사용자 가이드

AWS Control Tower

AWS Control Tower: 사용자 가이드

Table of Contents

AWS 컨트롤 타워란 무엇입니까?

AWS Control Tower는 규범적 모범 사례에 따라 AWS 다중 계정 환경을 설정하고 관리하는 간단한 방법을 제공합니다. AWS Control Tower는 AWS Organizations AWS Service Catalog AWS IAM Identity Center, 및 를 비롯한 여러 다른 AWS 서비스의 기능을 조정하여 1시간 이내에 랜딩 존을 구축합니다. 사용자를 대신하여 리소스가 설정되고 관리됩니다.

AWS Control Tower 오케스트레이션은 의 기능을 확장합니다. AWS OrganizationsAWS Control Tower는 모범 사례와 다른 방식으로 조직과 계정이 드리프트되는 것을 방지하기 위해 제어 (가드레일이라고도 함) 를 적용합니다. 예를 들어, 컨트롤을 사용하여 보안 로그와 필요한 계정 간 액세스 권한이 생성되고 변경되지 않도록 할 수 있습니다.

소수의 계정을 호스팅하는 경우 계정 배포 및 계정 거버넌스를 용이하게 하는 오케스트레이션 계층을 마련하는 것이 좋습니다. AWS Control Tower를 계정 및 인프라를 프로비저닝하는 기본 방법으로 채택할 수 있습니다. AWS Control Tower를 사용하면 기업 표준을 더 쉽게 준수하고, 규제 요구 사항을 충족하고, 모범 사례를 따를 수 있습니다.

AWS Control Tower를 사용하면 분산된 팀의 최종 사용자가 Account Factory에서 구성 가능한 계정 템플릿을 사용하여 새 AWS 계정을 신속하게 프로비저닝할 수 있습니다. 한편, 중앙 클라우드 관리자는 모든 계정이 확립된 전사적 규정 준수 정책을 준수하는지 모니터링할 수 있습니다.

간단히 말해, AWS Control Tower는 수천 개의 기업과 협력하여 구축한 모범 사례를 기반으로 안전하고 규정을 준수하는 다중 계정 AWS 환경을 설정하고 관리하는 가장 쉬운 방법을 제공합니다. AWS Control Tower와의 작업 및 AWS 다중 계정 전략에 설명된 모범 사례에 대한 자세한 내용은 을 참조하십시오. AWS 다중 계정 전략: 모범 사례 지침

특성

AWS Control Tower에는 다음과 같은 기능이 있습니다.

- 랜딩 존 — 랜딩 존은 보안 및 규정 준수 모범 사례를 기반으로 잘 설계된 다중 계정 환경입니다. 규정 준수 대상이 되는 조직 단위 (OU), 계정, 사용자 및 기타 리소스를 모두 보관하는 전사적 컨테이너입니다. 랜딩 영역은 모든 규모의 기업 요구 사항에 맞게 확장할 수 있습니다.
- 제어 — 제어 (가드레일이라고도 함) 는 전체 환경에 대한 지속적인 거버넌스를 제공하는 높은 수준의 규칙입니다. AWS 일반적인 언어로 표현됩니다. 제어 유형에는 예방, 탐지 및 사전 예방의 세 가지 종류가 있습니다. 규제 항목에는 필수, 적극 권장형, 선택형 등 세 가지 범주의 지침이 적용됩니다. 제어에 대한 자세한 내용은 제어 작동 방식을 참조하십시오.

- Account Factory — Account Factory는 사전 승인된 계정 구성으로 새 계정 프로비저닝을 표준화하는 데 도움이 되는 구성 가능한 계정 템플릿입니다. AWS Control Tower는 조직의 계정 프로비저닝 워크플로를 자동화하는 데 도움이 되는 기본 제공 Account Factory를 제공합니다. 자세한 설명은 Account Factory를 통한 계정 제공 및 관리 섹션을 참조하세요.
- 대시보드 — 대시보드를 통해 중앙 클라우드 관리자로 구성된 팀이 랜딩 존을 지속적으로 감독할 수 있습니다. 대시보드를 사용하여 기업 전체의 프로비저닝된 계정, 정책 시행에 사용할 수 있는 제어, 정책 비준수를 지속적으로 탐지할 수 있는 제어, 계정 및 OU별로 정리된 비준수 리소스를 확인할 수 있습니다.

AWS Control Tower가 다른 AWS 서비스와 상호 작용하는 방식

AWS Control Tower는 AWS Service Catalog AWS IAM Identity Center, 및 를 비롯한 신뢰할 수 있고 신뢰할 수 있는 AWS 서비스를 기반으로 구축되었습니다 AWS Organizations. 자세한 설명은 통합 서비스 섹션을 참조하세요.

AWS Control Tower를 다른 AWS 서비스와 통합하여 기존 워크로드를 마이그레이션하는 데 도움이 되는 솔루션에 통합할 AWS수 있습니다. 자세한 내용은 AWS Control Tower를 활용하고 워크로드를 AWS Control Tower로 CloudEndure 마이그레이션하는 방법을 참조하십시오. AWS

구성, 거버넌스 및 확장성

- 자동 계정 구성: AWS Control Tower는 프로비저닝된 제품 위에 추상화 형태로 구축된 Account Factory (또는 “자판기”) 를 통해 계정 배포 및 등록을 자동화합니다. AWS Service CatalogAccount Factory는 AWS 계정을 생성하고 등록할 수 있으며, 해당 계정에 제어 및 정책을 적용하는 프로세스를 자동화합니다.
- 중앙 집중식 거버넌스: AWS Control Tower는 의 AWS Organizations기능을 사용하여 다중 계정 환경 전반에서 일관된 규정 준수 및 거버넌스를 보장하는 프레임워크를 설정합니다. 이 AWS Organizations 서비스는 계정의 중앙 거버넌스 및 관리, AWS Organizations API를 통한 계정 생성, 서비스 제어 정책 (SCP) 등 다중 계정 환경을 관리하는 데 필요한 필수 기능을 제공합니다.

- 확장성: AWS Control Tower 콘솔뿐만 아니라 AWS Control Tower 콘솔에서도 AWS Organizations 직접 작업하여 자체 AWS Control Tower 환경을 구축하거나 확장할 수 있습니다. 기존 조직을 등록하고 기존 계정을 AWS Control Tower에 등록한 후에 변경 사항이 AWS Control Tower에 반영된 것을 확인할 수 있습니다. 변경 내용을 반영하도록 AWS Control Tower 랜딩 존을 업데이트할 수 있습니다. 워크로드에 추가 고급 기능이 필요한 경우 AWS Control Tower와 함께 다른 AWS 파트너 솔루션을 활용할 수 있습니다.

AWS Control Tower를 처음 사용하십니까?

이 서비스를 처음 사용하는 경우 다음을 읽어 보는 것이 좋습니다.

1. 착륙 지대를 계획하고 구성하는 방법에 대한 자세한 내용은 AWS Control Tower 랜딩 존을 계획하십시오. 및 을 참조하십시오AWS AWS Control Tower 랜딩 존을 위한 다중 계정 전략.
2. 첫 번째 랜딩 영역을 만들 준비가 되면 AWS Control Tower 시작하기 단원을 참조하십시오.
3. 드리프트 감지 및 방지에 대한 자세한 내용은 AWS Control Tower의 드리프트 감지 및 해결 단원을 참조하십시오.
4. 보안 세부 사항은 AWS Control Tower의 보안 단원을 참조하십시오.
5. landing zone 및 회원 계정 업데이트에 대한 자세한 내용은 을 참조하십시오AWS Control Tower에서의 구성 업데이트 관리.

AWS 컨트롤 타워 작동 방식

이 섹션에서는 AWS Control Tower의 작동 방식을 개괄적으로 설명합니다. Landing Zone은 모든 리소스를 위한 잘 설계된 다중 계정 환경입니다. AWS 이 환경을 사용하여 모든 계정에 규정 준수 규정을 적용할 수 있습니다. AWS

AWS 컨트롤 타워 랜딩 존의 구조

AWS Control Tower의 랜딩 존 구조는 다음과 같습니다.

- 루트 — 랜딩 존에 있는 다른 모든 OU를 포함하는 부모.
- 보안 OU - 이 OU에는 로그 아카이브 및 감사 계정이 들어 있습니다. 이러한 계정을 공유 계정이라고도 합니다. 랜딩 존을 시작할 때 이러한 공유 계정의 사용자 지정 이름을 선택할 수 있으며 보안 및 로깅을 위해 기존 AWS 계정을 AWS Control Tower로 가져올 수도 있습니다. 그러나 이러한 계정은 나중에 이름을 바꿀 수 없으며 처음 시작한 후에는 보안 및 로깅을 위해 기존 계정을 추가할 수 없습니다.
- 샌드박스 OU — 샌드박스 OU는 랜딩 존을 활성화한 경우 랜딩 존을 시작할 때 생성됩니다. 이 OU 및 기타 등록된 OU에는 사용자가 AWS 워크로드를 수행하는 데 사용하는 등록된 계정이 포함되어 있습니다.
- IAM ID 센터 디렉터리 — 이 디렉터리에는 IAM ID 센터 사용자가 있습니다. 각 IAM ID 센터 사용자의 권한 범위를 정의합니다.
- IAM Identity Center 사용자 — 사용자가 랜딩 존에서 AWS 워크로드를 수행하는 것으로 간주할 수 있는 ID입니다.

착륙 지대를 설정하면 어떻게 되나요?

랜딩 존을 설정하면 AWS Control Tower가 사용자를 대신하여 관리 계정에서 다음 작업을 수행합니다.

- 조직의 루트 구조 내에 포함된 보안과 샌드박스 (선택 사항) 라는 두 개의 AWS Organizations 조직 단위 (OU) 를 생성합니다.
- 보안 OU에 두 개의 공유 계정, 즉 로그 아카이브 계정과 감사 계정을 만들거나 추가합니다.
- 기본 AWS Control Tower 구성을 선택한 경우 사전 구성된 그룹 및 싱글 사인온 액세스를 포함하는 클라우드 네이티브 디렉터리를 IAM Identity Center에 생성하거나, 이를 통해 자격 증명 공급자를 자체 관리할 수 있습니다.
- 정책을 시행하기 위해 모든 필수 예방 제어를 적용합니다.
- 모든 필수 탐지 제어를 적용하여 구성 위반을 탐지합니다.
- 관리 계정에는 예방 제어가 적용되지 않습니다.
- 관리 계정을 제외한 컨트롤은 조직 전체에 적용됩니다.

AWS Control Tower 랜딩 존 및 계정 내의 리소스를 안전하게 관리

- landing Zone을 만들면 많은 AWS 리소스가 생성됩니다. AWS Control Tower를 사용하려면 이 안내서에 설명된 지원되는 방법 이외의 방법으로 이러한 AWS Control Tower 관리 리소스를 수정하거나 삭제해서는 안 됩니다. 이러한 리소스를 삭제하거나 수정하면 landding Zone이 알 수 없는 상태가 됩니다. 자세한 내용은 AWS Control Tower 리소스 생성 및 수정 지침을 참조하세요.
- 선택적 컨트롤 (강력히 권장되거나 선택적인 지침이 있는 컨트롤) 을 활성화하면 AWS Control Tower가 AWS 리소스를 생성하여 계정에서 관리합니다. AWS Control Tower에서 생성한 리소스를 수정하거나 삭제하지 마십시오. 이렇게 하면 제어가 알 수 없는 상태가 될 수 있습니다.

공유 계정이란 무엇인가요?

AWS Control Tower에서는 설치 과정에서 랜딩 존의 공유 계정, 즉 관리 계정, 로그 아카이브 계정, 감사 계정이 프로비저닝됩니다.

관리 계정이란 무엇입니까?

이 계정은 landding Zone을 위해 특별히 만든 계정입니다. 이 계정은 landding Zone의 모든 항목에 대한 청구에 사용됩니다. 또한 Account Factory에서 계정을 프로비저닝하고 OU 및 제어 기능을 관리하는 데에도 사용됩니다.

> **Note**
>
> AWS Control Tower 관리 계정에서 어떤 유형의 프로덕션 워크로드도 실행하지 않는 것이 좋습니다. 워크로드를 실행하려면 별도의 AWS Control Tower 계정을 생성하십시오.

자세한 정보는 관리 계정을 참조하세요.

로그 아카이브 계정이란 무엇입니까?

이 계정은 landing Zone에 있는 모든 계정의 API 활동 및 리소스 구성 로그를 저장하는 저장소 역할을 합니다.

자세한 정보는 로그 아카이브 계정을 참조하세요.

감사 계정이란 무엇입니까?

감사 계정은 보안 및 규정 준수 팀에 랜딩 존의 모든 계정에 대한 읽기 및 쓰기 액세스 권한을 제공하도록 설계된 제한된 계정입니다. 감사 계정에서, Lambda 함수에만 부여된 역할을 통해 프로그래밍 방식으로 액세스하여 계정을 검토할 수 있습니다. 감사 계정을 이용해 다른 계정에 수동으로 로그인할 수 없습니다. Lambda 함수 및 역할에 대한 자세한 내용은 다른 함수의 역할을 맡도록 Lambda 함수 구성을 참조하십시오. AWS 계정

자세한 정보는 감사 계정을 참조하세요.

제어 작동 방식

제어는 전체 AWS 환경에 대한 지속적인 거버넌스를 제공하는 높은 수준의 규칙입니다. 각 컨트롤은 단일 규칙을 적용하며 일반 언어로 표현됩니다. AWS Control Tower 콘솔 또는 AWS Control Tower API에서 시행 중인 선택적 규제 항목 또는 강력히 권장되는 규제 항목을 언제든지 변경할 수 있습니다. 필수 컨트롤은 항상 적용되며 변경할 수 없습니다.

예방적 통제는 조치가 취해지는 것을 방지합니다. 예를 들어 Amazon S3 버킷의 버킷 정책 변경 금지(이전에는 로그 아카이브에 대한 정책 변경 금지라고 함) 라는 선택적 제어는 로그 아카이브 공유 계정 내의 IAM 정책 변경을 방지합니다. 차단된 작업을 수행하려는 모든 시도는 거부되고 로그인됩니다. CloudTrail 리소스도 로그인됩니다 AWS Config.

Detective Controls는 특정 이벤트가 발생할 때 이를 감지하고 작업을 기록합니다. CloudTrail 예를 들어 Amazon EC2 인스턴스에 연결된 Amazon EBS 볼륨의 암호화 활성화 여부 감지라는 강력히 권장되

는 제어 기능은 암호화되지 않은 Amazon EBS 볼륨이 착륙 영역의 EC2 인스턴스에 연결되어 있는지 여부를 탐지합니다.

사전 예방적 제어를 통해 리소스가 계정에 프로비저닝되기 전에 리소스가 회사 정책 및 목표를 준수하는지 여부를 확인합니다. 리소스가 규정을 준수하지 않는 경우 리소스는 프로비저닝되지 않습니다. 사전 예방적 제어는 템플릿을 통해 계정에 배포될 리소스를 모니터링합니다. AWS CloudFormation

다음 사항에 익숙한 사용자를 위해 AWS: AWS Control Tower에서는 서비스 제어 정책 (SCP) 을 통해 예방 제어를 구현합니다. Detective 컨트롤은 규칙을 사용하여 AWS Config 구현됩니다. 사전 예방적 제어는 후크를 통해 AWS CloudFormation 구현됩니다.

관련 항목

- AWS Control Tower의 드리프트 감지 및 해결

AWS Control Tower는 다음과 함께 작동하는 방식 StackSets

AWS Control Tower는 사용자 계정에 리소스를 설정하는 AWS CloudFormation StackSets 데 사용합니다. 각 스택 세트에는 StackInstances 계정별, AWS 리전 계정별 스택 세트가 있습니다. AWS Control Tower는 계정 및 지역당 하나의 스택 세트 인스턴스를 배포합니다.

AWS Control Tower는 AWS CloudFormation 파라미터를 기반으로 특정 계정에 업데이트를 AWS 리전 선택적으로 적용합니다. 일부 스택 인스턴스에 업데이트가 적용되면 다른 스택 인스턴스는 Outdated(오래됨) 상태로 남아있을 수 있습니다. 이는 예상된 정상 동작입니다.

스택 인스턴스가 Outdated(오래됨) 상태가 되면 일반적으로 그 스택 인스턴스에 해당하는 스택이 스택 세트의 최신 템플릿과 정렬되지 않음을 의미합니다. 스택은 이전 템플릿에 남아 있으므로 최신 리소스 또는 파라미터가 포함되지 않을 수 있습니다. 스택은 여전히 완전히 사용할 수 있습니다.

다음은 업데이트 중에 지정된 AWS CloudFormation 파라미터를 기반으로 예상되는 동작에 대한 간략한 요약입니다.

스택 세트 업데이트에 템플릿 변경 사항이 포함된 경우 (즉, `TemplateBody` 또는 `TemplateURL` 속성이 지정된 경우) 또는 `Parameters` 속성이 지정된 경우, 지정된 계정의 스택 인스턴스를 업데이트하기 전에 모든 스택 인스턴스를 Outdated 상태로 AWS CloudFormation 표시합니다. AWS 리전스택 세트 업데이트에 템플릿 또는 매개 변수에 대한 변경 사항이 포함되지 않은 경우 다른 모든 스택 인스턴스는 기존 인스턴스 스택 상태를 유지한 채 지정된 계정 및 지역의 스택 인스턴스를 AWS CloudFormation 업데이트합니다. 스택 세트와 연결된 모든 스택 인스턴스를 업데이트하려면 `Accounts` 또는 `Regions` 속성을 지정하지 마십시오.

자세한 내용은 AWS CloudFormation 사용 설명서의 스택 세트 업데이트를 참조하십시오.

용어

다음은 AWS Control Tower 설명서에서 확인할 수 있는 몇 가지 용어에 대한 간략한 검토입니다.

먼저, AWS Control Tower는 이 문서 전반에 걸쳐 나타나는 조직 및 조직 단위 (OU) 라는 용어를 비롯하여 AWS Organizations 서비스와 많은 용어를 공유한다는 점을 알아두면 좋습니다.

- 조직 및 OU에 대한 자세한 내용은 AWS Organizations 용어 및 개념을 참조하십시오. AWS Control Tower를 처음 사용하는 경우 이 용어부터 시작하는 것이 좋습니다.
- AWS Organizations워크로드를 확장하고 확장할 때 환경을 중앙에서 관리할 수 있도록 지원하는 AWS 서비스입니다. AWS AWS Control Tower는 계정을 생성하고, OU 수준에서 예방적 제어를 적용하고, 중앙 집중식 청구를 제공하는 데 의존합니다 AWS Organizations .
- AWS 어카운트 팩토리 계정은 AWS 컨트롤 타워의 AWS Account Factory를 사용하여 프로비저닝된 계정입니다. Account Factory는 비공식적으로 계정의 “자판기”라고 불리기도 합니다.
- AWS 컨트롤 타워 홈 리전은 AWS 컨트롤 타워 랜딩 존이 배포된 AWS 지역입니다. 랜딩 존 설정에서 홈 지역을 볼 수 있습니다.
- AWS Service Catalog일반적으로 배포되는 IT 서비스를 중앙에서 관리할 수 있습니다. 이 문서의 맥락에서 Account Factory는 사용자 지정 블루프린트의 AWS 계정을 포함하여 새 계정을 AWS Service Catalog 프로비저닝하는 데 사용합니다.
- AWS CloudFormation StackSets단일 작업과 단일 템플릿으로 여러 계정 및 지역에서 스택을 생성, 업데이트 또는 삭제할 수 있도록 스택의 기능을 확장하는 리소스 유형입니다. CloudFormation
- 스택 인스턴스는 지역 내 대상 계정의 스택에 대한 참조입니다.
- 스택은 단일 단위로 관리할 수 있는 AWS 리소스 모음입니다.
- 애그리게이터는 조직 내 여러 계정 및 지역에서 AWS Config 구성 및 규정 준수 데이터를 수집하는 AWS Config 리소스 유형으로, 단일 계정 내에서 이러한 규정 준수 데이터를 보고 쿼리할 수 있습니다.
- 적합성 팩은 계정과 지역에서 단일 엔티티로 배포하거나 조직 전체에 배포할 수 있는 AWS Config 규칙 및 수정 조치의 모음입니다. AWS Organizations적합성 팩을 사용하면 AWS Control Tower 환경을 사용자 지정하는 데 도움이 될 수 있습니다. 자세한 내용을 제공하는 기술 블로그는 관련 정보를 참조하십시오.
- AWS Control Tower의 기준은 대상에 적용할 수 있는 리소스 및 특정 구성 그룹입니다. 가장 일반적인 기준 대상은 조직 단위 (OU) 일 수 있습니다. 예를 들어, AWS Control Tower에 OU를 등록하는 데 도움이 되는 기준선을 사용할 수 있습니다. `AWSControlTowerBaseline` 랜딩 존 설정 및 업데이트 중에 기본 타겟은 공유 계정이거나 랜딩 존 전체의 특정 설정일 수 있습니다.

- 블루프린트: 블루프린트는 일부 메타데이터를 캡슐화하는 아티팩트로, 계정 내에 배포되는 인프라 구성 요소를 설명합니다. 예를 들어, AWS CloudFormation 템플릿은 AWS Control Tower 계정의 청사진 역할을 할 수 있습니다.
- 드리프트: AWS Control Tower에서 설치하고 구성한 리소스의 변경. 드리프트가 없는 리소스를 사용하면 AWS Control Tower가 제대로 작동할 수 있습니다.
- 비준수 리소스: 특정 탐지 제어를 정의하는 AWS Config 규칙을 위반하는 리소스입니다.
- 공유 계정: 랜딩 존을 설정할 때 AWS Control Tower가 자동으로 생성하는 세 개의 계정 (관리 계정, 로그 아카이브 계정, 감사 계정) 중 하나입니다. 설정 중에 로그 아카이브 계정과 감사 계정의 사용자 지정 이름을 선택할 수 있습니다.
- 회원 계정: 회원 계정은 AWS Control Tower 조직에 속합니다. 회원 계정은 AWS Control Tower에 등록하거나 등록 취소할 수 있습니다. 등록된 OU에 등록된 계정과 등록되지 않은 계정이 혼합되어 있는 경우:
  - OU에서 활성화된 예방 제어는 등록되지 않은 계정을 포함하여 OU 내 모든 계정에 적용됩니다. SCP를 통해 계정 수준이 아닌 OU 수준에서 예방 제어를 적용하기 때문에 이는 사실입니다. 자세한 내용은 설명서의 서비스 제어 정책 상속을 AWS Organizations 참조하십시오.
  - OU에서 활성화된 Detective 컨트롤은 등록되지 않은 계정에는 적용되지 않습니다.

  계정은 한 번에 한 조직에만 속할 수 있으며 요금은 해당 조직의 관리 계정에 청구됩니다. 구성원 계정을 조직의 루트 컨테이너로 이동할 수 있습니다.
- AWS AWS 계정: 계정은 리소스 컨테이너 및 리소스 격리 경계 역할을 합니다. AWS 계정을 청구 및 결제와 연결할 수 있습니다. AWS 계정은 AWS Control Tower의 사용자 계정 (IAM 사용자 계정이라고도 함) 과 다릅니다. Account Factory 프로비저닝 프로세스를 통해 생성된 AWS 계정은 계정입니다. AWS 계정 등록 또는 OU 등록 프로세스를 통해 계정을 AWS Control Tower에 추가할 수도 있습니다.
- 제어: 컨트롤 (가드레일이라고도 함) 은 전체 AWS Control Tower 환경에 대한 지속적인 거버넌스를 제공하는 높은 수준의 규칙입니다. 각 컨트롤은 단일 규칙을 적용합니다. 예방 제어는 SCP를 통해 구현됩니다. Detective 컨트롤은 규칙을 사용하여 AWS Config 구현됩니다. 사전 예방적 제어는 후크를 통해 AWS CloudFormation 구현됩니다. 자세한 정보는 제어 작동 방식을 참조하세요.
- 랜딩 존: 랜딩 존은 기본 계정, 계정 구조, 네트워크 및 보안 레이아웃 등을 포함하여 권장되는 시작점을 제공하는 클라우드 환경입니다. Landing Zone에서 솔루션과 애플리케이션을 활용하는 워크로드를 배포할 수 있습니다.
- 중첩된 OU: AWS Control Tower의 중첩된 OU는 다른 OU에 포함된 OU입니다. 중첩된 OU에는 정확히 하나의 상위 OU가 있을 수 있으며 각 계정은 정확히 하나의 OU의 구성원이 될 수 있습니다. 중첩된 OU는 계층 구조를 만듭니다. 계층 구조의 OU 중 하나에 정책을 연결하면 해당 정책이 아래로 흘

러 내려가 해당 OU 아래에 있는 모든 OU와 계정에 영향을 미칩니다. AWS Control Tower의 중첩된 OU 계층 구조는 최대 5개 수준일 수 있습니다.

- 상위 OU: 계층 구조에서 현재 OU 바로 위에 있는 OU입니다. 각 OU에는 정확히 하나의 부모 OU가 있을 수 있습니다.
- 하위 OU: 계층 구조에서 현재 OU 아래에 있는 모든 OU. OU에는 하위 OU가 여러 개 있을 수 있습니다.
- OU 계층: AWS Control Tower에서는 중첩된 OU의 계층 구조가 최대 5단계로 구성될 수 있습니다. 중첩 순서를 레벨이라고 합니다. 계층의 최상위는 레벨 1로 지정됩니다.
- 최상위 OU: 최상위 OU는 루트 자체가 아니라 루트 바로 아래에 있는 모든 OU입니다. 루트는 OU로 간주되지 않습니다.

요금

AWS Control Tower 사용에 따른 추가 요금은 없습니다. AWS Control Tower에서 지원하는 AWS 서비스와 착륙 지역에서 사용한 서비스에 대한 비용만 지불하면 됩니다. 예를 들어 Account Factory를 통해 계정을 프로비저닝하고 랜딩 존에서 추적한 이벤트에 AWS CloudTrail 대해 Service Catalog 비용을 지불합니다. AWS Control Tower와 관련된 요금 및 요금에 대한 자세한 내용은 AWS Control Tower 요금을 참조하십시오.

AWS Control Tower의 계정에서 임시 워크로드를 실행하는 경우 이와 관련된 비용이 증가할 수 있습니다. AWS Config자세한 내용은 AWS Config 요금을 참조하십시오. 이러한 비용 관리에 대한 자세한 내용은 AWS 계정 담당자에게 문의하십시오. AWS Control Tower와의 AWS Config 작동 방식에 대한 자세한 내용은 을 참조하십시오다음을 사용하여 리소스 변경을 모니터링합니다. AWS Config.

AWS Control Tower 외부에서 AWS CloudTrail 트레일을 구현하는 경우 AWS Control Tower에서 해당 트레일을 사용할 수 있습니다. 하지만 AWS Control Tower에서 관리하는 트레일을 옵트인하는 경우 요금이 중복될 수 있습니다. 특정 요구 사항이 없는 한 외부 트레일을 설정하지 않는 것이 좋습니다. 랜딩 존 설정 또는 업데이트 중에 옵트인하기로 선택한 경우, AWS Control Tower는 관리 계정에서 조직 수준의 CloudTrail 트레일을 설정하고 활성화합니다. CloudTrail 비용 관리에 대한 자세한 내용은 비용 관리를 참조하십시오. CloudTrail

설정

AWS Control Tower 처음 사용하기 전에 이 섹션의 단계에 따라 계정을 만들고 AWS Control Tower 관리 AWS 계정을 보호하세요. 전용 추가 설정 작업에 대한 자세한 내용은 AWS Control Tower을 참조하십시오AWS Control Tower 시작하기.

등록하기: AWS

Amazon Web Services (AWS) 에 가입하면 다음을 AWS포함한 모든 서비스에 AWS 계정이 자동으로 등록됩니다 AWS Control Tower. 이미 AWS 계정이 있다면 다음 작업으로 건너뛰십시오. 계정이 없는 경우 다음 절차를 사용하여 AWS 계정을 만드십시오.

다른 작업에 필요하므로 AWS 계정 번호를 기록해 두십시오.

가입하여 AWS 계정

계정이 없는 경우 다음 단계를 완료하여 계정을 만드세요. AWS 계정

가입하려면 AWS 계정

1. https://portal.aws.amazon.com/billing/signup을 여세요.
2. 온라인 지시 사항을 따르세요.

   등록 절차 중에는 전화를 받고 키패드로 인증 코드를 입력하는 과정이 있습니다.

   에 AWS 계정가입하면 AWS 계정 루트 사용자a가 생성됩니다. 루트 사용자에게는 계정의 모든 AWS 서비스 및 리소스 액세스 권한이 있습니다. 보안 모범 사례는 사용자에게 관리 액세스 권한을 할당하고, 루트 사용자만 사용하여 루트 사용자 액세스 권한이 필요한 작업을 수행하는 것입니다.

AWS 가입 절차가 완료된 후 확인 이메일을 보냅니다. 언제든지 https://aws.amazon.com/으로 가서 내 계정(My Account)을 선택하여 현재 계정 활동을 보고 계정을 관리할 수 있습니다.

관리자 액세스 권한이 있는 사용자 생성

등록한 AWS 계정후에는 일상적인 작업에 루트 사용자를 사용하지 않도록 관리 사용자를 보호하고 AWS IAM Identity Center활성화하고 생성하십시오 AWS 계정 루트 사용자.

보안을 유지하세요. AWS 계정 루트 사용자

1. 루트 사용자를 선택하고 AWS 계정 이메일 주소를 입력하여 계정 AWS Management Console소유자로 로그인합니다. 다음 페이지에서 비밀번호를 입력합니다.

   루트 사용자를 사용하여 로그인하는 데 도움이 필요하면AWS 로그인 사용 설명서의 루트 사용자로 로그인을 참조하세요.
2. 루트 사용자의 다중 인증(MFA)을 활성화합니다.

   지침은 IAM 사용 설명서의 AWS 계정 루트 사용자 (콘솔) 에 대한 가상 MFA 디바이스 활성화를 참조하십시오.

관리자 액세스 권한이 있는 사용자 생성

1. IAM Identity Center를 활성화합니다.

   지침은 AWS IAM Identity Center 사용 설명서의 AWS IAM Identity Center설정을 참조하세요.
2. IAM Identity Center에서 사용자에게 관리 액세스 권한을 부여합니다.

   를 ID 소스로 사용하는 방법에 대한 자습서는 사용 설명서의 기본값으로 IAM Identity Center 디렉터리사용자 액세스 구성을 참조하십시오. IAM Identity Center 디렉터리 AWS IAM Identity Center

관리 액세스 권한이 있는 사용자로 로그인

- IAM IDentity Center 사용자로 로그인하려면 IAM IDentity Center 사용자를 생성할 때 이메일 주소로 전송된 로그인 URL을 사용합니다.

  IAM Identity Center 사용자를 사용하여 로그인하는 데 도움이 필요하면 사용 설명서의 AWS 액세스 포털에 로그인을 참조하십시오.AWS 로그인

추가 사용자에게 액세스 권한 할당

1. IAM Identity Center에서 최소 권한 적용 모범 사례를 따르는 권한 세트를 생성합니다.

   지침은AWS IAM Identity Center 사용 설명서의 Create a permission set를 참조하세요.
2. 사용자를 그룹에 할당하고, 그룹에 Single Sign-On 액세스 권한을 할당합니다.

   지침은AWS IAM Identity Center 사용 설명서의 Add groups를 참조하세요.

계정 보안

AWS Control Tower 계정 보안을 보호하는 베스트 프랙티스를 설정하는 방법에 대한 추가 지침은 AWS Organizations 설명서에서 확인할 수 있습니다.

- 관리 계정 모범 사례
- 회원 계정 모범 사례

다음 단계

AWS Control Tower 시작하기

AWS Control Tower 시작하기

이 시작 절차는 AWS Control Tower 관리자를 대상으로 합니다. AWS Control Tower 콘솔 또는 API를 사용하여 랜딩 존을 설정할 준비가 되면 이 절차를 따르십시오.

현재 AWS Control Tower를 처음 사용하는 AWS 고객이라면 진행하기 전에 라는 섹션을 검토해 AWS Control Tower 랜딩 존을 계획하십시오. 보는 것이 좋습니다.

주제

- AWS Control 타워 퀵 스타트 가이드
- 전제 조건: 관리 계정에 대한 자동화된 사전 출시 확인
- 콘솔에서 AWS Control Tower를 시작하기
- API를 사용하여 AWS 컨트롤 타워 시작하기
- 다음 단계

AWS Control 타워 퀵 스타트 가이드

처음 사용하는 경우 이 섹션의 단계에 따라 AWS Control Tower를 빠르게 시작할 수 있습니다. AWSAWS Control Tower 환경을 즉시 사용자 지정하려면 을 참조하십시오 단계 2. 랜딩 존 구성 및 시작 .

> **Note**
>
> AWS 컨트롤 타워는,, 아마존, 아마존 S3 AWS CloudTrail AWS ConfigCloudWatch, 아마존 VPC와 같은 유료 서비스를 설정합니다. 요금 페이지에 표시된 것처럼 이러한 서비스를 사용할 경우 비용이 발생할 수 있습니다. AWS 관리 콘솔에는 모든 유료 서비스의 사용량과 발생한 비용이 표시됩니다. AWS Control Tower 자체에서는 추가 비용이 발생하지 않습니다.

시작하기 전에

설치 프로세스를 시작하기 전에 내려야 할 가장 중요한 결정은 거주 지역을 선택하는 것입니다. 홈 리전은 대부분의 워크로드를 실행하거나 대부분의 데이터를 저장할 AWS 지역입니다. AWS Control Tower 랜딩 존을 설정한 후에는 변경할 수 없습니다. 홈 리전을 선택하는 방법에 대한 자세한 내용은 을 참조하십시오 Landing Zone 설정을 위한 관리 팁 .

> **Note**
>
> 기본적으로 AWS Control Tower는 사용자 계정이 현재 운영되고 있는 지역을 홈 리전으로 선택합니다. AWS 관리 콘솔 화면 오른쪽 상단에서 현재 지역을 확인할 수 있습니다.

빠른 시작 절차에서는 AWS Control Tower 환경의 리소스 기본값을 수락한다고 가정합니다. 이러한 선택 사항 중 다수는 나중에 변경할 수 있습니다. 라는 Landding Zone 구성에 대한 기대치 섹션에 몇 가지 일회성 선택 항목이 나열되어 있습니다.

새 AWS 계정을 만들면 AWS Control Tower 설정에 필요한 사전 요구 사항이 자동으로 충족됩니다. 다음 단계를 계속 진행할 수 있습니다.

빠른 시작 단계

1. 관리자 사용자 자격 증명으로 AWS 관리 콘솔에 로그인합니다.
2. https://console.aws.amazon.com/controltower 에서 AWS Control Tower 콘솔로 이동하십시오.
3. 원하는 거주 지역에서 일하고 있는지 확인하십시오.
4. 랜딩 존 설정을 선택합니다.
5. 콘솔의 지침을 따르고 모든 기본값을 그대로 적용합니다. 계정의 이메일 주소, 로그 아카이브 계정, 감사 계정을 입력해야 합니다.
6. 선택 사항을 확인하고 랜딩 존 설정을 선택합니다.
7. AWS Control Tower는 랜딩 존에 모든 리소스를 설정하는 데 약 30분이 걸립니다.

환경을 사용자 지정하는 방법을 포함하여 AWS Control Tower를 설정하는 방법에 대한 자세한 내용은 다음 몇 가지 항목의 절차를 읽고 따르십시오.

> **Note**
>
> 처음 이용하는 고객인데 설정 문제가 발생하는 경우 Support에 연락하여 진단 AWS 지원을 받으십시오.

전제 조건: 관리 계정에 대한 자동화된 사전 출시 확인

AWS Control Tower는 랜딩 존을 설정하기 전에 계정에서 일련의 사전 시작 검사를 자동으로 실행합니다. 이러한 점검에는 별도의 조치가 필요하지 않으므로 Management Account가 landing Zone을 설정

하는 변경 사항에 대비할 수 있습니다. 랜딩 존을 설정하기 전에 AWS Control Tower가 실행하는 검사는 다음과 같습니다.

- 에 대한 기존 서비스 한도는 AWS Control Tower를 시작하기에 AWS 계정 충분해야 합니다. 자세한 설명은 AWS Control Tower의 한도 및 할당량 섹션을 참조하세요.
- 다음 AWS 서비스에 AWS 계정 가입해야 합니다.
  - Amazon Simple Storage Service(S3)
  - Amazon Elastic Compute Cloud(Amazon EC2)
  - Amazon SNS
  - Amazon Virtual Private Cloud(VPC)
  - AWS CloudFormation
  - AWS CloudTrail
  - 아마존 CloudWatch
  - AWS Config
  - AWS Identity and Access Management (IAM)
  - AWS Lambda

> **Note**
>
> 기본적으로 모든 계정은 이러한 서비스를 구독합니다.

AWS IAM Identity Center (IAM ID 센터) 고객을 위한 고려 사항

- AWS IAM Identity Center (IAM ID 센터) 가 이미 설정되어 있는 경우, AWS Control Tower 홈 지역은 IAM 자격 증명 센터 지역과 동일해야 합니다.
- IAM ID 센터는 조직의 관리 계정에만 설치할 수 있습니다.
- 선택한 ID 소스에 따라 IAM ID 센터 디렉터리에는 세 가지 옵션이 적용됩니다.
  - IAM ID 센터 사용자 스토어: AWS Control Tower에 IAM 자격 증명 센터를 설치한 경우, AWS Control Tower는 IAM ID 센터 디렉터리에 그룹을 생성하고, 선택한 사용자에 대해 멤버 계정으로 이러한 그룹에 대한 액세스 권한을 제공합니다.
  - Active Directory: AWS Control Tower용 IAM ID 센터가 Active Directory와 함께 설정된 경우, AWS Control Tower는 IAM ID 센터 디렉터리를 관리하지 않습니다. 새 AWS 계정에 사용자나 그룹을 배정하지 않습니다.

- 외부 ID 공급자: AWS Control Tower용 IAM ID 센터를 외부 ID 공급자 (IdP) 로 설정한 경우, AWS Control Tower는 IAM ID 센터 디렉터리에 그룹을 생성하고 멤버 계정으로 선택한 사용자에게 이러한 그룹에 대한 액세스 권한을 제공합니다. 계정 생성 시 Account Factory에서 외부 IdP의 기존 사용자를 지정할 수 있으며, AWS Control Tower는 IAM Identity Center와 외부 IdP 간에 동일한 이름의 사용자를 동기화할 때 이 사용자에게 새로 벤딩된 계정에 대한 액세스 권한을 부여합니다. 또한 외부 IdP에 그룹을 생성하여 AWS Control Tower의 기본 그룹 이름과 일치하도록 할 수 있습니다. 이러한 그룹에 사용자를 할당하면 해당 사용자는 등록된 계정에 액세스할 수 있습니다.

IAM ID 센터 및 AWS Control Tower와의 작업에 대한 자세한 내용은 을 참조하십시오. IAM 자격 증명 센터 계정 및 AWS Control Tower에 대해 알아야 할 사항

AWS Config 및 AWS CloudTrail 고객에 대한 고려 사항

- AWS Config 또는 에 대해서는 조직 관리 계정에서 신뢰할 수 있는 액세스를 활성화할 수 AWS 계정 없습니다 CloudTrail. 신뢰할 수 있는 액세스를 사용하지 않도록 설정하는 방법에 대한 자세한 내용은 신뢰할 수 있는 액세스를 사용하거나 사용하지 않도록 설정하는 방법에 대한 AWS Organizations 설명서를 참조하십시오.
- AWS Control Tower에 등록하려는 기존 계정에 기존 AWS Config 레코더, 전송 채널 또는 집계 설정이 있는 경우, 계정을 등록하기 전, 즉 랜딩 존이 설정된 후에 이러한 구성을 수정하거나 제거해야 합니다. 이 사전 점검은 랜딩 존 출시 시 AWS Control Tower 관리 계정에는 적용되지 않습니다. 자세한 설명은 기존 AWS Config 리소스가 있는 계정 등록 섹션을 참조하세요.
- AWS Control Tower의 계정에서 임시 워크로드를 실행하는 경우 Config와 관련된 비용이 증가할 수 있습니다. AWS 이러한 비용 관리에 대한 자세한 내용은 AWS 계정 담당자에게 문의하십시오.
- 계정을 AWS Control Tower에 등록하면 해당 계정은 AWS Control Tower 조직의 AWS CloudTrail 트레일에 따라 관리됩니다. 계정에 CloudTrail 트레일을 기존에 배포한 경우, AWS Control Tower에 등록하기 전에 해당 계정의 기존 트레일을 삭제하지 않는 한 요금이 중복될 수 있습니다. 조직 수준의 트레일 및 AWS Control Tower에 대한 자세한 내용은 을 참조하십시오. 요금

> **Note**
>
> 시작 시 AWS Control Tower가 관리하는 모든 지역의 관리 계정에서 AWS 보안 토큰 서비스 (STS) 엔드포인트를 활성화해야 합니다. 그렇지 않으면 중간에 구성 프로세스에서 시작이 실패할 수 있습니다.

콘솔에서 AWS Control Tower를 시작하기

이 시작 절차는 AWS Control Tower 관리자를 대상으로 합니다. AWS Control Tower 콘솔을 사용하여 랜딩 존을 설정할 준비가 되면 이 절차를 따르십시오. 처음부터 끝까지 약 30분이 소요됩니다. 이 절차에는 몇 가지 전제 조건과 세 가지 주요 단계가 필요합니다.

현재 AWS Control Tower를 처음 사용하는 AWS 고객이라면 진행하기 전에 라는 섹션을 검토해 AWS Control Tower 랜딩 존을 계획하십시오. 보는 것이 좋습니다.

주제

1단계: 공유 계정 이메일 주소 생성

새 AWS 계정랜딩 존을 설정하는 경우 을 참조하십시오설정.

- 새 공유 계정으로 랜딩 존을 설정하려면 AWS Control Tower에는 아직 연결되지 않은 두 개의 고유한 이메일 주소가 필요합니다 AWS 계정. 각 이메일 주소는 AWS Control Tower와 관련된 특정 작업을 수행하는 기업 내 다양한 사용자를 위한 공동 수신함 (공유 이메일 계정) 역할을 합니다.
- AWS Control Tower를 처음으로 설정하고 기존 보안 및 로그 아카이브 계정을 AWS Control Tower로 가져오는 경우 기존 AWS 계정의 현재 이메일 주소를 입력할 수 있습니다.

이메일 주소는 다음과 같은 경우에 필요합니다.

- 감사 계정 — 이 계정은 AWS Control Tower에서 제공하는 감사 정보에 액세스해야 하는 사용자 팀을 위한 것입니다. 이 계정을 환경의 프로그래밍 방식 감사를 수행하여 규정 준수를 위해 감사하는 데 도움이 되는 타사 도구의 액세스 지점으로 사용할 수도 있습니다.
- 로그 아카이브 계정 — 이 계정은 랜딩 존에 등록된 OU 내에 등록된 모든 계정의 모든 로깅 정보에 액세스해야 하는 사용자 팀을 위한 것입니다.

이러한 계정은 랜딩 존을 생성할 때 보안 OU에 설정됩니다. 모범 사례로, 이러한 계정에서 작업을 수행할 때는 적절한 범위의 권한을 가진 IAM Identity Center 사용자를 사용하는 것이 좋습니다.

> **Note**
>
> 기존 AWS 계정을 감사 및 로그 아카이브 계정으로 지정하는 경우 기존 계정은 시작 전 몇 가지 검사를 통과하여 리소스가 AWS Control Tower 요구 사항과 충돌하지 않는지 확인해야 합니다. 이러한 검사에 실패하면 landing Zone 설정이 성공하지 못할 수 있습니다. 특히 계정에 기존 AWS Config 리소스가 없어야 합니다. 자세한 정보는 기존 보안 또는 로깅 계정을 가져올 때 고려할 사항을 참조하세요.

명확성을 위해 이 사용 설명서에서는 항상 공유 계정을 기본 이름 (로그 아카이브 및 감사) 으로 참조합니다. 이 문서를 읽을 때는 이러한 계정을 사용자 지정하기로 선택한 경우 처음에 해당 계정에 지정한 사용자 지정 이름을 대체하는 것을 잊지 마십시오. 계정 세부 정보 페이지에서 사용자 지정된 이름이 있는 계정을 볼 수 있습니다.

> **Note**
>
> AWS 다중 계정 전략에 맞게 일부 AWS Control Tower OU (조직 구성 단위) 의 기본 이름에 관한 용어를 변경하고 있습니다. 이러한 이름의 명확성을 개선하기 위해 전환하는 과정에서 일부 불일치를 발견할 수 있습니다. 이전에는 보안 OU를 코어 OU라고 불렀습니다. 샌드박스 OU는 이전에 사용자 지정 OU라고 불렸습니다.

Landding Zone 구성에 대한 기대치

AWS Control Tower 랜딩 존을 설정하는 프로세스는 여러 단계로 이루어집니다. AWS Control Tower 랜딩 존의 특정 측면을 구성할 수 있습니다. 설정 후에는 다른 선택 사항을 변경할 수 없습니다.

설정 중에 구성할 주요 항목

- 설치 중에 최상위 OU 이름을 선택할 수 있으며, 랜딩 존을 설정한 후에 OU 이름을 변경할 수도 있습니다. 기본적으로 최상위 OU의 이름은 보안 및 샌드박스로 지정됩니다. 자세한 정보는 잘 설계된 환경을 설정하기 위한 지침을 참조하세요.
- 설정 중에 AWS Control Tower가 생성하는 공유 계정의 사용자 지정 이름 (기본적으로 로그 아카이브 및 감사라고 함) 을 선택할 수 있지만, 설정 후에는 이러한 이름을 변경할 수 없습니다. (이는 일회성 선택입니다.)
- 설정 중에 감사 및 로그 아카이브 AWS 계정으로 사용할 AWS Control Tower의 기존 계정을 선택적으로 지정할 수 있습니다. 기존 AWS 계정을 지정하려는 경우 해당 계정에 기존 AWS Config 리소스

가 있는 경우, 계정을 AWS Control Tower에 등록하려면 먼저 기존 AWS Config 리소스를 삭제해야 합니다. (이는 일회성 선택입니다.)

- 처음으로 설정하거나 landing zone 버전 3.0으로 업그레이드하는 경우, AWS Control Tower가 조직에 맞게 조직 수준의 AWS CloudTrail 트레일을 설정하도록 허용할지 또는 AWS Control Tower에서 관리하는 트레일을 옵트아웃하고 자체 트레일을 관리할 수 있습니다. CloudTrail 랜딩 존을 업데이트할 때마다 AWS Control Tower에서 관리하는 조직 수준의 트레일을 옵트인하거나 옵트아웃할 수 있습니다.
- 랜딩 존을 설정하거나 업데이트할 때 Amazon S3 로그 버킷 및 로그 액세스 버킷에 대한 사용자 지정 보존 정책을 선택적으로 설정할 수 있습니다.
- 필요에 따라 AWS Control Tower 콘솔에서 사용자 지정 멤버 계정을 프로비저닝하는 데 사용할 이전에 정의된 블루프린트를 지정할 수 있습니다. 청사진을 사용할 수 없는 경우 나중에 계정을 사용자 지정할 수 있습니다. AFC (Account Factory Customize) 로 계정을 사용자 지정하세요 섹션을 참조하십시오.

취소할 수 없는 구성 선택

- landing Zone을 설정한 후에는 거주 지역을 변경할 수 없습니다.
- Account Factory 계정을 VPC로 프로비저닝하는 경우 VPC CIDR은 생성된 후에는 변경할 수 없습니다.

단계 2. 랜딩 존 구성 및 시작

AWS Control Tower 랜딩 존을 시작하기 전에 가장 적합한 홈 리전을 결정하십시오. 자세한 정보는 Landing Zone 설정을 위한 관리 팁 을 참조하세요.

> **Important**
>
> AWS Control Tower 랜딩 존을 배포한 후 홈 리전을 변경하려면 지원 부서의 지원과 AWS 함께 서비스 해제가 필요합니다. 이 방법은 권장되지 않습니다.

in을 사용하여 landing Zone을 구성하고 시작하는 방법을 알아보십시오API를 사용하여 AWS 컨트롤 타워 시작하기. AWS CLI

콘솔에서 랜딩 존을 구성하고 시작하려면 다음 일련의 단계를 수행하십시오.

준비: AWS Control Tower 콘솔로 이동

1. 웹 브라우저를 열고 https://console.aws.amazon.com/controltower 에서 AWS Control Tower 콘솔로 이동합니다.
2. 콘솔에서 원하는 홈 리전에서 AWS Control Tower를 사용하고 있는지 확인하십시오. 그런 다음 랜딩 존 설정을 선택합니다.

2a단계. 지역 검토 및 선택 AWS

홈 AWS 지역으로 선택한 지역을 올바르게 지정했는지 확인하세요. AWS Control Tower를 배포한 후에는 홈 지역을 변경할 수 없습니다.

설치 프로세스의 이 섹션에서는 필요한 AWS 지역을 더 추가할 수 있습니다. 필요한 경우 나중에 지역을 더 추가할 수 있으며 지역을 거버넌스에서 제거할 수 있습니다.

관리할 추가 AWS 지역을 선택하려면

1. 패널에는 현재 지역 선택이 표시됩니다. 드롭다운 메뉴를 열어 거버넌스가 가능한 추가 지역 목록을 확인하세요.
2. 각 지역 옆의 확인란을 선택하여 AWS Control Tower의 거버넌스를 적용하십시오. 홈 지역 선택은 편집할 수 없습니다.

특정 지역에 대한 액세스를 거부하려면

특정 AWS 지역의 AWS 리소스 및 워크로드에 대한 액세스를 거부하려면 지역 거부 제어 섹션에서 활성화를 선택합니다. 기본적으로 이 컨트롤의 설정은 활성화되지 않습니다.

2b단계. 조직 단위 (OU) 구성

이러한 OU의 기본 이름을 그대로 사용하는 경우 설치를 계속하기 위해 취해야 할 조치는 없습니다. OU 이름을 변경하려면 양식 필드에 새 이름을 직접 입력합니다.

- 기본 OU — AWS 컨트롤 타워는 처음에 보안 OU라고 명명된 기본 OU를 사용합니다. 초기 설정 중에 그리고 이후에 OU 세부 정보 페이지에서 이 OU의 이름을 변경할 수 있습니다. 이 보안 OU에는 기본적으로 로그 아카이브 계정과 감사 계정이라고 하는 두 개의 공유 계정이 포함되어 있습니다.
- 추가 OU — AWS Control Tower는 사용자를 위해 하나 이상의 추가 OU를 설정할 수 있습니다. 랜딩 존에는 보안 OU 외에 추가 OU를 하나 이상 프로비저닝하는 것이 좋습니다. 이 추가 OU를 개발 프로젝트용으로 사용하는 경우 에 나와 있는 대로 샌드박스 OU로 이름을 지정하는 것이 좋습니다. 잘

설계된 환경을 설정하기 위한 지침 AWS Organizations에 이미 기존 OU가 있는 경우, AWS Control Tower에서 추가 OU 설정을 건너뛰는 옵션이 표시될 수 있습니다.

2c단계. 공유 계정, 로깅, 암호화를 구성합니다.

설정 프로세스의 이 섹션에는 공유 AWS Control Tower 계정의 이름에 대한 기본 선택 항목이 패널에 표시됩니다. 이 계정은 랜딩 존의 필수적인 부분입니다. 이러한 공유 계정을 이동하거나 삭제하지 마십시오. 설정 중에 감사 및 로그 아카이브 계정의 사용자 지정 이름을 선택할 수 있습니다. 기존 AWS 계정을 공유 계정으로 지정하는 일회성 옵션도 있습니다.

로그 아카이브 및 감사 계정에 고유한 이메일 주소를 제공해야 하며, 이전에 관리 계정에 제공한 이메일 주소를 확인할 수 있습니다. 편집 가능한 기본값을 변경하려면 편집 버튼을 선택합니다.

공유 계정 정보

- 관리 계정 — AWS Control Tower 관리 계정은 루트 수준의 일부입니다. 관리 계정은 AWS Control Tower 청구를 허용합니다. 이 계정에는 또한 landing Zone에 대한 관리자 권한이 있습니다. AWS Control Tower에서 청구 및 관리자 권한을 위한 별도의 계정을 생성할 수 없습니다.

  관리 계정에 표시된 이메일 주소는 이 설정 단계에서 편집할 수 없습니다. 확인 메시지로 표시되므로 계정이 여러 개인 경우 관리 계정이 올바르게 편집되고 있는지 확인할 수 있습니다.
- 두 개의 공유 계정 — 이 두 계정에 대해 사용자 지정 이름을 선택하거나 직접 계정을 가져올 수 있으며, 신규 또는 기존 계정마다 고유한 이메일 주소를 제공해야 합니다. AWS Control Tower에서 새 공유 계정을 생성하도록 선택한 경우, 이메일 주소에 이미 연결된 AWS 계정이 없어야 합니다.

공유 계정을 구성하려면 요청된 정보를 입력하십시오.

1. 콘솔에서 처음에 로그 아카이브 계정이라고 불렸던 계정의 이름을 입력합니다. 많은 고객이 이 계정의 기본 이름을 유지하기로 결정합니다.
2. 이 계정의 고유한 이메일 주소를 제공하십시오.
3. 처음에 감사 계정이라고 불렸던 계정의 이름을 입력합니다. 많은 고객이 이 계정을 보안 계정이라고 부릅니다.
4. 이 계정의 고유한 이메일 주소를 제공하십시오.

선택적으로 로그 보존을 구성할 수 있습니다.

이 설정 단계에서 AWS Control Tower에 AWS CloudTrail 로그를 저장하는 Amazon S3 버킷의 로그 보존 정책을 일 또는 년 단위로 최대 15년까지 사용자 지정할 수 있습니다. 로그 보존을 사용자 지정하지 않기로 선택한 경우 기본 설정은 표준 계정 로깅의 경우 1년, 액세스 로깅의 경우 10년입니다. 이 기능은 landing zone을 업데이트하거나 재설정할 때도 사용할 수 있습니다.

선택적으로 액세스를 자체 관리할 수 AWS 계정 있습니다.

AWS Control Tower가 AWS Identity and Access Management (IAM) 을 통해 AWS 계정 액세스를 설정할지, 아니면 IAM Identity AWS 계정 Center를 통해 직접 계정 페더레이션을 수행할지 또는 AWS IAM Identity Center를 통한 여러 계정으로의 페더레이션을 위해 IAM Identity Center 사용자, 역할 및 권한을 직접 설정하고 사용자 지정할 수 있는 외부 IdP와 같은 다른 방법을 사용하여 액세스를 관리할지 여부를 선택할 수 있습니다. 이 선택은 나중에 변경할 수 있습니다.

기본적으로 AWS Control Tower는 여러 계정을 사용하여 AWS 환경 구성에 정의된 모범 사례 지침에 따라 랜딩 존에 AWS IAM Identity Center를 설정합니다. 대부분의 고객은 기본값을 선택합니다. 특정 산업 또는 국가의 규정 준수를 위해 또는 AWS IAM Identity Center를 사용할 수 AWS 리전 없는 경우 대체 액세스 방법이 필요할 수 있습니다.

계정 수준에서 ID 제공자를 선택하는 것은 지원되지 않습니다. 이 옵션은 전체 착륙 지대에만 적용됩니다.

자세한 정보는 IAM ID 센터 지침을 참조하세요.

선택적으로 AWS CloudTrail 트레일을 구성할 수 있습니다.

가장 좋은 방법은 로깅을 설정하는 것입니다. AWS Control Tower가 조직 수준의 CloudTrail 트레일을 설정하고 관리하도록 허용하려면 옵트인을 선택하십시오. 자체 CloudTrail 트레일이나 타사 로깅 도구를 사용하여 로깅을 관리하려면 옵트아웃을 선택하십시오. 콘솔에서 선택 사항을 확인하라는 요청을 받으면 선택을 확인하십시오. landing Zone을 업데이트할 때 선택 항목을 변경하고 조직 수준의 트레일을 옵트인하거나 옵트아웃할 수 있습니다.

조직 수준 및 계정 수준 트레일을 포함하여 언제든지 자체 CloudTrail 트레일을 설정하고 관리할 수 있습니다. 중복 CloudTrail 트레일을 설정하는 경우 이벤트가 기록될 때 중복 비용이 발생할 수 있습니다. CloudTrail

선택적으로 구성할 수 있습니다. AWS KMS keys

리소스를 암호화 키로 암호화하고 복호화하려면 체크박스를 AWS KMS 선택합니다. 기존 키가 있는 경우 드롭다운 메뉴에 표시된 식별자에서 해당 키를 선택할 수 있습니다. 키 만들기를 선택하여 새 키를 생성할 수 있습니다. 랜딩 존을 업데이트할 때마다 KMS 키를 추가하거나 변경할 수 있습니다.

랜딩 존 설정을 선택하면 AWS Control Tower가 사전 검사를 수행하여 KMS 키를 검증합니다. 키는 다음 요구 사항을 충족해야 합니다.

- 활성화됨
- 대칭
- 멀티 리전 키가 아님
- 정책에 올바른 권한이 추가되었습니다.
- 키는 관리 계정에 있습니다.

키가 이러한 요구 사항을 충족하지 않으면 오류 배너가 표시될 수 있습니다. 이 경우 다른 키를 선택하거나 키를 생성하십시오. 다음 섹션에 설명된 대로 키의 권한 정책을 편집해야 합니다.

KMS 키 정책 업데이트

KMS 키 정책을 업데이트하려면 먼저 KMS 키를 생성해야 합니다. 자세한 내용은 AWS Key Management Service 개발자 안내서의 키 정책 생성을 참조하세요.

AWS Control Tower에서 KMS 키를 사용하려면 및 에 필요한 최소 권한을 추가하여 기본 KMS 키 정책을 업데이트해야 합니다. AWS Config AWS CloudTrail모범 사례로서 모든 정책에 필요한 최소 권한을 포함하는 것이 좋습니다. KMS 키 정책을 업데이트할 때 단일 JSON 문에서 권한을 그룹으로 추가하거나 한 줄씩 추가할 수 있습니다.

이 절차에서는 암호화를 AWS Config 허용하고 암호화에 사용할 AWS KMS 수 있는 정책 설명을 추가하여 AWS KMS 콘솔에서 기본 KMS 키 정책을 CloudTrail 업데이트하는 방법을 설명합니다. 정책 설명에는 다음 정보를 포함해야 합니다.

- **`YOUR-MANAGEMENT-ACCOUNT-ID`**— AWS Control Tower가 설치될 관리 계정의 ID.
- **`YOUR-HOME-REGION`**— AWS Control Tower를 설정할 때 선택할 홈 지역.
- **`YOUR-KMS-KEY-ID`**— 정책과 함께 사용될 KMS 키 ID.

KMS 키 정책을 업데이트하려면

1. 다음 위치에서 AWS KMS 콘솔을 엽니다. https://console.aws.amazon.com/kms
2. 탐색 창에서 고객 관리 키를 선택합니다.
3. 테이블에서 편집하려는 키를 선택합니다.
4. 키 정책 탭에서 키 정책을 볼 수 있는지 확인합니다. 키 정책을 볼 수 없는 경우 정책 보기로 전환을 선택합니다.

5. 편집을 선택하고 및 에 대한 AWS Config 다음 정책 설명을 추가하여 기본 KMS 키 정책을 업데이트하십시오. CloudTrail

AWS Config 정책 설명

```
{
    "Sid": "Allow Config to use KMS for encryption",
    "Effect": "Allow",
    "Principal": {
        "Service": "config.amazonaws.com"
    },
    "Action": [
        "kms:Decrypt",
        "kms:GenerateDataKey"
    ],
    "Resource": "arn:aws:kms:YOUR-HOME-REGION:YOUR-MANAGEMENT-ACCOUNT-ID:key/YOUR-KMS-KEY-ID"
}
```

CloudTrail 정책 성명서

```
{
    "Sid": "Allow CloudTrail to use KMS for encryption",
    "Effect": "Allow",
    "Principal": {
        "Service": "cloudtrail.amazonaws.com"
    },
    "Action": [
        "kms:GenerateDataKey*",
        "kms:Decrypt"
    ],
    "Resource": "arn:aws:kms:YOUR-HOME-REGION:YOUR-MANAGEMENT-ACCOUNT-ID:key/YOUR-KMS-KEY-ID",
    "Condition": {
        "StringEquals": {
            "aws:SourceArn": "arn:aws:cloudtrail:YOUR-HOME-REGION:YOUR-MANAGEMENT-ACCOUNT-ID:trail/aws-controltower-BaselineCloudTrail"
        },
        "StringLike": {
            "kms:EncryptionContext:aws:cloudtrail:arn": "arn:aws:cloudtrail:*:YOUR-MANAGEMENT-ACCOUNT-ID:trail/*"
        }
```

```
    }
}
```

6. 변경 사항 저장을 선택합니다.

KMS 키 정책 예시

다음 예제 정책은 부여하는 정책 AWS Config 설명과 CloudTrail 필요한 최소 권한을 추가한 후의 KMS 키 정책의 모습을 보여줍니다. 예제 정책에는 기본 KMS 키 정책이 포함되어 있지 않습니다.

```
{
    "Version": "2012-10-17",
    "Id": "CustomKMSPolicy",
    "Statement": [
        {
        ... YOUR-EXISTING-POLICIES ...
        },
        {
            "Sid": "Allow Config to use KMS for encryption",
            "Effect": "Allow",
            "Principal": {
                "Service": "config.amazonaws.com"
            },
            "Action": [
                "kms:Decrypt",
                "kms:GenerateDataKey"
            ],
            "Resource": "arn:aws:kms:YOUR-HOME-REGION:YOUR-MANAGEMENT-ACCOUNT-
ID:key/YOUR-KMS-KEY-ID"
        },
        {
            "Sid": "Allow CloudTrail to use KMS for encryption",
            "Effect": "Allow",
            "Principal": {
                "Service": "cloudtrail.amazonaws.com"
            },
            "Action": [
                "kms:GenerateDataKey*",
                "kms:Decrypt"
              ],
            "Resource": "arn:aws:kms:YOUR-HOME-REGION:YOUR-MANAGEMENT-ACCOUNT-
ID:key/YOUR-KMS-KEY-ID",
            "Condition": {
```

```
                "StringEquals": {
                    "aws:SourceArn": "arn:aws:cloudtrail:YOUR-HOME-REGION:YOUR-
MANAGEMENT-ACCOUNT-ID:trail/aws-controltower-BaselineCloudTrail"
                },
                "StringLike": {
                    "kms:EncryptionContext:aws:cloudtrail:arn":
 "arn:aws:cloudtrail:*:YOUR-MANAGEMENT-ACCOUNT-ID:trail/*"
                }
            }
        }
    ]
}
```

다른 예제 정책을 보려면 다음 페이지를 참조하십시오.

- 사용 AWS CloudTrail 설명서의 암호화 권한 부여.
- 개발자 안내서의 서비스 연결 Roless3 버킷 전송 사용 시 KMS 키에 필요한 권한.AWS Config

> **공격자로부터 보호**
>
> 정책에 특정 조건을 추가하면 특정 유형의 공격 (혼동 보조 공격) 을 방지하는 데 도움이 될 수 있습니다. 이러한 공격은 특정 주체가 더 많은 권한을 가진 주체에게 서비스 간 사칭과 같은 조치를 취하도록 강요하는 경우 발생합니다. 정책 조건에 대한 일반적인 내용은 을 참조하십시오. 정책에서 조건 지정

AWS Key Management Service (AWS KMS) 를 사용하면 다중 지역 KMS 키와 비대칭 키를 생성할 수 있지만 AWS Control Tower는 다중 지역 키 또는 비대칭 키를 지원하지 않습니다. AWS Control Tower는 기존 키의 사전 검사를 수행합니다. 멀티 리전 키 또는 비대칭 키를 선택하면 오류 메시지가 표시될 수 있습니다. 이 경우 AWS Control Tower 리소스와 함께 사용할 다른 키를 생성하십시오.

에 대한 AWS KMS자세한 내용은 AWS KMS 개발자 안내서를 참조하십시오.

참고로, AWS Control Tower의 고객 데이터는 기본적으로 SSE-S3 기술을 사용하여 유휴 상태에서 암호화됩니다.

필요에 따라 사용자 지정 멤버 계정을 구성 및 생성할 수 있습니다.

계정 생성 워크플로에 따라 멤버 계정을 추가할 때, 선택적으로 AWS Control Tower 콘솔에서 사용자 지정 멤버 계정을 프로비저닝하는 데 사용할 이전에 정의한 블루프린트를 지정할 수 있습니다. 청사진을 사용할 수 없는 경우 나중에 계정을 사용자 지정할 수 있습니다. AFC (Account Factory Customize)로 계정을 사용자 지정하세요 섹션을 참조하십시오.

단계 3. landing Zone 검토 및 설정

설정의 다음 섹션에서는 AWS Control Tower가 랜딩 존에 필요한 권한을 보여줍니다. 확인란을 선택하여 각 주제를 확장하십시오. 여러 계정에 영향을 미칠 수 있는 이러한 권한에 동의하고 전체 서비스 약관에 동의하라는 메시지가 표시됩니다.

최종 결정하려면

1. 콘솔에서 서비스 권한을 검토하고 준비가 되면 AWS Control Tower가 나를 대신하여 AWS 리소스를 관리하고 규칙을 적용하는 데 사용할 권한을 이해합니다를 선택합니다.
2. 선택을 마무리하고 출시를 초기화하려면 Set up landing zone을 선택합니다.

이 일련의 단계를 통해 착륙 지대 설정 프로세스가 시작되며 완료하는 데 약 30분이 소요될 수 있습니다. 설정 과정에서 AWS Control Tower는 루트 수준, 보안 OU 및 공유 계정을 생성합니다. 다른 AWS 리소스는 생성, 수정 또는 삭제됩니다.

> ⚠ SNS 구독 확인
>
> 감사 계정에 제공한 이메일 주소는 AWS Control Tower에서 지원하는 모든 AWS 지역으로부터 AWS 알림 — 구독 확인 이메일을 받게 됩니다. 감사 계정에서 규정 준수 이메일을 받으려면 AWS Control Tower에서 지원하는 각 AWS 지역의 각 이메일에서 구독 확인 링크를 선택해야 합니다.

API를 사용하여 AWS 컨트롤 타워 시작하기

이 시작 절차는 AWS Control Tower 관리자를 대상으로 합니다. 이 절차에는 몇 가지 전제 조건이 필요하며 여기에는 두 가지 주요 단계가 포함됩니다.

이 절차에서는 AWS Control Tower 및 기타 AWS 서비스의 API를 사용하여 랜딩 존을 구성하고 시작합니다. 이러한 API를 사용하면 AWS CloudFormation 콘솔이나 를 통해 프로그래밍 방식으로 AWS Control Tower 환경을 만들 수 있습니다. AWS CLI

AWS Control Tower 랜딩 존을 시작하기 전에 다음과 같은 사전 필수 작업을 수행하십시오.

- 가장 적합한 홈 리전을 결정하십시오. 자세한 정보는 Landing Zone 설정을 위한 관리 팁 을 참조하세요.
- 관리 계정이 랜딩 존 (landing zone) 을 설정하는 변경 사항에 대비할 준비가 되었는지 확인하는 자동화된 사전 출시 검사에 대해 알아보세요. 전제 조건: 관리 계정에 대한 자동화된 사전 출시 확인

주제

API를 사용한 랜딩 존 구성에 대한 기대치

AWS Control Tower 랜딩 존을 설정하는 프로세스는 여러 단계로 이루어집니다. AWS Control Tower 랜딩 존의 특정 측면을 구성할 수 있습니다. 설정 후에는 다른 옵션을 변경할 수 없습니다.

설정 중에 구성할 주요 항목

- 설치 중에 기본 OU 이름을 선택할 수 있으며, 랜딩 존을 설정한 후에 OU 이름을 변경할 수도 있습니다. 기본 OU의 이름은 기본적으로 보안 및 샌드박스로 지정됩니다. 자세한 정보는 잘 설계된 환경을 설정하기 위한 지침을 참조하세요.
- 설정 중에 AWS Control Tower가 생성하는 공유 계정의 사용자 지정 이름 (기본적으로 로그 아카이브 및 감사라고 함) 을 선택할 수 있지만, 설정 후에는 이러한 이름을 변경할 수 없습니다. (이는 일회성 선택입니다.)
- API로 설정하는 동안 감사 및 로그 아카이브 계정으로 사용할 AWS Control Tower의 기존 AWS 계정을 지정해야 합니다. 기존 AWS 계정을 지정하려면 해당 계정에 기존 AWS Config 리소스가 있는 경우 계정을 AWS Control Tower에 등록하기 전에 기존 AWS Config 리소스를 삭제하거나 수정해야 합니다. (이는 일회성 선택입니다.)

- 처음으로 설정하거나 landing zone 버전 3.0으로 업그레이드하는 경우, AWS Control Tower가 조직에 맞게 조직 수준의 AWS CloudTrail 트레일을 설정하도록 허용할지 또는 AWS Control Tower에서 관리하는 트레일을 옵트아웃하고 자체 트레일을 관리할 수 있습니다. CloudTrail 랜딩 존을 업데이트할 때마다 AWS Control Tower에서 관리하는 조직 수준의 트레일을 옵트인하거나 옵트아웃할 수 있습니다.
- 랜딩 존을 설정하거나 업데이트할 때 Amazon S3 로그 버킷 및 로그 액세스 버킷에 대한 사용자 지정 보존 정책을 선택적으로 설정할 수 있습니다.

취소할 수 없는 구성 선택

- landing Zone을 설정한 후에는 거주 지역을 변경할 수 없습니다.
- VPC로 계정을 프로비저닝하는 경우 VPC CIDR은 생성된 후에는 변경할 수 없습니다.

다음 섹션에서는 설명 및 주의 사항과 함께 설정 사전 요구 사항 및 단계를 자세히 설명합니다. 추가 코드 예제는 예: API만 사용하여 AWS Control Tower 랜딩 존 설정 단원을 참조하세요.

1단계: 랜딩 존 구성

AWS Control Tower 랜딩 존을 설정하는 프로세스는 여러 단계로 이루어집니다. AWS Control Tower 랜딩 존의 특정 부분은 구성할 수 있지만 설정 후에는 다른 선택 사항을 변경할 수 없습니다. landing Zone을 발사하기 전에 이러한 중요한 고려 사항에 대해 자세히 알아보려면 검토하세요 Landding Zone 구성에 대한 기대치 .

AWS Control Tower 랜딩 존 API를 사용하기 전에 먼저 다른 AWS 서비스에서 API를 호출하여 시작 전에 랜딩 존을 구성해야 합니다. 이 프로세스에는 세 가지 주요 단계가 포함됩니다.

- 새 AWS Organizations 조직 만들기,
- 공유 계정 이메일 주소 설정,
- 그리고 landing zone API를 호출하는 데 필요한 권한을 가진 IAM 역할 또는 IAM ID 센터 사용자를 생성합니다.

단계 1. 착륙 지대를 포함할 조직을 만드십시오.

1. AWS Organizations `CreateOrganization`API를 호출하고 모든 기능을 활성화하여 기본 OU를 생성합니다. AWS Control Tower는 처음에 이를 보안 OU라고 명명했습니다. 이 보안 OU에는 기본적으로 로그 아카이브 계정과 감사 계정이라고 하는 두 개의 공유 계정이 포함되어 있습니다.

```
aws organizations create-organization --feature-set ALL
```

AWS Control Tower는 하나 이상의 추가 OU를 설정할 수 있습니다. 랜딩 존에는 보안 OU 외에 추가 OU를 하나 이상 프로비저닝하는 것이 좋습니다. 이 추가 OU를 개발 프로젝트용으로 사용하는 경우에 나와 있는 대로 샌드박스 OU로 이름을 지정하는 것이 좋습니다. AWS AWS Control Tower 랜딩 존을 위한 다중 계정 전략

단계 2. 필요한 경우 공유 계정을 프로비저닝하십시오.

랜딩 존을 설정하려면 AWS Control Tower에 두 개의 이메일 주소가 필요합니다. 처음으로 랜딩 존 API를 사용하여 AWS Control Tower를 설정하는 경우 기존 보안 및 로그 아카이브 AWS 계정을 사용해야 합니다. 기존 AWS 계정이메일 주소의 현재 이메일 주소를 사용할 수 있습니다. 각 이메일 주소는 AWS Control Tower와 관련된 특정 작업을 수행하는 기업 내 다양한 사용자를 위한 공동 수신함 (공유 이메일 계정) 역할을 합니다.

기존 AWS 계정이 없는 경우 새 랜딩 존 설정을 시작하려면 AWS Organizations API를 사용하여 보안 및 로그 아카이브 AWS 계정을 프로비저닝할 수 있습니다.

1. AWS Organizations `CreateAccount`API를 호출하여 보안 OU에 로그 아카이브 계정 및 감사 계정을 생성합니다.

```
aws organizations create-account --email mylog@example.com --account-name "Logging
 Account"
```

```
aws organizations create-account --email mysecurity@example.com --account-name
 "Security Account"
```

2. (선택 사항) AWS Organizations `DescribeAccount` API를 사용하여 `CreateAccount` 작업 상태를 확인합니다.

단계 3. 필수 서비스 역할 생성

AWS Control Tower가 랜딩 존을 설정하는 데 필요한 API 호출을 수행할 수 있도록 다음과 같은 IAM 서비스 역할을 생성하십시오.

- `AWSControlTowerAdmin`
- `AWSControlTowerCloudTrailRole`

- AWSControlTowerStackSetRole
- AWSControlTowerConfigAggregatorRoleForOrganizations

이러한 역할 및 정책에 대한 자세한 내용은 을 참조하십시오AWS Control Tower에 대한 자격 증명 기반 정책 (IAM 정책) 사용.

IAM 역할을 만들려면:

1. 모든 landing zone API를 호출하는 데 필요한 권한을 가진 IAM 역할을 생성합니다. 또는 IAM Identity Center 사용자를 생성하고 필요한 권한을 할당할 수 있습니다.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "controltower:CreateLandingZone",
                "controltower:UpdateLandingZone",
                "controltower:ResetLandingZone",
                "controltower:DeleteLandingZone",
                "controltower:GetLandingZoneOperation",
                "controltower:GetLandingZone",
                "controltower:ListLandingZones",
                "controltower:ListTagsForResource",
                "controltower:TagResource",
                "controltower:UntagResource",
                "servicecatalog:*",
                "organizations:*",
                "sso:*",
                "sso-directory:*",
                "logs:*",
                "cloudformation:*",
                "kms:*",
                "iam:GetRole",
                "iam:CreateRole",
                "iam:GetSAMLProvider",
                "iam:CreateSAMLProvider",
                "iam:CreateServiceLinkedRole",
                "iam:ListRolePolicies",
                "iam:PutRolePolicy",
                "iam:ListAttachedRolePolicies",
```

```
                "iam:AttachRolePolicy",
                "iam:DeleteRole",
                "iam:DeleteRolePolicy",
                "iam:DetachRolePolicy"
            ],
            "Resource": "*"
        }
    ]
}
```

2단계: 랜딩 존 시작

AWS Control Tower CreateLandingZone API에는 입력 파라미터로 랜딩 존 버전과 매니페스트 파일이 필요합니다. 매니페스트 파일을 사용하여 다음 기능을 구성할 수 있습니다.

- 선택적으로 로그 보존을 구성할 수 있습니다.
- 선택적으로 액세스를 자체 관리할 수 AWS 계정 있습니다.
- 선택적으로 트레일을 구성할 AWS CloudTrail 수 있습니다.
- 선택적으로 구성할 수 있습니다. AWS KMS keys

매니페스트 파일을 컴파일하고 나면 새 랜딩 존을 만들 준비가 된 것입니다.

> **Note**
>
> AWS Control Tower는 API를 사용하여 랜딩 존을 구성하고 시작하는 경우 리전 거부 제어를 지원하지 않습니다. API를 사용하여 랜딩 존을 성공적으로 시작한 후에는 AWS Control Tower 콘솔을 사용하여 리전 거부 제어를 구성할 수 있습니다.

1. AWS 컨트롤 타워 CreateLandingZone API를 호출하십시오. 이 API를 입력하려면 landing Zone 버전과 매니페스트 파일이 필요합니다.

   ```
   aws controltower create-landing-zone --landing-zone-version 3.3 --manifest "file://
   LandingZoneManifest.json"
   ```

   LandingZoneManifest.json 매니페스트 예시:

   ```
   {
   ```

```
   "governedRegions": ["us-west-2","us-west-1"],
   "organizationStructure": {
       "security": {
           "name": "CORE"
       },
       "sandbox": {
           "name": "Sandbox"
       }
   },
   "centralizedLogging": {
        "accountId": "222222222222",
        "configurations": {
            "loggingBucket": {
                "retentionDays": 60
            },
            "accessLoggingBucket": {
                "retentionDays": 60
            },
            "kmsKeyArn": "arn:aws:kms:us-west-1:123456789123:key/
e84XXXXX-6bXX-49XX-9eXX-ecfXXXXXXXXX"
        },
        "enabled": true
   },
   "securityRoles": {
        "accountId": "333333333333"
   },
   "accessManagement": {
        "enabled": true
   }
}
```

> **Note**
>
> 예제에서 볼 수 있듯이, CentralizedLogging 와 SecurityRoles 계정의 AccountId용은 달라야 합니다.

출력:

```
{
   "arn": "arn:aws:controltower:us-west-2:123456789012:landingzone/1A2B3C4D5E6F7G8H",
   "operationIdentifier": "55XXXXXX-e2XX-41XX-a7XX-446XXXXXXXXX"
```

```
}
```

2. GetLandingZoneOperationAPI를 호출하여 CreateLandingZone 작업 상태를 확인합니다. GetLandingZoneOperationAPI는 SUCCEEDEDFAILED, 또는 상태를 반환합니다IN_PROGRESS.

