいシークレットを作成できます。
   - 既存のシークレットをドロップダウンに表示するには、 AWS Secrets Manager には、次のタグ (キー/値) が含まれています。
     - AmazonDataZoneProject: <projectID >
     - AmazonDataZoneDomain: <domainID >

     新しいシークレットを作成することを選択した場合、シークレットには上記のタグが自動的に付けられ、追加のステップは必要ありません。詳細については、「 でのデータベース認証情報の保存」を参照してください。 AWS Secrets Manager.

     の Amazon Redshift ユーザー AWS データソースを作成するために提供される シークレットには、公開するテーブルに対するSELECTアクセス許可が必要です。Amazon DataZone がユーザーに代わってサブスクリプション (アクセス) も管理できるようにする場合は、 のデータベースユーザー AWS シークレットには、次のアクセス許可も必要です。

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

10. データ選択 で、Amazon Redshift データベース、スキーマを指定し、テーブルまたはビューの選択基準を入力します。例えば、Include を選択して と入力すると`*corporate`、アセットにはという単語で終わるすべてのソーステーブルが含まれます`corporate`。

    1 つのデータベース内のテーブルに複数のインクルードルールを追加できます。別のデータベースを追加 ボタンを使用して、複数のデータベースを追加することもできます。

11. [Next (次へ)] を選択します。

12. 公開設定 で、アセットがデータカタログですぐに検出可能かどうかを選択します。インベントリにのみ追加する場合は、後でサブスクリプション条件を選択し、ビジネスデータカタログに発行できます。
13. 自動ビジネス名生成 では、アセットのメタデータが公開され、ソースから更新されるときに自動的に生成するかどうかを選択します。
14. (オプション) メタデータフォーム には、アセットが Amazon にインポートされたときに収集および保存されるメタデータを定義するフォームを追加します DataZone。詳細については、「the section called “メタデータフォームを作成する”」を参照してください。
15. 実行設定 で、データソースを実行するタイミングを選択します。
    - スケジュールに従って実行する – データソースを実行する日時を指定します。
    - オンデマンドで実行 — データソースの実行を手動で開始できます。
16. [Next (次へ)] を選択します。
17. データソース設定を確認し、 の作成を選択します。

> **Note**
>
> Amazon Redshift データソースが作成されると、Amazon は、データソースの作成に使用された環境への読み取り専用アクセス DataZone を許可し、データソースで使用される Amazon Redshift スキーマ内のすべてのテーブルにアクセスします。これらの権限のステータスは、環境の詳細ページのデータソースでモニタリングできます。
> 環境の作成に使用したものとは異なる Amazon Redshift クラスターまたは Serverless ワークグループを使用する場合は、次のことを確認する必要があります。 AWS タグがクラスターまたはワークグループに追加されます。これは、環境ユーザーが Amazon Redshift クエリエディタ V2 で付与されたデータベースを表示できるようにするために必要です。
> `DataZoneDiscoverable_${domainId}: true`
> Amazon の現在のリリースより前に作成された環境では DataZone、プロジェクトメンバーは Amazon Redshift で付与されたテーブルを表示できません。

データソースを編集する

Amazon DataZone データソースを作成したら、いつでも変更して、ソースの詳細またはデータ選択条件を変更できます。データソースが不要になった場合は、削除できます。

これらのステップを完了するには、 AmazonDataZoneFullAccess AWS マネージドポリシーがアタッチされました。詳細については、「the section called “AWS 管理ポリシー”」を参照してください。

Amazon DataZone データソースを編集して、テーブルの選択基準の追加、削除、変更など、データ選択設定を変更できます。データベースを追加または削除することもできます。データソースタイプやデータソースが公開されている環境を変更することはできません。

データソースを編集する

1. Amazon DataZone データポータルに移動URLし、シングルサインオン (SSO) または を使用してサインインします。 AWS 認証情報。Amazon DataZone 管理者の場合は、https://console.aws.amazon.com/datazone で Amazon DataZone コンソールに移動し、 でサインインできます。 AWS アカウント ドメインが作成された場所で、Open data portal を選択します。
2. 上部のナビゲーションペインからプロジェクトの選択を選択し、データソースが属するプロジェクトを選択します。
3. プロジェクトのデータタブに移動します。
4. 左側のナビゲーションペインからデータソースを選択し、変更するデータソースを選択します。
5. データソース定義タブに移動し、編集 を選択します。
6. データソース定義を変更します。データソースの詳細を更新し、データ選択条件を変更できます。
7. 変更が完了したら、[保存] を選択します。

データソースの削除

Amazon DataZone データソースを作成したら、いつでも変更して、ソースの詳細またはデータ選択条件を変更できます。

これらのステップを完了するには、 が必要です。 AmazonDataZoneFullAccess AWS マネージドポリシーがアタッチされました。詳細については、「the section called “AWS 管理ポリシー”」を参照してください。

Amazon DataZone データソースが不要になった場合は、それを完全に削除できます。データソースを削除した後も、そのデータソースから生成されたすべてのアセットはカタログで引き続き使用でき、ユーザーは引き続きサブスクライブできます。ただし、アセットはソースからの更新の受信を停止します。依存アセットを削除する前に、まず別のデータソースに移動することをお勧めします。

> **Note**
>
> データソースを削除する前に、データソースのすべてのフルフィルメントを削除する必要があります。詳細については、「データ検出、サブスクリプション、消費」を参照してください。

データソースを削除するには

1. プロジェクトのデータタブで、左側のナビゲーションペインからデータソースを選択します。
2. 削除するデータソースを選択します。
3. アクション、データソースの削除、削除の確認を選択します。

プロジェクトインベントリから Amazon DataZone カタログにアセットを発行する

Amazon DataZone アセットとそのメタデータをプロジェクトインベントリから Amazon DataZone カタログに公開できます。カタログに発行できるのは、アセットの最新バージョンのみです。

カタログにアセットを発行するときは、次の点を考慮してください。

- カタログにアセットを発行するには、そのプロジェクトの所有者または寄稿者である必要があります。
- Amazon Redshift アセットの場合、Amazon が Redshift テーブルとビューへのアクセス DataZone を管理するために、パブリッシャークラスターとサブスクライバークラスターの両方に関連付けられた Amazon Redshift クラスターが Amazon Redshift データ共有のすべての要件を満たしていることを確認します。「Amazon Redshift のデータ共有の概念」を参照してください。
- Amazon は、 から発行されたアセットのアクセス管理 DataZone のみをサポートします。 AWS Glue Data Catalog および Amazon Redshift。Amazon S3 オブジェクトなど、他のすべてのアセットの場合、Amazon DataZone は承認されたサブスクライバーのアクセスを管理しません。これらのアンマネージドアセットをサブスクライブすると、次のメッセージで通知されます。

  ```
  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.
  ```

アセットを公開する

データソースの作成時にデータカタログでアセットをすぐに検出可能にすることを選択しなかった場合は、次のステップを実行して後で公開します。

アセットを発行するには

1. Amazon DataZone データポータルに移動URLし、シングルサインオン (SSO) または を使用してサインインします。 AWS 認証情報。Amazon DataZone 管理者の場合は、https://console.aws.amazon.com/datazone で Amazon DataZone コンソールに移動し、 でサインインできます。 AWS アカウント ドメインが作成された場所で、Open data portal を選択します。
2. 上部のナビゲーションペインからプロジェクトの選択を選択し、アセットが属するプロジェクトを選択します。
3. プロジェクトのデータタブに移動します。
4. 左側のナビゲーションペインからインベントリデータを選択し、公開するアセットを選択します。

   > **Note**
   >
   > デフォルトでは、すべてのアセットにはサブスクリプションの承認が必要です。つまり、データ所有者はアセットへのすべてのサブスクリプションリクエストを承認する必要があります。アセットを公開する前にこの設定を変更する場合は、アセットの詳細を開き、サブスクリプションの承認 の横にある編集 を選択します。この設定は、アセットを変更して再発行することで後で変更できます。

5. アセットの発行 を選択します。アセットはカタログに直接発行されます。

   承認要件の変更など、アセットに変更を加えた場合は、再発行を選択してカタログに更新を発行できます。

インベントリの管理とアセットのキュレート

Amazon を使用してデータを DataZone カタログ化するには、まずデータ (アセット) を Amazon のプロジェクトのインベントリとして持ち込む必要があります DataZone。特定のプロジェクトのインベントリを作成すると、そのプロジェクトのメンバーのみがアセットを検出できるようになります。

アセットがプロジェクトインベントリに作成されると、そのメタデータをキュレーションできます。例えば、アセットの名前、説明を編集したり、読んだりできます。アセットを編集するたびに、ア

セットの新しいバージョンが作成されます。アセットの詳細ページの履歴タブを使用して、すべてのアセットバージョンを表示できます。

「Read Me」セクションを編集し、アセットの詳細な説明を追加できます。Read Me セクションはマークダウンをサポートしているため、必要に応じて説明をフォーマットし、アセットに関する重要な情報をコンシューマーに説明できます。

用語集の用語は、利用可能なフォームに入力することでアセットレベルで追加できます。

スキーマをキュレートするには、列を確認し、ビジネス名、説明を追加し、列レベルで用語集用語を追加します。

データソースの作成時にメタデータの自動生成が有効になっている場合、アセットと列のビジネス名は、個別にまたはすべて一度に確認および承認または拒否できます。

サブスクリプション条件を編集して、アセットの承認が必要かどうかを指定することもできます。

Amazon のメタデータフォーム DataZone では、カスタム定義属性 (販売地域、販売年、販売四半期など) を追加して、データアセットのメタデータモデルを拡張できます。アセットタイプにアタッチされたメタデータフォームは、そのアセットタイプから作成されたすべてのアセットに適用されます。データソースの実行の一環として、または作成後に、個々のアセットにメタデータフォームを追加することもできます。新しいフォームの作成については、「」を参照してくださいthe section called “メタデータフォームを作成する”。

アセットのメタデータを更新するには、アセットが属するプロジェクトの所有者または寄稿者である必要があります。

アセットのメタデータを更新するには

1. Amazon DataZone データポータルに移動URLし、シングルサインオン (SSO) または を使用してサインインします。 AWS 認証情報。Amazon DataZone 管理者の場合は、https://console.aws.amazon.com/datazone で Amazon DataZone コンソールに移動し、 でサインインできます。 AWS アカウント ドメインが作成された場所で、Open data portal を選択します。
2. 上部のナビゲーションペインからプロジェクトを選択を選択し、メタデータを更新するアセットを含むプロジェクトを選択します。
3. プロジェクトのデータタブに移動します。
4. 左側のナビゲーションペインからインベントリデータを選択し、メタデータを更新するアセットの名前を選択します。
5. アセットの詳細ページのメタデータフォーム で、必要に応じて既存のフォームを編集および編集を選択します。追加のメタデータフォームをアセットにアタッチすることもできます。詳細に

ついては、「the section called “追加のメタデータフォームをアセットにアタッチする”」を参照してください。

6. 更新が完了したら、フォームの保存 を選択します。

   フォームを保存すると、Amazon はアセットの新しいインベントリバージョン DataZone を生成します。更新したバージョンをカタログに発行するには、アセットの再発行 を選択します。

追加のメタデータフォームをアセットにアタッチする

デフォルトでは、ドメインにアタッチされたメタデータフォームは、そのドメインに発行されるすべてのアセットにアタッチされます。データパブリッシャーは、追加のコンテキストを提供するために、追加のメタデータフォームを個々のアセットに関連付けることができます。

追加のメタデータフォームをアセットにアタッチするには

1. Amazon DataZone データポータルに移動URLし、シングルサインオン (SSO) または を使用してサインインします。 AWS 認証情報。Amazon DataZone 管理者の場合は、https://console.aws.amazon.com/datazone で Amazon DataZone コンソールに移動し、 でサインインできます。 AWS アカウント ドメインが作成された場所で、Open data portal を選択します。
2. 上部のナビゲーションペインからプロジェクトを選択を選択し、メタデータを追加するアセットを含むプロジェクトを選択します。
3. プロジェクトのデータタブに移動します。
4. 左側のナビゲーションペインからインベントリデータを選択し、メタデータを追加するアセットの名前を選択します。
5. アセットの詳細ページのメタデータフォーム で、フォームの追加 を選択します。
6. アセットに追加するフォーム (複数可) を選択し、フォームの追加 を選択します。
7. 各メタデータフィールドに値を入力し、フォームの保存 を選択します。

   フォームを保存すると、Amazon はアセットの新しいインベントリバージョン DataZone を生成します。更新したバージョンをカタログに公開するには、アセットの再公開 を選択します。

キュレーション後にカタログにアセットを発行する

アセットキュレーションに満足すると、データ所有者はアセットバージョンを Amazon DataZone カタログに発行し、すべてのドメインユーザーが検出できるようになります。アセットには、インベントリバージョンと公開されたバージョンが表示されます。検出カタログには、最新の公開バージョン

のみが表示されます。公開後にメタデータが更新されると、新しいインベントリバージョンがカタログに公開できるようになります。

アセットを手動で作成する

Amazon では DataZone、アセットは、単一の物理データオブジェクト (テーブル、ダッシュボード、ファイルなど) または仮想データオブジェクト (ビューなど) を表示するエンティティです。詳細については、「Amazon DataZone の用語と概念」を参照してください。アセットを手動で公開するのは 1 回限りのオペレーションです。アセットの実行スケジュールを指定しないため、ソースが変更されても自動的には更新されません。

プロジェクトを通じてアセットを手動で作成するには、そのプロジェクトの所有者または寄稿者である必要があります。

アセットを手動で作成するには

1. Amazon DataZone データポータルに移動URLし、シングルサインオン (SSO) または を使用してサインインします。 AWS 認証情報。Amazon DataZone 管理者の場合は、https://console.aws.amazon.com/datazone で Amazon DataZone コンソールに移動し、 でサインインできます。 AWS アカウント ドメインが作成された場所で、データポータルを開く を選択します。
2. 上部のナビゲーションペインからプロジェクトの選択を選択し、アセットを作成するプロジェクトを選択します。
3. プロジェクトのデータタブに移動します。
4. 左側のナビゲーションペインからデータソースを選択し、データアセットの作成を選択します。
5. アセットの詳細 では、次の設定を行います。

   - アセットタイプ – アセットのタイプ。
   - 名前 – アセットの名前。
   - 説明 – アセットの説明。
6. S3 の場所 には、ソース S3 バケットの Amazon リソースネーム (ARN) を入力します。

   必要に応じて、S3 アクセスポイントを入力します。詳細については、Amazon S3 アクセスポイントによるデータアクセスの管理を参照してください。
7. 公開設定 で、カタログでアセットをすぐに検出可能にするかどうかを選択します。インベントリにのみ追加する場合は、後でサブスクリプション条件を選択してカタログに発行できます。
8. [Create] (作成) を選択します。

アセットが作成されると、カタログ内のアクティブなアセットとして直接公開されるか、公開するまでインベントリに保存されます。

Amazon DataZone カタログからアセットを公開解除する

カタログから Amazon DataZone アセットを公開解除すると、グローバル検索結果に表示されなくなります。新規ユーザーはカタログ内のアセットリストを検索またはサブスクライブすることはできませんが、既存のサブスクリプションはすべて同じままです。

アセットの公開を解除するには、アセットが属するプロジェクトの所有者または寄稿者である必要があります。

アセットの公開を解除するには

1. Amazon DataZone データポータルに移動URLし、シングルサインオン (SSO) または を使用してサインインします。 AWS 認証情報。Amazon DataZone 管理者の場合は、https://console.aws.amazon.com/datazone で Amazon DataZone コンソールに移動し、 でサインインできます。 AWS アカウント ドメインが作成された場所で、Open data portal を選択します。
2. 上部のナビゲーションペインからプロジェクトの選択を選択し、アセットが属するプロジェクトを選択します。
3. プロジェクトのデータタブに移動します。
4. 左側のナビゲーションペインから公開されたデータを選択します。
5. 公開されたアセットのリストからアセットを検索し、「公開解除」を選択します。

   アセットはカタログから削除されます。Publish を選択すると、いつでもアセットを再発行できます。

Amazon DataZone アセットを削除する

Amazon でアセットが不要になった場合は DataZone、完全に削除できます。アセットの削除は、カタログからアセットを非公開にする場合とは異なります。カタログ内のアセットとその関連リストを削除して、検索結果に表示されないようにすることができます。アセットリストを削除するには、まずそのすべてのサブスクリプションを取り消す必要があります。

アセットを削除するには、アセットが属するプロジェクトの所有者または寄稿者である必要があります。

> **Note**
>
> アセットリストを削除するには、まずアセットへの既存のサブスクリプションをすべて取り消す必要があります。既存のサブスクライバーを持つアセットリストを削除することはできません。

とアセットを削除するには

1. Amazon DataZone データポータルに移動URLし、シングルサインオン (SSO) または を使用してサインインします。 AWS 認証情報。Amazon DataZone 管理者の場合は、https://console.aws.amazon.com/datazone で Amazon DataZone コンソールに移動し、 でサインインできます。 AWS アカウント ドメインが作成された場所で、Open data portal を選択します。
2. 上部のナビゲーションペインからプロジェクトの選択を選択し、削除するアセットを含むプロジェクトを選択します。
3. プロジェクトのデータタブに移動します。
4. 左側のナビゲーションペインから公開されたデータを選択し、削除するアセットを見つけて選択します。アセットの詳細ページが開きます。
5. アクション、削除、削除の確認を選択します。

   アセットを削除すると、そのアセットは表示できなくなり、ユーザーはアセットをサブスクライブできなくなります。

Amazon でデータソース実行を手動で開始する DataZone

データソースを実行すると、Amazon はソースからすべての新規または変更されたメタデータを DataZone プルし、インベントリ内の関連するアセットを更新します。Amazon にデータソースを追加するときは DataZone、ソースの実行設定を指定します。これにより、ソースがスケジュールに従って実行されるか、オンデマンドで実行されるかが定義されます。ソースがオンデマンドで実行されている場合は、データソースの実行を手動で開始する必要があります。

ソースがスケジュールに従って実行されていても、いつでも手動で実行できます。ビジネスメタデータをアセットに追加した後、アセットを選択して Amazon DataZone カタログに公開することで、すべてのドメインユーザーがこれらのアセットを検出できるようになります。公開されたアセットのみが、他のドメインユーザーが検索できます。

データソースを手動で実行するには

1. Amazon DataZone データポータルに移動URLし、シングルサインオン (SSO) または を使用してサインインします。 AWS 認証情報。Amazon DataZone 管理者の場合は、https://console.aws.amazon.com/datazone で Amazon DataZone コンソールに移動し、 でサインインできます。 AWS アカウント ドメインが作成された場所で、データポータルを開く を選択します。
2. 上部のナビゲーションペインからプロジェクトの選択を選択し、データソースが属するプロジェクトを選択します。
3. プロジェクトのデータタブに移動します。
4. 左側のナビゲーションペインからデータソースを選択し、実行するデータソースを見つけて選択します。データソースの詳細ページが開きます。
5. オンデマンドで実行 を選択します。

   Amazon がアセットメタデータをソースの最新のデータで DataZone 更新Runningすると、データソースのステータスは に変わります。データソース実行タブで実行のステータスをモニタリングできます。

Amazon でのアセットリビジョン DataZone

Amazon は、ビジネスメタデータまたは技術メタデータを編集するときに、アセットのリビジョンを DataZone 増分します。これらの編集には、アセット名、説明、用語集、列名、メタデータフォーム、メタデータフォームフィールド値の変更が含まれます。これらの変更は、手動編集、データソースジョブの実行、またはAPIオペレーションによって発生する可能性があります。Amazon は、アセットを編集するたびに新しいアセットリビジョン DataZone を自動的に生成します。

アセットを更新し、新しいリビジョンを生成したら、新しいリビジョンをカタログに公開して、サブスクライバーがアセットを更新して使用できるようにする必要があります。詳細については、「the section called “プロジェクトインベントリからカタログにアセットを発行する”」を参照してください。カタログに発行できるのは、アセットの最新バージョンのみです。

アセットの過去のリビジョンを表示するには

1. Amazon DataZone データポータルに移動URLし、シングルサインオン (SSO) または を使用してサインインします。 AWS 認証情報。Amazon DataZone 管理者の場合は、https://console.aws.amazon.com/datazone で Amazon DataZone コンソールに移動し、 でサインイン

できます。 AWS アカウント ドメインが作成された場所で、データポータルを開く を選択します。

2. 上部のナビゲーションペインからプロジェクトの選択を選択し、アセットを含むプロジェクトを選択します。
3. プロジェクトのデータタブに移動し、アセットを見つけて選択します。アセットの詳細ページが開きます。
4. 履歴タブに移動し、アセットの過去のリビジョンのリストを表示します。

Amazon のデータ品質 DataZone

Amazon のデータ品質メトリクス DataZone は、データソースの完全性、タイムライン、精度など、さまざまな品質メトリクスを理解するのに役立ちます。Amazon DataZone は と統合します AWS Glue Data Quality と はAPIs、サードパーティーのデータ品質ソリューションのデータ品質メトリクスを統合するための を提供しています。データユーザーは、サブスクライブしたアセットのデータ品質メトリクスが時間の経過とともにどのように変化するかを確認できます。データ品質ルールを作成して実行するには、 などの任意のデータ品質ツールを使用できます。 AWS Glue データ品質。Amazon のデータ品質メトリクスを使用すると DataZone、データコンシューマーはアセットと列のデータ品質スコアを視覚化できるため、意思決定に使用するデータの信頼を構築できます。

前提条件とIAMロールの変更

Amazon DataZoneの を使用している場合 AWS 管理ポリシー。追加の設定手順はなく、これらの管理ポリシーは自動的に更新され、データ品質がサポートされます。サポートされている サービスと相互運用するために必要なアクセス許可 DataZone を Amazon に付与するロールに独自のポリシーを使用している場合は、これらのロールにアタッチされているポリシーを更新して、 の読み取りのサポートを有効にする必要があります。 AWS の Glue データ品質情報。 AWS マネージドポリシー：AmazonDataZoneGlueManageAccessRolePolicy および AWS マネージドポリシー：AmazonDataZoneDomainExecutionRolePolicy APIsの時系列のサポートを有効にしますAWS マネージドポリシー： AmazonDataZoneFullUserAccess。

のデータ品質の有効化 AWS Glue アセット

Amazon DataZone が からデータ品質メトリクスを取得する AWS Glue は、ビジネスデータカタログの検索など、特定の時点にコンテキストを提供します。データユーザーは、サブスクライブしたアセットのデータ品質メトリクスが時間の経過とともにどのように変化するかを確認できます。データプロデューサーが取り込むことができる AWS スケジュールに基づく Glue データ品質スコア。Amazon DataZone ビジネスデータカタログでは、データ品質 を通じてサードパーティーシステ

ムからのデータ品質メトリクスを表示することもできますAPIs。詳細については、「」を参照してくださいAWS Glue Data Quality と の開始方法 AWS データカタログ の Glue Data Quality。

Amazon DataZone アセットのデータ品質メトリクスは、次の方法で有効にできます。

- データポータルまたは Amazon DataZone APIs を使用して のデータ品質を有効にする AWS 新規作成時または既存の編集時に Amazon DataZone データポータル経由でデータソースを Glue する AWS Glue データソース。

  ポータルを介してデータソースのデータ品質を有効にする方法の詳細については、「」を参照してくださいの Amazon DataZone データソースを作成して実行する AWS Glue Data Catalog。

  > **Note**
  >
  > データポータルを使用して、 のデータ品質のみを有効にすることができます。 AWS Glue インベントリアセット。このリリースの Amazon では、データポータル経由で Amazon Redshift またはカスタムタイプアセットのデータ品質 DataZone を有効にすることはサポートされていません。

  を使用してAPIs、新規または既存のデータソースのデータ品質を有効にすることもできます。これを行うには、 CreateDataSourceまたは を呼び出しUpdateDataSource、`autoImportDataQualityResult`パラメータを「True」に設定します。

  データ品質が有効になったら、オンデマンドまたはスケジュールに従ってデータソースを実行できます。各実行では、アセットごとに最大 100 個のメトリクスを取り込むことができます。データソースを品質に使用するときに、フォームを作成したり、メトリクスを手動で追加したりする必要はありません。アセットが公開されると、データ品質フォームに対して行われた更新 (履歴ルールごとに最大 30 個のデータポイント) がコンシューマーのリストに反映されます。その後、アセットにメトリクスが新しく追加されるたびに、自動的にリストに追加されます。コンシューマーが最新のスコアを利用できるように、アセットを再発行する必要はありません。

カスタムアセットタイプのデータ品質の有効化

Amazon DataZone APIs を使用して、任意のカスタムタイプアセットのデータ品質を有効にできます。詳細については、次を参照してください。

- PostTimeSeriesDataPoints

- ListTimeSeriesDataPoints
- GetTimeSeriesDataPoint
- DeleteTimeSeriesDataPoints

次の手順では、 APIsまたは を使用して Amazon のアセットのサードパーティーメトリクスCLIをインポートする例を示します DataZone。

1. PostTimeSeriesDataPoints API 次のように を呼び出します。

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

次のペイロードを使用します。

```
"domainId": "dzd_5oo7xzoqltu8mf",
    "entityId": "4wyh64k2n8czaf",
    "entityType": "ASSET",
    "form": {
        "content": "{\n  \"evaluations\" : [ {\n    \"types\" : [ \"MaximumLength
\" ],\n    \"description\" : \"ColumnLength \\\"ShippingCountry\\\" <= 6\",\n
   \"details\" : { },\n    \"applicableFields\" : [ \"ShippingCountry\" ],\n
   \"status\" : \"PASS\"\n  }, {\n    \"types\" : [ \"MaximumLength\" ],\n
 \"description\" : \"ColumnLength \\\"ShippingState\\\" <= 2\",\n    \"details
\" : { },\n    \"applicableFields\" : [ \"ShippingState\" ],\n    \"status\" :
 \"PASS\"\n  }, {\n    \"types\" : [ \"MaximumLength\" ],\n    \"description
\" : \"ColumnLength \\\"ShippingCity\\\" <= 8\",\n    \"details\" : { },\n
 \"applicableFields\" : [ \"ShippingCity\" ],\n    \"status\" : \"PASS\"\n  },
 {\n    \"types\" : [ \"Completeness\" ],\n    \"description\" : \"Completeness \
\\"ShippingStreet\\\" >= 0.59\",\n    \"details\" : { },\n    \"applicableFields
\" : [ \"ShippingStreet\" ],\n    \"status\" : \"PASS\"\n  }, {\n    \"types\" :
 [ \"MaximumLength\" ],\n    \"description\" : \"ColumnLength \\\"ShippingStreet\\
\" <= 101\",\n    \"details\" : { },\n    \"applicableFields\" : [ \"ShippingStreet
\" ],\n    \"status\" : \"PASS\"\n  }, {\n    \"types\" : [ \"MaximumLength\" ],\n
    \"description\" : \"ColumnLength \\\"BillingCountry\\\" <= 6\",\n    \"details
\" : { },\n    \"applicableFields\" : [ \"BillingCountry\" ],\n    \"status\" :
 \"PASS\"\n  }, {\n    \"types\" : [ \"Completeness\" ],\n    \"description\" :
 \"Completeness \\\"biLlingcountry\\\" >= 0.5\",\n    \"details\" : {\n
 \"EVALUATION_MESSAGE\" : \"Value: 0.26666666666666666 does not meet the constraint
```

```
 requirement!\"\n    },\n    \"applicableFields\" : [ \"biLlingcountry\" ],\n
    \"status\" : \"FAIL\"\n  }, {\n    \"types\" : [ \"Completeness\" ],\n
 \"description\" : \"Completeness \\\"Billingstreet\\\" >= 0.5\",\n    \"details
\" : { },\n    \"applicableFields\" : [ \"Billingstreet\" ],\n    \"status\" :
 \"PASS\"\n  } ],\n  \"passingPercentage\" : 88.0,\n  \"evaluationsCount\" : 8\n}",
        "formName": "shortschemaruleset",
        "id": "athp9dyw75gzhj",
        "timestamp": 1.71700477757E9,
        "typeIdentifier": "amazon.datazone.DataQualityResultFormType",
        "typeRevision": "8"
    },
    "formName": "shortschemaruleset"
}
```

このペイロードは、 GetFormTypeアクションを呼び出すことで取得できます。

```
aws datazone get-form-type --domain-identifier <your_domain_id> --form-type-
identifier amazon.datazone.DataQualityResultFormType --region <domain_region> --
output text --query 'model.smithy'
```

2. DeleteTimeSeriesDataPoints API 次のように を呼び出します。

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

機械学習と生成 AI の使用

> **Note**
>
> Amazon Bedrock を利用： AWS は、自動不正検出を実装しています。Amazon の説明機能に関する AI の推奨事項 DataZone は Amazon Bedrock 上に構築されているため、ユー

ザーは Amazon Bedrock に実装されているコントロールを継承して、AI の安全性、セキュリティ、責任ある使用を強制します。

Amazon の現在のリリースでは DataZone、AI レコメンデーションを使用してデータ検出とカタログ化を自動化する説明機能を使用できます。Amazon での生成 AI と機械学習のサポートにより、アセットと列の説明 DataZone が作成されます。これらの説明を使用して、データのビジネスコンテキストを追加し、データセットの分析を推奨できます。これにより、データ検出の結果を高めることができます。

Amazon Bedrock の大規模言語モデルを活用した Amazon のデータアセットの説明に関する AI レコメンデーションは、データが理解しやすく、簡単に検出できるようにする DataZone のに役立ちます。AI レコメンデーションでは、データセットに最も関連性の高い分析アプリケーションも提案されています。ドキュメントの手動タスクを減らし、適切なデータ使用量をアドバイスすることで、自動生成された説明は、データの信頼度を高め、貴重なデータを最小限に抑えて、情報に基づいた意思決定を加速させるのに役立ちます。

Important

現在の Amazon DataZone リリースでは、説明機能に関する AI レコメンデーションは以下のリージョンでのみサポートされています。

- 米国東部 (バージニア北部)
- 米国西部 (オレゴン)
- 欧州 (フランクフルト)
- アジアパシフィック (東京)

次の手順では、Amazon で説明の AI レコメンデーションを生成する方法について説明します DataZone。

1. Amazon DataZone データポータル に移動しURL、シングルサインオン (SSO) または を使用してサインインします。 AWS 認証情報。Amazon DataZone 管理者の場合は、https://console.aws.amazon.com/datazone で Amazon DataZone コンソールに移動し、 でサインインします。 AWS アカウント ドメインが作成された場所を選択し、Open data portal を選択します。

2. 上部のナビゲーションペインで、プロジェクトの選択 を選択し、説明の AI レコメンデーションを生成するアセットを含むプロジェクトを選択します。
3. プロジェクトのデータタブに移動します。
4. 左側のナビゲーションペインで、インベントリデータ を選択し、アセットの説明に関する AI レコメンデーションを生成するアセットの名前を選択します。
5. アセットの詳細ページのビジネスメタデータタブで、説明の生成 を選択します。
6. 説明が生成されたら、編集、承認、または拒否できます。データアセットに対して自動的に生成された各メタデータの説明の横に、緑色のアイコンが表示されます。ビジネスメタデータタブで、自動生成された概要 の横にある緑色のアイコンを選択し、編集、承諾、拒否を選択して生成された説明に対処できます。また、ビジネスメタデータタブが選択されているときにページの上部に表示されるすべてのオプションを受け入れるか拒否するかを選択して、自動的に生成されたすべての説明に対して選択したアクションを実行することもできます。

