aws

사용자 가이드

Amazon DataZone

Amazon DataZone: 사용자 가이드

Table of Contents

아마존이란 DataZone 무엇입니까? 1
..... 1
Amazon이 다른 제품을 DataZone 지원하고 통합하는 방법 AWS 서비스? 2
Amazon에 액세스하려면 어떻게 해야 DataZone 합니까? 2
용어 및 개념 4
Amazon DataZone 구성 요소 4
Amazon DataZone 도메인이란 무엇입니까? 5
Amazon DataZone 프로젝트 및 환경이란 무엇입니까? 5
Amazon DataZone 청사진이란 무엇입니까? 7
Amazon DataZone 인벤토리 및 게시 워크플로란 무엇입니까? 9
프로젝트 인벤토리 자산 생성 9
Amazon DataZone 카탈로그에 프로젝트 인벤토리 자산 게시 10
Amazon DataZone 구독 및 이행 워크플로란 무엇입니까? 11
Amazon의 사용자 페르소나 DataZone 11
Amazon DataZone 용어 12
무엇이 새로워졌나요? 20
2024년 20
Amazon DataZone , 도메인 단위 및 권한 부여 정책 출시 20
아마존 DataZone , 데이터 제품 출시 20
Amazon DataZone , 세분화된 액세스 제어 기능 출시 20
Amazon DataZone , 데이터 계보 기능 출시 21
아마존 DataZone , 커스텀 출시 AWS 서비스 청사진 21
데이터 소스 생성 흐름의 개선 22
아마존 DataZone , 아마존과의 통합 시작 SageMaker 22
아마존 DataZone , 다음과 통합 시작 AWS Lake Formation 하이브리드 액세스 모드 22
아마존 DataZone , 다음과 통합 시작 AWS Glue 데이터 품질 22
Amazon 내 설명에 대한 AI 권장 사항의 일반 출시 DataZone 23
아마존 DataZone , 아마존 Redshift 통합 개선 사항 출시 23
AWS Amazon을 위한 클라우드 구성 지원 DataZone 24
IAM주도자를 Amazon 프로젝트의 구성원으로 직접 추가 DataZone 24
데이터 포털의 사용자 지정 자산 유형 지원 25
2023년 25
도메인 삭제 25
하이브리드 모드 25

HIPAA자격 25
Amazon 설명에 대한 AI 권장 사항 DataZone (미리 보기) 26
DefaultDataLake 청사진 개선 26
설정 27
가입하세요. AWS account 27
관리 콘솔을 사용하는 데 필요한 IAM 권한을 구성합니다. 28
관리 콘솔 액세스를 위한 필수 및 선택적 정책을 사용자, 그룹 또는 역할에 첨부 28
관리 서비스 콘솔의 간소화된 역할 생성이 가능하도록 IAM 권한에 대한 사용자 지정 정책을 생성하십시오. 29
도메인과 연결된 계정을 관리할 수 있는 권한에 대한 사용자 지정 정책을 생성하십시오. 30
(선택 사항) 에 대한 사용자 지정 정책 생성 AWS 도메인에 대한 SSO 사용자 및 SSO 그룹 액세스 추가 및 제거를 위한 Identity Center 권한 33
(선택 사항) 고객 관리 키를 사용하여 도메인을 생성하려면 IAM 보안 주체를 키 사용자로 추가합니다. AWS KMS 34
데이터 포털을 사용하는 데 필요한 IAM 권한을 구성합니다. 34
데이터 포털 액세스를 위한 필수 정책을 사용자, 그룹 또는 역할에 연결 35
카탈로그 액세스를 위한 필수 정책을 사용자, 그룹 또는 역할에 연결 36
도메인이 고객 관리 키로 암호화된 경우 데이터 포털 또는 카탈로그 액세스를 위한 선택적 정책을 사용자, 그룹 또는 역할에 연결합니다. AWS KMS 37
설정 AWS IAM아마존 아이덴티티 센터 DataZone 38
시작하기 40
샘플 AWS Glue 데이터가 포함된 빠른 시작 가이드 40
1단계 - Amazon DataZone 도메인 및 데이터 포털 생성 41
2단계 - 게시 프로젝트 생성 43
3단계 - 환경 생성 43
4단계 - 게시를 위한 데이터 생성 43
5단계 - Glue에서 AWS 메타데이터 수집 44
6단계 - 데이터 자산 큐레이트 및 게시 45
7단계 - 데이터 분석을 위한 프로젝트 생성 45
8단계 - 데이터 분석을 위한 환경 생성 45
9단계 - 데이터 카탈로그 검색 및 데이터 구독 46
10단계 - 구독 요청 승인 46
11단계 - Amazon Athena에서 쿼리를 빌드하고 데이터를 분석합니다. 46
샘플 Amazon Redshift 데이터가 포함된 빠른 시작 가이드 47
1단계 - Amazon DataZone 도메인 및 데이터 포털 생성 47
2단계 - 게시 프로젝트 생성 49

3단계 - 환경 생성 49
4단계 - 게시를 위한 데이터 생성 50
5단계 - Amazon Redshift에서 메타데이터 수집 51
6단계 - 데이터 자산 큐레이트 및 게시 51
7단계 - 데이터 분석을 위한 프로젝트 생성 52
8단계 - 데이터 분석을 위한 환경 생성 52
9단계 - 데이터 카탈로그 검색 및 데이터 구독 53
10단계 - 구독 요청 승인 53
11단계 - Amazon Redshift에서 쿼리를 빌드하고 데이터 분석 53
일반적인 작업에 대한 샘플 스크립트 54
Amazon DataZone 도메인 및 데이터 포털 생성 54
게시 프로젝트 생성 55
환경 프로파일 생성 55
환경 생성 57
Glue에서 AWS 메타데이터 수집 58
데이터 자산 큐레이트 및 게시 61
데이터 카탈로그 검색 및 데이터 구독 64
데이터 카탈로그에서 자산 검색 64
기타 유용한 샘플 스크립트 67
도메인 및 사용자 액세스 69
도메인 생성 69
도메인 편집 71
도메인 삭제 72
Amazon용 IAM Identity Center 활성화 DataZone 73
Amazon용 IAM Identity Center 비활성화 DataZone 74
Amazon DataZone 콘솔에서 사용자 관리 75
IAM 역할 및 사용자 관리 76
SSO 사용자 관리 77
SSO 그룹 관리 78
데이터 포털에서 사용자 권한 관리 79
도메인 단위 및 권한 부여 정책 80
도메인 단위 생성 81
도메인 단위 편집 82
도메인 단위 삭제 83
도메인 유닛 소유자 관리 83
도메인 유닛 내의 사용자 및 그룹에 권한 부여 정책 할당 84

도메인 단위 계층의 프로젝트 멤버십 정책 85
도메인 유닛 내의 프로젝트에 권한 부여 정책 할당 91
블루프린트 구성 내에서 권한 부여 정책 할당 92
빌트인 블루프린트 94
에서 빌트인 블루프린트를 활성화합니다. AWS Amazon DataZone 도메인을 소유한 계정 94
SageMaker Amazon을 신뢰할 수 있는 서비스로 추가 AWS Amazon DataZone 도메인을 소유한 계정 100
사용자 지정 AWS 서비스 청사진 101
사용자 지정 AWS 서비스 청사진 활성화 101
사용자 지정 AWS 서비스 청사진을 사용하여 환경 생성 102
사용자 지정 AWS 서비스 환경에서 작업 생성 103
사용자 지정 AWS 서비스 환경에 프로젝트 멤버 추가 104
AWS 서비스 환경에서 데이터 소스 구성 104
AWS 서비스 환경에서 구독 대상 구성 105
연결된 계정 106
다른 AWS 계정과의 연결 요청 106
고객 관리형 KMS 키에 대한 계정 액세스 권한 제공 107
Amazon DataZone 도메인에서 계정 연결 요청을 수락하고 환경 청사진 활성화 107
연결된 AWS 계정에서 환경 청사진 활성화 108
연결된 AWS 계정에서 Amazon SageMaker 을 신뢰할 수 있는 서비스로 추가 114
Amazon DataZone 도메인에서 계정 연결 요청 거부 114
Amazon에서 연결된 계정 제거 DataZone 114
데이터 카탈로그 116
비즈니스 용어집 생성 117
비즈니스 용어집 편집 118
비즈니스 용어집 삭제 118
용어집에서 용어 생성 119
용어집에서 용어 편집 120
용어집에서 용어 삭제 121
메타데이터 양식 생성 122
메타데이터 양식 편집 122
메타데이터 양식 삭제 123
메타데이터 형식으로 필드 생성 124
메타데이터 양식의 필드 편집 125
메타데이터 양식의 필드 삭제 125
프로젝트 및 환경 127

환경 프로파일 생성 128
환경 프로파일 편집 130
환경 프로필 삭제 131
새 환경 생성 132
환경 편집 132
환경을 삭제합니다. 133
새 프로젝트 만들기 134
프로젝트 편집 134
프로젝트 삭제 135
프로젝트 나가기 136
프로젝트에 멤버 추가 137
프로젝트에서 멤버 제거 138
데이터 인벤토리 및 게시 139
Amazon에 대한 Lake Formation 권한 구성 DataZone 140
AWS Lake Formation 하이브리드 모드와 Amazon DataZone 통합 141
사용자 지정 자산 유형 생성 144
에 대한 데이터 소스 생성 및 실행 AWS Glue Data Catalog 148
Amazon Redshift용 데이터 소스 생성 및 실행 151
데이터 소스 편집 153
데이터 원본 삭제 154
프로젝트 인벤토리에서 카탈로그에 자산 게시 155
자산 게시 155
인벤토리 관리 및 자산 큐레이트 156
자산에 추가 메타데이터 양식 연결 157
큐레이션 후 카탈로그에 자산 게시 158
자산 수동 생성 158
카탈로그에서 자산 게시 취소 159
자산 삭제 160
데이터 소스 실행 수동 시작 160
자산 버전 관리 161
Amazon의 데이터 품질 DataZone 162
AWS Glue 자산에 대한 데이터 품질 활성화 162
사용자 지정 자산 유형에 대한 데이터 품질 활성화 163
Amazon에서 기계 학습 및 생성형 AI 사용 DataZone 165
Amazon의 데이터 계보 DataZone (미리 보기) 167
Amazon의 계보 노드 유형 DataZone 168

계보 노드의 키 속성 169
데이터 계보 시각화 169
Amazon의 데이터 계보 권한 부여 DataZone 170
Amazon에서의 데이터 계보 샘플 경험 DataZone 170
프로그래밍 방식으로 Amazon DataZone 데이터 계보 사용 171
데이터 제품 172
새 데이터 제품 생성 172
데이터 제품 게시 173
데이터 제품 편집 174
데이터 제품 게시 취소 175
데이터 제품 삭제 176
데이터 제품 구독 176
구독 요청을 검토하고 데이터 제품에 구독을 부여합니다. 177
데이터 제품 다시 게시 178
데이터 검색, 구독 및 소비 180
카탈로그에서 자산 검색 및 보기 181
자산 구독 요청 182
구독 요청 승인 또는 거부 182
기존 구독 취소 184
구독 요청 취소 185
자산 구독 취소 185
기존 IAM 역할을 사용하여 Amazon DataZone 구독 이행 186
관리 AWS Glue Data Catalog 형 자산에 대한 액세스 권한 부여 188
관리형 Amazon Redshift 자산에 대한 액세스 권한 부여 190
관리되지 않는 자산에 대해 승인된 구독에 대한 액세스 권한 부여 191
Amazon Athena 또는 Amazon Redshift에서 데이터 쿼리 191
Amazon Athena를 사용하여 데이터 쿼리 192
Amazon Redshift를 사용하여 데이터 쿼리 195
데이터에 대한 세분화된 액세스 제어 197
행 필터 생성 197
열 필터 생성 198
행 또는 열 필터 삭제 199
행 또는 열 필터 편집 200
필터로 액세스 권한 부여 200
AWS Glue 테이블 201
Amazon Redshift 201

이벤트 및 알림 202
Amazon DataZone 데이터 포털의 전용 수신함을 통한 이벤트 202
Amazon EventBridge 기본 버스를 통한 이벤트 207
보안 210
데이터 보호 211
데이터 암호화 212
전송 중 암호화 212
인터네트워크 트래픽 개인 정보 보호 212
Amazon에 대한 저장 데이터 암호화 DataZone 212
Amazon용 인터페이스 VPC 엔드포인트 사용 DataZone 220
Amazon에서의 권한 부여 DataZone 221
Amazon DataZone 콘솔의 권한 부여 221
Amazon DataZone 포털의 권한 부여 221
Amazon DataZone 프로필 및 역할 222
액세스 제어 222
AWS 관리형 정책 223
IAM Amazon의 역할 DataZone 316
임시 자격 증명 325
보안 주체 권한 326
규정 준수 확인 326
보안 모범 사례 327
최소 권한 액세스 구현 327
IAM 역할 사용 327
종속 리소스에서 서버 측 암호화 구현 328
CloudTrail 를 사용하여 API 통화 모니터링 328
복원력 328
데이터 소스 복원력 329
자산 복원력 329
자산 유형 및 메타데이터 형식 복원력 329
용어 복원력 329
글로벌 검색 복원력 330
구독 복원력 330
환경 복원력 330
환경 청사진 복원력 330
프로젝트 복원력 330
RAM 복원력 331

사용자 프로필 관리 복원력 331
도메인 복원력 331
Amazon의 인프라 보안 DataZone 331
Amazon의 교차 서비스 혼동 대리자 방지 DataZone 331
의 Amazon용 구성 및 취약성 분석 DataZone 332
허용 목록에 추가할 도메인 332
모니터링 333
이벤트 모니터링 333
CloudTrail 로그 334
아마존 DataZone 정보 입력 CloudTrail 334
문제 해결 335
Amazon에 대한 AWS Lake Formation 권한 문제 해결 DataZone 335
Amazon DataZone 계보 자산과 업스트림 데이터 세트 연결 문제 해결 337
SourceIdentifier 계보 노드의 337
Amazon은 OpenLineage 이벤트 sourceIdentifier 에서 를 어떻게 DataZone 구성하나요? 337
대체 접근 방식 343
자산 계보 노드의 업스트림 부족 문제 해결 344
할당량 348
문서 기록 350
..... ccclxxix

아마존이란 DataZone 무엇입니까?

DataZone Amazon은 여러 곳에 저장된 데이터를 더 빠르고 쉽게 카탈로그, 검색, 공유 및 관리할 수 있게 해주는 데이터 관리 서비스입니다. AWS, 온프레미스 및 타사 소스. DataZoneAmazon을 사용하면 조직의 데이터 자산을 감독하는 관리자가 세밀한 제어를 통해 데이터 액세스를 관리하고 제어할 수 있습니다. 이러한 제어를 통해 적절한 수준의 권한과 컨텍스트로 액세스를 보장할 수 있습니다. Amazon을 DataZone 사용하면 엔지니어, 데이터 과학자, 제품 관리자, 분석가 및 비즈니스 사용자가 조직 전체에서 데이터를 쉽게 공유하고 액세스하여 데이터를 발견하고 사용하고 협업하여 데이터 기반 통찰력을 도출할 수 있습니다.

DataZone Amazon은 Amazon Redshift, Amazon Athena, Amazon 등의 데이터 관리 서비스를 통합하여 최종 사용자에게 직접 데이터를 전달하고 아키텍처를 단순화할 수 있도록 지원합니다. QuickSight AWS Glue, AWS Lake Formation, 온프레미스 소스, 타사 소스 등.

주제

- Amazon으로 무엇을 할 수 있나요 DataZone?
- Amazon이 다른 제품을 DataZone 지원하고 통합하는 방법 AWS 서비스?
- Amazon에 액세스하려면 어떻게 해야 DataZone 합니까?

Amazon으로 무엇을 할 수 있나요 DataZone?

DataZoneAmazon에서는 다음과 같은 작업을 수행할 수 있습니다.

- 조직 경계를 초월한 데이터 액세스를 관리합니다. DataZoneAmazon을 사용하면 개별 자격 증명을 사용하지 않고도 조직의 보안 규정에 따라 올바른 사용자가 올바른 목적으로 올바른 데이터에 액세스하도록 할 수 있습니다. 또한 통제된 워크플로를 통해 데이터 자산 사용에 투명성을 제공하고 데이터 구독을 승인할 수 있습니다. 또한 사용 감사 기능을 통해 프로젝트 전반의 데이터 자산을 모니터링할 수 있습니다.
- 공유 데이터 및 도구를 통해 데이터 작업자를 연결하여 비즈니스 통찰력을 확보하세요. DataZoneAmazon을 사용하면 팀 간에 원활하게 협업하고 데이터 및 분석 도구에 대한 셀프 서비스 액세스를 제공하여 비즈니스 팀의 효율성을 높일 수 있습니다. 비즈니스 용어를 사용하여 에 저장된 카탈로그 데이터를 검색, 공유 및 액세스할 수 있습니다. AWS, 온프레미스 또는 타사 제공업체와 함께. 또한 Amazon DataZone 비즈니스 용어집을 사용하여 사용하려는 데이터에 대해 자세히 알아볼 수 있습니다.

- 기계 학습으로 데이터 검색 및 카탈로그 작성을 자동화하십시오. DataZoneAmazon을 사용하면 비즈니스 데이터 카탈로그에 데이터 속성을 수동으로 입력하는 데 소요되는 시간을 줄일 수 있습니다. 데이터 카탈로그의 데이터가 풍부해지면 검색 환경도 개선됩니다.

Amazon이 다른 제품을 DataZone 지원하고 통합하는 방법 AWS 서비스?

DataZone Amazon은 다른 제품과의 세 가지 유형의 통합을 지원합니다. AWS 서비스:

- 생산자 데이터 소스 - 저장된 데이터에서 Amazon DataZone 카탈로그에 데이터 자산을 게시할 수 있습니다. AWS Glue 데이터 카탈로그 및 Amazon Redshift 테이블 및 뷰. Amazon Simple Storage Service (S3) 의 객체를 Amazon 카탈로그에 수동으로 게시할 수도 있습니다. DataZone
- 소비자 도구 - Amazon Athena 또는 Amazon Redshift 쿼리 편집기를 사용하여 데이터 자산에 액세스하고 분석할 수 있습니다.
- 액세스 제어 및 주문 처리 - Amazon은 다음 항목에 대한 액세스 권한 DataZone 부여를 지원합니다. AWS 레이크 포메이션 관리 AWS Glue 테이블과 Amazon Redshift 테이블 및 뷰. 기타 모든 데이터 자산의 경우 Amazon은 사용자의 활동 (예: 구독 요청에 대한 승인) 과 관련된 표준 이벤트를 EventBridge Amazon에 DataZone 게시합니다. 이러한 표준 이벤트를 사용하여 다른 이벤트와 통합할 수 있습니다. AWS 맞춤형 통합을 위한 서비스 또는 타사 솔루션.

Amazon에 액세스하려면 어떻게 해야 DataZone 합니까?

다음 방법 중 하나로 DataZone Amazon에 액세스할 수 있습니다.

- 아마존 DataZone 콘솔

  Amazon DataZone 관리 콘솔을 사용하여 Amazon DataZone 도메인, 블루프린트 및 사용자에 액세스하고 구성할 수 있습니다. 자세한 내용은 /datazone을 참조하십시오. https://console.aws.amazon.com Amazon DataZone 관리 콘솔은 Amazon DataZone 데이터 포털을 생성하는 데도 사용됩니다.

- 아마존 DataZone 데이터 포털

  Amazon DataZone 데이터 포털은 셀프 서비스 방식으로 데이터를 카탈로그, 검색, 관리, 공유 및 분석할 수 있는 브라우저 기반 웹 애플리케이션입니다. 데이터 포털은 다음을 통해 ID 공급자의 자격 증명으로 사용자를 인증할 수 있습니다. AWS IAM아이덴티티 센터 (후속) AWS SSO) 또는 IAM 자

격 증명과 함께. https://console.aws.amazon.com/datazone에서 아마존 URL DataZone 콘솔에 액세스하여 데이터 포털을 얻을 수 있습니다.

- 아마존 DataZone HTTPS API

  서비스에 직접 HTTPS 요청을 보낼 수 있는 DataZone HTTPS API Amazon을 사용하여 DataZone 프로그래밍 방식으로 Amazon에 액세스할 수 있습니다. 자세한 내용은 Amazon DataZone API 레퍼런스를 참조하십시오.

Amazon DataZone 용어 및 개념

Amazon DataZone 은 , 온프레미스 및 타사 소스 AWS에 저장된 데이터를 더 빠르고 쉽게 카탈로그화, 검색, 공유 및 관리할 수 있는 데이터 관리 서비스입니다. Amazon 를 사용하면 조직의 데이터 자산을 감독하는 DataZone관리자 및 데이터 관리자가 세분화된 제어를 사용하여 데이터에 대한 액세스를 관리하고 제어할 수 있습니다. 이러한 제어는 적절한 수준의 권한 및 컨텍스트를 사용하여 액세스를 보장하도록 설계되었습니다. Amazon DataZone 을 사용하면 엔지니어, 데이터 과학자, 제품 관리자, 분석가 및 비즈니스 사용자가 조직 전체에서 데이터에 더 쉽게 액세스하여 데이터 기반 인사이트를 검색, 사용 및 협업할 수 있습니다.

Amazon 를 시작할 때 주요 개념 DataZone, 용어 및 구성 요소를 이해하는 것이 중요합니다.

주제

- Amazon DataZone 구성 요소
- Amazon DataZone 도메인이란 무엇입니까?
- Amazon DataZone 프로젝트 및 환경이란 무엇입니까?
- Amazon DataZone 청사진이란 무엇입니까?
- Amazon DataZone 인벤토리 및 게시 워크플로란 무엇입니까?
- Amazon DataZone 구독 및 이행 워크플로란 무엇입니까?
- Amazon의 사용자 페르소나 DataZone
- Amazon DataZone 용어

Amazon DataZone 구성 요소

Amazon에는 다음과 같은 네 가지 주요 구성 요소가 DataZone 포함되어 있습니다.

- 비즈니스 데이터 카탈로그 - 이 구성 요소를 사용하여 비즈니스 컨텍스트로 조직 전반의 데이터를 카탈로그화할 수 있으므로 조직의 모든 사람이 데이터를 빠르게 찾고 이해할 수 있습니다.
- 워크플로 게시 및 구독 - 이러한 자동화된 워크플로를 사용하여 생산자와 소비자 간의 데이터를 셀프서비스 방식으로 보호하고 조직의 모든 사람이 올바른 목적에 맞는 데이터에 액세스할 수 있도록 할 수 있습니다.
- 프로젝트 및 환경
  - Amazon DataZone 프로젝트에는 AWS 분석 액세스를 단순화하는 데 사용되는 사람, 자산(데이터) 및 도구의 비즈니스 사용 사례 기반 그룹화가 있습니다. 프로젝트는 프로젝트 멤버가 협업하

고, 데이터를 교환하고, 자산을 공유할 수 있는 영역을 제공합니다. 기본적으로 프로젝트는 프로젝트에 명시적으로 추가된 사용자만 해당 프로젝트 내의 데이터 및 분석 도구에 액세스할 수 있도록 구성됩니다. 프로젝트는 데이터 소비자가 액세스할 수 있는 프로젝트 정책에 따라 생성된 자산의 소유권을 관리합니다.

  - Amazon DataZone 프로젝트 내에서 환경은 지정된 보안 IAM 주체 집합(예: 기여자 권한이 있는 사용자)이 작동할 수 있는 0개 이상의 구성된 리소스(예: Amazon S3 버킷, AWS Glue 데이터베이스 또는 Amazon Athena 작업 그룹)의 모음입니다.
- 데이터 포털(AWS 관리 콘솔 외부) - 다양한 사용자가 셀프 서비스 방식으로 데이터를 카탈로그화, 검색, 관리, 공유 및 분석할 수 있는 브라우저 기반 웹 애플리케이션입니다. 데이터 포털은 를 통해 자격 IAM 증명 또는 자격 증명 공급자의 기존 자격 증명을 사용하여 사용자를 인증합니다 AWS IAM Identity Center.

Amazon DataZone 도메인이란 무엇입니까?

Amazon DataZone 도메인을 사용하여 자산, 사용자 및 해당 프로젝트를 구성할 수 있습니다. 추가 AWS 계정을 Amazon DataZone 도메인과 연결하면 데이터 소스를 통합할 수 있습니다. 그런 다음 메타데이터 양식과 용어집을 사용하여 이러한 데이터 소스의 자산을 도메인의 카탈로그에 게시하여 메타데이터 완전성과 품질을 개선할 수 있습니다. 또한 이러한 자산을 검색하고 검색하여 도메인에 게시된 데이터를 확인할 수 있습니다. 또한 프로젝트에 참여하여 다른 사용자와 협업하고, 자산을 구독하고, 프로젝트 환경을 사용하여 Amazon Athena 및 Amazon Redshift를 포함한 분석 도구에 액세스할 수 있습니다. Amazon DataZone 도메인을 사용하면 기업에 대한 단일 Amazon 도메인을 생성하든 다른 사업부에 대한 여러 Amazon DataZone 도메인을 생성하든 관계없이 조직 구조의 데이터 및 분석 요구 사항을 유연하게 반영 DataZone 할 수 있습니다.

Amazon DataZone 프로젝트 및 환경이란 무엇입니까?

Amazon을 DataZone 사용하면 팀과 분석 사용자가 팀, 도구 및 데이터의 사용 사례 기반 그룹화를 생성하여 프로젝트에서 협업할 수 있습니다.

- Amazon 에서 DataZone프로젝트는 사용자 그룹이 Amazon DataZone 카탈로그의 데이터 게시, 검색, 구독 및 소비와 관련된 다양한 비즈니스 사용 사례에 대해 협업할 수 있도록 합니다. 프로젝트 멤버는 Amazon DataZone 카탈로그의 자산을 사용하고 하나 이상의 분석 워크플로를 사용하여 새 자산을 생성합니다. 프로젝트는 데이터 포털 내에서 다음 활동을 지원합니다.
  - 프로젝트 소유자는 소유자, 기여자, 소비자, 관리인 및 최종 사용자 권한이 있는 멤버를 추가할 수 있습니다.
  - 프로젝트 멤버는 SSO 사용자, SSO 그룹 및 IAM 사용자일 수 있습니다.

- 프로젝트 멤버는 데이터 카탈로그의 자산에 대한 구독을 요청할 수 있습니다.

  프로젝트에 구독 승인이 제공됩니다.

	프로젝트 생성/삭제	프로젝트 프로필 생성/삭제	환경 프로필 생성/삭제	환경 생성/삭제	프로젝트에 멤버 추가/삭제	검색 및 검색	Create delete metad forms/ glo ssarie	데이터 소스 실행 생성 및 데이터 수집	데이터 게시	구독 요청	구독 요청 승인/거부	Amazon Athena 및 Amazon Redshift에서 구독 데이터 읽기
소유자	도메인 유닛 멤버에서 관리	도메인 유닛 멤버에서 관리	도메인 유닛 멤버에서 관리	도메인 유닛 멤버에서 관리	예	예	예	예	예	예	예	예
기고자	도메인 유닛 멤버에서 관리	도메인 유닛 멤버에서 관리	도메인 유닛 멤버에서 관리	도메인 유닛 멤버에서 관리	아니요	예	예	예	예	예	예	예
소비자	도메인 유닛 멤버에서 관리	도메인 유닛 멤버에서 관리	도메인 유닛 멤버에서 관리	도메인 유닛 멤버에서 관리	아니요	예	아니요	아니요	아니요	예	아니요	예

	프로젝트 생성/삭제	프로젝트 프로필 생성/삭제	환경 프로필 생성/삭제	환경 생성/삭제	프로젝트에 멤버 추가/삭제	검색 및 검색	Create delete metadforms/glossarie	데이터 소스 실행 생성 및 데이터 수집	데이터 게시	구독 요청	구독 요청 승인/거부	Amazon Athena 및 Amazon Redshift에서 구독 데이터 읽기
뷰어	도메인 유닛 멤버에서 관리	도메인 유닛 멤버에서 관리	도메인 유닛 멤버에서 관리	도메인 유닛 멤버에서 관리	아니요	예	아니요	아니요	아니요	아니요	아니요	예
스튜어드	도메인 유닛 멤버에서 관리	도메인 유닛 멤버에서 관리	도메인 유닛 멤버에서 관리	도메인 유닛 멤버에서 관리	아니요	예	예	예	예	아니요	예	예

- Amazon DataZone 프로젝트에서 환경은 0개 이상의 구성된 리소스(예: Amazon S3, AWS Glue 데이터베이스 또는 Amazon Athena 작업 그룹)의 컬렉션으로, 해당 리소스에서 작동할 수 있는 지정된 IAM 보안 주체 집합이 있습니다. 환경은 환경을 생성하기 위해 재사용 가능한 템플릿을 제공하는 미리 구성된 리소스 및 청사진 세트인 환경 프로파일을 사용하여 생성됩니다. 환경 프로파일은 환경이 배포되는 AWS 계정 또는 리전과 같은 설정을 정의합니다.

Amazon DataZone 청사진이란 무엇입니까?

환경이 생성되는 청사진은 환경이 속한 프로젝트의 AWS 도구 및 서비스(예: AWS Glue Amazon Redshift) 멤버가 Amazon DataZone 카탈로그의 자산으로 작업할 때 사용할 수 있는 도구를 정의합니다.

Amazon 의 현재 릴리스에서는 다음과 같은 기본 청사진 DataZone이 지원됩니다.

청사진 이름	설명	생성할 리소스
Data Lake 청사진	Amazon DataZone 프로젝트 멤버가 환경 내에서 Data Lake 생산자 및 소비자 서비스를 시작할 수 있습니다. 소비자 인 Amazon DataZone 프로젝트 멤버는 이를 통해 Amazon Athena 및 기타 Lake Formation 지원 쿼리 엔진에서 Lake Formation 관리형 자산의 '읽기 전용' 사본에 직접 액세스할 수 있습니다. 생산자 인 Amazon DataZone 프로젝트 멤버는 Amazon Athena를 사용하여 새 LakeFormation관리형 테이블을 생성하고 Amazon DataZone 카탈로그에 게시할 수 있습니다.	사용자에게 Amazon Athena 를 사용하여 Lake Formation 테이블을 생성하고 쿼리할 수 있는 기능을 제공합니다. Amazon Athena 작업 그룹, '읽기 전용' Lake Formation 권한, '읽기 전용' IAM 권한 및 프로젝트에서 관리하는 Amazon S3에 대한 액세스 권한이 있는 AWS Glue 데이터베이스. '생성' 및 '승인' Lake Formation 권한, '읽기' 및 '쓰기' IAM 권한(AWS Glue ETL추출, 변환 및 로드)과 태그 지정이 있는 AWS Glue 데이터베이스.
데이터 웨어하우스 청사진	소비자로서 이 청사진을 통해 Amazon DataZone 프로젝트 멤버는 자체 Amazon Redshift 클러스터에 연결하여 원격 데이터 스토어를 쿼리하고 새 데이터 세트를 생성하고 저장할 수 있습니다. 생산자 인 이 청사진을 통해 Amazon DataZone 프로젝트 멤버는 자체 Amazon Redshift 클러스터에 연결하여 원격 데이터 스토어를 쿼리하고,	Amazon Redshift 쿼리 편집기에 대한 액세스, Amazon DataZone 카탈로그에서 구독한 데이터 소스에 대한 '읽기' 액세스, 구성된 Amazon Redshift 클러스터에서 로컬 자산을 생성하는 기능. Amazon Redshift 쿼리 편집기에 대한 액세스, Amazon DataZone 카탈로그에서 구독한 데이터 소스에 대한 '읽기' 액세스, 구성된 Amazon Redshift 클러스터

청사진 이름	설명	생성할 리소스
	새 데이터 세트를 생성하고, Amazon DataZone 카탈로그에 게시할 수 있습니다.	에서 자산을 생성하고 게시하는 기능.
Amazon Sagemaker 청사진	이 청사진은 데이터 생산자와 소비자가 Amazon으로 원활하게 전환 SageMaker 하여 기계 학습(ML) 프로젝트에서 협업하는 동시에 데이터 및 ML 자산에 대한 액세스 거버넌스를 적용하는 데 도움이 됩니다. Amazon DataZone 과 Amazon 간의 새로운 내장 통합을 통해 SageMaker데이터 소비자와 생산자는 인프라 설정 전반에 걸쳐 ML 거버넌스를 간소화하고, 비즈니스 이니셔티브에서 협업하고, 데이터 및 ML 자산을 쉽게 관리할 수 있습니다.	Amazon 에서 데이터 및 ML 자산을 검색, 구독 및 게시할 수 있는 Amazon SageMaker 도메인을 생성할 수 있습니다 DataZone. 또한 구성된 대로 AWS Glue 데이터베이스 및 레이크 형성을 구독하고 게시할 수 있습니다.

Amazon DataZone 인벤토리 및 게시 워크플로란 무엇입니까?

프로젝트 인벤토리 자산 생성

Amazon DataZone 을 사용하여 데이터를 카탈로그화하려면 먼저 Amazon 에서 데이터(자산)를 프로젝트의 인벤토리로 가져와야 합니다 DataZone. 프로젝트의 인벤토리를 생성하면 해당 프로젝트의 구성원만 자산을 검색할 수 있습니다. 프로젝트 인벤토리 자산은 명시적으로 게시되지 않는 한 검색/찾아보기에서 모든 도메인 사용자가 사용할 수 있는 것은 아닙니다. Amazon 의 현재 릴리스에서는 다음과 같은 방법으로 프로젝트 인벤토리에 자산을 추가할 DataZone수 있습니다.

- 데이터 포털을 통해 또는 Amazon 를 사용하여 데이터 소스를 생성하고 실행합니다 DataZone APIs. Amazon 의 현재 릴리스에서는 AWS Glue 및 Amazon Redshift에 대한 데이터 소스를 생성하고 실행할 DataZone수 있습니다. AWS Glue 또는 Amazon Redshift 데이터 소스를 생성하고 실행하면 선택한 프로젝트 인벤토리에 자산을 생성하고 소스 데이터베이스 테이블 또는 데이터 웨어하우스에서 해당 기술 메타데이터를 인벤토리로 Amazon 로 가져옵니다 DataZone.

- 를 사용하면 사용 가능한 시스템 자산 유형(AWS Glue, Amazon Redshift, Amazon S3 객체) 또는 사용자 지정 자산 유형에서 자산을 생성할 APIs수 있습니다.
  - Amazon 를 사용하여 프로젝트 인벤토리에 사용자 지정 자산 유형을 생성합니다 DataZone APIs. 사용자 지정 자산 유형에는 ML 모델, 대시보드, 온프레미스 테이블 등이 포함될 수 있습니다.
  - Amazon 를 사용하여 이러한 사용자 지정 자산 유형에서 자산을 생성합니다 DataZone APIs.
- Amazon DataZone 데이터 포털을 사용하여 S3 객체에 대한 자산을 수동으로 생성합니다.

프로젝트 인벤토리 자산 큐레이팅 - 프로젝트 인벤토리를 생성한 후 데이터 소유자는 비즈니스 이름(자산 및 스키마), 설명(자산 및 스키마), 읽기 권한, 용어집 용어(자산 및 스키마) 및 메타데이터 양식을 추가하거나 업데이트하여 필요한 비즈니스 메타데이터로 인벤토리 자산을 큐레이팅할 수 있습니다. 데이터 포털 또는 Amazon 를 사용하여 이 작업을 수행할 수 있습니다 DataZone APIs. 자산을 편집할 때마다 새 인벤토리 버전이 생성됩니다.

Amazon DataZone 카탈로그에 프로젝트 인벤토리 자산 게시

Amazon DataZone 을 사용하여 데이터를 카탈로그화하는 다음 단계는 도메인 사용자가 프로젝트의 인벤토리 자산을 검색할 수 있도록 하는 것입니다. 인벤토리 자산을 Amazon DataZone 카탈로그에 게시하여 이 작업을 수행할 수 있습니다. 최신 버전의 인벤토리 자산만 카탈로그에 게시할 수 있으며 최신 게시 버전만 검색 카탈로그에서 활성화됩니다. 인벤토리 자산이 Amazon DataZone 카탈로그에 게시된 후 업데이트되는 경우 최신 버전이 검색 카탈로그에 포함되도록 다시 명시적으로 게시해야 합니다. Amazon 의 현재 릴리스에서는 다음과 같은 방법으로 Amazon DataZone 카탈로그에 프로젝트 인벤토리 자산을 게시할 DataZone수 있습니다.

- 데이터 포털을 통해 또는 Amazon 를 사용하여 Amazon DataZone 카탈로그에 프로젝트 인벤토리 자산을 수동으로 게시합니다 DataZone APIs.
- 데이터 소스 생성 또는 편집의 일환으로 선택 사항인 AWS Glue 자산을 카탈로그에 게시하거나 Amazon Redshift 자산을 카탈로그 설정에 게시하여 예약되거나 자동화된 데이터 소스 실행 중에 사용할 수 있도록 합니다. 이 설정이 활성화되면 데이터 소스 실행이 프로젝트의 인벤토리에 자산을 추가한 다음 인벤토리 자산을 Amazon DataZone 카탈로그에 게시합니다. 직접 게시하는 경우 자산에 비즈니스 메타데이터가 없을 수 있으며 모든 도메인 사용자가 직접 검색할 수 있습니다. 데이터 포털을 통해 또는 Amazon 를 사용하여 데이터 소스에서 이 설정을 사용할 수 있습니다 DataZone APIs.

Amazon DataZone 구독 및 이행 워크플로란 무엇입니까?

자산이 Amazon DataZone 카탈로그에 게시되면 도메인 사용자는 이러한 자산을 검색하고, 이러한 자산에 대한 액세스를 요청 및 획득하고, Amazon DataZone 을 계속 사용하여 이러한 자산을 관리, 공유 및 분석할 수 있습니다.

사용자는 프로젝트를 대신하여 해당 자산을 구독하여 자산에 대한 액세스를 요청합니다. 구독 요청이 생성되면 자산 소유자는 알림을 받고 구독 요청을 검토하고 승인할지 거부할지 결정할 수 있습니다. 데이터 소유자가 구독 요청을 승인하면 구독 프로젝트에 해당 자산에 대한 액세스 권한이 부여됩니다.

구독 요청이 승인되면 Amazon은 AWS Lake Formation 또는 Amazon Redshift에서 필요한 권한을 생성하여 프로젝트 내의 모든 해당 환경에 자산을 자동으로 추가하는 구독 이행 워크플로를 DataZone 시작합니다. 이를 통해 구독 프로젝트 멤버는 환경에서 쿼리 도구(Amazon Athena 또는 Amazon Redshift 쿼리 편집기) 중 하나를 사용하여 자산을 쿼리할 수 있습니다.

Amazon은 관리형 자산에 대해서만 이 자동 이행 로직을 트리거할 DataZone 수 있습니다(AWS Glue 테이블 및 Amazon Redshift 테이블 및 뷰 포함). 다른 모든 자산 유형(관리되지 않는 자산)의 경우 Amazon은 이행을 자동으로 트리거할 DataZone 수 없지만 대신 Amazon Eventbridge에 이벤트 페이로드에 필요한 모든 세부 정보를 포함하는 이벤트를 게시하여 Amazon 외부에서 필요한 권한을 생성할 수 있습니다 DataZone. DataZone 또한 Amazon은 Amazon 외부`updateSubscriptionStatus`API에서 구독이 이행되면 구독 상태를 업데이트할 DataZone 수 DataZone 있는 를 제공하므로 Amazon은 프로젝트 멤버에게 자산 소비를 시작할 수 있음을 알릴 수 있습니다.

Amazon의 사용자 페르소나 DataZone

다음은 기본 Amazon DataZone 사용자 페르소나입니다.

- Amazon을 조직의 분석 플랫폼 DataZone 으로 설정하는 도메인 관리자입니다.

  Amazon 의 맥락에서 DataZone도메인 관리자는 AWS 계정에 Amazon DataZone 을 설치하고, Amazon DataZone 도메인을 생성하고, Amazon 도메인과의 AWS 계정 연결 및 자격 증명 공급자 연결을 구성합니다 DataZone . 도메인 관리자는 AWS Organization and Service Catalog와 같은 다른 AWS 서비스 콘솔을 사용하여 Amazon 를 구성합니다 DataZone.
- 분석 및 기계 학습 작업을 위한 Amazon의 주요 사용자 DataZone (자산 게시자 및 구독자)인 데이터 사용자입니다.

  데이터 사용자에는 데이터 분석 작업자, 데이터 과학자 및 데이터 자산을 생산하고 소비하는 시스템 사용자가 포함됩니다. Amazon 의 맥락에서 DataZone데이터 사용자는 프로젝트 및 환경을 생성 및

조인하고, 사전 구성된 분석 또는 기계 학습 도구를 사용하여 데이터 자산을 구독 및 소비하고, 출력 데이터 자산을 Amazon DataZone 도메인 카탈로그에 다시 게시하여 다른 사용자와 공유합니다.

- 사용자 지정 인프라 템플릿을 구축하고 Amazon DataZone 을 내부 카탈로그 또는 프로덕션 시스템과 통합하는 시스템 개발자입니다.

  Amazon 의 맥락에서 DataZone시스템 개발자는 환경 청사진(인프라 템플릿) 또는 Infrastructure-As-Code 환경 공급자인 CI/CD 파이프라인, 환경 전반의 데이터 자산을 홍보하는 데이터 파이프라인, 내부 카탈로그와 통합하기 위한 카탈로그 동기화 및 구독 권한 부여 이행 어댑터 또는 필요한 경우 Amazon DataZoneAPIs과 내부 사용자 인터페이스 또는 프로덕션 시스템 간의 통합을 구축합니다.
- 조직 보안, 개인정보 보호 및 기타 규정 준수 정책의 정의와 위험을 소유하고 DataZone 조직에서 Amazon을 사용하는 것이 이러한 정의를 준수하는지 확인하는 데이터 거버넌스 책임자.

Amazon DataZone 용어

도메인

Amazon DataZone 도메인은 자산, 사용자 및 해당 프로젝트를 함께 연결하기 위한 조직 엔터티입니다. Amazon DataZone 도메인을 사용하면 기업을 위한 단일 Amazon DataZone 도메인을 생성하든 여러 비즈니스 단위 또는 팀을 위한 여러 데이터 영역, 도메인을 생성하든 관계없이 조직 구조의 데이터 및 분석 요구 사항을 유연하게 반영할 수 있습니다.

도메인 단위

도메인 단위를 사용하면 특정 사업부 및 팀에서 자산 및 기타 도메인 엔터티를 쉽게 구성할 수 있습니다. 조직의 사업부 내에서 그리고 사업부 간에 안전하고 효율적인 데이터 공유를 설정하려면 Amazon 내에서 도메인 단위를 생성하고 각 사업부 내에서 선택한 사용자가 카탈로그에 로그인하여 자산을 공유할 수 DataZone 있도록 할 수 있습니다. 또한 도메인 단위를 사용하여 AWS 계정 소유자와 같은 리소스 소유자가 리소스에 대한 Amazon DataZone 권한 부여 권한을 설정할 수 있습니다. 도메인 유닛은 계정 소유자로부터 도메인 유닛 소유자에게 위임된 권한을 제공하며 계정 소유자를 대신하여 환경 프로파일(청사진 구성을 사용하여 생성됨)에 대한 권한 부여 권한을 설정할 수 있습니다. 자세한 내용은 Amazon의 도메인 단위 및 권한 부여 정책 DataZone 단원을 참조하십시오.

권한 부여 정책

Amazon DataZone 권한 부여 정책은 프로젝트, 청사진, 환경, 용어집 및 메타데이터 양식과 같은 엔터티에 DataZone 적용되는 Amazon 내의 제어 집합입니다. 이러한 정책은 Amazon DataZone 포털에서 이러한 엔터티를 생성하고 수명 주기를 관리할 수 있는 사용자를 정의합니다.

Amazon DataZone 도메인 유닛 내에서 사용자 및 그룹에 다음 권한 부여 정책을 할당하여 특정 권한을 부여할 수 있습니다.

- 도메인 단위 생성 정책
- 프로젝트 생성 정책
- 프로젝트 멤버십 정책
- 도메인 유닛 소유권 가정 정책
- 프로젝트 소유권 가정 정책

자세한 내용은 Amazon DataZone 도메인 유닛 내의 사용자 및 그룹에 권한 부여 정책 할당 단원을 참조하십시오.

Amazon DataZone 도메인 유닛 내에서 프로젝트에 다음 권한 부여 정책을 할당하여 특정 권한을 부여할 수 있습니다.

- 용어 생성 정책
- 메타데이터 양식 생성 정책
- 사용자 지정 자산 유형 생성 정책

자세한 내용은 Amazon DataZone 도메인 유닛 내의 프로젝트에 권한 부여 정책 할당 단원을 참조하십시오.

특정 청사진 구성 내에서 프로젝트 및 도메인 유닛 소유자에게 다음과 같은 권한 부여 정책을 할당할 수 있습니다.

- 이 청사진을 사용하여 환경 프로파일 생성 - 이 정책은 Amazon DataZone 프로젝트에 할당할 수 있으며 이 청사진을 사용하여 환경 프로파일을 생성할 수 있는 권한을 부여합니다.
- 이 청사진을 사용하여 환경 프로파일을 생성할 수 있는 권한을 부여합니다. 이 정책은 도메인 유닛 소유자에게 할당할 수 있으며 이 청사진을 사용하여 환경 프로파일을 생성할 수 있는 권한을 프로젝트에 부여합니다.

자세한 내용은 Amazon DataZone 블루프린트 구성 내에서 권한 부여 정책 할당 단원을 참조하십시오.

연결된 계정

AWS 계정을 Amazon DataZone 도메인과 연결하면 이러한 AWS 계정의 데이터를 Amazon DataZone 카탈로그에 게시하고 여러 AWS 계정에서 데이터를 사용할 Amazon DataZone 프로젝트를 생성할 수 있습니다. 계정 연결 요청은 Amazon DataZone 도메인을 소유한 AWS 계정에서만 시작할 수 있습니다. 계정 연결 요청은 초대된 AWS 계정의 관리 사용자만 수락할 수 있습니다. AWS 계정이 Amazon DataZone 도메인과 연결되면 이 계정의 AWS Glue 카탈로그 및 Amazon

Redshift와 같은 데이터 소스를 이 도메인에 등록할 수 있습니다. 또한 계정을 연결하면 AWS 계정이 Amazon DataZone 프로젝트 및 환경을 생성할 수 있습니다.

는 하나 이상의 Amazon DataZone 도메인과 연결할 AWS 계정 수 있습니다.

데이터 소스

Amazon 에서는 데이터 소스를 사용하여 소스 데이터베이스 또는 데이터 웨어하우스에서 Amazon 로 자산(데이터)의 기술적 메타데이터를 가져올 DataZone수 있습니다 DataZone. Amazon 의 현재 릴리스에서는 AWS Glue 및 Amazon Redshift에 대한 데이터 소스를 생성하고 실행할 DataZone 수 있습니다. 데이터 소스를 생성하면 Amazon DataZone 과 소스(AWS Glue Data Catalog 또는 Amazon Redshift Warehouse) 간에 연결을 설정하여 테이블 이름, 열 이름 및 데이터 유형을 비롯한 기술적 메타데이터를 읽을 수 있습니다. 데이터 소스를 생성하면 Amazon 에서 새 를 생성하거나 기존 자산을 업데이트하는 초기 데이터 소스 실행도 시작됩니다 DataZone. 데이터 소스를 생성하는 동안 또는 데이터 소스가 성공적으로 생성된 후 데이터 소스 실행 일정을 지정하는 옵션도 있습니다.

데이터 소스 실행

Amazon 에서 DataZone데이터 소스 실행은 Amazon이 프로젝트 인벤토리에 자산을 생성하고 선택적으로 Amazon DataZone 카탈로그에 프로젝트 인벤토리 자산을 게시하기 위해 DataZone 수행하는 작업입니다. 데이터 소스 실행은 자동화(데이터 소스가 처음 생성될 때 시작됨)하거나 예약하거나 수동으로 수행할 수 있습니다. 데이터 선택 기준을 사용하면 프로젝트 인벤토리 또는 Amazon DataZone 카탈로그에 수집할 기존 및 향후 데이터 세트와 해당 인벤토리 또는 카탈로그 자산에 대한 메타데이터 업데이트 빈도를 미세 조정할 수 있습니다.

구독 대상

Amazon 에서 DataZone구독 대상을 사용하면 프로젝트에서 구독한 데이터에 액세스할 수 있습니다. 구독 대상은 Amazon DataZone 프로젝트 멤버가 구독한 데이터에 대한 쿼리를 시작할 DataZone 수 있도록 Amazon이 소스 데이터와의 연결을 설정하고 필요한 권한을 생성하는 데 사용할 수 있는 위치(예: 데이터베이스 또는 스키마)와 필요한 권한(예: IAM 역할)을 지정합니다.

구독 요청

Amazon 에서 DataZone구독 요청은 특정 자산에 대한 액세스 권한을 부여받기 위해 Amazon DataZone 프로젝트가 따라야 하는 프로세스입니다. 구독 요청은 승인, 거부, 취소 또는 부여할 수 있습니다.

자산

Amazon 에서 DataZone자산은 단일 물리적 데이터 객체(예: 테이블, 대시보드, 파일) 또는 가상 데이터 객체(예: 뷰)를 제공하는 엔터티입니다.

애셋 유형

자산 유형은 Amazon DataZone 카탈로그에서 자산을 나타내는 방법을 정의합니다. 자산 유형은 특정 유형의 자산에 대한 스키마를 정의합니다. 자산이 생성되면 자산 유형(기본적으로 최신 버전)에 의해 정의된 스키마에 대해 검증됩니다. 자산 업데이트가 발생하면 Amazon은 새 자산 버전을 DataZone 생성하고 Amazon DataZone 사용자가 모든 자산 버전에서 작업할 수 있도록 합니다.

비즈니스 용어집

Amazon 에서 DataZone비즈니스 용어집은 자산과 연결될 수 있는 비즈니스 용어 모음입니다. 비즈니스 용어집은 조직 전체에서 다양한 데이터 분석 작업 전반에 걸쳐 동일한 용어와 정의를 사용하도록 하는 데 도움이 됩니다.

비즈니스 용어집의 용어는 자산 및 열에 추가하여 검색 중에 이러한 속성의 식별을 분류하거나 개선할 수 있습니다. 용어집은 자산과 연결된 메타데이터 형식의 필드에 대한 값 유형으로 선택할 수 있습니다. 자산의 메타데이터 양식 필드 값으로 특정 용어를 선택하면 사용자는 비즈니스 용어집 용어를 검색하고 관련 자산을 찾을 수 있습니다.

메타데이터 양식 유형

메타데이터 양식 유형은 자산이 인벤토리로 생성되거나 Amazon DataZone 도메인에 게시될 때 수집 및 저장되는 메타데이터를 정의하는 템플릿입니다. 메타데이터 양식 유형은 데이터 자산과 연결할 수 있습니다. 메타데이터 양식 유형은 도메인 관리자가 규정 준수 정보, 규제 정보 또는 분류와 같은 도메인에 필요한 메타데이터 양식을 정의하는 데 도움이 됩니다. 이를 통해 도메인 관리자는 자산에 대한 추가 메타데이터를 사용자 지정할 수 있습니다. Amazon DataZone 에는 asset-common-details-form-type, column-business-metadata-form-type,, glue-table-form-type,, glue-view-form-type redshift-table-form-type redshift-view-form-type, s3-object-collection-form-type subscription-terms-form-type, 및 와 같은 시스템 메타데이터 양식 유형이 있습니다 suggestion-form-type.

메타데이터 양식

Amazon 에서 DataZone메타데이터 양식은 자산이 인벤토리로 생성되거나 Amazon DataZone 도메인에 게시될 때 수집 및 저장되는 메타데이터를 정의합니다. 메타데이터 양식 정의는 도메인 관리자가 카탈로그 도메인에 생성합니다. 메타데이터 양식 정의는 부울, 날짜, 십진수, 정수, 문자열 및 비즈니스 용어집 필드 값 데이터 유형을 지원하는 하나 이상의 필드 정의로 구성됩니다.

도메인 관리자는 메타데이터 양식을 도메인에 추가하여 메타데이터 양식을 도메인의 자산에 적용합니다. 그런 다음 자산 게시자는 메타데이터 양식에 선택적 필수 필드 값을 제공합니다.

프로젝트

Amazon 에서 DataZone프로젝트는 사용자 그룹이 프로젝트 인벤토리에서 자산을 생성하여 모든 프로젝트 멤버가 검색할 수 있도록 한 다음 Amazon DataZone 카탈로그에 자산을 게시, 검색, 구독 및 소비하는 다양한 비즈니스 사용 사례에 대해 협업할 수 있도록 합니다. 프로젝트 멤버는 Amazon DataZone 카탈로그의 자산을 사용하고 하나 이상의 분석 워크플로를 사용하여 새 자산을 생성합니다. 프로젝트 멤버는 소유자, 기여자, 소비자, 관리인 및 최종 사용자일 수 있습니다.

	프로젝트 생성/삭제	프로젝트 프로필 생성/삭제	환경 프로필 생성/삭제	환경 생성/삭제	프로젝트에 멤버 추가/삭제	검색 및 검색	Create delete metadforms/glossarie	데이터 소스 실행 생성 및 데이터 수집	데이터 게시	구독 요청	구독 요청 승인/거부	Amazon Athena 및 Amazon Redshift에서 구독 데이터 읽기
소유자	도메인 유닛 멤버에서 관리	도메인 유닛 멤버에서 관리	도메인 유닛 멤버에서 관리	도메인 유닛 멤버에서 관리	예	예	예	예	예	예	예	예
기고자	도메인 유닛 멤버에서 관리	도메인 유닛 멤버에서 관리	도메인 유닛 멤버에서 관리	도메인 유닛 멤버에서 관리	아니요	예	예	예	예	예	예	예
소비자	도메인 유닛 멤버	도메인 유닛 멤버	도메인 유닛 멤버	도메인 유닛 멤버	아니요	예	아니요	아니요	아니요	예	아니요	예

	프로젝트 생성/삭제	프로젝트 프로필 생성/삭제	환경 프로필 생성/삭제	환경 생성/삭제	프로젝트에 멤버 추가/삭제	검색 및 검색	Create delete metadforms/glossarie	데이터 소스 실행 생성 및 데이터 수집	데이터 게시	구독 요청	구독 요청 승인/거부	Amazon Athena 및 Amazon Redshift에서 구독 데이터 읽기
	에서 관리	에서 관리	에서 관리	에서 관리								
뷰어	도메인 유닛 멤버에서 관리	도메인 유닛 멤버에서 관리	도메인 유닛 멤버에서 관리	도메인 유닛 멤버에서 관리	아니요	예	아니요	아니요	아니요	아니요	아니요	예
스튜어드	도메인 유닛 멤버에서 관리	도메인 유닛 멤버에서 관리	도메인 유닛 멤버에서 관리	도메인 유닛 멤버에서 관리	아니요	예	예	예	예	아니요	예	예

프로젝트 소유자는 다른 사용자를 소유자 또는 기여자로 추가하거나 제거할 수 있으며 프로젝트를 수정하거나 삭제할 수 있습니다. 기여자에 대한 기타 제한은 정책을 통해 정의할 수 있습니다. 사용자가 프로젝트를 생성하면 해당 프로젝트의 첫 번째 소유자가 됩니다.

환경

환경은 구성된 리소스(예: Amazon S3 버킷, AWS Glue 데이터베이스 또는 Amazon Athena 작업 그룹)의 모음으로, 해당 리소스에서 작동할 수 있는 지정된 IAM 보안 주체 집합(할당된 기여자 권한 있음)이 있습니다. 각 환경에는 리소스에 액세스하고 구독 및 이행을 통해 데이터에 액세스할 수 있는 권한이 있는 사용자 보안 주체가 있을 수도 있습니다. 환경은 AWS 서비스 및 외부 IDEs 및 콘솔

에 실행 가능한 링크를 저장하도록 설계되었습니다. 프로젝트 구성원은 환경 내에 구성된 딥 링크를 통해 Amazon Athena 콘솔 등과 같은 서비스에 액세스할 수 있습니다. SSO 프로젝트의 사용자 및 IAM 사용자는 특정 환경을 사용/액세스하도록 범위를 더 줄일 수 있습니다.

환경 프로파일

Amazon 에서 DataZone환경 프로파일은 환경을 생성하는 데 사용할 수 있는 템플릿입니다. 환경 프로파일은 청사진을 사용하여 생성됩니다.

환경 프로파일을 사용하면 도메인 관리자가 블루프린트를 사전 구성된 파라미터로 래핑한 다음 데이터 워커는 기존 환경 프로파일을 선택하고 새 환경의 이름을 지정하여 원하는 수의 새 환경을 빠르게 생성할 수 있습니다. 이를 통해 데이터 워커는 프로젝트와 환경을 효율적으로 관리하는 동시에 도메인 관리자가 시행하는 데이터 거버넌스 정책을 충족할 수 있습니다.

청사진

환경이 생성되는 청사진은 환경이 속한 프로젝트의 AWS 도구 및 서비스(예: AWS Glue Amazon Redshift) 멤버가 Amazon DataZone 카탈로그의 자산으로 작업할 때 사용할 수 있는 도구를 정의합니다.

Amazon의 현재 릴리스에서는 다음과 DataZone 같은 기본 청사진이 지원됩니다.

- 데이터 레이크 청사진
- 데이터 웨어하우스 청사진
- Amazon Sagemaker 청사진

사용자 프로필

사용자 프로필은 Amazon DataZone 사용자를 나타냅니다. Amazon DataZone 은 다양한 목적으로 Amazon DataZone Management Console 및 데이터 포털과 상호 작용할 수 있는 IAM 역할과 SSO 자격 증명을 모두 지원합니다. 도메인 관리자는 IAM 역할을 사용하여 새 Amazon 도메인 생성, 메타데이터 양식 유형 구성, 정책 구현을 포함하여 Amazon DataZone Management Console에서 초기 관리 DataZone 도메인 관련 작업을 수행합니다. 데이터 워커는 Identity Center를 통해 SSO 기업 자격 증명을 사용하여 Amazon DataZone Data Portal에 로그인하고 멤버십이 있는 프로젝트에 액세스합니다.

그룹 프로필

그룹 프로필은 Amazon DataZone 사용자 그룹을 나타냅니다. 그룹을 수동으로 생성하거나 엔터프라이즈 고객 Active Directory 그룹에 매핑할 수 있습니다. Amazon 에서 DataZone그룹은 두 가지 목적을 수행합니다. 먼저 그룹은 조직도의 사용자 팀에 매핑할 수 있으므로 팀에 합류하거나 퇴근하는 신입 직원이 있을 때 Amazon DataZone 프로젝트 소유자의 관리 작업을 줄일 수 있습니다.

둘째, 기업 관리자는 Active Directory 그룹을 사용하여 사용자 상태를 관리하고 업데이트하므로 Amazon DataZone 도메인 관리자는 이러한 그룹 멤버십을 사용하여 Amazon DataZone 도메인 정책을 구현할 수 있습니다.

도메인 관리자

Amazon 에서 Amazon DataZone 도메인을 생성하는 DataZone IAM 보안 주체는 해당 도메인의 기본 도메인 관리자입니다. Amazon의 도메인 관리자는 도메인 생성, 다른 도메인 관리자 할당, 데이터 소스 및 구독 대상 추가, 프로젝트 및 환경 생성, 프로젝트 소유자 할당 등 도메인에 대한 주요 기능을 DataZone 수행합니다.

게시자

Amazon 에서 DataZone게시자는 Amazon DataZone 카탈로그에 자산을 게시하고 게시하는 자산의 메타데이터를 편집할 수 있습니다. 이 권한이 부여되면 게시자는 Amazon DataZone 카탈로그에 게시한 자산에 대한 구독 요청을 승인하거나 거부할 수 있습니다.

구독자

Amazon 에서 구독 DataZone자는 Amazon DataZone 카탈로그에서 자산을 검색, 액세스 및 소비하려는 Amazon DataZone 프로젝트입니다.

AWS 계정 owner

Amazon 에서 DataZone AWS 계정 소유자는 에 Amazon DataZone 도메인과 연결할 AWS 계정 수 AWS 계정 있는 역할, 정책 및 권한을 생성합니다.

Amazon의 새로운 점은 무엇입니까 DataZone?

이 섹션에서는 출시 DataZone 날짜별로 Amazon의 새로운 기능 및 개선 사항을 설명합니다.

주제

- 2024년
- 2023년

2024년

Amazon DataZone , 도메인 단위 및 권한 부여 정책 출시

2024년 8월 12일에 출시되었습니다.

Amazon은 고객이 비즈니스 단위/팀 수준의 조직을 만들고 비즈니스 요구 사항에 따라 정책을 관리할 수 있도록 도메인 단위 및 권한 부여 정책이라는 새로운 데이터 거버넌스 기능 세트를 DataZone 도입합니다. 도메인 단위를 추가하면 사용자는 사업부 또는 팀과 관련된 데이터 자산 및 프로젝트를 구성, 생성, 검색 및 찾을 수 있습니다. 권한 부여 정책을 통해 해당 도메인 단위 사용자는 Amazon DataZone 내에서 프로젝트, 용어집 생성 및 컴퓨팅 리소스 사용에 대한 액세스 정책을 설정할 수 있습니다. 자세한 내용은 Amazon의 도메인 단위 및 권한 부여 정책 DataZone 단원을 참조하십시오.

아마존 DataZone , 데이터 제품 출시

2024년 8월 5일에 출시되었습니다

Amazon은 데이터 자산을 특정 비즈니스 사용 사례에 맞게 잘 정의된 독립형 패키지로 그룹화할 수 있는 데이터 제품을 DataZone 소개합니다. 예를 들어 마케팅 분석 데이터 제품은 마케팅 캠페인 데이터, 파이프라인 데이터, 고객 데이터와 같은 다양한 데이터 자산을 번들로 묶을 수 있습니다. 데이터 제품을 사용하면 고객은 검색 및 구독 프로세스를 단순화하여 비즈니스 목표에 맞게 조정하고 개별 자산 처리 시 중복되는 문제를 줄일 수 있습니다. 자세한 내용은 을 참조하십시오. Amazon DataZone 데이터 제품

Amazon DataZone , 세분화된 액세스 제어 기능 출시

2024년 7월 2일에 출시되었습니다.

DataZone Amazon은 세분화된 액세스 제어를 도입하여 데이터 레이크 및 데이터 웨어하우스에 걸친 Amazon DataZone 비즈니스 데이터 카탈로그의 데이터 자산을 세밀하게 제어할 수 있도록 합니다. 새

로운 기능을 통해 이제 데이터 소유자는 전체 데이터 자산에 대한 액세스 권한을 부여하는 대신 행 및 열 수준에서 특정 데이터 레코드에 대한 액세스를 제한할 수 있습니다. 예를 들어 데이터에 개인 식별 정보 (PII) 와 같은 민감한 정보가 포함된 열이 포함된 경우 필요한 열로만 액세스를 제한하여 민감하지 않은 데이터에 대한 액세스는 허용하면서 중요한 정보는 보호할 수 있습니다. 마찬가지로 행 수준에서 액세스를 제어하여 사용자가 자신의 역할 또는 작업과 관련된 레코드만 볼 수 있도록 할 수 있습니다. 자세한 내용은 Amazon의 데이터에 대한 세분화된 액세스 제어 DataZone 단원을 참조하세요.

Amazon DataZone , 데이터 계보 기능 출시

2024년 6월 27일에 출시되었습니다.

Amazon은 미리 보기 모드로 데이터 계보를 DataZone 출시하여 고객이 OpenLineage 지원 시스템에서 발생하거나 소스에서 소비에 이르는 데이터 이동을 통해 계보 이벤트를 API 시각화하고 추적할 수 있도록 지원합니다. DataZoneAmazon과 OpenLineage 호환되는 APIs 기능을 사용하면 도메인 관리자와 데이터 생산자는 Amazon S3에서의 변환을 포함하여 Amazon에서 사용할 수 있는 것 이상의 계보 이벤트를 캡처하고 저장할 수 있습니다. DataZone AWS Glue 및 기타 서비스. 또한 Amazon은 각 이벤트에 따라 계보를 DataZone 버전화하여 사용자가 언제든지 계보를 시각화하거나 자산 또는 작업 기록의 변화를 비교할 수 있도록 합니다. 이 과거 계보를 통해 데이터가 어떻게 진화했는지 더 깊이 이해할 수 있으며, 이는 데이터 자산의 문제 해결, 감사 및 무결성 검증에 필수적입니다. 자세한 내용은 Amazon의 데이터 계보 DataZone (미리 보기) 단원을 참조하세요.

아마존 DataZone , 커스텀 출시 AWS 서비스 청사진

2024년 6월 17일에 출시되었습니다

커스텀 포함 AWS 서비스 청사진 (기존 청사진 있는 경우) AWS IAM역할, 데이터 레이크, 데이터 메시, Amazon S3 버킷, Amazon Redshift 클러스터를 비롯한 리소스에서 이제 고유한 IAM 사용자 지정 역할을 사용하여 이러한 기존 리소스에 대한 권한을 지정할 수 있으므로 DataZone Amazon 사용자는 게시 및 구독을 활용하여 이러한 리소스를 공유하고 관리할 수 있습니다. 사용자 지정 기능을 사용하면 AWS 서비스 블루프린트, Amazon DataZone 관리자가 구성할 수 있는 기능 AWS 자체 사용자 지정 역할을 사용하는 서비스 환경. 이를 위한 작업 링크를 구성할 수 있습니다. AWS 서비스 환경을 제공하므로 기존 환경 모두에 대한 페더레이션 액세스를 제공합니다. AWS 있습니다. 또한 이러한 사용자 지정으로 구독 대상 및 데이터 소스를 구성할 수 있습니다. AWS 서비스 환경. 관리자가 설정할 수 있습니다. AWS 데이터를 게시, 구독, 검색 또는 관리하려는 Amazon DataZone 도메인 계정 또는 관련 계정의 서비스 환경 자세한 내용은 Amazon DataZone 사용자 지정 AWS 서비스 청사진 단원을 참조하십시오.

데이터 소스 생성 흐름의 개선

2024년 6월 10일에 출시되었습니다

DataZone Amazon은 데이터 생산자의 액세스 관리를 단순화하기 위해 데이터 소스 생성 흐름을 개선했습니다. 이번 업데이트를 통해 데이터 생산자가 데이터 출판을 위한 데이터 소스를 생성하면 AWS Glue 및 Amazon Redshift 자산에서 Amazon은 DataZone 프로젝트 구성원에게 읽기 전용 권한을 부여합니다. 를 생성할 때 AWS Glue 데이터 소스의 경우 Amazon은 데이터 소스를 생성하는 데 사용된 환경 IAM 역할에 '읽기 전용' 권한을 DataZone 자동으로 부여하여 관련 테이블의 모든 테이블에 액세스할 수 있도록 합니다. AWS Glue 데이터베이스. 마찬가지로 Amazon Redshift 데이터 소스의 경우 Amazon은 데이터 소스에서 사용되는 Amazon Redshift 스키마의 모든 테이블에 대해 '읽기 전용' 액세스 권한을 DataZone 부여합니다. 자세한 내용은 에 대한 Amazon DataZone 데이터 소스 생성 및 실행 AWS Glue Data Catalog 및 Amazon Redshift용 Amazon DataZone 데이터 소스 생성 및 실행 단원을 참조하세요.

아마존 DataZone , 아마존과의 통합 시작 SageMaker

2024년 5월 6일에 출시되었습니다

Amazon은 SageMakerAmazon과의 통합을 DataZone 시작하여 데이터 생산자와 소비자가 Amazon으로 원활하게 전환하여 기계 학습 (ML) 프로젝트에서 SageMaker 협업하는 동시에 데이터 및 ML 자산에 대한 액세스 거버넌스를 적용할 수 있도록 지원합니다. DataZone Amazon과 Amazon SageMaker 간의 새로운 통합 기능을 통해 데이터 소비자와 생산자는 인프라 설정 전반에서 ML 거버넌스를 간소화하고, 비즈니스 이니셔티브에 대해 협업하고, 데이터와 ML 자산을 쉽게 관리할 수 있습니다. 자세한 내용은 아마존 DataZone 빌트인 블루프린트 및 Amazon의 연결된 계정 DataZone 단원을 참조하세요.

아마존 DataZone , 다음과 통합 시작 AWS Lake Formation 하이브리드 액세스 모드

2024년 4월 3일에 출시되었습니다

DataZone Amazon은 다음과 같은 통합을 도입했습니다. AWS Lake Formation 하이브리드 액세스 모드. 이 통합을 통해 귀하의 데이터를 쉽게 게시하고 공유할 수 있습니다. AWS 테이블을 등록할 필요 없이 DataZone Amazon을 통해 테이블을 접착할 수 있습니다. AWS 먼저 레이크 포메이션. 시작하려면 관리자가 Amazon DataZone 콘솔의 `DefaultDataLake` 블루프린트에서 데이터 위치 등록 설정을 활성화해야 합니다. 그런 다음, 데이터 소비자가 구독하면 AWS IAM권한을 통해 관리되는 Glue 테이블에서는 Amazon이 DataZone 먼저 하이브리드 모드에서 이 테이블의 Amazon S3 위치를 등록한 다음, 테이블에 대한 권한을 관리하여 데이터 소비자에게 액세스 권한을 부여합니다. AWS 레이크 포메이션.

이렇게 하면 새로 부여된 후에도 테이블에 대한 IAM 권한이 계속 유지됩니다. AWS 기존 워크플로를 방해하지 않는 Lake Formation 권한. 자세한 정보는 AWS Lake Formation 하이브리드 모드와 Amazon DataZone 통합 단원을 참조하십시오.

아마존 DataZone , 다음과 통합 시작 AWS Glue 데이터 품질

2024년 4월 3일에 출시되었습니다

아마존 DataZone , 다음과 통합 시작 AWS Glue Data Quality는 타사 데이터 품질 솔루션의 데이터 품질 메트릭을 APIs 통합하는 기능을 제공합니다. 새로운 통합을 통해 자동 게시할 수 있습니다. AWS Data Quality 점수를 Amazon DataZone 비즈니스 데이터 카탈로그에 붙입니다. Amazon은 타사 소스의 품질 지표를 수집하는 데 사용할 DataZone APIs 수 있습니다. 게시되면 데이터 소비자는 데이터 자산을 쉽게 검색하고, 세분화된 품질 지표를 보고, 실패한 검사 및 규칙을 식별하여 비즈니스 의사 결정을 내릴 수 있습니다. 자세한 정보는 Amazon의 데이터 품질 DataZone 단원을 참조하십시오.

Amazon 내 설명에 대한 AI 권장 사항의 일반 출시 DataZone

2024년 3월 27일에 출시되었습니다.

Amazon은 비즈니스 데이터 카탈로그를 강화하여 데이터 검색, 데이터 이해 및 데이터 사용을 개선할 수 있는 새로운 제너레이티브 AI 기반 기능의 정식 출시를 DataZone 발표했습니다. 데이터 생산자는 클릭 한 번으로 포괄적인 비즈니스 데이터 설명 및 컨텍스트를 생성하고, 영향력 있는 열을 강조 표시하고, 분석 사용 사례에 대한 권장 사항을 포함할 수 있습니다. 이번 출시에는 데이터 생산자가 자산에 대한 APIs 설명을 프로그래밍 방식으로 생성하는 데 사용할 수 있는 지원이 추가되었습니다. 자세한 내용은 Amazon에서 기계 학습 및 생성형 AI 사용 DataZone 단원을 참조하십시오.

아마존 DataZone , 아마존 Redshift 통합 개선 사항 출시

2024년 3월 21일에 출시되었습니다.

DataZone 아마존은 Amazon Redshift 테이블 및 뷰를 게시하고 구독하는 프로세스를 간소화하기 위해 Amazon Redshift 통합에 몇 가지 개선 사항을 도입했습니다. 이러한 업데이트는 데이터 생산자와 소비자 모두의 경험을 간소화하여 Amazon DataZone 관리자가 제공하는 사전 구성된 자격 증명과 연결 매개변수를 사용하여 데이터 웨어하우스 환경을 빠르게 만들 수 있도록 합니다. 또한 이러한 개선 사항을 통해 관리자는 자신의 리소스를 누가 사용할 수 있는지 더 잘 제어할 수 있습니다. AWS 계정 및 Amazon Redshift 클러스터, 그리고 어떤 용도로 사용됩니까?

- 블루프린트 구성: 블루프린트를 활성화하면 활성화된 `DefaultDataWarehouseBlueprint` 블루프린트에 관리 프로젝트를 할당하여 계정에서 `DefaultDataWarehouseBlueprint` 블루프린트를 사용하여 환경 프로필을 생성할 수 있는 프로젝트를 제어할 수 있습니다. 클러스터, 데이터베이

스, 등의 파라미터를 DefaultDataWarehouseBlueprint 제공하여 그 위에 파라미터 세트를 생성할 수도 있습니다. AWS 시크릿. 만들 수도 있습니다. AWS Amazon DataZone 콘솔 내부의 비밀.

- 환경 프로필: 환경 프로필을 생성할 때 Amazon Redshift 파라미터를 직접 제공하거나 블루프린트 구성의 파라미터 세트 중 하나를 사용할 수 있습니다. 블루프린트 구성에서 생성한 파라미터 세트를 사용하기로 선택한 경우 AWS 비밀번호에는 AmazonDataZoneDomain 태그만 필요합니다 (환경 프로파일에 자체 파라미터 세트를 제공하기로 선택한 경우에만 AmazonDataZoneProject 태그가 필요합니다). 환경 프로필에서 승인된 프로젝트 목록을 지정할 수 있습니다. 승인된 프로젝트만 이 환경 프로필을 사용하여 데이터 웨어하우스 환경을 만들 수 있습니다. 또한 어떤 데이터 인증 프로젝트를 게시할 수 있는지 지정할 수 있습니다. 현재 다음 옵션 중 하나를 선택할 수 있습니다. 1) 모든 스키마에서 게시, 2) 기본 환경 스키마에서 게시, 3) 게시 허용 안 함.
- 환경: 이제 데이터 생산자 또는 소비자는 다음과 같은 자체 Amazon Redshift 파라미터를 제공할 필요 없이 환경 프로필을 선택하여 환경을 만들 수 있습니다. AWS 시크릿, 클러스터, 워크그룹, 데이터베이스. 이러한 매개변수는 환경 프로파일에서 환경으로 포팅됩니다. Amazon은 환경 생성과 함께 DataZone 이제 환경에 대한 기본 스키마도 생성합니다. 프로젝트 구성원은 이 스키마에 대한 읽기 및 쓰기 액세스 권한을 가지며 환경 생성의 일환으로 생성된 기본 데이터 소스를 실행하여 이 스키마에서 생성된 테이블을 카탈로그에 쉽게 게시할 수 있습니다. 환경을 생성하는 데 사용되는 Amazon Redshift 파라미터를 사용하여 새 데이터 소스를 생성할 수도 있습니다 (데이터 생산자가 데이터 소스 생성 시 자체 파라미터를 제공하는 대신).

AWS Amazon을 위한 클라우드 구성 지원 DataZone

2024년 1월 18일에 출시되었습니다

Amazon 사용자는 이제 활용할 DataZone 수 있습니다 AWS CloudFormation Amazon DataZone 리소스 제품군을 효과적으로 모델링하고 관리합니다. 이 접근 방식은 일관된 리소스 프로비저닝을 용이하게 하는 동시에 코드형 인프라 프랙티스를 통해 수명 주기 관리를 가능하게 합니다. 사용자 지정 템플릿을 사용하면 필요한 리소스와 상호 종속성을 정확하게 정의할 수 있습니다. 자세한 내용은 Amazon DataZone 리소스 유형 참조를 참조하십시오.

IAM주도자를 Amazon 프로젝트의 구성원으로 직접 추가 DataZone

2024년 1월 5일에 출시되었습니다.

이제 IAM 주도자가 아직 Amazon에 로그인하지 않았더라도 IAM 주도자를 프로젝트 구성원으로 추가할 수 있습니다 DataZone (이전 요구 사항). 도메인 관리자 또는 IT 관리자가 도메인의 도메인 실행 역할을 iam:GetUser 추가한 후 프로젝트 소유자는 역할 또는 사용자의 Amazon Resource IAM Name (ARN) 을 제공하기만 하면 주체를 구성원으로 추가할 수 있습니다. iam:GetRole IAM IAM IAM보안

주체는 여전히 Amazon에 액세스하는 데 필요한 IAM 권한을 가지고 있어야 DataZone 하며 이러한 권한은 IAM 콘솔에서 구성할 수 있습니다. 자세한 내용은 프로젝트에 멤버 추가 단원을 참조하십시오.

데이터 포털의 사용자 지정 자산 유형 지원

2024년 1월 5일에 출시되었습니다.

사용자 지정 자산이 지원되므로 DataZone Amazon은 Data Portal을 통해 대시보드, 쿼리, 모델 등의 비정형 데이터에 대한 자산을 카탈로그화할 수 있으므로 이전에 API 제공되었던 지원과 함께 데이터 포털에서 직접 사용자 지정 자산을 더 쉽게 추가할 수 있습니다. DataZoneAmazon에서 사용자 지정 자산을 생성, 업데이트 및 게시할 수 있으므로 모든 유형의 자산을 공유, 검색, 구독하고 해당 자산에 대한 거버넌스를 제공하는 비즈니스 워크플로를 구축할 수 있습니다. 자세한 내용은 Amazon에서 사용자 지정 자산 유형 생성 DataZone 단원을 참조하십시오.

2023년

도메인 삭제

2023년 12월 27일에 출시되었습니다

도메인을 더 쉽게 삭제할 수 있는 기능입니다. 이제 비어 있지 않아도 도메인 삭제를 진행할 수 있습니다 (예: 프로젝트, 환경, 자산, 데이터 원본 등이 포함된 경우). 자세한 내용은 Amazon DataZone 도메인 삭제 단원을 참조하십시오.

하이브리드 모드

2023년 12월 22일에 출시되었습니다

DataZone Amazon은 다음에 대한 지원을 추가했습니다. AWS 레이크 포메이션 하이브리드 모드. 이 지원을 통해 게시하면 AWS 그것으로 Amazon에 테이블을 DataZone 붙이세요 AWS 하이브리드 모드에서 Lake Formation에 등록된 S3 위치에서 Amazon은 이 테이블을 관리 자산으로 DataZone 취급하며 이 테이블에 대한 구독 허가를 관리할 수 있습니다. 이 기능이 출시되기 전에 Amazon은 DataZone 이 테이블을 비관리 자산으로 취급했습니다. 즉, DataZone Amazon은 이 테이블에 대한 구독을 승인할 수 없었습니다. 자세한 내용은 Amazon에 대한 Lake Formation 권한 구성 DataZone 단원을 참조하십시오.

HIPAA자격

2023년 12월 14일에 출시되었습니다

DataZone Amazon은 현재 1996년 미국 건강 보험 양도 및 책임법 (HIPAA) 을 준수하고 있습니다. 목록을 보려면 AWS HIPAA규정 준수가 적용되는 서비스는 https://aws.amazon.com/compliance/hipaa-eligible-services-reference/를 참조하십시오.

Amazon 설명에 대한 AI 권장 사항 DataZone (미리 보기)

2023년 11월 28일에 출시되었습니다.

AWS 비즈니스 데이터 카탈로그를 보강하여 데이터 검색, 데이터 이해 및 데이터 사용을 개선할 수 DataZone 있는 Amazon의 새로운 제너레이티브 AI 기반 기능의 미리보기를 발표합니다. 데이터 생산자는 클릭 한 번으로 포괄적인 비즈니스 데이터 설명 및 컨텍스트를 생성하고, 영향력 있는 열을 강조 표시하고, 분석 사용 사례에 대한 권장 사항을 포함할 수 있습니다. DataZoneAmazon의 설명에 대한 AI 권장 사항을 통해 데이터 소비자는 분석에 필요한 데이터 테이블과 열을 식별할 수 있으므로 데이터 검색 가능성이 향상되고 데이터 생산자와의 back-and-forth 커뮤니케이션이 줄어듭니다. 미리보기는 다음에서 프로비저닝된 Amazon DataZone 도메인에서 사용할 수 있습니다. AWS 지역: 미국 동부 (버지니아 북부), 미국 서부 (오레곤). 자세한 내용은 Amazon에서 기계 학습 및 생성형 AI 사용 DataZone 단원을 참조하십시오.

DefaultDataLake 청사진 개선

2023년 11월 20일에 출시되었습니다

DataZone Amazon은 누가 귀하의 데이터를 게시할 수 있는지 더 잘 제어할 수 있도록 DefaultDataLake 청사진에 개선 사항을 추가했습니다. AWS 계정. 이번 기능 출시와 함께 도입된 두 가지 주요 변경 사항이 있습니다.

- 콘솔에서 블루프린트를 활성화하면 활성화된 DefaultDataLake 블루프린트에 프로젝트 관리를 할당하여 계정의 DefaultDataLake 블루프린트를 사용하여 환경 프로필을 만들 수 있는 프로젝트를 제어할 수 있습니다.
- 두 번째 변경사항은 포털에 있습니다. DefaultDataLake 블루프린트를 사용하여 환경 프로필을 만드는 경우 환경 생성에 환경 프로필을 사용할 수 있는 승인된 프로젝트를 선택할 수도 있습니다. 기본적으로 모든 프로젝트에서 데이터 레이크 환경 프로필을 사용할 수 있지만 환경 프로필을 특정 프로젝트로 제한하고 프로필로 만든 환경을 사용하여 게시할 수 있는 데이터를 제어할 수도 있습니다.

자세한 내용은 환경 프로파일 생성 단원을 참조하십시오.

아마존 설정 DataZone

Amazon을 DataZone 설정하려면 다음이 있어야 합니다. AWS 계정을 지정하고 Amazon에 필요한 IAM 정책 및 권한을 설정합니다 DataZone.

Amazon DataZone 권한을 설정한 후에는 Amazon DataZone 도메인 생성, 데이터 포털 URL 확보, 데이터 생산자 및 데이터 소비자를 위한 기본 Amazon DataZone 워크플로를 안내하는 시작하기 섹션의 단계를 완료하는 것이 좋습니다.

주제

- 가입하세요. AWS account
- Amazon DataZone 관리 콘솔을 사용하는 데 필요한 IAM 권한을 구성합니다.
- Amazon DataZone 데이터 포털을 사용하는 데 필요한 IAM 권한을 구성합니다.
- 설정 AWS IAM아마존 아이덴티티 센터 DataZone

가입하세요. AWS account

가지고 있지 않은 경우 AWS 계정을 만들려면 다음 단계를 완료하세요.

가지고 있는 경우 AWS 조직, 계정 만들기:

1. 에 로그인 AWS 에서 관리 콘솔을 열고 조직 콘솔을 엽니다 https://console.aws.amazon.com/organizations/.
2. 탐색 창에서 다음을 선택합니다. AWS 계정.
3. 추가를 선택합니다. AWS 계정.
4. [만들기] 를 선택합니다. AWS 계정을 만들고 요청된 세부 정보를 제공하십시오. 만들기를 선택합니다. AWS 계정.

가입하려면 AWS account

1. https://portal.aws.amazon.com/billing/등록 열기
2. 온라인 지시 사항을 따릅니다.

   등록 절차 중 전화를 받고 전화 키패드로 확인 코드를 입력하는 과정이 있습니다.

가입할 때 AWS 계정, AWS 계정 루트 사용자가 생성됩니다. 루트 사용자는 모두에 액세스할 수 있습니다. AWS 계정의 서비스 및 리소스. 보안 모범 사례는 관리 사용자에게 관리자 액세스 권한을 할당하고, 루트 사용자만 루트 사용자 액세스 권한이 필요한 태스크를 수행하는 것입니다.

Amazon DataZone 관리 콘솔을 사용하는 데 필요한 IAM 권한을 구성합니다.

Amazon DataZone 도메인, 블루프린트, 사용자에 액세스하여 구성하고 Amazon DataZone 데이터 포털을 생성하려면 Amazon 관리 콘솔을 사용해야 합니다. DataZone

Amazon DataZone Management 콘솔을 사용하려는 사용자, 그룹 또는 역할에 대한 필수 및/또는 선택적 권한을 구성하려면 다음 절차를 완료해야 합니다.

관리 콘솔 IAM 사용 권한을 설정하는 절차

- Amazon DataZone 콘솔 액세스를 위해 사용자, 그룹 또는 역할에 필수 및 선택적 정책 첨부
- Amazon DataZone 서비스 콘솔의 간소화된 역할 생성을 활성화하기 위한 IAM 권한에 대한 사용자 지정 정책을 생성합니다.
- Amazon DataZone 도메인과 연결된 계정을 관리할 수 있는 권한에 대한 사용자 지정 정책을 생성합니다.
- (선택 사항) 에 대한 사용자 지정 정책 생성 AWS Amazon DataZone 도메인에 대한 SSO 사용자 및 SSO 그룹 액세스 추가 및 제거를 위한 ID 센터 권한
- (선택 사항) IAM 보안 주체를 키 사용자로 추가하여 고객 관리 키로 Amazon DataZone 도메인을 생성합니다. AWS 키 관리 서비스 () KMS

Amazon DataZone 콘솔 액세스를 위해 사용자, 그룹 또는 역할에 필수 및 선택적 정책 첨부

필수 및 선택적 사용자 지정 정책을 사용자, 그룹 또는 역할에 첨부하려면 다음 절차를 완료하십시오. 자세한 내용은 AWS Amazon용 관리형 정책 DataZone 단원을 참조하십시오.

1. 에 로그인하십시오. AWS 에서 관리 콘솔을 열고 IAM 콘솔을 엽니다 https://console.aws.amazon.com/iam/.
2. 탐색 창에서 Policies를 선택합니다.
3. 사용자, 그룹 또는 역할에 연결할 다음 정책을 선택합니다.

- 정책 목록에서 옆의 확인란을 선택합니다 AmazonDataZoneFullAccess. [Filter] 메뉴와 검색 상자를 사용하여 정책 목록을 필터링할 수 있습니다. 자세한 내용은 AWS 관리형 정책: AmazonDataZoneFullAccess 단원을 참조하십시오.
- (선택 사항) Amazon DataZone 서비스 콘솔의 간소화된 역할 생성을 활성화하기 위한 IAM 권한에 대한 사용자 지정 정책을 생성합니다.
- (선택 사항) 에 대한 사용자 지정 정책 생성 AWS Amazon DataZone 도메인에 대한 SSO 사용자 및 SSO 그룹 액세스를 추가 및 제거할 수 있는 ID 센터 권한

4. 작업(Actions)을 선택한 후 연결(Attach)을 선택합니다.
5. 정책을 연결할 사용자, 그룹 또는 역할을 선택합니다. 필터 메뉴와 검색 상자를 사용하면 보안 주체 개체 목록을 필터링할 수 있습니다. 사용자, 그룹 또는 역할을 선택한 후 정책 연결을 선택합니다.

Amazon DataZone 서비스 콘솔의 간소화된 역할 생성을 활성화하기 위한 IAM 권한에 대한 사용자 지정 정책을 생성합니다.

다음 절차를 완료하여 DataZone Amazon이 필요한 역할을 생성할 수 있도록 필요한 권한을 갖도록 사용자 지정 인라인 정책을 생성하십시오. AWS 사용자를 대신하여 관리 콘솔을 사용하십시오.

1. 에 로그인하십시오. AWS 에서 관리 콘솔을 열고 IAM 콘솔을 엽니다 https://console.aws.amazon.com/iam/.
2. 탐색 창에서 사용자 또는 사용자 그룹을 선택합니다.
3. 목록에서 정책을 삽입할 사용자 또는 그룹 이름을 선택합니다.
4. 권한 탭을 선택하고 필요하다면 Permissions policies(권한 정책) 섹션을 확장합니다.
5. 권한 추가 및 인라인 정책 생성 링크를 선택합니다.
6. 정책 생성 화면의 정책 편집기 섹션에서 선택합니다 JSON.

