



ユーザーガイド

# Amazon DataZone



# Amazon DataZone: ユーザーガイド

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

Amazon の商標とトレードドレスは、Amazon 以外の製品またはサービスとの関連において、顧客に混乱を招いたり、Amazon の名誉または信用を毀損するような方法で使用することはできません。Amazon が所有しない他の商標はすべてそれぞれの所有者に帰属します。所有者は必ずしも Amazon との提携や関連があるわけではありません。また、Amazon の支援を受けているとはかぎりません。

# Table of Contents

Amazon とは DataZone .....	1
.....	1
Amazon が他の AWS のサービス DataZone をどのようにサポートし、統合するか。 .....	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
Amazon の新機能 DataZone .....	17
2024 .....	17
Amazon がデータシステム機能 DataZone を起動 .....	17
Amazon がカスタム AWS サービスブループリント DataZone を起動 .....	17
データソース作成フローの強化 .....	18
Amazon が Amazon との統合 DataZone を開始 SageMaker .....	18
Amazon が AWS Lake Formation ハイブリッドアクセスモードとの統合 DataZone を開 始 .....	18
Amazon が AWS Glue Data Quality との統合 DataZone を開始 .....	18
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 .....	19
Amazon が Amazon Redshift 統合の機能強化 DataZone を開始 .....	19
AWS Amazon の Cloud Formation サポート DataZone .....	20
Amazon DataZone プロジェクトのメンバーとして IAM プリンシパルを直接追加する .....	21
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 .....	21
2023 .....	21
ドメインの削除 .....	21
ハイブリッドモード .....	22
HIPAA 適格性 .....	22
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) .....	22

DefaultDataLake ブループリントの拡張 .....	23
セットアップ .....	24
AWS アカウントにサインアップする .....	24
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 .....	25
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 .....	25
IAM アクセス許可のカスタムポリシーを作成して、Amazon DataZone サービスコンソールのロール作成を簡素化する .....	26
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 .....	28
( オプション) AWS Identity Center アクセス許可のカスタムポリシーを作成して、ドメインのシングルサインオン (SSO) を有効にする .....	30
( オプション) AWS Identity Center のアクセス許可のカスタムポリシーを作成して、Amazon DataZone 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します。 .....	31
( オプション) IAM プリンシパルをキーユーザーとして追加し、Key Management Service (KMS) のカスタマーマネージドキーを使用して Amazon AWS DataZone ドメインを作成します。 .....	33
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 .....	33
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 .....	34
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 .....	35
ドメインが AWS Key Management Service (KMS) 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 .....	36
Amazon 用 AWS IAM Identity Center のセットアップ DataZone .....	37
開始 .....	39
AWS Glue データを使用した Amazon DataZone クイックスタート .....	39
ステップ 1 - Amazon DataZone ドメインとデータポータルを作成する .....	40
ステップ 2 - 公開プロジェクトを作成する .....	42
ステップ 3 - 環境を作成する .....	42
ステップ 4 - 公開用のデータを生成する .....	43
ステップ 5 - Glue から AWS メタデータを収集する .....	44
ステップ 6 - データアセットをキュレートして公開する .....	44

ステップ 7 - データ分析用のプロジェクトを作成する .....	44
ステップ 8 - データ分析用の環境を作成する .....	45
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 .....	45
ステップ 10 - サブスクリプションリクエストを承認する .....	46
ステップ 11 - Amazon Athena でクエリを構築し、データを分析する .....	46
Amazon Redshift データを使用した Amazon DataZone クイックスタート .....	46
ステップ 1 - Amazon DataZone ドメインとデータポータルを作成する .....	47
ステップ 2 - 公開プロジェクトを作成する .....	48
ステップ 3 - 環境を作成する .....	49
ステップ 4 - 公開用のデータを生成する .....	50
ステップ 5 - Amazon Redshift からメタデータを収集する .....	51
ステップ 6 - データアセットをキュレートして公開する .....	51
ステップ 7 - データ分析用のプロジェクトを作成する .....	51
ステップ 8 - データ分析用の環境を作成する .....	52
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 .....	53
ステップ 10 - サブスクリプションリクエストを承認する .....	53
ステップ 11 - Amazon Redshift でクエリを構築し、データを分析する .....	53
サンプルスクリプトを使用した Amazon DataZone クイックスタート .....	54
Amazon DataZone ドメインとデータポータルを作成する .....	54
公開プロジェクトを作成する .....	55
環境プロファイルを作成する .....	55
環境の作成 .....	57
AWS Glue からメタデータを収集する .....	58
データアセットをキュレートして公開する .....	61
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 .....	64
その他の便利なサンプルスクリプト .....	66
Amazon DataZone ドメインとユーザーアクセスの管理 .....	68
ドメインの作成 .....	68
ドメインの編集 .....	70
ドメインの削除 .....	71
Amazon の IAM Identity Center を有効にする DataZone .....	72
Amazon 用 IAM Identity Center を無効にする DataZone .....	73
Amazon DataZone コンソールでユーザーを管理する .....	74
IAM ロールとユーザーの管理 .....	75
SSO ユーザーを管理する .....	76
SSO グループの管理 .....	77

Amazon DataZone データポータルでのユーザーアクセス許可の管理 .....	79
Amazon DataZone 組み込みブループリントの使用 .....	80
Amazon DataZone ドメインを所有するアカウントで AWS 組み込みブループリントを有効にする .....	80
Amazon DataZone ドメインを所有する AWS アカウントに Amazon を信頼されたサービス SageMaker として追加する .....	86
Amazon でのカスタム AWS サービスブループリントの使用 DataZone .....	87
カスタム AWS サービスブループリントを有効にする .....	87
カスタム AWS サービスブループリントを使用して環境を作成する .....	88
カスタム AWS サービス環境でアクションを作成する .....	89
カスタム AWS サービス環境にプロジェクトメンバーを追加する .....	89
AWS サービス環境でデータソースを設定する .....	90
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 .....	90
関連するアカウントを使用してデータを発行および使用する .....	92
他の AWS アカウントとの関連付けをリクエストする .....	92
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 .....	93
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 .....	94
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 .....	95
関連付けられた AWS アカウントで環境ブループリントを有効にする .....	95
関連付けられた AWS アカウントに Amazon を信頼されたサービス SageMaker として追加する .....	101
関連付けられたアカウントを削除する .....	101
Amazon DataZone データカタログの使用 .....	102
ビジネス用語集を作成、編集、削除する .....	102
用語集で用語を作成、編集、削除する .....	104
メタデータフォームの作成、編集、削除 .....	106
メタデータフォームのフィールドを作成、編集、削除する .....	107
Amazon でのプロジェクトと環境の使用 DataZone .....	110
環境プロファイルを作成する .....	110
環境プロファイルを編集する .....	113
環境プロファイルを削除する .....	114
新しい環境を作成する .....	115
環境を編集する .....	116
環境を削除する .....	116
の新規プロジェクトの作成 .....	117

プロジェクトの編集 .....	117
プロジェクトを削除する .....	118
プロジェクトを離れる .....	119
プロジェクトにメンバーを追加する .....	120
プロジェクトからメンバーを削除する .....	121
Amazon でのインベントリの作成とデータの公開 DataZone .....	123
Amazon の Lake Formation アクセス許可を設定する DataZone .....	124
Amazon と AWS Lake Formation ハイブリッドモード DataZone の統合 .....	125
カスタムアセットタイプを作成する .....	128
のデータソースを作成して実行する AWS Glue Data Catalog .....	133
Amazon Redshift のデータソースを作成して実行する .....	135
既存のデータソースの管理 .....	138
データソースを編集する .....	139
データソースの削除 .....	139
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 .....	140
アセットを公開する .....	141
インベントリの管理とアセットのキュレート .....	141
追加のメタデータフォームをアセットにアタッチする .....	143
キュレーション後にカタログにアセットを発行する .....	143
アセットを手動で作成する .....	144
カタログからアセットを公開解除する .....	145
アセットを削除する .....	145
データソースの実行を手動で開始する .....	146
アセットのバージョニング .....	147
Amazon のデータ品質 DataZone .....	148
AWS Glue アセットのデータ品質の有効化 .....	148
カスタムアセットタイプのデータ品質の有効化 .....	149
機械学習と生成 AI の使用 .....	151
Amazon のデータシステム DataZone (プレビュー) .....	153
Amazon のシステムノードのタイプ DataZone .....	154
システムノードの主要な属性 .....	155
データシステムの視覚化 .....	156
Amazon でのデータシステム認証 DataZone .....	157
Amazon でのデータシステムサンプルエクスペリエンス DataZone .....	157
Amazon DataZone データシステムをプログラムで使用する .....	158
Amazon でのデータの検出、サブスクライブ、消費 DataZone .....	159

データの検出 .....	159
カタログでアセットを検索して表示する .....	160
データへのサブスクライブ .....	161
アセットへのサブスクリプションをリクエストする .....	161
サブスクリプションリクエストを承認または拒否する .....	162
既存のサブスクリプションを取り消す .....	163
サブスクリプションリクエストをキャンセルする .....	164
アセットのサブスクリプションを解除する .....	165
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 .....	165
データへのアクセスの許可 .....	168
マネージド AWS Glue Data Catalog アセットへのアクセスを許可する .....	169
マネージド Amazon Redshift アセットへのアクセスを許可する .....	170
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 .....	171
データの消費 .....	172
Amazon Athena または Amazon Redshift でデータをクエリする .....	172
Amazon DataZone イベントと通知の使用 .....	177
Amazon DataZone データポータル専用受信トレイを介したイベントの操作 .....	177
Amazon EventBridge デフォルトバスによるイベントの操作 .....	184
セキュリティ .....	187
データ保護 .....	188
データ暗号化 .....	189
転送中の暗号化 .....	189
ネットワーク間トラフィックのプライバシー .....	189
Amazon の保管時のデータ暗号化 DataZone .....	189
Amazon のインターフェイス VPC エンドポイントの使用 DataZone .....	198
Amazon での認可 DataZone .....	198
Amazon DataZone コンソールでの承認 .....	199
Amazon DataZone ポータルでの承認 .....	199
Amazon DataZone プロファイルとロール .....	200
アクセスの制御 .....	200
AWS マネージドポリシー .....	201
Amazon の IAM ロール DataZone .....	293
一時認証情報 .....	302
プリンシパル権限 .....	303
コンプライアンス検証 .....	303
セキュリティのベストプラクティス .....	304

最小特権アクセスの実装 .....	305
IAM ロールの使用 .....	305
依存リソースでのサーバー側の暗号化の実装 .....	305
CloudTrail を使用して API コールをモニタリングする .....	305
耐障害性 .....	306
データソースの耐障害性 .....	306
アセットレジリエンス .....	307
アセットタイプとメタデータフォームの耐障害性 .....	307
用語集の耐障害性 .....	307
グローバル検索の耐障害性 .....	307
サブスクリプションの耐障害性 .....	308
環境レジリエンス .....	308
環境設計図の耐障害性 .....	308
プロジェクトの耐障害性 .....	308
RAM の耐障害性 .....	308
ユーザープロファイル管理の耐障害性 .....	309
ドメインレジリエンス .....	309
Amazon のインフラストラクチャセキュリティ DataZone .....	309
Amazon でのサービス間の混乱した代理の防止 DataZone .....	309
for Amazon での設定と脆弱性の分析 DataZone .....	310
許可リストに追加するドメイン .....	311
モニタリング .....	312
イベントのモニタリング .....	312
CloudTrail ログ .....	313
の Amazon DataZone 情報 CloudTrail .....	313
トラブルシューティング .....	315
Amazon の AWS Lake Formation 許可のトラブルシューティング DataZone .....	315
クォータ .....	319
ドキュメント履歴 .....	320
.....	cccxxiv

# Amazon とは DataZone

Amazon DataZone は、オンプレミス、およびサードパーティーのソースに保存されたデータのカatalog化、検出 AWS、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。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、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。

## トピック

- [Amazon で何ができますか DataZone ?](#)
- [Amazon が他の AWS のサービス DataZone をどのようにサポートし、統合するか。](#)
- [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、個々の認証情報に依存することなく、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、オンプレミス、またはサードパーティープロバイダーに保存されているカatalog化されたデータを検索 AWS、共有、およびアクセスできます。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 AWS のサービス DataZone をどのようにサポートし、統合するか。

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

- プロデューサーデータソース - AWS Glue Data DataZone Catalog および Amazon Redshift テーブルとビューに保存されているデータから Amazon カタログにデータアセットを発行できます。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、Lake Formation マネージド AWS Glue テーブルと Amazon Redshift テーブルおよびビューへのアクセス AWS の付与をサポートしています。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、カスタム統合用の他の AWS サービスまたはサードパーティソリューションと統合できます。

## 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、AWS IAM

Identity Center ( AWS SSO の後継) または IAM 認証情報を使用して、ID プロバイダーからの認証情報でユーザーを認証できます。データポータル URL は、<https://console.aws.amazon.com/datazone> の Amazon DataZone コンソールにアクセスして取得できます。

- Amazon DataZone HTTPS API

Amazon DataZone HTTPS API を使用して DataZone プログラムで Amazon にアクセスできます。これにより、HTTPS リクエストをサービスに直接発行できます。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 の使用を開始する際には 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リプション** - 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、AWS 分析へのアクセスを簡素化します。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、特定の一連の IAM プリンシパル (寄稿者アクセス許可を持つユーザーなど) が操作できる 0 個以上の設定済みリソース (Amazon S3 バケット、AWS Glue データベース、Amazon Athena ワークグループなど) のコレクションです。
- データポータル (AWS マネジメントコンソール外) - 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、IAM 認証情報または 経由で ID プロバイダーからの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 AWS アカウントを Amazon DataZone ドメインに関連付けることで、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、0 個以上の設定済みリソース (Amazon S3、AWS Glue データベース、Amazon Athena ワークグループなど) のコレクションであり、そ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が含まれます。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、環境がデプロイされる AWS アカウント やリージョンなどの設定を定義します。

## 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、環境が属するプロジェクトのどの AWS ツールやサービス (AWS Glue Amazon Redshift など) メンバーが Amazon DataZone カタログのアセットを操作するとき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	<p>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。</p> <p>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 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。</p> <p>プロデューサーとして、Amazon DataZone プロ</p>	<p>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、「読み取り専用」Lake Formation 許可を持つ AWS Glue データベース、「読み取り専用」IAM 許可を持つデータベース、および「作成」および「付与」Lake Formation 許可を持つ project. AWS Glue database によって管理される Amazon S3 へのアクセス、「読み取り」および「書き込み」IAM 許可、タグ付け付き</p>

設計図名	説明	作成されたりソース
	<p>ジェクトメンバーが 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るようにします。</p>	<p>の AWS Glue ETL (抽出、変換、ロード)。</p>
データウェアハウスの設計図	<p>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。</p> <p>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。</p>	<p>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。</p>

設計図名	説明	作成されたりソース
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 で機械学習 (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。また、設定に従って AWS Glue データベースとレイクフォーメーションをサブスクライブして公開することもできます。

組み込みのブループリントに加えて、組織で既にセットアップされている独自の既存の IAM ロールと AWS サービスを使用する DataZone ように Amazon を設定できるカスタム AWS シーラスブループリントを有効にすることもできます。詳細については、「[Amazon でのカスタム AWS サービスブループリントの使用 DataZone](#)」を参照してください。

## 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。

- データポータルを介して、または Amazon DataZone APIs。Amazon の現在のリリースでは DataZone、AWS Glue と Amazon Redshift のデータソースを作成して実行できます。AWS Glue または Amazon Redshift データソースを作成して実行することで、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。
- APIs を使用して、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アセットを作成できます。
  - Amazon 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 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。これは、データポータルまたは Amazon DataZone APIs を使用して実行できます。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 API を使用して、プロジェクトインベントリアセットを Amazon DataZone カタログに手動で発行します。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 AWS Glue アセットをカタログに発行するか、Amazon Redshift アセットをカタログ設定に発行して、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、データポータル経由で、または Amazon DataZone APIs を使用してデータソースで使用できます。

## 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、AWS Lake Formation または Amazon Redshift で必要な許可を作成して、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。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 テーブルとビューが含まれます)。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。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できる `updateSubscriptionStatus` API DataZone も提供します。DataZone これにより、Amazon はプロジェクトメンバーにアセットの消費を開始できることを通知 DataZone できます。

# 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 Amazon DataZone を AWS アカウントにインストールし、Amazon DataZone ドメインを作成し、Amazon DataZone ドメインとの AWS アカウントの関連付けと ID プロバイダーの関連付けを設定します。ドメイン管理者は、AWS Organization や AWS Service Catalog などの他のサービスコンソールを使用して Amazon を設定します DataZone。

- Amazon DataZone (アセットパブリッシャーとサブスクライバー) の分析タスクと機械学習タスクの主要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して参加し、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して消費し、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。カタログ同期とサブスクリプションは、内部カタログと統合するためのフルフィルメントアダプター、または必要に応じて Amazon DataZone APIs と内部ユーザーインターフェイスまたは本番稼働システムの統合を可能にします。

- 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 DataZone ドメインを作成する場合でも、複数のデータゾー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。また、異なるビジネスユニットやチーム用のドメインも柔軟に反映できます。