   または、スキーマタブを選択し、一度に 1 つの列の説明の緑色のアイコンを選択し、 の承諾または拒否を選択して、自動的に生成された説明に個別に対処できます。スキーマタブでは、すべて受け入れるかすべて拒否するかを選択して、自動的に生成されたすべての説明に対して選択したアクションを実行することもできます。
7. 生成された説明を使用してアセットをカタログに発行するには、アセットの発行 を選択し、アセットの発行ポップアップウィンドウでアセットを再度選択してこのアクションを確認します。

> **Note**
>
> アセットに対して生成された説明を承諾または拒否せず、このアセットを公開した場合、この未確認の自動生成されたメタデータは公開されたデータアセットに含まれません。

Amazon のデータ系統 DataZone （プレビュー）

> **Important**
>
> 現在、Amazon のデータ系統機能はプレビューリリース DataZone 中です。

Amazon のデータ系統 DataZone は、 APIが OpenLineage有効なシステムから、または を介して系統イベントをキャプチャして視覚化し、データオリジンの追跡APIs、変換の追跡、組織間のデータ使用量の表示を行うのに役立つ、 駆動型の OpenLineage互換性のある機能です。これにより、データアセットを包括的に表示して、アセットのオリジンとその接続チェーンを確認できます。系統データには、カタログ化されたアセット、それらのアセットのサブスクライバー、および を使用してプログラムでキャプチャされたビジネス DataZoneデータカタログ外で発生するアクティビティに関する情報など、Amazon のビジネスデータカタログ内のアクティビティに関する情報が含まれます APIs。

Amazon DataZoneの OpenLineageと互換性のある を使用するとAPIs、ドメイン管理者とデータプロデューサーは、Amazon S3 での変換など DataZone、Amazon で利用できるもの以外の系統イベントをキャプチャして保存できます。 AWS Glue およびその他の サービス。これにより、データコンシューマーがアセットのオリジンを包括的に把握し、アセットのオリジンを信頼できるようになります。一方、データプロデューサーは、その使用状況を理解することで、アセットへの変更の影響を評価できます。さらに、Amazon DataZone バージョンは各イベントに系統付けられており、ユーザーは任意の時点で系統を視覚化したり、アセットまたはジョブの履歴全体の変換を比較したりできます。この過去の系統は、データの進化方法をより深く理解し、トラブルシューティング、監査、データアセットの整合性の確保に不可欠です。

データ系統を使用すると、Amazon で次のことを実行できます DataZone。

- データの出所を理解する: データの出所を知ると、その起源、依存関係、変換を明確に理解できるため、データの信頼が促進されます。この透明性は、信頼できるデータ主導の意思決定に役立ちます。
- データパイプラインへの変更の影響を理解します。データパイプラインに変更が加えられると、系統を使用して、影響を受けるすべてのダウンストリームコンシューマーを特定できます。これにより、重要なデータフローを中断することなく、変更を確実に行うことができます。
- データ品質の問題の根本原因を特定します。ダウンストリームレポートでデータ品質の問題が検出された場合、系統、特に列レベルの系統を使用してデータをトレースし (列レベルで) 、問題を特定してソースに戻すことができます。これにより、データエンジニアは問題を特定して修正できます。
- データガバナンスとコンプライアンスの向上: データガバナンスとプライバシー規制への準拠を示すために、列レベルの系統を使用できます。例えば、列レベルの系統を使用して、機密データ (などPII) の保存場所とダウンストリームアクティビティでの処理方法を表示できます。

Amazon の系統ノードのタイプ DataZone

Amazon では DataZone、データ系統情報はテーブルとビューを表すノードに表示されます。プロジェクトのコンテキストに応じて、例えば、データポータルの左上で選択されたプロジェクトでは、プロデューサーはインベントリアセットと公開アセットの両方を表示できますが、コンシューマーは公開アセットのみを表示できます。アセットの詳細ページで系統タブを初めて開くと、カタログ化されたデータセットノードが系統グラフの系統ノードを上流または下流に移動する開始点になります。

Amazon でサポートされているデータ系統ノードのタイプは次のとおりです DataZone。

- データセットノード - このノードタイプには、特定のデータアセットに関するデータ系統情報が含まれます。
  - に関する情報を含むデータセットノード AWS Amazon DataZone カタログで公開された Glue または Amazon Redshift アセットは自動生成され、対応する が含まれます。 AWS ノード内の Glue または Amazon Redshift アイコン。
  - Amazon DataZone カタログで公開されていないアセットに関する情報を含むデータセットノードは、ドメイン管理者 (プロデューサー) によって手動で作成され、ノード内のデフォルトのカスタムアセットアイコンで表されます。
- ジョブ (実行) ノード - このノードタイプには、特定のジョブの最新の実行や実行の詳細など、ジョブの詳細が表示されます。このノードはジョブの複数の実行もキャプチャし、ノードの詳細の履歴タブで表示できます。ノードアイコンを選択すると、ノードの詳細を表示できます。

系統ノードの主要な属性

系統ノードの `sourceIdentifier` 属性は、データセットで発生するイベントを表します。系統ノード`sourceIdentifier`の は、データセット (テーブル/ビューなど) の識別子です。これは系統ノードでの一意性の適用に使用されます。例えば、同じ を持つ 2 つの系統ノードを持つことはできません`sourceIdentifier`。以下は、さまざまなタイプのノード`sourceIdentifier`の値の例です。

- それぞれのデータセットタイプを持つデータセットノードの場合 :
  - アセット: amazon.datazone.asset/<assetId >
  - 一覧表示 (公開アセット): amazon.datazone.listing/<listingId >
  - AWS Glue テーブル: arn:aws:glue:<region>:<account-id>:table/<database>/<table-name>

  - Amazon Redshift テーブル/ビュー: arn:aws:<redshift/redshift-serverless>:<region>:<account-id>:<table-type(table/view etc)>/<clusterIdentifier/workgroupName>/<database>/<schema>/<table-name>
  - オープン系統実行イベントを使用してインポートされた他のタイプのデータセットノードの場合、入出力データセットの <名前空間>/<名前> がノードsourceIdentifierの として使用されます。
- ジョブの場合：
  - オープン系統実行イベントを使用してインポートされたジョブノードの場合、<jobs_namespace>.<job_name> が として使用されますsourceIdentifier。
- ジョブ実行の場合：
  - オープン系統実行イベントを使用してインポートされたジョブ実行ノードの場合、<jobs_namespace>.<job_name>/<run_id> が として使用されますsourceIdentifier。

を使用して作成されたアセットの場合API、 createAsset を使用して を更新createAssetRevisionAPIし、アセットをアップストリームリソースにマッピングできるようにsourceIdentifierする必要があります。

データ系統の視覚化

Amazon DataZoneのアセット詳細ページでは、データ系統をグラフィカルに表示できるため、アップストリームまたはダウンストリームのデータ関係を簡単に視覚化できます。アセットの詳細ページには、グラフをナビゲートするための以下の機能があります。

- 列レベルの系統: データセットノードで使用可能な場合は、列レベルの系統を拡張します。これにより、ソース列情報が利用可能な場合、アップストリームまたはダウンストリームのデータセットノードとの関係が自動的に表示されます。
- 列検索: 列数のデフォルト表示が 10 の場合。列が 10 を超える場合、ページ分割がアクティブ化され、残りの列に移動します。特定の列をすばやく表示するには、検索された列のみを一覧表示するデータセットノードで検索できます。
- データセットノードのみを表示する: データセット系統ノードのみを表示し、ジョブノードを除外するように切り替える場合は、グラフビューワーの左上にあるオープンビューコントロールアイコンを選択し、データセットノードのみを表示オプションを切り替えることができます。これにより、グラフからすべてのジョブノードが削除され、データセットノードのみをナビゲートできます。ビューのみのデータセットノードがオンになっている場合、グラフをアップストリームまたはダウンストリームに展開することはできません。

- 詳細ペイン: 各系統ノードには詳細がキャプチャされ、選択時に表示されます。
  - データセットノードには、特定のタイムスタンプについてそのノードについてキャプチャされたすべての詳細を表示する詳細ペインがあります。すべてのデータセットノードには、系統情報、スキーマ、履歴タブの 3 つのタブがあります。履歴タブには、そのノードでキャプチャされた系統イベントのさまざまなバージョンが一覧表示されます。からキャプチャされたすべての詳細はAPI、メタデータフォームまたはJSONビューワーを使用して表示されます。
  - ジョブノードには、ジョブの詳細ペインがあり、ジョブ情報、履歴などのタブが表示されます。詳細ペインには、ジョブ実行の一部としてキャプチャされたクエリまたは式もキャプチャされます。履歴タブには、そのジョブでキャプチャされたジョブ実行イベントのさまざまなバージョンが一覧表示されます。からキャプチャされたすべての詳細はAPI、メタデータフォームまたはJSONビューワーを使用して表示されます。
- バージョンタブ: Amazon DataZone データ系統のすべての系統ノードにはバージョニングがあります。すべてのデータセットノードまたはジョブノードについて、バージョンは履歴としてキャプチャされ、さまざまなバージョン間を移動して、時間の経過とともに何が変更されたかを特定できます。各バージョンでは、リネージページに新しいタブが開き、比較やコントラストに役立ちます。

Amazon でのデータ系統認証 DataZone

書き込みアクセス許可 - 系統データを Amazon に発行するには DataZone、 に対する `ALLOW`アクションを含むアクセス許可ポリシーを持つ `PostLineageEvent` IAMロールが必要ですAPI。このIAM認証はAPIゲートウェイレイヤーで行われます。

読み取りアクセス許可 - 2 つのオペレーションがあります。 `ListLineageNodeHistory` `GetLineageNode`と はAmazonDataZoneDomainExecutionRolePolicy管理ポリシーに含まれているため、Amazon DataZone ドメインのすべてのユーザーがこれらを呼び出してデータ系統グラフをトラバースできます。

Amazon でのデータ系統のサンプルエクスペリエンス DataZone

データ系統サンプルエクスペリエンスを使用して、データ系統グラフのアップストリームまたはダウンストリームのトラバース DataZone、バージョンと列レベルのリネージの探索など、Amazon のデータ系統を参照および理解できます。

Amazon でサンプルデータ系統エクスペリエンスを試すには、以下の手順を実行します DataZone。

1. Amazon DataZone データポータルに移動URLし、シングルサインオン (SSO) または を使用してサインインします。 AWS 認証情報。Amazon DataZone 管理者の場合は、https://

console.aws.amazon.com/datazone で Amazon DataZone コンソールに移動し、 でサインインできます。 AWS アカウント ドメインが作成された場所で、Open data portal を選択します。

2. 使用可能なデータアセットを選択して、アセットの詳細ページを開きます。
3. アセットの詳細ページで、系統タブを選択し、プレビュー を選択し、サンプル系統を試す を選択します。
4. データ系統ポップアップウィンドウで、ガイド付きデータ系統ツアーの開始を選択します。

   この時点で、系統情報の全領域を示す全画面表示タブが表示されます。サンプルデータ系統グラフは、最初は、アップストリームとダウンストリームの両端に深さが 1 のベースノードで表示されます。グラフはアップストリームまたはダウンストリームに展開できます。列情報は、系統がノードをどのように流れるかを選択して確認することもできます。

Amazon DataZone データ系統をプログラムで使用する

Amazon でデータ系統機能を使用するには DataZone、次の を呼び出すことができますAPIs。

- GetLineageNode
- ListLineageNodeHistory
- PostLineageEvent

Amazon DataZone データ製品

Amazon DataZone を使用すると、データプロデューサーは、特定のビジネスユースケースに合わせてカスタマイズされたデータ製品と呼ばれる明確に定義された自己完結型のパッケージにデータアセットをグループ化できます。まとまりのあるビジネスに沿ったデータ製品を使用すると、公開プロセスとサブスクリプションプロセスの両方が強化されます。データコンシューマーは、相互接続されたデータアセットを検索して 1 つのユニットとして検索することで、簡単に識別できます。このアプローチにより、すべての関連情報を見つけるために必要な時間と労力が削減され、重要なデータが欠落するリスクが軽減されます。また、データ製品では、統一されたアクセスモデルを実装することで、単一のリクエストでデータへのアクセスを簡素化します。これにより、複数のアクセス許可が不要になり、データ分析の開始が高速化されます。さらに、アセットをデータ製品としてカタログ化することで、データプロデューサーは、メタデータとアクセスコントロールの管理をデータ製品レベルで個別にではなく有効にすることで、管理オーバーヘッドを削減します。さらに、これらの専用に構築されたグループ化されたアセットを消費のために表示できるため、アクセスガバナンスとデータ使用率がより効率的になり、ビジネス目標に合致し、意図した用途で簡単にアクセスできるようになります。データガバナンスチームは、これらのデータ製品の消費率をモニタリングし、データリテラシーの成熟度に関する貴重なインサイトを提供できます。詳細については、「Amazon DataZone の用語と概念」を参照してください。

トピック

- 新しいデータ製品を作成する
- データ製品の公開
- データ製品を編集する
- データ製品の公開解除
- データ製品を削除する
- データ製品をサブスクライブする
- サブスクリプションリクエストを確認し、データ製品にサブスクリプションを付与する
- データ製品を再発行する

新しいデータ製品を作成する

Amazon DataZone を使用すると、データプロデューサーは、特定のビジネスユースケースに合わせてカスタマイズされたデータ製品と呼ばれる明確に定義された自己完結型のパッケージにデータア

セットをグループ化できます。詳細については、「Amazon DataZone の用語と概念」を参照してください。

データポータルへのアクセスに必要な権限を持つ Amazon DataZone ユーザーは、Amazon DataZone データ製品を作成できます。

新しいデータ製品を作成するには、次のステップを実行します。

1. Amazon DataZone データポータルに移動URLし、シングルサインオン (SSO) または を使用してサインインします。 AWS 認証情報。Amazon DataZone 管理者の場合は、https://console.aws.amazon.com/datazone で Amazon DataZone コンソールに移動し、 でサインインできます。 AWS アカウント ドメインが作成された場所で、Open data portal を選択します。
2. Amazon DataZone データポータルで、データ製品を作成するプロジェクトを選択します。
3. データタブを選択し、インベントリデータ を選択し、新しいデータ製品の作成 を選択します。
4. 「新しいデータ製品の作成」ページで、データ製品の名前と説明を指定し、「アセットの選択」を選択して、さまざまなアセットをデータ製品に追加します。「アセットの選択」ポップアップウィンドウで、このデータ製品に追加するアセットを選択し、「 の選択」を選択します。データ製品の作成を完了するには、 の作成 を選択します。

データ製品の公開

Amazon DataZone を使用すると、データプロデューサーは、特定のビジネスユースケースに合わせてカスタマイズされたデータ製品と呼ばれる明確に定義された自己完結型のパッケージにデータアセットをグループ化できます。詳細については、「Amazon DataZone の用語と概念」を参照してください。

データポータルへのアクセスに必要な権限を持つ Amazon DataZone ユーザーは、Amazon DataZone データ製品を公開できます。

データ製品を公開するには、次のステップを実行します。

1. Amazon DataZone データポータルに移動URLし、シングルサインオン (SSO) または を使用してサインインします。 AWS 認証情報。Amazon DataZone 管理者の場合は、https://console.aws.amazon.com/datazone で Amazon DataZone コンソールに移動し、 でサインインできます。 AWS アカウント ドメインが作成された場所で、データポータルを開く を選択します。
2. Amazon DataZone データポータルで、公開するデータ製品があるプロジェクトを選択します。

3. データタブを選択し、インベントリデータ を選択し、データ製品フィルターを選択します。これにより、未公開の既存のデータ製品がすべて表示されます。
4. 発行するデータ製品を選択し、 の発行を選択します。データ製品の発行 を選択して、このデータ製品の発行を確認します。

> **Note**
>
> このデータ製品に含まれる未公開のデータアセットは公開されますが、このデータ製品を通じてのみ利用できます。

データ製品を編集する

Amazon DataZone を使用すると、データプロデューサーは、特定のビジネスユースケースに合わせてカスタマイズされたデータ製品と呼ばれる明確に定義された自己完結型のパッケージにデータアセットをグループ化できます。詳細については、「Amazon DataZone の用語と概念」を参照してください。

データポータルへのアクセスに必要な権限を持つ Amazon DataZone ユーザーは、Amazon DataZone データ製品を編集できます。

データ製品を編集するには、次のステップを実行します。

1. Amazon DataZone データポータルに移動URLし、シングルサインオン (SSO) または を使用してサインインします。 AWS 認証情報。Amazon DataZone 管理者の場合は、https://console.aws.amazon.com/datazone で Amazon DataZone コンソールに移動し、 でサインインできます。 AWS アカウント ドメインが作成された場所で、Open data portal を選択します。
2. Amazon DataZone データポータルで、公開するデータ製品があるプロジェクトを選択します。
3. データタブを選択し、インベントリデータまたは公開データ を選択し、データ製品フィルターを選択します。
4. 編集するデータ製品を選択します。データ製品の編集の一環として、次のことを実行できます。
   - readme の作成 を選択して readme を追加すると、ユーザーはこのページをよりよく理解できます。
   - 用語集用語を追加するには、用語の追加を選択します。 ウィンドウで用語集の用語を選択し、用語の追加 を選択します。

- メタデータフォームの追加 を選択し、メタデータフォームの追加 ウィンドウでフォームを選択し、 の追加 を選択します。
- アクション を展開し、編集 を選択し、データ製品の名前と説明を編集してから、更新 を選択します。

データ製品の公開解除

Amazon DataZone を使用すると、データプロデューサーは、特定のビジネスユースケースに合わせてカスタマイズされたデータ製品と呼ばれる明確に定義された自己完結型のパッケージにデータアセットをグループ化できます。詳細については、「Amazon DataZone の用語と概念」を参照してください。

データポータルへのアクセスに必要な権限を持つ Amazon DataZone ユーザーは、Amazon DataZone データ製品の公開を解除できます。

データ製品の公開を解除するには、次のステップを実行します。

1. Amazon DataZone データポータルに移動URLし、シングルサインオン (SSO) または を使用してサインインします。 AWS 認証情報。Amazon DataZone 管理者の場合は、https://console.aws.amazon.com/datazone で Amazon DataZone コンソールに移動し、 でサインインできます。 AWS アカウント ドメインが作成された場所で、データポータルを開く を選択します。
2. Amazon DataZone データポータルで、公開を解除するデータ製品があるプロジェクトを選択します。
3. データタブを選択し、インベントリデータまたは公開データ を選択し、データ製品フィルターを選択します。これにより、既存のすべてのデータ製品が表示されます。
4. 公開解除するデータ製品を選択し、アクションを展開して の公開解除を選択します。の発行解除を選択して、このデータ製品の発行解除を確認します。

> **Note**
>
> データ製品の公開を解除すると、次の効果があります。
>
> - このデータ製品は、表示またはサブスクライブできなくなります。
> - このデータ製品を通じてのみ利用可能なデータアセットは利用できなくなります。
> - このデータ製品に対するアクティブなサブスクリプションはすべて残ります。

- 個別に公開されたデータアセットは影響を受けません。

データ製品を削除する

Amazon DataZone を使用すると、データプロデューサーは、特定のビジネスユースケースに合わせてカスタマイズされたデータ製品と呼ばれる明確に定義された自己完結型のパッケージにデータアセットをグループ化できます。詳細については、「Amazon DataZone の用語と概念」を参照してください。

データポータルへのアクセスに必要な権限を持つ Amazon DataZone ユーザーは、Amazon DataZone データ製品を削除できます。

データ製品を削除するには、次のステップを実行します。

1. Amazon DataZone データポータルに移動URLし、シングルサインオン (SSO) または を使用してサインインします。 AWS 認証情報。Amazon DataZone 管理者の場合は、https://console.aws.amazon.com/datazone で Amazon DataZone コンソールに移動し、 でサインインできます。 AWS アカウント ドメインが作成された場所で、Open data portal を選択します。
2. Amazon DataZone データポータルで、削除するデータ製品が存在するプロジェクトを選択します。
3. データタブを選択し、インベントリデータ または公開データ を選択し、データ製品フィルターを選択します。これにより、既存のすべてのデータ製品が表示されます。
4. 削除するデータ製品を選択し、アクションを展開して削除を選択します。テキストフィールドに「」と入力し、`delete`「削除」を選択して、このデータ製品の削除を確認します。

> **Note**
>
> データ製品を削除すると、次の効果があります。
>
> - データ製品は、公開、表示、またはサブスクライブできなくなります。
> - このデータ製品でのみ利用可能なデータアセットは、データカタログに表示されなくなります。インベントリアセットから削除されることはありません。

データ製品をサブスクライブする

Amazon DataZone を使用すると、データプロデューサーは、特定のビジネスユースケースに合わせてカスタマイズされたデータ製品と呼ばれる明確に定義された自己完結型のパッケージにデータアセットをグループ化できます。詳細については、「Amazon DataZone の用語と概念」を参照してください。

データポータルへのアクセスに必要な権限を持つ Amazon DataZone ユーザーは、Amazon DataZone データ製品をサブスクライブできます。

データ製品をサブスクライブまたはサブスクライブ解除するには、次のステップを実行します。

1. Amazon DataZone データポータルに移動URLし、シングルサインオン (SSO) または を使用してサインインします。 AWS 認証情報。Amazon DataZone 管理者の場合は、https://console.aws.amazon.com/datazone で Amazon DataZone コンソールに移動し、 でサインインできます。 AWS アカウント ドメインが作成された場所で、Open data portal を選択します。
2. カタログを参照 を選択してサブスクライブするデータ製品を検索し、そのデータ製品を選択します。
3. データ製品の詳細ページで、サブスクライブ を選択します。
4. プロジェクトとサブスクライブの理由を指定し、サブスクライブ を選択します。

サブスクリプションリクエストを確認し、データ製品にサブスクリプションを付与する

Amazon DataZone を使用すると、データプロデューサーは、特定のビジネスユースケースに合わせてカスタマイズされたデータ製品と呼ばれる明確に定義された自己完結型のパッケージにデータアセットをグループ化できます。詳細については、「Amazon DataZone の用語と概念」を参照してください。

データ製品の所有プロジェクトは、Amazon DataZone データ製品へのサブスクリプションを確認して付与できます。

サブスクリプションリクエストを確認し、データ製品にサブスクリプションを付与するには、次のステップを実行します。

1. Amazon DataZone データポータルに移動URLし、シングルサインオン (SSO) または を使用してサインインします。 AWS 認証情報。Amazon DataZone 管理者の場合は、https://

console.aws.amazon.com/datazone で Amazon DataZone コンソールに移動し、 でサインインできます。 AWS アカウント ドメインが作成された場所で、Open data portal を選択します。

2. レビューする受信サブスクリプションリクエストがあるデータ製品を所有するプロジェクトを選択します。
3. データタブを選択し、受信リクエストを選択します。
4. レビューするリクエストを選択し、サブスクリプションリクエストウィンドウで の承認または拒否を選択し、拒否コメントを入力します。

データ製品を再発行する

Amazon DataZone を使用すると、データプロデューサーは、特定のビジネスユースケースに合わせてカスタマイズされたデータ製品と呼ばれる明確に定義された自己完結型のパッケージにデータアセットをグループ化できます。詳細については、「Amazon DataZone の用語と概念」を参照してください。

データポータルへのアクセスに必要な権限を持つ Amazon DataZone ユーザーは、Amazon DataZone データ製品を再発行できます。

データ製品を再発行するには、次のステップを実行します。

1. Amazon DataZone データポータルに移動URLし、シングルサインオン (SSO) または を使用してサインインします。 AWS 認証情報。Amazon DataZone 管理者の場合は、https://console.aws.amazon.com/datazone で Amazon DataZone コンソールに移動し、 でサインインできます。 AWS アカウント ドメインが作成された場所で、データポータルを開く を選択します。
2. Amazon DataZone データポータルで、再公開するデータ製品があるプロジェクトを選択します。
3. データタブを選択し、公開データ を選択し、データ製品フィルターを選択します。
4. 再発行するデータ製品を選択し、アセットタブを選択します。
5. アセット タブで、次のいずれかを実行します。

   - データ製品内の既存のアセットの 1 つを削除するには、そのアセットを選択し、アクションアイコンを展開し、アセットの削除を選択します。アセットの削除ポップアップウィンドウで削除を選択して、アセットの削除を確認します。再発行すると、このアセットはこのデータ製品のすべてのサブスクライバーから削除されます。

- データ製品に追加するアセットを追加するには、追加 ボタンを選択し、データ製品に追加するアセットを 1 つ以上選択します。

6. データ製品の詳細ページで、再発行を選択します。データ製品の再発行ポップアップウィンドウで再発行を選択して、このアクションを確認します。

> **Note**
>
> このデータ製品を再発行すると、すべてのサブスクライバーについて以下が更新されます。
>
> - アセットがデータ製品から削除された場合、サブスクライバーはこれらのアセットにアクセスできなくなります。
> - アセットがデータ製品に追加されている場合、サブスクライバーはこれらのアセットにアクセスできます。
> - データアセットの新しい公開バージョンが利用可能になります。

Amazon DataZone データ検出、サブスクリプション、消費

Amazon では DataZone、アセットがドメインに公開されると、サブスクライバーはこのアセットのサブスクリプションを検出してリクエストできます。サブスクリプションプロセスは、サブスクライバーがカタログを検索して閲覧し、必要なアセットを見つけることから始めます。Amazon DataZone ポータルから、根拠とリクエストの理由を含むサブスクリプションリクエストを送信して、アセットをサブスクライブすることを選択します。公開契約で定義されているサブスクリプション承認者は、アクセスリクエストを確認します。リクエストを承認または拒否できます。

サブスクリプションが付与されると、フルフィルメントプロセスによってサブスクライバーのアセットへのアクセスが容易になります。アセットのアクセスコントロールとフルフィルメントには、主にAmazon DataZoneが管理するアセット用と、Amazon が管理していないアセット用の 2 つのモードがあります DataZone。

- マネージドアセット – Amazon DataZone は、 などのマネージドアセットのフルフィルメントとアクセス許可を管理できます。 AWS Glue テーブルと Amazon Redshift テーブルとビュー。
- アンマネージドアセット – Amazon は、アクション (サブスクリプションリクエストに対する承認など) に関連する標準イベントを Amazon に DataZone 発行します EventBridge。これらの標準イベントを使用して、他の と統合できます。 AWS カスタム統合用の サービスまたはサードパーティーソリューション。

トピック

- カタログでアセットを検索して表示する
- アセットへのサブスクリプションをリクエストする
- サブスクリプションリクエストを承認または拒否する
- 既存のサブスクリプションを取り消す
- サブスクリプションリクエストをキャンセルする
- アセットのサブスクリプションを解除する
- 既存のIAMロールを使用して Amazon DataZone サブスクリプションを満たす
- マネージド へのアクセスを許可する AWS Glue Data Catalog アセット
- マネージド Amazon Redshift アセットへのアクセスを許可する
- 承認済みサブスクリプションのアクセスをアンマネージドアセットに許可する
- Amazon Athena または Amazon Redshift でデータをクエリする

カタログでアセットを検索して表示する

Amazon DataZone は、データを検索する効率的な方法を提供します。データポータルへのアクセス許可を持つ Amazon DataZone ユーザーは、Amazon DataZone カタログ内のアセットを検索し、アセット名とそれらに割り当てられたメタデータを表示できます。アセットの詳細ページを確認することで、アセットを詳しく確認できます。

> **Note**
>
> アセットに含まれる実際のデータを表示するには、まずアセットにサブスクライブし、サブスクリプションリクエストを承認してアクセスを許可する必要があります。

カタログ内のアセットを検索するには

1. Amazon DataZone データポータルに移動URLし、シングルサインオン (SSO) または を使用してサインインします。 AWS 認証情報。Amazon DataZone 管理者の場合は、https://console.aws.amazon.com/datazone で Amazon DataZone コンソールに移動し、 でサインインできます。 AWS アカウント ドメインが作成された場所で、Open data portal を選択します。
2. データポータルのホームページの検索バーに、探しているアセットの名前を入力できます。
3. 名前空間を参照するには、ページの右上から Catalog を選択してカタログを開きます。このカタログでは、、データ所有者、用語集などの条件を検索してアセットを検索できます。
4. 検索ボックスに検索語を入力します。検索を実行した後、さまざまなフィルターを適用して結果を絞り込むことができます。フィルターには、アセットタイプ、ソースアカウント、および が含まれます。 AWS リージョン アセットが属する 。
5. 特定のアセットの詳細を表示するには、アセットを選択して詳細ページを開きます。詳細ページには、次の情報が含まれます。

   - アセット名、データソース (AWS Glue、Amazon Redshift、または Amazon S3)、タイプ (テーブル、ビュー、または S3 オブジェクト) 、列数、およびサイズ。
   - アセットの説明。
   - アセットの現在公開されているリビジョン、所有者、サブスクリプションの承認が必要かどうか、名前空間、および更新履歴。
   - 用語集の用語とメタデータフォームを含む概要タブ。

- ビジネス列名と技術列名、データ型、列のビジネス説明など、アセットのスキーマを表示するスキーマタブ。スキーマタブは、テーブルとビューにのみ表示されます (Amazon S3 オブジェクトには表示されません)。
- ドメインのサブスクライバーのリストを含むサブスクリプションタブ。
- アセットの過去のリビジョンのリストを含む履歴タブ。

アセットへのサブスクリプションをリクエストする

Amazon DataZone では、Amazon DataZone カタログ内のアセットを検索、アクセス、使用できます。アクセスするアセットがカタログにある場合は、そのアセットをサブスクライブする必要があります。これにより、サブスクリプションリクエストが作成されます。その後、承認者はリクエストを承認またはリクエストできます。

そのプロジェクト内のアセットへのサブスクリプションをリクエストするには、プロジェクトのメンバーである必要があります。

アセットをサブスクライブするには

1. Amazon DataZone データポータルに移動URLし、シングルサインオン (SSO) または を使用してサインインします。 AWS 認証情報。Amazon DataZone 管理者の場合は、https://console.aws.amazon.com/datazone で Amazon DataZone コンソールに移動し、 でサインインできます。 AWS アカウント ドメインが作成された場所で、Open data portal を選択します。
2. 検索バーを使用して、サブスクライブするアセットを検索して選択し、サブスクライブ を選択します。
3. サブスクライブポップアップウィンドウで、次の情報を入力します。
   - アセットにサブスクライブするプロジェクト。
   - サブスクリプションリクエストの簡単な根拠。
4. [サブスクライブ] を選択します。

   パブリッシャーがリクエストを承認すると、データポータルに通知が送信されます。

サブスクリプションリクエストのステータスを表示するには、アセットをサブスクライブしたプロジェクトを見つけて選択します。プロジェクトのデータタブに移動し、左側のナビゲーションペインからリクエストされたデータを選択します。このページには、プロジェクトがアクセスをリクエストしたアセットが一覧表示されます。リクエストのステータスでリストをフィルタリングできます。

サブスクリプションリクエストを承認または拒否する

Amazon DataZone では、Amazon DataZone カタログ内のアセットを検索、アクセス、使用できます。アクセスするアセットがカタログにある場合は、アセットをサブスクライブしてサブスクリプションリクエストを作成する必要があります。その後、承認者はリクエストを承認または拒否できます。

サブスクリプションリクエストを承認または拒否するには、所有プロジェクト (アセットを発行したプロジェクト) のメンバーである必要があります。

サブスクリプションリクエストを承認または拒否するには

1. Amazon DataZone データポータルに移動URLし、シングルサインオン (SSO) または を使用してサインインします。 AWS 認証情報。Amazon DataZone 管理者の場合は、https://console.aws.amazon.com/datazone で Amazon DataZone コンソールに移動し、 でサインインできます。 AWS アカウント ドメインが作成された場所で、Open data portal を選択します。
2. データポータルで、プロジェクトリストを参照を選択し、サブスクリプションリクエストを含むアセットを含むプロジェクトを選択します。
3. データタブに移動し、左側のナビゲーションペインから受信リクエストを選択します。
4. リクエストを見つけ、リクエストを表示 を選択します。保留中でフィルタリングすると、まだ開いているリクエストのみを表示できます。
5. サブスクリプションリクエストとアクセスの理由を確認し、承認または拒否するかどうかを決定します。
6. 承認するには、次の 2 つのオプションから選択します。

   - フルアクセス : フルアクセスオプションを使用してサブスクリプションを承認すると、サブスクライバーはデータアセット内のすべての行と列にアクセスできます。
   - 行フィルターと列フィルターで承認 : データの特定の行と列へのアクセスを制限するには、行フィルターと列フィルターで承認するオプションを選択できます。詳細については、「Amazon のデータへのきめ細かなアクセスコントロール DataZone」を参照してください。
     - フィルターの選択 を選択し、ドロップダウンから、サブスクリプションに適用する使用可能なフィルターを 1 つ以上選択します。
     - 新しいフィルターを作成するには、新しいフィルターの作成オプションを選択します。これにより、新しいページが開き、新しい行または列フィルターが作成されます。詳細については、「列フィルターの作成」および「行フィルターの作成」を参照してください。
7. (オプション) リクエストを承諾または拒否する理由を説明するレスポンスを入力します。

8. を承認または拒否を選択します。

プロジェクト所有者は、いつでもサブスクリプションを取り消すことができます。詳細については、「the section called “既存のサブスクリプションを取り消す”」を参照してください。

すべてのサブスクリプションリクエストを表示するには、「」を参照してくださいイベントと通知。

> **Note**
>
> Amazon DataZone が のきめ細かなアクセスコントロールをサポート AWS Glue テーブル、Amazon Redshift テーブル、および Amazon Redshift ビュー。

既存のサブスクリプションを取り消す

Amazon DataZone では、Amazon DataZone カタログ内のアセットを検索、アクセス、使用できます。アクセスするアセットがカタログにある場合は、アセットをサブスクライブしてサブスクリプションリクエストを作成する必要があります。その後、承認者はリクエストを承認またはリクエストできます。承認が間違えられたか、サブスクライバーがアセットにアクセスする必要がなくなったために、承認後にサブスクリプションを取り消す必要がある場合があります。

サブスクリプションを取り消すには、所有プロジェクト (アセットを公開したプロジェクト) のメンバーである必要があります。

サブスクリプションを取り消すには

1. Amazon DataZone データポータルに移動URLし、シングルサインオン (SSO) または を使用してサインインします。 AWS 認証情報。Amazon DataZone 管理者の場合は、https://console.aws.amazon.com/datazone で Amazon DataZone コンソールに移動し、 でサインインできます。 AWS アカウント ドメインが作成された場所で、データポータルを開く を選択します。
2. 上部のナビゲーションペインからプロジェクトの選択を選択し、取り消すサブスクリプションを含むプロジェクトを選択します。
3. データタブに移動し、左側のナビゲーションペインから受信リクエストを選択します。
4. 取り消すサブスクリプションを見つけ、サブスクリプションの表示 を選択します。
5. (オプション) サブスクライバーがプロジェクトのサブスクリプションターゲットにアセットを保持できるようにするには、チェックボックスを有効にします。サブスクリプションターゲットは、サブスクライブされたデータを環境内で利用できる一連のリソースへの参照です。

後でサブスクリプションターゲットからアセットへのアクセスを取り消す場合は、 で取り消します。 AWS Lake Formation.