```
aws controltower get-landing-zone-operation --operation-identifier "55XXXXXX-
eXXX-4XXX-aXXX-44XXXXXXXXXX"
```

출력:

```
{
    "operationDetails": {
        "operationType": "CREATE",
        "startTime": "Thu Nov 09 20:39:19 UTC 2023",
        "endTime": "Thu Nov 09 21:02:01 UTC 2023",
        "status": "SUCCEEDED"
    }
}
```

3. 상태가 로 SUCCEEDED 반환되면 GetLandingZone API를 호출하여 landing zone 구성을 검토할 수 있습니다.

```
aws controltower get-landing-zone --landing-zone-identifier "arn:aws:controltower:us-
west-2:123456789123:landingzone/1A2B3C4D5E6F7G8H"
```

출력:

```
{
    "landingZone": {
        "arn": "arn:aws:controltower:us-
west-2:123456789012:landingzone/1A2B3C4D5E6F7G8H",
        "driftStatus": {
            "status": "IN_SYNC"
        },
        "latestAvailableVersion": "3.3",
        "manifest": {
            "accessManagement": {
                "enabled": true
            },
            "securityRoles": {
                "accountId": "333333333333"
```

```
            },
            "governedRegions": [
                "us-west-1",
                "eu-west-3",
                "us-west-2"
            ],
            "organizationStructure": {
                "sandbox": {
                    "name": "Sandbox"
                },
                "security": {
                    "name": "CORE"
                }
            },
            "centralizedLogging": {
                "accountId": "222222222222",
                "configurations": {
                    "loggingBucket": {
                        "retentionDays": 60
                    },
                    "kmsKeyArn": "arn:aws:kms:us-west-1:123456789123:key/
e84XXXXX-6bXX-49XX-9eXX-ecfXXXXXXXXX",
                    "accessLoggingBucket": {
                        "retentionDays": 60
                    }
                },
                "enabled": true
            }
        },
        "status": "PROCESSING",
        "version": "3.3"
    }
}
```

랜딩 존 확인하기

전화를 통해 계정이 이미 AWS Control Tower에 설정되어 있는지 확인할 `ListLandingZones` 수 있습니다. 이 API는 랜딩 존의 홈 지역과 상관없이 모든 상업 지역에서 하나의 랜딩 존 식별자 (ARN) 를 반환합니다. 랜딩 존 ARN은 지역별로 고유합니다.

```
aws controltower list-landing-zones --region us-east-1
```

옵트인 지역의 경우 *ListLandingZones* API는 API의 홈 리전과 동일한 리전에서 API를 호출하는 경우에만 랜딩 존 식별자를 반환합니다. 예를 들어, 랜딩 존이 af-south-1로 설정되어 있고 af-south-1을 ListLandingZones 호출하면 API는 랜딩 존 식별자를 반환합니다. 랜딩 존이 af-south-1에 설정되어 있고 ap-east-1을 ***ListLandingZones*** 호출하는 경우 API는 랜딩 존 식별자를 반환하지 않습니다.

출력:

```
{
   "landingZones" [
        "arn": "arn:aws:controltower:us-
west-2:123456789123:landingzone/1A2B3C4D5E6F7G8H"
   ]
}
```

랜딩 존 업데이트

새 랜딩 존 버전을 사용할 수 있거나 랜딩 존 구성을 추가로 업데이트하려면 UpdateLandingZone API를 호출하여 업데이트된 매니페스트 파일을 참조할 수 있습니다. 이 API는 를 반환하며OperationIdentifier, 이를 사용하여 GetLandingZoneOperation API를 호출하여 업데이트 작업 상태를 확인할 수 있습니다.

랜딩 존을 업데이트하려면

1. AWS Control Tower UpdateLandingZone API를 호출하여 업데이트된 랜딩 존 버전 또는 업데이트된 매니페스트를 참조하십시오.

   ```
   aws controltower update-landing-zone --landing-zone-version 3.3 --landing-zone-
   identifier "arn:aws:controltower:us-west-2:123456789123:landingzone/1A2B3C4D5E6F7G8H"
    --manifest file://LandingZoneManifest.json
   ```

LandingZoneManifest.json:

```
{
   "governedRegions": ["us-west-2","us-west-1"],
   "organizationStructure": {
       "security": {
           "name": "CORE"
       },
       "sandbox": {
```

```
            "name": "Sandbox"
        }
    },
    "centralizedLogging": {
         "accountId": "222222222222",
         "configurations": {
             "loggingBucket": {
                 "retentionDays":2555
             },
             "accessLoggingBucket": {
                 "retentionDays": 2555
             },
             "kmsKeyArn": "arn:aws:kms:us-west-1:123456789123:key/
e84XXXXX-6bXX-49XX-9eXX-ecfXXXXXXXXX"
         },
         "enabled": true
    },
    "securityRoles": {
         "accountId": "333333333333"
    },
    "accessManagement": {
         "enabled": true
    }
}
```

출력:

```
{
   "operationIdentifier": "55XXXXXX-e2XX-41XX-a7XX-446XXXXXXXXX"
}
```

선택적으로 OU를 재등록하여 계정을 업데이트합니다.

계정이 300개 미만인 등록된 AWS Control Tower OU의 경우, AWS Control Tower 콘솔을 사용하여 대시보드의 OU 페이지에 액세스한 다음 OU 재등록을 선택하여 해당 OU의 계정을 업데이트할 수 있습니다.

드리프트를 해결하기 위해 착륙 지대를 재설정하십시오.

랜딩 존을 만들면 랜딩 존과 모든 OU (조직 구성 단위), 계정, 리소스는 선택한 컨트롤에서 적용되는 거버넌스 규칙을 준수합니다. 사용자와 조직 구성원이 landing Zone을 사용할 때 이 규정 준수 상태가 변경될 수 있습니다. 이러한 변경을 드리프트라고 합니다.

랜딩 존이 드리프트 상태인지 확인하기 위해 `GetLandingZone` API를 호출할 수 있습니다. 이 API는 착륙 지대의 드리프트 상태를 또는 로 `DRIFTED` 반환합니다. `IN_SYNC`

랜딩 존 내의 드리프트를 해결하려면 `ResetLandingZone` API를 사용하여 랜딩 존을 원래 구성으로 재설정할 수 있습니다. 예를 들어, AWS Control Tower는 기본적으로 IAM Identity Center를 활성화하여 AWS 계정관리를 지원하지만 IAM Identity Center를 비활성화한 상태에서 원래 랜딩 존 파라미터를 구성하는 경우 호출하면 비활성화된 IAM ID 센터 구성이 `ResetLandingZone` 그대로 유지됩니다.

사용 가능한 최신 landing zone 버전을 사용하는 경우에만 `ResetLandingZone` API를 사용할 수 있습니다. `GetLandingZone`API를 호출하여 landing Zone 버전을 사용 가능한 최신 버전과 비교할 수 있습니다. 필요한 경우, landing Zone이 사용 가능한 최신 버전을 사용하도록 할 랜딩 존 업데이트 수 있습니다. 이 예시에서는 버전 3.3을 최신 버전으로 사용하고 있습니다.

1. `GetLandingZone` API를 호출하세요. API가 드리프트 상태를 반환하면 착륙 지대가 드리프트 상태인 것입니다. `DRIFTED`
2. `ResetLandingZone`API를 호출하여 랜딩 존을 원래 구성으로 재설정합니다.

```
aws controltower reset-landing-zone --landing-zone-identifier
 "arn:aws:controltower:us-west-2:123456789123:landingzone/1A2B3C4D5E6F7G8H"
```

출력:

```
{
   "operationIdentifier": "55XXXXXX-e2XX-41XX-a7XX-446XXXXXXXXX"
}
```

> **Note**
>
> 랜딩 존을 재설정해도 랜딩 존 버전은 업데이트되지 않습니다. landing zone 버전 업데이트에 랜딩 존 업데이트 대한 세부 정보를 확인하세요.

랜딩 존을 폐기하세요

랜딩 존의 모든 자원을 정리하는 프로세스를 랜딩 존 해체라고 합니다.

> **Important**
>
> 랜딩 영역 사용을 중지하려는 경우에만 이 폐기 프로세스를 수행하는 것이 좋습니다. 기존 랜딩 영역을 폐기한 후에는 다시 생성할 수 없습니다.

AWS Control Tower가 사용자 데이터 및 기존 AWS Organizations데이터를 처리하는 방식에 대한 중요한 정보를 포함하여 랜딩 존 해제에 대한 자세한 내용은 을 참조하십시오. 둘러보기: AWS Control Tower 랜딩 존 해체

랜딩 존을 해제하려면 `DeleteLandingZone` API를 호출하세요. 이 API는 를 반환하며`OperationIdentifier`, 이를 사용하여 `GetLandingZoneOperation` API를 호출하여 삭제 작업 상태를 확인할 수 있습니다.

```
aws controltower delete-landing-zone --landing-zone-identifier
"arn:aws:controltower:us-west-2:123456789012:landingzone/1A2B3C4D5E6F7G8H"
```

출력:

```
{
   "operationIdentifier": "55XXXXXX-e2XX-41XX-a7XX-446XXXXXXXXX"
}
```

예: API만 사용하여 AWS Control Tower 랜딩 존 설정

이 예제 안내는 첨부 문서입니다. 설명, 주의 사항 및 자세한 내용은 API를 사용하여 AWS Control Tower 시작하기를 참조하십시오.

사전 조건

AWS Control Tower 랜딩 존을 생성하기 전에 조직 1개, 공유 계정 2개, IAM 역할 몇 개를 생성해야 합니다. 이 안내 자습서에는 이러한 단계와 CLI 명령 예시 및 출력이 포함되어 있습니다.

단계 1. 조직과 두 개의 필수 계정을 생성합니다.

```
aws organizations create-organization --feature-set ALL
aws organizations create-account --email example+log@example.com --account-name "Log
 archive account"
aws organizations create-account --email example+aud@example.com --account-name "Audit
 account"
```

단계 2. 필수 IAM 역할을 생성합니다.

AWSControlTowerAdmin

```
cat <<EOF >controltower_trust.json
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "controltower.amazonaws.com"
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
EOF
aws iam create-role --role-name AWSControlTowerAdmin --path /service-role/ --assume-
role-policy-document file://controltower_trust.json
cat <<EOF >ct_admin_role_policy.json
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "ec2:DescribeAvailabilityZones",
            "Resource": "*"
        }
    ]
}
EOF
aws iam put-role-policy --role-name AWSControlTowerAdmin --policy-name
 AWSControlTowerAdminPolicy --policy-document file://ct_admin_role_policy.json
aws iam attach-role-policy --role-name AWSControlTowerAdmin --policy-arn
 arn:aws:iam::aws:policy/service-role/AWSControlTowerServiceRolePolicy
```

AWSControlTowerCloudTrailRole

```
cat <<EOF >controltower_trust.json
        {
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "Service": "cloudtrail.amazonaws.com"
            },
            "Action": "sts:AssumeRole"
        }
    ]
}
EOF
aws iam create-role --role-name AWSControlTowerCloudTrailRole --path /service-role/ --
assume-role-policy-document file://cloudtrail_trust.json
cat <<EOF >cloudtrail_role_policy.json
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": "logs:CreateLogStream",
            "Resource": "arn:aws:logs:*:*:log-group:aws-controltower/CloudTrailLogs:*",
            "Effect": "Allow"
        },
        {
            "Action": "logs:PutLogEvents",
            "Resource": "arn:aws:logs:*:*:log-group:aws-controltower/CloudTrailLogs:*",
            "Effect": "Allow"
        }
    ]
}
EOF
aws iam put-role-policy --role-name AWSControlTowerCloudTrailRole --
policy-name AWSControlTowerCloudTrailRolePolicy --policy-document file://
cloudtrail_role_policy.json
```

AWSControlTowerStackSetRole

```
cat <<EOF >cloudformation_trust.json
{
```

```
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "Service": "cloudformation.amazonaws.com"
            },
            "Action": "sts:AssumeRole"
        }
    ]
}
EOF
aws iam create-role --role-name AWSControlTowerStackSetRole --path /service-role/ --
assume-role-policy-document file://cloudformation_trust.json
cat <<EOF >stackset_role_policy.json
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": [
                "sts:AssumeRole"
            ],
            "Resource": [
                "arn:aws:iam::*:role/AWSControlTowerExecution"
            ],
            "Effect": "Allow"
        }
    ]
}
EOF
aws iam put-role-policy --role-name AWSControlTowerStackSetRole --policy-name
 AWSControlTowerStackSetRolePolicy --policy-document file://stackset_role_policy.json
```

AWSControlTowerConfigAggregatorRoleForOrganizations

```
cat <<EOF >config_trust.json
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "Service": "config.amazonaws.com"
```

```
            },
            "Action": "sts:AssumeRole"
        }
    ]
}
EOF
aws iam create-role --role-name AWSControlTowerConfigAggregatorRoleForOrganizations --
path /service-role/ --assume-role-policy-document file://config_trust.json
aws iam attach-role-policy --role-name
 AWSControlTowerConfigAggregatorRoleForOrganizations --policy-arn
 arn:aws:iam::aws:policy/service-role/AWSConfigRoleForOrganizations
```

단계 3. 계정 ID를 얻고 landing Zone 매니페스트 파일을 생성합니다.

다음 예제의 처음 두 명령은 1단계에서 만든 계정의 계정 ID를 변수에 저장합니다. 그러면 이 변수들이 landing zone 매니페스트 파일을 생성하는 데 도움이 됩니다.

```
sec_account_id=$(aws organizations list-accounts | jq -r '.Accounts[] | select(.Name ==
 "Audit account") | .Id')
log_account_id=$(aws organizations list-accounts | jq -r '.Accounts[] | select(.Name ==
 "Log archive account") | .Id')

cat <<EOF >landing_zone_manifest.json
{
   "governedRegions": ["us-west-1", "us-west-2"],
   "organizationStructure": {
       "security": {
           "name": "Security"
       },
       "sandbox": {
           "name": "Sandbox"
       }
   },
   "centralizedLogging": {
        "accountId": "$log_account_id",
        "configurations": {
            "loggingBucket": {
                "retentionDays": 60
            },
            "accessLoggingBucket": {
                "retentionDays": 60
            }
        },
```

```
        "enabled": true
    },
    "securityRoles": {
        "accountId": "$sec_account_id"
    },
    "accessManagement": {
        "enabled": true
    }
}
EOF
```

단계 4. 최신 버전으로 랜딩 존을 생성하십시오.

매니페스트 파일과 최신 버전으로 랜딩 존을 설정해야 합니다. 이 예제는 버전 3.3을 보여줍니다.

```
aws --region us-west-1 controltower create-landing-zone --manifest file://
landing_zone_manifest.json --landing-zone-version 3.3
```

출력에는 다음 예제와 같이 arn과 작업 식별자가 포함됩니다.

```
{
    "arn": "arn:aws:controltower:us-west-1:0123456789012:landingzone/4B3H0ULNUOL2AXXX",
    "operationIdentifier": "16bb47f7-b7a2-4d90-bc71-7df4ca1201xx"
}
```

단계 5. (선택 사항) landing Zone 생성 작업의 상태를 추적할 수 있습니다.

상태를 추적하려면 이전 `create-landing-zone` 명령 출력의 OperationIdentifier를 사용하십시오.

```
aws --region us-west-1 controltower get-landing-zone-operation --operation-identifier
 16bb47f7-b7a2-4d90-bc71-7df4ca1201xx
```

샘플 상태 출력:

```
{
    "operationDetails": {
        "operationType": "CREATE",
        "startTime": "2024-02-28T21:49:31Z",
        "status": "IN_PROGRESS"
    }
}
```

다음 예제 스크립트를 사용하면 로그 파일처럼 작업 상태를 반복해서 보고하는 루프를 설정할 수 있습니다. 그러면 명령을 계속 입력할 필요가 없습니다.

```
while true; do echo "$(date) $(aws --region us-west-1 controltower get-landing-
zone-operation --operation-identifier 16bb47f7-b7a2-4d90-bc71-7df4ca1201xx | jq -
r .operationDetails.status)"; sleep 15; done
```

착륙 지대에 대한 자세한 정보를 표시하려면

단계 1. 랜딩 존의 ARN 찾기

```
aws --region us-west-1 controltower list-landing-zones
```

출력에는 다음 출력 예와 같이 착륙 지대의 식별자가 포함됩니다.

```
{
    "landingZones": [
        {
            "arn": "arn:aws:controltower:us-
west-1:123456789012:landingzone/4B3H0ULNUOL2AXXX"
        }
    ]
}
```

단계 2. 정보 가져오기

```
aws --region us-west-1 controltower get-landing-zone --landing-zone-identifier
 arn:aws:controltower:us-west-1:123456789012:landingzone/4B3H0ULNUOL2AXXX
```

다음은 표시될 수 있는 출력 유형의 예시입니다.

```
{
    "landingZone": {
        "arn": "arn:aws:controltower:us-
west-1:123456789012:landingzone/4B3H0ULNUOL2AXXX",
        "driftStatus": {
            "status": "IN_SYNC"
        },
        "latestAvailableVersion": "3.3",
        "manifest": {
```

```
            "accessManagement": {
                "enabled": true
            },
            "securityRoles": {
                "accountId": "9750XXXX4444"
            },
            "governedRegions": [
                "us-west-1",
                "us-west-2"
            ],
            "organizationStructure": {
                "sandbox": {
                    "name": "Sandbox"
                },
                "security": {
                    "name": "Security"
                }
            },
            "centralizedLogging": {
                "accountId": "012345678901",
                "configurations": {
                    "loggingBucket": {
                        "retentionDays": 60
                    },
                    "accessLoggingBucket": {
                        "retentionDays": 60
                    }
                },
                "enabled": true
            }
        },
        "status": "ACTIVE",
        "version": "3.3"
    }
}
```

를 사용하여 랜딩 존 시작하기 AWS CloudFormation

AWS CloudFormation 콘솔이나 를 통해 랜딩 존을 구성하고 시작할 수 AWS CLI있습니다. AWS CloudFormation 이 섹션에서는 API를 사용하여 landing Zone을 시작하는 지침과 예제를 제공합니다. AWS CloudFormation

주제

- 다음을 사용하여 랜딩 존을 시작하기 위한 전제 조건 AWS CloudFormation
- 를 사용하여 새 랜딩 존 생성 AWS CloudFormation
- 를 사용하여 기존 Landding Zone을 관리합니다. AWS CloudFormation

다음을 사용하여 랜딩 존을 시작하기 위한 전제 조건 AWS CloudFormation

1. 에서 AWS CLI AWS Organizations `CreateOrganization` API를 사용하여 조직을 만들고 모든 기능을 활성화합니다.

   자세한 지침은 1단계: 랜딩 존 구성 검토하세요.

2. AWS CloudFormation 콘솔에서 또는 를 AWS CLI사용하여 관리 계정에 다음 리소스를 생성하는 AWS CloudFormation 템플릿을 배포하십시오.
   - 로그 아카이브 계정 (“로깅” 계정이라고도 함)
   - 감사 계정 (“보안” 계정이라고도 함)
   - AWSControlTowerAdmin, AWSControlTowerCloudTrailRoleAWSControlTowerConfigAggregatorRoleForOrganizations, 및 AWSControlTowerStackSetRole서비스 역할.

     AWS Control Tower가 이러한 역할을 사용하여 랜딩 존 API 호출을 수행하는 방법에 대한 자세한 내용은 1단계: 랜딩 존 구성을 참조하십시오.

```
Parameters:
  LoggingAccountEmail:
    Type: String
    Description: The email Id for centralized logging account
  LoggingAccountName:
    Type: String
    Description: Name for centralized logging account
  SecurityAccountEmail:
    Type: String
    Description: The email Id for security roles account
  SecurityAccountName:
    Type: String
    Description: Name for security roles account
Resources:
  MyOrganization:
    Type: 'AWS::Organizations::Organization'
    Properties:
      FeatureSet: ALL
```

```
  LoggingAccount:
    Type: 'AWS::Organizations::Account'
    Properties:
      AccountName: !Ref LoggingAccountName
      Email: !Ref LoggingAccountEmail
  SecurityAccount:
    Type: 'AWS::Organizations::Account'
    Properties:
      AccountName: !Ref SecurityAccountName
      Email: !Ref SecurityAccountEmail
  AWSControlTowerAdmin:
    Type: 'AWS::IAM::Role'
    Properties:
      RoleName: AWSControlTowerAdmin
      AssumeRolePolicyDocument:
        Version: 2012-10-17
        Statement:
          - Effect: Allow
            Principal:
              Service: controltower.amazonaws.com
            Action: 'sts:AssumeRole'
      Path: '/service-role/'
      ManagedPolicyArns:
        - !Sub >-
          arn:${AWS::Partition}:iam::aws:policy/service-role/
AWSControlTowerServiceRolePolicy
  AWSControlTowerAdminPolicy:
    Type: 'AWS::IAM::Policy'
    Properties:
      PolicyName: AWSControlTowerAdminPolicy
      PolicyDocument:
        Version: 2012-10-17
        Statement:
          - Effect: Allow
            Action: 'ec2:DescribeAvailabilityZones'
            Resource: '*'
      Roles:
        - !Ref AWSControlTowerAdmin
  AWSControlTowerCloudTrailRole:
    Type: 'AWS::IAM::Role'
    Properties:
      RoleName: AWSControlTowerCloudTrailRole
      AssumeRolePolicyDocument:
        Version: 2012-10-17
```

```
        Statement:
          - Effect: Allow
            Principal:
              Service: cloudtrail.amazonaws.com
            Action: 'sts:AssumeRole'
      Path: '/service-role/'
  AWSControlTowerCloudTrailRolePolicy:
    Type: 'AWS::IAM::Policy'
    Properties:
      PolicyName: AWSControlTowerCloudTrailRolePolicy
      PolicyDocument:
        Version: 2012-10-17
        Statement:
          - Action:
              - 'logs:CreateLogStream'
              - 'logs:PutLogEvents'
            Resource: !Sub >-
              arn:${AWS::Partition}:logs:*:*:log-group:aws-controltower/
CloudTrailLogs:*
            Effect: Allow
      Roles:
        - !Ref AWSControlTowerCloudTrailRole
  AWSControlTowerConfigAggregatorRoleForOrganizations:
    Type: 'AWS::IAM::Role'
    Properties:
      RoleName: AWSControlTowerConfigAggregatorRoleForOrganizations
      AssumeRolePolicyDocument:
        Version: 2012-10-17
        Statement:
          - Effect: Allow
            Principal:
              Service: config.amazonaws.com
            Action: 'sts:AssumeRole'
      Path: '/service-role/'
      ManagedPolicyArns:
        - !Sub arn:${AWS::Partition}:iam::aws:policy/service-role/
AWSConfigRoleForOrganizations
  AWSControlTowerStackSetRole:
    Type: 'AWS::IAM::Role'
    Properties:
      RoleName: AWSControlTowerStackSetRole
      AssumeRolePolicyDocument:
        Version: 2012-10-17
        Statement:
```

```
          - Effect: Allow
            Principal:
              Service: cloudformation.amazonaws.com
            Action: 'sts:AssumeRole'
      Path: '/service-role/'
  AWSControlTowerStackSetRolePolicy:
    Type: 'AWS::IAM::Policy'
    Properties:
      PolicyName: AWSControlTowerStackSetRolePolicy
      PolicyDocument:
        Version: 2012-10-17
        Statement:
          - Action: 'sts:AssumeRole'
            Resource: !Sub 'arn:${AWS::Partition}:iam::*:role/
AWSControlTowerExecution'
            Effect: Allow
      Roles:
        - !Ref AWSControlTowerStackSetRole

Outputs:
  LogAccountId:
    Value:
      Fn::GetAtt: LoggingAccount.AccountId
    Export:
      Name: LogAccountId
  SecurityAccountId:
    Value:
      Fn::GetAtt: SecurityAccount.AccountId
    Export:
      Name: SecurityAccountId
```

를 사용하여 새 랜딩 존 생성 AWS CloudFormation

AWS CloudFormation 콘솔에서 또는 를 사용하여 다음 AWS CLI AWS CloudFormation 템플릿을 배포하여 landing Zone을 생성합니다.

```
Parameters:
  Version:
    Type: String
    Description: The version number of Landing Zone
  GovernedRegions:
    Type: List
```

```
    Description: List of governed regions
  SecurityOuName:
    Type: String
    Description: The security Organizational Unit name
  SandboxOuName:
    Type: String
    Description: The sandbox Organizational Unit name
  CentralizedLoggingAccountId:
    Type: String
    Description: The AWS account ID for centralized logging
  SecurityAccountId:
    Type: String
    Description: The AWS account ID for security roles
  LoggingBucketRetentionPeriod:
    Type: Number
    Description: Retention period for centralized logging bucket
  AccessLoggingBucketRetentionPeriod:
    Type: Number
    Description: Retention period for access logging bucket
  KMSKey:
    Type: String
    Description: KMS key ARN used by CloudTrail and Config service to encrypt data in
 logging bucket
Resources:
  MyLandingZone:
    Type: 'AWS::ControlTower::LandingZone'
    Properties:
      Version:
        Ref: Version
      Tags:
        - Key: "keyname1"
          Value: "value1"
        - Key: "keyname2"
          Value: "value2"
      Manifest:
        governedRegions:
          Ref: GovernedRegions
        organizationStructure:
          security:
            name:
              Ref: SecurityOuName
          sandbox:
            name:
              Ref: SandboxOuName
```

```
        centralizedLogging:
          accountId:
            Ref: CentralizedLoggingAccountId
          configurations:
            loggingBucket:
              retentionDays:
                Ref: LoggingBucketRetentionPeriod
            accessLoggingBucket:
              retentionDays:
                Ref: AccessLoggingBucketRetentionPeriod
            kmsKeyArn:
              Ref: KMSKey
          enabled: true
        securityRoles:
          accountId:
            Ref: SecurityAccountId
        accessManagement:
          enabled: true
```

를 사용하여 기존 Landding Zone을 관리합니다. AWS CloudFormation

새 스택이나 기존 AWS CloudFormation 스택에서 랜딩 존을 가져와서 이미 시작한 랜딩 존을 관리하는 AWS CloudFormation 데 사용할 수 있습니다. 세부 정보 및 지침은 기존 리소스를 CloudFormation 경영진으로 가져오는 것을 검토하세요.

랜딩 존 내의 드리프트를 감지하고 해결하려면 AWS Control Tower 콘솔 AWS CLI, 또는 `ResetLandingZoneAPI`를 사용할 수 있습니다.

다음 단계

이제 Landing Zone이 설정되었으므로 사용할 준비가 되었습니다.

AWS Control Tower를 사용하는 방법에 대해 자세히 알아보려면 다음 주제를 참조하십시오.

- 권장되는 관리 방법은 모범 사례를 참조하십시오.
- IAM Identity Center 사용자 및 그룹을 특정 역할과 권한으로 설정할 수 있습니다. 권장 사항은 그룹, 역할, 정책 설정을 위한 권장 사항 단원을 참조하십시오.
- AWS Organizations 배포에서 조직 및 계정 등록을 시작하려면 기존 조직 및 계정 관리를 참조하십시오.
- 최종 사용자는 Account Factory를 사용하여 랜딩 존에서 자신의 AWS 계정을 프로비저닝할 수 있습니다. 자세한 설명은 계정 구성 및 프로비저닝을 위한 권한 섹션을 참조하세요.

- 이를 보장하기 AWS Control Tower의 규정 준수 검증 위해 중앙 클라우드 관리자는 Log Archive 계정의 로그 아카이브를 검토하고 지정된 타사 감사자는 보안 OU의 구성원인 감사 (공유) 계정의 감사 정보를 검토할 수 있습니다.
- AWS Control Tower의 기능에 대해 자세히 알아보려면 관련 정보를 참조하십시오.
- AWS Control Tower 기능을 사용하는 방법을 자세히 설명하는 엄선된 YouTube 동영상 목록을 방문해 보십시오.
- 최신 백엔드 업데이트, 최신 제어 기능을 사용하고 랜딩 존을 유지하기 위해 때때로 랜딩 up-to-date 존을 업데이트해야 할 수 있습니다. 자세한 설명은 AWS Control Tower에서의 구성 업데이트 관리 섹션을 참조하세요.
- AWS Control Tower를 사용하는 동안 문제가 발생하는 경우 을 참조하십시오문제 해결.

> **Important**
>
> 계정의 루트 사용자에 대해 아직 MFA를 활성화하지 않았다면 지금 활성화하십시오. 루트 사용자의 모범 사례에 대한 자세한 내용은 계정의 루트 사용자를 보호하기 위한 모범 사례를 참조하십시오.

AWS Control Tower의 한도 및 할당량

이 장에서는 AWS Control Tower를 사용할 때 염두에 두어야 하는 AWS 서비스 제한 및 할당량에 대해 다룹니다. 서비스 쿼터 문제로 인해 landing Zone을 설정할 수 없는 경우 문의하세요 AWS Support.

제어와 관련된 제한에 대한 자세한 내용은 을 참조하십시오관리 제한.

> **새 제어 참조 가이드**
>
> AWS Control Tower 규제 항목에 대한 정보는 AWS Control Tower 규제 참조 안내서로 이동되었습니다.

AWS Control Tower의 한계

이 섹션에서는 AWS Control Tower의 알려진 제한 사항 및 지원되지 않는 사용 사례를 설명합니다.

- AWS Control Tower에는 전반적인 동시성 제한이 있습니다. 일반적으로 한 번에 하나의 작업이 허용됩니다. 이 제한에는 다음과 같은 두 가지 예외가 허용됩니다.
  - 선택적 컨트롤은 비동기 프로세스를 통해 동시에 활성화 및 비활성화할 수 있습니다. 콘솔에서 호출하든 API에서 호출하든 관계없이 제어 관련 작업을 한 번에 최대 100개까지 진행할 수 있습니다. 이러한 100개의 작업 중 한 번에 최대 20개까지 사전 제어 작업이 될 수 있습니다.
  - 비동기 프로세스를 통해 Account Factory에서 동시에 계정을 프로비저닝, 업데이트 및 등록할 수 있으며, 계정 관련 작업은 최대 다섯 (5) 개까지 동시에 진행됩니다. 계정 관리를 취소하는 작업은 한 번에 한 계정씩 수행해야 합니다.
- 보안 OU에 있는 공유 계정의 이메일 주소는 변경할 수 있지만, AWS Control Tower 콘솔에서 이러한 변경 사항을 확인하려면 랜딩 존을 업데이트해야 합니다.
- AWS Control Tower 랜딩 존에 있는 OU에는 OU당 5개의 SCP 제한이 적용됩니다.
- AWS Control Tower는 랜딩 존 조직 내에서 모든 OU에 나누어 최대 10,000개의 계정을 지원합니다.
- 300개 이상의 직접 중첩 계정을 보유한 기존 OU는 AWS Control Tower에 등록하거나 재등록할 수 없습니다. OU 등록 제한에 대한 자세한 내용은 을 참조하십시오. 지역 및 스택 세트 제한
- 다음은 AWS 리전일부 종속성을 사용할 수 없기 때문에 AWS Control Tower (cFCT) 에 대한 사용자 지정을 사용할 수 없습니다.
  - 아시아 태평양 (자카르타 및 오사카)
  - 이스라엘(텔아비브)

  - 중동(UAE)
  - 유럽(스페인)
  - 아시아 태평양(하이데라바드)
  - 유럽(취리히)
  - 캐나다 서부(캘거리)

  cFCT를 AWS Control Tower 홈 지역에 배포하는 경우 cFCT를 사용하여 이러한 지역에 리소스를 배포하고 관리할 수 있지만, 이러한 지역에는 CFCT를 구축할 수 없습니다.
- 다음 AWS 리전버전에서는 AWS Control Tower Account Factory for Terraform (AFT) 을 사용할 수 없습니다. 일부 종속성을 사용할 수 없기 때문입니다.
  - 이스라엘(텔아비브)
  - 중동(UAE)
  - 유럽(스페인)
  - 아시아 태평양(하이데라바드)
  - 유럽(취리히)
  - 캐나다 서부(캘거리)
- 다음 지역은 IAM ID 센터를 지원하지 않습니다.
  - 중동 (UAE) 지역, me-central-1
  - 아시아 태평양 (하이데라바드) 지역, ap-south-2
  - 캐나다 서부 (캘거리), ca-west-1

  IAM ID 센터에 대한 자세한 내용 AWS 리전 및 지원은 Identity 및 Access Management 사용 설명서의 지역 및 엔드포인트를 참조하십시오.AWS
- 다음 지역은 지원하지 않습니다. AWS Service Catalog
  - 캐나다 서부 (캘거리), ca-west-1

  지원하지 AWS Service Catalog않는 지역의 AWS Control Tower 기능에 대한 자세한 내용은 을 참조하십시오AWS Control Tower는 AWS 캐나다 서부 (캘거리) 에서 사용 가능.
- 제어 API를 호출하여 컨트롤을 활성화하거나 비활성화하는 경우, AWS Control Tower의 동시 작업 수 `EnableControl` 및 `DisableControl` 업데이트는 100개의 동시 작업으로 제한됩니다. 10개의 작업 (10개) 을 동시에 진행하고 나머지 작업은 대기열에 둘 수 있습니다. 완료될 때까지 기다리려면 코드를 조정해야 할 수도 있습니다.

- 전체 한도인 100회의 제어 작업 내에서 한 번에 최대 20개의 작업이 사전 제어 작업이 될 수 있습니다.
- Terraform을 기반으로 하는 블루프린트를 사용하여 AFC (Account Factory Cutomations) 를 통해 계정을 프로비저닝하면 해당 블루프린트를 하나에만 배포할 수 있습니다. AWS 리전기본적으로 AWS Control Tower는 홈 지역에 배포합니다.

할당량 증가 요청

Service Quotas 콘솔은 AWS Control Tower 할당량에 대한 정보를 제공합니다. Service Quotas 콘솔을 사용하면 기본 서비스 할당량을 확인하고 조정 가능한 할당량에 대한 할당량 증가를 요청할 수 있습니다.

Service Quotas 콘솔을 통해 다음 할당량을 확인할 수 있습니다.

- 동시 계정 작업 할당량: 동시에 수행할 수 있는 최대 동시 계정 작업 수입니다. 기본값: 5, 최대: 10, 조정 가능
- 단일 OU의 계정 수: OU 하나에 존재할 수 있는 AWS Control Tower 관리 계정의 최대 수입니다. 이 한도를 초과하여 계정을 추가하면 AWS Control Tower에서의 OU 등록 프로세스를 수행할 수 없습니다. OU당 계정 수에 대한 자세한 내용은 AWS Control Tower 설명서를 참조하십시오. 지역 및 스택 세트 제한 기본값: 300, 조정 불가.
- 조직 단위 (OU) 의 동시 작업: 동시에 수행할 수 있는 OU 관련 동시 작업의 최대 수입니다. 기본값: 1, 조정 불가.

예를 들어, 최대 10개의 동시 계정 관련 작업 중 5개에서 할당량 증가를 요청할 수 있습니다. 일부 AWS Control Tower 성능 특성은 할당량 증가 후에 변경될 수 있습니다. 예를 들어 OU에 계정이 더 많으면 OU를 업데이트하는 데 시간이 더 오래 걸릴 수 있습니다. 또는 SCP가 5개인 OU에서 작업을 완료하는 데 SCP가 3개인 경우보다 시간이 더 오래 걸릴 수 있습니다.

> **Note**
>
> 서비스 할당량 증가 요청은 효력이 발생하기까지 최대 2일이 소요될 수 있습니다. AWS Control Tower 홈 리전에 할당량 증가를 요청해야 합니다.

또는 AWS Support에 문의하여 AWS Control Tower의 일부 리소스에 대한 할당량 증가를 요청할 수 있습니다. 또는 다음 동영상을 보고 특정 서비스 할당량 증가를 자동화하는 방법을 배울 수 있습니다.

동영상: AWS Control Tower와 관련된 서비스의 서비스 할당량 증가 요청 자동화

이 동영상 (7:24) 은 AWS Control Tower에서의 배포를 기반으로 관련 통합 AWS 서비스의 서비스 할당량 증가를 자동화하는 방법을 설명합니다. 또한 조직의 AWS Enterprise Support에 새 계정을 자동으로 등록하는 방법도 보여줍니다. 동영상 오른쪽 하단에 있는 아이콘을 선택하여 전체 화면으로 확대하면 더 잘 보입니다. 자막을 사용할 수 있습니다.

AWS Control Tower의 할당량 증가에 대한 동영상 안내.

이 환경에서 새 계정을 프로비저닝할 때 수명 주기 이벤트를 사용하여 지정된 서비스 할당량 증가에 대한 자동 요청을 트리거할 수 있습니다. AWS 리전

AWS 할당량에 대한 자세한 내용은 일반 참조에서 확인할 수 있습니다.AWS

관리 제한

> **새로운 컨트롤 레퍼런스 가이드**
>
> AWS Control Tower 규제 항목에 대한 정보는 AWS Control Tower 규제 참조 안내서로 이동되었습니다.

SCP와 같은 AWS Control Tower 리소스를 수정하거나 Config 레코더 또는 애그리게이터와 같은 AWS Config 리소스를 제거하는 경우, AWS Control Tower는 더 이상 제어가 설계된 대로 작동한다고 보장할 수 없습니다. 따라서 다중 계정 환경의 보안이 손상될 수 있습니다. 보안의 AWS 공동 책임 모델은 사용자가 변경할 수 있는 모든 사항에 적용됩니다.

> **Note**
>
> AWS Control Tower는 랜딩 존을 업데이트할 때 컨트롤의 SCP를 표준 구성으로 재설정하여 환경의 무결성을 유지하는 데 도움이 됩니다. SCP에 적용한 변경 사항은 설계상 표준 버전의 제어로 대체됩니다.

AWS Control Tower의 일부 제어 기능은 AWS Control Tower가 제공되는 특정 AWS 리전 지역에서 작동하지 않습니다. 이는 해당 지역이 필수 기본 기능을 지원하지 않기 때문입니다. 이 제한은 Security Hub Service에서 관리하는 표준: AWS Control Tower의 특정 탐지 제어, 사전 예방 제어 및 특정 제어 항목에 영향을 미칩니다. 지역별 가용성에 대한 자세한 내용은 지역 서비스 목록 설명서 및 Security Hub 제어 참조 설명서를 참조하십시오.

복합 거버넌스의 경우 제어 동작도 제한됩니다. 자세한 정보는 지역을 구성할 때 복합 거버넌스를 피하세요.을 참조하세요.

AWS Control Tower가 지역 및 규제 항목의 제한을 관리하는 방법에 대한 자세한 내용은 을 참조하십시오옵트인 지역 활성화 AWS 고려 사항.

AWS Control Tower 콘솔에서 각 컨트롤의 지역을 확인할 수 있습니다.

다음 AWS 지역은 Security Hub 서비스 관리형 표준에 속하는 규제 항목을 지원하지 않습니다: AWS Control Tower.

- 아시아 태평양 (홍콩) 지역, ap-east-1
- 아시아 태평양 (자카르타) 지역, ap-southeast-3
- 아시아 태평양 (오사카) 지역, ap-northeast-3
- 유럽 (밀라노) 지역, eu-south-1
- 아프리카 (케이프타운) 지역, af-south-1
- 중동 (바레인) 지역, me-south-1
- 이스라엘 (텔아비브), il-central-1
- 중동 (UAE) 지역, me-central-1
- 유럽 (스페인) 지역, eu-south-2
- 아시아 태평양 (하이데라바드) 지역, ap-south-2
- 유럽 (취리히) 지역, eu-central-2
- 아시아 태평양 (멜버른) 지역, ap-southeast-4
- 캐나다 서부 (캘거리), ca-west-1

다음은 AWS 리전 사전 통제를 지원하지 않습니다.

- 캐나다 서부(캘거리)

다음 표에는 특정 지역에서 지원되지 않는 사전 예방적 제어가 나와 있습니다. AWS 리전

컨트롤 식별자	지원되지 않는 지역
CT.REDSHIFT.PR.5	ap-southeast-4, ap-south-2, ap-southeast-3, eu-central-2, eu-south-2, il-central-1, me-central-1, me-central-1
CT.DAX.PR.2	us-west-1
CT.GLUE.PR.2	지원되지 않음

다음 표는 특정 AWS 리전지역에서 지원되지 않는 AWS Control Tower 탐지 제어를 보여줍니다.

컨트롤 식별자	지원되지 않는 지역
AWS-GR_AUTOSCALING_LAUNCH_CONFIG_PUBLIC_IP_DISABLED	ap-northeast-3, ap-southeast-3, il-central-1, ap-southeast-4, ca-west-1
AWS-GR_LAMBDA_FUNCTION_PUBLIC_ACCESS_PROHIBITED	eu-south-2
AWS-GR_EMR_MASTER_NO_PUBLIC_IP	ap-northeast-3, ap-southeast-3, af-south-1, eu-south-1, eu-south-1, il-central-1, me-central-1, eu-south-2, ap-south-2, eu-south-2, eu-central-2, eu-central-2 2, ap-southeast-4, ca-west-1
AWS-GR_EBS_SNAPSHOT_PUBLIC_RESTORABLE_CHECK	eu-south-2
AWS-GR_NO_UNRESTRICTED_ROUTE_TO_IGW	ap-northeast-3, ap-southeast-3, ap-south-2, eu-south-2, ca-west-1
AWS-GR_SAGEMAKER_NOTEBOOK_NO_DIRECT_INTERNET_ACCESS	ap-northeast-3, ap-southeast-3, af-south-1, eu-south-1, eu-south-1, il-central-1, me-central-1, eu-south-2, ap-south-2, eu-south-2, eu-central-2, eu-central-2 2, ap-southeast-4, ca-west-1
AWS-GR_EC2_INSTANCE_NO_PUBLIC_IP	ap-northeast-3

컨트롤 식별자	지원되지 않는 지역
AWS-GR_EKS_ENDPOINT_NO_PUBLIC_ACCESS	ap-northeast-3, ap-southeast-3, af-south-1, eu-south-1, us-west-1, il-central-1, me-central-1, me-central-1, eu-south-2, ap-south-2, eu-central-2, ap-southeast-4, ca-west-1
AWS-GR_ELASTICSEARCH_IN_VPC_ONLY	ap-southeast-3, il-central-1, eu-south-2, ap-south-2, ap-south-2, eu-central-2, ap-southeast-4, ca-west-1
AWS-GR_RESTRICTED_SSH	af-south-1, ap-northeast-3, ap-south-2, ap-southeast-3, ap-southeast-3, ap-southeast-4, eu-central-2, eu-south-1, eu-south-2, il-central-2, il-central-2, il-central-2, il-entral-2 il-central-1, me-central-1
AWS-GR_DMS_REPLICATION_NOT_PUBLIC	af-south-1, ap-south-2, ap-southeast-3, ap-southeast-4, eu-central-2, eu-south-1, eu-south-2, il-central-1, il-central-1, me-central-1 1, ca-west-1
AWS-GR_RDS_SNAPSHOTS_PUBLIC_PROHIBITED	af-south-1, ap-southeast-4, eu-central-2, eu-south-1, eu-south-2, il-central-1
AWS-GR_SUBNET_AUTO_ASSIGN_PUBLIC_IP_DISABLED	ap-northeast-3
AWS-GR_ENCRYPTED_VOLUMES	af-south-1, ap-northeast-3, eu-south-1, il-central-1
AWS-GR_RESTRICTED_COMMON_PORTS	af-south-1, ap-northeast-3, eu-central-2, eu-south-1, eu-south-2, il-central-1, me-central-1, me-central-1
AWS-GR_IAM_USER_MFA_ENABLED	il-central-1, me-central-1, eu-south-2, ap-south-2, ap-south-2, eu-central-2, ap-southeast-4, ca-west-1

컨트롤 식별자	지원되지 않는 지역
AWS-GR_MFA_ENABLED_FOR_IAM_CONSOLE_ACCESS	il-central-1, me-central-1, eu-south-2, ap-south-2, ap-south-2, eu-central-2, ap-southeast-4, ca-west-1
AWS-GR_SSM_DOCUMENT_NOT_PUBLIC	il-central-1, ca-west-1
AWS-GR_ROOT_ACCOUNT_MFA_ENABLED	il-central-1, me-central-1, ca-west-1
AWS-GR_S3_ACCOUNT_LEVEL_PUBLIC_ACCESS_BLOCKS_PERIODIC	il-central-1, eu-south-2, eu-central-2
AWS-GR_RDS_STORAGE_ENCRYPTED	eu-central-2, eu-south-2
AWS-GR_RDS_INSTANCE_PUBLIC_ACCESS_CHECK	ap-south-2, eu-south-2
AWS-GR_REDSHIFT_CLUSTER_PUBLIC_ACCESS_CHECK	ap-south-2, ap-southeast-3, eu-south-2, ca-west-1
AWS-GR_EC2_VOLUME_INUSE_CHECK	ca-west-1
AWS-GR_EBS_OPTIMIZED_INSTANCE	ca-west-1

지역 및 스택 세트 제한

많은 수의 계정을 보유한 OU로 거버넌스를 확장하려는 경우 AWS CloudFormation 스택 세트로 인해 조직의 전체 규모가 제한될 수 있습니다. AWS 리전다음 공식을 사용하여 한도를 추정할 수 있습니다.

조직의 관리 계정 수 x 관리 지역 수 150,000 미만

일반적으로 OU로 거버넌스를 확장할 때 지원되는 계정 수는 관리되는 지역의 수에 따라 줄어들 것으로 예상됩니다.

거버넌스를 OU로 확장할 때 AWS Control Tower를 사용할 수 있는 지역이 15개 이상 활성화되면 이러한 제한이 명확해집니다. 조직 단위 (OU) 당 계정 수의 상한이 축소되었습니다.

예를 들어 22개 지역을 활성화한 경우 OU당 계정 수는 300개가 아닌 220개로 제한됩니다. 계정이 220개가 넘는 OU로 거버넌스를 확장해야 하는 경우 활성화된 지역 수를 줄여야 합니다. 이러한 감소는 스택 세트 제한 때문입니다.

가이드라인:

- 15개 활성화 지역에서 최대 300개 계정의 OU가 지원됩니다.
- 22개 활성화 지역에서는 최대 220개 계정의 OU가 지원됩니다.
- 활성화된 지역이 16~21개인 경우 지원되는 최대 OU 크기는 계정 220-300개 범위입니다.
- 23개 이상의 활성화 지역에서 지원되는 최대 OU 크기는 계정 220개 미만입니다.

AWS Control Tower 기능의 지역별 차이

AWS Control Tower는 다른 AWS 서비스의 동작을 조정하기 때문에 AWS Control Tower의 동작에는 몇 가지 차이점이 있습니다. AWS 리전예:

- AWS Service Catalog AWS Control Tower를 사용할 수 AWS 리전 있는 모든 지역에서 사용할 수 있는 것은 아니며, 이로 인해 해당 지역의 Account Factory의 동작이 변경됩니다.
- Service Catalog가 블루프린트의 기본 기능을 지원하는 데 사용할 수 없기 때문에 특정 지역에서는 AFC (Account Factory Custations) 를 사용할 수 없습니다.
- 기본 기능이 AWS 리전 부족하여 일부 컨트롤을 모두 사용할 수 있는 것은 아닙니다.
- 기본 기능이 부족하여 AFT와 cFCt를 모두 AWS 리전 사용할 수 있는 것은 아닙니다.

AWS Control Tower 환경의 행동을 가장 잘 판단하려면 거주 지역을 확인하십시오. 그런 다음 다음 항목을 평가하십시오. 자세한 내용은 AWS Control Tower의 제한 및 할당량을 참조하십시오.

- 원하는 홈 리전에서 AWS Service Catalog 사용할 수 있습니까?
- 필요한 제어 기능을 사용할 수 있습니까? 제어 제한을 참조하십시오.
- 원하는 홈 지역에서 IAM ID 센터를 사용할 수 있습니까?

신규: AWS Control Tower 제어 참조 가이드

AWS Control Tower의 규제 항목에 대한 정보는 새 안내서인 AWS Control Tower 규제 참조 안내서로 이동했습니다.

AWS Control Tower 관리자를 위한 모범 사례

이 항목은 주로 관리 계정 관리자를 대상으로 합니다.

관리 계정 관리자는 AWS Control Tower 규제 때문에 회원 계정 관리자가 수행할 수 없는 일부 작업을 설명할 책임이 있습니다. 이 주제에서는 이러한 지식을 이전하기 위한 몇 가지 모범 사례와 절차를 설명하고, AWS Control Tower 환경을 효율적으로 설정하고 유지 관리하기 위한 기타 팁을 제공합니다.

사용자 액세스 설명

AWS Control Tower 콘솔은 관리 계정 관리자 권한을 가진 사용자만 사용할 수 있습니다. 이러한 사용자만 landing Zone 내에서 관리 작업을 수행할 수 있습니다. 모범 사례에 따르면 대부분의 사용자 및 회원 계정 관리자는 AWS Control Tower 콘솔을 전혀 보지 못할 것입니다. 관리 계정 관리자 그룹의 일원으로서 회원 계정의 사용자와 관리자에게 다음 정보를 적절하게 설명하는 것은 귀하의 책임입니다.

- 사용자 및 관리자가 landing zone 내에서 액세스할 수 있는 AWS 리소스에 대해 설명하십시오.
- 다른 관리자가 그에 따라 AWS 워크로드를 계획하고 실행할 수 있도록 각 OU (조직 구성 단위) 에 적용되는 예방 제어를 나열하세요.

리소스 액세스 설명

일부 관리자 및 기타 사용자에게는 랜딩 존 내에서 액세스할 수 있는 AWS 리소스에 대한 설명이 필요할 수 있습니다. 이 액세스에는 프로그래밍 방식 액세스와 콘솔 기반 액세스가 포함될 수 있습니다. 일반적으로 AWS 리소스에 대한 읽기 액세스 및 쓰기 액세스는 허용됩니다. 내에서 AWS작업을 수행하려면 사용자가 작업을 수행하는 데 필요한 특정 서비스에 일정 수준의 액세스 권한이 있어야 합니다.

AWS 개발자와 같은 일부 사용자는 엔지니어링 솔루션을 만들려면 액세스 권한이 있는 리소스에 대해 알아야 할 수 있습니다. AWS 서비스에서 실행되는 애플리케이션의 최종 사용자와 같은 다른 사용자는 착륙 영역 내의 AWS 리소스에 대해 알 필요가 없습니다.

AWS 사용자의 AWS 리소스 액세스 범위를 식별하는 도구를 제공합니다. 사용자 액세스 범위를 식별한 후에는 조직의 정보 관리 정책에 따라 해당 정보를 사용자와 공유할 수 있습니다. 이 도구에 대한 자세한 내용은 다음 링크를 참조하십시오.

- AWS 액세스 어드바이저 — AWS Identity and Access Management (IAM) 액세스 어드바이저 도구를 사용하면 사용자, 역할 또는 그룹과 같은 IAM 개체가 서비스를 호출했을 때의 마지막 타임스탬프를 분석하여 개발자가 보유한 권한을 확인할 수 있습니다. AWS 서비스 액세스를 감사하고 불필요한

권한을 제거할 수 있으며, 필요한 경우 프로세스를 자동화할 수 있습니다. 자세한 내용은 AWS 보안 블로그 게시물을 참조하십시오.

- IAM 정책 시뮬레이터 - IAM 정책 시뮬레이터를 사용하면 IAM 기반 및 리소스 기반 정책을 테스트하고 문제를 해결할 수 있습니다. 자세한 내용은 IAM 정책 시뮬레이터를 사용한 IAM 정책 테스트를 참조하십시오.
- AWS CloudTrail 로그 - AWS CloudTrail 로그를 검토하여 사용자, 역할 또는 역할이 수행한 작업을 확인할 수 있습니다. AWS 서비스에 대한 CloudTrail 자세한 내용은 AWS CloudTrail 사용 설명서를 참조하십시오.

  AWS Control Tower 랜딩 존 관리자가 취한 조치는 랜딩 존 관리 계정에서 확인할 수 있습니다. 회원 계정 관리자와 사용자가 취한 조치는 공유 로그 아카이브 계정에서 확인할 수 있습니다.

  활동 페이지에서 AWS Control Tower 이벤트의 요약 표를 볼 수 있습니다.

예방 규제 항목 설명

예방적 제어를 통해 조직의 계정이 회사 정책을 지속적으로 준수하도록 할 수 있습니다. 예방 통제의 상태는 시행되거나 활성화되지 않을 수 있습니다. 예방 제어는 SCP (서비스 제어 정책) 를 사용하여 정책 위반을 방지합니다. 이에 비해 탐지 컨트롤은 정의된 규칙을 통해 존재하는 다양한 이벤트 또는 상태를 알려줍니다. AWS Config

AWS 개발자와 같은 일부 사용자는 엔지니어링 솔루션을 개발하기 위해 자신이 사용하는 모든 계정 및 OU에 적용되는 예방 제어 기능에 대해 알아야 할 수 있습니다. 다음 절차에서는 조직의 정보 관리 정책에 따라 적합한 사용자에게 이 정보를 제공하는 방법에 대한 몇 가지 지침을 제공합니다.

> **Note**
>
> 이 절차에서는 이미 적어도 한 명의 AWS IAM Identity Center 사용자뿐만 아니라 landding Zone 내에 적어도 한 명의 하위 OU를 만들었다고 가정합니다.

알 필요가 있는 사용자에게 예방 제어 기능을 보여주기 위함입니다.

1. https://console.aws.amazon.com/controltower/ 에서 AWS Control Tower 콘솔에 로그인합니다.
2. 왼쪽 탐색 메뉴에서 조직을 선택합니다.
3. 테이블에서 사용자에게 해당 컨트롤에 대한 정보가 필요한 OU 중 하나의 이름을 선택합니다.
4. OU 이름과 이 OU에 적용되는 컨트롤을 기록해 두십시오.

5. 사용자가 정보를 필요로 하는 각 OU에 대해 앞의 두 단계를 반복합니다.

제어 항목 및 기능에 대한 자세한 내용은 AWS Control Tower의 제어 정보를 참조하십시오.

AWS Control Tower 랜딩 존을 계획하십시오.

설정 프로세스를 진행하면 AWS Control Tower가 사용자 계정과 관련된 주요 리소스인 랜딩 존(landing zone) 을 시작합니다. 이 리소스는 조직 및 해당 계정을 위한 홈 역할을 합니다.

> **Note**
>
> 조직당 하나의 랜딩 영역을 가질 수 있습니다.

landing Zone을 계획하고 설정할 때 따라야 할 몇 가지 모범 사례에 대한 자세한 내용은 을 참조하십시오AWS AWS Control Tower 랜딩 존을 위한 다중 계정 전략.

AWS Control Tower를 설정하는 방법

기존 조직에 AWS Control Tower 랜딩 존을 설정하거나 AWS Control Tower 랜딩 존을 포함하는 새 조직을 생성하여 시작할 수 있습니다.

- 기존 조직에서 AWS Control Tower 시작: 이 섹션은 기존 고객이 AWS Control Tower를 통해 거버넌스를 도입할 AWS Organizations 준비가 되어 있는 고객을 대상으로 합니다.
- 새 조직에서 AWS Control Tower를 시작하세요: 이 섹션은 기존 AWS OrganizationsOU 및 계정이 없는 고객을 대상으로 합니다.

> **Note**
>
> 이미 AWS Organizations 랜딩 존이 있는 경우, AWS Control Tower 거버넌스를 기존 랜딩 존에서 조직 내 기존 OU 및 계정 일부 또는 전체로 확장할 수 있습니다. 기존 조직 및 계정 관리를 참조하십시오.

기능 비교

다음은 기존 조직에 AWS Control Tower를 추가하는 것과 OU 및 계정으로 AWS Control Tower 거버넌스를 확장하는 것의 차이점을 간략하게 비교한 것입니다. 또한 AWS 랜딩 존 솔루션에서 AWS Control Tower로 이전하는 경우 몇 가지 특별한 고려 사항이 적용됩니다.

기존 조직에 추가 정보: AWS Control Tower를 기존 조직에 추가하는 작업은 콘솔 내에서 수행할 수 있습니다. AWS 이 경우에는 AWS Organizations 서비스에 이미 조직을 생성했고, 해당 조직은 현재 AWS Control Tower에 등록되어 있지 않으며, 이후에 landing Zone을 추가하려고 합니다.

기존 조직에 랜딩 존을 추가하면 AWS Control Tower는 해당 AWS Organizations 수준에서 병렬 구조를 설정합니다. 기존 조직 내의 OU와 계정은 변경되지 않습니다.

거버넌스 확장 정보: 거버넌스 확장은 이미 AWS Control Tower에 등록된 단일 조직 내의 특정 OU 및 계정에 적용됩니다. 즉, 해당 조직을 위한 랜딩 존이 이미 존재합니다. 거버넌스를 확장한다는 것은 AWS Control Tower 규제 항목이 해당 등록 조직 내의 특정 OU 및 계정에 적용되도록 확장된다는 것을 의미합니다. 이 경우에는 새 랜딩 존을 시작하는 것이 아니라 조직의 현재 랜딩 존만 확장하는 것입니다.

> **Important**
>
> 특별 고려 사항: 현재 AWS Landing Zone 솔루션 (ALZ) 을 사용 중인 경우 AWS Organizations, 조직에서 AWS Control Tower를 활성화하기 전에 AWS 솔루션스 아키텍트에게 문의하십시오. AWS Control Tower는 AWS Control Tower가 현재 랜딩 존 배포를 방해할 수 있는지 여부를 판단하는 사전 검사를 수행할 수 없습니다. 자세한 설명은 둘러보기: ALZ에서 AWS 컨트롤 타워로 이동 섹션을 참조하세요. 또한 한 착륙 지대에서 다른 착륙 지대로 계정을 이동하는 방법에 대한 자세한 내용은 을 참조하십시오. 계정이 사전 요구 사항을 충족하지 않으면 어떻게 됩니까?

기존 조직에서 AWS Control Tower 시작

기존 조직에 AWS Control Tower 랜딩 존을 설정하면 기존 AWS Organizations 환경과 병렬로 즉시 작업을 시작할 수 있습니다. 내에서 생성된 다른 AWS Organizations OU는 AWS Control Tower에 등록되지 않았으므로 변경되지 않습니다. 이러한 OU 및 계정은 그대로 계속 사용할 수 있습니다.

AWS Control Tower는 기존 조직의 관리 계정을 관리 계정으로 사용하여 통합합니다. 새 관리 계정은 필요하지 않습니다. 기존 관리 계정에서 AWS Control Tower 랜딩 존을 시작할 수 있습니다.

> **Note**
>
> 기존 조직에 AWS Control Tower를 설정하려면 서비스 한도에 최소 두 개의 추가 계정 생성이 허용되어야 합니다.

기존 조직에 AWS Control Tower를 추가할 때의 효과

AWS Control Tower는 조직에 감사 계정과 로깅 계정이라는 두 개의 계정을 생성합니다. 이러한 계정은 개별 최종 사용자 계정에 팀이 수행한 작업을 기록합니다. 감사 및 로그 아카이브 계정은 AWS Control Tower 랜딩 존 내의 보안 OU에 표시됩니다.

랜딩 존을 설정하면 AWS Control Tower에서 추가한 계정은 기존 계정의 일부가 되며 AWS Organizations, 따라서 기존 조직에 대한 청구에도 포함됩니다.

기능 요약

기존 AWS Organizations 조직에서 AWS Control Tower를 활성화하면 조직에 몇 가지 주요 개선 사항이 제공됩니다.

- AWS Control Tower에서 추가한 계정은 기존 조직의 일부가 되므로 조직 그룹 전체에 통합 결제가 가능합니다.
- 이를 통해 OU의 관리 계정 하나에서 모든 계정을 관리할 수 있습니다.
- 기존 계정과 새 계정의 보안 및 규정 준수를 포괄하는 제어를 적용하고 적용하는 방법을 간소화합니다.

> **Important**
>
> 기존 AWS Organizations 조직에서 AWS Control Tower 랜딩 존을 시작해도 해당 조직에서 AWS Control Tower에 등록되지 않은 다른 OU 또는 계정으로 AWS Control Tower 거버넌스를 확장할 수 없습니다.

기존 조직에서 AWS Control Tower를 시작하려면 에 AWS Control Tower 시작하기 설명된 프로세스를 따르십시오.

AWS Control Tower가 기존 AWS Organizations 조직과 상호 작용하는 방식에 대한 자세한 내용은 을 참조하십시오AWS Control Tower를 사용하여 조직 및 계정을 관리합니다..

새 조직에서 AWS Control Tower를 시작하세요

AWS Control Tower를 처음 사용하고 사용해 본 적이 없다면 먼저 설명서를 참조하는 것이 좋습니다. AWS Organizations설정

AWS Control Tower는 조직이 설정되어 있지 않을 경우 자동으로 조직을 설정합니다.

AWS AWS Control Tower 랜딩 존을 위한 다중 계정 전략

AWS Control Tower 고객은 AWS 환경을 설정하고 최상의 결과를 얻는 방법에 대한 지침을 자주 구합니다.AWS 는 다중 계정 전략이라고 하는 통합 권장 사항 세트를 만들어 AWS Control Tower 랜딩 존을 비롯한 AWS 리소스를 최대한 활용할 수 있도록 지원합니다.

기본적으로 AWS Control Tower는 다른 AWS 서비스와 함께 작동하는 오케스트레이션 계층 역할을 하며, 이를 통해 계정 및 계정에 대한 AWS AWS 다중 계정 권장 사항을 구현하는 데 도움이 됩니다. AWS Organizations랜딩 존이 설정된 후에도 AWS Control Tower는 여러 계정과 워크로드에 걸쳐 기업 정책 및 보안 관행을 유지할 수 있도록 지속적으로 지원합니다.

대부분의 랜딩 존은 시간이 지남에 따라 발전합니다. AWS Control Tower 랜딩 존의 조직 단위 (OU)와 계정 수가 증가함에 따라 워크로드를 효과적으로 구성하는 데 도움이 되는 방식으로 AWS Control Tower 배포를 확장할 수 있습니다. 이 장에서는 AWS 다중 계정 전략에 따라 AWS Control Tower 랜딩 존을 계획 및 설정하고 시간이 지남에 따라 확장하는 방법에 대한 규범적 지침을 제공합니다.

조직 단위의 모범 사례에 대한 일반적인 논의는 조직 단위의 모범 사례를 참조하십시오. AWS Organizations

AWS 다중 계정 전략: 모범 사례 지침

AWS 잘 설계된 환경의 모범 사례에서는 리소스와 워크로드를 여러 계정으로 분리하는 것이 좋습니다. AWS AWS 계정은 격리된 리소스 컨테이너라고 생각할 수 있습니다. 계정은 워크로드 분류는 물론 문제 발생 시 폭발 반경 감소 기능을 제공합니다.

계정의 정의: AWS

> AWS 계정은 리소스 컨테이너 및 리소스 격리 경계 역할을 합니다.

> **Note**
>
> AWS 계정은 페더레이션 또는 AWS Identity and Access Management (IAM) 을 통해 설정된 사용자 계정과 다릅니다.

계정에 대한 자세한 정보 AWS

AWS 계정은 리소스를 격리하고 AWS 워크로드에 대한 보안 위협을 억제하는 기능을 제공합니다. 또한 계정은 워크로드 환경의 청구 및 거버넌스를 위한 메커니즘을 제공합니다.

AWS 계정은 워크로드에 리소스 컨테이너를 제공하는 기본 구현 메커니즘입니다. 환경이 잘 설계되어 있으면 여러 AWS 계정을 효과적으로 관리할 수 있으므로 여러 워크로드와 환경을 관리할 수 있습니다.

AWS Control Tower는 잘 설계된 환경을 설정합니다. 이는 여러 계정으로 확장될 수 있는 환경 변경을 관리하는 데 도움이 되는 AWS 계정과 AWS Organizations함께 계정에 의존합니다.

잘 설계된 환경의 정의

> AWS 는 잘 설계된 환경을 랜딩 존으로 시작하는 환경으로 정의합니다.

AWS Control Tower는 자동으로 설정되는 랜딩 존을 제공합니다. 환경 내 여러 계정에 걸쳐 기업 지침을 준수할 수 있도록 제어를 적용합니다.

랜딩 존의 정의

> Landing Zone은 기본 계정, 계정 구조, 네트워크 및 보안 레이아웃 등을 포함하여 권장되는 시작점을 제공하는 클라우드 환경입니다. Landing Zone에서 솔루션과 애플리케이션을 활용하는 워크로드를 배포할 수 있습니다.

잘 설계된 환경을 설정하기 위한 지침

다음 섹션에서 설명하는 잘 설계된 환경의 세 가지 주요 구성 요소는 다음과 같습니다.

- 여러 계정 AWS
- 여러 조직 단위 (OU)
- 잘 계획된 구조

여러 AWS 계정 사용

하나의 계정으로는 잘 설계된 환경을 설정하기에 충분하지 않습니다. 여러 계정을 사용하면 보안 목표와 비즈니스 프로세스를 가장 잘 지원할 수 있습니다. 다중 계정 접근 방식을 사용할 때 얻을 수 있는 몇 가지 이점은 다음과 같습니다.

- 보안 제어 — 애플리케이션은 보안 프로필이 다르므로 서로 다른 제어 정책 및 메커니즘이 필요합니다. 예를 들어, 감사자와 상담하여 결제 카드 산업 (PCI) 워크로드를 호스팅하는 단일 계정을 추천하는 것이 훨씬 쉽습니다.
- 격리 – 계정은 보안 보호의 한 단위입니다. 잠재적 위험과 보안 위협은 다른 사람에게 영향을 주지 않으면서 계정 내에 억제할 수 있습니다. 따라서 보안 요구 사항에 따라 계정을 서로 격리해야 할 수 있습니다. 예를 들어 보안 프로필이 서로 다른 팀이 있을 수 있습니다.
- 많은 팀 — 팀마다 책임과 리소스 요구 사항이 다릅니다. 계정을 여러 개 설정하면 같은 계정을 사용할 때처럼 팀이 서로 간섭할 수 없습니다.
- 데이터 격리 — 데이터 저장소를 하나의 계정으로 격리하면 데이터에 액세스하고 데이터 저장소를 관리할 수 있는 사람의 수를 제한하는 데 도움이 됩니다. 이러한 격리는 매우 개인적인 데이터의 무단 노출을 방지하는 데 도움이 됩니다. 예를 들어, 데이터 격리는 일반 데이터 보호 규정 (GDPR) 준수를 지원하는 데 도움이 됩니다.
- 비즈니스 프로세스 — 사업부 또는 제품은 목적과 프로세스가 완전히 다른 경우가 많습니다. 개별 계정을 설정하여 비즈니스별 요구 사항을 충족할 수 있습니다.
- 청구 — 계정은 이체 수수료 등을 포함하여 청구 수준에서 항목을 구분할 수 있는 유일한 방법입니다. 다중 계정 전략을 사용하면 사업부, 직무 팀 또는 개별 사용자 간에 별도의 청구 가능 항목을 만들 수 있습니다.
- 할당량 할당 — AWS 할당량은 계정별로 설정됩니다. 워크로드를 여러 계정으로 분리하면 각 계정 (예: 프로젝트) 에 잘 정의된 개별 할당량이 부여됩니다.

여러 조직 단위를 사용하십시오.

AWS Control Tower 및 기타 계정 오케스트레이션 프레임워크는 계정 경계를 넘나드는 변경을 수행할 수 있습니다. 따라서 AWS 모범 사례는 잠재적으로 환경을 손상시키거나 보안을 약화시킬 수 있는 계정 간 변경을 다룹니다. 경우에 따라 변경 사항이 정책을 넘어 전체 환경에 영향을 미칠 수 있습니다. 따라서 최소한 두 개의 필수 계정, 즉 프로덕션 계정과 스테이징을 설정하는 것이 좋습니다.

또한 거버넌스 및 제어를 위해 AWS 계정을 조직 단위 (OU) 로 그룹화하는 경우가 많습니다. OU는 여러 계정에 대한 정책 시행을 처리하도록 설계되었습니다.

최소한 프로덕션 환경과는 별개의 제어 및 정책을 포함하는 사전 프로덕션 (또는 스테이징) 환경을 만드는 것이 좋습니다. 프로덕션 및 스테이징 환경을 별도의 OU로 만들고 관리할 수 있으며 별도의 계정으로 비용을 청구할 수 있습니다. 또한 코드 테스트용 샌드박스 OU를 설정할 수도 있습니다.

착륙 지대의 OU에 대해 잘 계획된 구조를 사용하십시오.

AWS Control Tower는 일부 OU를 자동으로 설정합니다. 시간이 지남에 따라 워크로드와 요구 사항이 확장되면 원래 landing Zone 구성을 필요에 맞게 확장할 수 있습니다.

> **Note**
>
> 예제에 제공된 이름은 다중 계정 환경 설정을 위한 권장 AWS 명명 규칙을 따릅니다. AWS 랜딩 존을 설정한 후 OU 세부 정보 페이지에서 편집을 선택하여 OU 이름을 변경할 수 있습니다.

권장 사항

AWS Control Tower가 첫 번째 필수 OU인 보안 OU를 설정한 후에는 랜딩 존에 OU를 몇 개 더 생성하는 것이 좋습니다.

AWS Control Tower가 샌드박스 OU라고 하는 추가 OU를 하나 이상 생성하도록 허용하는 것이 좋습니다. 이 OU는 소프트웨어 개발 환경을 위한 것입니다. AWS Control Tower는 사용자가 선택한 경우 랜딩 존 생성 중에 샌드박스 OU를 자동으로 설정할 수 있습니다.

직접 설정할 수 있는 다른 권장 OU 두 개가 있습니다. 하나는 공유 서비스 및 네트워킹 계정을 포함하는 인프라 OU이고 다른 하나는 프로덕션 워크로드를 포함하는 워크로드 OU라고 합니다. 조직 단위 페이지의 AWS Control Tower 콘솔을 통해 랜딩 존에 OU를 추가할 수 있습니다.

자동으로 설정되는 OU 이외의 권장 OU

- 인프라 OU - 공유 서비스 및 네트워킹 계정을 포함합니다.

  > **Note**
  >
  > AWS Control Tower는 사용자를 위해 인프라 OU를 설정하지 않습니다.

- 샌드박스 OU — 소프트웨어 개발 OU. 예를 들어 지출 한도가 고정되어 있거나 프로덕션 네트워크에 연결되어 있지 않을 수 있습니다.

> **Note**
>
> AWS Control Tower는 샌드박스 OU 설정을 권장하지만, 이는 선택 사항입니다. 랜딩 존 구성의 일부로 자동으로 설정할 수 있습니다.

- 워크로드 OU - 워크로드를 실행하는 계정을 포함합니다.

> **Note**
>
> AWS Control Tower는 사용자를 위해 워크로드 OU를 설정하지 않습니다.

자세한 내용은 AWS Control Tower를 통한 프로덕션 스타터 조직을 참조하십시오.

완전한 다중 계정 OU 구조를 갖춘 AWS Control Tower의 예

AWS Control Tower는 중첩된 OU 계층 구조를 지원하므로 조직의 요구 사항에 맞는 계층적 OU 구조를 생성할 수 있습니다. AWS 다중 계정 전략 지침에 맞게 AWS Control Tower 환경을 구축할 수 있습니다.

또한 성능이 우수하고 AWS 다중 계정 지침에 부합하는 더 단순하고 평평한 OU 구조를 구축할 수 있습니다. 계층적 OU 구조를 구축할 수 있다고 해서 반드시 그렇게 해야 하는 것은 아닙니다.

- AWS 다중 계정 지침과 함께 확장된 플랫 AWS Control Tower 환경의 OU 예제 세트를 보여주는 다이어그램을 보려면 예제: 플랫 OU 구조의 워크로드를 참조하십시오.
- AWS Control Tower가 중첩된 OU 구조에서 작동하는 방식에 대한 자세한 내용은 을 참조하십시오AWS Control Tower의 중첩된 OU.
- AWS Control Tower가 이 AWS 지침을 어떻게 준수하는지에 대한 자세한 내용은 AWS 백서 “다중 계정을 사용한 AWS 환경 구성”을 참조하십시오.

연결된 페이지의 다이어그램은 더 많은 기본 OU와 더 많은 추가 OU가 생성되었음을 보여줍니다. 이러한 OU는 대규모 배포의 추가 요구 사항을 충족합니다.

기본 OU 열에는 기본 구조에 두 개의 OU가 추가되었습니다.

- Security_Prod OU — 보안 정책을 위한 읽기 전용 영역과 보안 감사 영역을 제공합니다.
- 인프라 OU — 이전에 권장한 인프라 OU를 Infrastructure_Test (사전 프로덕션 인프라용) 와 Infrastructure_Prod (프로덕션 인프라용) 라는 두 개의 OU로 분리할 수 있습니다.

추가 OU 영역에는 기본 구조에 OU가 몇 개 더 추가되었습니다. 다음은 환경이 확장됨에 따라 생성할 다음 권장 OU입니다.

- 워크로드 OU - 이전에는 권장되었지만 선택 사항이었던 워크로드 OU는 Workloads_Test (사전 프로덕션 워크로드용) 와 Workloads_Prod (프로덕션 워크로드용) 라는 두 개의 OU로 분리되었습니다.
- PolicyStaging OU — 시스템 관리자가 제어 및 정책에 대한 변경 사항을 완전히 적용하기 전에 테스트할 수 있습니다.
- 일시 중단된 OU - 일시적으로 비활성화되었을 수 있는 계정을 위한 위치를 제공합니다.

루트 정보

루트는 OU가 아닙니다. 관리 계정과 조직 내 모든 OU 및 계정을 위한 컨테이너입니다. 개념적으로 루트에는 모든 OU가 포함됩니다. 삭제할 수 없습니다. AWS Control Tower 내의 루트 수준에서는 등록된 계정을 관리할 수 없습니다. 대신 OU 내 등록 계정을 관리하십시오. 유용한 다이어그램은 설명서를 참조하십시오. AWS Organizations

Landing Zone 설정을 위한 관리 팁

- 일을 가장 많이 하는 AWS 지역은 홈 지역이어야 합니다.
- 랜딩 존을 설정하고 거주 지역 내에서 Account Factory 계정을 배포하세요.
- 여러 AWS 지역에 투자하는 경우 클라우드 리소스가 대부분의 클라우드 관리 작업을 수행하고 워크로드를 실행할 지역에 있는지 확인하세요.
- 워크로드와 로그를 동일한 AWS 지역에 보관하면 지역 간에 로그 정보를 이동하고 검색하는 데 드는 비용을 줄일 수 있습니다.
- 감사 및 기타 Amazon S3 버킷은 AWS Control Tower를 시작한 AWS 지역과 동일한 지역에 생성됩니다. 이러한 버킷은 이동하지 않는 것이 좋습니다.
- Log Archive 계정에서 자체 로그 버킷을 만들 수 있지만 권장하지는 않습니다. AWS Control Tower에서 생성한 버킷은 그대로 두어야 합니다.
- Amazon S3 액세스 로그는 원본 버킷과 동일한 AWS 지역에 있어야 합니다.
- 시작 시 AWS Control Tower에서 지원하는 모든 지역의 관리 계정에서 AWS 보안 토큰 서비스 (STS) 엔드포인트를 활성화해야 합니다. 그렇지 않으면 중간에 구성 프로세스에서 시작이 실패할 수 있습니다.
- AWS Control Tower는 활성화된 컨트롤에 대한 태깅만 지원합니다. 자세한 정보는 AWS Control Tower는 활성화된 컨트롤에 대한 태그 지정을 지원합니다.을 참조하세요.

- AWS Control Tower가 관리하는 모든 계정에 대해 멀티 팩터 인증 (MFA) 을 활성화하는 것이 좋습니다.

VPC에 대한 고려 사항

- AWS 컨트롤 AWS 리전 타워에서 생성한 VPC는 AWS 컨트롤 타워를 사용할 수 있는 곳으로 제한됩니다. 지원되지 않는 지역에서 워크로드를 실행하는 일부 고객은 Account Factory 계정으로 생성된 VPC를 비활성화하고자 할 수 있습니다. 고객은 Service Catalog 포트폴리오를 사용하여 새 VPC를 만들거나 필요한 지역에서만 실행되는 사용자 지정 VPC를 만드는 것을 선호할 수 있습니다.
- AWS Control Tower에서 생성한 VPC는 모두를 위해 생성되는 기본 VPC와 다릅니다. AWS 계정 AWS 컨트롤 타워가 지원되는 지역의 경우, AWS 컨트롤 타워는 AWS 컨트롤 타워 VPC를 생성할 때 기본 VPC를 삭제합니다.
- 홈 리전에서 기본 VPC를 삭제하는 경우 다른 AWS 모든 AWS 리전에서 삭제하는 것이 가장 좋습니다.

그룹, 역할, 정책 설정을 위한 권장 사항

랜딩 존을 설정할 때 특정 계정에 액세스해야 하는 사용자와 그 이유에 대해 미리 결정하는 것이 좋습니다. 예를 들어 보안 계정은 보안팀만 액세스할 수 있어야 하고, 관리 계정은 클라우드 관리자 팀만 액세스할 수 있어야 하는 식입니다.

이 주제에 대한 자세한 내용은 을 참조하십시오. AWS Control Tower의 자격 증명 및 액세스 관리

권장 제한 사항

관리자가 AWS Control Tower 작업만 관리할 수 있도록 허용하는 IAM 역할 또는 정책을 설정하여 조직에 대한 관리 액세스 범위를 제한할 수 있습니다. 권장되는 접근 방식은 IAM 정책을 사용하는 것입니다. `arn:aws:iam::aws:policy/service-role/AWSControlTowerServiceRolePolicy` `AWSControlTowerServiceRolePolicy`역할이 활성화되면 관리자는 AWS Control Tower만 관리할 수 있습니다. 각 계정에는 예방 규제 항목 및 SCP 관리에 적합한 액세스 권한과 탐지 규제 항목 관리를 위한 액세스 권한을 포함해야 AWS Config합니다. AWS Organizations

랜딩 존에서 공유 감사 계정을 설정할 때 해당 `AWSSecurityAuditors` 그룹을 계정의 타사 감사자에게 할당하는 것이 좋습니다. 이 그룹은 멤버에게 읽기 전용 권한을 부여합니다. 감사자의 업무 분리 요구 사항 준수를 위반할 수 있으므로 계정에는 감사 중인 환경에 대한 쓰기 권한이 없어야 합니다.

역할 신뢰 정책에 조건을 부과하여 AWS Control Tower에서 특정 역할과 상호 작용하는 계정 및 리소스를 제한할 수 있습니다. 광범위한 액세스 권한을 허용하므로 `AWSControlTowerAdmin` 역할에 대

한 액세스를 제한하는 것이 좋습니다. 자세한 내용은 역할 신뢰 관계에 대한 선택적 조건을 참조하십시오.

AWS Control Tower 리소스 생성 및 수정 지침

AWS Control Tower에서 리소스를 생성하고 수정할 때는 다음 모범 사례를 따르는 것이 좋습니다. 서비스가 업데이트될 경우 이 지침이 변경될 수 있습니다. 공동 책임 모델은 AWS Control Tower 환경에 적용된다는 점을 기억하십시오.

일반 지침

- 관리 계정, 공유 계정 및 멤버 계정의 리소스를 포함하여 AWS Control Tower에서 생성한 리소스를 수정하거나 삭제하지 마십시오. 이러한 리소스를 수정하면 landding Zone을 업데이트하거나 OU를 다시 등록해야 할 수 있으며, 수정하면 규정 준수 보고가 부정확해질 수 있습니다.

  특히:

  - 액티브 AWS Config 레코더를 보관하세요. Config 레코더를 삭제하면 탐지 컨트롤이 드리프트를 감지하고 보고할 수 없습니다. 정보가 충분하지 않아 규정을 준수하지 않는 리소스는 규정 준수로 보고될 수 있습니다.
  - 보안 조직 구성 단위 AWS Identity and Access Management (OU) 의 공유 계정 내에 생성된 (IAM) 역할을 수정하거나 삭제하지 마십시오. 이러한 역할을 수정하려면 랜딩 영역을 업데이트해야 합니다.
  - 등록되지 않은 계정이라도 멤버 계정에서 `AWSControlTowerExecution` 역할을 삭제하지 마세요. 그렇게 하면 이러한 계정을 AWS Control Tower에 등록하거나 직계 부모 OU를 등록할 수 없습니다.
- SCP 또는 AWS Security Token Service () 를 AWS 리전 통한 사용을 금지하지 마십시오.AWS STS 이렇게 하면 AWS Control Tower가 정의되지 않은 상태로 전환됩니다. 를 사용하여 AWS STS지역을 허용하지 않으면 해당 지역에서는 인증을 사용할 수 없으므로 해당 지역에서 기능이 작동하지 않습니다. 대신, 컨트롤에 표시된 대로 AWS Control Tower 지역 거부 기능 AWS 리전, 요청에 AWS 따른 액세스 거부 기능 (landing zone 수준에서 작동) 또는 OU 수준에서 작동하여 지역에 대한 액세스를 제한하는 OU에 적용되는 제어 지역 거부 제어를 사용하십시오.
- AWS Organizations `FullAWSAccess`SCP를 적용해야 하며 다른 SCP와 병합해서는 안 됩니다. 이 SCP에 대한 변경은 드리프트로 보고되지 않습니다. 그러나 특정 리소스에 대한 액세스가 거부되는 경우 일부 변경 사항이 예상치 못한 방식으로 AWS Control Tower 기능에 영향을 미칠 수 있습니다. 예를 들어, SCP가 분리되거나 수정되면 계정이 AWS Config 레코더에 액세스할 수 없게 되거나 로그인에 공백이 생길 수 있습니다. CloudTrail

- 랜딩 존을 설정한 조직에 대한 AWS Control Tower 서비스 액세스를 AWS Organizations `DisableAWSServiceAccess` API를 사용하여 끄지 마십시오. 이렇게 하면 메시징 지원이 없으면 특정 AWS Control Tower 드리프트 탐지 기능이 제대로 작동하지 않을 수 있습니다. AWS Organizations이러한 드리프트 탐지 기능은 AWS Control Tower가 조직 내 조직 단위, 계정 및 컨트롤의 규정 준수 상태를 정확하게 보고할 수 있도록 보장합니다. 자세한 내용은 AWS Organizations API API_DisableAWSServiceAccess 참조를 참조하십시오.
- 일반적으로 AWS Control Tower는 한 번에 하나의 작업을 수행하며, 다른 작업을 시작하기 전에 작업을 완료해야 합니다. 예를 들어, 컨트롤을 활성화하는 프로세스가 이미 작동 중일 때 계정을 프로비저닝하려고 하면 계정 프로비저닝이 실패합니다.

  예외:

  - AWS Control Tower를 사용하면 동시 작업을 통해 선택적 제어를 배포할 수 있습니다. 자세한 내용은 선택적 제어 기능의 동시 배포를 참조하십시오.
  - AWS Control Tower에서는 Account Factory를 사용하여 최대 10개의 계정 생성, 업데이트 또는 등록 작업을 동시에 수행할 수 있습니다.

> **Note**
>
> AWS Control Tower에서 생성한 리소스에 대한 자세한 내용은 을 참조하십시오공유 계정이란 무엇인가요?.

계정 및 OU에 대한 팁

- 등록된 각 OU를 최대 300개의 계정으로 유지하는 것이 좋습니다. 그러면 거버넌스를 위한 새 지역을 구성할 때와 같이 계정 업데이트가 필요할 때마다 OU 재등록 기능으로 해당 계정을 업데이트할 수 있습니다.
- OU를 등록하는 데 필요한 시간을 줄이려면 OU당 계정 수는 OU당 300개로 제한되더라도 OU당 계정 수를 약 150개로 유지하는 것이 좋습니다. 일반적으로 OU를 등록하는 데 필요한 시간은 OU가 운영되는 지역 수에 OU의 계정 수를 곱한 값에 따라 늘어납니다.
- 추정치에 따르면 계정이 150개인 OU의 경우 컨트롤을 등록하고 활성화하는 데 약 2시간, 다시 등록하는 데 약 1시간이 소요됩니다. 또한 컨트롤이 많은 OU는 컨트롤이 거의 없는 OU보다 등록 시간이 더 오래 걸립니다.
- OU 등록 기간이 길어지는 것에 대한 한 가지 우려는 이 프로세스가 다른 작업을 차단한다는 것입니다. 일부 고객은 각 OU에 더 많은 계정을 허용하는 것을 선호하기 때문에 OU를 등록하거나 다시 등록하는 데 더 오랜 시간을 허용하는 것을 선호합니다.

루트 사용자로 로그인하는 경우

특정 관리 작업을 수행하려면 루트 사용자로 로그인해야 합니다. AWS Control Tower의 어카운트 팩토리에서 생성한 계정에 루트 사용자로 로그인할 수 있습니다. AWS 계정

다음 작업을 수행하려면 루트 사용자로 로그인해야 합니다.

- 계정 이름, 루트 사용자 암호 또는 이메일 주소를 비롯한 특정 계정 설정을 변경합니다. 자세한 정보는 AWS Control Tower 또는 다음을 통해 계정 팩토리 계정을 업데이트하고 이전하십시오. AWS Service Catalog을 참조하세요.
- 를 종료하려면 AWS 계정.
- 루트 사용자 로그인 자격 증명이 필요한 작업에 대한 자세한 내용은 AWS Account Management 참조 안내서의 루트 사용자 자격 증명이 필요한 작업을 참조하십시오.

> **Note**
>
> AWS Support 플랜을 변경하거나 활성화하려면 루트 사용자 또는 적절한 IAM 권한을 가진 사용자로 로그인해야 합니다. .

루트 사용자로 로그인하려면

1. AWS 로그인 페이지를 엽니다.

   액세스가 필요한 이메일 주소가 없는 경우 AWS Control Tower에서 받을 수 있습니다. AWS 계정 관리 계정의 콘솔을 열고 [Accounts] 를 선택한 다음 이메일 주소를 찾습니다.
2. 액세스가 필요한 이메일 주소를 입력하고 다음을 선택합니다. AWS 계정
3. Forgot password?(암호 찾기)를 선택하여 암호 재설정 지침을 루트 사용자 이메일 주소로 보냅니다.
4. 루트 사용자 메일박스에서 암호 재설정 이메일 메시지를 열고 지침에 따라 암호를 재설정합니다.
5. AWS 로그인 페이지를 연 다음 재설정한 비밀번호로 로그인합니다.

AWS Organizations 지침

- AWS Organizations 설명서에서 AWS Control Tower 관리 계정 및 회원 계정의 보안을 보호하는 모범 사례에 대한 지침을 찾을 수 있습니다.

  - 관리 계정 모범 사례
  - 회원 계정 모범 사례
- AWS Control AWS Organizations Tower에 등록된 OU에 연결된 서비스 제어 정책 (SCP) 을 업데이트하는 데는 사용하지 마십시오. 이렇게 하면 컨트롤이 알 수 없는 상태로 전환되어 랜딩 존을 재설정하거나 AWS Control Tower에 OU를 다시 등록해야 합니다. 대신 AWS Control Tower에서 생성한 SCP를 편집하는 대신 새 SCP를 생성하여 OU에 연결할 수 있습니다.
- 이미 등록된 개인 계정을 등록된 OU 외부에서 AWS Control Tower로 이전하면 드리프트가 발생하므로 이를 해결해야 합니다. 거버넌스 드리프트 유형를 참조하세요.
- 를 사용하여 AWS Control AWS Organizations Tower에 등록된 조직 내에서 계정을 생성, 초대 또는 이전하는 경우, 해당 계정은 AWS Control Tower에 등록되지 않으며 이러한 변경 사항도 기록되지 않습니다. SSO를 통해 이러한 계정에 액세스해야 하는 경우 멤버 계정 액세스를 참조하십시오.
- 를 사용하여 AWS Organizations OU를 AWS Control Tower에서 만든 조직으로 옮기는 경우 외부 OU는 AWS Control Tower에 등록되지 않습니다.
- AWS Control AWS Organizations Tower는 권한 필터링을 처리하는 방식과 다르게 처리합니다. 계정에 AWS Control Tower 어카운트 팩토리가 프로비저닝된 경우, 최종 사용자는 AWS Control Tower 콘솔에서 모든 OU의 이름과 상위 객체를 볼 수 있습니다. 이는 해당 OU의 이름과 상위 객체를 직접 검색할 권한이 없더라도 마찬가지입니다. AWS Organizations
- AWS Control Tower는 OU의 상위 항목을 볼 수는 있지만 OU 이름을 볼 수는 없는 권한과 같이 조직에 대한 혼합 권한을 지원하지 않습니다. 이러한 이유로 AWS Control Tower 관리자는 모든 권한을 보유해야 합니다.
- AWS Organizations `FullAWSAccess`SCP를 적용해야 하며 다른 SCP와 병합해서는 안 됩니다. 이 SCP에 대한 변경은 드리프트로 보고되지 않습니다. 그러나 특정 리소스에 대한 액세스가 거부되는 경우 일부 변경 사항이 예상치 못한 방식으로 AWS Control Tower 기능에 영향을 미칠 수 있습니다. 예를 들어, SCP가 분리되거나 수정되면 계정이 AWS Config 레코더에 액세스할 수 없게 되거나 로그인에 공백이 생길 수 있습니다. CloudTrail
- 랜딩 존을 설정한 조직에 대한 AWS Control Tower 서비스 액세스를 AWS Organizations `DisableAWSServiceAccess` API를 사용하여 끄지 마십시오. 이렇게 하면 메시징 지원이 없으면 특정 AWS Control Tower 드리프트 탐지 기능이 제대로 작동하지 않을 수 있습니다. AWS Organizations이러한 드리프트 탐지 기능은 AWS Control Tower가 조직 내 조직 단위, 계정 및 컨트롤의 규정 준수 상태를 정확하게 보고할 수 있도록 보장합니다. 자세한 내용은 AWS Organizations API API_DisableAWSServiceAccess 참조를 참조하십시오.

IAM ID 센터 지침

> **Note**
>
> SSO는 기술 업계에서 싱글 사인온을 나타내는 데 사용되는 약어입니다. 일반적으로 SSO는 세션 및 사용자 인증 서비스입니다. 이를 통해 사용자는 한 세트의 로그인 자격 증명을 사용하여 여러 애플리케이션에 액세스할 수 있습니다. 에서 AWS싱글 사인온 기능을 언급할 때는 IAM 또는 IAM Identity AWS Identity and Access ManagementCenter라고 하며 약칭되는 AWS 서비스를 말합니다.

AWS Control Tower는 AWS Identity and Access Management (IAM) 을 사용하여 사용자 액세스 권한을 규제할 AWS 계정것을 권장합니다. 하지만 AWS Control Tower에서 IAM Identity Center를 자동으로 설정할지, 비즈니스 요구 사항을 가장 효과적으로 충족하는 방식으로 IAM Identity Center를 설정할지, 계정 액세스를 위한 다른 방법을 선택할지 선택할 수 있습니다.

기본적으로 AWS Control Tower는 여러 계정을 사용하여 AWS 환경 구성에 정의된 모범 사례 지침에 따라 랜딩 존에 AWS IAM Identity Center를 설정합니다. 대부분의 고객은 기본값을 선택합니다. 특정 산업 또는 국가의 규정 준수를 위해 또는 AWS IAM Identity Center를 사용할 수 AWS 리전 없는 경우 대체 액세스 방법이 필요할 수 있습니다.

옵션 선택

AWS Control Tower에서 대신 IAM Identity Center를 설정하도록 허용하는 대신, 콘솔에서 랜딩 존 설정 프로세스 중에 IAM Identity Center를 자체 관리하도록 선택할 수 있습니다. 나중에 언제든지 랜딩 존 설정을 수정하고 랜딩 존 설정 페이지에서 랜딩 존을 업데이트하여 이 선택을 변경할 수 있습니다.

AWS Control Tower에서 AWS IAM 자격 증명 센터를 중단하거나 AWS IAM 자격 증명 센터 사용을 시작하려면

1. 랜딩 존 설정 페이지로 이동합니다.
2. 구성 탭을 선택합니다.
3. 그런 다음 적절한 라디오 버튼을 선택하여 AWS IAM Identity Center에 대한 선택 항목을 변경합니다.

AWS IAM ID 센터를 IdP로 자체 관리하기로 선택하면 AWS Control Tower는 AWS Control Tower를 관리하는 데 필요한 역할과 정책 (예: 및) 만 생성합니다. `AWSControlTowerAdmin`

AWSControlTowerAdminPolicy 자체 관리하는 랜딩 존의 경우, AWS Control Tower는 더 이상 고객별 용도를 위한 IAM 역할 및 그룹을 생성하지 않습니다. 랜딩 존 설정 프로세스나 Account Factory를 통한 계정 프로비저닝 중에는 없습니다.

> **Note**
>
> AWS Control Tower 랜딩 존에서 AWS IAM Identity Center를 제거해도 AWS Control Tower가 생성한 사용자, 그룹 및 권한 집합은 제거되지 않습니다. 이러한 리소스를 제거하는 것이 좋습니다.

Azure AD, Ping 또는 Okta와 같은 대체 ID 공급자 (IdPs) 를 보유한 Account Factory 고객은 AWS IAM ID 센터 프로세스에 따라 외부 ID 공급자에 연결하고 IdP를 온보딩할 수 있습니다. 랜딩 존 설정을 수정하여 언제든지 AWS Control Tower가 그룹과 역할을 생성하도록 할 수 있습니다.

- 자격 증명 소스를 기반으로 AWS Control Tower가 IAM Identity Center와 연동되는 방식에 대한 구체적인 정보는 이 사용 설명서의 시작 페이지에 있는 사전 출시 점검 섹션에서 AWS IAM Identity Center 고객을 위한 고려 사항을 참조하십시오.
- AWS Control Tower의 동작이 IAM Identity Center 및 다양한 자격 증명 소스와 상호 작용하는 방식에 대한 추가 정보는 IAM ID 센터 사용 설명서의 자격 증명 소스 변경 고려 사항을 참조하십시오.
- AWS Control Tower 및 IAM 자격 증명 센터 사용에 AWS IAM 아이덴티티 센터 및 AWS 컨트롤 타워와의 협력 대한 자세한 내용은 을 참조하십시오.

Account Factory 지침

Account Factory를 사용하여 AWS Control Tower에서 새 계정을 프로비저닝할 때 문제가 발생할 수 있습니다. 이러한 문제를 해결하는 방법에 대한 자세한 내용은 AWS Control Tower 사용 설명서의 문제 새 계정 프로비저닝 실패 해결에 있는 섹션을 참조하십시오.

IAM 사용자 대신 페더레이션 사용자 또는 IAM 역할을 생성하는 것이 좋습니다. 연동 사용자 및 IAM 역할은 임시 자격 증명을 제공합니다. IAM 사용자는 관리가 어려울 수 있는 장기 자격 증명을 가지고 있습니다. 자세한 내용은 IAM 사용 설명서의 IAM 자격 증명 (사용자, 사용자 그룹, 역할) 을 참조하십시오.

Account Factory에서 새 계정을 프로비저닝하거나 계정 등록 기능인 AWS Control Tower를 사용할 때 IAM 사용자 또는 IAM Identity Center 사용자로 인증된 경우, 사용자가 포트폴리오에 액세스할 수 있는지 확인하십시오. AWS Service Catalog 그렇지 않으면 Service Catalog에서 오류 메시지를 받을 수 있

습니다. 자세한 내용은 AWS Control Tower 사용 설명서의 문제 해결 섹션을 참조하십시오시작 경로를 찾을 수 없음 오류.

> **Note**
>
> 한 번에 최대 5개의 계정을 프로비저닝할 수 있습니다.

SNS 주제 구독에 대한 지침

- `aws-controltower-AllConfigNotifications`SNS 주제는 규정 준수 알림 및 Amazon 이벤트 알림을 AWS Config포함하여 에서 게시한 모든 CloudWatch 이벤트를 수신합니다. 예를 들어, 이 주제는 제어 위반이 발생했는지 여부를 알려줍니다. 또한 다른 유형의 이벤트에 대한 정보도 제공합니다. (이 항목이 구성될 때 게시되는 내용에 AWS Config대해 자세히 알아보십시오.)
- `aws-controltower-BaselineCloudTrail`트레일의 데이터 이벤트는 `aws-controltower-AllConfigNotifications` SNS 주제에도 게시되도록 설정됩니다.
- 자세한 규정 준수 알림을 받으려면 `aws-controltower-AllConfigNotifications` SNS 주제를 구독하는 것이 좋습니다. 이 주제에서는 모든 자녀 계정의 규정 준수 알림을 집계합니다.
- 드리프트 알림 및 기타 알림과 규정 준수 알림을 수신하되 전체적으로 알림 수를 줄이려면 `aws-controltower-AggregateSecurityNotifications` SNS 주제를 구독하는 것이 좋습니다.
- AWS Control Tower Account Factory for Terraform (AFT) 오류에 대한 알림을 받으려면 AFT 리포지토리에 나와 있는 라는 aft_failure_notificationsSNS 주제를 구독하면 됩니다. 예:

