aws

규제된 AWS 랜딩 존의 OU 구조: 제약 산업의 예

# AWS 권장 가이드

# AWS 권장 가이드: 규제된 AWS 랜딩 존의 OU 구조: 제약 산업의 예

# Table of Contents

# 규제 AWS 랜딩 존의 OU 구조: 제약 산업의 예

Katja Mueller, Petar Forai, Keval Sheth, Amazon Web Services(AWS)

2023년 3월(문서 기록)

AWS 는 의료를 포함한 특정 산업을 지원하는 여러 랜딩 존 액셀러레이터 구성을 제공합니다. 의료용 Landing Zone Accelerator는 AWS 모범 사례 및 여러 글로벌 규정 준수 프레임워크에 부합하는 다중 계정 환경의 관리 및 거버넌스를 용이하게 AWS Control Tower 하기 위해와 함께 사용됩니다. 거버넌스 오케스트레이션의 중요한 측면 중 하나는 조직 단위(OUs)를 사용하여 AWS 계정 그룹화하여 단일 단위로 관리할 수 있다는 것입니다.

이 가이드에서는 회사의 클라우드 성숙도가 증가함에 따라 기존 OU 구조를 재설계하기 위한 모범 사례와 고려 사항을 설명합니다. 대규모 제약 회사의 AWS Control Tower 구현을 기반으로 한 실제 예제를 소개하고 해당 구현에서 얻은 교훈을 설명합니다. AWS 랜딩 존 설계는 일회성 작업이 아닙니다. 진화할 수 있고 진화할 수 있어야 해야 합니다. 이 가이드에서 강조한 AWS 모범 사례와 팁을 적용하여 이러한 변화를 성공하고 효율적으로 달성할 수 있습니다.

# 개요

다국적 제약 회사와 협력하여 AWS에서 개념 증명(PoC) 활동을 실행함으로써 온프레미스에서 AWS 클라우드로 애플리케이션을 마이그레이션하는 방법을 탐색했습니다. 프로덕션 워크로드를 포함하도록 마이그레이션 워크플로를 규모를 조정하고 가속화하기 시작하면서 목표를 지원하기 위해 규제되고 규정을 준수하는 AWS 랜딩 존이 필요했습니다. 그래서 AWS Control Tower를 사용하여 새 AWS 랜딩 존을 설계하고 구현했습니다.

새로운 AWS 랜딩 존과 조직에서 조직 단위(OU)의 구조가 중요합니다. OU는 AWS Organizations를 사용하여 생성된 AWS 계정의 논리적 그룹입니다. OU를 사용하면 계층 구조로 AWS 계정을 구성하고 관리 및 거버넌스 제어를 일관된 방식으로 쉽게 적용할 수 있습니다.

정책 기반 제어를 OU 및 AWS 계정에 연결할 수 있습니다. OU 내의 하위 OU는 이러한 제어를 자동으로 상속합니다. 따라서 OU는 AWS Organizations에서 보안 및 거버넌스를 관리하는 데 중요한 역할을 합니다.

정책은 AWS 계정 그룹에 적용하려는 제어를 정의하는 하나 이상의 명령문이 포함된 JSON 문서입니다. AWS Organizations에서는 현재 서비스 제어 정책(SCP)이라고도 하는 네 가지 유형의 정책을 지원합니다. SCP는 서로 다른 AWS 계정에서 사용할 수 있는 AWS 서비스 및 작업을 정의합니다. 예를 들어 SCP를 사용하여 Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스가 특정 인스턴스 유형을 사용하도록 요구할 수 있습니다.

## 정책 유형

SCP 정책 유형은 다음을 포함합니다.