## 関連付けられたアカウント

AWS アカウントを Amazon DataZone ドメインに関連付けると、これらの AWS アカウントのデータを Amazon DataZone カタログに公開し、複数の AWS アカウントでデータを操作するための Amazon DataZone プロジェクトを作成できます。アカウント関連付けリクエストは、Amazon DataZone ドメインを所有する AWS アカウントでのみ開始できます。アカウント関連付けリクエストは、招待された AWS アカウントの管理ユーザーのみが受け入れることができます。AWS アカウントが Amazon DataZone ドメインに関連付けられていると、このアカウントの AWS Glue カタログや Amazon Redshift などのデータソースをこのドメインに登録できます。また、関連付けられると、AWS アカウントは Amazon DataZone プロジェクトと環境を作成できます。

は、1 つ以上の Amazon DataZone ドメインに関連付ける AWS アカウント 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、AWS Glue と Amazon Redshift のデータソースを作成して実行できます。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) 間の接続を確立します。これにより、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時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、自動化 (データソー

スが最初に作成されたときに開始) することも、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と列に追加して、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形式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、ビジネス用語集のフィールド値データ型をサポートしています。

ドメイン管理者は、メタデータフォームをドメインに追加して、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、Amazon Athena ワークグループなど) のコレクションで、そ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) を持ちます。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による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 AWS サービス、外部 IDEs、コンソールに保存できるように設計されています。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。プロジェクトの SSO ユーザーと 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、環境が属するプロジェクトのどの AWS ツールやサービス (AWS Glue Amazon Redshift など) メンバーが Amazon DataZone カタログのアセットを操作するとき使用できるかを定義します。

Amazon の現在のリリースでは DataZone、次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
- カスタム AWS サービスの設計図

## 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 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 SSO 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初期管理 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、使用したい Amazon DataZone プロジェクトです。

### AWS アカウント 所有者

Amazon では DataZone、AWS アカウント 所有者はロール、ポリシー、アクセス許可 AWS アカウント を作成し、これら AWS アカウント を Amazon DataZone ドメインに関連付けることができます。

# 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、OpenLineage対応システムから、または API を通じて系統イベントを視覚化し、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互換 APIs を使用すると、ドメイン管理者とデータプロデューサーは、Amazon S3 DataZone、AWS Glue、その他の サービスでの変換など、Amazon で利用可能な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。Amazon S3 さらに、Amazon DataZone バージョンは各イベントに系統を置き、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 AWS サービスブループリント DataZone を起動

06/17/2024 にリリース

カスタム AWS サービスブループリントでは、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 クラスターなどの既存の AWS リソースがある場合、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し、管理できます。カスタム AWS サービスブループリントを使用すると、Amazon DataZone 管理者は独自のカスタムロールを使用して AWS サービス環境を設定できます。これらの AWS サービス環境のアクションリンクを設定し、既存の AWS リソースへのフェデレーションアクセスを提供できます。これらのカスタム AWS サービス環境でサブ

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。管理者は、独自の Amazon DataZone ドメインアカウント、またはデータの公開、サブスクライブ、検出、管理を行う関連アカウントに AWS サービス環境を設定できます。詳細については、「[Amazon でのカスタム AWS サービスブループリントの使用 DataZone](#)」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 AWS Glue および Amazon Redshift アセットを発行するためのデータソースを作成すると、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。AWS Glue データソースを作成すると、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、関連する AWS Glue データベース内のすべてのテーブルへのアクセスを許可します。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 で機械学習 (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。詳細については、「[Amazon DataZone 組み込みブループリントの使用](#)」および「[関連するアカウントを使用してデータを発行および使用する](#)」を参照してください。

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

04/03/2024 にリリース

Amazon DataZone は Lake Formation AWS ハイブリッドアクセスモードとの統合を導入しました。この統合により、最初に AWS Lake Formation に登録しなくても DataZone、Amazon を介して AWS Glue テーブルを簡単に公開および共有できます。開始するには、管理者は Amazon DataZone コンソールの DefaultDataLake プルアッ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 IAM アクセス許可で管理されている AWS Glue テーブルにサブスクライブすると、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、AWS Lake Formation を通じ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にアクセスを許可します。これにより、既存のワークフローを中断することなく、新しく付与された AWS Lake Formation 許可でテーブルに対する IAM 許可が存続します。詳細については、「[Amazon と AWS Lake Formation ハイブリッドモード DataZone の統合](#)」を参照してください。

## Amazon が AWS Glue Data Quality との統合 DataZone を開始

04/03/2024 にリリース

Amazon は AWS Glue Data Quality との統合 DataZone を開始し、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 APIs を提供します。新しい統合により、AWS Glue Data Quality スコアを Amazon DataZone ビジネスデータカタログに自動発行できます。Amazon DataZone APIs を使用して、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ことができます。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推奨事項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 APIs 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 AWS、アカウントと Amazon Redshift クラスター内のリソースを使用できるユーザーと目的をより細かく制御できます。

- **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ブループリントにプロジェクトの管理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、AWS シークレット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。Amazon DataZone コンソール内から AWS シークレットを作成することもできます。
- **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、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。また、どのデータ認可プロジェクトを公開することを許可す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、AWS シークレット、クラスター、ワークグループ、データベースなどの独自の 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。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 のユーザーは DataZone 、 AWS CloudFormation を活用して、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できるようになりました。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 IAM プリンシパルを直接追加する

01/05/2024 にリリース

IAM プリンシパルがまだ 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 を追加すると、プロジェクト所有者は、IAM ロールまたは IAM ユーザーの Amazon リソース名前 (ARN) を指定するだけで、IAM プリン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 IAM アクセス許可が依然として必要です。これらのアクセス許可は 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、任意のタイプのアセットを共有、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、「[ドメインの削除](#)」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 は AWS Lake Formation ハイブリッドモードのサポートを追加しました。このサポートにより、ハイブリッドモードで Lake Formation に登録された AWS S3 ロケーション DataZone で AWS Glue テーブルを Amazon に発行する場合、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。HIPAA 準拠 AWS のサービスのリストを表示するには、<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、データ使用量を改善できます。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推奨事項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、米国東部 (バージニア北部)、米国西部 (オレゴン) の各 AWS リージョン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。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 ブループリントの拡張

11/20/2023 にリリース

Amazon DataZone は、AWS アカウントからどのデータを公開できるユーザー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。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 ブループリントにプロジェクト管理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た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。

# セットアップ

Amazon をセットアップするには DataZone、AWS アカウントがあり、Amazon に必要な IAM ポリシーとアクセス許可を設定する必要があります 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 URL の取得、およびデータプロデューサーとデータコンシューマーの基本的な Amazon DataZone ワークフローについて説明します。

## トピック

- [AWS アカウントにサインアップする](#)
- [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](#)
- [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 用 AWS IAM Identity Center のセットアップ DataZone](#)

## AWS アカウントにサインアップする

AWS アカウントがない場合は、次のステップを実行してアカウントを作成します。

AWS 組織がある場合は、アカウントを作成します。

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

AWS アカウントにサインアップするには

1. <https://portal.aws.amazon.com/billing/signup> を開きます。
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。

AWS アカウントにサインアップすると、AWS アカウントのルートユーザーが作成されます。ルートユーザーは、アカウント内のすべての AWS サービスとリソースにアクセスできます。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 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、またはロールには、必要なアクセス許可が必要です。

### トピック

- [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](#)
- [IAM アクセス許可のカスタムポリシーを作成して、Amazon DataZone サービスコンソールのロール作成を簡素化する](#)
- [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](#)
- [\(オプション\) AWS Identity Center アクセス許可のカスタムポリシーを作成して、ドメインのシングルサインオン \(SSO\) を有効にする](#)
- [\(オプション\) AWS Identity Center のアクセス許可のカスタムポリシーを作成して、Amazon DataZone 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します。](#)
- [\(オプション\) IAM プリンシパルをキーユーザーとして追加し、Key Management Service \(KMS\) のカスタマーマネージドキーを使用して Amazon AWS DataZone ドメインを作成します。](#)

## 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. AWS マネジメントコンソールにサインインし、<https://console.aws.amazon.com/iam/> で IAM コンソールを開きます。

- ナビゲーションペインで、ポリシー を選択します。
- 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 管理ポリシー: AmazonDataZoneFullAccess](#)」を参照してください。
  - ( オプション) [IAM アクセス許可のカスタムポリシーを作成して、Amazon DataZone サービスコンソールのロール作成を簡素化します。](#)
  - ( オプション) [AWS Identity Center アクセス許可のカスタムポリシーを作成して、ドメインのシングルサインオン \(SSO\) を有効にします。](#)
  - ( オプション) [Amazon DataZone ドメインに 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 AWS Identity Center アクセス許可のカスタムポリシーを作成します。](#)
- [Actions (アクション)] を選択し、[Attach (アタッチ)] を選択します。
- 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。

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

次の手順を実行して、カスタムインラインポリシーを作成し、Amazon がユーザーに代わって マネジメントコンソールで必要なロールを作成できるように DataZone するために必要なアクセス許可を付与します AWS 。

- AWS マネジメントコンソールにサインインし、 <https://console.aws.amazon.com/iam/> で IAM コンソールを開きます。
- 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。
- 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。
- [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。
- 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。
- 「ポリシーの作成」画面の「ポリシーエディタ」セクションで、「JSON」を選択します。

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

カスタムインラインポリシーを作成して、関連付けられた AWS アカウントで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、および無効にするために必要なアクセス許可を付与するには、次の手順を実行します。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IAM アクセス許可のカスタムポリシーを作成して、Amazon DataZone サービスコンソールのロール作成を簡素化する](#)。

1. AWS マネジメントコンソールにサインインし、<https://console.aws.amazon.com/iam/> で IAM コンソールを開きます。
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、「JSON」を選択します。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-datzone*"
  }
]
}

```

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) AWS Identity Center アクセス許可のカスタムポリシーを作成して、ドメインのシングルサインオン (SSO) を有効にする

Amazon の AWS IAM Identity Center を使用してシングルサインオン (SSO) を有効に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を作成するには、以下の手順を実行します DataZone。

1. AWS マネジメントコンソールにサインインし、<https://console.aws.amazon.com/iam/> で IAM コンソールを開きます。
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、「JSON」を選択します。

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:DeleteManagedApplicationInstance",
        "sso:CreateManagedApplicationInstance",
        "sso:PutApplicationAssignmentConfiguration"
      ],
      "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) AWS Identity Center のアクセス許可のカスタムポリシーを作成して、Amazon DataZone 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します。

以下の手順を実行して、カスタムインラインポリシーを作成し、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付与します。

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

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、「JSON」を選択します。

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

オプションで Key Management Service (KMS) のカスタマーマネージドキー (CMK) を使用して Amazon AWS DataZone ドメインを作成する前に、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. AWS マネジメントコンソールにサインインし、<https://console.aws.amazon.com/kms/> で KMS コンソールを開きます。
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 KMS キーのエイリアスまたはキー 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 AWS アカウントに KMS キーの使用を許可または禁止するには、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 KMS 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 データポータルまたはカタログの使用を希望するユーザー、グループ、またはロールには、必要なアクセス許可が必要です。

### トピック

- [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 AWS Key Management Service \(KMS\) 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](#)

## 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、AWS 認証情報または Single Sign-On (SSO) 認証情報を使用します。以下のセクションの手順に従って、AWS 認証情報を使用して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。SSO DataZone で Amazon を使用する方法の詳細については、「」を参照してください[Amazon 用 AWS IAM Identity Center のセットアップ DataZone](#)。

### Note

ドメインのデータポータルにアクセスできるのは、ドメインの AWS アカウントの IAM プリンシパルのみです。他の AWS アカウントの IAM プリンシパルは、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. AWS マネジメントコンソールにサインインし、<https://console.aws.amazon.com/iam/> で IAM コンソールを開きます。
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、「JSON」を選択します。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 AWS アカウントの IAM プリンシパルのみがドメインのカタログにアクセスできます。他の AWS アカウントの IAM プリンシパルは、ドメインのカタログにアクセスできません。

API と SDK を使用して、以下の手順で Amazon DataZone ドメインのカタログへのアクセス権を IAM ID に付与できます。これらの IAM ID に Amazon DataZone データポータルにもアクセスさせたい場合は、上記の手順でに進みます [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. AWS マネジメントコンソールにサインインし、<https://console.aws.amazon.com/iam/> で IAM コンソールを開きます。
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 AWS Key Management Service (KMS) 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

データ暗号化用に独自の 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、IAM プリンシパルにアタッチして 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する必要があります。

1. AWS マネジメントコンソールにサインインし、<https://console.aws.amazon.com/iam/> で IAM コンソールを開きます。
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の作成 リンクを選択します。
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、「JSON」を選択します。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。

## Amazon 用 AWS IAM Identity Center のセットアップ DataZone

### Note

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

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 認証情報を使用します。このセクションの手順に従って、Amazon 用の IAM Identity Center を設定します AWS DataZone。AWS 認証情報 DataZone で Amazon を使用する方法の詳細については、「」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](#)。

Amazon DataZone ドメインを作成するのと同じ AWS リージョンで AWS IAM Identity Center (Single Sign-On の後継) AWS が既に有効になっており、設定されている場合は、このセクションの手順をスキップできます。

AWS IAM Identity Center (Single Sign-On の後継) を有効にするには、AWS 以下の手順を実行します。

1. AWS IAM Identity Center を有効にするには、AWS Organizations AWS 管理アカウントの認証情報を使用して マネジメントコンソールにサインインする必要があります。Organizations メンバーアカウントの認証情報を使用してサインインしている間は AWS、IAM Identity Center を有効にすることはできません。詳細については、「[Organizations ユーザーガイド](#)」の「[組織の作成と管理](#)」を参照してください。AWS
2. [AWS IAM Identity Center \(Single Sign-On の後継\) AWS コンソール](#)を開き、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、Amazon DataZone ドメインを作成する AWS リージョンを選択します。

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、ユーザー管理を迅速かつ簡単に行うために IAM Identity Center ストアを利用できます。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 SSO を使用するよう招待する E メールを受信する必要があります。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、AWS Identity Center for Amazon を有効に DataZone し、SSO ユーザーと SSO グループへのアクセスを提供できます。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。

# 開始

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

- [AWS Glue データを使用した Amazon DataZone クイックスタート](#)
- [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](#)

### Important

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 AWS アカウントを使用している場合は、[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。既存の AWS Glue Data Catalog オブジェクトを持つ AWS アカウントを使用している場合は、[Amazon への Lake Formation アクセス許可も設定 DataZone](#)する必要があります。

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

### トピック

- [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 - Glue から AWS 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 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、ドメインを表示 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、AWS が所有および管理するキーでデフォルトで暗号化されます。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 の保管時のデータ暗号化 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、このアカウントの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。この URL を使用して Amazon DataZone データポータルにアクセスし、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生成された URL 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、名前を に 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、プロジェクトが使用できる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、AWS Glue Catalog、および Amazon Athena 内のデータを操作できます。
  - 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。
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、プロジェクトの認証情報を使用して認証用の Athena クエリエディタが開きます。Amazon 環境ドロップダウンで公開 DataZone 環境が選択され、クエリエディタで<environment\_name>%\_pub\_dbデータベースが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 `mkt_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 - Glue から AWS メタデータを収集する

このセクションでは、このワークフローのために AWS Glue 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。

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. Catalog Sales Data 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、次に着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

### トピック

- [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> 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 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、AWS が所有および管理するキーでデフォルトで暗号化されます。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 の保管時のデータ暗号化 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。
  - 「高速セットアップ」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は変更せずに、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。この URL を使用して Amazon DataZone データポータルにアクセスし、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生成された URL 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 URL を使用して Amazon データポータルに移動し、シングルサインオン (SSO) または AWS IAM 認証情報を使用してログインします。
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 クラスターのシークレット ARN を指定します。

### Note

AWS Secrets Manager のシークレットに次のタグ (キー/値) が含まれていることを確認します。

- 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、[「AWS Secrets Manager 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 で指定するデータベースユーザーには、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、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. 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
```

mkt\_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. mkt\_sls\_table アセットを公開するには、公開を選択します。

## 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 クラスターのシークレット ARN を指定します。

### Note

AWS Secrets Manager のシークレットに次のタグ (キー/値) が含まれていることを確認します。

- 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、[「AWS Secrets Manager 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 で指定するデータベースユーザーには、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、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. 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. Amazon DataZone データポータルでステップ 9 を完了したら、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

次のセクションでは、以下のタスクを完了するために使用できるさまざまな Amazon DataZone APIs を呼び出すサンプルスクリプトについて説明します。

## トピック

- [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](#)
- [AWS Glue からメタデータを収集する](#)
- [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、CreateEnvironmentProfileAPI 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 API を呼び出します。

```
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
```

CreateEnvironmentProfile API が呼び出された後のサンプル出力ペイロードです。

```
{
  "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
```

## AWS Glue からメタデータを収集する

このサンプルスクリプトを使用して、AWS Glue からメタデータを収集できます。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 DataZone ドメインとユーザーアクセスの管理

## トピック

- [ドメインの作成](#)
- [ドメインの編集](#)
- [ドメインの削除](#)
- [Amazon の IAM Identity Center を有効にする DataZone](#)
- [Amazon 用 IAM Identity Center 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 データポータルでのユーザーアクセス許可の管理](#)

## ドメインの作成

### Note

AWS アイデンティティセンター DataZone で Amazon を使用して SSO ユーザーおよびグループへのアクセスを提供する場合、現在、Amazon DataZone ドメインは AWS アイデンティティセンターインスタンスと同じ AWS リージョンに存在する必要があります。