```
resource "aws_sns_topic" "aft_failure_notifications" {
    name = "aft-failure-notifications"
    kms_master_key_id = "alias/aws/sns"
}
```

- 모든 SNS 주제는 디스크 암호화를 통해 유휴 상태에서 암호화됩니다. 자세한 내용은 데이터 암호화를 참조하십시오.

SNS 주제 및 규정 준수에 대한 자세한 내용은 예방 및 알림을 참조하십시오.

KMS 키에 대한 지침

AWS Control Tower는 AWS Key Management Service (AWS KMS) 와 함께 작동합니다. 원하는 경우, 관리하는 암호화 키를 사용하여 AWS Control Tower 리소스를 암호화하고 복호화하려는 경우 생성 및

구성할 수 있습니다. AWS KMS keys랜딩 존을 업데이트할 때마다 KMS 키를 추가하거나 변경할 수 있습니다. 가장 좋은 방법은 자체 KMS 키를 사용하고 수시로 변경하는 것입니다.

AWS KMS 다중 지역 KMS 키와 비대칭 키를 생성할 수 있습니다. 하지만 AWS Control Tower는 다중 지역 키 또는 비대칭 키를 지원하지 않습니다. AWS Control Tower는 기존 키의 사전 검사를 수행합니다. 멀티 리전 키 또는 비대칭 키를 선택하면 오류 메시지가 표시될 수 있습니다. 이 경우 AWS Control Tower 리소스와 함께 사용할 다른 키를 생성하십시오.

AWS CloudHSM 클러스터를 운영하는 고객의 경우: CloudHSM 클러스터와 연결된 사용자 지정 키 스토어를 생성하십시오. 그런 다음 생성한 CloudHSM 사용자 지정 키 스토어에 있는 KMS 키를 생성할 수 있습니다. 이 KMS 키를 AWS 컨트롤 타워에 추가할 수 있습니다.

KMS 키가 AWS Control Tower에서 작동하도록 하려면 KMS 키의 권한 정책을 구체적으로 업데이트해야 합니다. 자세한 내용은 라는 KMS 키 정책 업데이트 섹션을 참조하십시오.

AI 기반 서비스 및 AWS 컨트롤 타워

AI 기반 서비스가 데이터를 저장하지 않도록 선택할 수 있는 서비스 제어 정책 (SCP) 을 만들 수 있습니다. AWS이러한 SCP 정책은 Amazon Rekognition 또는 Amazon과 같은 AI 기반 서비스가 사용자 데이터를 저장하고 다른 AI 기반 서비스를 개선하는 CodeWhisperer 데 사용할 수 없도록 규정합니다. AWS

이러한 AI 옵트아웃 SCP 정책은 조직 전체, OU 또는 특정 계정에 적용할 수 있습니다. 정책은 전 세계적으로 유효합니다. 이러한 정책에 대한 자세한 내용은 AWS Organizations 설명서의 AI 서비스 옵트아웃 정책에서 확인할 수 있습니다.

정책 예와 함께 AI를 사용하는 AWS 서비스 목록은 사용 AWS Organizations 설명서의 AI 서비스 옵트아웃 정책 구문 및 예를 참조하십시오.

AWS Control Tower에서의 구성 업데이트 관리

Landing Zone을 최신 상태로 유지하는 것은 중앙 클라우드 관리자 팀 구성원의 책임입니다. 랜딩 존을 업데이트하면 AWS Control Tower에 패치가 적용되고 업데이트됩니다. 또한 잠재적인 규정 준수 문제로부터 랜딩 존을 보호하려면 중앙 클라우드 관리자 팀 구성원이 드리프트 문제가 감지되고 보고되는 즉시 해결해야 합니다.

> **Note**
>
> AWS Control Tower 콘솔은 랜딩 존을 업데이트해야 하는 시기를 알려줍니다. 업데이트 옵션이 보이지 않는 경우, landing zone이 이미 최신 상태인 것입니다.

다음 표에는 AWS Control Tower 랜딩 존 업데이트 릴리스 목록과 각 릴리스에 대한 설명 링크가 포함되어 있습니다.

버전	릴리스 날짜	설명
3.3	12-12-2023	랜딩 존 버전 3.3
3.2	6-09-2023	랜딩 존 버전 3.2
3.1	2-09-2023	랜딩 존 버전 3.1
3.0	7-26-2022	랜딩 존 버전 3.0
2.9	4-22-2022	랜딩 존 버전 2.9
2.8	2-10-2022	랜딩 존 버전 2.8
2.7	4-8-2021	랜딩 존 버전 2.7
2.6	2020년 12월 29일	랜딩 존 버전 2.6
2.5	11월 18일 (2020년 11월 18일)	랜딩 존 버전 2.5
2.4	None	None
2.3	3-5-2020	랜딩 존 버전 2.3

버전	릴리스 날짜	설명
2.2	11-13-19	랜딩 존 버전 2.2
2.1	6-24-19	랜딩 존 버전 2.1

랜딩 존을 업데이트할 때마다 랜딩 존 설정을 수정할 수 있습니다.

업데이트의 이점

- 관리 지역을 변경할 수 있습니다.
- 로그 보존 정책을 변경할 수 있습니다.
- 지역 거부 제어를 추가 또는 제거할 수 있습니다.
- AWS KMS 암호화 키를 적용할 수 있습니다.
- 조직 CloudTrail 수준 트레일을 활성화하거나 비활성화할 수 있습니다.
- Landding Zone 드리프트를 해결할 수 있습니다

랜딩 존을 업데이트하면 AWS Control Tower의 최신 기능을 자동으로 받게 됩니다. 랜딩 존 설정 페이지에서 현재 랜딩 존 버전을 확인하세요.

업데이트가 실패하는 경우, AWS Control Tower는 이전 랜딩 존 버전으로 롤백하지 않습니다. 착륙 지대가 불확실한 상태일 수 있습니다. 그렇다면 지원팀에 문의하세요 AWS . 업데이트 실패 문제 해결에 대한 자세한 내용은 을 참조하십시오랜딩 존을 업데이트할 수 없습니다..

랜딩 존을 업데이트할 때 사용하지 않는 AWS Identity center (이전 명칭 AWS SSO) 매핑을 지울 수 있습니다. 자세한 내용은 필드 노트: AWS Control Tower 업그레이드 중에 사용하지 않는 IAM ID 센터 매핑을 자동으로 지우십시오.

> 업데이트 및 재설정을 위한 사전 요구 사항 — 요청자 지불 해제
>
> 랜딩 존을 업데이트하거나 재설정하기 전에 Log Archive 계정의 Amazon S3 로깅 버킷에 요청자 지불 기능이 활성화되어 있지 않은지 확인하십시오. 업데이트 또는 재설정 프로세스를 시작하기 전에 해당 기능을 꺼야 합니다. AWS Control Tower가 로깅 버킷을 설정할 때는 이 기능이 활성화되지 않습니다. 따라서 이후에 요청자 지불 기능을 활성화한 고객만 이 기능을 사용 중지해야 합니다. 자세한 내용은 요청자 지불 버킷에 대한 Amazon S3 버킷 정책 CloudTrail 및 사용을 참조하십시오.

업데이트

거버넌스 드리프트를 수정하거나 새 버전의 AWS Control Tower로 이동하려면 업데이트가 필요합니다. AWS Control Tower를 완전히 업데이트하려면 먼저 랜딩 존을 업데이트한 다음 등록된 계정을 개별적으로 업데이트해야 합니다. 경우에 따라 다음 세 가지 유형의 업데이트를 수행해야 할 수 있습니다.

- 랜딩 존 업데이트: 대부분의 경우 이러한 유형의 업데이트는 랜딩 존 설정 페이지에서 업데이트를 선택하여 수행됩니다. 특정 유형의 드리프트를 해결하려면 landing Zone 업데이트를 수행해야 할 수 있으며 필요한 경우 Reset을 선택할 수 있습니다.
- 하나 이상의 개별 계정 업데이트: 연결된 정보가 변경되거나 특정 유형의 드리프트가 발생한 경우 계정을 업데이트해야 합니다. 계정에 업데이트가 필요한 경우 계정 페이지에 계정 상태에 업데이트 가능 여부가 표시됩니다.

  단일 계정을 업데이트하려면 계정 세부 정보 페이지로 이동한 다음 계정 업데이트를 선택합니다. 또한 이 페이지의 뒷부분에 설명된 수동 프로세스, OU 재등록 선택 또는 자동 스크립팅 접근 방식을 사용하여 계정을 업데이트할 수도 있습니다.
- 전체 업데이트: 전체 업데이트에서는 먼저 랜딩 영역을 업데이트한 후 등록된 OU에 있는 등록된 모든 계정을 업데이트합니다. 2.9, 3.0 등과 같은 AWS Control Tower의 새 릴리스에는 전체 업데이트가 필요합니다.

> **Note**
>
> Landing Zone 업데이트를 완료한 후에는 업데이트를 취소하거나 이전 버전으로 다운그레이드할 수 없습니다.

랜딩 영역 업데이트

AWS Control Tower 랜딩 존을 업데이트하는 가장 쉬운 방법은 랜딩 존 설정 페이지를 이용하는 것입니다. 이 페이지는 AWS Control Tower 대시보드의 왼쪽 탐색 영역에서 랜딩 존 설정을 선택하여 액세스할 수 있습니다.

Landing zone 설정 페이지에는 현재 버전의 landding Zone이 표시되며 사용 가능한 모든 업데이트된 버전이 나열됩니다. 버전을 업데이트해야 하는 경우 업데이트 버튼을 이용할 수 있습니다.

> **Note**
>
> 또는 랜딩 존을 수동으로 업데이트할 수 있습니다. 업데이트 버튼을 사용하든 수동 프로세스를 사용하든 업데이트에 소요되는 시간은 거의 동일합니다. 랜딩 영역의 수동 업데이트만 수행하려면 아래 1단계와 2단계를 참조하십시오.

수동 업데이트

다음 절차는 AWS Control Tower의 전체 업데이트 단계를 수동으로 안내합니다. 개별 계정을 업데이트하려면 을 참조하십시오콘솔에서 계정 업데이트.

OU당 계정 수에 관계없이 랜딩 존을 수동으로 업데이트하려면

1. 웹 브라우저를 열고 https://console.aws.amazon.com/controltower/home/update 에서 AWS Control Tower 콘솔로 이동합니다.
2. 마법사의 정보를 검토하고 업데이트를 선택합니다. 이렇게 하면 landing zone의 백엔드와 공유 계정이 업데이트됩니다. 이 프로세스는 30분 이상 걸릴 수 있습니다.
3. 구성원 계정을 업데이트하십시오 (계정이 300개가 넘는 OU의 경우 이 절차를 따라야 함).
4. 왼쪽 탐색 창에서 조직을 선택합니다.
5. 각 계정을 업데이트하려면 에 나와 있는 단계를 따르십시오콘솔에서 계정 업데이트.

> **필요한 경우 OU를 재등록하여 계정을 업데이트합니다.**
>
> 계정이 300개 미만인 등록된 AWS Control Tower OU의 경우 대시보드의 OU 페이지로 이동하여 OU 재등록을 선택하여 해당 OU의 계정을 업데이트할 수 있습니다.

재설정 및 재등록을 통해 드리프트를 해결하십시오.

사용자와 조직 구성원이 randing Zone을 사용할 때 드리프트가 자주 발생합니다.

AWS Control Tower에서는 드리프트 감지가 자동으로 이루어집니다. SCP를 자동으로 스캔하면 변경 사항이 필요한 리소스 또는 편차 해결을 위해 구성 업데이트가 필요한 리소스를 식별할 수 있습니다.

대부분의 유형의 드리프트를 복구하려면 랜딩 존 설정 페이지에서 재설정을 선택하십시오. 또한 OU 재등록을 선택하여 일부 유형의 드리프트를 해결할 수 있습니다. 드리프트 유형 및 해결 방법에 대한

자세한 내용은 및 을 참조하십시오. 거버넌스 드리프트 유형 AWS Control Tower의 드리프트 감지 및 해결

역할 드리프트의 경우 한 가지 특별한 드리프트 해결이 발생합니다. 필수 역할을 사용할 수 없는 경우 콘솔에 경고 페이지와 역할 복원 방법에 대한 몇 가지 지침이 표시됩니다. 역할 드리프트가 해결되기 전까지는 Landding Zone을 사용할 수 없습니다. 이 드리프트 리셋은 풀 랜딩 존 리셋과 다릅니다. 자세한 내용은 라는 즉시 해결해야 할 드리프트 유형 섹션의 필수 역할 삭제 안 함을 참조하십시오.

⚠ Landding Zone 버전에서 드리프트를 해결하기 위한 조치를 취하면 두 가지 동작이 가능합니다.

- 최신 랜딩 존 버전을 사용 중인 경우 Reset을 선택한 다음 Confirm (확인) 을 선택하면 드리프트된 랜딩 존 리소스가 저장된 AWS Control Tower 구성으로 재설정됩니다. Landding Zone 버전은 동일하게 유지됩니다.
- 최신 버전을 사용하고 있지 않은 경우 업데이트를 선택해야 합니다. 랜딩 존이 최신 랜딩 존 버전으로 업그레이드되었습니다. 이 프로세스의 일부로 드리프트가 해결되었습니다.

자동화를 사용하여 계정을 프로비저닝하고 업데이트합니다.

다음과 같은 몇 가지 방법으로 AWS Control Tower에서 개별 계정을 프로비저닝하거나 업데이트할 수 있습니다.

- AWS Control Tower Account Factory for Terraform (AFT) 을 사용하여 계정을 프로비저닝하고 사용자 지정할 수 있습니다. 자세한 정보는 테라폼용 AWS Control Tower 어카운트 팩토리 (AFT) 개요을 참조하세요.
- AWS Control Tower (cFCT) 에 대한 사용자 지정을 사용하여 계정을 업데이트할 수 있습니다. 자세한 정보는 AWS 컨트롤 타워 (cFCT) 에 대한 사용자 지정 개요 을 참조하세요.
- 스크립트 자동화: API 접근 방식을 선호하는 경우 Service Catalog의 API 프레임워크를 사용하여 계정을 업데이트한 다음 AWS CLI 일괄 프로세스로 계정을 업데이트할 수 있습니다. 각 계정에 대해 Service Catalog의 `UpdateProvisionedProduct`API를 호출합니다. 이 API를 사용하여 계정을 하나씩 업데이트하는 스크립트를 작성할 수 있습니다. 거버넌스를 위한 지역을 추가할 때 이 접근 방식에 대한 자세한 내용은 블로그 게시물인 새 AWS 지역의 가드레일 활성화에서 확인할 수 있습니다.

  한 번에 최대 다섯 (5) 개의 계정을 업데이트할 수 있습니다. 다음 계정 업데이트를 시작하기 전에 최소한 한 번의 계정 업데이트가 완료될 때까지 기다려야 합니다. 따라서 계정이 많은 경우 프로세스가

오래 걸릴 수 있지만 복잡하지는 않습니다. 이 방법에 대한 자세한 내용은 둘러보기: Service Catalog API를 이용한 AWS Control Tower의 계정 프로비저닝 자동화 단원을 참조하십시오.

> **비디오 안내**
>
> 비디오 안내는 스크립트를 사용한 자동 계정 프로비저닝을 위해 설계되었지만 이 단계는 계정 업데이트에도 적용됩니다. `UpdateProvisionedProduct`API 대신 API를 `ProvisionProduct` 사용하세요.

스크립트를 통한 자동화의 다음 단계는 AWS Control Tower **`UpdateLandingZone`** 수명 주기 이벤트의 Success 상태를 확인하는 것입니다. 동영상에 설명된 대로 이를 트리거로 사용하여 개별 계정 업데이트를 시작하십시오. 라이프사이클 이벤트는 일련의 활동이 완료되었음을 나타내므로 이 이벤트가 발생하면 landing zone 업데이트가 완료됩니다. 계정 업데이트를 시작하기 전에 랜딩 영역 업데이트를 완료해야 합니다. 수명 주기 이벤트 작업에 대한 자세한 내용은 수명 주기 이벤트를 참조하십시오.

다음 섹션도 참조하세요.

- AWS CloudShell 작업에 사용 AWS Control Tower.
- AWS Control Tower에서의 작업 자동화 .

AWS Control Tower에서의 작업 자동화

많은 고객이 계정 프로비저닝, 제어 할당 및 감사와 같은 작업을 AWS Control Tower에서 자동화하는 것을 선호합니다. 다음과 같은 호출을 통해 이러한 자동 작업을 설정할 수 있습니다.

- AWS Service Catalog API
- AWS Organizations API
- AWS 컨트롤 타워 API
- AWS CLI

이 관련 정보 페이지에는 AWS Control Tower에서 작업을 자동화하는 데 도움이 되는 많은 훌륭한 기술 블로그 게시물로 연결되는 링크가 포함되어 있습니다. 다음 섹션에는 이 AWS Control Tower 사용 설명서에서 작업 자동화에 도움이 되는 영역으로 연결되는 링크가 제공됩니다.

제어 작업 자동화

AWS Control Tower API를 통해 제어 (가드레일이라고도 함) 의 적용 및 제거와 관련된 작업을 자동화할 수 있습니다. 자세한 내용은 AWS Control Tower API 레퍼런스를 참조하십시오.

AWS Control Tower API를 사용하여 제어 작업을 수행하는 방법에 대한 자세한 내용은 조직 단위에 사전 정의된 제어 기능인 AWS Control Tower 릴리스 API라는 블로그 게시물을 참조하십시오.

랜딩 존 작업 자동화

AWS Control Tower 랜딩 존 API는 랜딩 존과 관련된 특정 작업을 자동화하는 데 도움이 됩니다. 자세한 내용은 AWS Control Tower API 레퍼런스를 참조하십시오.

OU 등록 자동화

AWS Control Tower 기본 API는 OU 등록과 같은 특정 작업을 자동화하는 데 도움이 됩니다. 자세한 내용은 AWS Control Tower API 레퍼런스를 참조하십시오.

자동 계정 폐쇄

AWS Organizations API를 사용하여 AWS Control Tower 회원 계정을 자동으로 폐쇄할 수 있습니다. 자세한 정보는 다음을 통해 AWS Control Tower 회원 계정을 폐쇄하십시오. AWS Organizations을 참조하세요.

자동 계정 프로비저닝 및 업데이트

AWS Control Tower 어카운트 팩토리 사용자 지정 (AFC) 을 사용하면 AWS Control Tower 콘솔에서 블루프린트라고 하는 사용자 지정 AWS CloudFormation 템플릿을 사용하여 계정을 생성할 수 있습니다. 이 프로세스는 단일 블루프린트를 설정한 후 파이프라인을 유지 관리할 필요 없이 새 계정을 생성하고 계정을 반복적으로 업데이트할 수 있다는 점에서 자동화됩니다.

AWS Control Tower Account Factory for Terraform (AFT) 은 AWS Control Tower의 계정 프로비저닝 및 계정 업데이트 프로세스를 자동화하는 GitOps 모델을 따릅니다. 자세한 정보는 테라폼용 AWS Control Tower 어카운트 팩토리 (AFT) 를 통해 계정 프로비저닝 을 참조하세요.

AWS Control Tower (cFCT) 에 대한 사용자 지정을 통해 AWS Control Tower 랜딩 존을 사용자 지정하고 모범 사례를 준수할 수 있습니다. AWS 사용자 지정은 AWS CloudFormation 템플릿과 서비스 제어 정책 (SCP) 으로 구현됩니다. 자세한 정보는 AWS 컨트롤 타워 (cFCT) 에 대한 사용자 지정 개요 을 참조하세요.

자동 계정 프로비저닝에 대한 자세한 내용과 동영상은 안내: AWS Control Tower의 자동 계정 프로비저닝 및 IAM 역할을 사용한 자동 프로비저닝을 참조하십시오.

스크립트별 계정 업데이트도 참조하십시오.

프로그래밍 방식의 계정 감사

프로그래밍 방식으로 계정을 감사하는 방법에 대한 자세한 내용은 AWS Control Tower 감사 계정의 프로그래밍 역할 및 신뢰 관계를 참조하십시오.

기타 작업 자동화

자동 요청 방법으로 특정 AWS Control Tower 서비스 할당량을 늘리는 방법에 대한 자세한 내용은 다음 동영상을 참조하십시오. 자동 서비스 한도 증가.

자동화 및 통합 사용 사례를 다루는 기술 블로그는 자동화 및 통합을 참조하십시오.

에는 보안과 관련된 특정 자동화 작업에 도움이 되는 두 개의 오픈 소스 샘플이 있습니다. GitHub

- aws-control-tower-org-setup-sample이라는 샘플은 보안 관련 서비스의 위임 관리자로서 감사 계정을 자동으로 설정하는 방법을 보여줍니다.
- aws-control-tower-account-라는 샘플은 새 계정을 프로비저닝하고 구성할 때 Step Functions를 사용하여 보안 모범 사례를 자동화하는 방법을 setup-using-step-functions 보여줍니다. 이 샘플에는 조직 공유 AWS Service Catalog 포트폴리오에 보안 주체를 추가하고 조직 전체의 IAM Identity Center 그룹을 새 계정에 자동으로 연결하는 작업이 포함됩니다. AWS 또한 모든 지역에서 기본 VPC를 삭제하는 방법도 설명합니다.

AWS 보안 참조 아키텍처에는 AWS Control Tower와 관련된 작업을 자동화하기 위한 코드 예제가 포함되어 있습니다. 자세한 내용은 AWS 규범 지침 페이지 및 관련 리포지토리를 참조하십시오. GitHub

CLI에서의 작업을 용이하게 해주는 AWS CloudShell AWS 서비스인 AWS Control Tower를 사용하는 방법에 대한 자세한 내용은 AWS CLI를AWS CloudShell AWS 참조하십시오.

AWS Control Tower는 오케스트레이션 레이어이기 때문에 API와 AWS CLI를 통해 다른 많은 AWS 서비스를 사용할 수 있습니다. AWS Organizations자세한 내용은 관련 서비스를 참조하십시오. AWS

AWS CloudShell 작업에 사용 AWS Control Tower

AWS CloudShell AWS CLI에서 작업을 용이하게 해주는 AWS 서비스로서, 브라우저 기반의 사전 인증된 셸로서 에서 직접 실행할 수 있습니다. AWS Management Console명령줄 도구를 다운로드하거나 설치할 필요가 없습니다. 원하는 셸 (Bash PowerShell 또는 Z 셸) 에서 AWS CLI 명령 AWS Control Tower 및 기타 AWS 서비스를 실행할 수 있습니다.

AWS CloudShell 에서 실행하면 콘솔에 AWS Management Console 로그인하는 데 사용한 AWS 자격 증명을 새 셸 세션에서 사용할 수 있습니다. 다른 AWS 서비스와 상호 작용할 AWS Control Tower 때는 구성 자격 증명을 입력하지 않아도 됩니다. 그러면 셸의 컴퓨팅 환경에 사전 설치된 AWS CLI 버전 2를 사용하게 됩니다. 사전 인증을 받은 것입니다. AWS CloudShell

IAM 권한 취득 대상 AWS CloudShell

AWS Identity and Access Management 관리자가 IAM 사용자 및 IAM Identity Center 사용자에게 액세스 권한을 부여할 수 있는 액세스 관리 리소스를 제공합니다. AWS CloudShell

관리자가 사용자에게 액세스 권한을 부여하는 가장 빠른 방법은 관리형 AWS 정책을 사용하는 것입니다. AWS 관리형 정책은 AWS에서 생성 및 관리하는 독립 실행형 정책입니다. 다음과 같은 AWS 관리형 정책을 IAM ID에 연결할 CloudShell 수 있습니다.

- `AWSCloudShellFullAccess`: 모든 기능에 대한 전체 액세스 AWS CloudShell 권한과 함께 사용할 수 있는 권한을 부여합니다.

IAM 사용자 또는 IAM Identity Center 사용자가 수행할 수 있는 작업의 범위를 제한하려는 경우 `AWSCloudShellFullAccess` 관리형 정책을 템플릿으로 AWS CloudShell사용하는 사용자 지정 정책을 생성할 수 있습니다. 에서 CloudShell 사용자가 수행할 수 있는 작업을 제한하는 방법에 대한 자세한 내용은 사용 설명서의 IAM 정책을 통한 AWS CloudShell 액세스 및 사용 관리를 참조하십시오.AWS CloudShell

> **Note**
>
> 또한 IAM ID에는 호출 권한을 부여하는 정책이 필요합니다. AWS Control Tower자세한 내용은 AWS Control Tower 콘솔 사용에 필요한 권한을 참조하십시오.

사용과 상호 작용하기 AWS Control TowerAWS CloudShell

AWS CloudShell 에서 시작한 후에는 명령줄 인터페이스에서 즉시 상호 AWS Control Tower 작용을 시작할 수 있습니다. AWS Management Console AWS CLI 명령은 에서 표준 방식으로 작동합니다 CloudShell.

> **Note**
>
> AWS CLI AWS CloudShellin을 사용하면 추가 리소스를 다운로드하거나 설치할 필요가 없습니다. 셸 내에서 이미 인증되었으므로 전화를 걸기 전에 자격 증명을 구성할 필요가 없습니다.

시작 AWS CloudShell

- 에서 탐색 표시줄에서 사용할 수 있는 다음 옵션을 CloudShell 선택하여 시작할 수 있습니다. AWS Management Console
  - CloudShell 아이콘을 선택합니다.
  - 검색 상자에 “cloudshell”을 입력하기 시작한 다음 옵션을 선택합니다. CloudShell

  이제 CloudShell 시작했으니 작업에 필요한 모든 AWS CLI 명령을 입력할 수 있습니다. AWS Control Tower예를 들어, AWS Config 상태를 확인할 수 있습니다.

설정에 도움이 되는 AWS CloudShell 데 사용 AWS Control Tower

이 절차를 수행하기 전에 달리 명시되지 않는 한, 랜딩 존의 홈 리전에 로그인하고 랜딩 존이 포함된 관리 계정에 대한 관리자 권한을 가진 IAM Identity Center 사용자 또는 IAM 사용자로 로그인해야 합니다. AWS Management Console

1. 다음은 AWS Control Tower landing Zone 구성을 시작하기 전에 AWS Config CLI 명령을 사용하여 컨피그레이션 레코더 및 전송 채널의 상태를 확인하는 방법입니다. AWS CloudShell

상태를 확인하세요. AWS Config

보기 명령:

- `aws configservice describe-delivery-channels`
- `aws configservice describe-delivery-channel-status`
- `aws configservice describe-configuration-recorders`
- `The normal response is something like "name": "default"`

2. AWS Control Tower Landing Zone을 설정하기 전에 삭제해야 하는 기존 AWS Config 레코더 또는 전송 채널이 있는 경우 다음과 같은 명령을 입력할 수 있습니다.

   기존 AWS Config 리소스 관리

   삭제 명령:

   - `aws configservice stop-configuration-recorder --configuration-recorder-name NAME-FROM-DESCRIBE-OUTPUT`
   - `aws configservice delete-delivery-channel --delivery-channel-name NAME-FROM-DESCRIBE-OUTPUT`
   - `aws configservice delete-configuration-recorder --configuration-recorder-name NAME-FROM-DESCRIBE-OUTPUT`

   > **Important**
   >
   > AWS Config에 대한 AWS Control Tower 리소스를 삭제하지 마십시오. 이러한 리소스가 손실되면 AWS Control Tower 일관성 없는 상태가 될 수 있습니다.

   자세한 내용은 AWS Config 설명서를 참조하십시오.

   - 구성 레코더 관리(AWS CLI)
   - 전송 채널 관리

3. 이 예에서는 신뢰할 수 있는 액세스를 활성화하거나 AWS CloudShell 비활성화하기 위해 입력하는 AWS CLI 명령을 보여줍니다. AWS Organizations신뢰할 AWS Control Tower 수 있는 액세스를 활성화하거나 비활성화할 필요가 없으므로 이는 예시일 뿐입니다. AWS Organizations하지만

에서 작업을 자동화하거나 사용자 지정하는 경우 다른 AWS 서비스에 대해 신뢰할 수 있는 액세스를 활성화하거나 비활성화해야 할 수 있습니다. AWS Control Tower

신뢰할 수 있는 서비스 액세스를 활성화 또는 비활성화합니다.

- `aws organizations enable-aws-service-access`
- `aws organizations disable-aws-service-access`

다음을 사용하여 Amazon S3 버킷을 생성합니다. AWS CloudShell

다음 예제에서는 를 AWS CloudShell 사용하여 Amazon S3 버킷을 만든 다음 PutObject메서드를 사용하여 코드 파일을 해당 버킷의 객체로 추가할 수 있습니다.

1. 지정된 AWS 지역에 버킷을 생성하려면 명령줄에 다음 CloudShell 명령을 입력합니다.

```
aws s3api create-bucket --bucket insert-unique-bucket-name-here --region us-east-1
```

직접 호출이 성공하면 명령줄에 다음 출력과 비슷한 서비스의 응답이 표시됩니다.

```
{
    "Location": "/insert-unique-bucket-name-here"
}
```

> **Note**
>
> 버킷 이름 지정 규칙 (예: 소문자만 사용) 을 준수하지 않으면 다음 오류가 표시됩니다. CreateBucket 작업을 호출하는 동안 오류가 발생했습니다 (InvalidBucketName). 지정된 버킷이 유효하지 않습니다.

2. 파일을 업로드하고 방금 만든 버킷에 객체로 추가하려면 메서드를 호출하십시오. PutObject

```
aws s3api put-object --bucket insert-unique-bucket-name-here --key add_prog --body
 add_prog.py
```

객체가 Amazon S3 버킷에 성공적으로 업로드되면 명령줄에 다음 출력과 유사한 서비스의 응답이 표시됩니다.

```
{
```

```
            "ETag": "\"ab123c1:w:wad4a567d8bfd9a1234ebeea56\""}
```

저장된 객체의 해시입니다. ETag Amazon S3에 업로드된 객체의 무결성을 확인하는 데 사용할 수 있습니다.

를 사용하여 AWS Control Tower 리소스 생성 AWS CloudFormation

AWS Control Tower 와 AWS CloudFormation통합되어 리소스를 모델링하고 설정하는 데 도움이 되므로 AWS 리소스와 인프라를 만들고 관리하는 데 소요되는 시간을 줄일 수 있습니다. 컨트롤과 같이 AWS::ControlTower::EnabledControl 원하는 모든 AWS 리소스를 설명하는 템플릿을 만듭니다. AWS CloudFormation 이러한 리소스를 자동으로 프로비저닝하고 구성합니다.

를 사용하면 AWS CloudFormation템플릿을 재사용하여 AWS Control Tower 리소스를 일관되고 반복적으로 설정할 수 있습니다. 리소스를 한 번 설명한 다음 여러 AWS 계정 지역과 지역에서 동일한 리소스를 반복해서 프로비저닝하세요.

AWS Control Tower 및 AWS CloudFormation 템플릿

리소스 AWS Control Tower 및 관련 서비스를 프로비저닝하고 구성하려면 AWS CloudFormation 템플릿을 이해해야 합니다. 템플릿은 JSON 또는 YAML로 서식 지정된 텍스트 파일입니다. 이러한 템플릿은 AWS CloudFormation 스택에 프로비저닝하려는 리소스를 설명합니다. JSON이나 YAML에 익숙하지 않은 경우 AWS CloudFormation Designer를 사용하여 템플릿을 시작하는 데 도움을 받을 수 있습니다. AWS CloudFormation 자세한 내용은 AWS CloudFormation 사용 설명서에서 AWS CloudFormation Designer이란 무엇인가요?를 참조하세요.

AWS Control Tower 에서 AWS::ControlTower::EnabledControl (제어 리소스), AWS::ControlTower::LandingZone (랜딩 영역) 및 AWS::ControlTower::EnabledBaseline (베이스라인) 생성을 지원합니다. AWS CloudFormation이러한 리소스 유형에 대한 JSON 및 YAML 템플릿의 예를 비롯한 자세한 내용은 사용 설명서의 내용을 참조하십시오 AWS Control Tower.AWS CloudFormation

> **Note**
>
> 동시 작업 수 EnableControl 및 DisableControl 업데이트는 100개의 동시 AWS Control Tower 작업이며, 이 중 사전 예방적 제어와 관련된 작업은 최대 20개입니다.

CLI 및 콘솔에 대한 몇 가지 AWS Control Tower 예를 보려면 제어 활성화를 참조하십시오. AWS CloudFormation

에 대해 자세히 알아보십시오. AWS CloudFormation

자세히 AWS CloudFormation알아보려면 다음 리소스를 참조하십시오.

- AWS CloudFormation
- AWS CloudFormation 사용 설명서
- AWS CloudFormation API 참조
- AWS CloudFormation 명령줄 인터페이스 사용 설명서

AWS Control Tower 랜딩 존을 사용자 지정하십시오

지역 선택 및 선택적 제어와 같은 AWS Control Tower 랜딩 존의 특정 측면은 콘솔에서 구성할 수 있습니다. 자동화를 통해 콘솔 외부에서 기타 변경 사항을 적용할 수 있습니다.

예를 들어, AWS CloudFormation 템플릿 및 AWS Control Tower 수명 주기 이벤트와 함께 작동하는 GitOps 스타일 사용자 지정 프레임워크인 AWS Control Tower 사용자 지정 기능을 사용하여 랜딩 존을 보다 광범위하게 사용자 지정할 수 있습니다.

AWS Control Tower 콘솔에서 사용자 지정

랜딩 존을 사용자 지정하려면 AWS Control Tower 콘솔에서 제공하는 단계를 따르십시오.

설정 중에 사용자 지정된 이름을 선택합니다.

- 설정 중에 최상위 OU 이름을 선택할 수 있습니다. AWS Organizations 콘솔을 사용하여 언제든지 OU 이름을 바꿀 수 있지만 OU를 변경하면 복구 가능한 변동이 AWS Organizations 발생할 수 있습니다.
- 공유 감사 및 로그 아카이브 계정의 이름을 선택할 수 있지만 설정 후에는 이름을 변경할 수 없습니다. (이는 일회성 선택입니다.)

> 도움말
>
> 에서 OU 이름을 변경해도 Account Factory에 프로비저닝된 해당 제품이 업데이트되지는 AWS Organizations 않는다는 점을 기억하십시오. 프로비저닝된 제품을 자동으로 업데이트하고 드리프트를 방지하려면 AWS Control Tower를 통해 OU 생성, 삭제 또는 재등록을 포함한 OU 작업을 수행해야 합니다.

지역 AWS 선택

- 거버넌스를 위한 특정 AWS 지역을 선택하여 랜딩 존을 사용자 지정할 수 있습니다. AWS Control Tower 콘솔의 단계를 따르십시오.
- 랜딩 존을 업데이트할 때 거버넌스 대상 AWS 지역을 선택하거나 선택 취소할 수 있습니다.
- 지역 거부 제어를 사용 또는 사용 안 함으로 설정하고 관리되지 않는 지역의 대부분의 AWS 서비스에 대한 사용자 액세스를 제어할 수 있습니다. AWS

cFCT에 배포 제한이 AWS 리전 있는 위치에 대한 자세한 내용은 을 참조하십시오. 관리 제한

선택적 컨트롤을 추가하여 사용자 지정하십시오.

- 강력히 권장되는 컨트롤과 선택적 컨트롤은 선택 사항이므로 어느 것을 활성화할지 선택하여 랜딩 존의 적용 수준을 사용자 지정할 수 있습니다. 선택적 제어는 기본적으로 활성화되어 있지 않습니다.
- 선택적 데이터 레지던시 제어를 사용하면 데이터를 저장하고 데이터에 대한 액세스를 허용할 지역을 사용자 지정할 수 있습니다.
- 통합 Security Hub 표준에 속하는 선택적 제어를 사용하면 AWS Control Tower 환경을 스캔하여 보안 위험을 확인할 수 있습니다.
- 선택적 사전 제어를 사용하면 리소스가 프로비저닝되기 전에 AWS CloudFormation 리소스를 확인하여 새 리소스가 환경의 제어 목표를 준수하는지 확인할 수 있습니다.

트레일을 사용자 지정하세요. AWS CloudTrail

- 랜딩 존을 버전 3.0 이상으로 업데이트하면 AWS Control Tower에서 관리하는 조직 수준 CloudTrail 트레일을 옵트인하거나 옵트아웃할 수 있습니다. landing Zone을 업데이트할 때마다 이 선택을 변경할 수 있습니다. AWS Control Tower는 관리 계정에 조직 수준의 트레일을 생성하며, 이 트레일은 선택에 따라 활성 또는 비활성 상태로 전환됩니다. 랜딩 존 3.0은 계정 수준 CloudTrail 트레일을 지원하지 않지만, 필요한 경우 자체 트레일을 구성하고 관리할 수 있습니다. 트레일이 중복되면 추가 비용이 발생할 수 있습니다.

콘솔에서 사용자 지정 멤버 계정을 만드세요.

- AWS Control Tower 콘솔에서 사용자 지정된 AWS Control Tower 멤버 계정을 생성하고 기존 멤버 계정을 업데이트하여 사용자 지정을 추가할 수 있습니다. 자세한 정보는 AFC (Account Factory Customize) 로 계정을 사용자 지정하세요을 참조하세요.

AWS Control Tower 콘솔 외부에서 사용자 지정 자동화

일부 사용자 지정은 AWS Control Tower 콘솔을 통해 사용할 수 없지만 다른 방법으로 구현할 수 있습니다. 예:

- Account Factory for Terraform (AFT) 을 사용하여 프로비저닝 중에 GitOps -스타일 워크플로우에서 계정을 사용자 지정할 수 있습니다.

  AFT는 AFT 리포지토리에서 사용할 수 있는 Terraform 모듈과 함께 배포됩니다.

- AWS CloudFormation 템플릿과 서비스 제어 정책 (SCP) 을 기반으로 구축된 기능 패키지인 AWS Control Tower 사용자 지정 (cFCT) 을 사용하여 AWS Control Tower 랜딩 존을 사용자 지정할 수 있습니다. 사용자 지정 템플릿과 정책을 조직 내 개별 계정 및 조직 단위 (OU) 에 배포할 수 있습니다.

  CFCT의 소스 코드는 저장소에서 사용할 수 있습니다. GitHub

AWS Control Tower (cFCT) 에 대한 사용자 지정의 이점

AWS Control Tower 사용자 지정 (cFCT) 이라고 하는 기능 패키지를 사용하면 AWS Control Tower 콘솔에서 생성할 수 있는 것보다 더 광범위한 랜딩 존 사용자 지정을 생성할 수 있습니다. A GitOps 스타일의 자동화된 프로세스를 제공합니다. 비즈니스 요구 사항에 맞게 landing Zone을 재구성할 수 있습니다.

이 infrastructure-as-code사용자 지정 프로세스는 AWS CloudFormation 템플릿을 AWS 서비스 제어 정책 (SCP) 및 AWS Control Tower 수명 주기 이벤트와 통합하여 리소스 배포가 랜딩 존과 동기화된 상태를 유지하도록 합니다. 예를 들어 Account Factory를 사용하여 새 계정을 생성하면 계정과 OU에 연결된 리소스를 자동으로 배포할 수 있습니다.

> **Note**
>
> Account Factory 및 AFT와 달리 CFCT는 특별히 새 계정을 생성하기 위한 것이 아니라 지정한 리소스를 배포하여 랜딩 존의 계정 및 OU를 사용자 지정하기 위한 것입니다.

이점

- 사용자 지정되고 안전한 AWS 환경 확장 — 다중 계정 AWS Control Tower 환경을 더 빠르게 확장하고 AWS 모범 사례를 반복 가능한 사용자 지정 워크플로에 통합할 수 있습니다.
- 요구 사항 인스턴스화 — 정책 의도를 표현하는 AWS CloudFormation 템플릿 및 서비스 제어 정책을 사용하여 비즈니스 요구 사항에 맞게 AWS Control Tower 랜딩 존을 사용자 지정할 수 있습니다.
- AWS Control Tower 수명 주기 이벤트로 추가 자동화 — 수명 주기 이벤트를 사용하면 이전 일련의 이벤트 완료를 기반으로 리소스를 배포할 수 있습니다. 수명 주기 이벤트를 사용하면 리소스를 계정과 OU에 자동으로 배포할 수 있습니다.
- 네트워크 아키텍처 확장 — 트랜짓 게이트웨이와 같이 연결성을 개선하고 보호하는 맞춤형 네트워크 아키텍처를 배포할 수 있습니다.

추가 cFCT 예제

- AWS Control Tower 사용자 지정 (cFCT) 을 사용한 네트워킹 사용 사례 예시는 AWS 아키텍처 블로그 게시물인 Service Catalog 및 AWS Control Tower 사용자 지정을 통한 일관된 DNS 배포에 나와 있습니다.
- cFCT 및 Amazon과 관련된 구체적인 예는 GuardDuty GitHub 리포지토리에서 확인할 수 있습니다. `aws-samples`
- CFCT와 관련된 추가 코드 예제는 AWS 보안 참조 아키텍처의 일부로 리포지토리에서 사용할 수 있습니다. `aws-samples` 이러한 예제의 대부분은 라는 디렉터리에 샘플 `manifest.yaml` 파일을 포함하고 있습니다. `customizations_for_aws_control_tower`

AWS 보안 참조 아키텍처에 대한 자세한 내용은 AWS 규범적 지침 페이지를 참조하십시오.

AWS 컨트롤 타워 (cFCT) 에 대한 사용자 지정 개요

AWS Control Tower (cFCT) 에 대한 사용자 지정을 통해 AWS Control Tower 랜딩 존을 사용자 지정하고 모범 사례를 준수할 수 있습니다. AWS 사용자 지정은 AWS CloudFormation 템플릿과 서비스 제어 정책 (SCP) 으로 구현됩니다.

이 cFCT 기능은 AWS Control Tower 수명 주기 이벤트와 통합되므로 리소스 배포가 랜딩 존과 동기화된 상태를 유지합니다. 예를 들어 어카운트 팩토리를 통해 새 계정을 생성하면 계정에 연결된 모든 리소스가 자동으로 배포됩니다. 사용자 지정 템플릿과 정책을 조직 내 개별 계정 및 OU (조직 단위) 에 배포할 수 있습니다.

다음 비디오에서는 확장 가능한 cFCT 파이프라인 및 일반적인 cFCT 사용자 지정을 배포하기 위한 모범 사례를 설명합니다.

다음 섹션에서는 AWS Control Tower (cFCT) 용 사용자 지정을 배포하기 위한 아키텍처 고려 사항 및 구성 단계를 제공합니다. 여기에는 보안 및 가용성 AWS 모범 사례에 따라 필요한 AWS 서비스를 시작, 구성 및 실행하는 AWS CloudFormation템플릿 링크가 포함되어 있습니다.

이 주제는 클라우드 아키텍처 설계 실무 경험이 있는 IT 인프라 설계자와 개발자를 대상으로 합니다. AWS

AWS Control Tower 사용자 지정 (cFCT) 의 최신 업데이트 및 변경 사항에 대한 자세한 내용은 리포지토리의 ChangeLog.md 파일을 참조하십시오. GitHub

아키텍처 개요

cFCT를 배포하면 클라우드에 다음과 같은 환경이 구축됩니다. AWS

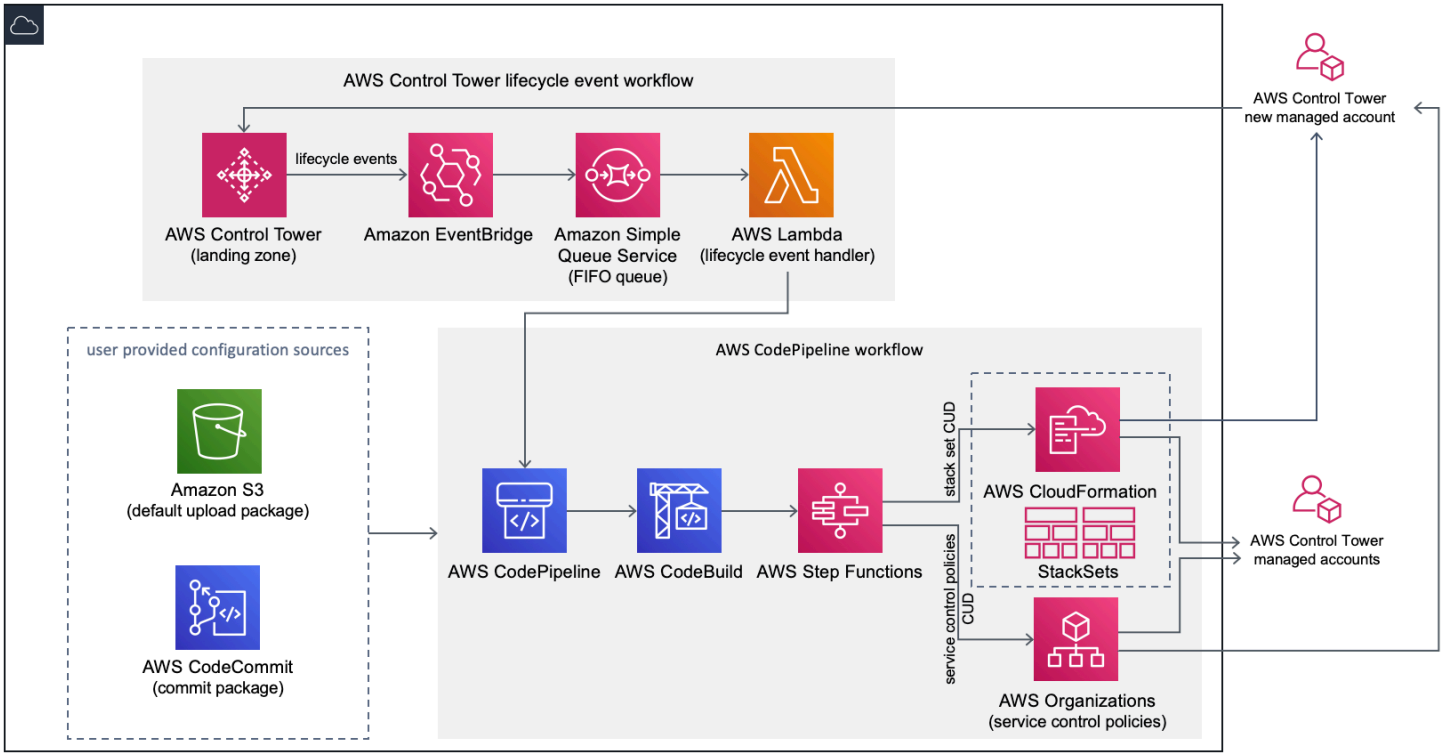


그림 1: AWS 컨트롤 타워 아키텍처의 사용자 지정

CFCT에는 AWS Control Tower 관리 계정에 배포하는 AWS CloudFormation 템플릿이 포함되어 있습니다. 템플릿은 워크플로를 구축하는 데 필요한 모든 구성 요소를 실행하므로 AWS Control Tower 랜딩 존을 사용자 지정할 수 있습니다.

> **참고**
>
> CFCt는 AWS Control Tower 홈 지역 및 AWS Control Tower 관리 계정에 배포해야 합니다. AWS Control Tower 랜딩 존이 배포되는 곳이기 때문입니다. AWS Control Tower 랜딩 존 설정에 대한 자세한 내용은 을 참조하십시오시작하기.

CFCt를 배포하면 Amazon 심플 스토리지 서비스 (Amazon S3) 를 통해 사용자 지정 리소스를 패키징하고 코드 파이프라인 소스에 업로드합니다. 업로드 프로세스는 SCP (서비스 제어 정책) 상태 머신과 상태 머신을 자동으로 호출하여 SCP를 OU 수준에서 배포하거나 OU 또는 계정 수준에서 스택 인스턴스를 배포합니다. AWS CloudFormation StackSets

> **참고**
>
> 기본적으로 cFct는 Amazon S3 버킷을 생성하여 파이프라인 소스를 저장하지만 위치를 리포지토리로 변경할 수 있습니다. AWS CodeCommit 자세한 내용은 Amazon S3를 구성 소스로 설정을 참조하십시오.

cFct는 두 가지 워크플로를 배포합니다.

- AWS CodePipeline워크플로우
- 및 AWS Control Tower 수명 주기 이벤트 워크플로.

AWS CodePipeline 워크플로

AWS CodePipeline 워크플로는 조직 내 SCP를 구성하고 AWS CodePipelineAWS Step Functions, AWS CodeBuild프로젝트를 AWS CloudFormation StackSets 구성하고, 이를 오케스트레이션합니다.

구성 패키지를 업로드하면 CFCT는 코드 파이프라인을 호출하여 3단계를 실행합니다.

- 빌드 단계 — CodeBuild AWS를 사용하여 구성 패키지의 콘텐츠를 검증합니다.
- SCP 스테이지 — AWS Organizations API를 호출하여 SCP를 생성하는 서비스 제어 정책 상태 머신을 호출합니다.
- AWS CloudFormation Stage — 스택 세트 상태 머신을 호출하여 매니페스트 파일에 제공한 계정 또는 OU 목록에 지정된 리소스를 배포합니다.

각 단계에서 코드 파이프라인은 스택 세트 및 SCP 단계 함수를 호출하여 사용자 지정 스택 세트와 SCP를 대상 개별 계정이나 전체 조직 단위에 배포합니다.

> **참고**
>
> 구성 패키지 사용자 지정에 대한 자세한 내용은 을 참조하십시오. cFCT 커스터마이징 가이드

AWS Control Tower 수명 주기 이벤트 워크플로

AWS Control Tower에서 새 계정을 생성하면 수명 주기 이벤트가 AWS CodePipeline 워크플로를 호출할 수 있습니다. Amazon EventBridge 이벤트 규칙, Amazon 심플 큐 서비스 (Amazon SQS) 선입선출

(FIFO) 대기열 및 함수로 구성된 이 워크플로를 통해 구성 패키지를 사용자 지정할 수 있습니다. AWS Lambda

Amazon EventBridge 이벤트 규칙은 일치하는 수명 주기 이벤트를 감지하면 이벤트를 Amazon SQS FIFO 대기열로 전달하고 함수를 호출하고 코드 파이프라인을 AWS Lambda 호출하여 스택 세트와 SCP의 다운스트림 배포를 수행합니다.

비용

CFCT 실행 비용은 실행 횟수, AWS CodePipeline 실행 기간, AWS Lambda 함수 수 및 기간, 게시된 Amazon EventBridge 이벤트 수에 따라 달라집니다. AWS CodeBuild 예를 들어 각 빌드가 5분 동안 실행되는 build.general1.small을 사용하여 한 달에 100개의 빌드를 실행하는 경우 cFCT를 실행하는 데 드는 대략적인 비용은 월 3.00 USD입니다. 실행 중인 각 서비스의 요금 웹페이지에서 자세한 내용을 확인할 수 있습니다. AWS

Amazon Simple Storage Service (Amazon S3) 버킷과 CodeCommit AWS Git 기반 리포지토리 리소스는 템플릿을 삭제한 후에도 보존되어 구성 정보를 보호합니다. 선택한 옵션에 따라 Amazon S3 버킷에 저장된 데이터의 양과 Git 요청 수를 기준으로 요금이 부과됩니다 (Amazon S3 리소스에는 적용되지 않음). 자세한 내용은 Amazon S3 및 AWS CodeCommit 요금을 참조하십시오.

컴포넌트 서비스

다음 AWS 서비스는 AWS Control Tower (cFCT) 사용자 지정의 구성 요소입니다.

AWS CodeCommit

AWS CloudFormation 템플릿에 입력한 내용을 기반으로 CFCt는 Amazon Simple Storage Service 섹션에 설명된 것과 동일한 샘플 구성으로 AWS CodeCommit리포지토리를 생성할 수 있습니다.

cFCT AWS CodeCommit 리포지토리를 로컬 컴퓨터에 복제하려면 사용 설명서에 설명된 대로 리포지토리에 대한 임시 액세스를 제공하는 자격 증명을 생성해야 합니다.AWS CodeCommit 버전 호환성에 대한 자세한 내용은 설정을 참조하십시오. AWS CodeCommit

AWS CodePipeline

AWS CodePipeline 기본 Amazon S3 버킷 또는 리포지토리에서 수행하게 될 구성 패키지의 업데이트를 기반으로 변경 사항을 검증, 테스트 및 구현합니다. AWS CodeCommit 구성 소스 제어를 로 AWS CodeCommit변경하는 방법에 대한 자세한 내용은 Amazon S3를 구성 소스로 사용을 참조하십시오. 파이프라인에는 구성 파일 및 템플릿, 핵심 계정, AWS Organizations 서비스 제어 정책 등을 검증하고

관리하는 단계가 포함됩니다 AWS CloudFormation StackSets. 파이프라인 단계에 대한 자세한 내용은 을 참조하십시오. cFCT 커스터마이징 가이드

AWS Key Management Service

Cfct는 AWS Key Management Service(AWS KMS) `CustomControlTowerKMSKey` 암호화 키를 생성합니다. 이 키는 Amazon S3 구성 버킷, Amazon SQS 대기열에 있는 객체 및 Systems AWS Manager 파라미터 스토어의 민감한 파라미터를 암호화하는 데 사용됩니다. 기본적으로 CFCT에서 프로비저닝한 역할에만 이 키로 암호화 또는 암호 해독 작업을 수행할 권한이 있습니다. 구성 파일, FIFO 대기열 또는 매개변수 저장소 `SecureString` 값에 액세스하려면 관리자를 정책에 추가해야 합니다. `CustomControlTowerKMSKey` 자동 키 순환은 기본적으로 활성화되어 있습니다.

AWS Lambda

CFCt는 AWS Control Tower 수명 주기 이벤트 중에 AWS CloudFormation StackSets 또는 AWS Organizations SCP의 초기 설치 및 배포 중에 AWS Lambda 함수를 사용하여 설치 구성 요소를 호출합니다.

Amazon Simple Notification Service

CFCt는 워크플로 중에 Amazon 심플 알림 서비스 (Amazon SNS) 주제에 대한 파이프라인 승인과 같은 알림을 게시할 수 있습니다. Amazon SNS는 파이프라인 승인 알림을 수신하도록 선택한 경우에만 시작됩니다.

Amazon Simple Storage Service(S3)

cFCT를 배포하면 cFCT는 고유한 이름을 가진 아마존 심플 스토리지 서비스 (Amazon S3) 버킷을 생성합니다.

예: Amazon S3 버킷 이름

`custom-control-tower-configuration-`*`accountID`*`-`*`region`*

버킷에는 라는 샘플 구성 파일이 들어 있습니다. `_custom-control-tower-configuration.zip`

파일 이름의 맨 앞에 있는 밑줄을 확인하십시오.

이 zip 파일은 필요한 폴더 구조를 설명하는 샘플 매니페스트와 관련 샘플 템플릿을 제공합니다. 이 예제는 구성 패키지를 개발하여 AWS Control Tower 랜딩 존을 사용자 지정하는 데 도움이 됩니다. 샘플 매니페스트는 사용자 지정을 구현할 때 필요한 스택 세트 및 서비스 제어 정책 (SCP) 에 필요한 구성을 식별합니다.

이 샘플 구성 패키지를 모델로 사용하여 사용자 지정 패키지를 개발하고 업로드할 수 있습니다. 그러면 cFCT 구성 파이프라인이 자동으로 트리거됩니다.

구성 파일 사용자 지정에 대한 자세한 내용은 을 참조하십시오. cFCT 커스터마이징 가이드

Amazon Simple Queue Service

CFCT는 아마존 심플 큐 서비스 (Amazon SQS) FIFO 대기열을 사용하여 아마존에서 라이프사이클 이벤트를 캡처합니다. EventBridge 이는 배포 또는 SCP를 AWS CodePipeline 호출하는 AWS Lambda 함수를 트리거합니다. AWS CloudFormation StackSets SCP에 대한 자세한 내용은 을 참조하십시오. AWS Organizations

AWS Step Functions

Cfct는 사용자 지정 배포를 오케스트레이션하기 위해 Step Functions를 생성합니다. 이러한 Step Functions는 구성 파일을 변환하여 필요에 따라 환경 전체에 사용자 지정을 배포합니다.

AWS Systems Manager 파라미터 스토어

AWS Systems Manager 파라미터 스토어는 cFCT 구성 파라미터를 저장합니다. 이러한 파라미터를 통해 관련 구성 템플릿을 통합할 수 있습니다. 예를 들어, 중앙 집중식 Amazon S3 버킷에 AWS CloudTrail 데이터를 기록하도록 각 계정을 구성할 수 있습니다. 또한 Systems Manager 매개변수 저장소는 관리자가 cFCT 입력 및 매개변수를 볼 수 있는 중앙 위치를 제공합니다.

배포 고려 사항

AWS Control Tower 랜딩 존이 배포된 동일한 계정 및 리전에서 AWS 컨트롤 타워 사용자 지정 (cFCT)를 실행해야 합니다. 즉, AWS 컨트롤 타워 홈 리전의 AWS Control Tower 관리 계정에 배포해야 합니다. 기본적으로 cFct는 해당 계정 및 지역에서 구성 파이프라인을 설정하여 landing Zone 구성 패키지를 생성하고 실행합니다.

배포 준비

초기 배포를 위해 AWS CloudFormation 템플릿을 준비할 때 사용할 수 있는 몇 가지 옵션이 있습니다. 구성 소스를 선택하고 파이프라인 배포의 수동 승인을 허용할 수 있습니다. 다음 두 섹션에서는 이러한 옵션에 대해 자세히 설명합니다.

구성 소스를 선택하세요.

기본적으로 템플릿은 Amazon Simple Storage Service (Amazon S3) 버킷을 생성하여 샘플 구성 패키지를 `.zip` 라는 파일로 저장합니다. `_custom-control-tower-configuration.zip` Amazon S3 버킷은 버전이 관리되며 필요에 따라 구성 패키지를 업데이트할 수 있습니다. 구성 패키지 업데이트에 대한 자세한 내용은 Amazon S3를 구성 소스로 사용을 참조하십시오.

> **참고**
>
> 샘플 구성 패키지 파일 이름은 밑줄 (_) 로 시작하므로 자동으로 AWS CodePipeline 시작되지 않습니다. 구성 패키지 사용자 지정을 마쳤으면 밑줄 (_) `custom-control-tower-configuration.zip` 없이 파일을 업로드해야 배포를 시작할 수 있습니다. AWS CodePipeline

파라미터에서 `AWS CodeCommit` 옵션을 선택하여 구성 패키지의 스토리지 위치를 S3 버킷에서 AWS CodeCommit Git 리포지토리로 변경할 수 있습니다. AWS CloudFormation 이 옵션을 사용하면 버전 제어를 쉽게 관리할 수 있습니다.

> **참고**
>
> 기본 S3 버킷을 사용하는 경우 구성 패키지를 `.zip` 파일로 사용할 수 있는지 확인하십시오. AWS CodeCommit 리포지토리를 사용할 때는 파일을 압축하지 않고 구성 패키지를 리포지토리에 배치해야 합니다. 에서 AWS CodeCommit구성 패키지를 만들고 저장하는 방법에 대한 자세한 내용은 을 참조하십시오cFCT 커스터마이징 가이드.

샘플 구성 패키지를 사용하여 사용자 지정 구성 원본을 만들 수 있습니다. 사용자 정의 구성을 배포할 준비가 되면 구성 패키지를 Amazon S3 버킷 또는 AWS CodeCommit 리포지토리에 수동으로 업로드합니다. 구성 파일을 업로드하면 파이프라인이 자동으로 시작됩니다.

> **참고**
>
> 를 AWS CodeCommit 사용하여 구성 패키지를 저장하는 경우 패키지를 압축할 필요가 없습니다. 구성 패키지를 만들고 저장하는 방법에 대한 자세한 내용은 AWS CodeCommit을 참조하십시오cFCT 커스터마이징 가이드.

파이프라인 구성 승인 매개변수를 선택합니다.

AWS CloudFormation 템플릿은 구성 변경 사항 배포를 수동으로 승인하는 옵션을 제공합니다. 기본적으로 수동 승인은 활성화되지 않습니다. 자세한 내용은 1단계를 참조하십시오. 스택을 실행합니다.

수동 승인이 활성화되면 구성 파이프라인은 AWS Control Tower 파일 매니페스트와 템플릿에 대한 사용자 지정을 검증한 다음 수동 승인이 승인될 때까지 프로세스를 일시 중지합니다. 승인 후 배포는 필요에 따라 나머지 파이프라인 단계를 실행하여 AWS Control Tower (cFCT) 에 대한 사용자 지정 기능을 구현합니다.

수동 승인 파라미터를 사용하면 파이프라인을 통한 첫 번째 실행 시도를 거부함으로써 AWS Control Tower 구성에 대한 사용자 지정 작업이 실행되지 않도록 할 수 있습니다. 또한 이 파라미터를 사용하면 구현 전 최종 제어 수단으로 AWS Control Tower 구성 변경에 대한 사용자 지정을 수동으로 검증할 수 있습니다.

AWS Control Tower의 사용자 지정을 업데이트하려면

이전에 cFCT를 배포한 경우 cFCT 프레임워크의 최신 버전을 가져오려면 AWS CloudFormation 스택을 업데이트해야 합니다. 자세한 내용은 스택 업데이트를 참조하십시오.

템플릿 및 소스 코드

AWS Control Tower (cFCT) 에 대한 사용자 지정 내용은 템플릿을 시작한 후 관리 계정에 배포됩니다. AWS CloudFormation 에서 템플릿을 다운로드한 다음 에서 GitHub 시작할 수 있습니다. AWS CloudFormation

customizations-for-aws-control-tower.template은 다음을 배포합니다.

- AWS CodeBuild 프로젝트
- AWS CodePipeline 프로젝트
- 아마존 EventBridge 규칙
- AWS Lambda 함수
- Amazon 심플 큐 서비스 대기열
- 샘플 구성 패키지가 포함된 Amazon 심플 스토리지 서비스 버킷
- AWS Step Functions

> **Note**
>
> 특정 요구 사항에 따라 템플릿을 사용자 지정할 수 있습니다.

소스 코드 리포지토리

GitHub 리포지토리를 방문하여 CFCT용 템플릿과 스크립트를 다운로드하고, 사용자 지정된 랜딩 존 (landing zone) 을 다른 사람과 공유할 수 있습니다.

배포 자동화

자동 배포를 시작하기 전에 고려 사항을 검토하세요. 이 섹션의 step-by-step 지침에 따라 솔루션을 구성하고 AWS Control Tower 관리 계정에 배포하십시오.

배포 시간: 약 15분

필수 조건

CFCT는 AWS 컨트롤 타워 관리 계정과 AWS 컨트롤 타워 홈 리전에 배포해야 합니다. 착륙 지대를 설정하지 않은 경우 을 참조하십시오시작하기.

배포 단계

CFCT 배포 절차는 두 가지 주요 단계로 구성됩니다. 자세한 지침은 각 단계에 대한 링크를 따르십시오.

단계 1. 스택 시작

- 관리 계정에서 AWS CloudFormation 템플릿을 실행합니다.
- 템플릿 매개변수를 검토하고 필요한 경우 조정하십시오.

단계 2. 사용자 지정 패키지 만들기

- 사용자 지정 구성 패키지를 만드세요.

> **Important**
>
> 올바른 AWS CloudFormation 템플릿을 다운로드하고 CFCT를 실행하려면 이 섹션에 제공된 GitHub 링크를 따르십시오. 이전에 지정된 S3 버킷으로 연결되는 이전 링크를 따라가지 마십시오.

단계 1. 스택 시작

이 섹션의 AWS CloudFormation 템플릿은 사용자 계정에 AWS Control Tower (cFCT) 에 대한 사용자 지정을 배포합니다.

> **참고**
>
> cFCT를 실행하는 동안 사용되는 AWS 서비스 비용은 사용자 부담입니다. 자세한 내용은 비용를 참조하세요.

1. AWS Control Tower용 사용자 지정을 시작하려면 에서 GitHub 템플릿을 다운로드한 다음 에서 AWS CloudFormation시작하십시오.
2. 이 템플릿은 기본적으로 미국 동부(버지니아 북부) 리전에서 시작됩니다. 다른 AWS 지역에서 CFCT를 시작하려면 콘솔 탐색 표시줄의 지역 선택기를 사용하십시오.

   > **Note**
   >
   > CFCT는 AWS Control Tower 랜딩 존 (홈 리전) 을 배포한 지역과 동일한 리전 및 계정에서 시작해야 합니다.

3. 스택 생성 페이지에서 URL 텍스트 상자에 올바른 템플릿 URL이 표시되는지 확인하고 다음을 선택합니다.
4. 스택 세부 정보 지정 페이지에서 cFCT 스택에 이름을 할당합니다.
5. 매개 변수에서 다음 매개 변수를 검토하고 필요한 경우 템플릿에서 해당 매개 변수를 수정하십시오.

파이프라인 구성		
파라미터	기본값	설명
파이프라인 승인 단계	No	파이프라인 구성을 기본 자동 승인 단계에서 수동 승인 단계로 변경할지 여부를 선택합니다. 자세한 설명은 the section called “cFCT 커스터마이징 가이드” 섹션을 참조하세요.
파이프라인 승인 이메일 주소	<Optional Input>	승인 알림을 위한 이메일 주소입니다. 이 매개변수를 사용하려면 파이프라인 승인 단계 매개변수를 로 설정해야 `Yes` 합니다.
AWS CodePipeline 소스	`Amazon S3`	cFCT 사용자 지정을 저장하고 구성할 위치를 선택하는 CodePipeline 데 도움이 되는 AWS 소스입니다.
AWS CodeCommit 설치		
파라미터	기본값	설명
기존 CodeCommit 리포지토리?	No	기존 CodeCommit Git 리포지토리를 사용할지 여부를 선택합니다. 원하는 `Yes` 경우 CodePipeline Source 매개변수를 로 설정해야 합니다. `AWS CodeCommit`

AWS CodeCommit 설치		
파라미터	기본값	설명
CodeCommit 리포지토리 이름	`custom-control-tower-configuration`	Git 리포지토리 이름. 이 파라미터를 사용하려면 AWS CodePipeline Source 파라미터를 로 설정해야 `AWS CodeCommit` 합니다. 이 이름은 새 Git 리포지토리를 만드는 데 사용되며 고유해야 합니다. 기존 Git 리포지토리의 이름을 제공하는 경우 기존 리포지토리를 설정해야 합니까? CodeCommit 매개 변수를 Yes로 설정하고 해당 리포지토리의 정확한 이름을 입력합니다.
CodeCommit 브랜치 이름	`main`	사용자 지정 패키지가 저장되는 Git 브랜치입니다. Git 리포지토리에는 여러 브랜치가 있을 수 있습니다. Git 리포지토리의 브랜치에 지정된 기본 이름입니다. 이 파라미터를 사용하려면 CodePipeline Source 파라미터를 로 `AWS CodeCommit` 설정해야 합니다.

AWS CloudFormation StackSets 구성		
파라미터	기본값	설명
리전 동시성 유형	PARALLEL	지역 내 배포 StackSets 작업의 동시성 유형을 선택합니다. 이 설정은 워크플로를 만들고, 업데이트하고, 삭제하는 데 적용됩니다. 기타 허용되는 값은 입니다SEQUENTIAL .
최대 동시 사용 비율	100	한 번에 이 작업을 수행할 최대 계정 백분율입니다. 최대 허용 값은 100입니다. 자세한 내용은 스택 세트 작업 옵션을 참조하십시오.
실패 허용 오차 백분율	10	AWS가 해당 지역에서 작업을 CloudFormation 중단하기 전에 이 스택 작업이 실패할 수 있는 리전별 계정의 비율입니다. 최소 허용 값은 0이고 최대 허용 값은 100입니다. 자세한 내용은 스택 세트 작업 옵션을 참조하십시오.

6. 다음을 선택합니다.
7. Configure stack options(스택 옵션 구성) 페이지에서 Next(다음)를 선택합니다.
8. 검토 페이지에서 설정을 검토하고 확인합니다. 템플릿이 AWS Identity and Access Management (IAM) 리소스를 생성한다는 것을 확인하는 확인란을 선택해야 합니다.
9. [스택 생성(Create stack)]을 선택하여 스택을 배포합니다.

   AWS CloudFormation 콘솔의 상태 열에서 스택 상태를 볼 수 있습니다. 약 15분 후에 CREATE_COMPLETE 상태가 표시될 것입니다.

단계 2. 사용자 지정 패키지 만들기

출시된 스택을 사용하면 포함된 구성 패키지를 사용자 지정하여 AWS Control Tower 랜딩 존 및 SCP (서비스 제어 정책) 에 사용자 지정을 추가할 수 있습니다. 사용자 지정 패키지 생성에 대한 자세한 지침은 를 참조하십시오. cFCT 커스터마이징 가이드

> **참고**
>
> 파이프라인은 사용자 지정 구성 패키지를 업로드하지 않으면 실행되지 않습니다.

스택 업데이트

이전에 AWS Control Tower (cFCT) 용 사용자 지정을 배포한 경우, 절차에 따라 cFCT 프레임워크의 최신 버전에 맞게 AWS CloudFormation 스택을 업데이트하십시오.

> **Important**
>
> 다음 절차를 완료하려면 먼저 Amazon Simple Storage Service (Amazon S3) GitHub 버킷에 최신 템플릿을 업로드해야 합니다. Amazon S3를 시작하는 방법에 대한 지침은 Amazon 심플 스토리지 서비스 사용 설명서의 Amazon S3 시작하기를 참조하십시오.

1. AWS CloudFormation 콘솔에 로그인합니다.
2. AWS Control Tower (cFCT) CloudFormation 스택의 기존 사용자 지정을 선택한 다음 업데이트를 선택합니다.
3. 사전 요구 사항 — 템플릿 준비에서 현재 템플릿 교체를 선택합니다.
4. 템플릿 지정에서 다음을 수행합니다.
   a. 템플릿 소스의 경우 현재 템플릿 바꾸기를 선택합니다.
   b. Amazon S3 URL의 경우, 이전에 Amazon GitGub S3로 업로드한 템플릿의 템플릿 URL을 입력하고 다음을 선택합니다.
   c. 템플릿 URL이 정확한지 확인하십시오. 그런 다음 [다음] 과 [다음] 을 다시 선택합니다.
5. 파라미터에서 템플릿의 파라미터를 검토하고 필요에 따라 수정합니다. 1단계를 참조하십시오. 스택을 실행하여 파라미터에 대한 세부 정보를 확인하십시오.
6. 다음을 선택합니다.

7. Configure stack options(스택 옵션 구성) 페이지에서 Next(다음)를 선택합니다.
8. 검토 페이지에서 설정을 검토하고 확인합니다. 템플릿이 AWS Identity and Access Management (IAM) 리소스를 생성할 수 있음을 확인하는 체크박스를 반드시 체크하세요.
9. 변경 세트 보기를 선택하고 변경 사항을 확인합니다.
10. 스택 생성을 선택하여 스택을 배포합니다.

    AWS CloudFormation 콘솔의 상태 열에서 스택 상태를 확인할 수 있습니다. 약 15분 후에 UPDATE_COMPLETE 상태가 표시될 것입니다.

스택 세트 삭제

매니페스트 파일에서 스택 세트 삭제를 활성화한 경우 스택 세트를 삭제할 수 있습니다. 기본적으로 `enable_stack_set_deletion` 파라미터는 `false`로 설정됩니다. 이 구성에서는 cFCT 매니페스트 파일에서 리소스가 제거될 때 관련 스택 세트를 삭제하기 위한 조치가 취해지지 않습니다.

매니페스트 파일에서 값을 `enable_stack_set_deletion` to 로 `true` 변경하면 매니페스트 파일에서 관련 리소스를 제거하면 CFCT는 스택 세트와 해당 리소스를 모두 삭제합니다.

이 기능은 매니페스트 파일의 v2에서 지원됩니다.

> **Important**
>
> 처음에 값을 `enable_stack_set_deletion` 로 `true` 설정하면 다음에 cFCt를 호출할 때 접두사로 `CustomControlTower-` 시작하고 관련 키 태그가 `Key:AWS_Solutions, Value: CustomControlTowerStackSet` 있고 매니페스트 파일에 선언되지 않은 모든 리소스가 삭제 스테이징됩니다.

파일에 이 파라미터를 설정하는 방법의 예는 다음과 같습니다. `manifest.yaml`