- 허용 목록과 거부 목록은 SCP를 적용하여 계정에 사용 가능한 권한을 필터링할 수 있는 보완적인 전략입니다.
- 태그 정책을 사용하면 여러 계정에서 태그 키와 태그 값의 기본 대소문자 처리를 포함해 태그를 일관된 방식으로 유지 관리할 수 있습니다.
- 백업 정책은 백업 기간 및 AWS 리전에서의 백업을 위한 대상 볼트와 같이 지원되는 리소스 유형에 대한 백업을 구성합니다.
- AI 서비스 옵트아웃 정책은 전 세계적으로 AWS 인공 지능(AI) 서비스의 지속적인 개선을 활성화하거나 비활성화합니다.

정책 상속 동작: 정책을 특정 OU에 연결하면 해당 OU 또는 하위 OU 바로 아래에 있는 계정이 정책을 상속합니다. 정책을 특정 계정에 연결하면 정책은 해당 계정에만 영향을 미칩니다. 예외 정책을 도입하

여 상속된 정책을 덮어쓸 수 있습니다. 권한을 거부하지 않는 한 상속을 통해 명시적으로 모든 권한이 루트(OU)에서 해당 OU 및 하위 OU의 모든 AWS 계정으로 전달될 수 있습니다. 권한을 거부하려면 추가 정책을 생성하여 적절한 OU 또는 AWS 계정에 연결합니다. 정책 상속 및 예외에 대한 자세한 내용은 AWS Organizations 설명서를 참조하세요.

또한 AWS Control Tower는 OU 구조를 사용하여 자체 감지 및 예방적 제어(가드레일이라고도 함) 세트를 제공합니다. AWS Control Tower 예방적 제어는 AWS Organizations의 SCP를 사용하여 작업을 방지합니다. 감지 제어는 AWS Config를 사용하여 제어에 대한 구성 드리프트를 보고합니다. 이러한 제어에 대한 자세한 내용은 AWS Control Tower 설명서를 참조하세요.

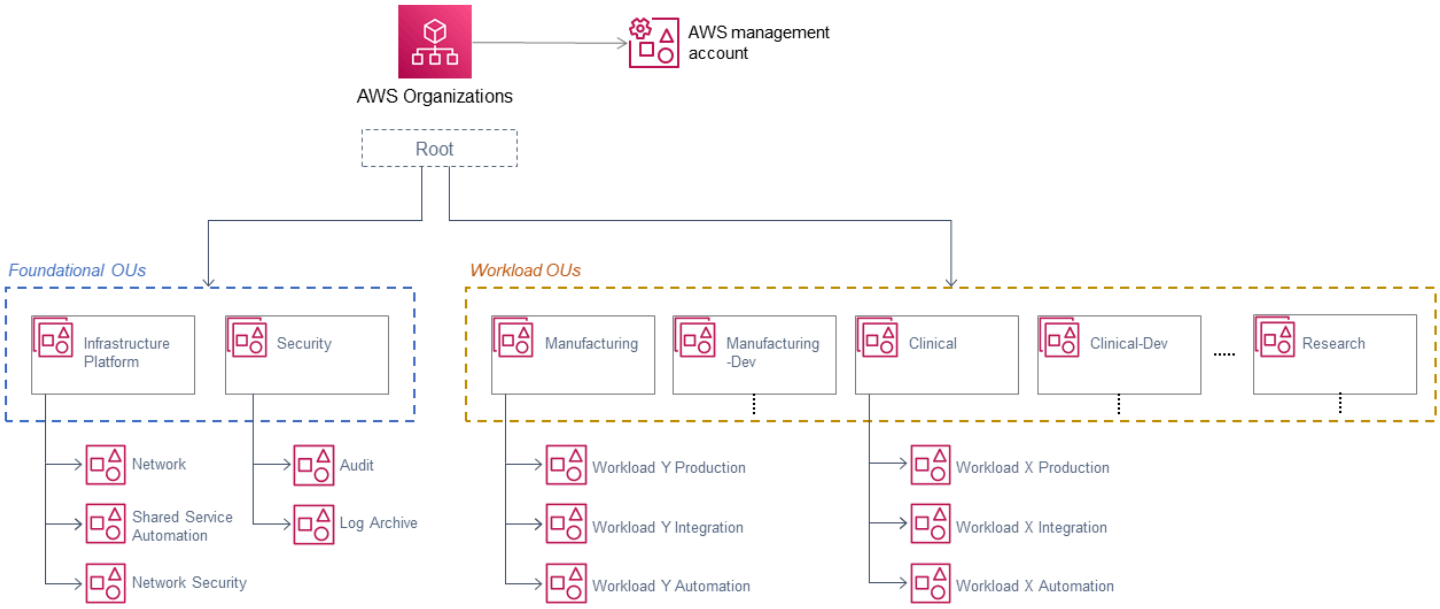
또한 AWS Security Hub CSPM를 활성화하여 보안 모범 사례 검사를 자동화하고, 보안 알림을 단일 위치 및 형식으로 집계하며, 모든 AWS 계정에서 전반적인 보안 태세를 파악할 수 있습니다.