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、ドメイン作成時にロール作成権限を持つ IAM ロールを引き受ける必要があります。[IAM アクセス許可のカスタムポリシーを作成して、Amazon](#)

[DataZone サービスコンソールのロール作成を簡素化する](#) 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 AmazonDataZoneGlueManageAccessRole を作成します AmazonDataZoneRedshiftManageAccessRole AmazonDataZoneProvisioningRole。

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 AWS リージョンを選択します。
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、Amazon に固有の AWS キーを使用して Key Management Service (KMS) によって暗号化されます DataZone。このフィールドを使用して、所有キーを使用するか、AWS 別の AWS KMS キーを選択するかを指定します。

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 の保管時のデータ暗号化 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、AWS Glue および Amazon Redshift リソースへのアクセスのプロビジョニング、取り込み、管理のための 3 つの IAM ロールを作成し、新しい Amazon S3 バケットを作成し、管理用の Amazon DataZone プロジェクトを作成し、データレイクとデータウェアハウスのデフォルトの設計図の環境プロファイルを作成します。
- タグ - (オプション) ドメインの AWS タグ (キーと値のペア) を指定します。
- 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。

## ドメインの編集

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、後で説明の変更、IAM Identity Center の有効化、タグキーとその値の追加、編集、削除を行うようにドメインを編集できます。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、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. AWS マネジメントコンソールにサインインし、<https://console.aws.amazon.com/datazone> で Amazon 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。
4.
  - **説明** を編集します。

- IAM Identity Center の設定を行います。これらの設定の詳細については、「」を参照してください [Amazon 用 AWS IAM Identity Center のセットアップ 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。

## ドメインの削除

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、IAM ロール、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など、Amazon が作成に役立たせた DataZone 可能性のある Amazon 以外の DataZone AWS リソースは削除されません。これらのリソースが不要になった場合は、それぞれの AWS サービスで削除します。

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 DataZone、IAM で設定できる Amazon の管理者 IAM アクセス許可が必要です。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. AWS マネジメントコンソールにサインインし、<https://console.aws.amazon.com/datazone> で Amazon 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. 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 が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 はドメインまたは関連するアカウントに AWS リソースを作成し、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、Amazon がドメイン内のプロジェクト用に作成できる AWS リソースのリストと、デフォルト名です。ドメインを削除しても、アカウント AWS 内のこれらの AWS リソースは削除されません。

- IAM ロール: `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既に存在する場合、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、Amazon DataZone ドメインと同じ AWS リージョンで AWS IAM Identity Center が有効になっている必要があります。

AWS IAM Identity Center を使用して、SSO ユーザーとグループに Amazon DataZone データポータルへのアクセスを提供できます。を完了すると [Amazon 用 AWS IAM Identity Center のセットアップ 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。

AWS IAM Identity Center を Amazon DataZone ドメインで使用できるようにするには、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。 [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 [IAM アクセス許可のカスタムポリシーを作成して、Amazon DataZone サービスコンソールのロール作成を簡素化する](#) は、IAM Identity Center を Amazon で使用できるように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。

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

1. AWS マネジメントコンソールにサインインし、<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、IAM Identity 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、IAM Identity 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。

## Amazon 用 IAM Identity Center を無効にする DataZone

Amazon DataZone ドメインの AWS IAM Identity Center を無効にすると、すべての SSO ユーザーのアクセスが削除されます。

### 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](#)。

AWS IAM Identity Center を使用して、SSO ユーザーとグループに Amazon DataZone データポータルへのアクセスを提供できます。Amazon の AWS IAM Identity Center を有効にしている場合は 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。

Amazon DataZone ドメインで使用する AWS IAM Identity Center を無効にするには、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。[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 [IAM アクセス許可の](#)

[カスタムポリシーを作成して、Amazon DataZone サービスコンソールのロール作成を簡素化する](#)は、IAM Identity Center を Amazon で使用するのを無効に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。

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

1. AWS マネジメントコンソールにサインインし、<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. <https://console.aws.amazon.com/singlesignon/> で IAM Identity Center コンソールを開きます。
5. [Applications] (アプリケーション) を選択します。
6. AWS IAM Identity Center を無効にするドメインを選択します。これにより、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が削除されます。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. Amazon DataZone ドメインの AWS IAM Identity Center を再度有効にするには、AWS IAM Identity Center を再度有効にするドメインを選択し、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、認証情報または Single Sign-On (SSO) 認証情報を使用して AWS Amazon DataZone データポータルにアクセスできます。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 AWS Identity and Access Management (IAM) を使用して作成され、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、自分のアカウントのユーザーまたは関連付けられたアカウントのユーザーの IAM ユーザー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. AWS マネジメントコンソールにサインインし、<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ユーザー 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、ユーザータイプのドロップダウンメニューで IAM 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の ARN 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。
    - 割り当て済み は、IAM ユーザーが Amazon を使用するように割り当てられていることを意味します 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 API を呼び出した、コマンドを発行した (コマンドラインインターフェイス経由)、またはドメインの Amazon DataZone ポータルにアクセスしたことを意味します。ユーザーのサブスクリプションに対して課金されます。

- 非アクティブ化とは、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され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。IAM 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、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 ユーザーは、AWS IAM Identity Center で ID プロバイダーを作成または同期されます。詳細については、[Amazon 用 AWS IAM Identity Center のセットアップ DataZone](#) 「」および「」を参照して [Amazon の IAM Identity Center を有効にする DataZone](#)、Amazon の AWS IAM Identity Center を有効にして設定します 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. AWS マネジメントコンソールにサインインし、<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、SSO ユーザーの現在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。
    - 割り当て済み 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 にアクセスできません 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ていたが、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 ユーザーの追加 を選択して SSO 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せん。
  - 追加するユーザーのリストに満足したら、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 SSO 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 SSO 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、非アクティブ化された SSO 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 グループは、AWS IAM Identity Center の ID プロバイダーで作成または同期されます。詳細については、[Amazon 用 AWS IAM Identity Center のセットアップ DataZone 「」](#) および [「」](#) を参照

して [Amazon の IAM Identity Center を有効にする DataZone](#)、Amazon の AWS IAM Identity Center を有効にして設定します 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. AWS マネジメントコンソールにサインインし、<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 SSO グループの現在のリストを表示します。
  - 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。
    - 割り当て済み 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 グループを追加するには、**グループの追加** と **グループの追加** を選択します。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済み のステータスで割り当てられます。
  - 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。このグループへのメンバー

シッ プ DataZone を通じて Amazon へのアクセスを取得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 データポータルでのユーザーアクセス許可の管理

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 DataZone 組み込みブループリントの使用

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

## トピック

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

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

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 SageMaker ブループリントの複数のブルー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、Amazon DataZone カタログでデータレイクアセットを公開および使用するための一連のサービス (AWS Glue、AWS Lake Formation、Amazon Athena ) を起動および設定するための定義が含まれています。
- 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、この Amazon DataZone ドメインを格納する AWS アカウント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。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。

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> で 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 管理アクセスロール に、AWS Glue と AWS Lake Formation のテーブルへのアクセスを取り込んで管理するための Amazon DataZone 認可を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。
  - 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 SageMaker 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。

**⚠ 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には、環境アカウントとリージョン AWS CloudFormation でを使用して環境リソースを作成および設定する 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-Glue データソースの Amazon S3 バケットに、AWS アカウント内のすべての SageMaker 環境で使用される Amazon S3 バケットを指定します。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。

## 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> で 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、(複数の) 選択したブループリント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 DefaultDataWarehouse、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。

AWS アカウントで DefaultDataWarehouse ブループリントを有効にすると、パラメータセットをブループリント設定に追加できます。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、データベースの名前、およびクラスターの認証情報を保持する AWS シークレットが含まれます。

### DefaultDataWarehouse 設計図へのパラメータセットの追加

1. <https://console.aws.amazon.com/datazone> で 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、DefaultDataWarehouse 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。
  - 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を保持するシーク AWS レット ARN を選択します。シー AWS クレットをパラメー

タセット内で使用するためには、AmazonDataZoneDomain : [Domain\_ID] タグでタグ付けする必要があります。

- 既存の AWS シークレットがない場合は、新しいシークレットの作成 を選択して新しい AWS シークレットを作成することもできます。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。新しい AWS シークレットの作成 を選択すると、Amazon DataZone は AWS Secrets Manager サービスに新しいシークレットを作成し、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にタグが付けら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、ドロップダウンリスト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。

AWS アカウントで Amazon SageMaker ブループリントを有効にすると、パラメータセットをブループリント設定に追加できます。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> で 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 (SSO) のいずれかを選択できます。

- AWS リージョンを指定します。
- データ暗号化用の AWS KMS キーを指定します。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 環境の VPC に使用している ID。既存の VPC を指定するか、新しい VPC を作成できます。
  - サブネット - VPC 内の特定のリソースの IP アドレス範囲の 1 つ以上の IDs。
  - 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 と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。
    - 選択した Amazon Redshift クラスターの認証情報を保持するシークレット AWS クレジット ARN を指定します。シークレットをパラメータセット内で使用するためには、AmazonDataZoneDomain : [Domain\_ID] タグでタグ付けする必要があります。

既存の AWS シークレットがない場合は、新しいシークレットの作成を選択して新しい AWS シークレットを作成することもできます。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。新しい AWS シークレットの作成を選択すると、Amazon は AWS Secrets Manager サービスに新しいシークレット DataZone を作成し、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にタグが付けら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
  - 選択した Amazon Redshift クラスターの認証情報を保持するシークレット AWS クレジット ARN を指定します。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 AWS シークレットがない場合は、新しいシークレットの作成を選択して新しい AWS シークレットを作成することもできます。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。新しい AWS シークレットの作成 を選択すると、Amazon は AWS Secrets Manager サービスに新しいシークレット DataZone を作成し、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にタグが付けら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。

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

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> で 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 でのカスタム AWS サービスブループリントの使用 DataZone

Amazon では DataZone、カスタム AWS サービスブループリントにより、組織で既に設定されている独自の既存の AWS Identity and Access Management (IAM) ロールと AWS サービスを使用する DataZone ように Amazon を設定することで、リソースの使用状況とコストを最適化できます。

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が Amazon DataZone カタログ内のアセットを操作するときに使用できるツールとサービスを定義します。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 DataZone カスタム AWS サービスブループリントを使用すると、組織で現在使用している任意の AWS サービスに合わせて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。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共同作業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 AWS サービスブループリントを有効にする](#)
- [カスタム AWS サービスブループリントを使用して環境を作成する](#)
- [カスタム AWS サービス環境でアクションを作成する](#)
- [カスタム AWS サービス環境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](#)

## カスタム AWS サービスブループリントを有効にする

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

1. AWS マネジメントコンソールにサインインし、<https://console.aws.amazon.com/datazone> で Amazon DataZone マネジメントコンソールを開きます。
2. ドメインを表示を選択し、カスタム AWS サービスブループリントを有効に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、使用可能なブループリントのリストからAWS 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 AWS サービスブループリントを使用して環境を作成する

カスタム AWS サービスブループリントを使用して環境を作成するには、次の手順を実行します。

1. AWS マネジメントコンソールにサインインし、<https://console.aws.amazon.com/datazone> で Amazon DataZone マネジメントコンソールを開きます。
2. ドメインを表示を選択し、カスタム AWS サービスブループリントが有効になってい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、有効な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。プロジェクトにより、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 - この環境内の Amazon S3 や AWS Glue などの既存の AWS サービスやリソース 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。Amazon S3

### Note

Amazon DataZone はこのロールをプロビジョニングしません。この環境で有効にする既存の AWS サービスとリソースへのアクセス許可を持つ既存の IAM ロールが必要です。

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、この環境で有効にする サービスとリソースにのみ AWS アクセスできるようにスコープダウンされていることを確認します。

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

## カスタム AWS サービス環境でアクションを作成する

カスタム AWS サービス環境でアクションを作成するには、次の手順を実行します。カスタム AWS サービス環境でアクションを作成することで、この環境で利用できる分析ツールに Amazon DataZone データポータルへのディープリンクを追加できます。

1. AWS マネジメントコンソールにサインインし、<https://console.aws.amazon.com/datazone> で Amazon DataZone マネジメントコンソールを開きます。
2. ドメインを表示を選択し、カスタム AWS サービスブループリントが有効になってい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、有効なAWS サービスブループリントを選択し AWS、アクションを追加するサービス環境を選択します。
4. AWS コンソールリンクページで、人気リンクまたはカスタム AWS リンクセクションからリンク (アクション) を選択して、Amazon データポータル経由でこの環境から 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 コンソールリソースへのディープリンクを有効にします。 AWS DataZone
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 AWS サービス環境にプロジェクトメンバーを追加する

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

1. AWS マネジメントコンソールにサインインし、<https://console.aws.amazon.com/datazone> で Amazon DataZone マネジメントコンソールを開きます。
2. プロジェクト タブを選択し、メンバーを追加する AWS サービス環境内のプロジェクトを選択します。

3. 追加 を選択し、メンバーの追加 ページで、IAM ユーザー、SSO ユーザー、または SSO グループ からメンバーを検索して追加します。所有者または寄稿者 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。

## AWS サービス環境でデータソースを設定する

AWS サービス環境でデータソースを設定するには、次の手順を実行します。

1. AWS マネジメントコンソールにサインインし、<https://console.aws.amazon.com/datazone> で Amazon DataZone マネジメントコンソールを開きます。
2. ブループリント タブを選択し、カスタム AWS サービスブループリントを選択します。
3. 作成済み環境 で、データソースを設定する AWS サービス環境を選択します。
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 - AWS Glue または Amazon Redshift を選択します。
    - 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 のいずれかを選択し、Redshift 認証情報を指定します。これには、新規または既存の 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、指定したデータベース内のスキーマが含まれます。
  - アクセス許可 - Lake Formation (AWS Glue 用) のテーブルへのアクセスを AWS Amazon に取り込み、管理するための DataZone 許可を提供するか、Amazon Redshift のテーブルへのアクセスを取り込み、管理するための DataZone 許可を Amazon に付与する管理アクセスロールを指定します。
  - 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。このターゲットを使用して、プロジェクト DataZone でサブスクライブしたデータへのアクセスを有効にします。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。

## 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

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、AWS 次の手順を実行します。

1. AWS マネジメントコンソールにサインインし、<https://console.aws.amazon.com/datazone> で Amazon DataZone マネジメントコンソールを開きます。
2. ブループリント タブを選択し、サービスブループリントを選択します AWS。
3. 作成済み環境 で、サブスクリプションターゲットを設定する AWS サービス環境を選択します。
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 - AWS Glue または Amazon Redshift を選択します。
    - 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、Redshift 認証情報を指定します。これには、新規または既存の 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、指定したデータベース内のスキーマが含まれます。
  - アクセス許可 - Lake Formation のテーブル (AWS Glue 用) へのアクセスを AWS Amazon に取り込み、管理する DataZone 権限を付与する、または Amazon Redshift のテーブルへのアクセスを取り込み、管理する DataZone 権限を Amazon に付与する管理アクセスロールを指定します。
  - 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。

# 関連するアカウントを使用してデータを発行および使用する

AWS アカウントを Amazon DataZone ドメインに関連付けると、ドメインユーザーはこれらの AWS アカウントのデータを公開して使用できます。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、関連付けをリクエストして、目的の AWS アカウントとドメインを共有します。AWS アカウントがドメインの AWS アカウントと異なる場合、Amazon は AWS Resource Access Manager (RAM) DataZone を使用します。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、AWS Glue データベースや Amazon Redshift クラスターなどのアカウント内のリソースを作成およびアクセスするために必要な IAM ロールとリソース設定をドメイン内のユーザーに提供します。

## トピック

- [他の AWS アカウントとの関連付けをリクエストする](#)
- [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 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](#)
- [関連付けられた AWS アカウントで環境ブループリントを有効にする](#)
- [関連付けられた AWS アカウントに Amazon を信頼されたサービス SageMaker として追加する](#)
- [関連付けられたアカウントを削除する](#)

## 他の AWS アカウントとの関連付けをリクエストする

### Note

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

Amazon DataZone ドメインの Amazon DataZone コンソール内の他の AWS アカウントとの関連付けをリクエストするには、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、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する必要があります。

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

1. AWS マネジメントコンソールにサインインし、<https://console.aws.amazon.com/datazone> で Amazon DataZone マネジメント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. 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アカウントの IDs を入力します。アカウント 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。関連付けられたアカウント `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。which は `AWSRAMPermissionDataZoneDefault`、関連付けられたアカウントが Amazon DataZone APIs のみを実行することを許可し、データポータルアクセスを提供しません。DataZone 次に、Amazon は、入力されたアカウント ID (複数可) をプリンシパルとして、アカウントに代わって AWS Resource Access Manager にリソース共有を作成します。
6. リクエストを受け入れるには、他の AWS アカウントの所有者に通知する必要があります (複数可)。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、 が保持するキーを使用して (デフォルトで) AWS、または (オプションで) ドメインの作成時に所有および提供する AWS Key Management Service (KMS) のカスタマーマネージドキーを使用して暗号化されます。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. AWS マネジメントコンソールにサインインし、<https://console.aws.amazon.com/kms/> で KMS コンソールを開きます。
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 KMS キーのエイリアスまたはキー ID を選択します。
5. 外部 AWS アカウントに KMS キーの使用を許可または禁止するには、ページの「その他の AWS アカウント」セクションのコントロールを使用します。これらのアカウントの IAM 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 KMS 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、[こちら](#)が必要です。