   다음 JSON 명령문이 포함된 정책 문서를 만든 후 다음을 선택합니다.

```
{
    "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. 정책 검토 화면에서 정책 이름을 입력합니다. 정책에 만족하면 정책 생성을 선택합니다. 화면 상단에 있는 빨간색 상자에 표시되는 오류가 있지 않은지 확인합니다. 표시되는 오류가 있다면 수정합니다.

Amazon DataZone 도메인과 연결된 계정을 관리할 수 있는 권한에 대한 사용자 지정 정책을 생성합니다.

다음 절차를 완료하여 관련 사용자에게 필요한 권한을 부여하는 사용자 지정 인라인 정책을 만드십시오. AWS 도메인의 리소스 공유를 나열, 수락 및 거부한 다음 관련 계정에서 환경 블루프린트를 활성화, 구성 및 비활성화하는 계정입니다. 블루프린트 구성 중에 옵션으로 제공되는 Amazon DataZone 서비스 콘솔 간소화 역할 생성을 활성화하려면 반드시 활성화해야 합니다. Amazon DataZone 서비스 콘솔의 간소화된 역할 생성을 활성화하기 위한 IAM 권한에 대한 사용자 지정 정책을 생성합니다.

1. 에 로그인하십시오. AWS 에서 관리 콘솔을 열고 IAM 콘솔을 엽니다 https://console.aws.amazon.com/iam/.

2. 탐색 창에서 사용자 또는 사용자 그룹을 선택합니다.
3. 목록에서 정책을 삽입할 사용자 또는 그룹 이름을 선택합니다.
4. 권한 탭을 선택하고 필요하다면 Permissions policies(권한 정책) 섹션을 확장합니다.
5. 권한 추가 및 인라인 정책 생성 링크를 선택합니다.
6. 정책 생성 화면의 정책 편집기 섹션에서 선택합니다 JSON. 다음 JSON 명령문이 포함된 정책 문서를 만든 후 다음을 선택합니다.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "datazone:ListEnvironmentBlueprintConfigurations",
                "datazone:PutEnvironmentBlueprintConfiguration",
                "datazone:GetDomain",
                "datazone:ListDomains",
                "datazone:GetEnvironmentBlueprintConfiguration",
                "datazone:ListEnvironmentBlueprints",
                "datazone:GetEnvironmentBlueprint",
                "datazone:ListAccountEnvironments",
                "datazone:DeleteEnvironmentBlueprintConfiguration"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": "iam:PassRole",
            "Resource": [
                "arn:aws:iam::*:role/AmazonDataZone",
                "arn:aws:iam::*:role/service-role/AmazonDataZone*"
            ],
            "Condition": {
                "StringEquals": {
                    "iam:passedToService": "datazone.amazonaws.com"
                }
            }
        },
        {
            "Effect": "Allow",
```

```
            "Action": "iam:AttachRolePolicy",
            "Resource": "arn:aws:iam::*:role/service-role/AmazonDataZone*",
            "Condition": {
                "ArnLike": {
                    "iam:PolicyARN": [
                        "arn:aws:iam::aws:policy/AmazonDataZone*",
                        "arn:aws:iam::*:policy/service-role/AmazonDataZone*"
                    ]
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": "iam:ListRoles",
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "iam:CreatePolicy",
                "iam:CreateRole"
            ],
            "Resource": [
                "arn:aws:iam::*:policy/service-role/AmazonDataZone*",
                "arn:aws:iam::*:role/service-role/AmazonDataZone*"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "ram:AcceptResourceShareInvitation",
                "ram:RejectResourceShareInvitation",
                "ram:GetResourceShareInvitations"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "s3:ListAllMyBuckets",
                "s3:ListBucket",
                "s3:GetBucketLocation"
            ],
            "Resource": "*"
```

```
        },
        {
            "Effect": "Allow",
            "Action": "s3:CreateBucket",
            "Resource": "arn:aws:s3:::amazon-datazone*"
        }
    ]
}
```

7. 정책 검토 화면에서 정책 이름을 입력합니다. 정책에 만족하면 정책 생성을 선택합니다. 화면 상단에 있는 빨간색 상자에 표시되는 오류가 있지 않은지 확인합니다. 표시되는 오류가 있다면 수정합니다.

(선택 사항) 에 대한 사용자 지정 정책 생성 AWS Amazon DataZone 도메인에 대한 SSO 사용자 및 SSO 그룹 액세스 추가 및 제거를 위한 ID 센터 권한

Amazon DataZone 도메인에 대한 사용자 및 SSO 그룹 액세스 권한을 추가 및 제거하는 데 필요한 권한을 갖도록 SSO 사용자 지정 인라인 정책을 생성하려면 다음 절차를 완료하십시오.

1. 에 로그인하십시오. AWS 에서 관리 콘솔을 열고 IAM 콘솔을 엽니다 https://console.aws.amazon.com/iam/.
2. 탐색 창에서 사용자 또는 사용자 그룹을 선택합니다.
3. 목록에서 정책을 삽입할 사용자 또는 그룹 이름을 선택합니다.
4. 권한 탭을 선택하고 필요하다면 Permissions policies(권한 정책) 섹션을 확장합니다.
5. 권한 추가 및 인라인 정책 생성을 선택합니다.
6. 정책 생성 화면의 정책 편집기 섹션에서 선택합니다 JSON.

   다음 JSON 명령문이 포함된 정책 문서를 만든 후 다음을 선택합니다.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "sso:GetManagedApplicationInstance",
        "sso:ListProfiles",
```

```
        "sso:GetProfiles",
        "sso:AssociateProfile",
        "sso:DisassociateProfile",
        "sso:GetProfile"
      ],
      "Resource": "*"
    }
  ]
}
```

7. 정책 검토 화면에서 정책 이름을 입력합니다. 정책에 만족하면 정책 생성을 선택합니다. 화면 상단에 있는 빨간색 상자에 표시되는 오류가 있지 않은지 확인합니다. 표시되는 오류가 있다면 수정합니다.

(선택 사항) IAM 보안 주체를 키 사용자로 추가하여 고객 관리 키로 Amazon DataZone 도메인을 생성합니다. AWS 키 관리 서비스 () KMS

필요한 경우 에서 제공하는 고객 관리 키 (CMK) 를 사용하여 Amazon DataZone 도메인을 생성할 수 있습니다. AWS 키 관리 서비스 (KMS) 에서 다음 절차를 완료하여 IAM 보안 주체를 키 사용자로 설정하십시오KMS.

1. 에 로그인하십시오. AWS 에서 관리 콘솔을 열고 KMS 콘솔을 엽니다 https://console.aws.amazon.com/kms/.
2. 해당 계정에서 직접 생성하고 관리하는 키를 보려면 탐색 창에서 고객 관리형 키를 선택합니다.
3. 키 목록에서 검사하려는 KMS 키의 별칭 또는 KMS 키 ID를 선택합니다.
4. 주요 사용자 추가 또는 제거, 외부 사용자 허용 또는 금지 AWS 계정을 사용하여 KMS 키를 사용하려면 페이지의 주요 사용자 섹션에 있는 컨트롤을 사용하십시오. 주요 사용자는 암호화, 복호화, 재암호화 및 데이터 키 생성과 같은 암호화 작업에 KMS 키를 사용할 수 있습니다.

Amazon DataZone 데이터 포털을 사용하는 데 필요한 IAM 권한을 구성합니다.

Amazon DataZone 데이터 포털 (AWSManagement Console 외부) 은 사용자가 셀프 서비스 방식으로 데이터를 카탈로그 작성, 검색, 관리, 공유 및 분석할 수 있는 브라우저 기반 웹 애플리케이션입니다. 데이터 포털은 다음을 통해 ID 공급자의 IAM 자격 증명 또는 기존 자격 증명으로 사용자를 인증합니다. AWS IAM아이덴티티 센터.

Amazon DataZone 데이터 포털 또는 카탈로그를 사용하려는 사용자, 그룹 또는 역할에 필요한 권한을 구성하려면 다음 절차를 완료해야 합니다.

데이터 포털 IAM 사용 권한을 구성하는 절차

- Amazon DataZone 데이터 포털 액세스에 필요한 정책을 사용자, 그룹 또는 역할에 연결
- Amazon DataZone 카탈로그 액세스에 필요한 정책을 사용자, 그룹 또는 역할에 연결
- 고객 관리 키로 도메인을 암호화한 경우 Amazon DataZone 데이터 포털 또는 카탈로그 액세스에 대한 선택적 정책을 사용자, 그룹 또는 역할에 연결합니다. AWS 키 관리 서비스 () KMS

Amazon DataZone 데이터 포털 액세스에 필요한 정책을 사용자, 그룹 또는 역할에 연결

다음 중 하나를 사용하여 Amazon DataZone 데이터 포털에 액세스할 수 있습니다. AWS 자격 증명 또는 싱글 사인온 (SSO) 자격 증명. 아래 섹션의 지침에 따라 데이터 포털에 액세스하는 데 필요한 권한을 설정하십시오. AWS 자격 증명. Amazon을 사용하는 방법에 대한 자세한 내용은 DataZone SSO 을 참조하십시오설정 AWS IAM아마존 아이덴티티 센터 DataZone.

> **Note**
>
> IAM도메인의 보안 주체만 AWS 계정은 도메인의 데이터 포털에 접근할 수 있습니다. IAM다른 사람의 주도자 AWS 계정은 도메인의 데이터 포털에 접근할 수 없습니다.

필요한 정책을 사용자, 그룹 또는 역할에 연결하려면 다음 절차를 완료하십시오. 자세한 내용은 AWS Amazon용 관리형 정책 DataZone 단원을 참조하십시오.

1. 에 로그인하십시오. AWS 에서 관리 콘솔을 열고 IAM 콘솔을 엽니다 https://console.aws.amazon.com/iam/.
2. 탐색 창에서 사용자, 사용자 그룹 또는 역할을 선택합니다.
3. 목록에서 정책을 내장할 사용자, 그룹 또는 역할의 이름을 선택합니다.
4. 권한 탭을 선택하고 필요하다면 Permissions policies(권한 정책) 섹션을 확장합니다.
5. 권한 추가 및 인라인 정책 생성 링크를 선택합니다.
6. 정책 생성 화면의 정책 편집기 섹션에서 선택합니다 JSON. 다음 JSON 명령문이 포함된 정책 문서를 만든 후 다음을 선택합니다.

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

7. 정책 검토 화면에서 정책 이름을 입력합니다. 정책에 만족하면 정책 생성을 선택합니다. 화면 상단에 있는 빨간색 상자에 표시되는 오류가 있지 않은지 확인합니다. 표시되는 오류가 있다면 수정합니다.

Amazon DataZone 카탈로그 액세스에 필요한 정책을 사용자, 그룹 또는 역할에 연결

> **Note**
>
> IAM도메인의 보안 주체만 AWS 계정은 도메인의 카탈로그에 액세스할 수 있습니다. IAM다른 사람의 주체 AWS 계정은 도메인의 카탈로그에 액세스할 수 없습니다.

다음 절차를 통해 API 및 를 통해 IAM 자격 증명에 Amazon DataZone 도메인 카탈로그에 대한 액세스 권한을 SDK 부여할 수 있습니다. 이러한 IAM ID가 Amazon DataZone 데이터 포털에도 액세스할 수 있도록 하려면 Amazon DataZone 데이터 포털 액세스에 필요한 정책을 사용자, 그룹 또는 역할에 연결 위의 절차를 추가로 따르십시오. 자세한 내용은 AWS Amazon용 관리형 정책 DataZone 단원을 참조하십시오.

1. 로그인하십시오. AWS 에서 관리 콘솔을 열고 IAM 콘솔을 엽니다 https://console.aws.amazon.com/iam/.
2. 탐색 창에서 Policies를 선택합니다.

3. 정책 목록에서 정책 옆에 있는 라디오 버튼을 선택합니다. AmazonDataZoneFullUserAccess [Filter] 메뉴와 검색 상자를 사용하여 정책 목록을 필터링할 수 있습니다. 자세한 내용은 AWS 관리형 정책: AmazonDataZoneFullUserAccess 단원을 참조하세요.
4. 작업(Actions)을 선택한 후 연결(Attach)을 선택합니다.
5. 각 보안 주체 옆의 확인란을 선택하여 정책을 연결할 사용자, 그룹 또는 역할을 선택합니다. 필터 메뉴와 검색 상자를 사용하면 보안 주체 개체 목록을 필터링할 수 있습니다. 사용자, 그룹 또는 역할을 선택한 후 Attach policy (정책 연결) 를 선택합니다.

고객 관리 키로 도메인을 암호화한 경우 Amazon DataZone 데이터 포털 또는 카탈로그 액세스에 대한 선택적 정책을 사용자, 그룹 또는 역할에 연결합니다. AWS 키 관리 서비스 () KMS

데이터 암호화를 위한 자체 KMS 키로 Amazon DataZone 도메인을 생성하는 경우, 다음 권한이 있는 인라인 정책도 생성하고 이를 보안 주체에 연결하여 IAM 보안 주체가 Amazon DataZone 데이터 포털 또는 카탈로그에 액세스할 수 있도록 해야 합니다.

1. 로그인하십시오. AWS 에서 관리 콘솔을 열고 IAM 콘솔을 엽니다 https://console.aws.amazon.com/iam/.
2. 탐색 창에서 사용자, 사용자 그룹 또는 역할을 선택합니다.
3. 목록에서 정책을 내장할 사용자, 그룹 또는 역할의 이름을 선택합니다.
4. 권한 탭을 선택하고 필요하다면 Permissions policies(권한 정책) 섹션을 확장합니다.
5. 권한 추가 및 인라인 정책 생성 링크를 선택합니다.
6. 정책 생성 화면의 정책 편집기 섹션에서 선택합니다 JSON. 다음 JSON 명령문이 포함된 정책 문서를 만든 후 다음을 선택합니다.

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

```
            "Resource": "*"
        }
    ]
}
```

7. 정책 검토 화면에서 정책 이름을 입력합니다. 정책에 만족하면 정책 생성을 선택합니다. 화면 상단에 있는 빨간색 상자에 표시되는 오류가 있지 않은지 확인합니다. 표시되는 오류가 있다면 수정합니다.

설정 AWS IAM아마존 아이덴티티 센터 DataZone

> **Note**
>
> AWS 동일한 위치에서 ID 센터를 활성화해야 합니다. AWS 지역은 Amazon DataZone 도메인입니다. 현재, AWS ID 센터는 한 곳에서만 활성화할 수 있습니다. AWS 리전.

Single Sign-On (SSO) 자격 증명을 사용하여 Amazon DataZone 데이터 포털에 액세스할 수 있습니다. AWS 자격 증명. 설정하려면 이 섹션의 지침을 따르십시오. AWS IAM아마존 아이덴티티 센터 DataZone. DataZone Amazon을 다음과 같이 사용하는 방법에 대한 자세한 내용은 AWS 자격 증명은 을 참조하십시오Amazon DataZone 관리 콘솔을 사용하는 데 필요한 IAM 권한을 구성합니다..

이미 절차를 완료한 경우 이 섹션의 절차를 건너뛰어도 됩니다. AWS IAM아이덴티티 센터 (후속) AWS SSO (Single Sign-On) 가 활성화되고 동일한 환경에서 구성됨 AWS Amazon DataZone 도메인을 생성하려는 지역.

다음 절차를 완료하여 활성화하십시오. AWS IAM아이덴티티 센터 (후속) AWS 싱글 사인온).

1. 활성화하려면 AWS IAMID 센터에 로그인해야 합니다. AWS 다음 자격 증명을 사용하여 관리 콘솔을 실행하십시오. AWS 조직 관리 계정. 에서 발급한 자격 증명으로 로그인한 상태에서는 IAM Identity Center를 활성화할 수 없습니다. AWS Organizations 회원 계정. 자세한 내용은 에서 조직 생성 및 관리를 참조하십시오. AWS 조직 사용자 가이드.
2. AWS IAM아이덴티티 센터 (후속) AWS Single Sign-On (Single Sign-On) 콘솔을 선택하고 상단 탐색 표시줄의 지역 선택기를 사용하여 다음을 선택합니다. AWS Amazon DataZone 도메인을 생성하려는 지역.
3. 활성화를 선택합니다.
4. ID 소스를 선택하세요.

기본적으로 빠르고 쉬운 사용자 관리를 위한 IAM ID 센터 스토어가 제공됩니다. 선택적으로 외부 ID 공급자를 대신 연결할 수도 있습니다. 이 절차에서는 기본 IAM ID 센터 저장소를 사용합니다.

자세한 내용은 ID 소스 선택을 참조하십시오.

5. IAMID 센터 탐색 창에서 그룹을 선택하고 그룹 생성을 선택합니다. 그룹 이름을 입력하고 [생성]을 선택합니다.
6. IAMID 센터 탐색 창에서 [사용자] 를 선택합니다.
7. 사용자 추가 화면에서 필수 정보를 입력하고 사용자에게 암호 설정 지침이 포함된 이메일 보내기를 선택합니다. 사용자는 다음 설정 단계에 대한 이메일을 받게 됩니다.
8. 다음: 그룹을 선택하고 원하는 그룹을 선택한 다음 사용자 추가를 선택합니다. 사용자는 사용을 SSO 권유하는 이메일을 받게 됩니다. 이 이메일에서 사용자는 초대 수락을 선택하고 비밀번호를 설정해야 합니다.

Amazon DataZone 도메인을 생성한 후 활성화할 수 있습니다. AWS DataZone Amazon용 ID 센터를 제공하며 SSO 사용자 및 SSO 그룹에 대한 액세스를 제공합니다. 자세한 내용은 Amazon용 IAM Identity Center 활성화 DataZone 단원을 참조하십시오.

Amazon 시작하기 DataZone

이 섹션의 정보는 Amazon 사용을 시작하는 데 도움이 됩니다 DataZone. Amazon 를 처음 사용하는 경우 DataZone먼저 에 나와 있는 개념과 용어를 숙지하세요Amazon DataZone 용어 및 개념.

이러한 빠른 시작 워크플로의 단계를 시작하기 전에 이 가이드의 설정 섹션에 설명된 절차를 완료해야 합니다. 새 AWS 계정을 사용하는 경우 Amazon DataZone 관리 콘솔을 사용하는 데 필요한 권한을 구성해야 합니다. 기존 AWS Glue Data Catalog 객체가 있는 AWS 계정을 사용하는 경우 Amazon 에 대한 Lake Formation 권한도 구성 DataZone해야 합니다.

이 시작하기 섹션에서는 다음 Amazon DataZone 빠른 시작 워크플로를 안내합니다.

주제

- AWS Glue 데이터를 사용한 Amazon DataZone 빠른 시작
- Amazon Redshift 데이터를 사용한 Amazon DataZone 빠른 시작
- 샘플 스크립트를 사용한 Amazon DataZone 빠른 시작

AWS Glue 데이터를 사용한 Amazon DataZone 빠른 시작

다음 빠른 시작 단계를 완료하여 샘플 AWS Glue 데이터를 DataZone 사용하여 Amazon에서 전체 데이터 생산자 및 데이터 소비자 워크플로를 실행합니다.

빠른 시작 단계

- 1단계 - Amazon DataZone 도메인 및 데이터 포털 생성
- 2단계 - 게시 프로젝트 생성
- 3단계 - 환경 생성
- 4단계 - 게시를 위한 데이터 생성
- 5단계 - Glue에서 AWS 메타데이터 수집
- 6단계 - 데이터 자산 큐레이트 및 게시
- 7단계 - 데이터 분석을 위한 프로젝트 생성
- 8단계 - 데이터 분석을 위한 환경 생성
- 9단계 - 데이터 카탈로그 검색 및 데이터 구독
- 10단계 - 구독 요청 승인
- 11단계 - Amazon Athena에서 쿼리를 빌드하고 데이터를 분석합니다.

1단계 - Amazon DataZone 도메인 및 데이터 포털 생성

이 섹션에서는 이 워크플로에 대한 Amazon DataZone 도메인 및 데이터 포털을 생성하는 단계를 설명합니다.

Amazon DataZone 도메인을 생성하려면 다음 절차를 완료하세요. Amazon DataZone 도메인에 대한 자세한 내용은 섹션을 참조하세요Amazon DataZone 용어 및 개념.

1. https://console.aws.amazon.com/datazone의 Amazon DataZone 콘솔로 이동하여 로그인한 다음 도메인 생성을 선택합니다.

   > **Note**
   >
   > 이 워크플로에 기존 Amazon DataZone 도메인을 사용하려면 도메인 보기를 선택한 다음 사용하려는 도메인을 선택한 다음 게시 프로젝트 생성의 2단계로 이동합니다.

2. 도메인 생성 페이지에서 다음 필드에 값을 입력합니다.

   - 이름 - 도메인의 이름을 지정합니다. 이 워크플로를 위해 이 도메인 마케팅 을 호출할 수 있습니다.
   - 설명 - 선택적 도메인 설명을 지정합니다.
   - 데이터 암호화 - 기본적으로 데이터를 AWS 소유하고 관리하는 키로 암호화됩니다. 이 사용 사례의 경우 기본 데이터 암호화 설정을 그대로 둘 수 있습니다.

     고객 관리형 키 사용에 대한 자세한 내용은 섹션을 참조하세요Amazon에 대한 저장 데이터 암호화 DataZone. 데이터 암호화에 자체 KMS 키를 사용하는 경우 기본 에 다음 문을 포함해야 합니다AmazonDataZoneDomainExecutionRole.

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

```
  ]
}
```

- 서비스 액세스 - 기본적으로 선택한 상태로 둡니다. 기본 역할 사용 옵션은 변경되지 않습니다.

> **Note**
>
> 이 워크플로에 기존 Amazon DataZone 도메인을 사용하는 경우 기존 서비스 역할 사용 옵션을 선택한 다음 드롭다운 메뉴에서 기존 역할을 선택할 수 있습니다.

- 빠른 설정에서 데이터 소비 및 게시를 위해 이 계정 설정을 선택합니다. 이 옵션은 데이터 레이크 및 데이터 웨어하우스 의 기본 제공 Amazon DataZone 청사진을 활성화하고 이 계정에 필요한 권한, 리소스, 기본 프로젝트, 기본 데이터 레이크 및 데이터 웨어하우스 환경 프로필을 구성합니다. Amazon DataZone 청사진에 대한 자세한 내용은 섹션을 참조하세요Amazon DataZone 용어 및 개념.
- 권한 세부 정보 아래의 나머지 필드는 변경하지 않습니다.

> **Note**
>
> 기존 Amazon DataZone 도메인이 있는 경우 기존 서비스 역할 사용 옵션을 선택한 다음 Glue Manage Access 역할 , Redshift Manage Access 역할 및 프로비저닝 역할 에 대한 드롭다운 메뉴에서 기존 역할을 선택할 수 있습니다.

- 태그 아래의 필드는 변경되지 않습니다.
- 도메인 생성(Create domain)을 선택합니다.

3. 도메인이 성공적으로 생성되면 이 도메인을 선택하고 도메인의 요약 페이지에서 이 도메인의 데이터 포털URL을 기록해 둡니다. 이를 사용하여 Amazon DataZone 데이터 포털에 URL 액세스하여 이 워크플로의 나머지 단계를 완료할 수 있습니다. 데이터 포털 열기 를 선택하여 데이터 포털로 이동할 수도 있습니다.

> **Note**
>
> Amazon 의 현재 릴리스에서 도메인이 생성 DataZone되면 데이터 포털에 대해 URL 생성된 를 수정할 수 없습니다.

도메인 생성을 완료하는 데 몇 분 정도 걸릴 수 있습니다. 다음 단계로 진행하기 전에 도메인의 상태가 사용 가능이 될 때까지 기다립니다.

2단계 - 게시 프로젝트 생성

이 섹션에서는 이 워크플로에 대한 게시 프로젝트를 생성하는 데 필요한 단계를 설명합니다.

1. 위의 1단계를 완료하고 도메인을 생성하면 Amazon에 오신 것을 환영합니다 DataZone! 창이 표시됩니다. 이 창에서 프로젝트 생성을 선택합니다.
2. 프로젝트 이름을 지정합니다. 예를 들어, 이 워크플로의 경우 이름을 지정한 SalesDataPublishingProject다음 나머지 필드를 변경하지 않은 상태로 두고 생성을 선택합니다.

3단계 - 환경 생성

이 섹션에서는 이 워크플로의 환경을 생성하는 데 필요한 단계를 설명합니다.

1. 위의 2단계를 완료하고 프로젝트를 생성하면 프로젝트를 사용할 준비가 된 창이 표시됩니다. 이 창에서 환경 생성을 선택합니다.
2. 환경 생성 페이지에서 다음을 지정한 다음 환경 생성을 선택합니다.
3. 다음 값을 지정합니다.
   - 이름 - 환경의 이름을 지정합니다. 이 연습에서는 라고 부를 수 있습니다`Default data lake environment`.
   - 설명 - 환경에 대한 설명을 지정합니다.
   - 환경 프로파일 - DataLakeProfile 환경 프로파일을 선택합니다. 이를 통해 이 워크플로 DataZone 에서 Amazon을 사용하여 Amazon S3, AWS Glue Catalog 및 Amazon Athena 의 데이터를 사용할 수 있습니다.
   - 이 연습을 위해 나머지 필드는 변경하지 않습니다.
4. 환경 생성을 선택합니다.

4단계 - 게시를 위한 데이터 생성

이 섹션에서는 이 워크플로에 게시하기 위한 데이터를 생성하는 데 필요한 단계를 설명합니다.

1. 위의 3단계를 완료한 후 `SalesDataPublishingProject` 프로젝트에서 오른쪽 패널의 분석 도구 아래에서 Amazon Athena 선택합니다. 이렇게 하면 인증을 위해 프로젝트의 보안 인증 정보를

사용하여 Athena 쿼리 편집기가 열립니다. Amazon 환경 드롭다운에서 게시 DataZone 환경을 선택하고 쿼리 편집기에서와 같이 <environment_name>%_pub_db 데이터베이스를 선택해야 합니다.

2. 이 연습에서는 테이블 생성을 선택() 쿼리 스크립트로 사용하여 Amazon 에 게시할 새 테이블을 생성합니다 DataZone.CTAS 쿼리 편집기에서 이 CTAS 스크립트를 실행하여 게시하고 검색 및 구독에 사용할 수 있는 mkt_sls_table 테이블을 생성합니다.

```
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
```

왼쪽의 테이블 및 보기 섹션에서 mkt_sls_table 테이블이 성공적으로 생성되었는지 확인합니다. 이제 Amazon DataZone 카탈로그에 게시할 수 있는 데이터 자산이 있습니다.

5단계 - Glue에서 AWS 메타데이터 수집

이 섹션에서는 이 워크플로를 위해 AWS Glue에서 메타데이터를 수집하는 단계를 설명합니다.

1. 위의 4단계를 완료한 후 Amazon DataZone 데이터 포털에서 SalesDataPublishingProject 프로젝트를 선택한 다음 데이터 탭을 선택하고 왼쪽 패널에서 데이터 소스를 선택합니다.
2. 환경 생성 프로세스의 일부로 생성된 소스를 선택합니다.
3. 작업 드롭다운 메뉴 옆의 실행을 선택한 다음 새로 고침 버튼을 선택합니다. 데이터 소스 실행이 완료되면 자산이 Amazon DataZone 인벤토리에 추가됩니다.

6단계 - 데이터 자산 큐레이트 및 게시

이 섹션에서는 이 워크플로에서 데이터 자산을 큐레이팅하고 게시하는 단계를 설명합니다.

1. 위의 5단계를 완료한 후 Amazon DataZone 데이터 포털에서 이전 단계에서 생성한 `SalesDataPublishingProject` 프로젝트를 선택하고 데이터 탭을 선택한 다음 왼쪽 패널에서 인벤토리 데이터를 선택하고 `mkt_sls_table` 테이블을 찾습니다.
2. `mkt_sls_table` 자산의 세부 정보 페이지를 열어 자동으로 생성된 비즈니스 이름을 확인합니다. 자산 및 열에 대해 자동 생성된 이름을 보려면 자동 생성된 메타데이터 아이콘을 선택합니다. 각 이름을 개별적으로 수락하거나 거부하거나 모두 수락을 선택하여 생성된 이름을 적용할 수 있습니다. 선택적으로 사용 가능한 메타데이터 양식을 자산에 추가하고 용어집 용어를 선택하여 데이터를 분류할 수도 있습니다.
3. 자산 게시를 선택하여 `mkt_sls_table` 자산을 게시합니다.

7단계 - 데이터 분석을 위한 프로젝트 생성

이 섹션에서는 데이터 분석을 위한 프로젝트를 생성하는 단계를 설명합니다. 이는 이 워크플로의 데이터 소비자 단계의 시작입니다.

1. 위의 6단계를 완료한 후 Amazon DataZone 데이터 포털의 프로젝트 드롭다운 메뉴에서 프로젝트 생성을 선택합니다.
2. 프로젝트 생성 페이지에서 프로젝트 이름을 지정합니다. 예를 들어 이 워크플로의 경우 이름을 지정한 MarketingDataAnalysisProject다음 나머지 필드를 변경하지 않고 그대로 두고 생성을 선택합니다.

8단계 - 데이터 분석을 위한 환경 생성

이 섹션에서는 데이터 분석을 위한 환경을 생성하는 단계를 설명합니다.

1. 위의 7단계를 완료한 후 Amazon DataZone 데이터 포털에서 `MarketingDataAnalysisProject` 프로젝트를 선택한 다음 환경 탭을 선택하고 환경 생성을 선택합니다.
2. 환경 생성 페이지에서 다음을 지정한 다음 환경 생성을 선택합니다.
   - 이름 - 환경의 이름을 지정합니다. 이 연습에서는 라고 부를 수 있습니다`Default data lake environment`.

- 설명 - 환경에 대한 설명을 지정합니다.
- 환경 프로파일 - 기본 제공 DataLakeProfile 환경 프로파일을 선택합니다.
- 이 연습을 위해 나머지 필드는 변경하지 않습니다.

9단계 - 데이터 카탈로그 검색 및 데이터 구독

이 섹션에서는 데이터 카탈로그를 검색하고 데이터를 구독하는 단계를 설명합니다.

1. 위의 8단계를 완료하면 Amazon DataZone 데이터 포털에서 Amazon DataZone 아이콘을 선택하고 Amazon DataZone 검색 필드에서 데이터 포털의 검색 표시줄에서 키워드(예: '카탈로그' 또는 '판매')를 사용하여 데이터 자산을 검색합니다.

   필요한 경우 필터 또는 정렬을 적용하고 제품 판매 데이터 자산을 찾으면 이를 선택하여 자산의 세부 정보 페이지를 열 수 있습니다.
2. 카탈로그 판매 데이터 자산의 세부 정보 페이지에서 구독을 선택합니다.
3. 구독 대화 상자에서 드롭다운에서 MarketingDataAnalysisProject 소비자 프로젝트를 선택한 다음 구독 요청 이유를 지정한 다음 구독을 선택합니다.

10단계 - 구독 요청 승인

이 섹션에서는 구독 요청을 승인하는 단계를 설명합니다.

1. 위의 9단계를 완료한 후 Amazon DataZone 데이터 포털에서 자산을 게시한 SalesDataPublishingProject 프로젝트를 선택합니다.
2. 데이터 탭을 선택한 다음 게시된 데이터 를 선택한 다음 수신 요청 을 선택합니다.
3. 이제 승인이 필요한 새 요청의 행을 볼 수 있습니다. 요청 보기를 선택합니다. 승인 이유를 입력하고 승인을 선택합니다.

11단계 - Amazon Athena에서 쿼리를 빌드하고 데이터를 분석합니다.

이제 Amazon DataZone 카탈로그에 자산을 성공적으로 게시하고 구독했으므로 분석할 수 있습니다.

1. Amazon DataZone 데이터 포털에서 MarketingDataAnalysisProject 소비자 프로젝트를 선택한 다음 오른쪽 패널의 분석 도구 에서 Amazon Athena 를 사용하여 데이터 쿼리 링크를 선택합니다. 이렇게 하면 인증을 위해 프로젝트의 보안 인증 정보를 사용하여 Amazon Athena 쿼리 편집기가 열

립니다. 쿼리 편집기의 Amazon DataZone 환경 드롭다운에서 MarketingDataAnalysisProject 소비자 환경을 선택한 다음 데이터베이스 드롭다운<environment_name>%sub_db에서 프로젝트를 선택합니다.

2. 이제 구독한 테이블에서 쿼리를 실행할 수 있습니다. 테이블 및 뷰 에서 테이블을 선택한 다음 미리 보기를 선택하여 편집기 화면에 선택한 문을 표시할 수 있습니다. 쿼리를 실행하여 결과를 확인합니다.

Amazon Redshift 데이터를 사용한 Amazon DataZone 빠른 시작

다음 빠른 시작 단계를 완료하여 샘플 Amazon Redshift 데이터를 DataZone 사용하여 Amazon에서 전체 데이터 생산자 및 데이터 소비자 워크플로를 실행합니다.

빠른 시작 단계

- 1단계 - Amazon DataZone 도메인 및 데이터 포털 생성
- 2단계 - 게시 프로젝트 생성
- 3단계 - 환경 생성
- 4단계 - 게시를 위한 데이터 생성
- 5단계 - Amazon Redshift에서 메타데이터 수집
- 6단계 - 데이터 자산 큐레이트 및 게시
- 7단계 - 데이터 분석을 위한 프로젝트 생성
- 8단계 - 데이터 분석을 위한 환경 생성
- 9단계 - 데이터 카탈로그 검색 및 데이터 구독
- 10단계 - 구독 요청 승인
- 11단계 - Amazon Redshift에서 쿼리를 빌드하고 데이터 분석

1단계 - Amazon DataZone 도메인 및 데이터 포털 생성

Amazon DataZone 도메인을 생성하려면 다음 절차를 완료하세요. Amazon DataZone 도메인에 대한 자세한 내용은 섹션을 참조하세요Amazon DataZone 용어 및 개념.

1. https://console.aws.amazon.com/datazone의 Amazon DataZone 콘솔로 이동하여 로그인한 다음 도메인 생성을 선택합니다.

> **Note**
>
> 이 워크플로에 기존 Amazon DataZone 도메인을 사용하려면 도메인 보기를 선택한 다음 사용하려는 도메인을 선택한 다음 게시 프로젝트 생성의 2단계로 이동합니다.

2. 도메인 생성 페이지에서 다음 필드에 값을 입력합니다.

- 이름 - 도메인의 이름을 지정합니다. 이 워크플로를 위해 이 도메인 을 호출할 수 있습니다`Marketing`.
- 설명 - 선택적 도메인 설명을 지정합니다.
- 데이터 암호화 - 기본적으로 데이터를 AWS 소유하고 관리하는 키로 암호화됩니다. 이 연습에서는 기본 데이터 암호화 설정을 그대로 둘 수 있습니다.

  고객 관리형 키 사용에 대한 자세한 내용은 섹션을 참조하세요Amazon에 대한 저장 데이터 암호화 DataZone. 데이터 암호화에 자체 KMS 키를 사용하는 경우 기본 에 다음 문을 포함해야 합니다AmazonDataZoneDomainExecutionRole.

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

- 서비스 액세스 - 사용자 지정 서비스 역할 사용 옵션을 선택한 다음 드롭다운 메뉴에서 AmazonDataZoneDomainExecutionRole 를 선택합니다.
- 빠른 설정에서 데이터 소비 및 게시를 위해 이 계정 설정을 선택합니다. 이 옵션은 데이터 레이크 및 데이터 웨어하우스 의 기본 제공 Amazon DataZone 청사진을 활성화하고 이 워크플로의 나머지 단계를 완료하는 데 필요한 권한과 리소스를 구성합니다. Amazon DataZone 청사진에 대한 자세한 내용은 섹션을 참조하세요Amazon DataZone 용어 및 개념.

- 권한 세부 정보 및 태그의 나머지 필드를 변경하지 않고 유지한 다음 도메인 생성을 선택합니다.

3. 도메인이 성공적으로 생성되면 이 도메인을 선택하고 도메인의 요약 페이지에서 이 도메인의 데이터 포털URL을 기록해 둡니다. 이를 사용하여 Amazon DataZone 데이터 포털에 URL 액세스하여 이 워크플로의 나머지 단계를 완료할 수 있습니다.

> **Note**
>
> Amazon 의 현재 릴리스에서 도메인이 생성 DataZone되면 데이터 포털에 대해 URL 생성된 를 수정할 수 없습니다.

도메인 생성을 완료하는 데 몇 분 정도 걸릴 수 있습니다. 다음 단계로 진행하기 전에 도메인의 상태가 사용 가능이 될 때까지 기다립니다.

2단계 - 게시 프로젝트 생성

다음 섹션에서는 이 워크플로에서 게시 프로젝트를 생성하는 단계를 설명합니다.

1. 1단계를 완료하면 DataZone 데이터 포털을 사용하여 Amazon 데이터 포털로 이동하여 Single Sign-On(SSO) 또는 AWS IAM 보안 인증 정보를 사용하여 URL 로그인합니다.
2. 프로젝트 생성을 선택하고 프로젝트 이름을 지정합니다. 예를 들어, 이 워크플로의 경우 이름을 지정한 SalesDataPublishingProject다음 나머지 필드를 변경하지 않은 상태로 두고 생성을 선택합니다.

3단계 - 환경 생성

다음 섹션에서는 이 워크플로에서 환경을 생성하는 단계를 설명합니다.

1. 2단계를 완료한 후 Amazon DataZone 데이터 포털에서 이전 단계에서 생성한 `SalesDataPublishingProject` 프로젝트를 선택한 다음 환경 탭을 선택하고 환경 생성을 선택합니다.
2. 환경 생성 페이지에서 다음을 지정한 다음 환경 생성을 선택합니다.

   - 이름 - 환경의 이름을 지정합니다. 이 연습에서는 를 호출할 수 있습니다`Default data warehouse environment`.
   - 설명 - 환경에 대한 설명을 지정합니다.

- 환경 프로파일 - DataWarehouseProfile 환경 프로파일을 선택합니다.
- Amazon Redshift 클러스터의 이름, 데이터베이스 이름 및 데이터가 저장되는 ARN Amazon Redshift 클러스터의 보안 암호를 입력합니다.

> **Note**
>
> AWS Secrets Manager의 보안 암호에 다음 태그(키/값)가 포함되어 있는지 확인합니다.
>
> - Amazon Redshift 클러스터의 경우 - datazone.rs.cluster: <cluster_name:database name>
>
> Amazon Redshift Serverless 작업 그룹의 경우 - datazone.rs.workgroup: <workgroup_name:database_name>
> - AmazonDataZoneProject: <projectID >
> - AmazonDataZoneDomain: <domainID >
>
> 자세한 내용은 AWS Secrets Manager에 데이터베이스 보안 인증 정보 저장을 참조하세요.
>
> AWS Secrets Manager에 제공하는 데이터베이스 사용자는 수퍼 사용자 권한이 있어야 합니다.

4단계 - 게시를 위한 데이터 생성

다음 섹션에서는 이 워크플로에 게시할 데이터를 생성하는 단계를 설명합니다.

1. 3단계를 완료한 후 Amazon DataZone 데이터 포털에서 `SalesDataPublishingProject` 프로젝트를 선택한 다음 오른쪽 패널의 분석 도구 아래에서 Amazon Redshift를 선택합니다. 이렇게 하면 인증을 위해 프로젝트의 보안 인증 정보를 사용하여 Amazon Redshift 쿼리 편집기가 열립니다.
2. 이 연습에서는 테이블 생성을 선택() 쿼리 스크립트로 사용하여 Amazon 에 게시할 새 테이블을 생성합니다 DataZone.CTAS 쿼리 편집기에서 이 CTAS 스크립트를 실행하여 게시하고 검색 및 구독에 사용할 수 있는 `mkt_sls_table` 테이블을 생성합니다.

```
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 테이블이 성공적으로 생성되었는지 확인합니다. 이제 Amazon DataZone 카탈로그에 게시할 수 있는 데이터 자산이 있습니다.

5단계 - Amazon Redshift에서 메타데이터 수집

다음 섹션에서는 Amazon Redshift에서 메타데이터를 수집하는 단계를 설명합니다.

1. 4단계를 완료하면 Amazon DataZone 데이터 포털에서 `SalesDataPublishingProject` 프로젝트를 선택한 다음 데이터 탭을 선택하고 데이터 소스 를 선택합니다.
2. 환경 생성 프로세스의 일부로 생성된 소스를 선택합니다.
3. 작업 드롭다운 메뉴 옆의 실행을 선택한 다음 새로 고침 버튼을 선택합니다. 데이터 소스 실행이 완료되면 자산이 Amazon DataZone 인벤토리에 추가됩니다.

6단계 - 데이터 자산 큐레이트 및 게시

다음 섹션에서는 이 워크플로에서 데이터 자산을 큐레이팅하고 게시하는 단계를 설명합니다.

1. 5단계를 완료하면 Amazon DataZone 데이터 포털에서 `SalesDataPublishingProject` 프로젝트를 선택한 다음 데이터 탭을 선택하고 인벤토리 데이터 를 선택한 다음 `mkt_sls_table` 테이블을 찾습니다.
2. `mkt_sls_table` 자산의 세부 정보 페이지를 열어 자동으로 생성된 비즈니스 이름을 확인합니다. 자산 및 열에 대해 자동 생성된 이름을 보려면 자동 생성된 메타데이터 아이콘을 선택합니다. 각 이름을 개별적으로 수락하거나 거부하거나 모두 수락을 선택하여 생성된 이름을 적용할 수 있습니다. 선택적으로 사용 가능한 메타데이터 양식을 자산에 추가하고 용어집 용어를 선택하여 데이터를 분류할 수도 있습니다.
3. 게시를 선택하여 `mkt_sls_table` 자산을 게시합니다.

7단계 - 데이터 분석을 위한 프로젝트 생성

다음 섹션에서는 이 워크플로에서 데이터 분석을 위한 프로젝트를 생성하는 단계를 설명합니다.

1. 6단계를 완료한 후 Amazon DataZone 데이터 포털에서 프로젝트 생성 을 선택합니다.
2. 프로젝트 생성 페이지에서 프로젝트 이름을 지정합니다. 예를 들어, 이 워크플로의 경우 이름을 지정한 MarketingDataAnalysisProject다음 나머지 필드를 변경하지 않은 상태로 두고 생성을 선택합니다.

8단계 - 데이터 분석을 위한 환경 생성

다음 섹션에서는 이 워크플로에서 데이터 분석을 위한 환경을 생성하는 단계를 설명합니다.

1. 7단계를 완료한 후 Amazon DataZone 데이터 포털에서 이전 단계에서 생성한 `MarketingDataAnalysisProject` 프로젝트를 선택한 다음 환경 탭을 선택하고 환경 추가를 선택합니다.
2. 환경 생성 페이지에서 다음을 지정한 다음 환경 생성을 선택합니다.
   - 이름 - 환경의 이름을 지정합니다. 이 연습에서는 를 호출할 수 있습니다`Default data warehouse environment`.
   - 설명 - 환경에 대한 설명을 지정합니다.
   - 환경 프로파일 - DataWarehouseProfile 환경 프로파일을 선택합니다.
   - Amazon Redshift 클러스터의 이름, 데이터베이스 이름 및 데이터가 저장되는 ARN Amazon Redshift 클러스터의 보안 암호를 입력합니다.

> **Note**
>
> AWS Secrets Manager의 보안 암호에 다음 태그(키/값)가 포함되어 있는지 확인합니다.
>
> - Amazon Redshift 클러스터의 경우 - datazone.rs.cluster: <cluster_name:database name>
>
> Amazon Redshift Serverless 작업 그룹의 경우 - datazone.rs.workgroup: <workgroup_name:database_name>
> - AmazonDataZoneProject: <projectID >
> - AmazonDataZoneDomain: <domainID >

자세한 내용은 AWS Secrets Manager에 데이터베이스 보안 인증 정보 저장을 참조하세요.
AWS Secrets Manager에 제공하는 데이터베이스 사용자는 수퍼 사용자 권한이 있어야 합니다.

- 이 연습을 위해 나머지 필드는 변경하지 않습니다.

9단계 - 데이터 카탈로그 검색 및 데이터 구독

다음 섹션에서는 데이터 카탈로그를 검색하고 데이터를 구독하는 단계를 설명합니다.

1. 8단계를 완료하면 Amazon DataZone 데이터 포털의 검색 표시줄에서 키워드(예: '카탈로그' 또는 '판매')를 사용하여 데이터 자산을 검색합니다.

   필요한 경우 필터 또는 정렬을 적용하고 제품 판매 데이터 자산을 찾으면 이를 선택하여 자산의 세부 정보 페이지를 열 수 있습니다.
2. 제품 판매 데이터 자산의 세부 정보 페이지에서 구독을 선택합니다.
3. 대화 상자에서 드롭다운에서 소비자 프로젝트를 선택하고 액세스 요청 이유를 입력한 다음 구독을 선택합니다.

10단계 - 구독 요청 승인

다음 섹션에서는 이 워크플로에서 구독 요청을 승인하는 단계를 설명합니다.

1. 9단계를 완료한 후 Amazon DataZone 데이터 포털에서 자산을 게시한 SalesDataPublishingProject 프로젝트를 선택합니다.
2. 데이터 탭을 선택한 다음 게시된 데이터 를 선택하고 수신 요청 을 선택합니다.
3. 요청 보기 링크를 선택한 다음 승인을 선택합니다.

11단계 - Amazon Redshift에서 쿼리를 빌드하고 데이터 분석

이제 Amazon DataZone 카탈로그에 자산을 성공적으로 게시하고 구독했으므로 분석할 수 있습니다.

1. Amazon DataZone 데이터 포털의 오른쪽 패널에서 Amazon Redshift 링크를 클릭합니다. 이렇게 하면 인증에 대한 프로젝트의 자격 증명을 사용하여 Amazon Redshift 쿼리 편집기가 열립니다.

2. 이제 구독한 테이블에서 쿼리(문 선택)를 실행할 수 있습니다. 테이블(three-vertical-dots 선택 사항)을 클릭하고 미리 보기를 선택하여 편집기 화면에서 문을 선택할 수 있습니다. 쿼리를 실행하여 결과를 확인합니다.

샘플 스크립트를 사용한 Amazon DataZone 빠른 시작

관리 포털 또는 Amazon DataZone 데이터 포털을 DataZone 통해 Amazon에 액세스하거나 Amazon를 사용하여 프로그래밍 방식으로 Amazon DataZone HTTPS 에 액세스할 수 API있습니다. 이렇게 하면 서비스에 직접 HTTPS 요청을 발행할 수 있습니다. 이 섹션에는 다음과 같은 일반적인 작업을 완료하는 데 사용할 수 있는 Amazon DataZone APIs을 호출하는 샘플 스크립트가 포함되어 있습니다.

샘플 스크립트

- Amazon DataZone 도메인 및 데이터 포털 생성
- 게시 프로젝트 생성
- 환경 프로파일 생성
- 환경 생성
- Glue에서 AWS 메타데이터 수집
- 데이터 자산 큐레이트 및 게시
- 데이터 카탈로그 검색 및 데이터 구독
- 데이터 카탈로그에서 자산 검색
- 기타 유용한 샘플 스크립트

Amazon DataZone 도메인 및 데이터 포털 생성

다음 샘플 스크립트를 사용하여 Amazon DataZone 도메인을 생성할 수 있습니다. Amazon DataZone 도메인에 대한 자세한 내용은 섹션을 참조하세요Amazon DataZone 용어 및 개념.

```
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",
    )
```

게시 프로젝트 생성

다음 샘플 스크립트를 사용하여 Amazon 에서 게시 프로젝트를 생성할 수 있습니다 DataZone.

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

환경 프로파일 생성

다음 샘플 스크립트를 사용하여 Amazon 에서 환경 프로파일을 생성할 수 있습니다 DataZone.

이 샘플 페이로드는 `CreateEnvironmentProfile`API가 호출될 때 사용됩니다.

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

이 샘플 스크립트는 CreateEnvironmentProfile 를 호출합니다API.

```
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
```

가 호출되면 샘플 출력 페이로드CreateEnvironmentProfileAPI입니다.

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

환경 생성

다음 샘플 스크립트를 사용하여 Amazon 에서 환경을 생성할 수 있습니다 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
```

Glue에서 AWS 메타데이터 수집

이 샘플 스크립트를 사용하여 AWS Glue에서 메타데이터를 수집할 수 있습니다. 이 스크립트는 표준 일정에 따라 실행됩니다. 샘플 스크립트에서 파라미터를 검색하여 전역으로 만들 수 있습니다. 표준 함

수를 사용하여 프로젝트, 환경 및 도메인 ID를 가져옵니다. AWS Glue 데이터 소스는 스크립트의 cron 섹션에서 업데이트할 수 있는 표준 시간에 생성되고 실행됩니다.

```
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"
    }
}
```

데이터 자산 큐레이트 및 게시

다음 샘플 스크립트를 사용하여 Amazon 에서 데이터 자산을 큐레이션하고 게시할 수 있습니다 DataZone.

다음 스크립트를 사용하여 사용자 지정 양식 유형을 생성할 수 있습니다.

```
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"
    )
```

다음 샘플 스크립트를 사용하여 사용자 지정 자산 유형을 생성할 수 있습니다.

```
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,
    )
```

다음 샘플 스크립트를 사용하여 사용자 지정 자산을 생성할 수 있습니다.

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

다음 샘플 스크립트를 사용하여 용어집을 생성할 수 있습니다.

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

다음 샘플 스크립트를 사용하여 용어를 생성할 수 있습니다.

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

다음 샘플 스크립트를 사용하여 시스템 정의 자산 유형을 사용하여 자산을 생성할 수 있습니다.

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

다음 샘플 스크립트를 사용하여 자산 개정을 생성하고 용어를 연결할 수 있습니다.

```
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:>"]
    )
```

다음 샘플 스크립트를 사용하여 자산을 게시할 수 있습니다.

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

데이터 카탈로그 검색 및 데이터 구독

다음 샘플 스크립트를 사용하여 데이터 카탈로그를 검색하고 데이터를 구독할 수 있습니다.

```
def search_asset(domainId, projectId, text):
    return dzclient.search(
```

```
        domainIdentifier = domainId,
        owningProjectIdentifier = projectId,
        searchScope = "ASSET",
        searchText = text,
    )
```

다음 샘플 스크립트를 사용하여 자산의 목록 ID를 가져올 수 있습니다.

```
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']
```

다음 샘플 스크립트를 사용하여 목록 ID를 사용하여 구독 요청을 생성할 수 있습니다.

```
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 위의 를 사용하여 를 가져온 subscription_request_id다음 다음 다음 샘플 스크립트를 사용하여 구독을 수락/승인합니다.

```
subscription_request_id = create_subscription_response["id"]

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

데이터 카탈로그에서 자산 검색

자유 텍스트 검색을 사용하는 다음 샘플 스크립트를 사용하여 Amazon DataZone 카탈로그에서 게시된 데이터 자산(목록)을 검색할 수 있습니다.

- 다음 예제는 도메인에서 자유 텍스트 키워드 검색을 수행하고 제공된 키워드 'credit'과 일치하는 모든 목록을 반환합니다.

```
aws datazone search-listings \
  --domain-identifier dzd_c1s7uxe71prrtz \
  --search-text "credit"
```

- 여러 키워드를 결합하여 검색 범위를 더욱 좁힐 수도 있습니다. 예를 들어 멕시코에서 판매와 관련된 데이터가 있는 게시된 모든 데이터 자산(목록)을 찾는 경우 두 개의 키워드 'Mexico'와 'sales'를 사용하여 쿼리를 공식화할 수 있습니다.

```
          aws datazone search-listings \
  --domain-identifier dzd_c1s7uxe71prrtz \
  --search-text "mexico sales"
```

필터를 사용하여 목록을 검색할 수도 있습니다. 의 filters 파라미터를 SearchListings API 사용하면 도메인에서 필터링된 결과를 검색할 수 있습니다. 는 여러 기본 필터를 API 지원하며 두 개 이상의 필터를 결합하여 AND/OR 작업을 수행할 수도 있습니다. 필터 절은 두 가지 파라미터, 즉 속성과 값을 사용합니다. 지원되는 기본 필터 속성은 typeName, 및 owningProjectId입니다glossaryTerms.

- 다음 예제에서는 목록이 Redshift Table의 유형인 assetType 필터를 사용하여 지정된 도메인의 모든 목록을 검색합니다.

```
            aws datazone search-listings \
--domain-identifier dzd_c1s7uxe71prrtz \
--filters '{"or":[{"filter":
{"attribute":"typeName","value":"RedshiftTableAssetType"}} ]}'
```

- AND/OR 작업을 사용하여 여러 필터를 결합할 수도 있습니다. 다음 예제에서는 typeName 및 project 필터를 결합합니다.

```
            aws datazone search-listings \
--domain-identifier dzd_c1s7uxe71prrtz \
--filters '{"or":[{"filter":
{"attribute":"typeName","value":"RedshiftTableAssetType"}},  {"filter":
{"attribute":"owningProjectId","value":"cwrrjch7f5kppj"}} ]}'
```

- 필터와 함께 자유 텍스트 검색을 결합하여 정확한 결과를 찾고 다음 예제와 같이 목록의 생성/최종 업데이트 시간을 기준으로 정렬할 수도 있습니다.

```
            aws datazone search-listings \
--domain-identifier dzd_c1s7uxe71prrtz \
--search-text "finance sales" \
--filters '{"or":[{"filter":{"attribute":"typeName","value":"GlueTableViewType"}} ]}'
 \
--sort '{"attribute": "UPDATED_AT", "order":"ASCENDING"}'
```

기타 유용한 샘플 스크립트

다음 샘플 스크립트를 사용하여 Amazon 에서 데이터를 사용할 때 다양한 작업을 완료할 수 있습니다 DataZone.

다음 샘플 스크립트를 사용하여 기존 Amazon DataZone 도메인을 나열합니다.

```
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
```

다음 샘플 스크립트를 사용하여 기존 Amazon DataZone 프로젝트를 나열합니다.

```
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
```

다음 샘플 스크립트를 사용하여 기존 Amazon DataZone 메타데이터 양식을 나열합니다.