# OU 설계: 1단계

이 예제의 다국적 제약 회사의 경우의 조직 및 OUs는 설정에 대한 AWS 권장 사항을 AWS Organizations 긴밀히 따랐습니다 AWS Control Tower. 예를 들어, 의 Landing Zone Accelerator AWS for Healthcare를 참조OUs, 플랫폼 인프라 OU 및 회사별 OU를 포함하여 공통 기본 OU로 간단한 OU 구조를 AWS Control Tower 초기에 프로비저닝했습니다. AWS Organizations OUs

## 아키텍처 설계

다음 다이어그램에서는 초기 OU 아키텍처를 보여줍니다.




## 보안 OU

보안 OU는 보안 기능과 AWS 계정 관련된 광범위한 그룹을 구성하고 두 계정(감사 및 로그 아카이브)을 사용하여 Amazon GuardDuty 및와 같은 environment. AWS core 보안 서비스에 대한 중앙 로깅 및 감사 액세스를 위해 보안 운영 데이터를 저장합니다 AWS Security Hub CSPM .

## 인프라 플랫폼 OU

인프라 기반 플랫폼 OU는 인프라 기반을 AWS 계정 제공하는 그룹입니다. 처음에이 OU 내에 배포된는 중앙 네트워킹 구성 요소(게이트웨이, 방화벽, 중앙 네트워킹 허브 및 유사한 서비스)를 AWS 계정 위한 입니다.

# 추가 OU

다른 회사별 OU(예: 임상 OU)는 하위 수준 계층 구조 내에서 기본 OU를 보강합니다. 워크로드는 다중 계정 구조와 해당 OU 내 분리된 환경으로 구현됩니다.

몇 가지 고려 사항 때문에 초기에 이와 같이 설계되었습니다.

- 중첩된 OUs 당시에서 사용할 수 없었 AWS Control Tower 기 때문에 광범위한 사용자 지정이 필요했습니다.
- 클라우드용으로 지정된 초기 워크로드는 임상 시험 또는 제조 장비 분석(기능 보기)과 같은 회사의 특정 측면에 중점을 둡니다.
- 회사는 다섯 가지 워크로드 환경(개발, 검증, 통합, 교육 및 프로덕션)을 구분합니다. 이 회사는 프로덕션 워크로드에 필요한 AWS 제어를 통한 엄격한 거버넌스 없이 애플리케이션을 개발하기 위한 플레이그라운드가 필요했습니다. 이를 위해 Manufacturing-Dev OU와 같은 개발 OU가 할당되었습니다.
- 워크로드 자동화는 각 애플리케이션 에코시스템의 일부였으며 분리가 필요하지 않았습니다.
- 인프라 검증(IQ) 및 GxP 규정 준수 프로세스에서는 OU 수준에서 AWS 제어를 구분할 필요가 없었습니다.

# OU 설계: 2단계

이 예제의 제약 회사는 검증된 프로덕션 워크로드를 기존 OU에 배포하여 클라우드의 새로운 성숙도 단계로 빠르게 진입했습니다. 이로 인해 초기 설계 검토가 시작되었으며, 규제된 AWS 랜딩 존으로 마이그레이션되는 워크로드가 많아짐에 따라 1단계 구조에 문제가 발생했습니다.

