



Add a permission의

AWS 변환



AWS 변환: Add a permission의

Copyright © 2026 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

Amazon의 상표 및 브랜드 디자인은 Amazon 외 제품 또는 서비스와 관련하여 고객에게 혼동을 일으킬 수 있는 방식이나 Amazon 브랜드 이미지를 떨어뜨리는 방식으로 사용할 수 없습니다. Amazon이 소유하지 않은 기타 모든 상표는 Amazon과 제휴 관계이거나 관련이 있거나 후원 관계와 관계없이 해당 소유자의 자산입니다.

Table of Contents

AWS 변환이란 무엇입니까?	1
용어	1
시작하기	4
설정	4
시작하기 전 준비 사항	4
에 가입 AWS 계정	4
IAM 전용 액세스 시작하기	4
IAM 자격 증명 사용	5
시작하기 AWS Organizations	6
시작하기 AWS IAM Identity Center	7
타사 자격 증명 공급자 사용	8
온보딩	10
자체 S3 버킷 사용	12
AWS 변환 활성화	20
빠른 시작: AWS 변환 시도	21
사용자 관리	22
IAM Identity Center에서 사용자 추가	22
AWS 변환에 사용자 추가	23
IAM 전용 액세스 권한이 있는 사용자 관리	23
공동 작업자 권한 이해	24
AWS 환경 변환	26
언어 설정	28
프로젝트 시작	28
AWS 채팅 변환	29
개발자 도구	31
Kiro 파워	31
에이전트 플러그인	31
IDE 플러그인	32
MCP 서버	32
Authentication	33
AWS 변환을 위한 사용자 지정 에이전트 구축	33
마이그레이션 평가	35
사전 조건	35
마이그레이션 평가 작동 방식	35

인벤토리 데이터 업로드	36
검색 결과 검토	36
인벤토리 범위 관리	37
평가 시나리오 구성	37
평가 기능	38
Amazon EC2 올바른 크기 조정	38
Amazon EBS 스토리지	38
Amazon FSx	38
Amazon RDS for SQL Server	38
Amazon EC2 SQL Server	39
온프레미스 요금	39
지속 가능성	39
비즈니스 가치 평가	40
네트워크 비용	40
지원 비용	40
최종 사용자 컴퓨팅	40
채팅 기반 평가 사용	40
제한된 데이터를 사용한 대략적인 추정	41
채팅을 통해 인벤토리 추가	41
비용 수정 및 서비스 추가	41
시나리오 비교	42
시나리오 생성	42
비교 실행	42
what-if 분석	42
결과물 생성	43
관련 주제	43
사용자 지정	44
사용자 지정 AWS 변환이란 무엇입니까?	44
주요 기능	44
변환 패턴	44
사용자 지정 AWS 변환 작동 방식	46
주요 개념 이해	47
변환 정의	47
변환 레지스트리	47
초안 변환과 게시된 변환 비교	48
참조와 교훈 비교	48

빌드 및 검증 명령	49
지속적인 학습	49
클라이언트 측 기술	50
시작하기	50
사전 조건	50
AWS 변환 CLI 설치	51
인증 구성	52
AWS 리전 구성	54
첫 번째 변환 실행	57
변환 결과 이해	58
사용자 지정 변환 생성	58
AWS 웹 애플리케이션 변환(선택 사항)	59
사용자 지정 변환 명령 소개	59
워크플로	60
변환 실행	60
지속적인 학습	65
고급 구성	66
사용자 지정 변환 생성	79
명령 참조	83
대화형 명령	83
변환 정의 명령	83
단원 명령	86
태그 명령	87
업데이트 명령	87
MCP 명령	87
AWS관리형 변환	88
개요	88
사용 가능한 AWS관리형 변환	88
AWS관리형 변환 사용자 지정	101
일반 사용 사례	102
Lambda 런타임 업그레이드	102
VPC 엔드포인트(AWS PrivateLink)	103
AWS Transform 사용자 지정 VPC 엔드포인트에 대한 고려 사항	104
사전 조건	104
AWS Transform 사용자 지정을 위한 인터페이스 VPC 엔드포인트 생성	104
AWS Transform 사용자 지정에 대한 VPC 엔드포인트 정책 생성	105

온프레미스 컴퓨터를 사용하여 AWS Transform 사용자 지정 엔드포인트에 연결	105
문제 해결	106
로그 위치	106
공통 문제	107
지원 받기	109
S3 액세스 문제	109
CLI 버전 기록	110
지속적인 현대화	119
지속적인 현대화 AWS 혁신이란 무엇입니까?	119
주요 기능	119
분석 유형	120
주요 개념 이해	121
소스	121
리포지토리	121
분석	121
조사 결과	121
문제 해결	121
변환 정의	122
지속적 현대화 AWS 의 작동 방식	122
컴퓨팅 옵션	122
보안 에이전트 설정	124
시작하기	125
사전 조건	125
빠른 시작	125
지속적인 현대화 작업	126
소스 관리	126
리포지토리 검색 및 관리	127
분석 실행	128
조사 결과 관리	128
문제 해결 생성	129
AWS 웹 애플리케이션 변환(선택 사항)	130
개발자 도구	130
에이전트 스킴	131
CLI 참조	132
문제 해결	133
검색 도구	135

워크플로	135
검색 도구 설정	136
사전 조건	136
VMware에 배포	138
Hyper-V에 배포	139
Linux에 배포	140
검색 도구 구성	142
필수 권한	154
VMware vCenter	154
Hyper-V 호스트(Windows)	154
Linux 서버(SSH)	155
Windows 서버(WinRM) - OS 지표	157
Windows 서버(WinRM) - SQL Server 컬렉션	158
Oracle Database(SQL)	159
네트워크 컬렉션	159
빠른 참조: 사용 사례별 최소 권한	160
데이터 수집	161
수집 일정	161
검색된 인벤토리	162
OS 관련 데이터	165
보안 고려 사항	181
검색 도구 VM 보안	181
보안 자격 증명	181
자격 증명 스토리지	183
주의하여 자동 연결 기능 사용	183
CSV 가져오기 보안	184
액세스 고려 사항 취소	185
검색 도구 문제 해결	185
vCenter에 대한 검색 도구 연결 확인	185
WinRM 문제 해결	187
Kerberos 문제 해결	188
Oracle Database 문제 해결	191
SNMP 문제 해결	193
네트워크 수집 오류	194
OS 지표 수집 오류	195
검색된 인벤토리의 액세스 문제	195

SSH 키 인증 문제 해결	195
Linux 설치 관리자 문제 해결	196
일반적인 오류 메시지	197
릴리스 노트	197
커넥터	202
에이전트 작업에 대한 사용자 추적성	202
커넥터 관리	203
마이그레이션(VMware 포함)	205
기능 및 주요 기능	205
아키텍처	205
마이그레이션 작업	206
워크스페이스 가져오기	206
작업 유형	207
작업 생성 및 시작	208
워크스페이스 요약 보고서 다운로드	208
제한 사항	209
소스 데이터 검색	209
마이그레이션 계획 수립	210
워크플로	211
7Rs 권장 사항	213
다이어그램 및 보고서	214
대상 AWS 계정 및 리전 연결	215
1단계: 마이그레이션 유형 선택	215
2단계: MAP 계약	216
3단계: 커넥터 구성	216
랜딩 존 구축	221
커넥터 설정	222
파운데이션 설정	223
워크로드 계정 설계	226
IaC 형식	228
배포 승인 프로세스	229
랜딩 존 리소스에 태그 지정	229
변경 사항 되돌리기	230
관련 리소스	230
네트워크를 로 마이그레이션 AWS	230
1단계: 소스 네트워크 매핑	231

2단계: 추가 구성 파일	232
3단계: 네트워크 토폴로지	233
4단계: 보안 그룹 매핑	236
5단계: 네트워크 검토 및 최적화	238
6단계: 네트워크 다이어그램	241
7단계: 리소스 태그 지정 구성	242
8단계: 네트워크 배포	243
배포된 네트워크 리소스 삭제	245
구성 파일 추출	245
서버 마이그레이션	246
사전 조건 및 마이그레이션 기본값 구성	247
1단계: 마이그레이션 웨이브 설정	249
2단계: 인벤토리 검증 및 확인	252
3단계: 복제 에이전트 배포	253
4단계: 데이터 복제	260
5단계: 테스트	261
5b단계: 애플리케이션을 전환 준비 완료로 표시	261
6단계: 전환	261
서버 수명 주기 상태	262
배포 승인	263
릴리스 노트	263
2026년 6월	263
2026년 5월	264
2026년 4월	264
2026년 3월	264
2026년 2월	264
2026년 1월	264
2025년 12월	265
2025년 10월	265
2025년 9월	265
2025년 8월	265
2025년 5월	265
소스 코드 컨테이너화	267
기능 및 주요 기능	267
컨테이너화 작동 방식	268
사전 조건	268

컨테이너화 워크플로	268
컨테이너화 작업 시작	269
권한	269
기본 정책	270
네트워킹 정책	270
스토리지 정책	270
AWS KMS 정책	271
Amazon ECS 정책	271
Amazon EKS 정책	271
1단계: 보안 고지 사항	271
면책 조항에서 다루는 내용	272
알아야 할 내용	272
2단계: 소스 코드 복제	272
옵션 1: Git 리포지토리	273
옵션 2: Zip 파일 업로드	273
선택 사항: 프라이빗 종속성 구성	274
컨테이너화 기본 설정 확인	274
3단계: 컨테이너화	275
컨테이너화 중에 발생하는 일	275
지원되는 애플리케이션 유형	275
알아야 할 내용	276
4단계: 아티팩트 검토	276
Git 리포지토리의 변경 사항 검토	276
zip 업로드의 변경 사항 검토	276
변경 요청	276
5단계: 이미지 게시	277
게시 중에 발생하는 일	277
알아야 할 내용	277
6단계: IaC 생성	278
Amazon Elastic Kubernetes Service(Kubernetes)	278
Amazon Elastic Container Service(Terraform)	278
자동 검증 및 보안 스캔	279
게시된 이미지 없이 IaC 생성	279
알아야 할 내용	279
7단계: 테스트 인프라 배포	280
테스트 배포 중에 발생하는 일	280

알아야 할 내용	280
인프라에서 반복	280
세션 복구	281
8단계: 테스트 인프라 정리	281
알아야 할 내용	281
9단계: 전환 인프라 배포	281
알아야 할 내용	281
세션 복구	282
메인프레임 현대화	283
기능 및 주요 기능	283
개괄적인 연습	284
루프의 사람(HITL)	284
메인프레임 애플리케이션의 변환에 지원되는 파일 유형	284
메인프레임 AWS 변환에 지원되는 리전 및 할당량	285
현대화 여정	286
1단계: 평가	286
2단계: 동원	287
3단계: 마이그레이션 및 현대화	288
4단계: 운영, 최적화 및 혁신	289
메인프레임 애플리케이션 워크플로의 변환	290
사전 조건: S3에서 프로젝트 입력 준비	290
메인프레임 소스 아티팩트 컬렉션	291
로그인 및 작업 생성	300
변환 진행 상황 추적	300
커넥터 설정	301
작업 계획 평가 및 재구상	305
작업 계획 재구상	310
사용자 지정 작업 계획	310
현대화된 애플리케이션 구축 및 배포	338
사전 조건	339
1단계: 현대화된 코드 검색	339
2단계: 현대화된 애플리케이션 구축	340
3단계: 테스트 환경 구성	340
4단계: 현대화된 애플리케이션 배포	341
5단계: 현대화된 애플리케이션 테스트	341
추가 예	342

풀 스택 Windows 현대화	343
.NET	343
환경	343
기능 및 주요 기능	344
지원되는 버전 및 프로젝트 유형	344
제한 사항	345
인적 개입	345
추가 정보	346
.NET 웹 앱	346
.NET IDE	361
UI 계층 코드 이식	369
변환 보고서	371
모범 사례	372
SQL Server 현대화	377
지원되는 리전	378
기능 및 주요 기능	378
지원되는 버전 및 프로젝트 유형	379
SQL Server 요구 사항	383
애플리케이션 요구 사항	383
인프라 요구 사항	384
리포지토리 요구 사항	385
SQL Server 설정	385
AWS 변환 설정	393
SQL Server 현대화 작업 생성	393
SQL Server 현대화 워크플로	400
변환 후 테스트 및 배포	431
모범 사례 및 문제 해결	433
보안	438
데이터 보호	438
교차 리전 처리	440
데이터 암호화	448
서비스 개선	458
ID 및 액세스 관리	458
대상	459
ID를 통한 인증	459
정책을 사용하여 액세스 관리	461

AWS 변환이 IAM과 작동하는 방식	462
ID 기반 정책 예시	467
문제 해결	476
서비스 연결 역할 사용	478
AWS 관리형 정책	484
AWS 변환 권한 참조	497
규정 준수 확인	499
복원력	499
VPC 엔드포인트(AWS PrivateLink)	499
AWS Transform VPC 엔드포인트에 대한 고려 사항	500
사전 조건	500
에 대한 인터페이스 VPC 엔드포인트 생성 AWS Transform	500
온프레미스 컴퓨터를 사용하여 AWS Transform 엔드포인트에 연결	501
웹 애플리케이션 VPC 액세스	502
작동 방식	502
아키텍처	502
사전 조건	503
VPC 엔드포인트 정책 구성	503
제어된 인터넷 송신 설정	504
Verification(확인)	511
문제 해결	512
비용 고려 사항	513
정리	513
모니터링	515
CloudTrail 로그	515
AWS CloudTrail에서 정보 변환	516
AWS 변환 로그 파일 항목 이해	516
알림	517
이메일 알림	517
할당량	519
지원되는 리전:	523
지원됨 AWS 리전 (기본적으로 활성화됨)	523
Support	525
사전 조건	525
지원 사례 관리 활성화	525
지원 사례 생성	525

지원 사례 보기	526
사례에 통신 추가	527
사례 해결	527
지원 사례 관리 비활성화	527
사용량 원격 측정	528
운영 데이터	529
변경 로그	530
문서 기록	548
.....	dlv

AWS 변환이란 무엇입니까?

AWS 변환은 에이전트 AI 경험을 통해 인프라, 애플리케이션 및 코드의 변환을 가속화하고 간소화하는 데 도움이 되는 서비스입니다. 다양한 워크로드에서 현대화 및 마이그레이션 작업을 간소화하는 전문 도구를 제공합니다.

AWS 변환을 사용하면 다음을 수행할 수 있습니다.

- IBM z/OS 및 Fujitsu GS21을 현대화하고 로 마이그레이션 AWS
- VMware 워크로드를 Amazon EC2로 마이그레이션
- .NET 애플리케이션을 Linux 지원 교차 플랫폼 .NET으로 현대화
- 워크로드의 마이그레이션 준비 상태 평가

AWS 변환은 언어, 프레임워크 및 인프라에 대한 전문 지식을 갖춘 AI 에이전트에게 검색, 계획 및 실행 단계에서 노동 집약적이고 복잡한 변환 작업을 오프로드하는 데 도움이 됩니다. 이 접근 방식을 사용하면 팀이 혁신에 집중할 수 있으며 통합 웹 경험을 통해 복잡한 대규모 프로젝트를 효율적으로 변환할 수 있습니다.

AWS 변환을 사용하는 데 따르는 추가 요금은 없습니다.

용어

이 섹션 내에서 기울임꼴은 다른 용어의 정의 내에서 공식 용어를 나타냅니다.

계정 연결

이 컨텍스트의 계정은 AWS 계정 또는 GitHub 계정과 같은 또는 원격 서비스의 리소스에 대한 고객 소유 컨테이너 AWS 또는 보안 경계에 대한 일반화된 참조입니다.

아티팩트

AWS 변환에서 생성된 출력 결과물입니다.

관리자

관리자는 워크스페이스의 모든 항목을 읽고 변경할 수 있습니다. 변환으로 채팅을 시작하고 AWS , 작업을 시작 및 중지하고, 아티팩트를 업로드/다운로드할 수 있습니다. 관리자는 human-in-the-loop 루프(HITL) 작업을 위해 실행 중인 작업과 상호 작용할 수 있으며, 기본 작업에 병합, 그래프 분해

수행 또는 프로덕션 환경에 코드 배포와 같은 중요한 HITL 작업을 승인할 수 있습니다. 관리자는 [워크스페이스](#), [커넥터](#) 및 사용자를 변경할 수 있습니다.

에이전트

특정 변환 유형을 실행하는 작업별 서비스입니다. VMware 마이그레이션을 예로 들 수 있습니다.

승인자

승인자는 워크스페이스, 커넥터 또는 사용자를 변경할 권한이 없다는 점을 제외하면 관리자와 유사한 권한을 가집니다. 승인자는 [워크스페이스](#), [커넥터](#) 또는 사용자를 변경할 수 없습니다.

자산

변환 [작업에](#) 대한 입력입니다. 예: 고객의 소스 코드, 서버, 데이터베이스, 네트워크. 자산은 [커넥터](#)를 통해 액세스됩니다.

공동 작업자 요청

AWS 변환이 인간에게 무언가를 하도록 요청하는 작업입니다.

커넥터

커넥터는 AWS 변환 외부 시스템의 고객 소유 리소스에 대한 액세스를 허용하는 자산 공급자입니다.

커넥터를 설정할 때 연결하려는 계정의 관리자가 연결을 수락해야 합니다. 연결을 수락하려면 [커넥터 수락자 정책에](#) 부여된 권한이 있어야 합니다.

다음 두 계정은 동일하거나 동일한 AWS Organizations 조직에 있어야 합니다.

- AWS 변환 관리자가 서비스를 활성화하는 계정입니다.
- 변환의 수신 종료에 있을 계정입니다. 이 계정에는 [커넥터를](#) 사용할 수 있는 IAM 역할이 할당되어야 합니다.

기고자

기여자는 워크스페이스의 모든 것을 읽을 수 있습니다. 변환으로 AWS 채팅을 시작하고, 작업을 시작 및 중지하고, 아티팩트를 업로드 또는 다운로드하고, HITL 작업에 대해 실행 중인 [작업](#)과 상호 작용할 수 있습니다. 그러나 메인으로 병합, 그래프 분해 수행 또는 프로덕션 환경에 코드 배포와 같은 중요한 HITL 작업은 수행할 수 없습니다. 또한 기여자는 [워크스페이스](#), [커넥터](#) 또는 사용자를 변경할 수 없습니다.

목표

AWS 변환이 작동하는 사용자 정의 종료 상태입니다. 사용자는 이 문서를 작성한 다음 AWS 변환은 목표를 필요한 경우 사용자와 협력하여 수행하는 일련의 작업으로 변환합니다.

작업

사용자가 정의한 [목표를](#) 이행하기 위해 AWS 변환이 작업하는 장기 실행 프로세스(주/월+)입니다. 여러 [작업](#)과 [공동 작업자 요청](#)으로 구성됩니다.

계획

AWS Transform이 [목표를](#) 달성하기 위해 (인간 사용자의 도움을 받아) 수행하는 [작업](#) 목록입니다.

리더

독자는 AWS 변환 작업의 상태와 결과를 볼 수 있지만 변경할 수는 없습니다. 워크[스페이스](#)의 모든 것을 읽고, 아티팩트를 다운로드하고, [작업을](#) 보고, human-in-the-loop(HITL) 작업을 볼 수 있습니다. 그러나 리더는 AWS 변환에서 변경 작업을 수행할 수 없습니다.

작업

작업의 일부인 개별 [작업](#) 단위입니다.

작업 로그

AWS 변환 및 사용자가 [작업](#)의 일부로 수행한 작업에 대한 로그입니다.

Workspace

[커넥터](#) 및 [작업](#)과 같은 다른 리소스가 포함된 AWS 변환 리소스입니다. [워크스페이스](#)는 권한 경계 역할을 합니다.

AWS 변환 시작하기

주제

- [AWS 변환 설정](#)
- [AWS 변환 활성화](#)
- [빠른 시작: AWS 변환 시도](#)
- [사용자 관리](#)
- [AWS 환경 변환](#)

AWS 변환 설정

시작하기 전 준비 사항

AWS 변환을 설정하기 전에 관리자 액세스 권한이 있는 AWS 계정이 있는지 확인합니다.

Note

proof-of-concept으로 AWS 변환을 시도하거나 테스트 환경에서 변환을 시도하려면 [빠른 시작: AWS 변환 시도](#)를 참조하세요.

에 가입 AWS 계정

를 시작하려면이 AWS필요합니다 AWS 계정. 생성에 대한 자세한 AWS 계정내용은 AWS Account Management 참조 안내서의 [시작하기 AWS 계정](#)를 참조하세요.

IAM 전용 액세스 시작하기

IAM 전용 액세스를 통해 사용자는 기존 AWS 자격 증명으로 인증합니다.

IAM 전용 액세스를 설정하려면:

1. AWS 콘솔에서 AWS 변환으로 이동하여 시작하기를 선택합니다.
2. 계정 설정 구성을 완료합니다.
3. 사용자 액세스에서 IAM 전용 액세스를 선택합니다.

4. 활성화를 선택하여 프로필을 생성합니다.

사용자는 [AWS 로그인](#)을 통해 AWS 변환 웹 애플리케이션에 로그인합니다. 웹 애플리케이션의 사용자 식별자는 IAM 보안 주체를 기반으로 합니다.

Important

설정이 완료된 후에는 자격 증명 공급자를 추가할 수 없습니다. IAM Identity Center 또는 기존 자격 증명 공급자를 사용하여 사용자를 관리하려면 초기 설정 중에 이러한 옵션 중 하나를 선택합니다.

IAM 전용 액세스를 사용하면 프로필 리소스에 대한 `transform:AccessTransformProfile` 권한이 있는 모든 IAM 보안 주체가 AWS 변환에 액세스할 수 있습니다. ID 제공업체 사용자 할당이 아닌 IAM 정책을 통해 사용자 액세스를 관리합니다.

`transform:AccessTransformProfile` 작업은 AWS 변환에 대한 액세스 권한만 부여합니다. AWS 변환 내에서 워크스페이스 역할은 사용자가 수행할 수 있는 작업을 제어합니다. 이러한 역할에는 관리자, 기여자, 승인자 및 읽기 전용이 포함됩니다. Workspace 역할은 사용자 인증 방법에 관계없이 적용됩니다.

IAM 자격 증명 사용

사용자 정보 처리

IAM 보안 주체가 AWS 변환에 액세스하는 경우 서비스는 자격 증명 공급자 기반 액세스와 다르게 사용자 자격 증명을 처리합니다.

사용자 자격 증명

IAM 사용자는 [IAM 보안 주체](#)로 식별됩니다.

이중 자격 증명

자격 증명 공급자 자격 증명(예: IAM Identity Center)과 IAM 세션이 모두 있는 사용자는 AWS 변환에 별도의 두 사용자로 표시됩니다. 이들의 작업은 두 자격 증명 간에 연결되지 않습니다.

이메일 알림

이메일 알림은 SSO 사용자에게만 활성화됩니다. IAM 보안 주체는 여전히 워크스페이스에 추가할 수 있지만 이메일 알림은 받지 않습니다.

감사

IAM API 호출은 호출자의 IAM 자격 증명 AWS CloudTrail 으로 로그인됩니다. 작업에서 IAM 사용자가 수행하는 작업은 AWS 변환 작업 로그에서도 추적할 수 있습니다.

자격 증명 공급자와 함께 IAM 액세스 활성화

IAM Identity Center 또는 타사 자격 증명 공급자를 사용하여 AWS 변환을 설정한 경우 인증하는 추가 방법으로 IAM 액세스를 활성화할 수도 있습니다. 이렇게 하면 IAM 보안 주체가 기존 자격 증명 공급자 사용자와 함께 AWS 변환에 액세스할 수 있습니다.

IAM Identity Center 또는 타사 ID 제공업체를 사용하여 프로필을 생성하면 기본적으로 IAM 액세스가 활성화됩니다. 언제든지 IAM 액세스를 활성화하거나 비활성화하려면:

1. AWS 변환 콘솔에서 설정으로 이동합니다.
2. IAM 자격 증명을 사용한 액세스 AWS 변환에서 IAM 액세스 활성화를 켜거나 끕니다.

IAM 액세스가 활성화되면 자격 증명 공급자 사용자와 IAM 보안 주체 모두 AWS 변환을 사용할 수 있습니다. IAM 사용자와 자격 증명 공급자 사용자는 동일한 워크스페이스에서 협업할 수 있습니다.

시작하기 AWS Organizations

다음 단계에 따라 AWS 변환을 설정합니다.

1. AWS Organizations 관리 계정에 로그인합니다.
2. AWS 변환 서비스로 이동합니다.
3. 조직에서 AWS 변환을 사용하도록 서비스 활성화를 선택합니다.
4. 조직 멤버 계정에 필요한 권한을 구성합니다.
5. 멤버 계정에서 AWS 변환 웹 경험에 액세스합니다.

Note

AWS 솔루션의 Landing Zone Accelerator(LZA)를 사용하여 마이그레이션 기능을 위한 AWS 변환과 함께 랜딩 존을 빌드하려면 AWS 변환 계정과 LZA 설치가 동일한 AWS 조직에 있어야 합니다. LZA 및 AWS 변환 배포에 별도의 조직 IDs를 사용하면 조직 관리 및 리소스 배포에 불일치가 발생할 수 있으므로 지원되지 않습니다. Organizations를 사용하여 LZA 설치를 설정

하는 방법을 알아보려면 구현 가이드의 Landing Zone Accelerator 사용 설명서에서 [고도로 규제된 워크로드 및 복잡한 규정 준수 요구 사항을 지원하는 클라우드 기반 배포](#)를 참조하세요.

AWS

시작하기 AWS IAM Identity Center

다음 단계에 따라 AWS 변환에 IAM Identity Center를 사용하고 사용자 및 그룹을 추가합니다.

기본적으로 변환을 처음 활성화할 때 AWS 변환에 액세스할 수 있는 사용자는 없습니다.

Note

IAM Identity Center는 설정된 리전으로 제한되지 않습니다. AWS 변환에서 지원하지 않는 리전에 IAM Identity Center를 이미 설정한 경우 AWS 변환에 사용할 수 있습니다.

1. IAM Identity Center [의 인스턴스를 활성화하려면의 지침에 따라 IAM Identity Center](#)를 설정합니다.

외부 엔터프라이즈 자격 증명 공급자를 사용하도록 IAM Identity Center를 구성하고 사용자 및 그룹 정보를 IAM Identity Center에 복제합니다.

2. AWS 콘솔에서 AWS 변환을 선택하고 시작하기를 선택합니다.
3. 조직에서 AWS 변환을 사용하도록 서비스 활성화를 선택합니다.
4. 암호화 키를 선택합니다. 기본 선택은 AWS 관리형 키입니다. 사용자 지정 키를 사용하려면:
 - a. 암호화 키에서 암호화 설정 사용자 지정을 선택합니다.
 - b. AWS KMS 키 사용을 선택합니다.
 - c. 기존 키를 선택하거나 새 키를 생성합니다.
 - d. 제출을 선택하여 변경 사항을 적용한 다음 AWS 변환 활성화를 선택합니다.

프로필 보기를 선택하여 구성을 봅니다. 웹 애플리케이션 URL은 사용자가 통합 웹 환경 AWS 변환에 액세스하는 데 사용됩니다.

5. 탐색 창에서 사용자를 선택하고 사용자 또는 그룹 할당을 선택합니다.
6. AWS 변환을 사용하도록 승인하려는 사용자 또는 그룹의 이름을 검색합니다. 검색은 자격 증명 공급자로부터 전파된 사용자 및 그룹을 참조합니다.

7. 그룹 또는 사용자를 선택하고 완료를 선택한 다음 할당을 선택합니다. 이러한 사용자는 AWS 변환 통합 웹 인터페이스를 사용할 수 있는 권한이 있습니다.

타사 자격 증명 공급자 사용

AWS 변환은 Azure Active Directory(Entra ID) 및 Okta Workforce Identity와 같은 타사 ID 제공업체(IdPs)와의 통합을 지원합니다. 이렇게 하면 기존 자격 증명 관리 시스템을 사용자 인증에 사용할 수 있습니다.

사전 조건

타사 자격 증명 공급자 통합을 구성하기 전에 자격 증명 공급자의 사용자에게 이름, 이메일 및 사용자 이름 속성이 구성되어 있는지 확인합니다.

저장된 정보

IdPs와 함께 AWS 변환을 사용하는 경우는 암호화되고 보호되는 최소한의 사용자 정보를 AWS 저장합니다.

저장된 사용자 정보

AWS 변환은 처음 로그인할 때 표시 이름, 이메일 주소, 사용자 이름(preferred_username) 및 고유한 사용자 식별자를 포함한 기본 사용자 프로필 정보를 저장합니다. 이 정보는 고객의 AWS 변환 프로필 구성에 따라 고객 소유 KMS 키 또는 서비스 소유 키를 사용하여 암호화됩니다. 데이터는 AWS 변환의 인증 데이터베이스에 저장되며 초기 로그인 세션 중에만 수집됩니다. 이렇게 하면 다른 사용자를 워크스페이스에 초대할 때 검색 결과가 채워집니다.

데이터 수명 주기

사용자 정보는 AWS 변환 웹 앱에 한 번 이상 로그인한 사용자에게 대해서만 저장되며, 사용자가 AWS 변환에 다시 로그인하지 않고 자격 증명 공급자에서 정보를 업데이트하면 기한이 경과할 수 있습니다. AWS 변환 프로필이 삭제되면 저장된 모든 사용자 정보가 삭제됩니다.

클라이언트 보안 암호 스토리지

설정 중에 제공된 클라이언트 보안 암호는 계정의 서비스 연결 보안 암호(SLS)를 AWS Secrets Manager 통해를 사용하여 저장됩니다.

사용자 식별자 처리

Entra

"oid"(객체 식별자) 클레임을 고유한 사용자 식별자로 사용합니다. 이 식별자는 변경할 수 없으며 Microsoft 테넌트 전체에서 사용자를 고유하게 식별합니다. 이 값은 Entra 콘솔에서 고객에게 표시되며 CloudTrail 로그에 표시됩니다.

Okta 작업 인력 자격 증명

토큰 유형에 따라 사용자 식별에 다른 클레임을 사용합니다. ID 토큰의 "sub" 클레임과 액세스 토큰의 "uid" 클레임입니다. AWS 변환은 인증 중에 두 클레임이 동일한 값을 포함하는지 확인합니다. 이 값은 Okta 콘솔에서 고객에게 표시되며 CloudTrail 로그에 표시됩니다.

Azure Active Directory 설정(Entra ID)

AWS 변환과 Azure Active Directory 통합을 구성하려면:

1. Azure 포털로 이동하여 Azure Active Directory를 선택합니다.
2. 왼쪽 탐색 창에서 관리 > 앱 등록을 선택합니다.
3. + 새 등록을 선택합니다.
4. 애플리케이션 이름을 입력하고 지원되는 계정 유형을 선택한 다음 리디렉션 URI를 비워 두고 등록을 선택합니다.
5. 왼쪽 탐색 창에서 관리 > 매니페스트를 선택합니다.
6. requestedAccessTokenVersion에서 null로 업데이트하고 저장을 선택합니다.
7. 관리 > API 노출을 선택하고 범위 추가를 선택합니다.
8. 기본 구조를 사용하여 애플리케이션 ID URI를 생성합니다 `api://<client-id>`.
9. 범위를 추가합니다 `transform:read_write`.
10. 인증서 또는 보안 암호 추가를 선택하고 새 클라이언트 보안 암호를 생성합니다. 프로필 생성에 필요하므로 이 값을 저장합니다.
11. 엔드포인트를 선택하고 OpenID Connect 메타데이터 문서를 선택하여 발급자 URL을 찾습니다. 메타데이터의 "발급자" 필드는 발급자 URL입니다.
12. 클라이언트 ID, 클라이언트 보안 암호 및 발급자 URL을 사용하여 AWS 변환 콘솔에서 프로필을 생성합니다.
13. 프로필을 생성한 후 플랫폼 추가를 선택하고 웹을 선택한 다음을 입력하여 리디렉션 URI를 추가합니다 `<web-application-url>/login/callback`.

Okta 인력 자격 증명 설정

AWS 변환과 Okta Workforce Identity 통합을 구성하려면:

1. Okta Workforce Identity 콘솔로 이동합니다.
2. 애플리케이션 > 애플리케이션을 선택하고 앱 통합 생성을 선택합니다.
3. OIDC - OpenID Connect 및 웹 애플리케이션을 선택한 후 다음을 선택합니다.
4. 애플리케이션의 이름을 지정하고 권한 부여 유형을 권한 부여 코드로 그대로 두고, 리디렉션 URIs 비워 두고, 사용자 할당을 구성하고, 저장을 선택합니다.
5. 로그인 탭으로 이동하여 발급자를 Dynamic 대신 Okta URL로 설정합니다.
6. 보안 > API로 이동하여 권한 부여 서버를 추가하여 클라이언트 ID를 복사하고 권한 부여 서버의 대상으로 구성합니다.
7. 권한 부여 서버의 범위 탭에서 transform:read_write 범위를 추가합니다.
8. OIDC 애플리케이션이이 권한 부여 서버를 사용하도록 허용하는 액세스 정책을 추가하고 정책에 대한 규칙을 구성합니다.
9. 권한 부여 서버 설정 페이지에서 AWS 변환에서 프로필을 생성하기 위한 발급자 URL을 기록해 둡니다.
10. 애플리케이션 설정의 발급자 URL, 클라이언트 ID 및 클라이언트 보안 암호를 사용하여 AWS 변환에서 프로필을 생성합니다.
11. 프로필을 생성한 후 애플리케이션의 일반 탭에서 리디렉션 URL<web-application-url>/login/callback로 추가합니다.

Note

로그아웃 후 웹 애플리케이션 AWS 변환으로 다시 리디렉션하려면 보안 > API에서 웹 애플리케이션 URL을 신뢰할 수 있는 오리진으로 구성해야 합니다.

사용자 온보딩

이 섹션에서는 AWS 변환에 대한 액세스 권한이 부여된 사용자의 경험을 설명합니다.

초대 수락

사용자가 AWS 변환에 추가되면 다음을 포함하는 이메일 초대를 받게 됩니다.

- 초대에 대한 인사말 및 정보
- AWS 변환 웹 애플리케이션 URL
- 사용자 이름
- 초대를 수락하고 암호를 설정하는 링크

계정을 설정하려면:

1. 사용자가 이메일에서 "초대 수락" 링크를 클릭합니다.
2. "신규 사용자 가입" 페이지에서 암호를 입력하고 확인합니다.
3. 암호는 다음을 포함한 보안 요구 사항을 충족해야 합니다.
 - 8자 이상
 - 하나 이상의 대문자
 - 하나 이상의 소문자
 - 하나 이상의 숫자
 - 하나 이상의 특수 문자
4. 암호를 생성한 후 계정이 성공적으로 생성되었다는 확인 메시지가 표시됩니다.

AWS 변환에 로그인

AWS 변환에 로그인하려면:

1. 초대 이메일에 제공된 웹 애플리케이션 URL AWS 변환으로 이동합니다.
2. 사용자 이름을 입력합니다.
3. 다음을 선택합니다.
4. 암호를 입력합니다.
5. 로그인을 선택합니다.

환영 경험

처음 로그인하면 다음과 같은 AWS 변환 시작 페이지가 표시됩니다.

- 개인 맞춤형 인사말
- 사용 가능한 변환 기능

- 워크스페이스 생성 옵션

시작 페이지에서는 다음을 포함하여 변환에서 사용할 수 있는 AWS 변환 기능에 대한 정보를 제공합니다.

- IBM z/OS 마이그레이션을 로 현대화 AWS
- VMware 워크로드를 Amazon EC2로 마이그레이션
- .NET 애플리케이션을 Linux 지원 교차 플랫폼 .NET으로 현대화
- 워크로드의 마이그레이션 준비 상태 평가

사용자는 먼저 워크스페이스를 생성하거나 팀에 기존 워크스페이스에 추가하도록 요청할 수 있습니다.

자체 Amazon S3 버킷 사용

기본적으로 AWS 변환은 서비스 관리형 Amazon S3 버킷을 사용하여 변환 아티팩트를 저장합니다. 데이터 스토리지, 암호화 및 액세스 정책을 더 잘 제어하기 위해 대신 자체 Amazon S3 버킷을 사용하도록 선택할 수 있습니다.

Note

메인프레임 변환을 위한 Amazon S3 버킷이 있는 경우 해당 S3 커넥터를 계속 사용할 수 있으며 이 기능을 사용할 필요가 없습니다.

Note

Amazon S3 버킷은 상호 작용하는 업로드 및 변환 아티팩트만 저장합니다. 내부 시스템 생성 아티팩트는 버킷에 저장되지 않습니다. 또한 AWS 변환은 버킷의 아티팩트를 인덱싱합니다. 인덱싱된 데이터는 풍부한 채팅 경험을 제공하는 데 사용되는 서비스 관리형 지식 기반에 저장됩니다.

사전 조건

자체 Amazon S3 버킷을 구성하기 전에 다음 요구 사항을 충족하는지 확인합니다.

- 버킷은 AWS 변환이 활성화된 리전과 동일한 AWS 리전에 있어야 합니다.
- 필요한 버킷 정책을 버킷에 적용해야 합니다. 자세한 내용은 [the section called “필수 버킷 정책”](#) 단원을 참조하십시오.
- AWS 변환 웹 애플리케이션을 사용하는 경우 버킷에 CORS를 구성해야 합니다. 자세한 내용은 [the section called “필수 CORS 구성”](#) 단원을 참조하십시오.
- 사용자 지정 AWS KMS 키를 사용하는 경우 필요한 키 정책을 적용해야 합니다. 자세한 내용은 [the section called “KMS 키 정책\(선택 사항\)”](#) 단원을 참조하십시오.

지원되는 암호화 구성

버킷은 다음 암호화 구성 중 하나를 사용해야 합니다.

- SSE-S3(AES256) - KMS 키 필드를 비워 둡니다. AWS 변환은 암호화 헤더를 지정하지 않고 객체를 쓰고 Amazon S3는 S3-managed 키를 사용하여 버킷의 기본 암호화를 적용합니다. 자세한 내용은 Amazon S3 사용 설명서의 [Amazon S3 관리형 키를 사용한 서버 측 암호화\(SSE-S3\) 사용](#)을 참조하십시오.
- 고객 관리형 KMS 키가 있는 SSE-KMS - KMS 키 ARN을 제공합니다. AWS 변환은 제공된 키를 `x-amz-server-side-encryption: aws:kms` 사용하여 로 객체를 씁니다. [the section called “KMS 키 정책\(선택 사항\)”](#)의 내용을 따릅니다.

다음은 지원하지 않습니다.

- 관리형 KMS 키가 있는 SSE AWS-KMS(예: `aws/s3`)
- SSE-C
- DSSE-KMS
- 비대칭 KMS 키 또는 SYMMETRIC_DEFAULT 이외의 키 사양이 있는 KMS 키

Warning

AWS관리형 KMS 키는 지원되지 않습니다. 버킷이 로 암호화된 경우 AWS 변환과 함께 버킷을 사용하기 전에 고객 관리형 키 또는 SSE-S3로 `aws/s3` 마이그레이션합니다.

Amazon S3 버킷 구성

AWS 변환 콘솔에서 자체 Amazon S3 버킷을 사용하도록 AWS 변환을 구성할 수 있습니다.

자체 Amazon S3 버킷을 사용하려면

1. AWS 변환 콘솔에서 설정을 선택합니다.
2. 아티팩트 스토리지에서 내 S3 버킷 사용을 선택합니다. 현재 AWS 계정 또는 다른 계정에서 버킷을 사용할 수 있습니다.
3. 버킷에 Amazon S3 URI를 입력합니다.
4. (선택 사항) KMS 키에 AWS KMS 키 ARN을 입력하여 버킷의 객체를 암호화합니다. 이 필드를 비워 두면 AWS 변환은 암호화 헤더 없이 객체를 쓰고 Amazon S3는 버킷의 기본 암호화 설정을 적용합니다. 자세한 내용은 Amazon S3 사용 설명서의 [Amazon S3 버킷에 대한 기본 서버 측 암호화 동작 설정](#)을 참조하세요.

버킷의 기본 암호화가 SSE-KMS인 경우 이 필드에 고객 관리형 KMS 키 ARN을 입력하고 키 정책을 업데이트합니다. 자세한 내용은 [the section called “KMS 키 정책\(선택 사항\)”](#) 단원을 참조하십시오.

5. 저장을 선택합니다. AWS 변환은 구성을 적용하기 전에 버킷 구성 및 권한을 검증합니다.

구성을 저장한 후 AWS 변환은 버킷을 사용하여 변환 아티팩트를 저장합니다.

Note

AWS 변환은 저장 시에만 구성을 검증합니다. 나중에 버킷 정책, CORS 구성 또는 KMS 키 정책을 변경하는 경우 프로필 설정을 다시 저장하여 다시 검증합니다.

필수 버킷 정책

AWS 변환 액세스 권한을 부여하도록 버킷 정책을 구성해야 합니다. AWS 변환 서비스 보안 주체가 변환 아티팩트를 읽고, 쓰고, 삭제하고, 나열할 수 있도록 Amazon S3 버킷에 다음 버킷 정책을 추가합니다.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": [
          "transform.amazonaws.com"
        ]
      }
    }
  ]
}
```

```

        ]
    },
    "Action": [
        "s3:GetObject",
        "s3:PutObject",
        "s3:DeleteObject",
        "s3:AbortMultipartUpload",
        "s3:ListMultipartUploadParts",
        "s3:PutObjectTagging"
    ],
    "Resource": "arn:aws:s3:::bucket-name/AWSTransform/*",
    "Condition": {
        "StringEquals": {
            "aws:SourceAccount": "profile-account-id",
            "aws:SourceArn": "profile-arn"
        }
    }
},
{
    "Effect": "Allow",
    "Principal": {
        "Service": [
            "transform.amazonaws.com"
        ]
    },
    "Action": "s3:ListBucket",
    "Resource": "arn:aws:s3:::bucket-name",
    "Condition": {
        "StringEquals": {
            "aws:SourceAccount": "profile-account-id",
            "aws:SourceArn": "profile-arn"
        }
    }
}
]
}

```

다음 값을 교체합니다.

- *bucket-name* - Amazon S3 버킷의 이름입니다.
- *profile-account-id* - AWS 변환 프로필과 연결된 AWS 계정 ID입니다.
- *profile-arn* - AWS 변환 프로필의 ARN입니다.

필수 CORS 구성

웹 애플리케이션 AWS 변환을 사용하는 경우 Amazon S3 버킷에서 CORS(Cross-Origin Resource Sharing)를 구성해야 합니다. AWS 변환을 활성화한 후 웹 애플리케이션 도메인을 찾을 수 있습니다. 자세한 내용은 [시작하기](#) 단원을 참조하십시오.

```
[
  {
    "AllowedHeaders": [
      "host",
      "content-type",
      "if-none-match",
      "x-amz-checksum-sha256",
      "x-amz-expected-bucket-owner",
      "x-amz-server-side-encryption",
      "x-amz-server-side-encryption-aws-kms-key-id",
      "x-amz-server-side-encryption-context",
      "x-amz-source-account",
      "x-amz-source-arn"
    ],
    "AllowedMethods": [
      "GET",
      "PUT",
      "HEAD"
    ],
    "AllowedOrigins": [
      "webapp-domain"
    ],
    "ExposeHeaders": [
      "ETag",
      "x-amz-checksum-sha256",
      "x-amz-request-id",
      "x-amz-id-2"
    ],
    "MaxAgeSeconds": 3600
  }
]
```

다음 값을 교체합니다.

- **webapp-domain** – AWS 변환 설정 페이지에서 찾을 수 있는 웹 애플리케이션 오리진 URL(예: `https://1a2b3c4d5e6f7a8b9.transform.us-east-1.on.aws`)입니다. 후행 슬래시는 포함하지 마십시오.

KMS 키 정책(선택 사항)

이 섹션은 버킷이 고객 관리형 KMS 키로 암호화된 경우에만 적용됩니다. 버킷에서 SSE-S3를 사용하는 경우 이 섹션을 건너뜁니다.

버킷 암호화를 위해 자체 AWS KMS 키를 지정하는 경우 키 정책에 다음 문을 추가합니다. AWS 변환은 전달 액세스 세션(FAS)을 사용하여 서비스 보안 주체에 대한 권한 부여를 생성합니다. 이러한 권한 부여는 Amazon S3 버킷의 키 및 액세스 아티팩트를 검증하는 데 사용됩니다.

```
{
  "Sid": "AllowAWSTransformServiceAccess",
  "Effect": "Allow",
  "Principal": {
    "AWS": "arn:aws:iam::key-owner-account-id:root"
  },
  "Action": [
    "kms:CreateGrant",
    "kms:DescribeKey"
  ],
  "Resource": "*",
  "Condition": {
    "StringEquals": {
      "kms:ViaService": "transform.region.amazonaws.com"
    }
  }
}
```

다음 값을 교체합니다.

- **key-owner-account-id** - KMS 키를 소유한 AWS 계정 ID입니다.
- **region** - AWS 변환이 활성화된 AWS 리전입니다(예: `us-east-1`).

기본 버킷으로 다시 전환

언제든지 서비스 관리형 버킷으로 다시 전환할 수 있습니다.

관리형 스토리지 AWS 변환으로 전환하려면

1. AWS 변환 콘솔에서 설정을 선택합니다.
2. 아티팩트 스토리지에서 편집을 선택합니다.
3. AWS 관리형 스토리지 변환을 선택합니다.
4. 저장을 선택합니다.

Warning

변환 작업이 진행되는 동안 스토리지 구성을 전환하면 해당 작업이 실패합니다. 진행 중인 작업에서 이미 생성된 아티팩트도 액세스할 수 없습니다.

Important

서비스 관리형 버킷으로 다시 전환하는 경우:

- 버킷의 아티팩트는 자동으로 마이그레이션되지 않습니다. 아티팩트를 유지하려면 Amazon S3 버킷에서 아티팩트를 다운로드하고 AWS 변환 웹 애플리케이션을 통해 해당 워크스페이스 및 작업에 대한 아티팩트 스토어로 다시 업로드합니다.
- AWS 변환은 KMS 키에 대한 권한 부여를 사용 중지합니다. 버킷에 기록된 객체는 버킷에 남아 있습니다. 더 이상 필요하지 않은 경우 수동으로 삭제합니다.

버킷에 직접 파일 업로드

AWS 변환 웹 애플리케이션을 사용하지 않고도 Amazon S3 버킷에 직접 파일을 업로드할 수 있습니다. 업로드된 파일을 변환 에이전트가 사용할 수 있도록 하려면 해당 파일을 작업의 User Uploads 폴더에 업로드합니다. 이 폴더의 디렉터리 경로는 다음 형식을 사용합니다.

```
AWSTransform/Workspaces/workspace-id/Jobs/job-id/User Uploads/
```

다음 값을 교체합니다.

- *workspace-id* - AWS 변환 워크스페이스의 ID입니다.
- *job-id* - 변환 작업의 ID입니다.

AWS 변환의 각 작업에는 고유한 User Uploads 폴더가 있습니다. 이 경로에 업로드하는 파일은 웹 애플리케이션에 표시되며, 변환 에이전트가 작업을 완료하는 동안 사용할 수 있습니다.

파일 경로에는 ..., // 또는 선행 또는 후행 공백이 포함되어서는 안 됩니다. 이러한 제약 조건을 위반하는 파일은 에이전트에게 표시되지 않습니다.

Important

버킷이 SSE-KMS를 사용하는 경우 직접 업로드할 때마다 다음 헤더를 포함합니다.

```
x-amz-server-side-encryption: aws:kms
x-amz-server-side-encryption-aws-kms-key-id: your-kms-key-arn
```

객체는 AWS 변환 프로필에 등록된 KMS 키로 암호화해야 합니다. 다른 키로 암호화된 객체는 AWS 변환에 액세스할 수 없습니다.

호환성 매트릭스

다음 표에는 AWS 변환과 일반적인 Amazon S3 버킷 기능의 호환성이 요약되어 있습니다.

기능	호환성	참고
버킷 버전 관리	지원됨	수명 주기 규칙을 사용하여 비최신 버전을 관리합니다.
객체 소유권	필수: 버킷 소유자 적용됨	버킷 소유자 기본 설정 및 객체 라이터는 지원되지 않습니다.
ACL	지원되지 않음	버킷에서 ACLs을 비활성화해야 합니다.
객체 잠금(정부 모드)	일부 지원	보존 설정으로 인해 삭제가 차단될 수 있습니다.
객체 잠금(규정 준수 모드)	지원되지 않음	—
퍼블릭 액세스 차단	지원됨	—
요청자 지불	지원되지 않음	—

기능	호환성	참고
S3 액세스 포인트	지원되지 않음	버킷 이름을 사용합니다.
S3 객체 Lambda 액세스 포인트	지원되지 않음	버킷 이름을 사용합니다.
S3 on Outposts	지원되지 않음	—
S3 Express One Zone(디렉터리 버킷)	지원되지 않음	—
교차 리전 버킷	지원되지 않음	—
교차 계정 버킷	지원됨	—
교차 계정 KMS 키	지원되지 않음	—
수명주기 규칙	지원됨	—
CloudTrail 데이터 이벤트	지원됨	—

AWS 변환 활성화

AWS 변환을 활성화하려면:

1. AWS Management Console에 로그인합니다.
2. 콘솔 상단의 검색 창에서 AWS 변환을 검색합니다.
3. 검색 결과에서 AWS 변환을 선택합니다.
4. 현재 리전에서 서비스를 활성화하려면 시작하기를 선택합니다.
5. 선택 사항: IAM Identity Center를 구성합니다. 또한 이후 단계에서 [타사 ID 제공업체\(IdP\)](#)를 사용하도록 선택할 수 있습니다.
6. 암호화 키: 기본 AWS 관리형 키 또는 암호화 설정 사용자 지정을 선택합니다.
7. 선택 사항: 자체 Amazon S3 버킷을 사용합니다. 기본적으로 AWS 변환은 서비스 관리형 Amazon S3 버킷을 사용하여 변환 아티팩트를 저장합니다. 대신 자체 버킷을 사용하도록 선택할 수 있습니다. 자세한 내용은 [자체 Amazon S3 버킷 사용](#) 단원을 참조하십시오.

8. 활성화하려는 AWS 변환 기능을 선택합니다.

- 명령줄 인터페이스(CLI), [사용자 지정 변환](#)을 생성하고 실행하는 데 필요합니다. CLI를 활성화하려면 다운로드 지침을 보고 따르십시오.
- 웹 애플리케이션, 현대화를 위한 에이전트 사용자 인터페이스. 웹 애플리케이션을 사용하려면 웹 애플리케이션 활성화를 선택합니다.

9. AWS 변환 활성화를 선택합니다.

10. 선택 사항: 프로필 보기 활성화를 선택하여 사용자, 설정 및 커넥터 AWS 변환 탭에 액세스하거나 사용자 관리를 선택하여 사용자를 관리합니다.

콘솔의 왼쪽 상단에 있는 메뉴 아이콘을 선택하여 언제든지 사용자, 설정 및 커넥터 탭에 액세스할 수 있습니다.

11. 다음 옵션 중 하나를 선택하여 사용자 액세스를 구성합니다.

- IAM Identity Center
- [타사 ID 제공업체\(IdP\)](#)
- [IAM 전용 액세스](#)

Note

이 선택은 완료되며 AWS 변환을 활성화하면 변경할 수 없습니다.

12. 웹 애플리케이션 활성화를 선택합니다.

13. 필요한 리소스를 생성하는 동안 시스템에 "AWS 변환 활성화"가 표시됩니다.

AWS 변환이 활성화되면 설정 탭에 다음 정보가 표시됩니다.

- 웹 애플리케이션 URL - AWS 변환 웹 애플리케이션에 액세스하기 위한 URL
- IDE용 시작 URL - 통합 개발 환경에서 AWS 변환에 액세스하기 위한 URL
- 리전 - AWS 변환이 활성화된 AWS 리전

빠른 시작: AWS 변환 시도

AWS 변환을 시도하는 가장 쉬운 방법은 독립 실행형 AWS 계정을 사용하는 것입니다. proof-of-concept으로 또는 테스트 환경에서이 작업을 수행할 수 있습니다. 다음 절차를 사용합니다.

1. AWS Management Console에 로그인합니다.
2. AWS 변환 서비스로 이동합니다.
3. 시작하기를 선택하여 서비스를 활성화합니다.
4. 자격 증명 공급자를 선택하고 설정합니다.
5. 사용자를 AWS 변환 서비스에 할당합니다.
6. 서비스가 활성화되면 AWS 변환 웹 애플리케이션 URL이 표시됩니다.
7. 새 브라우저 창에서 해당 URL을 열어 AWS 변환 웹 환경에 액세스합니다.

이제 워크스페이스를 설정할 준비가 되었습니다.

사용자 관리

AWS 변환에 대한 사용자 액세스를 관리하는 방법은 설정 중에 선택한 액세스 모델에 따라 다릅니다. IAM Identity Center를 구성한 경우 IAM Identity Center를 통해 사용자를 추가합니다. 타사 자격 증명 공급자를 구성한 경우 해당 공급자의 사용자를 관리합니다. IAM 전용 액세스를 선택한 경우 사용자 액세스는 IAM 정책을 통해 관리됩니다.

IAM Identity Center에서 사용자 추가

IAM Identity Center에서 사용자를 추가하려면:

1. IAM Identity Center 콘솔로 이동합니다.
2. 탐색 창에서 사용자를 선택합니다.
3. 사용자 추가를 선택합니다.
4. 필수 정보를 입력합니다.
 - 사용자 이름 - 사용자의 고유 식별자(나중에 변경할 수 없음)
 - 이메일 주소 - 사용자의 이메일 주소
 - 이름 및 성 - 사용자 이름
 - 표시 이름 - 사용자 목록에 표시되는 이름입니다.
5. 암호에서 사용자가 암호를 받는 방법을 선택합니다.
 - 이메일 전송 - 이메일을 통해 설정 지침 전송
 - 일회용 암호 생성 - 수동으로 공유할 암호 생성
6. 다음을 선택하여 사용자 정보를 검토합니다.

7. 세부 정보를 검토하고 사용자 추가를 선택합니다.

사용자가 추가되면 IAM Identity Center 계정을 설정하라는 이메일 초대를 받게 됩니다. 초대 링크는 7 일 동안 유효합니다.

이 비디오에서 IAM Identity Center 및 AWS 변환 작업에 대해 알아볼 수도 있습니다.

[VideoTitle](#)

AWS 변환에 사용자 추가

IAM Identity Center에 사용자를 추가한 후 사용자에게 AWS 변환에 대한 액세스 권한을 부여할 수 있습니다.

1. AWS 변환 콘솔로 돌아갑니다.
2. 탐색 창에서 사용자 및 그룹을 선택합니다.
3. 사용자 탭 또는 그룹 탭을 선택합니다.
4. IAM Identity Center에서 추가할 사용자 또는 그룹을 검색하고 선택합니다.
5. 선택한 사용자 또는 그룹에 변환에 대한 액세스 권한을 부여하려면 사용자 및 그룹 할당을 선택합니다. AWS

사용자를 추가하면 초대를 수락하고 로그인할 때까지 사용자 목록에 상태가 “보류 중”으로 표시됩니다.

IAM 전용 액세스 권한이 있는 사용자 관리

IAM 전용 액세스를 AWS 변환을 구성한 경우 사용자 액세스는 IAM 정책을 통해 관리됩니다. 프로필 리소스에 대한 `transform:AccessTransformProfile` 권한이 있는 모든 IAM 보안 주체는 AWS 변환에 액세스할 수 있습니다.

사용자 또는 역할에 AWS 변환에 대한 액세스 권한을 부여하려면:

1. IAM 콘솔로 이동합니다.
2. `transform:AccessTransformProfile` 작업이 포함된 정책을 IAM 사용자 또는 역할에 연결합니다. 예제 정책은 [사용자가 IAM 자격 증명을 사용하여 AWS 변환에 액세스하도록 허용](#)을 참조하세요.

액세스를 취소하려면 IAM 사용자 또는 역할에서 정책을 제거합니다.

공동 작업자 권한 이해

AWS 변환은 워크스페이스 기반 권한 모델을 사용하여 리소스 및 작업에 대한 액세스를 제어합니다. 각 사용자에게는 작업 영역 내에서 수행할 수 있는 작업을 결정하는 특정 역할이 할당됩니다. 사용자는 서로 다른 워크스페이스에서 서로 다른 역할을 가질 수 있습니다.

사용자 역할

AWS 변환은 각 워크스페이스 내에서 5개의 사용자 역할을 지원합니다. 이러한 역할은 워크스페이스의 컨텍스트 내에서 적용되며 사용자는 멤버인 각 워크스페이스에 역할이 할당됩니다. 각 역할에 정의된 액세스 권한은 작업 영역에 구애받지 않으므로 작업 영역 A에 관리자 역할이 있는 사용자 A는 작업 영역 B에 관리자 역할이 있는 사용자 B와 동일한 권한을 갖습니다.

역할 권한

각 역할에 대한 세부 권한:

작업	ResourceType	관리자	승인자	기고자	ReadOnly
생성	워크스페이스	✓	✓	✓	✓
List	워크스페이스	✓	✓	✓	✓
Get	워크스페이스	✓	✓	✓	✓
업데이트	워크스페이스	✓	✗	✗	✗
Delete	워크스페이스	✓	✗	✗	✗
생성	ChatMessage	✓	✓	✓	✗
읽기	ChatMessage	✓	✓	✓	✓
생성	RoleAssociation	✓	✗	✗	✗
읽기	RoleAssociation	✓	✓	✓	✓
업데이트	RoleAssociation	✓	✗	✗	✗
Delete	RoleAssociation	✓	✗	✗	✗

작업	ResourceType	관리자	승인자	기고자	ReadOnly
읽기	CriticalHITLTask	✓	✓	✓	✓
업데이트	CriticalHITLTask	✓	✓	✗	✗
Delete	CriticalHITLTask	✓	✓	✗	✗
읽기	HITLTask	✓	✓	✓	✓
업데이트	HITLTask	✓	✓	✓	✗
Delete	HITLTask	✓	✓	✓	✗
생성	작업	✓	✓	✓	✗
읽기	작업	✓	✓	✓	✓
업데이트	작업	✓	✓	✓	✗
Delete	작업	✓	✓	✓	✗
읽기	작업 로그	✓	✓	✓	✓
생성	아티팩트	✓	✓	✓	✗
읽기	아티팩트	✓	✓	✓	✓
업데이트	아티팩트	✓	✓	✓	✗
Delete	아티팩트	✓	✓	✓	✗
생성	커넥터	✓	✓	✓	✗
읽기	커넥터	✓	✓	✓	✓
업데이트	커넥터	✓	✓	✓	✗
Delete	커넥터	✓	✓	✓	✗

Human-in-the-loop(HITL) 작업

AWS 변환은 표준 및 중요라는 두 가지 유형의 HITL 작업을 제공합니다.

표준 HITL 작업

이는 기고자, 승인자 또는 관리자 역할을 가진 사용자가 수행할 수 있는 일상적인 작업입니다.

중요한 HITL 작업

이는 상당한 영향을 미치는 작업이므로 더 높은 권한 수준이 필요합니다. 그러한 예는 다음과 같습니다.

- 코드를 기본 브랜치에 병합
- 그래프 분해 수행
- 프로덕션 환경에 코드 배포

중요한 HITL 작업은 승인자 또는 관리자 역할이 있는 사용자만 수행할 수 있습니다.

AuthZ 정책에서 표준 HITL 작업과 중요 HITL 작업 간에 차이가 있는지 확인하기 위해 AWS 변환은 표준 HITL 작업을 완료하기 위한 API와 중요한 HITL 작업을 완료하기 위한 API라는 두 개의 개별 HITL APIs를 제공합니다.

AWS 환경 변환

AWS 변환은 자연어 처리를 사용하여 워크로드 변환을 계획하고 실행하는 데 도움이 되는 에이전트 서비스입니다. 주로 대화 인터페이스를 통해 AWS 변환과 상호 작용합니다. 여기서 서비스는 토론의 컨텍스트에 따라 조정되고 응답합니다. 예를 들어 "온프레미VMs를 EC2로 마이그레이션해야 합니다"와 같은 일상적인 언어를 사용하여 현재 아키텍처 및 혁신 목표를 설명하는 것부터 시작할 수 있습니다.

AWS 변환과 대화할 때 서비스는 특정 요구 사항에 맞는 사용자 지정 작업 계획을 구축합니다. 대화 흐름은 동적이며 사용자가 주도하므로 변환 계획을 반복적으로 세분화할 수 있습니다. 대화 중에 "프로덕션 전환 전에 테스트 단계 추가" 또는 "솔루션이 이미 있으므로 백업 단계 제거"와 같은 요청을 하여 작업 계획을 수정할 수 있습니다. 이전 작업으로 돌아가서 다시 수행할 수도 있습니다. AWS 변환은 입력에 따라 계획을 지속적으로 업데이트하여 최종 변환 전략이 기술 및 비즈니스 요구 사항을 충족하도록 합니다.

AWS 변환을 열 때 표시되는 내용은 다음과 같습니다.

- 보기 제어 창: AWS 변환 왼쪽의 좁은 창입니다. 아이콘 중 하나를 선택하여 보기 제어 창의 오른쪽에 표시되는 보기를 선택할 수 있습니다. 보기를 설명하는 도구 설명의 각 아이콘 위에 마우스를 올려 놓습니다. 위에서 아래로 표준 보기 제공은 다음과 같습니다.

- 작업 계획
- 대시보드
- 승인
- 아티팩트
- 작업 로그

일부 워크플로는 추가 보기를 제공합니다.

작업 계획에서 작업하는 경우 보기는 다음과 같습니다.

- Chat
- 승인
- 아티팩트 스토어
- 작업 로그

워크스페이스에 있는 경우 보기가 맨 위에 있습니다.

- 작업
- 아티팩트
- 공동 작업자(사용자)
- 커넥터
- 설정
- 보기 창은 보기 컨트롤 옆에 있습니다.
- 채팅 창은 중앙에 있습니다. 여기에서 AWS 변환과 대화를 수행합니다.

Note

읽기 전용 권한이 있는 사용자는 채팅에서 메시지를 보낼 수 없습니다.

- 오른쪽에는 협업 창이 있습니다. 이는 루프 내 인간(HITL) 활동이 다음과 같이 수행될 때 나타납니다.
 - 데이터 파일 업로드
 - AWS 변환에서 제공하는 정보 및 계획 검토

언어 설정

AWS 변환은 일부 워크플로에 대한 현지화를 지원합니다. 오른쪽 상단의 설정 아이콘을 선택하고 언어 메뉴에서 원하는 언어를 선택하여 웹 애플리케이션의 표시 언어를 변경할 수 있습니다.

지원되는 언어는 다음과 같습니다.

- 영어(미국)
- 영어(영국)
- Deutsch(독일어)
- 스페인어(스페인어)
- Français(프랑스어)
- " (일본어)
- 인도네시아어 바하사(인도네시아어)
- 이탈리아어(이탈리아어)
- 포르투갈어(포르투갈어)
- 한국어(한국어)
- " (")(중국어 간체)
- " (")(중국어 번체)
- Türkçe(터키어)

다음 워크플로는 현지화를 지원합니다.

- [마이그레이션\(VMware 포함\)](#)

Note

기타 AWS 변환 워크플로는 현재 영어로만 제공됩니다. 향후 업데이트에서 추가 워크플로에 대한 현지화 지원이 추가될 수 있습니다.

프로젝트 시작

AWS 변환은 현대화 및 마이그레이션 프로젝트를 안내합니다. 시작하려면 다음을 수행하세요.

1. 프로젝트를 호스팅할 워크스페이스를 생성합니다. 워크스페이스 페이지에서 워크스페이스 생성을 선택합니다. 지침에 따라 워크스페이스를 엽니다.
2. 채팅 창에서 "작업 생성"을 입력합니다.
3. 작업을 선택하고 AWS 변환에서 제공하는 지침을 따릅니다. 입력이 필요한 경우 협업 창이 나타나고 필요한 사항이 설명되어 있습니다.

워크플로 유연성

AWS 변환 워크플로 환경은 현대화 프로젝트의 진행에 유연성을 제공합니다. 채팅 창에서 자연어를 사용하여 다음을 수행할 수 있습니다.

- AWS 변환이 이미 완료된 작업을 재시도하여 그 과정에서 다른 human-in-the-loop 입력을 제공합니다.
- 예를 들어 현대화 소스에 변경 사항이 있는 경우 작업을 다시 실행합니다.

AWS 변환과 채팅

AWS 변환 채팅은 프로젝트의 모든 단계에서 사용할 수 있습니다. 채팅을 열려면 웹 콘솔의 오른쪽 하단에 있는 보라색 육각형 아이콘을 클릭합니다.

채팅을 통해 무엇이든 질문할 수 있습니다. 예를 들어 채팅에 개념을 설명하도록 요청하거나, 프로세스를 안내하거나, AWS 변환 요청 또는 응답을 설명하거나, AWS 변환 보고서를 설명할 수 있습니다.

Note

읽기 전용 권한이 있는 사용자는 채팅에서 메시지를 보낼 수 없습니다.

AWS 채팅 통합 변환

AWS 변환 채팅은 다음과 통합됩니다.

경험 기반 가속화

[경험 기반 가속화\(EBA\)](#)는 AWS 변환 채팅을 통해 제공됩니다. 이를 통해 Windows 워크로드에 대한 EBA 평가를 수행하고 계획을 생성할 수 있습니다. 먼저 CAST에서 평가 결과를 가져올 수 있습니다. 이를 통해 애플리케이션 포트폴리오를 검색할 수 있습니다. 그런 다음 AWS 변환 채팅을 사용하여 비즈니스 요구 사항에 맞는 애플리케이션을 선택할 수 있습니다(예: 복잡성 또는 코드 라인을 기반으로

애플리케이션 필터링). 그런 다음 선택한 애플리케이션에 대한 심층 평가를 수행하고 현대화 계획을 생성할 수 있습니다.

AWS 카운트다운 프리미엄

AWS 변환에 통합된 [AWS Countdown Premium](#)(CDP)은 지정된 AWS 엔지니어링 지원을 통해 지속적인 전문가 지침을 제공합니다. 지정된 CDP 엔지니어는 기술 스택을 심층적으로 분석하여 문제가 발생할 때 개인화된 컨텍스트 인식 지원을 제공합니다. 사용자는 AWS 변환을 활용하여 채팅 인터페이스에서 직접 지원 티켓을 로깅할 수 있습니다. 지원 티켓에는 작업 로그와 작업 계획 세부 정보가 포함되어 지원에서 고객의 컨텍스트를 이해하는 데 도움이 됩니다. 고객 또는 파트너가 CDP 프로그램의 일부인 경우 지원 티켓은 지정된 CDP 엔지니어에게 자동으로 라우팅되어 문제를 디버깅하고, 변환 출력을 해석하고, 신속한 문제 해결을 위한 진행 상황을 촉진할 수 있습니다. 예제:

- .NET 워크로드의 경우 CDP는 리포지토리 커넥터 문제, 종속성 해결 및 변환 후 배포를 지원할 수 있습니다.
- 메인프레임 시나리오에서 CDP는 리팩터링된 Java 코드 문제를 해결하고, 데이터베이스 마이그레이션 도구를 구성하고, CI/CD 파이프라인을 구축하는 데 도움이 될 수 있습니다.
- VMware 마이그레이션에서 CDP는 네트워크 구성, MGN 설정 및 에이전트 설치를 가속화할 수 있습니다.

AWS Skill Builder

[AWS Skill Builder](#)는 채팅을 통해 관련 학습 모듈을 제공합니다. 학습 요구 사항에 대해 AWS 변환 채팅에 요청할 수 있으며 관련 과정 카탈로그를 제공합니다. Skill Builder는 변환 단계를 진행하면서 상황별 마이크로 러닝 경험을 제공합니다.

개발자 도구

에이전트 IDEs, 에이전트 플러그인 및 MCP 서버에서 AWS 변환 에이전트에 액세스할 수 있습니다. 워크플로에 맞는 표면을 선택합니다.

Note

Kiro Power 및 에이전트 플러그인은 MCP 서버를 자동으로 설치합니다. Kiro Power 또는 에이전트 플러그인 없이 MCP 서버를 사용하려면 MCP 서버를 수동으로 설치해야 합니다.

Kiro 파워

[AWS 변환 Kiro Power](#)는 Kiro IDE에서 AWS 변환 에이전트에 대한 전체 액세스 권한을 제공합니다.

AWS 변환 Kiro Power를 설치하려면

1. Kiro IDE를 열고 전원 패널로 이동합니다.
2. 목록에서 AWS 변환을 찾아 설치합니다.
3. Kiro Chat을 열고 Power를 클릭한 다음 Try power를 선택합니다.

또는 전원 패널에서 사용자 지정 전원 추가 > GitHub에서 전원 가져오기를 선택하고 붙여넣습니다.

<https://github.com/kirodotdev/powers/tree/main/aws-transform>

에이전트 플러그인

AWS 변환 에이전트 플러그인은 `plugins/aws-transform` GitHub의 [aws-labs/agent-plugins](#) 디렉터리에서 사용할 수 있습니다. 플러그인은 Claude Code, Codex 및 Cursor를 지원합니다.

플러그인에는 `.claude-plugin`, `.codex-plugin` 및 `.mcp.json` 구성이 포함됩니다. .NET, 메인프레임, VMware, SQL Server 및 사용자 지정 AWS 변환과 같은 모든 변환 에이전트에 대한 액세스를 제공합니다.

Claude Code에를 설치하려면

다음 명령을 실행합니다.

```
/plugin marketplace add awslabs/agent-plugins  
/plugin install aws-transform@agent-plugins-for-aws
```

Codex 또는 Cursor에를 설치하려면

agent-plugins 리포지토리 README의 지침을 따릅니다.

IDE 플러그인

AWS Transform IDE 플러그인은 VS Code 및 Open VSX 호환 편집기에서 사용할 수 있습니다. 변환 정의 생성 및 실행을 포함하여 변환 AWS 사용자 지정 기능을 노출합니다. 또한 현대화 요구 사항, 비즈니스 규칙 및 소스 코드 간의 추적성을 비롯한 메인프레임 기능과 온디맨드 기술 문서를 생성할 수 있는 기능도 제공합니다. 시작하려면 다음 방법 중 하나를 사용하여를 설치합니다.

- VS Code: [VS Code Marketplace](#)에서를 설치합니다.
- Open VSX: [Open VSX 레지스트리](#)에서를 설치합니다.

MCP 서버

MCP 서버를 사용하여 프로그래밍 방식으로 AWS 변환을 MCP 호환 클라이언트와 통합합니다. PyPI 에서 MCP 서버를 로 설치할 수 있습니다 `awslabs.aws-transform-mcp-server`. 워크스페이스 관리, 작업 관리, human-in-the-loop(HITL) 작업, 아티팩트 처리, 커넥터 관리, 채팅 및 리소스 브라우징을 위한 19가지 도구를 제공합니다.

사전 조건

- Python 3.10 이상

설치

Claude 코드

```
claude mcp add awslabs.aws-transform-mcp-server -- uvx awslabs.aws-transform-mcp-server@latest
```

Kiro

에 추가~/.kiro/settings/mcp.json:

```
{
  "mcpServers": {
    "awslabs.aws-transform-mcp-server": {
      "command": "uvx",
      "args": ["awslabs.aws-transform-mcp-server@latest"]
    }
  }
}
```

특정 MCP 클라이언트에 대한 구성 세부 정보는 GitHub의 [aws-transform-mcp-server](#) README를 참조하세요.

Authentication

AWS 변환은 SSO(AWS Identity and Access Management Identity Center) 및 IAM 역할 기반 인증을 지원합니다.

SSO(IAM Identity Center)

AI 어시스턴트에게 "SO로 AWS 변환 구성"을 요청합니다. 어시스턴트는 시작 URL을 제공하고 로그인 을 위해 브라우저를 엽니다.

IAM 역할

환경은 자격 AWS 증명을 자동으로 제공합니다. MCP 클라이언트 구성 env 블록AWS_PROFILE에서 설정하여 특정 프로필을 선택합니다.

AWS 변환에 대한 인증 설정에 대한 자세한 내용은 섹션을 참조하세요[AWS 변환 시작하기](#).

AWS 변환을 위한 사용자 지정 에이전트 구축

[에이전트 빌더 툴킷](#)을 사용하면 AWS 파트너와 고객이 AWS 변환 내에서 작동하는 특정 현대화 요구 사항에 맞는 에이전트를 구축할 수 있습니다.

에이전트 빌더 툴킷을 설치하려면

1. Kiro IDE를 열고 전원 패널로 이동합니다.
2. 목록에서 AWS Transform Agent Toolkit을 찾아 설치합니다.

또는 전원 패널에서 사용자 지정 전원 추가 > GitHub에서 전원 가져오기를 선택하고 붙여넣습니다.
<https://github.com/kirodotdev/powers/tree/main/aws-transform-agent-toolkit>

에이전트 빌더 툴킷을 사용하면 마이그레이션 및 현대화 역량 파트너, ISVs 또는 고객이 특정 사용 사례에 맞는 변환 솔루션을 생성할 수 있습니다. 특수 에이전트, 도구, 지식 기반 및 워크플로를 에이전트 AI 기능 AWS 변환과 통합할 수 있습니다.

에이전트 수명 주기

빌드

Kiro Power를 사용하여 기본 에이전트와 SDK를 결합하여 사용자 지정 에이전트를 직접 작성합니다.

공유

팀과 함께 또는 파트너 네트워크에 에이전트를 배포합니다.

등록

다른 사용자가 검색할 수 있도록 에이전트를 AWS 변환에 등록합니다.

마이그레이션 평가

AWS 변환 평가는 온프레미스 인프라를 로 마이그레이션하는 데 따른 비용, 타당성 및 비즈니스 가치를 평가하는 데 도움이 됩니다. AWS. 평가는 채팅을 통해 자동화된 올바른 크기 조정 권장 사항, 다중 시나리오 비교 및 대화형 구체화를 제공합니다.

마이그레이션 평가를 사용하여 다음을 수행할 수 있습니다.

- Amazon RDS for SQL Server, Amazon EC2, Amazon EBS, Amazon S3 및 Amazon FSx에 대한 예상 비용 가져오기
- 자동 올바른 크기 조정 권장 사항 받기
- 비즈니스 가치 및 지속 가능성에 미치는 영향 평가
- 여러 마이그레이션 시나리오를 나란히 비교
- 채팅을 통해 대화형으로 평가 개선
- 경영진 프레젠테이션 및 세부 보고서 생성

사전 조건

마이그레이션 평가를 생성하기 전에 다음이 있는지 확인합니다.

- AWS 변환 워크스페이스
- 지원되는 형식의 인벤토리 데이터 또는 채팅을 통해 대략적인 추정을 사용할 수 있음
- 평가를 생성하고 실행할 수 있는 적절한 권한

마이그레이션 평가 작동 방식

마이그레이션 평가는 초기 데이터 업로드부터 최종 결과물 생성까지 안내하는 구조화된 워크플로를 따릅니다.

마이그레이션 평가를 완료하려면

1. AWS 변환 워크스페이스에서 마이그레이션 평가 작업을 생성합니다.
2. 온프레미스 인벤토리 데이터를 업로드합니다.
3. AWS 변환이 데이터에서 생성하는 검색 결과를 검토합니다.
4. 서버를 제외하거나 그룹화를 조정하여 인벤토리 범위를 관리합니다.

5. 요금 및 인프라 가정을 사용하여 평가 시나리오를 구성합니다.
6. 평가를 실행합니다.
7. 채팅을 통해 결과를 검토하고 구체화합니다.

결과를 검토한 후 추가 시나리오를 생성하고, 시나리오를 비교하고, 프레젠테이션 및 보고서와 같은 결과물을 생성할 수 있습니다.

인벤토리 데이터 업로드

AWS 변환은 여러 소스의 인벤토리 데이터를 수락합니다. 다음 표에는 지원되는 데이터 형식이 나열되어 있습니다.

데이터 소스	설명
AWS 검색 도구 내보내기 변환	AWS 변환 검색 도구에서 검색한 자동화된 서버 인벤토리
RVTools	VMware 환경에서 ZIP/CSV 또는 Excel 형식으로 내보냅니다. 전체 내보내기와 vInfo 전용 내보내기가 모두 지원됩니다.
CMDB 데이터	구성 관리 데이터베이스 내보내기
파트너 검색 도구	AWS 파트너 검색 도구의 데이터
마이그레이션 평가자	마이그레이션 평가기 콘솔의 Quick Insights 파일
MPA 형식	마이그레이션 포트폴리오 평가 가져오기 파일
AWS 데이터 템플릿 변환	AWS 변환 평가 데이터 템플릿에서 생성된 Microsoft Excel 파일

AWS 변환은 수집 중에 파일 형식을 자동으로 식별합니다. 수집 프로세스는 데이터를 검증하고, 일부 필드가 누락된 경우 부분 데이터를 수락하며, 중복 업로드를 지원합니다. 언제든지 추가 파일을 업로드하여 인벤토리를 보완할 수 있습니다.

검색 결과 검토

AWS 변환은 인벤토리 데이터를 처리한 후 검색 요약을 생성합니다. 요약에는 다음 정보가 포함됩니다.

- 운영 체제별 서버 수
- 물리적 및 가상 서버 분석
- SQL Server 감지
- 스토리지 요약
- 데이터 품질 경고

평가를 진행하기 전에 검색 결과를 검토하여 AWS 변환이 인프라를 올바르게 식별했는지 확인합니다.

인벤토리 범위 관리

검색 결과를 검토한 후 평가 범위를 세분화할 수 있습니다. 다음 작업을 사용하여 인벤토리 범위를 관리합니다.

- 특정 서버 또는 워크로드에 대한 인벤토리 쿼리
- 평가 범위에서 서버 제외
- 서버 그룹화 및 애플리케이션 종속성 검토
- 특수 평가를 위한 SQL Server 워크로드 식별

평가 시나리오 구성

평가를 실행하기 전에 AWS Transform이 권장 사항을 생성하는 데 사용하는 가정을 구성합니다. 언제든지 이러한 가정을 수정하고 다른 구성으로 새 시나리오를 실행할 수 있습니다.

다음 표에는 사용 가능한 가정 범주가 나열되어 있습니다.

가정	설명
요금 모델	데이터베이스 Savings Plans(SQL Server용 Amazon RDS용), 온 디맨드 또는 예약 인스턴스
대상 AWS 리전	마이그레이션된 워크로드를 호스팅하려는 AWS 리전
인스턴스 유형 제외	추천에서 제외할 Amazon EC2 인스턴스 패밀리 또는 유형
Amazon EBS 구성	스토리지의 볼륨 유형 및 성능 설정

가정	설명
SQL Server 라이선싱	Amazon RDS for SQL Server의 경우 기존 보유 미디어 사용 (BYOM) 또는 라이선스 포함(LI), EC2의 경우 기존 보유 라이선스 사용(BYOL)

평가 기능

AWS 변환 평가는 마이그레이션의 여러 차원을 다룹니다. 다음 섹션에서는 각 평가 기능에 대해 설명합니다.

Amazon EC2 올바른 크기 조정

AWS 변환은 온프레미스 서버 사양을 분석하고 적절한 크기의 Amazon EC2 인스턴스를 권장합니다. 권장 사항은 CPU, 메모리 및 성능 요구 사항을 고려합니다.

Amazon EBS 스토리지

AWS Transform은 현재 스토리지 사용량 및 성능 요구 사항에 따라 Amazon EBS 볼륨 유형 및 구성을 권장합니다.

Amazon FSx

AWS 변환은 파일 스토리지 워크로드를 평가하고 지원되는 Amazon FSx 파일 시스템 유형에 대한 예상 비용을 포함하여 Amazon FSx 마이그레이션에 대한 권장 사항을 제공합니다.

Amazon RDS for SQL Server

AWS 변환은 온프레미스 SQL Server 데이터베이스를 Amazon RDS for SQL Server로 마이그레이션하는 데 드는 비용을 평가합니다. AI 기반 에이전트를 사용하는 AWS Transform은 온프레미스 SQL Server 환경을 분석하고 워크로드 요구 사항에 맞는 컴퓨팅 및 메모리 권장 사항과 함께 몇 분 만에 완전한 마이그레이션 비즈니스 사례를 제공하므로 과다 프로비저닝을 방지하고 필요한 만큼만 비용을 지불할 수 있습니다.

RDS for SQL Server 평가에는 다음 기능이 포함됩니다.

- 기존 SQL Server 라이선스를 사용할 수 있는 BYOM(Bring Your Own Media) 라이선스
- 라이선스 포함(LI) 라이선스 옵션

- 온디맨드 요금에 비해 최대 20%의 비용 절감을 제공하는 데이터베이스 Savings Plans을 사용한 비용 최적화
- AWS 마이그레이션 비용 상쇄를 위한 크레딧 및 지원을 제공하는 마이그레이션 가속화 프로그램 (MAP)의 자격 평가

RVTools 내보내기, 구성 관리 데이터베이스(CMDB) 데이터, 변환 검색 도구의 내보내기 및 기타 타사 검색 도구를 포함하여 지원되는 모든 데이터 형식으로 RDS for SQL Server 평가를 시작할 수 있습니다. AWS 가정 시나리오를 생성하여 여러 비용 모델을 리전, 리소스 사용률 및 요금 조건을 포함한 사용자 지정 가정과 비교합니다.

프롬프트 예제:

- “SQL Server 데이터베이스를 RDS for SQL Server로 마이그레이션하는 데 드는 비용 추정”
- “RDS for SQL Server의 BYOM과 라이선스 포함 요금 비교”
- “RDS 워크로드에 대한 데이터베이스 Savings Plans 옵션 표시”

Amazon EC2 SQL Server

AWS 변환은 SQL Server 워크로드를 평가하고 라이선스 분석 및 전용 호스트 매핑을 포함하여 Amazon EC2에서 SQL Server를 실행하기 위한 권장 사항을 제공합니다.

온프레미스 요금

AWS 변환은 현재 온프레미스 비용을 추정하여 AWS 요금과 비교하기 위한 기준을 제공합니다. 채팅을 통해 전반적인 비용을 조정할 수 있습니다. 온프레미스 비용 조정은 PDF 보고서 및 채팅 응답에 반영되지만 PPTX 내보내기에는 반영되지 않습니다.

프롬프트 예제:

- “온프레미스 서버 비용을 서버당 매월 500 USD로 업데이트”
- “연간 데이터 센터 시설 비용 50,000 USD 추가”

지속 가능성

AWS 변환은 로 마이그레이션하여 발생하는 탄소 발자국 감소를 추정합니다 AWS. 채팅을 통해 지속 가능성 지표를 탐색할 수 있습니다.

다음과 같은 프롬프트를 사용해 보세요.

- “이 마이그레이션의 예상 탄소 감소를 보여줘.”
- “의 워크로드에 대한 에너지 효율성 개선은 무엇인가요 AWS?”

비즈니스 가치 평가

AWS 변환은 인프라 비용 절감을 넘어 마이그레이션의 광범위한 비즈니스 가치를 평가합니다. 평가는 직원 생산성, 복원력 및 비즈니스 민첩성을 다룹니다.

다음은 몇 가지 예제 프롬프트입니다.

- "로 마이그레이션하여 직원 생산성 향상 추정 AWS"
- "마이그레이션 후 어떤 복원력 개선을 기대할 수 있습니까?"
- “이 마이그레이션의 비즈니스 민첩성 이점을 보여줘.”

네트워크 비용

AWS 변환은 데이터 전송 및 연결 요구 사항을 포함하여 마이그레이션에 대한 네트워크 관련 비용을 추정합니다.

지원 비용

AWS 변환에는 선택한 AWS 지원 티어를 기반으로 하는 평가에 Support 플랜 비용이 포함됩니다.

최종 사용자 컴퓨팅

AWS 변환은 최종 사용자 컴퓨팅 워크로드를 평가하고 AWS 최종 사용자 컴퓨팅 서비스에 대한 권장 사항을 제공합니다.

채팅 기반 평가 사용

채팅을 통해 AWS 변환과 상호 작용하여 평가를 생성하고 세분화할 수 있습니다. 채팅은 세 가지 상호 작용 모드를 지원합니다.

대화를 계속하여 평가를 반복적으로 세분화할 수 있습니다. AWS 변환은 메시지 전반의 컨텍스트를 유지하고 입력에 따라 평가 결과를 업데이트합니다.

제한된 데이터를 사용한 대략적인 추정

자세한 인벤토리 파일을 업로드하지 않고도 채팅으로 환경을 설명하여 대략적인 비용을 추정할 수 있습니다. 대략적인 추정은 독립 실행형 기능이며 채팅을 통해 업로드된 인벤토리 데이터 또는 데이터 보강과 결합할 수 없습니다.

다음과 같은 프롬프트를 사용할 수 있습니다.

- “Windows 서버 200개와 Linux 서버 150개가 있습니다. 비용을 추정합니다 AWS.”
- “500개의 VMs하기 위한 대략적인 추정치를 알려주세요 AWS.”
- “평균 CPU가 8CPUs에 대한 예상 비용”

채팅을 통해 인벤토리 추가

채팅을 통해 직접 인벤토리 세부 정보를 제공하여 업로드된 파일을 보완하거나 교체할 수 있습니다.

다음과 같은 프롬프트를 사용합니다.

- “128GB RAM이 있는 CPU 4CPUs에서 Oracle을 실행하는 데이터베이스 서버 포함”
- “4개의 CPUs와 16GB RAM이 있는 Linux를 실행하는 20개의 웹 서버 추가”

비용 수정 및 서비스 추가

채팅을 통해 온프레미스 비용을 조정하고 평가에 AWS 서비스를 추가할 수 있습니다.

온프레미스 조정을 위한 프롬프트 예제:

- “향후 하드웨어 새로 고침을 고려하기 위해 온프레미스 비용을 15% 늘립니다.”
- “온프레미스 기준에 연간 유지 관리 비용 100,000 USD 추가”

AWS 변환 평가에서 완전히 지원되지 않는 AWS 서비스에 대한 대략적인 예상 비용을 추가할 수도 있습니다. 이렇게 하면 보다 완전한 분석이 제공되지만 이러한 추정치는 자동 권장 사항보다 정확도가 떨어집니다.

- “마이그레이션된 모든 서버에 대한 AWS 백업 비용 추가”
- “추정치에 Amazon CloudWatch 모니터링 비용 포함”

- “10Gbps 연결에 대한 AWS Direct Connect 비용 추가”

시나리오 비교

다양한 가정으로 여러 평가 시나리오를 생성하고 비교하여 최적의 마이그레이션 전략을 식별할 수 있습니다.

시나리오 생성

다음과 같은 프롬프트를 사용해 보세요.

- “SQL Server 데이터베이스를 RDS for SQL Server로 마이그레이션하기 위한 BYOM 시나리오 생성”
- “RDS for SQL Server용 데이터베이스 Savings Plans을 사용하여 시나리오 생성”
- “EC2의 모든 SQL Server 워크로드에 대한 LI 시나리오 생성”
- “us-west-2의 모든 워크로드를 포함하는 시나리오 생성”

비교 실행

다음은 몇 가지 예제 프롬프트입니다.

- “모든 시나리오에서 비용 비교를 보여줘.”
- “총 소유 비용이 가장 낮은 시나리오는 무엇입니까?”

what-if 분석

완전히 새로운 시나리오를 생성하지 않고 특정 변경 사항이 미치는 영향을 모델링합니다.

프롬프트 예제:

- “SQL Server 워크로드를 EC2 대신 RDS for SQL Server로 옮기면 어떻게 되나요?”
- “DYOM과 RDS for SQL Server에 포함된 라이선스 간의 비용 차이는 무엇입니까?”
- “마이그레이션에서 가장 작은 서버 50개를 제외하면 어떻게 되나요?”
- “스토리지 최적화 인스턴스만 사용하는 경우 어떻게 됩니까?”
- “gp3 볼륨에서 io2 볼륨으로 이동하면 어떤 영향이 있나요?”

결과물 생성

평가를 완료한 후 여러 형식으로 결과물을 생성할 수 있습니다. 다음 표에서는 사용 가능한 출력 형식을 설명합니다.

형식	설명	사용자 지정
PPTX(PowerPoint)	요약 조사 결과 및 권장 사항이 포함된 경영진 프레젠테이션	고정 구조
XLSX(Excel)	서버 수준 권장 사항 및 비용 분석을 사용한 세부 데이터 내보내기	고정 구조
PDF	보고서 문서	채팅을 통해 사용자 지정 가능

관련 주제

- [시작하기](#)
- [사용자 지정 작업](#)
- [검색 도구](#)

사용자 지정

사용자 지정 AWS 변환이란 무엇입니까?

AWS 사용자 지정 변환은 에이전트 AI를 사용하여 소프트웨어, 코드, 라이브러리 및 프레임워크를 대규모로 현대화하여 기술 부채를 줄입니다. 언어 버전 업그레이드, API 및 서비스 마이그레이션, 프레임워크 업그레이드 및 마이그레이션, 코드 리팩터링, 조직별 변환을 비롯한 다양한 시나리오를 처리합니다.

에이전트는 지속적인 학습을 통해 모든 실행 및 개발자 피드백을 개선하여 특별한 자동화 전문 지식 없이도 고품질의 반복 가능한 변환을 제공합니다.

주요 기능

AWS 변환 사용자 지정은 다음과 같은 기능을 제공합니다.

- 자연어 기반 변환 정의 - 자연어, 설명서 및 코드 샘플을 사용하여 사용자 지정 변환 생성
- 변환 실행 - 여러 코드베이스에 걸쳐 일관되고 안정적으로 변환 적용
- 지속적인 학습 - 모든 실행에서 변환 품질 자동 개선
- AWS관리형 변환 - 일반적인 시나리오ready-to-use 수 있는 AWS검증된 변환 사용

변환 패턴

AWS 변환 사용자 지정은 현대화 요구 사항을 해결하기 위해 다양한 변환 패턴을 지원합니다. 각 패턴은 필요한 변경 사항의 범위와 특성에 따라 복잡성 특성이 다릅니다.

패턴	설명	복잡성	예제
API 및 서비스 마이그레이션	기능을 유지하면서 API 버전 또는 동등한 서비스 간에 마이그레이션	중간	AWS SDK v1→v2(Java, Python, JavaScript), Boto2→Boto3, JUnit 4→5, javax→jakarta
언어 버전 업그레이드	동일한 프로그래밍 언어의 최신 버전으로 업그레이드, 새로운 기능	Low-Medium	Java 8→17, Python 3.9→3.13, Node.js

패턴	설명	복잡성	예제
	채택 및 더 이상 사용되지 않는 기능 교체		12→22, TypeScript 버전 업그레이드
프레임워크 업그레이드	동일한 프레임워크의 최신 버전으로 업그레이드하여 주요 변경 사항 해결	중간	Spring Boot 2.x→3.x, React 17→18, Angular 업그레이드, Django 업그레이드
프레임워크 마이그레이션	유사한 목적을 제공하는 완전히 다른 프레임워크로 마이그레이션	높음	Angular→React, Redux→Zustand, Vue.js→React
라이브러리 및 종속성 업그레이드	동일한 언어와 프레임워크를 유지하면서 타사 라이브러리를 최신 버전으로 업그레이드	Low-Medium	Pandas 1.x→2.x, NumPy 업그레이드, Hadoop/HBase/Hive 라이브러리 업그레이드, Lodash 업그레이드
코드 리팩터링 및 패턴 현대화	외부 기능을 변경하지 않고 코드 패턴 현대화 및 모범 사례 채택	Low-Medium	인쇄→로깅 프레임워크, 문자열 연결→f-문자열, 유형 힌트 채택, 관찰성 계층
스크립트 및 File-by-File 번역	파일이 대부분 독립형인 독립 스크립트 또는 구성 파일 번역	Low-Medium	AWS CDK→Terraform, Terraform→CloudFormation, Excel→Python 노트북, Bash→PowerShell
아키텍처 마이그레이션	코드 변경을 최소화하면서 하드웨어 아키텍처 또는 런타임 환경 간에 마이그레이션	중간-높음	x86→AWS Graviton(ARM), 온프레미스→Lambda, 기존 서버→컨테이너

패턴	설명	복잡성	예제
Language-to-Language 마이그레이션	한 프로그래밍 언어에서 다른 프로그래밍 언어로 코드베이스 변환	매우 높음	Java→Python, JavaScript→TypeScript, C→Rust, Python→Go
사용자 지정 및 조직별 변환	고유한 조직 요구 사항 및 특수 현대화 요구 사항	다양	사용자 지정 내부 라이브러리 마이그레이션, 조직별 코딩 표준, 독점 프레임워크 마이그레이션

Note

COBOL/메인프레임 언어의 경우 메인프레임 AWS 변환을 사용합니다. .NET Core로 .NET Framework를 업그레이드하려면 Windows용 AWS 변환을 고려하세요. VMware 마이그레이션의 경우 VMware용 AWS 변환을 AWS고려하세요.

사용자 지정 AWS 변환 작동 방식

AWS 변환 사용자 지정은 일반적으로 여러 코드베이스 또는 모듈이 변환되는 대규모 프로젝트에서 사용됩니다. 팀은 일반적으로 4단계 워크플로를 따릅니다.

변환 정의 - 에이전트에 자연어 프롬프트, 설명서 및 코드 샘플을 제공하여 초기 변환 정의를 생성합니다. 이 정의는 채팅 또는 직접 편집을 통해 반복적으로 세분화할 수 있습니다. AWS관리형 변환을 사용할 때는 이 단계를 건너뛸 수 있습니다.

파일럿 또는 Proof-of-Concept 샘플 코드베이스에서 변환을 테스트하고 결과를 기반으로 구체화합니다. 이 검증 단계는 전체 변환의 비용과 노력을 추정하는 데 도움이 됩니다. 지속적인 학습은 이 단계에서 품질을 개선합니다.

확장된 실행 - 개발자가 결과를 검토하고 검증하여 CLI를 사용하여 자동 대량 실행을 설정합니다. 웹 애플리케이션을 사용하여 진행 상황을 모니터링하고 여러 리포지토리에서 변환을 추적합니다.

모니터링 및 검토 - 지속적인 학습은 변환 품질을 자동으로 개선합니다. 이전 실행에서 추출한 교훈을 검토하여 품질 표준을 충족하는지 확인하고 유용하지 않은 내용을 보관합니다.

주요 개념 이해

이 섹션에서는 사용자 지정 AWS 변환 작업을 위한 주요 개념을 설명합니다.

변환 정의

변환 정의에는 특정 코드 변환을 수행하는 데 필요한 지침과 지식이 포함되어 있습니다. 스킬로 표현되며 다음으로 구성됩니다.

- SKILL.md (필수) - 코어 변환 로직 및 실행 지침이 포함된 YAML 프론트미터(name 및 description 필드)를 사용한 마크다운의 지침
- references/ 폴더(선택 사항) - 변환 실행 중에 필요에 따라 로드된 설명서
- scripts/ 폴더(선택 사항) - 실행 중에 변환이 다운로드하고 실행하는 스크립트

AWS 변환 CLI는 실행, 검사 또는 수정에 필요한 경우 변환 정의를 현재 디렉터리에 자동으로 다운로드합니다.

Important

변환을 게시할 때 디렉터리에는 SKILL.md 선택적으로 references/ 폴더, scripts/ 폴더 또는 둘 다만 포함되어야 합니다. 다른 파일 또는 하위 디렉터리는 허용되지 않습니다.

Note

CLI 버전 2.0 이상에서는 기술 형식을 사용합니다. 기존 변환 정의는 CLI에서 자동으로 처리됩니다.

변환 레지스트리

변환 레지스트리는 변환 정의를 저장하고 관리하기 위한 AWS 계정의 중앙 집중식 리포지토리입니다. 레지스트리의 변환은 다음과 같을 수 있습니다.

- 를 사용하여 나열됨 `atx custom def list`
- 여러 코드베이스에서 실행됨
- AWS 계정의 다른 사용자와 공유

- 버전 관리형

⚠ Important

변환 정의는 계정별로 다릅니다. 다른 AWS 계정에서 변환을 사용하려면 해당 계정에 별도로 게시해야 합니다.

초안 변환과 게시된 변환 비교

AWS 변환 사용자 지정은 레지스트리의 변환에 대해 두 가지 상태를 지원합니다.

초안 변환은 진행 중이거나 테스트되지 않은 변환 정의입니다. 특정 버전으로 저장되며 해당 특정 버전을 참조하는 사용자가 검색, 업데이트 및 실행할 수 있습니다. 초안은 팀과 변환을 공유할 준비가 되기 전에 반복 개발, 테스트 및 개선에 유용합니다. 초안은 특정 대화에도 연결됩니다. CLI를 다시 시작하는 경우를 사용하여 이전 CLI를 복원 `atx --conversation-id {id}` 할 수 있습니다.

게시된 변환은 필요한 IAM 권한이 있는 다른 사용자가 실행할 수 있도록 계정의 변환 레지스트리에서 사용할 수 있습니다. 게시된 변환은를 사용하여 검색할 수 있습니다 `atx custom def list`.

일반적인 워크플로는 다음과 같습니다.

1. 로컬에서 변환 생성
2. 테스트를 위해 초안으로 저장(`atx custom def save-draft`)
3. 구체화 및 검증
4. 게시하여 팀과 공유(`atx custom def publish`)

변환을 초안으로 저장하지 않고 직접 게시할 수도 있습니다.

참조와 교훈 비교

AWS 변환 사용자 지정은 두 가지 유형의 지식을 사용하여 변환 품질을 개선합니다.

참조는 변환 정의의 `references/` 폴더에 저장된 사용자 제공 설명서입니다. 참조는 텍스트 파일만 지원하며(모든 파일의 경우 최대 총 10MB) 일반적으로 설명서, API 사양, 마이그레이션 가이드 및 코드 샘플을 포함합니다. 참조는 변환 실행 중에 필요에 따라 로드됩니다. 대화형 모드에서 변환 정의를 생성하거나 업데이트할 때 참조를 추가합니다.

단원은 이전 변환 실행에서 자동으로 추출됩니다. 지속적 학습 시스템은 실행 궤적, 개발자 피드백 및 변환 중에 발생하는 코드 수정에서 이를 생성합니다. 관련 교훈을 범주로 그룹화하여 함께 검토할 수 있습니다. 선결제를 제공하는 참조와 달리, 여러 코드베이스에서 변환을 실행하면 시간이 지남에 따라 교훈이 누적되고 시스템은 이를 자동으로 적용하여 향후 실행을 개선합니다. 를 사용하여 대화형으로 단원을 검토하고 관리합니다

빌드 및 검증 명령

빌드 또는 검증 명령은 변환 프로세스 중에 코드를 검증하는 방법을 지정하는 선택적 파라미터입니다. 이 명령은 코드 무결성을 보장하기 위해 변환 중 다양한 지점에서 실행됩니다.

결과를 검증하고 검증에 실패할 경우 문제를 반환하는 명령을 제공하는 것은 지속적인 학습을 통해 변환 품질을 개선하는 데 매우 중요합니다. 빌드 또는 검증이 필요하지 않은 경우 입력에서 생략합니다.

예제와 자세한 지침은 워크플로 섹션의 빌드 및 검증 명령을 참조하세요.

지속적인 학습

지속적인 학습은 모든 변환 실행의 피드백을 자동으로 캡처하고 시간이 지남에 따라 변환 품질을 개선하는 시스템입니다. 시스템은 다음을 통해 정보를 수집합니다.

- 명시적 피드백 - 대화형 모드에서 제공되는 설명 및 코드 수정
- 암시적 관찰 - 코드를 변환하고 디버깅하는 동안 에이전트가 발견하는 문제

지속적 학습 시스템은 이 정보를 처리하여 향후 변환을 개선하기 위해 변환 정의에 추가하는 교훈을 생성합니다. 시스템은 변환이 완료된 후 학습 프로세스를 자동으로 실행하므로 사용자의 추가 입력이 필요하지 않습니다.

Important

교훈은 변환별로 다르며 다른 변환 또는 다른 고객 계정 간에 공유되지 않습니다.

단원 관리

시스템은 자동으로 교훈을 생성하지만 사용자는 향후 실행에 적용되는 교훈을 계속 제어할 수 있습니다. `atx custom def learnings` 명령은 변환이 누적한 교훈을 검토하고 큐레이션하기 위한 대화형 터미널 세션을 엽니다.

이 세션에서는 다음을 수행할 수 있습니다.

- 범주로 그룹화된 단원을 찾아보고 각 범주에 포함된 활성 단원의 수를 확인합니다.
- 단원을 열어 단원 본문, 그 영향, 참조한 이전 실행 수를 비롯한 전체 세부 정보를 읽습니다.
- 시스템이 향후 실행에 적용하지 못하도록 단원을 보관하고 필요한 경우 나중에 복원합니다.
- 더 이상 유용하지 않은 보관된 단원을 영구적으로 삭제합니다.

단계별 지침은 [the section called “지속적인 학습”](#) 섹션을 참조하세요.

클라이언트 측 기술

클라이언트 측 기술은 변환 실행 중에 에이전트를 확장하는 추가 기능입니다. 수행할 변환을 정의하는 변환 정의와 달리 클라이언트 측 기술은 에이전트가 변환 중에 내장 기능과 함께 사용할 수 있는 보조 도구, 스크립트 및 지침을 제공합니다.

클라이언트 측 스킬은 프로젝트 수준 및 사용자 수준 디렉터리에서 발견됩니다. 리포지토리에 특정한 표준을 적용할 때는 프로젝트 수준에서, 모든 프로젝트에 적용할 때는 사용자 수준에서 기술을 배치합니다. 프로젝트 수준 스킬은 코드 리포지토리 경로가 제공된 경우에만 사용할 수 있습니다. 자세한 구성 및 사용량은 섹션을 참조하세요 [the section called “클라이언트 측 기술”](#).

시작하기

이 섹션에서는 사용자 지정 AWS 변환을 설정하고 첫 번째 변환을 실행하는 방법을 설명합니다.

사전 조건

사용자 지정 AWS 변환을 설치하기 전에 다음이 있는지 확인합니다.

지원되는 플랫폼

AWS 사용자 지정 변환은 다음 운영 체제를 지원합니다.

- Linux - 모든 Linux 배포에 대한 전체 지원
- macOS - macOS 시스템에 대한 전체 지원
- Windows - Windows 터미널 및 PowerShell을 사용하여 기본 Windows에 대한 전체 지원(Windows에서는 `atx ct` 명령이 아직 지원되지 않음)

- Linux용 Windows 하위 시스템(WSL) - WSL에서 실행할 때 지원됨

필수 소프트웨어

- Node.js 22 이상 - <https://nodejs.org/en/download> 다운로드
- Git - 변환을 실행하려면 설치되고 작업 디렉터리가 유효한 Git 리포지토리어야 합니다. 를 실행
`git init; git add .; git commit -m "Initial commit"`하여 작업 디렉터리에서 Git 리포지토리를 초기화합니다.

네트워크 요구 사항

다음 엔드포인트에 액세스할 수 있는 인터넷 연결이 필요합니다.

- `transform-cli.awsstatic.com`
- `transform-custom.<region>.api.aws`
- `*.s3.amazonaws.com`

인터넷 제한 환경에서 작업하는 경우 방화벽 규칙을 업데이트하여 이러한 URLs.

AWS 변환 CLI 설치

권장 설치 방법은 설치 스크립트를 사용하는 것입니다. 운영 체제의 탭을 선택합니다.

AWS 변환 CLI를 설치하려면

1. 설치 스크립트를 실행합니다.

Linux and macOS

```
curl -fsSL https://transform-cli.awsstatic.com/install.sh | bash
```

Windows (PowerShell)

기본 Windows에서는 PowerShell을 사용하여 Windows 터미널에서 설치 스크립트를 실행합니다.

```
irm https://transform-cli.awsstatic.com/install.ps1 | iex
```

2. 설치를 확인합니다.

```
atx --version
```

명령에는 AWS Transform CLI의 설치된 버전이 표시되어야 합니다.

인증 구성

AWS 사용자 지정 변환에는 서비스로 인증하기 위한 AWS 자격 증명이 필요합니다. 다음 방법 중 하나를 사용하여 인증을 구성합니다.

환경 변수

다음 환경 변수를 설정합니다.

Linux and macOS

```
export AWS_ACCESS_KEY_ID=your_access_key
export AWS_SECRET_ACCESS_KEY=your_secret_key
export AWS_SESSION_TOKEN=your_session_token
```

Windows (PowerShell)

```
$env:AWS_ACCESS_KEY_ID="your_access_key"
$env:AWS_SECRET_ACCESS_KEY="your_secret_key"
$env:AWS_SESSION_TOKEN="your_session_token"
```

AWS_PROFILE 환경 변수를 사용하여 프로파일을 지정할 수도 있습니다.

Linux and macOS

```
export AWS_PROFILE=your_profile_name
```

Windows (PowerShell)

```
$env:AWS_PROFILE="your_profile_name"
```

Note

PowerShell\$env:에서 로 설정된 환경 변수는 현재 세션에만 적용됩니다. 세션 간에 유지하려면 시스템 속성 > 환경 변수를 통해 설정하거나 사용하십시오 [System.Environment]::SetEnvironmentVariable().

AWS 자격 증명 파일

Linux 및 macOS 또는 Windows의 ~/.aws/credentials에 있는 자격 증명 파일%USERPROFILE%\aws\credentials에서 AWS 자격 증명을 구성합니다.

```
[default]
aws_access_key_id = your_access_key
aws_secret_access_key = your_secret_key
```

IAM 권한

자격 AWS 증명에는 AWS 사용자 지정 변환 서비스를 호출할 수 있는 권한이 있어야 합니다.

[AWSTransformCustomFullAccess](#) AWS 관리형 정책을 IAM 사용자 또는 역할에 연결하는 것이 좋습니다. 이 정책은 계정으로 CloudWatch 지표를 내보내는 데 필요한 [서비스 연결 역할](#)을 생성할 수 있는 권한을 포함하여 사용자 지정 AWS 변환에 대한 전체 액세스 권한을 제공합니다.

보다 세분화된 제어를 위해 AWS Transform 사용자 지정은 다음과 같은 AWS 관리형 정책도 제공합니다.

- [AWSTransformCustomExecuteTransformations](#) - 변환을 실행할 수 있는 액세스 권한을 제공합니다.
- [AWSTransformCustomManageTransformations](#) - 변환 리소스를 생성, 업데이트, 읽기 및 삭제하고 변환을 실행할 수 있는 액세스 권한을 제공합니다.

이러한 정책에 대한 자세한 내용은 [AWSAWS 변환에 대한 관리형 정책을 참조하세요](#). 리소스 수준 권한이 있는 사용자 지정 IAM 정책은 사용자 [AWS 지정 IAM 서비스 권한 부여 변환 참조 가이드](#)를 참조하세요.

 Note

- 변환 정의는 ARNs(Amazon AWS 리소스 이름)이 있는 리소스입니다. IAM 정책을 사용하여 IAM 정책 리소스 문에 변환 ARN을 지정하여 특정 변환 또는 변환 그룹에 대한 액세스를 제어할 수 있습니다. 태그는 그룹화된 액세스 제어에 사용할 수 있습니다.
- AWS IAM Identity Center는 AWS 변환에 액세스하는 데 필요하지만 CLI를 사용하는 데 필요하지 않습니다.

AWS 리전 구성

AWS 사용자 지정 변환은 특정 AWS 리전에서 사용할 수 있으며 표준 AWS CLI 우선 순위를 사용하여 리전 구성을 자동으로 감지합니다.

지원되는 리전:

AWS 변환 사용자 지정은 다음 AWS 리전에서 사용할 수 있습니다.

- us-east-1 (미국 동부 - 버지니아 북부)
- eu-central-1 (유럽 - 프랑크푸르트)
- eu-west-2 (유럽 - 런던)
- ca-central-1 (캐나다 - 중부)
- ap-northeast-1 (아시아 태평양 - 도쿄)
- ap-northeast-2 (아시아 태평양 - 서울)
- ap-southeast-2 (아시아 태평양 - 시드니)
- ap-south-1 (아시아 태평양 - 뭄바이)

리전 결정 방법

CLI는 이러한 소스를 우선순위에 따라 확인하여 사용할 리전을 결정합니다.

1. AWS_REGION 환경 변수(가장 높은 우선 순위)
2. AWS_DEFAULT_REGION 환경 변수
3. AWS 구성 파일에서 선택한 프로필(AWS_PROFILE 환경 변수를 통해)
4. AWS 구성 파일의 기본 프로필

5. 구성을 찾을 수 없는 us-east-1 경우 기본 대체

Note

AWS 구성 파일은 Linux 및 macOS 또는 Windows~/.aws/config의 %USERPROFILE%\ .aws\config에 있습니다.

Note

ATX_CUSTOM_ENDPOINT이 설정된 경우 리전은 엔드포인트 URL에서 추출되고 다른 모든 설정을 재정의합니다.

리전 설정

다음 방법 중 하나를 선택하여 리전을 구성합니다.

옵션 1: 환경 변수(임시 사용 권장):

Linux and macOS

```
export AWS_REGION=<your-region>
```

Windows (PowerShell)

```
$env:AWS_REGION="<your-region>"
```

옵션 2: AWS CLI 구성(영구적 설정에 권장):

```
aws configure set region <your-region>
```

옵션 3: 프로필별 구성:

Linux and macOS

```
aws configure set region <your-region> --profile your_profile_name
```

```
export AWS_PROFILE=your_profile_name
```

Windows (PowerShell)

```
aws configure set region <your-region> --profile your_profile_name  
$env:AWS_PROFILE="your_profile_name"
```

옵션 4: 직접 파일 편집:

AWS 구성 파일을 직접 편집합니다(~/.aws/configLinux 및 macOS의 경우 또는 Windows%USERPROFILE%\aws\config의 경우).

```
[default]  
region = <your-region>  
  
[profile your_profile_name]  
region = <your-region>
```

리전 구성 확인

사용자 지정에서 사용할 리전 AWS 변환을 확인하려면:

현재 리전 설정 확인:

```
aws configure get region
```

환경 변수를 확인합니다.

Linux and macOS

```
echo "AWS_REGION: $AWS_REGION"  
echo "AWS_DEFAULT_REGION: $AWS_DEFAULT_REGION"  
echo "AWS_PROFILE: $AWS_PROFILE"
```

Windows (PowerShell)

```
echo "AWS_REGION: $env:AWS_REGION"  
echo "AWS_DEFAULT_REGION: $env:AWS_DEFAULT_REGION"  
echo "AWS_PROFILE: $env:AWS_PROFILE"
```

디버그 로그에서 자세한 리전 확인 보기:

Linux and macOS

```
tail -f ~/.aws/atx/logs/debug.log
```

Windows (PowerShell)

```
Get-Content "$env:USERPROFILE\.aws\atx\logs\debug.log" -Wait -Tail 10
```

리전 소스를 보여주는 로그 출력의 예:

```
2026-01-07 22:34:28 [DEBUG]: Initializing FrontendServiceClient with config:
{
  "endpoint": "https://transform-custom.us-east-1.api.aws",
  "region": "us-east-1",
  "regionSource": "AWS_REGION"
}
```

regionSource 필드는 리전이 파생된 위치를 보여줍니다(예: "aws-config (profile: default)", "AWS_REGION", "default").

Important

리전 구성이 지원되지 않는 리전을 가리키는 경우 CLI는 구성을 지원되는 리전으로 업데이트 하는 지침과 함께 명확한 오류 메시지를 표시합니다.

첫 번째 변환 실행

시작하는 가장 빠른 방법은 AWS관리형 변환을 사용하는 것입니다. AWS관리형 변환은 설정 없이 바로 사용할 수 있는 사전 구축되고 AWS검증된 변환입니다.

AWS관리형 변환을 대화형으로 실행하려면:

```
atx
```

그런 다음 에이전트에게 변환을 실행하도록 요청합니다.

```
Execute the AWS/java-aws-sdk-v1-to-v2 transformation on the codebase at ./my-java-project
```

변환을 대화형으로 실행하려면:

```
atx custom def exec -n AWS/java-aws-sdk-v1-to-v2 -p ./my-java-project -c "mvn clean install" -x -t
```

실행 모드, 구성 옵션 및 명령 플래그에 대한 자세한 내용은 섹션을 참조하세요 [the section called “명령 참조”](#).

변환 결과 이해

변환이 완료되면 AWS 변환 사용자 지정은 결과를 설명하는 보고서를 제공합니다. 변환이 검증되지 않은 경우(예: Java 애플리케이션의 성공적인 빌드) 보고서는 추가 작업에 대한 권장 사항을 제공합니다.

대부분의 변환은 Git을 사용하여 중간 변환을 커밋하는 여러 단계로 수행됩니다. 표준 Git 명령을 사용하여 변환의 변경 사항을 검토할 수 있습니다.

```
git status
git log
git diff <original commit-id>
```

사용자 지정 변환 생성

AWS관리형 변환이 요구 사항을 충족하지 않는 경우 특정 요구 사항에 맞게 사용자 지정 변환을 생성할 수 있습니다.

사용자 지정 변환을 생성하려면

1. 대화형 모드에서 AWS 변환 CLI를 시작합니다.

```
atx
```

2. 에이전트에게 새 변환을 생성하도록 알리고 요구 사항을 설명합니다.
3. 품질 향상을 위해 설명서 및 코드 샘플과 같은 참조 자료를 제공합니다.
4. 변환을 반복적으로 테스트하고 구체화합니다.
5. 조직의 변환 레지스트리에 게시합니다.

사용자 지정 변환 생성에 대한 자세한 지침은 섹션을 참조하세요 [the section called “워크플로”](#).

AWS 웹 애플리케이션 변환(선택 사항)

AWS 변환 웹 애플리케이션은 여러 리포지토리에서 대규모 변환 캠페인을 모니터링하기 위한 선택적 인터페이스입니다. AWS 변환 웹 애플리케이션을 사용하기 전에 조직의 AWS 변환에 액세스하려면 사용자 자격 증명을 활성화해야 합니다. AWS 변환 활성화에 대한 자세한 내용은 [AWS 변환 설정을 참조하세요](#).

AWS 변환 웹 애플리케이션을 사용하려면:

1. <https://aws.amazon.com/transform/> 방문하여 AWS IAM Identity Center 자격 증명을 사용하여 로그인합니다.
2. AWS 변환 웹 애플리케이션에서 "사용자 지정/코드" 작업 유형을 선택합니다.
3. 에이전트에게 사용하려는 변환 정의의 이름을 알려줍니다.
4. 웹 애플리케이션은 팀과 공유할 수 있는 AWS 변환 CLI 명령을 제공합니다. 이 명령은 변환 정의를 호출하고 실행 결과를 웹 애플리케이션에 로깅합니다.
5. 변환 결과를 캡처한 후 대시보드에서 통계, 시간 절약 추정값을 보고 작업 진행 상황에 대해 질문합니다.

웹 애플리케이션은 여러 코드베이스에서 변환을 중앙 집중식으로 모니터링해야 하는 엔터프라이즈 규모의 작업을 위해 설계되었습니다.

Note

AWS 변환 웹 애플리케이션에 액세스하려면 IAM Identity Center가 필요합니다. CLI에는 IAM Identity Center가 필요하지 않으며 표준 AWS 자격 증명만 필요합니다.

사용자 지정 변환 명령 소개

다음은 사용자 지정 변환에 사용할 수 있는 몇 가지 명령입니다. 명령의 전체 목록은 사용자 [AWS 지정 변환 변환 명령 참조에 있습니다](#).

- `atx custom`
 - 사용자 지정 변환 대화형 환경을 실행하여 변환의 생성, 검색, 실행 및 구체화를 허용합니다.
 - 의 기본 명령입니다 `atx`.

- `--trust-all-tools (-t)`는 선택 사항이며 에이전트가 요청한 모든 도구 요청을 암시적으로 허용합니다. 특히 프로덕션 환경에서는 주의해야 합니다. 신뢰 [설정 파일을 사용하여 특정 도구 및 명령에 대한 도구 신뢰를](#) 구성할 수 있습니다.
- `atx custom --help` | `atx custom -h`
 - 도움말 메뉴를 표시합니다.
 - 각 명령에는와 같은 도움말 메뉴도 포함되어 있습니다 `atx custom def exec --help`.
- `atx --version` | `atx -v`
 - 버전을 표시합니다.
 - 버전 번호는 릴리스마다 변경됩니다.
- `atx custom def list`
 - 변환 레지스트리에서 사용 가능한 변환 목록을 인쇄합니다.
- `atx custom def exec`
 - 변환을 실행합니다.
- `atx custom def learnings`
 - 대화형 세션을 열어 변환이 이전 실행에서 학습한 교훈을 보고 관리합니다.
- `atx mcp`
 - MCP 서버 구성을 관리하는 데 사용됩니다.

워크플로

변환 실행

이 섹션에서는 변환을 실행하는 다양한 방법과 실행 동작을 제어하는 옵션에 대해 설명합니다.

실행 모드

AWS 사용자 지정 변환은 서로 다른 워크플로를 수용하기 위해 세 가지 실행 모드를 지원합니다.

대화형 대화 모드

로 CLI를 시작하고 에이전트에게 자연어를 통해 변환을 실행하도록 `atx` 요청합니다. 이 모드를 사용하면 에이전트와 전체 대화를 나누고, 언제든지 실행을 중단하고, 변환 프로세스 중에 피드백을 제공할 수 있습니다.

이 모드를 사용하면 에이전트를 최대한 제어하고 복잡한 시나리오를 안내할 수 있습니다.

직접 대화형 실행

`atx custom def exec -n <transformation-name> -p <path>`를 사용하여 대화형으로 특정 변환을 시작합니다. 이 모드를 사용하면 실행 시작 시, 도중 또는 종료 시 에이전트를 검토하고 에이전트와 상호 작용할 수 있습니다. 에이전트는 주요 결정 시점에서 일시 중지하고 입력을 요청합니다.

이는 변환을 자율적으로 실행하기 전에 변환을 테스트하고 구체화하는 데 적합합니다.

비대화 모드 또는 헤드리스 모드에서 변환을 실행할 수 있습니다. 비대화 모드는 명명된 변환 중에 프롬프트를 억제합니다. 헤드리스 모드를 사용하면 대화형 인터페이스를 완전히 우회하여 일반 텍스트 프롬프트로 에이전트를 실행할 수 있습니다.

비대화형 모드

전체 자동화 `atx custom def exec -n <transformation-name> -p <path> -x -t`에를 사용합니다. `-x`를 추가하여 비대화형 모드에서 실행하고 `-t`를 추가하여 프롬프트 없이 모든 도구를 자동으로 신뢰합니다.

이 모드는 인적 개입을 사용할 수 없거나 원하지 않는 CI/CD 파이프라인 통합 및 대량 실행을 위해 설계되었습니다.

헤드리스 모드

에이전트와 상호 작용하지 않고 작업을 완료하려면 `atx -x "<prompt>" -t`하고 일반 텍스트로 지침을 제공합니다.

헤드리스 변환 실행

이 모드를 사용하여 코드베이스에 기존 변환 정의를 적용합니다. 변환은 승인 없이 각 단계를 자동으로 실행합니다.

```
atx -x "apply transformation definition <transformation_definition_name> to
<codebase_path>" -t
```

헤드리스 변환 개발

변환 정의를 생성하거나 수정합니다.

레거시 변환 정의를 새 스킬 형식(`SKILL.md + references/`)으로 변환하려면 다음 명령을 실행합니다.

```
atx -x "convert <legacy_transformation_definition_name> transformation definition to
skill and save as draft" -t
```

새 변환 정의를 생성하려면 다음 명령을 실행합니다.

```
atx -x "create a transformation definition to <description> with references docs
<reference_docs_path>" -t
```

공통 명령 플래그

를 사용하여 변환 `atx custom def exec`을 실행할 때 일반적으로 다음 플래그가 사용됩니다.

- `-n` 또는 `--transformation-name` - 실행할 변환의 이름을 지정합니다.
- `-p` 또는 `--code-repository-path` - 코드베이스의 경로를 지정합니다(현재 디렉터리의 경우 `."` 사용).
- `-c` 또는 `--build-command` - 실행할 빌드 또는 검증 명령을 지정합니다.
- `-x` 또는 `--non-interactive` - 비대화형 모드 활성화(사용자 프롬프트 없음)
- `-t` 또는 `--trust-all-tools` - 프롬프트 없이 모든 도구를 자동으로 신뢰합니다.
- `-d` 또는 `--do-not-learn` -이 실행에서 단위 추출을 방지합니다.
- `--tv` 또는 `--transformation-version` - 변환의 특정 버전을 지정합니다.
- `-g` 또는 `--configuration` - 구성 파일 또는 인라인 구성을 제공합니다.

Important

`-t` 또는 `--trust-all-tools` 플래그는 프롬프트 없이 모든 도구 실행을 자동으로 승인하고 대부분의 보안 가드레일을 우회합니다(에 의해 재정의되지 않는 한 `alwaysPromptCommands` 목록과 일치하는 명령에는 여전히 명시적 권한이 필요합니다 `trustedShellCommands`). 완전히 자율적인 경험을 위해서는 `--non-interactive` 및 `전달--trust-all-tools`해야 하지만 변환을 실행하는 데는 필요하지 않습니다. 프로덕션 환경에서는 주의하여 사용하세요.

구성 파일 사용

AWS 사용자 지정 변환은 YAML 또는 JSON 형식의 선택적 구성 파일을 지원합니다. 구성 파일을 사용하면 실행 파라미터를 지정하고 에이전트에 추가 컨텍스트를 제공할 수 있습니다.

구성 파일을 사용하려면:

```
atx custom def exec --configuration file://config.yaml
```

구성을 인라인 카값 페어로 제공할 수도 있습니다.

```
atx custom def exec --configuration "key=value,key2=value2"
```

예제 구성 파일(config.yaml):

```
codeRepositoryPath: ./my-project
transformationName: my-transformation
buildCommand: mvn clean install
additionalPlanContext: |
  The target Java version to upgrade to is Java 17.
  Ensure compatibility with our internal logging framework version 2.3.
validationCommands: |
  mvn test
  mvn verify
```

additionalPlanContext 파라미터는 에이전트의 실행 계획에 대한 추가 컨텍스트를 제공합니다. 이는 관리 AWS형 변환을 통해 특정 요구 사항에 맞게 동작을 사용자 지정하는 데 특히 유용합니다.

빌드 및 검증 명령

빌드 또는 검증 명령은 변환 프로세스 중에 코드를 검증하는 방법을 지정하는 선택적 파라미터입니다. AWS 변환 사용자 지정은 지정되지 않은 경우 변환을 기반으로 최상의 빌드 명령을 추론하려고 시도하지만 품질에 특정한 것이 좋습니다.

빌드 및 검증 명령의 예:

- Java: mvn clean install 또는 gradle build
- Python: pytest 또는 python -m py_compile
- Node.js: npm run build 또는 npm test
- 린터: eslint . 또는 pylint .

빌드가 필요하지 않은 언어 또는 변환의 경우에도 결과를 검증하고 검증에 실패할 경우 문제를 반환하는 명령을 제공하는 것이 변환 품질을 개선하는 데 매우 중요합니다.

빌드 또는 검증이 필요하지 않은 경우 입력에서 생략합니다.

학습 동작 제어

기본적으로 AWS 변환 사용자 지정은 모든 변환 실행에서 교훈을 추출합니다. 특정 실행에 대한 학습을 방지할 수 있습니다.

실행에서 학습하지 않으려면:

```
atx custom def exec -n my-transformation -p ./my-project -d
```

-d 또는 --do-not-learn 플래그는 현재 실행에서 레슨 추출을 허용하지 않도록 옵트아웃합니다.

대화 재개

AWS 사용자 지정 변환을 사용하면 생성 후 30일 이내에 이전 대화를 재개할 수 있습니다.

가장 최근 대화를 재개하려면:

```
atx --resume
```

특정 대화를 재개하려면:

```
atx --conversation-id <conversation-id>
```

Important

대화는 생성 후 30일 이내에만 재개할 수 있습니다. 30일이 지나면 대화를 더 이상 재개할 수 없습니다.

추적 에이전트 분

AWS 사용자 지정 변환은 변환 세션 중에 사용된 [에이전트 시간](#)을 추적합니다. 에이전트 시간은 대화 수명 주기 동안 누적되며 대화가 종료될 때 표시됩니다.

```
Agent minutes used: 12.50
```

에이전트 시간은 중단 후에도 지속됩니다. Ctrl+C로 세션을 중단했다가 나중에 재개하는 경우 이전에 누적된 분은 이월되어 재개된 세션에서 계속 누적됩니다.

대화형 세션 중에 Agent Minutes를 확인하려면:

입력 프롬프트/usage에를 입력하여 대화를 종료하지 않고 현재 누적된 Agent Minutes를 표시합니다.

에이전트 분 예산 한도를 설정하려면:

```
atx custom def exec -n my-transformation -p ./my-project --limit 30
```

--limit 옵션은 세션에 대한 최대 [에이전트 분](#) 예산을 설정합니다. 에이전트 분은 벽시계 시간이 아닌 활성 에이전트 작업 시간을 반영합니다. 한도에 도달하면 CLI에 메시지가 표시되고 재개 지침과 함께 종료됩니다.

```
## Budget limit reached: 30.00 / 30.00 Agent Minutes. Exiting.
```

나중에 제한을 늘려 대화를 재개할 수 있습니다.

```
atx --conversation-id <conversation_id> -t --limit <increased_limit>
```

지속적인 학습

이 섹션에서는 지속적인 학습으로 생성된 교훈을 검토하고 관리하는 방법을 설명합니다.

단원 이해

연속 학습 시스템은 이전 변환 실행에서 교훈을 자동으로 추출합니다. 시스템은 다음을 기반으로 비동기적으로 생성합니다.

- 대화형 모드로 제공되는 개발자 피드백
- 변환 중에 발생하는 코드 문제

여러 코드베이스에서 변환을 실행하면 시간이 지남에 따라 교훈이 누적됩니다. 시스템은 향후 실행을 개선하기 위해 자동으로 이를 적용합니다. 각 단원은 유사한 도메인의 모든 단원을 포함하는 범주에 속하므로 관련 단원을 함께 검토할 수 있습니다. 사용하지 않으려는 단원의 경우 단원을 완전히 보관하거나 삭제할 수 있습니다.

단원 보기 및 관리

learnings 명령을 사용하여 변환 정의의 교훈을 찾아보고 관리하기 위한 대화형 세션을 엽니다.

단원 뷰어를 열려면:

```
atx custom def learnings -n my-transformation
```

뷰어는 포함된 활성 레슨의 수를 각각 보여주는 레슨 범주 목록에서 열립니다. 범주를 선택하여 해당 단원을 확인한 다음 단원을 선택하여 단원 본문, 그 영향 및 해당 단원을 참조한 이전 실행 수를 포함한 전체 세부 정보를 봅니다.

단원 보관 및 복원

시스템은 자동으로 단원을 적용합니다. 시스템이 단원을 적용하지 않도록 하려면이 단원을 보관할 수 있습니다. 시스템은 보관된 레슨을 유지하지만 향후 실행에는 적용하지 않습니다. 보관된 모든 레슨은 함께 그룹화되므로 이를 검토하고를 활성 사용으로 복원할 수 있습니다.

단원 삭제

유용하지 않은 단원을 영구적으로 제거합니다. 삭제는 취소할 수 없으며 시스템은 향후 실행에서 삭제된 단원을 다시 학습할 수 있습니다.

삭제하려면 먼저 단원을 아카이브해야 합니다.

고급 구성

이 섹션에서는 사용자 지정 AWS 변환을 위한 고급 기능 및 구성 옵션에 대해 설명합니다.

환경 변수

환경 변수를 사용하여 CLI 동작을 사용자 지정할 수 있습니다.

Note

다음 예제에서는 Linux 및 macOS 구문(`export`)을 보여줍니다. Windows에서는를 사용하여 PowerShell에서 환경 변수를 설정합니다 `$env:NAME="value"`. 동등한 명령은 Windows(PowerShell) 탭을 참조하세요.

ATX_SHELL_TIMEOUT

셸 명령의 기본 제한 시간(900초/15분)을 재정의합니다.

Linux and macOS

```
export ATX_SHELL_TIMEOUT=1800 # 30 minutes
```

Windows (PowerShell)

```
$env:ATX_SHELL_TIMEOUT=1800 # 30 minutes
```

이는 대규모 코드베이스 또는 장기 실행 빌드 프로세스에 유용합니다.

ATX_DISABLE_UPDATE_CHECK

명령 실행 중에 자동 버전 확인 및 업데이트 알림을 비활성화합니다.

Linux and macOS

```
export ATX_DISABLE_UPDATE_CHECK=true
```

Windows (PowerShell)

```
$env:ATX_DISABLE_UPDATE_CHECK="true"
```

ATX_GIT_COMMITTER_NAME 및 ATX_GIT_COMMITTER_EMAIL

AWS 변환 중에 변경 사항을 적용할 때 변환 사용자 지정이 리포지토리에 생성하는 체크포인트 커밋에 사용되는 작성자 자격 증명을 구성합니다. 이러한 변수를 설정하지 않으면 체크포인트 커밋은 기본 자격 증명()에 귀속됩니다. ATX Bot <checkpoint@atx.bot>. 체크포인트를 특정 작성자로 속성 지정 하도록 두 변수를 설정합니다.

Linux and macOS

```
export ATX_GIT_COMMITTER_NAME="Jane Developer"
export ATX_GIT_COMMITTER_EMAIL="jane@example.com"
```

Windows (PowerShell)

```
$env:ATX_GIT_COMMITTER_NAME="Jane Developer"
```

```
$env:ATX_GIT_COMMITTER_EMAIL="jane@example.com"
```

신뢰 설정

신뢰 설정을 사용하면 프롬프트 없이 실행할 특정 도구 및 명령을 사전 승인할 수 있습니다. 신뢰 수준에 관계없이 특정 셸 명령에 대한 명시적 권한을 요구할 수도 있습니다. 이러한 설정은 `~/.aws/atx/trust-settings.yaml` 파일에서 구성됩니다.

파일에는 다음 세 가지 목록이 포함되어 있습니다.

- `trustedTools` - 프롬프트 없이 실행할 수 있는 도구
- `trustedShellCommands` - 프롬프트 없이 실행할 수 있는 셸 명령
- `alwaysPromptCommands` - `-t` 플래그 또는 세션 신뢰에 `trustedShellCommands` 관계없이에서 재정의하지 않는 한 명시적 권한이 필요한 셸 명령 패턴입니다. 이러한 패턴은 비대화형 모드()에서는 적용되지 않습니다-x.

신뢰할 수 있는 기본 도구:

- `file_read`
- `get_transformation_from_registry`
- `list_available_transformations_from_registry`

신뢰 설정 편집:

`trust-settings.yaml` 파일을 수동으로 편집하여 신뢰할 수 있는 도구 및 명령을 추가하거나 제거할 수 있습니다. `trustedShellCommands` 및 모두를 사용하여 `glob` 와일드카드 패턴을 `alwaysPromptCommands` 지원합니다*.

Note

명령이 두 목록과 일치하는 경우가 우선 `trustedShellCommands` 순위를 갖습니다.

다음은 각 명령 목록을 설명하고 예제를 제공합니다.

- `trustedShellCommands` - 이러한 패턴과 일치하는 명령은 다른 모든 가드레일을 우회하여 프롬프트 없이 실행됩니다. 패턴은 전체 명령 문자열과 일치합니다.

예시:

- `cd *` - `cd`로 시작하는 복합 명령과 일치
- `*&&*` - `&&` 연산자를 사용하여 모든 명령을 신뢰합니다.
- `alwaysPromptCommands -t` 플래그 또는 세션 신뢰에 `trustedShellCommands`관계없이에서 재정의하지 않는 한 이러한 패턴과 일치하는 명령에는 명시적 권한이 필요합니다. 이러한 패턴은 대화형 모드()에서는 적용되지 않습니다-x. 패턴은 복합 표현식(`&&`, `|`, 명령 대체)의 각 하위 명령과 일치합니다.

예시:

- `rm -rf *` - 항상 재귀적 강제 삭제 명령을 묻는 프롬프트
- `sudo *` - 항상 `sudo`로 실행되는 명령에 대한 프롬프트
- `find * -exec *` - 항상 `-exec`을 사용하여 찾기 명령 프롬프트 표시

세션 수준 신뢰:

대화형 프롬프트 중에 다음을 선택할 수 있습니다.

- (y)es - 한 번 실행
- (n)o - 거부
- (t)rust - 현재 세션에만 대한 신뢰

세션 수준 신뢰 설정은 일시적이며 CLI가 다시 시작될 때 재설정되므로 `trust-settings.yaml`을 영구적으로 수정하지 않고 임시 승인을 제공합니다.

Note

`alwaysPromptCommands` 목록과 일치하는 명령에는 세션 신뢰를 사용할 수 없습니다.

모델 컨텍스트 프로토콜(MCP) 서버

AWS 변환 CLI는 추가 도구를 사용하여 기능을 확장하는 모델 컨텍스트 프로토콜(MCP) 서버를 지원합니다.

구성:

~/.aws/atx/mcp.json 파일에서 MCP 서버를 구성합니다. AWS 변환 CLI는 로컬 명령 기반 서버와 원격 HTTP 서버의 두 가지 유형의 MCP 서버를 지원합니다.

로컬 명령 기반 서버:

로컬 서버는 시스템에서 하위 프로세스로 실행됩니다. command 속성을 사용하여 구성합니다.