```
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
```

Amazon의 도메인 및 사용자 액세스 DataZone

이 섹션에서는 Amazon 에서 도메인 및 사용자 액세스를 생성하고 관리하는 방법을 설명합니다 DataZone.

Amazon DataZone 도메인은 자산, 사용자 및 해당 프로젝트를 함께 연결하기 위한 조직 엔터티입니다. Amazon DataZone 도메인을 사용하면 기업을 위한 단일 Amazon 도메인을 생성하든 여러 비즈니스 단위 또는 팀을 위한 여러 데이터 영역, DataZone 도메인을 생성하든 관계없이 조직 구조의 데이터 및 분석 요구 사항을 유연하게 반영할 수 있습니다.

또한 이 섹션에서는 Amazon DataZone 콘솔 및 Amazon DataZone 포털에 대한 사용자 액세스를 관리하는 방법에 대해서도 설명합니다.

자세한 내용은 Amazon DataZone 용어 및 개념 단원을 참조하십시오.

주제

- Amazon DataZone 도메인 생성
- Amazon DataZone 도메인 편집
- Amazon DataZone 도메인 삭제
- Amazon용 IAM Identity Center 활성화 DataZone
- Amazon용 IAM Identity Center 비활성화 DataZone
- Amazon DataZone 콘솔에서 사용자 관리
- Amazon DataZone 데이터 포털에서 사용자 권한 관리

Amazon DataZone 도메인 생성

> **Note**
>
> Amazon DataZone with AWS Identity Center를 사용하여 SSO 사용자 및 그룹에 대한 액세스를 제공하는 경우 현재 Amazon DataZone 도메인은 AWS Identity Center 인스턴스와 동일한 AWS 리전에 있어야 합니다.

Amazon DataZone, 도메인은 자산, 사용자 및 해당 프로젝트를 함께 연결하기 위한 조직 엔터티입니다. 자세한 내용은 Amazon DataZone 용어 및 개념 단원을 참조하십시오.

Amazon DataZone 도메인을 생성하려면 관리 권한이 있는 계정에서 IAM 역할을 맡아야 합니다. Amazon DataZone 관리 콘솔을 사용하는 데 필요한 IAM 권한을 구성합니다.를 사용하여 도메인을 생성하는 데 필요한 최소 권한을 얻어야 합니다.

Amazon은 기본 구성으로 도메인 사용자를 대신하여 작업을 수행하기 DataZone 위해 추가 IAM 역할이 필요합니다. 이러한 IAM 역할을 미리 생성하거나 Amazon에서 직접 DataZone 생성하도록 할 수 있습니다. 도메인 생성 프로세스 중에 Amazon이 이러한 IAM 역할을 생성 DataZone 하도록 하려면 도메인 생성의 경우 역할 생성 권한이 있는 IAM 역할을 수임해야 합니다. Amazon DataZone 서비스 콘솔의 간소화된 역할 생성을 활성화하기 위한 IAM 권한에 대한 사용자 지정 정책을 생성합니다.을 참조하세요. 도메인 생성 선택에 따라 Amazon DataZone 은 , , 및 AmazonDataZoneDomainExecutionRole의 최대 4개의 새 IAM 역할을 생성합니다AmazonDataZoneGlueManageAccessRoleAmazonDataZoneRedshiftManageAccessRoleAmazonDataZon

Amazon DataZone 도메인을 생성하려면 다음 절차를 완료하세요.

1. https://console.aws.amazon.com/datazone의 Amazon DataZone 콘솔로 이동하여 상단 탐색 모음의 리전 선택기를 사용하여 적절한 AWS 리전을 선택합니다.
2. 도메인 생성을 선택하고 다음 필드에 값을 제공합니다.

   - 이름 - 도메인의 표시 이름을 지정합니다. 도메인이 생성되면 이 이름을 변경할 수 없습니다.
   - 설명 - (선택 사항) 도메인 설명을 지정합니다.
   - 데이터 암호화 - Amazon DataZone 도메인, 메타데이터 및 보고 데이터는 Amazon 에 고유한 키를 사용하여 AWS Key Management Service(KMS)에 의해 암호화됩니다 DataZone. 이 필드를 사용하여 소유 키를 사용할 AWS 지 아니면 다른 AWS KMS 키를 선택할지 지정합니다.

     고객 관리형 키 사용에 대한 자세한 내용은 섹션을 참조하세요Amazon에 대한 저장 데이터 암호화 DataZone. 데이터 암호화에 자체 KMS 키를 사용하는 경우 기본 에 다음 문을 포함해야 합니다AmazonDataZoneDomainExecutionRole.

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

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

- 서비스 액세스 - Amazon에서 새 를 DataZone 생성하여 사용할지 DomainExecutionRole 아니면 기존 IAM 역할을 선택할지 선택합니다.
- 빠른 설정 - (선택 사항) Amazon에서 데이터 소비 및 게시를 위해 계정을 DataZone 설정하여 더 빠르게 시작하려면 이 상자를 선택합니다. Amazon DataZone 은 AWS Glue 및 Amazon Redshift 리소스에 대한 액세스를 프로비저닝, 수집 및 관리하기 위한 세 가지 IAM 역할을 생성하고, 새 Amazon S3 버킷을 생성하고, 관리 Amazon DataZone 프로젝트를 생성하고, 데이터 레이크 및 데이터 웨어하우스 기본 청사진에 대한 환경 프로파일을 생성합니다.
- 태그 - (선택 사항) 도메인에 대한 AWS 태그(키 및 값 페어)를 지정합니다.
- 도메인이 성공적으로 생성되면 브라우저를 새로 고쳐 새 Amazon DataZone 도메인의 세부 정보 페이지를 표시해야 합니다.

Amazon DataZone 도메인 편집

Amazon 에서 도메인은 자산 DataZone, 사용자 및 해당 프로젝트를 함께 연결하기 위한 조직 엔터티입니다. 자세한 내용은 Amazon DataZone 용어 및 개념 단원을 참조하십시오.

Amazon DataZone 도메인을 생성한 후 나중에 설명을 변경하고, IAM Identity Center를 활성화하고, 태그 키와 해당 값을 추가, 편집 또는 제거하도록 도메인을 편집할 수 있습니다. Amazon DataZone 도메인을 편집하려면 관리 권한이 있는 계정에서 IAM 역할을 맡아야 합니다. Amazon DataZone 관리 콘솔을 사용하는 데 필요한 IAM 권한을 구성합니다.를 사용하여 도메인을 편집하는 데 필요한 최소 권한을 얻어야 합니다.

도메인을 편집하려면 다음 단계를 완료합니다.

1. AWS 관리 콘솔에 로그인하고 https://console.aws.amazon.com/datazone 에서 Amazon DataZone 콘솔을 엽니다.
2. 도메인 보기를 선택하고 목록에서 도메인 이름을 선택합니다. 이름은 하이퍼링크입니다.
3. 도메인의 세부 정보 페이지에서 편집을 선택합니다.
4. • 설명 을 편집합니다.

- IAM Identity Center 설정 을 설정합니다. 에서 이러한 설정에 대해 자세히 알아보세요설정 AWS IAM아마존 아이덴티티 센터 DataZone.
- 태그 키와 해당 값을 추가, 편집 또는 제거합니다.

5. 편집한 후에는 도메인 업데이트를 선택합니다.

Amazon DataZone 도메인 삭제

Amazon 에서 도메인은 자산 DataZone, 사용자 및 해당 프로젝트를 함께 연결하기 위한 조직 엔터티입니다. 자세한 내용은 Amazon DataZone 용어 및 개념 단원을 참조하십시오.

도메인을 삭제하는 작업은 최종적입니다. 삭제하면 데이터 소스, 프로젝트, 환경, 자산, 용어집 및 메타데이터 양식을 포함한 모든 Amazon DataZone 엔터티를 취소할 수 없습니다. 삭제는 Amazon이 IAM 역할, S3 버킷, AWS Glue 데이터베이스, LakeFormation 또는 Redshift를 통한 구독 권한 부여와 같이 생성에 도움이 되었을 DataZone 수 있는 Amazon 이외의 DataZone AWS 리소스를 삭제하지 않습니다. 이러한 리소스가 더 이상 필요하지 않은 경우 해당 AWS 서비스에서 해당 리소스를 삭제합니다.

누군가가 도메인을 악의적으로 삭제하지 못하도록 하려면 도메인을 삭제하려면 Amazon 에 대한 관리 IAM 권한이 필요하며 DataZone, 이 권한은 로 구성할 수 있습니다IAM. 누군가가 실수로 도메인을 삭제하지 못하도록 하려면 도메인을 삭제하려면 확인 단어(Amazon DataZone 콘솔에서)가 필요합니다.

도메인을 삭제하려면 다음 단계를 완료합니다.

1. AWS 관리 콘솔에 로그인하고 https://console.aws.amazon.com/datazone 에서 Amazon DataZone 콘솔을 엽니다.
2. 도메인 보기를 선택하고 목록에서 도메인 이름을 선택합니다. 이름은 하이퍼링크입니다.
3. 삭제를 선택하고 정보 경고를 검토합니다.
4. 요청된 텍스트를 입력하여 이러한 경고를 이해했는지 확인합니다. Delete(삭제)를 선택합니다.

> **Important**
>
> 도메인을 삭제하는 것은 사용자 또는 에서 취소할 수 없는 취소 불가능한 작업입니다 AWS.

> **Note**
>
> 사용자 또는 도메인 사용자가 프로젝트에서 환경을 생성하면 Amazon DataZone은 도메인 또는 연결된 계정에 AWS 리소스를 생성하여 사용자와 도메인 사용자에게 기능을 제공합니다. 다음은 Amazon이 도메인의 프로젝트에 대해 생성할 DataZone 수 있는 AWS 리소스 목록과 기본 이름입니다. 도메인을 삭제해도 계정에서 AWS 이러한 AWS 리소스는 삭제되지 않습니다.
>
> - IAM 역할: datazone_usr_<environmentId>.
> - Glue 데이터베이스: (1) <environmentName>_pub_db-*, (2) <environmentName>_sub_db-*. 이 이름의 기존 데이터베이스가 이미 있는 경우 Amazon DataZone 은 환경 ID를 추가합니다.
> - Athena 작업 그룹: <environmentName>-*. 이 이름의 기존 작업 그룹이 이미 있는 경우 Amazon DataZone 은 환경 ID를 추가합니다.
> - CloudWatch 로그 그룹: datazone_<environmentId>

Amazon용 IAM Identity Center 활성화 DataZone

> **Note**
>
> 이 절차를 완료하려면 Amazon DataZone 도메인과 AWS IAM 동일한 AWS 리전에서 Identity Center가 활성화되어 있어야 합니다.

AWS IAM Identity Center를 사용하여 SSO 사용자 및 그룹에 Amazon DataZone 데이터 포털에 대한 액세스 권한을 제공할 수 있습니다. 를 완료한 후 SSO 사용자 및 그룹이 Amazon DataZone 도메인 데이터 포털에 액세스하도록 활성화할 설정 AWS IAM아마존 아이덴티티 센터 DataZone수 있습니다.

Identity Center를 Amazon DataZone 도메인과 함께 사용하도록 설정하려면 AWS IAM 관리 권한이 있는 계정에서 IAM 역할을 맡아야 합니다. Amazon DataZone 관리 콘솔을 사용하는 데 필요한 IAM 권한을 구성합니다. 및 Amazon DataZone 서비스 콘솔의 간소화된 역할 생성을 활성화하기 위한 IAM 권한에 대한 사용자 지정 정책을 생성합니다.를 사용하여 IAM Identity Center를 Amazon 에서 사용하도록 설정하는 데 필요한 최소 권한을 얻어야 합니다 DataZone.

다음 절차를 완료하여 Identity Center for Amazon 를 AWS IAM 활성화합니다 DataZone.

1. AWS 관리 콘솔에 로그인하고 https://console.aws.amazon.com/datazone 에서 DataZone 콘솔을 엽니다.
2. 도메인 보기를 선택하고 목록에서 도메인 이름을 선택합니다. 이름은 하이퍼링크입니다.
3. 도메인의 세부 정보 페이지에서 편집을 선택합니다.
   - IAM Identity Center에서 사용자 활성화 확인란을 선택합니다.
   - IAM Identity Center의 조직 인스턴스에 연결할지 또는 IAM Identity Center의 계정 인스턴스에 연결할지 선택합니다.
   - 두 사용자 할당 모드 중에서 선택합니다. 도메인이 선택 항목으로 업데이트되면 나중에 변경할 수 없습니다.
     - 암시적 사용자 할당 을 사용하면 IAM Identity Center 디렉터리에 추가된 모든 사용자가 Amazon DataZone 도메인에 액세스할 수 있습니다.
     - 명시적 사용자 할당 을 사용하면 IAM Identity Center 디렉터리의 특정 사용자 또는 그룹을 추가하여 Amazon DataZone 도메인에 대한 액세스 권한을 제공합니다. Amazon DataZone 콘솔에서 나중에 이러한 사용자 및 그룹을 추가하고 제거합니다.
4. 선택한 항목에 만족하면 도메인 업데이트를 선택합니다.

Amazon용 IAM Identity Center 비활성화 DataZone

Amazon DataZone 도메인에 Identity Center를 비활성화 AWS IAM하면 모든 SSO 사용자의 액세스 권한이 제거됩니다.

> **Note**
>
> IAM Identity Center를 비활성화해도 SSO 사용자에 대한 결제가 중지되지 않습니다. SSO 사용자의 결제를 중지하려면 도메인에서 사용자를 비활성화해야 합니다. 결제는 사용자가 비활성화된 달이 끝날 때까지 계속됩니다. 사용자를 비활성화하려면 섹션을 참조하세요Amazon DataZone 콘솔에서 사용자 관리.

AWS IAM Identity Center를 사용하여 SSO 사용자 및 그룹에 Amazon DataZone 데이터 포털에 대한 액세스 권한을 제공할 수 있습니다. Amazon용 Identity Center를 활성화 AWS IAM한 경우 나중에 모든 사용자의 액세스를 비활성화할 DataZone수 있습니다.

Identity Center를 Amazon DataZone 도메인과 함께 사용하도록 비활성화 AWS IAM하려면 관리 권한이 있는 계정에서 IAM 역할을 수임해야 합니다. Amazon DataZone 관리 콘솔을 사용하는 데 필요한

IAM 권한을 구성합니다. 및 Amazon DataZone 서비스 콘솔의 간소화된 역할 생성을 활성화하기 위한 IAM 권한에 대한 사용자 지정 정책을 생성합니다.를 사용하여 IAM Identity Center를 Amazon 에서 사용하지 않도록 비활성화하는 데 필요한 최소 권한을 얻어야 합니다 DataZone.

다음 절차를 완료하여 Identity Center for Amazon 를 AWS IAM 비활성화합니다 DataZone.

1. AWS 관리 콘솔에 로그인하고 https://console.aws.amazon.com/datazone 에서 DataZone 콘솔을 엽니다.
2. 도메인 보기를 선택하고 목록에서 도메인 이름을 선택합니다. 이름은 하이퍼링크입니다.
3. arn:aws:datazone:<regionName>:<>:accountIddomain/<domainName>로 시작하는 도메인의 Amazon 리소스 이름(ARN)을 복사합니다.
4. 에서 IAM Identity Center 콘솔을 엽니다https://console.aws.amazon.com/singlesignon/.
5. [Applications]를 선택합니다.
6. Identity Center를 비활성화 AWS IAM하려는 도메인을 선택하면 모든 SSO 사용자의 도메인 데이터 포털에 대한 액세스 권한이 제거됩니다. 필터 메뉴와 검색 상자를 사용하여 애플리케이션 목록을 필터링할 수 있습니다.
7. 작업 메뉴에서 비활성화를 선택합니다.
8. SSO 사용자가 Amazon DataZone 도메인에 액세스할 수 없게 됩니다.
9. Amazon DataZone 도메인에 대해 Identity Center를 다시 활성화 AWS IAM하려면 Identity Center를 다시 활성화 AWS IAM하려는 도메인을 선택하고 작업 메뉴에서 활성화를 선택합니다.

Amazon DataZone 콘솔에서 사용자 관리

사용자는 자격 AWS 증명 또는 Single Sign-On(SSO) 자격 증명을 사용하여 Amazon DataZone 데이터 포털에 액세스할 수 있습니다. Amazon DataZone DataZone 도메인에 대한 Amazon 콘솔에서 사용자를 관리하려면 관리 권한이 있는 계정에서 IAM 역할을 맡아야 합니다. Amazon DataZone 관리 콘솔을 사용하는 데 필요한 IAM 권한을 구성합니다.를 사용하여 Amazon DataZone 콘솔에서 사용자를 관리하는 데 필요한 최소 권한을 얻어야 합니다.

주제

- IAM 역할 및 사용자 관리
- SSO 사용자 관리
- SSO 그룹 관리

IAM 역할 및 사용자 관리

IAM 역할 및 사용자는 AWS Identity and Access Management(IAM)를 사용하여 생성되며 정책을 통해 연결된 권한을 통해 Amazon DataZone 도메인에 액세스할 수 있습니다. 자세한 내용은 Amazon DataZone 데이터 포털을 사용하는 데 필요한 IAM 권한을 구성합니다. 단원을 참조하십시오. Amazon의 현재 릴리스에서 Amazon DataZone 도메인 소유자 계정의 DataZone관리자는 자신의 계정에 있는 사용자 또는 연결된 계정의 사용자에 대한 IAM 사용자 프로필을 생성할 수 있습니다. Amazon DataZone 도메인 소유자 계정의 관리자는 기존 사용자의 상태를 할당됨 또는 할당되지 않음으로 설정하거나(Amazon 을 사용하도록 할당되거나 할당되지 않음 DataZone) 기존 사용자를 활성화 또는 비활성화할 수도 있습니다.

1. AWS 관리 콘솔에 로그인하고 https://console.aws.amazon.com/datazone 에서 DataZone 콘솔을 엽니다.
2. 도메인 보기를 선택하고 목록에서 도메인 이름을 선택합니다. 이름은 하이퍼링크입니다.
3. 도메인의 세부 정보 페이지에서 사용자 관리 를 선택합니다.
4. Amazon DataZone 도메인 소유자 계정 또는 연결된 계정에서 사용자 IAM 사용자를 추가하려면 추가를 선택한 다음 IAM 사용자 추가를 선택합니다.
5. 사용자 추가 페이지에서 현재 계정 또는 연결된 계정 을 선택하고 사용자 또는 역할 찾기 및 추가 필드를 사용하여 추가하려는 사용자를 찾은 다음 사용자 추가 를 선택합니다.
6. 기존 IAM 사용자의 상태를 보려면 사용자 관리 페이지에서 IAM 사용자 유형 드롭다운 메뉴에서 사용자를 선택합니다.

   - 이름 열에는 IAM 사용자 또는 역할ARN의 가 표시됩니다.
   - 상태 열에는 도메인에서 IAM 사용자 또는 역할의 현재 상태가 표시됩니다.
     - 할당됨이란 IAM 사용자가 Amazon 를 사용하도록 할당되었음을 의미합니다 DataZone.
     - 할당되지 않음은 IAM 사용자가 Amazon 를 사용하도록 할당되지 않았음을 의미합니다 DataZone.
     - 활성화됨이란 IAM 사용자 또는 역할이 를 호출하거나, (명령줄 인터페이스를 통해) 명령을 실행하거나API, 도메인의 Amazon DataZone 포털에 액세스했으며, 사용자의 구독 요금이 청구되고 있음을 의미합니다.
     - 비활성화됨이란 IAM 사용자 또는 역할이 Amazon DataZone 도메인에 대한 액세스가 차단되었음을 의미합니다.
7. 현재 활성화된 IAM 사용자 또는 역할을 비활성화하려면 사용자 옆의 확인란을 선택하고 작업 메뉴에서 비활성화를 선택합니다. 사용자가 Amazon DataZone 도메인에 액세스할 수 없게 됩니다. 사용자에 대한 결제는 현재 역월 말에 종료됩니다.

8. 현재 비활성화된 IAM 사용자 또는 역할을 활성화하려면 사용자 옆의 확인란을 선택하고 작업 메뉴에서 활성화를 선택합니다. 사용자 또는 역할에 적절한 권한이 있는 경우 IAM 사용자는 Amazon DataZone 도메인에 액세스할 수 있습니다. 사용자에 대한 결제가 다시 시작됩니다.

SSO 사용자 관리

SSO 사용자는 Identity Center에서 AWS IAM 자격 증명 공급자와 생성 또는 동기화됩니다. 자세한 내용은 설정 AWS IAM아마존 아이덴티티 센터 DataZone 및 Amazon용 IAM Identity Center 활성화 DataZone 를 참조하여 Amazon용 Identity Center를 활성화하고 구성합니다 AWS IAM DataZone. 도메인에 할당된 SSO 사용자 목록을 보고, SSO 사용자를 추가하고, SSO 사용자를 제거할 수 있습니다.

1. AWS 관리 콘솔에 로그인하고 https://console.aws.amazon.com/datazone 에서 DataZone 콘솔을 엽니다.
2. 도메인 보기를 선택하고 목록에서 도메인 이름을 선택합니다. 이름은 하이퍼링크입니다.
3. 도메인의 세부 정보 페이지에서 아래로 스크롤하여 사용자 관리 를 선택합니다.
4. 사용자 유형에서 SSO 사용자를 선택하여 현재 SSO 사용자 목록을 봅니다.

    - 이름 열에는 SSO 사용자의 이름이 표시됩니다.
    - 상태 열에는 도메인에 있는 SSO 사용자의 현재 상태가 표시됩니다.
        - 할당됨은 SSO 사용자가 도메인에 명시적으로 할당되었음을 의미합니다. 따라서 사용자는 Amazon 에 액세스할 수 있습니다 DataZone. 이 상태는 도메인의 자격 증명 공급자 모드가 명시적 할당으로 설정된 경우에만 사용됩니다.
        - 활성화됨은 SSO 사용자가 도메인의 Amazon DataZone 포털에 액세스했으며 사용자의 구독에 대한 요금이 청구되고 있음을 의미합니다. 활성화는 자동으로 이루어집니다.
        - 비활성화됨은 도메인의 데이터 포털에 대한 SSO 사용자의 액세스가 차단되었음을 의미합니다. 사용자의 액세스가 비활성화된 달의 말일에 종료된 사용자에 대한 결제입니다.
        - 제거됨은 SSO 사용자가 이전에 도메인에 할당되었지만 액세스하기 전에 제거되었음을 의미합니다.
5. SSO 사용자 추가 및 추가를 선택하여 사용자를 추가합니다. 도메인이 암시적 사용자 할당으로 설정된 경우 이 옵션을 사용할 수 없습니다. 즉, 자격 증명 풀의 모든 사용자가 Amazon DataZone 도메인에 액세스할 수 있습니다.

    - 사용자 추가 페이지에서 추가하려는 사용자의 별칭을 검색합니다. 검색 상자 아래에 일치하는 목록이 표시됩니다.
    - 추가할 사용자를 선택합니다. 별칭은 검색 상자 아래에 칩으로 표시됩니다.

- 추가하려는 사용자 목록에 만족하면 사용자 추가(Add user)를 선택합니다.
- 사용자는 상태가 '할당됨'인 Amazon DataZone 도메인에 할당됩니다.
- 사용자가 도메인의 데이터 포털에 처음 액세스하면 상태가 자동으로 활성화됨으로 변경되고 사용자의 구독에 대한 요금이 청구되기 시작합니다.

6. SSO 사용자를 선택하고 작업 메뉴에서 비활성화를 선택하여 할당된 사용자를 제거합니다. 따라서 사용자는 Amazon DataZone 도메인에 대한 액세스 권한을 잃게 됩니다. 사용자의 상태는 제거됨으로 표시됩니다. 도메인이 암시적 사용자 할당으로 설정된 경우 이 옵션을 사용할 수 없습니다.
7. 사용자를 선택하고 작업 메뉴에서 비활성화를 선택하여 활성화된 SSO 사용자를 비활성화합니다. 따라서 Amazon DataZone 도메인에 대한 사용자의 액세스 권한이 손실되고 차단됩니다. 사용자의 구독에 대한 결제는 월말까지 계속됩니다. 사용자의 상태는 비활성화 로 표시됩니다.
8. SSO 사용자를 선택하고 작업 메뉴에서 활성화를 선택하여 비활성화된 사용자를 활성화합니다. 따라서 사용자는 Amazon DataZone 도메인에 다시 액세스할 수 있습니다. 결제가 즉시 시작됩니다. 사용자는 활성화된 로 표시됩니다.

SSO 그룹 관리

SSO 그룹은 Identity Center의 AWS IAM 자격 증명 공급자와 생성 또는 동기화됩니다. 자세한 내용은 설정 AWS IAM아마존 아이덴티티 센터 DataZone 및 Amazon용 IAM Identity Center 활성화 DataZone를 참조하여 Amazon용 Identity Center를 활성화하고 구성합니다 AWS IAM DataZone. 도메인에 할당된 SSO 그룹 목록을 보고, SSO 그룹을 추가하고, SSO 그룹을 제거할 수 있습니다.

1. AWS 관리 콘솔에 로그인하고 https://console.aws.amazon.com/datazone 에서 DataZone 콘솔을 엽니다.
2. 도메인 보기를 선택하고 목록에서 도메인 이름을 선택합니다. 이름은 하이퍼링크입니다.
3. 도메인의 세부 정보 페이지에서 아래로 스크롤하여 사용자 관리 를 선택합니다.
4. 사용자 유형에서 SSO 그룹을 선택하여 현재 SSO 그룹 목록을 봅니다.

- 이름 열에는 SSO 그룹의 이름이 표시됩니다.
- 상태 열에는 도메인에 있는 SSO 그룹의 현재 상태가 표시됩니다.
  - 할당됨이란 SSO 그룹이 도메인에 명시적으로 할당되었음을 의미합니다. 따라서 그룹의 모든 사용자는 도메인의 데이터 포털에 액세스할 수 있습니다(사용자가 비활성화되지 않은 경우).
  - 할당되지 않음은 SSO 그룹이 도메인에서 제거되었음을 의미합니다. 그룹의 사용자는 이 그룹의 멤버십을 통해 도메인의 데이터 포털에 액세스할 수 없습니다.

5. SSO 그룹 추가 및 추가를 선택하여 그룹을 추가합니다. 도메인이 암시적 사용자 할당으로 설정된 경우 이 옵션을 사용할 수 없습니다. 즉, 자격 증명 풀의 모든 사용자는 그룹 멤버십에 관계없이 Amazon DataZone 도메인에 액세스할 수 있습니다.

   - 그룹 추가 페이지에서 추가하려는 그룹의 별칭을 검색합니다. 검색 상자 아래에 일치하는 목록이 표시됩니다.
   - 추가할 그룹을 선택합니다. 별칭은 검색 상자 아래에 칩으로 표시됩니다.
   - 추가하려는 그룹 목록에 만족하면 그룹 추가(Add group)를 선택합니다.
   - 그룹은 상태가 '할당됨'인 Amazon DataZone 도메인에 할당됩니다.
   - 그룹의 멤버가 도메인의 데이터 포털에 액세스하면 상태가 자동으로 활성화됨으로 변경되고 사용자의 구독에 대한 요금이 청구되기 시작합니다.
6. 그룹을 선택하고 작업 메뉴에서 할당 취소를 선택하여 할당된 SSO 그룹을 제거합니다. 따라서 그룹은 Amazon DataZone 도메인에 대한 액세스 권한을 잃게 됩니다. 그룹의 상태는 할당되지 않음 으로 표시됩니다. 이 그룹의 멤버십을 DataZone 통해 Amazon에 액세스한 사용자는 액세스 권한을 상실합니다. 도메인이 암시적 사용자 할당으로 설정된 경우 이 옵션을 사용할 수 없습니다. 그룹 할당을 취소하여 액세스가 제거된 사용자의 결제를 중지하려면 다음으로 사용자 프로필을 수동으로 선택하고 비활성화해야 합니다.

Amazon DataZone 데이터 포털에서 사용자 권한 관리

Amazon 의 현재 릴리스에서 기본 권한 부여 메커니즘 DataZone을 사용하면 Amazon DataZone 도메인의 모든 인증된 사용자(IAM 및 SSO)가 프로젝트를 생성하고, 프로젝트 내에 엔터티를 생성하고, 검색을 수행할 수 있습니다. 프로젝트 멤버는 지정된 프로젝트 소유자 또는 프로젝트 기여자 역할에 따라 자신에게 부여된 권한을 계속 준수해야 합니다.

Amazon의 도메인 단위 및 권한 부여 정책 DataZone

도메인 단위를 사용하면 특정 사업부 및 팀에서 자산 및 기타 도메인 엔터티를 쉽게 구성할 수 있습니다. 조직의 사업부 내에서 그리고 사업부 간에 안전하고 효율적인 데이터 공유를 설정하려면 Amazon DataZone 내에서 도메인 유닛을 생성하고 각 사업부 내에서 선택한 사용자가 카탈로그에 로그인하여 자산을 공유할 수 있도록 할 수 있습니다. 엔터프라이즈의 모든 위치에 있는 사용자는 해당 사업부에서 자산을 쉽게 검색하고 해당 자산에 대한 액세스를 요청할 수 있습니다. 또한 도메인 단위를 사용하여 AWS 계정 소유자와 같은 리소스 소유자가 리소스에 대한 Amazon DataZone 권한 부여 권한을 설정할 수 있습니다. 도메인 유닛은 계정 소유자로부터 도메인 유닛 소유자에게 위임된 권한을 제공하며 계정 소유자를 대신하여 환경 프로파일(청사진 구성을 사용하여 생성됨)에 대한 권한 부여 권한을 설정할 수 있습니다. 이를 통해 소속 사업부에 따라 환경 프로필을 생성하고 사용할 수 있는 사용자를 쉽게 제한할 수 있습니다. Amazon DataZone 권한 부여 권한은 메타데이터 표준을 적용하고 선택한 프로젝트만 메타데이터 양식 및 용어집을 생성할 수 있도록 하는 데도 사용할 수 있습니다. 이렇게 하면 일관되고 품질 좋은 메타데이터를 유지하는 데 도움이 될 수 있습니다. 자세한 내용은 Amazon DataZone 용어 및 개념 단원을 참조하십시오.

Amazon DataZone 도메인 유닛 내에서 사용자 및 그룹에 다음 권한 부여 정책을 할당하여 특정 권한을 부여할 수 있습니다.

- 도메인 단위 생성 정책
- 프로젝트 생성 정책
- 프로젝트 멤버십 정책
- 도메인 유닛 소유권 가정 정책
- 프로젝트 소유권 가정 정책

자세한 내용은 Amazon DataZone 도메인 유닛 내의 사용자 및 그룹에 권한 부여 정책 할당 단원을 참조하십시오.

Amazon DataZone 도메인 유닛 내에서 프로젝트에 다음 권한 부여 정책을 할당하여 특정 권한을 부여할 수 있습니다.

- 용어 생성 정책
- 메타데이터 양식 생성 정책
- 사용자 지정 자산 유형 생성 정책

자세한 내용은 Amazon DataZone 도메인 유닛 내의 프로젝트에 권한 부여 정책 할당 단원을 참조하십시오.

Amazon에서 권한 부여 메커니즘을 사용하는 또 다른 방법은 Amazon DataZone 청사진 구성 내의 프로젝트 및 도메인 유닛 소유자에게 권한 부여 정책을 적용하는 DataZone 것입니다.

Amazon DataZone 블루프린트 구성은 사용자 워크플로 게시 및 구독에 사용되는 리소스를 생성하고 구성하는 데 필요한 정보를 캡슐화하는 엔터티입니다. 이 정보에는 AWS 계정 번호 및 리전, CFN 템플릿, VPCs 및 서브넷과 같은 계정 수준 파라미터가 포함되며 데이터베이스 연결 정보 및 보안 인증 정보도 포함될 수 있습니다. 비용을 제어하고 보안을 개선하기 위해 데이터 플랫폼 사용자는 이러한 청사진을 사용하고 환경을 생성할 수 있는 사용자를 제어할 수 있는 기능이 필요합니다.

특정 청사진 구성 내에서 프로젝트 및 도메인 유닛 소유자에게 다음과 같은 권한 부여 정책을 할당할 수 있습니다.

- 이 청사진을 사용하여 환경 프로파일 생성 - 이 정책은 Amazon DataZone 프로젝트에 할당할 수 있으며 이 청사진을 사용하여 환경 프로파일을 생성할 수 있는 권한을 부여합니다.
- 이 청사진을 사용하여 환경 프로파일을 생성할 수 있는 권한을 부여합니다. 이 정책은 도메인 유닛 소유자에게 할당할 수 있으며 이 청사진을 사용하여 환경 프로파일을 생성할 수 있는 권한을 프로젝트에 부여합니다.

자세한 내용은 Amazon DataZone 블루프린트 구성 내에서 권한 부여 정책 할당 단원을 참조하십시오.

주제

- Amazon에서 도메인 유닛 생성 DataZone
- Amazon에서 도메인 단위 편집 DataZone
- Amazon에서 도메인 유닛 삭제 DataZone
- Amazon에서 도메인 유닛 소유자 관리 DataZone
- Amazon DataZone 도메인 유닛 내의 사용자 및 그룹에 권한 부여 정책 할당
- Amazon DataZone 도메인 유닛 내의 프로젝트에 권한 부여 정책 할당
- Amazon DataZone 블루프린트 구성 내에서 권한 부여 정책 할당

Amazon에서 도메인 유닛 생성 DataZone

Amazon 에서 DataZone도메인 단위를 사용하면 특정 사업부 및 팀에서 자산 및 기타 도메인 엔터티를 구성할 수 있습니다. 자세한 내용은 Amazon DataZone 용어 및 개념 단원을 참조하십시오.

도메인 유닛을 생성하려면

1. DataZone 데이터 포털을 사용하여 Amazon 데이터 포털로 이동URL하고 SSO 또는 AWS 자격 증명을 사용하여 로그인합니다. Amazon DataZone 관리자인 경우 Amazon DataZone 도메인이 생성된 AWS 계정의 https://console.aws.amazon.com/datazone에서 Amazon DataZone 콘솔에 액세스URL하여 데이터 포털을 얻을 수 있습니다.
2. 도메인 보기를 선택하고 도메인 단위를 생성할 도메인을 선택합니다.
3. 도메인 세부 정보 페이지에서 도메인 단위 탭으로 이동합니다.
4. 도메인 유닛 생성을 선택합니다.
5. 다음을 지정한 다음 도메인 유닛 생성을 선택합니다.
   - 도메인 단위 세부 정보 에서 이름 에 도메인 단위 이름을 지정합니다.
   - 도메인 단위 세부 정보 에서 설명 에 도메인 단위 설명을 지정합니다.
   - 도메인 단위 상위 - 새 도메인 단위를 추가할 상위 도메인 단위를 선택합니다.
   - 도메인 단위 소유자 - 이 도메인 단위를 편집할 수 있는 도메인 단위 소유자를 지정합니다.

Amazon에서 도메인 단위 편집 DataZone

Amazon 에서 DataZone도메인 단위를 사용하면 특정 사업부 및 팀에서 자산 및 기타 도메인 엔터티를 구성할 수 있습니다. 자세한 내용은 Amazon DataZone 용어 및 개념 단원을 참조하십시오.

도메인 단위를 편집하려면

1. DataZone 데이터 포털을 사용하여 Amazon 데이터 포털로 이동URL하고 SSO 또는 AWS 자격 증명을 사용하여 로그인합니다. Amazon DataZone 관리자인 경우 Amazon DataZone 도메인이 생성된 AWS 계정의 https://console.aws.amazon.com/datazone에서 Amazon DataZone 콘솔에 액세스URL하여 데이터 포털을 얻을 수 있습니다.
2. 도메인 보기를 선택하고 도메인 단위를 편집할 도메인을 선택합니다.
3. 도메인 세부 정보 페이지에서 도메인 단위 탭으로 이동하여 편집할 도메인 단위를 선택합니다.
4. 작업을 확장하고 도메인 유닛 편집을 선택합니다.
5. 도메인 단위 이름과 설명을 변경한 다음 변경 사항 저장을 선택합니다.

Amazon에서 도메인 유닛 삭제 DataZone

Amazon 에서 DataZone도메인 단위를 사용하면 특정 사업부 및 팀에서 자산 및 기타 도메인 엔터티를 구성할 수 있습니다. 자세한 내용은 Amazon DataZone 용어 및 개념 단원을 참조하십시오.

도메인 단위를 편집하려면

1. DataZone 데이터 포털을 사용하여 Amazon 데이터 포털로 이동URL하고 SSO 또는 AWS 자격 증명을 사용하여 로그인합니다. Amazon DataZone 관리자인 경우 Amazon DataZone 도메인이 생성된 AWS 계정의 https://console.aws.amazon.com/datazone에서 Amazon DataZone 콘솔에 액세스URL하여 데이터 포털을 얻을 수 있습니다.
2. 도메인 보기를 선택하고 도메인 단위를 삭제할 도메인을 선택합니다.
3. 도메인 세부 정보 페이지에서 도메인 단위 탭으로 이동하여 삭제할 도메인 단위를 선택합니다.
4. 작업을 확장하고 도메인 유닛 삭제를 선택합니다.
5. 도메인 단위 삭제 팝업 창에서 도메인 단위 삭제를 선택하여 삭제를 확인합니다.

Amazon에서 도메인 유닛 소유자 관리 DataZone

Amazon 에서 DataZone도메인 단위를 사용하면 특정 사업부 및 팀에서 자산 및 기타 도메인 엔터티를 구성할 수 있습니다. 자세한 내용은 Amazon DataZone 용어 및 개념 단원을 참조하십시오.

Amazon DataZone 관리 콘솔을 통해 최상위 도메인 유닛에 소유자를 추가하려면 다음 단계를 완료합니다.

1. https://console.aws.amazon.com/datazone의 Amazon DataZone 콘솔로 이동하여 계정 자격 증명으로 로그인합니다.
2. 도메인 보기를 선택하고 DataZone 도메인 단위 소유자를 추가할 Amazon 도메인을 선택합니다.
3. 도메인 세부 정보 페이지에서 도메인 루트 소유자 탭으로 이동합니다.
4. 추가를 선택한 다음 도메인 유닛 소유자 추가 팝업 창에서 도메인 유닛 소유자를 만들 사용자를 지정합니다. 소유자 추가를 선택합니다.

Amazon DataZone Data Portal을 통해 도메인 유닛 소유자를 추가하려면 다음 절차를 완료합니다.

1. DataZone 데이터 포털을 사용하여 Amazon 데이터 포털로 이동URL하고 SSO 또는 AWS 자격 증명을 사용하여 로그인합니다. Amazon DataZone 관리자인 경우 Amazon DataZone 도메인이 생

성된 AWS 계정의 https://console.aws.amazon.com/datazone에서 Amazon DataZone 콘솔에 액세스URL하여 데이터 포털을 얻을 수 있습니다.

2. 도메인 보기를 선택하고 도메인 소유자를 추가할 도메인과 도메인 단위를 선택합니다.
3. 도메인 단위 세부 정보 페이지에서 소유자 탭을 선택한 다음 소유자 추가를 선택합니다.
4. 도메인 유닛 소유자 추가 팝업 창에서 도메인 유닛 소유자를 만들 사용자를 지정한 다음 소유자 추가를 선택합니다.

Amazon DataZone 도메인 유닛 내의 사용자 및 그룹에 권한 부여 정책 할당

Amazon 에서 DataZone도메인 단위를 사용하면 특정 사업부 및 팀에서 자산 및 기타 도메인 엔터티를 구성할 수 있습니다. 자세한 내용은 Amazon DataZone 용어 및 개념 단원을 참조하십시오.

Amazon DataZone 도메인 유닛에서 사용자 및 그룹에 다음 권한 부여 정책을 할당하여 이 도메인 유닛 내에서 다양한 권한 부여 권한을 부여할 수 있습니다.

- 도메인 단위 생성 정책
- 프로젝트 생성 정책
- 프로젝트 멤버십 정책
- 도메인 유닛 소유권 가정 정책
- 프로젝트 소유권 가정 정책

도메인 유닛 내의 사용자 및 그룹에 권한 부여 정책을 할당하려면 다음 절차를 완료합니다.

1. Amazon DataZone 데이터 포털로 이동하여 Single Sign-On(SSO) 또는 자격 AWS 증명을 사용하여 URL 로그인합니다. Amazon DataZone 관리자인 경우 https://console.aws.amazon.com/datazone의 Amazon DataZone 콘솔로 이동하여 도메인이 생성된 AWS 계정 로 로그인한 다음 데이터 포털 열기를 선택합니다.
2. 도메인 보기를 선택하고 권한 부여 정책을 할당할 도메인과 도메인 단위를 선택합니다.
3. 도메인 단위 세부 정보 페이지에서 사용자/그룹에 할당할 권한 부여 정책을 선택한 다음 사용자 추가를 선택합니다.
4. 사용자 추가 팝업 창에서 다음 중 하나를 수행합니다.

    - 선택한 사용자 및 그룹 을 선택하고 선택한 권한 부여 정책을 할당할 사용자 및 그룹을 지정한 다음 사용자 추가 를 선택합니다.

- 모든 사용자를 선택한 다음 사용자 추가를 선택합니다.
- 모든 그룹을 선택한 다음 사용자 추가를 선택합니다.

5. 선택한 사용자에 대해 선택한 권한 부여 정책의 캐스케이드 권한을 활성화하거나 비활성화할 수도 있습니다. 이렇게 하려면 캐스케이드 권한을 활성화하려는 사용자(들)를 선택한 다음 작업 을 확장하고 캐스케이드 권한을 true로 설정을 선택합니다. 선택한 사용자는 이 도메인 단위의 모든 하위 도메인 단위에서 이 정책에 따라 부여된 권한을 갖습니다. 또는 캐스케이드 권한을 비활성화할 사용자(들)를 선택한 다음 작업 을 확장하고 캐스케이드 권한 설정을 false 로 설정할 수 있습니다.

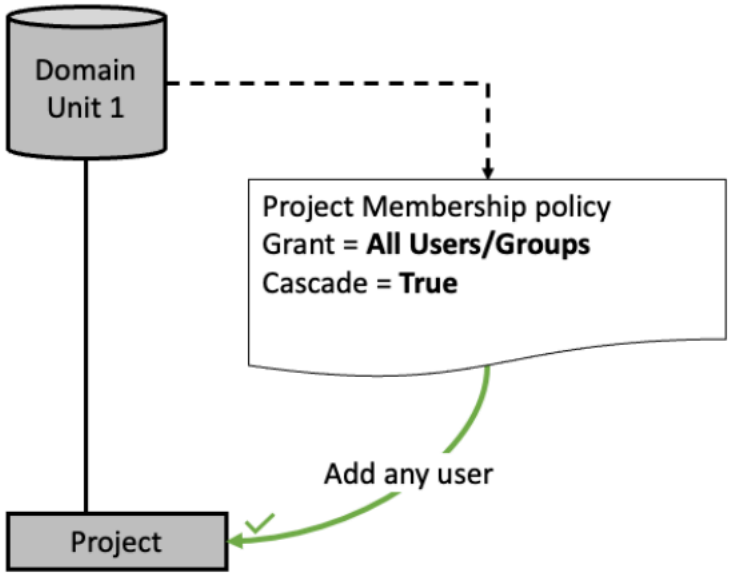
도메인 단위 계층의 프로젝트 멤버십 정책

프로젝트 멤버십 정책은 도메인 유닛 내의 프로젝트에 멤버로 추가할 수 있는 개인 또는 그룹을 정의합니다. 이 주제에서는 계층 구조에서 개별 도메인 유닛 및 도메인 유닛과 관련된 정책의 영향에 대한 시나리오를 설명합니다.

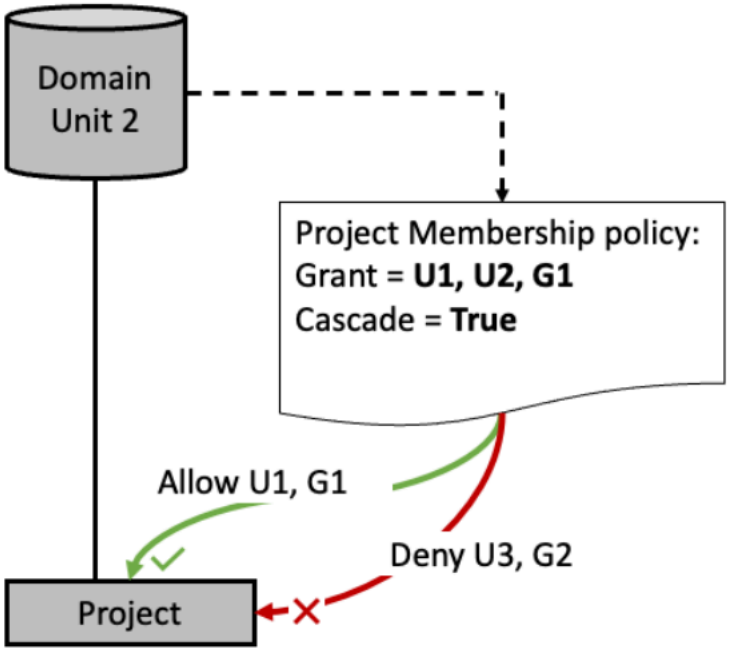
이 주제에 사용되는 몇 가지 개념을 기록하는 것이 중요합니다.

- 멤버십 풀 - 프로젝트 멤버십 정책을 통해 액세스 권한이 부여된 보안 주체(사용자 또는 그룹)는 프로젝트 멤버십 풀의 일부로 간주됩니다. 예를 들어 도메인 유닛에 대한 정책DU1이 사용자 U1 및 U2와 Single Sign-On(SSO) 그룹 G1에 부여된 경우 의 프로젝트 멤버십 풀DU1은 {U1, U2, G1}로 구성됩니다.
- 캐스캐이드 - 도메인 유닛 계층 구조를 통해 연결된 모든 하위 도메인 유닛에 권한을 전달하는 기능입니다.
- 권한 부여 - 사용자 또는 그룹이 작업을 수행할 수 있는 권한입니다.

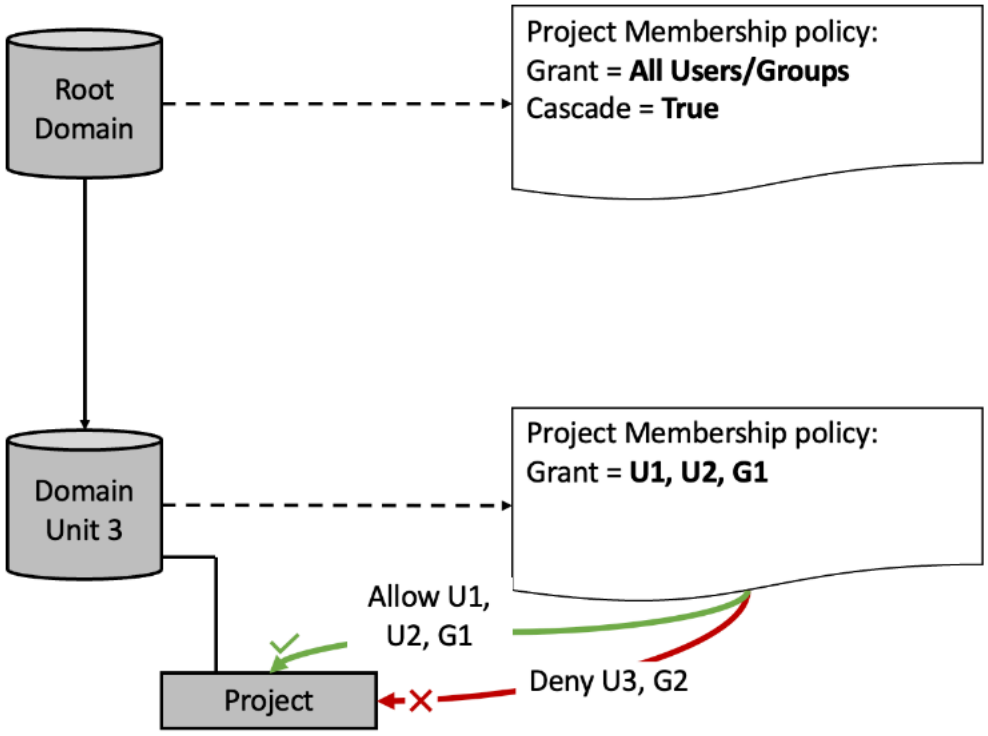
시나리오 1 - 멤버십 풀이 {모든 사용자/그룹}으로 구성되므로 도메인 유닛 1의 모든 사용자 또는 그룹을 프로젝트에 추가할 수 있습니다.



시나리오 2 - 사용자 {U1, G1}은 도메인 유닛 2의 멤버십 풀에 속하므로 도메인 유닛 2의 프로젝트에 추가할 수 있습니다. {U3, G2} 사용자는 멤버십 풀에 속하지 않으므로 프로젝트에 추가할 수 없습니다.

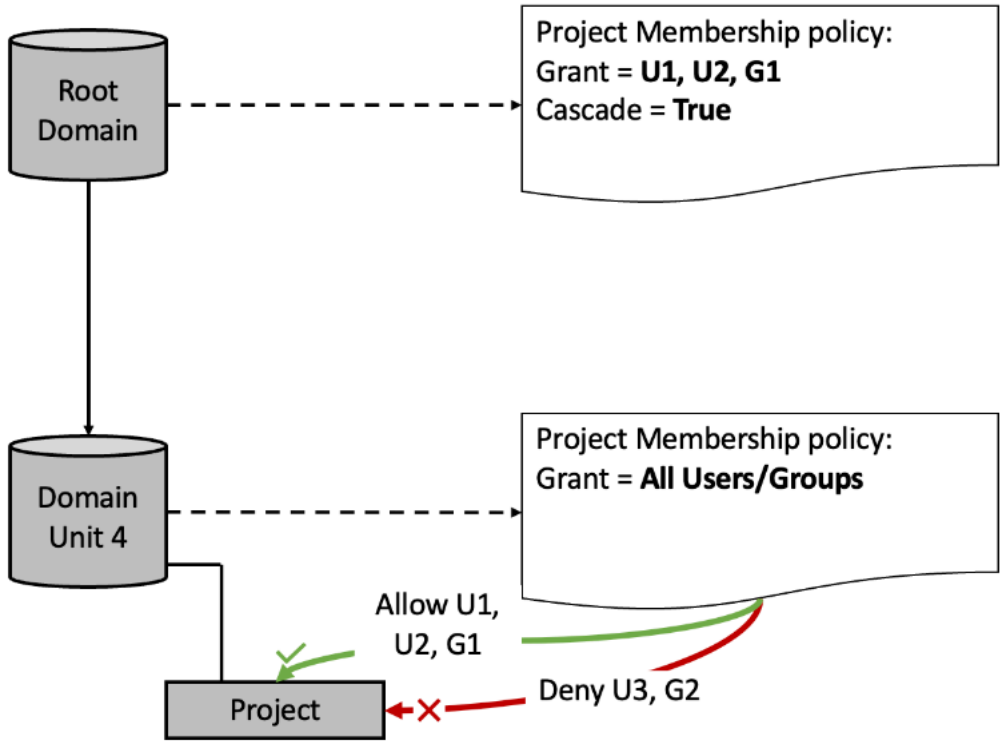


시나리오 3 - 멤버십 풀 교차: 서로 다른 도메인 유닛 계층 구조 수준에 멤버십 풀이 있는 경우 모든 멤버십 풀에 있는 사용자 및 그룹만 프로젝트에 추가할 수 있습니다.



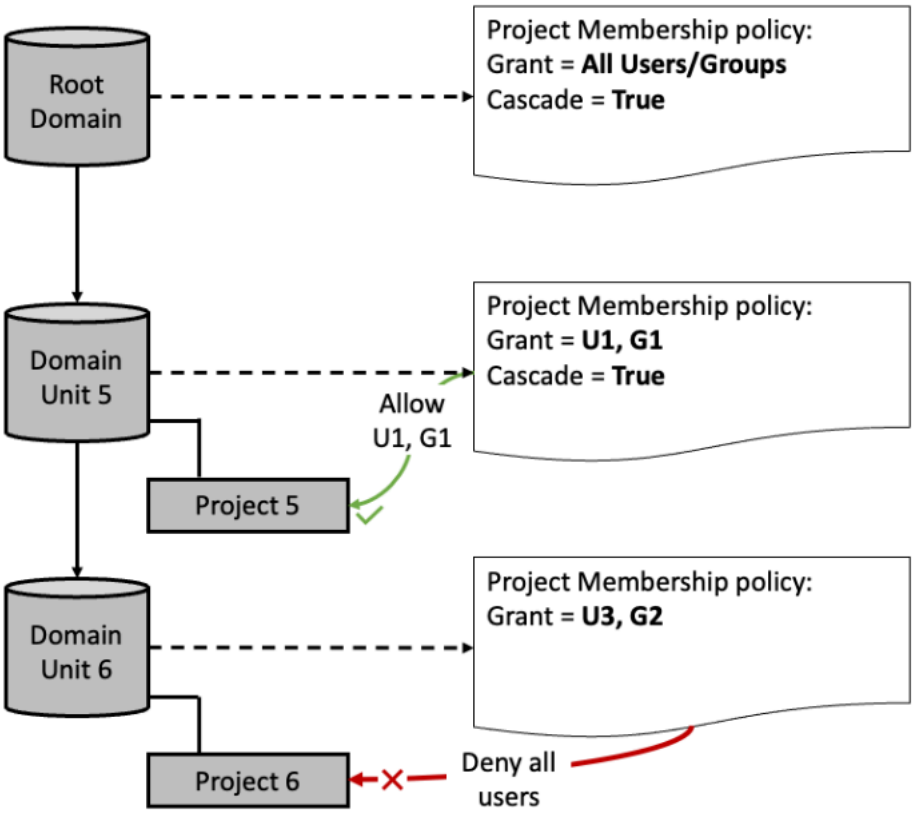
- 두 멤버십 풀에서 사용자의 교차점은 {U1, U2, G1}입니다.
- 사용자 {U1, U2, G1}는 도메인 유닛 3에서 프로젝트에 추가할 수 있습니다.
- 모든 사용자 및 모든 그룹이 루트 도메인 단위 수준에서 멤버십 풀에 있더라도 {U3, G2} 사용자는 도메인 단위 3의 프로젝트에 추가할 수 없습니다.

시나리오 4 - 멤버십 풀 교차: 서로 다른 도메인 유닛 계층 구조 수준에 멤버십 풀이 있는 경우 모든 멤버십 풀에 있는 사용자 및 그룹만 프로젝트에 추가할 수 있습니다.

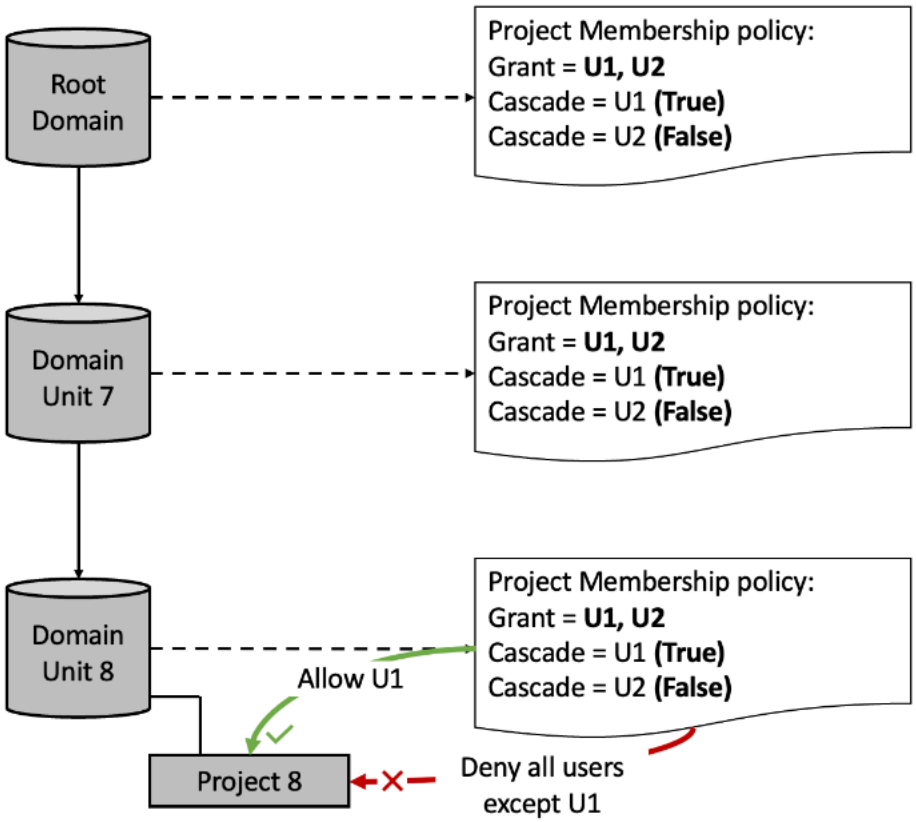


- 두 멤버십 풀에서 사용자의 교차점은 {U1, U2, G1}입니다.
- 도메인 유닛 4의 멤버십 풀은 {모든 사용자 / 그룹}이지만 멤버십 풀은 루트 도메인 {U1, U2, G1}의 멤버십 풀 이상으로 확장할 수 없습니다.
- 모든 사용자 및 모든 그룹이 도메인 유닛 4의 멤버십 풀에 있더라도 {U3, G2} 사용자는 도메인 유닛 4의 프로젝트에 추가할 수 없습니다.

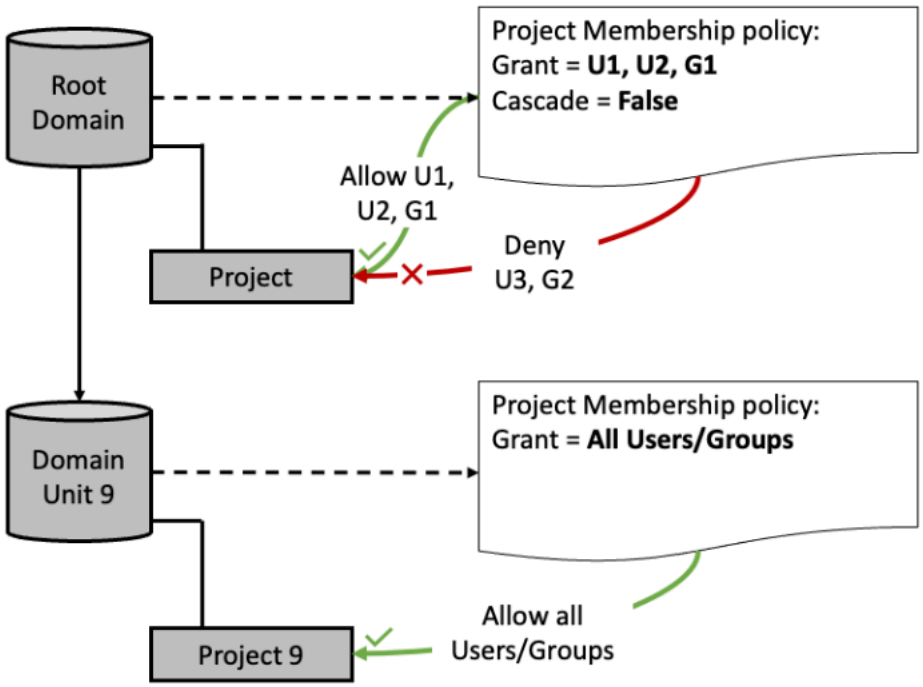
시나리오 5 - 사용자 {U1, G1}은 루트 도메인과 도메인 유닛 5 간의 멤버십 풀 교차점의 일부로 프로젝트 5에 추가할 수 있습니다. 세 멤버십 풀의 교차점이 비어 있으므로 프로젝트 6에 사용자/그룹을 추가할 수 없습니다.



시나리오 6 - 세 멤버십 풀 모두의 교차점은 사용자 {U1}만 프로젝트 8에 추가할 수 있음을 의미합니다. 도메인 유닛 8에 대한 의 교차 풀은 {U1}, {U1}, {U1, U2}이며, 세 개에 걸쳐 {U1}만 공통입니다.



시나리오 7 - {U1, U2, G1} 사용자는 루트 도메인의 멤버십 풀의 일부로 루트 도메인의 프로젝트에 추가할 수 있습니다. 멤버십 풀이 {All Users/Groups}로 구성되므로 도메인 유닛 9 아래의 프로젝트에 모든 사용자 또는 그룹을 추가할 수 있습니다. 그 위의 루트 도메인에서 캐스케이드가 false로 설정되어 있기 때문입니다.



Amazon DataZone 도메인 유닛 내의 프로젝트에 권한 부여 정책 할당

Amazon 에서 DataZone도메인 단위를 사용하면 특정 사업부 및 팀에서 자산 및 기타 도메인 엔터티를 구성할 수 있습니다. 자세한 내용은 Amazon DataZone 용어 및 개념 단원을 참조하십시오.

Amazon DataZone 도메인 유닛에서는 프로젝트에 다음 권한 부여 정책을 할당하여 이 도메인 유닛 내에서 이러한 개체에 다양한 권한 부여 권한을 부여할 수 있습니다.

- 용어 생성 정책
- 메타데이터 양식 생성 정책
- 사용자 지정 자산 유형 생성 정책

도메인 유닛 내의 프로젝트에 권한 부여 정책을 할당하려면 다음 절차를 완료합니다.

1. Amazon DataZone 데이터 포털로 이동하여 Single Sign-On(SSO) 또는 자격 AWS 증명을 사용하여 URL 로그인합니다. Amazon DataZone 관리자인 경우 https://console.aws.amazon.com/datazone의 Amazon DataZone 콘솔로 이동하여 도메인이 생성된 AWS 계정 로 로그인한 다음 데이터 포털 열기를 선택합니다.

2. 도메인 보기를 선택하고 권한 부여 정책을 할당할 도메인과 도메인 단위를 선택합니다.
3. 도메인 단위 세부 정보 페이지에서 프로젝트에 할당할 권한 부여 정책을 선택한 다음 프로젝트 추가를 선택합니다.
4. 프로젝트 추가 팝업 창에서 다음 중 하나를 수행합니다.
   - 도메인 유닛에서 선택한 프로젝트를 선택하고 선택한 권한 부여 정책을 할당할 프로젝트를 지정한 다음 프로젝트 추가를 선택합니다.
   - 도메인 단위의 모든 프로젝트를 선택합니다.
5. 허용된 지정 에서 소유자 , 기여자 또는 관리자 를 프로젝트 멤버가 이 정책을 사용해야 하는 지정으로 지정합니다.
6. 프로젝트 및 지정 추가를 선택합니다.

Amazon DataZone 블루프린트 구성 내에서 권한 부여 정책 할당

Amazon에서 권한 부여 메커니즘을 사용하는 또 다른 방법은 Amazon DataZone 청사진 구성 내의 프로젝트 및 도메인 유닛 소유자에게 권한 부여 정책을 적용하는 DataZone 것입니다.

Amazon DataZone 블루프린트 구성은 사용자 워크플로 게시 및 구독에 사용되는 리소스를 생성하고 구성하는 데 필요한 정보를 캡슐화하는 엔터티입니다. 이 정보에는 AWS 계정 번호 및 리전, CFN 템플릿, VPCs 및 서브넷과 같은 계정 수준 파라미터가 포함되며 데이터베이스 연결 정보 및 보안 인증 정보도 포함될 수 있습니다. 비용을 제어하고 보안을 개선하기 위해 데이터 플랫폼 사용자는 이러한 청사진을 사용하고 환경을 생성할 수 있는 사용자를 제어할 수 있는 기능이 필요합니다.

특정 청사진 구성 내에서 프로젝트 및 도메인 유닛 소유자에게 다음과 같은 권한 부여 정책을 할당할 수 있습니다.

- 이 청사진을 사용하여 환경 프로파일 생성 - 이 정책은 Amazon DataZone 프로젝트에 할당할 수 있으며 이 청사진을 사용하여 환경 프로파일을 생성할 수 있는 권한을 부여합니다.
- 이 청사진을 사용하여 환경 프로파일을 생성할 수 있는 권한을 부여합니다. 이 정책은 도메인 유닛 소유자에게 할당할 수 있으며 이 청사진을 사용하여 환경 프로파일을 생성할 수 있는 권한을 프로젝트에 부여합니다.

Amazon DataZone 데이터 포털을 통해 블루프린트 구성의 프로젝트에 이 블루프린트 권한 부여 정책을 사용하여 환경 프로파일 생성 할당

1. Amazon DataZone 데이터 포털로 이동하여 Single Sign-On(SSO) 또는 자격 AWS 증명을 사용하여 URL 로그인합니다. Amazon DataZone 관리자인 경우 https://console.aws.amazon.com/

datazone의 Amazon DataZone 콘솔로 이동하여 도메인이 생성된 AWS 계정 로 로그인한 다음 데이터 포털 열기를 선택합니다.

2. 데이터 포털에서 작업하려는 블루프린트가 활성화된 도메인을 선택한 다음 블루프린트 구성 탭으로 이동합니다.
3. 블루프린트 구성 탭에서 작업할 활성화된 블루프린트를 선택한 다음 이 블루프린트의 세부 정보 페이지에서 권한 부여 정책 탭으로 이동한 다음 이 블루프린트 권한 부여 정책을 사용하여 환경 프로파일 생성을 선택합니다.
4. 이 청사진 권한 부여 정책 세부 정보를 사용하여 환경 프로파일 생성 페이지에서 작업을 확장하고 프로젝트 추가를 선택합니다.
5. 프로젝트 추가 팝업 창에서 다음 중 하나를 수행할 수 있습니다.

   - 도메인 단위의 모든 프로젝트 옵션을 선택한 다음 이 청사진을 사용하여 환경 프로파일을 생성하도록 권한을 부여하려는 프로젝트가 포함된 도메인 단위를 검색하고 지정한 다음 프로젝트 추가를 선택합니다.
   - 도메인 단위에서 선택한 프로젝트를 선택한 다음 이 정책을 할당할 프로젝트가 포함된 도메인 단위를 검색하고 지정한 다음 이 정책을 할당할 프로젝트를 검색하고 선택한 다음 프로젝트 추가를 선택합니다.

Amazon DataZone 관리 콘솔을 통해 블루프린트 구성에서 도메인 유닛 소유자에게 이 블루프린트 권한 부여 정책을 사용하여 환경 프로파일을 생성할 수 있는 권한 부여를 할당합니다.

1. https://console.aws.amazon.com/datazone의 Amazon DataZone 콘솔로 이동하여 계정 자격 증명으로 로그인합니다.
2. Amazon DataZone 콘솔에서 작업하려는 블루프린트가 활성화된 도메인을 선택한 다음 블루프린트 탭으로 이동합니다.
3. 청사진 탭에서 작업할 활성화된 청사진을 선택한 다음 청사진의 세부 정보 페이지에서 위임된 권한 탭으로 이동합니다.
4. 위임된 권한 탭에서 이 청사진 정책을 사용하여 환경 프로파일을 생성할 수 있는 권한 부여를 할당하려는 소유자에게 도메인 단위를 검색하고 선택한 다음 위임된 권한 추가를 선택합니다.

아마존 DataZone 빌트인 블루프린트

환경을 만드는 블루프린트는 환경이 속한 프로젝트의 구성원이 Amazon DataZone 카탈로그의 자산을 사용할 때 사용할 수 있는 도구 및 서비스를 정의합니다. DataZoneAmazon의 현재 릴리스에는 다음과 같은 기본 제공 블루프린트가 있습니다.

- 데이터 레이크 블루프린트
- 데이터 웨어하우스 청사진
- 아마존 SageMaker 블루프린트

다음 절차의 단계를 실행하여 DataZone Amazon에서 기본 블루프린트를 활성화할 수 있습니다.

- 에서 빌트인 블루프린트를 활성화합니다. AWS Amazon DataZone 도메인을 소유한 계정
- SageMaker Amazon을 신뢰할 수 있는 서비스로 추가 AWS Amazon DataZone 도메인을 소유한 계정

에서 빌트인 블루프린트를 활성화합니다. AWS Amazon DataZone 도메인을 소유한 계정

환경을 만드는 블루프린트는 환경이 속한 프로젝트의 구성원이 Amazon DataZone 카탈로그의 자산을 사용할 때 사용할 수 있는 도구 및 서비스를 정의합니다.

Amazon의 현재 릴리스에는 데이터 레이크 청사진 DataZone, 데이터 웨어하우스 청사진, Amazon 청사진 등 여러 가지 기본 제공 청사진이 있습니다. SageMaker

- 데이터 레이크 블루프린트에는 일련의 서비스를 시작하고 구성하기 위한 정의가 포함되어 있습니다 (AWS Glue, AWS Lake Formation, Amazon Athena) 에서 아마존 DataZone 카탈로그에 데이터 레이크 자산을 게시하고 사용할 수 있습니다.
- 데이터 웨어하우스 블루프린트에는 아마존 카탈로그에 Amazon Redshift 자산을 게시하고 사용하기 위한 서비스 세트 (Amazon Redshift) 를 시작하고 구성하는 데 대한 정의가 포함되어 있습니다. DataZone
- Amazon SageMaker Blueprint에는 Amazon DataZone 카탈로그에 Amazon SageMaker 자산을 게시하고 사용하기 위한 서비스 세트 (Amazon SageMaker Studio) 를 시작하고 구성하는 데 대한 정의가 포함되어 있습니다.

자세한 내용은 Amazon DataZone 용어 및 개념 단원을 참조하십시오.

Amazon DataZone 도메인을 생성할 때 기본 데이터 레이크와 기본 데이터 웨어하우스 내장 블루프린트를 도메인 생성 프로세스의 일부로 자동으로 활성화하는 빠른 설정을 선택할 수 있습니다. 또한 Quick Setup은 이러한 내장된 블루프린트를 사용하여 기본 환경 프로필과 기본 환경을 생성합니다.

Amazon DataZone 도메인을 생성할 때 빠른 설정을 선택하지 않는 경우 아래 절차에 따라 사용 가능한 내장 블루프린트를 활성화할 수 있습니다. AWS 이 Amazon DataZone 도메인이 있는 계정 기본 제공 블루프린트를 사용하여 이 도메인에서 환경 프로필 및 환경을 만들려면 먼저 이러한 빌트인 블루프린트를 활성화해야 합니다.

Amazon DataZone 관리 콘솔을 통해 Amazon DataZone 도메인에 내장된 블루프린트를 활성화하려면 관리자 권한이 있는 계정에서 IAM 역할을 수임해야 합니다. Amazon DataZone 관리 콘솔을 사용하는 데 필요한 IAM 권한을 구성합니다.최소 권한을 얻으려면

Amazon DataZone 도메인에서 빌트인 블루프린트를 활성화하세요

1. https://console.aws.amazon.com/datazone의 Amazon DataZone 콘솔로 이동하여 계정 자격 증명으로 로그인합니다.
2. View domain (도메인 보기) 를 선택하고 하나 이상의 빌트인 블루프린트를 활성화하려는 도메인을 선택합니다.
3. 도메인 세부정보 페이지에서 블루프린트 탭으로 이동합니다.
4. 블루프린트 목록에서, DefaultDataLake또는 Amazon SageMaker 블루프린트를 DefaultDataWarehouse선택합니다.
5. 선택한 블루프린트의 세부 정보 페이지에서 이 계정에서 활성화를 선택합니다.
6. 권한 및 리소스 페이지에서 다음을 지정합니다.

   - DefaultDataLake블루프린트를 활성화하는 경우, Glue Manage Access 역할에 대해 Amazon에 테이블에 대한 액세스를 수집하고 관리할 DataZone 권한을 부여하는 신규 또는 기존 서비스 역할을 지정하세요. AWS Glue 및 AWS 레이크 포메이션.
   - DefaultDataWarehouse블루프린트를 활성화하는 경우 Redshift 액세스 관리 역할의 경우 DataZone Amazon Redshift의 데이터 공유, 테이블 및 뷰에 대한 액세스를 수집하고 관리할 권한을 Amazon에 부여하는 신규 또는 기존 서비스 역할을 지정하십시오.
   - Amazon SageMaker 블루프린트를 활성화하는 경우 액세스 SageMaker 관리 역할에 Amazon SageMaker 데이터를 카탈로그에 게시할 DataZone 권한을 Amazon에 부여하는 새 서비스 역할 또는 기존 서비스 역할을 지정하십시오. 또한 Amazon에 카탈로그에 SageMaker 게시된 자산에

대한 액세스 DataZone 권한을 부여하거나 액세스 권한을 취소할 수 있는 권한을 Amazon에 부여합니다.

> **Important**
>
> Amazon SageMaker 블루프린트를 활성화하면 Amazon은 다음 Amazon IAM 역할이 현재 계정 및 지역에 DataZone 존재하는지 DataZone 확인합니다. 이러한 역할이 없는 경우 Amazon은 DataZone 해당 역할을 자동으로 생성합니다.
>
> - AmazonDataZoneGlueAccess- <region>-< > domainId
> - AmazonDataZoneRedshiftAccess- - <region>-< > domainId

- 프로비저닝 역할의 경우 Amazon에 다음을 사용하여 환경 리소스를 생성 및 구성할 수 있는 DataZone 권한을 부여하는 새 서비스 역할 또는 기존 서비스 역할을 지정합니다. AWS CloudFormation 환경 계정 및 지역에서.
- Amazon SageMaker 블루프린트를 활성화하는 경우, SageMaker-Glue 데이터 소스용 Amazon S3 버킷의 경우, 다음 데이터 소스의 모든 SageMaker 환경에서 사용할 Amazon S3 버킷을 지정하십시오. AWS 계정. 지정하는 버킷 접두사는 다음 중 하나여야 합니다.
  - 아마존-데이터존*
  - 데이터존 세이지메이커*
  - 세이지메이커 - 데이터존*
  - DataZone- 세이지메이커*
  - 세이지메이커- * DataZone
  - DataZone-SageMaker*
  - SageMaker-DataZone*

7. 블루프린트 활성화를 선택합니다.

선택한 블루프린트를 활성화하면 계정의 블루프린트를 사용하여 환경 프로필을 생성할 수 있는 프로젝트를 제어할 수 있습니다. 블루프린트 구성에 관리 프로젝트를 할당하여 이 작업을 수행할 수 있습니다.

> **Important**
>
> 기본적으로 환경 블루프린트에는 관리 프로젝트가 지정되어 있지 않습니다. 즉, 모든 Amazon DataZone 사용자가 환경 블루프린트에 대한 프로필을 생성할 수 있습니다. 따라서 더 강력한 거버넌스를 보장하기 위해 항상 환경 청사진에 대한 관리 프로젝트를 지정하는 것이 좋습니다.

활성화된 블루프린트에 대한 프로젝트 관리를 지정하세요.

1. https://console.aws.amazon.com/datazone의 Amazon DataZone 콘솔로 이동하여 계정 자격 증명으로 로그인합니다.
2. View Domains를 선택한 다음 선택한 블루프린트에 대한 관리 프로젝트를 추가할 도메인을 선택합니다.
3. 블루프린트 탭을 선택한 다음 작업하려는 블루프린트를 선택합니다.
4. 기본적으로 도메인 내의 모든 프로젝트는 계정의 DefaultDataLake or 또는 또는 DefaultDataWareshouse Amazon SageMaker 블루프린트를 사용하여 환경 프로필을 생성할 수 있습니다. 하지만 블루프린트에 관리 프로젝트를 할당하여 이를 제한할 수 있습니다. 관리 프로젝트를 추가하려면 관리 프로젝트 선택을 선택한 다음 드롭다운 메뉴에서 관리 프로젝트로 추가할 프로젝트를 선택한 다음 관리 프로젝트 선택을 선택합니다.

DefaultDataWarehouse 블루프린트를 활성화한 후에는 AWS 계정에서 파라미터 세트를 블루프린트 구성에 추가할 수 있습니다. 파라미터 세트는 Amazon이 Amazon DataZone Redshift 클러스터에 연결하는 데 필요한 키와 값의 그룹이며 데이터 웨어하우스 환경을 생성하는 데 사용됩니다. 이러한 파라미터에는 Amazon Redshift 클러스터의 이름, 데이터베이스 및 AWS 클러스터에 대한 자격 증명을 보관하는 암호입니다.

DefaultDataWarehouse 블루프린트에 파라미터 세트 추가

1. https://console.aws.amazon.com/datazone의 Amazon DataZone 콘솔로 이동하여 계정 자격 증명으로 로그인합니다.
2. View domain (도메인 보기) 를 선택한 다음 파라미터 세트를 추가할 도메인을 선택합니다.
3. 블루프린트 탭을 선택한 다음 블루프린트를 선택하여 DefaultDataWareshouse 블루프린트 세부 정보 페이지를 엽니다.
4. 블루프린트 디테일 페이지의 파라미터 세트 탭에서 파라미터 세트 생성을 선택합니다.
   - 파라미터 세트의 이름을 입력합니다.

- 파라미터 세트에 대한 설명을 제공할 수도 있습니다.
- 리전 선택
- Amazon Redshift 클러스터 또는 Amazon Redshift 서버리스를 선택합니다.
- 다음을 선택합니다. AWS 선택한 Amazon Redshift 클러스터 또는 Amazon Redshift 서버리스 워크그룹에 대한 자격 증명을 ARN 보유하는 암호입니다. The AWS 비밀번호에 `AmazonDataZoneDomain : [Domain_ID]` 태그를 지정해야 파라미터 세트 내에서 사용할 수 있습니다.
  - 기존 파일이 없는 경우 AWS 비밀번호인 경우 새로 만들기를 선택하여 새 비밀번호를 생성할 수도 있습니다. AWS 시크릿. 그러면 암호 이름, 사용자 이름 및 암호를 제공할 수 있는 대화 상자가 열립니다. 새로 만들기를 선택하면 AWS 비밀, Amazon은 새로운 비밀을 DataZone 만듭니다. AWS Secrets Manager 서비스를 통해 매개 변수 세트를 생성하려는 도메인으로 암호에 태그가 지정되었는지 확인합니다.
- 위 단계에서 Amazon Redshift 클러스터를 선택했다면 이제 드롭다운에서 클러스터를 선택하십시오. 위 단계에서 Amazon Redshift 워크그룹을 선택했다면 이제 드롭다운에서 워크그룹을 선택하십시오.
- 선택한 Amazon Redshift 클러스터 또는 Amazon Redshift 서버리스 워크그룹 내의 데이터베이스 이름을 입력합니다.
- 파라미터 세트 생성을 선택합니다.

> **Note**
>
> DefaultDataWarehouse블루프린트에 파라미터 세트를 10개까지만 추가할 수 있습니다.

Amazon SageMaker 블루프린트를 활성화하면 AWS 계정에서 블루프린트 구성에 파라미터 세트를 추가할 수 있습니다. 파라미터 세트는 Amazon이 DataZone Amazon에 연결하는 데 필요한 키와 값의 SageMaker 그룹이며, 이는 sagemaker 환경을 만드는 데 사용됩니다.

Amazon SageMaker 블루프린트에 파라미터 세트 추가

1. https://console.aws.amazon.com/datazone의 Amazon DataZone 콘솔로 이동하여 계정 자격 증명으로 로그인합니다.
2. View domain (도메인 보기) 를 선택한 다음 파라미터 세트를 추가하려는 활성화된 블루프린트가 들어 있는 도메인을 선택합니다.

3. Blueprints 탭을 선택한 다음 Amazon SageMaker 청사진을 선택하여 청사진의 세부 정보 페이지를 엽니다.
4. 블루프린트 세부 정보 페이지의 파라미터 세트 탭에서 파라미터 세트 생성을 선택하고 다음을 지정합니다.

   - 파라미터 세트의 이름을 입력합니다.
   - 파라미터 세트에 대한 설명을 제공할 수도 있습니다.
   - Amazon SageMaker 도메인 인증 유형을 지정합니다. 둘 중 하나를 IAM 선택하거나 IAM ID 센터 (SSO) 를 선택할 수 있습니다.
   - 다음을 지정하십시오. AWS 지역.
   - 다음을 지정하십시오. AWS KMS데이터 암호화를 위한 키. 기존 키를 선택하거나 새 키를 만들 수 있습니다.
   - 환경 매개변수에서 다음을 지정합니다.
     - VPCID - Amazon SageMaker 환경에서 사용하는 ID입니다. VPC 기존 항목을 지정하거나 새로 만들 수 VPC 있습니다.
     - 서브넷 - 내 특정 리소스의 IP 주소 범위를 위한 하나 이상의 IDs 서브넷 VPC
     - 네트워크 액세스 - VPC전용 또는 공용 인터넷만을 선택합니다.
     - 보안 그룹 - 서브넷을 구성할 VPC 때 사용할 보안 그룹입니다.
   - 데이터 소스 매개변수에서 다음 중 하나를 선택합니다.
     - AWS Glue 전용
     - AWS Glue + 아마존 Redshift 서버리스. 이 옵션을 선택하는 경우 다음을 지정하십시오.
       - 다음을 지정하십시오. AWS 선택한 Amazon Redshift 클러스터의 자격 증명을 보관하는 ARN 암호입니다. The AWS 비밀번호에 `AmazonDataZoneDomain : [Domain_ID]` 태그를 지정해야 파라미터 세트 내에서 사용할 수 있습니다.

         기존 파일이 없는 경우 AWS 비밀번호인 경우 새로 만들기를 선택하여 새 비밀번호를 생성할 수도 있습니다. AWS 시크릿. 그러면 암호 이름, 사용자 이름 및 암호를 제공할 수 있는 대화 상자가 열립니다. 새로 만들기를 선택하면 AWS 비밀, Amazon은 새로운 비밀을 DataZone 만듭니다. AWS Secrets Manager 서비스를 통해 매개 변수 세트를 생성하려는 도메인으로 암호에 태그가 지정되었는지 확인합니다.
       - 환경을 생성할 때 사용할 Amazon Redshift 워크그룹을 지정하십시오.
       - 환경을 생성할 때 사용하려는 데이터베이스 (선택한 작업 그룹 내) 의 이름을 지정합니다.
     - AWS Glue only + 아마존 Redshift 클러스터

- 다음을 지정하십시오. AWS 선택한 Amazon Redshift 클러스터의 자격 증명을 보관하는 ARN 암호입니다. The AWS 비밀번호에 `AmazonDataZoneDomain : [Domain_ID]` 태그를 지정해야 파라미터 세트 내에서 사용할 수 있습니다.

  기존 파일이 없는 경우 AWS 비밀번호인 경우 새로 만들기를 선택하여 새 비밀번호를 생성할 수도 있습니다. AWS 시크릿. 그러면 암호 이름, 사용자 이름 및 암호를 제공할 수 있는 대화 상자가 열립니다. 새로 만들기를 선택하면 AWS 비밀, Amazon은 새로운 비밀을 DataZone 만듭니다. AWS Secrets Manager 서비스를 통해 매개 변수 세트를 생성하려는 도메인으로 암호에 태그가 지정되었는지 확인합니다.
- 환경을 생성할 때 사용하려는 Amazon Redshift 클러스터를 지정하십시오.
- 환경을 만들 때 사용하려는 데이터베이스 (선택한 클러스터 내) 의 이름을 지정합니다.

5. 파라미터 세트 생성을 선택합니다.

SageMaker Amazon을 신뢰할 수 있는 서비스로 추가 AWS Amazon DataZone 도메인을 소유한 계정

Amazon SageMaker 블루프린트를 활성화한 경우 Amazon DataZone 내에 신뢰할 수 있는 서비스 중 SageMaker 하나로 추가해야 합니다. 이렇게 하려면 다음 절차를 완료하십시오.

1. https://console.aws.amazon.com/datazone의 Amazon DataZone 콘솔로 이동하여 계정 자격 증명으로 로그인합니다.
2. View domain (도메인 보기) 를 선택한 다음 활성화된 블루프린트가 들어 있는 도메인을 선택합니다. SageMaker
3. 신뢰할 수 있는 서비스를 선택한 다음 SageMakerAmazon을 선택한 다음 활성화를 선택합니다.

Amazon DataZone 사용자 지정 AWS 서비스 청사진

Amazon 에서 DataZone사용자 지정 AWS 서비스 청사진을 사용하면 조직에서 이미 설정한 기존 AWS Identity and Access Management(IAM) 역할 및 AWS 서비스를 DataZone 사용하도록 Amazon을 구성하여 리소스 사용량과 비용을 최적화할 수 있습니다.

Amazon DataZone 환경이 생성되는 청사진은 환경이 속한 프로젝트의 구성원이 Amazon DataZone 카탈로그의 자산으로 작업할 때 사용할 수 있는 도구 및 서비스 구성원을 정의합니다. Amazon 의 현재 릴리스에는 다음과 같은 기본 블루프린트 DataZone가 있습니다.

- 데이터 레이크 청사진
- 데이터 웨어하우스 청사진
- Amazon SageMaker 청사진

Amazon DataZone 사용자 지정 AWS 서비스 청사진을 사용하면 조직에서 현재 사용 중인 모든 AWS 서비스에 사용자 지정된 환경 및 프로젝트를 생성할 수 있습니다. 사용자 지정 블루프린트를 사용하면 기존 IAM 역할을 사용하여 인프라 설정 전반의 거버넌스를 개선하고 비즈니스 이니셔티브 DataZone 에서 협업하도록 구성하여 기존 데이터 파이프라인에 Amazon을 포함할 수 있습니다.

주제

- 사용자 지정 AWS 서비스 청사진 활성화
- 사용자 지정 AWS 서비스 청사진을 사용하여 환경 생성
- 사용자 지정 AWS 서비스 환경에서 작업 생성
- 사용자 지정 AWS 서비스 환경에 프로젝트 멤버 추가
- AWS 서비스 환경에서 데이터 소스 구성
- AWS 서비스 환경에서 구독 대상 구성

사용자 지정 AWS 서비스 청사진 활성화

도메인에서 사용자 지정 AWS 서비스 청사진을 활성화하려면 다음 절차를 완료하세요.

1. AWS 관리 콘솔에 로그인하고 https://console.aws.amazon.com/datazone 에서 Amazon DataZone 관리 콘솔을 엽니다.
2. 도메인 보기를 선택하고 사용자 지정 AWS 서비스 청사진을 활성화하려는 도메인을 선택합니다.

3. 청사진 탭을 선택한 다음 사용 가능한 청사진 목록에서 AWS 서비스 청사진을 선택하고 활성화를 선택합니다.

사용자 지정 AWS 서비스 청사진을 사용하여 환경 생성

사용자 지정 AWS 서비스 청사진을 사용하여 환경을 생성하려면 다음 절차를 완료합니다.

1. AWS 관리 콘솔에 로그인하고 https://console.aws.amazon.com/datazone 에서 Amazon DataZone 관리 콘솔을 엽니다.
2. 도메인 보기를 선택하고 사용자 지정 AWS 서비스 블루프린트가 활성화된 도메인을 선택합니다.
3. 블루프린트 탭을 선택한 다음 활성화된 AWS 서비스 블루핀을 선택하고 환경 생성을 선택합니다.
4. 환경 생성 페이지에서 다음을 지정한 다음 환경 생성을 선택합니다.

   - 이름 - 환경의 이름을 지정합니다.
   - 설명 - 환경에 대한 설명을 지정합니다.
   - 프로젝트 - 환경에 대한 신규 또는 기존 소유 프로젝트를 지정합니다. 프로젝트를 사용하면 사용자 그룹이 Amazon 에서 자산을 검색, 게시, 구독 및 소비할 수 있습니다 DataZone. 이 환경은 지정된 프로젝트의 모든 구성원이 사용할 수 있습니다. 모든 환경은 사용자가 환경에 액세스할 수 있는 프로젝트에서 소유합니다.
   - 환경 역할 - 이 환경에서 Amazon S3 및 AWS Glue와 같은 기존 AWS 서비스 및 리소스에 대한 DataZone 액세스 권한을 Amazon에 부여하는 기존 IAM 역할을 지정합니다. Amazon S3

     > **Note**
     >
     > Amazon DataZone 은 이 역할을 프로비저닝하지 않습니다. 이 환경에서 활성화하려는 기존 AWS 서비스 및 리소스에 대한 권한이 있는 기존 IAM 역할이 있어야 합니다.
     > 이 IAM 역할에 최소 필수 권한이 있는지 확인합니다. 즉, 이 환경에서 활성화하려는 서비스 및 리소스에 대한 액세스 권한만 AWS 제공하도록 범위가 축소되어 있는지 확인합니다.
     > AWS 정책 생성기를 사용하여 요구 사항에 맞는 정책을 빌드하고 사용하려는 사용자 지정 IAM 역할에 연결할 수 있습니다.
     > 규칙을 따르AmazonDataZone려면 역할이 로 시작하는지 확인합니다. 필수는 아니지만 권장됩니다. IAM 관리자가 AmazonDataZoneFullAccess 정책을 사용하는 경우 패스 역할 확인 검증이 있으므로 이 규칙을 따라야 합니다.
     > 사용자 지정 역할을 생성할 때 해당 역할이 신뢰 정책을 datazone.amazonaws.com 신뢰하는지 확인합니다.

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

- AWS 리전 - 이 환경을 생성할 AWS 리전을 지정합니다.

사용자 지정 AWS 서비스 환경에서 작업 생성

다음 절차를 완료하여 사용자 지정 AWS 서비스 환경에서 작업을 생성합니다. 사용자 지정 AWS 서비스 환경에서 작업을 생성하면 Amazon DataZone 데이터 포털에 대한 딥 링크를 이 환경에서 사용할 수 있는 분석 도구에 추가합니다.

1. AWS 관리 콘솔에 로그인하고 https://console.aws.amazon.com/datazone 에서 Amazon DataZone 관리 콘솔을 엽니다.
2. 도메인 보기를 선택하고 사용자 지정 AWS 서비스 블루프린트가 활성화된 도메인을 선택합니다.
3. 블루프린트 탭을 선택한 다음 활성화된 AWS 서비스 블루핀을 선택한 다음 작업을 추가할 서비스 환경을 선택합니다 AWS .
4. AWS 콘솔 링크 페이지에서 인기 링크 또는 사용자 지정 링크 섹션에서 AWS 링크(작업)를 선택하여 Amazon S3 버킷, Amazon Athena 작업 그룹, AWS Glue 작업 또는 Amazon DataZone 데이터 포털을 통해 이 환경의 다른 사용자 지정 AWS 콘솔 리소스에 대한 딥 링크를 활성화합니다. AWS

5. 이 환경의 요약 섹션에서 데이터 포털 링크를 사용하여 데이터 포털에서 이 환경으로 이동하는 경우 분석 도구 섹션에서 추가한 딥 링크를 볼 수 있습니다.

사용자 지정 AWS 서비스 환경에 프로젝트 멤버 추가

다음 절차를 완료하여 AWS 서비스 환경에 프로젝트 멤버를 추가합니다.

1. AWS 관리 콘솔에 로그인하고 https://console.aws.amazon.com/datazone 에서 Amazon DataZone 관리 콘솔을 엽니다.
2. 프로젝트 탭을 선택한 다음 멤버를 추가할 AWS 서비스 환경 내의 프로젝트를 선택합니다.
3. 추가를 선택한 다음 멤버 추가 페이지에서 IAM 사용자, 사용자 또는 SSO 그룹 에서 멤버SSO를 찾아 추가합니다. 소유자 , 기여자 , 소비자 , 관리인 또는 뷰어 의 할당된 프로젝트 역할을 지정합니다. 멤버 찾기 및 추가가 완료되면 멤버 추가를 선택합니다.

AWS 서비스 환경에서 데이터 소스 구성

AWS 서비스 환경에서 데이터 소스를 구성하려면 다음 절차를 완료합니다.

1. AWS 관리 콘솔에 로그인하고 https://console.aws.amazon.com/datazone 에서 Amazon DataZone 관리 콘솔을 엽니다.
2. 블루프린트 탭을 선택한 다음 사용자 지정 AWS 서비스 블루프린트를 선택합니다.
3. 생성된 환경 에서 데이터 소스를 구성하려는 AWS 서비스 환경을 선택합니다.
4. 데이터 소스 탭을 선택하고 추가를 선택한 다음 다음을 지정한 다음 추가를 선택합니다.

   - 이름 - 데이터 소스 이름입니다.
   - 리소스 - AWS Glue 또는 Amazon Redshift를 선택합니다.
     - AWS Glue에 리소스 데이터베이스를 지정합니다.
     - Amazon Redshift의 경우 클러스터 또는 서버리스 를 선택한 다음, 환경을 생성할 때 사용하려는 새 보안 암호 또는 기존 AWS 보안 암호, 클러스터 또는 서버리스 작업 그룹, 환경을 생성할 때 사용하려는 데이터베이스, 지정된 데이터베이스 내의 스키마를 포함하여 Redshift 보안 인증 을 지정합니다.
   - 권한 - Amazon에 AWS Lake Formation(AWS Glue용)의 테이블에 대한 액세스를 수집 및 관리할 수 있는 DataZone 권한을 부여하거나 Amazon에 Amazon Redshift의 테이블에 대한 액세스를 수집 및 관리할 수 DataZone 있는 권한을 부여하는 액세스 관리 역할을 지정합니다.

- 데이터 소비에 사용 - Amazon 에서 DataZone프로젝트 멤버는 Amazon DataZone이 프로젝트에서 구독한 데이터에 대한 액세스를 활성화하는 데 사용하는 구독 대상을 통해 데이터를 소비할 수 있습니다. 이 데이터 소스를 구독 대상으로 추가할지 여부를 지정합니다.

AWS 서비스 환경에서 구독 대상 구성

서비스 환경에서 구독 대상 AWS 을 구성하려면 다음 절차를 완료합니다.

1. AWS 관리 콘솔에 로그인하고 https://console.aws.amazon.com/datazone 에서 Amazon DataZone 관리 콘솔을 엽니다.
2. 블루프린트 탭을 선택한 다음 서비스 블루프린트를 AWS 선택합니다.
3. 생성된 환경 에서 구독 대상을 구성하려는 AWS 서비스 환경을 선택합니다.
4. 구독 대상 탭을 선택하고 추가를 선택한 다음 다음을 지정한 다음 추가를 선택합니다.

   - 이름 - 구독 대상 이름입니다.
   - 리소스 - AWS Glue 또는 Amazon Redshift를 선택합니다.
     - AWS Glue에 리소스 데이터베이스를 지정합니다.
     - Amazon Redshift에서 클러스터 또는 서버리스 를 선택한 다음, 환경을 생성할 때 사용하려는 새 또는 기존 AWS 보안 암호, 클러스터 또는 서버리스 작업 그룹, 환경을 생성할 때 사용하려는 데이터베이스, 지정된 데이터베이스 내의 스키마를 포함하여 Redshift 보안 인증 을 지정합니다.
   - 권한 - Amazon에 AWS Lake Formation(AWS Glue용)의 테이블에 대한 액세스를 수집 및 관리할 수 있는 DataZone 권한을 부여하거나 Amazon에 Amazon Redshift의 테이블에 대한 액세스를 수집 및 관리할 수 DataZone 있는 권한을 부여하는 액세스 관리 역할을 지정합니다.
   - 데이터 소비에 사용 - Amazon 에서는 메타데이터 수집을 허용하는 데이터 소스를 통해 데이터 카탈로그에 데이터를 게시할 DataZone수 있습니다. 이 구독 대상을 데이터 소스로 추가할지 여부를 지정합니다.

Amazon의 연결된 계정 DataZone

AWS 계정을 Amazon DataZone 도메인과 연결하면 도메인 사용자가 이러한 AWS 계정의 데이터를 게시하고 사용할 수 있습니다. 계정 연결을 설정하는 세 단계가 있습니다.

- 먼저 연결을 요청하여 도메인을 원하는 AWS 계정과 공유합니다. Amazon은 AWS 계정이 도메인 계정과 다른 경우 AWS Resource Access Manager(RAM)를 DataZone 사용합니다 AWS . 계정 연결은 Amazon DataZone 도메인에서만 시작할 수 있습니다.
- 둘째, 계정 소유자가 연결 요청을 수락하도록 합니다.
- 셋째, 계정 소유자가 원하는 환경 청사진을 활성화하도록 합니다. 블루프린트를 활성화하면 계정 소유자는 도메인의 사용자에게 AWS Glue 데이터베이스 및 Amazon Redshift 클러스터와 같은 계정의 리소스를 생성하고 액세스하는 데 필요한 IAM 역할 및 리소스 구성을 제공합니다.

다음 단계를 완료하여 계정을 Amazon 에 연결합니다 DataZone.

- 1단계 - 다른 AWS 계정과의 연결 요청
- 2단계 - Amazon DataZone 도메인에서 계정 연결 요청을 수락하고 환경 청사진 활성화
- 3단계 - 연결된 AWS 계정에서 환경 청사진 활성화

다른 AWS 계정과의 연결 요청

> **Note**
>
> 다른 AWS 계정으로 연결 요청을 보내면 AWS Resource Access Manager()를 사용하여 다른 AWS 계정과 도메인을 공유합니다RAM. 입력한 계정 ID의 정확성을 확인해야 합니다.

Amazon DataZone 도메인에 대해 Amazon DataZone 콘솔의 다른 AWS 계정과의 연결을 요청하려면 관리 권한이 있는 계정에서 IAM 역할을 맡아야 합니다. Amazon DataZone 관리 콘솔을 사용하는 데 필요한 IAM 권한을 구성합니다.를 사용하여 계정 연결을 요청하는 데 필요한 최소 권한을 얻어야 합니다.

다른 AWS 계정과의 연결을 요청하려면 다음 절차를 완료하세요.

1. AWS 관리 콘솔에 로그인하고 https://console.aws.amazon.com/datazone 에서 Amazon DataZone 관리 콘솔을 엽니다.
2. 도메인 보기를 선택하고 목록에서 도메인 이름을 선택합니다. 이름은 하이퍼링크입니다.

3. 연결된 계정 탭으로 스크롤하여 연결 요청 을 선택합니다.
4. 연결을 요청하려는 계정IDs의 를 입력합니다. 계정 목록에 만족하면 연결 요청 을 IDs선택합니다.
5. RAM 정책에서 계정 연결 RAM 정책을 지정합니다. 연결된 계정이 Amazon DataZone APIs을 실행하고 데이터 포털에 액세스할 수 `AWSRAMPermissionDataZonePortalReadWrite` 있도록 할 것인지 또는 `AWSRAMPermissionDataZoneDefault`를 선택할 수 있습니다. 여기서 연결된 계정은 Amazon DataZone APIs만 실행하도록 허용하고 데이터 포털 액세스는 제공하지 않습니다. DataZone 그런 다음 Amazon은 입력된 계정 ID(들)를 보안 주체로 사용하여 계정을 대신하여 AWS Resource Access Manager에 리소스 공유를 생성합니다.
6. 요청을 수락하려면 다른 AWS 계정(들)의 소유자에게 알려야 합니다. 초대장은 칠(7) 일 후에 만료됩니다.

고객 관리형 KMS 키에 대한 계정 액세스 권한 제공

Amazon DataZone 도메인 및 메타데이터는 도메인 생성 중에 KMS소유하고 제공하는 Key AWS Management Service()의 고객 관리형 키(선택 사항) AWS또는 (기본적으로) 에서 보유한 키를 사용하여 암호화됩니다. 도메인이 고객 관리형 키로 암호화된 경우 아래 절차에 따라 연결된 계정에 KMS 키를 사용할 수 있는 권한을 부여합니다.

1. AWS 관리 콘솔에 로그인하고 에서 KMS 콘솔을 엽니다https://console.aws.amazon.com/kms/.
2. 해당 계정에서 직접 생성하고 관리하는 키를 보려면 탐색 창에서 고객 관리형 키를 선택합니다.
3. 해당 계정에서 직접 생성하고 관리하는 키를 보려면 탐색 창에서 고객 관리형 키를 선택합니다.
4. KMS 키 목록에서 검사하려는 키의 별칭 또는 KMS 키 ID를 선택합니다.
5. 외부 AWS 계정이 KMS 키를 사용하도록 허용하거나 허용하지 않으려면 페이지의 기타 AWS 계정 섹션에 있는 제어를 사용합니다. IAM 이러한 계정의 보안 주체(적절한 KMS 권한 있음)는 암호화, 복호화, 재암호화 및 데이터 KMS 키 생성과 같은 암호화 작업에 키를 사용할 수 있습니다.

Amazon DataZone 도메인에서 계정 연결 요청을 수락하고 환경 청사진 활성화

Amazon DataZone 관리 콘솔에서 Amazon DataZone 도메인과의 연결을 수락하려면 관리 권한이 있는 계정에서 IAM 역할을 맡아야 합니다. Amazon DataZone 관리 콘솔을 사용하는 데 필요한 IAM 권한을 구성합니다.를 사용하여 최소 권한을 얻어야 합니다.

Amazon DataZone 도메인과의 연결을 수락하려면 다음을 완료하세요.

1. AWS 관리 콘솔에 로그인하고 https://console.aws.amazon.com/datazone 에서 Amazon DataZone 관리 콘솔을 엽니다.
2. 요청 보기를 선택하고 목록에서 초대 도메인을 선택합니다. 초대 상태는 요청됨 이어야 합니다. 요청 검토를 선택합니다.
3. 둘 다 또는 상자 중 하나를 선택하여 기본 데이터 레이크 및/또는 데이터 웨어하우스 환경 청사진을 활성화할지 여부를 선택합니다. 나중에 이 작업을 수행할 수 있습니다.
   - 데이터 레이크 환경 청사진을 사용하면 도메인 사용자가 AWS Glue, Amazon S3 및 Amazon Athena 리소스를 생성하고 관리하여 데이터 레이크에서 게시하고 사용할 수 있습니다.
   - 데이터 웨어하우스 환경 청사진을 사용하면 도메인 사용자가 Amazon Redshift 리소스를 생성하고 관리하여 데이터 웨어하우스에서 게시하고 사용할 수 있습니다.
4. 기본 환경 청사진 중 하나 또는 둘 다를 선택하는 경우 다음 권한 및 리소스를 구성합니다.
   - 액세스 관리 IAM 역할은 도메인 사용자가 AWS Glue 및 Amazon DataZone Redshift와 같은 테이블에 대한 액세스를 수집 및 관리할 수 있는 권한을 Amazon에 제공합니다. Amazon에서 새 IAM 역할을 DataZone 생성하고 사용하도록 선택하거나 기존 IAM 역할 목록에서 선택할 수 있습니다.
   - 프로비저닝 IAM 역할은 Amazon DataZone에 도메인 사용자가 AWS Glue 데이터베이스와 같은 환경 리소스를 생성하고 구성할 수 있는 권한을 제공합니다. Amazon에서 새 IAM 역할을 DataZone 생성하고 사용하도록 선택하거나 기존 IAM 역할 목록에서 선택할 수 있습니다.
   - Data Lake용 Amazon S3 버킷은 도메인 사용자가 데이터 레이크 데이터를 저장할 때 Amazon 이 사용할 버킷 또는 경로 DataZone 입니다. Amazon에서 선택한 기본 버킷을 사용하거나 경로 문자열을 입력하여 DataZone 기존 Amazon S3 경로를 선택할 수 있습니다. 자체 Amazon S3 경로를 선택하는 경우 IAM 정책을 업데이트하여 Amazon에 사용할 수 DataZone 있는 권한을 제공해야 합니다.
5. 구성에 만족하면 연결 수락 및 구성을 선택합니다.

연결된 AWS 계정에서 환경 청사진 활성화

Amazon DataZone 관리 콘솔에서 환경 청사진을 활성화하려면 관리 권한이 있는 계정에서 IAM 역할을 맡아야 합니다. Amazon DataZone 관리 콘솔을 사용하는 데 필요한 IAM 권한을 구성합니다.에서 최소 권한을 얻어야 합니다.

연결된 도메인에서 청사진을 활성화하려면 다음을 완료하세요.

1. AWS 관리 콘솔에 로그인하고 https://console.aws.amazon.com/datazone 에서 Amazon DataZone 관리 콘솔을 엽니다.
2. 왼쪽 탐색 패널을 열고 연결된 도메인 을 선택합니다.
3. 환경 청사진을 활성화할 도메인을 선택합니다.
4. 블루프린트 목록에서 DefaultDataLake 또는 DefaultDataWarehouse, 또는 Amazon SageMaker 또는 Custom AWS Service 블루프린트를 선택합니다.

> **Note**
>
> 사용자 지정 AWS 서비스 청사진을 활성화하는 경우 액세스 관리 역할을 지정할 필요가 없습니다. 사용자 지정 AWS 서비스 블루 핀에 대한 권한 및 권한 부여 메커니즘은 이 블루프린트를 사용하여 환경을 생성할 때 처리됩니다. 자세한 내용은 사용자 지정 AWS 서비스 청사진을 사용하여 환경 생성 단원을 참조하십시오.

5. 선택한 청사진의 세부 정보 페이지에서 이 계정에서 활성화를 선택합니다.
6. 권한 및 리소스 페이지에서 다음을 지정합니다.

- DefaultDataLake 블루프린트를 활성화하는 경우 Glue Manage Access 역할 에 Glue and AWS Lake Formation의 AWS 테이블에 대한 액세스를 수집 및 관리할 수 있는 DataZone 권한을 Amazon에 부여하는 새 또는 기존 서비스 역할을 지정합니다.
- DefaultDataWarehouse 블루프린트를 활성화하는 경우 Redshift 액세스 관리 역할 에 Amazon Redshift에서 데이터 공유, 테이블 및 뷰에 대한 액세스를 수집 및 관리할 수 있는 DataZone 권한을 Amazon에 부여하는 새 또는 기존 서비스 역할을 지정합니다.
- Amazon SageMaker 청사진을 활성화하는 경우 SageMaker 액세스 관리 역할 에 Amazon SageMaker 데이터를 카탈로그에 게시할 수 있는 DataZone 권한을 Amazon에 부여하는 새 또는 기존 서비스 역할을 지정합니다. 또한 카탈로그에 게시 SageMaker 된 Amazon 자산에 대한 액세스 권한을 부여하거나 취소할 수 있는 DataZone 권한을 Amazon에 부여합니다.

> **Important**
>
> Amazon SageMaker 청사진을 활성화할 때 Amazon은 Amazon에 대한 다음 IAM 역할이 현재 계정 및 리전에 DataZone 존재하는지 DataZone 확인합니다. 이러한 역할이 없는 경우 Amazon은 해당 역할을 DataZone 자동으로 생성합니다.
>
> - AmazonDataZoneGlueAccess-<region>-<domainId>
> - AmazonDataZoneRedshiftAccess-<region>-<domainId>

- 프로비저닝 역할 의 경우 환경 계정 및 리전 AWS CloudFormation 에서 를 사용하여 환경 리소스를 생성하고 구성할 수 있는 DataZone 권한을 Amazon에 부여하는 새 또는 기존 서비스 역할을 지정합니다.
- Amazon SageMaker 청사진을 활성화하는 경우 SageMaker-Glue 데이터 소스용 Amazon S3 버킷 에 계정의 모든 SageMaker 환경에서 사용할 Amazon S3 버킷을 AWS 지정합니다. 지정하는 버킷 접두사는 다음 중 하나여야 합니다.
  - amazon-datazone*
  - datazone-sagemaker*
  - sagemaker-datazone*
  - DataZone-Sagemaker*
  - Sagemaker-DataZone*
  - DataZone-SageMaker*
  - SageMaker-DataZone*

7. 블루프린트 활성화를 선택합니다.

선택한 청사진(들)을 활성화하면 계정에서 청사진(들)을 사용하여 환경 프로파일을 생성할 수 있는 프로젝트를 제어할 수 있습니다. 블루프린트의 구성에 프로젝트 관리를 할당하여 이 작업을 수행할 수 있습니다.

활성화된 DefaultDataLake 또는 DefaultDataWarehouse 블루프린트에서 프로젝트 관리 지정

1. https://console.aws.amazon.com/datazone의 Amazon DataZone 콘솔로 이동하여 계정 자격 증명으로 로그인합니다.
2. 왼쪽 탐색 패널을 열고 연결된 도메인을 선택한 다음 프로젝트 관리를 추가할 도메인을 선택합니다.
3. 블루프린트 탭을 선택한 다음 DefaultDataLake 또는 DefaultDataWareshouse 블루프린트를 선택합니다.
4. 기본적으로 도메인 내의 모든 프로젝트는 계정의 DefaultDataLake 또는 DefaultDataWareshouse 청사진을 사용하여 환경 프로파일을 생성할 수 있습니다. 그러나 블루프린트에 프로젝트 관리를 할당하여 이를 제한할 수 있습니다. 프로젝트 관리를 추가하려면 프로젝트 관리 선택()을 선택한 다음 드롭다운 메뉴에서 프로젝트 관리로 추가하려는 프로젝트를 선택한 다음 프로젝트 관리 선택을 선택합니다.

AWS 계정에서 DefaultDataWarehouse 블루프린트를 활성화하면 블루프린트 구성에 파라미터 세트를 추가할 수 있습니다. 파라미터 세트는 Amazon Redshift 클러스터에 대한 연결을 설정하는 DataZone 데 필요한 키 및 값의 그룹으로, 데이터 웨어하우스 환경을 생성하는 데 사용됩니다. 이러한 파라미터에는 Amazon Redshift 클러스터의 이름, 데이터베이스 및 클러스터에 보안 인증을 보유한 AWS 보안 암호가 포함됩니다.

> **Important**
>
> 기본적으로 환경 청사진에 대한 관리 프로젝트는 에 지정되지 않습니다. 즉, 모든 Amazon DataZone 사용자가 환경 청사진에 대한 프로필을 생성할 수 있습니다. 따라서 더 강력한 거버넌스를 보장하기 위해 항상 환경 청사진에 대한 프로젝트 관리를 지정하는 것이 좋습니다.

블루프린트에 DefaultDataWarehouse 파라미터 세트 추가

1. https://console.aws.amazon.com/datazone의 Amazon DataZone 콘솔로 이동하여 계정 자격 증명으로 로그인합니다.
2. 왼쪽 탐색 패널을 열고 연결된 도메인을 선택한 다음 파라미터 세트를 추가할 도메인을 선택합니다.
3. 청사진 탭을 선택한 다음 DefaultDataWareshouse 청사진을 선택하여 청사진 세부 정보 페이지를 엽니다.
4. 블루프린트 세부 정보 페이지의 파라미터 세트 탭에서 파라미터 세트 생성을 선택합니다.
   - 파라미터 세트의 이름을 입력합니다.
   - 선택적으로 파라미터 세트에 대한 설명을 제공합니다.
   - 리전 선택
   - Amazon Redshift 클러스터 또는 Amazon Redshift Serverless를 선택합니다.
   - 선택한 Amazon Redshift 클러스터 또는 Amazon Redshift Serverless 작업 그룹에 보안 인증 정보를 ARN 보유한 AWS 보안 암호를 선택합니다. 파라미터 세트 내에서 사용할 수 있으려면 AWS 보안 암호에 `AmazonDataZoneDomain : [Domain_ID]` 태그가 지정되어야 합니다.
     - 기존 AWS 보안 암호가 없는 경우 새 보안 암호 생성 을 선택하여 새 보안 AWS 암호를 생성할 수도 있습니다. 그러면 보안 암호, 사용자 이름 및 암호를 입력할 수 있는 대화 상자가 열립니다. 새 AWS 보안 암호 생성 을 선택하면 Amazon은 AWS Secrets Manager 서비스에서 새 보안 암호를 DataZone 생성하고 보안 암호에 파라미터 세트를 생성하려는 도메인으로 태그가 지정되도록 합니다.
   - Amazon Redshift 클러스터 또는 Amazon Redshift Serverless 작업 그룹을 선택합니다.

- 선택한 Amazon Redshift 클러스터 또는 Amazon Redshift Serverless 작업 그룹 내에 데이터베이스 이름을 입력합니다.
- 파라미터 세트 생성을 선택합니다.

> **Note**
>
> DefaultDataWarehouse 블루프린트에는 최대 10개의 파라미터 세트만 추가할 수 있습니다.

AWS 계정에서 Amazon SageMaker 블루프린트를 활성화하면 블루프린트 구성에 파라미터 세트를 추가할 수 있습니다. 파라미터 세트는 Amazon이 Amazon에 대한 연결을 설정하는 DataZone 데 필요한 키 SageMaker 및 값의 그룹으로, 사이지메이커 환경을 생성하는 데 사용됩니다.

Amazon SageMaker 블루프린트에 파라미터 세트 추가

1. https://console.aws.amazon.com/datazone의 Amazon DataZone 콘솔로 이동하여 계정 자격 증명으로 로그인합니다.
2. 도메인 보기를 선택한 다음 파라미터 세트를 추가하려는 활성화된 청사진이 포함된 도메인을 선택합니다.
3. 청사진 탭을 선택한 다음 Amazon SageMaker 청사진을 선택하여 청사진의 세부 정보 페이지를 엽니다.
4. 블루프린트 세부 정보 페이지의 파라미터 세트 탭에서 파라미터 세트 생성을 선택한 다음 다음을 지정합니다.
   - 파라미터 세트의 이름을 입력합니다.
   - 선택적으로 파라미터 세트에 대한 설명을 제공합니다.
   - Amazon SageMaker 도메인 인증 유형을 지정합니다. IAM 또는 IAM Identity Center()를 선택할 수 있습니다SSO.
   - AWS 리전을 지정합니다.
   - 데이터 암호화를 AWS KMS 위한 키를 지정합니다. 기존 키를 선택하거나 새 키를 생성할 수 있습니다.
   - 환경 파라미터 에서 다음을 지정합니다.
     - VPC ID - Amazon SageMaker 환경VPC의 에 사용 중인 ID입니다. 기존 를 지정하거나 새 를 생성할 수 있습니다VPC.
     - 서브넷 - 내의 특정 리소스IDs에 대한 IP 주소 범위에 대해 하나 이상입니다VPC.

- 네트워크 액세스 - VPC 전용 또는 퍼블릭 인터넷 전용을 선택합니다.
- 보안 그룹 - VPC 및 서브넷을 구성할 때 사용할 보안 그룹입니다.

- 데이터 소스 파라미터에서 다음 중 하나를 선택합니다.
  - AWS Glue만 해당
  - AWS Glue + Amazon Redshift Serverless. 이 옵션을 선택하는 경우 다음을 지정합니다.
    - 선택한 Amazon Redshift 클러스터에 보안 인증 정보를 ARN 보유한 AWS 보안 암호를 지정합니다. 파라미터 세트 내에서 사용할 수 있으려면 AWS 보안 암호에 `AmazonDataZoneDomain : [Domain_ID]` 태그가 지정되어야 합니다.

      기존 AWS 보안 암호가 없는 경우 새 보안 암호 생성 을 선택하여 새 보안 AWS 암호를 생성할 수도 있습니다. 그러면 보안 암호, 사용자 이름 및 암호를 입력할 수 있는 대화 상자가 열립니다. 새 AWS 보안 암호 생성 을 선택하면 Amazon은 AWS Secrets Manager 서비스에서 새 보안 암호를 DataZone 생성하고 보안 암호에 파라미터 세트를 생성하려는 도메인으로 태그가 지정되도록 합니다.
    - 환경을 생성할 때 사용할 Amazon Redshift 작업 그룹을 지정합니다.
    - 환경을 생성할 때 사용할 데이터베이스의 이름(선택한 작업 그룹 내)을 지정합니다.
  - AWS Glue 전용 + Amazon Redshift 클러스터
    - 선택한 Amazon Redshift 클러스터에 보안 인증 정보를 ARN 보유한 AWS 보안 암호를 지정합니다. 파라미터 세트 내에서 사용할 수 있으려면 AWS 보안 암호에 `AmazonDataZoneDomain : [Domain_ID]` 태그가 지정되어야 합니다.

      기존 AWS 보안 암호가 없는 경우 새 보안 암호 생성 을 선택하여 새 보안 AWS 암호를 생성할 수도 있습니다. 그러면 보안 암호, 사용자 이름 및 암호를 입력할 수 있는 대화 상자가 열립니다. 새 AWS 보안 암호 생성 을 선택하면 Amazon은 AWS Secrets Manager 서비스에서 새 보안 암호를 DataZone 생성하고 보안 암호에 파라미터 세트를 생성하려는 도메인으로 태그가 지정되도록 합니다.
    - 환경을 생성할 때 사용할 Amazon Redshift 클러스터를 지정합니다.
    - 환경을 생성할 때 사용할 데이터베이스의 이름(선택한 클러스터 내)을 지정합니다.

5. 파라미터 세트 생성을 선택합니다.

연결된 AWS 계정에서 Amazon SageMaker 을 신뢰할 수 있는 서비스로 추가

Amazon SageMaker 블루프린트를 활성화한 경우 Amazon 내에서 신뢰할 수 있는 서비스 중 SageMaker 하나로 를 추가해야 합니다 DataZone. 이렇게 하려면 다음 절차를 완료합니다.

1. https://console.aws.amazon.com/datazone의 Amazon DataZone 콘솔로 이동하여 계정 자격 증명으로 로그인합니다.
2. 도메인 보기를 선택한 다음 활성화된 SageMaker 청사진이 포함된 도메인을 선택합니다.
3. 신뢰할 수 있는 서비스 를 선택한 다음 Amazon SageMaker를 선택하고 활성화 를 선택합니다.

Amazon DataZone 도메인에서 계정 연결 요청 거부

Amazon 도메인에서 Amazon DataZone DataZone 관리 콘솔의 연결 요청을 거부하려면 관리 권한이 있는 계정에서 IAM 역할을 맡아야 합니다. Amazon DataZone 관리 콘솔을 사용하는 데 필요한 IAM 권한을 구성합니다.를 사용하여 최소 권한을 얻어야 합니다.

Amazon DataZone 도메인에서 연결 요청을 거부하려면 다음을 완료하세요.

1. AWS 관리 콘솔에 로그인하고 https://console.aws.amazon.com/datazone 에서 Amazon DataZone 관리 콘솔을 엽니다.
2. 요청 보기를 선택하고 목록에서 초대 도메인을 선택합니다. 초대 상태는 요청됨이어야 합니다. 연결 거부를 선택합니다. 연결 거부를 선택하여 선택을 확인합니다.

Amazon에서 연결된 계정 제거 DataZone

Amazon DataZone 관리 콘솔에서 연결된 AWS 계정을 제거하려면 관리 권한이 있는 계정에서 IAM 역할을 맡아야 합니다. Amazon DataZone 관리 콘솔을 사용하는 데 필요한 IAM 권한을 구성합니다.를 사용하여 최소 권한을 얻어야 합니다.

도메인에서 연결된 계정을 제거하려면 다음 절차를 완료하세요.

1. AWS 관리 콘솔에 로그인하고 https://console.aws.amazon.com/datazone 에서 Amazon DataZone 관리 콘솔을 엽니다.
2. 도메인 보기를 선택하고 목록에서 도메인 이름을 선택합니다. 이름은 하이퍼링크입니다.
3. 연결된 계정 탭까지 아래로 스크롤합니다. 제거할 계정의 AWS 계정 ID를 선택합니다.

4. 연결 해제를 선택합니다. 필드에 연결 해제를 입력하고 연결 해제를 선택하여 선택을 확인합니다.
5. 이제 계정이 도메인에서 제거되어 도메인 사용자가 데이터를 게시하고 사용하는 데 사용할 수 없습니다.

Amazon DataZone 데이터 카탈로그

Amazon DataZone 비즈니스 데이터 카탈로그를 사용하여 비즈니스 컨텍스트로 조직 전반의 데이터를 카탈로그화할 수 있으므로 조직의 모든 사람이 데이터를 빠르게 찾고 이해할 수 있습니다.

Amazon DataZone 을 사용하여 데이터를 카탈로그화하려면 먼저 Amazon 에서 프로젝트 인벤토리로 데이터(자산)를 가져와야 합니다 DataZone. 프로젝트의 인벤토리를 생성하면 해당 프로젝트의 구성원만 자산을 검색할 수 있습니다. 프로젝트 인벤토리 자산은 명시적으로 게시되지 않는 한 검색/찾아보기에서 모든 도메인 사용자가 사용할 수 있는 것은 아닙니다.

프로젝트 인벤토리를 생성한 후 데이터 소유자는 비즈니스 이름(자산 및 스키마), 설명(자산 및 스키마), 읽기 권한, 용어집 용어(자산 및 스키마) 및 메타데이터 양식을 추가하거나 업데이트하여 필요한 비즈니스 메타데이터로 인벤토리 자산을 큐레이션할 수 있습니다.

Amazon DataZone 을 사용하여 데이터를 카탈로그화하는 다음 단계는 도메인 사용자가 프로젝트의 인벤토리 자산을 검색할 수 있도록 하는 것입니다. 인벤토리 자산을 Amazon DataZone 카탈로그에 게시하여 이 작업을 수행할 수 있습니다. 카탈로그에는 인벤토리 자산의 최신 버전만 게시할 수 있으며 검색 카탈로그에는 게시된 최신 버전만 활성화됩니다. 인벤토리 자산이 Amazon DataZone 카탈로그에 게시된 후 업데이트되는 경우 최신 버전이 검색 카탈로그에 포함되도록 다시 명시적으로 게시해야 합니다.

자세한 내용은 Amazon DataZone 용어 및 개념 단원을 참조하십시오.

주제

- Amazon에서 비즈니스 용어집 생성 DataZone
- Amazon에서 비즈니스 용어집 편집 DataZone
- Amazon에서 비즈니스 용어집 삭제 DataZone
- Amazon의 용어집에서 용어 생성 DataZone
- Amazon의 용어집에서 용어 편집 DataZone
- Amazon의 용어집에서 용어 삭제 DataZone
- Amazon에서 메타데이터 양식 생성 DataZone
- Amazon에서 메타데이터 양식 편집 DataZone
- Amazon에서 메타데이터 양식 삭제 DataZone
- Amazon에서 메타데이터 형식으로 필드 생성 DataZone
- Amazon의 메타데이터 양식에서 필드 편집 DataZone

- Amazon의 메타데이터 양식에서 필드 삭제 DataZone

Amazon에서 비즈니스 용어집 생성 DataZone

Amazon 에서 DataZone비즈니스 용어집은 자산(데이터)과 연결될 수 있는 비즈니스 용어(단어) 모음입니다. 데이터 분석 시 조직 전체에서 동일한 정의를 사용할 수 있도록 비즈니스 사용자를 위한 비즈니스 용어 목록과 해당 정의를 적절한 어휘로 제공합니다. 비즈니스 용어집은 카탈로그 도메인에서 생성되며 자산 및 열에 적용하여 해당 자산 또는 열의 주요 특성을 이해하는 데 도움이 될 수 있습니다. 하나 이상의 용어집 용어를 적용할 수 있습니다. 비즈니스 용어집은 비즈니스 용어집의 모든 용어를 다른 용어의 하위 목록과 연결할 수 있는 용어의 평면 목록일 수 있습니다. 자세한 내용은 Amazon DataZone 용어 및 개념 단원을 참조하십시오. Amazon DataZone 도메인에서 용어집을 생성, 편집 또는 삭제하려면 해당 도메인에 대한 올바른 권한이 있는 소유 프로젝트의 구성원이어야 합니다.

용어집을 생성하려면 다음 단계를 완료합니다.

1. DataZone 데이터 포털을 사용하여 Amazon 데이터 포털로 이동URL하고 SSO 또는 AWS 자격 증명을 사용하여 로그인합니다. Amazon DataZone 관리자인 경우 Amazon DataZone 도메인이 생성된 AWS 계정의 https://console.aws.amazon.com/datazone에서 Amazon DataZone 콘솔에 액세스URL하여 데이터 포털을 얻을 수 있습니다.
2. 검색 옆의 상단 탐색 모음에서 카탈로그 메뉴로 이동합니다.
3. Amazon DataZone Data Portal에서 용어집 을 선택한 다음 용어집 생성 을 선택합니다.
4. 용어집의 이름, 설명, 소유자를 지정한 다음 용어집 생성을 선택합니다.
5. 활성화된 토글을 선택하여 새 용어집을 활성화합니다.
6. 용어집의 세부 정보 페이지에서 읽어보기 생성을 선택하여 이 용어집에 대한 몇 가지 추가 정보를 추가할 수 있습니다.

비즈니스 용어집을 비활성화하거나 활성화하려면 다음 단계를 완료합니다.

1. DataZone 데이터 포털을 사용하여 Amazon 데이터 포털로 이동URL하고 SSO 또는 AWS 자격 증명을 사용하여 로그인합니다. Amazon DataZone 관리자인 경우 Amazon DataZone 도메인이 생성된 AWS 계정의 https://console.aws.amazon.com/datazone에서 Amazon DataZone 콘솔에 액세스URL하여 데이터 포털을 얻을 수 있습니다.
2. 검색 옆의 상단 탐색 모음에서 카탈로그 메뉴로 이동합니다.
3. Amazon DataZone Data Portal에서 용어집 을 선택하고 비활성화/활성화하려는 비즈니스 용어집을 찾습니다.

4. 용어집 세부 정보 페이지에서 활성화/비활성화 토글을 찾아 선택한 용어집을 활성화 또는 비활성화하는 데 사용합니다.

> **Note**
>
> 용어집을 비활성화하면 포함된 모든 용어도 비활성화됩니다.

Amazon에서 비즈니스 용어집 편집 DataZone

Amazon 에서 DataZone비즈니스 용어집은 자산(데이터)과 연결될 수 있는 비즈니스 용어(단어) 모음입니다. 데이터 분석 시 조직 전체에서 동일한 정의를 사용할 수 있도록 비즈니스 사용자를 위한 비즈니스 용어 목록과 해당 정의를 적절한 어휘로 제공합니다. 비즈니스 용어집은 카탈로그 도메인에서 생성되며 자산 및 열에 적용하여 해당 자산 또는 열의 주요 특성을 이해하는 데 도움이 될 수 있습니다. 하나 이상의 용어집 용어를 적용할 수 있습니다. 비즈니스 용어집은 비즈니스 용어집의 모든 용어를 다른 용어의 하위 목록과 연결할 수 있는 용어의 평면 목록일 수 있습니다. 자세한 내용은 Amazon DataZone 용어 및 개념 단원을 참조하십시오. Amazon DataZone 도메인에서 용어집을 편집하려면 해당 도메인에 대한 올바른 권한이 있는 소유 프로젝트의 구성원이어야 합니다.

비즈니스 용어집을 편집하려면 다음 단계를 완료합니다.

1. DataZone 데이터 포털을 사용하여 Amazon 데이터 포털로 이동URL하고 SSO 또는 AWS 자격 증명을 사용하여 로그인합니다. Amazon DataZone 관리자인 경우 Amazon DataZone 도메인이 생성된 AWS 계정의 https://console.aws.amazon.com/datazone에서 Amazon DataZone 콘솔에 액세스URL하여 데이터 포털을 얻을 수 있습니다.
2. 검색 옆의 상단 탐색 모음에서 카탈로그 메뉴로 이동합니다.
3. Amazon DataZone Data Portal에서 용어집 을 선택하고 편집하려는 비즈니스 용어집을 찾습니다.
4. 용어집 세부 정보 페이지에서 작업을 확장한 다음 편집을 선택하여 용어집을 편집합니다.
5. 이름, 설명을 업데이트한 다음 저장을 선택합니다.

Amazon에서 비즈니스 용어집 삭제 DataZone

Amazon 에서 DataZone비즈니스 용어집은 자산(데이터)과 연결될 수 있는 비즈니스 용어(단어) 모음입니다. 데이터 분석 시 조직 전체에서 동일한 정의를 사용할 수 있도록 비즈니스 사용자를 위한 비즈니스 용어 목록과 해당 정의를 적절한 어휘로 제공합니다. 비즈니스 용어집은 카탈로그 도메인에서 생성되며 자산 및 열에 적용하여 해당 자산 또는 열의 주요 특성을 이해하는 데 도움이 될 수 있습니

다. 하나 이상의 용어집 용어를 적용할 수 있습니다. 비즈니스 용어집은 비즈니스 용어집의 모든 용어를 다른 용어의 하위 목록과 연결할 수 있는 용어의 평면 목록일 수 있습니다. 자세한 내용은 Amazon DataZone 용어 및 개념 단원을 참조하십시오. Amazon DataZone 도메인에서 용어집을 삭제하려면 해당 도메인에 대한 올바른 권한이 있는 소유 프로젝트의 구성원이어야 합니다.

비즈니스 용어집을 삭제하려면 다음 단계를 완료합니다.

1. DataZone 데이터 포털을 사용하여 Amazon 데이터 포털로 이동URL하고 SSO 또는 AWS 자격 증명을 사용하여 로그인합니다. Amazon DataZone 관리자인 경우 Amazon DataZone 도메인이 생성된 AWS 계정의 https://console.aws.amazon.com/datazone에서 Amazon DataZone 콘솔에 액세스URL하여 데이터 포털을 얻을 수 있습니다.
2. 검색 옆의 상단 탐색 모음에서 카탈로그 메뉴로 이동합니다.
3. Amazon DataZone Data Portal에서 용어집 을 선택하고 삭제할 비즈니스 용어집을 찾습니다.
4. 용어집 세부 정보 페이지에서 작업을 확장한 다음 삭제를 선택하여 용어집을 삭제합니다.

   > **Note**
   >
   > 용어집을 삭제하려면 먼저 용어집의 기존 용어를 모두 삭제해야 합니다.

5. 삭제를 선택하여 용어집 삭제를 확인합니다.

Amazon의 용어집에서 용어 생성 DataZone

Amazon 에서 DataZone비즈니스 용어집은 자산(데이터)과 연결될 수 있는 비즈니스 용어 모음입니다. 자세한 내용은 Amazon DataZone 용어 및 개념 단원을 참조하십시오. Amazon DataZone 도메인의 용어집에서 용어를 생성, 편집 또는 삭제하려면 해당 도메인에 대한 올바른 권한이 있는 소유 프로젝트의 구성원이어야 합니다.

Amazon 에서는 DataZone비즈니스 용어집 용어에 대해 자세히 설명할 수 있습니다. 특정 용어의 컨텍스트를 설정하려면 용어 간의 관계를 지정할 수 있습니다. 용어에 대한 관계를 정의하면 관련 용어의 정의에 자동으로 추가됩니다. Amazon에서 사용할 수 있는 용어 설명에는 다음이 DataZone 포함됩니다.

- 유형 - 현재 용어가 식별된 용어의 유형임을 나타냅니다. 식별된 용어가 현재 용어의 상위 용어임을 나타냅니다.
- Has Types - 현재 용어가 표시된 특정 용어 또는 용어의 일반 용어임을 나타냅니다. 이 관계는 일반 용어의 하위 용어를 나타낼 수 있습니다.

새 용어를 생성하려면 다음 단계를 완료합니다.

1. DataZone 데이터 포털을 사용하여 Amazon 데이터 포털로 이동URL하고 SSO 또는 AWS 자격 증명을 사용하여 로그인합니다. Amazon DataZone 관리자인 경우 Amazon DataZone 도메인이 생성된 AWS 계정의 https://console.aws.amazon.com/datazone에서 Amazon DataZone 콘솔에 액세스URL하여 데이터 포털을 얻을 수 있습니다.
2. 검색 옆의 상단 탐색 모음에서 카탈로그 메뉴로 이동합니다.
3. Amazon DataZone Data Portal에서 용어집 을 선택한 다음 새 용어를 생성할 용어집을 선택합니다.
4. 용어의 이름, 설명, 소유자를 지정한 다음 용어 생성을 선택합니다.
5. 활성화된 토글을 선택하여 새 용어를 활성화합니다.
6. Readme을 추가하려면 용어 세부 정보 페이지로 이동한 다음 Readme 생성을 선택하여 이 용어집에 대한 몇 가지 추가 정보를 추가할 수 있습니다.
7. 관계를 추가하려면 용어 세부 정보 페이지로 이동하여 용어 관계 섹션을 선택한 다음 용어집 용어 추가를 선택합니다. 대화 상자에서 관계와 연결할 용어를 선택한 다음 닫기를 선택하여 적절한 관계 유형에 용어를 추가합니다. 이 관계는 관련된 모든 용어에도 추가됩니다.

Amazon의 용어집에서 용어 편집 DataZone

Amazon 에서 DataZone비즈니스 용어집은 자산(데이터)과 연결될 수 있는 비즈니스 용어 모음입니다. 자세한 내용은 Amazon DataZone 용어 및 개념 단원을 참조하십시오. Amazon DataZone 도메인의 용어집에서 용어를 생성, 편집 또는 삭제하려면 해당 도메인에 대한 올바른 권한이 있는 소유 프로젝트의 구성원이어야 합니다.

Amazon 에서는 DataZone비즈니스 용어집 용어에 대해 자세히 설명할 수 있습니다. 특정 용어의 컨텍스트를 설정하려면 용어 간의 관계를 지정할 수 있습니다. 용어에 대한 관계를 정의하면 관련 용어의 정의에 자동으로 추가됩니다. Amazon에서 사용할 수 있는 용어 설명에는 다음이 DataZone 포함됩니다.

- 유형 - 현재 용어가 식별된 용어의 유형임을 나타냅니다. 식별된 용어가 현재 용어의 상위 용어임을 나타냅니다.
- Has Types - 현재 용어가 표시된 특정 용어 또는 용어의 일반 용어임을 나타냅니다. 이 관계는 일반 용어의 하위 용어를 나타낼 수 있습니다.

용어집에서 용어를 편집하려면 다음 단계를 완료하세요.

1. DataZone 데이터 포털을 사용하여 Amazon 데이터 포털로 이동URL하고 SSO 또는 AWS 자격 증명을 사용하여 로그인합니다. Amazon DataZone 관리자인 경우 Amazon DataZone 도메인이 생성된 AWS 계정의 https://console.aws.amazon.com/datazone에서 Amazon DataZone 콘솔에 액세스URL하여 데이터 포털을 얻을 수 있습니다.
2. 검색 옆의 상단 탐색 모음에서 카탈로그 메뉴로 이동합니다.
3. Amazon DataZone Data Portal에서 용어집 을 선택하고 편집하려는 용어가 포함된 용어집을 찾은 다음 해당 용어를 선택합니다.
4. 용어 세부 정보 페이지에서 작업을 확장한 다음 편집을 선택하여 용어를 편집합니다.
5. 이름, 설명 을 업데이트한 다음 저장을 선택합니다.

Amazon의 용어집에서 용어 삭제 DataZone

Amazon 에서 DataZone비즈니스 용어집은 자산(데이터)과 연결될 수 있는 비즈니스 용어 모음입니다. 자세한 내용은 Amazon DataZone 용어 및 개념 단원을 참조하십시오. Amazon DataZone 도메인의 용어집에서 용어를 생성, 편집 또는 삭제하려면 해당 도메인에 대한 올바른 권한이 있는 소유 프로젝트의 구성원이어야 합니다.

Amazon 에서는 DataZone비즈니스 용어집 용어에 대해 자세히 설명할 수 있습니다. 특정 용어의 컨텍스트를 설정하려면 용어 간의 관계를 지정할 수 있습니다. 용어에 대한 관계를 정의하면 관련 용어의 정의에 자동으로 추가됩니다. Amazon에서 사용할 수 있는 용어 설명에는 다음이 DataZone 포함됩니다.

- 유형 - 현재 용어가 식별된 용어의 유형임을 나타냅니다. 식별된 용어가 현재 용어의 상위 용어임을 나타냅니다.
- 유형 있음 - 현재 용어가 표시된 특정 용어 또는 용어의 일반 용어임을 나타냅니다. 이 관계는 일반 용어의 하위 용어를 나타낼 수 있습니다.

용어집에서 용어를 삭제하려면 다음 단계를 완료합니다.

1. DataZone 데이터 포털을 사용하여 Amazon 데이터 포털로 이동URL하고 SSO 또는 AWS 자격 증명을 사용하여 로그인합니다. Amazon DataZone 관리자인 경우 Amazon DataZone 도메인이 생성된 AWS 계정의 https://console.aws.amazon.com/datazone에서 Amazon DataZone 콘솔에 액세스URL하여 데이터 포털을 얻을 수 있습니다.
2. 검색 옆의 상단 탐색 모음에서 카탈로그 메뉴로 이동합니다.
3. Amazon DataZone Data Portal에서 용어집 을 선택하고 삭제하려는 용어가 포함된 용어집을 찾은 다음 해당 용어를 선택합니다.

4. 용어집 세부 정보 페이지에서 작업을 확장한 다음 삭제를 선택하여 용어를 삭제합니다.
5. 삭제를 선택하여 용어 삭제를 확인합니다.

Amazon에서 메타데이터 양식 생성 DataZone

Amazon 에서 DataZone메타데이터 양식은 카탈로그의 자산 메타데이터에 대한 추가 비즈니스 컨텍스트를 보강하는 간단한 양식입니다. 이는 데이터 소유자가 데이터를 검색하고 찾을 때 데이터 사용자에게 도움이 될 수 있는 정보로 자산을 강화하는 확장 가능한 메커니즘 역할을 합니다. 메타데이터 양식은 Amazon DataZone 카탈로그에 게시되는 모든 자산에 일관성을 적용하는 메커니즘도 제공할 수 있습니다.

메타데이터 양식 정의는 부울, 날짜, 십진수, 정수, 문자열 및 비즈니스 용어집 필드 값 데이터 유형을 지원하는 하나 이상의 필드 정의로 구성됩니다. 자세한 내용은 Amazon DataZone 용어 및 개념 단원을 참조하십시오. Amazon DataZone 도메인에서 메타데이터 양식을 생성, 편집 또는 삭제하려면 자격 증명이 적절한 소유 프로젝트의 구성원이어야 합니다.

메타데이터 양식을 생성하려면 다음 단계를 완료하세요.

1. DataZone 데이터 포털을 사용하여 Amazon 데이터 포털로 이동URL하고 SSO 또는 AWS 자격 증명을 사용하여 로그인합니다. Amazon DataZone 관리자인 경우 Amazon DataZone 도메인이 생성된 AWS 계정의 https://console.aws.amazon.com/datazone에서 Amazon DataZone 콘솔에 액세스URL하여 데이터 포털을 얻을 수 있습니다.
2. 검색 옆의 상단 탐색 모음에서 카탈로그 메뉴로 이동합니다.
3. Amazon DataZone Data Portal에서 메타데이터 양식을 선택한 다음 양식 생성을 선택합니다.
4. 메타데이터 양식 이름, 설명, 소유자를 지정한 다음 양식 생성을 선택합니다.

Amazon에서 메타데이터 양식 편집 DataZone

Amazon 에서 DataZone메타데이터 양식은 카탈로그의 자산 메타데이터에 대한 추가 비즈니스 컨텍스트를 보강하는 간단한 양식입니다. 이는 데이터 소유자가 데이터를 검색하고 찾을 때 데이터 사용자에게 도움이 될 수 있는 정보로 자산을 강화하는 확장 가능한 메커니즘 역할을 합니다. 메타데이터 양식은 Amazon DataZone 카탈로그에 게시되는 모든 자산에 일관성을 적용하는 메커니즘도 제공할 수 있습니다.

메타데이터 양식 정의는 부울, 날짜, 십진수, 정수, 문자열 및 비즈니스 용어집 필드 값 데이터 유형을 지원하는 하나 이상의 필드 정의로 구성됩니다. 자세한 내용은 Amazon DataZone 용어 및 개념 단원을

참조하십시오. Amazon DataZone 도메인에서 메타데이터 양식을 생성, 편집 또는 삭제하려면 자격 증명이 적절한 소유 프로젝트의 구성원이어야 합니다.

메타데이터 양식을 편집하려면 다음 단계를 완료하세요.

1. DataZone 데이터 포털을 사용하여 Amazon 데이터 포털로 이동URL하고 SSO 또는 AWS 자격 증명을 사용하여 로그인합니다. Amazon DataZone 관리자인 경우 Amazon DataZone 도메인이 생성된 AWS 계정의 https://console.aws.amazon.com/datazone에서 Amazon DataZone 콘솔에 액세스URL하여 데이터 포털을 얻을 수 있습니다.
2. 검색 옆의 상단 탐색 모음에서 카탈로그 메뉴로 이동합니다.
3. Amazon DataZone Data Portal에서 메타데이터 양식 을 선택한 다음 편집하려는 메타데이터 양식을 찾습니다.
4. 메타데이터 양식의 세부 정보 페이지에서 작업 을 확장한 다음 편집 을 선택합니다.
5. 이름, 설명, 소유자 필드에 대한 업데이트를 수행한 다음 양식 업데이트를 선택합니다.

Amazon에서 메타데이터 양식 삭제 DataZone

Amazon 에서 DataZone메타데이터 양식은 카탈로그의 자산 메타데이터에 대한 추가 비즈니스 컨텍스트를 보강하는 간단한 양식입니다. 이는 데이터 소유자가 데이터를 검색하고 찾을 때 데이터 사용자에게 도움이 될 수 있는 정보로 자산을 강화하는 확장 가능한 메커니즘 역할을 합니다. 메타데이터 양식은 Amazon DataZone 카탈로그에 게시되는 모든 자산에 일관성을 적용하는 메커니즘도 제공할 수 있습니다.

메타데이터 양식 정의는 부울, 날짜, 십진수, 정수, 문자열 및 비즈니스 용어집 필드 값 데이터 유형을 지원하는 하나 이상의 필드 정의로 구성됩니다. 자세한 내용은 Amazon DataZone 용어 및 개념 단원을 참조하십시오. Amazon DataZone 도메인에서 메타데이터 양식을 생성, 편집 또는 삭제하려면 자격 증명이 적절한 소유 프로젝트의 구성원이어야 합니다.

메타데이터 양식을 삭제하려면 다음 단계를 완료합니다.

> **Note**
>
> 메타데이터 양식을 삭제하려면 먼저 메타데이터 양식이 적용된 모든 자산 유형 또는 자산에서 메타데이터 양식을 제거해야 합니다.

1. DataZone 데이터 포털을 사용하여 Amazon 데이터 포털로 이동URL하고 SSO 또는 AWS 자격 증명을 사용하여 로그인합니다. Amazon DataZone 관리자인 경우 Amazon DataZone 도메인이 생

성된 AWS 계정의 https://console.aws.amazon.com/datazone에서 Amazon DataZone 콘솔에 액세스URL하여 데이터 포털을 얻을 수 있습니다.

2. 검색 옆의 상단 탐색 모음에서 카탈로그 메뉴로 이동합니다.
3. Amazon DataZone Data Portal에서 메타데이터 양식 을 선택한 다음 삭제할 메타데이터 양식을 찾습니다.
4. 삭제하려는 메타데이터 양식이 활성화된 경우 활성화 토글을 선택하여 메타데이터 양식을 비활성화합니다.
5. 메타데이터 양식의 세부 정보 페이지에서 작업 을 확장한 다음 삭제 를 선택합니다.
6. 삭제를 선택하여 삭제를 확인합니다.

Amazon에서 메타데이터 형식으로 필드 생성 DataZone

Amazon 에서 DataZone메타데이터 양식은 카탈로그의 자산 메타데이터에 대한 추가 비즈니스 컨텍스트를 보강하는 간단한 양식입니다. 이는 데이터 소유자가 데이터를 검색하고 찾을 때 데이터 사용자에게 도움이 될 수 있는 정보로 자산을 강화하는 확장 가능한 메커니즘 역할을 합니다. 메타데이터 양식은 Amazon DataZone 카탈로그에 게시되는 모든 자산에 일관성을 적용하는 메커니즘도 제공할 수 있습니다.

메타데이터 양식 정의는 부울, 날짜, 십진수, 정수, 문자열 및 비즈니스 용어집 필드 값 데이터 유형을 지원하는 하나 이상의 필드 정의로 구성됩니다. 자세한 내용은 Amazon DataZone 용어 및 개념 단원을 참조하십시오. Amazon DataZone 도메인의 메타데이터 양식에서 필드를 생성, 편집 또는 삭제하려면 올바른 보안 인증 정보가 있는 소유 프로젝트의 구성원이어야 합니다.

메타데이터 형식으로 필드를 생성하려면 다음 단계를 완료합니다.

1. DataZone 데이터 포털을 사용하여 Amazon 데이터 포털로 이동URL하고 SSO 또는 AWS 자격 증명을 사용하여 로그인합니다. Amazon DataZone 관리자인 경우 Amazon DataZone 도메인이 생성된 AWS 계정의 https://console.aws.amazon.com/datazone에서 Amazon DataZone 콘솔에 액세스URL하여 데이터 포털을 얻을 수 있습니다.
2. 검색 옆의 상단 탐색 모음에서 카탈로그 메뉴로 이동합니다.
3. Amazon DataZone Data Portal에서 메타데이터 양식을 선택한 다음 필드(들)를 생성할 메타데이터 양식을 선택합니다.
4. 양식의 세부 정보 페이지에서 필드 생성을 선택합니다.
5. 필드 이름, 설명, 유형 및 필수 필드인지 여부를 지정한 다음 필드 생성을 선택합니다.

Amazon의 메타데이터 양식에서 필드 편집 DataZone

Amazon 에서 DataZone메타데이터 양식은 카탈로그의 자산 메타데이터에 대한 추가 비즈니스 컨텍스트를 보강하는 간단한 양식입니다. 이는 데이터 소유자가 데이터를 검색하고 찾을 때 데이터 사용자에게 도움이 될 수 있는 정보로 자산을 강화하는 확장 가능한 메커니즘 역할을 합니다. 메타데이터 양식은 Amazon DataZone 카탈로그에 게시되는 모든 자산에 일관성을 적용하는 메커니즘도 제공할 수 있습니다.

메타데이터 양식 정의는 부울, 날짜, 십진수, 정수, 문자열 및 비즈니스 용어집 필드 값 데이터 유형을 지원하는 하나 이상의 필드 정의로 구성됩니다. 자세한 내용은 Amazon DataZone 용어 및 개념 단원을 참조하십시오. Amazon DataZone 도메인의 메타데이터 양식에서 필드를 생성, 편집 또는 삭제하려면 올바른 보안 인증 정보가 있는 소유 프로젝트의 구성원이어야 합니다.

메타데이터 양식의 필드를 편집하려면 다음 단계를 완료합니다.

1. DataZone 데이터 포털을 사용하여 Amazon 데이터 포털로 이동URL하고 SSO 또는 AWS 자격 증명을 사용하여 로그인합니다. Amazon DataZone 관리자인 경우 Amazon DataZone 도메인이 생성된 AWS 계정의 https://console.aws.amazon.com/datazone에서 Amazon DataZone 콘솔에 액세스URL하여 데이터 포털을 얻을 수 있습니다.
2. 검색 옆의 상단 탐색 모음에서 카탈로그 메뉴로 이동합니다.
3. Amazon DataZone Data Portal에서 메타데이터 양식을 선택한 다음 필드를 편집할 메타데이터 양식을 선택합니다().
4. 양식의 세부 정보 페이지에서 편집할 필드를 선택한 다음 작업 을 확장하고 편집 을 선택합니다.
5. 필드 이름, 설명, 유형 및 필수 필드인지 여부를 업데이트한 다음 필드 업데이트를 선택합니다.

Amazon의 메타데이터 양식에서 필드 삭제 DataZone

Amazon 에서 DataZone메타데이터 양식은 카탈로그의 자산 메타데이터에 대한 추가 비즈니스 컨텍스트를 보강하는 간단한 양식입니다. 이는 데이터 소유자가 데이터를 검색하고 찾을 때 데이터 사용자에게 도움이 될 수 있는 정보로 자산을 강화하는 확장 가능한 메커니즘 역할을 합니다. 메타데이터 양식은 Amazon DataZone 카탈로그에 게시되는 모든 자산에 일관성을 적용하는 메커니즘도 제공할 수 있습니다.

메타데이터 양식 정의는 부울, 날짜, 십진수, 정수, 문자열 및 비즈니스 용어집 필드 값 데이터 유형을 지원하는 하나 이상의 필드 정의로 구성됩니다. 자세한 내용은 Amazon DataZone 용어 및 개념 단원을 참조하십시오. Amazon DataZone 도메인의 메타데이터 양식에서 필드를 생성, 편집 또는 삭제하려면 자격 증명이 올바른 소유 프로젝트의 구성원이어야 합니다.

메타데이터 양식에서 필드를 삭제하려면 다음 단계를 완료합니다.

1. DataZone 데이터 포털을 사용하여 Amazon 데이터 포털로 이동URL하고 SSO 또는 AWS 자격 증명을 사용하여 로그인합니다. Amazon DataZone 관리자인 경우 Amazon DataZone 도메인이 생성된 AWS 계정의 https://console.aws.amazon.com/datazone에서 Amazon DataZone 콘솔에 액세스URL하여 데이터 포털을 얻을 수 있습니다.
2. 검색 옆의 상단 탐색 모음에서 카탈로그 메뉴로 이동합니다.
3. Amazon DataZone Data Portal에서 메타데이터 양식을 선택한 다음 필드(들)를 삭제할 메타데이터 양식을 선택합니다.
4. 양식의 세부 정보 페이지에서 삭제할 필드를 선택한 다음 작업 을 확장하고 삭제를 선택합니다.
5. 삭제를 선택하여 삭제를 확인합니다.

Amazon DataZone 프로젝트 및 환경

Amazon 에서 DataZone프로젝트는 사용자 그룹이 Amazon DataZone 카탈로그의 데이터 자산 게시, 검색, 구독 및 소비와 관련된 다양한 비즈니스 사용 사례에 대해 협업할 수 있도록 합니다. 각 Amazon DataZone 프로젝트에는 권한 있는 개인, 그룹 및 역할만 프로젝트 및 이 프로젝트가 구독하는 데이터 자산에 액세스할 수 있고 프로젝트 권한으로 정의된 도구만 사용할 수 있도록 액세스 제어 세트가 적용됩니다. 프로젝트는 기본 리소스에 대한 액세스 권한을 받는 자격 증명 보안 주체 역할을 하므로 Amazon은 개별 사용자의 자격 증명에 의존하지 않고 조직의 인프라 내에서 운영 DataZone 할 수 있습니다.

Amazon 에서 DataZone환경은 구성된 리소스(예: Amazon S3 버킷, AWS Glue 데이터베이스 또는 Amazon Athena 작업 그룹)의 모음으로, 해당 리소스에서 작동할 수 있는 지정된 IAM 보안 주체 세트(할당된 기여자 권한 있음)가 있습니다. 각 환경에는 리소스에 액세스하고 구독 및 이행을 통해 데이터에 액세스할 수 있는 권한이 있는 사용자 보안 주체가 있을 수도 있습니다. 환경은 AWS 서비스 및 외부 IDEs 및 콘솔에 실행 가능한 링크를 저장하도록 설계되었습니다. 프로젝트 구성원은 환경 내에 구성된 딥 링크를 통해 Amazon Athena 콘솔 등과 같은 서비스에 액세스할 수 있습니다. SSO 프로젝트의 사용자와 IAM 사용자는 특정 환경을 사용/액세스하도록 범위를 더 줄일 수 있습니다.

Amazon 에서는 환경 프로파일이라는 템플릿을 사용하여 환경을 DataZone생성합니다. 환경 프로필은 기본 제공 및 사용자 지정 AWS 서비스 청사진을 사용하여 생성됩니다. 환경 프로파일을 사용하면 도메인 관리자가 블루프린트를 사전 구성된 파라미터로 래핑한 다음 데이터 워커는 기존 환경 프로파일을 선택하고 새 환경의 이름을 지정하여 원하는 수의 새 환경을 빠르게 생성할 수 있습니다. 이를 통해 데이터 워커는 프로젝트와 환경을 효율적으로 관리하는 동시에 도메인 관리자가 시행하는 데이터 거버넌스 정책을 충족할 수 있습니다.

자세한 내용은 Amazon DataZone 용어 및 개념 단원을 참조하세요.

주제

- 환경 프로파일 생성
- 환경 프로파일 편집
- 환경 프로필 삭제
- 새 환경 생성
- 환경 편집
- 환경을 삭제합니다.
- 새 프로젝트 만들기
- 프로젝트 편집

- 프로젝트 삭제
- 프로젝트 나가기
- 프로젝트에 멤버 추가
- 프로젝트에서 멤버 제거

환경 프로파일 생성

Amazon 에서 DataZone환경 프로파일은 환경을 생성하는 데 사용할 수 있는 템플릿입니다. 환경 프로파일의 목적은 프로파일 내에 AWS 계정 및 리전과 같은 배치 정보를 포함시켜 환경 생성을 단순화하는 것입니다. 자세한 내용은 Amazon DataZone 용어 및 개념 단원을 참조하십시오. Amazon DataZone 도메인에서 환경 프로파일을 생성하려면 Amazon DataZone 프로젝트에 속해야 합니다. 모든 환경 프로필은 프로젝트에서 소유하며 모든 프로젝트의 승인된 모든 사용자가 새 환경을 생성하는 데 사용할 수 있습니다.

환경 프로파일을 생성하려면

1. DataZone 데이터 포털을 사용하여 Amazon 데이터 포털로 이동URL하고 SSO 또는 AWS 자격 증명을 사용하여 로그인합니다. Amazon DataZone 관리자인 경우 Amazon DataZone 도메인이 생성된 AWS 계정의 https://console.aws.amazon.com/datazone에서 Amazon DataZone 콘솔에 액세스URL하여 데이터 포털을 얻을 수 있습니다.
2. 데이터 포털에서 프로젝트 찾아보기를 선택하고 환경 프로파일을 생성할 프로젝트를 선택합니다.
3. 프로젝트 내의 환경 탭으로 이동한 다음 환경 프로필 생성 을 선택합니다.
4. 다음 필드를 구성합니다.

    - 이름 - 환경 프로파일의 이름입니다.
    - 설명 - (선택 사항) 환경 프로파일에 대한 설명입니다.
    - 소유자 프로젝트 - 이 필드에서 프로필이 생성되는 프로젝트가 기본적으로 선택됩니다.
    - 청사진 - 이 프로파일이 생성되는 청사진입니다. 기본 Amazon DataZone 청사진(데이터 레이크 또는 데이터 웨어하우스) 중 하나를 선택할 수 있습니다.

      데이터 웨어하우스 청사진을 지정한 경우 다음을 수행합니다.

      - 파라미터 세트를 제공합니다. 기존 파라미터 세트를 선택하려면 파라미터 세트 선택 옵션을 선택합니다. 자체 파라미터를 입력하려면 자체 입력 을 선택합니다.
      - 기존 파라미터를 선택하는 경우 다음을 수행합니다.
        - 드롭다운에서 AWS 계정을 선택합니다.

- 드롭다운에서 파라미터 세트를 선택합니다.
- 자체 파라미터를 입력하도록 선택한 경우 다음을 수행합니다.
  - 드롭다운에서 계정 및 리전을 AWS 선택하여 AWS 파라미터를 제공합니다.
  - Redshift Data Wareshoue 파라미터 제공:
    - Amazon Redshift 클러스터 또는 Amazon Redshift Serverless를 선택합니다.
    - 선택한 Amazon Redshift 클러스터 또는 Amazon Redshift Serverless 작업 그룹에 보안 인증 정보를 ARN 보유한 AWS 보안 암호를 입력합니다. 보안 AWS 암호에는 환경 프로파일을 생성하는 도메인 ID 및 프로젝트 ID로 태그를 지정해야 합니다.
      - `AmazonDataZoneDomain: [Domain_ID]`
      - `AmazonDataZoneProject: [Project_ID]`
    - Amazon Redshift 클러스터 또는 Amazon Redshift Serverless 작업 그룹의 이름을 입력합니다.
    - 선택한 Amazon Redshift 클러스터 또는 Amazon Redshift Serverless 작업 그룹 내에 데이터베이스 이름을 입력합니다.
  - 승인된 프로젝트 섹션에서 환경 프로필로 환경을 생성할 수 있는 프로젝트를 지정합니다. 기본적으로 도메인 내의 모든 프로젝트는 계정의 환경 프로파일을 사용하여 환경을 생성할 수 있습니다. 이 기본 설정을 유지하려면 모든 프로젝트 를 선택합니다. 그러나 환경에 승인된 프로젝트를 할당하여 이를 제한할 수 있습니다. 이렇게 하려면 승인된 프로젝트만 선택한 다음 이 프로젝트 프로파일을 사용하여 환경을 생성할 수 있는 프로젝트를 지정합니다.
  - 게시 섹션에서 다음 옵션 중 하나를 선택합니다.
    - 스키마에서 게시 : 이 옵션을 선택하면 이 환경 프로파일을 사용하여 생성된 환경을 위에 제공된 Redshift 파라미터에서 선택한 데이터베이스 내의 스키마에서 게시하는 데 사용할 수 있습니다. 이 환경 프로파일을 사용하여 생성된 환경의 사용자는 자체 Amazon Redshift 파라미터를 제공하여 환경 프로파일에서 선택한 AWS 계정 및 리전 내의 스키마에서 게시할 수도 있습니다.
    - 기본 환경 스키마에서만 게시 : 이 옵션을 선택하면 이 옵션을 사용하여 생성된 환경은 해당 환경에 DataZone 대해 Amazon에서 생성한 기본 스키마에서만 게시하는 데 사용할 수 있습니다. 이 환경 프로파일을 사용하여 생성된 환경의 사용자는 자체 Amazon Redshift 파라미터를 제공할 수 없습니다.
    - 게시 허용 안 함: 이 옵션을 선택하면 이 환경 프로파일을 사용하여 생성된 환경을 데이터 구독 및 소비에만 사용할 수 있습니다. 환경을 사용하여 데이터를 게시할 수 없습니다.

Data Lake 청사진을 지정한 경우 다음을 수행합니다.

- AWS 계정 파라미터 섹션에서 AWS 계정 번호와 잠재적 환경이 생성될 AWS 계정 리전을 지정합니다.
- 승인된 프로젝트 섹션에서 환경을 생성하기 위해 내장된 Data Lake 환경 프로파일과 함께 환경 프로파일을 사용할 수 있는 프로젝트를 지정합니다. 기본적으로 도메인 내의 모든 프로젝트는 계정의 데이터 레이크 청사진을 사용하여 환경 프로파일을 생성할 수 있습니다. 이 기본 설정을 유지하려면 모든 프로젝트 를 선택합니다. 그러나 블루프린트에 프로젝트를 할당하여 이를 제한할 수 있습니다. 이렇게 하려면 승인된 프로젝트만 선택한 다음 이 프로젝트 프로파일을 사용하여 환경을 생성할 수 있는 프로젝트를 지정합니다.
- 데이터베이스 섹션에서 아무 데이터베이스나 선택하여 환경이 생성된 AWS 계정 및 리전 내의 데이터베이스에서 게시를 활성화하거나 기본 데이터베이스만 선택하여 환경으로 생성된 기본 게시 데이터베이스에서만 게시를 활성화합니다.

5. 환경 프로필 생성을 선택합니다.

환경 프로파일 편집

Amazon 에서 DataZone환경 프로파일은 환경을 생성하는 데 사용할 수 있는 템플릿입니다. 자세한 내용은 Amazon DataZone 용어 및 개념 단원을 참조하십시오. Amazon DataZone 도메인에서 기존 환경 프로파일을 편집하려면 Amazon DataZone 프로젝트에 속해야 합니다.

환경 프로파일을 편집하려면

1. Amazon DataZone 데이터 포털로 이동하여 Single Sign-On(SSO) 또는 자격 AWS 증명을 사용하여 URL 로그인합니다. Amazon DataZone 관리자인 경우 https://console.aws.amazon.com/datazone의 Amazon DataZone 콘솔로 이동하여 도메인이 생성된 AWS 계정 로 로그인한 다음 데이터 포털 열기를 선택합니다.
2. 데이터 포털에서 프로젝트 찾아보기를 선택하고 환경 프로파일을 편집할 프로젝트를 선택합니다.
3. 프로젝트 내의 환경 탭으로 이동한 다음 환경 프로파일 을 선택한 다음 편집하려는 환경 프로파일을 선택합니다.

   Data Warehouse 환경 프로파일을 편집하는 경우 기존 환경 프로파일의 이름과 설명만 편집할 수 있습니다.

   Data Lake 환경 프로파일을 편집하는 경우 프로파일의 이름과 설명을 편집할 수 있으며, 이 프로파일을 사용하여 환경을 생성할 수 있는 권한이 부여된 프로젝트를 편집하고 데이터베이스를 편집할 수도 있습니다. 이러한 설정을 편집하려면 다음을 수행합니다.

- 승인된 프로젝트 섹션에서 환경을 생성하기 위해 기본 제공 Data Lake 환경 프로파일과 함께 환경 프로파일을 사용할 수 있는 프로젝트를 지정합니다. 기본적으로 도메인 내의 모든 프로젝트는 계정의 데이터 레이크 청사진을 사용하여 환경 프로파일을 생성할 수 있습니다. 이 기본 설정을 유지하려면 모든 프로젝트 를 선택합니다. 그러나 블루프린트에 프로젝트를 할당하여 이를 제한할 수 있습니다. 이렇게 하려면 승인된 프로젝트만 선택한 다음 이 프로젝트 프로파일을 사용하여 환경을 생성할 수 있는 프로젝트를 지정합니다.
- 데이터베이스 섹션에서 아무 데이터베이스나 선택하여 환경이 생성된 AWS 계정 및 리전 내의 데이터베이스에서 게시를 활성화하거나 기본 데이터베이스만 선택하여 환경으로 생성된 기본 게시 데이터베이스에서만 게시를 활성화합니다.

편집을 완료하면 환경 프로필 편집을 선택합니다.

환경 프로필 삭제

Amazon 에서 DataZone환경 프로파일은 환경을 생성하는 데 사용할 수 있는 템플릿입니다. 환경 프로파일의 목적은 프로파일 내에 AWS 계정 및 리전과 같은 배치 정보를 포함시켜 환경 생성을 단순화하는 것입니다. 자세한 내용은 Amazon DataZone 용어 및 개념 단원을 참조하십시오. Amazon DataZone 도메인에서 환경 프로파일을 삭제하려면 Amazon DataZone 프로젝트에 속해야 합니다.

> **Note**
>
> 환경 프로파일을 삭제하면 이 프로파일을 사용하여 더 이상 환경을 생성할 수 없습니다.

환경 프로파일을 삭제하려면

1. Amazon DataZone 데이터 포털로 이동하여 Single Sign-On(SSO) 또는 자격 AWS 증명을 사용하여 URL 로그인합니다. Amazon DataZone 관리자인 경우 https://console.aws.amazon.com/datazone의 Amazon DataZone 콘솔로 이동하여 도메인이 생성된 AWS 계정 로 로그인한 다음 데이터 포털 열기를 선택합니다.
2. 데이터 포털에서 프로젝트 찾아보기를 선택하고 환경 프로파일을 삭제할 프로젝트를 선택합니다.
3. 프로젝트 내의 환경 탭으로 이동한 다음 환경 프로필 을 선택한 다음 삭제할 환경 프로필을 선택합니다.
4. 삭제할 환경 프로파일을 선택한 다음 작업 , 삭제 및 삭제 확인을 선택합니다.

새 환경 생성

Amazon DataZone 프로젝트에서 환경은 구성된 리소스(예: Amazon S3 버킷, AWS Glue 데이터베이스 또는 Amazon Athena 작업 그룹)의 모음으로, 해당 리소스에서 작업할 수 있는 소유자 또는 기여자 권한이 할당된 지정된 보안 IAM 주체(환경 사용자 역할) 집합입니다. 자세한 내용은 Amazon DataZone 용어 및 개념 단원을 참조하십시오.

데이터 포털에 액세스하는 데 필요한 권한이 있는 모든 Amazon DataZone 사용자는 프로젝트 내에 Amazon DataZone 환경을 생성할 수 있습니다.

새 환경을 생성하려면 다음 단계를 완료합니다.

1. Amazon DataZone 데이터 포털로 이동하여 Single Sign-On(SSO) 또는 자격 AWS 증명을 사용하여 URL 로그인합니다. Amazon DataZone 관리자인 경우 https://console.aws.amazon.com/datazone의 Amazon DataZone 콘솔로 이동하여 도메인이 생성된 AWS 계정 로 로그인한 다음 데이터 포털 열기를 선택합니다.
2. 모든 프로젝트 찾아보기를 선택하고 새 환경을 만들 프로젝트를 선택합니다.
3. 환경 생성을 선택하고 다음 필드에 값을 지정한 다음 환경 생성을 선택합니다.

   - 이름 - 환경 이름
   - 설명 - 환경에 대한 설명
   - 환경 프로파일 - 기존 환경 프로파일을 선택하거나 새 환경 프로파일을 생성합니다. 환경 프로필은 환경을 생성하는 데 사용할 수 있는 템플릿입니다. 자세한 내용은 Amazon DataZone 용어 및 개념 단원을 참조하십시오.

     환경 프로파일을 선택한 후 파라미터 섹션에서 이 환경 프로파일의 일부인 필드의 값을 지정합니다.

환경 편집

Amazon DataZone 프로젝트에서 환경은 구성된 리소스(예: Amazon S3 버킷, AWS Glue 데이터베이스 또는 Amazon Athena 작업 그룹)의 모음으로, 해당 리소스에서 작동할 수 있는 지정된 IAM 보안 주체 세트(기여자 권한이 할당된)가 있습니다. 자세한 내용은 Amazon DataZone 용어 및 개념 단원을 참조하십시오.

데이터 포털에 액세스하는 데 필요한 권한이 있는 모든 Amazon DataZone 사용자는 프로젝트 내에서 Amazon DataZone 환경을 편집할 수 있습니다.

기존 환경을 편집하려면 다음 단계를 완료합니다.

1. Amazon DataZone 데이터 포털로 이동하여 Single Sign-On(SSO) 또는 자격 AWS 증명을 사용하여 URL 로그인합니다. Amazon DataZone 관리자인 경우 https://console.aws.amazon.com/datazone의 Amazon DataZone 콘솔로 이동하여 도메인이 생성된 AWS 계정 로 로그인한 다음 데이터 포털 열기를 선택합니다.
2. 상단 탐색 창에서 프로젝트 찾아보기를 선택하고 편집하려는 환경이 포함된 프로젝트를 선택합니다.
3. 환경을 찾아 선택하여 세부 정보 페이지를 엽니다. 그런 다음 작업을 확장하고 환경 편집 을 선택합니다.
4. 환경의 이름과 설명을 편집한 다음 변경 사항 저장을 선택합니다.

환경을 삭제합니다.

Amazon DataZone 프로젝트에서 환경은 구성된 리소스(예: Amazon S3 버킷, AWS Glue 데이터베이스 또는 Amazon Athena 작업 그룹)의 모음으로, 해당 리소스에서 작동할 수 있는 지정된 IAM 보안 주체 세트(기여자 권한이 할당된)가 있습니다. 자세한 내용은 Amazon DataZone 용어 및 개념 단원을 참조하십시오.

데이터 포털에 액세스하는 데 필요한 권한이 있는 모든 Amazon DataZone 사용자는 프로젝트 내에서 Amazon DataZone 환경을 삭제할 수 있습니다.

기존 환경을 삭제하려면 다음 단계를 완료합니다.

1. Amazon DataZone 데이터 포털로 이동하여 Single Sign-On(SSO) 또는 자격 AWS 증명을 사용하여 URL 로그인합니다. Amazon DataZone 관리자인 경우 https://console.aws.amazon.com/datazone의 Amazon DataZone 콘솔로 이동하여 도메인이 생성된 AWS 계정 로 로그인한 다음 데이터 포털 열기를 선택합니다.
2. 상단 탐색 창에서 프로젝트 찾아보기를 선택하고 삭제할 환경이 포함된 프로젝트를 선택합니다.
3. 환경을 찾아 선택하여 세부 정보 페이지를 연 다음 작업을 확장하고 환경 삭제를 선택합니다.
4. 환경 삭제 팝업 창에서 필드에 입력하여 삭제`Delete`를 확인한 다음 환경 삭제를 선택합니다.

   이 환경에 종속된 모든 엔터티가 삭제된 후에만 환경을 성공적으로 삭제할 수 있습니다. 환경을 삭제하려면 먼저 연결된 모든 데이터 소스와 구독 대상을 삭제해야 합니다.

새 프로젝트 만들기

Amazon 에서 DataZone프로젝트는 사용자 그룹이 Amazon DataZone 카탈로그의 데이터 자산 게시, 검색, 구독 및 소비와 관련된 다양한 비즈니스 사용 사례에 대해 협업할 수 있도록 합니다. 자세한 내용은 Amazon DataZone 용어 및 개념 단원을 참조하십시오.

데이터 포털에 액세스하는 데 필요한 권한이 있는 모든 Amazon DataZone 사용자는 Amazon DataZone 프로젝트를 생성할 수 있습니다.

새 프로젝트를 생성하려면 다음 단계를 완료하세요.

1. Amazon DataZone 데이터 포털로 이동하여 Single Sign-On(SSO) 또는 자격 AWS 증명을 사용하여 URL 로그인합니다. Amazon DataZone 관리자인 경우 https://console.aws.amazon.com/datazone의 Amazon DataZone 콘솔로 이동하여 도메인이 생성된 AWS 계정 로 로그인한 다음 데이터 포털 열기를 선택합니다.
2. Amazon DataZone 데이터 포털에서 프로젝트 생성을 선택합니다.
3. 다음 필드의 값을 지정한 다음 프로젝트 생성을 선택합니다.
   - 이름 - 프로젝트 이름입니다.
   - 설명 - 프로젝트에 대한 설명입니다.
   - 도메인 단위 - 이 프로젝트를 생성할 도메인 단위입니다.

프로젝트 편집

Amazon 에서 DataZone프로젝트는 사용자 그룹이 Amazon DataZone 카탈로그의 데이터 자산 게시, 검색, 구독 및 소비와 관련된 다양한 비즈니스 사용 사례에 대해 협업할 수 있도록 합니다. 자세한 내용은 Amazon DataZone 용어 및 개념 단원을 참조하십시오. Amazon DataZone 프로젝트를 편집하려면 해당 프로젝트의 소유자이거나 이 프로젝트가 포함된 도메인의 도메인 관리자여야 합니다.

기존 프로젝트를 편집하려면 다음 단계를 완료합니다.

1. Amazon DataZone 데이터 포털로 이동하여 Single Sign-On(SSO) 또는 자격 AWS 증명을 사용하여 URL 로그인합니다. Amazon DataZone 관리자인 경우 https://console.aws.amazon.com/datazone의 Amazon DataZone 콘솔로 이동하여 도메인이 생성된 AWS 계정 로 로그인한 다음 데이터 포털 열기를 선택합니다.
2. 프로젝트 찾아보기 를 선택합니다.

3. 편집하려는 프로젝트를 선택합니다. 프로젝트 목록에서 쉽게 볼 수 없는 경우 프로젝트 찾기 필드에 프로젝트 이름을 지정하여 검색할 수 있습니다.
4. 작업을 확장하고 프로젝트 편집 을 선택합니다.
5. 프로젝트 이름 및 설명에 대한 업데이트를 수행한 다음 저장을 선택합니다.

프로젝트 삭제

Amazon 에서 DataZone프로젝트는 사용자 그룹이 Amazon DataZone 카탈로그의 데이터 자산 게시, 검색, 구독 및/또는 소비와 관련된 다양한 비즈니스 사용 사례에 대해 협업할 수 있도록 합니다. 자세한 내용은 Amazon DataZone 용어 및 개념 단원을 참조하십시오.

프로젝트를 삭제하는 작업은 최종적입니다. 삭제하면 데이터 소스, 환경, 자산, 용어집 및 메타데이터 양식을 포함하여 프로젝트의 콘텐츠가 취소 불가능한 방식으로 삭제됩니다. Amazon DataZone 이 Lake Formation 및 Amazon Redshift를 통해 관리형 자산에 배치 DataZone 한 권한 부여를 취소합니다. 프로젝트를 삭제해도 Amazon이 생성에 도움이 되었을 DataZone 수 있는 Amazon 이외의 DataZone AWS 리소스는 삭제되지 않습니다. 이러한 AWS 리소스가 더 이상 필요하지 않은 경우 해당 AWS 서비스 및 계정에서 해당 리소스를 삭제합니다.

Amazon DataZone 프로젝트를 삭제하려면 프로젝트의 소유자여야 합니다.

기존 프로젝트를 삭제하려면 다음 단계를 완료합니다.

1. Amazon DataZone 데이터 포털로 이동하여 Single Sign-On(SSO) 또는 자격 AWS 증명을 사용하여 URL 로그인합니다. IAM 보안 주체는 https://console.aws.amazon.com/datazone의 Amazon DataZone 콘솔로 이동하여 도메인이 생성된 AWS 계정 로 로그인한 다음 데이터 포털 열기를 선택할 수 있습니다.
2. 상단 탐색 창에서 프로젝트 찾아보기를 선택합니다.
3. 삭제할 프로젝트를 선택합니다. 프로젝트 목록에 표시되지 않는 경우 프로젝트 찾기 필드에 프로젝트 이름을 지정하여 검색할 수 있습니다.
4. 작업을 확장하고 프로젝트 삭제 를 선택합니다.

   프로젝트 삭제의 잠재적 영향에 대한 정보 경고를 검토합니다.
5. 경고를 수락하면 확인 텍스트를 입력하고 삭제를 선택합니다.

> **Important**
>
> 프로젝트 삭제는 사용자 또는 에서 취소할 수 없는 취소 불가능한 작업입니다 AWS.

> **Note**
>
> 사용자 또는 도메인 사용자가 프로젝트에서 환경을 생성할 때 Amazon DataZone은 도메인 또는 연결된 계정에 AWS 리소스를 생성하여 사용자와 도메인 사용자에게 기능을 제공합니다. 다음은 Amazon이 프로젝트에 대해 생성할 DataZone 수 있는 AWS 리소스 목록과 기본 이름입니다. 프로젝트를 삭제해도 AWS 계정에서 이러한 AWS 리소스는 삭제되지 않습니다.
>
> - IAM 역할: datazone_usr_<environmentId>.
> - Glue 데이터베이스: (1) <environmentName>_pub_db-*, (2) <environmentName>_sub_db-*. 이 이름의 기존 데이터베이스가 이미 있는 경우 Amazon DataZone 은 환경 ID를 추가합니다.
> - Athena 작업 그룹: <environmentName>-*. 이 이름의 기존 작업 그룹이 이미 있는 경우 Amazon DataZone 은 환경 ID를 추가합니다.
> - CloudWatch 로그 그룹: datazone_<environmentId>

프로젝트 나가기

Amazon 에서 DataZone프로젝트는 사용자 그룹이 Amazon DataZone 카탈로그의 데이터 자산 게시, 검색, 구독 및 소비와 관련된 다양한 비즈니스 사용 사례에 대해 협업할 수 있도록 합니다. 자세한 내용은 Amazon DataZone 용어 및 개념 단원을 참조하십시오.

기존 프로젝트를 종료하려면 다음 단계를 완료합니다.

1. Amazon DataZone 데이터 포털로 이동하여 Single Sign-On(SSO) 또는 자격 AWS 증명을 사용하여 URL 로그인합니다. Amazon DataZone 관리자인 경우 https://console.aws.amazon.com/datazone의 Amazon DataZone 콘솔로 이동하여 도메인이 생성된 AWS 계정 로 로그인한 다음 데이터 포털 열기를 선택합니다.
2. 상단 탐색 창에서 프로젝트 선택을 선택하고 프로젝트를 선택합니다.
3. 종료하려는 프로젝트를 선택합니다. 프로젝트 목록에서 쉽게 볼 수 없는 경우 프로젝트 찾기 필드에 프로젝트 이름을 지정하여 검색할 수 있습니다.
4. 작업을 확장하고 프로젝트 나가기 를 선택합니다.

프로젝트에 멤버 추가

Amazon 에서 DataZone프로젝트는 사용자 그룹이 Amazon DataZone 카탈로그의 데이터 자산 게시, 검색, 구독 및 소비와 관련된 다양한 비즈니스 사용 사례에 대해 협업할 수 있도록 합니다. 자세한 내용은 Amazon DataZone 용어 및 개념 단원을 참조하십시오.

프로젝트에 멤버를 추가하려면 프로젝트 소유자 또는 기여자여야 합니다. SSO 그룹, SSO 사용자 또는 IAM 보안 주체(역할 또는 사용자)를 프로젝트 멤버로 추가할 수 있습니다.

기존 프로젝트에 멤버를 추가하려면 다음 단계를 완료합니다.

1. Amazon DataZone 데이터 포털로 이동하여 Single Sign-On(SSO) 또는 자격 AWS 증명을 사용하여 URL 로그인합니다. Amazon DataZone 관리자인 경우 https://console.aws.amazon.com/datazone의 Amazon DataZone 콘솔로 이동하여 도메인이 생성된 AWS 계정 로 로그인한 다음 데이터 포털 열기를 선택합니다.
2. 상단 탐색 창에서 프로젝트 선택을 선택하고 프로젝트를 선택합니다.
3. memebr을 추가할 프로젝트를 선택합니다. 프로젝트 목록에서 쉽게 볼 수 없는 경우 프로젝트 찾기 필드에 프로젝트 이름을 지정하여 검색할 수 있습니다.
4. 프로젝트의 세부 정보 페이지에서 멤버 탭을 선택하고 모든 멤버 노드를 선택합니다.
5. 프로젝트 멤버 탭에서 멤버 추가를 선택합니다.
6. 프로젝트에 멤버 추가 팝업 창에서 추가할 사용자(들)를 지정하고 프로젝트 내에서 역할(소유자, 기여자, 소비자, 관리인 또는 뷰어)을 지정한 다음 멤버 추가를 선택합니다.

> **Important**
>
> 이 프로젝트가 있는 도메인 유닛에 대해 구성된 프로젝트 멤버십 권한 부여 정책에 따라 이 프로젝트의 멤버가 될 권한이 있는 프로젝트 멤버로만 해당 사용자를 추가할 수 있습니다. 자세한 정보는 Amazon DataZone 도메인 유닛 내의 사용자 및 그룹에 권한 부여 정책 할당을 참조하십시오.

> **Note**
>
> 보안 IAM 주체가 도메인에 이미 Amazon DataZone 사용자 프로필을 가지고 있는 경우 보안 주체를 프로젝트 멤버로 추가할 수 있습니다. Amazon은 포털, API또는 를 통해 도메인과 성공적으로 상호 작용할 때 IAM 보안 주체의 사용자 프로필을 DataZone 자동으로 생성합니다

CLI. IAM 보안 주체의 사용자 프로필은 생성할 수 없습니다. 보안 IAM 주체가 도메인에 기존 Amazon DataZone 사용자 프로필이 없는 경우 IAM 보안 주체를 프로젝트 멤버로 추가하려면 관리자에게 IAM 콘솔의 도메인 AmazonDataZoneDomainExecutionRole 에 다음 두 가지 IAM 권한을 추가하도록 요청합니다`iam:GetRole`. `iam:GetUser` 및 별도로 도메인에서 작업을 수행하려면 IAM 보안 주체가 해당 작업에 대한 해당 IAM 권한을 가져야 합니다.

프로젝트에서 멤버 제거

Amazon 에서 DataZone프로젝트는 사용자 그룹이 Amazon DataZone 카탈로그의 데이터 자산 게시, 검색, 구독 및 소비와 관련된 다양한 비즈니스 사용 사례에 대해 협업할 수 있도록 합니다. 자세한 내용은 Amazon DataZone 용어 및 개념 단원을 참조하십시오. 프로젝트에서 멤버를 제거하려면 프로젝트 소유자여야 합니다.

종료 중인 프로젝트에서 멤버를 제거하려면 다음 단계를 완료합니다.

1. DataZone 데이터 포털을 사용하여 Amazon 데이터 포털로 이동URL하고 SSO 또는 AWS 자격 증명을 사용하여 로그인합니다. Amazon DataZone 관리자인 경우 Amazon DataZone 도메인이 생성된 AWS 계정의 https://console.aws.amazon.com/datazone에서 Amazon DataZone 콘솔에 액세스URL하여 데이터 포털을 얻을 수 있습니다.
2. 상단 탐색 창에서 프로젝트 선택을 선택하고 프로젝트를 선택합니다.
3. memebr을 제거할 프로젝트를 선택합니다. 프로젝트 목록에서 쉽게 볼 수 없는 경우 프로젝트 찾기 필드에 프로젝트 이름을 지정하여 검색할 수 있습니다.
4. 프로젝트의 세부 정보 페이지에서 멤버 탭을 선택하고 모든 멤버 노드를 선택합니다.
5. 프로젝트 멤버 탭에서 프로젝트에서 제거할 멤버(들)를 선택한 다음 제거를 선택합니다.
6. 멤버 제거 팝업 창에서 멤버 제거 를 선택하여 제거를 확인합니다.

Amazon에서 데이터 인벤토리 및 게시 DataZone

이 섹션에서는 Amazon에서 데이터 인벤토리를 생성하고 Amazon 에 데이터를 게시하기 위해 수행하려는 작업 DataZone 및 절차에 대해 설명합니다 DataZone.

Amazon DataZone 을 사용하여 데이터를 카탈로그화하려면 먼저 Amazon 에서 데이터(자산)를 프로젝트의 인벤토리로 가져와야 합니다 DataZone. 특정 프로젝트에 대한 인벤토리를 생성하면 해당 프로젝트의 구성원만 자산을 검색할 수 있습니다. 프로젝트 인벤토리 자산은 명시적으로 게시되지 않는 한 검색/찾아보기에서 모든 도메인 사용자가 사용할 수 있는 것은 아닙니다. 프로젝트 인벤토리를 생성한 후 데이터 소유자는 비즈니스 이름(자산 및 스키마), 설명(자산 및 스키마), 읽기 권한, 용어집 용어(자산 및 스키마) 및 메타데이터 양식을 추가하거나 업데이트하여 필요한 비즈니스 메타데이터로 인벤토리 자산을 큐레이션할 수 있습니다.

Amazon DataZone 을 사용하여 데이터를 카탈로그화하는 다음 단계는 도메인 사용자가 프로젝트의 인벤토리 자산을 검색할 수 있도록 하는 것입니다. 인벤토리 자산을 Amazon DataZone 카탈로그에 게시하여 이 작업을 수행할 수 있습니다. 최신 버전의 인벤토리 자산만 카탈로그에 게시할 수 있으며 최신 게시 버전만 검색 카탈로그에서 활성화됩니다. 인벤토리 자산이 Amazon DataZone 카탈로그에 게시된 후 업데이트되는 경우 최신 버전이 검색 카탈로그에 포함되도록 다시 명시적으로 게시해야 합니다.

자세한 내용은 Amazon DataZone 용어 및 개념 단원을 참조하세요.

주제

- Amazon에 대한 Lake Formation 권한 구성 DataZone
- Amazon에서 사용자 지정 자산 유형 생성 DataZone
- 에 대한 Amazon DataZone 데이터 소스 생성 및 실행 AWS Glue Data Catalog
- Amazon Redshift용 Amazon DataZone 데이터 소스 생성 및 실행
- Amazon에서 데이터 소스 편집 DataZone
- Amazon에서 데이터 소스 삭제 DataZone
- 프로젝트 인벤토리에서 Amazon DataZone 카탈로그에 자산 게시
- Amazon에서 인벤토리 관리 및 자산 큐레이트 DataZone
- Amazon에서 수동으로 자산 생성 DataZone
- Amazon DataZone 카탈로그에서 자산 게시 취소
- Amazon DataZone 자산 삭제
- Amazon에서 데이터 소스 실행 수동 시작 DataZone

- Amazon의 자산 개정 DataZone
- Amazon의 데이터 품질 DataZone
- Amazon에서 기계 학습 및 생성형 AI 사용 DataZone
- Amazon의 데이터 계보 DataZone (미리 보기)

Amazon에 대한 Lake Formation 권한 구성 DataZone

내장 데이터 레이크 청사진(DefaultDataLake)을 사용하여 환경을 생성하면 이 환경 생성 프로세스의 DataZone 일부로 Amazon에 AWS Glue 데이터베이스가 추가됩니다. 이 AWS Glue 데이터베이스의 자산을 게시하려는 경우 추가 권한이 필요하지 않습니다.

그러나 자산을 게시하고 Amazon DataZone 환경 외부에 있는 AWS Glue 데이터베이스의 자산을 구독하려면 Amazon에 이 외부 AWS Glue 데이터베이스의 테이블에 액세스할 수 DataZone 있는 권한을 명시적으로 제공해야 합니다. 이렇게 하려면 AWS Lake Formation에서 다음 설정을 완료하고 필요한 Lake Formation 권한을 AmazonDataZoneGlueAccess-<region>-<domainId> 에 연결해야 합니다.

- AWS Lake Formation 권한 모드 또는 하이브리드 액세스 모드 를 사용하여 Lake Formation의 데이터 레이크에 대한 Amazon S3 위치를 구성합니다. 자세한 내용은 https://docs.aws.amazon.com/lake-formation/latest/dg/register-data-lake.html을 참조하세요.
- Amazon이 `IAMAllowedPrincipals` 권한을 DataZone 처리하는 Amazon Lake Formation 테이블에서 권한을 제거합니다. 자세한 내용은 https://docs.aws.amazon.com/lake-formation/latest/dg/upgrade-glue-lake-formation-background.html 을 참조하세요.
- 다음 AWS Lake Formation 권한을 에 연결합니다AmazonDataZoneGlueAccess-<region>-<domainId>.
  - `Describe` 및 테이블이 있는 데이터베이스에 대한 `Describe grantable` 권한
  - `Describe`, `Select`, `Describe Grantable`, 사용자를 대신하여 액세스를 관리 DataZone 하려는 위 데이터베이스의 모든 테이블에 대한 `Select Grantable` 권한.

> **Note**
>
> Amazon은 AWS Lake Formation Hybrid 모드를 DataZone 지원합니다. Lake Formation 하이브리드 모드를 사용하면 Lake Formation을 통해 AWS Glue 데이터베이스 및 테이블에 대한 권한 관리를 시작하는 동시에 이러한 테이블 및 데이터베이스에 대한 기존 IAM 권한을 계속 유

지할 수 있습니다. 자세한 내용은 AWS Lake Formation 하이브리드 모드와 Amazon DataZone 통합 단원을 참조하세요.

자세한 내용은 Amazon에 대한 AWS Lake Formation 권한 문제 해결 DataZone 단원을 참조하십시오.

AWS Lake Formation 하이브리드 모드와 Amazon DataZone 통합

Amazon DataZone 은 AWS Lake Formation 하이브리드 모드와 통합됩니다. 이 통합을 통해 먼저 AWS Lake Formation에 등록하지 않고도 Amazon DataZone을 통해 AWS Glue 테이블을 쉽게 게시하고 공유할 수 있습니다. 하이브리드 모드를 사용하면 AWS Lake Formation을 통해 AWS Glue 테이블에 대한 권한 관리를 시작하는 동시에 이러한 테이블에 대한 기존 IAM 권한을 계속 유지할 수 있습니다.

시작하려면 Amazon DataZone 관리 콘솔의 DefaultDataLake 청사진에서 데이터 위치 등록 설정을 활성화할 수 있습니다.

AWS Lake Formation 하이브리드 모드와의 통합 활성화

1. https://console.aws.amazon.com/datazone의 Amazon DataZone 콘솔로 이동하여 계정 자격 증명으로 로그인합니다.
2. 도메인 보기를 선택하고 AWS Lake Formation 하이브리드 모드와의 통합을 활성화하려는 도메인을 선택합니다.
3. 도메인 세부 정보 페이지에서 청사진 탭으로 이동합니다.
4. 청사진 목록에서 DefaultDataLake 청사진을 선택합니다.
5. DefaultDataLake 블루프린트가 활성화되어 있는지 확인합니다. 활성화되지 않은 경우 의 단계에 따라 계정에서 에서 빌트인 블루프린트를 활성화합니다. AWS Amazon DataZone 도메인을 소유한 계정 활성화하세요 AWS .
6. DefaultDataLake 세부 정보 페이지에서 프로비저닝 탭을 열고 페이지 오른쪽 상단 모서리에 있는 편집 버튼을 선택합니다.
7. 데이터 위치 등록에서 데이터 위치 등록을 활성화하려면 확인란을 선택합니다.
8. 데이터 위치 관리 역할의 경우 새 IAM 역할을 생성하거나 기존 IAM 역할을 선택할 수 있습니다. Amazon DataZone 은 이 역할을 사용하여 AWS Lake Formation 하이브리드 액세스 모드를 사용하여 Data Lake에 대해 선택한 Amazon S3 버킷(들)에 대한 읽기/쓰기 액세스를 관리합니다. 자세한 내용은 AmazonDataZoneS3Manage -<region>-<domainId> 단원을 참조하십시오.
9. 선택적으로, Amazon이 하이브리드 모드에서 자동으로 등록하지 않도록 하려면 특정 Amazon S3 위치를 제외 DataZone 하도록 선택할 수 있습니다. 이를 위해 다음 단계를 완료합니다.

- 토글 버튼을 선택하여 지정된 Amazon S3 위치를 제외합니다.
- 제외하려는 Amazon S3 버킷URI의 를 제공합니다.
- 버킷을 추가하려면 S3 위치 추가를 선택합니다.

> **Note**
>
> Amazon은 루트 S3 위치 DataZone 만 제외할 수 있습니다. 루트 S3 위치 경로 내의 모든 S3 위치는 자동으로 등록에서 제외됩니다.

- Save changes(변경 사항 저장)를 선택합니다.

계정 AWS 에서 데이터 위치 등록 설정을 활성화한 후 데이터 소비자가 IAM 권한을 통해 관리되는 AWS Glue 테이블을 구독하면 Amazon DataZone 은 먼저 이 테이블의 Amazon S3 위치를 하이브리드 모드로 등록한 다음 AWS Lake Formation을 통해 테이블의 권한을 관리하여 데이터 소비자에게 액세스 권한을 부여합니다. 이렇게 하면 기존 워크플로를 중단하지 않고 새로 부여된 AWS Lake Formation IAM 권한으로 테이블에 대한 권한이 계속 유지됩니다.

Amazon에서 AWS Lake Formation 하이브리드 모드 통합을 활성화할 때 암호화된 Amazon S3 위치를 처리하는 방법 DataZone

고객 관리형 또는 AWS 관리형 KMS 키로 암호화된 Amazon S3 위치를 사용하는 경우 AmazonDataZoneS3Manage 역할에KMS는 키를 사용하여 데이터를 암호화하고 복호화할 수 있는 권한이 있거나 KMS 키 정책이 역할에 키에 대한 권한을 부여해야 합니다.

Amazon S3 위치가 AWS 관리형 키로 암호화된 경우 AmazonDataZoneDataLocationManagement 역할에 다음 인라인 정책을 추가합니다.