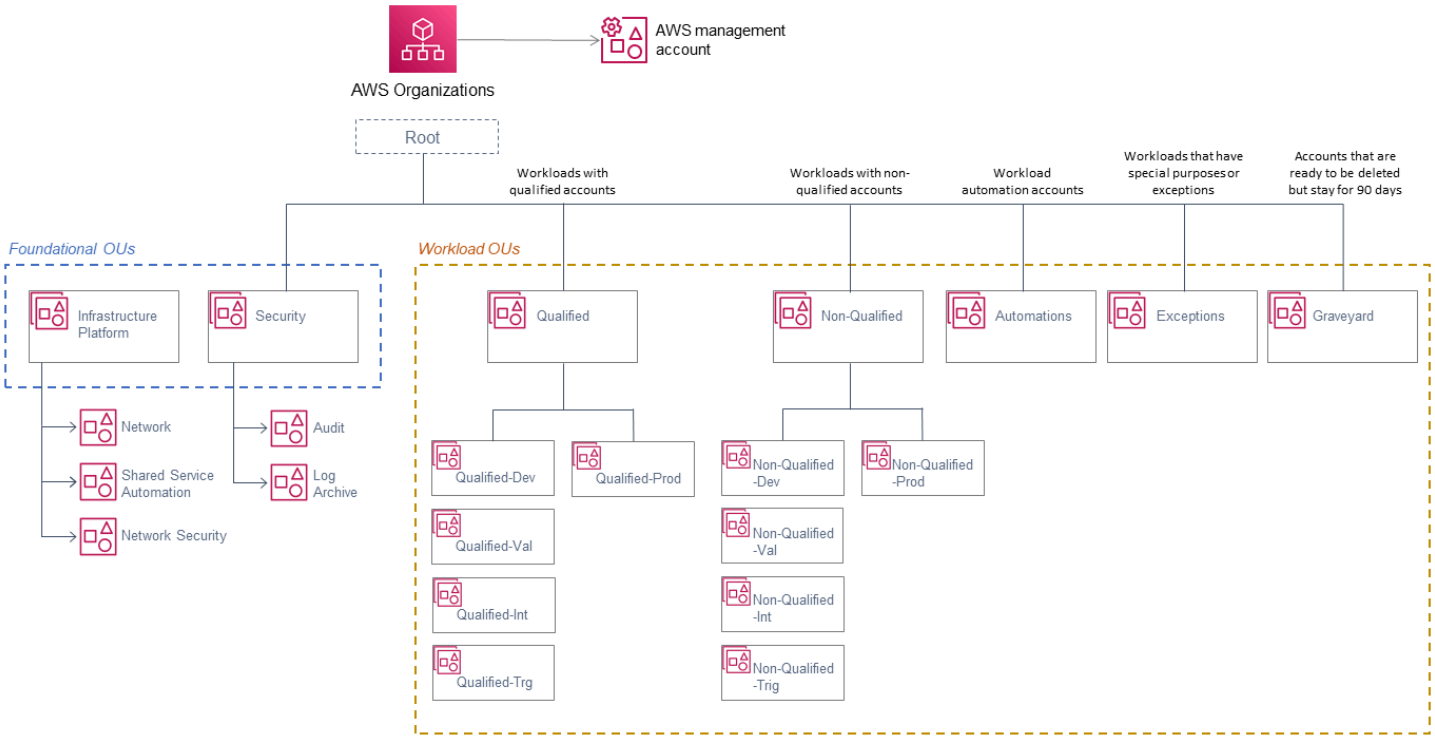
다음과 같은 새로운 요구 사항과 인사이트가 중요해졌습니다.