6. サブスクリプションの取り消し を選択します。

サブスクリプションを取り消した後で再承認することはできません。サブスクライバーは、アセットを承認するためにアセットに再度サブスクライブする必要があります。

サブスクリプションリクエストをキャンセルする

Amazon DataZone では、Amazon DataZone カタログ内のアセットを検索、アクセス、使用できます。アクセスするアセットがカタログにある場合は、アセットをサブスクライブしてサブスクリプションリクエストを作成する必要があります。その後、承認者はリクエストを承認またはリクエストできます。保留中のサブスクリプションリクエストは、誤って送信したか、アセットへの読み取りアクセスが不要になったためにキャンセルする必要がある場合があります。

サブスクリプションリクエストをキャンセルするには、プロジェクト所有者または寄稿者である必要があります。

サブスクリプションリクエストをキャンセルするには

1. Amazon DataZone データポータルに移動URLし、シングルサインオン (SSO) または を使用してサインインします。 AWS 認証情報。Amazon DataZone 管理者の場合は、https://console.aws.amazon.com/datazone で Amazon DataZone コンソールに移動し、 でサインインできます。 AWS アカウント ドメインが作成された場所で、Open data portal を選択します。
2. 上部のナビゲーションペインからプロジェクトの選択を選択し、サブスクリプションリクエストを含むプロジェクトを選択します。
3. プロジェクトのデータタブに移動し、左側のナビゲーションペインからリクエストされたデータを選択します。このページには、プロジェクトがアクセスをリクエストしたアセットが一覧表示されます。
4. リクエストでフィルタリングして、まだ保留中のリクエストのみを表示します。リクエストを見つけ、リクエストを表示 を選択します。
5. サブスクリプションリクエストを確認し、リクエストをキャンセル を選択します。

アセット (または別のアセット) に再サブスクライブする場合は、「」を参照してくださいthe section called “アセットへのサブスクリプションをリクエストする”。

アセットのサブスクリプションを解除する

Amazon DataZone では、Amazon DataZone カタログ内のアセットを検索、アクセス、使用できます。アクセスするアセットがカタログにある場合は、アセットをサブスクライブしてサブスクリプションリクエストを作成する必要があります。その後、承認者はリクエストを承認またはリクエストできます。誤ってサブスクライブして承認されたか、アセットへの読み取りアクセスが不要になったために、アセットのサブスクライブを解除する必要がある場合があります。

アセットのいずれかのサブスクリプションを解除するには、プロジェクトのメンバーである必要があります。

アセットのサブスクリプションを解除するには

1. Amazon DataZone データポータルに移動URLし、シングルサインオン (SSO) または を使用してサインインします。 AWS 認証情報。Amazon DataZone 管理者の場合は、https://console.aws.amazon.com/datazone で Amazon DataZone コンソールに移動し、 でサインインできます。 AWS アカウント ドメインが作成された場所で、Open data portal を選択します。
2. 上部のナビゲーションペインからプロジェクトを選択を選択し、サブスクリプションを解除するアセットを含むプロジェクトを選択します。
3. プロジェクトのデータタブに移動し、左側のナビゲーションペインからリクエストされたデータを選択します。このページには、プロジェクトがアクセスをリクエストしたアセットが一覧表示されます。
4. 承認済みでフィルタリングして、承認済みのリクエストのみを表示します。リクエストを見つけ、サブスクリプションの表示 を選択します。
5. サブスクリプションを確認し、サブスクリプション解除 を選択します。

アセット (または別のアセット) に再サブスクライブする場合は、「」を参照してくださいthe section called “アセットへのサブスクリプションをリクエストする”。

既存のIAMロールを使用して Amazon DataZone サブスクリプションを満たす

現在のリリースでは、Amazon は既存のIAMロールを使用してデータにアクセスすること DataZone をサポートしています。これを実現するには、サブスクリプションを満たすために使用している Amazon DataZone 環境でサブスクリプションターゲットを作成できます。関連付けられている のい

ずれかで環境のサブスクリプションターゲットを作成するには AWS アカウントでは、次のステップを使用できます。

ステップ 1: Amazon DataZone ドメインがポリシーのバージョン 2 以降を使用していることを確認する RAM

1. 「」の「Shared by me: Resource shares」ページに移動します。 AWS RAM コンソール。
2. なぜなら、 AWS RAM リソース共有は特定の に存在します AWS リージョン、該当する を選択します。 AWS コンソールの右上隅にあるドロップダウンリストからのリージョン。
3. Amazon DataZone ドメインに対応するリソース共有を選択し、 の変更を選択します。Amazon DataZone ドメインRAMの共有は、名前 でRAM作成されたドメインの名前または ID を使用して識別できますDataZone-<domain-name>-<domain-id>。
4. Next を選択して次のステップに進み、RAMポリシーのバージョンを確認して変更します。
5. RAM ポリシーのバージョンがバージョン 2 以降であることを確認します。そうでない場合は、ドロップダウンを使用してバージョン 2 以降を選択します。
6. ステップ 4: の確認と更新にスキップを選択します。
7. リソース共有の更新 を選択します。

ステップ 2: 関連付けられたアカウントからサブスクリプションターゲットを作成する

- 現在のリリースでは、Amazon は APIsのみを使用してサブスクリプションターゲットを作成すること DataZone をサポートしています。以下は、 へのサブスクリプションを満たすためのサブスクリプションターゲットの作成に使用できるペイロードの例です。 AWS Glue テーブルと Amazon Redshift テーブルまたはビュー。詳細については、「」を参照してくださいCreateSubscriptionTarget。

  のサブスクリプションターゲットの例 AWS 接着語

```
{
        "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"
}
```

Amazon Redshift のサブスクリプションターゲットの例：

```
{
        "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

- 上記のAPI呼び出し environmentIdentifier で使用する は、API呼び出し元のアカウントと同じ関連アカウントに存在する必要があります。そうしないと、API呼び出しは成功しません。
- authorizedPrincipals DataZone ARN 「」で使用するIAMロールは、サブスクライブされたアセットがサブスクリプションターゲットに追加された後に Amazon がアクセスを許可するロールです。これらの認可されたプリンシパルは、サブスクリプションターゲットが作成される環境と同じアカウントに属している必要があります。
- プロバイダーフィールドの値は、Amazon がサブスクリプションフルフィルメントを完了 DataZone できるようにするには、「Amazon DataZone」である必要があります。

- で指定されたデータベース名は、ターゲットが作成されるアカウントに既に存在している subscriptionTargetConfig 必要があります。Amazon DataZone はこのデータベースを作成しません。また、アクセスロールの管理にこのデータベースに対するアクセスCREATETABLE許可があることを確認してください。
- また、 ロール (IAM の ロール AWS 認証されたプリンシパルとして提供されている Glue と Amazon Redshift のデータベースロール) は、環境アカウントに既に存在します。Amazon Redshift サブスクリプションターゲットの場合、クラスターへの接続中に引き受けるロールには追加の更新が必要です。このロールには、ロールに RedshiftDbRoles タグがアタッチされている必要があります。タグの値はカンマ区切りのリストにすることができます。値は、サブスクリプションターゲットの作成時に承認されたプリンシパルとして提供されたデータベースロールである必要があります。

ステップ 3: 新しいテーブルをサブスクライブし、新しいターゲットへのサブスクリプションを満たす

- サブスクリプションターゲットを作成したら、新しいテーブルをサブスクライブできます。Amazon DataZone はそれを上記のターゲットに実行します。

マネージド へのアクセスを許可する AWS Glue Data Catalog アセット

Amazon では DataZone、アセットへの読み取りアクセスのサブスクリプションリクエストと承認または付与されたサブスクリプションは、サブスクリプション承認者によって管理されます。アセットのサブスクリプション承認者は、このアセットが Amazon DataZone カタログに公開された発行契約によって決定されます。

> **Note**
>
> のアクセス管理 AWS Glue Data Catalog を使用する アセット AWS Lake Formation LF-TBAC メソッドはサポートされていません。
> でのアセットのクロスリージョン共有のサポート AWS Glue Data Catalog はサポートされていません。

マネージドへのサブスクリプションリクエスト AWS Glue Data Catalog アセットが承認されると、Amazon DataZone はこれらのアセットをプロジェクト内のすべての既存のデータレイク環境に自動的に追加します。 DataZone その後、Amazon は承認済み へのアクセスを許可および管理します。 AWS Glue Data Catalog を通じてユーザーに代わって テーブルを使用する AWS Lake Formation。 サブスクライバープロジェクトの場合、付与されたアセットは に表示されます。 AWS Glue Data Catalog を アカウントのリソースとして指定します。その後、Amazon Athena を使用してテーブルをクエリできます。

> **Note**
>
> サブスクライブ後に新しいデータレイク環境がプロジェクトに追加された場合 AWS Glue Data Catalog アセットが既存のデータレイク環境に自動的に追加されました。これらのサブスクライブは手動で追加する必要があります AWS Glue Data Catalog この新しいデータレイク環境への アセット。これを行うには、Amazon DataZone データポータルのプロジェクトの概要ページのデータタブで許可の追加オプションを選択します。

Amazon DataZone が へのアクセスを許可できるようにするには AWS Glue Data Catalog テーブルでは、次の条件を満たす必要があります。

- - AWS Amazon DataZone は Lake Formation のアクセス許可を管理してアクセスを許可するため、 Glue テーブルは Lake Formation で管理されている必要があります。
- の公開に使用されるデータレイク環境のアクセスロールの管理 AWS Glue Data Catalog テーブルには、次の Lake Formation 許可が必要です。
  - `DESCRIBE` に対する および アクセス`DESCRIBE GRANTABLE`許可 AWS 公開されたテーブルを含む Glue データベース。
  - `DESCRIBE`公開されたテーブル自体に対する Lake Formation `SELECT`の `DESCRIBE GRANTABLE`、、、 アクセス`SELECT GRANTABLE`許可。

詳細については、「」の「カタログリソースに対するアクセス許可の付与と取り消し」を参照してください。 AWS Lake Formation デベロッパーガイド 。

マネージド Amazon Redshift アセットへのアクセスを許可する

Amazon では DataZone、アセットへの読み取りアクセスに対するサブスクリプションリクエストと承認または付与されたサブスクリプションは、サブスクリプション承認者によって管理されます。ア

セットのサブスクリプション承認者は、このアセットが Amazon DataZone カタログに公開された発行契約によって決定されます。

Amazon Redshift テーブルまたはビューへのサブスクリプションが承認されると、Amazon DataZone はサブスクライブされたアセットをプロジェクト内のすべてのデータウェアハウス環境に自動的に追加し、プロジェクトのメンバーは環境内の Amazon Redshift クエリエディタリンクを使用してデータをクエリできます。内部では、Amazon はソースとサブスクリプションターゲットの間で必要な権限とデータ共有 DataZoneを作成します。

アクセスを許可するプロセスは、ソースデータベース (パブリッシャー) とターゲットデータベース (サブスクライバー) の場所によって異なります。

- 同じクラスター、同じデータベース - 同じデータベース内でデータを共有する必要がある場合、Amazon はソーステーブルに対して直接アクセス許可 DataZone を付与します。
- 同じクラスター、異なるデータベース - 同じクラスター内の 2 つのデータベース間でデータを共有する必要がある場合、Amazon はターゲットデータベースにビュー DataZone を作成し、作成されたビューにアクセス許可が付与されます。
- 同じアカウント別のクラスター - Amazon DataZone は、ソースクラスターとターゲットクラスター間でデータ共有を作成し、共有テーブルの上にビューを作成します。ビューに対するアクセス許可が付与されます。
- クロスアカウント - 上記と同じですが、プロデューサークラスター側でクロスアカウントデータ共有を許可するには追加のステップが必要であり、コンシューマークラスター側でデータ共有を関連付ける別のステップが必要です。

> **Note**
>
> サブスクライブされた Amazon Redshift アセットが既存のデータウェアハウス環境に自動的に追加された後に新しいデータウェアハウス環境がプロジェクトに追加される場合は、これらのサブスクライブされた Amazon Redshift アセットをこの新しいデータウェアハウス環境に手動で追加する必要があります。これを行うには、Amazon DataZone データポータルのプロジェクトの概要ページのデータタブで許可の追加オプションを選択します。

Amazon Redshift クラスターの公開とサブスクライブが Amazon Redshift データ共有のすべての要件を満たしていることを確認します。詳細については、「Amazon Redshift デベロッパーガイド」を参照してください。

> **Note**
>
> Amazon DataZone は、Amazon Redshift クラスターと Amazon Redshift Serverless アセットの両方へのサブスクリプションの自動付与をサポートしています。
> Amazon Redshift を使用したクロスリージョンデータ共有はサポートされていません。

承認済みサブスクリプションのアクセスをアンマネージドアセットに許可する

Amazon では DataZone、アセットへの読み取りアクセスのサブスクリプションリクエストと承認または付与されたサブスクリプションは、サブスクリプション承認者によって管理されます。アセットのサブスクリプション承認者は、このアセットが Amazon DataZone カタログに公開された発行契約によって決定されます。

Amazon DataZone では、ユーザーはビジネスデータカタログで任意のタイプのアセットを発行できます。これらのアセットの一部について、Amazon はアクセス許可を自動的に管理 DataZone できます。これらのアセットはマネージドアセットと呼ばれ、Lake Formation が管理するアセットが含まれます。 AWS Glue データカタログテーブルと Amazon Redshift テーブルとビュー。Amazon がサブスクリプションを自動的に付与 DataZone できない他のすべてのアセットは、アンマネージド と呼ばれます。

Amazon DataZone は、アンマネージドアセットのアクセス許可を管理するためのパスを提供します。ビジネスデータカタログ内のアセットへのサブスクリプションがデータ所有者によって承認 DataZone されると、Amazon は、ソースとターゲット間のアクセス許可を作成できるペイロード内のすべての必要な情報とともに、アカウントの Amazon EventBridge でイベントを発行します。このイベントを受信すると、イベント内の情報を使用して必要な許可またはアクセス許可を作成できるカスタムハンドラーをトリガーできます。アクセスを許可したら、Amazon でサブスクリプションのステータスをレポートおよび更新 DataZone して、アセットをサブスクライブしたユーザー (複数可) にアセットの消費を開始できることを通知できます。詳細については、「Amazon DataZone イベントと通知」を参照してください。

Amazon Athena または Amazon Redshift でデータをクエリする

Amazon では DataZone、サブスクライバーがカタログ内のアセットにアクセスできると、Amazon Athena または Amazon Redshift クエリエディタ v2 を使用してアセットを消費 (クエリと分析) できます。このタスクを完了するには、プロジェクト所有者または寄稿者である必要があります。プロ

ジェクトで有効になっているブループリントに応じて、Amazon DataZone は、データポータルのプロジェクトページの右側ペインに Amazon Athena または Amazon Redshift クエリエディタ v2 へのリンクを提供します。

1. Amazon DataZone データポータルに移動URLし、シングルサインオン (SSO) または を使用してサインインします。 AWS 認証情報。Amazon DataZone 管理者の場合は、https://console.aws.amazon.com/datazone で Amazon DataZone コンソールに移動し、 でサインインできます。 AWS アカウント ドメインが作成された場所で、データポータルを開く を選択します。
2. Amazon DataZone データポータルで、プロジェクトリストを参照を選択し、分析するデータがあるプロジェクトを検索して選択します。
3. このプロジェクトで Data Lake ブループリントが有効になっている場合、Amazon Athena へのリンクがプロジェクトのホームページの右側パネルに表示されます。

   このプロジェクトでデータウェアハウスの設計図が有効になっている場合、クエリエディタへのリンクがプロジェクトのホームページの右側パネルに表示されます。

   > **Note**
   >
   > ブループリントは、プロジェクトが作成される環境プロファイルで定義されます。

トピック

- Amazon Athena を使用してデータをクエリする
- Amazon Redshift を使用してデータをクエリする

Amazon Athena を使用してデータをクエリする

Amazon Athena リンクを選択して、プロジェクトの認証情報を使用してブラウザの新しいタブで Amazon Athena クエリエディタを開きます。作業している Amazon DataZone プロジェクトは、クエリエディタで現在のワークグループとして自動的に選択されます。

Amazon Athena クエリエディタで、クエリを記述して実行します。一般的なタスクには、次のようなものがあります。

- サブスクライブしたアセットのクエリと分析
- 新しいテーブルを作成する

- 外部 S3 バケットからのクエリ結果 (CTAS) からテーブルを作成する

サブスクライブしたアセットのクエリと分析

プロジェクトがサブスクライブされているアセットへのアクセスが Amazon によって自動的に許可されない場合は DataZone、基盤となるデータへのアクセスを許可する必要があります。これらのアセットへのアクセスを許可する方法の詳細については、「」を参照してください承認済みサブスクリプションのアクセスをアンマネージドアセットに許可する。

プロジェクトがサブスクライブされているアセットへのアクセスが Amazon によって自動的に付与 DataZoneされている場合は、テーブルに対してSQLクエリを実行し、Amazon Athena で結果を確認できます。Amazon Athena SQLでの の使用の詳細については、「SQLAthena のリファレンス」を参照してください。

プロジェクトのホームページの右側パネルで Amazon Athena リンクを選択した後に Amazon Athena クエリエディタに移動すると、Amazon Athena クエリエディタの右上隅にプロジェクトドロップダウンが表示され、プロジェクトコンテキストが自動的に選択されます。

データベースドロップダウンには、次のデータベースが表示されます。

- 公開データベース (*{environmentname}*_pub_db)。このデータベースの目的は、プロジェクトのコンテキスト内で新しいデータを生成し、このデータを Amazon DataZone カタログに公開できる環境を提供することです。プロジェクト所有者と寄稿者は、このデータベースへの読み取りおよび書き込みアクセス権を持っています。プロジェクトビューワーは、このデータベースへの読み取りアクセス権のみを持ちます。
- サブスクリプションデータベース (*{environmentname}*_sub_db)。このデータベースの目的は、Amazon DataZone カタログでプロジェクトメンバーとしてサブスクライブしたデータを共有し、そのデータをクエリできるようにすることです。

新しいテーブルを作成する

外部 S3 バケットに接続している場合は、Amazon Athena を使用して、外部 Amazon S3 バケットのアセットをクエリおよび分析できます。このシナリオでは、Amazon には外部 Amazon S3 バケット内の基盤となるデータに直接アクセスを許可するアクセス許可 DataZone がなく、プロジェクト外で作成された外部 Amazon S3 データは Lake Formation で自動的に管理されず、Amazon によって管理することもできません DataZone。別の方法として、Amazon Athena の CREATE TABLEステートメントを使用して、外部 Amazon S3 バケットからプロジェクトの Amazon S3 バケット内の新しい

テーブルにデータをコピーすることもできます。Amazon Athena でCREATE TABLEクエリを実行するときは、テーブルを に登録します。 Amazon Athena AWS Glue Data Catalog.

以下の例にあるように、Amazon S3 内のデータへのパスを指定するには、LOCATION プロパティを使用します。

```
CREATE EXTERNAL TABLE 'test_table'(
...
)
ROW FORMAT ...
STORED AS INPUTFORMAT ...
OUTPUTFORMAT ...
LOCATION 's3://bucketname/folder/'
```

詳細については、Amazon S3のテーブルの場所」を参照してください。

外部 S3 バケットからのクエリ結果 (CTAS) からテーブルを作成する

アセットをサブスクライブすると、基盤となるデータへのアクセスは読み取り専用になります。Amazon Athena を使用してテーブルのコピーを作成できます。Amazon Athena では、A CREATE TABLE AS SELECT (CTAS)クエリは別のクエリからのSELECTステートメントの結果から Amazon Athena に新しいテーブルを作成します。CTAS 構文の詳細については、CREATETABLE「AS 」を参照してください。

次の例では、テーブルからすべての列をコピーしてテーブルを作成します。

```
CREATE TABLE new_table AS
SELECT *
FROM old_table;
```

同じ例の次のバリエーションで、SELECT ステートメントには WHERE 句も含まれています。この場合、クエリはテーブルから、WHERE 句を満たす行のみを選択します。

```
CREATE TABLE new_table AS
SELECT *
FROM old_table WHERE condition;
```

次の例では、別のテーブルからの列のセットで実行される新しいクエリが作成されます。

```
CREATE TABLE new_table AS
SELECT column_1, column_2, ... column_n
FROM old_table;
```

同じ例のこのバリエーションで、複数のテーブルの特定の列から新しいテーブルを作成します。