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. AWS マネジメントコンソールにサインインし、<https://console.aws.amazon.com/datazone> で Amazon DataZone マネジメントコンソールを開きます。
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 AWS Glue、Amazon S3、および Amazon Athena リソースを作成および管理して、データレイクから発行および消費できます。
  - 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 リソースを作成および管理して、データウェアハウスから発行および消費できます。
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 AWS Glue や Amazon DataZone Redshift 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 に

提供します。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 AWS Glue データベース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。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 が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 パスを選択する場合は、IAM ポリシーを更新して、Amazon にそのパスを使用する DataZone アクセス許可を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。

## 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で 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. AWS マネジメントコンソールにサインインし、<https://console.aws.amazon.com/datazone> で Amazon DataZone マネジメントコンソールを開きます。
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 AWS アカウントで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. AWS マネジメントコンソールにサインインし、<https://console.aws.amazon.com/datazone> で Amazon DataZone マネジメントコンソールを開きます。
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 AWS サービスブループリントのいずれかを選択します。

 Note

カスタム AWS サービスブループリントを有効にする場合は、アクセスロールの管理を指定する必要はありません。Custom Service AWS Blueprint のアクセス許可と承認メカニズムは、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 AWS サービスブループリントを使用して環境を作成する](#)」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 管理アクセスロール で、Glue と AWS Lake Formation の AWS テーブル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。
  - 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、環境アカウントとリージョン AWS CloudFormation でを使用して環境リソースを作成および設定する 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-Glue データソースの Amazon S3 バケットに、アカウント内のすべての SageMaker 環境 AWS で使用される Amazon S3 バケットを指定します。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> で 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 DefaultDataWarehouse 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 DefaultDataWarehouse 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。

AWS アカウントで DefaultDataWarehouse ブループリントを有効にすると、パラメータセットをブループリント設定に追加できます。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、データベースの名前、およびクラスターへの認証情報を保持する AWS シークレットが含まれます。

#### 設計図への DefaultDataWarehouseパラメータセットの追加

1. <https://console.aws.amazon.com/datazone> で 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、DefaultDataWarehouse 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。
  - 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を保持するシーク AWS レット ARN を選択します。シーク AWS クレットをパラメータセット内で使用するためには、AmazonDataZoneDomain : [Domain\_ID] タグでタグ付けする必要があります。

- 既存の AWS シークレットがない場合は、新しいシークレットの作成 を選択して新しい AWS シークレットを作成することもできます。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。新しい AWS シークレットの作成 を選択すると、Amazon は AWS Secrets Manager サービスに新しいシークレット DataZone を作成し、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にタグが付けら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。

AWS アカウントで Amazon SageMaker ブループリントを有効にすると、パラメータセットをブループリント設定に追加できます。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> で 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 (SSO) のいずれかを選択できます。
  - AWS リージョンを指定します。
  - データ暗号化用の AWS KMS キーを指定します。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 環境の VPC に使用している ID。既存の VPC を指定するか、新しい VPC を作成できます。
  - サブネット - VPC 内の特定のリソースの IP アドレス範囲の 1 つ以上の IDs。
  - 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 と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。
    - 選択した Amazon Redshift クラスターの認証情報を保持するシーク AWS レット ARN を指定します。シーク AWS クレットをパラメータセット内で使用するためには、AmazonDataZoneDomain : [Domain\_ID] タグでタグ付けする必要があります。

既存の AWS シークレットがない場合は、新しいシークレットの作成を選択して新しい AWS シークレットを作成することもできます。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。新しい AWS シークレットの作成を選択すると、Amazon は AWS Secrets Manager サービスに新しいシークレット DataZone を作成し、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にタグが付けら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
  - 選択した Amazon Redshift クラスターの認証情報を保持するシーク AWS レット ARN を指定します。シーク AWS クレットをパラメータセット内で使用するためには、AmazonDataZoneDomain : [Domain\_ID] タグでタグ付けする必要があります。

既存の AWS シークレットがない場合は、新しいシークレットの作成を選択して新しい AWS シークレットを作成することもできます。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。新しい AWS シークレットの作成を選択すると、Amazon は AWS Secrets Manager サービスに新しいシークレット DataZone を作成し、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にタグが付けら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 AWS アカウントに Amazon を信頼されたサービス SageMaker として追加する

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> で 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。

## 関連付けられたアカウントを削除する

Amazon DataZone マネジメントコンソールで関連付けられた AWS アカウントを削除するには、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。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. AWS マネジメントコンソールにサインインし、<https://console.aws.amazon.com/datazone> で Amazon DataZone マネジメント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. 下にスクロールして、関連アカウントタブに移動します。削除するアカウントの AWS アカウント ID を選択します。
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を入力し、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 データカタログの使用

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。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、編集、削除する](#)
- [用語集で用語を作成、編集、削除する](#)
- [メタデータフォームの作成、編集、削除](#)
- [メタデータフォームのフィールドを作成、編集、削除する](#)

## ビジネス用語集を作成、編集、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. DataZone データポータル URL を使用して Amazon データポータルに移動し、SSO または AWS 認証情報を使用してログインします。Amazon DataZone 管理者の場合は、Amazon DataZone ドメインが作成された AWS アカウントの <https://console.aws.amazon.com/datzone> にある Amazon DataZone コンソールにアクセスして、データポータル URL を取得できます。
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せん。

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. DataZone データポータル URL を使用して Amazon データポータルに移動し、SSO または AWS 認証情報を使用してログインします。Amazon DataZone 管理者の場合は、Amazon DataZone ドメインが作成された AWS アカウントの <https://console.aws.amazon.com/datazone> にある Amazon DataZone コンソールにアクセスして、データポータル URL を取得できます。
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、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には、次のステップを実行します。

1. DataZone データポータル URL を使用して Amazon データポータルに移動し、SSO または AWS 認証情報を使用してログインします。Amazon DataZone 管理者の場合は、Amazon DataZone ドメインが作成された AWS アカウントの <https://console.aws.amazon.com/datazone> にある Amazon DataZone コンソールにアクセスして、データポータル URL を取得できます。
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には、次のステップを実行します。

1. DataZone データポータル URL を使用して Amazon データポータルに移動し、SSO または AWS 認証情報を使用してログインします。Amazon DataZone 管理者の場合は、Amazon

DataZone ドメインが作成された AWS アカウントの <https://console.aws.amazon.com/datazone> にある Amazon DataZone コンソールにアクセスして、データポータル URL を取得できます。

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。

## 用語集で用語を作成、編集、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。

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. DataZone データポータル URL を使用して Amazon データポータルに移動し、SSO または AWS 認証情報を使用してログインします。Amazon DataZone 管理者の場合は、Amazon DataZone ドメインが作成された AWS アカウントの <https://console.aws.amazon.com/datazone> にある Amazon DataZone コンソールにアクセスして、データポータル URL を取得できます。
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、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には、次のステップを実行します。

1. DataZone データポータル URL を使用して Amazon データポータルに移動し、SSO または AWS 認証情報を使用してログインします。Amazon DataZone 管理者の場合は、Amazon DataZone ドメインが作成された AWS アカウントの <https://console.aws.amazon.com/datazone> にある Amazon DataZone コンソールにアクセスして、データポータル URL を取得できます。
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、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には、次のステップを実行します。

1. DataZone データポータル URL を使用して Amazon データポータルに移動し、SSO または AWS 認証情報を使用してログインします。Amazon DataZone 管理者の場合は、Amazon DataZone ドメインが作成された AWS アカウントの <https://console.aws.amazon.com/datazone> にある Amazon DataZone コンソールにアクセスして、データポータル URL を取得できます。
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の作成、編集、削除

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をサポートしています。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. DataZone データポータル URL を使用して Amazon データポータルに移動し、SSO または AWS 認証情報を使用してログインします。Amazon DataZone 管理者の場合は、Amazon DataZone ドメインが作成された AWS アカウントの <https://console.aws.amazon.com/datzone> にある Amazon DataZone コンソールにアクセスして、データポータル URL を取得できます。
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、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には、次のステップを実行します。

1. DataZone データポータル URL を使用して Amazon データポータルに移動し、SSO または AWS 認証情報を使用してログインします。Amazon DataZone 管理者の場合は、Amazon DataZone ドメインが作成された AWS アカウントの <https://console.aws.amazon.com/datzone> にある Amazon DataZone コンソールにアクセスして、データポータル URL を取得できます。
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. DataZone データポータル URL を使用して Amazon データポータルに移動し、SSO または AWS 認証情報を使用してログインします。Amazon DataZone 管理者の場合は、Amazon DataZone ドメインが作成された AWS アカウントの <https://console.aws.amazon.com/datzone> にある Amazon DataZone コンソールにアクセスして、データポータル URL を取得できます。
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認します。

## メタデータフォームのフィールドを作成、編集、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 DataZone ポータル URL を使用して Amazon データポータルに移動し、SSO または AWS 認証情報を使用してログインします。Amazon DataZone 管理者の場合は、Amazon DataZone ドメインが作成された AWS アカウントの <https://console.aws.amazon.com/datazone> にある Amazon DataZone コンソールにアクセスして、データポータル URL を取得できます。
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には、次のステップを実行します。

1. データ DataZone ポータル URL を使用して Amazon データポータルに移動し、SSO または AWS 認証情報を使用してログインします。Amazon DataZone 管理者の場合は、Amazon DataZone ドメインが作成された AWS アカウントの <https://console.aws.amazon.com/datazone> にある Amazon DataZone コンソールにアクセスして、データポータル URL を取得できます。
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、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には、次のステップを実行します。

1. データ DataZone ポータル URL を使用して Amazon データポータルに移動し、SSO または AWS 認証情報を使用してログインします。Amazon DataZone 管理者の場合は、Amazon DataZone ドメインが作成された AWS アカウントの <https://console.aws.amazon.com/datazone> にある Amazon DataZone コンソールにアクセスして、データポータル URL を取得できます。
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、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、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 でのプロジェクトと環境の使用 DataZone

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、ロールのみがプロジェクトと、このプロジェクトがサブスクライブする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。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](#)
- [プロジェクトを削除する](#)
- [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、AWS アカウントやリージョンなどの配置情報をプロファイルに埋め込むことで、環境の作成を簡素化することです。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 DataZone ポータル URL を使用して Amazon データポータルに移動し、SSO または AWS 認証情報を使用してログインします。Amazon DataZone 管理者の場合は、Amazon DataZone ドメインが作成された AWS アカウントの <https://console.aws.amazon.com/datazone> にある Amazon DataZone コンソールにアクセスして、データポータル URL を取得できます。
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。
  - ドロップダウンから AWS アカウントを選択します。
  - 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。
  - ドロップダウンからアカウントとリージョンを選択して AWS、AWS パラメータを指定します。
  - 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

- 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を保持する AWS シークレット ARN を入力します。AWS シークレットには、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 をタグ付ける必要があります。
- 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、環境プロファイルで選択された AWS アカウントとリージョン内の任意のスキーマから発行することもできます。
  - デフォルトの環境スキーマからのみ発行: 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、潜在的な環境を作成する AWS アカウント番号と AWS アカウントリージョンを指定します。

- 「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環境が作成された AWS アカウントとリージョン内の任意のデータベースからの発行を有効にするか、デフォルトデータベースのみを選択して、環境で作成されたデフォルトの発行データベースからの発行のみを有効にします。

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 URL に移動し、シングルサインオン (SSO) または AWS 認証情報を使用してサインインします。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、AWS アカウントドメインが作成された でサインインし、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を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 環境プロフィールで環境プロフィー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ィールを作成できます。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ィー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環境が作成された AWS アカウントとリージョン内の任意のデータベースからの発行を有効にするか、デフォルトデータベースのみを選択して、環境で作成されたデフォルトの発行データベースからの発行を有効にします。

編集が完了したら、環境プロフィールの編集 を選択します。

## 環境プロフィールを削除する

Amazon では DataZone、環境プロフィールは環境の作成に使用できるテンプレートです。環境プロフィールの目的は、AWS アカウントやリージョンなどの配置情報をプロフィールに埋め込むことで、環境の作成を簡素化することです。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 ドメインの環境プロフィールを削除するには、Amazon DataZone プロジェクトに属している必要があります。

### Note

環境プロフィールを削除すると、このプロフィールを使用して環境を作成できなくなります。

環境プロフィールを削除するには

1. Amazon DataZone データポータル URL に移動し、シングルサインオン (SSO) または AWS 認証情報を使用してサインインします。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、AWS アカウント ドメインが作成された でサインインし、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、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、Amazon Athena ワークグループなど) のコレクションであり、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た特定の IAM プリンシパル (環境ユーザーロール) のセットが含まれます。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 URL に移動し、シングルサインオン (SSO) または AWS 認証情報を使用してサインインします。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、AWS アカウント ドメインが作成された でサインインし、データポータルを開く 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、Amazon Athena ワークグループなど) のコレクションであり、それらのリソースを操作できる特定の IAM プリンシパル (寄稿者アクセス許可が割り当てられている) のセットが含まれます。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 URL に移動し、シングルサインオン (SSO) または AWS 認証情報を使用してサインインします。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、AWS アカウント ドメインが作成された でサインインし、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、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、Amazon Athena ワークグループなど) のコレクションであり、それらのリソースを操作できる特定の IAM プリンシパル (寄稿者アクセス許可が割り当てられている) のセットが含まれます。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 URL に移動し、シングルサインオン (SSO) または AWS 認証情報を使用してサインインします。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、AWS アカウント ドメインが作成された でサインインし、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、サブスクリプション、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 URL に移動し、シングルサインオン (SSO) または AWS 認証情報を使用してサインインします。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、AWS アカウントドメインが作成されたでサインインし、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。

## 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、サブスクリプション、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 URL に移動し、シングルサインオン (SSO) または AWS 認証情報を使用してサインインします。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、AWS アカウント ドメインが作成された でサインインし、データポータルを開く 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、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は取り消し不能で削除されません。Amazon は、Amazon DataZone が Lake Formation と Amazon Redshift を介して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 が作成した DataZone Amazon 以外の DataZone AWS リソースは削除されません。これらの AWS リソースが不要になった場合は、それぞれの AWS サービスとアカウントでリソースを削除します。

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 URL に移動し、シングルサインオン (SSO) または AWS 認証情報を使用してサインインします。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、AWS アカウント ドメインが作成された でサインインし、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で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 が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 はドメインまたは関連するアカウントに AWS リソースを作成し、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、Amazon がプロジェクト用に作成 DataZone できる AWS リソースのリストと、デフォルト名です。プロジェクトを削除しても、AWS アカウント内のこれらの AWS リソースは削除されません。

- IAM ロール: `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 URL に移動し、シングルサインオン (SSO) または AWS 認証情報を使用してサインインします。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、AWS アカウント ドメインが作成された でサインインし、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。

メンバーをプロジェクトに追加するには、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 URL に移動し、シングルサインオン (SSO) または AWS 認証情報を使用してサインインします。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、AWS アカウント ドメインが作成された でサインインし、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. member 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。

#### Note

IAM プリンシパルがドメインに既に Amazon DataZone ユーザープロファイルを持っている場合は、その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 CLI 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。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 IAM プリンシパルをプロジェクトメンバーとして追加するには、管理者に IAM コンソール AmazonDataZoneDomainExecutionRole のドメインの に次の 2 つの IAM アクセス許可を追加するように依頼します iam:GetUseriam: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 プリンシパルに、そのようなアクションに対する対応する IAM アクセス許可が必要です。

## 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. DataZone データポータル URL を使用して Amazon データポータルに移動し、SSO または AWS 認証情報を使用してログインします。Amazon DataZone 管理者の場合は、Amazon DataZone ドメインが作成された AWS アカウントの <https://console.aws.amazon.com/datzone> にある Amazon DataZone コンソールにアクセスして、データポータル URL を取得できます。
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. member 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 でのインベントリの作成とデータの公開 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。

## 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](#)
- [既存の Amazon DataZone データソースを管理する](#)
- [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 でデータソースの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 のデータシステム 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と、この環境の作成プロセス DataZone の一環として AWS Glue データベースが Amazon に追加されます。この AWS Glue データベースからアセットを発行する場合、追加のアクセス許可は必要ありません。

ただし、Amazon DataZone 環境の外部に存在する AWS Glue データベースからアセットを公開してサブスクライブする場合は、この外部 AWS Glue データベース DataZone の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。これを行うには、AWS Lake Formation で次の設定を完了し、必要な Lake Formation アクセス許可を [AmazonDataZoneGlueAccess-<region>-<domainId >](#) にアタッチする必要があります。

- Lake Formation アクセス許可モード またはハイブリッドアクセスモード を使用して、AWS Lake Formation でデータレイクの Amazon S3 の場所を設定します。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。
- 次の AWS Lake Formation 許可を にアタッチします [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 Select Describe Grantable、DataZone、のアクセス Select Grantable 許可。

### Note

Amazon は AWS Lake Formation ハイブリッドモード DataZone をサポートしています。Lake Formation ハイブリッドモードでは、Lake Formation を通じて AWS Glue データ

ベースとテーブルに対するアクセス許可の管理を開始できますが、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されます。詳細については、「[Amazon と AWS Lake Formation ハイブリッドモード DataZone の統合](#)」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 AWS Lake Formation ハイブリッドモード DataZone の統合