```
{
  "mcpServers": {
    "my-local-server": {
      "command": "npx",
      "args": ["-y", "@example/mcp-server"]
    }
  }
}
```

원격 HTTP 서버:

원격 서버는 HTTP 또는 HTTPS URL에서 호스팅되는 MCP 서버에 연결됩니다. url 속성을 사용하여 구성합니다.

```
{
  "mcpServers": {
    "my-remote-server": {
      "url": "https://api.example.com/mcp",
      "headers": {
        "Authorization": "Bearer ${MCP_API_TOKEN}"
      }
    }
  }
}
```

headers 속성은 선택 사항이며 구문을 사용하여 환경 변수 확장 \${VAR_NAME}을 지원합니다. 이렇게 하면 구성 파일이 아닌 환경 변수에 API 토큰과 같은 민감한 값을 저장할 수 있습니다.

구성 속성:

로컬 명령 기반 서버는 다음 속성을 지원합니다.

- command (필수) - 서버를 실행하는 명령입니다.
- args (선택 사항) - 명령줄 인수 배열
- env (선택 사항) - 서버 프로세스에 전달할 환경 변수

원격 HTTP 서버는 다음 속성을 지원합니다.

- `url` (필수) - 원격 MCP 서버의 HTTP 또는 HTTPS URL
- `headers` (선택 사항) - `${VAR_NAME}` 환경 변수 확장을 지원하는 요청에 포함할 HTTP 헤더

MCP 서버 관리:

구성된 MCP 서버 목록 보기:

```
atx mcp tools
```

특정 MCP 서버에서 제공하는 사용 가능한 도구를 나열합니다.

```
atx mcp tools --server <server-name>
```

사용량 추적:

CLI는 변환 실행 중에 MCP 도구 사용을 자동으로 추적합니다. 사용 통계는와 함께 대화 디렉터리 `mcp_usage.json`에서 로 유지됩니다 `metadata.json`. 파일은 다음을 포함하여 각 실행에 대한 도구별 지표를 기록합니다.

- 도구당 호출 수
- 도구당 오류 수
- 도구당 총 실행 시간
- 마지막 오류 세부 정보(있는 경우)

클라이언트 측 기술

클라이언트 측 기술은 변환 실행 중에 에이전트를 확장하는 추가 기능입니다. 이를 통해 에이전트가 내장 기능과 함께 사용할 수 있는 사용자 지정 도구, 스크립트 및 지침을 제공할 수 있습니다.

스킬 검색 디렉터리:

스킬은 네 개의 디렉터리에서 우선적으로 검색됩니다. 이름이 같은 스킬이 여러 디렉터리에 있는 경우 목록의 첫 번째 디렉터리가 우선합니다.

1. `<project>/aws/atx/skills/` - 프로젝트 수준, AWS CLI별 변환

2. <project>/agents/skills/ - 프로젝트 수준, 교차 클라이언트(호환되는 모든 에이전트 도구에서 사용 가능)
3. ~/.aws/atx/skills/ - 사용자 수준, AWS CLI별 변환
4. ~/.agents/skills/ - 사용자 수준, 교차 클라이언트(호환되는 모든 에이전트 도구에서 사용 가능)

.aws/atx/skills/ 디렉터리는 AWS 변환 CLI에 고유합니다. 디렉터리는 교차 클라이언트이므로 AWS Transform CLI 이외의 호환되는 에이전트 도구에서 해당 .agents/skills/ 디렉터리에 배치된 기술을 사용할 수 있습니다.

Skill 디렉터리 구조:

각 스킬은 YAML 프론트미터가 있는 SKILL.md 파일이 포함된 디렉터리입니다.

```
~/.aws/atx/skills/
### my-skill/
    ### SKILL.md           # Required: frontmatter + instructions
    ### references/        # Optional: reference docs the agent can read
    #   ### guide.md
    ### scripts/           # Optional: scripts the agent can execute
    ### validate.py
```

SKILL.md 형식:

```
---
name: my-skill
description: When to use this skill
---
# Skill Title

Instructions for the agent...
```

name 필드는 상위 디렉터리 이름과 일치해야 합니다.

스킬 비활성화:

스킬이 파일을 제거하지 않고 로드되지 않도록 하려면 `disable-model-invocation: true`를 프론트미터에 추가합니다.

```
---
```

```
name: my-skill
description: When to use this skill
disable-model-invocation: true
---
```

이 속성이 설정되면 CLI는 검색 중에 스킬을 건너뜁니다. 변환 정의가 스킬 파일을 읽도록 명시적으로 지시하지 않는 한 에이전트는 스킬을 보거나 사용할 수 없습니다. 이를 사용하여 일시적으로 스킬을 비활성화하거나, work-in-progress으로 표시하거나, 인적 독자 전용 참조 자료를 유지할 수 있습니다.

Note

비활성화된 스킬의 파일은 디스크에 남아 있습니다. 변환 정의가 에이전트에게 특정 파일 경로를 읽도록 지시하는 경우에도 에이전트는 여전히 콘텐츠에 액세스할 수 있습니다. `disable-model-invocation` 속성은 파일 시스템 액세스가 아닌 자동 검색 및 컨텍스트 삽입을 방지합니다.

실행 모드별 스킬 가용성:

- 실행 모드(atx custom def exec 포함 --code-repository-path) - 사용자 수준 디렉터리와 프로젝트 수준 디렉터리 모두에서 스킬을 검색합니다.
- 대화형 모드(atx) - 처음에는 사용자 수준 스킬만 검색됩니다. 세션 중에 코드 리포지토리 경로를 제공하면 프로젝트 수준 스킬도 로드됩니다.

스킬 검색 확인:

실행 후 CLI의 디버그 로그를 확인하여 검색된 스킬을 확인합니다.

Linux and macOS

```
grep -i "skill" ~/.aws/atx/logs/debug.log | tail -20
```

Windows (PowerShell)

```
Select-String -Pattern "skill" "$env:USERPROFILE\.aws\atx\logs\debug.log" | Select-Object -Last 20
```

검중에 실패한 스킬은 디버그 로그의 경고와 함께 건너뜁니다.

Note

클라이언트 측 스킬에는 CLI 버전 2.0 이상이 필요합니다.

프로젝트 수준 스킬과 사용자 수준 스킬 중에서 선택

스킬을 배치하는 위치에 따라 스킬의 이점과 활성화 시기가 결정됩니다.

프로젝트 수준 기술(<project>/aws/atx/skills/):

리포지토리에 대해 변환을 실행하는 모든 팀원이 자동으로 검색할 수 있도록 버전 관리로 커밋합니다. 다음을 위해 프로젝트 수준 기술을 사용합니다.

- 리포지토리별 규정 준수 검사(Dockerfile 규칙, Terraform 정책, 마이그레이션 안전 검사기)
- 이 코드베이스에 적용되는 조직 코딩 표준(관찰성 패턴, 오류 처리, 이름 지정 규칙)
- 프로젝트에 고유한 스크립트 빌드 또는 테스트(사용자 지정 린터, 아키텍처 피트니스 함수)
- 이 리포지토리에 사용되는 내부 라이브러리에 대한 API 마이그레이션 가이드

사용자 수준 기술(~aws/atx/skills/):

이는 시스템에 남아 있으며 대상 리포지토리에 관계없이 모든 변환 중에 활성화됩니다. 다음에 대해 사용자 수준 기술을 사용합니다.

- 개인 워크플로 도구(변경 로그 생성기, 커밋 메시지 형식자)
- 교차 프로젝트 기본 설정(선호하는 테스트 패턴, 설명서 스타일 미리 알림)
- 모든 리포지토리에서 조직에 필요한 라이선스 규정 준수 검사
- 작업하는 모든 코드베이스에 적용하는 적용 범위 임계값 또는 품질 게이트

효과적인 기술을 위한 팁:

- SKILL.md 프론트미터에 명확한 description 필드를 작성합니다. 에이전트는 이 필드를 사용하여 스킬이 관련된 시기를 결정합니다.
- 성공 시 코드 0으로 검증 스크립트를 종료하고 실패 시 0이 아닌 스크립트를 종료합니다. 에이전트는 종료 코드를 해석하여 규정 준수를 결정합니다.
- 스크립트에서 명확하고 실행 가능한 오류 메시지를 인쇄합니다. 에이전트는 수정해야 할 사항을 이해하기 위해 출력을 읽습니다.

- 기술을 어느 수준에서든 클라이언트 간 디렉터리(.agents/skills/)에 배치하여 AWS Transform CLI 이외의 다른 AI 개발 도구와 공유합니다.

클라이언트 측 스킬 예제

이 예제에서는 스크립트 기반 검증 스킬과 참조 전용 스킬이라는 두 가지 일반적인 패턴을 보여줍니다.

예: Dockerfile 규정 준수 검사기(스크립트 기반)

이 기술은 보안 및 운영 모범 사례를 기준으로 Dockerfiles를 검증합니다. 에이전트가 변경 전후에 실행하는 검증 스크립트를 사용합니다.

디렉터리 구조:

```
.aws/atx/skills/
### dockerfile-compliance/
    ### SKILL.md
    ### scripts/
    #   ### lint_dockerfile.sh
    ### references/
        ### dockerfile-best-practices.md
```

SKILL.md:

```
---
name: dockerfile-compliance
description: Validates Dockerfiles against security and operational best practices
---
# Dockerfile Compliance Checker

When a transformation creates or modifies Dockerfiles, run the compliance checker.

## When to use

- After creating a new Dockerfile
- After modifying FROM, RUN, USER, or EXPOSE directives
- When containerizing an application as part of a transformation

## How to use

Run: `bash scripts/lint_dockerfile.sh <path-to-Dockerfile>`
```

```
If violations are found, consult `references/dockerfile-best-practices.md`
for compliant patterns.
```

검증 스크립트는 루트로 실행되는 고정되지 않은 기본 이미지 태그, ENV 명령의 하드 코딩된 보안 암호, 누락된 HEALTHCHECK 정의가 있는지 확인합니다. 에이전트는 스크립트를 실행하고, 참조 파일의 패턴을 사용하여 위반을 수정하고, 스크립트를 다시 실행하여 규정 준수를 확인합니다.

예: API 사용 중단 도우미(참조 전용)

이 스킬은 업그레이드 변환 중에 더 이상 사용되지 않는 API 호출을 교체하는 과정을 에이전트에게 안내합니다. 스크립트가 없는 참조 파일만 사용합니다.

디렉터리 구조:

```
.aws/atx/skills/
### api-deprecation-helper/
    ### SKILL.md
    ### references/
        ### aws-sdk-v2-to-v3.md
        ### react-class-to-hooks.md
```

SKILL.md:

```
---
name: api-deprecation-helper
description: Guides the agent through replacing deprecated API calls with modern
  equivalents
---
# API Deprecation Helper

When performing upgrade transformations, use this skill to identify and replace
deprecated API calls with their modern equivalents.

## When to use

- During any version upgrade transformation
- When build warnings mention deprecated APIs
- When transforming code that uses legacy patterns

## Process

1. Identify deprecated API calls in the codebase
```

2. For each deprecated call, find the replacement in `references/`
3. Apply the replacement, preserving the original behavior
4. Verify the replacement compiles and tests pass

참조 파일에는 before-and-after 코드 예제가 포함되어 있습니다. 예를 들어 `aws-sdk-v2-to-v3.md`는 `S3Client` 및 `s3.putObject(params).promise()`를 사용하여와 같은 패턴을 모듈식 `v3`에 매핑합니다 `PutObjectCommand`.

태그 및 조직

액세스 제어 및 분류를 위해 태그를 사용하여 변환을 구성할 수 있습니다.

Note

이러한 명령 중 일부는 변환 정의에 대한 Amazon 리소스 이름(ARN)을 지정해야 합니다. ARN 구조는 다음과 같습니다. `arn:aws:transform-custom:<region>:<account-id>:package/<td-name>`

변환에 대한 태그를 나열하려면:

```
atx custom def list-tags --arn <transformation-arn>
```

변환에 태그를 추가하려면:

```
atx custom def tag --arn <transformation-arn> --tags '{"env":"prod","team":"backend"}'
```

변환에서 태그를 제거하려면:

```
atx custom def untag --arn <transformation-arn> --tag-keys "env,team"
```

태그는 IAM 정책에서 그룹화된 액세스 제어에 사용할 수 있습니다. 특정 태그가 있는 모든 변환(예: `team:frontend` 또는 태그가 지정된 모든 변환 `environment:production`)에 권한을 부여하는 정책을 생성할 수 있습니다.

로그

AWS 변환 CLI는 문제 해결 및 디버깅을 위해 세 가지 유형의 로그를 유지합니다.

대화 로그:

Linux and macOS

```
~/.aws/atx/custom/<conversation_id>/logs/<timestamp>-conversation.log
```

Windows

```
%USERPROFILE%\aws\atx\custom\<conversation_id>\logs\<timestamp>-conversation.log
```

이러한 로그에는 특정 세션에 대한 전체 대화 기록이 포함됩니다.

하위 에이전트 로그:

Linux and macOS

```
~/.aws/atx/custom/<conversation_id>/logs/subagents/<name>.log
```

Windows

```
%USERPROFILE%\aws\atx\custom\<conversation_id>\logs\subagents\<name>.log
```

이러한 로그에는 변환 중에 기본 에이전트가 생성하는 하위 에이전트의 출력이 포함됩니다. 하위 에이전트를 직접 관리할 필요는 없습니다.

개발자 디버그 로그:

Linux and macOS

```
~/.aws/atx/logs/debug*.log  
~/.aws/atx/logs/error.log
```

Windows

```
%USERPROFILE%\aws\atx\logs\debug*.log  
%USERPROFILE%\aws\atx\logs\error.log
```

이러한 로그는 CLI 자체에 대한 고급 문제 해결 정보를 제공합니다.

Note

로그 디렉터리에 디버그 로그 파일이 여러 개 있을 수 있습니다(예: debug1.log, debug2.log). 더 빠른 해결을 위해 지원 티켓을 열 때 ~/.aws/atx/custom/<conversation-id>/* 및 ~/.aws/atx/logs/*와 같은 모든 관련 로그를 검토하고 제공합니다.

CLI 업데이트

CLI를 최신 상태로 유지하여 새로운 기능 및 개선 사항에 액세스합니다.

업데이트를 확인하려면:

```
atx update --check
```

최신 버전으로 업데이트하려면:

```
atx update
```

특정 버전으로 업데이트하려면:

```
atx update --target-version <version>
```

사용자 지정 변환 생성

이 섹션에서는 사용자 지정 변환 정의를 생성, 수정 및 관리하는 방법을 설명합니다.

새 변환 생성

대화형 CLI를 사용하여 새 변환 정의를 생성합니다.

변환 정의를 생성하려면

1. AWS 변환 CLI를 시작합니다.

```
atx
```

2. 에이전트에게 새 변환을 생성하도록 지시합니다.

3. 변환 목표에 대한 명확하고 자세한 설명을 제공합니다. 포함:
 - 소스 및 대상 상태(예: "버전 X에서 버전 Y로 업그레이드")
 - 필요한 특정 변경 사항(예: "가져오기 문 업데이트, 더 이상 사용되지 않는 메서드 교체")
 - 특별 고려 사항 또는 제약 조건
4. 에이전트가 설명 또는 추가 정보를 요청할 때 특정 예제와 참조 자료를 제공합니다.
5. 에이전트가 생성한 초기 변환 정의를 검토합니다.
6. 샘플 코드베이스에서 변환을 테스트합니다.
7. 피드백, 코드 수정 또는 추가 예제를 제공하여 반복합니다.
8. 변환을 로컬에 저장하거나 레지스트리에 게시합니다.

변환 생성 모범 사례:

- 복잡한 변환을 시도하기 전에 간단하고 잘 정의된 변환으로 시작합니다.
- 마이그레이션 가이드 및 코드 샘플을 포함한 포괄적인 참조 자료 제공
- 게시하기 전에 여러 샘플 코드베이스에서 테스트
- 결정적 빌드 또는 검증 명령을 사용하여 지속적인 학습 활성화
- 복잡한 변환을 여러 개의 작은 단계로 나누는 것이 좋습니다.
- 중요한 정보를 변환 정의에 "CRITICAL:" 또는 "IMPORTANT:"로 표시하여 에이전트가 이러한 요구 사항을 우선시하도록 합니다.
- 정확한 요구 사항을 따라야 하는 경우(예: 특정 명령 또는 문자열 값 사용) 변환 정의에 전체 문자열을 명시적으로 지정합니다. 이를 bash 따옴표로 묶어 터미널 명령 또는 리터럴 문자열임을 명확하게 나타내 변동성을 줄이고 일관된 실행을 보장할 수 있습니다.

참조 자료 제공

대화 중에 파일 경로를 지정하여 사용자 지정 AWS 변환에 참조 파일을 제공할 수 있습니다. 이러한 파일은 변환 정의의 references/ 폴더에 저장됩니다.

권장되는 참조 파일 유형:

- 이전/이후 예제 코드
- 관련 APIs, 라이브러리 또는 기능에 대한 설명서
- 사람이 읽을 수 있는 마이그레이션 가이드

참조 파일을 제공하려면:

Take a look at the documentation here: `/path/to/migration-guide.md`

여러 참조 파일이 포함된 디렉터리를 제공할 수도 있습니다.

Take a look at the docs we have here: `/path/to/docs/`

Note

텍스트 기반 파일(.md, .html, .txt, 코드 파일)만 지원됩니다. 이진 파일, 이미지 및 서식 있는 텍스트 파일(예: .pdf, .png, .docx)은 현재 지원되지 않습니다. 텍스트 콘텐츠를 추출하여 참조로 사용할 수 있는 경우가 많습니다. 작은 텍스트 파일이 많은 경우 설명이 포함된 파일 몇 개로 연결하는 것이 좋습니다. 모든 파일에 대해 총 10MB로 제한됩니다.

기존 변환 수정

사용자 지정 변환을 초안으로 저장하거나 게시하기 전과 후에 모두 수정할 수 있습니다. AWS관리형 변환은 수정할 수 없습니다. 사용자 지정해야 하는 경우 구성 파일을 사용하여 추가 컨텍스트를 제공할 수 있습니다.

기존 변환을 수정하려면

1. AWS 변환 CLI를 시작합니다.

```
atx
```

2. 에이전트에게 기존 변환을 수정하도록 지시합니다.
3. 다음을 수행할지 여부를 선택합니다.
 - 로컬에 저장된 변환에 대한 파일 경로를 제공합니다(예: 저장된 초안 또는 게시되지 않음).
 - 레지스트리에서 변환 목록 요청
4. 레지스트리에서 선택하는 경우 수정하려는 변환을 선택합니다.
5. 에이전트와 협력하여 변경하려는 사항을 설명합니다.
6. 샘플 코드베이스에서 업데이트된 변환을 테스트합니다.
7. 원하는 경우 레지스트리에 업데이트를 게시합니다.

변환 게시 및 관리

대화형 환경을 사용하거나 다음 명령을 사용하여 변환을 게시하고 관리할 수 있습니다.

변환을 초안으로 저장하려면:

```
atx custom def save-draft -n my-transformation --description "Description of the transformation" --sd ./transformation-directory
```

변환을 게시하려면:

```
atx custom def publish -n my-transformation --description "Description of the transformation" --sd ./transformation-directory
```

사용 가능한 변환을 나열하려면

```
atx custom def list
```

변환 정의를 다운로드하려면:

```
atx custom def get -n my-transformation
```

그러면 변환 정의가 현재 작업 디렉터리로 다운로드됩니다. --td 플래그가 있는 대상 디렉터리와 --tv 플래그가 있는 버전을 지정할 수 있습니다.

변환 정의를 삭제하려면:

```
atx custom def delete -n my-transformation
```

Important

이렇게 하면 계정에서 지정된 변환 정의가 영구적으로 삭제됩니다.

변환 버전 관리

AWS 변환 사용자 지정은 변환 정의의 버전을 유지합니다. 변환을 실행하거나 다운로드할 때 버전을 지정할 수 있습니다.

특정 버전을 실행하려면:


```
atx custom def exec -n my-transformation --tv v1 -p ./my-project
```

특정 버전을 다운로드하려면:

```
atx custom def get -n my-transformation --tv v1
```

버전을 지정하지 않으면 최신 버전이 사용됩니다.

명령 참조

이 섹션에서는 모든 AWS Transform 사용자 지정 CLI 명령에 대한 포괄적인 참조를 제공합니다.

대화형 명령

atx

AWS 변환 CLI를 사용하여 대화형 대화를 시작합니다.

```
atx                # Start new conversation
atx --resume       # Resume most recent conversation
atx --conversation-id <id> # Resume specific conversation
atx -t            # Start with all tools trusted
```

대화형 세션 명령

대화형 세션 중에 입력 프롬프트에 다음 명령을 입력할 수 있습니다.

- /usage - 현재 세션에 대해 누적된 [에이전트 분](#) 표시

변환 정의 명령

atx 사용자 지정 def exec

코드 리포지토리에서 변환 정의를 실행합니다.

옵션	긴 형식	파라미터	설명
-p	--code-repository-path	<path>	변환할 코드 리포지토리의 경로입니다. 현재

옵션	긴 형식	파라미터	설명
			디렉터리의 경우 ""를 사용합니다.
-c	--build-command	<command>	리포지토리를 빌드할 때 실행할 명령
-n	--transformation-name	<name>	레지스트리의 변환 정의 이름
-x	--non-interactive	-	사용자 지원 없이 변환을 실행합니다.
-t	--trust-all-tools	-	모든 도구를 신뢰합니다(도구 프롬프트 없음).
-d	--do-not-learn	-	이 실행에서 단위 추출 허용 옵트아웃
-g	--configuration	<config>	구성 파일(JSON 또는 YAML) 또는 키=값 페어 경로
--tv	--transformation-version	<version>	사용할 변환 정의의 버전
--limit	--limit	<limit>	에이전트 분 예산 한도를 설정합니다. 한도에 도달하면 변환이 종료되고 한도가 증가하면 변환을 재개할 수 있습니다.
-h	--help	-	명령에 대한 도움말 표시

atx 사용자 지정 def 목록

사용 가능한 변환 정의를 나열합니다.

```
atx custom def list
atx custom def list --json    # Output in JSON format
```

atx 사용자 지정 def get

특정 변환 정의에 대한 세부 정보를 가져옵니다.

옵션	긴 형식	파라미터	설명
-n	--transfo rmation-name	<name>	검색할 변환 정의의 이름입니다.
--tv	--transfo rmation-v ersion	<version>	검색할 변환 정의의 버전입니다.
--td	--target- directory	<directory>	변환 정의를 저장할 대상 디렉터리(기본값: ".")
--json	--json	-	JSON 형식의 출력 응답
-h	--help	-	명령에 대한 도움말 표시

atx 사용자 지정 def 삭제

변환 정의를 영구적으로 삭제합니다.

```
atx custom def delete -n <transformation-name>
```

atx 사용자 지정 def 게시

변환 정의를 레지스트리에 게시합니다.

옵션	긴 형식	파라미터	설명
-n	--transformation-name	<name>	게시할 변환 정의의 이름입니다.
--tv	--transformation-version	<version>	사용할 변환 정의의 버전(--description 또는 --source-directory에는 적용되지 않음)
--sd	--source-directory	<directory>	로컬 변환 정의 파일을 읽을 소스 디렉터리(--transformation-version에는 해당되지 않음)
--description	--description	<description>	변환 정의에 대한 설명(--transformation-version에는 해당되지 않음)
--json	--json	-	JSON 형식의 출력 응답
-h	--help	-	명령에 대한 도움말 표시

atx 사용자 지정 def 저장-초안

변환 정의를 레지스트리에 초안으로 저장합니다. 초안은 30일 후에 만료되며 레지스트리에 표시되지 않습니다. 이 명령은 초안의 버전 번호를 반환합니다. 변환 이름과 버전 번호를 사용하여 초안을 명시적으로 실행하고 검색해야 합니다.

```
atx custom def save-draft -n <transformation-name> --description "Description" --sd <directory>
```

단원 명령

atx 사용자 지정 def 학습

대화형 세션을 열어 변환 정의가 이전 실행에서 학습한 내용을 보고 관리합니다. 범주별로 단원을 찾아 보고, 단원 세부 정보를 보고, 단원을 아카이브, 복원 또는 삭제합니다.

```
atx custom def learnings -n <transformation-name>
```

태그 명령

atx 사용자 지정 def list-tags

변환 정의에 대한 태그를 나열합니다.

```
atx custom def list-tags --arn <transformation-arn>
```

atx 사용자 지정 def 태그

변환 정의에 태그를 추가합니다.

```
atx custom def tag --arn <arn> --tags '{"env":"prod","team":"backend"}'
```

atx 사용자 지정 def 태그 해제

변환 정의에서 태그를 제거합니다.

```
atx custom def untag --arn <arn> --tag-keys "env,team"
```

업데이트 명령

atx 업데이트

AWS 변환 CLI를 업데이트합니다.

```
atx update                # Update to latest version
atx update --check        # Check for updates only
atx update --target-version <version> # Update to specific version
```

MCP 명령

atx mcp 도구

클라이언트가 MCP 도구 구성을 보고 확인할 수 있도록 허용합니다. 구성 업데이트는 ~/.aws/atx/mcp.json 파일을 통해 직접 관리해야 합니다.

```
atx mcp tools      # View list of MCP servers
atx mcp tools -s   # List tools for the specified server
```

AWS관리형 변환

AWS관리형 변환은 추가 설정 없이 사용할 수 있는 일반적인 사용 사례를 위해 사전 구축되고 AWS검증된 변환입니다.

개요

AWS관리형 변환의 특징은 다음과 같습니다.

- 검증자 AWS - 이러한 변환은 고품질 AWS 이 되도록에서 검토됩니다.
- 즉시 사용 가능 - 추가 설정이 필요하지 않음
- 지속적인 성장 - 추가 변환이 지속적으로 추가되고 있습니다.
- 사용자 지정 가능 - additionalPlanContext 구성 파라미터를 사용하여 조직의 요구 사항에 맞는 추가 지침 또는 요구 사항을 제공하여 사전 구축된 변환을 사용자 지정할 수 있습니다.
- 조기 액세스 지원 - 일부 변환은 추가 테스트 및 개선을 거치면서 조기 액세스로 표시될 수 있습니다.

사용 가능한 AWS관리형 변환

다음 카탈로그에는 현재 사용 가능한 AWS관리형 변환이 사용 사례별로 그룹화되어 나열되어 있습니다. 각 테이블에는 변환 이름, 변환이 적용되는 언어 또는 스택, 상태가 표시됩니다. 변환을 빠르게 찾으려면이 페이지 상단의 검색 상자를 사용하여 이름, 언어 또는 사용 사례별로 검색합니다.

이 카탈로그는 AWS관리형 변환의 정식 목록입니다. Kiro Power, 에이전트 플러그인, VS Code 플러그인 및 CLI는 모두 동일한 변환을 실행합니다. 레지스트리에서 사용 가능한 변환을 나열하려면 실행합니다 `atx custom def list`.

Note

조기 액세스로 표시된 변환은 작동하지만 고객 피드백에 따라 자주 업데이트될 수 있습니다.

런타임 업그레이드

언어 또는 런타임을 최신 버전으로 업그레이드하거나 런타임 배포를 변경합니다.

트랜스포메이션	언어/스택	Status	설명
AWS/java-version-upgrade	Java	정식 버전	Jakarta EE 마이그레이션, 데이터베이스 드라이버, ORM 프레임워크, Spring 에코시스템 업데이트를 포함한 종속성 현대화를 통해 모든 소스 JDK 버전에서 모든 대상 JDK 버전으로 모든 빌드 시스템을 사용하여 Java 애플리케이션을 업그레이드합니다. 채팅에서 또는 additionalPlanContext 파라미터를 사용하여 대상 JDK 버전을 지정합니다.
AWS/python-version-upgrade	Python	정식 버전	기능과 성능을 유지하면서 Python 프로젝트를 Python 3.8 또는 3.9에서 Python 3.11, 3.12 또는 3.13으로 마이그레이션합니다. 채팅에서 또는 additionalPlanContext 파라미터를 사용하여 대상 Python 버전을 지정합니다.
AWS/nodejs-version-upgrade	Node.js	정식 버전	소스 Node.js 버전에서 대상 Node.js 버전으로 Node.js 애플리케이션을 업그레이드

트랜스포메이션	언어/스택	Status	설명
			이드합니다. 채팅에 서 또는 additionalPlanContext 파 라미터를 사용하여 대 상 버전을 지정합니다.
AWS/lambda- nodejs-runtime- upgrade	Node.js(Lambda)	조기 액세스	AWS Lambda 함수를 이전 Node.js 런타임 (nodejs4.3~ nodejs22. x)에서 nodejs24.x 로 업그레이드하여 Lambda 런타임 인터 페이스 클라이언트 (RIC) 및 Node.js 24 언어 런타임의 주요 변 경 사항을 해결합니다.
AWS/oracle- java-to- corretto	Java(JDK 배포)	조기 액세스	Java 프로젝트를 Oracle JDK에서 Amazon Corretto로 마이그레이션합니다. Oracle 전용 내부 APIs 를 표준 Java로 대체하 고, 빌드 구성(Maven 및 Gradle) 및 컨테이 너 기본 이미지를 업데 이트하고, 상용 JVM 플래그를 제거하고, 라 이선스 보고서를 생성 합니다.

트랜스포메이션	언어/스택	Status	설명
AWS/ruby-upgrade	Ruby	조기 액세스	Ruby 애플리케이션을 Ruby 2.x에서 Ruby 4.0으로 업그레이드하고 해당 프레임워크를 Rails 8.0 또는 Sinatra 4.1로 업그레이드합니다. Rails 및 ActiveRecord 앱, Sinatra 앱 및 독립 실행형 Gem에서 이 변환을 사용할 수 있습니다. 변환은 각 Ruby 버전 범프를 일치하는 프레임워크 업그레이드와 페어링하고 테스트 제품군을 실행합니다. 그런 다음 다음 버전으로 진행하기 전에 장애를 격리합니다.

SDK 마이그레이션

AWS SDK의 메이저 버전 간에 마이그레이션합니다.

트랜스포메이션	언어/스택	Status	설명
AWS/java-aws-sdk-v1-to-v2	Java	정식 버전	Maven 또는 Gradle을 사용하여 Java 프로젝트용 AWS SDK를 v1에서 v2로 업그레이드합니다.
AWS/python-boto2-to-boto3	Python	정식 버전	공식 마이그레이션 설명서에 따라 Python 애플리케이션을 boto2에

트랜스포메이션	언어/스택	Status	설명
			서 boto3로 AWS 마이그레이션합니다.
AWS/nodejs-aws-sdk-v2-to-v3	Node.js	정식 버전	Node.js 버전을 변경하지 않고도 모듈식 아키텍처, 일류 TypeScript 지원 및 향상된 성능을 위해 Node.js 애플리케이션을 AWS SDK for JavaScript v2에서 v3로 업그레이드합니다.

프레임워크 업그레이드 및 마이그레이션

프레임워크를 최신 버전으로 업그레이드하거나 다른 프레임워크로 마이그레이션합니다.

트랜스포메이션	언어/스택	Status	설명
AWS/spring-boot-version-upgrade	Java/스프링 부트	정식 버전	빌드 파일 및 스타터, 속성, Jackson 3 패키지, Spring Security 7 DSL, 테스트 인프라 및 관찰성 종속성을 포함하여 이전 Spring Boot 애플리케이션을 대상 Spring Boot 버전으로 업그레이드합니다.
AWS/JBoss-to-Spring-Boot	Java(JBoss 또는 WildFly에서 Spring Boot로)	조기 액세스	JBoss EAP 또는 WildFly에서 실행되는 Java EE 또는 Jakarta EE 엔터프라이즈 애플리케이션을 Spring Boot로 마이그레이션

트랜스포메이션	언어/스택	Status	설명
			하여 클라우드 네이티브 컨테이너화된 배포 모델에 대한 애플리케이션 서버 종속성을 제거합니다.
AWS/early-access-angular-to-react-migration	반응 각도	조기 액세스	Angular 애플리케이션을 React로 변환합니다.
AWS/angular-version-upgrade	Angular(각)	조기 액세스	구성 요소, 서비스, 템플릿 및 라우팅을 포함하여 이전 Angular 애플리케이션을 대상 Angular 버전으로 업그레이드합니다.
AWS/vue.js-version-upgrade	Vue.js	조기 액세스	Vue.js 2에서 Vue.js 3으로 메이저 버전 업그레이드를 수행하여 구성 요소, 상태 관리, 라우팅 및 글로벌 APIs. 마이너 및 패치 업데이트는 범위를 벗어납니다.

GenAI 및 모델 마이그레이션

생성형 AI 워크로드를 로 마이그레이션합니다.

트랜스포메이션	언어/스택	Status	설명
AWS/GenAI-to-Bedrock-Migration-Assessment	생성형 AI 워크로드	조기 액세스	타사 공급자(OpenAI, Google Gemini, Anthropic 다이렉트 및 오픈 소스 모델)에서 로 마이그레이션하기 위한 생성형 AI 워크로드를 평가합니다. SDK 사용량 및 모델을 검색하고, 요구 사항을 명확히 하고, 모델 매핑을 설계하고, 비용 및 위험을 추정하고, 평가 아티팩트를 생성합니다. 평가 전용, 소스 코드는 수정하지 않습니다. CrewAI, LangGraph, Strands와 같은 에이전트 프레임워크도 다룹니다.

Language-to-language 마이그레이션

한 프로그래밍 언어에서 다른 프로그래밍 언어로 코드베이스를 변환합니다.

트랜스포메이션	언어/스택	Status	설명
AWS/vba-to-python-migration	VBA에서 Python으로	조기 액세스	openpyxl, pandas, tkinter 또는 PyQt6 및 표준 라이브러리를 사용하여 Excel VBA 매크로, 모듈, UserForms 및 임베디드 로직을 동등한 Python 스크립트 및 모

트랜스포메이션	언어/스택	Status	설명
			둘로 마이그레이션합니다. PyQt6 대상 언어는 Python 3.8 이상입니다. .bas, .cls, .frm 또는 .xism 포함 VBA 코드를 변환할 때를 사용합니다.

데이터베이스 마이그레이션

현재 데이터베이스별 AWS관리형 변환은 사용할 수 없습니다. Microsoft SQL Server 데이터베이스 및 관련 .NET 애플리케이션을 Amazon Aurora PostgreSQL로 현대화하려면 섹션을 참조하세요 [the section called “SQL Server 현대화”](#).

관찰성

로깅 및 모니터링을 네이티브 서비스로 현대화 AWS합니다.

트랜스포메이션	언어/스택	Status	설명
AWS/early-access-log4j-to-slf4j-migration	Java(로깅)	조기 액세스	Logback 백엔드를 사용하여 Java 애플리케이션을 Log4j(1.x 또는 2.x)에서 SLF4J로 마이그레이션합니다. 소스 코드, 종속성 관리(Maven 및 Gradle) 및 로깅 구성 파일을 처리하고 컴파일, 테스트 및 잔차 가져오기 스캔을 통해 검증합니다.
AWS/datadog-monitors-to-cloudwatch-alarms	코드형 인프라/모니터링	조기 액세스	AWS 서비스 지표 및 사용자 지정 지표를 추적하는 DataDog 지표 모니터를 코드형 인프라

트랜스포메이션	언어/스택	Status	설명
			라로 기본 CloudWatch 경보로 마이그레이션합니다. CloudFormation YAML, CDK TypeScript 및 Terraform HCL을 생성합니다.

아키텍처

애플리케이션을 다시 설계, 리플랫폼 또는 최적화합니다 AWS.

트랜스포메이션	언어/스택	Status	설명
AWS/java-performance-optimization	Java(성능)	정식 버전	JFR 프로파일링 데이터를 분석하여 CPU 및 메모리 핫스팟과 안티 패턴을 감지한 다음 대상 코드 수정을 적용하여 Java 애플리케이션 성능을 최적화합니다. JFR 데이터 수집에 대한 지침은 JFR 런타임 가이드를 참조하세요 .
AWS/early-access-java-x86-to-graviton	Java(Arm64 / Graviton)	조기 액세스	AWS Graviton 프로세서용 Arm64 아키텍처와 Java 애플리케이션 호환성을 검증하고, 종속성을 업데이트하고, 아키텍처별 코드 패턴을 감지하고, 소스 코드를 사용할 수 있을 때 네이티브 라이브러리를 다시 컴파일하

트랜스포메이션	언어/스택	Status	설명
			여 비호환성을 해결합니다. 많은 최신 Java 애플리케이션은 이미 Arm64-compatible됩니다.
AWS/oracle-service-bus-to-aws	Java / 서버리스에 통합	조기 액세스	Oracle Service Bus(OSB) 및 BPEL 프로세스 구성을 AWS 네이티브 서버리스 아키텍처로 마이그레이션하여 Amazon API Gateway, AWS Lambda 및 AWS Step Functions를 사용하여 배포 가능한 CDK TypeScript 프로젝트를 생성합니다.

트랜스포메이션	언어/스택	Status	설명
AWS/mulesoft-to-aws-native	Java/MuleSoft에서 서버리스로	조기 액세스	MuleSoft Mule 3.x 및 4.x 애플리케이션을 SnapStart를 사용하여 AWS Lambda의 Java 17을 대상으로 하는 AWS 서버리스 아키텍처(Amazon API Gateway, AWS Lambda 및 AWS Step Functions)로 변환합니다. 변환은 흐름 트리거를 AWS 이벤트 소스에 매핑하고, DataWeave 및 MEL(MuleSoft Expression Language) 표현식을 AWS 동등한 것으로 변환하고, 커넥터를 AWS SDK for Java v2 호출로 대체합니다. SAM 템플릿, AWS Lambda 핸들러 및 JUnit 5 테스트를 생성합니다.

트랜스포메이션	언어/스택	Status	설명
AWS/payshield-hsm-to-aws-payment-cryptography	Java(HSM에서 AWS Payment Cryptography로)	정식 버전	Java 애플리케이션을 Thales PayShield 하드웨어 보안 모듈 (HSM) 프로토콜에서 AWS Payment Cryptography SDK v2로 마이그레이션합니다. 마이그레이션에는 명령 매핑, 키 마이그레이션, 종속성 설정 및 패리티 테스트가 포함됩니다.

코드베이스 분석

코드베이스와 포트폴리오를 분석하여 현대화를 계획합니다. 이러한 변환은 보고서를 생성하고 코드를 수정하지 않습니다.

트랜스포메이션	언어/스택	Status	설명
AWS/comprehensive-codebase-analysis	여러 언어	정식 버전	코드베이스에 대한 심층 정적 분석을 수행하여 기술 부채 인사이트에 중점을 두고 동작 분석, 아키텍처 문서 및 비즈니스 인텔리전스를 결합하는 계층적이고 상호 참조된 문서를 생성합니다.
AWS/agent-readiness-analysis	여러 언어	조기 액세스	APIs, 자격 증명, 상태 관리, human-in-the-loop 및 관찰성을 포함하여 AI 에이전트가 시스템을 안전하게 호출

트랜스포메이션	언어/스택	Status	설명
			할 준비가 되었는지 평가합니다.
AWS/modernization-readiness-analysis	여러 언어	조기 액세스	포트폴리오를 스캔하여 클라우드 네이티브 성숙도 격차를 확인하고 조사 결과를 AWS 현대화 경로에 매핑합니다.
AWS/portfolio-agentic-readiness-analysis	Portfolio	조기 액세스	애플리케이션 포트폴리오에서 개별 에이전트 준비 분석 보고서를 집계하여 교차 커팅 블로커, 공유 문제 해결 패턴 및 우선 순위가 지정된 권장 사항을 식별합니다.
AWS/portfolio-modernization-readiness-analysis	Portfolio	조기 액세스	포트폴리오 전반의 개별 현대화 분석 보고서를 우선순위가 지정된 마이그레이션 웨이브와 권장되는 현대화 경로를 갖춘 통합 로드맵으로 집계합니다.

트랜스포메이션	언어/스택	Status	설명
AWS/business-rules-extraction	여러 언어	조기 액세스	이 변환은 모놀리식 코드베이스를 정적으로 분석하여 빌드, 실행 또는 소스 코드 수정 없이 재작성 가능한 설명서를 생성합니다. 시스템을 경계 도메인으로 분해하고 도메인별 비즈니스 규칙, 워크플로, 교차 커팅 문제 및 데이터베이스 구조를 추출합니다. 출력에는 현대화 또는 전체 재작성을 안내하기 위한 시스템 읽기 가능 매니페스트, 대화형 대시보드, 도메인당 언어 중립적 구현 사양이 포함됩니다.

AWS관리형 변환 사용자 지정

additionalPlanContext 구성 파라미터를 통해 추가 컨텍스트를 제공하여 조직의 특정 요구 사항을 충족하도록 사용자 지정 AWS관리형 변환을 사용자 지정할 수 있습니다.

예: Java 버전 업그레이드 사용자 지정

```
codeRepositoryPath: ./my-project
transformationName: AWS/java-version-upgrade
buildCommand: mvn clean install
additionalPlanContext: |
  The target Java version to upgrade to is Java 17.
  Update all internal library dependencies to versions compatible with Java 17.
  Ensure compatibility with our custom authentication framework.
```

예: AWS SDK 마이그레이션 사용자 지정

```
codeRepositoryPath: ./my-project
transformationName: AWS/java-aws-sdk-v1-to-v2
buildCommand: gradle build
additionalPlanContext: |
    Maintain our existing error handling patterns.
    Use our organization's standard credential provider chain.
    Update logging to use our internal logging framework.
```

일반 사용 사례

이 섹션에서는 AWS 변환 CLI를 사용하는 일반적인 변환 시나리오에 대한 step-by-step 지침을 제공합니다.

Lambda 런타임 업그레이드

Lambda는 오래된 언어 런타임을 주기적으로 중단하므로 팀에서 Lambda 함수를 지원되는 버전으로 업그레이드해야 합니다. AWS 변환 사용자 지정은 AWS관리형 언어 버전 업그레이드 변환을 사용하여 이러한 업그레이드를 자동화할 수 있습니다. 예를 들어 Python 3.9로 작성된 Lambda 함수를 Python 3.13으로 업그레이드하려면 AWS/python-version-upgrade 변환을 사용합니다. 가장 일반적인 Lambda 런타임 언어를 다루는 Java(AWS/java-version-upgrade) 및 Node.js(AWS/nodejs-version-upgrade)에서도 유사한 변환을 사용할 수 있습니다.

단일 Lambda 함수를 대화형으로 업그레이드하려면 함수의 소스 리포지토리 루트로 이동하여 로 AWS 변환 CLI를 시작합니다. 대화형 세션에서 "이 Python 3.9 Lambda 함수를 Python 3.13으로 업그레이드"와 같이 필요한 업그레이드를 설명합니다. 에이전트는 적절한 AWS관리형 변환을 선택하고, 코드를 분석하고, 언어 구문을 업데이트하고, 종속성을 조정하고, 더 이상 사용되지 않는 API 호출을 현대화합니다. 에이전트가 변환된 코드가 테스트를 컴파일하고 통과하는지 확인할 수 `python -m py_compile *.py` 있도록 `pytest` 또는와 같은 빌드 또는 검증 명령을 제공할 수 있습니다. 대화형 세션 전체에서 에이전트가 제안한 변경 사항을 검토하고, 피드백을 제공하고, 최종 결과를 수락하기 전에 조정을 요청할 수 있습니다.

여러 리포지토리에서 Lambda 런타임을 업그레이드해야 하는 경우 비대화형 모드를 사용하여 대규모로 변환을 실행합니다. 각 리포지토리에 대해 사용자 입력 없이 실행할 적절한 플래그를 사용하여 CLI를 호출합니다. 예를 들어 Node.js 16 Lambda 함수를 Node.js 22로 업그레이드하려면

```
atx custom def exec \
  -n AWS/nodejs-version-upgrade \
  -p ./my-lambda-repo \
  -c "npm test" \
```

```
-g "additionalPlanContext='Upgrade from Node.js 16 to Node.js 22'" \
-x -t
```

-x 플래그는 변환을 비대화적으로 실행하고 모든 도구 실행을 -t 신뢰하므로 프롬프트가 필요하지 않습니다. 간단한 셸 루프를 사용하여 수십 또는 수백 개의 리포지토리에이 명령을 스크립트로 작성할 수 있습니다. 각 변환이 완료되면 Git diff를 검토하여 변경 사항을 확인하고 테스트 제품군을 실행하여 업그레이드된 함수가 올바르게 작동하는지 확인합니다. 또한 사용자 지정 AWS 변환을 CI/CD 파이프라인에 통합하여 더 이상 사용되지 않는 Lambda 함수를 지속적으로 식별할 수 있습니다. 이 접근 방식은 더 이상 사용되지 않는 런타임의 즉각적인 문제를 해결할 뿐만 아니라 end-of-support 상태에 도달하기 전에 함수를 감지하고 업그레이드하는 지속적인 프로세스를 설정합니다.

중앙 플랫폼 팀은 [AWS 변환 웹 애플리케이션](#)을 통해 캠페인을 생성하여 변환을 정의하고, 대상 Lambda 리포지토리를 지정하고, 조직 전체의 진행 상황을 추적할 수 있습니다. AWS 배치를 사용하여 프로덕션급 확장 배포 솔루션을 구축하는 자세한 방법은 [AWS Transform custom을 사용하여 확장 가능한 코드 현대화 솔루션 구축](#)을 참조하세요.

AWS Transform 사용자 지정 및 인터페이스 엔드포인트(AWS PrivateLink)

인터페이스 VPC 엔드포인트를 생성하여 VPC와 AWS Transform 사용자 지정 간에 프라이빗 연결을 설정할 수 있습니다. 인터페이스 엔드포인트는 인터넷 게이트웨이 [AWS PrivateLink](#), NAT 디바이스, VPN 연결 또는 Direct Connect 연결 없이 사용자 AWS Transform 지정 서비스에 비공개로 액세스할 수 있는 기술로 구동됩니다. VPC와 AWS Transform 사용자 지정 간의 트래픽은 Amazon 네트워크를 벗어나지 않습니다.

각 인터페이스 엔드포인트는 서브넷에서 하나 이상의 [Elastic Network Interfaces](#)로 표현됩니다.

자세한 내용은 Amazon VPC 사용 설명서의 [인터페이스 VPC 엔드포인트\(AWS PrivateLink\)](#)를 참조하세요.

Note

- AWS Transform 사용자 지정에서 S3 API를 호출하므로 Amazon S3에 대한 AWS PrivateLink 통합을 활성화해야 합니다. 자세한 지침은 [AWS PrivateLink Amazon S3용](#) 설명서를 참조하세요. AWS Transform 사용자 지정을 사용하는 동안 S3 액세스 문제가 발생하면 문제 [해결 가이드](#)를 참조하세요.
- AWS PrivateLink 프라이빗 DNS 기능을 사용하지 않는 경우(프라이빗 [DNS](#) 참조) 다음을 수행해야 합니다.

- VPC 인터페이스 엔드포인트로의 라우팅 구성([VPC 인터페이스 엔드포인트로의 라우팅 설명서 참조](#))
- ATX_CUSTOM_ENDPOINT 환경 변수를 설정하여 사용자 지정 도메인을 지정합니다. 예를 들면 다음과 같습니다.

```
ATX_CUSTOM_ENDPOINT=https://transform-custom.<region>.api.aws atx
```

AWS Transform 사용자 지정 VPC 엔드포인트에 대한 고려 사항

AWS Transform 사용자 지정에 대한 인터페이스 VPC 엔드포인트를 설정하기 전에 Amazon VPC 사용 설명서의 [인터페이스 엔드포인트 속성 및 제한](#) 사항을 검토해야 합니다.

AWS Transform 사용자 지정은 인터페이스 엔드포인트를 통해 모든 API 작업을 호출할 수 있도록 지원합니다.

사전 조건

아래 절차를 시작하기 전에 다음 사항이 준비되어 있는지 확인하세요.

- 리소스를 생성하고 구성할 수 있는 적절한 권한이 있는 AWS 계정입니다.
- AWS 계정에 이미 생성된 VPC입니다.
- AWS 서비스, 특히 Amazon VPC 및 AWS Transform 사용자 지정에 대한 지식.

AWS Transform 사용자 지정을 위한 인터페이스 VPC 엔드포인트 생성

Amazon VPC 콘솔 또는 AWS Command Line Interface ()를 사용하여 AWS Transform 사용자 지정 서비스에 대한 VPC 엔드포인트를 생성할 수 있습니다AWS CLI. 자세한 내용은 Amazon VPC 사용 설명서의 [인터페이스 엔드포인트 생성](#)을 참조하세요.

이 서비스 이름을 사용하여 AWS Transform 사용자 지정에 대해 다음 VPC 엔드포인트를 생성합니다.

- com.amazonaws.*region*.transform-custom

*region*을 com.amazonaws.us-east-1.transform-custom과 같이 AWS Transform 사용자 지정 CLI를 사용하려는 AWS 리전으로 바꿉니다.

자세한 내용은 Amazon VPC 사용 설명서의 [인터페이스 엔드포인트를 통해 서비스 액세스](#)를 참조하세요.

AWS Transform 사용자 지정에 대한 VPC 엔드포인트 정책 생성

사용자 AWS Transform 지정에 대한 액세스를 제어하는 VPC 엔드포인트에 엔드포인트 정책을 연결할 수 있습니다. 이 정책은 다음 정보를 지정합니다.

- 작업을 수행할 수 있는 위탁자.
- 수행할 수 있는 작업.
- 작업을 수행할 수 있는 리소스.

자세한 내용은 Amazon VPC 사용 설명서의 [VPC 엔드포인트를 통해 서비스에 대한 액세스 제어](#)를 참조하세요.

예: AWS Transform 사용자 지정 작업에 대한 VPC 엔드포인트 정책

다음은 AWS Transform 사용자 지정에 대한 엔드포인트 정책의 예입니다. 엔드포인트에 연결되면 이 정책은 모든 리소스의 모든 보안 주체에 대해 나열된 AWS Transform 사용자 지정 작업에 대한 액세스 권한을 부여합니다.

```
{
  "Statement": [
    {
      "Principal": "*",
      "Effect": "Allow",
      "Action": [
        "transform-custom:*"
      ],
      "Resource": "*"
    }
  ]
}
```

온프레미스 컴퓨터를 사용하여 AWS Transform 사용자 지정 엔드포인트에 연결

이 섹션에서는 온프레미스 컴퓨터를 사용하여 AWS VPC의 AWS PrivateLink 엔드포인트를 통해 AWS Transform 사용자 지정에 연결하는 프로세스를 설명합니다.

1. [온프레미스 디바이스와 VPC 간에 VPN 연결을 생성합니다.](#)
2. [AWS Transform 사용자 지정을 위한 인터페이스 VPC 엔드포인트를 생성합니다.](#)
3. [인바운드 Amazon Route 53 엔드포인트를 설정합니다.](#) 이렇게 하면 온프레미스 디바이스에서 AWS Transform 사용자 지정 엔드포인트의 DNS 이름을 사용할 수 있습니다.

문제 해결

이 섹션에서는 사용자 지정 AWS 변환과 관련된 일반적인 문제를 해결하기 위한 지침을 제공합니다.

로그 위치

AWS 변환 CLI는 다음 위치에 로그를 유지합니다.

대화 로그:

Linux and macOS

```
~/.aws/atx/custom/<conversation_id>/logs/<timestamp>-conversation.log
```

Windows

```
%USERPROFILE%\aws\atx\custom\<conversation_id>\logs\<timestamp>-conversation.log
```

이러한 로그에는 특정 변환 실행을 디버깅하기 위한 전체 대화 기록이 포함되어 있습니다.

하위 에이전트 로그:

Linux and macOS

```
~/.aws/atx/custom/<conversation_id>/logs/subagents/<name>.log
```

Windows

```
%USERPROFILE%\aws\atx\custom\<conversation_id>\logs\subagents\<name>.log
```

이러한 로그에는 변환 중에 기본 에이전트가 생성하는 하위 에이전트의 출력이 포함됩니다. 하위 에이전트를 직접 관리할 필요는 없습니다.

개발자 디버그 로그:

Linux and macOS

```
~/ .aws/atx/logs/debug*.log  
~/ .aws/atx/logs/error.log
```

Windows

```
%USERPROFILE%\ .aws\atx\logs\debug*.log  
%USERPROFILE%\ .aws\atx\logs\error.log
```

이러한 로그는 CLI 작업 및 오류에 대한 자세한 정보를 제공합니다. 각 로그 파일은 롤오버되기 전에 5MB 제한이 있습니다. 이 디렉터리에는 debug1.log 및 debug2.log와 같은 여러 디버그 로그가 있을 수 있습니다.

공통 문제

설치 문제:

설치에 실패하면 Node.js 22 이상이 설치되어 있는지 확인합니다.

```
node --version
```

필요한 경우 <https://nodejs.org/en/download> Node.js를 다운로드합니다.

인증 문제:

자격 AWS 증명이 올바르게 구성되었는지 확인합니다.

```
aws sts get-caller-identity
```

IAM 사용자 또는 역할에 필요한 transform-custom:* 권한이 있는지 확인합니다.

네트워크 연결 문제:

연결 오류가 발생하면 필요한 엔드포인트에 대한 네트워크 액세스를 확인합니다.

- transform-cli.awsstatic.com

- `transform-custom.<region>.api.aws`
- `*.s3.amazonaws.com`

인터넷 제한 환경에서 작업하는 경우 방화벽 규칙을 업데이트하여 이러한 URLs 허용 목록에 추가합니다.

리전 구성 문제:

리전 관련 오류가 발생하는 경우:

- 리전이 지원되는지 확인
- 구성을 재정의할 수 있는 환경 변수를 확인합니다. `echo $AWS_REGION $AWS_DEFAULT_REGION`
- 리전 구성을 확인합니다. `aws configure get region`
- 필요한 경우 리전을 업데이트합니다. `aws configure set region <your-region>`
- 디버그 로그에서 리전 확인 세부 정보 확인

Git 문제:

Git이 설치되어 있고 리포지토리가 git 소스 제어 대상인지 확인합니다.

```
git --version
git status
```

AWS 사용자 지정 변환을 수행하려면 리포지토리가 git 소스 제어 대상이어야 합니다.

변환 실행 문제:

변환에 실패하는 경우:

1. 에서 대화 로그 검토 `~/.aws/atx/custom/<conversation_id>/logs/`
2. 변환 출력에서 빌드 또는 테스트 실패 확인
3. 프로젝트에 빌드 명령이 올바른지 확인
4. 대화형 모드에서 변환을 실행하여 피드백을 제공하세요.

대화 재개 문제:

대화를 재개할 수 없는 경우:

- 대화가 30일 미만인지 확인
- 대화 ID가 올바른지 확인
- 네트워크 연결이 있는지 확인

지원 받기

추가 지원이 필요하면 [AWS 콘솔](#)을 통한 AWS 지원을 참조하세요.

지원 티켓을 열 때 다음을 포함합니다.

- 의 대화 로그 ~/.aws/atx/custom/<conversation_id>/logs/
- 의 하위 에이전트 로그 ~/.aws/atx/custom/<conversation_id>/logs/subagents/
- 에서 로그 디버깅 ~/.aws/atx/logs/
- 문제를 재현하는 단계
- AWS 변환 CLI 버전(atx --version)

S3 액세스 문제

AWS 변환 사용자 지정 서비스는 S3 미리 서명된 URLs 제공하여 클라이언트 시스템과 잠재적으로 큰 변환 파일을 쉽게 업로드하고 다운로드할 수 있도록 합니다. 즉, CLI는 AWS 변환 서비스 엔드포인트와 상호 작용할 뿐만 아니라 S3 서비스 엔드포인트와도 상호 작용합니다. 이러한 상호 작용은 미리 서명된 URLs 사용하므로 클라이언트의 IAM 자격 증명에 S3 권한이 필요하지 않지만 로컬 시스템의 프록시 서버 구성과 네트워크의 S3 VPC 엔드포인트 정책이이 트래픽을 제한할 수 있습니다.

변환 파일 다운로드 및 업로드와 관련된 도구 실패 또는 S3 액세스 거부의 근본 원인을 찾는 데 도움이 되는 [the section called “로그 위치”](#) 자세한 오류 메시지를 검토하세요.

https_proxy 및 no_proxy 환경 변수를 활용하는 VPN/프록시 서버를 사용하는 경우 환경 no_proxy 변수 값에 다음 값을 추가하여 S3 및 사용자 지정 서비스 엔드포인트 AWS 변환에 대한 프록시를 우회하는 것이 좋습니다.

Linux and macOS

```
export no_proxy=.s3.amazonaws.com,transform-custom.<region>.api.aws
```

Windows (PowerShell)

```
$env:no_proxy=".s3.amazonaws.com,transform-custom.<region>.api.aws"
```

VPC에서 [AWS Amazon S3용 PrivateLink](#)를 사용하는 경우 S3 트래픽을 제한하는 정책이 정의되어 있을 수 있습니다. S3 VPC 엔드포인트 정책이 사용자 지정 서비스 소유 버킷 AWS에 대해 GetObject 및 PutObject 작업을 허용하는지 확인하세요. VPC 엔드포인트 정책에 다음 문을 추가하여이 작업을 수행할 수 있습니다.

```
{
  "Effect": "Allow",
  "Principal": "*",
  "Action": ["s3:PutObject", "s3:GetObject"],
  "Resource": "arn:aws:s3::aws-transform-custom-*/*"
}
```

정책의 명시적 Deny 문이 Allow 문보다 우선합니다. 액세스를 제한할 수 있는 Deny 문에 대한 S3 VPC 엔드포인트 정책을 검토합니다.

AWS CLI 버전 기록 변환

AWS 변환 CLI의 현재 및 이전 릴리스에 대한 자세한 내용은 다음 표를 검토하세요. 테이블에는 각 버전의 버전, 릴리스 날짜 및 릴리스 정보가 포함되어 있습니다.

버전	릴리스 날짜	릴리스 노트
3.6.0(최신)	2026년 7월 17일	- 이전 실행을 기반으로 변환 정의에 대해 자동으로 생성된 학습을 보고 관리할 수 있는 대화형 TUI 세션을 여는 <code>atx custom def learnings</code> 하위 명령이 추가되었습니다. - 변환 실행 중에 사용량 원격 측정 수집이 추가되었습니다. 원격 측정을 비활성화하려면 <code>ATX_DISABLE_TELEMETRY=true</code> 환경 변수를 설정합니다. 자세한 내용은 사용량 원격 측정 단원을 참조하십시오. - Windows에서 ~ (홈 디렉터리) 경로를 사용하는 파일 작업이 예기치 않은 디렉터리로 해결되는 문제를 수정했습니다. 이로 인해 세션 중에 파일 읽기/쓰기가 실패했습니다.

버전	릴리스 날짜	릴리스 노트
		특수 문자가 포함된 MCP 서버 및 도구 이름으로 인해 연결 실패가 발생할 수 있는 문제를 수정했습니다. 이제 CLI는 유효한 문자만 사용하도록 이름을 자동으로 삭제합니다.
3.5.0	2026년 7월 8일	- 기본 Windows 지원이 추가되었습니다. 이제 Windows에서 직접 사용자 지정 AWS 변환 명령을 실행할 수 있습니다. (Windows에서는 아직 <code>atx ct</code> 명령이 지원되지 않음) - 에이전트 준비 및 현대화 준비 분석에 기본 설정을 반영 <code>atx ct analysis run</code>하도록에 조향 입력을 추가했습니다. 전략적 프레이밍 <code>--context</code> 에 <code>--agent-scope</code> 를 사용하고, 에이전트 준비에 대한 에이전트 액세스를 설정하고, <code>--prefer/--avoid</code>를 사용하여 특정 기술에 대한 현대화 권장 사항을 조정합니다. - 이제 스킴 형식의 변환 정의에 <code>scripts/</code> 폴더가 포함될 수 있으므로 <code>SKILL.md</code> 및 참조와 함께 헬퍼 스크립트를 번들링할 수 있습니다. - 수정이 완료될 때까지 대기 <code>atx ct remediation create</code>하는가 <code>--wait</code>에 추가되었습니다. - 원샷 실행을 위한 헤드리스 모드가 추가되었습니다. 를 실행 <code>atx -x "prompt" -t</code>하여 프롬프트를 전달하고, 응답을 받고, 대화형 프롬프트 없이 종료합니다. 헤드리스 모드에서는 모든 도구를 신뢰해야 합니다.
3.4.1	2026년 7월 2일	버전 3.4.0에서 도입한 대화형 세션 문제를 수정했습니다. 에이전트가 응답을 완료한 후 CLI는 입력 프롬프트로 돌아가는 대신 "Thinking" 프롬프트(UI에 줄임표로 표시됨)를 유지할 수 있습니다. 이제 CLI는 각 응답 후 입력 프롬프트로 돌아갑니다.

버전	릴리스 날짜	릴리스 노트
3.4.0(권장되지 않음)	2026년 6월 29일	 알려진 문제 대화형 세션에서 CLI는 에이전트가 응답을 완료한 후 "Thinking" 프롬프트(UI에 줄임표로 표시됨)를 유지할 수 있습니다. 이렇게 하면 다음 메시지를 입력할 수 없습니다. 이 문제를 해결하려면 실행하여 버전 3.4.1 이상으로 업그레이드합니다 <code>atx update</code>. - 스크립팅 및 자동화를 위한 전체 <code>atx ct</code> 명령 표면의 기계 판독 가능 매니페스트 <code>atx ct schema</code> 인가 추가되었습니다. - 소스 추가 또는 업데이트 시 토큰 범위 검증이 추가되어 분석 중 나중에 실패하는 대신 자격 증명 또는 권한 문제가 즉시 표시됩니다. - 결과 컨텍스트를 포함하고 보다 검토 가능한 PRs. - 현재 활동, 예상 에이전트 분 및 하위 에이전트 활동에 대한 실시간 컨텍스트로 CLI 진행 상황 피드백을 개선했습니다. <code>ATX_GIT_COMMITTER_NAME</code> 및 <code>ATX_GIT_COMMITTER_EMAIL</code> 환경 변수를 통해 구성 가능한 체크포인트 커밋 작성자 자격 증명을 추가했습니다. - 다양한 소규모 버그 수정 및 개선.
3.3.0	2026년 6월 18일	<code>atx ct</code> 명령 간에 일관성 <code>--json</code>과 <code>--help</code> 지원이 추가되었습니다. - 설정 중에 에이전트 공간이 생성되고 해체 시 제거되도록 보안 에이전트 설정을 수정했습니다. - 다양한 소규모 버그 수정 및 개선.

버전	릴리스 날짜	릴리스 노트
3.2.0	2026년 6월 15 일	• 모든 사용자의 표준 CLI 배포에 지속적 현대화 명령(atx ct)이 추가되었습니다. • 서버 응답을 기다리는 동안 "Thinking..." 스피너를 표시하도록 하위 에이전트 실행을 개선하여 작업이 진행 중이라는 명확한 시각적 피드백을 제공했습니다. • 에이전트 출력 후 3초가 지나면 "작업 중..."으로 자동으로 다시 시작하도록 스피너가 개선되어 처리 단계 사이에 터미널이 고정되지 않습니다. • 은은하게 반짝이는 애니메이션을 사용하여 보다 정교한 시각적 모양을 위해 사고 스피너를 개선했습니다.
3.1.0	2026년 6월 3일	• 최대 검증 루프를 구성하기 위한 ATX_MAX_VALIDATION_LOOPS 환경 변수가 추가되었습니다. • 설치된 버전이 레지스트리 버전보다 이미 최신 버전인 경우 수정 업데이트 검사에 더 이상 잘못된 "업데이트 사용 가능" 경고가 표시되지 않습니다. • 가 더 이상 비의미한 확인 프롬프트를 표시delete -- transformation-name "" 하지 않도록 수정했습니다. 이제 빈 값이 명확한 검증 오류와 함께 거부됩니다. • 이제 인식할 수 없는 하위 명령이 혼동되는 내부 오류 메시지 대신 "알 수 없음 명령"으로 표시됩니다. • 업데이트 검사에 문자열 불평등 대신 숫자 비교를 사용하도록 버전 비교를 수정했습니다.

버전	릴리스 날짜	릴리스 노트
3.0.0	2026년 5월 21 일	- 이름을 찾을 수 없을 때 레지스트리에서 유사한 이름을 제안하는 사전 변환 이름 검증이 추가되어 별도의 목록 명령 없이 오타를 포착할 수 있습니다. - 셸 명령에 대한 선택적 설명을 추가하여 셸 명령이 수행하는 작업과 이유를 보여줍니다. - 도구 권한에 대한 자세한 정보를 포함하도록 신뢰 설정 배너를 개선했습니다. - do-not-learn 플래그를 사용할 때 학습 비활성화 배너가 추가되어 학습 기능과 활성화 방법을 확인할 수 있습니다. - 주요 변경 사항: 이제 Node.js 22 이상이 필요합니다. 이전 버전을 사용하는 경우 https://nodejs.org/ 업그레이드합니다.

버전	릴리스 날짜	릴리스 노트
2.0.0	2026년 5월 14 일	- 원격 MCP 서버 지원 추가 - 자동 SSE 폴백, 헤더의 환경 변수 확장을 통한 베어러 토큰 인증, 프록시 지원(HTTP_PROXY/HTTPS_PROXY)을 사용하여 HTTP 및 HTTPS MCP 서버에 연결합니다. - atx resume 하위 명령을의 별칭으로 추가했습니다atx -- resume. - 출력 제어를 사용하는 다중 파일 텍스트 검색 grep 도구 추가 - 정규식 패턴, 파일 glob 필터링, 대/소문자를 구분하지 않는 검색, 구성 가능한 깊이/결과 제한 및 출력 잘림을 지원합니다. - 보다 일관된 동작과 향후 MCP 기능에 대한 더 쉬운 지원을 위해 표준 MCP SDK를 사용하도록 MCP 구현을 개선했습니다. - 셸 출력 처리 개선 - 이제 출력이 하드 오류를 발생시키는 대신 스트림당 30K 문자로 정상적으로 잘려 컨텍스트에 대한 출력의 시작과 끝을 유지합니다. - 대화형 세션 중에 현재 작업을 중단하고 프롬프트로 돌아가는 대신 Linux/macOS에서 Ctrl+C가 CLI를 조기에 종료할 수 있는 문제를 수정했습니다. - 명령에 권한 부여가 필요한 이유와 별도로 신뢰를 사용할 수 없는 이유에 대한 전용 이유를 표시하도록 신뢰 거부 메시지가 수정되었습니다. - 명령이에 있을 때 더 이상 신뢰를 언급하지 않는 위험한 명령 경고를 수정했습니다alwaysPromptCommands .

버전	릴리스 날짜	릴리스 노트
1.10.0	2026년 4월 29일	• 도구 간 지침으로 도구 설명을 개선하여 에이전트가 각 작업에 가장 적합한 도구를 선택하고 불필요한 셀 사용을 줄일 수 있습니다. • <code>alwaysPromptCommands</code>에 추가됨 <code>trust-settings.yaml</code> - 신뢰 설정에 관계없이 항상 명시적 권한이 필요한 셀 명령 패턴을 구성합니다. 복합 표현식에서 각 하위 명령에 대한 glob 와일드카드 및 일치를 지원합니다. 이러한 패턴을 재정의 <code>trustedShellCommands</code> 할 수 있습니다. 자동 파이프라인이 손상되지 않도록 비대화형 모드에서는 적용되지 않습니다. • 절대 경로로 해석되지 않는 상대 경로를 수정했습니다.
1.9.0	2026년 4월 23일	• 도구 승인 프롬프트 개선 - 이제 각 옵션에 인라인으로 수행하는 작업이 표시되고, 승인이 필요한 이유를 설명하는 “이유” 메시지가 표시되며, 신뢰 확인에는 영구적인 신뢰 <code>trust-settings.yaml</code>에 대한 힌트가 포함됩니다.
1.8.0	2026년 4월 16일	• 사용자 입력과 에이전트 출력을 보다 명확하게 시각적으로 구분> 하기 ATX: 위해 에이전트 출력 접두사에서 로 변경했습니다. • CLI 재시도가 소진될 때 재개 명령 표시를 수정했습니다. • 다른 작업 디렉터리에서 재개를 수정했습니다. 대화형 모드에서는 수정된 경로를 묻는 메시지를 표시하고, 비대화형 모드에서는 설명 오류와 함께 빠르게 실패합니다.
1.7.1	2026년 4월 9일	• 자격 증명 공급자 리전이 프로필의과 다를 때 SSO 로그인 실패(“세션 토큰을 찾을 수 없거나 유효하지 않음”)를 수정했습니다 <code>sso_region</code>. • 디스크에서 자격 증명을 교체할 때 장기 실행 세션이 더 이상 실패하지 않도록 자격 증명 캐싱을 수정했습니다.

버전	릴리스 날짜	릴리스 노트
1.7.0	2026년 4월 2일	- 입력 검증 오류 시 코드 1과 함께 종료하는 <code>exec</code> 명령을 수정하여 스크립트 및 CI/CD 파이프라인에서 CLI를 안정적으로 유지합니다. - 서비스의 경고 메시지 표시를 추가했습니다. - AWS 자격 증명 프로필에 대한 MFA 프롬프트 지원이 추가되었습니다. - HTTP(S) 프록시 설정을 준수하기 위해 STS 자격 증명 호출을 수정했습니다.
1.6.0	2026년 3월 18일	<code>exec</code> 및 <code>interactive</code> 명령에 대한 에이전트 분 예산을 설정하는 <code>--limit <minutes></code> 옵션이 추가되었습니다. 한도에 도달하면 CLI에 사용량이 표시되고 재개 지침과 함께 종료됩니다. - 대화 로그에서 초기 사용자 메시지의 로깅을 수정했습니다.
1.5.0	2026년 3월 11일	- 동시 작업 실행에 대한 지원이 추가되어 더 빠른 변환이 가능합니다. - 각 대화가 끝날 때 Agent Minutes 사용량이 표시되고 대화형 모드에서 언제든지 사용량을 확인하는 <code>/usage</code> 명령이 추가되었습니다.
1.4.0	2026년 3월 2일	- 지원되지 않는 파일로 변환 정의를 저장할 때 오류 메시지가 개선되었습니다. - 연결이 중단될 때 CLI가 중단되지 않도록 서비스 호출에 제한 시간이 추가되었습니다. - 완료 후 CLI 프로세스가 중단되는 문제를 수정했습니다. - 대화를 재개할 때 리전 검증을 수정했습니다.
1.3.0	2026년 2월 19일	- MCP 서버 경로에 대한 제한 제거 - 이제 사용자는 MCP 구성에서 <code>command</code> 속성에 대한 경로를 지정할 수 있습니다. - MCP 서버 연결의 안정성이 향상되었습니다.

버전	릴리스 날짜	릴리스 노트
1.2.0	2026년 2월 9일	- 환경 변수(https_proxy , no_proxy등)를 통한 프록시 구성에 대한 지원이 추가되었습니다. - 일반적인 안정성 개선 및 버그 수정.
1.1.1	2026년 1월 16일	버그를 수정하고 안정성을 개선했습니다.
1.1.0	2026년 1월 13일	AWS CLI 리전 구성 지원, 조기 자격 증명 검증 검사 및 고정 캠페인 재개 기능이 추가되었습니다.
1.0.1	2025년 12월 18일	정상적인 종료, 더 깨끗한 오류 로그 및 일반적인 개선 사항.
1.0.0	2025년 12월 1일	AWS 변환 CLI의 최초 릴리스입니다.

AWS 지속적인 현대화 혁신

지속적인 현대화 AWS 혁신이란 무엇입니까?

AWS 지속적인 현대화를 혁신하면 소스 코드 리포지토리에 대한 분석 및 수정이 가능합니다. GitHub 조직, GitLab 그룹, Bitbucket 워크스페이스 및 로컬 리포지토리를 연결한 다음 자동화된 분석을 실행하여 전체 코드베이스에서 기술적 부채, 보안 취약성, 현대화 기회 및 에이전트 준비를 식별할 수 있습니다.

모든 분석 및 수정은 자격 증명을 AWS 계정 사용하여에서 실행됩니다. 소스 코드는 사용자가 제어할 수 있습니다.

Note

Kiro Power 또는 에이전트 플러그인으로 시작하는 것이 좋습니다. 에이전트 스킴은 인프라 프로비저닝, 소스 구성, 분석 실행, 결과 분류 및 문제 해결을 포함한 지속적인 현대화의 설정, 온보딩 및 지속적인 사용을 오케스트레이션합니다. 설치 지침은 [개발자 도구](#)를 확인하세요.

주요 기능

AWS 지속적인 현대화 혁신은 다음과 같은 기능을 제공합니다.

- 기술 부채 분석 - 오래된 종속성, 보안 취약성, 코드 품질 문제 및 현대화 기회가 있는지 리포지토리를 스캔합니다. 패키지 매니페스트 또는 포괄적인 코드 수준 분석에서 빠른 메타데이터 스캔을 실행합니다. 환경에 맞는 변환 정의를 사용하여 사용자 지정 분석 기준을 정의합니다.
- 자율 문제 해결 - 대규모로 검증된 풀 요청을 생성합니다. 연결된 변환 정의를 사용하여 각 결과를 자동으로 수정할 수 있습니다. 문제 해결은 GitHub, GitLab 및 Bitbucket에서 브랜치를 생성하고 PRs/MRs 자동으로 엽니다.
- 보고 - 심각도, 리포지토리 및 분석 유형별로 조사 결과를 보여주는 HTML 보고서를 생성합니다. 시간 경과에 따른 문제 해결 진행 상황 및 결과 해결을 추적합니다.
- 지속적 모니터링 - Amazon EventBridge 스케줄러를 사용하여 반복 분석을 예약합니다. 포트폴리오에 새로운 문제가 있는지 지속적으로 모니터링하도록 일별, 주별 또는 사용자 지정 cron 일정을 구성합니다.

분석 유형

AWS 지속적인 현대화 혁신은 현대화 요구 사항을 해결하기 위해 다음과 같은 분석 유형을 지원합니다.

유형	설명
rapid-techdebt-analysis	오래된 버전과 오래된 종속성을 식별하기 위한 패키지 매니페스트(pom.xml, package.json, requirements.txt)의 빠른 메타데이터 전용 스캔. 소스 코드를 분석하지 않습니다.
tech-debt-comprehensive	AWS 변환 에이전트를 사용한 심층 코드 수준 기술 부채 분석. 소스 코드를 검사하여 부채 패턴, 코드 품질 문제, 아키텍처 문제 및 개선 기회를 식별합니다.
security	Security Agent를 사용한 AWS 보안 취약성 및 CVE 탐지. 소스 코드 및 종속성에서 알려진 취약성, 안전하지 않은 코딩 패턴 및 악용 가능한 약점을 스캔합니다. 일회성 인프라 설정이 필요합니다.
agentic-readiness	AI 및 에이전트 통합 준비 상태 평가. 인프라 및 플랫폼, 애플리케이션 아키텍처, 데이터 기반, Identity/Security/Governance, 운영 및 관찰성의 5가지 범주에서 기준 56점을 획득합니다.
modernization-readiness	클라우드 현대화 기회 평가. 인프라, 애플리케이션, 데이터, 보안 및 운영 차원에서 준비 상태를 평가합니다. 컨테이너화, 서버리스 마이그레이션 및 플랫폼 업그레이드의 후보를 식별합니다.
custom	변환 정의(TD)를 분석으로 실행합니다. 이 유형을 사용하여 자체 분석 기준을 정의하거나 기본 제공 유형에서 다루지 않는 AWS 관리형 변환을 실행합니다.

주요 개념 이해

소스

소스는 리포지토리의 위치를 지속적으로 현대화합니다. 지원되는 소스 유형:

- GitHub - 개인 액세스 토큰이 있는 조직(클래식)
- GitLab - 자체 호스팅 인스턴스를 포함한 그룹 또는 사용자
- Bitbucket — Workspaces(클라우드) 또는 프로젝트(데이터 센터)
- 로컬 - git 리포지토리가 포함된 상위 디렉터리

리포지토리

리포지토리는 스캔 소스에서 검색됩니다. 검색 후 소스, 레이블 또는 기타 기준을 기준으로 필터링하고, 조직(팀, 우선순위, 마이그레이션 웨이브)에 레이블을 적용하고, 분석 또는 문제 해결을 위해 특정 리포지토리를 대상으로 지정할 수 있습니다.

분석

분석은 특정 분석 유형을 사용하여 하나 이상의 리포지토리를 스캔하는 것입니다. 각 분석은 코드의 문제를 식별하는 결과를 생성합니다. 필요에 따라 분석을 실행하거나 자동으로 실행되도록 예약할 수 있습니다. 분석 유형에는 rapid-techdebt-analysis, tech-debt-comprehensive, security, agentic-readiness, modernization-readiness 및 custom이 포함됩니다. 각 분석은 상태(보류 중, 실행 중, 완료, 취소 또는 실패)와 스캔한 리포지토리를 추적합니다.

조사 결과

결과는 분석 결과입니다. 각 결과에는 심각도(높음, 중간 또는 낮음), 상태(열림, 무시됨 또는 더 이상 사용되지 않음), 이를 해결할 수 있는 수정 변환(자동 수정 가능한 경우)이 포함됩니다. 새 조사 결과는 열린 상태로 시작됩니다. 사용자는 이유와 함께 조사 결과를 무시할 수 있습니다. 재분석은 해결된 결과를 자동으로 더 이상 사용되지 않는 것으로 표시합니다.

문제 해결

문제 해결은 변환 정의를 적용하여 결과를 수정합니다. 조사 결과 기반(각 조사 결과는 자체 수정 변환 사용), TD 재정의(지정된 조사 결과에 대한 변환 정의 재정의), 직접 TD(조사 결과 없이 리포지토리에 대한 변환 실행)의 세 가지 모드입니다. 출력은 소스 공급자(GitHub PR, GitLab MR, Bitbucket PR 또는 로컬 브랜치)에 따라 달라집니다.

변환 정의

변환 정의에는 특정 코드 변환을 수행하는 데 필요한 지침과 지식이 포함되어 있습니다. 지속적인 현대화는 사용자 지정 분석(--type custom --transformation-name *name*) 및 문제 해결()에 변환 정의를 사용합니다--transformation-name *name*. 를 사용하여 사용 가능한 변환 정의를 나열합니다atx custom def list.

지속적 현대화 AWS 의 작동 방식

AWS 변환 지속적 현대화는 일반적으로 여러 코드베이스에 지속적인 분석 및 수정이 필요한 대규모 프로젝트에서 사용됩니다. 팀은 일반적으로 다음 워크플로를 따릅니다.

1. 소스 연결 - GitHub 조직, GitLab 그룹, Bitbucket 워크스페이스 또는 로컬 디렉터리를 소스로 추가합니다. 인증 토큰에 적절한 범위를 제공합니다.
2. 리포지토리 검색 - 검색 스캔을 실행하여 소스의 모든 리포지토리를 열거합니다. 레이블을 사용하여 팀, 우선순위 또는 마이그레이션 웨이브별로 리포지토리를 구성합니다.
3. 분석 실행 - 포트폴리오에서 분석을 실행합니다. 빠른 결과를 얻으려면 빠른 스캔을 선택하고 자세한 결과를 얻으려면 포괄적인 분석을 선택합니다. 보안 분석에는 일회성 인프라 설정이 필요합니다.
4. 결과 분류 - 심각도, 리포지토리 또는 분석 유형별로 결과를 검토합니다. 문서화된 이유와 함께 거짓 긍정을 무시합니다. 분석을 다시 실행하여 해결된 문제를 더 이상 사용되지 않음으로 표시합니다.
5. 문제 해결 - 문제 해결을 생성하여 조사 결과를 수정합니다. 지속적 현대화는 브랜치를 자동으로 생성하고 수정 사항을 사용하여 풀/병합 요청을 엽니다. 문제 해결 상태를 추적하고 실패를 다시 시도합니다.
6. 연속 분석 설정 - Amazon EventBridge 스케줄러를 사용하여 반복 분석을 예약합니다. 분석 주기(일별, 주별 또는 사용자 지정 cron)를 구성하여 포트폴리오에 새로운 문제가 있는지 지속적으로 모니터링합니다. 자동 문제 해결과 결합하여 시간이 지남에 따라 코드 상태를 유지합니다.

컴퓨팅 옵션

지속적 현대화는 분석 및 문제 해결을 실행하기 위한 세 가지 컴퓨팅 옵션을 지원합니다. Kiro Power 및 에이전트 플러그인의 에이전트 스킴은 각 옵션에 대한 인프라를 설정하는 데 도움이 됩니다.

Note

컴퓨팅 옵션과 관계없이 모든 분석 및 수정은 자격 증명을 사용하여 AWS 계정 에서 수행됩니다. 소스 코드는 사용자가 제어할 수 있습니다.

로컬(기본값)

기본적으로 분석은 로컬 시스템에서 실행됩니다. 이 옵션에는 추가 인프라가 필요하지 않습니다. 서버는 로컬에서 실행되고 로컬 컴퓨팅 리소스를 사용하여 분석을 실행합니다. 도구, 작은 리포지토리 또는 개별 사용을 시도하는 데 적합합니다.

Amazon EC2

의 영구 Amazon EC2 인스턴스에서 분석을 실행합니다 AWS 계정. 이 옵션은 로컬 시스템에서 컴퓨팅을 오프로드하고, 대규모 분석을 지원하고, 예약된 반복 분석을 활성화합니다. 인스턴스는 제출 사이에 계속 실행됩니다.

에이전트 스킬은 다음을 포함하는 AWS CloudFormation 스택을 프로비저닝합니다.

- Docker 및 지속적 현대화 컨테이너가 있는 Amazon EC2 인스턴스(Amazon Linux 2023)
- AWS 변환, Amazon S3, AWS KMS, Secrets Manager 및 보안 에이전트에 대한 권한이 있는 IAM 역할
- AmazonSSMManagedInstanceCore SSM을 통한 셸 액세스용(SSH 키 페어 또는 인바운드 포트 필요 없음)
- 인바운드 규칙이 없는 보안 그룹

IAM 사용자 또는 역할에는 Amazon EC2 수명 주기 관리, AWS CloudFormation 스택 작업, IAM 역할 생성, Amazon S3 버킷 작업, Secrets Manager 보안 암호 관리 및 SSM 명령에 대한 권한이 필요합니다.

EC2 실행을 설정하려면 Kiro Power 또는 에이전트 플러그인을 설치한 다음(참조 [개발자 도구](#)) 에이전트에게 “지속적인 현대화 분석을 위해 EC2 인스턴스 설정”을 요청합니다. 에이전트는 인프라를 프로비저닝하고, 컨테이너가 정상인지 확인하고, SSH 없이 SSM을 통해 분석을 제출합니다.

AWS 배치(Fargate)

서버리스 컴퓨팅을 위해 Fargate를 사용한 AWS 배치에서 격리된 작업으로 분석을 실행합니다. 각 분석은 영구 인프라를 관리하지 않고 자체 컨테이너에서 실행됩니다. 여러 소스 또는 분석 유형의 병렬 분석에 적합합니다.

이 옵션은 AWS 변환 CDK 인프라 스택을 재사용합니다. 에이전트 스킬은 다음을 포함하여 필요한 인프라를 배포합니다.

- AWS 배치 작업 대기열 및 컴퓨팅 환경

- 지속적 현대화 컨테이너 이미지를 사용한 작업 정의
- 배치 작업 실행을 위한 IAM 역할
- 작업 제출을 위한 Lambda 함수

배치 실행을 설정하려면 Kiro Power 또는 에이전트 플러그인을 설치한 다음(참조 [개발자 도구](#)) 에이전트에게 "Fargate에서 내 분석 실행" 또는 "지속적인 현대화를 위한 배치 실행 설정"을 요청합니다. 에이전트는 CDK 스택을 배포하고, 소스 자격 증명을 Secrets Manager에 저장하고, 분석 작업을 AWS Batch에 제출합니다.

보안 에이전트 설정

security 분석 유형은 취약성 및 CVE 탐지를 위해 AWS Security Agent 서비스를 사용합니다. 다른 분석 유형과 달리에서 일회성 인프라 설정이 필요합니다 AWS 계정.

설정 명령은 다음을 포함하는 AWS CloudFormation 스택을 프로비저닝합니다.

- 소스 코드 업로드를 위한 Amazon S3 버킷
- 에서 수입하는 IAM 역할 securityagent.amazonaws.com
- 보안 에이전트 역할에 대한 관리형 정책

설정을 실행하려면 IAM 사용자 또는 역할에 다음과 같은 추가 권한이 있어야 합니다.

- cloudformation:CreateStack, cloudformation:UpdateStack, cloudformation:DescribeStacks
- iam:CreateRole, iam:PutRolePolicy, iam:AttachRolePolicy, iam:CreatePolicy
- s3:CreateBucket, s3:PutBucketEncryption, s3:PutBucketPublicAccessBlock

다음 명령을 사용하여 보안 에이전트 인프라를 관리합니다.

```
# Provision the security agent infrastructure
atx ct setup security-agent

# Check the status
atx ct setup security-agent --status

# Delete the infrastructure
atx ct setup security-agent --delete
```

설정이 완료되면 다른 분석 유형과 동일한 방식으로 보안 분석을 실행할 수 있습니다.

시작하기

사전 조건

지속적인 현대화를 효과적으로 사용하려면 Git 버전 제어, 소스 코드 플랫폼(GitHub, GitLab 또는 Bitbucket)에 대한 지식, AWS IAM 권한에 대한 실무 지식, 명령줄 도구에 대한 경험을 기본적으로 이해해야 합니다.

지속적 현대화를 사용하기 전에 다음이 있는지 확인합니다.

- AWS 설치된 CLI 변환:

```
curl -fsSL https://transform-cli.awsstatic.com/install.sh | bash
```

- Node.js 22 이상
- 유효한 AWS 자격 증명(AWS_PROFILE 또는 환경 변수)
- IAM 사용자 또는 역할에 AWSTransformCustomFullAccess 연결된 AWS 관리형 정책

빠른 시작

1. 지속적 현대화 서버를 시작합니다.

```
atx ct server &
```

2. 소스 추가:

```
atx ct source add --name name --provider provider --org org-or-group --token token
```

여기서 *name*은 소스의 설명 식별자이고, *provider*는 플랫폼(github, bitbucket, 또는 local)이고 gitlab, *org-or-group*은 조직 또는 그룹 이름이고, *token*은 인증 토큰입니다.

3. 리포지토리 검색:

```
atx ct discovery scan --source name
```

4. 분석을 실행합니다.

```
atx ct analysis run --type type --source name --wait
```

5. 조사 결과 살펴보기:

```
atx ct findings list --json
```

6. 결과 수정:

```
atx ct remediation create --ids id1,id2 --name "remediation-name"
```

지속적인 현대화 작업

소스 관리

atx ct source 명령을 사용하여 리포지토리를 연결합니다. 지원되는 공급자: GitHub, GitLab, Bitbucket, local.

GitHub 조직

토큰: repo 범위가 있는 개인 액세스 토큰(클래식). 분석의 경우 읽기 전용, 문제 해결을 위한 전체 리포지토리.

```
atx ct source add --name name --provider github --org org --token pat
```

GitLab 그룹 및 사용자

토큰: api 범위가 있는 개인 액세스 토큰입니다.

```
atx ct source add --name name --provider gitlab --org group-or-user --token pat
# Self-hosted:
atx ct source add --name name --provider gitlab --org group-or-user --token pat --url
https://gitlab.example.com
```

Bitbucket 워크스페이스 및 프로젝트

Bitbucket Cloud - 범위: read:repository:bitbucket, write:repository:bitbucket, read:pullrequest:bitbucket, write:pullrequest:bitbucket. 또한 --email 및가 필요합니다--username.

```
atx ct source add --name name --provider bitbucket --org workspace --token api-token --email email --username username
```

Bitbucket 데이터 센터:

```
atx ct source add --name name --provider bitbucket --org project-key --token http-access-token --url https://bitbucket.example.com
```

로컬 리포지토리

```
atx ct source add --name name --provider local --path parent-directory
```

Important

--path는 단일 리포지토리가 아닌 하위 디렉터리로 git 리포지토리가 포함된 상위 디렉터리를 가리켜야 합니다.

소스 관리

```
atx ct source list
atx ct source remove --name name
```

리포지토리 검색 및 관리

```
atx ct discovery scan --source name
atx ct discovery status --source name
atx ct discovery scan --source name --path new-directory
```

검색 후:

```
atx ct repository list
atx ct repository list --source name
atx ct repository list --labels "team:frontend,priority:high"
atx ct repository update --source name --repo "source::slug" --labels "team:frontend,priority:high"
atx ct repository update --source name --labels "migration:wave-1"
```

분석 실행

--type 플래그는 실행할 분석의 종류를 지정합니다.

- rapid-techdebt-analysis - 오래된 종속성과 쉬운 성공.
- tech-debt-comprehensive - 종속성, 보안, 패턴, 성능, 유지 관리 가능성, 아키텍처, 코드 품질 및 인프라 조사 결과를 다루는 더 심층적인 AI 기반 분석.
- security - 보안 취약성 및 노출.
- agentic-readiness - AI 에이전트를 위한 리포지토리 준비 상태(프레임워크, APIs, 설명서).
- modernization-readiness - 인프라, 애플리케이션, 데이터, 보안 및 운영 차원 전반의 현대화 기회.

```
atx ct analysis run --type type --source name [--repo source::slug] [--wait]
atx ct analysis get --id id --json
atx ct analysis list --json
atx ct analysis list --status pending/running/complete/cancelled/failed --json
atx ct analysis list --type type --json
atx ct analysis cancel --id id
atx ct analysis delete --id id [--cascade-findings]
```

사용자 지정 분석

```
atx ct analysis run --type custom --transformation-name name --source source --
repo source::slug --wait
```

-g 플래그가 있는 구성: 카값, JSON 또는 파일 경로.

TDs 나열: `atx custom def list`

조사 결과 관리

```
atx ct findings list --json
atx ct findings list --repo source::slug --source name --severity high/medium/low
--type analysis-type --status open/dismissed/obsolete --analysis-id id --fix-
transform transform-name --json
```

상태 찾기

- open - 활성
- dismissed - 수동으로 무시됨(이유 필요)
- obsolete - 재분석으로 더 이상 조사 결과가 생성되지 않을 때 시스템 설정

```
atx ct findings update --id id --status dismissed --reason "reason"
atx ct findings update --id id --status open
atx ct findings batch-update --ids id1,id2 --status dismissed --reason "reason"
atx ct findings get --id id
atx ct findings delete --id id
```

폐기 결과

재분석은 해결된 결과를 더 이상 사용되지 않는 것으로 표시합니다. 다시 열 수 없습니다. 감사용으로 보관됩니다.

문제 해결 생성

결과 기반, TD 재정의, 직접 TD의 세 가지 모드입니다.

```
atx ct remediation create --ids id1,id2 --name "name"
atx ct remediation create --ids id1,id2 --transformation-name TD
atx ct remediation create --transformation-name TD --repo source::slug
```

공급자별 출력: GitHub PR, GitLab MR, Bitbucket PR, Local branch.

Note

토큰에는 PR/MR 생성을 위한 쓰기 액세스 권한이 있어야 합니다.

--local 플래그가 있는 로컬 실행.

```
atx ct remediation create --transformation-name TD --repo source::slug -g
  "additionalPlanContext=Upgrade to Node.js 22"
atx ct remediation list
atx ct remediation status --id id
atx ct remediation retry --id id
```

```
atx ct remediation delete --id id
```

AWS 웹 애플리케이션 변환(선택 사항)

AWS 변환 웹 애플리케이션은 코드 소스 포트폴리오 전반에서 지속적인 현대화 분석, 조사 결과 및 문제 해결을 모니터링하기 위한 선택적 인터페이스입니다.

AWS 변환 웹 애플리케이션을 사용하기 전에 조직의 AWS 변환에 액세스하려면 사용자 자격 증명이 활성화되어 있어야 합니다. AWS 변환 활성화에 대한 자세한 내용은 [AWS 변환 설정을 참조하세요](#).

AWS 변환 웹 애플리케이션을 사용하려면:

1. <https://aws.amazon.com/transform/>를 방문하여 AWS IAM Identity Center 자격 증명을 사용하여 로그인합니다.
2. 로그인한 후 지속적인 현대화가 나타나지 않으면 대신 IAM 자격 증명으로 로그인합니다. IAM 자격 증명 로그인을 활성화하려면:
 - a. AWS 관리 콘솔에서 AWS 변환을 열고 설정을 선택합니다.
 - b. IAM 자격 증명을 사용한 액세스 AWS 변환 섹션에서 IAM 자격 증명 액세스를 활성화합니다.
 - c. 동일한 설정 페이지에서 웹 애플리케이션 URL(IAM 사용) 아래에 표시된 로그인 링크를 복사합니다.
 - d. Management Console이 열려 있는 동일한 브라우저 창에 로그인 URL을 AWS 붙여 넣습니다. 이렇게 하면 웹 애플리케이션이 해당 계정의 AWS 자격 증명을 사용할 수 있습니다.
3. 왼쪽 탐색 메뉴를 열고 지속적 현대화를 선택합니다. 대시보드에는 소스, 리포지토리, 심각도별 총 조사 결과 및 분석 유형을 포함한 요약 통계가 표시됩니다.
4. 분석, 결과 및 문제 해결 탭을 사용하여 자세한 결과를 볼 수 있습니다.
5. 웹 애플리케이션에서 직접 AWS 변환과 채팅하여 분석, 조사 결과 또는 문제 해결에 대해 질문합니다.

웹 애플리케이션은 여러 코드베이스에서 지속적인 현대화 분석 및 문제 해결을 중앙 집중식으로 파악해야 하는 엔터프라이즈 규모의 운영을 위해 설계되었습니다.

개발자 도구

AWS Transform Power 및 에이전트 플러그인을 사용하여 에이전트 IDEs에서 지속적인 현대화에 액세스할 수 있습니다. 에이전트는 대화형 상호 작용을 통해 지속적인 현대화의 설정, 온보딩 및 지속적인 사용을 오케스트레이션합니다.

- Kiro IDE - [AWS 변환 Kiro 파워](#)를 설치합니다. Kiro Chat을 열고 에이전트에게 지속적인 현대화 워크플로를 지원해 달라고 요청합니다.
- Claude Code, Codex, Cursor - [aws-labs/agent-plugins](#)(plugins/aws-transform 디렉터리)를 설치합니다. 에이전트 플러그인은 Kiro Power와 동일한 기능을 제공합니다.

에이전트 스킬

Kiro Power 및 에이전트 플러그인에는 대화형 상호 작용을 통해 지속적인 현대화 워크플로를 오케스트레이션하는 기술이 포함되어 있습니다.

스킬	설명
Guide	전체 워크플로를 단계별로 안내하는 대화형 온보딩
소스	소스 연결 추가, 나열 및 제거
Discovery	소스를 스캔하여 리포지토리 검색
분석	모든 유형에서 분석 실행 및 관리
조사 결과	분석 결과 쿼리, 필터링 및 관리
문제 해결	조사 결과를 수정하기 위한 문제 해결 생성 및 관리
EC2 실행	원격 분석을 위한 Amazon EC2 인스턴스 프로비저닝 및 관리
배치 실행	Fargate를 사용하여 AWS Batch에 분석 작업 제출
일정	Amazon EventBridge 스케줄러를 사용하여 cron 일정에 대한 반복 분석 설정
보고	조사 결과, 심각도 분포 및 문제 해결 진행 상황을 보여주는 차트를 사용하여 독립형 HTML 보고서 생성

CLI 참조

다음 표에는 모든 `atx ct` 하위 명령이 요약되어 있습니다.

하위 명령	설명
<code>atx ct server</code>	지속적 현대화 서버 시작
<code>atx ct status</code>	소스, 리포지토리, 분석, 조사 결과 및 문제 해결을 포함한 시스템 상태 보기
<code>atx ct source add</code>	소스 추가(GitHub, GitLab, Bitbucket 또는 로컬)
<code>atx ct source list</code>	구성된 소스 나열
<code>atx ct source remove</code>	소스 제거
<code>atx ct discovery scan</code>	소스에서 리포지토리 검색
<code>atx ct discovery status</code>	검색 스캔 상태 확인
<code>atx ct repository list</code>	선택적 필터를 사용하여 리포지토리 나열
<code>atx ct repository get</code>	단일 리포지토리 가져오기
<code>atx ct repository update</code>	리포지토리 레이블 업데이트
<code>atx ct repository delete</code>	리포지토리 삭제
<code>atx ct analysis run</code>	리포지토리에 대한 분석 실행
<code>atx ct analysis get</code>	분석 세부 정보 가져오기
<code>atx ct analysis list</code>	선택적 상태 및 유형 필터를 사용하여 분석 나열
<code>atx ct analysis cancel</code>	실행 중인 분석 취소
<code>atx ct analysis delete</code>	분석 삭제
<code>atx ct findings list</code>	리포지토리, 소스, 심각도, 유형, 상태 및 분석에 대한 필터를 사용하여 조사 결과 나열

하위 명령	설명
<code>atx ct findings get</code>	단일 결과 가져오기
<code>atx ct findings update</code>	결과 상태 업데이트(열림 또는 무시됨)
<code>atx ct findings batch-update</code>	여러 결과 일괄 업데이트
<code>atx ct findings delete</code>	무시되거나 더 이상 사용되지 않는 결과 삭제
<code>atx ct remediation create</code>	결과 또는 변환 정의에서 문제 해결 생성
<code>atx ct remediation list</code>	모든 수정 사항 나열
<code>atx ct remediation status</code>	문제 해결 상태 확인 및 PR/MR 링크 보기
<code>atx ct remediation retry</code>	실패한 문제 해결 재시도
<code>atx ct remediation delete</code>	문제 해결 삭제
<code>atx ct setup security-agent</code>	보안 에이전트 인프라 프로비저닝 또는 관리
<code>atx ct schema</code>	에이전트와 자동화가 도움말 텍스트를 구문 분석하지 않고 CLI를 검색할 수 있도록 모든 명령, 옵션 및 인수와 같은 전체 <code>atx ct</code> 명령 표면의 기계 판독 가능 JSON 매니페스트를 인쇄합니다.

문제 해결

연결이 거부되었거나 서버가 실행되지 않음

지속적 현대화 CLI에는 실행 중인 서버가 필요합니다. 로 시작하고 로 `atx ct server &` 확인합니다 `atx ct status --health`.

검색 스캔은 리포지토리 0개를 반환합니다.

로컬 소스의 경우 리포지토리가 포함된 상위 디렉터리(예: `/home/user/repos`)를 하위 디렉터리로 `--path` 가리키고 리포지토리를 직접 가리키지 않는지 확인합니다(예: `/home/user/repos/my-app`). 스캐너는 `.git` 폴더가 포함된 하위 디렉터를 찾습니다.

SETUP_REQUIRED 오류

소스가 계정에 존재하지만 자격 증명이어 시스템에 구성되지 않았습니다. 를 실행 `atx ct source add --name name` 하여 로컬에서 자격 증명을 구성합니다.

AUTH_REQUIRED 오류

소스에 유효한 토큰을 찾을 수 없습니다. 토큰이 올바르고 필요한 범위가 있는지 확인합니다. GitHub의 경우 토큰에 `repo` 범위가 있는지 확인합니다. GitLab의 경우 `api` 범위를 확인합니다.

INVALID_INPUT 오류

올바른 분석 유형 이름을 사용하고 있는지 확인합니다. 유효한 값은 `rapid-techdebt-analysis`, `tech-debt-comprehensive`, `security`, `agentic-readiness`, `modernization-readiness`, `custom`입니다.

문제 해결 중 권한 오류

문제 해결은 리포지토리에 대한 쓰기 액세스 권한이 필요한 브랜치와 풀/병합 요청을 생성합니다. 쓰기 권한으로 토큰을 업데이트합니다. GitHub의 경우 전체 `repo` 범위를 확인합니다. GitLab의 경우 `api` 범위를 확인합니다. Bitbucket의 경우 `write:repository:bitbucket` 및 `write:pullrequest:bitbucket` 범위를 확인합니다.

보안 에이전트 설정 실패

IAM 사용자 또는 역할에의 보안 에이전트 설정 섹션에 나열된 필수, AWS CloudFormation IAM 및 Amazon S3 권한이 있는지 확인합니다 [지속적 현대화 AWS의 작동 방식](#). 를 사용하여 상태를 확인합니다 `atx ct setup security-agent --status`.

웹 애플리케이션에 지속적인 현대화가 표시되지 않음

AWS 변환 웹 애플리케이션에 로그인한 후에도 지속적인 현대화가 나타나지 않으면 IAM Identity Center 대신 AWS 계정 AWS 변환이 활성화된의 AWS IAM 자격 증명으로 로그인합니다. 단계는 [AWS 웹 애플리케이션 변환\(선택 사항\)](#)를 참조하세요.

검색 도구

AWS Transform 검색 도구를 사용하면 조직의 서버 인벤토리를 자동으로 검색하여 마이그레이션을 준비할 수 있습니다. 이 도구는 VMware vCenter, Microsoft Hyper-V 및 가져온 서버를 지원합니다. 검색 도구를 사용하려면 하나 이상의 검색 소스를 구성하고 도구를 실행한 다음 검색된 인벤토리 창에서 결과를 검토합니다.

검색 소스를 구성한 후 검색 도구가 정보 수집을 시작합니다. 검색 도구가 네트워크를 완전히 분석하는데 필요한 시간은 환경의 크기에 따라 다릅니다. 방향성 마이그레이션 비즈니스 사례의 경우 서버 컬렉션이 완료된 후 도구가 생성하는 마이그레이션 포트폴리오 평가(MPA) 파일을 사용할 수 있습니다.

검색 도구 워크플로

검색 도구 워크플로는 두 가지 유형의 활동으로 구성됩니다.

- 구성 활동
- 데이터 검토 및 사용

다음 단계에서는 검색 도구를 설치 및 사용하고 수집된 데이터로 작업하는 방법을 설명합니다.

1. 검색 도구를 설치합니다.
2. 검색 소스를 구성합니다. CSV 파일 가져오기를 통해 VMware vCenter, Microsoft Hyper-V 호스트 또는 서버 중 하나 이상을 구성할 수 있습니다. 데이터 검색은 소스를 구성한 후 시작됩니다.
3. OS 액세스를 설정한 다음 서버, 데이터베이스 및 네트워크 연결의 수집 상태를 검토합니다.
 - 필요에 따라 OS 자격 증명을 조정합니다.
4. (선택 사항) 직접 SQL 수집을 활성화하거나 SSH 또는 WinRM을 통한 OS 수준 폴백 감지를 사용하도록 Oracle 자격 증명을 구성합니다.
5. 마이그레이션 비즈니스 사례를 생성하려면 .zip 파일을 [마이그레이션 평가에](#) 업로드하거나 압축을 풀고 mpa_exports 디렉터리에서 MPA 파일을 업로드합니다. 내보내기에는 구성된 모든 소스의 데이터가 포함되며 VMware, Hyper-V 및 가져온 서버에 대한 MPA 파일이 포함됩니다.

검색 도구는 다음 검색 경로를 지원합니다.

- VMware vCenter 자동 검색 - VMware vCenter에서 관리하는 서버를 자동으로 검색합니다.

- Hyper-V 자동 검색 - Microsoft Hyper-V 호스트에서 관리하는 서버를 자동으로 검색합니다.
- 서버 가져오기 - CSV 파일을 통해 서버 인벤토리를 수동으로 가져옵니다.

검색 도구 설정

사전 조건

다음은 AWS Transform 검색 도구를 사용하기 위한 사전 조건입니다.

일반적인 사전 조건

- 이 도구에는 vCPU 4개, RAM 16GB, 하드 디스크 35GB가 필요합니다.
- 검색 도구 VM의 네트워크에서 DHCP를 사용할 수 있어야 합니다.
- 이 도구는 중앙 집중식 접근 방식을 사용하여 데이터를 수집합니다. 범위 내 서버는 검색 도구 VM에서 인바운드 연결을 허용해야 합니다(기본 포트, 사용자 지정 포트 구성 지원).
 - Linux – SSH TCP/22
 - Windows – HTTP의 경우 TCP/5985, HTTPS의 경우 TCP/5986
 - SNMP - UDP/161(네트워크 수집에만 사용되며 OS 지표에는 사용되지 않음)
- Linux의 경우 SSH를 사용하여 서버에 연결할 수 있는 사용자 계정입니다. 검색 도구는 네트워크 수집 및 OS 지표에 대해 SSH를 통해 명령을 실행합니다. 대부분의 명령은 일반 사용자로 실행됩니다. 소수의 명령은 sudo를 시도하고 sudo를 사용할 수 없는 경우 dmidecode (서버 UUID 및 제조업체), lvsdisplay (LVM 감지) 및 ss 또는 netstat (프로세스 정보가 포함된 네트워크 연결)로 자동 대체됩니다. sudo가 없으면 검색 도구는 여전히 대부분의 데이터를 수집하지만 UUID, LVM 및 프로세스 수준 네트워크 세부 정보는 누락됩니다. 완전한 데이터 수집을 위해 SSH 사용자에게 대해 암호 없는 sudo를 구성하는 것이 좋습니다. 자세한 내용은 단원을 참조하십시오 [the section called “필수 권한”](#).

VMware 사전 조건

- VMware vCenter Server 버전 6.5, 6.7, 7.0 또는 8.0.
- VMware vCenter에 OVA를 배포할 수 있는 권한.
- VMware vCenter Server 설정의 경우 루트 데이터 센터 수준에서 읽기 전용 역할이 할당된 vCenter 사용자입니다. 자세한 내용은 [the section called “필수 권한”](#)을 참조하세요.

Hyper-V 사전 조건

- Hyper-V 역할이 활성화된 Windows Server.
- Hyper-V 호스트에서 WinRM이 활성화되었습니다.
- 각 Hyper-V 호스트의 원격 관리 사용자, Hyper-V 관리자 및 성능 모니터 사용자 그룹의 멤버인 사용자 계정으로, root\cimv2 네임스페이스에 대한 WMI 읽기 액세스 권한이 있습니다. 자세한 내용은 [the section called “필수 권한”](#)을 참조하세요.
- 지원되는 인증: NTLM(HTTPS만 해당) 및 Kerberos(HTTP 또는 HTTPS).

서버 가져오기 사전 조건

- 검색 도구에서 구성하거나 구성할 OS 자격 증명의 표시 이름에 매핑되는 서버 호스트 이름 또는 IP 주소와 자격 증명 이름(선택 사항)이 있는 CSV 파일입니다. CSV는 다음 헤더를 사용해야 합니다.

```
hostname_or_ip,os_credential_name,oracle_credential_name
```

- 검색 도구 VM에서 서버에 연결할 수 있어야 합니다. 기본 포트: Linux용 SSH 포트 22, Windows용 WinRM 포트 5985/5986. 사용자 지정 포트가 지원됩니다.

Linux 설치 관리자 사전 조건

- 지원되는 Linux 배포: Amazon Linux 2, Amazon Linux 2023, RHEL 8–9, Rocky Linux 8–9, AlmaLinux 9, Ubuntu 20.04–24.04, Debian 10–12 또는 SLES 15 SP5.
- 최소 4개의 vCPU, 16GB RAM, 35GB 사용 가능한 디스크 공간.
- 포트 5000을 사용할 수 있어야 합니다(다른 서비스에서 사용하지 않음).
- systemd는 서비스 관리에 필요합니다.
- 검색 도구 VM에는 대상 인프라에 대한 네트워크 액세스 권한이 있어야 합니다. 기본 포트: 포트 443의 vCenter, 포트 5985/5986의 Hyper-V 호스트, 포트 22의 서버. 사용자 지정 포트는 SSH, WinRM 및 SNMP에서 지원됩니다.

Oracle Database 사전 조건

- 검색 도구에서 포트 1521(또는 사용자 지정 포트)의 Oracle 호스트로의 네트워크 액세스.
- 지원되는 Oracle 버전: 직접 SQL 연결을 통해 Oracle Database 12c 릴리스 1(12.1) 이상을 수집할 수 있습니다. OS 수준 폴백 감지는 모든 Oracle 버전에서 작동합니다.
- SELECT_CATALOG_ROLE 권한이 있는 읽기 전용 Oracle 서비스 계정입니다. 자세한 내용은 [the section called “Oracle Database\(SQL\)”](#)을 참조하세요.

- OS 수준 폴백 감지의 경우: Oracle 호스트에 대한 SSH 또는 WinRM 액세스(기존 OS 자격 증명 사용).

VMware에 배포

VMware 가상 머신 사양

- 운영 체제 - Amazon Linux 2023
- RAM - 16GB
- CPU - 코어 4개
- 디스크 - 35GB
- VMware 요구 사항 - [VMware에서 AL2023을 실행하기 위한 VMware 호스트 요구 사항](#) 참조

VMware OVA 배포

1. 다음 URL에서 OVA 파일을 다운로드합니다. <https://s3.us-east-1.amazonaws.com/atx.discovery.collector.bundle/releases/latest/AWS-Transform-discovery-tool.ova>
2. vCenter에 VMware 관리자로 로그인합니다.
3. 다음 방법 중 하나를 사용하여 OVA 파일을 설치합니다.
 - a. UI 사용: 파일을 선택하고 OVF 템플릿 배포를 선택한 다음 1단계에서 다운로드한 검색 도구 OVA 파일을 선택한 다음 마법사를 완료합니다. 서버 관리 대시보드의 프록시 설정이 올바르게 구성되었는지 확인합니다.
 - b. 명령줄 사용: 명령줄에서 검색 도구 OVA 파일을 설치하려면 VMware Open Virtualization Format Tool(ovftool)을 다운로드하여 사용합니다. ovftool을 다운로드하려면 [OVF 도구 설명서](#) 페이지에서 릴리스를 선택합니다. 다음은 ovftool 명령줄 도구를 사용하여 검색 도구 OVA 파일을 설치하는 예제입니다.

```
ovftool --acceptAllEulas --name='discovery tool' --datastore=datastore1 -  
dm=thin AWS-Transform-discovery-tool.ova 'vi://username:password@vcenterurl/  
Datacenter/host/esxi/'
```

예제의 대체 가능한 값에 대한 설명:

- 이름은 검색 도구 VM에 사용할 이름입니다.
- 데이터 스토어는 vCenter에 있는 데이터 스토어의 이름입니다.

- OVA 파일 이름은 다운로드한 검색 도구 OVA 파일의 이름입니다.
 - 사용자 이름/암호는 vCenter 자격 증명입니다.
 - vcenterurl은 vCenter의 URL입니다.
 - vi 경로는 VMware ESXi 호스트의 경로입니다.
4. vCenter에서 배포된 검색 도구를 찾습니다. VM을 마우스 오른쪽 버튼으로 클릭한 다음 전원, 전원 켜기를 선택합니다.
 5. 몇 분 후 검색 도구의 IP 주소가 vCenter에 표시됩니다. 이 IP 주소를 사용하여 검색 도구에 연결합니다.

Hyper-V에 배포

Hyper-V 가상 머신 사양

- 운영 체제 - Amazon Linux 2023
- RAM - 최소 16GB를 할당하는 것이 좋습니다.
- CPU - 최소 4개의 코어를 할당하는 것이 좋습니다.
- 디스크 - 35GB(VOD에 포함됨)
- Hyper-V 요구 사항 - [Hyper-V에서 AL2023을 실행하기 위한 Hyper-V 호스트 요구 사항](#) 참조

Hyper-V VHD 배포

1. 다음 URL에서 VHD 파일을 다운로드합니다. <https://s3.us-east-1.amazonaws.com/atx.discovery.collector.bundle/releases/latest/AWS-Transform-discovery-tool.vhd>
2. VHD 파일을 Hyper-V 역할이 활성화된 Windows Server 시스템에 복사합니다.
3. Hyper-V Manager를 엽니다.
4. 새로 만들기를 선택한 다음 가상 머신을 선택합니다.
5. 설정 마법사를 완료합니다. 생성 지정 페이지에서 1세대를 선택합니다. 2세대 가상 머신은 VHD 형식을 지원하지 않습니다. 메모리 할당 페이지에서 최소 16384MB를 할당합니다. 가상 하드 디스크 연결 페이지에서 기존 가상 하드 디스크 사용을 선택하고 복사한 VHD 파일을 선택합니다.
6. VM을 시작합니다. 몇 분 후 Hyper-V Manager에서 VM의 네트워킹 탭을 확인하여 IP 주소를 찾거나 VM 콘솔에 연결하고를 실행합니다ip addr. 이 IP 주소를 사용하여 검색 도구에 연결합니다.

Linux에 배포

검색 도구는 지원되는 Linux 배포판에 배포하기 위한 독립 실행형 Linux 설치 관리자로 사용할 수 있습니다. 가상 머신을 배포하는 대신 기존 Linux 서버에 직접 검색 도구를 설치하려는 경우 이 옵션을 사용합니다.

Linux 서버 사양

- RAM - 최소 16GB를 할당하는 것이 좋습니다.
- CPU - 최소 4개의 코어를 할당하는 것이 좋습니다.
- 디스크 - 35GB

지원되는 배포판

- Amazon Linux – Amazon Linux 2, Amazon Linux 2023
- Red Hat Enterprise Linux 및 파생 - RHEL 8–9, Rocky Linux 8–9, AlmaLinux 9
- Ubuntu – 20.04, 22.04, 24.04
- Debian – 10, 11, 12
- SUSE – SLES 15 SP5

검색 도구 설치

다음 URL에서 설치 프로그램 스크립트를 다운로드합니다. <https://s3.us-east-1.amazonaws.com/atx.discovery.collector.bundle/releases/latest/AWS-Transform-discovery-tool.sh>

Linux에 검색 도구를 설치하려면

1. 설치 프로그램 스크립트를 Linux 서버에 다운로드합니다.

```
curl -O https://s3.us-east-1.amazonaws.com/atx.discovery.collector.bundle/releases/latest/AWS-Transform-discovery-tool.sh
chmod +x AWS-Transform-discovery-tool.sh
```

2. (선택 사항) 호환성 검사를 실행하여 시스템이 요구 사항을 충족하는지 확인합니다.

```
sudo ./AWS-Transform-discovery-tool.sh check
```

3. 검색 도구를 설치합니다. 다음 옵션 중 하나를 선택하세요.

옵션 1: 자동 종속성 설치로 설치(권장)

이 옵션은 서비스를 설치하기 전에 누락된 시스템 종속성을 자동으로 설치합니다.

```
sudo ./AWS-Transform-discovery-tool.sh install --install-deps
```

옵션 2: 자동 종속성 설치 없이 설치

이 옵션은 누락된 종속성을 확인하고 중요한 종속성이 누락된 경우 수동 설치 지침과 함께 오류를 표시합니다. 조직에서 자동 패키지 설치를 제한하고 시스템 패키지를 수동으로 관리하려는 경우 이 옵션을 사용합니다.

```
sudo ./AWS-Transform-discovery-tool.sh install
```

4. 검색 도구 서비스를 시작합니다.

```
sudo ./AWS-Transform-discovery-tool.sh start
```

5. 에서 검색 도구에 액세스합니다 https://ip_address:5000.

검색 도구를 제거하려면 실행합니다 `sudo ./AWS-Transform-discovery-tool.sh uninstall`.

다음 명령을 사용하여 서비스를 관리할 수도 있습니다.

- `sudo ./AWS-Transform-discovery-tool.sh status` - 서비스가 실행 중인지 확인합니다.
- `sudo ./AWS-Transform-discovery-tool.sh stop` - 서비스를 중지합니다.
- `sudo ./AWS-Transform-discovery-tool.sh logs` - 서비스 로그를 봅니다.

시스템 종속성

설치 관리자는 다음 시스템 종속성을 확인합니다.

종속성	심각도	용도
OpenSSL	심각	데이터베이스 암호화 키를 생성합니다.
libcrypt	심각	Python 런타임에 필요

종속성	심각도	용도
Kerberos 라이브러리	경고	Windows 서버에 대한 Kerberos 인증에 필요합니다. 이 기능이 없으면 NTLM 및 기본 인증이 계속 작동합니다.

검색 도구를 시작하려면 중요한 종속성이 필요합니다. 누락된 경우 옵션 2(제외--install-deps)를 선택하면 설치 관리자가 수동으로 설치하라는 지침과 함께 오류를 표시합니다. 경고 수준 종속성은 선택 사항입니다. 설치 관리자는 경고를 표시하지만 설치를 진행합니다.

Note

설치 관리자는 glibc 버전 및 시스템 가용성을 포함한 시스템 호환성을 확인합니다. systemd 250 이상이 설치된 시스템(Amazon Linux 2023, RHEL 9, Rocky 9, AlmaLinux 9, Ubuntu 24.04 이상, Debian 12 이상)에서 데이터베이스 암호화 키는 systemd-creds를 사용하여 저장 시 암호화됩니다. 이전 시스템에서 암호화 키는 권한 보호 파일로 저장됩니다.

검색 도구 구성

검색 도구 콘솔에 액세스

1. 웹 브라우저 액세스: `https://ip_address:5000`에서 `ip_address`는 Deploy Discovery Tool에서 검색 도구의 IP 주소입니다. 검색 도구는 HTTPS 연결에 자체 서명된 인증서를 사용하여 보안 경고를 발생시킵니다. 위험 수락을 선택하고 검색 도구 콘솔로 계속 진행합니다.
2. 검색 도구 콘솔에 처음 액세스하는 경우 검색 도구 로그인 암호를 생성합니다. 향후 로그인에 사용할 암호를 생성합니다.

Important

이 암호를 기억하세요. 암호 복구 메커니즘은 없습니다.

검색 도구 VM에 액세스

- 검색 도구 VM은 기본적으로 사용자 이름과 암호("discovery", "password")와 함께 제공됩니다. 강력한 보안을 위해 하이퍼바이저의 콘솔(예: VMware용 vSphere Client 또는 Hyper-V용 Hyper-V

Manager)을 통해 VM에 로그인한 `sudo passwd discovery` 후를 사용하여 암호를 업데이트하는 것이 좋습니다.

- SSH 액세스는 기본적으로 비활성화되어 있습니다. 사용자는 미리 구성된 `enablessh` 및 `disablessh`별칭을 사용하여 검색 도구 VM에 대한 SSH 액세스를 활성화/비활성화할 수 있습니다. 사용자는 SSH 액세스를 활성화한 `ssh discovery@<VM-IP>` 후를 통해 VM으로 SSH할 수 있습니다. 대부분의 경우 SSH 액세스를 비활성화한 상태로 유지하고 적극적으로 필요한 경우에만 활성화하는 것이 좋습니다. 를 실행할 때 암호 변경이 적용됩니다 `enablessh`.
- 에서 검색 도구 데이터 디렉터리에 액세스하려면 `sudo su ec2-user`로 전환하는 `/home/ec2-user/.local/share/DiscoveryTool`가 좋습니다.

Kerberos 인증 구성

Kerberos 인증은 검색 도구에서 Windows 서버에 연결하는 데 권장되는 방법입니다. 검색 도구 VM은 네이티브 Amazon Linux 2023 Kerberos 라이브러리를 사용하여 Active Directory 도메인에 대해 인증합니다.

다음은 검색 도구 VM에서 Kerberos 인증에 대한 주요 사항입니다.

- `kinit` 명령을 사용하여 Kerberos 티켓을 가져오고 티켓을 `klist` 확인합니다.
- Kerberos 구성 파일은 `/etc/krb5.conf`에 있습니다.
- 검색 도구를 구성하기 전에 검색 도구 VM의 CLI에서 `kinit` 성공하는지 확인합니다.

Kerberos 사전 조건

Kerberos 인증을 구성하기 전에 다음 정보와 네트워크 연결이 있는지 확인합니다.

1. Active Directory 관리자로부터 다음 정보를 얻습니다.

- Kerberos 영역 이름(일반적으로 도메인 이름은 대문자입니다. 예: `EXAMPLE.COM`).
- 일반적으로 도메인 컨트롤러(예:)인 Key Distribution Center(KDC)의 호스트 이름 또는 IP 주소입니다 `dc01.example.com`.
- 대상 Windows 서버에 대해 인증할 수 있는 권한이 있는 서비스 계정입니다.

2. 검색 도구 VM에 다음에 대한 네트워크 연결이 있는지 확인합니다.

- Kerberos 인증을 위한 포트 88(TCP 및 UDP)의 KDC입니다.
- WinRM 포트의 대상 Windows 서버(HTTP의 경우 5985, HTTPS의 경우 5986).

Kerberos 구성

다음 단계를 완료하여 검색 도구 VM에서 Kerberos 인증을 구성합니다.

1. 검색 도구 VM에 대한 SSH입니다.

```
ssh discovery@<discovery-tool-vm-ip>
```

2. 에서 Kerberos 구성 파일을 편집합니다/etc/krb5.conf.

```
sudo nano /etc/krb5.conf
```

다음 구성을 추가하여 자리 표시자 값을 환경 세부 정보로 바꿉니다.

```
[libdefaults]
    default_realm = EXAMPLE.COM
    dns_lookup_realm = false
    dns_lookup_kdc = true

[realms]
    EXAMPLE.COM = {
        kdc = dc01.example.com
    }

[domain_realm]
    .example.com = EXAMPLE.COM
    example.com = EXAMPLE.COM
```

Important

Kerberos는 대/소문자를 구분합니다. 영역 이름은 대문자여야 합니다(예:가 EXAMPLE.COM아닌 example.com). [domain_realm] 섹션의 도메인 이름은 소문자여야 합니다.

여러 Active Directory 도메인

검색 도구는 다양한 Active Directory 도메인에 대해 여러 Kerberos 자격 증명을 지원합니다. 각 자격 증명은 독립적으로 인증되므로 여러 자격 증명을 정상적으로 구성할 수 있으며 격리는 자동으로 이루어집니다.

여러 도메인에 서버가 있는 경우 /etc/krb5.conf 파일의 각 영역에 대한 항목을 추가합니다.

```
[libdefaults]
    default_realm = DEV.COMPANY.COM
    dns_lookup_realm = false
    dns_lookup_kdc = true

[realms]
    DEV.COMPANY.COM = {
        kdc = dc01.dev.company.com
    }
    PROD.COMPANY.COM = {
        kdc = dc01.prod.company.com
    }

[domain_realm]
    .dev.company.com = DEV.COMPANY.COM
    dev.company.com = DEV.COMPANY.COM
    .prod.company.com = PROD.COMPANY.COM
    prod.company.com = PROD.COMPANY.COM
```

3. kinit 명령을 실행하여 Kerberos 티켓을 얻을 수 있는지 확인합니다.

```
kinit username@REALM.COM
```

메시지가 표시되면 암호를 입력합니다. 명령이 오류 없이 완료되면 인증이 성공한 것입니다.

4. klist 명령을 실행하여 티켓을 확인합니다.

```
klist
```

예상 출력은 다음과 유사합니다.

```
Ticket cache: FILE:/tmp/krb5cc_1000
Default principal: username@REALM.COM

Valid starting          Expires                Service principal
01/01/2025 12:00:00    01/01/2025 22:00:00    krbtgt/REALM.COM@REALM.COM
```

5. 에서 사용한 것과 동일한 대/소문자를 구분하는 보안 주체kinit(예: username@REALM.COM)로 검색 도구를 구성합니다.

환경에 Kerberos 서비스 검색을 위해 구성된 DNS SRV 레코드가 있는 경우 명시적 krb5.conf 구성이 필요하지 않을 수 있습니다. Kerberos 구성 옵션에 대한 자세한 내용은 [MIT Kerberos krb5.conf 설명서](#) 및 [샘플 krb5.conf 파일을](#) 참조하세요.

도메인에 조인된 시스템에서 Kerberos 구성 찾기

Kerberos 구성 세부 정보가 없는 경우 도메인에 조인된 Windows 시스템에서 검색할 수 있습니다. 도메인에 조인된 시스템의 명령 프롬프트에서 다음 명령을 실행합니다.

도메인 이름을 찾으려면 다음 명령을 실행합니다.

```
echo %USERDNSDOMAIN%
```

출력 예시:

```
EXAMPLE.COM
```

도메인 컨트롤러 호스트 이름을 찾으려면 다음 명령을 실행합니다.