```
CREATE TABLE new_table AS
SELECT column_1, column_2, ... column_n
FROM old_table_1, old_table_2, ... old_table_n;
```

これらの新しく作成されたテーブルは、プロジェクトの AWS Glue データベース、および は、データをアセットとして Amazon カタログに公開することで、他のユーザーが検出できるようにしたり、他の Amazon DataZone DataZone プロジェクトと共有したりできます。

Amazon Redshift を使用してデータをクエリする

Amazon DataZone データポータルで、データウェアハウスの設計図を使用する環境を開きます。環境ページの右側のパネルにある Amazon Redshift リンクを選択します。これにより、Amazon Redshift クエリエディタ v2.0 で環境の Amazon Redshift クラスターまたは Amazon Redshift Serverless ワークグループへの接続を確立するのに役立つ、必要な詳細を含む確認ダイアログが開きます。接続を確立するために必要な詳細を特定したら、Amazon Redshift を開くボタンを選択します。これにより、Amazon DataZone 環境の一時的な認証情報を使用して、ブラウザの新しいタブで Amazon Redshift クエリエディタ v2.0 が開きます。

クエリエディタで、環境が Amazon Redshift Serverless ワークグループを使用しているか、Amazon Redshift クラスターを使用しているかに応じて、以下のステップに従います。

Amazon Redshift Serverless ワークグループの場合

1. クエリエディタで、Amazon DataZone 環境の Amazon Redshift Serverless ワークグループを特定し、右クリックして接続の作成を選択します。
2. 認証にフェデレーティッドユーザーを選択します。

3. Amazon DataZone 環境のデータベースの名前を指定します。
4. [Create connection] (接続の作成) を選択します。

Amazon Redshift クラスターの場合：

1. クエリエディタで、Amazon DataZone 環境の Amazon Redshift クラスターを特定し、右クリックして接続の作成を選択します。
2. 認証に IAM ID を使用して一時的な認証情報を選択します。
3. 上記の認証方法が利用できない場合は、左下隅にある歯車ボタンを選択してアカウント設定を開き、IAM認証情報で認証を選択して保存します。これは設定です one-time-only。
4. 接続を作成する Amazon DataZone 環境のデータベースの名前を指定します。
5. [Create connection] (接続の作成) を選択します。

これで、Amazon DataZone 環境用に設定された Amazon Redshift クラスターまたは Amazon Redshift Serverless ワークグループ内のテーブルとビューに対するクエリを開始できます。

サブスクライブしている Amazon Redshift テーブルまたはビューは、環境用に設定された Amazon Redshift クラスターまたは Amazon Redshift Serverless ワークグループにリンクされます。テーブルとビューをサブスクライブしたり、環境のクラスターまたはデータベースに作成した新しいテーブルとビューを公開したりできます。

例えば、環境が というAmazon Redshift クラスター`redshift-cluster-1`と、そのクラスター`dev`内の というデータベースにリンクされているシナリオを考えてみましょう。Amazon DataZone データポータルを使用して、環境に追加されるテーブルとビューをクエリできます。データポータルの右側ペインの `Analytics tools`セクションで、この環境の Amazon Redshift リンクを選択すると、クエリエディタが開きます。その後、`redshift-cluster-1`クラスターを右クリックし、IAMID を使用して一時的な認証情報を使用して接続を作成できます。接続が確立されると、環境が dev データベースでアクセスできるすべてのテーブルとビューが表示されます。

Amazon のデータへのきめ細かなアクセスコントロール DataZone

Amazon の現在のリリースでは DataZone、データのきめ細かなアクセス制御がサポートされているため、機密データをきめ細かく制御できます。Amazon DataZone ビジネスデータカタログに公開されたデータアセット内の特定のデータレコードにアクセスできるプロジェクトを制御できます。Amazon DataZone は、きめ細かなアクセスコントロールを実装するための行フィルターと列フィルターをサポートしています。

行フィルターを使用すると、定義した条件に基づいて特定の行へのアクセスを制限できます。例えば、テーブルに 2 つのリージョン (米国と欧州) のデータが含まれており、欧州の従業員がそのリージョンに関連するデータにのみアクセスできるようにする場合は、そのリージョンが欧州 (リージョン = '欧州' など) の行を含む行フィルターを作成できます。これにより、欧州の従業員は米国のデータにアクセスできなくなります。

列フィルターを使用すると、データアセット内の特定の列へのアクセスを制限できます。例えば、テーブルに個人を特定できる情報 (PII) などの機密情報が含まれている場合、列を除外するPII列フィルターを作成できます。これにより、サブスクライバーは機密性の高いデータにのみアクセスできます。

きめ細かなアクセスコントロールを利用するには、 AWS Amazon の Glue および Amazon Redshift アセット DataZone。データアセットにアクセスするサブスクリプションリクエストを受け取ったら、適切な行と列のフィルターを適用して承認できます。Amazon DataZone は、サブスクライバーがサブスクリプションの承認時に適用したフィルターで許可されている行と列にのみアクセスできるようにします。

トピック

- 行フィルターの作成
- 列フィルターの作成
- 行または列フィルターの削除
- 行または列フィルターの編集
- フィルターを使用したアクセス許可の付与

行フィルターの作成

Amazon DataZone では、サブスクリプションの承認時に使用できる行フィルターを作成して、サブスクライバーが行フィルターで定義されているデータ行にのみアクセスできるようにすることができます。行フィルターを作成するには、以下の手順に従います。

1. Amazon DataZone データポータルに移動URLし、シングルサインオン (SSO) または を使用してサインインします。 AWS 認証情報。Amazon DataZone 管理者の場合は、https://console.aws.amazon.com/datazone で Amazon DataZone コンソールに移動し、 でサインインできます。 AWS アカウント ドメインが作成された場所で、データポータルを開く を選択します。
2. 上部のナビゲーションペインからプロジェクトの選択を選択し、アセットが属するプロジェクトを選択します。
3. プロジェクトのデータタブに移動します。
4. 左側のナビゲーションペインから公開されたデータを選択し、行フィルターを作成するアセットを選択します。Amazon のデータアセット DataZone のタイプが の場合、行フィルターを追加できます。 AWS Glue テーブル、Amazon Redshift テーブル、または Amazon Redshift ビュー。
5. アセットの詳細ページで、アセットフィルタータブに移動し、アセットフィルターの追加 を選択します。
6. 次のフィールドを設定します。
   - 名前 - フィルターの名前
   - 説明 – フィルターの説明
7. フィルタータイプで、行フィルター を選択します。
8. 行フィルター式で、行フィルターに 1 つ以上の式を指定します。
   - ドロップダウンの列から列を選択します。
   - 演算子ドロップダウンから演算子を選択します。
   - 値フィールドに値を入力します。
9. フィルター式に別の条件を追加するには、条件の追加 を選択します。
10. 行フィルター式で複数の条件を使用する場合は、And または Or を選択して条件をリンクします。
11. [フィルターの作成] をクリックします。

サブスクリプションに行フィルターを適用する方法については、サブスクリプションリクエストを承認または拒否する「」を参照してください。

列フィルターの作成

Amazon DataZone では、サブスクリプションの承認時に使用できる列フィルターを作成して、サブスクライバーが列フィルターで定義されているデータ列にのみアクセスできるようにします。列フィルターを作成するには、以下の手順に従います。

1. Amazon DataZone データポータルに移動URLし、シングルサインオン (SSO) または を使用してサインインします。 AWS 認証情報。Amazon DataZone 管理者の場合は、https://console.aws.amazon.com/datazone で Amazon DataZone コンソールに移動し、 でサインインできます。 AWS アカウント ドメインが作成された場所で、データポータルを開く を選択します。
2. 上部のナビゲーションペインからプロジェクトの選択を選択し、アセットが属するプロジェクトを選択します。
3. プロジェクトのデータタブに移動します。
4. 左側のナビゲーションペインから公開されたデータを選択し、列フィルターを作成するアセットを選択します。Amazon のデータアセット DataZone のタイプが の場合、列フィルターを追加できます。 AWS Glue テーブル、Amazon Redshift テーブル、または Amazon Redshift ビュー。
5. アセットの詳細ページで、アセットフィルタータブに移動し、アセットフィルターの追加 を選択します。
6. 次のフィールドを設定します。
   - Name – フィルターの名前
   - 説明 – フィルターの説明
7. フィルタータイプで、列フィルター を選択します。
8. データアセットの列を再度使用するチェックボックスを使用して、フィルターに含める列を選択します。
9. フィルターの作成 を選択します。

列フィルターをサブスクリプションに適用する方法については、サブスクリプションリクエストを承認または拒否する「」を参照してください。

行または列フィルターの削除

行または列フィルターを削除するには、以下の手順に従います。

1. Amazon DataZone データポータルに移動URLし、シングルサインオン (SSO) または を使用してサインインします。 AWS 認証情報。Amazon DataZone 管理者の場合は、https://console.aws.amazon.com/datazone で Amazon DataZone コンソールに移動し、 でサインインできます。 AWS アカウント ドメインが作成された場所で、Open data portal を選択します。
2. プロジェクトのデータタブに移動します。
3. 左側のナビゲーションペインから公開データまたはインベントリデータを選択し、行または列フィルターを削除するアセットを選択します。
4. アセットの詳細ページで、アセットフィルタータブに移動し、削除するフィルターを開きます。
5. アクション 、削除 を選択し、削除を確定します。

> **Note**
>
> フィルターは、アクティブなサブスクリプションで使用されていない場合にのみ削除できます。

行または列フィルターの編集

行または列フィルターを編集するには、以下のステップに従います。

1. Amazon DataZone データポータルに移動URLし、シングルサインオン (SSO) または を使用してサインインします。 AWS 認証情報。Amazon DataZone 管理者の場合は、https://console.aws.amazon.com/datazone で Amazon DataZone コンソールに移動し、 でサインインできます。 AWS アカウント ドメインが作成された場所で、Open data portal を選択します。
2. プロジェクトのデータタブに移動します。
3. 左側のナビゲーションペインから公開データまたはインベントリデータを選択し、行または列フィルターを編集するアセットを選択します。
4. アセットの詳細ページで、アセットフィルタータブに移動し、編集するフィルターを開きます。
5. 次のフィールドを編集できます。

    - 名前 — フィルターの名前

- 説明 – フィルターの説明

6. 行フィルターを編集する場合は、行フィルター式を更新できます。
7. 列フィルターを編集する場合は、フィルターで選択した列を追加または削除できます。
8. 変更を加えたら、アセットフィルターの編集 を選択します。

> **Note**
>
> アクティブなサブスクリプションで使用されているフィルターを編集すると、Amazon DataZone はサブスクライバープロジェクトに付与されたアクセス許可を自動的に更新します。つまり、サブスクライバーは、更新されたフィルターで定義されている行または列にのみアクセスできるため、データアクセスポリシーが一貫して適用されます。

フィルターを使用したアクセス許可の付与

Amazon DataZone は、定義された行と列のフィルターを の適切な許可に変換することで、きめ細かなアクセスコントロールを可能にします。 AWS Lake Formation と Amazon Redshift。以下は、Amazon が両方のフィルターをどのようにマ DataZone テリアライズするかの説明です。 AWS Glue テーブルと Amazon Redshift。

AWS Glue テーブル

へのサブスクリプションの場合 AWS 行フィルターや列フィルターを含む Glue テーブルが承認され、Amazon は で許可を作成してサブスクリプションをマ DataZone テリアライズします。 AWS データセルフィルターを使用した Lake Formation により、サブスクライバープロジェクトのメンバーは、サブスクリプションに適用されたフィルターに基づいてアクセスが許可されている行と列にのみアクセスできるようになります。

Amazon は DataZone 、まず Amazon で適用された行と列のフィルターを に変換 DataZone します。 AWS Lake Formation データセルフィルター。複数の行フィルターと列フィルターが使用されている場合、Amazon はすべての列とすべての行フィルター条件を DataZone 結合して、行レベルと列レベルの両方で有効なアクセス許可を計算します。 DataZone 次に、Amazon は 1 つの AWS 有効な行と列のアクセス許可を使用した Lake Formation データセルフィルター。

データセルフィルターが作成されると、Amazon は で読み取り専用 (SELECT) アクセス許可を作成して、サブスクライバープロジェクトとサブスクライブされたテーブル DataZone を共有します。 AWS このデータセルフィルターを使用する Lake Formation。

Amazon Redshift

行フィルターや列フィルターを含む Amazon Redshift テーブル/ビューへのサブスクリプションが承認されると、Amazon Redshift でスコープダウンされた遅延バインディングビューを作成してサブスクリプションを DataZone マテリアライズします。これにより、サブスクライバープロジェクトのメンバーは、サブスクリプションに適用された行と列フィルターに基づいて、アクセスが許可されている行と列にのみアクセスできます。

Amazon は DataZone まず、Amazon のサブスクリプションに適用された行と列のフィルター DataZone を Amazon Redshift 遅延バインディングビューに変換します。複数の行フィルターと列フィルターが使用されている場合、Amazon はすべての列とすべての行フィルター条件を から DataZone 結合して、行レベルと列レベルの両方で有効なアクセス許可を計算します。 DataZone 次に、Amazon は有効な行と列のアクセス許可を使用して遅延バインディングビューを作成します。

遅延バインディングビューが作成されると、Amazon Redshift で読み取り専用 (SELECT) アクセス許可を作成して、Amazon はこのビューをサブスクライバープロジェクトのメンバー DataZone と共有します。

Amazon DataZone イベントと通知

Amazon DataZone では、サブスクリプションリクエスト、更新、コメント、システムイベントなど、データポータル内の重要なアクティビティについて常に把握できます。Amazon DataZone は、データポータルの専用受信トレイまたは Amazon の EventBridge デフォルトバス経由でメッセージを配信することで、この情報を提供します。

Amazon DataZone データポータルの専用受信トレイ経由のイベント

Amazon DataZone は、メッセージを表示してアクションを実行できる専用の受信トレイをデータポータルに提供します。最近のメッセージは、ホームページ、プロジェクトページ、カタログページにも表示されます。例えば、ユーザーがデータアセットへのアクセスをリクエストし、そのアセットのプロジェクトの所有者と寄稿者を公開すると、データポータルでリクエストが表示され、アクションが実行されると、このリクエストに関連するサブスクライブプロジェクトのプロジェクトメンバーは、データポータルで通知を確認します。メッセージには次の 2 種類があります。

- タスク - これらのメッセージは、どこかでアクションが必要であることを受信者に通知します。追跡に使用できるオプションのステータスフィールドがあります。
- イベント - これらのメッセージは情報であり、割り当てられたステータスはありません。イベントは、最近の更新の監査証跡を提供します。

Amazon では DataZone、次のイベントタイプに対してメッセージが生成されます。

イベントカテゴリ	イベント名	イベントの説明	イベントタイプ
サブスクリプション	サブスクリプションリクエストが作成されました	サブスクリプションリクエストの作成時にイベントが生成されます。	タスク
サブスクリプション	サブスクリプションリクエストが承諾されました	サブスクリプションリクエストが受け入れられるとイベントが生成されます。	イベント

イベントカテゴリ	イベント名	イベントの説明	イベントタイプ
サブスクリプション	サブスクリプションリクエストが拒否されました	サブスクリプションリクエストが拒否されるとイベントが生成されます	イベント
サブスクリプション	サブスクリプションリクエストが削除されました	サブスクリプションリクエストが削除されるとイベントが生成されます。	イベント
プロジェクト	プロジェクトの作成に成功しました	イベントは、プロジェクトの作成が成功したときに生成されます。	イベント
プロジェクトメンバーシップ	プロジェクトメンバーの追加に成功しました	イベントは、新しいメンバーがプロジェクトに追加されると生成されます。	イベント
プロジェクトメンバーシップ	プロジェクトメンバーの削除に成功しました	メンバーがプロジェクトから削除されるとイベントが生成されます。	イベント
プロジェクトメンバーシップ	プロジェクトメンバーロールの変更に成功しました	イベントが生成されます。プロジェクト内のメンバーのロールが変更されます。	イベント
環境	環境のデプロイが開始されました	イベントは、環境デプロイが開始されたときに生成されます。	イベント

イベントカテゴリ	イベント名	イベントの説明	イベントタイプ
環境	環境のデプロイが完了しました	イベントは、環境のデプロイが正常に完了すると生成されます。	イベント
環境	環境のデプロイに失敗しました	環境のデプロイが失敗するとイベントが生成されます。	イベント
環境	環境デプロイカスタムワークフローが開始されました	イベントは、カスタムワークフローを使用する環境が開始されたときに生成されます。	イベント
データアセット	インベントリに追加されたアセット	イベントは、新しいデータアセットがインベントリに追加されると生成されます。つまり、ドラフト状態でカタログに追加されます。	イベント
データアセット	アセットの公開	イベントは、新しいデータアセットが公開されたとき、つまりサブスクリプションに利用できるときに生成されます。	イベント
データアセット	アセットスキーマが変更されました	イベントは、前回の取り込みジョブ以降にアセットスキーマが変更されたときに生成されます。	イベント

イベントカテゴリ	イベント名	イベントの説明	イベントタイプ
登録中	サブスクリプションが作成されました	イベントは、誰かがデータアセットのサブスクライブをリクエストしたときに生成されます。	タスク
登録中	サブスクリプションが承認されました	イベントは、サブスクリプションがパブリッシュしているプロジェクトの所有者または寄稿者によって承認されたときに生成されます。	イベント
登録中	サブスクリプションが拒否されました	イベントは、サブスクリプションがパブリッシュしているプロジェクトの所有者または寄稿者によって拒否されたときに生成されます。	イベント
登録中	サブスクリプションが削除されました	サブスクライバーがサブスクリプションをキャンセルすると、イベントが生成されます。	イベント
登録中	サブスクリプション付与のリクエスト	イベントは、誰かがアセットへのアクセスをリクエストしたときに生成されます。	イベント

イベントカテゴリ	イベント名	イベントの説明	イベントタイプ
登録中	サブスクリプション付与が完了しました	イベントは、サブスクリプションがパブリッシュしているプロジェクトの所有者または寄稿者によってアセットへのアクセスが付与されたときに生成されます。	イベント
登録中	サブスクリプションの付与に失敗しました	サブスクリプション許可が失敗するとイベントが生成されます	イベント
登録中	サブスクリプション付与の取り消しがリクエストされました	イベントは、サブスクリプション付与の取り消しが、パブリッシングプロジェクト所有者または寄稿者によって開始されたときに生成されます。	イベント
登録中	サブスクリプション付与の取り消しが完了しました	サブスクリプション許可の取り消しが完了するとイベントが生成されます。	イベント
登録中	サブスクリプション許可の取り消しに失敗しました	サブスクリプション許可の取り消しが失敗するとイベントが生成されます	イベント

イベントカテゴリ	イベント名	イベントの説明	イベントタイプ
会社名の自動生成	生成されたビジネス名は成功しました	自動ビジネス名生成ジョブが正常に完了すると生成されるイベント	イベント
会社名の自動生成	生成されたビジネス名に失敗しました	イベントは、自動ビジネス名生成ジョブが失敗した場合に生成されます。	イベント
データソースの実行	データソースの作成	イベントは、新しいデータソースの作成時に生成されます。	イベント
データソースの実行	データソースの更新	イベントは、既存のデータソースが更新されると生成されます。	イベント
データソースの実行	データソース実行のトリガー	イベントは、データソースの実行が開始されたときに生成されます。	イベント
データソースの実行	データソースの実行が成功しました	イベントは、データソースの実行が成功したときに生成されます。	イベント
データソースの実行	データソースの実行に失敗しました	イベントは、データソースの実行が失敗すると生成されます。	イベント

データポータルの受信トレイでタスクを表示するには、次のステップを実行します。

1. データポータルを使用して Amazon DataZone データポータルに移動URLし、 SSOまたは を使用してログインします。 AWS 認証情報。Amazon DataZone 管理者の場合は、 の https://console.aws.amazon.com/datazone にある Amazon DataZone コンソールURLにアクセスしてデータポータルを取得できます。 AWS Amazon DataZone ドメインが作成された アカウント。
2. データポータルで、最近の一連のタスクを含むポップアップを表示するには、検索バーの横にあるベルアイコンを選択します。
3. すべて表示 を選択して、すべてのタスクを表示します。イベントタブを選択すると、ビューを変更したり、すべてのイベントを表示したりできます。
4. 検索は、イベント件名、アクティブまたは非アクティブなステータス、または日付範囲でフィルタリングできます。
5. 個々のタスクを選択して、タスクに応答できる場所に移動します。

データポータルの受信トレイでイベントを表示するには、次のステップを実行します。

1. データポータルを使用して Amazon DataZone データポータルに移動URLし、 SSOまたは を使用してログインします。 AWS 認証情報。Amazon DataZone 管理者の場合は、 の https://console.aws.amazon.com/datazone にある Amazon DataZone コンソールURLにアクセスしてデータポータルを取得できます。 AWS Amazon DataZone ルートドメインが作成された アカウント。
2. データポータルで、最近の一連のイベントのポップアップを表示するには、検索バーの横にあるベルアイコンを選択します。
3. すべて表示 を選択して、すべてのイベントを表示します。タスクタブを選択すると、ビューを変更したり、すべてのタスクを表示したりできます。
4. イベント件名または日付範囲で検索をフィルタリングします。
5. 個々のイベントを選択して、そのイベントの詳細を表示できる場所に移動します。

Amazon EventBridge デフォルトバス経由のイベント

データポータルの専用受信トレイにメッセージを送信するだけでなく、 はこれらのメッセージを同じ の Amazon EventBridge デフォルトイベントバス DataZone にも送信します。 AWS Amazon DataZone ルートドメインがホストされている アカウント。これにより、サブスクリプションフルフィルメントや他のツールとのカスタム統合など、イベント駆動型の自動化が可能になります。受信する Amazon EventBridge イベントに一致するルールを作成し、処理のために Amazon EventBridge ターゲットに送信できます。1 つのルールで複数のターゲットにイベントを送信し、それを並行して実行することができます。

イベントの例を次に示します。

```
{
  "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"
        }
      ]
    }
  }
}
```

Amazon でサポートされている詳細タイプの詳細なリスト DataZone は次のとおりです。

- サブスクリプションリクエストが作成されました
- サブスクリプションリクエストが承諾されました
- サブスクリプションリクエストが拒否されました
- サブスクリプションリクエストが削除されました
- サブスクリプション付与のリクエスト
- サブスクリプションの付与が完了しました
- サブスクリプションの付与に失敗しました
- サブスクリプション付与の取り消しがリクエストされました
- サブスクリプション付与の取り消しが完了しました
- サブスクリプション付与の取り消しに失敗しました
- インベントリに追加されたアセット
- カタログに追加されたアセット
- アセットスキーマが変更されました
- データソースステータスの変更
- データソースの作成
- データソースの更新
- データソース実行のトリガー
- データソースの実行が成功しました
- データソースの実行に失敗しました
- ドメイン作成が成功
- ドメインの作成に失敗しました
- ドメインの削除が成功しました
- ドメインの削除に失敗しました
- 環境デプロイが開始されました
- 環境のデプロイが完了しました
- 環境のデプロイに失敗しました
- 環境の削除が開始されました

- 環境の削除が完了しました
- 環境の削除に失敗しました
- プロジェクト作成に成功しました
- プロジェクトメンバーの追加が成功
- プロジェクトメンバーの削除に成功しました
- プロジェクトメンバーロールの変更が成功
- 環境デプロイカスタマーワークフロー開始
- ビジネス名の生成が成功
- ビジネス名の生成に失敗しました

詳細については、「Amazon EventBridge」を参照してください。

Amazon のセキュリティ DataZone

でのクラウドセキュリティ AWS が最優先事項です。として AWS のお客様は、セキュリティを最も重視する組織の要件を満たすように構築されたデータセンターとネットワークアーキテクチャからメリットを得られます。

セキュリティは、 間で共有される責任です。 AWS とユーザー。責任共有モデルでは、これをクラウドのセキュリティおよびクラウド内のセキュリティと説明しています。

- クラウドのセキュリティ – AWS は、 が実行するインフラストラクチャを保護する責任があります。 AWS の サービス AWS クラウド. AWS は、安全に使用できる サービスも提供します。サードパーティーの監査者は、 の一環として当社のセキュリティの有効性を定期的にテストおよび検証します。 AWS コンプライアンスプログラム。Amazon に適用されるコンプライアンスプログラムの詳細については、 DataZone「」を参照してください。 AWS コンプライアンスプログラムによる対象範囲内のサービス。
- クラウド内のセキュリティ — お客様の責任は によって決まります。 AWS 使用する サービス。また、お客様は、データの機密性、会社の要件、適用される法律や規制など、その他の要因についても責任を負います。

このドキュメントは、Amazon の使用時に責任共有モデルを適用する方法を理解するのに役立ちます DataZone。以下のトピックでは、セキュリティおよびコンプライアンスの目的を達成する DataZone ように Amazon を設定する方法について説明します。また、他の の使用方法についても説明します。 AWS Amazon DataZone リソースのモニタリングと保護に役立つ のサービス。

トピック

- Amazon でのデータ保護 DataZone
- Amazon での認可 DataZone
- を使用した Amazon DataZone リソースへのアクセスの制御 IAM
- Amazon のコンプライアンス検証 DataZone
- Amazon のセキュリティのベストプラクティス DataZone
- Amazon の耐障害性 DataZone
- Amazon のインフラストラクチャセキュリティ DataZone
- Amazon でのサービス間の混乱した代理の防止 DataZone
- Amazon の設定と脆弱性の分析 DataZone

- 許可リストに追加するドメイン

Amazon でのデータ保護 DataZone

- AWS 責任共有モデル 、Amazon のデータ保護に適用されます DataZone。このモデルで説明されているように、 AWS は、すべての を実行するグローバルインフラストラクチャを保護する責任があります。 AWS クラウド。 お客様は、このインフラストラクチャでホストされているコンテンツの制御を維持する責任があります。また、 のセキュリティ設定と管理タスクについても責任を負います。 AWS のサービス 使用する 。データプライバシーの詳細については、「データプライバシー FAQ」を参照してください。欧州でのデータ保護の詳細については、「」を参照してください。 AWS の責任共有モデルとGDPRブログ記事 AWS セキュリティブログ 。

データ保護の目的で、 を保護することをお勧めします。 AWS アカウント 認証情報と を使用して個々のユーザーをセットアップする AWS IAM Identity Center または AWS Identity and Access Management （ IAM ）。この方法により、それぞれのジョブを遂行するために必要な権限のみが各ユーザーに付与されます。また、次の方法でデータを保護することもお勧めします:

- 各アカウントで多要素認証 (MFA) を使用します。
- SSL/TLS を使用して と通信する AWS リソースの使用料金を見積もることができます。1TLS.2 が必要で、1.3 TLS をお勧めします。
- で APIとユーザーアクティビティの ログ記録を設定する AWS CloudTrail。 CloudTrail 証跡を使用してキャプチャする方法については、「」を参照してください。 AWS アクティビティ、「」の「証 CloudTrail 跡の使用」を参照してください。 AWS CloudTrail ユーザーガイド 。
- 使用アイテム AWS 暗号化ソリューションと 内のすべてのデフォルトのセキュリティコントロール AWS のサービス.
- Amazon Macie などの高度なマネージドセキュリティサービスを使用します。これらは、Amazon S3 に保存されている機密データの検出と保護を支援します。
- アクセス時に FIPS 140-3 検証済みの暗号化モジュールが必要な場合 AWS コマンドラインインターフェイスまたは を介してAPI、FIPSエンドポイントを使用します。使用可能なFIPSエンドポイントの詳細については、「連邦情報処理標準 (FIPS) 140-3」を参照してください。

お客様の E メールアドレスなどの極秘または機密情報は、タグ、または名前フィールドなどの自由形式のテキストフィールドに配置しないことを強くお勧めします。これは、Amazon DataZone または他の を使用する場合も同様です。 AWS のサービス コンソール、API、 AWS CLI、または AWS SDKs。名前に使用する自由記述のテキストフィールドやタグに入力したデータは、課金や診断ログ

に使用される場合があります。URL を外部サーバーに提供する場合は、そのサーバーへのリクエストを検証URLするために認証情報を に含めないことを強くお勧めします。

データ暗号化

アクセス許可を付与するときは、Amazon DataZone リソースに対するアクセス許可を誰が取得するかを決定します。つまり、該当リソースに対して許可する特定のアクションを有効にするということです。このため、タスクの実行に必要な許可のみを付与する必要があります。最小限の特権アクセスの実装は、セキュリティリスクはもちろん、エラーや悪意ある行動によってもたらされる可能性のある影響を減らす上での基本となります。

保管中の暗号化

Amazon はデフォルトですべてのデータを で DataZone 暗号化します。 AWS Key Management Service (AWS KMS) キー AWS はお客様に代わって を所有および管理します。で管理するキーを使用して、Amazon DataZone カタログに保存されているデータを暗号化することもできます。 AWS KMS.

Amazon でドメインを作成する場合 DataZone、Data Encryption の暗号化設定のカスタマイズ (アドバンスト) の横にあるチェックボックスを選択し、キーを指定することで、暗号化設定を指定できます。 KMS

転送中の暗号化

Amazon DataZone は転送中の暗号化に Transport Layer Security (TLS) とクライアント側の暗号化を使用します。Amazon との通信 DataZone は常に を介して行われるHTTPSため、データは転送中に常に暗号化されます。

ネットワーク間トラフィックのプライバシー

アカウント間の接続を保護するために、Amazon DataZone はサービスロールと IAM ロールを使用してお客様のアカウントに安全に接続し、お客様に代わってオペレーションを実行します。

トピック

- Amazon の保管中のデータ暗号化 DataZone
- Amazon のインターフェイスVPCエンドポイントの使用 DataZone

Amazon の保管中のデータ暗号化 DataZone

保管中のデータをデフォルトで暗号化することで、機密データの保護におけるオーバーヘッドと複雑な作業を減らすのに役立ちます。同時に、セキュリティを重視したアプリケーションを構築して、暗号化のコンプライアンスと規制の厳格な要件を満たすことができます。

Amazon DataZone がデフォルトを使用する AWS保管中のデータを自動的に暗号化するための 所有キー。の使用を表示、管理、または監査することはできません AWS 所有キー。詳細については、「」を参照してくださいAWS 所有キー 。

この暗号化レイヤーを無効にしたり、代替の暗号化タイプを選択したりすることはできませんが、既存の に 2 つ目の暗号化レイヤーを追加できます。 AWS Amazon DataZone ドメインの作成時にカスタマーマネージドキーを選択して、 が所有する暗号化キー。Amazon は、既存の に 2 番目の暗号化レイヤーを追加するために作成、所有、管理できる対称カスタマーマネージドキーの使用 DataZone をサポートしています。 AWS 所有の暗号化。この暗号化レイヤーは完全に制御できるため、このレイヤーでは次のタスクを実行できます。

- キーポリシーの確立と維持
- IAM ポリシーと許可の確立と維持
- キーポリシーの有効化と無効化
- キー暗号化マテリアルのローテーション
- タグを追加する
- キーエイリアスの作成
- 削除のキーをスケジュールする

詳細については、「カスタマーマネージドキー」を参照してください。

> **Note**
>
> Amazon は、 を使用して保管時の暗号化 DataZone を自動的に有効にします。 AWS は、顧客データを無償で保護するための 所有キーです。
> AWS KMS カスタマーマネージドキーの使用には 料金が適用されます。料金の詳細については、「」を参照してください。 AWS Key Management Service の料金

Amazon が で許可 DataZone を使用する方法 AWS KMS

Amazon DataZone では、カスタマーマネージドキーを使用するには 3 つの許可が必要です。カスタマーマネージドキーで暗号化された Amazon DataZone ドメインを作成すると、Amazon DataZone は にCreateGrantリクエストを送信することで、ユーザーに代わって許可とサブ許可を作成します。AWS KMS。の許可 AWS KMS は、アカウントのKMSキー DataZone へのアクセスを Amazon に許可するために使用されます。Amazon は、以下の内部オペレーションでカスタマーマネージドキーを使用する以下の権限 DataZone を作成します。

次のオペレーションで保管中のデータを暗号化するための 1 つの許可。

- へのDescribeKeyリクエストの送信 AWS KMS Amazon DataZone ドメインコレクションの作成時に入力された対称カスタマーマネージドKMSキー ID が有効であることを確認するには、 を使用します。
- GenerateDataKeyrequests に送信 AWS KMS カスタマーマネージドキーで暗号化されたデータキーを生成するには、 を使用します。
- Decrypt リクエストを に送信する AWS KMS は、暗号化されたデータキーを復号して、データの暗号化に使用できます。
- RetireGrant は、ドメインが削除されたときにグラントを廃止します。

データの検索と検出のための 2 つの許可 :

- 権限 2:
  - DescribeKey
  - GenerateDataKey
  - 暗号化、復号、 ReEncrypt
  - CreateGrant の子許可を作成する AWS によって内部的に使用される サービス DataZone。
  - RetireGrant
- 権限 3:
  - GenerateDataKey
  - Decrypt
  - RetireGrant

任意のタイミングで、許可に対するアクセス権を取り消したり、カスタマーマネージドキーに対するサービスからのアクセス権を削除したりできます。これを行うと、Amazon はカスタマーマネージ

ドキーによって暗号化されたデータにアクセスでき DataZone なくなり、そのデータに依存するオペレーションに影響します。例えば、Amazon がアクセス DataZone できないデータアセットの詳細を取得しようとすると、オペレーションは`AccessDeniedException`エラーを返します。

カスタマーマネージドキーを作成する

を使用して、対称カスタマーマネージドキーを作成できます。 AWS マネジメントコンソール、または AWS KMS APIs.

対称カスタマーマネージドキーを作成するには、「」の「対称カスタマーマネージドキーの作成」の手順に従います。 AWS Key Management Service デベロッパーガイド。

キーポリシー - キーポリシーは、カスタマーマネージドキーへのアクセスを制御します。すべてのカスタマーマネージドキーには、キーポリシーが 1 つだけ必要です。このポリシーには、そのキーを使用できるユーザーとその使用方法を決定するステートメントが含まれています。カスタマーマネージドキーを作成する際に、キーポリシーを指定することができます。詳細については、「」の「カスタマーマネージドキーへのアクセスの管理」を参照してください。 AWS Key Management Service デベロッパーガイド。

Amazon DataZone リソースでカスタマーマネージドキーを使用するには、キーポリシーで次のAPIオペレーションを許可する必要があります。

- kms:CreateGrant – は、カスタマーマネージドキーに許可を追加します。指定されたKMSキーへのアクセスを制御する権限を付与します。これにより、Amazon が DataZone 必要とする許可オペレーションへのアクセスを許可します。Grants の使用の詳細については、「」を参照してください。 AWS Key Management Service デベロッパーガイド。
- kms:DescribeKey — Amazon がキー DataZone を検証できるように、カスタマーマネージドキーの詳細を提供します。
- kms:GenerateDataKey – の外部で使用する一意の対称データキーを返します。 AWS KMS.
- kms:Decrypt – KMSキーによって暗号化された暗号文を復号します。

Amazon に追加できるポリシーステートメントの例を次に示します 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**
>
> Amazon DataZone データポータルからアクセスされるリソースには、KMSポリシーの拒否は適用されません。

ポリシー でのアクセス許可の指定の詳細については、「」を参照してください。 AWS Key Management Service デベロッパーガイド。

キーアクセスのトラブルシューティングの詳細については、「」を参照してください。 AWS Key Management Service デベロッパーガイド。

Amazon のカスタマーマネージドキーの指定 DataZone

Amazon DataZone 暗号化コンテキスト

暗号化コンテキストは、データに関する追加のコンテキスト情報が含まれたキーと値のペアのオプションのセットです。

AWS KMS は、追加の認証データとして暗号化コンテキストを使用して、認証された暗号化 をサポートします。データの暗号化リクエストに暗号化コンテキストを含めると、 AWS KMS は、暗号化コンテキストを暗号化されたデータにバインドします。データを復号化するには、そのリクエストに (暗号化時と) 同じ暗号化コンテキストを含めます。

Amazon は次の暗号化コンテキスト DataZone を使用します。

```
"encryptionContextSubset": {
    "aws:datazone:domainId": "{root-domain-uuid}"
```

```
}
```

モニタリングに暗号化コンテキストを使用する - 対称カスタマーマネージドキーを使用して Amazon を暗号化する場合 DataZone、監査レコードとログで暗号化コンテキストを使用して、カスタマーマネージドキーがどのように使用されているかを特定することもできます。暗号化コンテキストは、によって生成されたログにも表示されます。 AWS CloudTrail または Amazon CloudWatch Logs。

暗号化コンテキストを使用してカスタマーマネージドキーへのアクセスを制御する - 対称カスタマーマネージドキーへのアクセスを制御する条件として、キーポリシーおよびIAMポリシーの暗号化コンテキストを使用できます。付与する際に、暗号化コンテキストの制約を使用することもできます。

Amazon DataZone は、権限で暗号化コンテキストの制約を使用して、アカウントまたはリージョンのカスタマーマネージドキーへのアクセスを制御します。権限の制約では、権限によって許可されるオペレーションで指定された暗号化コンテキストを使用する必要があります。

次に、特定の暗号化コンテキストのカスタマーマネージドキーへのアクセスを付与するキーポリシーステートメントの例を示します。このポリシーステートメントの条件では、権限に暗号化コンテキストを指定する暗号化コンテキスト制約が必要です。