```
 {
"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 위치가 고객 관리형 키로 암호화된 경우 다음을 수행합니다.

1. https://console.aws.amazon.com/km에서 콘솔을 열고 AWS KMS Identity and Access Management(IAM) 관리 사용자 또는 위치를 암호화하는 데 사용되는 KMS 키의 키 정책을 수정할 수 있는 사용자로 로그인 AWS 합니다.
2. 탐색 창에서 고객 관리형 키 를 선택한 다음 원하는 KMS 키의 이름을 선택합니다.
3. KMS 키 세부 정보 페이지에서 키 정책 탭을 선택한 다음 다음 중 하나를 수행하여 사용자 지정 역할 또는 Lake Formation 서비스 연결 역할을 KMS 키 사용자로 추가합니다.

   - 기본 보기가 표시되는 경우(키 관리자, 키 삭제, 키 사용자 및 기타 AWS 계정 섹션 포함) - 키 사용자 섹션에서 AmazonDataZoneDataLocationManagement 역할을 추가합니다.
   - 키 정책(JSON)이 표시되는 경우 다음 예와 같이 정책을 편집하여 객체에 AmazonDataZoneDataLocationManagement 역할을 추가합니다. “키 사용 허용”

```
...
        {
            "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 키 또는 Amazon S3 위치가 데이터 카탈로그와 동일한 AWS 계정에 없는 경우 계정 간에 AWS 암호화된 Amazon S3 위치 등록의 지침을 따릅니다.

Amazon에서 사용자 지정 자산 유형 생성 DataZone

Amazon 에서 DataZone자산은 데이터베이스 테이블, 대시보드 또는 기계 학습 모델과 같은 특정 유형의 데이터 리소스를 나타냅니다. 카탈로그 자산을 설명할 때 일관성과 표준화를 제공하려면 Amazon DataZone 도메인에 카탈로그에서 자산을 나타내는 방법을 정의하는 자산 유형 집합이 있어야 합니다. 자산 유형은 특정 유형의 자산에 대한 스키마를 정의합니다. 자산 유형에는 필수 및 선택적 이름 지정 가능 메타데이터 양식 유형(예: govForm 또는) 세트가 있습니다 GovernanceFormType. Amazon의 자산 유형은 버전 관리 DataZone 됩니다. 자산이 생성되면 자산 유형(일반적으로 최신 버전)에 의해 정의된 스키마에 대해 검증되고 잘못된 구조가 지정되면 자산 생성이 실패합니다.

시스템 자산 유형 - Amazon은 서비스 소유 시스템 자산 유형(GlueTableAssetType, GlueViewAssetType, RedshiftTableAssetType RedshiftViewAssetType및 S3ObjectCollectionAssetType 포함) 및 시스템 양식 유형(DataSourceReferenceFormType AssetCommonDetailsFormType, 및 포함)을 DataZone 프로비저닝합니다 SubscriptionTermsFormType. 시스템 자산 유형은 편집할 수 없습니다.

사용자 지정 자산 유형 - 사용자 지정 자산 유형을 생성하려면 먼저 양식 유형에 사용할 필수 메타데이터 양식 유형과 용어집을 생성합니다. 그런 다음 필수 또는 선택 사항일 수 있는 이름, 설명 및 관련 메타데이터 양식을 지정하여 사용자 지정 자산 유형을 생성할 수 있습니다.

구조화된 데이터가 있는 자산 유형의 경우 데이터 포털에서 열 스키마를 나타내려면 `RelationalTableFormType`를 사용하여 열 이름, 설명 및 데이터 유형을 포함한 기술적 메타데이터를 열에 추가하고) 를 사용하여 비즈니스 이름, 용어 및 사용자 지정 키 값 페어 `ColumnBusinessMetadataForm`를 포함한 열의 비즈니스 설명을 추가할 수 있습니다.

데이터 포털을 통해 사용자 지정 자산 유형을 생성하려면 다음 단계를 완료합니다.

1. Amazon DataZone 데이터 포털로 이동하여 Single Sign-On(SSO) 또는 자격 AWS 증명을 사용하여 URL 로그인합니다. Amazon DataZone 관리자인 경우 https://console.aws.amazon.com/

datazone의 Amazon DataZone 콘솔로 이동하여 도메인이 생성된 AWS 계정 로 로그인한 다음 데이터 포털 열기를 선택합니다.

2. 상단 탐색 창에서 프로젝트 선택을 선택하고 사용자 지정 자산 유형을 생성할 프로젝트를 선택합니다.
3. 프로젝트의 데이터 탭으로 이동합니다.
4. 왼쪽 탐색 창에서 자산 유형을 선택한 다음 자산 유형 생성을 선택합니다.
5. 다음을 지정한 다음 생성을 선택합니다.
   - 이름 - 사용자 지정 자산 유형의 이름
   - 설명 - 사용자 지정 자산 유형에 대한 설명입니다.
   - 메타데이터 양식 추가를 선택하여 이 사용자 지정 자산 유형에 메타데이터 양식을 추가합니다.
6. 사용자 지정 자산 유형이 생성되면 이를 사용하여 자산을 생성할 수 있습니다.

를 통해 사용자 지정 자산 유형을 생성하려면 다음 단계를 APIs완료합니다.

1. `CreateFormType` API 작업을 호출하여 메타데이터 양식 유형을 생성합니다.

   다음은 Amazon 예제입니다 SageMaker .

```
m_model = "

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

   @required
   modelArn: String

   @required
   creationTime: String
}
"

CreateFormType(
    domainIdentifier="my-dz-domain",
    owningProjectIdentifier="d4bywm0cja1dbb",
    name="SageMakerModelFormType",
```

```
    model=m_model
    status="ENABLED"
    )
```

2. 다음으로 CreateAssetType API 작업을 호출하여 자산 유형을 생성할 수 있습니다. 사용 가능한 시스템 양식 유형(SubscriptionTermsFormType아래 예제에서) 또는 사용자 지정 양식 유형을 사용하여 Amazon DataZone APIs을 통해서만 자산 유형을 생성할 수 있습니다. 시스템 양식 유형의 경우 유형 이름은 로 시작해야 합니다amazon.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,
        },
    },
)
```

다음은 구조화된 데이터에 대한 자산 유형을 생성하는 예제입니다.

```
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. 이제 위 단계에서 생성한 사용자 지정 자산 유형을 사용하여 자산을 생성할 수 있습니다.

```
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}"
        }
        ]
)
```

이 예제에서는 구조화된 데이터 자산을 생성합니다.

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

에 대한 Amazon DataZone 데이터 소스 생성 및 실행 AWS Glue Data Catalog

Amazon 에서는 AWS Glue Data Catalog 데이터 소스를 생성하여 에서 데이터베이스 테이블의 기술적 메타데이터를 가져올 DataZone수 있습니다 AWS Glue. 에 대한 데이터 소스를 추가하려면 소스 데이터베이스 AWS Glue Data Catalog가 에 이미 있어야 합니다 AWS Glue.

AWS Glue 데이터 소스를 생성하고 실행할 때 소스 AWS Glue 데이터베이스의 자산을 Amazon DataZone 프로젝트의 인벤토리에 추가합니다. 설정된 일정 또는 온디맨드로 AWS Glue 데이터 소스를 실행하여 자산의 기술 메타데이터를 생성하거나 업데이트할 수 있습니다. 데이터 소스가 실행되는

동안 선택적으로 자산을 Amazon DataZone 카탈로그에 게시하여 모든 도메인 사용자가 검색할 수 있도록 할 수 있습니다. 비즈니스 메타데이터를 편집한 후 프로젝트 인벤토리 자산을 게시할 수도 있습니다. 도메인 사용자는 게시된 자산을 검색 및 검색하고 이러한 자산에 대한 구독을 요청할 수 있습니다.

AWS Glue 데이터 소스를 추가하려면

1. Amazon DataZone 데이터 포털로 이동하여 Single Sign-On(SSO) 또는 자격 AWS 증명을 사용하여 URL 로그인합니다. Amazon DataZone 관리자인 경우 https://console.aws.amazon.com/datazone의 Amazon DataZone 콘솔로 이동하여 도메인이 생성된 AWS 계정 로 로그인한 다음 데이터 포털 열기를 선택합니다.
2. 상단 탐색 창에서 프로젝트 선택을 선택하고 데이터 소스를 추가할 프로젝트를 선택합니다.
3. 프로젝트의 데이터 탭으로 이동합니다.
4. 왼쪽 탐색 창에서 데이터 소스를 선택한 다음 데이터 소스 생성 을 선택합니다.
5. 다음 필드를 구성합니다.
   - 이름 - 데이터 소스 이름입니다.
   - 설명 - 데이터 소스 설명입니다.
6. 데이터 소스 유형에서 를 선택합니다AWS Glue.
7. 환경 선택에서 AWS Glue 테이블을 게시할 환경을 지정합니다.
8. 데이터 선택 에서 AWS Glue 데이터베이스를 제공하고 테이블 선택 기준을 입력합니다. 예를 들어 포함을 선택하고 를 입력하면 `*corporate`데이터베이스에 단어로 끝나는 모든 소스 테이블이 포함됩니다`corporate`.

   드롭다운에서 AWS Glue 데이터베이스를 선택하거나 데이터베이스 이름을 입력할 수 있습니다. 드롭다운에는 게시 데이터베이스와 환경의 구독 데이터베이스라는 두 개의 데이터베이스가 포함됩니다. 환경에서 생성하지 않은 데이터베이스에서 자산을 가져오려면 드롭다운에서 선택하는 대신 데이터베이스 이름을 입력해야 합니다.

   단일 데이터베이스 내에서 테이블에 대한 여러 포함 및 제외 규칙을 추가할 수 있습니다. 다른 데이터베이스 추가 버튼을 사용하여 여러 데이터베이스를 추가할 수도 있습니다.

9. 데이터 품질 에서 이 데이터 소스 에 대한 데이터 품질 활성화를 선택할 수 있습니다. 이렇게 하면 Amazon DataZone은 기존 AWS Glue 데이터 품질 출력을 Amazon DataZone 카탈로그로 가져옵니다. 기본적으로 Amazon은 AWS Glue에서 만료 날짜가 없는 최신 기존 100개 품질 보고서를 DataZone 가져옵니다.

Amazon의 데이터 품질 지표는 데이터 소스의 완전성과 정확성을 이해하는 데 DataZone 도움이 됩니다. Amazon은 예를 들어 비즈니스 데이터 카탈로그 검색 중에 컨텍스트를 제공하기 위해 AWS Glue에서 이러한 데이터 품질 지표를 DataZone 가져옵니다. 데이터 사용자는 구독한 자산에 대해 시간이 지남에 따라 데이터 품질 지표가 어떻게 변화하는지 확인할 수 있습니다. 데이터 생산자는 일정에 따라 AWS Glue 데이터 품질 점수를 수집할 수 있습니다. Amazon DataZone 비즈니스 데이터 카탈로그는 데이터 품질 을 통해 타사 시스템의 데이터 품질 지표를 표시할 수도 있습니다APIs. 자세한 내용은 Amazon의 데이터 품질 DataZone 단원을 참조하세요.

10. Next(다음)를 선택합니다.
11. 설정 게시 에서 비즈니스 데이터 카탈로그에서 자산을 즉시 검색할 수 있는지 여부를 선택합니다. 인벤토리에만 추가하는 경우 나중에 구독 조건을 선택하여 비즈니스 데이터 카탈로그에 게시할 수 있습니다.
12. 자동 비즈니스 이름 생성 에서 자산이 소스에서 가져올 때 자산에 대한 메타데이터를 자동으로 생성할지 여부를 선택합니다.
13. (선택 사항) 메타데이터 양식의 경우, Amazon 로 자산을 가져올 때 수집 및 저장되는 메타데이터를 정의하는 양식을 추가합니다 DataZone. 자세한 내용은 the section called “메타데이터 양식 생성” 단원을 참조하십시오.
14. 실행 기본 설정 에서 데이터 소스를 실행할 시기를 선택합니다.
    - 일정에 따라 실행 - 데이터 소스를 실행할 날짜와 시간을 지정합니다.
    - 온디맨드 실행 - 데이터 소스 실행을 수동으로 시작할 수 있습니다.
15. Next(다음)를 선택합니다.
16. 데이터 소스 구성을 검토하고 생성을 선택합니다.

> **Note**
>
> AWS Glue 데이터 소스가 생성되면 Amazon은 데이터 소스에 사용되는 AWS Glue 데이터베이스의 모든 테이블에 액세스하기 위해 데이터 소스를 생성하는 데 사용되는 환경의 IAM 역할에 대한 Lake Formation '읽기 전용' 권한을 DataZone 생성합니다. 환경의 세부 정보 페이지의 데이터 소스에서 이러한 권한 부여의 상태를 모니터링할 수 있습니다. Amazon은 AWS 게시 환경의 IAM 역할에 대한 액세스 권한을 부여할 때 Glue 데이터베이스에 다음 AWS 태그를 DataZone 추가합니다. `DataZoneDiscoverable_${domainId}: true`
> Amazon 의 현재 릴리스 이전에 생성된 환경의 경우 DataZone프로젝트 멤버는 Amazon Athena 에서 부여된 테이블을 볼 수 없습니다.

Amazon Redshift용 Amazon DataZone 데이터 소스 생성 및 실행

Amazon 에서는 Amazon Redshift 데이터 웨어하우스에서 데이터베이스 테이블 및 뷰의 기술적 메타데이터를 가져오기 위해 Amazon Redshift 데이터 소스를 생성할 DataZone수 있습니다. Amazon Redshift에 Amazon DataZone 데이터 소스를 추가하려면 소스 데이터 웨어하우스가 Amazon Redshift에 이미 있어야 합니다.

Amazon Redshift 데이터 소스를 생성하고 실행할 때 소스 Amazon Redshift 데이터 웨어하우스의 자산을 Amazon DataZone 프로젝트의 인벤토리에 추가합니다. Amazon Redshift 데이터 소스를 설정된 일정 또는 온디맨드로 실행하여 자산의 기술 메타데이터를 생성하거나 업데이트할 수 있습니다. 데이터 소스가 실행되는 동안 선택적으로 프로젝트 인벤토리 자산을 Amazon DataZone 카탈로그에 게시하여 모든 도메인 사용자가 검색할 수 있도록 할 수 있습니다. 비즈니스 메타데이터를 편집한 후 인벤토리 자산을 게시할 수도 있습니다. 도메인 사용자는 게시된 자산을 검색 및 검색하고 이러한 자산에 대한 구독을 요청할 수 있습니다.

Amazon Redshift 데이터 소스를 추가하려면

1. Amazon DataZone 데이터 포털로 이동하여 Single Sign-On(SSO) 또는 자격 AWS 증명을 사용하여 URL 로그인합니다. Amazon DataZone 관리자인 경우 https://console.aws.amazon.com/datazone의 Amazon DataZone 콘솔로 이동하여 도메인이 생성된 AWS 계정 로 로그인한 다음 데이터 포털 열기를 선택합니다.
2. 상단 탐색 창에서 프로젝트 선택을 선택하고 데이터 소스를 추가할 프로젝트를 선택합니다.
3. 프로젝트의 데이터 탭으로 이동합니다.
4. 왼쪽 탐색 창에서 데이터 소스를 선택한 다음 데이터 소스 생성을 선택합니다.
5. 다음 필드를 구성합니다.
   - 이름 - 데이터 소스 이름입니다.
   - 설명 - 데이터 소스 설명입니다.
6. 데이터 소스 유형에서 Amazon Redshift를 선택합니다.
7. 환경 선택에서 Amazon Redshift 테이블을 게시할 환경을 지정합니다.
8. 선택한 환경에 따라 Amazon DataZone 은 Amazon Redshift 보안 인증 정보 및 기타 파라미터를 환경에서 직접 자동으로 적용하거나 직접 선택할 수 있는 옵션을 제공합니다.
   - 환경의 기본 Amazon Redshift 스키마에서만 게시를 허용하는 환경을 선택한 경우 Amazon DataZone 은 Amazon Redshift 자격 증명과 Amazon Redshift 클러스터 또는 작업 그룹 이름, AWS 보안 암호, 데이터베이스 이름 및 스키마 이름을 포함한 기타 파라미터를 자동으로 적용합니다. 이러한 자동 채워진 파라미터는 편집할 수 없습니다.

- 에서 데이터를 게시할 수 없는 환경을 선택하면 데이터 소스 생성을 진행할 수 없습니다.
- 스키마에서 데이터를 게시할 수 있는 환경을 선택하면 환경의 보안 인증 정보 및 기타 Amazon Redshift 파라미터를 사용하거나 자체 보안 인증 정보/파라미터를 입력하는 옵션이 표시됩니다.

9. 자체 자격 증명을 사용하여 데이터 소스를 생성하도록 선택한 경우 다음 세부 정보를 제공합니다.

   - Amazon Redshift 보안 인증 정보 제공에서 프로비저닝된 Amazon Redshift 클러스터 또는 Amazon Redshift Serverless 워크스페이스를 데이터 소스로 사용할지 여부를 선택합니다.
   - 위 단계의 선택에 따라 드롭다운 메뉴에서 Amazon Redshift 클러스터 또는 작업 공간을 선택한 다음 AWS Secrets Manager에서 인증에 사용할 보안 암호를 선택합니다. 기존 보안 암호를 선택하거나 새 보안 암호를 생성할 수 있습니다.
   - 기존 보안 암호가 드롭다운에 표시되도록 하려면 AWS Secrets Manager의 보안 암호에 다음 태그(키/값)가 포함되어 있는지 확인합니다.
     - AmazonDataZoneProject: <projectID >
     - AmazonDataZoneDomain: <domainID >

     새 보안 암호를 생성하도록 선택하면 보안 암호에 위에 참조된 태그가 자동으로 지정되므로 추가 단계가 필요하지 않습니다. 자세한 내용은 의 데이터베이스 보안 인증 정보 저장을 참조하세요 AWS Secrets Manager.

     데이터 소스를 생성하기 위해 제공된 AWS 보안 암호의 Amazon Redshift 사용자는 게시할 테이블에 대한 SELECT 권한이 있어야 합니다. Amazon이 사용자를 대신하여 구독(액세스)도 관리 DataZone 하도록 하려면 보안 암호의 데이터베이스 사용자에게 AWS 다음 권한도 있어야 합니다.
     - `CREATE DATASHARE`
     - `ALTER DATASHARE`
     - `DROP DATASHARE`

10. 데이터 선택 에서 Amazon Redshift 데이터베이스, 스키마를 제공하고 테이블 또는 보기 선택 기준을 입력합니다. 예를 들어 포함을 선택하고 `*corporate`를 입력하면 자산에는 단어로 끝나는 모든 소스 테이블이 포함됩니다`corporate`.

    단일 데이터베이스 내에서 테이블에 대한 여러 포함 규칙을 추가할 수 있습니다. 다른 데이터베이스 추가 버튼을 사용하여 여러 데이터베이스를 추가할 수도 있습니다.

11. Next(다음)를 선택합니다.

12. 설정 게시 에서 데이터 카탈로그에서 자산을 즉시 검색할 수 있는지 여부를 선택합니다. 인벤토리에만 추가하는 경우 나중에 구독 조건을 선택하여 비즈니스 데이터 카탈로그에 게시할 수 있습니다.
13. 자동 비즈니스 이름 생성 에서 자산이 게시되고 소스에서 업데이트될 때 자산에 대한 메타데이터를 자동으로 생성할지 여부를 선택합니다.
14. (선택 사항) 메타데이터 양식의 경우, Amazon 로 자산을 가져올 때 수집 및 저장되는 메타데이터를 정의하는 양식을 추가합니다 DataZone. 자세한 내용은 the section called “메타데이터 양식 생성” 단원을 참조하십시오.
15. 실행 기본 설정 에서 데이터 소스를 실행할 시기를 선택합니다.
    - 일정에 따라 실행 - 데이터 소스를 실행할 날짜와 시간을 지정합니다.
    - 온디맨드 실행 - 데이터 소스 실행을 수동으로 시작할 수 있습니다.
16. Next(다음)를 선택합니다.
17. 데이터 소스 구성을 검토하고 생성을 선택합니다.

> **Note**
>
> Amazon Redshift 데이터 소스가 생성되면 Amazon은 데이터 소스에 사용되는 Amazon Redshift 스키마의 모든 테이블에 액세스하기 위해 데이터 소스를 생성하는 데 사용되는 환경에 대한 읽기 전용 액세스 권한을 DataZone 부여합니다. 환경의 세부 정보 페이지의 데이터 소스에서 이러한 권한 부여의 상태를 모니터링할 수 있습니다.
> 환경을 생성하는 데 사용되는 것과 다른 Amazon Redshift 클러스터 또는 Serverless 작업 그룹을 사용하는 경우 클러스터 또는 작업 그룹에 다음 AWS 태그가 추가되었는지 확인해야 합니다. 이는 환경 사용자가 Amazon Redshift 쿼리 편집기 V2에서 부여된 데이터베이스를 볼 수 있는 데 필요합니다. `DataZoneDiscoverable_${domainId}: true`
> Amazon 의 현재 릴리스 이전에 생성된 환경의 경우 DataZone프로젝트 멤버는 Amazon Redshift에서 부여된 테이블을 볼 수 없습니다.

Amazon에서 데이터 소스 편집 DataZone

Amazon DataZone 데이터 소스를 생성한 후 언제든지 수정하여 소스 세부 정보 또는 데이터 선택 기준을 변경할 수 있습니다. 더 이상 데이터 소스가 필요하지 않으면 삭제할 수 있습니다.

이 단계를 완료하려면 AmazonDataZoneFullAccess AWS 관리형 정책이 연결되어 있어야 합니다. 자세한 내용은 the section called “AWS 관리형 정책” 단원을 참조하십시오.

Amazon DataZone 데이터 소스를 편집하여 테이블 선택 기준 추가, 제거 또는 변경을 포함하여 데이터 선택 설정을 수정할 수 있습니다. 데이터베이스를 추가하고 제거할 수도 있습니다. 데이터 소스 유형 또는 데이터 소스가 게시되는 환경을 변경할 수 없습니다.

데이터 원본을 편집하려면

1. Amazon DataZone 데이터 포털로 이동하여 Single Sign-On(SSO) 또는 자격 AWS 증명을 사용하여 URL 로그인합니다. Amazon DataZone 관리자인 경우 https://console.aws.amazon.com/datazone의 Amazon DataZone 콘솔로 이동하여 도메인이 생성된 AWS 계정 로 로그인한 다음 데이터 포털 열기를 선택합니다.
2. 상단 탐색 창에서 프로젝트 선택을 선택하고 데이터 소스가 속한 프로젝트를 선택합니다.
3. 프로젝트의 데이터 탭으로 이동합니다.
4. 왼쪽 탐색 창에서 데이터 소스를 선택한 다음 수정하려는 데이터 소스를 선택합니다.
5. 데이터 소스 정의 탭으로 이동하여 편집을 선택합니다.
6. 데이터 소스 정의를 변경합니다. 데이터 소스 세부 정보를 업데이트하고 데이터 선택 기준을 변경할 수 있습니다.
7. 변경 작업을 마치면 저장을 선택합니다.

Amazon에서 데이터 소스 삭제 DataZone

Amazon DataZone 데이터 소스를 생성한 후 언제든지 수정하여 소스 세부 정보 또는 데이터 선택 기준을 변경할 수 있습니다.

이 단계를 완료하려면 AmazonDataZoneFullAccess AWS 관리형 정책이 연결되어 있어야 합니다. 자세한 내용은 the section called “AWS 관리형 정책” 단원을 참조하십시오.

Amazon DataZone 데이터 소스가 더 이상 필요하지 않은 경우 영구적으로 제거할 수 있습니다. 데이터 소스를 삭제한 후에도 해당 데이터 소스에서 시작된 모든 자산은 카탈로그에서 계속 사용할 수 있으며 사용자는 계속 구독할 수 있습니다. 그러나 자산은 소스로부터 업데이트 수신을 중지합니다. 종속 자산을 삭제하기 전에 먼저 다른 데이터 소스로 이동하는 것이 좋습니다.

> **Note**
>
> 데이터 소스를 삭제하려면 먼저 데이터 소스에서 모든 이행을 제거해야 합니다. 자세한 내용은 데이터 검색, 구독 및 소비 단원을 참조하십시오.

데이터 소스를 삭제하기

1. 프로젝트의 데이터 탭에서 왼쪽 탐색 창에서 데이터 소스를 선택합니다.
2. 삭제할 데이터 소스를 선택합니다.
3. 작업 , 데이터 소스 삭제를 선택하고 삭제를 확인합니다.

프로젝트 인벤토리에서 Amazon DataZone 카탈로그에 자산 게시

프로젝트 인벤토리의 Amazon DataZone 자산과 메타데이터를 Amazon DataZone 카탈로그에 게시할 수 있습니다. 최신 버전의 자산만 카탈로그에 게시할 수 있습니다.

카탈로그에 자산을 게시할 때는 다음 사항을 고려하세요.

- 카탈로그에 자산을 게시하려면 해당 프로젝트의 소유자 또는 기여자여야 합니다.
- Amazon Redshift 자산의 경우 Amazon이 Redshift 테이블 및 뷰에 대한 액세스를 관리하기 위해 게시자 및 구독자 클러스터와 연결된 Amazon Redshift 클러스터가 Amazon Redshift 데이터 공유에 대한 모든 요구 사항을 충족하는 DataZone 지 확인합니다. Amazon Redshift의 데이터 공유 개념을 참조하세요.
- Amazon은 AWS Glue Data Catalog 및 Amazon Redshift에서 게시된 자산에 대한 액세스 관리 DataZone 만 지원합니다. Amazon S3 객체와 같은 다른 모든 자산의 경우 Amazon DataZone은 승인된 구독자의 액세스를 관리하지 않습니다. 이러한 관리되지 않는 자산을 구독하면 다음 메시지가 표시됩니다.