Amazon DataZone は AWS Lake Formation ハイブリッドモードと統合されています。この統合により、最初に AWS Lake Formation に登録しなくても、Amazon DataZone を通じて AWS Glue テーブルを簡単に公開および共有できます。ハイブリッドモードでは、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、AWS Lake Formation を通じて AWS Glue テーブルに対するアクセス許可の管理を開始できます。

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。

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

1. <https://console.aws.amazon.com/datazone> で 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、AWS Lake Formation ハイブリッドモードとの統合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[Amazon DataZone ドメインを所有するアカウントで AWS 組み込みブループリントを有効にする](#)、アカウントで有効にします AWS。
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の場合、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、AWS Lake Formation ハイブリッドアクセスモードを使用して 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。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 バケットの URI 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。

- [変更の保存] を選択します。

アカウント AWS でデータロケーション登録設定を有効にすると、データコンシューマーが IAM アクセス許可で管理されている AWS Glue テーブルにサブスクライブすると、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 AWS Lake Formation でテーブルに対するアクセス許可を管理してデータコンシューマーへのアクセスを許可します。これにより、既存のワークフローを中断することなく、新しく付与された AWS Lake Formation 許可でテーブルに対する IAM 許可が引き続き存在できるようになります。

## Amazon で AWS Lake Formation ハイブリッドモード統合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 DataZone

カスタマー管理の KMS キーまたは AWS マネージド KMS キーで暗号化された Amazon S3 ロケーションを使用している場合、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 ロケーションが AWS マネージドキーで暗号化されている場合は、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. <https://console.aws.amazon.com/kms> で AWS KMS コンソールを開き、AWS Identity and Access Management (IAM) 管理ユーザーとして、またはロケーションの暗号化に使用される KMS キーのキーポリシーを変更できるユーザーとしてログインします。
2. ナビゲーションペインで [Customer managed keys] (カスタマー管理型のキー) を選択してから、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 [Key policy] (キーポリシー) タブを選択してから、以下のいずれかを行って、カスタムロールまたは Lake Formation サービスリンクロールを KMS キーユーザーとして追加します。
  - デフォルトビュー (キー管理者、キー削除、キーユーザー、その他の AWS アカウントセクションを含む) が表示されている場合は、キーユーザーセクションに 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 の場所がデータカタログと同じ AWS アカウント内にない場合は、[「アカウント間で AWS 暗号化された Amazon S3 の場所を登録する」](#)の手順に従います。

## 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、カタログでのアセットの表現方法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 (govForm や など) のセットがあります GovernanceFormType。Amazon のアセットタイプ DataZone はバージョン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技術的な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ス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 URL に移動し、シングルサインオン (SSO) または AWS 認証情報を使用してサインインします。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、 AWS アカウントドメインが作成された でサインインし、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、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。

APIs 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. 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"  
)
```

- 次に、CreateAssetType API アクションを呼び出すことで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,
        },
    },
)
```

構造化データのアセットタイプを作成する例を次に示します。

```
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\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.datzone.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、 からデータベーステーブルの技術的なメタデータをインポート AWS Glue Data Catalog するためにデータソースを作成できます 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が に既に存在している必要があります AWS Glue。

AWS Glue データソースを作成して実行するときは、ソース AWS Glue データベースから Amazon DataZone プロジェクトのインベントリにアセットを追加します。AWS Glue 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、オプションでアセットを Amazon DataZone カタログに公開することを選択し、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に、プロジェクト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、これらのアセットのサブスクリプションをリクエストできます。

AWS Glue データソースを追加するには

1. Amazon DataZone データポータル URL に移動し、シングルサインオン (SSO) または AWS 認証情報を使用してサインインします。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、AWS アカウント ドメインが作成された でサインインし、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、 AWS Glue テーブルを発行する環境を指定します。
  8. 「データ選択」で、 AWS Glue データベースを指定し、テーブルの選択条件を入力します。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。

ドロップダウンから AWS Glue データベースを選択するか、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 AWS Glue データ品質出力を Amazon DataZone カタログにインポートします。デフォルトでは、Amazon は AWS Glue から有効期限のない最新の既存の 100 品質レポート DataZone をインポートします。

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、ビジネスデータカタログの検索中など、特定の時点でコンテキストを提供するために、これらのデータ品質メトリクスを AWS Glue から DataZone 取得します。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は、スケジュールに従って AWS Glue データ品質スコアを取り込むことができます。Amazon DataZone ビジネスデータカタログでは、データ品質 APIs を通じてサードパーティ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。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. [次へ] をクリックします。
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。詳細については、「[the section called “既存のデータソースの管理”](#)」を参照してください。

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 で、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の作成、編集、削除”](#)」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. [次へ] をクリックします。
16. データソース設定を確認し、 の作成を選択します。

#### Note

AWS Glue 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る AWS Glue データベース内のすべてのテーブルにアクセスするための、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 DataZone を作成します。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。Amazon は、公開環境の AWS IAM ロールへのアクセスを許可するときに、次の AWS タグを Glue データベース DataZone に追加します。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 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技術的な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から Amazon DataZone プロジェクトのインベントリにアセットを追加します。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 URL に移動し、シングルサインオン (SSO) または AWS 認証情報を使用してサインインします。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、AWS アカウント ドメインが作成された でサインインし、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、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 スキーマからの発行のみを許可する環境を選択した場合、Amazon Redshift 認証情報と、Amazon Redshift クラスターまたはワークグループ名、AWS シークレット、データベース名、スキーマ名などの他のパラメータ DataZone が Amazon Redshift に自動的に適用されます。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、認証に使用する AWS Secrets Manager のシークレットを選択します。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 のシークレットに次のタグ (キー/値) が含まれていることを確認します。
  - 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 AWS Secrets Manager」](#)を参照してください。

データソースの作成用に提供された AWS シークレットの Amazon Redshift ユーザーには、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には、シークレット内の AWS データベースユーザーにも次のアクセス許可が必要です。

- 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. [次へ] をクリックします。
  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。詳細については、[「the section called “既存のデータソースの管理”](#)」を参照してください。

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 で、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の作成、編集、削除”](#)」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. [次へ] をクリックします。
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 AWS タグがクラスターまたはワークグループに追加されていることを確認する必要があります。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。

## 既存の Amazon DataZone データソースを管理する

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 管理ポリシーがアタッチされている必要があります。詳細については、「[the section called “AWS マネージドポリシー”](#)」を参照してください。

## トピック

- [データソースを編集する](#)
- [データソースの削除](#)

## データソースを編集する

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 URL に移動し、シングルサインオン (SSO) または AWS 認証情報を使用してサインインします。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、AWS アカウントドメインが作成された でサインインし、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、データ選択基準を変更できます。
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すると、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そのデータソースを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、「[Amazon でのデータの検出、サブスクライブ、消費 DataZone](#)」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

プロジェクトインベントリから Amazon DataZone アセットとそのメタデータを 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、AWS Glue Data Catalog および Amazon Redshift 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。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、次のメッセージが表示されます。

```
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 URL に移動し、シングルサインオン (SSO) または AWS 認証情報を使用してサインインします。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、AWS アカウント ドメインが作成された でサインインし、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。

アセットの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、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、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の作成、編集、削除”](#)。

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 URL に移動し、シングルサインオン (SSO) または AWS 認証情報を使用してサインインします。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、AWS アカウントドメインが作成された でサインインし、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

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公開するには、アセットの再公開 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 URL に移動し、シングルサインオン (SSO) または AWS 認証情報を使用してサインインします。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、AWS アカウント ドメインが作成された でサインインし、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 カタログに公開し、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を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 URL に移動し、シングルサインオン (SSO) または AWS 認証情報を使用してサインインします。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、AWS アカウントドメインが作成された でサインインし、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 については、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 ロケーション 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. [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 URL に移動し、シングルサインオン (SSO) または AWS 認証情報を使用してサインインします。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、AWS アカウントドメインが作成された でサインインし、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ます。
5. 公開されたアセットのリストからアセットを見つけ、の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。アセットは、パブリッシュ を選択していつでも再パブリッシュできます。

## 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 URL に移動し、シングルサインオン (SSO) または AWS 認証情報を使用してサインインします。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、AWS アカウント ドメインが作成された でサインインし、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 でデータソースの実行を手動で開始する DataZone

データソースを実行すると、Amazon DataZone 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取得し、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 URL に移動し、シングルサインオン (SSO) または AWS 認証情報を使用してサインインします。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、AWS アカウント ドメインが作成された でサインインし、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からの最新のデータで 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 URL に移動し、シングルサインオン (SSO) または AWS 認証情報を使用してサインインします。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、AWS アカウント ドメインが作成された でサインインし、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 AWS Glue Data Quality と統合し、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 APIs 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。データ品質ルールを作成して実行するには、AWS Glue データ品質などの任意のデータ品質ツールを使用できます。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 AWS 管理ポリシーを使用している場合、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たポリシーを更新して、で AWS Glue データ品質情報を読み取るためのサポート[AWS マネージドポリシー: AmazonDataZoneGlueManageAccessRolePolicy](#)を有効にし[AWS 管理ポリシー: AmazonDataZoneDomainExecutionRolePolicy](#)、およびで時系列 APIsのサポートを有効にする必要があります[AWS マネージドポリシー: AmazonDataZoneFullUserAccess](#)。

## AWS Glue アセットのデータ品質の有効化

Amazon DataZone は、ビジネスデータカタログ検索など、特定の時点にコンテキストを提供するために、AWS Glue からデータ品質メトリクスを取得します。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は、スケジュールに従って AWS Glue データ品質スコアを取り込むことができます。Amazon DataZone ビジネスデータカタログでは、データ品質 APIs 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。詳細については、[AWS](#)

「[Glue Data Quality](#)」および「[データカタログの AWS Glue Data Quality の開始方法](#)」を参照してください。

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、新規または既存の AWS Glue データソースの作成中に、Amazon DataZone データポータル経由で AWS Glue データソースのデータ品質を有効にします。

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、[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「」を参照してください。[既存の Amazon DataZone データソースを管理する](#)。

#### Note

データポータルを使用して、Glue インベントリアセットのデータ品質のみを有効にできます AWS。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の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。

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 [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。データソースをデータ品質に使用するとき、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、が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、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。



```

\"Completeness \\\"billingcountry\\\" >= 0.5\", \n  \"details\" : { \n
  \"EVALUATION_MESSAGE\" : \"Value: 0.266666666666666666 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 を次のように呼び出します。