```
{
    "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}"
        }
    }
}
```

Amazon の暗号化キーのモニタリング DataZone

を使用する場合 AWS KMS Amazon DataZone リソースで カスタマーマネージドキーを使用すると、 AWS CloudTrail Amazon が DataZone に送信するリクエストを追跡するには AWS KMS。以下の例を示します。 AWS CloudTrail カスタマーマネージドキーによって暗号化されたデータにアクセスDescribeKeyするために Amazon CreateGrant GenerateDataKeyによって呼び出されるKMSオペレーションをモニタリング DataZone するための Decrypt、、、および の イベント。を使用する場合 AWS KMS Amazon DataZone ドメインを暗号化する カスタマーマネージドキー。Amazon DataZone はユーザーに代わって のKMSキーにアクセスするCreateGrantリクエストを送信します。 AWS アカウント。Amazon が DataZone 作成する許可は、 に関連付けられたリソースに固有です。 AWS KMS カスタマーマネージドキー。さらに、Amazon DataZone は、ドメインを削除するときに、 RetireGrantオペレーションを使用してグラントを削除します。以下のイベント例では CreateGrant オペレーションを記録しています。

```
{
    "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"
}
```

暗号化を含む Data Lake 環境の作成 AWS Glue カタログ

の高度なユースケースでは、 AWS 暗号化された Glue カタログでは、カスタマーマネージドKMSキーを使用するには Amazon DataZone サービスへのアクセスを許可する必要があります。これを行うには、カスタムKMSポリシーを更新し、キーにタグを追加します。暗号化された のデータを操作する Amazon DataZone サービスへのアクセスを許可するには AWS Glue カタログで、以下を完了します。

- カスタムKMSキーに次のポリシーを追加します。詳細については、キーポリシーの変更を参照してください。

```
{
  "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*"
    }
  }
}
```

- カスタムKMSキーに次のタグを追加します。詳細については、「タグを使用してKMSキー へのアクセスを制御する」を参照してください。

```
key: AmazonDataZoneEnvironment
value: all
```

Amazon のインターフェイスVPCエンドポイントの使用 DataZone

Amazon Virtual Private Cloud (Amazon VPC) を使用して をホストする場合 AWS リソースでは、Amazon VPCと Amazon 間の接続を確立できます DataZone。この接続は、パブリックインターネットを経由 DataZone せずに Amazon で使用できます。

Amazon VPC では を起動できます AWS カスタム仮想ネットワーク内の リソース。を使用して、IPアドレス範囲、サブネット、ルートテーブル、ネットワークゲートウェイなどのネットワーク設定をVPC制御できます。の詳細についてはVPCs、「Amazon ユーザーガイドVPC」を参照してください。

Amazon VPCを Amazon に接続するには DataZone、まずインターフェイスVPCエンドポイントを定義する必要があります。これにより、 VPCを他の に接続できます。 AWS サービス。エンドポイントは、インターネットゲートウェイ、ネットワークアドレス変換 (NAT) インスタンス、または 接続を必要とせずに、信頼性が高くスケーラブルなVPN接続を提供します。VPC エンドポイントの作成方法の詳細と詳細な手順については、「インターフェイスVPCエンドポイント (AWS PrivateLinkAmazon VPCユーザーガイドの)。

> **Important**
>
> ではVPC、エンドポイントポリシーはリソースベースのポリシーであり、VPCエンドポイントにアタッチして、どのポリシーをコントロールできます。 AWS プリンシパルはエンドポイントを使用して にアクセスできます。 AWS サービス。
> Amazon の現在のリリースでは DataZone、エンドポイントポリシーの使用は、Amazon VPCと Amazon 間の接続の確立と使用ではサポートされていません DataZone。Amazon DataZone アクセス管理は、サービスレベルで定義されたRAM設定ポリシーとIAMプリンシパルポリシーに依存します。

Amazon での認可 DataZone

Amazon DataZoneのインターフェイスは、 内の管理コンソールで構成されます。 AWS およびコンソール外のウェブアプリケーション (データポータル) 。

Amazon DataZone マネジメントコンソールは、 で使用できます。 AWS ドメインの作成と管理を含む top-level-resource APIs、 の 管理者 AWS これらのドメインの アカウントの関連付け、およびアクセス管理を Amazon に委任するデータソース DataZone。Amazon DataZone マネジメントコンソールを使用して、明示的に設定されたアクセス管理コントロールを Amazon DataZone サービスに委任するために必要なすべてのIAMロールと設定を管理できます。 AWS アカウント。Amazon DataZone データポータルはファーストパーティーです AWS SSO ユーザー向けの Identity Center アプリケーション。有効にすると、認証されたIAMプリンシパルが SSO ID を使用する代わりにコンソールを使用してデータポータルにフェデレーションすることもできます。

Amazon DataZoneのデータポータルは、主に によって使用されるように設計されています。 AWS IAM Identity Center で認証されたユーザーは、データへのアクセスを管理し、データの公開、検出、サブスクリプション、分析タスクを実行します。

Amazon DataZone コンソールでの承認

Amazon DataZone コンソール認証モデルはIAM認証を使用します。コンソールは、主に管理者がセットアップに使用します。Amazon がドメイン管理者の概念 DataZone を使用する AWS アカウント、およびメンバー AWS アカウント、およびコンソールは、これらのすべてのアカウントから使用され、 AWS 組織の境界。

Amazon DataZone ポータルでの承認

Amazon DataZone データポータル認証モデルは、管理者とビューワーを含む静的ロールアーキタイプ (プロファイル) ACLを持つ階層型です。例えば、ユーザーは管理者またはユーザーのプロファイルを持つことができます。ドメインのレベルでは、ドメインユーザーがデータ所有者を指定している場合があります。プロジェクトのレベルでは、ユーザーは所有者または寄稿者になることができます。これらのプロファイルは、ユーザーとグループの 2 つのタイプのいずれかとして設定できます。その後、これらのプロファイルはドメインとプロジェクトに関連付けられ、これらのアクセス許可の状態は関連付けテーブルに保存されます。

この承認モデル内では、Amazon DataZone はユーザーがユーザーおよびグループのアクセス許可を管理できるようにします。ユーザーは、プロジェクトメンバーシップの管理、プロジェクトへのメンバーシップのリクエスト、メンバーシップの承認を行います。ユーザーは、データの公開、データサブスクリプション承認者の定義、データのサブスクライブ、サブスクリプションの承認を行います。

ユーザーは、データポータルクライアントが特定のプロジェクトコンテキストにおけるユーザーの有効なプロファイルに基づいて Amazon が DataZone 生成するIAMセッション認証情報をリクエストするときに、特定のプロジェクトでデータ分析を実行します。このセッションは、ユーザーのアクセス

許可と特定のプロジェクトのリソースの両方を対象としています。その後、ユーザーは Athena または Redshift にドロップして関連するデータをクエリし、基盤となるすべてのIAM作業が完全に抽象化されます。

Amazon DataZone プロファイルとロール

ユーザーが認証されると、認証されたコンテキストはユーザープロファイル ID にマッピングされます。このユーザープロファイルには、ユーザーの承認に使用される複数の異なる関連付け (プロジェクト所有者、ドメイン管理者など) を含めることができます。各関連付け (プロジェクト所有者、ドメイン管理者など) には、コンテキストに基づいて特定のアクティビティに対するアクセス許可があります。例えば、ドメイン管理者の関連付けを持つユーザーは、追加のドメインを作成し、他のドメイン管理者をドメインに割り当て、ドメイン内にプロジェクトテンプレートを作成できます。プロジェクト所有者は、プロジェクトのプロジェクトメンバーを追加または削除したり、ドメインとの発行契約を作成したり、アセットをドメインに発行したりできます。

を使用した Amazon DataZone リソースへのアクセスの制御 IAM

必要な AWS Identity and Access Management （ IAM) を使用して、以下のセキュリティ関連のタスクを完了します。

- でユーザーとグループを作成する AWS アカウント.
- の下にある各ユーザーに一意のセキュリティ認証情報を割り当てる AWS アカウント.
- でタスクを実行するための各ユーザーのアクセス許可を制御する AWS リソースの使用料金を見積もることができます。
- 別の のユーザーを許可する AWS アカウント を共有するための AWS リソースの使用料金を見積もることができます。
- のロールを作成する AWS アカウント および は、それらを引き受けることができるユーザーまたはサービスを定義します。
- エンタープライズの既存の ID を使用して、 を使用してタスクを実行するためのアクセス許可を付与する AWS リソース

の詳細についてはIAM、以下を参照してください。

- AWS Identity and Access Management (IAM)
- IAM の使用開始
- IAM ユーザーガイド

以下のセクションでは、ドメイン (ドメインを含む) 、関連するアカウント、プロジェクト、データソースなど、Amazon DataZone とそのコンポーネントをセットアップするために必要なポリシーとアクセス許可について説明します。詳細については、「Amazon DataZone の用語と概念」を参照してください。

内容

- AWS Amazon の マネージドポリシー DataZone
- IAM Amazon の ロール DataZone
- 一時認証情報
- プリンシパル権限

AWS Amazon の マネージドポリシー DataZone

An AWS 管理ポリシーは、 によって作成および管理されるスタンドアロンポリシーです。 AWS. AWS マネージドポリシーは、多くの一般的なユースケースにアクセス許可を付与するように設計されているため、ユーザー、グループ、ロールにアクセス許可の割り当てを開始できます。

次の点に注意してください。 AWS マネージドポリシーは、すべての で利用できるため、特定のユースケースに対して最小特権のアクセス許可を付与しない場合があります。 AWS を使用する のお客様。ユースケース別にカスタマーマネージドポリシーを定義して、マネージドポリシーを絞り込むことをお勧めします。

で定義されているアクセス許可は変更できません AWS マネージドポリシー。If AWS は、 で定義されているアクセス許可を更新します。 AWS 管理ポリシー、更新は、ポリシーがアタッチされているすべてのプリンシパル ID (ユーザー、グループ、ロール) に影響します。 AWS は、 を更新する可能性が最も高いです。 AWS 新しい のときの 管理ポリシー AWS のサービス が起動されるか、既存のサービスで新しいAPIオペレーションが使用可能になります。

詳細については、「」を参照してくださいAWSIAM ユーザーガイドの マネージドポリシー。

内容

- AWS マネージドポリシー：AmazonDataZoneFullAccess
- AWS マネージドポリシー： AmazonDataZoneFullUserAccess
- AWS マネージドポリシー： AmazonDataZoneCustomEnvironmentDeploymentPolicy
- AWS マネージドポリシー：AmazonDataZoneEnvironmentRolePermissionsBoundary
- AWS マネージドポリシー：AmazonDataZoneRedshiftGlueProvisioningPolicy

- AWS マネージドポリシー：AmazonDataZoneGlueManageAccessRolePolicy
- AWS マネージドポリシー：AmazonDataZoneRedshiftManageAccessRolePolicy
- AWS マネージドポリシー：AmazonDataZoneCrossAccountAdmin
- AWS マネージドポリシー：AmazonDataZoneDomainExecutionRolePolicy
- AWS マネージドポリシー：AmazonDataZoneSageMakerProvisioning
- AWS マネージドポリシー：AmazonDataZoneSageMakerAccess
- AWS マネージドポリシー：AmazonDataZoneSageMakerEnvironmentRolePermissionsBoundary
- への Amazon DataZone の更新 AWS 管理ポリシー

AWS マネージドポリシー：AmazonDataZoneFullAccess

IAM ID にAmazonDataZoneFullAccessポリシーをアタッチできます。

このポリシーは、 DataZone 経由で Amazon へのフルアクセスを提供します。 AWS Management Console.

許可の詳細

このポリシーには、以下の許可が含まれています。

- datazone – 経由で Amazon DataZone へのフルアクセスをプリンシパルに付与します AWS Management Console.
- kms — プリンシパルがエイリアスを一覧表示し、キーを記述できるようにします。
- s3 — プリンシパルが Amazon DataZone データを保存するための既存の S3 バケットを選択するか、新しい S3 バケットを作成できるようにします。
- ram — プリンシパルが 間で Amazon DataZone ドメインを共有できるようにします AWS アカウント.
- iam — プリンシパルがロールを一覧表示して渡し、ポリシーを取得できるようにします。
- sso – プリンシパルが のリージョンを取得できるようにします。 AWS IAM Identity Center が有効になっています。
- secretsmanager – プリンシパルが特定のプレフィックスを持つシークレットを作成、タグ付け、および一覧表示できるようにします。

```
{
```

```
    "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",
                "ram:ListResourceSharePermissions"
            ],
            "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": "DataZoneTagOnCreateDomainProjectTags",
            "Effect": "Allow",
            "Action": [
                "secretsmanager:TagResource"
            ],
            "Resource": "arn:aws:secretsmanager:*:*:secret:AmazonDataZone-*",
            "Condition": {
                "ForAllValues:StringEquals": {
                    "aws:TagKeys": [
                        "AmazonDataZoneDomain",
                        "AmazonDataZoneProject"
                    ]
                },
                "StringLike": {
                    "aws:RequestTag/AmazonDataZoneDomain": "dzd_*",
                    "aws:ResourceTag/AmazonDataZoneDomain": "dzd_*"
                }
            }
        },
```

```
        {
            "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_*"
                }
            }
        },
        {
            "Sid": "CreateSecretStatement",
            "Effect": "Allow",
            "Action": [
                "secretsmanager:CreateSecret"
            ],
            "Resource": "arn:aws:secretsmanager:*:*:secret:AmazonDataZone-*",
            "Condition": {
                "StringLike": {
                    "aws:RequestTag/AmazonDataZoneDomain": "dzd_*"
                }
            }
        }
    ]
}
```

ポリシーに関する考慮事項と制限事項

AmazonDataZoneFullAccess ポリシーでカバーされない特定の機能があります。

- 独自の で Amazon DataZone ドメインを作成する場合 AWS KMS key、ドメインの作成を成功させるkms:CreateGrantには に対するアクセス許可が必要です。そのキーkms:GenerateDataKeykms:Decryptが listDataSourcesやAPIsなどの他の Amazon DataZone を呼び出すには に対するアクセス

許可が必要ですcreateDataSource。また、そのキーのリソースポリシーkms:DescribeKeyでkms:CreateGrant、kms:Decrypt、kms:GenerateDataKey、、および に対するアクセス許可も必要です。

デフォルトのサービス所有KMSキーを使用する場合、これは必須ではありません。

詳細については、「」を参照してくださいAWS Key Management Service.

- Amazon DataZone コンソールでロールの作成および更新機能を使用する場合は、管理者権限を持っているか、IAMロールの作成とポリシーの作成/更新に必要なIAMアクセス許可を持っている必要があります。必要なアクセス許可には、iam:CreateRole、iam:CreatePolicy、iam:CreatePolicyVersion、iam:DeletePolicyVおよび アクセスiam:AttachRolePolicy許可が含まれます。
- DataZone を使用して Amazon で新しいドメインを作成する場合 AWS IAM Identity Center ユーザーがログインをアクティブ化した場合、または Amazon の既存のドメインに対してログインをアクティブ化する場合は DataZone、次のアクセス許可が必要です。
  - 組織：DescribeOrganization
  - 組織：ListDelegatedAdministrators
  - sso:CreateInstance
  - sso:ListInstances
  - sso:GetSharedSsoConfiguration
  - sso:PutApplicationGrant
  - sso:PutApplicationAssignmentConfiguration
  - sso:PutApplicationAuthenticationMethod
  - sso:PutApplicationAccessScope
  - sso:CreateApplication
  - sso:DeleteApplication
  - sso:CreateApplicationAssignment
  - sso:DeleteApplicationAssignment
- を受け入れるには AWS Amazon での アカウントの関連付けリクエストには DataZone、 アクセスram:AcceptResourceShareInvitation許可が必要です。

AWS マネージドポリシー： AmazonDataZoneFullUserAccess

このポリシーは Amazon へのフルアクセスを許可しますが DataZone、ドメイン、ユーザー、または関連するアカウントの管理は許可しません。

許可の詳細

```
{
 "Version": "2012-10-17",
 "Statement": [
  {
   "Sid": "AmazonDataZoneUserOperations",
   "Effect": "Allow",
   "Action": [
    "datazone:AcceptPredictions",
    "datazone:AcceptSubscriptionRequest",
    "datazone:AddEntityOwner",
    "datazone:AddPolicyGrant",
    "datazone:CancelMetadataGenerationRun",
    "datazone:CancelSubscription",
    "datazone:CreateAsset",
    "datazone:CreateAssetFilter",
    "datazone:CreateAssetRevision",
    "datazone:CreateAssetType",
    "datazone:CreateDataProduct",
    "datazone:CreateDataProductRevision",
    "datazone:CreateDataSource",
    "datazone:CreateDomainUnit",
    "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:DeleteAssetFilter",
    "datazone:DeleteAssetType",
```

```
    "datazone:DeleteDataProduct",
    "datazone:DeleteDataSource",
    "datazone:DeleteDomainUnit",
    "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:DeleteTimeSeriesDataPoints",
    "datazone:GetAsset",
    "datazone:GetAssetFilter",
    "datazone:GetAssetType",
    "datazone:GetDataProduct",
    "datazone:GetDataSource",
    "datazone:GetDataSourceRun",
    "datazone:GetDomain",
    "datazone:GetDomainUnit",
    "datazone:GetEnvironment",
    "datazone:GetEnvironmentActionLink",
    "datazone:GetEnvironmentBlueprint",
    "datazone:GetEnvironmentCredentials",
    "datazone:GetEnvironmentProfile",
    "datazone:GetFormType",
    "datazone:GetGlossary",
    "datazone:GetGlossaryTerm",
    "datazone:GetGroupProfile",
    "datazone:GetIamPortalLoginUrl",
    "datazone:GetLineageNode",
    "datazone:GetListing",
    "datazone:GetMetadataGenerationRun",
    "datazone:GetProject",
    "datazone:GetSubscription",
    "datazone:GetSubscriptionEligibility",
    "datazone:GetSubscriptionGrant",
    "datazone:GetSubscriptionRequestDetails",
    "datazone:GetSubscriptionTarget",
    "datazone:GetTimeSeriesDataPoint",
```

```
    "datazone:GetUserProfile",
    "datazone:ListAccountEnvironments",
    "datazone:ListAssetFilters",
    "datazone:ListAssetRevisions",
    "datazone:ListDataProductRevisions",
    "datazone:ListDataSourceRunActivities",
    "datazone:ListDataSourceRuns",
    "datazone:ListDataSources",
    "datazone:ListDomainUnitsForParent",
    "datazone:ListEntityOwners",
    "datazone:ListEnvironmentBlueprintConfigurations",
    "datazone:ListEnvironmentBlueprints",
    "datazone:ListEnvironmentProfiles",
    "datazone:ListEnvironments",
    "datazone:ListGroupsForUser",
    "datazone:ListLineageNodeHistory",
    "datazone:ListMetadataGenerationRuns",
    "datazone:ListNotifications",
    "datazone:ListPolicyGrants",
    "datazone:ListProjectMemberships",
    "datazone:ListProjects",
    "datazone:ListSubscriptionGrants",
    "datazone:ListSubscriptionRequests",
    "datazone:ListSubscriptionTargets",
    "datazone:ListSubscriptions",
    "datazone:ListTimeSeriesDataPoints",
    "datazone:ListWarehouseMetadata",
    "datazone:PostTimeSeriesDataPoints",
    "datazone:RejectPredictions",
    "datazone:RejectSubscriptionRequest",
    "datazone:RemoveEntityOwner",
    "datazone:RemovePolicyGrant",
    "datazone:RevokeSubscription",
    "datazone:Search",
    "datazone:SearchGroupProfiles",
    "datazone:SearchListings",
    "datazone:SearchTypes",
    "datazone:SearchUserProfiles",
    "datazone:StartDataSourceRun",
    "datazone:StartMetadataGenerationRun",
    "datazone:UpdateAssetFilter",
    "datazone:UpdateDataSource",
    "datazone:UpdateDomainUnit",
    "datazone:UpdateEnvironment",
```

```
    "datazone:UpdateEnvironmentBlueprint",
    "datazone:UpdateEnvironmentDeploymentStatus",
    "datazone:UpdateEnvironmentProfile",
    "datazone:UpdateGlossary",
    "datazone:UpdateGlossaryTerm",
    "datazone:UpdateProject",
    "datazone:UpdateSubscriptionGrantStatus",
    "datazone:UpdateSubscriptionRequest"
   ],
   "Resource": "*"
  },
  {
   "Sid": "RAMResourceShareOperations",
   "Effect": "Allow",
   "Action": "ram:GetResourceShareAssociations",
   "Resource": "*"
  }
 ]
}
```

AWS マネージドポリシー： AmazonDataZoneCustomEnvironmentDeploymentPolicy

このポリシーを使用して、カスタムブループリントを使用して作成された環境の設定を更新できます。このポリシーは、Amazon DataZone サブスクリプションターゲットとデータソースの作成にも使用できます。

許可の詳細

```
{
 "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 マネージドポリシー：AmazonDataZoneEnvironmentRolePermissionsBoundary

> **Note**
>
> このポリシーはアクセス許可の境界です。アクセス許可の境界は、アイデンティティベースのポリシーがIAMエンティティに付与できるアクセス許可の上限を設定します。Amazon アクセス DataZone 許可の境界ポリシーを自分で使用してアタッチしないでください。Amazon DataZone アクセス許可の境界ポリシーは、Amazon DataZone マネージドロールにのみアタッチする必要があります。アクセス許可の境界の詳細については、「 IAMユーザーガイド」の「 IAMエンティティのアクセス許可の境界」を参照してください。

Amazon DataZone データポータルを介して環境を作成すると、Amazon はこのアクセス許可の境界をIAM環境の作成時に生成されるロール DataZone に適用します。アクセス許可の境界は、Amazon が DataZone 作成するロールの範囲と、追加するロールを制限します。

Amazon DataZone は `AmazonDataZoneEnvironmentRolePermissionsBoundary`マネージドポリシーを使用して、アタッチされているプロビジョニングされたIAMプリンシパルを制限します。プリンシパルは、Amazon が DataZone インタラクティブなエンタープライズユーザーまたは分析サービス (AWS Glueなど) の後に、Amazon S3 からの読み取りと書き込みや実行などのデータを処理するためのアクションを実行します。 AWS Glue クローラー.

この`AmazonDataZoneEnvironmentRolePermissionsBoundary`ポリシーは、Amazon の読み取りおよび書き込みアクセス DataZone を などのサービスに付与します。 AWS Glue、Amazon S3、AWS Lake Formation、Amazon Redshift、および Amazon Athena 。このポリシーは、ネットワークインターフェイスや などのこれらのサービスを使用するために必要な一部のインフラストラクチャリソースに対する読み取りおよび書き込みアクセス許可も付与します。 AWS KMS キー。

Amazon が DataZone を適用 AmazonDataZoneEnvironmentRolePermissionsBoundary AWS すべての Amazon DataZone 環境ロール (所有者と寄稿者) のアクセス許可の境界としての マネージドポリシー。このアクセス許可の境界により、環境に必要なリソースとアクションへのアクセスのみを許可するように、これらのロールが制限されます。

境界には、次のJSONステートメントが含まれます。

```
{
  "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 マネージドポリシー：AmazonDataZoneRedshiftGlueProvisioningPolicy

- AmazonDataZoneRedshiftGlueProvisioningPolicy ポリシー DataZone は、 との相互運用に必要なアクセス許可を Amazon に付与します。 AWS Glue と 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 マネージドポリシー：AmazonDataZoneGlueManageAccessRolePolicy

このポリシーは、Amazon に を発行する DataZone アクセス許可を付与します。 AWS データをカタログに Glue します。また、 へのアクセスを許可または取り消すための Amazon アクセス DataZone 許可も付与します。 AWS Glue がカタログに公開したアセット。

```
{
 "Version": "2012-10-17",
 "Statement": [
  {
   "Sid": "GlueTagDatabasePermissions",
   "Effect": "Allow",
   "Action": [
    "glue:TagResource",
    "glue:UntagResource",
    "glue:GetTags"
   ],
   "Resource": "*",
   "Condition": {
    "StringEquals": {
     "aws:ResourceAccount": "${aws:PrincipalAccount}"
    },
    "ForAnyValue:StringLikeIfExists": {
     "aws:TagKeys": "DataZoneDiscoverable_*"
    }
   }
  },
  {
   "Sid": "GlueDataQualityPermissions",
   "Effect": "Allow",
   "Action": [
    "glue:ListDataQualityResults",
    "glue:GetDataQualityResult"
   ],
   "Resource": "arn:aws:glue:*:*:dataQualityRuleset/*",
   "Condition": {
    "StringEquals": {
     "aws:ResourceAccount": "${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:CreateDataCellsFilter",
     "lakeformation:CreateLakeFormationOptIn",
     "lakeformation:DeleteDataCellsFilter",
     "lakeformation:DeleteLakeFormationOptIn",
     "lakeformation:GrantPermissions",
     "lakeformation:GetDataCellsFilter",
     "lakeformation:GetResourceLFTags",
     "lakeformation:ListDataCellsFilter",
     "lakeformation:ListLakeFormationOptIns",
     "lakeformation:ListPermissions",
     "lakeformation:RegisterResource",
     "lakeformation:RevokePermissions",
     "lakeformation:UpdateDataCellsFilter",
     "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 マネージドポリシー：AmazonDataZoneRedshiftManageAccessRolePolicy

このポリシーは、Amazon Redshift データをカタログに発行するアクセス DataZone 許可を Amazon に付与します。また、カタログ内の Amazon Redshift または Amazon Redshift Serverless が公開したアセットへのアクセスを許可または取り消すアクセス DataZone 許可も Amazon に付与します。

```
{
 "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 マネージドポリシー：AmazonDataZoneCrossAccountAdmin

IAM ID に AmazonDataZoneCrossAccountAdmin ポリシーをアタッチできます。

このポリシーにより、ユーザーは Amazon DataZone 関連のアカウントを操作できます。

```
{
    "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 マネージドポリシー：AmazonDataZoneDomainExecutionRolePolicy

これは Amazon DataZone `DomainExecutionRole` サービスロールのデフォルトポリシーです。このロールは、Amazon DataZone ドメイン内のデータをカタログ化、検出、管理、共有、分析 DataZone するために Amazon によって使用されます。このロールは、データポータルの使用に必要なすべての Amazon DataZone APIs へのアクセスと、Amazon DataZone ドメイン内の関連アカウントの使用をサポートするRAMアクセス許可を提供します。

AmazonDataZoneDomainExecutionRolePolicy ポリシーを にアタッチできます`AmazonDataZoneDomainExecutionRole`。

```
{
 "Version": "2012-10-17",
 "Statement": [
  {
   "Sid": "DomainExecutionRoleStatement",
   "Effect": "Allow",
   "Action": [
    "datazone:AcceptPredictions",
    "datazone:AcceptSubscriptionRequest",
    "datazone:AddEntityOwner",
```

```
    "datazone:AddPolicyGrant",
    "datazone:CancelMetadataGenerationRun",
    "datazone:CancelSubscription",
    "datazone:CreateAsset",
    "datazone:CreateAssetFilter",
    "datazone:CreateAssetRevision",
    "datazone:CreateAssetType",
    "datazone:CreateDataProduct",
    "datazone:CreateDataProductRevision",
    "datazone:CreateDataSource",
    "datazone:CreateDomainUnit",
    "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:DeleteAssetFilter",
    "datazone:DeleteAssetType",
    "datazone:DeleteDataProduct",
    "datazone:DeleteDataSource",
    "datazone:DeleteDomainUnit",
    "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:DeleteTimeSeriesDataPoints",
    "datazone:GetAsset",
    "datazone:GetAssetFilter",
    "datazone:GetAssetType",
```

```
    "datazone:GetDataProduct",
    "datazone:GetDataSource",
    "datazone:GetDataSourceRun",
    "datazone:GetDomain",
    "datazone:GetDomainUnit",
    "datazone:GetEnvironment",
    "datazone:GetEnvironmentAction",
    "datazone:GetEnvironmentActionLink",
    "datazone:GetEnvironmentBlueprint",
    "datazone:GetEnvironmentCredentials",
    "datazone:GetEnvironmentProfile",
    "datazone:GetFormType",
    "datazone:GetGlossary",
    "datazone:GetGlossaryTerm",
    "datazone:GetGroupProfile",
    "datazone:GetLineageNode",
    "datazone:GetListing",
    "datazone:GetMetadataGenerationRun",
    "datazone:GetProject",
    "datazone:GetSubscription",
    "datazone:GetSubscriptionEligibility",
    "datazone:GetSubscriptionGrant",
    "datazone:GetSubscriptionRequestDetails",
    "datazone:GetSubscriptionTarget",
    "datazone:GetTimeSeriesDataPoint",
    "datazone:GetUserProfile",
    "datazone:ListAccountEnvironments",
    "datazone:ListAssetFilters",
    "datazone:ListAssetRevisions",
    "datazone:ListDataProductRevisions",
    "datazone:ListDataSourceRunActivities",
    "datazone:ListDataSourceRuns",
    "datazone:ListDataSources",
    "datazone:ListDomainUnitsForParent",
    "datazone:ListEntityOwners",
    "datazone:ListEnvironmentActions",
    "datazone:ListEnvironmentBlueprintConfigurationSummaries",
    "datazone:ListEnvironmentBlueprintConfigurations",
    "datazone:ListEnvironmentBlueprints",
    "datazone:ListEnvironmentProfiles",
    "datazone:ListEnvironments",
    "datazone:ListGroupsForUser",
    "datazone:ListLineageNodeHistory",
    "datazone:ListMetadataGenerationRuns",
```

```
    "datazone:ListNotifications",
    "datazone:ListPolicyGrants",
    "datazone:ListProjectMemberships",
    "datazone:ListProjects",
    "datazone:ListSubscriptionGrants",
    "datazone:ListSubscriptionRequests",
    "datazone:ListSubscriptionTargets",
    "datazone:ListSubscriptions",
    "datazone:ListTimeSeriesDataPoints",
    "datazone:ListWarehouseMetadata",
    "datazone:RejectPredictions",
    "datazone:RejectSubscriptionRequest",
    "datazone:RemoveEntityOwner",
    "datazone:RemovePolicyGrant",
    "datazone:RevokeSubscription",
    "datazone:Search",
    "datazone:SearchGroupProfiles",
    "datazone:SearchListings",
    "datazone:SearchTypes",
    "datazone:SearchUserProfiles",
    "datazone:StartDataSourceRun",
    "datazone:StartMetadataGenerationRun",
    "datazone:UpdateAssetFilter",
    "datazone:UpdateDataSource",
    "datazone:UpdateDomainUnit",
    "datazone:UpdateEnvironment",
    "datazone:UpdateEnvironmentBlueprint",
    "datazone:UpdateEnvironmentDeploymentStatus",
    "datazone:UpdateEnvironmentProfile",
    "datazone:UpdateGlossary",
    "datazone:UpdateGlossaryTerm",
    "datazone:UpdateProject",
    "datazone:UpdateSubscriptionGrantStatus",
    "datazone:UpdateSubscriptionRequest"
   ],
   "Resource": "*"
  },
  {
   "Sid": "RAMResourceShareStatement",
   "Effect": "Allow",
   "Action": "ram:GetResourceShareAssociations",
   "Resource": "*"
  }
 ]
```

```
}
```

AWS マネージドポリシー：AmazonDataZoneSageMakerProvisioning

この AmazonDataZoneSageMakerProvisioning ポリシー DataZone は、Amazon と相互運用するために必要なアクセス許可を Amazon に付与します 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 マネージドポリシー：AmazonDataZoneSageMakerAccess