```
nltest /dsgetdc:EXAMPLE.COM
```

출력 예시:

```
DC: \\dc01.example.com
Address: \\10.0.1.100
Dom Guid: xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx
Dom Name: EXAMPLE.COM
Forest Name: example.com
Dc Site Name: Default-First-Site-Name
Our Site Name: Default-First-Site-Name
Flags: 0xe00033fd
The command completed successfully
```

다음과 같이 출력을 krb5.conf 구성에 매핑합니다.

- 영역 -의 값을 대문자%USERDNSDOMAIN%로 사용합니다(예: EXAMPLE.COM).
- KDC - nltest 출력의 DC 호스트 이름을 사용합니다(예: dc01.example.com).

vCenter 액세스 구성

1. 검색 도구 페이지의 1단계에서 검색 소스를 구성하고 소스 구성을 선택합니다.
2. 검색 소스 구성 페이지에서 표시 이름, vCenter FQDN/IP, 사용자 이름 및 암호를 입력합니다.
3. 구성 저장을 선택합니다.

검색 도구는 [검색된 인벤토리](#)에 설명된 대로 vCenter 정보를 수집하기 시작합니다.

초기 구성 후 검색 도구 상태 프레임에서 vCenter 액세스 편집을 선택하여 vCenter 액세스 설정을 변경합니다.

검색 도구는 구성된 모든 vCenter 서버에서 병렬로 수집합니다. 수집 중에 하나의 vCenter 서버에 연결할 수 없는 경우 도구는 부분적인 성공을 보고하고 나머지 vCenter 서버에서 계속 수집합니다.

VM이 여러 vCenter 서버에 나타나는 경우(예: 공유 ESXi 호스트 또는 교차 vCenter vMotion으로 인해) 검색 도구는 VMs. 각 고유 VM은 인벤토리에 한 번만 나타납니다.

Hyper-V 액세스 구성

1. 검색 도구 페이지의 1단계에서 검색 소스를 구성하고 소스 구성을 선택합니다.
2. 검색 소스 구성 페이지에서 표시 이름, 호스트 FQDN 또는 IP 주소, 인증 유형(NTLM 또는 Kerberos), WinRM 사용자 이름 및 WinRM 암호를 제공합니다.
3. 구성 저장을 선택합니다.

검색 도구는 [검색된 인벤토리](#)에 설명된 대로 Hyper-V 정보를 수집하기 시작합니다.

자격 증명을 저장하면 수집이 자동으로 시작됩니다.

Hyper-V 장애 조치 클러스터의 경우 동일한 클러스터에 여러 호스트를 추가할 수 있습니다. 이 도구는 둘 이상의 호스트에 나타나는 VMs 자동으로 중복 제거합니다.

서버 가져오기

1. 검색 도구 홈페이지에서 서버 가져오기 페이지로 이동합니다.
2. (필수), hostname_or_ip (os_credential_name선택 사항) 및 oracle_credential_name (선택 사항) 열이 있는 CSV 파일을 준비합니다.
 - hostname_or_ip 값은 유효한 IPv4 주소 또는 정규화된 도메인 이름(FQDN)이어야 합니다.

- `os_credential_name` 값이 제공된 경우 이미 구성한 OS 자격 증명의 표시 이름(SSH, WinRM 또는 SNMP)과 일치해야 합니다. 아직 OS 자격 증명을 구성하지 않은 서버의 경우 비워둡니다.
 - `oracle_credential_name` 값이 제공된 경우 이미 구성한 Oracle 자격 증명의 표시 이름과 일치해야 합니다.
3. CSV 파일을 업로드합니다. 도구는 모든 행을 검증하고 행이 유효하지 않은 경우 파일을 거부합니다.

가져오기에 성공하면 OS 자격 증명에 구성된 경우 도구가 가져온 서버에 대한 데이터베이스, 네트워크 및 OS 지표 수집을 자동으로 시작합니다. 다른 CSV 파일을 업로드하면 중복을 생성하지 않고 기존 레코드가 업데이트되고 새 레코드가 인벤토리에 병합됩니다.

자체 서명된 인증 기관을 검색 도구로 가져오기(선택 사항)

이는 자체 서명된 인증 기관(CA)에서 서명한 WinRM HTTPS 인증서를 사용하여 HTTPS를 통한 WinRM 및 대상 서버를 사용하고 검색 도구에서 "서버 SSL 인증서 검증"을 활성화하려는 경우에 필요합니다.

사전 조건

1. 대상 서버의 WinRM HTTPS 인증서에 서명하는 데 사용된 자체 서명 CA 인증서
2. PEM 형식의 인증서(.pem 또는 .crt 확장)

검색 도구 VM에서 자체 서명된 인증 기관을 가져오려면:

1. Ssh to Discovery 도구 VM
2. 대상 서버의 WinRM 인증서에 서명한 CA 인증서(들)를 검색 도구 VM의 트러스트 스토어 디렉터리/etc/pki/ca-trust/source/anchors/에 배치합니다. 예를 들어 `sudo cp winrm-ca.pem /etc/pki/ca-trust/source/anchors/winrm-ca.pem`입니다. 참고: 대상 서버가 다른 CAs에서 서명한 인증서를 사용하는 경우 모든 관련 CA 인증서들이 디렉터리에 복사합니다.
3. 인증서 트러스트 스토어를 업데이트합니다. `sudo update-ca-trust`
4. VM 재부팅
5. (선택 사항) 인증서를 성공적으로 가져왔는지 확인하려면 다음 명령을 실행할 수 있습니다. `sudo trust list --filter=ca-anchors | grep -A 5 "<certificate_name>"`

[Windows 원격 관리의 설치 및 구성](#) 참조

OS 액세스를 위한 검색 도구 구성

검색 도구가 다음을 수행할 수 있도록 OS 액세스를 구성합니다.

- 데이터베이스 평가를 수행하고 VM 마이그레이션을 지원하는 데이터베이스를 검색합니다.
- 각 연결과 연결된 프로세스를 포함하여 인벤토리의 서버 간 네트워크 연결을 추적하여 애플리케이션 종속성 매핑 및 웨이브 계획을 지원합니다. 두 엔드포인트가 모두 검색 도구의 인벤토리에 있는 연결만 포함됩니다.

검색 도구 OS 액세스 활성화

1. OS 액세스 설정 페이지로 이동하여 Windows 및 Linux 자격 증명을 제공합니다.
2. 자격 증명을 추가할 프로토콜을 선택합니다.
3. 선택한 프로토콜에 필요한 자격 증명을 제공합니다.
4. 자동 연결을 선택하여 검색 도구가 각 서버에 대해 일치하는 자격 증명이 발견될 때까지 검색된 서버에서 제공된 모든 자격 증명을 시도할 수 있도록 합니다.

자동 연결 기능과 관련된 중요한 보안 권장 사항은 [the section called “주의하여 자동 연결 기능 사용”](#) 섹션을 참조하세요.

5. 설정 및 연결을 선택합니다.

OS 일치 프로세스가 완료되면 데이터 수집이 진행 중이라는 메시지와 자격 증명 일치를 찾을 수 없는 서버에 대한 오류가 표시됩니다.

지원되는 프로토콜 설정

검색 도구가 대상 서버와 통신하려면 대상 서버에 WinRM, SSH 및 SNMP 프로토콜을 설정해야 합니다.

WinRM 및 WMI 설정

WinRM은 현재 지원되는 모든 버전의 Windows 운영 체제와 함께 자동으로 설치됩니다.

WinRM 구성을 확인하거나 편집하려면 `winrm` 명령줄 도구를 사용합니다.

- 설치된 WinRM 리스너를 확인합니다. `winrm enumerate winrm/config/listener`
- WinRM 구성 확인: `winrm get winrm/config`

- WinRM을 설정하는 명령의 예: `winrm quickconfig -transport:https`

리스너 포트

기본 HTTP 포트는 5985이고 HTTPS는 5986입니다. 필요에 따라 다른 포트를 사용할 수 있습니다. 검색 도구와 대상 서버 간에 포트가 열려 있어야 합니다.

암호화(Encryption)

검색 도구는 암호화된 WinRM 통신을 사용합니다. 대상 서버의 WinRM 리스너도 암호화를 사용하는 것이 좋습니다. `winrm set winrm/config/service '@{AllowUnencrypted="false"}'`

NTLM과 Kerberos 비교

WinRM 인증 프로토콜 Kerberos 및 NTLM은 검색 도구에서 지원됩니다. NTLM은 HTTPS에서만 사용할 수 있으며 Kerberos는 HTTP 또는 HTTPS 모두에서 사용할 수 있습니다.

WMI 요구 사항

검색 도구는 다음 WMI 네임스페이스를 쿼리합니다. WinRM 계정에는 컬렉션 모듈과 관련된 각 네임스페이스에 대한 읽기 액세스 권한이 필요합니다.

WMI 네임스페이스	사용처
root\cimv2	OS 지표, Hyper-V 호스트 메타데이터, SQL Server 컬렉션
root\virtualization\v2	Hyper-V VM 인벤토리
root\StandardCIMV2	네트워크 컬렉션
root\Microsoft\SqlServer\ComputerManagement*	SQL Server 컬렉션
root\Microsoft\SqlServer\ReportServer*	SQL Server 컬렉션(SSRS)

네트워크 수집의 경우 다음 조건이 충족되는지 확인합니다.

- ICMP를 통한 네트워크 연결 허용

- TCP 포트 135 + 임시 TCP 포트 범위(49152~65535)를 통한 네트워크 연결 허용
- UAC 비활성화
- 원격 DCOM 권한이 설정됨
- 최소한의 필수 권한으로 전용 서비스 계정 생성
- WMI 네임스페이스 권한은 네임스페이스가 `\\root\\standardcimv2, MSFT_NetTCPConnection` 클래스인 Windows 계정에 대해 설정됩니다.

SQL Server 컬렉션의 경우 복잡한 WMI 객체 권한 요구 사항으로 인해 로컬 관리자 그룹에 속한 Windows 계정(로컬 또는 도메인)이 필요합니다.

SSH 설정

- 기본 포트는 22입니다. 사용자 지정 포트가 지원됩니다. 구성된 포트는 검색 도구와 대상 서버 간에 열려 있어야 합니다.
- SSH 네트워크 컬렉션이 제대로 작동하려면 암호 없는 sudo에 대해 구성된 사용자를 제공합니다.
- 대상 Linux 서버(대부분의 배포에 기본적으로 설치됨)에서 `ss` 또는 네트워크 수집 `netstat`의 경우 및 OS 지표 수집 `df`의 경우, `lsblk`, `iostat`, `dmidecode`, `smartctl`, `top`, `ip`, `ps` free 및 명령을 사용할 수 있는지 확인합니다.

검색 도구는 SSH에 대해 두 가지 인증 방법을 지원합니다.

옵션 1: 사용자 이름 및 암호

SSH 사용자 이름과 암호를 입력합니다. 기본 인증 방법입니다.

옵션 2: SSH 프라이빗 키

SSH 사용자 이름과 프라이빗 키를 PEM 형식으로 제공합니다. 이 옵션을 사용하려면 SSH 자격 증명을 구성할 때 인증 유형 드롭다운에서 SSH 키를 선택합니다. 프라이빗 키가 암호로 암호화된 경우 선택적 키 암호 필드에 암호를 입력합니다.

지원되는 키 형식은 다음과 같습니다.

- RSA
- ECDSA
- Ed25519

- OpenSSH 형식
- PKCS#8 형식

두 인증 방법 모두 자동 연결을 지원합니다. 자격 증명은 저장 시 암호화된 상태로 저장됩니다.

SNMP 설정

- 기본 포트는 161/UDP입니다. 사용자 지정 포트가 지원됩니다. 구성된 포트는 검색 도구와 대상 서버 간에 열려 있어야 합니다.
- SNMP v2의 경우: TCP 연결 OIDs 제공합니다.
- SNMP v3의 경우: TCP 연결 OIDs에 액세스할 수 있는 읽기 전용 권한으로 사용자 이름/암호 및 인증/프라이버시 세부 정보 제공

검색 도구를 사용하려면 다음에 액세스해야 합니다.

- "1.3.6.1.2.1.6.13.1.1." (tcpConnState)
- "1.3.6.1.2.1.6.19.1.8." (tcpConnectionProcess)
- "1.3.6.1.2.1.25.4.2.1.2." (hrSWRunName)

Oracle 데이터베이스 액세스 구성

SQL 연결을 통해 직접 자세한 Oracle 데이터베이스 메타데이터를 수집하도록 Oracle 데이터베이스 액세스를 구성합니다. 수집된 메타데이터에는 CDB 및 PDB 토폴로지, 기능 사용 및 설치된 옵션이 포함됩니다. 이 데이터는 Oracle 데이터베이스 마이그레이션을 보다 정확하게 계획하는 데 도움이 됩니다. 직접 SQL 연결을 통해 Oracle Database 12c 릴리스 1(12.1) 이상을 수집할 수 있습니다. OS 수준 폴백 감지는 모든 Oracle 버전에서 작동합니다.

검색 도구에서 Oracle 자격 증명 구성

1. 검색 도구 페이지의 사이드바에서 데이터베이스 액세스를 선택합니다.
2. Oracle 자격 증명 추가를 선택합니다.
3. 다음 정보를 제공합니다.
 - 표시 이름 -이 자격 증명을 설명하는 이름입니다(예: Oracle Production).
 - 포트 - Oracle 리스너 포트(기본값 1521).
 - 서비스 이름 - 대상 데이터베이스의 Oracle 서비스 이름입니다.

- 사용자 이름 - Oracle 서비스 계정 사용자 이름입니다.
 - 암호 - Oracle 서비스 계정 암호입니다.
 - 자동 연결 - 인벤토리의 모든 서버에 대해 자격 증명을 시도하려면이 옵션을 켭니다. 특정 서버에 자격 증명을 수동으로 할당하려면이 옵션을 끕니다.
4. 자격 증명을 더 추가하려면(예: 다른 Oracle 환경의 경우) Oracle 자격 증명 추가를 다시 선택합니다.
 5. 저장을 선택합니다.

자격 증명 모드

Oracle 자격 증명을 구성할 때 다음 두 가지 모드 중에서 선택할 수 있습니다.

- 수동 - 자격 증명을 특정 서버에 고정합니다. 검색 도구는 해당 서버에 대해서만 해당 자격 증명을 사용합니다. 연결이 실패하면 대체가 발생하지 않습니다. 자격 증명 구성을 수정하여 문제를 해결합니다.
- 자동 연결 - 검색 도구는 인벤토리의 모든 서버에 대해 각 자동 연결 자격 증명을 시도합니다. 서버에 대한 자격 증명에 성공하면 검색 도구는 모든 후속 컬렉션 라운드에 해당 자격 증명을 사용합니다.

감지 흐름

Oracle 자격 증명을 구성하면 검색 도구가 먼저 직접 SQL 연결을 시도합니다. 모든 데이터베이스 자격 증명에 실패하면 도구가 SSH 또는 WinRM을 통한 OS 수준 탐지로 돌아가므로 데이터베이스 액세스 없이 Oracle 설치를 계속 검색할 수 있습니다.

검색 도구 업데이트

검색 도구에는 자동 업데이트 기능이 없지만 30일 설치 후 업데이트 알림이 전송됩니다. 최신 기능과 보안 패치를 받으려면 애플리케이션을 up-to-date 상태로 유지하는 것이 좋습니다.

도구를 수동으로 업데이트하려면

1. 제공된 링크에서 최신 검색 도구 이미지 파일(VMware용 OVA 또는 Hyper-V용 VHD)을 다운로드합니다.
2. (선택 사항) 최신 검색 도구를 배포하기 전에 이전 검색 도구 이미지 파일을 삭제하는 것이 좋습니다.
3. 검색 도구 배포 섹션의 단계에 따라 업데이트된 버전을 배포합니다.

액세스 취소

각 검색 소스에 대한 액세스를 독립적으로 취소할 수 있습니다. 한 소스에 대한 액세스를 취소해도 다른 소스의 데이터는 영향을 받지 않습니다.

- vCenter 액세스 취소 - vCenter 자격 증명 및 VMware에서 수집한 데이터를 삭제합니다. Hyper-V 데이터, 가져온 서버 데이터 또는 OS 자격 증명은 삭제하지 않습니다.
- Hyper-V 액세스 취소 - Hyper-V 자격 증명 및 Hyper-V-collected 데이터만 삭제합니다.
- 가져온 서버 삭제 - 가져온 서버를 인벤토리에서 제거합니다. 해당 서버에서 수집된 다운스트림 컬렉션 데이터(네트워크, 데이터베이스)는 유지됩니다.

검색 도구에 필요한 권한

검색 도구는 여러 프로토콜을 사용하여 인프라에 연결합니다. 각 프로토콜 및 컬렉션 모듈에는 특정 계정 권한이 필요합니다. 이 섹션에서는 전체 데이터 수집에 필요한 최소 권한과 특정 권한을 사용할 수 없는 경우 손실되는 데이터에 대해 설명합니다.

VMware vCenter

검색 도구는 포트 443(HTTPS)의 VMware vCenter Server에 연결하고 읽기 전용 작업을 수행합니다. vCenter 환경은 변경되지 않습니다.

최소 필수 역할: vCenter 루트 수준에서 할당된 읽기 전용.

읽기 전용 역할은 검색 도구가 VM 인벤토리(이름, UUID, CPU, 메모리, 디스크, 네트워크, 전원 상태, 게스트 OS) 및 성능 지표(CPU 사용률, 메모리 사용률, 디스크 IOPS 및 처리량)를 수집하는 데 필요한 모든 액세스를 제공합니다.

권장 사항: 루트 데이터 센터 수준에서 읽기 전용 역할이 내장된 전용 vCenter 사용자를 생성합니다.

Hyper-V 호스트(Windows)

검색 도구는 WinRM(HTTP의 경우 포트 5985, HTTPS의 경우 포트 5986)을 통해 Hyper-V 호스트에 연결하고 PowerShell 명령을 실행하여 VM 인벤토리, 호스트 메타데이터 및 스토리지 성능을 수집합니다.

각 Hyper-V 호스트에 필요한 최소 그룹 멤버십:

Windows 그룹	필요한 이유
원격 관리 사용자	기본 WinRM 원격 액세스
Hyper-V 관리자	VM 인벤토리 수집(VM 목록, 디스크, 네트워크, 메모리, 게스트 OS)
성능 모니터 사용자	스토리지 I/O 성능 카운터(읽기/쓰기 IOPS 및 VM당 처리량)

또한 계정에는 호스트 OS 버전 및 하드웨어 UUID의 root\cimv2 네임스페이스에 대한 WMI 읽기 액세스 권한이 필요합니다. 이 액세스 권한은 기본적으로 로컬 관리자에게 부여되지만 관리자가 아닌 계정에 대해 명시적으로 구성해야 합니다.

권장 사항: 전용 도메인 서비스 계정을 생성하고 각 Hyper-V 호스트의 원격 관리 사용자, Hyper-V 관리자 및 성능 모니터링 사용자 그룹에 추가합니다. 도메인 관리자 계정을 사용하지 마세요.

Linux 서버(SSH)

검색 도구는 SSH(포트 22)를 통해 Linux 서버에 연결하여 OS 지표, 네트워크 연결 및 서버 인벤토리를 수집합니다. 대부분의 데이터 수집은 일반 사용자로 실행됩니다. 소수의 명령이 시도sudo되고 sudo를 사용할 수 없는 경우 자동으로 감소합니다.

필요한 최소 액세스: 대상 서버에 로그인할 수 있는 SSH 사용자 계정입니다.

권장 액세스: 전체 데이터 수집을 위해 암호 없는 sudo로 구성된 것과 동일한 SSH 사용자입니다.

sudo가 필요한 사항과 sudo 없이 발생하는 상황:

수집된 데이터	Sudo가 필요합니까?	sudo 없이 잃어버리는 것
서버 이름, OS, CPU, 메모리, IP, 디스크 수	아니요	없음 - 일반 사용자로 수집됨
CPU, 메모리 및 네트워크 사용률	아니요	없음 - 일반 사용자로 수집됨
디스크 IOPS, 처리량 및 공간	아니요	없음 - 일반 사용자로 수집됨

수집된 데이터	Sudo가 필요합니까?	sudo 없이 잃어버리는 것
네트워크 인터페이스 구성	아니요	없음 - 일반 사용자로 수집됨
실행 중인 프로세스(이름, PID, 명령)	아니요	없음 - 일반 사용자로 수집됨
서버 UUID 및 SMBIOS UUID	예	내보내기에서 UUID 필드가 비어 있음
하드웨어 제조업체(물리적 탐지와 가상 탐지)	예	이전 배포에서는 리소스 유형 감지의 정확도가 떨어집니다.
LVM 논리적 볼륨 감지	예	LVM 볼륨이 감지되지 않습니다. 볼륨 유형은 "알 수 없음"으로 표시될 수 있습니다.
프로세스 이름 및 PID를 사용한 네트워크 연결	예	연결은 여전히 수집되지만 프로세스 속성은 없습니다(PID 및 프로세스 이름 열이 비어 있음).
Oracle Database OS 수준 감지 (Oracle 자격 증명이 구성되지 않은 경우 대체)	예	기본 Oracle 존재 감지(oratab, 프로세스 모니터)는 sudo 없이 작동합니다. 세부 컬렉션(opatch, lsnrctl, ASM, Grid Infrastructure)을 사용하려면 Oracle 홈 바이너리에 암호 없이 <code>sudo -u oracle</code> 액세스해야 합니다.

Note

sudo 부족으로 인해 검색 도구가 완전히 실패하지는 않습니다. 가능한 것을 수집하고 부분적인 결과를 보고합니다. 그러나 가장 완전한 데이터, 특히 프로세스 이름을 사용한 네트워크 종속성 매핑의 경우 암호 없는 sudo를 사용하는 것이 좋습니다.

대상 서버에 필요한 유틸리티: `ss` 또는 `, netstat, , , lsbblk, ,` 및 명령을 사용할 수 있어야 합니다(대부분의 Linux 배포판에 기본적으로 설치됨 `toppsfreeipdfhostnameatnprocgrep`). 추가 데이터의 경우 선택 사항: `iostat` (디스크 I/O 세부 정보), `dmidecode` (하드웨어 UUID), `smartctl` (디스크 인터페이스 유형), `lvdisplay` (LVM 감지).

Windows 서버(WinRM) - OS 지표

검색 도구는 WinRM을 통해 Windows 서버에 연결하여 OS 지표(서버 인벤토리, 성능, 스토리지, 네트워크 인터페이스 및 실행 중인 프로세스)를 수집합니다.

최소 필수 액세스: 대상 서버에 원격으로 액세스할 수 있는 WinRM 지원 사용자 계정입니다.

권장 액세스: 전체 데이터 수집을 위한 로컬 관리자 그룹의 사용자입니다.

권한 수준	활성화 대상	손실이 없는 경우
원격 관리 사용자 (WinRM 액세스)	모든 Windows 데이터 수집	서버에서 수집된 데이터 없음
에 대한 WMI 읽기 액세스 root\cimv2	서버 이름, OS 버전, 메모리, UUID, BIOS 직렬, 디스크 공간	서버 인벤토리 필드가 비어 있음
성능 모니터 사용자	CPU 사용률, 네트워크 처리량, 디스크 IOPS 및 처리량	성능 지표가 수집되지 않음
로컬 관리자	프로세스 소유자 이름 실행	프로세스 목록이 수집되었지만 사용자/소유자 열이 비어 있음

Note

로컬 관리자 멤버십은 묵시적으로 성능 모니터 사용자에게 액세스 및 WMI 읽기 액세스 권한을 부여하므로 위의 모든 요구 사항을 충족합니다.

Note

Windows의 Oracle Database OS 수준 폴백 감지는 Oracle 자격 증명이 구성되지 않은 경우 레지스트리 쿼리와 Get-Service 및 Get-Process 명령을 사용합니다. 이러한 명령에는 표준 원격 관리 사용자 액세스만 필요합니다. OS 지표 요구 사항 이외의 추가 권한은 필요하지 않습니다.

Windows 서버(WinRM) - SQL Server 컬렉션

SQL Server 컬렉션은 Windows 서버에서 SQL Server 인스턴스, Reporting Services(SSRS) 및 Integration Services(SSIS)를 검색합니다.

권장 액세스: 각 대상 Windows 서버의 로컬 관리자 그룹에 속한 사용자입니다.

SQL Server 검색은 여러 WMI 네임스페이스를 쿼리하고 일부 작업에 대해 승격된 액세스가 필요하므로 로컬 관리자가 권장됩니다.

검색된 내용	필요한 권한	손실이 없는 경우
SQL Server Database Engine 인스턴스(버전, 에디션, 상태)	root\Microsoft\SqlServer\ComputerManagement* 네임스페이스에 대한 WMI 읽기 액세스	SQL Server 인스턴스가 검색되지 않음
SSRS(SQL Server Reporting Services)	root\Microsoft\SqlServer\ReportServer 네임스페이스에 대한 WMI 읽기 액세스	SSRS 구성 요소가 검색되지 않음
SSRS URL 및 포트 구성	권한 상승(로컬 관리자)	SSRS URL 예약 세부 정보 누락
SSIS(SQL Server Integration Services)	레지스트리 읽기 액세스 (HKLM)	SSIS 버전 및 에디션 누락
Port-to-service 연결	TCP 리스너 열거에 대한 액세스	수신 포트를 SQL Server 서비스와 연결할 수 없음

Note

SQL Server 컬렉션은 Windows 전용입니다. 검색 도구는 SQL Server 검색을 위해 Linux 서버를 건너뛵니다.

Oracle Database(SQL)

Oracle Database 컬렉션은 포트 1521(또는 사용자 지정 포트)의 Oracle 인스턴스에 직접 연결하여 데이터베이스 메타데이터를 수집합니다. 검색 도구에는 DBA 또는 SYSDBA 권한이 필요하지 않습니다.

최소 필수 액세스: SELECT_CATALOG_ROLE 권한이 있는 읽기 전용 Oracle 서비스 계정입니다.

검색 도구는 진단 팩 또는 튜닝 팩 보기에 액세스하지 않으므로 데이터 수집에 추가 Oracle 라이선스가 필요하지 않습니다.

계정을 생성하기 위한 SQL:

```
CREATE USER discovery_user IDENTIFIED BY <password>;
GRANT CREATE SESSION TO discovery_user;
GRANT SELECT_CATALOG_ROLE TO discovery_user;
```

OS 수준 대체: 데이터베이스 자격 증명이 구성되지 않았거나 연결이 실패하는 경우 검색 도구는 기존 SSH 또는 WinRM OS 자격 증명을 사용하여 Oracle 설치를 감지합니다. OS 지표 모듈에 필요한 것 외에 Oracle 관련 OS 권한은 추가로 필요하지 않습니다.

네트워크 컬렉션

네트워크 컬렉션은 서버의 운영 체제에 따라 다른 프로토콜을 사용합니다.

서버 OS	프로토콜	필요한 권한
Linux	SSH	연결 데이터에 대한 일반 사용자입니다. 프로세스 수준 세부 정보 (PID 및 프로세스 이름)에는 암호 없는 sudo가 권장됩니다.
Linux	SNMPv2	TCP MIB(tcpConnState, tcpConnectionProcess) 및 호스트 리소스 MIB(hrSWRunName)에 액세스할 수 있는 읽기 전용 커뮤니티 문자열입니다.
Linux	SNMPv3	SNMPv2와 동일한 MIBs에 대한 읽기 액세스 권한이 있는 USM 사용자. noAuthNoPriv, authNoPriv 및 authPriv 보안 수준을 지원합니다.
Windows	WinRM	root\StandardCIMV2 네임스페이스(MSFT_NetTCP Connection 클래스)에 대한 WMI 읽기 액세스입니다.

빠른 참조: 사용 사례별 최소 권한

사용 사례:	계정 유형	최소 권한
VMware VM 검색	vCenter 사용자	루트 데이터 센터 수준에서 읽기 전용 역할
Hyper-V VM 검색	Windows 도메인 또는 로컬 계정	각 호스트의 원격 관리 사용자 + Hyper-V 관리자 + 성능 모니터 사용자
Linux OS 지표 - 전체 데이터	SSH 사용자	암호 없는 sudo
Linux OS 지표 - 부분 데이터	SSH 사용자	일반 사용자(sudo 없음). UUID, 제조업체, LVM 및 네트워크 프로세스 정보가 누락됩니다.
Windows OS 지표 - 전체 데이터	WinRM 사용자	로컬 관리자
Windows OS 지표 - 기본 데이터	WinRM 사용자	원격 관리 사용자 +에 대한 WMI 읽기 액세스 root\cimv2
SQL Server 데이터베이스 검색	WinRM 사용자	로컬 관리자
Oracle 데이터베이스 검색(SQL)	Oracle 서비스 계정	SELECT_CATALOG_ROLE(읽기 전용, DBA 또는 SYSDBA 없음)
네트워크 컬렉션 - Linux(SSH)	SSH 사용자	프로세스 수준 데이터용 암호 없는 sudo, 연결 데이터 전용 일반 사용자
네트워크 컬렉션 - Linux(SNMP)	SNMP 커뮤니티 문자열 또는 USM 사용자	TCP 및 호스트 리소스 MIBs 읽기 액세스
네트워크 컬렉션 - Windows	WinRM 사용자	에 대한 WMI 읽기 액세스 root\StandardCIMV2

데이터 수집

검색 도구 수집 일정

초기 검색 수집 후 검색 도구는 리소스 경합을 방지하기 위해 시차를 둔 일정에 따라 계속 실행됩니다.

- VMware 검색 - 매시간(:00 UTC)
- Hyper-V 검색 - 매시간(:20 UTC)

또한 검색 도구는 다음과 같은 독립 모듈을 통해 OS 지표를 수집하며, 각 모듈에는 시차가 지정된 고유한 일정이 있습니다.

- 네트워크 지표 - 15초마다 대규모 환경에서 빈도가 낮을 수 있습니다.
- 서버 성능 지표 - 10분마다(:03, :13, :23, :33, :43, :53 UTC)
- 스토리지 성능 지표 - 10분마다(:07, :17, :27, :37, :47, :57 UTC)
- 프로세스 실행 - 시간당(:40 UTC)
- 서버 프로비저닝 데이터 - 일별(00:05 UTC)
- 스토리지 프로비저닝 데이터 - 일별(00:35 UTC)
- 네트워크 인터페이스 - 일별(01:05 UTC)
- SQL Server 검색 - 일별(03:05 UTC)
- Oracle 데이터베이스 검색 - 매일(05:05 UTC)

지금 데이터 수집을 사용하여 각 OS 지표 모듈을 독립적으로 시작, 중지 또는 트리거할 수 있습니다.

컬렉션을 수동으로 실행하려면 작업 메뉴에서 다음을 선택합니다.

- 시작 - 검색 모듈을 활성화합니다.
- 중지 - 검색 모듈을 비활성화합니다.
- 지금 데이터 수집 - 검색을 즉시 시작합니다. 예를 들어 네트워크를 변경한 후 옵션을 사용합니다.

이러한 작업은 모듈별로 적용됩니다. OS 지표 모듈을 개별적으로 제어할 수 있습니다.

OS 데이터 수집 시도

새 서버가 검색되면 검색 도구는 각 IP 주소와 호스트 이름에 대해 구성된 각 자격 증명을 시도합니다. 검색 도구가 유효한 자격 증명을 찾으면 새 자격 증명을 추가하지 않는 한 해당 자격 증명을 계속 사용합니다.

수집 실패 후 검색 도구는 3분, 30분, 2시간, 6시간 후에 서버의 네트워킹 데이터를 수집하려고 시도합니다. 4번의 시도가 실패하면 검색 도구는 구성된 모든 자격 증명을 6시간마다 한 번씩 계속 시도합니다.

검색된 인벤토리

검색 소스를 구성한 후 검색 도구 상태 프레임의 검색된 서버 수 값이 증가하기 시작합니다. 구성된 소스의 검색 상태가 컬렉션 모듈 프레임에서 활성화됨으로 변경됩니다. 인벤토리 페이지에는 VMware VMs Hyper-V VM, 가져온 서버 등 구성된 모든 소스의 서버VMs 표시됩니다. 각 서버는 모듈당 소스 및 컬렉션 상태를 표시합니다.

검색된 인벤토리 페이지로 이동하여 검색 도구가 찾은 서버를 확인합니다. 이 페이지에서 인벤토리 다운로드를 선택하여 구성된 모든 소스에 대한 MPA 파일, 성능 사용률 데이터, 데이터베이스 정보 및 server-to-server 통신 정보를 포함하여 최대 30일간 수집된 데이터가 포함된 ZIP 파일 (discovery_tool_export.zip)을 다운로드합니다.

검색 도구가 계속 작동하는 동안 ZIP 파일을 다운로드하고 일부 결과를 얻을 수 있습니다. 마이그레이션을 [위한 비즈니스 사례를 얻으려면이 파일을 마이그레이션 평가에](#) 업로드합니다.

내보내기 옵션

데이터를 내보낼 때 다음 옵션을 사용하여 내보내기를 사용자 지정할 수 있습니다.

날짜 범위

시작 날짜와 종료 날짜를 선택하여 해당 기간 내에 수집된 데이터만 내보냅니다. 두 날짜 모두 포함됩니다. 최대 날짜 범위는 30일입니다.

Note

검색 도구는 수집된 데이터를 최대 30일 동안 저장합니다. 30일 이상의 데이터가 필요한 경우 30일마다 증분 내보내기를 실행하여 모든 데이터를 캡처합니다.

모듈 선택

내보내기에 포함할 데이터 모듈을 선택합니다. 모든 모듈을 내보내거나 특정 모듈을 선택할 수 있습니다.

모듈	설명
VMware 데이터	vCenter 서버의 가상 머신 인벤토리
Hyper-V 데이터	Hyper-V 호스트의 가상 머신 인벤토리
네트워크 데이터	서버 간 네트워크 연결
서버 인벤토리	서버 하드웨어 및 OS 정보
서버 성능 지표	CPU, 메모리 및 네트워크 사용률
서버 스토리지 성능	디스크 IOPS 및 처리량
스토리지 구성	디스크 및 볼륨 구성
네트워크 인터페이스	네트워크 어댑터 세부 정보
프로세스 지표	실행 중인 프로세스
SQL Server 데이터	SQL Server 데이터베이스 인벤토리
Oracle Database 데이터	Oracle 데이터베이스 인벤토리 - CDBs, PDBs, 기능, 옵션 및 구성 요소

모듈을 선택하지 않으면 검색 도구가 사용 가능한 모든 데이터를 내보냅니다.

수집된 데이터 포인트

검색 도구는 VMware, Hyper-V, OS 지표, 데이터베이스 및 네트워크 구성 요소 전반에서 포괄적인 데이터를 수집합니다. 다음 섹션에서는 각 구성 요소에 대해 수집된 특정 데이터 포인트를 자세히 설명합니다.

VMware 데이터 수집

이 표에서는 검색 도구에서 수집한 VMware 가상 머신 정보를 설명합니다.

이름	유형	카테고리	샘플 값
vm_name	문자열	VM 정보	"w2k22-snmpd-v2-en-us-mssql-2022-testcase4-1"
vm_id	문자열	VM 정보	"vm-30920"
vm_uuid	문자열	VM 정보	"4201ecf8-cc44-ee7e-01da-34dfb2acf6c0"
전원 상태	문자열	VM 정보	"poweredOn"
host	문자열	VM 정보	"esxi-70-node1.testlab.local"
primary_ip_address	문자열	VM 정보	"192.168.0.52"
cpus	Integer	VM 정보	2
메모리	Integer	VM 정보	4096
total_disk_capacity_mib	Integer	VM 정보	32768
os_according_to_the_configuration_file	문자열	VM 정보	"Microsoft Windows Server 2016 이상(64비트)"
max_cpu_usage_pct_dec	Float	VM 성능	79.33
avg_cpu_usage_pct_dec	Float	VM 성능	45.06
max_ram_usage_pct_dec	Float	VM 성능	63.99
avg_ram_util_pct_dec	Float	VM 성능	29.27

Hyper-V 데이터 수집

이 표에서는 검색 도구에서 수집한 Hyper-V 가상 머신 정보를 설명합니다.

이름	유형	카테고리	샘플 값
vm_name	문자열	VM 정보	"win2022-hyperv-test-01"

이름	유형	카테고리	샘플 값
vm_id	문자열	VM 정보	"a1b2c3d4-e5f6-7890-abcd-ef1234567890"
전원 상태	문자열	VM 정보	"실행"
cpus	Integer	VM 정보	4
memory_mb	Integer	VM 정보	8192
disk_paths	문자열	디스크	"C:\\VMs\\disk1.vhdx"
디스크_크기_gb	Float	디스크	127.0
network_adapters	문자열	Network	"00:15:5D:01:02:03"
ip_addresses	문자열	Network	"10.0.1.50"
host_name	문자열	Host	"hyperv-host-01.example.com"
호스트_os_버전	문자열	Host	"Windows Server 2022 Datacenter"
cluster_name	문자열	Host	"FailoverCluster01"
하이퍼바이저	문자열	VM 정보	"Hyper-V"

가져온 서버 데이터

가져온 서버는 자동으로 검색되지 않습니다. CSV 파일을 통해 가져옵니다. 검색 도구는 가져온 서버에 대한 하이퍼바이저 수준 데이터를 수집하지 않습니다. 대신 가져오기 중에 각 서버와 연결된 OS 자격 증명을 사용하여 데이터베이스, 네트워크 및 OS 지표 데이터를 수집합니다.

검색 도구의 OS 관련 데이터

검색 도구는 SSH(Linux) 및 WinRM(Windows)을 통해 서버 인벤토리, 성능, 스토리지, 네트워크 인터페이스를 수집하고 데이터를 처리합니다. 다음 표에서는 수집된 데이터 포인트를 설명합니다.

서버 인벤토리(server_inventory.csv)

서버 프로비저닝(하드웨어 및 OS 구성)을 집계된 스토리지 성능과 결합합니다. 24시간마다 수집됩니다.

이름	유형	카테고리	샘플 값
server_id	문자열	서버 정보	"vm-web-server-01"
server_name	문자열	서버 정보	"웹 서버-01"
resource_type	문자열	서버 정보	"가상_기계"
power_state	문자열	서버 정보	"실행"
os_type	문자열	서버 정보	"Linux"
os_name	문자열	서버 정보	"Amazon Linux"
os_version	문자열	서버 정보	"2023"
primary_hostname	문자열	서버 정보	"web-server-01.example.com"
primary_ip_address	문자열	서버 정보	"10.0.2.101"
넷마스크	문자열	서버 정보	"255.255.255.0"
total_num_network_cards	Integer	서버 정보	2
total_num_disks	Integer	서버 정보	1
cpu_count	Integer	서버 정보	4
total_memory_gb	Float	서버 정보	15.88
server_uuid	문자열	서버 정보	"4201ecf8-cc44-ee7e-01da-34dfb2acf6c0"
smbios_uuid	문자열	서버 정보	"4201ecf8-cc44-ee7e-01da-34dfb2acf6c0"

이름	유형	카테고리	샘플 값
cluster_name	문자열	서버 정보	"production-cluster-01"
하이퍼바이저_객체_id	문자열	서버 정보	"vm-30920"
하이퍼바이저_유형	문자열	서버 정보	"VMware"
하이퍼바이저_버전	문자열	서버 정보	"8.0.0"
하이퍼바이저_호스트 이름	문자열	서버 정보	"esxi-node1.example.com"
하이퍼바이저_호스트_id	문자열	서버 정보	"host-1234"
하이퍼바이저_id	문자열	서버 정보	"4201ecf8-cc44-ee7e-01da-34dfb2acf6c0"
disk_read_iops_avg	Float	스토리지 성능	12.5
disk_read_iops_peak	Float	스토리지 성능	245.0
디스크_쓰기_iops_평균	Float	스토리지 성능	8.3
disk_write_iops_peak	Float	스토리지 성능	180.0
disk_total_iops_avg	Float	스토리지 성능	20.8
disk_total_iops_peak	Float	스토리지 성능	425.0
disk_read_throughput_avg_mbps	Float	스토리지 성능	1.2
disk_read_throughput_peak_mbps	Float	스토리지 성능	24.5

이름	유형	카테고리	샘플 값
디스크_쓰기_처리량_평균_mbps	Float	스토리지 성능	0.8
디스크_쓰기_처리량_피크_mbps	Float	스토리지 성능	18.0
disk_total_throughput_avg_mbps	Float	스토리지 성능	2.0
디스크_총_처리량_피크_mbps	Float	스토리지 성능	42.5

서버 성능 지표(server_performance_metrics.csv)

CPU, 메모리 및 네트워크 처리량 사용률. 10분마다 샘플링되고 30일 동안 집계됩니다.

이름	유형	카테고리	샘플 값
server_id	문자열	서버 정보	"vm-web-server-01"
data_source	문자열	서버 정보	"OS"
cpu_utilization_avg_pct	Float	CPU	45.06
cpu_utilization_peak_pct	Float	CPU	79.33
cpu_count	Integer	CPU	4
memory_total_gb	Float	Memory	15.88
memory_utilization_avg_pct	Float	Memory	29.27
memory_utilization_peak_pct	Float	Memory	63.99
network_in_avg_mbps	Float	Network	0.52
network_in_peak_mbps	Float	Network	12.3

이름	유형	카테고리	샘플 값
network_out_avg_mbps	Float	Network	0.31
network_out_peak_mbps	Float	Network	8.7
network_total_avg_mbps	Float	Network	0.83
network_total_peak_mbps	Float	Network	21.0

스토리지 성능(server_storage_performance.csv)

볼륨당 디스크 I/O 및 공간 사용률. 10분마다 샘플링되고 30일 동안 집계됩니다.

이름	유형	카테고리	샘플 값
server_id	문자열	서버 정보	"vm-web-server-01"
data_source	문자열	서버 정보	"OS"
disk_volume_id	문자열	볼륨 정보	"/dev/nvme0n1p1"
disk_mount_point	문자열	볼륨 정보	"/"
file_system	문자열	볼륨 정보	"xfs"
disk_total_gb	Float	디스크 공간	30.0
disk_used_gb	Float	디스크 공간	12.5
disk_free_gb	Float	디스크 공간	17.5
disk_read_iops_avg	Float	디스크 I/O	12.5
disk_read_iops_peak	Float	디스크 I/O	245.0
디스크_쓰기_iops_평균	Float	디스크 I/O	8.3
disk_write_iops_peak	Float	디스크 I/O	180.0

이름	유형	카테고리	샘플 값
disk_total_iops_avg	Float	디스크 I/O	20.8
disk_total_iops_peak	Float	디스크 I/O	425.0
disk_read_throughput_avg_mbps	Float	디스크 처리량	1.2
disk_read_throughput_peak_mbps	Float	디스크 처리량	24.5
디스크_쓰기_처리량_평균_mbps	Float	디스크 처리량	0.8
디스크_쓰기_처리량_피크_mbps	Float	디스크 처리량	18.0
disk_total_throughput_avg_mbps	Float	디스크 처리량	2.0
디스크_총_처리량_피크_mbps	Float	디스크 처리량	42.5

스토리지 구성(storage_config.csv)

물리적 디스크 하드웨어 세부 정보입니다. 24시간마다 수집됩니다.

이름	유형	카테고리	샘플 값
server_id	문자열	서버 정보	"vm-web-server-01"
disk_controller_id	문자열	디스크 정보	"/dev/sda"
vmdk_vhd_file_name	문자열	디스크 정보	"웹 서버-01.vmdk"
disk_volume_type	문자열	디스크 정보	"가상"
disk_provisioned_gb	Float	디스크 정보	30.0

이름	유형	카테고리	샘플 값
disk_device_type	문자열	디스크 정보	"SCSI HDD"
disk_interface_type	문자열	디스크 정보	"SCSI"
disk_protocol	문자열	디스크 정보	"LSI 로직 SAS"

네트워크 인터페이스(network_interfaces.csv)

네트워크 어댑터 구성. 24시간마다 수집됩니다.

이름	유형	카테고리	샘플 값
server_id	문자열	서버 정보	"vm-web-server-01"
interface_name	문자열	인터페이스 정보	"eth0"
interface_index	Integer	인터페이스 정보	2
mac_address	문자열	인터페이스 정보	"0A:1B:2C:3D:4E:5F"
adapter_type	문자열	인터페이스 정보	"vmxnet3"
가상_네트워크_이름	문자열	인터페이스 정보	"VM 네트워크"
가상_네트워크_id	문자열	인터페이스 정보	"dvportgroup-1234"
가상_스위치	문자열	인터페이스 정보	"vSwitch0"
ipv4_address	문자열	IP 구성	"10.0.2.101"

이름	유형	카테고리	샘플 값
ipv4_subnet_mask	문자열	IP 구성	"255.255.255.0"
ipv4_gateway	문자열	IP 구성	"10.0.2.1"
ipv6_address	문자열	IP 구성	"fe80::a1b:2cff:fe3d:4e5f"
ipv6_prefix_length	Integer	IP 구성	64
ipv6_게이트웨이	문자열	IP 구성	"fe80::1"
dns_서버	문자열	IP 구성	"10.0.0.2"
dhcp_enabled	부울	IP 구성	false
interface_status	문자열	인터페이스 정보	"위로"
vlan_id	Integer	인터페이스 정보	100
is_primary	부울	인터페이스 정보	true

프로세스 실행(process_metrics.csv)

실행 중인 프로세스의 스냅샷입니다. 1시간마다 수집되며 30일 동안 중복 제거됩니다.

이름	유형	카테고리	샘플 값
server_id	문자열	서버 정보	"vm-web-server-01"
process_name	문자열	프로세스 정 보	"sshd"
process_id	Integer	프로세스 정 보	1234

이름	유형	카테고리	샘플 값
process_command_line	문자열	프로세스 정보	"/usr/sbin/sshd -D"
process_user	문자열	프로세스 정보	"루트"

네트워크 컬렉션

네트워크 수집 모듈은 온프레미스 데이터 센터의 서버 간 종속성을 검색하는 데 도움이 됩니다. 이 네트워크 데이터는 애플리케이션이 서버 간에 통신하는 방식에 대한 가시성을 제공하여 마이그레이션 계획을 가속화합니다.

이 모듈은 VMware, Hyper-V 및 가져온 서버를 포함하여 구성된 모든 소스에서 서버의 네트워크 데이터를 수집합니다. WinRM을 사용하여 Windows 서버에서 데이터를 수집하고 SSH, SNMPv2 및 SNMPv3를 사용하여 Linux 서버에서 데이터를 수집합니다.

네트워크 데이터 수집

네트워크 컬렉션 모듈은 검색된 인벤토리의 서버 간에 TCP IPv4 연결을 ESTABLISHED 또는 TIME_WAIT 상태로 캡처합니다. 소스 및 대상 IP 주소가 모두 검색 도구가 검색했거나 가져온 서버에 속하는 경우에만 출력에 연결이 나타납니다. 외부 서비스, 클라우드 엔드포인트 또는 검색 도구에 아직 추가되지 않은 서버와 같이 인벤토리 외부의 IP 주소와의 연결은 포함되지 않습니다.

이 설계는 애플리케이션 종속성 매핑 및 마이그레이션 웨이브 계획에 필요한 정보인 환경 내 server-to-server 종속성에 네트워크 데이터를 집중적으로 다룹니다.

이러한 데이터 포인트는 각 연결에 대해 수집됩니다.

이름	유형	카테고리	샘플 값
소스 IP	문자열	Connection	"192.168.1.10"
원본 포트	Integer	Connection	49152
소스 프로세스 ID	Integer	프로세스	1234
소스 프로세스 이름	문자열	프로세스	"java"

이름	유형	카테고리	샘플 값
대상 IP	문자열	Connection	"192.168.1.20"
대상 포트	Integer	Connection	5432
대상 프로세스 ID	Integer	프로세스	5678
대상 프로세스 이름	문자열	프로세스	"postgres"
State	문자열	Connection	"ESTABLISHED"
전송 프로토콜	문자열	Connection	"TCP"
IP 버전	문자열	Connection	"IPv4"
개수	Integer	Connection	42

Tip

네트워크 종속성 맵의 완전성을 극대화하려면 네트워크 데이터를 검토하기 전에 모든 검색 소스(VMware, Hyper-V 및 서버 CSV 가져오기)를 구성하고 OS 자격 증명을 추가합니다. 인벤토리에 서버가 많을수록 네트워크 모듈이 캡처할 수 있는 연결이 늘어납니다.

프라이빗 주소 네트워크 컬렉션

기본적으로 네트워크 컬렉션 모듈은 두 엔드포인트가 모두 검색된 인벤토리의 서버인 연결만 캡처합니다. 프라이빗 주소 수집을 활성화하여 인벤토리에 없는 RFC 1918 프라이빗 IP 주소(10.0.0.0/8, 172.16.0.0/12, 192.168.0.0/16)와의 연결을 캡처할 수도 있습니다.

프라이빗 주소 수집을 시작하려면

1. 수집기 구성 페이지에서 컬렉션 모듈 섹션을 찾습니다.
2. 애플리케이션 검색에서 네트워크 연결 검색을 찾습니다.
3. 작업 드롭다운을 엽니다.
4. 프라이빗 주소 수집 시작을 선택합니다.
5. 모듈 상태가 활성화됨이면 활성화됨 · 프라이빗 주소 켜짐으로 변경되는 것을 볼 수 있습니다.

프라이빗 주소 수집을 중지하려면 작업 드롭다운을 열고 프라이빗 주소 수집 중지를 선택합니다. 이전에 수집된 프라이빗 주소 데이터는 중지 후에도 유지됩니다.

프라이빗 주소 연결은 전체 CSV 내보내기(ZIP 파일 내부)에만 표시되며 MPA CSV 파일에는 표시되지 않습니다. IP 주소가 이미 인벤토리에 있는 서버에 속하는 경우 이 설정과 관계없이 항상 검색된 서버 ID로 식별됩니다.

이 설정은 재시작 후에도 유지됩니다. 언제든지 프라이빗 주소 수집을 시작하거나 중지할 수 있습니다. 이전에 수집된 프라이빗 주소 데이터는 현재 설정에 관계없이 내보내집니다.

SQL Server 컬렉션

SQL Server 컬렉션 모듈은 VMware, Hyper-V 및 가져온 서버를 포함하여 구성된 모든 소스의 Windows 서버에서 SQL Server 정보를 수집합니다. 모듈은 WinRM을 사용하여 각 Windows 서버에 원격으로 연결하고 PowerShell 쿼리를 실행합니다. WMI 네임스페이스, 레지스트리 및 파일 속성을 사용하여 설치된 모든 SQL Server 서비스(구성 요소)에 대한 정보를 수집합니다.

SQL Server 구성 요소는 Windows 서버에 SQL Server 배포의 일부로 설치된 특정 서비스 또는 기능 인스턴스입니다. 검색 도구는 데이터베이스 엔진, 분석 서비스, 보고 서비스 및 통합 서비스를 수집합니다.

SQL Server 데이터 수집

SQL Server 컬렉션 모듈은 SQL Server 구성 요소 정보를 수집합니다. 이 표에서는 수집된 주요 데이터 포인트를 설명합니다.

이름	유형	카테고리	샘플 값
엔진 유형	문자열	구성 요소	sql_서버
엔진 구성 요소입니까?	부울	구성 요소	Y
Status	문자열	서비스	실행 중, 중지됨, StartPending
버전	문자열	서비스	2015년 131월 5026.0일
Edition	문자열	서비스	Developer Edition(64비트)
SQL 서비스 이름	문자열	서비스	MsDtsServer130, Mssql

이름	유형	카테고리	샘플 값
SQL 서비스 유형	문자열	서비스	SQL Server 서비스, 통합 서비스 서비스
인스턴스 이름	문자열	Instance	MSSQLSERVER
표시 이름	문자열	서비스	SQL Server(MSSQLSERVER 2017)
시작 모드	문자열	서비스	자동, 수동, 비활성화됨
서비스 계정 이름	문자열	서비스	NT 서비스/MsDtsServer130
클러스터링됨	부울	구성	N

Note

전체 형식에는 모든 서비스 유형이 포함됩니다. MPA 형식에는 데이터베이스 엔진 구성 요소만 포함됩니다. SQL 서비스 유형 및 구성에 따라 모든 필드를 사용할 수 있는 것은 아닙니다.

Oracle Database 컬렉션

Oracle Database 컬렉션을 사용하면 VMware, Hyper-V 및 가져온 서버를 포함하여 구성된 모든 소스에서 Oracle 데이터베이스 인스턴스를 검색할 수 있습니다. 모듈은 다음 데이터를 수집합니다.

- 컨테이너 데이터베이스(CDB) 및 플러그형 데이터베이스(PDB) 열거
- 버전 및 에디션
- 설치된 옵션
- 기능 사용 통계
- 구성 요소 인벤토리(DBA_REGISTRY)
- 데이터 파일 크기 조정
- 토폴로지 플래그(RAC, Data Guard 및 멀티테넌트 아키텍처)

데이터베이스 연결(SQL)

Oracle 자격 증명을 구성하면 검색 도구가 읽기 전용 서비스 계정을 사용하여 Oracle 데이터베이스에 직접 연결됩니다. 이렇게 하면 PDB 세부 정보, 기능 사용 및 설치된 옵션을 포함한 전체 SQL 수준 컬렉션이 제공됩니다. 모든 CSV 파일에는 전체 데이터가 포함됩니다.

OS 수준 대체

데이터베이스 자격 증명을 구성하지 않았거나 연결이 실패하는 경우 검색 도구는 SSH 또는 WinRM을 사용하여 Oracle 설치를 감지합니다. 데이터베이스 액세스 없이 Oracle 홈, 리스너, 패치, 버전 및 에디션을 검색합니다. OS 감지 호스트의 경우 내보낸 CDB CSV에는 인스턴스 이름, 호스트 이름, 버전 및 에디션이 포함됩니다. PDB, 기능, 옵션 및 구성 요소 CSV 파일에는 행이 없습니다.

Oracle 컬렉션은 내보내기 ZIP에 다음과 같은 CSV 파일을 생성합니다. 각 표는 파일당 수집된 데이터 포인트를 설명합니다.

CDB 데이터(oracle_data_cdb_full.csv)

CDB 인스턴스당 행 1개. 이 표에서는 수집된 CDB 데이터 포인트를 설명합니다.

이름	유형	카테고리	샘플 값	소스
인스턴스 이름	문자열	ID	"ORCL"	SQL, OS
호스트 이름	문자열	ID	"oracledb01.example.com"	SQL, OS
DB 이름	문자열	ID	"ORCL"	SQL 전용
DB 고유 이름	문자열	ID	"ORCL_PRIMARY"	SQL 전용
DBID	Integer	ID	1234567890	SQL 전용
버전	문자열	버전	"19.0.0.0"	SQL, OS
버전 가독 참	문자열	버전	"19.21.0.0.0"	SQL 전용
Edition	문자열	버전	"Enterprise Edition"	SQL, OS
데이터베이스 유형	문자열	구성	"단일"	SQL 전용
데이터베이스 역할	문자열	구성	"프라이머리"	SQL 전용
열기 모드	문자열	구성	"쓰기 읽기"	SQL 전용

이름	유형	카테고리	샘플 값	소스
로그 모드	문자열	구성	"ARCHIVELOG"	SQL 전용
플랫폼	문자열	구성	"Linux x86 64비트"	SQL 전용
CDB 플래그	문자열	구성	"예"	SQL 전용
RAC임	문자열	토폴로지	"예" 또는 "아니요"	SQL 전용
데이터 가드 대기 여부	문자열	토폴로지	"예" 또는 "아니요"	SQL 전용
보호 모드	문자열	토폴로지	"최대 성능"	SQL 전용
Data Guard 브로커	문자열	토폴로지	"활성화"	SQL 전용
NLS 문자 집합	문자열	구성	"AL32UTF8"	SQL 전용
PDB 수	Integer	크기 조정	3	SQL 전용
플래시백 켜기	문자열	구성	"예"	SQL 전용
감지 경로	문자열	Metadata	"phase2" 또는 "phase1b"	SQL, OS

PDB 데이터(oracle_data_pdb_full.csv)

PDB당 행 1개(플러그형 데이터베이스). 이 표에서는 수집된 PDB 데이터 포인트를 설명합니다.

Note

PDB 데이터에는 Oracle 데이터베이스 자격 증명(SQL 연결)이 필요합니다. OS 수준 대체는 이 CSV를 채우지 않습니다.

이름	유형	카테고리	샘플 값	소스
CDB 인스턴스 이름	문자열	ID	"ORCL"	SQL 전용
PDB 이름	문자열	ID	"APPPDB1"	SQL 전용

이름	유형	카테고리	샘플 값	소스
열기 모드	문자열	Status	"쓰기 읽기"	SQL 전용
수명 주기 상태	문자열	Status	"정상"	SQL 전용
테이블스페이스 수	Integer	크기 조정	5	SQL 전용
데이터 파일 수	Integer	크기 조정	12	SQL 전용
총 크기 바이트	Integer	크기 조정	5368709120	SQL 전용
사용자 스키마 수	Integer	크기 조정	8	SQL 전용
DB 링크 수	Integer	연결	2	SQL 전용
설치된 구성 요소	문자열	구성	"APEX;JVM;XML"	SQL 전용
암호화된 테이블스페이스 수	Integer	보안	1	SQL 전용

특성 사용 데이터(oracle_data_features_full.csv)

DBA_FEATURE_USAGE_STATISTICS의 기능 사용 항목당 행 1개. 이 표에서는 수집된 기능 사용 데이터 포인트를 설명합니다.

Note

기능 사용 데이터에는 Oracle 데이터베이스 자격 증명(SQL 연결)이 필요합니다. OS 수준 대체는 이 CSV를 채우지 않습니다.

이름	유형	카테고리	샘플 값	소스
CDB 인스턴스 이름	문자열	ID	"ORCL"	SQL 전용
이름	문자열	기능	"파티션(사용자)"	SQL 전용
감지된 사용량	Integer	용도	42	SQL 전용

이름	유형	카테고리	샘플 값	소스
현재 사용 중	문자열	용도	"TRUE"	SQL 전용
첫 번째 사용 날짜	DateTime	용도	"2024-01-15T00:00:00"	SQL 전용
마지막 사용 날짜	DateTime	용도	"2026-06-01T00:00:00"	SQL 전용

옵션 데이터(oracle_data_options_full.csv)

CDB당 V\$OPTION 항목당 행 1개. 이 표에서는 수집된 설치된 옵션 데이터 포인트를 설명합니다.

Note

옵션 데이터에는 Oracle 데이터베이스 자격 증명(SQL 연결)이 필요합니다. OS 수준 대체는 이 CSV를 채우지 않습니다.

이름	유형	카테고리	샘플 값	소스
CDB 인스턴스 이름	문자열	ID	"ORCL"	SQL 전용
옵션 이름	문자열	옵션	"고급 분석"	SQL 전용
설치됨	문자열	옵션	"TRUE"	SQL 전용
컨테이너 ID입니다	Integer	옵션	0	SQL 전용

구성 요소 데이터(oracle_data_components_full.csv)

DBA_REGISTRY 구성 요소당 행 1개. 이 표에서는 수집된 구성 요소 데이터 포인트를 설명합니다.

Note

구성 요소 데이터에는 Oracle 데이터베이스 자격 증명(SQL 연결)이 필요합니다. OS 수준 대체는 이 CSV를 채우지 않습니다.

이름	유형	카테고리	샘플 값	소스
CDB 인스턴스 이름	문자열	ID	"ORCL"	SQL 전용
PDB 이름	문자열	ID	"APPPDB1"	SQL 전용
구성 요소 ID	문자열	구성 요소	"APEX"	SQL 전용
구성 요소 이름	문자열	구성 요소	"Oracle Application Express"	SQL 전용
버전	문자열	구성 요소	"22.1.0.15.0"	SQL 전용
Status	문자열	구성 요소	"VALID"	SQL 전용
스키마	문자열	구성 요소	"APEX_220100"	SQL 전용

보안 고려 사항

검색 도구 VM 보안

검색 도구 VM 보안은 검색 도구 VM에 모든 자격 증명, 로그 및 고객 데이터를 저장하기 때문에 매우 중요합니다.

검색 도구 VM에는 기본적으로 ssh 액세스가 비활성화되어 있으며 클라이언트에서만 액세스할 수 있습니다vCenter UI -> "Launch Web Console".

검색 도구 VM에는 사용자 "discovery"에 대한 기본 로그인 암호 "password"가 함께 제공됩니다.

- 배포 직후이 암호를 업데이트하는 것이 좋습니다.
- vCenter를 사용하여 로그인한 enablessh 후 명령을 사용하여 ssh를 활성화하려면 암호를 업데이트해야 합니다Launch Web Console. 이 명령을 호출할 때마다 명령을 재설정해야 합니다.

보안 자격 증명

자격 증명 관리에 대한 일반적인 모범 사례

- 자격 증명을 안전하게 저장

- 모든 자격 증명을 정기적으로 교체
- 암호 관리자 또는 보안 볼트 사용
- 자격 증명 사용량 모니터링
- 최소 권한 원칙을 따르고 필요한 최소 권한만 부여합니다.

SNMP v2 자격 증명

- 복잡하고 기본이 아닌 커뮤니티 문자열 사용
- "퍼블릭" 또는 "프라이빗"과 같은 일반적인 문자열은 피합니다.
- 커뮤니티 문자열을 암호처럼 취급

SNMP v3 자격 증명

- 인증 및 개인 정보 보호 모두 활성화
- 강력한 인증 프로토콜 사용(MD5보다 SHA 선호)
- 강력한 암호화 프로토콜 사용(DES보다 AES 선호)
- 인증 및 개인 정보 보호 모두에 복잡한 암호 사용
- 고유한 사용자 이름 사용(일반 이름 피하기)

WinRM 자격 증명

- WinRM 인증서 검사를 비활성화하지 마세요.
- 최소한의 필수 권한으로 전용 서비스 계정을 생성하는 것이 좋습니다.
- SQL Server 컬렉션이 필요하지 않은 한 도메인 관리자 또는 로컬 관리자 계정을 사용하지 마세요. SQL Server 컬렉션은 여러 WMI 네임스페이스를 쿼리하고 승격된 명령을 사용하기 때문에 로컬 관리자 액세스가 필요합니다. SQL Server 검색이 없는 OS 지표의 경우 원격 관리 사용자, 성능 모니터 사용자 및에 대한 WMI 읽기 액세스 권한이 있는 관리자가 아닌 계정으로 충분root\cimv2합니다. 모듈별 세부 정보는 섹션을 참조[the section called “필수 권한”](#)하세요.

Hyper-V 자격 증명

- 최소한의 Hyper-V 관리 권한으로 전용 서비스 계정을 사용합니다.
- 도메인 관리자 계정을 사용하지 마세요.
- Hyper-V 자격 증명은 NTLM(HTTPS만 해당) 및 Kerberos 인증을 지원합니다.

- 검색 도구는 SQLCipher를 사용하여 저장 시 암호화된 자격 증명을 저장합니다.

Oracle 자격 증명

- SELECT_CATALOG_ROLE만 있는 전용 읽기 전용 서비스 계정을 사용합니다. DBA, SYSDBA 또는 SYSOPER 권한을 사용하지 마십시오.
- 검색 도구는 읽기 작업만 수행하고 Oracle 데이터베이스에는 쓰지 않습니다.
- 검색 도구는 진단 팩 또는 튜닝 팩 보기에 액세스하지 않으므로 추가 Oracle 라이선스가 필요하지 않습니다.
- Oracle 서비스 계정 암호를 정기적으로 교체하고 검색 도구에서 자격 증명을 업데이트합니다.

자격 증명 스토리지

검색 도구는 데이터베이스 암호화 키를 사용하여 저장된 자격 증명을 암호화합니다. systemd 250 이상이 설치된 시스템에서 이 키는 systemd-creds를 사용하여 암호화됩니다. 이전 시스템에서 키는 권한 보호 파일로 저장됩니다. 두 경우 모두 검색 도구 호스트에 대한 루트 액세스 권한이 있는 공격자는 암호화 키에 액세스하고 저장된 자격 증명을 해독할 수 있습니다. 검색 도구 호스트에 대한 액세스를 제한하고 환경의 권한 있는 시스템으로 취급합니다.

주의하여 자동 연결 기능 사용

검색 도구는 두 가지 메커니즘, 즉 자동 연결과 수동을 사용하여 OS 수준 수집 중에 서버에 자격 증명을 할당합니다. OS 수준 컬렉션에는 네트워크, SQL Server, Oracle Database 및 OS 지표 모듈이 포함됩니다. 이러한 모듈은 VMware VMs, Hyper-V VMs 및 가져온 서버를 포함한 모든 소스의 개별 서버에 연결됩니다.

수동: 서버를 특정 자격 증명과 수동으로 연결할 수 있습니다. 이 경우 검색 도구는 성공 또는 실패에 관계없이 해당 자격 증명만 사용합니다. 해당 서버의 수집 상태를 수동으로 모니터링하고 조정해야 합니다.

자동 연결: 서버와 수동으로 연결된 자격 증명이 없는 경우 검색 도구는 해당 서버의 자동 연결 메커니즘을 사용합니다. 이는 다음을 의미합니다.

- 각 컬렉션 라운드가 시작되면 검색 도구는 해당 서버에 사용할 수 있는 자격 증명 목록(OS 유형 기반)을 가져오고 "자동 연결 가능"으로 구성됩니다.
- 그런 다음 검색 도구는 루프의 서버에 대해 모든 자격 증명을 테스트합니다.

- 작동하는 자격 증명이 발견되면 서버의 컬렉션 라운드가 성공한 것입니다. 검색 도구는 이를 기억하고 다음 번에 먼저 시도합니다.
- 작동하는 자격 증명이 없으면 서버의 컬렉션 라운드가 실패한 것입니다.
 - 네트워크 모듈: 서버는 백오프 일정을 사용하여 각 장애 후 3분, 30분, 2시간 및 6시간 후에 다음 수집 라운드를 시작합니다(지수 백오프와 유사).
 - SQL Server 컬렉션: 검색 도구가 재시도하지 않습니다. 매일 서버당 한 번 시도합니다.

영향/위험:

시스템에서 위험이 완화되었다고 확신하는 경우에만 자동 연결을 사용합니다.

위험 1: 잘못된 여러 자격 증명에 자동 연결이 구성된 경우 서버에 대해 자동 시도하면 잠금 정책이 구성된 프로덕션 환경에 대한 계정 잠금이 트리거될 수 있습니다. 예를 들어 데이터 센터는 SSH 로그인 시도가 3번 실패한 후 VMs이 잠기도록 설정할 수 있습니다. 이 경우 3개의 잘못된 SSH 자격 증명에 대해 자동 연결이 구성된 경우 합법적인 계정 잠금이 발생합니다. 여러 시스템에서 잠금이 발생하면 중요한 비즈니스 프로세스에 영향을 주어 종속 시스템에서 계단식 장애가 발생할 수 있습니다. 또한 보안 운영 센터는 대량 인증 실패 이벤트로 인한 경고 폭풍을 겪어 리소스를 비우고 실제 공격을 마스킹하는 오탐 보안 인시던트를 생성할 수 있습니다.

위험 2: 검색 도구(검색 도구 암호 알고 있음)에 액세스할 수 있는 액터는 많은 수의 테스트 자격 증명을 구성하고 자동 연결을 사용하여 성공적인 자격 증명을 찾아 모든 서버에서 OS 자격 증명을 무차별 적용할 수 있습니다.

완화:

아래 지침을 따르세요.

- 검색 도구 암호가 제대로 보호되고 승인된 액터에게만 알려졌는지 확인합니다.
- 잠금 정책이 마련되어 있는 경우 환경에 적합한 자격 증명에 입력되었는지 확인합니다. 개별 VMs에 대한 운영 로드를 최소화하려면 계정 잠금 정책이 없는 경우에도 알려진 작동 자격 증명만 구성하는 것이 좋습니다.
- "자동 연결"은 옵트인 기능입니다. 계정 잠금이 환경에 문제가 되는 경우 이를 선택하지 말고 수동 자격 증명 할당을 사용합니다.

CSV 가져오기 보안

CSV 파일을 사용하여 서버를 가져올 때 다음과 같은 보안 영향을 고려합니다.

- CSV 파일에는 내부 서버의 호스트 이름 또는 IP 주소가 포함될 수 있습니다. 이를 민감한 데이터로 취급합니다.
- `os_credential_name` 및 `oracle_credential_name` 열은 미리 구성된 자격 증명을 표시 이름으로 참조합니다. CSV에는 보안 암호가 포함되어 있지 않습니다.
- All-or-nothing 검증: CSV의 행이 유효하지 않으면 전체 업로드가 거부됩니다. 이렇게 하면 혼란스러운 상태를 생성할 수 있는 부분 가져오기가 방지됩니다.
- 가져온 서버는 인벤토리에 즉시 표시되며 수집이 가능합니다. 가져오기 전에 OS 및 Oracle 자격 증명의 범위가 올바른지 확인합니다.

액세스 고려 사항 취소

액세스를 취소하면 삭제 범위가 특정 소스로 지정됩니다.

- vCenter 액세스를 취소하면 vCenter 데이터만 삭제됩니다. Hyper-V 또는 가져온 서버 데이터에는 영향을 주지 않습니다.
- Hyper-V 액세스를 취소하면 Hyper-V 데이터만 삭제됩니다. VMware 또는 가져온 서버 데이터에는 영향을 주지 않습니다.
- 가져온 서버를 삭제하면 인벤토리에서 제거되지만 다운스트림 컬렉션 데이터(네트워크, 데이터베이스, OS 지표)는 유지됩니다.
- 모든 소스별 인벤토리 데이터를 제거하려면 각 소스를 독립적으로 취소하거나 삭제해야 합니다. 다운스트림 수집 데이터(네트워크, 데이터베이스, OS 지표)는 모든 소스가 취소된 후에도 유지됩니다.

문제 해결

vCenter에 대한 검색 도구 연결 확인

VMware 모듈 구성 오류가 발생하면 다음 단계에 따라 연결을 확인합니다.

검색 도구 VM에 액세스

- 검색 도구 VM에 로그인하고 vCenter에서 원격 콘솔을 엽니다.
 - 사용자 이름: discovery
 - 암호: 암호

vCenter 연결 테스트

1. vCenter API 액세스 테스트:

```
curl -v --insecure -u <username>:<password> https://<vcenter-ip-or-hostname>:443/
mob
```

2. 예상 성공 결과:

```
[ec2-user@discoverytool ~]$ curl -v --insecure -u <user>:<password> https://vcsa/
mob > tmp.txt
% Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
           %             %             Dload  Upload  Total   Spent    Left   Speed
  0     0    0     0    0     0      0     0  --:--:-- --:--:-- --:--:--    0*
Trying 192.168.2.125:443...
* Connected to vcsa (192.168.2.125) port 443 (#0)
...
</xml>
* Connection #0 to host vcsa left intact
```

SSL 인증서 테스트

1. 다음 명령을 실행합니다.

```
openssl s_client -showcerts -servername <hostname> -connect <hostname>:443
```

2. 예상 성공 결과:

- vSphere 인증서 세부 정보를 표시해야 합니다.
- 포트 443에서 SSL/TLS 연결 확인

```
[ec2-user@discoverytool ~]$ openssl s_client -showcerts -servername vcsa -connect
vcsa:443
CONNECTED(00000003)
depth=0 CN = vcsa.onpremsim.env, C = US
verify error:num=20:unable to get local issuer certificate
verify return:1
depth=0 CN = vcsa.onpremsim.env, C = US
verify error:num=21:unable to verify the first certificate
verify return:1
```



```

---
Certificate chain
 0 s:/CN=vcsa.onpremsim.env/C=US
  i:/CN=CA/DC=vsphere/DC=local/C=US/ST=California/O=vcsa.onpremsim.env/OU=VMware
  Engineering
-----BEGIN CERTIFICATE-----
...
-----END CERTIFICATE-----
---
Server certificate
subject=/CN=vcsa.onpremsim.env/C=US
issuer=/CN=CA/DC=vsphere/DC=local/C=US/ST=California/O=vcsa.onpremsim.env/OU=VMware
  Engineering
---
```

WinRM 문제 해결

WinRM에 연결 문제가 발생하는 경우 다음 단계에 따라 연결을 테스트합니다. 이 단계는 검색 도구가 WinRM을 사용하여 Hyper-V 호스트와 통신하기 때문에 Hyper-V 연결 문제에도 적용됩니다.

포트 5985(HTTP) 및 5986(HTTPS)을 사용하여 기본 WinRM 연결을 테스트합니다. 포트 5986(HTTPS)에서 연결이 작동하는지 확인해야 합니다.

```

# Check WinRM listener configuration
winrm enumerate winrm/config/listener

# Note: Replace <HOST> with the target computer's hostname or IP address. Adjust the
  username and password as needed.
# Test WinRM connection on port 5985 (HTTP)
$cred = Get-Credential
Test-WSMan -Computer <HOST> -Authentication Negotiate -Credential $cred -Port 5985

# Test WinRM connection on port 5986 (HTTPS)
Test-WSMan -Computer <HOST> -Authentication Negotiate -Credential $cred -Port 5986
```

위의 테스트가 실패하면 인증서 검증이 비활성화된 상태에서 PowerShell 세션을 설정해 보세요.

```

$cred = Get-Credential
$so = New-PsSessionOption -SkipCACheck -SkipCNCheck -SkipRevocationCheck
Enter-PSSession -ComputerName <HOST> -Credential $cred -Port 5985 -SessionOption $so
```

Kerberos 문제 해결

Windows 서버에서 데이터를 수집할 때 Kerberos 인증 실패가 발생하는 경우 다음 섹션을 사용하여 일반적인 문제를 진단하고 해결합니다.

네트워크 요구 사항 확인

Kerberos 인증 문제를 해결하기 전에 검색 도구가 필요한 네트워크 엔드포인트에 도달할 수 있는지 확인합니다.

Kerberos의 네트워크 요구 사항을 확인하려면

1. 도메인 컨트롤러에 대한 DNS 확인을 확인합니다. 검색 도구 VM에서 다음 명령을 실행합니다.

```
nslookup dc01.example.com
```

또는 dig를 사용할 수 있습니다.

```
dig dc01.example.com
```

DNS 확인에 실패하면 Active Directory 도메인을 확인할 수 있는 DNS 서버를 사용하도록 검색 도구 VM이 구성되어 있는지 확인합니다. 네임서버 항목이 도메인 DNS 서버를 가리키는지 `/etc/resolv.conf` 확인하고 확인합니다.

2. 포트 88에서 키 배포 센터(KDC)에 대한 연결을 확인합니다. 다음 명령을 실행합니다.

```
nc -zv dc01.example.com 88
```

예상 결과:

```
Connection to dc01.example.com 88 port [tcp/kerberos] succeeded!
```

연결이 실패하면 검색 도구 VM에서 포트 88의 도메인 컨트롤러로의 트래픽을 차단하는 방화벽 규칙이 없는지 확인합니다.

3. WinRM 포트에서 대상 Windows 서버에 대한 연결을 확인합니다. 다음 명령을 실행합니다.

```
nc -zv <windows-server> 5985  
nc -zv <windows-server> 5986
```

연결이 실패하면 대상 서버에서 WinRM이 활성화되어 있고 방화벽 규칙이 포트 5985 및 5986에서 인바운드 트래픽을 허용하는지 확인합니다.

일반적인 Kerberos 문제

다음은 일반적인 Kerberos 문제와 해결 방법입니다.

대/소문자 구분 오류

증상: 인증 중에 "Server not found in Kerberos database" 오류가 발생합니다.

이 오류는 일반적으로 Kerberos 영역 이름이 대문자가 아닌 경우에 발생합니다. Kerberos 영역은 `krb5.conf` 파일의 대문자로 지정해야 합니다. 예를 들어 `example.com` 대신 `EXAMPLE.COM`을 사용하세요.

계정 잠금 방지

검색 도구는 백오프 메커니즘을 사용하여 계정 잠금이 반복적으로 실패한 인증 시도를 방지합니다. 서비스 계정이 잠긴 경우의 검색 도구 웹 UI를 통해 컬렉션 모듈을 중지한 다음 시작하여 컬렉션 프로세스를 재설정할 수 있습니다 `https://<discovery-tool-vm-ip>:5000`.

CLI에서 kinit 실패

다음 표에는 일반적인 kinit 오류와 해결 방법이 나와 있습니다.

오류	원인	솔루션
영역에 대한 KDC를 찾을 수 없음	KDC 호스트 이름 또는 IP 주소에 연결할 수 없거나 영역이 구성되어 있지 않습니다 <code>krb5.conf</code> .	<code>krb5.conf</code> 파일에 올바른 KDC 호스트 이름과 영역이 포함되어 있는지 확인합니다. 포트 88에서 KDC에 대한 DNS 확인 및 네트워크 연결을 확인합니다.
사전 인증 실패	서비스 계정의 암호가 잘못되었습니다.	암호를 확인하고 다시 시도하세요. 계정이 잠긴 경우 다시 시도하기 전에 Active Directory에서 잠금을 해제합니다.
Kerberos 데이터베이스에서 클라이언트를 찾을 수 없음	보안 주체 이름이 Active Directory의 계정과 일치하지 않습니다.	보안 주체 이름이 대소문자를 포함하여 계정 이름과 정확히 일치하는지 확인합니다.

오류	원인	솔루션
		인합니다. 영역을 대문자username@REALM 로 하여 형식을 사용합니다.
KDC의 네트워크 주소를 확인할 수 없음	DNS가 KDC 호스트 이름을 확인할 수 없습니다.	에서 DNS 구성을 확인합니다/etc/resolv.conf . DNS 서버가 KDC 호스트 이름을 확인할 수 있는지 확인합니다. nslookup 또는를 사용하여 테스트합니다dig.

성공적인 kinit에도 불구하고 수집 실패

가 kinit 성공했지만 데이터 수집이 여전히 실패하는 경우 다음을 확인합니다.

1. 수집에 사용되는 보안 주체 이름이에서 사용되는 사례와 kinit 정확히 일치하는지 확인합니다.
2. 서비스 계정에 대상 서버에 필요한 권한이 있는지 확인합니다.
3. 대상 서버에서 WinRM이 활성화되어 있는지 확인합니다.
4. 컬렉션에 사용되는 호스트 이름이 Active Directory에 등록된 호스트 이름과 일치하는지 확인합니다.

Kerberos는 일부 서버에서 작동하지만 다른 서버에서는 작동하지 않습니다.

일부 서버에서는 Kerberos 인증이 성공하지만 다른 서버에서는 실패하는 경우 다음 영역을 조사합니다.

서버가 여러 Active Directory 도메인에 걸쳐 있는 경우 각 도메인에 대해 별도의 Kerberos 자격 증명을 구성합니다. /etc/krb5.conf 파일에 모든 영역에 대한 항목이 포함되어 있는지 확인합니다. 각 도메인에는 올바른 username@REALM 보안 주체가 있는 자체 자격 증명が必要です.

작동 중인 서버의 WinRM 구성을 장애가 있는 서버와 비교합니다. 각 서버에서 다음 명령을 실행합니다.

```
winrm get winrm/config
```

원격 데스크톱과의 연결을 테스트하여 문제를 격리합니다. 검색 도구는 형식을 사용하는 username@DOMAIN반면 원격 데스크톱은 형식을 사용합니다DOMAIN\username.

서비스 계정이 장애가 발생한 서버의 로컬 관리자 그룹의 멤버인지 확인합니다. 대상 서버에서 다음 명령을 실행합니다.

```
net localgroup Administrators
```

WMI는 운영 체제 정보에 액세스하려면 로컬 관리자 권한이 필요합니다. SQL Server 컬렉션에서는 서비스 계정에 대상 서버에 대한 로컬 관리자 액세스 권한이 있어야 합니다.

Kerberos 구성 체크리스트

데이터 수집을 시작하기 전에 다음 체크리스트를 사용하여 Kerberos 구성을 확인합니다.

- krb5.conf 파일은 검색 도구 VM에 있습니다.
- 영역 이름은에서 대문자로 표시됩니다krb5.conf.
- 서비스 계정으로 kinit를 실행하면 오류 없이 성공합니다.
- 를 실행하면 유효하고 만료되지 않은 티켓이 klist 표시됩니다.
- 보안 주체 이름은 Active Directory 계정 이름과 정확히 일치합니다.
- DNS 확인은 KDC 호스트 이름에 대해 작동합니다.
- 포트 88에서 KDC에 대한 네트워크 연결이 확인됩니다.
- 포트 5985 및 5986의 대상 Windows 서버에 대한 네트워크 연결이 확인됩니다.
- (다중 도메인) 각 Active Directory 도메인에는 검색 도구에 자체 자격 증명이 구성되어 있으며 모든 도메인에 대한 [realms] 및 [domain_realm] 항목이 krb5.conf 포함되어 있습니다.

Oracle Database 문제 해결

누락된 데이터 또는 오류와 같은 Oracle Database 수집 문제를 진단하려면 다음을 확인하세요.

연결 거부 또는 제한 시간

증상: Oracle 컬렉션 상태에 서버의 연결 오류가 표시됩니다.

이 문제를 해결하려면 다음을 확인 하세요.

- Oracle 리스너가 대상 호스트에서 실행 중인지 확인합니다. `lsnrctl status`
- 검색 도구에서 포트 1521(또는 사용자 지정 포트)의 Oracle 호스트로의 네트워크 연결을 확인합니다. `nc -zv <oracle-host> 1521`
- 방화벽 규칙이 Oracle 리스너 포트에서 인바운드 연결을 허용하는지 확인합니다.

- Oracle 호스트 `lsnrctl services`에서를 실행하여 서비스 이름을 확인합니다. 서비스 이름이 올바르지 않으면 Oracle 리스너가 연결을 거부합니다.

인증 실패(ORA-01017)

증상: 잘못된 사용자 이름 또는 암호 오류로 인해 수집이 실패합니다.

이 문제를 해결하려면 다음을 확인 하세요.

- Oracle 서비스 계정이 존재하고 잠겨 있지 않은지 확인합니다. `SELECT account_status FROM dba_users WHERE username = 'DISCOVERY_USER';`
- 수동으로 연결하여 암호가 올바른지 확인합니다. `sqlplus discovery_user/<password>@<host>:1521/<service_name>`
- 계정이 잠긴 경우 잠금을 해제합니다. `ALTER USER discovery_user ACCOUNT UNLOCK;`

권한 부족(ORA-01031)

증상: 연결이 성공했지만 컬렉션이 불완전한 데이터를 반환합니다.

이 문제를 해결하려면 다음을 확인 하세요.

- `SELECT_CATALOG_ROLE`이 부여되었는지 확인합니다. `SELECT * FROM dba_role_privs WHERE grantee = 'DISCOVERY_USER';`
- 누락된 경우 필요한 역할을 부여합니다. `GRANT SELECT_CATALOG_ROLE TO discovery_user;`

수동 자격 증명에 오류가 표시되지만 자동 연결이 작동합니다.

자격 증명을 서버에 수동으로 고정하면 연결이 실패해도 검색 도구가 폴백되지 않습니다. 자격 증명에 구성한 포트 및 서비스 이름이 해당 특정 서버의 Oracle 리스너와 일치하는지 확인합니다. 서버에 비표준 포트 또는 서비스 이름이 있는 경우 그에 따라 자격 증명 구성을 업데이트합니다.

OS 수준 대체가 Oracle을 감지하지 못함

데이터베이스 자격 증명이 구성되지 않았고 OS 수준 대체가 Oracle을 감지하지 못하는 경우:

- SSH 또는 WinRM OS 자격 증명이 구성되어 있고 서버에서 작동하는지 확인합니다(OS 지표 수집 상태 확인).

- Linux 호스트의 경우가 /etc/oratab 존재하거나 Oracle 프로세스 모니터(pmon) 프로세스가 실행 중인지 확인합니다.
- Windows 호스트의 경우 Oracle 레지스트리 항목이 HKLM\SOFTWARE\Oracle 아래에 있거나 oracle.exe 프로세스가 실행 중인지 확인합니다.

SNMP 문제 해결

검색 도구 VM에 액세스

- 검색 도구 VM에 로그인하고 vCenter에서 원격 콘솔을 엽니다.
 - 사용자 이름: discovery
 - 암호: 암호

SNMP 도구 설치(필요한 경우)

- `sudo yum install net-snmp-utils -y`

Linux 서버에 대한 SNMP 연결 테스트

1. `snmptable -v 2c -c <COMMUNITY_STRING> <REMOTE_SERVER_IP> .1.3.6.1.2.1.6.13.1`
2. 예제:

```
#SNMPv2c:
snmptable -v 2c -c public 192.168.1.100 .1.3.6.1.2.1.6.13.1

#SNMPv3 (with authentication):
snmptable -v 3 -u <username> -a MD5 -A <auth_password>
192.168.1.100 .1.3.6.1.2.1.6.13.1

#SNMPv3 (with privacy):
snmptable -v 3 -u <username> -a MD5 -A <auth_password> -x DES -X <priv_password>
192.168.1.100 .1.3.6.1.2.1.6.13.1
```

네트워크 수집 오류

암호를 읽으려면 터미널이 필요합니다.

오류:

```
ss command failed on <host>: sudo: a terminal is required to read the password; either
use the -S option to read from standard input or configure an askpass helper sudo: a
password is required
```

ss 명령이 사용자 암호를 묻는 메시지를 표시합니다. 구성된 ssh 사용자는 sudoers 그룹에 있어야 하며 ss/netstat 명령에 대한 암호 없는 sudo로 구성되어야 합니다. 암호 없는 sudo를 구성하려면:

1. 새 sudoers 파일을 생성합니다.

```
sudo vi -f /etc/sudoers.d/<username>
```

2. 줄을 추가합니다.

```
<username> ALL=(ALL) NOPASSWD: /usr/sbin/ss, /usr/bin/netstat
```

3. 이 변경 후 암호를 입력하지 않고 `sudo ss -tnap` 및 `sudo netstat -tnap` 실행해야 합니다.

sudo 없이 실행된 네트워크 컬렉션

검색된 인벤토리 페이지에 다음 경고가 표시되는 경우:

```
Network collection ran without sudo. Process-level connection data may be missing.
```

이 경고는 SSH 사용자 계정에 대상 서버에 대한 sudo 액세스 권한이 없음을 나타냅니다. sudo가 없으면 검색 도구는 여전히 네트워크 연결 데이터를 수집할 수 있지만 각 연결을 소유하는 프로세스를 결정할 수는 없습니다. 전체 프로세스 수준 연결 데이터를 수집하려면 SSH 사용자에게 대상 서버에 대한 sudo 액세스 권한이 있는지 확인합니다.

OS 지표 수집 오류

Linux 서버용 서버 UUID 누락

검색 도구가 Linux 서버의 서버 UUID(비어 있거나 누락된 것으로 표시됨)를 수집할 수 없는 경우 해당 서버에 대해 구성된 SSH 자격 증명에 sudo 권한이 있는지 확인합니다. 이 도구는 dmidecode를 사용하여 서버 UUID를 읽습니다. dmidecode가 설치되지 않은 경우 도구는 읽기로 되돌아가 /sys/class/dmi/id/product_uuidsudo 액세스도 필요합니다. sudo가 없으면 두 메서드 모두 UUID를 검색할 수 없습니다.

해결 방법: 검색 도구에 제공된 SSH 사용자 계정에 대상 Linux 서버에 대한 sudo 액세스 권한이 있는지 확인합니다.

검색된 인벤토리의 액세스 문제

자격 증명 누락 또는 액세스 거부와 같은 메시지가 서버 컬렉션 상태에 표시되는 경우:

1. 검색된 서버 테이블에서 서버를 선택합니다.
2. 액세스 자격 증명 관리를 선택합니다. 다음을 선택할 수 있습니다.
 - a. 자격 증명 선택 드롭다운에서 대체 자격 증명을 선택합니다.
 - b. 새 자격 증명 사용을 선택하고 새 자격 증명을 제공합니다.
3. 저장을 클릭합니다.

변경 사항을 저장한 후 검색 도구가 연결을 다시 시도합니다.

SSH 키 인증 문제 해결

검색 도구에서 SSH 키 연결 테스트

SSH 키 인증이 실패하면 검색 도구에서 대상 서버로의 연결을 확인합니다.

1. 검색 도구에 로그인합니다(vSphere 콘솔 또는 SSH를 통해 Linux 호스트로).
2. 프라이빗 키를 사용하여 SSH 연결을 테스트합니다.

```
ssh -i /path/to/private_key -o StrictHostKeyChecking=no <username>@<target_ip>
```

3. 연결이 성공하면 키가 검색 도구에 업로드된 방식과 관련된 문제가 발생합니다. 키를 다시 업로드하고 사용자 이름이 일치하는지 확인합니다.

4. 연결이 실패하면 다음 표의 오류 메시지를 확인합니다.

오류 메시지	원인	해결 방법
Permission denied (publickey)	퍼블릭 키가 대상 서버의 <code>authorized_keys</code> 파일에 없거나 사용자 이름이 잘못되었습니다.	올바른 사용자의 대상 서버의 <code>~/.ssh/authorized_keys</code> 에 퍼블릭 키를 추가합니다. 파일 권한 확인: <code>chmod 700 ~/.ssh && chmod 600 ~/.ssh/authorized_keys</code> .
Connection timed out after 20s	검색 도구에서 포트 22에 연결할 수 없습니다.	검색 도구와 대상 서버 간에 포트 22가 열려 있는지 확인합니다. 방화벽 및 보안 그룹을 확인합니다.
Connection refused	SSH 서비스가 대상 서버에서 실행되고 있지 않습니다.	SSH 서비스 시작: <code>sudo systemctl start sshd</code> .
Invalid SSH key for credential ' <i>name</i> '	키 형식이 지원되지 않거나, 키 데이터가 손상되었거나, 암호가 누락되었거나 잘못되었습니다.	키 형식이 PEM, OpenSSH 또는 PKCS#8 형식의 RSA, ECDSA 또는 Ed25519인지 확인합니다. 키가 암호화된 경우 암호가 올바른지 확인합니다.

Linux 설치 관리자 문제 해결

포트 5000이 이미 사용 중입니다.

증상: 설치 후 검색 도구 서비스가 시작되지 않습니다.

해결 방법: 포트 5000을 사용하여 프로세스를 식별하고 중지합니다.

```
sudo ss -tlnp | grep :5000
```

충돌하는 프로세스를 중지한 다음 검색 도구를 다시 시작합니다.

```
sudo ./AWS-Transform-discovery-tool.sh start
```

일반적인 오류 메시지

이 표에서는 일반적인 오류 메시지와 해당 설명을 설명합니다.

메시지	Location	설명
암호가 이미 생성되었습니다.	암호 생성 페이지	두 사용자가 동시에 암호를 생성하는 레이스 조건, 새로 고침
내보내기 실패	인벤토리 페이지	로그 재시도 또는 전송
온디맨드 컬렉션이 이미 진행 중입니다.	인벤토리 페이지	두 사용자가 동시에 수동 수집을 시작하는 레이스 조건입니다. 현재 수동 수집이 완료된 후 다시 시도하세요.
Command timed out after 60s	서버 컬렉션 상태	대상 서버의 명령이 60초 이내에 완료되지 않았습니다. 이는 로드가 많은 서버에서 발생할 수 있습니다. 컬렉션을 다시 시도하거나 대상 서버의 로드를 조사합니다.
하나 이상의 자격 증명에 알 수 없는 UUIDs	OS 액세스 페이지	두 사용자가 OS 자격 증명을 동시에 편집하는 레이스 조건입니다. 다시 시도하세요.
잘못된 암호	로그인 페이지	로그인 암호가 잘못되었습니다. 관리자에게 문의하거나 문의하세요.
세션이 만료되었습니다. 다시 로그인하세요.	로그인 페이지	세션 시간이 초과되었습니다. 다시 로그인해야 합니다.
내부 오류가 발생했습니다.	다양한 페이지	로그 재시도 또는 전송

릴리스 노트

이 섹션에서는 릴리스 날짜별로 구성된 AWS Transform 검색 도구의 기능, 개선 사항 및 버그 수정에 대해 설명합니다.

Date	버전	릴리스 노트
2026년 6월 30일	1.0.1646	새로운 기능 • Oracle Database 검색을 추가했습니다. 이 도구는 CDB 및 PDB 토폴로지, 버전, 에디션, 설치된 옵션, 기능 사용량 및 구성 요소 인벤토리를 수집합니다. 검색 도구는 SSH 또는 WinRM을 통한 직접 SQL 연결(SELECT_CATALOG_ROLE 사용) 및 OS 수준 폴백 감지를 지원합니다. • 다양한 Active Directory 도메인에서 여러 Kerberos 자격 증명에 대한 지원이 추가되었습니다. 각 자격 증명은 독립적으로 인증되므로 인증 충돌 없이 여러 도메인의 Windows 서버에서 수집할 수 있습니다. 개선 사항 • 레거시 호스트에 대한 OS 지표 수집을 개선했습니다. 최신 명령을 사용할 수 없는 이전 운영 체제(RHEL 5, SLES 11, Windows Server 2008 R2)에 대한 폴백 데이터 수집이 추가되었습니다. 이제 스토리지, 성능 및 네트워크 인터페이스 데이터가 대체 시스템 인터페이스를 사용하여 수집됩니다. 버그 수정 • Hyper-V를 통해 검색된 서버의 Kerberos 인증 실패를 수정했습니다. 이제 검색 도구는 Kerberos SPN 일치에 필요한 Hyper-V 게스트 메타데이터에서 서버 호스트 이름(FQDN)을 올바르게 확인합니다.
2026년 5월 14일	1.0.1363	새로운 기능 • 지원되는 Linux 배포판(Amazon Linux 2, Amazon Linux 2023, RHEL 8–9, Rocky Linux 8–9, AlmaLinux 9, Ubuntu 20.04–24.04, Debian 10–12, SLES 15 SP5)에 검색 도구를 배포하기 위한 Linux 설치 관리자가 추가되었습니다. • vCenter 간에 자동 VM 중복 제거를 사용하여 여러 VMware vCenters 서버를 구성하기 위한 지원이 추가되었습니다.

Date	버전	릴리스 노트
		- Linux OS 액세스를 위한 사용자 이름 및 암호 대신 SSH 프라이빗 키 인증을 추가했습니다. 지원되는 키 형식에는 RSA, ECDSA, Ed25519, OpenSSH 및 PKCS#8이 포함됩니다. - 검색된 인벤토리에 없는 RFC 1918 프라이빗 IP 주소와의 연결을 캡처하는 프라이빗 주소 네트워크 컬렉션이 추가되었습니다. - 사용자 지정 날짜 범위를 선택하고 내보내기에 포함할 데이터 모듈을 선택하는 내보내기 옵션이 추가되었습니다. 개선 사항 - 수집기 일정에 시차를 두고 예약된 수집 신뢰성을 개선했습니다. - SSH 명령 일괄 처리를 통해 OS 지표 수집 성능을 개선했습니다. - 자격 증명 변경은 이제 이전에 실패한 서버를 즉시 재시도합니다. - OS 지표 수집은 이제 일부 명령이 빈 결과를 반환할 때 부분 상태를 보고합니다. - 대시보드의 vCenter 연결 문제에 대한 오류 가시성이 개선되었습니다.

Date	버전	릴리스 노트
2026년 4월 7 일	1.0.1074	새로운 기능 - 장애 조치 클러스터 중복 제거가 있는 Hyper-V 호스트에서 VMs 자동 검색을 포함하여 Microsoft Hyper-V 검색에 대한 지원이 추가되었습니다. - CSV 파일 업로드를 통한 서버 가져오기에 대한 지원이 추가되었습니다. - 서버 성능, 스토리지 성능, 서버 프로비저닝, 스토리지 프로비저닝, 네트워크 인터페이스, 실행 프로세스 등 6개의 독립 모듈이 포함된 OS 지표 컬렉션이 추가되었습니다. - VHD 이미지 파일을 사용하여 Hyper-V 배포 옵션을 추가했습니다. - EC2-specific 서비스를 제거하고 인스턴스 메타데이터 엔드포인트에 대한 액세스를 차단하여 온프레미스 보안 강화를 개선했습니다.
2026년 3월 26일	1.0.1014	버그 수정 및 개선 - Kerberos 도메인 대문자 검증을 백엔드에서 프론트엔드로 이동했습니다. - Python-kerberos에서 Python-pykerberos로 전환되고 파일 기반 캐시를 기본값으로 설정했습니다. - 대소문자를 구분하지 않는 대량 편집 서버 ID 검증을 수정했습니다. - ZIP 파일 이름 내보내기를 수정했습니다(현재 <code>discovery_tool_export.zip</code>). - 검사를 실행하는 서비스를 수정하고 시스템 자격 증명에 대한 디버그 로그를 추가했습니다. - 아티팩트를 빌드하기 위한 네트워크 구성 스크립트가 추가되었습니다.

Date	버전	릴리스 노트
2025년 12월 16일	1.0.718	새로운 기능 및 개선 사항 • 다운스트림 서비스에서 VM 중복을 방지하기 위한 SMBIOS UUID 지원이 추가되었습니다. • 향상된 리소스 모니터링을 위해 Min/Max/Avg 추적 및 확장된 스토리지 지표를 도입했습니다. • API 검증 개선 사항이 추가되었습니다. • 컨텍스트 지침이 포함된 도움말 패널 기능이 추가되었습니다. • 인터페이스 전체에서 용어를 "컬렉터"에서 "도구"로 업데이트했습니다.
2025년 10월 31일	1.0.0	최초 릴리스 AWS Transform 검색 도구의 초기 시작. 이번 릴리스에는 다음이 포함됩니다. • 오프라인 수집(AWS 계정 또는 Application Discovery Service에 대한 종속성 없음). • VMware 검색 및 모니터링. • SQL Server 데이터베이스 검색. • SSH, WMI 및 SNMP를 통한 Server-to-server 통신 컬렉션.

AWS 커넥터 변환

AWS 변환 커넥터를 사용하면 마이그레이션 및 현대화 워크플로를 위해 계정 경계 전반에 걸쳐 리소스에 안전하게 액세스할 수 있습니다. 이를 통해 계정 경계를 넘어 리소스에 액세스하고 관리하는 동시에 보안 제어 및 권한을 유지할 수 있습니다. 커넥터는 AWS 변환이 활성화된 소스 계정과 AWS 대상 계정 또는 타사 시스템의 외부 리소스 간의 연결을 나타냅니다.

커넥터에는 소스 커넥터의 액세스 요청과 대상 계정 소유자의 승인이 필요합니다. 소스 커넥터를 설정할 때 요청을 합니다. 마찬가지로 다른 계정이 계정에 액세스할 수 있도록 대상 커넥터를 승인하라는 요청을 받을 수 있습니다.

- 커넥터 생성: AWS 변환이 활성화된 소스 계정에서 커넥터를 생성하여 대상 계정과 필요한 권한을 지정합니다.
- 권한 설정: AWS 변환을 수행하려면 대상 계정의 특정 IAM 역할과 권한이 필요합니다. 여기에는 다음이 포함됩니다.
 - 를 사용하여 마이그레이션 데이터 관리 AWS KMS
 - 리전 간 API 직접 호출
 - VMware 서버에 복제 에이전트 설치
 - 네트워크 인프라(VPCs, 서브넷, 라우팅) 생성
 - Amazon EC2 인스턴스 시작 및 CloudFormation 스택 배포
 - Migration Hub를 통해 마이그레이션 워크플로 실행
- 승인 프로세스: AWS 변환이 리소스에 액세스할 수 있으려면 대상 커넥터 요청을 승인해야 합니다.
- 활성 연결: 커넥터를 승인하면 AWS 변환 작업이 대상 계정의 리소스에 안전하게 액세스하고 관리할 수 있습니다.

에이전트 작업에 대한 사용자 추적성

기본적으로는 AWS 리소스에 대한 에이전트 작업을 AWS 변환 서비스 자격 증명 아래에 AWS CloudTrail 기록합니다. 사용자 추적성은 작업을 시작하거나 상호 작용한 특정 AWS IAM Identity Center 사용자에게 이러한 작업을 속성화하여 개별 사용자 수준에서 보안 감사 및 인시던트 조사를 활성화합니다.

Note

사용자 추적성은 IAM Identity Center(IDC) 사용자에게만 지원됩니다.

사용자 추적성을 활성화하려면 AWS 변환 프로필 설정에서 백그라운드 세션을 활성화합니다. 활성화 되면 AWS Transform은 작업과 상호 작용할 때 IAM Identity Center [백그라운드 세션](#)을 자동으로 생성하고 이를 사용하여 커넥터 작업을 위한 ID 강화 IAM 역할 세션을 생성합니다. 이러한 세션은 다운스트림 AWS 서비스 호출 및 AWS CloudTrail 이벤트에 사용자 자격 증명을 포함합니다. 백그라운드 세션이 비활성화되면 AWS 변환은 사용자 자격 증명 컨텍스트 없이 표준 위임된 역할 세션으로 돌아갑니다.

새 커넥터는 사용자 추적성을 지원하도록 자동으로 구성됩니다. 기존 커넥터sts:SetContext의 경우 커넥터 역할의 신뢰 정책에 수동으로 추가해야 합니다.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": { "Service": ["transform.amazonaws.com"] },
      "Action": ["sts:AssumeRole", "sts:SetContext"],
      "Condition": {
        "StringEquals": { "aws:SourceAccount": "your-account-id" }
      }
    }
  ]
}
```

작업 페이지의 백그라운드 세션 탭에서 활성 백그라운드 세션을 보고 취소할 수 있습니다. 세션을 취소하면 세션과 세션에서 파생된 커넥터 세션이 즉시 무효화됩니다.

자세한 내용은 AWS IAM Identity Center 사용 설명서의 [신뢰할 수 있는 ID 전파 개요](#)를 참조하세요.

커넥터 관리

커넥터 페이지에서 다음을 확인할 수 있습니다.

- 소스 커넥터 탭: 다른 계정에 연결하기 위해 생성한 모든 커넥터를 나열하여 대상 계정 및 커넥터 상태를 표시합니다.

- 대상 커넥터 탭: 리소스에 액세스하려는 다른 계정의 수신 커넥터 요청을 표시하며 승인 또는 거부가 필요합니다.

AWS 변환은 활성 마이그레이션 워크플로를 방해할 수 있는 우발적인 변경을 방지하기 위해 커넥터 승인, 거부 또는 삭제와 같은 중요한 작업에 대한 확인이 필요합니다.

커넥터를 생성하려면

1. 소스 커넥터 탭으로 이동합니다.
2. 대상 계정 및 리소스 유형을 지정합니다.
3. 필요한 권한 및 액세스 범위를 구성합니다.

권한을 설정하려면

1. 필요한 권한이 있는 새 IAM 역할을 생성하도록 선택하거나
2. 커넥터에 대해 이전에 생성한 기존 역할을 선택합니다.
3. 역할에 AWS 변환 작업에 필요한 모든 권한이 있는지 확인합니다.

수신 요청을 관리하려면

1. 대상 커넥터 탭에서 커넥터 요청을 검토합니다.
2. 교차 계정 액세스를 활성화하기 위한 합법적인 요청을 승인합니다.
3. 무단 또는 불필요한 연결 시도를 거부합니다.

커넥터를 관리하려면

1. 활성 커넥터의 보안 및 규정 준수를 모니터링합니다.
2. 커넥터가 더 이상 필요하지 않으면 삭제합니다. 이로 인해 커넥터를 사용하여 작업을 실행하지 못할 수 있습니다.
3. 요구 사항이 변경되면 권한을 업데이트합니다.

마이그레이션(VMware 포함)

AWS 변환은 VMware, Hyper-V 및 기타 소스를 포함한 생성형 AI를 사용하여 가상 및 베어 메탈 서버 환경을 Amazon EC2로 마이그레이션하는 데 도움이 될 수 있습니다. 이 장에서는 마이그레이션 기능 AWS 변환과 마이그레이션 프로세스의 워크플로에 대한 개요를 제공합니다.

기능 및 주요 기능

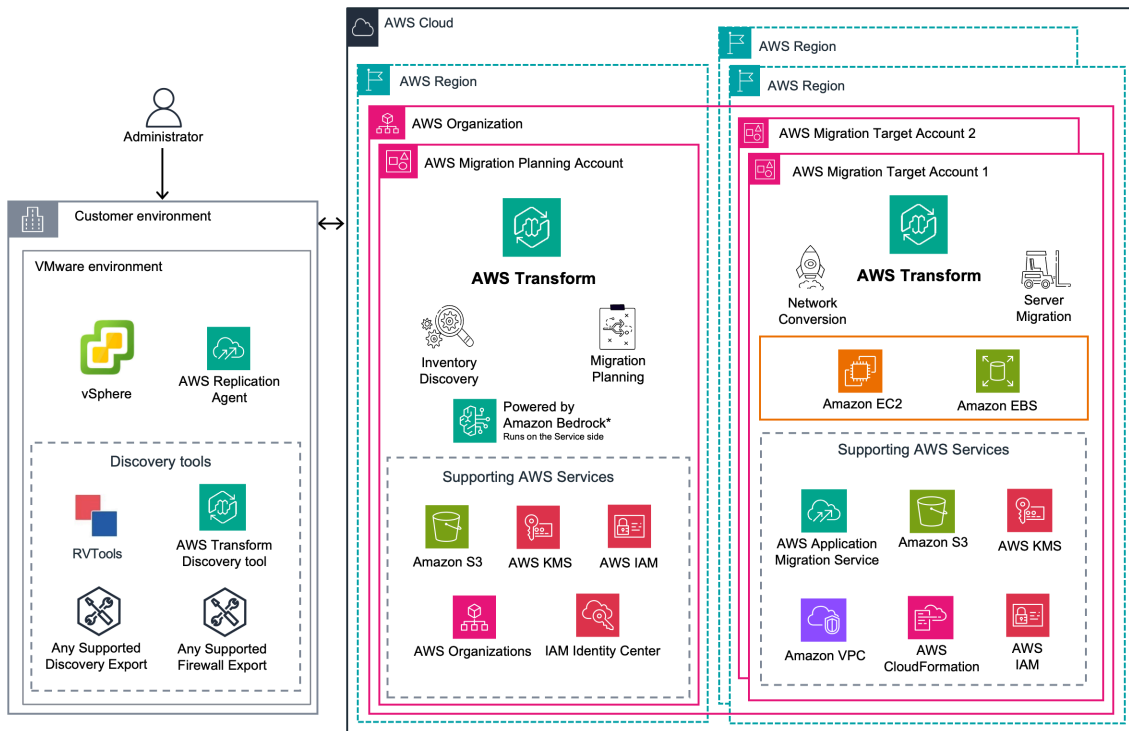
AWS 변환은 서버 환경을 로 마이그레이션하기 위한 다음과 같은 기능과 주요 기능을 제공합니다 AWS.

- 여러 검색 옵션:
 - 의 수집기를 사용하여 VMware 환경 검색을 지원했습니다 AWS Application Discovery Service.
 - 오픈 소스 [Export for vCenter](#) 도구(VMware 환경)를 사용합니다.
 - 독립적으로 수집된 검색 데이터 가져오기(모든 소스 환경).
- 소스 네트워크 구성을 Amazon VPC 네트워크 아키텍처로 AI 기반 변환.
- 애플리케이션 그룹화 및 제안된 마이그레이션 웨이브를 포함한 AI 기반 마이그레이션 계획 생성.
- Amazon EC2에서 기본적으로 실행되도록 서버를 리호스팅합니다.
- 로컬화된 웹 애플리케이션 인터페이스를 사용하면 원하는 언어로 마이그레이션할 때 AWS 변환을 사용할 수 있습니다. 자세한 내용은 [언어 설정](#) 단원을 참조하십시오.

AWS 변환은 지원되는 운영 체제의 Windows 및 Linux 서버 마이그레이션을 지원합니다. 지원되는 운영 체제의 전체 목록은 AWS Transform MGN 사용 설명서의 [지원되는 운영 체제](#)를 참조하세요.

AWS 마이그레이션 아키텍처 변환

이 다이어그램은 마이그레이션 아키텍처 AWS 변환에 대한 개요를 보여줍니다.



마이그레이션 작업

마이그레이션에 AWS 변환을 사용하려면 먼저 하나 이상의 변환 작업을 생성할 수 있는 논리적 컨테이너인 워크스페이스가 필요합니다. 이 주제의 섹션에서는 워크스페이스를 가져오는 방법과 워크스페이스에서 마이그레이션 작업을 생성하고 시작하는 방법을 설명합니다.

워크스페이스 가져오기

워크스페이스 가져오기에 대한 자세한 내용은 시작하기를 참조하세요.

사용하는 워크스페이스에 따라 변환 작업을 생성할 수 있는 AWS 리전이 결정됩니다. 작업이 AWS 리전 상주하는 위치입니다. 검색 데이터 및 AWS 변환 권장 사항도 여기에 포함됩니다. 다른 워크스페이스와 작업을 생성하려면 관리자에게 다른 워크스페이스를 생성하도록 AWS 리전 요청합니다. 지원되는에 대한 자세한 내용은 단원을 AWS 리전 참조하십시오. [지원되는 리전](#).

작업을 생성하고 검색 데이터 및 권장 사항을 저장할 수 있는 AWS 리전에는 AWS 변환 관리자가 결정하지만 마이그레이션 대상으로 다른 리전을 지정할 수 있습니다. 즉, 검색을 실행하고 한에서 AWS 변환 권장 사항을 수신한 다음 다른 리전에서 대상 환경을 생성할 수 있습니다. 이렇게 하면 데이터를 전송할 수 있습니다. 자세한 내용은 [the section called “대상 AWS 계정 및 리전 연결”](#) 단원을 참조하십시오.

작업 유형

AWS 변환은 마이그레이션 요구 사항에 따라 선택할 수 있는 다음과 같은 유형의 마이그레이션 작업을 제공합니다. 이러한 사전 설정 옵션 외에도 언제든지 작업에서 단계를 동적으로 추가하거나 제거하여 마이그레이션 워크플로를 사용자 지정할 수 있습니다.

End-to-end 마이그레이션

1. 검색 수행
2. 마이그레이션 계획 수립
3. 대상 계정 연결
4. 랜딩 존 구축
5. 네트워크 마이그레이션
6. 서버 마이그레이션

검색 및 마이그레이션 계획

1. 검색 수행
2. 마이그레이션 계획 수립

네트워크 마이그레이션

1. 대상 계정 연결
2. 네트워크 마이그레이션

랜딩 존

1. 대상 계정 연결
2. 랜딩 존 구축

랜딩 존, 네트워크 및 서버 마이그레이션

1. 대상 계정 연결
2. 랜딩 존 구축

3. 네트워크 마이그레이션
4. 서버 마이그레이션

마이그레이션 계획 및 서버 마이그레이션

검색, 웨이브 플랜 및 리호스팅이 포함됩니다.

1. 검색 수행
2. 마이그레이션 계획 수립
3. 대상 계정 연결
4. 서버 마이그레이션

작업 생성 및 시작

마이그레이션 프로젝트의 첫 번째 단계는 AWS 변환 작업을 생성하는 것입니다. 마이그레이션 프로젝트의 경우 목표에 따라 다른 작업 유형을 선택할 수 있습니다. 다음 절차에서는 모든 유형의 새 마이그레이션 작업을 생성하고 시작하는 방법을 설명합니다. 다양한 작업 유형에 대한 자세한 내용은 섹션을 참조하세요 [the section called “작업 유형”](#).

새 마이그레이션 작업을 생성하고 시작하려면

1. 워크스페이스 랜딩 페이지에서 작업 생성을 선택합니다.
2. 마이그레이션 옵션을 선택한 다음 생성할 마이그레이션 작업 유형을 지정합니다. 각 마이그레이션 작업 유형에 포함된 단계에 대한 자세한 내용은 섹션을 참조하세요 [the section called “작업 유형”](#).
3. 모든 채팅 질문에 답한 후 작업 생성을 선택합니다.

워크스페이스 요약 보고서 다운로드

마이그레이션 중에 언제든지 워크스페이스 요약 보고서를 다운로드 가능한 PDF로 생성할 수 있습니다. 이 보고서는 작업 상태 및 현재 워크플로 단계, 사용자 작업 및 승인, 웨이브 계획 세부 정보, 네트워크 마이그레이션 토폴로지, 랜딩 존 구성, 리호스팅 진행 상황, 컨테이너화 결정, 생성된 주요 아티팩트를 포함하여 워크스페이스의 모든 마이그레이션 작업에 대한 통합 보기를 제공합니다. 보고서를 생성하려면 채팅의 에이전트에게 "모든 작업의 마이그레이션 진행 상황에 대한 워크스페이스 요약 제공"과 같은 워크스페이스 요약을 요청합니다. 에이전트는 모든 작업의 데이터를 컴파일하고 채팅에서 직접

PDF를 다운로드 가능한 파일로 전송합니다. 이 보고서를 사용하여 전체 마이그레이션 진행 상황을 추적하거나 이해관계자와 상태를 공유할 수 있습니다.

제한 사항

AWS 변환에는 다음과 같은 제한 사항이 있습니다.

- 실행 중인 마이그레이션 작업을 중지한 다음 에이전트에게 다시 시작하도록 요청하면 작업이 처음부터 다시 시작되고 작업 진행 상황이 손실됩니다. 그러나 작업을 다시 시작하기 전에 작업에서 생성된 아티팩트는 계속 사용할 수 있습니다.
- 마이그레이션 작업 AWS 리전 당 하나의 대상을 지정할 수 있습니다. 애플리케이션을 다른 대상 리전으로 마이그레이션하려면 여러 마이그레이션 작업을 생성합니다.
- 다중 계정 마이그레이션 - 단일 리전만 해당 - 단일 내에서 여러 계정으로 마이그레이션할 수 있습니다. 다 AWS 리전. 다중 리전 마이그레이션의 경우 각 대상 리전에 대해 별도의 프로젝트를 생성해야 합니다.
- 다중 계정 마이그레이션 - 웨이브당 하나의 계정 - 각 마이그레이션 웨이브는 하나의 계정만 대상으로 할 수 있습니다. 서로 다른 대상 계정이 필요한 애플리케이션은 별도의 웨이브에 배치해야 합니다.
- 다중 계정 마이그레이션 - AWS 조직 필요 - 모든 대상 계정은 AWS 조직의 일부여야 합니다.

소스 데이터 검색

온프레미스 데이터를 검색하고 수집하려면 [AWS 변환 검색 도구](#), AWS마이그레이션 평가기 수집기를 사용하거나 RVTools 및 ModelizeIT에서 내보내기를 업로드하고 Cloudamize와 같은 도구에서 생성된 AWS마이그레이션 포트폴리오 평가(MPA) 형식 내보내기를 사용할 수 있습니다. AWS 변환은 AWS 변환 검색 도구 내보내기를 ZIP 파일 형식의 CSV 및 JSON 파일로 처리하고, RVTools 내보내기를 Excel 파일 또는 CSV 파일이 포함된 ZIP 파일로 처리하고, ModelizeIT CSV 내보내기를 ZIP 파일로 처리할 수 있습니다. 각 데이터 소스에 대해 AWS 변환은 기본 서버 파일을 개별적으로 수락합니다. 그러나 연결과 같은 보조 파일은 서버 파일이 있는 ZIP 파일 또는 서버 시트가 있는 Excel 파일에 포함된 경우에만 처리됩니다.

데이터 완전성과 정확성을 보장하기 위해 업로드하기 전에 사용 가능한 가장 상세한 데이터를 업로드하고 내보내기 파일을 검토하는 것이 좋습니다. 업로드에 필요한 모든 파일이 포함되어 있는지 확인하고 데이터가 현재 환경 상태를 반영하는지 확인합니다. 이 예비 검토는 재업로드 필요성을 최소화하고 AWS Transform이 온프레미스 환경을 더 정확하게 캡처하고 애플리케이션 그룹화 및 웨이브 계획을 포함한 마이그레이션 계획을 더 잘 지원할 수 있도록 합니다. 더 나은 데이터를 얻으면서 데이터를 점진적으로 추가할 수도 있습니다.

AWS 변환은 파일 형식 및 구조를 자동으로 감지하고, 구조화된 엔터티 레코드를 구문 분석 및 추출하고, 여러 파일에서 중복을 제거하고, 데이터 품질을 검증하고, 문제를 보고한 다음, 다운스트림 마이그레이션 계획을 위한 요약을 준비합니다.

온프레미스 데이터를 공유하고 확인한 후 작업 계획에서 온프레미스 데이터 검색을 확장하고 인벤토리 준비 상태 요약을 선택하여 검색 데이터를 검토할 수 있습니다. 또한 업로드한 데이터에 대해 질문하여 AWS 변환이 모든 것을 올바르게 수집했는지 확인하거나 데이터 처리의 실수를 식별하고 수정할 수 있습니다. 예를 들어 운영 체제 및 버전에 대해 질문할 수 있습니다. 실수를 수정해야 하는 경우 사용한 검색 도구에서 인벤토리 데이터를 다시 업로드하면 AWS 변환이 업데이트된 레코드를 자동으로 처리, 중복 제거 및 병합합니다. 해당 인벤토리 데이터를 더 이상 사용하지 않으려면 이전에 업로드한 파일을 제거할 수도 있습니다.

마이그레이션 계획 수립

VMware용 AWS 변환 내의 마이그레이션 계획 작업 단계는 대규모 마이그레이션을 계획하기 위한 협업 채팅 기반 경험입니다. AWS 변환 에이전트는 AWS 권장 지침을 적용하여 고객이 온프레미스 데이터를 분석하는 것부터 완료된 마이그레이션 웨이브 계획에 이르기까지 안내합니다.

온프레미스 데이터 검색 작업이 성공적으로 완료되면 AWS 변환은 검색 데이터를 사용하여 애플리케이션을 마이그레이션 웨이브로 그룹화합니다. AWS 변환은 서버를 분석하고 범위를 지정하고, 이를 애플리케이션으로 그룹화하고, 이동 그룹을 생성하고, 마이그레이션 웨이브를 빌드하는 단계를 안내합니다. 온프레미스 환경을 분석할 때 질문을 통해 AWS Transform이 서버 종속성 및 네트워크 아키텍처와 같이 설치된 소프트웨어를 분석한 방법을 더 잘 이해할 수 있습니다.

AWS 변환은 애플리케이션 그룹 및 웨이브 내에서 범위 조정을 지원합니다. 언제든지 검색 데이터를 다시 업로드할 수 있으며, AWS 변환은 새 레코드를 자동으로 처리, 중복 제거 및 기존 데이터와 병합합니다. 새로 발견된 종속성 또는 인프라 추가와 같은 변경 사항이 감지되면 AWS 변환은 영향을 받는 종속성 그룹에 플래그를 지정하고 웨이브 플랜 조정에 대한 권장 사항을 제공합니다. 마이그레이션 계획은 비정형 텍스트 데이터를 사용하여 계획 프로세스를 강화할 수도 있습니다.

마이그레이션 계획 단계에는 네 가지가 있습니다.

- 범위 및 분석에서 검색 데이터를 검토하고, 소프트웨어 및 네트워크 환경에 대해 질문하고, 마이그레이션 범위의 리소스를 확인할 수 있습니다.
- 그룹 앱에서는 예를 들어 호스트 이름 분석, 네트워크 종속성 및 비즈니스 규칙과 관련된 비즈니스 및 기술 규칙의 조합을 제공하여 마이그레이션 계획을 통해 인프라를 애플리케이션으로 그룹화할 수 있습니다. 이미 애플리케이션 인벤토리가 있는 경우 마이그레이션 계획에서 이를 대신 사용할 수 있습니다.

- 이동 그룹 생성에서 마이그레이션 계획에 기술 및 비즈니스 요구 사항을 제공하여 함께 이동해야 하는 애플리케이션을 결정할 수 있습니다. 기술 종속성에는 데이터베이스, 메시지 대기열 또는 여러 앱 간에 공유되는 기타 리소스가 포함됩니다. 비즈니스 및 운영 종속성에는 비즈니스 중요도, RPO 및 RTO, 데이터 센터 위치, 애플리케이션 소유자가 포함됩니다.
- 마지막으로 빌드 웨이브에서 타임라인 및 우선순위에 대한 마이그레이션 계획 컨텍스트를 제공하여 마이그레이션할 수 있는 웨이브 계획을 구축할 수 있습니다. 우선 순위 점수, 이동 그룹 크기, 사용자 수, 애플리케이션 복잡성과 같은 요인을 기반으로 웨이브에 포함할 이동 그룹을 선택할 수 있습니다.

마이그레이션 계획 용어:

- 마이그레이션 웨이브는 함께 마이그레이션되는 논리적 그룹입니다. 마이그레이션 웨이브는 하나 이상의 이동 그룹으로 구성됩니다.
- 이동 그룹은 함께 이동해야 하는 공동 종속 애플리케이션 세트입니다. 공유 데이터베이스와 같은 기술 종속성이 있거나 공유 비즈니스 기능 지원과 같은 비즈니스 종속성이 있을 수 있습니다.
- 종속성은 시스템 간의 관계입니다. 종속성에는 다음과 같은 몇 가지 유형이 있습니다.
 - 시스템이 종속성 없이 작동할 수 없는 중요 종속성 또는 하드 종속성입니다. 일반적인 예로는 데이터베이스, 다른 애플리케이션 또는 서비스에 의존하는 애플리케이션이 있습니다.
 - 시스템 작동에 중요하지 않은 소프트 종속성입니다. 일반적인 예로는 독립적으로 마이그레이션할 수 있는 지연 시간에 민감하지 않은 종속성이 있습니다.
 - 비기술 종속성에는 비즈니스, 조직, 운영 및 규정 준수 종속성이 포함됩니다. 이는 조직 및 우선순위와 관련된 종속성입니다. 여기에는 공유 비즈니스 기능 및 조직 소유권이 포함됩니다.

워크플로

마이그레이션 계획은 대화형의 반복 워크플로입니다. 언제든지 돌아가서 이전 단계를 변경할 수 있습니다. 일반적인 마이그레이션 계획 워크플로는 다음과 같습니다.

1. 마이그레이션 계획은 사용 가능한 검색 데이터를 요약하는 것부터 시작합니다. 사용 가능한 데이터를 검토하고 언제든지 검색 단계로 돌아가 추가 데이터를 제공합니다.
2. 범위 지정 및 분석 단계 내에서 온프레미스 환경에 대해 질문하여 수집한 데이터를 검증할 수 있습니다. 예제 질문은 다음과 같습니다.
 - a. 운영 체제별로 내 서버 나열
 - b. 온프레미스 네트워크 토폴로지 요약
 - c. 내 환경에서 실행되는 가장 일반적인 기술을 나열합니다.

3. 환경을 분석하는 동안 마이그레이션 범위에 속하지 않아야 하는 서버를 식별하는 경우 AWS 변환에 해당 리소스를 제외하도록 지시할 수 있습니다. 예를 들면 다음과 같습니다.
 - a. 호스트 이름에 레거시가 있는 모든 서버 제거
 - b. 10.0.2.0/24 서브넷의 모든 서버 제거
 - c. 2022년 이전 버전의 Windows를 실행하는 모든 서버 제거
4. 환경을 충분히 탐색하고 마이그레이션 범위를 결정한 후에는 AWS 변환에 다음 마이그레이션 계획 단계로 이동하도록 지시할 수 있습니다.
5. 다음 단계는 애플리케이션 그룹화입니다. 서버에 이미 애플리케이션에 매핑되어 있는 경우 AWS 변환에 해당 매핑을 사용하도록 지시하고이 단계를 건너뛸 수 있습니다. 애플리케이션이 미리 정의되어 있지 않은 경우 애플리케이션을 정의하는 기술 및 비즈니스 로직을 제공할 수 있습니다. AWS 변환은 애플리케이션 그룹화 프로세스를 안내하고 서버를 애플리케이션으로 효과적으로 그룹화하기 위해 제공할 수 있는 데이터 포인트를 제안합니다. 온프레미스 애플리케이션에 대해 더 많은 정보를 제공할수록 AWS 변환이 서버를 앱으로 그룹화할 수 있습니다. 충분한 정보를 제공했으면 AWS 변환에 애플리케이션 그룹화를 수행하도록 지시할 수 있습니다.
6. 애플리케이션 그룹화가 수행되면 애플리케이션 그룹을 검토합니다. AWS 변환에 필요한 변경을 지시할 수 있습니다. 예를 들면 다음과 같습니다.
 - a. 서버 example-server를 application-5로 이동
 - b. application-5 "HR 앱 테스트 환경" 이름 바꾸기
 - c. IIS Dev Farm에서 모든 Linux 서버 제거
7. 앱이 그룹화되면 AWS 변환에 다음 단계로 이동하도록 지시합니다.
8. 다음 단계는 그룹화 이동입니다. 이동 그룹화 단계에서는 함께 이동해야 하는 애플리케이션을 식별합니다. 기술 및 비기술 종속성에 대한 컨텍스트를 제공합니다. AWS 변환은 프로세스를 안내하고 앱을 함께 그룹화하기 위해 제공할 수 있는 데이터 포인트를 제안합니다. 이 단계에서 고려해야 할 몇 가지 사항은 다음과 같습니다.
 - a. 이동 그룹의 대상 크기는 얼마여야 합니까?
 - b. 각 앱에 대해 개발, 테스트 및 생산과 같은 환경을 결합하거나 분할하시겠습니까?
 - c. 네트워크 종속성을 어떻게 고려하시겠습니까? 모든 종속성이 중요합니까? 아니면 일부 종속성이 소프트웨어 종속성으로 간주되어 이동 그룹 간에 분할될 수 있습니까?
9. 이동 그룹화 규칙을 제공했으면 AWS 변환에 이동 그룹화 전략을 실행하도록 지시합니다. 그런 다음 이동 그룹을 검토하고 수정할 수 있습니다. 이동 그룹을 검토한 후에는 AWS 변환에 최종 마이그레이션 계획 단계로 이동하도록 지시할 수 있습니다.
10. 웨이브 계획은 마이그레이션 계획의 마지막 단계입니다. 이 단계에서는 이동 그룹을 마이그레이션 웨이브로 그룹화하고 해당 웨이브의 우선순위를 지정합니다. 웨이브 계획 단계에서 AWS 혁신은 이

동 그룹을 웨이브로 그룹화한 다음 해당 웨이브의 우선 순위를 지정하는 데 필요한 비즈니스 우선 순위를 제공하는 과정을 안내합니다. 웨이브 계획의 고려 사항은 다음과 같습니다.

- a. 각 이동 그룹의 비즈니스 중요도
- b. 각 이동 그룹의 마이그레이션 타임라인 및 타임라인
- c. 각 이동 그룹과 관련된 위험
- d. 웨이브당 마이그레이션할 서버 수

11. 웨이브로 그룹화하는 방법에 대한 충분한 지침을 제공했으면 웨이브 계획을 실행하도록 AWS 변환에 지시합니다. 그런 다음 웨이브를 검토하고 수정할 수 있습니다.

12. 웨이브 플랜을 완료한 후에는 마이그레이션 계획을 완료하고 실행으로 이동할 수 있습니다. 언제든지 마이그레이션 계획으로 돌아가 계획을 구체화하고 반복할 수 있습니다.

13. 각 웨이브에 대해 리호스팅(서버를 Amazon EC2로 마이그레이션) 및 컨테이너화(소스 코드를 컨테이너화하고 Amazon Elastic Container Service 또는 Amazon Elastic Kubernetes Service에 배포)와 같은 마이그레이션 전략을 할당할 수 있습니다. 전략 컨테이너화에 웨이브를 할당하면 AWS Transform은 마이그레이션 실행 중에 해당 웨이브에 대한 소스 코드 컨테이너화 워크플로를 실행합니다. 자세한 내용은 [소스 코드 컨테이너화](#) 단원을 참조하십시오. 7Rs 프레임워크에서 권장 AWS 전략을 할당하기 전에 가져오려면 섹션을 참조하세요 [the section called “7Rs 권장 사항”](#).

마이그레이션 전략(7R) 권장 사항

마이그레이션 계획 중에 AWS Transform은 검색된 인벤토리를 분석하고 모든 서버 및 애플리케이션에 대해 업계 표준 7Rs 중 하나인 마이그레이션 전략을 추천할 수 있습니다. 각 권장 사항에는 제안된 AWS 대상 서비스, 신뢰도 점수 및 그 근거가 포함됩니다. 이를 통해 웨이브 플랜의 방어 가능한 출발점을 제공하고 그렇지 않으면 놓칠 수 있는 현대화 기회를 표면화할 수 있습니다.

7가지 전략은 리호스팅, 리플랫폼, 리팩터링, 리구매, 사용 중지, 보존 및 재배포입니다. AWS는 운영 체제, 사용률 및 워크로드 유형과 같은 데이터의 읽기 신호를 변환하여 설명 가능한 권장 사항을 제시합니다. 예를 들어 유헴 또는 end-of-life 서버를 사용 중지하고, SQL Server 또는 오픈 소스 데이터베이스를 Amazon RDS로 이동하고, 이메일 및 협업 워크로드를 Microsoft 365로 이동하고, 특수 레거시 시스템을 유지하고, Amazon EC2에서 나머지 워크로드를 리호스팅하는 것이 좋습니다. 권장 사항은 전략 및 웨이브 레벨 요약별 중요도 보기를 통해 개별 서버에서 애플리케이션으로, 그리고 전체 포트폴리오로 롤업됩니다.

마이그레이션 전략(7R) 보고서를 생성하려면:

1. 온프레미스 데이터 검색 단계를 완료하고 서버를 애플리케이션으로 그룹화합니다. AWS 변환이 서버별 및 애플리케이션별 권장 사항을 제공할 수 있으려면 둘 다 필요합니다.

2. 마이그레이션 계획 채팅에서 AWS 변환에 마이그레이션 전략(7R) 보고서, 예를 들어 R 전략 보고서 생성을 요청합니다. 애플리케이션 그룹화가 완료되면 AWS 변환은 에도 보고서를 생성하도록 제안합니다.
3. AWS 변환은 인벤토리를 분석하고, 7Rs를 적용하고, 보고서를 생성합니다. 조직 이름 및 필터와 같은 세부 정보를 제공하여 분석 범위를 지정할 수 있습니다.
4. 권장 사항을 검토합니다. 권장 사항을 조정하려면 채팅에서 AWS 변환에 지시하여 단일 서버 또는 애플리케이션을 변경하거나 변경 사항을 대량으로 적용합니다(예: 운영 체제, 환경, 웨이브 또는 우선 순위). AWS 변환은 보고서를 변경 사항으로 업데이트합니다.

기본적으로 AWS 변환은 필터링하고 탐색할 수 있는 대화형 HTML 대시보드를 생성합니다. 요청 시 이해관계자와 공유할 PDF 문서 또는 Microsoft PowerPoint(PPTX) 슬라이드 데크를 생성할 수도 있습니다. PDF 및 PowerPoint 출력은 동일한 분석의 point-in-time 스냅샷입니다. 보고서에는 모든 서버 및 애플리케이션에 대한 권장 전략 및 AWS 대상 서비스, 신뢰도 점수 및 추론, 강조 표시된 현대화 기회, 전략별 중요도 보기, 웨이브 레벨 요약 및 위험 플래그가 포함되어 있습니다.

이 보고서에서 권장하는 전략은 웨이브 계획 중에 할당하는 웨이브별 전략을 보완합니다. 소스 코드 컨테이너화는 섹션을 참조하세요 [소스 코드 컨테이너화](#).