  ```
  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.
  ```

Amazon에 자산 게시 DataZone

데이터 소스를 생성할 때 데이터 카탈로그에서 자산을 즉시 검색하도록 선택하지 않은 경우 다음 단계를 수행하여 나중에 게시합니다.

자산을 게시하려면

1. Amazon DataZone 데이터 포털로 이동하여 Single Sign-On(SSO) 또는 자격 AWS 증명을 사용하여 URL 로그인합니다. Amazon DataZone 관리자인 경우 https://console.aws.amazon.com/

datazone의 Amazon DataZone 콘솔로 이동하여 도메인이 생성된 AWS 계정 로 로그인한 다음 데이터 포털 열기를 선택합니다.

2. 상단 탐색 창에서 프로젝트 선택을 선택하고 자산이 속한 프로젝트를 선택합니다.
3. 프로젝트의 데이터 탭으로 이동합니다.
4. 왼쪽 탐색 창에서 인벤토리 데이터를 선택한 다음 게시할 자산을 선택합니다.

> **Note**
>
> 기본적으로 모든 자산에는 구독 승인이 필요합니다. 즉, 데이터 소유자가 자산에 대한 모든 구독 요청을 승인해야 합니다. 자산을 게시하기 전에 이 설정을 변경하려면 자산 세부 정보를 열고 구독 승인 옆의 편집을 선택합니다. 나중에 자산을 수정하고 다시 게시하여 이 설정을 변경할 수 있습니다.

5. 자산 게시를 선택합니다. 자산은 카탈로그에 직접 게시됩니다.

   승인 요구 사항 수정과 같이 자산을 변경하는 경우 다시 게시를 선택하여 카탈로그에 업데이트를 게시할 수 있습니다.

Amazon에서 인벤토리 관리 및 자산 큐레이트 DataZone

Amazon DataZone 을 사용하여 데이터를 카탈로그화하려면 먼저 Amazon 에서 프로젝트 인벤토리로 데이터(자산)를 가져와야 합니다 DataZone. 특정 프로젝트에 대한 인벤토리를 생성하면 해당 프로젝트의 구성원만 자산을 검색할 수 있습니다.

프로젝트 인벤토리에서 자산이 생성되면 메타데이터를 큐레이션할 수 있습니다. 예를 들어 자산의 이름, 설명을 편집하거나 내게 읽어줄 수 있습니다. 자산을 편집할 때마다 자산의 새 버전이 생성됩니다. 자산 세부 정보 페이지의 기록 탭을 사용하여 모든 자산 버전을 볼 수 있습니다.

Read Me 섹션을 편집하고 자산에 대한 풍부한 설명을 추가할 수 있습니다. Read Me 섹션은 가격 인하를 지원하므로 필요에 따라 설명을 포맷하고 자산에 대한 주요 정보를 소비자에게 설명할 수 있습니다.

용어집 용어는 사용 가능한 양식을 작성하여 자산 수준에서 추가할 수 있습니다.

스키마를 큐레이션하려면 열을 검토하고, 비즈니스 이름, 설명을 추가하고, 열 수준에서 용어집 용어를 추가할 수 있습니다.

데이터 소스가 생성될 때 자동 메타데이터 생성이 활성화된 경우 자산 및 열의 비즈니스 이름을 개별적으로 또는 모두 한 번에 검토하고 수락하거나 거부할 수 있습니다.

구독 조건을 편집하여 자산에 대한 승인이 필요한지 여부를 지정할 수도 있습니다.

Amazon의 메타데이터 양식을 DataZone 사용하면 사용자 지정 정의 속성(예: 영업 리전, 영업 연도 및 영업 분기)을 추가하여 데이터 자산의 메타데이터 모델을 확장할 수 있습니다. 자산 유형에 연결된 메타데이터 양식은 해당 자산 유형에서 생성된 모든 자산에 적용됩니다. 데이터 소스 실행의 일부로 또는 생성된 후 개별 자산에 메타데이터 양식을 추가할 수도 있습니다. 새 양식을 생성하려면 섹션을 참조하세요the section called “메타데이터 양식 생성”.

자산의 메타데이터를 업데이트하려면 자산이 속한 프로젝트의 소유자 또는 기여자여야 합니다.

자산의 메타데이터를 업데이트하려면

1. Amazon DataZone 데이터 포털로 이동하여 Single Sign-On(SSO) 또는 자격 AWS 증명을 사용하여 URL 로그인합니다. Amazon DataZone 관리자인 경우 https://console.aws.amazon.com/datazone의 Amazon DataZone 콘솔로 이동하여 도메인이 생성된 AWS 계정 로 로그인한 다음 데이터 포털 열기를 선택합니다.
2. 상단 탐색 창에서 프로젝트 선택을 선택하고 업데이트하려는 메타데이터의 자산이 포함된 프로젝트를 선택합니다.
3. 프로젝트의 데이터 탭으로 이동합니다.
4. 왼쪽 탐색 창에서 인벤토리 데이터를 선택한 다음 업데이트하려는 메타데이터의 자산 이름을 선택합니다.
5. 자산 세부 정보 페이지의 메타데이터 양식에서 필요에 따라 기존 양식 편집 및 편집을 선택합니다. 추가 메타데이터 양식을 자산에 연결할 수도 있습니다. 자세한 내용은 the section called “자산에 추가 메타데이터 양식 연결” 단원을 참조하십시오.
6. 업데이트가 완료되면 양식 저장을 선택합니다.

   양식을 저장하면 Amazon이 자산의 새 인벤토리 버전을 DataZone 생성합니다. 업데이트된 버전을 카탈로그에 게시하려면 자산 다시 게시를 선택합니다.

자산에 추가 메타데이터 양식 연결

기본적으로 도메인에 연결된 메타데이터 양식은 해당 도메인에 게시된 모든 자산에 연결됩니다. 데이터 게시자는 추가 컨텍스트를 제공하기 위해 추가 메타데이터 양식을 개별 자산에 연결할 수 있습니다.

자산에 추가 메타데이터 양식을 연결하려면

1. Amazon DataZone 데이터 포털로 이동하여 Single Sign-On(SSO) 또는 자격 AWS 증명을 사용하여 URL 로그인합니다. Amazon DataZone 관리자인 경우 https://console.aws.amazon.com/

datazone의 Amazon DataZone 콘솔로 이동하여 도메인이 생성된 AWS 계정 로 로그인한 다음 데이터 포털 열기를 선택합니다.

2. 상단 탐색 창에서 프로젝트 선택을 선택하고 메타데이터를 추가하려는 자산이 포함된 프로젝트를 선택합니다.
3. 프로젝트의 데이터 탭으로 이동합니다.
4. 왼쪽 탐색 창에서 인벤토리 데이터를 선택한 다음 메타데이터를 추가할 자산의 이름을 선택합니다.
5. 자산 세부 정보 페이지의 메타데이터 양식에서 양식 추가를 선택합니다.
6. 자산에 추가할 양식(들)을 선택한 다음 양식 추가를 선택합니다.
7. 각 메타데이터 필드의 값을 입력한 다음 양식 저장을 선택합니다.

   양식을 저장하면 Amazon이 자산의 새 인벤토리 버전을 DataZone 생성합니다. 업데이트된 버전을 카탈로그에 게시하려면 자산 다시 게시를 선택합니다.

Amazon에서 큐레이션 후 카탈로그에 자산 게시 DataZone

자산 큐레이션에 만족하면 데이터 소유자는 자산 버전을 Amazon DataZone 카탈로그에 게시하여 모든 도메인 사용자가 검색할 수 있도록 할 수 있습니다. 자산에는 인벤토리 버전과 게시된 버전이 표시됩니다. 검색 카탈로그에는 게시된 최신 버전만 표시됩니다. 게시 후 메타데이터가 업데이트되면 카탈로그에 게시할 새 인벤토리 버전을 사용할 수 있습니다.

Amazon에서 수동으로 자산 생성 DataZone

Amazon 에서 DataZone자산은 단일 물리적 데이터 객체(예: 테이블, 대시보드, 파일) 또는 가상 데이터 객체(예: 뷰)를 제공하는 엔터티입니다. 자세한 내용은 Amazon DataZone 용어 및 개념 단원을 참조하십시오. 자산을 수동으로 게시하는 것은 일회성 작업입니다. 자산에 대한 실행 일정을 지정하지 않으므로 소스가 변경되면 자동으로 업데이트되지 않습니다.

프로젝트를 통해 자산을 수동으로 생성하려면 해당 프로젝트의 소유자 또는 기여자여야 합니다.

자산을 수동으로 생성하려면

1. Amazon DataZone 데이터 포털로 이동하여 Single Sign-On(SSO) 또는 자격 AWS 증명을 사용하여 URL 로그인합니다. Amazon DataZone 관리자인 경우 https://console.aws.amazon.com/datazone의 Amazon DataZone 콘솔로 이동하여 도메인이 생성된 AWS 계정 로 로그인한 다음 데이터 포털 열기를 선택합니다.

2. 상단 탐색 창에서 프로젝트 선택을 선택하고 자산을 생성할 프로젝트를 선택합니다.
3. 프로젝트의 데이터 탭으로 이동합니다.
4. 왼쪽 탐색 창에서 데이터 소스를 선택한 다음 데이터 자산 생성 을 선택합니다.
5. 자산 세부 정보 에서 다음 설정을 구성합니다.

   - 자산 유형 - 자산 유형입니다.
   - 이름 - 자산의 이름입니다.
   - 설명 - 자산에 대한 설명입니다.
6. S3 위치 에 소스 S3 버킷의 Amazon 리소스 이름(ARN)을 입력합니다.

   선택적으로 S3 액세스 포인트를 입력합니다. 자세한 내용을 알아보려면 Amazon S3 액세스 지점을 사용한 데이터 액세스 관리를 참조하십시오.
7. 게시 설정 에서 카탈로그에서 자산을 즉시 검색할 수 있는지 여부를 선택합니다. 인벤토리에만 추가하는 경우 나중에 구독 조건을 선택하여 카탈로그에 게시할 수 있습니다.
8. 생성(Create)을 선택합니다.

   자산이 생성되면 카탈로그에 활성 자산으로 직접 게시되거나 게시하기로 결정할 때까지 인벤토리에 저장됩니다.

Amazon DataZone 카탈로그에서 자산 게시 취소

카탈로그에서 Amazon DataZone 자산을 게시 취소하면 글로벌 검색 결과에 더 이상 표시되지 않습니다. 신규 사용자는 카탈로그의 자산 목록을 찾거나 구독할 수 없지만 기존 구독은 모두 동일합니다.

자산을 게시 취소하려면 자산이 속한 프로젝트의 소유자 또는 기여자여야 합니다.

자산을 게시 취소하려면

1. Amazon DataZone 데이터 포털로 이동하여 Single Sign-On(SSO) 또는 자격 AWS 증명을 사용하여 URL 로그인합니다. Amazon DataZone 관리자인 경우 https://console.aws.amazon.com/datazone의 Amazon DataZone 콘솔로 이동하여 도메인이 생성된 AWS 계정 로 로그인한 다음 데이터 포털 열기를 선택합니다.
2. 상단 탐색 창에서 프로젝트 선택을 선택하고 자산이 속한 프로젝트를 선택합니다.
3. 프로젝트의 데이터 탭으로 이동합니다.
4. 왼쪽 탐색 창에서 게시된 데이터를 선택합니다.
5. 게시된 자산 목록에서 자산을 찾은 다음 게시 취소를 선택합니다.

카탈로그에서 자산이 제거됩니다. 게시를 선택하여 언제든지 자산을 다시 게시할 수 있습니다.

Amazon DataZone 자산 삭제

Amazon 에서 자산이 더 이상 필요하지 않으면 영구적으로 삭제할 DataZone수 있습니다. 자산을 삭제하는 것은 카탈로그에서 자산을 게시 취소하는 것과 다릅니다. 검색 결과에 자산과 관련 목록이 표시되지 않도록 카탈로그에서 자산 및 관련 목록을 삭제할 수 있습니다. 자산 목록을 삭제하려면 먼저 모든 구독을 취소해야 합니다.

자산을 삭제하려면 자산이 속한 프로젝트의 소유자 또는 기여자여야 합니다.

> **Note**
>
> 자산 목록을 삭제하려면 먼저 자산에 대한 기존 구독을 모두 취소해야 합니다. 기존 구독자가 있는 자산 목록은 삭제할 수 없습니다.

및 자산을 삭제하려면

1. Amazon DataZone 데이터 포털로 이동하여 Single Sign-On(SSO) 또는 자격 AWS 증명을 사용하여 URL 로그인합니다. Amazon DataZone 관리자인 경우 https://console.aws.amazon.com/datazone의 Amazon DataZone 콘솔로 이동하여 도메인이 생성된 AWS 계정 로 로그인한 다음 데이터 포털 열기를 선택합니다.
2. 상단 탐색 창에서 프로젝트 선택을 선택하고 삭제할 자산이 포함된 프로젝트를 선택합니다.
3. 프로젝트의 데이터 탭으로 이동합니다.
4. 왼쪽 탐색 창에서 게시된 데이터를 선택한 다음 삭제할 자산을 찾아 선택합니다. 그러면 자산 세부정보 페이지가 열립니다.
5. 작업 , 삭제를 선택하고 삭제를 확인합니다.

   자산이 삭제되면 더 이상 볼 수 없으며 사용자는 자산을 구독할 수 없습니다.

Amazon에서 데이터 소스 실행 수동 시작 DataZone

데이터 소스를 실행하면 Amazon은 소스에서 모든 새 메타데이터 또는 수정된 메타데이터를 DataZone 가져와 인벤토리의 관련 자산을 업데이트합니다. Amazon 에 데이터 소스를 추가할 때 소스

의 실행 기본 설정을 DataZone지정합니다. 이 기본 설정은 소스가 일정에 따라 실행되는지 아니면 온디맨드 방식으로 실행되는지를 정의합니다. 소스가 필요에 따라 실행되는 경우 데이터 소스 실행을 수동으로 시작해야 합니다.

소스가 일정에 따라 실행되더라도 언제든지 수동으로 실행할 수 있습니다. 자산에 비즈니스 메타데이터를 추가한 후 자산을 선택하고 Amazon DataZone 카탈로그에 게시하여 모든 도메인 사용자가 이러한 자산을 검색할 수 있도록 할 수 있습니다. 게시된 자산만 다른 도메인 사용자가 검색할 수 있습니다.

데이터 소스를 수동으로 실행하려면

1. Amazon DataZone 데이터 포털로 이동하여 Single Sign-On(SSO) 또는 자격 AWS 증명을 사용하여 URL 로그인합니다. Amazon DataZone 관리자인 경우 https://console.aws.amazon.com/datazone의 Amazon DataZone 콘솔로 이동하여 도메인이 생성된 AWS 계정 로 로그인한 다음 데이터 포털 열기를 선택합니다.
2. 상단 탐색 창에서 프로젝트 선택을 선택하고 데이터 소스가 속한 프로젝트를 선택합니다.
3. 프로젝트의 데이터 탭으로 이동합니다.
4. 왼쪽 탐색 창에서 데이터 소스를 선택한 다음 실행할 데이터 소스를 찾아 선택합니다. 그러면 데이터 소스 세부 정보 페이지가 열립니다.
5. 온디맨드 실행을 선택합니다.

   Amazon이 자산 메타데이터를 소스의 최신 데이터로 DataZone 업데이트Running하면 데이터 소스 상태가 로 변경됩니다. 데이터 소스 실행 탭에서 실행 상태를 모니터링할 수 있습니다.

Amazon의 자산 개정 DataZone

Amazon은 비즈니스 또는 기술 메타데이터를 편집할 때 자산의 개정을 DataZone 증가시킵니다. 이러한 편집에는 자산 이름, 설명, 용어집 용어, 열 이름, 메타데이터 양식 및 메타데이터 양식 필드 값 수정이 포함됩니다. 이러한 변경은 수동 편집, 데이터 소스 작업 실행 또는 API 작업으로 인해 발생할 수 있습니다. Amazon은 자산을 편집할 때마다 새 자산 개정을 DataZone 자동으로 생성합니다.

자산을 업데이트하고 새 개정이 생성된 후에는 새 개정을 카탈로그에 게시하여 구독자가 업데이트하고 사용할 수 있도록 해야 합니다. 자세한 내용은 the section called “프로젝트 인벤토리에서 카탈로그에 자산 게시” 단원을 참조하십시오. 최신 버전의 자산만 카탈로그에 게시할 수 있습니다.

자산의 이전 개정을 보려면

1. Amazon DataZone 데이터 포털로 이동하여 Single Sign-On(SSO) 또는 자격 AWS 증명을 사용하여 URL 로그인합니다. Amazon DataZone 관리자인 경우 https://console.aws.amazon.com/

datazone의 Amazon DataZone 콘솔로 이동하여 도메인이 생성된 AWS 계정 로 로그인한 다음 데이터 포털 열기를 선택합니다.

2. 상단 탐색 창에서 프로젝트 선택을 선택하고 자산이 포함된 프로젝트를 선택합니다.
3. 프로젝트의 데이터 탭으로 이동한 다음 자산을 찾아 선택합니다. 그러면 자산 세부 정보 페이지가 열립니다.
4. 자산의 과거 개정 목록을 표시하는 기록 탭으로 이동합니다.

Amazon의 데이터 품질 DataZone

Amazon의 데이터 품질 지표는 데이터 소스의 완전성, 적시성 및 정확성과 같은 다양한 품질 지표를 이해하는 데 DataZone 도움이 됩니다. Amazon DataZone은 AWS Glue 데이터 품질과 통합하고 를 제공하여 타사 데이터 품질 솔루션의 데이터 품질 지표APIs를 통합합니다. 데이터 사용자는 구독한 자산에 대해 시간이 지남에 따라 데이터 품질 지표가 어떻게 변화하는지 확인할 수 있습니다. 데이터 품질 규칙을 작성하고 실행하려면 AWS Glue 데이터 품질과 같이 선택한 데이터 품질 도구를 사용할 수 있습니다. Amazon 의 데이터 품질 지표를 사용하면 DataZone데이터 소비자는 자산 및 열의 데이터 품질 점수를 시각화하여 결정에 사용하는 데이터에 대한 신뢰를 구축할 수 있습니다.

사전 조건 및 IAM 역할 변경

Amazon DataZone의 AWS 관리형 정책을 사용하는 경우 추가 구성 단계가 없으며 이러한 관리형 정책은 데이터 품질을 지원하기 위해 자동으로 업데이트됩니다. Amazon에 지원되는 서비스와 상호 운용하는 데 DataZone 필요한 권한을 부여하는 역할에 대해 자체 정책을 사용하는 경우, 에서 AWS Glue 데이터 품질 정보를 읽을 수 있도록 지원하고 AWS 관리형 정책: AmazonDataZoneGlueManageAccessRolePolicy 및 APIs AWS 관리형 정책: AmazonDataZoneDomainExecutionRolePolicy 에서 시계열에 대한 지원을 활성화하도록 이러한 역할에 연결된 정책을 업데이트해야 합니다AWS 관리형 정책: AmazonDataZoneFullUserAccess.

AWS Glue 자산에 대한 데이터 품질 활성화

Amazon은 AWS Glue에서 데이터 품질 지표를 DataZone 가져와서 특정 시점, 예를 들어 비즈니스 데이터 카탈로그 검색 중에 컨텍스트를 제공합니다. 데이터 사용자는 구독한 자산에 대해 시간이 지남에 따라 데이터 품질 지표가 어떻게 변화하는지 확인할 수 있습니다. 데이터 생산자는 일정에 따라 AWS Glue 데이터 품질 점수를 수집할 수 있습니다. Amazon DataZone 비즈니스 데이터 카탈로그는 데이터 품질 을 통해 타사 시스템의 데이터 품질 지표를 표시할 수도 있습니다APIs. 자세한 내용은 AWS Glue 데이터 품질 및 데이터 카탈로그 의 AWS Glue 데이터 품질 시작하기를 참조하세요.

다음과 같은 방법으로 Amazon DataZone 자산에 대한 데이터 품질 지표를 활성화할 수 있습니다.

- 데이터 포털 또는 Amazon DataZone APIs을 사용하여 새 AWS Glue 데이터 소스를 생성하거나 기존 Glue 데이터 소스를 편집하는 동안 Amazon DataZone 데이터 포털을 통해 AWS Glue 데이터 소스에 대한 데이터 품질을 활성화합니다.

  포털을 통해 데이터 소스에 대한 데이터 품질을 활성화하는 방법에 대한 자세한 내용은 섹션을 참조하세요에 대한 Amazon DataZone 데이터 소스 생성 및 실행 AWS Glue Data Catalog.

  > **Note**
  >
  > Data Portal을 사용하여 Glue 인벤토리 자산에 대해서만 데이터 품질을 활성화할 수 있습니다 AWS . 이번 릴리스에서는 데이터 포털을 통해 Amazon Redshift 또는 사용자 지정 유형 자산에 대한 데이터 품질 DataZone 활성화가 지원되지 않습니다.

  APIs 를 사용하여 새 또는 기존 데이터 소스에 대한 데이터 품질을 활성화할 수도 있습니다. CreateDataSource 또는 를 호출UpdateDataSource하고 `autoImportDataQualityResult` 파라미터를 'True'로 설정하여 이 작업을 수행할 수 있습니다.

  데이터 품질이 활성화된 후 필요에 따라 또는 일정에 따라 데이터 소스를 실행할 수 있습니다. 각 실행은 자산당 최대 100개의 지표를 가져올 수 있습니다. 데이터 품질을 위해 데이터 소스를 사용할 때는 양식을 생성하거나 지표를 수동으로 추가할 필요가 없습니다. 자산이 게시되면 데이터 품질 양식(이력 규칙당 최대 30개의 데이터 포인트)에 대한 업데이트가 소비자 목록에 반영됩니다. 그런 다음 자산에 지표를 새로 추가할 때마다 목록에 자동으로 추가됩니다. 소비자가 최신 점수를 사용할 수 있도록 자산을 다시 게시할 필요가 없습니다.

사용자 지정 자산 유형에 대한 데이터 품질 활성화

Amazon DataZone APIs을 사용하여 사용자 지정 유형 자산에 대한 데이터 품질을 활성화할 수 있습니다. 자세한 내용은 다음 자료를 참조하세요.

- PostTimeSeriesDataPoints
- ListTimeSeriesDataPoints
- GetTimeSeriesDataPoint
- DeleteTimeSeriesDataPoints

다음 단계에서는 APIs 또는 CLI 를 사용하여 Amazon 의 자산에 대한 타사 지표를 가져오는 예를 제공합니다. DataZone

1. 다음과 PostTimeSeriesDataPoints API 같이 를 호출합니다.

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

다음 페이로드 포함:

```
"domainId": "dzd_5oo7xzoqltu8mf",
    "entityId": "4wyh64k2n8czaf",
    "entityType": "ASSET",
    "form": {
        "content": "{\n  \"evaluations\" : [ {\n    \"types\" : [ \"MaximumLength
\" ],\n    \"description\" : \"ColumnLength \\\"ShippingCountry\\\" <= 6\",\n
   \"details\" : { },\n    \"applicableFields\" : [ \"ShippingCountry\" ],\n
   \"status\" : \"PASS\"\n  }, {\n    \"types\" : [ \"MaximumLength\" ],\n
 \"description\" : \"ColumnLength \\\"ShippingState\\\" <= 2\",\n    \"details
\" : { },\n    \"applicableFields\" : [ \"ShippingState\" ],\n    \"status\" :
 \"PASS\"\n  }, {\n    \"types\" : [ \"MaximumLength\" ],\n    \"description
\" : \"ColumnLength \\\"ShippingCity\\\" <= 8\",\n    \"details\" : { },\n
 \"applicableFields\" : [ \"ShippingCity\" ],\n    \"status\" : \"PASS\"\n  },
 {\n    \"types\" : [ \"Completeness\" ],\n    \"description\" : \"Completeness \
\\"ShippingStreet\\\" >= 0.59\",\n    \"details\" : { },\n    \"applicableFields
\" : [ \"ShippingStreet\" ],\n    \"status\" : \"PASS\"\n  }, {\n    \"types\" :
 [ \"MaximumLength\" ],\n    \"description\" : \"ColumnLength \\\"ShippingStreet\\
\" <= 101\",\n    \"details\" : { },\n    \"applicableFields\" : [ \"ShippingStreet
\" ],\n    \"status\" : \"PASS\"\n  }, {\n    \"types\" : [ \"MaximumLength\" ],\n
    \"description\" : \"ColumnLength \\\"BillingCountry\\\" <= 6\",\n    \"details
\" : { },\n    \"applicableFields\" : [ \"BillingCountry\" ],\n    \"status\" :
 \"PASS\"\n  }, {\n    \"types\" : [ \"Completeness\" ],\n    \"description\" :
 \"Completeness \\\"biLlingcountry\\\" >= 0.5\",\n    \"details\" : {\n
 \"EVALUATION_MESSAGE\" : \"Value: 0.26666666666666666 does not meet the constraint
 requirement!\"\n    },\n    \"applicableFields\" : [ \"biLlingcountry\" ],\n
    \"status\" : \"FAIL\"\n  }, {\n    \"types\" : [ \"Completeness\" ],\n
 \"description\" : \"Completeness \\\"Billingstreet\\\" >= 0.5\",\n    \"details
\" : { },\n    \"applicableFields\" : [ \"Billingstreet\" ],\n    \"status\" :
 \"PASS\"\n  } ],\n  \"passingPercentage\" : 88.0,\n  \"evaluationsCount\" : 8\n}",
        "formName": "shortschemaruleset",
        "id": "athp9dyw75gzhj",
        "timestamp": 1.71700477757E9,
        "typeIdentifier": "amazon.datazone.DataQualityResultFormType",
```

```
        "typeRevision": "8"
    },
    "formName": "shortschemaruleset"
}
```

GetFormType 작업을 호출하여 이 페이로드를 가져올 수 있습니다.

```
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. 다음과 DeleteTimeSeriesDataPoints API 같이 를 호출합니다.

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

Amazon에서 기계 학습 및 생성형 AI 사용 DataZone

> **Note**
>
> Amazon Bedrock 기반:자동 남용 탐지 AWS 를 구현합니다. Amazon의 설명 기능에 대한 AI 권장 사항은 Amazon Bedrock을 기반으로 DataZone 구축되므로 사용자는 Amazon Bedrock에 구현된 제어를 상속하여 AI의 안전, 보안 및 책임 있는 사용을 적용합니다.

Amazon 의 현재 릴리스에서는 설명 기능에 대한 AI 권장 사항을 사용하여 데이터 검색 및 카탈로그 작성을 자동화할 DataZone수 있습니다. Amazon에서 생성형 AI 및 기계 학습을 지원하면 자산 및 열에 대한 설명이 DataZone 생성됩니다. 이 설명을 사용하여 데이터에 대한 비즈니스 컨텍스트를 추가하고 데이터 검색 결과를 높이는 데 도움이 될 수 있는 데이터 세트 분석을 추천할 수 있습니다.

Amazon Bedrock의 대규모 언어 모델로 구동되는 Amazon의 데이터 자산 설명에 대한 AI 권장 사항은 데이터를 이해하고 쉽게 검색할 수 있도록 하는 데 DataZone 도움이 됩니다. AI 권장 사항은 데이터 세

트에 가장 적합한 분석 애플리케이션도 제안합니다. 수동 문서화 작업을 줄이고 적절한 데이터 사용에 대한 조언을 제공하면 자동 생성된 설명을 통해 데이터의 신뢰성을 높이고 중요한 데이터의 간과를 최소화하여 정보에 입각한 의사 결정을 가속화할 수 있습니다.

> **Important**
>
> 현재 Amazon DataZone 릴리스에서는 설명 기능에 대한 AI 권장 사항이 다음 리전에서만 지원됩니다.
>
> - 미국 동부(버지니아 북부)
> - 미국 서부(오리건)
> - 유럽(프랑크푸르트)
> - 아시아 태평양(도쿄)

다음 절차에서는 Amazon 에서 설명에 대한 AI 권장 사항을 생성하는 방법을 설명합니다 DataZone.

1. Amazon DataZone 데이터 포털 로 이동URL한 다음 Single Sign-On(SSO) 또는 자격 AWS 증명을 사용하여 로그인합니다. Amazon DataZone 관리자인 경우 https://console.aws.amazon.com/datazone의 Amazon DataZone 콘솔로 이동하여 도메인이 생성된 AWS 계정 로 로그인한 다음 데이터 포털 열기를 선택합니다.
2. 상단 탐색 창에서 프로젝트 선택을 선택한 다음 설명에 대한 AI 권장 사항을 생성하려는 자산이 포함된 프로젝트를 선택합니다.
3. 프로젝트의 데이터 탭으로 이동합니다.
4. 왼쪽 탐색 창에서 인벤토리 데이터 를 선택한 다음, 자산에 대한 설명을 위한 AI 권장 사항을 생성하려는 자산의 이름을 선택합니다.
5. 자산의 세부 정보 페이지의 비즈니스 메타데이터 탭에서 설명 생성을 선택합니다.
6. 설명이 생성되면 설명을 편집, 수락 또는 거부할 수 있습니다. 녹색 아이콘은 데이터 자산에 대해 자동으로 생성된 각 메타데이터 설명 옆에 표시됩니다. 비즈니스 메타데이터 탭에서 자동으로 생성된 요약 옆의 녹색 아이콘을 선택한 다음 편집, 수락 또는 거부를 선택하여 생성된 설명을 처리할 수 있습니다. 비즈니스 메타데이터 탭이 선택된 경우 페이지 상단에 표시되는 모든 옵션 수락 또는 모든 옵션 거부를 선택하여 자동으로 생성된 모든 설명에 대해 선택한 작업을 수행할 수도 있습니다.

   또는 스키마 탭을 선택한 다음 한 번에 하나의 열 설명에 대해 녹색 아이콘을 선택한 다음 수락 또는 거부를 선택하여 자동으로 생성된 설명을 개별적으로 처리할 수 있습니다. 스키마 탭에서 모두

수락 또는 모두 거부를 선택하여 자동으로 생성된 모든 설명에 대해 선택한 작업을 수행할 수도 있습니다.

7. 생성된 설명과 함께 자산을 카탈로그에 게시하려면 자산 게시 를 선택한 다음 자산 게시 팝업 창에서 자산 다시 게시를 선택하여 이 작업을 확인합니다.

> **Note**
>
> 자산에 대해 생성된 설명을 수락하거나 거부하지 않은 다음 이 자산을 게시하면 검토되지 않은 이 자동 생성된 메타데이터는 게시된 데이터 자산에 포함되지 않습니다.

Amazon의 데이터 계보 DataZone (미리 보기)

> **Important**
>
> 현재 Amazon의 데이터 계보 기능은 미리 보기 릴리스에 DataZone 있습니다.

Amazon의 데이터 계보 DataZone 는 OpenLineageAPI-활성화된 시스템에서 또는 를 통해 계보 이벤트를 캡처하고 시각화APIs하여 데이터 오리진을 추적하고, 변환을 추적하고, 조직 간 데이터 소비를 보는 데 도움이 될 수 있는 호환되는 구동 OpenLineage기능입니다. 데이터 자산에 대한 포괄적인 뷰를 제공하여 자산의 오리진과 연결 체인을 확인할 수 있습니다. 계보 데이터에는 카탈로그화된 자산, 해당 자산의 구독자 및 를 사용하여 프로그래밍 방식으로 캡처된 DataZone비즈니스 데이터 카탈로그 외부에서 발생하는 활동에 대한 정보를 포함하여 Amazon 의 비즈니스 데이터 카탈로그 내 활동에 대한 정보가 포함됩니다APIs.

Amazon DataZone의 OpenLineage호환 APIs를 사용하면 도메인 관리자 및 데이터 생산자는 Amazon S3 DataZone, AWS Glue 및 기타 서비스의 변환을 포함하여 Amazon 에서 사용할 수 있는 것 이상의 계보 이벤트를 캡처하고 저장할 수 있습니다. 이를 통해 데이터 소비자에게 포괄적인 뷰를 제공하고 자산의 오리진에 대한 확신을 얻는 데 도움이 되며, 데이터 생산자는 사용량을 이해하여 자산에 대한 변경의 영향을 평가할 수 있습니다. 또한 Amazon은 각 이벤트와 함께 계보를 DataZone 버전하므로 사용자는 언제든지 계보를 시각화하거나 자산 또는 작업 기록 전반의 변환을 비교할 수 있습니다. 이 과거 계보는 데이터 자산의 문제 해결, 감사 및 무결성 보장에 필수적인 데이터가 어떻게 진화했는지에 대한 심층적인 이해를 제공합니다.

데이터 계보를 사용하면 Amazon 에서 다음을 수행할 수 있습니다 DataZone.

- 데이터의 출처 이해: 데이터의 출처를 파악하면 데이터의 출처, 종속성 및 변환을 명확하게 이해하여 데이터에 대한 신뢰를 높일 수 있습니다. 이러한 투명성은 신뢰할 수 있는 데이터 기반 결정을 내리는 데 도움이 됩니다.
- 데이터 파이프라인에 대한 변경 사항의 영향 이해: 데이터 파이프라인이 변경되면 계보를 사용하여 영향을 받을 모든 다운스트림 소비자를 식별할 수 있습니다. 이렇게 하면 중요한 데이터 흐름을 중단하지 않고 변경 사항을 적용할 수 있습니다.
- 데이터 품질 문제의 근본 원인을 식별합니다. 다운스트림 보고서에서 데이터 품질 문제가 감지되는 경우, 계보, 특히 열 수준 계보를 사용하여 데이터를 역추적(열 수준에서)하여 해당 문제를 소스로 다시 식별할 수 있습니다. 이렇게 하면 데이터 엔지니어가 문제를 식별하고 해결하는 데 도움이 될 수 있습니다.
- 데이터 거버넌스 및 규정 준수 개선: 열 수준 계보를 사용하여 데이터 거버넌스 및 개인정보 보호 규정 준수를 입증할 수 있습니다. 예를 들어 열 수준 계보를 사용하여 민감한 데이터(예: PII)가 저장되는 위치와 다운스트림 활동에서 처리되는 방법을 표시할 수 있습니다.

Amazon의 계보 노드 유형 DataZone

Amazon 에서 DataZone데이터 계보 정보는 테이블 및 뷰를 나타내는 노드로 표시됩니다. 예를 들어 데이터 포털의 왼쪽 상단에서 선택한 프로젝트와 같이 프로젝트의 컨텍스트에 따라 생산자는 인벤토리 및 게시된 자산을 모두 볼 수 있는 반면 소비자는 게시된 자산만 볼 수 있습니다. 자산 세부 정보 페이지에서 계보 탭을 처음 열면 카탈로그화된 데이터 세트 노드가 계보 그래프의 계보 노드를 통해 업스트림 또는 다운스트림을 탐색하기 위한 시작점입니다.

다음은 Amazon 에서 지원되는 데이터 계보 노드의 유형입니다 DataZone.

- 데이터 세트 노드 - 이 노드 유형에는 특정 데이터 자산에 대한 데이터 계보 정보가 포함됩니다.
  - Amazon DataZone 카탈로그에 게시된 AWS Glue 또는 Amazon Redshift 자산에 대한 정보가 포함된 데이터 세트 노드는 자동으로 생성되며 노드 내에 해당 AWS Glue 또는 Amazon Redshift 아이콘이 포함됩니다.
  - Amazon DataZone 카탈로그에 게시되지 않은 자산에 대한 정보가 포함된 데이터 세트 노드는 도메인 관리자(생산자)가 수동으로 생성하며 노드 내의 기본 사용자 지정 자산 아이콘으로 표시됩니다.
- 작업(실행) 노드 - 이 노드 유형은 특정 작업의 최신 실행 및 실행 세부 정보를 포함하여 작업의 세부 정보를 표시합니다. 또한 이 노드는 여러 작업 실행을 캡처하며 노드 세부 정보의 기록 탭에서 볼 수 있습니다. 노드 아이콘을 선택하여 노드 세부 정보를 볼 수 있습니다.

계보 노드의 키 속성

계보 노드의 `sourceIdentifier` 속성은 데이터 세트에서 발생하는 이벤트를 나타냅니다. 계보 노드`sourceIdentifier`의 는 데이터 세트의 식별자(테이블/보기 등)입니다. 계보 노드에서 고유성을 적용하는 데 사용됩니다. 예를 들어 가 동일한 계보 노드는 두 개일 수 없습니다`sourceIdentifier`. 다음은 다양한 유형의 노드에 대한 `sourceIdentifier` 값의 예입니다.

- 각 데이터 세트 유형이 있는 데이터 세트 노드의 경우:
  - 자산: amazon.datazone.asset/<assetId>
  - 목록(게시된 자산): amazon.datazone.listing/<listingId>
  - AWS Glue 테이블: arn:aws:glue:<region>:<account-id>:table/<database>/<table-name>
  - Amazon Redshift 테이블/보기: arn:aws:<redshift/redshift-serverless>:<region>:<account-id>:<table-type(table/view etc)>/<clusterIdentifier/workgroupName>/<database>/<schema>/<table-name>
  - 오픈 리니지 실행 이벤트를 사용하여 가져온 다른 유형의 데이터 세트 노드의 경우 노드 `sourceIdentifier` 기준으로 입력/출력 데이터 세트의 <namespace>/<name>이 사용됩니다.
- 작업의 경우:
  - 오픈 리니지 실행 이벤트를 사용하여 가져온 작업 노드의 경우 <jobs_namespace>.<job_name>이로 사용됩니다sourceIdentifier.
- 작업 실행의 경우:
  - 오픈 리니지 실행 이벤트를 사용하여 가져온 작업 실행 노드의 경우 <jobs_namespace>.<job_name>/<run_id>가 로 사용됩니다sourceIdentifier.

를 사용하여 생성한 자산의 경우 API자산을 `createAsset` 업스트림 리소스에 매핑`createAssetRevision`API할 수 있도록 를 사용하여 를 업데이트해야 `sourceIdentifier` 합니다.

데이터 계보 시각화

Amazon DataZone의 자산 세부 정보 페이지는 데이터 계보를 그래픽으로 표시하므로 데이터 관계를 업스트림 또는 다운스트림으로 더 쉽게 시각화할 수 있습니다. 자산 세부 정보 페이지에서는 그래프를 탐색할 수 있는 다음과 같은 기능을 제공합니다.

- 열 수준 계보: 데이터 세트 노드에서 사용 가능한 경우 열 수준 계보를 확장합니다. 소스 열 정보를 사용할 수 있는 경우 업스트림 또는 다운스트림 데이터 세트 노드와의 관계가 자동으로 표시됩니다.

- 열 검색: 열 수의 기본 표시가 10인 경우. 열이 10개 이상인 경우 페이지 매김이 활성화되어 나머지 열로 이동합니다. 특정 열을 빠르게 보려면 검색된 열만 나열하는 데이터 세트 노드를 검색할 수 있습니다.
- 데이터 세트 노드만 보기: 데이터 세트 계보 노드만 보고 작업 노드를 필터링하도록 전환하려면 그래프 뷰어 왼쪽 상단에 있는 보기 제어 열기 아이콘을 선택하고 데이터 세트 노드만 표시 옵션을 전환할 수 있습니다. 이렇게 하면 그래프에서 모든 작업 노드가 제거되고 데이터 세트 노드만 탐색할 수 있습니다. 보기 전용 데이터 세트 노드가 켜져 있으면 그래프를 업스트림 또는 다운스트림으로 확장할 수 없습니다.
- 세부 정보 창: 각 계보 노드에는 세부 정보가 캡처되어 선택 시 표시됩니다.
  - 데이터 세트 노드에는 지정된 타임스탬프에 대해 해당 노드에 대해 캡처된 모든 세부 정보를 표시하는 세부 정보 창이 있습니다. 모든 데이터 세트 노드에는 계보 정보, 스키마 및 기록 탭이라는 세 개의 탭이 있습니다. 기록 탭에는 해당 노드에 대해 캡처된 다양한 버전의 계보 이벤트가 나열됩니다. 에서 캡처한 모든 세부 정보는 메타데이터 양식 또는 JSON 뷰어를 사용하여 API 표시됩니다.
  - 작업 노드에는 탭, 즉 작업 정보 및 기록과 함께 작업 세부 정보를 표시하는 세부 정보 창이 있습니다. 세부 정보 창은 작업 실행의 일부로 캡처된 쿼리 또는 표현식도 캡처합니다. 기록 탭에는 해당 작업에 대해 캡처된 다양한 버전의 작업 실행 이벤트가 나열됩니다. 에서 캡처한 모든 세부 정보는 메타데이터 양식 또는 JSON 뷰어를 사용하여 API 표시됩니다.
- 버전 탭: Amazon DataZone 데이터 계보의 모든 계보 노드에는 버전 관리가 있습니다. 모든 데이터 세트 노드 또는 작업 노드에 대해 버전은 기록으로 캡처되며, 이를 통해 여러 버전 간에 탐색하여 초과 근무 시 변경된 사항을 식별할 수 있습니다. 각 버전은 계보 페이지에서 비교 또는 대비를 위한 새 탭을 엽니다.

Amazon의 데이터 계보 권한 부여 DataZone

쓰기 권한 - Amazon 에 계보 데이터를 게시하려면 `PostLineageEvent` 에 대한 `ALLOW` 작업이 포함된 권한 정책이 있는 IAM 역할이 DataZone있어야 합니다API. 이 IAM 권한 부여는 API Gateway 계층에서 발생합니다.

읽기 권한 - `AmazonDataZoneDomainExecutionRolePolicy` 관리형 정책에 `ListLineageNodeHistory` 포함된 `GetLineageNode` 및 두 가지 작업이 있으므로 Amazon DataZone 도메인의 모든 사용자는 이러한 작업을 호출하여 데이터 계보 그래프를 통과할 수 있습니다.

Amazon에서의 데이터 계보 샘플 경험 DataZone

데이터 계보 샘플 경험을 사용하여 데이터 계보 그래프의 업스트림 또는 다운스트림 횡단 DataZone, 버전 및 열 수준 계보 탐색을 포함하여 Amazon 의 데이터 계보를 탐색하고 이해할 수 있습니다.

후속 절차를 완료하여 Amazon 에서 샘플 데이터 계보 경험을 시도합니다 DataZone.

1. Amazon DataZone 데이터 포털로 이동하여 Single Sign-On(SSO) 또는 자격 AWS 증명을 사용하여 URL 로그인합니다. Amazon DataZone 관리자인 경우 https://console.aws.amazon.com/datazone의 Amazon DataZone 콘솔로 이동하여 도메인이 생성된 AWS 계정 로 로그인한 다음 데이터 포털 열기를 선택합니다.
2. 사용 가능한 데이터 자산을 선택하여 자산의 세부 정보 페이지를 엽니다.
3. 자산의 세부 정보 페이지에서 계보 탭을 선택한 다음 미리 보기를 선택하고 샘플 계보 사용해보기를 선택합니다.
4. 데이터 계보 팝업 창에서 안내형 데이터 계보 투어 시작을 선택합니다.

   이 시점에서 계보 정보의 모든 공간을 제공하는 전체 화면 탭이 표시됩니다. 샘플 데이터 계보 그래프는 처음에 업스트림 및 다운스트림의 양쪽 끝에 1-깊이 있는 기본 노드와 함께 표시됩니다. 그래프 업스트림 또는 다운스트림을 확장할 수 있습니다. 열 정보는 노드를 통해 계보가 흐르는 방식을 선택하고 확인할 수도 있습니다.

프로그래밍 방식으로 Amazon DataZone 데이터 계보 사용

Amazon 에서 데이터 계보 기능을 사용하려면 다음을 호출 DataZone할 수 있습니다APIs.

- GetLineageNode
- ListLineageNodeHistory
- PostLineageEvent

Amazon DataZone 데이터 제품

Amazon을 DataZone 사용하면 데이터 생산자가 데이터 자산을 특정 비즈니스 사용 사례에 맞게 조정된 데이터 제품이라고 하는 잘 정의된 독립형 패키지로 그룹화할 수 있습니다. 응집력 있는 비즈니스 정렬 데이터 제품을 사용하면 게시 및 구독 프로세스가 모두 향상됩니다. 데이터 소비자는 상호 연결된 데이터 자산을 단일 단위로 검색하고 찾아 쉽게 식별할 수 있습니다. 이 접근 방식은 모든 관련 정보를 찾는 데 필요한 시간과 노력을 줄이고 중요한 데이터가 누락될 위험을 낮춥니다. 또한 데이터 제품은 통합 액세스 모델을 구현하여 단일 요청으로 데이터에 대한 액세스를 단순화합니다. 이렇게 하면 여러 권한이 필요하지 않으므로 데이터 분석을 빠르게 시작할 수 있습니다. 또한 자산을 데이터 제품으로 카탈로그화하여 데이터 생산자는 개별적으로가 아니라 데이터 제품 수준에서 메타데이터 및 액세스 제어 관리를 활성화하여 관리 오버헤드를 줄입니다. 또한 이러한 용도에 맞게 설계된 그룹화된 자산을 표면화하여 사용할 수 있는 기능을 통해 액세스 거버넌스 및 데이터 사용률을 더 효율적으로 만들어 비즈니스 목표에 맞게 조정하고 의도한 용도로 쉽게 액세스할 수 있습니다. 데이터 거버넌스 팀은 이러한 데이터 제품의 소비율을 모니터링하여 데이터 리터러시 성숙도에 대한 귀중한 통찰력을 제공할 수 있습니다. 자세한 내용은 Amazon DataZone 용어 및 개념 단원을 참조하십시오.

주제

- Amazon에서 새 데이터 제품 생성 DataZone
- Amazon에 데이터 제품 게시 DataZone
- Amazon에서 데이터 제품 편집 DataZone
- Amazon에서 데이터 제품 게시 취소 DataZone
- Amazon에서 데이터 제품 삭제 DataZone
- Amazon에서 데이터 제품 구독 DataZone
- 구독 요청을 검토하고 Amazon의 데이터 제품에 구독을 부여합니다. DataZone
- Amazon에 데이터 제품 다시 게시 DataZone

Amazon에서 새 데이터 제품 생성 DataZone

Amazon을 DataZone 사용하면 데이터 생산자가 데이터 자산을 특정 비즈니스 사용 사례에 맞게 조정된 데이터 제품이라고 하는 잘 정의된 독립형 패키지로 그룹화할 수 있습니다. 자세한 내용은 Amazon DataZone 용어 및 개념 단원을 참조하십시오.

데이터 포털에 액세스하는 데 필요한 권한이 있는 모든 Amazon DataZone 사용자는 Amazon DataZone 데이터 제품을 생성할 수 있습니다.

새 데이터 제품을 생성하려면 다음 단계를 완료하세요.

1. Amazon DataZone 데이터 포털로 이동하여 Single Sign-On(SSO) 또는 자격 AWS 증명을 사용하여 URL 로그인합니다. Amazon DataZone 관리자인 경우 https://console.aws.amazon.com/datazone의 Amazon DataZone 콘솔로 이동하여 도메인이 생성된 AWS 계정 로 로그인한 다음 데이터 포털 열기를 선택합니다.
2. Amazon DataZone 데이터 포털에서 데이터 제품을 생성할 프로젝트를 선택합니다.
3. 데이터 탭을 선택한 다음 인벤토리 데이터 를 선택하고 새 데이터 제품 생성을 선택합니다.
4. 새 데이터 제품 생성 페이지에서 데이터 제품의 이름과 설명을 지정한 다음 자산 선택을 선택하여 데이터 제품에 다양한 자산을 추가합니다. 자산 선택 팝업 창에서 이 데이터 제품에 추가할 자산을 선택한 다음 선택을 선택합니다. 데이터 제품 생성을 완료하려면 생성 을 선택합니다.

Amazon에 데이터 제품 게시 DataZone

Amazon을 DataZone 사용하면 데이터 생산자가 데이터 자산을 특정 비즈니스 사용 사례에 맞게 조정된 데이터 제품이라고 하는 잘 정의된 독립형 패키지로 그룹화할 수 있습니다. 자세한 내용은 Amazon DataZone 용어 및 개념 단원을 참조하십시오.

데이터 포털에 액세스하는 데 필요한 권한이 있는 모든 Amazon DataZone 사용자는 Amazon DataZone 데이터 제품을 게시할 수 있습니다.

데이터 제품을 게시하려면 다음 단계를 완료하세요.

1. Amazon DataZone 데이터 포털로 이동하여 Single Sign-On(SSO) 또는 자격 AWS 증명을 사용하여 URL 로그인합니다. Amazon DataZone 관리자인 경우 https://console.aws.amazon.com/datazone의 Amazon DataZone 콘솔로 이동하여 도메인이 생성된 AWS 계정 로 로그인한 다음 데이터 포털 열기를 선택합니다.
2. Amazon DataZone 데이터 포털에서 게시하려는 데이터 제품이 있는 프로젝트를 선택합니다.
3. 데이터 탭을 선택한 다음 데이터 인벤토리 를 선택한 다음 데이터 제품 필터를 선택합니다. 이렇게 하면 게시되지 않은 기존 데이터 제품이 모두 표시됩니다.
4. 게시하려는 데이터 제품을 선택한 다음 게시를 선택합니다. 데이터 제품 게시를 선택하여 이 데이터 제품의 게시를 확인합니다.

> **Note**
>
> 이 데이터 제품에 있는 게시되지 않은 데이터 자산은 게시되지만 이 데이터 제품을 통해서만 사용할 수 있습니다.

Amazon에서 데이터 제품 편집 DataZone

Amazon을 DataZone 사용하면 데이터 생산자가 데이터 자산을 특정 비즈니스 사용 사례에 맞게 조정된 데이터 제품이라고 하는 잘 정의된 독립형 패키지로 그룹화할 수 있습니다. 자세한 내용은 Amazon DataZone 용어 및 개념 단원을 참조하십시오.

데이터 포털에 액세스하는 데 필요한 권한이 있는 모든 Amazon DataZone 사용자는 Amazon DataZone 데이터 제품을 편집할 수 있습니다.

데이터 제품을 편집하려면 다음 단계를 완료하세요.

1. Amazon DataZone 데이터 포털로 이동하여 Single Sign-On(SSO) 또는 자격 AWS 증명을 사용하여 URL 로그인합니다. Amazon DataZone 관리자인 경우 https://console.aws.amazon.com/datazone의 Amazon DataZone 콘솔로 이동하여 도메인이 생성된 AWS 계정 로 로그인한 다음 데이터 포털 열기를 선택합니다.
2. Amazon DataZone 데이터 포털에서 게시하려는 데이터 제품이 있는 프로젝트를 선택합니다.
3. 데이터 탭을 선택한 다음 인벤토리 데이터 또는 게시된 데이터 를 선택한 다음 데이터 제품 필터를 선택합니다.
4. 편집하려는 데이터 제품을 선택합니다. 데이터 제품 편집의 일환으로 다음을 수행할 수 있습니다.
   - 읽기메 생성을 선택하여 읽기메를 추가하면 사용자가 이 페이지를 더 잘 이해하는 데 도움이 됩니다.
   - 용어 추가를 선택하여 용어집 용어를 추가합니다. 창에서 용어집 용어를 선택한 다음 용어 추가를 선택합니다.
   - 메타데이터 양식 추가를 선택한 다음 메타데이터 양식 추가 창에서 양식을 선택하고 추가를 선택합니다.
   - 작업 을 확장하고 편집 을 선택한 다음 데이터 제품의 이름과 설명을 편집한 다음 업데이트를 선택합니다.

Amazon에서 데이터 제품 게시 취소 DataZone

Amazon을 DataZone 사용하면 데이터 생산자가 데이터 자산을 특정 비즈니스 사용 사례에 맞게 조정된 데이터 제품이라고 하는 잘 정의된 독립형 패키지로 그룹화할 수 있습니다. 자세한 내용은 Amazon DataZone 용어 및 개념 단원을 참조하십시오.

데이터 포털에 액세스하는 데 필요한 권한이 있는 모든 Amazon DataZone 사용자는 Amazon DataZone 데이터 제품을 게시 취소할 수 있습니다.

데이터 제품의 게시를 취소하려면 다음 단계를 완료하세요.

1. Amazon DataZone 데이터 포털로 이동하여 Single Sign-On(SSO) 또는 자격 AWS 증명을 사용하여 URL 로그인합니다. Amazon DataZone 관리자인 경우 https://console.aws.amazon.com/datazone의 Amazon DataZone 콘솔로 이동하여 도메인이 생성된 AWS 계정 로 로그인한 다음 데이터 포털 열기를 선택합니다.
2. Amazon DataZone 데이터 포털에서 게시 취소하려는 데이터 제품이 있는 프로젝트를 선택합니다.
3. 데이터 탭을 선택한 다음 인벤토리 데이터 또는 게시된 데이터 를 선택한 다음 데이터 제품 필터를 선택합니다. 그러면 기존 데이터 제품이 모두 표시됩니다.
4. 게시 취소하려는 데이터 제품을 선택한 다음 작업을 확장하고 게시 취소를 선택합니다. 게시 취소를 선택하여 이 데이터 제품의 게시 취소를 확인합니다.

> **Note**
>
> 데이터 제품의 게시를 취소하면 다음과 같은 영향이 있습니다.
>
> - 이 데이터 제품은 더 이상 보거나 구독할 수 없습니다.
> - 이 데이터 제품을 통해서만 사용할 수 있는 모든 데이터 자산은 더 이상 사용할 수 없습니다.
> - 이 데이터 제품에 대한 모든 활성 구독은 유지됩니다.
> - 개별적으로 게시된 데이터 자산은 영향을 받지 않습니다.

Amazon에서 데이터 제품 삭제 DataZone

Amazon을 DataZone 사용하면 데이터 생산자가 데이터 자산을 특정 비즈니스 사용 사례에 맞게 조정된 데이터 제품이라고 하는 잘 정의된 독립형 패키지로 그룹화할 수 있습니다. 자세한 내용은 Amazon DataZone 용어 및 개념 단원을 참조하십시오.

데이터 포털에 액세스하는 데 필요한 권한이 있는 모든 Amazon DataZone 사용자는 Amazon DataZone 데이터 제품을 삭제할 수 있습니다.

데이터 제품을 삭제하려면 다음 단계를 완료하세요.

1. Amazon DataZone 데이터 포털로 이동하여 Single Sign-On(SSO) 또는 자격 AWS 증명을 사용하여 URL 로그인합니다. Amazon DataZone 관리자인 경우 https://console.aws.amazon.com/datazone의 Amazon DataZone 콘솔로 이동하여 도메인이 생성된 AWS 계정 로 로그인한 다음 데이터 포털 열기를 선택합니다.
2. Amazon DataZone 데이터 포털에서 수명을 삭제하려는 데이터 제품이 속한 프로젝트를 선택합니다.
3. 데이터 탭을 선택한 다음 인벤토리 데이터 또는 게시된 데이터 를 선택한 다음 데이터 제품 필터를 선택합니다. 그러면 기존 데이터 제품이 모두 표시됩니다.
4. 삭제할 데이터 제품을 선택한 다음 작업을 확장하고 삭제를 선택합니다. 텍스트 필드에 를 입력한 다음 삭제를 선택하여 이 데이터 제품의 삭제`delete`를 확인합니다.

> **Note**
>
> 데이터 제품을 삭제하면 다음과 같은 효과가 있습니다.
>
> - 데이터 제품은 더 이상 게시, 보기 또는 구독할 수 없습니다.
> - 이 데이터 제품을 통해서만 사용할 수 있는 모든 데이터 자산은 더 이상 데이터 카탈로그에 표시되지 않습니다. 인벤토리 자산에서 삭제되지 않습니다.

Amazon에서 데이터 제품 구독 DataZone

Amazon을 DataZone 사용하면 데이터 생산자가 데이터 자산을 특정 비즈니스 사용 사례에 맞게 조정된 데이터 제품이라고 하는 잘 정의된 독립형 패키지로 그룹화할 수 있습니다. 자세한 내용은 Amazon DataZone 용어 및 개념 단원을 참조하십시오.

데이터 포털에 액세스하는 데 필요한 권한이 있는 모든 Amazon DataZone 사용자는 Amazon DataZone 데이터 제품을 구독할 수 있습니다.

데이터 제품을 구독하거나 구독 취소하려면 다음 단계를 완료하세요.

1. Amazon DataZone 데이터 포털로 이동하여 Single Sign-On(SSO) 또는 자격 AWS 증명을 사용하여 URL 로그인합니다. Amazon DataZone 관리자인 경우 https://console.aws.amazon.com/datazone의 Amazon DataZone 콘솔로 이동하여 도메인이 생성된 AWS 계정 로 로그인한 다음 데이터 포털 열기를 선택합니다.
2. 카탈로그 찾아보기를 선택하여 구독하려는 데이터 제품을 찾은 다음 해당 데이터 제품을 선택합니다.
3. 데이터 제품의 세부 정보 페이지에서 구독을 선택합니다.
4. 프로젝트와 구독 이유를 지정한 다음 구독을 선택합니다.

구독 요청을 검토하고 Amazon의 데이터 제품에 구독을 부여합니다. DataZone

Amazon을 DataZone 사용하면 데이터 생산자가 데이터 자산을 특정 비즈니스 사용 사례에 맞게 조정된 데이터 제품이라고 하는 잘 정의된 독립형 패키지로 그룹화할 수 있습니다. 자세한 내용은 Amazon DataZone 용어 및 개념 단원을 참조하십시오.

데이터 제품의 소유 프로젝트는 Amazon DataZone 데이터 제품에 대한 구독을 검토하고 부여할 수 있습니다.

구독 요청을 검토하고 데이터 제품에 구독을 부여하려면 다음 단계를 완료하세요.

1. Amazon DataZone 데이터 포털로 이동하여 Single Sign-On(SSO) 또는 자격 AWS 증명을 사용하여 URL 로그인합니다. Amazon DataZone 관리자인 경우 https://console.aws.amazon.com/datazone의 Amazon DataZone 콘솔로 이동하여 도메인이 생성된 AWS 계정 로 로그인한 다음 데이터 포털 열기를 선택합니다.
2. 검토하려는 수신 구독 요청이 있는 데이터 제품을 소유하는 프로젝트를 선택합니다.
3. 데이터 탭을 선택한 다음 수신 요청 을 선택합니다.
4. 검토할 요청을 선택한 다음 구독 요청 창에서 승인 또는 거부를 선택하고 대상 주석을 입력합니다.

Amazon에 데이터 제품 다시 게시 DataZone

Amazon을 DataZone 사용하면 데이터 생산자가 데이터 자산을 특정 비즈니스 사용 사례에 맞게 조정된 데이터 제품이라고 하는 잘 정의된 독립형 패키지로 그룹화할 수 있습니다. 자세한 내용은 Amazon DataZone 용어 및 개념 단원을 참조하십시오.

데이터 포털에 액세스하는 데 필요한 권한이 있는 모든 Amazon DataZone 사용자는 Amazon DataZone 데이터 제품을 다시 게시할 수 있습니다.

데이터 제품을 다시 게시하려면 다음 단계를 완료하세요.

1. Amazon DataZone 데이터 포털로 이동하여 Single Sign-On(SSO) 또는 자격 AWS 증명을 사용하여 URL 로그인합니다. Amazon DataZone 관리자인 경우 https://console.aws.amazon.com/datazone의 Amazon DataZone 콘솔로 이동하여 도메인이 생성된 AWS 계정 로 로그인한 다음 데이터 포털 열기를 선택합니다.
2. Amazon DataZone 데이터 포털에서 다시 게시하려는 데이터 제품이 있는 프로젝트를 선택합니다.
3. 데이터 탭을 선택한 다음 게시된 데이터 를 선택한 다음 데이터 제품 필터를 선택합니다.
4. 다시 게시하려는 데이터 제품을 선택한 다음 자산 탭을 선택합니다.
5. 자산 탭에서 다음 중 하나를 수행합니다.
   - 해당 자산을 선택한 다음 작업 아이콘을 확장하고 자산 제거를 선택하여 데이터 제품의 기존 자산 중 하나를 제거합니다. 자산 제거 팝업 창에서 제거를 선택하여 자산 제거를 확인합니다. 다시 게시하면 이 데이터 제품의 모든 구독자에서 이 자산이 제거됩니다.
   - 추가 버튼을 선택한 다음 데이터 제품에 추가할 자산을 하나 이상 선택하여 데이터 제품에 새 자산을 추가합니다.
6. 데이터 제품의 세부 정보 페이지에서 다시 게시를 선택합니다. 데이터 제품 다시 게시 팝업 창에서 다시 게시를 선택하여 이 작업을 확인합니다.

> **Note**
>
> 이 데이터 제품을 다시 게시하면 모든 구독자에 대해 다음이 업데이트됩니다.
>
> - 데이터 제품에서 자산이 제거된 경우 구독자는 더 이상 이러한 자산에 액세스할 수 없습니다.
> - 자산이 데이터 제품에 추가된 경우 구독자는 이러한 자산에 액세스할 수 있습니다.

- 새로 게시된 버전의 데이터 자산을 사용할 수 있습니다.

Amazon DataZone 데이터 검색, 구독 및 소비

Amazon 에서 자산이 도메인에 게시 DataZone되면 구독자는 이 자산을 검색하고 구독을 요청할 수 있습니다. 구독 프로세스는 구독자가 카탈로그를 검색하고 검색하여 원하는 자산을 찾는 것으로 시작됩니다. Amazon DataZone 포털에서 정당한 사유와 요청 사유가 포함된 구독 요청을 제출하여 자산을 구독하기로 선택합니다. 그러면 게시 계약에 정의된 구독 승인자가 액세스 요청을 검토합니다. 요청을 승인하거나 거부할 수 있습니다.

구독이 부여되면 구독자의 자산에 대한 액세스를 용이하게 하기 위한 이행 프로세스가 시작됩니다. 자산 액세스 제어 및 이행에는 Amazon DataZone관리형 자산과 Amazon에서 관리하지 않는 자산의 두 가지 기본 모드가 있습니다 DataZone.

- 관리형 자산 - Amazon은 AWS Glue 테이블, Amazon Redshift 테이블 및 뷰와 같은 관리형 자산의 이행 및 권한을 관리할 DataZone 수 있습니다.
- 관리되지 않는 자산 - Amazon은 작업(예: 구독 요청에 대한 승인)과 관련된 표준 이벤트를 Amazon에 DataZone 게시합니다 EventBridge. 이러한 표준 이벤트를 사용하여 사용자 지정 통합을 위한 다른 AWS 서비스 또는 타사 솔루션과 통합할 수 있습니다.

주제

- Amazon DataZone 카탈로그에서 자산 검색 및 보기
- Amazon의 자산에 대한 구독 요청 DataZone
- Amazon에서 구독 요청 승인 또는 거부 DataZone
- Amazon에서 기존 구독 취소 DataZone
- Amazon에서 구독 요청 취소 DataZone
- Amazon의 자산 구독 취소 DataZone
- 기존 IAM 역할을 사용하여 Amazon DataZone 구독 이행
- Amazon의 관리 AWS Glue Data Catalog 형 자산에 대한 액세스 권한 부여 DataZone
- Amazon의 관리형 Amazon Redshift 자산에 대한 액세스 권한 부여 DataZone
- Amazon의 관리되지 않는 자산에 대해 승인된 구독에 대한 액세스 권한 부여 DataZone
- Amazon Athena의 데이터 쿼리 또는 Amazon의 Amazon Redshift DataZone

Amazon DataZone 카탈로그에서 자산 검색 및 보기

Amazon은 데이터를 검색하는 간소화된 방법을 DataZone 제공합니다. 데이터 포털에 액세스할 수 있는 권한이 있는 모든 Amazon DataZone 사용자는 Amazon DataZone 카탈로그에서 자산을 검색하고 자산 이름과 할당된 메타데이터를 볼 수 있습니다. 세부 정보 페이지를 검토하여 자산을 자세히 살펴볼 수 있습니다.

> **Note**
>
> 자산에 포함된 실제 데이터를 보려면 먼저 자산을 구독하고 구독 요청을 승인하고 액세스 권한을 부여받아야 합니다.

카탈로그에서 자산을 검색하려면

1. Amazon DataZone 데이터 포털로 이동하여 Single Sign-On(SSO) 또는 자격 AWS 증명을 사용하여 URL 로그인합니다. Amazon DataZone 관리자인 경우 https://console.aws.amazon.com/datazone의 Amazon DataZone 콘솔로 이동하여 도메인이 생성된 AWS 계정 로 로그인한 다음 데이터 포털 열기를 선택합니다.
2. 데이터 포털 홈 페이지의 검색 창에 찾고 있는 자산의 이름을 입력할 수 있습니다.
3. 네임스페이스를 검색하려면 페이지 오른쪽 상단에서 카탈로그를 선택하여 카탈로그를 엽니다. 카탈로그는 , 데이터 소유자 및 용어집 용어와 같은 기준을 검색하여 자산을 찾을 수 있는 패싯 검색 환경을 제공합니다.
4. 검색 상자 중 하나에 검색 용어를 입력합니다. 검색을 실행한 후 다양한 필터를 적용하여 결과를 좁힐 수 있습니다. 필터에는 자산 유형, 소스 계정 및 자산이 속한 AWS 리전 이 포함됩니다.
5. 특정 자산에 대한 세부 정보를 보려면 자산을 선택하여 세부 정보 페이지를 엽니다. 세부 정보 페이지에는 다음 정보가 포함되어 있습니다.

   - 자산 이름, 데이터 소스(AWS Glue, Amazon Redshift 또는 Amazon S3), 유형(테이블, 뷰 또는 S3 객체), 열 수 및 크기입니다.
   - 자산에 대한 설명입니다.
   - 자산의 현재 게시된 개정, 소유자, 구독에 대한 승인 필요 여부, 네임페이스 및 업데이트 기록.
   - 용어집 용어 및 메타데이터 양식을 포함하는 개요 탭입니다.
   - 비즈니스 및 기술 열 이름, 데이터 유형, 열의 비즈니스 설명을 포함하여 자산의 스키마를 표시하는 스키마 탭입니다. 스키마 탭은 테이블 및 뷰(Amazon S3 객체 제외)에만 표시됩니다.
   - 도메인 구독자 목록이 포함된 구독 탭입니다.

- 자산의 과거 개정 목록을 포함하는 기록 탭입니다.

Amazon의 자산에 대한 구독 요청 DataZone

Amazon을 DataZone 사용하면 Amazon DataZone 카탈로그에서 자산을 찾고, 액세스하고, 사용할 수 있습니다. 카탈로그에서 액세스하려는 자산을 찾으면 자산을 구독해야 하므로 구독 요청이 생성됩니다. 그러면 승인자가 요청을 승인하거나 요청할 수 있습니다.

해당 프로젝트 내의 자산에 대한 구독을 요청하려면 프로젝트의 구성원이어야 합니다.

자산을 구독하려면

1. Amazon DataZone 데이터 포털로 이동하여 Single Sign-On(SSO) 또는 자격 AWS 증명을 사용하여 URL 로그인합니다. Amazon DataZone 관리자인 경우 https://console.aws.amazon.com/datazone의 Amazon DataZone 콘솔로 이동하여 도메인이 생성된 AWS 계정 로 로그인한 다음 데이터 포털 열기를 선택합니다.
2. 검색 창을 사용하여 구독하려는 자산을 검색하고 선택한 다음 구독을 선택합니다.
3. 구독 팝업 창에서 다음 정보를 제공합니다.
   - 자산을 구독하려는 프로젝트입니다.
   - 구독 요청에 대한 간단한 정당화입니다.
4. 구독을 선택합니다.

   게시자가 요청을 승인하면 데이터 포털에서 알림을 받습니다.

구독 요청의 상태를 보려면 자산을 구독한 프로젝트를 찾아 선택합니다. 프로젝트의 데이터 탭으로 이동한 다음 왼쪽 탐색 창에서 요청된 데이터를 선택합니다. 이 페이지에는 프로젝트가 액세스를 요청한 자산이 나열됩니다. 요청 상태를 기준으로 목록을 필터링할 수 있습니다.

Amazon에서 구독 요청 승인 또는 거부 DataZone

Amazon을 DataZone 사용하면 Amazon DataZone 카탈로그에서 자산을 찾고, 액세스하고, 사용할 수 있습니다. 카탈로그에서 액세스하려는 자산을 찾으면 자산을 구독해야 합니다. 그러면 구독 요청이 생성됩니다. 그러면 승인자가 요청을 승인하거나 거부할 수 있습니다.

구독 요청을 승인하거나 거부하려면 소유 프로젝트(자산을 게시한 프로젝트)의 구성원이어야 합니다.

구독 요청을 승인 또는 거부하려면

1. Amazon DataZone 데이터 포털로 이동하여 Single Sign-On(SSO) 또는 자격 AWS 증명을 사용하여 URL 로그인합니다. Amazon DataZone 관리자인 경우 https://console.aws.amazon.com/datazone의 Amazon DataZone 콘솔로 이동하여 도메인이 생성된 AWS 계정 로 로그인한 다음 데이터 포털 열기를 선택합니다.
2. 데이터 포털에서 프로젝트 목록 찾아보기를 선택하고 구독 요청이 있는 자산이 포함된 프로젝트를 선택합니다.
3. 데이터 탭으로 이동한 다음 왼쪽 탐색 창에서 수신 요청을 선택합니다.
4. 요청을 찾아 요청 보기를 선택합니다. 보류 중으로 필터링하여 아직 열려 있는 요청만 볼 수 있습니다.
5. 구독 요청과 액세스 이유를 검토하고 이를 승인할지 거부할지 결정합니다.
6. 승인하려면 다음 두 옵션 중에서 선택합니다.
   - 전체 액세스 : 전체 액세스 옵션으로 구독을 승인하도록 선택하면 구독자는 데이터 자산의 모든 행과 열에 액세스할 수 있습니다.
   - 행 및 열 필터로 승인 : 데이터의 특정 행 및 열에 대한 액세스를 제한하려면 행 및 열 필터로 승인할 옵션을 선택할 수 있습니다. 자세한 내용은 Amazon의 데이터에 대한 세분화된 액세스 제어 DataZone 단원을 참조하십시오.
     - 필터 선택을 선택한 다음 드롭다운에서 구독에 적용할 하나 이상의 사용 가능한 필터를 선택합니다.
     - 새 필터를 생성하려면 새 필터 생성 옵션을 선택하면 새 페이지가 열리고 새 행 또는 열 필터가 생성됩니다. 자세한 내용은 Amazon에서 열 필터 생성 DataZone 및 Amazon에서 행 필터 생성 DataZone 단원을 참조하세요.
7. (선택 사항) 요청을 수락하거나 거부하는 이유를 설명하는 응답을 입력합니다.
8. 승인 또는 거부를 선택합니다.

프로젝트 소유자는 언제든지 구독을 취소할 수 있습니다. 자세한 내용은 the section called “기존 구독 취소” 단원을 참조하십시오.

모든 구독 요청을 보려면 섹션을 참조하세요이벤트 및 알림.

> **Note**
>
> Amazon은 AWS Glue 테이블, Amazon Redshift 테이블 및 Amazon Redshift 뷰에 대한 세분화된 액세스 제어를 DataZone 지원합니다.

Amazon에서 기존 구독 취소 DataZone

Amazon을 DataZone 사용하면 Amazon DataZone 카탈로그에서 자산을 찾고, 액세스하고, 사용할 수 있습니다. 카탈로그에서 액세스하려는 자산을 찾으면 자산을 구독해야 하므로 구독 요청이 생성됩니다. 그러면 승인자가 요청을 승인하거나 요청할 수 있습니다. 승인은 실수였거나 구독자가 더 이상 자산에 액세스할 필요가 없기 때문에 구독을 승인한 후 구독을 취소해야 할 수 있습니다.

구독을 취소하려면 소유 프로젝트(자산을 게시한 프로젝트)의 구성원이어야 합니다.

구독을 취소하려면

1. Amazon DataZone 데이터 포털로 이동하여 Single Sign-On(SSO) 또는 자격 AWS 증명을 사용하여 URL 로그인합니다. Amazon DataZone 관리자인 경우 https://console.aws.amazon.com/datazone의 Amazon DataZone 콘솔로 이동하여 도메인이 생성된 AWS 계정 로 로그인한 다음 데이터 포털 열기를 선택합니다.
2. 상단 탐색 창에서 프로젝트 선택을 선택하고 취소하려는 구독이 포함된 프로젝트를 선택합니다.
3. 데이터 탭으로 이동한 다음 왼쪽 탐색 창에서 수신 요청을 선택합니다.
4. 취소하려는 구독을 찾아 구독 보기를 선택합니다.
5. (선택 사항) 구독자가 프로젝트의 구독 대상에 자산을 유지하도록 허용하려면 확인란을 활성화합니다. 구독 대상은 환경 내에서 구독 데이터를 사용할 수 있는 리소스 집합에 대한 참조입니다.

   나중에 구독 대상에서 자산에 대한 액세스를 취소하려면 에서 취소해야 합니다 AWS Lake Formation.
6. 구독 취소를 선택합니다.

구독을 취소한 후에는 다시 승인할 수 없습니다. 자산을 승인하려면 구독자가 자산을 다시 구독해야 합니다.

Amazon에서 구독 요청 취소 DataZone

Amazon을 DataZone 사용하면 Amazon DataZone 카탈로그에서 자산을 찾고, 액세스하고, 사용할 수 있습니다. 카탈로그에서 액세스하려는 자산을 찾으면 자산을 구독해야 하므로 구독 요청이 생성됩니다. 그러면 승인자가 요청을 승인하거나 요청할 수 있습니다. 실수로 구독 요청을 제출했거나 자산에 대한 읽기 액세스가 더 이상 필요하지 않기 때문에 보류 중인 구독 요청을 취소해야 할 수 있습니다.

구독 요청을 취소하려면 프로젝트 소유자 또는 기여자여야 합니다.

구독 요청을 취소하려면

1. Amazon DataZone 데이터 포털로 이동하여 Single Sign-On(SSO) 또는 자격 AWS 증명을 사용하여 URL 로그인합니다. Amazon DataZone 관리자인 경우 https://console.aws.amazon.com/datazone의 Amazon DataZone 콘솔로 이동하여 도메인이 생성된 AWS 계정 로 로그인한 다음 데이터 포털 열기를 선택합니다.
2. 상단 탐색 창에서 프로젝트 선택을 선택하고 구독 요청이 포함된 프로젝트를 선택합니다.
3. 프로젝트의 데이터 탭으로 이동한 다음 왼쪽 탐색 창에서 요청된 데이터를 선택합니다. 이 페이지에는 프로젝트가 액세스를 요청한 자산이 나열됩니다.
4. 아직 보류 중인 요청만 보려면 요청됨으로 필터링합니다. 요청을 찾아 요청 보기를 선택합니다.
5. 구독 요청을 검토하고 요청 취소를 선택합니다.

자산(또는 다른 자산)을 다시 구독하려면 섹션을 참조하세요the section called “자산 구독 요청”.

Amazon의 자산 구독 취소 DataZone

Amazon을 DataZone 사용하면 Amazon DataZone 카탈로그에서 자산을 찾고, 액세스하고, 사용할 수 있습니다. 카탈로그에서 액세스하려는 자산을 찾으면 자산을 구독해야 하므로 구독 요청이 생성됩니다. 그러면 승인자가 요청을 승인하거나 요청할 수 있습니다. 실수로 구독하고 승인을 받았거나 더 이상 자산에 대한 읽기 액세스가 필요하지 않기 때문에 자산 구독을 취소해야 할 수 있습니다.

자산 중 하나를 구독 취소하려면 프로젝트의 멤버여야 합니다.

자산 구독을 취소하려면

1. Amazon DataZone 데이터 포털로 이동하여 Single Sign-On(SSO) 또는 자격 AWS 증명을 사용하여 URL 로그인합니다. Amazon DataZone 관리자인 경우 https://console.aws.amazon.com/datazone의 Amazon DataZone 콘솔로 이동하여 도메인이 생성된 AWS 계정 로 로그인한 다음 데이터 포털 열기를 선택합니다.

2. 상단 탐색 창에서 프로젝트 선택을 선택하고 구독 취소하려는 자산이 포함된 프로젝트를 선택합니다.
3. 프로젝트의 데이터 탭으로 이동한 다음 왼쪽 탐색 창에서 요청된 데이터를 선택합니다. 이 페이지에는 프로젝트가 액세스를 요청한 자산이 나열됩니다.
4. 승인된 요청만 보려면 승인됨으로 필터링합니다. 요청을 찾아 구독 보기를 선택합니다.
5. 구독을 검토하고 구독 취소를 선택합니다.

자산(또는 다른 자산)을 다시 구독하려면 섹션을 참조하세요the section called “자산 구독 요청”.

기존 IAM 역할을 사용하여 Amazon DataZone 구독 이행

현재 릴리스에서 Amazon은 기존 IAM 역할을 사용하여 데이터에 액세스할 수 있도록 DataZone 지원합니다. 이를 위해 구독을 이행하는 데 사용하는 Amazon DataZone 환경에서 구독 대상을 생성할 수 있습니다. 연결된 AWS 계정 중 하나의 환경에 대한 구독 대상을 생성하려면 다음 단계를 사용할 수 있습니다.

1단계: Amazon DataZone 도메인이 RAM 정책 버전 2 이상을 사용하고 있는지 확인합니다.

1. 콘솔에서 내 공유 : 리소스 공유 페이지로 AWS RAM 이동합니다.
2. 리소스 공유는 특정 AWS 리전에 존재하므로 AWS RAM 콘솔의 오른쪽 상단 모서리에 있는 드롭다운 목록에서 적절한 AWS 리전을 선택합니다.
3. Amazon DataZone 도메인에 해당하는 리소스 공유를 선택한 다음 수정을 선택합니다. RAM 공유가 이름으로 생성되면 DataZone 도메인의 이름 또는 ID를 사용하여 Amazon 도메인의 RAM 공유를 식별할 수 있습니다`DataZone-<domain-name>-<domain-id>`.
4. 다음을 선택하여 RAM 정책의 버전을 확인하고 수정할 수 있는 다음 단계로 진행합니다.
5. RAM 정책의 버전이 버전 2 이상인지 확인합니다. 그렇지 않은 경우 드롭다운을 사용하여 버전 2 이상을 선택합니다.
6. 4단계로 건너뛰기: 검토 및 업데이트를 선택합니다.
7. 리소스 공유 업데이트를 선택합니다.

2단계: 연결된 계정에서 구독 대상 생성

- 현재 릴리스에서 Amazon은 APIs 만 사용하여 구독 대상 생성을 DataZone 지원합니다. 다음은 AWS Glue 테이블 및 Amazon Redshift 테이블 또는 뷰에 대한 구독을 이행하기 위

한 구독 대상을 생성하는 데 사용할 수 있는 페이로드의 몇 가지 예입니다. 자세한 내용은 CreateSubscriptionTarget를 참조하세요.

AWS Glue 구독 대상의 예

```
{
        "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 Redshift의 구독 대상 예:

```
{
        "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**
>
> - 위의 API 호출에 environmentIdentifier 사용하는 는 API 호출하는 것과 동일한 연결 계정에 있어야 합니다. 그렇지 않으면 API 호출이 성공하지 못합니다.
> - “authorizedPrincipals”에서 ARN 사용하는 IAM 역할은 구독 대상에 구독 자산을 추가한 후 Amazon이 액세스 권한을 DataZone 부여하는 역할입니다. 이러한 승인된 보안 주체는 구독 대상이 생성되는 환경과 동일한 계정에 속해야 합니다.
> - Amazon이 구독 이행을 완료 DataZone 하려면 공급자 필드의 값이 “Amazon DataZone”이어야 합니다.
> - 에 제공된 데이터베이스 이름은 대상을 생성하는 계정에 이미 있어야 subscriptionTargetConfig 합니다. Amazon DataZone 은 이 데이터베이스를 생성하지 않습니다. 또한 관리 액세스 역할에 이 데이터베이스에 대한 CREATE TABLE 권한이 있는지 확인합니다.
> - 또한 권한 있는 보안 주체로 제공되는 역할(IAM AWS Glue의 역할 및 Amazon Redshift의 데이터베이스 역할)이 환경 계정에 이미 있는지 확인합니다. Amazon Redshift 구독 대상의 경우 클러스터에 연결하는 동안 수임되는 역할에 대한 추가 업데이트가 필요합니다. 이 역할에는 역할에 연결된 RedshiftDbRoles 태그가 있어야 합니다. 태그의 값은 쉼표로 구분된 목록일 수 있습니다. 값은 구독 대상을 생성하는 동안 승인된 보안 주체로 제공된 데이터베이스 역할이어야 합니다.

3단계: 새 테이블 구독 및 새 대상 구독 이행

- 구독 대상을 생성한 후에는 새 테이블을 구독할 수 있으며 Amazon DataZone 은 해당 테이블을 위의 대상으로 이행합니다.

Amazon의 관리 AWS Glue Data Catalog 형 자산에 대한 액세스 권한 부여 DataZone

Amazon 에서는 DataZone자산에 대한 읽기 액세스에 대한 구독 요청과 승인 또는 부여된 구독을 구독 승인자가 관리합니다. 자산에 대한 구독 승인자는 이 자산이 Amazon DataZone 카탈로그에 게시된 게시 계약에 따라 결정됩니다.

> **Note**
>
> AWS Lake Formation LF-TBAC 메서드를 사용하는 AWS Glue Data Catalog 자산에 대한 액세스 관리는 지원되지 않습니다.
> 에서 자산의 리전 간 공유에 대한 지원 AWS Glue Data Catalog 은 지원되지 않습니다.

관리형 AWS Glue Data Catalog 자산에 대한 구독 요청이 승인되면 Amazon DataZone은 프로젝트의 모든 기존 데이터 레이크 환경에 이러한 자산을 자동으로 추가합니다. DataZone 그런 다음 Amazon 은 를 통해 사용자를 대신하여 승인된 AWS Glue Data Catalog 테이블에 대한 액세스 권한을 부여하고 관리합니다 AWS Lake Formation. 구독자 프로젝트의 경우 부여되는 자산은 에 계정의 리소스 AWS Glue Data Catalog 로 표시됩니다. 그런 다음 Amazon Athena를 사용하여 테이블을 쿼리할 수 있습니다.

> **Note**
>
> 구독한 AWS Glue Data Catalog 자산을 기존 데이터 레이크 환경에 자동으로 추가한 후 새 데이터 레이크 환경이 프로젝트에 추가되는 경우 이러한 구독한 AWS Glue Data Catalog 자산을 이 새 데이터 레이크 환경에 수동으로 추가해야 합니다. Amazon 데이터 포털의 프로젝트 개요 페이지의 DataZone 데이터 탭에서 권한 부여 추가 옵션을 선택하여 이 작업을 수행할 수 있습니다.

Amazon이 AWS Glue Data Catalog 테이블에 대한 액세스 권한을 부여 DataZone 하려면 다음 조건을 충족해야 합니다.

- Amazon DataZone은 Lake Formation 권한을 관리하여 액세스 권한을 부여하므로 AWS Glue 테이블은 Lake Formation 관리형이어야 합니다.
- AWS Glue Data Catalog 테이블을 게시하는 데 사용되는 데이터 레이크 환경의 액세스 관리 역할에는 다음 Lake Formation 권한이 있어야 합니다.
  - `DESCRIBE` 및 게시된 테이블이 포함된 AWS Glue 데이터베이스에 대한 `DESCRIBE GRANTABLE` 권한.
  - `DESCRIBE`게시된 테이블 자체의 Lake Formation에 있는 `SELECT`, `DESCRIBE GRANTABLE`, , `SELECT GRANTABLE` 권한.

자세한 내용은 AWS Lake Formation 개발자 안내서의 카탈로그 리소스에 대한 권한 부여 및 취소를 참조하세요.

Amazon의 관리형 Amazon Redshift 자산에 대한 액세스 권한 부여 DataZone

Amazon 에서는 DataZone자산에 대한 읽기 액세스에 대한 구독 요청과 승인 또는 부여된 구독을 구독 승인자가 관리합니다. 자산에 대한 구독 승인자는 이 자산이 Amazon DataZone 카탈로그에 게시된 게시 계약에 따라 결정됩니다.

Amazon Redshift 테이블 또는 뷰에 대한 구독이 승인되면 Amazon DataZone은 프로젝트 내의 모든 데이터 웨어하우스 환경에 구독 자산을 자동으로 추가할 수 있으므로 프로젝트 구성원은 환경 내에서 Amazon Redshift 쿼리 편집기 링크를 사용하여 데이터를 쿼리할 수 있습니다. Amazon DataZone는 후드 아래에서 소스와 구독 대상 간에 필요한 권한 부여 및 데이터 공유를 생성합니다.

액세스 권한 부여 프로세스는 소스 데이터베이스(퍼블리셔)와 대상 데이터베이스(구독자)의 위치에 따라 달라집니다.

- 동일한 클러스터, 동일한 데이터베이스 - 동일한 데이터베이스 내에서 데이터를 공유해야 하는 경우 Amazon은 소스 테이블에 직접 권한을 DataZone 부여합니다.
- 동일한 클러스터, 다른 데이터베이스 - 동일한 클러스터 내의 두 데이터베이스 간에 데이터를 공유해야 하는 경우 Amazon은 대상 데이터베이스에 뷰를 DataZone 생성하고 생성된 뷰에 권한이 부여됩니다.
- 동일한 계정의 다른 클러스터 - Amazon DataZone 은 소스 클러스터와 대상 클러스터 간에 데이터 공유를 생성하고 공유 테이블 위에 뷰를 생성합니다. 뷰에 권한이 부여됩니다.
- 크로스 계정 - 위와 동일하지만 생산자 클러스터 측에서 크로스 계정 데이터 공유를 승인하려면 추가 단계가 필요하고 소비자 클러스터 측에서 데이터 공유를 연결하려면 또 다른 단계가 필요합니다.

> **Note**
>
> 구독한 Amazon Redshift 자산이 기존 데이터 웨어하우스 환경에 자동으로 추가된 후 새 데이터 웨어하우스 환경이 프로젝트에 추가되는 경우 이 구독한 Amazon Redshift 자산을 이 새 데이터 웨어하우스 환경에 수동으로 추가해야 합니다. Amazon 데이터 포털의 프로젝트 개요 페이지의 DataZone 데이터 탭에서 권한 부여 추가 옵션을 선택하여 이 작업을 수행할 수 있습니다.

Amazon Redshift 클러스터 게시 및 구독이 Amazon Redshift 데이터 공유에 대한 모든 요구 사항을 충족하는지 확인합니다. 자세한 내용은 Amazon Redshift 개발자 안내서를 참조하세요.

> **Note**
>
> Amazon은 Amazon Redshift 클러스터 및 Amazon Redshift Serverless 자산 모두에 대한 구독 자동 부여를 DataZone 지원합니다.
> Amazon Redshift를 사용한 리전 간 데이터 공유는 지원되지 않습니다.

Amazon의 관리되지 않는 자산에 대해 승인된 구독에 대한 액세스 권한 부여 DataZone

Amazon 에서는 DataZone자산에 대한 읽기 액세스에 대한 구독 요청 및 승인되거나 부여된 구독을 구독 승인자가 관리합니다. 자산에 대한 구독 승인자는 이 자산이 Amazon DataZone 카탈로그에 게시된 게시 계약에 따라 결정됩니다.

Amazon을 DataZone 사용하면 사용자가 비즈니스 데이터 카탈로그에 모든 유형의 자산을 게시할 수 있습니다. 이러한 자산 중 일부의 경우 Amazon DataZone 은 액세스 권한 부여를 자동으로 관리할 수 있습니다. 이러한 자산을 관리형 자산이라고 하며 Lake Formation 관리형 AWS Glue 데이터 카탈로그 테이블과 Amazon Redshift 테이블 및 뷰가 포함됩니다. Amazon이 구독을 자동으로 부여할 DataZone 수 없는 다른 모든 자산은 관리되지 않는 이라고 합니다.