このポリシーは、Amazon SageMaker アセットをカタログに発行するアクセス DataZone 許可を Amazon に付与します。また、カタログ内の Amazon が SageMaker 公開したアセットへのアクセスを許可または取り消すアクセス DataZone 許可も Amazon に付与します。

このポリシーには以下を実行するための許可が含まれています。

- cloudtrail – CloudTrail 証跡に関する情報を取得します。
- cloudwatch – 現在の CloudWatch アラームを取得します。
- logs – CloudWatch ログのメトリクスフィルターを取得します。
- sns – SNSトピックへのサブスクリプションのリストを取得します。
- config – 設定レコーダー、リソース、および に関する情報を取得します。 AWS Config ルール。また、サービスにリンクされたロールが を作成および削除できるようにします。 AWS ルールと を設定して、ルールに対して評価を実行します。
- iam – アカウントの認証情報レポートを取得して生成します。
- organization – 組織のアカウントと組織単位 (OU) 情報を取得します。
- securityhub – Security Hub サービス、標準、コントロールの設定方法に関する情報を取得します。
- tag – リソースタグに関する情報を取得します。

```
{
 "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 マネージドポリシー：AmazonDataZoneSageMakerEnvironmentRolePermissionsBoundary

> **Note**
>
> このポリシーはアクセス許可の境界です。アクセス許可の境界は、アイデンティティベースのポリシーがIAMエンティティに付与できるアクセス許可の上限を設定します。Amazon アクセス DataZone 許可の境界ポリシーを自分で使用してアタッチしないでください。Amazon DataZone アクセス許可の境界ポリシーは、Amazon DataZone マネージドロールにのみアタッチする必要があります。アクセス許可の境界の詳細については、「 IAMユーザーガイド」のIAM「エンティティのアクセス許可の境界」を参照してください。

Amazon SageMaker DataZone データポータルを介して Amazon 環境を作成すると、Amazon はこのアクセス許可の境界を環境の作成中に生成されるIAMロール DataZone に適用します。アクセス許可の境界は、Amazon が DataZone 作成するロールの範囲と、追加するロールを制限します。

Amazon DataZone は、`AmazonDataZoneSageMakerEnvironmentRolePermissionsBoundary`マネージドポリシーを使用して、アタッチされているプロビジョニングされたIAMプリンシパルを制限します。プリンシパルは、Amazon が DataZone インタラクティブなエンタープライズユーザーまたは分析サービス (AWS SageMakerなど) から、Amazon S3 または Amazon Redshift からの読み取りと書き込み、実行などのデータを処理するためのアクションを実行します。 AWS Glue クローラー。

この`AmazonDataZoneSageMakerEnvironmentRolePermissionsBoundary`ポリシーは、Amazon の読み取りおよび書き込みアクセス DataZone を Amazon SageMaker、 などのサービスに付与します。 AWS Glue、Amazon S3、 AWS Lake Formation、Amazon Redshift、および Amazon Athena このポリシーは、ネットワークインターフェイス、Amazon ECRリポジトリ、 などのこれらのサービスを使用するために必要な一部のインフラストラクチャリソースに対する読み取りおよび書き込みアクセス許可も付与します。 AWS KMS キー。また、Amazon SageMaker Canvas などの Amazon SageMaker アプリケーションへのアクセスも許可します。

Amazon は、すべての Amazon DataZone 環境ロール (所有者と寄稿者) のアクセス許可の境界として `AmazonDataZoneSageMakerEnvironmentRolePermissionsBoundary`マネージドポリシー DataZone を適用します。このアクセス許可の境界により、環境に必要なリソースとアクションへのアクセスのみを許可するように、これらのロールが制限されます。

```
        {
```

```
"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": "*"
  }
 ]
```

```
}
```

への Amazon DataZone の更新 AWS 管理ポリシー

の更新に関する詳細を表示する AWS Amazon の マネージドポリシーは、このサービスがこれらの変更の追跡を開始 DataZone してからです。このページの変更に関する自動通知については、Amazon DataZone ドキュメント履歴ページのRSSフィードにサブスクライブしてください。

変更	説明	日付
AmazonDataZoneDomainExecutionRolePolicy および AmazonDataZoneFullUserAccess - ポリシーの更新	AmazonDataZoneDomainExecutionRolePolicy およびのポリシーの更新 AmazonDataZoneFullUserAccess- Amazon DataZone ドメインユニットとデータ製品の作成と管理APIsに使用される新しいのサポートを有効にします。	2024 年 7 月 31 日
AmazonDataZoneGlueManageAccessRolePolicy - ポリシーの更新	ポリシーの更新 AmazonDataZoneGlueManageAccessRolePolicy - Amazon DataZone は、Lake FormationでのIAM許可付与の範囲を絞り込むために、きめ細かなアクセスコントロール機能に使用される許可を追加しています。	2024 年 7 月 2 日
AmazonDataZoneExecutionRolePolicy および AmazonDataZoneFullUserAccess - ポリシーの更新	データ系統AmazonDataZoneExecutionRolePolicy ときめ細かなアクセスコントロール のサポートを有効にするAmazonDataZoneFull	2024 年 6 月 27 日

変更	説明	日付
	UserAccessために、 と のポリシーを更新しましたAPIs。	
AmazonDataZoneGlueManageAccessRolePolicy - ポリシーの更新	Amazon のセルフサブスクライブ機能に必要なIAMアクセス許可AmazonDataZoneGlueManageAccessRolePolicyを追加して、レイクフォーメーションで付与されるアクセス許可の範囲を絞り込む DataZone ポリシーを に更新しました。セルフサブスクライブ機能を使用すると、レイクフォーメーション許可はタグ付けされたリソースにのみ付与できます。	2024 年 6 月 14 日
AmazonDataZoneDomainExecutionRolePolicy - ポリシーの更新	ポリシーを に更新AmazonDataZoneDomainExecutionRolePolicy しAPIs、ユーザーが Amazon DataZone 環境のアクションを設定 DataZone できるようにする新しい を Amazon に追加しました。	2024 年 6 月 14 日

変更	説明	日付
AmazonDataZoneFullAccess - ポリシーの更新	Amazon DataZone マネジメントコンソールAmazonDataZoneFullAccessがユーザーに代わってドメインタグとプロジェクトタグの両方を使用してシークレットを作成できるようにする へのポリシーの更新。また、ドメイン所有者アカウントから管理を有効にして、関連付けられたアカウントのアカウント関連付けステータスを表示できるようにするram:ListResourceSharePermissions アクションも含まれます。	2024 年 6 月 14 日
AmazonDataZoneSageMakerEnvironmentRolePermissionsBoundary - 新しいアクセス許可の境界	という新しいアクセス許可の境界AmazonDataZoneSageMakerEnvironmentRolePermissionsBoundary 。Amazon DataZone データポータルを介して Amazon SageMaker 環境を作成すると、Amazon はこのアクセス許可の境界を環境の作成中に生成されるIAMロール DataZone に適用します。アクセス許可の境界は、Amazon が DataZone 作成するロールの範囲と、追加するロールを制限します。	2024 年 4 月 30 日

変更	説明	日付
AmazonDataZoneSageMakerAccess - 新しいポリシー	という新しいポリシーAmazonDataZoneSageMakerAccess は、Amazon SageMaker アセットをカタログに発行するアクセス DataZone 許可を Amazon に付与します。また、カタログ内の Amazon DataZone が SageMaker 公開したアセットへのアクセスを許可または取り消すアクセス許可も Amazon に付与します。	2024 年 4 月 30 日
AmazonDataZoneFullAccess - ポリシーの更新	コンソールでブループリントを設定するアカウント管理者が使用しやすくするための `DescribeSecurityGroups` アクションと、指定された管理AmazonDataZoneFullAccessポリシーに関する情報を取得するのに役立つ `GetPolicy` アクションへのアクセスを追加するポリシーの更新。	2024 年 4 月 30 日
AmazonDataZoneSageMakerProvisioning - 新しいポリシー	という新しいポリシー DataZone は、Amazon と相互運用するために必要なアクセス許可を Amazon にAmazonDataZoneSageMakerProvisioning付与しますSageMaker。	2024 年 4 月 30 日

変更	説明	日付
AmazonDataZoneS3Manage - <region>-<domainId> - 新しいロール	Amazon AmazonDataZone が を呼び出すときに使用される S3Manage -<region>-<domainId > と呼ばれる新しいロール DataZone AWS Amazon Simple Storage Service (Amazon S3) ロケーションを登録する Lake Formation。 AWS Lake Formation は、その場所のデータにアクセスするときにこのロールを引き受けます。	2024 年 4 月 1 日
AmazonDataZoneGlue ManageAccessRolePolicy - ポリシーの更新	を更新AmazonDataZoneGlue ManageAccessRolePolicyして、Amazon がデータ DataZone への発行とアクセス許可を有効にできるようにするアクセス許可のサポートを有効にしました。	2024 年 4 月 1 日
AmazonDataZoneDomainExecutionRolePolicy および AmazonDataZoneFullUserAccess - ポリシーの更新	AmazonDataZoneDomainExecutionRolePolicy と を更新AmazonDataZoneFullUserAccessして、`CancelMetadataGenerationRun` のサポートを有効にしましたAPI。	2024 年 3 月 29 日

変更	説明	日付
AmazonDataZoneFullAccess - ポリシーの更新	ユーザーがテキストボックスに入力するのではなく、Amazon DataZone マネジメントコンソールでシークレット、クラスター、vpc の 、サブネットを選択`AmazonDataZoneFullAccess` できるように を更新しました。	2024 年 3 月 13 日
AmazonDataZoneDomainExecutionRolePolicy - ポリシーの更新	を更新`AmazonDataZoneDomainExecutionRolePolicy`して、どのアカウントとリージョンでどのブループリントが有効になっているかを特定することで、環境プロファイルの作成`ListEnvironmentBlueprintConfigurationSummaries` APIに必要なのサポートを有効にしました。	2024 年 2 月 1 日
AmazonDataZoneGlueManageAccessRolePolicy - ポリシーの更新	のサポートを有効にする`AmazonDataZoneGlueManageAccessRolePolicy`ように を更新しました AWS Lake Formation ハイブリッドモード。	2023 年 12 月 14 日

変更	説明	日付
AmazonDataZoneFullUserAccess および AmazonDataZoneDomainExecutionRolePolicy - ポリシーの更新	Amazon の生成 AI を活用したデータ記述機能をサポートするように AmazonDataZoneFullUserAccessおよび AmazonDataZoneDomainExecutionRolePolicyポリシーを更新しました DataZone。	2023 年 11 月 28 日
AmazonDataZoneEnvironmentRolePermissionsBoundary - ポリシーの更新	Amazon DataZone は、`ResourceTag` 条件でスコープダウンされた追加の`athena:GetQueryResultsStream` アクセス許可で構成される AmazonDataZoneEnvironmentRolePermissionsBoundaryマネージドポリシーを更新しました。	2023 年 11 月 17 日
AmazonDataZoneRedshiftManageAccessRolePolicy - ポリシーの更新	Amazon は、 `redshift:AssociateDataShareConsumer` アクションの組織 ID のチェックを削除AmazonDataZoneRedshiftManageAccessRolePolicyして DataZone を更新しました。これにより、 間でリソースを共有できます。 AWS 組織。	2023 年 11 月 16 日

変更	説明	日付
AmazonDataZoneFull UserAccess - ポリシーの更新	Amazon は、Amazon へのフルアクセスを許可するAmazonDataZoneFull UserAccessポリシー DataZone を更新しましたが DataZone、ドメイン、ユーザー、または関連するアカウントの管理は許可しません。	2023 年 10 月 2 日
AmazonDataZonePort alFullAccessPolicy - ポリシーは廃止されました	Amazon は を DataZone 廃止しましたAmazonDat aZonePortalFullAccessPolicy 。	2023 年 9 月 29 日
AmazonDataZonePrev iewConsoleFullAccess - ポリシーは廃止されました	Amazon は を DataZone 廃止しましたAmazonDat aZonePreviewConsol eFullAccess。	2023 年 9 月 29 日

変更	説明	日付
AmazonDataZoneDomainExecutionRolePolicy - 新しいポリシー	Amazon は、 という新しいポリシー DataZone を追加しましたAmazonDataZoneDomainExecutionRolePolicy。 これは Amazon DataZone `AmazonDataZoneDomainExecutionRole` サービスロールのデフォルトポリシーです。このロールは、Amazon DataZone ドメイン内のデータをカタログ化、検出、管理、共有、分析 DataZone するために Amazon によって使用されます。 `AmazonDataZoneDomainExecutionRolePolicy` ポリシーを にアタッチできます`AmazonDataZoneDomainExecutionRole` 。	2023 年 9 月 25 日
AmazonDataZoneCrossAccountAdmin - 新しいポリシー	Amazon は、ユーザーが Amazon DataZone および関連するアカウントを使用AmazonDataZoneCrossAccountAdminできるようにする という新しいポリシー DataZone を追加しました。	2023 年 9 月 19 日

変更	説明	日付
AmazonDataZoneFull UserAccess - 新しいポリシー	Amazon は、Amazon へのフルアクセスAmazonDataZoneFullUserAccessを許可する という新しいポリシー DataZone を追加しましたが DataZone、ドメイン、ユーザー、または関連するアカウントの管理は許可しません。	2023 年 9 月 12 日
AmazonDataZoneRedshiftManageAccessRolePolicy - 新しいポリシー	Amazon は、Amazon AmazonDataZoneRedshiftManageAccessRolePolicy がデータへの発行とアクセス許可を有効にするためのアクセス許可 DataZone を付与する という新しいポリシー DataZone を追加しました。	2023 年 9 月 12 日
AmazonDataZoneGlueManageAccessRolePolicy - 新しいポリシー	Amazon は、公開するアクセス DataZone 許可を Amazon に付与AmazonDataZoneGlueManageAccessRolePolicyする という新しいポリシー DataZone を追加しました。AWS データをカタログに Glue します。また、 へのアクセスを許可または取り消すためのアクセス DataZone 許可を Amazon に付与します。AWS Glue がカタログに公開したアセット。	2023 年 9 月 12 日

変更	説明	日付
AmazonDataZoneRedshiftGlueProvisioningPolicy - 新しいポリシー	Amazon は、サポートされているデータソースとの相互運用に必要なアクセス許可 DataZone を Amazon に付与AmazonDataZoneRedshiftGlueProvisioningPolicyする という新しいポリシー DataZone を追加しました。	2023 年 9 月 12 日
AmazonDataZoneEnvironmentRolePermissionsBoundary - 新しいポリシー	Amazon は、それがアタッチされているプロビジョニングされたIAMプリンシパルAmazonDataZoneEnvironmentRolePermissionsBoundaryを制限する という新しいポリシー DataZone を追加しました。	2023 年 9 月 12 日
AmazonDataZoneFullAccess - 新しいポリシー	Amazon は、 DataZone 経由で Amazon へのフルアクセスAmazonDataZoneFullAccessを提供する という新しいポリシー DataZone を追加しました。 AWS マネジメントコンソール。	2023 年 9 月 12 日
マネージドポリシーの更新	追加の`iam:GetPolicy` アクセス許可で構成されるAmazonDataZonePreviewConsoleFullAccessマネージドポリシーの更新。	2023 年 6 月 13 日

変更	説明	日付
Amazon が変更の追跡 DataZone を開始しました	Amazon が の変更の追跡 DataZone を開始しました AWS マネージドポリシー。	2023 年 3 月 20 日

IAM Amazon の ロール DataZone

トピック

- AmazonDataZoneProvisioningRole-<domainAccountId>
- AmazonDataZoneDomainExecutionRole
- AmazonDataZoneGlueAccess-<region>-<domainId >
- AmazonDataZoneRedshiftAccess-<region>-<domainId >
- AmazonDataZoneS3Manage-<region>-<domainId >
- AmazonDataZoneSageMakerManageAccessRole-<region>-<domainId >
- AmazonDataZoneSageMakerProvisioningRole-<domainAccountId>

AmazonDataZoneProvisioningRole-<domainAccountId>

AmazonDataZoneProvisioningRole-<domainAccountId> には がAmazonDataZoneRedshiftGlueProvisioningPolicyアタッチされています。このロール DataZone は、 との相互運用に必要なアクセス許可を Amazon に付与します。 AWS Glue と Amazon Redshift。

デフォルトAmazonDataZoneProvisioningRole-<domainAccountId>には、次の信頼ポリシーがアタッチされています。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "datazone.amazonaws.com"
      },
```

```
      "Action": "sts:AssumeRole",
      "Condition": {
        "StringEquals": {
            "aws:SourceAccount": "{{domain_account}}"
        }
      }
    }
  ]
}
```

AmazonDataZoneDomainExecutionRole

AmazonDataZoneDomainExecutionRole には があります。 AWS マネージドポリシーAmazonDataZoneDomainExecutionRolePolicyがアタッチされました。Amazon DataZone はユーザーに代わってこのロールを作成します。データポータルの特定のアクションについて、Amazon はロールが作成されたアカウントでこのロールを DataZone 引き受け、このロールがアクションを実行する権限があることを確認します。

AmazonDataZoneDomainExecutionRole ロールは で必要です AWS アカウント Amazon DataZone ドメインをホストする 。このロールは、Amazon DataZone ドメインを作成するときに自動的に作成されます。

デフォルトのAmazonDataZoneDomainExecutionRoleロールには、次の信頼ポリシーがあります。

```
{
    "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 >

AmazonDataZoneGlueAccess-<region>-<domainId> ロールには がAmazonDataZoneGlueManageAccessRolePolicyアタッチされています。このロールは、 を発行する DataZone アクセス許可を Amazon に付与します。 AWS データをカタログに Glue します。また、 へのアクセスを許可または取り消すためのアクセス DataZone 許可を Amazon に付与します。 AWS Glue がカタログに公開したアセット。

デフォルトのAmazonDataZoneGlueAccess-<region>-<domainId>ロールには、次の信頼ポリシーがアタッチされています。

```
{
  "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 >

AmazonDataZoneRedshiftAccess-<region>-<domainId> ロールには がAmazonDataZoneRedshiftManageAccessRolePolicyアタッチされています。このロールは、Amazon Redshift データをカタログに発行するアクセス DataZone 許可を Amazon に付与します。また、カタログ内の Amazon Redshift または Amazon Redshift Serverless が公開したアセットへのアクセスを許可または取り消すアクセス DataZone 許可も Amazon に付与します。

デフォルトのロールAmazonDataZoneRedshiftAccess-<region>-<domainId>には、次のインラインアクセス許可ポリシーがアタッチされています。

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Sid": "RedshiftSecretStatement",
         "Effect":"Allow",
         "Action":"secretsmanager:GetSecretValue",
         "Resource":"*",
         "Condition":{
            "StringEquals":{
               "secretsmanager:ResourceTag/AmazonDataZoneDomain":"{{domainId}}"
            }
         }
      }
   ]
}
```

デフォルトAmazonDataZoneRedshiftManageAccessRole<timestamp>には、次の信頼ポリシーがアタッチされています。

```
{
  "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}}"
            }
        }
    }
  ]
}
```

AmazonDataZoneS3Manage-<region>-<domainId >

AmazonDataZoneS3Manage -<region>-<domainId> は、Amazon DataZone が を呼び出すときに使用されます。 AWS Amazon Simple Storage Service (Amazon S3) ロケーションを登録する Lake Formation。 AWS Lake Formation は、その場所のデータにアクセスするときにこのロールを引き受けます。詳細については、「ロケーションの登録に使用されるロールの要件」を参照してください。

このロールには、次のインラインアクセス許可ポリシーがアタッチされています。

```
{
    "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}}"
                }
            }
        }
    ]
}
```

AmazonDataZoneS3Manage -<region>-<domainId> には、次の信頼ポリシーがアタッチされています。

```
{
    "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 >

AmazonDataZoneSageMakerManageAccessRole ロールには、AmazonDataZoneSageMakerAccess、AmazonDataZoneRedshiftManageAccessRolePolicy、および がAmazonDataZoneGlueManageAccessRolePolicyアタッチされています。このロールは、データレイク、データウェアハウス、および Amazon Sagemaker アセットのサブスクリプションを公開および管理するためのアクセス DataZone 許可を Amazon に付与します。

AmazonDataZoneSageMakerManageAccessRole ロールには、次のインラインポリシーがアタッチされています。

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Sid": "RedshiftSecretStatement",
         "Effect":"Allow",
         "Action":"secretsmanager:GetSecretValue",
         "Resource":"*",
         "Condition":{
            "StringEquals":{
               "secretsmanager:ResourceTag/AmazonDataZoneDomain":"{{domainId}}"
            }
         }
      }
   ]
}
```

AmazonDataZoneSageMakerManageAccessRole ロールには、次の信頼ポリシーがアタッチされています。

```
{
  "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>

AmazonDataZoneSageMakerProvisioningRole ロールには、AmazonDataZoneSageMakerProvisioningとがAmazonDataZoneRedshiftGlueProvisioningPolicyアタッチされています。このロールは、 との相互運用に必要な Amazon アクセス DataZone 許可を付与します。 AWS Glue、Amazon Redshift、Amazon Sagemaker。

AmazonDataZoneSageMakerProvisioningRole ロールには、次のインラインポリシーがアタッチされています。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "SageMakerStudioTagOnCreate",
            "Effect": "Allow",
            "Action": [
                "sagemaker:AddTags"
            ],
```

```
            "Resource": "arn:aws:sagemaker:*:{{AccountId}}:*/*",
            "Condition": {
                "Null": {
                    "sagemaker:TaggingAction": "false"
                }
            }
        }
    ]
}
```

AmazonDataZoneSageMakerProvisioningRole ロールには、次の信頼ポリシーがアタッチされています。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "DataZoneTrustPolicyStatement",
      "Effect": "Allow",
      "Principal": {
        "Service": "datazone.amazonaws.com"
      },
      "Action": "sts:AssumeRole",
      "Condition": {
        "StringEquals": {
            "aws:SourceAccount": "{{domain_account}}"
        }
      }
    }
  ]
}
```

一時認証情報

ある程度 AWS 一時的な認証情報を使用してサインインすると、 サービスは機能しません。以下を含む追加情報 AWS のサービスは一時的な認証情報を使用します。「」を参照してください。 AWS ユーザーガイドIAMの「 と連携する IAM のサービス」。

にサインインする場合、一時的な認証情報を使用している AWS Management Console ユーザー名とパスワード以外の方法を使用する。例えば、 にアクセスする場合 AWS 会社のシングルサインオン (SSO) リンクを使用すると、そのプロセスによって一時的な認証情報が自動的に作成されます。また、ユーザーとしてコンソールにサインインしてからロールを切り替える場合も、一時的な認証情報が自動的に作成されます。ロールの切り替えの詳細については、「 IAMユーザーガイド」の「ロールへの切り替え (コンソール) 」を参照してください。

を使用して、一時的な認証情報を手動で作成できます。 AWS CLI または AWS API。その後、これらの一時的な認証情報を使用して にアクセスできます。 AWS. AWS では、長期的なアクセスキーを使用する代わりに、一時的な認証情報を動的に生成することをお勧めします。詳細については、「」の「一時的なセキュリティ認証情報IAM」を参照してください。

プリンシパル権限

IAM ユーザーまたはロールを使用して でアクションを実行する場合 AWS、ユーザーはプリンシパルと見なされます。ポリシーによって、プリンシパルに許可が付与されます。一部のサービスを使用する際に、アクションを実行することで、別サービスの別アクションがトリガーされることがあります。この場合、両方のアクションを実行するための権限が必要です。アクションがポリシーで追加の依存アクションを必要とするかどうかを確認するには、「 のアクション、リソース、および条件キー」を参照してください。 AWS 「サービス認証リファレンス」の「ドキュメントの要点」。

Amazon のコンプライアンス検証 DataZone

が AWS のサービス は特定のコンプライアンスプログラムの範囲内にあります。「」を参照してください。 AWS のサービス コンプライアンスプログラムによる対象範囲内による対象範囲内で、関心のあるコンプライアンスプログラムを選択します。一般的な情報については、「」を参照してください。 AWS コンプライアンスプログラム。

サードパーティーの監査レポートは、 を使用してダウンロードできます。 AWS Artifact。 詳細については、「 でのレポートのダウンロード」を参照してください。 AWS Artifact.

を使用する際のお客様のコンプライアンス責任 AWS のサービス は、データの機密性、企業のコンプライアンス目的、適用可能な法律および規制によって決まります。 AWS では、コンプライアンスに役立つ以下のリソースを提供しています。

- セキュリティとコンプライアンスのクイックスタートガイド – これらのデプロイガイドでは、アーキテクチャ上の考慮事項について説明し、 にベースライン環境をデプロイする手順について説明します。 AWS セキュリティとコンプライアンスに重点を置いた 。

- アマゾン ウェブ サービスHIPAAのセキュリティとコンプライアンスのためのアーキテクチャ – このホワイトペーパーでは、企業が を使用する方法について説明します。 AWS HIPAA対象アプリケーションを作成するための 。

> **Note**
>
> すべてではない AWS のサービス がHIPAA対象です。詳細については、HIPAA「対象サービスリファレンス」を参照してください。

- AWS コンプライアンスリソース – このワークブックとガイドのコレクションは、お客様の業界や地域に適用される場合があります。
- AWS カスタマーコンプライアンスガイド — コンプライアンスの観点から責任共有モデルを理解します。このガイドでは、 を保護するためのベストプラクティスをまとめています。 AWS のサービス と は、ガイダンスを複数のフレームワーク (米国国立標準技術研究所 (NIST) 、Payment Card Industry Security Standards Council (PCI) 、国際標準化機構 (ISO) を含む) のセキュリティコントロールにマッピングします。
- のルールによるリソースの評価 AWS Config デベロッパーガイド – AWS Config サービスは、リソース設定が社内プラクティス、業界ガイドライン、および規制にどの程度準拠しているかを評価します。
- AWS Security Hub – これは AWS のサービス は、 内のセキュリティ状態を包括的に表示します。 AWS。 Security Hub は、セキュリティコントロールを使用して を評価します。 AWS リソース と を使用して、セキュリティ業界標準およびベストプラクティスに照らしてコンプライアンスをチェックします。サポートされているサービスとコントロールのリストについては、Security Hub のコントロールリファレンスを参照してください。
- Amazon GuardDuty – これは AWS のサービス が に対する潜在的な脅威を検出する AWS アカウント、ワークロード、コンテナ、およびデータをモニタリングして、不審なアクティビティや悪意のあるアクティビティがないかを確認します。 PCI GuardDuty は、特定のコンプライアンスフレームワークで義務付けられている侵入検知要件を満たすことでDSS、 などのさまざまなコンプライアンス要件に対応するのに役立ちます。
- AWS Audit Manager – これは AWS のサービス は、 の継続的な監査に役立ちます。 AWS を使用して、リスクの管理方法と規制や業界標準への準拠を簡素化します。

Amazon のセキュリティのベストプラクティス DataZone

Amazon DataZone には、独自のセキュリティポリシーを開発および実装する際に考慮すべきセキュリティ機能が多数用意されています。以下のベストプラクティスは一般的なガイドラインであり、完

全なセキュリティソリューションを説明するものではありません。これらのベストプラクティスはお客様の環境に適切ではないか、十分ではない場合があるため、これらは処方箋ではなく、有用な考慮事項と見なしてください。

最小特権アクセスの実装

アクセス許可を付与するときは、Amazon DataZone リソースに対するアクセス許可を取得するユーザーを決定します。これらのリソースで許可したい特定のアクションを有効にするのも、お客様になります。このため、タスクの実行に必要なアクセス許可のみを付与する必要があります。最小特権アクセスの実装は、セキュリティリスクと、エラーや悪意によってもたらされる可能性のある影響の低減における基本になります。

IAM ロールを使用する

プロデューサーアプリケーションとクライアントアプリケーションは、Amazon DataZone リソースにアクセスするために有効な認証情報を持っている必要があります。保存しないでください AWS クライアントアプリケーションまたは Amazon S3 バケット内の 認証情報。これらは自動的にローテーションされない長期的な認証情報であり、漏洩するとビジネスに大きな影響が及ぶ場合があります。

代わりに、 IAMロールを使用して、プロデューサーおよびクライアントアプリケーションが Amazon DataZone リソースにアクセスするための一時的な認証情報を管理する必要があります。ロールを使用するときは、他のリソースにアクセスするために長期的な認証情報 (ユーザー名とパスワード、またはアクセスキーなど) を使用する必要がありません。

詳細については、「 IAMユーザーガイド」の以下のトピックを参照してください。

- IAM ロール
- ロールの一般的なシナリオ: ユーザー、アプリケーション、およびサービス

依存リソースでのサーバー側の暗号化の実装

保管中のデータと転送中のデータは、Amazon で暗号化できます DataZone。

CloudTrail を使用してAPI通話をモニタリングする

Amazon DataZone は と統合されています AWS CloudTrail、ユーザー、ロール、または によって実行されたアクションの記録を提供するサービス AWS Amazon の サービス DataZone。

で収集された情報を使用して CloudTrail、Amazon に対するリクエスト DataZone、リクエスト元の IP アドレス、リクエスト者、リクエスト日時などの詳細を確認できます。

Amazon の耐障害性 DataZone

- AWS グローバルインフラストラクチャは AWS リージョン およびアベイラビリティーゾーン。AWS リージョン は、低レイテンシー、高スループット、および高度に冗長なネットワークで接続された、物理的に分離および分離された複数のアベイラビリティーゾーンを提供します。アベイラビリティーゾーンでは、ゾーン間で中断することなく自動的にフェイルオーバーするアプリケーションとデータベースを設計および運用することができます。アベイラビリティーゾーンは、従来の単一または複数のデータセンターインフラストラクチャよりも可用性が高く、フォールトトレラントで、スケーラブルです。

の詳細については、「」を参照してください。 AWS リージョン およびアベイラビリティーゾーンについては、「」を参照してください。 AWS グローバルインフラストラクチャ 。

に加えて AWS グローバルインフラストラクチャである Amazon DataZone には、データの耐障害性とバックアップのニーズをサポートするのに役立ついくつかの機能があります。

トピック

- データソースの耐障害性
- アセットレジリエンス
- アセットタイプとメタデータフォームの耐障害性
- 用語集の耐障害性
- グローバル検索の耐障害性
- サブスクリプションの耐障害性
- 環境レジリエンス
- 環境設計図の耐障害性
- プロジェクトの耐障害性
- RAM レジリエンス
- ユーザープロファイル管理の耐障害性
- ドメインレジリエンス

データソースの耐障害性

Amazon の DataZone 可用性イベント中、DataSourceジョブは最大 24 時間定期的に再試行されます。設定ミスが原因でジョブが失敗すると、DataSourceRunFailedイベントが発生します。Amazon DataZone ドメインにKMSキーが設定されていて、ジョブの実行中に がこのキーにア

クセス AmazonDataZoneDomainExecutionRole できない場合、実行は INACCESSIBLE状態で終了します。KMS アクセスが復元されたら、ジョブを手動で更新して、使用可能な状態への移行をトリガーする必要があります。