- 이 회사는 데이터 공유 모델 워크로드를 구현했으므로 애플리케이션은 더 이상 임상 또는 제조와 같은 별도의 OU에 할당할 수 없는 다목적 특성을 확보했습니다.
- 검증(특히 지속적인 검증)은 많은 워크로드의 중요한 측면이 되었습니다. 이러한 워크로드는 보안 모범 사례를 보다 쉽게 따를 수 있도록 운영 프로세스에 통합되어야 했습니다. 적격 워크로드에는 1단계의 OU 수준에서 설정된 보다 엄격한 AWS 제어가 필요했습니다.
- 중첩된 OU 기능을에서 사용할 수 있게 되었습니다 AWS Control Tower.
- 기술 향상과 경험을 통해 워크로드와 관련된 특정 정책을 더 잘 이해할 수 있었습니다.
- 회사가 책임 조정을 기반으로 운영 모델을 정의하고 이에 합의했습니다.
- 워크로드 세분화 및 구성 블루프린트는 성숙되어 워크로드 마이그레이션에 채택되었습니다.

그 결과 2단계에서 새로운 설계가 구현되고 AWS 계정 이 새로운 구조로 마이그레이션되었습니다. 이 새로운 구조에는 다음 섹션에 설명된 OU가 포함되어 있습니다.

## 아키텍처 설계

다음 다이어그램에서는 2단계의 OU 아키텍처를 보여줍니다.




# 보안 OU

보안 OU에는 보안 기능과 광범위하게 AWS 계정 관련된가 포함되어 있으며 두 계정(감사 및 로그 아카이브)을 사용하여 Amazon GuardDuty와 같은 Environment. AWS core 보안 서비스에 대한 중앙 로깅 및 감사 액세스를 위한 보안 운영 데이터를 저장하고 감사 계정에 AWS Security Hub CSPM 상주합니다. 이 OU는 원래 설계에서 변경되지 않은 상태입니다.

# 인프라 플랫폼 OU

인프라 플랫폼 OU에는 네트워킹 및 AWS 랜딩 존 전반의 공유 자동화와 같은 기본 인프라 계정이 포함되어 있습니다. 이 OU는 원래 설계에서 변경되지 않은 상태입니다.

# 적격한 OU

적격한 OU에는 엄격한 변경 관리, 자격 확인 및 검증과 같은 적격한 인프라가 필요한 워크로드가 포함되어 있습니다.

# 비적격 OU

비적격 OU에는 GxP 요구 사항이 없거나 비즈니스에 중요하지 않은 워크로드가 포함되어 있습니다.

# 자동화 OU

자동화 OU에는 인프라 관리를 위한 지속적 통합 및 지속적 전송(CI/CD) 파이프라인과 같은 워크로드 자동화를 위한 공유 리소스가 포함되어 있습니다. 요구 사항에 따라 자동화를 여러 환경에서 분할하거나 단일 AWS 계정에서 호스팅할 수 있습니다.

# 예외 OU

예외 OU에는 특별한 처리가 필요한 워크로드(그렇지 않은 경우 정책에 의해 금지됨)가 포함되어 있습니다. 예를 들어 널리 액세스 가능하고 읽기 가능한 Amazon Simple Storage Service(Amazon S3) 버킷은 예외 OU에 속합니다.

# Graveyard OU

Graveyard OU에는 삭제할 워크로드 AWS 계정 에 대한가 포함되어 있습니다. 계정이 만료되거나 삭제될 때까지 효과적이고 간단한 관리 액세스를 위해 이러한 계정의 정책은 제거해야 합니다.

# OU 마이그레이션 및 확인

이 예제에서 다국적 제약 회사의 경우 클라우드 플랫폼 엔지니어링 및 변경 관리 팀은 마이그레이션 계획 및 일정에 동의했습니다. AWS 계정은 계획의 일환으로 비즈니스 영향 및 중요도에 따라 검토되고 순위가 매겨졌습니다.

새 정책의 스테이징과 증분 마이그레이션을 허용하도록 새 OU 구조가 기존 OU 구조와 함께 배포되었습니다. 그리고 하위 OU와 함께 새로운 빈 OU를 생성하고 해당 하위 OU에 AWS Organizations 정책 및 AWS Control Tower 제어를 할당했습니다.