다이어그램 작성 및 보고

마이그레이션 계획 중에 AWS 변환은 검색된 인벤토리 및 계획 결과를 시각적 다이어그램 및 분석 보고서로 변환합니다. "네트워크 토폴로지 다이어그램 표시" 또는 "리스크 보고서 생성"과 같이 계획 채팅에서 대화식으로 생성합니다. AWS 변환은 설정 없이 이미 제공한 데이터에서 빌드합니다.

다이어그램은 대화형이며 환경을 시각적으로 탐색할 수 있습니다. 사용 가능한 다이어그램은 다음과 같습니다.

- 네트워크 토폴로지 - 수천 개의 노드로 구성된 대규모 환경으로 확장하도록 설계된 서버 및 네트워크 관계의 대화형 맵입니다.
- 애플리케이션 종속성 - 관찰된 네트워크 연결에서 파생된 application-to-application 관계를 지시합니다.
- Wave Gantt 차트 - 일정, 종속성, 마일스톤 및 진행 상황(파도 계획 후 사용 가능)을 보여주는 마이그레이션 파도의 타임라인 보기입니다.
- 일반 차트 - 선택한 데이터 차원에 대한 파이형 차트, 막대형 차트, 히스토그램, 트리맵 및 요약 테이블입니다.

보고서는 마이그레이션 데이터에 대한 서술 분석 및 권장 사항을 제공합니다. 사용 가능한 보고서에는 다음이 포함됩니다.

- 위험 평가 - 애플리케이션별, 웨이브별 및 포트폴리오 전체 요약과 함께 기술적 복잡성, 종속성 위험, 마이그레이션 준비 상태 및 운영 위험 전반에 걸쳐 각 애플리케이션을 평가합니다.
- 마이그레이션 전략(7R) - 서버별 및 애플리케이션별 전략 권장 사항입니다. 자세한 내용은 [the section called “7Rs 권장 사항”](#) 단원을 참조하십시오.
- 일반 및 사용자 지정 보고서 - 실행 준비 요약, cost-versus-risk층, 컨테이너화 후보 평가와 같은 요청에 대한 분석 보고서입니다.

일부 출력은 계획 단계에 따라 달라집니다. 예를 들어 애플리케이션 종속성 다이어그램은 네트워크 연결 데이터를 사용합니다. 웨이브 계획 완료 후 웨이브 Gantt 차트 및 웨이브 수준 보고서 요약을 사용할 수 있습니다. 사전 조건이 누락된 경우 AWS 변환은 필요한 사항을 알려주고 먼저 필요한 단계를 실행할 수 있습니다.

AWS 변환은 다이어그램을 필터링하고 탐색할 수 있는 대화형 HTML로 제공합니다. 기본적으로 AWS 변환은 보고서를 독립형 HTML 파일로 전송합니다. 요청 시 AWS 변환은 이해관계자와 공유할 PDF 문서 또는 제공할 Microsoft PowerPoint(PPTX) 슬라이드 데크도 생성할 수 있습니다. PDF 및 PowerPoint 출력은 동일한 분석의 point-in-time 스냅샷입니다.

대상 AWS 계정 및 리전 연결

네트워크 마이그레이션, 랜딩 존 빌드 및 서버 마이그레이션을 위해 대상 AWS 계정 커넥터를 구성합니다. 여기에는 마이그레이션 유형 선택, MAP 계약 세부 정보 제공(해당하는 경우), 커넥터 설정의 세 단계가 포함됩니다. 이러한 설정은 네트워크 마이그레이션, 랜딩 존, 서버 리호스팅 등 모든 마이그레이션 단계에 적용됩니다.

1단계: 마이그레이션 유형 선택

단일 계정 마이그레이션을 수행할지 아니면 다중 계정 마이그레이션을 수행할지 선택합니다.

- 단일 계정 마이그레이션 - 모든 워크로드가 하나의 대상으로 마이그레이션됩니다. AWS 계정. 커넥터 대상 계정과 대상 계정은 동일합니다.
- 다중 계정 마이그레이션 - 워크로드가 다른 대상 계정으로 마이그레이션됩니다. 커넥터는 조직 관리 계정 또는 및 CloudFormation StackSets 모두에 AWS Transform MGN 등록된 위임된 관리자(DA) 계정에 연결되어야 합니다.

2단계: MAP 계약

마이그레이션이 AWS 마이그레이션 가속화 프로그램(MAP 2.0)의 일부인 경우 마이그레이션 포트폴리오 경험(MPE) ID를 제공합니다. 이 ID는 대문자와 숫자(예: ABCDE12345)를 사용하는 10자 코드입니다. MPE ID를 제공하면 네트워크 마이그레이션, 랜딩 존 및 서버 리호스팅 단계에서 생성된 모든 리소스에 MAP 태그가 적용됩니다. 태그 형식은 다음과 같습니다.

- 키: map-migrated 값: migMPE_ID

MAP 크레딧을 받으려면 MAP 태그를 적용해야 합니다. MAP에 대한 자세한 내용은 [AWS 마이그레이션 가속화 프로그램을 참조하세요](#).

3단계: 커넥터 구성

대상 계정 커넥터를 사용하여 마이그레이션 후 워크로드가 상주할 AWS 환경에 마이그레이션 작업을 연결합니다. 시작하기 전에 대상에 마이그레이션된 인프라를 지원하는 데 필요한 권한, 할당량 및 구성 AWS 계정 이 있는지 확인합니다.

커넥터 요청을 승인할 때 다음에 AWS 변환 권한을 부여합니다.

- Migration Hub 및 AWS Application Migration Service(MGN)에 대한 액세스 권한과 함께 VMware 마이그레이션을 위한 Amazon S3 버킷 작업(읽기/쓰기)을 관리합니다. 여기에는 다음 항목에 대한 권한이 포함되며, 모두 CreatedBy:AWSTransform 또는 로 태그가 지정된 대상 계정 내의 리소스로 제한됩니다. CreatedFor:AWSTransform
 - 마이그레이션 웨이브를 관리합니다.
 - 네트워크 구성(Amazon EC2, VPC, Transit Gateway, Direct Connect, 로드 밸런서, Network Firewall)을 관리합니다.
 - CloudFormation 스택 배포를 관리합니다.
 - Systems Manager를 통해 자동 에이전트 설치를 수행합니다.
- 검색 리전에 저장된 정보를 사용하여 온프레미스 워크로드를 대상 AWS 계정 및 리전으로 마이그레이션합니다.
- 대상 및 리전에서 랜딩 존 인프라를 프로비저닝 AWS 계정 하고 관리합니다. 여기에는 해당하는 CreatedBy:AWSTransform 경우 태그가 지정된 리소스로 제한된 다음 항목에 대한 권한이 포함됩니다.
 - 로 시작하는 버킷에 대해 Amazon S3 버킷 작업(생성, 읽기, 쓰기, 삭제)을 수행합니다.
 - 다transform-vmware-landing-zone-.

- CloudFormation 스택 배포를 관리하고 랜딩 존 스택의 세트를 변경합니다.
- AWS Control Tower 작업을 수행합니다. 랜딩 존을 관리하고, 기준을 활성화하고, 제어를 활성화할 수 있습니다.
- AWS 조직을 관리합니다. 조직 단위를 생성 및 관리하고, 계정을 생성하고, 계정을 이동할 수 있습니다.
- Control Tower SCPs)을 관리합니다. AWS
- AWS Service Catalog 프로비저닝 아티팩트를 관리합니다.

Note

새 기능에 관한 변경이 필요한 경우 커넥터 유형이 업데이트될 수 있습니다. 대상 계정 커넥터 유형의 현재 버전은 2.0입니다. 새 커넥터를 생성하면 최신 버전을 사용합니다.

커넥터를 설정하기 전에 마이그레이션과 관련된 계정 역할을 이해합니다.

Account	설명
AWS 계정 변환	AWS 변환을 설정한 AWS 조직의 모든 멤버 계정입니다. 여기에서 AWS 변환 워크스페이스가 실행됩니다. 관리 계정일 필요는 없습니다.
커넥터 대상 계정	AWS 변환 커넥터가 구성된 계정입니다. 이는 마이그레이션 유형에 따라 다릅니다. • 단일 계정 마이그레이션 - 워크로드를 마이그레이션할 계정에 연결합니다. 커넥터 대상 계정과 대상 계정은 동일합니다. • 다중 계정 마이그레이션 - 조직 관리 계정 또는 위임된 관리자(DA) 계정에 연결합니다. DA 계정은 조직의 MGN 및 CloudFormation StackSets AWS 모두에 대한 위임된 관리자로 등록되어야 합니다. AWS 변환은 연결된 계정이 관리 계정인지 DA 계정인지 확인하고 그에 따라 동작을 조정합니다.
대상 계정	워크로드가 마이그레이션 AWS 계정 되는 입니다. 단일 계정 마이그레이션에서는 커넥터 대상 계정과 동일합니다. 다중 계정 마이그레이션에서는 마이그레이션된 워크로드를 수신하는 개별 멤버 계정입니다.

위임된 관리자 계정 사용

다중 계정 마이그레이션의 경우 조직 관리 계정이 아닌 위임된 관리자(DA) 계정을 직접 사용하는 것이 AWS 좋습니다. DA 계정은 마이그레이션 작업에 필요한 권한 범위를 제한하여 최소 권한 원칙을 따릅니다. DA 계정은 AWS 조직의 MGN 및 CloudFormation StackSets 모두에 대해 위임된 관리자로 등록되어야 합니다.

두 옵션의 주요 차이점은 다음과 같습니다.

- 관리 계정 - 조직 전체에서 MGN 및 CloudFormation StackSets에 대한 신뢰할 수 있는 액세스를 활성화할 수 있습니다.를 사용하여 calls CloudFormation StackSets APIs를 AWS 변환합니다CallAs: SELF.
- 위임된 관리자 계정 - 신뢰할 수 있는 액세스를 직접 활성화할 수 없지만(관리 계정에서 수행해야 함), MGN 소스 서버를 관리하고, 인스턴스를 시작하고, 멤버 계정 간에 CloudFormation StackSets를 배포할 수 있습니다. AWS 를 사용하여 calls CloudFormation StackSets APIs를 변환합니다CallAs: DELEGATED_ADMIN.

자세한 내용은 [MGN 사용 설명서의 MGN에 대한 위임된 관리자](#)를 참조하세요.

커넥터 설정 중에 생성된 IAM 역할

커넥터 설정 중에 AWS 변환은 대상 계정에 다음 IAM 역할을 생성합니다.

- AWSTransform-Connector-role- - AWS 조직의 관리 계정 또는 위임된 관리자 계정에서 대상 계정 커넥터를 설정할 때 생성됩니다. 이 역할을 통해 AWS 변환은 대상 계정에 연결하고 사용자를 대신하여 마이그레이션 작업을 실행할 수 있습니다.

대상 계정 커넥터 설정

Important

커넥터 설정 중에 대상에 Amazon S3 버킷이 생성됩니다 AWS 계정. 이 버킷은 기본적으로 HTTPS 전용 액세스(SecureTransport)를 적용하지 않습니다. 버킷 정책에 보안 전송을 포함하려면 정책을 직접 업데이트해야 합니다. 자세한 내용은 [Amazon S3의 보안 모범 사례를 참조하세요](#).

기존 대상 계정 커넥터를 사용하려면

1. 작업 계획 창에서 대상 계정 선택을 확장한 다음 커넥터 생성 또는 선택을 선택합니다.
2. 공동 작업 탭에서 기존 커넥터를 선택한 다음 커넥터 사용을 선택합니다. 커넥터를 사용할 수 없는 경우 해당 버전이 선택한 작업 유형과 호환되지 않습니다.

Important

AWS 변환 리전과 다른 대상을 가진 커넥터를 지정하면 AWS 변환 AWS 리전 이 데이터를 전송합니다 AWS 리전.

3. 계속을 선택합니다.

새 커넥터를 생성하려면

1. 작업 계획 창에서 대상 계정 연결을 확장한 다음 커넥터 생성 또는 선택을 선택합니다.
2. 대상에 AWS 리전 대해 AWS 계정 및를 지정한 후 다음을 선택합니다.

Important

대상이 검색과 AWS 리전 다른 경우 AWS 리전 AWS 변환은를 통해 데이터를 전송합니다 AWS 리전.

3. 암호화에 Amazon S3 관리형 키를 사용할지 여부를 선택합니다. 자체 KMS 키를 지정하는 경우 기본 키 정책 또는 덜 허용적인 정책을 사용할 수 있습니다. KMS 키를 생성하는 방법에 관한 자세한 내용은 AWS Key Management Service 개발자 안내서의 [KMS 키 생성](#)을 참조하세요.

AWS 변환은 kms:DescribeKey 권한을 사용하여 키가 존재하는지 확인하고, kms:GenerateDataKey 및 kms:Decrypt를 사용하여 Amazon S3 버킷의 작업 데이터를 암호화하고 해독합니다. 자세한 내용은 [Amazon S3 버킷 키를 사용하여 SSE-KMS 비용 절감](#)을 참조하세요.

4. 계속을 선택합니다.
5. 확인 링크를 복사 AWS 계정하여 대상의 관리자와 공유하고 연결 요청을 승인하도록 요청합니다.
6. 관리자가 요청을 승인한 후 목록에서 새로 생성된 커넥터를 선택하고 커넥터 사용을 선택합니다.
7. AWS 변환으로 전송을 선택합니다.

시작 후 작업을 활성화하도록 AWS Transform MGN 템플릿을 수정하려는 경우 대상 커넥터 역할에 다음 권한을 추가합니다. 이 JSON 정책 설명은 시작 후 작업 역할에 대한 iam:PassRole 권한을 부여합니다. 커넥터가 생성된 후 협업 탭에서 역할 이름을 찾을 수 있습니다. 역할에 권한을 추가하는 방법에 대한 자세한 내용은 IAM 사용 설명서의 [역할에 대한 권한 업데이트](#)를 참조하세요.

```
{
  "Sid": "MGNPostLaunchActions",
  "Effect": "Allow",
  "Action": [
    "iam:PassRole"
  ],
  "Resource": "arn:aws:iam::target-account-ID:role/service-role/
AWSApplicationMigrationLaunchInstanceWithSsmRole"
}
```

지원되는 대상 리전

마이그레이션 대상 리전은 랜딩 존, 네트워크 인프라 및 서버 리호스팅을 포함하여 마이그레이션된 리소스가 배포 AWS 리전 되는 입니다. 커넥터를 생성할 때 대상을 지정합니다 AWS 리전. AWS 리전다음 중 하나를 사용할 수 있습니다.

- 미국 동부(버지니아 북부)
- 미국 동부(오하이오)
- 미국 서부(캘리포니아 북부)
- 미국 서부(오리건)
- 아프리카(케이프타운)
- 아시아 태평양(홍콩)
- 아시아 태평양(타이베이)
- 아시아 태평양(뭄바이)
- 아시아 태평양(하이데라바드)
- 아시아 태평양(도쿄)
- 아시아 태평양(서울)
- 아시아 태평양(오사카)
- 아시아 태평양(싱가포르)
- 아시아 태평양(시드니)
- 아시아 태평양(자카르타)

- 아시아 태평양(멜버른)
- 아시아 태평양(말레이시아)
- 아시아 태평양(뉴질랜드)
- 아시아 태평양(태국)
- 캐나다(중부)
- 캐나다 서부(캘거리)
- 유럽(프랑크푸르트)
- 유럽(취리히)
- 유럽(아일랜드)
- 유럽(런던)
- 유럽(파리)
- 유럽(스톡홀름)
- 유럽(밀라노)
- 유럽(스페인)
- 이스라엘(텔아비브)
- 멕시코(중부)
- 남아메리카(상파울루)

Important

AWS 변환 AWS 리전 과 다른 대상을 지정하면 AWS 리전 일부 데이터가 간에 전송됩니다
AWS 리전.

서버 복제 데이터는 소스 환경에서 대상 계정 및 리전으로 직접 이동합니다.

랜딩 존 구축

AWS 변환은 마이그레이션 프로젝트의 일부로 AWS 랜딩 존을 설계하고 배포하는 과정을 안내합니다. 랜딩 존은 워크로드가 도착하기 전에 조직 경계, 거버넌스 제어 및 계정 구조를 갖춘 워크로드의 기반 역할을 하는 다중 계정 AWS 환경입니다. AWS 변환은 마이그레이션 인벤토리 및 비즈니스 요구 사항을 분석하여 조직 단위(OU) 및 계정 구조를 권장하고, 권장 서비스 제어 정책(SCPs) 적용하고, 코드형 인프라(IaC)를 생성 및/또는 배포합니다.

랜딩 존 에이전트는 다음 두 단계를 안내합니다.

- 파운데이션 설정 - 코어 랜딩 존 구조인 AWS Control Tower, 기본 OUs 및 코어 계정을 설정합니다.
- 워크로드 계정 설계 - 마이그레이션 웨이브, 사업부 및 환경 분리 요구 사항에 따라 워크로드 OUs 및 계정을 설계하고 생성합니다.

AWS 변환은 그린필드 환경(기존 랜딩 존 없음)과 브라운필드 환경(기존 OUs 및 계정이 이미 배포됨)을 모두 지원합니다. 브라운필드 시나리오에서 AWS 변환은 기존 조직 구조를 감지하고 AWS 모범 사례와의 격차를 해소하는 데 필요한 변경 사항만 권장합니다.

커넥터 설정

랜딩 존 에이전트는 조직 관리 계정에서 리소스를 프로비저닝하기 위해 대상 AWS 계정 커넥터가 필요합니다. 커넥터에는 다음과 같은 권한이 있습니다.

- [AWS Control Tower](#) 설정
- [조직 단위 및 계정](#) 생성
- [서비스 제어 정책\(SCPs\)](#) 구성

커넥터 요청을 승인할 때 다음에 AWS 변환 권한을 부여합니다.

- 대상 및 리전에서 랜딩 존 인프라를 프로비저닝 AWS 계정 하고 관리합니다. 여기에는 해당하는 `ATWorkspace:{workspace-id}` 경우 `CreatedBy:AWSTransform` 및 로 태그가 지정된 리소스로 제한된 다음 항목에 대한 권한이 포함됩니다.
 - 로 시작하는 버킷에 대한 S3 버킷 작업(생성, 읽기, 쓰기, 삭제) `transform-vmware-landing-zone-`
 - CloudFormation 랜딩 존 스택에 대한 스택 배포 및 변경 세트 관리
 - AWS Control Tower 작업(랜딩 존 관리, 기준 및 제어 활성화)
 - [AWS 조직](#) 관리(조직 단위 생성 및 관리, 계정 생성, 계정 이동)
 - AWS Control Tower를 통한 서비스 제어 정책(SCP) 관리
 - [AWS Service Catalog](#) 프로비저닝 아티팩트 관리

커넥터를 생성할 때 대상을 지정합니다 AWS 리전. 이 리전은 홈 Control Tower 리전과 동일해야 합니다. Control Tower 리전에 대한 자세한 내용은 [AWS Control Tower로 작업하는 방법을 AWS 리전참조](#) 하세요.

랜딩 존 설정을 시작할 때 AWS 변환은 커넥터 구성을 검색하고 확인을 위해 AWS 조직 관리 계정 ID와 대상 리전을 제공합니다. 자세한 내용은 [커넥터](#) 단원을 참조하십시오.

Important

IAM Identity Center 리전 종속성 - AWS 변환에는 AWS IAM Identity Center(IAM Identity Center)가 필요합니다. 즉, 커넥터 리전이 AWS Control Tower 홈 리전과 IAM Identity Center 리전 모두와 일치해야 합니다. 조직에 AWS IAM Identity Center가 이미 구성되어 있는 경우 커넥터가 다른 리전을 대상으로 하면 Control Tower 초기화가 실패합니다. 자세한 내용은 Control Tower 사용 설명서의 [IAM Identity Center 고객에 대한 고려 사항을](#) 참조하세요 AWS .

파운데이션 설정

파운데이션 설정 단계에서는 [AWS Control Tower](#)를 사용하여 코어 랜딩 존 인프라를 설정합니다. AWS Control Tower가 랜딩 존을 설정하면 전체 AWS 조직의 거버넌스 기반을 구성하는 관리 계정에 관리형 리소스 세트를 자동으로 프로비저닝합니다.

- 루트 - 랜딩 존의 모든 OUs가 포함된 최상위 상위 항목입니다.
- 보안 OU - Control Tower에서 자동으로 생성됩니다. 로그 아카이브 계정(조직 전체의 모든 AWS API 활동 및 리소스 변경 사항에 대한 변경 불가능한 중앙 집중식 로깅)과 감사 계정(보안 및 규정 준수 검토를 위해 모든 계정에 대한 읽기 전용 액세스)이라는 두 개의 공유 계정이 포함되어 있습니다. 초기 설정 후에는 이러한 계정의 이름을 바꾸거나 바꿀 수 없습니다.
- 필수 제어(가드레일) - Control Tower는 조직 전체에 예방 및 탐지 제어를 자동으로 적용하여 기존 거버넌스 정책을 적용합니다. 비활성화할 수 없습니다.
- IAM Identity Center 디렉터리 - Control Tower는 랜딩 존 사용자를 위해 미리 구성된 그룹과 Single Sign-On 액세스 권한이 있는 클라우드 네이티브 디렉터리를 생성합니다. 자세한 내용은 [AWS IAM Identity Center](#)를 참조하세요.

Control Tower는 [CloudFormation StackSets](#)를 사용하여 조직의 모든 계정 및 리전에 이러한 리소스를 일관되게 배포하고 관리합니다. 지원되는 방법 외부에서 Control Tower 관리형 리소스를 수정하거나 삭제하면 랜딩 존이 알 수 없는 상태가 될 수 있으므로 이렇게 하면 안 됩니다.

계정 이메일 규칙

AWS에는 각 계정에 고유한 이메일 주소가 필요합니다. 이러한 이메일은 계정에 대한 중요한 알림을 받습니다. AWS 변환은 더하기 주소 지정을 사용하여 단일 사서함에서 고유한 계정 이메일을 생성합니다.

형식: `prefix+account-name@domain`

접두사(예: `aws-admin`)와 도메인(예: `acme.com`)을 제공하면 AWS 변환이 모든 계정 이메일을 자동으로 추출합니다. 예제:

- 감사 계정: `aws-admin+audit@acme.com`
- 로그 아카이브 계정: `aws-admin+log-archive@acme.com`
- 샌드박스 계정: `aws-admin+sandbox@acme.com`

브라운필드 시나리오에서 AWS 변환은 기존 계정 이메일을 검사하여 이미 사용 중인 더하기 주소 지정 규칙을 유추하고 동일한 패턴으로 계속할 것을 제안합니다.

권장 파운데이션 구조

AWS 모범 사례에 따라 AWS Transform은 다음과 같은 파운데이션 OU 구조를 권장합니다. 생성 전에 사용자 지정할 수 있습니다.

OU	용도	계정
보안	중앙 집중식 감사 로깅 및 모니터링. 전용 계정에서 이러한 서비스를 격리하는 것은 감사 추적을 워크로드 팀과 분리하는 데 도움이 되도록 설계되었습니다.	감사, 로그 아카이브
인프라	공유 네트워킹(전송 게이트웨이, VPN), DNS 및 공통 서비스. 중복을 줄이고 네트워크 팀에 연결을 관리할 수 있는 단일 위치를 제공하는 데 도움이 되도록 이를 중앙 집중화하는 것이 좋습니다.	없음(비어 있음)

OU	용도	계정
샌드박스	지출 한도 및 제한된 액세스를 사용한 개발자 실험. 개발자에게 프로덕션 리소스 위험 없이 실험할 수 있는 공간을 제공하는 것이 좋습니다.	샌드박스
워크로드	프로덕션, 비프로덕션 및 선택적으로 규제된 하위 OUs 포함합니다. 워크로드 계정은 마이그레이션 요구 사항에 따라 다음 단계에서 설계됩니다.	없음(비어 있음)

Note

[감사 및 로그 아카이브 계정](#)이 있는 보안 OU는 Control Tower 파운데이션 설정의 일부로 생성됩니다. 인프라, 샌드박스 및 워크로드 OUs는 구조를 확인한 후 별도로 생성됩니다.

브라운필드 시나리오에서 AWS 변환은 기존 기반율이 권장 구조와 비교하고 격차만 보고합니다. 예: “파운데이션에는 보안 및 인프라 OUs 있지만 샌드박스 OU는 없습니다.”

서비스 제어 정책(SCP)

SCPs는 [조직의 모든 계정에 대한 최대 권한을 설정하는 조직 수준의 권한 가드레일](#)입니다. AWS 액세스 권한을 부여하지 않습니다. 대신 계정 관리자를 포함하여 계정의 어느 누구도 초과할 수 없는 경계를 정의합니다.

Control Tower 배포의 일부로 기존 가드레일이 자동으로 적용됩니다. AWS Transform은 조직의 태세를 강화하는 데 도움이 되도록 설계된 추가 SCPs도 권장합니다. 이는 실행 가능한 최소 랜딩 존의 AWS 모범 사례를 기반으로 합니다.

SCPs 인프라, 샌드박스 및 워크로드 OUs. 보안 OU는 Control Tower에서 관리하며 도구들 통해 SCPs가 대상으로 지정할 수 없습니다.

Important

보안 OU는 Control Tower에서 관리하는 파운데이션 OU입니다. 랜딩 존 에이전트를 통해 계정, SCPs 또는 리소스를 추가할 수 없습니다.

브라운필드 시나리오에서 AWS 변환은 이미 적용된 SCPs 확인하고 격차를 메울 수 있는 SCP만 권장합니다.

파운데이션 배포

파운데이션 설계가 완료되면 배포 방법을 선택합니다.

- 내게 배포 - AWS 변환은 파운데이션 OUs, 계정 및 SCPs를 AWS 조직에 배포합니다.
- 직접 배포하겠습니다. AWS 변환은 원하는 형식으로 다운로드할 코드형 인프라(IaC) 아티팩트를 생성합니다(참조 [the section called “IaC 형식”](#)).
- 워크로드 계정 먼저 설계 - 배포를 건너뛰고 워크로드 계정 설계 단계로 진행합니다. 나중에 모든 것을 함께 배포할 수 있습니다.

Control Tower 초기화

AWS 변환이 조직에서 AWS Control Tower가 아직 초기화되지 않았음을 감지하면 사용자에게 AWS 변환 콘솔 페이지에 대한 링크를 제공합니다. 링크에서 작업을 생성하면 Control Tower를 부트스트랩할 CloudFormation 스택이 생성됩니다. 이 프로세스는 대상 리전의 CloudFormation 콘솔에서이 스택을 생성합니다. 스택 생성이 완료되면 AWS 변환은 배포를 계속합니다.

워크로드 계정 설계

워크로드 계정 설계 단계에서 AWS Transform은 마이그레이션 인벤토리, 비즈니스 요구 사항 및 환경 분리 기본 설정을 기반으로 애플리케이션 워크로드에 대한 OU 및 계정 구조를 설계합니다.

마이그레이션 계획 컨텍스트

AWS 변환은 웨이브 계획, server-to-application 매핑, 공유 컨텍스트를 포함하여 마이그레이션 계획 단계에서 데이터를 검색합니다. 마이그레이션 계획 데이터를 사용할 수 있는 경우 AWS 변환은 요약 표시하고 확인 또는 조정을 요청합니다. 마이그레이션 계획 데이터를 사용할 수 없는 경우 AWS 변환은 검색 질문을 직접 합니다.

Discovery

AWS 변환은 워크로드 요구 사항을 이해하기 위한 질문을 합니다. 질문을 건너뛸 수 있습니다. 포함된 주제:

- 를 사용하는 사업부 또는 팀 수 AWS

- 산업 및 관련 프레임워크(HIPAA, PCI-DSS, SOC2, FedRAMP)
- 워크로드가 민감한 데이터를 처리하는지 여부(PII, PHI, 재무)
- 환경 분리 기본 설정(dev/test/staging/prod를 별도의 계정 또는 공유로 제공)
- 워크로드 격리 요구 사항
- 비즈니스 애플리케이션 및 용도
- 애플리케이션으로 서버 그룹화
- 비용 추적 및 할당 요구 사항(비즈니스 단위, 프로젝트, 환경별)
- 향후 12~24개월 동안 예상 성장률
- 계정 전략 기본 설정(계정당 단일 앱, 그룹화 또는 환경 기반)

제안된 워크로드 구조

답변 및 마이그레이션 계획 데이터를 기반으로 AWS 변환은 워크로드 OU에서 OU 및 계정 구조를 제안합니다. 제안에는 각 설계 결정의 근거가 포함되어 있습니다.

AWS 변환은 다음과 같은 설계 원칙을 따릅니다.

- 마이그레이션 웨이브의 모든 서버는 동일한 계정으로 이동합니다. 웨이브는 계정 간에 분할할 수 없습니다. 이는 웨이브 실행 중 리호스팅 제한입니다.
- 격리된 환경을 요청하는 경우 AWS 변환은 워크로드/프로덕션 및 워크로드/비프로덕션 하위 OUs를 생성합니다.
- 적용 가능한 프레임워크가 식별되면 AWS 변환은 워크로드/규정 및 워크로드/표준 하위 OUs를 생성합니다.
- 여러 사업부에 다른 거버넌스가 필요한 경우 AWS 변환은 워크로드에서 business-unit-specific OUs를 생성합니다.
- 중요 또는 민감한 데이터 애플리케이션은 계정당 단일 앱을 가져옵니다. 이 경우 웨이브 플랜을 반복 하라는 메시지가 표시될 수 있습니다.
- 공유 종속성이 있는 긴밀하게 연결된 애플리케이션은 하나의 계정으로 그룹화됩니다.

제안된 각 계정에는 이름, 용도, 대상 OU 및 사업부가 포함됩니다. AWS 변환에는 사용 중인 이름 지정 규칙이 표시됩니다(예: <business-unit>-<environment>-<workload>).

AWS 변환이 변경 사항을 적용하기 전에 제안된 구조를 검토하고 수정할 수 있습니다. 적용 후 반복하여 만족할 때까지 추가로 변경할 수 있습니다.

워크로드 SCP 구성

워크로드 구조가 생성되면 AWS 변환은 사용 가능한 SCPs 제공하고 워크로드 OUs. 적용할 SCPs와 OUs 선택합니다. AWS 변환은 SCPs를 적용하고 SCP 요약 테이블과 함께 업데이트된 조직 트리를 표시합니다.

워크로드 배포

워크로드 설계가 완료되면 배포 방법을 선택합니다.

- 내게 배포 - AWS 변환은 워크로드 OUs, 계정 및 SCPs를 AWS 조직에 배포합니다.
- 직접 배포하겠습니다. AWS 변환은 원하는 형식으로 다운로드할 IaC 아티팩트를 생성합니다(참조 [the section called “IaC 형식”](#)).

IaC 형식

자체 배포를 선택하면 AWS 변환은 다음 형식으로 코드형 인프라 아티팩트를 생성합니다.

- [AWS Cloud Development Kit \(AWS CDK\)](#) - 프로그래밍 방식의 인프라 배포를 위한 TypeScript 프로젝트입니다.
- HashiCorp Terraform - 랜딩 존 리소스를 관리하기 위한 HashiCorp 구성 언어(HCL) 템플릿을 생성합니다.
- Landing Zone Accelerator(LZA) - LZA 범용 구성 버전 1.1.0을 기반으로 YAML 파일을 구성합니다. 이러한 엔터프라이즈 지원 템플릿은 Landing Zone Accelerator와 함께 작동 AWS 하여 다중 계정 AWS 환경을 설정합니다. 생성된 파일에는 AWS 모범 사례에 맞는 거버넌스, 조직 구조 및 네트워킹에 대해 사전 구성된 설정이 포함되어 있습니다. 자세한 내용은 [LZA 범용 구성](#)을 참조하세요.

Note

Landing Zone Accelerator(LZA) 파이프라인을 통해 배포하는 경우 AWS 변환 계정과 LZA 설치가 동일한 AWS 조직에 있어야 합니다. AWS 변환에 사용된 조직 IDs와 LZA 간에 불일치가 있는 경우 배포가 실패합니다. Organizations를 사용하여 LZA 설치를 설정하는 방법을 알아보려면 [AWS 조직 기반 설치를 참조하세요](#).

형식을 선택하면 AWS 변환이 아티팩트를 생성하고 다운로드할 수 있도록 합니다.

다운로드한 파일이 손상되거나 변조되지 않았는지 확인하려면 체크섬을 생성 및 다운로드한 다음 다음을 사용하여 로컬에서 생성된 해시와 비교합니다.

```
openssl dgst -sha256 -binary <file.zip> | base64
```

배포 승인 프로세스

랜딩 존 배포 요청은 실행 전에 명시적 승인이 필요합니다. 배포 요청을 제출하면 승인 AWS 변환 탭을 통해 승인된 승인자에게 자동으로 라우팅됩니다.

승인자는 CloudFormation 템플릿과 랜딩 존 구성을 검토합니다. AWS 변환에서 관리자 역할을 가진 사용자만 배포 요청을 승인할 수 있습니다. 각 제출은 새 검토 주기를 트리거하고 배포는 확인을 받은 후에만 진행됩니다.

승인자가 요청을 거부하는 경우 직접 연락하여 필요한 수정 사항에 대해 논의합니다. 시스템은 감사 목적으로 모든 승인 결정을 추적하고 배포 기록을 유지합니다.

랜딩 존 리소스에 태그 지정

AWS 변환은 추적을 위해 로 생성된 모든 리소스에 정의 및 실행 IDs와 "CreatedBy": "AWSTransform" 함께 태그를 자동으로 지정합니다.

자동 태그

모든 랜딩 존 리소스는 다음 태그를 받습니다.

- CreatedBy - AWSTransform
- ATWorkspace - Workspace 식별자

Note

마이그레이션이 AWS 마이그레이션 가속화 프로그램(MAP 2.0)의 일부인 경우 필요한 MAP 태그: 키: map-migrated 값: migMPE_ID (여기서 MPE_ID는 마이그레이션 포트폴리오 평가 식별자)을 포함할 수 있습니다. 커넥터 설정 단계에서 MAP 태그가 요청됩니다. AWS 변환은 랜딩 존 배포 중에 이러한 태그를 적용합니다.

변경 사항 되돌리기

배포되지 않은 요소만 제거할 수 있습니다. OU 또는 계정이 배포되면 랜딩 존 에이전트를 통해 제거할 수 없습니다.

요소를 제거할 때는 순서가 중요합니다. 상위 요소보다 먼저 하위 요소를 제거해야 합니다.

1. 먼저 계정을 제거합니다(이메일).
2. OUs에서 SCPs를 제거합니다.
3. 하위 OUs 제거 - 아직 계정 또는 중첩된 OU가 있는 경우 OUs 제거할 수 없습니다.

관련 리소스

- [the section called “대상 AWS 계정 및 리전 연결”](#)
- [the section called “네트워크를 로 마이그레이션 AWS”](#)
- [AWS Control Tower 사용 설명서](#)
- [AWS Organizations 사용 설명서](#)
- [AWS IAM Identity Center 사용 설명서](#)
- [CloudFormation 사용 설명서](#)
- [의 랜딩 존 액셀러레이터 AWS](#)
- [AWS Well-Architected 프레임워크](#)
- [AWS 권장 가이드: 랜딩 존 구축](#)

네트워크를 로 마이그레이션 AWS

AWS 변환을 사용하면 네트워크를 로 마이그레이션할 수 있습니다 AWS. AWS 변환은 필요에 따라 소스 환경 구성을 VPCs, 서브넷, 보안 그룹, NAT 게이트웨이, 전송 게이트웨이, 탄력적 IPs, 경로 및 라우팅 테이블과 같은 AWS동등한 네트워크 리소스로 변환합니다. 배포 전에 생성된 네트워크 구성을 검토하고 수정할 수 있습니다. 네트워크 연결을 AWS 변환하고 분석하여 구성을 배포할 수 있습니다. 또는 자체 배포를 선택하고 선호하는 형식 AWS Cloud Development Kit (AWS CDK)인 Landing Zone Accelerator(LZA) 또는 HashiCorp Terraform으로 코드형 인프라(IaC)를 수신할 수 있습니다. HashiCorp

네트워크를 마이그레이션하려면 다음 단계를 따르세요.

1. 소스 네트워크 파일을 업로드합니다.
2. 추가 구성 파일을 업로드합니다(RVTools 환경의 경우 선택 사항).
3. 네트워크 토폴로지를 선택합니다.
4. 보안 그룹 매핑 전략을 선택합니다.
5. 네트워크를 검토하고 최적화합니다.
6. 네트워크 다이어그램을 생성합니다(선택 사항).
7. 리소스 태그 지정을 구성합니다.
8. 네트워크를 배포합니다.

Note

다중 계정 배포의 경우 네트워크 마이그레이션을 시작하기 전에 AWS Organizations에 대한 교차 계정 IAM 역할과 신뢰할 수 있는 액세스를 구성해야 합니다. 마이그레이션 유형에 대한 자세한 내용은 섹션을 참조하세요 [the section called “1단계: 마이그레이션 유형 선택”](#).

1단계: 소스 네트워크 매핑

네트워크 매핑 프로세스를 수행하려면 소스 환경에서 구성 파일을 업로드해야 합니다. 선택하는 도구는 소스 네트워크 유형에 따라 다릅니다.

- 소프트웨어 정의 네트워크(SDN): VMware NSX 네트워크 가상화용 가져오기/내보내기 또는 Cisco Application Centric Infrastructure용 Cisco ACI 구성.
- VMware vSphere 네트워크: [RVTools](#). RVTools 파일을 사용하는 경우 AWS 변환은 Amazon VPC 구성만 생성합니다. 보안 그룹 구성에는 방화벽 또는 소프트웨어 정의 네트워크 파일의 추가 입력이 필요합니다. 추가 파일에서 보안 그룹을 생성하는 방법에 대한 자세한 내용은 [추가 구성 파일을](#) 참조하세요.
- 방화벽 구성 데이터를 기반으로 하는 네트워크: Palo Alto Networks Firewall, Fortinet FortiGate Firewall 또는 Cisco ACI에서 파일을 내보냅니다. 지원되는 버전 및 추출 지침에 대한 자세한 내용은 [구성 파일 추출](#)을 참조하세요.
- VMware 워크로드와 비 VMware 워크로드를 모두 실행하는 하이브리드 네트워크: [AWS 검색 도구 또는 modelizeIT를 변환](#)합니다. modelizeIT
- 기타 파일 유형: 구성 파일이 위에 나열된 지원되는 형식 중 하나가 아닌 경우 파일이 지원되는 형식으로 자동으로 변환됩니다. 이 변환은 파일 크기와 복잡성에 따라 최대 2시간이 걸릴 수 있습니다.

Note

지원되는 최대 소스 네트워크 파일 크기는 70MB입니다.

Warning

<https://www.dell.com/en-us/shop/vmware/sl/rvtools> 공식 Dell 사이트에서만 RVTools를 다운로드합니다. 비공식 소스에서 RVTools를 다운로드하지 마십시오.

각 소스 네트워크 세그먼트는 고유한 VPC에 매핑됩니다. 네트워크 세분화는 소스 유형에 따라 다릅니다.

- vNetwork: AWS Transform은 vSwitch 및 가상 LAN(VLAN)별로 VMs. VLANs 여러 vSwitches(VLAN 0 제외).
- NSX 네트워크: AWS Tier-1 라우터를 기반으로 네트워크를 세그먼트화하여 라우터를 그룹화하고 세그먼트를 수집합니다.

2단계: 추가 구성 파일

RVTools 소스 환경의 경우 선택적으로 추가 구성 파일을 업로드하여 보안 그룹 생성을 활성화할 수 있습니다. 추가 구성 파일을 업로드하지 않으면 RVTools 기반 마이그레이션에 대한 보안 그룹이 생성되지 않습니다.

AWS 변환은 다음과 같은 추가 구성 파일 유형을 지원합니다. 하나의 플랫폼에서 하나의 구성 파일만 업로드할 수 있습니다.

- Cisco Application Centric Infrastructure(ACI)는 네트워크 정책 구성을 제공합니다.
- Palo Alto Networks는 방화벽 보안 정책을 제공합니다.
- Fortinet FortiGate는 방화벽 보안 정책을 제공합니다.

방화벽 또는 Cisco ACI 파일을 업로드하면 AWS 변환이 네트워크 인프라 및 보안 그룹을 생성합니다. RVTools 파일만 업로드하면 AWS 변환은 네트워크 인프라만 생성합니다.

지원되는 버전 및 추출 지침에 대한 자세한 내용은 [구성 파일 추출](#)을 참조하세요.

3단계: 네트워크 토폴로지

네트워크 정의 단계에서 네트워크 토폴로지를 선택합니다. 격리된 VPCs 토폴로지 또는 허브 및 스포크 토폴로지를 선택할 수 있습니다.

격리된 VPC

배포된 항목

격리VPCs는 내부에서 별도의 단위로 작동하는 독립적인 네트워크 환경입니다 AWS. VPCs는 서로 내장된 통신 경로 없이 완전히 격리됩니다. 이 분리는 가장 높은 수준의 네트워크 경계 보호를 제공합니다.

AWS 변환은 다음 리소스를 생성합니다.

- 감지된 각 소스 네트워크 세그먼트에 대한 전용 VPC입니다.
- 소스 네트워크 구성을 기반으로 하는 프라이빗 서브넷입니다.
- 보안 그룹(방화벽 또는 SDN 구성 파일을 제공한 경우).

설정 완료

AWS 변환은 네트워크 인프라를 배포하지만 인터넷 액세스 및 VPC 간 연결을 그대로 유지하므로 조직의 요구 사항에 맞는 구성을 선택할 수 있습니다.

격리된 VPC에 대한 인터넷 액세스를 활성화하려면 다음 단계를 완료합니다.

1. [인터넷 게이트웨이](#)를 생성하여 VPC에 연결합니다.
2. 인터넷 액세스가 필요한 각 가용 영역에 퍼블릭 서브넷을 생성합니다. 인터넷 게이트웨이를 0.0.0.0/0 가리키는 경로를 추가합니다. 서브넷 구성에 대한 자세한 내용은 [VPC의 서브넷을 참조하세요](#).
3. 퍼블릭 서브넷에 [NAT 게이트웨이](#)를 생성합니다(고가용성을 위해 AZ당 하나). 각 NAT 게이트웨이에 탄력적 IP를 할당합니다.
4. 프라이빗 서브넷 [라우팅 테이블](#) 업데이트 - 동일한 AZ에서 NAT 게이트웨이를 0.0.0.0/0 가리키는 경로를 추가합니다.
5. [보안 그룹 규칙](#) 검토 - 아웃바운드 규칙이 워크로드에 필요한 트래픽(HTTPS, DNS 등)을 허용하는지 확인합니다.

VPC-to-VPC 통신의 경우 [VPC 피어링](#) 또는 [Transit Gateway](#)를 설정하고 각 VPC의 라우팅 테이블을 업데이트하여 트래픽을 피어링 연결 또는 TGW 연결로 라우팅합니다.

허브 및 스포크

이 모델에서 [AWS Transit Gateway](#)는 여러 워크로드 VPCs(스포크)를 연결하는 중앙 허브 역할을 합니다.

배포된 항목

AWS 변환은 다음 리소스를 생성합니다.

- 스포크 VPCs: 프라이빗 서브넷과 Transit Gateway 연결이 있는 감지된 소스 네트워크 세그먼트당 하나의 VPC입니다.
- 검사 VPC: 트래픽 검사를 위해 방화벽 어플라이언스를 호스팅합니다. 모든 VPC 간 트래픽은 이 VPC를 통해 라우팅됩니다. Transit Gateway 연결은 연결의 양방향에 대해 동일한 어플라이언스를 통해 트래픽이 대칭적으로 흐르도록 하는 설정인 어플라이언스 [모드](#)를 사용합니다.
- 인바운드 VPC: 퍼블릭 인터넷(북남 인바운드)에서 네트워크로 들어오는 트래픽을 처리합니다. [인터넷 게이트웨이](#)와 여러 가용 영역의 퍼블릭 서브넷을 포함합니다.
- 아웃바운드 VPC: 네트워크에서 퍼블릭 인터넷(남북 아웃바운드)으로 전송되는 트래픽을 처리합니다. 인터넷 게이트웨이, [고가용성을 위해 각 가용 영역에 탄력적 IP 주소가 있는 NAT 게이트웨이](#), Transit Gateway 연결을 위한 프라이빗 서브넷이 포함됩니다. <https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/elastic-ip-addresses-eip.html>
- Transit Gateway 라우팅 테이블: 두 개의 라우팅 테이블이 검사 VPC를 통해 트래픽을 조향합니다. 검사되지 않은 테이블은 스포크 VPCs, 인바운드 VPC 및 아웃바운드 VPC와 연결됩니다. 모든 트래픽(0.0.0.0/0)을 검사 VPC 연결로 라우팅하며 기본 연결 라우팅 테이블입니다. Inspected 테이블은 검사 VPC와 연결되어 있습니다. 여기에는 모든 스포크 VPCs의 전파된 경로가 포함되며 기본 전파 라우팅 테이블입니다.

다중 계정 배포의 경우 Transit Gateway는 [AWS Resource Access Manager\(RAM\)](#)를 통해 계정 간에 공유됩니다.

트래픽 흐름

모든 VPC 간 트래픽은 다음 경로를 따릅니다.

1. 스포크 VPC의 트래픽은 Transit Gateway로 전송됩니다(기본 경로 0.0.0.0/0).

2. 검사되지 않은 라우팅 테이블은 트래픽을 검사 VPC로 라우팅합니다.
3. 검사 VPC의 방화벽은 트래픽을 검사하고 Transit Gateway로 다시 전달합니다.
4. 검사된 라우팅 테이블은 전파된 경로를 사용하여 트래픽을 대상 스포크 VPC로 라우팅합니다.

아웃바운드 인터넷 트래픽의 경우 검사된 라우팅 테이블은 트래픽을 아웃바운드 VPC로 라우팅합니다. NAT 게이트웨이는 트래픽이 인터넷 게이트웨이로 전달되기 전에 프라이빗 IP 주소를 변환합니다. 아웃바운드 VPC 퍼블릭 라우팅 테이블에는 Transit Gateway로 돌아가는 각 스포크 VPC Classless Inter-Domain Routing(CIDR) 범위에 대한 특정 경로가 포함되어 있습니다. 이러한 경로를 통해 반환 트래픽이 올바른 스포크 VPC에 도달할 수 있습니다.

인바운드 인터넷 트래픽은 인바운드 VPC의 인터넷 게이트웨이를 통해 들어오고 동일한 검사 경로를 따라 스포크 VPCs.

설정 완료

AWS 변환은 네트워크 인프라를 배포하지만 방화벽 구성과 인바운드 서비스 설정을 그대로 유지하므로 조직의 요구 사항에 맞는 보안 어플라이언스와 정책을 선택할 수 있습니다.

Note

기본적으로 VPC 간 트래픽은 검사 없이 검사 VPC를 통과합니다. 트래픽 검사를 활성화하려면 방화벽을 배포해야 합니다.

방화벽 배포: 방화벽 엔드포인트에 대해 검사 VPC에 추가 서브넷을 생성합니다. AWS 변환은 Transit Gateway 연결에 대해서만 서브넷을 생성합니다. TGW 연결 서브넷에서 방화벽 엔드포인트로 트래픽을 라우팅하고 방화벽 서브넷에서 Transit Gateway로 다시 라우팅합니다. [AWS Network Firewall](#) 또는 타사 어플라이언스를 배포할 수 있습니다. Transit Gateway를 사용하여 방화벽을 배포하는 방법에 대한 자세한 내용은 [Transit Gateway를 사용하여 방화벽 생성을 참조하세요](#).

연결 확인: 방화벽을 배포한 후 스포크 VPC 인스턴스(예: `curl https://aws.amazon.com`)에서 아웃바운드 인터넷 액세스를 테스트합니다. [Reachability Analyzer](#)를 사용하여 연결 문제를 해결할 수 있습니다.

인바운드 서비스 설정: 퍼블릭 서비스를 호스팅하려면 인바운드 VPC 퍼블릭 서브넷에 [Application Load Balancer](#) 또는 [Network Load Balancer](#)를 배포합니다. Transit Gateway를 통해 스포크 VPCs의 인스턴스를 가리키는 대상 그룹을 구성하고 검사된 라우팅 테이블에 인바운드 VPC에 대한 반환 경로가 있는지 확인합니다.

VPCs 간의 통신을 세밀하게 제어하려면 격리된 VPCs 옵션을 선택하고 생성된 네트워크를 수정하여 필요한 특정 통신 경로를 생성합니다.

4단계: 보안 그룹 매핑

소스 보안 정책이 AWS 보안 그룹으로 변환되는 방법을 선택합니다. AWS 변환은 소스 환경 구성을 기반으로 보안 그룹을 생성합니다. 보안 정책, 보안 정책 규칙, 게이트웨이 정책 및 게이트웨이 정책 규칙은 보안 그룹으로 변환됩니다.

Important

AWS 변환은 소스 환경에 맞게 최선을 다해 보안 그룹을 생성합니다. 생성된 보안 그룹을 검토하고 수정하여 회사의 요구 사항과 보안 정책을 충족하는지 확인합니다.

보안 그룹 참조

보안 그룹이 생성되면 AWS 변환은 지원되는 위치를 참조하는 보안 그룹을 사용합니다. 보안 그룹 참조는 특정 IP 주소 범위(CIDR 블록)가 아닌 다른 보안 그룹 ID를 기반으로 보안 규칙을 설정합니다. 이 접근 방식은 보다 유연하고 유지 관리 가능한 보안 구성을 제공합니다.

보안 그룹 규칙은 동일한 VPC 내의 다른 보안 그룹 또는 동일한 리전 내에 연결된 VPC에서만 참조할 수 있습니다. 교차 계정 참조도 지원됩니다. 연결되지 않은 VPC 또는 여러 리전에서 보안 그룹을 참조할 수 없습니다. 연결된 VPCs 경우 인바운드 규칙만 VPC 간 보안 그룹 참조를 지원합니다. 아웃바운드 규칙은 CIDR 기반 규칙을 사용해야 합니다. AWS 변환이 보안 그룹 규칙을 생성하는 방법은 선택한 네트워크 토폴로지에 따라 달라집니다.

- 허브 및 스포크: Transit Gateway는 VPCs 간에 네트워크 연결을 제공합니다. AWS 변환은 VPC 내 및 교차 VPC/교차 계정 수신 규칙 모두에 대한 참조를 사용합니다. 교차 VPC/교차 계정 송신(아웃바운드) 규칙은 CIDR 기반 규칙을 사용합니다.
- 격리VPCs: VPCs 간에 네트워크 연결이 없습니다. AWS 변환은 VPC 내 규칙에 대해서만 참조를 사용합니다. 모든 VPC 간 및 계정 간 규칙은 CIDR 기반 규칙을 사용합니다.

CIDR 기반 규칙은 소스 구성이 대칭이 아닌 경우에도 사용됩니다.

다음 보안 그룹 매핑 전략 중 하나를 선택합니다.

- MAP: 소스 환경의 보안 규칙을 AWS 보안 그룹 및 규칙으로 변환합니다. 고정 IP 주소 지정을 사용하는 마이그레이션에는 이 옵션을 사용합니다.

- MAP_DHCP(DHCP 지원으로 변환): DHCP 호환성을 사용하여 소스 환경에서 보안 규칙을 변환합니다. DHCP는 서브넷의 CIDR 범위에서 동적으로 IP 주소를 할당합니다. 따라서 전체 대상 서브넷 CIDR과 일치하도록 VPC 간 송신 규칙이 확장됩니다. CIDR이 좁을수록 해당 범위를 벗어나는 DHCP 할당 IPs 차단됩니다. 마이그레이션 후 이러한 규칙을 검토합니다.

VPC 간 Transit Gateway 통신을 통한 DHCP 지원에이 옵션을 사용합니다. 또한 정적 IPs에서도 작동하지만 MAP보다 더 광범위한 규칙을 생성할 수 있습니다.

- 건너뛰기: 보안 규칙을 변환하지 않습니다. 마이그레이션 후 AWS 보안 그룹을 수동으로 구성합니다. 고정 IP 및 DHCP 환경 모두에서 작동합니다. 추가 구성 파일이 없는 RVTools 소스 환경의 경우 AWS 변환은 자동으로 SKIP를 사용합니다.

Note

매핑 전략에 따라 IP 할당 옵션이 결정됩니다. MAP는 고정 IP만 지원합니다. MAP_DHCP 및 SKIP는 정적 및 DHCP를 모두 지원합니다.

IP 마이그레이션 접근 방식

마이그레이션에는 두 가지 네트워크 구성이 있습니다.

네트워크 범위 선택

- 기존 범위 유지(IP 주소 범위 보존): 마이그레이션 중에 원래 IP 주소 범위를 유지합니다. 수정(lift-and-shift) AWS 없이 애플리케이션을 로 이동하는 마이그레이션, 특히 하드 코딩된 IP 종속성 또는 기존 방화벽 규칙이 있는 레거시 애플리케이션에 적합합니다.
- 새 IP 범위로 업데이트(CIDR 업데이트): 마이그레이션 중에 각 VPC CIDR 범위를 수정할 수 있으며 변환은 서브넷, 라우팅 테이블 및 보안 그룹에 대한 변경 사항을 AWS 자동으로 전파합니다.

IP 주소 할당

- 고정 IP 주소(정적): AWS 변환은 CIDR을 기반으로 고정 IPs를 할당합니다. 이는 예측 가능한 네트워크 동작, DNS 관리 또는 IP 기반 액세스 제어가 필요한 애플리케이션에 가장 적합합니다. IPs 인스턴스에 연결된 가상 네트워크 카드인 탄력적 네트워크 인터페이스(ENIs)를 통해 인스턴스 재시작 간에 유지됩니다.

- 동적 IP 할당(AWS DHCP): 인스턴스 시작 시 서브넷 풀의 IPs 자동으로 할당합니다. 클라우드 및 Auto Scaling 워크로드에서 실행되도록 설계된 애플리케이션에 적합합니다. 운영 오버헤드를 줄이지만 애플리케이션이 DNS 또는 서비스 검색을 사용해야 합니다.

두 범위 선택 중 하나를 IP 할당 방법과 결합할 수 있습니다.

Note

IP 주소 할당 전략은 웨이브 수준에서 설정됩니다. 웨이브 파일을 사용자 지정하여 특정 서버에 다양한 전략을 할당할 수 있습니다. 예를 들어 웨이브에 정적 IP 주소 접근 방식을 선택했지만 특정 서버에 동적 접근 방식을 할당하려는 경우 MGN 사용 설명서의 [구성 편집](#)에 설명된 [RESET_VALUE] 대로를 사용합니다.

5단계: 네트워크 검토 및 최적화

AWS 변환이 대상 네트워크 구성을 생성한 후 AWS 인프라에 수렴된 온프레미스 네트워크 세그먼트를 검토할 수 있습니다. 시각적 인터페이스를 사용하여 네트워크를 검토하고 채팅 인터페이스를 사용하여 변경하고 안내된 권장 사항을 받습니다. AWS 변환은 계단식 영향 분석을 수행하고 필요한 변경 사항을 구현하여 네트워크 일관성과 모범 사례 준수를 유지합니다. AWS 변환에 네트워크를 분석하고 최적화를 제안하도록 요청할 수도 있습니다. [권장 사항 가이드](#)를 참조하세요.

대상 계정VPCs

대상 계정에 이전 마이그레이션 단계 또는 병렬 인프라 프로젝트의 VPCs가 이미 포함되어 있는 경우 AWS 변환은 검토 프로세스 중에 VPC를 자동으로 감지하고 매핑된 VPCs와 함께 표시합니다. 다중 계정 마이그레이션의 경우 AWS 변환은 AWS 조직의 모든 계정에서 기존 VPCs 감지합니다.

이러한 가시성은 계획된 네트워크가 기존 인프라와 어떤 관련이 있는지 이해하고, 잠재적 CIDR 충돌을 식별하고, 배포 전에 정보에 입각한 결정을 내리는 데 도움이 됩니다.

Note

AWS 변환은 기존 VPCs만 감지합니다(서브넷 또는 기타 리소스 제외). 감지는 읽기 전용입니다. AWS 변환은 기존 VPCs 수정하지 않습니다.

네트워크 최적화

Note

이러한 작업은 워크로드 VPCs에만 적용됩니다. 허브 및 스포크 토폴로지(검사, 인바운드, 아웃바운드)의 어플라이언스 VPCs의 경우 IP 주소 변경만 지원됩니다.

삭제, 병합 및 분할 작업은 실행 취소할 수 없습니다. 이러한 변경 사항을 적용하기 전에 구성을 주의 깊게 검토합니다.

VPCs

- 삭제: 구성에서 VPC를 영구적으로 제거합니다. 마이그레이션해서는 안 되는 더 이상 사용되지 않는 네트워크 세그먼트에 사용합니다 AWS.
- 제외: 단계별 마이그레이션 전략을 위해 마이그레이션에서 VPC를 일시적으로 제거합니다. 제외 VPCs는 배포되지 않지만 나중에 다시 포함할 수 있습니다.
- 포함: 이전에 제외된 VPC를 마이그레이션에 다시 추가합니다.
- 병합: 두 VPCs. 첫 번째 VPC는 자격 증명을 유지하고 두 번째 VPC에서 모든 서브넷을 흡수합니다. 보안 그룹은 병합된 VPC로 이동되고 그에 따라 연결이 다시 빌드됩니다. 첫 번째 VPC의 CIDR은 원래 CIDR을 모두 포함하는 가장 작은 CIDRs 범위로 확장되며 라우팅은 자동으로 업데이트됩니다. 두 번째 VPC는 구성에서 제거됩니다.

병합 요구 사항:

- 서브넷 CIDRs 두 VPCs 간에 겹치지 않아야 합니다.
- 병합된 CIDR은 /16을 초과해서는 안 됩니다.
- 다중 계정 배포의 경우 두 VPCs 동일한 계정에 할당해야 합니다.
- IP 주소 변경: 동일한 접두사 길이를 유지하면서 VPC CIDR의 기본 IP 주소를 변경합니다. AWS 변환은 모든 서브넷 CIDRs으로 자동으로 변환합니다. 예를 들어 VPC에서 10.0.0.0/16로 변경하면 서브넷에서 10.0.1.0/24로 10.20.0.0/16로 전환됩니다 10.20.1.0/24.

이전 VPC CIDR과 정확히 일치하는 보안 그룹 규칙은 자동으로 업데이트됩니다. 이전 CIDR과 부분적으로 겹치거나 일치하지 않는 규칙은 변경되지 않습니다. 변경 후 이러한 규칙을 검토하세요.

- 이름 바꾸기: 비용 할당, 규정 준수 추적 및 운영 표준에 대한 조직의 이름 지정 규칙에 맞게 VPC 이름을 변경합니다.
- 크기 조정: VPC CIDR의 접두사 길이를 변경하여 IP 주소 범위를 확장하거나 줄입니다.

- 접두사 길이 감소(IPs, 예: /20~/16): 서브넷이 여전히 더 큰 범위에 맞습니다. 서브넷을 변경할 필요가 없습니다.
- 접두사 길이 증가(IPs 감소, 예: /16~/20): 새 범위를 벗어나는 서브넷은 먼저 서브넷 크기 조정 작업을 사용하여 크기를 조정해야 합니다.

이전 VPC CIDR과 정확히 일치하는 보안 그룹 규칙은 자동으로 업데이트됩니다. 이전 CIDR과 부분적으로 겹치거나 일치하지 않는 규칙은 변경되지 않습니다. 크기 조정 후 이러한 규칙을 검토하세요.

크기 조정 요구 사항:

- 새 CIDR은 /16에서 /28 사이여야 합니다.
- 새 CIDR은 네트워크의 다른 VPCs(허브 및 스포크 토폴로지)와 겹치지 않아야 합니다.
- CIDR을 줄일 때 모든 기존 서브넷이 새 CIDR에 맞아야 합니다. 필요한 경우 먼저 서브넷의 크기를 조정합니다.
- 분할: 제공하는 CIDR 경계에 따라 VPC를 VPCs로 나눕니다. 서브넷은 CIDR에 포함된 새 VPC에 할당됩니다. 보안 그룹은 두 새 VPCs 모두에 복제되지만 보안 그룹 규칙 CIDRs은 자동으로 업데이트되지 않습니다. 분할 후 규칙을 검토하여 VPC 간 통신이 예상대로 작동하는지 확인하세요. 원래 VPC는 두 개의 새 VPCs.

분할 요구 사항:

- 정확히 두 개의 CIDR 범위를 제공해야 합니다.
- 두 CIDRs 됩니다.
- 각 CIDR은 /16에서 /28 사이여야 합니다.
- 모든 서브넷은 두 CIDRs. 서브넷이 맞지 않으면 작업이 거부됩니다.

서브넷에 사용할 수 있는 작업은 다음과 같습니다.

- IP 주소 변경: 동일한 접두사 길이를 유지하면서 서브넷 CIDR의 기본 IP 주소를 변경합니다.
- 삭제: 상위 VPC에 영향을 주지 않고 구성에서 서브넷을 영구적으로 제거합니다.
- 크기 조정: 서브넷 CIDR의 접두사 길이를 변경하여 IP 주소 범위를 확장하거나 줄입니다.

서브넷 크기 조정 요구 사항:

- 새 CIDR은 /16에서 /28 사이여야 합니다.
- 새 CIDR은 동일한 VPC의 다른 서브넷과 겹치지 않아야 합니다.
- 새 CIDR은 상위 VPC CIDR 내에 있어야 합니다.

각 작업 후 AWS Transform은 보안 그룹 참조를 재평가하여 CIDR 기반 규칙을 보안 그룹 참조로 변환하거나 그 반대로 변환할 수 있습니다. 변경 후 보안 그룹 규칙을 검토하여 요구 사항을 충족하는지 확인합니다.

가이드 네트워크 권장 사항

AWS 변환은 매핑된 네트워크를 분석하고 채팅 인터페이스를 통해 우선순위가 지정된 권장 사항을 제공합니다. 권장 사항은 네트워크 데이터를 기반으로 하며 변경 사항이 적용되기 전에 확인이 필요합니다.

AWS 변환은 다음과 같은 최적화를 권장할 수 있습니다.

- CIDR 충돌 해결: AWS 조직의 모든 계정에서 매핑된 VPCs와 기존 VPCs 간에 중첩되는 CIDR 범위에 플래그를 지정합니다. 충돌 VPCs가 먼저 표시됩니다. 매핑된 VPC를 다시 주소 지정하거나, 제외 또는 삭제하거나, 충돌을 확인하고 배포 후 직접 해결하여 충돌을 해결할 수 있습니다.
- 이름 지정 표준화: 일관된 패턴을 따르지 않는 VPC 이름(예: 하드웨어 참조가 포함된 이름)에 플래그를 지정합니다. AWS 변환은 교체를 제안하기 전에 클라우드 이름 지정 규칙을 요청합니다.
- 범위 검토: 폐기 보류 중인 레거시 시스템 또는 구문 AWS와 같이 마이그레이션할 필요가 없을 수 있는 네트워크 세그먼트를 식별합니다. AWS 변환은 구문을 제외하기 전에 확인을 요청합니다.
- VPC 용량 적정 크기 조정: CIDR이 포함된 서브넷에 대해 크기가 크거나 작게 나타나는 VPCs를 표시합니다. AWS 변환은 현재 용량 데이터를 제공하고 크기를 조정할지 여부를 결정할 수 있습니다.
- 보안 검토: 검토를 위해 무제한 인바운드 트래픽(0.0.0.0/0)을 허용하는 보안 그룹 규칙에 플래그를 지정합니다.
- VPC 통합: 논리적 격리 요구 사항이 아닌 물리적 인프라 제한으로 구분되어 나타나는 조각화된 VPCs를 식별하고 병합을 제안합니다.

Note

모든 권장 사항은 AWS 변환이 변경 사항을 적용하기 전에 명시적 확인이 필요합니다. AWS 변환은 권장 사항이 네트워크의 여러 측면에 영향을 미칠 때 장단점을 제공합니다.

6단계: 네트워크 다이어그램

생성된 VPC 구성을 검토한 후 선택적으로 네트워크 다이어그램을 생성하여 네트워크 토폴로지를 시각화할 수 있습니다. AWS 변환은 다음 다이어그램 형식을 지원합니다.

- Mermaid 코드(.mmd): 이 형식은 Mermaid 호환 도구로 렌더링할 수 있는 텍스트 기반 다이어그램 정의 파일을 생성합니다.
- 이미지(.png): 이 형식은 네트워크 토폴로지의 렌더링된 이미지를 생성합니다.

7단계: 리소스 태그 지정 구성

네트워크 리소스에는 시작 및 복제를 위한 태그가 지정됩니다. 사용자 지정 태그와 AWS Migration Acceleration Program(MAP) 태그를 추가할 수도 있습니다.

시작 및 복제를 위한 자동 태그

AWS 변환은 마이그레이션된 네트워크 리소스(VPCs, 서브넷, 보안 그룹 및 라우팅 테이블)에 다음 태그를 사용하여 자동으로 태그를 지정합니다.

- 키: CreatedBy 값: AWSApplicationMigrationService
- 키: ATWorkspace 값: *workspace-id*

이러한 태그를 사용하면 VPC 및 서브넷을 사용하여에서 테스트 및 전환 인스턴스를 시작할 수 있습니다 AWS.

Note

마이그레이션된 VPCs 및 서브넷에는 기본적으로 인터넷 연결이 포함되어 있지 않으므로 복제를 위한 스테이징 영역으로 적합하지 않습니다.

또한 VPC 및 서브넷을 스테이징 영역(복제)으로 사용하려면 다음 태그를 수동으로 추가합니다.

- 키: CreatedFor 값: AWSTransform
- 키: ATWorkspace 값: *workspace-id*

이러한 태그를 기존 AWS 네트워크 리소스에 적용하여 복제에 사용할 수 있도록 할 수도 있습니다.

AWS 변환 웹 앱 URL에서 워크스페이스 ID 찾기: <https://.../workspace/workspace-id/job/job-id>

사용자 지정 태그

AWS 변환에 의해 자동으로 적용되는 태그 외에도 선택적으로 사용자 지정 태그를 추가하여 마이그레이션된 네트워크 리소스에 대한 규정 준수를 구성, 비용 추적 및 관리할 수 있습니다. 두 가지 수준에서 사용자 지정 태그를 적용할 수 있습니다.

- 작업 수준 태그: 모든 VPCs, 보안 그룹 및 라우팅 테이블을 포함하여이 작업에서 생성된 모든 리소스에 적용됩니다.
- VPC 수준 태그: 특정 VPC에 적용하고 연결된 모든 리소스(서브넷, 보안 그룹, 라우팅 테이블)에 자동으로 캐스케이드합니다.

Note

요청당 최대 40개의 태그. 각 태그에는 키와 value. AWS tagging 규칙이 필요합니다.

AWS 변환은 코드형 인프라 템플릿을 생성할 때 이러한 태그를 적용합니다.

AWS 마이그레이션 가속화 프로그램

마이그레이션이 AWS 마이그레이션 가속화 프로그램(MAP 2.0)의 일부인 경우 AWS 변환은 리소스에 MAP 태그를 적용합니다. 마이그레이션 프로세스 초기에 MPE ID를 제공한 경우 태그가 자동으로 적용됩니다. 그렇지 않으면 생성된 VPC 구성 검토를 완료한 후 AWS 변환은 MAP 계약이 있는지 묻고 대문자와 숫자(예: ABCDE12345)를 사용하는 10자 코드인 MPE ID를 제공하라는 메시지를 표시합니다. 적용된 태그는 형식을 사용합니다.

- 키: map-migrated 값: migMPE_ID

8단계: 네트워크 배포

태그 지정 후 배포 전략을 선택합니다.

- AWS 변환 관리형 배포: AWS 변환은 CloudFormation 템플릿을 사용하여 네트워크를 배포하고 Reachability Analyzer를 실행하여 여러 VPCs와 동일한 VPC 내의 서브넷 간 연결을 확인합니다.

Note

네트워크 배포 요청이 실행되기 전에 명시적 승인을 받아야 합니다. [배포 승인 프로세스를 참조하세요.](#)

- 자체 배포: AWS 변환은 코드형 인프라(IaC) 템플릿을 생성합니다. CloudFormation 템플릿은 기본적으로 생성됩니다. 추가 출력 형식을 선택할 수도 있습니다.
- AWS CDK는 프로그래밍 방식의 인프라 배포를 위한 TypeScript 프로젝트를 생성합니다.
- HashiCorp Terraform은 네트워크 리소스를 관리하기 위한 HashiCorp 구성 언어(HCL) 템플릿을 생성합니다.
- Landing Zone Accelerator(LZA)는 LZA 네트워크 구성을 위한 network-config.yaml 파일을 생성합니다.

Note

Landing Zone Accelerator(LZA) 파이프라인을 통해 배포하는 경우 AWS 변환 계정과 LZA 설치가 동일한 AWS 조직에 있어야 합니다. 조직 IDs.

자체 배포의 경우 제공된 링크를 사용하여 생성된 템플릿이 포함된 zip 파일을 다운로드합니다. zip 폴더에는 생성된 템플릿을 사용하는 방법을 설명하는 README.md 파일이 포함되어 있습니다.

다운로드한 파일이 손상되거나 변조되지 않았는지 확인하려면 체크섬을 생성 및 다운로드한 다음 `openssl dgst -sha256 -binary <file.zip> | base64` 명령을 사용하여 로컬에서 생성된 해시와 비교합니다.

배포 승인 프로세스

네트워크 변경이 조직의 보안 표준 및 아키텍처 요구 사항을 준수하도록 하기 위해 모든 배포 요청은 승인 워크플로를 거칩니다. 네트워크 배포 요청이 실행되기 전에 명시적 승인을 받아야 합니다. 배포 요청을 제출하면 승인 AWS 변환 탭을 통해 승인된 승인자에게 자동으로 라우팅됩니다. 승인자는 CloudFormation 템플릿과 네트워크 구성을 모두 검증하여 보안 표준 및 아키텍처 요구 사항을 준수하는지 확인합니다. 각 제출은 새 검토 주기를 트리거하고 배포는 확인을 받은 후에만 진행됩니다. 승인자가 요청을 거부하는 경우 직접 연락하여 필요한 수정 사항에 대해 논의합니다. AWS 변환은 감사 목적으로 모든 승인 결정을 추적하고 배포 기록을 유지합니다.

배포된 네트워크 리소스 삭제

배포를 롤백해야 하는 경우 AWS Transform이 배포한 네트워크 리소스를 삭제할 수 있습니다. 배포가 완료된 직후 리소스를 삭제할 수 있습니다. 배포 후 배포된 네트워크 리소스를 수정하면 리소스를 자동으로 삭제할 수 없습니다.

- AWS 변환 관리형 배포: AWS 변환은 배포 중에 생성된 모든 CloudFormation 스택을 제거합니다. 이 작업을 수행하려면 AWS 변환 승인 탭을 통한 승인이 필요합니다.
- 자체 배포: AWS 관리 콘솔 또는 AWS CLI를 통해 배포된 리소스를 수동으로 삭제해야 합니다.

구성 파일 추출

소스 환경에서 Cisco ACI, Palo Alto Networks 또는 Fortinet FortiGate를 사용하는 경우 AWS 변환에 제공할 구성 파일을 추출해야 합니다. 이러한 파일을 독립 실행형 소스 파일로 사용하여 네트워크 인프라 및 보안 그룹을 생성하거나 RVTools 업로드와 함께 보완 파일로 사용하여 보안 그룹 생성을 추가할 수 있습니다. 추출 프로세스는 두 경우 모두 동일합니다.

방화벽 및 네트워크 환경에서 구성 파일을 추출하려면 다음 절차를 따르세요. 최신 정보는 공급업체 설명서를 참조하세요.

Fortinet FortiGate

- 펌웨어 버전은 v7.0 이상이어야 합니다.
- 글로벌 수준에서 super_admin 또는 super_admin_readonly 권한이 필요합니다.
- 단계:
 1. SSH 또는 내장 CLI 클라이언트를 통해 방화벽에 연결
 2. 실행: `show | grep "" (| grep ""`페이지 매김 비활성화)
 3. show 명령부터 모든 출력을 파일에 저장

Palo Alto Networks

- 펌웨어 버전은 10.1 이상이어야 합니다.
- 수퍼 관리자 역할이 필요합니다.
- SSH를 통해 방화벽에 연결하고, 다음 명령을 실행하여 페이지 매김을 비활성화하고, 출력 형식을 설정하고, 구성 모드로 전환하고, 구성 및 사전 정의된 객체를 내보냅니다. 출력을 저장합니다.

```
set cli pager off
set cli config-output-format set
configure
show                # Save as palo-conf.txt
show predefined     # Save as palo-default.txt
```

Cisco ACI

- 펌웨어 버전은 6.0 이상이어야 합니다.
- 모든 권한과 구성된 Secure Copy Protocol(SCP), SSH File Transfer Protocol(SFTP) 또는 File Transfer Protocol(FTP) 대상이 있는 관리자 역할이 필요합니다.
- 단계:
 1. 브라우저를 통해 APIC(Application Policy Infrastructure Controller)에 연결
 2. 관리자 메뉴를 열고 구성 롤백을 선택합니다.
 3. 스냅샷 생성 대화 상자에서 원격 위치 옵션을 선택하고 지금 스냅샷 생성을 선택합니다.
 4. “전송 성공” 메시지를 수신한 후 원격 위치 서버에 연결하고 최신 스냅샷 파일(.gz 파일)을 검색합니다.

서버 마이그레이션

AWS 변환은 AWS Transform MGN (MGN)을 사용하여 서버를 Amazon EC2로 리호스팅합니다. 마이그레이션 서버 워크플로는 각 마이그레이션 웨이브를 설정하고, 서버 인벤토리를 검증하고, 복제 에이전트를 배포하고, 데이터 복제를 모니터링하고, 마이그레이션된 인스턴스를 테스트하고, 최종 전환을 수행하는 방법을 안내합니다. 자세한 내용은 [란 무엇입니까 AWS Transform MGN?를 참조하십시오.](#) MGN 사용 설명서의 .

서버 마이그레이션은 웨이브별로 구성됩니다. 각 웨이브는 함께 마이그레이션되는 서버 그룹을 나타냅니다. 각 웨이브에 대해 다음 단계를 완료합니다.

컨테이너화 마이그레이션 전략이 있는 웨이브의 경우 AWS 변환은 아래 설명된 리호스팅 단계 대신 소스 코드 컨테이너화 워크플로를 실행합니다. 컨테이너화 워크플로는 소스 코드 복제, Docker 아티팩트 생성, 컨테이너 이미지 게시, Amazon Elastic Container Service 또는 Amazon Elastic Kubernetes Service에 배포를 안내합니다. 전체 컨테이너화 워크플로는 섹션을 참조하세요 [소스 코드 컨테이너화](#).

1. 사전 조건 및 마이그레이션 기본값 구성

2. 1단계: 마이그레이션 웨이브 설정
3. 2단계: 인벤토리 검증 및 확인
4. 3단계: 복제 에이전트 배포
5. 4단계: 데이터 복제
6. 5단계: 테스트
7. 6단계: 전환

사전 조건 및 마이그레이션 기본값 구성

사전 조건

리호스팅 마이그레이션을 시작하기 전에 다음을 준비해야 합니다.

Note

AWS 변환에서 end-to-end 마이그레이션 작업의 모든 단계를 완료하면 대상 계정과 인벤토리 파일이 이미 준비됩니다. 마이그레이션 계획 단계에서 인벤토리 파일이 자동으로 생성됩니다. 네트워크 마이그레이션 AWS 변환을 통해 설정된 네트워크 인프라도 준비됩니다. AWS 변환을 통해 네트워크 인프라를 구축하지 않은 경우 리호스팅 마이그레이션을 시작하기 전에 네트워크 인프라를 미리 설정해야 합니다.

리호스팅 마이그레이션을 시작하기 전에 서버를 호스팅할 네트워킹 리소스와 인프라가 있는지 확인합니다. AWS 변환 랜딩 존 및 네트워크 마이그레이션 기능 또는 이를 위한 기타 도구를 사용할 수 있습니다.

- 지원되는 운영 체제 - 소스 서버는 지원되는 운영 체제를 실행해야 합니다. 전체 목록은 MGN 사용 설명서의 [지원되는 운영 체제](#)를 참조하세요.
- 마이그레이션 대상 계정 - 서버를 마이그레이션해야 하는 AWS 계정 IDs. AWS 변환 랜딩 존 또는 기타 도구를 사용하여 인프라를 설정할 수 있습니다.
- 네트워크 인프라 구축 - 배포 및 구성된 VPCs, 서브넷 및 보안 그룹. AWS 변환 네트워크 마이그레이션 또는 기타 도구를 사용하여 네트워크 인프라를 설정할 수 있습니다.
- 인벤토리 파일 - 서버 세부 정보, 웨이브 할당, 대상 계정 정보 및 Amazon EC2 인스턴스 유형 기본 설정으로 준비됩니다. AWS 변환 마이그레이션 계획을 사용하여이 파일을 생성할 수 있습니다.

마이그레이션 기본값 구성

다중 계정 마이그레이션 실행을 시작하기 전에 모든 대상 계정에 적용되는 기본 설정을 구성해야 합니다. 이러한 기본값은 Amazon EC2 인스턴스를 시작하는 방법과 일반 마이그레이션을 구성하는 방법을 정의합니다. 웨이브 설정 중에 웨이브 수준에서 이러한 기본값을 재정의할 수 있습니다.

Amazon EC2 권장 사항 기본 설정

AWS 변환은 소스 VM의 사용률 사양을 기반으로 Amazon EC2 인스턴스 유형 권장 사항을 제공합니다. VMs Amazon EC2 권장 사항 기본 설정을 구성하여 마이그레이션된 서버에 대해 인스턴스 유형을 선택하는 방법을 제어할 수 있습니다.

Amazon EC2 권장 사항 생성에 대한 자세한 내용은 [에서 Amazon EC2 권장 사항 생성을 AWS Migration Hub](#) 참조하세요.

Note

[마이그레이션 평가기](#), [AWS 최적화 및 라이선스 평가\(OLA\)](#) 또는 AWS 변환 평가 작업의 권장 사항을 포함하도록 제안된 Amazon EC2 인스턴스 유형을 수정할 수 있습니다.

마이그레이션 초기화

마이그레이션을 시작하기 위해 AWS Transform은 마이그레이션하려는 모든 AWS 리전 과 서비스가 사용될 모든 대상 계정에 대해 MGN을 초기화합니다. 초기화 프로세스 중:

- 필요한 IAM 역할 및 정책이 생성됩니다.
- 필요한 기본 템플릿이 구성되어 있습니다.

초기화 프로세스에 대한 자세한 내용은 MGN 사용 설명서 [의 콘솔 AWS Transform MGN 로 초기화](#)를 참조하세요.

Amazon EC2 시작 템플릿

시작 설정에는 일반 시작 설정과의 각 소스 서버에 대해 테스트 또는 전환 인스턴스가 시작되는 방식을 결정하는 Amazon EC2 시작 템플릿의 두 부분이 포함됩니다 AWS.

Amazon EC2 시작 템플릿을 포함한 시작 설정은 계정 수준에서 정의할 수 있으며, 소스 서버를 AWS 변환 MGN에 추가할 때마다 각 소스 서버에 자동으로 적용됩니다. 이 섹션에 정의된 시작 설정 기본값은 모든 대상 계정에 자동으로 적용할 수 있습니다.

AWS 변환은 사용 가능한 시작 템플릿 설정 목록을 표시합니다. 기본값을 계속 사용하거나 시작 템플릿을 구성하도록 선택할 수 있습니다. 구성하도록 선택하면 AWS 변환은 시작 템플릿 설정의 모든 파라미터를 포함하는 human-in-the-loop(HITL) 검토에 대한 링크를 제공합니다. 원하는 파라미터에 대해 채팅 인터페이스를 통해 직접 수정할 수도 있습니다.

[소스 서버](#)는 계정 시작 템플릿 설정으로 생성됩니다. 이러한 기본 설정으로 소스 서버가 생성되면 소스 서버 시작 설정 수준에서 변경할 수 있습니다. 채팅 인터페이스를 사용하여 모든 파라미터의 소스 서버 설정을 변경하거나, 도중 인벤토리 Excel 파일을 사용하여 대량 작업을 수행할 수 있습니다. [2단계: 인벤토리 검증 및 확인](#).

시작 템플릿 설정 및 세부 정보의 전체 목록을 검토하려면 MGN 사용 설명서의 [일반 설정 시작](#)을 참조하세요.

추가 Amazon EC2 시작 템플릿 변경 사항

추가 Amazon EC2 시작 템플릿 변경 사항은 각 대상 계정의 템플릿 ID에서 수행해야 합니다. 이 옵션은 웨이브 설정 내에서 사용할 수 있습니다. AWS 변환은 이를 안내하고 적절한 링크를 제공합니다.

1단계: 마이그레이션 웨이브 설정

이 단계에서 AWS 변환은 대상 계정을 구성하고, 서비스 권한을 확인하고, 리소스 태그를 설정하고, 인벤토리에 네트워킹 데이터를 추가하고, 복제 및 시작 설정을 구성하여 마이그레이션 웨이브를 준비합니다.

마이그레이션 모드 및 계정 구성

AWS 변환은 두 가지 마이그레이션 모드를 지원합니다.

- 단일 계정 마이그레이션 - 웨이브의 모든 서버가 커넥터에 구성된 것과 동일한 대상 계정으로 마이그레이션됩니다.
- 다중 계정 마이그레이션 - 서버가 인벤토리 파일에 지정된 다른 대상 계정으로 마이그레이션됩니다. 다중 계정 마이그레이션의 경우 인벤토리 파일에 각 서버의 대상 계정 ID가 있는 `mgn:account-id` 열이 포함되어야 합니다.

AWS 변환은 대상 계정 구성을 확인하고 각 대상 계정에서 MGN이 초기화되었는지 확인합니다. MGN이 아직 초기화되지 않은 경우 AWS 변환은 초기화를 완료하기 위한 지침을 제공합니다. 초기화 중에 MGN은 복제 및 시작 작업을 위해 다음과 같은 IAM 서비스 역할을 생성합니다.

- `AWSApplicationMigrationReplicationServerRole`

- AWSApplicationMigrationConversionServerRole
- AWSApplicationMigrationMGHRole
- AWSApplicationMigrationLaunchInstanceWithDrsRole
- AWSApplicationMigrationLaunchInstanceWithSsmRole
- AWSApplicationMigrationAgentRole

이러한 역할에 대한 자세한 내용은 [MGN 사용 설명서의 콘솔을 사용하여 MGN 초기화 또는 API를 사용하여 MGN 초기화](#)를 참조하세요.

다중 계정 마이그레이션의 경우 AWS Transform은 초기화 단계 중에 다음 역할도 생성합니다. `AWSTransformRehostSharingRole_<management-or-delegated-admin-account-id>`. 이 역할은 모든 마이그레이션 대상 계정에 배포됩니다.

리소스 태그 지정 확인

서비스 권한이 확인되면 AWS 변환은 에이전트가 마이그레이션을 성공적으로 운영하는 데 필요한 모든 리소스에 적절한 태그가 지정되었는지 확인합니다. 필요한 태그가 누락된 리소스가 있는 경우 AWS 변환은 계속하기 전에 누락된 태그를 적용할 수 있는 태그 지정 페이지에 대한 링크를 제공합니다. 다음 태그가 필요합니다.

- 기존 소스 서버에는 `CreatedBy: AWSTransform` 및 태그가 있어야 합니다. `ATWorkspace: <workspace_id>`. 소스 서버에서 복제를 이미 시작하고 AWS 변환 MGN 서비스에서 생성한 경우 변환이 온프레미스 환경에서 검색된 소스 서버와 상호 연관시킬 AWS 수 있도록 이러한 서버에 태그를 지정하고 중복 소스 서버를 불필요하게 생성하지 않도록 해야 합니다. AWS 변환은 사용자가 제공한 ID, FQDN 또는 호스트 이름 키를 사용하여 이러한 서버 간에 자동으로 상호 연관됩니다.
- 복제(스테이징 영역) 및 시작 인스턴스 모두에 대해 네트워크 리소스에 적절한 태그를 지정해야 합니다. AWS 변환은 대상 계정의 전체 네트워크 리소스 목록을 표시하고 각 리소스에 이미 태그가 지정되었는지 여부를 나타냅니다. 목록을 검토하고 추가할 태그가 지정되지 않은 리소스를 선택할 수 있습니다. 선택한 각 리소스에 대해 AWS 변환은 관련 태그를 적용합니다.
 - `CreatedBy: AWSTransform` 리소스 유형에 `CreatedFor: AWSTransform` 따라 또는 .
 - `ATWorkspace: <workspace_id>`는 선택한 모든 리소스에 적용됩니다.

AWS 변환 네트워크 마이그레이션 에이전트가 생성한 VPCs 및 서브넷에는 자동으로 태그가 지정됩니다.

- VPCs 및 서브넷 외에도 AWS 변환에는 대상 계정에서 찾은 모든 기존 탄력적 네트워크 인터페이스(ENIs)도 표시됩니다. AWS 변환이 인스턴스 시작의 일부로 사용하도록 하려면 `CreatedFor:`

AWSTransform 및 로 태그를 지정해야 합니다ATWorkspace: <workspace_id>. Amazon EC2 시작 템플릿에 ENIs를 연결하거나 추가하는 방법에 대한 자세한 내용은 MGN 사용 설명서의 [세부 고려 사항을](#) 참조하세요.

인벤토리에 네트워킹 데이터 추가

AWS 변환은 네트워크 마이그레이션의 네트워킹 정보를 인벤토리 파일에 추가합니다. 이 단계에서는 네트워크 마이그레이션 단계에서 생성된 네트워크 구성을 기반으로 서버를 적절한 대상 서브넷 및 보안 그룹에 매핑합니다.

복제 및 시작 설정

복제 설정 구성

복제 설정은 소스 서버에서 데이터를 복제하는 방법을 결정합니다 AWS. 소스 서버를 AWS 변환 MGN에 추가하기 전에 복제 템플릿에서 복제 설정을 구성합니다. AWS 변환에는 모든 복제 설정 파라미터가 표시됩니다. 전용 HITL 또는 채팅 인터페이스를 통해 파라미터를 구성할 수 있습니다.

복제 설정 파라미터에 대한 자세한 내용은 MGN 사용 설명서의 [복제 설정 템플릿](#)을 참조하세요.

시작 템플릿 설정

시작 템플릿을 사용하면 AWS 변환 MGN이 인스턴스를 시작하는 방식을 제어할 수 있습니다 AWS. 템플릿에 정의된 기본 구성은 새로 추가된 모든 서버에 자동으로 적용됩니다. 전용 HITL 또는 채팅 인터페이스를 통해 시작 템플릿 설정을 구성할 수 있습니다.

시작 템플릿 설정 파라미터에 대한 자세한 내용은 MGN 사용 설명서의 [시작 템플릿](#)을 참조하세요.

AWS 또한 변환은 시작 템플릿과 연결된 Amazon EC2 시작 템플릿 ID에 대한 링크를 제공하므로 추가 Amazon EC2 시작 템플릿 속성을 변경할 수 있습니다. Amazon EC2 시작 템플릿을 편집하려면 MGN 사용 설명서의 [시작 템플릿](#)의 지침을 따르세요.

IP 할당 전략

마이그레이션된 서버에 IP 주소를 할당하는 방법을 선택합니다.

- 정적 IP - 소스 서버의 IP 주소가 유지됩니다. CIDR 변환이 필요한 경우 AWS 변환은 새 CIDR과 일치하도록 IP 주소를 자동으로 변환합니다.
- 동적 IP(DHCP) - 각 서버에는 서브넷의 IP 풀에서 새 IP 주소가 할당됩니다.

Note

네트워크 마이그레이션 중에 MAP 보안 그룹 매핑 전략을 선택한 경우 정적 IP 할당만 사용할 수 있습니다. 자세한 내용은 [보안 그룹 매핑](#)을 참조하세요.

2단계: 인벤토리 검증 및 확인

서버 데이터를 MGN으로 로드하기 전에 AWS 변환은 검토를 위해 인벤토리 파일을 준비합니다. CSV 또는 XLSX 형식으로 파일을 다운로드하고, 서버 구성을 검토하고, 필요한 경우 변경할 수 있습니다.

인벤토리 파일에는 서버 이름, 운영 체제, Amazon EC2 인스턴스 유형 권장 사항, 대상 서브넷, 보안 그룹, IP 할당 및 라이선스 옵션과 같은 세부 정보가 포함됩니다. 필수 필드는 다음과 같습니다.

- 서버 정보 - 서버 이름, VMID 및 소스 사양입니다.
- 웨이브 할당 - 마이그레이션 웨이브 그룹화.
- 애플리케이션 그룹화 - 논리적 애플리케이션 연결입니다.
- 대상 구성 - 대상 계정, 리전 및 Amazon EC2 인스턴스 유형입니다.
- 네트워크 구성 - 대상 서브넷 및 보안 그룹입니다.

파일을 수정하여 Amazon EC2 구성을 조정하고, 운영 체제 라이선스 옵션(BYOL 또는 라이선스 포함)을 변경하고, 테넌시 설정을 업데이트할 수 있습니다.

인벤토리를 검토한 후 표시된 대로 수락하거나 수정된 버전을 업로드할 수 있습니다. 그런 다음 AWS 변환은 데이터를 MGN으로 로드하여 웨이브의 각 서버에 대한 소스 서버 레코드를 생성합니다.

Note

인벤토리 파일에서 열을 제거하거나 열 헤더를 변경하지 마십시오. AWS 변환하려면 원본 파일 구조가 데이터를 올바르게 처리해야 합니다.

Note

AWS 변환을 사용하면 지정된 대상 AWS 계정과 대상으로 AWS 리전 한 번에 하나씩 가져올 수 있습니다. 둘 이상의 웨이브에서 동시에 작업하거나 동일한 대상 계정으로 실행 중인 마이

그레이션 작업이 두 개 이상 있는 경우 다른 웨이브 또는 작업에서 다른 가져오기를 수행하려면 가져오기가 완료될 때까지 기다려야 합니다.

인벤토리 파일 열 밑에서 구성을 지정하여 운영 체제 라이선스 옵션(BYOL 또는 라이선스 포함) `mgn:launch:placement:operating-system-licensing` 및 테넌시를 제어할 수 있습니다. `mgn:launch:placement:tenancy`. 자세한 내용은 MGN 사용 설명서의 [파라미터 가져오기](#)를 참조하세요.

3단계: 복제 에이전트 배포

소스 서버에서 로 데이터 복제를 시작하려면 각 소스 서버에 AWS Replication Agent를 AWS설치합니다. AWS 변환은 세 가지 설치 방법을 제공합니다.

- 조직 도구 - 조직의 기존 배포 도구(예: SCCM, Ansible 또는 Chef)를 사용하여 서버에 에이전트를 설치합니다. AWS 변환은 `--no-prompt`, `--aws-secret-access-key`, `--aws-access-key-id`,를 포함한 자동 설치를 위한 추가 파라미터와 함께 설치 명령을 제공합니다 `--aws-session-token`.
- MGN 커넥터 - MGN 커넥터를 사용하여 에이전트 설치를 자동화합니다. 커넥터는 SSH(Linux) 또는 WinRM(Windows)을 통해 소스 시스템에 연결하고 복제 에이전트를 자동으로 설치합니다. 구성되면 여러 웨이브와 다른 대상에서 커넥터를 재사용할 수 있습니다 AWS 계정. MGN 커넥터에 대한 자세한 내용은 [MGN 사용 설명서의 MGN 커넥터 설정](#)을 참조하세요.

Note

AWS 변환과 함께 MGN 커넥터를 사용하기 전에 AWS Systems Manager Fleet Manager에서 커넥터의 관리형 인스턴스에 다음 태그를 지정해야 합니다.

- 키: CreatedFor 값: AWSTransform

- 키: ATWorkspace 값: *workspace-id*

관리형 인스턴스에 태그를 지정하려면 AWS Systems Manager 콘솔을 열고 노드 도구에서 Fleet Manager로 이동하여 MGN 커넥터의 관리형 인스턴스를 선택하고 위의 태그를 적용합니다. AWS 변환 웹 앱 URL에서 워크스페이스 ID를 찾습니다 `https://.../workspace/workspace-id/job/job-id`.

- 수동 설치 - 각 소스 서버에 에이전트를 직접 설치합니다. 이 방법을 사용하려면 각 서버에 직접 액세스해야 하지만 설치 프로세스를 완전히 제어할 수 있습니다.

AWS MGN 커넥터 설정 변환

AWS 변환 MGN 커넥터는 소스 서버에 복제 에이전트를 자동으로 배포합니다. 커넥터는 온프레미스 환경의 전용 Linux 시스템에 배포된 경량 클라이언트입니다. SSH(Linux) 또는 WinRM(Windows)을 통해 소스 서버에 연결하여 복제 에이전트를 설치하고 구성하므로 여러 AWS 서비스에서 수동으로 조정할 필요가 없습니다.

커넥터 작동 방식

커넥터는 다음 구성 요소를 통해 작동합니다.

- 커넥터 클라이언트 - 환경의 전용 Linux 시스템에 배포됩니다.
- SSM 에이전트 - 보안 통신을 활성화하기 위해 동일한 시스템에 설치됩니다 AWS.
- SSM 하이브리드 활성화 - 안전한 명령 실행을 위해 커넥터 시스템을 AWS Systems Manager에 연결합니다.
- 자격 증명 관리 - AWS Secrets Manager에서 소스 서버 자격 증명을 검색합니다.

에이전트를 배포할 때 AWS 변환은 SSM 문서를 커넥터 머신으로 보냅니다. 그런 다음 커넥터는 AWS Secrets Manager에서 소스 서버 자격 증명을 검색하고, 각 소스 서버에 대한 연결을 설정하고, 소스 서버가 사전 조건을 충족하는지 확인하고, 복제 에이전트를 설치 및 구성하고, 성공적인 설치를 확인합니다.

커넥터 머신 요구 사항

요구 사항	세부 정보
운영 체제	지원되는 Linux 운영 체제입니다. 전체 목록은 MGN 사용 설명서의 MGN 커넥터 사전 조건을 참조하세요 .
네트워크 액세스	모든 소스 서버에 연결해야 함(SSH를 통한 Linux, WinRM을 통한 Windows)
인터넷 연결	AWS 엔드포인트(Systems Manager, Secrets Manager, MGN)에 대한 아웃바운드 HTTPS(443)
디스크 공간	최소 200MB 무료
권한	루트 또는 sudo 액세스

Note

커넥터는 Linux 시스템에 설치해야 하지만 Linux 및 Windows 소스 서버 모두에 에이전트를 배포할 수 있습니다.

설정 프로세스

AWS 변환은 커넥터를 설정하는 다음 단계를 안내합니다.

1단계: 커넥터 구성

커넥터의 이름을 제공하거나 자동 생성된 기본 이름을 사용합니다. 커넥터는 관리 계정 또는 MGN의 위임된 관리자 계정에 설치할 수 있습니다. 다중 계정 마이그레이션의 경우 커넥터는 멤버 계정 전반의 서버에 에이전트를 배포할 수 있습니다.

2단계: 리소스 AWS 스 설정

AWS 변환하면 자격 AWS 증명을 사용하여 브라우저에서 실행되는 설정 페이지가 열립니다. AWS 관리 계정 또는 위임된 관리자 계정으로 관리 콘솔에 로그인해야 합니다. 이 계정은 AWS 변환 대상 커넥터가 연결된 계정과 동일해야 합니다.

설정 페이지는 다음 리소스를 자동으로 생성합니다.

- IAM 역할(명동적으로 생성됨 - 이미 존재하는 경우 건너뛸):
 - `AWSEApplicationMigrationConnectorManagementRole` - 에이전트 설치 중에 자격 증명에 액세스하는 데 사용됩니다.
 - `AWSEApplicationMigrationConnectorSharingRole_<ACCOUNT-ID>` - 에이전트 설치 권한을 포함합니다.
- SSM 하이브리드 활성화 - 30일 만료 기간. 커넥터 시스템을 Systems Manager에 AWS 연결하고 보안 활성화 자격 증명을 생성합니다.

또는 설정 페이지에서 CloudFormation 템플릿을 다운로드하여 IAM 역할을 직접 배포할 수 있습니다.

설정 페이지에서는 필요한 모든 자격 증명과 구성이 포함된 한 줄 설치 명령을 생성합니다.

⚠ Important

설치가 완료될 때까지 설정 페이지를 열어 둡니다. 이를 닫으려면 프로세스를 다시 시작해야 합니다. 모든 자격 증명은 브라우저에만 존재하며 AWS 변환에 저장되지 않습니다.

3단계: 커넥터 설치

환경의 Linux 시스템에 커넥터를 설치합니다.

1. 설정 페이지에서 설치 링크를 복사합니다.
2. SSH를 선택한 Linux 시스템으로 바꿉니다.
3. 설치 명령을 붙여넣고 실행합니다.
4. 설치가 완료될 때까지 기다립니다(일반적으로 2~3분).

4단계: 소스 서버 연결

설치 후 AWS 변환은 현재 웨이브에 속하는 모든 소스 서버를 식별하여 MGN 커넥터에 자동으로 연결합니다.

5단계: 자격 증명 구성

소스 서버 자격 증명에 대한 AWS Secrets Manager ARNs을 제공합니다. AWS 변환은 세 가지 자격 증명 구성 옵션을 제공합니다.

- Linux 서버의 단일 보안 암호 - 모든 Linux 소스 서버의 SSH 키 또는 사용자 이름/암호가 포함된 하나의 공유 보안 암호입니다.
- Windows 서버의 단일 보안 암호 - 모든 Windows 소스 서버의 사용자 이름과 암호를 포함하는 하나의 공유 보안 암호입니다.
- 서버당 여러 보안 암호 - 서버 또는 서버 그룹별로 보안 암호가 다릅니다. 서버의 자격 증명이 다를 때 사용합니다. AWS 변환은 서버 목록으로 미리 채워진 CSV 파일을 생성합니다. 각 서버의 `secret_arn` 열을 작성하고 완료된 파일을 업로드합니다.

Note

두 서버 유형 모두 각각 하나의 공유 보안 암호가 있는 경우 Linux 및 Windows 단일 보안 암호 옵션을 결합할 수 있습니다. 서버별 보안 암호 옵션은 단일 보안 암호 옵션과 상호 배타적입니다.

자격 증명 보안 암호 형식입니다. 자세한 내용은 [MGN 사용 설명서의 MGN 커넥터 자격 증명을](#) 참조하세요.

```
{
  "WinConnectionProtocol": "HTTPS",
  "WinUserName": "windows_username",
  "WinPassword": "windows_password",
  "LinuxUserName": "linux_username",
  "LinuxPrivateKey": "linux_private_key",
  "LinuxHostKeyValidation": false
}
```

에이전트 배포

자격 증명이 구성되고 확인되면 AWS 변환은 복제 에이전트를 소스 서버에 배포합니다. 현재 웨이브의 모든 서버에 배포하거나 특정 서버를 선택할 수 있습니다.

각 서버의 배포 프로세스:

1. AWS 변환은 SSM을 통해 배포 명령을 커넥터로 보냅니다.
2. 커넥터는 AWS Secrets Manager에서 자격 증명을 검색합니다.
3. 커넥터는 구성된 자격 증명을 사용하여 소스 서버에 연결합니다.
4. 커넥터는 소스 서버가 복제 에이전트를 실행하는 데 필요한 모든 사전 조건을 충족하는지 확인합니다.
5. 커넥터는 복제 에이전트를 설치하고 구성합니다.
6. 커넥터는 설치 및 연결이 성공했는지 확인합니다.

현재 설치 단계, 경과 시간, 남은 예상 시간을 포함하여 서버당 상태 추적을 통해 배포 진행 상황을 실시간으로 모니터링할 수 있습니다. 서버가 실패하면 AWS 변환에 실패 이유가 표시되고 서버당 재시도 옵션이 제공됩니다. 성공적으로 배포된 서버는 실패한 서버를 재시도하는 동안 독립적으로 진행할 수 있습니다.

커넥터 재사용 및 수명 주기

후속 웨이브에 에이전트를 배포할 때 기존 커넥터를 재사용하거나 새 커넥터를 생성할 수 있습니다. AWS 변환에는 커넥터 이름, 상태(활성 또는 만료됨), 연결된 서버 수 및 하이브리드 활성화 만료 날짜가 표시된 계정에 구성된 모든 커넥터가 나열됩니다.

- 활성 커넥터 - 하이브리드 활성화는 여전히 유효합니다. AWS 변환은 새 웨이브에 대한 IAM 역할을 확인하고 자격 증명 구성을 진행합니다. 새 하이브리드 활성화는 필요하지 않습니다.
- 만료된 커넥터 - SSM Hybrid Activation이 만료되었습니다. 만료된 활성화는 갱신할 수 없습니다. 다른 커넥터를 선택하거나 새 커넥터를 생성해야 합니다.

SSM Hybrid Activations는 30일 후에 만료됩니다. 정품 인증은 Linux 시스템에 커넥터를 설치하는 경우에만 필요합니다. 커넥터가 설치되면 활성화가 만료된 후에도 커넥터를 계속 사용하여 소스 서버에 복제 에이전트를 설치할 수 있습니다. 활성화가 만료된 후 새 시스템에 커넥터를 설치해야 하는 경우 설정 프로세스를 통해 새 커넥터를 생성해야 합니다.

수동 에이전트 설치

수동 설치의 경우 먼저 AWS 자격 증명(임시 또는 영구)을 생성한 다음 각 소스 서버에 에이전트를 설치합니다.

자격 증명 옵션:

- 임시 자격 증명(권장) - AWSApplicationMigrationAgentInstallationPolicy 관리형 정책을 사용하여 IAM 역할을 생성한 다음 `aws sts assume-role`를 사용하여 임시 자격 증명을 생성합니다. 자세한 내용은 MGN 사용 설명서의 [에이전트 설치 권한](#)을 참조하세요.
- 영구 자격 증명 - AWSApplicationMigrationAgentInstallationPolicy 관리형 정책을 사용하여 IAM 사용자를 생성하고 액세스 키를 생성합니다.

설치 단계:

Linux 서버의 경우 설치 관리자를 다운로드하여 실행합니다.

```
wget -O ./aws-replication-installer-init \
  https://aws-application-migration-service-region.s3.region.amazonaws.com/latest/
linux/aws-replication-installer-init
sudo chmod +x aws-replication-installer-init
sudo ./aws-replication-installer-init --region region --user-provided-id server-
  identifier
```


Windows 서버의 경우 PowerShell을 관리자로 사용하여 적절한 설치 프로그램을 다운로드하고 실행합니다.

```
Invoke-WebRequest -Uri "https://aws-application-migration-
service-region.s3.region.amazonaws.com/latest/windows/
AwsReplicationWindowsInstaller.exe" `
-OutFile "C:\AwsReplicationWindowsInstaller.exe"
C:\AwsReplicationWindowsInstaller.exe --region region --user-provided-id server-
identifier
```

Important

--user-provided-id 파라미터가 필요합니다. *server-identifier*를 인벤토리 파일의 mgn:server:user-provided-id 열에 있는 정확한 값으로 바꿉니다. 이 식별자는 물리적 서버를 MGN 소스 서버 레코드에 연결합니다.

에이전트 설치에 대한 자세한 내용은 MGN 사용 설명서의 [Linux 에이전트](#) 및 [Windows 에이전트](#)를 참조하세요.

설치 후 AWS 변환은 서버에 INITIATING 또는 복제 상태가 표시되는지 확인하여 모든 에이전트가 성공적으로 연결되었는지 확인합니다 INITIAL_SYNC.

Note

AWS 변환은 MGN 에이전트 없는 복제를 지원하지 않습니다. 에이전트 없는 복제에 대한 자세한 내용은 MGN 사용 설명서의 [에이전트 없는 복제 개요](#)를 참조하세요.

Note

웨이브의 모든 서버에 복제 에이전트를 설치해야 합니다. 복제 에이전트를 설치하지 않는 서버의 연결을 해제하고 보관합니다. disconnect-from-service 명령을 사용하여 서버를 연결 해제하고 mark-as-archived 명령을 사용하여 연결 해제된 서버를 보관할 수 있습니다. 아카이빙 명령은 수명 주기 상태가 인 소스 서버에서만 작동합니다 DISCONNECTED.

복제와 관련된 할당량은 [MGN 사용 설명서의 MGN 서비스 할당량 제한](#)을 참조하세요.

4단계: 데이터 복제

복제 에이전트가 설치되면 데이터 복제가 자동으로 시작됩니다. AWS 변환은 연속 블록 수준 복제를 사용하여 소스 서버에서 로 데이터를 동기화합니다 AWS.

복제 프로세스는 다음 두 단계로 구성됩니다.

- 초기 동기화 - 소스 서버 데이터의 전체 사본입니다 AWS. 데이터는 구성된 대상 스토리지 유형에 따라 대상 계정의 Amazon Elastic Block Store(Amazon EBS) 스냅샷 또는 Amazon FSx for NetApp ONTAP(FSx for ONTAP) 볼륨으로 저장됩니다. 자세한 내용은 MGN 사용 설명서의 [대상 스토리지 유형을](#) 참조하세요. 기간은 데이터 볼륨 및 네트워크 대역폭에 따라 달라집니다.
- 지속적 복제 - 소스 서버 성능에 미치는 영향을 최소화하면서 변경된 블록을 지속적으로 동기화합니다. 에서 up-to-date 사본을 유지합니다 AWS.

복제 서버는 스테이징 영역 서브넷에 배포된 임시 Amazon EC2 인스턴스입니다. 소스 서버에서 복제된 데이터를 수신하고 MGN에서 자동으로 관리합니다. 자세한 내용은 MGN 사용 설명서의 [복제 서버 설정을](#) 참조하세요.

AWS 변환은 복제 진행 상황을 모니터링하고 복제 상태, 복제 지연(소스와 복제된 데이터 간의 시간 차이), 대역폭 사용량을 포함한 상태 업데이트를 제공합니다.

복제 중에 각 서버는 다음 상태를 진행합니다.

- 준비되지 않음 - 서버가 초기 동기화 프로세스를 진행 중이며 아직 테스트할 준비가 되지 않았습니다.
- 테스트 준비 완료 - 서버가 성공적으로 추가되고 데이터 복제가 시작되었습니다. 이제 테스트 또는 전환 인스턴스를 시작할 수 있습니다.

웨이브의 모든 서버가 NOT_READY 상태 이상으로 진행되면 데이터 복제 단계가 완료되고 테스트를 진행할 수 있습니다.

언제든지 개별 서버 또는 전체 웨이브에 대한 복제를 제어할 수 있습니다.

- 복제 일시 중지 - 특정 서버 또는 전체 웨이브에 대한 복제를 일시적으로 일시 중지합니다.
- 복제 재개 - 이전에 일시 중지된 복제를 재개합니다.
- 복제 중지 - 복제를 영구적으로 중지합니다. 중지된 복제는 다시 시작할 수 있지만 초기 동기화부터 시작됩니다.

5단계: 테스트

데이터 복제가 완료되면 테스트 인스턴스를 시작하여 마이그레이션된 서버를 검증한 후 최종 전환을 수행할 수 있습니다. 자세한 내용은 MGN 사용 설명서의 [테스트 인스턴스 시작](#)을 참조하세요. AWS 변환은 두 가지 테스트 옵션을 지원합니다.

- 전체 웨이브 테스트 - 웨이브의 모든 서버에 대해 테스트 인스턴스를 시작합니다.
- 선택적 테스트 - 인벤토리 파일에서 사용자가 제공한 IDs를 제공하여 선택한 특정 서버에 대해 테스트 인스턴스를 시작합니다.

AWS 변환은 복제된 데이터에서 Amazon EC2 인스턴스를 시작하고 인스턴스 IDs를 제공하므로 테스트 인스턴스에 연결하고 검증할 수 있습니다. 테스트 후 다음을 수행할 수 있습니다.

- 테스트가 성공하면 전환으로 진행합니다.
- 새 테스트 인스턴스를 시작하여 다시 테스트합니다.
- 다시 테스트하기 전에 테스트 인스턴스를 종료하고 문제를 해결합니다.

5b단계: 애플리케이션을 전환 준비 완료로 표시

테스트가 완료되고 결과에 만족하면 애플리케이션을 전환 준비 완료로 표시합니다. AWS 변환은 각 애플리케이션의 복제 상태를 검토하고 모든 복제 알림을 해결한 후 계속 진행합니다. 복제 상태가 깨끗한 애플리케이션만 전환 대상으로 표시할 수 있습니다.

6단계: 전환

전환은 프로덕션 워크로드가 이동되는 마지막 마이그레이션 단계입니다 AWS. 자세한 내용은 MGN 사용 설명서의 [전환 인스턴스 시작](#)을 참조하세요. 테스트와 마찬가지로 AWS 변환은 특정 서버에 대한 전체 웨이브 전환 또는 선택적 전환을 지원합니다.

전환 중에 AWS 변환은 복제된 최신 데이터에서 Amazon EC2 인스턴스를 시작하고 각 서버의 인스턴스 IDs를 제공합니다. 전환 인스턴스를 확인한 후 전환을 완료하면 진행 중인 소스 시스템 복제가 중지됩니다.

전환 프로세스에는 다음 단계가 포함됩니다.

1. 전환 인스턴스 시작 - AWS 변환은 선택한 서버에 대해 Amazon EC2 인스턴스를 시작합니다. 전체 웨이브 전환 또는 선택적 전환을 선택할 수 있습니다.

2. 전환 인스턴스 확인 - 시작된 인스턴스에 연결하고 올바르게 작동하는지 확인합니다.
3. 전환 완료 - 소스 시스템 복제를 중지하려면 전환을 확인합니다. 웨이브의 모든 서버를 완료하거나 특정 서버를 선택할 수 있습니다. 마무리는 복제 에이전트의 데이터 전송을 중지하고, 소스 서버에서 복제 에이전트를 제거하고, 서버 수명 주기 상태를 잠급니다. 이 작업은 쉽게 취소할 수 없습니다. 자세한 내용은 MGN 사용 설명서의 [전환 완료](#)를 참조하세요.
4. 아카이브 소스 서버(선택 사항) - 완료 후 소스 서버를 아카이브된 것으로 표시하여 계정의 소스 서버 할당량을 확보할 수 있습니다.

Important

전환을 완료하면 진행 중인 소스 시스템 복제가 중지됩니다. 마무리하기 전에 전환 인스턴스를 확인했는지 확인합니다.

Note

가동 중지 시간은 소스 종료와 전환 인스턴스 가용성 사이에 발생합니다. 그에 따라 전환 기간을 계획합니다.

서버 수명 주기 상태

마이그레이션 중에 각 서버는 다음 수명 주기 상태를 진행합니다. 자세한 내용은 MGN 사용 설명서의 [소스 서버 수명 주기](#)를 참조하세요.

- 준비되지 않음 - 서버가 초기 동기화 프로세스를 진행 중이며 아직 테스트할 준비가 되지 않았습니다.
- 테스트 준비 완료 - 데이터 복제가 시작되었으며 테스트 또는 전환 인스턴스를 시작할 수 있습니다.
- 테스트 진행 중 - 테스트 인스턴스가 현재 시작 중입니다.
- 전환 준비 - 서버가 테스트되었으며 전환 준비가 되었습니다.
- 전환 진행 중 - 전환 인스턴스가 현재 시작 중입니다.
- 전환 완료 - 서버가 전환되었습니다. 모든 데이터가 AWS 전환 인스턴스로 마이그레이션되었습니다.
- 연결 해제됨 - 서버가 MGN에서 연결 해제되었습니다.

마이그레이션 중에 언제든지 서버 상태에 대해 AWS 변환에 요청할 수 있습니다. AWS 변환은 마이그레이션 수명 주기, 복제 상태 및 권장되는 다음 단계를 포함한 모든 관련 서버 정보를 표시하는 대화형 웨이브 상태 테이블을 제공합니다. 예를 들어 다음과 같이 자연어로 질문할 수도 있습니다.

- 서버의 상태는 어떻게 됩니까?
- 파도 상태는 어떻게 됩니까?
- 현재 진행 중인 단계의 상태는 어떻게 됩니까?

웨이브 마이그레이션 중에 AWS 변환에 개별 서버의 상태를 업데이트하거나 변경하도록 요청할 수 있습니다. 예를 들어 웨이브의 서버 10개 중 9개가 테스트 단계를 통과했지만 1개가 실패한 경우 실패한 서버에서 테스트를 다시 실행하는 동안 AWS 변환이 9개의 서버를 다음 단계로 계속 이동하도록 허용할 수 있습니다.

배포 승인

일부 마이그레이션 작업은 실행 전에 명시적 승인이 필요합니다. 작업에 승인이 필요한 경우 AWS 변환은 승인 탭을 통해 승인된 승인자에게 요청을 라우팅합니다. AWS 변환에서 관리자 역할을 가진 사용자만 배포 요청을 승인할 수 있습니다. 배포는 확인을 받은 후에만 진행됩니다.

릴리스 노트

다음 릴리스 정보에서는에 대한 최신 변경 사항을 다룹니다 [마이그레이션\(VMware 포함\)](#). 지원되는 AWS 변환 리전은 [지원되는 리전을 참조하세요](#). 지원되는 대상 리전은 [계정 커넥터 설정 페이지](#)를 참조하세요.

2026년 6월

- AWS 이제 마이그레이션을 위한 변환이 현지화를 지원합니다. 마이그레이션 워크플로를 사용할 때 웹 애플리케이션의 표시 언어를 변경할 수 있습니다. [언어 설정에 대해 자세히 알아봅니다](#).
- AWS 이제 변환을 통해 마이그레이션을 위한 복제 설정 및 시작 설정을 구성할 수 있습니다. 대상 계정별 또는 특정 소스 서버 간에 구성을 설정할 수 있습니다. [복제 및 시작 설정에 대해 자세히 알아봅니다](#).
- AWS 이제 변환을 통해 기존 탄력적 네트워크 인터페이스(ENIs)를 시작 템플릿에 연결할 수 있습니다. 인스턴스가 시작될 때 사용할 수 있도록 대상 계정의 ENIs에 태그를 지정할 수 있습니다. [네트워크 리소스 태그 지정에 대해 자세히 알아봅니다](#).
- AWS 이제 마이그레이션을 위한 변환은 중동(바레인) 및 중동(UAE)을 제외한 모든 AWS 상용 리전을 마이그레이션 대상으로 지원합니다. [지원되는 대상 리전에 대해 자세히 알아봅니다](#).

2026년 5월

- AWS 이제 변환은 네트워크 마이그레이션 검토 중에 대상 계정의 기존 VPCs를 감지합니다. 매핑된 VPCs와 함께 기존 VPCs 보고, CIDR 충돌을 식별하고, 배포 전에 해결할 수 있습니다. [기존 VPC 감지에 대해 자세히 알아봅니다.](#)
- AWS 변환은 로 마이그레이션하는 동안 소스 코드 리포지토리를 컨테이너로 리플랫폼하는 것을 지원합니다 AWS. [컨테이너화에 대해 자세히 알아봅니다.](#)

2026년 4월

- 마이그레이션 워크플로 내에 직접 랜딩 존 생성을 추가했습니다. 기존 파운데이션에 대한 검사를 AWS 변환하고, 조직 단위(OU) 구조 및 대상 계정을 권장하며, 자동 배포 또는 코드형 인프라(IaC) 출력(CloudFormation AWS CDK, 또는 랜딩 존 액셀러레이터(LZA) 형식)을 제공합니다. [랜딩 존 생성에 대해 자세히 알아봅니다.](#)
- 네트워크 마이그레이션 중에 보안 그룹 매핑이 포함된 DHCP에 대한 지원이 추가되었습니다. [보안 그룹 생성에 대해 자세히 알아봅니다.](#)

2026년 3월

- 네트워크 마이그레이션을 위한 퍼블릭 APIs 추가되어 파트너 및 프로그래밍 방식으로 네트워크 마이그레이션 기능에 액세스할 수 있습니다. [네트워크 마이그레이션 API 참조](#)를 참조하세요.

2026년 2월

- 네트워크 마이그레이션은 이제 [RVTools 검색 데이터](#) 없이 [방화벽 또는 소프트웨어 정의 네트워크\(SDN\) 구성 파일](#) 수집을 지원합니다. 방화벽 또는 SDN 구성 파일을 독립적으로 사용하거나 RVTools 내보내기와 결합할 수 있습니다.

2026년 1월

- 네트워크 마이그레이션 요소에 대한 [Migration Acceleration Program\(MAP\) 태그 지정 및 사용자 정의 태그 지정](#)에 대한 지원이 추가되어 MAP 크레딧 및 조직 목적으로 마이그레이션 리소스를 추적할 수 있습니다.

2025년 12월

- 워크플로를 재설계하고 사용성을 개선하여 새로운 [마이그레이션 환경을](#) 추가했습니다. 자세한 내용은 [Accelerating VMware migration: AWS Transform의 새로운 경험을 참조하세요.](#)
- 자동 [랜딩 존 설정을 위한 랜딩 존 액셀러레이터\(LZA\) 네트워크 구성](#)이 추가되었습니다.
- 마이그레이션 실행 시 [여러 대상 AWS 계정에](#) 대한 지원이 추가되어 계정 간에 워크로드를 마이그레이션할 수 있습니다.
- [Cisco ACI, Palo Alto, FortiGate 및 ModelizeIT 소스 형식](#)에 대한 네트워크 마이그레이션 지원이 추가되었습니다.

2025년 10월

- 아시아 태평양(오사카)을 추가하여 [16개의 대상 리전](#)으로 마이그레이션 실행을 확장했습니다.

2025년 9월

- 웨이브당 기존 보유 라이선스 사용(BYOL) 또는 라이선스 포함 옵션을 지정할 수 있도록 [리호스팅](#) 웨이브의 라이선스 구성에 대한 지원이 추가되었습니다.
- [네트워크 마이그레이션에서 Terraform](#)에 대한 지원이 추가되어 Terraform 템플릿을 사용하여 네트워크 인프라를 배포할 수 있습니다.
- 복제 서브넷 구성 업데이트에 대한 지원이 추가되어 대상 계정의 기본 VPC에 대한 요구 사항이 제거되었습니다.

2025년 8월

- 미국 동부(오하이오), 유럽(스톡홀름) 및 유럽(아일랜드)을 추가하여 [15개의 대상 리전](#)으로 마이그레이션 실행(네트워크 마이그레이션 및 리호스팅)을 확장했습니다.
- 네트워크 마이그레이션을 위한 [유연한 CIDR 범위 기능이](#) 추가되어 네트워크 배포 중에 IP 주소 범위를 사용자 지정할 수 있습니다.

2025년 5월

- 의 초기 서비스 출시로 [검색마이그레이션\(VMware 포함\)](#), 평가, 마이그레이션 [계획](#), 네트워크 마이그레이션 및 서버 리호스팅을 포함한 end-to-end 마이그레이션 기능을 제공합니다.

- 미국 동부(버지니아 북부), 미국 서부(오레곤), 캐나다(중부), 남아메리카(상파울루), 유럽(프랑크푸르트), 유럽(런던), 유럽(파리), 아시아 태평양(뭄바이), 아시아 태평양(서울), 아시아 태평양(도쿄), 아시아 태평양(싱가포르), 아시아 태평양(시드니) 등 12개 [대상 리전](#)에서 마이그레이션 실행을 지원했습니다.

소스 코드 컨테이너화

AWS 변환은 로 마이그레이션하는 동안 컨테이너로 애플리케이션 리플랫폼을 지원합니다 AWS. 이 장에서는 소스 코드의 컨테이너화를 자동화하는 AWS Transform의 에이전트 AI 기능에 대해 설명합니다. 병렬로 마이그레이션하고 현대화하여 온프레미스에서 클라우드 네이티브 아키텍처로 전환하는 데 드는 시간과 복잡성을 줄일 수 있습니다. GitHub, Bitbucket, GitLab 또는 .zip 파일에서 소스 코드를 컨테이너화하고, Docker 이미지를 생성하고, Amazon Elastic Container Registry(Amazon ECR)에 게시하고, Amazon Elastic Container Service(Amazon ECS) 또는 Amazon Elastic Kubernetes Service(Amazon EKS)에 배포할 수 있습니다. 이렇게 하면 리호스팅 마이그레이션을 계획하고 실행하는 데 사용하는 것과 동일한 워크플로로 컨테이너화가 이루어집니다.

Note

소스 코드 컨테이너화는 아직 컨테이너화되지 않은 애플리케이션을 위해 설계되었습니다. 애플리케이션 소스 코드에 액세스해야 하며 기존 컨테이너화된 워크로드 마이그레이션을 지원하지 않습니다. 기존 컨테이너를 로 마이그레이션하려면 Amazon Elastic Container Service 또는 Amazon Elastic Kubernetes Service의 표준 배포 방법을 AWS사용합니다.

기능 및 주요 기능

AWS 변환은 애플리케이션을 컨테이너화하기 위한 다음과 같은 기능을 제공합니다.

- AI 기반 소스 코드 분석 - 애플리케이션 소스 코드를 분석하고 Dockerfiles 및 관련 구성 파일을 포함한 Docker 아티팩트를 자동으로 생성합니다.
- 컨테이너 이미지 빌드 및 게시 - AI 기반 Docker 빌드를 사용하여 컨테이너 이미지를 빌드 및 테스트하고 자동 취약성 스캔을 통해 Amazon Elastic Container Registry에 게시합니다.
- 코드형 인프라 생성 - 자동 검증 및 보안 스캔을 통해 Amazon Elastic Kubernetes Service(Helm 차트) 또는 Amazon Elastic Container Service(Terraform 모듈)에 대한 배포 인프라를 생성합니다.
- 프라이빗 종속성 지원 - 선택적으로 빌드의 종속성 소스로 AWS CodeArtifact 리포지토리(Maven, PyPI, npm) 및 프라이빗 Amazon ECR 기본 이미지를 구성할 수 있습니다.
- 반복 테스트 및 전환 배포 - 검증을 위해 테스트 인프라를 배포한 다음 프로덕션 전환을 위해 최종 인프라를 배포합니다.

컨테이너화 작동 방식

AWS 변환은 AI 기반 에이전트를 사용하여 채팅 기반 워크플로의 컨테이너화 프로세스를 안내합니다. AWS 변환은 소스 코드 분석, 도커 이미지 생성, 인프라 생성과 같은 특수 작업을 조정합니다. 워크플로의 주요 지점에서 계속하기 전에 출력을 검토하고 승인합니다.

VMware 마이그레이션 작업을 생성하여 소스 코드 컨테이너화에 액세스할 수 있습니다. 작업 내에서 컨테이너화를 독립 실행형 워크플로로 실행하거나 웨이브의 마이그레이션 전략이 컨테이너화로 설정된 경우 end-to-end 마이그레이션의 일부로 실행할 수 있습니다. VMware 마이그레이션에 대한 자세한 내용은 섹션을 참조하세요 [마이그레이션\(VMware 포함\)](#).

사전 조건

시작하기 전에 다음이 있는지 확인하십시오.

- AWS 변환 워크스페이스. 워크스페이스 가져오기에 대한 자세한 내용은 시작하기를 참조 [하세요](#).
- AWS CodeConnections를 통해 액세스할 수 있거나 업로드를 위해 zip 파일로 패키징된 Git 리포지토리의 애플리케이션 소스 코드입니다. 개별 파일은 1GB를 초과할 수 없으며 모든 소스 코드의 총 크기는 8GB를 초과할 수 없습니다.
- (선택 사항) 컨테이너 이미지를 게시하기 위한 Amazon ECR 리포지토리입니다. 게시할 준비가 되면 워크플로의 뒷부분에서 Amazon ECR 액세스를 구성할 수 있습니다.
- Amazon EKS 배포의 경우: 기존 Amazon EKS 클러스터 또는 필요한 인프라를 생성할 수 있는 권한.
- Amazon ECS 배포의 경우: Terraform AWS CloudFormation또는를 사용하여 Amazon ECS 클러스터, 서비스 및 관련 리소스를 생성할 수 있는 권한 AWS Cloud Development Kit (AWS CDK).

컨테이너화 워크플로

컨테이너화 워크플로는 다음 단계로 구성됩니다. AWS 변환 에이전트는 채팅 인터페이스의 각 단계를 안내합니다.

1. [the section called “1단계: 보안 고지 사항”](#) - 보안 고지 사항을 검토하고 수락합니다.
2. [the section called “2단계: 소스 코드 복제”](#) - 애플리케이션 소스 코드를 제공합니다.
3. [the section called “3단계: 컨테이너화”](#) - AI 에이전트가 코드를 분석하고 Docker 아티팩트를 생성합니다.
4. [the section called “4단계: 아티팩트 검토”](#) - 생성된 아티팩트를 검토하고 코드 변경을 승인합니다.

5. [the section called “5단계: 이미지 게시”](#) - Amazon ECR에 컨테이너 이미지를 게시합니다.
6. [the section called “6단계: IaC 생성”](#) - Amazon EKS 또는 Amazon ECS 배포 템플릿을 생성합니다.
7. [the section called “7단계: 테스트 인프라 배포”](#) - 테스트 인프라를 배포하고 검증합니다.
8. [the section called “8단계: 테스트 인프라 정리”](#) - 테스트 리소스를 분해합니다.
9. [the section called “9단계: 전환 인프라 배포”](#) - 프로덕션 인프라를 배포합니다.

컨테이너화 작업 시작

애플리케이션을 컨테이너화하려면 먼저 AWS 변환 워크스페이스에서 VMware 마이그레이션 작업을 생성합니다. 작업 내에서 독립형 컨테이너화 워크플로 또는 컨테이너화를 포함하는 end-to-end 마이그레이션 흐름을 실행하도록 선택할 수 있습니다.

- 독립 실행형 컨테이너화 - 전체 VMware 마이그레이션을 수행하지 않고 소스 코드를 컨테이너화합니다. 인프라 마이그레이션과 독립적으로 애플리케이션을 컨테이너화하려는 옵션을 선택합니다.
- 컨테이너화를 통한 End-to-end 마이그레이션 - 하나 이상의 웨이브에 할당된 컨테이너화 마이그레이션 전략을 사용하여 전체 VMware 마이그레이션 워크플로를 실행합니다. 컨테이너화 워크플로는 해당 웨이브에 대한 마이그레이션의 일부로 실행됩니다. VMware 마이그레이션에 대한 자세한 내용은 섹션을 참조하세요 [마이그레이션\(VMware 포함\)](#).

컨테이너화 작업을 시작하려면

1. 워크스페이스 랜딩 페이지에서 작업 생성을 선택합니다.
2. VMware 마이그레이션을 선택합니다.
3. 독립형 컨테이너화 워크플로를 실행할지 아니면 컨테이너화를 포함하는 end-to-end 마이그레이션 흐름을 실행할지 선택합니다.
4. AWS 변환은 로 시작하는 워크플로 단계를 안내합니다 [the section called “1단계: 보안 고지 사항”](#).

컨테이너화 권한

컨테이너화 워크플로 중에 AWS Transform은가 컨테이너 이미지를 빌드하고 인프라를 배포 AWS 계정 하는 데 사용하는 IAM 역할을 배포합니다. 워크플로를 계속하기 전에이 역할의 생성을 검토하고 승인하라는 메시지가 표시됩니다.

역할의 이름은 AWSTransformCodeBuildExecutionRole 이며 AWS CloudFormation 스택을 통해 배포됩니다. 여기에는 다음과 같은 관리형 정책이 포함됩니다.

기본 정책

컨테이너화 워크플로에 대한 핵심 권한을 제공합니다.

- Amazon S3 - aws-transform-* 버킷의 객체 읽기 및 쓰기
- Amazon ECR - 인증, 이미지 가져오기(태그 지정Project: atx-migration) 및 태그 지정 리포지토리로 이미지 푸시 CreatedBy: AWSTransform
- AWS CodeArtifact - 태그가 지정된 리포지토리에서 읽고Project: atx-migration, 리포지토리를 나열하고, 권한 부여 토큰을 얻고, 리포지토리 엔드포인트를 읽습니다. 이러한 권한은 워크플로 중에 구성된 퍼블릭 종속성 확인 및 프라이빗 종속성 소스를 모두 지원합니다.
- Amazon CloudWatch Logs - 로그 그룹 및 스트림을 생성하고 및 Amazon ECS 로그 그룹에 대한 로그 이벤트 작성
- AWS KMS - 키 설명 및 복호화(Amazon S3 via-service 조건에 해당)
- Amazon EC2 - VPC 지원 프로젝트를 위한 네트워크 인터페이스 생성 및 관리
- AWS CodeConnections - 연결을 사용하여 구성된 CodeConnections ARN을 통해 소스 코드 리포지토리에 액세스

네트워킹 정책

배포된 애플리케이션의 네트워킹 리소스를 관리합니다.

- Elastic Load Balancing - 로드 밸런서, 대상 그룹, 리스너 및 규칙 생성, 설명 및 관리(로 태그 지정CreatedBy: AWSTransform)
- Route 53 - 호스팅 영역 및 DNS 레코드 생성 및 관리
- AWS Cloud Map - 서비스 검색을 위한 네임스페이스 및 서비스 생성 및 관리(로 태그 지정CreatedBy: AWSTransform)

스토리지 정책

배포된 애플리케이션의 스토리지 리소스를 관리합니다.

- Amazon S3 - 암호화, 버전 관리, 수명 주기 및 액세스 정책을 포함한 버킷 생성 및 관리
- Amazon EFS - 파일 시스템, 탑재 대상 및 액세스 포인트 생성 및 관리(로 태그 지정CreatedBy: AWSTransform)
- Amazon EBS - 볼륨 및 스냅샷 생성 및 관리(로 태그 지정CreatedBy: AWSTransform)

AWS KMS 정책

암호화 키 작업을 관리합니다.