アセットレジリエンス

Amazon では DataZone、アセットはバージョニングされます。アセットのバージョンをロールバックする必要がある場合は、最新の安定バージョンのコンテンツを使用して新しいバージョンを作成できます。アセットバージョンは公開できます。アセットの公開バージョンは、新しいバージョンを公開する場合を除き、編集できません。公開されたアセット (別名出品) はサブスクライブできます。アセットへの新しいサブスクリプションを防ぐには、アセットを非公開にすることができます。アセットの公開解除は、既存のサブスクリプションには影響しません。アセットを削除すると、アセットの未公開バージョンがすべて削除されます。アセットの公開バージョンは個別に削除する必要があります。アセットの公開バージョンは、サブスクリプションがない場合にのみ削除できます。

アセットタイプとメタデータフォームの耐障害性

Amazon では DataZone、アセットタイプとメタデータフォームタイプがバージョニングされます。アセットタイプは、アセットで使用されている場合は削除できません。メタデータフォームタイプは、アセットタイプまたはアセットで使用されている場合は削除できません。特定の metadata-form-type をキュレーションに使用しない場合は、既にアタッチされているものに影響を与えない無効にできます。

用語集の耐障害性

Amazon では DataZone、用語集と用語集用語が使用されている場合、それらを削除することはできません。特定の用語集または用語集用語をキュレーションに使用しない場合は、既にアタッチされている用語集や用語集用語に影響を与えない用語集を無効にすることができます。

グローバル検索の耐障害性

Amazon では DataZone、公開されたアセット (別名出品) はグローバル検索で検出できます。アセットの公開は、アセットの公開を解除することでロールバックできます。アセットの公開を解除しても、既存のサブスクリプションには影響しません。公開されたアセットは、そのバージョンを再公開することで、特定のバージョンのアセットにロールバックできます。これは既存のサブスクリプションには影響しません。

サブスクリプションの耐障害性

Amazon では DataZone、 subscriptionGrant フルフィルメントは失敗する前に 2 回のリタイアを試みます。失敗した場合は、手動で削除して再試行する必要があります。Amazon がサブスクリプションのアクセス許可を取り消す DataZone ことができない場合、サブスクリプションの削除が失敗する可能性があります。基盤となるエラーに対処するか、 `retainPermissions`フラグを `DeleteSubscriptionGrant` API オペレーションで使用して、アクセス許可を取り消す DataZone ことなく Amazon から権限を強制的に削除できます。

Amazon DataZone ドメインにKMSキーが設定されていて、`SubscriptionGrant`ワークフロー中にがこのキーにアクセス`AmazonDataZoneDomainExecutionRole`できない場合、許可は とマークされます`INACCESSIBLE`。KMS アクセスが復元されたら、`INACCESSIBLE`許可を削除して再作成する必要があります。

環境レジリエンス

Amazon DataZone ドメインにKMSキーが設定されていて、環境ワークフロー中に がこのキーにアクセス`AmazonDataZoneDomainExecutionRole`できない場合、環境は とマークされます`INACCESSIBLE`。KMS アクセスが復元されたら、`INACCESSIBLE`環境を削除して再作成する必要があります。環境の作成は、失敗する前に 2 回廃止を試みます。失敗した場合は、手動で削除して再試行する必要があります。環境ワークフローが失敗すると、環境は失敗状態になります。この時点では、削除して再作成することしかできません。

環境設計図の耐障害性

Amazon では DataZone、基盤となる環境プロファイルがある場合、環境ブループリントを削除することはできません。

プロジェクトの耐障害性

Amazon では DataZone、含まれている環境がある場合、プロジェクトを削除することはできません。

RAM レジリエンス

RAM 耐障害性の詳細については、https://docs.aws.amazon.com/ram/「 latest/userguide/security-disaster-recovery-resiliency.html」を参照してください。

ユーザープロファイル管理の耐障害性

ユーザープロファイルの耐障害性情報については、「」を参照してください。 AWS Identity Center 。

ドメインレジリエンス

Amazon では DataZone、ドメインにプロジェクトまたはデータソースが含まれている場合、ドメインを削除することはできません。

Amazon のインフラストラクチャセキュリティ DataZone

マネージドサービスである Amazon DataZone は によって保護されています。 AWS グローバルネットワークセキュリティ。参考情報 AWS セキュリティサービスとその方法 AWS インフラストラクチャを保護するには、「」を参照してください。 AWS クラウドセキュリティ 。を設計するには AWS インフラストラクチャセキュリティのベストプラクティスを使用する 環境、「セキュリティの柱」の「インフラストラクチャの保護」を参照してください。 AWS Well-Architected フレームワーク 。

を使用する AWS は、ネットワーク DataZone 経由で Amazon にアクセスするためのAPI呼び出しを発行しました。クライアントは以下をサポートする必要があります:

- Transport Layer Security (TLS) 。1TLS.2 が必要で、1.3 TLS をお勧めします。
- (Ephemeral Diffie-HellmanPFS) や DHE (Elliptic Curve Ephemeral Diffie-Hellman) などの完全前方秘匿性 ECDHE () を備えた暗号スイート。これらのモードは、Java 7 以降など、ほとんどの最新システムでサポートされています。

さらに、リクエストは、 IAMプリンシパルに関連付けられたアクセスキー ID とシークレットアクセスキーを使用して署名する必要があります。または、 AWS Security Token Service (AWS STS) リクエストに署名するための一時的なセキュリティ認証情報を生成します。

Amazon でのサービス間の混乱した代理の防止 DataZone

混乱した代理問題は、アクションを実行するためのアクセス許可を持たないエンティティが、より特権のあるエンティティにアクションの実行を強制できてしまう場合に生じる、セキュリティ上の問題です。In AWS、サービス間のなりすましは、混乱した代理問題を引き起こす可能性があります。サービス間でのなりすましは、1 つのサービス (呼び出し元サービス) が、別のサービス (呼び出し対

象サービス) を呼び出すときに発生する可能性があります。呼び出し元サービスは、本来ならアクセスすることが許可されるべきではない方法でその許可を使用して、別のお客様のリソースに対する処理を実行するように操作される場合があります。これを防ぐには、 AWS は、アカウント内のリソースへのアクセスが許可されているサービスプリンシパルを使用して、すべてのサービスのデータを保護するのに役立つツールを提供します。

リソースポリシーで aws:SourceAccount global 条件コンテキストキーを使用して、Amazon が別のサービスに DataZone 付与するアクセス許可をリソースに制限することをお勧めします。そのアカウントのリソースをクロスサービスの使用に関連付けることを許可するSourceAccount 場合は、aws: を使用します。

Amazon の設定と脆弱性の分析 DataZone

AWS は、ゲストオペレーティングシステム (OS) やデータベースのパッチ適用、ファイアウォール設定、ディザスタリカバリなどの基本的なセキュリティタスクを処理します。これらの手順は適切なサードパーティーによって確認され、認証されています。詳細については、「」を参照してください。 AWS 責任共有モデル 。

許可リストに追加するドメイン

Amazon DataZone データポータルが Amazon DataZone サービスにアクセスするには、データポータルがサービスにアクセスしようとしているネットワークの許可リストに次のドメインを追加する必要があります。

- `*.api.aws`
- `*.on.aws`

Amazon のモニタリング DataZone

モニタリングは、Amazon DataZone およびその他の AWS ソリューションの信頼性、可用性、パフォーマンスを維持する上で重要な部分です。 AWS は、Amazon をモニタリングし DataZone、問題が発生した場合は報告し、必要に応じて自動アクションを実行するために、以下のモニタリングツールを提供しています。

- Amazon CloudWatch は、 AWS リソースと、 で実行しているアプリケーションを AWS リアルタイムでモニタリングします。メトリクスの収集と追跡、カスタマイズしたダッシュボードの作成、および指定したメトリクスが指定したしきい値に達したときに通知またはアクションを実行するアラームの設定を行うことができます。例えば、 で Amazon EC2 インスタンスの CPU 使用率やその他のメトリクス CloudWatch を追跡し、必要に応じて新しいインスタンスを自動的に起動できます。詳細については、「Amazon ユーザーガイド CloudWatch 」を参照してください。
- Amazon CloudWatch Logs を使用すると、Amazon EC2 インスタンスやその他のソースからログファイルをモニタリング、保存 CloudTrail、アクセスできます。 CloudWatch ログはログファイル内の情報をモニタリングし、特定のしきい値に達したときに通知できます。高い耐久性を備えたストレージにログデータをアーカイブすることもできます。詳細については、「Amazon CloudWatch Logs ユーザーガイド」を参照してください。
- Amazon EventBridge を使用すると、 AWS サービスを自動化し、アプリケーションの可用性の問題やリソースの変更などのシステムイベントに自動的に対応できます。 AWS サービスからのイベントは、ほぼリアルタイムで EventBridge に配信されます。簡単なルールを記述して、注目するイベントと、イベントがルールに一致した場合に自動的に実行するアクションを指定できます。詳細については、「Amazon ユーザーガイド EventBridge 」を参照してください。
- AWS CloudTrail は、 AWS アカウントによって、またはアカウントに代わって行われた API コールおよび関連イベントをキャプチャし、指定した Amazon S3 バケットにログファイルを配信します。を呼び出したユーザーとアカウント AWS、呼び出し元のソース IP アドレス、呼び出しが発生した日時を特定できます。詳細については、「AWS CloudTrail ユーザーガイド」を参照してください。

Amazon での Amazon DataZone イベントのモニタリング EventBridge

で Amazon DataZone イベントをモニタリングできます。これにより EventBridge、独自のアプリケーション、 software-as-a-service (SaaS) アプリケーション、および AWS サービスからリアルタイムデータのストリームが配信されます。 EventBridge は、そのデータを AWS Lambda や Amazon

Simple Notification Service などのターゲットにルーティングします。これらのイベントは、Amazon CloudWatch Events に表示されるイベントと同じです。Amazon Events は、 AWS リソースの変更を記述するシステムイベントのほぼリアルタイムのストリームを提供します。

詳細については、「Amazon EventBridge デフォルトバス経由のイベント」を参照してください。

を使用した Amazon DataZone API コールのログ記録 AWS CloudTrail

Amazon DataZone は、Amazon のユーザー AWS CloudTrail、ロール、または サービスによって実行されたアクションを記録する AWS サービスである と統合されています DataZone。 は、Amazon のすべての API コールをイベント DataZone として CloudTrail キャプチャします。キャプチャされた呼び出しには、Amazon DataZone コンソールからの呼び出しと、Amazon DataZone API オペレーションへのコード呼び出しが含まれます。証跡を作成する場合は、Amazon の CloudTrail イベントなど、Amazon S3 バケットへのイベントの継続的な配信を有効にすることができます DataZone。 Amazon S3 証跡を設定しない場合でも、 CloudTrail コンソールのイベント履歴 で最新のイベントを表示できます。によって収集された情報を使用して CloudTrail、Amazon に対するリクエスト DataZone、リクエスト元の IP アドレス、リクエスト者、リクエスト日時などの詳細を確認できます。

の詳細については CloudTrail、「 AWS CloudTrail ユーザーガイド」を参照してください。

の Amazon DataZone 情報 CloudTrail

CloudTrail アカウントを作成する AWS アカウント と、 で が有効になります。Amazon DataZone マネジメントコンソールでアクティビティが発生すると、そのアクティビティは CloudTrail イベント履歴 の他の AWS サービスイベントとともにイベントに記録されます。で最近のイベントを表示、検索、ダウンロードできます AWS アカウント。詳細については、「イベント履歴 で CloudTrail イベントを表示する」を参照してください。

Amazon のイベントなど AWS アカウント、 のイベントの継続的な記録については DataZone、証跡を作成します。証跡により CloudTrail 、 はログファイルを Amazon S3 バケットに配信できます。デフォルトでは、コンソールで証跡を作成するときに、証跡がすべての AWS リージョンに適用されます。証跡は、 AWS パーティション内のすべてのリージョンからのイベントを口グに記録し、指定した Amazon S3 バケットにログファイルを配信します。さらに、 CloudTrail 口グで収集されたイベントデータをさらに分析し、それに基づいて行動するように他の AWS サービスを設定できます。詳細については、次を参照してください:

- 「証跡作成の概要」
- CloudTrail がサポートするサービスと統合
- の Amazon SNS 通知の設定 CloudTrail
- 複数のリージョンからの CloudTrail ログファイルの受信と複数のアカウントからの CloudTrail ログファイルの受信

すべての Amazon DataZone アクションは によって ログに記録されます CloudTrail。

Amazon のトラブルシューティング DataZone

Amazon DataZone の使用時にアクセスが拒否された問題や同様の問題が発生した場合は、このセクションのトピックを参照してください。

Amazon の AWS Lake Formation 許可のトラブルシューティング DataZone

このセクションでは、 時に発生する可能性のある問題のトラブルシューティング手順について説明しますAmazon の Lake Formation アクセス許可を設定する DataZone。

データポータルのエラーメッセージ	解決方法
データアクセスロールを引き受けることができません。	このエラーは、Amazon DataZone がアカウントDefaultDataLakeBlueprintで を有効にするためにAmazonDataZoneGlueDataAccessRole使用した を引き受けられない場合に表示されます。この問題を解決するには、データアセットが存在するアカウントの コンソールに移動 AWS IAMし、 AmazonDataZoneGlueDataAccessRole が Amazon DataZone サービスプリンシパルと適切な信頼関係にあることを確認します。詳細については、「AmazonDataZoneGlueAccess-<region>-<domainId>」を参照してください
データアクセスロールには、サブスクライブしようとしているアセットのメタデータを読み取るために必要なアクセス許可がありません。	このエラーは、Amazon がAmazonDataZoneGlueDataAccessRoleロールを DataZone 正常に引き受けたが、ロールに必要なアクセス許可がない場合に表示されます。この問題を解決するには、データアセットが存在するアカウントのコンソールに移動 AWS IAMし、ロールにアAmazonDataZoneGlueManageAccessRolePolicyタッチされていることを確認します。詳細については、「AmazonDat

データポータルのエラーメッセージ	解決方法
	aZoneGlueAccess-<region>-<domainId> 」を参照してください。
アセットはリソースリンクです。Amazon DataZone は、リソースリンクのサブスクリプションをサポートしていません。	このエラーは、Amazon に公開しようとしているアセット DataZone が AWS Glue テーブルへのリソースリンクである場合に表示されます。

データポータルのエラーメッセージ	解決方法
アセットは AWS Lake Formation によって管理されません。	このエラーは、公開するアセットに AWS Lake Formation 許可が適用されていないことを示します。これは、次の場合に発生する可能性があります。 • アセットの Amazon S3 の場所は AWS Lake Formation に登録されていません。この問題を解決するには、テーブルが存在するアカウントの Lake Formation コンソールにログインし、Amazon S3 の場所を AWS Lake Formation モードまたはハイブリッドモードで登録します AWS 。詳細については、「Amazon S3 ロケーションの登録」を参照してください。さらに変更が必要なシナリオがいくつかあります。これには、暗号化された AmazonS3 バケットまたはクロスアカウント S3 バケットと AWS Glue Catalog の設定が含まれます。このような場合は、 KMS および/または S3 設定の変更が必要になる場合があります。詳細については、「暗号化された Amazon S3 の場所の登録」を参照してください。 • Amazon S3 の場所は AWS Lake Formation モードで登録されますがIAMAllowedPrincipal、テーブルのアクセス許可に追加されます。この問題を解決するには、テーブルのアクセス許可IAMAllowedPrincipalから を削除するか、ハイブリッドモードで S3 ロケーションを登録します。詳細については、「Lake Formation アクセス許可モデルへのアップグレードについて」を参照してください。S3 ロケーションが暗号化されている場合、または S3 ロケーションが Glue テーブルとは異なるアカウントにある場合は

データポータルのエラーメッセージ	解決方法
	AWS 、「暗号化された Amazon S3 ロケーションの登録」の手順に従います。
データアクセスロールには、このアセットへのアクセスを許可するために必要な Lake Formation 許可がありません。	このエラーAmazonDataZoneGlueDataAccessRoleは、アカウントDefaultDataLakeBlueprintで を有効にするために使用しているに、Amazon が公開されたアセットに対するアクセス許可 DataZone を管理するために必要なアクセス許可がないことを示します。この問題を解決するには、 AWS Lake Formation 管理者AmazonDataZoneGlueDataAccessRoleとして を追加するか、公開するアセットAmazonDataZoneGlueDataAccessRoleの に次のアクセス許可を付与します。 • アセットが存在するデータベースに対する付与可能なアクセス許可の説明と説明 • Amazon がユーザーに代わって管理するacecss のデータベース内のすべてのアセットに対する許可を記述、選択、付与可能 DataZone の説明、付与可能の選択を選択します。

アップストリームデータセットとの Amazon DataZone 系統アセットリンクのトラブルシューティング

このセクションでは、Amazon DataZone 系統で発生する可能性のある問題のトラブルシューティング手順について説明します。一部の AWS Glue および Amazon Redshift 関連のオープン系統実行イベントでは、アセット系統がアップストリームデータセットにリンクされていないことがあります。このトピックでは、問題を軽減するためのシナリオといくつかのアプローチについて説明します。系統の詳細については、「」を参照してくださいAmazon のデータ系統 DataZone （プレビュー）。

SourceIdentifier 系統ノード上の

系統ノードの sourceIdentifier 属性は、データセットで発生するイベントを表します。詳細については、「系統ノードのキー属性」を参照してください。

系統ノードは、対応するデータセットまたはジョブで発生するすべてのイベントを表します。系統ノードには、対応するデータセット/ジョブの識別子を含むsourceIdentifier「」属性が含まれています。オープン系統イベントをサポートするため、デフォルトでは、データセット、ジョブ、ジョブ実行の「名前空間」と「名前」の組み合わせとしてsourceIdentifier値が設定されます。

AWS Glue や Amazon Redshift などの AWS リソースsourceIdentifierの場合、 は AWS Glue 、Amazon DataZone が run-event やその他の詳細を次のように構築ARNsする テーブルと ARN Redshift テーブルになります。

> **Note**
>
> では AWS、 には、すべてのリソースの accountId、リージョン、データベース、テーブルなどの情報ARNが含まれています。

- OpenLineage これらのデータセットの イベントには、データベース名とテーブル名が含まれます。
- リージョンは、実行の「環境プロパティ」ファセットにキャプチャされます。存在しない場合、システムは発信者認証情報のリージョンを使用します。
- AccountId は発信者の認証情報から取得されます。

SourceIdentifier 内のアセットの DataZone

AssetCommonDetailForm には、アセットsourceIdentifierが表すデータセットの識別子を表す「」という属性があります。アセット系統ノードをアップストリームデータセットにリンクするには、属性にデータセットノードの と一致する値を入力する必要がありますsourceIdentifier。アセットがデータソースによってインポートされる場合、ワークフローはsourceIdentifier AWS Glue テーブルARN/Redshift テーブルとしてARN自動的に入力されますが、 を介して作成された他のアセット (カスタムアセットを含む) CreateAssetAPIには、発信者がその値を入力する必要があります。

Amazon は OpenLineage イベント sourceIdentifier から をどのように DataZone 構築しますか？

AWS Glue および Redshift アセットの場合、 sourceIdentifierは Glue と Redshift から構築されますARNs。Amazon がこれ DataZone を構築する方法は次のとおりです。

AWS Glue ARN

目標は、出力系統ノードの が次の OpenLineage イベントを構築するsourceIdentifierことです。

```
arn:aws:glue:us-east-1:123456789012:table/testlfdb/testlftb-1
```

実行が のデータを使用しているかどうかを判断するには AWS Glue、ファenvironment-propertiesセットに特定のキーワードが存在するかどうかを確認します。具体的には、これらの指定されたフィールドのいずれかが存在する場合、システムは のRunEvent発信元を想定します AWS Glue。

- GLUE_VERSION
- GLUE_COMMAND_CRITERIA
- GLUE_PYTHON_VERSION

```
"run": {
   "runId":"4e3da9e8-6228-4679-b0a2-fa916119fthr",
   "facets":{
      "environment-properties":{
         "_producer":"https://github.com/OpenLineage/OpenLineage/tree/1.9.1/
integration/spark",
         "_schemaURL":"https://openlineage.io/spec/2-0-2/OpenLineage.json#/$defs/
RunFacet",
         "environment-properties":{
            "GLUE_VERSION":"3.0",
            "GLUE_COMMAND_CRITERIA":"glueetl",
            "GLUE_PYTHON_VERSION":"3"
         }
      }
   }
```

AWS Glue 実行では、symlinksファセットの名前を使用してデータベース名とテーブル名を取得できます。これは、 の構築に使用できますARN。

名前が であることを確認する必要がありますdatabaseName.tableName。

```
"symlinks": {
   "_producer":"https://github.com/OpenLineage/OpenLineage/tree/1.9.1/integration/
spark",
   "_schemaURL":"https://openlineage.io/spec/facets/1-0-0/SymlinksDatasetFacet.json#/
$defs/SymlinksDatasetFacet",
   "identifiers":[
      {
         "namespace":"s3://object-path",
         "name":"testlfdb.testlftb-1",
         "type":"TABLE"
      }
   ]
}
```

サンプルCOMPLETEイベント：

```
{
   "eventTime":"2024-07-01T12:00:00.000000Z",
   "producer":"https://github.com/OpenLineage/OpenLineage/tree/1.9.1/integration/glue",
   "schemaURL":"https://openlineage.io/spec/2-0-2/OpenLineage.json#/$defs/RunEvent",
   "eventType":"COMPLETE",
   "run": {
      "runId":"4e3da9e8-6228-4679-b0a2-fa916119fthr",
      "facets":{
         "environment-properties":{
            "_producer":"https://github.com/OpenLineage/OpenLineage/tree/1.9.1/
integration/spark",
            "_schemaURL":"https://openlineage.io/spec/2-0-2/OpenLineage.json#/$defs/
RunFacet",
            "environment-properties":{
               "GLUE_VERSION":"3.0",
               "GLUE_COMMAND_CRITERIA":"glueetl",
               "GLUE_PYTHON_VERSION":"3"
            }
         }
      }
   },
   "job":{
```

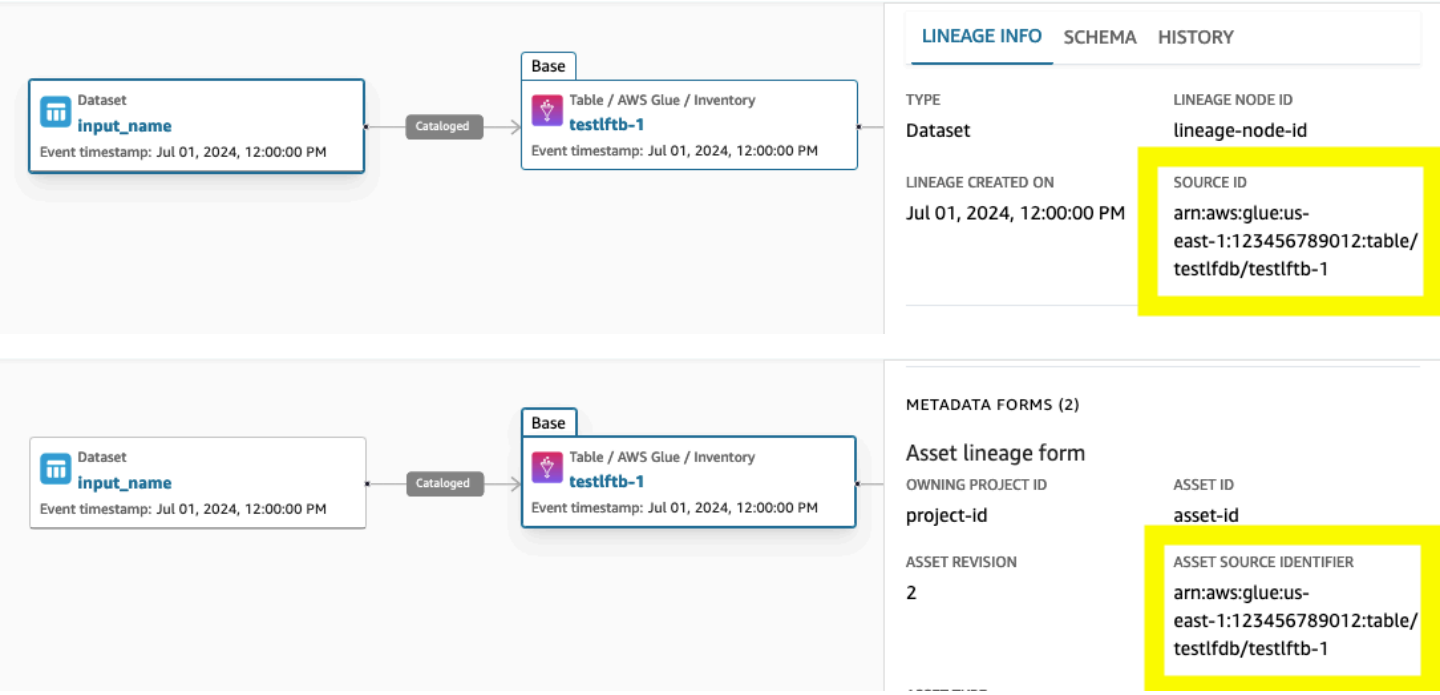
```
      "namespace":"namespace",
      "name":"job_name",
      "facets":{
         "jobType":{
            "_producer":"https://github.com/OpenLineage/OpenLineage/tree/1.9.1/
integration/glue",
            "_schemaURL":"https://openlineage.io/spec/facets/2-0-2/
JobTypeJobFacet.json#/$defs/JobTypeJobFacet",
            "processingType":"BATCH",
            "integration":"glue",
            "jobType":"JOB"
         }
      }
   },
   "inputs":[
      {
         "namespace":"namespace",
         "name":"input_name"
      }
   ],
   "outputs":[
      {
         "namespace":"namespace.output",
         "name":"output_name",
         "facets":{
            "symlinks":{
               "_producer":"https://github.com/OpenLineage/OpenLineage/tree/1.9.1/
integration/spark",
               "_schemaURL":"https://openlineage.io/spec/facets/1-0-0/
SymlinksDatasetFacet.json#/$defs/SymlinksDatasetFacet",
               "identifiers":[
                  {
                     "namespace":"s3://object-path",
                     "name":"testlfdb.testlftb-1",
                     "type":"TABLE"
                  }
               ]
            }
         }
      }
   ]
}
```

送信されたOpenLineageイベントに基づいて、出力系統ノードsourceIdentifierの は次のようになります。

```
arn:aws:glue:us-east-1:123456789012:table/testlfdb/testlftb-1
```

出力系統ノードは、アセットの系統ノードに接続され、アセットの sourceIdentifierは次のようになります。

```
arn:aws:glue:us-east-1:123456789012:table/testlfdb/testlftb-1
```



Amazon Redshift ARN

目標は、出力系統ノードの が次の OpenLineage イベントを構築するsourceIdentifierことです。

```
arn:aws:redshift:us-east-1:123456789012:table/workgroup-20240715/tpcds_data/public/
dws_tpcds_7
```

システムは、入力または出力が名前空間に基づいて Redshift に保存されるかどうかを決定します。具体的には、名前空間が redshift:// で始まるか、文字列 redshift-serverless.amazonaws.comまたは が含まれている場合redshift.amazonaws.com、Redshift リソースです。

```
"outputs": [
    {
        "namespace":"redshift://workgroup-20240715.123456789012.us-
east-1.redshift.amazonaws.com:5439",
        "name":"tpcds_data.public.dws_tpcds_7"
    }
]
```

名前空間は次の形式である必要があることに注意してください。

```
provider://{cluster_identifier}.{region_name}:{port}
```

redshift-serverless の場合:

```
"outputs": [
    {
        "namespace":"redshift://workgroup-20240715.123456789012.us-east-1.redshift-
serverless.amazonaws.com:5439",
        "name":"tpcds_data.public.dws_tpcds_7"
    }
]
```

次の結果になります。 sourceIdentifier

```
arn:aws:redshift-serverless:us-east-1:123456789012:table/workgroup-20240715/tpcds_data/
public/dws_tpcds_7
```

送信された OpenLineage イベントに基づいて、ダウンストリーム (つまり、イベントの出力) 系統ノードにマッピングsourceIdentifierされる は次のとおりです。

```
arn:aws:redshift-serverless:us-e:us-east-1:123456789012:table/workgroup-20240715/
tpcds_data/public/dws_tpcds_7
```

これは、カタログ内のアセットの系統を視覚化するのに役立つマッピングです。

代替アプローチ

上記のいずれの条件も満たされない場合、システムは名前空間 /name を使用して を構築しますsourceIdentifier。

```
"inputs": [
  {
     "namespace":"arn:aws:redshift:us-east-1:123456789012:table",
     "name":"workgroup-20240715/tpcds_data/public/dws_tpcds_7"
  }
],
"outputs": [
  {
     "namespace":"arn:aws:glue:us-east-1:123456789012:table",
     "name":"testlfdb/testlftb-1"
  }
]
```

アセット系統ノードのアップストリームの欠如のトラブルシューティング

アセット系統ノードのアップストリームが表示されない場合は、以下を実行して、データセットにリンクされていない理由をトラブルシューティングできます。

1. domainId と を指定GetAssetしながら を呼び出しますassetId。

```
aws datazone get-asset --domain-identifier <domain-id> --identifier <asset-id>
```

レスポンスは次のように表示されます。

```
{
    .....
    "formsOutput": [
        .....
        {
            "content": "{\"sourceIdentifier\":\"arn:aws:glue:eu-
west-1:123456789012:table/testlfdb/testlftb-1\"}",
            "formName": "AssetCommonDetailsForm",
            "typeName": "amazon.datazone.AssetCommonDetailsFormType",
            "typeRevision": "6"
        },
        .....
    ],
    "id": "<asset-id>",
    ....
}
```

2. を呼び出しGetLineageNodeて、データセット系統ノードsourceIdentifierの を取得します。対応するデータセットノードの系統ノードを直接取得する方法がないため、ジョブの実行GetLineageNode時に から始めることができます。

```
aws datazone get-lineage-node --domain-identifier <domain-id> --identifier
 <job_namespace>.<job_name>/<run_id>

if you are using the getting started scripts, job name and run ID are printed in the
 console
and namespace is "default". Otherwise you can get these values from run event
 content.
```

サンプルレスポンスは次のようになります。

```
{
    .....
    "downstreamNodes": [
        {
            "eventTimestamp": "2024-07-24T18:08:55+08:00",
            "id": "afymge5k4v0euf"
        }
    ],
    "formsOutput": [
        <some forms corresponding to run and job>
    ],
    "id": "<system generated node-id for run>",
    "sourceIdentifier": "default.redshift.create/2f41298b-1ee7-3302-
a14b-09addffa7580",
    "typeName": "amazon.datazone.JobRunLineageNodeType",
    ....
    "upstreamNodes": [
        {
            "eventTimestamp": "2024-07-24T18:08:55+08:00",
            "id": "6wf2z27c8hghev"
        },
        {
            "eventTimestamp": "2024-07-24T18:08:55+08:00",
            "id": "4tjbcsnre6banb"
        }
    ]
}
```

3. ダウンストリーム/アップストリームノード識別子 (アセットノードにリンクされているはずです) を渡すことで、データセットに対応するようにGetLineageNode再度呼び出します。

   上記のレスポンス例を使用したサンプルコマンド：

```
aws datazone get-lineage-node --domain-identifier <domain-id> --identifier
 afymge5k4v0euf
```