```

aws datazone delete-time-series-data-points \
--domain-identifier dzd_bqq1k3nz21zp2f \
--entity-identifier dzd_bqq1k3nz21zp2f \
--entity-type ASSET \
--form-name rulesET1 \

```

## 機械学習と生成 AI の使用

### Note

Amazon Bedrock を搭載: 不正使用の自動検出 AWS を実装します。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説明機能を使用して、データ検出とカタログ化を自動化できます。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。手動でのドキュメントタスクを減らし、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、貴重なデータを隠すのを最小限に抑えて、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 URL に移動し、シングルサインオン (SSO) または AWS 認証情報を使用してサインインします。Amazon DataZone 管理者の場合は、<https://console.aws.amazon.com/datazone> の Amazon DataZone コンソールに移動し、AWS アカウント ドメインが作成された でサインインし、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、自動的に生成された概要 の横にある緑色のアイコンを選択し、生成された説明に対処するために編集、承諾、または拒否 を選択できます。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、自動生成された説明に個別に対処することもできます。スキーマタブでは、すべて受け入れるまたはすべて拒否を選択して、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 駆動型の OpenLineage 互換性のある機能であり、OpenLineage 対応システムから、または APIs 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、変換の追跡、組織間のデータ使用量の表示に役立ちます。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。システムデータには、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、APIs 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。

Amazon DataZone の OpenLineage 互換 APIs を使用すると、ドメイン管理者とデータプロデューサーは、Amazon S3 DataZone、AWS Glue、その他の サービスでの変換など、Amazon で利用可能なものを超えるシステムイベントをキャプチャして保存できます。Amazon S3 これにより、データコンシューマーが包括的なビューを表示し、アセットのオリジンの信頼性を高めることができます。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リネージされるため、ユーザーは任意の時点でリネージを視覚化したり、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。この過去のシステムは、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。

データシステムを使用すると、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、システムを使用して、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、システム、特に列レベルのシステム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、列レベルのシステムを使用できます。例えば、列レベルのシステムを使用して、機密データ (PII など) 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 のシステムノードのタイプ DataZone

Amazon では DataZone、データシステム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システム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せん。

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。
  - Amazon DataZone カタログで公開された AWS Glue または Amazon Redshift アセットに関する情報を含むデータセットノードは自動生成され、ノード内に対応する AWS Glue または Amazon Redshift アイコンが含まれます。
  - 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：

- オープンシステム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 sourceIdentifier として使用されます。
- ジョブ実行の場合：
  - オープンシステム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 sourceIdentifier として使用されます。

createAsset API を使用して作成されたアセットの場合、は createAssetRevision API を使用して更新し、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。

## データシステムの視覚化

Amazon DataZoneのアセット詳細ページでは、データシステム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の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。API からキャプチャされたすべての詳細は、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、ジョブの詳細を、ジョブ情報、履歴などのタブで表示する詳細ペインがあります。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。API からキャプチャされたすべての詳細は、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 データシステムのすべてのシステムノードにはバージョンがあります。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、異なる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 でのデータシステム認証 DataZone

書き込みアクセス許可 - Amazon にシステムデータを発行するには DataZone、PostLineageEventAPI 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 IAM ロールが必要です。この IAM 認証は API Gateway 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。GetLineageNode

ListLineageNodeHistory 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読み出してデータシステムグラフをトラバースできます。

## Amazon でのデータシステムサンプルエクスペリエンス DataZone

データシステムサンプルエクスペリエンスを使用して、データシステム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 のデータシステムを参照および理解できます。

Amazon でサンプルデータシステム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 URL に移動し、シングルサインオン (SSO) または AWS 認証情報を使用してサインインします。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、AWS アカウントドメインが作成された でサインインし、データポータルを開く 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、システムタブを選択し、プレビュー を選択し、サンプルシステムを試す を選択します。
4. データシステムポップアップウィンドウで、ガイド付きデータシステムツアーの開始を選択します。

この時点で、系統情報のすべてのスペースを提供する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 APIs を呼び出すことができます。

- [GetLineageNode](#)
- [ListLineageNodeHistory](#)
- [PostLineageEvent](#)

# Amazon でのデータの検出、サブスクライブ、消費 DataZone

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、目的のアセットを見つけることから始まります。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、AWS Glue テーブルや Amazon Redshift テーブルやビュー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。
- 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、カスタム統合用の他の AWS サービスまたはサードパーティーソリューションと統合できます。

## トピック

- [データの検出](#)
- [データへのサブスクライブ](#)
- [データへのアクセスの許可](#)
- [データの消費](#)

## データの検出

以下のタスクでは、Amazon でデータを検出するさまざまな方法について説明します DataZone。

## トピック

- [カタログでアセットを検索して表示する](#)

## 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。詳細については、「[データへのサブスクライブ](#)」を参照してください。

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 URL に移動し、シングルサインオン (SSO) または AWS 認証情報を使用してサインインします。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、AWS アカウントドメインが作成された でサインインし、データポータルを開く 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、アセットが属 AWS リージョン する が含まれます。
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。

## データへのサブスクライブ

以下のタスクでは、Amazon のアセットへのサブスクライブの詳細について説明します DataZone。

### トピック

- [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](#)

## 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、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。

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 URL に移動し、シングルサインオン (SSO) または AWS 認証情報を使用してサインインします。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、AWS アカウントドメインが作成された でサインインし、データポータルを開く 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 URL に移動し、シングルサインオン (SSO) または AWS 認証情報を使用してサインインします。Amazon DataZone 管理者の場合は、<https://console.aws.amazon.com/datzone> で Amazon DataZone コンソールに移動し、AWS アカウントドメインが作成された でサインインし、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、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. (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。
7. 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 [Amazon DataZone イベントと通知の使用](#)。

## 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を取り消すには

1. Amazon DataZone データポータル URL に移動し、シングルサインオン (SSO) または AWS 認証情報を使用してサインインします。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、AWS アカウント ドメインが作成された でサインインし、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、「」で行う必要があります 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、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。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 URL に移動し、シングルサインオン (SSO) または AWS 認証情報を使用してサインインします。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、AWS アカウント ドメインが作成された でサインインし、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、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、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せん。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 URL に移動し、シングルサインオン (SSO) または AWS 認証情報を使用してサインインします。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、AWS アカウント ドメインが作成された でサインインし、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を表示 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 AWS アカウントの 1 つ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、次のステップを使用します。

## ステップ 1: Amazon DataZone ドメインが RAM 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

1. AWS RAM コンソールの「Shared by me: Resource shares」ページに移動します。
2. AWS RAM リソース共有は特定の AWS リージョンに存在するため、コンソールの右上隅にあるド롭ダウンリストから適切な AWS リージョンを選択します。
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 ドメインの RAM 共有は、RAM 共有が という名前で作成されるときに、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롭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 のみを使用したサブスクリプションターゲットの作成 DataZone をサポートしています。以下は、AWS Glue テーブルおよび Amazon Redshift テーブルまたはビュー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を作成するために使用できるペイロードの例です。詳細については、「」を参照してください [CreateSubscriptionTarget](#)。

### AWS Glue 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": "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 コールで使用する environmentIdentifier は、API コールを行うの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 コールは成功しません。
- authorizedPrincipals」で使用する IAM ロール ARN 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 がアクセス権を付与するロール DataZone 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

スを作成しません。また、アクセスロールの管理には、このデータベースに対する CREATE TABLE アクセス許可があることを確認してください。

- また、承認されたプリンシパルとして提供されるロール (AWS Glue の IAM ロールと Amazon Redshift のデータベースロール) が環境アカウントに既に存在していることを確認します。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、新しいテーブルに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。詳細については、「[データへのサブスクライブ](#)」を参照してください。

## データへのアクセスの許可

以下のタスクでは、Amazon のアセットへの承認済みサブスクリプションへのアクセス許可を付与する詳細について説明します DataZone。

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。

### トピック

- [マネージド AWS Glue Data Catalog アセットへのアクセスを許可する](#)
- [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](#)

## マネージド AWS Glue Data Catalog アセットへのアクセスを許可する

### Note

AWS Lake Formation LF-TBAC メソッドを使用した AWS Glue Data Catalog アセットのアクセス管理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 AWS Glue Data Catalog はサポートされていません。

マネージド AWS Glue Data Catalog アセットへのサブスクリプションリクエストが承認されると、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 を通じてユーザーに代わって承認済み AWS Glue Data Catalog テーブルへのアクセスを許可および管理します AWS Lake Formation。サブスクライバプロジェクトの場合、付与されたアセットは、アカウント内のリソース AWS Glue Data Catalog として に表示されます。その後、Amazon Athena を使用してテーブルをクエリできます。

### Note

サブスクライブされた 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た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る場合は、これらのサブスクライブされた AWS Glue Data Catalog アセットをこの新しいデータレイク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 が AWS Glue Data Catalog テーブルへのアクセスを許可 DataZone できるようにするには、次の条件を満たす必要があります。

- 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、AWS Glue テーブルは Lake Formation で管理されている必要があります。
- AWS Glue Data Catalog テーブル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には、次の Lake Formation 許可が必要です。
  - DESCRIBE 公開されたテーブルを含む AWS Glue データベースに対する および アクセス DESCRIBE GRANTABLE 許可。
  - 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、[「デベロッパーガイド」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

## マネージド Amazon Redshift アセットへのアクセスを許可する

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。

#### Note

現在のリリースでは、ソースとターゲットの Amazon Redshift クラスターまたはワークグループが同じ組織に属する AWS AWS アカウントにある場合にのみ、Amazon Redshift テーブルとビューへのアクセスを管理 DataZone できます。

## 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 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では、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 AWS Glue データカタログテーブルと Amazon Redshift テーブルおよびビューが含まれます。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して更新し、アセットをサブスクライブしたユーザー (複数可) DataZone 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 イベントと通知の使用」](#)を参照してください。

## データの消費

以下のタスクでは、Amazon でサブスクライブしているデータの消費の詳細を示します DataZone。

### トピック

- [Amazon Athena または Amazon Redshift でデータをクエリする](#)

## 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、データポータルプロジェクトページの右側ペインに Amazon Athena および/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 URL に移動し、シングルサインオン (SSO) または AWS 認証情報を使用してサインインします。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、AWS アカウント ドメインが作成された でサインインし、Open data portal 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 での SQL の使用の詳細については、「Athena [の SQL 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。

- 発行データベース (`{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 で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 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、[「CREATE TABLE 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 データベースの一部になりました。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 Redshift クラスターまたは Amazon DataZone 環境に設定された 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すると、環境に追加されてい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、IAM ID 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 DataZone イベントと通知の使用

Amazon DataZone 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を常に把握します。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。

### トピック

- [Amazon DataZone データポータルの専用受信トレイを介したイベントの操作](#)
- [Amazon EventBridge デフォルトバスによるイベントの操作](#)

## Amazon DataZone データポータルの専用受信トレイを介したイベントの操作

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用意しています。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、そのリクエストがデータポータルに表示され、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、データポータルの通知を確認します。メッセージには 2 種類あります。

- **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、ステータスは割り当てられていません。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

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
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

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
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、つまりドラフト状態でカタログに追加され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

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
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
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ングプロジェクト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ング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

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
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せん	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許可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

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
ビジネス名の自動生成	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
ビジネス名の自動生成	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	作成されたデータソース	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

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
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

データポータルを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 DataZone ポータル URL を使用して Amazon データポータルに移動し、SSO または AWS 認証情報を使用してログインします。Amazon DataZone 管理者の場合は、Amazon DataZone ドメインが作成された AWS アカウントの <https://console.aws.amazon.com/datazone> にある Amazon DataZone コンソールにアクセスして、データポータル URL を取得できます。
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へ移動します。

データポータルを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 DataZone ポータル URL を使用して Amazon データポータルに移動し、SSO または AWS 認証情報を使用してログインします。Amazon DataZone 管理者の場合は、Amazon DataZone ルートドメインが作成された AWS アカウントの <https://console.aws.amazon.com/datazone> にある Amazon DataZone コンソールにアクセスして、データポータル URL を取得できます。
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へ移動します。

## Amazon EventBridge デフォルトバスによるイベントの操作

データポータル専用受信トレイにメッセージを送信するだけでなく、は、Amazon DataZone ルートドメインがホストされているのと同じ AWS アカウントの Amazon EventBridge デフォルトイベントバス DataZone にもメッセージを送信します。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
- 環境の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

のクラウドセキュリティが最優先事項 AWS です。お客様は AWS、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、AWS とユーザーの間で共有される責任です。[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、で AWS サービスを実行するインフラストラクチャを保護する責任を担います AWS クラウド。また、は、安全に使用できるサービス AWS も提供します。コンプライアンス[AWS プログラム](#)コンプライアンスプログラムの一環として、サードパーティーの監査者は定期的にセキュリティの有効性をテストおよび検証。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、「[コンプライアンスプログラムAWS による対象範囲内のサービスコンプライアンスプログラム](#)」を参照してください。
- クラウドのセキュリティ — お客様の責任は、使用する AWS サービスによって決まります。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、Amazon DataZone リソースのモニタリングや保護に役立つ他の AWS のサービスの使用方法についても説明します。

## トピック

- [Amazon でのデータ保護 DataZone](#)
- [Amazon での認可 DataZone](#)
- [IAM を使用した Amazon DataZone リソースへのアクセスの制御](#)
- [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](#)

# Amazon でのデータ保護 DataZone

責任 AWS [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に対する管理を維持する責任があります。また、使用する AWS のサービスのセキュリティ設定と管理タスクもユーザーの責任となります。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のよくある質問](#)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、AWS セキュリティブログに投稿された[AWS 責任共有モデルおよび GDPR](#)のブログ記事を参照してください。

データ保護の目的で、認証情報を保護し AWS アカウント、AWS IAM Identity Center または AWS Identity and Access Management (IAM) を使用して個々のユーザーを設定することをお勧めします。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 AWS リソースと通信します。TLS 1.2 は必須であり TLS 1.3 がお勧めです。
- で API とユーザーアクティビティのログ記録を設定します AWS CloudTrail。
- 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を使用します 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。
- コマンドラインインターフェイスまたは API AWS を介して にアクセスするときに FIPS 140-2 検証済みの暗号化モジュールが必要な場合は、FIPS エンドポイントを使用します。利用可能な FIPS エンドポイントの詳細については、「[連邦情報処理規格 \(FIPS\) 140-2](#)」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、コンソール、API、DataZone または AWS のサービス SDK を使用して Amazon AWS CLI または他の を操作する場合も同様です。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。外部サーバーへの URL を提供する場合は、そのサーバーへのリクエストを検証するための認証情報を URL に含めないように強くお勧めします。

## データ暗号化

アクセス許可を付与するときは、Amazon リソースに対する DataZone アクセス許可を取得するユーザーを決定します。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、が AWS 所有および管理する [AWS Key Management Service \(AWS KMS\)](#) キーを使用して、デフォルトですべてのデータを DataZone 暗号化します。KMS で AWS 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。

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、KMS キーを指定することで、暗号化設定を指定できます。

### 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 HTTPS 経由で行われるため、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 の保管時のデータ暗号化 DataZone](#)
- [Amazon のインターフェイス VPC エンドポイントの使用 DataZone](#)

## Amazon の保管時のデータ暗号化 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 は、デフォルトの AWS 所有キーを使用して、保管中のデータを自動的に暗号化します。AWS 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。詳細については、「[AWS 所有キー](#)」を参照してください。

この暗号化レイヤーを無効にしたり、別の暗号化タイプを選択したりすることはできませんが、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することで、既存の AWS 所有の暗号化キーに 2 つ目の暗号化レイヤーを追加できます。Amazon DataZone は、ユーザーが作成、所有、管理できる対称カスタマーマネージドキーの使用をサポートし、既存の AWS 所有暗号化に 2 番目の暗号化レイヤーを追加します。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、AWS 所有キーを使用して保管時の暗号化 DataZone を自動的に有効にし、顧客データを無償で保護します。

AWS KMS 料金は、カスタマーマネージドキーの使用に適用されます。料金の詳細については、[AWS 「Key Management Service の料金」](#)を参照してください。

## Amazon が AWS KMS で許可 DataZone を使用する方法

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 AWS KMS 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 の許可は、Amazon にアカウントの KMS キー DataZone へのアクセスを許可するために使用されます。Amazon DataZone 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。

- 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 AWS リクエストを KMS [DescribeKey](#) に送信します。
- を AWS KMS [GenerateDataKeyrequests](#) に送信して、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します。
- [Decrypt](#) リクエストを AWS KMS に送信して、暗号化されたデータキーを復号し、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](#) は、 によって内部的に使用される AWS サービスの子許可を作成します 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、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

対称カスタマーマネージドキーは、AWS マネジメントコンソール、または AWS KMS APIs を使用して作成できます。

対称カスタマーマネージドキーを作成するには、AWS「[Key Management Service デベロッパーガイド](#)」の「[対称カスタマーマネージドキーの作成](#)」のステップに従います。

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、「[Key Management Service デベロッパーガイド](#)」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

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[付与とオペレーション](#)へのアクセスを許可します。[グラントの使用の詳細については](#)、AWS「[Key Management Service デベロッパーガイド](#)」を参照してください。
- [kms:DescribeKey](#) - は、Amazon がキーを検証できるように DataZone、カスタマーマネージドキーの詳細を提供します。
- [kms:GenerateDataKey](#) - AWS KMS の外部で使用する一意の対称データキーを返します。
- [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](#)、AWS 「Key Management Service デベロッパーガイド」を参照してください。

[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](#)、AWS 「Key Management Service デベロッパーガイド」を参照してください。

## 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[認証済みデータ](#)として暗号化コンテキストを使用して、[認証済み暗号化](#)をサポートします。データを暗号化する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、AWS CloudTrail または Amazon CloudWatch Logs によって生成されたログにも表示されます。

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、キーポリシーと IAM ポリシーで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

Amazon DataZone リソースで AWS KMS カスタマーマネージドキーを使用する場合、[AWS CloudTrail](#)を使用して、Amazon が AWS KMS DataZone に送信するリクエストを追跡できます。次の例は CreateGrant、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 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 GenerateDataKey の AWS CloudTrail イベントです。AWS KMS カスタマーマネージドキーを使用して Amazon DataZone ドメインを暗号化すると、Amazon DataZone はユーザーに代わって AWS アカウントの KMS キーにアクセスする CreateGrant リクエストを送信します。Amazon が DataZone 作成する権限は、AWS KMS カスタマーマネージドキーに関連付けられたリソースに固有です。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": "AROAIQDTESTANDEXAMPLE:Sampleuser01",
    "arn": "arn:aws:sts::111122223333:assumed-role/Admin/Sampleuser01",
    "accountId": "111122223333",
    "accessKeyId": "AKIAIOSFODNN7EXAMPLE3",
    "sessionContext": {
      "sessionIssuer": {
        "type": "Role",
        "principalId": "AROAIQDTESTANDEXAMPLE: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"
}

```

## 暗号化された AWS Glue カタログを含む Data Lake 環境の作成

高度なユースケースでは、暗号化された AWS Glue カタログを使用する場合は、カスタマー管理の KMS キーを使用するために 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 AWS Glue カタログ内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、次の手順を実行します。

- 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 AWS リソースをホストする場合、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、カスタム仮想ネットワークで AWS リソースを起動できます。VPC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制御できます。Amazon VPC の詳細については、「[Amazon VPC ユーザーガイド](#)」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 AWS サービスに接続できます。このエンドポイントを使用すると、インターネットゲートウェイやネットワークアドレス変換 (NAT) インスタンス、または VPN 接続などを必要とせずに、信頼性の高いスケーラブルな方法で接続できるようになります。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、「[Amazon VPC ユーザーガイド](#)」の「[インターフェイス VPC エンドポイント \(AWS PrivateLink\)](#)」を参照してください。

### Important

VPC では、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、エンドポイントを使用して サービスにアクセスできる AWS AWS プリンシパルを制御できます。

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 AWS と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) で構成されます。

Amazon DataZone マネジメントコンソールは、AWS 管理者が top-level-resource APIsに使用できます。これには、ドメインの作成と管理、これらのドメインの AWS アカウントの関連付け、Amazon にアクセス管理を委任するデータソースが含まれます 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 AWS アカウントの Amazon サービスに

アクセス管理コントロールを DataZone 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。Amazon DataZone データポータルは、SSO ユーザー向けのファーストパーティー AWS Identity Center アプリケーションです。有効にすると、認可された 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、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、および分析タスクを実行するために、AWS IAM Identity Center で認証されたユーザーが主に使用するよう設計されています。

## 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 DataZone はドメイン管理者 AWS アカウントとメンバー AWS アカウントの概念を使用し、コンソールはこれらのすべてのアカウントから使用して、AWS 組織の境界を尊重しながら信頼関係を構築します。

## 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) を持つ階層 ACL 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で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したときに、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ィール ID にマッピングされます。このユーザープロフィールには、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。

## IAM を使用した Amazon DataZone リソースへのアクセスの制御

AWS Identity and Access Management (IAM) は、以下のセキュリティ関連のタスクを完了する必要があります。

- の下にユーザーとグループを作成します AWS アカウント。
- で各ユーザーに一意的なセキュリティ認証情報を割り当てます AWS アカウント。
- AWS リソースを使用して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します。
- 別のユーザーが AWS リソースを共有 AWS アカウント できるようにします。
- のロール AWS アカウント を作成し、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、AWS リソース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

IAM の詳細については、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](#)
- [Amazon の IAM 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

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 管理ポリシーは、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。

AWS 管理ポリシーは、すべての AWS お客様が使用できるため、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ることに注意してください。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。

AWS 管理ポリシーで定義されているアクセス許可は変更できません。が AWS 管理ポリシーで定義されたアクセス許可 AWS を更新すると、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) が更新されます。は、新しい AWS のサービスが起動されたとき、または既存のサービスで新しい API AWS オペレーションが使用可能になったときに、AWS 管理ポリシーを更新する可能性が最も高くなります。

詳細については、「IAM ユーザーガイド」の「[AWS 管理ポリシー](#)」を参照してください。

## 内容

- [AWS 管理ポリシー: 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 管理ポリシー: AmazonDataZoneDomainExecutionRolePolicy](#)
- [AWS 管理ポリシー: AmazonDataZoneSageMakerProvisioning](#)

- [AWS 管理ポリシー: AmazonDataZoneSageMakerAccess](#)
- [AWS マネージドポリシー: AmazonDataZoneSageMakerEnvironmentRolePermissionsBoundary](#)
- [AWS マネージドポリシーに対する Amazon DataZone の更新](#)

## AWS 管理ポリシー: AmazonDataZoneFullAccess

AmazonDataZoneFullAccess ポリシーは IAM ID にアタッチできます。

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に既存の S3 バケットを選択したり、新しい S3 バケットを作成したり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 AWS IAM Identity Center が有効になっているリージョンを取得できるようにします。
- `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 AWS KMS キーを使用して Amazon DataZone ドメインを作成する場合、ドメイン作成を成功させる `kms:CreateGrant` には に対するアクセス許可が必要です。そのキーが `listDataSources` や などの他の Amazon DataZone APIs を呼び出すには `kms:GenerateDataKey` `kms:Decrypt` 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:Decrypt` `kms:CreateGrant`、`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、「[AWS Key Management Service](#)」を参照してください。

- 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>DeletePolicyVersion および アクセスiam:AttachRolePolicy許可が含まれます。
- AWS IAM Identity Center ユーザーのログインを有効に DataZone して Amazon で新しいドメインを作成する場合、または Amazon の既存のドメインに対してそのドメインをアクティブ化する場合は DataZone、sso:CreateManagedApplicationInstance、sso>DeleteManagedApplicationInstance および に対するアクセス許可が必要ですsso:PutApplicationAssignmentConfiguration。
- Amazon で AWS アカウント関連付けリクエストを受け入れるには 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:PostTimeSeriesDataPoints",
        "datazone:ListTimeSeriesDataPoints",
        "datazone:GetTimeSeriesDataPoint",
        "datazone>DeleteTimeSeriesDataPoints",
        "datazone:GetDomain",
        "datazone>CreateFormType",
        "datazone:GetFormType",
        "datazone:GetIamPortalLoginUrl",
        "datazone:SearchUserProfiles",
        "datazone:SearchGroupProfiles",
```