```
version: 2021-03-15
region: us-east-1
enable_stack_set_deletion: true   #New opt-in functionality


resources:
  - name: demo_resource_1
    resource_file: s3://demo_bucket/resource.template
    deployment_targets:
```

```
    accounts:
      - 012345678912
  deploy_method: stack_set
  ...
  regions:
  - us-east-1
  - us-west-2

- name: demo_resource_2
  resource_file: s3://demo_bucket/resource.template
  deployment_targets:
    accounts:
      - 012345678912
  deploy_method: stack_set
  ...
  regions:
  - us-east-1
  - eu-north-1
```

Amazon S3를 구성 소스로 설정

AWS Control Tower용 사용자 지정을 설정하면 파일이라는 `_custom-control-tower-configuration.zip` 초기 구성 파일이 Amazon Simple Storage Service (Amazon S3) 버킷에 저장되고 이름이 지정됩니다. `custom-control-tower-configuration-`*`account-ID`*`-`*`region`*

> **참고**
>
> 이 파일을 다운로드하고 수정하려면 변경 내용을 압축하고 이름이 지정된 `custom-control-tower-configuration.zip` 새 파일로 저장한 다음 동일한 Amazon S3 버킷에 다시 업로드해야 합니다.
>
> Amazon S3 버킷은 파이프라인의 기본 소스입니다. 기본 설정이 적용되면 파일 이름에 밑줄 접두사가 없는 구성 zip 파일을 S3 버킷으로 업로드하면 파이프라인이 자동으로 시작됩니다.

zip 파일은 () 를 사용한 서버 측 암호화 (SSE) 및 KMS 키 사용 거부로 AWS Key Management Service 보호됩니다.AWS KMSzip 파일에 액세스하려면 KMS 키 정책을 업데이트하여 액세스 권한을 부여해야 하는 역할을 지정해야 합니다. 역할은 관리자 역할, 사용자 또는 둘 다일 수 있습니다. 다음 절차를 따르십시오.

1. AWS Key Management Service 콘솔로 이동합니다.
2. 고객 관리 키에서 CustomControlTowerKMSkey를 선택합니다.
3. 키 정책 탭을 선택합니다. 그런 다음 편집을 선택합니다.
4. 키 정책 편집 페이지에서 코드의 키 사용 허용 섹션을 찾아 다음 권한 중 하나를 추가합니다.
   - 관리 역할을 추가하려면:

     ```
     arn:aws:iam::<account-ID>:role/<administrator-role>
     ```
   - 사용자 추가하기:

     ```
     arn:aws:iam::<account-ID>:user/<username>
     ```
5. 변경 사항 저장(Save Changes)을 선택합니다.
6. Amazon S3 콘솔로 이동하여 구성 zip 파일이 들어 있는 S3 버킷을 찾은 다음 다운로드를 선택합니다.
7. 매니페스트 파일 및 템플릿 파일의 구성을 필요에 따라 변경합니다. 매니페스트 및 템플릿 파일을 사용자 지정하는 방법에 대한 자세한 내용은 을 참조하십시오. the section called “cFCT 커스터마이징 가이드”
8. 변경 내용 업로드:
   a. 수정된 구성 파일을 압축하고 파일 이름을 다음과 같이 지정합니다`custom-control-tower-configuration.zip`.
   b. AWS KMS 마스터 키:와 함께 SSE를 사용하여 Amazon S3에 파일을 업로드합니다. `CustomControlTowerKMSKey`

운영 지표 수집

AWS Control Tower (cFCT) 에 대한 사용자 지정에는 익명의 운영 지표를 전송할 수 있는 옵션이 포함됩니다. AWS AWS 이 데이터를 사용하여 고객이 cFCT와 기타 관련 서비스 및 제품을 어떻게 사용하고 있는지 이해합니다. 데이터 수집이 활성화되면 다음 정보가 다음 주소로 전송됩니다. AWS

- 솔루션 ID: AWS 솔루션 식별자
- 고유 ID (UUID): 각 배포에 대해 무작위로 생성되는 고유 식별자
- 타임스탬프: 데이터 수집 타임스탬프
- 상태 시스템 실행 수: 이 상태 머신이 실행되는 횟수를 점진적으로 계산합니다.
- 매니페스트 버전: 구성에 사용된 매니페스트 버전

> **Note**
>
> AWS 수집한 데이터를 소유합니다. 데이터 수집에는 AWS 개인정보 보호정책이 적용됩니다.

익명 운영 지표 전송을 AWS거부하려면 다음 작업 중 하나를 완료하십시오.

- AWS CloudFormation 템플릿 매핑 섹션을 다음과 같이 업데이트하십시오.

  에서

  ```
  AnonymousData:
       SendAnonymousData:
          Data: Yes
  ```

  ~

  ```
  AnonymousData:
       SendAnonymousData:
          Data: No
  ```

- cFCT를 배포한 후 파라미터 스토어 콘솔에서 **/org/primary/metrics_flag** SSM 파라미터 키를 찾아 값을 로 업데이트합니다. **No**

cFCT 커스터마이징 가이드

AWS Control Tower (cFCT) 사용자 지정 가이드는 회사와 고객을 위해 AWS Control Tower 환경을 사용자 지정하고 확장하려는 관리자, DevOps 전문가, 독립 소프트웨어 공급업체, IT 인프라 설계자 및 시스템 통합자를 위한 것입니다. cFCT 사용자 지정 패키지를 사용하여 AWS Control Tower 환경을 사용자 지정하고 확장하는 방법에 대한 정보를 제공합니다.

> **Note**
>
> 배포 및 구성 (cFCT) 하려면 구성 패키지를 배포하고 처리해야 합니다. AWS CodePipeline다음 섹션에서는 프로세스를 자세히 설명합니다.

코드 파이프라인 개요

구성 패키지에는 아마존 심플 스토리지 서비스 (Amazon S3) 및 AWS CodePipeline. 구성 패키지에는 다음 항목이 들어 있습니다.

- 매니페스트 파일
- 함께 제공되는 템플릿 세트
- AWS Control Tower 환경 사용자 지정을 설명하고 구현하기 위한 기타 JSON 파일

기본적으로 `_custom-control-tower-configuration.zip` 구성 패키지는 다음과 같은 명명 규칙에 따라 Amazon S3 버킷에 로드됩니다.

`custom-control-tower-configuration-`*`accountID`*`-`*`region`*.

> **Note**
>
> 기본적으로 cFct는 Amazon S3 버킷을 생성하여 파이프라인 소스를 저장하지만 원본 위치를 리포지토리로 변경할 수 있습니다. AWS CodeCommit 자세한 내용은 AWS CodePipeline 사용 설명서의 파이프라인 편집을 참조하십시오. CodePipeline

매니페스트 파일은 landing zone을 사용자 지정하기 위해 배포할 수 있는 AWS 리소스를 설명하는 텍스트 파일입니다. CodePipeline 다음 작업을 수행합니다.

- 매니페스트 파일, 함께 제공되는 템플릿 세트 및 기타 JSON 파일을 추출합니다.
- 매니페스트 및 템플릿 검증을 수행합니다.
- 매니페스트 파일의 섹션을 호출하여 특정 파이프라인 단계를 실행합니다.

매니페스트 파일을 사용자 지정하고 구성 패키지 파일 이름에서 밑줄 (_) 을 제거하여 구성 패키지를 업데이트하면 자동으로 시작됩니다. AWS CodePipeline

> **Note**
>
> 샘플 구성 패키지 파일 이름은 밑줄 (_) 로 시작하므로 자동으로 트리거되지 않습니다. AWS CodePipeline 구성 패키지의 사용자 지정을 완료한 후 밑줄 (_) `custom-control-tower-configuration.zip` 없이 파일을 업로드하여 에서 배포를 트리거하십시오. AWS CodePipeline

AWS CodePipeline 스테이지

cFCT 파이프라인은 AWS Control Tower 환경을 구현하고 업데이트하기 위해 여러 AWS CodePipeline 단계를 거쳐야 합니다.

1. 소스 스테이지

   소스 단계는 초기 단계입니다. 사용자 지정 구성 패키지가 이 파이프라인 단계를 시작합니다. 의 원본은 Amazon S3 버킷 또는 구성 패키지를 호스팅할 AWS CodePipeline 수 있는 AWS CodeCommit 리포지토리일 수 있습니다.
2. 빌드 단계

   빌드 단계에서는 구성 패키지의 내용을 AWS CodeBuild 검증해야 합니다. 이러한 검사에는 패키지에 포함되거나 원격으로 호스팅되는 모든 AWS CloudFormation 템플릿과 함께 `manifest.yaml` 파일 구문 AWS CloudFormation `validate-template` 및 스키마를 테스트하는 작업이 포함됩니다`cfn_nag`. 매니페스트 파일과 AWS CloudFormation 템플릿이 테스트를 통과하면 파이프라인은 다음 단계로 계속 진행됩니다. 테스트가 실패할 경우 CodeBuild 로그를 검토하여 문제를 식별하고 필요에 따라 구성 소스 파일을 편집할 수 있습니다.
3. 수동 승인 단계 (선택 사항)

   수동 승인 단계는 선택 사항입니다. 이 단계를 활성화하면 구성 파이프라인을 추가로 제어할 수 있습니다. 배포 중에 승인이 내려질 때까지 파이프라인이 일시 중지됩니다. 스택을 시작할 때 파이프라인 승인 단계 파라미터를 Yes로 편집하여 수동 승인을 선택할 수 있습니다.
4. 서비스 제어 정책 단계

   서비스 제어 정책 단계에서는 서비스 제어 정책 상태 머신을 호출하여 서비스 제어 정책 (SCP) 을 생성하는 AWS Organizations API를 호출합니다.
5. AWS CloudFormation 리소스 스테이지

   AWS CloudFormation 리소스 스테이지는 스택 세트 상태 머신을 호출하여 매니페스트 파일에 제공한 계정 또는 OU (조직 구성 단위) 목록에 지정된 리소스를 배포합니다. AWS CloudFormation 리소스 종속성을 지정하지 않는 한 상태 머신은 매니페스트 파일에 지정된 순서대로 리소스를 만듭니다.

사용자 지정 구성을 정의하세요.

매니페스트 파일, 함께 제공되는 템플릿 세트 및 기타 JSON 파일을 사용하여 사용자 지정 AWS Control Tower 구성을 정의합니다. 다음 코드 예제와 같이 이러한 파일을 폴더 구조로 패키징하고 Amazon S3 버킷에 `.zip` 파일로 배치합니다.

사용자 지정 구성 폴더 구조

```
- manifest.yaml
- policies/                                                [optional]
   - service control policies files (*.json)
- templates/                                               [optional]
   - template files for AWS CloudFormation Resources (*.template)
```

이전 예에서는 사용자 지정 구성 폴더의 구조를 보여 줍니다. 원본 스토리지 위치로 Amazon S3를 선택하든 AWS CodeCommit 리포지토리를 선택하든 폴더 구조는 동일하게 유지됩니다. Amazon S3를 원본 스토리지로 선택하는 경우 모든 폴더와 파일을 파일로 압축하고 지정된 Amazon S3 버킷에 `.zip` 파일만 업로드합니다. `custom-control-tower-configuration.zip`

> **Note**
>
> 를 사용하는 AWS CodeCommit경우 파일을 압축하지 않고 리포지토리에 저장하십시오.

매니페스트 파일

`manifest.yaml`파일은 리소스를 AWS 설명하는 텍스트 파일입니다. 다음 예제는 매니페스트 파일의 구조를 보여줍니다.

```
---
region: String
version: 2021-03-15

resources:
  #set of CloudFormation resources or SCP policies
...
```

이전 코드 예제에서 볼 수 있듯이 매니페스트 파일의 처음 두 줄은 지역 및 버전 키워드의 값을 지정합니다. 이러한 키워드의 정의는 다음과 같습니다.

지역 — AWS Control Tower 기본 지역의 텍스트 문자열입니다. 이 값은 유효한 AWS 지역 이름 (예: `us-east-1`eu-west-1, 또는`ap-southeast-1`) 이어야 합니다. 리소스별 리전이 더 지정되지 않는 한, 사용자 지정 AWS Control Tower 리소스 (예: AWS CloudFormation StackSets) 를 생성할 때 기본적으로 AWS Control Tower 홈 리전이 됩니다.

```
region:your-home-region
```

버전 — 매니페스트 스키마 버전 번호입니다. 지원되는 최신 버전은 2021-03-15입니다.

```
version: 2021-03-15
```

> **Note**
>
> 최신 버전을 사용하는 것이 좋습니다. 최신 버전에서 매니페스트 속성을 업데이트하려면 을 매니페스트 버전 업그레이드 참조하십시오.

이전 예제에 표시된 다음 키워드는 resources 키워드입니다. 매니페스트 파일의 리소스 섹션은 고도로 구조화되어 있습니다. 여기에는 CFCT 파이프라인에 의해 자동으로 배포되는 AWS 리소스의 세부 목록이 포함되어 있습니다. 리소스에 대한 이러한 설명과 사용 가능한 매개변수는 다음 섹션에 나와 있습니다.

매니페스트 파일의 리소스 섹션

이 항목에서는 사용자 지정에 필요한 리소스를 정의하는 매니페스트 파일의 리소스 섹션에 대해 설명합니다. 매니페스트 파일의 이 섹션은 리소스 키워드에서 시작하여 파일 끝까지 이어집니다.

매니페스트 파일의 리소스 섹션은 CFCT가 코드 파이프라인을 통해 자동으로 배포하는 AWS CloudFormation StackSets 또는 AWS Organizations SCP를 지정합니다. OU, 계정, 지역을 나열하여 스택 인스턴스를 배포할 수 있습니다.

스택 인스턴스는 OU 수준이 아닌 계정 수준에서 배포됩니다. SCP는 OU 수준에서 배포됩니다. 자세한 내용은 사용자 지정 항목 만들기를 참조하십시오.

다음 예제 템플릿은 매니페스트 파일의 리소스 섹션에 사용할 수 있는 항목을 설명합니다.

```
resources: # List of resources
  - name: [String]
    resource_file: [String] [Local File Path, S3 URI, S3 URL]
    deployment_targets: # account and/or organizational unit names
      accounts: # array of strings, [0-9]{12}
        - 012345678912
        - AccountName1
      organizational_units: #array of strings
        - OuName1
        - OuName2
```

```
    deploy_method: scp | stack_set
    parameters: # List of parameters [SSM, Alfred, Values]
      - parameter_key: [String]
        parameter_value: [String]
    export_outputs: # list of ssm parameters to store output values
      - name: /org/member/test-ssm/app-id
        value: $[output_ApplicationId]
    regions: #list of strings
    - [String]
```

이 항목의 나머지 부분에서는 이전 코드 예제에 표시된 키워드에 대한 자세한 정의를 제공합니다.

이름 — 과 관련된 이름입니다. AWS CloudFormation StackSets 제공하는 문자열은 스택 세트에 보다 사용자에게 친숙한 이름을 할당합니다.

- 타입: 문자열
- 필수 항목 여부: 예
- 유효한 값: a-z, A-Z, 0-9 및 밑줄 (_). 다른 문자는 자동으로 밑줄 (_) 로 바뀝니다.

설명 - 리소스에 대한 설명입니다.

- 타입: 문자열
- 필수 항목 여부: 아니요

resource_file — 이 파일은 리소스 또는 SCP 생성을 위한 JSON의 AWS CloudFormation 템플릿 또는 AWS Organizations 서비스 제어 정책을 가리키는 Amazon S3 URI 또는 URL인 매니페스트 파일의 상대 위치로 지정할 수 있습니다. AWS CloudFormation

- 타입: 문자열
- 필수 항목 여부: 예

1. 다음 예제는 구성 패키지 내 `resource_file` 리소스 파일의 상대 위치로 지정된 를 보여줍니다.

```
resources:
  - name: SecurityRoles
    resource_file: templates/custom-security.template
```

2. 다음 예제는 Amazon S3 URI로 제공된 리소스 파일을 보여줍니다.

```
resources:
  - name: SecurityRoles
    resource_file: s3://bucket-name/[key-name]
```

3. 다음 예제는 Amazon S3 HTTPS URL로 제공된 리소스 파일을 보여줍니다.

```
resources:
  - name: SecurityRoles
    resource_file: https://bucket-name.s3.Region.amazonaws.com/key-name
```

> **Note**
>
> Amazon S3 URL을 제공하는 경우, 버킷 정책이 cFCT를 배포하려는 AWS Control Tower 관리 계정에 대한 읽기 액세스를 허용하는지 확인하십시오. Amazon S3 HTTPS URL을 제공하는 경우 경로가 점 표기법을 사용하는지 확인하십시오. 예를 들어 `S3.us-west-1`입니다. cFCT는 S3와 리전 사이에 대시가 포함된 엔드포인트 (예:) 를 지원하지 않습니다. `S3-us-west-2`

4. 다음 예제는 리소스가 저장되는 Amazon S3 버킷 정책과 ARN을 보여줍니다.

```
{
   "Version": "2012-10-17",
   "Statement": [
       {
        "Effect": "Allow",
        "Principal": {"AWS": "arn:aws:iam::AccountId:root"},
        "Action": "s3:GetObject",
        "Resource": "arn:aws:s3:::my-bucket/*”
       }
   ]
}
```

예제에 표시된 *AccountId*변수를 cFCT를 배포하는 관리 AWS 계정의 계정 ID로 대체합니다. 자세한 예는 Amazon 심플 스토리지 서비스 사용 설명서의 버킷 정책 예제를 참조하십시오.

매개 변수 — 매개 변수의 이름과 값을 지정합니다 AWS CloudFormation .

- 유형: MapList

- 필수 항목 여부: 아니요

매개변수 섹션에는 키/값 매개변수 쌍이 포함되어 있습니다. 다음 유사 템플릿은 매개변수 섹션을 간략하게 설명합니다.

```
parameters:
  - parameter_key: [String]
    parameter_value: [String]
```

- parameter_key — 파라미터와 관련된 키입니다.
  - 타입: 문자열
  - 필수: 예 (매개변수 속성 아래)
  - 유효한 값: a-z, A-Z, 0-9
- 매개변수_값 — 매개변수와 관련된 입력 값입니다.
  - 타입: 문자열
  - 필수: 예 (매개변수 속성 아래)

deploy_method — 계정에 리소스를 배포하기 위한 배포 방법입니다. 현재 deploy_method는 리소스를 통해 AWS CloudFormation StackSets 배포하는 옵션 또는 SCP를 배포하는 경우 `stack_set` 옵션을 사용하여 리소스를 배포할 수 있도록 지원합니다. `scp`

- 타입: 문자열
- 유효한 값: `stack_set` | `scp`
- 필수 항목 여부: 예

deployment_targets — CFCT가 리소스를 배포할 계정 또는 조직 단위 (OU) 목록으로, 계정 또는 조직_유닛으로 지정됩니다. AWS CloudFormation

> **Note**
>
> SCP를 배포하려는 경우 대상은 계정이 아닌 OU여야 합니다.

- 유형: 문자열 목록 `account name` 또는 `account number` 이 리소스가 지정된 계정 목록에 배포될 것임을 나타내거나 `OU names` 이 리소스가 지정된 OU 목록에 배포될 것임을 나타냅니다.

- 필수: 계정 또는 Organizational_units 중 하나 이상
  - 계정:

    유형: 문자열 목록 `account name` 또는 `account number` 이 리소스가 지정된 계정 목록에 배포될 것임을 나타냅니다.
  - 조직_단위:

    유형: 이 리소스가 `OU names` 지정된 OU 목록에 배포될 것임을 나타내는 문자열 목록입니다. 계정을 포함하지 않는 OU를 제공하고 계정 속성이 추가되지 않은 경우 Cfct는 스택 세트만 만듭니다.

    > **Note**
    >
    > 조직의 관리 계정 ID는 허용된 값이 아닙니다. CFCT는 조직의 관리 계정에 스택 인스턴스를 배포하는 것을 지원하지 않습니다.

export_output — SSM 파라미터 키를 나타내는 이름/값 쌍의 목록입니다. 이러한 SSM 파라미터 키를 사용하면 템플릿 출력을 SSM 파라미터 저장소에 저장할 수 있습니다. 출력은 매니페스트 파일 앞에 정의된 다른 리소스에서 참조하기 위한 것입니다.

```
export_outputs: # List of SSM parameters
  - name: [String]
    value: [String]
```

- 유형: 이름 및 값 키 쌍 목록. 이름에는 SSM 파라미터 저장소 키 `name` 문자열이 포함되고 값에는 파라미터 `value` 문자열이 포함됩니다.
- 유효한 값: CfnOutput *`-Logical-id# ### ##`* 변수에 해당하는 모든 문자열 또는 `$[output_`*`CfnOutput-Logical-ID`*`]` 변수 AWS CloudFormation 템플릿의 출력 섹션에 대한 자세한 내용은 사용 설명서의 출력을 참조하십시오.AWS CloudFormation
- 필수 항목 여부: 아니요

예를 들어, 다음 코드 스니펫은 템플릿 `VPCID` 출력 변수를 이름이 지정된 SSM 파라미터 키에 저장합니다. `/org/member/audit/vpc_id`

```
export_outputs: # List of SSM parameters
  - name: /org/member/audit/VPC-ID
```

```
    value: $[output_VPCID]
```

> **Note**
>
> export_output 키 이름에는 이외의 값이 포함될 수 있습니다. output 예를 들어, 이름이 인 경우 값은 다음과 /org/environment-name 같을 수 있습니다. production

지역 — CFCt가 AWS CloudFormation 스택 인스턴스를 배포할 지역 목록입니다.

- 입력: 모든 AWS 상용 지역 이름 목록을 입력하면 해당 리소스가 해당 지역 목록에 배포될 것임을 나타냅니다. 매니페스트 파일에 이 키워드가 없는 경우 리소스는 홈 지역에만 배포됩니다.
- 필수 항목 여부: 아니요

루트 OU

cFct는 매니페스트 V2 버전 (2021-03-15) organizational_units 에서 루트를 조직 단위 (OU) 의 값으로 지원합니다.

- 의 배포 방법을 선택한 경우scp, 루트를 추가하면 AWS Control Tower가 루트 아래의 organizational_units 모든 OU에 정책을 적용합니다. 의 stack_set 배포 방법을 선택한 경우 Root를 추가하면 cFct는 관리 계정을 제외하고 AWS Control Tower에 등록된 루트 아래의 모든 계정에 스택 세트를 배포합니다. organizational_units
- AWS Control Tower 모범 사례에 따르면 관리 계정은 회원 계정 관리 및 청구 목적으로만 사용됩니다. AWS Control Tower 관리 계정에서 프로덕션 워크로드를 실행하지 마십시오.

  모범 사례 지침에 따라 AWS Control Tower 배포는 관리 계정을 루트 OU 아래에 두어 전체 액세스 권한을 가지며 추가 리소스를 실행하지 않도록 합니다. 이러한 이유로 AWSControlTowerExecution역할은 관리 계정에 배포되지 않습니다.
- 관리 계정에 대한 다음 모범 사례를 따르는 것이 좋습니다. 관리 계정에 스택셋을 배포해야 하는 특정 사용 사례가 있는 경우 계정을 배포 대상으로 포함하고 관리 계정을 지정하십시오. 그렇지 않으면 계정을 배포 대상으로 포함하지 마세요. 관리 계정에서 필수 IAM 역할을 포함하여 누락된 리소스를 생성해야 합니다.

관리 계정에 스택셋을 배포하려면 배포 대상으로 포함하고 accounts 관리 계정을 지정하십시오. 그렇지 않으면 계정을 배포 대상으로 포함하지 마십시오.

```
---
region: your-home-region
version: 2021-03-15

resources:

  …truncated…

    deployment_targets:
      organizational_units:
        - Root
```

> **Note**
>
> 루트 OU 기능은 V2 버전의 매니페스트 파일 (2021-03-15) 에서만 지원됩니다. 에서 루트를 OU로 추가하는 경우 다른 `organizational_units` OU는 추가하지 마십시오.

중첩된 OU

CFCT는 매니페스트 V2 버전 (2021-03-15) 의 `organizational_units` 키워드 아래에 하나 이상의 중첩된 OU를 나열할 수 있도록 지원합니다.

OU 구분 기호로 콜론을 사용하여 중첩된 OU의 전체 경로 (루트 제외) 를 지정해야 합니다. 배포 방법의 경우`scp`, AWS Control Tower는 중첩된 OU 경로의 마지막 OU에 SCP를 배포합니다. 배포 방법의 경우`stack_set`, AWS Control Tower는 스택 세트를 중첩된 OU 경로의 마지막 OU 아래에 있는 모든 계정에 배포합니다.

경로를 예로 들어 보겠습니다. `OUName1:OUName2:OUName3` 경로의 마지막 OU는 입니다`OUName3`. Cfct는 바로 아래에 있는 모든 계정에만 SCP를 `OUName3` 배포하고 해당 계정에만 세트를 스택합니다. `OUName3`

```
---
region: your-home-region
version: 2021-03-15

resources:

  …truncated…

    deployment_targets:
```

```
    organizational_units:
      - OuName1:OUName2:OUName3
```

> **Note**
>
> 중첩된 OU 기능은 V2 버전의 매니페스트 파일 (2021-03-15) 에서만 지원됩니다.

사용자 지정 항목을 직접 만들어 보세요.

사용자 지정 항목을 직접 만들려면 SCP (서비스 제어 정책) 및 리소스를 추가하거나 업데이트하여 `manifest.yaml` 파일을 수정할 수 있습니다. AWS CloudFormation 배포해야 하는 리소스의 경우 계정 및 OU를 추가하거나 제거할 수 있습니다. 패키지 폴더에서 템플릿을 추가 또는 수정하고, 자체 폴더를 만들고, `manifest.yaml` 파일에 있는 템플릿 또는 폴더를 참조할 수 있습니다.

이 섹션에서는 사용자 지정 항목을 직접 만드는 데 필요한 두 가지 주요 부분에 대해 설명합니다.

- 서비스 제어 정책을 위한 자체 구성 패키지를 설정하는 방법
- AWS CloudFormation 스택 세트를 위한 자체 구성 패키지를 설정하는 방법

서비스 제어 정책을 위한 구성 패키지 설정

이 섹션에서는 서비스 제어 정책 (SCP) 용 구성 패키지를 만드는 방법을 설명합니다. 이 프로세스의 두 가지 주요 부분은 (1) 매니페스트 파일 준비와 (2) 폴더 구조 준비입니다.

1단계: 매니페스트.yaml 파일 편집

샘플 `manifest.yaml` 파일을 시작점으로 사용하십시오. 필요한 구성을 모두 입력합니다. `resource_file`및 `deployment_targets` 세부 정보를 추가합니다.

다음 스니펫은 기본 매니페스트 파일을 보여줍니다.

```
---
region: us-east-1
version: 2021-03-15

resources: []
```

의 `region` 값은 배포 중에 자동으로 추가됩니다. cFCT를 배포한 지역과 일치해야 합니다. 이 지역은 AWS Control Tower 지역과 동일해야 합니다.

Amazon S3 버킷에 저장된 zip 패키지의 `example-configuration` 폴더에 사용자 지정 SCP를 추가하려면 `example-manifest.yaml` 파일을 열고 편집을 시작합니다.

```
---
region: your-home-region
version: 2021-03-15

resources:
  - name: test-preventive-controls
    description: To prevent from deleting or disabling resources in member accounts
    resource_file: policies/preventive-controls.json
    deploy_method: scp
    #Apply to the following OU(s)
    deployment_targets:
      organizational_units: #array of strings
        - OUName1
        - OUName2

…truncated…
```

다음 스니펫은 사용자 지정 매니페스트 파일의 예를 보여줍니다. 한 번의 변경으로 정책을 두 개 이상 추가할 수 있습니다.

```
---
region: us-east-1
version: 2021-03-15

resources:
  - name: block-s3-public-access
    description: To S3 buckets to have public access
    resource_file: policies/block-s3-public.json
    deploy_method: scp
    #Apply to the following OU(s)
    deployment_targets:
      organizational_units: #array of strings
        - OUName1
        - OUName2
```

2단계: 폴더 구조 생성

리소스 파일에 Amazon S3 URL을 사용하고 키/값 쌍이 있는 파라미터를 사용하는 경우 이 단계를 건너뛸 수 있습니다.

매니페스트 파일은 JSON 파일을 참조하므로 매니페스트를 지원하려면 JSON 형식의 SCP 정책을 포함해야 합니다. 파일 경로가 매니페스트 파일에 제공된 경로 정보와 일치하는지 확인하십시오.

- 정책 JSON 파일에는 OU에 배포할 SCP가 포함되어 있습니다.

다음 스니펫은 샘플 매니페스트 파일의 폴더 구조를 보여줍니다.

```
- manifest.yaml
- policies/
   - block-s3-public.json
```

다음 스니펫은 정책 파일의 예입니다. `block-s3-public.json`

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Sid":"GuardPutAccountPublicAccessBlock",
         "Effect":"Deny",
         "Action":"s3:PutAccountPublicAccessBlock",
         "Resource":"arn:aws:s3:::*"
      }
   ]
}
```

에 대한 구성 패키지 설정 AWS CloudFormation StackSets

이 섹션에서는 의 구성 패키지를 설정하는 방법을 설명합니다. AWS CloudFormation StackSets 이 프로세스의 두 가지 주요 부분은 (1) 매니페스트 파일 준비 및 (2) 폴더 구조 업데이트입니다.

1단계: 기존 매니페스트 파일 편집

이전에 편집한 매니페스트 파일에 새 AWS CloudFormation StackSets 정보를 추가합니다.

검토를 위한 것으로, 다음 스니펫에는 SCP용 구성 패키지를 설정하기 위해 이전에 보여준 것과 동일한 사용자 지정 매니페스트 파일이 들어 있습니다. 이제 리소스에 대한 세부 정보를 포함하도록 이 파일을 추가로 편집할 수 있습니다.

```
---
region: us-east-1
version: 2021-03-15
```

```
resources:

  - name: block-s3-public-access
    description: To S3 buckets to have public access
    resource_file: policies/block-s3-public.json
    deploy_method: scp
    #Apply to the following OU(s)
    deployment_targets:
    organizational_units: #array of strings
    - OUName1
    - OUName2
```

다음 스니펫은 세부 정보가 포함된 편집된 샘플 매니페스트 파일을 보여줍니다. resources 의 순서에 resources 따라 종속성 생성 실행 순서가 결정됩니다. resources 비즈니스 요구 사항에 따라 다음 예제 매니페스트 파일을 편집할 수 있습니다.

```
---
region: your-home-region
version: 2021-03-15

…truncated…

resources:
  - name: stackset-1
    resource_file: templates/create-ssm-parameter-keys-1.template
    parameters:
      - parameter_key: parameter-1
        parameter_value: value-1
    deploy_method: stack_set
    deployment_targets:
      accounts: # array of strings, [0-9]{12}
        - account number or account name
        - 123456789123
      organizational_units: #array of strings, ou ids, ou-xxxx
        - OuName1
        - OUName2
    export_outputs:
      - name: /org/member/test-ssm/app-id
        value: $[output_ApplicationId]
    regions:
      - region-name
```

```
  - name: stackset-2
    resource_file: s3://bucket-name/key-name
    parameters:
      - parameter_key: parameter-1
        parameter_value: value-1
    deploy_method: stack_set
    deployment_targets:
      accounts: # array of strings, [0-9]{12}
        - account number or account name
        - 123456789123
      organizational_units: #array of strings
        - OuName1
        - OUName2
regions:
  - region-name
```

다음 예제는 매니페스트 파일에 AWS CloudFormation 리소스를 두 개 이상 추가할 수 있음을 보여줍니다.

```
---
region: us-east-1
version: 2021-03-15

resources:
  - name: block-s3-public-access
    description: To S3 buckets to have public access
    resource_file: policies/block-s3-public.json
    deploy_method: scp
    #Apply to the following OU(s)
    deployment_targets:
      organizational_units: #array of strings
        - Custom
        - Sandbox

  - name: transit-network
    resource_file: templates/transit-gateway.template
    parameter_file: parameters/transit-gateway.json
    deploy_method: stack_set
    deployment_targets:
      accounts: # array of strings, [0-9]{12}
        - Prod
        - 123456789123 #Network
      organizational_units: #array of strings
```

```
      - Custom
  export_outputs:
    - name: /org/network/transit-gateway-id
      value: $[output_TransitGatewayID]
  regions:
    - us-east-1
```

2단계: 폴더 구조 업데이트

폴더 구조를 업데이트할 때 매니페스트 파일에 있는 모든 지원 AWS CloudFormation 템플릿 파일과 SCP 정책 파일을 포함할 수 있습니다. 파일 경로가 매니페스트 파일에 제공된 경로와 일치하는지 확인하십시오.

- 템플릿 파일에는 OU 및 계정에 배포할 AWS 리소스가 포함되어 있습니다.
- 정책 파일에는 템플릿 파일에 사용되는 입력 매개 변수가 들어 있습니다.

다음 예제는 1단계에서 만든 샘플 매니페스트 파일의 폴더 구조를 보여줍니다.

```
- manifest.yaml
- policies/
   - block-s3-public.json
- templates/
   - transit-gateway.template
```

'alfred' 헬퍼와 파라미터 파일 AWS CloudFormation

cFCT는 템플릿에 정의된 SSM 파라미터 저장소 키의 값을 가져오는 알프레드 도우미라는 메커니즘을 제공합니다. AWS CloudFormation alfred 도우미를 사용하면 템플릿을 업데이트하지 않고도 SSM 파라미터 저장소에 저장된 값을 사용할 수 있습니다. AWS CloudFormation 자세한 내용은 템플릿이란 무엇입니까? 를 참조하십시오. AWS CloudFormation AWS CloudFormation 사용 설명서에서.

> **Important**
>
> 알프레드 헬퍼에는 두 가지 제한이 있습니다. 파라미터는 AWS Control Tower 관리 계정의 홈 지역에서만 사용할 수 있습니다. 스택 인스턴스 간에 변경되지 않는 값을 사용하는 것이 가장 좋습니다. 'alfred' 도우미는 매개변수를 가져오면 변수를 내보내는 스택 세트에서 임의의 스택 인스턴스를 선택합니다.

예

스택 세트가 두 개 있다고 가정해 보겠습니다. AWS CloudFormation 스택 세트 1에는 스택 인스턴스가 하나 있으며 한 지역의 한 계정에 배포됩니다. 가용 영역에 Amazon VPC와 서브넷을 생성하고, 및 를 파라미터 값으로 스택 세트 2에 *subnet ID* 전달해야 합니다. VPC ID 를 subnet ID 사용하여 VPC ID and를 스택 세트 2에 전달하려면 를 VPC ID 사용하여 스택 세트 1에 *subnet ID* 저장해야 합니다. AWS:::SSM::Parameter 자세한 내용은AWS CloudFormation 사용 설명서의 AWS:::SSM::Parameter를 참조하십시오.

AWS CloudFormation 스택 세트 1:

다음 스니펫에서 alfred 헬퍼는 파라미터 subnet ID 저장소에서 VPC ID 및 의 값을 가져와서 상태 머신에 입력으로 전달할 수 있습니다. StackSet

```
VpcIdParameter:
    Type: AWS::SSM::Parameter
    Properties:
      Name: '/stack_1/vpc/id'
      Description: Contains the VPC id
      Type: String
      Value: !Ref MyVpc

SubnetIdParameter:
    Type: AWS::SSM::Parameter
    Properties:
      Name: '/stack_1/subnet/id'
      Description: Contains the subnet id
      Type: String
      Value: !Ref MySubnet
```

AWS CloudFormation 스택 세트 2:

스니펫은 AWS CloudFormation stack 2 manifest.yaml 파일에 지정된 매개변수를 보여줍니다.

```
parameters:
      - parameter_key: VpcId
        parameter_value: $[alfred_ssm_/stack_1/vpc/id]
      - parameter_key: SubnetId
        parameter_value: $[alfred_ssm_/stack_1/subnet/id]
```

AWS CloudFormation 스택 세트 2.1:

스니펫은 유형의 매개변수를 지원하는 `alfred_ssm` 속성을 나열할 수 있음을 보여줍니다. CommaDelimitedList 자세한 내용은AWS CloudFormation 사용 설명서의 `Parameters`를 참조하십시오.

```
parameters:
      - parameter_key: VpcId # Type: String
        parameter_value: $[alfred_ssm_/stack_1/vpc/id']
      - parameter_key: SubnetId # Type: String
        parameter_value: $[ alfred_ssm_/stack_1/subnet/id']
      - parameter_key: AvailablityZones # Type: CommaDelimitedList
        parameter_value:
  - "$[alfred_ssm_/availability_zone_1]"
 - "$[alfred_ssm_/availability_zone_2]"
```

사용자 지정 패키지의 JSON 스키마

CFCT용 사용자 지정 패키지의 JSON 스키마는 의 소스 코드 저장소에 있습니다. GitHub 이 스키마는 즐겨 사용하는 여러 개발 도구와 함께 사용할 수 있으며, 파일을 직접 빌드할 때 오류를 줄이는 데 유용할 수 있습니다. `manifest.yaml`

매니페스트 버전 업그레이드

최신 버전의 AWS Control Tower 사용자 지정 (cFCT) 에 대한 자세한 내용은 리포지토리의 ChangeLog.md 파일을 참조하십시오. GitHub

Warning

AWS Control Tower (CfcT) 사용자 지정 버전 2.2.0에는 관련 서비스 API에 맞게 매니페스트 스키마 (버전 2021-03-15) 가 도입되었습니다. AWS 매니페스트 스키마를 사용하면 단일 manifest.yaml 파일로 분리된 워크플로를 통해 지원되는 리소스 (템플릿 및 SCP) 를 관리할 수 있습니다.AWS CloudFormation DevOps

매니페스트 스키마를 버전 2020-01-01에서 버전 2021-03-15 이상으로 업데이트하는 것이 좋습니다.

CfcT는 이 파일의 버전 2021-03-15 및 2020-01-01을 계속 지원합니다. `manifest.yaml` 기존 구성을 변경할 필요는 없습니다. 하지만 버전 2020-01-01은 지원이 종료되었습니다. 더 이상 버전 2020-01-01에 대한 업데이트를 제공하거나 개선 사항을 추가하지 않습니다. 루트 OU 및 중첩된 OU 기능은 버전 2020-01-01에서 지원되지 않습니다.

매니페스트 버전 2021-03-15에서 더 이상 사용되지 않는 속성:

```
organization_policies
policy_file
apply_to_accounts_in_ou

cloudformation_resources
template_file
deploy_to_account
deploy_to_ou
ssm_parameters
```

필수 업그레이드 단계

매니페스트 스키마 버전 2021-03-15 버전으로 업그레이드할 때 파일을 업데이트하기 위해 변경해야 하는 사항은 다음과 같습니다. 다음 섹션에서는 전환에 필요한 필수 및 권장 변경 사항을 간략하게 설명합니다.

조직 및 정책

1. 조직_정책 아래 SCP를 새 재산 자원으로 옮기세요.
2. policy_file 속성을 새 속성 resource_file로 변경하십시오.
3. apply_to_accounts_in_ou를 새 속성 배포_대상으로 변경합니다. OU 목록은 하위 속성인 조직_유닛에서 정의해야 합니다. 계정 하위 속성은 조직 정책에 지원되지 않습니다.
4. scp 값을 가진 새 속성 deploy_method 를 추가합니다.

AWS CloudFormation 리소스

1. CloudFormation 클라우드포메이션_리소스 아래의 리소스를 새 속성 리소스로 이동합니다.
2. 템플릿_파일 속성을 새 속성 리소스_파일로 변경합니다.
3. deploy_to_ou를 새 속성 배포_타겟으로 변경합니다. OU 목록은 조직 단위 하위 속성에서 정의해야 합니다.
4. 배포_to_accounts를 새 속성 배포_대상으로 변경합니다. 계정 목록은 하위 속성 계정 아래에 정의해야 합니다.
5. ssm_parameters 속성을 새 속성 export_output 으로 변경합니다.

적극 권장되는 업그레이드 단계

AWS CloudFormation 파라미터

1. parameter_file 속성을 새 속성 매개변수로 변경합니다.
2. parameter_file 속성 값에서 파일 경로를 제거합니다.
3. 기존 파라미터 JSON 파일의 파라미터 키와 파라미터 값을 파라미터 속성의 새 형식으로 복사합니다. 이렇게 하면 매니페스트 파일에서 관리하는 데 도움이 됩니다.

> **Note**
>
> 파라미터_file 속성은 매니페스트 버전 2021-03-15에서 지원됩니다.

AWS Control Tower에서의 네트워킹

AWS Control Tower는 VPC를 통한 네트워킹에 대한 기본 지원을 제공합니다.

AWS Control Tower VPC의 기본 구성 또는 기능이 요구 사항을 충족하지 못하는 경우 다른 AWS 서비스를 사용하여 VPC를 구성할 수 있습니다. VPC와 AWS Control Tower를 사용하는 방법에 대한 자세한 내용은 확장 가능하고 안전한 다중 VPC AWS 네트워크 인프라 구축을 참조하십시오.

관련 주제

- 기존 VPC가 있는 계정을 등록할 때 AWS Control Tower가 작동하는 방식에 대한 자세한 내용은 을 참조하십시오. 기존 계정을 VPC에 등록
- Account Factory를 사용하면 AWS 컨트롤 타워 VPC가 포함된 계정을 프로비저닝하거나 VPC 없이 계정을 프로비저닝할 수 있습니다. AWS 컨트롤 타워 VPC를 삭제하거나 VPC 없이 AWS 컨트롤 타워 계정을 구성하는 방법에 대한 자세한 내용은 을 참조하십시오. 둘러보기: VPC 없이 AWS 컨트롤 타워 구성
- VPC의 계정 설정을 변경하는 방법에 대한 자세한 내용은 계정 업데이트에 대한 Account Factory 설명서를 참조하십시오.
- AWS Control Tower에서 네트워킹 및 VPC를 사용하는 방법에 대한 자세한 내용은 이 사용 설명서의 관련 정보 페이지에 있는 네트워킹 관련 섹션을 참조하십시오.

AWS Control AWS Tower의 VPC 및 지역

계정 생성의 표준 부분으로, AWS Control Tower로 관리하지 않는 지역을 포함하여 모든 지역에 AWS-default VPC를 AWS 생성합니다. 이 기본 VPC는 AWS Control Tower가 프로비저닝된 계정에 대해 생성하는 VPC와 동일하지 않지만, IAM 사용자는 비관리 지역의 기본 AWS VPC에 액세스할 수 있습니다.

관리자는 지역 거부 제어를 활성화하여 최종 사용자가 AWS Control Tower에서 지원하지만 관리 대상 지역 외부에 있는 지역의 VPC에 연결할 수 있는 권한을 갖지 않도록 할 수 있습니다. 지역 거부 제어를 구성하려면 랜딩 존 설정 페이지로 이동하여 설정 수정을 선택합니다.

지역 거부 제어는 비관리 서비스의 대부분의 서비스에 대한 API 호출을 차단합니다. AWS 리전자세한 내용은 요청에 AWS 따른 액세스 거부를 참조하십시오. AWS 리전.

> **Note**
>
> 지역 거부 제어로 인해 IAM 사용자가 AWS Control Tower가 지원되지 않는 지역의 기본 AWS VPC에 연결하는 것을 막을 수는 없습니다.

선택적으로 비관리 지역의 AWS 기본 VPC를 제거할 수 있습니다. 지역의 기본 VPC를 나열하려면 다음 예제와 유사한 CLI 명령을 사용할 수 있습니다.

```
aws ec2 --region us-west-1 describe-vpcs --filter Name=isDefault,Values=true
```

AWS Control 타워 및 VPC의 개요

다음은 AWS Control Tower VPC에 대한 몇 가지 필수 사실입니다.

- Account Factory에서 계정을 프로비저닝할 때 AWS 컨트롤 타워에서 생성되는 VPC는 기본 AWS VPC와 다릅니다.
- AWS Control Tower가 지원되는 AWS 지역에 새 계정을 설정하면 AWS Control Tower는 자동으로 기본 AWS VPC를 삭제하고 AWS Control Tower에서 구성한 새 VPC를 설정합니다.
- 각 AWS 컨트롤 타워 계정에는 AWS 컨트롤 타워에서 생성한 VPC 1개가 허용됩니다. 계정 한도 내에서 계정에 추가 AWS VPC를 보유할 수 있습니다.
- 모든 AWS Control Tower VPC는 미국 서부 (캘리포니아 북부) 지역을 제외한 모든 지역에 세 개의 가용 영역을 보유하고 있으며 두 개의 가용 영역을 갖추고 있습니다. `us-west-1` `us-west-1` 기본적으로 각 가용 영역에는 퍼블릭 서브넷 1개와 프라이빗 서브넷 2개가 할당됩니다. 따라서 미국 서부 (캘리포니아 북부) 를 제외한 지역의 각 AWS Control Tower VPC에는 기본적으로 3개의 가용 영역으로 나누어진 9개의 서브넷이 포함됩니다. 미국 서부 (캘리포니아 북부) 에서는 6개의 서브넷이 두 가용 영역에 분산되어 있습니다.
- AWS Control Tower VPC의 각 서브넷에는 동일한 크기의 고유한 범위가 할당됩니다.
- VPC의 서브넷 수는 구성 가능합니다. VPC 서브넷 구성을 변경하는 방법에 대한 자세한 내용은 Account Factory 주제를 참조하십시오.
- IP 주소가 겹치지 않기 때문에 AWS Control Tower VPC 내의 6개 또는 9개 서브넷은 제한 없이 서로 통신할 수 있습니다.

VPC를 사용할 때 AWS Control Tower는 지역 수준에서 구분하지 않습니다. 모든 서브넷은 지정하는 정확한 CIDR 범위에서 할당됩니다. VPC 서브넷은 모든 리전에 존재할 수 있습니다.

참고

> **VPC 비용 관리**
>
> 새 계정을 프로비저닝할 때 퍼블릭 서브넷이 활성화되도록 Account Factory VPC 구성을 설정하면 Account Factory는 NAT 게이트웨이를 생성하도록 VPC를 구성합니다. 따라서 Amazon VPC에서 사용량에 대한 요금이 청구됩니다.

> **VPC 및 제어 설정**
>
> VPC 인터넷 액세스 설정이 활성화된 상태에서 Account Factory 계정을 프로비저닝하는 경우, 해당 Account Factory 설정은 고객이 관리하는 Amazon VPC 인스턴스에 대한 인터넷 액세스 허용 안 함 제어보다 우선합니다. 새로 프로비전된 계정에 대한 인터넷 액세스를 활성화하지 않으려면 Account Factory에서 설정을 변경해야 합니다. 자세한 내용은 안내: VPC 없이 AWS Control Tower 구성을 참조하십시오.

VPC 및 AWS Control Tower를 위한 CIDR 및 피어링

이 섹션은 주로 네트워크 관리자용입니다. 일반적으로 회사의 네트워크 관리자는 AWS Control Tower 조직의 전체 CIDR 범위를 선택하는 사람입니다. 네트워크 관리자는 특정한 목적에 맞게 해당 범위 내에서 서브넷을 할당합니다.

VPC의 CIDR 범위를 선택하면 AWS Control Tower는 RFC 1918 사양에 따라 IP 주소 범위를 검증합니다. Account Factory는 다음 범위의 CIDR 차단을 허용합니다. /16

- `10.0.0.0/8`
- `172.16.0.0/12`
- `192.168.0.0/16`
- `100.64.0.0/10`(인터넷 공급자가 이 범위의 사용을 허용하는 경우에만 해당)

/16 구분 기호는 최대 65,536개의 고유 IP 주소를 허용합니다.

다음 범위에서 유효한 IP 주소를 할당할 수 있습니다.

- `10.0.x.x to 10.255.x.x`

- 172.16.x.x - 172.31.x.x
- 192.168.0.0 - 192.168.255.255(192.168 범위를 벗어난 IP 없음)

지정한 범위가 범위를 벗어나는 경우, AWS Control Tower는 오류 메시지를 제공합니다.

기본 CIDR 범위는 172.31.0.0/16입니다.

AWS Control Tower는 사용자가 선택한 CIDR 범위를 사용하여 VPC를 생성하면 조직 단위 (OU) 내에 생성하는 모든 계정에 대해 모든 VPC에 동일한 CIDR 범위를 할당합니다. 기본적으로 중복되는 IP 주소로 인해 이 구현에서는 OU에 있는 AWS Control Tower VPC 간의 피어링이 처음에는 허용되지 않습니다.

서브넷

각 VPC 내에서 AWS Control Tower는 지정된 CIDR 범위를 9개의 서브넷으로 균등하게 나눕니다 (서브넷이 6개인 미국 서부 (캘리포니아 북부) 제외). VPC 내의 서브넷은 중첩되지 않습니다. 따라서 VPC 내에서 모두 서로 통신할 수 있습니다.

요약하면 VPC 내의 서브넷 통신은 기본적으로 제한이 없습니다. VPC 서브넷 간의 통신을 제어하는 모범 사례는 필요한 경우 허용된 트래픽 흐름을 정의하는 규칙으로 액세스 제어 목록을 설정하는 것입니다. 특정 인스턴스 간의 트래픽을 제어하기 위해 보안 그룹을 사용합니다. AWS Control Tower에서 보안 그룹 및 방화벽을 설정하는 방법에 대한 자세한 내용은 안내: Firewall AWS Manager를 사용하여 AWS Control Tower에서 보안 그룹 설정을 참조하십시오.

피어링

AWS Control Tower는 여러 VPC 간의 통신을 위한 VPC 간 피어링을 제한하지 않습니다. 하지만 기본적으로 모든 AWS Control Tower VPC의 기본 CIDR 범위는 동일합니다. 피어링을 지원하려면 Account Factory의 설정에서 CIDR 범위를 수정하여 IP 주소가 겹치지 않도록 할 수 있습니다.

Account Factory의 설정에서 CIDR 범위를 변경하면 이후에 AWS 컨트롤 타워에서 Account Factory를 사용하여 생성하는 모든 새 계정에 새 CIDR 범위가 할당됩니다. 이전 계정은 업데이트되지 않습니다. 예를 들어 계정을 생성한 다음 CIDR 범위를 변경하고 새 계정을 생성하면 두 계정에 할당된 VPC를 피어링할 수 있습니다. IP 주소 범위가 동일하지 않으므로 피어링이 가능합니다.

필요한 역할 및 권한

AWS Control Tower는 IAM 역할을 사용하여 리소스에 대한 액세스를 관리하는 데 도움을 줍니다.

역할에 대한 일반 정보는 사용자 그룹, 역할 및 권한 집합을 참조하십시오.

권한 정보

- AWS 컨트롤 타워에서의 IAM 그룹 및 해당 권한에 대한 자세한 내용은 AWS Control Tower의 IAM ID 센터 그룹을 참조하십시오.
- 계정을 프로비저닝하는 데 필요한 권한에 대한 자세한 내용은 계정에 필요한 권한을 참조하십시오.
- AWS Control Tower에 필요한 콘솔 권한에 대한 자세한 내용은 AWS Control Tower 콘솔 사용에 필요한 권한을 참조하십시오.

역할 정보

- 프로그래밍 방식 액세스를 위해 설계된 권한을 포함하여 역할을 생성하는 방법에 대한 자세한 내용은 역할 생성 및 권한 할당, AWS Control Tower 감사 계정의 프로그래밍 역할 및 신뢰 관계를 참조하십시오.
- AWS Control Tower가 계정을 관리하는 데 사용하는 다른 역할에 대한 자세한 내용은 AWS Control Tower의 자격 증명 기반 정책 (IAM 정책) 사용 및 AWS Control Tower의 관리형 정책 사용을 참조하십시오.
- AWS 컨트롤 타워 및 AWS Config 역할에 대한 자세한 내용은 AWS 컨트롤 타워를 참조하십시오 ConfigRecorderRole.
- AWS Control Tower가 계정 AWS Config 정보를 집계하는 데 사용하는 역할에 대한 자세한 내용은 AWS Control Tower가 비관리형 OU 및 계정의 AWS Config 규칙을 집계하는 방법을 참조하십시오.
- 역할 및 권한을 할당할 때 리소스를 보호하는 방법에 대한 자세한 내용은 역할 신뢰 관계에 대한 선택적 조건, 선택적 AWS KMS 키 구성, 서비스 간 도용 방지를 참조하십시오.
- IAM 역할을 사용한 AWS Control Tower의 자동 계정 프로비저닝에 대한 자세한 내용은 IAM 역할을 사용한 자동 계정 프로비저닝을 참조하십시오.
- SNS 주제를 보호하는 정책을 보려면 AWS Config SNS 주제 정책을 참조하십시오. AWS Config

AWS Control Tower가 역할을 사용하여 계정을 생성하고 관리하는 방법

일반적으로 역할은 에서 ID 및 액세스 관리 (IAM) 의 일부입니다. AWS의 IAM 및 역할에 대한 일반 정보는 IAM 사용 설명서의 IAM 역할 주제를 참조하십시오. AWSAWS

역할 및 계정 생성

AWS Control Tower는 의 `CreateAccount` API를 호출하여 고객의 계정을 생성합니다 AWS Organizations. 이 계정을 AWS Organizations 생성하면 해당 계정 내에 역할이 생성되며, AWS Control Tower는 API에 파라미터를 전달하여 이름을 지정합니다. 역할의 이름은 `AWSControlTowerExecution`입니다.

AWS Control Tower는 Account Factory에서 생성한 모든 계정의 `AWSControlTowerExecution` 역할을 대신합니다. AWS Control Tower는 이 역할을 사용하여 계정을 기준으로 설정하고 필수 (및 기타 활성화된) 제어를 적용하여 다른 역할을 생성합니다. 이러한 역할은 다음과 같은 다른 서비스에서 차례로 사용됩니다. AWS Config

> **Note**
>
> 계정의 기준을 설정하는 것은 계정을 설정하는 것입니다. 여기에는 블루프린트라고도 하는 Account Factory 템플릿과 컨트롤이 포함됩니다. 또한 베이스라인 프로세스에서는 템플릿 배포의 일환으로 계정에 대한 중앙 집중식 로깅 및 보안 감사 역할을 설정합니다. AWS Control Tower 기준은 등록된 모든 계정에 적용하는 역할에 포함되어 있습니다.

계정 및 리소스에 대한 자세한 내용은 을 참조하십시오. AWS Control AWS 계정 타워에 대한 정보

AWSControlTowerExecution 역할, 설명

등록된 모든 계정에 `AWSControlTowerExecution` 역할이 있어야 합니다. 이를 통해 AWS Control Tower는 개별 계정을 관리하고 이에 대한 정보를 감사 및 로그 아카이브 계정에 보고할 수 있습니다.

다음과 같이 여러 가지 방법으로 계정에 `AWSControlTowerExecution` 역할을 추가할 수 있습니다.

- 보안 OU 계정 (코어 계정이라고도 함) 의 경우 AWS Control Tower는 초기 AWS Control Tower 설정 시 역할을 생성합니다.
- AWS 컨트롤 타워 콘솔을 통해 생성된 Account Factory 계정의 경우, AWS 컨트롤 타워는 계정 생성 시 이 역할을 생성합니다.

- 단일 계정 등록의 경우, 고객에게 수동으로 역할을 생성한 다음 AWS Control Tower에 계정을 등록하도록 요청합니다.
- 거버넌스를 OU로 확장할 때 AWS Control Tower는 StackSetAWSControlTowerExecutionRole-를 사용하여 해당 OU의 모든 계정에 역할을 생성합니다.

AWSControlTowerExecution역할의 목적:

- AWSControlTowerExecution스크립트와 Lambda 함수를 사용하여 계정을 자동으로 생성하고 등록할 수 있습니다.
- AWSControlTowerExecution을 통해 전체 계정의 모든 로그가 로깅 계정으로 전송되도록 조직의 로깅을 구성할 수 있습니다.
- AWSControlTowerExecutionAWS Control Tower에 개인 계정을 등록할 수 있습니다. 먼저 해당 계정에 AWSControlTowerExecution 역할을 추가해야 합니다. 역할을 추가하는 방법에 대한 단계는 을 참조하십시오필요한 IAM 역할을 기존 역할에 수동으로 AWS 계정 추가하고 등록하십시오..

OU에서 AWSControlTowerExecution 역할이 작동하는 방식:

AWSControlTowerExecution역할은 선택한 AWS Control Tower 제어 항목이 조직의 모든 개별 계정, 각 OU, 그리고 AWS Control Tower에서 생성하는 모든 새 계정에 자동으로 적용되도록 합니다. 결과:

- AWS Control Tower 컨트롤에 구현된 감사 및 로깅 기능을 기반으로 규정 준수 및 보안 보고서를 보다 쉽게 제공할 수 있습니다.
- 보안 및 규정 준수 팀은 모든 요구 사항이 충족되었는지 그리고 조직 드리프트가 발생하지 않았는지 확인할 수 있습니다.

드리프트에 대한 자세한 내용은 AWS Control Tower에서의 드리프트 감지 및 해결을 참조하십시오.

요약하면 AWSControlTowerExecution 역할 및 관련 정책을 통해 조직 전체에서 보안 및 규정 준수를 유연하게 제어할 수 있습니다. 따라서 보안 또는 프로토콜 위반이 발생할 가능성이 적습니다.

역할 신뢰 관계를 위한 선택적 조건

역할 신뢰 정책에 조건을 부과하여 AWS Control Tower에서 특정 역할과 상호 작용하는 계정 및 리소스를 제한할 수 있습니다. 역할에는 광범위한 액세스 권한이 허용되므로 AWSControlTowerAdmin 역할에 대한 액세스를 제한하는 것이 좋습니다.

공격자가 리소스에 액세스하는 것을 방지하려면 AWS Control Tower 신뢰 정책을 수동으로 편집하여 정책 설명에 하나 이상의 aws:SourceArn 또는 aws:SourceAccount 조건을 추가하십시오. 특정 계정 및 특정 리소스에 대한 액세스를 제한하는 것보다 aws:SourceAccount 더 구체적이므로 보안 모범 사례로 aws:SourceArn 조건을 추가하는 것이 좋습니다.

리소스의 전체 ARN을 모르거나 여러 리소스를 지정하는 경우 ARN의 알 수 없는 부분에 대해 와일드카드 (*) 와 함께 aws:SourceArn 조건을 사용할 수 있습니다. 예를 들어 지역을 arn:aws:controltower:*:123456789012:* 지정하지 않으려는 경우에 사용할 수 있습니다.

다음 예는 IAM 역할 신뢰 정책과 함께 aws:SourceArn IAM 조건을 사용하는 방법을 보여줍니다. 역할의 신뢰 관계에 조건을 추가하십시오. AWS Control Tower 서비스 보안 주체가 해당 AWSControlTowerAdmin역할과 상호 작용하기 때문입니다.