새 구조에서 원하는 정책을 적용하여 AWS Organizations 정책을 수동으로 마이그레이션했습니다. AWS Control Tower 제어를 확인하기 위한 메커니즘을 자동화하고 AWS Organizations 정책을 확인하기 위해 수동 스팟 검사를 사용했습니다. AWS 계정은 이러한 검사가 성공한 후에만 새 OU로 이동되었습니다.

계정 마이그레이션은 반자동화되었으며 시간차 접근 방식 또는 배치 접근 방식을 따랐습니다. 초기 마이그레이션에서는 다소 덜 중요한 것으로 간주된 AWS 계정을 목표로 삼았으며, 이때 마이그레이션 실행당 5개의 AWS 계정 배치를 사용했습니다. 마이그레이션 배치에서는 10개의 계정을 초과하지 않았습니다. 계정이 마이그레이션될 때 검토자와 테스터는 AWS Control Tower 콘솔을 사용하여 이러한 계정이 올바른 OU로 이동되었는지 확인하고 AWS CloudTrail 로그에 오류가 있는지 모니터링했습니다. 또한 검토자는 AWS Service Catalog 및 AWS Control Tower 콘솔에서 테인트되거나 알 수 없는 상태의 계정 또는 드리프트가 있는지 확인했습니다.

계정의 OU 배치에 대한 변경 사항은 리소스의 연결 또는 접근성에 영향을 미치지 않았습니다. 프로덕션 애플리케이션에서 중단은 보고되지 않았습니다.

# 학습한 교훈 및 모범 사례

- OU 구조 설계는 일회성 작업이 아닙니다. 회사가 클라우드 채택을 늘리고 추가 워크로드를 AWS 랜딩 존으로 마이그레이션함에 따라 OU 설계(및 묵시적으로 정책 개념)도 자연스럽게 발전합니다.
- OU를 폴더로 오해하지 말고, 정책의 대상으로 간주합니다. OU 및 해당 계층 구조는 AWS 계정에 대한 구성 요소를 제공하며 항상 정책의 컨테이너로 처리해야 합니다. 동일한 정책 세트가 필요한 모든 AWS 계정을 동일한 OU에 배치하는 것이 좋습니다. 이 지침은 중첩된 OU(OU 내 OU)로도 확장됩니다.

  중앙에서 공유 기능과 워크로드 간 데이터 공유 기능(엔터프라이즈 데이터 플랫폼에서 자주 볼 수 있음)이 필요한 AWS 환경은 사업부(LOB) 기능 분류를 기반으로 하지 않는 OU 구조에서 더 쉽게 수용할 수 있습니다. 예를 들어 제조 애플리케이션의 프로덕션 환경은 AWS Organizations의 정책 측면에서 임상 시험 분석 애플리케이션의 프로덕션 환경과 다르지 않습니다.
- 상속을 존중하고 사용합니다. 정책을 특정 OU에 연결하면 해당 OU 바로 아래 또는 하위 OU 아래에 있는 AWS 계정이 정책을 상속합니다. 정책을 특정 AWS 계정에 연결하면 정책은 해당 AWS 계정에만 영향을 미칩니다.