Amazon DataZone 은 관리되지 않는 자산에 대한 액세스 권한을 관리할 수 있는 경로를 제공합니다. 데이터 소유자가 비즈니스 데이터 카탈로그의 자산에 대한 구독을 승인하면 Amazon은 소스와 대상 간에 액세스 권한을 생성할 수 있도록 페이로드의 모든 필수 정보와 함께 EventBridge 계정의 Amazon에 이벤트를 DataZone 게시합니다. 이 이벤트를 받으면 이벤트의 정보를 사용하여 필요한 권한 부여 또는 권한을 생성할 수 있는 사용자 지정 핸들러를 트리거할 수 있습니다. 액세스 권한을 부여한 후에는 Amazon에서 구독 상태를 보고하고 업데이트 DataZone 하여 자산을 구독한 사용자(들)에게 자산 소비를 시작할 수 있음을 알릴 수 있습니다. 자세한 내용은 아마존 DataZone 이벤트 및 알림 단원을 참조하십시오.

Amazon Athena의 데이터 쿼리 또는 Amazon의 Amazon Redshift DataZone

Amazon 에서는 구독자가 카탈로그의 자산에 액세스할 수 있게 DataZone되면 Amazon Athena 또는 Amazon Redshift 쿼리 편집기 v2를 사용하여 자산을 소비(쿼리 및 분석)할 수 있습니다. 이 작업을 완료하려면 프로젝트 소유자 또는 기여자여야 합니다. 프로젝트에 활성화된 청사진에 따라 Amazon은 데이터 포털의 프로젝트 페이지 오른쪽 창에 Amazon Athena 및/또는 Amazon Redshift 쿼리 편집기 v2에 대한 링크를 DataZone 제공합니다.

1. Amazon DataZone 데이터 포털로 이동하여 Single Sign-On(SSO) 또는 자격 AWS 증명을 사용하여 URL 로그인합니다. Amazon DataZone 관리자인 경우 https://console.aws.amazon.com/datazone의 Amazon DataZone 콘솔로 이동하여 도메인이 생성된 AWS 계정 로 로그인한 다음 데이터 포털 열기를 선택합니다.
2. Amazon DataZone 데이터 포털에서 프로젝트 목록 찾아보기를 선택한 다음 분석하려는 데이터가 있는 프로젝트를 찾아 선택합니다.
3. 이 프로젝트에서 Data Lake 청사진이 활성화된 경우 Amazon Athena에 대한 링크가 프로젝트 홈 페이지의 오른쪽 패널에 표시됩니다.

   이 프로젝트에서 Data Warehouse 청사진이 활성화된 경우 쿼리 편집기에 대한 링크가 프로젝트 홈 페이지의 오른쪽 패널에 표시됩니다.

   > **Note**
   >
   > 청사진은 프로젝트가 생성되는 환경 프로파일에 정의됩니다.

주제

- Amazon Athena를 사용하여 데이터 쿼리
- Amazon Redshift를 사용하여 데이터 쿼리

Amazon Athena를 사용하여 데이터 쿼리

Amazon Athena 링크를 선택하여 인증을 위한 프로젝트의 보안 인증 정보를 사용하여 브라우저의 새 탭에서 Amazon Athena 쿼리 편집기를 엽니다. 작업 중인 Amazon DataZone 프로젝트는 쿼리 편집기에서 현재 작업 그룹으로 자동으로 선택됩니다.

Amazon Athena 쿼리 편집기에서 쿼리를 작성하고 실행합니다. 몇 가지 일반적인 작업은 다음과 같습니다.

- 구독한 자산 쿼리 및 분석
- 새 테이블 생성
- 외부 S3 버킷의 쿼리 결과(CTAS)에서 테이블 생성

구독한 자산 쿼리 및 분석

Amazon 에서 프로젝트가 구독하는 자산에 대한 액세스 권한을 자동으로 부여하지 않는 경우 기본 데이터에 액세스할 수 있는 권한이 있어야 DataZone합니다. 이러한 자산에 대한 액세스 권한을 부여하는 방법에 대한 자세한 내용은 섹션을 참조하세요Amazon의 관리되지 않는 자산에 대해 승인된 구독에 대한 액세스 권한 부여 DataZone.

Amazon 에서 프로젝트가 구독하는 자산에 대한 액세스 권한을 자동으로 부여 DataZone한 경우 테이블에서 SQL 쿼리를 실행하고 Amazon Athena 에서 결과를 볼 수 있습니다. Amazon Athena SQL 에서를 사용하는 방법에 대한 자세한 내용은 SQL Athena 참조를 참조하세요.

프로젝트 홈 페이지의 오른쪽 패널에서 Amazon Athena 링크를 선택한 후 Amazon Athena 쿼리 편집기로 이동하면 Amazon Amazon Athena 쿼리 편집기의 오른쪽 상단에 프로젝트 드롭다운이 표시되고 프로젝트 컨텍스트가 자동으로 선택됩니다.

데이터베이스 드롭다운에서 다음 데이터베이스를 볼 수 있습니다.

- 게시 데이터베이스(*{environmentname}*_pub_db). 이 데이터베이스의 목적은 프로젝트의 컨텍스트 내에서 새 데이터를 생성한 다음 Amazon DataZone 카탈로그에 이 데이터를 게시할 수 있는 환경을 제공하는 것입니다. 프로젝트 소유자와 기여자는 이 데이터베이스에 대한 읽기 및 쓰기 액세스 권한을 갖습니다. 프로젝트 뷰어는 이 데이터베이스에 대한 읽기 액세스 권한만 가집니다.
- 구독 데이터베이스(*{environmentname}*_sub_db). 이 데이터베이스의 목적은 Amazon DataZone 카탈로그에서 프로젝트 멤버로 구독한 데이터를 공유하고 해당 데이터를 쿼리할 수 있도록 하기 위한 것입니다.

새 테이블 생성

외부 S3 버킷에 연결한 경우 Amazon Athena를 사용하여 외부 Amazon S3 버킷에서 자산을 쿼리하고 분석할 수 있습니다. 이 시나리오에서 Amazon DataZone 은 외부 Amazon S3 버킷의 기본 데이터에 대한 직접 액세스 권한을 부여할 권한이 없으며, 프로젝트 외부에서 생성된 외부 Amazon S3 데이터는 Lake Formation에서 자동으로 관리되지 않으며 Amazon 에서 관리할 수 없습니다 DataZone. 대안은 Amazon Athena 의 `CREATE TABLE` 문을 사용하여 외부 Amazon S3 버킷의 데이터를 프로젝트의 Amazon S3 버킷 내의 새 테이블로 복사하는 것입니다. Amazon Athena 에서 `CREATE TABLE` 쿼리를 실행하면 테이블을 에 등록합니다 AWS Glue Data Catalog.

Amazon S3의 데이터에 대한 경로를 지정하려면 다음 예와 같이 `LOCATION` 속성을 사용합니다.

```
CREATE EXTERNAL TABLE 'test_table'(
```

```
...
)
ROW FORMAT ...
STORED AS INPUTFORMAT ...
OUTPUTFORMAT ...
LOCATION 's3://bucketname/folder/'
```

자세한 내용은 Amazon S3의 테이블 위치를 참조하세요.

외부 S3 버킷의 쿼리 결과(CTAS)에서 테이블 생성

자산을 구독하면 기본 데이터에 대한 액세스는 읽기 전용입니다. Amazon Athena를 사용하여 테이블 사본을 생성할 수 있습니다. Amazon Athena 에서 A CREATE TABLE AS SELECT (CTAS) 쿼리는 다른 쿼리의 SELECT 문 결과에서 Amazon Athena에 새 테이블을 생성합니다. CTAS 구문에 대한 자세한 내용은 CREATE TABLE AS 를 참조하세요.

다음 예제에서는 테이블의 모든 열을 복사해 테이블을 만듭니다.

```
CREATE TABLE new_table AS
SELECT *
FROM old_table;
```

동일한 예제의 다음 변형에서 SELECT 문에는 WHERE 절이 포함되어 있습니다. 이 경우, 쿼리는 테이블에서 WHERE 절을 충족하는 행만 선택합니다.

```
CREATE TABLE new_table AS
SELECT *
FROM old_table WHERE condition;
```

다음 예제에서는 다른 테이블의 열 세트에 대해 실행할 새 쿼리를 생성합니다.

```
CREATE TABLE new_table AS
SELECT column_1, column_2, ... column_n
FROM old_table;
```

동일한 예제의 이번 변형에서는 여러 테이블의 특정 열을 바탕으로 새 테이블을 생성합니다.

```
CREATE TABLE new_table AS
SELECT column_1, column_2, ... column_n
FROM old_table_1, old_table_2, ... old_table_n;
```

새로 생성된 이러한 테이블은 이제 프로젝트 AWS Glue 데이터베이스의 일부이며, 다른 사용자가 검색할 수 있도록 하고 데이터를 Amazon 카탈로그에 자산으로 게시하여 다른 Amazon DataZone DataZone 프로젝트와 공유할 수 있습니다.

Amazon Redshift를 사용하여 데이터 쿼리

Amazon DataZone 데이터 포털에서 데이터 웨어하우스 청사진을 사용하는 환경을 엽니다. 환경 페이지의 오른쪽 패널에서 Amazon Redshift 링크를 선택합니다. 그러면 Amazon Redshift 쿼리 편집기 v2.0에서 환경의 Amazon Redshift 클러스터 또는 Amazon Redshift Serverless 작업 그룹에 대한 연결을 설정하는 데 도움이 되는 필수 세부 정보가 포함된 확인 대화 상자가 열립니다. 연결을 설정하는 데 필요한 세부 정보를 식별했으면 Amazon Redshift 열기 버튼을 선택합니다. 그러면 Amazon DataZone 환경의 임시 보안 인증 정보를 사용하여 브라우저의 새 탭에서 Amazon Redshift 쿼리 편집기 v2.0이 열립니다.

쿼리 편집기에서 환경이 Amazon Redshift Serverless 작업 그룹을 사용하는지 아니면 Amazon Redshift 클러스터를 사용하는지에 따라 아래 단계를 따릅니다.

Amazon Redshift Serverless 작업 그룹의 경우

1. 쿼리 편집기에서 Amazon DataZone 환경의 Amazon Redshift Serverless 작업 그룹을 식별하고 마우스 오른쪽 버튼으로 클릭한 다음 연결 생성 을 선택합니다.
2. 인증할 페더레이션 사용자를 선택합니다.
3. Amazon DataZone 환경의 데이터베이스 이름을 입력합니다.
4. 연결 생성을 선택합니다.

Amazon Redshift 클러스터의 경우:

1. 쿼리 편집기에서 Amazon DataZone 환경의 Amazon Redshift 클러스터를 식별하고 마우스 오른쪽 버튼으로 클릭한 다음 연결 생성 을 선택합니다.
2. 인증을 위해 IAM 자격 증명을 사용하여 임시 자격 증명을 선택합니다.

3. 위의 인증 방법을 사용할 수 없는 경우 왼쪽 하단 모서리에 있는 기어 버튼을 선택하여 계정 설정을 열고 자격 IAM 증명으로 인증을 선택하고 저장합니다. 이는 설정입니다 one-time-only.
4. 연결을 생성할 Amazon DataZone 환경의 데이터베이스 이름을 입력합니다.
5. 연결 생성을 선택합니다.

이제 Amazon Redshift 클러스터 또는 Amazon DataZone 환경에 대해 구성된 Amazon Redshift Serverless 작업 그룹 내의 테이블 및 뷰에 대한 쿼리를 시작할 수 있습니다.

구독한 모든 Amazon Redshift 테이블 또는 뷰는 환경에 대해 구성된 Amazon Redshift 클러스터 또는 Amazon Redshift Serverless 작업 그룹에 연결됩니다. 테이블 및 뷰를 구독하고 환경의 클러스터 또는 데이터베이스에 생성한 새 테이블 및 뷰를 게시할 수 있습니다.

예를 들어 환경이 라는 Amazon Redshift 클러스터`redshift-cluster-1`와 해당 클러스터`dev`의 라는 데이터베이스에 연결되는 시나리오를 살펴보겠습니다. Amazon DataZone 데이터 포털을 사용하여 환경에 추가된 테이블과 뷰를 쿼리할 수 있습니다. 데이터 포털의 오른쪽 창의 `Analytics tools` 섹션에서 이 환경에 대한 Amazon Redshift 링크를 선택하여 쿼리 편집기를 열 수 있습니다. 그런 다음 `redshift-cluster-1` 클러스터를 마우스 오른쪽 버튼으로 클릭하고 IAM 자격 증명 을 사용하여 임시 자격 증명을 사용하여 연결을 생성할 수 있습니다. 연결이 설정되면 개발 데이터베이스에서 환경에 액세스할 수 있는 모든 테이블과 뷰를 볼 수 있습니다.

Amazon의 데이터에 대한 세분화된 액세스 제어 DataZone

Amazon 의 현재 릴리스에서는 데이터에 대한 DataZone세분화된 액세스 제어가 지원되므로 민감한 데이터를 세부적으로 액세스할 수 있습니다. Amazon DataZone 비즈니스 데이터 카탈로그에 게시된 데이터 자산 내의 특정 데이터 레코드에 액세스할 수 있는 프로젝트를 제어할 수 있습니다. Amazon DataZone 은 행 및 열 필터를 지원하여 세분화된 액세스 제어를 구현합니다.

행 필터를 사용하면 정의한 기준에 따라 특정 행에 대한 액세스를 제한할 수 있습니다. 예를 들어 테이블에 두 리전(미국 및 유럽)에 대한 데이터가 포함되어 있고 유럽의 직원이 해당 리전과 관련된 데이터에만 액세스할 수 있도록 하려면 리전이 유럽인 행(예: 리전 = '유럽')을 포함하는 행 필터를 생성할 수 있습니다. 이렇게 하면 유럽의 직원은 미국 데이터에 액세스할 수 없습니다.

열 필터를 사용하면 데이터 자산 내의 특정 열에 대한 액세스를 제한할 수 있습니다. 예를 들어 테이블에 개인 식별 정보(PII)와 같은 민감한 정보가 포함된 경우 열 필터를 생성하여 PII 열을 제외할 수 있습니다. 이렇게 하면 구독자가 민감하지 않은 데이터에만 액세스할 수 있습니다.

세분화된 액세스 제어를 활용하려면 Amazon 에서 AWS Glue 및 Amazon Redshift 자산에 대한 행 및 열 필터를 생성할 수 있습니다 DataZone. 데이터 자산에 액세스하기 위한 구독 요청이 수신되면 적절한 행 및 열 필터를 적용하여 승인할 수 있습니다. Amazon DataZone 은 구독 승인 시 적용한 필터에서 허용하는 행과 열에만 구독자가 액세스할 수 있도록 합니다.

주제

- Amazon에서 행 필터 생성 DataZone
- Amazon에서 열 필터 생성 DataZone
- Amazon에서 행 또는 열 필터 삭제 DataZone
- Amazon에서 행 또는 열 필터 편집 DataZone
- Amazon에서 필터로 액세스 권한 부여 DataZone

Amazon에서 행 필터 생성 DataZone

Amazon을 DataZone 사용하면 구독을 승인할 때 사용할 수 있는 행 필터를 생성하여 구독자가 행 필터에 정의된 대로만 데이터 행에 액세스할 수 있도록 할 수 있습니다. 행 필터를 생성하려면 다음 단계를 따르세요.

1. Amazon DataZone 데이터 포털로 이동하여 Single Sign-On(SSO) 또는 자격 AWS 증명을 사용하여 URL 로그인합니다. Amazon DataZone 관리자인 경우 https://console.aws.amazon.com/

datazone의 Amazon DataZone 콘솔로 이동하여 도메인이 생성된 AWS 계정 로 로그인한 다음 데이터 포털 열기를 선택합니다.

2. 상단 탐색 창에서 프로젝트 선택을 선택하고 자산이 속한 프로젝트를 선택합니다.
3. 프로젝트의 데이터 탭으로 이동합니다.
4. 왼쪽 탐색 창에서 게시된 데이터를 선택한 다음 행 필터를 생성할 자산을 선택합니다. Amazon의 데이터 자산 DataZone 이 AWS Glue 테이블, Amazon Redshift 테이블 또는 Amazon Redshift 뷰 유형인 경우 행 필터를 추가할 수 있습니다.
5. 자산 세부 정보 페이지에서 자산 필터 탭으로 이동한 다음 자산 필터 추가를 선택합니다.
6. 다음 필드를 구성합니다.

   - 이름 - 필터의 이름
   - 설명 - 필터에 대한 설명
7. 필터 유형에서 행 필터 를 선택합니다.
8. 행 필터 표현식에서 행 필터에 하나 이상의 표현식을 제공합니다.

   - 드롭다운에서 열을 선택합니다.
   - 연산자 드롭다운에서 연산자를 선택합니다.
   - 값 필드에 값을 입력합니다.
9. 필터 표현식에 다른 조건을 추가하려면 조건 추가를 선택합니다.
10. 행 필터 표현식에 여러 조건을 사용하는 경우 And 또는 Or를 선택하여 조건을 연결합니다.
11. Create filter(필터 생성)를 선택합니다.

행 필터를 구독에 적용하는 방법에 대한 자세한 내용은 Amazon에서 구독 요청 승인 또는 거부 DataZone 섹션을 참조하세요.

Amazon에서 열 필터 생성 DataZone

Amazon을 DataZone 사용하면 구독을 승인할 때 사용할 수 있는 열 필터를 생성하여 구독자가 열 필터에 정의된 데이터 열에만 액세스할 수 있도록 할 수 있습니다. 열 필터를 생성하려면 다음 단계를 따르세요.

1. Amazon DataZone 데이터 포털로 이동하여 Single Sign-On(SSO) 또는 자격 AWS 증명을 사용하여 URL 로그인합니다. Amazon DataZone 관리자인 경우 https://console.aws.amazon.com/datazone의 Amazon DataZone 콘솔로 이동하여 도메인이 생성된 AWS 계정 로 로그인한 다음 데이터 포털 열기를 선택합니다.

2. 상단 탐색 창에서 프로젝트 선택을 선택하고 자산이 속한 프로젝트를 선택합니다.
3. 프로젝트의 데이터 탭으로 이동합니다.
4. 왼쪽 탐색 창에서 게시된 데이터를 선택한 다음 열 필터를 생성할 자산을 선택합니다. Amazon의 데이터 자산 DataZone 이 AWS Glue 테이블, Amazon Redshift 테이블 또는 Amazon Redshift 뷰 유형인 경우 열 필터를 추가할 수 있습니다.
5. 자산 세부 정보 페이지에서 자산 필터 탭으로 이동한 다음 자산 필터 추가를 선택합니다.
6. 다음 필드를 구성합니다.
   - 이름 - 필터의 이름
   - 설명 - 필터에 대한 설명
7. 필터 유형에서 열 필터 를 선택합니다.
8. 확인란을 다시 사용하여 필터에 포함할 열을 선택하고 데이터 자산의 열을 선택합니다.
9. 필터 생성을 선택합니다.

구독에 열 필터를 적용하는 방법에 대한 자세한 내용은 Amazon에서 구독 요청 승인 또는 거부 DataZone 섹션을 참조하세요.

Amazon에서 행 또는 열 필터 삭제 DataZone

행 또는 열 필터를 삭제하려면 다음 단계를 따릅니다.

1. Amazon DataZone 데이터 포털로 이동하여 Single Sign-On(SSO) 또는 자격 AWS 증명을 사용하여 URL 로그인합니다. Amazon DataZone 관리자인 경우 https://console.aws.amazon.com/datazone의 Amazon DataZone 콘솔로 이동하여 도메인이 생성된 AWS 계정 로 로그인한 다음 데이터 포털 열기를 선택합니다.
2. 프로젝트의 데이터 탭으로 이동합니다.
3. 왼쪽 탐색 창에서 게시된 데이터 또는 인벤토리 데이터를 선택한 다음 행 또는 열 필터를 삭제할 자산을 선택합니다.
4. 자산 세부 정보 페이지에서 자산 필터 탭으로 이동한 다음 삭제할 필터를 엽니다.
5. 작업 , 삭제를 선택한 다음 삭제를 확인합니다.

> **Note**
>
> 활성 구독에 사용되지 않는 필터만 삭제할 수 있습니다.

Amazon에서 행 또는 열 필터 편집 DataZone

행 또는 열 필터를 편집하려면 아래 단계를 따르세요.

1. Amazon DataZone 데이터 포털로 이동하여 Single Sign-On(SSO) 또는 자격 AWS 증명을 사용하여 URL 로그인합니다. Amazon DataZone 관리자인 경우 https://console.aws.amazon.com/datazone의 Amazon DataZone 콘솔로 이동하여 도메인이 생성된 AWS 계정 로 로그인한 다음 데이터 포털 열기를 선택합니다.
2. 프로젝트의 데이터 탭으로 이동합니다.
3. 왼쪽 탐색 창에서 게시된 데이터 또는 인벤토리 데이터를 선택한 다음 행 또는 열 필터를 편집할 자산을 선택합니다.
4. 자산 세부 정보 페이지에서 자산 필터 탭으로 이동한 다음 편집하려는 필터를 엽니다.
5. 다음 필드를 편집할 수 있습니다.
   - 이름 - 필터의 이름
   - 설명 - 필터에 대한 설명
6. 행 필터를 편집하는 경우 행 필터 표현식을 업데이트할 수 있습니다.
7. 열 필터를 편집하는 경우 필터에서 선택한 열을 추가하거나 제거할 수 있습니다.
8. 변경한 후에는 자산 필터 편집을 선택합니다.

> **Note**
>
> 활성 구독에서 사용 중인 필터를 편집하면 Amazon DataZone 은 구독자 프로젝트에 부여된 권한을 자동으로 업데이트합니다. 즉, 구독자는 업데이트된 필터에 정의된 대로만 행 또는 열에 액세스할 수 있으므로 데이터 액세스 정책이 일관되게 적용됩니다.

Amazon에서 필터로 액세스 권한 부여 DataZone

Amazon은 정의된 행 및 열 필터를 AWS Lake Formation 및 Amazon Redshift에 대한 적절한 권한 부여로 변환하여 세분화된 액세스 제어를 DataZone 지원합니다. 다음은 Amazon이 AWS Glue 테이블과 Amazon Redshift 모두에 대해 이러한 필터를 DataZone 구체화하는 방법에 대한 설명입니다.

AWS Glue 테이블

행 및/또는 열 필터가 있는 AWS Glue 테이블에 대한 구독이 승인되면 Amazon은 AWS Lake Formation with Data Cell Filters에서 권한 부여를 생성하여 구독 프로젝트의 멤버가 구독에 적용된 필터를 기반으로 액세스가 허용된 행 및 열에만 액세스할 수 있도록 함으로써 구독을 DataZone 구체화합니다.

Amazon은 DataZone 먼저 Amazon에 적용된 행 및 열 필터를 AWS Lake Formation 데이터 셀 필터 DataZone 로 변환합니다. 여러 행 및 열 필터를 사용하는 경우 Amazon은 모든 열과 모든 행 필터 조건을 DataZone 결합하여 행 및 열 수준 모두에서 유효 권한을 계산합니다. DataZone 그런 다음 Amazon은 유효한 행 및 열 권한을 사용하여 단일 AWS Lake Formation 데이터 셀 필터를 생성합니다.

데이터 셀 필터가 생성되면 Amazon은 이 데이터 셀 필터를 사용하여 AWS Lake Formation에서 읽기 전용(SELECT) 권한을 생성하여 구독자 프로젝트와 구독 테이블을 DataZone 공유합니다.

Amazon Redshift

Amazon Redshift table/view with row and/or 열 필터에 대한 구독이 승인되면 Amazon Redshift에서 범위가 축소된 후기 바인딩 뷰를 생성하여 구독 프로젝트의 멤버가 구독에 적용된 행 및 열 필터를 기반으로 액세스할 수 있는 행 및 열에만 액세스할 수 있도록 함으로써 구독을 DataZone 구체화합니다.

Amazon은 DataZone 먼저 Amazon의 구독에 적용된 행 및 열 필터를 Amazon Redshift 후기 바인딩 보기 DataZone 로 변환합니다. 여러 행 및 열 필터를 사용하는 경우 Amazon은 모든 열과 의 모든 행 필터 조건을 DataZone 결합하여 행 및 열 수준 모두에서 유효 권한을 계산합니다. DataZone 그런 다음 Amazon은 유효한 행 및 열 권한을 사용하여 지연 바인딩 보기를 생성합니다.

지연 바인딩 뷰가 생성되면 Amazon Redshift에서 읽기 전용(SELECT) 권한을 생성하여 Amazon은 구독자 프로젝트 멤버와 이 뷰를 DataZone 공유합니다.

아마존 DataZone 이벤트 및 알림

DataZone Amazon은 구독 요청, 업데이트, 의견, 시스템 이벤트 등 데이터 포털 내의 중요한 활동을 지속적으로 알려줍니다. Amazon은 데이터 포털의 전용 수신함이나 Amazon EventBridge 기본 버스를 통해 메시지를 전송하여 이 정보를 DataZone 제공합니다.

Amazon DataZone 데이터 포털의 전용 수신함을 통한 이벤트

DataZone Amazon은 데이터 포털에 메시지를 보고 조치를 취할 수 있는 전용 수신함을 제공합니다. 최근 메시지는 홈페이지, 프로젝트 페이지, 카탈로그 페이지에도 표시됩니다. 예를 들어 사용자가 데이터 자산에 대한 액세스를 요청하면 해당 자산의 게시 프로젝트 소유자 및 기여자는 데이터 포털에서 요청을 확인하고, 조치가 취해지면 이 요청과 관련된 구독 프로젝트의 프로젝트 구성원은 데이터 포털의 알림을 볼 수 있습니다. 메시지에는 두 가지 유형이 있습니다.

- 태스크 - 이 메시지는 수신자에게 어딘가에 필요한 조치가 있음을 알립니다. 추적에 사용할 수 있는 선택적 상태 필드가 있습니다.
- 이벤트 - 이러한 메시지는 정보 제공용이며 상태가 지정되지 않습니다. 이벤트는 최근 업데이트에 대한 감사 추적을 제공합니다.

DataZoneAmazon에서는 다음 이벤트 유형에 대해 메시지가 생성됩니다.

이벤트 범주	이벤트 이름	이벤트 설명	이벤트 유형
구독	구독 요청 생성됨	구독 요청이 생성되면 이벤트가 생성됩니다.	작업
구독	구독 요청이 수락되었습니다.	구독 요청이 수락되면 이벤트가 생성됩니다.	Event
구독	구독 요청이 거부되었습니다.	구독 요청이 거부되면 이벤트가 생성됩니다.	Event
구독	구독 요청이 삭제되었습니다.	구독 요청이 삭제되면 이벤트가 생성됩니다.	Event

이벤트 범주	이벤트 이름	이벤트 설명	이벤트 유형
프로젝트	프로젝트 생성 성공	프로젝트 생성이 성공하면 이벤트가 생성됩니다.	Event
프로젝트 멤버십	프로젝트 멤버 추가 성공	프로젝트에 새 멤버가 추가되면 이벤트가 생성됩니다.	Event
프로젝트 멤버십	프로젝트 멤버 제거 성공	멤버가 프로젝트에서 제거되면 이벤트가 생성됩니다.	Event
프로젝트 멤버십	프로젝트 멤버 역할 변경 성공	이벤트가 생성되었습니다. 프로젝트에서 구성원의 역할이 변경됩니다.	Event
환경	환경 배포가 시작되었습니다.	환경 배포가 시작될 때 이벤트가 생성됩니다.	Event
환경	환경 배포가 완료되었습니다.	환경 배포가 성공적으로 완료되면 이벤트가 생성됩니다.	Event
환경	환경 배포에 실패했습니다.	환경 배포가 실패하면 이벤트가 생성됩니다.	Event
환경	환경 배포 사용자 지정 워크플로가 시작됨	사용자 지정 워크플로가 있는 환경이 시작되면 이벤트가 생성됩니다.	Event
데이터 자산	인벤토리에 추가된 자산	새 데이터 자산이 인벤토리에 추가될 때 (즉, 카탈로그에 초안 상태로 추가될 때) 이벤트가 생성됩니다.	Event

이벤트 범주	이벤트 이름	이벤트 설명	이벤트 유형
데이터 자산	자산 공개	새 데이터 자산이 게시될 때 (예: 구독이 가능한 경우) 이벤트가 생성됩니다.	Event
데이터 자산	에셋 스키마가 변경되었습니다.	이전 수집 작업 이후 자산 스키마가 변경되면 이벤트가 생성됩니다.	Event
구독	구독이 생성되었습니다.	누군가가 데이터 자산 구독을 요청하면 이벤트가 생성됩니다.	작업
구독	구독이 승인되었습니다.	게시 프로젝트 소유자 또는 기여자가 구독을 승인하면 이벤트가 생성됩니다.	Event
구독	구독이 거부되었습니다.	게시 프로젝트 소유자 또는 기여자가 구독을 거부하면 이벤트가 생성됩니다.	Event
구독	구독이 삭제되었습니다.	구독자가 구독을 취소하면 이벤트가 생성됩니다.	Event
구독	구독 허가가 요청되었습니다.	누군가가 자산에 대한 액세스를 요청하면 이벤트가 생성됩니다.	Event

이벤트 범주	이벤트 이름	이벤트 설명	이벤트 유형
구독	구독 허가가 완료되었습니다.	게시 프로젝트 소유자 또는 기여자가 구독에 에셋 액세스 권한을 부여하면 이벤트가 생성됩니다.	Event
구독	구독 권한 부여 실패	구독 허가가 실패하면 이벤트가 생성됩니다.	Event
구독	구독 허가 취소가 요청되었습니다.	게시 프로젝트 소유자 또는 기여자가 취소된 구독 허가를 시작하면 이벤트가 생성됩니다.	Event
구독	구독 허가 취소 완료	구독 허가 취소가 완료되면 이벤트가 생성됩니다.	Event
구독	구독 허가 취소에 실패했습니다.	구독 허가 취소가 실패하면 이벤트가 생성됩니다.	Event
자동 비즈니스 이름 생성	비즈니스 이름 생성 성공	자동화된 비즈니스 이름 생성 작업이 성공적으로 완료될 때 이벤트가 생성됩니다.	Event
자동 비즈니스 이름 생성	비즈니스 이름 생성 실패	자동 비즈니스 이름 생성 작업이 실패하면 이벤트가 생성됩니다.	Event
데이터 소스 실행	데이터 소스가 생성되었습니다.	새 데이터 소스가 생성되면 이벤트가 생성됩니다.	Event

이벤트 범주	이벤트 이름	이벤트 설명	이벤트 유형
데이터 소스 실행	데이터 소스 업데이트	기존 데이터 소스가 업데이트되면 이벤트가 생성됩니다.	Event
데이터 소스 실행	데이터 소스 실행이 트리거됨	데이터 소스 실행이 시작될 때 이벤트가 생성됩니다.	Event
데이터 소스 실행	데이터 소스 실행 성공	데이터 소스 실행이 성공하면 이벤트가 생성됩니다.	Event
데이터 소스 실행	데이터 소스 실행 실패	데이터 소스 실행이 실패하면 이벤트가 생성됩니다.	Event

데이터 포털 수신함에서 작업을 보려면 다음 단계를 완료하세요.

1. 데이터 포털을 사용하여 Amazon DataZone 데이터 포털로 URL 이동하고 다음을 사용하여 SSO 로그인합니다. AWS 자격 증명. Amazon DataZone 관리자인 경우 Amazon DataZone 콘솔의 URL https://console.aws.amazon.com/datazone에 액세스하여 데이터 포털을 이용할 수 있습니다. AWS Amazon DataZone 도메인이 생성된 계정
2. 데이터 포털에서 최근 작업 세트가 포함된 팝업을 보려면 검색 표시줄 옆에 있는 종 아이콘을 선택합니다.
3. 모든 작업을 보려면 모두 보기를 선택합니다. 이벤트 탭을 선택하여 보기를 변경하고 모든 이벤트를 볼 수 있습니다.
4. 이벤트 제목, 활성 또는 비활성 상태 또는 날짜 범위를 기준으로 검색을 필터링할 수 있습니다.
5. 개별 작업을 선택하여 작업에 응답할 수 있는 위치로 이동합니다.

데이터 포털 수신함에서 이벤트를 보려면 다음 단계를 완료하세요.

1. 데이터 포털을 사용하여 Amazon DataZone 데이터 포털로 URL 이동하고 다음을 사용하여 SSO 로그인합니다. AWS 자격 증명. Amazon DataZone 관리자인 경우 Amazon DataZone 콘솔의 URL

https://console.aws.amazon.com/datazone에 액세스하여 데이터 포털을 이용할 수 있습니다. AWS Amazon DataZone 루트 도메인이 생성된 계정

2. 데이터 포털에서 최근 이벤트 세트의 팝업을 보려면 검색 표시줄 옆에 있는 종 아이콘을 선택합니다.
3. 모든 이벤트를 보려면 모두 보기를 선택합니다. 태스크 탭을 선택하여 보기를 변경하고 모든 작업을 볼 수 있습니다.
4. 이벤트 제목 또는 날짜 범위를 기준으로 검색을 필터링합니다.
5. 개별 이벤트를 선택하여 해당 이벤트에 대한 세부 정보를 볼 수 있는 위치로 이동합니다.

Amazon EventBridge 기본 버스를 통한 이벤트

데이터 포털의 전용 수신함으로 메시지를 보내는 것 외에도 메시지를 동일한 위치에 있는 Amazon EventBridge 기본 이벤트 버스로 보낼 DataZone 수도 있습니다. AWS Amazon DataZone 루트 도메인이 호스팅되는 계정 이를 통해 구독 이행 또는 다른 도구와의 사용자 지정 통합과 같은 이벤트 기반 자동화가 가능합니다. 들어오는 Amazon EventBridge 이벤트와 일치하는 규칙을 생성하고 이를 Amazon EventBridge 대상으로 전송하여 처리할 수 있습니다. 단일 규칙으로 이벤트를 여러 대상으로 전송한 다음, 병렬로 실행할 수 있습니다.

샘플 이벤트는 다음과 같습니다.


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

DataZone Amazon에서 지원하는 상세 유형의 전체 목록은 다음과 같습니다.

- 구독 요청 생성됨
- 구독 요청 수락됨
- 구독 요청 거부됨
- 구독 요청 삭제됨
- 구독 허가가 요청되었습니다.
- 구독 보조금 완료
- 구독 보조금 실패
- 구독 보조금 취소 요청
- 구독 보조금 취소 완료
- 구독 보조금 취소 실패
- 자산이 인벤토리에 추가됨
- 카탈로그에 추가된 자산

- 에셋 스키마 변경됨
- 데이터 소스 상태 변경
- 데이터 소스 생성됨
- 데이터 소스 업데이트
- 데이터 소스 실행이 트리거됨
- 데이터 소스 실행 성공
- 데이터 소스 실행 실패
- 도메인 생성 성공
- 도메인 생성 실패
- 도메인 삭제 성공
- 도메인 삭제 실패
- 환경 배포 시작됨
- 환경 배포가 완료되었습니다.
- 환경 배포 실패
- 환경 삭제가 시작됨
- 환경 삭제가 완료되었습니다.
- 환경 삭제 실패
- 프로젝트 생성 성공
- 프로젝트 멤버 추가 성공
- 프로젝트 멤버 제거 성공
- 프로젝트 멤버 역할 변경 성공
- 환경 배포, 고객 워크플로가 시작되었습니다.
- 비즈니스 이름 생성 성공
- 비즈니스 이름 생성 실패

자세한 내용은 Amazon을 참조하십시오 EventBridge.

Amazon의 보안 DataZone

의 클라우드 보안 AWS 이 최우선 순위입니다. AWS 고객은 가장 보안에 민감한 조직의 요구 사항을 충족하도록 구축된 데이터 센터 및 네트워크 아키텍처의 이점을 누릴 수 있습니다.

보안은 AWS 와 사용자 간의 공동 책임입니다. 공동 책임 모델은 이 사항을 클라우드의 보안 및 클라우드 내 보안으로 설명합니다.

- 클라우드 보안 - 에서 AWS 서비스를 실행하는 인프라를 보호할 AWS 책임이 있습니다 AWS 클라우드. AWS 또한 는 안전하게 사용할 수 있는 서비스를 제공합니다. 타사 감사자는 AWS 규정 준수 프로그램 프로그램의 일환으로 보안의 효과를 정기적으로 테스트하고 확인합니다. Amazon 에 적용되는 규정 준수 프로그램에 대한 자세한 내용은 규정 준수 AWS 프로그램 의 범위 내 서비스 규정 준수 프로그램 DataZone참조하세요.
- 클라우드의 보안 - 사용자의 책임은 사용하는 AWS 서비스에 따라 결정됩니다. 또한 귀하는 귀사의 데이터의 민감도, 귀사의 요구 사항, 관련 법률 및 규정을 비롯한 기타 요소에 대해서도 책임이 있습니다.

이 설명서는 Amazon 를 사용할 때 공동 책임 모델을 적용하는 방법을 이해하는 데 도움이 됩니다 DataZone. 다음 주제에서는 보안 및 규정 준수 목표에 맞게 Amazon DataZone 을 구성하는 방법을 보여줍니다. 또한 Amazon DataZone 리소스를 모니터링하고 보호하는 데 도움이 되는 다른 AWS 서비스를 사용하는 방법도 알아봅니다.

주제

- Amazon의 데이터 보호 DataZone
- Amazon에서의 권한 부여 DataZone
- 를 사용하여 Amazon DataZone 리소스에 대한 액세스 제어 IAM
- Amazon에 대한 규정 준수 검증 DataZone
- Amazon의 보안 모범 사례 DataZone
- Amazon의 복원력 DataZone
- Amazon의 인프라 보안 DataZone
- Amazon의 교차 서비스 혼동 대리자 방지 DataZone
- Amazon의 구성 및 취약성 분석 DataZone
- 허용 목록에 추가할 도메인

Amazon의 데이터 보호 DataZone

AWS 공동 책임 모델 Amazon 의 데이터 보호에 적용됩니다 DataZone. 이 모델에 설명된 대로 AWS 는 모든 를 실행하는 글로벌 인프라를 보호할 책임이 있습니다 AWS 클라우드. 사용자는 인프라에서 호스팅되는 콘텐츠를 관리해야 합니다. 사용하는 AWS 서비스 의 보안 구성과 관리 작업에 대한 책임도 사용자에게 있습니다. 데이터 프라이버시에 대한 자세한 내용은 데이터 프라이버시 섹션을 FAQ참조하세요. 유럽의 데이터 보호에 대한 자세한 내용은 AWS 보안 블로그의 AWS 책임 공유 모델 및 GDPR 블로그 게시물을 참조하세요.

데이터 보호를 위해 자격 증명을 보호하고 AWS 계정 AWS IAM Identity Center 또는 AWS Identity and Access Management ()를 사용하여 개별 사용자를 설정하는 것이 좋습니다IAM. 이렇게 하면 개별 사용자에게 자신의 직무를 충실히 이행하는 데 필요한 권한만 부여됩니다. 또한 다음과 같은 방법으로 데이터를 보호하는 것이 좋습니다.

- 각 계정에 다단계 인증(MFA)을 사용합니다.
- SSL/TLS를 사용하여 AWS 리소스와 통신합니다. TLS 1.2가 필요하며 TLS 1.3을 권장합니다.
- 를 사용하여 API 및 사용자 활동 로깅을 설정합니다 AWS CloudTrail. CloudTrail 추적을 사용하여 AWS 활동을 캡처하는 방법에 대한 자세한 내용은 AWS CloudTrail 사용 설명서의 CloudTrail 추적 작업을 참조하세요.
- AWS 암호화 솔루션과 내의 모든 기본 보안 제어를 사용합니다 AWS 서비스.
- Amazon S3에 저장된 민감한 데이터를 검색하고 보호하는 데 도움이 되는 Amazon Macie와 같은 고급 관리형 보안 서비스를 사용하세요.
- 명령줄 인터페이스 또는 FIPS 를 AWS 통해 액세스할 때 140-3 검증 암호화 모듈이 필요한 경우 FIPS 엔드포인트를 API사용합니다. 사용 가능한 FIPS 엔드포인트에 대한 자세한 내용은 연방 정보 처리 표준(FIPS) 140-3을 참조하세요.

고객의 이메일 주소와 같은 기밀 정보나 중요한 정보는 태그나 이름 필드와 같은 자유 양식 필드에 입력하지 않는 것이 좋습니다. 여기에는 콘솔, 또는 를 사용하여 Amazon DataZone 또는 기타 AWS 서비스 에서 작업하는 경우가 포함됩니다API AWS CLI AWS SDKs. 이름에 사용되는 태그 또는 자유 형식 텍스트 필드에 입력하는 모든 데이터는 청구 또는 진단 로그에 사용될 수 있습니다. 외부 서버에 URL 를 제공하는 경우 해당 서버에 대한 요청을 검증URL하기 위해 에 보안 인증 정보를 포함하지 않는 것이 좋습니다.

데이터 암호화

권한을 부여할 때 누가 어떤 Amazon DataZone 리소스에 대한 권한을 받을지 결정합니다. 해당 리소스에서 허용할 작업을 사용 설정합니다. 따라서 작업을 수행하는 데 필요한 권한만 부여해야 합니다. 최소 권한 액세스를 구현하는 것이 오류 또는 악의적인 의도로 인해 발생할 수 있는 보안 위험과 영향을 최소화할 수 있는 근본적인 방법입니다.

저장 중 암호화

Amazon은 기본적으로 사용자를 AWS 소유 및 관리하는 AWS Key Management Service(AWS KMS) 키를 사용하여 모든 데이터를 DataZone 암호화합니다. 로 관리하는 키를 사용하여 Amazon DataZone 카탈로그에 저장된 데이터를 암호화할 수도 있습니다 AWS KMS.

Amazon 에서 도메인을 생성할 때 데이터 암호화 에서 암호화 설정 사용자 지정(고급) 옆의 확인란을 선택하고 키를 제공하여 암호화 설정을 제공할 DataZone수 있습니다. KMS

전송 중 암호화

Amazon DataZone 은 전송 계층 보안(TLS) 및 클라이언트 측 암호화를 사용하여 전송 중 암호화를 수행합니다. Amazon과의 통신 DataZone 은 항상 를 통해 수행HTTPS되므로 전송 중에 데이터가 항상 암호화됩니다.

인터네트워크 트래픽 개인 정보 보호

계정 간 연결을 보호하기 위해 Amazon은 서비스 역할 및 IAM 역할을 DataZone 사용하여 고객 계정에 안전하게 연결하고 고객을 대신하여 작업을 실행합니다.

주제

- Amazon에 대한 저장 데이터 암호화 DataZone
- Amazon용 인터페이스 VPC 엔드포인트 사용 DataZone

Amazon에 대한 저장 데이터 암호화 DataZone

저장 데이터를 기본적으로 암호화하면 민감한 데이터 보호와 관련된 운영 오버헤드와 복잡성을 줄이는 데 도움이 됩니다. 동시에 엄격한 암호화 규정 준수 및 규제 요구 사항을 충족하는 안전한 애플리케이션을 구축할 수 있습니다.

Amazon DataZone 은 기본 AWS소유 키를 사용하여 저장 데이터를 자동으로 암호화합니다. AWS 소유 키의 사용을 보거나 관리하거나 감사할 수 없습니다. 자세한 내용은 AWS 소유 키 를 참조하세요.

이 암호화 계층을 비활성화하거나 대체 암호화 유형을 선택할 수는 없지만 Amazon DataZone 도메인을 생성할 때 고객 관리형 키를 선택하여 기존 AWS 소유 암호화 키에 두 번째 암호화 계층을 추가할 수 있습니다. Amazon은 기존 소유 암호화에 두 번째 암호화 계층을 추가하기 위해 생성, 소유 및 관리할 수 있는 대칭 고객 관리 AWS 형 키 사용을 DataZone 지원합니다. 이 암호화 계층을 완전히 제어할 수 있으므로 이 계층에서 다음 작업을 수행할 수 있습니다.

- 주요 정책 수립 및 유지 관리
- IAM 정책 및 권한 부여 설정 및 유지
- 키 정책 활성화 및 비활성화
- 키 암호화 자료 교체
- 태그 추가
- 키 별칭 생성
- 삭제할 일정 키

자세한 내용은 고객 관리형 키 섹션을 참조하세요.

> **Note**
>
> Amazon은 AWS 소유 키를 사용하여 저장 시 암호화를 DataZone 자동으로 활성화하여 고객 데이터를 무료로 보호합니다.
> AWS KMS 고객 관리형 키를 사용하는 경우 요금이 부과됩니다. 요금에 대한 자세한 내용은 AWS Key Management Service 요금 섹션을 참조하세요.

Amazon이 에서 권한 부여를 DataZone 사용하는 방법 AWS KMS

Amazon에서 고객 관리형 키를 사용하려면 세 가지 권한 부여가 DataZone 필요합니다. 고객 관리형 키로 암호화된 Amazon DataZone 도메인을 생성하면 Amazon은 에 CreateGrant 요청을 전송하여 사용자를 대신하여 권한 부여 및 하위 권한 부여를 DataZone 생성합니다 AWS KMS. 의 AWS KMS 권한 부여는 Amazon에 계정의 KMS 키에 대한 DataZone 액세스 권한을 부여하는 데 사용됩니다. Amazon은 다음과 같은 내부 작업에 고객 관리형 키를 사용하도록 다음과 같은 권한을 DataZone 생성합니다.

다음 작업을 위해 저장 데이터를 암호화할 수 있는 권한 1개:

- Amazon DataZone 도메인 컬렉션을 생성할 때 입력한 대칭 고객 관리형 KMS 키 ID가 유효한지 확인하기 위해 AWS KMS 에 DescribeKey 요청을 보냅니다.

- GenerateDataKeyrequests 로 AWS KMS 전송하여 고객 관리형 키로 암호화된 데이터 키를 생성합니다.
- 에 AWS KMS 복호화 요청을 보내 암호화된 데이터 키를 복호화하여 데이터를 암호화하는 데 사용할 수 있도록 합니다.
- RetireGrant 도메인이 삭제될 때 부여를 사용 중지합니다.

데이터 검색 및 검색에 대한 두 가지 권한 부여:

- 권한 부여 2:
  - DescribeKey
  - GenerateDataKey
  - 암호화, 복호화, ReEncrypt
  - CreateGrant 에서 내부적으로 사용하는 AWS 서비스에 대한 하위 권한 부여를 생성합니다 DataZone.
  - RetireGrant
- 권한 부여 3:
  - GenerateDataKey
  - Decrypt
  - RetireGrant

언제든지 권한 부여에 대한 액세스 권한을 취소하거나 고객 관리형 키에 대한 서비스 액세스를 제거할 수 있습니다. 이 경우 Amazon DataZone 은 고객 관리형 키로 암호화된 데이터에 액세스할 수 없으며, 이는 해당 데이터에 의존하는 작업에 영향을 미칩니다. 예를 들어 Amazon이 액세스할 DataZone 수 없는 데이터 자산 세부 정보를 가져오려고 하면 작업이 `AccessDeniedException` 오류를 반환합니다.

고객 관리형 키 생성

AWS 관리 콘솔 또는 를 사용하여 대칭 고객 관리형 키를 생성할 수 있습니다 AWS KMSAPIs.

대칭 고객 관리형 키를 생성하려면 AWS Key Management Service 개발자 안내서의 대칭 고객 관리형 키 생성 단계를 따르세요.

키 정책 - 키 정책은 고객 관리형 키에 대한 액세스를 제어합니다. 모든 고객 관리형 키에는 키를 사용할 수 있는 사람과 키를 사용하는 방법을 결정하는 문장이 포함된 정확히 하나의 키 정책이 있어야 합니다. 고객 관리형 키를 생성할 때 키 정책을 지정할 수 있습니다. 자세한 내용은 AWS Key Management Service 개발자 안내서의 고객 관리형 키에 대한 액세스 관리를 참조하세요.

Amazon DataZone 리소스와 함께 고객 관리형 키를 사용하려면 키 정책에서 다음 API 작업을 허용해야 합니다.

- kms:CreateGrant – 고객 관리형 키에 권한을 추가합니다. 지정된 KMS 키에 대한 제어 액세스 권한을 부여합니다. 이렇게 하면 Amazon에서 DataZone 요구하는 작업에 대한 액세스 권한을 부여할 수 있습니다. 권한 부여 사용에 대한 자세한 내용은 AWS Key Management Service 개발자 안내서를 참조하세요.
- kms:DescribeKey – Amazon이 키를 DataZone 검증할 수 있도록 고객 관리형 키 세부 정보를 제공합니다.
- kms:GenerateDataKey – 외부에서 사용할 수 있는 고유한 대칭 데이터 키를 반환합니다 AWS KMS.
- kms:Decrypt – KMS 키로 암호화된 암호 텍스트를 해독합니다.

다음은 Amazon 에 추가할 수 있는 정책 설명 예제입니다 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**
>
> KMS 정책에 대한 거부는 Amazon DataZone 데이터 포털을 통해 액세스하는 리소스에 적용되지 않습니다.

정책 에서 권한을 지정하는 방법에 대한 자세한 내용은 AWS Key Management Service 개발자 안내서를 참조하세요.

키 액세스 문제 해결에 대한 자세한 내용은 AWS 키 관리 서비스 개발자 안내서를 참조하세요.

Amazon의 고객 관리형 키 지정 DataZone

Amazon DataZone 암호화 컨텍스트

암호화 컨텍스트는 데이터에 대한 추가 컨텍스트 정보를 포함하는 선택적 키-값 페어 세트입니다.

AWS KMS 는 암호화 컨텍스트를 추가 인증 데이터로 사용하여 인증된 암호화 를 지원합니다. 데이터 AWS KMS 암호화 요청에 암호화 컨텍스트를 포함하면 는 암호화 컨텍스트를 암호화된 데이터에 바인딩합니다. 요청에 동일한 암호화 컨텍스트를 포함해야 이 데이터를 해독할 수 있습니다.

Amazon은 다음 암호화 컨텍스트를 DataZone 사용합니다.

```
"encryptionContextSubset": {
    "aws:datazone:domainId": "{root-domain-uuid}"
}
```

모니터링을 위한 암호화 컨텍스트 사용 - 대칭 고객 관리형 키를 사용하여 Amazon 를 암호화하는 경우 감사 레코드 및 로그의 암호화 컨텍스트를 사용하여 고객 관리형 키가 어떻게 사용되고 있는지 식별할 수도 DataZone있습니다. 암호화 컨텍스트는 AWS CloudTrail 또는 Amazon Logs에서 생성한 CloudWatch 로그에도 나타납니다.

암호화 컨텍스트를 사용하여 고객 관리형 키에 대한 액세스 제어 - 키 정책 및 IAM 정책의 암호화 컨텍스트를 조건으로 사용하여 대칭 고객 관리형 키에 대한 액세스를 제어할 수 있습니다. 또한 권한 부여에서 암호화 컨텍스트 제약 조건을 사용할 수 있습니다.

Amazon은 권한 부여에서 암호화 컨텍스트 제약 조건을 DataZone 사용하여 계정 또는 리전의 고객 관리형 키에 대한 액세스를 제어합니다. 권한 부여 제약 조건에 따라 권한 부여가 허용하는 작업은 지정된 암호화 컨텍스트를 사용해야 합니다.

다음은 특정 암호화 컨텍스트에서 고객 관리형 키에 대한 액세스 권한을 부여하는 키 정책 설명의 예입니다. 이 정책 설명의 조건에 따라 권한 부여에는 암호화 컨텍스트를 지정하는 암호화 컨텍스트 제약 조건이 있어야 합니다.

```
{
```

```
    "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}"
        }
    }
}
```

Amazon용 암호화 키 모니터링 DataZone

Amazon DataZone 리소스와 AWS KMS 함께 고객 관리형 키를 사용하는 경우 AWS CloudTrail를 사용하여 Amazon이 에 DataZone 보내는 요청을 추적할 수 있습니다 AWS KMS. 다음 예제는 고객 관리형 키로 암호화된 데이터에 액세스`DescribeKey`하기 위해 Amazon에서 호출하는 KMS 작업을 모니터링 DataZone 하기 위한 `CreateGrant`, `GenerateDataKey`, `Decrypt`, 및 AWS CloudTrail 이벤트입니다. 고객 관리형 키를 사용하여 AWS KMS Amazon DataZone 도메인을 암호화하면 Amazon은 사용자를 대신하여 AWS 계정의 KMS 키에 액세스하라는 `CreateGrant` 요청을 DataZone 보냅니다. Amazon이 DataZone 생성하는 권한은 고객 관리형 키와 AWS KMS 연결된 리소스에 따라 다릅니다. 또한 Amazon DataZone 은 도메인을 삭제할 때 `RetireGrant` 작업을 사용하여 권한을 제거합니다. 다음 예제 이벤트는 `CreateGrant` 작업을 기록합니다.

```
{
    "eventVersion": "1.08",
    "userIdentity": {
```

```
        "type": "AssumedRole",
        "principalId": "AROAIGDTESTANDEXAMPLE:Sampleuser01",
        "arn": "arn:aws:sts::111122223333:assumed-role/Admin/Sampleuser01",
        "accountId": "111122223333",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE3",
        "sessionContext": {
            "sessionIssuer": {
                "type": "Role",
                "principalId": "AROAIGDTESTANDEXAMPLE:Sampleuser01",
                "arn": "arn:aws:sts::111122223333:assumed-role/Admin/Sampleuser01",
                "accountId": "111122223333",
                "userName": "Admin"
            },
            "webIdFederationData": {},
            "attributes": {
                "mfaAuthenticated": "false",
                "creationDate": "2021-04-22T17:02:00Z"
            }
        },
        "invokedBy": "datazone.amazonaws.com"
    },
    "eventTime": "2021-04-22T17:07:02Z",
    "eventSource": "kms.amazonaws.com",
    "eventName": "CreateGrant",
    "awsRegion": "us-west-2",
    "sourceIPAddress": "172.12.34.56",
    "userAgent": "ExampleDesktop/1.0 (V1; OS)",
    "requestParameters": {
        "constraints": {
            "encryptionContextSubset": {
                "aws:datazone:domainId": "SAMPLE-root-domain-uuid"
            }
        },
        "keyId": "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-123456SAMPLE",
        "operations": [
            "Decrypt",
            "GenerateDataKey",
            "RetireGrant",
            "DescribeKey"
        ],
        "granteePrincipal": "datazone.us-west-2.amazonaws.com"
    },
    "responseElements": {
```

```
        "grantId":
 "0ab0ac0d0b000f00ea00cc0a0e00fc00bce000c000f0000000c0bc0a0000aaafSAMPLE",
        "keyId": "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-123456SAMPLE"
    },
    "requestID": "ff000af-00eb-00ce-0e00-ea000fb0fba0SAMPLE",
    "eventID": "ff000af-00eb-00ce-0e00-ea000fb0fba0SAMPLE",
    "readOnly": false,
    "resources": [
        {
            "accountId": "111122223333",
            "type": "AWS::KMS::Key",
            "ARN": "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-123456SAMPLE"
        }
    ],
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "eventCategory": "Management",
    "recipientAccountId": "111122223333"
}
```

암호화된 AWS Glue 카탈로그가 포함된 Data Lake 환경 생성

고급 사용 사례에서는 암호화된 AWS Glue 카탈로그를 사용할 때 고객 관리형 KMS 키를 사용하려면 Amazon DataZone 서비스에 대한 액세스 권한을 부여해야 합니다. 사용자 지정 KMS 정책을 업데이트하고 키에 태그를 추가하여 이 작업을 수행할 수 있습니다. 암호화된 AWS Glue 카탈로그의 데이터로 작업할 수 있는 Amazon DataZone 서비스에 대한 액세스 권한을 부여하려면 다음을 수행합니다.

- 사용자 지정 KMS 키에 다음 정책을 추가합니다. 자세한 내용은 키 정책 변경을 참조하세요.

```
{
  "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*"
    }
  }
}
```

- 사용자 지정 KMS 키에 다음 태그를 추가합니다. 자세한 내용은 태그 사용을 참조하세요KMS.

```
key: AmazonDataZoneEnvironment
value: all
```

Amazon용 인터페이스 VPC 엔드포인트 사용 DataZone

Amazon Virtual Private Cloud(Amazon VPC)를 사용하여 AWS 리소스를 호스팅하는 경우 AmazonVPC과 Amazon 간에 연결을 설정할 수 있습니다 DataZone. 퍼블릭 인터넷을 통과 DataZone 하지 않고도 Amazon에서 이 연결을 사용할 수 있습니다.

Amazon을 VPC 사용하면 사용자 지정 가상 네트워크에서 AWS 리소스를 시작할 수 있습니다. VPC 를 사용하여 IP 주소 범위, 서브넷, 라우팅 테이블 및 네트워크 게이트웨이와 같은 네트워크 설정을 제어할 수 있습니다. 에 대한 자세한 내용은 Amazon VPC 사용 설명서 섹션을 VPCs참조하세요.

Amazon을 Amazon VPC에 연결하려면 먼저 인터페이스 VPC 엔드포인트를 정의해야 DataZone합니다. 이렇게 하면 를 다른 AWS 서비스에 연결할 VPC 수 있습니다. 엔드포인트는 인터넷 게이트웨이, 네트워크 주소 변환(NAT) 인스턴스 또는 연결 없이 안정적이고 확장 가능한 VPN 연결을 제공합니다. VPC 엔드포인트를 생성하는 방법에 대한 자세한 내용과 단계는 Amazon VPC 사용 설명서의 인터페이스 VPC 엔드포인트(AWS PrivateLink)를 참조하세요.

> **Important**
>
> 에서 VPC엔드포인트 정책은 VPC 엔드포인트에 연결하여 엔드포인트를 사용하여 서비스에 액세스할 수 있는 AWS 보안 주체를 제어할 수 있는 리소스 기반 정책입니다 AWS .

Amazon 의 현재 릴리스에서는 Amazon과 Amazon 간의 연결을 설정하고 사용하는 데 DataZone엔드포인트 정책 사용이 지원되지 않습니다VPC DataZone. Amazon DataZone 액세스 관리는 서비스 수준에서 정의된 RAM 구성 및 IAM 보안 주체 정책에 의존합니다.

Amazon에서의 권한 부여 DataZone

Amazon DataZone의 인터페이스는 내의 관리 콘솔 AWS 과 비콘솔 웹 애플리케이션(데이터 포털)으로 구성됩니다.

Amazon DataZone 관리 콘솔은 도메인 생성 및 관리APIs, 이러한 도메인에 대한 AWS 계정 연결, Amazon top-level-resource 에 액세스 관리를 위임하려는 데이터 소스를 포함하여 AWS 관리자가 에 사용할 수 있습니다 DataZone. Amazon DataZone 관리 콘솔을 사용하여 명시적으로 구성된 AWS 계정에 대해 Amazon DataZone 서비스에 액세스 관리 제어를 위임하는 데 필요한 모든 IAM 역할과 구성을 관리할 수 있습니다. Amazon DataZone 데이터 포털은 SSO 사용자를 위한 자사 AWS Identity Center 애플리케이션입니다. 활성화된 경우 권한 있는 IAM 보안 주체가 SSO 자격 증명을 사용하는 대신 콘솔을 사용하여 데이터 포털에 페더레이션할 수도 있습니다.

Amazon DataZone의 데이터 포털은 주로 Identity Center 인증 사용자가 데이터에 대한 AWS IAM 액세스를 관리하고 데이터 게시, 검색, 구독 및 분석 작업을 수행하는 데 사용하도록 설계되었습니다.

Amazon DataZone 콘솔의 권한 부여

Amazon DataZone 콘솔 권한 부여 모델은 IAM 권한을 사용합니다. 콘솔은 관리자가 주로 설정에 사용합니다. Amazon은 도메인 관리자 AWS 계정 및 멤버 AWS 계정의 개념을 DataZone 사용하며, 이러한 모든 계정에서 콘솔을 사용하여 AWS 조직 경계를 준수하면서 신뢰 관계를 구축합니다.

Amazon DataZone 포털의 권한 부여

Amazon DataZone 데이터 포털 권한 부여 모델은 관리자와 시청자를 포함하는 ACL 정적 역할 아키타입(프로필)이 있는 계층적 모델입니다. 예를 들어 사용자는 관리자 또는 사용자의 프로필을 가질 수 있습니다. 도메인 수준에서는 도메인 사용자 지정이 데이터 소유자일 수 있습니다. 프로젝트 수준에서 사용자는 소유자 또는 기여자일 수 있습니다. 이러한 프로파일은 사용자와 그룹이라는 두 가지 유형 중 하나로 구성할 수 있습니다. 그런 다음 이러한 프로필은 도메인 및 프로젝트와 연결되고 이러한 권한의 상태는 연결 테이블에 저장됩니다.

이 권한 부여 모델 내에서 Amazon DataZone 은 사용자가 사용자 및 그룹 권한을 관리할 수 있도록 허용합니다. 사용자는 프로젝트 멤버십을 관리하고, 프로젝트에 대한 멤버십을 요청하고, 멤버십을 승인

합니다. 사용자는 데이터를 게시하고, 데이터 구독 승인자를 정의하고, 데이터를 구독하고, 구독을 승인합니다.

사용자는 데이터 포털 클라이언트가 특정 프로젝트 컨텍스트에서 사용자의 유효 프로필을 기반으로 Amazon이 DataZone 생성하는 IAM 세션 자격 증명을 요청할 때 특정 프로젝트에서 데이터 분석을 수행합니다. 이 세션은 사용자의 권한과 특정 프로젝트의 리소스 모두에 적용됩니다. 그런 다음 사용자는 Athena 또는 Redshift로 이동하여 관련 데이터를 쿼리하면 모든 기본 IAM 작업이 완전히 추상화됩니다.

Amazon DataZone 프로필 및 역할

사용자가 인증되면 인증된 컨텍스트가 사용자 프로필 ID에 매핑됩니다. 이 사용자 프로필에는 사용자에게 권한을 부여하는 데 사용되는 여러 개의 서로 다른 연결(프로젝트 소유자, 도메인 관리자 등)이 있을 수 있습니다. 각 연결(예: 프로젝트 소유자, 도메인 관리자 등)에는 컨텍스트를 기반으로 특정 활동에 대한 권한이 있습니다. 예를 들어 도메인 관리자 연결이 있는 사용자는 추가 도메인을 생성하고, 도메인에 다른 도메인 관리자를 할당하고, 도메인 내에 프로젝트 템플릿을 생성할 수 있습니다. 프로젝트 소유자는 프로젝트의 프로젝트 멤버를 추가하거나 제거할 수 있으며, 도메인과 게시 계약을 생성하고, 자산을 도메인에 게시할 수 있습니다.

를 사용하여 Amazon DataZone 리소스에 대한 액세스 제어 IAM

다음 보안 관련 작업을 완료하려면 AWS Identity and Access Management (IAM)가 필요합니다.

- 에서 사용자 및 그룹을 생성합니다 AWS 계정.
- 의 각 사용자에게 고유한 보안 자격 증명을 할당합니다 AWS 계정.
- AWS 리소스로 작업을 수행할 수 있는 각 사용자의 권한을 제어합니다.
- 다른 의 사용자가 AWS 리소스를 공유 AWS 계정 하도록 허용합니다.
- 에 대한 역할을 생성하고 이를 수임할 수 있는 사용자 또는 서비스를 AWS 계정 정의합니다.
- 엔터프라이즈의 기존 자격 증명을 사용하여 AWS 리소스를 사용하여 작업을 수행할 수 있는 권한을 부여합니다.

에 대한 자세한 내용은 다음을 IAM참조하세요.

- AWS Identity and Access Management (IAM)
- 시작하기
- IAM 사용 설명서

다음 섹션에서는 도메인(도메인 포함), 관련 계정, 프로젝트 및 데이터 소스와 같은 Amazon DataZone 및 해당 구성 요소를 설정하는 데 필요한 정책 및 권한을 설명합니다. 자세한 내용은 Amazon DataZone 용어 및 개념 단원을 참조하십시오.

내용

- AWS Amazon용 관리형 정책 DataZone
- IAM Amazon의 역할 DataZone
- 임시 자격 증명
- 보안 주체 권한

AWS Amazon용 관리형 정책 DataZone

AWS 관리형 정책은 에서 생성 및 관리하는 독립 실행형 정책입니다 AWS. AWS 관리형 정책은 사용자, 그룹 및 역할에 권한 할당을 시작할 수 있도록 많은 일반적인 사용 사례에 대한 권한을 제공하도록 설계되었습니다.

AWS 관리형 정책은 모든 AWS 고객이 사용할 수 있으므로 특정 사용 사례에 대해 최소 권한 권한을 부여하지 않을 수 있다는 점에 유의하세요. 사용 사례에 고유한 고객 관리형 정책을 정의하여 권한을 줄이는 것이 좋습니다.

AWS 관리형 정책에 정의된 권한은 변경할 수 없습니다. 가 AWS 관리형 정책에 정의된 권한을 AWS 업데이트하면 정책이 연결된 모든 보안 주체 자격 증명(사용자, 그룹 및 역할)에 영향을 미칩니다. AWS 는 새 AWS 서비스 가 시작되거나 기존 서비스에 새 API 작업을 사용할 수 있게 되면 AWS 관리형 정책을 업데이트할 가능성이 높습니다.

자세한 내용은 IAM 사용 설명서의 AWS 관리형 정책을 참조하세요.

내용

- AWS 관리형 정책: AmazonDataZoneFullAccess
- AWS 관리형 정책: AmazonDataZoneFullUserAccess
- AWS 관리형 정책: AmazonDataZoneCustomEnvironmentDeploymentPolicy
- AWS 관리형 정책: AmazonDataZoneEnvironmentRolePermissionsBoundary
- AWS 관리형 정책: AmazonDataZoneRedshiftGlueProvisioningPolicy
- AWS 관리형 정책: AmazonDataZoneGlueManageAccessRolePolicy
- AWS 관리형 정책: AmazonDataZoneRedshiftManageAccessRolePolicy
- AWS 관리형 정책: AmazonDataZoneCrossAccountAdmin

- AWS 관리형 정책: AmazonDataZoneDomainExecutionRolePolicy
- AWS 관리형 정책: AmazonDataZoneSageMakerProvisioning
- AWS 관리형 정책: AmazonDataZoneSageMakerAccess
- AWS 관리형 정책: AmazonDataZoneSageMakerEnvironmentRolePermissionsBoundary
- AWS 관리형 정책에 대한 Amazon DataZone 업데이트

AWS 관리형 정책: AmazonDataZoneFullAccess

`AmazonDataZoneFullAccess` 정책을 IAM 자격 증명에 연결할 수 있습니다.

이 정책은 를 DataZone 통해 Amazon에 대한 전체 액세스를 제공합니다 AWS Management Console.

권한 세부 정보

이 정책에는 다음 권한이 포함되어 있습니다.

- `datazone` – 보안 주체에게 를 통해 Amazon DataZone에 대한 전체 액세스 권한을 부여합니다 AWS Management Console.
- `kms` - 보안 주체가 별칭을 나열하고 키를 설명할 수 있습니다.
- `s3` - 보안 주체가 Amazon DataZone 데이터를 저장할 기존 S3 버킷을 선택하거나 새 S3 버킷을 생성할 수 있습니다.
- `ram` - 보안 주체가 에서 Amazon DataZone 도메인을 공유할 수 있도록 허용합니다 AWS 계정.
- `iam` - 보안 주체가 역할을 나열 및 전달하고 정책을 가져올 수 있도록 허용합니다.
- `sso` - 보안 주체가 이 활성화된 리전을 가져올 AWS IAM Identity Center 수 있도록 허용합니다.
- `secretsmanager` - 보안 주체가 특정 접두사가 있는 보안 암호를 생성, 태그 지정 및 나열할 수 있습니다.

```
{
    "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_*"
                }
            }
        }
    ]
}
```

정책 고려 사항 및 제한 사항

AmazonDataZoneFullAccess 정책에서 다루지 않는 특정 기능이 있습니다.

- 자체 AWS KMS 키로 Amazon DataZone 도메인을 생성하는 경우 도메인 생성에 성공하려면 에 kms:CreateGrant 대한 권한이 있고, 해당 키가 listDataSources 및 APIs 와 같은 다른 Amazon DataZone을 호출하려면 에 kms:GenerateDataKey kms:Decrypt 대한 권한이 있어야 합니다createDataSource. 또한 해당 키의 리소스 정책에 kms:CreateGrant, kms:GenerateDataKey, 및 kms:Decryptkms:DescribeKey에 대한 권한도 있어야 합니다.

  기본 서비스 소유 KMS 키를 사용하는 경우 필요하지 않습니다.

  자세한 내용은 AWS Key Management Service 단원을 참조하십시오.
- Amazon DataZone 콘솔에서 역할 생성 및 업데이트 기능을 사용하려면 관리자 권한이 있거나 IAM 역할을 생성하고 정책을 생성/업데이트하는 데 필요한 IAM 권

한이 있어야 합니다. 필수 권한에는 `iam:CreateRole`, `iam:CreatePolicy`, `iam:CreatePolicyVersioniam:DeletePolicyVersion`, 및 `iam:AttachRolePolicy` 권한이 포함됩니다.

- AWS IAM Identity Center 사용자 로그인이 활성화된 DataZone 상태에서 Amazon에서 새 도메인을 생성하거나 Amazon 의 기존 도메인에 대해 새 도메인을 활성화 DataZone하는 경우 다음 권한이 있어야 합니다.
  - 조직:DescribeOrganization
  - 조직:ListDelegatedAdministrators
  - sso:CreateInstance
  - sso:ListInstances
  - sso:GetSharedSsoConfiguration
  - sso:PutApplicationGrant
  - sso:PutApplicationAssignmentConfiguration
  - sso:PutApplicationAuthenticationMethod
  - sso:PutApplicationAccessScope
  - sso:CreateApplication
  - sso:DeleteApplication
  - sso:CreateApplicationAssignment
  - sso:DeleteApplicationAssignment
- Amazon 에서 AWS 계정 연결 요청을 수락하려면 `ram:AcceptResourceShareInvitation` 권한이 DataZone있어야 합니다.

AWS 관리형 정책: AmazonDataZoneFullUserAccess

이 정책은 Amazon 에 대한 전체 액세스 권한을 부여 DataZone하지만 도메인, 사용자 또는 관련 계정의 관리를 허용하지 않습니다.

권한 세부 정보

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

```
    "Effect": "Allow",
    "Action": [
     "datazone:AcceptPredictions",
     "datazone:AcceptSubscriptionRequest",
     "datazone:AddEntityOwner",
     "datazone:AddPolicyGrant",
     "datazone:CancelMetadataGenerationRun",
     "datazone:CancelSubscription",
     "datazone:CreateAsset",
     "datazone:CreateAssetFilter",
     "datazone:CreateAssetRevision",
     "datazone:CreateAssetType",
     "datazone:CreateDataProduct",
     "datazone:CreateDataProductRevision",
     "datazone:CreateDataSource",
     "datazone:CreateDomainUnit",
     "datazone:CreateEnvironment",
     "datazone:CreateEnvironmentBlueprint",
     "datazone:CreateEnvironmentProfile",
     "datazone:CreateFormType",
     "datazone:CreateGlossary",
     "datazone:CreateGlossaryTerm",
     "datazone:CreateListingChangeSet",
     "datazone:CreateProject",
     "datazone:CreateProjectMembership",
     "datazone:CreateSubscriptionGrant",
     "datazone:CreateSubscriptionRequest",
     "datazone:DeleteAsset",
     "datazone:DeleteAssetFilter",
     "datazone:DeleteAssetType",
     "datazone:DeleteDataProduct",
     "datazone:DeleteDataSource",
     "datazone:DeleteDomainUnit",
     "datazone:DeleteEnvironment",
     "datazone:DeleteEnvironmentBlueprint",
     "datazone:DeleteEnvironmentProfile",
     "datazone:DeleteFormType",
     "datazone:DeleteGlossary",
     "datazone:DeleteGlossaryTerm",
     "datazone:DeleteListing",
     "datazone:DeleteProject",
     "datazone:DeleteProjectMembership",
     "datazone:DeleteSubscriptionGrant",
     "datazone:DeleteSubscriptionRequest",
```

```
    "datazone:DeleteSubscriptionTarget",
    "datazone:DeleteTimeSeriesDataPoints",
    "datazone:GetAsset",
    "datazone:GetAssetFilter",
    "datazone:GetAssetType",
    "datazone:GetDataProduct",
    "datazone:GetDataSource",
    "datazone:GetDataSourceRun",
    "datazone:GetDomain",
    "datazone:GetDomainUnit",
    "datazone:GetEnvironment",
    "datazone:GetEnvironmentActionLink",
    "datazone:GetEnvironmentBlueprint",
    "datazone:GetEnvironmentCredentials",
    "datazone:GetEnvironmentProfile",
    "datazone:GetFormType",
    "datazone:GetGlossary",
    "datazone:GetGlossaryTerm",
    "datazone:GetGroupProfile",
    "datazone:GetIamPortalLoginUrl",
    "datazone:GetLineageNode",
    "datazone:GetListing",
    "datazone:GetMetadataGenerationRun",
    "datazone:GetProject",
    "datazone:GetSubscription",
    "datazone:GetSubscriptionEligibility",
    "datazone:GetSubscriptionGrant",
    "datazone:GetSubscriptionRequestDetails",
    "datazone:GetSubscriptionTarget",
    "datazone:GetTimeSeriesDataPoint",
    "datazone:GetUserProfile",
    "datazone:ListAccountEnvironments",
    "datazone:ListAssetFilters",
    "datazone:ListAssetRevisions",
    "datazone:ListDataProductRevisions",
    "datazone:ListDataSourceRunActivities",
    "datazone:ListDataSourceRuns",
    "datazone:ListDataSources",
    "datazone:ListDomainUnitsForParent",
    "datazone:ListEntityOwners",
    "datazone:ListEnvironmentBlueprintConfigurations",
    "datazone:ListEnvironmentBlueprints",
    "datazone:ListEnvironmentProfiles",
    "datazone:ListEnvironments",
```

```
    "datazone:ListGroupsForUser",
    "datazone:ListLineageNodeHistory",
    "datazone:ListMetadataGenerationRuns",
    "datazone:ListNotifications",
    "datazone:ListPolicyGrants",
    "datazone:ListProjectMemberships",
    "datazone:ListProjects",
    "datazone:ListSubscriptionGrants",
    "datazone:ListSubscriptionRequests",
    "datazone:ListSubscriptionTargets",
    "datazone:ListSubscriptions",
    "datazone:ListTimeSeriesDataPoints",
    "datazone:ListWarehouseMetadata",
    "datazone:PostTimeSeriesDataPoints",
    "datazone:RejectPredictions",
    "datazone:RejectSubscriptionRequest",
    "datazone:RemoveEntityOwner",
    "datazone:RemovePolicyGrant",
    "datazone:RevokeSubscription",
    "datazone:Search",
    "datazone:SearchGroupProfiles",
    "datazone:SearchListings",
    "datazone:SearchTypes",
    "datazone:SearchUserProfiles",
    "datazone:StartDataSourceRun",
    "datazone:StartMetadataGenerationRun",
    "datazone:UpdateAssetFilter",
    "datazone:UpdateDataSource",
    "datazone:UpdateDomainUnit",
    "datazone:UpdateEnvironment",
    "datazone:UpdateEnvironmentBlueprint",
    "datazone:UpdateEnvironmentDeploymentStatus",
    "datazone:UpdateEnvironmentProfile",
    "datazone:UpdateGlossary",
    "datazone:UpdateGlossaryTerm",
    "datazone:UpdateProject",
    "datazone:UpdateSubscriptionGrantStatus",
    "datazone:UpdateSubscriptionRequest"
   ],
   "Resource": "*"
  },
  {
   "Sid": "RAMResourceShareOperations",
   "Effect": "Allow",
```

```
    "Action": "ram:GetResourceShareAssociations",
    "Resource": "*"
   }
  ]
}
```

AWS 관리형 정책: AmazonDataZoneCustomEnvironmentDeploymentPolicy

이 정책을 사용하여 사용자 지정 청사진을 사용하여 생성된 환경의 구성을 업데이트할 수 있습니다. 이 정책은 Amazon DataZone 구독 대상 및 데이터 소스를 생성하는 데도 사용할 수 있습니다.

권한 세부 정보

```
{
 "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 관리형 정책: AmazonDataZoneEnvironmentRolePermissionsBoundary

> **Note**
>
> 이 정책은 권한 경계입니다. 권한 경계는 자격 증명 기반 정책이 IAM엔터티에 부여할 수 있는 최대 권한을 설정합니다. Amazon DataZone 권한 경계 정책을 단독으로 사용하고 연결해서는 안 됩니다. Amazon DataZone 권한 경계 정책은 Amazon DataZone 관리형 역할에만 연결해야 합니다. 권한 경계에 대한 자세한 내용은 IAM 사용 설명서의 IAM엔터티에 대한 권한 경계를 참조하세요.

Amazon DataZone 데이터 포털을 통해 환경을 생성할 때 AmazonIAM은 환경 생성 중에 생성되는 역할에 이 권한 경계를 DataZone 적용합니다. 권한 경계는 Amazon이 DataZone 생성하는 역할의 범위와 추가하는 모든 역할을 제한합니다.

Amazon은 `AmazonDataZoneEnvironmentRolePermissionsBoundary` 관리형 정책을 DataZone 사용하여 연결된 프로비저닝된 IAM 보안 주체를 제한합니다. 보안 주체는 대화형 엔터프라이즈 사용자 또는 분석 서비스(예:)를 대신하여 Amazon이 수임할 수 있는 사용자 역할의 형태를 취한 다음 Amazon S3에서 읽고 쓰거나 를 실행하는 등의 데이터를 처리하는 작업을 수행할 수 있습니다 AWS Glue 크롤러. DataZone AWS Glue

이 `AmazonDataZoneEnvironmentRolePermissionsBoundary` 정책은 AWS Glue, Amazon S3, Amazon Redshift 및 AWS Lake Formation Amazon Athena와 같은 DataZone 서비스에 대한 Amazon의 읽기 및 쓰기 액세스 권한을 부여합니다. Amazon Athena 또한 이 정책은 네트워크 인터페이스 및 AWS KMS 키와 같이 이러한 서비스를 사용하는 데 필요한 일부 인프라 리소스에 읽기 및 쓰기 권한을 부여합니다.

Amazon은 `AmazonDataZoneEnvironmentRolePermissionsBoundary` AWS 관리형 정책을 모든 Amazon DataZone 환경 역할(소유자 및 기여자)에 대한 권한 경계로 DataZone 적용합니다. 이 권한 경계는 환경에 필요한 필수 리소스 및 작업에 대한 액세스만 허용하도록 이러한 역할을 제한합니다.

경계에는 다음 JSON 문이 포함됩니다.

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

```
      "Action": [
        "ec2:CreateTags",
        "ec2:DeleteTags"
      ],
      "Resource": [
        "arn:aws:ec2:*:*:network-interface/*"
      ],
      "Condition": {
        "ForAllValues:StringEquals": {
          "aws:TagKeys": [
            "aws-glue-service-resource"
          ]
        }
      }
    },
    {
      "Sid": "GlueOperations",
      "Effect": "Allow",
      "Action": [
        "glue:*DataQuality*",
        "glue:BatchCreatePartition",
        "glue:BatchDeleteConnection",
        "glue:BatchDeletePartition",
        "glue:BatchDeleteTable",
        "glue:BatchDeleteTableVersion",
        "glue:BatchGetJobs",
        "glue:BatchGetWorkflows",
        "glue:BatchStopJobRun",
        "glue:BatchUpdatePartition",
        "glue:CreateBlueprint",
        "glue:CreateConnection",
        "glue:CreateCrawler",
        "glue:CreateDatabase",
        "glue:CreateJob",
        "glue:CreatePartition",
        "glue:CreatePartitionIndex",
        "glue:CreateTable",
        "glue:CreateWorkflow",
        "glue:DeleteBlueprint",
        "glue:DeleteColumnStatisticsForPartition",
        "glue:DeleteColumnStatisticsForTable",
        "glue:DeleteConnection",
        "glue:DeleteCrawler",
        "glue:DeleteJob",
```

```
        "glue:DeletePartition",
        "glue:DeletePartitionIndex",
        "glue:DeleteTable",
        "glue:DeleteTableVersion",
        "glue:DeleteWorkflow",
        "glue:GetColumnStatisticsForPartition",
        "glue:GetColumnStatisticsForTable",
        "glue:GetConnection",
        "glue:GetDatabase",
        "glue:GetDatabases",
        "glue:GetTable",
        "glue:GetTables",
        "glue:GetPartition",
        "glue:GetPartitions",
        "glue:ListSchemas",
        "glue:ListJobs",
        "glue:NotifyEvent",
        "glue:PutWorkflowRunProperties",
        "glue:ResetJobBookmark",
        "glue:ResumeWorkflowRun",
        "glue:SearchTables",
        "glue:StartBlueprintRun",
        "glue:StartCrawler",
        "glue:StartCrawlerSchedule",
        "glue:StartJobRun",
        "glue:StartWorkflowRun",
        "glue:StopCrawler",
        "glue:StopCrawlerSchedule",
        "glue:StopWorkflowRun",
        "glue:UpdateBlueprint",
        "glue:UpdateColumnStatisticsForPartition",
        "glue:UpdateColumnStatisticsForTable",
        "glue:UpdateConnection",
        "glue:UpdateCrawler",
        "glue:UpdateCrawlerSchedule",
        "glue:UpdateDatabase",
        "glue:UpdateJob",
        "glue:UpdatePartition",
        "glue:UpdateTable",
        "glue:UpdateWorkflow"
      ],
      "Resource": "*",
      "Condition": {
        "Null": {
```

```
          "aws:ResourceTag/AmazonDataZoneEnvironment": "false"
        }
      }
    },
    {
      "Sid": "PassRole",
      "Effect": "Allow",
      "Action": [
        "iam:PassRole"
      ],
      "Resource": [
        "arn:aws:iam::*:role/datazone*"
      ],
      "Condition": {
        "StringEquals": {
          "iam:PassedToService": "glue.amazonaws.com"
        }
      }
    },
    {
      "Sid": "SameAccountKmsOperations",
      "Effect": "Allow",
      "Action": [
        "kms:DescribeKey",
        "kms:Decrypt",
        "kms:ListKeys"
      ],
      "Resource": "*",
      "Condition": {
        "StringNotEquals": {
          "aws:ResourceAccount": "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid": "KmsOperationsWithResourceTag",
      "Effect": "Allow",
      "Action": [
        "kms:DescribeKey",
        "kms:Decrypt",
        "kms:ListKeys",
        "kms:Encrypt",
        "kms:GenerateDataKey",
        "kms:Verify",
```

```
        "kms:Sign"
      ],
      "Resource": "*",
      "Condition": {
        "Null": {
          "aws:ResourceTag/AmazonDataZoneEnvironment": "false"
        }
      }
    },
    {
      "Sid": "AnalyticsOperations",
      "Effect": "Allow",
      "Action": [
        "datazone:*",
        "sqlworkbench:*"
      ],
      "Resource": "*"
    },
    {
      "Sid": "QueryOperations",
      "Effect": "Allow",
      "Action": [
        "athena:BatchGetNamedQuery",
        "athena:BatchGetPreparedStatement",
        "athena:BatchGetQueryExecution",
        "athena:CreateNamedQuery",
        "athena:CreateNotebook",
        "athena:CreatePreparedStatement",
        "athena:CreatePresignedNotebookUrl",
        "athena:DeleteNamedQuery",
        "athena:DeleteNotebook",
        "athena:DeletePreparedStatement",
        "athena:ExportNotebook",
        "athena:GetDatabase",
        "athena:GetDataCatalog",
        "athena:GetNamedQuery",
        "athena:GetPreparedStatement",
        "athena:GetQueryExecution",
        "athena:GetQueryResults",
        "athena:GetQueryRuntimeStatistics",
        "athena:GetTableMetadata",
        "athena:GetWorkGroup",
        "athena:ImportNotebook",
        "athena:ListDatabases",
```

```
        "athena:ListDataCatalogs",
        "athena:ListEngineVersions",
        "athena:ListNamedQueries",
        "athena:ListPreparedStatements",
        "athena:ListQueryExecutions",
        "athena:ListTableMetadata",
        "athena:ListTagsForResource",
        "athena:ListWorkGroups",
        "athena:StartCalculationExecution",
        "athena:StartQueryExecution",
        "athena:StartSession",
        "athena:StopCalculationExecution",
        "athena:StopQueryExecution",
        "athena:TerminateSession",
        "athena:UpdateNamedQuery",
        "athena:UpdateNotebook",
        "athena:UpdateNotebookMetadata",
        "athena:UpdatePreparedStatement",
        "ec2:CreateNetworkInterface",
        "ec2:DeleteNetworkInterface",
        "ec2:Describe*",
        "glue:BatchCreatePartition",
        "glue:BatchDeletePartition",
        "glue:BatchDeleteTable",
        "glue:BatchDeleteTableVersion",
        "glue:BatchGetJobs",
        "glue:BatchGetPartition",
        "glue:BatchGetWorkflows",
        "glue:BatchUpdatePartition",
        "glue:CreateBlueprint",
        "glue:CreateConnection",
        "glue:CreateCrawler",
        "glue:CreateDatabase",
        "glue:CreateJob",
        "glue:CreatePartition",
        "glue:CreatePartitionIndex",
        "glue:CreateTable",
        "glue:CreateWorkflow",
        "glue:DeleteColumnStatisticsForPartition",
        "glue:DeleteColumnStatisticsForTable",
        "glue:DeletePartition",
        "glue:DeletePartitionIndex",
        "glue:DeleteTable",
        "glue:DeleteTableVersion",
```

```
        "glue:GetColumnStatisticsForPartition",
        "glue:GetColumnStatisticsForTable",
        "glue:GetConnection",
        "glue:GetDatabase",
        "glue:GetDatabases",
        "glue:GetTable",
        "glue:GetTables",
        "glue:GetPartition",
        "glue:GetPartitions",
        "glue:ListSchemas",
        "glue:ListJobs",
        "glue:NotifyEvent",
        "glue:SearchTables",
        "glue:UpdateColumnStatisticsForPartition",
        "glue:UpdateColumnStatisticsForTable",
        "glue:UpdateDatabase",
        "glue:UpdatePartition",
        "glue:UpdateTable",
        "iam:GetRole",
        "iam:GetRolePolicy",
        "iam:ListGroups",
        "iam:ListRolePolicies",
        "iam:ListRoles",
        "iam:ListUsers",
        "logs:DescribeLogGroups",
        "logs:DescribeLogStreams",
        "logs:DescribeMetricFilters",
        "logs:DescribeQueries",
        "logs:DescribeQueryDefinitions",
        "logs:DescribeMetricFilters",
        "logs:StartQuery",
        "logs:StopQuery",
        "logs:GetLogEvents",
        "logs:GetLogGroupFields",
        "logs:GetQueryResults",
        "logs:GetLogRecord",
        "logs:PutLogEvents",
        "logs:CreateLogStream",
        "logs:FilterLogEvents",
        "lakeformation:GetDataAccess",
        "lakeformation:GetDataLakeSettings",
        "lakeformation:GetResourceLFTags",
        "lakeformation:ListPermissions",
        "redshift-data:ListTables",
```

```
        "redshift-data:DescribeTable",
        "redshift-data:ListSchemas",
        "redshift-data:ListDatabases",
        "redshift-data:ExecuteStatement",
        "redshift-data:GetStatementResult",
        "redshift-data:DescribeStatement",
        "redshift:CreateClusterUser",
        "redshift:DescribeClusters",
        "redshift:DescribeDataShares",
        "redshift:GetClusterCredentials",
        "redshift:GetClusterCredentialsWithIAM",
        "redshift:JoinGroup",
        "redshift-serverless:ListNamespaces",
        "redshift-serverless:ListWorkgroups",
        "redshift-serverless:GetNamespace",
        "redshift-serverless:GetWorkgroup",
        "redshift-serverless:GetCredentials",
        "secretsmanager:ListSecrets",
        "tag:GetResources"
      ],
      "Resource": "*"
    },
    {
      "Sid": "QueryOperationsWithResourceTag",
      "Effect": "Allow",
      "Action": [
        "athena:GetQueryResultsStream"
      ],
      "Resource": "*",
      "Condition": {
        "Null": {
          "aws:ResourceTag/AmazonDataZoneEnvironment": "false"
        }
      }
    },
    {
      "Sid": "SecretsManagerOperationsWithTagKeys",
      "Effect": "Allow",
      "Action": [
        "secretsmanager:CreateSecret",
        "secretsmanager:TagResource"
      ],
      "Resource": "arn:aws:secretsmanager:*:*:secret:AmazonDataZone-*",
      "Condition": {
```

```
        "StringLike": {
          "aws:ResourceTag/AmazonDataZoneDomain": "*",
          "aws:ResourceTag/AmazonDataZoneProject": "*"
        },
        "Null": {
          "aws:TagKeys": "false"
        },
        "ForAllValues:StringEquals": {
          "aws:TagKeys": [
            "AmazonDataZoneDomain",
            "AmazonDataZoneProject"
          ]
        }
      }
    },
    {
      "Sid": "DataZoneS3Buckets",
      "Effect": "Allow",
      "Action": [
        "s3:AbortMultipartUpload",
        "s3:DeleteObject",
        "s3:DeleteObjectVersion",
        "s3:GetObject",
        "s3:PutObject",
        "s3:PutObjectRetention",
        "s3:ReplicateObject",
        "s3:RestoreObject"
      ],
      "Resource": [
        "arn:aws:s3:::*/datazone/*"
      ]
    },
    {
      "Sid": "DataZoneS3BucketLocation",
      "Effect": "Allow",
      "Action": [
        "s3:GetBucketLocation"
      ],
      "Resource": "*"
    },
    {
      "Sid": "ListDataZoneS3Bucket",
      "Effect": "Allow",
      "Action": [
```

```
        "s3:ListBucket"
      ],
      "Resource": [
        "*"
      ],
      "Condition": {
        "StringLike": {
          "s3:prefix": [
            "*/datazone/*",
            "datazone/*"
          ]
        }
      }
    },
    {
      "Sid": "NotDeniedOperations",
      "Effect": "Deny",
      "NotAction": [
        "datazone:*",
        "sqlworkbench:*",
        "athena:BatchGetNamedQuery",
        "athena:BatchGetPreparedStatement",
        "athena:BatchGetQueryExecution",
        "athena:CreateNamedQuery",
        "athena:CreateNotebook",
        "athena:CreatePreparedStatement",
        "athena:CreatePresignedNotebookUrl",
        "athena:DeleteNamedQuery",
        "athena:DeleteNotebook",
        "athena:DeletePreparedStatement",
        "athena:ExportNotebook",
        "athena:GetDatabase",
        "athena:GetDataCatalog",
        "athena:GetNamedQuery",
        "athena:GetPreparedStatement",
        "athena:GetQueryExecution",
        "athena:GetQueryResults",
        "athena:GetQueryResultsStream",
        "athena:GetQueryRuntimeStatistics",
        "athena:GetTableMetadata",
        "athena:GetWorkGroup",
        "athena:ImportNotebook",
        "athena:ListDatabases",
        "athena:ListDataCatalogs",
```

```
        "athena:ListEngineVersions",
        "athena:ListNamedQueries",
        "athena:ListPreparedStatements",
        "athena:ListQueryExecutions",
        "athena:ListTableMetadata",
        "athena:ListTagsForResource",
        "athena:ListWorkGroups",
        "athena:StartCalculationExecution",
        "athena:StartQueryExecution",
        "athena:StartSession",
        "athena:StopCalculationExecution",
        "athena:StopQueryExecution",
        "athena:TerminateSession",
        "athena:UpdateNamedQuery",
        "athena:UpdateNotebook",
        "athena:UpdateNotebookMetadata",
        "athena:UpdatePreparedStatement",
        "ec2:CreateNetworkInterface",
        "ec2:CreateTags",
        "ec2:DeleteNetworkInterface",
        "ec2:DeleteTags",
        "ec2:Describe*",
        "glue:*DataQuality*",
        "glue:BatchCreatePartition",
        "glue:BatchDeleteConnection",
        "glue:BatchDeletePartition",
        "glue:BatchDeleteTable",
        "glue:BatchDeleteTableVersion",
        "glue:BatchGetJobs",
        "glue:BatchGetPartition",
        "glue:BatchGetWorkflows",
        "glue:BatchStopJobRun",
        "glue:BatchUpdatePartition",
        "glue:CreateBlueprint",
        "glue:CreateConnection",
        "glue:CreateCrawler",
        "glue:CreateDatabase",
        "glue:CreateJob",
        "glue:CreatePartition",
        "glue:CreatePartitionIndex",
        "glue:CreateTable",
        "glue:CreateWorkflow",
        "glue:DeleteBlueprint",
        "glue:DeleteColumnStatisticsForPartition",
```

```
        "glue:DeleteColumnStatisticsForTable",
        "glue:DeleteConnection",
        "glue:DeleteCrawler",
        "glue:DeleteJob",
        "glue:DeletePartition",
        "glue:DeletePartitionIndex",
        "glue:DeleteTable",
        "glue:DeleteTableVersion",
        "glue:DeleteWorkflow",
        "glue:GetColumnStatisticsForPartition",
        "glue:GetColumnStatisticsForTable",
        "glue:GetConnection",
        "glue:GetDatabase",
        "glue:GetDatabases",
        "glue:GetTable",
        "glue:GetTables",
        "glue:GetPartition",
        "glue:GetPartitions",
        "glue:ListSchemas",
        "glue:ListJobs",
        "glue:NotifyEvent",
        "glue:PutWorkflowRunProperties",
        "glue:ResetJobBookmark",
        "glue:ResumeWorkflowRun",
        "glue:SearchTables",
        "glue:StartBlueprintRun",
        "glue:StartCrawler",
        "glue:StartCrawlerSchedule",
        "glue:StartJobRun",
        "glue:StartWorkflowRun",
        "glue:StopCrawler",
        "glue:StopCrawlerSchedule",
        "glue:StopWorkflowRun",
        "glue:UpdateBlueprint",
        "glue:UpdateColumnStatisticsForPartition",
        "glue:UpdateColumnStatisticsForTable",
        "glue:UpdateConnection",
        "glue:UpdateCrawler",
        "glue:UpdateCrawlerSchedule",
        "glue:UpdateDatabase",
        "glue:UpdateJob",
        "glue:UpdatePartition",
        "glue:UpdateTable",
        "glue:UpdateWorkflow",
```

```
        "iam:GetRole",
        "iam:GetRolePolicy",
        "iam:List*",
        "iam:PassRole",
        "kms:DescribeKey",
        "kms:Decrypt",
        "kms:Encrypt",
        "kms:GenerateDataKey",
        "kms:ListKeys",
        "kms:Verify",
        "kms:Sign",
        "logs:DescribeLogGroups",
        "logs:DescribeLogStreams",
        "logs:DescribeMetricFilters",
        "logs:DescribeQueries",
        "logs:DescribeQueryDefinitions",
        "logs:StartQuery",
        "logs:StopQuery",
        "logs:GetLogEvents",
        "logs:GetLogGroupFields",
        "logs:GetQueryResults",
        "logs:GetLogRecord",
        "logs:PutLogEvents",
        "logs:CreateLogStream",
        "logs:FilterLogEvents",
        "lakeformation:GetDataAccess",
        "lakeformation:GetDataLakeSettings",
        "lakeformation:GetResourceLFTags",
        "lakeformation:ListPermissions",
        "redshift-data:ListTables",
        "redshift-data:DescribeTable",
        "redshift-data:ListSchemas",
        "redshift-data:ListDatabases",
        "redshift-data:ExecuteStatement",
        "redshift-data:GetStatementResult",
        "redshift-data:DescribeStatement",
        "redshift:CreateClusterUser",
        "redshift:DescribeClusters",
        "redshift:DescribeDataShares",
        "redshift:GetClusterCredentials",
        "redshift:GetClusterCredentialsWithIAM",
        "redshift:JoinGroup",
        "redshift-serverless:ListNamespaces",
        "redshift-serverless:ListWorkgroups",
```

```
        "redshift-serverless:GetNamespace",
        "redshift-serverless:GetWorkgroup",
        "redshift-serverless:GetCredentials",
        "s3:AbortMultipartUpload",
        "s3:DeleteObject",
        "s3:DeleteObjectVersion",
        "s3:GetObject",
        "s3:GetBucketLocation",
        "s3:ListBucket",
        "s3:PutObject",
        "s3:PutObjectRetention",
        "s3:ReplicateObject",
        "s3:RestoreObject",
        "secretsmanager:CreateSecret",
        "secretsmanager:ListSecrets",
        "secretsmanager:TagResource",
        "tag:GetResources"
      ],
      "Resource": [
        "*"
      ]
    }
  ]
}
```

AWS 관리형 정책: AmazonDataZoneRedshiftGlueProvisioningPolicy

는 AmazonDataZoneRedshiftGlueProvisioningPolicy 정책은 AWS Glue 및 Amazon Redshift와 상호 운용하는 데 필요한 DataZone 권한을 Amazon에 부여합니다.