예제에서 볼 수 있듯이 소스 ARN의 형식은 다음과 같습니다. arn:aws:controltower:*${HOME_REGION}*:*${CUSTOMER_AWSACCOUNT_id}*:*

문자열을 자신의 홈 지역 ${HOME_REGION} 및 통화 계정의 계정 ${CUSTOMER_AWSACCOUNT_id} ID로 바꾸십시오.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": [
          "controltower.amazonaws.com"
        ]
      },
      "Action": "sts:AssumeRole",
      "Condition": {
        "ArnEquals": {
          "aws:SourceArn": "arn:aws:controltower:us-west-2:012345678901:*"
        }
      }
    }
  ]
}
```

이 예에서는 로 지정된 소스 ARN이 작업을 수행할 수 있는 유일한 arn:aws:controltower:us-west-2:012345678901:* ARN입니다. sts:AssumeRole 즉, us-west-2 리전에

서 계정 012345678901 ID에 로그인할 수 있는 사용자만이 AWS Control Tower 서비스에 대해 이러한 특정 역할 및 신뢰 관계를 요구하는 작업을 수행할 수 있습니다 (로 지정)controltower.amazonaws.com.

다음 예는 역할 신뢰 정책에 적용되는 aws:SourceAccount 및 aws:SourceArn 조건을 보여줍니다.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": [
          "controltower.amazonaws.com"
        ]
      },
      "Action": "sts:AssumeRole",
      "Condition": {
        "StringEquals": {
          "aws:SourceAccount": "012345678901"
        },
        "StringLike": {
          "aws:SourceArn": "arn:aws:controltower:us-west-2:012345678901:*"
        }
      }
    }
  ]
}
```

이 예제는 aws:SourceArn 조건문이 추가된 aws:SourceAccount 조건문을 보여줍니다. 자세한 정보는 서비스 간 사칭 방지을 참조하세요.

AWS Control Tower의 권한 정책에 대한 일반 정보는 을 참조하십시오리소스에 대한 액세스를 관리합니다..

권장 사항:

AWS Control Tower가 생성하는 역할에는 조건을 추가하는 것이 좋습니다. 이러한 역할은 다른 AWS 서비스에서 직접 위임되기 때문입니다. 자세한 내용은 AWSControlTowerAdmin이 섹션 앞부분에 나와 있는 예제를 참조하십시오. AWS Config 레코더 역할의 경우 Config 레코더 ARN을 허용된 소스 ARN으로 지정하여 aws:SourceArn 조건을 추가하는 것이 좋습니다.

모든 관리 계정에서 AWS Control Tower Audit 계정이 맡을 수 있는 AWSControlTowerExecution역할이나 기타 프로그래밍 방식의 역할의 경우, 이러한 역할의 신뢰 정책에 `aws:PrincipalOrgID` 조건을 추가하는 것이 좋습니다. 그러면 리소스에 액세스하는 보안 주체가 올바른 조직의 계정에 속해 있는지 확인할 수 있습니다. AWS `aws:SourceArn`조건문은 예상대로 작동하지 않으므로 추가하지 마십시오.

> **Note**
>
> 드리프트의 경우 특정 상황에서 AWS Control Tower 역할이 재설정될 수 있습니다. 역할을 사용자 지정한 경우 역할을 정기적으로 다시 확인하는 것이 좋습니다.

AWS Control Tower가 비관리형 OU 및 계정의 AWS Config 규칙을 집계하는 방법

AWS Control Tower 관리 계정은 외부 AWS Config 규칙을 탐지하는 데 도움이 되는 조직 수준의 애그리게이터를 생성하므로 AWS Control Tower는 관리되지 않는 계정에 액세스할 필요가 없습니다. AWS Control Tower 콘솔은 특정 계정에 대해 외부에서 생성한 AWS Config 규칙의 수를 보여줍니다. 계정 세부 정보 페이지의 외부 Config 규칙 준수 탭에서 이러한 외부 규칙에 대한 세부 정보를 볼 수 있습니다.

애그리게이터를 생성하기 위해 AWS Control Tower는 조직을 설명하고
그 아래에 계정을 나열하는 데 필요한 권한을 가진 역할을 추가합니다.
`AWSControlTowerConfigAggregatorRoleForOrganizations`역할에는
`AWSConfigRoleForOrganizations` 관리형 정책과 신뢰 관계가 필요합니다.
`config.amazonaws.com`

역할에 연결된 IAM 정책 (JSON 아티팩트) 은 다음과 같습니다.

```
{
    "Version": "2012-10-17",
      "Statement": [
       {
        "Effect": "Allow",
        "Action": [
          "organizations:ListAccounts",
          "organizations:DescribeOrganization",
          "organizations:ListAWSServiceAccessForOrganization"
         ],
```

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

신뢰 관계는 다음과 AWSControlTowerConfigAggregatorRoleForOrganizations 같습니다.

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

관리 계정에 이 기능을 배포하기 위해 관리형 정책에 AWSControlTowerServiceRolePolicy 다음과 같은 권한을 추가해야 합니다. 이 권한은 AWS Config 애그리게이터를 생성할 때 AWSControlTowerAdmin 역할이 사용합니다.

```
{
  "Version": "2012-10-17",
    "Statement": [
      {
        "Effect": "Allow",
        "Action": [
          "config:PutConfigurationAggregator",
          "config:DeleteConfigurationAggregator",
          "iam:PassRole"
          ],
        "Resource": [
          "arn:aws:iam:::role/service-role/
AWSControlTowerConfigAggregatorRoleForOrganizations",
          "arn:aws:config:::config-aggregator/"
          ]
        },
      {
```

```
        "Effect": "Allow",
        "Action": "organizations:EnableAWSServiceAccess",
        "Resource": "*"
      }
    ]
}
```

새 리소스 생성: 및 AWSControlTowerConfigAggregatorRoleForOrganizations aws-controltower-ConfigAggregatorForOrganizations

준비가 되면 계정을 개별적으로 등록하거나 OU를 등록하여 그룹으로 등록할 수 있습니다. 계정을 등록한 후 에서 AWS Config규칙을 생성하면 AWS Control Tower가 새 규칙을 감지합니다. 애그리게이터는 외부 규칙의 수를 보여주고 계정에 대한 각 외부 규칙의 세부 정보를 볼 수 있는 AWS Config 콘솔 링크를 제공합니다. AWS Config 콘솔과 AWS Control Tower 콘솔의 정보를 사용하여 계정에 적절한 제어 기능이 활성화되어 있는지 확인하십시오.

AWS Control Tower 감사 계정의 프로그래밍 방식 역할 및 신뢰 관계

감사 계정에 로그인하여 프로그래밍 방식으로 다른 계정을 검토하는 역할을 맡을 수 있습니다. 감사 계정을 이용해 다른 계정에 수동으로 로그인할 수 없습니다.

감사 계정을 사용하면 AWS Lambda 함수에만 부여되는 일부 역할을 통해 다른 계정에 프로그래밍 방식으로 액세스할 수 있습니다. 보안을 위해 이러한 역할은 다른 역할과 신뢰 관계를 맺고 있습니다. 즉, 역할을 활용할 수 있는 조건이 엄격하게 정의되어 있습니다.

AWS Control Tower 스택 세트는 감사 계정에서 다음과 같은 프로그래밍 전용 계정 간 역할을 StackSet-AWSControlTowerBP-BASELINE-ROLES 생성합니다.

- AWS-컨트롤 타워- AdministratorExecutionRole
- AWS - 컨트롤 타워 - AuditAdministratorRole
- AWS - 컨트롤 타워 - ReadOnlyExecutionRole
- AWS - 컨트롤 타워 - AuditReadOnlyRole

ReadOnlyExecutionRole:단, 이 역할을 사용하면 감사 계정이 전체 조직의 Amazon S3 버킷에 있는 객체를 읽을 수 있습니다 (SecurityAudit정책에서는 메타데이터 액세스만 허용).

AWS-컨트롤타워-: AdministratorExecutionRole

- 관리자 권한이 있습니다.

- 콘솔에서는 가정할 수 없습니다.
- 감사 계정의 역할만 맡을 수 있습니다. aws-controltower-AuditAdministratorRole

다음 아티팩트는 에 대한 신뢰 관계를 보여줍니다. aws-controltower-AdministratorExecutionRole 플레이스홀더 번호는 012345678901 감사 계정 Audit_acct_ID 번호로 대체됩니다.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::012345678901:role/aws-controltower-AuditAdministratorRole"
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

AWS-컨트롤 타워-: AuditAdministratorRole

- AWS Lambda 서비스에서만 가정 가능
- 문자열 로그로 시작하는 이름을 가진 Amazon S3 객체에 대해 읽기 (Get) 및 쓰기 (Put) 작업을 수행할 권한이 있습니다.

첨부된 정책:

1. AWSLambdaExecute— AWS 관리형 정책

2. AssumeRole-aws-controltower- AuditAdministratorRole — 인라인 정책 — AWS Control Tower에서 만든 것으로, 아티팩트는 다음과 같습니다.

```
{
  "Version": "2012-10-17",
  "Statement": [
 {
 "Action": [
   "sts:AssumeRole"
   ],
```

```
 "Resource": [
   "arn:aws:iam::*:role/aws-controltower-AdministratorExecutionRole"
   ],
 "Effect": "Allow"
 }
   ]
}
```

다음 아티팩트는 다음에 대한 신뢰 관계를 보여줍니다. aws-controltower-AuditAdministratorRole

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

AWS-컨트롤 타워-: ReadOnlyExecutionRole

- 콘솔에서는 가정할 수 없습니다.
- 감사 계정의 다른 역할인 다음 역할만 맡을 수 있습니다. AuditReadOnlyRole

다음 아티팩트는 에 대한 신뢰 관계를 보여줍니다. aws-controltower-ReadOnlyExecutionRole 플레이스홀더 번호는 012345678901 감사 계정 Audit_acct_ID 번호로 대체됩니다.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::012345678901:role/aws-controltower-AuditReadOnlyRole "
      },
```

```
      "Action": "sts:AssumeRole"
    }
  ]
}
```

AWS-컨트롤 타워-: AuditReadOnlyRole

- AWS Lambda 서비스에서만 가정 가능
- 문자열 로그로 시작하는 이름을 가진 Amazon S3 객체에 대해 읽기 (Get) 및 쓰기 (Put) 작업을 수행할 권한이 있습니다.

첨부된 정책:

1. AWSLambdaExecute— AWS 관리형 정책

2. AssumeRole-aws-controltower- AuditReadOnlyRole — 인라인 정책 — AWS Control Tower에서 만든 것으로, 아티팩트는 다음과 같습니다.

```
{
  "Version": "2012-10-17",
  "Statement": [
 {
 "Action": [
  "sts:AssumeRole"
 ],
 "Resource": [
  "arn:aws:iam::*:role/aws-controltower-ReadOnlyExecutionRole"
 ],
 "Effect": "Allow"
   }
  ]
}
```

다음 아티팩트는 다음에 대한 신뢰 관계를 보여줍니다. `aws-controltower-AuditAdministratorRole`

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
```

```
      "Principal": {
        "Service": "lambda.amazonaws.com"
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

IAM 역할을 사용한 자동화된 계정 프로비저닝

Account Factory 계정을 보다 자동화된 방식으로 구성하려면 멤버 계정에서 역할을 맡는 AWS Control Tower 관리 계정에서 Lambda 함수를 생성할 수 있습니다. AWSControlTowerExecution 그런 다음 관리 계정은 역할을 사용하여 각 구성원 계정에서 원하는 구성 단계를 수행합니다.

Lambda 함수를 사용하여 계정을 프로비저닝하는 경우 이 작업을 수행할 자격 증명에는 다음과 같은 IAM 권한 정책이 추가로 포함되어야 합니다. `AWSServiceCatalogEndUserFullAccess`

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AWSControlTowerAccountFactoryAccess",
            "Effect": "Allow",
            "Action": [
                "sso:GetProfile",
                "sso:CreateProfile",
                "sso:UpdateProfile",
                "sso:AssociateProfile",
                "sso:CreateApplicationInstance",
                "sso:GetSSOStatus",
                "sso:GetTrust",
                "sso:CreateTrust",
                "sso:UpdateTrust",
                "sso:GetPeregrineStatus",
                "sso:GetApplicationInstance",
                "sso:ListDirectoryAssociations",
                "sso:ListPermissionSets",
                "sso:GetPermissionSet",
                "sso:ProvisionApplicationInstanceForAWSAccount",
                "sso:ProvisionApplicationProfileForAWSAccountInstance",
                "sso:ProvisionSAMLProvider",
                "sso:ListProfileAssociations",
                "sso-directory:ListMembersInGroup",
```

```
                "sso-directory:AddMemberToGroup",
                "sso-directory:SearchGroups",
                "sso-directory:SearchGroupsWithGroupName",
                "sso-directory:SearchUsers",
                "sso-directory:CreateUser",
                "sso-directory:DescribeGroups",
                "sso-directory:DescribeDirectory",
                "sso-directory:GetUserPoolInfo",
                "controltower:CreateManagedAccount",
                "controltower:DescribeManagedAccount",
                "controltower:DeregisterManagedAccount",
                "s3:GetObject",
                "organizations:describeOrganization",
                "sso:DescribeRegisteredRegions"
            ],
            "Resource": "*"
        }
    ]
}
```

AWS Control Tower Account Factory에서 AWS IAM 자격 증명 센터와 상호 작용하기 위해 필요한 권한 `sso:GetPeregrineStatus` `sso:ProvisionApplicationInstanceForAWSAccountsso:ProvisionApplicationProfileForA` 및 `sso:ProvisionSAMLProvide`

AWS Control Tower의 리소스

- AWS Control Tower의 리소스 소유권에 대한 일반 정보는 을 참조하십시오AWS Control Tower 리소스에 대한 액세스 권한 관리 개요.
- AWS Control Tower가 공유 계정에서 생성하는 리소스에 대한 자세한 내용은 을 참조하십시오공유 계정 정보.
- AWS Control Tower가 Account Factory를 통해 계정을 프로비저닝할 때 생성하는 리소스에 대한 자세한 내용은 을 참조하십시오Account Factory에 대한 리소스 고려 사항.
- AWS Control Tower API와 함께 사용하기 위해 AWS Control Tower에서 정의한 AWS 리소스 유형에 대한 세부 정보를 보려면 사용 설명서의 AWS Control Tower 리소스 유형 참조를 참조하십시오.AWS CloudFormation

AWS 지역별로 AWS Control Tower를 활용하는 방법

현재 AWS Control Tower는 다음 AWS 지역에서 지원됩니다.

- 미국 동부(버지니아 북부)
- 미국 동부(오하이오)
- 미국 서부(오레곤)
- 캐나다(중부)
- 아시아 태평양(시드니)
- 아시아 태평양(싱가포르)
- 유럽(프랑크푸르트)
- 유럽(아일랜드)
- Europe (London)
- 유럽(스톡홀름)
- 아시아 태평양(뭄바이)
- 아시아 태평양(서울)
- 아시아 태평양(도쿄)
- 유럽(파리)
- 남아메리카(상파울루)
- 미국 서부(캘리포니아 북부)
- 아시아 태평양(홍콩)
- 아시아 태평양(자카르타)
- 아시아 태평양(오사카)
- 유럽(밀라노)
- 아프리카(케이프타운)
- 중동(바레인)
- 이스라엘(텔아비브)
- 중동(UAE)
- 유럽(스페인)
- 아시아 태평양(하이데라바드)
- 유럽(취리히)

- 아시아 태평양(멜버른)
- 캐나다 서부(캘거리)

거주 지역 정보

랜딩 존을 생성하면 AWS 관리 콘솔에 액세스하는 데 사용하는 리전이 AWS Control Tower의 홈 AWS 리전이 됩니다. 생성 프로세스 중에 일부 리소스가 홈 리전에 프로비저닝됩니다. OU 및 AWS 계정과 같은 기타 리소스는 전 세계에 있습니다.

홈 지역을 선택한 후에는 변경할 수 없습니다.

제어 및 지역

현재 모든 예방 통제는 전 세계적으로 시행되고 있습니다. 그러나 탐지 및 사전 예방적 제어는 AWS Control Tower가 지원되는 지역에서만 작동합니다. 새 지역에서 AWS Control Tower를 활성화할 때의 제어 동작에 대한 자세한 내용은 을 참조하십시오AWS 컨트롤 타워 지역 구성.

AWS 컨트롤 타워 지역 구성

이 섹션에서는 AWS Control Tower 랜딩 존을 새 리전으로 확장하거나 랜딩 존 구성에서 AWS 리전을 제거할 때 예상할 수 있는 동작을 설명합니다. 일반적으로 이 작업은 AWS Control Tower 콘솔의 업데이트 기능을 통해 수행됩니다.

> **Note**
>
> AWS Control Tower 랜딩 존을 워크로드를 실행할 필요가 없는 AWS 지역으로 확장하지 않는 것이 좋습니다. 리전에서 옵트아웃해도 해당 리전에 리소스를 배포할 수 있는 것은 아니지만, 해당 리소스는 AWS Control Tower 거버넌스의 범위를 벗어나게 됩니다.

새 지역을 구성하는 동안 AWS Control Tower는 랜딩 존을 업데이트합니다. 즉, 랜딩 존의 기준이 됩니다.

- 새로 선택된 모든 지역에서 활발하게 운영되고,
- 선택되지 않은 지역의 자원 관리를 중단합니다.

AWS Control Tower에서 관리하는 조직 단위 (OU) 내의 개별 계정은 이 랜딩 존 업데이트 프로세스의 일부로 업데이트되지 않습니다. 따라서 OU를 다시 등록하여 계정을 업데이트해야 합니다.

AWS Control Tower 지역을 구성할 때는 다음 권장 사항 및 제한 사항을 숙지하십시오.

- AWS 리소스 또는 워크로드를 호스팅할 계획이 있는 지역을 선택하십시오.
- 리전에서 옵트아웃해도 해당 리전에 리소스를 배포할 수 있는 것은 아니지만, 해당 리소스는 AWS Control Tower 거버넌스의 범위를 벗어나게 됩니다.

새 지역에 대한 랜딩 존을 구성할 때 AWS Control Tower 탐지 컨트롤은 다음 규칙을 준수합니다.

- 기존 요소의 가드레일 동작은 동일하게 유지. 기존 계정, 기존 OU 및 기존 리전의 감지 및 방지 가드레일 동작은 변경되지 않습니다.
- 업데이트되지 않은 계정을 포함하는 기존 OU에는 새로운 탐지 제어를 적용할 수 없습니다. AWS Control Tower 랜딩 존을 새 리전으로 구성한 경우 (랜딩 존 업데이트), 기존 OU의 기존 계정을 업데이트해야 해당 OU 및 계정에서 새로운 탐지 제어를 활성화할 수 있습니다.
- 계정을 업데이트하는 즉시 기존 탐지 컨트롤이 새로 구성된 지역에서 작동하기 시작합니다. 새 지역을 구성하도록 AWS Control Tower 랜딩 존을 업데이트한 다음 계정을 업데이트하면 OU에 이미 활성화되어 있는 탐지 컨트롤이 새로 구성된 지역의 해당 계정에서 작동하기 시작합니다.

AWS Control 타워 지역 구성

1. 다음 주소에서 AWS Control Tower 콘솔에 로그인하십시오. https://console.aws.amazon.com/controltower
2. 왼쪽 창 탐색 메뉴에서 랜딩 존 설정을 선택합니다.
3. 랜딩 존 설정 페이지의 세부 정보 섹션에서 오른쪽 상단의 설정 수정 버튼을 선택합니다. 새 지역을 관리하거나 지역을 거버넌스에서 제거하려면 최신 랜딩 존 버전으로 업데이트해야 하기 때문에 랜딩 존 업데이트 워크플로로 이동합니다.
4. 거버넌스를 위한 추가 AWS 지역에서 관리하려는 (또는 관리를 중단하려는) 지역을 검색하십시오. 주 열에는 현재 관할하는 지역과 관리하지 않는 지역이 표시됩니다.
5. 관리할 각 추가 지역의 확인란을 선택합니다. 거버넌스를 제거하려는 각 지역의 체크박스를 선택해제하십시오.

   > **Note**
   >
   > 지역을 관리하지 않기로 선택한 경우에도 해당 지역에 리소스를 배포할 수 있지만 해당 리소스는 AWS Control Tower 거버넌스의 범위를 벗어납니다.

6. 나머지 워크플로를 완료한 다음, Update landding Zone을 선택합니다.

7. Landing Zone 설정이 완료되면 OU를 다시 등록하여 새 지역의 계정을 업데이트하십시오. 자세한 정보는 AWS 컨트롤 타워 OU 및 계정 업데이트 시기을 참조하세요.

새 지역을 구성한 후 개별 계정을 프로비저닝하거나 업데이트하는 또 다른 방법은 Service Catalog의 API 프레임워크를 사용하고 일괄 프로세스로 계정을 AWS CLI업데이트하는 것입니다. 자세한 정보는 자동화를 사용하여 계정을 프로비저닝하고 업데이트합니다.을 참조하세요.

지역을 구성할 때 복합 거버넌스를 피하세요.

AWS Control Tower 거버넌스를 새 것으로 확장한 후 AWS 리전, 그리고 AWS Control Tower 거버넌스를 지역에서 제거한 후에는 OU의 모든 계정을 업데이트하는 것이 중요합니다.

복합 거버넌스는 OU를 관리하는 제어 항목이 OU 내 각 계정을 관리하는 제어 항목과 완전히 일치하지 않는 경우 발생할 수 있는 바람직하지 않은 상황입니다. AWS Control Tower가 거버넌스를 새로운 AWS 리전것으로 확장하거나 거버넌스를 제거한 후 계정이 업데이트되지 않으면 OU에서 혼합 거버넌스가 발생합니다.

이 경우 OU 내의 특정 계정은 OU의 다른 계정과 비교할 때 또는 랜딩 영역의 전반적인 거버넌스 상태와 비교할 때 지역마다 다른 통제가 적용될 수 있습니다.

복합 거버넌스가 있는 OU에서 새 계정을 프로비저닝하면 새 계정이 랜딩 영역과 동일한 (업데이트된) 지역 및 OU 거버넌스 상태를 받게 됩니다. 하지만 아직 업데이트되지 않은 기존 계정에는 업데이트된 지역 거버넌스 상태가 적용되지 않습니다.

일반적으로 복합 거버넌스는 AWS Control Tower 콘솔에서 모순되거나 부정확한 상태 지표를 생성할 수 있습니다. 예를 들어 복합 거버넌스 중에는 아직 업데이트되지 않은 계정에 대해 등록된 OU에 옵트인 지역이 비규제 상태로 표시됩니다.

> **Note**
>
> AWS Control Tower는 복합 거버넌스 상태에서는 제어 기능을 활성화하는 것을 허용하지 않습니다.

복합 거버넌스 기간 동안의 규제 동작

- 복합 거버넌스 중에는 OU의 일부 계정이 업데이트되지 않았기 때문에 OU에 이미 규제 대상으로 표시된 지역에 AWS Config 규칙 (즉, 탐지 제어) 을 기반으로 하는 제어 항목을 일관되게 배포할 수 없습니다. `FAILED_TO_ENABLE`오류 메시지가 표시될 수 있습니다.

- 복합 거버넌스 중에 OU의 계정이 아직 업데이트되지 않은 상태에서 랜딩 영역의 거버넌스를 옵트인 지역으로 확장하면 OU의 `EnableControl` API 작업이 탐지 및 사전 제어에 실패합니다. OU 내에서 업데이트되지 않은 구성원 계정이 아직 해당 지역에서 옵트인되지 않았으므로 `FAILED_TO_ENABLE` 오류 메시지가 표시됩니다.
- 복합 거버넌스의 경우, Security Hub Service 관리형 표준: AWS Control Tower에 속하는 규제 항목은 랜딩 존 구성과 업데이트되지 않은 계정 간에 불일치가 있는 지역에서 규정 준수를 정확하게 보고할 수 없습니다.
- 복합 거버넌스는 모든 관리 지역의 OU 내 모든 계정에 균일하게 적용되는 SCP 기반 제어 (예방 제어) 의 동작을 변경하지 않습니다.

> **Note**
>
> 복합 거버넌스는 드리프트와 동일하지 않으며 드리프트로 보고되지도 않습니다.

복합 거버넌스를 복구하기 위해

- 콘솔의 Organizations 페이지에 업데이트 가능 상태가 표시된 OU의 각 계정에 대해 계정 업데이트를 선택합니다.
- 계정이 300개 미만인 OU의 경우 OU의 모든 계정을 자동으로 업데이트하는 Organizations 페이지에서 OU 재등록을 선택합니다.

옵트인 지역 활성화 AWS 고려 사항

AWS 리전 대부분은 기본적으로 AWS 계정활성화되지만 특정 지역은 수동으로 선택한 경우에만 활성화됩니다. 이 문서에서는 이러한 지역을 옵트인 지역이라고 합니다. 반면, 계정을 AWS 계정 만들자마자 기본적으로 활성화되는 지역은 상업 지역 또는 간단히 말해 지역이라고 합니다.

옵트인이라는 용어는 역사적 근거를 가지고 있습니다. 2019년 3월 20일 이후에 AWS 리전 도입된 모든 지역은 옵트인 지역으로 간주됩니다. 옵트인 지역은 옵트인 지역에서 활성화된 계정을 통한 IAM 데이터 공유와 관련하여 상업 지역보다 보안 요구 사항이 더 높습니다. 사용자, 그룹, 역할, 정책, ID 공급자, 관련 데이터 (예: X.509 서명 인증서 또는 컨텍스트별 자격 증명), 암호 정책 및 계정 별칭과 같은 기타 계정 수준 설정을 포함하여 IAM 서비스를 통해 관리되는 모든 데이터는 ID 데이터로 간주됩니다.

랜딩 존 설정 중에 옵트인 지역을 선택하여 자동으로 활성화할 수 있습니다. 선택한 모든 지역에서 Landing Zone이 활성화됩니다.

옵트인 지역을 AWS Control Tower 홈 지역으로 선택하려면 먼저 AWS Management Console에 로그인한 후 지역 활성화의 단계에 따라 활성화하십시오. 옵트인 지역에서 기존 로그 아카이브 및 감사 계정을 가져오려면 먼저 해당 지역을 수동으로 활성화하십시오.

AWS 옵트인 지역에는 AWS Control Tower를 사용할 수 있는 여러 지역이 포함됩니다.

- 아시아 태평양 (홍콩) 지역, ap-east-1
- 아시아 태평양 (자카르타) 지역, ap-southeast-3
- 유럽 (밀라노) 지역, eu-south-1
- 아프리카 (케이프타운) 지역, af-south-1
- 중동 (바레인) 지역, me-south-1
- 이스라엘 (텔아비브), il-central-1
- 중동 (UAE) 지역, me-central-1
- 유럽 (스페인) 지역, eu-south-2
- 아시아 태평양 (하이데라바드) 지역, ap-south-2
- 유럽 (취리히) 지역, eu-central-2
- 아시아 태평양 (멜버른) 지역, ap-southeast-4
- 캐나다 서부 (캘거리) 지역, ca-west-1

AWS Control Tower에는 옵트인 리전과 상용 리전에서 다르게 작동하는 일부 컨트롤이 있습니다. 자세한 정보는 관리 제한을 참조하세요. 다음은 옵트인 지역에 워크로드를 배포할 때 염두에 두어야 할 몇 가지 고려 사항입니다.

> **관리 또는 활성화?**
>
> 지역 관리는 AWS Control Tower 콘솔에서 선택할 수 있는 작업이므로 해당 지역에 제어를 적용할 수 있다는 점을 기억하십시오. 옵트인 지역을 활성화하거나 비활성화하는 것은 AWS 콘솔에서 선택할 수 있는 다른 작업이며, 이렇게 하면 계정에 해당 지역이 열리고 리전에 리소스와 워크로드를 배포할 수 있습니다.

동작 고려 사항

- 옵트인 지역을 관리하기로 선택한 경우 워크로드에 장애가 발생할 수 있으므로 관리되는 옵트인 지역을 비활성화 (옵트아웃) 하지 않는 것이 좋습니다. AWS Control Tower에서는 AWS Control Tower

콘솔 내에서 규제 지역을 비활성화할 수 없지만, AWS Billing 콘솔 또는 SDK와 같은 AWS Control Tower 외부 소스에서 규제 지역을 비활성화하지 않도록 주의하십시오. AWS

- AWS Control Tower가 거버넌스를 옵트인 지역으로 확장하면 모든 멤버 계정에서 해당 리전에 대한 옵트인 (옵트인) 이 활성화됩니다. 거버넌스에서 지역을 제거해도 AWS Control Tower는 멤버 계정에서 해당 지역을 비활성화 (옵트아웃) 하지 않습니다.
- 지역 선택 취소 시 AWS Control Tower는 옵트인 지역 (예: AWS Billing Console 또는 SDK) 의 AWS Control Tower 외부 소스의 계정에 대해 해당 지역을 수동으로 비활성화한 경우 옵트인 지역에서 리소스를 제거하지 않습니다. AWS 비활성화한 지역에서 리소스를 제거하는 것이 좋습니다. 그렇지 않으면 해당 리소스에 대해 예상치 못한 청구 요금이 부과될 수 있습니다.
- 랜딩 존이 사용 중지되면 AWS Control Tower는 옵트인 지역을 포함하여 모든 관리 대상 지역의 리소스를 정리합니다. 하지만 AWS Control Tower는 옵트인 지역을 비활성화하지 않습니다. 서비스 해제 후 추가 단계로 옵트인 지역을 비활성화할 수 있습니다.
- 홈 지역이 옵트인 지역이고 기존 계정을 로그 아카이브 및 감사 계정으로 등록하려는 경우 먼저 옵트인 지역을 수동으로 활성화해야 랜딩 존의 홈 지역으로 선택할 수 있습니다. 지역 활성화를 참조하십시오.
- 옵트인 지역을 홈 리전으로 설정하여 AWS AWS Control Tower를 설정하고 다른 리전의 콘솔에서 AWS Control Tower 서비스를 방문해도 콘솔은 자동으로 홈 리전으로 리디렉션하지 않습니다.
- 기본 API에는 용량 제한이 있어 지역, 계정 및 서비스 부하 수에 따라 지연 시간이 몇 분에서 몇 시간까지 늘어날 수 있습니다. 가장 좋은 방법은 워크로드를 실행할 AWS 리전 지역에만 옵트인하고 한 번에 한 지역씩 옵트인하는 것입니다.

거버넌스 및 통제에 대한 중요한 제한사항

- 옵트인 리전에서 지원되지 않는 AWS Control Tower 컨트롤을 현재 활성화한 경우, 해당 리전에서 컨트롤이 지원되기 전까지는 해당 옵트인 리전으로 AWS Control Tower 거버넌스를 확장할 수 없습니다. 자세한 내용은 관리 제한단원을 참조하세요.
- AWS Control Tower 거버넌스를 특정 컨트롤이 지원되지 않는 옵트인 리전으로 확장하는 경우, AWS Control Tower로 규제하는 모든 리전에서 컨트롤이 지원되기 전까지는 어느 지역에서도 제어를 활성화할 수 없습니다. 자세한 내용은 을 참조하십시오. 관리 제한
- 옵트인 지역을 포함하여 AWS Control Tower를 사용할 수 있는 22개 상업 지역이 모두 활성화되면 거버넌스를 OU로 확장할 때 조직 단위 (OU) 당 계정 수의 상한선이 줄어듭니다. 한도는 계정 300개가 아닌 220개입니다. 이러한 감소는 StackSet 제한으로 인한 것입니다. 계정이 220개가 넘는 OU로 거버넌스를 확장해야 하는 경우 활성화된 지역 수를 줄이십시오.

지역 거부 제어를 구성합니다.

AWS Control Tower는 두 개의 지역 거부 제어를 제공합니다. 하나의 컨트롤이 GRREGIONDENY 활성화되면 전체 랜딩 존에 적용됩니다. 다른 컨트롤이 CTMULTISERVICEPV1 활성화되면 지정한 특정 OU에 적용할 수 있습니다. 자세한 내용은 요청된 항목에 AWS 따른 액세스 거부 AWS 리전및 OU에 적용된 지역 거부 제어를 참조하십시오.

지역 거부 GRREGIONDENY 제어는 특정 OU가 아닌 전체 landing Zone에 적용되므로 고유합니다. 지역 거부 제어를 구성하려면 랜딩 영역 설정 페이지로 이동하여 설정 수정을 선택합니다.

- 이 설정은 나중에 변경할 수 있습니다.
- 활성화된 경우 이 컨트롤은 등록된 모든 OU에 적용됩니다.
- 개별 OU에 대해 이 컨트롤을 구성할 수는 없습니다.

> **Note**
>
> 제어를 적용한 후에는 리소스에 액세스할 수 없으므로 지역 거부 제어를 활성화하기 전에 이러한 지역에 기존 리소스가 없는지 확인하십시오. 컨트롤이 활성화되어 있는 동안에는 거부된 지역에 리소스를 배포할 수 없습니다.

지역 거부 제어는 AWS Control Tower 지역 구성에 따라 AWS 서비스에 대한 액세스를 금지합니다. 미관리 상태인 AWS 지역에 대한 액세스는 거부됩니다. 또한 지역 거부 통제는 AWS Control Tower를 사용할 수 없는 지역에 대한 액세스를 거부합니다. 홈 리전에 대한 액세스를 거부할 수 없습니다. IAM 및 같은 특정 글로벌 AWS 서비스는 지역 AWS Organizations거부 제어에서 제외됩니다. 자세한 내용은 요청에 AWS 따른 액세스 거부를 참조하십시오. AWS 리전

제어를 활성화하면 계층 구조에 등록된 모든 최상위 OU에 적용되며 체인의 하위 OU에 상속됩니다. 컨트롤을 제거하면 등록된 모든 OU에서 제거되고, AWS Control Tower의 모든 비규제 지역은 비규제 상태로 유지되며, AWS Control Tower가 제공되지 않는 지역에 리소스를 배포할 수 있습니다.

- 전체 제어 이름: 요청된 지역에 AWS 따라 액세스를 거부합니다. AWS
- 가드레일 설명: 지정된 지역 이외의 글로벌 및 지역 서비스의 미등록 사업에 대한 액세스를 허용하지 않습니다.
- 이는 예방 지침이 포함된 선택적 통제입니다.

지역 거부 제어 SCP의 템플릿을 보려면 AWS Control Tower Control 참조의 요청에 AWSAWS 리전따른 액세스 거부를 참조하십시오. AWS Control Tower SCP는 의 SCP와 AWS Organizations비슷하지만 동일하지는 않습니다.

지역 서비스 페이지에서 지역 서비스 엔드포인트를 확인할 수 있습니다.

OU 수준 지역 거부 제어에 대한 고려사항

OU 수준 지역 거부 제어에 대한 주요 고려 사항은 두 가지가 모두 활성화된 경우 착륙 지대 지역 거부 제어와 상호 작용하는 방식을 결정하는 것입니다. 자세한 내용은 OU에 적용된 지역 거부 제어를 참조하십시오.

AWS Control Tower에서 계정 프로비저닝 및 관리

이 장에는 AWS Control Tower 랜딩 존에서 멤버 계정을 프로비저닝하고 관리하기 위한 개요와 절차가 포함되어 있습니다.

또한 기존 AWS 계정을 AWS Control Tower에 등록하기 위한 개요 및 절차도 포함되어 있습니다.

AWS Control Tower의 계정에 대한 자세한 내용은 을 참조하십시오AWS Control AWS 계정 타워에 대한 정보. AWS Control Tower에 여러 계정을 등록하는 방법에 대한 자세한 내용은 을 참조하십시오. 기존 조직 단위를 AWS Control Tower에 등록

> **Note**
>
> 프로비저닝, 업데이트 및 등록을 포함하여 최대 5개의 계정 관련 작업을 동시에 수행할 수 있습니다.

프로비저닝 방법

AWS Control Tower는 회원 계정을 생성하고 업데이트하는 몇 가지 방법을 제공합니다. 일부 방법은 주로 콘솔 기반이고 일부 방법은 주로 자동화되어 있습니다.

개요

멤버 계정을 만드는 표준 방법은 서비스 카탈로그의 일부인 콘솔 기반 제품인 Account Factory를 사용하는 것입니다. 랜딩 존이 드리프트 상태가 아닌 경우, 계정 생성을 콘솔에서 새 계정을 추가하는 방법으로 사용하고, 계정 등록을 사용하여 기존 AWS 계정을 AWS Control Tower에 등록할 수 있습니다.

Account Factory를 사용하면 AWS 컨트롤 타워 기본 설정을 사용하여 기본 계정을 프로비저닝할 수 있습니다. 또한 특수 사용 사례의 요구 사항을 충족하는 사용자 지정 계정을 프로비저닝할 수 있습니다.

AFC (Account Factory Customization) 는 AWS Control Tower 콘솔에서 사용자 지정 계정을 프로비저닝하는 방법이며, 계정의 사용자 지정 및 배포를 자동화합니다. 몇 가지 일회성 설정 단계를 거친 후 콘솔 기반의 자동 프로비저닝이 가능하므로 스크립트를 작성하거나 파이프라인을 설정할 필요가 없습니다. 자세한 정보는 AFC (Account Factory Customize) 로 계정을 사용자 지정하세요을 참조하세요.

콘솔 기반 메서드:

- 기본 계정 또는 사용자 지정 계정의 경우 Account Factory 콘솔을 통해 AWS Service Catalog세부 정보 및 Account Factory를 통한 계정 제공 및 관리 지침을 검토하십시오.

- 랜딩 존이 드리프트 상태에 있지 않은 경우, AWS Control Tower의 계정 등록 기능을 통해 기존 계정 등록를 참조하세요.
- AWS Control Tower 콘솔에서는 Account Factory를 사용하여 동시에 최대 5개의 계정을 생성, 업데이트 또는 등록할 수 있습니다.

자동화된 방법:

- Lambda 코드: AWS Control Tower 랜딩 존의 관리 계정에서 Lambda 코드 및 적절한 IAM 역할을 사용합니다. IAM 역할을 사용한 자동 계정 프로비저닝을 참조하십시오.
- 테라폼: Account Factory와 모델을 기반으로 계정 프로비저닝 및 GitOps 업데이트를 자동화할 수 있는 AWS Control Tower Account Factory for Terraform (AFT) 에서 가져온 것입니다. 테라폼용 AWS Control Tower 어카운트 팩토리 (AFT) 를 통해 계정 프로비저닝 를 참조하세요.
- AWS Control Tower 콘솔의 Account Factory 사용자 지정: 설정 단계가 끝나면 향후 사용자 지정 계정을 프로비저닝할 때 추가 구성이나 파이프라인 유지 관리가 필요하지 않습니다. 계정은 블루프린트라는 AWS Service Catalog 제품을 통해 프로비저닝됩니다. 블루프린트는 템플릿 또는 Terraform AWS CloudFormation 템플릿을 사용할 수 있습니다.

> **Note**
>
> AWS CloudFormation 블루프린트는 리소스를 여러 지역에 배포할 수 있습니다. Terraform 블루프린트는 단일 지역에만 리소스를 배포할 수 있습니다. 기본적으로 이 지역이 홈 지역입니다.

AWS Control Tower가 계정을 생성하면 어떻게 되나요?

AWS Control Tower의 새 계정은 AWS Control Tower AWS Organizations, 및 간의 상호 작용을 통해 생성되고 프로비저닝됩니다. AWS Service Catalog AWS Control Tower AWS 계정 콘솔을 사용하여 기존 콘솔을 등록하는 단계는 을 참조하십시오기존 계정 등록.

계정 생성의 비하인드 스토리

1. 예를 들어, AWS Control Tower Account Factory 페이지에서 또는 AWS Service Catalog 콘솔에서 직접 또는 Service Catalog `ProvisionProduct` API를 호출하여 요청을 시작합니다.
2. AWS Service Catalog AWS Control Tower에 전화를 겁니다.
3. AWS Control Tower는 첫 단계로 AWS Organizations `CreateAccount` API를 호출하는 워크플로를 시작합니다.

4. 계정을 AWS Organizations 생성한 후, AWS Control Tower는 청사진과 제어를 적용하여 프로비저닝 프로세스를 완료합니다.
5. Service Catalog는 계속해서 AWS Control Tower를 폴링하여 프로비저닝 프로세스가 완료되었는지 확인합니다.
6. AWS Control Tower의 워크플로가 완료되면 Service Catalog는 계정 상태를 확정하고 사용자 (요청자) 에게 결과를 알려줍니다.

계정에 필요한 권한

계정을 프로비저닝하고 업데이트하는 각 방법에 필요한 권한은 각 섹션에서 각각 설명합니다. 적절한 사용자 그룹 권한이 있으면 제공자는 조직의 모든 계정에 대해 표준화된 기준과 네트워크 구성을 지정할 수 있습니다.

> **Note**
>
> 계정을 프로비전할 때 계정 요청자는 항상 및 권한을 가지고 있어야 합니다. `CreateAccount` `DescribeCreateAccountStatus` 이 권한 집합은 관리자 역할의 일부이며 요청자가 관리자 역할을 맡으면 자동으로 부여됩니다. 계정을 프로비저닝할 권한을 위임하는 경우 계정 요청자를 위해 이러한 권한을 직접 추가해야 할 수 있습니다.

Account Factory를 사용하여 AWS Control Tower 콘솔에서 계정을 생성할 때는 AWS Control Tower 콘솔 사용 권한과 함께 `AWSServiceCatalogEndUserFullAccess` 정책이 활성화된 IAM 사용자의 계정으로 로그인해야 하며 루트 사용자로 로그인할 수 없습니다.

AWS Control Tower에 필요한 권한에 대한 일반적인 정보는 을 참조하십시오AWS Control Tower에 대한 자격 증명 기반 정책 (IAM 정책) 사용. AWS Control Tower의 역할 및 계정에 대한 자세한 내용은 역할 및 계정을 참조하십시오.

> **계정 보안**
>
> AWS Organizations 설명서에서 AWS Control Tower 관리 계정 및 회원 계정의 보안을 보호하는 모범 사례에 대한 지침을 찾을 수 있습니다.
>
> - 관리 계정 모범 사례
> - 회원 계정 모범 사례

AWS Control AWS 계정 타워에 대한 정보

AWS 계정 An은 소유한 모든 리소스를 담는 컨테이너입니다. 이러한 리소스에는 계정에서 허용하는 AWS Identity and Access Management (IAM) ID가 포함되며, 이를 통해 해당 계정에 액세스할 수 있는 사용자를 결정합니다. IAM ID에는 사용자, 그룹, 역할 등이 포함될 수 있습니다. AWS Control Tower에서 IAM, 사용자, 역할 및 정책을 사용하는 방법에 대한 자세한 내용은 AWS Control Tower의 자격 증명 및 액세스 관리를 참조하십시오.

리소스 및 계정 생성 시간

AWS Control Tower는 계정을 생성하거나 등록할 때 Account Factory 템플릿 형태의 리소스와 랜딩 존의 기타 리소스를 포함하여 계정에 필요한 최소 리소스 구성을 배포합니다. 이러한 리소스에는 IAM 역할, AWS CloudTrail 트레일, Service Catalog 프로비저닝 제품, IAM ID 센터 사용자 등이 포함될 수 있습니다. 또한 AWS Control Tower는 제어 구성에서 요구하는 대로 새 계정이 멤버 계정이 될 조직 단위(OU) 에 리소스를 배포합니다.

AWS Control Tower는 사용자를 대신하여 이러한 리소스의 배포를 조정합니다. 배포를 완료하는 데 리소스당 몇 분이 소요될 수 있으므로 계정을 만들거나 등록하기 전에 총 시간을 고려하십시오. 계정의 리소스 관리에 대한 자세한 내용은 을 참조하십시오AWS Control Tower 리소스 생성 및 수정 지침.

기존 보안 또는 로깅 계정을 가져올 때 고려할 사항

보안 또는 로깅 계정으로 승인하기 전에 AWS Control Tower는 계정에 AWS Control Tower 요구 사항과 충돌하는 리소스가 있는지 확인합니다. AWS 계정 예를 들어, AWS Control Tower에서 요구하는 것과 동일한 이름의 로깅 버킷이 있을 수 있습니다. 또한 AWS Control Tower는 계정이 리소스를 프로비저닝할 수 있는지 확인합니다. 예를 들어, AWS Security Token Service (AWS STS) 가 활성화되어 있고 계정이 일시 중단되지 않았는지, AWS Control Tower가 계정 내에서 리소스를 프로비저닝할 권한이 있는지 확인합니다.

AWS Control Tower는 사용자가 제공한 로깅 및 보안 계정의 기존 리소스를 제거하지 않습니다. 하지만 거부 기능을 활성화하기로 선택한 경우 지역 AWS 리전 거부 제어는 거부된 지역의 리소스에 대한 액세스를 차단합니다.

계정 보기

조직 페이지에는 OU 또는 AWS Control Tower의 등록 상태와 상관없이 조직 내 모든 OU와 계정이 나열됩니다. 각 계정이 등록 전제 조건을 충족하는 경우 회원 계정을 개별적으로 또는 OU 그룹별로 보고 AWS Control Tower에 등록할 수 있습니다.

조직 페이지에서 특정 계정을 보려면 오른쪽 상단의 드롭다운 메뉴에서 계정만을 선택한 다음 표에서 계정 이름을 선택하면 됩니다. 또는 테이블에서 상위 OU의 이름을 선택하고 해당 OU의 세부 정보 페이지에서 해당 OU 내의 모든 계정 목록을 볼 수 있습니다.

조직 페이지와 계정 세부 정보 페이지에서 다음 중 하나인 계정 상태를 확인할 수 있습니다.

- 미등록 — 계정이 상위 OU의 구성원이지만 AWS Control Tower에서 완전히 관리하지는 않습니다. 상위 OU가 등록된 경우 해당 계정은 등록된 상위 OU에 대해 구성된 예방 제어 항목에 의해 관리되지만 OU의 탐지 컨트롤은 이 계정에는 적용되지 않습니다. 상위 OU가 등록되지 않은 경우 이 계정에는 컨트롤이 적용되지 않습니다.
- 등록 — AWS Control Tower에서 계정을 거버넌스로 전환하고 있습니다. 상위 OU의 제어 구성에 맞게 계정을 조정하고 있습니다. 이 프로세스에는 계정 리소스당 몇 분이 소요될 수 있습니다.
- 등록됨 - 이 계정은 상위 OU에 구성된 컨트롤에 의해 관리됩니다. AWS Control Tower에서 완벽하게 관리합니다.
- 등록 실패 — 계정을 AWS Control Tower에 등록할 수 없습니다. 자세한 정보는 등록 실패의 일반적인 원인을 참조하세요.
- 업데이트 가능 — 계정에 업데이트가 있습니다. 이 상태의 계정은 아직 등록 상태이지만 환경에 적용된 최근 변경 사항을 반영하도록 계정을 업데이트해야 합니다. 단일 계정을 업데이트하려면 계정 세부 정보 페이지로 이동한 다음 계정 업데이트를 선택합니다.

  단일 OU에 이 상태의 계정이 여러 개 있는 경우 OU를 다시 등록하고 해당 계정을 함께 업데이트할 수 있습니다.

공유 계정에서 생성된 리소스

이 섹션에서는 착륙 지대를 설정할 때 AWS Control Tower가 공유 계정에 생성하는 리소스를 보여줍니다.

회원 계정 리소스에 대한 자세한 내용은 을 참조하십시오Account Factory에 대한 리소스 고려 사항.

관리 계정 리소스

landing Zone을 설정하면 관리 계정 내에 다음과 같은 AWS 리소스가 생성됩니다.

AWS 서비스	리소스 유형	리소스 이름
AWS Organizations	계정	audit

AWS 서비스	리소스 유형	리소스 이름
		log archive
AWS Organizations	OU	Security Sandbox
AWS Organizations	서비스 제어 정책	aws-guardrails-*
AWS CloudFormation	스택	AWSControlTowerBP-BASELINE-CLOUDTRAIL-MASTER AWSControlTowerBP-BASELINE-CONFIG-MASTER(버전 2.6 이상)

AWS 서비스	리소스 유형	리소스 이름
AWS CloudFormation	StackSets	AWSControlTowerBP-BASELINE-CLOUDTRAIL(3.0 이상에는 배포되지 않음) AWSControlTowerBP_BASELINE_SERVICE_LINKED_ROLE (Deployed in 3.2 and later) AWSControlTowerBP-BASELINE-CLOUDWATCH AWSControlTowerBP-BASELINE-CONFIG AWSControlTowerBP-BASELINE-ROLES AWSControlTowerBP-BASELINE-SERVICE-ROLES AWSControlTowerBP-SECURITY-TOPICS AWSControlTowerGuardrailAWS-GR-AUDIT-BUCKET-PUBLIC-READ-PROHIBITED AWSControlTowerGuardrailAWS-GR-AUDIT-BUCKET-PUBLIC-WRITE-PROHIBITED AWSControlTowerLoggingResources

AWS 서비스	리소스 유형	리소스 이름
		AWSControlTowerSecurityResources AWSControlTowerExecutionRole
AWS Service Catalog	제품	AWS Control 타워 어카운트 팩토리
AWS Config	집계자	aws-controltower-ConfigAggregatorForOrganizations
AWS CloudTrail	추적	aws-controltower-BaselineCloudTrail
아마존 CloudWatch	CloudWatch 로그	aws-controltower/CloudTrailLogs
AWS Identity and Access Management	역할	AWSControlTowerAdmin AWSControlTowerStackSetRole AWSControlTowerCloudTrailRolePolicy
AWS Identity and Access Management	정책	AWSControlTowerServiceRolePolicy AWSControlTowerAdminPolicy AWSControlTowerCloudTrailRolePolicy AWSControlTowerStackSetRolePolicy

AWS 서비스	리소스 유형	리소스 이름
AWS IAM Identity Center	디렉터리 그룹	AWSAccountFactory AWSAuditAccountAdmins AWSControlTowerAdmins AWSLogArchiveAdmins AWSLogArchiveViewers AWSSecurityAuditors AWSSecurityAuditPowerUsers AWSServiceCatalogAdmins
AWS IAM Identity Center	권한 세트	AWSAdministratorAccess AWSPowerUserAccess AWSServiceCatalogAdminFullAccess AWSServiceCatalogEndUserAccess AWSReadOnlyAccess AWSOrganizationsFullAccess

Note

landing Zone 버전 3.0 이상에는 AWS CloudFormation StackSet `BP_BASELINE_CLOUDTRAIL` 배포되지 않습니다. 그러나 착륙 지대를 업데이트할 때까지 이전 버전의 착륙 지대에는 계속 존재합니다.

로그 아카이브 계정 리소스

landing Zone을 설정하면 로그 아카이브 계정 내에 다음과 같은 AWS 리소스가 생성됩니다.

AWS 서비스	리소스 유형	Resource Name
AWS CloudFormation	스택	StackSet-AWSControlTowerGuardrailAWS-GR-AUDIT-BUCKET-PUBLIC-READ-PROHIBITED- StackSet-AWSControlTowerGuardrailAWS-GR-AUDIT-BUCKET-PUBLIC-WRITE-PROHIBITED StackSet-AWSControlTowerBP-BASELINE-CLOUDWATCH- StackSet-AWSControlTowerBP-BASELINE-CONFIG- StackSet-AWSControlTowerBP-BASELINE-CLOUDTRAIL- StackSet-AWSControlTowerBP-BASELINE-SERVICE-ROLES- StackSet-AWSControlTowerBP-BASELINE-SERVICE-LINKED-ROLE-(In 3.2 and later) StackSet-AWSControlTowerBP-BASELINE-ROLES-

AWS 서비스	리소스 유형	Resource Name
		StackSet-AWSControlTowerLoggingResources-
AWS Config	AWS Config 규칙	AWSControlTower_AWS-GR_AUDIT_BUCKET_PUBLIC_READ_PROHIBITED AWSControlTower_AWS-GR_AUDIT_BUCKET_PUBLIC_WRITE_PROHIBIT
AWS CloudTrail	추적	aws-controltower-BaselineCloudTrail
아마존 CloudWatch	CloudWatch 이벤트 규칙	aws-controltower-ConfigComplianceChangeEventRule
아마존 CloudWatch	CloudWatch 로그	/aws/lambda/aws-controltower-NotificationForwarder
AWS Identity and Access Management	역할	aws-controltower-AdministratorExecutionRole aws-controltower-CloudWatchLogsRole aws-controltower-ConfigRecorderRole aws-controltower-ForwardSnsNotificationRole aws-controltower-ReadOnlyExecutionRole AWSControlTowerExecution

AWS 서비스	리소스 유형	Resource Name
AWS Identity and Access Management	정책	AWSControlTowerServiceRolePolicy
Amazon Simple Notification Service	주제	aws-controltower-SecurityNotifications
AWS Lambda	애플리케이션	StackSet-AWSControlTowerBP-BASELINE-CLOUDWATCH-*
AWS Lambda	함수	aws-controltower-NotificationForwarder
Amazon Simple Storage Service(S3)	버킷	aws-controltower-logs-* aws-controltower-s3-access-logs-*

감사 계정 리소스

landing Zone을 설정하면 감사 계정 내에 다음과 같은 AWS 리소스가 생성됩니다.

AWS 서비스	리소스 유형	리소스 이름
AWS CloudFormation	스택	StackSet-AWSControlTowerGuardrailAWS-GR-AUDIT-BUCKET-PUBLIC-READ-PROHIBITED- StackSet-AWSControlTowerGuardrailAWS-GR-AUDIT-BUCKET-PUBLIC-WRITE-PROHIBITED-

AWS 서비스	리소스 유형	리소스 이름
		StackSet-AWSControlTowerBP-BASELINE-CLOUDWATCH- StackSet-AWSControlTowerBP-BASELINE-CONFIG- StackSet-AWSControlTowerBP-BASELINE-CLOUDTRAIL- StackSet-AWSControlTowerBP-BASELINE-SERVICE-ROLES- StackSet-AWSControlTowerBP-BASELINE-SERVICE-LINKED-ROLE-(In 3.2 and later) StackSet-AWSControlTowerBP-SECURITY-TOPICS- StackSet-AWSControlTowerBP-BASELINE-ROLES- StackSet-AWSControlTowerSecurityResources-*
AWS Config	집계자	aws-controltower-GuardrailsComplianceAggregator

AWS 서비스	리소스 유형	리소스 이름
AWS Config	AWS Config 규칙	AWSControlTower_AWS-GR_AUDIT_BUCKET_PUBLIC_READ_PROHIBITED AWSControlTower_AWS-GR_AUDIT_BUCKET_PUBLIC_WRITE_PROHIBITED
AWS CloudTrail	추적	aws-controltower-BaselineCloudTrail
아마존 CloudWatch	CloudWatch 이벤트 규칙	aws-controltower-ConfigComplianceChangeEventRule
아마존 CloudWatch	CloudWatch 로그	/aws/lambda/aws-controltower-NotificationForwarder

AWS 서비스	리소스 유형	리소스 이름
AWS Identity and Access Management	역할	aws-controltower-AdministratorExecutionRole aws-controltower-CloudWatchLogsRole aws-controltower-ConfigRecorderRole aws-controltower-ForwardSnsNotificationRole aws-controltower-ReadOnlyExecutionRole aws-controltower-AuditAdministratorRole aws-controltower-AuditReadOnlyRole AWSControlTowerExecution
AWS Identity and Access Management	정책	AWSControlTowerServiceRolePolicy
Amazon Simple Notification Service	주제	aws-controltower-AggregateSecurityNotifications aws-controltower-AllConfigNotifications aws-controltower-SecurityNotifications
AWS Lambda	함수	aws-controltower-NotificationForwarder

공유 계정 정보

AWS Control AWS 계정 Tower에는 관리 계정, 감사 계정, 로그 아카이브 계정 등 세 개의 특수 계정이 연결되어 있습니다. 이러한 계정은 일반적으로 공유 계정 또는 핵심 계정이라고 합니다.

- Landing Zone을 설정할 때 감사 및 로그 아카이브 계정의 사용자 지정 이름을 선택할 수 있습니다. 계정 이름 변경에 대한 자세한 내용은 AWS Control Tower 리소스 이름 외부 변경을 참조하십시오.
- 또한 초기 랜딩 존 설정 프로세스 중에 기존 AWS 계정 계정을 AWS Control Tower 보안 또는 로깅 계정으로 지정할 수 있습니다. 이 옵션을 사용하면 AWS Control Tower가 새로운 공유 계정을 생성할 필요가 없습니다. (이는 일회성 선택입니다.)

공유 계정 및 관련 리소스에 대한 자세한 내용은 을 참조하십시오공유 계정에서 생성된 리소스.

관리 계정

이로써 AWS Control Tower가 AWS 계정 시작됩니다. 기본적으로 이 계정의 루트 사용자와 이 계정의 IAM 사용자 또는 IAM 관리자는 landing Zone 내의 모든 리소스에 대한 전체 액세스 권한을 가집니다.

> **Note**
>
> AWS Control Tower 콘솔 내에서 관리 기능을 수행할 때는 이 계정의 루트 사용자 또는 IAM 관리자 사용자로 로그인하는 대신 관리자 권한이 있는 IAM Identity Center 사용자로 로그인하는 것이 가장 좋습니다.

관리 계정에서 사용할 수 있는 역할 및 리소스에 대한 자세한 내용은 을 참조하십시오. 공유 계정에서 생성된 리소스

로그 아카이브 계정

Landding Zone을 생성할 때 로그 아카이브 공유 계정이 자동으로 설정됩니다.

이 계정에는 랜딩 존에 있는 다른 모든 계정의 모든 AWS CloudTrail 계정과 AWS Config 로그 파일의 사본을 저장하는 중앙 Amazon S3 버킷이 포함되어 있습니다. 가장 좋은 방법은 규정 준수 및 조사를 담당하는 팀과 관련 보안 또는 감사 도구로만 로그 아카이브 계정 액세스를 제한하는 것입니다. 이 계정은 자동화된 보안 감사에 사용하거나 Lambda 함수와 같은 사용자 지정 AWS Config 규칙함수를 호스팅하여 수정 작업을 수행하는 데 사용할 수 있습니다.

> **Amazon S3 버킷 정책**
>
> AWS Control Tower 랜딩 존 버전 3.3 이상에서는 계정이 감사 버킷에 대한 쓰기 권한 `aws:SourceOrgID` 조건을 충족해야 합니다. 이 조건은 조직 내 계정을 대신하여 S3 버킷에 CloudTrail 로그만 쓸 수 있도록 하고, 조직 외부의 CloudTrail 로그가 AWS Control Tower S3 버킷에 기록하는 것을 방지합니다. 자세한 정보는 AWS 컨트롤 타워 랜딩 존 버전 3.3을 참조하세요.

로그 아카이브 계정에서 사용할 수 있는 역할 및 리소스에 대한 자세한 내용은 을 참조하십시오. 로그 아카이브 계정 리소스

> **Note**
>
> 이러한 로그는 변경할 수 없습니다. 모든 로그는 계정 활동과 관련된 감사 및 규정 준수 조사 목적으로 저장됩니다.

감사 계정

이 공유 계정은 landing Zone을 생성할 때 자동으로 설정됩니다.

감사 계정은 Landing Zone의 모든 계정에 대해 감사자 (읽기 전용) 및 관리자 (전체 액세스) 계정 간 역할을 가진 보안 및 규정 준수 팀으로 제한해야 합니다. 보안 및 규정 준수 팀은 이러한 역할을 다음과 같은 용도로 사용하기 위한 것입니다.

- 사용자 지정 AWS Config 규칙 Lambda 함수 호스팅과 같은 AWS 메커니즘을 통해 감사를 수행합니다.
- 수정 조치와 같은 자동화된 보안 작업을 수행합니다.

감사 계정은 Amazon Simple Notification 서비스 (Amazon SNS) 서비스를 통해서도 알림을 받습니다. 다음과 같은 세 가지 범주의 알림을 받을 수 있습니다.

- 모든 구성 이벤트 - 이 항목에서는 landing Zone에 있는 모든 계정의 모든 CloudTrail AWS Config 알림과 알림을 집계합니다.
- 보안 알림 집계 - 이 항목에서는 특정 CloudWatch 이벤트, AWS Config 규칙 규정 준수 상태 변경 이벤트 및 조사 결과의 모든 보안 알림을 집계합니다. GuardDuty

- 드리프트 알림 — 이 항목은 랜딩 존의 모든 계정, 사용자, OU, SCP에서 발견된 모든 드리프트 경고를 집계합니다. 드리프트에 대한 자세한 내용은 을 참조하십시오. AWS Control Tower의 드리프트 감지 및 해결

멤버 계정 내에서 트리거되는 감사 알림은 로컬 Amazon SNS 주제에 알림을 보낼 수도 있습니다. 이 기능을 통해 계정 관리자는 개별 회원 계정에만 적용되는 감사 알림을 구독할 수 있습니다. 따라서 관리자는 모든 계정 알림을 중앙 감사 계정에 집계하면서 개별 계정에 영향을 미치는 문제를 해결할 수 있습니다. 자세한 설명은 Amazon Simple Notification Service 개발자 안내서를 참조하세요.

감사 계정에서 사용할 수 있는 역할 및 리소스에 대한 자세한 내용은 을 참조하십시오. 감사 계정 리소스

프로그래밍 방식 감사에 대한 자세한 내용은 AWS Control Tower 감사 계정의 프로그래밍 역할 및 신뢰 관계를 참조하십시오.

> **Important**
>
> 감사 계정에 제공한 이메일 주소는 AWS Control Tower에서 AWS 리전 지원하는 모든 사용자로부터 AWS 알림 — 구독 확인 이메일을 수신합니다. 감사 계정에서 규정 준수 이메일을 받으려면 AWS Control Tower에서 AWS 리전 지원하는 각 이메일에서 구독 확인 링크를 선택해야 합니다.

회원 계정 정보

멤버 계정은 사용자가 AWS 워크로드를 수행하는 데 사용하는 계정입니다. 이러한 멤버 계정은 Account Factory에서 생성하거나, Service Catalog 콘솔에서 관리자 권한을 가진 IAM Identity Center 사용자가 생성하거나, 자동화된 방법을 통해 생성할 수 있습니다. 이러한 멤버 계정은 생성 시 AWS Control Tower 콘솔에서 생성되었거나 AWS Control Tower에 등록된 OU에 존재합니다. 자세한 내용은 다음 관련 주제를 참조하십시오.

- Account Factory를 통한 계정 제공 및 관리
- AWS Control Tower에서의 작업 자동화
- AWS AWS Organizations 사용자 안내서의 조직 용어 및 개념

테라폼용 AWS Control Tower 어카운트 팩토리 (AFT) 를 통해 계정 프로비저닝 단원도 참조하세요.

> **계정 및 제어**
>
> 회원 계정은 AWS Control Tower에 등록하거나 등록 취소할 수 있습니다. 컨트롤은 등록된 계정과 등록되지 않은 계정에 다르게 적용되며, 컨트롤은 상속에 따라 중첩된 OU의 계정에 적용될 수 있습니다.

AWS Control Tower가 할당하는 회원 계정 리소스에 대한 자세한 내용은 을 참조하십시오Account Factory에 대한 리소스 고려 사항.

기존 등록 AWS 계정

이미 AWS Control Tower에서 관리하는 조직 단위 (OU) 에 AWS 계정 등록하면 기존 개인까지 AWS Control Tower 거버넌스를 확장할 수 있습니다. 적격 계정은 AWS Control Tower OU와 동일한 AWS Organizations 조직에 속하는 미등록 OU에 있습니다.

> **Note**
>
> 초기 landing Zone 설정 중일 때를 제외하고는 기존 계정을 감사 또는 로그 아카이브 계정으로 등록할 수 없습니다.

먼저 신뢰할 수 있는 액세스를 설정하십시오.

기존 계정을 AWS Control AWS 계정 Tower에 등록하려면 먼저 AWS Control Tower가 계정을 관리하거나 관리할 수 있는 권한을 부여해야 합니다. 특히, AWS Control Tower에는 선택한 조직의 계정에 스택을 자동으로 AWS CloudFormation 배포할 수 있도록 사용자 간에 AWS CloudFormation 또는 사용자를 대신하여 신뢰할 수 있는 액세스를 설정할 수 있는 권한이 필요합니다. AWS Organizations 이 신뢰할 수 있는 액세스를 통해 `AWSControlTowerExecution` 역할은 각 계정을 관리하는 데 필요한 활동을 수행합니다. 따라서 등록하기 전에 각 계정에 이 역할을 추가해야 합니다.

신뢰할 AWS CloudFormation 수 있는 액세스를 활성화하면 한 번의 작업으로 여러 계정에서 스택을 생성, 업데이트 또는 삭제할 수 있습니다. AWS 리전 AWS Control Tower는 이러한 신뢰 기능을 사용하여 기존 계정을 등록된 조직 단위로 이전하기 전에 역할과 권한을 적용하여 거버넌스 하에 둘 수 있습니다.

신뢰할 수 있는 액세스에 대해 자세히 AWS CloudFormationStackSets 알아보려면 및 을 참조하십시오 AWS CloudFormationStackSets. AWS Organizations

계정 등록 중에는 어떻게 되나요?

등록 프로세스 중에 AWS Control Tower는 다음과 같은 작업을 수행합니다.

- 다음 스택 세트의 배포를 포함하여 계정에 베이스라인을 설정합니다.
  - `AWSControlTowerBP-BASELINE-CLOUDTRAIL`
  - `AWSControlTowerBP-BASELINE-CLOUDWATCH`
  - `AWSControlTowerBP-BASELINE-CONFIG`
  - `AWSControlTowerBP-BASELINE-ROLES`
  - `AWSControlTowerBP-BASELINE-SERVICE-ROLES`
  - `AWSControlTowerBP-BASELINE-SERVICE-LINKED-ROLES`
  - `AWSControlTowerBP-VPC-ACCOUNT-FACTORY-V1`

  이러한 스택 세트의 템플릿을 검토하고 기존 정책과 충돌하지 않도록 하는 것이 좋습니다.
- 또는 를 통해 계정을 식별합니다. AWS IAM Identity Center AWS Organizations
- 지정한 OU에 계정을 배치합니다. 보안 상태가 일관되게 유지되도록 현재 OU에 적용된 모든 SCP를 적용해야 합니다.
- 선택한 OU 전체에 적용되는 SCP를 통해 계정에 필수 제어를 적용합니다.
- 계정의 AWS Config 모든 리소스를 기록하도록 설정하고 설정합니다.
- 계정에 AWS Control Tower 탐지 제어를 적용하는 AWS Config 규칙을 추가합니다.

> **계정 및 조직 수준 CloudTrail 트레일**
>
> OU의 모든 구성원 계정은 등록 여부에 관계없이 OU의 AWS CloudTrail 트레일에 의해 관리됩니다.
>
> - 계정을 AWS Control Tower에 등록하면 새 조직의 AWS CloudTrail 트레일이 계정에 적용됩니다. 기존 CloudTrail 트레일을 배포한 경우, AWS Control Tower에 등록하기 전에 해당 계정의 기존 트레일을 삭제하지 않는 한 요금이 중복될 수 있습니다.
> - 예를 들어 콘솔을 통해 계정을 등록된 OU로 AWS Organizations 이전하고 AWS Control Tower에 계정을 등록하지 않는 경우, 계정에 남아 있는 계정 수준 트레일을 모두 제거해야 할 수 있습니다. 기존에 트레일을 배포한 경우 요금이 중복되어 발생합니다. CloudTrail CloudTrail

랜딩 존을 업데이트하고 조직 수준 트레일을 옵트아웃하거나 랜딩 존이 버전 3.0 이전인 경우, 조직 수준 CloudTrail 트레일은 계정에 적용되지 않습니다.

기존 계정을 VPC에 등록

AWS Control Tower는 Account Factory에서 새 계정을 프로비저닝할 때와 기존 계정을 등록할 때 VPC를 다르게 처리합니다.

- 새 계정을 생성하면 AWS Control Tower는 자동으로 AWS 기본 VPC를 제거하고 해당 계정에 대한 새 VPC를 생성합니다.
- 기존 계정을 등록할 때 AWS Control Tower는 해당 계정에 대한 새 VPC를 생성하지 않습니다.
- 기존 계정을 등록할 때 AWS Control Tower는 계정과 연결된 기존 VPC 또는 AWS 기본 VPC를 제거하지 않습니다.

Tip

Account Factory를 구성하여 새 계정의 기본 동작을 변경할 수 있습니다. 이렇게 하면 AWS Control Tower에 속한 조직의 계정에 대해 기본적으로 VPC가 설정되지 않습니다. 자세한 정보는 VPC 없이 AWS Control Tower에서 계정 생성을 참조하세요.

등록을 위한 사전 요구 사항

기존 계정을 AWS Control AWS 계정 Tower에 등록하려면 다음 사전 요구 사항이 필요합니다.

1. 기존 AWS 계정계정을 등록하려면 등록하려는 계정에 해당 `AWSControlTowerExecution` 역할이 있어야 합니다. 계정 등록을 검토하여 세부 정보 및 지침을 확인할 수 있습니다.
2. AWS 계정 등록하려는 기존 `AWSControlTowerExecution` 역할에는 역할 외에도 다음과 같은 권한과 신뢰 관계가 있어야 합니다. 그렇지 않으면 등록이 실패합니다.