```
"datazone:GetUserProfile",
"datazone:GetGroupProfile",
"datazone:ListGroupsWithUser",
"datazone>DeleteFormType",
"datazone>CreateAssetType",
"datazone:GetAssetType",
"datazone>DeleteAssetType",
"datazone>CreateGlossary",
"datazone:GetGlossary",
"datazone>DeleteGlossary",
"datazone:UpdateGlossary",
"datazone>CreateGlossaryTerm",
"datazone:GetGlossaryTerm",
"datazone>DeleteGlossaryTerm",
"datazone:UpdateGlossaryTerm",
"datazone>CreateAsset",
"datazone:GetAsset",
"datazone>DeleteAsset",
"datazone>CreateAssetRevision",
"datazone:ListAssetRevisions",
"datazone:AcceptPredictions",
"datazone:RejectPredictions",
"datazone:Search",
"datazone:SearchTypes",
"datazone>CreateListingChangeSet",
"datazone>DeleteListing",
"datazone:SearchListings",
"datazone:GetListing",
"datazone>CreateDataSource",
"datazone:GetDataSource",
"datazone>DeleteDataSource",
"datazone:UpdateDataSource",
"datazone:ListDataSources",
"datazone:StartDataSourceRun",
"datazone:GetDataSourceRun",
"datazone:ListDataSourceRuns",
"datazone:ListDataSourceRunActivities",
"datazone:ListEnvironmentBlueprintConfigurations",
"datazone>CreateEnvironmentBlueprint",
"datazone:GetEnvironmentBlueprint",
"datazone>DeleteEnvironmentBlueprint",
"datazone:UpdateEnvironmentBlueprint",
"datazone:ListEnvironmentBlueprints",
"datazone>CreateProject",
```

```
"datazone:UpdateProject",
"datazone:GetProject",
"datazone>DeleteProject",
"datazone:ListProjects",
"datazone:CreateProjectMembership",
"datazone>DeleteProjectMembership",
"datazone:ListProjectMemberships",
"datazone:CreateEnvironmentProfile",
"datazone:GetEnvironmentProfile",
"datazone:UpdateEnvironmentProfile",
"datazone>DeleteEnvironmentProfile",
"datazone:ListEnvironmentProfiles",
"datazone:CreateEnvironment",
"datazone:GetEnvironment",
"datazone>DeleteEnvironment",
"datazone:UpdateEnvironment",
"datazone:UpdateEnvironmentDeploymentStatus",
"datazone:ListEnvironments",
"datazone:ListAccountEnvironments",
"datazone:GetEnvironmentActionLink",
"datazone:GetEnvironmentCredentials",
"datazone:GetSubscriptionTarget",
"datazone>DeleteSubscriptionTarget",
"datazone:ListSubscriptionTargets",
"datazone:CreateSubscriptionRequest",
"datazone:AcceptSubscriptionRequest",
"datazone:UpdateSubscriptionRequest",
"datazone:ListWarehouseMetadata",
"datazone:RejectSubscriptionRequest",
"datazone:GetSubscriptionRequestDetails",
"datazone:ListSubscriptionRequests",
"datazone>DeleteSubscriptionRequest",
"datazone:GetSubscription",
"datazone:CancelSubscription",
"datazone:GetSubscriptionEligibility",
"datazone:ListSubscriptions",
"datazone:RevokeSubscription",
"datazone:CreateSubscriptionGrant",
"datazone>DeleteSubscriptionGrant",
"datazone:GetSubscriptionGrant",
"datazone:ListSubscriptionGrants",
"datazone:UpdateSubscriptionGrantStatus",
"datazone:ListNotifications",
"datazone:StartMetadataGenerationRun",
```

```

        "datazone:GetMetadataGenerationRun",
        "datazone:CancelMetadataGenerationRun",
        "datazone:ListMetadataGenerationRuns",
        "datazone:ListLineageNodeHistory",
        "datazone:GetLineageNode",
        "datazone:CreateAssetFilter",
        "datazone>DeleteAssetFilter",
        "datazone:GetAssetFilter",
        "datazone:ListAssetFilters",
        "datazone:UpdateAssetFilter"
    ],
    "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 データポータルを使用して環境を作成すると、Amazon はこのアクセス許可の境界を[環境の作成時に生成される 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、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、インタラクティブなエンタープライズ[ユーザーや分析サービス \(など\) に代わって Amazon が引き受けることができるユーザーロール](#)の形式をとり AWS Glue、Amazon S3 からの読み取りと書き込みやの実行などのデータを処理するためのアクションを実行する場合があります AWS Glue クローラー。DataZone

このAmazonDataZoneEnvironmentRolePermissionsBoundaryポリシーは、Amazon S3、AWS Glue、Amazon Redshift、AWS Lake Formation Amazon Athena などのサービス DataZone への Amazon の読み取りおよび書き込みアクセスを許可します。Amazon S3 このポリシーは、ネット

ワークインターフェイスや AWS KMS キーなど、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。

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 AmazonDataZoneEnvironmentRolePermissionsBoundary AWS 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。

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": [
    "datzone:*",
    "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

このAmazonDataZoneRedshiftGlueProvisioningPolicyポリシー DataZone は、AWS Glue および Amazon Redshift との相互運用に必要なアクセス許可を Amazon に付与します。

```
{
  "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-*",
  "Condition": {
    "ForAnyValue:StringLike": {
      "aws:TagKeys": "AmazonDataZoneEnvironment"
    },
    "Null": {
      "aws:ResourceTag/AmazonDataZoneEnvironment": "false"
    },
    "StringEquals": {
      "aws:CalledViaFirst": [
        "cloudformation.amazonaws.com"
      ]
    }
  }
}
```

```
"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、AWS Glue 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 AWS Glue 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ためのアクセス DataZone 許可を Amazon に付与します。

```
{
  "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:CreateLakeFormationOptIn",
    "lakeformation>DeleteLakeFormationOptIn",
    "lakeformation:GrantPermissions",
    "lakeformation:GetResourceLFTags",
    "lakeformation:ListLakeFormationOptIns",
    "lakeformation:ListPermissions",
    "lakeformation:RegisterResource",
    "lakeformation:RevokePermissions",
    "glue:GetDatabase",
    "glue:GetTable",
    "organizations:DescribeOrganization",
    "ram:GetResourceShareInvitations",
    "ram:ListResources"
  ],
  "Resource": "*"
},
{
  "Sid": "CrossAccountRAMResourceSharingPermissions",
  "Effect": "Allow",
  "Action": [
    "glue>DeleteResourcePolicy",
    "glue:PutResourcePolicy"
  ],
  "Resource": [
    "arn:aws:glue:*:*:catalog",
    "arn:aws:glue:*:*:database/*",
    "arn:aws:glue:*:*:table/*"
  ]
}
```

```
],
"Condition": {
  "ForAnyValue:StringEquals": {
    "aws:CalledVia": [
      "ram.amazonaws.com"
    ]
  }
},
{
  "Sid": "CrossAccountLakeFormationResourceSharingPermissions",
  "Effect": "Allow",
  "Action": [
    "ram:CreateResourceShare"
  ],
  "Resource": "*",
  "Condition": {
    "StringEqualsIfExists": {
      "ram:RequestedResourceType": [
        "glue:Table",
        "glue:Database",
        "glue:Catalog"
      ]
    }
  },
  "ForAnyValue:StringEquals": {
    "aws:CalledVia": [
      "lakeformation.amazonaws.com"
    ]
  }
},
{
  "Sid": "CrossAccountRAMResourceShareInvitationPermission",
  "Effect": "Allow",
  "Action": [
    "ram:AcceptResourceShareInvitation"
  ],
  "Resource": "arn:aws:ram:*:*:resource-share-invitation/*"
},
{
  "Sid": "CrossAccountRAMResourceSharingViaLakeFormationPermissions",
  "Effect": "Allow",
  "Action": [
    "ram:AssociateResourceShare",
```

```
"ram:DeleteResourceShare",
"ram:DisassociateResourceShare",
"ram:GetResourceShares",
"ram:ListResourceSharePermissions",
"ram:UpdateResourceShare"
],
"Resource": "*",
"Condition": {
  "StringLike": {
    "ram:ResourceShareName": [
      "LakeFormation*"
    ]
  },
  "ForAnyValue:StringEquals": {
    "aws:CalledVia": [
      "lakeformation.amazonaws.com"
    ]
  }
},
},
{
  "Sid": "CrossAccountRAMResourceSharingViaLakeFormationHybrid",
  "Effect": "Allow",
  "Action": "ram:AssociateResourceSharePermission",
  "Resource": "*",
  "Condition": {
    "StringLike": {
      "ram:PermissionArn": "arn:aws:ram::aws:permission/AWSRAMLFEnabled*"
    },
    "ForAnyValue:StringEquals": {
      "aws:CalledVia": [
        "lakeformation.amazonaws.com"
      ]
    }
  }
},
{
  "Sid": "KMSDecryptPermission",
  "Effect": "Allow",
  "Action": [
    "kms:Decrypt"
  ],
  "Resource": "*",
  "Condition": {
```

```
    "StringEquals": {
      "aws:ResourceTag/datazone:projectId": "proj-all"
    }
  },
  {
    "Sid": "GetRoleForDataZone",
    "Effect": "Allow",
    "Action": [
      "iam:GetRole"
    ],
    "Resource": [
      "arn:aws:iam::*:role/AmazonDataZone*",
      "arn:aws:iam::*:role/service-role/AmazonDataZone*"
    ]
  },
  {
    "Sid": "PassRoleForDataLocationRegistration",
    "Effect": "Allow",
    "Action": [
      "iam:PassRole"
    ],
    "Resource": [
      "arn:aws:iam::*:role/AmazonDataZone*",
      "arn:aws:iam::*:role/service-role/AmazonDataZone*"
    ],
    "Condition": {
      "StringEquals": {
        "iam:PassedToService": [
          "lakeformation.amazonaws.com"
        ]
      }
    }
  }
]
```

## AWS 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

AmazonDataZoneCrossAccountAdmin ポリシーを IAM ID にアタッチできます。

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 管理ポリシー: 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:ListTimeSeriesDataPoints",
        "datazone:GetTimeSeriesDataPoint",
        "datazone>DeleteTimeSeriesDataPoints",
        "datazone:AcceptPredictions",
        "datazone:AcceptSubscriptionRequest",
        "datazone:CancelSubscription",
        "datazone>CreateAsset",
        "datazone>CreateAssetRevision",
        "datazone>CreateAssetType",

```

```
"datazone:CreateDataSource",
"datazone:CreateEnvironment",
"datazone:CreateEnvironmentBlueprint",
"datazone:CreateEnvironmentProfile",
"datazone:CreateFormType",
"datazone:CreateGlossary",
"datazone:CreateGlossaryTerm",
"datazone:CreateListingChangeSet",
"datazone:CreateProject",
"datazone:CreateProjectMembership",
"datazone:CreateSubscriptionGrant",
"datazone:CreateSubscriptionRequest",
"datazone>DeleteAsset",
"datazone>DeleteAssetType",
"datazone>DeleteDataSource",
"datazone>DeleteEnvironment",
"datazone>DeleteEnvironmentBlueprint",
"datazone>DeleteEnvironmentProfile",
"datazone>DeleteFormType",
"datazone>DeleteGlossary",
"datazone>DeleteGlossaryTerm",
"datazone>DeleteListing",
"datazone>DeleteProject",
"datazone>DeleteProjectMembership",
"datazone>DeleteSubscriptionGrant",
"datazone>DeleteSubscriptionRequest",
"datazone>DeleteSubscriptionTarget",
"datazone:GetAsset",
"datazone:GetAssetType",
"datazone:GetDataSource",
"datazone:GetDataSourceRun",
"datazone:GetDomain",
"datazone:GetEnvironment",
"datazone:GetEnvironmentActionLink",
"datazone:GetEnvironmentBlueprint",
"datazone:GetEnvironmentCredentials",
"datazone:GetEnvironmentProfile",
"datazone:GetFormType",
"datazone:GetGlossary",
"datazone:GetGlossaryTerm",
"datazone:GetGroupProfile",
"datazone:GetListing",
"datazone:GetProject",
"datazone:GetSubscription",
```

```
"datazone:GetSubscriptionEligibility",
"datazone:GetSubscriptionGrant",
"datazone:GetSubscriptionRequestDetails",
"datazone:GetSubscriptionTarget",
"datazone:GetUserProfile",
"datazone:ListAccountEnvironments",
"datazone:ListAssetRevisions",
"datazone:ListDataSourceRunActivities",
"datazone:ListDataSourceRuns",
"datazone:ListDataSources",
"datazone:ListEnvironmentBlueprintConfigurations",
"datazone:ListEnvironmentBlueprintConfigurationSummaries",
"datazone:ListEnvironmentBlueprints",
"datazone:ListEnvironmentProfiles",
"datazone:ListEnvironments",
"datazone:ListGroupsForUser",
"datazone:ListNotifications",
"datazone:ListProjectMemberships",
"datazone:ListProjects",
"datazone:ListSubscriptionGrants",
"datazone:ListSubscriptionRequests",
"datazone:ListSubscriptionTargets",
"datazone:ListSubscriptions",
"datazone:ListWarehouseMetadata",
"datazone:RejectPredictions",
"datazone:RejectSubscriptionRequest",
"datazone:RevokeSubscription",
"datazone:Search",
"datazone:SearchGroupProfiles",
"datazone:SearchListings",
"datazone:SearchTypes",
"datazone:SearchUserProfiles",
"datazone:StartDataSourceRun",
"datazone:UpdateDataSource",
"datazone:UpdateEnvironment",
"datazone:UpdateEnvironmentBlueprint",
"datazone:UpdateEnvironmentDeploymentStatus",
"datazone:UpdateEnvironmentProfile",
"datazone:UpdateGlossary",
"datazone:UpdateGlossaryTerm",
"datazone:UpdateProject",
"datazone:UpdateSubscriptionGrantStatus",
"datazone:UpdateSubscriptionRequest",
"datazone:StartMetadataGenerationRun",
```

```

        "datazone:GetMetadataGenerationRun",
        "datazone:CancelMetadataGenerationRun",
        "datazone:ListMetadataGenerationRuns",
        "datazone:GetEnvironmentAction",
        "datazone:ListEnvironmentActions",
        "datazone:ListLineageNodeHistory",
        "datazone:GetLineageNode",
        "datazone:CreateAssetFilter",
        "datazone>DeleteAssetFilter",
        "datazone:GetAssetFilter",
        "datazone:ListAssetFilters",
        "datazone:UpdateAssetFilter"
    ],
    "Resource": "*"
},
{
    "Sid": "RAMResourceShareStatement",
    "Effect": "Allow",
    "Action": "ram:GetResourceShareAssociations",
    "Resource": "*"
}
]
}

```

## AWS 管理ポリシー: 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、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 管理ポリシー: 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 AWS Config ルールに関する情報を取得します。また、サービスにリンクされたロールが AWS Config ルールを作成および削除し、ルールに対して評価を実行できるようにします。
- `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": "AmazonSageMakerKMSSGrantPermission",
  "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により、Amazon が DataZone 作成するロールの範囲と追加するロールが制限されます。

Amazon DataZone は

AmazonDataZoneSageMakerEnvironmentRolePermissionsBoundary マネージドポリシーを使用して、アタッチ先の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 がインタラクティブなエンタープライズユーザーや分析サービス ( など) に代わって

引き受け DataZone ることができるユーザーロールの形式をとりAWS SageMaker、Amazon S3 や Amazon Redshift からの読み取りと書き込み、AWS Glue クローラの実行などのデータを処理するためのアクションを実行する場合があります。