- 키 설명, 별칭 나열 및 키 정책 읽기
- 데이터 키 암호화, 복호화 및 생성(Amazon CloudWatch Logs, Amazon EFS, Amazon EC2 및 Amazon S3 서비스 조건 범위)

Amazon ECS 정책

컨테이너 배포를 위한 Amazon Elastic Container Service 리소스를 관리합니다.

- 클러스터, 서비스 및 작업 정의 생성 및 관리(로 태그 지정CreatedBy: AWSTransform)
- 작업 정의 등록 및 등록 취소, 작업 실행
- Amazon ECS 태스크 및 서비스에 IAM 역할 전달
- IAM 역할 정보 및 ACM 인증서 읽기
- Amazon EC2 VPCs, 서브넷, 보안 그룹 및 네트워크 인터페이스 설명

Amazon EKS 정책

Kubernetes 배포를 위한 Amazon Elastic Kubernetes Service 리소스를 관리합니다.

- Kubernetes API에 액세스, 클러스터 설명 및 추가 기능 나열
- Amazon EKS에 IAM 역할 전달

Note

모든 권한의 범위는 AWS 계정 및 로 지정됩니다 AWS 리전. AWS 변환에서 생성된 리소스는 로 태그가 지정되며CreatedBy: AWSTransform, 쓰기 작업은 해당하는 경우이 태그가 있는 리소스로 제한됩니다.

1단계: 보안 면책 조항 검토

컨테이너화 워크플로가 시작되기 전에 AWS 변환은 검토하고 수락해야 하는 보안 면책 조항을 제공합니다.

면책 조항에서 다루는 내용

컨테이너화 프로세스를 수행하려면 애플리케이션 종속성(예: npm, PyPI 또는 Maven Central과 같은 퍼블릭 레지스트리의 패키지)을 다운로드하기 위한 인터넷 액세스가 필요합니다. 보안 고지 사항은 다음을 알려줍니다.

- 빌드 환경에는 애플리케이션의 빌드 구성에 지정된 종속성을 확인하고 다운로드할 수 있는 아웃바운드 인터넷 액세스 권한이 있습니다.
- 애플리케이션에 필요한 종속성을 검토하고 조직의 보안 정책을 충족하는지 확인하는 것은 사용자의 책임입니다.
- 나중에 퍼블릭 레지스트리에서 다운로드하지 않도록 프라이빗 종속성 소스(예: AWS CodeArtifact 리포지토리 또는 프라이빗 Amazon ECR 기본 이미지)를 선택적으로 구성할 수 있습니다.

알아야 할 내용

보안 고지 사항을 검토하고 수락하려면

1. AWS 변환이 제공하는 보안 고지 사항을 읽습니다.
2. 고지 사항을 수락하여 컨테이너화 워크플로를 진행합니다.

고지 사항을 수락하면 AWS 변환은 소스 코드를 제공하는 다음 단계로 진행합니다.

Note

AWS CodeConnections 및 Amazon ECR의 커넥터 구성은 더 이상 선결제할 필요가 없습니다. AWS Transform은 필요한 경우에만 워크플로의 뒷부분에서 이러한 서비스에 대한 액세스를 구성하라는 메시지를 표시합니다. 예를 들어 Git 리포지토리에서 복제하도록 선택하면 CodeConnections를 구성하고 컨테이너 이미지를 게시할 준비가 되면 Amazon ECR 액세스를 구성합니다.

2단계: 소스 코드 복제

이 단계에서는 AWS 변환에 애플리케이션 소스 코드를 제공합니다. Git 리포지토리에서 또는 zip 파일을 업로드하여 소스 코드를 제공할 수 있습니다.

옵션 1: Git 리포지토리

Git 리포지토리에서 소스 코드를 제공할 수 있습니다. 아직 AWS CodeConnections를 구성하지 않은 경우 AWS 지금 CodeConnections ARN을 제공하라는 메시지가 변환됩니다. 두 가지 방법으로 리포지토리를 지정할 수 있습니다.

- CSV 파일 업로드 - repo_name 및 열이 있는 CSV 파일을 준비합니다. branch. 는 owner/repo-name 형식이어야 repo_name 합니다. branch 열은 선택 사항입니다. 리포지토리의 기본 브랜치를 사용하려면 비워 둡니다. 예제:

```
repo_name,branch
owner/my-app,main
owner/api-service,develop
owner/another-repo,
```

- 채팅에 리포지토리 세부 정보 제공 - CSV를 업로드하는 대신 채팅에서 리포지토리 이름(들)과 브랜치(들)를 직접 AWS 변환합니다.

AWS 변환은 각 리포지토리가 존재하고 CodeConnections 구성을 통해 액세스할 수 있는지 확인한 다음 리포지토리를 복제합니다.

Note

개별 파일은 1GB를 초과할 수 없으며 모든 리포지토리의 총 크기는 8GB를 초과할 수 없습니다. 더 빠른 처리를 위해 여러 리포지토리를 동시에 복제 AWS 합니다.

Important

여러 리포지토리에 걸쳐 있는 애플리케이션은 Git 복제 옵션을 통해 지원되지 않습니다. 애플리케이션에 여러 리포지토리의 소스 코드가 필요한 경우 zip 파일로 함께 패키징하고 대신 zip 업로드 옵션을 사용합니다.

옵션 2: Zip 파일 업로드

CodeConnections를 구성하지 않았거나 소스 코드를 직접 업로드하려는 경우 zip 파일을 업로드할 수 있습니다.

소스 코드를 zip 파일로 업로드하려면

1. 메시지가 표시되면 애플리케이션당 하나의 zip 파일을 업로드합니다. 파일을 채팅으로 드래그하거나 연결 버튼을 사용할 수 있습니다.
2. 각 zip 파일에는 하나의 애플리케이션에 대한 소스 코드가 포함되어야 합니다.
3. 개별 파일은 1GB를 초과할 수 없으며 모든 업로드의 총 크기는 8GB를 초과할 수 없습니다.

선택 사항: 프라이빗 종속성 구성

애플리케이션이 프라이빗 레지스트리의 패키지에 의존하는 경우 이 단계에서 프라이빗 종속성 소스를 구성할 수 있습니다. AWS 변환은 다음과 같은 프라이빗 종속성 유형을 지원합니다.

- AWS CodeArtifact 리포지토리 - AWS CodeArtifact에서 호스팅되는 Maven, PyPI 또는 npm 리포지토리를 구성합니다. AWS 변환에는 계정에서 선택할 수 있는 리포지토리 목록이 표시됩니다.
- 프라이빗 Amazon ECR 기본 이미지 - Dockerfiles가 프라이빗 Amazon ECR 리포지토리의 기본 이미지를 사용하는 경우 빌드 환경에서 이러한 이미지를 가져올 수 있도록 리포지토리 세부 정보를 제공합니다.

프라이빗 종속성을 구성할 때 AWS 변환은 이러한 리소스가 호스팅 AWS 계정 되는에 연결하라는 메시지를 표시합니다. 이 커넥터 구성은 프라이빗 종속성을 사용하는 경우에만 필요합니다.

컨테이너화 기본 설정 확인

소스 코드를 사용할 수 있게 되면 AWS Transform은 컨테이너화를 수행하는 방법에 대한 구체적인 지침이 있는지 묻습니다. 선택적으로 다음을 지정할 수 있습니다.

- 새 Dockerfile을 생성할지 아니면 기존 Dockerfile을 재사용할지 여부입니다.
- 모노 리포지토리에서 특정 서비스를 처리할지 아니면 모든 서비스를 처리할지 여부입니다.
- 컨테이너화 프로세스에 대한 기타 기본 설정입니다.

기본값은 다음과 같습니다.

1. Amazon Linux 2023 기본 이미지(public.ecr.aws/amazonlinux/amazonlinux:latest)를 사용합니다.
2. 리포지토리의 모든 애플리케이션을 처리합니다.
3. 기존 Dockerfile이 있는 경우 재사용하고 필요한 경우 약간 수정합니다.

기본값으로 진행하도록 확인하거나 특정 지침을 제공할 수 있습니다.

3단계: 컨테이너화

이 단계에서 AWS 변환 AI 에이전트는 애플리케이션 소스 코드를 분석하고 Docker 아티팩트를 생성합니다. AWS 변환은 애플리케이션의 구조, 종속성 및 런타임 요구 사항을 검사하여 적절한 Dockerfiles 및 관련 구성 파일을 생성합니다.

컨테이너화 중에 발생하는 일

컨테이너화 에이전트는 다음 작업을 수행합니다.

1. 소스 코드 분석 - AWS 변환은 애플리케이션의 프로젝트 파일, 종속성, 빌드 구성 및 런타임 요구 사항을 검사합니다. AWS 또한 변환은 하드코딩된 값(예: 데이터베이스 IP 주소 또는 DNS 이름)을 대체하고, 환경 변수를 식별하고, 볼륨을 감지하고, 로그를 표준 출력으로 리디렉션하려고 시도합니다.
2. Dockerfile 생성 - 분석을 기반으로 AWS 변환은 애플리케이션에 맞는 Dockerfile을 생성합니다.
3. 컨테이너 이미지 빌드 및 테스트 - AWS 변환은 컨테이너 이미지를 빌드하고 테스트를 실행하여 Dockerfile이 작업 이미지를 생성하는지 확인합니다. 빌드에 실패하면 AWS 변환은 Dockerfile에서 자동으로 반복합니다.
4. 보안 분석 - AWS 변환은 생성된 아티팩트에서 자격 증명, API 키 또는 기타 민감한 데이터와 같은 하드 코딩된 값을 스캔하고 검토를 위해 결과에 플래그를 지정합니다.

여러 서비스와 함께 여러 리포지토리 또는 모노리포지토리를 제공한 경우는 각 서비스를 병렬로 처리합니다.

지원되는 애플리케이션 유형

AWS 변환은 다음 애플리케이션 유형의 컨테이너화를 지원합니다.

- .NET 7 이상 - 버전 7 이상에서 실행되는 .NET 애플리케이션에 최적화된 컨테이너화.
- 일반 애플리케이션 - Java, Python, Node.js, Go 등을 포함한 모든 언어 또는 프레임워크로 빌드된 애플리케이션을 위한 컨테이너화입니다.
- 지원되지 않는 애플리케이션 - Windows, Xcode 또는 독점 빌드 환경은 지원되지 않습니다.

알아야 할 내용

이 단계는 자동으로 실행됩니다. AWS 변환은 각 애플리케이션을 분석하고 컨테이너화할 때 진행률 업데이트를 표시합니다. AWS 변환에 문제가 발생하면 설명이나 추가 정보를 요청할 수 있습니다.

컨테이너화가 완료되면 AWS 변환은 생성된 아티팩트를 검토하는 다음 단계로 이동합니다. 출력은 아티팩트 스토어에 저장됩니다.

4단계: Docker 아티팩트 및 코드 변경 사항 검토

이 단계에서는 변환이 컨테이너화 중에 AWS 생성한 Docker 아티팩트 및 코드 변경 사항을 검토합니다.

Git 리포지토리의 변경 사항 검토

Git 리포지토리에서 소스 코드를 제공한 경우 AWS 변환은 컨테이너화 변경 사항을 각 리포지토리의 새 브랜치에 커밋합니다. 리포지토리가 여러 개 있는 경우 AWS 변환은 모든 변경 사항을 통합 검토를 위한 배치로 표시합니다.

변경 사항을 검토하고 승인하려면

1. AWS 변환이 제공하는 코드 차이 링크를 검토합니다. 각 diff에는 Dockerfiles, 구성 파일 및 소스 코드 변경 사항을 포함하여 추가되거나 수정된 모든 파일이 표시됩니다.
2. AWS 변환에 승인 대화 상자가 표시되면 변경 사항을 승인하거나 거부합니다. 여러 리포지토리의 경우 단일 배치 작업의 모든 변경 사항을 승인합니다.
3. 승인하면 AWS 변환은 리포지토리의 새 브랜치에 변경 사항을 푸시합니다.
4. 다음 단계로 진행할 준비가 되었는지 확인합니다.

zip 업로드의 변경 사항 검토

소스 코드를 zip 파일로 업로드한 경우 AWS 변환은 컨테이너화된 아티팩트에 대한 다운로드 링크를 제공합니다. 생성된 Dockerfiles 및 소스 코드 수정 사항이 포함된 아티팩트를 다운로드하고 검토합니다.

변경 요청

생성된 아티팩트를 수정해야 하는 경우 업데이트된 지침에 따라 컨테이너화 단계를 다시 시작하고 검토를 위해 새 아티팩트를 생성하는 AWS 변환에 피드백을 제공할 수 있습니다.

5단계: 이미지 게시

이 단계에서 AWS 변환은 컨테이너 이미지를 Amazon Elastic Container Registry에 게시합니다. Amazon ECR 액세스를 아직 구성하지 않은 경우 AWS 지금 Amazon ECR 리포지토리 세부 정보를 제공하라는 메시지가 변환됩니다.

게시 중에 발생하는 일

AWS 변환은 각 컨테이너 이미지에 대해 다음 작업을 수행합니다.

1. 커넥터 구성 - Amazon ECR 액세스를 아직 구성하지 않은 경우 AWS 변환은 Amazon ECR 리포지토리 ARN을 제공하고 연결하는 커넥터 양식을 제공합니다 AWS 계정.
2. 승인 요청 - AWS 변환은 게시할 이미지 목록을 표시하고 승인을 요청합니다. 게시 작업을 승인하거나 거부할 수 있습니다.
3. 이미지 푸시 - 승인 후 AWS 변환은 사용하여 컨테이너 이미지를 Amazon ECR 리포지토리에 게시합니다. 서비스가 여러 개 있는 경우 AWS 변환은 모든 이미지를 단일 배치 작업으로 게시합니다.
4. 취약성 스캔 - Amazon ECR은 게시된 이미지에서 알려진 취약성을 자동으로 스캔합니다. AWS 변환은 스캔 결과를 보고합니다. 보다 포괄적인 분석을 위해 AWS ECR 고급 스캔 및 AWS GuardDuty 런타임 모니터링을 활성화합니다.

Note

이미지 게시는를 사용하여 비동기적으로 실행됩니다. 게시 중에 세션이 중단되면 다시 연결하면 AWS 변환이 작업을 자동으로 복구합니다.

알아야 할 내용

- 게시할 이미지 목록을 검토합니다.
- 게시 작업을 승인하거나 거부합니다. 거부하면 AWS 변환은 이미지 게시를 건너뛰고 게시된 이미지 없이 다음 단계로 진행할 수 있습니다.
- 게시가 완료된 후 취약성 스캔 결과를 검토합니다.

게시 후 AWS Transform은 인프라 배포 단계에서 사용되는 이미지 URIs를 제공합니다.

6단계: 코드형 인프라 생성

이 단계에서 AWS 변환은 컨테이너화된 애플리케이션을 배포하기 위한 AWS 인프라 템플릿을 생성합니다. Amazon Elastic Kubernetes Service와 Amazon Elastic Container Service 중에서 대상 플랫폼으로 선택합니다.

Amazon Elastic Kubernetes Service(Kubernetes)

Amazon EKS를 선택하면 AWS 변환은 애플리케이션에 대한 Kubernetes 매니페스트가 있는 차트 Helm을 생성합니다. 생성된 템플릿에는 다음이 포함됩니다.

- 배포 및 서비스
- 수신 규칙
- ConfigMaps 및 SecretProviderClass 리소스
- 서비스 계정
- 영구 볼륨 클레임(EBS 및 EFS)
- Route 53 DNS 레코드
- 상태 확인 구성

선택 사항: CloudWatch 로깅

AWS 변환은 Amazon EKS 배포에 CloudWatch 로깅을 포함할지 묻습니다. 옵트인하면 AWS 변환은 포드 로그를 수집하여 CloudWatch Logs로 전송하는 Fluent Bit DaemonSet 구성을 생성합니다.

CloudWatch 로깅을 선택하는 경우 클러스터 관리자는 배포 전에 다음 사전 조건을 완료해야 합니다.

1. 클러스터에서 amazon-cloudwatch 네임스페이스를 생성합니다.
2. CloudWatch Logs 쓰기 권한을 사용하여 Fluent Bit 서비스 계정에 대한 IAM 역할을 생성합니다. 배포 중에 역할 ARN을 입력하라는 메시지가 표시됩니다.

Amazon Elastic Container Service(Terraform)

Amazon ECS를 선택하면 AWS 변환이 애플리케이션을 배포하기 위한 Terraform 모듈을 생성합니다. 생성된 템플릿에는 다음이 포함됩니다.

- ECS 클러스터

- 작업 정의가 있는 ECS 서비스
- 액세스 로깅이 포함된 Application Load Balancer
- 영구 스토리지용 Amazon EFS
- 서비스 검색을 위한 프라이빗 호스팅 영역
- 상태 확인 구성

자동 검증 및 보안 스캔

AWS 변환은 생성된 인프라 템플릿을 제시하기 전에 자동으로 검증합니다. 검증에는 다음이 포함됩니다.

- Terraform: terraform fmt 및 terraform validate의 경우 구문 및 구성 정확성을 확인합니다.
- Helm의 경우: 생성된 매니페스트의 형식이 올바른지 확인하기 위한 차트 검증입니다.
- Checkov를 사용하여 생성된 인프라 코드에서 잠재적인 보안 구성 오류를 식별하는 보안 스캔입니다.

AWS 변환은 계속하기 전에 모든 검증 문제를 보고하고 해결합니다.

게시된 이미지 없이 IaC 생성

이전 단계에서 컨테이너 이미지를 게시하지 않은 경우에도 인프라 템플릿을 생성할 수 있습니다. 생성된 템플릿은 나중에 실제 이미지 위치로 업데이트할 수 있는 자리 표시자 이미지 URIs를 사용합니다.

알아야 할 내용

인프라 템플릿을 생성하려면

1. 메시지가 표시되면 대상 플랫폼인 Amazon EKS 또는 Amazon ECS를 선택합니다.
2. Amazon EKS를 선택한 경우 AWS 변환은 CloudWatch 로깅을 포함할지 여부를 묻습니다. 예 또는 아니요로 응답합니다.
3. 메시지가 표시되면 애플리케이션의 상태 확인 엔드포인트 세부 정보(예: /health 경로)를 제공합니다.
4. AWS 변환은 인프라 템플릿을 생성하고 검증합니다. 이 단계는 자동으로 실행되며 AWS 변환에는 검증 또는 보안 스캔 결과를 포함한 진행 상황 업데이트가 표시됩니다.
5. AWS 변환에서 템플릿을 표시할 때 생성된 템플릿을 검토합니다.

7단계: 테스트 인프라 배포

이 단계에서 AWS 는 Transform이 테스트 인프라를 배포하므로 프로덕션 전환 전에 컨테이너화된 애플리케이션을 검증할 수 있습니다.

테스트 배포 중에 발생하는 일

AWS 변환은 이전 단계에서 생성된 인프라 템플릿에 배포합니다 AWS 계정. Amazon EKS 배포의 경우 Helm을 사용합니다. Amazon ECS 배포의 경우 Terraform을 사용합니다.

배포하기 전에 AWS 변환은 리소스 이름, 복제본 수 및 환경별 설정과 같은 배포 파라미터를 구성할 수 있는 인프라 값 양식을 제공합니다. AWS 변환은 생성될 리소스를 보여주는 배포 미리 보기도 생성하므로 승인 전에 변경 사항을 검토할 수 있습니다.

알아야 할 내용

테스트 인프라를 배포하고 검증하려면

1. 배포 구성으로 인프라 값 양식을 작성합니다. 양식에는 클러스터 이름, 네임스페이스, 복제본 수 및 기타 환경별 설정과 같은 파라미터가 포함됩니다.
2. 생성 또는 수정할 리소스를 보여주는 배포 미리 보기를 검토합니다.
3. AWS Transform이 인프라 배포를 요청할 때 인프라 배포를 승인합니다.
4. 배포가 완료될 때까지 기다립니다. AWS 변환은 배포 결과를 표시합니다.
5. 배포된 애플리케이션을 테스트하여 컨테이너에서 올바르게 실행되고 인프라가 요구 사항을 충족하는지 확인합니다.
6. 배포에 만족하는지 또는 인프라를 수정하고 재배포할지 여부를 AWS 변환에 알립니다.

인프라에서 반복

인프라 템플릿을 수정해야 하는 경우 업데이트된 템플릿을 업로드하고 재배포할 수 있습니다.

1. AWS 변환에 IaC를 수정하도록 지시합니다.
2. 수정된 인프라 템플릿이 포함된 zip 파일을 업로드합니다.
3. AWS 변환은 템플릿을 대체하고 종분 업데이트(Terraform 적용 또는 Helm 업그레이드)를 수행합니다.
4. 업데이트된 배포 결과를 검토합니다.

배포에 만족할 때까지이 주기를 반복할 수 있습니다.

세션 복구

인프라 배포를 사용하여 비동기적으로 실행됩니다. 배포 중에 세션이 중단되면 다시 연결하면 AWS 변환이 자동으로 작업을 복구하고 배포 결과를 표시합니다.

8단계: 테스트 인프라 정리

검증을 완료하면 AWS 변환은 불필요한 비용을 방지하기 위해 테스트 인프라를 해체합니다.

알아야 할 내용

테스트 인프라를 정리하려면

1. AWS 변환은 테스트 인프라가 손상됨을 알려줍니다.
2. AWS Transform이 요청하면 삭제 작업을 승인합니다.
3. 정리가 완료될 때까지 기다립니다. AWS 변환은 모든 테스트 리소스가 제거되면 결과를 표시합니다.

Amazon ECS 배포의 경우이 단계에서는 컴퓨팅 리소스, 로드 밸런서, 스토리지 및 네트워킹 구성 요소를 포함하여 테스트 배포 중에 생성된 모든 리소스를 제거합니다.

Amazon EKS 배포의 경우 정리는 레이블에 따라 특정 프로젝트에 따라 범위가 지정됩니다. 이 컨테이너화 워크플로에 대해 태그가 지정된 리소스만 제거됩니다. 동일한 Amazon EKS 클러스터에서 실행되는 다른 워크로드는 영향을 받지 않습니다.

9단계: 전환 인프라 배포

이 마지막 단계에서 AWS Transform은 프로덕션용 최종 인프라를 배포합니다. 전환 배포는 테스트 배포 단계에서 검증한 것과 동일한 인프라 템플릿을 사용합니다.

알아야 할 내용

전환 인프라를 배포하려면

1. 프로덕션 배포 구성으로 인프라 값 양식을 작성합니다. 테스트 배포에서 파라미터를 조정하거나 동일한 값을 사용할 수 있습니다.

2. 생성될 프로덕션 리소스를 보여주는 배포 미리 보기를 검토합니다.
3. AWS 변환이 요청하면 프로덕션 배포를 승인합니다.
4. 배포가 완료될 때까지 기다립니다. AWS 변환은 전환 배포 결과를 표시합니다.
5. 프로덕션 환경에서 애플리케이션이 올바르게 실행되고 있는지 확인합니다.

Important

팀과 함께 생성된 인프라 구성을 검토하여 조직의 보안, 규정 준수 및 비즈니스 요구 사항을 충족하는지 확인합니다. AWS 변환은 자동 구성 권장 사항을 제공하지만 전환 배포를 진행하기 전에 필요에 맞게 설정을 검증하고 조정할 책임은 사용자에게 있습니다.

세션 복구

프로덕션 배포는를 사용하여 비동기적으로 실행됩니다. 배포 중에 세션이 중단되면 다시 연결하면 AWS 변환이 자동으로 작업을 복구하고 배포 결과를 표시합니다.

메인프레임 애플리케이션의 현대화

AWS 변환은 레거시 메인프레임 애플리케이션의 현대화를 가속화하도록 설계되었습니다. 메인프레임 코드베이스 분석을 오케스트레이션하고, 설명서를 생성하고, 비즈니스 로직을 추출하고, 모놀리식 구조를 분해하고, 레거시 코드를 변환하고, 필요한 경우 인적 입력(HITL)을 사용하여 전체 여정을 관리합니다. 메인프레임 애플리케이션을 현대화하고 마이그레이션하기 위한 AWS Transform의 변환 기능을 사용하면 변환 프로세스 전반에 걸쳐 비즈니스 크리티컬 로직을 유지하면서 중요한 메인프레임 애플리케이션을 더 빠르게 현대화할 수 있습니다.

주제

- [기능 및 주요 기능](#)
- [개괄적인 연습](#)
- [루프의 사람\(HITL\)](#)
- [메인프레임 애플리케이션의 변환에 지원되는 파일 유형](#)
- [메인프레임 AWS 변환에 지원되는 리전 및 할당량](#)
- [메인프레임 현대화 여정에 대한 개략적인 개요](#)
- [메인프레임 애플리케이션의 변환](#)
- [리팩터링 후 현대화된 애플리케이션 구축 및 배포](#)

기능 및 주요 기능

AWS 변환은 메인프레임 현대화를 위해 다음과 같은 기능을 제공합니다.

- 연결된 JCL(작업 제어 언어), CICS(고객 정보 제어 시스템) 트랜잭션, BMS(기본 매핑 지원) 화면, Db2 데이터베이스 및 VSAM(가상 스토리지 액세스 방법) 데이터 파일을 사용하여 COBOL(일반 비즈니스 지향 언어) 및 PL/I(프로그래밍 언어 1)로 작성된 z/OS 메인프레임 애플리케이션의 현대화를 지원합니다.
- PSAM(Presentation Service Access Method), 일본어 문자 집합 및 NDB(Network Data Base) 데이터 파일을 사용하여 Fujitsu GS21 메인프레임 애플리케이션의 리팩터링을 지원합니다.
- 목표 기반 추론, 분석, 분해, 계획, 문서 생성 및 코드 리팩터링을 수행합니다.
- COBOL 기반 메인프레임 워크로드를 클라우드에 최적화된 최신 Java 애플리케이션으로 자동 리팩터링합니다.
- 분석, 설명서, 분해, 계획 및 코드 리팩터링을 실행하는 기본 도구를 원활하게 오케스트레이션하고 통합합니다.

- ready-to-use 수 있는 코드형 인프라(IaC) 템플릿을 제공하여 현대화된 메인프레임 애플리케이션을 위한 클라우드 환경을 설정할 수 있습니다.

개괄적인 연습

다음은 메인프레임 애플리케이션을 현대화하고 마이그레이션하기 위한 AWS 변환에 대한 개략적인 안내입니다.

1. AWS 변환으로 채팅을 시작하고 목표를 입력합니다.
2. 목표에 따라 AWS 혁신은 높은 수준의 목표를 중간 단계로 나누는 현대화 계획을 제안합니다.
3. 제공한 목표에 따라 AWS 변환은 다음을 수행할 수 있습니다.
 - 코드베이스 평가 및 재구상
 - 목표에 따라 사용자 지정 작업 생성

그 과정에서 AWS 변환은 작업을 실행하기 위해 사용자에게 정보를 요청할 수 있습니다.

Note

메인프레임 리팩터링 기능을 위한 AWS 변환에 대한 자세한 내용은 메인프레임 리팩터링을 위한 AWS 변환 설명서의 [프로젝트 생성](#)을 참조하세요.

루프의 사람(HITL)

메인프레임 애플리케이션의 변환 전반에 걸쳐 변환 웹 경험을 통해 AWS 변환 작업의 진행 상황과 상태를 모니터링할 수 있습니다.

AWS 변환은 다음 시나리오에서 사용자로부터 추가 정보를 수집합니다.

- 작업을 실행하는 데 추가 정보가 필요한 경우.
- 중간 아티팩트(예: 도메인 분해 또는 웨이브 계획)에 대한 승인이 필요한 경우.
- 문제가 발생하여 AWS 변환이 자동으로 해결되지 않는 경우.

메인프레임 애플리케이션의 변환에 지원되는 파일 유형

z/OS에 지원되는 파일 유형은 다음과 같습니다.

- COBOL 아티팩트 및 관련 CPY(Copybooks)
- PL/I 소스 파일
- JCL(작업 제어 언어) 및 JCL 절차(PROC)
- CICS 시스템 정의(CSD)
- BMS(기본 매핑 지원)
- Db2 데이터베이스
- VSAM(가상 스토리지 액세스 방법)
- IMS TM(트랜잭션 관리자)

Fujitsu GS21에 지원되는 파일 유형은 다음과 같습니다.

- PSAM(프레젠테이션 서비스 액세스 방법)
- ADL(AIM 정의 언어)
- NDB(네트워크 데이터베이스)

Fujitsu GS21에 대한 자세한 내용은 AWS 메인프레임용 변환 마이그레이션 가이드에서 다음 주제를 참조하세요.

- [GS21](#)
- [캡처 및 재생 - GS21 터미널](#)
- [메인프레임, AS400, Open VMS 및 GS21](#)

메인프레임 AWS 변환에 지원되는 리전 및 할당량

지원되는 리전 목록은 [섹션을 참조하세요](#) [에 지원되는 리전 AWS Transform](#).

Note

AWS 변환을 사용하는 리전과 다른 리전에서 데이터가 처리될 수 있습니다. 리전 간 처리에 대한 자세한 내용은 [섹션을 참조하세요](#) [the section called “교차 리전 처리”](#).

할당량 한도는 [섹션을 참조하세요](#) [할당량](#).

메인프레임 현대화 여정에 대한 개략적인 개요

메인프레임 애플리케이션을 로 현대화 AWS 하는 작업은 일반적으로 (a) 평가, (b) 동원, (c) 마이그레이션 및 현대화, (d) 운영, 최적화 및 혁신의 4단계로 이루어집니다. 이러한 각 단계는 현대화 여정을 지원하기 위한 목표 및 관련 활동과 함께 자세히 설명됩니다.

단계

- [1단계: 평가](#)
- [2단계: 동원](#)
- [3단계: 마이그레이션 및 현대화](#)
- [4단계: 운영, 최적화 및 혁신](#)

1단계: 평가

목표: 현대화 준비 상태를 이해하고 초기 현대화 계획을 개발합니다.

AWS Transform을 사용하면 메인프레임 애플리케이션, 인프라 및 운영을 평가하여 비즈니스 요구 사항에 적합한 현대화 접근 방식을 결정할 수 있습니다.

Note

각 단계에는 메인프레임 애플리케이션을 현대화할 때 수행할 수 있는 가능한 모든 활동의 목록이 포함되어 있습니다. 사용 사례 또는 목표에 맞지 않는 일부 활동은 건너뛸 수 있습니다.

활동

- 현대화에 대한 비공식 대화로 시작하고 방에 적합한 사람을 확보하여 기회 검증을 수행합니다.
- 기회 검증 결정
- 애플리케이션 종속성 매핑 계획 및 애플리케이션 아키텍처를 사용하여 최초 통화 프레젠테이션 수행
- 마이그레이션 중 인프라 비용, 마이그레이션 인건비, 프로덕션 후 비용, 프로젝트 기간이 포함된 ROM(거의 크기 순서) 결정
- 신속한 포트폴리오 감지:
 - 패턴 및 도구 지침 평가 실행

- 소스 코드 분석 수행
- 개념 증명(POC) 후보 식별
- 기술 지원 교육 생성:
 - 침수 일수
 - 일반 주제가 포함된 워크숍
- 대규모 메인프레임 현대화 프로젝트 또는 신규 AWS 고객을 위한 마이그레이션 준비 상태 평가 (MRA) 보고서 생성
- 동원 단계에 대한 작업 명세서 생성

2단계: 동원

목표: 성공적인 개념 증명 또는 파일럿 현대화를 통해 기반을 구축하고 접근 방식을 검증합니다.

동원 단계를 사용하면 메인프레임 현대화를 대규모로 지원하는 데 필요한 프레임워크, 도구 및 프로세스를 설정할 수 있습니다.

활동

- 파일럿과 식별된 POC로 현대화 계획을 시작합니다.
 - 파일럿 분석 및 현대화를 위한 코드 설정
 - 파일럿 현대화 데이터 구축 및 테스트
 - 결과를 제공하고 파일럿을 검토하여 대규모 데이터 현대화를 위한 세부 솔루션을 생성합니다.
- 플랫폼의 경우:
 - 보안, 규정 준수 및 모니터링 계획 생성
 - AWS 메인프레임 랜딩 존 및 계정 구조를 사용하여 랜딩 존 환경 설정
 - 아키텍처 인프라, 애플리케이션, 통합 등을 결정합니다.
- 사람과 프로세스에 대해 생각해 보세요.
 - Cloud Center of Excellence는 좋은 리소스입니다.
 - 작업 모델
- 다양한 애플리케이션 시나리오에 대한 포괄적인 포트폴리오 분석을 생성합니다.
 - 상위 수준 설명서가 포함된 포괄적인 검색
 - 분해 계획(모든 애플리케이션용)
 - 모든 애플리케이션에 대한 패턴 및 도구 지침

- 초기 현대화 및 마이그레이션 계획 수립
- 파일럿, 플랫폼, 인력 및 프로세스, 포괄적인 포트폴리오 분석을 고려한 상세한 솔루션 생성
- 비즈니스 사례 결정
- 다음 단계의 작업 설명을 위한 솔루션으로 성공적인 파일럿 완료

3단계: 마이그레이션 및 현대화

목표: 계획된 일정 및 예산 내에서 현대화 및 마이그레이션을 완료합니다.

이 단계에서는 메인프레임 애플리케이션과 데이터를 마이그레이션하고 현대화할 수 있습니다 AWS.

활동

- 프로덕션 지원 애플리케이션 코드에 리소스 할당
- 기존 설명서를 사용하거나 주제 전문가(SMEs).
- 테스트 시나리오 정의
- 적절한 런타임, 데이터베이스 및 타사 소프트웨어를 사용하여 현대화 환경 설정
- 소스 코드 및 데이터를 마이그레이션하고 현대화합니다.
 - 애플리케이션 코드베이스의 비즈니스 도메인을 기반으로 애플리케이션을 반복적으로 현대화할 수 있습니다.
 - 필요에 따라 현대화 환경을 확장하여 현대화 워크로드 지원
- CI/CD(지속적 통합, 지속적 전달) 파이프라인 설정
- 선택한 워크로드를 마이그레이션하여 현대화를 시작합니다.
- 애플리케이션 프로그램을 전송하고 필요에 따라 환경 조정을 조정합니다.
 - 필요에 따라 환경을 확장하거나 축소할 수 있습니다.
 - 코드 안정성 테스트를 실행하여 작업 패키지 현대화
 - 필요에 따라 소스 코드와 재동기화
- 포괄적인 테스트를 실행하고 마이그레이션을 확인합니다.
 - 초기 상태 데이터 수집
 - 메인프레임에서 테스트 시나리오 기록
 - 스테이지 환경, 애플리케이션 및 데이터
 - 클라우드에서 테스트 시나리오 실행

- 소스 및 대상 테스트 결과 비교
- 자동화된 테스트 시나리오 실행 파이프라인 구축
- KPIs 및 보고서 생성
- 프로덕션 설정을 위한 데이터 검증
- 다음을 통해 진행 상황을 검증합니다.
 - 통합 및 시스템 테스트 실행
 - 성능 테스트 실행
 - 사용자 수락 테스트 실행
 - HA/DR 테스트 실행
- 애플리케이션 소유자와 함께 롤아웃 계획을 정의하고 교육 및 지식 이전을 위한 계획을 생성합니다.
- 전환 고려 및 프로덕션 전환 실행
- 애플리케이션 기능에 대한 운영, 모니터링, 기능 계획 및 보증과 같은 프로덕션 후 활동에 대한 지속적인 지원을 설정합니다.

4단계: 운영, 최적화 및 혁신

목표: 현대화된 애플리케이션의 운영 우수성과 지속적인 개선을 지원합니다.

현대화 후에는 혁신을 위해 AWS 서비스를 활용하면서 애플리케이션의 성능, 보안 및 비용을 최적화할 수 있습니다.

활동

- 애플리케이션을 모니터링하여 다음을 수행합니다.
 - 성능 지표
 - 보안 관행
 - 규정 준수 지침
 - 비용
- 로깅 세부 정보
- 애플리케이션 작업 관리:
 - 인프라 관리
 - 트랜잭션 및 작업 관리
 - 런타임 환경 지원

- 애플리케이션 최적화 및 현대화
- 애플리케이션 개발 및 유지 관리:
 - 코딩 IDE
 - 빌드
 - 통합
 - 테스트
 - 배포

메인프레임 애플리케이션의 변환

AWS 변환은 메인프레임 현대화 애플리케이션의 변환을 가속화합니다. 이 주제에서는 사용 가능한 기능에 대해 설명합니다.

주제

- [사전 조건: S3에서 프로젝트 입력 준비](#)
- [메인프레임 소스 아티팩트 컬렉션](#)
- [로그인 및 작업 생성](#)
- [변환 진행 상황 추적](#)
- [커넥터 설정](#)
- [작업 계획 평가 및 재구상](#)
- [작업 계획 재구상](#)
- [사용자 지정 작업 계획](#)

사전 조건: S3에서 프로젝트 입력 준비

AWS 변환은 복잡한 메인프레임 코드베이스를 처리할 수 있습니다. 코드베이스를 사용하려면 S3 위치에 모든 자산이 있어야 합니다.

주요 프로젝트 입력:

- 소스 코드: 메인프레임 소스 코드 파일을 S3에 업로드해야 합니다. 여기에는 COBOL 프로그램, JCL 스크립트, 카피북 및 기타 관련 소스 파일이 포함됩니다.
- 데이터 파일: 메인프레임 애플리케이션에서 사용하는 VSAM 파일 또는 기타 데이터 파일이 있는 경우 S3에 업로드해야 합니다.

- 구성 파일: 메인프레임 환경과 관련된 구성 파일을 포함합니다.

기타 프로젝트 입력

- 시스템 관리 시설(SMF) 레코드: 해당하는 경우 소스 코드가 저장된 S3 버킷의 새 폴더에 SMF 레코드를 업로드합니다. 이러한 레코드는 .zip 파일 형식이어야 합니다.
- 형식 지정: 기술 설명서 생성의 경우 선택적 구성 파일을 활용하여 헤더, 바닥글, 로고 및 사용자 지정 정보를 포함하여 필요한 형식 및 표준에 맞는 PDF 문서를 생성할 수 있습니다.
- 용어집: AWS 변환은 문서 생성 및 비즈니스 규칙 추출을 위해 생성형 AI를 통한 자동화를 AWS 활용합니다. zip 파일의 루트 디렉터리에 중요한 약어 및 용어에 대한 정보가 포함된 용어집 CSV 파일을 포함하면 생성된 설명서 품질을 개선하는 데 도움이 됩니다.
- 테스트 데이터: 사용 가능한 경우 현대화된 애플리케이션을 검증하는 데 사용할 수 있는 테스트 데이터 세트를 업로드합니다. 이 데이터는 소스 코드가 저장된 S3 버킷의 새 폴더에 저장되어야 합니다.

프로젝트 입력에 대한 자세한 내용은 [여기에서](#) 확인할 수 있습니다.

메인프레임 소스 아티팩트 컬렉션

이 주제에서는 AWS 변환을 사용하여 메인프레임 현대화 이니셔티브를 지원하기 위해 메인프레임 소스 코드 및 관련 아티팩트를 수집하는 프로세스를 간략하게 설명합니다. 소스 아티팩트의 적절한 수집 및 준비는 성공적인 분석, 마이그레이션 계획 및 구현에 매우 중요합니다.

소스 코드 인벤토리

애플리케이션 소스 코드 유형

지원되는 애플리케이션 소스 코드 유형은 다음과 같습니다.

- COBOL 프로그램
- JCL 스크립트
- 어셈블러 프로그램
- PL/I 프로그램
- CICS 트랜잭션
- 자연 프로그램
- REXX 스크립트

- Easytrieve 프로그램
- 카피북 및 포함
- Proc 라이브러리

데이터베이스 자산

지원되는 데이터베이스 자산은 다음과 같습니다.

- DB2 DCLGEN 및 DDL 스크립트
- IMS 데이터베이스 정의(PSBs 및 DBDs)
- VSAM 파일 정의
- 물리적 및 논리적 데이터베이스 스키마
- 데이터베이스 절차 및 트리거

소스 코드 파일 확장명

확장을 잘 모르는 경우 비워 두거나 .txt로 두면 AWS 변환이 이를 분류합니다.

다음 표에는 메인프레임 소스 아티팩트의 일반적인 파일 확장명이 나열되어 있습니다.

메인프레임 소스 코드 파일 확장명

언어/유형	일반 확장	설명
COBOL	.cbl, .cob, .cobol	COBOL 소스 프로그램
JCL	.jcl	작업 제어 언어 스크립트
어셈블러	.asm	어셈블러 언어 프로그램
PL/I	.pl1	PL/I 언어 프로그램
CICS 정의	.csd	CICS 시스템 정의(CSD)
자연어	.nat	자연 프로그램
REXX	.rex, .rexx	REXX 스크립트
Easytrieve	.ezt	Easytrieve 보고서 프로그램

언어/유형	일반 확장	설명
카피북	.cpy	COBOL 카피북
BMS	.bms	기본 매핑 지원(BMS)
PL/I 카피북	.pl1_copy	PL/I 카피북
Db2 DCLGEN	.dcl	Db2 선언 생성기
Db2 정의	.sql, .ddl	Db2 데이터베이스 정의
IMS 정의	.ims	IMS 리소스 정의 데이터 세트(IMS 1단계)
MFS	.mfs	IMS MFS(메시지 형식 서비스)
PSB	.psb	IMS PSB(프로그램 사양 블록)
DBD	.dbd	IMS 데이터베이스 정의
JCL Proc	.prc, .proc	JCL 프로시저 라이브러리
JCL 포함 사항	.inc	JCL 파일 포함
매크로	.mac	어셈블러 매크로
컨트롤 카드	.ctl	JCL 유틸리티 제어 카드

수집 방법

소스 코드 추출

메인프레임 PDS 라이브러리에서 대화형 소스 코드를 추출하려면 보안 FTP 클라이언트(WinSCP/ FileZilla)를 사용합니다.

DB2 스키마 추출

DB2 LUW(Linux, UNIX 및 Windows) 클라이언트 소프트웨어에는 db2look 유틸리티가 설치 패키지의 일부로 포함되어 있습니다. db2look 유틸리티는 DB2 데이터베이스에서 DDL(데이터 정의 언어) 문을 추출합니다.

다음 명령을 실행합니다.

```
db2look -d DATABASE_NAME -i userid -w password -a -e -m -l -x -f -createdb -printdbcfg
-o DATABASE_NAME.sql
```

다음 목록은 파라미터를 설명합니다.

- -d **DATABASE_NAME**: 스키마를 추출할 데이터베이스의 이름을 지정합니다.
- -i **userid**: 데이터베이스 인증을 위한 사용자 ID
- -w **password**: 데이터베이스 인증을 위한 암호
- -a: 권한 부여 정보 추출(grants)
- -e: 모든 데이터베이스 객체(테이블, 뷰, 인덱스 등)를 추출합니다.
- -m: 통계 및 물리적 특성 추출
- -l: 테이블 및 열 주석 추출
- -x: 설명 테이블 추출
- -f: 더 나은 가독성을 위해 출력의 형식을 지정합니다.
- -createdb: 데이터베이스 생성 문 포함
- -printdbcfg: 데이터베이스 구성 파라미터 포함
- -o **DATABASE_NAME.sql**: 출력 파일 이름을 지정합니다.

메인프레임에서 카탈로그 정보 추출

IDCAMS의 LISTCAT 명령은 메인프레임의 데이터 세트에 대한 카탈로그 정보를 검색하는 유틸리티입니다. 이는 메인프레임 현대화 프로젝트에서 데이터 세트를 인벤토리로 만들고 특성을 이해하는 데 유용합니다.

```
//LSTCATJ JOB 'LISTCAT',CLASS=A,MSGCLASS=X,NOTIFY=&SYSUID
//*
//STEP1 EXEC PGM=IDCAMS
//*
//SYSPRINT DD DSN=AWS.M2.CATALOG.LIST,
//          DISP=(NEW,CATLG,DELETE),
//          SPACE=(CYL,(1,1),RLSE),
//          DCB=(RECFM=FBA,LRECL=133,BLKSIZE=0)
//*
//SYSIN DD *
LISTCAT ENT('AWS.M2.CARDDemo.*') ALL
```

```
LISTCAT ENT('SYS1.*') ALL
/*
```

CICS 정의 추출

IBM 제공 DFHCSDUP 유틸리티는 CICS 시스템 정의(CSD) 파일에서 CICS 리소스 정의를 추출할 수 있습니다.

다음 JCL을 사용하여 DFHCSD에서 기존 정의를 언로드합니다.

```
//CSDEXTJ JOB 'EXTRACT CSD',CLASS=A,MSGCLASS=X,NOTIFY=&SYSUID
/*
//STEP1 EXEC PGM=DFHCSDUP,REGION=0M,
//          PARM='CSD(READONLY),PAGESIZE(60),NOCOMPAT'
/*
//STEPLIB DD DSN=your-hlq.SDFHLOAD,DISP=SHR
//DFHCSD DD DSN=your-hlq.DFHCSD,DISP=SHR
/*
//CBDOUT DD DSN=your-hlq.CSD,
//          DISP=(NEW,CATLG,DELETE),
//          SPACE=(CYL,(1,1),RLSE),
//          DCB=(RECFM=FB,LRECL=80,BLKSIZE=0)
//SYSPRINT DD SYSOUT=*
//SYSIN DD *
          EXTRACT GROUP(cics-group) USERPROGRAM(DFH0CBDC) OBJECTS
/*
```

IMS 정의 추출

IMS 정의를 추출하려면 DFSURDD0 유틸리티를 사용하여 IMS 트랜잭션 파일을 생성할 수 있습니다. 이 유틸리티는 마이그레이션 목적으로 사용할 수 있는 1단계 매크로 문을 생성합니다. 현재는 IMS 1단계만 지원됩니다.

다음 JCL을 사용하여 IMS 정의를 추출합니다.

```
//IMSEXTJ JOB 'IMS STAGE 1',CLASS=A,MSGCLASS=X,NOTIFY=&SYSUID
/*
//STEP1 EXEC PGM=DFSURDD0,MEMLIMIT=12G
/*
//STEPLIB DD DISP=SHR,DSN=your-hlq.SDFSRESL
/*
//RDDSDSN DD DISP=SHR,DSN=your-rdds
```

```

/*
//SYSOUT DD DSN=your-hlq.STAGE1.IMS,
//          DISP=(NEW,CATLG,DELETE),
//          SPACE=(CYL,(1,1),RLSE),
//          DCB=(RECFM=FB,LRECL=80,BLKSIZE=0)
//SYSPRINT DD SYSOUT=*
//SYSIN DD *
        OUTPUT=MAC
/*

```

CA-7 스케줄러 정보 추출

CA-7 작업 일정 정보는 LJOB 보고서에 포함되어 있습니다. LIST=NODD 파라미터와 함께 LJOB 유틸리티를 사용하여 메인프레임에서 보고서를 생성합니다. 보고서에는 .ca7 확장자가 있어야 합니다. 각 보고서에는 열 1에 ANSI 캐리지 컨트롤 문자가 있어야 합니다. LJOB 유틸리티를 실행하는 데 사용되는 JCL에 DCB=RECFM=FBA (또는 FA)를 지정하여 열 1에 캐리지 컨트롤 문자가 있는 보고서를 생성할 수 있습니다.

예: LJOB, JOB=ZBN*, LIST=ALL

자세한 내용은 [Broadcom 설명서를](#) 참조하세요.

SMF 데이터 추출

시스템 관리 시설(SMF) 레코드는 AWS 변환에서 배치 작업 및 CICS 트랜잭션 사용량을 분석하는 데 사용하는 활동 지표를 제공합니다. 지원되는 SMF 레코드 유형은 14, 15, 30(하위 유형 5), 64, 102, 110(하위 유형 1, 데이터 클래스 1, 3, 4)입니다.

SMF 레코드의 형식 요구 사항:

- 레코드 유형 30 및 110을 포함해야 합니다(최소).
- RDW(Record Descriptor Word) 바이트가 포함된 원시 바이너리 EBCDIC 형식이어야 합니다.
- 다음 중 하나로 제공해야 합니다.
 - .zip 형식으로 압축된 최대 600MB의 파일
 - .tar.gz 또는 .gz 형식으로 압축된 최대 5GB의 파일
- Amazon S3의 소스 코드와 별도의 폴더에 저장해야 합니다.

최소 13개월의 SMF 레코드를 제공하여 연간 배치 주기와 짧은 기간에 놓칠 수 있는 계절 패턴을 캡처합니다.

옵션 1: SMF 레코드 추출 및 정렬

다음 샘플 JCL을 사용하여 SMF 레코드를 추출하고 정렬합니다.

```
//SMFEXTR JOB (ACCT),'EXTRACT SMF',CLASS=A,
//          MSGCLASS=X,NOTIFY=&SYSUID
//*-----*
/** SMF RECORD EXTRACTION TEMPLATE
/** CUSTOMIZE: Job card, dataset names, date range, record types
/**-----*
/**
/** STEP 1: EXTRACT SMF RECORDS
/**
//EXTRACT EXEC PGM=IFASMFDP
//SYSPRINT DD SYSOUT=*
/**
/** INPUT: Specify your SMF datasets (MAN files or GDG)
/**
//DUMPIN DD DISP=SHR,DSN=SYS1.MAN1
//        DD DISP=SHR,DSN=SYS1.MAN2
//        DD DISP=SHR,DSN=SYS1.MAN3
/**
/** OUTPUT: Extracted SMF records
/**
//DUMPOUT DD DSN=your.hlq.SMF.EXTRACT,
//          DISP=(NEW,CATLG,DELETE),
//          UNIT=SYSDA,
//          SPACE=(CYL,(500,100),RLSE),
//          DCB=(RECFM=VBS,LRECL=32760,BLKSIZE=27998)
/**
/** CONTROL CARDS
/**
//SYSIN DD *
        INDD(DUMPIN,OPTIONS(DUMP))
        OUTDD(DUMPOUT,TYPE(14,15,30,110))
        DATE(yyyy/ddd,yyyy/ddd)
        START(0000)
        END(2359)
/*
/**
/** STEP 2: SORT EXTRACTED RECORDS (OPTIONAL)
/**
//SORT EXEC PGM=SORT
//SORTIN DD DISP=SHR,DSN=your.hlq.SMF.EXTRACT
```

```
//SORTOUT DD DSN=your.hlq.SMF.SORTED,
//          DISP=(NEW,CATLG,DELETE),
//          UNIT=SYSDA,
//          SPACE=(CYL,(500,100),RLSE),
//          DCB=(RECFM=VBS,LRECL=32760)
//SORTWK01 DD UNIT=SYSDA,SPACE=(CYL,(50))
//SORTWK02 DD UNIT=SYSDA,SPACE=(CYL,(50))
//SORTWK03 DD UNIT=SYSDA,SPACE=(CYL,(50))
//SYSOUT DD SYSOUT=*
//SYSPRINT DD SYSOUT=*
//SYSIN DD *
      SORT FIELDS=(11,4,CH,A,7,4,CH,A,15,4,CH,A),EQUALS
/*
```

이전 JCL에서 다음 값을 사용자 지정합니다.

1. 작업 카드: 계정, 클래스 및 msgclass 업데이트
2. DUMPIN: SMF 데이터 세트를 가리킵니다.
3. DUMPOUT: 출력 데이터 세트 이름 및 HLQ 지정
4. 유형: 레코드 유형 선택(14, 15, 30, 110 또는 기타)
5. 날짜: 형식 yyyy/ddd(예: 2026/055,2026/056)
6. 공간: 예상 데이터 볼륨에 따라 조정
7. 필요하지 않은 경우 SORT 단계 제거

옵션 2: DFSORT를 사용하여 SMF 데이터 추출

DFSORT를 사용하여 기록 SMF 데이터를 통합하고 보고할 수 있습니다. 이는 SMF 레코드를 일별 또는 주별로 GDG에 저장하는 경우에 유용합니다. 다음 작업은 DFSORT를 사용하여 SORTIN 파일에서 SMF 레코드를 통합하고 INCLUDE COND 파라미터에 지정된 레코드를 기반으로 필터링합니다.

```
//EXTRSMF JOB 'EXTRACT SMF RECORDS',CLASS=S,MSGCLASS=H,
// MSGLEVEL=(1,1),REGION=0M,NOTIFY=&SYSUID,TIME=1440
//SORTJES2 EXEC PGM=SORT,REGION=0M
//SYSOUT DD SYSOUT=*
//SORTMSG DD SYSOUT=*
//SORTIN DD DISP=SHR,DSN=your.hlq.SMF.EXTRACT
//SORTOUT DD DSN=your.hlq.SMF.OUTPUT,
// DISP=(MOD,CATLG,DELETE),
// DCB=(BUFNO=20,
// RECFM=VBS,LRECL=32760,BLKSIZE=27998),
```



```
// SPACE=(CYL,(1400,900),RLSE)
//SORTWK1 DD UNIT=SYSDA,SPACE=(CYL,(30,50))
//SORTWK2 DD UNIT=SYSDA,SPACE=(CYL,(30,50))
//SORTWK3 DD UNIT=SYSDA,SPACE=(CYL,(30,50))
//SORTWK4 DD UNIT=SYSDA,SPACE=(CYL,(30,50))
//SYSIN DD *
OPTION COPY
INCLUDE COND=(6,1,BI,EQ,X'0E',OR,6,1,BI,EQ,X'0F',OR,
6,1,BI,EQ,X'1E',OR,6,1,BI,EQ,X'40',OR,
6,1,BI,EQ,X'50',OR,6,1,BI,EQ,X'59',OR,
6,1,BI,EQ,X'5C',OR,6,1,BI,EQ,X'65',OR,
6,1,BI,EQ,X'66',OR,6,1,BI,EQ,X'6E')
```

RDW 데이터를 유지하면서 데이터를 다운로드하려면 FTP 서버를 사용하여 추출된 파일을 수신할 수 있습니다. RDW가 데이터 전송에 포함되도록 데이터가 이진 형식으로 전송되고 RDW 옵션이 사용되는지 확인합니다. 다음 작업은 이 파일을 전송하는 샘플 FTP 작업을 보여줍니다.

```
//EXTRSMF JOB 'EXTRACT SMF RECORDS',CLASS=A,MSGCLASS=H,
// MSGLEVEL=(1,1),REGION=0M,NOTIFY=&SYSUID,TIME=1440
//STEP1 EXEC PGM=FTP,REGION=2048K
//SYSIN DD *
10.10.10.10
userid
password
type i
LOCSITE RDW
put 'your.h1q.SMF.OUTPUT' SMFREQS.SMF
quit
```

SCRT 보고서 업로드

SCRT(Sub-Capacity Reporting Tool) 보고서를 AWS 변환에 업로드할 수도 있습니다.

애플리케이션 인벤토리 업로드

모든 아티팩트를 수집한 후 다음 단계를 완료합니다.

1. 아티팩트 유형(예: /cobol, /jcl, /copybooks, /db2, /ims, /cics, /ca7)별로 파일을 하위 폴더로 구성합니다.
2. 최상위 폴더를 단일 .zip 파일로 압축합니다.
3. AWS 변환 작업 영역에 연결된 Amazon S3 버킷에 .zip 파일을 업로드합니다.

Note

SMF 레코드는 Amazon S3 버킷 내의 소스 코드와 별도의 폴더에 있어야 하며 .tar.gz 또는 .gz 형식이어야 합니다.

Amazon S3 버킷을 AWS 변환에 연결하는 방법에 대한 자세한 지침은 [섹션을 참조하세요](#) [the section called “커넥터 설정”](#).

로그인 및 작업 생성

AWS 변환 웹 환경에 로그인하려면 설명서의 [AWS 변환 시작하기](#) 섹션에 있는 모든 지침을 따르세요.

작업을 생성하고 시작하려면: [프로젝트 시작의 단계를 따릅니다](#).

워크스페이스 생성: 작업, 공동 작업자 및 관련 아티팩트가 저장될 워크스페이스의 이름을 지정하고 설명합니다.

작업 생성: 미리 구성된 작업 계획 중에서 선택하여 작업을 생성하거나 지원되는 기능 목록에서 선택하여 목표에 따라 작업 계획을 사용자 지정합니다.

Important

AWS 적절한 권한이 없는 경우 변환은 작업을 거부합니다. 예를 들어 기여자는 메인프레임 애플리케이션의 작업 변환을 취소하거나 작업을 삭제할 수 없습니다. 관리자만 이러한 함수를 수행할 수 있습니다.

작업을 생성할 때 아래 기능 중에서 선택할 수 있지만 프로젝트의 소스 코드 위치가 위치하므로 항상 Kickoff 단계가 필요합니다. 워크스페이스에 설정된 첫 번째 작업에서는 Amazon S3 버킷에 대한 커넥터를 설정해야 합니다.

변환 진행 상황 추적

다음 두 가지 방법으로 프로세스 전반의 변환 진행 상황을 추적할 수 있습니다.

- 작업 로그 - 변환이 AWS 수행하는 작업에 대한 자세한 로그와 인적 입력 요청 및 해당 요청에 대한 응답을 제공합니다.
- 대시보드 - 메인프레임 애플리케이션 변환에 대한 상위 수준 요약を提供합니다. 변환된 작업 수, 변환 적용 및 메인프레임 애플리케이션의 변환을 완료하는 데 걸리는 예상 시간에 대한 지표를 보여줍니다.

니다. 파일 유형별 코드 줄, 각 파일 유형별로 생성된 설명서, 분해된 코드, 마이그레이션 계획 등 각 단계의 세부 정보를 볼 수도 있습니다.

커넥터 설정

AWS 변환은 커넥터를 사용하여 메인프레임 현대화 함수에 필요한 계정의 리소스에 액세스합니다. 커넥터는 워크스페이스에서 실행하는 첫 번째 작업으로 자동으로 구성됩니다. 선택한 작업 계획에 따라 AWS 변환은 커넥터를 생성하도록 안내합니다.

메인프레임 재구성 커넥터

메인프레임 재구성 커넥터는 평가 및 재구성 워크플로를 실행하는 작업을 위한 것입니다. S3 버킷을 사용하여 변환 리소스에 액세스하고 저장할 뿐만 아니라 Amazon Neptune 클러스터를 사용하여 추출된 아티팩트를 저장합니다. Neptune 클러스터는 작업에 대해 추출된 모든 아티팩트를 저장하는 통합 지식 그래프 역할을 하며, 지식 그래프는 AWS 변환 채팅 인터페이스의 모든 질문에 대한 답변을 제공합니다.

AWS 변환이 탄력적 네트워크 인터페이스(ENI)를 생성할 수 있는 VPC에 Amazon Neptune 클러스터를 배포합니다. ENIs 이는 AWS 변환이 VPC의 Neptune과 안전하게 통신하여 데이터를 로드하고 지식 그래프를 쿼리할 수 있도록 하는 네트워크 연결입니다.

AWS CloudFormation

다음 CloudFormation 템플릿을 사용하여 메인프레임 재구성 커넥터에 필요한 리소스를 생성하는 것이 좋습니다. CloudFormation 템플릿을 실행할 때 커넥터에 사용할 것과 동일한 S3 버킷을 사용합니다. CloudFormation 템플릿 사용에 대한 자세한 내용은 [템플릿 작업을](#) 참조하세요.

CloudFormation 템플릿을 다운로드하려면 [neptune-kg-setup.yaml](#)을 선택합니다.

템플릿은 다음 파라미터를 허용합니다.

- BucketName - 필수 항목입니다. Neptune 대량 로더 액세스를 위한 S3 버킷 이름입니다. AWS 변환 커넥터에서 사용하려는 것과 동일한 S3 버킷을 사용해야 합니다.
- KmsKeyId - 선택 사항입니다. Neptune 암호화를 위한 KMS 키입니다. 키 ID, ARN, 별칭 이름 또는 별칭 ARN을 허용합니다. 기본값은 생략된 경우 AWS 관리형 키입니다.

커넥터를 구성할 때 다음 세부 정보를 제공합니다.

- S3 버킷 ARN

- Neptune 클러스터 ARN
- Neptune 클러스터 리소스 ID
- 애플리케이션 서브넷 IDs
- 애플리케이션 보안 그룹 ID
- Neptune S3 대량 로더 역할 ARN

Important

CloudFormation 템플릿의 출력 탭에는 커넥터를 구성할 때 AWS 변환에 제공해야 하는 세부 정보가 포함되어 있습니다.

사용자 지정 구성

기존 VPC 또는 기타 도구를 사용하여 필요한 인프라를 생성하려면 환경이 다음 요구 사항을 충족해야 합니다.

Neptune 클러스터

- 엔진 버전 1.4.5.1 이상이 설치된 Amazon Neptune Serverless
 - IAM 인증 활성화됨
 - 스토리지 암호화 활성화됨(AWS 관리형 키 또는 고객 관리형 KMS 키)
- 서버리스 조정 구성(권장: 1~128NCUs)
- (권장) 고가용성과 향상된 읽기 성능을 위해 두 번째 가용 영역의 읽기 전용 복제본

네트워킹

- DNS 지원 및 DNS 호스트 이름이 활성화된 VPC
- 별도의 가용 영역에 두 개 이상의 서브넷이 있습니다. AWS 변환은 이러한 서브넷에 ENIs를 생성하여 동일한 서브넷 또는 전용 서브넷에 상주할 수 있는 Neptune 클러스터에 액세스합니다. VPC 엔드포인트 및 애플리케이션 ENIs.
- VPC 인터페이스 엔드포인트(AWS PrivateLink)를 통해 서브넷에서 다음 AWS 서비스로 네트워크 연결:
 - AWS Transform Agents API - 메인프레임 현대화 작업을 조정합니다.
 - Amazon Bedrock 런타임 - 분석 및 추론을 위해 파운데이션 모델을 호출합니다.

- Amazon Relational Database Service(RDS) – Neptune 클러스터 관리
- Amazon Elastic Compute Cloud(Amazon EC2) - ENIs 관리
- Amazon CloudWatch - AWS 변환 관찰성을 위한 지표
- 서브넷과 연결된 라우팅 테이블에 연결된 S3 게이트웨이 엔드포인트입니다. AWS 변환은 이 엔드포인트를 사용하여 S3 버킷에서 Neptune 클러스터로 데이터를 로드합니다.

보안 그룹

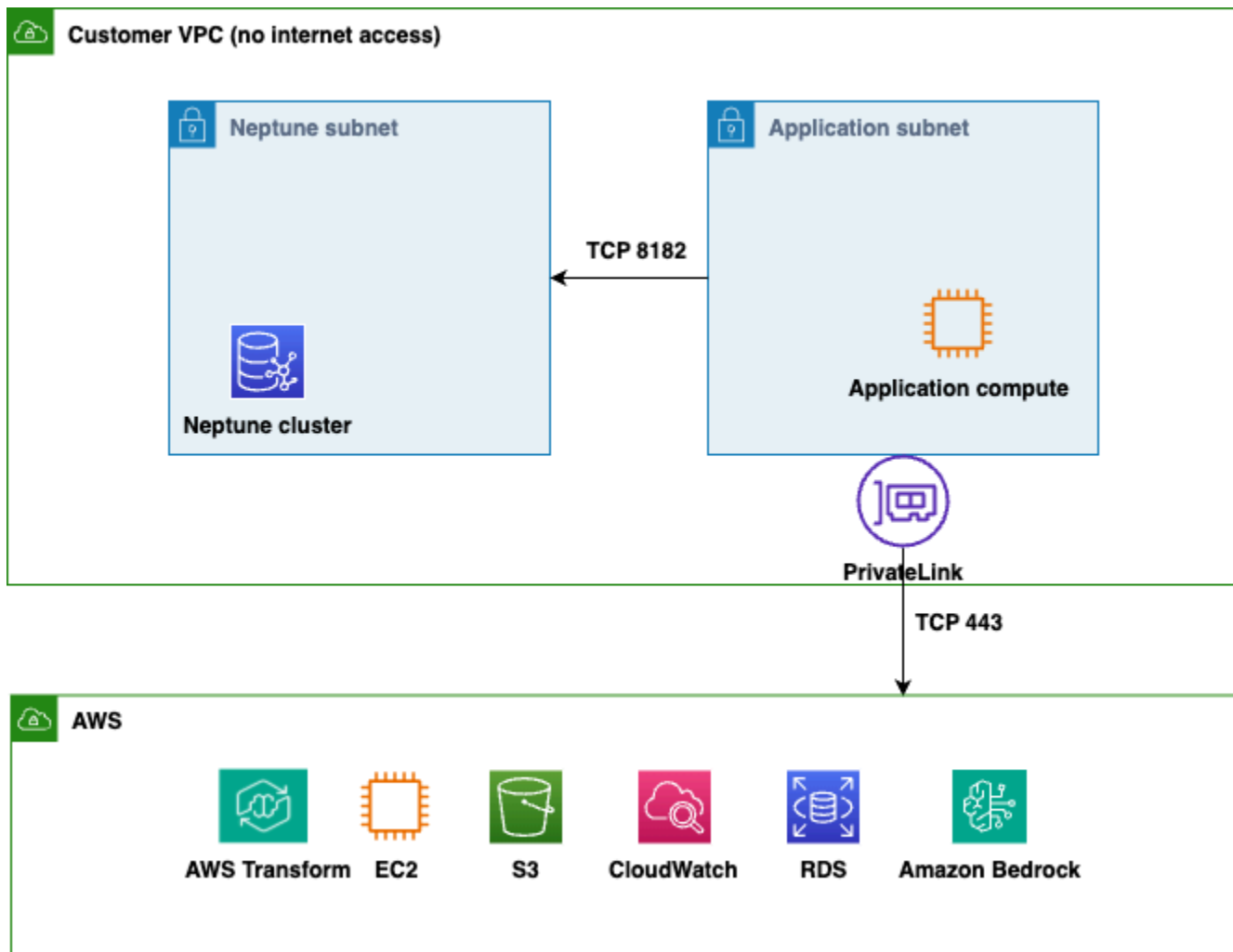
보안 그룹은 서브넷이 아닌 ENIs에 연결됩니다. AWS 변환 ENIs와 Neptune이 동일한 서브넷에 상주하는 경우에도 별도의 보안 그룹은 ENI와 Neptune 간의 액세스를 제어합니다.

- 다음을 허용하는 보안 그룹(AWS 변환에서 생성한 ENIs에 연결됨)입니다.
 - Neptune 보안 그룹에 대한 아웃바운드 TCP 8182
 - VPC 엔드포인트에 도달하기 위한 아웃바운드 TCP 443
- 다음을 허용하는 보안 그룹(Neptune 클러스터에 연결됨)입니다.
 - 애플리케이션 보안 그룹의 인바운드 TCP 8182
- 다음을 허용하는 VPC 엔드포인트 보안 그룹(인터페이스 ENIs에 연결됨)입니다.
 - 애플리케이션 보안 그룹의 인바운드 TCP 443

IAM

- S3 버킷에 s3:GetObject, s3:ListBucket 및 s3:GetBucketLocation에 대한 신뢰 정책 `rds.amazonaws.com`이 있는 IAM 역할
- 지식 그래프 데이터를 대량 로드하려면 이 역할을 Neptune 클러스터와 연결해야 합니다.

다음 다이어그램은 권장 아키텍처를 보여줍니다.



S3 커넥터

사용자 지정 계획이 있는 작업의 경우 AWS 변환은 S3 커넥터를 사용할 수 있습니다. S3 커넥터는 S3 버킷을 사용하여 변환 리소스에 액세스하고 저장하며 인덱싱된 출력을 위한 S3 벡터 버킷을 사용합니다.

⚠ Important

데이터는 워크스페이스의 AWS 변환 아티팩트 스토어에 저장되고 유지되며 작업 실행에만 사용됩니다.

S3 벡터 버킷의 선택적 구성입니다.

S3 벡터 버킷을 사용할 수 있는 리전에서 AWS 변환은 AI 기반 검색 및 채팅 경험을 제공하기 위해 정의된 S3 벡터 버킷에 작업 출력의 검색 가능한 벡터 인코딩을 저장합니다. 데이터는 이 작업 외부에서 사용되지 않으며 모델 훈련에 사용되지 않습니다. 이를 활성화하려면 S3 벡터 버킷을 생성하고 제공해야 합니다. AWS 변환은 이 버킷에 쓰는 데 필요한 권한이 있는 역할을 자동으로 생성하고 연결합니다.

S3 버킷 CORS 권한

커넥터를 구성한 후 AWS 변환 콘솔에서 직접 아티팩트를 보고 비교할 수 있도록 다음 CORS 정책을 S3 버킷에 추가합니다. 이 정책이 올바르게 설정되지 않은 경우 AWS 변환의 인라인 보기 또는 파일 비교 기능을 사용하지 못할 수 있습니다.

```
[
  {
    "AllowedHeaders": [],
    "AllowedMethods": [
      "GET"
    ],
    "AllowedOrigins": [
      "https://*.transform.eu-central-1.on.aws",
      "https://*.transform.ap-south-1.on.aws",
      "https://*.transform.ap-northeast-1.on.aws",
      "https://*.transform.ap-northeast-2.on.aws",
      "https://*.transform.ap-southeast-2.on.aws",
      "https://*.transform.ca-central-1.on.aws",
      "https://*.transform.eu-west-2.on.aws",
      "https://*.transform.us-east-1.on.aws",
      "https://*.transform.sa-east-1.on.aws"
    ],
    "ExposeHeaders": [],
    "MaxAgeSeconds": 0
  }
]
```

작업 계획 평가 및 재구상

평가 및 재구상 작업 계획은 메인프레임 애플리케이션을 현대화하기 위한 사전 정의된 워크플로입니다. 코드베이스를 평가하여 비즈니스 기능을 식별하고 선택한 기능을 재구상하는 두 단계를 안내합니다. 대신 개별 기능을 선택하려면 사용자 지정 작업 계획을 사용합니다.

평가

메인프레임 현대화 여정은 일반적으로 코드베이스를 평가하여 콘텐츠를 식별하고 관계 및 종속성을 이해하는 것으로 시작됩니다. 이 평가 후 현대화할 소스 코드의 일부를 분해하고 선택할 수 있습니다. 분해 경계는 비즈니스 기능에 따라 결정됩니다.

비즈니스 함수 카탈로그는 코드베이스를 개별 비즈니스 함수로 분해합니다. 이 기능은 각 비즈니스 함수를 처음부터 끝까지 매핑하는 결정론적 데이터 경로의 토대를 기반으로 구축됩니다. 데이터 경로는 비즈니스 트리거부터 메인프레임 코드 내의 최종 쓰기까지 데이터가 취하는 경로입니다. 시스템은 분석을 단일 진입점으로 제한하는 대신 배치 작업, CICS 트랜잭션 및 공유 데이터 스토어를 포괄하여 일관된 비즈니스 작업 단위를 식별합니다.

비즈니스 함수는 비즈니스 트리거에서 시작하여 측정 가능한 비즈니스 성과로 끝나는 일련의 작업입니다. AWS 혁신은 사업부가 조치를 취할 수 있는 비즈니스 함수의 카탈로그를 제공하여 먼저 현대화할 대상에 대해 정보에 입각한 결정을 내릴 수 있도록 합니다.

비즈니스 기능을 사용하여 현대화하기 위한 코드베이스 평가의 이점:

- 전체 상태 가시성 - 배치 작업, 온라인 트랜잭션 및 데이터 스토어가 비즈니스에 의미 있는 함수에 연결되는 방법을 이해합니다.
- 실행 가능한 경계 - 식별된 각 비즈니스 기능은 line-of-business 이해관계자가 현대화 노력을 위해 검토하고 우선순위를 지정할 수 있는 독립형 단위입니다.
- 코드 간 일관성 - 비즈니스 함수를 정의하는 동일한 코드 블록을 사용하여 변환 계층이나 조정 없이 사양을 생성합니다.
- 검색 시간 단축 - 자동 탐지는 몇 개월 동안의 수동 부족 지식 인터뷰를 체계적이고 반복 가능한 분석으로 대체합니다.

채팅을 통해 제공된 평가 결과

채팅을 통해 제공되는 평가 결과에는 데이터 경로 수, 배치 및 CICS 트랜잭션 측면에서 각 함수의 범위, 비즈니스 설명을 포함한 비즈니스 함수 목록이 포함됩니다. Amazon S3 버킷에서 생성된 아티팩트에 대한 링크가 제공되며 채팅을 통해 액세스할 수도 있습니다. 비즈니스 함수 세부 정보 및 비즈니스 함수 요약이라는 두 가지 아티팩트가 제공됩니다.

- 비즈니스 기능 요약 - 비즈니스 기능 목록과 코드 내 요소가 수행하는 기능에 대한 자연어 설명을 제공합니다.
- 비즈니스 함수 세부 정보 - 소스 코드 전반의 관계를 보여주는 대화형 그래프를 제공합니다.

그래프와 상호 작용하려면 요소를 선택하여 그래프에 대한 추가 세부 정보를 표시하거나 요소를 열어 세부 정보를 조사합니다. 각 페이지 내에는 해당 수준의 모든 요소에 대한 요약과 다음을 포함하여 각 구성 요소와 상호 작용하고 이에 대해 자세히 알아볼 수 있는 그래픽 인터페이스가 있습니다.

- 비즈니스 기능 - 어떤 비즈니스 기능이 서로 연결되어 있는지 설명하고 각 비즈니스 기능에 대한 개요를 제공합니다. 비즈니스 기능을 선택하면 다음 정보가 제공됩니다.
 - 데이터 경로 수
 - 코드 줄 수
 - 비즈니스 설명: 코드 내 요소가 수행하는 기능을 자연어로 설명하는 비즈니스 함수의 개요입니다.
 - 인터페이스: 비즈니스 기능 내의 데이터 요소가 어떻게 관련되어 있는지 자세히 설명합니다(예: 교환 또는 쓰기).
- 비즈니스 기능 세부 정보 - 단일 비즈니스 기능 내의 데이터 경로 간 연결을 보여 주므로 비즈니스 기능의 구성에 대해 자세히 알아볼 수 있습니다. 요소를 선택하면 다음 세부 정보와 함께 해당 요소가 비즈니스 기능에 어떻게 연결되는지 확인할 수 있습니다.
 - 데이터 스토어: 데이터 스토어의 작성자 및 리더입니다.
 - 기타 요소: 데이터 경로 내에서 처리되는 작업 및 결과, 프로그램 목록, 독자 및 작성자를 자연어로 설명하는 관련 데이터 경로의 개요입니다.
- 데이터 경로 - 한 데이터 경로의 세부 정보와 데이터 경로 내의 요소가 서로 어떻게 관련되어 있는지 보여줍니다.
 - 설명: 데이터 경로 내에서 처리되는 작업 및 결과를 자연어로 설명하는 데이터 경로의 개요입니다.
 - 데이터 경로의 내용:
 - 진입점
 - 읽기
 - 쓰기
 - 프로그램

채팅을 통해 출력을 조사하여 각 비즈니스 기능에 포함된 요소를 이해하고 비즈니스 함수 그래프를 통해 경계를 탐색할 수 있습니다.

현대화의 경계를 식별하면 채팅에서 재구상하려는 비즈니스 기능을 선택하라는 메시지가 표시됩니다. 단일 비즈니스 함수 또는 여러 비즈니스 함수를 선택할 수 있습니다. AWS 변환은 선택한 경계와 필요한 평가 출력을 재구상 흐름으로 전송하여 현대화 여정을 계속합니다.

첫 번째 현대화를 완료한 후 채팅을 사용하여 현대화할 추가 비즈니스 기능 세트를 선택할 수 있습니다.

재구상

재구상 단계에서는 평가에서 식별한 비즈니스 기능 중 하나 또는 전부를 선택하고 현대화를 준비할 수 있습니다. 이렇게 하면 비즈니스 로직 추출이 트리거되고 선택한 비즈니스 기능에 대한 요구 사항이 생성됩니다. 생성된 요구 사항은 미래 엔지니어링을 위한 기본 입력으로, 레거시 시스템 이해를 현대화된 애플리케이션이 제공해야 하는 대상의 정확한 사양으로 변환합니다.

비즈니스 로직 추출

하나 이상의 비즈니스 기능을 선택한 후 AWS 변환은 선택한 비즈니스 기능에 대한 비즈니스 로직 생성을 시작합니다. 추출이 완료되면 AWS 변환은 다운스트림 사용을 위해 결과를 Amazon S3 버킷에 JSON 형식으로 저장합니다. 추출 진행 상황을 모니터링하고 AWS 변환 콘솔 내에서 직접 문제를 검토할 수 있습니다.

비즈니스 로직 추출 결과를 검토하려면

1. 왼쪽 탐색 창에서 비즈니스 로직 추출 단계를 선택하여 확장합니다.
2. 단계 세부 정보에서 다음을 확인합니다.
 - S3 버킷 링크: 추출된 비즈니스 로직 결과가 JSON 형식으로 저장되는 위치입니다.
 - 문제: 비즈니스 로직 추출 프로세스 중에 발생하는 모든 문제의 목록입니다.

추출 중에 문제가 발생한 파일이 있는 경우 영향을 받는 각 파일에 대해 다음 세부 정보가 표시됩니다.

- 파일 이름: 문제가 발생한 파일의 이름입니다.
- 파일 유형: 파일의 유형입니다(예: COBOL 또는 JCL).
- 파일 경로: 애플리케이션 내 파일의 위치입니다.
- 상태: 파일 추출의 현재 상태입니다.
- 세부 정보: 발생한 문제에 대한 설명입니다.

Note

추출 단계가 완료되면 AWS 변환이 자동으로 요구 사항 생성을 시작합니다. 이 프로세스가 시작되기 전에 추가 입력을 입력하라는 메시지가 표시되지 않습니다.

요구 사항 생성

비즈니스 로직 추출이 완료되면 Generate Requirements 에이전트는 추출된 아티팩트(코드 분석, 데이터 분석, 비즈니스 규칙)를 사용하고 현대화 요구 사항을 생성합니다. 이러한 요구 사항은 기술에 구애받지 않고 테스트 가능한 수락 기준을 포함하는 공식 기능 사양입니다. AWS 변환은 선택한 각 비즈니스 기능에 대해 하나의 requirements.md 파일을 생성하고 출력을 Amazon S3 버킷에 저장합니다. 출력의 Amazon S3 위치를 보려면 요구 사항 생성 단계를 선택합니다.

각 requirements.md 파일은 다음과 같은 부분으로 구성됩니다.

- 제목 - 비즈니스 함수와 비즈니스 함수가 나타내는 워크플로의 이름을 지정합니다.
- 글로벌 사전 조건 - 처리 전과 처리 중에 전체 워크플로에서 true를 유지해야 하는 조건입니다. 구성 가능한 값은 파라미터 자리 표시자로 표시됩니다.
- 번호가 매겨진 워크플로 섹션 - 각 섹션은 비즈니스 기능의 개별 단계를 나타냅니다. 모든 섹션에는 다음이 포함됩니다.
 - 목표, 역할이 수행하려는 작업, 결과 결과를 설명하는 사용자 스토리입니다.
 - 각각 고유한 식별자가 있는 EARS(Easy Approach to Requirements Syntax) 형식의 요구 사항 목록입니다.

Note

두 번째 비즈니스 함수 세트를 선택하면 새로 선택한 함수에 대한 재구상 단계가 다시 시작됩니다. 그러면 콘솔에 새 선택에 대한 결과만 표시되므로 이전 비즈니스 기능의 비즈니스 규칙과 비즈니스 로직 및 요구 사항에 대한 출력을 저장하는 Amazon S3 링크에 문제가 더 이상 표시되지 않습니다. 이전 출력은 손실되지 않습니다. 아티팩트 탭이나 Amazon S3 버킷에서 여전히 액세스할 수 있습니다.

변환 아티팩트 간 추적성

AWS 변환은 평가 및 재구상 워크플로 전반에 걸쳐 생성되는 아티팩트 간의 추적성을 유지합니다. 추적성을 사용하면 각 요구 사항을 추출된 비즈니스 규칙 또는 요구 사항을 생성한 원래 소스 코드로 직접 추적할 수 있습니다.

traceability.yaml 파일을 사용하여 각 비즈니스 기능에 대한 모든 추적성 세부 정보를 볼 수 있습니다. 각 비즈니스 규칙이 요구 사항에 매핑되는 방법을 설명합니다.

대화형 추적성을 위해 VS Code 및 Open VSX 호환 편집기에서 IDE 플러그인을 사용할 수 있습니다. 자세한 내용은 [개발자 도구를](#) 참조하세요.

작업 계획 재구상

현대화 범위가 지정되어 재구상할 준비가 된 애플리케이션의 경우 독립 실행형 재구상 작업을 실행할 수 있습니다. 작업은 코드와 데이터를 분석하고, 비즈니스 로직을 추출하고, 비즈니스 도메인을 식별하고, 각 비즈니스 도메인에 대한 현대화 요구 사항을 생성합니다.

사용자 지정 작업 계획

사용자 지정 작업 계획을 사용하면 실행하려는 기능을 선택하여 자체 현대화 워크플로를 구축할 수 있습니다. 포함된 기능을 완벽하게 제어할 수 있습니다. 현대화 목표에 따라 다음 기능 중에서 선택합니다. 일부 기능은 먼저 실행되는 기능에 따라 달라집니다. 예를 들어 코드 분석은 대부분의 다른 기능에 필요합니다.

코드 분석

Amazon S3 버킷 경로를 AWS 변환과 공유하면 파일 이름, 파일 유형, 코드 줄 및 경로와 같은 세부 정보와 함께 각 파일의 코드를 분석합니다.

Note

작업 또는 작업 영역 수준에서 아티팩트 탭을 통해 코드 결과 분석을 다운로드할 수 있습니다. 작업 수준에서 왼쪽 탐색 메뉴의 'Artifacts' 옵션으로 이동하여 'results' 폴더를 열거나 워크스페이스 수준에서 작업 이름을 찾아 'results' 폴더를 엽니다. 그러면 수동 분류 워크플로, 자산 목록, 종속성 JSON 파일 및 누락된 파일 목록에 대한 분류 파일이 포함된 zip 파일이 다운로드됩니다.

작업 계획의 왼쪽 탐색 창에서 코드 분석을 선택하여 결과를 봅니다. 코드 분석 결과는 여러 가지 방법으로 볼 수 있습니다.

- 목록 보기 - 메인프레임에 대해 변환하려는 Amazon S3 버킷의 모든 파일
- 파일 유형 보기 - 파일 유형별로 표시되는 Amazon S3 버킷의 모든 파일입니다. 지원되는 파일 유형 목록은 [지원되는 파일을 참조하세요](#).
- 폴더 보기 - 폴더 구조로 표시된 Amazon S3 버킷의 모든 파일입니다.

파일 결과 내에서 AWS 변환은 선택한 파일 보기에 따라 다음 정보를 제공합니다.

- 이름
- 파일 유형
- 총 코드 줄 수
- 파일 경로
- 주석 줄
- 빈 줄
- 효과적인 코드 줄
- 파일 수
- 순환 복잡성 - 순환 복잡성은 프로그램의 소스 코드를 통한 선형 독립 경로 수를 나타냅니다. AWS 변환은 각 파일에 대한 순환 복잡성을 표시합니다.

누락된 파일 - 메인프레임 현대화 코드 분석에서 누락된 파일입니다. 이러한 파일은 Amazon S3 버킷의 소스 입력의 일부로 추가해야 하며, 더 나은 결과를 얻으려면 분석 단계를 다시 실행해야 합니다.

동일한 이름 - AWS 변환은 동일한 이름과 가능한 동일한 특성(예: 코드 줄 수)을 공유하는 파일 목록을 제공합니다. 한 번에 두 파일의 내용 차이를 비교할 수 없습니다.

중복 IDs- Cobol 프로그램을 사용하면 프로그램 ID 필드가 파일의 고유 식별자 역할을 합니다. 이 ID는 프로젝트 전체에서 프로그램을 호출하는 데 사용되므로 고유해야 합니다. 그러나 일부 프로젝트에는 이름이 다르지만 프로그램 ID가 동일한 COBOL 파일이 있을 수 있습니다. 평가 중에 이러한 파일 목록을 가져오면 모든 프로그램의 종속성을 이해하는 데 도움이 될 수 있습니다.

Note

이는 COBOL 코드 및 파일에만 해당됩니다.

IDs가 중복된 프로그램이 있는 경우 COBOL 코드에서 각 파일에 대한 고유 식별자를 갖도록 이러한 파일의 프로그램 IDs를 변경하는 것이 좋습니다. 그런 다음 작업을 다시 실행하여 더 정확하고 포괄적인 코드 분석 결과를 얻을 수 있습니다.

중복된 프로그램 IDs 확인하면 다음을 수행할 수 있습니다.

- 코드 명확성 및 유지 관리성 개선
- 프로그램 호출의 잠재적 충돌 감소
- 종속성 매핑의 정확도 향상

- 향후 현대화 작업 간소화

코드베이스 문제 - 현대화 프로젝트를 계속하기 전에 해결해야 하는 코드베이스 내에서 탐지된 잠재적 문제입니다. 이러한 문제에는 관련 문에 대한 참조 누락 또는 코드에서 지원되지 않는 링크가 포함될 수 있습니다.

업데이트 분류 - 수동 재분류를 사용하면 새 분류로 JSON 파일을 업로드하여 대량 업데이트 기능을 사용하여 파일을 재분류할 수 있습니다.

 Important

이는 UNKNOWN 및 TXT 파일에만 사용할 수 있습니다.

재분류 후 AWS 변환은 다음을 수행합니다.

1. 분류 결과를 업데이트합니다.
2. 새 파일 유형으로 종속성 분석을 다시 실행합니다.
3. 영향을 받는 모든 분석 결과를 새로 고칩니다.

 Note

초기 분석 루프가 완료된 후에만 파일을 재분류할 수 있습니다.

인라인 뷰어 및 파일 비교

인라인 뷰어는 메인프레임 기능 AWS 변환의 기능으로, 두 가지 주요 시각화 기능을 제공합니다.

- 파일 보기: 작업에서 선택한 레거시 파일의 콘텐츠 보기
- 파일 비교: 두 레거시 파일의 콘텐츠를 side-by-side 비교

입력 파일 보기

코드 분석 단계에서 파일을 보려면

- 코드 분석 결과 보기에서 목록의 확인란을 사용하여 파일을 선택합니다.

작업 보기 버튼을 선택합니다(항목 1개를 선택한 경우 활성화됨).

파일 콘텐츠는 파일 보기 구성 요소의 화면에 렌더링됩니다.

파일 비교

코드 분석 단계의 파일을 비교하려면

1. 코드 분석 결과 보기에서 목록의 확인란을 사용하여 두 개의 파일을 선택합니다.
2. 작업 비교 버튼을 선택합니다(항목 2개를 선택한 경우에만 활성화됨).
3. 파일은 파일 비교 구성 요소에 side-by-side 표시됩니다.

Note

파일을 비교할 파일을 두 개 이상 선택할 수 없습니다.

Important

인라인 뷰어 또는 파일 비교에 문제가 있는 경우 S3 버킷이 올바르게 설정되었는지 확인합니다. S3 버킷의 CORS 정책에 대한 자세한 내용은 섹션을 참조하세요 [the section called “S3 버킷 CORS 권한”](#).

데이터 분석

AWS 변환은 데이터 관계 및 요소가 메인프레임 현대화 프로젝트에 미치는 영향을 이해하는 데 도움이 되는 데이터 분석을 제공합니다. 제공되는 두 가지 출력은 다음과 같습니다.

- 데이터 계보: 데이터 소스, 작업 및 프로그램 간의 관계를 매핑하여 데이터의 수명 주기를 추적합니다.
- 데이터 사전: 레거시 데이터 요소의 구조적 메타데이터를 문서화하는 리포지토리 역할을 합니다.

분석이 완료되면 각 출력에 대해 두 개의 탭이 있으며, 데이터 계보와 사전 모두에 대해 아래에 설명된 여러 보기를 사용할 수 있습니다.

Note

데이터 분석을 요청할 때 analysis. AWS Transform은 데이터 분석을 수행하는 데 필요한 코드 분석을 수행합니다.

데이터 계보

AWS 변환은 현대화 중인 코드 베이스에서 이해해야 하는 데이터 관계를 기반으로 여러 보기를 제공합니다. 데이터 계보에서 사용할 수 있는 네 가지 테이블 보기는 다음과 같습니다.

- 데이터 세트: 이 보기는 읽기, 쓰기, 업데이트 및 삭제를 구분하는 데 도움이 되는 작업 추적을 포함한 포괄적인 영향 분석을 제공합니다.
- Db2 테이블: Db2 테이블 및 작업과 관련된 영향 분석 제공
- Program-to-data: 각 데이터 세트를 참조하는 COBOL 프로그램 식별
- JCL-to-data 관계: 각 데이터 세트를 참조하는 JCL 스크립트 식별

요약은 데이터 소스의 개요, 프로그램 및 JCLs과의 관계, 데이터 소스의 활용 방식 및 코드베이스에서 발견된 총 작업에 대한 요약 정보를 제공합니다.

데이터 사전

코드베이스에 있는 데이터 소스 내의 데이터 요소를 이해하는 것은 다양한 데이터 소스가 어떻게 종속 되는지를 실현하는 다음 단계입니다. 데이터 사전은 정확한 변환 매핑을 위한 비즈니스 언어 설명과 함께 필드 수준 메타데이터를 제공하는 데이터 카탈로그입니다.

- COBOL 데이터 구조: 필드 속성 및 비즈니스 정의를 포함하여 코드베이스에 있는 COBOL 카피북 및 인라인 참조 전반의 필드 정보를 제공합니다.
- Db2 테이블: 기본 및 외래 키, 스키마 및 인덱스 정보, 데이터 유형을 포함하여 코드베이스에 있는 Db2 테이블 전반의 열 및 테이블 속성을 제공합니다.

데이터 계보와 사전 간의 관계는 데이터 소스를 선택한 다음 데이터 계보 또는 데이터 사전 버튼을 활용하여 데이터 소스와 데이터 요소 간의 관계를 자세히 살펴볼 수 있습니다. 데이터 계보와 사전 간의 탐색은 데이터 계보와 통합된 데이터 가시성을 제공하여 "대상" - 사용 및 관계와 함께 "대상" - 구조와 의미를 제공합니다.

활동 지표 분석

활동 지표 분석을 사용하면 유형 14, 15, 30, 64, 102 및 110의 시스템 관리 시설(SMF) 레코드를 분석할 수 있습니다. 분석은 메인프레임 애플리케이션 내에서 요소가 사용되는 방식에 대한 인사이트를 제공합니다. 사용되지 않는 코드를 사용 중지하거나 현대화된 애플리케이션의 대상 아키텍처에 대한 결정을 내리는 데 도움이 될 수 있습니다. 작업에 활동 지표 분석을 포함하는 경우 코드 분석 단계를 완료하면 먼저 더 풍부한 SMF 출력이 제공되지만 필수는 아닙니다.

Note

메인프레임 현대화를 위한 작업 계획을 협상할 때 코드 분석 및 분해 단계를 완료하면 먼저 더 풍부한 출력이 제공됩니다.

분석을 위한 SMF 레코드 온보딩

SMF 분석을 위한 초기 단계로 Amazon S3 버킷 내의 SMF 레코드 위치를 제공해야 합니다. 최소 13개월의 레코드를 제공하여 짧은 기간 동안 놓칠 수 있는 연간 발생 횟수를 캡처합니다. 13개월이 권장되지만 감지 가능한 SMF 레코드가 있는 모든 기간은 분석 결과를 생성합니다.

SMF 추출은 다음 형식 요구 사항을 충족해야 합니다.

- 유형 14, 15, 30(하위 유형 5), 64, 102 및 110을 포함합니다.
- EBCDIC 형식의 원시 바이너리 파일을 사용합니다.
- RDW 바이트를 포함합니다.

Amazon S3 버킷 내의 SMF 레코드에 대한 링크를 제공하여 레코드가 소스 코드와 별도의 폴더에 있는지 확인합니다. 형식 옵션에는 압축된 .zip(최대 600MB) 또는 .tar.gz(최대 5GB)가 포함됩니다. SMF 레코드가 감지되지 않는 폴더에 대한 링크를 제공하면 오류 메시지가 표시되고 분석이 완료되지 않습니다.

분석 출력

분석 출력에는 레코드 유형에 따라 테이블 형식 보기와 .csv 출력(Amazon S3 버킷에서 사용 가능)이라는 두 가지 구성 요소가 포함됩니다. AWS 변환 내에서 출력은 유형 30 및 110에 대해 표시됩니다. Amazon S3 버킷의 아티팩트를 통해 다른 유형의 레코드에 대한 분석을 탐색할 수 있습니다. 사용자 인터페이스에서 헤더는 제공된 레코드의 시간 범위를 표시하므로 누락된 키 날짜를 식별할 수 있습니다. 예를 들어 레코드가 5월 1일부터 10월 31일까지 지속되지만 추수 감사절 이후 바쁜 날을 제외하

면 키 레코드가 누락된 것을 확인할 수 있습니다. 웹 애플리케이션의 타임스탬프는 시스템의 시간대와 SMF 레코드를 반영합니다.

Amazon S3에서 사용할 수 있는 아티팩트는 제공된 레코드에 있는 모든 레코드 유형에 대한 분석을 제공합니다.

테이블 형식 보기

SMF 30 및 110에만 사용할 수 있는 테이블 형식 보기에는 배치 작업 및 CICS 트랜잭션을 위한 최대 3개의 주요 구성 요소가 포함되어 있습니다.

- 요약 - 주요 작업 및 트랜잭션을 제공합니다.
- 배치 작업/CICS 트랜잭션 분석 - 작업 및 트랜잭션 전반에 걸쳐 집계된 분석을 제공합니다.
- 코드 분석 비교(배치만 해당) - SMF 분석 전에 코드 분석 단계가 실행될 때 비교 데이터를 제공합니다.

검색 요약은 심층 분석을 위한 항목을 빠르게 식별하는 데 도움이 되는 세 가지 작업 및 트랜잭션 그룹을 제공합니다.

배치 작업 및 CICS 트랜잭션 분석은 작업 및 트랜잭션 전반에 걸쳐 집계된 분석을 제공합니다. 분석 결과의 일부 열은 기본적으로 숨겨집니다. 기어 아이콘을 선택하면 추가 필드가 표시됩니다.

트랜잭션 키는 CICS 트랜잭션에 대한 고유한 데이터 집계를 생성하여 네 개의 필드를 단일 키 값으로 결합합니다.

- 트랜잭션 ID
- 프로그램 이름
- SysPlex ID
- SysID

전체 키 또는 분석 출력의 키 구성 요소별로 검색할 수 있습니다.

코드 분석 비교는 SMF 레코드 또는 코드 분석 단계에서 찾았지만 둘 다에는 없는 작업을 강조 표시합니다. 이는 SMF 레코드 기간 동안 실행되지 않았거나 코드 분석 단계에 없는 작업을 보여줍니다. 이 출력은 작업에서 SMF 분석 전에 코드 분석 단계를 실행하는 경우에만 사용할 수 있습니다.

모범 사례

배치 작업에 대한 포괄적인 출력(유형 30)을 가져오려면 JCL 파일 이름이 작업 이름과 일치하는지 확인하여 코드 분석 비교에서 의미 있는 출력을 얻어야 합니다.

기술 설명서 생성

현대화 중인 메인프레임 애플리케이션에 대한 기술 설명서를 생성할 수 있습니다. 코드를 분석하여 AWS 변환은 레거시 시스템에 있는 프로그램 로직, 흐름, 통합 및 종속성에 대한 설명을 포함하여 애플리케이션 프로그램에 대한 자세한 설명서를 자동으로 생성할 수 있습니다. 이 설명서 기능은 지식 격차를 해소하는 데 도움이 되므로 애플리케이션을 최신 클라우드 아키텍처로 전환할 때 정보에 입각한 결정을 내릴 수 있습니다.

Note

기술 설명서 생성을 요청하면 AWS Transform은 설명서를 생성하는 데 필요한 코드 종속성 분석을 포함한 코드 분석을 수행합니다.

기술 설명서를 생성하려면

1. 왼쪽 탐색 창의 기술 설명서 생성에서 파일 선택 및 설정 구성을 선택합니다.
2. 설명서를 생성하려는 Amazon S3 버킷의 파일을 선택하고 협업 탭에서 설정을 구성합니다.

Note

선택한 파일은 동일한 인코딩 유형(즉, 모두 동일한 CCSID - UTF8 또는 ASCII)을 가져야 합니다. 그렇지 않으면 생성된 기술 설명서에 빈 필드 또는 섹션이 있을 수 있습니다.

3. 설명서 세부 정보 수준을 선택합니다.
 - 요약 - 범위의 각 파일에 대한 개략적인 개요를 제공합니다. 또한 각 파일에 대한 한 줄 요약을 제공합니다.
 - 세부 기능 사양 - 메인프레임 애플리케이션 변환 범위의 각 파일에 대한 포괄적인 세부 정보를 제공합니다. 일부 세부 정보에는 로직 및 흐름, 종속성, 입력 및 출력 처리, 다양한 트랜잭션 세부 정보가 포함됩니다.

Note

설명서는 COBOL 및 JCL 파일에 대해서만 생성할 수 있습니다.

4. 계속을 선택합니다.
5. AWS 변환이 설명서를 생성하면 결과가 생성되고 저장되는 콘솔의 Amazon S3 버킷 경로에 따라 설명서 결과를 검토합니다.
6. 설명서가 생성되면 채팅 AWS 변환을 사용하여 생성된 설명서에 대해 질문하고 다음 단계를 결정할 수도 있습니다.

설명서에 사용자 정보 추가

```
ARTIFACT_ID.zip
### app/
    ### File1.CBL
    ### File2.JCL
    ### subFolder/
    #   # File3.CBL
### glossary.csv
### pdf_config.json
### header-logo.png
### footer-logo.png
# ...
```

zip 파일에 선택적 파일을 추가하여 생성된 설명서 품질을 개선하고 사용자 지정 PDF 커버 페이지를 제공할 수 있습니다. 이 중 일부는 다음과 같습니다.

- glossary.csv 파일: S3 버킷의 zip 파일에 선택적 용어집을 제공하고 업로드하도록 선택할 수 있습니다. 용어집은 CSV 형식입니다. 이 용어집은 고객 어휘에 따라 관련 설명이 포함된 문서를 생성하는데 도움이 됩니다. 샘플 glossary.csv 파일은 다음과 같습니다.

```
LOL, Laugh out loud
ASAP, As soon as possible
WIP, Work in progress
SWOT, "Strengths, Weaknesses, Opportunities and Threats"
```

- pdf_config.json:이 선택적 구성 파일을 활용하여 헤더, 바닥글, 로고 및 사용자 지정 정보를 포함하여 회사의 형식 및 표준에 맞는 PDF 문서를 생성할 수 있습니다. 샘플은 다음과 pdf_config.json 같습니다.

```
{
  "header": {
    "text": "Acme Corporation Documentation",
    "logo": "header-logo.png"
  },
  "customSection": {
    "variables": [
      {
        "key": "business Unit",
        "value": "XYZ"
      },
      {
        "key": "application Name",
        "value": "ABC"
      },
      {
        "key": "xxxxxxxxxxx",
        "value": "yyyyyyyyyyyyyy"
      },
      {
        "key": "urls",
        "value": [
          {
            "text": "Product Intranet Site",
            "url": "https://example.com/intranet"
          },
          {
            "text": "Compliance Policies",
            "url": "https://example.com/policies"
          }
        ]
      }
    ]
  },
  "footer": {
    "text": "This document is intended for internal use only. Do not distribute without permission.",
    "logo": "footer-logo.png",
    "pageNumber": true
  }
}
```

```
}
}
```

- 헤더:
 - 커버 페이지 PDF 파일의 경우 기본 텍스트는 프로젝트 이름이 됩니다.
 - 각 프로그램 PDF 파일의 기본 텍스트는 프로그램 이름이 됩니다.
 - 기본 로고는 없습니다. 헤더 로고가 구성되지 않은 경우 로고가 표시되지 않습니다.
 - 글꼴 크기와 로고 크기는 단어 수 또는 로고 파일 크기에 따라 동적으로 변경됩니다.
- 사용자 지정 섹션:
 - 사용자 지정 섹션이 구성되지 않은 경우 PDF에서 생략됩니다.
 - 링크를 클릭할 수 있어야 합니다.
- 바닥글:
 - 바닥글에는 기본 텍스트나 로고가 없습니다.
 - 달리 명시적으로 구성되지 않는 한 페이지 번호는 기본적으로 바닥글에 표시됩니다.
 - 글꼴 크기와 로고 크기는 단어 수 또는 로고 파일 크기에 따라 동적으로 변경됩니다.

설명서 인라인 뷰어 생성

기술 문서 생성 단계에서 PDF 파일을 볼 수 있습니다.

PDF 파일을 보려면

1. 설명서 결과 검토 탭으로 이동합니다.
2. 생성된 PDF를 나열하는 테이블에서 PDFs 찾습니다.
3. 파일을 선택한 다음 보기를 선택하거나 파일 이름에 오버레이된 링크 요소를 선택합니다.

오른쪽 상단의 화면을 확장하는 옵션과 함께 PDF가 AWS 변환에서 열립니다.

Note

AWS 또한 변환을 사용하면 생성된 기술 설명서의 PDF 버전의 XML을 다운로드할 수 있습니다.

⚠ Important

설명서 인라인 뷰어에 문제가 있는 경우 S3 버킷이 올바르게 설정되었는지 확인합니다. S3 버킷의 CORS 정책에 대한 자세한 내용은 섹션을 참조하세요 [the section called “S3 버킷 CORS 권한”](#).

비즈니스 로직 추출

현대화 중인 메인프레임 애플리케이션에서 필수 비즈니스 로직을 추출할 수 있습니다. AWS Transform은 코드를 자동으로 분석하여 세부 프로세스 흐름 및 애플리케이션에 포함된 비즈니스 로직을 비롯한 중요한 비즈니스 요소를 식별하고 문서화합니다. 이 기능은 현대화 여정에서 여러 이해관계자에게 도움이 됩니다. 비즈니스 분석가는 추출된 로직을 활용하여 정확한 비즈니스 요구 사항을 생성하고 현재 구현의 격차 또는 불일치를 식별할 수 있습니다. 개발자는 광범위한 메인프레임 전문 지식 없이 복잡한 레거시 시스템 기능을 빠르게 이해할 수 있습니다.

i Note

비즈니스 로직 추출을 요청할 때, AWS Transform은 비즈니스 로직 추출을 수행하는 데 필요한 코드 종속성 및 진입점 분석을 포함한 코드 분석을 수행합니다.

비즈니스 로직을 추출하려면

1. 왼쪽 탐색 창의 비즈니스 로직 추출에서 설정 구성을 선택합니다.
2. 협업 탭에서 비즈니스 로직을 추출하는 방법을 선택합니다.
 - 애플리케이션 수준: 모든 비즈니스 기능, 트랜잭션, 배치 작업 및 파일에 대한 비즈니스 문서를 생성합니다. 이렇게 하면 애플리케이션의 모든 파일이 선택됩니다.
 - 파일 수준: 파일 테이블에서 선택한 파일에 대해서만 비즈니스 문서를 생성합니다.

i Note

- 두 옵션 중 하나에서 세부 기능 사양 포함을 선택하여 AWS 변환에 선택한 파일에 대한 제어 흐름과 포괄적인 비즈니스 규칙이 포함되도록 할 수 있습니다.
- 선택한 파일은 동일한 인코딩 유형(즉, 모두 동일한 CCSID - UTF8 또는 ASCII)을 가져야 합니다. 그렇지 않으면 생성된 설명서에 빈 필드 또는 섹션이 있을 수 있습니다.

- 설명서는 COBOL 및 JCL 파일에 대해서만 생성할 수 있습니다.
- 애플리케이션 수준의 경우 CICS 트랜잭션 및 배치 작업에 사용되는 프로그램은 함께 그룹화되고 다른 모든 프로그램은 할당되지 않음으로 분류됩니다.

3. 계속을 선택합니다.
4. AWS Transform이 비즈니스 로직을 추출하면 결과를 JSON 형식으로 Amazon S3 버킷에 저장하므로 온라인으로 볼 수 있습니다.

Note

생성된 비즈니스 규칙 파일의 수가 초기 선택보다 클 수 있습니다. 선택한 일부 파일은 추가 종속 파일을 포함하도록 비즈니스 규칙 추출을 트리거할 수 있으며, 결과 테이블에도 표시됩니다.

추출된 비즈니스 설명서 인라인 보기

비즈니스 규칙 추출 단계에서 비즈니스 로직을 볼 수 있습니다. 방법은 다음과 같습니다.

1. 비즈니스 로직 추출 결과 검토로 이동합니다.
2. 테이블에서 보려는 문서를 선택한 다음 결과 보기 버튼을 클릭합니다.

비즈니스 설명서 페이지가 새 브라우저 탭에서 열립니다.

분해

프로그램과 구성 요소 간의 종속성을 설명하는 도메인으로 코드를 분해할 수 있습니다. 이렇게 하면 관련 파일과 프로그램을 동일한 도메인 내에서 적절하게 그룹화할 수 있습니다. 또한 분해 프로세스 중에 애플리케이션 로직의 무결성을 유지하는 데 도움이 됩니다.

Note

분해를 요청하면 AWS 변환은 분해를 수행하는 데 필요한 코드 종속성 분석을 포함하여 코드 분석을 수행합니다. 또한 더 나은 결과를 얻으려면 분해 전에 비즈니스 로직 추출을 수행하는 것이 좋습니다.

애플리케이션 분해를 시작하려면:

1. 왼쪽 탐색 창에서 코드 분해를 선택합니다.

 Note

도메인과 연결되지 않은 모든 파일에 대해 할당되지 않은 하나의 도메인이 자동으로 생성됩니다. 애플리케이션 수준 비즈니스 로직 추출에서 도메인이 제안되지 않은 경우 초기 탐색 시 모든 파일을 할당되지 않음에 연결해야 합니다.

2. 작업 메뉴를 통해 새 도메인을 생성한 다음 도메인 생성을 선택합니다.
3. 도메인 생성에서 도메인 이름, 선택적 설명을 제공하고 일부 파일을 시드로 표시합니다.
 - CICS 구성 파일(CSD) 및 스케줄러 구성 파일(SCL)은 자동 시드 감지에 사용할 수 있습니다.
 - 하나의 도메인만 공통 구성 요소로 설정할 수도 있습니다. 이 도메인의 파일은 여러 도메인에 공통됩니다.
4. 생성(Create)을 선택합니다.

 Note

다른 파일을 시드로 사용하여 여러 도메인을 생성할 수 있습니다.

5. 모든 도메인과 시드를 확인한 후 분해를 선택합니다.
6. AWS 변환은 소스 코드 파일을 확인한 다음 유사한 사용 사례와 높은 프로그래밍 종속성을 가진 프로그램 및 데이터 세트가 있는 도메인으로 분해됩니다.

AWS 변환은 분해된 도메인의 표형 및 그래프 보기를 종속성으로 제공합니다. 그래프 보기에는 세 가지 옵션이 있습니다.

- 도메인 보기 - 시각적 형식으로 서로 다른 도메인이 서로 어떻게 관련되어 있는지 볼 수 있습니다.
- 종속성 보기 - 각 도메인의 모든 파일을 복잡한 종속성 그래프로 볼 수 있습니다. 도메인에 추가된 노드가 동일한 도메인의 시드로부터 정보를 수신하지 못한 경우 이 노드는 할당되지 않음(노드가 정보를 수신하지 않음), 연결 해제됨(시드 정보를 수신하지 않은 하위 그래프) 또는 다른 도메인(노드가 최소한 해당 도메인으로부터 정보를 수신함)으로 예측됩니다.
- Subgraph 보기 - 사용자는 하위 그래프를 생성하여 노드 하위 집합을 시각화하여 해당 노드 컬렉션의 관계적 영향과 경계를 더 명확하게 이해할 수 있습니다.
 - 하위 그래프를 생성하려면 노드 그룹을 선택하고 도구 모음에서 하위 그래프 추출 옵션을 선택합니다.

- 병합하려는 두 하위 그래프 외에도 새 세 번째 하위 그래프를 병합할 때 하위 그래프를 병합할 수 있습니다.

Note

이 단계를 반복하여 도메인을 추가하거나 현재 도메인 구조가 마음에 들지 않는 경우 이미 생성된 도메인을 다른 시드 세트로 재구성합니다.

7. 완료되면 계속을 선택합니다.

시드

시드는 분해 코드 단계의 기본 입력입니다. 각 구성 요소 또는 파일(예: JCL, COBOL, Db2 테이블, CSD 및 스케줄러 파일)을 하나의 도메인에만 시드로 할당하여 분해 프로세스 중에 명확한 경계와 정렬을 보장할 수 있습니다.

시드 식별은 애플리케이션 또는 포트폴리오의 구조에 따라 달라집니다. 일반적인 메인프레임 레거시 애플리케이션의 경우 설정된 명명 규칙, 스케줄러의 배치 수준 그룹화, CICS 시스템에 정의된 트랜잭션 수준 그룹화를 준수하여 시드를 결정할 수 있습니다. 또한 데이터베이스 테이블은 시드 역할을 하여 분해를 위한 또 다른 구조 계층을 제공할 수도 있습니다.

종속성 파일 가져오기 및/또는 업데이트

분해 중에 AWS Transform이 수행하는 종속성 분석에서 생성된 기존 파일을 대체하는 종속성에 대한 JSON 파일을 업로드할 수 있습니다.

종속성 내보내기 함수를 사용하면 분해 단계에서 생성된 종속성 json 파일을 다운로드할 수 있습니다. 다운로드 후 요구 사항에 따라 파일을 수정할 수 있습니다. 그런 다음 종속성 분석에서 생성된 파일을 대체하는 종속성의 새 JSON 파일을 업로드할 수 있는 변환의 업로드 기능을 사용하여 종속성을 가져올 수 있습니다. AWS 그런 다음 분해 단계의 그래프가 업데이트됩니다.

종속성을 내보내고 수정하고 가져오려면

1. 분해 결과 보기 페이지에서 작업을 선택합니다.
2. 드롭다운 목록의 기타 작업에서 종속성 파일 업데이트 옵션을 선택합니다.
3. 종속성 업데이트 파일 모달에서
 - a. 기존 분석 결과에서 생성된 종속성 파일 AWS 변환을 다운로드합니다.
 - b. 다운로드한 파일에서 원하는 것을 기반으로 종속성을 수정합니다.

- c. 수정한 후 종속성 파일 업로드 버튼을 사용하여이 파일을 저장하고 업로드합니다.

 Note

허용되는 유일한 파일 형식은 JSON 파일입니다.

4. 그런 다음 가져오기를 선택합니다.

AWS 변환은 종속성 파일을 가져오고 입력을 기반으로 새 종속성 그래프를 생성합니다.

도메인 가져오기 및/또는 업데이트

분해 단계 전에 도메인, 시드 및/또는 파일 관계가 매핑된 고객의 경우 작업 메뉴를 통해 사용할 수 있는 도메인 파일 가져오기 함수를 통해이 도메인 정의를 업로드할 수 있습니다. 이 함수를 사용할 수 있는 몇 가지 예:

- 다른 작업에서 분해 가져오기
- 이 매핑을 제공하는 주제 전문가

도메인 파일을 가져오면 사용자는 도메인 정의에 대해 분해를 실행하거나 만족하면 도메인 정의를 저장한 다음 제출할 수 있습니다.

Parent/child/neighbor 파일

종속성 그래프에서 프로그램은 서로 다른 유형의 연결을 통해 서로 관련이 있습니다. 이러한 관계를 이해하면 메인프레임 애플리케이션을 변환하는 동안 프로그램 종속성을 분석할 수 있습니다. 또한 도메인의 경계를 이해하는 데 도움이 됩니다. 예를 들어 도메인을 선택한 다음 상위 수준을 한 수준 선택하면 연결된 노드가 표시됩니다.

상위 관계 - 상위 파일이 다른 프로그램을 호출하거나 제어합니다. 상위 항목은 계층 구조에서 종속 프로그램 위에 있습니다. 한 수준 또는 모든 수준에서 상위를 선택할 수 있습니다.

하위 관계 - 상위 프로그램에서 하위 파일을 호출하거나 제어합니다. 하위 항목은 파일 계층 구조에서 상위 항목 아래에 있습니다.

이웃 관계 - 이웃은 동일한 계층 수준의 파일입니다. 동일한 상위 프로그램을 공유하며 서로 직접 상호 작용할 수 있습니다.

코드 재포지토리

Reforge는 대형 언어 모델(LLMs)을 사용하여 리팩터링된 코드의 품질을 개선합니다. 초기 COBOL-to-Java 변환은 COBOL 영향을 받는 데이터 구조와 레거시 시스템의 변수 이름을 유지하면서 기능적 동등성을 유지합니다. 리포지토리에서는 최신 Java 관행과 관용구를 따르도록 코드를 재구성하여 COBOL 스타일 구문을 네이티브 Java 컬렉션 및 명명 규칙으로 대체합니다. 이렇게 하면 Java 개발자가 코드를 더 읽기 쉽고 유지 관리할 수 있습니다.

Note

강화 할당량은 다음과 같습니다.

- 작업당 3,000,000줄의 코드
- 매월 사용자당 50,000,000줄의 코드

다음 단계에 따라 리팩터링 후 코드를 리포지토리합니다.

1. 왼쪽 탐색 창에서 Java 코드 재포지토리를 선택한 다음 코드 재포지 구성을 선택합니다.
2. 압축된 빌드 가능한 소스 프로젝트에 S3 위치를 제공하고 계속을 선택합니다. 이 zip 구조를 사용합니다.

```
input.zip
    ### PROJECT-pom
    ### PROJECT-entities
    ### PROJECT-service
    ### PROJECT-tools
    ### PROJECT-web (optional)
    ### pom.xml
```

AWS 변환은 zip 패키지를 분석하여 PROJECT-service 디렉터리 내에서 파일을 찾아 재포지토리할 수 있는 선택 가능한 클래스 목록을 제공할 수 있도록 합니다. 이러한 클래스에는 접미사가 있습니다ProcessImpl.java.

3. 리포지토리할 클래스 선택 페이지를 완료하고 계속을 선택합니다. Worklog 탭에서 재포지 상태를 추적합니다.
4. 클래스당 재포지 상태를 표시하는 결과 보기 페이지에서 완료된 재포지의 결과를 봅니다. 또한 S3 버킷에서 Reforge 결과를 찾을 위치를 지정합니다.

AWS 변환이 입력을 가져오면 Reforge 결과가 포함된 다운로드 가능한 파일이 제공됩니다.

이는 성공적인 재포지션으로 인한 zip 구조입니다.

```
reforge.zip
### maven_project
### reforge.log
###tokenizer_map.json
```

- maven_project에는 보강된 소스 코드가 포함되어 있습니다.
 - 리팩터링되었지만 컴파일이 성공적으로 완료되지 않은 파일은에 있으며 이름이 /src/main/resources/reforge/originalClassName.java.incomplete입니다originalClassName.java.incomplete. 이를 파일의 원래 버전과 비교하여 저장하려는 재조립된 함수를 선택합니다.
 - AWS 변환에 제공되고 성공적으로 리팩터링된 소스 파일은에 백업src/main/resources/reforge/originalClassName.java.original되며 이름이 지정됩니다originalClassName.java.original. 리팩터링된 버전의 파일은 AWS 변환에 제공된 소스 파일을 대체합니다.

Note

보강 프로세스가 성공한 경우에만 originalClassName.java 파일이 보강된 파일로 대체됩니다. 그렇지 않으면 원본 콘텐츠가 유지됩니다.

- reforge.log에는 작업 실패를 진단하거나 문제 발생 시를 AWS 지원하는 데 사용할 수 있는 로그가 포함되어 있습니다.
- tokenizer_map.json에는 개인 정보 보호를 위해 로그에 토큰화된 파일 경로 및 클래스/메서드 이름과 같은 데이터에 대한 토큰 IDs 매핑이 포함되어 있습니다. 문제가 발생할 경우 AWS 이 파일을 지원하도록 제공할 수 있습니다.

현대화된 애플리케이션 테스트 계획

추출된 코드 속성, 작업 복잡성 및 스케줄러 경로를 기반으로 메인프레임 현대화된 애플리케이션에 대한 테스트 계획을 생성하고 관리할 수 있습니다. AWS 변환은 각 테스트 사례에 필요한 특정 아티팩트를 테스트하고 식별할 작업의 우선순위를 지정하는 데 도움이 됩니다. 테스트 계획 프로세스는 구성, 범위 지정 및 검토의 세 가지 주요 단계로 나뉩니다.

테스트 계획을 생성하려면

1. 테스트 계획 설정 구성

- a. 왼쪽 탐색 창의 테스트 계획에서 설정 구성을 선택합니다.
- b. (선택 사항) 비즈니스 로직 추출(BLE)을 위한 S3 경로를 제공합니다. 이러한 아티팩트는 테스트 계획 품질을 향상시킵니다. BLE 아티팩트가 없으면 테스트 계획의 일부 필드가 불완전하게 유지될 수 있습니다.

2. 테스트 계획 범위 정의

- a. 테스트 계획에 포함할 배치 작업과 같은 진입점을 선택합니다.
- b. 여러 속성을 기반으로 작업을 필터링하고 정렬합니다.
 - 비즈니스 기능(BRE BLE에서 발체)
 - 도메인(분해 단계에서)
 - 파일 경로 및 위치
 - 사용자 지정 검색 기준
- c. 테스트할 개별 작업 또는 전체 그룹을 선택합니다.
- d. 작업 관계 및 종속성을 검토합니다.

3. 테스트 계획 검토 및 조정

생성된 테스트 계획은 다음을 포함한 포괄적인 정보를 제공합니다.

- 종속성을 기반으로 하는 기본 실행 순서
- 스케줄러의 작업 그룹 할당
- 테스트 사례에 대한 집계 점수인 복잡성 점수
- 비즈니스 도메인 연결
- 순환 복잡성 지표
- 데이터 세트 및 테이블 종속성
- 코드 지표 행
- 비즈니스 함수 매핑

테스트 계획 사용자 지정 옵션

특정 요구 사항을 충족하도록 테스트 계획을 사용자 지정할 수 있습니다. 예를 들어, 다음을 수행할 수 있습니다.

- 여러 진입점을 선택하여 새 테스트 사례 생성
- 기존 테스트 사례를 병합하여 관련 기능 결합
- 보다 세분화된 테스트를 위한 테스트 사례 분할
- 불필요한 테스트 사례 제거
- 기존 테스트 사례에 대한 진입점 추가 또는 제거
- 테스트 사례 설명 및 속성 수정
- 실행 순서 조정

자세한 테스트 사례 정보

각 테스트 사례는 콘텐츠와 관련 데이터 세트 또는 데이터 파일을 설명하는 세부 정보를 제공합니다.

- 테스트 범위에 대한 포괄적인 설명
- 포함된 진입점의 전체 목록
- 복잡성과 크기를 보여주는 집계 지표
- 비즈니스 규칙 및 자동화된 테스트 사례 지침
- 방향(입력/출력)이 있는 데이터 세트 및 테이블 종속성
- 대화형 종속성 그래프 시각화
- 실행 사전 조건 및 요구 사항

데이터 관리 기능

이러한 세부 정보는 테스트 사례와 관련된 데이터를 이해하는 데 도움이 됩니다. 다음을 수행할 수 있습니다.

- 입력/출력 방향을 기준으로 데이터 세트 필터링
- 테스트 실행에 필요한 아티팩트 식별
- 테스트 사례 간 데이터 종속성 추적
- 테스트 계획 전반의 데이터 세트 사용량 모니터링

Note

AWS 변환은 스케줄러 종속성을 자동으로 분석하고 복잡성 점수를 할당하여 테스트 작업의 우선순위를 정하는 데 도움이 됩니다. 복잡성 점수가 높을수록 테스트 프로세스 중에 더 철저한 테스트 또는 격리가 필요할 수 있는 작업을 나타냅니다.

비즈니스 규칙 및 테스트 사례 지침

AWS 변환 테스트 계획은 비즈니스 규칙 추출을 기반으로 테스트 사례 계획에 대한 권장 사항을 제공합니다.

- LLM을 사용한 비즈니스 규칙 자동 처리
- 합성 테스트 사례 생성
- 특정 비즈니스 시나리오에 대한 테스트 지침
- 규칙과 테스트 사례 간의 추적성

최종 테스트 계획은 지정된 S3 위치에 저장되며 테스트 전략을 효과적으로 실행하는 데 필요한 모든 정보를 포함합니다. 다른 테스트 도구 또는 설명서 시스템과의 통합을 위해 테스트 계획을 내보낼 수 있습니다.

Note

합성 테스트 사례 지침이 제공되지만 실제 테스트 아티팩트는 지침에 따라 별도로 생성해야 합니다. 테스트 계획은 테스트 전략을 위한 포괄적인 청사진 역할을 하지만 테스트 데이터 또는 실행 스크립트는 생성하지 않습니다.

테스트 사례 생성 규칙 - 요약**일반 규칙**

- 테스트 사례에는 일정 실행 순서로 1~ 많은 JCLs 포함됩니다.
- 테스트 사례는 지원되는 유효한 스케줄러(CA7 및 Control-M)에서 생성됩니다.
- 테스트는 스케줄러 자체 또는 예약된 작업이 아닌 JCLs을 실행합니다.
- 예약된 작업은 고유하며 하나의 JCL만 실행합니다.

- 여러 예약된 작업에서 하나의 JCL을 실행할 수 있습니다.
- 일정에 없는 JCL 하나가 존재할 수 있습니다.

기본 테스트 사례 생성 규칙

- 테스트 케이스에 단일 JCL이 있는 경우:
 - JCL이 일정에 관여하지 않음
 - JCL은 여러 브랜치로 분기되는 예약된 작업에 의해 실행됩니다.
 - 일정의 브랜치에는이 JCL만 포함됩니다.
- 테스트 사례에서 여러 JCL인 경우:는 일정 브랜치 내의 선형 실행 경로 시퀀스를 나타냅니다.
- JCL이 서로 다른 예약된 작업에 있는 경우: JCL은 별도의 테스트 케이스가 됩니다.
- JCL이 수렴 예약 작업에 있는 경우: JCL은 새 테스트 사례를 시작할 수 있지만 이전 브랜치에는 포함되지 않습니다.
- 누락된 JCLs 건너뛰고 실행을 계속합니다(누락된 JCL 지점에서 테스트 사례를 잘라내기 위한 향후 개선 계획).

사용자 작업 규칙

- 테스트 사례 생성: 사용자가 사용 가능한 JCLs 중에서 선택
 - JCLs이 일정 실행 브랜치 시퀀스에 존재하는 경우 성공
 - 일정 실행 순서를 따릅니다.
- 테스트 사례에 JCL 추가: 사용자가 사용 가능한 JCLs 중에서 선택
 - 테스트 사례의 일정 실행 브랜치/경로에 JCL이 존재할 수 있는지 확인
- 테스트 사례에서 JCL 제거: 사용자는 테스트 사례에서 모든 JCL을 제거할 수 있습니다.
 - 실행 경로 간격이 발생하더라도 허용됨
- 테스트 사례 병합: 사용자가 결합할 두 개의 테스트 사례를 선택합니다.
 - JCLs이 동일한 일정 실행 브랜치에 함께 존재할 수 있는 경우 성공
 - 일정 실행 순서를 유지합니다.
- 테스트 사례 분할: 사용자가 테스트 사례에서 분할할 JCL 하나를 선택합니다.
 - 분할 지점에서 앞으로 새 테스트 사례를 생성합니다.
 - 분할점을 지나 JCLs 제외하도록 수정된 원래 테스트 사례
- 테스트 사례 삭제: 사용자가 생성된 테스트 사례를 삭제할 수 있습니다.

Note

다른 스케줄러 브랜치/경로에서 테스트 사례를 생성, 추가 또는 병합할 수 없습니다. 스케줄러에서 분산/수렴 작업을 초과하는 작업을 허용하도록 향후 개선이 계획되어 있습니다.

테스트 데이터 수집 스크립트 생성

JCL 스크립트를 생성하여 이전 단계에서 생성된 테스트 계획을 기반으로 메인프레임 시스템에서 테스트 데이터를 수집할 수 있습니다. AWS 변환은 포괄적인 테스트에 필요한 데이터 세트, 데이터베이스 테이블 및 순차 파일에 대한 데이터 수집 스크립트를 자동으로 생성합니다. 데이터 수집 프로세스는 입력 구성, 테스트 사례 선택, 스크립트 구성, 스크립트 생성의 네 가지 주요 단계로 나뉩니다.

테스트 데이터 수집 스크립트를 생성하려면

1. 테스트 계획 입력 제공
 - a. 왼쪽 탐색 창의 테스트 데이터 수집에서 테스트 계획 입력 제공을 선택합니다.
 - b. [현대화된 애플리케이션 테스트 계획에서 테스트 계획](#) JSON 파일의 S3 경로를 지정합니다.
 - c. 이전 작업 단계에서 테스트 계획이 생성된 경우 입력 필드가 미리 채워집니다.
 - d. 적절한 S3 위치를 지정하여 다른 작업에서 테스트 계획을 선택할 수도 있습니다.
2. 데이터 수집을 위한 테스트 사례 선택
 - a. 테스트 계획에서 테스트 사례의 전체 목록을 검토합니다.
 - b. 여러 속성을 기반으로 테스트 사례를 필터링하고 정렬합니다.
 - 비즈니스 기능 및 도메인
 - 데이터베이스 테이블 종속성
 - 데이터 세트 요구 사항
 - 복잡성 지표
 - 사용자 지정 검색 기준
 - c. 개별 테스트 사례를 선택하거나 대량 선택 옵션을 사용합니다.
 - d. 세부 정보를 보려면 테스트 사례 하나를 클릭하여 진입점, 지표 및 비즈니스 규칙을 포함한 테스트 사례 세부 정보를 검토합니다.
3. 데이터 수집 스크립트 구성
 - a. 참조용 샘플 템플릿 및 구성 파일을 다운로드합니다.

- AWS 변환은 프로세스에 필요한 템플릿 종류에 대한 지침으로 사용할 Db2 데이터베이스 언로드, VSAM 파일 REPRO 및 순차 데이터 세트 처리를 위한 샘플 템플릿을 제공합니다.
 - 표준은 사이트마다 다를 수 있으므로 고객은 자체 표준에 따라 이러한 템플릿을 수정하거나 교체해야 합니다.
 - 이러한 수정된 템플릿은 테스트 데이터 수집이 처리할 수 있는 S3 버킷에 업로드해야 합니다.
- b. 다음을 포함하는 변수 구성 파일(JSON 형식)을 제공합니다.
- 사용자 접두사 및 환경별 상수
 - 데이터베이스 구성 파라미터
 - 대상 엔드포인트 설정 및 데이터 전송 파라미터
 - 사용자가 정의하고 JCL 템플릿에 사용할 기타 필수 파라미터
- c. 다양한 데이터 수집 방법에 대한 JCL 템플릿을 업로드합니다.
- Db2 템플릿: 데이터베이스 테이블 언로드용(BMC, IBM DSN 또는 기타 언로드 유틸리티에 맞게 사용자 지정)
 - VSAM 템플릿: VSAM 파일 처리용(일반적으로 REPRO 유틸리티 사용)
 - 순차 데이터 세트 템플릿: 순차 데이터 세트, 분할된 데이터 세트, GDGs.

4. 생성된 스크립트 검토 및 관리

생성된 스크립트는 다음을 포함한 포괄적인 데이터 수집 기능을 제공합니다.

- "이전" 및 "이후" 테스트 실행 데이터 수집에 대한 별도의 스크립트
- 테스트 사례 및 데이터 유형별로 구성된 스크립트 구조
- 스크립트는 쉽게 액세스하고 전송할 수 있도록 S3 버킷에 자동으로 저장됩니다.
- 생성된 JCL 스크립트가 메인프레임 실행 준비 완료
- 변수 대체는 템플릿에 정의된 사용자 구성을 기반으로 합니다.

스크립트 생성 기능

생성된 스크립트는 템플릿 및 구성에 따라 자동으로 사용자 지정됩니다.

- 템플릿 기반 생성: 변수 대체와 함께 제공된 JCL 템플릿을 사용합니다.
- 환경: 특정 메인프레임 구성 통합

- 데이터 유형 처리: 순차 데이터 세트, VSAM 파일 및 데이터베이스 테이블에 적합한 스크립트를 생성합니다.
- 테스트 사례 수집: "이전" 및 "이후" 데이터 수집 스크립트를 모두 생성합니다.
- 순차적 데이터 세트 처리: AWS 제공된 샘플은 파일 전송 함수를 제공하지만 사이트에서 사용할 수 있는 압축 유틸리티 또는 Connect Direct 또는 관리형 파일 전송 등과 같은 유틸리티에 맞게 사용자 지정할 수 있습니다.

데이터 수집 전략

생성된 스크립트는 포괄적인 데이터 수집 전략을 지원합니다.

- 순차적 데이터 세트 수집: VSAM 및 플랫 파일의 REPRO 및 복사 유틸리티
- 데이터베이스 테이블 언로드: 사용자 지정 가능한 Db2 언로드 프로세스
- 순차 데이터 세트 처리: 압축, 관리형 파일 전송 서비스 등과 같은 순차 데이터 세트의 사용자 지정 가능한 사후 처리
- 종속성 관리: 테스트 사례 정의를 기반으로 조정된 컬렉션

Note

AWS 변환은 템플릿과 구성을 기반으로 스크립트를 생성합니다. 메인프레임 환경에서 실행하기 전에 생성된 모든 JCL을 검토하여 특정 시스템 구성 및 보안 요구 사항과의 호환성을 확인합니다.

템플릿 사용자 지정 및 모범 사례

ATX 테스트 데이터 수집은 유연한 템플릿 사용자 지정 기능을 제공합니다.