   역할 권한: `AdministratorAccess` (AWS 관리형 정책)

   역할 신뢰 관계:

```
{
```

```
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::Management Account ID:root"
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

3. 계정에는 AWS Config 구성 레코더 또는 전송 채널이 없어야 합니다. 계정을 AWS CLI 등록하기 전에 를 통해 삭제하거나 수정할 수 있습니다. 그렇지 않으면 기존 리소스가 있는 등록 계정에서 기존 AWS Config 리소스를 수정하는 방법에 대한 지침을 검토하세요.
4. 등록하려는 계정은 AWS Control Tower 관리 계정과 동일한 AWS Organizations 조직에 있어야 합니다. 기존 계정은 AWS Control Tower에 이미 등록된 OU의 AWS Control Tower 관리 계정과 동일한 조직에만 등록할 수 있습니다.

등록을 위한 다른 사전 요구 사항을 확인하려면 AWS Control Tower 시작하기를 참조하십시오.

> **Note**
>
> 계정을 AWS Control Tower에 등록하면 해당 계정은 AWS Control Tower 조직의 AWS CloudTrail 트레일에 따라 관리됩니다. 기존 CloudTrail 트레일을 배포한 경우, AWS Control Tower에 등록하기 전에 해당 계정의 기존 트레일을 삭제하지 않는 한 요금이 중복될 수 있습니다.

기존 계정 등록

계정 등록 기능은 AWS Control Tower 콘솔에서 사용할 수 있으며, 기존 콘솔을 등록하여 AWS Control Tower의 적용을 AWS 계정 받도록 할 수 있습니다. 자세한 내용은 기존 등록 섹션을 참조하십시오. AWS 계정

등록 계정 기능은 랜딩 존이 드리프트 상태에 있지 않을 때 사용할 수 있습니다. 콘솔에서 이 기능을 보려면:

- AWS Control Tower의 조직 페이지로 이동합니다.

- 등록하려는 계정의 이름을 찾으십시오. 계정을 찾으려면 오른쪽 상단의 드롭다운 메뉴에서 계정만을 선택한 다음 필터링된 표에서 계정 이름을 찾으십시오.
- 섹션에 표시된 대로 개별 계정을 등록하는 단계를 따르십시오. 계정 등록 단계

> **Note**
>
> 기존 이메일 주소를 등록할 AWS 계정때는 기존 이메일 주소를 확인하십시오. 그렇지 않으면 새 계정이 생성될 수 있습니다.

특정 오류가 발생하면 페이지를 새로 고치고 다시 시도해야 할 수 있습니다. 랜딩 영역이 드리프트 상태인 경우 계정 등록 기능을 사용하지 못할 수 있습니다. 랜딩 존 드리프트가 해결될 때까지 Account Factory를 통해 새 계정을 프로비저닝해야 합니다.

AWS Control Tower 콘솔에서 계정을 등록할 때는 AWS Control Tower 콘솔을 사용하기 위한 관리자 액세스 권한과 함께 `AWSServiceCatalogEndUserFullAccess` 정책이 활성화된 사용자 계정으로 로그인해야 하며, 루트 사용자로 로그인할 수 없습니다.

등록한 계정은 다른 계정을 업데이트하는 것과 마찬가지로 AWS Control Tower 계정 팩토리를 통해 업데이트할 수 있습니다. AWS Service Catalog 업데이트 절차는 AWS Control Tower 또는 다음을 통해 계정 팩토리 계정을 업데이트하고 이전하십시오. AWS Service Catalog 단원에 나와 있습니다.

계정 등록 단계

기존 계정에 AdministratorAccess권한 (정책) 이 적용된 후 다음 단계에 따라 계정을 등록하십시오.

AWS Control Tower에 개인 계정을 등록하려면

- AWS Control Tower 조직 페이지로 이동합니다.
- 조직 페이지에서 등록할 자격이 있는 계정을 통해 섹션 상단의 작업 드롭다운 메뉴에서 등록을 선택할 수 있습니다. 또한 이러한 계정을 계정 세부 정보 페이지에서 볼 때 계정 등록 버튼이 표시됩니다.
- 계정 등록을 선택하면 계정 등록 페이지가 나타나고 계정에 `AWSControlTowerExecution` 역할을 추가하라는 메시지가 표시됩니다. 일부 지침은 을 참조하십시오. 필요한 IAM 역할을 기존 역할에 수동으로 AWS 계정 추가하고 등록하십시오.
- 그런 다음 드롭다운 목록에서 등록된 OU를 선택합니다. 계정이 이미 등록된 OU에 있는 경우 이 목록에 OU가 표시됩니다.
- 계정 등록을 선택합니다.
- `AWSControlTowerExecution`역할을 추가하고 작업을 확인하라는 양식 알림이 표시됩니다.

- [등록] 을 선택합니다.
- AWS Control Tower가 등록 프로세스를 시작하고 계정 세부 정보 페이지로 돌아가게 됩니다.

등록 실패의 일반적인 원인

- 기존 계정을 등록하려면 등록 중인 계정에 해당 `AWSControlTowerExecution` 역할이 있어야 합니다.
- IAM 보안 주체에는 계정을 프로비저닝하는 데 필요한 권한이 부족할 수 있습니다.
- AWS Security Token Service (AWS STS) 는 사용자 AWS 계정 거주 지역 또는 AWS Control Tower에서 지원하는 모든 지역에서 비활성화됩니다.
- 의 Account Factory 포트폴리오에 추가해야 하는 계정에 로그인되어 있을 수 AWS Service Catalog 있습니다. 계정을 추가해야 Account Factory에 액세스하여 AWS Control Tower에서 계정을 만들거나 등록할 수 있습니다. Account Factory 포트폴리오에 적절한 사용자 또는 역할을 추가하지 않은 경우 계정을 추가하려고 하면 오류 메시지가 표시됩니다. AWS Service Catalog 포트폴리오에 대한 액세스 권한을 부여하는 방법에 대한 지침은 사용자에게 액세스 권한 부여를 참조하십시오.
- 루트로 로그인되어 있을 수 있습니다.
- 등록하려는 계정의 AWS Config 설정이 남아 있을 수 있습니다. 특히 계정에는 구성 레코더 또는 전송 채널이 있을 수 있습니다. 계정을 등록하려면 AWS CLI 먼저 를 통해 삭제하거나 수정해야 합니다. 자세한 내용은 기존 AWS Config 리소스가 있는 계정 등록 및 사용과 상호 작용하기 AWS Control TowerAWS CloudShell 섹션을 참조하세요.
- 계정이 다른 AWS Control Tower OU를 포함하여 관리 계정을 가진 다른 OU에 속하는 경우, 다른 OU에 가입하려면 먼저 현재 OU에서 계정을 해지해야 합니다. 원래 OU에서 기존 리소스를 제거해야 합니다. 그렇지 않으면 등록이 실패합니다.
- 대상 OU의 SCP에서 해당 계정에 필요한 모든 리소스를 생성할 수 없는 경우 계정 공급 및 등록이 실패합니다. 예를 들어 대상 OU의 SCP가 특정 태그가 없으면 리소스 생성을 차단할 수 있습니다. 이 경우 AWS Control Tower가 리소스 태그 지정을 지원하지 않기 때문에 계정 프로비저닝 또는 등록이 실패합니다. 도움이 필요하면 계정 담당자에게 문의하거나. AWS Support

새 계정을 만들거나 기존 계정을 등록할 때 AWS Control Tower가 역할을 처리하는 방법에 대한 자세한 내용은 역할 및 계정을 참조하십시오.

> **Tip**
>
> 기존 계정이 등록 사전 요구 AWS 계정 사항을 충족하는지 확인할 수 없는 경우 등록 OU를 설정하고 해당 OU에 계정을 등록할 수 있습니다. 등록이 성공적으로 완료되면 계정을 원하는

OU로 이동할 수 있습니다. 등록이 실패할 경우 다른 계정이나 OU는 실패의 영향을 받지 않습니다.

기존 계정 및 해당 구성이 AWS Control Tower와 호환되는지 의심스러운 경우 다음 섹션에서 권장하는 모범 사례를 따를 수 있습니다.

권장 사항: 계정 등록에 대한 2단계 접근 방식을 설정할 수 있습니다.

- 먼저, 규정 AWS Config 준수 팩을 사용하여 일부 AWS Control Tower 제어 항목이 계정에 어떤 영향을 미칠 수 있는지 평가하십시오. AWS Control Tower 등록이 계정에 어떤 영향을 미칠 수 있는지 알아보려면 적합성 팩을 사용한 AWS AWS Config Control Tower 거버넌스 확장을 참조하십시오.
- 그런 다음 계정을 등록할 수 있습니다. 규정 준수 결과가 만족스럽다면 예기치 않은 결과 없이 계정을 등록할 수 있으므로 마이그레이션 과정이 더 원활해집니다.
- 평가를 완료한 후 AWS Control Tower 랜딩 존을 설정하기로 결정했다면 평가를 위해 생성된 AWS Config 전송 채널 및 구성 레코더를 제거해야 할 수 있습니다. 그러면 AWS Control Tower를 성공적으로 설정할 수 있습니다.

> **Note**
>
> 적합성 팩은 계정이 AWS Control Tower에서 등록한 OU에 위치하지만 워크로드는 AWS Control Tower가 지원하지 않는 AWS 지역 내에서 실행되는 상황에서도 사용할 수 있습니다. 적합성 팩을 사용하여 AWS Control Tower가 배포되지 않은 지역에 있는 계정의 리소스를 관리할 수 있습니다.

계정이 사전 요구 사항을 충족하지 않으면 어떻게 됩니까?

전제 조건으로 AWS Control Tower 거버넌스에 등록할 수 있는 계정이 동일한 전체 조직에 속해야 한다는 점을 기억하십시오. 계정 등록을 위한 이 사전 요구 사항을 충족하려면 다음 준비 단계에 따라 계정을 AWS Control Tower와 동일한 조직으로 이동할 수 있습니다.

계정을 AWS Control Tower와 동일한 조직에 통합하기 위한 준비 단계

1. 기존 조직에서 계정을 삭제하십시오. 이 방법을 사용할 경우 별도의 결제 방법을 제공해야 합니다.
2. 계정을 초대하여 AWS Control Tower 조직에 가입하십시오. 자세한 내용은 AWS Organizations 사용 설명서의 조직 가입을 위한 AWS 계정 초대를 참조하십시오.

3. 초대를 수락하십시오. 계정이 조직의 루트에 표시됩니다. 이 단계에서는 계정을 AWS Control Tower와 동일한 조직으로 이전하고 SCP와 통합 결제를 설정합니다.

> **Tip**
>
> 계정이 기존 조직에서 탈퇴하기 전에 새 조직에 대한 초대를 보낼 수 있습니다. 계정이 기존 조직에서 공식적으로 탈퇴할 때까지 초대는 대기하게 됩니다.

나머지 사전 요구 사항을 충족하기 위한 단계:

1. 필요한 `AWSControlTowerExecution` 역할을 생성합니다.
2. 기본 VPC를 지우십시오. (이 부분은 선택 사항입니다. AWS Control Tower는 기존 기본 VPC를 변경하지 않습니다.)
3. OR를 통해 기존 AWS Config 구성 레코더 또는 전송 채널을 AWS CLI 삭제하거나 AWS CloudShell수정하십시오. 자세한 내용은 리소스 상태에 대한 예제 AWS Config CLI 명령 및 기존 AWS Config 리소스가 있는 계정 등록 섹션을 참조하세요.

이러한 준비 단계를 완료한 후 계정을 AWS Control Tower에 등록할 수 있습니다. 자세한 정보는 계정 등록 단계을 참조하세요. 이 단계는 계정을 완전한 AWS Control Tower 거버넌스로 전환합니다.

계정을 등록하고 스택을 유지할 수 있도록 계정 프로비저닝을 해제하는 선택적 단계

1. 적용된 AWS CloudFormation 스택을 유지하려면 스택 세트에서 스택 인스턴스를 삭제하고 해당 인스턴스에 대해 Retain stacks를 선택합니다.
2. Account Factory에서 AWS Service Catalog 계정 프로비저닝된 제품을 종료합니다. (이 단계는 프로비저닝된 제품만 AWS Control Tower에서 제거합니다. 계정은 삭제되지 않습니다.
3. 조직에 속하지 않는 계정의 경우 필요에 따라 필요한 결제 세부 정보를 사용하여 계정을 설정합니다. 그런 다음 조직에서 계정을 제거합니다. (이렇게 하면 계정이 AWS Organizations 할당량 총액에 포함되지 않습니다.)
4. 리소스가 남아 있는 경우 계정을 정리한 다음, 의 계정 폐쇄 단계에 따라 계정을 폐쇄하세요계정 관리 취소.
5. 컨트롤이 정의되어 있는 일시 중단된 OU가 있는 경우 1단계를 수행하는 대신 계정을 해당 OU로 이동할 수 있습니다.

리소스 상태에 대한 예제 AWS Config CLI 명령

다음은 컨피그레이션 레코더 및 전송 채널의 상태를 확인하는 데 사용할 수 있는 몇 가지 예제 AWS Config CLI 명령입니다.

보기 명령:

- `aws configservice describe-delivery-channels`
- `aws configservice describe-delivery-channel-status`
- `aws configservice describe-configuration-recorders`

일반적인 응답은 다음과 같습니다. `"name": "default"`

삭제 명령:

- `aws configservice stop-configuration-recorder --configuration-recorder-name NAME-FROM-DESCRIBE-OUTPUT`
- `aws configservice delete-delivery-channel --delivery-channel-name NAME-FROM-DESCRIBE-OUTPUT`
- `aws configservice delete-configuration-recorder --configuration-recorder-name NAME-FROM-DESCRIBE-OUTPUT`

필요한 IAM 역할을 기존 역할에 수동으로 AWS 계정 추가하고 등록하십시오.

AWS Control Tower 랜딩 존을 이미 설정한 경우, AWS Control Tower에 등록된 OU에 조직의 계정을 등록하기 시작할 수 있습니다. 랜딩 존을 설정하지 않은 경우, AWS Control Tower 사용 설명서의 시작하기, 2단계에 설명된 단계를 따르십시오. 랜딩 존이 준비되면 다음 단계를 완료하여 수동으로 기존 계정을 AWS Control Tower에서 거버넌스로 전환하십시오.

이 장의 이전 부분에서 등록을 위한 사전 요구 사항 언급한 내용을 반드시 검토하십시오.

AWS Control Tower에 계정을 등록하기 전에 AWS Control Tower에 해당 계정을 관리할 권한을 부여해야 합니다. 이렇게 하려면 다음 단계에 나와 있는 것처럼 계정에 대한 전체 액세스 권한을 가진 역할을 추가해야 합니다. 등록한 각 계정에 대해 이러한 단계를 수행해야 합니다.

각 계정의 경우:

1단계: 등록하려는 계정이 현재 포함되어 있는 조직의 관리 계정에 관리자 액세스 권한을 사용하여 로그인합니다.

예를 들어 에서 AWS Organizations 이 계정을 만들고 교차 계정 IAM 역할을 사용하여 로그인하는 경우 다음 단계를 따를 수 있습니다.

1. 조직의 관리 계정에 로그인합니다.
2. AWS Organizations로 이동합니다.
3. 계정에서 등록하려는 계정을 선택하고 계정 ID를 복사합니다.
4. 상단 내비게이션 바에서 계정 드롭다운 메뉴를 열고 역할 전환을 선택합니다.
5. 역할 전환 양식에서 다음 필드를 채웁니다.
   - 계정에서 복사한 계정 ID를 입력합니다.
   - 역할에서 이 계정에 대한 교차 계정 액세스를 가능하게 하는 IAM 역할의 이름을 입력합니다. 이 역할의 이름은 계정 생성 시 정의되었습니다. 계정을 만들 때 역할 이름을 지정하지 않은 경우 기본 역할 이름인 을 입력합니다`OrganizationAccountAccessRole`.
6. 역할 전환을 선택합니다.
7. 이제 자녀 계정으로 로그인해야 합니다. AWS Management Console
8. 작업을 마쳤으면 다음 절차를 위해 자녀 계정을 계속 사용하세요.
9. 관리 계정 ID는 다음 단계에서 입력해야 하므로 기록해 두십시오.

2단계: AWS Control Tower에 계정 관리 권한을 부여합니다.

1. IAM으로 이동합니다.
2. 역할로 이동합니다.
3. 역할 생성을 선택합니다.
4. 역할 대상 서비스를 선택하라는 메시지가 표시되면 사용자 지정 신뢰 정책을 선택합니다.
5. 여기에 표시된 코드 예제를 복사하여 정책 문서에 붙여넣습니다. 문자열을 관리 계정의 실제 관리 계정 *`Management Account ID`*ID로 바꾸십시오. 붙여넣을 정책은 다음과 같습니다.

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
      "Effect":"Allow",
      "Principal":{
```

```
        "AWS": "arn:aws:iam::Management Account ID:root"
        },
        "Action": "sts:AssumeRole",
        "Condition": {}
    }
 ]
}
```

6. 정책을 첨부하라는 메시지가 표시되면 선택합니다 AdministratorAccess.
7. 다음: 태그를 선택합니다.
8. 태그 추가라는 제목의 선택적 화면이 표시될 수 있습니다. 다음:검토를 선택하여 지금은 이 화면을 건너뛰세요.
9. 검토 화면의 역할 이름 필드에 를 입력합니다. `AWSControlTowerExecution`
10. 설명 상자에 간단한 설명 (예: 등록을 위한 전체 계정 액세스 허용) 을 입력합니다.
11. 역할 생성을 선택합니다.

3단계: 계정을 등록된 OU로 이동하여 계정을 등록하고 등록을 확인합니다.

역할을 생성하여 필요한 권한을 설정한 후 다음 단계에 따라 계정을 등록하고 등록을 확인하십시오.

1. 관리자로 다시 로그인하고 AWS Control Tower로 이동하십시오.
2. 계정을 등록하십시오.
   - AWS Control Tower의 조직 페이지에서 계정을 선택한 다음 오른쪽 상단의 작업 드롭다운 메뉴에서 등록을 선택합니다.
   - 페이지에 표시된 대로 개별 계정을 등록하는 단계를 따르십시오. 계정 등록 단계
3. 등록을 확인하세요.
   - AWS Control Tower의 왼쪽 탐색 메뉴에서 조직을 선택합니다.
   - 최근에 등록한 계정을 찾아보십시오. 초기 상태에는 등록 상태가 표시됩니다.
   - 상태가 등록됨으로 변경되었을 때 이동이 성공한 것입니다.

이 프로세스를 계속하려면 AWS Control Tower에 등록하려는 조직의 각 계정으로 로그인하십시오. 각 계정의 사전 단계 및 등록 단계를 반복합니다.

계정 자동 등록 AWS Organizations

기존 AWS 계정을 AWS Control Tower에 등록이라는 블로그 게시물에 설명된 등록 방법을 사용하여 프로그래밍 프로세스를 통해 계정을 AWS Control Tower에 등록할 수 있습니다 AWS Organizations .

다음 YAML 템플릿은 프로그래밍 방식으로 등록할 수 있도록 계정에 필요한 역할을 생성하는 데 도움이 될 수 있습니다.

```
AWSTemplateFormatVersion: 2010-09-09
Description: Configure the AWSControlTowerExecution role to enable use of your
  account as a target account in AWS CloudFormation StackSets.
Parameters:
  AdministratorAccountId:
    Type: String
    Description: AWS Account Id of the administrator account (the account in which
      StackSets will be created).
    MaxLength: 12
    MinLength: 12
Resources:
  ExecutionRole:
    Type: AWS::IAM::Role
    Properties:
      RoleName: AWSControlTowerExecution
      AssumeRolePolicyDocument:
        Version: 2012-10-17
        Statement:
          - Effect: Allow
            Principal:
              AWS:
                - !Ref AdministratorAccountId
            Action:
              - sts:AssumeRole
      Path: /
      ManagedPolicyArns:
        - !Sub arn:${AWS::Partition}:iam::aws:policy/AdministratorAccess
```

기존 AWS Config 리소스가 있는 계정 등록

이 항목에서는 기존 AWS Config 리소스가 있는 계정을 등록하는 방법에 대한 step-by-step 접근 방법을 제공합니다. 기존 리소스를 확인하는 방법의 예는 을 참조하십시오리소스 상태에 대한 예제 AWS Config CLI 명령.

> **Note**
>
> 기존 AWS 계정을 감사 및 로그 보관 계정으로 AWS Control Tower에 가져오고 해당 계정에 기존 AWS Config 리소스가 있는 경우, 기존 AWS Config 리소스를 완전히 삭제해야 이러한 계정을 AWS Control Tower에 등록할 수 있습니다. 감사 및 로그 보관 계정이 아닌 계정의 경우 기존 Config 리소스를 수정할 수 있습니다.

리소스의 AWS Config 예

계정에 이미 있을 수 있는 몇 가지 유형의 AWS Config 리소스는 다음과 같습니다. 계정을 AWS Control Tower에 등록하려면 이러한 리소스를 수정해야 할 수 있습니다.

- AWS Config 레코더
- AWS Config 딜리버리 채널
- AWS Config 어그리게이션 권한 부여

가정

- AWS 컨트롤 타워 랜딩 존을 배포했습니다.
- 계정이 아직 AWS Control Tower에 등록되어 있지 않습니다.
- 계정에는 관리 계정이 관리하는 AWS Control Tower 지역 중 하나 이상에 있는 기존 AWS Config 리소스가 하나 이상 있습니다.
- 귀하의 계정은 AWS Control Tower 관리 계정이 아닙니다.
- 귀하의 계정은 거버넌스 드리프트에 속하지 않습니다.

기존 리소스로 계정을 등록하는 자동화된 접근 방식을 설명하는 블로그는 기존 AWS Config 리소스를 사용하여 AWS Control Tower에 계정을 자동으로 등록하는 것을 참조하십시오. AWS Config 에 설명된 대로 등록하려는 모든 계정에 대해 단일 지원 티켓을 제출할 수 있습니다. 1단계: 티켓을 가지고 고객 지원 팀에 문의하여 계정을 AWS Control Tower 허용 목록에 추가합니다.

제한 사항

- 계정은 거버넌스 확장을 위한 AWS Control Tower 워크플로를 사용해야만 등록할 수 있습니다.
- 리소스가 수정되어 계정에 드리프트가 발생하는 경우, AWS Control Tower는 리소스를 업데이트하지 않습니다.

- AWS Config AWS Control Tower의 적용을 받지 않는 지역의 리소스는 변경되지 않습니다.

> **Note**
>
> 허용 목록에 계정을 추가하지 않고 기존 Config 리소스가 있는 계정을 등록하려고 하면 등록이 실패합니다. 이후 동일한 계정을 허용 목록에 추가하려고 하면 AWS Control Tower는 계정이 올바르게 프로비저닝되었는지 검증할 수 없습니다. 허용 목록을 요청하고 등록하려면 먼저 AWS Control Tower에서 계정 프로비저닝을 해제해야 합니다. 계정을 다른 AWS Control Tower OU로만 이동하는 경우 거버넌스 드리프트가 발생하여 계정이 허용 목록에 추가되지 못하게 됩니다.

이 프로세스에는 5가지 주요 단계가 있습니다.

1. 계정을 AWS Control Tower 허용 목록에 추가합니다.
2. 계정에 새 IAM 역할을 생성합니다.
3. 기존 AWS Config 리소스를 수정합니다.
4. AWS Config 리소스가 존재하지 않는 AWS 지역에 리소스를 생성하세요.
5. AWS Control Tower에 계정을 등록하십시오.

진행하기 전에 이 프로세스에 대한 다음 기대치를 고려하십시오.

- AWS Control Tower는 이 계정에서 AWS Config 리소스를 생성하지 않습니다.
- 등록 후에는 AWS Control Tower 컨트롤이 새 IAM 역할을 포함하여 사용자가 생성한 AWS Config 리소스를 자동으로 보호합니다.
- 등록 후 AWS Config 리소스가 변경된 경우 계정을 재등록하려면 먼저 해당 리소스를 AWS Control Tower 설정에 맞게 업데이트해야 합니다.

1단계: 티켓을 가지고 고객 지원 팀에 문의하여 계정을 AWS Control Tower 허용 목록에 추가합니다.

티켓 제목에 다음 문구를 포함하세요.

기존 AWS Config 리소스가 있는 계정을 AWS Control Tower에 등록

티켓 본문에 다음 세부 정보를 포함하십시오.

- 관리 계좌 번호
- 기존 AWS Config 리소스가 있는 회원 계정의 계정 번호
- AWS Control Tower 설정을 위해 선택한 홈 지역

> **Note**
>
> 계정을 허용 목록에 추가하는 데 필요한 시간은 영업일 기준 2일입니다.

2단계: 멤버 계정에 새 IAM 역할 생성

1. 멤버 계정의 AWS CloudFormation 콘솔을 엽니다.
2. 다음 템플릿을 사용하여 새 스택을 생성합니다.

```
AWSTemplateFormatVersion: 2010-09-09
Description: Configure AWS Config

Resources:
  CustomerCreatedConfigRecorderRole:
    Type: AWS::IAM::Role
    Properties:
      RoleName: aws-controltower-ConfigRecorderRole-customer-created
      AssumeRolePolicyDocument:
        Version: 2012-10-17
        Statement:
          - Effect: Allow
            Principal:
              Service:
                - config.amazonaws.com
            Action:
              - sts:AssumeRole
      Path: /
      ManagedPolicyArns:
        - arn:aws:iam::aws:policy/service-role/AWS_ConfigRole
        - arn:aws:iam::aws:policy/ReadOnlyAccess
```

3. 스택 이름을 CustomerCreatedConfigRecorderRoleForControlTower로 입력합니다.
4. 스택을 생성합니다.

> **Note**
>
> 생성하는 모든 SCP는 `aws-controltower-ConfigRecorderRole*` 역할을 제외해야 합니다. AWS Config 규칙의 평가 수행 능력을 제한하는 권한을 수정하지 마십시오.
> Config 호출을 `aws-controltower-ConfigRecorderRole*` 차단하는 SCP가 `AccessDeniedException` 있을 때 알림을 받지 않도록 다음 지침을 따르세요.

3단계: 기존 리소스가 있는 AWS 지역 식별

계정의 각 관리 지역 (AWS Control Tower 관리) 에 대해 이전에 표시된 기존 AWS Config 리소스 예제 유형 중 하나 이상이 있는 지역을 식별하여 기록해 둡니다.

4단계: 리소스가 전혀 없는 AWS 지역을 식별하십시오. AWS Config

계정의 각 관리 지역 (AWS Control Tower 관리) 에 대해 이전에 표시된 예제 유형의 AWS Config 리소스가 없는 지역을 식별하여 기록해 둡니다.

5단계: 각 지역의 기존 리소스 수정 AWS

이 단계를 수행하려면 AWS Control Tower 설정에 대한 다음 정보가 필요합니다.

- `LOGGING_ACCOUNT`- 로깅 계정 ID
- `AUDIT_ACCOUNT`- 감사 계정 ID
- `IAM_ROLE_ARN`- 1단계에서 생성한 IAM 역할 ARN
- `ORGANIZATION_ID`- 관리 계정의 조직 ID
- `MEMBER_ACCOUNT_NUMBER`- 수정 중인 멤버 계정
- `HOME_REGION`- AWS Control Tower 설정을 위한 홈 지역.

다음 섹션 5a~5c에 나와 있는 지침에 따라 기존 리소스를 각각 수정하십시오.

5a단계. AWS Config 레코더 리소스

AWS 지역당 하나의 AWS Config 레코더만 존재할 수 있습니다. 존재하는 경우 다음과 같이 설정을 수정하십시오. 거주 지역의 항목을 `GLOBAL_RESOURCE_RECORDING` true로 바꾸십시오. AWS Config 레코더가 있는 다른 지역의 경우 항목을 false로 바꾸십시오.

- 이름: 변경하지 마세요
- RoLearn: `IAM_ROLE_ARN`
  - RecordingGroup:
  - AllSupported: 맞아요
  - IncludeGlobalResourceTypes: `GLOBAL_RESOURCE_RECORDING`
  - ResourceTypes: 비어 있음

이 수정은 다음 명령을 사용하여 AWS CLI를 통해 수행할 수 있습니다. 문자열을 `RECORDER_NAME` 기존 AWS Config 레코더 이름으로 바꿉니다.

```
aws configservice put-configuration-recorder --configuration-recorder
  name=RECORDER_NAME,roleARN=arn:aws:iam::MEMBER_ACCOUNT_NUMBER:role/
aws-controltower-ConfigRecorderRole-customer-created --recording-group
 allSupported=true,includeGlobalResourceTypes=GLOBAL_RESOURCE_RECORDING --
region CURRENT_REGION
```

5b단계. AWS Config 전송 채널 리소스 수정

지역당 하나의 AWS Config 전송 채널만 존재할 수 있습니다. 다른 것이 있는 경우 다음과 같이 설정을 수정하십시오.

- 이름: 변경하지 마세요
- ConfigSnapshotDeliveryProperties: TwentyFour _시간
- S3BucketName: AWS Control Tower 로깅 계정의 로깅 버킷 이름

  `aws-controltower-logs-LOGGING_ACCOUNT-HOME_REGION`
- S3KeyPrefix: *##_ID*
- SnsTopicARN: 감사 계정의 SNS 주제 ARN으로, 다음 형식입니다.

  `arn:aws:sns:CURRENT_REGION:AUDIT_ACCOUNT:aws-controltower-AllConfigNotifications`

이 수정은 다음 명령을 사용하여 AWS CLI를 통해 수행할 수 있습니다. 문자열을 *DELIVERY_CHANNEL_NAME* 기존 AWS Config 레코더 이름으로 바꿉니다.

```
aws configservice put-delivery-channel --delivery-channel
 name=DELIVERY_CHANNEL_NAME,s3BucketName=aws-controltower-
logs-LOGGING_ACCOUNT_ID-
HOME_REGION,s3KeyPrefix="ORGANIZATION_ID",configSnapshotDeliveryProperties={deliveryFrequency=T
controltower-AllConfigNotifications --region CURRENT_REGION
```

5c단계. AWS Config 집계 권한 부여 리소스 수정

지역별로 여러 집계 승인이 존재할 수 있습니다. AWS Control Tower에는 감사 계정을 승인된 계정으로 지정하고 AWS Control Tower의 홈 지역을 권한 있는 지역으로 지정하는 집계 권한이 필요합니다. 계정이 없는 경우 다음 설정을 사용하여 새 계정을 생성하십시오.

- AuthorizedAccountId: 감사 계정 ID
- AuthorizedAwsRegion: AWS Control Tower 설정을 위한 홈 지역

이 수정은 다음 명령을 사용하여 AWS CLI를 통해 수행할 수 있습니다.

```
aws configservice put-aggregation-authorization --authorized-account-
id AUDIT_ACCOUNT_ID --authorized-aws-region HOME_REGION --region
CURRENT_REGION
```

6단계: AWS Control Tower가 관리하는 지역에서 리소스가 존재하지 않는 곳에 리소스 생성

다음 예와 같이 홈 리전의 IncludeGlobalResourcesTypes파라미터에 값이 GLOBAL_RESOURCE_RECORDING 포함되도록 AWS CloudFormation 템플릿을 수정하십시오. 또한 이 섹션에 지정된 대로 템플릿의 필수 필드를 업데이트하십시오.

거주 지역의 항목을 GLOBAL_RESOURCE_RECORDING true로 바꾸십시오. AWS Config 레코더가 있는 다른 지역의 경우 항목을 false로 바꾸십시오.

1. 관리 계정의 AWS CloudFormation 콘솔로 이동합니다.
2. 이름을 StackSet 사용하여 새 계정을 만드십시오 CustomerCreatedConfigResourcesForControlTower.
3. 다음 템플릿을 복사하고 업데이트하십시오.

```
AWSTemplateFormatVersion: 2010-09-09
Description: Configure AWS Config
Resources:
  CustomerCreatedConfigRecorder:
    Type: AWS::Config::ConfigurationRecorder
    Properties:
      Name: aws-controltower-BaselineConfigRecorder-customer-created
      RoleARN: !Sub arn:aws:iam::${AWS::AccountId}:role/aws-controltower-
ConfigRecorderRole-customer-created
      RecordingGroup:
        AllSupported: true
        IncludeGlobalResourceTypes: GLOBAL_RESOURCE_RECORDING
        ResourceTypes: []
  CustomerCreatedConfigDeliveryChannel:
    Type: AWS::Config::DeliveryChannel
    Properties:
      Name: aws-controltower-BaselineConfigDeliveryChannel-customer-created
      ConfigSnapshotDeliveryProperties:
        DeliveryFrequency: TwentyFour_Hours
      S3BucketName: aws-controltower-logs-LOGGING_ACCOUNT-HOME_REGION
      S3KeyPrefix: ORGANIZATION_ID
      SnsTopicARN: !Sub arn:aws:sns:${AWS::Region}:AUDIT_ACCOUNT:aws-controltower-
AllConfigNotifications
  CustomerCreatedAggregationAuthorization:
    Type: "AWS::Config::AggregationAuthorization"
    Properties:
      AuthorizedAccountId: AUDIT_ACCOUNT
      AuthorizedAwsRegion: HOME_REGION
```

필수 필드로 템플릿을 업데이트하십시오.

a. S3 BucketName *#### ##_##_ID# #_### #####.*

b. S3 KeyPrefix 필드에서 *##_ID#* 교체합니다.

c. SnsTopicARN *#### AUDIT_ACCOUNT# #####.*

d. AuthorizedAccountId*#### AUDIT_ACCOUNT# ######.*

e. AuthorizedAwsRegion*#### HOME_REGION# ######.*

4. AWS CloudFormation 콘솔에 배포하는 동안 회원 계정 번호를 추가합니다.
5. 4단계에서 식별된 AWS 지역을 추가합니다.
6. 스택 세트를 배포합니다.

7단계: AWS 컨트롤 타워에 OU 등록

AWS Control Tower 대시보드에서 OU를 등록합니다.

> **Note**
>
> 계정 등록 워크플로는 이 작업에 성공하지 못합니다. OU 등록 또는 OU 재등록을 선택해야 합니다.

Account Factory를 통한 계정 제공 및 관리

이 장에는 Account Factory를 사용하여 AWS Control Tower 랜딩 존에서 새 회원 계정을 프로비저닝하기 위한 개요와 절차가 포함되어 있습니다.

계정 구성 및 프로비저닝을 위한 권한

AWS Control Tower Account Factory를 사용하면 클라우드 관리자와 사용자가 랜딩 존에서 계정을 AWS IAM Identity Center 프로비저닝할 수 있습니다. 기본적으로 계정을 프로비저닝하는 IAM Identity Center 사용자는 `AWSAccountFactory` 그룹 또는 관리 그룹에 속해야 합니다.

> **Note**
>
> 조직 전체에서 권한이 있는 계정을 사용할 때와 마찬가지로 관리 계정으로 작업할 때는 주의해야 합니다.

AWS Control Tower 관리 계정은 `AWSControlTowerExecution` 역할과 신뢰 관계를 맺고 있으므로 일부 자동 계정 설정을 포함하여 관리 계정에서 계정을 설정할 수 있습니다. `AWSControlTowerExecution`역할에 대한 자세한 내용은 역할 및 계정을 참조하십시오.

> **Note**
>
> 기존 계정을 AWS Control AWS 계정 Tower에 등록하려면 해당 계정에 `AWSControlTowerExecution` 역할이 활성화되어 있어야 합니다. 기존 계정을 등록하는 방법에 대한 자세한 내용은 기존 등록 AWS 계정 단원을 참조하십시오.

권한에 대한 자세한 내용은 계정에 필요한 권한을 참조하세요.

Account Factory를 통한 AWS Service Catalog 계정 프로비저닝

다음 절차는 IAM Identity Center에서 사용자로서 계정을 생성하고 프로비저닝하는 방법을 설명합니다. AWS Service Catalog이 절차를 고급 계정 프로비저닝 또는 수동 계정 프로비저닝이라고도 합니다. 선택적으로 AWS CLI 또는 AWS Control Tower Account Factory for Terraform (AFT) 을 사용하여 프로그래밍 방식으로 계정을 프로비저닝할 수 있습니다. 이전에 사용자 지정 블루프린트를 설정한 경우 콘솔에서 사용자 지정 계정을 프로비저닝할 수 있습니다. 커스터마이징에 대한 자세한 내용은 을 참조하십시오AFC (Account Factory Customize) 로 계정을 사용자 지정하세요.

사용자로서 Account Factory에서 계정을 개별적으로 프로비저닝하려면

1. 사용자 포털 URL에서 로그인합니다.
2. 애플리케이션에서 AWS 계정을 선택합니다.
3. 계정 목록에서 관리 계정의 계정 ID를 선택합니다. 이 ID에는 (관리) 와 같은 레이블도 있을 수 있습니다.
4. 에서 관리 AWSServiceCatalogEndUserAccess콘솔을 선택합니다. 그러면 이 계정에서 해당 사용자의 계정이 열립니다. AWS Management Console
5. 프로비저닝 계정을 올바르게 AWS 리전 선택했는지 확인하십시오. 이 계정은 AWS Control Tower 지역이어야 합니다.
6. Service Catalog를 검색하고 선택하여 서비스 카탈로그 콘솔을 엽니다.
7. 탐색 창에서 제품을 선택합니다.
8. AWS Control Tower Account Factory를 선택한 다음 제품 시작 버튼을 선택합니다. 선택하면 마법사가 시작되어 새 계정을 프로비저닝합니다.
9. 정보를 입력합니다. 이때 다음 사항에 유의하십시오.

    - SSO는 새 이메일 주소이거나 기존 IAM Identity Center 사용자와 연결된 이메일 주소일 UserEmail 수 있습니다. 어떤 주소를 선택하든 이 사용자는 프로비저닝 중인 계정에 대한 관리 액세스 권한을 갖습니다.
    - 아직 연결되지 않은 이메일 AccountEmail주소여야 합니다. AWS 계정UserEmailSSO에서 새 이메일 주소를 사용한 경우 여기에서 해당 이메일 주소를 사용할 수 있습니다.
10. 알림을 정의하거나 TagOptions활성화하지 마세요. 그렇지 않으면 계정이 프로비저닝되지 않을 수 있습니다. 작업을 마치면 제품 시작을 선택합니다.
11. 계정 설정을 검토한 다음 시작을 선택합니다. 리소스 계획을 만들지 마세요. 그렇지 않으면 계정이 프로비저닝되지 않습니다.

12. 계정이 프로비저닝 중입니다. 이 작업은 완료하는 데 몇 분 정도 걸릴 수 있습니다. 페이지를 새로 고쳐 표시된 상태 정보를 업데이트할 수 있습니다.

> **Note**
>
> 한 번에 최대 5개의 계정을 프로비전할 수 있습니다.

Account Factory에서 계정을 관리할 때 고려할 사항

Account Factory를 통해 생성하고 제공하는 계정을 업데이트, 관리 취소, 폐쇄할 수 있습니다. 용도를 변경하려는 계정의 사용자 매개변수를 업데이트하여 계정을 재활용할 수 있습니다. 계정의 OU (조직 구성 단위) 를 변경할 수도 있습니다.

> **Note**
>
> Account Factory가 판매하는 계정과 연결된 프로비저닝된 제품을 업데이트할 때 새 사용자 이메일 주소를 지정하면 AWS Control Tower가 IAM Identity Center에 새 사용자를 생성합니다. AWS IAM Identity Center이전에 만든 계정은 제거되지 않습니다. IAM ID 센터에서 이전 IAM Identity Center 사용자 이메일 주소를 제거하는 방법에 대한 자세한 내용은 사용자 비활성화를 참조하십시오.

AWS Control Tower 또는 다음을 통해 계정 팩토리 계정을 업데이트하고 이전하십시오. AWS Service Catalog

등록된 계정을 업데이트하는 가장 쉬운 방법은 AWS Control Tower 콘솔을 사용하는 것입니다. 개별 계정 업데이트는 다음과 같은 드리프트를 해결하는 데 유용합니다. 이동된 멤버 계정 전체 landing Zone 업데이트의 일환으로 계정 업데이트도 필요합니다.

한 OU (조직 구성 단위) 에서 다른 OU로 계정을 이동하는 경우 새 OU에서 적용하는 컨트롤이 이전 OU의 컨트롤과 다를 수 있다는 점을 기억하십시오. 새 OU의 컨트롤이 계정에 대한 정책 요구 사항을 충족하는지 확인하십시오.

계정 간 이동 시 동작 제어 OU

OU 간에 계정을 이동하면 대상 OU에 대한 제어가 다음 OU에 적용됩니다. 계정. 하지만 이전 OU의 계정에 적용된 컨트롤은 그렇지 않습니다. 제거되었습니다. 컨트롤의 정확한 동작은 구현에 따라 다릅니다. 이전 OU와 대상 OU에서 활성화된 컨트롤.

- AWS Config 규칙으로 구현된 컨트롤의 경우: 이전 OU의 컨트롤 제거되지 않습니다. 이러한 컨트롤은 수동으로 제거해야 합니다.
- SCP로 구현한 컨트롤의 경우: 이전 OU의 SCP 기반 컨트롤은 다음과 같습니다. 제거되었습니다. 대상 OU의 SCP 기반 컨트롤이 이 계정에 적용됩니다.
- AWS CloudFormation 후크로 구현된 컨트롤의 경우: 이 동작 새 OU의 컨트롤 상태에 따라 달라집니다.
  - 대상 OU에 후크 기반 컨트롤이 활성화되어 있지 않은 경우: 이전 이동된 계정의 컨트롤은 제거하지 않는 한 활성 상태로 유지됩니다. 수동으로.
  - 대상 OU에 후크 컨트롤이 활성화된 경우: 이전 컨트롤은 다음과 같습니다. 제거되고 대상 OU의 컨트롤이 해당 OU에 적용됩니다. 계정.

콘솔에서 계정 업데이트

AWS Control Tower 콘솔에서 계정을 업데이트하려면

1. AWS Control Tower에 로그인하면 조직 페이지로 이동합니다.
2. OU 및 계정 목록에서 업데이트하려는 계정의 이름을 선택합니다. 업데이트할 수 있는 계정의 상태는 업데이트 가능으로 표시됩니다.
3. 다음으로 선택한 계정의 계정 세부 정보 페이지가 표시됩니다.
4. 오른쪽 상단에서 계정 업데이트를 선택합니다.

프로비저닝된 제품 업데이트

다음 절차는 Service Catalog에서 계정의 프로비저닝된 제품을 업데이트하여 Account Factory에서 계정을 업데이트하거나 새 OU로 이동하는 방법을 안내합니다.

서비스 카탈로그를 통해 Account Factory 계정을 업데이트하거나 해당 OU를 변경하려면

1. AWS 관리 콘솔에 로그인하고 https://console.aws.amazon.com/servicecatalog/ 에서 AWS Service Catalog 콘솔을 엽니다.

   > **Note**
   >
   > Service Catalog에서 새 제품을 프로비전할 권한이 있는 사용자 (예: `AWSAccountFactory` 또는 `AWSServiceCatalogAdmins` 그룹의 IAM Identity Center 사용자) 로 로그인해야 합니다.

2. 탐색 창에서 프로비저닝을 선택한 다음 프로비저닝된 제품을 선택합니다.
3. 나열된 각 구성원 계정에 대해 다음 단계를 수행하여 모든 구성원 계정을 업데이트하십시오.

   a. 멤버 계정을 선택합니다. 해당 계정의 프로비저닝된 제품 세부 정보 페이지로 이동합니다.
   b. 프로비저닝된 제품 세부 정보 페이지에서 이벤트 탭을 선택합니다.
   c. 다음 파라미터를 기록해 둡니다.

      - SSO UserEmail (제공된 제품 세부 정보에서 사용 가능)
      - AccountEmail(제공된 제품 세부 정보에서 사용 가능)
      - SSO UserFirstName (IAM ID 센터에서 사용 가능)
      - SSOU SerLastName (IAM 아이덴티티 센터에서 사용 가능)
      - AccountName(IAM 자격 증명 센터에서 사용 가능)

   d. 작업에서 업데이트를 선택합니다.
   e. 업데이트하려는 제품의 버전 옆에 있는 버튼을 선택하고 다음을 선택합니다.
   f. 앞서 언급한 파라미터 값을 제공합니다.

      - 기존 OU를 유지하려면 계정이 이미 속해 있던 OU를 선택하십시오. ManagedOrganizationalUnit
      - 계정을 새 OU로 마이그레이션하려면 해당 계정의 ManagedOrganizationalUnit새 OU를 선택하십시오.

      중앙 클라우드 관리자는 AWS Control Tower 콘솔의 조직 페이지에서 이 정보를 찾을 수 있습니다.

   g. 다음을 선택합니다.
   h. 변경 사항을 검토한 다음 업데이트를 선택합니다. 이 프로세스는 계정당 몇 분 정도 걸릴 수 있습니다.

등록된 계정의 이메일 주소 변경

AWS Control Tower에 등록된 회원 계정의 이메일 주소를 변경하려면 이 섹션의 절차를 따르십시오.

> **Note**
>
> 다음 절차로는 관리 계정, 로그 아카이브 계정 또는 감사 계정의 이메일 주소를 변경할 수 없습니다. 자세한 내용은 내 AWS 계정에 연결된 이메일 주소를 변경하려면 어떻게 해야 하나요? 를 참조하십시오. 또는 AWS Support에 문의하십시오.

AWS Control Tower가 생성한 계정의 이메일 주소를 변경하려면

1. 계정의 루트 사용자 암호를 복구하십시오. 분실하거나 잊어버린 AWS 비밀번호는 어떻게 복구하나요? 문서의 단계를 따를 수 있습니다.
2. 루트 사용자 암호로 계정에 로그인합니다.
3. 다른 AWS 계정이메일 주소와 마찬가지로 이메일 주소를 변경하고 변경 내용이 반영될 때까지 기다리세요 AWS Organizations. 이메일 주소 변경 업데이트가 완료되는 동안 지연이 발생할 수 있습니다.
4. 이전에 계정에 속했던 이메일 주소를 사용하여 Service Catalog에서 프로비저닝된 제품을 업데이트합니다. 프로비저닝된 제품을 업데이트하는 프로세스에는 새 이메일 주소를 프로비저닝된 제품과 연결하는 작업이 포함됩니다. 이렇게 하면 이메일 주소 변경이 AWS Control Tower에 적용됩니다. 이후에 프로비저닝되는 제품을 업데이트하려면 새 이메일 주소를 사용하십시오.

만들 때 사용한 AWS Organizations멤버 계정의 비밀번호나 이메일 주소를 변경하려면 사용 설명서의 루트 사용자로 멤버 계정 액세스를 참조하십시오.AWS Organizations

등록된 계정의 이름 변경

이 섹션의 절차에 따라 등록된 AWS Control Tower 계정의 이름을 변경하십시오.

> **Note**
>
> AWS 관리자 계정의 이름을 변경하려면 관리자 권한이 있어야 하며 계정의 루트 사용자로 로그인해야 합니다.

AWS Control Tower에서 생성한 계정의 이름을 변경하려면

1. 계정의 루트 암호를 복구하십시오. 이 문서에 설명된 단계를 따를 수 있습니다. 분실하거나 잊어버린 AWS 비밀번호는 어떻게 복구하나요?

2. 루트 비밀번호로 계정에 로그인합니다.
3. AWS Billing 콘솔에서 계정 설정 페이지로 이동합니다.
4. 다른 계정과 마찬가지로 계정 설정에서 이름을 변경합니다 AWS 계정.
5. AWS Control Tower는 이름 변경을 반영하여 자동으로 업데이트합니다. 이 업데이트는 프로비저닝된 제품에 반영되지 않습니다. AWS Service Catalog

Amazon Virtual Private Cloud 설정을 사용하여 어카운트 팩토리를 구성합니다.

Account Factory를 사용하면 조직 내 계정에 대해 사전 승인된 기준 및 구성 옵션을 만들 수 있습니다. AWS Service Catalog를 통해 새 계정을 구성 및 프로비저닝할 수 있습니다.

Account Factory 페이지에서 조직 단위 (OU) 목록과 해당 허용 목록 상태를 볼 수 있습니다. 기본적으로 모든 OU는 허용 목록에 있으므로 계정이 해당 계정 아래 프로비저닝될 수 있습니다. 를 통해 AWS Service Catalog계정 프로비저닝이 가능하도록 특정 OU를 비활성화할 수 있습니다.

최종 사용자가 새 계정을 프로비저닝할 때 사용할 수 있는 Amazon VPC 구성 옵션을 볼 수 있습니다.

Account Factory에서 아마존 VPC 설정을 구성하려면

1. 중앙 클라우드 관리자로서 관리 계정의 관리자 권한을 사용하여 AWS Control Tower 콘솔에 로그인합니다.
2. 대시보드 왼쪽에서 Account Factory를 선택하여 Account Factory 네트워크 구성 페이지로 이동합니다. 여기에 기본 네트워크 설정이 표시됩니다. 편집하려면 편집을 선택하고 Account Factory 네트워크 구성 설정의 편집 가능한 버전을 확인하십시오.
3. 필요에 따라 기본 설정의 각 필드를 수정할 수 있습니다. 최종 사용자가 생성할 수 있는 모든 새 Account Factory 계정에 대해 설정하려는 VPC 구성 옵션을 선택하고 필드에 설정을 입력합니다.

- Amazon VPC에서 퍼블릭 서브넷을 생성하려면 비활성화 또는 활성화를 선택합니다. 기본적으로 인터넷 액세스가 가능한 서브넷은 허용되지 않습니다.

> **Note**
>
> 새 계정을 프로비저닝할 때 퍼블릭 서브넷이 활성화되도록 Account Factory VPC 구성을 설정하면 Account Factory에서 NAT 게이트웨이를 생성하도록 Amazon VPC가 구성됩니다. 따

라서 Amazon VPC에서 사용량에 대한 요금이 청구됩니다. 자세한 내용은 VPC 요금을 참조하십시오.

- 목록에서 Amazon VPC의 최대 프라이빗 서브넷 수를 선택합니다. 기본적으로 1이 선택됩니다. 허용되는 최대 프라이빗 서브넷 수는 가용 영역당 2개입니다.
- 계정 VPC를 생성하기 위한 IP 주소 범위를 입력합니다. 이 값은 CIDR(Classless Inter-Domain Routing) 블록 형식이어야 합니다(기본값 `172.31.0.0/16`). 이 CIDR 블록은 Account Factory가 계정에 대해 생성하는 VPC의 전체 서브넷 IP 주소 범위를 제공합니다. VPC 내에서 서브넷은 지정한 범위에서 자동으로 할당되고 크기는 동일합니다. 기본적으로 VPC 내의 서브넷은 중첩되지 않습니다. 그러나 프로비저닝한 모든 계정의 VPC에서 서브넷 IP 주소 범위는 중첩될 수 있습니다.
- 계정이 프로비저닝될 때 VPC를 생성하기 위해 한 리전 또는 모든 리전을 선택합니다. 사용 가능한 모든 리전이 기본적으로 선택되어 있습니다.
- 목록에서 각 VPC의 서브넷을 구성할 가용 영역 수를 선택합니다. 기본값으로 권장되는 수는 3개입니다.
- 저장을 선택합니다.

또한 이러한 구성 옵션을 설정하여 VPC가 포함되지 않은 새 계정을 만들 수도 있습니다. 시연을 참조하십시오.

계정 관리 취소

Account Factory에서 계정을 생성했거나 계정을 AWS 계정등록했는데 더 이상 랜딩 존에서 AWS Control Tower가 계정을 관리하는 것을 원하지 않는 경우, AWS Control Tower 콘솔에서 계정 관리를 취소할 수 있습니다.

AWS Control Tower 계정을 관리 취소하면 청사진을 포함하여 AWS Control Tower에서 프로비저닝한 모든 리소스가 제거됩니다. 계정은 모든 AWS Control Tower OU에서 루트 영역으로 이동됩니다. 계정은 더 이상 등록된 OU의 일부가 아니며 더 이상 AWS Control Tower SCP의 적용을 받지 않습니다. 를 통해 AWS Organizations계정을 폐쇄할 수 있습니다.

`AWSAccountFactory`그룹의 IAM Identity Center 사용자가 프로비저닝된 제품을 종료하여 Service Catalog 콘솔에서 계정 관리를 취소할 수도 있습니다. IAM Identity Center 사용자 또는 그룹에 대한 자세한 내용은 사용자 및 액세스 관리를 참조하십시오. AWS IAM Identity Center 다음 절차는 Service Catalog에서 구성원 계정을 관리 취소하는 방법을 설명합니다.

등록된 계정을 관리 취소하려면

1. 웹 브라우저에서 Service Catalog 콘솔을 엽니다https://console.aws.amazon.com/servicecatalog.

2. 왼쪽 탐색 창에서 프로비저닝된 제품 목록을 선택합니다.
3. 프로비저닝된 계정 목록에서 AWS Control Tower가 더 이상 관리하지 않도록 하려는 계정의 이름을 선택합니다.
4. Provisioned product details(프로비저닝된 제품 세부 정보) 페이지의 작업 메뉴에서 종료를 선택합니다.
5. 나타나는 대화 상자에서 종료를 선택합니다.

> **Important**
>
> 종료라는 단어는 Service Catalog에만 해당됩니다. Service Catalog Account Factory에서 계정을 종료해도 계정은 폐쇄되지 않습니다. 이 작업을 수행하면 해당 OU와 landzone에서 계정이 제거됩니다.

6. 계정이 관리되지 않으면 상태가 [등록 안 됨] 으로 변경됩니다.
7. 계정이 더 이상 필요하지 않으면 계정을 폐쇄하세요. AWS 계정 폐쇄에 대한 자세한 내용은 AWS Billing 사용 설명서의 계정 해지를 참조하십시오.

사용자 지정 계정을 관리 취소하면 AWS Control Tower는 청사진이 배포한 리소스는 물론 AWS Control Tower가 계정 내에 생성한 기타 모든 리소스를 제거합니다. 계정 관리를 취소한 후에는 계정을 폐쇄할 수 있습니다. AWS Organizations

> **Note**
>
> 관리되지 않는 계정은 폐쇄되거나 삭제되지 않습니다. 계정을 관리하지 않아도 Account Factory에서 계정을 생성할 때 선택한 IAM Identity Center 사용자는 여전히 계정에 대한 관리자 액세스 권한을 가집니다. 이 사용자에게 관리 액세스 권한을 부여하지 않으려면 Account Factory에서 계정을 업데이트하고 계정에 대한 IAM Identity Center 사용자 이메일 주소를 변경하여 IAM Identity Center에서 이 설정을 변경해야 합니다. 자세한 정보는 AWS Control Tower 또는 다음을 통해 계정 팩토리 계정을 업데이트하고 이전하십시오. AWS Service Catalog을 참조하세요.

비디오 안내

이 동영상 (3:25) 은 AWS Control Tower에서 계정을 제거하고, 계정에 대한 루트 액세스 권한을 얻고, 마지막으로 계정을 폐쇄하는 방법을 설명합니다. AWS 계정AWS Organizations API를 사용하여 계정

을 폐쇄할 수도 있습니다. 동영상 오른쪽 하단에 있는 아이콘을 선택하여 전체 화면으로 확대하면 더 잘 보입니다. 자막을 사용할 수 있습니다.

AWS Control Tower의 계정 폐쇄에 대한 동영상 안내.

AWS Control Tower의 일반적인 작업을 설명하는 AWS YouTube 동영상 목록을 볼 수 있습니다.

Account Factory에서 생성한 계정 폐쇄

Account Factory에서 생성한 계정은 다음과 같습니다 AWS 계정. AWS 계정폐쇄에 대한 자세한 내용은 계정 관리 참조 가이드의AWS 계정 해지를 참조하십시오.

> **Note**
>
> AWS 계정 폐쇄는 AWS Control Tower에서 계정 관리를 취소하는 것과 다릅니다. 이는 별도의 조치입니다. 계정을 폐쇄하기 전에 계정 관리를 취소해야 합니다.

다음을 통해 AWS Control Tower 회원 계정을 폐쇄하십시오. AWS Organizations

루트 자격 증명으로 각 회원 계정에 개별적으로 로그인할 필요 없이 조직의 관리 계정에서 AWS Control Tower 회원 계정을 폐쇄할 수 AWS Organizations있습니다. 하지만 이런 방법으로는 관리 계정을 폐쇄할 수 없습니다.

AWS Organizations CloseAccountAPI를 호출하거나 AWS Organizations 콘솔에서 계정을 폐쇄하면 다른 경우와 마찬가지로 AWS 계정 멤버 계정이 90일 동안 격리됩니다. 계정에는 AWS Control Tower 및 에서 일시 중단된 상태가 표시됩니다 AWS Organizations. 90일 동안 해당 계정을 사용하려고 하면 AWS Control Tower에서 오류 메시지를 표시합니다.

다른 계정과 마찬가지로 90일이 만료되기 전에 회원 계정을 복원할 수 있습니다. AWS 계정 90일이 지나면 계정 기록이 제거됩니다.

가장 좋은 방법은 계정을 폐쇄하기 전에 회원 계정을 관리 해제하는 것입니다. 먼저 관리를 취소하지 않고 회원 계정을 폐쇄하는 경우, AWS Control Tower는 계정 상태가 일시 중단됨으로 표시되지만 등록됨으로도 표시됩니다. 따라서 90일 기간 동안 계정의 OU를 다시 등록하려고 하면 AWS Control Tower에서 오류 메시지가 표시됩니다. 일시 중단된 계정은 사전 확인 실패로 인한 재등록 작업을 근본적으로 차단합니다. OU에서 계정을 제거하면 OU를 다시 등록할 수 있지만 계정에 대한 결제 방법이 누락되어 오류가 AWS 발생할 수 있습니다. 이 제약 조건을 해결하려면 다시 등록하기 전에 다른 OU를 만들고 해당 OU로 계정을 이동하십시오. 이 OU의 이름을 일시 중단된 OU로 지정하는 것이 좋습니다.

> **Note**
>
> 계정을 폐쇄하기 전에 계정 관리를 취소하지 않는 경우 90일이 지난 AWS Service Catalog 후에 계정의 프로비저닝된 제품을 삭제해야 합니다.

자세한 내용은 API 관련 AWS Organizations 설명서를 참조하십시오. CloseAccount

Account Factory에 대한 리소스 고려 사항

Account Factory로 계정을 프로비전하면 계정 내에 다음과 같은 AWS 리소스가 생성됩니다.

AWS 서비스	리소스 유형	리소스 이름
AWS CloudFormation	스택	StackSet-AWSControlTowerBP-BASELINE-CLOUDTRAIL-* StackSet-AWSControlTowerBP-BASELINE-CLOUDWATCH-* StackSet-AWSControlTowerBP-BASELINE-CONFIG-* StackSet-AWSControlTowerBP-BASELINE-ROLES-* StackSet-AWSControlTowerBP-BASELINE-SERVICE-ROLES-*
AWS CloudTrail	추적	aws-controltower-BaselineCloudTrail
아마존 CloudWatch	CloudWatch 이벤트 규칙	aws-controltower-ConfigComplianceChangeEventRule

AWS 서비스	리소스 유형	리소스 이름
아마존 CloudWatch	CloudWatch 로그	aws-controltower/CloudTrail Logs /aws/lambda/aws-controltower-NotificationForwarder
AWS Identity and Access Management	역할	aws-controltower-AdministratorExecutionRole aws-controltower-CloudWatchLogsRole aws-controltower-ConfigRecorderRole aws-controltower-ForwardSnsNotificationRole aws-controltower-ReadOnlyExecutionRole AWSControlTowerExecution
AWS Identity and Access Management	정책	AWSControlTowerServiceRolePolicy
Amazon Simple Notification Service	주제	aws-controltower-SecurityNotifications
AWS Lambda	애플리케이션	StackSet-AWSControlTowerBP-BASELINE-CLOUDWATCH-*
AWS Lambda	함수	aws-controltower-NotificationForwarder

AFC (Account Factory Customize) 로 계정을 사용자 지정하세요

AWS Control Tower를 사용하면 AWS Control Tower 콘솔에서 리소스를 AWS 계정 프로비저닝할 때 신규 및 기존 리소스를 사용자 지정할 수 있습니다. 계정 팩토리 사용자 지정을 설정하면 AWS Control Tower가 향후 프로비저닝을 위해 이 프로세스를 자동화하므로 파이프라인을 유지 관리할 필요가 없습니다. 사용자 지정 계정은 리소스가 프로비저닝된 후 즉시 사용할 수 있습니다.

사용자 지정 계정은 계정 팩토리, AWS CloudFormation 템플릿 또는 Terraform을 통해 프로비저닝됩니다. 사용자 지정 계정 청사진 역할을 하는 템플릿을 정의합니다. 블루프린트는 계정을 프로비저닝할 때 필요한 특정 리소스와 구성을 설명합니다. AWS 파트너가 구축하고 관리하는 사전 정의된 블루프린트도 사용할 수 있습니다. 파트너 관리 블루프린트에 대한 자세한 내용은 시작 라이브러리를 참조하십시오.AWS Service Catalog

> **Note**
>
> AWS Control Tower에는 AWS Control Tower의 AWS CloudFormation 리소스를 모니터링하는 사전 예방적 제어 기능이 포함되어 있습니다. 선택적으로, 착륙 지대에서 이러한 컨트롤을 활성화할 수 있습니다. 사전 예방 제어를 적용하면 계정에 배포하려는 리소스가 조직의 정책 및 절차를 준수하는지 확인합니다. 사전 예방적 제어에 대한 자세한 내용은 사전 제어를 참조하십시오.

계정 청사진은 에 저장되며 AWS 계정, 당사에서는 이를 허브 계정이라고 합니다. 블루프린트는 Service Catalog 제품 형태로 저장됩니다. 이 제품을 다른 Service Catalog 제품과 구별하기 위해 블루프린트라고 합니다. Service Catalog 제품을 만드는 방법에 대한 자세한 내용은 AWS Service Catalog 관리자 안내서에서 제품 생성을 참조하십시오.

기존 계정에 청사진 적용

또한 AWS Control Tower 콘솔의 계정 업데이트 단계에 따라 기존 계정에 사용자 지정 블루프린트를 적용할 수 있습니다. 자세한 내용은 콘솔에서 계정 업데이트단원을 참조하세요.

> **시작하기 전 준비 사항**
>
> AWS Control Tower Account Factory에서 사용자 지정 계정을 생성하려면 먼저 AWS Control Tower 랜딩 존 환경을 배포하고, 새로 생성한 계정을 배치할 AWS Control Tower에 등록된 조직 단위 (OU) 가 있어야 합니다.

AFC 사용에 대한 자세한 내용은 AWS Control Tower의 Account Factory 사용자 지정을 사용한 계정 사용자 지정 자동화를 참조하십시오.

사용자 지정을 위한 준비

- 허브 계정으로 사용할 새 계정을 만들거나 기존 계정을 사용할 수 있습니다 AWS 계정. AWS Control Tower 관리 계정을 블루프린트 허브 계정으로 사용하지 않는 것이 좋습니다.
- AWS Control AWS 계정 Tower에 등록하고 사용자 지정하려는 경우, AWS Control Tower에 등록하려는 다른 계정과 마찬가지로 먼저 해당 계정에 `AWSControlTowerExecution` 역할을 추가해야 합니다.
- 마켓플레이스 구독 요구 사항이 있는 파트너 블루프린트를 사용하려는 경우, 파트너 블루프린트를 어카운트 팩토리 사용자 지정 블루프린트로 배포하기 전에 AWS Control Tower Management 계정에서 이를 구성해야 합니다.

주제

사용자 지정을 위한 설정

다음 섹션에서는 사용자 지정 프로세스를 위해 Account Factory를 설정하는 단계를 설명합니다. 이 단계를 시작하기 전에 허브 계정의 위임 관리자를 설정하는 것이 좋습니다.

요약

- 단계 1. 필요한 역할을 생성합니다. AWS Control Tower가 (허브) 계정에 액세스할 수 있는 권한을 부여하는 IAM 역할을 생성합니다. 이 계정에는 Blueprint라고도 하는 Service Catalog 제품이 저장되어 있습니다.
- 단계 2. 제품 생성. AWS Service Catalog 사용자 지정 계정의 기준을 설정하는 데 필요한 AWS Service Catalog 제품 (“청사진 제품”이라고도 함) 을 만드세요.
- 단계 3. 사용자 지정 청사진을 검토하세요. 만든 AWS Service Catalog 제품 (청사진) 을 살펴보세요.
- 단계 4. 블루프린트를 호출하여 사용자 지정 계정을 만드세요. 계정을 생성하는 동안 AWS Control Tower 콘솔의 Account Factory의 해당 필드에 청사진 제품 정보와 역할 정보를 입력합니다.

단계 1. 필요한 역할을 생성하십시오.

계정을 사용자 지정하기 전에 AWS Control Tower와 허브 계정 간의 신뢰 관계를 포함하는 역할을 설정해야 합니다. 역할을 맡으면 AWS Control Tower에 허브 계정을 관리할 수 있는 액세스 권한을 부여합니다. 역할에는 이름을 지정해야 합니다. AWSControlTowerBlueprintAccess

AWS Control Tower는 이 역할을 맡아 사용자를 대신하여 포트폴리오 리소스를 만든 다음 청사진을 이 포트폴리오에 Service Catalog 제품으로 추가한 다음 계정 프로비저닝 중에 이 포트폴리오와 청사진을 회원 계정과 공유합니다. AWS Service Catalog

다음 섹션에 설명된 대로 `AWSControlTowerBlueprintAccess` 역할을 생성하게 됩니다.

> IAM 콘솔로 이동하여 필요한 역할을 설정합니다.

등록된 AWS Control Tower 계정에서 역할을 설정하려면

1. AWS Control Tower 관리 계정에서 보안 주체로 페더레이션하거나 로그인하십시오.
2. 관리 계정의 페더레이션된 보안 주체에서 `AWSControlTowerExecution` 역할을 맡거나 블루프린트 허브 계정으로 사용하도록 선택한 등록된 AWS Control Tower 계정의 역할로 역할을 전환합니다.
3. 등록된 AWS Control Tower 계정의 `AWSControlTowerBlueprintAccess` 역할에서 적절한 권한 및 신뢰 관계를 가진 역할을 생성합니다. `AWSControlTowerExecution`

> **Note**
>
> AWS 모범 사례 지침을 준수하려면 역할을 생성한 후 즉시 해당 `AWSControlTowerExecution` 역할에서 로그아웃하는 것이 중요합니다. `AWSControlTowerBlueprintAccess` 의도하지 않은 리소스 변경을 방지하기 위해 이 `AWSControlTowerExecution` 역할은 AWS Control Tower에서만 사용할 수 있습니다.

블루프린트 허브 계정이 AWS Control Tower에 등록되지 않은 경우, `AWSControlTowerExecution` 역할은 계정에 존재하지 않으므로 역할 설정을 계속하기 전에 역할을 맡을 필요가 없습니다. `AWSControlTowerBlueprintAccess`

등록되지 않은 멤버 계정에서 역할을 설정하려면

1. 허브 계정으로 지정하려는 계정을 원하는 방법으로 페더레이션하거나 계정 주체로 로그인합니다.
2. 계정의 보안 주체로 로그인한 경우 적절한 권한과 신뢰 관계를 사용하여 `AWSControlTowerBlueprintAccess` 역할을 생성하십시오.

두 명의 주체에게 신뢰를 부여하려면 AWSControlTowerBlueprintAccess역할을 설정해야 합니다.

- AWS 컨트롤 타워 관리 계정에서 AWS 컨트롤 타워를 운영하는 주체 (사용자).
- AWS Control Tower 관리 계정에 지정된 `AWSControlTowerAdmin` 역할.

다음은 역할에 포함해야 하는 것과 유사한 신뢰 정책의 예시입니다. 이 정책은 최소 권한 액세스 권한을 부여하는 모범 사례를 보여줍니다. 자체 정책을 만들 때는 *`YourManagementAccountId`*용어를 AWS Control Tower 관리 계정의 실제 계정 *`YourControlTowerUserRole`*ID로 바꾸고, 이 용어는 관리 계정의 IAM 역할 식별자로 바꾸십시오.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "AWS": [
                "arn:aws:iam::YourManagementAccountId:role/service-role/
AWSControlTowerAdmin",
```

```
                "arn:aws:iam::YourManagementAccountId:role/YourControlTowerUserRole"
                ]
            },
            "Action": "sts:AssumeRole"
        }
    ]
}
```

필수 권한 정책

AWS Control Tower에서는 이름이 지정된 관리형 정책을 `AWSControlTowerBlueprintAccess` 역할에 `AWSServiceCatalogAdminFullAccess` 연결해야 합니다. 이 정책은 AWS Control Tower가 AWS Service Catalog 언제 포트폴리오와 AWS Service Catalog 제품 리소스를 관리할 수 있는지 확인하는 권한을 제공합니다. IAM 콘솔에서 역할을 생성할 때 이 정책을 추가할 수 있습니다.

추가 권한이 필요할 수 있습니다.

- 청사진을 Amazon S3에 저장하는 경우, AWS Control Tower에도 `AWSControlTowerBlueprintAccess` 역할에 대한 `AmazonS3ReadOnlyAccess` 권한 정책이 필요합니다.
- AWS Service Catalog Terraform 유형의 제품에서는 기본 관리 정책을 사용하지 않는 경우 AFC 사용자 지정 IAM 정책에 몇 가지 추가 권한을 추가해야 합니다. Terraform 템플릿에서 정의한 리소스를 생성하는 데 필요한 권한 외에도 이러한 권한이 필요합니다.

단계 2. 제품 생성 AWS Service Catalog

AWS Service Catalog 제품을 만들려면 AWS Service Catalog 관리자 안내서의 제품 만들기의 단계를 따르십시오. AWS Service Catalog 제품을 생성할 때 계정 블루프린트를 템플릿으로 추가해야 합니다.

Important

HashiCorp의 업데이트된 Terraform 라이선스에 따라 Terraform 오픈 소스 제품 및 프로비저닝된 제품에 대한 지원이 External이라는 새로운 제품 유형으로 AWS Service Catalog 변경되었습니다. 기존 계정 청사진을 외부 제품 유형으로 업데이트하는 방법을 포함하여 이번 변경이 AFC에 미치는 영향에 대해 자세히 알아보려면 외부 제품 유형으로의 전환을 검토하세요.

청사진을 만드는 단계 요약

- 계정 청사진이 될 AWS CloudFormation 템플릿 또는 Terraform tar.gz 구성 파일을 만들거나 다운로드하세요. 일부 템플릿 예제는 이 섹션 뒷부분에 나와 있습니다.
- Account Factory 블루프린트를 저장하는 AWS 계정 곳 (허브 계정이라고도 함) 에 로그인합니다.
- AWS Service Catalog 콘솔로 이동합니다. 제품 목록을 선택한 다음 새 제품 업로드를 선택합니다.
- 제품 세부 정보 창에 이름, 설명 등 청사진 제품에 대한 세부 정보를 입력합니다.
- 템플릿 파일 사용을 선택한 다음 파일 선택을 선택합니다. 블루프린트로 사용하기 위해 개발하거나 다운로드한 템플릿 또는 구성 파일을 선택하거나 붙여넣습니다.
- 콘솔 페이지 하단에서 제품 생성을 선택합니다.

AWS Service Catalog 참조 아키텍처 리포지토리에서 AWS CloudFormation 템플릿을 다운로드할 수 있습니다. 해당 리포지토리의 한 가지 예는 리소스에 대한 백업 계획을 설정하는 데 도움이 됩니다.

다음은 Best Pets라는 가상의 회사를 위한 예제 템플릿입니다. 이는 애완 동물 데이터베이스와의 연결을 설정하는 데 도움이 됩니다.

```
Resources:
  ConnectionStringGeneratorLambdaRole:
    Type: AWS::IAM::Role
    Properties:
      AssumeRolePolicyDocument:
        Version: "2012-10-17"
        Statement:
          - Effect: Allow
            Principal:
              Service:
                - lambda.amazonaws.com
            Action:
              - "sts:AssumeRole"
  ConnectionStringGeneratorLambda:
    Type: AWS::Lambda::Function
    Properties:
      FunctionName: !Join ['-', ['ConnectionStringGenerator', !Select [4, !Split
 ['-', !Select [2, !Split ['/', !Ref AWS::StackId]]]]]]
      Description: Retrieves the connection string for this account to access the Pet
 Database
      Role: !GetAtt ConnectionStringGeneratorLambdaRole.Arn
      Runtime: nodejs16.x
      Handler: index.handler
```

```
      Timeout: 5
      Code:
        ZipFile: >
          const response = require("cfn-response");
          exports.handler = function (event, context) {
            const awsAccountId = context.invokedFunctionArn.split(":")[4]
            const connectionString= "fake connection string that's specific to account
" + awsAccountId;
            const responseData = {
              Value: connectionString,
            }
            response.send(event, context, response.SUCCESS, responseData);
            return connectionString;
          };

  ConnectionString:
    Type: Custom::ConnectionStringGenerator
    Properties:
      ServiceToken: !GetAtt ConnectionStringGeneratorLambda.Arn

  PetDatabaseConnectionString:
    DependsOn: ConnectionString
    # For example purposes we're using SSM parameter store.
    # In your template, use secure alternatives to store
    # sensitive values such as connection strings.
    Type: AWS::SSM::Parameter
    Properties:
      Name: pet-database-connection-string
      Description: Connection information for the BestPets pet database
      Type: String
      Value: !GetAtt ConnectionString.Value
```

단계 3. 맞춤형 청사진을 검토하세요.

콘솔에서 블루프린트를 볼 수 있습니다. AWS Service Catalog 자세한 내용은 Service Catalog 관리자 안내서의 제품 관리를 참조하십시오.

4단계. 청사진을 호출하여 사용자 지정 계정을 생성하십시오.

AWS Control Tower 콘솔에서 계정 생성 워크플로를 따라가면 계정을 사용자 지정하는 데 사용할 블루프린트에 대한 정보를 입력할 수 있는 선택적 섹션이 표시됩니다.

> **Note**
>
> 사용자 지정 허브 계정을 설정하고 청사진 (Service Catalog 제품) 을 하나 이상 추가해야 해당 정보를 AWS Control Tower 콘솔에 입력하고 사용자 지정 계정을 프로비저닝하기 시작할 수 있습니다.

AWS Control Tower 콘솔에서 사용자 지정 계정을 생성하거나 업데이트하십시오.

1. 블루프린트가 포함된 계정의 계정 ID를 입력합니다.
2. 해당 계정에서 기존 Service Catalog 제품 (기존 청사진) 을 선택합니다.
3. 버전이 두 개 이상인 경우 적절한 버전의 청사진 (Service Catalog 제품) 을 선택하십시오.
4. (선택 사항) 프로세스의 이 시점에서 블루프린트 프로비저닝 정책을 추가하거나 변경할 수 있습니다. 블루프린트 프로비저닝 정책은 JSON으로 작성되고 IAM 역할에 연결되므로 블루프린트 템플릿에 지정된 리소스를 프로비저닝할 수 있습니다. AWS Control Tower는 Service Catalog가 AWS CloudFormation 스택 세트를 사용하여 리소스를 배포할 수 있도록 멤버 계정에 이 역할을 생성합니다. 이 역할의 이름은 `AWSControlTower-BlueprintExecution-bp-`*`xxxx`*입니다. `AdministratorAccess`정책은 기본적으로 여기에 적용됩니다.
5. 이 블루프린트에 따라 계정을 배포하려는 지역 AWS 리전 또는 지역을 선택합니다.
6. 블루프린트에 파라미터가 포함된 경우, AWS Control Tower 워크플로의 추가 필드에 파라미터 값을 입력할 수 있습니다. 추가 값에는 GitHub 리포지토리 이름, GitHub 브랜치, Amazon ECS 클러스터 이름, 리포지토리 소유자의 GitHub ID 등이 포함될 수 있습니다.
7. 허브 계정이나 블루프린트가 아직 준비되지 않은 경우 계정 업데이트 프로세스에 따라 나중에 계정을 사용자 지정할 수 있습니다.

자세한 내용은 블루프린트에서 사용자 지정 계정을 만드세요.를 참조하세요.

블루프린트에서 사용자 지정 계정을 만드세요.

사용자 지정 블루프린트를 생성한 후에는 AWS Control Tower 계정 팩토리에서 사용자 지정 계정 생성을 시작할 수 있습니다.

새 AWS 계정을 생성할 때 다음 단계에 따라 사용자 지정 청사진을 배포하십시오.

1. 의 AWS Control Tower로 이동하십시오 AWS Management Console.
2. 어카운트 팩토리를 선택하고 계정 생성을 선택합니다.

3. 계정 이름 및 이메일 주소와 같은 계정 세부 정보를 입력합니다.
4. 이메일 주소 및 사용자 이름으로 IAM ID 센터 세부 정보를 구성합니다.
5. 계정을 추가할 등록된 OU를 선택합니다.
6. 어카운트 팩토리 사용자 지정 섹션을 확장하세요.
7. Service Catalog 제품이 들어 있는 블루프린트 허브 계정의 계정 ID를 입력하고 Validate를 선택합니다. 블루프린트 허브 계정에 대한 자세한 내용은 을 참조하십시오. AFC (Account Factory Customize) 로 계정을 사용자 지정하세요
8. Service Catalog 제품 목록의 모든 청사진 (모든 사용자 지정 및 파트너 청사진) 이 포함된 드롭다운 메뉴를 선택합니다. 배포할 블루프린트와 해당 버전을 선택합니다.
9. 블루프린트에 파라미터가 포함된 경우, 이 필드는 사용자가 채울 수 있도록 표시됩니다. 기본값은 미리 채워집니다.
10. 마지막으로, 블루프린트를 배포할 위치 (홈 지역 또는 모든 관리 지역) 를 선택합니다. Route 53 또는 IAM과 같은 글로벌 리소스는 단일 지역에만 배포해야 할 수 있습니다. Amazon EC2 인스턴스 또는 Amazon S3 버킷과 같은 지역 리소스를 모든 관리 지역에 배포할 수 있습니다.
11. 모든 필드를 작성한 후 계정 생성을 선택합니다.

> **Note**
>
> Terraform으로 만든 블루프린트는 한 지역에만 배포할 수 있으며 여러 지역에 배포할 수 없습니다.

조직 페이지에서 계정 프로비저닝 진행 상황을 확인할 수 있습니다. 계정 프로비저닝이 완료되면 블루프린트에서 지정한 리소스가 이미 그 안에 배포되어 있습니다. 계정 및 청사진의 세부 정보를 보려면 계정 세부 정보 페이지로 이동하세요.

계정 등록 및 사용자 지정

AWS Control Tower 콘솔에서 계정을 등록하고 사용자 지정합니다.

1. AWS Control Tower 콘솔로 이동한 다음 왼쪽 탐색 메뉴에서 조직을 선택합니다.
2. 사용 가능한 계정 목록이 표시됩니다. 사용자 지정 블루프린트로 등록하려는 계정을 식별하십시오. 해당 계정의 상태 열에는 미등록 상태인 계정이 반영되어야 합니다.
3. 계정 왼쪽에 있는 라디오 버튼을 선택하고 화면 오른쪽 상단의 작업 드롭다운 메뉴를 선택합니다. 여기서 등록 옵션을 선택합니다.

4. 계정의 IAM ID 센터 정보를 사용하여 액세스 구성 섹션을 완료하십시오.
5. 계정이 구성원이 될 등록된 OU를 선택합니다.
6. 계정 만들기 절차의 7-12와 동일한 단계를 사용하여 계정 팩토리 사용자 지정 섹션을 완료하십시오. 자세한 내용은 Account Factory 계정 프로비저닝을 참조하십시오 AWS Service Catalog.

조직 페이지에서 계정 진행 상태를 볼 수 있습니다. 계정 등록이 완료되면 블루프린트에서 지정한 리소스가 이미 계정 내에 배포되어 있습니다.

AWS Control Tower 계정에 청사진 추가

기존 AWS Control Tower 회원 계정에 청사진을 추가하려면 AWS Control Tower 콘솔의 계정 업데이트 워크플로를 따르고 계정에 추가할 새 청사진을 선택하십시오. 자세한 내용은 AWS Control Tower 또는 AWS Control Tower를 통한 Account Factory 계정 업데이트 및 이동을 참조하십시오 AWS Service Catalog.

> **Note**
>
> 계정에 새 청사진을 추가하면 기존 청사진을 덮어씁니다.

> **Note**
>
> AWS Control Tower 계정당 하나의 블루프린트를 배포할 수 있습니다.

청사진 업데이트

다음 절차는 커스텀 블루프린트를 업데이트하는 방법과 이를 배포하는 방법을 설명합니다.

커스텀 블루프린트를 업데이트하려면

1. 새 구성으로 AWS CloudFormation 템플릿 또는 Terraform tar.gz 파일 (청사진) 을 업데이트하세요.
2. 업데이트된 블루프린트를 새 버전으로 에 저장합니다. AWS Service Catalog

업데이트된 블루프린트를 배포하려면

1. AWS Control Tower 콘솔에서 조직 페이지로 이동합니다.

2. 블루프린트 이름 및 버전을 기준으로 조직 페이지를 필터링합니다.
3. 계정 업데이트 프로세스에 따라 계정에 최신 블루프린트 버전을 배포하세요.

블루프린트 업데이트가 실패한 경우

AWS Control Tower는 프로비저닝된 제품이 주 내에 있을 때 블루프린트 업데이트를 허용합니다. `AVAILABLE` 프로비저닝된 제품이 특정 `TAINTED` 상태에 있는 경우 업데이트가 실패합니다. 다음 해결 방법을 사용하는 것이 좋습니다.

1. AWS Service Catalog 콘솔에서 `TAINTED` 프로비저닝된 제품을 수동으로 업데이트하여 상태를 로 변경합니다. `AVAILABLE` 자세한 내용은 프로비저닝된 제품 업데이트를 참조하십시오.
2. 그런 다음, AWS Control Tower의 계정 업데이트 프로세스에 따라 블루프린트 배포 오류를 수정하십시오.

이 수동 단계를 권장하는 이유는 다음과 같습니다. 블루프린트를 제거하면 멤버 계정의 리소스가 제거될 수 있기 때문입니다. 리소스를 제거하면 기존 워크로드에 영향을 미칠 수 있습니다. 이러한 이유로, 특히 프로덕션 워크로드를 실행하는 경우 원본 블루프린트를 제거하고 교체하는 블루프린트를 업데이트하는 다른 방법보다는 이 방법을 사용하는 것이 좋습니다.

계정에서 블루프린트 삭제하기

계정에서 블루프린트를 제거하려면 계정 업데이트 워크플로에 따라 블루프린트를 제거하고 계정을 AWS Control Tower 기본 구성으로 되돌립니다.

콘솔에서 계정 업데이트 워크플로를 시작하면 모든 계정 세부 정보가 채워지고 사용자 지정 세부 정보는 채워지지 않은 것을 볼 수 있습니다. 이러한 AFC 세부 정보를 비워 두면 AWS Control Tower가 계정에서 청사진을 제거합니다. 작업이 시작되기 전에 경고 메시지가 표시됩니다.

> **Note**
>
> AWS Control Tower는 계정 생성 또는 계정 업데이트 프로세스 중에 청사진을 선택한 경우에만 계정에 청사진을 추가합니다.

파트너 청사진

AWS Control Tower Account Factory Customization (AFC) 은 파트너가 구축하고 관리하는 사전 정의된 사용자 지정 청사진에 대한 액세스를 제공합니다. AWS 이 파트너 블루프린트는 특정 사용 사례에

맞게 계정을 사용자 지정하는 데 도움이 됩니다. 각 파트너의 청사진은 특정 파트너가 제공하는 제품과 함께 작동하도록 사전 구성된 맞춤형 계정을 구축하는 데 도움이 됩니다.

AWS Control Tower 파트너 청사진의 전체 목록을 보려면 콘솔의 Service Catalog 시작 라이브러리로 이동하십시오. 소스 유형 AWS Control Tower 블루프린트를 검색하십시오.

AFC (어카운트 팩토리 커스터마이징) 고려 사항

- AFC는 단일 AWS Service Catalog 블루프린트 제품만을 사용한 커스터마이징을 지원합니다.
- AWS Service Catalog 블루프린트 제품은 허브 계정에서 생성되어야 하며, AWS Control Tower 랜딩 존 홈 리전과 동일한 리전에 생성되어야 합니다.
- `AWSControlTowerBlueprintAccess`IAM 역할은 적절한 이름, 권한 및 신뢰 정책을 사용하여 생성되어야 합니다.
- AWS Control Tower는 블루프린트에 대한 두 가지 배포 옵션을 지원합니다. 하나는 홈 지역에만 배포하거나 AWS Control Tower가 관리하는 모든 지역에 배포하는 것입니다. 지역 선택은 불가능합니다.
- 멤버 계정에서 블루프린트를 업데이트할 때 블루프린트 허브 계정 ID와 AWS Service Catalog 블루프린트 제품은 변경할 수 없습니다.
- AWS Control Tower는 단일 청사진 업데이트 작업에서 기존 청사진을 제거하고 새 청사진을 추가하는 것을 지원하지 않습니다. 블루프린트를 제거한 다음 별도의 작업으로 새 블루프린트를 추가할 수 있습니다.
- AWS Control Tower는 사용자 지정 계정을 생성 또는 등록하는지 아니면 사용자 지정 계정이 아닌 계정을 생성하는지 여부에 따라 동작을 변경합니다. 블루프린트로 사용자 지정 계정을 만들거나 등록하지 않는 경우, AWS Control Tower는 (Service Catalog를 통해) AWS 컨트롤 타워 관리 계정에서 Account Factory가 프로비저닝한 제품을 생성합니다. 블루프린트로 계정을 만들거나 등록할 때 사용자 지정을 지정하는 경우, AWS Control Tower는 AWS Control Tower 관리 계정에 Account Factory가 프로비저닝한 제품을 생성하지 않습니다.

블루프린트 오류가 발생한 경우

블루프린트 적용 중 오류가 발생했습니다.

블루프린트를 계정 (새 계정 또는 AWS Control Tower에 등록한 기존 계정) 에 적용하는 과정에서 오류가 발생하는 경우 복구 절차는 동일합니다. 계정은 존재하지만 사용자 지정되지 않고 AWS Control Tower에 등록되어 있지도 않습니다. 계속하려면 단계에 따라 계정을 AWS Control Tower에 등록하고 등록 시 청사진을 추가하십시오.

역할 생성 중 오류 발생 및 해결 방법 **AWSControlTowerBlueprintAccess**

AWS Control Tower 계정에서 AWSControlTowerBlueprintAccess 역할을 생성할 때는 AWSControlTowerExecution 역할을 사용하여 보안 주체로 로그인해야 합니다. 다른 사람과 마찬가지로 로그인한 경우 다음 아티팩트에서 볼 수 있듯이 SCP가 CreateRole 작업을 차단합니다.