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、AWS Glue、Amazon S3、AWS Lake Formation、Amazon Redshift、Amazon Athena などのサービスに付与します。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、AWS KMS キーなど、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。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:*",
    "datzone:*",
    "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": "*"
}
]
}

```

## AWS マネージドポリシーに対する Amazon DataZone の更新

Amazon の AWS マネージドポリシーの更新に関する詳細を、このサービスがこれらの変更の追跡を開始した DataZone 以降の分について表示します。このページの変更に関する自動アラートについては、Amazon DataZone [ドキュメント履歴](#) ページの RSS フィードをサブスクライブしてください。

変更	説明	日付
AmazonDataZoneExecutionRolePolicy および AmazonDataZoneFullUserAccess - ポリシーの更新	データシステムAmazonDataZoneExecutionRolePolicy と きめ細かなアクセスコントロール API のサポートを有効にするAmazonDataZoneFullUserAccessために、このポリシーを更新しました。 APIs	2024 年 6 月 27 日

変更	説明	日付
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 DataZone、レイク形成で付与されるアクセス許可の範囲を絞り込む 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。	2024 年 6 月 14 日
AmazonDataZoneDomainExecutionRolePolicy - ポリシーの更新	ポリシーを に更新 AmazonDataZoneDomainExecutionRolePolicy し、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 APIs 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するための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 が AWS Lake Formation AmazonDataZone を呼び出して Amazon Simple Storage Service (Amazon S3) ロケーションを登録するときに使用される S3Manage-<region>-<domainId > と呼ばれる新しいロール。DataZone Amazon S3 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	2024 年 4 月 1 日
AmazonDataZoneGlueManageAccessRolePolicy - ポリシーの更新	データAmazonDataZoneGlueManageAccessRolePolicyへの許可の発行とアクセスを Amazon DataZone に許可する許可のサポートを有効にするように を更新しました。	2024 年 4 月 1 日
AmazonDataZoneDomainExecutionRolePolicy および AmazonDataZoneFullUserAccess - ポリシーの更新	CancelMetadataGenerationRun API のサポートを有効にするAmazonDataZoneFullUserAccessために、 AmazonDataZoneDomainExecutionRolePolicyと を更新しました。	2024 年 3 月 29 日

変更	説明	日付
AmazonDataZoneFullAccess - ポリシーの更新	が更新され、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 AmazonDataZoneFull Access できるようになりました。	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グループ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 ListEnvironmentBlueprintConfigurationsSummaries API 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	AWS Lake Formation ハイブリッドモードのサポートを有効にするAmazonDataZoneGlueManageAccessRolePolicyように を更新しました。	2023 年 12 月 14 日

変更	説明	日付
AmazonDataZoneFull UserAccess および AmazonDataZoneDoma inExecutionRolePolicy - 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 AmazonDat aZoneFullUserAccessおよ び AmazonDataZoneDoma inExecutionRolePolicyポ リシーを更新しました DataZone。	2023 年 11 月 28 日
AmazonDataZoneEnvi ronmentRolePermiss ionsBoundary - 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:GetQueryRes ultsStream アクセス許 可で構成される AmazonDat aZoneEnvironmentRo lePermissionsBoundaryマネー ジドポリシーを更新しまし た。	2023 年 11 月 17 日
AmazonDataZoneReds hiftManageAccessRolePolicy - ポリシーの更新	Amazon は、redshift: AssociateDataShare Consumer アクションの 組織 ID のチェックを削 除AmazonDataZoneReds hiftManageAccessRo lePolicyして DataZone を更新 しました。これにより、組織 間で AWS リソースを共有で きます。	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ていません。	2023 年 10 月 2 日
AmazonDataZonePortalFullAccessPolicy - ポリシーは廃止されました	Amazon は を DataZone 廃止しましたAmazonDataZonePortalFullAccessPolicy。	2023 年 9 月 29 日
AmazonDataZonePreviewConsoleFullAccess - ポリシーは廃止されました	Amazon は を DataZone 廃止しましたAmazonDataZonePreviewConsoleFullAccess。	2023 年 9 月 29 日

変更	説明	日付
AmazonDataZoneDomainExecutionRolePolicy - 新しいポリシー	<p>Amazon は、 という新しいポリシー DataZone を追加しましたAmazonDataZoneDomainExecutionRolePolicy。</p> <p>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。</p> <p>AmazonDataZoneDomainExecutionRolePolicy ポリシーを にアタッチできますAmazonDataZoneDomainExecutionRole 。</p>	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と連携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
AmazonDataZoneFullUserAccess - 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、AWS Glue データをカタログAmazonDataZoneGlueManageAccessRolePolicyに発行するDataZone アクセス許可をAmazon に付与するという新しいポリシーDataZone を追加しました。また、カタログ内のAWS Glue 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Amazon アクセスDataZone 許可も付与します。	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、アタッチ先の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、AWS マネジメントコンソール 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。	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
Amazon が変更の追跡 DataZone を開始しました	Amazon が AWS マネージドポリシーの変更の追跡 DataZone を開始しました。	2023 年 3 月 20 日

## Amazon の IAM 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 AmazonDataZoneRedshiftGlueProvisioningPolicy がアタッチされています。このロール DataZone は、AWS Glue および Amazon Redshift との相互運用に必要なアクセス許可を Amazon に付与します。

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 AWS 管理ポリシーが AmazonDataZoneDomainExecutionRolePolicy アタッチされています。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、Amazon DataZone ドメインをホスト AWS アカウント する が必要です。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、AmazonDataZoneGlueManageAccessRolePolicyがアタッチされています。このロールは、AWS Glue 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 AWS Glue 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ためのアクセス DataZone 許可を Amazon に付与します。

デフォルトのロールAmazonDataZoneGlueAccess-<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": [
    {
      "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、AmazonDataZoneRedshiftManageAccessRolePolicyが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 AWS Lake Formation を呼び出して Amazon Simple Storage Service (Amazon S3) ロケーションを登録するときに使用されます。AWS Lake Formation は、そのロケーション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 `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、AWS Glue、Amazon Redshift、および Amazon Sagemaker との相互運用に必要な Amazon アクセス DataZone 許可を付与します。

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

一部の AWS サービスは、一時的な認証情報を使用してサインインすると機能しません。一時的な認証情報を使用する AWS サービスなどの詳細については、[AWS 「IAM ユーザーガイド」の「IAM と連携する のサービス」](#)を参照してください。

ユーザー名とパスワード以外の AWS Management Console 方法で にサインインする場合、一時的な認証情報を使用します。例えば、会社の Single Sign-On (SSO) リンク AWS を使用して にアクセスすると、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。ロールの切り替えに関する詳細については、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。

一時的な認証情報は、AWS CLI または AWS API を使用して手動で作成できます。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します AWS。AWS 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、[IAM の一時的セキュリティ認証情報](#)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と AWS、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、「サービス認証リファレンス」の[AWS 「ドキュメントの必須要素のアクション、リソース、および条件キー」](#)を参照してください。

## Amazon のコンプライアンス検証 DataZone

AWS のサービスが特定のコンプライアンスプログラムの範囲内にあるかどうかを確認するには、コンプライアンスプログラム[AWS のサービスによる対象範囲内のコンプライアンスプログラム](#)を参照し、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、[AWS 「コンプライアンスプログラム」](#)を参照してください。

を使用して、サードパーティーの監査レポートを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 AWS Artifact](#)」の」を参照してください。

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、お客様のデータの機密性、貴社のコンプライアンス目的、適用される法律および規制によって決まります。は、コンプライアンスに役立つ以下のリソース AWS 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、セキュリティとコンプライアンスに重点を置いたベースライン環境 AWS をにデプロイする手順について説明します。
- [アマゾン ウェブ サービスにおける HIPAA セキュリティとコンプライアンスのアーキテクチャー](#) – このホワイトペーパーでは、企業が AWS を使用して HIPAA 対象アプリケーションを作成する方法について説明します。

**Note**

すべて AWS のサービス HIPAA の対象となるわけではありません。詳細については、[HIPAA 対応サービスのリファレンス](#)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、ガイダンスを保護し AWS のサービス、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するためのベストプラクティスをまとめています。
- [「デベロッパーガイド」の「ルールによるリソースの評価」](#) – この 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 Config
- [AWS Security Hub](#) – これにより AWS のサービス、内のセキュリティ状態を包括的に確認できます AWS。Security Hub では、セキュリティコントロールを使用して AWS リソースを評価し、セキュリティ業界標準とベストプラクティスに対する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](#) – これにより AWS アカウント、疑わしいアクティビティや悪意のあるアクティビティがないか環境を監視することで、、、ワークロード、コンテナ、データに対する潜在的な脅威 AWS のサービスを検出します。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、PCI DSS などのさまざまなコンプライアンス要件への対応に役立ちます。
- [AWS Audit Manager](#) – これにより AWS のサービス、AWS 使用状況を継続的に監査し、リスクの管理方法と規制や業界標準への準拠を簡素化できます。

## 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 ロールの使用

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。AWS 認証情報は、クライアントアプリケーションまたは Amazon S3 バケットに直接保存しないでください。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」にある下記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 コールをモニタリングする

Amazon DataZone は、Amazon のユーザー AWS CloudTrail、ロール、または の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。

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ゾーンを中心に構築されています。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ゾーン AWS リージョンを提供します。アベイラビリティゾーンでは、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。

AWS リージョン およびアベイラビリティゾーンの詳細については、[AWS 「グローバルインフラストラクチャ」](#)を参照してください。

Amazon DataZone は、AWS グローバルインフラストラクチャに加えて、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を提供しています。

### 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 の耐障害性](#)
- [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 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

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ンングされます。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ンングされます。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には影響しない用語集または用語集用語を無効にできます。

## 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 (リストとも呼ばれます) は、グローバル検索を通じて検出できます。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、DeleteSubscriptionGrant API オペレーションで retainPermissions フラグを使用して、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 の耐障害性

RAM の耐障害性については、<https://docs.aws.amazon.com/ram/latest/userguide/security-disaster-recovery-resiliency.html> を参照してください。

## ユーザープロフィール管理の耐障害性

ユーザープロフィールの耐障害性情報については、[AWS 「Identity Center」](#) を参照してください。

## 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 グローバル AWS ネットワークセキュリティで保護されています。AWS セキュリティサービスと [インフラストラクチャ AWS](#) を保護する方法については、[AWS 「クラウドセキュリティ」](#) を参照してください。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して AWS 環境を設計するには、「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

が AWS 公開した API コールを使用して、ネットワーク DataZone 経由で Amazon にアクセスします。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)。TLS 1.2 は必須で TLS 1.3 がお勧めです。
- DHE (楕円ディフィー・ヘルマン鍵共有) や ECDHE (楕円曲線ディフィー・ヘルマン鍵共有) などの完全前方秘匿性 (PFS) による暗号スイート。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。

また、リクエストには、アクセスキー ID と、IAM プリンシパルに関連付けられている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 \(AWS STS\)](#) を使用して、一時的なセキュリティ認証情報を生成し、リクエストに署名することもできます。

## 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。では AWS、サービス間のなりすましにより、混乱した代理問題が発生する可能性があります。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。これを防ぐために、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持つ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 AWS 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、AWS [「責任共有モデル」](#) を参照してください。

## 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 デフォルトバスによるイベントの操作](#)」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ログに記録し、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 ロ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 AWS IAM コンソールに移動し、 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、「 <a href="#">AmazonDataZoneGlue Access-&lt;region&gt;-&lt;domainId &gt;</a> 」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 AWS IAM コンソールに移動し、ロールにAmazonDataZoneGlueManageAccessRolePolicyタッチされていることを確認します。詳細については、「 <a href="#">AmazonDat</a>

データポータルのエラーメッセージ	解決方法
	<a href="#">aZoneGlueAccess-&lt;region&gt;-&lt;domainId &gt;</a> 」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。	<p>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。</p> <ul style="list-style-type: none"><li>• 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 ロケーションを 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、「<a href="#">Amazon S3 ロケーションの登録</a>」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 や S3 の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、「<a href="#">暗号化された Amazon S3 の場所の登録</a>」を参照してください。</li><li>• Amazon S3 の場所は AWS Lake Formation モードで登録されていますが、テーブルのアクセス許可に IAMAllowedPrincipal が追加されます。この問題を解決するには、テーブルのアクセス許可から IAMAllowedPrincipal 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、「<a href="#">Lake Formation アクセス許可モデルへのアップグレードについて</a>」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</li></ul>

データポータルのエラーメッセージ	解決方法
<p>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。</p>	<p>AWS、<a href="#">「暗号化された Amazon S3 ロケーションの登録」</a>の手順に従います。</p> <p>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 次のアクセス許可を付与します。</p> <ul style="list-style-type: none"> <li>• 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</li> <li>• Amazon がユーザーに代わって管理する access 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、付与可能な選択を選択します。</li> </ul>

## Amazon のクォータ DataZone

AWS アカウントには、各 AWS サービスについて、以前は制限と呼ばれていたデフォルトのクォータがあります。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の最大合計数	10000
ドメイン内の環境	Amazon DataZone ドメイン内の環境の最大数	500

# 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
<a href="#">AmazonDataZoneExecutionRolePolicy および AmazonDataZoneFullUserAccess - ポリシーの更新</a>	データシステムAmazonDataZoneExecutionRolePolicyと きめ細かなアクセスコントロール API のサポートを有効にするAmazonDataZoneFullUserAccessために、このポリシーを更新しました。APIs 詳細については、「 <a href="#">Amazon DataZone updates to AWS managed policies</a> 」を参照してください。	2024 年 6 月 27 日
<a href="#">AmazonDataZoneGlueManageAccessRolePolicy - ポリシーの更新</a>	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、レイク形成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、「 <a href="#">Amazon DataZone updates to AWS managed policies</a> 」を参照してください。	2024 年 6 月 14 日
<a href="#">AmazonDataZoneFullAccess - ポリシーの更新</a>	Amazon DataZone マネジメントコンソールAmazonDat	2024 年 6 月 14 日

aZoneFullAccess 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、[「Amazon DataZone updates to AWS managed policies」](#) を参照してください。

### [AmazonDataZoneDomainExecutionRolePolicy - ポリシーの更新](#)

ポリシーを に更新AmazonDataZoneDomainExecutionRolePolicy し、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 APIs を Amazon に追加しました。詳細については、[「Amazon DataZone updates to AWS managed policies」](#) を参照してください。

2024 年 6 月 14 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、SageMaker。詳細については、「[Amazon DataZone updates to AWS managed policies](#)」を参照してください。

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 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。詳細については、「[Amazon DataZone updates to AWS managed policies](#)」を参照してください。

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 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 SageMaker に付与します。詳細については、[「Amazon DataZone updates to AWS managed policies」](#)を参照してください。

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 アクションへのアクセスと、指定された管理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 AmazonDataZoneFullAccess を追加するポリシーの更新。詳細については、[「Amazon DataZone updates to AWS managed policies」](#)を参照してください。

2024 年 4 月 30 日

### [AmazonDataZoneS3Manage - <region>-<domainId > - 新しいロール](#)

Amazon が AWS Lake Formation AmazonDataZone を呼び出して Amazon Simple Storage Service (Amazon S3) ロケーションを登録するときに使用される S3Manage - <region>-<domainId > と呼ばれる新しいロール。AWS Lake Formation は、そのロケーション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。DataZone Amazon S3 詳細については、[「Amazon DataZone updates to AWS managed policies」](#) を参照してください。

2024 年 4 月 1 日

### [AmazonDataZoneGlue ManageAccessRolePolicy - ポリシーの更新](#)

データAmazonDataZoneGlue ManageAccessRolePolicyへの許可の発行とアクセスを Amazon DataZone に許可する許可のサポートを有効にするように を更新しました。詳細については、[「Amazon DataZone updates to AWS managed policies」](#) を参照してください。

2024 年 4 月 1 日

[AmazonDataZoneDomainExecutionRolePolicy および AmazonDataZoneFullUserAccess - ポリシーの更新](#)

CancelMetadataGenerationRun API のサポートを有効にするAmazonDataZoneFullUserAccessのために、AmazonDataZoneDomainExecutionRolePolicyとを更新しました。詳細については、「[Amazon DataZone updates to AWS managed policies](#)」を参照してください。

2024 年 3 月 29 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 できるように更新しました。詳細については、「[Amazon DataZone updates to AWS managed policies](#)」を参照してください。

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 ListEnvironmentBlueprintConfigurationSummaries API のサポートを有効にしました。詳細については、[「Amazon DataZone updates to AWS managed policies」](#)を参照してください。

2024 年 2 月 1 日

[AmazonDataZoneGlueManageAccessRolePolicy - ポリシーの更新](#)

AWS Lake Formation ハイブリッドモードのサポートを有効にするAmazonDataZoneGlueManageAccessRolePolicyようにを更新しました。詳細については、[「Amazon DataZone updates to AWS managed policies」](#)を参照してください。

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、[「Amazon DataZone updates to AWS managed policies」](#) を参照してください。

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。詳細については、[「Amazon DataZone updates to AWS managed policies」](#) を参照してください。

2023 年 11 月 17 日

[AmazonDataZoneRedshiftManageAccessRolePolicy - ポリシーの更新](#)

Amazon は、redshift: AssociateDataShare Consumer 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、AWS 組織間でリソースを共有できます。詳細については、「[Amazon DataZone updates to AWS managed policies](#)」を参照してください。

2023 年 11 月 16 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、「[AWS 管理ポリシーに対する Amazon DataZone の更新](#)」を参照してください。

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、「Amazon による [AWS マネージドポリシー DataZone の更新](#)」を参照してください。

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、「[Amazon による AWS マネージドポリシー DataZone の更新](#)」を参照してください。

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、「[Amazon DataZone updates to AWS managed policies](#)」を参照してください。

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、「[Amazon DataZone updates to AWS managed policies](#)」を参照してください。

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、「[Amazon DataZone updates to AWS managed policies](#)」を参照してください。

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、「[Amazon DataZone updates to AWS managed policies](#)」を参照してください。

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、AWS Glue データをカタログに発行するアクセス許可を Amazon DataZone にAmazonDataZoneGlueManageAccessRolePolicy付与しました。また、カタログ内の AWS Glue 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 Amazon アクセス許可も付与 DataZoneします。詳細については、「[Amazon DataZone updates to AWS managed policies](#)」を参照してください。

2023 年 9 月 12 日

### [AmazonDataZoneFull UserAccess - 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 AmazonDataZoneFull UserAccess 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、[「Amazon DataZone updates to AWS managed policies」](#) を参照してください。

2023 年 9 月 12 日

### [AmazonDataZoneFullAccess - 新しいポリシー](#)

Amazon は、AWS マネジメントコンソール DataZone 経由で Amazon へのフルアクセス AmazonDataZoneFull Access を提供する 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、[「Amazon DataZone updates to AWS managed policies」](#) を参照してください。

2023 年 9 月 12 日

### [AmazonDataZoneEnvironmentRolePermissionsBoundary - 新しいポリシー](#)

Amazon は、アタッチ先の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、[「Amazon DataZone updates to AWS managed policies」](#) を参照してください。

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、[「Amazon DataZone updates to AWS managed policies」](#)を参照してください。

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、[「Amazon DataZone updates to AWS managed policies」](#)を参照してください。

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。