   これにより、データセットに対応する系統ノードの詳細 afymge5k4v0euf が返されます。

```
{
    .....
    "domainId": "dzd_cklzc5s2jcr7on",
    "downstreamNodes": [],
    "eventTimestamp": "2024-07-24T18:08:55+08:00",
    "formsOutput": [
        .....
    ],
    "id": "afymge5k4v0euf",
    "sourceIdentifier": "arn:aws:redshift:us-east-1:123456789012:table/
workgroup-20240715/tpcds_data/public/dws_tpcds_7",
    "typeName": "amazon.datazone.DatasetLineageNodeType",
    "typeRevision": "1",
    ....
    "upstreamNodes": [
        ...
    ]
}
```

4. このデータセットノードsourceIdentifierの と からのレスポンスを比較しますGetAsset。リンクされていない場合、これらは一致しないため、系統 UI に表示されません。

一致しないシナリオと緩和策

以下は、これらが一致しない一般的なシナリオと、考えられる緩和策です。

根本原因 : テーブルは Amazon DataZone ドメインアカウントのアカウントとは異なるアカウントにあります。

緩和策： 関連付けられたアカウントから PostLineageEventオペレーションを呼び出すことができます。を構築accountIdするための ARNが発信者の認証情報から選択されたら、入門スクリプト

の実行時または の呼び出し時に、テーブルを含むアカウントからロールを引き受けることができますPostLineageEvent。これにより、 ARNsを正しく構築し、アセットノードにリンクするのに役立ちます。

根本原因: ARN for Redshift テーブル/ビューには、 OpenLineage 実行イベント内の対応するデータセット情報の名前空間と名前属性に基づいて Redshift/Redshift-serverless が含まれています。

緩和: 指定された名前がクラスターまたはワークグループに属しているかどうかを知る決定論的な方法がないため、次のヒューリスティックを使用します。

- データセットに対応する「名前」に「」が含まれている場合はredshift-serverless.amazonaws.com、 の一部として redshift-serverless を使用します。それ以外の場合はARN、デフォルトで「redshift」になります。
- 上記は、ワークグループ名のエイリアスが機能しないことを意味します。

根本原因 : アップストリームデータセットがカスタムアセットに対して適切にリンクされていません。

緩和策 : データセットノードsourceIdentifierの と一致する CreateAsset/CreateAssetRevision (カスタムノードの場合は <namespace>/<name>) を呼び出して、アセットsourceIdentifierに を入力します。

Amazon のクォータ DataZone

AWS アカウントには、以前 AWS は制限と呼ばれていたデフォルトのクォータがサービスごとにあります。特に明記されていない限り、クォータはリージョンごとに存在します。

Amazon DataZone には、次のクォータと制限があります。

リソース	説明	値
データアセットタイプ	DataZone ドメインで作成できるデータアセットタイプの最大数	1,000
データアセット	Amazon DataZone ドメインで作成できるデータアセットの最大数	100 万件
用語集	ドメインで作成できるビジネス用語集の最大数	1,000
ビジネス用語集の用語	ドメインで作成できるビジネス用語集用語の最大数	10000
ドメイン内の環境	Amazon DataZone ドメイン内の環境の最大数	500
アセットあたりのアセットフィルターの数	Amazon アセットあたりの DataZone アセットフィルターの最大数	100
サブスクリプションあたりのフィルター数	Amazon DataZone サブスクリプションあたりのフィルターの最大数	5
ドメイン内のドメイン単位	Amazon ドメイン内の DataZone ドメインユニットの最大数	100

リソース	説明	値
ドメイン単位の階層レベル	ドメイン単位の階層レベルの最大数	5
ドメイン単位あたりのポリシーあたりの許可	ドメイン単位あたりのポリシーあたりのグラントの最大数	20
データ製品	DataZone ドメインで作成できるデータ製品の最大数	500,000

Amazon DataZone ユーザーガイドのドキュメント履歴

次の表に、Amazon のドキュメントリリースを示します DataZone。

変更	説明	日付
ドメイン単位	Amazon では、お客様がビジネスユニット/チームレベルの組織を作成し、ビジネスニーズに応じてポリシーを管理できるようにする、ドメイン単位と承認ポリシーと呼ばれる一連の新しいデータガバナンス機能 DataZone が導入されています。ドメインユニットを追加すると、ユーザーはビジネスユニットやチームに関連するデータアセットやプロジェクトを整理、作成、検索、検索できます。承認ポリシーを使用すると、これらのドメイン単位のユーザーは、Amazon 内でプロジェクト、用語集、およびコンピューティングリソースを使用するためのアクセスポリシーを設定できます DataZone。	2024 年 8 月 5 日
データ製品	Amazon はデータ製品 DataZone を導入します。これにより、データアセットを、特定のビジネスユースケースに合わせた明確に定義された自己完結型のパッケージにグループ化できます。例えば、マーケティング分析データ製	2024 年 8 月 5 日

	品は、マーケティングキャンペーンデータ、パイプラインデータ、顧客データなど、さまざまなデータアセットをバンドルできます。データ製品を使用すると、お客様は検出プロセスとサブスクリプションプロセスを簡素化し、ビジネス目標に合わせて調整し、個々のアセットの処理の冗長性を軽減できます。	
AmazonDataZoneDomainExecutionRolePolicy および AmazonDataZoneFullUserAccess - ポリシーの更新	Amazon DataZone ドメインユニットAmazonDataZoneDomainExecutionRolePolicyとデータ製品の作成と管理に使用される新しい のサポートAmazonDataZoneFullUserAccessを有効にするために、 と のポリシーを更新APIsしました。詳細については、「 への Amazon DataZone の更新」を参照してください。AWS マネージドポリシー 。	2024 年 8 月 5 日

きめ細かなアクセスコントロール	Amazon DataZone はきめ細かなアクセスコントロールを導入し、データレイクとデータウェアハウス全体で Amazon のビジネスデータカタログのデータアセット DataZoneをきめ細かく制御できるようになりました。新機能により、データ所有者は、データアセット全体へのアクセス権を付与するのではなく、行レベルと列レベルで特定のデータレコードへのアクセスを制限できるようになりました。例えば、データに個人を特定できる情報 (PII) などの機密情報を含む列が含まれている場合、必要な列のみへのアクセスを制限して、機密情報を保護しながら、機密性のないデータへのアクセスを許可できます。同様に、行レベルでアクセスを制御できるため、ユーザーは自分のロールまたはタスクに関連するレコードのみを表示できます。	2024 年 7 月 2 日

AmazonDataZoneGlueManageAccessRolePolicy - ポリシーの更新	ポリシーの更新 AmazonDataZoneGlueManageAccessRolePolicy - Amazon DataZone は、Lake FormationでのIAM許可付与の範囲を絞り込むために、きめ細かなアクセスコントロール機能に使用される許可を追加しています。詳細については、「 へのAmazon DataZone の更新」を参照してください。 AWS マネージドポリシー 。	2024 年 7 月 2 日

データ系統	Amazon はプレビューでデータ系統 DataZone を起動し、対応システムから、またはOpenLineageを介して系統イベントを視覚化APIし、ソースから消費へのデータ移動を追跡するのに役立ちます。Amazon DataZoneのOpenLineageと互換性のあるを使用するとAPIs、ドメイン管理者とデータプロデューサーは、Amazon S3 での変換など DataZone、Amazon で利用できるもの以外の系統イベントをキャプチャして保存できます。 AWS Glue およびその他の サービス。さらに、Amazon DataZone バージョンは各イベントに系統付けられており、ユーザーは任意の時点で系統を視覚化したり、アセットまたはジョブの履歴全体の変換を比較したりできます。この過去の系統は、データアセットの整合性のトラブルシューティング、監査、検証に不可欠な、データがどのように進化したかをより深く理解するのに役立ちます。	2024 年 6 月 27 日

AmazonDataZoneExecutionRolePolicy および AmazonDataZoneFullUserAccess - ポリシーの更新	AmazonDataZoneExecutionRolePolicy および へのポリシーの更新AmazonDataZoneFullUserAccessにより、データ系統ときめ細かなアクセスコントロール のサポートが可能になります APIs。詳細については、「 への Amazon DataZone の更新」を参照してください。AWS マネージドポリシー 。	2024 年 6 月 27 日

カスタム AWS サービス設計図	カスタム AWS 既存の がある場合は、 サービスのブループリント AWS IAM ロール、データレイク、データメッシュ、Amazon S3 バケット、Amazon Redshift クラスターなどの リソースでは、独自のカスタムIAMロールを使用してこれらの既存のリソースへのアクセス許可を指定できるようになりました。これにより、Amazon DataZone ユーザーはパブリケーションとサブスクリプションを活用してこれらのリソースを共有および管理できます。カスタム AWS サービスブループリント、Amazon DataZone 管理者は を設定できます AWS 独自のカスタムロールを使用する サービス環境。これらの のアクションリンクを設定できます。 AWS サービス環境により、既存の へのフェデレーションアクセスが提供されます。 AWS リソースの使用料金を見積もることができます。これらのカスタム でサブスクリプションターゲットとデータソースを設定することもできます。 AWS サービス環境。管理者は を設定できます AWS 独自の Amazon DataZone ドメインアカウント、またはデータを発行、サブスクライブ、検出、管理した	2024 年 6 月 17 日

	い関連アカウントの サービス環境。	
AmazonDataZoneGlueManageAccessRolePolicy - ポリシーの更新	Amazon のセルフサブスクライブ機能に必要なIAMアクセス許可AmazonDataZoneGlueManageAccessRolePolicy を追加して、レイクフォーメーションで付与されるアクセス許可の範囲を絞り込む DataZone へのポリシーの更新。セルフサブスクライブ機能を使用すると、レイクフォーメーション許可はタグ付けされたリソースにのみ付与できます。詳細については、「 への Amazon DataZone の更新」を参照してください。AWS マネージドポリシー 。	2024 年 6 月 14 日

AmazonDataZoneFullAccess - ポリシーの更新	Amazon DataZone マネジメントコンソールAmazonDataZoneFullAccess がユーザーに代わってドメインタグとプロジェクトタグの両方を使用してシークレットを作成できるようにする へのポリシーの更新。また、ドメイン所有者アカウントから管理を有効にして、関連付けられたアカウントのアカウント関連付けステータスを表示できるようにするram:ListResourceSharePermissions アクションも含まれます。詳細については、「 への Amazon DataZone の更新」を参照してください。 AWS マネージドポリシー 。	2024 年 6 月 14 日
AmazonDataZoneDomainExecutionRolePolicy - ポリシーの更新	ポリシーを に更新AmazonDataZoneDomainExecutionRolePolicy しAPIs、ユーザーが Amazon DataZone 環境のアクションを設定 DataZone できるようにする新しい を Amazon に追加しました。詳細については、「 への Amazon DataZone の更新」を参照してください。 AWS マネージドポリシー 。	2024 年 6 月 14 日

データソース作成環境	Amazon DataZone は、データソース作成フローの機能強化を追加し、データプロデューサーのアクセス管理を簡素化しました。これらの更新により、データプロデューサーがを公開するためのデータソースを作成するとき AWS Glue および Amazon Redshift アセットでは、Amazon はプロジェクトメンバーに読み取り専用アクセス許可 DataZone を付与します。を作成する場合 AWS Glue データソース、Amazon はデータソースの作成に使用される環境のIAMロールに「読み取り専用」アクセス許可 DataZone を自動的に付与し、関連付けられた 内のすべてのテーブルへのアクセスを許可します。AWS Glue データベース。同様に、Amazon Redshift データソースの場合、Amazon はデータソースで使用される Amazon Redshift スキーマ内のすべてのテーブルへの読み取り専用アクセス DataZone を許可します。	2024 年 6 月 10 日

Amazon との統合 SageMaker	Amazon は Amazon SageMaker との統合 DataZone を開始して、データプロデューサーとコンシューマーが Amazon にシームレスに切り替え SageMaker て機械学習 (ML) プロジェクトで共同作業を行い、データおよび ML アセットへのアクセスガバナンスを強制できるようにします。Amazon DataZone と Amazon の新しい組み込み統合により SageMaker、データコンシューマーとプロデューサーは、インフラストラクチャのセットアップ全体の ML ガバナンスを合理化し、ビジネスイニシアチブに共同作業を行い、データと ML アセットを簡単に管理できます。	2024 年 5 月 6 日
AmazonDataZoneSageMakerProvisioning - 新しいポリシー	という新しいポリシー DataZone は、Amazon と相互運用するために必要なアクセス許可を Amazon にAmazonDataZoneSageMakerProvisioning付与します SageMaker。詳細については、「 への Amazon DataZone の更新」を参照してください。 AWS マネージドポリシー 。	2024 年 4 月 30 日

AmazonDataZoneSageMakerEnvironmentRolePermissionsBoundary - 新しいアクセス許可の境界	という新しいアクセス許可の境界AmazonDataZoneSageMakerEnvironmentRolePermissionsBoundary 。Amazon DataZone データポータルを介して Amazon SageMaker 環境を作成すると、Amazon DataZone はこのアクセス許可の境界を環境の作成中に生成されるIAMロールに適用します。アクセス許可の境界は、Amazon が DataZone 作成するロールの範囲と、追加するロールを制限します。詳細については、「 への Amazon DataZone の更新」を参照してください。AWS マネージドポリシー 。	2024 年 4 月 30 日
AmazonDataZoneSageMakerAccess - 新しいポリシー	という新しいポリシーAmazonDataZoneSageMakerAccess は DataZone 、Amazon SageMaker 環境のさまざまなリソースへのアクセスをユーザーに許可するために必要なアクセス許可を Amazon に付与します。詳細については、「 への Amazon DataZone の更新」を参照してください。AWS マネージドポリシー 。	2024 年 4 月 30 日

AmazonDataZoneFullAccess - ポリシーの更新	コンソールでブループリントを設定するアカウント管理者が使用しやすくするための `DescribeSecurityGroups` アクションと、指定された管理AmazonDataZoneFullAccessポリシーに関する情報を取得するための `GetPolicy` アクションへのアクセスを追加するポリシーの更新。詳細については、「 への Amazon DataZone の更新」を参照してください。 AWS マネージドポリシー 。	2024 年 4 月 30 日

Lake Formation ハイブリッドアクセスモード	Amazon DataZone は との統合を導入しました AWS Lake Formation ハイブリッドアクセスモード。この統合により、 を簡単に公開および共有できます。 AWS で登録しなくても DataZone、Amazon を介してテーブルを Glue で登録できます。 AWS Lake Formation を最初に使用します。開始するには、管理者は Amazon DataZone コンソールのDefaultDataLake ブループリントでデータロケーション登録設定を有効にします。次に、データコンシューマーが にサブスクライブすると、 AWS アクセスIAM許可によって管理される Glue テーブル。Amazon DataZone はまずこのテーブルの Amazon S3 ロケーションをハイブリッドモードで登録し、 を介してテーブルに対するアクセス許可を管理することでデータコンシューマーへのアクセスを許可します。 AWS Lake Formation。これにより、新しく付与された でテーブルに対するIAMアクセス許可が引き続き存在するようになります。 AWS 既存のワークフローを中断することなく、Lake Formation のアクセス許可。詳細については、「Amazon と AWS Lake	2024 年 4 月 3 日

	Formation ハイブリッドモード DataZone の統合」を参照してください。	
データ品質	Amazon が との統合 DataZone を開始 AWS Glue Data Quality と はAPIs、サードパーティーのデータ品質ソリューションのデータ品質メトリクスを統合するための を提供しています。新しい統合により、自動発行が可能になります。 AWS Data Quality スコアを Amazon DataZone ビジネスデータカタログにまとめます。Amazon DataZone APIs は、サードパーティーのソースから品質メトリクスを取り込むために使用できます。公開されると、データコンシューマーはデータアセットの検索、品質メトリクスの詳細な表示、失敗したチェックとルールの特定を簡単に行えるようになり、ビジネス上の意思決定に役立ちます。詳細については、「Amazon のデータ品質 DataZone」を参照してください。	2024 年 4 月 3 日

AmazonDataZoneS3Manage - <region>-<domainId> - 新しいロール	Amazon AmazonDataZone が を呼び出すときに使用される S3Manage -<region>-<domainId > と呼ばれる新しいロール DataZone AWS Amazon Simple Storage Service (Amazon S3) ロケーションを登録する Lake Formation。 AWS Lake Formation は、その場所のデータにアクセスするときにこのロールを引き受けます。詳細については、「 への Amazon DataZone の更新」を参照してください。 AWS マネージドポリシー 。	2024 年 4 月 1 日
AmazonDataZoneGlue ManageAccessRolePolicy - ポリシーの更新	を更新AmazonDataZoneGlue ManageAccessRolePolicyして、Amazon がデータ DataZone への発行とアクセス許可を有効にできるようにするアクセス許可のサポートを有効にしました。詳細については、「 への Amazon DataZone の更新」を参照してください。 AWS マネージドポリシー 。	2024 年 4 月 1 日

AmazonDataZoneDomainExecutionRolePolicy および AmazonDataZoneFullUserAccess - ポリシーの更新	AmazonDataZoneDomainExecutionRolePolicy と を更新AmazonDataZoneFullUserAccessして、`CancelMetadataGenerationRun` のサポートを有効にしましたAPI。詳細については、「 への Amazon DataZone の更新」を参照してください。 AWS マネージドポリシー 。	2024 年 3 月 29 日
AmazonDataZoneFullAccess - ポリシーの更新	Amazon は、ビジネスデータカタログを強化することで、データ検出、データ理解、データ使用量を向上させるための新しい生成 AI ベースの機能の一般提供リリース DataZone を発表しました。ワンクリックで、データプロデューサーは包括的なビジネスデータの説明とコンテキストを生成し、影響のある列を強調し、分析ユースケースに関するレコメンデーションを含めることができます。起動により、データプロデューサーAPIsがアセットの説明をプログラムで生成するために使用できる のサポートが追加されました。	2024 年 3 月 27 日

AmazonDataZoneFullAccess - ポリシーの更新	Amazon DataZone では、Amazon Redshift の統合にいくつかの機能強化が導入され、Amazon Redshift テーブルとビューの公開とサブスクライブのプロセスが簡素化されました。これらの更新により、データプロデューサーとコンシューマーの両方のエクスペリエンスが効率化され、Amazon DataZone 管理者が提供する事前設定された認証情報と接続パラメータを使用してデータウェアハウス環境をすばやく作成できます。さらに、これらの機能強化により、管理者は自分の 内のリソースを使用できるユーザーをより詳細に制御できます。AWS アカウントと Amazon Redshift クラスター、および目的。	2024 年 3 月 21 日
AmazonDataZoneFullAccess - ポリシーの更新	ユーザーがテキストボックスに入力するのではなく、Amazon DataZone マネジメントコンソールでシークレット、クラスター、vpc の 、サブネットを選択AmazonDataZoneFullAccess できるように を更新しました。詳細については、「 への Amazon DataZone の更新」を参照してください。 AWS マネージドポリシー 。	2024 年 3 月 13 日

AmazonDataZoneDomainExecutionRolePolicy - ポリシーの更新	を更新AmazonDataZoneDomainExecutionRolePolicyして、どのアカウントとリージョンでどのブループリントが有効になっているかを特定することで、環境プロファイルの作成に必要な のサポート ListEnvironmentBlueprintConfigurationSummaries APIを有効にしました。詳細については、「 への Amazon DataZone の更新」を参照してください。 AWS マネージドポリシー 。	2024 年 2 月 1 日
Cloud Formation の使用の強化	Amazon のユーザーが DataZone を利用できるようになりました AWS CloudFormation Amazon DataZone リソースのスイートを効果的にモデル化および管理するための 。このアプローチにより、 リソースの一貫したプロビジョニングが容易になり、コードプラクティスとしてのインフラストラクチャによるライフサイクル管理も可能になります。カスタムテンプレートを使用すると、必要なリソースとその相互依存関係を正確に定義できます。詳細については、「Amazon DataZone リソースタイプのリファレンス」を参照してください。	2024 年 1 月 18 日

カスタムアセット	カスタムアセットのサポートにより、Amazon DataZone はデータポータルを介してダッシュボード、クエリ、モデルなどの非構造化データ用にアセットをカタログ化できるため、以前に利用可能なAPIサポートとともに、カスタムアセットをデータポータルに直接追加することが容易になります。Amazon でカスタムアセットを作成、更新、公開する機能により DataZone、あらゆる種類のアセットを共有、検索、サブスクライブし、それらのアセットのガバナンスを提供するビジネスワークフローを構築できます。詳細については、「カスタムアセットタイプの作成」を参照してください。	2024 年 1 月 5 日

プリンIAMシパルをプロジェクトメンバーとして追加する	プリンIAMシパルがまだ Amazon にログインしていない場合でも DataZone （以前の要件）、IAMプリンシパルをプロジェクトメンバーとして追加できるようになりました。ドメイン管理者または IT 管理者がドメインのドメイン実行ロール`iam:GetRole` に `iam:GetUser` と を追加した後、プロジェクト所有者はIAM、ロールまたはIAMユーザーの Amazon リソース名 (ARN) を指定するだけで、プリンIAMシパルをメンバーとして追加できます。IAM プリンシパルには、Amazon へのアクセスに必要なアクセスIAM許可が依然として必要です。アクセス許可は DataZone 、IAMコンソールで設定できます。詳細については、「プロジェクトにメンバーを追加する」を参照してください。	2024 年 1 月 5 日

ドメインの削除	ドメインの削除は、ドメインをより簡単に削除できる機能です。これで、ドメインが空でなくても (にプロジェクト、環境、アセット、データソースなどが含まれているように) 、ドメインの削除を続行できます。詳細については、「Amazon DataZone ドメインの削除」を参照してください。	2023 年 12 月 27 日
Lake Formation ハイブリッドモード	Amazon DataZone が のサポートを追加 AWS Lake Formation ハイブリッドモード。このサポートにより、 を公開する場合 AWS Glue テーブルを DataZone で Amazon に AWS Lake Formation でハイブリッドモードで登録された S3 口ケーション。Amazon はこのテーブルをマネージドアセットとして DataZone 扱い、このテーブルへのサブスクリプション許可を管理できます。この機能リリース以前 DataZone は、Amazon はこのテーブルをアンマネージドアセットとして扱い DataZone ます。つまり、Amazon はこのテーブルにサブスクリプションを付与できません。詳細については、「Amazon の Lake Formation アクセス許可 DataZoneを設定する」を参照してください。	2023 年 12 月 22 日

HIPAA コンプライアンス	Amazon DataZone は、1996 年米国の医療保険の相互運用性と説明責任に関する法律 (HIPAA) に準拠するようになりました。のリストを表示するには AWS HIPAA コンプライアンスを備えた のサービスについては、https://aws.amazon.com/compliance/hipaa-eligible-services-reference「/」を参照してください。	2023 年 12 月 14 日
AmazonDataZoneGlueManageAccessRolePolicy - ポリシーの更新	のサポートを有効にするAmazonDataZoneGlueManageAccessRolePolicyように を更新しました AWS Lake Formation ハイブリッドモード。詳細については、「 への Amazon DataZone の更新」を参照してください。 AWS マネージドポリシー 。	2023 年 12 月 14 日
AmazonDataZoneFullUserAccess および AmazonDataZoneDomainExecutionRolePolicy - ポリシーの更新	Amazon は、Amazon の生成 AI を活用したデータ記述機能をサポートするように AmazonDataZoneFullUserAccessおよび AmazonDataZoneDomainExecutionRolePolicyポリシー DataZone を更新しました DataZone。詳細については、「 への Amazon DataZone の更新」を参照してください。 AWS マネージドポリシー 。	2023 年 11 月 28 日

AI レコメンデーション	AWS は、Amazon で新しい生成 AI ベースの機能のプレビューを発表しました。これにより、ビジネスデータカタログを強化することで、データ検出、データ理解、データ使用量 DataZone が向上します。ワンクリックで、データプロデューサーは包括的なビジネスデータの説明とコンテキストを生成し、影響のある列を強調し、分析ユースケースに関するレコメンデーションを含めることができます。Amazon での説明に関する AI レコメンデーションを使用すると DataZone、データコンシューマーは分析に必要なデータテーブルと列を特定できるため、データ検出性が向上し、データプロデューサーとの back-and-forth 通信が削減されます。プレビューは、次でプロビジョニングされた Amazon DataZone ドメインで利用できます。 AWS リージョン: 米国東部 (バージニア北部) 、米国西部 (オレゴン) 。詳細については、「機械学習と生成 AI の使用」を参照してください。	2023 年 11 月 28 日

DefaultDataLake ブループリント	Amazon DataZone は、 からどのデータを公開できるかをより適切に制御できる拡張機能を DefaultDataLake ブループリントに追加しました。AWS アカウント。この機能の起動に伴って導入された主な変更点が 2 つあります。	2023年11月20日
AmazonDataZoneEnvironmentRolePermissionsBoundary - ポリシーの更新	Amazon DataZone は、`ResourceTag` 条件でスコープダウンされた追加の`athena:GetQueryResultsStream` アクセス許可で構成される AmazonDataZoneEnvironmentRolePermissionsBoundaryマネージドポリシーを更新しました。詳細については、「 への Amazon DataZone の更新」を参照してください。 AWS マネージドポリシー 。	2023 年 11 月 17 日

AmazonDataZoneRedshiftManageAccessRolePolicy - ポリシーの更新	Amazon は、 `redshift:AssociateDataShareConsumer` アクションの組織 ID のチェックを削除してAmazonDataZoneRedshiftManageAccessRolePolicyポリシー DataZone を更新しました。これにより、 間でリソースを共有できます。 AWS 組織。詳細については、「 への Amazon DataZone の更新」を参照してください。 AWS マネージドポリシー 。	2023 年 11 月 16 日
ユーザーガイドの GA リリース	Amazon ユーザーガイドの一般提供 (GA) DataZone リリース。	2023 年 10 月 15 日
AmazonDataZoneFullUserAccess - ポリシーの更新	Amazon は、Amazon へのフルアクセスを許可するAmazonDataZoneFullUserAccessポリシー DataZone を更新しましたが DataZone、ドメイン、ユーザー、または関連するアカウントの管理は許可しません。詳細については、「 への Amazon DataZone の更新」を参照してください。 AWS マネージドポリシー 。	2023 年 10 月 2 日

AmazonDataZonePreviewConsoleFullAccess - ポリシーは廃止されました	Amazon は を DataZone 非推奨にしましたAmazonDataZonePreviewConsoleFullAccess。詳細については、「 の Amazon DataZone アップデート」を参照してください。 AWS マネージドポリシー 。	2023 年 9 月 29 日
AmazonDataZonePortalFullAccessPolicy - ポリシーは廃止されました	Amazon は を DataZone 非推奨にしましたAmazonDataZonePortalFullAccessPolicy。詳細については、「 の Amazon DataZone アップデート」を参照してください。 AWS マネージドポリシー 。	2023 年 9 月 29 日

AmazonDataZoneDomainExecutionRolePolicy - 新しいポリシー	Amazon は、 という新しいポリシー DataZone を追加しましたAmazonDataZoneDomainExecutionRolePolicy。これは Amazon DataZone `AmazonDataZoneDomainExecutionRole` サービスロールのデフォルトポリシーです。このロールは、Amazon DataZone ドメイン内のデータをカタログ化、検出、管理、共有、分析 DataZone するために Amazon によって使用されます。`AmazonDataZoneDomainExecutionRolePolicy` ポリシーを にアタッチできます `AmazonDataZoneDomainExecutionRole` 。詳細については、「 への Amazon DataZone の更新」を参照してください。 AWS マネージドポリシー 。	2023 年 9 月 25 日
AmazonDataZoneCrossAccountAdmin - 新しいポリシー	Amazon は、ユーザーが Amazon DataZone および関連するアカウントを使用AmazonDataZoneCrossAccountAdminできるようにする という新しいポリシー DataZone を追加しました。詳細については、「 への Amazon DataZone の更新」を参照してください。 AWS マネージドポリシー 。	2023 年 9 月 19 日

AmazonDataZoneRedshiftManageAccessRolePolicy - 新しいポリシー	Amazon は、Amazon AmazonDataZoneRedshiftManageAccessRolePolicy がデータへの発行とアクセス許可を有効にするためのアクセス許可 DataZone を付与する という新しいポリシー DataZone を追加しました。詳細については、「 への Amazon DataZone の更新」を参照してください。 AWS マネージドポリシー 。	2023 年 9 月 12 日
AmazonDataZoneRedshiftGlueProvisioningPolicy - 新しいポリシー	Amazon は、サポートされているデータソースとの相互運用に必要なアクセス許可を Amazon DataZone に付与AmazonDataZoneRedshiftGlueProvisioningPolicyする という新しいポリシー DataZone を追加しました。詳細については、「 への Amazon DataZone の更新」を参照してください。 AWS マネージドポリシー 。	2023 年 9 月 12 日

AmazonDataZoneGlueManageAccessRolePolicy - 新しいポリシー	Amazon は、 という新しいポリシー DataZone を追加し、Amazon DataZone に発行するアクセス許可AmazonDataZoneGlueManageAccessRolePolicyを付与します。AWS データをカタログに Glue します。また、 へのアクセスを許可または取り消すためのアクセス許可を Amazon DataZone に付与します。 AWS Glue がカタログに公開したアセット。詳細については、「 への Amazon DataZone の更新」を参照してください。 AWS マネージドポリシー 。	2023 年 9 月 12 日
AmazonDataZoneFullUserAccess - 新しいポリシー	Amazon は、 データポータル DataZone 経由で Amazon へのフルアクセスを許可する AmazonDataZoneFullUserAccess という新しいポリシー DataZone を追加しました。詳細については、「 への Amazon DataZone の更新」を参照してください。 AWS マネージドポリシー 。	2023 年 9 月 12 日

AmazonDataZoneFullAccess - 新しいポリシー	Amazon は、 DataZone 経由で Amazon へのフルアクセスAmazonDataZoneFullAccessを提供する という新しいポリシー DataZone を追加しました。 AWS マネジメントコンソール。詳細については、「 への Amazon DataZone の更新」を参照してください。 AWS マネージドポリシー 。	2023 年 9 月 12 日
AmazonDataZoneEnvironmentRolePermissionsBoundary - 新しいポリシー	Amazon は、それがアタッチされているプロビジョニングされたIAMプリンシパルAmazonDataZoneEnvironmentRolePermissionsBoundaryを制限する という新しいポリシー DataZone を追加しました。詳細については、「 への Amazon DataZone の更新」を参照してください。 AWS マネージドポリシー 。	2023 年 9 月 12 日
マネージドポリシーの更新	AmazonDataZonePreviewConsoleFullAccess 管理ポリシーの更新。詳細については、「 への Amazon DataZone の更新」を参照してください。 AWS マネージドポリシー 。	2023 年 6 月 13 日

マネージドポリシーの更新	AmazonDataZoneProjectDeploymentPermissionsBoundary 管理ポリシーの更新。詳細については、「 への Amazon DataZone の更新」を参照してください。AWS マネージドポリシー 。	2023 年 4 月 3 日
???	Amazon DataZone （プレビュー) ユーザーガイドの初回リリース。	2023 年 3 月 29 日

翻訳は機械翻訳により提供されています。提供された翻訳内容と英語版の間で齟齬、不一致または矛盾がある場合、英語版が優先します。