- 다중 유틸리티 지원: 다양한 메인프레임 유틸리티(BMC, IBM, DSN)에 맞게 템플릿 조정
- 변수 기반 구성: 환경별 파라미터에 상수 사용
- 재사용 가능한 템플릿: 일관된 스크립트 생성을 위한 표준화된 템플릿 생성
- 데이터 처리: 조직별 데이터 처리 요구 사항 통합
- 보안 통합: 적절한 보안 및 액세스 제어 포함
- 성능 최적화: 효율적인 데이터 수집 및 전송을 위한 구성

생성된 출력 구조

생성된 스크립트는 S3 버킷에 다음과 같은 구조로 구성됩니다.

- 테스트 사례 조직: 관련 테스트 사례별로 그룹화된 스크립트
- 수집 타이밍: "이전" 및 "이후" 데이터 수집을 위한 별도의 폴더
- 데이터 유형 분류: 순차 데이터 세트, 데이터베이스 테이블 및 전송별로 구성된 스크립트
- 메타데이터 파일: 요약 정보 및 실행 지침
- Ready-to-transfer 가능 형식: 직접 메인프레임 배포를 위한 JCL 형식

최종 스크립트 컬렉션은 지정된 S3 위치에 저장되며 데이터 수집 전략을 효과적으로 실행하는 데 필요한 모든 JCL을 포함합니다. 스크립트를 다운로드하여 메인프레임 환경으로 전송하거나 자동 배포 프로세스와 통합할 수 있습니다.

Note

포괄적인 JCL 스크립트가 생성되는 동안 메인프레임 환경에서 실제 실행을 수행해야 합니다. 스크립트는 ready-to-use 데이터 수집 도구 역할을 하지만 적절한 메인프레임 액세스 및 실행 권한이 필요합니다.

자동화 스크립트 생성 테스트

테스트 자동화 스크립트를 생성하여 이전 단계에서 생성한 테스트 계획을 기반으로 현대화된 애플리케이션에서 테스트 사례를 실행할 수 있습니다. AWS 변환은 테스트 데이터 수집 프로세스에서 수집된 데이터를 활용하는 포괄적인 테스트 스크립트를 자동으로 생성합니다. 테스트 자동화 스크립트 생성 프로세스는 입력 구성, 테스트 사례 선택, 스크립트 생성 결과의 세 가지 주요 단계로 구성됩니다.

테스트 스크립트를 생성하려면

1. 테스트 계획 입력 제공
 - a. 왼쪽 탐색 창의 자동화 스크립트 생성 테스트에서 테스트 계획 입력 제공을 선택합니다.
 - b. [현대화된 애플리케이션 테스트 계획에서 테스트 계획](#) JSON 파일의 S3 경로를 지정합니다.
 - c. 이전 작업 단계에서 테스트 계획이 생성된 경우 입력 필드가 미리 채워집니다.
 - d. 적절한 S3 위치를 지정하여 다른 작업에서 테스트 계획을 선택할 수도 있습니다.
 - e. 시스템은 이 테스트 계획을 자동화 스크립트를 생성하기 위한 기반으로 사용합니다.

2. 스크립트 생성을 위한 테스트 사례 선택

- a. 테스트 계획에서 테스트 사례의 전체 목록을 검토합니다.
- b. 여러 속성을 기반으로 테스트 사례를 필터링하고 정렬합니다.
 - 비즈니스 기능 및 도메인
 - 데이터베이스 테이블 종속성
 - 데이터 세트 요구 사항
 - 복잡성 지표
 - 사용자 지정 검색 기준
- c. 개별 테스트 사례를 선택하거나 모두 확인 및 모두 선택 취소 버튼이 있는 대량 선택 옵션을 사용합니다.
- d. 개별 테스트 사례를 클릭하여 진입점, 지표 및 비즈니스 규칙을 포함한 테스트 사례 세부 정보를 검토합니다.

선택한 테스트 사례에는 현대화된 애플리케이션에서 실행하기 위해 생성된 자동화 스크립트가 있습니다.

3. 생성된 테스트 자동화 스크립트를 검토하고 관리합니다.

- 스크립트 생성 완료를 확인하는 성공 메시지가 표시됩니다.
- 생성된 테스트 스크립트는 지정된 S3 버킷 위치에 자동으로 저장됩니다.
- 해당 S3 위치를 사용하여 생성된 테스트 스크립트의 전체 목록에 액세스합니다.
- 각 테스트 사례에는 개별 S3 위치에 저장된 해당 자동화 스크립트가 있습니다.
- 스크립트는 현대화된 애플리케이션 환경에서 배포 및 실행할 준비가 되어 있습니다.

자동화 스크립트 기능 테스트

생성된 자동화 스크립트는 포괄적인 테스트 기능을 제공합니다.

- 현대화된 애플리케이션 테스트: 스크립트는 변환된 애플리케이션에서 테스트 사례를 실행하도록 특별히 설계되었습니다.
- 데이터 통합: 이전 테스트 데이터 수집 단계에서 수집한 테스트 데이터를 사용하므로 각 테스트 사례에 대해 이러한 데이터를 폴더에 복사해야 합니다.
- 자동 실행: 스크립트를 사용하여 데이터 싱크를 설정하고, 테스트 사례를 실행하고, 결과를 비교할 수 있으며, 일부 파라미터는 배포 환경에 따라 설정해야 합니다.

- 조직 구조: 스크립트는 S3 버킷의 테스트 사례별로 체계적으로 구성됩니다.
- Ready-to-deploy 가능 형식: 스크립트는 테스트 환경에 직접 배포하도록 형식이 지정됩니다.

생성된 출력 구조

생성된 테스트 자동화 스크립트는 S3 버킷에 다음과 같은 구조로 구성되어 있습니다.

- 테스트 사례 조직: 각 테스트 사례에는 개별 S3 폴더에 저장된 전용 스크립트가 있습니다.
- 실행 준비 형식: 스크립트는 환경에 따라 일부 변수를 설정한 후 즉시 배포 및 실행하도록 형식이 지정됩니다.
- 중앙 집중식 액세스: 간편한 관리를 위해 단일 S3 버킷 위치에서 모든 스크립트에 액세스할 수 있습니다.

테스트 실행 전략

생성된 스크립트는 포괄적인 테스트 실행 워크플로를 지원합니다.

- 환경 설정: 스크립트에는 테스트를 실행하도록 초기 데이터를 설정하는 기능이 포함되어 있습니다.
- 데이터 준비: 테스트 사례 데이터 수집 단계에서 수집된 테스트 데이터와 통합
- 테스트 사례 실행: 현대화된 애플리케이션에서 개별 테스트 사례의 자동 실행
- 결과 비교: 테스트 결과를 비교하고 애플리케이션 동작을 검증하기 위한 기본 제공 기능

Note

AWS 변환은 테스트 계획 및 선택한 테스트 사례를 기반으로 테스트 자동화 스크립트를 생성합니다. 스크립트는 현대화된 애플리케이션 환경에서 실행하도록 설계되었으며 이전 단계에서 수집된 테스트 데이터를 활용합니다. 배포 전에 생성된 모든 스크립트를 검토하여 특정 애플리케이션 구성 및 테스트 요구 사항과의 호환성을 확인합니다.

테스트 자동화 모범 사례

- 환경 검증: 스크립트 실행 전에 현대화된 애플리케이션 환경이 올바르게 구성되었는지 확인합니다.
- 데이터 확인: 수집 단계의 필수 테스트 데이터를 사용할 수 있고 액세스할 수 있는지 확인합니다.
- 스크립트 사용자 지정: 특정 테스트 요구 사항에 따라 생성된 스크립트를 검토하고 사용자 지정합니다.

- 실행 모니터링: 테스트 스크립트 실행 중에 적절한 모니터링 및 로깅 구현
- 결과 분석: 테스트 결과를 분석하고 애플리케이션 문제를 식별하기 위한 프로세스 설정

테스트 자동화 스크립트의 최종 모음은 현대화된 애플리케이션 기능을 검증하기 위한 완전한 테스트 프레임워크를 제공합니다. 스크립트는 지속적 테스트 프로세스에 통합하거나 애플리케이션 검증 워크플로의 일부로 실행할 수 있습니다.

AWS 변환의 배포 기능

AWS 변환은 ready-to-use 수 있는 코드형 인프라(IaC) 템플릿을 제공하여 현대화된 메인프레임 애플리케이션을 위한 클라우드 환경을 설정하는 데 도움이 됩니다. 채팅 인터페이스 AWS 변환을 통해 컴퓨팅 리소스, 데이터베이스, 스토리지 및 보안 제어와 같은 필수 구성 요소를 생성하는 사전 구축된 템플릿에 액세스할 수 있습니다. 템플릿은 CloudFormation (CFN) AWS Cloud Development Kit (AWS CDK) 및 Terraform을 비롯한 인기 있는 형식으로 제공되므로 인프라를 유연하게 배포할 수 있습니다.

이러한 템플릿은 현대화된 메인프레임 애플리케이션에 대한 환경을 구성하는 데 필요한 시간과 전문 지식을 줄이는 구성 요소 역할을 합니다. 필요에 맞게 이러한 템플릿을 사용자 지정하여 배포 환경을 구축할 수 있는 기반을 제공할 수 있습니다.

IaC 템플릿을 검색하려면 AWS 선호하는 현대화 패턴(예: 메인프레임 리팩터링을 위한 AWS 변환), 선호하는 토폴로지(독립 실행형 대 고가용성) 및 선호하는 형식(CloudFormation 대 클라우드 개발 키트 대 Terraform)을 명확히 설명하는 Infrastructure-as-Code 템플릿을 변환 채팅에서 요청하세요.

리팩터링 후 현대화된 애플리케이션 구축 및 배포

AWS 변환으로 리팩터링 프로세스를 완료한 후 현대화된 Java 애플리케이션을 빌드하고 배포할 수 있습니다. 이 가이드에서는 현대화된 코드를 검색하고, 환경을 구성하고, 애플리케이션을 배포 및 테스트하는 방법을 안내합니다.

Note

여기에 제공된 지침 외에도 AWS 변환 생성 코드 패키지에는 [개발자 런타임](#)과 IDE(통합 개발 환경)를 설정하는 지침을 제공하는 AWS 자동 리팩터 개발 환경 설정 문서가 포함됩니다.

주제

- [사전 조건](#)

- [1단계: 현대화된 코드 검색](#)
- [2단계: 현대화된 애플리케이션 구축](#)
- [3단계: 테스트 환경 구성](#)
- [4단계: 현대화된 애플리케이션 배포](#)
- [5단계: 현대화된 애플리케이션 테스트](#)
- [추가 예](#)

사전 조건

시작하기 전에, 다음 사항을 확인해야 합니다.

- AWS 변환으로 리팩터링 작업을 성공적으로 완료했습니다.
- 현대화된 코드에 대한 액세스.
- [Apache Maven 또는 Apache Tomcat](#)과 같은 개발 시스템에 빌드 소프트웨어 도구 스택을 설치하고 구성했습니다. 런타임 버전 관리에 대한 자세한 내용은 [AWS 메인프레임 런타임용 변환 릴리스 정보를 참조하세요](#).
- Amazon Corretto 또는 Java 런타임 버전을 설치하고 구성했습니다. Amazon Corretto 설치에 대한 자세한 내용은 [Amazon Corretto 24](#)를 참조하세요.
- 필요한 경우 런타임 구성 요소에 대한 Amazon Aurora PostgreSQL 데이터베이스를 생성하고 구성할 수 있는 액세스 권한. Aurora PostgreSQL 데이터베이스 생성에 대한 자세한 내용은 [Amazon Aurora PostgreSQL 작업을 참조하세요](#).
- 런타임 환경에 애플리케이션을 배포하기 위한 관리 액세스.
- AWS 자동화된 리팩터링 솔루션으로 현대화된 애플리케이션의 기본 개념에 대한 [AWS 메인프레임 런타임용 변환](#) 개념을 검토했습니다.

1단계: 현대화된 코드 검색

현대화된 코드를 검색하려면

1. 생성된 코드 패키지를 다운로드하고 추출합니다.
2. `codebase/app-pom/pom.xml` 열고 필요한 런타임 엔진 버전을 기록해 둡니다. 예:
`<gapwalk.version>4.6.0</gapwalk.version>`.
3. 참조용으로 다운로드한 코드 패키지에서 AWS 자동 리팩터링 개발 환경 설정 문서를 찾습니다.

2단계: 현대화된 애플리케이션 구축

현대화된 애플리케이션을 빌드하려면

1. 메인프레임용 AWS 변환 도구 상자에서 런타임에 액세스합니다.
2. 로컬 개발 시스템에 적절한 런타임 버전(에서 식별됨 [the section called “1단계: 현대화된 코드 검색”](#))을 다운로드하여 설치합니다.

Note

로컬 시스템에 런타임 종속성을 설치하기 위한 추가 정보는 AWS 자동 리팩터링 개발 환경 설정 문서의 섹션 3.1에서 확인할 수 있습니다.

3. 명령 프롬프트를 열고 애플리케이션의 루트 디렉터리로 이동합니다.
4. 현대화된 애플리케이션을 위한 배포 가능한 패키지를 빌드하려면 Maven 빌드 명령을 실행합니다.

```
mvn package
```

현대화된 코드의 기본 구성에 대한 자세한 내용은 [Application Organization](#) 페이지를 참조하세요. 예를 들어 프런트 엔드 웹 애플리케이션이 포함된 현대화된 애플리케이션의 경우 런타임 구성 요소 외에도 다음과 같은 배포 가능한 .war 집계가 필요할 수 있습니다.

- 서비스 프로젝트: 레거시 비즈니스 로직 현대화 요소 포함

```
<business-app>-service.*.war
```

- 웹 프로젝트: 사용자 인터페이스 관련 요소의 현대화 포함

```
<business-app>-web.*.war
```

3단계: 테스트 환경 구성

테스트 환경을 구성하려면

1. 현대화된 애플리케이션 런타임을 구성합니다. 자세한 내용은 AWS Mainframe Modernization 사용 설명서의 [런타임에 대한 구성 설정](#) 섹션을 참조하세요.

Note

런타임 구성 요소별 구성 예제는 AWS 자동 리팩터링 개발 환경 설정 가이드의 섹션 5를 참조하세요.

2. 현대화된 애플리케이션을 위한 입력 및 출력(I/O) 데이터 세트를 준비합니다. 현대화된 애플리케이션은 순차 I/O 데이터 세트, VSAM 데이터 세트 등을 처리할 수 있습니다.

Note

예제는 자동 리팩터링 개발 환경 설정의 섹션 6을 참조하세요 AWS .

3. 런타임 환경 - 기존 런타임 환경을 사용하거나 새 런타임 환경을 생성할 수 있습니다.
 - 비관리형 런타임 환경을 구성하려면 [비관리형 애플리케이션 설정을 참조하세요](#).
 - 관리형 런타임 환경을 구성하려면 [관리형 애플리케이션 설정을 참조하세요](#).

테스트 환경을 구성한 후 현대화된 애플리케이션을 배포하는 다음 단계로 이동합니다.

4단계: 현대화된 애플리케이션 배포

[the section called “2단계: 현대화된 애플리케이션 구축”](#) 및 [the section called “3단계: 테스트 환경 구성”](#) 섹션에서 생성 및/또는 구성한 런타임에 애플리케이션 아티팩트를 배포합니다.

현대화된 애플리케이션 배포에 대한 추가 지침은 다음 링크를 사용하여 확인할 수 있습니다.

- [Amazon EC2에 배포](#)
- [Amazon ECS 및 Amazon EKS의 컨테이너에 배포](#)
- [AWS Mainframe Modernization 애플리케이션 생성](#)

5단계: 현대화된 애플리케이션 테스트

배포 후

1. 현대화된 애플리케이션과 상호 작용하는 방법은 사용 가능한 [런타임 APIs](#)를 검토하세요.
2. 애플리케이션을 테스트하여 기능적 동등성을 레거시 애플리케이션과 일치시킵니다. 예를 들어 사용 [AWS Mainframe Modernization 설명서의 샘플 애플리케이션 테스트를 참조하세요](#).

추가 예

AWS 변환을 사용하여 메인프레임 애플리케이션을 현대화하는 구체적인 예는 [CardDemo 메인프레임 애플리케이션 현대화를](#) 참조하세요.

풀 스택 Windows 현대화

AWS 변환은 .NET 현대화 및 SQL Server 현대화를 포함한 풀 스택 Windows 현대화를 제공합니다.

.NET용 AWS 변환 에이전트를 사용하면 .NET 애플리케이션을 교차 플랫폼 .NET과 호환되도록 현대화할 수 있습니다. .NET [웹 앱 또는 .NET IDE를 사용하여 .NET](#)을 현대화할 수 있습니다.

AWS [SQL Server 현대화](#)를 위한 변환은 Microsoft SQL Server 데이터베이스 및 관련 .NET 애플리케이션을 Amazon Aurora PostgreSQL로 전체 스택 현대화를 자동화하는 AI 기반 서비스입니다. 이 서비스는 스키마 변환, 데이터 마이그레이션, 새로운 대상 PostgreSQL과 일치하도록 애플리케이션 코드 수정 등 전체 마이그레이션 여정을 오케스트레이션하므로 복잡하고 노동 집약적인 작업을 자동화하여 팀의 생산성을 높일 수 있습니다.

주제

- [AWS 변환을 통한 .NET 현대화](#)
- [SQL Server 현대화](#)

AWS 변환을 통한 .NET 현대화

.NET용 AWS 변환 에이전트를 사용하면 .NET 애플리케이션을 교차 플랫폼 .NET과 호환되도록 현대화할 수 있습니다. 이 기능을 .NET 현대화라고 합니다. AWS 변환 [AWS 환경 변환](#) 후 .NET 현대화 변환 작업을 생성할 수 있습니다.

환경

AWS 변환은 다음과 같은 여러 환경에서 사용할 수 있습니다.

- 웹 콘솔: 한 번에 최대 500개의 리포지토리를 대규모로 변환하는 데 사용됩니다.
- Visual Studio IDE: 에이전트와 함께 대화식 및 반복적으로 작동하는 솔루션 또는 프로젝트의 개발자 주도 변환입니다. 중간 규모에서 대규모 프로젝트에 권장됩니다.

웹 콘솔과 IDE 간에 자유롭게 전환하여 변환 작업을 수행할 수 있습니다.

다른 IDEs 및 AI 코드 컴패니언에서 AWS 변환을 호출할 수도 있습니다.

- Kiro: Kiro용 변환 파워를 사용하여 Kiro에서 AWS 변환합니다.

- 기타 AI 코드 컴패니언: 변환 MCP 에이전트를 사용하여 선호하는 AI 코딩 어시스턴트에서 AWS 변환합니다.

기능 및 주요 기능

- 소스 제어 시스템의 .NET Framework 코드베이스를 분석합니다. 여기에는 프라이빗 NuGet 지원, 교차 리포지토리 종속성 식별, 분석 보고서 제공이 포함됩니다.
- 레거시 .NET Framework 애플리케이션을 교차 플랫폼 .NET, 이메일 알림 및 변환 요약 보고서로 자동 변환합니다.
- 소스 제어 플랫폼(BitBucket, GitHub 및 GitLab)과 쉽게 통합하여 기존 코드를 수집하고 변환된 코드를 새 브랜치에 커밋합니다.
- 단위 테스트를 통한 변환된 코드 검증.

지원되는 버전 및 프로젝트 유형

AWS 변환은 다음 .NET 버전에 대한 변환을 지원합니다.

- .NET Framework 3.5 이상
- .NET Core 3.1
- .NET 5.x 이상
- .NET 8

AWS 변환은 다음과 같은 대상 .NET 버전으로 변환할 수 있습니다.

- .NET 8
- .NET 10

AWS 변환은 다음과 같은 유형의 프로젝트 변환을 지원합니다(C#만 해당).

- 클래스 라이브러리
- 콘솔 애플리케이션
- ASP.NET:
 - 프런트엔드 Razor Views를 포함한 모델 보기 컨트롤러(MVC)
 - 단일 페이지 애플리케이션(SPA) 백엔드(비즈니스 로직 계층)

- 웹 API
- 웹 양식
- 단위 테스트 프로젝트(NUnit, xUnit 및 MSTest)
- Windows Communication Foundation(WCF) 서비스
- 타사 또는 프라이빗 NuGet 패키지에 제공된 교차 플랫폼 버전이 있는 프로젝트. 교차 플랫폼이 누락되거나 사용할 수 없는 경우.NET용 AWS 변환은 최선의 변환을 시도합니다.

AWS 또한 변환은 다음 프로젝트 유형을 최신 .NET으로 변환할 수 있습니다. 이 기능은 미리 보기 기능이며 지원되는 프로젝트 유형만큼 완전히 변환되지 않을 수 있습니다.

- WinForms 데스크톱 프로젝트.
- WPF 데스크톱 프로젝트.
- Xamarin 모바일 프로젝트.
- VB.NET 작성된 프로젝트.

제한 사항

AWS 변환의 할당량 및 제한에 대한 자세한 내용은 섹션을 참조하세요 [AWS 변환 할당량](#).

AWS 변환은 다음을 변환하지 않습니다.

- Blazor UI 구성 요소
- 코어 호환 라이브러리가 없는 Win32 DLLs
- 솔루션이 포함되지 않은 리포지토리.

AWS 변환은 원래 리포지토리 브랜치를 수정하지 않으며 변환 계획에 지정된 별도의 대상 브랜치에만 쓸 수 있습니다.

인적 개입

.NET Framework 애플리케이션을 교차 플랫폼 .NET으로 이식하는 동안 다음 시나리오에서 입력 또는 승인을 제공하도록 요청할 수 있습니다.

- 소스 코드 및 권한에 대한 커넥터 설정
- 제안된 현대화 계획 검증

- 누락된 패키지 종속성을 NuGets로 업로드
- 변환된 코드 검토 및 수락

추가 정보

AWS 변환 웹 애플리케이션 또는 AWS 도구 키트를 사용하여 .NET 코드를 현대화할 수 있습니다 Visual Studio.

- [AWS 변환 웹 애플리케이션을 사용하여 .NET 코드 현대화](#)
- [IDE에서 .NET 현대화](#)
- [.NET 변환 모범 사례](#)

AWS 변환 웹 애플리케이션을 사용하여 .NET 코드 현대화

AWS .NET용 변환은 레거시 .NET 애플리케이션을 현대화하도록 설계된 새로운 생성형 AI 기반 에이전트입니다. AWS 변환 웹 애플리케이션 또는 Visual Studio AWS 도구 키트 확장을 사용하여 레거시 .NET 코드를 현대화할 수 있습니다.

AWS 변환 웹 애플리케이션을 사용하여 .NET 코드를 현대화하려면 다음 세부 단계를 따릅니다.

1. [AWS Transform .NET 작업 계획 생성](#)
2. [소스 코드 리포지토리 커넥터 생성](#)
3. [변환을 준비할 리포지토리 확인](#)
4. [변환을 준비하기 위한 패키지 종속성 해결](#)
5. [계획을 검토하여 변환 준비](#)
6. [.NET 코드 변환](#)

AWS Transform .NET 작업 계획 생성

워크스페이스를 생성한 후 작업 탭에서 작업 생성을 선택합니다. 그런 다음 채팅 창에서 자연어를 사용하여 AWS 변환의 프롬프트를 따릅니다. 다음은 .NET 현대화 작업을 생성하기 위한 일반적인 단계입니다.

1. AWS 변환은 생성하려는 변환 작업의 유형을 묻습니다. 채팅에 .NET 현대화를 입력합니다.
2. AWS 변환은 작업 이름을 제안하고 작업 이름을 변경할지 묻는 메시지를 표시합니다. 작업 이름을 변경하려면 자연어로 AWS 변환을 지시합니다. 예를 들어 작업 이름을 ExampleCorpDotNet1로 변

경합합니다. 그렇지 않으면 채팅에서 제안된 작업 이름을 수락할 수 있습니다. 작업 이름을 수락하면 AWS 변환은 채팅 창에서 작업을 생성 중임을 알립니다.

3. AWS 변환은 변환 작업을 생성합니다.

AWS Transform .NET 작업 계획의 구성 요소

.NET AWS 변환 작업 표시에는 왼쪽 끝에 있는 세로 아이콘 중에서 선택할 수 있는 작업, 대시보드, 승인, 아티팩트, 작업 로그의 5개 탭이 있습니다. 각 탭에는 왼쪽 창과 중앙 채팅 창이 있습니다. 추가 세부 정보를 표시하고 인적 입력을 요청하기 위해 때때로 오른쪽 공동 작업 창이 나타날 수 있습니다.

작업(작업 계획)

이 탭은 왼쪽 창에 작업 계획을 표시합니다. .NET 작업은 5단계로 구성됩니다.

1. 변환할 리소스 가져오기: 이 단계에서는 AWS CodeConnections를 사용하여 코드 리포지토리에 대한 커넥터를 생성합니다. 리포지토리 권한에 따라 코드 리포지토리의 관리자가 커넥터를 승인하고 리포지토리에 AWS 대한 변환 액세스 권한을 부여해야 할 수 있습니다.
2. 변환을 위한 리소스 검색: 이 단계에서 AWS 변환은 소스 제어에서 리포지토리를 검색하고 평가를 위해 일부 또는 전부를 선택합니다.
3. 변환을 위한 코드 평가: 선택한 리포지토리가 평가되며 평가 보고서를 볼 수 있습니다.
4. 변환 준비: 이 단계에서 AWS 는 리포지토리에서 종속성이 누락된 경우 변환에서 알립니다. 누락된 종속성을 업로드하거나 무시할 수 있습니다. 리포지토리의 관리자가 아닌 경우 관리자가 최종 변환 계획을 승인해야 할 수 있습니다.
5. 변환: 이 단계에서 AWS 변환은 리포지토리를 변환하고 변환이 완료될 때까지 변환 중에 진행 중인 상태를 제공합니다. 변환 보고서를 검토하여 변경된 내용과 이유를 이해할 수 있습니다.

각 단계의 상태를 확인할 수 있습니다.

- 시작되지 않음
- 사용자 입력 대기
- 진행 중
- 완료됨

대시보드

대시보드 탭은 변환에 대한 상위 수준 요약を提供합니다. 변환된 작업 수, 적용된 변환 및 변환 완료 예상 시간에 대한 지표를 표시합니다. 대시보드 아래에는 리포지토리 및 리포지토리의 상태인 진행 중, 실패 또는 성공 테이블이 있습니다.

승인

작업에 대한 승인 요청이 탭에 표시되고 완료됩니다.

아티팩트

작업 관련 아티팩트는 이 탭에서 업로드 또는 다운로드됩니다.

작업 로그

AWS 변환은 작업 로그 탭에서 해당 작업을 로깅합니다. Worklog는 AWS 변환이 수행하는 작업과 인적 입력 요청 및 해당 요청에 대한 응답에 대한 자세한 로그를 제공합니다.

소스 코드 리포지토리 커넥터 생성

이후 [AWS Transform .NET 작업 계획 생성](#) 작업 탭에서 AWS 변환 창의 왼쪽 창에 변환 작업의 단계가 나열됩니다. 첫 번째 단계는 변환할 리소스 가져오기입니다. 이 단계에서는 공동 작업자를 초대하고 소스 코드 리포지토리를 연결할 수 있습니다. AWS 변환 창의 오른쪽 창에서 세부 정보를 지정합니다.

각 변환 작업에는 소스 코드 리포지토리 커넥터가 하나만 있어야 합니다. AWS 변환 에이전트는 이 커넥터를 사용하여 [AWS CodeConnections](#)를 사용하여 GitHub, GitLab 또는 Bitbucket에서 .NET 코드베이스를 다운로드합니다. AWS 변환 작업과 동일한 리전에서 AWS CodeConnections를 설정해야 합니다. 또는 [소스 코드 리포지토리 대신 Amazon S3의 소스 코드에 연결할 수 있습니다.](#)

Note

기존 소스 코드 리포지토리 커넥터가 있는 경우 AWS 변환에서 알림을 보냅니다. 이 커넥터를 사용하려면 기존 커넥터 사용을 선택합니다. 기존 커넥터를 사용하지 않으려면 [기존 커넥터 삭제](#) 이전 단원을 참조하십시오 [새 커넥터 추가](#). 작업당 하나의 소스 리포지토리 커넥터만 가질 수 있습니다.

새 커넥터 추가

새 소스 코드 리포지토리 커넥터를 생성하려면:

1. AWS CodeConnections 커넥터에 사용할 AWS 계정 번호를 입력합니다.
2. 동일한 AWS 계정에 대해 up AWS CodeConnections를 설정하지 않은 경우 Set [up AWS CodeConnections](#)를 설정합니다.
3. [AWS 개발자 도구 콘솔](#)을 사용하여 [Bitbucket](#), [GitHub](#), [GitHub Enterprise Server](#), [GitLab](#) 또는 [AzureDevOps](#) 리포지토리에 대한 연결을 생성합니다.
4. 생성한 연결의 Amazon 리소스 이름(ARN)을 복사합니다.
5. AWS 변환으로 돌아가서 생성한 연결의 ARN을 붙여 넣습니다.
6. 커넥터의 이름을 입력합니다.

 Note

커넥터 이름의 일부로 개인 정보를 입력하지 마십시오.

7. 커넥터 생성 시작을 선택합니다.
8. AWS 변환은 현재 변환 작업과 동일한 리전에 입력한 AWS 계정에 대한 커넥터를 생성하도록 요청하고 AWS 관리 콘솔에서 AWS 관리자가 승인 요청을 승인할 준비가 되었음을 알립니다. 확인 링크 복사를 선택합니다.
9. AWS 관리자인 경우 AWS 계정에 로그인하고 확인 링크로 이동하여 연결 요청을 승인합니다. AWS 관리자가 아닌 경우 AWS 관리자에게 확인 링크를 제공합니다.
10. AWS 관리자가 커넥터 요청을 승인한 후 커넥터 완성을 선택하여 커넥터 생성 프로세스를 완료합니다. 다른 커넥터를 사용하려면 다시 시작을 선택하여 커넥터 생성 프로세스를 다시 시작합니다.

공동 작업 탭에는 다음과 같은 커넥터에 대한 세부 정보도 포함되어 있습니다.

- 상태 - 승인됨 또는 승인 보류 중
- AWS 계정 ID
- AWS 리전
- 연결 ARN

기존 커넥터 삭제

Note

기존 소스 코드 리포지토리 커넥터가 있는 경우 AWS 변환에서 알림을 보냅니다. 기존 커넥터 사용 또는 삭제를 선택하고 새 커넥터를 생성합니다.

기존 소스 코드 리포지토리 연결을 삭제하도록 선택하면 커넥터를 실제로 삭제하기 전에 AWS 변환에서 경고를 보냅니다.

- 다음과 같은 몇 가지 방법으로 기존 커넥터를 삭제할 수 있습니다.
 - AWS 변환에 메시지가 표시되면 삭제를 선택하고 새 커넥터를 생성할 수 있습니다.
 - 프롬프트에서 다시 시작을 선택할 수도 있습니다. 이 커넥터를 수정하려면 다시 시작해야 합니다.
- AWS 변환은 다시 시작하면 커넥터가 삭제된다는 경고를 표시합니다. 커넥터를 삭제하려면 다시 시작을 선택합니다.
- AWS 변환은 커넥터를 삭제하면 Bitbucket, GitHub 및 GitLab과 같은 타사 리포지토리에 대한 연결이 제거됨을 다시 경고합니다. 또한 커넥터를 삭제하면 이 커넥터를 사용하는 모든 AWS 변환 작업이 실패합니다. 삭제를 확인하려면 delete를 입력하고 Delete를 선택합니다.
- 새 소스 코드 리포지토리 커넥터를 추가하려면 섹션을 참조하세요 [새 커넥터 추가](#).

Amazon S3의 소스 코드에 연결

소스 코드 리포지토리를 연결하는 대신 AWS 변환을 Amazon S3의 소스 코드에 연결할 수 있습니다. <https://docs.aws.amazon.com/transform/latest/userguide/dotnet-creating-repo-connector.html>

S3 버킷 조직

원본 소스 코드와 변환된 코드는 아래와 같이 구성된 공통 S3 버킷에 저장됩니다. AWS 변환 작업과 동일한 리전에 S3 버킷을 설정해야 합니다. 루트 수준에서 소스 코드를 zip 파일로 버킷에 업로드합니다. zip 파일에는 각 리포지토리에 대한 최상위 폴더가 포함되어야 합니다.

변환 중에 AWS 변환은 변환 출력 폴더를 생성하고 변환 결과를 해당 폴더에 저장합니다. 변환은 변환된 코드가 포함된 transformed-code.zip이라는 zip 파일을 생성합니다. 여기에는 프로젝트 수준에서 파일 변경 사항을 강조 표시하는 코드 차이 보고서 파일 이름 diff.txt가 포함됩니다.

```
<customer-bucket>/
### source-code.zip
    ### repo 1
    ### repo 2
    ### .....
    ### repo n
### transform-output/
    ### transformed-code.zip
```

새 S3 커넥터 추가

새 S3 소스 코드 리포지토리 커넥터를 생성하려면:

1. AWS 콘솔에서 S3 버킷을 생성합니다.
2. 소스 코드를 S3 버킷에 zip 파일로 업로드합니다.
3. AWS 변환 웹 앱에서 .NET 변환 작업을 시작합니다. 소스 코드 리포지토리 연결 단계에서 S3 버킷에 소스 코드 연결을 선택하고 저장을 선택합니다.
4. 다음 페이지에서 S3 버킷 세부 정보를 입력하고 제출을 선택합니다.
 - a. 커넥터 이름
 - b. AWS 계정 ID
 - c. S3 버킷 Arn
 - d. S3 버킷 암호화 키(선택 사항)
5. 커넥터를 승인합니다.
 - a. 다음 페이지에서 확인 링크를 복사합니다.
 - b. 승인자가 링크를 찾아 AWS 커넥터 생성 요청 페이지로 이동하도록 합니다.
 - c. 를 선택하여 새 역할을 생성하거나 기존 역할을 사용합니다.
 - d. 요청을 검토한 후 저장 및 승인을 선택하여 요청을 승인합니다.
6. S3 zip 파일 위치를 지정합니다.
 - a. AWS 변환 웹 앱에서 상태가 승인됨으로 표시될 때까지 기다립니다.
 - b. 자산 위치 지정 페이지에서 코드 zip 파일의 S3 URL을 형식으로 입력하고 AWS 변환으로 전송을 s3://bucket-name/zip-file-name 선택합니다.
 - c. 작업은 검색 단계로 진행하여 변환을 계속합니다.

S3 커넥터 삭제

기존 S3 커넥터를 삭제하려면:

1. AWS 변환 웹 앱에서 오른쪽 상단의 커넥터 관리를 선택합니다.
2. 커넥터 관리 창에서 커넥터를 선택합니다.
3. 삭제를 선택합니다.

변환을 준비할 리포지토리 확인

이후 [소스 코드 리포지토리 커넥터 생성](#) 변환을 준비하는 첫 번째 단계로 리포지토리를 확인합니다. 다음을 수행할 수 있습니다.

- 계획 내용에 영향을 [기본 설정](#) 미치는 검토 및 변경.
- 검색된 리포지토리를 검토하고 변환을 위해 평가할 리포지토리를 선택합니다.
- [리포지토리 평가 보고서를](#) 검토하고 내용에 대해 AWS 변환과 채팅합니다.
- [AWS 변환에서 생성된 계획 사용](#).
- [변환 계획 사용자 지정](#) 웹 앱을 사용하거나 JSON 파일을 다운로드하여 수정하고 AWS 변환에 업로드합니다.

기본 설정

공동 작업 탭의 작업 세부 정보 섹션에서 다음을 설정할 수 있습니다.

작업 탭의 변환 준비 - 변환할 리포지토리 확인 단계에서 다음을 설정할 수 있습니다.

- 변환된 코드가 리포지토리에 기록되는 대상 브랜치 이름을 설정합니다.
- 대상 .NET 버전을 설정합니다.
 - .NET 8: 모든 프로젝트를 .NET 8로 변환
 - .NET 10: 모든 프로젝트를 .NET 10으로 변환
- 기본 작업 설정을 업데이트하거나 그대로 둘 수 있습니다. 다음이 포함됩니다.
 - 변환 계획에서 .NET Standard 프로젝트 제외이 설정은 기본적으로 선택됩니다. 선택하면 AWS 변환은 변환 계획에서 .NET Standard 프로젝트를 제외합니다. 이 설정을 선택 취소하면 .NET Standard 프로젝트가 변환되어 더 이상 .NET Framework와 호환되지 않습니다.
 - NuGet 소스를 확인하고 .NET 호환 패키지 버전을 가져옵니다. AWS 변환이 변환하려는 코드에 대해 .NET 호환 패키지 버전을 검색하고 가져올 수 있도록 허용합니다.

리포지토리 평가 보고서 검토

리포지토리 평가 보고서는 AWS 변환에서 감지된 각 리포지토리에 대한 정보를 표 형식으로 보여줍니다. 여기에는 다음이 포함됩니다.

- 리포지토리 소유자
- 평가 브랜치
- 솔루션 수
- 프로젝트 수
- 총 코드 행
- 감지된 .NET 버전
- 감지된 프로젝트 유형
- 프라이빗 Nuget 종속성 수
- 퍼블릭 Nuget 종속성 수
- 변환 복잡성

파일을 다운로드하려면:

1. 워크스페이스에서 협업 탭을 선택합니다.
2. 리포지토리 선택 창에서 다운로드를 선택하고 HTML로 다운로드 또는 JSON으로 다운로드를 선택합니다.

리포지토리 요약 보고서에 대한 채팅

리포지토리 요약이 매우 길 수 있습니다. 채팅을 사용하여 내용을 더 잘 이해할 수 있습니다. 작업 로그 탭에이 메시지가 표시되면 채팅에 보고서를 사용할 수 있습니다. 이제 평가 보고서를 채팅에서 쿼리에 사용할 수 있습니다. 채팅을 열려면 웹 콘솔의 오른쪽 하단에 있는 보라색 육각형 아이콘을 클릭합니다. 다음은 몇 가지 예제 프롬프트입니다.

- 검색되거나 평가된 모든 리포지토리를 나열합니다.
- 평가에서 발견된 .NET 6 프로젝트는 몇 개입니까?
- 복잡성이 가장 높은 프로젝트는 무엇입니까?

AWS 변환에서 생성된 계획 사용

마지막 수정, 루트 및 교차 종속 리포지토리를 포함하여 AWS 변환 성공 확률이 높은 리포지토리를 검색하여 생성된 변환 계획을 사용하도록 선택할 수 있습니다.

AWS 변환에는 변환 계획에 대한 다음과 같은 몇 가지 상위 수준 세부 정보가 나열됩니다.

- 검색된 총 리포지토리 수 변환이 소스 코드 리포지토리 커넥터를 사용하여 AWS 검색한 레거시 .NET 리포지토리 수입입니다. AWS 변환은 각 작업에서 최대 1,000개의 리포지토리를 스캔할 수 있습니다. 스캔하거나 변환할 리포지토리가 더 있는 경우 여러 변환 작업을 생성할 수 있습니다.
- 선택한 리포지토리 AWS 변환이 변환을 위해 선택한 레거시 .NET 리포지토리 수입입니다.
- 선택한 종속성 선택한 리포지토리에 필요한 종속성 수로, AWS 변환이 자동으로 감지되어 변환 계획에 추가되었습니다.

선택한 리포지토리 테이블에는 선택한 리포지토리가 나열됩니다. 이름으로 리포지토리를 검색하고, 리포지토리의 추가 페이지로 이동하고, 선택한 리포지토리와 해당 종속성을 나열하는 JSON 형식 파일을 다운로드할 수 있습니다. 이 보기에서 변경할 수 있습니다.

선택한 리포지토리 테이블에는 AWS 변환을 위해 선택한 리포지토리에 대한 다음 세부 정보가 나열됩니다.

- 리포지토리 이름
- 소스 브랜치
- 마지막 수정 날짜 및 시간
- 코드 행 할당량 한도에 근접하고 있는지 확인할 수 있습니다. 자세한 내용은 [AWS 변환 할당량](#) 단원을 참조하십시오.
- 종속 리포지토리 종속 리포지토리 수를 클릭하면 이러한 종속성에 대한 자세한 내용을 볼 수 있습니다.

AWS 변환 생성 변환 계획에 만족하는 경우 리포지토리 확인을 선택합니다.

AWS 변환 생성 변환 계획을 변경하려면 [변환 계획 사용자 지정](#).

변환 계획 사용자 지정

를 선택하지 않으면 다음 옵션 중 하나를 사용하여 변환할 리포지토리 목록을 사용자 [AWS 변환에서 생성된 계획 사용](#) 지정할 수 있습니다.

1. 선택한 리포지토리 테이블에서 리포지토리를 선택합니다.
 - a. 계획에 리포지토리를 추가하면 AWS 변환은 리포지토리의 종속성을 자동으로 선택하여 변환 계획에 추가합니다.
 - b. 테이블에서 리포지토리를 선택 취소할 수도 있습니다.
2. 리포지토리 및 브랜치의 AWS 변환 생성 JSON 목록을 다운로드합니다.
 - a. 다운로드를 선택한 다음 JSON으로 다운로드를 선택합니다.
 - b. JSON을 검토하고 수정합니다. 변환하지 않으려는 리포지토리 또는 리포지토리 내의 솔루션을 제거할 수 있습니다.
 - c. 사용자 지정 계획 업로드를 선택하여 수정된 JSON을 업로드합니다.
 - d. JSON이 성공적으로 업로드되면 선택한 리포지토리 테이블에 선택한 항목이 표시됩니다.
3. 종속 리포지토리 표시를 선택하여 검색된 AWS 변환이 선택한 리포지토리의 종속성인 리포지토리 목록을 표시할 수 있습니다.
4. 필요한 경우이 단계를 반복할 수 있습니다. 사용자 지정 계획에 만족하면 리포지토리 확인을 선택합니다.

변환을 준비하기 위한 패키지 종속성 해결

이후에 AWS 변환에서 누락된 패키지 종속성을 발견하면 [변환을 준비할 리포지토리 확인](#)하면이 단계를 완료해야 합니다. Windows PowerShell 스크립트를 실행하여 Visual Studio 개발 환경과 동일한 디바이스에서 누락된 패키지 종속성을 가져오거나 누락된 패키지를 수동으로 검색할 수 있습니다. 그런 다음 누락된 패키지를 업로드합니다.

누락된 패키지 종속성은 다음 두 가지 방법으로 업데이트할 수 있습니다.

- 아티팩트 커넥터를 사용하여 해결: 아티팩트 커넥터가 구성되지 않고 패키지가 누락된 경우 표시되는 전용 Connect 아티팩트 리포지토리 HITL 워크플로를 통해 아티팩트 리포지토리(ADO NuGet 커넥터)를 구성하여 해결합니다.
- 누락된 패키지 업데이트: AWS 변환은 누락된 패키지 종속성 테이블에 누락된 패키지를 나열합니다. 검색 상자에서 이름별로 누락된 패키지를 검색할 수 있습니다. 이 표에는 누락된 패키지에 대한 다음 세부 정보가 포함되어 있습니다.
 - 이름
 - 연결된 리포지토리
 - 프레임워크 버전 상태
 - 코어 버전 상태

누락된 패키지 종속성을 해결하려면 . [누락된 패키지 업로드](#)

누락된 패키지 업로드

1. 선택한 경우 Windows PowerShell 헬퍼 스크립트를 다운로드하여 Visual Studio 개발 환경 내에서 누락된 패키지 종속성을 검색할 수 있습니다. 또는 누락된 패키지를 수동으로 찾을 수 있습니다.

Windows PowerShell 스크립트를 사용하려면:

- a. Windows PowerShell 스크립트 다운로드를 선택합니다.
 - b. 누락된 패키지 종속성 파일이 포함된 리포지토리에 대한 활성 연결을 사용하여 로컬에서 스크립트를 실행합니다.
 - c. 이 스크립트를 사용하면 누락된 패키지 종속성을 로컬 환경에 다운로드할 수 있습니다.
2. 스크립트는 단일 아카이브의 모든 종속성을 포함하는 업로드할 단일 zip 파일을 생성합니다. 각 종속성에 대해 개별 .nupkg 또는 zip 파일을 업로드할 수도 있습니다.
 3. 패키지 파일 업로드를 선택합니다.
 4. 종속성 파일 업로드 모달에서 파일 선택을 선택하고 디바이스에서 누락된 압축 패키지 파일의 위치를 찾습니다.
 5. 업로드를 선택합니다.
 6. AWS 변환은 업로드한 파일을 검증합니다. 검증 중에는 업데이트할 수 없습니다. AWS 변환은 누락된 패키지 종속성 테이블 위에 검증 상태를 보고합니다.
 7. AWS 또한 변환은 누락된 패키지 종속성 테이블의 상태 열을 누락에서 해결됨으로 업데이트합니다. 패키지 검증에 실패하면 패키지 상태가 유효하지 않음이 됩니다. 잘못된 파일의 경우 다음을 수행합니다.
 - a. 패키지 종속성 누락 테이블에서 확인란을 사용하여 잘못된 패키지를 선택합니다.
 - b. 업로드된 파일 제거를 선택합니다.
 - c. 그러면 상태가 다시 누락으로 변경됩니다.
 8. 누락된 패키지를 업로드하고 패키지 종속성을 해결한 후 검토 계속을 선택합니다.

누락된 패키지 종속성을 해결하지 않고 검토 계속을 선택하면 AWS 변환은 누락된 패키지 없이 변환 작업을 시작할지 묻습니다. 누락된 패키지 종속성 무시를 선택하면 AWS 변환은 어셈블리 참조를 사용하여 코드를 변환합니다. 이 작업을 진행하면 관련 리소스에 영향을 미칠 수 있습니다.

폴더 구조 요구 사항

NuGet 업로드의 경우 AWS 변환에는 다음 중 하나가 필요합니다.

- 수동으로 업로드한 패키지에 대해 루트 수준에 배치할 .nuspec 파일 또는
- 제공된 PowerShell 스크립트를 사용하여 올바른 구조 생성

버전 일치 요구 사항

- 프레임워크 상태: AWS 파일.csproj(소스 코드)에 지정된 종속성 버전과 업로드된 종속성 버전을 일치시키려는 변환 시도입니다. 정확히 일치하면 성공 상태가 됩니다.
- 코어 상태: AWS 변환은 업로드된 .nuspec 파일의 종속성 섹션에서 코어 버전 사양을 예상합니다. 발견되면 코어 상태는 성공입니다.

예제 형식:

```
<dependencies>
  <group targetFramework="net8.0" />
</dependencies>
```

일반적인 버전은 다음과 같습니다.

- .NET 5.0(net5.0)
- .NET 6.0(net6.0)
- .NET 7.0(net7.0)
- .NET 8.0(net8.0)

계획을 검토하여 변환 준비

[변환을 준비할 리포지토리 확인](#), 및 이후 [변환을 준비하기 위한 패키지 종속성 해결](#) AWS 계정 관리자는 변환 계획을 검토하고 AWS 변환에서 승인해야 합니다.

AWS 변환에는 변환을 위해 선택한 작업의 리포지토리, 종속 리포지토리 및 종속 패키지 목록이 표시 됩니다.

변환 계획 검토

AWS 변환에는 변환을 위해 선택한 작업의 리포지토리, 종속 리포지토리 및 종속 패키지 목록이 표시 됩니다.

 Note

AWS 변환은 변환 계획당 최대 100개의 종속성과 리포지토리를 변환할 수 있습니다.

1. AWS 계정 관리자가 아닌 경우 작업 계획을 검토하고 수락하면 승인을 위해 전송을 선택합니다.
2. AWS 계정 관리자인 경우 계획을 검토하고 준비가 되면 계획을 승인하여 변환을 시작해야 합니다. 작업 계획을 검토한 후 다음 중 하나를 선택합니다.
 - a. 거부 AWS 계정 관리자가 아닌 사용자가 작업을 생성한 경우 작업 생성자에게 작업을 다시 시작하도록 알리는 것이 좋습니다.
 - b. 변환을 승인하고 시작합니다.

작업 검토에는 다음 세부 정보가 포함됩니다.

1. 작업 요약 여기에는 다음이 포함됩니다.
 - a. AWS 변환이 변환된 코드를 배치할 대상 브랜치입니다.
 - b. 대상 .NET 버전, .NET 8.0 또는 .NET 10.
 - c. 작업 설정:
 - i. .NET 표준 프로젝트 제외
 - d. 변환을 위해 선택한 리포지토리 수
 - e. 종속 리포지토리 수
 - f. 프라이빗 NuGet 패키지 수
 - g. 작업에 대한 총 코드 줄
2. 선택한 리포지토리 변환을 위해 선택한 리포지토리입니다. MVC, 웹, Windows 통신 기반(WCF), 콘솔, 클래스 라이브러리, UI 프레임워크 - Razor 페이지 또는 단위 테스트 패키지여야 합니다. 이 표에는 다음 정보가 포함되어 있습니다.
 - a. 이름
 - b. 소스 브랜치
 - c. 지원되는 프로젝트
 - d. 코드 행
 - e. 감지된 프로젝트
 - f. 건너뛴 프로젝트
 - g. 종속성이 감지됨

3. 종속 리포지토리가 추가된 변환을 위해 추가된 종속 리포지토리입니다. MVC, 웹, Windows 통신 기반(WCF), 콘솔, 클래스 라이브러리, UI 프레임워크 - Razor 페이지 또는 단위 테스트 패키지여야 합니다. 이 표에는 다음 정보가 포함되어 있습니다.
 - a. 이름
 - b. 에 필요
 - c. 소스 브랜치
 - d. 지원되는 프로젝트
 - e. 코드 행
 - f. 감지된 프로젝트
 - g. 건너뛴 프로젝트
4. 종속 패키지 변환을 위해 추가된 종속 패키지입니다. MVC, 웹, Windows 통신 기반(WCF), 콘솔, 클래스 라이브러리, UI 프레임워크 - Razor 페이지 또는 단위 테스트 패키지여야 합니다. 이 표에는 다음 정보가 포함되어 있습니다.
 - a. 이름
 - b. 연결된 리포지토리
 - c. 프레임워크 버전 상태
 - d. 코어 버전 상태

.NET 코드 변환

AWS 계정 관리자가를 완료하면 변환 작업의 대시보드 탭에서 변환 진행 상황을 볼 [계획을 검토하여 변환 준비](#)수 있습니다.

Note

리포지토리 및 종속성을 변환하는 것 외에도 AWS 변환은 완전히 변환된(빌드 오류 없음) 단위 테스트 프로젝트를 실행할 수 있습니다. AWS 변환은 변환 전에 단위 테스트 결과에 액세스할 수 없으며 변환 후 결과만 공유할 수 있습니다. 그런 다음 변환 전에 기존 데이터를 변환 후 결과와 비교하여 잠재적 격차를 파악할 수 있습니다.

오른쪽 상단 모서리에서 다음 값 중 하나를 가진 작업 상태를 볼 수 있습니다.

- 사용자 입력 대기
- 경과 시간

- 실행

다음 아이콘을 볼 수도 있습니다.

- 변환 중지 아이콘
- 새로 고침 아이콘
- 설정 아이콘

대시보드는 변환에 대한 상위 수준 요약を提供합니다. 변환된 작업 수 및 적용된 변환에 대한 지표와 변환을 완료하는 데 걸리는 예상 시간을 보여줍니다.

대시보드에는 다음이 포함됩니다.

1. 변환 작업 세부 정보 섹션은 다음을 포함하여 변환 작업의 기본 설정과 세부 정보를 나열합니다.
 - a. 대상 브랜치 대상 코드를 변환하기 위해 AWS 변환은 코드 리포지토리에서 변환된 코드에 대한 새 브랜치를 생성합니다.
 - b. 대상 .NET 버전, .NET 8.0 또는 .NET 10
 - c. AWS 변환 작업 ID입니다.
 - d. 작업 설정:
 - i. .NET 표준 프로젝트 제외
2. 변환 요약 섹션에는 다음이 포함되어 있습니다.
 - a. 변환을 위해 선택한 리포지토리 수
 - b. 변환할 프로젝트 수
 - c. 이러한 리포지토리 및 프로젝트의 총 코드 줄

변환이 시작되면 파이형 차트가 리포지토리 상태, 패키지 상태 및 단위 테스트 상태 섹션에 나타나 진행 상황을 실시간으로 표시합니다. 단위 테스트 상태는 변환 후 AWS 변환이 실행되어 변환된 코드를 테스트하는 리포지토리에 있는 단위 테스트의 상태를 보여줍니다. AWS 변환은 고객이 통과 및 실패한 단위 테스트 목록을 검토할 수 있도록 개별 테스트 이름과 함께 실행된 테스트 결과를 공유합니다.

Note

리포지토리 섹션에는 AWS 변환이 권장하거나 변환을 위해 선택한 리포지토리가 나열됩니다. JSON 다운로드를 선택하여 변환 계획의 리포지토리, 종속성 및 패키지 목록을 다운로드합니다.

변환 보고서 검토

변환 작업이 완료되면 [변환 보고서를](#) 다운로드할 수 있습니다.

- [변환 요약 보고서](#): 이 보고서는 HTML 또는 JSON 형식의 변환에 대한 개요를 제공합니다. 대시보드 탭에서 변환 요약 보고서를 다운로드합니다. 다운로드를 선택하고 HTML로 다운로드 또는 JSON으로 다운로드를 선택합니다.
- [변환 세부 정보 보고서](#): 이 보고서는 변환에 대한 심층 정보를 HTML 형식으로 제공합니다. 대시보드 탭에서 변환 세부 정보 보고서를 다운로드합니다. 리포지토리 목록에서 세부 보고서 다운로드 링크를 선택하여 세부 보고서를 다운로드합니다.

AWS 변환 보고서에 대해 변환과 채팅

리포지토리가 완전히 처리된 후 또는 변환 작업이 완료된 후 변환 보고서에 AWS 대해 변환과 채팅할 수 있습니다. Worklog 탭에는 채팅에 사용할 수 있는 각 리포지토리에 대해 이 메시지가 표시됩니다. 이제 쿼리를 위해 채팅에서 리포지토리 `repository_name` 변환 세부 정보를 사용할 수 있습니다. 변환 작업이 완료되면 AWS 변환 작업이 완료되었다는 메시지가 표시됩니다.

채팅을 열려면 웹 콘솔의 오른쪽 하단에 있는 보라색 육각형 아이콘을 클릭합니다.

다음은 몇 가지 예제 프롬프트입니다.

- 성공적으로 변환된 프로젝트는 무엇입니까?
- 부분적으로 이식된 프로젝트는 무엇입니까?
- `repo_name` 리포지토리에 적용된 변경 사항은 무엇입니까?
- `project_name` 프로젝트에서 업그레이드된 패키지는 무엇입니까?

IDE에서 .NET 현대화

AWS 변환에는 AWS Toolkit for에 대화형 에이전트 AI 어시스턴트가 포함되어 있습니다Visual Studio. 이를 통해 IDE에서 직접 대화형 step-by-step 안내 환경을 통해 애플리케이션을 현대화할 수 있습니다

다. .NET 솔루션 또는 프로젝트를 변환하기 위해 AWS 변환 에이전트는 코드베이스를 분석하고, 애플리케이션을 이식하는 데 필요한 업데이트를 결정하고, 변환이 시작되기 전에 평가 보고서와 변환 계획을 생성합니다.

Visual Studio IDE 환경은 IAM Identity Center의 인증만 지원합니다. 자세한 내용은 [IAM Identity Center에서 사용자 추가](#) 단원을 참조하십시오.

IDE 경험은 자율 및 대화형 모드를 제공합니다. 야간 또는 장기 실행 작업에 적합한 무인 변환에 자율 모드를 사용합니다. 대화형 모드를 사용하면 변환에 대한 높은 가시성, 사용자 지정 가능한 변환 계획, 각 프로젝트의 step-by-step 검토를 통해 채팅에서 에이전트와 협력할 수 있습니다. 반복하여 결과를 구체화하거나 만족할 때까지 방향을 변경할 수 있습니다.

변환 작업이 활성화되면 다음 세 가지 기간과 상호 작용할 수 있습니다.

- 채팅 창은 변환 에이전트와의 기본 상호 작용 지점입니다. 채팅을 사용하여 질문하고, 옵션에 대해 토론하고, 혁신을 주도하고, 반복합니다.
- AWS 작업 계획 변환 창에는 진행 단계가 표시되며 아티팩트를 다운로드 또는 업로드하거나 코드 변경 차이를 볼 수 있습니다.
- Worklog 창에는 자연어로 변환 활동 로그가 표시됩니다.

AWS 변환은 .NET 애플리케이션을 Linux로 이식하는 네 가지 주요 작업을 수행합니다.

- .NET 및 언어 버전 업그레이드 - 이전 .NET C# 코드를 현재 .NET 및 언어 버전으로 업그레이드합니다.
- .NET 프레임워크에서 크로스 플랫폼 .NET으로 마이그레이션 - Windows 종속 .NET 프레임워크에서 Linux와 호환되는 크로스 플랫폼 .NET으로 프로젝트 및 패키지를 마이그레이션합니다.
- Linux 호환성을 위한 코드 재작성 - 더 이상 사용되지 않거나 비효율적인 코드 구성 요소를 리팩터링하고 재작성합니다.
- Linux 호환성 준비 보고서 생성 - Linux에서 코드를 빌드하고 실행하기 위해 사용자 개입이 필요한 개방형 작업의 경우 AWS 변환은 변환 후 애플리케이션을 구성하는 데 필요한 작업에 대한 자세한 보고서를 제공합니다.

AWS 변환이 .NET 변환을 수행하는 방법에 대한 자세한 내용은 섹션을 참조하세요 [AWS Transform 이 .NET 애플리케이션을 현대화하는 방법](#).

Visual Studio IDE에서 AWS 변환을 사용하여 .NET 코드를 현대화하려면 다음을 참조하세요.

- [에서 AWS 변환을 사용하여 .NET 현대화 Visual Studio](#)

- [AWS Transform이 .NET 애플리케이션을 현대화하는 방법](#)
- [IDE에서 .NET 트랜스포메이션 문제 해결](#)

할당량

IDE의 AWS Transform .NET 변환 할당량은 섹션을 참조하세요 [AWS 변환 할당량](#).

에서 AWS 변환을 사용하여 .NET 현대화 Visual Studio

2026년 또는 2022년에 AWS 변환을 사용하여 Windows 기반 .NET 애플리케이션을 Linux 호환 교차 플랫폼 Visual Studio .NET 애플리케이션으로 이식하려면 다음 단계를 완료하세요.

1단계: 사전 조건

계속하기 전에 Visual Studio Marketplace에서 [AWS Amazon Q를 사용하여 Toolkit 확장](#)을 다운로드하고 설치했는지 확인합니다. .NET 현대화를 위한 AWS 변환 [기능](#) 및 [제한](#) 사항을 검토하여 코드를 변환할 수 있는지 확인합니다.

2단계: Visual Studio에서 인증

Toolkit for Visual Studio에서 AWS 계정에 연결하려면 AWS Toolkit 사용자 인터페이스 시작하기(연결 UI)를 엽니다.

1. Visual Studio 기본 메뉴에서 확장 > AWS 도구 키트 > 시작하기로 이동하여 시작하기: AWS 도구 키트 페이지를 엽니다.
2. 인증 AWS 변환을 선택합니다.
3. 기존 프로필을 선택하거나 새 프로필을 생성합니다. 새 프로파일을 생성할 때 프로파일의 이름과 관리자가 IAM Identity Center에 추가한 후 이메일로 전송한 AWS 변환 시작 URL을 입력합니다.
4. 연결을 선택합니다. 프롬프트에 따라 웹 브라우저를 통해 로그인하고 액세스 권한을 부여합니다. Visual Studio에는 IAM Identity Center와 연결됨이 표시됩니다.
5. 로그인하면 AWS 변환 대시보드로 이동합니다. 이 랜딩 페이지에서 다음을 수행할 수 있습니다.
 - AWS 변환 프로필 선택(리전)
 - 워크스페이스 선택 또는 생성
 - 변환 작업 상태 보기

3단계: 애플리케이션 변환

.NET 솔루션 또는 프로젝트를 트랜스포메이션하려면 다음 절차를 완료하세요.

변환 시작

1. 변환Visual Studio하려는에서 C# 또는 VB.NET 기반 솔루션 또는 프로젝트를 엽니다.
2. 솔루션 탐색기에서 변환하려는 솔루션 또는 프로젝트를 마우스 오른쪽 버튼으로 클릭하고 AWS 변환이 포함된 포트를 선택합니다.
3. AWS 변환이 있는 포트 대화 상자가 나타납니다.
 - a. 워크스페이스 선택 드롭다운에서 워크스페이스를 생성하거나 기존 워크스페이스를 선택합니다. Workspace를 사용하면 AWS 변환 웹 애플리케이션에서 활동을 볼 수 있으며, 여기에서 공동 작업자를 초대하여 변환 작업을 보고 채팅할 수 있습니다.
 - b. .NET 대상 선택 드롭다운 메뉴에서 업그레이드할 .NET 버전을 선택합니다.
 - c. 변환 모드에서 무인 변환의 경우 자율을 선택하고 대화형 변환의 경우 대화형을 선택합니다.
 - d. 시작을 선택하여 변환을 시작합니다.
4. 변환 작업이 시작되면 AWS 변환 작업 계획, 채팅 및 작업 로그 창이 나타납니다.

평가 및 변환 계획

1. AWS 변환이 코드를 분석하면 평가 보고서와 변환 계획이 채팅에 표시됩니다. 대화형 모드에서 채팅은 일시 중지되어 검토할 수 있습니다. 채팅에서 검토하지 않으려면 다음 대안을 사용할 수 있습니다.
 - 코드 편집기에서 평가 또는 계획을 보려면 변환 작업 계획 창에서 평가 표시 또는 AWS 변환 계획 표시를 선택합니다.
 - 평가 또는 계획을 다운로드하려면 작업 계획 창의 다운로드 아이콘을 사용합니다.
2. 선택적으로 변환 계획을 수정합니다. 다른 옵션을 탐색하는 등 채팅을 통해 계획에 대해 논의할 수 있습니다. 채팅에서 지침을 제공하거나 작업 계획 창의 다운로드 아이콘을 사용하여 수정된 변환 계획을 업로드하여 계획을 변경합니다. 단계를 자유롭게 추가, 제거 또는 수정할 수 있습니다. Chat은 수정된 계획을 사용하여 지침에 대한 이해를 확인합니다.
3. 선택적으로 조향 문서를 업로드합니다. 채팅 창에서 업로드 아이콘을 사용하여 애플리케이션 사양, 조직 기술 스택 기본 설정 및 규칙 또는 코딩 예제와 같은 조향 문서를 업로드합니다. 조향 문서를 업로드한 후 채팅 창에 설명하여 에이전트 컨텍스트를 제공합니다.
4. 계획에 만족하면 채팅에서 승인을 제공하면 변환이 시작됩니다.
5. 대화형 모드에서 검토를 위해 프로젝트를 변환한 후 체크포인트를 중지하도록 설정할 수 있습니다. 작업 계획 창의 코드 변환에 있는 단계에는 라운드 체크포인트 아이콘이 있습니다. 모든 프로

젝트에는 기본적으로 체크포인트가 활성화되어 있습니다. 확인란을 사용하여 체크포인트를 지우거나 설정합니다.

변환 및 체크포인트 검토

1. AWS 변환은 코드 변환을 시작합니다. 변환 작업 계획 창에서 AWS 변환 단계의 진행 상황을 모니터링할 수 있습니다. 작업 계획 창에는 남은 예상 최대 시간과 작업 ID가 표시됩니다.
2. 프로젝트가 변환되면 요약이 채팅에 표시되고 코드 변경 사항이 적용됩니다.
3. 대화형 모드에서 체크포인트에 도달하면 에이전트가 일시 중지되므로 결과를 검토할 수 있습니다. 작업 계획 창에는 코드 차이를 검토할 수 있는 일시 중지된 단계에 대한 결과 보기 버튼이 표시됩니다. 변경 사항을 검토한 후 채팅에서 추가 변경 사항을 요청하거나에서 직접 코드를 변경할 수 있습니다Visual Studio.
4. 체크포인트에서 원하는 만큼 반복할 수 있습니다. 만족하면 채팅에 계속 진행하도록 지시하면 다음 프로젝트로 이동합니다.

변환 종료

1. 프로젝트를 변환한 후 .NET 에이전트에서 로컬 빌드를 트리거Visual Studio하여 코드가 로컬 시스템에 성공적으로 빌드되는지 확인합니다. 오류가 있는 경우 오류를 해결하는 데 사용됩니다.
2. 변환이 완료되면 변환 작업이 수행할 AWS 수 없거나 Linux 호환성에 필요한 변경 사항과 같은 추가 단계가 필요할 수 있습니다. AI 코드 컴패니언에 대한 프롬프트로 사용할 수 있는 다음 단계 마크다운 파일(NextSteps.md)을 다운로드할 수 있습니다. 작업 계획 창의 다운로드 아이콘 버튼을 사용하여 NextSteps.md를 다운로드합니다.
3. 채팅에서 계속 상호 작용하여 질문을 하거나 추가 변경을 요청할 수 있습니다.
4. 변환 작업을 종료할 준비가 되면 채팅에 알립니다.

AWS Transform이 .NET 애플리케이션을 현대화하는 방법

AWS 변환을 사용한 .NET 변환의 작동 방식에 대한 자세한 내용은 다음 섹션을 검토하세요.

애플리케이션 분석 및 트랜스포메이션 계획 생성

변환이 시작되기 전에 AWS 변환은 로컬에서 코드를 빌드하여 변환을 위해 코드를 빌드하고 올바르게 구성되었는지 확인합니다. 코드가 빌드되지 않으면 AWS 변환은 변환을 계속할지 여부를 묻는 메시지를 표시합니다. AWS 그런 다음 변환은 안전하고 암호화된 빌드 환경에 코드를 업로드하고 AWS, 코드 베이스를 분석하고, 애플리케이션을 이식하는 데 필요한 업데이트를 결정합니다.

이 분석 중에 AWS 변환은 .NET 솔루션 또는 프로젝트를 코드 그룹으로 나눕니다. 코드 그룹은 DLL(동적 링크 라이브러리) 또는 실행 파일과 같은 빌드 가능한 코드 단위를 함께 생성하는 프로젝트 및 모든 종속 항목입니다. 변환할 모든 프로젝트 종속성을 선택하지 않은 경우에도 AWS 변환은 선택한 프로젝트를 빌드하는 데 필요한 종속성을 결정하고 변환하여 변환된 애플리케이션을 빌드하고 사용할 준비가 되도록 합니다.

코드를 분석한 후 AWS 변환은 변환할 코드 그룹 및 종속성 목록을 포함하여 제안된 변경 사항을 요약하는 변환 계획을 생성합니다.

애플리케이션 트랜스포메이션

변환을 시작하기 위해 AWS 변환은 보안 빌드 환경에서 코드를 다시 빌드하여 원격으로 빌드할 수 있는지 확인합니다. 그런 다음 AWS 변환은 애플리케이션 이식을 시작합니다. 이 작업은 가장 낮은 수준의 종속성부터 시작하여 높은 종속성으로 진행합니다. AWS 변환이 종속성을 이식하는 데 문제가 발생하면 변환을 중지하고 오류의 원인에 대한 정보를 제공합니다.

트랜스포메이션에는 애플리케이션에 대한 다음 업데이트가 포함됩니다.

- 오래된 코드 C# 버전을 Linux 호환 C# 버전으로 교체
- 다음을 포함하여 .NET 프레임워크를 크로스 플랫폼 .NET으로 업그레이드
 - 패키지, 라이브러리 및 API 식별 및 반복 교체
 - NuGet 패키지 및 API 업그레이드 및 교체
 - 크로스 플랫폼 런타임으로 전환
 - 미들웨어 설정 및 런타임 구성 업데이트
 - 프라이빗 또는 서드 파티 패키지 교체
 - IIS 및 WCF 구성 요소 처리
 - 빌드 오류 디버깅
- 기존 코드를 포팅하기 위해 더 이상 사용되지 않고 비효율적인 코드 리팩터링 및 재작성을 포함하여 Linux 호환성을 위한 코드 재작성

변환 보고서 검토 및 변경 사항 수락

변환이 완료되면 AWS 변환은 변경된 파일 수, 업데이트된 패키지, 변경된 APIs 등 애플리케이션에 대해 제안된 업데이트에 대한 정보가 포함된 변환 보고서를 제공합니다. 영향을 받는 파일 또는 파일 부분과 빌드 시도 중에 발생한 오류를 포함하여 실패한 트랜스포메이션에 플래그를 지정합니다. 빌드 로그가 포함된 빌드 요약을 보고 변경 사항에 대해 자세히 알아볼 수도 있습니다.

또한 변환 보고서는 애플리케이션 Linux를 호환하기 위해 추가 사용자 입력이 필요한지 여부를 나타내는 Linux 이식 상태를 제공합니다. 코드 그룹의 항목 중 하나라도 사용자의 입력이 필요한 경우 빌드 시 AWS 변환이 해결할 수 없는 Windows별 고려 사항이 포함된 Linux 준비 보고서를 다운로드합니다. 코드 그룹 또는 파일에 대한 입력이 필요하다면 보고서를 검토하여 여전히 수행해야 하는 변경 유형에 대한 세부 정보를 확인하세요. 해당하는 경우 코드를 업데이트하는 방법에 대한 권장 사항도 함께 확인하세요. Linux에서 애플리케이션을 실행하려면 먼저 이러한 변경을 수동으로 수행해야 합니다.

제안된 변경 사항 diff 보기에서 AWS 변환한 후 파일에 대한 현재 위치 업데이트로 수락할 수 있습니다. 파일을 업데이트하고 Linux 준비 보고서의 항목을 해결하면 애플리케이션이 크로스 플랫폼 .NET에서 실행될 준비가 된 것입니다.

AWS 변환 또는 AI 코드 컴패니언을 사용하여 계속 변환하라는 메시지가 표시된 다음 단계 마크다운 파일을 다운로드할 수 있습니다. 파일을 다운로드하려면 보고서 오른쪽 상단의 다음 단계 다운로드 버튼을 선택합니다.

IDE에서 .NET 트랜스포메이션 문제 해결

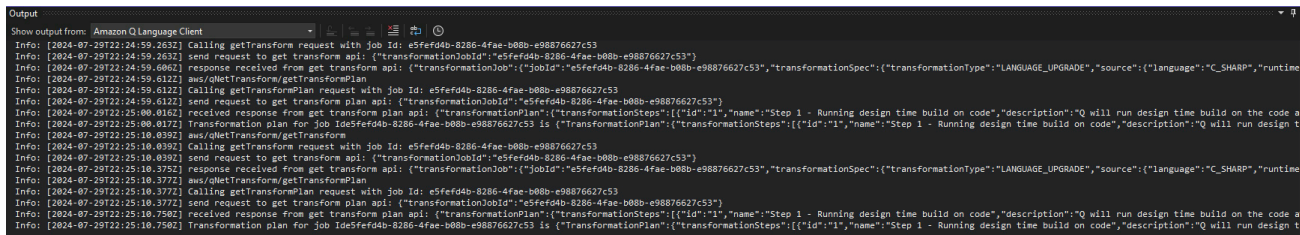
다음 섹션을 사용하여 AWS 변환을 사용하는 IDE에서 .NET 변환과 관련된 일반적인 문제를 해결합니다.

작업이 진행 중인지 알 수 있는 방법은 무엇인가요?

Worklog 창에 정기적인 활동이 표시되어야 합니다. AWS 변환이 AWS 작업 계획 변환 창의 단계에 오랜 시간을 소비하는 것처럼 보이는 경우 출력 로그에서 작업이 여전히 활성 상태인지 확인할 수 있습니다. 진단 메시지가 생성되는 경우 작업은 여전히 활성 상태입니다.

출력을 확인하려면에서 출력 탭을 선택합니다Visual Studio. 출력 표시 출처: 메뉴에서 Amazon Q Language Client를 선택합니다.

다음 스크린샷은 AWS 변환 중에 변환이 생성하는 출력의 예를 보여줍니다.



```

Output
Show output from: Amazon Q Language Client
Info: [2024-07-29T22:24:59.263Z] Calling getTransform request with job Id: e5fef04b-8286-4fae-b08b-e98876627c53
Info: [2024-07-29T22:24:59.263Z] send request to get transform api: ("transformationJobId":"e5fef04b-8286-4fae-b08b-e98876627c53")
Info: [2024-07-29T22:24:59.468Z] response received from get transform api: ("transformationJobId":"e5fef04b-8286-4fae-b08b-e98876627c53","transformationSpec":{"transformationType":"LANGUAGE_UPGRADE","source":{"language":"C_SHARP","runtime":
Info: [2024-07-29T22:24:59.612Z] aws/GetTransform/getTransformPlan
Info: [2024-07-29T22:24:59.612Z] Calling getTransformPlan request with job Id: e5fef04b-8286-4fae-b08b-e98876627c53
Info: [2024-07-29T22:24:59.612Z] send request to get transform plan api: ("transformationJobId":"e5fef04b-8286-4fae-b08b-e98876627c53")
Info: [2024-07-29T22:25:10.015Z] received response from get transform plan api: ("transformationPlan":{"transformationSteps":[{"id":"1","name":"Step 1 - Running design time build on code","description":"Q will run design time build on the code a
Info: [2024-07-29T22:25:10.039Z] Transformation plan for job Id e5fef04b-8286-4fae-b08b-e98876627c53 is ("transformationPlan":{"transformationSteps":[{"id":"1","name":"Step 1 - Running design time build on code","description":"Q will run design t
Info: [2024-07-29T22:25:10.039Z] aws/GetTransform/getTransform
Info: [2024-07-29T22:25:10.039Z] Calling getTransform request with job Id: e5fef04b-8286-4fae-b08b-e98876627c53
Info: [2024-07-29T22:25:10.039Z] send request to get transform api: ("transformationJobId":"e5fef04b-8286-4fae-b08b-e98876627c53")
Info: [2024-07-29T22:25:10.375Z] response received from get transform api: ("transformationJobId":"e5fef04b-8286-4fae-b08b-e98876627c53","transformationSpec":{"transformationType":"LANGUAGE_UPGRADE","source":{"language":"C_SHARP","runtime":
Info: [2024-07-29T22:25:10.377Z] aws/GetTransform/getTransformPlan
Info: [2024-07-29T22:25:10.377Z] Calling getTransformPlan request with job Id: e5fef04b-8286-4fae-b08b-e98876627c53
Info: [2024-07-29T22:25:10.377Z] send request to get transform plan api: ("transformationJobId":"e5fef04b-8286-4fae-b08b-e98876627c53")
Info: [2024-07-29T22:25:10.750Z] received response from get transform plan api: ("transformationPlan":{"transformationSteps":[{"id":"1","name":"Step 1 - Running design time build on code","description":"Q will run design t
Info: [2024-07-29T22:25:10.750Z] Transformation plan for job Id e5fef04b-8286-4fae-b08b-e98876627c53 is ("transformationPlan":{"transformationSteps":[{"id":"1","name":"Step 1 - Running design time build on code","description":"Q will run design t
  
```

일부 프로젝트가 트랜스포메이션을 위해 선택되지 않은 이유는 무엇인가요?

AWS 변환은 지원되는 .NET 프로젝트 유형만 변환할 수 있습니다. 지원되는 프로젝트 유형 및 .NET 프로젝트를 트랜스포메이션하기 위한 기타 사전 조건 목록은 [1단계: 사전 조건](#) 섹션을 참조하세요.

프로젝트 또는 솔루션이 변환되지 않는 경우 지원을 받으려면 어떻게 해야 하나요?

문제를 직접 해결할 수 없는 경우 또는 AWS 계정 팀에 문의하여 지원 지원 사례를 제출할 수 있습니다.

지원을 받으려면가 실패한 작업을 조사할 AWS 수 있도록 변환 작업 ID를 제공합니다. 변환 작업 ID를 찾으려면에서 출력 탭을 선택합니다Visual Studio. 출력 표시 출처: 메뉴에서 Amazon Q Language Client를 선택합니다.

방화벽이 트랜스포메이션 작업을 방해하지 않도록 하려면 어떻게 해야 하나요?

조직에서 방화벽을 사용하는 경우의 변환을 방해할 수 있습니다Visual Studio. Node.js에서 보안 검사를 일시적으로 비활성화하여 트랜스포메이션 실행을 방해하는 문제를 해결하거나 테스트할 수 있습니다.

환경 변수 `NODE_TLS_REJECT_UNAUTHORIZED`는 중요한 보안 검사를 제어합니다.

`NODE_TLS_REJECT_UNAUTHORIZED`를 "0"으로 설정하면 Node.js의 무단 TLS/SSL 인증서 거부가 비활성화됩니다. 이는 다음을 의미합니다.

- 자체 서명 인증서가 수락됩니다.
- 만료된 인증서가 허용됩니다.
- 호스트 이름이 일치하지 않는 인증서가 허용됩니다.
- 다른 인증서 검증 오류가 무시됩니다.

프록시가 자체 인증서를 사용하는 경우 `NODE_TLS_REJECT_UNAUTHORIZED`를 비활성화하는 대신 다음 환경 변수를 설정할 수 있습니다.

```
NODE_OPTIONS = -use-openssl-ca
NODE_EXTRA_CA_CERTS = Path/To/Corporate/Certs
```

그렇지 않으면 프록시에서 `NODE_TLS_REJECT_UNAUTHORIZED`를 비활성화하는 데 사용하는 CA 인증서를 지정해야 합니다.

Windows에서 `NODE_TLS_REJECT_UNAUTHORIZED`를 분할하려면

1. 시작 메뉴를 열고 환경 변수를 검색합니다.
2. 시스템 환경 변수 편집을 선택합니다.
3. 시스템 속성 창에서 환경 변수를 선택합니다.

4. 시스템 변수에서 새로 만들기를 선택합니다.
5. 변수 이름을 NODE_TLS_REJECT_UNAUTHORIZED로 설정하고 변수 값을 0으로 설정합니다.
6. 확인을 선택하여 변경 사항을 저장합니다.
7. Visual Studio를 다시 시작합니다.

UI 계층 코드 이식

AWS 변환은 ASP.NET 웹 사이트의 UI 계층을 Linux에서 실행할 수 있는 ASP.NET Core와 호환되는 UI 프레임워크로 이식할 수 있습니다. 다음과 같은 변환을 사용할 수 있습니다.

- MVC Razor UI 이식
- Web Forms에서 Blazor로 UI 이식

MVC Razor UI 이식

Razor Views UI가 있는 ASP.NET MVC 프로젝트는 동일한 UI 프레임워크에 남아 있는 ASP.NET Core의 MVC Razor Views로 포팅할 수 있습니다. Razor 뷰는 ASP.NET 및 ASP.NET Core 간에 유사하지만 포팅 코드 변경이 필요한 차이점이 있습니다.

- ASP.NET MVC Razor Views는 System.Web.Mvc 네임스페이스를 사용하며 .NET Framework와 밀접하게 연결되어 있습니다.
- ASP.NET Core Razor Views는 Microsoft.AspNetCore.Mvc,를 기반으로 하는 모듈식이며 종속성 주입이 개선되었습니다.
- ASP.NET Core에는 태그 헬퍼 및 구성 요소 보기를 비롯한 새로운 기능이 있습니다.

AWS 변환은 Razor Views에서 일반적인 호환되지 않는 구성 요소 및 구문을 감지하고 포트를 생성합니다.

Web Forms에서 Blazor로 UI 이식

ASP.NET Web Forms UI에는 ASP.NET Core에 해당하는 것이 없습니다. AWS 변환은 Web Forms UI 계층 코드를 ASP.NET Core의 Blazor Server로 포팅할 수 있습니다. 대상 UI 프레임워크에 대해 UI 계층 코드가 다시 작성됩니다.

Web Forms to Blazor UI 이식을 활성화하거나 비활성화하려면 UI ASP.NET Web Forms to Blazor 작업 설정을 확인하거나 선택 취소합니다.

변환 세부 정보

Web Forms 프로젝트는 서버 측 호스팅이 있는 Blazor 프로젝트로 변환됩니다. 변환 중에 다음과 같은 프로젝트 및 파일이 변경됩니다.

파일 변환 매핑

From	목적	설명
*.aspx, *.ascx	*.razor	.aspx 페이지 및 .ascx 사용자 지정 컨트롤은 .razor 파일이 됩니다.
Web.config	appsettings.json	Web.config 설정이 appsettings.json 설정이 됩니다.
Global.asax	Program.cs	Global.asax 코드가 Program.cs 코드가 됩니다.
*.master	*layout.razor	마스터 파일은 layout.razor 파일이 됩니다.

변환 후 프로젝트 구조

변환 후 변환된 파일은 다음 프로젝트 위치에 있습니다.

- 구성 요소 폴더: 모든™ 구성 요소(*.razor)는 프로젝트의 .csproj 파일과 동일한 수준에서 생성된 구성 요소 폴더에 배치됩니다.
- 페이지 매핑: Web Forms 페이지(*.aspx)는 구성 요소/페이지 폴더 구조로 변환됩니다.
- 제어 매핑: Web Forms 제어(*.ascx)는 구성 요소 폴더 바로 아래에 배치됩니다.

제한 사항 및 지원되지 않는 기능

현재 다음 기능은 지원되지 않습니다. 워크로드에서 이러한 기능을 사용하는 경우 해당 코드를 수동으로 이식하거나 변환 후 AI 코드 컴패니언과 함께 이식해야 합니다.

- .svc 파일(서비스 파일)
- .ashx 파일(일반 핸들러 파일)
- 서비스 참조 및 웹 참조(reference.map, reference.cs, .wsdl 파일)
- 동일한 프로젝트의 .aspx(Web Forms) 파일과 .cshtml(Razor) 파일 혼합
- .NET용 AWS 변환에서 아직 지원하지 않는 프로젝트 유형에 대한 종속성

- 타사 공급업체 UI 라이브러리/컨트롤
- 웹 사이트 프로젝트

웹 애플리케이션 프로젝트(.csproj 파일 포함)만 지원됩니다. 웹 사이트 프로젝트를 웹 애플리케이션 프로젝트로 변환하려면 Microsoft 지침 [웹 사이트 프로젝트를 웹 애플리케이션 프로젝트로 변환을 참조하세요](#).

변환 보고서

.NET 변환 작업이 완료되면 이러한 변환 보고서를 사용할 수 있습니다.

- [변환 요약 보고서](#)
- [변환 세부 정보 보고서](#)

변환 요약 보고서

변환 작업이 완료되면 웹 콘솔에서 변환 요약 보고서를 사용할 수 있습니다. 대시보드 탭에서 변환 요약 보고서를 다운로드합니다. 변환 요약 보고서 다운로드를 선택하고 HTML로 다운로드 또는 JSON으로 다운로드를 선택합니다.

변환 요약 보고서는 변환에 대한 개요와 다음을 포함하여 변환된 각 리포지토리와 관련된 정보를 제공합니다.

- 작업 세부 정보
 - 변환 작업 개요
 - 변환 결과 개요
 - 파일 개요
- 리포지토리 목록 및 각 리포지토리의 경우:
 - 리포지토리 이름 개요
 - 솔루션 변환 요약
 - 상태, 유형, .NET 버전, 총 코드 행, 변환된 코드 행, 변경된 파일을 포함한 프로젝트 세부 정보

변환 세부 정보 보고서

변환 작업이 완료되면 웹 콘솔과 IDE 사용자 모두 변환 세부 정보 보고서를 사용할 수 있습니다.

- 웹 콘솔 사용자: 변환된 각 리포지토리에 대해 세부 보고서를 사용할 수 있습니다. 대시보드 탭에서 리포지토리 목록의 세부 보고서 다운로드 링크를 사용하여 세부 보고서를 다운로드합니다.
- IDE 사용자: 다운로드 아이콘을 사용하여 변환 AWS 작업 계획 창에서 변환 보고서를 다운로드합니다.

변환 세부 정보 보고서는 대화형 HTML 보고서입니다. 여기에는 파일 변경 이유 및 실행 가능한 오류 세부 정보를 포함하여 변환에 대한 심층적인 정보가 포함되어 있습니다. 정보는 다음 계층 구조로 정렬됩니다.

- 작업 정보
- 각 솔루션의 경우:
 - 솔루션 변환 요약
 - 변환 개요
 - Projects
 - 각 프로젝트에 대해:
 - 프로젝트 요약
 - 빌드 오류 요약
 - NuGet 패키지 변경 사항
 - 파일 변경 사항
 - 빌드 오류
 - 단위 테스트 결과
 - Linux 준비 보고서

예제가 포함된 변환 세부 정보 보고서 섹션에 대한 연습은 블로그 게시물 [Announcing AWS Transform for .NET detailed transformation reports](#)를 참조하세요.

.NET 변환 모범 사례

AWS 변환을 통해 더 나은 .NET 현대화 결과를 얻으려면이 지침을 따르세요. 이러한 모범 사례는 현재 IDE에 사용할 수 있는 .NET 대화형 AI Visual Studio 어시스턴트에 적용됩니다.

주제

- [변환하기 전에](#)
- [평가 및 계획](#)

- [대화형 또는 자율적으로 변환](#)
- [검증 및 마무리](#)

변환하기 전에

.NET 변환 작업을 시작하기 전에 다음 권장 사항을 검토합니다.

.NET 대화형 AI 어시스턴트 사용

최상의 변환 결과를 얻으려면 새 .NET 에이전트를 사용합니다. 대화형 AI 어시스턴트는 [AWS Toolkit for Visual Studio](#)를 Visual Studio 통해 사용할 수 있습니다. 변환 및 AWS 변환 AWS MCP 에이전트의 Kiro 기능을 통해 [Kiro](#) 또는 기타 IDEs에도 사용할 수 있습니다. 새 .NET 에이전트는 아직 웹 콘솔에서 사용할 수 없습니다.

목표가 .NET에서 .NET으로 변환이 아닌 경우 다른 도구를 사용합니다.

AWS .NET용 변환은 .NET Framework에서 .NET 코드 현대화로, .NET에서 이후 버전으로 업그레이드하는 데 적합합니다. 비를 포함하는 변환에는 적합하지 않습니다.Java 또는 비와 같은 NET 언어.React와 같은 NET 프레임워크. 또한 애플리케이션 아키텍처 리팩터링을 제공하지 않습니다. 이러한 종류의 현대화Kiro에는 [AWS 사용자 지정](#) 변환 또는를 사용합니다.

안정적인 버전의 Visual Studio, 가급적이면 VS2026 사용

미리 보기 소프트웨어로 인한 복잡성을 방지하려면 미리 보기 또는 내부자 에디션 Visual Studio 대신의 GA 에디션을 사용합니다. 도구 AWS 키트는 Visual Studio 2026 또는 2022에서 사용할 수 있습니다. VS2026은 메모리 소비를 줄이면서 성능이 더 우수하기 때문에 권장됩니다.

용 최신 AWS 도구 키트 사용 Visual Studio

버그 수정 및 기능 업데이트를 Visual Studio 위해 최신 버전의 AWS Toolkit for를 유지하십시오. 확장 > 확장 관리 > 설치에서 도구 키트 버전을 확인하고 업그레이드할 수 있습니다.

중간 이상의 복잡성 프로젝트를 위해 Visual Studio IDE에서 작업

IDE 환경은 프로젝트를 변환할 때 .NET 에이전트와 함께 작업할 수 있는 가장 심층적인 변환 보기를 제공합니다. 중간, 높음 또는 중요 복잡성 프로젝트의 경우 웹 콘솔 대신 IDE를 사용합니다.

검증 계획 수립

변환한 후 애플리케이션의 정확성을 검증하는 방법을 결정합니다. 변환 후 실행 시 올바르게 동작하고 작동하는지, 보안 제어, 비즈니스 로직 및 데이터 스토리지가 손상되지 않았는지 확인해야 합니다. 검

중은 수동으로 수행되거나 테스트 자동화를 사용하여 수행됩니까? 솔루션에 단위 테스트가 포함된 경우 AWS 변환은 이를 이식하여 실행하고 변환 보고서에 결과가 표시됩니다.

NuGet 프라이빗 패키지 종속성 제공

솔루션이 프라이빗 패키지에 의존하는 경우 IDE 및 AWS 변환에서 찾을 수 있도록 로컬 시스템에서 사용할 수 있는지 확인합니다.

패키지 교체를 지정하거나 에이전트 추천을 요청합니다.

최신 .NET 버전이 없는 패키지의 경우 변환 계획을 사용자 지정하여 원하는 패키지 대체를 지정하거나 에이전트에게 권장 사항을 요청할 수 있습니다.

더 이상 변경하지 않을 때까지 작업을 종료하지 마십시오.

변환이 완료된 후 추가 변경을 원하는 경우 작업을 즉시 종료하지 마십시오. 변환은 그렇게 말할 때까지 완료되지 않습니다. 작업을 완료할 때까지 변경 사항을 요청할 수 있습니다.

변환 후 AI 코드 컴패니언에게 전달하여 앱을 마무리합니다.

AWS 변환을와 같은 AI 코드 컴패니언과 결합해야 합니다Kiro. 일반적인 패턴은 먼저 AWS Transform for .NET으로 변환한 다음 AI 코드 컴패니언에 전달하여 애플리케이션을 완료하는 것입니다. 이 마무리 작업에는 런타임 오류, 동작 문제 및 UX 스타일 식별 및 수정이 포함될 수 있습니다.

현대화 여정에서 AWS 변환은 목표를 향해 먼 길을 가고 AI 코드 컴패니언은 최종 목적지로 가는 현지 여행이라고 생각하세요.

AWS 변환에서 AI 코드 컴패니언으로의 핸드오프를 지원하기 위해 AWS 변환은 변환이 끝날 때 HTML 변환 보고서와 다음 단계 마크다운 문서를 제공합니다.

평가 및 계획

변환 작업을 시작한 후 AWS 변환은 코드를 분석하고 평가 보고서와 변환 계획을 생성합니다. 다음 모범 사례를 사용하여이 단계를 최대한 활용하세요.

평가를 검토하고 질문을 통해 기대치를 설정합니다.

평가 결과를 주의 깊게 검토하여 변환하기 어려운 프로젝트와 그 이유를 이해합니다. 에이전트는 복잡성 수준(낮음, 중간, 높음, 중요)으로 프로젝트를 제시하고 해당 등급을 받은 이유를 설명합니다.

어려운 영역에 대해 자세히 알아보려면 질문하세요. 예제:

- 에이전트에게 프로젝트 변환 또는 사용 사례에 대한 신뢰도 수준을 물어보세요.
- 에이전트에게 AI 코드 컴패니언과 함께 어떤 변환 후 작업이 필요할지 물어보세요.

계획을 검토하고 에이전트와 옵션에 대해 논의합니다.

에이전트는 검토를 위한 변환 계획을 제공합니다. 이 계획에 대해 설명하고 수정할 수 있습니다. 먼저 옵션을 이해합니다. 에이전트에게 계획의 어떤 부분에 대한 대안이 있는지 물어보세요.

예를 들어 변환 계획은 WCF 서비스를 ASP.NET 웹 APIs. 그러나 조직은 WCF를 계속 사용하는 것을 선호합니다. 에이전트에게 옵션을 요청하고 대안은 옵션을 로 변환하는 것임을 알아봅니다CoreWCF.

조직의 계획을 조정하기 위한 조향 문서 업로드

원래 변환 계획은 조직의 요구 사항 및 기본 설정을 이해하지 않고 생성됩니다. 에이전트에게 조직 규칙, 애플리케이션 사양, 기본 기술 스택 및 기본 코딩 패턴 예제를 알릴 수 있습니다.

조향 문서를 업로드한 후 이를 설명하여 에이전트 컨텍스트를 제공합니다. 조향 문서의 추가 정보를 통해 에이전트는 조직이 선호하는 작업 방식에 맞는 계획을 준비할 수 있습니다.

자유롭게 계획 사용자 지정

.NET 에이전트는 유연하며 .NET에서 .NET으로의 변환 도메인 내에서 변환 계획을 자유롭게 사용자 지정할 수 있습니다. 채팅에서 계획 변경을 요청하거나 원하는 경우 마크다운 파일로 작업할 수 있습니다. 만족할 때까지 계획을 검토하고 구체화합니다.

여러 이해관계자가 계획을 검토해야 하는 경우 계획을 마크다운 파일로 다운로드하여 공유하고 나중에 사용자 지정 계획을 업로드할 수 있습니다.

예를 들어 변환 계획을 검토하고 클래스 라이브러리 프로젝트를 .NET 10 대신 .NET Standard로 변환하기로 결정합니다. 채팅에서 "모든 클래스 라이브러리를 .NET Standard 2.0으로 변환할 계획을 수정합니다"라고 말하면 에이전트가 수정된 계획을 제시합니다.

대화형 또는 자율적으로 변환

Visual Studio IDE 경험은 변환 중 상호 작용 정도를 제어하는 자율 및 대화형 모드를 제공합니다.

대화형 및 자율 모드를 사용하여 상호 작용 정도 제어

변환을 시작할 때 모드를 선택하면 채팅 창 상단의 드롭다운을 통해 언제든지 변경할 수 있습니다.

- 야간 또는 장기 실행 작업에 적합한 무인 변환에 자율 모드를 사용합니다. 여전히 결과를 검토하고 작업 종료 시 변경 사항을 요청할 수 있습니다.
- 대화형 모드를 사용하면 사용자 지정 가능한 변환 계획, 변환 세부 정보에 대한 높은 가시성, 각 프로젝트의 step-by-step 검토를 통해 변환 프로세스 전반에 걸쳐 채팅에서 에이전트와 협력할 수 있습니다. 반복하여 결과를 구체화하거나 만족할 때까지 방향을 변경할 수 있습니다.

모드를 결합할 수 있습니다. 예를 들어 대화형 모드에서 시작하여 변환 계획을 검토하고 조정한 다음 자율 모드로 전환하여 프로젝트를 자동으로 변환합니다.

에이전트에게 코드 변경 사항을 설명하도록 요청

이해되지 않는 코드 변경 사항이 표시되면 에이전트에게 설명을 요청하세요.

체크포인트를 사용하여 검토 또는 변경을 위해 프로젝트에서 중지

대화형 모드에서 계획을 승인한 후 모든 프로젝트에 대해 체크포인트를 설정하거나 지울 수 있습니다. 체크포인트가 있는 프로젝트가 변환되면 변환된 코드가 IDE의 프로젝트에 적용되고 에이전트가 검토를 위해 일시 중지됩니다. 결과를 검토할 수 있으며, 결과가 마음에 들지 않는 경우 더 많은 변경 사항을 요청할 수 있습니다.

체크포인트에서 중지된 동안 다음을 수행할 수 있습니다.

- 채팅에 표시된 결과를 검토하고 채팅에서 질문합니다. 예: "파일 X에서 암호화 API를 변경한 이유는 무엇입니까?"
- 작업 계획 AWS 변환 창에서 프로젝트의 결과 보기 버튼을 선택하여 코드 변경 사항을 봅니다.
- 추가 변경 사항을 요청하여 변환을 구체화합니다. 예: "로거 X를 사용하려면 변경" 또는 "패키지 Y 대신 패키지 X를 사용하려면 변경".
- 변환을 다시 시도하고 다른 지침에 따라 변환을 다시 시도합니다. 예: "이 클래스 라이브러리를 .NET 10 대신 .NET Standard를 대상으로 변경" 또는 "이 변환을 재시도하고 대상에서 MVC Razor PagesBlazor로 변경".
- IDE에서 코드를 직접 변경합니다.
- 에이전트에게 다음 프로젝트 체크포인트로 계속 진행하라고 지시합니다.

만족할 때까지 반복

현대화는 본질적으로 반복적이며 에이전트와 반복될 수 있습니다. 프로젝트 체크포인트 및 변환 종료 시에도 변경할 수 있습니다. 만족할 때까지 필요에 따라 반복합니다. 변환은 그렇게 말할 때까지 완료되지 않습니다.

체크포인트에서 중지될 때 에이전트와 함께 코딩

에이전트와 작업할 때 코드를 직접 변경할 수 있습니다. 체크포인트에서 중지되면에서 코드 파일을 편집할 수 있습니다Visual Studio. 에이전트에게 계속 진행하도록 지시하면 변경 사항이 동기화됩니다.

검증 및 마무리

변환이 완료되면 변환된 애플리케이션을 검증하고 프로덕션용으로 마무리합니다.

변환 보고서와 다음 단계를 검토하여 완료된 작업과 남은 작업을 이해합니다.

HTML 변환 보고서를 검토하여 수행된 작업을 이해합니다. 다음 단계 마크다운 파일을 검토하여 아직 남아 있는 작업을 이해합니다. 에이전트에게 명확하지 않은 부분이 있으면 명확히 해 달라고 요청합니다.

AI 코드 컴패니언을 사용하여 애플리케이션 검증, 디버깅 및 완료

변환된 애플리케이션의 정확성을 검토합니다. 와 같은 AI 코드 컴패니언[Kiro](#)을 사용하여 문제를 해결합니다.

단위 테스트 검증

솔루션에 단위 테스트 프로젝트(NUnit, xUnit또는 MSTest)가 포함된 경우 AWS 변환은 이를 최신 .NET으로 이식하고 테스트를 실행합니다. HTML 변환 보고서에서 단위 테스트 결과를 확인합니다. AI 코드 컴패니언을 사용하여 실패한 테스트를 수정합니다.

애플리케이션 기능 검증

애플리케이션을 실행하고 해당 기능이 원본과 일치하는지 확인합니다. 기능 문제와 런타임 오류를 기록해 둡니다. AI 코드 컴패니언으로 수정합니다.

애플리케이션 UI 검증

애플리케이션을 실행하고 탐색 및 라우팅을 포함하여 원래 애플리케이션처럼 보이고 작동하는지 확인합니다. 애플리케이션에 스타일이 없는 경우 .css 파일이 올바른 위치에 있지 않을 수 있습니다. AI 코드 컴패니언으로 수정합니다.

SQL Server 현대화

AWS SQL Server 현대화를 위한 변환은 Microsoft SQL Server 데이터베이스 및 관련 .NET 애플리케이션을 Amazon Aurora PostgreSQL로 전체 스택 현대화를 자동화하는 AI 기반 서비스입니다. 이 서비스는 스키마 변환, 데이터 마이그레이션, 새로운 대상 PostgreSQL과 일치하도록 애플리케이션 코드

수정 등 전체 마이그레이션 여정을 오케스트레이션하므로 복잡하고 노동 집약적인 작업을 자동화하여 팀의 생산성을 높일 수 있습니다.

지원되는 리전

AWS SQL Server용 변환은 미국 동부(버지니아 북부) - us-east-1에서 사용할 수 있습니다.

리전 간 사용: 지원되지 않는 리전의 데이터베이스의 경우 변환을 위해 데이터베이스를 지원되는 리전에 복제한 다음 결과를 대상 리전에 다시 배포할 수 있습니다.

기능 및 주요 기능

데이터베이스 변환

- 스키마 변환: 테이블, 뷰, 인덱스, 제약 조건 및 관계를 포함하여 SQL Server 스키마를 Aurora PostgreSQL로 자동 변환합니다.
- 저장 프로시저 변환: AI 향상된 정확도로 T-SQL 저장 프로시저를 PL/pgSQL로 변환합니다.
- 데이터 마이그레이션: AWS Database Migration Service(DMS)를 사용하여 무결성 검증으로 데이터 마이그레이션
- 데이터베이스 객체: 트리거, 함수, 뷰, 계산된 열 및 자격 증명 열 지원
- 검증: 자동화된 데이터 무결성 확인 및 참조 무결성 검사

애플리케이션 변환

- 개체 프레임워크 변환: PostgreSQL에 대한 개체 프레임워크 6.3-6.5 및 EF Core 1.0-8.0 구성을 업데이트합니다.
- ADO.NET 변환: ADO.NET 데이터 액세스 코드를 SQL Server에서 PostgreSQL 공급자로 변환합니다.
- 연결 문자열 업데이트: 모든 데이터베이스 연결 문자열을 새 대상 PostgreSQL 데이터베이스로 자동 업데이트
- 데이터베이스 공급자 변경: SQL Server 공급자를 Npgsql(PostgreSQL 공급자)로 대체
- ORM 구성 업데이트: 데이터 유형 매핑, 자격 증명 열 및 데이터베이스별 구성을 수정합니다.

오케스트레이션 및 검증

- 웨이브 기반 현대화: 대규모 자산을 논리적 마이그레이션 단계로 구성

- 종속성 매핑: 애플리케이션과 데이터베이스 간의 관계를 식별합니다.
- Human-in-the-loop(HITL) 체크포인트: 중요한 단계에서 검토 및 승인 게이트를 제공합니다.
- 자동 검증: 스키마 호환성, 데이터 무결성 및 애플리케이션 기능을 테스트합니다.
- CI/CD 통합: 기존 개발 파이프라인과 통합

배포

- Amazon ECS 및 Amazon EC2 배포: 자동 크기 조정을 지원하는 자동화된 컨테이너식 배포
- Infrastructure-as-code 생성: CloudFormation 또는 AWS CDK 템플릿을 생성합니다.
- 자동 배포 검증: 상태 확인을 통해 성공적인 배포 확인
- 롤백 기능: 문제가 발생할 경우 롤백 절차를 지원합니다.

지원되는 버전 및 프로젝트 유형

SQL Server 버전

AWS 변환은 다음 SQL Server 버전을 지원합니다.

SQL Server 버전	지원 상태
SQL Server 2022	지원됨
SQL Server 2019	지원됨
SQL Server 2017	지원됨
SQL Server 2016	지원됨
SQL Server 2014	지원됨
SQL Server 2012	지원됨
SQL Server 2008 R2	지원됨

Note

모든 SQL Server 에디션이 지원됩니다(Express, Standard, Enterprise). SQL Server는 AWS (SQL Server용 Amazon RDS 또는 Amazon EC2의 SQL Server)에서 호스팅하거나 외부에서 호스팅할 수 있습니다 AWS.

.NET 버전

.NET 버전	지원 상태
.NET 10	지원됨
.NET 8	지원됨
.NET 7	지원됨
.NET 6(코어)	지원됨
.NET Framework 4.x 이하	지원되지 않음

Important

레거시 .NET Framework 4.x 및 이전 버전은 지원되지 않습니다. 애플리케이션이 .NET Framework를 사용하는 경우 SQL Server AWS 변환 기능을 사용하기 전에 먼저 Transform for .NET 현대화를 사용하여 .NET Core 6+로 업그레이드해야 합니다.

Entity Framework 버전

프레임워크	지원되는 버전
개체 프레임워크 6	6.3, 6.4, 6.5
개체 프레임워크 코어	1.0~8.0
ADO.NET	모든 버전(GA)

소스 코드 리포지토리

AWS 변환은 다음 소스 코드 플랫폼을 지원합니다.

- GitHub 및 GitHub Enterprise Server
- GitLab.com 및 GitLab 자체 관리형
- Bitbucket Cloud 및 Bitbucket 데이터 센터
- Azure DevOps 및 Azure DevOps Server
- Amazon S3

대상 데이터베이스

AWS 최신 Aurora 기능 및 최적화를 지원하여 Amazon Aurora PostgreSQL(PostgreSQL 15+ 호환)을 대상으로 변환합니다.

기술 요구 사항

데이터베이스 요구 사항

- Microsoft SQL Server 버전 2008 R2~2022
- (AWS Amazon RDS for SQL Server 또는 SQL Server on Amazon EC2)에서 호스팅되거나 외부에서 호스팅되는 SQL Server AWS
- AWS호스팅된 데이터베이스의 경우 데이터베이스와 AWS 변환이 동일한 AWS 리전에 있어야 합니다.
- 외부에서 호스팅되는 데이터베이스의 경우 AWS 변환 서비스에 대한 AWS네트워크 연결이 필요합니다.
- VIEW DEFINITION 및 VIEW DATABASE STATE 권한이 있는 데이터베이스 사용자
- 인쇄 가능한 ASCII 문자만 사용하는 데이터베이스 암호('/', '@', '' 및 공백 제외)
- 소스 SQL Server가 포함된 VPC에는 최소 2개의 서로 다른 가용 영역에 서브넷이 있어야 합니다 (DMS 복제 서브넷 그룹에 필요).

애플리케이션 요구 사항

- .NET Core 6, 7 또는 8 애플리케이션
- Entity Framework 6.3-6.5 또는 Entity Framework Core 1.0-8.0 또는 ADO.NET

- 소스 코드에서 데이터베이스 연결 검색 가능
- 애플리케이션이 성공적으로 빌드되고 실행됨
- 지원되는 리포지토리 플랫폼의 소스 코드

AWS 계정 요구 사항

- AWS 관리자 액세스 권한이 있는 계정
- IAM Identity Center 활성화
- 생성된 필수 서비스 역할(아래 설정 지침 참조)
- 적절한 네트워크 구성이 있는 VPC

데이터 처리 및 스토리지

처리 위치

- 스키마 처리는 VPC 내의 DMS 인스턴스에서 발생합니다.
- 데이터 마이그레이션은 선택 사항이며 필요한 경우 제외할 수 있습니다.
- 변환 아티팩트는 AWS 변환 서비스 리전에 저장됩니다.

저장된 아티팩트

다음 항목은 서비스 리전에 저장됩니다.

- 에이전트 로그
- 평가 결과
- SQL 스키마 파일
- DMS 출력 아티팩트

Important

데이터 레지던시에 중요: 데이터 마이그레이션을 옵트아웃하더라도 메타데이터 및 처리 아티팩트는 서비스 리전에 저장됩니다. 이는 데이터 레지던시 요구 사항이 엄격한 조직에 중요합니다.

아티팩트 관리

- 자체 KMS 키를 사용한 암호화를 위한 고객 옵션
- 모든 아티팩트에 대해 정의된 TTL(time-to-live) 기간
- 오프라인 스토리지를 위해 아티팩트를 다운로드할 수 있습니다.

SQL Server 요구 사항

데이터베이스 요구 사항

외부에서 호스팅되는 데이터베이스

외부에서 호스팅되는 데이터베이스 AWS 가 지원됩니다. 외부에서 호스팅되는 데이터베이스를 사용하려면 데이터베이스와 AWS 변환 서비스 간의 네트워크 연결을 보장해야 합니다.

SSIS 워크로드

- 제한: SQL Server Integration Services(SSIS) 변환은 지원되지 않습니다.
- 해결 방법: SSIS 마이그레이션에 AWS Glue 또는 기타 ETL 서비스를 사용합니다.

연결된 서버

- 제한: 연결된 서버를 통한 외부 데이터베이스 연결에는 인적 구성이 필요합니다.
- 해결 방법: 마이그레이션 후 연결된 서버를 재구성하거나 데이터베이스 링크 또는 애플리케이션 수준 통합과 같은 대체 접근 방식을 사용합니다.

복잡한 T-SQL 패턴

- 제한: 일부 고급 T-SQL 패턴은 사람의 개입이 필요할 수 있습니다.
- 해결 방법: 복잡한 SQL 변환에 Amazon Kiro CLI를 사용합니다. AWS 변환 프로세스 중에 검토를 위해 변환 플래그를 지정합니다.

애플리케이션 요구 사항

레거시 .NET Framework

- 제한 사항: .NET Framework 4.x 및 이전 버전은 지원되지 않습니다.

- 해결 방법: .NET용 AWS 변환을 사용하여 먼저 .NET Core 6 이상으로 업그레이드한 다음 SQL Server 변환을 사용합니다.

Entity Framework 버전

- 제한: Entity Framework 6.3-6.5 및 EF Core 1.0-8.0만 지원됩니다.
- 해결 방법: 변환 전에 지원되는 Entity Framework 버전으로 업그레이드합니다.

VB.NET 애플리케이션

- 제한: VB.NET 지원되지 않습니다.
- 해결 방법: C#로 변환하거나 사용자 지정 AWS 변환을 사용하여 VB.NET C#으로 변환합니다.

데이터베이스 간 종속성

- 제한: 데이터베이스 스키마가 여러 데이터베이스 간에 상호 작용할 때 발생하는 문제입니다.
- 해결 방법: 마이그레이션 전에 데이터베이스 간 쿼리를 검토하고 리팩터링합니다. 데이터베이스를 통합하거나 PostgreSQL 스키마를 사용하는 것이 좋습니다.
- 영향: 복잡한 데이터베이스 간 시나리오에 대해 사람의 개입이 필요할 수 있습니다.

리포지토리-데이터베이스 결합

- 제한: 단일 리포지토리가 여러 데이터베이스를 제공할 때 발생하는 문제입니다.
- 해결 방법: 리포지토리 재구성 또는 단계별 마이그레이션 접근 방식을 고려합니다.
- 영향: 웨이브 기반 마이그레이션을 위한 추가 계획이 필요할 수 있습니다.

인프라 요구 사항

작업당 단일 계정/리전

- 제한: 각 변환 작업은 하나의 AWS 계정과 리전을 대상으로 합니다.
- 해결 방법: 다중 계정 또는 다중 리전 배포를 위한 여러 변환 작업을 생성합니다.

배포 대상

- 제한: Amazon ECS 및 Amazon EC2 배포가 지원됩니다.

리포지토리 요구 사항

프라이빗 NuGet 패키지

- 제한 사항: 프라이빗 NuGet 패키지에는 추가 구성이 필요합니다.
- 해결 방법: 작업을 시작하기 전에 변환 설정에서 프라이빗 NuGet 피드를 구성합니다.

SQL Server 설정

SQL Server 환경에서 다음 단계를 수행하여 현대화 AWS 변환을 활성화합니다.

데이터베이스 설정 및 구성

1단계: 필요한 권한이 있는 데이터베이스 사용자 생성

필요한 권한을 가진 AWS 변환 전용 데이터베이스 사용자를 생성합니다. 이미 DMS Schema Conversion 사용자가 있는 경우 재사용할 수 있습니다.

SQL Server 인스턴스에 연결하고 다음 명령을 실행합니다.

```
-- Create the login in master database
USE master;
CREATE LOGIN [atx_user] WITH PASSWORD = 'YourStrongPassword123!';

-- Switch to your application database
USE [YourDatabaseName];
CREATE USER [atx_user] FOR LOGIN [atx_user];

-- Grant required permissions
GRANT VIEW DEFINITION TO [atx_user];
GRANT VIEW DATABASE STATE TO [atx_user];
ALTER ROLE [db_datareader] ADD MEMBER [atx_user];

-- Grant master database permissions
USE master;
GRANT VIEW SERVER STATE TO [atx_user];
```

```
GRANT VIEW ANY DEFINITION TO [atx_user];
```

Note

현대화하려는 각 데이터베이스에 대해 데이터베이스별 명령(USE, CREATE USER, GRANT)을 반복합니다.

db_datareader 역할은 스키마 변환에만 필요하지 않고 데이터 마이그레이션에만 필요합니다.

- db_datareader 역할은 데이터베이스의 모든 테이블에 대한 읽기 액세스 권한을 부여합니다.
- 이 역할은 데이터 마이그레이션을 수행할 때만 필요합니다.
- 스키마 변환의 경우에만(데이터 마이그레이션 제외) db_datareader 역할은 필요하지 않습니다.
- 다른 권한(VIEW DEFINITION, VIEW DATABASE STATE 등)은 스키마 변환에 충분합니다.

2단계: AWS Secrets Manager에 자격 증명 저장

데이터베이스 자격 증명을 AWS Secrets Manager에 안전하게 저장합니다. DMS에 대한 보안 암호가 이미 생성된 경우 이 단계를 건너뛵니다.

1. 콘솔에서 AWS Secrets Manager로 이동
2. 새 보안 암호 저장을 선택합니다.
3. 보안 암호를 구성합니다.
 - 보안 암호 유형: 다른 데이터베이스의 자격 증명
 - 데이터베이스: Microsoft SQL Server
 - 사용자 이름: atx_user(또는 선택한 사용자 이름)
 - 암호: 생성한 암호
 - 서버 이름: SQL Server 엔드포인트
 - 데이터베이스 이름: 데이터베이스 이름
 - 포트: 1433(또는 사용자 지정 포트)
4. 다음을 선택합니다.
5. 보안 암호 이름 입력: atx-db-modernization-sqlserver
6. 필수 태그를 추가합니다(이러한 태그는 필수).
 - 키: 프로젝트, 값: atx-db-modernization

- 키: 소유자, 값: 데이터베이스 커넥터
- 나머지 화면에서 다음을 선택합니다.
 - 스토어 선택
 - 다음 단계에서 사용할 보안 암호 ARN을 기록해 둡니다.

Important

데이터베이스 암호는 '/', '@', '"' 및 공백을 제외한 인쇄 가능한 ASCII 문자만 사용해야 합니다. 삭제가 예약된 보안 암호는 변환 실패를 일으킬 수 있습니다.

3단계: 필수 DMS 역할 생성

AWS 변환에는 DMS 작업에 대한 특정 IAM 역할이 필요합니다. 아래 CloudFormation 템플릿을 사용하여 이러한 역할을 배포합니다.

Note

AWS 계정에 이미 기존 DMS 관련 역할이 있는 경우 중복을 생성하는 대신 해당 리소스를 재사용하도록 템플릿을 수정합니다.

다음 콘텐츠를 사용하여 dms-roles.yaml이라는 파일을 생성합니다.

```
AWSTemplateFormatVersion: '2010-09-09'
Description: 'DMS Service Roles for AWS Transform SQL Server Modernization'

Resources:
  DMSCloudWatchLogsRole:
    Type: AWS::IAM::Role
    Properties:
      RoleName: dms-cloudwatch-logs-role
      AssumeRolePolicyDocument:
        Version: '2012-10-17'
        Statement:
          - Effect: Allow
            Principal:
              Service:
                - dms.amazonaws.com
```

```

        - schema-conversion.dms.amazonaws.com
    Action: sts:AssumeRole
    ManagedPolicyArns:
        - arn:aws:iam::aws:policy/service-role/AmazonDMSCloudWatchLogsRole

```

DMSS3AccessRole:

Type: AWS::IAM::Role

Properties:

RoleName: dms-s3-access-role

AssumeRolePolicyDocument:

Version: '2012-10-17'

Statement:

- Effect: Allow

Principal:

Service:

- dms.amazonaws.com
- schema-conversion.dms.amazonaws.com

Action: sts:AssumeRole

Policies:

- PolicyName: S3TaggedAccess

PolicyDocument:

Version: '2012-10-17'

Statement:

- Effect: Allow

Action:

- s3:GetBucketLocation
- s3:GetBucketVersioning
- s3:PutObject
- s3:PutBucketVersioning
- s3:GetObject
- s3:GetObjectVersion
- s3:ListBucket
- s3:DeleteObject

Resource: arn:aws:s3:::atx-db-modernization-*

Condition:

StringEquals:

aws:ResourceAccount: !Ref AWS::AccountId

DMSecretsManagerRole:

Type: AWS::IAM::Role

Properties:

RoleName: dms-secrets-manager-role

AssumeRolePolicyDocument:

Version: '2012-10-17'

Statement:

- Effect: Allow

Principal:

Service:

- dms.amazonaws.com
- schema-conversion.dms.amazonaws.com

Action: sts:AssumeRole

Policies:

- PolicyName: SecretsManagerTaggedAccess

PolicyDocument:

Version: '2012-10-17'

Statement:

- Effect: Allow

Action:

- secretsmanager:GetSecretValue
- secretsmanager:DescribeSecret

Resource: '*'

Condition:

StringEquals:

secretsmanager:ResourceTag/Project: atx-db-modernization
secretsmanager:ResourceTag/Owner: database-connector

DMSVPCRole:

Type: AWS::IAM::Role

Properties:

RoleName: dms-vpc-role

AssumeRolePolicyDocument:

Version: '2012-10-17'

Statement:

- Effect: Allow

Principal:

Service:

- dms.amazonaws.com
- schema-conversion.dms.amazonaws.com

Action: sts:AssumeRole

ManagedPolicyArns:

- arn:aws:iam::aws:policy/service-role/AmazonDMSVPCManagementRole

DMSServerlessRole:

Type: AWS::IAM::ServiceLinkedRole

Properties:

AWSServiceName: dms.amazonaws.com

Description: 'Service Linked Role for AWS DMS Serverless'

Outputs:**DMSCloudWatchLogsRoleArn:**

Description: ARN of the DMS CloudWatch Logs Role

Value: !GetAtt DMSCloudWatchLogsRole.Arn

DMSS3AccessRoleArn:

Description: ARN of the DMS S3 Access Role

Value: !GetAtt DMSS3AccessRole.Arn

DMSSecretsManagerRoleArn:

Description: ARN of the DMS Secrets Manager Role

Value: !GetAtt DMSecretsManagerRole.Arn

DMSVPCRoleArn:

Description: ARN of the DMS VPC Role

Value: !GetAtt DMSVPCRole.Arn

Export:

Name: !Sub \${AWS::StackName}-VPCRole

DMSServerlessRoleArn:

Description: ARN of the DMS Serverless Role

Value: !Sub 'arn:aws:iam::\${AWS::AccountId}:role/aws-service-role/dms.amazonaws.com/AWSServiceRoleForDMSServerless'

Export:

Name: !Sub \${AWS::StackName}-ServerlessRole

AWS CLI를 사용하여 CloudFormation 스택을 배포합니다.

```
aws cloudformation create-stack \
  --stack-name dms-roles \
  --template-body file://dms-roles.yaml \
  --capabilities CAPABILITY_NAMED_IAM \
  --region us-east-1
```

또는 AWS 콘솔을 사용하여 배포합니다.

1. AWS 콘솔에서 CloudFormation으로 이동
2. 스택 생성을 선택합니다.
3. 템플릿 파일 업로드를 선택합니다.
4. dms-roles.yaml 파일 업로드
5. 스택 이름 입력: dms-roles
6. IAM 기능 승인
7. 스택 생성을 선택합니다.

4단계: 네트워크 보안 구성

AWS 변환, SQL Server 데이터베이스 및 기타 AWS 서비스 간에 네트워크 연결이 적절한지 확인합니다.

보안 그룹 구성(권장 접근 방식)

권장 접근 방식: IP 기반 규칙 대신 보안 그룹 기반 액세스 제어를 사용합니다. 이렇게 하면 보안이 향상되고 관리가 쉬워지며 AWS Transform의 아키텍처와 원활하게 작동합니다.

보안 그룹 기반 액세스 제어가 필요한 이유

- DMS Schema Conversion은 VPC 내에 탄력적 네트워크 인터페이스(ENIs)를 생성합니다.
- 데이터베이스에 공개적으로 액세스할 필요가 없습니다.
- AWS 변환은 프라이빗 IP 주소를 노출하지 않으므로 IP 기반 규칙이 복잡합니다.
- 보안 그룹 참조는 리소스 규모에 따라 동적 자동 업데이트를 제공합니다.

SQL Server 보안 그룹 구성

AWS 변환에서 DMS Schema Conversion Instance Profile을 구성할 때 DMS SC 인스턴스에 대한 보안 그룹을 지정합니다. 데이터베이스 보안 그룹은 DMS SC 보안 그룹의 인바운드 트래픽을 허용해야 합니다.

Step-by-step 구성:

1. DMS Schema Conversion 보안 그룹을 식별합니다.
 - AWS 변환에서 인스턴스 프로파일을 생성할 때 지정됩니다.
 - 보안 그룹 ID 기록(예: sg-0123456789abcdef0)
2. SQL Server 보안 그룹 인바운드 규칙을 업데이트합니다.
 - 유형: 사용자 지정 TCP
 - 포트: 1433(또는 사용자 지정 SQL Server 포트)
 - 소스: DMS Schema Conversion Security Group ID
 - 설명: "DMS Schema Conversion 액세스 허용"
3. Aurora PostgreSQL 대상의 경우(생성 후):
 - 유형: PostgreSQL
 - 포트: 5432(또는 사용자 지정 PostgreSQL 포트)
 - 소스: DMS Schema Conversion 보안 그룹 ID

- 설명: "DMS Schema Conversion 액세스 허용"

Important

최소 권한 보안 모델에 중요: 조직에서 기본적으로 모든 트래픽을 차단하는 "최소 권한" 보안 모델을 사용하는 경우 DMS Schema Conversion Security Group에서 데이터베이스 포트로의 인바운드 트래픽을 명시적으로 허용해야 합니다. 모든 소스 또는 IP 범위에 대해 포트 1433을 열지 마십시오.

필수 AWS 서비스 연결

VPC가 다음과 통신할 수 있는지 확인합니다.

- AWS 서비스 엔드포인트 변환
- AWS DMS 엔드포인트
- Aurora PostgreSQL 엔드포인트
- 아티팩트 스토리지용 S3 엔드포인트
- AWS Secrets Manager 엔드포인트
- AWS CodeConnections 엔드포인트

VPC 엔드포인트: 프라이빗 네트워크의 경우 인터넷 게이트웨이 종속성을 방지하기 위해 필요한 AWS 서비스에 대한 VPC 엔드포인트를 구성합니다.

외부 호스팅 데이터베이스에 대한 요구 사항

SQL Server 데이터베이스가 외부에서 호스팅되는 경우 AWS다음 사전 조건을 충족하는지 확인한 다음 현대화를 시작하기 전에 설정 단계를 완료합니다.

사전 조건

- VPC가 있는 AWS 계정
- VPC와 외부 데이터베이스 간의 네트워크 연결. 네트워크 연결 구성에 대한 자세한 내용은 AWS DMS 사용 설명서의 [네트워크 연결 구성](#)을 참조하세요.

설정 단계

1. 외부 데이터베이스의 연결 세부 정보를 AWS Secrets Manager 사용하여에서 보안 암호를 생성합니다. 자세한 내용은 [the section called “2단계: AWS Secrets Manager에 자격 증명 저장”](#) 단원을 참조하십시오.
2. 메시지가 표시되면 외부 데이터베이스에 연결하기 위한 VPC ID와 보안 그룹 ID를 제공합니다. 보안 암호의 데이터베이스 호스트 이름을 AWS 계정 내에서 확인할 수 없으므로 AWS 변환에이 정보를 입력하라는 메시지가 표시됩니다.

AWS 변환 설정

AWS 변환 콘솔에 액세스하고 새로운 현대화 프로젝트를 시작하여 현대화 여정을 시작합니다. 이 단계에서는 워크스페이스를 설정하고 풀 스택 변환을 위한 기본 구성을 설정합니다.

완료할 작업:

- AWS 관리 콘솔에서 AWS 변환 서비스로 이동합니다.
- 서비스 옵션에서 Microsoft Modernization을 선택합니다.
- 새 현대화 프로젝트 생성을 선택합니다.
- 프로젝트 이름 및 설명 제공
- 대상 AWS 리전 선택(SQL Server 위치와 일치해야 함)
- 프로젝트 설정 검토 및 확인

Note

모범 사례: 애플리케이션 이름과 대상 환경(예: 'CustomerPortal-Production-Modernization')을 포함하는 설명이 포함된 프로젝트 이름을 사용하여 다중 웨이브 시나리오에서 프로젝트를 쉽게 식별할 수 있습니다.

SQL Server 현대화 작업 생성

데이터베이스 및 소스 코드 리포지토리 연결

데이터베이스 커넥터 구성

데이터베이스 커넥터를 구성하여 SQL Server 데이터베이스에 대한 보안 연결을 설정합니다. 커넥터는 환경 분석, 종속성 검색을 수행하고 AWS Transform이 평가 및 변환을 위해 데이터베이스 스키마 및 메타데이터에 액세스할 수 있도록 합니다.

완료할 작업:

- 설정 마법사에서 데이터베이스 커넥터 구성을 선택합니다.
- 연결 방법 선택: 새 연결 또는 기존 연결
- SQL Server 연결 세부 정보(엔드포인트, 포트, 데이터베이스 이름) 제공
- 인증 및 테스트 연결 구성
- 검색된 데이터베이스 검토 및 선택 확인

Note

네트워크 연결: SQL Server 보안 그룹 및 NACLs AWS 변환 서비스 엔드포인트로부터의 inbound 연결을 허용하는지 확인합니다.

소스 코드 리포지토리 연결

AWS 변환을 활성화하여 .NET 애플리케이션 소스 코드에 액세스합니다. AWS 변환은 PAT(Personal Access Token) 커넥터(권장), AWS CodeConnections 또는 Amazon S3의 세 가지 소스 코드 제공 방법을 지원합니다. 이 통합을 통해 서비스는 애플리케이션 코드를 분석하고, 데이터베이스 종속성을 식별하고, PostgreSQL 호환성을 위한 자동 코드 변환을 수행할 수 있습니다.

완료할 작업:

- 소스 코드 리포지토리 연결 섹션으로 이동
- 인증 방법 선택: PAT 커넥터(권장), AWS CodeConnections 또는 Amazon S3
- .NET 애플리케이션이 포함된 리포지토리 선택
- 분석을 위한 브랜치 지정(일반적으로 메인/마스터 또는 개발)
- 리포지토리 액세스 및 코드 구조 검증

Note

리포지토리 검색: AWS 변환은 리포지토리를 자동으로 스캔하여 .NET 프로젝트, Entity Framework 구성, 데이터베이스 연결 문자열 및 SQL 종속성을 식별합니다.

Note

보안 참고: AWS 변환은 리포지토리에 대한 읽기 액세스 권한만 필요하며 변환된 코드에 대한 새 기능 브랜치를 생성합니다. 기본 브랜치는 그대로 유지됩니다.

루프의 사람

AWS 변환은 human-in-the-loop(HITL) 메커니즘을 사용하여 품질을 보장하고 중요한 변환 결정을 검토하고 승인할 수 있습니다. 다음 체크포인트에는 주의가 필요합니다.

웨이브 플랜 검토 및 승인

검토 내용: 그룹화된 데이터베이스와 애플리케이션, 웨이브 시퀀스를 포함하여 제안된 마이그레이션 웨이브입니다.

다음을 수행할 수 있습니다.

- 웨이브 플랜 승인
- 파도 간에 데이터베이스를 이동하여 파도 사용자 지정
- 웨이브 시퀀스 수정
- 웨이브 분할 또는 병합

승인 후 AWS 변환은 스키마 변환을 진행합니다.

스키마 변환 검토

검토 내용: 테이블, 저장 프로시저, 함수 및 트리거를 포함한 변환된 데이터베이스 객체입니다. 작업 항목은 주의가 필요한 객체를 강조 표시합니다.

다음을 수행할 수 있습니다.

- 변환된 코드 수락

- 변환된 코드 수정
- 변환 후 인적 검토를 위한 플래그
- 원본 코드와 변환된 코드의 side-by-side 비교 보기

approval:Transform 이후 발생하는 작업 AWS에서는 스키마를 Aurora PostgreSQL에 적용하고 데이터 마이그레이션을 진행합니다(구성된 경우).

애플리케이션 코드 검토

검토 내용: Entity Framework 구성, 연결 문자열, 데이터 액세스 코드 및 저장 프로시저 호출을 포함한 모든 애플리케이션 코드 변경 사항입니다.

다음을 수행할 수 있습니다.

- 각 파일에 대한 변경 사항 수락
- 변환된 코드 수정
- 변경 사항 거부(권장되지 않음)
- 팀에 대한 설명 추가
- 로컬 검토를 위해 변환된 코드 다운로드

승인 후 발생하는 일: AWS 변환은 리포지토리의 새 브랜치에 변경 사항을 커밋하고 검증을 진행합니다.

검증 결과 검토

검토 내용: 스키마 호환성, 데이터 무결성 검사 및 애플리케이션 빌드 상태를 포함한 자동 검증 결과입니다.

다음을 수행할 수 있습니다.

- 통과된 테스트 검토
- 실패한 테스트 조사
- 경고 해결
- 배포로 진행하거나 문제 해결로 돌아갑니다.

approval: AWS Transform은 대상 환경에 배포하기 위해 준비합니다.

배포 승인

검토 내용: infrastructure-as-code 템플릿, ECS 서비스 구성 및 배포 설정을 포함한 배포 구성.

다음을 수행할 수 있습니다.

- 배포 설정 검토 및 사용자 지정
- 계속하려면 배포 승인
- 추가 테스트를 위한 배포 지연
- 검토를 위한 인프라 코드 다운로드

승인 후 AWS Transform은 현대화된 애플리케이션과 데이터베이스를 대상 환경에 배포합니다.

평가 및 웨이브 계획

랜딩 존 설정

현대화된 애플리케이션을 배포할 대상 인프라 환경을 구성합니다. 랜딩 존 설정에는 Aurora PostgreSQL 프로비저닝, 네트워킹 구성 및 참조 배포 구성이 포함됩니다.

완료할 작업:

- 구성 메뉴에서 랜딩 존 설정을 선택합니다.
- Aurora PostgreSQL 대상 구성(버전, 인스턴스 클래스, 다중 AZ)
- 네트워크 및 보안 설정 구성(VPC, 서브넷, 보안 그룹)

Note

비용 고려 사항: Aurora PostgreSQL 인스턴스에는 지속적인 비용이 발생합니다. 개발/테스트 환경에 Aurora Serverless v2를 사용하는 것이 좋습니다.

평가

데이터베이스 스키마, 애플리케이션 코드 및 종속성에 대한 포괄적인 분석을 수행합니다. 평가 단계에서는 변환 복잡성 등급을 제공하고, 잠재적 문제를 식별하고, 자세한 보고서를 생성합니다.

완료할 작업:

- 코드 분석을 위한 리포지토리 브랜치 선택
- 변환할 리포지토리 및 데이터베이스 선택
- 평가 결과 및 복잡성 등급 검토
- 노력 예측을 사용하여 평가 보고서 생성
- 이해관계자 검토 및 승인을 위한 보고서 내보내기

Note

평가 인사이트: 평가는 스키마 객체, 저장 프로시저, 애플리케이션 종속성에 대한 자세한 분석을 제공하고 필요한 인적 개입 수준을 추정합니다.