```
{
            "Condition": {
                "ArnNotLike": {
                    "aws:PrincipalArn": [
                        "arn:aws:iam::*:role/AWSControlTowerExecution",
                        "arn:aws:iam::*:role/stacksets-exec-*"
                    ]
                }
            },
            "Action": [
                "iam:AttachRolePolicy",
                "iam:CreateRole",
                "iam:DeleteRole",
                "iam:DeleteRolePermissionsBoundary",
                "iam:DeleteRolePolicy",
                "iam:DetachRolePolicy",
                "iam:PutRolePermissionsBoundary",
                "iam:PutRolePolicy",
                "iam:UpdateAssumeRolePolicy",
                "iam:UpdateRole",
                "iam:UpdateRoleDescription"
            ],
            "Resource": [
                "arn:aws:iam::*:role/aws-controltower-*",
                "arn:aws:iam::*:role/*AWSControlTower*",
                "arn:aws:iam::*:role/stacksets-exec-*"
            ],
            "Effect": "Deny",
            "Sid": "GRIAMROLEPOLICY"
        }
```

다음과 같은 해결 방법을 사용할 수 있습니다.

- (가장 권장됨) AWSControlTowerExecution 역할을 맡고 역할을 생성합니다. AWSControlTowerBlueprintAccess 이 해결 방법을 선택한 경우 의도하지 않은 리소스 변경을 방지하기 위해 즉시 AWSControlTowerExecution 역할에서 로그아웃해야 합니다.

- AWS Control Tower에 등록되지 않았으므로 이 SCP의 적용을 받지 않는 계정으로 로그인하십시오.
- 작업을 허용하도록 이 SCP를 일시적으로 편집하십시오.
- (강력히 권장하지 않음) SCP의 적용을 받지 않도록 AWS Control Tower 관리 계정을 허브 계정으로 사용하십시오.

다음을 기반으로 AFC 청사진에 맞게 정책 문서를 사용자 지정합니다. CloudFormation

어카운트 팩토리를 통해 블루프린트를 활성화하면 AWS Control Tower가 사용자 대신 블루프린트를 AWS CloudFormation StackSet 생성하도록 지시합니다. AWS CloudFormation 에서 AWS CloudFormation 스택을 생성하려면 관리형 계정에 대한 액세스 권한이 필요합니다. StackSet 역할을 통해 AWS CloudFormation 이미 관리 계정에 대한 관리자 권한을 가지고 있지만 이 `AWSControlTowerExecution` 역할을 맡을 수는 없습니다. AWS CloudFormation

청사진 활성화의 일환으로 AWS Control Tower는 회원 계정에 역할을 생성하며, 이 역할은 StackSet 관리 작업을 완료하는 것으로 AWS CloudFormation 간주될 수 있습니다. Account Factory를 통해 사용자 지정 청사진을 활성화하는 가장 간단한 방법은 모두 허용 정책을 사용하는 것입니다. 이러한 정책은 모든 청사진 템플릿과 호환되기 때문입니다.

하지만 모범 AWS CloudFormation 사례에서는 대상 계정의 권한을 제한해야 한다고 제안합니다. 사용자 지정 정책을 제공할 수 있으며, 이 정책은 AWS Control Tower가 생성한 역할에 AWS CloudFormation 적용하여 사용할 수 있습니다. 예를 들어, 블루프린트에서 무언가-important라는 SSM 파라미터를 생성하는 경우 다음 정책을 제공할 수 있습니다.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AllowCloudFormationActionsOnStacks",
            "Effect": "Allow",
            "Action": "cloudformation:*",
            "Resource": "arn:aws:cloudformation:*:*:stack/*"
        },
        {
            "Sid": "AllowSsmParameterActions",
            "Effect": "Allow",
            "Action": [
                "ssm:PutParameter",
                 "ssm:DeleteParameter",
```

```
                "ssm:GetParameter",
                "ssm:GetParameters"
            ],
            "Resource": "arn:*:ssm:*:*:parameter/something-important"
        }
    ]
}
```

이 AllowCloudFormationActionsOnStacks 명령문은 모든 AFC 커스텀 정책에 필요합니다. 이 역할을 AWS CloudFormation 사용하여 스택 인스턴스를 생성하므로 스택에서 작업을 수행할 권한이 필요합니다. AWS CloudFormation 이 AllowSsmParameterActions 섹션은 활성화되는 템플릿에만 해당됩니다.

권한 문제 해결

제한된 정책으로 블루프린트를 활성화하면 블루프린트를 활성화하는 데 필요한 권한이 충분하지 않을 수 있습니다. 이러한 문제를 해결하려면 정책 문서를 수정하고 수정된 정책을 사용하도록 회원 계정의 블루프린트 환경설정을 업데이트하세요. 정책이 블루프린트를 활성화하기에 충분한지 확인하려면 AWS CloudFormation 권한이 부여되고 해당 역할을 사용하여 스택을 직접 생성할 수 있는지 확인하세요.

Terraform 기반 서비스 카탈로그 제품 생성에 필요한 추가 권한

AFC용 Terraform 구성 파일을 사용하여 AWS Service Catalog 외부 제품을 만들 때는 템플릿에 정의된 리소스를 생성하는 데 필요한 권한 외에도 AFC 사용자 지정 IAM 정책에 특정 권한을 추가해야 합니다. AWS Service Catalog 기본 전체 관리자 정책을 선택하면 이러한 추가 권한을 추가할 필요가 없습니다.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": [
                "resource-groups:CreateGroup",
                "resource-groups:ListGroupResources",
                "resource-groups:DeleteGroup",
                "resource-groups:Tag"
            ],
            "Resource": "*",
            "Effect": "Allow"
        },
```

```
        {
            "Action": [
                "tag:GetResources",
                "tag:GetTagKeys",
                "tag:GetTagValues",
                "tag:TagResources",
                "tag:UntagResources"
            ],
            "Resource": "*",
            "Effect": "Allow"
        },
        {
            "Action": "s3:GetObject",
            "Effect": "Allow",
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "s3:ExistingObjectTag/servicecatalog:provisioning": "true"
                }
            }
        }
    ]
}
```

외부 제품 유형을 사용하여 Terraform 제품을 만드는 방법에 대한 자세한 내용은 Service Catalog 관리자 가이드의 5단계: 시작 역할 생성을 참조하십시오. AWS Service Catalog

테라폼용 AWS Control Tower 어카운트 팩토리 (AFT) 를 통해 계정 프로비저닝

AWS Control Tower Account Factory for Terraform (AFT) 은 AWS Control Tower에서 계정 프로비저닝 및 업데이트 프로세스를 자동화하는 GitOps 모델을 채택했습니다.

> **Note**
>
> AFT는 AWS Control Tower의 워크플로 성능에 영향을 주지 않습니다. AFT 또는 Account Factory를 통해 계정을 프로비저닝하는 경우 동일한 백엔드 워크플로가 발생합니다.

AFT를 사용하면 AFT 워크플로를 호출하는 입력이 포함된 계정 요청 Terraform 파일을 생성합니다. 계정 프로비저닝 및 업데이트가 완료된 후 AFT 계정 프로비저닝 프레임워크 및 계정 사용자 지정 단계를 실행하여 AFT 워크플로는 계속됩니다.

필수 조건

AFT를 시작하기 전에 다음을 생성해야 합니다.

- 완전히 배포된 AFT 환경. 자세한 내용은 테라폼용 AWS Control Tower 어카운트 팩토리 (AFT) 개요 및 테라폼용 AWS Control Tower 어카운트 팩토리 배포 (AFT) 를 참조하십시오.
- 완전히 배포된 AFT 환경에 있는 하나 이상의 AFT `git` 리포지토리. 자세한 내용은 AFT의 배포 후 단계를 참조하십시오.

> **Tip**
>
> aft-account-customizations저장소에 계정 템플릿 폴더를 만들 수도 있습니다.

AFT에 배포 제한이 AWS 리전 있는 위치에 대한 자세한 내용은 AWS Control Tower의 한도 및 할당량 및 을 참조하십시오관리 제한.

AFT에 새 계정을 프로비저닝하세요

AFT에 새 계정을 프로비저닝하려면 계정 요청 Terraform 파일을 생성하십시오. 이 파일에는 리포지토리의 매개 변수에 대한 입력이 들어 있습니다. aft-account-request 계정 요청 Terraform 파일을 생성한 후 를 실행하여 계정 요청 처리를 시작합니다. `git push` 이 명령은 계정 프로비저닝이 완료된 후 AFT 관리 계정에 생성되는 에서 `ct-aft-account-request` 작업을 호출합니다. AWS CodePipeline자세한 내용은 AFT 계정 프로비저닝 파이프라인을 참조하십시오.

계정 요청 테라폼 파일 매개변수

계정 요청 Terraform 파일에 다음 매개변수를 포함해야 합니다. 에서 계정 요청 Terraform 파일의 예를 볼 수 있습니다. GitHub

- 의 값은 요청별로 `module name` 고유해야 합니다. AWS 계정
- 의 `module source` 값은 AFT가 제공하는 계정 요청 Terraform 모듈의 경로입니다.
- 의 값은 AWS Control Tower 계정을 생성하는 데 필요한 입력을 `control_tower_parameters` 캡처합니다. 값에는 다음 입력 필드가 포함됩니다.

- `AccountEmail`
- `AccountName`
- `ManagedOrganizationalUnit`
- `SSOUserEmail`
- `SSOUserFirstName`
- `SSOUserLastName`

> **Note**
>
> 제공하는 입력은 계정 공급 중에 변경할 `control_tower_parameters` 수 없습니다. `ManagedOrganizationalUnit`aft-account-request저장소에서 지정할 수 있는 형식은 `OUName` 및 `OUName (OU-ID)` 입니다.

- `account_tags`비즈니스 기준에 AWS 계정 따라 태그를 지정할 수 있는 사용자 정의 키와 값을 캡처합니다. 자세한 내용은 AWS Organizations 사용 설명서의 AWS Organizations 리소스 태깅을 참조하십시오.
- 의 값은 계정 요청이 생성된 이유, 계정 요청을 시작한 사람 등의 추가 정보를 `change_management_parameters` 캡처합니다. 값에는 다음 입력 필드가 포함됩니다.
  - `change_reason`
  - `change_requested_by`
- `custom_fields`/aft/account-request/custom-fields/ 아래의 벤드 계정에 SSM 매개변수로 배포되는 키와 값을 사용하여 추가 메타데이터를 캡처합니다. 계정 사용자 지정 중에 이 메타데이터를 참조하여 적절한 제어 기능을 배포할 수 있습니다. 예를 들어 규제 준수 대상인 계정은 추가 AWS Config 규칙배포를 할 수 있습니다. 수집한 메타데이터로 인해 계정 프로비저닝 및 업데이트 중에 추가 처리가 필요할 `custom_fields` 수 있습니다. 계정 요청에서 사용자 지정 필드가 제거되면 벤딩 계정의 SSM 파라미터 저장소에서 사용자 지정 필드가 제거됩니다.
- (선택 사항) 저장소의 계정 템플릿 폴더를 `account_customizations_name` 캡처합니다 aft-account-customizations. 자세한 내용은 계정 사용자 지정을 참조하십시오.

여러 계정 요청 제출

AFT는 계정 요청을 한 번에 하나씩 처리하지만 AFT 파이프라인에 여러 계정 요청을 제출할 수 있습니다. AFT 파이프라인에 여러 계정 요청을 제출하면 AFT는 선입선출 순서로 계정 요청을 대기하고 처리합니다.

> **Note**
>
> AFT가 프로비저닝하도록 하려는 각 계정에 대해 계정 요청 Terraform 파일을 만들거나 단일 계정 요청 Terraform 파일에서 여러 계정 요청을 단계적으로 처리할 수 있습니다.

기존 계정 업데이트

이전에 제출한 계정 요청을 편집하고 실행하여 AFT가 제공하는 계정을 업데이트할 수 `git push` 있습니다. 이 명령은 계정 프로비저닝 워크플로를 호출하고 계정 업데이트 요청을 처리할 수 있습니다. 필수 값의 `ManagedOrganizationalUnit` 일부인 입력 양식 및 계정 요청 Terraform `control_tower_parameters` 파일의 기타 매개 변수를 업데이트할 수 있습니다. 자세한 내용은 AFT로 새 계정 프로비저닝을 참조하십시오.

> **Note**
>
> 제공하는 입력은 계정 프로비저닝 중에는 변경할 `control_tower_parameters` 수 없습니다.
>
> `ManagedOrganizationalUnit`aft-account-request저장소에서 지정할 수 있는 형식은 `OUName` 및 `OUName (OU-ID)` 입니다.

AFT가 프로비저닝하지 않는 계정 업데이트

aft-account-request리포지토리에서 계정을 지정하여 AFT 외부에서 생성된 AWS Control Tower 계정을 업데이트할 수 있습니다.

> **Note**
>
> 모든 계정 세부 정보가 정확하고 AWS Control Tower 조직 및 AWS Service Catalog 프로비저닝된 각 제품과 일치하는지 확인하십시오.

AFT로 기존 제품을 업데이트하기 위한 사전 요구 사항 AWS 계정

- AWS Control Tower에 등록되어 AWS 계정 있어야 합니다.
- AWS Control Tower 조직의 AWS 계정 일원이어야 합니다.

테라폼용 AWS Control Tower 어카운트 팩토리 (AFT) 배포

이 섹션은 기존 환경에서 Account Factory for Terraform (AFT) 을 설정하려는 AWS Control Tower 환경 관리자를 위한 것입니다. 새로운 전용 AFT 관리 계정을 사용하여 Account Factory for Terraform (AFT) 환경을 설정하는 방법을 설명합니다.

> **Note**
>
> 테라폼 모듈은 AFT를 배포합니다. 이 모듈은 의 AFT 리포지토리에서 사용할 수 있으며 전체 AFT 리포지토리가 모듈로 간주됩니다. GitHub
> AFT 리포지토리를 복제하는 GitHub 대신 AFT 모듈을 참조하는 것이 좋습니다. 이렇게 하면 모듈에 대한 업데이트를 사용 가능한 대로 제어하고 사용할 수 있습니다.

AWS Control Tower Account Factory for Terraform (AFT) 기능의 최신 릴리스에 대한 자세한 내용은 이 GitHub 리포지토리의 릴리스 파일을 참조하십시오.

배포 사전 요구 사항

AFT 환경을 구성하고 시작하기 전에 다음이 있어야 합니다.

- AWS Control Tower 랜딩 존. 자세한 내용은 AWS Control Tower 랜딩 존 계획을 참조하십시오.
- AWS Control Tower 랜딩 존의 홈 리전. 자세한 내용은 AWS Control Tower를 사용하는 방법을 AWS 리전 참조하십시오.
- 테라폼 버전 및 배포판. 자세한 내용은 테라폼 및 AFT 버전을 참조하십시오.
- 코드 및 기타 파일의 변경 사항을 추적하고 관리하는 VCS 공급자입니다. 기본적으로 AFT는 사용합니다 AWS CodeCommit. 자세한 내용은 AWS CodeCommit무엇입니까를 참조하십시오. AWS CodeCommit 사용 설명서에서. 다른 VCS 공급자를 선택하려면 AFT의 소스 코드 버전 관리를 위한 대안을 참조하십시오.
- AFT를 설치하는 Terraform 모듈을 실행할 수 있는 런타임 환경입니다.
- AFT 기능 옵션. 자세한 내용은 기능 옵션 활성화를 참조하십시오.

테라폼용 AWS Control Tower Account Factory를 구성하고 실행하십시오.

다음 단계에서는 Terraform 워크플로를 잘 알고 있다고 가정합니다. 또한 AWS 워크샵 스튜디오 웹 사이트의 AFT 랩 소개를 참조하여 AFT 배포에 대해 자세히 알아볼 수 있습니다.

1단계: AWS Control Tower 랜딩 존 시작

AWS Control Tower 시작하기의 단계를 완료하십시오. 여기에서 AWS Control Tower 관리 계정을 생성하고 AWS Control Tower 랜딩 존을 설정합니다.

> **Note**
>
> AdministratorAccess자격 증명이 있는 AWS Control Tower 관리 계정에 대한 역할을 생성해야 합니다. 자세한 내용은 다음을 참조하십시오.
>
> - 사용 설명서의 IAM ID (사용자, 사용자 그룹, 역할)AWS Identity and Access Management
> - AdministratorAccess AWS관리형 정책 참조 가이드에서

2단계: AFT용 새 조직 단위 만들기 (권장)

AWS 조직에 별도의 OU를 만드는 것이 좋습니다. 여기서 AFT 관리 계정을 배포합니다. AWS Control Tower 관리 계정으로 새 OU를 생성합니다. 자세한 내용은 새 OU 생성을 참조하십시오.

3단계: AFT 관리 계정 프로비저닝

AFT를 사용하려면 AFT 관리 작업 전용 AWS 계정을 프로비저닝해야 합니다. AWS Control Tower 랜딩 존과 연결된 AWS Control Tower 관리 계정은 AFT 관리 계정을 판매합니다. 자세한 내용은 Account Factory를 통한 AWS Service Catalog 계정 프로비저닝을 참조하십시오.

> **Note**
>
> AFT에 대해 별도의 OU를 생성한 경우 AFT 관리 계정을 생성할 때 이 OU를 선택해야 합니다.

AFT 관리 계정을 완전히 프로비저닝하는 데 최대 30분이 걸릴 수 있습니다.

4단계: Terraform 환경을 배포할 수 있는지 확인

이 단계에서는 Terraform을 사용해 본 경험이 있고 Terraform을 실행하기 위한 절차가 마련되어 있다고 가정합니다. 자세한 내용은 개발자 웹 사이트의 Command: init를 참조하십시오. HashiCorp

> **Note**
>
> AFT는 테라폼 버전 `1.2.0` 이상을 지원합니다.

5단계: AFT를 배포하려면 테라폼 모듈용 Account Factory를 호출하십시오.

AdministratorAccess자격 증명이 있는 AWS Control Tower 관리 계정에 대해 생성한 역할을 사용하여 AFT 모듈을 호출합니다. AWS Control Tower는 AWS Control Tower 관리 계정을 통해 Terraform 모듈을 프로비저닝합니다. 이 계정은 AWS Control Tower Account Factory 요청을 오케스트레이션하는 데 필요한 모든 인프라를 설정합니다.

AFT 모듈은 AFT 리포지토리에서 볼 수 있습니다. GitHub 전체 GitHub 리포지토리는 AFT 모듈로 간주됩니다. AFT 모듈을 실행하고 AFT를 배포하는 데 필요한 입력에 대한 자세한 내용은 README 파일을 참조하십시오. 또는 Terraform 레지스트리에서 AFT 모듈을 볼 수도 있습니다.

AFT 모듈에는 AWS Control Tower가 중앙 AFT 관리 계정의 가상 사설 클라우드 (VPC) 내에서 계정 리소스를 프로비저닝할지 여부를 지정하는 `aft_enable_vpc` 파라미터가 포함되어 있습니다. 기본적으로 파라미터는 로 설정됩니다. `true` 이 파라미터를 로 `false` 설정하면 AWS Control Tower는 VPC와 프라이빗 네트워킹 리소스 (예: NAT 게이트웨이 또는 VPC 엔드포인트) 를 사용하지 않고 AFT를 배포합니다. 비활성화하면 일부 사용 패턴에서 AFT 운영 비용을 줄이는 데 도움이 *`aft_enable_vpc`* 될 수 있습니다.

> **Note**
>
> `aft_enable_vpc`파라미터를 다시 활성화하려면 (값을 에서 `false` 로 전환`true`) `terraform apply` 명령을 두 번 연속으로 실행해야 할 수 있습니다.

환경에 Terraform 관리를 위해 설정된 파이프라인이 있는 경우 AFT 모듈을 기존 워크플로에 통합할 수 있습니다. 그렇지 않으면 필요한 자격 증명으로 인증된 모든 환경에서 AFT 모듈을 실행하세요.

타임아웃으로 인해 배포가 실패합니다. 전체 배포에 충분한 제한 시간을 확보하려면 AWS Security Token Service (STS) 자격 증명을 사용하는 것이 좋습니다. AWS STS 자격 증명의 최소 제한 시간은 60분입니다. 자세한 내용은 사용 AWS Identity and Access Management 설명서의 IAM의 임시 보안 자격 증명을 참조하십시오.

> **Note**
>
> AFT가 Terraform 모듈을 통한 배포를 완료할 때까지 최대 30분까지 기다릴 수 있습니다.

6단계: 테라폼 상태 파일 관리

AFT를 배포할 때 테라폼 상태 파일이 생성됩니다. 이 아티팩트는 Terraform이 생성한 리소스의 상태를 설명합니다. AFT 버전을 업데이트하려는 경우 테라폼 상태 파일을 보존하거나 Amazon S3 및 DynamoDB를 사용하여 테라폼 백엔드를 설정해야 합니다. AFT 모듈은 백엔드 테라폼 상태를 관리하지 않습니다.

> **Note**
>
> Terraform 상태 파일을 보호하는 것은 사용자의 책임입니다. 일부 입력 변수에는 개인 ssh 키 또는 Terraform 토큰과 같은 민감한 값이 포함될 수 있습니다. 배포 방법에 따라 Terraform 상태 파일에서 이러한 값을 일반 텍스트로 볼 수 있습니다. 자세한 내용은 웹 사이트의 주 내 민감한 데이터를 참조하십시오. HashiCorp

배포 후 단계

AFT 인프라 배포가 완료되면 다음 추가 단계에 따라 설정 프로세스를 완료하고 계정을 프로비저닝할 준비를 하십시오.

1단계: (선택 사항) 원하는 VCS CodeConnections 공급자와 함께 작성

타사 VCS 공급자를 선택하면 AFT가 CodeConnections 설립하고 사용자가 이를 확인합니다. 선호하는 AFT의 소스 코드 버전 관리를 위한 대안 VCS로 AFT를 설정하는 방법을 알아보려면 을 참조하십시오.

AWS CodeStar 연결 설정의 초기 단계는 AFT를 통해 수행됩니다. 연결을 확인해야 합니다.

2단계: (필수) 각 리포지토리 채우기

AFT를 사용하려면 네 개의 리포지토리를 관리해야 합니다.

1. 계정 요청 - 이 리포지토리는 계정 요청의 배치 또는 업데이트를 처리합니다. 예시를 사용할 수 있습니다. AFT 계정 요청에 대한 자세한 내용은 을 참조하십시오AFT에 새 계정을 프로비저닝하세요.
2. AFT 계정 프로비저닝 사용자 지정 - 이 리포지토리는 글로벌 사용자 지정 단계를 시작하기 전에 AFT에서 생성하고 관리하는 모든 계정에 적용되는 사용자 지정을 관리합니다. 예제를 사용할 수 있

습니다. AFT 계정 프로비저닝 사용자 지정을 생성하려면 을 참조하십시오. AFT 계정 프로비저닝 사용자 지정 상태 머신을 생성하세요.

3. 글로벌 사용자 지정 — 이 리포지토리는 AFT에서 생성하고 AFT로 관리하는 모든 계정에 적용되는 사용자 지정을 관리합니다. 예를 사용할 수 있습니다. AFT 글로벌 사용자 지정을 만들려면 을 참조하십시오글로벌 사용자 지정 적용.
4. 계정 사용자 지정 - 이 리포지토리는 AFT에서 생성하고 관리하는 특정 계정에만 적용되는 사용자 지정을 관리합니다. 예를 사용할 수 있습니다. AFT 계정 사용자 지정을 생성하려면 을 참조하십시오계정 사용자 지정 적용.

AFT는 이러한 각 리포지토리가 특정 디렉터리 구조를 따를 것으로 예상합니다. 리포지토리를 채우는 데 사용되는 템플릿과 템플릿을 채우는 방법을 설명하는 지침은 AFT github 리포지토리의 Account Factory for Terraform 모듈에서 사용할 수 있습니다.

테라폼용 AWS Control Tower 어카운트 팩토리 (AFT) 개요

Account Factory for Terraform (AFT) 은 AWS Control Tower에서 계정을 프로비저닝하고 사용자 지정하는 데 도움이 되는 테라폼 파이프라인을 설정합니다. AFT는 Terraform 기반 계정 프로비저닝의 이점을 제공하는 동시에 AWS Control Tower를 통해 계정을 관리할 수 있도록 합니다.

AFT를 사용하면 계정 요청 Terraform 파일을 생성하여 계정 프로비저닝을 위한 AFT 워크플로를 트리거하는 입력을 받을 수 있습니다. 계정 프로비저닝 단계가 완료되면 AFT는 계정 사용자 지정 단계가 시작되기 전에 일련의 단계를 자동으로 실행합니다. 자세한 내용은 AFT 계정 프로비저닝 파이프라인을 참조하십시오.

AFT는 테라폼 클라우드, 테라폼 엔터프라이즈, 테라폼 커뮤니티 에디션을 지원합니다. AFT를 사용하면 입력 파일과 간단한 `git push` 명령을 사용하여 계정 생성을 시작하고 신규 또는 기존 계정을 사용자 지정할 수 있습니다. 계정 생성에는 조직의 표준 보안 절차 및 규정 준수 지침을 충족하는 데 도움이 되는 모든 AWS Control Tower 거버넌스 혜택과 계정 사용자 지정이 포함됩니다.

AFT는 계정 사용자 지정 요청 추적을 지원합니다. 계정 사용자 지정 요청을 제출할 때마다 AFT는 AFT 사용자 지정 AWS Step Functions 상태 시스템을 통과하는 고유한 추적 토큰을 생성합니다. 이 시스템은 실행의 일부로 토큰을 기록합니다. 그런 다음 Amazon CloudWatch Logs 인사이트 쿼리를 사용하여 타임스탬프 범위를 검색하고 요청 토큰을 검색할 수 있습니다. 따라서 토큰과 함께 제공되는 페이로드를 확인할 수 있으므로 전체 AFT 워크플로에서 계정 사용자 지정 요청을 추적할 수 있습니다. CloudWatch 로그 및 Step Functions에 대한 자세한 내용은 다음을 참조하십시오.

- 아마존 CloudWatch 로그란 무엇입니까? Amazon CloudWatch Logs 사용 설명서에서

- 무엇입니까 AWS Step Functions? AWS Step Functions 개발자 안내서에서

AFT는 다른 AWS 서비스의 기능을 프레임워크를 구축할 때 Terraform IaC (코드형 인프라) 를 배포하는 파이프라인과 결합합니다. 컴포넌트 서비스 AFT를 사용하면 다음을 수행할 수 있습니다.

- 모델에서 계정 프로비저닝 및 업데이트 요청 제출 GitOps
- 계정 메타데이터 및 감사 기록 저장
- 계정 수준 태그 적용
- 모든 계정, 계정 세트 또는 개별 계정에 사용자 지정 추가
- 기능 옵션 활성화

AFT는 AFT 관리 계정이라는 별도의 계정을 생성하여 AFT 기능을 배포합니다. AFT를 설정하려면 먼저 기존 AWS Control Tower 랜딩 존이 있어야 합니다. AFT 관리 계정은 AWS Control Tower 관리 계정과 동일하지 않습니다.

AFT는 유연성을 제공합니다.

- 플랫폼의 유연성: AFT는 초기 배포 및 지속적인 운영을 위한 모든 Terraform 배포판 (커뮤니티 에디션, 클라우드 및 엔터프라이즈) 을 지원합니다.
- 버전 제어 시스템의 유연성: AFT는 기본적으로 이를 기반으로 AWS CodeCommit하지만 대체 소스를 지원합니다. CodeConnections

AFT는 기능 옵션을 제공합니다.

모범 사례에 따라 여러 기능 옵션을 활성화할 수 있습니다.

- 데이터 이벤트 로깅을 CloudTrail 위한 조직 수준 만들기
- 계정의 AWS 기본 VPC 삭제
- 프로비저닝된 계정을 Enterprise AWS Support 플랜에 등록

> **Note**
>
> AFT 파이프라인은 Amazon EC2 인스턴스와 같이 계정에서 애플리케이션을 실행하는 데 필요한 리소스를 배포하는 데 사용하기 위한 것이 아닙니다. 이는 AWS Control Tower 계정을 자동으로 프로비저닝하고 사용자 지정하는 용도로만 사용됩니다.

비디오 안내

이 동영상 (7:33) 에서는 Terraform용 AWS Control Tower Account Factory를 사용하여 계정을 배포하는 방법을 설명합니다. 동영상 오른쪽 하단에 있는 아이콘을 선택하여 전체 화면으로 확대하면 더 잘 보입니다. 자막을 사용할 수 있습니다.

AWS Control Tower의 자동 계정 프로비저닝에 대한 동영상 설명.

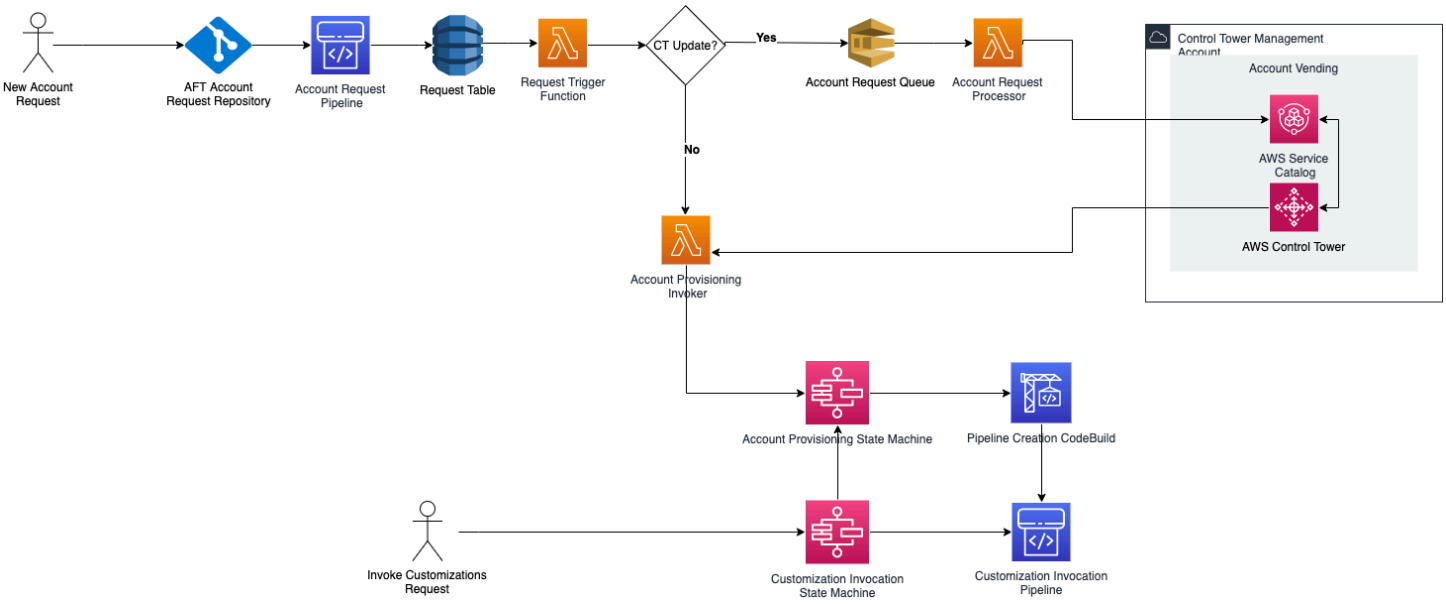
AFT 아키텍처

작업 순서

AFT 관리 계정에서 AFT 작업을 실행합니다. 전체 계정 프로비저닝 워크플로의 경우 다이어그램에서 왼쪽에서 오른쪽으로 단계 순서는 다음과 같습니다.

1. 계정 요청이 생성되어 파이프라인에 제출됩니다. 한 번에 두 개 이상의 계정 요청을 생성하고 제출할 수 있습니다. Account Factory는 요청을 first-in-first-out 주문으로 처리합니다. 자세한 내용은 복수 계정 요청 제출을 참조하십시오.
2. 각 계정이 프로비저닝됩니다. 이 단계는 AWS Control Tower 관리 계정에서 실행됩니다.
3. 글로벌 사용자 지정은 벤더 계정별로 생성된 파이프라인에서 실행됩니다.
4. 초기 계정 프로비저닝 요청에서 사용자 지정을 지정한 경우 사용자 지정은 대상 계정에서만 실행됩니다. 이미 프로비저닝된 계정이 있는 경우 계정 파이프라인에서 추가 사용자 지정을 수동으로 시작해야 합니다.

테라폼용 AWS Control Tower 어카운트 팩토리 — 계정 프로비저닝 워크플로



비용

AFT에는 추가 요금이 부과되지 않습니다. AFT에서 배포한 리소스, AFT에서 지원하는 AWS 서비스, AFT 환경에 배포한 리소스에 대해서만 비용을 지불하면 됩니다.

기본 AFT 구성에는 향상된 데이터 보호 및 보안을 위한 AWS PrivateLink 엔드포인트 할당과 지원에 필요한 NAT 게이트웨이가 포함됩니다. AWS CodeBuild 이 인프라 요금에 대한 자세한 내용은 NAT Gateway의 AWS PrivateLink 요금 및 Amazon VPC 요금을 참조하십시오. 이러한 비용 관리에 대한 자세한 내용은 AWS 계정 담당자에게 문의하십시오. AFT의 기본 설정을 변경할 수 있습니다.

테라폼 및 AFT 버전

Account Factory for Terraform (AFT) 은 테라폼 버전 이상을 지원합니다. `1.2.0` 다음 예와 같이 AFT 배포 프로세스의 입력 매개변수로 Terraform 버전을 제공해야 합니다.

```
terraform_version = "1.2.0"
```

테라폼 배포판

AFT는 세 가지 테라폼 배포판을 지원합니다.

- 테라폼 커뮤니티 에디션
- 테라폼 클라우드
- 테라폼 엔터프라이즈

이러한 배포판은 다음 섹션에 설명되어 있습니다. AFT 부트스트랩 프로세스 중에 선택한 Terraform 분포를 입력 매개변수로 제공하십시오. AFT 배포 및 입력 매개변수에 대한 자세한 내용은 을 참조하십시오. 테라폼용 AWS Control Tower 어카운트 팩토리 (AFT) 배포

Terraform Cloud 또는 Terraform Enterprise 배포판을 선택하는 경우 지정하는 API 토큰은 사용자 또는 팀 API `terraform_token` 토큰이어야 합니다. 조직 토큰은 모든 필수 API에 지원되지 않습니다. 보안상의 이유로 다음 예와 같이 terraform 변수를 할당하여 버전 제어 시스템 (VCS) 에 이 토큰의 값을 체크인하지 않도록 해야 합니다.

```
# Sensitive variable managed in Terraform Cloud:
terraform_token = var.terraform_cloud_token
```

테라폼 커뮤니티 에디션

Terraform 커뮤니티 에디션을 배포판으로 선택하면 AFT가 AFT 관리 계정에서 Terraform 백엔드를 관리합니다. AFT는 `terraform-cli` 지정된 Terraform 버전을 다운로드하여 AFT 배포 및 AFT 파이프라인 단계에서 실행합니다. 결과 Terraform 상태 구성은 다음 형식으로 이름이 지정된 Amazon S3 버킷에 저장됩니다.

```
aft-backend-[account_id]-primary-region
```

또한 AFT는 재해 복구를 위해 Terraform 상태 구성을 다른 AWS 리전버킷에 복제하는 Amazon S3 버킷을 생성합니다. 이 버킷은 다음 형식으로 이름이 지정됩니다.

```
aft-backend-[account_id]-secondary-region
```

이러한 Terraform 상태 Amazon S3 버킷에서 삭제 기능에 대해 멀티 팩터 인증 (MFA) 을 활성화하는 것이 좋습니다. Terraform 커뮤니티 에디션에 대한 자세한 내용은 Terraform 설명서를 참조하십시오.

Terraform OSS를 배포판으로 선택하려면 다음 입력 매개변수를 제공하십시오.

```
terraform_distribution = "oss"
```

테라폼 클라우드

Terraform Cloud를 배포판으로 선택하면 AFT는 Terraform Cloud 조직에 다음 구성 요소에 대한 작업 공간을 생성하여 API 기반 워크플로를 시작합니다.

- 계정 요청
- AFT가 제공하는 계정에 대한 AFT 사용자 지정
- AFT가 프로비저닝하는 계정의 계정 사용자 지정
- AFT가 프로비저닝하는 계정의 글로벌 사용자 지정

Terraform Cloud는 결과 Terraform 상태 구성을 관리합니다.

Terraform Cloud를 배포판으로 선택하는 경우 다음 입력 매개변수를 제공하십시오.

- `terraform_distribution = "tfc"`
- `terraform_token`— 이 파라미터는 테라폼 클라우드 토큰의 값을 포함합니다. AFT는 를 민감한 것으로 표시하고 값을 AFT 관리 계정의 SSM 파라미터 저장소에 보안 문자열로 저장합니다. 회사

의 보안 정책 및 규정 준수 지침에 따라 Terraform 토큰의 값을 주기적으로 교체하는 것이 좋습니다. Terraform 토큰은 사용자 또는 팀 수준 API 토큰이어야 합니다. 조직 토큰은 지원되지 않습니다.

- `terraform_org_name`— 이 매개변수에는 Terraform Cloud 조직의 이름이 포함됩니다.

> **Note**
>
> 단일 Terraform Cloud 조직에서의 다중 AFT 배포는 지원되지 않습니다.

Terraform Cloud를 설정하는 방법에 대한 자세한 내용은 Terraform 설명서를 참조하십시오.

테라폼 엔터프라이즈

Terraform Enterprise를 배포판으로 선택하면 AFT는 Terraform Enterprise 조직에 다음 구성 요소에 대한 작업 공간을 생성하고 결과 Terraform 실행에 대한 API 기반 워크플로를 트리거합니다.

- 계정 요청
- AFT에서 제공하는 계정에 대한 AFT 계정 프로비저닝 사용자 지정
- AFT에서 제공하는 계정의 계정 사용자 지정
- AFT에서 제공하는 계정의 글로벌 사용자 지정

결과 Terraform 상태 구성은 Terraform Enterprise 설정에 의해 관리됩니다.

Terraform Enterprise를 배포판으로 선택하려면 다음 입력 매개변수를 제공하십시오.

- `terraform_distribution = "tfe"`
- `terraform_token`— 이 파라미터는 테라폼 엔터프라이즈 토큰의 값을 포함합니다. AFT는 해당 값을 민감한 것으로 표시하고 AFT 관리 계정의 SSM 파라미터 저장소에 보안 문자열로 저장합니다. 회사의 보안 정책 및 규정 준수 지침에 따라 Terraform 토큰의 값을 주기적으로 교체하는 것이 좋습니다.
- `terraform_org_name`— 이 매개변수에는 Terraform Enterprise 조직의 이름이 포함됩니다.
- `terraform_api_endpoint`— 이 파라미터는 테라폼 엔터프라이즈 환경의 URL을 포함합니다. 이 매개 변수의 값은 다음 형식이어야 합니다.

```
https://{fqdn}/api/v2/
```

Terraform Enterprise를 설정하는 방법에 대한 자세한 내용은 Terraform 설명서를 참조하십시오.

AFT 버전을 확인하세요.

AWS SSM 파라미터 스토어 키를 쿼리하여 배포된 AFT 버전을 확인할 수 있습니다.

```
/aft/config/aft/version
```

레지스트리 방법을 사용하는 경우 버전을 고정할 수 있습니다.

```
module "control_tower_account_factory" {
  source  = "aws-ia/control_tower_account_factory/aws"
  version = "1.3.2"
  # insert the 6 required variables here
}
```

AFT 리포지토리에서 AFT 버전에 대한 자세한 정보를 볼 수 있습니다.

AFT 버전 업데이트

배포된 AFT 버전을 `main` 리포지토리 브랜치에서 가져와서 업데이트할 수 있습니다.

```
terraform get -update
```

가져오기가 완료되면 Terraform 계획을 다시 실행하거나 apply를 실행하여 AFT 인프라를 최신 변경 사항으로 업데이트할 수 있습니다.

기능 옵션 활성화

AFT는 모범 사례를 기반으로 기능 옵션을 제공합니다. AFT 배포 중에 기능 플래그를 사용하여 이러한 기능을 옵트인할 수 있습니다. AFT 입력 구성 매개변수에 AFT에 새 계정을 프로비저닝하세요 대한 자세한 내용은 를 참조하십시오.

이러한 기능은 기본적으로 활성화되지 않습니다. 환경에서 각 기능을 명시적으로 활성화해야 합니다.

주제

- AWS CloudTrail 데이터 이벤트
- AWS 엔터프라이즈 지원 플랜
- AWS 기본 VPC 삭제

AWS CloudTrail 데이터 이벤트

활성화되면 AWS CloudTrail 데이터 이벤트 옵션이 이러한 기능을 구성합니다.

- 다음과 같은 경우 AWS Control Tower 관리 계정에 조직 트레일을 생성합니다. CloudTrail
- Amazon S3 및 Lambda 데이터 이벤트에 대한 로깅을 활성화합니다.
- 암호화를 통해 모든 CloudTrail 데이터 이벤트를 암호화하여 AWS Control Tower Log Archive 계정의 `aws-aft-logs-*` S3 버킷으로 AWS KMS 내보냅니다.
- 로그 파일 검증 설정을 활성화합니다.

이 옵션을 활성화하려면 AFT 배포 입력 구성에서 다음 기능 플래그를 True로 설정하십시오.

```
aft_feature_cloudtrail_data_events
```

사전 조건

이 기능 옵션을 활성화하기 전에 조직에서 신뢰할 수 있는 AWS CloudTrail 액세스가 활성화되어 있는지 확인하세요.

신뢰할 수 있는 액세스의 상태를 확인하려면 CloudTrail :

1. AWS Organizations 콘솔로 이동합니다.
2. 서비스 > 를 선택합니다 CloudTrail.
3. 그런 다음 필요한 경우 오른쪽 상단에서 신뢰할 수 있는 액세스 활성화를 선택합니다.

AWS CloudTrail 콘솔 사용을 권장하는 경고 메시지가 표시될 수 있지만 이 경우에는 경고를 무시하세요. AFT는 신뢰할 수 있는 액세스를 허용한 후 이 기능 옵션을 활성화하는 과정의 일환으로 트레일을 생성합니다. 신뢰할 수 있는 액세스가 활성화되지 않은 경우 AFT가 데이터 이벤트에 대한 트레일을 만들려고 할 때 오류 메시지가 표시됩니다.

> **Note**
>
> 이 설정은 조직 수준에서 작동합니다. 이 설정을 활성화하면 AFT로 관리되는지 여부에 관계없이 에 AWS Organizations있는 모든 계정에 영향을 줍니다. 활성화 당시 AWS Control Tower Log Archive 계정의 모든 버킷은 Amazon S3 데이터 이벤트에서 제외됩니다. 자세한 내용은 AWS CloudTrail 사용 설명서를 참조하십시오. CloudTrail

AWS 엔터프라이즈 지원 플랜

이 옵션을 활성화하면 AFT 파이프라인은 AFT에서 프로비저닝한 계정에 대해 AWS Enterprise Support 플랜을 활성화합니다.

AWS 계정에는 기본적으로 AWS Basic Support 플랜이 활성화되어 있습니다. AFT는 AFT가 제공하는 계정에 대해 기업 지원 수준에 자동 등록을 제공합니다. 프로비저닝 프로세스에서 해당 계정에 대한 지원 티켓을 열고 AWS Enterprise Support 플랜에 추가하도록 요청합니다.

Enterprise Support 옵션을 활성화하려면 AFT 배포 입력 구성에서 다음 기능 플래그를 True로 설정합니다.

```
aft_feature_enterprise_support=false
```

AWS Support Plan에 대한 자세한 내용은 AWS 지원 플랜 비교를 참조하십시오.

> **Note**
>
> 이 기능을 사용하려면 지급자 계정을 Enterprise Support 플랜에 등록해야 합니다.

AWS 기본 VPC 삭제

이 옵션을 활성화하면 AFT는 관리 계정의 모든 AWS 기본 VPC를 삭제하며 AWS 리전, 관리 계정에 AWS Control Tower 리소스를 배포하지 않았더라도 모든 기본 VPC를 삭제합니다. AWS 리전

AFT는 AFT가 프로비저닝하는 모든 AWS Control Tower 계정 또는 AFT를 통해 AWS Control Tower에 등록한 기존 AWS 계정의 AWS 기본 VPC를 자동으로 삭제하지 않습니다.

기본적으로 각 AWS AWS 리전계정에 VPC가 설정되어 새 계정이 생성됩니다. 기업에는 VPC를 만드는 표준 관행이 있을 수 있습니다. 이 경우 AWS 기본 VPC를 삭제하고 활성화하지 않도록 해야 하며, 특히 AFT 관리 계정의 경우 더욱 그렇습니다.

이 옵션을 활성화하려면 AFT 배포 입력 구성에서 다음 기능 플래그를 True로 설정하십시오.

```
aft_feature_delete_default_vpcs_enabled
```

기본 VPC에 대한 자세한 내용은 기본 VPC 및 기본 서브넷을 참조하십시오.

테라폼용 AWS Control Tower Account Factory에 대한 리소스 고려 사항

Terraform용 AWS Control Tower Account Factory를 사용하여 랜딩 존을 설정하면 계정 AWS 내에 여러 유형의 AWS 리소스가 생성됩니다.

리소스 검색

- 태그를 사용하여 가장 업데이트된 AFT 리소스 목록을 검색할 수 있습니다. 검색에 사용되는 키-값 쌍은 다음과 같습니다.

```
Key: managed_by | Value: AFT
```

- 태그를 지원하지 않는 구성 요소 서비스의 경우 리소스 `aft` 이름에서 를 검색하여 리소스를 찾을 수 있습니다.

처음 생성된 리소스 테이블 (계정별)

테라폼 관리 계정을 위한 AWS Control Tower 어카운트 팩토리

AWS service	리소스 유형	리소스 이름
AWS Identity and Access Management	역할	AWSAFTAdministrator AWSAFTExecution AWSAFTService aws-ct-aft-*
AWS Identity and Access Management	정책	aws-ct-aft-*
CodeCommit	리포지토리	aws-ct-aft-*
CodeBuild	빌드 프로젝트	aws-ct-aft-*
코드 파이프라인	파이프라인	*-baseline-*
Amazon S3	버킷	*-aws-ct-aft-* aws-ct-aft-*

AWS service	리소스 유형	리소스 이름
Lambda	함수	aws-ct-aft-*
Lambda	계층	aws-ct-aft-common-layer
DynamoDB	표	aws-ct-aft-request aws-ct-aft-request-audit aws-ct-aft-request-metadata aws-ct-aft-controltower-events
Step Functions	스테이트 머신	aws-ct-aft-prebaseline aws-ct-aft-prebaseline-customizations aws-ct-aft-trigger-baseline aws-ct-aft-features
VPC	VPC	aws-ct-aft-vpc
Amazon SNS	주제	aws-ct-aft-notifications aws-ct-aft-failure-notifications
아마존 EventBridge	이벤트 버스	aws-ct-aft-events-from-ct-management
아마존 EventBridge	이벤트 규칙	aws-ct-aft-capture-ct-events aws-ct-aft-lambda-account-request-processor
키 관리 서비스 (KMS)	고객 관리형 키	*-aws-ct-aft-* aws-ct-aft-*

AWS service	리소스 유형	리소스 이름
AWS Systems Manager	파라미터 스토어	/aws-ct-aft/account/* /aws/ct-aft/config/*
Amazon SQS	대기열	aws-ct-aft-account-request.fifo aws-ct-aft-account-request-dlg.fifo
CloudWatch	로그 그룹	/aws/*/aws-ct-aft-* aws-ct-aft-*
AWS 지원 센터 (선택 사항)	Support 플랜	Enterprise

AWS 테라폼용 AWS Control Tower Account Factory를 통해 프로비저닝된 계정

AWS service	리소스 유형	리소스 이름
AWS Identity and Access Management	역할	AWSAFTExecution
AWS 지원 센터 (선택 사항)	Support 플랜	Enterprise

AWS Control 타워 관리 계정

AWS service	리소스 유형	리소스 이름
AWS Identity and Access Management	역할	AWSAFTExecutionRole AWSAFTExecution aws-ct-aft-controltower-events-rule
AWS Systems Manager	파라미터 스토어	/aws-ct-aft/account/aws-ct-aft-management/account-id

AWS service	리소스 유형	리소스 이름
AWS Organizations (선택 사항)	서비스 제어 정책	aws-ct-aft-protect-resources
CloudTrail (선택 사항)	추적	aws-ct-aft-BaselineCloudTrail
AWS 지원 센터 (선택 사항)	Support 플랜	Enterprise

AWS Control 타워 로그 아카이브 계정

AWS service	리소스 유형	리소스 이름
AWS Identity and Access Management	역할	AWSAFTExecutionRole AWSAFTExecution aws-ct-aft-cloudtrail-data-events-role
키 관리 서비스 (KMS)	고객 관리형 키	*-aws-ct-aft-kms-gd-findings
Amazon S3	버킷	*-aws-ct-aft-logs* aws-ct-aft-s3-access-logs*
AWS 지원 센터 (선택 사항)	Support 플랜	Enterprise

AWS Control 타워 감사 계정

AWS service	리소스 유형	리소스 이름
AWS Identity and Access Management	역할	AWSAFTExecutionRole AWSAFTExecution
AWS 지원 센터 (선택 사항)	Support 플랜	Enterprise

필수 역할

일반적으로 역할과 정책은 IAM (ID 및 액세스 관리) 의 AWS일부입니다. 자세한 내용은 AWS IAM 사용 설명서를 참조하십시오.

AFT는 AFT 파이프라인 운영을 지원하기 위해 AFT 관리 및 AWS Control Tower 관리 계정에 여러 IAM 역할 및 정책을 생성합니다. 이러한 역할은 최소 권한 액세스 모델을 기반으로 생성되며, 이 모델은 각 역할 및 정책에 필요한 최소 작업 및 리소스 세트로 권한을 제한합니다. 식별을 위해 이러한 역할과 정책에는 AWS 태그 `key:value` 쌍이 할당됩니다. `managed_by:AFT`

이러한 IAM 역할 외에도 AFT는 다음과 같은 세 가지 필수 역할을 생성합니다.

- 역할 `AWSAFTAdmin`
- `AWSAFTExecution`역할
- `AWSAFTService`역할

이러한 역할은 다음 섹션에 설명되어 있습니다.

AWSAFTAdmin 역할, 설명

AFT를 배포하면 AFT 관리 계정에 `AWSAFTAdmin` 역할이 생성됩니다. 이 역할을 통해 AFT 파이프라인은 AWS Control Tower 및 AFT 프로비저닝 계정에서 `AWSAFTExecution` 역할을 맡아 계정 프로비저닝 및 사용자 지정과 관련된 작업을 수행할 수 있습니다.

역할에 연결된 인라인 정책 (JSON 아티팩트) 은 다음과 같습니다. `AWSAFTAdmin`

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "sts:AssumeRole",
            "Resource": [
                "arn:aws:iam::*:role/AWSAFTExecution",
                "arn:aws:iam::*:role/AWSAFTService"
            ]
        }
    ]
}
```

다음 JSON 아티팩트는 역할에 대한 신뢰 관계를 보여줍니다. AWSAFTAdmin 플레이스홀더 012345678901 번호는 AFT 관리 계정 ID 번호로 대체됩니다.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::012345678901:root"
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

AWSAFTExecution 역할, 설명

AFT를 배포하면 AFT 관리 및 AWS Control Tower 관리 계정에 AWSAFTExecution 역할이 생성됩니다. 나중에 AFT 파이프라인은 AFT 계정 프로비저닝 단계에서 각 AFT 프로비저닝 계정에 AWSAFTExecution 역할을 생성합니다.

AFT는 처음에 AWSControlTowerExecution 역할을 활용하여 지정된 계정에서 AWSAFTExecution 역할을 생성합니다. 이 AWSAFTExecution 역할을 통해 AFT 파이프라인은 AFT 프레임워크의 프로비저닝 및 프로비저닝 사용자 지정 단계 (AFT 프로비저닝 계정 및 공유 계정) 에서 수행되는 단계를 실행할 수 있습니다.

> 고유한 역할을 통해 범위를 제한할 수 있습니다.
>
> 가장 좋은 방법은 사용자 지정 권한을 리소스를 처음 배포할 때 허용된 권한과 분리하여 유지하는 것입니다. AWSAFTService역할은 계정 프로비저닝을 위한 것이고 AWSAFTExecution 역할은 계정 사용자 지정을 위한 것임을 기억하십시오. 이러한 분리로 인해 파이프라인의 각 단계에서 허용되는 권한 범위가 제한됩니다. 공유 계정에는 청구 세부 정보 또는 사용자 정보와 같은 민감한 정보가 포함될 수 있으므로 AWS Control Tower 공유 계정을 사용자 지정하는 경우 이러한 구분이 특히 중요합니다.

AWSAFTExecution역할 권한: AdministratorAccess— AWS 관리형 정책

다음 JSON 아티팩트는 역할에 연결된 IAM 정책 (신뢰 관계) 을 보여줍니다. AWSAFTExecution 플레이스홀더 012345678901 번호는 AFT 관리 계정 ID 번호로 대체됩니다.

에 대한 신뢰 정책 AWSAFTExecution

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::012345678901:role/AWSAFTAdmin"
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

AWSAFTService 역할, 설명

이 AWSAFTService 역할은 공유 계정 및 관리 계정을 포함하여 등록 및 관리되는 모든 계정에 AFT 리소스를 배포합니다. 이전에는 리소스가 역할로만 배포되었습니다. AWSAFTExecution

AWSAFTService역할은 서비스 인프라에서 프로비저닝 단계에서 리소스를 배포하는 데 사용하기 위한 것이고, AWSAFTExecution 역할은 사용자 지정을 배포하는 데만 사용하기 위한 것입니다. 이러한 방식으로 역할을 수임하면 각 단계에서 보다 세분화된 액세스 제어를 유지할 수 있습니다.

AWSAFTService역할 권한: AdministratorAccess— AWS 관리형 정책

다음 JSON 아티팩트는 역할에 연결된 IAM 정책 (신뢰 관계) 을 보여줍니다. AWSAFTService 플레이스홀더 012345678901 번호는 AFT 관리 계정 ID 번호로 대체됩니다.

에 대한 신뢰 정책 AWSAFTService

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::012345678901:role/AWSAFTAdmin"
      },
      "Action": "sts:AssumeRole"
```

```
    }
  ]
}
```

컴포넌트 서비스

AFT를 배포하면 이러한 각 AWS 서비스의 구성 요소가 AWS 환경에 추가됩니다.

- AWS 컨트롤 타워 — AFT는 AWS 컨트롤 타워 관리 계정의 AWS 컨트롤 타워 어카운트 팩토리를 사용하여 계정을 프로비저닝합니다.
- Amazon DynamoDB — AFT는 계정 요청, 계정 업데이트의 감사 기록, 계정 메타데이터 및 AWS Control Tower 수명 주기 이벤트를 저장하는 AFT 관리 계정에 Amazon DynamoDB 테이블을 생성합니다. 또한 AFT는 DynamoDB Lambda 트리거를 생성하여 AFT 계정 프로비저닝 워크플로 시작과 같은 다운스트림 프로세스를 시작합니다.
- Amazon 심플 스토리지 서비스 — AFT는 AFT 관리 계정과 AWS 컨트롤 타워 로그 아카이브 계정에 Amazon Simple Storage Service (S3) 버킷을 생성합니다. 이 계정에는 AFT 파이프라인에 필요한 AWS 서비스에서 생성된 로그를 저장합니다. 또한 AFT는 기본 및 보조 AWS 리전에 Terraform 백엔드 S3 버킷을 생성하여 AFT 파이프라인 워크플로 중에 생성된 Terraform 상태를 저장합니다.
- Amazon 단순 알림 서비스 — AFT는 AFT 관리 계정에 Amazon Simple Notification Service (SNS) 주제를 생성합니다. 이 주제는 모든 AFT 계정 요청을 처리한 후 성공 및 실패 알림을 저장합니다. 선택한 프로토콜을 사용하여 이러한 메시지를 수신할 수 있습니다.
- 아마존 심플 큐잉 서비스 — AFT는 AFT 관리 계정에 아마존 심플 큐잉 서비스 (Amazon SQS) FIFO 대기열을 생성합니다. 대기열을 사용하면 여러 계정 요청을 병렬로 제출할 수 있지만, 한 번에 하나의 요청을 AWS Control Tower Account Factory로 전송하여 순차적으로 처리합니다.
- AWS CodeBuild — AFT는 AFT 관리 계정에 AWS CodeBuild 빌드 프로젝트를 생성하여 다양한 빌드 단계에서 AFT 소스 코드에 대한 Terraform 계획을 초기화, 컴파일, 테스트 및 적용합니다.
- AWS CodePipeline — AFT는 AFT 관리 계정에 AWS CodePipeline 파이프라인을 생성하여 선택한 지원 AWS CodeStar 연결 공급자와 AFT 소스 코드를 통합하고 CodeBuild AWS에서 빌드 작업을 트리거합니다.
- AWS Lambda — AFT는 계정 요청, AFT 계정 프로비저닝 및 계정 사용자 지정 프로세스 중에 단계를 수행하기 위해 AFT 관리 계정에 AWS Lambda 함수 및 계층을 생성합니다.
- AWS Systems Manager Parameter Store — AFT는 AFT 관리 계정에 AWS Systems Manager Parameter Store를 설정하여 AFT 파이프라인 프로세스에 필요한 구성 파라미터를 저장합니다.
- Amazon CloudWatch — AFT는 AFT 파이프라인에서 사용하는 AWS 서비스에서 생성된 로그를 저장하기 위해 AFT 관리 계정에 Amazon CloudWatch 로그 그룹을 생성합니다. CloudWatch 로그 보존 기간은 로 설정되어 `Never Expire` 있습니다.

- Amazon VPC — AFT는 Amazon VPC (가상 사설 클라우드) 를 생성하여 AFT 관리 계정의 서비스와 리소스를 별도의 네트워킹 환경으로 분리하여 보안을 강화합니다.
- AWS KMS — AFT는 AFT 관리 계정과 AWS 컨트롤 타워 로그 아카이브 계정에서 AWS KMS (키 관리 서비스) 를 사용합니다. AFT는 Terraform 상태, DynamoDB 테이블에 저장된 데이터 및 SNS 주제를 암호화하는 키를 생성합니다. 이러한 로그와 아티팩트는 AFT에서 AWS 리소스 및 서비스를 배포할 때 생성됩니다. AFT에서 생성한 KMS 키는 기본적으로 연간 순환이 활성화되어 있습니다.
- AWS ID 및 액세스 관리 (IAM) — AFT는 권장되는 최소 권한 모델을 따릅니다. 필요에 따라 AFT 관리 계정, AWS Control Tower 계정, AFT 프로비저닝 계정에 AWS Identity and Access Management (IAM) 역할과 정책을 생성하여 AFT 파이프라인 워크플로 중에 필요한 작업을 수행합니다.
- AWS Step Functions — AFT는 AFT 관리 계정에 AWS Step Functions 상태 머신을 생성합니다. 이러한 상태 머신은 AFT 계정 프로비저닝 프레임워크 및 사용자 지정을 위한 프로세스와 단계를 오케스트레이션하고 자동화합니다.
- Amazon EventBridge — AFT는 AFT 및 AWS Control Tower 관리 계정에서 Amazon EventBridge 이벤트 버스를 생성하여 AWS Control Tower 수명 주기 이벤트를 캡처하여 AFT 관리 계정의 DynamoDB 테이블에 장기간 저장합니다. AFT는 AFT 관리 계정과 AWS Control Tower 관리 계정에 AWS CloudWatch 이벤트 규칙을 생성하여 AFT 파이프라인 워크플로를 실행하는 동안 필요한 여러 단계를 트리거합니다.
- AWS CloudTrail (선택 사항) — 이 기능을 활성화하면 AFT는 Amazon S3 버킷 및 AWS Lambda 함수에 대한 데이터 이벤트를 로깅하기 위해 AWS 컨트롤 타워 관리 계정에 AWS CloudTrail 조직 트레일을 생성합니다. AFT는 이러한 로그를 AWS Control Tower 로그 아카이브 계정의 중앙 S3 버킷으로 전송합니다.
- AWS Support (선택 사항) — 이 기능을 활성화하면 AFT는 AFT에서 프로비저닝한 계정에 대해 AWS 엔터프라이즈 지원 플랜을 활성화합니다. 기본적으로 AWS 계정은 AWS Basic Support 플랜이 활성화된 상태에서 생성됩니다.

AFT 계정 프로비저닝 파이프라인

파이프라인의 계정 프로비저닝 단계가 완료된 후에도 AFT 프레임워크는 계속됩니다. 단계가 시작되기 전에 일련의 단계를 자동으로 실행하여 새로 프로비저닝된 계정에 세부 정보가 있는지 확인합니다. 계정 사용자 지정

AFT 파이프라인이 실행되는 다음 단계는 다음과 같습니다.

1. 계정 요청 입력을 검증합니다.
2. 제공된 계정에 대한 정보 (예: 계정 ID) 를 검색합니다.

3. 계정 메타데이터를 AFT 관리 계정의 DynamoDB 테이블에 저장합니다.
4. 새로 프로비저닝된 AWSAFTExecution계정에 IAM 역할을 생성합니다. AFT는 이 역할을 맡아 계정 사용자 지정 단계를 수행합니다. 이 역할은 어카운트 팩토리 포트폴리오에 대한 액세스 권한을 부여하기 때문입니다.
5. 계정 요청 입력 매개 변수의 일부로 제공한 계정 태그를 적용합니다.
6. AFT 배포 시 선택한 AFT 기능 옵션을 적용합니다.
7. 제공한 AFT 계정 프로비저닝 사용자 정의를 적용합니다. 다음 섹션에서는 `git` 리포지토리에서 AWS Step Functions 상태 머신을 사용하여 이러한 사용자 지정을 설정하는 방법에 대해 자세히 설명합니다. 이 단계를 계정 프로비저닝 프레임워크 단계라고도 합니다. 이는 핵심 프로비저닝 프로세스의 일부이지만, 다음 단계에서 계정에 추가 사용자 지정을 추가하기 전에 이전에 계정 프로비저닝 워크플로의 일부로 사용자 지정 기능을 제공하는 프레임워크를 설정했습니다.
8. 프로비저닝된 각 계정에 대해 AFT 관리 계정이 AWS CodePipeline 생성되며, 이 계정을 실행하여 (다음, 글로벌) 단계를 수행합니다. 계정 사용자 지정
9. 프로비저닝 (및 대상) 된 각 계정에 대해 계정 사용자 지정 파이프라인을 호출합니다.
10. 성공 또는 실패 알림을 SNS 주제로 전송하며, 이 주제에서 메시지를 검색할 수 있습니다.

스테이트 머신을 사용하여 계정 프로비저닝 프레임워크 사용자 지정을 설정합니다.

계정을 프로비저닝하기 전에 Terraform이 아닌 사용자 지정 통합을 설정하면 이러한 사용자 지정이 AFT 계정 프로비저닝 워크플로에 포함됩니다. 예를 들어, AFT에서 생성한 모든 계정이 보안 표준과 같은 조직의 표준 및 정책을 준수하도록 특정 사용자 지정을 요구할 수 있으며, 추가 사용자 지정 전에 이러한 표준을 계정에 추가할 수 있습니다. 이러한 계정 공급 프레임워크 사용자 지정은 다음 글로벌 계정 사용자 지정 단계가 시작되기 전에 프로비전된 모든 계정에 구현됩니다.

> **Note**
>
> 이 섹션에 설명된 AFT 기능은 AWS Step Functions의 기능을 이해하는 고급 사용자를 대상으로 합니다. 대안으로, 계정 사용자 지정 단계에서 글로벌 도우미와 함께 작업하는 것이 좋습니다.

AFT 계정 프로비저닝 프레임워크는 사용자가 정의한 AWS Step Functions 상태 머신을 호출하여 사용자 지정을 구현합니다. 가능한 스테이트 머신 통합에 대해 자세히 알아보려면 AWS Step Functions 설명서를 참조하십시오.

다음은 몇 가지 일반적인 통합입니다.

- AWS Lambda는 사용자가 선택한 언어로 함수를 제공합니다.
- 도커 컨테이너를 사용하는 AWS ECS 또는 AWS Fargate 작업
- AWS 또는 온프레미스에서 호스팅되는 사용자 지정 작업자를 사용한 AWS Step Functions 활동
- Amazon SNS 또는 SQS 통합

AWS Step Functions 상태 머신이 정의되지 않은 경우 스테이지는 작업 없이 통과합니다. AFT 계정 프로비저닝 사용자 지정 상태 머신을 생성하려면 의 지침을 따르십시오. AFT 계정 프로비저닝 사용자 지정 상태 머신을 생성하세요. 사용자 지정을 추가하기 전에 사전 요구 사항을 마련했는지 확인하세요.

이러한 유형의 통합은 AWS Control Tower의 일부가 아니며 AFT 계정 사용자 지정의 글로벌 사전 API 단계에서 추가할 수 없습니다. 대신 AFT 파이프라인을 사용하면 프로비저닝 프로세스의 일부로 이러한 사용자 지정을 설정할 수 있으며, 이러한 사용자 지정은 프로비저닝 워크플로에서 실행됩니다. 다음 섹션에 설명된 대로 AFT 계정 프로비저닝 단계를 시작하기 전에 미리 상태 머신을 만들어 이러한 사용자 지정을 구현해야 합니다.

스테이트 머신을 생성하기 위한 사전 요구 사항

- 완전히 배포된 AFT. AFT 배포에 테라폼용 AWS Control Tower 어카운트 팩토리 (AFT) 배포 대한 자세한 내용은 을 참조하십시오.
- AFT 계정 프로비저닝 사용자 지정을 위한 `git` 리포지토리를 환경에 설정하십시오. 자세한 내용은 배포 후 단계를 참조하세요.

AFT 계정 프로비저닝 사용자 지정 상태 머신을 생성하세요.

1단계: 스테이트 머신 정의 수정

예제 `customizations.asl.json` 스테이트 머신 정의를 수정합니다. 이 예제는 배포 후 단계에서 AFT 계정 프로비저닝 사용자 지정을 저장하기 위해 설정한 `git` 리포지토리에서 사용할 수 있습니다. 상태 머신 정의에 대한 자세한 내용은 AWS Step Functions 개발자 안내서를 참조하십시오.

2단계: 해당 Terraform 구성 포함

사용자 지정 통합을 위한 상태 머신 정의와 함께 동일한 `git` 리포지토리에 `.tf` 확장자가 있는 Terraform 파일을 포함하세요. 예를 들어, 상태 머신 작업 정의에서 Lambda 함수를 호출하기로 선택한 경우 해당 파일을 동일한 디렉터리에 포함시킬 `lambda.tf` 수 있습니다. 사용자 지정 구성에 필요한 IAM 역할 및 권한을 포함해야 합니다.

적절한 입력을 제공하면 AFT 파이프라인이 자동으로 스테이트 머신을 호출하고 AFT 계정 프로비저닝 프레임워크 단계의 일부로 사용자 지정을 배포합니다.

AFT 계정 프로비저닝 프레임워크 및 사용자 지정을 다시 시작하려면

AFT는 AFT 파이프라인을 통해 벤딩되는 모든 계정에 대해 계정 프로비저닝 프레임워크 및 사용자 지정 단계를 실행합니다. 계정 프로비저닝 사용자 지정을 다시 시작하려면 다음 두 가지 방법 중 하나를 사용할 수 있습니다.

1. 계정 요청 리포지토리에서 기존 계정을 변경하세요.
2. AFT에 새 계정을 프로비저닝하세요.

계정 사용자 지정

AFT는 프로비저닝된 계정에 표준 또는 사용자 지정 구성을 배포할 수 있습니다. AFT 관리 계정에서 AFT는 계정당 하나의 파이프라인을 제공합니다. 이 파이프라인을 사용하면 모든 계정, 계정 집합 또는 개별 계정에서 사용자 지정을 구현할 수 있습니다. Python 스크립트, bash 스크립트 및 Terraform 구성을 실행하거나 계정 사용자 지정 단계의 일부로 AWS CLI와 상호 작용할 수 있습니다.

개요

글로벌 사용자 지정을 저장하거나 계정 사용자 지정을 저장하는 `git` 리포지토리에서 사용자 지정을 지정한 후 AFT 파이프라인에 의해 계정 사용자 지정 단계가 자동으로 완료됩니다. 계정을 소급하여 사용자 지정하려면 을 참조하십시오. 사용자 지정 항목 다시 호출

글로벌 사용자 지정 (선택 사항)

AFT에서 제공하는 모든 계정에 특정 사용자 지정을 적용하도록 선택할 수 있습니다. 예를 들어 특정 IAM 역할을 생성하거나 모든 계정에 사용자 지정 컨트롤을 배포해야 하는 경우 AFT 파이프라인의 글로벌 사용자 지정 단계를 통해 자동으로 배포할 수 있습니다.

계정 사용자 지정 (선택 사항)

다른 AFT 프로비저닝 계정과 다르게 개별 계정 또는 계정 세트를 사용자 지정하려면 AFT 파이프라인의 계정 사용자 지정 부분을 활용하여 계정별 구성을 구현할 수 있습니다. 예를 들어 특정 계정에만 인터넷 게이트웨이 액세스 권한이 필요할 수 있습니다.

사용자 지정 사전 요구 사항

계정을 사용자 지정하기 전에 이러한 사전 요구 사항이 제대로 갖추어져 있는지 확인하세요.

- 완전히 배포된 AFT. 배포 방법에 대한 자세한 내용은 을 참조하십시오테라폼용 AWS Control Tower Account Factory를 구성하고 실행하십시오..
- 사용자 환경의 글로벌 사용자 지정 및 계정 사용자 지정을 위해 미리 채워진 `git` 리포지토리. 자세한 내용은 3단계: 각 리포지토리 채우기를 참조하십시오. 배포 후 단계

글로벌 사용자 지정 적용

글로벌 사용자 지정을 적용하려면 선택한 저장소에 특정 폴더 구조를 푸시해야 합니다.

- 사용자 정의 구성이 Python 프로그램 또는 스크립트 형태인 경우 저장소의 api_helpers/python 폴더에 배치하십시오.
- 사용자 지정 구성이 Bash 스크립트 형식인 경우 저장소의 api_helpers 폴더에 배치하십시오.
- 사용자 지정 구성이 Terraform 형식인 경우 저장소의 terraform 폴더 아래에 배치하십시오.
- 사용자 지정 구성 생성에 대한 자세한 내용은 글로벌 사용자 지정 README 파일을 참조하십시오.

> **Note**
>
> 글로벌 커스터마이징은 AFT 파이프라인의 AFT 계정 프로비저닝 프레임워크 단계 이후에 자동으로 적용됩니다.

계정 사용자 지정 적용

선택한 저장소에 특정 폴더 구조를 푸시하여 계정 사용자 지정을 적용할 수 있습니다. 계정 사용자 지정은 AFT 파이프라인에서 그리고 글로벌 사용자 지정 단계 이후에 자동으로 적용됩니다. 또한 계정 사용자 지정 리포지토리에서 다양한 계정 사용자 지정을 포함하는 여러 폴더를 만들 수 있습니다. 필요한 각 계정 사용자 지정에 대해 다음 단계를 사용하십시오.

계정 사용자 지정을 적용하려면

1. 1단계: 계정 사용자 지정을 위한 폴더 만들기

   선택한 저장소에서 AFT가 제공하는 `ACCOUNT_TEMPLATE` 폴더를 새 폴더에 복사합니다. 새 폴더의 이름은 계정 요청에 입력한 이름과 일치해야 합니다. `account_customizations_name`
2. 특정 계정 사용자 지정 폴더에 구성을 추가합니다.

   구성 형식에 따라 계정 사용자 지정 폴더에 구성을 추가할 수 있습니다.

- 사용자 정의 구성이 Python 프로그램 또는 스크립트 형태인 경우 저장소에 있는 ***[account_customations_name] /api_helpers/python*** 폴더에 배치하십시오.
- ***### ## ### Bash #### ### ## #### ## [account_customations_name] / api_helpers ### ######.***
- ***### ## ### Terraform ### ## ###### ## [account_customations_name] / terraform ### ######.***

사용자 지정 구성 생성에 대한 자세한 내용은 계정 사용자 지정 README 파일을 참조하십시오.

3. 계정 요청 파일의 특정 **account_customizations_name** 매개변수를 참조하십시오.

   AFT 계정 요청 파일에는 입력 매개변수가 포함되어 account_customizations_name 있습니다. 계정 사용자 지정 이름을 이 매개변수의 값으로 입력합니다.

> **Note**
>
> 사용자 환경의 계정에 대해 여러 계정 요청을 제출할 수 있습니다. 다르거나 유사한 계정 사용자 지정을 적용하려면 계정 요청의 account_customizations_name 입력 매개변수를 사용하여 계정 사용자 지정을 지정하십시오. 자세한 내용은 복수 계정 요청 제출을 참조하십시오.

사용자 지정 항목 다시 호출

AFT는 AFT 파이프라인에서 사용자 지정을 다시 호출하는 방법을 제공합니다. 이 방법은 새 사용자 지정 단계를 추가했거나 기존 사용자 지정을 변경할 때 유용합니다. 다시 호출하면 AFT는 사용자 지정 파이프라인을 시작하여 AFT 프로비저닝 계정을 변경합니다. event-source-based 재호출을 통해 개별 계정, 모든 계정, OU에 따른 계정 또는 태그에 따라 선택한 계정에 사용자 지정을 적용할 수 있습니다.

다음 세 단계에 따라 AFT에서 제공하는 계정의 사용자 지정을 다시 호출하십시오.

1단계: 글로벌 또는 계정 사용자 지정 리포지토리에 변경 내용 푸시 **git**

필요에 따라 글로벌 및 계정 사용자 지정을 업데이트하고 변경 사항을 리포지토리로 다시 푸시할 수 있습니다. git 이 시점에서는 아무 일도 일어나지 않습니다. 다음 두 단계에 설명된 대로 사용자 지정 파이프라인은 이벤트 소스에서 호출해야 합니다.

2단계: 사용자 지정 재호출을 위한 AWS Step 함수 실행 시작

AFT는 AFT 관리 `aft-invoke-customizations` 계정에서 호출되는 AWS Step 함수를 제공합니다. 이 함수의 목적은 AFT로 프로비저닝된 계정의 사용자 지정 파이프라인을 다시 호출하는 것입니다.

다음은 입력을 `aft-invoke-customizations` AWS Step Function에 전달하기 위해 생성할 수 있는 이벤트 스키마 (JSON 형식) 의 예입니다.