  한 OU 구조에서 다른 OU 구조로 마이그레이션하는 작업은 기존 정책이 OU 또는 AWS 계정 수준에서 얼마나 광범위하게 구성되었는지에 따라 달라집니다. 또 다른 중요한 요소는 기존 OU 계층 구조에서 사용된 정책 상속의 양 또는 상속이 중단된 경우입니다. 불규칙하거나 다른 상속 경로가 구현되면 마이그레이션의 복잡성이 증가합니다. 예를 들어 개별 AWS 계정 수준에서 정책을 적용하거나 정책 예외가 자주 발생하는 경우(상속이 중단됨) 해당 정책을 새 구조로 마이그레이션하려면 훨씬 더 많은 노력이 필요합니다. 이와 같이 복잡성이 높은 경우 마이그레이션 계획 중에 시간을 투자하여 정책 상속을 검토하고 재설계하는 것이 좋습니다.
- AWS Organizations 정책과 AWS Control Tower 제어를 모두 관리합니다. OU 구조는 AWS Control Tower 및 AWS Organizations 사이에서 공유됩니다. AWS Control Tower에서는 자체 감지 및 예방적 제어 세트를 제공합니다. 이러한 제어는 AWS 계정 또는 OU 수준에서 적용됩니다. AWS Organizations는 OU 수준에서 정책을 오케스트레이션합니다. OU 마이그레이션에서는 AWS Organizations 정책을 먼저 마이그레이션하는 것이 좋습니다. 규정 준수에 더 많은 가중치를 부여하기 때문입니다. 두 번째 마이그레이션 단계에서 새 OU 구조에 AWS Control Tower 제어를 적용하는 것이 좋습니다.
- AWS 계정을 업데이트하는 데 시간이 걸립니다. AWS Control Tower를 사용하여 기존 AWS 계정을 새 OU 구조에 개별적으로 다시 등록해야 합니다. 이 작업에는 시간이 걸립니다. 계정이 많은 경우 자동화를 통해 이 작업을 간소화하여 AWS 계정의 OU 배치를 제어하고 자동화하는 것이 좋습니다. 다음은 두 가지 시나리오 예제입니다.

- 소규모 마이그레이션을 위한 수동 변경: 마이그레이션 리드는 이전 OU에서 AWS Management Console의 새 OU로 각 AWS 계정을 재할당합니다. 모든 AWS 계정에 대해 재할당이 완료되면 마이그레이션 리드가 각 AWS 계정에 대해 개별적으로 또는 모든 OU에 대해 AWS Control Tower를 엽니다. AWS Control Tower에서 AWS 계정을 재등록하려면 계정 내에서 사용된 AWS 리전 수에 따라 각 AWS 계정에서 10~15분이 소요됩니다. AWS Control Tower에서는 이러한 종류의 동시 작업을 최대 5개까지 병렬로 실행할 수 있습니다.
- 사용자 지정 변경 자동화: 자동화는 작업을 단순화하고 관련 노력을 줄여줍니다. 예를 들어 수명 주기 생성부터 마이그레이션 및 종료까지 AWS 계정 수명 주기 관리를 자동화할 수 있습니다. AWS Control Tower Account Factory를 사용하여 AWS 계정에 대한 OU 할당을 변경하고 재등록 프로세스를 실행할 수 있습니다. 이 자동화는 수백 개의 AWS 계정을 포함하는 대규모 마이그레이션을 지원합니다.

# 리소스

- AWS Organizations 사용 설명서(AWS 설명서)
- AWS Organizations terminology and concepts(AWS 설명서)
- Service control policies (SCPs)(AWS 설명서)
- AWS Organizations API 참조(AWS 설명서)
- AWS Control Tower 사용 설명서(AWS 설명서)
- Introducing Landing Zone Accelerator for Healthcare(AWS 블로그 게시물)
- Managing the multi-account environment using AWS Organizations and AWS Control Tower(AWS 블로그 게시물)
- Best Practices for Organizational Units with AWS Organizations(AWS 블로그 게시물)
- AWS 보안 참조 아키텍처(AWS SRA)(AWS 권장 가이드)
- Establishing Your Cloud Foundation on AWS(AWS 백서)
- Organizing Your AWS Environment Using Multiple Accounts(AWS 백서)

# 문서 기록

아래 표에 이 가이드의 주요 변경 사항이 설명되어 있습니다. 향후 업데이트에 대한 알림을 받으려면 RSS 피드를 구독하십시오.

| 변경 사항 | 설명 | 날짜 |
| --- | --- | --- |
| 최초 게시 | — | 2023년 3월 28일 |

기계 번역으로 제공되는 번역입니다. 제공된 번역과 원본 영어의 내용이 상충하는 경우에는 영어 버전이 우선합니다.