```
{
 "Version": "2012-10-17",
 "Statement": [
  {
   "Sid": "AmazonDataZonePermissionsToCreateEnvironmentRole",
   "Effect": "Allow",
   "Action": [
    "iam:CreateRole",
    "iam:DetachRolePolicy",
```

```
    "iam:DeleteRolePolicy",
    "iam:AttachRolePolicy",
    "iam:PutRolePolicy"
   ],
   "Resource": "arn:aws:iam::*:role/datazone*",
   "Condition": {
    "StringEquals": {
     "iam:PermissionsBoundary": "arn:aws:iam::aws:policy/
AmazonDataZoneEnvironmentRolePermissionsBoundary",
     "aws:CalledViaFirst": [
      "cloudformation.amazonaws.com"
     ]
    }
   }
  },
  {
   "Sid": "IamPassRolePermissions",
   "Effect": "Allow",
   "Action": [
    "iam:PassRole"
   ],
   "Resource": [
    "arn:aws:iam::*:role/datazone*"
   ],
   "Condition": {
    "StringEquals": {
     "iam:PassedToService": [
      "glue.amazonaws.com",
      "lakeformation.amazonaws.com"
     ],
     "aws:CalledViaFirst": [
      "cloudformation.amazonaws.com"
     ]
    }
   }
  },
  {
   "Sid": "AmazonDataZonePermissionsToManageCreatedEnvironmentRole",
   "Effect": "Allow",
   "Action": [
    "iam:DeleteRole",
    "iam:GetRole"
   ],
   "Resource": "arn:aws:iam::*:role/datazone*",
```

```
    "Condition": {
     "StringEquals": {
      "aws:CalledViaFirst": [
       "cloudformation.amazonaws.com"
      ]
     }
    }
   },
   {
    "Sid": "AmazonDataZoneCFStackCreationForEnvironments",
    "Effect": "Allow",
    "Action": [
     "cloudformation:CreateStack",
     "cloudformation:TagResource"
    ],
    "Resource": [
     "arn:aws:cloudformation:*:*:stack/DataZone*"
    ],
    "Condition": {
     "ForAnyValue:StringLike": {
      "aws:TagKeys": "AmazonDataZoneEnvironment"
     },
     "Null": {
      "aws:ResourceTag/AmazonDataZoneEnvironment": "false"
     }
    }
   },
   {
    "Sid": "AmazonDataZoneCFStackManagementForEnvironments",
    "Effect": "Allow",
    "Action": [
     "cloudformation:DeleteStack",
     "cloudformation:DescribeStacks",
     "cloudformation:DescribeStackEvents"
    ],
    "Resource": [
     "arn:aws:cloudformation:*:*:stack/DataZone*"
    ]
   },
   {
    "Sid": "AmazonDataZoneEnvironmentParameterValidation",
    "Effect": "Allow",
    "Action": [
     "lakeformation:GetDataLakeSettings",
```

```
    "lakeformation:PutDataLakeSettings",
    "lakeformation:RevokePermissions",
    "lakeformation:ListPermissions",
    "glue:CreateDatabase",
    "glue:GetDatabase",
    "athena:GetWorkGroup",
    "logs:DescribeLogGroups",
    "redshift-serverless:GetNamespace",
    "redshift-serverless:GetWorkgroup",
    "redshift:DescribeClusters",
    "secretsmanager:ListSecrets"
   ],
   "Resource": "*"
  },
  {
   "Sid": "AmazonDataZoneEnvironmentLakeFormationPermissions",
   "Effect": "Allow",
   "Action": [
    "lakeformation:RegisterResource",
    "lakeformation:DeregisterResource",
    "lakeformation:GrantPermissions",
    "lakeformation:ListResources"
   ],
   "Resource": "*",
   "Condition": {
    "StringEquals": {
     "aws:CalledViaFirst": [
      "cloudformation.amazonaws.com"
     ]
    }
   }
  },
  {
   "Sid": "AmazonDataZoneEnvironmentGlueDeletePermissions",
   "Effect": "Allow",
   "Action": [
    "glue:DeleteDatabase"
   ],
   "Resource": "*",
   "Condition": {
    "StringEquals": {
     "aws:CalledViaFirst": [
      "cloudformation.amazonaws.com"
     ]
```

```
    }
   }
  },
  {
   "Sid": "AmazonDataZoneEnvironmentAthenaDeletePermissions",
   "Effect": "Allow",
   "Action": [
    "athena:DeleteWorkGroup"
   ],
   "Resource": "*",
   "Condition": {
    "StringEquals": {
     "aws:CalledViaFirst": [
      "cloudformation.amazonaws.com"
     ]
    }
   }
  },
  {
   "Sid": "AmazonDataZoneEnvironmentAthenaResourceCreation",
   "Effect": "Allow",
   "Action": [
    "athena:CreateWorkGroup",
    "athena:TagResource",
    "iam:TagRole",
    "iam:TagPolicy",
    "logs:TagLogGroup"
   ],
   "Resource": "*",
   "Condition": {
    "ForAnyValue:StringLike": {
     "aws:TagKeys": "AmazonDataZoneEnvironment"
    },
    "Null": {
     "aws:ResourceTag/AmazonDataZoneEnvironment": "false"
    },
    "StringEquals": {
     "aws:CalledViaFirst": [
      "cloudformation.amazonaws.com"
     ]
    }
   }
  },
  {
```

```
    "Sid": "AmazonDataZoneEnvironmentLogGroupCreation",
    "Effect": "Allow",
    "Action": [
     "logs:CreateLogGroup",
     "logs:DeleteLogGroup"
    ],
    "Resource": "arn:aws:logs:*:*:log-group:datazone-*",
    "Condition": {
     "ForAnyValue:StringLike": {
      "aws:TagKeys": "AmazonDataZoneEnvironment"
     },
     "Null": {
      "aws:ResourceTag/AmazonDataZoneEnvironment": "false"
     },
     "StringEquals": {
      "aws:CalledViaFirst": [
       "cloudformation.amazonaws.com"
      ]
     }
    }
   },
   {
    "Sid": "AmazonDataZoneEnvironmentLogGroupManagement",
    "Action": [
     "logs:PutRetentionPolicy"
    ],
    "Resource": "arn:aws:logs:*:*:log-group:datazone-*",
    "Effect": "Allow",
    "Condition": {
     "StringEquals": {
      "aws:CalledViaFirst": [
       "cloudformation.amazonaws.com"
      ]
     }
    }
   },
   {
    "Sid": "AmazonDataZoneEnvironmentIAMPolicyManagement",
    "Effect": "Allow",
    "Action": [
     "iam:DeletePolicy",
     "iam:CreatePolicy",
     "iam:GetPolicy",
     "iam:ListPolicyVersions"
```

```
    ],
    "Resource": [
     "arn:aws:iam::*:policy/datazone*"
    ],
    "Condition": {
     "StringEquals": {
      "aws:CalledViaFirst": [
       "cloudformation.amazonaws.com"
      ]
     }
    }
   },
   {
    "Sid": "AmazonDataZoneEnvironmentS3ValidationPermissions",
    "Effect": "Allow",
    "Action": [
     "s3:ListAllMyBuckets",
     "s3:ListBucket"
    ],
    "Resource": "arn:aws:s3:::*"
   },
   {
    "Sid": "AmazonDataZoneEnvironmentKMSDecryptPermissions",
    "Effect": "Allow",
    "Action": [
     "kms:GenerateDataKey",
     "kms:Decrypt"
    ],
    "Resource": "*",
    "Condition": {
     "Null": {
      "aws:ResourceTag/AmazonDataZoneEnvironment": "false"
     }
    }
   },
   {
    "Sid": "PermissionsToTagAmazonDataZoneEnvironmentGlueResources",
    "Effect": "Allow",
    "Action": [
     "glue:TagResource"
    ],
    "Resource": "*",
    "Condition": {
     "ForAnyValue:StringLike": {
```

```
      "aws:TagKeys": "AmazonDataZoneEnvironment"
     },
     "Null": {
      "aws:RequestTag/AmazonDataZoneEnvironment": "false"
     }
    }
   },
   {
    "Sid": "PermissionsToGetAmazonDataZoneEnvironmentBlueprintTemplates",
    "Effect": "Allow",
    "Action": "s3:GetObject",
    "Resource": "*",
    "Condition": {
     "StringNotEquals": {
      "aws:ResourceAccount": "${aws:PrincipalAccount}"
     },
     "StringEquals": {
      "aws:CalledViaFirst": [
       "cloudformation.amazonaws.com"
      ]
     }
    }
   },
   {
    "Sid": "RedshiftDataPermissions",
    "Effect": "Allow",
    "Action": [
     "redshift-data:ListSchemas",
     "redshift-data:ExecuteStatement"
    ],
    "Resource": [
     "arn:aws:redshift-serverless:*:*:workgroup/*",
     "arn:aws:redshift:*:*:cluster:*"
    ]
   },
   {
    "Sid": "DescribeStatementPermissions",
    "Effect": "Allow",
    "Action": [
     "redshift-data:DescribeStatement"
    ],
    "Resource": "*"
   },
   {
```

```
    "Sid": "GetSecretValuePermissions",
    "Effect": "Allow",
    "Action": [
     "secretsmanager:GetSecretValue"
    ],
    "Resource": "*",
    "Condition": {
     "StringLike": {
      "secretsmanager:ResourceTag/AmazonDataZoneDomain": "dzd*"
     }
    }
   }
  ]
}
```

AWS 관리형 정책: AmazonDataZoneGlueManageAccessRolePolicy

이 정책은 Amazon에 카탈로그에 AWS Glue 데이터를 게시할 수 있는 DataZone 권한을 부여합니다. 또한 Amazon에 카탈로그에 게시된 AWS Glue 자산에 대한 액세스 권한을 부여하거나 취소할 수 있는 DataZone 권한을 부여합니다.

```
{
 "Version": "2012-10-17",
 "Statement": [
  {
   "Sid": "GlueTagDatabasePermissions",
   "Effect": "Allow",
   "Action": [
    "glue:TagResource",
    "glue:UntagResource",
    "glue:GetTags"
   ],
   "Resource": "*",
   "Condition": {
    "StringEquals": {
     "aws:ResourceAccount": "${aws:PrincipalAccount}"
    },
    "ForAnyValue:StringLikeIfExists": {
     "aws:TagKeys": "DataZoneDiscoverable_*"
```

```
    }
   }
  },
  {
   "Sid": "GlueDataQualityPermissions",
   "Effect": "Allow",
   "Action": [
    "glue:ListDataQualityResults",
    "glue:GetDataQualityResult"
   ],
   "Resource": "arn:aws:glue:*:*:dataQualityRuleset/*",
   "Condition": {
    "StringEquals": {
     "aws:ResourceAccount": "${aws:PrincipalAccount}"
    }
   }
  },
  {
   "Sid": "GlueTableDatabasePermissions",
   "Effect": "Allow",
   "Action": [
    "glue:CreateTable",
    "glue:DeleteTable",
    "glue:GetDatabases",
    "glue:GetTables"
   ],
   "Resource": [
    "arn:aws:glue:*:*:catalog",
    "arn:aws:glue:*:*:database/*",
    "arn:aws:glue:*:*:table/*"
   ],
   "Condition": {
    "StringEquals": {
     "aws:ResourceAccount": "${aws:PrincipalAccount}"
    }
   }
  },
  {
   "Sid": "LakeformationResourceSharingPermissions",
   "Effect": "Allow",
   "Action": [
    "lakeformation:BatchGrantPermissions",
    "lakeformation:BatchRevokePermissions",
    "lakeformation:CreateDataCellsFilter",
```

```
    "lakeformation:CreateLakeFormationOptIn",
    "lakeformation:DeleteDataCellsFilter",
    "lakeformation:DeleteLakeFormationOptIn",
    "lakeformation:GrantPermissions",
    "lakeformation:GetDataCellsFilter",
    "lakeformation:GetResourceLFTags",
    "lakeformation:ListDataCellsFilter",
    "lakeformation:ListLakeFormationOptIns",
    "lakeformation:ListPermissions",
    "lakeformation:RegisterResource",
    "lakeformation:RevokePermissions",
    "lakeformation:UpdateDataCellsFilter",
    "glue:GetDatabase",
    "glue:GetTable",
    "organizations:DescribeOrganization",
    "ram:GetResourceShareInvitations",
    "ram:ListResources"
   ],
   "Resource": "*"
  },
  {
   "Sid": "CrossAccountRAMResourceSharingPermissions",
   "Effect": "Allow",
   "Action": [
    "glue:DeleteResourcePolicy",
    "glue:PutResourcePolicy"
   ],
   "Resource": [
    "arn:aws:glue:*:*:catalog",
    "arn:aws:glue:*:*:database/*",
    "arn:aws:glue:*:*:table/*"
   ],
   "Condition": {
    "ForAnyValue:StringEquals": {
     "aws:CalledVia": [
      "ram.amazonaws.com"
     ]
    }
   }
  },
  {
   "Sid": "CrossAccountLakeFormationResourceSharingPermissions",
   "Effect": "Allow",
   "Action": [
```

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

```
    "ForAnyValue:StringEquals": {
     "aws:CalledVia": [
      "lakeformation.amazonaws.com"
     ]
    }
   }
  },
  {
   "Sid": "CrossAccountRAMResourceSharingViaLakeFormationHybrid",
   "Effect": "Allow",
   "Action": "ram:AssociateResourceSharePermission",
   "Resource": "*",
   "Condition": {
    "StringLike": {
     "ram:PermissionArn": "arn:aws:ram::aws:permission/AWSRAMLFEnabled*"
    },
    "ForAnyValue:StringEquals": {
     "aws:CalledVia": [
      "lakeformation.amazonaws.com"
     ]
    }
   }
  },
  {
   "Sid": "KMSDecryptPermission",
   "Effect": "Allow",
   "Action": [
    "kms:Decrypt"
   ],
   "Resource": "*",
   "Condition": {
    "StringEquals": {
     "aws:ResourceTag/datazone:projectId": "proj-all"
    }
   }
  },
  {
   "Sid": "GetRoleForDataZone",
   "Effect": "Allow",
   "Action": [
    "iam:GetRole"
   ],
   "Resource": [
    "arn:aws:iam::*:role/AmazonDataZone*",
```

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

AWS 관리형 정책: AmazonDataZoneRedshiftManageAccessRolePolicy

이 정책은 Amazon Redshift 데이터를 카탈로그에 게시할 수 있는 DataZone 권한을 Amazon에 부여합니다. 또한 카탈로그에 게시된 Amazon Redshift 또는 Amazon Redshift Serverless 자산에 대한 액세스 권한을 부여하거나 취소할 수 있는 DataZone 권한을 Amazon에 부여합니다.

```
{
 "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 관리형 정책: AmazonDataZoneCrossAccountAdmin

AmazonDataZoneCrossAccountAdmin 정책을 IAM 자격 증명에 연결할 수 있습니다.

이 정책을 통해 사용자는 Amazon DataZone 연결 계정으로 작업할 수 있습니다.

```
{
    "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 관리형 정책: AmazonDataZoneDomainExecutionRolePolicy

Amazon 서비스 역할의 DataZone `DomainExecutionRole` 기본 정책입니다. 이 역할은 Amazon DataZone 도메인의 데이터를 카탈로그화, 검색, 관리, 공유 및 분석하는 DataZone 데 사용됩니다. 이 역할은 데이터 포털 사용에 필요한 모든 Amazon DataZone APIs에 대한 액세스 권한과 Amazon DataZone 도메인에서 연결된 계정 사용을 지원할 수 있는 RAM 권한을 제공합니다.

AmazonDataZoneDomainExecutionRolePolicy 정책을 에 연결할 수 있습니다`AmazonDataZoneDomainExecutionRole`.

```
{
 "Version": "2012-10-17",
 "Statement": [
  {
   "Sid": "DomainExecutionRoleStatement",
   "Effect": "Allow",
   "Action": [
    "datazone:AcceptPredictions",
    "datazone:AcceptSubscriptionRequest",
    "datazone:AddEntityOwner",
    "datazone:AddPolicyGrant",
    "datazone:CancelMetadataGenerationRun",
    "datazone:CancelSubscription",
    "datazone:CreateAsset",
    "datazone:CreateAssetFilter",
    "datazone:CreateAssetRevision",
    "datazone:CreateAssetType",
    "datazone:CreateDataProduct",
    "datazone:CreateDataProductRevision",
    "datazone:CreateDataSource",
    "datazone:CreateDomainUnit",
    "datazone:CreateEnvironment",
    "datazone:CreateEnvironmentBlueprint",
    "datazone:CreateEnvironmentProfile",
    "datazone:CreateFormType",
    "datazone:CreateGlossary",
    "datazone:CreateGlossaryTerm",
    "datazone:CreateListingChangeSet",
    "datazone:CreateProject",
    "datazone:CreateProjectMembership",
```

```
    "datazone:CreateSubscriptionGrant",
    "datazone:CreateSubscriptionRequest",
    "datazone:DeleteAsset",
    "datazone:DeleteAssetFilter",
    "datazone:DeleteAssetType",
    "datazone:DeleteDataProduct",
    "datazone:DeleteDataSource",
    "datazone:DeleteDomainUnit",
    "datazone:DeleteEnvironment",
    "datazone:DeleteEnvironmentBlueprint",
    "datazone:DeleteEnvironmentProfile",
    "datazone:DeleteFormType",
    "datazone:DeleteGlossary",
    "datazone:DeleteGlossaryTerm",
    "datazone:DeleteListing",
    "datazone:DeleteProject",
    "datazone:DeleteProjectMembership",
    "datazone:DeleteSubscriptionGrant",
    "datazone:DeleteSubscriptionRequest",
    "datazone:DeleteSubscriptionTarget",
    "datazone:DeleteTimeSeriesDataPoints",
    "datazone:GetAsset",
    "datazone:GetAssetFilter",
    "datazone:GetAssetType",
    "datazone:GetDataProduct",
    "datazone:GetDataSource",
    "datazone:GetDataSourceRun",
    "datazone:GetDomain",
    "datazone:GetDomainUnit",
    "datazone:GetEnvironment",
    "datazone:GetEnvironmentAction",
    "datazone:GetEnvironmentActionLink",
    "datazone:GetEnvironmentBlueprint",
    "datazone:GetEnvironmentCredentials",
    "datazone:GetEnvironmentProfile",
    "datazone:GetFormType",
    "datazone:GetGlossary",
    "datazone:GetGlossaryTerm",
    "datazone:GetGroupProfile",
    "datazone:GetLineageNode",
    "datazone:GetListing",
    "datazone:GetMetadataGenerationRun",
    "datazone:GetProject",
    "datazone:GetSubscription",
```

```
    "datazone:GetSubscriptionEligibility",
    "datazone:GetSubscriptionGrant",
    "datazone:GetSubscriptionRequestDetails",
    "datazone:GetSubscriptionTarget",
    "datazone:GetTimeSeriesDataPoint",
    "datazone:GetUserProfile",
    "datazone:ListAccountEnvironments",
    "datazone:ListAssetFilters",
    "datazone:ListAssetRevisions",
    "datazone:ListDataProductRevisions",
    "datazone:ListDataSourceRunActivities",
    "datazone:ListDataSourceRuns",
    "datazone:ListDataSources",
    "datazone:ListDomainUnitsForParent",
    "datazone:ListEntityOwners",
    "datazone:ListEnvironmentActions",
    "datazone:ListEnvironmentBlueprintConfigurationSummaries",
    "datazone:ListEnvironmentBlueprintConfigurations",
    "datazone:ListEnvironmentBlueprints",
    "datazone:ListEnvironmentProfiles",
    "datazone:ListEnvironments",
    "datazone:ListGroupsForUser",
    "datazone:ListLineageNodeHistory",
    "datazone:ListMetadataGenerationRuns",
    "datazone:ListNotifications",
    "datazone:ListPolicyGrants",
    "datazone:ListProjectMemberships",
    "datazone:ListProjects",
    "datazone:ListSubscriptionGrants",
    "datazone:ListSubscriptionRequests",
    "datazone:ListSubscriptionTargets",
    "datazone:ListSubscriptions",
    "datazone:ListTimeSeriesDataPoints",
    "datazone:ListWarehouseMetadata",
    "datazone:RejectPredictions",
    "datazone:RejectSubscriptionRequest",
    "datazone:RemoveEntityOwner",
    "datazone:RemovePolicyGrant",
    "datazone:RevokeSubscription",
    "datazone:Search",
    "datazone:SearchGroupProfiles",
    "datazone:SearchListings",
    "datazone:SearchTypes",
    "datazone:SearchUserProfiles",
```

```
    "datazone:StartDataSourceRun",
    "datazone:StartMetadataGenerationRun",
    "datazone:UpdateAssetFilter",
    "datazone:UpdateDataSource",
    "datazone:UpdateDomainUnit",
    "datazone:UpdateEnvironment",
    "datazone:UpdateEnvironmentBlueprint",
    "datazone:UpdateEnvironmentDeploymentStatus",
    "datazone:UpdateEnvironmentProfile",
    "datazone:UpdateGlossary",
    "datazone:UpdateGlossaryTerm",
    "datazone:UpdateProject",
    "datazone:UpdateSubscriptionGrantStatus",
    "datazone:UpdateSubscriptionRequest"
   ],
   "Resource": "*"
  },
  {
   "Sid": "RAMResourceShareStatement",
   "Effect": "Allow",
   "Action": "ram:GetResourceShareAssociations",
   "Resource": "*"
  }
 ]
}
```

AWS 관리형 정책: AmazonDataZoneSageMakerProvisioning

이 AmazonDataZoneSageMakerProvisioning 정책은 Amazon DataZone 와 상호 운용하는 데 필요한 권한을 Amazon에 부여합니다 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 관리형 정책: AmazonDataZoneSageMakerAccess

이 정책은 Amazon SageMaker 자산을 카탈로그에 게시할 수 있는 DataZone 권한을 Amazon에 부여합니다. 또한 카탈로그에 SageMaker 게시된 Amazon 자산에 대한 액세스 권한을 부여하거나 취소할 수 있는 DataZone 권한을 Amazon에 부여합니다.

이 정책에는 다음을 할 수 있는 권한이 포함되어 있습니다.

- cloudtrail - CloudTrail 추적에 대한 정보를 검색합니다.
- cloudwatch - 현재 CloudWatch 경보를 검색합니다.
- 로그 - CloudWatch 로그에 대한 지표 필터를 검색합니다.
- sns - SNS 주제에 대한 구독 목록을 검색합니다.
- config - 구성 레코더, 리소스 및 AWS Config 규칙에 대한 정보를 검색합니다. 또한 서비스 연결 역할이 AWS Config 규칙을 생성 및 삭제하고 규칙에 대한 평가를 실행할 수 있습니다.
- iam - 계정에 대한 자격 증명 보고서를 가져오고 생성합니다.
- 조직 - 조직의 계정 및 조직 단위(OU) 정보를 검색합니다.
- securityhub - Security Hub 서비스, 표준 및 제어가 구성된 방법에 대한 정보를 검색합니다.
- 태그 - 리소스 태그에 대한 정보를 검색합니다.

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

```
{
 "Sid": "AmazonSageMakerReadPermission",
 "Effect": "Allow",
 "Action": [
  "sagemaker:DescribeFeatureGroup",
  "sagemaker:ListModelPackages",
  "sagemaker:DescribeModelPackage",
  "sagemaker:DescribeModelPackageGroup",
  "sagemaker:DescribeAlgorithm",
  "sagemaker:ListTags",
  "sagemaker:DescribeDomain",
  "sagemaker:GetModelPackageGroupPolicy",
  "sagemaker:Search"
 ],
 "Resource": "*"
},
{
 "Sid": "AmazonSageMakerTaggingPermission",
 "Effect": "Allow",
 "Action": [
  "sagemaker:AddTags",
  "sagemaker:DeleteTags"
 ],
 "Resource": "*",
 "Condition": {
  "ForAnyValue:StringLike": {
   "aws:TagKeys": [
    "sagemaker:shared-with:*"
   ]
  }
 }
},
{
 "Sid": "AmazonSageMakerModelPackageGroupPolicyPermission",
 "Effect": "Allow",
 "Action": [
  "sagemaker:PutModelPackageGroupPolicy",
  "sagemaker:DeleteModelPackageGroupPolicy"
 ],
 "Resource": [
  "arn:*:sagemaker:*:*:model-package-group/*"
 ]
},
{
```

```
    "Sid": "AmazonSageMakerRAMPermission",
    "Effect": "Allow",
    "Action": [
     "ram:GetResourceShares",
     "ram:GetResourceShareInvitations",
     "ram:GetResourceShareAssociations"
    ],
    "Resource": "*"
   },
   {
    "Sid": "AmazonSageMakerRAMResourcePolicyPermission",
    "Effect": "Allow",
    "Action": [
     "sagemaker:PutResourcePolicy",
     "sagemaker:GetResourcePolicy",
     "sagemaker:DeleteResourcePolicy"
    ],
    "Resource": [
     "arn:*:sagemaker:*:*:feature-group/*"
    ]
   },
   {
    "Sid": "AmazonSageMakerRAMTagResourceSharePermission",
    "Effect": "Allow",
    "Action": [
     "ram:TagResource"
    ],
    "Resource": "arn:*:ram:*:*:resource-share/*",
    "Condition": {
     "Null": {
      "aws:RequestTag/AwsDataZoneDomainId": "false"
     }
    }
   },
   {
    "Sid": "AmazonSageMakerRAMDeleteResourceSharePermission",
    "Effect": "Allow",
    "Action": [
     "ram:DeleteResourceShare"
    ],
    "Resource": "arn:*:ram:*:*:resource-share/*",
    "Condition": {
     "Null": {
      "aws:ResourceTag/AwsDataZoneDomainId": "false"
```

```
    }
   }
  },
  {
   "Sid": "AmazonSageMakerRAMCreateResourceSharePermission",
   "Effect": "Allow",
   "Action": [
    "ram:CreateResourceShare"
   ],
   "Resource": "*",
   "Condition": {
    "StringLikeIfExists": {
     "ram:RequestedResourceType": [
      "sagemaker:*"
     ]
    },
    "Null": {
     "aws:RequestTag/AwsDataZoneDomainId": "false"
    }
   }
  },
  {
   "Sid": "AmazonSageMakerS3BucketPolicyPermission",
   "Effect": "Allow",
   "Action": [
    "s3:DeleteBucketPolicy",
    "s3:PutBucketPolicy",
    "s3:GetBucketPolicy"
   ],
   "Resource": [
    "arn:aws:s3:::sagemaker-datazone*",
    "arn:aws:s3:::SageMaker-DataZone*",
    "arn:aws:s3:::datazone-sagemaker*",
    "arn:aws:s3:::DataZone-SageMaker*",
    "arn:aws:s3:::amazon-datazone*"
   ]
  },
  {
   "Sid": "AmazonSageMakerS3Permission",
   "Effect": "Allow",
   "Action": [
    "s3:GetObject",
    "s3:ListBucket"
   ],
```

```
    "Resource": [
     "arn:aws:s3:::sagemaker-datazone*",
     "arn:aws:s3:::SageMaker-DataZone*",
     "arn:aws:s3:::datazone-sagemaker*",
     "arn:aws:s3:::DataZone-SageMaker*",
     "arn:aws:s3:::amazon-datazone*"
    ]
   },
   {
    "Sid": "AmazonSageMakerECRPermission",
    "Effect": "Allow",
    "Action": [
     "ecr:GetRepositoryPolicy",
     "ecr:SetRepositoryPolicy",
     "ecr:DeleteRepositoryPolicy"
    ],
    "Resource": "*",
    "Condition": {
     "Null": {
      "aws:ResourceTag/AmazonDataZoneEnvironment": "false"
     }
    }
   },
   {
    "Sid": "AmazonSageMakerKMSReadPermission",
    "Effect": "Allow",
    "Action": [
     "kms:DescribeKey"
    ],
    "Resource": "*",
    "Condition": {
     "ForAnyValue:StringEquals": {
      "aws:TagKeys": [
       "AmazonDataZoneEnvironment"
      ]
     }
    }
   },
   {
    "Sid": "AmazonSageMakerKMSGrantPermission",
    "Effect": "Allow",
    "Action": [
     "kms:CreateGrant"
    ],
```

```
    "Resource": "*",
    "Condition": {
     "ForAnyValue:StringEquals": {
      "aws:TagKeys": [
       "AmazonDataZoneEnvironment"
      ]
     },
     "ForAllValues:StringEquals": {
      "kms:GrantOperations": [
       "Decrypt"
      ]
     }
    }
   }
  ]
}
```

AWS 관리형 정책: AmazonDataZoneSageMakerEnvironmentRolePermissionsBoundary

> **Note**
>
> 이 정책은 권한 경계입니다. 권한 경계는 자격 증명 기반 정책이 IAM엔터티에 부여할 수 있는 최대 권한을 설정합니다. Amazon DataZone 권한 경계 정책을 단독으로 사용하고 연결해서는 안 됩니다. Amazon DataZone 권한 경계 정책은 Amazon DataZone 관리형 역할에만 연결해야 합니다. 권한 경계에 대한 자세한 내용은 IAM 사용 설명서의 IAM엔터티에 대한 권한 경계를 참조하세요.

Amazon SageMaker DataZone 데이터 포털을 통해 Amazon 환경을 생성할 때 Amazon은 환경 생성 중에 생성되는 IAM 역할에 이 권한 경계를 DataZone 적용합니다. 권한 경계는 Amazon이 DataZone 생성하는 역할의 범위와 추가하는 역할을 제한합니다.

Amazon은 `AmazonDataZoneSageMakerEnvironmentRolePermissionsBoundary` 관리형 정책을 DataZone 사용하여 연결된 프로비저닝된 IAM 보안 주체를 제한합니다. 보안 주체는 대화형 엔터프라이즈 사용자 또는 분석 서비스(예AWS SageMaker:)를 대신하여 Amazon이 수임할 DataZone 수 있는 사용자 역할의 형태를 취한 다음 Amazon S3 또는 Amazon Redshift에서 읽고 쓰거나 AWS Glue 크롤러를 실행하는 등의 데이터를 처리하는 작업을 수행할 수 있습니다.

이 AmazonDataZoneSageMakerEnvironmentRolePermissionsBoundary 정책은 Amazon SageMaker, AWS Glue, Amazon S3, AWS Lake Formation, Amazon Redshift 및 Amazon Athena 와 같은 DataZone 서비스에 Amazon에 대한 읽기 및 쓰기 액세스 권한을 부여합니다. 또한 이 정책은 네트워크 인터페이스, Amazon ECR리포지토리 및 키와 같이 이러한 서비스를 사용하는 데 필요한 일부 인프라 리소스에 대한 읽기 및 AWS KMS 쓰기 권한을 부여합니다. 또한 Amazon SageMaker SageMaker Canvas와 같은 Amazon 애플리케이션에 액세스할 수 있습니다.

Amazon은 AmazonDataZoneSageMakerEnvironmentRolePermissionsBoundary 관리형 정책을 모든 Amazon DataZone 환경 역할(소유자 및 기여자)에 대한 권한 경계로 DataZone 적용합니다. 이 권한 경계는 환경에 필요한 필수 리소스 및 작업에 대한 액세스만 허용하도록 이러한 역할을 제한합니다.

```
       {
"Version": "2012-10-17",
"Statement": [
 {
  "Sid": "AllowAllNonAdminSageMakerActions",
  "Effect": "Allow",
  "Action": [
   "sagemaker:*",
   "sagemaker-geospatial:*"
  ],
  "NotResource": [
   "arn:aws:sagemaker:*:*:domain/*",
   "arn:aws:sagemaker:*:*:user-profile/*",
   "arn:aws:sagemaker:*:*:app/*",
   "arn:aws:sagemaker:*:*:space/*",
   "arn:aws:sagemaker:*:*:flow-definition/*"
  ]
 },
 {
  "Sid": "AllowSageMakerProfileManagement",
  "Effect": "Allow",
  "Action": [
   "sagemaker:CreateUserProfile",
   "sagemaker:DescribeUserProfile",
   "sagemaker:UpdateUserProfile",
   "sagemaker:CreatePresignedDomainUrl"
  ],
  "Resource": "arn:aws:sagemaker:*:*:*/*"
 },
```

```
{
 "Sid": "AllowLakeFormation",
 "Effect": "Allow",
 "Action": [
  "lakeformation:GetDataAccess"
 ],
 "Resource": "*"
},
{
 "Sid": "AllowAddTagsForAppAndSpace",
 "Effect": "Allow",
 "Action": [
  "sagemaker:AddTags"
 ],
 "Resource": [
  "arn:aws:sagemaker:*:*:app/*",
  "arn:aws:sagemaker:*:*:space/*"
 ],
 "Condition": {
  "StringEquals": {
   "sagemaker:TaggingAction": [
    "CreateApp",
    "CreateSpace"
   ]
  }
 }
},
{
 "Sid": "AllowStudioActions",
 "Effect": "Allow",
 "Action": [
  "sagemaker:CreatePresignedDomainUrl",
  "sagemaker:DescribeApp",
  "sagemaker:DescribeDomain",
  "sagemaker:DescribeSpace",
  "sagemaker:DescribeUserProfile",
  "sagemaker:ListApps",
  "sagemaker:ListDomains",
  "sagemaker:ListSpaces",
  "sagemaker:ListUserProfiles"
 ],
 "Resource": "*"
},
{
```

```
    "Sid": "AllowAppActionsForUserProfile",
    "Effect": "Allow",
    "Action": [
     "sagemaker:CreateApp",
     "sagemaker:DeleteApp"
    ],
    "Resource": "arn:aws:sagemaker:*:*:app/*/*/*/*",
    "Condition": {
     "Null": {
      "sagemaker:OwnerUserProfileArn": "true"
     }
    }
   },
   {
    "Sid": "AllowAppActionsForSharedSpaces",
    "Effect": "Allow",
    "Action": [
     "sagemaker:CreateApp",
     "sagemaker:DeleteApp"
    ],
    "Resource": "arn:aws:sagemaker:*:*:app/${sagemaker:DomainId}/*/*/*",
    "Condition": {
     "StringEquals": {
      "sagemaker:SpaceSharingType": [
       "Shared"
      ]
     }
    }
   },
   {
    "Sid": "AllowMutatingActionsOnSharedSpacesWithoutOwner",
    "Effect": "Allow",
    "Action": [
     "sagemaker:CreateSpace",
     "sagemaker:DeleteSpace",
     "sagemaker:UpdateSpace"
    ],
    "Resource": "arn:aws:sagemaker:*:*:space/${sagemaker:DomainId}/*",
    "Condition": {
     "Null": {
      "sagemaker:OwnerUserProfileArn": "true"
     }
    }
   },
```

```
  {
   "Sid": "RestrictMutatingActionsOnSpacesToOwnerUserProfile",
   "Effect": "Allow",
   "Action": [
    "sagemaker:CreateSpace",
    "sagemaker:DeleteSpace",
    "sagemaker:UpdateSpace"
   ],
   "Resource": "arn:aws:sagemaker:*:*:space/${sagemaker:DomainId}/*",
   "Condition": {
    "ArnLike": {
     "sagemaker:OwnerUserProfileArn": "arn:aws:sagemaker:*:*:user-profile/
${sagemaker:DomainId}/${sagemaker:UserProfileName}"
    },
    "StringEquals": {
     "sagemaker:SpaceSharingType": [
      "Private",
      "Shared"
     ]
    }
   }
  },
  {
   "Sid": "RestrictMutatingActionsOnPrivateSpaceAppsToOwnerUserProfile",
   "Effect": "Allow",
   "Action": [
    "sagemaker:CreateApp",
    "sagemaker:DeleteApp"
   ],
   "Resource": "arn:aws:sagemaker:*:*:app/${sagemaker:DomainId}/*/*/*",
   "Condition": {
    "ArnLike": {
     "sagemaker:OwnerUserProfileArn": "arn:aws:sagemaker:*:*:user-profile/
${sagemaker:DomainId}/${sagemaker:UserProfileName}"
    },
    "StringEquals": {
     "sagemaker:SpaceSharingType": [
      "Private"
     ]
    }
   }
  },
  {
   "Sid": "AllowFlowDefinitionActions",
```

```
    "Effect": "Allow",
    "Action": "sagemaker:*",
    "Resource": [
     "arn:aws:sagemaker:*:*:flow-definition/*"
    ],
    "Condition": {
     "StringEqualsIfExists": {
      "sagemaker:WorkteamType": [
       "private-crowd",
       "vendor-crowd"
      ]
     }
    }
   },
   {
    "Sid": "AllowAWSServiceActions",
    "Effect": "Allow",
    "Action": [
     "sqlworkbench:*",
     "datazone:*",
     "application-autoscaling:DeleteScalingPolicy",
     "application-autoscaling:DeleteScheduledAction",
     "application-autoscaling:DeregisterScalableTarget",
     "application-autoscaling:DescribeScalableTargets",
     "application-autoscaling:DescribeScalingActivities",
     "application-autoscaling:DescribeScalingPolicies",
     "application-autoscaling:DescribeScheduledActions",
     "application-autoscaling:PutScalingPolicy",
     "application-autoscaling:PutScheduledAction",
     "application-autoscaling:RegisterScalableTarget",
     "aws-marketplace:ViewSubscriptions",
     "cloudformation:GetTemplateSummary",
     "cloudwatch:DeleteAlarms",
     "cloudwatch:DescribeAlarms",
     "cloudwatch:GetMetricData",
     "cloudwatch:GetMetricStatistics",
     "cloudwatch:ListMetrics",
     "cloudwatch:PutMetricAlarm",
     "cloudwatch:PutMetricData",
     "codecommit:BatchGetRepositories",
     "codecommit:CreateRepository",
     "codecommit:GetRepository",
     "codecommit:List*",
     "ec2:CreateNetworkInterface",
```

```
    "ec2:CreateNetworkInterfacePermission",
    "ec2:DeleteNetworkInterface",
    "ec2:DeleteNetworkInterfacePermission",
    "ec2:DescribeDhcpOptions",
    "ec2:DescribeNetworkInterfaces",
    "ec2:DescribeRouteTables",
    "ec2:DescribeSecurityGroups",
    "ec2:DescribeSubnets",
    "ec2:DescribeVpcEndpoints",
    "ec2:DescribeVpcEndpointServices",
    "ec2:DescribeVpcs",
    "ecr:BatchCheckLayerAvailability",
    "ecr:BatchGetImage",
    "ecr:Describe*",
    "ecr:GetAuthorizationToken",
    "ecr:GetDownloadUrlForLayer",
    "ecr:StartImageScan",
    "elastic-inference:Connect",
    "elasticfilesystem:DescribeFileSystems",
    "elasticfilesystem:DescribeMountTargets",
    "fsx:DescribeFileSystems",
    "groundtruthlabeling:*",
    "iam:GetRole",
    "iam:ListRoles",
    "kms:DescribeKey",
    "kms:ListAliases",
    "lambda:ListFunctions",
    "logs:CreateLogDelivery",
    "logs:CreateLogGroup",
    "logs:CreateLogStream",
    "logs:DeleteLogDelivery",
    "logs:DescribeLogGroups",
    "logs:DescribeLogStreams",
    "logs:GetLogDelivery",
    "logs:GetLogEvents",
    "logs:ListLogDeliveries",
    "logs:PutLogEvents",
    "logs:UpdateLogDelivery",
    "redshift-data:BatchExecuteStatement",
    "redshift-data:CancelStatement",
    "redshift-data:DescribeStatement",
    "redshift-data:DescribeTable",
    "redshift-data:ExecuteStatement",
    "redshift-data:GetStatementResult",
```

```
    "redshift-data:ListSchemas",
    "redshift-data:ListTables",
    "redshift-serverless:GetCredentials",
    "redshift-serverless:GetNamespace",
    "redshift-serverless:GetWorkgroup",
    "redshift-serverless:ListNamespaces",
    "redshift-serverless:ListWorkgroups",
    "secretsmanager:ListSecrets",
    "servicecatalog:Describe*",
    "servicecatalog:List*",
    "servicecatalog:ScanProvisionedProducts",
    "servicecatalog:SearchProducts",
    "servicecatalog:SearchProvisionedProducts",
    "sns:ListTopics",
    "tag:GetResources"
   ],
   "Resource": "*"
  },
  {
   "Sid": "AllowRAMInvitation",
   "Effect": "Allow",
   "Action": "ram:AcceptResourceShareInvitation",
   "Resource": "*",
   "Condition": {
    "StringLike": {
     "ram:ResourceShareName": "dzd_*"
    }
   }
  },
  {
   "Sid": "AllowECRActions",
   "Effect": "Allow",
   "Action": [
    "ecr:SetRepositoryPolicy",
    "ecr:CompleteLayerUpload",
    "ecr:CreateRepository",
    "ecr:BatchDeleteImage",
    "ecr:UploadLayerPart",
    "ecr:DeleteRepositoryPolicy",
    "ecr:InitiateLayerUpload",
    "ecr:DeleteRepository",
    "ecr:PutImage",
    "ecr:TagResource",
    "ecr:UntagResource"
```

```
    ],
    "Resource": [
     "arn:aws:ecr:*:*:repository/sagemaker*",
     "arn:aws:ecr:*:*:repository/datazone*"
    ]
   },
   {
    "Sid": "AllowCodeCommitActions",
    "Effect": "Allow",
    "Action": [
     "codecommit:GitPull",
     "codecommit:GitPush"
    ],
    "Resource": [
     "arn:aws:codecommit:*:*:*sagemaker*",
     "arn:aws:codecommit:*:*:*SageMaker*",
     "arn:aws:codecommit:*:*:*Sagemaker*"
    ]
   },
   {
    "Sid": "AllowCodeBuildActions",
    "Action": [
     "codebuild:BatchGetBuilds",
     "codebuild:StartBuild"
    ],
    "Resource": [
     "arn:aws:codebuild:*:*:project/sagemaker*",
     "arn:aws:codebuild:*:*:build/*"
    ],
    "Effect": "Allow"
   },
   {
    "Sid": "AllowStepFunctionsActions",
    "Action": [
     "states:DescribeExecution",
     "states:GetExecutionHistory",
     "states:StartExecution",
     "states:StopExecution",
     "states:UpdateStateMachine"
    ],
    "Resource": [
     "arn:aws:states:*:*:statemachine:*sagemaker*",
     "arn:aws:states:*:*:execution:*sagemaker*:*"
    ],
```

```
    "Effect": "Allow"
   },
   {
    "Sid": "AllowSecretManagerActions",
    "Effect": "Allow",
    "Action": [
     "secretsmanager:DescribeSecret",
     "secretsmanager:GetSecretValue",
     "secretsmanager:CreateSecret",
     "secretsmanager:PutResourcePolicy"
    ],
    "Resource": [
     "arn:aws:secretsmanager:*:*:secret:AmazonSageMaker-*"
    ]
   },
   {
    "Sid": "AllowServiceCatalogProvisionProduct",
    "Effect": "Allow",
    "Action": [
     "servicecatalog:ProvisionProduct"
    ],
    "Resource": "*"
   },
   {
    "Sid": "AllowServiceCatalogTerminateUpdateProvisionProduct",
    "Effect": "Allow",
    "Action": [
     "servicecatalog:TerminateProvisionedProduct",
     "servicecatalog:UpdateProvisionedProduct"
    ],
    "Resource": "*",
    "Condition": {
     "StringEquals": {
      "servicecatalog:userLevel": "self"
     }
    }
   },
   {
    "Sid": "AllowS3ObjectActions",
    "Effect": "Allow",
    "Action": [
     "s3:AbortMultipartUpload",
     "s3:DeleteObject",
     "s3:DeleteObjectVersion",
```

```
    "s3:GetObject",
    "s3:PutObject",
    "s3:PutObjectRetention",
    "s3:ReplicateObject",
    "s3:RestoreObject",
    "s3:GetBucketAcl",
    "s3:PutObjectAcl"
   ],
   "Resource": [
    "arn:aws:s3:::SageMaker-DataZone*",
    "arn:aws:s3:::DataZone-SageMaker*",
    "arn:aws:s3:::Sagemaker-DataZone*",
    "arn:aws:s3:::DataZone-Sagemaker*",
    "arn:aws:s3:::sagemaker-datazone*",
    "arn:aws:s3:::datazone-sagemaker*",
    "arn:aws:s3:::amazon-datazone*"
   ]
  },
  {
   "Sid": "AllowS3GetObjectWithSageMakerExistingObjectTag",
   "Effect": "Allow",
   "Action": [
    "s3:GetObject"
   ],
   "Resource": [
    "arn:aws:s3:::*"
   ],
   "Condition": {
    "StringEqualsIgnoreCase": {
     "s3:ExistingObjectTag/SageMaker": "true"
    }
   }
  },
  {
   "Sid": "AllowS3GetObjectWithServiceCatalogProvisioningExistingObjectTag",
   "Effect": "Allow",
   "Action": [
    "s3:GetObject"
   ],
   "Resource": [
    "arn:aws:s3:::*"
   ],
   "Condition": {
    "StringEquals": {
```

```
      "s3:ExistingObjectTag/servicecatalog:provisioning": "true"
     }
    }
   },
   {
    "Sid": "AllowS3BucketActions",
    "Effect": "Allow",
    "Action": [
     "s3:GetBucketLocation",
     "s3:ListBucket",
     "s3:ListAllMyBuckets",
     "s3:GetBucketCors",
     "s3:PutBucketCors"
    ],
    "Resource": [
     "arn:aws:s3:::SageMaker-DataZone*",
     "arn:aws:s3:::DataZone-SageMaker*",
     "arn:aws:s3:::Sagemaker-DataZone*",
     "arn:aws:s3:::DataZone-Sagemaker*",
     "arn:aws:s3:::sagemaker-datazone*",
     "arn:aws:s3:::datazone-sagemaker*",
     "arn:aws:s3:::amazon-datazone*"
    ]
   },
   {
    "Sid": "ReadSageMakerJumpstartArtifacts",
    "Effect": "Allow",
    "Action": "s3:GetObject",
    "Resource": [
     "arn:aws:s3:::jumpstart-cache-prod-us-west-2/*",
     "arn:aws:s3:::jumpstart-cache-prod-us-east-1/*",
     "arn:aws:s3:::jumpstart-cache-prod-us-east-2/*",
     "arn:aws:s3:::jumpstart-cache-prod-eu-west-1/*",
     "arn:aws:s3:::jumpstart-cache-prod-eu-central-1/*",
     "arn:aws:s3:::jumpstart-cache-prod-ap-south-1/*",
     "arn:aws:s3:::jumpstart-cache-prod-ap-northeast-2/*",
     "arn:aws:s3:::jumpstart-cache-prod-ap-northeast-1/*",
     "arn:aws:s3:::jumpstart-cache-prod-ap-southeast-1/*",
     "arn:aws:s3:::jumpstart-cache-prod-ap-southeast-2/*"
    ]
   },
   {
    "Sid": "AllowLambdaInvokeFunction",
    "Effect": "Allow",
```

```
    "Action": [
     "lambda:InvokeFunction"
    ],
    "Resource": [
     "arn:aws:lambda:*:*:function:*SageMaker*",
     "arn:aws:lambda:*:*:function:*sagemaker*",
     "arn:aws:lambda:*:*:function:*Sagemaker*",
     "arn:aws:lambda:*:*:function:*LabelingFunction*"
    ]
   },
   {
    "Sid": "AllowCreateServiceLinkedRoleForSageMakerApplicationAutoscaling",
    "Action": "iam:CreateServiceLinkedRole",
    "Effect": "Allow",
    "Resource": "arn:aws:iam::*:role/aws-service-role/sagemaker.application-
autoscaling.amazonaws.com/AWSServiceRoleForApplicationAutoScaling_SageMakerEndpoint",
    "Condition": {
     "StringLike": {
      "iam:AWSServiceName": "sagemaker.application-autoscaling.amazonaws.com"
     }
    }
   },
   {
    "Sid": "AllowSNSActions",
    "Effect": "Allow",
    "Action": [
     "sns:Subscribe",
     "sns:CreateTopic",
     "sns:Publish"
    ],
    "Resource": [
     "arn:aws:sns:*:*:*SageMaker*",
     "arn:aws:sns:*:*:*Sagemaker*",
     "arn:aws:sns:*:*:*sagemaker*"
    ]
   },
   {
    "Sid": "AllowPassRoleForSageMakerRoles",
    "Effect": "Allow",
    "Action": [
     "iam:PassRole"
    ],
    "Resource": [
     "arn:aws:iam::*:role/sm-provisioning/datazone_usr_sagemaker_execution_role_*"
```

```
    ],
    "Condition": {
     "StringEquals": {
      "iam:PassedToService": [
       "glue.amazonaws.com",
       "bedrock.amazonaws.com",
       "states.amazonaws.com",
       "lakeformation.amazonaws.com",
       "events.amazonaws.com",
       "sagemaker.amazonaws.com",
       "forecast.amazonaws.com"
      ]
     }
    }
   },
   {
    "Sid": "CrossAccountKmsOperations",
    "Effect": "Allow",
    "Action": [
     "kms:DescribeKey",
     "kms:Decrypt",
     "kms:ListKeys"
    ],
    "Resource": "*",
    "Condition": {
     "StringNotEquals": {
      "aws:ResourceAccount": "${aws:PrincipalAccount}"
     }
    }
   },
   {
    "Sid": "KmsOperationsWithResourceTag",
    "Effect": "Allow",
    "Action": [
     "kms:DescribeKey",
     "kms:Decrypt",
     "kms:ListKeys",
     "kms:Encrypt",
     "kms:GenerateDataKey",
     "kms:RetireGrant"
    ],
    "Resource": "*",
    "Condition": {
     "Null": {
```

```
      "aws:ResourceTag/AmazonDataZoneEnvironment": "false"
     }
    }
   },
   {
    "Sid": "AllowAthenaActions",
    "Effect": "Allow",
    "Action": [
     "athena:BatchGetNamedQuery",
     "athena:BatchGetPreparedStatement",
     "athena:BatchGetQueryExecution",
     "athena:CreateNamedQuery",
     "athena:CreateNotebook",
     "athena:CreatePreparedStatement",
     "athena:CreatePresignedNotebookUrl",
     "athena:DeleteNamedQuery",
     "athena:DeleteNotebook",
     "athena:DeletePreparedStatement",
     "athena:ExportNotebook",
     "athena:GetDatabase",
     "athena:GetDataCatalog",
     "athena:GetNamedQuery",
     "athena:GetPreparedStatement",
     "athena:GetQueryExecution",
     "athena:GetQueryResults",
     "athena:GetQueryResultsStream",
     "athena:GetQueryRuntimeStatistics",
     "athena:GetTableMetadata",
     "athena:GetWorkGroup",
     "athena:ImportNotebook",
     "athena:ListDatabases",
     "athena:ListDataCatalogs",
     "athena:ListEngineVersions",
     "athena:ListNamedQueries",
     "athena:ListPreparedStatements",
     "athena:ListQueryExecutions",
     "athena:ListTableMetadata",
     "athena:ListTagsForResource",
     "athena:ListWorkGroups",
     "athena:StartCalculationExecution",
     "athena:StartQueryExecution",
     "athena:StartSession",
     "athena:StopCalculationExecution",
     "athena:StopQueryExecution",
```

```
    "athena:TerminateSession",
    "athena:UpdateNamedQuery",
    "athena:UpdateNotebook",
    "athena:UpdateNotebookMetadata",
    "athena:UpdatePreparedStatement"
   ],
   "Resource": [
    "*"
   ]
  },
  {
   "Sid": "AllowGlueCreateDatabase",
   "Effect": "Allow",
   "Action": [
    "glue:CreateDatabase"
   ],
   "Resource": [
    "arn:aws:glue:*:*:catalog",
    "arn:aws:glue:*:*:database/default"
   ]
  },
  {
   "Sid": "AllowRedshiftGetClusterCredentials",
   "Effect": "Allow",
   "Action": [
    "redshift:GetClusterCredentials"
   ],
   "Resource": [
    "arn:aws:redshift:*:*:dbuser:*/sagemaker_access*",
    "arn:aws:redshift:*:*:dbname:*"
   ]
  },
  {
   "Sid": "AllowListTags",
   "Effect": "Allow",
   "Action": [
    "sagemaker:ListTags"
   ],
   "Resource": [
    "arn:aws:sagemaker:*:*:user-profile/*",
    "arn:aws:sagemaker:*:*:domain/*"
   ]
  },
  {
```

```
    "Sid": "AllowCloudformationListStackResources",
    "Effect": "Allow",
    "Action": [
     "cloudformation:ListStackResources"
    ],
    "Resource": "arn:aws:cloudformation:*:*:stack/SC-*"
   },
   {
    "Sid": "AllowGlueActions",
    "Effect": "Allow",
    "Action": [
     "glue:GetColumnStatisticsForPartition",
     "glue:GetColumnStatisticsForTable",
     "glue:ListJobs",
     "glue:CreateSession",
     "glue:RunStatement",
     "glue:BatchCreatePartition",
     "glue:CreatePartitionIndex",
     "glue:CreateTable",
     "glue:BatchGetWorkflows",
     "glue:BatchUpdatePartition",
     "glue:BatchDeletePartition",
     "glue:GetPartition",
     "glue:GetPartitions",
     "glue:UpdateTable",
     "glue:DeleteTableVersion",
     "glue:DeleteTable",
     "glue:DeleteColumnStatisticsForPartition",
     "glue:DeleteColumnStatisticsForTable",
     "glue:DeletePartitionIndex",
     "glue:UpdateColumnStatisticsForPartition",
     "glue:UpdateColumnStatisticsForTable",
     "glue:BatchDeleteTableVersion",
     "glue:BatchDeleteTable",
     "glue:CreatePartition",
     "glue:DeletePartition",
     "glue:UpdatePartition",
     "glue:CreateBlueprint",
     "glue:CreateJob",
     "glue:CreateConnection",
     "glue:CreateCrawler",
     "glue:CreateDataQualityRuleset",
     "glue:CreateWorkflow",
     "glue:GetDatabases",
```

```
    "glue:GetTables",
    "glue:GetTable",
    "glue:SearchTables",
    "glue:NotifyEvent",
    "glue:ListSchemas",
    "glue:BatchGetJobs",
    "glue:GetConnection",
    "glue:GetDatabase"
   ],
   "Resource": [
    "*"
   ]
  },
  {
   "Sid": "AllowGlueActionsWithEnvironmentTag",
   "Effect": "Allow",
   "Action": [
    "glue:SearchTables",
    "glue:NotifyEvent",
    "glue:StartBlueprintRun",
    "glue:PutWorkflowRunProperties",
    "glue:StopCrawler",
    "glue:DeleteJob",
    "glue:DeleteWorkflow",
    "glue:UpdateCrawler",
    "glue:DeleteBlueprint",
    "glue:UpdateWorkflow",
    "glue:StartCrawler",
    "glue:ResetJobBookmark",
    "glue:UpdateJob",
    "glue:StartWorkflowRun",
    "glue:StopCrawlerSchedule",
    "glue:ResumeWorkflowRun",
    "glue:ListSchemas",
    "glue:DeleteCrawler",
    "glue:UpdateBlueprint",
    "glue:BatchStopJobRun",
    "glue:StopWorkflowRun",
    "glue:BatchGetJobs",
    "glue:BatchGetWorkflows",
    "glue:UpdateCrawlerSchedule",
    "glue:DeleteConnection",
    "glue:UpdateConnection",
    "glue:GetConnection",
```

```
    "glue:GetDatabase",
    "glue:GetTable",
    "glue:GetPartition",
    "glue:GetPartitions",
    "glue:BatchDeleteConnection",
    "glue:StartCrawlerSchedule",
    "glue:StartJobRun",
    "glue:CreateWorkflow",
    "glue:*DataQuality*"
   ],
   "Resource": "*",
   "Condition": {
    "Null": {
     "aws:ResourceTag/AmazonDataZoneEnvironment": "false"
    }
   }
  },
  {
   "Sid": "AllowGlueDefaultAccess",
   "Effect": "Allow",
   "Action": [
    "glue:BatchGet*",
    "glue:Get*",
    "glue:SearchTables",
    "glue:List*",
    "glue:RunStatement"
   ],
   "Resource": [
    "arn:aws:glue:*:*:catalog",
    "arn:aws:glue:*:*:database/default",
    "arn:aws:glue:*:*:connection/dz-sm-*",
    "arn:aws:glue:*:*:session/*"
   ]
  },
  {
   "Sid": "AllowRedshiftClusterActions",
   "Effect": "Allow",
   "Action": [
    "redshift:GetClusterCredentialsWithIAM",
    "redshift:DescribeClusters"
   ],
   "Resource": [
    "arn:aws:redshift:*:*:cluster:*",
    "arn:aws:redshift:*:*:dbname:*"
```

```
    ]
   },
   {
    "Sid": "AllowCreateClusterUser",
    "Effect": "Allow",
    "Action": [
     "redshift:CreateClusterUser"
    ],
    "Resource": [
     "arn:aws:redshift:*:*:dbuser:*"
    ]
   },
   {
    "Sid": "AllowCreateSecretActions",
    "Effect": "Allow",
    "Action": [
     "secretsmanager:CreateSecret",
     "secretsmanager:TagResource"
    ],
    "Resource": "arn:aws:secretsmanager:*:*:secret:AmazonDataZone-*",
    "Condition": {
     "StringLike": {
      "aws:ResourceTag/AmazonDataZoneDomain": "dzd_*",
      "aws:RequestTag/AmazonDataZoneDomain": "dzd_*"
     },
     "Null": {
      "aws:TagKeys": "false",
      "aws:ResourceTag/AmazonDataZoneProject": "false",
      "aws:ResourceTag/AmazonDataZoneDomain": "false",
      "aws:RequestTag/AmazonDataZoneDomain": "false",
      "aws:RequestTag/AmazonDataZoneProject": "false"
     },
     "ForAllValues:StringEquals": {
      "aws:TagKeys": [
       "AmazonDataZoneDomain",
       "AmazonDataZoneProject"
      ]
     }
    }
   },
   {
    "Sid": "ForecastOperations",
    "Effect": "Allow",
    "Action": [
```

```
    "forecast:CreateExplainabilityExport",
    "forecast:CreateExplainability",
    "forecast:CreateForecastEndpoint",
    "forecast:CreateAutoPredictor",
    "forecast:CreateDatasetImportJob",
    "forecast:CreateDatasetGroup",
    "forecast:CreateDataset",
    "forecast:CreateForecast",
    "forecast:CreateForecastExportJob",
    "forecast:CreatePredictorBacktestExportJob",
    "forecast:CreatePredictor",
    "forecast:DescribeExplainabilityExport",
    "forecast:DescribeExplainability",
    "forecast:DescribeAutoPredictor",
    "forecast:DescribeForecastEndpoint",
    "forecast:DescribeDatasetImportJob",
    "forecast:DescribeDataset",
    "forecast:DescribeForecast",
    "forecast:DescribeForecastExportJob",
    "forecast:DescribePredictorBacktestExportJob",
    "forecast:GetAccuracyMetrics",
    "forecast:InvokeForecastEndpoint",
    "forecast:GetRecentForecastContext",
    "forecast:DescribePredictor",
    "forecast:TagResource",
    "forecast:DeleteResourceTree"
   ],
   "Resource": [
    "arn:aws:forecast:*:*:*Canvas*"
   ]
  },
  {
   "Sid": "RDSOperation",
   "Effect": "Allow",
   "Action": "rds:DescribeDBInstances",
   "Resource": "*"
  },
  {
   "Sid": "AllowEventBridgeRule",
   "Effect": "Allow",
   "Action": [
    "events:PutRule"
   ],
   "Resource": "arn:aws:events:*:*:rule/*",
```

```
    "Condition": {
     "StringEquals": {
      "aws:RequestTag/sagemaker:is-canvas-data-prep-job": "true"
     }
    }
   },
   {
    "Sid": "EventBridgeOperations",
    "Effect": "Allow",
    "Action": [
     "events:DescribeRule",
     "events:PutTargets"
    ],
    "Resource": "arn:aws:events:*:*:rule/*",
    "Condition": {
     "StringEquals": {
      "aws:ResourceTag/sagemaker:is-canvas-data-prep-job": "true"
     }
    }
   },
   {
    "Sid": "EventBridgeTagBasedOperations",
    "Effect": "Allow",
    "Action": [
     "events:TagResource"
    ],
    "Resource": "arn:aws:events:*:*:rule/*",
    "Condition": {
     "StringEquals": {
      "aws:RequestTag/sagemaker:is-canvas-data-prep-job": "true",
      "aws:ResourceTag/sagemaker:is-canvas-data-prep-job": "true"
     }
    }
   },
   {
    "Sid": "EventBridgeListTagOperation",
    "Effect": "Allow",
    "Action": "events:ListTagsForResource",
    "Resource": "*"
   },
   {
    "Sid": "AllowEMR",
    "Effect": "Allow",
    "Action": [
```

```
    "elasticmapreduce:DescribeCluster",
    "elasticmapreduce:ListInstanceGroups",
    "elasticmapreduce:ListClusters"
   ],
   "Resource": "*"
  },
  {
   "Sid": "AllowSSOAction",
   "Effect": "Allow",
   "Action": [
    "sso:CreateApplicationAssignment",
    "sso:AssociateProfile"
   ],
   "Resource": "*"
  },
  {
   "Sid": "DenyNotAction",
   "Effect": "Deny",
   "NotAction": [
    "sagemaker:*",
    "sagemaker-geospatial:*",
    "sqlworkbench:*",
    "datazone:*",
    "forecast:*",
    "application-autoscaling:DeleteScalingPolicy",
    "application-autoscaling:DeleteScheduledAction",
    "application-autoscaling:DeregisterScalableTarget",
    "application-autoscaling:DescribeScalableTargets",
    "application-autoscaling:DescribeScalingActivities",
    "application-autoscaling:DescribeScalingPolicies",
    "application-autoscaling:DescribeScheduledActions",
    "application-autoscaling:PutScalingPolicy",
    "application-autoscaling:PutScheduledAction",
    "application-autoscaling:RegisterScalableTarget",
    "athena:BatchGetNamedQuery",
    "athena:BatchGetPreparedStatement",
    "athena:BatchGetQueryExecution",
    "athena:CreateNamedQuery",
    "athena:CreateNotebook",
    "athena:CreatePreparedStatement",
    "athena:CreatePresignedNotebookUrl",
    "athena:DeleteNamedQuery",
    "athena:DeleteNotebook",
    "athena:DeletePreparedStatement",
```

```
    "athena:ExportNotebook",
    "athena:GetDatabase",
    "athena:GetDataCatalog",
    "athena:GetNamedQuery",
    "athena:GetPreparedStatement",
    "athena:GetQueryExecution",
    "athena:GetQueryResults",
    "athena:GetQueryResultsStream",
    "athena:GetQueryRuntimeStatistics",
    "athena:GetTableMetadata",
    "athena:GetWorkGroup",
    "athena:ImportNotebook",
    "athena:ListDatabases",
    "athena:ListDataCatalogs",
    "athena:ListEngineVersions",
    "athena:ListNamedQueries",
    "athena:ListPreparedStatements",
    "athena:ListQueryExecutions",
    "athena:ListTableMetadata",
    "athena:ListTagsForResource",
    "athena:ListWorkGroups",
    "athena:StartCalculationExecution",
    "athena:StartQueryExecution",
    "athena:StartSession",
    "athena:StopCalculationExecution",
    "athena:StopQueryExecution",
    "athena:TerminateSession",
    "athena:UpdateNamedQuery",
    "athena:UpdateNotebook",
    "athena:UpdateNotebookMetadata",
    "athena:UpdatePreparedStatement",
    "aws-marketplace:ViewSubscriptions",
    "cloudformation:GetTemplateSummary",
    "cloudformation:ListStackResources",
    "cloudwatch:DeleteAlarms",
    "cloudwatch:DescribeAlarms",
    "cloudwatch:GetMetricData",
    "cloudwatch:GetMetricStatistics",
    "cloudwatch:ListMetrics",
    "cloudwatch:PutMetricAlarm",
    "cloudwatch:PutMetricData",
    "codebuild:BatchGetBuilds",
    "codebuild:StartBuild",
    "codecommit:BatchGetRepositories",
```

```
    "codecommit:CreateRepository",
    "codecommit:GetRepository",
    "codecommit:List*",
    "codecommit:GitPull",
    "codecommit:GitPush",
    "ec2:CreateNetworkInterface",
    "ec2:CreateNetworkInterfacePermission",
    "ec2:DeleteNetworkInterface",
    "ec2:DeleteNetworkInterfacePermission",
    "ec2:DescribeDhcpOptions",
    "ec2:DescribeNetworkInterfaces",
    "ec2:DescribeRouteTables",
    "ec2:DescribeSecurityGroups",
    "ec2:DescribeSubnets",
    "ec2:DescribeVpcEndpoints",
    "ec2:DescribeVpcEndpointServices",
    "ec2:DescribeVpcs",
    "ecr:BatchCheckLayerAvailability",
    "ecr:BatchGetImage",
    "ecr:CreateRepository",
    "ecr:Describe*",
    "ecr:GetAuthorizationToken",
    "ecr:GetDownloadUrlForLayer",
    "ecr:SetRepositoryPolicy",
    "ecr:CompleteLayerUpload",
    "ecr:BatchDeleteImage",
    "ecr:UploadLayerPart",
    "ecr:DeleteRepositoryPolicy",
    "ecr:InitiateLayerUpload",
    "ecr:DeleteRepository",
    "ecr:PutImage",
    "ecr:StartImageScan",
    "ecr:TagResource",
    "ecr:UntagResource",
    "elastic-inference:Connect",
    "elasticfilesystem:DescribeFileSystems",
    "elasticfilesystem:DescribeMountTargets",
    "elasticmapreduce:DescribeCluster",
    "elasticmapreduce:ListInstanceGroups",
    "elasticmapreduce:ListClusters",
    "events:PutRule",
    "events:DescribeRule",
    "events:PutTargets",
    "events:TagResource",
```

```
    "events:ListTagsForResource",
    "fsx:DescribeFileSystems",
    "glue:SearchTables",
    "glue:NotifyEvent",
    "glue:StartBlueprintRun",
    "glue:PutWorkflowRunProperties",
    "glue:StopCrawler",
    "glue:DeleteJob",
    "glue:DeleteWorkflow",
    "glue:UpdateCrawler",
    "glue:DeleteBlueprint",
    "glue:UpdateWorkflow",
    "glue:StartCrawler",
    "glue:ResetJobBookmark",
    "glue:UpdateJob",
    "glue:StartWorkflowRun",
    "glue:StopCrawlerSchedule",
    "glue:ResumeWorkflowRun",
    "glue:DeleteCrawler",
    "glue:UpdateBlueprint",
    "glue:BatchStopJobRun",
    "glue:StopWorkflowRun",
    "glue:BatchGet*",
    "glue:UpdateCrawlerSchedule",
    "glue:DeleteConnection",
    "glue:UpdateConnection",
    "glue:Get*",
    "glue:BatchDeleteConnection",
    "glue:StartCrawlerSchedule",
    "glue:StartJobRun",
    "glue:CreateWorkflow",
    "glue:*DataQuality*",
    "glue:List*",
    "glue:CreateSession",
    "glue:RunStatement",
    "glue:BatchCreatePartition",
    "glue:CreateDatabase",
    "glue:CreatePartitionIndex",
    "glue:CreateTable",
    "glue:BatchUpdatePartition",
    "glue:BatchDeletePartition",
    "glue:UpdateTable",
    "glue:DeleteTableVersion",
    "glue:DeleteTable",
```

```
    "glue:DeleteColumnStatisticsForPartition",
    "glue:DeleteColumnStatisticsForTable",
    "glue:DeletePartitionIndex",
    "glue:UpdateColumnStatisticsForPartition",
    "glue:UpdateColumnStatisticsForTable",
    "glue:BatchDeleteTableVersion",
    "glue:BatchDeleteTable",
    "glue:CreatePartition",
    "glue:DeletePartition",
    "glue:UpdatePartition",
    "glue:CreateBlueprint",
    "glue:CreateJob",
    "glue:CreateConnection",
    "glue:CreateCrawler",
    "groundtruthlabeling:*",
    "iam:CreateServiceLinkedRole",
    "iam:GetRole",
    "iam:ListRoles",
    "iam:PassRole",
    "kms:DescribeKey",
    "kms:ListAliases",
    "kms:Decrypt",
    "kms:ListKeys",
    "kms:Encrypt",
    "kms:GenerateDataKey",
    "kms:RetireGrant",
    "lakeformation:GetDataAccess",
    "lambda:ListFunctions",
    "lambda:InvokeFunction",
    "logs:CreateLogDelivery",
    "logs:CreateLogGroup",
    "logs:CreateLogStream",
    "logs:DeleteLogDelivery",
    "logs:Describe*",
    "logs:GetLogDelivery",
    "logs:GetLogEvents",
    "logs:ListLogDeliveries",
    "logs:PutLogEvents",
    "logs:UpdateLogDelivery",
    "ram:AcceptResourceShareInvitation",
    "rds:DescribeDBInstances",
    "redshift:CreateClusterUser",
    "redshift:GetClusterCredentials",
    "redshift:GetClusterCredentialsWithIAM",
```

```
    "redshift:DescribeClusters",
    "redshift-data:BatchExecuteStatement",
    "redshift-data:CancelStatement",
    "redshift-data:DescribeStatement",
    "redshift-data:DescribeTable",
    "redshift-data:ExecuteStatement",
    "redshift-data:GetStatementResult",
    "redshift-data:ListSchemas",
    "redshift-data:ListTables",
    "redshift-serverless:ListNamespaces",
    "redshift-serverless:ListWorkgroups",
    "redshift-serverless:GetNamespace",
    "redshift-serverless:GetWorkgroup",
    "redshift-serverless:GetCredentials",
    "s3:GetBucketAcl",
    "s3:PutObjectAcl",
    "s3:GetObject",
    "s3:PutObject",
    "s3:DeleteObject",
    "s3:AbortMultipartUpload",
    "s3:CreateBucket",
    "s3:GetBucketLocation",
    "s3:ListBucket",
    "s3:ListAllMyBuckets",
    "s3:GetBucketCors",
    "s3:PutBucketCors",
    "s3:DeleteObjectVersion",
    "s3:PutObjectRetention",
    "s3:ReplicateObject",
    "s3:RestoreObject",
    "secretsmanager:ListSecrets",
    "secretsmanager:DescribeSecret",
    "secretsmanager:GetSecretValue",
    "secretsmanager:CreateSecret",
    "secretsmanager:PutResourcePolicy",
    "secretsmanager:TagResource",
    "servicecatalog:Describe*",
    "servicecatalog:List*",
    "servicecatalog:ScanProvisionedProducts",
    "servicecatalog:SearchProducts",
    "servicecatalog:SearchProvisionedProducts",
    "servicecatalog:ProvisionProduct",
    "servicecatalog:TerminateProvisionedProduct",
    "servicecatalog:UpdateProvisionedProduct",
```

```
    "sns:ListTopics",
    "sns:Subscribe",
    "sns:CreateTopic",
    "sns:Publish",
    "states:DescribeExecution",
    "states:GetExecutionHistory",
    "states:StartExecution",
    "states:StopExecution",
    "states:UpdateStateMachine",
    "tag:GetResources",
    "sso:CreateApplicationAssignment",
    "sso:AssociateProfile"
   ],
   "Resource": "*"
  }
 ]
}
```

AWS 관리형 정책에 대한 Amazon DataZone 업데이트

이 서비스가 이러한 변경 사항을 추적하기 시작한 DataZone 이후 Amazon의 AWS 관리형 정책 업데이트에 대한 세부 정보를 봅니다. 이 페이지의 변경 사항에 대한 자동 알림을 받으려면 Amazon DataZone 문서 기록 페이지에서 RSS 피드를 구독하세요.

변경 사항	설명	날짜
AmazonDataZoneDomainExecutionRolePolicy 및 AmazonDataZoneFullUserAccess - 정책 업데이트	정책이 AmazonDataZoneDomainExecutionRolePolicy 및 AmazonDataZoneFullUserAccess-로 업데이트APIs되어 Amazon DataZone 도메인 유닛 및 데이터 제품을 생성하고 관리하는 데 사용되는 새 에 대한 지원을 활성화합니다.	2024년 7월 31일
		2024년 7월 2일

변경 사항	설명	날짜
AmazonDataZoneGlue ManageAccessRolePolicy - 정책 업데이트	에 대한 정책 업데이트 AmazonDataZoneGlue ManageAccessRolePolicy - Amazon DataZone 은 Lake Formation에서 IAM 권한 부여 범위를 줄이기 위해 세분화된 액세스 제어 기능에 사용되는 권한을 추가하고 있습니다.	
AmazonDataZoneExecutionRolePolicy 및 AmazonDataZoneFullUserAccess - 정책 업데이트	데이터 계보 및 세분화된 액세스 제어에 대한 지원을 활성화하기 AmazonDataZoneFullUserAccess 위해 AmazonDataZoneExecutionRolePolicy 및로 정책 업데이트APIs.	2024년 6월 27일
AmazonDataZoneGlue ManageAccessRolePolicy - 정책 업데이트	레이크 형성에서 부여AmazonDataZoneGlue ManageAccessRolePolicy 되는 IAM 권한의 범위를 줄이기 DataZone 위해 Amazon의 자체 구독 기능에 필요한 권한을 추가하는 에 대한 정책 업데이트입니다. 자체 구독 기능을 사용하면 태그가 지정된 리소스e에만 레이크 형성 권한을 부여할 수 있습니다.	2024년 6월 14일

변경 사항	설명	날짜
AmazonDataZoneDomainExecutionRolePolicy - 정책 업데이트	사용자가 Amazon DataZone 환경에 대한 작업을 구성할 수 DataZone 있도록 AmazonAPIs에 새 를 AmazonDataZoneDomainExecutionRolePolicy 추가하는 에 대한 정책 업데이트입니다.	2024년 6월 14일
AmazonDataZoneFullAccess - 정책 업데이트	Amazon DataZone 관리 콘솔이 사용자를 대신하여 도메인 태그와 프로젝트 태그를 모두 사용하여 보안 암호를 생성할 수 AmazonDataZoneFullAccess 있도록 하는 에 대한 정책 업데이트입니다. 또한 도메인 소유자 계정의 관리를 활성화하여 연결된 계정의 계정 연결 상태를 볼 수 있는 `ram:ListResourceSharePermissions` 작업도 포함됩니다.	2024년 6월 14일

변경 사항	설명	날짜
AmazonDataZoneSageMakerEnvironmentRolePermissionsBoundary - 새 권한 경계	라는 새 권한 경계입니다AmazonDataZoneSageMakerEnvironmentRolePermissionsBoundary . Amazon DataZone 데이터 포털을 통해 Amazon SageMaker 환경을 생성할 때 Amazon 은 환경 생성 중에 생성되는 IAM 역할에 이 권한 경계를 DataZone 적용합니다. 권한 경계는 Amazon이 DataZone 생성하는 역할의 범위와 추가하는 모든 역할을 제한합니다.	2024년 4월 30일
AmazonDataZoneSageMakerAccess - 새 정책	라는 새 정책은 Amazon SageMaker 자산을 카탈로그에 게시할 수 있는 DataZone 권한을 Amazon에 AmazonDataZoneSageMakerAccess 부여합니다. 또한 카탈로그에 SageMaker 게시된 Amazon DataZone 자산에 대한 액세스 권한을 부여하거나 취소할 수 있는 권한을 Amazon에 부여합니다.	2024년 4월 30일

변경 사항	설명	날짜
AmazonDataZoneFullAccess - 정책 업데이트	콘솔에서 청사진을 구성하는 계정 관리자의 사용성을 개선하기 위한 `DescribeSecurityGroups` 작업과 지정된 관리AmazonDataZoneFullAccess형 정책에 대한 정보를 검색하는 데 도움이 되는 `GetPolicy` 작업에 대한 액세스를 추가하는 정책 업데이트입니다.	2024년 4월 30일
AmazonDataZoneSageMakerProvisioning - 새 정책	라는 새 정책은 Amazon DataZone 와 상호 운용하는 데 필요한 권한을 Amazon 에 AmazonDataZoneSageMakerProvisioning 부여합니다 SageMaker.	2024년 4월 30일
AmazonDataZoneS3Manage-<region>-<domainId> - 새 역할	Amazon이 AWS Lake Formation을 DataZone 호출하여 Amazon Simple Storage Service(Amazon S3AmazonDataZone3) 위치를 등록할 때 사용되는 S3Manage-<region>-<domainId>라는 새 역할입니다. AWS Lake Formation은 해당 위치의 데이터에 액세스할 때 이 역할을 맡습니다.	2024년 4월 1일

변경 사항	설명	날짜
AmazonDataZoneGlueManageAccessRolePolicy - 정책 업데이트	AmazonAmazonDataZoneGlueManageAccessRolePolicy이 데이터에 대한 권한 부여를 게시하고 액세스할 수 있도록 허용하는 권한에 대한 지원을 활성화 DataZone 하도록 가 업데이트되었습니다.	2024년 4월 1일
AmazonDataZoneDomainExecutionRolePolicy 및 AmazonDataZoneFullUserAccess - 정책 업데이트	AmazonDataZoneDomainExecutionRolePolicy 및 를 업데이트AmazonDataZoneFullUserAccess하여 `CancelMetadataGenerationRun` 에 대한 지원을 활성화했습니다API.	2024년 3월 29일
AmazonDataZoneFullAccess - 정책 업데이트	사용자가 Amazon DataZone 관리 콘솔에서 암호, 클러스터, vpc 및 서브넷을 텍스트 상자에 입력하지 않고 선택할 수 `AmazonDataZoneFullAccess` 있도록 가 업데이트되었습니다.	2024년 3월 13일

변경 사항	설명	날짜
AmazonDataZoneDomainExecutionRolePolicy - 정책 업데이트	어떤 블루프린트가 어떤 계정 및 리전에서 활성화`ListEnvironmentBlueprintConfigurationSummaries` API되었는지 식별하여 환경 프로파일을 생성하는 데 필요한 에 대한 지원을 활성화AmazonDataZoneDomainExecutionRolePolicy하도록 가 업데이트되었습니다.	2024년 2월 1일
AmazonDataZoneGlueManageAccessRolePolicy - 정책 업데이트	AWS Lake Formation 하이브리드 모드에 대한 지원을 활성화AmazonDataZoneGlueManageAccessRolePolicy하도록 를 업데이트했습니다.	2023년 12월 14일
AmazonDataZoneFullUserAccess 및 AmazonDataZoneDomainExecutionRolePolicy - 정책 업데이트	Amazon 에서 생성형 AI 기반 데이터 설명 기능을 지원하도록 AmazonDataZoneFullUserAccess 및 AmazonDataZoneDomainExecutionRolePolicy 정책을 업데이트했습니다 DataZone.	2023년 11월 28일

변경 사항	설명	날짜
AmazonDataZoneEnvironmentRolePermissionsBoundary - 정책 업데이트	Amazon은 관리AmazonDataZoneEnvironmentRolePermissionsBoundary형 정책을 업데이트 DataZone 했으며, 이 정책은 `ResourceTag` 조건에 따라 범위가 축소된 추가 `athena:GetQueryResultsStream` 권한으로 구성됩니다.	2023년 11월 17일
AmazonDataZoneRedshiftManageAccessRolePolicy - 정책 업데이트	Amazon은 `redshift:AssociateDataShareConsumer` 작업에 대한 조직 ID 확인을 AmazonDataZoneRedshiftManageAccessRolePolicy 제거하여를 DataZone 업데이트했습니다. 이를 통해 조직 간에 AWS 리소스를 공유할 수 있습니다.	2023년 11월 16일
AmazonDataZoneFullUserAccess - 정책 업데이트	Amazon은 Amazon 에 대한 전체 액세스 권한을 부여하는 AmazonDataZoneFullUserAccess 정책을 DataZone 업데이트 DataZone했지만 도메인, 사용자 또는 관련 계정의 관리를 허용하지 않습니다.	2023년 10월 2일
AmazonDataZonePortalFullAccessPolicy - 정책 사용 중단	Amazon은 를 DataZone 더 이상 사용하지 않았습니다AmazonDataZonePortalFullAccessPolicy.	2023년 9월 29일

변경 사항	설명	날짜
AmazonDataZonePreviewConsoleFullAccess - 정책 사용 중단	Amazon은 를 DataZone 더 이상 사용하지 않았습니다AmazonDataZonePreviewConsoleFullAccess.	2023년 9월 29일
AmazonDataZoneDomainExecutionRolePolicy - 새 정책	Amazon은 라는 새 정책을 DataZone 추가했습니다AmazonDataZoneDomainExecutionRolePolicy. 이는 Amazon DataZone `AmazonDataZoneDomainExecutionRole` 서비스 역할의 기본 정책입니다. 이 역할은 Amazon DataZone 도메인의 데이터를 카탈로그화, 검색, 관리, 공유 및 분석하는 DataZone 데 사용됩니다. `AmazonDataZoneDomainExecutionRolePolicy` 정책을 에 연결할 수 있습니다`AmazonDataZoneDomainExecutionRole` .	2023년 9월 25일
AmazonDataZoneCrossAccountAdmin - 새 정책	Amazon은 사용자가 Amazon DataZone 및 관련 계정에서 작업할 수 AmazonDataZoneCrossAccountAdmin 있도록 라는 새 정책을 DataZone 추가했습니다.	2023년 9월 19일

변경 사항	설명	날짜
AmazonDataZoneFull UserAccess - 새 정책	Amazon은 Amazon 에 대한 전체 액세스 권한을 AmazonDataZoneFullUserAccess 부여하는 라는 새 정책을 DataZone 추가 DataZone했지만 도메인, 사용자 또는 관련 계정의 관리를 허용하지 않습니다.	2023년 9월 12일
AmazonDataZoneRedshiftManageAccessRolePolicy - 새 정책	Amazon은 AmazonAmazonDataZoneRedshiftManageAccessRolePolicy이 데이터에 대한 권한 부여를 DataZone 게시하고 액세스할 수 있는 권한을 부여하는 새로운 정책을 DataZone 추가했습니다.	2023년 9월 12일
AmazonDataZoneGlueManageAccessRolePolicy - 새 정책	Amazon은 카탈로그에 AWS Glue 데이터를 게시할 수 AmazonDataZoneGlueManageAccessRolePolicy 있는 DataZone 권한을 Amazon 에 부여하는 라는 새 정책을 DataZone 추가했습니다. 또한 Amazon에 카탈로그에 게시된 AWS Glue 자산에 대한 액세스 권한을 부여하거나 취소할 수 있는 DataZone 권한을 부여합니다.	2023년 9월 12일

변경 사항	설명	날짜
AmazonDataZoneRedshiftGlueProvisioningPolicy - 새 정책	Amazon은 지원되는 데이터 소스와 상호 운용AmazonDataZoneRedshiftGlueProvisioningPolicy하는 데 필요한 DataZone 권한을 Amazon 에 부여하는 라는 새 정책을 DataZone 추가했습니다.	2023년 9월 12일
AmazonDataZoneEnvironmentRolePermissionsBoundary - 새 정책	Amazon은 연결된 프로비저닝된 IAM 보안 주체를 제한AmazonDataZoneEnvironmentRolePermissionsBoundary하는 라는 새 정책을 DataZone 추가했습니다.	2023년 9월 12일
AmazonDataZoneFullAccess - 새 정책	Amazon은 AWS 관리 콘솔을 DataZone 통해 Amazon에 대한 전체 액세스를 AmazonDataZoneFullAccess 제공하는 라는 새 정책을 DataZone 추가했습니다.	2023년 9월 12일
관리형 정책 업데이트	추가 `iam:GetPolicy` 권한으로 구성된 AmazonDataZonePreviewConsoleFullAccess 관리형 정책에 대한 업데이트입니다.	2023년 6월 13일
Amazon에서 변경 사항 추적 DataZone 시작	Amazon은 AWS 관리형 정책에 대한 변경 사항을 추적하기 DataZone 시작했습니다.	2023년 3월 20일

IAM Amazon의 역할 DataZone

주제

- AmazonDataZoneProvisioningRole-<domainAccountId>
- AmazonDataZoneDomainExecutionRole
- AmazonDataZoneGlueAccess-<region>-<domainId>
- AmazonDataZoneRedshiftAccess-<region>-<domainId>
- AmazonDataZoneS3Manage -<region>-<domainId>
- AmazonDataZoneSageMakerManageAccessRole-<region>-<domainId>
- AmazonDataZoneSageMakerProvisioningRole-<domainAccountId>

AmazonDataZoneProvisioningRole-<domainAccountId>

`AmazonDataZoneProvisioningRole-<domainAccountId>` 에는 이 `AmazonDataZoneRedshiftGlueProvisioningPolicy` 연결되어 있습니다. 이 역할은 AWS Glue 및 Amazon Redshift와 상호 운용하는 데 필요한 DataZone 권한을 Amazon에 부여합니다.

기본값에는 다음과 같은 신뢰 정책`AmazonDataZoneProvisioningRole-<domainAccountId>`이 연결되어 있습니다.

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

AmazonDataZoneDomainExecutionRole

에는 AWS 관리형 정책AmazonDataZoneDomainExecutionRole이 AmazonDataZoneDomainExecutionRolePolicy 연결되어 있습니다. Amazon은 사용자를 대신하여 이 역할을 DataZone 생성합니다. 데이터 포털의 특정 작업의 경우 Amazon은 역할이 생성된 계정에서 이 역할을 DataZone 수임하고 이 역할이 작업을 수행할 권한이 있는지 확인합니다.

AmazonDataZoneDomainExecutionRole 역할은 Amazon DataZone 도메인을 호스팅 AWS 계정 하는 에 필요합니다. 이 역할은 Amazon DataZone 도메인을 생성할 때 자동으로 생성됩니다.

기본 AmazonDataZoneDomainExecutionRole 역할에는 다음과 같은 신뢰 정책이 있습니다.