웨이브 계획

변환 복잡성, 비즈니스 우선 순위 및 애플리케이션 종속성을 기반으로 현대화를 관리 가능한 웨이브로 구성합니다. AWS 변환은 사용자 지정할 수 있는 지능형 웨이브 권장 사항을 생성합니다.

완료할 작업:

- AI 생성 웨이브 플랜 및 권장 사항 검토
- 비즈니스 우선 순위에 따라 Wave Configuration 사용자 지정
- 애플리케이션과 데이터베이스 간의 종속성 검증
- 대화형 인터페이스를 사용하여 Wave Plan 마무리
- 웨이브 실행 우선 순위 설정 및 책임 할당

Note

AI 기반 권장 사항: 자연어를 통해 AI와 상호 작용하여 'Move CustomerDB to Wave 1' 또는 'Combine these two applications into same wave' 권장 사항을 조정할 수 있습니다.

Note

모범 사례: 1~2개의 복잡성이 낮은 데이터베이스가 포함된 파일럿 웨이브로 시작하여 프로세스를 설정하고 팀 신뢰를 구축합니다.

각 웨이브에 대한 데이터 마이그레이션

각 웨이브에 대한 스키마 변환

AI 강화 변환 기능을 사용하여 SQL Server 데이터베이스 스키마를 PostgreSQL 호환 스키마로 변환합니다. 이 프로세스는 테이블, 저장 프로시저, 함수, 트리거 및 기타 데이터베이스 객체를 변환합니다.

완료할 작업:

- 스키마 변환 대상 제공 및 기본 설정 구성
- DMS Schema Conversion 서비스를 사용하여 자동 변환 실행
- 변환 결과 검토 및 인적 개입 항목 식별
- HITL 프롬프트를 통한 수동 개입 처리
- 인적 수정을 검증하고 필요한 경우 변환을 다시 실행합니다.

Note

일반적인 수동 개입: 연결된 서버, 사용자 정의 유형, 고급 T-SQL 패턴 및 공급업체별 SQL 기능은 일반적으로 인적 검토 및 수정이 필요합니다.

각 웨이브에 대한 데이터 마이그레이션

AWS Database Migration Service (AWS DMS) 통합을 사용하여 SQL Server에서 Aurora PostgreSQL로 데이터를 전송합니다. 테스트 목적으로 프로덕션 데이터 마이그레이션 또는 합성 데이터 생성 중에서 선택합니다.

완료할 작업:

- 프로덕션 데이터 마이그레이션 또는 합성 데이터 생성을 선택합니다.
- 데이터 전송을 위한 DMS 복제 인스턴스 구성
- 마이그레이션 진행 상황 모니터링 및 데이터 불일치 처리
- 데이터 무결성 및 참조 제약 조건 검증
- 계속하기 전에 완료 확인

Note

자동 DMS 통합: AWS 변환은 엔드포인트 생성, 작업 구성 및 데이터 유형 매핑을 자동으로 처리하여 DMS 구성의 복잡성을 추상화합니다.

Note

데이터 검증: 이 서비스는 소스 데이터베이스와 대상 데이터베이스 모두에 대해 동일한 쿼리를 실행하여 데이터 일관성을 보장함으로써 경험적 테스트를 수행합니다.

각 웨이브에 대한 코드 마이그레이션

Entity Framework 구성 업데이트, 연결 문자열 수정, SQL 쿼리 적응 및 프레임워크별 조정을 포함하여 Aurora PostgreSQL에서 작동하도록 .NET 애플리케이션 코드를 변환합니다.

완료할 작업:

- SQL Server 종속성에 대한 자동 코드 분석 실행
- 프레임워크 변환 수행(엔터티 프레임워크 공급자 업데이트)
- PostgreSQL 호환 SQL에 SQL 쿼리 구문 적응
- 변환된 코드에 대한 대상 브랜치 관리 구성
- 복잡한 패턴에 대한 수동 개입 처리

SQL Server 현대화 워크플로

이 섹션에서는 AWS 변환을 사용한 전체 SQL Server 현대화 프로세스를 step-by-step로 안내합니다.

1단계: SQL Server 현대화 작업 생성

AWS 변환 콘솔에서 새 변환 작업을 생성하여 현대화 여정을 시작합니다.

1. AWS 변환 콘솔에 로그인
2. 현대화 작업을 생성을 선택합니다.
3. Windows 현대화 작업을 선택한 다음 SQL Server 현대화를 선택합니다.

4. 작업 세부 정보를 입력합니다.

- 작업 이름: 프로젝트의 설명 이름
- 설명: 선택적 설명
- 배포 대상 리전: AWS 리전

5. 작업 생성을 선택합니다.

Important

작업 이름에 개인 식별 정보(PII)를 포함하지 마십시오.

2단계: SQL Server 데이터베이스에 연결

AWS 변환을 SQL Server 데이터베이스에 연결하여 스키마 분석 및 변환을 활성화합니다.

데이터베이스 커넥터 생성

1. SQL Server 현대화 작업에서 리소스에 연결로 이동합니다.
2. SQL Server 데이터베이스에 연결을 선택합니다.
3. 새 커넥터 생성을 선택합니다.
4. 커넥터 정보를 입력합니다.
 - 어휘 이름: 설명 이름
 - AWS 계정 ID: SQL Server가 호스팅되는 계정
5. 확인되면 승인을 위한 링크를 받게 됩니다. 승인 링크를 복사하여 계정에 대한 AWS 관리자의 승인을 받습니다. 승인되면 다음 단계로 진행할 수 있습니다.
6. 관리자가 커넥터 요청을 승인한 후 제출을 클릭하여 소스 코드 연결 설정으로 진행합니다.

3단계: 소스 코드 리포지토리 연결

AWS 변환은 SQL Server 데이터베이스와 상호 작용하는 코드를 분석하고 변환하기 위해 .NET 애플리케이션 소스 코드에 대한 액세스 권한이 필요합니다. AWS 변환은 소스 코드를 제공하는 세 가지 방법을 지원합니다.

인증 방법 선택

개인용 액세스 토큰(PAT) 커넥터(권장)

사용자 지정 권한 범위, 자체 호스팅 공급자 지원 또는 GitHub Secrets와 같은 공급자별 APIs에 대한 액세스가 필요한 팀에 가장 적합합니다. 사용자 지정 권한을 사용하여 소스 코드 공급자에서 PAT를 생성하고, 저장하고 AWS Secrets Manager, 필요한 경우 AWS 변환이 이를 검색합니다. 토큰 교체 및 만료 관리는 사용자의 책임입니다.

AWS CodeConnections

자동 자격 증명 관리를 원하는 팀에 가장 적합합니다. AWS CodeConnections는 OAuth 2.0 권한 부여 흐름을 통해 인증을 처리하는 관리형 공급자 통합을 사용합니다.는 자동 토큰 새로 고침 및 교체를 포함한 전체 자격 증명 수명 주기를 AWS 관리합니다. 수동 자격 증명 관리는 필요하지 않습니다.

Amazon S3

소스 코드를 Amazon S3 버킷에 직접 업로드합니다. AWS 변환은 변환 작업 중에 버킷에서 코드에 액세스합니다.

기능	PAT 커넥터(권장)	AWS CodeConnections
보안 인증 정보 관리	수동(고객 관리형)	자동(AWS관리형)
토큰 수명 주기	수동 교체 필요	자동 새로 고침
권한 유연성	완전히 사용자 지정 가능한 범위	수정된 권한
자체 호스팅 공급자 지원	지원됨	사용할 수 없음
설정 복잡성	보통(수동 토큰 생성 및 스토리지)	낮음(일회성 권한 부여)
토큰 스토리지	고객의 AWS Secrets Manager	AWS관리형

PAT 커넥터 설정(권장)

PAT 커넥터를 사용하면 사용자 지정 권한이 있는 소스 코드 공급자에서 개인 액세스 토큰을 생성하고, 안전하게 저장하고 AWS Secrets Manager, 필요한 경우 AWS 변환이 이를 검색합니다. 교체 및 만료

를 포함하여 토큰 수명 주기를 관리할 책임이 있습니다. AWS 변환은 보안 암호에 액세스할 수 있는 권한이 있는 필요한 IAM 역할을 자동으로 생성합니다.

PAT 커넥터는 자체 호스팅 및 사용자 지정 DNS/URL 버전을 포함하여 다음 공급자를 지원합니다.

- GitHub 및 GitHub Enterprise Server
- GitLab.com 및 GitLab 자체 관리형
- Bitbucket Cloud 및 Bitbucket 데이터 센터
- Azure DevOps 및 Azure DevOps Server

개인 액세스 토큰 생성

소스 코드 공급자에서 PAT를 생성합니다. 필요한 권한은 공급자마다 다릅니다. 공급자의 탭을 선택합니다.

Important

생성 직후 토큰을 복사합니다. 다시 볼 수 없습니다. 변환 작업 기간 만료를 설정합니다. 만료를 만료되지 않도록 설정하지 마십시오.

Warning

PAT 토큰을 코드 리포지토리에 커밋하거나 안전하지 않은 채널을 통해 공유하지 마십시오. 항상 상에 저장합니다 AWS Secrets Manager.

GitHub

설정, 개발자 설정, 개인 액세스 토큰, 세분화된 토큰으로 이동합니다. 변환할 리포지토리를 선택하고 다음 권한을 부여합니다.

리포지토리 권한

권한	액세스	용도
내용	읽기 및 쓰기	소스 코드를 읽고 변환된 코드를 리포지토리에 다시 씁니다.

권한	액세스	용도
Metadata	읽기 전용	기본 리포지토리 정보에 액세스합니다.

조직 권한(조직 리포지토리에 필요)

권한	액세스	용도
Members	읽기 전용	리포지토리 검색을 위해 토큰에 액세스할 수 있는 조직을 나열합니다.

GitLab

프로필 편집, 토큰 액세스로 이동합니다. 다음 범위를 선택합니다.

Scope	용도
read_api	리포지토리 메타데이터, 프로젝트 정보, 사용자 세부 정보를 읽고 그룹 및 브랜치를 나열합니다.
read_repository	분석을 위해 소스 코드 파일 및 리포지토리 구조를 읽습니다.
write_repository	변환된 코드를 리포지토리에 다시 씁니다.

Bitbucket

계정 설정, 보안, API 토큰 생성 및 관리로 이동합니다. 필요한 범위는 토큰 유형에 따라 다릅니다.

Workspace/리포지토리 토큰(ATCT — 베어러 인증, 사용자 이름 필요 없음)

권한	액세스	용도
리포지토리	읽기 및 쓰기	git 푸시를 통해 리포지토리를 나열하고, 브랜치를 읽고, 변환된 코드를 씁니다.

계정 API 토큰(ATAT - 이메일이 포함된 기본 인증) 또는 앱 암호(ATBB - 사용자 이름이 포함된 기본 인증)

Scope	용도
read:account	인증된 사용자를 식별하여 리포지토리 멤버십 확인
read:workspace:bitbucket	AWS 변환이 리포지토리를 열거할 수 있도록 토큰이 액세스할 수 있는 워크스페이스를 나열합니다. 보안 암호에 워크스페이스 목록을 지정하는 경우 필요하지 않습니다.
read:repository:bitbucket	리포지토리를 나열하고 메타데이터 및 브랜치 정보를 읽습니다.
write:repository:bitbucket	git 푸시를 통해 변환된 코드를 리포지토리에 다시 씁니다.

Azure DevOps

사용자 설정, 개인 액세스 토큰으로 이동합니다. 사용자 지정 정의 범위를 선택합니다. 조직 범위에서 액세스 가능한 모든 조직(권장)을 선택하거나 단일 조직을 지정합니다.

Scope	액세스	용도
코드	읽기 및 쓰기	소스 코드를 읽고, 리포지토리 및 브랜치를 나열하고, 변환된 코드를 다시 작성합니다.
사용자 프로필	읽기	토큰 액세스를 검증하고 조직 조회를 위한 사용자 자격 증명을 검색합니다.
멤버 권한 관리	읽기	리포지토리 검색을 위해 토큰에 액세스할 수 있는 조직을 나열합니다.

에 PAT 저장 AWS Secrets Manager

1. AWS Secrets Manager 콘솔을 엽니다.
2. 새 보안 암호 저장을 선택합니다.

3. 보안 암호 유형에서 다른 유형의 보안 암호를 선택합니다.
4. 공급자 및 호스팅 유형에 따라 키-값 페어를 추가합니다.
 - 클라우드 호스팅 공급자 - PAT를 값으로 token 사용하여 라는 키를 추가합니다.
 - 특정 조직이 있는 Azure DevOps의 경우 조직 이름과 organization 함께 라는 이름의 키도 추가합니다.
 - Bitbucket 앱 암호(ATBB)의 경우 Bitbucket 사용자 이름과 username 함께 라는 키도 추가합니다. Bitbucket 계정 API 토큰(ATAT)의 경우 email Bitbucket 이메일 주소로 라는 키를 추가합니다.
 - 자체 호스팅 및 사용자 지정 DNS/URL 공급자 - host (서버 URL, 예: https://github.mycompany.com), provider_type (github, gitlabbitbucket, 또는 ado) 및 token (PAT) 키를 추가합니다.
 - 특정 조직이 있는 Azure DevOps의 경우 조직 이름과 organization 함께 라는 이름의 키도 추가합니다.
 - Bitbucket 앱 암호(ATBB)의 경우 Bitbucket 사용자 이름과 username 함께 라는 키도 추가합니다. Bitbucket 계정 API 토큰(ATAT)의 경우 email Bitbucket 이메일 주소로 라는 키를 추가합니다.

다음 예제는 보안 암호가 GitHub 클라우드 호스팅 공급자를 AWS Secrets Manager 찾는 방법을 보여줍니다.

```
{
  "token": "your-github-personal-access-token"
}
```

다음 예제에서는 Bitbucket 앱 암호(ATBB)를 보여줍니다.

```
{
  "token": "your-bitbucket-app-password",
  "username": "my-bitbucket-username"
}
```

다음 예제는 자체 호스팅 GitLab 인스턴스를 보여줍니다.

```
{
  "host": "https://gitlab.mycompany.com",
  "provider_type": "gitlab",
  "token": "your-gitlab-personal-access-token"
}
```

}

5. 다음을 선택합니다.
6. 와 같은 보안 암호 이름을 입력합니다 `github-pat-myproject`.
7. (선택 사항) 암호화를 위한 고객 관리형 KMS 키를 선택합니다.
8. 마법사를 완료하고 저장을 선택합니다.
9. 보안 암호 ARN을 복사합니다. AWS 변환 작업을 구성할 때 이 값이 필요합니다.

고객 관리형 KMS 키를 사용하여 보안 암호를 암호화하는 경우(기본 AWS 관리형 키 대신) AWS 변환이 보안 암호를 해독하도록 KMS 키 정책을 업데이트해야 합니다. 고객 관리형 KMS 키 정책에 다음 문을 추가합니다.

```
{
  "Sid": "Allow AWS Transform to decrypt secrets",
  "Effect": "Allow",
  "Principal": {
    "Service": "transform.amazonaws.com"
  },
  "Action": [
    "kms:Decrypt",
    "kms:DescribeKey"
  ],
  "Resource": "*",
  "Condition": {
    "StringEquals": {
      "kms:ViaService": "secretsmanager.REGION.amazonaws.com",
      "kms:EncryptionContext:SecretARN": "YOUR-SECRET-ARN"
    }
  }
}
```

*REGION*을 AWS 리전(예: `us-east-1`)으로 바꾸고 *YOUR-SECRET-ARN*을 보안 암호의 ARN으로 바꿉니다. `kms:ViaService` 조건은 KMS 키를 AWS Secrets Manager 서비스를 통해서만 사용할 수 있도록 합니다. `kms:EncryptionContext:SecretARN` 조건은 복호화를 특정 보안 암호로 제한합니다.

KMS 키 정책을 업데이트하려면:

1. 에서 AWS KMS 콘솔을 엽니다 <https://console.aws.amazon.com/kms>.
2. 탐색 창에서 고객 관리형 키를 선택합니다.

3. KMS 키를 선택합니다.
4. 키 정책 탭에서 편집을 선택합니다.
5. 기존 정책에 정책 설명을 추가합니다.
6. 변경 사항 저장을 선택합니다.

 Note

기본 AWS관리형 키(aws/secretsmanager)를 사용하는 경우 KMS 키 정책을 수정할 필요가 없습니다.

AWS 변환 작업 구성

1. AWS 변환 작업에서 리소스에 연결로 이동합니다.
2. 소스 코드 리포지토리 연결을 선택합니다.
3. 인증 방법으로 PAT 커넥터를 선택합니다.
4. 2단계의 보안 암호 ARN을 입력합니다.
5. (선택 사항) 고객 관리형 KMS 키를 사용한 경우 KMS 키 ARN을 입력합니다.
6. 리포지토리와 브랜치를 선택합니다.
7. 계속을 선택합니다.

AWS 변환은 보안 암호에 액세스하는 데 필요한 권한이 있는 IAM 역할을 자동으로 생성합니다.

토큰 교체 및 유지 관리

PAT 토큰이 만료되기 전에 교체하는 것은 사용자의 책임입니다. 토큰을 교체하려면:

1. 소스 코드 공급자에서 동일한 권한을 가진 새 PAT를 생성합니다.
2. 에서 보안 암호 값을 업데이트합니다 AWS Secrets Manager.
3. AWS 변환 작업이 새 토큰을 사용하여 리포지토리에 액세스할 수 있는지 확인합니다.
4. 소스 코드 공급자에서 이전 PAT를 취소합니다.

PAT 커넥터 문제 해결

액세스 거부됨 - 잘못된 PAT

PAT가 만료되지 않았는지 확인합니다. PAT에 공급자에 필요한 범위가 있는지 확인합니다. PAT가 올바르게 저장되어 있는지 확인합니다 AWS Secrets Manager.

보안 암호를 검색할 수 없음

보안 암호 ARN이 올바른지 확인합니다. 작업 로그를 확인하여 AWS 변환이 IAM 역할을 생성했는지 확인합니다. 고객 관리형 KMS 키를 사용하는 경우 키 정책을 확인합니다.

권한 부족

PAT에는 작업에 필요한 범위가 부족할 수 있습니다. 필요한 범위로 PAT를 재생성하고 보안 암호 값을 업데이트합니다 AWS Secrets Manager.

Set up AWS CodeConnections

AWS CodeConnections는 OAuth 2.0 권한 부여 흐름을 통해 임시 OAuth 자격 증명을 자동으로 검색하는 관리형 공급자 통합을 사용합니다. 권한은 공급자 앱에서 구성되며 전적으로에서 관리합니다 AWS. 앱을 한 번 승인하면가 모든 자격 증명 관리를 AWS 처리합니다.

1. SQL Server 현대화 작업에서 리소스에 연결로 이동합니다.
2. 소스 코드 리포지토리 연결을 선택합니다.
3. 기존 연결이 없는 경우 연결 생성을 선택합니다.
4. 리포지토리 공급자를 선택합니다.
 - GitHub/GitHub Enterprise
 - GitLab.com
 - Bitbucket Cloud
 - Azure 리포지토리
5. 공급자의 권한 부여 흐름을 따릅니다.
6. 권한 부여 후 연결을 선택합니다.

리포지토리 및 브랜치 선택

1. 목록에서 리포지토리를 선택합니다.

2. 변환하려는 브랜치(일반적으로 기본, 마스터 또는 개발)를 선택합니다.
3. (선택 사항) .NET 애플리케이션이 리포지토리 루트에 없는 경우 하위 디렉터리를 지정합니다.
4. 계속을 선택합니다.

Note

AWS 변환은 변환된 코드에 대한 새 브랜치를 생성합니다. 일반 코드 검토 프로세스를 통해 변경 사항을 검토하고 병합할 수 있습니다.

리포지토리 액세스 승인

GitHub 및 기타 플랫폼의 경우 리포지토리 관리자가 연결 요청을 승인해야 합니다.

1. AWS 변환에 확인 링크가 표시됩니다.
2. 이 링크를 리포지토리 관리자와 공유합니다.
3. 관리자는 리포지토리 설정에서 요청을 검토하고 승인합니다.
4. 관리자가 요청을 승인하면 연결 상태가 승인됨으로 변경됩니다.

Important

승인 프로세스는 조직의 정책에 따라 시간이 걸릴 수 있습니다. 이에 따라 적절한 계획을 수립해야 합니다.

4단계: 배포 커넥터 생성(선택 사항)

변환된 애플리케이션을 AWS 계정에 배포하려면 배포 커넥터를 선택할 수 있습니다.

배포 커넥터 설정

1. 애플리케이션을 배포하려면 예를 선택합니다. 아니요를 선택하면이 단계를 건너뜁니다.
2. 변환된 애플리케이션을 배포할 AWS 계정을 추가합니다.
3. 커넥터를 쉽게 기억하는 데 도움이 되는 이름 추가
4. 승인을 위해 커넥터 요청을 제출합니다.

배포 커넥터 승인

AWS 계정 관리자는 배포 커넥터에 대한 연결 요청을 승인해야 합니다.

1. AWS 변환에 확인 링크 표시
2. AWS 계정 관리자와 이 링크 공유
3. 관리자가 리포지토리 설정에서 요청을 검토하고 승인합니다.
4. 승인되면 연결 상태가 승인됨으로 변경됩니다.

Important

승인 프로세스는 조직의 정책에 따라 시간이 걸릴 수 있습니다. 이에 따라 적절한 계획을 수립해야 합니다.

5단계: 리소스 확인

데이터베이스 및 리포지토리에 연결한 후 AWS 변환은 필요한 모든 리소스에 액세스할 수 있고 변환할 준비가 되었는지 확인합니다.

AWS 변환이 확인하는 내용

- 데이터베이스 연결: 연결이 활성 상태이고, 사용자에게 필요한 권한이 있으며, 데이터베이스에 액세스할 수 있고, 버전이 지원됩니다.
- 리포지토리 액세스: 리포지토리에 액세스할 수 있음, 브랜치 존재, .NET 프로젝트 파일 감지됨, 데이터베이스 연결 검색 가능
- 환경 준비: VPC 구성에서 DMS 지원, 필수 AWS 서비스 역할 존재, 네트워크 연결 설정, 리전 호환성 확인

비행 전 체크리스트 검토

1. 작업 계획에서 리소스 확인으로 이동합니다.
2. 체크리스트 항목을 검토합니다.
 - # 데이터베이스 연결 확인됨
 - # 리포지토리 액세스 확인됨
 - # .NET 버전 지원

- # Entity Framework 또는 ADO.NET 감지됨
- # 네트워크 구성이 유효함
- # 부여된 필수 권한

3. 모든 항목이 완료로 표시되면 계속을 선택합니다.

4. 경고 또는 오류가 표시되는 항목이 있는 경우 계속하기 전에 해결합니다.

6단계: 검색 및 평가

AWS 변환은 SQL Server 데이터베이스와 .NET 애플리케이션을 분석하여 현대화의 범위와 복잡성을 이해합니다.

검색되는 내용

- 데이터베이스 객체: 테이블, 뷰, 인덱스, 저장 프로시저, 함수, 트리거, 제약 조건, 데이터 유형, 계산된 열, 자격 증명 열, 외래 키 관계
- 애플리케이션 코드: .NET 프로젝트 구조, Entity Framework 모델 및 구성, ADO.NET 데이터 액세스 코드, 데이터베이스 연결 문자열, 저장 프로시저 호출, 코드 내 SQL 쿼리
- 종속성: 어떤 애플리케이션이 어떤 데이터베이스, 데이터베이스 간 종속성, 공유된 저장 프로시저, 공통 데이터 액세스 패턴을 사용하는지

검색 프로세스

- AWS 리소스 확인 후 변환이 자동으로 검색 시작
- 데이터베이스 크기 및 애플리케이션 복잡성에 따라 일반적으로 검색에 5~15분이 소요됩니다.
- 작업 로그의 진행 상황 모니터링
- AWS 변환은 객체가 검색될 때 실시간 업데이트를 표시합니다.

검색 결과 검토

검색이 완료되면 검색 및 평가로 이동하여 다음을 검토합니다.

데이터베이스 분석:

- 객체 수: 테이블, 뷰, 저장 프로시저, 함수, 트리거 수
- 복잡성 점수: 변환 복잡성 평가(낮음, 중간, 높음)

- 작업 항목: 사람의 주의를 필요할 수 있는 객체
- 지원되는 기능: 자동으로 변환되는 데이터베이스 기능
- 지원되지 않는 기능: 해결 방법이 필요한 기능

애플리케이션 분석:

- 프로젝트 유형: ASP.NET Core, 콘솔 앱, 클래스 라이브러리 등
- .NET 버전: Detected .NET Core 버전
- 데이터 액세스 프레임워크: Entity Framework 버전 또는 ADO.NET
- 데이터베이스 연결: 발견된 연결 문자열 수
- 코드 복잡성: 변환 복잡성 평가

종속성 맵:

- application-to-database 관계의 시각적 표현
- 데이터베이스 간 종속성
- 공유 구성 요소

복잡성 평가 이해

AWS 변환은 현대화를 세 가지 범주로 분류합니다.

복잡성	특성	예상 결과
낮음(클래스 A)	표준 SQL 패턴(ANSI SQL), 간단한 저장 프로시저, 기본 데이터 형식, 표준 구성을 사용하는 Entity Framework	최소한의 인적 개입 예상, 높은 자동화 성공률
중간(클래스 B)	고급 T-SQL 패턴, 비즈니스 로직을 사용한 복잡한 저장 프로시저, 사용자 정의 함수, 계산된 열	사람의 개입이 일부 필요, 전문가 검토 권장
높음(클래스 C)	CLR 어셈블리, 연결된 서버, 서비스 브로커, 복잡한 전체 텍스트 검색	상당한 인적 리팩터링 필요, 단계별 접근 방식 고려

평가 보고서

AWS 변환은 다음을 포함하는 세부 평가 보고서를 생성합니다.

- 개략적인 개요가 포함된 실행 요약
- 전체 데이터베이스 인벤토리
- 애플리케이션 인벤토리
- 변환 준비 백분율
- 노력 추정
- 위험 평가 및 완화 전략
- 권장 접근 방식

오프라인 검토 및 이해관계자와의 공유를 위해 평가 보고서를 다운로드할 수 있습니다.

7단계: 웨이브 플랜 생성 및 검토

여러 데이터베이스 및 애플리케이션이 있는 대규모 자산의 경우 AWS 변환은 논리적 그룹에서 현대화를 시퀀스화하는 웨이브 플랜을 생성합니다.

웨이브 플랜이란 무엇입니까?

웨이브 플랜은 다음을 기반으로 현대화를 단계(웨이브)로 구성합니다.

- 데이터베이스와 애플리케이션 간의 종속성
- 비즈니스 우선순위
- 위험 허용치
- 리소스 가용성
- 기술적 복잡성

각 웨이브에는 종속성을 손상시키지 않고 함께 현대화할 수 있는 데이터베이스 및 애플리케이션 그룹이 포함되어 있습니다.

웨이브 플랜 검토

1. 작업 계획에서 웨이브 계획으로 이동합니다.
2. 제안된 웨이브 검토

3. 각 웨이브에 대해 다음을 검토합니다.

- 포함된 데이터베이스
- 포함된 애플리케이션
- 다른 웨이브에 대한 종속성
- 예상 변환 시간
- 복잡성 수준
- 배포 가능한 애플리케이션

웨이브 플랜 사용자 지정

다음 두 가지 방법으로 비즈니스 요구 사항에 맞게 웨이브 플랜을 사용자 지정할 수 있습니다.

JSON 사용:

1. 모든 웨이브 다운로드를 선택하여 모든 웨이브가 포함된 JSON 파일을 가져옵니다.
2. 다음과 같이 JSON의 웨이브를 수정합니다.
 - 파도 간 데이터베이스 이동
 - 파도를 더 작은 그룹으로 분할
 - 웨이브를 함께 병합
 - 웨이브 시퀀스 변경
 - 범위에서 데이터베이스 추가 또는 제거
3. 웨이브 플랜 업로드를 선택하여 JSON 파일을 콘솔에 다시 업로드합니다.
4. AWS 변환은 변경 사항을 검증하고 종속성이 위반되면 경고합니다.
5. 웨이브 확인을 선택하여 웨이브 플랜을 업데이트합니다.

채팅 사용:

에이전트와 채팅하고 리포지토리와 데이터베이스를 특정 웨이브로 이동하도록 요청하여 웨이브 계획을 수정할 수 있습니다. 이 접근 방식은 웨이브를 약간 편집해야 하는 경우에 적합합니다.

Important

웨이브를 사용자 지정할 때 종속성이 준수되는지 확인합니다. 데이터베이스 이전에 종속 애플리케이션을 변환하면 문제가 발생할 수 있습니다.

단일 데이터베이스 현대화

단일 데이터베이스 및 애플리케이션을 현대화하는 경우 AWS 변환은 하나의 웨이브로 간단한 계획을 생성합니다. 웨이브 계획 없이 직접 변환을 진행할 수 있습니다.

웨이브 플랜 승인

1. 검토 및 사용자 지정(필요한 경우) 후 웨이브 계획 승인을 선택합니다.
2. AWS 변환은 웨이브 계획을 잠그고 변환을 진행합니다.
3. 웨이브 계획 편집을 선택하여 나중에 계획을 수정할 수 있습니다.

8단계: 스키마 변환

AWS 변환은 테이블, 뷰, 저장 프로시저, 함수 및 트리거를 포함하여 SQL Server 데이터베이스 스키마를 Aurora PostgreSQL로 변환합니다.

스키마 변환 작동 방식

AWS 변환은 생성형 AI로 향상된 AWS DMS Schema Conversion을 사용하여 다음을 수행합니다.

- SQL Server 스키마 및 관계 분석
- SQL Server에서 PostgreSQL로 데이터 형식 매핑
- T-SQL을 PL/pgSQL로 변환
- 자격 증명 열, 계산된 열 및 제약 조건 처리
- 변환 및 참조 무결성 검증
- 인적 검토가 필요한 객체에 대한 작업 항목 생성

지원되는 변환

자동으로 변환됨:

- 테이블, 뷰 및 인덱스
- 기본 키 및 외래 키
- 제약 조건 및 기본값 확인
- 가장 일반적인 데이터 형식
- 간단한 저장 프로시저
- 기본 함수 및 트리거

- 자격 증명 열(직렬 또는 생성형으로 변환됨)
- 대부분의 계산된 열

인적 검토가 필요할 수 있습니다.

- 고급 T-SQL을 사용한 복잡한 저장 프로시저
- SQL Server 관련 함수(GETUTCDATE, SUSER_NAME 등)
- 복잡한 표현식이 있는 컴퓨팅된 열
- 전체 텍스트 검색 인덱스
- XML 데이터 형식 작업
- HIERARCHYID 데이터 형식(Itree 확장 필요)

자동으로 변환되지 않음:

- CLR 어셈블리
- 연결된 서버
- 서비스 브로커
- SQL Server 에이전트 작업

스키마 변환 시작

1. 작업 계획에서 스키마 변환으로 이동합니다.
2. 변환 설정을 검토합니다.
 - 대상 PostgreSQL 버전
 - 확장 옵션(Itree, PostGIS 등)
 - 이름 지정 규칙
3. 변환 시작을 선택합니다.
4. 작업 로그의 진행 상황 모니터링
5. 변환은 일반적으로 데이터베이스 객체 수에 따라 10~30분이 걸립니다.

변환 결과 검토

변환이 완료되면 스키마 변환 검토로 이동합니다.

변환 요약:

- 변환된 객체: 성공적으로 변환된 객체 수
- 작업 항목: 사람의 주의가 필요한 객체
- 경고: 검토할 잠재적 문제
- 오류: 변환할 수 없는 객체

객체 유형별 검토:

- 테이블: 데이터 형식 매핑, 제약 조건, 인덱스
- 저장 프로시저: T-SQL에서 PL/pgSQL로의 변환
- 함수: 함수 서명 및 로직 변경
- 트리거: 트리거 구문 및 타이밍 변경

작업 항목 검토

1. 작업 항목 보기를 선택합니다.
2. 각 작업 항목에 대해 다음을 검토합니다.
 - 객체 이름: 데이터베이스 객체
 - 문제 유형: 주의가 필요한 항목
 - 심각도: 심각, 경고 또는 정보
 - 권장 사항: 권장 해상도
 - 원본 코드: SQL Server 버전
 - 변환된 코드: PostgreSQL 버전
3. 각 작업 항목에 대해 다음을 수행할 수 있습니다.
 - 수락: 변환된 코드 사용
 - 수정: 변환된 코드 편집
 - 나중을 위한 플래그: 변환 후 인적 검토를 위해 표시

예: 저장 프로시저 변환

SQL Server T-SQL:

```
CREATE PROCEDURE GetProductsByCategory
```



```

    @CategoryId INT,
    @PageSize INT = 10
AS
BEGIN
    SET NOCOUNT ON;

    SELECT TOP (@PageSize)
        ProductId,
        Name,
        Price,
        DATEDIFF(DAY, CreatedDate, GETUTCDATE()) AS DaysOld
    FROM Products
    WHERE CategoryId = @CategoryId
    ORDER BY Name
END

```

변환된 PostgreSQL PL/pgSQL:

```

CREATE OR REPLACE FUNCTION get_products_by_category(
    p_category_id INTEGER,
    p_page_size INTEGER DEFAULT 10
)
RETURNS TABLE (
    product_id INTEGER,
    name VARCHAR(255),
    price NUMERIC(18,2),
    days_old INTEGER
) AS $$
BEGIN
    RETURN QUERY
    SELECT
        p.product_id,
        p.name,
        p.price,
        EXTRACT(DAY FROM (NOW() - p.created_date))::INTEGER AS days_old
    FROM products p
    WHERE p.category_id = p_category_id
    ORDER BY p.name
    LIMIT p_page_size;
END;
$$ LANGUAGE plpgsql;

```

변경 사항:

- TABLE을 반환하는 함수로 변환된 프로시저
- p_ 접두사가 붙은 파라미터 이름
- TOP을 LIMIT으로 변환
- EXTRACT로 변환된 DATEDIFF
- GETUTCDATE()를 NOW()로 변환
- 열 이름을 소문자로 변환(PostgreSQL 규칙)

스키마 변환 승인

1. 모든 작업 항목을 검토하고 필요한 수정을 수행한 후
2. 스키마 변환 승인 선택
3. AWS 변환은 Aurora PostgreSQL에 배포할 변환된 스키마를 준비합니다.

Note

오프라인 검토 또는 버전 관리를 위해 변환된 스키마를 SQL 스크립트로 다운로드할 수 있습니다.

9단계: 데이터 마이그레이션(선택 사항)

AWS 변환은 SQL Server에서 Aurora PostgreSQL로 데이터를 마이그레이션하는 옵션을 제공합니다. 데이터 마이그레이션은 선택 사항이며 스키마 및 코드 변환만 필요한 경우 건너뛸 수 있습니다.

데이터 마이그레이션 옵션

옵션 1: 프로덕션 데이터 마이그레이션

AWS DMS를 사용하여 실제 프로덕션 데이터를 마이그레이션합니다.

- 모든 데이터의 전체 초기 로드
- 테스트 중 지속적 복제(CDC)
- 가동 중지 시간 전환 최소화
- 데이터 검증 및 무결성 검사

옵션 2: 데이터 마이그레이션 건너뛰기

스키마 및 코드만 변환:

- 개발/테스트 환경에 유용
- 데이터가 별도로 마이그레이션되는 경우
- proof-of-concept 프로젝트의 경우

데이터 마이그레이션 구성

1. 작업 계획에서 데이터 마이그레이션으로 이동합니다.
2. 마이그레이션 옵션을 선택합니다.
 - 프로덕션 데이터 마이그레이션
 - 데이터 마이그레이션 건너뛰기
3. 프로덕션 데이터를 마이그레이션하는 경우 다음을 구성합니다.
 - 마이그레이션 유형: 전체 로드 또는 전체 로드 + CDC
 - 검증: 데이터 검증 활성화
 - 성능: DMS 인스턴스 크기
 - >마이그레이션 시작을 선택합니다.

프로덕션 데이터 마이그레이션 프로세스

프로덕션 데이터를 마이그레이션하도록 선택한 경우:

1. 초기 동기화: AWS DMS는 모든 테이블의 전체 로드를 수행합니다.
2. 연속 복제: (CDC가 활성화된 경우) 데이터 동기화 유지
3. 검증: 행 수 및 데이터 무결성 확인
4. 전환 준비: 최종 동기화 준비

마이그레이션 타임라인:

- 소규모 데이터베이스(< 10GB): 30분~2시간
- 중간 데이터베이스(10~100GB): 2~8시간
- 대규모 데이터베이스(> 100GB): 8시간 이상

데이터 유효성 검사

AWS 변환은 다음 검사를 통해 마이그레이션된 데이터를 검증합니다.

- 행 수 비교(소스 대 대상)
- 기본 키 무결성
- 외래 키 관계
- 데이터 형식 호환성
- 계산된 열 결과
- Null 값 처리

10단계: 애플리케이션 코드 변환

AWS 변환은 SQL Server 대신 Aurora PostgreSQL에서 작동하도록 .NET 애플리케이션 코드를 변환합니다. 변환된 소스 코드를 커밋하기 위해 리포지토리에서 대상 브랜치 이름을 요청합니다. 브랜치 이름을 입력하면 AWS 변환은 새 브랜치를 생성하고 PostgreSQL 데이터베이스와 일치하도록 변환을 시작합니다.

변환되는 항목

개체 프레임워크 변경 사항:

- 데이터베이스 공급자: UseSqlServer() → UseNpgsql()
- 연결 문자열: SQL Server 형식 → PostgreSQL 형식
- 데이터 형식 매핑: SQL Server 형식 → PostgreSQL 형식
- DbContext 구성: SQL Server별 → PostgreSQL별
- 마이그레이션 파일: PostgreSQL 호환성을 위해 업데이트됨

ADO.NET 변경 사항:

- 연결 클래스: SqlConnection → NpgsqlConnection
- 명령 클래스: SqlCommand → NpgsqlCommand
- 데이터 리더: SqlDataReader → NpgsqlDataReader
- 파라미터: SqlParameter → NpgsqlParameter
- SQL 구문: T-SQL → PostgreSQL SQL

구성 변경:

- appsettings.json의 연결 문자열
- 데이터베이스 공급자 NuGet 패키지
- 종속성 주입 구성
- 시작/Program.cs 구성

코드 변환 시작

1. 작업 계획에서 애플리케이션 변환으로 이동합니다.
2. 변환 설정을 검토합니다.
 - 대상 .NET 버전(업그레이드하는 경우)
 - PostgreSQL 공급자 버전
 - 코드 스타일 기본 설정
3. 변환 시작을 선택합니다.
4. 작업 로그의 진행 상황 모니터링
5. 변환은 일반적으로 코드베이스 크기에 따라 15~45분이 걸립니다.

11단계: 변환 결과 검토

배포를 진행하기 전에 전체 변환 결과를 검토하여 모든 것을 테스트할 준비가 되었는지 확인합니다.

다음은 위해 리포지토리 브랜치에서 변환된 코드를 다운로드할 수 있습니다.

- 로컬 테스트 및 검증
- IDE의 코드 검토
- CI/CD 파이프라인과 통합
- 버전 제어 커밋

변환 요약을 다운로드하여 변환의 일부로 AWS 변환에서 수행한 자연어 변경 사항을 검토할 수도 있습니다.

변환 요약

1. 작업 계획의 변환 요약으로 이동합니다.

2. 전체 결과를 검토합니다.

- 스키마 변환: 변환된 객체, 작업 항목, 경고
- 데이터 마이그레이션: 마이그레이션된 테이블, 전송된 행, 검증 상태
- 코드 변환: 파일 변경, 줄 수정, 문제 해결
- 준비 점수: 전체 배포 준비 상태

변환 보고서 생성

AWS 변환은 포괄적인 변환 보고서를 생성합니다.

1. 보고서 생성을 선택합니다.

2. 보고서 유형 선택:

- 개요: 이해관계자를 위한 개략적인 개요
- 기술 세부 정보: 전체 변환 설명서
- 작업 항목: 필요한 인적 작업 목록

3. 보고서 다운로드를 선택합니다.

보고서에는 다음이 포함됩니다.

- 변환 범위 및 목표
- 변환된 객체 및 코드
- 발생한 문제 및 해결 방법
- 검증 결과
- 배포 준비 상태 평가
- 테스트 권장 사항

12단계: 검증 및 테스트

프로덕션에 배포하기 전에 변환된 애플리케이션이 Aurora PostgreSQL에서 올바르게 작동하는지 확인합니다.

검증 유형

자동 검증: AWS 변환은 자동 검사를 수행합니다.

- 소스 데이터베이스에 대한 스키마 검증
- 데이터 무결성 확인
- 쿼리 동등성 테스트
- 연결 문자열 검증
- 구성 검증

인적 검증: 추가 테스트를 수행해야 합니다.

- 애플리케이션 기능의 기능 테스트
- 다른 시스템과의 통합 테스트
- 성능 테스트 및 벤치마킹
- 사용자 승인 테스트
- 보안 테스트

자동 검증 실행

1. 작업 계획의 검증으로 이동합니다.
2. 검증 실행을 선택합니다.
3. AWS 변환은 검증 테스트를 실행합니다.
 - 데이터베이스 연결
 - 스키마 호환성
 - 데이터 무결성
 - 애플리케이션 빌드
 - 기본 기능
4. 검증 결과 검토:
 - 통과: 성공한 테스트
 - 실패: 주의가 필요한 테스트
 - 경고: 검토할 잠재적 문제

테스트 체크리스트

데이터베이스 기능:

- 모든 테이블 액세스 가능
- 저장된 프로시저가 올바르게 실행됨
- 함수는 예상 결과를 반환합니다.
- 적절하게 발사를 트리거합니다.
- 제약 조건이 올바르게 적용됨
- 인덱스는 쿼리 성능을 개선합니다.

애플리케이션 기능:

- 애플리케이션이 성공적으로 시작됨
- 데이터베이스 연결 설정됨
- CRUD 작업이 올바르게 작동함
- 저장 프로시저 호출 성공
- 트랜잭션 커밋/롤백이 올바르게 수행됨
- 오류 처리는 예상대로 작동합니다.

데이터 무결성:

- 행 수가 소스와 일치
- 고유 기본 키
- 유효한 외래 키
- 계산된 열이 올바름
- 적절한 Null 처리
- 데이터 형식 호환

성능:

- 쿼리 응답 시간 허용 가능
- 연결 풀링 구성됨
- 인덱스 최적화
- N+1 쿼리 문제 없음
- 배치 작업 효율성

- 리소스 사용 합리적

13단계: 배포

검증에 성공하면 현대화된 애플리케이션과 데이터베이스를 프로덕션에 배포합니다.

배포 옵션

- Amazon ECS 및 Amazon EC2 Linux

배포 전 체크리스트

프로덕션에 배포하기 전에:

- 모든 검증 테스트 통과
- 성능 테스트 완료
- 보안 검토 완료
- 백업 및 롤백 계획 문서화
- 모니터링 및 알림 구성됨
- 새 환경에 대해 훈련된 팀
- 배포에 대한 정보를 제공받은 이해관계자
- 예약된 유지 관리 기간

Amazon EKS에 배포

1. 작업 계획의 배포로 이동합니다.
2. ECS에 배포를 선택합니다.
3. 배포 설정 구성:
 - 클러스터: ECS 클러스터 선택 또는 생성
 - 서비스: ECS 서비스 구성
 - 작업 정의: 생성된 작업 정의 검토
 - 로드 밸런서: ALB/NLB 구성
 - Auto Scaling: 조정 정책 설정
4. infrastructure-as-code(CloudFormation 템플릿 또는 AWS CDK 코드) 검토

5. 배포 선택

배포 모니터링

AWS 변환은 애플리케이션을 배포합니다.

1. Aurora PostgreSQL 클러스터를 생성합니다.
2. 데이터베이스 스키마 적용
3. 데이터 로드(해당하는 경우)
4. 애플리케이션 컨테이너를 배포합니다.
5. 로드 밸런서를 구성합니다.
6. Auto Scaling 설정

배포 진행 상황을 모니터링하고 다음을 확인합니다.

- 인프라 프로비저닝
- 데이터베이스 초기화
- 애플리케이션 배포
- 상태 확인 통과
- 애플리케이션 액세스 가능
- 데이터베이스 연결 작동
- 정상 작업을 보여주는 로그

배포 후 검증

배포 후:

연기 테스트:

- 중요한 기능 확인
- 키 사용자 워크플로 테스트
- 통합 지점 확인
- 오류율 모니터링

성능 모니터링:

- 응답 시간 추적
- 데이터베이스 쿼리 모니터링
- 리소스 사용률 확인
- 애플리케이션 로그 검토

사용자 검증:

- 사용자 수락 테스트 수행
- 피드백 수집
- 모든 문제 해결
- 학습한 교훈 문서화

롤백 절차

배포 후 문제가 발생하는 경우:

즉시 롤백:

- 이전 애플리케이션 버전으로 되돌리기
- SQL Server로 다시 전환(아직 사용할 수 있는 경우)
- 필요한 경우 백업에서 복원

부분 롤백:

- 특정 구성 요소 롤백
- 데이터베이스 변경 사항 유지
- 애플리케이션 코드만 되돌리기

수정 사항 전달:

- Aurora PostgreSQL 버전에 핫픽스 적용
- 업데이트된 애플리케이션 코드 배포
- 해상도 모니터링

⚠ Important

필요한 경우 롤백을 활성화하려면 전환 후 일정 기간 동안 SQL Server 데이터베이스를 사용할 수 있도록 유지합니다.

배포 후 최적화

배포 성공 후:

성능 튜닝:

- 느린 쿼리 최적화
- 연결 풀 설정 조정
- Aurora PostgreSQL 파라미터 미세 조정
- 인덱스 검토 및 최적화

비용 최적화:

- 적절한 크기의 Aurora 인스턴스
- Auto Scaling을 적절하게 구성
- 스토리지 설정 검토
- 백업 보존 최적화

모니터링 설정:

- CloudWatch 대시보드 구성
- 알림 설정
- 고급 모니터링 활성화
- 성능 개선 도우미 구성

설명서:

- 런북 업데이트
- 아키텍처 변경 사항 문서화
- 운영 팀 교육

- 문제 해결 가이드 생성

변환 후 테스트 및 배포

변환된 애플리케이션을 랜딩 존에 배포하고 애플리케이션과 변환된 데이터베이스 간의 연결을 검증하고 선택적으로 CI/CD 파이프라인을 설정합니다. 배포 자동화를 구현하는 데 도움이 되도록 샘플 CI/CD 파이프라인 구성이 참조로 생성됩니다. 이 마지막 단계에서는 전체 현대화를 검증합니다.

리소스 구성

IAM 역할, 인스턴스 프로파일 및 S3 버킷과 같이 배포에 사용되는 리소스를 구성해야 합니다. AWS 변환에는 S3 버킷을 생성하거나 IAM을 변경할 수 있는 권한이 없습니다. 이 작업은 새 역할을 생성할 권한이 있는 사용자가 수행해야 합니다. 일반적으로 계정 관리자입니다.

프로세스를 간소화하기 위해 자동으로 다음과 같은 설정 스크립트를 제공합니다.

- 필요한 CloudFormation 템플릿을 실행합니다.
- ECS 서비스 연결 역할을 생성합니다.
- 필요한 모든 IAM 리소스를 설정합니다.

Important

제공된 설정 스크립트를 있는 그대로 실행합니다. 배포 프로세스에 영향을 미칠 수 있으므로 템플릿 또는 스크립트에서 리소스 이름을 수정하지 마십시오.

Linux의 경우:

```
./setup.sh --region <YOUR-Region>
```

Windows의 경우:

```
./setup.ps1 -Region <YOUR-Region>
```

VPC에서 보안 그룹 확인

AWS 변환은 Aurora PostgreSQL 인스턴스와 동일한 서브넷 및 동일한 보안 그룹에 애플리케이션을 배포합니다.

애플리케이션이 Aurora 인스턴스에 연결되도록 하려면이 보안 그룹에 동일한 보안 그룹에 연결할 수 있는 아웃바운드 규칙과 동일한 보안 그룹에서 연결할 수 있는 인바운드 규칙이 있어야 합니다.

애플리케이션 선택 및 구성

AWS 변환 UI에는 배포할 수 있는 애플리케이션 목록이 표시됩니다. 애플리케이션을 선택하고 구성 및 커밋을 클릭하여 다음을 지정할 수 있는 구성 창을 엽니다.

- 애플리케이션의 대상 인프라: ECS 또는 EC2 인스턴스 중 하나를 선택합니다.
- 애플리케이션 또는 인스턴스 파라미터

구성 창을 완료하고 닫은 후 AWS 변환:

- 구성을 기반으로 배포 아티팩트를 생성합니다.
- 다음을 포함하여 이러한 아티팩트를 리포지토리에 커밋합니다.
 - 배포 스크립트
 - CloudFormation 템플릿
 - 샘플 CI/CD 파이프라인 구성(배포 자동화를 설정하기 위한 참조로 사용할 수 있음)

커밋이 완료되면 애플리케이션 상태가 구성됨 및 커밋됨으로 변경됩니다. 그런 다음 애플리케이션을 선택하고 오른쪽 상단의 배포 버튼을 사용하여 배포를 시작할 수 있습니다.

ECS 배포

대상 ECS가 있는 모든 애플리케이션은 계정에 생성된 새 ECS 클러스터에 배포됩니다. 각 애플리케이션은 자체 전용 컨테이너에 배포됩니다. 컨테이너당 여러 애플리케이션은 지원되지 않습니다. 필요한 CPU 및 메모리와 같은 각 애플리케이션에 대한 컨테이너 파라미터를 개별적으로 구성합니다.

EC2 배포

제안된 EC2 인스턴스 중 하나를 선택하고 인스턴스 유형과 같은 파라미터를 구성할 수 있습니다. 여러 애플리케이션을 동일한 EC2 인스턴스에 배포할 수 있습니다.

- 단일 인스턴스에 여러 애플리케이션을 배포하려면 구성 중에 이러한 각 애플리케이션에 대해 동일한 대상 EC2 인스턴스를 선택합니다.
- 동일한 인스턴스를 대상으로 선택한 모든 애플리케이션에는 해당 인스턴스에 배포되고 서로 다른 무작위 포트가 할당됩니다.

- 한 애플리케이션의 인스턴스 파라미터를 편집한 다음 동일한 인스턴스를 대상으로 하는 다른 애플리케이션을 편집하면 변경 사항이 해당 인스턴스에 배포된 모든 애플리케이션에 영향을 미칩니다.

배포 성공

배포에 성공하면 애플리케이션은 라이선스 비용 절감, 성능 향상, 클라우드 네이티브 확장성과 함께 Aurora PostgreSQL에서 실행됩니다. 명시적으로 중지되지 않는 한 작업은 열린 상태로 유지됩니다. 이렇게 하면 업데이트된 배포 파라미터를 사용하여 재배포할 수 있는 옵션을 사용할 수 있습니다.

모범 사례 및 문제 해결

현대화 프로세스 중 모범 사례, 일반적인 문제 및 해결 방법.

ECS 애플리케이션 로그

CloudWatch 로그

- 모든 ECS 컨테이너 로그는 CloudWatch Logs로 자동 전송됩니다.
- CloudWatch 콘솔의 로그 그룹 아래 액세스 로그
- 로그 그룹 이름 지정 형식: /aws/ecs/{application-name}
- 각 컨테이너 인스턴스는 그룹 내에 새 로그 스트림을 생성합니다.

로그 보기

AWS 콘솔을 통해:

- CloudWatch > 로그 그룹으로 이동
- 애플리케이션의 로그 그룹 선택
- 컨테이너 로그를 볼 관련 로그 스트림을 선택합니다.

AWS CLI 사용:

```
aws logs get-log-events --log-group-name /aws/ecs/your-app-name --log-stream-name your-stream-name
```

공통 로그 위치

- 애플리케이션 로그: CloudWatch Logs

- ECS 서비스 이벤트: ECS 콘솔 > 클러스터 > 서비스 > 이벤트 탭
- 컨테이너 상태: ECS 콘솔 > 클러스터 > 서비스 > 작업 탭

데이터베이스 연결 관리

애플리케이션은 데이터베이스 연결 설정에 환경 변수를 사용합니다.

연결 문제가 발생하는 경우:

- 환경 변수에서 현재 연결 설정 확인
- 필요에 따라 데이터베이스 연결 문자열을 수정하도록 환경 변수 업데이트
- 애플리케이션 재배포 없이 환경 변수 업데이트를 통해 연결 문자열을 변경할 수 있습니다.

데이터베이스 연결 문제

문제: AWS 변환을 SQL Server에 연결할 수 없음

솔루션

- AWS 변환과 SQL Server 간의 네트워크 연결 확인
- 보안 그룹 규칙에서 적절한 포트 액세스 확인(1433)
- Secrets Manager에서 데이터베이스 자격 증명 확인
- 생성된 사용자로 데이터베이스 권한 테스트
- SQL Server가 혼합 모드 인증을 위해 구성되어 있는지 확인
- 보안 암호에 필수 태그가 있는지 확인(프로젝트: atx-db-modernization, 소유자: 데이터베이스 커넥터)

방화벽 및 보안 그룹 문제

문제: 연결 제한 시간 또는 "데이터베이스에 연결할 수 없음" 오류

근본 원인: 트래픽을 차단ACLs

솔루션

1. 보안 그룹 구성 확인:

- SQL Server 보안 그룹에 DMS Schema Conversion 보안 그룹의 포트 1433을 허용하는 인바운드 규칙이 있는지 확인합니다.
- 소스가 IP 주소가 아닌 보안 그룹 ID(예: sg-0123456789abcdef0)인지 확인합니다.
- DMS Schema Conversion 보안 그룹이 인스턴스 프로파일에 올바르게 지정되었는지 확인
- 충돌하는 거부 규칙이 없는지 확인

2. 네트워크 ACLs 확인:

- 서브넷 수준 네트워크 ACLs 포트 1433에서 인바운드 트래픽을 허용하는지 확인
- 네트워크 ACLs 반환 트래픽에 대해 아웃바운드 임시 포트를 허용하는지 확인
- 데이터베이스 서브넷과 DMS 서브넷 네트워크 ACLs 모두 확인

3. VPC 구성 확인:

- DMS Schema Conversion 인스턴스와 SQL Server가 동일한 VPC에 있는지 또는 적절한 VPC 피어링이 있는지 확인
- 라우팅 테이블이 서브넷 간 트래픽을 허용하는지 확인
- 트래픽을 차단하는 방화벽 어플라이언스가 없는지 확인

4. 연결 테스트:

- DMS Schema Conversion과 동일한 서브넷에서 테스트 EC2 인스턴스 시작
- DMS Schema Conversion과 동일한 보안 그룹 연결
- telnet 또는 SQL Server Management Studio를 사용하여 SQL Server에 대한 연결 테스트
- 테스트에 성공하면 AWS 변환 구성에서 문제가 발생하고, 실패하면 네트워크/방화벽에서 문제가 발생합니다.

일반적인 실수: 포트 1433을 0.0.0.0/0(모든 소스)으로 여는 것은 보안 위험입니다. 항상 보안 그룹 기반 액세스 제어를 사용하여 DMS Schema Conversion 보안 그룹으로만 액세스를 제한합니다.

스키마 변환 문제

문제: 스키마 변환에 많은 작업 항목이 표시됨

솔루션

- 변환 보고서의 작업 항목 검토
- 영향을 기반으로 우선순위 지정
- 복잡한 SQL 변환에 Amazon Q Developer 사용
- 지침은 AWS Support에 문의하세요.

- 복잡한 데이터베이스에 대한 단계별 접근 방식 고려

애플리케이션 변환 문제

문제: 애플리케이션 변환 빌드 실패

솔루션

- 변환 보고서의 빌드 오류 검토
- 필요한 경우 프라이빗 NuGet 피드 구성
- 필요한 경우 패키지 참조 업데이트
- Windows별 종속성 확인
- 자세한 오류에 대한 변환 로그 검토

데이터 마이그레이션 문제

문제: 데이터 마이그레이션 검증 실패

솔루션

- 특정 실패에 대한 검증 보고서 검토
- 데이터 유형 매핑 확인
- 자격 증명 열 구성 확인(기본값으로 생성됨과 항상 생성됨)
- 계산된 열 표현식 검토
- 복잡한 데이터 문제는 AWS Support에 문의하세요.

리소스 정리 문제

문제: 리소스 오류와 함께 변환 작업이 실패함

솔루션

- 기존 DMS 리소스(마이그레이션 프로젝트, 데이터 공급자, 인스턴스 프로파일) 확인
- 이전 시도에서 실패했거나 불완전한 리소스 정리
- 보안 암호 삭제가 예약되지 않았는지 확인
- DMS 및 Aurora PostgreSQL에 대한 서비스 할당량 확인

- 정리로 문제가 해결되지 않으면 AWS Support에 문의하세요.

배포 관련 문제

문제: 변환된 애플리케이션을 Aurora PostgreSQL에 연결할 수 없음

솔루션

- PostgreSQL의 연결 문자열 형식 확인
- 보안 그룹 규칙 확인
- Secrets Manager에서 데이터베이스 자격 증명 확인
- SSL/TLS가 올바르게 구성되었는지 확인
- psql 또는 pgAdmin을 사용하여 연결 테스트

추가 도움말 받기

AWS Support에 문의할 때 다음을 제공하세요.

- 변환 작업 ID
- AWS 계정 ID
- 리전
- 오류 메시지 및 스크린샷
- 변환 로그(AWS 변환 콘솔에서 사용 가능)

AWS 변환 시 보안

의 클라우드 보안 AWS 이 최우선 순위입니다. AWS 고객은 보안에 가장 민감한 조직의 요구 사항을 충족하도록 구축된 데이터 센터 및 네트워크 아키텍처의 이점을 누릴 수 있습니다.

보안은 AWS와 사용자 간의 공동 책임입니다. [공동 책임 모델](#)은 이 사항을 클라우드의 보안 및 클라우드 내 보안으로 설명합니다.

- 클라우드 보안 - AWS 는에서 AWS 서비스를 실행하는 인프라를 보호할 책임이 있습니다 AWS 클라우드. AWS 또한는 안전하게 사용할 수 있는 서비스를 제공합니다. 타사 감사자는 [AWS 규정 준수 프로그램](#) 일환으로 보안의 효과를 정기적으로 테스트하고 확인합니다. AWS 변환에 적용되는 규정 준수 프로그램에 대한 자세한 내용은 규정 준수 프로그램 [AWS 제공 범위 내 서비스규정 준수 프로그램](#).
- 클라우드의 보안 - 사용자의 책임은 사용하는 AWS 서비스에 따라 결정됩니다. 또한 귀하는 귀사의 데이터 민감도, 귀사의 요구 사항, 관련 법률 및 규정을 비롯한 기타 요소에 대해서도 책임이 있습니다.

이 설명서는 AWS 변환을 사용할 때 공동 책임 모델을 적용하는 방법을 이해하는 데 도움이 됩니다. 다음 주제에서는 보안 및 규정 준수 목표에 맞게 AWS 변환을 구성하는 방법을 보여줍니다. 또한 AWS 변환 리소스를 모니터링하고 보호하는 데 도움이 되는 다른 AWS 서비스를 사용하는 방법을 알아봅니다.

주제

- [의 데이터 보호 AWS Transform](#)
- [AWS 변환을 위한 자격 증명 및 액세스 관리](#)
- [AWS 변환에 대한 규정 준수 검증](#)
- [AWS 변환의 복원력](#)
- [AWS Transform 및 인터페이스 엔드포인트\(AWS PrivateLink\)](#)
- [VPC에서 AWS Transform 웹 애플리케이션에 액세스](#)

의 데이터 보호 AWS Transform

[공동 책임 모델](#)은 AWS 의 데이터 보호에 적용됩니다 AWS Transform. 이 모델에 설명된 대로 AWS 는 모든를 실행하는 글로벌 인프라를 보호할 책임이 있습니다 AWS 클라우드. 사용자는 이 인프라에 호스팅되는 콘텐츠에 대한 통제 권한을 유지할 책임이 있습니다. 또한 사용하는에 대한 보안 구성 및 관리 작업도 담당 AWS 서비스 합니다. 데이터 프라이버시에 대한 자세한 내용은 [데이터 프라이버시](#)

[FAQ](#)를 참조하세요. 유럽의 데이터 보호에 대한 자세한 내용은 AWS Security Blog의 [AWS Shared Responsibility Model and GDPR](#) 블로그 게시물을 참조하세요.

데이터 보호를 위해 자격 증명을 보호하고 AWS 계정 AWS Identity and Access Management ()를 사용하여 개별 사용자를 설정하는 것이 좋습니다 IAM. 이러한 방식에서는 각 사용자에게 자신의 직무를 충실히 이행하는 데 필요한 권한만 부여됩니다. 또한 다음과 같은 방법으로 데이터를 보호하는 것이 좋습니다.

- 각 계정에 다중 인증(MFA)을 사용합니다.
- SSL/TLS를 사용하여 AWS 리소스와 통신합니다. TLS 1.2 이상을 권장합니다.
- 를 사용하여 API 및 사용자 활동 로깅을 설정합니다 AWS CloudTrail.
- 내의 모든 기본 보안 제어와 함께 AWS 암호화 솔루션을 사용합니다 AWS 서비스.
- 와 같은 고급 관리형 보안 서비스를 사용하면 Amazon Macie에 저장된 민감한 데이터를 검색하고 보호할 수 있습니다 Amazon S3.
- 명령줄 인터페이스 또는 API를 AWS 통해 액세스할 때 FIPS 140-2 검증 암호화 모듈이 필요한 경우 FIPS 엔드포인트를 사용합니다. 사용 가능한 FIPS 엔드포인트에 대한 자세한 내용은 [Federal Information Processing Standard\(FIPS\) 140-2](#)를 참조하세요.

고객의 이메일 주소와 같은 기밀 정보나 중요한 정보는 [태그](#)나 이름 필드와 같은 자유 형식 텍스트 필드에 입력하지 않는 것이 좋습니다. 여기에는 AWS Transform 또는 기타에서, API AWS Management Console, AWS Command Line Interface (AWS CLI) 또는 AWS SDKs를 AWS 서비스 사용하여 작업하는 경우가 포함됩니다. 이름에 사용되는 태그 또는 자유 형식 텍스트 필드에 입력하는 모든 데이터는 청구 또는 진단 로그에 사용될 수 있습니다. 에서 콘텐츠를 AWS Transform 사용하는 방법에 대한 자세한 내용은 단원을 참조하십시오 [AWS Transform 서비스 개선](#).

AWS Transform 는 질문, 응답, 콘솔 메타데이터 및 코드와 같은 추가 컨텍스트를 IDE에 저장하여 질문에 대한 응답을 생성합니다. 데이터를 암호화하는 방법에 대한 자세한 내용은 [의 데이터 암호화 AWS Transform](#) 섹션을 참조하세요. AWS 에서 사용자가 묻는 몇 가지 질문 AWS Transform 과 그 응답을 사용하여 서비스를 개선하는 방법에 대한 자세한 내용은 섹션을 참조하세요 [AWS Transform 서비스 개선](#).

에서 AWS Transform데이터는 AWS Transform 프로필이 생성된 AWS 리전에 저장됩니다.

교차 추론을 사용하면에 대한 요청이 데이터가 저장된 리전 내의 다른 리전에서 처리될 AWS Transform 수 있습니다. 자세한 내용은 [교차 리전 추론을 참조하세요](#).

주제

- [에서 리전 간 처리 AWS Transform](#)
- [의 데이터 암호화 AWS Transform](#)
- [AWS Transform 서비스 개선](#)

에서 리전 간 처리 AWS Transform

다음 섹션에서는 교차 리전 추론 및 교차 리전 호출을 사용하여 AWS Transform 서비스를 제공하는 방법을 설명합니다.

교차 리전 추론

AWS Transform 는 Amazon Bedrock으로 구동되며 교차 리전 추론을 사용하여 트래픽을 여러에 분산 AWS 리전 하여 대규모 언어 모델(LLM) 추론 성능과 신뢰성을 개선합니다. 교차 리전 추론을 사용하면 다음을 얻을 수 있습니다.

- 수요가 많은 기간에 처리량 및 복원력 향상
- 성능 개선
- Amazon Bedrock에서 호스팅되는 가장 강력한 LLMs에 의존하는 새로 시작된 AWS Transform 기능 및 기능에 대한 액세스

교차 리전 추론 요청은 데이터가 원래 상주 AWS 리전 하는 지리의 일부인 내에 유지됩니다. 예를 들어 미국의 AWS Transform 구성에서 이루어진 요청은 AWS 리전 미국의 내에 보관됩니다. 교차 리전 추론에서 데이터가 저장되는 위치는 변경되지 않지만 요청 및 출력 결과는 데이터가 원래 상주하는 리전 외부로 이동할 수 있습니다. 모든 데이터는 암호화된 상태로 Amazon의 보안 네트워크를 통해 전송됩니다. 교차 리전 추론을 사용하는 데 드는 추가 비용은 없습니다.

교차 리전 추론은 데이터가 저장되는 위치에 영향을 주지 않습니다. 사용 시 데이터가 저장되는 위치에 대한 자세한 내용은 섹션을 AWS Transform참조하세요 [의 데이터 보호 AWS Transform](#).

AWS Transform 교차 리전 추론에 지원되는 리전

에 대한 특정 요청에는 리전 간 호출이 필요할 AWS Transform 수 있습니다. 다음 표에서는 요청이 시작된 리전에 따라 요청이 라우팅될 수 있는 리전을 설명합니다.

소스 리전	대상 리전
미국 동부(버지니아 북부)(us-east-1)	미국 동부(버지니아 북부)(us-east-1)

소스 리전	대상 리전
	미국 동부(오하이오)(us-east-2)
	미국 서부(오리건)(us-west-2)
유럽(프랑크푸르트)(eu-central-1)	유럽(프랑크푸르트)(eu-central-1)
	유럽(스톡홀름)(eu-north-1)
	유럽(밀라노) (eu-south-1)
	유럽(스페인)(eu-south-2)
	유럽(아일랜드)(eu-west-1)
	유럽(파리)(eu-west-3)
아시아 태평양(뭄바이)(ap-south-1)	아시아 태평양(도쿄)(ap-northeast-1)
	아시아 태평양(서울)(ap-northeast-2)
	아시아 태평양(오사카) (ap-northeast-3)
	아시아 태평양(뭄바이)(ap-south-1)
	아시아 태평양(하이데라바드)(ap-south-2)
	아시아 태평양(싱가포르)(ap-southeast-1)
	아시아 태평양(시드니)(ap-southeast-2)
	아시아 태평양(멜버른)(ap-southeast-4)
아시아 태평양(도쿄)(ap-northeast-1)	아시아 태평양(도쿄)(ap-northeast-1)
	아시아 태평양(오사카) (ap-northeast-3)

소스 리전	대상 리전
아시아 태평양(서울)(ap-northeast-2)	아시아 태평양(도쿄)(ap-northeast-1) 아시아 태평양(서울)(ap-northeast-2) 아시아 태평양(오사카) (ap-northeast-3) 아시아 태평양(뭄바이)(ap-south-1) 아시아 태평양(하이데라바드)(ap-south-2) 아시아 태평양(싱가포르)(ap-southeast-1) 아시아 태평양(시드니)(ap-southeast-2) 아시아 태평양(멜버른)(ap-southeast-4)
아시아 태평양(시드니)(ap-southeast-2)	아시아 태평양(시드니)(ap-southeast-2) 아시아 태평양(멜버른)(ap-southeast-4)
유럽(런던)(eu-west-2)	유럽(프랑크푸르트)(eu-central-1) 유럽(스톡홀름)(eu-north-1) 유럽(밀라노) (eu-south-1) 유럽(스페인)(eu-south-2) 유럽(아일랜드)(eu-west-1) 유럽(런던) (eu-west-2) 유럽(파리)(eu-west-3)
캐나다(중부)(ca-central-1)	상용 AWS 리전 + 캐나다(중부)(ca-central-1)
남아메리카(상파울루)(sa-east-1)	상용 AWS 리전 + 남아메리카(상파울루)(sa-east-1)

사용할 수 있는 전체 리전 목록은 섹션을 [AWS Transform참조하세요](#)에 지원되는 리전 [AWS Transform](#).

리전 간 지식

AWS Transform 서비스, 변환 워크플로 또는 관련 AWS 설명서에 대해 일반적인 질문을 하면 미국 리전의 경우 미국 동부(버지니아)(us-east-1)에, 다른 모든 리전의 경우 유럽(프랑크푸르트)(eu-central-1)에 교차 리전 요청을 AWS Transform 하여 문서를 검색하고 요청을 이행할 수 있습니다. 예를 들어 Lambda와 같은 다른 AWS 서비스를 사용하는 방법에 대해 질문할 때 AWS Transform 는 교차 리전 호출을 수행하여 질문에 응답할 관련 AWS 문서를 검색할 수 있습니다. 다음 표에서는 요청이 시작된 리전에 따라 요청이 라우팅될 수 있는 리전을 설명합니다.

소스 리전	대상 리전
미국 동부(버지니아 북부)(us-east-1)	미국 동부(버지니아 북부)(us-east-1)
유럽(프랑크푸르트)(eu-central-1)	유럽(프랑크푸르트)(eu-central-1)
유럽(런던)(eu-west-2)	유럽(프랑크푸르트)(eu-central-1)
아시아 태평양(도쿄)(ap-northeast-1)	유럽(프랑크푸르트)(eu-central-1)
아시아 태평양(시드니)(ap-southeast-2)	유럽(프랑크푸르트)(eu-central-1)
아시아 태평양(서울)(ap-northeast-2)	유럽(프랑크푸르트)(eu-central-1)
아시아 태평양(뭄바이)(ap-south-1)	유럽(프랑크푸르트)(eu-central-1)
캐나다(중부)(ca-central-1)	유럽(프랑크푸르트) (eu-central-1)
남아메리카(상파울루)(sa-east-1)	유럽(프랑크푸르트)(eu-central-1)

이 설정은 기본적으로 활성화되어 있습니다. 계정 관리자는이 설정을 수정할 수 있습니다. 이 기능을 비활성화하면가 다른 리전에서 지식을 검색해야 하는 기능에 AWS Transform 대한 액세스 권한이 손실됩니다. 이로 인해 응답의 정확도가 떨어질 수 있습니다.

리전 간 호출을 비활성화하려면 AWS Transform다음을 수행합니다.

1. 처음 설정할 때 시작하기 페이지로 AWS Transform이동하여 구성을 완료합니다. 기존 AWS Transform 구성에 대한 경우 설정 페이지로 이동합니다.

2. 토글 교차 리전 호출을 활성화하여 끄기 위치에 대한 일반적인 AWS 관련 질문에 답변합니다.

AWS Transform Windows 교차 리전 추론용

다음 표에는 추론 프로파일을 직접적으로 호출할 수 있는 소스 리전과 요청을 라우팅할 수 있는 대상 리전이 나와 있습니다.

소스 리전	추론 대상 리전
미국 동부(버지니아 북부)(us-east-1)	미국 동부(버지니아 북부)(us-east-1)
	미국 동부(오하이오)(us-east-2)
	미국 서부(오리건)(us-west-2)
유럽(프랑크푸르트)(eu-central-1)	유럽(프랑크푸르트)(eu-central-1)
	유럽(스톡홀름)(eu-north-1)
	유럽(밀라노) (eu-south-1)
	유럽(스페인)(eu-south-2)
	유럽(아일랜드)(eu-west-1)
	유럽(파리)(eu-west-3)
아시아 태평양(도쿄)(ap-northeast-1)	아시아 태평양(도쿄)(ap-northeast-1)
	아시아 태평양(오사카) (ap-northeast-3)
아시아 태평양(시드니)(ap-southeast-2)	아시아 태평양(시드니)(ap-southeast-2)
	아시아 태평양(멜버른)(ap-southeast-4)
아시아 태평양(서울)(ap-northeast-2)	모든 상용 리전
아시아 태평양(뭄바이)(ap-south-1)	모든 상용 리전
캐나다(중부)(ca-central-1)	모든 상용 리전

AWS Transform 마이그레이션을 위한 리전 간 추론

다음 표에는 추론 프로파일을 직접적으로 호출할 수 있는 소스 리전과 요청을 라우팅할 수 있는 대상 리전이 나와 있습니다.

소스 리전	추론 대상 리전
미국 동부(버지니아 북부)(us-east-1)	모든 상용 리전
유럽(프랑크푸르트)(eu-central-1)	모든 상용 리전
유럽(런던)(eu-west-2)	모든 상용 리전
아시아 태평양(도쿄)(ap-northeast-1)	아시아 태평양(도쿄)(ap-northeast-1) 아시아 태평양(오사카) (ap-northeast-3)
아시아 태평양(시드니)(ap-southeast-2)	아시아 태평양(시드니)(ap-southeast-2) 아시아 태평양(멜버른)(ap-southeast-4)
아시아 태평양(서울)(ap-northeast-2)	모든 상용 리전
아시아 태평양(뭄바이)(ap-south-1)	모든 상용 리전
캐나다(중부)(ca-central-1)	모든 상용 리전

AWS Transform 메인프레임 교차 리전 추론용

AWS Transform 메인프레임용은 Amazon Bedrock 지리적 리전 간 추론을 사용합니다. 즉, 일부 호출이 소스 리전 AWS 리전 외부로 라우팅될 수 있습니다. 다음 표에는 추론 프로파일을 직접적으로 호출할 수 있는 소스 리전과 요청을 라우팅할 수 있는 대상 리전이 나와 있습니다.

소스 리전	추론 대상 리전
미국 동부(버지니아 북부)(us-east-1)	미국 동부(버지니아 북부)(us-east-1) 미국 동부(오하이오)(us-east-2) 미국 서부(오리건)(us-west-2)

소스 리전	추론 대상 리전
유럽(프랑크푸르트)(eu-central-1)	유럽(프랑크푸르트)(eu-central-1) 유럽(스톡홀름)(eu-north-1) 유럽(밀라노) (eu-south-1) 유럽(스페인)(eu-south-2) 유럽(아일랜드)(eu-west-1) 유럽(파리)(eu-west-3)
유럽(런던)(eu-west-2)	유럽(프랑크푸르트)(eu-central-1) 유럽(스톡홀름)(eu-north-1) 유럽(밀라노) (eu-south-1) 유럽(스페인)(eu-south-2) 유럽(아일랜드)(eu-west-1) 유럽(런던) (eu-west-2) 유럽(파리)(eu-west-3)
아시아 태평양(도쿄)(ap-northeast-1)	아시아 태평양(도쿄)(ap-northeast-1) 아시아 태평양(오사카) (ap-northeast-3)
아시아 태평양(시드니)(ap-southeast-2)	아시아 태평양(시드니)(ap-southeast-2) 아시아 태평양(멜버른)(ap-southeast-4)
아시아 태평양(서울)(ap-northeast-2)	모든 상용 리전
아시아 태평양(뭄바이)(ap-south-1)	모든 상용 리전

소스 리전	추론 대상 리전
캐나다(중부)(ca-central-1)	캐나다(중부)(ca-central-1) 미국 동부(버지니아 북부)(us-east-1) 미국 동부(오하이오)(us-east-2) 미국 서부(오리건)(us-west-2)
남아메리카(상파울루)(sa-east-1)	모든 상용 리전

AWS Transform 사용자 지정

AWS Transform 사용자 지정은 Amazon Bedrock 지리적 리전 간 추론을 사용합니다. 즉, 일부 호출이 소스 리전 AWS 리전 외부로 라우팅될 수 있습니다. 다음 표에는 추론 프로파일을 직접적으로 호출할 수 있는 소스 리전과 요청을 라우팅할 수 있는 대상 리전이 나와 있습니다.

소스 리전	추론 대상 리전
미국 동부(버지니아 북부)(us-east-1)	미국 동부(버지니아 북부)(us-east-1) 미국 동부(오하이오)(us-east-2) 미국 서부(오리건)(us-west-2)
유럽(프랑크푸르트)(eu-central-1)	유럽(프랑크푸르트)(eu-central-1) 유럽(스톡홀름)(eu-north-1) 유럽(밀라노) (eu-south-1) 유럽(스페인)(eu-south-2) 유럽(아일랜드)(eu-west-1) 유럽(파리)(eu-west-3)
유럽(런던)(eu-west-2)	유럽(프랑크푸르트)(eu-central-1) 유럽(스톡홀름)(eu-north-1)

소스 리전	추론 대상 리전
	유럽(밀라노) (eu-south-1)
	유럽(스페인)(eu-south-2)
	유럽(아일랜드)(eu-west-1)
	유럽(런던) (eu-west-2)
	유럽(파리)(eu-west-3)
아시아 태평양(도쿄)(ap-northeast-1)	모든 상용 리전
아시아 태평양(시드니)(ap-southeast-2)	아시아 태평양(시드니)(ap-southeast-2)
	아시아 태평양(멜버른)(ap-southeast-4)
아시아 태평양(서울)(ap-northeast-2)	모든 상용 리전
아시아 태평양(뭄바이)(ap-south-1)	모든 상용 리전
캐나다(중부)(ca-central-1)	캐나다(중부)(ca-central-1)
	미국 동부(버지니아 북부)(us-east-1)
	미국 동부(오하이오)(us-east-2)
	미국 서부(오리건)(us-west-2)

의 데이터 암호화 AWS Transform

이 주제에서는 전송 중 암호화 및 저장 중 암호화에 AWS Transform 대한 관련 정보를 제공합니다.

AWS Transform 는 기본적으로 암호화를 제공하여 AWS 소유 키를 사용한 암호화로 민감한 고객 저장 데이터를 보호합니다.

암호화 유형

전송 중 암호화

고객과 간의 통신 AWS Transform 과 AWS Transform 와 다운스트림 종속성 간의 통신은 TLS 1.2 이상의 연결을 사용하여 보호됩니다.

Important

[검색 계정을 연결](#)하면 AWS Transform은 사용자를 대신하여 해당 계정에서 Amazon S3 버킷을 생성합니다. 해당 버킷은 기본적으로 SecureTransport 활성화되어 있지 않습니다. 버킷 정책에 보안 전송을 포함하려면 정책을 업데이트해야 합니다. 자세한 내용은 [Amazon S3의 보안 모범 사례를 참조하세요](#).

저장 시 암호화

AWS Transform 는 Amazon DynamoDB 및 Amazon Simple Storage Service(Amazon S3)를 사용하여 저장 데이터를 저장합니다. 저장 데이터는 기본적으로 AWS 암호화 솔루션을 사용하여 암호화됩니다. 는 AWS Key Management Service (AWS KMS)의 AWS 소유 키를 사용하여 암호화로 데이터를 AWS Transform 암호화합니다. 데이터를 암호화하는 AWS 관리형 키를 보호하기 위해 어떤 조치도 취할 필요가 없습니다. 자세한 내용은 AWS Key Management Service 개발자 안내서의 [AWS 소유 키](#)를 참조하세요.

데이터 유형	AWS소유 키 암호화	고객 관리형 키 암호화 (선택 사항)
고객 버킷 데이터	활성화됨	활성화됨
Amazon S3 버킷에 저장된 코드 및 설명서와 같은 고객 입력 및 출력		
아티팩트 스토어	활성화됨	활성화됨
S3 버킷에 저장된 코드 변환의 일부로 사용되는 중간 아티팩트		
작업 목표	활성화됨	활성화됨

데이터 유형	AWS소유 키 암호화	고객 관리형 키 암호화 (선택 사항)
Amazon S3 버킷에 저장된 작업에 대한 고객의 의도		
채팅 메시지 Amazon S3 버킷에 AWS Transform 저장된 고객과 간의 메시지	활성화됨	활성화됨
채팅 지식 기반 Amazon OpenSearch에 저장되고 AWS Bedrock을 통해 처리되는 AWS Transform 및 고객 채팅과 관련된 인덱싱된 데이터	활성화됨	활성화됨

참고: 고객은 위의 모든 데이터 유형을 암호화하는 데 사용할 자체 고객 관리형 키(CMK)를 등록할 수 있습니다.

고객 관리형 키는 KMS 키에 대한 액세스를 제어하여 데이터에 대한 액세스를 직접 제어하기 위해 생성, 소유 및 관리하는 AWS 계정의 KMS 키입니다. 대칭 키만 지원됩니다. 자체 KMS 키 생성에 대한 자세한 내용은 AWS Key Management Service 개발자 안내서의 [키 생성](#)을 참조하세요.

고객 관리형 키를 사용하는 경우 AWS Transform 는 KMS 권한 부여를 사용하여 권한이 부여된 사용자, 역할 또는 애플리케이션이 KMS 키를 사용할 수 있도록 합니다. AWS Transform 관리자가 구성 중에 암호화에 고객 관리형 키를 사용하도록 선택하면 해당 키에 대한 권한이 생성됩니다. 이 권한 부여는 최종 사용자가 저장 데이터 암호화에 암호화 키를 사용할 수 있도록 허용합니다. 권한 부여에 대한 자세한 내용은 [AWS KMS의 권한 부여](#)를 참조하세요.

AWS 소유 키(기본값)

Note

AWS 소유 키 -는 기본적으로 이러한 키를 AWS Transform 사용하여 개인 식별 데이터를 자동으로 암호화합니다. AWS 소유 키를 보거나 관리하거나 사용하거나 사용을 감사할 수 없습니

다. 하지만 데이터를 암호화하는 키를 보호하기 위해 어떤 작업을 수행하거나 어떤 프로그램을 변경할 필요가 없습니다. 자세한 내용은 Key Management Service 개발자 안내서의 AWS 소유 AWS키를 참조하세요.

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.

이 암호화 계층을 비활성화하거나 대체 암호화 유형을 선택할 수는 없지만 변환을 생성할 때 고객 관리형 키를 선택하여 기존 AWS 소유 암호화 키에 두 번째 암호화 계층을 추가할 수 있습니다.

고객 관리형 키(선택 사항)

고객 관리형 키 - 사용자가 생성, 소유 및 관리하는 대칭 고객 관리형 키를 사용하여 AWS 소유 키를 사용하는 기존 암호화에 두 번째 암호화 계층을 추가할 수 있도록 AWS Transform 지원합니다. 이 암호화 계층을 완전히 제어할 수 있으므로 다음과 같은 작업을 수행할 수 있습니다.

- 키 정책 수립 및 유지
- IAM 정책 및 권한 부여 수립 및 유지
- 키 정책 활성화 및 비활성화
- 키 암호화 자료 교체
- 태그 추가
- 키 별칭 만들기
- 키 암호화 자료 교체
- 태그 추가
- 키 별칭 만들기
- 삭제를 위한 스케줄 키
- 자세한 내용은 AWS Key Management Service 개발자 안내서에서 [고객 관리형 키](#)를 참조하세요.

Note

AWS Transform 는 AWS 소유 키를 사용하여 저장 데이터 암호화를 자동으로 활성화하여 개인 식별 데이터를 무료로 보호합니다. 그러나 고객 관리형 키 사용에는 AWS KMS 요금이 적용됩니다. 요금에 대한 자세한 내용은 [AWS Key Management Service 요금](#)을 참조하십시오.

에 대한 자세한 내용은 [란 무엇입니까 AWS Key Management Service?](#)를 AWS KMS참조하십시오.

에서 권한 부여를 AWS Transform 사용하는 방법 AWS Key Management Service

AWS Transform 고객 관리형 키를 사용하려면 권한 부여가 필요합니다.

고객 관리형 키로 암호화된 [리소스 이름]을 생성하면 AWS Transform 는 CreateGrant 요청에 전송하여 사용자를 대신하여 권한을 생성합니다 AWS Key Management Service. 의 권한 부여 AWS Key Management Service 는 고객 계정의 KMS 키에 대한 AWS Transform 액세스 권한을 부여하는 데 사용됩니다.

AWS Transform 다음 내부 작업에 고객 관리형 키를 사용하려면 권한 부여가 필요합니다.

- [리소스 이름]을 생성할 때 입력한 대칭 고객 관리형 KMS 키 ID가 유효한지 확인하려면 AWS KMS 에 [KMS API] 요청을 보냅니다.
- [KMS API] 요청을 AWS KMS 로 보내 고객 관리형 키로 암호화된 데이터 키를 생성합니다.
- [KMS API] 요청을 AWS KMS 에 보내 암호화된 데이터 키를 복호화하여 데이터를 암호화하는 데 사용할 수 있도록 합니다.

언제든지 권한 부여에 대한 액세스 권한을 취소하거나 고객 관리형 키에 대한 서비스 액세스를 제거할 수 있습니다. 이렇게 하면 고객 관리형 키로 암호화된 데이터에 액세스할 수 AWS Transform 없으며, 이는 해당 데이터에 의존하는 작업에 영향을 미칩니다. 예를 들어 액세스할 AWS Transform 수 없는 암호화된 [리소스 이름]에서 [리소스 이름]을 가져오려고 하면 작업에서 AccessDeniedException 오류가 반환됩니다.

고객 관리형 키 생성

AWS 관리 콘솔 또는 AWS Key Management Service APIs.

대칭 고객 관리 키를 생성하려면 AWS Key Management Service 개발자 안내서의 [대칭 고객 관리 키 생성](#) 단계에 따르세요.

AWS Transform 리소스와 함께 고객 관리형 키를 사용하려면 키 정책에서 다음 API 작업을 허용해야 합니다.

kms:CreateGrant - 고객 관리형 키에 권한 부여를 추가합니다. 지정된 KMS 키에 대한 제어 액세스 권한을 부여하여 작업에 AWS Transform 필요한 권한 부여 액세스를 허용합니다. [권한 부여 사용](#)에 대한 자세한 내용은 AWS Key Management Service 개발자 안내서를 참조하세요.

이렇게 하면 AWS Transform 가 다음을 수행할 수 있습니다.

- 데이터 키가 암호화에 즉시 사용되지 않으므로 [KMS API([GenerateDataKeyWithoutPlainText/GenerateDatakey](#))]를 호출하여 암호화된 데이터 키를 생성하고 저장합니다.
- [KMS API([복호화](#))]를 호출하여 저장된 암호화된 데이터 키를 사용하여 암호화된 데이터에 액세스합니다.
- 서비스에서 [RetireGrant](#)를 허용하도록 사용 중지 보안 주체를 설정합니다.
- [kms:DescribeKey](#) - [서비스 이름]이 키를 검증할 수 있도록 고객 관리형 키 세부 정보를 제공합니다.

SQL 현대화를 위한 암호화

[SQL Server 현대화](#) 프로세스 중에 EC2 인스턴스, ECS 클러스터, ECR 이미지 및 S3 객체와 같은 리소스가 계정에 AWS Transform 생성됩니다. 계정의 데이터를 암호화하기 위해 고객 관리형 키를 제공할 수 있습니다. KMS 키에 CreatedFor 키와 값 AWSTransform 키를 태깅해야 합니다. 이 예제 정책은 기본 키 정책이 없는 경우 키 정책에 필요한 최소 권한을 나열합니다. 기본 키 정책이 있는 경우에도 ECS가 키를 사용할 수 있도록 기본 키 정책 외에도 KMS 키를 수동으로 업데이트해야 합니다.

```
"Statement": [
  {
    "Effect": "Allow",
    "Principal": {
      "AWS": "arn:aws:iam::111122223333:root"
    },
    "Action": [
      "kms:Decrypt",
      "kms:GenerateDataKey"
    ],
    "Resource": "*",
    "Condition": {
      "StringLike": {
        "kms:ViaService": "s3.*.amazonaws.com",
        "kms:EncryptionContext:aws-transform": "*"
      },
      "ArnLike": {
        "aws:PrincipalArn": "arn:aws:iam::*:role/*AWSTransform*"
      }
    }
  },
  {
    "Effect": "Allow",
    "Principal": {
```

```

    "AWS": "arn:aws:iam::111122223333:root"
  },
  "Action": [
    "kms:Decrypt",
    "kms:GenerateDataKey",
    "kms:GenerateDataKeyWithoutPlaintext",
    "kms:ReEncrypt*"
  ],
  "Resource": "*",
  "Condition": {
    "StringLike": {
      "kms:ViaService": "ec2.*.amazonaws.com"
    },
    "ArnLike": {
      "aws:PrincipalArn": "arn:aws:iam::*:role/*AWSTransform*"
    }
  }
},
{
  "Effect": "Allow",
  "Principal": {
    "AWS": "arn:aws:iam::111122223333:root"
  },
  "Action": "kms:CreateGrant",
  "Resource": "*",
  "Condition": {
    "StringLike": {
      "kms:ViaService": [
        "ec2.*.amazonaws.com",
        "ecr.*.amazonaws.com"
      ]
    },
    "Bool": {
      "kms:GrantIsForAWSResource": "true"
    },
    "ArnLike": {
      "aws:PrincipalArn": "arn:aws:iam::*:role/*AWSTransform*"
    }
  }
},
{
  "Effect": "Allow",
  "Principal": {
    "Service": "fargate.amazonaws.com"
  }
}

```

```

    },
    "Action": "kms:GenerateDataKeyWithoutPlaintext",
    "Resource": "*",
    "Condition": {
      "StringLike": {
        "kms:EncryptionContext:aws:ecs:clusterName": "AWSTransform*"
      }
    }
  },
  {
    "Effect": "Allow",
    "Principal": {
      "Service": "fargate.amazonaws.com"
    },
    "Action": "kms:CreateGrant",
    "Resource": "*",
    "Condition": {
      "StringLike": {
        "kms:EncryptionContext:aws:ecs:clusterName": "AWSTransform*"
      },
      "ForAllValues:StringEquals": {
        "kms:GrantOperations": "Decrypt"
      }
    }
  }
]

```

데이터베이스 마이그레이션을 위한 암호화

데이터베이스 마이그레이션 프로세스 중에는 AWS Database Migration Service(DMS)를 AWS Transform 사용하여 데이터베이스 데이터를 마이그레이션합니다. 선택적으로 고객 관리형 키를 제공하여 마이그레이션 중에 데이터베이스 데이터를 암호화할 수 있습니다.

다음 정책에는 세 개의 문이 포함되어 있습니다. 첫 번째 문은 AWS KMS 키에 대한 루트 계정 권한을 부여합니다. 두 번째 문을 사용하면 커넥터 역할이 검색 중에 키를 검증할 수 있습니다. 세 번째 문은 커넥터 역할이 DMS 작업에 키를 사용하도록 허용합니다.

```

"Statement": [
  {
    "Sid": "Enable IAM User Permissions",
    "Effect": "Allow",
    "Principal": { "AWS": "arn:aws:iam::111122223333:root" },
    "Action": "kms:*",

```

```

    "Resource": "*"
  },
  {
    "Sid": "Allow connector role to validate key during discovery",
    "Effect": "Allow",
    "Principal": { "AWS": "connector-role-arn" },
    "Action": "kms:DescribeKey",
    "Resource": "*"
  },
  {
    "Sid": "Allow connector role to use key via DMS",
    "Effect": "Allow",
    "Principal": { "AWS": "connector-role-arn" },
    "Action": [
      "kms:CreateGrant",
      "kms:Decrypt",
      "kms:DescribeKey",
      "kms:Encrypt",
      "kms:GenerateDataKey*",
      "kms:ReEncrypt*"
    ],
    "Resource": "*",
    "Condition": {
      "StringEquals": {
        "kms:ViaService": "dms.us-east-1.amazonaws.com"
      }
    }
  }
]

```

고객 관리형 KMS 키 사용

고객 관리형 KMS 키를 생성한 후 AWS Transform 관리자는 AWS Transform 콘솔에서 키를 제공하여 데이터를 암호화하는 데 사용해야 합니다.

데이터를 암호화하도록 고객 관리형 키를 설정하려면 AWS Transform 관리자에게 사용할 권한이 필요합니다 AWS KMS.

고객 관리형 키로 암호화된 기능을 사용하려면가 고객 관리형 키에 액세스할 수 AWS Transform 있는 권한이 필요합니다.

를 사용하는 동안 KMS 권한 부여와 관련된 오류가 표시되는 경우 AWS Transform가 권한 부여를 생성할 수 있도록 권한을 업데이트해야 AWS Transform 할 수 있습니다. 필요한 권한을 자동으로 구성하려

면 AWS Transform 콘솔로 이동하여 페이지 상단의 배너에서 권한 업데이트를 선택합니다. 가 권한 부여를 생성하도록 허용 AWS Transform 하려면 AWS Transform 콘솔 페이지에서 권한을 업데이트해야 합니다.

고객 관리형 키에 대한 AWS Transform 액세스 허용

다음 예제 정책 설명은 키에 대한 액세스를 허용하여 고객 관리형 키로 암호화된 기능에 AWS Transform 액세스할 수 있는 권한을 사용자에게 부여합니다. 관리자가 암호화를 위해 고객 관리형 키를 설정한 AWS Transform 경우이 정책을 사용해야 합니다.

Note

이 정보는 CMK를 사용하는 SQL Server 현대화 배포 워크플로에는 적용되지 않습니다.

```
"Statement": [
  {
    "Sid": "QKMSDecryptGenerateDataKeyPermissions",
    "Effect": "Allow",
    "Action": [
      "kms:Decrypt",
      "kms:GenerateDataKey",
      "kms:GenerateDataKeyWithoutPlaintext",
      "kms:ReEncryptFrom",
      "kms:ReEncryptTo"
    ],
    "Resource": [
      "arn:aws:kms:arn:aws::111122223333:key/[[key_id]]"
    ],
    "Condition": {
      "StringLike": {
        "kms:ViaService": [
          "q.us-east-1.amazonaws.com"
        ]
      }
    }
  }
]
```

AWS Transform 서비스 개선

가장 관련성이 높은 정보를 AWS Transform 제공하기 위해 당사는 서비스 개선을 위해 사용자가 묻는 질문 AWS Transform 및 응답 AWS Transform과 같은의 특정 콘텐츠를 사용할 수 있습니다. 이 페이지에서는 사용하는 콘텐츠와 옵트아웃 방법을 설명합니다.

AWS Transform 서비스 개선에 사용되는 콘텐츠

서비스 개선을 AWS Transform 위해의 특정 콘텐츠를 사용할 수 AWS Transform 있습니다. 예를 들어 일반적인 질문에 대한 더 나은 응답을 제공하거나, 운영 문제를 해결 AWS Transform 하거나, 디버깅 또는 모델 훈련을 위해이 콘텐츠를 사용할 수 있습니다.

가 서비스 개선에 사용할 AWS 수 있는 콘텐츠에는에 대한 질문 AWS Transform 과가 AWS Transform 생성하는 응답 및 코드가 포함됩니다.

옵트아웃 방법

서비스 개선을 위한 콘텐츠 AWS Transform 사용을 옵트아웃하는 방법은 사용하는 환경에 따라 다릅니다 AWS Transform.

에서 AI 서비스 옵트아웃 정책을 AWS Transform 구성합니다 AWS Organizations. 자세한 내용은 AWS Organizations 사용 설명서의 [AI 서비스 옵트아웃 정책](#)을 참조하세요.

Visual Studio IDE에서 콘텐츠 공유를 옵트아웃하려면 다음 절차를 사용합니다.

도구 -> 옵션 -> AWS 도구 키트 -> Amazon Q로 이동합니다.

AWS와 Amazon Q 콘텐츠 공유를 True 또는 False로 전환합니다.

AWS Toolkit for에서 원격 측정 데이터 공유를 옵트아웃하려면 다음 절차를 Visual Studio사용합니다.

1. 도구에서 옵션을 선택합니다.
2. 옵션 창에서 AWS 도구 키트 를 선택한 다음 일반을 선택합니다.
3. 도구 AWS 키트가 사용 정보를 수집하도록 허용을 선택 취소합니다.

AWS 변환을 위한 자격 증명 및 액세스 관리

AWS Identity and Access Management (IAM)는 관리자가 AWS 리소스에 대한 액세스를 안전하게 제어하는 데 도움이 AWS 서비스 되는입니다. IAM 관리자는 AWS 변환 리소스를 사용할 수 있는 인

중(로그인) 및 권한(권한 있음)을 받을 수 있는 사용자를 제어합니다. IAM은 추가 비용 없이 사용할 수 있는 AWS 서비스입니다.

주제

- [대상](#)
- [ID를 통한 인증](#)
- [정책을 사용하여 액세스 관리](#)
- [AWS 변환이 IAM과 작동하는 방식](#)
- [AWS 변환에 대한 자격 증명 기반 정책 예제](#)
- [자격 증명 및 액세스 AWS 변환 문제 해결](#)
- [에 대한 서비스 연결 역할 사용 AWS Transform](#)
- [AWS AWS 변환에 대한 관리형 정책](#)
- [AWS 변환 권한 참조](#)

대상

AWS Identity and Access Management (IAM)를 사용하는 방법은 역할에 따라 다릅니다.

- 서비스 사용자 - 기능에 액세스할 수 없는 경우 관리자에게 권한 요청([참조 자격 증명 및 액세스 AWS 변환 문제 해결](#))
- 서비스 관리자 - 사용자 액세스 결정 및 권한 요청 제출([AWS 변환이 IAM과 작동하는 방식](#) 참조)
- IAM 관리자 - 액세스를 관리하기 위한 정책 작성([AWS 변환에 대한 자격 증명 기반 정책 예제](#) 참조)

ID를 통한 인증

인증은 자격 증명 자격 증명을 AWS 사용하여 로그인하는 방법입니다. AWS 계정 루트 사용자, IAM 사용자 또는 IAM 역할을 수임하여 인증되어야 합니다.

AWS IAM Identity Center (IAM Identity Center), Single Sign-On 인증 또는 Google/Facebook 자격 증명과 같은 자격 증명 소스의 자격 증명을 사용하여 페더레이션 자격 증명으로 로그인할 수 있습니다. 로그인하는 방법에 대한 자세한 내용은 AWS 로그인 사용 설명서의 [AWS 계정에 로그인하는 방법](#) 섹션을 참조하세요.

프로그래밍 방식 액세스를 위해서는 요청에 암호화 방식으로 서명할 수 있는 SDK 및 CLI를 AWS 제공합니다. 자세한 내용은 IAM 사용 설명서의 [API 요청용 AWS Signature Version 4](#) 섹션을 참조하세요.

AWS 계정 루트 사용자

를 생성할 때 모든 AWS 서비스 및 리소스에 대한 완전한 액세스 권한이 있는 AWS 계정 theroot 사용자라는 하나의 로그인 자격 증명으로 AWS 계정시작합니다. 일상적인 태스크에 루트 사용자를 사용하지 않을 것을 강력히 권장합니다. 루트 사용자 자격 증명이 필요한 작업은 IAM 사용 설명서의 [루트 사용자 자격 증명이 필요한 작업](#) 섹션을 참조하세요.

페더레이션 ID

가장 좋은 방법은 인간 사용자에게 자격 증명 공급자와의 페더레이션을 사용하여 임시 자격 증명을 AWS 서비스 사용하여 액세스하도록 요구하는 것입니다.

페더레이션 자격 증명은 엔터프라이즈 디렉터리, 웹 자격 증명 공급자 또는 자격 증명 소스의 자격 증명을 AWS 서비스 사용하여 Directory Service 에 액세스하는 사용자입니다. 페더레이션 ID는 임시 자격 증명을 제공하는 역할을 수임합니다.

중앙 집중식 액세스 관리를 위해 AWS IAM Identity Center를 추천합니다. 자세한 정보는 AWS IAM Identity Center 사용 설명서의 [What is IAM Identity Center?](#)를 참조하세요.

IAM 사용자 및 그룹

[IAM 사용자](#)는 단일 개인 또는 애플리케이션에 대한 특정 권한을 가진 ID입니다. 장기 자격 증명에 있는 IAM 사용자 대신 임시 자격 증명을 사용하는 것이 좋습니다. 자세한 내용은 IAM 사용 설명서의 [자격 증명 공급자와의 페더레이션을 사용하여 임시 자격 증명을 AWS 사용하여 액세스하도록 인간 사용자에게 요구](#)하기를 참조하세요.

[IAM 그룹](#)은 IAM 사용자 모음을 지정하고 대규모 사용자 집합에 대한 관리 권한을 더 쉽게 만듭니다. 자세한 내용은 IAM 사용 설명서의 [IAM 사용자 사용 사례](#) 섹션을 참조하세요.

IAM 역할

[IAM 역할](#)은 임시 자격 증명을 제공하는 특정 권한이 있는 자격 증명입니다. [사용자에서 IAM 역할\(콘솔\)로 전환하거나 또는 API 작업을 호출하여 역할을](#) 수임할 수 있습니다. AWS CLI AWS 자세한 내용은 IAM 사용 설명서의 [역할 수임 방법](#)을 참조하세요.

IAM 역할은 페더레이션 사용자 액세스, 임시 IAM 사용자 권한, 교차 계정 액세스, 교차 서비스 액세스 및 Amazon EC2에서 실행되는 애플리케이션에 유용합니다. 자세한 내용은 IAM 사용 설명서의 [교차 계정 리소스 액세스](#)를 참조하세요.

정책을 사용하여 액세스 관리

정책을 AWS 생성하고 자격 증명 또는 리소스에 연결하여 AWS 에서 액세스를 제어합니다. 정책은 자격 증명 또는 리소스와 연결될 때 권한을 정의합니다.는 보안 주체가 요청할 때 이러한 정책을 AWS 평가합니다. 대부분의 정책은 JSON 문서 AWS 로 저장됩니다. JSON 정책 문서에 대한 자세한 내용은 IAM 사용 설명서의 [JSON 정책 개요](#) 섹션을 참조하세요.

정책을 사용하여 관리자는 어떤 보안 주체가 어떤 리소스에 대해 어떤 조건에서 작업을 수행할 수 있는지 정의하여 누가 무엇을 액세스할 수 있는지 지정합니다.

기본적으로 사용자 및 역할에는 어떠한 권한도 없습니다. IAM 관리자는 IAM 정책을 생성하고 사용자가 수임할 수 있는 역할에 추가합니다. IAM 정책은 작업을 수행하기 위해 사용하는 방법과 관계없이 작업에 대한 권한을 정의합니다.

ID 기반 정책

ID 기반 정책은 ID(사용자, 사용자 그룹 또는 역할)에 연결하는 JSON 권한 정책 문서입니다. 이러한 정책은 자격 증명이 수행할 수 있는 작업, 대상 리소스 및 이에 관한 조건을 제어합니다. ID 기반 정책을 생성하는 방법을 알아보려면 IAM 사용 설명서에서 [고객 관리형 정책으로 사용자 지정 IAM 권한 정의](#)를 참조하세요.

ID 기반 정책은 인라인 정책(단일 ID에 직접 포함) 또는 관리형 정책(여러 ID에 연결된 독립 실행형 정책)일 수 있습니다. 관리형 정책 또는 인라인 정책을 선택하는 방법을 알아보려면 IAM 사용 설명서의 [관리형 정책 및 인라인 정책 중에서 선택](#) 섹션을 참조하세요.

리소스 기반 정책

리소스 기반 정책은 리소스에 연결하는 JSON 정책 설명서입니다. 예를 들어 IAM 역할 신뢰 정책 및 Amazon S3 버킷 정책이 있습니다. 리소스 기반 정책을 지원하는 서비스에서 서비스 관리자는 이러한 정책을 사용하여 특정 리소스에 대한 액세스를 통제할 수 있습니다. 리소스 기반 정책에서 [보안 주체를 지정](#)해야 합니다.

리소스 기반 정책은 해당 서비스에 있는 인라인 정책입니다. 리소스 기반 정책에서는 IAM의 AWS 관리형 정책을 사용할 수 없습니다.

기타 정책 유형

AWS 는 보다 일반적인 정책 유형에서 부여한 최대 권한을 설정할 수 있는 추가 정책 유형을 지원합니다.

- 권한 경계 - ID 기반 정책에서 IAM 엔터티에 부여할 수 있는 최대 권한을 설정합니다. 자세한 정보는 IAM 사용 설명서의 [IAM 엔터티의 권한 범위](#)를 참조하세요.
- 서비스 제어 정책(SCP) - AWS Organizations내 조직 또는 조직 단위에 대한 최대 권한을 지정합니다. 자세한 내용은 AWS Organizations 사용 설명서의 [서비스 제어 정책](#)을 참조하세요.
- 리소스 제어 정책(RCP) - 계정의 리소스에 사용할 수 있는 최대 권한을 설정합니다. 자세한 내용은 AWS Organizations 사용 설명서의 [리소스 제어 정책\(RCP\)](#)을 참조하세요.
- 세션 정책 - 역할 또는 페더레이션 사용자에게 대해 임시 세션을 프로그래밍 방식으로 생성할 때 파라미터로 전달하는 고급 정책입니다. 자세한 내용은 IAM 사용 설명서의 [세션 정책](#)을 참조하세요.

여러 정책 유형

여러 정책 유형이 요청에 적용되는 경우, 결과 권한은 이해하기가 더 복잡합니다. 에서 여러 정책 유형이 관련될 때 요청을 허용할지 여부를 AWS 결정하는 방법을 알아보려면 IAM 사용 설명서의 [정책 평가 로직](#)을 참조하세요.

AWS 변환이 IAM과 작동하는 방식

IAM을 사용하여 AWS 변환에 대한 액세스를 관리하기 전에 AWS 변환에 사용할 수 있는 IAM 기능을 알아봅니다.

IAM 특성	AWS 변환 지원
자격 증명 기반 정책	예
리소스 기반 정책	아니요
정책 작업	예
정책 리소스	예
정책 조건 키	예
ACL	아니요
ABAC(정책 내 태그)	부분적
임시 자격 증명	예

IAM 특성	AWS 변환 지원
엔터티 권한	예
서비스 역할	예
서비스 연결 역할	예

AWS 변환 및 기타 AWS 서비스가 대부분의 IAM 기능과 작동하는 방법을 개괄적으로 알아보려면 IAM 사용 설명서의 [AWS IAM으로 작업하는 서비스](#)를 참조하세요.

AWS 변환을 위한 자격 증명 기반 정책

ID 기반 정책 지원: 예

ID 기반 정책은 IAM 사용자, 사용자 그룹 또는 역할과 같은 ID에 연결할 수 있는 JSON 권한 정책 문서입니다. 이러한 정책은 사용자 및 역할이 어떤 리소스와 어떤 조건에서 어떤 작업을 수행할 수 있는지를 제어합니다. 자격 증명 기반 정책을 생성하는 방법을 알아보려면 IAM 사용 설명서에서 [고객 관리형 정책으로 사용자 지정 IAM 권한 정의](#)를 참조하세요.

IAM ID 기반 정책을 사용하면 허용되거나 거부되는 작업과 리소스뿐 아니라 작업이 허용되거나 거부되는 조건을 지정할 수 있습니다. JSON 정책에서 사용할 수 있는 모든 요소에 대해 알아보려면 IAM 사용 설명서의 [IAM JSON 정책 요소 참조](#)를 참조하세요.

AWS 변환에 대한 자격 증명 기반 정책 예제

자격 증명 기반 정책 AWS 변환의 예를 보려면 섹션을 참조하세요 [AWS 변환에 대한 자격 증명 기반 정책 예제](#).

AWS 변환 내 리소스 기반 정책

리소스 기반 정책 지원: 아니요

리소스 기반 정책은 리소스에 연결하는 JSON 정책 설명서입니다. 리소스 기반 정책의 예제는 IAM 역할 신뢰 정책과 Amazon S3 버킷 정책입니다. 리소스 기반 정책을 지원하는 서비스에서 서비스 관리자는 이러한 정책을 사용하여 특정 리소스에 대한 액세스를 통제할 수 있습니다. 정책이 연결된 리소스의 경우 정책은 지정된 보안 주체가 해당 리소스와 어떤 조건에서 어떤 작업을 수행할 수 있는지를 정의합니다. 리소스 기반 정책에서 [보안 주체를 지정](#)해야 합니다. 보안 주체에는 계정, 사용자, 역할, 페더레이션 사용자 또는 이 포함될 수 있습니다 AWS 서비스.

교차 계정 액세스를 활성화하려는 경우, 전체 계정이나 다른 계정의 IAM 개체를 리소스 기반 정책의 보안 주체로 지정할 수 있습니다. 자세한 내용은 IAM 사용 설명서의 [IAM에서 교차 계정 리소스 액세스](#)를 참조하세요.

AWS 변환에 대한 정책 작업

정책 작업 지원: 예

관리자는 AWS JSON 정책을 사용하여 누가 무엇에 액세스할 수 있는지 지정할 수 있습니다. 즉, 어떤 보안 주체가 어떤 리소스와 어떤 조건에서 작업을 수행할 수 있는지를 지정할 수 있습니다.

JSON 정책의 Action요소는 정책에서 액세스를 허용하거나 거부하는 데 사용할 수 있는 작업을 설명합니다. 연결된 작업을 수행할 수 있는 권한을 부여하기 위한 정책에 작업을 포함하세요.

AWS 변환 작업 목록을 보려면 서비스 승인 참조의 [AWS 변환에 사용되는 작업, 리소스 및 조건 키](#)를 참조하세요.

사용자 지정 AWS 변환에 대한 작업 목록을 보려면 서비스 승인 참조의 사용자 [지정 AWS 변환에 대한 작업, 리소스 및 조건 키](#)를 참조하세요.

AWS 변환의 정책 작업은 작업 앞에 다음 접두사를 사용합니다.

```
transform
```

단일 문에서 여러 작업을 지정하려면 쉼표로 구분합니다.

```
"Action": [
    "transform:action1",
    "transform:action2"
]
```

자격 증명 기반 정책 AWS 변환의 예를 보려면 섹션을 참조하세요 [AWS 변환에 대한 자격 증명 기반 정책 예제](#).

AWS 변환을 위한 정책 리소스

정책 리소스 지원: 예

관리자는 AWS JSON 정책을 사용하여 누가 무엇에 액세스할 수 있는지 지정할 수 있습니다. 즉, 어떤 보안 주체가 어떤 리소스와 어떤 조건에서 작업을 수행할 수 있는지를 지정할 수 있습니다.

Resource JSON 정책 요소는 작업이 적용되는 하나 이상의 객체를 지정합니다. 모범 사례에 따라 [Amazon 리소스 이름\(ARN\)](#)을 사용하여 리소스를 지정합니다. 리소스 수준 권한을 지원하지 않는 작업의 경우, 와일드카드(*)를 사용하여 해당 문이 모든 리소스에 적용됨을 나타냅니다.

```
"Resource": "*"
```

AWS 변환 리소스 유형 및 해당 ARNs 목록과 각 리소스의 ARN을 지정할 수 있는 작업을 보려면 서비스 승인 참조의 [AWS 변환에 사용되는 작업, 리소스 및 조건 키](#)를 참조하세요.

리소스 유형 및 해당 ARNs 목록과 사용자 지정 AWS 변환을 위해 각 리소스의 ARN을 지정할 수 있는 작업을 보려면 서비스 승인 참조의 [사용자 지정 AWS 변환을 위한 작업, 리소스 및 조건 키](#)를 참조하세요.

자격 증명 기반 정책 AWS 변환의 예를 보려면 섹션을 참조하세요 [AWS 변환에 대한 자격 증명 기반 정책 예제](#).

AWS 변환을 위한 정책 조건 키

서비스별 정책 조건 키 지원: 예

관리자는 AWS JSON 정책을 사용하여 누가 무엇에 액세스할 수 있는지 지정할 수 있습니다. 즉, 어떤 보안 주체가 어떤 리소스와 어떤 조건에서 작업을 수행할 수 있는지를 지정할 수 있습니다.

Condition 요소는 정의된 기준에 따라 문이 실행되는 시기를 지정합니다. 같음(equals) 또는 미만(less than)과 같은 [조건 연산자](#)를 사용하여 정책의 조건을 요청의 값과 일치시키는 조건식을 생성할 수 있습니다. 모든 AWS 전역 조건 키를 보려면 IAM 사용 설명서의 [AWS 전역 조건 컨텍스트 키](#)를 참조하세요.

조건 키 AWS 변환 목록과 조건 키를 사용할 수 있는 작업 및 리소스를 보려면 서비스 승인 참조의 [AWS 변환에 사용되는 작업, 리소스 및 조건 키](#)를 참조하세요.

조건 키 목록과 사용자 지정 AWS 변환에 조건 키를 사용할 수 있는 작업 및 리소스를 보려면 서비스 승인 참조의 [사용자 지정 AWS 변환에 대한 작업, 리소스 및 조건 키](#)를 참조하세요.

자격 증명 기반 정책 AWS 변환의 예를 보려면 섹션을 참조하세요 [AWS 변환에 대한 자격 증명 기반 정책 예제](#).

AWS 변환ACLs

ACL 지원: 아니요

액세스 제어 목록(ACL)은 어떤 보안 주체(계정 멤버, 사용자 또는 역할)가 리소스에 액세스할 수 있는 권한을 가지고 있는지를 제어합니다. ACL은 JSON 정책 문서 형식을 사용하지 않지만 리소스 기반 정책과 유사합니다.

AWS 변환이 포함된 ABAC

ABAC 지원(정책의 태그): 부분적

속성 기반 액세스 제어(ABAC)는 태그라고 불리는 속성을 기반으로 권한을 정의하는 권한 부여 전략입니다. IAM 엔터티 및 AWS 리소스에 태그를 연결한 다음 보안 주체의 태그가 리소스의 태그와 일치할 때 작업을 허용하는 ABAC 정책을 설계할 수 있습니다.

태그에 근거하여 액세스를 제어하려면 `aws:ResourceTag/key-name`, `aws:RequestTag/key-name` 또는 `aws:TagKeys` 조건 키를 사용하여 정책의 [조건 요소](#)에 태그 정보를 제공합니다.

서비스가 모든 리소스 유형에 대해 세 가지 조건 키를 모두 지원하는 경우, 값은 서비스에 대해 예입니다. 서비스가 일부 리소스 유형에 대해서만 세 가지 조건 키를 모두 지원하는 경우, 값은 부분적입니다.

ABAC에 대한 자세한 내용은 IAM 사용 설명서의 [ABAC 권한 부여를 통한 권한 정의](#)를 참조하세요. ABAC 설정 단계가 포함된 자습서를 보려면 IAM 사용 설명서의 [속성 기반 액세스 제어\(ABAC\) 사용](#)을 참조하세요.

AWS 변환과 함께 임시 자격 증명 사용

임시 자격 증명 지원: 예

임시 자격 증명은 AWS 리소스에 대한 단기 액세스를 제공하며 페더레이션을 사용하거나 역할을 전환할 때 자동으로 생성됩니다. 장기 액세스 키를 사용하는 대신 임시 자격 증명을 동적으로 생성하는 것이 AWS 좋습니다. 자세한 내용은 IAM 사용 설명서의 [IAM의 임시 보안 자격 증명](#) 및 [IAM으로 작업하는 AWS 서비스](#) 섹션을 참조하세요.

AWS 변환에 대한 교차 서비스 보안 주체 권한

전달 액세스 세션(FAS) 지원: 예

전달 액세스 세션(FAS)은 호출하는 보안 주체의 권한을 다운스트림 서비스에 AWS 서비스 대한 요청과 AWS 서비스 함께 사용합니다. FAS 요청 시 정책 세부 정보는 [전달 액세스 세션](#)을 참조하세요.

AWS 변환을 위한 서비스 역할

서비스 역할 지원: 예

서비스 역할은 서비스가 사용자를 대신하여 작업을 수행하는 것으로 가정하는 [IAM 역할](#)입니다. IAM 관리자는 IAM 내에서 서비스 역할을 생성, 수정 및 삭제할 수 있습니다. 자세한 내용은 IAM 사용 설명서의 [AWS 서비스 AWS에 권한을 위임할 역할 생성](#)을 참조하세요.

Warning

서비스 역할에 대한 권한을 변경하면 AWS 변환 기능이 중단될 수 있습니다. AWS 변환이 관련 지침을 제공하는 경우에만 서비스 역할을 편집합니다.

AWS 변환을 위한 서비스 연결 역할

서비스 연결 역할 지원: 예

서비스 연결 역할은 연결된 서비스 역할의 한 유형입니다 AWS 서비스. 서비스는 사용자를 대신하여 작업을 수행하기 위해 역할을 수임할 수 있습니다. 서비스 연결 역할은 표시 AWS 계정 되며 서비스가 소유합니다. IAM 관리자는 서비스 연결 역할의 권한을 볼 수 있지만 편집은 할 수 없습니다.

AWS 변환 서비스 연결 역할 생성 또는 관리에 대한 자세한 내용은 [섹션을 참조하세요에 대한 서비스 연결 역할 사용 AWS Transform](#).

AWS 변환에 대한 자격 증명 기반 정책 예제

기본적으로 사용자 및 역할에는 AWS 변환 리소스를 생성하거나 수정할 수 있는 권한이 없습니다. 사용자에게 사용자가 필요한 리소스에서 작업을 수행할 권한을 부여하려면 IAM 관리자가 IAM 정책을 생성하면 됩니다.

이러한 예제 JSON 정책 문서를 사용하여 IAM ID 기반 정책을 생성하는 방법을 알아보려면 IAM 사용 설명서의 [IAM 정책 생성\(콘솔\)](#)을 참조하세요.

각 리소스 유형에 대한 ARNs 형식을 포함하여 AWS 변환에서 정의한 작업 및 리소스 유형에 대한 자세한 내용은 서비스 승인 참조의 [AWS 변환을 위한 작업, 리소스 및 조건 키를 참조하세요](#).

주제

- [정책 모범 사례](#)
- [AWS 변환 콘솔 사용](#)

- [사용자가 자신의 고유한 권한을 볼 수 있도록 허용](#)
- [관리자가 AWS 변환을 사용하여 계정의 커넥터 요청을 수락하도록 허용](#)
- [관리자가 기존 IAM Identity Center 사용자를 할당하고 AWS 변환에 할당할 새 IAM Identity Center 사용자를 생성하도록 허용](#)
- [관리자가 AWS 변환을 활성화하도록 허용](#)
- [사용자가 IAM 자격 증명을 사용하여 AWS 변환에 액세스하도록 허용](#)

정책 모범 사례

자격 증명 기반 정책에 따라 계정에서 사용자가 AWS 변환 리소스를 생성, 액세스 또는 삭제할 수 있는지 여부가 결정됩니다. 이 작업으로 인해 AWS 계정에 비용이 발생할 수 있습니다. ID 기반 정책을 생성하거나 편집할 때는 다음 지침과 권장 사항을 따르세요.

- AWS 관리형 정책을 시작하고 최소 권한으로 전환 - 사용자 및 워크로드에 권한 부여를 시작하려면 많은 일반적인 사용 사례에 대한 권한을 부여하는 AWS 관리형 정책을 사용합니다. 에서 사용할 수 있습니다 AWS 계정. 사용 사례에 맞는 AWS 고객 관리형 정책을 정의하여 권한을 추가로 줄이는 것이 좋습니다. 자세한 내용은 IAM 사용 설명서의 [AWS 관리형 정책](#) 또는 [AWS 직무에 대한 관리형 정책](#)을 참조하세요.
- 최소 권한 적용 - IAM 정책을 사용하여 권한을 설정하는 경우, 작업을 수행하는 데 필요한 권한만 부여합니다. 이렇게 하려면 최소 권한으로 알려진 특정 조건에서 특정 리소스에 대해 수행할 수 있는 작업을 정의합니다. IAM을 사용하여 권한을 적용하는 방법에 대한 자세한 정보는 IAM 사용 설명서에 있는 [IAM의 정책 및 권한](#)을 참조하세요.
- IAM 정책의 조건을 사용하여 액세스 추가 제한 - 정책에 조건을 추가하여 작업 및 리소스에 대한 액세스를 제한할 수 있습니다. 예를 들어, SSL을 사용하여 모든 요청을 전송해야 한다고 지정하는 정책 조건을 작성할 수 있습니다. AWS 서비스와 같은 특징을 통해 사용되는 경우 조건을 사용하여 서비스 작업에 대한 액세스 권한을 부여할 수도 있습니다 CloudFormation. 자세한 내용은 IAM 사용 설명서의 [IAM JSON 정책 요소: 조건](#)을 참조하세요.
- IAM Access Analyzer를 통해 IAM 정책을 확인하여 안전하고 기능적인 권한 보장 - IAM Access Analyzer에서는 IAM 정책 언어(JSON)와 모범 사례가 정책에서 준수되도록 새로운 및 기존 정책을 확인합니다. IAM Access Analyzer는 100개 이상의 정책 확인 항목과 실행 가능한 추천을 제공하여 안전하고 기능적인 정책을 작성하도록 돕습니다. 자세한 내용은 IAM 사용 설명서의 [IAM Access Analyzer에서 정책 검증](#)을 참조하세요.
- 다중 인증(MFA) 필요 -에서 IAM 사용자 또는 루트 사용자가 필요한 시나리오가 있는 경우 추가 보안을 위해 MFA를 AWS 계정입니다. API 작업을 직접적으로 호출할 때 MFA가 필요하다면 정책에 MFA 조건을 추가합니다. 자세한 내용은 IAM 사용 설명서의 [MFA를 통한 보안 API 액세스](#)를 참조하세요.

IAM의 모범 사례에 대한 자세한 내용은 IAM 사용 설명서의 [IAM의 보안 모범 사례](#)를 참조하세요.

AWS 변환 콘솔 사용

AWS 변환 콘솔에 액세스하려면 최소 권한 집합이 있어야 합니다. 이러한 권한은에서 AWS 변환 리소스에 대한 세부 정보를 나열하고 볼 수 있도록 허용해야 합니다 AWS 계정. 최소 필수 권한보다 더 제한적인 ID 기반 정책을 생성하는 경우, 콘솔이 해당 정책에 연결된 엔티티(사용자 또는 역할)에 대해 의도대로 작동하지 않습니다.

AWS CLI 또는 AWS API만 호출하는 사용자에게는 최소 콘솔 권한을 허용할 필요가 없습니다. 대신, 수행하려는 API 작업과 일치하는 작업에만 액세스할 수 있도록 합니다.

사용자가 자신의 고유한 권한을 볼 수 있도록 허용

이 예제는 IAM 사용자가 자신의 사용자 ID에 연결된 인라인 및 관리형 정책을 볼 수 있도록 허용하는 정책을 생성하는 방법을 보여줍니다. 이 정책에는 콘솔에서 또는 AWS CLI 또는 AWS API를 사용하여 프로그래밍 방식으로이 작업을 완료할 수 있는 권한이 포함됩니다.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "ViewOwnUserInfo",
      "Effect": "Allow",
      "Action": [
        "iam:GetUserPolicy",
        "iam:ListGroupsForUser",
        "iam:ListAttachedUserPolicies",
        "iam:ListUserPolicies",
        "iam:GetUser"
      ],
      "Resource": ["arn:aws:iam::*:user/${aws:username}"]
    },
    {
      "Sid": "NavigateInConsole",
      "Effect": "Allow",
      "Action": [
        "iam:GetGroupPolicy",
        "iam:GetPolicyVersion",
        "iam:GetPolicy",
        "iam:ListAttachedGroupPolicies",
        "iam:ListGroupPolicies",

```

```

        "iam:ListPolicyVersions",
        "iam:ListPolicies",
        "iam:ListUsers"
    ],
    "Resource": "*"
}
]
}

```

관리자가 AWS 변환을 사용하여 계정의 커넥터 요청을 수락하도록 허용

JSON

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "transform:GetConnector",
        "transform:AssociateConnectorResource",
        "transform:RejectConnector"
      ],
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": [
        "s3:GetBucketPublicAccessBlock",
        "s3:GetAccountPublicAccessBlock"
      ],
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": [
        "iam:CreateRole",
        "iam:AttachRolePolicy",
        "iam:PassRole"
      ],
      "Resource": "arn:aws:iam::111122223333:role/service-role/AWSTransform-*"
    }
  ]
}

```

```

    },
    {
      "Effect": "Allow",
      "Action": [
        "iam:CreatePolicy"
      ],
      "Resource": "arn:aws:iam::111122223333:policy/service-role/
AWSTransform-*"
    }
  ]
}

```

관리자가 기존 IAM Identity Center 사용자를 할당하고 AWS 변환에 할당할 새 IAM Identity Center 사용자를 생성하도록 허용

다음 정책은 관리자가 AWS 변환 콘솔에서 IAM Identity Center 사용자 및 그룹을 관리하는 데 필요한 권한을 부여합니다. 이 정책을 사용하면 관리자가 사용자 및 그룹을 할당 및 제거하고, 표시 이름을 보고, 새 IAM Identity Center 사용자를 생성하고, 애플리케이션 할당을 관리하고, 애플리케이션 세션 설정을 구성할 수 있습니다.

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "SSOApplicationAssignments",
      "Effect": "Allow",
      "Action": [
        "sso:ListApplicationAssignments",
        "sso:CreateApplicationAssignment",
        "sso:DeleteApplicationAssignment",
        "sso:ListInstances",
        "sso:DescribeInstance",
        "sso:ListDirectoryAssociations",
        "sso:GetApplicationGrant",
        "sso:GetApplicationAccessScope",
        "sso:GetApplicationSessionConfiguration",
        "sso:PutApplicationSessionConfiguration"
      ],
      "Resource": "*"
    },
    {

```

```

    "Sid": "SSODirectoryCreateUser",
    "Effect": "Allow",
    "Action": [
        "sso-directory:CreateUser"
    ],
    "Resource": "*"
},
{
    "Sid": "IdentityStoreAccess",
    "Effect": "Allow",
    "Action": [
        "identitystore:DescribeUser",
        "identitystore:DescribeGroup",
        "identitystore:ListUsers",
        "identitystore:ListGroups"
    ],
    "Resource": "*"
},
{
    "Sid": "AllowKmsAccessViaIdentityCenter",
    "Effect": "Allow",
    "Action": [
        "kms:Decrypt"
    ],
    "Resource": "*",
    "Condition": {
        "ArnLike": {
            "kms:EncryptionContext:aws:sso:instance-arn": "arn:*:sso:::instance/*"
        },
        "StringLike": {
            "kms:ViaService": "sso.*.amazonaws.com"
        }
    }
},
{
    "Sid": "AllowKmsAccessViaIdentityStore",
    "Effect": "Allow",
    "Action": [
        "kms:Decrypt"
    ],
    "Resource": "*",
    "Condition": {
        "ArnLike": {

```

```

    "kms:EncryptionContext:aws:identitystore:identitystore-arn":
      "arn:*:identitystore:*:identitystore/*"
    },
    "StringLike": {
      "kms:ViaService": "identitystore.*.amazonaws.com"
    }
  }
}
]
}

```

관리자가 AWS 변환을 활성화하도록 허용

다음 정책은 관리자가 AWS 콘솔을 통해 AWS 변환을 활성화하고 관리하는 데 필요한 권한을 부여합니다. 여기에는 프로필 관리, 에이전트 구성, 커넥터 관리가 포함됩니다. 이 정책은 관리자 전용이며 계정의 신뢰할 수 있는 보안 주체로 범위가 지정되어야 합니다.

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "SSOEnableTransform",
      "Effect": "Allow",
      "Action": [
        "sso:ListInstances",
        "sso:CreateInstance",
        "sso:CreateApplication",
        "sso:PutApplicationAuthenticationMethod",
        "sso:PutApplicationGrant",
        "sso:PutApplicationAssignmentConfiguration",
        "sso:ListApplications",
        "sso:GetSharedSsoConfiguration",
        "sso:DescribeInstance",
        "sso:PutApplicationAccessScope",
        "sso:DescribeApplication",
        "sso>DeleteApplication",
        "sso:UpdateApplication",
        "sso:DescribeRegisteredRegions",
        "sso:GetSSOStatus"
      ],
      "Resource": "*"
    },
    {

```

```
"Sid": "SSODirectoryActions",
"Effect": "Allow",
"Action": [
    "sso-directory:GetUserPoolInfo",
    "sso-directory:DescribeUsers",
    "sso-directory:DescribeGroups",
    "sso-directory:SearchGroups",
    "sso-directory:SearchUsers",
    "sso-directory:DescribeDirectory"
],
"Resource": "*"
},
{
    "Sid": "KMSListAliases",
    "Effect": "Allow",
    "Action": [
        "kms:ListAliases"
    ],
    "Resource": "*"
},
{
    "Sid": "KMSActions",
    "Effect": "Allow",
    "Action": [
        "kms:CreateGrant",
        "kms:Encrypt",
        "kms:Decrypt",
        "kms:GenerateDataKey*",
        "kms:RetireGrant",
        "kms:DescribeKey"
    ],
    "Resource": "*",
    "Condition": {
        "StringLike": {
            "kms:ViaService": "transform.*.amazonaws.com"
        }
    }
},
{
    "Sid": "IAMServiceLinkedRole",
    "Effect": "Allow",
    "Action": [
        "iam:CreateServiceLinkedRole"
    ],
```



```

    "Resource": [
      "arn:*:iam:*:role/aws-service-role/transform.amazonaws.com/
AWSServiceRoleForAWSTransform"
    ]
  },
  {
    "Sid": "TransformConsoleActions",
    "Effect": "Allow",
    "Action": [
      "transform:GetAccountSettings",
      "transform:UpdateAccountSettings",
      "transform:CreateProfile",
      "transform:UpdateProfile",
      "transform:DeleteProfile",
      "transform:ListProfiles",
      "transform:GetConnector",
      "transform:ListConnectors",
      "transform:DeleteConnector",
      "transform:AssociateConnectorResource",
      "transform:RejectConnector",
      "transform:ListAgents",
      "transform:GetAgent",
      "transform:GetAgentRuntimeConfiguration",
      "transform:PutAgentRuntimeConfiguration",
      "transform:UpdateAgentAccess",
      "transform:TagResource",
      "transform:UntagResource",
      "transform:ListTagsForResource",
      "transform:GetWebAppUrl"
    ],
    "Resource": "*"
  }
]
}

```

사용자가 IAM 자격 증명을 사용하여 AWS 변환에 액세스하도록 허용

다음 정책은 IAM 보안 인증 정보를 사용하여 IAM 보안 주체에게 AWS 변환 웹 애플리케이션 및 APIs에 대한 액세스 권한을 부여합니다. 이 정책은 IAM 전용 액세스 및 자격 증명 공급자와 함께 활성화된 IAM 액세스에 필요합니다.

region, *account-id* 및 *profile-id*를 값으로 바꿉니다. 프로필 ID는 AWS 변환 콘솔의 설정에서 찾을 수 있습니다.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowTransformAccess",
      "Effect": "Allow",
      "Action": "transform:AccessTransformProfile",
      "Resource": "arn:aws:transform:region:account-id:profile/profile-id"
    }
  ]
}
```

계정의 모든 프로필에 대한 액세스 권한을 부여하려면 프로필 ID에 와일드카드를 사용합니다.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowTransformAccessAllProfiles",
      "Effect": "Allow",
      "Action": "transform:AccessTransformProfile",
      "Resource": "arn:aws:transform:region:account-id:profile/*"
    }
  ]
}
```

Note

`transform:AccessTransformProfile` 작업은 AWS 변환에 대한 액세스 권한만 부여합니다. 워크스페이스 내의 작업은 IAM 정책이 아닌 AWS 변환 워크스페이스 역할(관리자, 기여자, 승인자, 읽기 전용)에 의해 제어됩니다. Workspace 역할은 작업 생성, 공동 작업자 관리, 작업 승인 등 사용자가 수행할 수 있는 작업을 결정합니다.