```
{
    "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> 역할에는 이 AmazonDataZoneGlueManageAccessRolePolicy 연결되어 있습니다. 이 역할은 카탈로그에 AWS Glue 데이터를 게시할 수 있는 DataZone 권한을 Amazon에 부여합니다. 또한 Amazon에 카탈로그에 게시된 AWS Glue 자산에 대한 액세스 권한을 부여하거나 취소할 수 있는 DataZone 권한을 부여합니다.

기본 AmazonDataZoneGlueAccess-<region>-<domainId> 역할에는 다음과 같은 신뢰 정책이 연결되어 있습니다.

```
{
  "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> 역할에는 이 AmazonDataZoneRedshiftManageAccessRolePolicy 연결되어 있습니다. 이 역할은 Amazon Redshift 데이터를 카탈로그에 게시할 수 있는 DataZone 권한을 Amazon에 부여합니다. 또한 카탈로

그의 Amazon Redshift 또는 Amazon Redshift Serverless 게시 자산에 대한 액세스 권한을 부여하거나 취소할 수 있는 DataZone 권한을 Amazon에 부여합니다.

기본 AmazonDataZoneRedshiftAccess-<region>-<domainId> 역할에는 다음과 같은 인라인 권한 정책이 연결되어 있습니다.

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Sid": "RedshiftSecretStatement",
         "Effect":"Allow",
         "Action":"secretsmanager:GetSecretValue",
         "Resource":"*",
         "Condition":{
            "StringEquals":{
               "secretsmanager:ResourceTag/AmazonDataZoneDomain":"{{domainId}}"
            }
         }
      }
   ]
}
```

기본값에는 다음과 같은 신뢰 정책AmazonDataZoneRedshiftManageAccessRole<timestamp>이 연결되어 있습니다.

```
{
  "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>은 Amazon DataZone이 AWS Lake Formation을 호출하여 Amazon Simple Storage Service(Amazon S3) 위치를 등록할 때 사용됩니다. AWS Lake Formation은 해당 위치의 데이터에 액세스할 때 이 역할을 맡습니다. 자세한 내용은 위치 등록에 사용되는 역할 요구 사항 섹션을 참조하세요.

이 역할에는 다음과 같은 인라인 권한 정책이 연결되어 있습니다.

```
{
    "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>에는 다음과 같은 신뢰 정책이 연결되어 있습니다.

```
{
    "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` 역할에는 `AmazonDataZoneSageMakerAccess`, 및 가 `AmazonDataZoneGlueManageAccessRolePolicy` 연결되어 `AmazonDataZoneRedshiftManageAccessRolePolicy`있습니다. 이 역할은 Amazon에

데이터 레이크, 데이터 웨어하우스 및 Amazon Sagemaker 자산에 대한 구독을 게시하고 관리할 수 있는 DataZone 권한을 부여합니다.

AmazonDataZoneSageMakerManageAccessRole 역할에는 다음과 같은 인라인 정책이 연결되어 있습니다.

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Sid": "RedshiftSecretStatement",
         "Effect":"Allow",
         "Action":"secretsmanager:GetSecretValue",
         "Resource":"*",
         "Condition":{
            "StringEquals":{
               "secretsmanager:ResourceTag/AmazonDataZoneDomain":"{{domainId}}"
            }
         }
      }
   ]
}
```

AmazonDataZoneSageMakerManageAccessRole 역할에는 다음과 같은 신뢰 정책이 연결되어 있습니다.

```
{
  "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 역할에는 AmazonDataZoneSageMakerProvisioning 및 가 AmazonDataZoneRedshiftGlueProvisioningPolicy 연결되어 있습니다. 이 역할은 AWS Glue, Amazon Redshift 및 Amazon Sagemaker와 상호 운용하는 데 필요한 DataZone 권한을 Amazon 에 부여합니다.

AmazonDataZoneSageMakerProvisioningRole 역할에는 다음과 같은 인라인 정책이 연결되어 있습니다.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "SageMakerStudioTagOnCreate",
            "Effect": "Allow",
            "Action": [
                "sagemaker:AddTags"
            ],
            "Resource": "arn:aws:sagemaker:*:{{AccountId}}:*/*",
            "Condition": {
                "Null": {
                    "sagemaker:TaggingAction": "false"
                }
            }
        }
    ]
}
```

AmazonDataZoneSageMakerProvisioningRole 역할에는 다음과 같은 신뢰 정책이 연결되어 있습니다.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "DataZoneTrustPolicyStatement",
      "Effect": "Allow",
      "Principal": {
        "Service": "datazone.amazonaws.com"
      },
      "Action": "sts:AssumeRole",
      "Condition": {
        "StringEquals": {
            "aws:SourceAccount": "{{domain_account}}"
        }
      }
    }
  ]
}
```

임시 자격 증명

임시 자격 증명을 사용하여 로그인할 때 일부 AWS 서비스가 작동하지 않습니다. 임시 자격 증명으로 작동하는 AWS 서비스를 비롯한 자세한 내용은 IAM 사용 설명서의 에서 AWS 로 작동하는 서비스를 IAM 참조하세요.

사용자 이름과 암호를 제외한 방법을 AWS Management Console 사용하여 에 로그인하는 경우 임시 보안 인증 정보를 사용합니다. 예를 들어 회사의 Single Sign-On(SSO) 링크를 AWS 사용하여 에 액세스하면 해당 프로세스가 임시 자격 증명을 자동으로 생성합니다. 또한 콘솔에 사용자로 로그인한 다음 역할을 전환할 때 임시 보안 인증을 자동으로 생성합니다. 역할 전환에 대한 자세한 내용은 IAM 사용 설명서의 역할(콘솔)로 전환을 참조하세요.

AWS CLI 또는 를 사용하여 임시 자격 증명을 수동으로 생성할 수 있습니다 AWS API. 그런 다음 이러한 임시 자격 증명을 사용하여 장기 액세스 키를 사용하는 대신 임시 자격 증명을 동적으로 생성하는

AWS. AWS recommends에 액세스할 수 있습니다. 자세한 내용은 의 임시 보안 자격 증명을 IAM참조하세요.

보안 주체 권한

IAM 사용자 또는 역할을 사용하여 에서 작업을 수행하는 경우 보안 주체로 AWS간주됩니다. 정책은 보안 주체에게 권한을 부여합니다. 일부 서비스를 사용할 때는 다른 서비스에서 다른 작업을 트리거하는 작업을 수행할 수 있습니다. 이 경우 두 작업을 모두 수행할 수 있는 권한이 있어야 합니다. 작업에 정책에서 추가 종속 작업이 필요한지 여부를 확인하려면 서비스 승인 참조의 AWS 문서 Essentials에 대한 작업, 리소스 및 조건 키를 참조하세요.

Amazon에 대한 규정 준수 검증 DataZone

AWS 서비스 가 특정 규정 준수 프로그램의 범위 내에 있는지 알아보려면 AWS 서비스 규정 준수 프로그램 범위 참조하고 관심 있는 규정 준수 프로그램을 선택합니다. 일반 정보는 AWS 규정 준수 프로그램 참조하세요.

를 사용하여 타사 감사 보고서를 다운로드할 수 있습니다 AWS Artifact. 자세한 내용은 의 보고서 다운로드 AWS Artifact.

를 사용할 때의 규정 준수 책임은 데이터의 민감도, 회사의 규정 준수 목표 및 관련 법률 및 규정에 따라 AWS 서비스 결정됩니다. 는 규정 준수를 돕기 위해 다음 리소스를 AWS 제공합니다.

- 보안 및 규정 준수 빠른 시작 안내서 - 이 배포 안내서에서는 아키텍처 고려 사항에 대해 설명하고 보안 및 규정 준수에 중점을 둔 에 기준 환경을 배포 AWS 하기 위한 단계를 제공합니다.
- Amazon Web Services의 HIPAA 보안 및 규정 준수를 위한 아키텍처 - 이 백서에서는 기업이 HIPAA를 사용하여 적격 애플리케이션을 AWS 생성하는 방법을 설명합니다.

> **Note**
>
> 모두 HIPAA 적합한 AWS 서비스 것은 아닙니다. 자세한 내용은 HIPAA 적격 서비스 참조를 참조하세요.

- AWS 규정 준수 리소스 - 이 워크북 및 가이드 모음은 해당 산업 및 위치에 적용될 수 있습니다.
- AWS 고객 규정 준수 가이드 - 규정 준수의 관점에서 공동 책임 모델을 이해합니다. 이 가이드는 여러 프레임워크(미국 국립표준기술연구소(), 결제카드 산업보안표준위원회(NIST), PCI국제표준화기구(ISO) 포함)의 보안 제어에 대한 지침을 보호하고 AWS 서비스 매핑하는 모범 사례를 요약합니다.

- AWS Config 개발자 안내서의 규칙을 사용하여 리소스 평가 - 이 AWS Config 서비스는 리소스 구성이 내부 관행, 업계 지침 및 규정을 얼마나 잘 준수하는지 평가합니다.
- AWS Security Hub - AWS 서비스 에서 보안 상태를 포괄적으로 볼 수 있습니다 AWS. Security Hub 는 보안 제어를 사용하여 AWS 리소스를 평가하고 보안 업계 표준 및 모범 사례에 대한 규정 준수를 확인합니다. 지원되는 서비스 및 제어 목록은 Security Hub 제어 참조를 참조하세요.
- Amazon GuardDuty - 의심스러운 활동 및 악의적인 활동이 있는지 환경을 모니터링하여 AWS 계정, 워크로드, 컨테이너 및 데이터에 대한 잠재적 위협을 AWS 서비스 탐지합니다. 는 특정 규정 준수 프레임워크에서 요구하는 침입 탐지 요구 사항을 충족DSS하여 PCI 와 같은 다양한 규정 준수 요구 사항을 해결하는 데 도움이 될 GuardDuty 수 있습니다.
- AWS Audit Manager - 이를 AWS 서비스 통해 AWS 사용량을 지속적으로 감사하여 위험 및 규정 및 업계 표준 준수를 관리하는 방법을 간소화할 수 있습니다.

Amazon의 보안 모범 사례 DataZone

Amazon DataZone 은 자체 보안 정책을 개발하고 구현할 때 고려해야 할 여러 보안 기능을 제공합니다. 다음 모범 사례는 일반적인 지침이며 완벽한 보안 솔루션을 나타내지는 않습니다. 이러한 모범 사례는 환경에 적절하지 않거나 충분하지 않을 수 있으므로 참고용으로만 사용해 주세요.

최소 권한 액세스 구현

권한을 부여할 때 누가 어떤 Amazon DataZone 리소스에 대한 권한을 얻는지 결정합니다. 해당 리소스에서 허용할 작업을 사용 설정합니다. 따라서 작업을 수행하는 데 필요한 권한만 부여해야 합니다. 최소 권한 액세스를 구현하는 것이 오류 또는 악의적인 의도로 인해 발생할 수 있는 보안 위험과 영향을 최소화할 수 있는 근본적인 방법입니다.

IAM 역할 사용

Amazon DataZone 리소스에 액세스하려면 프로듀서 및 클라이언트 애플리케이션에 유효한 보안 인증 정보가 있어야 합니다. 보안 AWS 인증 정보를 클라이언트 애플리케이션 또는 Amazon S3 버킷에 직접 저장해서는 안 됩니다. 이러한 보안 인증은 자동으로 교체되지 않으며 손상된 경우 비즈니스에 큰 영향을 줄 수 있는 장기 보안 인증입니다.

대신 IAM 역할을 사용하여 생산자와 클라이언트 애플리케이션이 Amazon DataZone 리소스에 액세스할 수 있는 임시 보안 인증을 관리해야 합니다. 역할을 사용하면 장기 자격 증명(예: 사용자 이름과 암호 또는 액세스 키)을 사용하여 다른 리소스에 액세스할 필요가 없습니다.

자세한 내용은 IAM 사용 설명서의 다음 주제를 참조하세요.

- IAM 역할
- 역할에 대한 일반적인 시나리오: 사용자, 애플리케이션 및 서비스

종속 리소스에서 서버 측 암호화 구현

저장 데이터 및 전송 중인 데이터는 Amazon 에서 암호화할 수 있습니다 DataZone.

CloudTrail 를 사용하여 API 통화 모니터링

Amazon DataZone 은 Amazon 에서 사용자 AWS CloudTrail, 역할 또는 서비스가 수행한 작업의 레코드를 제공하는 AWS 서비스인 와 통합됩니다 DataZone.

에서 수집한 정보를 사용하여 Amazon 에 수행된 요청 CloudTrail, 요청이 수행된 DataZoneIP 주소, 요청을 수행한 사람, 요청이 수행된 시간 및 추가 세부 정보를 확인할 수 있습니다.

Amazon의 복원력 DataZone

AWS 글로벌 인프라는 AWS 리전 및 가용 영역을 기반으로 구축됩니다. 는 지연 시간이 짧고 처리량이 높으며 중복성이 높은 네트워킹과 연결된 물리적으로 분리되고 격리된 여러 가용 영역을 AWS 리전 제공합니다. 가용 영역을 사용하면 중단 없이 영역 간에 자동으로 장애 극복 조치가 이루어지는 애플리케이션 및 데이터베이스를 설계하고 운영할 수 있습니다. 가용 영역은 기존의 단일 또는 다중 데이터 센터 인프라보다 가용성, 내결함성, 확장성이 뛰어납니다.

AWS 리전 및 가용 영역에 대한 자세한 내용은 AWS 글로벌 인프라 섹션을 참조하세요.

AWS 글로벌 인프라 외에도 Amazon DataZone 은 데이터 복원력 및 백업 요구 사항을 지원하는 데 도움이 되는 몇 가지 기능을 제공합니다.

주제

- 데이터 소스 복원력
- 자산 복원력
- 자산 유형 및 메타데이터 형식 복원력
- 용어 복원력
- 글로벌 검색 복원력
- 구독 복원력
- 환경 복원력

- 환경 청사진 복원력
- 프로젝트 복원력
- RAM 복원력
- 사용자 프로필 관리 복원력
- 도메인 복원력

데이터 소스 복원력

Amazon DataZone 가용성 이벤트 중에 `DataSource` 작업은 최대 24시간 동안 주기적으로 재시도합니다. 잘못된 구성으로 인해 작업이 실패하면 `DataSourceRunFailed` 이벤트가 발생합니다. Amazon DataZone 도메인이 KMS 키로 구성되어 있고 작업 실행 중에 에서 이 키에 대한 액세스 권한을 AmazonDataZoneDomainExecutionRole 잃으면 실행이 `INACCESSIBLE` 상태에서 종료됩니다. KMS 액세스가 복원되면 작업을 수동으로 업데이트하여 사용 가능한 상태로 전환을 다시 트리거해야 합니다.

자산 복원력

Amazon 에서는 DataZone자산의 버전이 지정됩니다. 자산의 버전을 롤백해야 하는 경우 마지막으로 안정적인 버전의 콘텐츠를 사용하여 새 버전을 생성할 수 있습니다. 자산 버전을 게시할 수 있습니다. 새 버전을 게시하는 경우를 제외하고 자산의 게시된 버전을 편집할 수 없습니다. 게시된 자산(일명 목록)을 구독할 수 있습니다. 자산에 대한 새 구독을 방지하기 위해 자산을 게시 취소할 수 있습니다. 자산을 게시 취소해도 기존 구독에는 영향을 미치지 않습니다. 자산을 삭제하면 자산의 게시되지 않은 모든 버전이 삭제됩니다. 자산의 게시된 버전은 별도로 삭제해야 합니다. 자산의 게시된 버전은 구독이 없는 경우에만 삭제할 수 있습니다.

자산 유형 및 메타데이터 형식 복원력

Amazon 에서는 DataZone자산 유형 및 메타데이터 양식 유형이 버전 관리됩니다. 자산에서 사용 중인 자산 유형은 삭제할 수 없습니다. 메타데이터 양식 유형은 자산 유형 또는 자산에서 사용 중인 경우 삭제할 수 없습니다. 큐레이션에 특정 metadata-form-type 을 사용하지 않으려면 이미 연결된 에 영향을 주지 않는 큐레이션을 비활성화할 수 있습니다.

용어 복원력

Amazon 에서 DataZone용어집 및 용어집 용어는 사용 중인 경우 삭제할 수 없습니다. 특정 용어집 또는 용어집 용어를 큐레이션에 사용하지 않으려면 이미 연결된 용어집에 영향을 주지 않는 용어집을 비활성화할 수 있습니다.

글로벌 검색 복원력

Amazon 에서는 글로벌 검색을 통해 DataZone게시된 자산(일명 목록)을 검색할 수 있습니다. 자산 게시는 자산을 게시 취소하여 롤백할 수 있습니다. 자산을 게시 취소해도 기존 구독에는 영향을 미치지 않습니다. 게시된 자산은 해당 버전을 다시 게시하여 자산의 특정 버전으로 롤백할 수 있습니다. 이는 기존 구독에는 영향을 미치지 않습니다.

구독 복원력

Amazon 에서 DataZone subscriptionGrant 이행은 실패하기 전에 두 번의 사용 중지를 시도합니다. 실패하면 수동으로 삭제하여 다시 시도해야 합니다. Amazon이 구독에 대한 권한을 취소할 수 DataZone 없는 경우 구독을 삭제하지 못할 수 있습니다. 기본 오류를 해결하거나 `DeleteSubscriptionGrant` API 작업에 `retainPermissions` 플래그를 사용하여 권한을 취소 DataZone 하지 않고 Amazon에서 권한 부여를 강제 삭제할 수 있습니다.

Amazon DataZone 도메인이 KMS 키로 구성되어 있고 `SubscriptionGrant` 워크플로 중에 가 이 키에 대한 액세스를 `AmazonDataZoneDomainExecutionRole` 잃으면 권한 부여가 로 표시됩니다`INACCESSIBLE`. KMS 액세스가 복원되면 `INACCESSIBLE` 권한 부여를 삭제하고 다시 생성해야 합니다.

환경 복원력

Amazon DataZone 도메인이 KMS 키로 구성되어 있고 환경 워크플로 중에 에서 이 키에 대한 액세스 권한을 `AmazonDataZoneDomainExecutionRole` 잃으면 환경이 로 표시됩니다`INACCESSIBLE`. KMS 액세스가 복원되면 `INACCESSIBLE` 환경을 삭제하고 다시 생성해야 합니다. 환경 생성은 실패하기 전에 두 번의 사용 중지를 시도합니다. 실패하면 수동으로 삭제하여 다시 시도해야 합니다. 환경 워크플로가 실패하면 환경이 실패 상태로 전환됩니다. 이 시점에서는 삭제하고 다시 생성할 수만 있습니다.

환경 청사진 복원력

Amazon 에서는 기본 환경 프로파일이 있는 경우 환경 청사진 DataZone을 삭제할 수 없습니다.

프로젝트 복원력

Amazon 에서는 포함된 환경이 있는 경우 DataZone프로젝트를 삭제할 수 없습니다.

RAM 복원력

RAM 복원력 정보는 https://docs.aws.amazon.com/ram/latest/userguide/security-disaster-recovery-resiliency.html을 참조하세요.

사용자 프로필 관리 복원력

사용자 프로필 복원력 정보는 AWS Identity Center를 참조하세요.

도메인 복원력

Amazon 에서는 도메인에 프로젝트 또는 데이터 소스 DataZone가 포함된 경우 도메인을 삭제할 수 없습니다.

Amazon의 인프라 보안 DataZone

관리형 서비스인 Amazon DataZone 은 AWS 글로벌 네트워크 보안으로 보호됩니다. AWS 보안 서비스 및 인프라 AWS 보호 방법에 대한 자세한 내용은 AWS Cloud Security 섹션을 참조하세요. 인프라 보안 모범 사례를 사용하여 AWS 환경을 설계하려면 Security Pillar AWS Well-Architected Framework의 인프라 보호를 참조하세요.

AWS 게시된 API 호출을 사용하여 네트워크를 DataZone 통해 Amazon에 액세스합니다. 고객은 다음을 지원해야 합니다.

- 전송 계층 보안(TLS). TLS 1.2가 필요하며 TLS 1.3을 권장합니다.
- DHE (Ephemeral Diffie-HellmanPFS) 또는 (Elliptic Curve Ephemeral Diffie-Hellman)과 같은 완벽한 순방향 보안ECDHE()이 포함된 Cipher 제품군입니다. Java 7 이상의 최신 시스템은 대부분 이러한 모드를 지원합니다.

또한 액세스 키 ID와 IAM 보안 주체와 연결된 보안 액세스 키를 사용하여 요청에 서명해야 합니다. 또는 AWS Security Token Service(AWS STS)를 사용하여 임시 보안 인증을 생성하여 요청에 서명할 수 있습니다.

Amazon의 교차 서비스 혼동 대리자 방지 DataZone

혼동된 대리자 문제는 작업을 수행할 권한이 없는 엔터티가 권한이 더 많은 엔터티에게 작업을 수행하도록 강요할 수 있는 보안 문제입니다. 에서 서비스 AWS간 사칭은 혼동된 대리자 문제를 초래할 수 있

습니다. 교차 서비스 가장은 한 서비스(호출하는 서비스)가 다른 서비스(호출되는 서비스)를 직접적으로 호출할 때 발생할 수 있습니다. 직접적으로 호출하는 서비스는 다른 고객의 리소스에 대해 액세스 권한이 없는 방식으로 작동하게 권한을 사용하도록 조작될 수 있습니다. 이를 방지하기 위해 는 계정의 리소스에 대한 액세스 권한이 부여된 서비스 보안 주체가 있는 모든 서비스에 대한 데이터를 보호하는 데 도움이 되는 도구를 AWS 제공합니다.

리소스 정책의 aws:SourceAccount global 조건 컨텍스트 키를 사용하여 Amazon이 리소스에 다른 서비스를 DataZone 제공하는 권한을 제한하는 것이 좋습니다. 해당 계정의 리소스를 교차 서비스 사용과 연결하도록 허용SourceAccount 하려면 aws:를 사용합니다.

Amazon의 구성 및 취약성 분석 DataZone

AWS 는 게스트 운영 체제(OS) 및 데이터베이스 패치, 방화벽 구성 및 재해 복구와 같은 기본 보안 작업을 처리합니다. 적합한 제3자가 이 절차를 검토하고 인증하였습니다. 자세한 내용은 AWS 공동 책임 모델 을 참조하세요.

허용 목록에 추가할 도메인

Amazon DataZone 데이터 포털이 Amazon DataZone 서비스에 액세스하려면 데이터 포털이 서비스에 액세스하려는 네트워크의 허용 목록에 다음 도메인을 추가해야 합니다.

- `*.api.aws`
- `*.on.aws`

아마존 모니터링 DataZone

모니터링은 Amazon 및 기타 AWS 솔루션의 안정성, 가용성 및 성능을 유지하는 데 DataZone 있어 중요한 부분입니다. AWS 는 Amazon을 감시하고, 문제 발생 시 보고하고 DataZone, 적절한 경우 자동 조치를 취할 수 있는 다음과 같은 모니터링 도구를 제공합니다.

- Amazon은 실행 중인 AWS 리소스와 애플리케이션을 AWS 실시간으로 CloudWatch 모니터링합니다. 지표를 수집 및 추적하고, 사용자 지정 대시보드를 생성할 수 있으며, 지정된 지표가 지정한 임계값에 도달하면 사용자에게 알리거나 조치를 취하도록 경보를 설정할 수 있습니다. 예를 들어 Amazon EC2 인스턴스의 CPU 사용량 또는 기타 지표를 CloudWatch 추적하고 필요할 때 새 인스턴스를 자동으로 시작할 수 있습니다. 자세한 내용은 Amazon CloudWatch 사용 설명서를 참조하십시오.
- Amazon CloudWatch Logs를 사용하면 Amazon EC2 인스턴스 및 기타 소스에서 로그 파일을 모니터링 CloudTrail, 저장 및 액세스할 수 있습니다. CloudWatch 로그는 로그 파일의 정보를 모니터링하고 특정 임계값이 충족되면 알려줄 수 있습니다. 또한 매우 내구력 있는 스토리지에 로그 데이터를 저장할 수 있습니다. 자세한 내용은 Amazon CloudWatch Logs 사용 설명서를 참조하십시오.
- Amazon을 사용하면 AWS 서비스를 자동화하고 애플리케이션 가용성 문제 또는 리소스 변경과 같은 시스템 이벤트에 자동으로 대응할 EventBridge 수 있습니다. AWS 서비스에서 발생하는 이벤트는 거의 EventBridge 실시간으로 전송됩니다. 원하는 이벤트만 표시하도록 간단한 규칙을 작성한 후 규칙과 일치하는 이벤트 발생 시 실행할 자동화 작업을 지정할 수 있습니다. 자세한 내용은 Amazon EventBridge 사용 설명서를 참조하십시오.
- AWS CloudTrail계정에서 또는 AWS 계정을 대신하여 이루어진 API 호출 및 관련 이벤트를 캡처하고 지정한 Amazon S3 버킷으로 로그 파일을 전송합니다. 어떤 사용자와 계정이 전화를 걸었는지 AWS, 어떤 소스 IP 주소에서 호출이 이루어졌는지, 언제 호출이 발생했는지 식별할 수 있습니다. 자세한 내용은 AWS CloudTrail 사용 설명서를 참조하십시오.

아마존에서 아마존 DataZone 이벤트 모니터링 EventBridge

자체 애플리케이션 EventBridge, software-as-a-service (SaaS) 애플리케이션 및 AWS 서비스로부터 실시간 데이터 스트림을 제공하는 Amazon DataZone 이벤트를 모니터링할 수 있습니다. EventBridge 해당 데이터를 Amazon 심플 알림 AWS Lambda 서비스와 같은 대상으로 라우팅합니다. 이러한 이벤트는 AWS 리소스 변경을 설명하는 시스템 CloudWatch 이벤트의 스트림을 거의 실시간으로 제공하는 Amazon Events에 나타나는 이벤트와 동일합니다.

자세한 내용은 Amazon EventBridge 기본 버스를 통한 이벤트을(를) 참조하세요.

를 사용하여 Amazon DataZone API 호출을 로깅합니다. AWS CloudTrail

DataZone Amazon은 Amazon에서 사용자 AWS CloudTrail, 역할 또는 서비스가 수행한 작업의 기록을 제공하는 AWS 서비스와 통합되어 DataZone 있습니다. CloudTrail Amazon에 대한 모든 API 호출을 DataZone 이벤트로 캡처합니다. 캡처된 호출에는 Amazon DataZone 콘솔에서의 호출 및 Amazon DataZone API 작업에 대한 코드 호출이 포함됩니다. 트레일을 생성하면 Amazon 이벤트를 포함하여 Amazon S3 버킷으로 CloudTrail 이벤트를 지속적으로 전송할 수 DataZone 있습니다. 트레일을 구성하지 않아도 CloudTrail 콘솔의 이벤트 기록에서 가장 최근 이벤트를 계속 볼 수 있습니다. 에서 수집한 CloudTrail 정보를 사용하여 Amazon에 요청한 내용 DataZone, 요청한 IP 주소, 요청한 사람, 요청 시기 및 추가 세부 정보를 확인할 수 있습니다.

자세한 CloudTrail 내용은 AWS CloudTrail 사용 설명서를 참조하십시오.

아마존 DataZone 정보 입력 CloudTrail

CloudTrail 계정을 만들 AWS 계정 때 활성화됩니다. Amazon DataZone 관리 콘솔에서 활동이 발생하면 해당 활동이 CloudTrail 이벤트 기록의 다른 AWS 서비스 이벤트와 함께 이벤트에 기록됩니다. 내 사이트에서 최근 이벤트를 보고, 검색하고, 다운로드할 수 있습니다 AWS 계정. 자세한 내용은 이벤트 기록으로 CloudTrail 이벤트 보기를 참조하십시오.

DataZoneAmazon의 이벤트를 포함하여 귀하의 이벤트에 대한 지속적인 기록을 AWS 계정보려면 트레일을 생성하십시오. 트레일을 사용하면 CloudTrail Amazon S3 버킷에 로그 파일을 전송할 수 있습니다. 콘솔에서 추적을 생성하면 기본적으로 모든 AWS 리전에 추적이 적용됩니다. 트레일은 AWS 파티션에 있는 모든 지역의 이벤트를 기록하고 지정한 Amazon S3 버킷으로 로그 파일을 전송합니다. 또한 CloudTrail 로그에서 수집된 이벤트 데이터를 추가로 분석하고 이에 따라 조치를 취하도록 다른 AWS 서비스를 구성할 수 있습니다. 자세한 내용은 다음을 참조하십시오.

- 추적 생성 개요
- CloudTrail 지원되는 서비스 및 통합
- 에 대한 Amazon SNS 알림 구성 CloudTrail
- 여러 지역에서 CloudTrail 로그 파일 수신 및 여러 계정으로부터 CloudTrail 로그 파일 수신

모든 Amazon DataZone 작업은 로그에 의해 기록됩니다 CloudTrail.

Amazon 문제 해결 DataZone

Amazon DataZone에서 작업할 때 액세스가 거부된 문제 또는 유사한 문제가 발생하는 경우 이 섹션의 주제를 참조하세요.

Amazon에 대한 AWS Lake Formation 권한 문제 해결 DataZone

이 섹션에는 에서 발생할 수 있는 문제에 대한 문제 해결 지침이 포함되어 있습니다Amazon에 대한 Lake Formation 권한 구성 DataZone.

데이터 포털의 오류 메시지	해결 방법
데이터 액세스 역할을 수임할 수 없습니다.	이 오류는 Amazon DataZone 이 계정DefaultDataLakeBlueprint에서 를 활성화하는 데 사용한 AmazonDataZoneGlueDataAccessRole 를 수임할 수 없는 경우 표시됩니다. 문제를 해결하려면 데이터 자산이 있는 계정의 콘솔로 AWS IAM 이동하여 AmazonDataZoneGlueDataAccessRole가 Amazon DataZone 서비스 보안 주체와 올바른 신뢰 관계가 있는지 확인합니다. 자세한 내용은 AmazonDataZoneGlueAccess-<region>-<domainId> 단원을 참조하세요.
데이터 액세스 역할에는 구독하려는 자산의 메타데이터를 읽는 데 필요한 권한이 없습니다.	이 오류는 Amazon이 AmazonDataZoneGlueDataAccessRole 역할을 DataZone 성공적으로 수임했지만 역할에 필요한 권한이 없는 경우에 표시됩니다. 문제를 해결하려면 데이터 자산이 있는 계정의 콘솔로 AWS IAM 이동하여 역할에 AmazonDataZoneGlueManageAccessRolePolicy 연결된 이 있는지 확인합니다. 자세한 내용은 AmazonDataZoneGlueAccess-<region>-<domainId> 단원을 참조하십시오.
자산은 리소스 링크입니다. Amazon DataZone 은 리소스 링크에 대한 구독을 지원하지 않습니다.	이 오류는 Amazon에 게시하려는 자산 DataZone 이 AWS Glue 테이블에 대한 리소스 링크일 때 표시됩니다.

데이터 포털의 오류 메시지	해결 방법
자산은 AWS Lake Formation에서 관리하지 않습니다.	이 오류는 게시하려는 자산에 AWS Lake Formation 권한이 적용되지 않음을 나타냅니다. 이는 다음과 같은 경우에 발생할 수 있습니다. • 자산의 Amazon S3 위치가 AWS Lake Formation에 등록되지 않았습니다. 문제를 해결하려면 테이블이 있는 계정에서 Lake Formation 콘솔에 로그인하고 AWS Lake Formation 모드 또는 Hybrid 모드에서 Amazon S3 위치를 등록합니다 AWS . 자세한 내용을 알아보려면 Registering an Amazon S3 location(Amazon S3 위치 등록)을 참조하세요. 추가 수정이 필요한 몇 가지 시나리오가 있습니다. 여기에는 암호화된 AmazonS3 버킷 또는 교차 계정 S3 버킷과 AWS Glue 카탈로그 설정이 포함됩니다. 이러한 경우 KMS 및/또는 S3 설정을 수정해야 할 수 있습니다. 자세한 내용을 알아보려면 암호화된 Amazon S3 위치 등록을 참조하십시오. • Amazon S3 위치는 AWS Lake Formation 모드에 등록되지만 테이블의 권한에 IAMAllowedPrincipal 추가됩니다. 문제를 해결하려면 테이블의 권한IAMAllowedPrincipal에서 를 제거하거나 하이브리드 모드에서 S3 위치를 등록할 수 있습니다. 자세한 내용은 Lake Formation 권한 모델 업그레이드 정보를 참조하세요. S3 위치가 암호화되었거나 S3 위치가 Glue 테이블과 다른 accout에 있는 AWS 경우 암호화된 Amazon S3 위치 등록의 지침을 따릅니다.

데이터 포털의 오류 메시지	해결 방법
데이터 액세스 역할에는 이 자산에 대한 액세스 권한을 부여하는 데 필요한 Lake Formation 권한이 없습니다.	이 오류는 계정DefaultDataLakeBlueprint에서를 활성화AmazonDataZoneGlueDataAccessRole하는 데 사용하는 에 Amazon이 게시된 자산에 대한 권한을 관리하는 DataZone 데 필요한 권한이 없음을 나타냅니다. AWS Lake Formation 관리자AmazonDataZoneGlueDataAccessRole로 를 추가하거나 게시하려는 자산의 AmazonDataZoneGlueDataAccessRole에 다음 권한을 부여하여 문제를 해결할 수 있습니다. • 자산이 있는 데이터베이스에 대한 부여 가능한 권한을 설명하고 설명합니다. • Amazon이 사용자를 대신하여 DataZone 관리할 acecss 데이터베이스의 모든 자산에 대한 설명, 선택, 부여 가능 설명, 부여 가능 선택 권한.

Amazon DataZone 계보 자산과 업스트림 데이터 세트 연결 문제 해결

이 섹션에는 Amazon 계 DataZone 보에서 발생할 수 있는 문제에 대한 문제 해결 지침이 포함되어 있습니다. AWS Glue 및 Amazon Redshift 관련 오픈 계보 실행 이벤트 중 일부의 경우 자산 계보가 업스트림 데이터 세트에 연결되지 않은 것을 볼 수 있습니다. 이 주제에서는 시나리오와 문제를 완화하기 위한 몇 가지 접근 방식을 설명합니다. 계보에 대한 자세한 내용은 섹션을 참조하세요Amazon의 데이터 계보 DataZone (미리 보기) .

SourceIdentifier 계보 노드의

계보 노드의 `sourceIdentifier` 속성은 데이터 세트에서 발생하는 이벤트를 나타냅니다. 자세한 내용은 계보 노드의 키 속성을 참조하세요.

계보 노드는 해당 데이터 세트 또는 작업에서 발생하는 모든 이벤트를 나타냅니다. 계보 노드에는 해당 데이터 세트/작업의 식별자가 포함된 “sourceIdentifier” 속성이 포함되어 있습니다. 오픈 계보 이

벤트를 지원하므로 sourceIdentifier 값은 기본적으로 데이터 세트, 작업 및 작업 실행에 대해 'namespace'와 'name'의 조합으로 채워집니다.

AWS Glue 및 Amazon Redshift와 같은 AWS 리소스의 경우 sourceIdentifier는 AWS Glue AmazonARNs이 다음과 같이 실행 이벤트 ARN 및 기타 세부 정보를 구성하는 테이블 및 Redshift 테이블 DataZone 입니다.

> **Note**
>
> 에는 모든 리소스에 대한 accountId, 리전, 데이터베이스 및 테이블과 같은 정보가 AWS ARN 포함되어 있습니다.

- OpenLineage 이러한 데이터 세트의 이벤트에는 데이터베이스와 테이블 이름이 포함됩니다.
- 리전은 실행의 '환경 속성' 패싯에 캡처됩니다. 존재하지 않는 경우 시스템은 발신자 보안 인증 정보의 리전을 사용합니다.
- AccountId 는 호출자 보안 인증 정보에서 가져옵니다.

SourceIdentifier 내의 자산에 DataZone

AssetCommonDetailForm 에는 자산이 나타내는 데이터 세트의 식별자를 나타내는 “sourceIdentifier”라는 속성이 있습니다. 자산 계보 노드를 업스트림 데이터 세트와 연결하려면 속성에 데이터 세트 노드의 와 일치하는 값을 채워야 합니다sourceIdentifier. 데이터 소스에서 자산을 가져오는 경우 워크플로는 AWS Glue 테이블 ARN / Redshift 테이블sourceIdentifier로 ARN 자동으로 채워지고 를 통해 생성된 다른 자산(사용자 지정 자산 포함)은 호출자가 해당 값을 채워CreateAssetAPI야 합니다.

Amazon은 OpenLineage 이벤트 sourceIdentifier 에서 를 어떻게 DataZone 구성하나요?

AWS Glue 및 Redshift 자산의 경우 sourceIdentifier 는 Glue 및 Redshift 로 구성됩니다ARNs. Amazon이 이를 DataZone 구성하는 방법은 다음과 같습니다.

AWS Glue ARN

목표는 출력 계보 노드가 다음과 같은 OpenLineage 이벤트를 구성하는 sourceIdentifier 것입니다.

```
arn:aws:glue:us-east-1:123456789012:table/testlfdb/testlftb-1
```

실행이 의 데이터를 사용하는지 확인하려면 environment-properties 패싯에 특정 키워드가 있는지 AWS Glue확인합니다. 특히 이러한 지정된 필드가 있는 경우 시스템은 에서 RunEvent 오리진을 가정합니다 AWS Glue.

- GLUE_VERSION
- GLUE_COMMAND_CRITERIA
- GLUE_PYTHON_VERSION

```
"run": {
   "runId":"4e3da9e8-6228-4679-b0a2-fa916119fthr",
   "facets":{
      "environment-properties":{
         "_producer":"https://github.com/OpenLineage/OpenLineage/tree/1.9.1/
integration/spark",
         "_schemaURL":"https://openlineage.io/spec/2-0-2/OpenLineage.json#/$defs/
RunFacet",
         "environment-properties":{
            "GLUE_VERSION":"3.0",
            "GLUE_COMMAND_CRITERIA":"glueetl",
            "GLUE_PYTHON_VERSION":"3"
         }
      }
   }
```

AWS Glue 실행의 경우 symlinks 패싯의 이름을 사용하여 데이터베이스와 테이블 이름을 가져올 수 있으며, 이를 사용하여 를 구성할 수 있습니다ARN.

이름이 인지 확인해야 합니다databaseName.tableName.

```
"symlinks": {
   "_producer":"https://github.com/OpenLineage/OpenLineage/tree/1.9.1/integration/
spark",
   "_schemaURL":"https://openlineage.io/spec/facets/1-0-0/SymlinksDatasetFacet.json#/
$defs/SymlinksDatasetFacet",
   "identifiers":[
      {
         "namespace":"s3://object-path",
         "name":"testlfdb.testlftb-1",
```

```
         "type":"TABLE"
      }
   ]
}
```

샘플 COMPLETE 이벤트:

```
{
   "eventTime":"2024-07-01T12:00:00.000000Z",
   "producer":"https://github.com/OpenLineage/OpenLineage/tree/1.9.1/integration/glue",
   "schemaURL":"https://openlineage.io/spec/2-0-2/OpenLineage.json#/$defs/RunEvent",
   "eventType":"COMPLETE",
   "run": {
      "runId":"4e3da9e8-6228-4679-b0a2-fa916119fthr",
      "facets":{
         "environment-properties":{
            "_producer":"https://github.com/OpenLineage/OpenLineage/tree/1.9.1/
integration/spark",
            "_schemaURL":"https://openlineage.io/spec/2-0-2/OpenLineage.json#/$defs/
RunFacet",
            "environment-properties":{
               "GLUE_VERSION":"3.0",
               "GLUE_COMMAND_CRITERIA":"glueetl",
               "GLUE_PYTHON_VERSION":"3"
            }
         }
      }
   },
   "job":{
      "namespace":"namespace",
      "name":"job_name",
      "facets":{
         "jobType":{
            "_producer":"https://github.com/OpenLineage/OpenLineage/tree/1.9.1/
integration/glue",
            "_schemaURL":"https://openlineage.io/spec/facets/2-0-2/
JobTypeJobFacet.json#/$defs/JobTypeJobFacet",
            "processingType":"BATCH",
            "integration":"glue",
            "jobType":"JOB"
         }
      }
   },
```

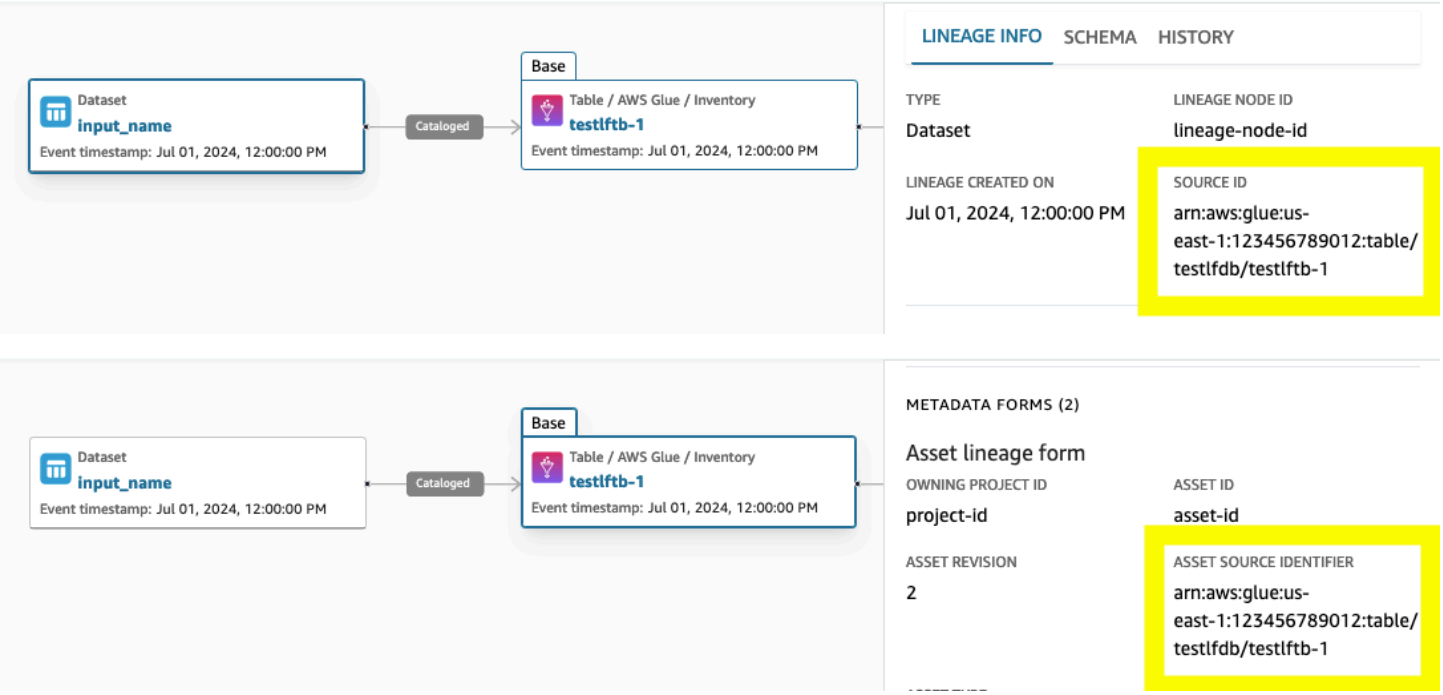
```
   "inputs":[
      {
         "namespace":"namespace",
         "name":"input_name"
      }
   ],
   "outputs":[
      {
         "namespace":"namespace.output",
         "name":"output_name",
         "facets":{
            "symlinks":{
               "_producer":"https://github.com/OpenLineage/OpenLineage/tree/1.9.1/
integration/spark",
               "_schemaURL":"https://openlineage.io/spec/facets/1-0-0/
SymlinksDatasetFacet.json#/$defs/SymlinksDatasetFacet",
               "identifiers":[
                  {
                     "namespace":"s3://object-path",
                     "name":"testlfdb.testlftb-1",
                     "type":"TABLE"
                  }
               ]
            }
         }
      }
   ]
}
```

제출된 OpenLineage 이벤트에 따라 출력 계보 노드sourceIdentifier의 는 다음과 같습니다.

```
arn:aws:glue:us-east-1:123456789012:table/testlfdb/testlftb-1
```

출력 계보 노드는 자산의 계보 노드에 연결되며, 여기서 자산은 다음과 sourceIdentifier 같습니다.

```
arn:aws:glue:us-east-1:123456789012:table/testlfdb/testlftb-1
```



Amazon Redshift ARN

목표는 출력 계보 노드가 다음과 같은 OpenLineage 이벤트를 구성하는 `sourceIdentifier` 것입니다.

```
arn:aws:redshift:us-east-1:123456789012:table/workgroup-20240715/tpcds_data/public/
dws_tpcds_7
```

시스템은 네임스페이스를 기반으로 입력 또는 출력이 Redshift에 저장되는지 여부를 결정합니다. 특히 네임스페이스가 redshift://로 시작하거나 문자열 `redshift-serverless.amazonaws.com` 또는 가 포함된 경우 `redshift.amazonaws.com`Redshift 리소스입니다.

```
"outputs": [
    {
        "namespace":"redshift://workgroup-20240715.123456789012.us-
east-1.redshift.amazonaws.com:5439",
        "name":"tpcds_data.public.dws_tpcds_7"
    }
]
```

네임스페이스는 다음 형식이어야 합니다.

```
provider://{cluster_identifier}.{region_name}:{port}
```

redshift-serverless의 경우:

```
"outputs": [
    {
        "namespace":"redshift://workgroup-20240715.123456789012.us-east-1.redshift-
serverless.amazonaws.com:5439",
        "name":"tpcds_data.public.dws_tpcds_7"
    }
]
```

다음과 같은 결과를 가져옵니다. sourceIdentifier

```
arn:aws:redshift-serverless:us-east-1:123456789012:table/workgroup-20240715/tpcds_data/
public/dws_tpcds_7
```

제출된 OpenLineage 이벤트에 따라 다운스트림(즉, 이벤트의 출력) 계보 노드에 매핑sourceIdentifier될 는 다음과 같습니다.

```
arn:aws:redshift-serverless:us-e:us-east-1:123456789012:table/workgroup-20240715/
tpcds_data/public/dws_tpcds_7
```

카탈로그에서 자산의 계보를 시각화하는 데 도움이 되는 매핑입니다.

대체 접근 방식

위의 조건 중 어느 것도 충족되지 않으면 시스템은 네임스페이스/이름을 사용하여 를 구성합니다sourceIdentifier.

```
"inputs": [
  {
     "namespace":"arn:aws:redshift:us-east-1:123456789012:table",
     "name":"workgroup-20240715/tpcds_data/public/dws_tpcds_7"
  }
],
"outputs": [
  {
     "namespace":"arn:aws:glue:us-east-1:123456789012:table",
     "name":"testlfdb/testlftb-1"
  }
]
```

자산 계보 노드의 업스트림 부족 문제 해결

자산 계보 노드의 업스트림이 표시되지 않는 경우 다음을 수행하여 데이터 세트와 연결되지 않은 이유를 해결할 수 있습니다.

1. domainId 및 를 제공하는 GetAsset 동안 호출assetId:

```
aws datazone get-asset --domain-identifier <domain-id> --identifier <asset-id>
```

응답은 다음과 같이 나타납니다.

```
{
    .....
    "formsOutput": [
        .....
        {
            "content": "{\"sourceIdentifier\":\"arn:aws:glue:eu-
west-1:123456789012:table/testlfdb/testlftb-1\"}",
            "formName": "AssetCommonDetailsForm",
            "typeName": "amazon.datazone.AssetCommonDetailsFormType",
            "typeRevision": "6"
        },
        .....
    ],
    "id": "<asset-id>",
    ....
}
```

2. 를 호출GetLineageNode하여 데이터 세트 계보 노드sourceIdentifier의 를 가져옵니다. 해당 데이터 세트 노드의 계보 노드를 직접 가져올 방법이 없으므로 작업 실행GetLineageNode에서 로 시작할 수 있습니다.

```
aws datazone get-lineage-node --domain-identifier <domain-id> --identifier
 <job_namespace>.<job_name>/<run_id>

if you are using the getting started scripts, job name and run ID are printed in the
 console
and namespace is "default". Otherwise you can get these values from run event
 content.
```

샘플 응답은 다음과 같습니다.

```
{
    .....
    "downstreamNodes": [
        {
            "eventTimestamp": "2024-07-24T18:08:55+08:00",
            "id": "afymge5k4v0euf"
        }
    ],
    "formsOutput": [
        <some forms corresponding to run and job>
    ],
    "id": "<system generated node-id for run>",
    "sourceIdentifier": "default.redshift.create/2f41298b-1ee7-3302-
a14b-09addffa7580",
    "typeName": "amazon.datazone.JobRunLineageNodeType",
    ....
    "upstreamNodes": [
        {
            "eventTimestamp": "2024-07-24T18:08:55+08:00",
            "id": "6wf2z27c8hghev"
        },
        {
            "eventTimestamp": "2024-07-24T18:08:55+08:00",
            "id": "4tjbcsnre6banb"
        }
    ]
}
```

3. 다운스트림/업스트림 노드 식별자(자산 노드에 연결해야 한다고 생각됨)를 데이터 세트에 해당하므로 를 전달하여 GetLineageNode 다시 호출합니다.

   위의 예제 응답을 사용한 샘플 명령:

```
aws datazone get-lineage-node --domain-identifier <domain-id> --identifier
 afymge5k4v0euf
```

   이렇게 하면 데이터 세트에 해당하는 계보 노드 세부 정보가 반환됩니다. afymge5k4v0euf

```
{
    .....
    "domainId": "dzd_cklzc5s2jcr7on",
```

```
    "downstreamNodes": [],
    "eventTimestamp": "2024-07-24T18:08:55+08:00",
    "formsOutput": [
        .....
    ],
    "id": "afymge5k4v0euf",
    "sourceIdentifier": "arn:aws:redshift:us-east-1:123456789012:table/
workgroup-20240715/tpcds_data/public/dws_tpcds_7",
    "typeName": "amazon.datazone.DatasetLineageNodeType",
    "typeRevision": "1",
    ....
    "upstreamNodes": [
        ...
    ]
}
```

4. 이 데이터 세트 노드sourceIdentifier의 와 의 응답을 비교합니다GetAsset. 연결되지 않은 경우 이러한 항목이 일치하지 않으므로 계보 UI에 표시되지 않습니다.

일치하지 않는 시나리오 및 완화 조치

다음은 일반적으로 알려져 있는 시나리오로, 일치하지 않는 시나리오와 가능한 완화 조치입니다.

근본 원인 : 테이블이 Amazon DataZone 도메인 계정과 다른 계정에 있습니다.

완화 : 연결된 계정에서 PostLineageEvent 작업을 호출할 수 있습니다. 구성할 이 호출자 보안 인증 정보에서 ARN 선택되면 시작하기 스크립트를 실행하거나 를 호출할 때 테이블이 포함된 계정에서 역할을 수임accountId할 수 있습니다PostLineageEvent. 이렇게 하면 를 ARNs 올바르게 구성하고 자산 노드와 연결하는 데 도움이 됩니다.

근본 원인 : RedshiftARN용 table/views contains Redshift/Redshift- OpenLineage 실행 이벤트에서 해당 데이터 세트 정보의 네임스페이스 및 이름 속성을 기반으로 하는 서버리스용 입니다.

완화 : 지정된 이름이 클러스터 또는 작업 그룹에 속하는지 여부를 알 수 있는 결정적인 방법이 없으므로 다음과 같은 휴리스틱을 사용합니다.

- 데이터 세트에 해당하는 “이름”에 “redshift-serverless.amazonaws.com”이 포함된 경우 의 일부로 redshift-serverless를 사용하며ARN, 그렇지 않으면 “redshift”로 기본 설정됩니다.
- 위는 작업 그룹 이름의 별칭이 작동하지 않음을 의미합니다.

근본 원인 : 업스트림 데이터 세트가 사용자 지정 자산에 대해 제대로 연결되지 않았습니다.

완화 : 데이터 세트 노드(사용자 지정 노드의 경우 <namespace>/<name>)sourceIdentifier의 와 일치하는 CreateAsset/CreateAssetRevision 를 호출하여 자산sourceIdentifier의 를 채워야 합니다.

아마존 할당량 DataZone

AWS 계정에는 각 서비스에 대한 기본 할당량 (이전에는 한도라고 함) 이 있습니다. AWS 다르게 표시되지 않는 한, 리전별로 각 할당량이 적용됩니다.

DataZone Amazon에는 다음과 같은 할당량 및 한도가 있습니다.

Resource	설명	값
데이터 자산 유형	DataZone 도메인에서 생성할 수 있는 최대 데이터 자산 유형 수	1000
데이터 자산	Amazon DataZone 도메인에서 생성할 수 있는 최대 데이터 자산 수	100만
용어집	도메인에서 만들 수 있는 비즈니스 용어집의 최대 개수	1000
비즈니스 용어집 용어	도메인에서 만들 수 있는 총 비즈니스 용어집 용어의 최대 수	10000
도메인 내 환경	Amazon DataZone 도메인의 최대 환경 수	500
자산당 자산 필터 수	Amazon DataZone 자산당 최대 자산 필터 수	100
구독당 필터 수	Amazon DataZone 구독당 최대 필터 수	5
도메인의 도메인 단위	Amazon DataZone 도메인의 최대 도메인 단위 수	100
도메인 단위의 계층 구조 수준	도메인 단위의 최대 계층 수준 수	5

Resource	설명	값
도메인 단위별 정책별 부여	도메인 단위별 정책당 최대 부여 수	20
데이터 제품	DataZone 도메인에서 생성할 수 있는 최대 데이터 제품 수	500,000

Amazon DataZone 사용 설명서의 문서 기록

다음 표에는 Amazon의 설명서 릴리스가 설명되어 DataZone 있습니다.

변경 사항	설명	날짜
도메인 단위	Amazon은 고객이 비즈니스 단위/팀 수준의 조직을 만들고 비즈니스 요구 사항에 따라 정책을 관리할 수 있도록 도메인 단위 및 권한 부여 정책이라는 새로운 데이터 거버넌스 기능 세트를 DataZone 도입합니다. 도메인 단위를 추가하면 사용자는 사업부 또는 팀과 관련된 데이터 자산 및 프로젝트를 구성, 생성, 검색 및 찾을 수 있습니다. 권한 부여 정책을 통해 해당 도메인 단위 사용자는 Amazon DataZone 내에서 프로젝트, 용어집 생성 및 컴퓨팅 리소스 사용에 대한 액세스 정책을 설정할 수 있습니다.	2024년 8월 5일
데이터 제품	Amazon은 데이터 자산을 특정 비즈니스 사용 사례에 맞게 잘 정의된 독립형 패키지로 그룹화할 수 있는 데이터 제품을 DataZone 소개합니다. 예를 들어 마케팅 분석 데이터 제품은 마케팅 캠페인 데이터, 파이프라인 데이터, 고객 데이터와 같은 다양한 데이터 자산을 번들로 묶을 수 있습니다. 데이터 제품을 사용하면 고객은 검색 및 구독 프로세스를 단순화하여	2024년 8월 5일

	비즈니스 목표에 맞게 조정하고 개별 자산 처리 시 중복되는 문제를 줄일 수 있습니다.	
AmazonDataZoneDomainExecutionRolePolicy 및 AmazonDataZoneFullUserAccess - 정책 업데이트	Amazon DataZone 도메인 유닛 AmazonDataZoneDomainExecutionRolePolicy및 데이터 상품을 생성하고 관리하는 데 사용되는 새 APIs 항목에 대한 지원을 AmazonDataZoneFullUserAccess활성화하기 위해 및 에 대한 정책 업데이트. 자세한 내용은 Amazon DataZone 업데이트를 참조하십시오. AWS 관리형 정책.	2024년 8월 5일

세분화된 액세스 제어	DataZone Amazon은 세분화된 액세스 제어를 도입하여 데이터 레이크 및 데이터 웨어하우스에 걸친 Amazon DataZone 비즈니스 데이터 카탈로그의 데이터 자산을 세밀하게 제어할 수 있도록 합니다. 새로운 기능을 통해 이제 데이터 소유자는 전체 데이터 자산에 대한 액세스 권한을 부여하는 대신 행 및 열 수준에서 특정 데이터 레코드에 대한 액세스를 제한할 수 있습니다. 예를 들어 데이터에 개인 식별 정보 (PII) 와 같은 민감한 정보가 포함된 열이 포함된 경우 필요한 열로만 액세스를 제한하여 민감하지 않은 데이터에 대한 액세스는 허용하면서 중요한 정보는 보호할 수 있습니다. 마찬가지로 행 수준에서 액세스를 제어하여 사용자가 자신의 역할 또는 작업과 관련된 레코드만 볼 수 있도록 할 수 있습니다.	2024년 7월 2일
AmazonDataZoneGlueManageAccessRolePolicy - 정책 업데이트	정책 업데이트 AmazonDataZoneGlueManageAccessRolePolicy- DataZone Amazon은 Lake Formation에서 IAM 권한 부여 범위를 좁히기 위해 세분화된 액세스 제어 기능에 사용되는 권한을 추가하고 있습니다. 자세한 내용은 Amazon DataZone 업데이트를 참조하십시오. AWS 관리형 정책.	2024년 7월 2일

데이터 계보	Amazon은 미리 보기 모드로 데이터 계보를 DataZone 출시하여 고객이 OpenLineage 지원 시스템에서 발생하거나 소스에서 소비에 이르는 데이터 이동을 통해 계보 이벤트를 API 시각화하고 추적할 수 있도록 지원합니다. DataZoneAmazon과 OpenLineage 호환되는 APIs 기능을 사용하면 도메인 관리자와 데이터 생산자는 Amazon S3에서의 변환을 포함하여 Amazon에서 사용할 수 있는 것 이상의 계보 이벤트를 캡처하고 저장할 수 있습니다. DataZone AWS Glue 및 기타 서비스. 또한 Amazon은 각 이벤트에 따라 계보를 DataZone 버전화하여 사용자가 언제든지 계보를 시각화하거나 자산 또는 작업 기록의 변화를 비교할 수 있도록 합니다. 이 과거 계보를 통해 데이터가 어떻게 진화했는지 더 깊이 이해할 수 있으며, 이는 데이터 자산의 문제 해결, 감사 및 무결성 검증에 필수적입니다.	2024년 6월 27일

AmazonDataZoneExecutionRolePolicy 및 - 정책 업데이트 AmazonDataZoneFullUserAccess	데이터 계보 AmazonDataZoneExecutionRolePolicy및 세밀한 액세스 제어에 대한 지원을 가능하게 AmazonDataZoneFullUserAccess하기 위한 및 정책 업데이트. APIs 자세한 내용은 Amazon DataZone 업데이트를 참조하십시오. AWS 관리형 정책.	2024년 6월 27일

사용자 지정 AWS 서비스 청사진	커스텀 포함 AWS 서비스 청사진 (기존 청사진 있는 경우) AWS IAM역할, 데이터 레이크, 데이터 메시, Amazon S3 버킷, Amazon Redshift 클러스터를 비롯한 리소스에서 이제 고유한 IAM 사용자 지정 역할을 사용하여 이러한 기존 리소스에 대한 권한을 지정할 수 있으므로 DataZone Amazon 사용자는 게시 및 구독을 활용하여 이러한 리소스를 공유하고 관리할 수 있습니다. 사용자 지정 기능을 사용하면 AWS 서비스 블루프린트, Amazon DataZone 관리자가 구성할 수 있는 기능 AWS 자체 사용자 지정 역할을 사용하는 서비스 환경. 이를 위한 작업 링크를 구성할 수 있습니다. AWS 서비스 환경을 제공하므로 기존 환경 모두에 대한 페더레이션 액세스를 제공합니다. AWS 있습니다. 또한 이러한 사용자 지정으로 구독 대상 및 데이터 소스를 구성할 수 있습니다. AWS 서비스 환경. 관리자가 설정할 수 있습니다. AWS 데이터를 게시, 구독, 검색 또는 관리하려는 Amazon DataZone 도메인 계정 또는 관련 계정의 서비스 환경.	2024년 6월 17일

AmazonDataZoneGlueManageAccessRolePolicy - 정책 업데이트	Lake AmazonDataZoneGlueManageAccessRolePolicy Formation에서 IAM 부여하는 권한의 범위를 좁히기 위해 DataZone Amazon의 자체 구독 기능에 필요한 권한을 추가하는 정책 업데이트입니다. 셀프 구독 기능을 사용하면 태그가 지정된 리소스에만 호수 형성 권한을 부여할 수 있습니다. 자세한 내용은 Amazon DataZone 업데이트를 참조하십시오. AWS 관리형 정책.	2024년 6월 14일
AmazonDataZoneFullAccess - 정책 업데이트	이에 대한 정책 업데이트는 Amazon DataZone Management Console이 사용자를 대신하여 도메인 및 프로젝트 태그 모두를 사용하여 비밀을 생성할 수 있도록 합니다. AmazonDataZoneFullAccess 또한 도메인 소유자 계정의 관리자가 관련 계정의 계정 연결 상태를 볼 수 있도록 하는 `ram:ListResourceSharePermissions` 작업도 포함됩니다. 자세한 내용은 Amazon DataZone 업데이트를 참조하십시오. AWS 관리형 정책.	2024년 6월 14일

AmazonDataZoneDomainExecutionRolePolicy - 정책 업데이트	정책 업데이트로 APIs Amazon에 새로운 기능이 추가되어 DataZone 사용자가 Amazon DataZone 환경에 맞게 작업을 구성할 수 있습니다. AmazonDataZoneDomainExecutionRolePolicy 자세한 내용은 Amazon DataZone 업데이트를 참조하십시오. AWS 관리형 정책.	2024년 6월 14일

데이터 소스 생성 개선 사항	DataZone Amazon은 데이터 생산자의 액세스 관리를 단순화하기 위해 데이터 소스 생성 흐름을 개선했습니다. 이번 업데이트를 통해 데이터 생산자가 데이터 출판을 위한 데이터 소스를 생성하면 AWS Glue 및 Amazon Redshift 자산에서 Amazon은 DataZone 프로젝트 구성원에게 읽기 전용 권한을 부여합니다. 를 생성할 때 AWS Glue 데이터 소스의 경우 Amazon은 데이터 소스를 생성하는 데 사용된 환경 IAM 역할에 '읽기 전용' 권한을 DataZone 자동으로 부여하여 관련 테이블의 모든 테이블에 액세스할 수 있도록 합니다. AWS Glue 데이터베이스. 마찬가지로 Amazon Redshift 데이터 소스의 경우 Amazon은 데이터 소스에서 사용되는 Amazon Redshift 스키마의 모든 테이블에 대해 '읽기 전용' 액세스 권한을 DataZone 부여합니다.	2024년 6월 10일

아마존과의 통합 SageMaker	Amazon은 SageMaker Amazon과의 통합을 DataZone 시작하여 데이터 생산자와 소비자가 Amazon으로 원활하게 전환하여 기계 학습 (ML) 프로젝트에서 SageMaker 협업하는 동시에 데이터 및 ML 자산에 대한 액세스 거버넌스를 적용할 수 있도록 지원합니다. DataZone Amazon과 Amazon SageMaker 간의 새로운 통합 기능을 통해 데이터 소비자와 생산자는 인프라 설정 전반에서 ML 거버넌스를 간소화하고, 비즈니스 이니셔티브에 대해 협업하고, 데이터와 ML 자산을 쉽게 관리할 수 있습니다.	2024년 5월 6일
AmazonDataZoneSageMakerProvisioning - 새 정책	Amazon이라는 새 정책은 DataZone Amazon과 상호 운용하는 데 필요한 권한을 SageMaker Amazon에 AmazonDataZoneSageMakerProvisioning부여합니다. 자세한 내용은 Amazon DataZone 업데이트를 참조하십시오. AWS 관리형 정책.	2024년 4월 30일

AmazonDataZoneSageMakerEnvironmentRolePermissionsBoundary - 새 권한 경계	새 권한 경계가 AmazonDataZoneSageMakerEnvironmentRolePermissionsBoundary 호출되었습니다. Amazon DataZone 데이터 포털을 통해 Amazon SageMaker 환경을 생성하면 Amazon 은 환경 생성 중에 생성되는 IAM 역할에 이 권한 경계를 DataZone 적용합니다. 권한 경계는 Amazon이 DataZone 생성하는 역할 및 사용자가 추가하는 모든 역할의 범위를 제한합니다. 자세한 내용은 Amazon DataZone 업데이트를 참조하십시오. AWS 관리형 정책.	2024년 4월 30일
AmazonDataZoneSageMakerAccess - 새 정책	라는 AmazonDataZoneSageMakerAccess 새 정책은 Amazon DataZone SageMaker 환경의 다양한 리소스에 대한 사용자 액세스 권한을 부여하는 데 필요한 권한을 Amazon 에 부여합니다. 자세한 내용은 Amazon DataZone 업데이트를 참조하십시오. AWS 관리형 정책.	2024년 4월 30일

AmazonDataZoneFullAccess - 정책 업데이트	콘솔에서 블루프린트를 구성하고 지정된 관리형 AmazonDataZoneFullAccess정책에 대한 정보를 검색하는 데 도움이 되는 `DescribeSecurityGroups` 작업을 구성하는 계정 관리자의 편의성을 개선하기 위해 `GetPolicy` 작업에 대한 액세스 권한을 추가하는 정책 업데이트입니다. 자세한 내용은 Amazon DataZone 업데이트를 참조하십시오. AWS 관리형 정책.	2024년 4월 30일

Lake Formation 하이브리드 액세스 모드	DataZone Amazon은 다음과 같은 통합을 도입했습니다. AWS Lake Formation 하이브리드 액세스 모드. 이 통합을 통해 귀하의 데이터를 쉽게 게시하고 공유할 수 있습니다. AWS 테이블을 등록할 필요 없이 DataZone Amazon을 통해 테이블을 접착할 수 있습니다. AWS 먼저 레이크 포메이션. 시작하려면 관리자가 Amazon DataZone 콘솔의 `DefaultDataLake` 블루프린트에서 데이터 위치 등록 설정을 활성화해야 합니다. 그런 다음, 데이터 소비자가 구독하면 AWS IAM권한을 통해 관리되는 Glue 테이블에서는 Amazon이 DataZone 먼저 하이브리드 모드에서 이 테이블의 Amazon S3 위치를 등록한 다음, 테이블에 대한 권한을 관리하여 데이터 소비자에게 액세스 권한을 부여합니다. AWS 레이크 포메이션. 이렇게 하면 새로 부여된 후에도 테이블에 대한 IAM 권한이 계속 유지됩니다. AWS 기존 워크플로를 방해하지 않는 Lake Formation 권한. 자세한 내용은 Amazon과 AWS Lake Formation 하이브리드 모드 DataZone 통합을 참조하십시오.	2024년 4월 3일

데이터 품질	아마존 DataZone , 다음과 통합 시작 AWS Glue Data Quality는 타사 데이터 품질 솔루션의 데이터 품질 메트릭을 APIs 통합하는 기능을 제공합니다. 새로운 통합을 통해 자동 게시할 수 있습니다. AWS Amazon DataZone 비즈니스 데이터 카탈로그에 데이터 품질 점수를 붙이세요. Amazon은 타사 소스의 품질 지표를 수집하는 데 사용할 DataZone APIs 수 있습니다. 게시되면 데이터 소비자는 데이터 자산을 쉽게 검색하고, 세분화된 품질 지표를 보고, 실패한 검사 및 규칙을 식별하여 비즈니스 의사 결정을 내릴 수 있습니다. 자세한 내용은 Amazon의 데이터 품질을 참조하십시오 DataZone.	2024년 4월 3일
AmazonDataZoneS3Manage- -< domainId > - 새 역할 <region>	아마존에서 전화를 걸 <region>때 AmazonDataZone 사용되는 S3Manage- -< domainId >라는 새로운 역할 DataZone AWS 레이크 포메이션, 아마존 심플 스토리지 서비스 (아마존 S3) 위치 등록 AWS Lake Formation은 해당 위치의 데이터에 액세스할 때 이 역할을 맡습니다. 자세한 내용은 Amazon DataZone 업데이트를 참조하십시오. AWS 관리형 정책.	2024년 4월 1일

AmazonDataZoneGlueManageAccessRolePolicy - 정책 업데이트	Amazon이 AmazonDataZoneGlueManageAccessRolePolicy데이터에 대한 게시 및 액세스 권한 DataZone 부여를 활성화할 수 있는 권한에 대한 지원을 활성화하도록 업데이트되었습니다. 자세한 내용은 Amazon DataZone 업데이트를 참조하십시오. AWS 관리형 정책.	2024년 4월 1일
AmazonDataZoneDomainExecutionRolePolicy 및 AmazonDataZoneFullUserAccess - 정책 업데이트	에 대한 지원을 AmazonDataZoneFullUserAccess활성화하도록 AmazonDataZoneDomainExecutionRolePolicy및 를 `CancelMetadataGenerationRun` API 업데이트했습니다. 자세한 내용은 Amazon DataZone 업데이트를 참조하십시오. AWS 관리형 정책.	2024년 3월 29일

AmazonDataZoneFullAccess - 정책 업데이트	Amazon은 비즈니스 데이터 카탈로그를 보강하여 데이터 검색, 데이터 이해 및 데이터 사용을 개선할 수 있는 새로운 제너레이티브 AI 기반 기능의 정식 출시를 DataZone 발표했습니다. 데이터 생산자는 클릭 한 번으로 포괄적인 비즈니스 데이터 설명 및 컨텍스트를 생성하고, 영향력 있는 열을 강조 표시하고, 분석 사용 사례에 대한 권장 사항을 포함할 수 있습니다. 이번 출시에는 데이터 생산자가 자산에 대한 APIs 설명을 프로그래밍 방식으로 생성하는 데 사용할 수 있는 지원이 추가되었습니다.	2024년 3월 27일

AmazonDataZoneFullAccess - 정책 업데이트	DataZone 아마존은 Amazon Redshift 테이블 및 뷰를 게시하고 구독하는 프로세스를 간소화하는 Amazon Redshift 통합에 몇 가지 개선 사항을 도입했습니다. 이러한 업데이트는 데이터 생산자와 소비자 모두의 경험을 간소화하여 Amazon DataZone 관리자가 제공하는 사전 구성된 자격 증명과 연결 매개변수를 사용하여 데이터 웨어하우스 환경을 빠르게 만들 수 있도록 합니다. 또한 이러한 개선 사항을 통해 관리자는 자신의 리소스를 누가 사용할 수 있는지 더 잘 제어할 수 있습니다. AWS 계정 및 Amazon Redshift 클러스터, 그리고 어떤 용도로 사용됩니까?	2024년 3월 21일
AmazonDataZoneFullAccess - 정책 업데이트	사용자가 텍스트 상자에 입력하지 않고 Amazon DataZone 관리 콘솔에서 암호, 클러스터, vpc 및 서브넷을 선택할 수 있도록 업데이트되었습니다. `AmazonDataZoneFullAccess` 자세한 내용은 Amazon DataZone 업데이트를 참조하십시오. AWS 관리형 정책.	2024년 3월 13일

AmazonDataZoneDomainExecutionRolePolicy - 정책 업데이트	어떤 계정과 지역에서 어떤 블루프린트가 활성화되었는지 식별하여 환경 프로필 생성에 필요한 지원이 가능하도록 업데이트되었습니다. AmazonDataZoneDomainExecutionRolePolicy ListEnvironmentBlueprintConfigurationSummaries API 자세한 내용은 Amazon DataZone 업데이트를 참조하십시오. AWS 관리형 정책.	2024년 2월 1일
클라우드 포메이션 사용 개선 사항	Amazon 사용자는 이제 활용할 DataZone 수 있습니다. AWS CloudFormation Amazon DataZone 리소스 제품군을 효과적으로 모델링하고 관리합니다. 이 접근 방식은 일관된 리소스 프로비저닝을 용이하게 하는 동시에 코드형 인프라 프랙티스를 통해 수명 주기 관리를 가능하게 합니다. 사용자 지정 템플릿을 사용하면 필요한 리소스와 상호 종속성을 정확하게 정의할 수 있습니다. 자세한 내용은 Amazon DataZone 리소스 유형 참조를 참조하십시오.	2024년 1월 18일

사용자 지정 자산	사용자 지정 자산에 대한 지원을 통해 DataZone Amazon은 Data Portal을 통해 대시보드, 쿼리, 모델 등의 비정형 데이터에 대한 자산을 카탈로그화할 수 있으므로 이전에 API 제공되었던 지원과 함께 데이터 포털에서 직접 사용자 지정 자산을 더 쉽게 추가할 수 있습니다. DataZoneAmazon에서 사용자 지정 자산을 생성, 업데이트 및 게시할 수 있으므로 모든 유형의 자산을 공유, 검색, 구독하고 해당 자산에 대한 거버넌스를 제공하는 비즈니스 워크플로를 구축할 수 있습니다. 자세한 내용은 사용자 지정 자산 유형 생성을 참조하십시오.	2024년 1월 5일

IAM주도자를 프로젝트 멤버로 추가	이제 IAM 주도자가 아직 Amazon에 로그인하지 않았더라도 IAM 주도자를 프로젝트 구성원으로 추가할 수 있습니다 DataZone (이전 요구 사항). 도메인 관리자 또는 IT 관리자가 도메인의 도메인 실행 역할을 `iam:GetUser` 추가한 후 프로젝트 소유자는 역할 또는 사용자의 Amazon Resource IAM Name (ARN) 을 제공하기만 하면 주체를 구성원으로 추가할 수 있습니다. `iam:GetRole` IAM IAM IAM보안 주체는 여전히 Amazon에 액세스하는 데 필요한 IAM 권한을 가지고 있어야 DataZone 하며 이러한 권한은 IAM 콘솔에서 구성할 수 있습니다. 자세한 내용은 프로젝트에 구성원 추가를 참조하십시오.	2024년 1월 5일
도메인 삭제	도메인 삭제는 도메인을 더 쉽게 삭제할 수 있는 기능입니다. 이제 비어 있지 않아도 도메인 삭제를 진행할 수 있습니다 (예: 프로젝트, 환경, 자산, 데이터 원본 등이 포함된 경우). 자세한 내용은 Amazon DataZone 도메인 삭제를 참조하십시오.	2023년 12월 27일

레이크 포메이션 하이브리드 모드	DataZone Amazon은 에 대한 지원을 추가했습니다. AWS 레이크 포메이션 하이브리드 모드. 이 지원을 통해 게시하면 AWS 그것으로 Amazon에 테이블을 DataZone 붙입니다. AWS 하이브리드 모드에서 Lake Formation에 등록된 S3 위치에서 Amazon은 이 테이블을 관리 자산으로 DataZone 취급하며 이 테이블에 대한 구독 허가를 관리할 수 있습니다. 이 기능이 출시되기 전에 Amazon은 DataZone 이 테이블을 비관리 자산으로 취급했습니다. 즉, DataZone Amazon은 이 테이블에 대한 구독을 승인할 수 없었습니다. 자세한 내용은 Amazon의 Lake Formation 권한 구성을 참조하십시오 DataZone.	2023년 12월 22일
HIPAA규정 준수	DataZone Amazon은 현재 1996년 미국 건강 보험 양도 및 책임법 (HIPAA) 을 준수하고 있습니다. 목록을 보려면 AWS HIPAA규정 준수가 적용되는 서비스는 https://aws.amazon.com/compliance/hipaa-eligible-services-reference/를 참조하십시오.	2023년 12월 14일

AmazonDataZoneGlueManageAccessRolePolicy - 정책 업데이트	에 대한 지원이 AmazonDataZoneGlueManageAccessRolePolicy가능하도록 업데이트되었습니다. AWS 레이크 포메이션 하이브리드 모드. 자세한 내용은 Amazon DataZone 업데이트를 참조하십시오. AWS 관리형 정책.	2023년 12월 14일
AmazonDataZoneFullUserAccess 및 AmazonDataZoneDomainExecutionRolePolicy - 정책 업데이트	Amazon은 Amazon의 생성적 AI 기반 데이터 설명 기능을 지원하도록 AmazonDataZoneFullUserAccess및 AmazonDataZoneDomainExecutionRolePolicy정책을 DataZone 업데이트했습니다. DataZone 자세한 내용은 Amazon DataZone 업데이트를 참조하십시오. AWS 관리형 정책.	2023년 11월 28일

AI 권장 사항	AWS 비즈니스 데이터 카탈로그를 보강하여 데이터 검색, 데이터 이해 및 데이터 사용을 개선할 수 DataZone 있는 Amazon의 새로운 제너레이티브 AI 기반 기능의 미리보기를 발표합니다. 데이터 생산자는 클릭 한 번으로 포괄적인 비즈니스 데이터 설명 및 컨텍스트를 생성하고, 영향력 있는 열을 강조 표시하고, 분석 사용 사례에 대한 권장 사항을 포함할 수 있습니다. DataZoneAmazon의 설명에 대한 AI 권장 사항을 통해 데이터 소비자는 분석에 필요한 데이터 테이블과 열을 식별할 수 있으므로 데이터 검색 가능성이 향상되고 데이터 생산자와의 back-and-forth 커뮤니케이션이 줄어듭니다. 미리보기는 다음에서 프로비저닝된 Amazon DataZone 도메인에서 사용할 수 있습니다. AWS 지역: 미국 동부 (버지니아 북부), 미국 서부 (오레곤). 자세한 내용은 기계 학습 및 제너레이티브 AI 사용을 참조하십시오.	2023년 11월 28일
DefaultDataLake 청사진	DataZone Amazon은 누가 귀하의 데이터를 게시할 수 있는지 더 잘 제어할 수 있도록 DefaultDataLake 청사진에 개선 사항을 추가했습니다. AWS 계정. 이번 기능 출시와 함께 도입된 두 가지 주요 변경 사항이 있습니다.	2023년 11월 20일

AmazonDataZoneEnvironmentRolePermissionsBoundary - 정책 업데이트	DataZone Amazon은 `ResourceTag` 조건에 따라 범위가 축소된 추가 `athena:GetQueryResultsStream` 권한으로 구성된 AmazonDataZoneEnvironmentRolePermissionsBoundary관리형 정책을 업데이트했습니다. 자세한 내용은 Amazon DataZone 업데이트를 참조하십시오. AWS 관리형 정책.	2023년 11월 17일
AmazonDataZoneRedshiftManageAccessRolePolicy - 정책 업데이트	Amazon은 해당 `redshift:AssociateDataShareConsumer` 작업에 대한 조직 ID 확인을 제거하여 AmazonDataZoneRedshiftManageAccessRolePolicy정책을 DataZone 업데이트했습니다. 이렇게 하면 리소스를 여러 곳에서 공유할 수 있습니다. AWS 조직. 자세한 내용은 Amazon DataZone 업데이트를 참조하십시오. AWS 관리형 정책.	2023년 11월 16일
GA 출시, 사용자 가이드	Amazon 사용 DataZone 설명서의 GA (일반 공급) 릴리스.	2023년 10월 15일

AmazonDataZoneFull UserAccess - 정책 업데이트	Amazon은 DataZone Amazon에 대한 전체 액세스 권한을 부여하는 AmazonDataZoneFull UserAccess정책을 DataZone 업데이트했지만 도메인, 사용자 또는 관련 계정의 관리는 허용하지 않습니다. 자세한 내용은 Amazon DataZone 업데이트를 참조하십시오. AWS 관리형 정책.	2023년 10월 2일
AmazonDataZonePreviewConsoleFullAccess - 정책이 더 이상 사용되지 않음	Amazon은 더 DataZone 이상 사용되지 않습니다 AmazonDataZonePreviewConsoleFullAccess. 자세한 내용은 Amazon 업데이트를 참조하십시오. DataZone AWS 관리형 정책.	2023년 9월 29일
AmazonDataZonePortalFullAccessPolicy - 정책이 더 이상 사용되지 않음	Amazon은 더 DataZone 이상 사용되지 않습니다 AmazonDataZonePortalFullAccessPolicy. 자세한 내용은 Amazon 업데이트를 참조하십시오. DataZone AWS 관리형 정책.	2023년 9월 29일

AmazonDataZoneDomainExecutionRolePolicy - 새 정책	Amazon은 이라는 새 정책을 DataZone 추가했습니다 AmazonDataZoneDomainExecutionRolePolicy. Amazon DataZone `AmazonDataZoneDomainExecutionRole` 서비스 역할의 기본 정책입니다. Amazon은 이 역할을 DataZone 사용하여 Amazon DataZone 도메인의 데이터를 카탈로그, 검색, 관리, 공유 및 분석합니다. 정책을 귀하의 `AmazonDataZoneDomainExecutionRolePolicy` `AmazonDataZoneDomainExecutionRole` 정책에 첨부할 수 있습니다. 자세한 내용은 Amazon DataZone 업데이트를 참조하십시오. AWS 관리형 정책.	2023년 9월 25일
AmazonDataZoneCrossAccountAdmin - 새 정책	Amazon은 사용자가 Amazon DataZone 및 관련 계정을 사용할 수 있도록 하는 새로운 정책을 DataZone 추가했습니다. AmazonDataZoneCrossAccountAdmin 자세한 내용은 Amazon DataZone 업데이트를 참조하십시오. AWS 관리형 정책.	2023년 9월 19일

AmazonDataZoneRedshiftManageAccessRolePolicy - 새 정책	Amazon은 AmazonDataZoneRedshiftManageAccessRolePolicyAmazon 이 데이터에 대한 게시 및 액세스 권한을 DataZone 허용할 수 있는 권한을 부여하는 새 정책을 DataZone 추가했습니다. 자세한 내용은 Amazon DataZone 업데이트를 참조하십시오. AWS 관리형 정책.	2023년 9월 12일
AmazonDataZoneRedshiftGlueProvisioningPolicy - 새 정책	Amazon은 지원되는 데이터 소스와 상호 AmazonDataZoneRedshiftGlueProvisioningPolicy운용하는 데 필요한 권한을 DataZone Amazon에 부여하는 새 정책을 DataZone 추가했습니다. 자세한 내용은 Amazon DataZone 업데이트를 참조하십시오. AWS 관리형 정책.	2023년 9월 12일

AmazonDataZoneGlueManageAccessRolePolicy - 새 정책	Amazon은 Amazon에 게시 DataZone 권한 AmazonDataZoneGlueManageAccessRolePolicy부여라는 새 정책을 DataZone 추가했습니다. AWS 데이터를 카탈로그에 붙입니다. 또한 Amazon에 액세스 DataZone 권한을 부여하거나 액세스 권한을 취소할 수 있는 권한을 부여합니다. AWS 카탈로그에 게시된 자산을 Glue로 작성하십시오. 자세한 내용은 Amazon DataZone 업데이트를 참조하십시오. AWS 관리형 정책.	2023년 9월 12일
AmazonDataZoneFullUserAccess - 새 정책	Amazon은 데이터 포털을 DataZone 통해 Amazon에 대한 전체 액세스 권한을 AmazonDataZoneFullUserAccess부여하는 새로운 정책을 DataZone 추가했습니다. 자세한 내용은 Amazon DataZone 업데이트를 참조하십시오. AWS 관리형 정책.	2023년 9월 12일
AmazonDataZoneFullAccess - 새 정책	Amazon은 다음을 DataZone 통해 Amazon에 대한 전체 액세스를 AmazonDataZoneFullAccess제공하는 새로운 정책을 DataZone 추가했습니다. AWS 관리 콘솔. 자세한 내용은 Amazon DataZone 업데이트를 참조하십시오. AWS 관리형 정책.	2023년 9월 12일

AmazonDataZoneEnvironmentRolePermissionsBoundary - 새 정책	Amazon은 연결된 프로비저닝된 IAM 보안 주체를 제한하는 새 정책을 DataZone 추가했습니다. AmazonDataZoneEnvironmentRolePermissionsBoundary 자세한 내용은 Amazon DataZone 업데이트를 참조하십시오. AWS 관리형 정책.	2023년 9월 12일
관리형 정책 업데이트	AmazonDataZonePreviewConsoleFullAccess 관리형 정책 업데이트. 자세한 내용은 Amazon DataZone 업데이트를 참조하십시오. AWS 관리형 정책.	2023년 6월 13일
관리형 정책 업데이트	AmazonDataZoneProjectDeploymentPermissionsBoundary 관리형 정책 업데이트. 자세한 내용은 Amazon DataZone 업데이트를 참조하십시오. AWS 관리형 정책.	2023년 4월 3일
???	Amazon DataZone (프리뷰) 사용 설명서의 최초 릴리스.	2023년 3월 29일

기계 번역으로 제공되는 번역입니다. 제공된 번역과 원본 영어의 내용이 상충하는 경우에는 영어 버전이 우선합니다.