자격 증명 및 액세스 AWS 변환 문제 해결

다음 정보를 사용하여 AWS 변환 및 IAM 작업 시 발생할 수 있는 일반적인 문제를 진단하고 수정할 수 있습니다.

주제

- [AWS 변환에서 작업을 수행할 권한이 없음](#)
- [iam:PassRole을 수행하도록 인증되지 않음](#)
- [내 외부의 사람이 내 AWS 변환 리소스 AWS 계정 에 액세스하도록 허용하고 싶습니다.](#)

AWS 변환에서 작업을 수행할 권한이 없음

작업을 수행할 권한이 없다는 오류가 표시되면 작업을 수행할 수 있도록 정책을 업데이트해야 합니다.

다음의 예제 오류는 mateojackson IAM 사용자가 콘솔을 사용하여 가상 *my-example-widget* 리소스에 대한 세부 정보를 보려고 하지만 가상 AWS Transform:*GetWidget* 권한이 없을 때 발생합니다.

```
User: arn:aws:iam::123456789012:user/mateojackson is not authorized to perform: AWS Transform:GetWidget on resource: my-example-widget
```

이 경우, AWS Transform:*GetWidget* 작업을 사용하여 *my-example-widget* 리소스에 액세스할 수 있도록 mateojackson 사용자 정책을 업데이트해야 합니다.

도움이 필요한 경우 AWS 관리자에게 문의하세요. 관리자는 로그인 자격 증명을 제공한 사람입니다.

iam:PassRole을 수행하도록 인증되지 않음

iam:PassRole 작업을 수행할 권한이 없다는 오류가 수신되면 AWS 변환에 역할을 전달할 수 있도록 정책을 업데이트해야 합니다.

일부 AWS 서비스에서는 새 서비스 역할 또는 서비스 연결 역할을 생성하는 대신 기존 역할을 해당 서비스에 전달할 수 있습니다. 이렇게 하려면 역할을 서비스에 전달할 권한이 있어야 합니다.

다음 예제 오류는 라는 IAM 사용자가 콘솔을 사용하여 AWS 변환에서 작업을 수행하려고 marymajor 할 때 발생합니다. 하지만 작업을 수행하려면 서비스 역할이 부여한 권한이 서비스에 있어야 합니다. Mary는 서비스에 역할을 전달할 권한이 없습니다.

```
User: arn:aws:iam::123456789012:user/marymajor is not authorized to perform: iam:PassRole
```

이 경우, Mary가 iam:PassRole작업을 수행할 수 있도록 Mary의 정책을 업데이트해야 합니다.

도움이 필요한 경우 AWS 관리자에게 문의하세요. 관리자는 로그인 자격 증명을 제공한 사람입니다.

내 외부의 사람이 내 AWS 변환 리소스 AWS 계정 에 액세스하도록 허용하고 싶습니다.

다른 계정의 사용자 또는 조직 외부의 사람이 리소스에 액세스할 때 사용할 수 있는 역할을 생성할 수 있습니다. 역할을 수임할 신뢰할 수 있는 사람을 지정할 수 있습니다. 리소스 기반 정책 또는 액세스 제어 목록(ACL)을 지원하는 서비스의 경우, 이러한 정책을 사용하여 다른 사람에게 리소스에 대한 액세스 권한을 부여할 수 있습니다.

자세한 내용은 다음을 참조하세요.

- AWS 변환이 이러한 기능을 지원하는지 여부를 알아보려면 섹션을 참조하세요 [AWS 변환이 IAM과 작동하는 방식](#).
- 소유 AWS 계정 한의 리소스에 대한 액세스 권한을 제공하는 방법을 알아보려면 [IAM 사용 설명서의 소유한 다른의 IAM 사용자에게 액세스 권한 제공을 참조 AWS 계정 하세요](#).
- 리소스에 대한 액세스 권한을 타사에 제공하는 방법을 알아보려면 IAM 사용 설명서의 [타사 AWS 계정 소유에 대한 액세스 권한 제공을](#) AWS 계정참조하세요.
- ID 페더레이션을 통해 액세스 권한을 제공하는 방법을 알아보려면 IAM 사용 설명서의 [외부에서 인증된 사용자에게 액세스 권한 제공\(ID 페더레이션\)](#)을 참조하세요.
- 크로스 계정 액세스에 대한 역할과 리소스 기반 정책 사용의 차이점을 알아보려면 IAM 사용 설명서의 [IAM의 크로스 계정 리소스 액세스](#)를 참조하세요.

에 대한 서비스 연결 역할 사용 AWS Transform

AWS Transform 는 AWS Identity and Access Management (IAM) [서비스 연결 역할](#)을 사용합니다. 서비스 연결 역할은 직접 연결된 고유한 유형의 IAM 역할입니다 AWS Transform. 서비스 연결 역할은에서 사전 정의 AWS Transform 하며 서비스가 사용자를 대신하여 다른 AWS 서비스를 호출하는 데 필요한 모든 권한을 포함합니다.

에 대한 서비스 연결 역할 사용 AWS Transform

AWS Transform 는 AWS Identity and Access Management (IAM) [서비스 연결 역할](#)을 사용합니다. 서비스 연결 역할은 직접 연결된 고유한 유형의 IAM 역할입니다 AWS Transform. 서비스 연결 역할은에서 사전 정의 AWS Transform 하며 서비스가 사용자를 대신하여 다른 AWS 서비스를 호출하는 데 필요한 모든 권한을 포함합니다.

필요한 권한을 수동으로 추가할 필요가 없으므로 서비스 연결 역할을 더 AWS Transform 쉽게 설정할 수 있습니다.는 서비스 연결 역할의 권한을 AWS Transform 정의하며, 달리 정의되지 않은 한 만 해당

역할을 수임할 AWS Transform 수 있습니다. 정의된 권한에는 신뢰 정책과 권한 정책이 포함되며 이 권한 정책은 다른 IAM 엔터티에 연결할 수 없습니다.

먼저 관련 리소스를 삭제한 후에만 서비스 연결 역할을 삭제할 수 있습니다. 이렇게 하면 AWS Transform 리소스에 대한 액세스 권한을 실수로 제거할 수 없기 때문에 리소스가 보호됩니다.

서비스 연결 역할을 지원하는 다른 서비스에 대한 자세한 내용은 [AWS IAM으로 작업하는 서비스를](#) 참조하고 서비스 연결 역할 열에서 Yes가 있는 서비스를 찾습니다. 해당 서비스에 대한 서비스 연결 역할 설명서를 보려면 예 링크를 선택합니다.

에 대한 서비스 연결 역할 권한 AWS Transform

AWS Transform 는 [AWSServiceRoleForAWSTransform](#)이라는 서비스 연결 역할을 사용합니다.이 서비스 연결 역할은 AWS 변환에 사용 정보를 제공하는 기능을 제공합니다.

AWSServiceRoleForAWSTransform 서비스 연결 역할은 역할을 수임하기 위해 다음 서비스를 신뢰합니다.

- transform.amazonaws.com

AWSServiceRoleForAWSTransform이라는 역할 권한 정책은가 지정된 리소스에서 다음 작업을 완료 AWS Transform 하도록 허용합니다.

- cloudwatch:PutMetricData
 - AWS Transform 작업을 위해 CloudWatch로 사용자 지정 지표 전송
 - 변환 진행 상황, 성공률 및 성능 지표 추적
 - 변환 워크플로에 대한 모니터링 및 알림 활성화
- sso:DescribeApplication
 - Identity Center에서 특정 애플리케이션에 대한 세부 정보 보기
 - 이름, 설명, 상태 및 구성과 같은 애플리케이션 메타데이터 가져오기
- sso:GetApplicationAssignmentConfiguration
 - 애플리케이션에 대한 할당 구성 설정 검색
 - 사용자/그룹이 애플리케이션에 할당되도록 구성된 방법 확인
- sso:ListApplicationAssignmentsForPrincipal
 - 특정 사용자 또는 그룹에 할당된 모든 애플리케이션 나열(보안 주체)
 - 특정 자격 증명이 액세스할 수 있는 애플리케이션 보기

- IAM Identity Center를 통해 액세스할 때 KMS로 암호화된 데이터의 복호화를 활성화합니다. 암호화 컨텍스트에 유효한 IAM Identity Center 인스턴스 ARN이 포함되어 있고 IAM Identity Center 서비스 엔드포인트를 통해 액세스해야 하는 경우에만 작동합니다.
- Identity Store를 통해 액세스할 때 KMS로 암호화된 데이터의 복호화를 허용합니다. 암호화 컨텍스트에 유효한 Identity Store ARN이 포함되어 있고 Identity Store 서비스 엔드포인트를 통해 액세스해야 하는 경우에만 작동합니다.
- secretsmanager:GetSecretValue
 - 외부 자격 증명 공급자의 클라이언트 보안 암호를 저장하는 데 사용되는 AWS Transform 서비스 연결 보안 암호 액세스
 - 리소스: arn:aws:secretsmanager:*:*:secret:transform-preprod!*
 - 조건: transform-preprod 서비스가 소유하고 동일한 계정에서 액세스해야 합니다.
- support:CreateCase, support:DescribeCases, support:DescribeCommunications, support:AddCommunicationToCase, support:ResolveCase
 - AWS Transform 웹 애플리케이션에서 프리미엄 지원 사례 생성 및 관리
 - 사례 세부 정보 및 커뮤니케이션 보기
 - 커뮤니케이션 추가 및 지원 사례 해결

사용자, 그룹 또는 역할이 서비스 연결 역할을 생성, 편집 또는 삭제할 수 있도록 사용 권한을 구성해야 합니다. 자세한 내용은 IAM 사용 설명서의 [서비스 연결 역할 권한](#)을 참조하세요.

에 대한 서비스 연결 역할 생성 AWS Transform

서비스 연결 역할은 수동으로 생성할 필요가 없습니다. AWS Transform 에서에 대한 프로필을 생성하면 서비스 연결 역할을 AWS Management Console AWS Transform 생성합니다.

이 서비스 연결 역할을 삭제했다가 다시 생성해야 하는 경우 동일한 프로세스를 사용하여 계정에서 역할을 다시 생성할 수 있습니다. 설정을 AWS Transform 업데이트하면에서 서비스 연결 역할을 다시 생성합니다.

IAM 콘솔 또는 AWS CLI를 사용하여 서비스 이름으로 transform.amazonaws.com 서비스 연결 역할을 생성할 수도 있습니다. 자세한 내용은 IAM 사용자 설명서의 [서비스 연결 역할 생성](#) 섹션을 참조하세요. 이 서비스 연결 역할을 삭제하면 동일한 프로세스를 사용하여 역할을 다시 생성할 수 있습니다.

에 대한 서비스 연결 역할 편집 AWS Transform

AWS Transform에서는 AWSServiceRoleForAWSTransform 서비스 연결 역할을 편집할 수 없습니다. 서비스 연결 역할을 생성한 후에는 다양한 개체가 역할을 참조할 수 있기 때문에 역할 이름을 변경할

수 없습니다. 하지만 IAM을 사용하여 역할의 설명을 편집할 수 있습니다. 자세한 내용은 IAM 사용 설명서의 [서비스 연결 역할 편집](#)을 참조하세요.

에 대한 서비스 연결 역할 삭제 AWS Transform

서비스 연결 역할이 필요한 기능 또는 서비스가 더 이상 필요 없는 경우에는 해당 역할을 삭제할 것을 권장합니다. 이렇게 하면 적극적으로 모니터링하거나 유지 관리하지 않은 미사용 엔터티가 없습니다. 단, 서비스 연결 역할에 대한 리소스를 먼저 정리해야 수동으로 삭제할 수 있습니다.

Note

리소스를 삭제하려고 할 때 AWS Transform 서비스가 역할을 사용하는 경우 삭제에 실패할 수 있습니다. 이 문제가 발생하면 몇 분 기다렸다가 작업을 다시 시도하세요.

IAM을 사용하여 수동으로 서비스 연결 역할을 삭제하려면 다음을 수행하세요.

IAM 콘솔 AWS CLI, 또는 AWS API를 사용하여 AWSServiceRoleForAWSTransform 서비스 연결 역할을 삭제합니다. 자세한 내용은 IAM 사용 설명서의 [서비스 연결 역할 삭제](#)를 참조하십시오.

AWS Transform 서비스 연결 역할에 지원되는 리전

AWS Transform 는 서비스를 사용할 수 있는 모든 리전에서 서비스 연결 역할 사용을 지원하지 않습니다. 다음 리전에서 AWSServiceRoleForAWSTransform 역할을 사용할 수 있습니다. 자세한 내용은 [AWS 리전 및 엔드포인트](#) 섹션을 참조하세요.

리전 이름	리전 자격 증명	에서 지원 AWS Transform
미국 동부(버지니아 북부)	us-east-1	예
유럽(프랑크푸르트)	eu-central-1	예

AWS Transform Custom에 서비스 연결 역할 사용

AWS Transform Custom은 AWSServiceRoleForAWSTransformCustom이라는 서비스 연결 역할을 사용하여 사용자를 대신하여 지표와 로그를 계정에 게시합니다. 이러한 지표를 사용하면 대시보드에서 직접 변환 수, 지연 시간 및 상태 코드를 모니터링할 수 있습니다. 로그는 변환 중에 발생하는 문제에 대한 가시성을 제공합니다.

이 [서비스 연결 역할](#)은 AWS Transform Custom에서 사전 정의하며 서비스에 필요한 권한만 포함합니다. 권한을 수동으로 추가할 필요는 없으며 역할은 AWS Transform Custom에서만 수임할 수 있습니다. 서비스 연결 역할에 대한 일반적인 내용은 IAM 사용 설명서의 [서비스 연결 역할 사용](#)을 참조하세요.

AWS Transform Custom에 대한 서비스 연결 역할 권한

AWSServiceRoleForAWSTransformCustom 서비스 연결 역할은 역할을 수임하기 위해 다음 서비스를 신뢰합니다.

- `transform-custom.amazonaws.com`

AWSServiceRoleForAWSTransformCustom이라는 역할 권한 정책은 AWS Transform Custom이 지정된 리소스에서 다음 작업을 완료하도록 허용합니다.

- `cloudwatch:PutMetricData` 모든 AWS 리소스의
 - AWS/TransformCustom 네임스페이스 아래의 운영 지표 게시
 - 변환 수, 지연 시간 및 상태 코드 추적
 - `cloudwatch:namespace` 조건 키를 통해 AWS/TransformCustom 네임스페이스로 범위가 지정됨
- `logs:CreateLogGroup` `logs:PutRetentionPolicy` /aws/TransformCustom 로그 그룹의 및
 - 변환 로그를 게시하기 위한 CloudWatch Logs 로그 그룹 생성
 - 로그 그룹에 로그 보존 정책 설정
 - 계정 내에서만 액세스를 보장하는 `aws:ResourceAccount` 조건으로 범위가 `arn:aws:logs:*:*:log-group:/aws/TransformCustom`로 지정됨
- `logs:CreateLogStream` 로그 그룹 내의 /aws/TransformCustom 로그 스트림 `logs:PutLogEvents`에 대한 및
 - 변환 작업에 대한 로그 스트림 생성 및 로그 이벤트 게시
 - 계정 내에서만 액세스를 보장하는 `aws:ResourceAccount` 조건으로 범위가 `arn:aws:logs:*:*:log-group:/aws/TransformCustom:log-stream:*`로 지정됨

사용자, 그룹 또는 역할이 서비스 연결 역할을 생성, 편집 또는 삭제할 수 있도록 사용 권한을 구성해야 합니다. 자세한 내용은 IAM 사용 설명서의 [서비스 연결 역할 권한](#)을 참조하세요.

AWS Transform Custom에 대한 서비스 연결 역할 생성

서비스 연결 역할은 수동으로 생성할 필요가 없습니다. AWS Transform Custom CLI를 사용하여 변환을 실행하면 AWS Transform Custom이 서비스 연결 역할을 생성합니다.

이 서비스 연결 역할을 삭제했다가 다시 생성해야 하는 경우 동일한 프로세스를 사용하여 계정에서 역할을 다시 생성할 수 있습니다. AWS Transform Custom CLI를 사용하여 변환을 실행하면 AWS Transform Custom이 서비스 연결 역할을 다시 생성합니다.

IAM 콘솔을 사용하여 `AWSServiceRoleForAWSTransformCustom` 사용 사례로 서비스 연결 역할을 생성할 수도 있습니다. AWS CLI 또는 AWS API에서 서비스 이름으로 `transform-custom.amazonaws.com` 서비스 연결 역할을 생성합니다. 자세한 내용은 IAM 사용자 설명서의 [서비스 연결 역할 생성](#) 섹션을 참조하세요. 이 서비스 연결 역할을 삭제하면 동일한 프로세스를 사용하여 역할을 다시 생성할 수 있습니다.

AWS Transform Custom에 대한 서비스 연결 역할 편집

AWS Transform Custom에서는 `AWSServiceRoleForAWSTransformCustom` 서비스 연결 역할을 편집할 수 없습니다. 서비스 연결 역할을 생성한 후에는 다양한 개체가 역할을 참조할 수 있기 때문에 역할 이름을 변경할 수 없습니다. 하지만 IAM을 사용하여 역할의 설명을 편집할 수 있습니다. 자세한 내용은 IAM 사용자 설명서의 [서비스 연결 역할 편집](#)을 참조하세요.

AWS Transform Custom에 대한 서비스 연결 역할 삭제

서비스 연결 역할이 필요한 기능 또는 서비스가 더 이상 필요 없는 경우에는 해당 역할을 삭제할 것을 권합니다. 그렇게 하면 적극적으로 모니터링하거나 유지 관리하지 않은 미사용 엔터티가 없습니다.

`AWSServiceRoleForAWSTransformCustom` 서비스 연결 역할은 계정에 영구 리소스를 생성하지 않습니다. 리소스 정리 없이 직접 삭제할 수 있습니다.

이 역할을 삭제한 후 나중에 AWS Transform Custom CLI를 사용하여 변환을 실행하면 서비스 연결 역할이 자동으로 다시 생성됩니다.

IAM을 사용하여 수동으로 서비스 연결 역할을 삭제하려면 다음을 수행하세요.

IAM 콘솔, AWS CLI, 또는 AWS API를 사용하여 `AWSServiceRoleForAWSTransformCustom` 서비스 연결 역할을 삭제합니다. 자세한 내용은 IAM 사용자 설명서의 [서비스 연결 역할 삭제](#)를 참조하십시오.

사용자 지정 서비스 연결 역할 AWS 변환에 지원되는 리전

AWS Transform Custom은 AWS Transform Custom을 사용할 수 있는 모든 리전에서 서비스 연결 역할 사용을 지원합니다. 지원되는 리전 목록은 [지원되는 리전을 참조하세요](#).

AWS AWS 변환에 대한 관리형 정책

AWS 관리형 정책은에서 생성하고 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 권한을 부여하지 않을 수 있습니다. 사용 사례에 고유한 [고객 관리형 정책](#)을 정의하여 권한을 줄이는 것이 좋습니다.

AWS 관리형 정책에 정의된 권한은 변경할 수 없습니다. 가 관리형 정책에 정의된 권한을 AWS 업데이트하는 AWS 경우 업데이트는 정책이 연결된 모든 보안 주체 자격 증명(사용자, 그룹 및 역할)에 영향을 줍니다. AWS AWS 서비스 는 새가 시작되거나 기존 서비스에 새 API 작업을 사용할 수 있게 될 때 AWS 관리형 정책을 업데이트할 가능성이 높습니다.

자세한 내용은 IAM 사용자 가이드의 [AWS 관리형 정책](#)을 참조하세요.

AWS AWS 관리형 정책에 대한 업데이트 변환

2021년 3월 1일 이후 AWS 변환의 AWS 관리형 정책 업데이트에 대한 세부 정보를 봅니다.

변경	설명	Date
AWSTransformInfrastructureExecutorAccessBatch – 새 정책	소스 코드 업로드, 결과 검색, AWS 배치 작업 상태 모니터링, 로그 읽기, 변환 일정 관리를 포함하여 배치를 사용하여 연속 현대화 AWS 변환 평가 및 변환을 실행하는 데 필요한 권한을 부여하는 새로운 AWS 관리형 정책이 추가되었습니다.	2026년 7월 20일
AWSTransformInfrastructureExecutorAccessEC2 – 새 정책	소스 코드 업로드, 결과 검색, 작업 상태 모니터링, AWS 변환 일정 관리를 포함하여 Amazon EC2를 사용하여 연속 현대화 변환 평가 및 변환을 실행하는 데 필요한 권한을 부여하는 새	2026년 7월 20일

변경	설명	Date
	로운 AWS 관리형 정책이 추가되었습니다.	
AWSTransformSecurityAgentExecutorAccess – 새 정책	스캔 아티팩트 업로드 및 조사 결과 검색을 포함하여 자동화된 코드 보안 검토 및 문제 해결을 위해 AWS Security Agent 서비스를 호출하는 데 필요한 권한을 AWS Transform Continuous Modernization에 부여하는 새로운 AWS 관리형 정책이 추가되었습니다.	2026년 6월 30일
AWSServiceRoleForAWSTransformCustom – 업데이트된 정책	사용자 지정 AWS 변환이 계정의 로그 그룹에 로그를 게시할 수 있도록 CloudWatch /aws/TransformCustom Logs 권한을 추가했습니다.	2026년 5월 5일
AWSTransformCustomExecuteTransformations – 업데이트된 정책	CloudWatch 지표를 고객 계정으로 내보낼 수 있도록 사용자 지정 서비스 연결 역할 AWS 변환(AWSServiceRoleForAWSTransformCustom)을 생성할 수 있는 권한이 추가되었습니다.	2026년 4월 27일
AWSTransformCustomManageTransformations – 업데이트된 정책	CloudWatch 지표를 고객 계정으로 내보낼 수 있도록 사용자 지정 서비스 연결 역할 AWS 변환(AWSServiceRoleForAWSTransformCustom)을 생성할 수 있는 권한이 추가되었습니다.	2026년 4월 27일

변경	설명	Date
AWSTransformCustomFullAccess – 업데이트된 정책	CloudWatch 지표를 고객 계정으로 내보낼 수 있도록 사용자 지정 서비스 연결 역할 AWS 변환(AWSServiceRoleForAWSTransformCustom)을 생성할 수 있는 권한이 추가되었습니다.	2026년 4월 7일
AWSServiceRoleForAWSTransformCustom – 새 정책	사용자 지정 서비스 연결 역할 AWS 변환에 대한 새 AWS 관리형 정책이 추가되었습니다. 이 정책은 사용자 지정 AWS 변환이 CloudWatch 지표를 계정에 게시하도록 허용합니다.	2026년 3월 23일
DBModProvisioningAndMigration – 새 정책	이 정책은 데이터베이스 프로비저닝 및 마이그레이션 기능을 부여합니다.	2026년 3월 24일
DBModDiscoveryAndAssessment – 새 정책	포괄적인 데이터베이스 현대화 검색 및 평가 기능을 제공하는 새로운 AWS 관리형 정책이 추가되었습니다.	2026년 3월 24일
AWSTransformCustomFullAccess – 새 정책	사용자 지정 AWS 변환에 대한 전체 액세스를 제공하는 새로운 AWS 관리형 정책이 추가되었습니다.	2025년 12월 5일
AWSTransformCustomExecuteTransformations – 새 정책	사용자 지정 변환에서 변환을 실행할 수 있는 액세스 권한을 제공하는 새 AWS 관리형 정책이 추가되었습니다.	2025년 12월 5일

변경	설명	Date
AWSTransformCustomManageTransformations – 새 정책	AWS 변환 사용자 지정에서 변환 리소스를 생성, 업데이트, 읽기 및 삭제하고 변환을 실행할 수 있는 액세스 권한을 제공하는 새로운 AWS 관리형 정책이 추가되었습니다.	2025년 12월 5일
AWSServiceRoleForAWSTransform – 업데이트된 정책	외부 자격 증명 공급자의 클라이언트 암호를 저장하는 데 사용되는 AWS 변환 서비스 연결 보안 암호에 액세스할 수 있는 권한이 추가되었습니다. AWS 변환 웹 앱에서 프리미엄 지원 사례를 생성할 수 있는 권한이 추가되었습니다.	2025년 12월 1일
AWSTransformApplicationECSDeploymentPolicy – 업데이트된 정책	ECR 암호화 지원을 위한 IAM 역할 검사 권한, ECS 서비스 연결 역할 생성 및 KMS 권한이 추가되었습니다.	2025년 11월 22일
AWSTransformApplicationDeploymentPolicy – 업데이트된 정책	EC2 네트워킹 권한, IAM 역할 검사 권한, S3 버킷 목록 권한 및 향상된 배포 기능에 대한 KMS 암호화 지원이 추가되었습니다.	2025년 11월 22일
AWSServiceRoleForAWSTransform – 업데이트된 정책	IAM Identity Center의 고객 관리형 키에 대한 지원이 추가되었습니다.	2025년 9월 17일

변경	설명	Date
AWSTransformApplicationDeploymentPolicy – 새 정책	Amazon EC2 인스턴스, CloudFormation 스택 및 관련 리소스를 생성하고 관리하여 AWS 변환이 변환된 .NET 애플리케이션을 배포할 수 있도록 하는 새로운 AWS 관리형 정책이 추가되었습니다.	2025년 8월 28일
AWSServiceRoleForAWSTransform – 업데이트된 정책	새 정책을 추가했습니다.	2025년 5월 15일

AWS 관리형 정책: AWSServiceRoleForAWSTransform

이 정책은 [AWSServiceRoleForAWSTransform](#) 서비스 연결 역할(SLR)에 연결됩니다.

권한 세부 정보

정책 권한 세부 정보를 보려면 AWS 관리형 정책 참조 안내서의 [AWSServiceRoleForAWSTransform](#)을 참조하세요.

AWS 관리형 정책: AWSServiceRoleForAWSTransformCustom

이 정책은 [AWSServiceRoleForAWSTransformCustom](#) 서비스 연결 역할(SLR)에 연결됩니다. 이 역할을 통해 AWS Transform custom은 사용자를 대신하여 CloudWatch 지표 및 로그를 계정에 게시할 수 있습니다.

설명

이 정책에는 다음 권한이 포함되어 있습니다.

- Amazon CloudWatch - AWS/TransformCustom 네임스페이스에서 CloudWatch에 지표를 게시할 수 있습니다. 이를 통해 CloudWatch 대시보드에서 변환 수, 지연 시간 및 상태 코드를 모니터링할 수 있습니다.
- Amazon CloudWatch Logs - 로그 그룹, 로그 스트림을 생성하고, 보존 정책을 설정하고, 로그 이벤트를 /aws/TransformCustom 로그 그룹에 게시할 수 있습니다. 이를 통해 변환 중에 발생하는 문제를 파악할 수 있습니다.

AWS 관리형 정책: AWSTransformApplicationDeploymentPolicy

이 정책을 통해 AWS 변환은 Amazon EC2 인스턴스, CloudFormation 스택 및 관련 리소스를 생성하고 관리하여 변환된 .NET 애플리케이션을 배포할 수 있습니다.

설명

이 정책에는 다음 권한이 포함되어 있습니다.

- CloudFormation - AWSTransform으로 시작하는 이름으로 CloudFormation 스택을 생성, 업데이트, 삭제 및 설명할 수 있습니다. 스택 작업은 CreatedBy: AWSTransform 태그가 지정된 리소스로 제한되며 동일한 AWS 계정으로 제한됩니다.
- Amazon EC2 - VPCs, 서브넷, 보안 그룹, 이미지, 인스턴스, 라우팅 테이블 및 인터넷 게이트웨이를 설명할 수 있습니다. CloudFormation을 통해 호출된 경우에만 EC2 인스턴스를 실행, 시작, 중지, 종료 및 수정할 수 있습니다. 태그 생성은 CloudFormation 작업 중에만 특정 허용된 태그 키로 제한됩니다.
- AWS Identity and Access Management (IAM) - AWSTransform 배포 인스턴스에 대한 특정 IAM 역할을 가져오고 전달할 수 있습니다. 역할 정책 및 첨부 파일을 검사할 수 있는 권한을 포함합니다. 액세스는 동일한 AWS 계정으로 제한됩니다.
- Amazon EC2 Systems Manager(SSM) AWS- 관리형 파라미터 스토어에서 Amazon Linux AMI 파라미터를 검색하고 AWSTransform 태그가 지정된 인스턴스로 명령을 전송할 수 있습니다.
- Amazon S3 - 버킷 나열 및 동일한 AWS 계정 내에서 버킷 위치 가져오기를 포함하여 AWSTransform 배포 버킷의 객체 관리를 허용합니다.
- AWS Key Management Service (KMS) - S3 및 EC2 서비스 사용에 대한 제한과 함께 AWSTransform에 태그가 지정된 KMS 키를 사용하여 암호화 및 복호화 작업을 허용합니다.

이 정책은 리소스 수준 권한, 태그 기반 조건,를 사용한 서비스 제어 제한aws:CalledVia, 계정 수준 제한 및 명시적 거부 문을 통해 최소 권한 액세스를 구현하여 CloudFormation 작업 외부에서 무단 태그 수정을 방지합니다.

권한 세부 정보

정책 권한 세부 정보를 보려면 AWS 관리형 정책 참조 안내서의 [AWSTransformApplicationDeploymentPolicy](#)를 참조하세요.

AWS 관리형 정책: AWSTransformApplicationECSDeploymentPolicy

이 정책을 통해 AWS 변환은 ECS 클러스터, 서비스, 작업 및 관련 리소스를 생성하고 관리하여 변환된 애플리케이션을 Amazon ECS에 배포할 수 있습니다.

설명

이 정책에는 다음 권한이 포함되어 있습니다.

- CloudFormation - AWSTransform으로 시작하는 이름으로 CloudFormation 스택을 생성, 업데이트, 삭제 및 설명할 수 있습니다. 스택 작업은 CreatedBy: AWSTransform 태그가 지정된 리소스로 제한되며 동일한 AWS 계정으로 제한됩니다.
- Amazon ECS - ECS 클러스터, 서비스 및 작업 정의를 생성, 업데이트 및 삭제할 수 있습니다. 작업 실행, 작업 나열 및 작업 상태 설명을 허용합니다. 모든 작업은 이름이 AWSTransform으로 시작하고 CreatedBy: AWSTransform으로 태그가 지정된 리소스로 제한됩니다.
- AWS Identity and Access Management (IAM) - ECS 태스크(AWSTransform-Deploy-ECS-Task-Role 및 AWSTransform-Deploy-ECS-Execution-Role)에 대한 특정 IAM 역할을 가져오고 전달할 수 있습니다. 역할 정책을 검사하고 필요한 경우 ECS 서비스 연결 역할을 생성할 수 있는 권한을 포함합니다.
- Amazon CloudWatch Logs - 이름이 /aws/ecs/AWSTransform 있습니다. 배포된 애플리케이션의 문제 해결을 위한 로그 이벤트를 검색할 수 있습니다.
- Amazon ECR - 애플리케이션 컨테이너 이미지를 저장하기 위해 이름이 awstransform으로 시작하는 컨테이너 리포지토리를 생성할 수 있습니다.
- AWS Key Management Service (KMS) - 고객 관리형 KMS 키를 사용할 때 ECR 암호화를 위한 권한 부여 생성 및 데이터 키 생성을 허용합니다.

이 정책은 리소스 수준 권한, 태그 기반 조건 및 계정 수준 제한을 통해 최소 권한 액세스를 구현하여 작업이 동일한 AWS 계정 내의 AWSTransform 관리형 리소스로 제한되도록 합니다.

권한 세부 정보

정책 권한 세부 정보를 보려면 AWS 관리형 정책 참조 안내서의 [AWSTransformApplicationECSDeploymentPolicy](#)를 참조하세요.

AWS 관리형 정책: AWSTransformCustomFullAccess

이 정책은 사용자 지정 AWS 변환에 대한 전체 액세스 권한을 제공합니다.

설명

이 정책에는 다음 권한이 포함되어 있습니다.

- AWS 사용자 지정 변환 - 모든 사용자 지정 AWS 변환 리소스에 대한 모든 작업을 허용합니다. 이렇게 하면 서비스에 대한 완전한 관리 액세스 권한이 제공됩니다.
- AWS Identity and Access Management (IAM) - [사용자 지정 서비스 연결 역할](#) AWS 변환()을 생성할 수 있습니다 `AWSServiceRoleForAWSTransformCustom`. 이 역할은 사용자 지정 AWS 변환이 CloudWatch 지표 및 로그를 계정에 내보내는 데 필요합니다. 권한은이 특정 서비스 연결 역할 생성만 허용하도록 범위가 지정됩니다.

권한 세부 정보

정책 권한 세부 정보를 보려면 AWS 관리형 정책 참조 안내서의 [AWSTransformCustomFullAccess](#)를 참조하세요.

AWS 관리형 정책: AWSTransformCustomExecuteTransformations

이 정책은 사용자 지정 변환에서 AWS 변환을 실행할 수 있는 액세스 권한을 제공합니다.

설명

이 정책에는 다음 권한이 포함되어 있습니다.

- AWS 사용자 지정 변환 - 대화를 스트리밍하고, 변환을 실행하고, 캠페인을 관리할 수 있습니다. 캠페인 세부 정보를 가져오고, 캠페인 리포지토리 상태를 업데이트하고, 캠페인을 업데이트할 수 있는 권한을 포함합니다.
- AWS Identity and Access Management (IAM) - [사용자 지정 서비스 연결 역할](#) AWS 변환()을 생성할 수 있습니다 `AWSServiceRoleForAWSTransformCustom`. 이 역할은 사용자 지정 AWS 변환이 CloudWatch 지표 및 로그를 계정에 내보내는 데 필요합니다. 권한은이 특정 서비스 연결 역할 생성만 허용하도록 범위가 지정됩니다.

권한 세부 정보

정책 권한 세부 정보를 보려면 AWS 관리형 정책 참조 안내서의 [AWSTransformCustomExecuteTransformations](#)를 참조하세요.

AWS 관리형 정책: AWSTransformCustomManageTransformations

이 정책은 AWS 사용자 지정 변환에서 변환 리소스를 생성, 업데이트, 읽기 및 삭제하고 변환을 실행할 수 있는 액세스 권한을 제공합니다.

설명

이 정책에는 다음 권한이 포함되어 있습니다.

- 사용자 AWS 지정 변환 - 스트리밍 대화, 변환 실행, 변환 패키지 관리 등 변환 리소스를 포괄적으로 관리할 수 있습니다. 변환 패키지 URLs 생성, 가져오기 및 삭제하고 패키지 업로드를 완료할 수 있습니다.
- 지식 관리 - 지식 항목과 구성 및 상태를 나열, 가져오기, 삭제 및 업데이트할 수 있습니다.
- 캠페인 관리 - 캠페인 세부 정보를 가져오고, 캠페인 리포지토리 상태를 업데이트하고, 캠페인을 업데이트할 수 있습니다.
- 리소스 태그 지정 - 사용자 지정 리소스 AWS 변환에 대한 태그를 나열, 추가 및 제거할 수 있습니다.
- AWS Identity and Access Management (IAM) - [사용자 지정 서비스 연결 역할](#) `AWS 변환()`을 생성할 수 있습니다 `AWSServiceRoleForAWSTransformCustom`. 이 역할은 사용자 지정 AWS 변환이 CloudWatch 지표 및 로그를 계정에 내보내는 데 필요합니다. 권한은이 특정 서비스 연결 역할 생성만 허용하도록 범위가 지정됩니다.

권한 세부 정보

정책 권한 세부 정보를 보려면 AWS 관리형 정책 참조 안내서의 [AWSTransformCustomManageTransformations](#)를 참조하세요.

AWS 관리형 정책: AWSTransformInfrastructureExecutorAccessBatch

이 정책은 AWS 배치를 사용하여 연속 현대화 AWS 변환 평가 및 변환을 실행하는 데 필요한 권한을 부여합니다. 이 정책을 계정의 IAM 역할에 연결합니다. 연속 현대화 AWS 변환 CLI 및 에이전트는이 역할을 수임하여 소스 코드를 업로드하고, 결과를 검색하고, 배치 작업 상태를 모니터링하고, 로그를 읽고, 변환 일정을 관리합니다.

설명

이 정책에는 다음 권한이 포함되어 있습니다.

- AWS Lambda atx- 변환 워크플로를 오케스트레이션하는 접두사가 붙은 Lambda 함수의 구성을 호출하고 검색할 수 있습니다.
- Amazon S3 - 소스 코드를 `atx-source-code-*` 버킷에 업로드하고 `atx-custom-output-*` 및 `atx-ct-output-*` 버킷에서 변환 결과를 다운로드할 수 있습니다.
- AWS Key Management Service (KMS) - AWS 변환 암호화 키()를 사용하여 데이터의 암호화 및 복호화를 허용합니다 `alias/atx-encryption-key`.

- Amazon CloudWatch Logs - 변환 모니터링 및 디버깅을 위해 배치 작업 및 Lambda 실행 로그 이벤트를 읽을 수 있습니다.
- Amazon CloudWatch - 운영 가시성을 위해 AWS 변환 CLI 대시보드를 가져오고 나열할 수 있습니다.
- AWS 배치 - 컴퓨팅 환경, 작업 대기열, 작업 정의 및 작업 상태를 설명하고 나열할 수 있습니다.
- CloudFormation - 배포 상태를 확인하기 위해 AWS 변환 인프라 스택을 설명하고 나열할 수 있습니다.
- 리소스 그룹 태그 지정 API - 태그가 지정된 리소스를 검색하여 계정의 AWS 변환 인프라를 검색할 수 있습니다.
- AWS Secrets Manager - atx/ 접두사 아래에 저장된 AWS 변환 보안 암호를 검색하고 설명할 수 있습니다.
- Amazon EventBridge 스케줄러 - atx-ct 일정 그룹 내에서 예약된 변환 작업을 관리할 수 있습니다.
- Amazon EC2 - 배치 컴퓨팅 환경 네트워킹을 위한 VPC, 서브넷, 보안 그룹, 라우팅 테이블 및 NAT 게이트웨이 구성을 설명할 수 있습니다.
- AWS Identity and Access Management (IAM) ATX- 접두사 및 Atx접두사 역할 구성을 읽어 인프라 설정을 검증하고 예약된 작업을 호출AtxSchedulerInvocationRole할 수 있도록 Amazon EventBridge 스케줄러에 전달할 수 있습니다.

이 정책은 리소스 수준 권한, 태그 기반 조건, `aws:ResourceAccount` 조건 및 서비스 범위 `iam:PassedToService` 조건을 통해 최소 권한 액세스를 구현하여 작업이 동일한 AWS 계정 내의 리소스 AWS 변환으로 제한되도록 합니다.

권한 세부 정보

정책 권한 세부 정보를 보려면 AWS 관리형 정책 참조 안내서의 [AWSTransformInfrastructureExecutorAccessBatch](#)를 참조하세요.

AWS 관리형 정책: AWSTransformInfrastructureExecutorAccessEC2

이 정책은 Amazon EC2를 사용하여 AWS 연속 현대화 변환 평가 및 변환을 실행하는 데 필요한 권한을 부여합니다. 이 정책을 계정의 IAM 역할에 연결합니다. 연속 현대화 AWS 변환 CLI 및 에이전트는 이 역할을 수입하여 소스 코드를 업로드하고, 결과를 검색하고, 작업 상태를 모니터링하고, 변환 일정을 관리합니다.

설명

이 정책에는 다음 권한이 포함되어 있습니다.

- CloudFormation - 배포 전에 AWS 변환 인프라 스택, 스택 이벤트, 스택 리소스 및 드리프트 감지 상태를 설명하고, 스택을 나열하고, CloudFormation 템플릿을 검증할 수 있습니다.
- Amazon EC2 - 인스턴스, AMIs, VPCs, 서브넷, 보안 그룹, 키 페어, 라우팅 테이블, NAT 게이트웨이 및 인터넷 게이트웨이를 설명할 수 있습니다. 태그가 지정된 EC2 인스턴스를 시작하고 중지할 수 있습니다 `atx-remote-infra: true`.
- Amazon EC2 Systems Manager(SSM) - 명령 실행 상태를 모니터링하고 AWS-RunShellScript 문서 실행을 포함하여 AWS 변환 태그가 지정된 인스턴스에서 명령 및 세션을 실행할 수 있습니다.
- Amazon S3 - 객체 가져오기, 넣기, 삭제 및 버킷 나열을 포함하여 AWS 변환 버킷의 소스 코드 및 출력 아티팩트를 관리할 수 있습니다.
- AWS Key Management Service (KMS) - AWS 변환 암호화 키()를 사용하여 데이터의 암호화 및 복호화를 허용합니다 `alias/atx-encryption-key`.
- AWS Secrets Manager - `atx/` 접두사 아래에 저장된 리포지토리 자격 증명과 같은 변환 보안 암호를 검색하고 설명할 수 있습니다.
- Amazon EventBridge 스케줄러 - `atx-ct` 일정 그룹 내에서 예약된 변환 작업을 관리할 수 있습니다.
- 리소스 그룹 태그 지정 API - 태그가 지정된 리소스를 검색하여 계정의 AWS 변환 인프라를 검색할 수 있습니다.
- AWS Identity and Access Management (IAM) - `atx-transform-role*` 역할을 Amazon EC2 및 Amazon EventBridge 스케줄러 `AtxSchedulerInvocationRole`로 전달하고 EC2 인스턴스에 대한 역할 및 인스턴스 프로파일 구성을 읽을 수 있습니다.

이 정책은 리소스 수준 권한, 태그 기반 조건, `aws:ResourceAccount` 조건 및 서비스 범위 `iam:PassedToService` 조건을 통해 최소 권한 액세스를 구현하여 작업이 동일한 AWS 계정 내의 리소스 AWS 변환으로 제한되도록 합니다.

권한 세부 정보

정책 권한 세부 정보를 보려면 AWS 관리형 정책 참조 안내서의 [AWSTransformInfrastructureExecutorAccessEC2](#)를 참조하세요.

AWS 관리형 정책: AWSTransformSecurityAgentExecutorAccess

이 정책은 자동화된 코드 보안 검토 및 문제 해결을 위해 AWS Security Agent 서비스를 호출하는 데 필요한 권한을 AWS Transform Continuous Modernization에 부여합니다. 연속 현대화 AWS 변환 CLI 및 에이전트가 스캔 아티팩트를 업로드하고 결과를 검색하기 위해 수입하는 계정의 IAM 역할에 이 정책을 연결합니다.

설명

이 정책에는 다음 권한이 포함되어 있습니다.

- AWS 보안 에이전트 - 에이전트 공간 나열, 코드 검토 생성, 코드 검토 작업 시작, 조사 결과 나열 및 검색, 코드 수정 시작을 허용합니다. 이러한 작업은 계정의 에이전트 공간으로 범위가 지정됩니다.
- Amazon S3 - kct-security-agent-* 버킷에서 스캔 결과 및 결과를 다운로드하고 보안 스캔을 위한 소스 코드를 해당 버킷 내의 security-scans/* 접두사에 업로드할 수 있습니다.
- AWS Identity and Access Management (IAM) - AWS Security Agent 서비스에 security-agent-* 역할을 전달하여 스캔을 수행할 수 있도록 허용합니다.

이 정책은 리소스 수준 권한, S3 버킷 및 키 접두사, aws:ResourceAccount 및 s3:ResourceAccount 조건, 서비스 범위 iam:PassedToService 조건을 통해 최소 권한 액세스를 구현하여 작업이 동일한 AWS 계정 내의 Security Agent 리소스로 AWS 제한되도록 합니다.

권한 세부 정보

정책 권한 세부 정보를 보려면 AWS 관리형 정책 참조 안내서의 [AWSTransformSecurityAgentExecutorAccess](#)를 참조하세요.

AWS 관리형 정책: DBModDiscoveryAndAssessment

이 정책은 AWS 변환을 위한 포괄적인 데이터베이스 현대화 검색 및 평가 기능을 제공합니다.

설명

이 정책에는 다음 권한이 포함되어 있습니다.

- Amazon EC2 - 인스턴스, VPCs, 서브넷, 보안 그룹, 가용 영역, VPC 엔드포인트 및 인터넷 게이트웨이를 포함한 인프라 구성 요소를 설명할 수 있습니다.
- Amazon RDS - 데이터베이스 인스턴스, 클러스터 및 서브넷 그룹을 설명할 수 있습니다. 마이그레이션 준비를 위해 동일한 AWS 계정 내에서 DB 서브넷 그룹을 수정할 수 있습니다.
- Amazon RDS Data API - HTTP 엔드포인트를 활성화 및 비활성화하고 데이터베이스 현대화 프로젝트에 대해 태그가 지정된 데이터베이스 클러스터에서 SQL 문을 실행할 수 있습니다.
- AWS DMS - 엔드포인트, 복제 인스턴스, 작업, 서브넷 그룹 및 순서 지정 가능한 인스턴스를 설명할 수 있습니다. 데이터 공급자, 인스턴스 프로파일 및 마이그레이션 프로젝트를 나열할 수 있습니다. 테이블 통계, 평가 실행 및 메타데이터 모델 작업을 설명할 수 있습니다. 자세한 설명 및 메타데이터 작업은 데이터베이스 현대화 프로젝트에 대해 태그가 지정된 리소스로 제한됩니다.
- - 데이터베이스 자격 증명을 검색하기 위한 보안 암호를 나열할 수 있습니다.

- AWS Identity and Access Management (IAM) - 특정 AWS DMS 서비스 역할 및 연결된 정책을 검사할 수 있습니다. 읽기 AWS관리형 AWS DMS 정책에 대한 액세스를 포함합니다.
- AWS Key Management Service (KMS) - 키 별칭을 나열하고 키를 설명할 수 있습니다. 동일한 AWS 계정으로 제한된 통합을 통한 보안 암호 해독을 허용합니다.

이 정책은 리소스 수준 권한, 태그 기반 조건 및 계정 수준 제한을 통해 최소 권한 액세스를 구현하여 작업이 동일한 AWS 계정 내의 데이터베이스 현대화 프로젝트 리소스로 제한되도록 합니다.

권한 세부 정보

정책 권한 세부 정보를 보려면 AWS 관리형 정책 참조 안내서의 [DBModDiscoveryAndAssessment](#)를 참조하세요.

AWS 관리형 정책: DBModProvisioningAndMigration

이 정책은 데이터베이스 현대화 프로젝트 AWS 변환을 위한 데이터베이스 프로비저닝 및 마이그레이션 기능을 제공합니다. 여기에는 마이그레이션 인프라를 생성 및 관리하고, 대상 데이터베이스를 프로비저닝하고, 마이그레이션 데이터를 저장할 수 있는 권한이 포함됩니다.

설명

이 정책에는 다음 권한이 포함되어 있습니다.

- AWS DMS - 복제 서브넷 그룹, 인스턴스 프로파일, 데이터 공급자, 마이그레이션 프로젝트, 엔드포인트, 복제 인스턴스 및 복제 작업을 생성하고 관리할 수 있습니다. 메타데이터 모델 가져오기, 변환, 내보내기 및 평가와 같은 스키마 변환 작업을 포함합니다. 복제 인스턴스(생성, 삭제, 수정, 재부팅) 및 복제 작업(삭제, 시작, 중지, 평가)의 수명 주기 관리를 허용합니다. 모든 쓰기 작업은 데이터베이스 현대화 프로젝트에 대해 태그가 지정된 리소스로 제한됩니다.
- Amazon RDS - 데이터베이스 서브넷 그룹, 데이터베이스 클러스터 및 데이터베이스 인스턴스를 생성할 수 있습니다. 데이터베이스 현대화 프로젝트를 위해 모든 리소스에 태그를 지정해야 합니다.
- - 데이터베이스 현대화 이름 지정 접두사를 사용하여 보안 암호를 생성, 업데이트 및 태깅할 수 있습니다. 보안 암호 값을 검색하고 태그가 지정된 리소스의 보안 암호를 설명할 수 있습니다.
- Amazon S3 - 마이그레이션 데이터 스토리지를 위한 S3 버킷 및 객체를 생성하고 관리할 수 있습니다. 버킷 태그 지정, 버전 관리 및 객체 수명 주기 작업을 포함합니다. 데이터베이스 현대화 이름 지정 접두사가 있는 버킷으로 제한됩니다.
- AWS Identity and Access Management (IAM) - 특정 AWS DMS 서비스 역할을 AWS DMS 및 스키마 변환 서비스에 전달할 수 있습니다. 데이터베이스 작업에 필요한 Amazon RDS 서비스 연결 역할을 생성할 수 있습니다.

이 정책은 리소스 수준 권한, 태그 기반 조건 및 계정 수준 제한을 통해 최소 권한 액세스를 구현하여 작업이 동일한 AWS 계정 내의 데이터베이스 현대화 프로젝트 리소스로 제한되도록 합니다.

권한 세부 정보

정책 권한 세부 정보를 보려면 AWS 관리형 정책 참조 안내서의 [DBModProvisioningAndMigration](#)을 참조하세요.

AWS 변환 권한 참조

이 섹션에서는 AWS 변환에 사용되는 APIs와 해당 작업에 대한 정보를 제공합니다.

주제

- [AWS 변환 APIs](#)

AWS 변환 APIs

- transform:BatchGetMessage
- transform:BatchGetUserDetails
- transform:CompleteArtifactUpload
- 변환:CreateArtifactDownloadUrl
- 변환:CreateArtifactUploadUrl
- transform:CreateAssetDownloadUrl
- 변환:CreateConnector
- 변환:CreateFeedback
- 변환:CreateJob
- 변환:CreateSession
- 변환:CreateWorkspace
- transform>DeleteConnector
- 변환>DeleteJob
- transform>DeleteSelfRoleMappings
- transform>DeleteUserRoleMappings
- 변환>DeleteWorkspace
- transform:DetectIsAllowedForOperation
- 변환:GetConnector

- 변환:GetFeedbackQuestions
- 변환:GetHitITask
- 변환:GetJob
- 변환:GetLoginRedirectUri
- transform:GetUserDetails
- transform:GetUserPreferences
- 변환:GetWebAppUrl
- 변환:GetWorkspace
- transform:ListArtifacts
- 변환:ListConnectors
- 변환:ListHitITasks
- transform:ListJobPlanSteps
- transform:ListJobs
- transform:ListMessages
- transform:ListPlanUpdates
- transform:ListUserRoleMappings
- 변환:ListWorklogs
- 변환:ListWorkspaces
- transform:PutUserPreferences
- transform:PutUserRoleMappings
- 변환:RevokeSession
- transform:SearchUsers
- transform:SearchUsersTypeahead
- 변환:SendMessage
- 변환:StartJob
- transform:StopJob
- 변환:SubmitCriticalHitITask
- 변환:SubmitStandardHitITask
- transform:TestReleaseTraitPreProd
- 변환:TestReleaseTraitProd

- 변환:UpdateHitTask
- 변환:UpdateJob
- 변환:UpdateWorkspace
- 변환:VerifySession

AWS 변환에 대한 규정 준수 검증

AWS 서비스 가 특정 규정 준수 프로그램의 범위 내에 있는지 알아보려면 [AWS 서비스 규정 준수 프로그램 범위 내](#) 참조하고 관심 있는 규정 준수 프로그램을 선택합니다. 일반 정보는 [AWS 규정 준수 프로그램](#).

를 사용하여 타사 감사 보고서를 다운로드할 수 있습니다 AWS Artifact. 자세한 내용은 [Downloading Reports in Downloading AWS Artifact](#)을 참조하세요.

사용 시 규정 준수 책임은 데이터의 민감도, 회사의 규정 준수 목표 및 관련 법률과 규정에 따라 AWS 서비스 결정됩니다. 사용 시 규정 준수 책임에 대한 자세한 내용은 [AWS 보안 설명서를](#) AWS 서비스 참조하세요.

AWS 변환의 복원력

AWS 글로벌 인프라는 AWS 리전 및 가용 영역을 중심으로 구축됩니다.는 물리적으로 분리되고 격리된 여러 가용 영역을 AWS 리전 제공하며,이 가용 영역은 지연 시간이 짧고 처리량이 높으며 중복성이 높은 네트워킹과 연결됩니다. 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 인프라를](#) 참조하세요.

AWS 글로벌 인프라 외에도 AWS Transform은 데이터 복원력 및 백업 요구 사항을 지원하는 몇 가지 기능을 제공합니다.

AWS Transform 및 인터페이스 엔드포인트(AWS PrivateLink)

인터페이스 VPC 엔드포인트를 생성 AWS Transform 하여 VPC와 간에 프라이빗 연결을 설정할 수 있습니다. 인터페이스 엔드포인트는 인터넷 게이트웨이 [AWS PrivateLink](#), NAT 디바이스, VPN 연결 또는 Direct Connect 연결 없이 AWS Transform 콘솔에 비공개로 액세스할 수 있는 기술로 구동됩니다. VPC와 간의 트래픽 AWS Transform 은 Amazon 네트워크를 벗어나지 않습니다.

각 인터페이스 엔드포인트는 서브넷에서 하나 이상의 [Elastic Network Interfaces](#)로 표현됩니다.

자세한 내용은 Amazon VPC 사용 설명서의 [인터페이스 VPC 엔드포인트\(AWS PrivateLink\)](#)를 참조하세요.

Note

AWS Transform 사용자 지정 PrivateLink 설명서는 섹션을 참조하세요 [AWS Transform 사용자 지정 및 인터페이스 엔드포인트\(AWS PrivateLink\)](#).

AWS Transform VPC 엔드포인트에 대한 고려 사항

에 대한 인터페이스 VPC 엔드포인트를 설정하기 전에 Amazon VPC 사용 설명서의 [인터페이스 엔드포인트 속성 및 제한 사항을](#) 검토해야 AWS Transform합니다.

사전 조건

아래 절차를 시작하기 전에 다음 사항이 준비되어 있는지 확인하세요.

- 리소스를 생성하고 구성할 수 있는 적절한 권한이 있는 AWS 계정입니다.
- AWS 계정에 이미 생성된 VPC입니다.
- AWS 서비스, 특히 Amazon VPC 및에 대한 지식 AWS Transform.

에 대한 인터페이스 VPC 엔드포인트 생성 AWS Transform

Amazon VPC 콘솔 또는 AWS Command Line Interface ()를 사용하여 AWS Transform 서비스에 대한 VPC 엔드포인트를 생성할 수 있습니다AWS CLI. 자세한 내용은 Amazon VPC 사용 설명서의 [인터페이스 엔드포인트 생성](#)을 참조하세요.

AWS Transform 는 다음 VPC 엔드포인트 서비스를 지원합니다.

서비스 이름	엔드포인트	Note
컨트롤 플레인	com.amazons. <i>region</i> .transform	

서비스 이름	엔드포인트	Note
에이전트 API	com.amazonaws. region .transform-agents	
웹 애플리케이션	com.amazonaws. region .api.transform	AWS Transform 웹 애플리케이션에 필요합니다. 가 VPC의 프라이빗 IP 주소로 api.transform. region .on.aws 확인 되도록 하려면이 엔드포인트에 프라이빗 DNS가 활성화되어 있어야 합니다(DNS 이름 활성화 옵션).

region을 com.amazonaws.us-east-1.transform과 같이 프로필이 설치된 AWS 리전으로 바꿉니다 AWS Transform .

Note

AWS Transform 웹 애플리케이션을 사용하는 경우 api.transform 엔드포인트가 필요합니다. 전체 설정 가이드는 섹션을 참조하세요 [VPC에서 AWS Transform 웹 애플리케이션에 액세스](#).

자세한 내용은 Amazon VPC 사용 설명서의 [에 지원되는 리전 AWS Transform](#) 및 [인터페이스 엔드포인트를 통한 서비스 액세스](#)를 참조하세요.

온프레미스 컴퓨터를 사용하여 AWS Transform 엔드포인트에 연결

이 섹션에서는 온프레미스 컴퓨터를 사용하여 AWS VPC의 AWS PrivateLink 엔드포인트를 AWS Transform 통해 연결하는 프로세스를 설명합니다.

1. [온프레미스 디바이스와 VPC 간에 VPN 연결을 생성합니다.](#)
2. [에 대한 인터페이스 VPC 엔드포인트를 생성합니다 AWS Transform.](#)
3. [인바운드 Amazon Route 53 엔드포인트를 설정합니다.](#) 이렇게 하면 온프레미스 디바이스에서 AWS Transform 엔드포인트의 DNS 이름을 사용할 수 있습니다.

VPC에서 AWS Transform 웹 애플리케이션에 액세스

AWS PrivateLink 를 사용하여 VPC에서 API에 AWS Transform 비공개로 액세스하는 경우 웹 애플리케이션에 추가 네트워크 구성이 필요합니다. 인터넷 연결이 필요한 CloudFront를 통해 정적 콘텐츠 (HTML, JavaScript, CSS)를 제공합니다. 웹 애플리케이션의 API 호출은 VPC 엔드포인트를 통과하여 완전히 비공개로 유지됩니다.

이 가이드에서는 VPC를 필수 도메인으로만 잠그면서 웹 애플리케이션이 로드될 수 있도록 VPC에서 제어된 인터넷 송신을 구성하는 방법을 보여줍니다.

작동 방식

AWS Transform 웹 애플리케이션은 두 개의 네트워크 경로를 사용합니다.

- API 호출 - 웹 애플리케이션(작업 시작, 워크스페이스 보기 등)과 상호 작용할 때 브라우저는 API 요청을 로 보냅니다 `api.transform.region.on.aws.com.amazonaws.region.api.transform` VPC 엔드포인트와 프라이빗 DNS를 활성화하면 이러한 요청은 VPC의 프라이빗 IP 주소로 확인되고 AWS 네트워크를 벗어나지 않습니다.
- 정적 콘텐츠 - 웹 애플리케이션의 HTML, JavaScript 및 CSS 파일을 통해 CloudFront를 통해 제공됩니다 `tenant-id.transform.region.on.aws`. CloudFront 콘텐츠 전송은 퍼블릭 인터넷을 통해서만 사용할 수 있으므로 이러한 파일을 로드하려면 인터넷 연결이 필요합니다.
- 인증 - AWS IAM Identity Center 로그인 흐름은 인터넷 연결 `region.signin.aws`도 필요한를 사용합니다.

보안을 유지하면서 웹 애플리케이션을 활성화하려면 도메인 기반 필터링과 함께 AWS Network Firewall을 사용하여 제어된 송신 경로를 생성합니다. 이렇게 하면 VPC가 웹 애플리케이션에 필요한 특정 도메인에만 도달하는 동시에 다른 모든 인터넷 트래픽을 차단할 수 있습니다.

아키텍처

다음 다이어그램은 웹 애플리케이션 트래픽의 네트워크 경로를 보여줍니다.

```

EC2 Instance / Workspace (Private Subnet)
|
| Route: 0.0.0.0/0 # Network Firewall Endpoint
v
AWS Network Firewall (Firewall Subnet)
  
```

```

| Allows: *.cloudfront.net, *.transform.<region>.on.aws,
|         <region>.signin.aws, S3 domains, S3 presigned URLs
| Blocks: everything else (TLS SNI inspection)
|
| Route: 0.0.0.0/0 # NAT Gateway
v
NAT Gateway (Public Subnet)
|
| Route: 0.0.0.0/0 # Internet Gateway
v
Internet Gateway # CloudFront Edge Locations

```

⚠ Important

Network Firewall은 TLS SNI 검사를 수행하려면 트래픽의 양방향(대칭 라우팅)을 확인해야 합니다. 프라이빗 서브넷으로 향하는 트래픽을 방화벽을 통해 다시 보내는 NAT 게이트웨이 서브넷에서 반환 경로를 구성해야 합니다. 이렇게 하지 않으면 도메인 기반 필터링 규칙이 작동하지 않습니다.

사전 조건

시작하기 전에 다음을 갖추었는지 확인하세요.

- VPC 리소스, 네트워크 방화벽 및 NAT 게이트웨이를 생성할 수 있는 권한이 있는 AWS 계정입니다.
- 인스턴스 또는 워크로드가 실행되는 프라이빗 서브넷이 있는 VPC입니다.
- VPC에 연결된 인터넷 게이트웨이(또는 VPC 생성 권한).
- 프라이빗 DNS가 활성화된 `com.amazonaws.region.api.transform`의 AWS Transform VPC 엔드포인트입니다. 웹 애플리케이션 브라우저 클라이언트에서 사용하는 엔드포인트입니다. 엔드포인트 생성에 대한 지침은 [섹션을 참조하세요](#) [AWS Transform 및 인터페이스 엔드포인트\(AWS PrivateLink\)](#).

VPC 엔드포인트 정책 구성

`com.amazonaws.region.api.transform` VPC 엔드포인트에 사용자 지정 엔드포인트 정책이 있는 경우 AWS Transform 작업을 허용하는 문을 추가해야 합니다. 이렇게 하지 않으면 웹 애플리케이션이 엔드포인트를 통해 API를 호출할 수 없습니다.

VPC 엔드포인트 정책에 다음 문을 추가합니다. ***AWS_TRANSFORM_PROFILE_ARN***을 설정 페이지의 AWS Transform 콘솔에서 찾을 수 있는 AWS Transform 서비스 프로파일 ARN으로 바꿉니다.

```
{
  "Statement": [
    {
      "Sid": "AllowAWSTransform",
      "Effect": "Allow",
      "Principal": "*",
      "Action": "*",
      "Resource": "*",
      "Condition": {
        "StringEquals": {
          "aws:PrincipalArn": [
            "AWS_TRANSFORM_PROFILE_ARN"
          ]
        }
      }
    }
  ]
}
```

Note

VPC 엔드포인트가 기본 정책(전체 액세스)을 사용하는 경우 변경할 필요가 없으며 이 단계를 건너뛸 수 있습니다.

제어된 인터넷 송신 설정

다음 단계를 완료하여 AWS Transform 웹 애플리케이션에 대한 도메인 기반 필터링으로 Network Firewall을 구성합니다.

1단계: 방화벽 서브넷 생성

Network Firewall 엔드포인트 전용의 작은 /28 서브넷을 생성합니다. 이 서브넷은 프라이빗 서브넷과 동일한 가용 영역에 있어야 합니다.

```
aws ec2 create-subnet \
```

```
--vpc-id your-vpc-id \  
--cidr-block firewall-subnet-cidr \  
--availability-zone your-az \  
--region region
```

2단계: NAT 게이트웨이에 대한 퍼블릭 서브넷 생성

```
aws ec2 create-subnet \  
  --vpc-id your-vpc-id \  
  --cidr-block public-subnet-cidr \  
  --availability-zone your-az \  
  --region region
```

3단계: 퍼블릭 서브넷 라우팅 테이블 구성

인터넷 트래픽을 인터넷 게이트웨이로 라우팅하는 퍼블릭 서브넷의 라우팅 테이블을 생성합니다.

```
# Create route table  
PUB_RTB=$(aws ec2 create-route-table \  
  --vpc-id your-vpc-id \  
  --region region \  
  --query 'RouteTable.RouteTableId' --output text)  
  
# Add default route to internet gateway  
aws ec2 create-route \  
  --route-table-id $PUB_RTB \  
  --destination-cidr-block 0.0.0.0/0 \  
  --gateway-id your-igw-id \  
  --region region  
  
# Associate with public subnet  
aws ec2 associate-route-table \  
  --route-table-id $PUB_RTB \  
  --subnet-id public-subnet-id \  
  --region region
```

4단계: NAT 게이트웨이 생성

```
# Allocate an Elastic IP
EIP=$(aws ec2 allocate-address --domain vpc \
  --region region --query 'AllocationId' --output text)

# Create NAT Gateway in the public subnet
NAT_ID=$(aws ec2 create-nat-gateway \
  --subnet-id public-subnet-id \
  --allocation-id $EIP \
  --region region \
  --query 'NatGateway.NatGatewayId' --output text)

# Wait for NAT Gateway to become available (~2 minutes)
aws ec2 wait nat-gateway-available \
  --nat-gateway-ids $NAT_ID --region region
```

5단계: Network Firewall 규칙 그룹 생성

AWS Transform 웹 애플리케이션에 필요한 도메인으로만 트래픽을 허용하는 상태 저장 규칙 그룹을 생성합니다.

```
aws network-firewall create-rule-group \
  --rule-group-name transform-webapp-domains \
  --type STATEFUL \
  --capacity 100 \
  --rule-group '{
    "StatefulRuleOptions": {
      "RuleOrder": "STRICT_ORDER"
    },
    "RulesSource": {
      "RulesSourceList": {
        "Targets": [
          ".cloudfront.net",
          ".transform.region.on.aws",
          "region.signin.aws",
          ".s3.region.amazonaws.com",
          "oidc.region.amazonaws.com",
          "portal.sso.region.amazonaws.com",
```



```

        "assets.sso-portal.region.amazonaws.com",
        "directory-id.awsapps.com"
    ],
    "TargetTypes": ["TLS_SNI", "HTTP_HOST"],
    "GeneratedRulesType": "ALLOWLIST"
}
}
}' \
--region region

```

*region*을 프로필이 설치된 AWS 리전으로 바꿉니다 AWS Transform (예: us-east-1).
*directory-id*를 IAM Identity Center 디렉터리 ID(예: d-1234567890)로 바꿉니다. 디렉터리 ID는 IAM Identity Center 콘솔에서 찾을 수 있습니다.

다음 표에서는 허용되는 도메인에 대해 설명합니다.

도메인	용도
.cloudfront.net	CloudFront CDN - 웹 애플리케이션 정적 자산(JavaScript, CSS, 이미지)을 제공합니다.
.transform. <i>region</i> .on.aws	웹 애플리케이션 테넌트 URL - 브라우저가 CloudFront를 통해이 도메인에서 초기 페이지를 로드합니다.
<i>region</i> .signin.aws	SSO 로그인 리디렉션 페이지
.s3. <i>region</i> .amazonaws.com	S3 미리 서명된 URLs - 아티팩트 업로드 및 다운로드
oidc. <i>region</i> .amazonaws.com	SSO 인증을 위한 OIDC 토큰 교환
portal.sso. <i>region</i> .amazonaws.com	SSO 포털 로그인 페이지
assets.sso-portal. <i>region</i> .amazonaws.com	SSO 포털 정적 자산(CSS, JavaScript)
<i>directory-id</i> .awsapps.com	조직의 IAM Identity Center 포털

Note

.cloudfront.net 와일드카드는 AWS Transform 웹 애플리케이션의 배포뿐만 아니라 모든 CloudFront 배포에 대한 트래픽을 허용합니다. CloudFront 엣지 IPs는 배포 간에 공유되고 TLS SNI 검사는 동일한 도메인 뒤의 개별 배포를 구별할 수 없으므로 더 좁은 도메인 필터는 불가능합니다.

Note

API 호출은 `api.transform.region.on.aws` 통과 AWS PrivateLink 하며 인터넷 송신이 필요하지 않습니다. 방화벽의 영향을 받지 않습니다.

6단계: 방화벽 정책 생성

정책은 기본 작업 `drop_established`으로 사용하여 `STRICT_ORDER` 규칙 평가를 사용해야 합니다. 이렇게 하면 허용 목록과 일치하지 않는 트래픽이 삭제됩니다.

```
# Get the rule group ARN
RG_ARN=$(aws network-firewall describe-rule-group \
  --rule-group-name transform-webapp-domains \
  --type STATEFUL --region region \
  --query 'RuleGroupResponse.RuleGroupArn' --output text)

# Create the firewall policy
aws network-firewall create-firewall-policy \
  --firewall-policy-name transform-webapp-policy \
  --firewall-policy "{
    \"StatelessDefaultActions\": [\"aws:forward_to_sfe\"],
    \"StatelessFragmentDefaultActions\": [\"aws:forward_to_sfe\"],
    \"StatefulRuleGroupReferences\": [
      {
        \"ResourceArn\": \"$RG_ARN\",
        \"Priority\": 1
      }
    ],
    \"StatefulEngineOptions\": {
      \"RuleOrder\": \"STRICT_ORDER\"
    }
  },
```

```
\\"StatefulDefaultActions\\": [\\"aws:drop_established\\", \\"aws:alert_established\\"]
}" \
--region region
```

7단계: 네트워크 방화벽 생성

```
# Get the policy ARN
FW_POLICY_ARN=$(aws network-firewall describe-firewall-policy \
  --firewall-policy-name transform-webapp-policy \
  --region region \
  --query 'FirewallPolicyResponse.FirewallPolicyArn' --output text)

# Create the firewall
aws network-firewall create-firewall \
  --firewall-name transform-webapp-firewall \
  --firewall-policy-arn $FW_POLICY_ARN \
  --vpc-id your-vpc-id \
  --subnet-mappings SubnetId=firewall-subnet-id \
  --region region

# Wait for the firewall to become READY (3-5 minutes)
while true; do
  STATUS=$(aws network-firewall describe-firewall \
    --firewall-name transform-webapp-firewall \
    --region region \
    --query 'FirewallStatus.Status' --output text)
  echo "Status: $STATUS"
  if [ "$STATUS" = "READY" ]; then break; fi
  sleep 15
done
```

8단계: 방화벽 엔드포인트 ID 가져오기

```
FW_ENDPOINT=$(aws network-firewall describe-firewall \
  --firewall-name transform-webapp-firewall \
  --region region \
  --query "FirewallStatus.SyncStates.\\"your-az\".Attachment.EndpointId" \
  --output text)
```

```
echo "Firewall endpoint: $FW_ENDPOINT"
```

9단계: 방화벽 서브넷 라우팅 테이블 구성

방화벽 서브넷에서 NAT 게이트웨이로 인터넷 바운드 트래픽을 라우팅합니다.

```
FW_RTB=$(aws ec2 create-route-table \
  --vpc-id your-vpc-id \
  --region region \
  --query 'RouteTable.RouteTableId' --output text)

aws ec2 create-route \
  --route-table-id $FW_RTB \
  --destination-cidr-block 0.0.0.0/0 \
  --nat-gateway-id $NAT_ID \
  --region region

aws ec2 associate-route-table \
  --route-table-id $FW_RTB \
  --subnet-id firewall-subnet-id \
  --region region
```

10단계: 프라이빗 서브넷 라우팅 테이블 업데이트

프라이빗 서브넷에서 방화벽을 통해 모든 인터넷 바인딩 트래픽을 라우팅합니다.

```
aws ec2 create-route \
  --route-table-id private-subnet-route-table-id \
  --destination-cidr-block 0.0.0.0/0 \
  --vpc-endpoint-id $FW_ENDPOINT \
  --region region
```

기본 경로가 이미 있는 경우 `replace-route` 대신 `create-route`를 사용합니다.

11단계: 대칭 반환 경로 추가(필수)

Important

이 단계는 매우 중요합니다. Network Firewall은 TLS SNI 검사를 사용하며 TCP 연결의 양방향을 확인해야 합니다. NAT 게이트웨이 서브넷의 라우팅 테이블에 프라이빗 서브넷으로 향하는 반환 트래픽을 방화벽을 통해 다시 보내는 경로를 추가합니다.

```
aws ec2 create-route \
  --route-table-id $PUB_RTB \
  --destination-cidr-block private-subnet-cidr \
  --vpc-endpoint-id $FW_ENDPOINT \
  --region region
```

*private-subnet-cidr*을 프라이빗 서브넷의 CIDR 블록으로 바꿉니다(예: 10.0.144.0/20).

대칭 라우팅이 없으면 방화벽은 트래픽의 한 방향만 볼 수 있습니다. TLS 검사 엔진은 TLS 핸드셰이크에서 서버 이름 표시(SNI)를 추출할 수 없으며 모든 도메인 기반 규칙이 자동으로 실패합니다.

12단계: IPv6 기본 경로 제거(있는 경우)

프라이빗 서브넷 라우팅 테이블에 인터넷 게이트웨이를 직접 가리키는 IPv6 기본 라우팅(::<0)이 있는 경우 IPv6-capable 대상으로 방화벽을 우회합니다. 제거:

```
aws ec2 delete-route \
  --route-table-id private-subnet-route-table-id \
  --destination-ipv6-cidr-block ::/0 \
  --region region
```

Verification(확인)

프라이빗 서브넷의 인스턴스에서 구성을 확인합니다.

```
# Should SUCCEED - web application content via CloudFront (allowed)
```

```
curl -vL --connect-timeout 15 \
  'https://tenant-id.transform.region.on.aws'

# Should SUCCEED - API via PrivateLink (does not use firewall)
curl -v --connect-timeout 15 \
  'https://api.transform.region.on.aws/'

# Should FAIL - non-allowlisted domain (blocked by firewall)
curl -v --connect-timeout 15 'https://www.example.com'
# Expected: TLS connection error (firewall drops after SNI inspection)
```

문제 해결

방화벽에 의해 api.transform에 대한 API 호출이 차단됨

도메인은 VPC 엔드포인트를 통해 프라이빗 IP 주소로 api.transform.region.on.aws 확인되어야 하며 인터넷 방화벽에 연결해서는 안 됩니다.

- com.amazonaws.region.api.transform 엔드포인트를 생성했는지 확인합니다.
- 엔드포인트에서 프라이빗 DNS가 활성화되어 있는지 확인합니다.

```
aws ec2 describe-vpc-endpoints \
  --filters "Name=service-name,Values=com.amazonaws.region.api.transform" \
  --query 'VpcEndpoints[*].[State,PrivateDnsEnabled]' \
  --output table
```

예상 결과: available | True

웹 애플리케이션이 로드되지 않음(연결 제한 시간)

- 프라이빗 서브넷 라우팅 테이블에 방화벽 엔드포인트를 가리키는 0.0.0.0/0 경로가 있는지 확인합니다.
- 방화벽 서브넷 라우팅 테이블에 NAT 게이트웨이를 가리키는 0.0.0.0/0 경로가 있는지 확인합니다.
- NAT 게이트웨이가 available 상태인지 확인합니다.

허용 목록에 없는 도메인은 차단되지 않습니다.

- 인터넷 게이트웨이를 가리키는 IPv6 :::/0 경로를 확인합니다. 이렇게 하면 방화벽이 우회합니다. 이를 제거합니다(12단계).

- 대칭 라우팅이 구성되어 있는지 확인합니다. NAT Gateway 서브넷 라우팅 테이블에는 프라이빗 서브넷 CIDR에 대한 방화벽을 통한 반환 경로가 있어야 합니다(11단계).
- 방화벽 정책이 drop_established 및 STRICT_ORDER를 기본 작업 alert_established으로 사용하는지 확인합니다.

비용 고려 사항

Resource	대략적인 비용
Network Firewall	가용 영역당 ~\$0.395/시간(~\$288/월)
NAT 게이트웨이	~\$0.045/시간(~\$33/월) + 데이터 처리 요금
탄력적 IP(퍼블릭 IPv4)	~\$0.005/시간(~\$3.60/월)
Network Firewall 데이터 처리	\$0.065/GB
NAT 게이트웨이 데이터 처리	\$0.045/GB

예상 기본 비용은 단일 가용 영역 배포의 경우 월 약 325 USD입니다. 프로덕션 배포의 경우 프라이빗 서브넷이 있는 각 가용 영역에 방화벽, NAT 게이트웨이 및 관련 서브넷을 배포합니다.

정리

이 가이드에서 생성한 모든 리소스를 제거하려면 다음 명령을 역순으로 실행합니다. 자리 표시자를 배포의 리소스 IDs로 바꿉니다. AWS 관리 콘솔에서 또는 설정 단계의 describe 명령을 사용하여 이러한 값을 찾을 수 있습니다.

```
# Remove return route from NAT Gateway subnet
aws ec2 delete-route --route-table-id pub-rtb-id \
  --destination-cidr-block private-subnet-cidr \
  --region region

# Remove route from private subnet
aws ec2 delete-route \
  --route-table-id private-subnet-route-table-id \
  --destination-cidr-block 0.0.0.0/0 --region region
```

```
# Delete Network Firewall (takes ~5 minutes)
aws network-firewall delete-firewall \
  --firewall-name transform-webapp-firewall \
  --region region

# Delete firewall policy and rule group
aws network-firewall delete-firewall-policy \
  --firewall-policy-name transform-webapp-policy \
  --region region
aws network-firewall delete-rule-group \
  --rule-group-name transform-webapp-domains \
  --type STATEFUL --region region

# Delete NAT Gateway (wait ~5 minutes for full deletion)
aws ec2 delete-nat-gateway --nat-gateway-id nat-gateway-id \
  --region region

# Release Elastic IP
aws ec2 release-address --allocation-id eip-allocation-id \
  --region region

# Delete subnets
aws ec2 delete-subnet --subnet-id firewall-subnet-id \
  --region region
aws ec2 delete-subnet --subnet-id public-subnet-id \
  --region region
```


AWS 변환 모니터링

모니터링은 AWS 변환 및 기타 AWS 솔루션의 안정성, 가용성 및 성능을 유지하는 데 중요한 부분입니다. AWS 변환을 모니터링하고, 이상이 있을 때 이를 보고하고, 적절한 경우 자동 조치를 취할 수 있도록 다음과 같은 모니터링 도구를 AWS 제공합니다.

- Amazon CloudWatch는 AWS 리소스와 실행 중인 애플리케이션을 AWS 실시간으로 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 CloudWatch에서 Amazon EC2 인스턴스의 CPU 사용량 또는 기타 지표를 추적하고 필요할 때 자동으로 새 인스턴스를 시작할 수 있습니다. 자세한 내용은 [Amazon CloudWatch 사용 설명서](#)를 참조하세요.
- Amazon CloudWatch Logs로 Amazon EC2 인스턴스, CloudTrail, 기타 소스의 로그 파일을 모니터링, 저장 및 액세스할 수 있습니다. CloudWatch Logs는 로그 파일의 정보를 모니터링하고 특정 임계값에 도달하면 사용자에게 알릴 수 있습니다. 또한 매우 내구성이 뛰어난 스토리지에 로그 데이터를 저장할 수 있습니다. 자세한 내용은 [Amazon CloudWatch Logs 사용자 안내서](#)를 참조하세요.
- Amazon EventBridge를 사용하여 AWS 서비스를 자동화하고 애플리케이션 가용성 문제 또는 리소스 변경과 같은 시스템 이벤트에 자동으로 대응할 수 있습니다. AWS 서비스의 이벤트는 거의 실시간으로 EventBridge로 전달됩니다. 원하는 이벤트만 표시하도록 간단한 규칙을 작성한 후 규칙과 일치하는 이벤트 발생 시 실행할 자동화 작업을 지정할 수 있습니다. 자세한 내용은 [Amazon EventBridge 사용 설명서](#)를 참조하세요.
- AWS CloudTrail는 AWS 계정에 의해 또는 계정을 대신하여 수행된 API 호출 및 관련 이벤트를 캡처하고 사용자가 지정한 Amazon S3 버킷에 로그 파일을 전송합니다. 호출한 사용자 및 계정 AWS, 호출이 수행된 소스 IP 주소, 호출이 발생한 시기를 식별할 수 있습니다. 자세한 내용은 [AWS CloudTrail 사용 설명서](#)를 참조하십시오.

를 사용하여 AWS 변환 API 호출 로깅 AWS CloudTrail

AWS 변환은 AWS 변환에서 사용자 AWS CloudTrail, 역할 또는 서비스가 수행한 작업에 대한 레코드를 제공하는 AWS 서비스와 통합됩니다. CloudTrail은 AWS 변환에 대한 모든 API 호출을 이벤트로 캡처합니다. 캡처되는 호출에는 AWS 변환 콘솔의 호출과 AWS 변환 API 작업에 대한 코드 호출이 포함됩니다. 추적을 생성하면 AWS 변환 이벤트를 포함하여 CloudTrail 이벤트를 지속적으로 Amazon S3 버킷에 배포할 수 있습니다. 추적을 구성하지 않은 경우에도 이벤트 기록에서 CloudTrail 콘솔의 최신 이벤트를 볼 수 있습니다. CloudTrail에서 수집한 정보를 사용하여 AWS 변환에 수행된 요청, 요청이 수행된 IP 주소, 요청을 수행한 사람, 요청이 수행된 시간 및 추가 세부 정보를 확인할 수 있습니다.

CloudTrail에 대한 자세한 내용은 [AWS CloudTrail 사용 설명서](#)를 참조하세요.

AWS CloudTrail에서 정보 변환

CloudTrail은 계정을 생성할 AWS 계정 때에서 활성화됩니다. AWS 변환에서 활동이 발생하면 해당 활동이 이벤트 기록의 다른 AWS 서비스 이벤트와 함께 CloudTrail 이벤트에 기록됩니다. 에서 최근 이벤트를 보고 검색하고 다운로드할 수 있습니다 AWS 계정. 자세한 내용은 [CloudTrail 이벤트 기록을 사용하여 이벤트 보기](#)를 참조하세요.

AWS 변환 이벤트를 AWS 계정포함하여에 이벤트를 지속적으로 기록하려면 추적을 생성합니다. CloudTrail은 추적을 사용하여 Amazon S3 버킷으로 로그 파일을 전송할 수 있습니다. 콘솔에서 트레일을 생성하면 기본적으로 모든 AWS 리전에 트레일이 적용됩니다. 추적은 AWS 파티션의 모든 리전에서 이벤트를 로깅하고 지정한 Amazon S3 버킷으로 로그 파일을 전송합니다. 또한 CloudTrail 로그에서 수집된 이벤트 데이터를 추가로 분석하고 조치를 취하도록 다른 AWS 서비스를 구성할 수 있습니다. 자세한 내용은 다음 자료를 참조하세요.

- [추적 생성 개요](#)
- [CloudTrail 지원 서비스 및 통합](#)
- [CloudTrail에 대한 Amazon SNS 알림 구성](#)
- [여러 리전에서 CloudTrail 로그 파일 받기](#) 및 [여러 계정에서 CloudTrail 로그 파일 받기](#)

모든 이벤트 또는 로그 항목에는 요청을 생성했던 사용자에 관한 정보가 포함됩니다. ID 정보를 이용하면 다음을 쉽게 판단할 수 있습니다.

- 요청이 루트 또는 AWS Identity and Access Management (IAM) 사용자 자격 증명으로 이루어졌는지 여부입니다.
- 역할 또는 페더레이션 사용자의 임시 자격 증명을 사용하여 요청이 생성되었는지 여부.
- 요청이 다른 AWS 서비스에 의해 이루어졌는지 여부입니다.

자세한 내용은 [CloudTrail userIdentity 요소](#)를 참조하세요.

AWS 변환 로그 파일 항목 이해

트레일이란 지정한 S3 버킷에 이벤트를 로그 파일로 입력할 수 있게 하는 구성입니다. CloudTrail 로그 파일에는 하나 이상의 로그 항목이 포함될 수 있습니다. 이벤트는 모든 소스로부터의 단일 요청을 나타내며 요청 작업, 작업 날짜와 시간, 요청 파라미터 등에 대한 정보가 들어 있습니다. CloudTrail 로그 파일은 퍼블릭 API 간접 호출의 주문 스택 트레이스가 아니므로 특정 순서로 표시되지 않습니다.

알림

AWS 변환은 작업 영역 액세스 변경, 작업 상태 업데이트 및 보류 중인 공동 작업자 요청에 대한 정보를 제공하는 이메일 알림을 제공합니다.

이메일 알림

이메일 알림은 기본적으로 활성화되어 있으며 작업에 대한 읽기 전용 이상의 권한이 있는 사용자에게 전송됩니다. 사용자는 알림 기본 설정을 수정할 수 있습니다. 이메일 알림에는 세 가지 범주가 있습니다.

- Workspace 액세스 업데이트

새 워크스페이스에 추가되고 워크스페이스 내에서 역할이 변경되면 알림을 받게 됩니다.

- 일일 다이제스트 이메일

하나 이상의 미결 필수 공동 작업자 요청이 있는 활성 작업이 있는 경우 태평양 표준시 오전 9시에 진행 중인 작업을 요약하는 일일 다이제스트 이메일을 받게 됩니다. 이메일에는 워크스페이스 이름, 작업 이름, 작업 상태, 공동 작업자 요청 세부 정보 및 필요한 작업(10행으로 제한)을 보여주는 테이블이 포함되어 있습니다.

Note

일일 다이제스트 이메일은 공동 작업자 요청이 필요한 작업에 대해서만 전송됩니다. 선택적 공동 작업자 요청은 다이제스트 이메일을 트리거하지 않습니다.

- 작업 상태 업데이트

에 액세스할 수 있는 작업이 완료되거나 실패하면 이메일을 받게 됩니다.

- 공동 작업자 요청 업데이트

작업에 입력, 검토 또는 승인이 필요할 때마다 이메일을 받게 됩니다.

이메일 알림 관리

애플리케이션의 오른쪽 상단에 있는 설정 톱니를 클릭하고 알림 설정을 선택하여 웹 애플리케이션에서 이메일 알림 기본 설정을 수정할 수 있습니다.

알림 설정 페이지에서는 다음과 같은 제어 기능을 제공합니다.

알림 유형	설명	기본 설정
Workspace 액세스 업데이트	워크스페이스에 추가되거나 워크스페이스 내에서 역할이 변경될 때 이메일 수신	활성화됨
일일 공동 작업자 요청 дай제스트	액세스 가능한 워크스페이스의 작업에 대한 열린 공동 작업자 요청의 일일 дай제스트 수신	활성화됨
작업 완료 업데이트	작업이 완료되거나 실패하면 이메일 수신	활성화됨
공동 작업자 요청 업데이트	사용자의 입력 또는 승인이 필요한 경우 이메일 수신	비활성화됨

일반 설정을 사용하여 모든 알림을 활성화 또는 비활성화하거나 개별 알림 유형을 개별적으로 구성할 수 있습니다.

AWS 변환 할당량

AWS 계정에는 각 AWS 서비스에 대한 이전 제한이라고 하는 기본 할당량이 있습니다. 다르게 표시되지 않는 한 리전별로 각 할당량이 적용됩니다. 일부 할당량에 대한 증가를 요청할 수 있으며 다른 할당량은 늘릴 수 없습니다.

AWS 변환 할당량을 보려면 [Service Quotas 콘솔](#)을 엽니다. 탐색 창에서 AWS 서비스를 선택하고 AWS 변환을 선택합니다.

할당량 증가를 요청하려면 Service Quotas 사용 설명서의 [할당량 증가 요청](#)을 참조하세요. Service Quotas에서 아직 할당량을 사용할 수 없는 경우 [한도 증가 양식](#)을 사용합니다.

AWS 계정에는 AWS 변환과 관련된 다음과 같은 할당량이 있습니다.

워크로드	측정 기준	할당량	조정 가능	설명
플랫폼	AWS Transform 활성화된 계정 AWS 리전 당 워크스페이스	지원되는 각에 대해 100개의 워크스페이스 AWS 리전	예	당 AWS Transform활성화된 계정당 최대 워크스페이스 수 AWS 리전
VMWare 마이그레이션	각 웨이브의 서버 수	각 웨이브: 서버 150개	아니요	웨이브의 최대 서버 수
메인프레임	각 IAM Identity Center 계정에 대한 동시 작업	지원되는 각 리전에 대해 작업 10개	예	IAM Identity Center 계정의 최대 동시 메인프레임 작업 수
	각 작업의 코드 행	지원되는 각 리전에 대해 3,000,000줄의 코드	아니요	각 작업의 최대 코드 줄 수입니다.
	월별 코드 행 분석	지원되는 각 리전에 대해	예	한 달 동안 코드 분석 작업 목표에

워크로드	측정 기준	할당량	조정 가능	설명
		100,000,000줄의 코드		사용할 수 있는 최대 코드 줄 수
	비즈니스 문서 생성 월별 코드 줄	지원되는 각 리전에 대해 50,000,000줄의 코드	예	한 달 동안 비즈니스 문서 생성 작업 목표에 사용할 수 있는 최대 코드 줄 수
	기술 문서 생성 월별 코드 라인	지원되는 각 리전에 대해 50,000,000줄의 코드	예	한 달 동안 기술 문서 생성 작업 목표에 사용할 수 있는 최대 코드 줄 수
	코드 줄 변환	지원되는 각 리전에 대해 10,000,000줄의 코드	예	한 달 동안 변환된 최대 코드 줄 수
	월별 코드 행 분해	지원되는 각 리전에 대해 50,000,000줄의 코드	예	한 달 동안 분해 작업 목표에 사용할 수 있는 최대 코드 줄 수
	월별 코드 줄 리포지토리	지원되는 각 리전에 대해 50,000,000줄의 코드	예	한 달 동안 리포지 작업 목표에 사용할 수 있는 최대 코드 줄 수
	추출된 비즈니스 로직 월별 코드 라인	지원되는 각 리전에 대해 50,000,000줄의 코드	예	한 달의 추출된 비즈니스 로직 작업 목표에 대한 최대 코드 줄 수

워크로드	측정 기준	할당량	조정 가능	설명
.NET	.NET 월별 코드 줄 수(웹 및 IDE)	지원되는 각 리전에 대해 1,000,000줄의 코드	예	IAM Identity Center 계정에서 지원되는 각에서 한 달에 변환할 수 있는 .NET 애플리케이션 코드 AWS 리전 의 최대 줄 수
	각 IAM Identity Center 계정에 대해 Microsoft Visual Studio 확장을 사용하는 동시 .NET 작업	지원되는 각 리전에 대해 작업 10 개	예	Microsoft Visual Studio 확장을 사용할 때 IAM Identity Center 계정에서 지원되는 각 AWS 리전 의 최대 동시 .NET 변환 작업 수입니다.
	각 IAM Identity Center 계정에 대한 동시 .NET 웹 작업	지원되는 각 리전에 대해 작업 5개	예	변환 웹 앱을 사용할 때 IAM Identity Center 계정에서 지원되는 각 AWS 리전 의 최대 동시 .NET 변환 작업 수입니다 AWS .
사용자 지정 변환	사용자 지정 변환 정의	1,000	예	사용자 지정 변환 정의의 최대 수

워크로드	측정 기준	할당량	조정 가능	설명
	사용자 지정 변환 정의 크기	10MB	아니요	문서 참조를 포함하여 변환 정의에 포함된 모든 파일의 최대 총 크기입니다.
	사용자 지정 변환 월별 CLI 대화 요청	1,000,000	예	CLI에서 한 달에 허용되는 사용자 지정 변환 대화 요청의 최대 수
평가	각 평가에 대한 서버 수 제한	각 평가: 30,000 개의 서버	아니요	단일 평가 작업의 최대 서버 수

에 지원되는 리전 AWS Transform

Note

가이 페이지에 나열되지 않은 옵트인 리전에서 정보를 검색 AWS Transform 하도록 요청하는 경우는 해당 리전을 호출할 수 AWS Transform 있습니다. 에서 호출할 AWS Transform 수 있는 리전에 대한 액세스를 관리하려면 섹션을 참조하세요 [AWS 변환 시 보안](#).

이 주제에서는 사용할 수 AWS 리전 있는에 대해 설명합니다 AWS Transform. 에 대한 자세한 내용은 AWS Account Management 참조 안내서의 계정에서 사용할 수 있는 지정을 AWS 리전참조하세요.

[AWS 리전](#)

데이터는 사용하는 리전과 다른 리전에서 처리될 수 있습니다 AWS Transform. 에서 리전 간 처리에 대한 자세한 내용은 섹션을 AWS Transform참조하세요 [교차 리전 처리](#). 처리 중에 데이터가 저장되는 위치에 대한 자세한 내용은 [데이터 보호](#) 섹션을 참조하세요.

지원됨 AWS 리전 (기본적으로 활성화됨)

다음에서 AWS Transform 워크스페이스를 생성할 수 있습니다 AWS 리전. 이러한 리전은 기본적으로 활성화되어 있으므로 사용하기 전에 활성화할 필요가 없습니다. 자세한 내용은 [기본적으로 활성화된 리전](#) 섹션을 참조하세요.

- 미국 동부(버지니아 북부)
- 유럽(프랑크푸르트)
- 아시아 태평양(뭄바이)
- 아시아 태평양(시드니)
- 아시아 태평양(도쿄)
- 유럽(런던)
- 아시아 태평양(서울)
- 캐나다(중부)
- 남아메리카(상파울루) - 메인프레임 현대화 에이전트만 해당

작업을 생성하는 워크스페이스에 따라 작업 AWS 리전 의가 결정됩니다. 다른 리전에서 작업을 생성하려면 원하는 리전에 있는 다른 워크스페이스를 사용해야 합니다.

VMware 프로젝트의 경우 워크스페이스의 리전이 검색에 사용됩니다. 그러나 다른 리전을 마이그레이션 대상으로 지정할 수 있습니다. 마이그레이션이 완료되면 워크로드가 호스팅되는 대상 리전입니다. 가능한 대상 리전 목록을 포함하여 VMware 마이그레이션 AWS 리전 고려 사항에 대한 자세한 내용은 [섹션을 참조하세요](#) [the section called “지원되는 대상 리전”](#).

AWS 에 대한 지원 AWS Transform

AWS Transform 를 사용하면 변환 작업 중에 문제가 발생할 경우 채팅을 통해 AWS 지원 사례를 생성하고 관리할 수 있습니다. 사례는 작업 컨텍스트로 자동으로 보강되고 적절한 지원 팀에 라우팅됩니다. 활성 Countdown Premium 고객인 경우 지정된 엔지니어가 문제 해결을 관리하기 위해에 문의합니다. [AWS Countdown Premium](#)에서 자세히 알아보세요. 그렇지 않으면 AWS Transform 지원 대기열의 지원 팀이 사례를 조사합니다.

사전 조건

지원 사례 관리를 사용하려면 먼저 다음이 필요합니다.

- 활성 AWS 지원 플랜 - Business, Enterprise On-Ramp 또는 Enterprise
- 기존 AWS Transform 애플리케이션

지원 사례 관리 활성화

1. AWS Transform 콘솔을 엽니다.
2. 탐색 창에서 설정을 선택합니다.
3. 지원에서 지원 사례 관리 활성화를 선택합니다.
4. 변경 사항 저장을 선택합니다.

AWS Transform 는 서비스 연결 역할(SLR)을 사용하여 사용자를 대신하여 지원 사례를 생성하고 관리합니다. 추가 IAM 권한은 필요하지 않습니다.

지원 사례 생성

지원 사례를 생성하려면 채팅 인터페이스를 사용합니다.

1. 에 지원 사례 생성을 요청합니다. 예제:
 - “실패한 변환 작업에 대한 지원 사례 생성”
 - “작업 오류에 대한 도움이 필요합니다. 사례를 생성합니다.”
2. 채팅에서 필수 정보를 묻는 메시지가 표시됩니다.

- 문제에 대한 간략한 설명
- 자세한 설명

3. 메시지가 표시되면 사례 생성을 확인합니다.

사례는 다음을 포함하여 변환 작업의 컨텍스트로 자동으로 채워집니다.

- 작업 ID 및 상태
- 작업 메타데이터
- 작업 실행 로그(작업 로그)
- 작업 계획

사례는 작업 유형 및 문제 범주에 따라 자동으로 할당됩니다.

지원 사례 보기

지원 사례를 보려면 채팅 메시지를 표시합니다.

- “지원 사례 나열”
- “지원 사례를 개설했음을 보여줘.”
- “내 사례의 상태는 어떻게 됩니까?”

채팅에 다음이 표시됩니다.

- 사례 ID
- 제목
- 미결, 보류 중, 해결됨 또는 종료됨과 같은 상태
- 마지막 업데이트 날짜
- 연결된 작업 ID

특정 사례의 세부 정보를 보려면:

- “[case-id] 사례에 대한 세부 정보 표시”
- “[case-id] 사례에 대한 최신 업데이트는 무엇인가요?”

사례에 통신 추가

기존 사례에 메시지를 추가하려면:

1. 채팅에 질문: "대/소문자에 메시지 추가 [case-id]"
2. 메시지가 표시되면 메시지를 제공합니다.
3. 채팅에서 메시지가 추가되었는지 확인합니다.

AWS Support가 사례에 응답하면 알림을 받게 됩니다.

사례 해결

지원 사례를 해결하려면:

1. 채팅에 질문: "[case-id] 사례 해결"
2. 메시지가 표시되면 해상도를 확인합니다.

Note

AWS Support에서 해결한 사례만 해결할 수 있습니다.

지원 사례 관리 비활성화

1. AWS Transform 콘솔을 엽니다.
2. 탐색 창에서 설정을 선택합니다.
3. 지원에서 지원 사례 관리 비활성화를 선택합니다.
4. 변경 사항 저장을 선택합니다.

Note

지원 사례 관리를 비활성화하면 채팅 기반 사례 관리 인터페이스는 제거되지만 기존 사례는 종료되지 않습니다. AWS 지원 센터를 통해 사례에 계속 액세스할 수 있습니다.

사용량 원격 측정

AWS Transform IDE 플러그인, AWS Transform Agent Skill 및 AWS Transform Kiro Power는 변환 실행 중에 기본적으로 사용량 원격 측정을 수집합니다. 원격 측정은 IDE 이름(예: VS Code 또는 Kiro), AI 에이전트 이름(예: Claude Code 또는 OpenAI Codex), 실행 모드(로컬 또는 원격)와 같은 다양한 데이터 포인트로 구성됩니다. 이 데이터는 AWS Transform에서 호환성 테스트와 지연 시간 및 안정성의 우선순위를 지정하는 데 사용됩니다.

원격 측정을 비활성화하려면 채팅 세션 중에 원격 측정을 내보내지 않도록 에이전트에게 알립니다. 이 옵트아웃은 현재 채팅 세션에만 적용되며 각 새 세션에 대해 반복해야 합니다. AWS 변환 CLI를 직접 실행하는 경우 `ATX_DISABLE_TELEMETRY=true` 환경 변수를 설정합니다.

운영 데이터

당사는 서비스를 제공하고 서비스 성능을 평가하기 위해 사용하는 기능, 오류 로그 및 자연어 피드백 (예: AWS 변환 계획 진행 승인 여부 또는 제안된 계획 반복 지침 제공 여부)을 기반으로 하는 지표와 같은 변환 사용과 관련된 운영 신호를 수집할 수 있습니다.

변경 로그

다음 표에서는 AWS 변환에 대한 주목할 만한 릴리스 및 업데이트에 대해 설명합니다.

Date	제목	설명	링크
2026-07-16	AWS 마이그레이션을 위한 변환에 다운로드 가능한 워크스페이스 요약 보고서 추가	AWS 이제 마이그레이션을 위한 변환을 통해 워크스페이스 요약 보고서를 다운로드 가능한 PDF로 생성할 수 있습니다. 이 보고서는 작업 상태, 워크플로 단계 진행 상황, 웨이브 계획, 네트워크 마이그레이션, 랜딩 존 구성, 리호스팅 진행 상황, 생성된 아티팩트 등 워크스페이스의 모든 마이그레이션 작업 데이터를 통합합니다.	워크스페이스 요약 보고서 다운로드
2026-07-03	AWS 변환 검색 도구에 Oracle Database 지원 추가	AWS 변환 검색 도구는 이제 VMware, Hyper-V 및 베어 메탈 서버의 데이터베이스에서 직접 자세한 Oracle 메타데이터를 수집합니다. 직접 SQL 연결을 통해 Oracle 인스턴스를 검색할 수 있습니다. 이 도구는 컨테이너 데이터베이스/플러깅 가능한 데이터베이스(CDB/PDB) 열거, 구성 요소 인벤토	Oracle Database 검색

Date	제목	설명	링크
		리 및 데이터 파일 크기를 수집합니다. 또한 Real Application Clusters(RAC), Data Guard 및 멀티테넌트 아키텍처에 대한 토폴로지 플래그를 캡처합니다. 데이터베이스 자격 증명을 구성하지 않은 경우 도구는 OS 수준 탐지로 돌아갑니다. 모든 Oracle 버전이 지원됩니다.	
2026-06-22	메인프레임 현대화 에이전트에 대한 남아메리카(상파울루) 리전 지원	AWS 이제 남아메리카(상파울루) 리전(sa-east-1)에서 메인프레임 현대화 에이전트에 대한 변환을 사용할 수 있습니다. 지원되는 리전 및 교차 리전 추론 테이블에 sa-east-1을 추가했습니다.	지원되는 리전 , 교차 리전 추론
2026-06-22	AWS VMware 마이그레이션을 위한 변환에서 현지화 지원	AWS 이제 VMware 마이그레이션을 위한 변환이 현지화를 지원합니다. 설정 아이콘을 선택하고 원하는 언어를 선택하여 VMware 마이그레이션 워크플로를 사용할 때 웹 애플리케이션의 표시 언어를 변경할 수 있습니다.	현지화 설정

Date	제목	설명	링크
2026-06-18	AWS 마이그레이션을 위한 변환은 모든 AWS 상용 리전을 마이그레이션 대상으로 지원합니다.	AWS VMware 마이그레이션을 위한 변환은 중동(바레인) 및 중동(UAE)을 제외한 모든 AWS 상용 리전을 마이그레이션 대상으로 지원합니다. 마이그레이션 대상 리전은 랜딩 존, 네트워크 인프라 및 서버 리호스팅을 포함하여 마이그레이션된 리소스가 배포되는 AWS 리전입니다.	지원되는 마이그레이션 대상 리전
2026-06-18	AWS 마이그레이션을 위한 변환을 사용하면 기존 ENIs를 시작 템플릿에 연결할 수 있습니다.	AWS 변환을 사용하면 마이그레이션을 위해 기존 탄력적 네트워크 인터페이스(ENIs)를 시작 템플릿에 연결할 수 있습니다. AWS 변환은 대상 계정에서 찾은 모든 기존 ENIs 표시하고 인스턴스가 시작될 때 시작 구성을 통해 사용할 수 있도록 태그를 지정할 수 있습니다.	마이그레이션을 위한 ENI 리소스 태그 지정

Date	제목	설명	링크
2026-06-18	AWS 마이그레이션을 위한 변환을 통해 복제 및 시작 설정을 구성할 수 있습니다.	AWS 변환을 사용하면 마이그레이션에 대한 복제 설정 및 시작 설정을 구성할 수 있습니다. 대상 계정별 또는 특정 소스 서버 간에 구성을 설정할 수 있습니다.	복제 및 시작 설정

Date	제목	설명	링크
2026-06-17	생성형 AI 워크로드에 대한 Model-to-model 마이그레이션 평가	AWS 변환은 이제 model-to-model 마이그레이션 사용자 지정 변환을 제공합니다. 변환은 생성형 AI 워크로드를 평가합니다. 타사 공급자에서 Amazon Bedrock으로 이전하기 위한 마이그레이션 계획을 생성합니다. AI 기반 에이전트는 코드베이스를 스캔하여 사용 중인 모든 AI SDK와 모델을 식별합니다. 에이전트는 대화형 질문을 통해 마이그레이션 요구 사항을 수집합니다. 그런 다음 투명한 비용 비교 및 프로덕션 지원 코드 변경으로 모델을 Amazon Bedrock에 매핑합니다. LiteLLM 또는 Ollama를 통해 OpenAI, Google Gemini, 직접 Anthropic SDK 사용 및 오픈 소스 모델에서의 마이그레이션을 지원합니다. LangChain, LlamaIndex, CrewAI, LangGraph 및 다중 공급자 라우팅 계층을 포함한 직접 SDK 통합	새로운 소식, 사용자 지정 변환

Date	제목	설명	링크
		및 프레임워크 래핑 패턴을 처리합니다. 표준 AWS 변환 요금 외에 추가 비용 없이 사용할 수 있습니다.	
2026-06-16	AWS 메인프레임용 변환은 추적 가능한 재구성 워크플로를 제공합니다.	AWS 메인프레임용 변환은 이제 평가부터 코드 생성까지 연결되고 추적 가능한 재구성 경험을 제공합니다. z/OS COBOL 및 PL/I 워크로드를 실행하는 기업은 포트폴리오를 평가하여 연결된 단일 워크플로에서 개별 비즈니스 기능을 식별하고, 비즈니스 규칙을 추출하고, 개발 준비된 요구 사항을 생성하고, 추적 가능한 클라우드 네이티브 코드를 생성할 수 있습니다. 모든 요구 사항은 전체 감사 가능성을 위해 소스 코드로 다시 추적됩니다.	새로운 소식, 설명서

Date	제목	설명	링크
2026-06-16	AWS 이제 변환에 서 Amazon FSx for NetApp ONTAP을 대 상 스토리지로 지원(퍼 블릭 미리 보기)	이제 컴퓨팅 리호스팅 의 일환으로 Amazon EBS 외에도 블록 스토리지 워크로드 를 Amazon FSx for NetApp ONTAP으로 마이그레이션할 수 있 습니다. AWS 변환은 컴퓨팅 및 네트워크를 처리하는 동일한 마이 그레이션 웨이브 내에 서 블록 스토리지 데이 터를 FSx for ONTAP 볼륨에 직접 복제합니 다.	새로운 소식 게시물, 설명서
2026-06-05	Amazon RDS for SQL Server TCO 평가 지원	이제 온프레미스 SQL Server 데이터베이스 를 Amazon RDS for SQL Server로 마이 그레이션할 때 비용 을 추정할 수 있습니 다. AWS 변환의 AI 기 반 TCO 평가를 사용 하여 환경을 분석하고 최적의 데이터베이스 인스턴스 권장 사항을 얻을 수 있습니다. 이 평가는 데이터베이스 Savings Plans하여 최 대 20%까지 절감할 수 있습니다.	새로운 소식 게시물, 설명서

Date	제목	설명	링크
2026-06-04	AWS 이제 변환 검색 도구가 네트워크 마이그레이션 입력 소스로 지원됩니다.	이제 AWS Transform Discovery 도구를 modelizeIT와 함께 네트워크 마이그레이션의 소스로 사용하여 VMware 워크로드와 비 VMware 워크로드를 모두 실행하는 환경에서 하이브리드 네트워크 마이그레이션을 활성화할 수 있습니다.	사용 설명서
2026-05-27	AWS 사용자 지정 설명서 변환에 클라이언트 측 스킴 예제 및 모범 사례 추가	이제 클라이언트 측 기술 설명서에는 Dockerfile 규정 준수, 데이터베이스 마이그레이션 안전, Terraform 정책 적용 및 API 사용 중단 도우미에 대한 실제 예제와 기술 구축 및 공유 모범 사례가 포함되어 있습니다.	설명서
2026-05-22	이제 AWS 변환에서 새로운 에이전트 마이그레이션 평가 기능을 사용할 수 있습니다.	AWS 이제 변환은 가정 시나리오, 사용자 지정 가능한 가정, 유연한 파일 형식 지원, 여러 새로운 총 소유 비용(TCO) 평가 기능을 포함한 고급 마이그레이션 평가 기능을 제공합니다.	새로운 소식 게시물, 설명서

Date	제목	설명	링크
2026-05-20	AWS 변환은 네트워크 마이그레이션 검토 중에 기존 VPCs	AWS 이제 변환은 네트워크 마이그레이션 검토 중에 대상 계정의 기존 VPCs를 감지합니다. 매핑된 VPCs와 함께 기존 VPCs 보고, CIDR 충돌을 식별하고, 배포 전에 해결할 수 있습니다.	설명서
2026-05-14	AWS 이제 Kiro, Claude, Cursor 및 Codex에서 변환 에이전트 사용 가능	AWS 이제 Kiro 전원, 에이전트 플러그인 및 AWS 변환 MCP 서버를 통해 변환 에이전트에 액세스할 수 있으므로 개발자가 원하는 개발 환경에서 직접 변환 기능을 사용할 수 있습니다.	새로운 내용 게시물
2026-05-14	AWS Transform은 사용자 지정 변환 에이전트를 빌드하기 위한 에이전트 빌더 툴킷을 소개합니다.	이제 파트너와 고객은 에이전트 빌더 도구 키트 Kiro 파워를 사용하여 전문 변환 에이전트를 구축, 공유 및 등록하고 사용자 지정 도구 및 워크플로를 AWS 변환과 통합할 수 있습니다.	새로운 내용 게시물

Date	제목	설명	링크
2026-05-14	AWS 변환은 AWS Toolkit for Visual Studio에 에이전트 AI 어시스턴트를 추가합니다.	이제 .NET 개발자는 IDE 및 웹 콘솔에서 전체 컨텍스트를 보존하면서 Visual Studio에서 직접 대화형 step-by-step 안내 환경을 통해 애플리케이션을 현대화할 수 있습니다.	새로운 소식 게시물
2026-05-14	AWS 변환은 이제 고객 소유 아티팩트 스토어를 지원합니다.	자체 Amazon S3 버킷을 구성하고 선택적으로 자체 AWS KMS 키로 아티팩트를 암호화하여 변환 아티팩트가 저장되는 위치를 완벽하게 제어할 수 있습니다.	새로운 소식 게시물 , 사용 설명서

Date	제목	설명	링크
2026-05-14	AWS Transform, 마이그레이션 전략(7R) 권장 사항 추가	이제 AWS 변환을 사용하여 검색된 인벤토리를 분석하고 모든 서버 및 애플리케이션에 대한 마이그레이션 전략 권장 사항을 얻을 수 있습니다. 권장 사항은 업계 표준 7가지 마이그레이션 전략(7R)을 따릅니다. 각 권장 사항에는 제안된 AWS 대상 서비스, 신뢰도 점수 및 그 근거가 포함됩니다. 대화형 HTML 대시보드, PDF 또는 Microsoft PowerPoint 출력을 생성할 수 있습니다.	7Rs 권장 사항
2026-05-11	AWS 변환은 마이그레이션 중에 컨테이너화 기능을 추가합니다.	AWS 이제 변환은 마이그레이션 중에 컨테이너로 애플리케이션 리플랫폼, Dockerfile 생성 자동화, CVE 스캔을 통한 컨테이너 이미지 빌드, Amazon ECS 또는 Amazon EKS로의 배포를 지원합니다.	새로운 소식 게시물, 사용 설명서

Date	제목	설명	링크
2026-05-01	AWS 이제 Transform에서 Power BI 및 Tableau용 BI 마이그레이션 에이전트를 빠른 속도로 제공	Wavicle Data Solutions의 파트너 구축 에이전트는 Power BI 및 Tableau 대시보드를 AWS 변환 워크플로 내의 빠른 자산으로 변환합니다.	새로운 소식 게시물
2026-04-21	AWS 이제 6개의 추가 AWS 리전에서 사용자 지정 변환을 사용할 수 있습니다.	AWS 사용자 지정 변환은 아시아 태평양, 캐나다 및 유럽(런던)으로 확장되어 총 8개 AWS 리전에 도달합니다.	새로운 소식 게시물
2026-04-15	AWS 변환은 마이그레이션 워크플로 내에 랜딩 존 생성을 추가합니다.	마이그레이션 워크플로 내에 직접 랜딩 존 생성을 추가했습니다. 기존 파운데이션에 대한 검사를 AWS 변환하고, 조직 단위(OU) 구조 및 대상 계정을 권장하며, 완전 자동화된 배포 또는 코드형 인프라(IaC) 출력(CloudFormation, AWS CDK 또는 랜딩 존 액셀러레이터(LZA) 형식)을 제공합니다.	새로운 소식 게시물, 설명서

Date	제목	설명	링크
2026-04-15	AWS 변환에 마이그레이션 계획 다이어그램 및 보고서 추가	이제 마이그레이션 계획 중에 대화형 다이어그램과 분석 보고서를 생성할 수 있습니다. 다이어그램 유형에는 네트워크 토폴로지 맵, 애플리케이션 종속성 그래프, 웨이브 Gantt 차트 및 일반 차트가 포함됩니다. 보고서 유형에는 위험 평가, 7Rs 사항 및 사용자 지정 분석 보고서가 포함됩니다. 출력은 대화형 HTML, PDF 또는 Microsoft PowerPoint(.pptx) 파일로 사용할 수 있습니다.	다이어그램 작성 및 보고
2026-04-14	AWS 이제 Kiro 및 VS Code에서 변환을 사용할 수 있습니다.	AWS 이제 IDE, CLI 및 웹 콘솔 표면에서 작업 상태를 공유하여 Kiro 및 VS Code에서 사용자 지정 변환에 액세스할 수 있습니다.	새로운 내용 게시물

Date	제목	설명	링크
2026-04-10	AWS 네트워크 마이그레이션을 위한 보안 그룹 매핑으로 DHCP를 추가하는 변환	네트워크 마이그레이션 중에 보안 그룹 매핑을 사용하는 DHCP에 대한 지원이 추가되었습니다. DHCP 지원 마이그레이션 워크로드가 있는 경우 이제 마이그레이션 후에도 보안 규칙이 유효한지 확인할 수 있습니다. 이는 Transit Gateway를 통해 참조하는 VPC 내 보안 그룹과 VPC 간 및 계정 간 아웃바운드 규칙 모두에 적용됩니다.	설명서
2026-03-31	AWS 사용자 지정 변환, 자동 코드베이스 분석의 일반 가용성 발표	포괄적인 코드베이스 분석 변환은 모든 언어에서 아키텍처 문서, 기술 부채 보고서 및 현대화 권장 사항을 생성하여 일반 가용성에 도달합니다.	새로운 게시물
2026-03-31	AWS 사용자 지정 변환은 대규모로 코드를 현대화하기 위한 새로운 관리형 변환을 도입합니다.	Node.js 업그레이드 (일반 가용성), Java 최적화, Log4j 마이그레이션, Angular-to-React, Angular 업그레이드, Vue 업그레이드 (조기 액세스) 등 7가지 새로운 관리형 변환이 추가되었습니다.	새로운 내용 게시물

Date	제목	설명	링크
2026-03-20	AWS 변환에 네트워크 마이그레이션을 위한 퍼블릭 APIs 추가	네트워크 마이그레이션을 위한 퍼블릭 APIs 추가되어 파트너 및 프로그래밍 방식으로 네트워크 마이그레이션 기능에 액세스할 수 있습니다.	API Reference
2026-01-14	AWS 사용자 지정 add AWS PrivateLink 지원 및 유럽(프랑크푸르트)으로 확장	AWS 변환 사용자 지정은 이제 AWS PrivateLink를 통한 프라이빗 VPC 액세스를 지원하며 미국 동부(버지니아 북부) 외에도 유럽(프랑크푸르트)에서도 사용할 수 있습니다.	새로운 소식 게시물
2025-12-23	AWS 변환을 통해 하이브리드 데이터 센터 마이그레이션을 위한 네트워크 변환 가능	AWS VMware용 변환은 수동 매핑 없이 하이브리드 데이터 센터 네트워크 구성(VLANs, IP 범위)을 AWS VPCs, 서브넷 및 보안 그룹으로 자동 변환합니다.	새로운 소식 게시물
2025-12-01	AWS 조직 전체의 현대화를 가속화하기 위해 사용자 지정 AWS 변환 출시	AWS 사용자 지정 변환은 일반 가용성에 도달하므로 조직은 단일 CLI 명령을 통해 대규모로 반복 가능한 코드 변환을 자동화할 수 있습니다.	새로운 소식 게시물

Date	제목	설명	링크
2025-12-01	AWS 엔터프라이즈 VMware 마이그레이션을 위한 새로운 에이전트 AI 기능 추가	AWS 이제 Transform의 VMware 에이전트는 온프레미스 환경을 검색하고, 종속성을 매핑하고, 마이그레이션 웨이브 계획을 생성하고, HyperV, Nutanix, KVM 및 베어 메탈 대상 간에 마이그레이션할 수 있습니다.	새로운 소식 게시물
2025-12-01	AWS 변환은 풀 스택 Windows 현대화를 위한 AI 에이전트를 시작합니다.	새로운 풀 스택 Windows 에이전트는 .NET 앱 및 SQL Server 데이터베이스를 Aurora PostgreSQL로 자동 변환하여 Amazon ECS 또는 EC2 Linux의 컨테이너에 배포합니다.	새로운 소식 게시물
2025-12-01	AWS 변환은 .NET 변환 기능을 확장하고 개발자 경험을 개선합니다.	AWS 변환은 AWS Toolkit for Visual Studio를 통해 .NET 10 지원, Blazor 이식예 ASP.NET Web Forms, 향상된 대화형 IDE 환경을 추가합니다.	새로운 소식 게시물

Date	제목	설명	링크
2025-12-01	AWS 메인프레임용 변환은 새로운 테스트 자동화 기능을 제공합니다.	AWS 메인프레임용 변환은 자동화된 테스트 계획 생성, 테스트 데이터 수집 스크립트 및 테스트 사례 자동화를 도입하여 메인프레임 현대화 테스트를 가속화합니다.	새로운 소식 게시물
2025-12-01	AWS 메인프레임용 변환이 이제 애플리케이션 재구상 지원	새로운 데이터 및 활동 분석과 비즈니스 로직 추출 기능을 통해 레거시 메인프레임 애플리케이션을 클라우드 네이티브 아키텍처로 분해할 수 있습니다.	새로운 게시물
2025-11-13	AWS 변환으로 Landing Zone Accelerator 네트워크 구성 자동화	AWS VMware용 변환은 LZA 호환 네트워크 YAML 파일을 자동으로 생성하여 VMware 환경에서 다중 계정 클라우드 인프라 설정을 간소화합니다.	새로운 게시물
2025-07-16	AWS 메인프레임용 변환에 향상된 코드 리팩터링 및 비즈니스 로직 기능 도입	AWS 메인프레임용 변환은 보강(코드 재구성)의 일반 가용성을 추가하고 애플리케이션 수준 비즈니스 로직 추출을 확장하여 코드 품질을 개선합니다.	새로운 소식 게시물

Date	제목	설명	링크
2025-05-15	AWS 이제 VMware용 변환을 정식으로 사용할 수 있습니다.	AWS 검색부터 배포까지 전체 VMware 현대화 수명 주기를 자동화하는 에이전트 AI 서비스인 VMware용 변환은 일반 가용성에 도달합니다.	새로운 내용 게시물
2025-05-15	AWS 이제 메인프레임에 대한 변환을 정식으로 사용할 수 있습니다.	AWS IBM z/OS 애플리케이션을 대규모로 현대화하기 위한 최초의 에이전트 AI 서비스인 메인프레임의 변환은 새로운 분석, 분해 및 작업 관리 기능을 통해 일반 가용성에 도달합니다.	새로운 내용 게시물

[이 데이터를 다운로드](#)합니다.

AWS 변환 사용 설명서의 문서 기록

다음 표에서는 AWS 변환 사용 설명서의 문서 기록을 설명합니다.

변경 사항	설명	날짜
지속적인 현대화 포트폴리오 분석 및 문제 해결	자동 코드 분석 및 문제 해결을 위한 지속적 현대화 AWS 변환 기능(atx ct 하위 명령)을 문서화하는 새 장을 추가했습니다. 지속적인 현대화를 참조하세요 .	2026년 6월 3일
브라운필드 네트워크: 기존 VPCs 가시성	네트워크 마이그레이션 검토 중에 기존 VPC 감지 기능이 추가되었습니다. AWS 변환은 대상 계정에 이미 배포된 VPCs를 자동으로 감지하고 매핑된 VPCs와 CIDR 충돌에 플래그를 지정합니다. 대상 계정VPCs를 참조하세요 .	2026년 5월 18일
사용자 지정 AWS 변환을 위한 기술 형식, 클라이언트 측 기술 및 하위 에이전트 로그 추가	변환 정의는 이제 스킴 형식 (SKILL.mdYAML 프론트미터 및 선택적 references/ 폴더 포함)을 사용합니다. 추가 기능으로 에이전트를 확장하기 위한 클라이언트 측 기술과 향상된 디버깅을 위한 하위 에이전트 로그가 추가되었습니다. CLI 버전 2.0 이상이 필요합니다. 변환 정의 및 클라이언트 측 기술을 참조하세요 . https://docs.aws.amazon.com/transform/latest/userguide/custom-	2026년 5월 11일

[workflows.html#custom-client-side-skills](#)

[소스 코드 컨테이너화 추가](#)

AWS 이제 변환은 생성형 AI를 사용하여 애플리케이션을 컨테이너화할 수 있습니다. Git 리포지토리 또는 zip 업로드에서 소스 코드를 제공하면 AWS Transform은 이를 분석하고, Docker 아티팩트를 생성하고, Amazon ECR에 컨테이너 이미지를 게시하고, 코드형 인프라를 생성하고, Amazon Elastic Container Service 또는 Amazon Elastic Kubernetes Service에 배포합니다. [소스 코드 컨테이너화](#)를 참조하세요.

2026년 5월 7일

[네트워크 최적화 작업 및 권장 사항 안내 추가](#)

VPC 및 서브넷 작업(삭제, 제외, 병합, 분할, 크기 조정, 이름 변경, IP 주소 변경)을 사용하여 5단계: 네트워크 검토 및 최적화와 이름 지정 표준화, 범위 검토, 용량 적정 크기 조정, 보안 검토 및 VPC 통합에 대한 권장 사항 안내가 추가되었습니다. [네트워크 검토 및 최적화](#)를 참조하세요.

2026년 4월 27일

[AWS 6개의 새 리전에서 사용할 가능한 사용자 지정 변환](#)

사용자 [AWS 지정 변환](#)에서 ca-central-1, eu-west-2, ap-northeast-1, ap-northeast-2, ap-southeast-2 및 ap-south-1에 대한 지원이 추가되었습니다.

2026년 4월 21일

커넥터 권한 설명서 업데이트	S3, MGN, Migration Hub 권한, 워크로드 마이그레이션 및 랜딩 존 인프라 프로비저닝을 포함하는 대상 AWS 계정 커넥터에 대한 자세한 권한 분류가 추가되었습니다. 대상 연결을 참조 AWS 계정하세요.	2026년 4월 19일
VMware 마이그레이션 작업 유형 업데이트	검색 및 마이그레이션 계획, 랜딩 존 및 랜딩 존, 네트워크 및 서버 마이그레이션 작업 유형이 추가되었습니다. Network migration only to Network migration and Migration planning to Build migration plan으로 이름을 변경했습니다. VMware 마이그레이션 작업 유형을 참조하세요.	2026년 4월 19일
재구성된 Connect 대상 AWS 계정	커넥터 설정을 지원되는 대상 리전, 계정 역할, 위임된 관리자 지침, IAM 역할을 포함한 마이그레이션 유형 선택, MAP 계약, 커넥터 구성의 세 단계로 재구성했습니다. 대상 연결을 참조 AWS 계정하세요.	2026년 4월 19일
추가 server-migration-only 대상 리전 추가	네트워크 마이그레이션 없이 서버 마이그레이션 작업에 사용할 수 있는 14개의 추가 상용 리전이 문서화되어 있으며 2026년 Q3까지 허용 목록 요구사항이 있습니다. 지원되는 대상 리전을 참조하세요.	2026년 4월 19일

서버 마이그레이션 장 추가	계정 구조, IAM 역할, 위임된 관리자 설정, 복제 에이전트 배포, 테스트 및 전환 등 전체 리호스팅 워크플로를 다루는 새로운 Migrate 서버 장이 추가되었습니다.	2026년 4월 19일
랜딩 존 빌드 장 추가	랜딩 존 프로비저닝에 대한 커넥터 권한 세부 정보가 포함된 새로운 랜딩 존 빌드 장이 추가되었습니다.	2026년 4월 19일
보안 그룹 매핑 및 참조	네트워크 마이그레이션 에 대한 문서를 참조하는 보안 그룹 매핑 전략(MAP, MAP_DHCP, SKIP) 및 보안 그룹이 추가되었습니다.	2026년 4월 13일
지원되지 않는 네트워크 파일 유형에 대한 자동 변환	네트워크 마이그레이션 에서 지원되지 않는 네트워크 구성 파일 유형의 자동 변환에 대한 지원이 추가되었습니다.	2026년 4월 6일
데이터베이스 마이그레이션을 위한 KMS 키 정책 추가	데이터베이스 마이그레이션을 위한 암호화 섹션이 추가되었습니다.	2026년 3월 26일
문서화된 새 AWS 관리형 정책	DBModProvisioningAndMigration 섹션이 추가되었습니다.	2026년 3월 24일
문서화된 새 AWS 관리형 정책	DBModDiscoveryAndAssessment 섹션이 추가되었습니다.	2026년 3월 24일
네트워크 다이어그램 생성	네트워크 마이그레이션 에 선택적 네트워크 다이어그램 생성(Mermaid 및 PNG 형식)이 추가되었습니다.	2026년 3월 18일

방화벽 및 SDN 구성 파일 지원	네트워크 마이그레이션 에서 네트워크 마이그레이션을 위한 Palo Alto Networks, Fortinet FortiGate 및 Cisco ACI 구성 파일에 대한 지원이 추가되었습니다.	2026년 2월 11일
네트워크 리소스에 대한 사용자 지정 태그 지정	Migrate 네트워크의 네트워크 마이그레이션에 대한 작업 수준 및 VPC 수준 사용자 지정 태그 지정 지원이 추가되었습니다.	2026년 1월 28일
지원 설명서 추가	섹션에 AWS 대한 지원이 추가되었습니다.	2025년 12월 23일
문서화된 새 AWS 관리형 정책	AWSTransformCustomFullAccess , AWSTransformCustomExecuteTransformations 및 AWSTransformCustomManageTransformations 섹션이 추가되었습니다.	2025년 12월 7일
VMware 마이그레이션	VMware 마이그레이션 섹션을 업데이트했습니다.	2025년 12월 1일
AWS 관리형 정책 업데이트	추가된 권한을 반영하도록 AWSServiceRoleForAWSTransform 설명서를 업데이트했습니다.	2025년 12월 1일
지원되는 리전	지원되는 리전 주제가 업데이트되었습니다.	2025년 12월 1일
메인프레임 현대화	메인프레임 현대화 섹션을 업데이트했습니다.	2025년 12월 1일

시작하기	시작하기 주제가 업데이트되었습니다.	2025년 12월 1일
풀 스택 Windows 현대화	업데이트된 .NET 섹션과 새로운 SQL Server 현대화 섹션이 포함된 풀 스택 Windows 현대화 주제가 추가되었습니다. https://docs.aws.amazon.com/transform/userguide/sql-server-modernization.html	2025년 12월 1일
검색 도구	검색 도구 섹션이 추가되었습니다.	2025년 12월 1일
업데이트된 AWS 관리형 정책	확장된 IAM 역할 검사 권한, ECS 서비스 연결 역할 생성 및 ECR 암호화 지원을 위한 KMS 권한으로 AWSTransformApplicationECSDeploymentPolicy 를 업데이트했습니다.	2025년 11월 22일
AWS 관리형 정책 업데이트	추가 EC2 네트워킹, IAM 역할 검사, S3 버킷 관리 및 KMS 암호화 권한으로 AWSTransformApplicationDeploymentPolicy 를 업데이트했습니다.	2025년 11월 22일
검색 수집기	AWS 검색 변환 도구 설명서가 추가되었습니다.	2025년 10월 31일
VMware 마이그레이션 아키텍처 다이어그램 추가	Migrate 네트워크 에 VMware 마이그레이션 아키텍처 다이어그램이 추가되었습니다.	2025년 10월 23일
VMware 마이그레이션 결과 업데이트	Migrate network 의 마이그레이션 결과 정보가 업데이트되었습니다.	2025년 10월 12일

VMware 마이그레이션 결과 업데이트	네트워크 마이그레이션에서 마이그레이션 결과 정보가 업데이트되었습니다.	2025년 10월 12일
S3 커넥터 설명서	.NET 웹 앱에 대한 S3 커넥터 설명서 가 추가되었습니다.	2025년 10월 8일
새 사용자 커넥터 주제	사용자 커넥터 주제가 추가되었습니다.	2025년 9월 21일
AWS 관리형 정책 업데이트	AWSServiceRoleForAWSTransform 설명서를 업데이트했습니다.	2025년 9월 17일
스토리지 평가 지원	스토리지 평가 에 대한 NetApp Data Infrastructure Insights(DII) 파일 지원이 추가되었습니다.	2025년 9월 2일
대상 리전 업데이트	지원되는 대상 리전 3개가 추가되었습니다.	2025년 8월 31일
관리형 정책 업데이트	AWSServiceRoleForAWSTransform 에서 사용할 IAM Identity Center 읽기 전용 권한이 추가되었습니다.	2025년 8월 29일
문서화된 새 AWS 관리형 정책	AWSTransformApplicationDeploymentPolicy 섹션이 추가되었습니다.	2025년 8월 28일
인터페이스 엔드포인트	인터페이스 엔드포인트 주제가 추가되었습니다.	2025년 7월 9일
최초 릴리스	AWS 변환 사용 설명서의 최초 릴리스입니다.	2025년 5월 15일

기계 번역으로 제공되는 번역입니다. 제공된 번역과 원본 영어의 내용이 상충하는 경우에는 영어 버전이 우선합니다.