```
{
  "include": [
    {
      "type": "all"
    },
    {
      "type": "ous",
      "target_value": [ "ou1","ou2"]
    },
    {
      "type": "tags",
      "target_value": [ {"key1": "value1"}, {"key2": "value2"}]
    },
    {
      "type": "accounts",
      "target_value": [ "acc1_ID","acc2_ID"]
    }
  ],

  "exclude": [
    {
      "type": "ous",
      "target_value": [ "ou1","ou2"]
    },
    {
      "type": "tags",
      "target_value": [ {"key1": "value1"}, {"key2": "value2"}]
    },
    {
      "type": "accounts",
      "target_value": [ "acc1_ID","acc2_ID"]
    }
  ]
}
```

예제 이벤트 스키마는 재호출 프로세스에 포함하거나 제외할 계정을 선택할 수 있음을 보여줍니다. 조직 단위 (OU), 계정 태그 및 계정 ID별로 필터링할 수 있습니다. 필터를 적용하지 않고 명령문을 `"type":"all"` 포함하면 AFT에서 제공하는 모든 계정의 사용자 지정이 다시 호출됩니다.

> **Note**
>
> 사용 중인 AWS Control Tower 버전이 1.6.5 이상인 경우, 중첩된 OU를 `OU Name (ou-id-1234` 구문으로 타깃팅할 수 있습니다. 자세한 내용은 다음 주제를 참조하십시오. GitHub

이벤트 파라미터를 채우면 Step Functions가 실행되어 해당 사용자 지정을 호출합니다. AFT는 한 번에 최대 5개의 사용자 지정을 호출할 수 있습니다. Step Functions는 이벤트 기준과 일치하는 모든 계정이 완료될 때까지 기다렸다가 반복합니다.

3단계: AWS 단계 함수 출력을 모니터링하고 AWS가 CodePipeline 실행되는 모습을 관찰합니다.

- 결과 Step Function 출력에는 Step Function 입력 이벤트 소스와 일치하는 계정 ID가 포함됩니다.
- 개발자 CodePipeline 도구에서 AWS로 이동하여 계정 ID에 해당하는 사용자 지정 파이프라인을 확인하십시오.

AFT 계정 사용자 지정 요청 추적을 통한 문제 해결

대상 계정 및 사용자 지정 요청 ID가 포함된 AWS Lambda 방출 로그를 기반으로 하는 계정 사용자 지정 워크플로. AFT를 사용하면 대상 계정 또는 사용자 지정 요청 ID를 기준으로 사용자 지정 요청과 관련된 CloudWatch CloudWatch 로그를 필터링하는 데 사용할 수 있는 Logs Insights 쿼리를 제공하여 Amazon CloudWatch Logs로 사용자 지정 요청을 추적하고 문제를 해결할 수 있습니다. 자세한 내용은 Amazon CloudWatch Logs 사용 설명서의 Amazon Logs를 사용한 CloudWatch 로그 데이터 분석을 참조하십시오.

AFT용 CloudWatch 로그 인사이트를 사용하려면

1. https://console.aws.amazon.com/cloudwatch/ 에서 CloudWatch 콘솔을 엽니다.
2. 탐색 창에서 로그를 선택한 다음 로그 통계를 선택합니다.
3. 쿼리를 선택합니다.
4. 샘플 쿼리에서 Terraform용 Account Factory를 선택하고 다음 쿼리 중 하나를 선택합니다.
    - 계정 ID별 사용자 지정 로그

> **Note**
>
> *"YOUR-ACCOUNT-ID"# ## ##* ID로 바꿔야 합니다.

```
fields @timestamp, log_message.account_id as target_account_id,
 log_message.customization_request_id as customization_request_id,
 log_message.detail as detail, @logStream
| sort @timestamp desc
| filter log_message.account_id == "YOUR-ACCOUNT-ID" and @message like /
customization_request_id/
```

- 사용자 지정 요청 ID별 사용자 지정 로그

> **Note**
>
> *"### ## ## ID"# ### ## ## ID#* 바꿔야 합니다. 사용자 지정 요청 ID는 AFT 계정 프로비저닝 프레임워크 상태 머신의 출력에서 찾을 수 있습니다. AWS Step Functions AFT 계정 프로비저닝 프레임워크에 대한 자세한 내용은 AFT 계정 프로비저닝 파이프라인을 참조하십시오.

```
fields @timestamp, log_message.account_id as target_account_id,
 log_message.customization_request_id as customization_request_id,
 log_message.detail as detail, @logStream
| sort @timestamp desc
| filter log_message.customization_request_id == "YOUR-CUSTOMIZATION-REQUEST-ID"
```

5. 쿼리를 선택한 후 시간 간격을 선택한 다음 쿼리 실행을 선택합니다.

AFT의 소스 코드 버전 관리를 위한 대안

AFT는 기본적으로 소스 코드 버전 제어 시스템 (VCS) 에 AWS CodeCommit 사용하지만 비즈니스 요구 사항이나 기존 아키텍처를 CodeConnections충족하는 다른 시스템도 사용할 수 있습니다. AFT 배포 사전 요구 사항의 일부로 타사 VCS를 지정할 수 있습니다.

AFT는 다음과 같은 소스 코드 제어 대안을 지원합니다.

- GitHub
- GitHub 엔터프라이즈 서버
- BitBucket

AWS CodeCommit VCS로 선택하면 추가 단계가 필요하지 않습니다. 기본적으로 AFT는 사용자 환경에 기본 이름을 사용하여 필요한 `git` 리포지토리를 생성합니다. 그러나 필요에 따라 조직 표준을 준수하도록 기본 저장소 이름을 재정의할 수 있습니다. CodeCommit

AFT를 사용하여 대체 소스 코드 버전 제어 시스템 (사용자 지정 VCS) 을 설정하십시오.

AFT 배포를 위한 대체 소스 코드 버전 제어 시스템을 설정하려면 다음 단계를 따르십시오.

1단계: 지원되는 타사 버전 제어 시스템 (VCS) 에서 **`git`** 리포지토리를 생성합니다.

를 사용하지 AWS CodeCommit않는 경우 AFT가 지원되는 타사 VCS 공급자 환경에서 다음 항목에 대한 `git` 리포지토리를 생성해야 합니다.

- AFT 계정 요청. 샘플 코드를 사용할 수 있습니다. AFT 계정 요청에 대한 자세한 내용은 을 참조하십시오AFT에 새 계정을 프로비저닝하세요.
- AFT 계정 프로비저닝 사용자 지정. 샘플 코드를 사용할 수 있습니다. AFT 계정 프로비저닝 사용자 지정에 대한 자세한 내용은 을 참조하십시오. AFT 계정 프로비저닝 사용자 지정 상태 머신을 생성하세요.
- AFT 글로벌 커스터마이징. 샘플 코드를 사용할 수 있습니다. AFT 글로벌 커스터마이징에 대한 자세한 내용은 을 참조하십시오계정 사용자 지정.
- AFT 계정 사용자 지정. 샘플 코드를 사용할 수 있습니다. AFT 계정 사용자 지정에 대한 자세한 내용은 을 참조하십시오계정 사용자 지정.

2단계: AFT 배포에 필요한 VCS 구성 매개 변수를 지정합니다.

AFT 배포의 일부로 VCS 공급자를 구성하려면 다음 입력 매개변수가 필요합니다.

- vcs_provider: 사용하지 않는 경우 사용 AWS CodeCommit사례에 따라 VCS 공급자를 `"bitbucket"` `"github"` `"githubenterprise"`, 또는 로 지정하십시오.
- github_enterprise_url: 엔터프라이즈 고객의 경우에만 URL을 지정하십시오. GitHub GitHub
- 계정_요청_저장소_이름: 기본적으로 이 값은 사용자용으로 설정됩니다. `aft-account-request` AWS CodeCommit AFT가 지원되는 타사 VCS 공급자 환경에서 CodeCommit 또는 AFT가 지원하는

타사 VCS 공급자 환경에서 새 이름으로 리포지토리를 생성한 경우 이 입력 값을 실제 리포지토리 이름으로 업데이트하십시오. BitBucket, Github 및 GitHub Enterprise의 경우 리포지토리 이름의 형식은 다음과 같아야 합니다. `[Org]/[Repo]`

- account_customations_repo_name: 기본적으로 이 값은 사용자용으로 설정됩니다. `aft-account-customizations` AWS CodeCommit AFT가 지원되는 타사 VCS 공급자 환경에서 CodeCommit 또는 AFT가 지원하는 타사 VCS 공급자 환경에서 새 이름으로 리포지토리를 생성한 경우 이 입력 값을 리포지토리 이름으로 업데이트하십시오. BitBucket, Github 및 GitHub Enterprise의 경우 리포지토리 이름의 형식은 다음과 같아야 합니다. `[Org]/[Repo]`
- 계정_프로비져닝_커스터마이징_리포_이름: 기본적으로 이 값은 사용자에 대해 로 설정됩니다. `aft-account-provisioning-customizations` AWS CodeCommit AFT가 지원되는 타사 VCS 공급자 환경에서 AWS CodeCommit 또는 AFT가 지원되는 타사 VCS 공급자 환경에서 새 이름으로 리포지토리를 생성한 경우 이 입력 값을 리포지토리 이름으로 업데이트하십시오. BitBucket, Github 및 GitHub Enterprise의 경우 리포지토리 이름의 형식은 다음과 같아야 합니다. `[Org]/[Repo]`
- global_customations_repo_name: 기본적으로 이 값은 사용자용으로 설정됩니다. `aft-global-customizations` AWS CodeCommit AFT가 지원되는 타사 VCS 공급자 환경에서 CodeCommit 또는 AFT가 지원하는 타사 VCS 공급자 환경에서 새 이름으로 리포지토리를 생성한 경우 이 입력 값을 리포지토리 이름으로 업데이트하십시오. BitBucket, Github 및 GitHub Enterprise의 경우 리포지토리 이름의 형식은 다음과 같아야 합니다. `[Org]/[Repo]`
- account_request_repo_branch: 기본적으로 브랜치가 사용되지만 값을 재정의할 수 있습니다. `main`

기본적으로 AFT는 각 리포지토리의 브랜치에서 소스를 가져옵니다. `main` `git` 추가 입력 파라미터로 브랜치 이름 값을 오버라이드할 수 있습니다. 입력 파라미터에 대한 자세한 내용은 AFT Terraform 모듈의 README 파일을 참조하십시오.

3단계: 타사 VCS 제공자에 대한 AWS CodeStar 연결 완료

배포가 실행되면 AFT는 필수 AWS CodeCommit 리포지토리를 생성하거나 선택한 타사 VCS 공급자에 대한 AWS CodeStar 연결을 생성합니다. 후자의 경우 AFT 관리 계정의 콘솔에 수동으로 로그인하여 보류 중인 연결을 완료해야 합니다. AWS CodeStar AWS CodeStar 연결 완료에 대한 자세한 지침은 AWS CodeStar 설명서를 참조하십시오.

데이터 보호

AWS 공동 책임 모델은 AFT의 데이터 보호에 적용됩니다. 데이터 보호를 위해 다음과 같은 보안 모범 사례를 권장합니다.

- AWS Control Tower에서 제공하는 데이터 보호 지침을 따르십시오. 자세한 내용은 AWS Control Tower에서의 데이터 보호 섹션을 참조하세요.
- AFT 배포 시 생성된 Terraform 상태 구성을 보존하십시오. 자세한 내용은 테라폼용 AWS Control Tower 어카운트 팩토리 (AFT) 배포 섹션을 참조하세요.
- 조직의 보안 정책에 따라 민감한 자격 증명을 주기적으로 교체하십시오. 비밀의 예로는 Terraform 토큰, `git` 토큰 등이 있습니다.

저장된 데이터 암호화

AFT는 키 관리 서비스 키를 사용하여 저장 시 암호화된 Amazon S3 버킷, Amazon SNS 주제, Amazon SQS 대기열, Amazon DynamoDB 데이터베이스를 생성합니다. AWS AFT에서 생성한 KMS 키는 기본적으로 연간 순환이 활성화되어 있습니다. Terraform의 Terraform Cloud 또는 Terraform Enterprise 배포판을 선택하는 경우 AFT에는 민감한 Terraform 토큰 값을 저장하는 AWS Systems Manager SecureString 매개변수가 포함됩니다.

AFT는 여기에 설명된 AWS 서비스, 컴포넌트 서비스 즉 기본적으로 저장 시 암호화되는 서비스를 사용합니다. 자세한 내용은 AFT의 각 구성 요소 AWS 서비스에 대한 AWS 설명서를 참조하고 각 서비스가 준수하는 데이터 보호 관행에 대해 알아보십시오.

전송 중 데이터 암호화

AFT는 에 컴포넌트 서비스 설명된 AWS 서비스를 사용하며 기본적으로 전송 중 암호화를 사용합니다. 자세한 내용은 AFT의 각 구성 요소 AWS 서비스에 대한 AWS 설명서를 참조하고 각 서비스가 준수하는 데이터 보호 관행에 대해 알아보십시오.

Terraform Cloud 또는 Terraform Enterprise 배포의 경우 AFT는 Terraform 조직에 액세스하기 위해 HTTPS 엔드포인트 API를 호출합니다. AWS CodeStar 연결을 지원하는 타사 VCS 공급자를 선택하면 AFT는 VCS 공급자 조직에 액세스하기 위해 HTTPS 엔드포인트 API를 호출합니다.

AFT에서 계정 삭제하기

이 항목에서는 AFT 파이프라인이 계정 배포 및 업데이트를 중단하도록 AFT에서 계정을 삭제하는 방법에 대해 설명합니다.

> **Important**
>
> AFT 파이프라인에서 계정을 제거하는 것은 되돌릴 수 없으며 상태가 손실될 수 있습니다.

사용 중지된 애플리케이션의 계정을 폐쇄하거나, 손상된 계정을 격리하거나, 한 조직에서 다른 조직으로 계정을 이동하려는 경우 AFT에서 계정을 제거할 수 있습니다.

> **Note**
>
> AFT에서 계정을 제거하는 것은 AWS Control Tower 계정 또는 을 삭제하는 것과 다릅니다 AWS 계정. AFT에서 계정을 제거해도 AWS Control Tower는 여전히 계정을 관리합니다. AWS Control Tower 계정을 AWS 계정삭제하려면 다음을 참조하십시오.
>
> - AWS Control Tower 사용 설명서에서 계정 관리를 취소하십시오.
> - AWS Billing 사용 설명서의 계정 해지.

AFT 파이프라인에서 계정 삭제하기

다음 절차는 AFT에서 계정을 제거하는 방법을 설명합니다.

1. 계정 요청을 저장하는 **`git`** 저장소에서 계정을 제거합니다.

   계정 요청을 저장하는 `git` 저장소에서 AFT에서 제거하려는 계정에 대한 계정 요청을 삭제합니다.

   계정 요청 리포지토리에서 계정 요청을 제거하면 AFT는 사용자 지정 파이프라인과 계정 메타데이터를 삭제합니다. 자세한 내용은 AFT on의 1.8.0 릴리스 노트를 참조하십시오. GitHub
2. 테라폼 작업 영역 삭제 (테라폼 클라우드 및 테라폼 엔터프라이즈 고객 전용)

   AFT에서 제거하려는 계정의 글로벌 사용자 지정 및 계정 사용자 지정 작업 영역을 삭제합니다.
3. Amazon S3 백엔드에서 테라폼 상태를 삭제합니다.

   AFT 관리 계정에서 AFT에서 제거하려는 계정의 Amazon S3 버킷 내 모든 관련 폴더를 삭제합니다.

   > **Tip**
   >
   > 다음 예시에서는 AFT 관리 계정 ID *`012345678901`* 번호로 대체하십시오.

   예: 테라폼 OSS

Terraform OSS를 선택하면 및 `aft-backend-012345678901-primary-region` `aft-backend-012345678901-secondary-region` Amazon S3 버킷에서 각 계정에 대해 3개의 폴더를 찾을 수 있습니다. 이러한 폴더는 계정 사용자 지정 상태, 사용자 지정 파이프라인 상태 및 글로벌 사용자 지정 상태와 관련이 있습니다.

예: 테라폼 클라우드 또는 테라폼 엔터프라이즈

Terraform Cloud 또는 Terraform Enterprise를 선택하면 및 `aft-backend-012345678901-primary-region` Amazon S3 `aft-backend-012345678901-secondary-region` 버킷에서 각 계정의 폴더를 찾을 수 있습니다. 이러한 폴더는 사용자 지정 파이프라인 상태와 관련이 있습니다.

운영 지표

기본적으로 Account Factory for Terraform (AFT) 은 익명의 운영 지표를 에 전송합니다. AWS우리는 이 데이터를 사용하여 고객이 AFT를 어떻게 사용하고 있는지 이해하여 솔루션의 품질과 기능을 개선할 수 있습니다. AFT 배포 중에 매개변수를 변경하여 데이터 수집을 거부할 수 있습니다. 수집이 활성화되면 다음 데이터가 다음으로 전송됩니다 AWS.

- 솔루션: AFT 전용 식별자
- 버전: AFT 버전
- 범용 고유 식별자 (UUID): 각 AFT 배포에 대해 무작위로 생성되는 고유 식별자
- 타임스탬프: 데이터 수집 타임스탬프
- 데이터: AFT 구성 및 고객이 취한 조치

AWS 수집된 데이터를 소유합니다. 데이터 수집에는 AWS 개인정보 보호정책이 적용됩니다.

> **Note**
>
> 1.6.0 이전의 AFT 버전에서는 사용량 지표를 보고하지 않습니다. AWS

지표 보고 수신을 거부하려면:

- 다음 예와 같이 Terraform 입력 구성 파일에서 입력 값을 `aft_metrics_reporting` `false` ~로 설정하고 AFT를 재배포합니다. 명시적으로 설정하지 않을 경우 이 값은 `true` 기본적으로 로 설정됩니다.

예제를 복사할 경우 문자열로 지정된 항목을 실제 ID 및 지역 값으로 대체해야 합니다. x

```
module "control_tower_account_factory" {
source = "aws-ia/control_tower_account_factory/aws"

# Required Vars
ct_management_account_id    = "xxxxxxxxxxx"
log_archive_account_id      = "xxxxxxxxxxx"
audit_account_id            = "xxxxxxxxxxx"
aft_management_account_id   = "xxxxxxxxxxx"
ct_home_region              = "xx-xxxx-x"
tf_backend_secondary_region = "xx-xxxx-x"

# Optional Vars
aft_metrics_reporting = false    # to opt out, set this value to false
}
```

Account Factory for Terraform (AFT) 문제 해결 가이드

이 섹션은 Account Factory for Terraform (AFT) 을 사용할 때 발생할 수 있는 일반적인 문제를 해결하는 데 도움이 될 수 있습니다.

주제

- 일반 문제
- 계정 프로비저닝/등록 관련 문제
- 사용자 지정 호출 관련 문제
- 계정 사용자 지정 워크플로와 관련된 문제

일반 문제

- 리소스 할당량 초과 AWS

로그 그룹에 AWS 리소스 할당량을 초과했다고 표시되면AWS Support에 문의하세요. Account Factory는 AWS CodeBuild AWS Organizations, 및 를 포함하는 리소스 할당량과 AWS 서비스 함께 사용합니다. AWS Systems Manager자세한 내용은 다음을 참조하십시오.

- 무엇입니까? AWS CodeBuild CodeBuild 사용 설명서에서
- 이게 뭐예요 AWS Organizations? Organizations 사용 설명서에서
- 이게 뭐야 AWS Systems Manager? Systems Manager 사용 설명서에서

- Account Factory의 오래된 버전

  문제가 발생하여 문제가 버그라고 생각되면 Account Factory가 최신 버전인지 확인하십시오. 자세한 내용은 Account Factory 버전 업데이트를 참조하십시오.

- Account Factory 소스 코드가 로컬에서 변경되었습니다.

  Account Factory는 오픈소스 프로젝트입니다. AWS 컨트롤 타워는 어카운트 팩토리 코어 코드를 지원합니다. Account Factory 코어 코드를 로컬에서 변경하는 경우, AWS Control Tower는 최선을 다해 Account Factory 배포만 지원합니다.

- Account Factory 역할 권한이 충분하지 않음

  Account Factory는 벤더 계정 배포 및 사용자 지정을 관리하기 위한 IAM 역할 및 정책을 생성합니다. 이러한 역할 또는 정책을 변경하면 Account Factory 파이프라인이 특정 작업을 수행하지 못할 수 있습니다. 자세한 내용은 필수 역할을 참조하십시오.

- 계정 리포지토리가 제대로 채워지지 않았습니다.

  계정을 프로비저닝하기 전에 배포 후 단계를 따라야 합니다.

- OU를 수동으로 변경한 후 드리프트가 감지되지 않음

> **Note**
>
> AWS Control Tower는 드리프트를 자동으로 감지합니다. 드리프트 해결에 대한 자세한 내용은 AWS Control Tower에서의 드리프트 감지 및 해결을 참조하십시오.

조직 단위 (OU) 를 수동으로 변경할 때는 드리프트가 감지되지 않습니다. 이는 Account Factory의 이벤트 기반 특성 때문입니다. 계정 요청이 제출되면 Terraform이 관리하는 리소스는 다이렉트 계정이 아닌 Amazon DynamoDB 항목입니다. 항목이 변경되면 요청이 대기열에 추가되고, AWS Control Tower는 Service Catalog (계정 세부 정보를 관리하는 서비스) 를 통해 요청을 처리합니다. OU를 수동으로 변경하는 경우 계정 요청이 변경되지 않았으므로 드리프트가 감지되지 않습니다.

계정 프로비저닝/등록 관련 문제

- 계정 요청 (이메일 주소/이름) 이 이미 있습니다.

  이 문제로 인해 일반적으로 프로비저닝 또는 AS `ConditionalCheckFailedException` 중에 Service Catalog 제품에 장애가 발생합니다.

  다음 중 하나를 수행하여 문제에 대한 자세한 정보를 찾을 수 있습니다.

  - Terraform 또는 CloudWatch 로그 로그 그룹을 검토하세요.
  - Amazon SNS 주제에 `aft-failure-notifications` 발생한 장애를 검토하십시오.
- 잘못된 계정 요청

  계정 요청이 예상 스키마를 따르는지 확인하세요. 예를 들어, 의 terraform-aws-control_tower_account_factory를 참조하십시오. GitHub
- AWS 조직 리소스 할당량 초과

  계정 요청이 AWS Organizations 리소스 할당량을 초과하지 않는지 확인하세요. 자세한 내용은 조직 AWS 할당량을 참조하십시오.

사용자 지정 호출 관련 문제

- 대상 계정이 Account Factory에 온보딩되지 않음

  사용자 지정 요청에 포함된 모든 계정이 Account Factory에 온보딩되었는지 확인하십시오. 자세한 내용은 기존 계정 업데이트를 참조하십시오.
- 사용자 지정 요청 대상으로 하는 계정이 DynamoDB **`aft-request-metadata`** 테이블에는 있지만 계정 요청 리포지토리에는 없습니다.

  다음 중 하나를 수행하여 문제가 되는 계정을 제외하도록 사용자 지정 호출 요청 형식을 지정하십시오.

  - DynamoDB `aft-request-metadata` 테이블에서 더 이상 계정 요청 리포지토리에 없는 계정을 참조하는 항목을 삭제합니다.
  - “all”을 대상으로 사용하지 않음.
  - 계정이 속한 OU를 대상으로 하지 않습니다.
  - 계정을 직접 타겟팅하지 않습니다.
- Terraform Cloud에 잘못된 토큰을 사용했습니다.

올바른 토큰을 설정했는지 확인하세요. Terraform Cloud는 팀 기반 토큰만 지원하며 조직 기반 토큰은 지원하지 않습니다.

- 계정 사용자 지정 파이프라인이 생성되기 전에 계정을 만들지 못했습니다. 계정을 사용자 지정할 수 없습니다.

  계정 요청 리포지토리에서 계정 사양을 변경하세요. 계정의 태그 값을 변경하는 등 변경할 경우 Account Factory는 파이프라인이 없더라도 파이프라인 생성을 시도하는 경로를 따릅니다.

계정 사용자 지정 워크플로와 관련된 문제

계정 사용자 지정 워크플로와 관련된 문제가 발생하는 경우 AFT 버전이 1.8.0 이상이고 DynamoDB 요청 테이블에서 계정 관련 메타데이터의 모든 인스턴스를 삭제해야 합니다.

AFT 버전 1.8.0에 대한 자세한 내용은 릴리스 1.8.0 on을 참조하십시오. GitHub

AFT 버전을 확인하고 업데이트하는 방법에 대한 자세한 내용은 다음을 참조하십시오.

- AFT 버전을 확인하세요.
- AFT 버전 업데이트

또한 Amazon CloudWatch Logs Insights 쿼리를 사용하여 대상 계정 및 사용자 지정 요청 ID가 포함된 로그를 필터링하여 사용자 지정 요청을 추적하고 문제를 해결할 수 있습니다. 자세한 내용은 AFT 계정 사용자 지정 요청 추적 문제 해결을 참조하십시오.

AWS Control Tower의 드리프트 감지 및 해결

드리프트를 식별하고 해결하는 것은 AWS Control Tower 관리 계정 관리자의 정규 운영 업무입니다. 드리프트를 해결하면 거버넌스 요구 사항을 준수하는 데 도움이 됩니다.

랜딩 존을 만들면 랜딩 존과 모든 OU (조직 구성 단위), 계정, 리소스는 선택한 컨트롤에서 적용되는 거버넌스 규칙을 준수합니다. 사용자 및 조직 구성원이 landing Zone을 사용할 때 이 규정 준수 상태가 변경될 수 있습니다. 일부 변경 사항은 실수일 수 있으며, 일부는 시간에 민감한 작업 이벤트에 의도적으로 응답하는 것일 수 있습니다.

드리프트 감지로 드리프트를 해결하기 위해 변경 또는 구성 업데이트가 필요한 리소스를 식별할 수 있습니다.

드리프트 감지

AWS Control Tower는 드리프트를 자동으로 감지합니다. 드리프트를 감지하려면 AWS Control Tower가 읽기 전용 API 호출을 할 수 있도록 해당 `AWSControlTowerAdmin` 역할에 대한 관리 계정에 대한 지속적인 액세스 권한이 필요합니다. AWS Organizations이러한 API 호출은 이벤트로 표시됩니다. AWS CloudTrail

드리프트는 감사 계정에 집계되는 Amazon Simple Notification Service (Amazon SNS) 알림에 표시됩니다. 각 멤버 계정의 알림은 로컬 Amazon SNS 주제 및 Lambda 함수에 알림을 보냅니다.

AWS Security Hub 서비스 관리형 표준: AWS Control Tower에 속하는 컨트롤의 경우, 드리프트는 AWS Control Tower 콘솔의 계정 및 계정 세부 정보 페이지와 Amazon SNS 알림을 통해 표시됩니다.

멤버 계정 관리자는 특정 계정에 대한 SNS 드리프트 알림을 구독할 수 있습니다(모범 사례로서 권장됨). 예를 들어, `aws-controltower-AggregateSecurityNotifications` SNS 주제는 드리프트 알림을 제공합니다. AWS Control Tower 콘솔은 드리프트가 발생한 경우 관리 계정 관리자에게 알려줍니다. 드리프트 감지 및 알림을 위한 SNS 주제에 대한 자세한 내용은 드리프트 방지 및 알림을 참조하십시오.

드리프트 알림 중복 제거

동일한 리소스 세트에서 동일한 유형의 드리프트가 여러 번 발생하는 경우, AWS Control Tower는 드리프트의 초기 인스턴스에 대해서만 SNS 알림을 보냅니다. AWS Control Tower가 이 드리프트 인스턴스가 해결되었음을 감지하면 동일한 리소스에 대해 드리프트가 다시 발생하는 경우에만 또 다른 알림을 보냅니다.

예: 계정 드리프트와 SCP 드리프트는 다음과 같은 방식으로 처리됩니다.

- 동일한 관리 SCP를 여러 번 수정하면 처음 수정할 때 알림을 받게 됩니다.
- 관리되는 SCP를 수정한 다음 드리프트를 수정한 다음 다시 수정하면 두 개의 알림을 받게 됩니다.
- 드리프트를 먼저 복구하지 않고 동일한 소스 및 대상 OU 간에 계정을 여러 번 이동하면 해당 OU 간에 계정을 두 번 이상 이동했더라도 단일 알림이 전송됩니다.

계정 드리프트 유형

- OU 간 계정 이동
- 조직에서 계정이 제거되었습니다.

> **Note**
>
> 한 OU에서 다른 OU로 계정을 이동할 때 이전 OU의 컨트롤은 제거되지 않습니다. 대상 OU에서 새 후크 기반 제어를 활성화하면 기존 OU가 계정에서 후크 기반 컨트롤이 제거되고 새 컨트롤이 이를 대체합니다. SCP와 AWS Config 규칙으로 구현된 컨트롤은 계정이 OU를 변경할 때 항상 수동으로 제거해야 합니다.

정책 드리프트 유형

- SCP 업데이트
- OU에 연결된 SCP
- OU에서 SCP가 분리되었습니다.
- 계정에 연결된 SCP

자세한 내용은 거버넌스 드리프트 유형을 참조하십시오.

드리프트 해결

감지는 자동으로 수행되지만 드리프트를 해결하는 단계는 콘솔을 통해 수행해야 합니다.

- 랜딩 존 설정 페이지를 통해 다양한 유형의 드리프트를 해결할 수 있습니다. 버전 섹션에서 재설정 버튼을 선택하여 이러한 유형의 드리프트를 해결할 수 있습니다.

- OU의 계정이 300개 미만인 경우 조직 페이지 또는 OU 세부 정보 페이지에서 OU 재등록을 선택하여 Account Factory에서 프로비저닝한 계정의 드리프트 또는 SCP 드리프트를 해결할 수 있습니다.
- 개별 계정을 업데이트하는 등의 이동된 멤버 계정 방법으로 계정 드리프트를 해결할 수 있습니다. 자세한 정보는 콘솔에서 계정 업데이트을 참조하세요.

⚠ landing zone 버전에서 드리프트를 해결하기 위한 조치를 취하면 두 가지 동작이 가능합니다.

- 최신 랜딩 존 버전을 사용 중인 경우 Reset을 선택한 다음 Confirm (확인) 을 선택하면 드리프트된 랜딩 존 리소스가 저장된 AWS Control Tower 구성으로 재설정됩니다. Landding Zone 버전은 동일하게 유지됩니다.
- 최신 버전을 사용하고 있지 않은 경우 업데이트를 선택해야 합니다. 랜딩 존이 최신 랜딩 존 버전으로 업그레이드되었습니다. 이 프로세스의 일부로 드리프트가 해결되었습니다.

드리프트 및 SCP 스캔에 대한 고려사항

AWS Control Tower는 매일 관리형 SCP를 스캔하여 해당 제어가 올바르게 적용되고 표류하지 않았는지 확인합니다. SCP를 검색하고 검사를 실행하기 위해 AWS Control Tower는 관리 계정의 역할을 사용하여 사용자를 대신하여 전화를 겁니다 AWS Organizations .

AWS Control Tower 스캔에서 드리프트가 발견되면 알림을 받게 됩니다. AWS Control Tower는 드리프트 문제당 하나의 알림만 전송하므로, 랜딩 존이 이미 드리프트 상태에 있는 경우 새 드리프트 항목이 발견되지 않는 한 추가 알림을 받지 않습니다.

AWS Organizations 각 API를 호출할 수 있는 빈도를 제한합니다. 이 한도는 초당 트랜잭션 수 (TPS)로 표시되며 TPS 한도, 제한 속도 또는 API 요청 속도라고 합니다. AWS Control Tower가 호출을 통해 SCP를 감사하는 AWS Organizations경우, AWS Control Tower가 거는 API 호출은 TPS 한도에 포함됩니다. AWS Control Tower는 관리 계정을 사용하여 전화를 걸기 때문입니다.

드문 경우이긴 하지만 타사 솔루션이나 사용자가 작성한 사용자 지정 스크립트를 통해 동일한 API를 반복해서 호출하면 이 한도에 도달할 수 있습니다. 예를 들어, 사용자와 AWS Control AWS Organizations Tower가 같은 시점에 (1초 이내) 동일한 API를 호출하고 TPS 한도에 도달하면 후속 호출이 제한됩니다. 즉, 이러한 호출은 다음과 같은 오류를 반환합니다. `Rate exceeded`

API 요청 비율을 초과한 경우

- AWS Control Tower가 한도에 도달하여 병목 현상이 발생하는 경우 감사 실행을 일시 중지하고 나중에 다시 시작합니다.

- 워크로드가 한도에 도달하여 병목 현상이 발생하는 경우 워크로드 구성 방식에 따라 약간의 지연 시간부터 심각한 오류까지 다양한 결과가 발생할 수 있습니다. 이 엣지 케이스는 주의해야 할 사항입니다.

일일 SCP 스캔은 다음과 같이 구성됩니다.

1. 최근에 활성화된 OU 검색.
2. 등록된 각 OU에 대해 OU에 연결된 AWS Control Tower에서 관리하는 모든 SCP를 검색합니다. 관리형 SCP에는 로 시작하는 식별자가 있습니다. `aws-guardrails`
3. OU에서 활성화된 각 예방 제어에 대해 해당 컨트롤의 정책 설명이 OU의 관리형 SCP에 있는지 확인합니다.

OU에는 관리되는 SCP가 하나 이상 있을 수 있습니다.

즉시 해결해야 할 드리프트 유형

대부분의 드리프트 유형은 관리자가 해결할 수 있습니다. AWS Control Tower 랜딩 존에서 요구하는 조직 단위 삭제를 포함하여 몇 가지 유형의 드리프트를 즉시 해결해야 합니다. 다음은 피해야 할 주요 드리프트의 몇 가지 예입니다.

- 보안 OU를 삭제하지 마십시오. AWS Control Tower에서 랜딩 존 설정 시 원래 이름이 보안인 조직 단위는 삭제하면 안 됩니다. 랜딩 존을 삭제하면 랜딩 존을 즉시 재설정하라는 오류 메시지가 표시됩니다. 재설정이 완료될 때까지는 AWS Control Tower에서 다른 작업을 수행할 수 없습니다.
- 필수 역할을 삭제하지 마십시오. AWS Control Tower는 IAM 역할 드리프트를 위해 콘솔에 로그인할 때 특정 AWS Identity and Access Management (IAM) 역할을 확인합니다. 이러한 역할이 없거나 액세스할 수 없는 경우, 착륙 지대를 재설정하라는 오류 페이지가 표시됩니다. 이러한 역할은 다음과 같습니다. `AWSControlTowerAdmin` `AWSControlTowerCloudTrailRole` `AWSControlTowerStackSetRole`

  이러한 역할에 대한 자세한 내용은 을 참조하십시오AWS Control Tower 콘솔 사용에 필요한 권한.
- 추가 OU를 모두 삭제하지 마십시오. AWS Control Tower에서 랜딩 존을 설정하는 동안 원래 이름이 Sandbox인 조직 단위를 삭제하면 랜딩 존은 드리프트 상태가 되지만 AWS Control Tower는 계속 사용할 수 있습니다. AWS Control Tower가 작동하려면 추가 OU가 하나 이상 필요하지만 샌드박스 OU가 아니어도 됩니다.

- 공유 계정을 제거하지 마세요. 보안 OU에서 로깅 계정을 제거하는 등 기본 OU에서 공유 계정을 제거하면 랜딩 존이 드리프트 상태가 됩니다. AWS Control Tower 콘솔을 계속 사용하려면 먼저 랜딩 존을 재설정해야 합니다.

복구 가능한 리소스 변경

다음은 해결 가능한 변동이 발생하지만 허용되는 AWS Control Tower 리소스 변경 목록입니다. 새로 고침이 필요할 수도 있지만 이렇게 허용된 작업의 결과는 AWS Control Tower 콘솔에서 확인할 수 있습니다.

이로 인한 편차를 해결하는 방법에 대한 자세한 내용은 AWS Control Tower 외부 리소스 관리를 참조하십시오.

AWS Control Tower 콘솔 외부에서 허용되는 변경

- 등록된 OU의 이름을 변경하십시오.
- 보안 OU의 이름을 변경합니다.
- 비기본 OU의 구성원 계정 이름을 변경합니다.
- 보안 OU에서 AWS Control Tower 공유 계정의 이름을 변경합니다.
- 기반이 아닌 OU를 삭제하십시오.
- 비기반 OU에서 등록된 계정을 삭제합니다.
- 보안 OU에서 공유 계정의 이메일 주소를 변경합니다.
- 등록된 OU에 있는 구성원 계정의 이메일 주소를 변경합니다.

> **Note**
>
> OU 간 계정 이동은 드리프트로 간주되며 이를 해결해야 합니다.

드리프트 및 새 계정 프로비저닝

랜딩 존이 드리프트 상태인 경우, AWS Control Tower의 계정 등록 기능이 작동하지 않습니다. 이 경우 AWS Service Catalog를 통해 새 계정을 프로비저닝해야 합니다. 지침은 Account Factory를 통한 AWS Service Catalog 계정 프로비저닝 섹션을 참조하세요.

특히 Service Catalog를 통해 포트폴리오의 이름을 변경하는 등 계정을 일부 변경한 경우 계정 등록 기능이 작동하지 않습니다.

거버넌스 드리프트 유형

조직 드리프트라고도 하는 거버넌스 드리프트는 OU, SCP 및 구성원 계정이 변경되거나 업데이트될 때 발생합니다. AWS Control Tower에서 탐지할 수 있는 거버넌스 드리프트 유형은 다음과 같습니다.

- 이동된 멤버 계정
- 제거된 멤버 계정
- 관리형 SCP에 대한 계획되지 않은 업데이트
- 멤버 계정에 연결된 SCP
- 관리형 OU에 연결된 SCP
- 관리형 OU에서 분리된 SCP
- 삭제된 기본 OU
- Security Hub 컨트롤 드리프트
- 신뢰할 수 있는 액세스가 비활성화됨

또 다른 유형의 드리프트는 landing Zone drift이며, 이는 관리 계정을 통해 찾을 수 있습니다. 랜딩 존 드리프트는 IAM 역할 드리프트 또는 특히 기본 OU 및 공유 계정에 영향을 미치는 모든 유형의 조직 드리프트로 구성됩니다.

landing Zone Drift의 특별한 경우는 필요한 역할을 사용할 수 없을 때 감지되는 역할 드리프트입니다. 이러한 유형의 드리프트가 발생하면 콘솔에 경고 페이지와 역할 복원 방법에 대한 몇 가지 지침이 표시됩니다. 역할 드리프트가 해결되기 전까지는 랜딩 존을 사용할 수 없습니다. 드리프트에 대한 자세한 내용은 라는 섹션의 필수 역할 삭제 안 함을 참조하십시오. 즉시 해결해야 할 드리프트 유형

AWS Control Tower는 IAM Identity Center 등을 비롯하여 CloudTrail 관리 계정과 함께 작동하는 다른 서비스와 관련하여 드리프트를 찾지 않습니다. CloudWatch AWS CloudFormation AWS Config자녀 계정은 예방적 필수 제어 기능으로 보호되므로 자녀 계정에서는 드리프트 감지 기능을 사용할 수 없습니다.

하지만 AWS Security Hub 서비스 관리형 표준인 AWS Control Tower의 일부인 규제 항목과 관련된 편차는 보고됩니다.

이동된 멤버 계정

이러한 유형의 드리프트는 OU가 아닌 계정에서 발생합니다. 이러한 유형의 드리프트는 AWS Control Tower 멤버 계정, 감사 계정 또는 로그 아카이브 계정이 등록된 AWS Control Tower OU에서 다른 OU로 이동될 때 발생할 수 있습니다. 다음은 이러한 유형의 드리프트가 감지될 때 Amazon SNS 알림을 보내는 예시입니다.

```
{
  "Message" : "AWS Control Tower has detected that your member account 'account-
email@amazon.com (012345678909)' has been moved from organizational unit 'Sandbox
 (ou-0123-eEXAMPLE)' to 'Security (ou-3210-1EXAMPLE)'. For more information, including
 steps to resolve this issue, see 'https://docs.aws.amazon.com/console/controltower/
move-account'",
  "ManagementAccountId" : "012345678912",
  "OrganizationId" : "o-123EXAMPLE",
  "DriftType" : "ACCOUNT_MOVED_BETWEEN_OUS",
  "RemediationStep" : "Re-register this organizational unit (OU), or if the OU has more
 than 300 accounts, you must update the provisioned product in Account Factory.",
  "AccountId" : "012345678909",
  "SourceId" : "012345678909",
  "DestinationId" : "ou-3210-1EXAMPLE"
}
```

해결 방법

최대 300개의 계정이 있는 OU의 Account Factory 프로비저닝 계정에서 이러한 유형의 드리프트가 발생하는 경우 다음과 같이 문제를 해결할 수 있습니다.

- AWS Control Tower 콘솔의 조직 페이지로 이동하여 계정을 선택하고 오른쪽 상단에서 계정 업데이트 (개별 계정의 경우 가장 빠른 옵션) 를 선택합니다.
- AWS Control Tower 콘솔의 조직 페이지로 이동한 다음 계정이 포함된 OU에 재등록 (여러 계정을 위한 가장 빠른 옵션) 을 선택합니다. 자세한 정보는 기존 조직 단위를 AWS Control Tower에 등록을 참조하세요.
- Account Factory에서 프로비저닝된 제품 업데이트 자세한 정보는 AWS Control Tower 또는 다음을 통해 계정 팩토리 계정을 업데이트하고 이전하십시오. AWS Service Catalog을 참조하세요.

> **Note**
>
> 업데이트해야 할 개별 계정이 여러 개 있는 경우 스크립트를 사용하여 업데이트하는 다음 방법도 참조하십시오. 자동화를 사용하여 계정을 프로비저닝하고 업데이트합니다.

- 계정이 300개 이상인 OU에서 이러한 유형의 드리프트가 발생하는 경우 다음 단락에서 설명하는 것처럼 이동된 계정 유형에 따라 드리프트 해결이 달라질 수 있습니다. 자세한 정보는 랜딩 영역 업데이트을 참조하세요.
  - Account Factory의 프로비저닝 계정이 이동된 경우 - 계정이 300개 미만인 OU의 경우 Account Factory에서 프로비저닝된 제품을 업데이트하거나, OU를 다시 등록하거나, 랜딩 영역을 업데이트하여 계정 드리프트를 해결할 수 있습니다.

    계정이 300개 이상인 OU에서는 OU를 재등록해도 업데이트가 수행되지 않으므로 AWS Control Tower 콘솔 또는 프로비저닝된 제품을 통해 이동된 각 계정을 업데이트하여 편차를 해결해야 합니다. 자세한 정보는 AWS Control Tower 또는 다음을 통해 계정 팩토리 계정을 업데이트하고 이전하십시오. AWS Service Catalog을 참조하세요.
  - 공유 계정이 이동된 경우 - landing Zone을 업데이트하여 감사 또는 로그 아카이브 계정 이동으로 인한 편차를 해결할 수 있습니다. 자세한 정보는 랜딩 영역 업데이트을 참조하세요.

> **더 이상 사용되지 않는 필드 이름**
>
> 필드 이름은 `MasterAccountID` 가이드라인을 `ManagementAccountID` AWS 준수하도록 변경되었습니다. 이전 이름은 더 이상 사용되지 않습니다. 2022년부터 지원 중단된 필드 이름을 포함하는 스크립트는 더 이상 작동하지 않습니다.

제거된 멤버 계정

이러한 유형의 드리프트는 등록된 AWS Control Tower 조직 단위에서 회원 계정이 제거될 때 발생할 수 있습니다. 다음 예는 이러한 유형의 드리프트가 감지될 때의 Amazon SNS 알림을 보여줍니다.

```
{
  "Message" : "AWS Control Tower has detected that the member account 012345678909 has
 been removed from organization o-123EXAMPLE. For more information, including steps
 to resolve this issue, see 'https://docs.aws.amazon.com/console/controltower/remove-
account'",
```

```
  "ManagementAccountId" : "012345678912",
  "OrganizationId" : "o-123EXAMPLE",
  "DriftType" : "ACCOUNT_REMOVED_FROM_ORGANIZATION",
  "RemediationStep" : "Add account to Organization and update Account Factory
 provisioned product",
  "AccountId" : "012345678909"
}
```

해결 방법

- 멤버 계정에서 이러한 유형의 드리프트가 발생하는 경우, AWS Control Tower 콘솔 또는 Account Factory에서 계정을 업데이트하여 드리프트를 해결할 수 있습니다. 예를 들어 Account Factory 업데이트 마법사에서 등록된 다른 OU에 계정을 추가할 수 있습니다. 자세한 정보는 AWS Control Tower 또는 다음을 통해 계정 팩토리 계정을 업데이트하고 이전하십시오. AWS Service Catalog을 참조하세요.
- 기본 OU에서 공유 계정을 제거한 경우, 랜딩 존을 재설정하여 드리프트를 해결해야 합니다. 이 문제가 해결될 때까지는 AWS Control Tower 콘솔을 사용할 수 없습니다.
- 계정 및 OU 드리프트 해결에 대한 자세한 내용은 AWS Control Tower 외부에서 리소스를 관리하는 경우 단원을 참조하십시오.

> **Note**
>
> Service Catalog에서 계정을 나타내는 Account Factory에서 프로비저닝한 제품은 계정을 제거하도록 업데이트되지 않았습니다. 대신 프로비저닝된 제품이 TAINTED 및 오류 상태로 표시됩니다. 정리하려면 Service Catalog로 이동하여 프로비저닝된 제품을 선택한 다음 종료를 선택합니다.

관리형 SCP에 대한 계획되지 않은 업데이트

이러한 유형의 드리프트는 AWS Organizations 콘솔에서 또는 AWS SDK 중 하나를 사용하여 프로그래밍 방식으로 컨트롤용 SCP를 업데이트할 때 발생할 수 있습니다. AWS CLI 다음은 이러한 유형의 드리프트가 감지될 때 Amazon SNS 알림을 보내는 예시입니다.

```
{
  "Message" : "AWS Control Tower has detected that the managed service control policy
 'aws-guardrails-012345 (p-tEXAMPLE)', attached to the registered organizational unit
```

```
 'Security (ou-0123-1EXAMPLE)', has been modified. For more information, including
 steps to resolve this issue, see 'https://docs.aws.amazon.com/console/controltower/
update-scp'",
  "ManagementAccountId" : "012345678912",
  "OrganizationId" : "o-123EXAMPLE",
  "DriftType" : "SCP_UPDATED",
  "RemediationStep" : "Update Control Tower Setup",
  "OrganizationalUnitId" : "ou-0123-1EXAMPLE",
  "PolicyId" : "p-tEXAMPLE"
}
```

해결 방법

최대 300개의 계정이 있는 OU에서 이러한 유형의 드리프트가 발생하는 경우 다음과 같이 해결할 수 있습니다.

- AWS Control Tower 콘솔의 조직 페이지로 이동하여 OU를 재등록합니다 (가장 빠른 옵션). 자세한 정보는 기존 조직 단위를 AWS Control Tower에 등록을 참조하세요.
- 랜딩 존 업데이트 (더 느린 옵션). 자세한 정보는 랜딩 영역 업데이트을 참조하세요.

계정이 300개 이상인 OU에서 이러한 유형의 드리프트가 발생하면 landing Zone을 업데이트하여 문제를 해결하십시오. 자세한 정보는 랜딩 영역 업데이트을 참조하세요.

관리형 OU에 연결된 SCP

컨트롤의 SCP가 다른 OU에 연결된 경우 이러한 유형의 드리프트가 발생할 수 있습니다. 이러한 현상은 AWS Control Tower 콘솔 외부에서 OU를 작업할 때 특히 흔합니다. 다음은 이러한 유형의 드리프트가 감지될 때 Amazon SNS 알림을 보내는 예시입니다.

```
{
  "Message" : "AWS Control Tower has detected that the managed service control
 policy 'aws-guardrails-012345 (p-tEXAMPLE)' has been attached to the registered
 organizational unit 'Sandbox (ou-0123-1EXAMPLE)'. For more information, including
 steps to resolve this issue, see 'https://docs.aws.amazon.com/console/controltower/
scp-detached-ou'",
  "ManagementAccountId" : "012345678912",
  "OrganizationId" : "o-123EXAMPLE",
  "DriftType" : "SCP_ATTACHED_TO_OU",
  "RemediationStep" : "Update Control Tower Setup",
  "OrganizationalUnitId" : "ou-0123-1EXAMPLE",
```

```
  "PolicyId" : "p-tEXAMPLE"
}
```

해결 방법

최대 300개의 계정이 있는 OU에서 이러한 유형의 드리프트가 발생하는 경우 다음과 같이 해결할 수 있습니다.

- AWS Control Tower 콘솔의 조직 페이지로 이동하여 OU를 재등록합니다 (가장 빠른 옵션). 자세한 정보는 기존 조직 단위를 AWS Control Tower에 등록을 참조하세요.
- 랜딩 존 업데이트 (더 느린 옵션). 자세한 정보는 랜딩 영역 업데이트을 참조하세요.

계정이 300개 이상인 OU에서 이러한 유형의 드리프트가 발생하면 landing Zone을 업데이트하여 문제를 해결하십시오. 자세한 정보는 랜딩 영역 업데이트을 참조하세요.

관리형 OU에서 분리된 SCP

이러한 유형의 드리프트는 컨트롤의 SCP가 AWS Control Tower에서 관리하는 OU에서 분리되었을 때 발생할 수 있습니다. 이러한 현상은 AWS Control Tower 콘솔 외부에서 작업할 때 특히 흔합니다. 다음은 이러한 유형의 드리프트가 감지될 때 Amazon SNS 알림을 보내는 예시입니다.

```
{
  "Message" : "AWS Control Tower has detected that the managed service control
 policy 'aws-guardrails-012345 (p-tEXAMPLE)' has been detached from the registered
 organizational unit 'Sandbox (ou-0123-1EXAMPLE)'. For more information, including
 steps to resolve this issue, see 'https://docs.aws.amazon.com/console/controltower/
scp-detached'",
  "ManagementAccountId" : "012345678912",
  "OrganizationId" : "o-123EXAMPLE",
  "DriftType" : "SCP_DETACHED_FROM_OU",
  "RemediationStep" : "Update Control Tower Setup",
  "OrganizationalUnitId" : "ou-0123-1EXAMPLE",
  "PolicyId" : "p-tEXAMPLE"
}
```

해결 방법

최대 300개의 계정이 있는 OU에서 이러한 유형의 드리프트가 발생하는 경우 다음과 같이 해결할 수 있습니다.

- AWS Control Tower 콘솔에서 OU로 이동하여 OU를 재등록합니다 (가장 빠른 옵션). 자세한 정보는 기존 조직 단위를 AWS Control Tower에 등록을 참조하세요.
- 랜딩 존 업데이트 (더 느린 옵션). 드리프트가 필수 제어에 영향을 미치는 경우 업데이트 프로세스는 새 서비스 제어 정책 (SCP) 을 만들고 이를 OU에 연결하여 드리프트를 해결합니다. 착륙 지대를 업데이트하는 방법에 대한 자세한 내용은 을 참조하십시오랜딩 영역 업데이트.

계정이 300개 이상인 OU에서 이러한 유형의 드리프트가 발생하면 landing Zone을 업데이트하여 문제를 해결하십시오. 드리프트가 필수 제어에 영향을 미치는 경우 업데이트 프로세스는 새 서비스 제어 정책 (SCP) 을 만들고 이를 OU에 연결하여 드리프트를 해결합니다. 착륙 지대를 업데이트하는 방법에 대한 자세한 내용은 을 참조하십시오랜딩 영역 업데이트.

멤버 계정에 연결된 SCP

이러한 유형의 드리프트는 컨트롤의 SCP가 Organizations 콘솔의 계정에 연결되어 있을 때 발생할 수 있습니다. AWS Control Tower 콘솔을 통해 OU에서 가드레일과 해당 SCP를 활성화하여 OU에 등록된 모든 계정에 적용할 수 있습니다. 다음은 이러한 유형의 드리프트가 감지될 때 Amazon SNS 알림을 보내는 예시입니다.

```
{
  "Message" : "AWS Control Tower has detected that the managed service control policy
 'aws-guardrails-012345 (p-tEXAMPLE)' has been attached to the member account 'account-
email@amazon.com (012345678909)'. For more information, including steps to resolve this
 issue, see 'https://docs.aws.amazon.com/console/controltower/scp-detached-account'",
  "ManagementAccountId" : "012345678912",
  "OrganizationId" : "o-123EXAMPLE",
  "DriftType" : "SCP_ATTACHED_TO_ACCOUNT",
  "RemediationStep" : "Re-register this organizational unit (OU)",
  "AccountId" : "012345678909",
  "PolicyId" : "p-tEXAMPLE"
}
```

해결 방법

이러한 유형의 드리프트는 OU가 아닌 계정에서 발생합니다.

보안 OU와 같은 기본 OU의 계정에서 이러한 유형의 드리프트가 발생하는 경우 해결 방법은 랜딩 영역을 업데이트하는 것입니다. 자세한 정보는 랜딩 영역 업데이트을 참조하세요.

최대 300개의 계정이 있는 비기본 OU에서 이러한 유형의 드리프트가 발생하는 경우 다음과 같이 해결할 수 있습니다.

- 어카운트 팩토리 계정에서 AWS Control Tower SCP를 분리합니다.
- AWS Control Tower 콘솔에서 OU로 이동하여 OU를 재등록합니다 (가장 빠른 옵션). 자세한 정보는 기존 조직 단위를 AWS Control Tower에 등록을 참조하세요.

계정이 300개 이상인 OU에서 이러한 유형의 드리프트가 발생하는 경우 해당 계정의 계정 팩토리 구성을 업데이트하여 문제를 해결할 수 있습니다. 문제를 성공적으로 해결하지 못할 수도 있습니다. 자세한 정보는 랜딩 영역 업데이트을 참조하세요.

삭제된 기본 OU

이러한 유형의 드리프트는 보안 OU와 같은 AWS Control Tower 기본 OU에만 적용됩니다. 기본 OU가 AWS Control Tower 콘솔 외부에서 삭제되는 경우 발생할 수 있습니다. OU를 이동하는 것은 OU를 삭제한 다음 다른 곳에 추가하는 것과 같기 때문에 이러한 유형의 드리프트를 생성하지 않고는 기본 OU를 이동할 수 없습니다. 랜딩 존을 업데이트하여 드리프트를 해결하면 AWS Control Tower가 원래 위치의 기본 OU를 대체합니다. 다음 예는 이러한 유형의 드리프트가 감지될 때 수신할 수 있는 Amazon SNS 알림을 보여줍니다.

```
{
  "Message" : "AWS Control Tower has detected that the registered organizational unit
 'Security (ou-0123-1EXAMPLE)' has been deleted. For more information, including steps
 to resolve this issue, see 'https://docs.aws.amazon.com/console/controltower/delete-
ou'",
  "ManagementAccountId" : "012345678912",
  "OrganizationId" : "o-123EXAMPLE",
  "DriftType" : "ORGANIZATIONAL_UNIT_DELETED",
  "RemediationStep" : "Delete organizational unit in Control Tower",
  "OrganizationalUnitId" : "ou-0123-1EXAMPLE"
}
```

해결 방법

이 드리프트는 기본 OU에서만 발생하므로 해결 방법은 landing zone을 업데이트하는 것입니다. 다른 유형의 OU가 삭제되면 AWS Control Tower가 자동으로 업데이트됩니다.

계정 및 OU 드리프트 해결에 대한 자세한 내용은 AWS Control Tower 외부에서 리소스를 관리하는 경우 단원을 참조하십시오.

Security Hub 컨트롤 드리프트

이러한 유형의 드리프트는 AWS Security Hub 서비스 관리형 표준: AWS Control Tower의 일부인 컨트롤이 드리프트 상태를 보고할 때 발생합니다. AWS Security Hub 서비스 자체는 이러한 컨트롤에 대한 드리프트 상태를 보고하지 않습니다. 대신 서비스는 조사 결과를 AWS Control Tower에 보냅니다.

또한, AWS Control Tower가 Security Hub로부터 24시간 이상 상태 업데이트를 받지 않은 경우에도 Security Hub 제어 드리프트를 감지할 수 있습니다. 이러한 결과가 예상대로 접수되지 않을 경우, AWS Control Tower는 제어가 드리프트 상태인지 확인합니다. 다음 예는 이러한 유형의 드리프트가 감지될 때 수신할 수 있는 Amazon SNS 알림을 보여줍니다.

```
{
"Message" : "AWS Control Tower has detected that an AWS Security Hub control
 was removed in your account example-account@amazon.com <mailto:example-
account@amazon.com>. The artifact deployed on the target OU and accounts does not match
 the expected template and configuration for the control. This mismatch indicates that
 configuration changes were made outside of AWS Control Tower. For more information,
 view Security Hub standard",
"MasterAccountId" : "123456789XXX",
"ManagementAccountId" : "123456789XXX",
"OrganizationId" : "o-123EXAMPLE",
"DriftType" : "SECURITY_HUB_CONTROL_DISABLED",
"RemediationStep" : "To remediate the issue, Re-register the OU, or remove the control
 and enable it again. If the problem persists, contact AWS support.",
"AccountId" : "7876543219XXX",
"ControlId" : "PYBETSAGNUZB",
"ControlName" : "EBS snapshots should not be publicly restorable",
"ApiControlIdentifier" : "arn:aws:controltower:us-east-1::control/PYBETSAGNUZB",
"Region" : "us-east-1"
}
```

해결 방법

계정이 300개 미만인 OU의 경우 해결 방법은 OU를 다시 등록하여 제어를 원래 상태로 재설정하는 것입니다. 모든 OU에 대해 콘솔 또는 AWS Control Tower API를 통해 제어를 제거했다가 다시 활성화할 수 있으며, 이렇게 하면 제어도 재설정됩니다.

계정 및 OU 드리프트 해결에 대한 자세한 내용은 AWS Control Tower 외부에서 리소스를 관리하는 경우 단원을 참조하십시오.

신뢰할 수 있는 액세스가 비활성화됨

이러한 유형의 드리프트는 AWS Control Tower 착륙 지역에 적용됩니다. 이는 AWS Control Tower 랜딩 존을 설정한 AWS Organizations 후 AWS Control Tower에 대한 신뢰할 수 있는 액세스를 비활성화할 때 발생합니다.

신뢰할 수 있는 액세스가 비활성화되면 AWS Control Tower는 더 이상 변경 이벤트를 수신하지 않습니다 AWS Organizations. AWS Control Tower는 이러한 변경 이벤트를 기반으로 동기화 상태를 유지합니다. AWS Organizations따라서 AWS Control Tower는 계정 및 OU의 조직 변경을 놓칠 수 있습니다. 따라서 landing Zone을 업데이트할 때마다 각 OU를 다시 등록하는 것이 중요합니다.

예: 아마존 SNS 알림

다음은 이러한 유형의 드리프트가 발생할 때 수신하는 Amazon SNS 알림의 예입니다.

```
{
  "Message" : "AWS Control Tower has detected that trusted access has been disabled in
 AWS Organizations. For more information, including steps to resolve this issue, see
 https://docs.aws.amazon.com/controltower/latest/userguide/drift.html#drift-trusted-
access-disabled",
  "ManagementAccountId" : "012345678912",
  "OrganizationId" : "o-123EXAMPLE",
  "DriftType" : "TRUSTED_ACCESS_DISABLED",
  "RemediationStep" : "Reset Control Tower landing zone."
}
```

해결 방법

AWS Control Tower는 AWS Control Tower 콘솔에서 이러한 유형의 드리프트가 발생하면 사용자에게 알려줍니다. 해결 방법은 AWS Control Tower 랜딩 존을 재설정하는 것입니다. 자세한 내용은 드리프트 해결을 참조하십시오.

AWS Control Tower 외부에서 리소스를 관리하는 경우

AWS Control Tower는 사용자를 대신하여 계정, 조직 단위 및 기타 리소스를 설정하지만 이러한 리소스의 소유자는 사용자입니다. 이러한 리소스는 AWS Control Tower 내부 또는 외부에서 변경할 수 있습니다. AWS Control Tower 외부에서 리소스를 변경하는 가장 일반적인 장소는 AWS Organizations 콘솔입니다. 이 주제에서는 AWS Control Tower 외부에서 변경을 수행할 때 AWS Control Tower 리소스에 대한 변경 사항을 조정하는 방법을 설명합니다.

리소스의 이름을 바꾸고, 리소스를 삭제하고, AWS Control Tower 콘솔 외부로 이동하면 콘솔이 동기화되지 않습니다. 많은 변경 사항이 자동으로 조정될 수 있습니다. 특정 변경 사항의 경우 AWS Control Tower 콘솔에 표시되는 정보를 업데이트하려면 착륙 지대를 재설정해야 합니다.

일반적으로 AWS Control Tower 콘솔 외부에서 AWS Control Tower 리소스를 변경하면 착륙 지대에 해결 가능한 드리프트 상태가 발생합니다. 이러한 변경에 대한 내용은 복구 가능한 리소스 변경 섹션을 참조하세요.

Landing Zone 재설정이 필요한 작업

- 보안 OU 삭제 (간단한 작업이 아닌 특별한 경우)
- 보안 OU에서 공유 계정 제거 (권장하지 않음)
- 보안 OU와 연결된 SCP 업데이트, 연결 또는 분리

AWS Control Tower에서 자동으로 업데이트하는 변경 사항

- 등록된 계정의 이메일 주소 변경
- 등록된 계정 이름 변경
- 새로운 최상위 조직 단위 (OU) 생성
- 등록된 OU 이름 변경
- 등록된 OU 삭제 (업데이트가 필요한 보안 OU 제외)
- 등록된 계정 삭제 (보안 OU의 공유 계정 제외)

> **Note**
>
> AWS Service Catalog 변경 사항을 AWS Control Tower와 다르게 처리합니다. AWS Service Catalog 변경 사항을 조정할 때 거버넌스 태세에 변화가 생길 수 있습니다. 프로비전된 제품 업데이트에 대한 자세한 내용은 설명서의 프로비저닝된 제품 업데이트를 참조하십시오. AWS Service Catalog

AWS Control Tower 외부의 리소스 참조

AWS Control Tower 외부에서 새 OU와 계정을 생성하는 경우, 해당 OU와 계정이 표시될 수는 있지만 AWS Control Tower의 규제를 받지 않습니다.

OU 만들기

AWS Control Tower 외부에서 생성된 조직 단위 (OU) 를 미등록이라고 합니다. 조직 페이지에 표시되지만 AWS Control Tower 컨트롤의 적용을 받지는 않습니다.

계정 생성

AWS Control Tower 외부에서 생성된 계정을 등록 취소라고 합니다. AWS Control Tower에 등록된 OU에 속하는 등록 및 미등록 계정이 조직 페이지에 표시됩니다. 등록된 OU에 속하지 않는 계정은 콘솔을 사용하여 초대할 수 있습니다. AWS Organizations 이 가입 초대를 받았다고 해서 계정이 AWS Control Tower에 등록되거나 AWS Control Tower 거버넌스가 해당 계정으로 확장되는 것은 아닙니다. 계정을 등록하여 거버넌스를 확장하려면 AWS Control Tower의 조직 페이지 또는 계정 세부 정보 페이지로 이동하여 계정 등록을 선택하십시오.

외부 AWS Control Tower 리소스 이름 변경

AWS Control Tower 콘솔 외부에서 조직 단위 (OU) 및 계정의 이름을 변경할 수 있으며, 콘솔은 이러한 변경 사항을 반영하도록 자동으로 업데이트됩니다.

OU 이름 변경

AWS Organizations에서는 AWS Organizations API 또는 콘솔을 사용하여 OU 이름을 변경할 수 있습니다. AWS Control Tower 외부에서 OU 이름을 변경하면 AWS Control Tower 콘솔에 이름 변경이 자동으로 반영됩니다. 하지만 를 사용하여 AWS Service Catalog계정을 프로비저닝하는 경우 AWS Control Tower가 일관성을 유지할 수 있도록 랜딩 존도 재설정해야 AWS Organizations합니다. 재설정 워크플로는 기본 OU와 추가 OU에 대한 서비스 전반의 일관성을 보장합니다. 랜딩 존 설정 페이지에서 이러한 유형의 드리프트를 해결할 수 있습니다. 의 “드리프트 해결” 섹션을 참조하십시오. AWS Control Tower의 드리프트 감지 및 해결

AWS Control Tower는 AWS 컨트롤 타워 대시보드의 조직 페이지에 OU 이름을 표시합니다. landing zone 재설정 작업이 성공했는지 확인할 수 있습니다.

등록된 계정 이름 변경

각 AWS 계정에는 AWS Billing and Cost Management 콘솔에서 계정의 루트 사용자가 변경할 수 있는 표시 이름이 있습니다. AWS Control Tower에 등록된 계정의 이름을 변경하면 이름 변경 내용이 AWS Control Tower에 자동으로 반영됩니다. 계정 이름 변경에 대한 자세한 내용은 AWS 결제 사용 설명서의 AWS 계정 관리를 참조하십시오.

보안 OU 삭제

이 유형의 드리프트는 특수한 경우입니다. Security OU를 삭제하면 착륙 영역을 재설정하라는 오류 메시지 페이지가 표시됩니다. AWS Control Tower에서 다른 작업을 수행하려면 먼저 랜딩 존을 재설정해야 합니다.

- 재설정이 완료되기 AWS Service Catalog 전까지는 AWS Control Tower 콘솔에서 어떤 작업도 수행할 수 없으며 새 계정을 생성할 수 없습니다.
- 랜딩 존 설정 페이지에서 재설정 버튼을 볼 수 없습니다.

이 경우, landing zone 재설정 프로세스는 새 보안 OU를 만들고 두 공유 계정을 새 보안 OU로 이동합니다. AWS Control Tower는 로그 아카이브 및 감사 계정을 드리프트된 것으로 표시합니다. 동일한 프로세스를 통해 이러한 계정의 편차가 해결됩니다.

보안 OU를 삭제해야 한다고 판단되면 다음 사항을 알아두어야 합니다.

보안 OU를 삭제하려면 먼저 보안 OU에 계정이 없는지 확인해야 합니다. 특히 OU에서 로그 아카이브 및 감사 계정을 제거해야 합니다. 이러한 계정을 다른 OU로 이동하는 것이 좋습니다.

> **Note**
>
> 보안 OU를 삭제하는 작업은 적절한 고려 없이 수행해서는 안 됩니다. 이 작업을 수행하면 로깅이 일시적으로 중단되고 일부 제어 기능이 적용되지 않을 수 있으므로 규정 준수 문제가 발생할 수 있습니다.

드리프트에 대한 일반적인 정보는 AWS Control Tower의 드리프트 감지 및 해결의 “드리프트 해결”을 참조하십시오.

보안 OU에서 계정 제거

공유 계정을 조직에서 제거하거나 보안 OU 외부로 옮기는 것은 권장하지 않습니다. 실수로 공유 계정을 제거한 경우 이 섹션의 수정 단계에 따라 계정을 복원할 수 있습니다.

- AWS Control Tower 콘솔 내에서: 수정 프로세스를 시작하려면 반수동 수정 단계를 따르십시오. AWS Control Tower 콘솔에 액세스하는 데 사용하는 사용자 또는 역할이 실행 권한을 가지고 있는지 확인하십시오`organizations:InviteAccountToOrganization`. 이러한 권한이 없는 경우, AWS Control Tower 콘솔과 콘솔을 모두 사용하는 수동 수정 단계를 따르십시오. AWS Organizations

- AWS Organizations 콘솔에서 시작: 이 수정 프로세스는 약간 더 긴 완전 수동 절차입니다. 수동 수정 단계를 수행하면 콘솔과 AWS Control Tower AWS Organizations 콘솔 사이를 전환하게 됩니다. 에서 AWS Organizations작업하려면 `AWSOrganizationsFullAccess` 관리형 정책 또는 이에 상응하는 사용자 또는 역할이 필요합니다. AWS Control Tower 콘솔에서 작업할 때는 `AWSControlTowerServiceRolePolicy` 관리형 정책 또는 이에 상응하는 정책을 가진 사용자 또는 역할, 그리고 모든 AWS Control Tower 작업 (controltower: *) 을 실행할 수 있는 권한이 필요합니다.
- 수정 단계를 수행해도 계정이 복원되지 않는 경우 문의해 주십시오. AWS Support

다음을 통해 AWS Organizations공유 계정을 제거한 결과:

- 이 계정은 더 이상 서비스 제어 정책 (SCP) 을 통한 AWS Control Tower 필수 제어에 의해 보호되지 않습니다. 결과: 계정에서 AWS Control Tower가 생성한 리소스는 수정되거나 삭제될 수 있습니다.
- 계정은 더 이상 AWS Organizations 관리 계정에 속하지 않습니다. 결과: AWS Organizations 관리 계정 관리자는 더 이상 계정의 지출을 확인할 수 없습니다.
- 해당 계정은 더 이상 모니터링이 보장되지 않습니다 AWS Config. 결과: AWS Organizations 관리 계정 관리자가 리소스 변경을 감지하지 못할 수 있습니다.
- 계정이 더 이상 조직에 없습니다. 결과: AWS Control Tower 업데이트 및 재설정이 실패합니다.

AWS Control Tower 콘솔을 사용하여 공유 계정을 복원하려면 (반수동 절차)

1. https://console.aws.amazon.com/controltower 에서 AWS 컨트롤 타워 콘솔에 로그인합니다. IAM 사용자, IAM ID 센터의 사용자 또는 실행 권한이 있는 역할로 로그인해야 합니다. `organizations:InviteAccountToOrganization` 이러한 권한이 없는 경우 이 주제 뒷부분에서 설명하는 수동 수정 절차를 사용하십시오.
2. 랜딩 존 드리프트 감지 페이지에서 Re-Invite를 선택하여 공유 계정을 조직에 다시 초대하여 공유 계정 제거 문제를 해결합니다. 자동으로 생성된 이메일이 해당 계정의 이메일 주소로 전송됩니다.
3. 초대를 수락하여 공유 계정을 다시 조직으로 가져오세요. 다음 중 하나를 수행하십시오.
    - 제거된 공유 계정에 로그인한 다음 https://console.aws.amazon.com/organizations/home#/invites 으로 이동합니다.
    - 계정을 다시 초대했을 때 보낸 이메일 메시지에 액세스할 수 있는 경우 제거된 계정에 로그인한 다음 메시지의 링크를 클릭하여 계정 초대로 바로 이동하십시오.
    - 제거된 공유 계정이 다른 조직에 속하지 않는 경우 해당 계정에 로그인하고 AWS Organizations 콘솔을 연 다음 초대로 이동합니다.

4. 관리 계정에 다시 로그인하거나, 이미 열려 있는 경우 AWS Control Tower 콘솔을 다시 로드하십시오. 랜딩 존 드리프트 페이지가 표시됩니다. Reset을 선택하여 랜딩 존을 복구하십시오.
5. 재설정 프로세스가 완료될 때까지 기다리세요.

수정이 성공하면 공유 계정이 정상 상태 및 규정 준수 상태로 나타납니다.

수정 단계를 수행해도 계정이 복원되지 않으면 문의하세요. AWS Support

AWS AWS Organizations Control Tower 및 콘솔을 사용하여 공유 계정을 복원하려면 (수동 수정)

1. 에서 콘솔에 로그인하십시오. AWS Organizations https://console.aws.amazon.com/organizations/ IAM 사용자, IAM Identity Center의 사용자 또는 `AWSOrganizationsFullAccess` 관리형 정책 또는 이와 동등한 역할을 사용하는 역할로 로그인해야 합니다.
2. 공유 계정을 다시 조직에 초대하십시오. 계정을 초대하기 AWS Organizations위한 요구 사항, 전제 조건 및 절차에 대한 자세한 내용은 사용 설명서의 조직에 AWS 계정 초대를 참조하십시오.AWS Organizations
3. 제거된 공유 계정에 로그인한 다음 https://console.aws.amazon.com/organizations/home#/invites 으로 이동하여 초대를 수락하십시오.
4. 관리 계정에 다시 로그인합니다.
5. `AWSControlTowerServiceRolePolicy`관리형 정책 또는 이에 상응하는 정책을 사용하는 사용자 또는 역할로 AWS Control Tower 콘솔에 로그인하고 모든 AWS Control Tower 작업 (controltower: *) 을 실행할 수 있는 권한을 갖습니다.
6. 랜딩 존을 재설정하는 옵션이 있는 랜딩 존 드리프트 페이지가 표시됩니다. Reset을 선택하여 랜딩 존을 복구하십시오.
7. 재설정 프로세스가 완료될 때까지 기다리세요.

수정이 성공하면 공유 계정이 정상 상태 및 규정 준수 상태로 나타납니다.

수정 단계를 수행해도 계정이 복원되지 않으면 문의하세요. AWS Support

자동으로 업데이트되는 외부 변경 사항

계정 이메일 주소를 변경하면 AWS Control Tower에서 자동으로 업데이트되지만 Account Factory는 이를 자동으로 업데이트하지 않습니다.

관리되는 계정의 이메일 주소 변경

AWS Control Tower는 콘솔 환경에 필요한 대로 이메일 주소를 검색하고 표시합니다. 따라서 공유 및 기타 계정 이메일 주소는 변경 후 AWS Control Tower에 지속적으로 업데이트되고 표시됩니다.

> **Note**
>
> 에서 AWS Service Catalog Account Factory는 프로비저닝된 제품을 생성할 때 콘솔에 지정된 매개변수를 표시합니다. 그러나 계정 이메일 주소가 변경되는 경우 원래 계정 이메일 주소가 자동으로 업데이트되지 않습니다. 계정이 프로비저닝된 제품 내에 개념적으로 포함되어 있고 프로비저닝된 제품과 동일하지 않기 때문입니다. 이 값을 업데이트하려면 프로비저닝된 제품을 업데이트해야 하며, 그 결과로 관리 상태가 바뀔 수 있습니다.

외부 규칙 적용 AWS Config

AWS Control Tower는 AWS Control Tower 콘솔 외부에서 활성화된 AWS Config 규칙을 포함하여 AWS Control Tower에 등록된 조직 단위에 배포된 모든 규칙의 규정 준수 상태를 표시합니다.

AWS 컨트롤 타워 외부의 AWS 컨트롤 타워 리소스 삭제

AWS Control Tower에서 OU 및 계정을 삭제할 수 있으며 업데이트를 확인하기 위해 추가 조치를 취할 필요가 없습니다. Account Factory는 OU를 삭제하면 자동으로 업데이트되지만 계정을 삭제할 때는 업데이트되지 않습니다.

등록된 OU 삭제 (보안 OU 제외)

내에서 AWS Organizations API 또는 콘솔을 사용하여 빈 OU (조직 구성 단위) 를 제거할 수 있습니다. 계정이 포함된 OU는 삭제할 수 없습니다.

AWS Control Tower는 OU가 AWS Organizations 삭제되면 알림을 받습니다. 등록된 OU 목록이 일관되게 유지되도록 Account Factory의 OU 목록을 업데이트합니다.

> **Note**
>
> AWS Service Catalog에서는 계정을 프로비저닝할 수 있는 사용 가능한 OU 목록에서 삭제된 OU가 제거되도록 Account Factory가 업데이트되었습니다.

OU에서 등록된 계정 삭제

등록된 계정을 삭제하면 AWS Control Tower가 알림을 수신하고 정보를 업데이트하여 정보의 일관성을 유지합니다.

> **Note**
>
> 에서 AWS Service Catalog관리 계정을 나타내는 Account Factory에서 제공하는 제품은 계정을 삭제하도록 업데이트되지 않습니다. 대신 프로비저닝된 제품이 `TAINTED` 및 오류 상태로 표시됩니다. 정리하려면 AWS Service Catalog로 이동하여 프로비저닝된 제품을 선택한 다음 종료를 선택합니다.

AWS Control Tower를 사용하여 조직 및 계정을 관리합니다.

AWS Control Tower에서 생성하는 모든 조직 단위 (OU) 및 계정은 AWS Control Tower에 의해 자동으로 관리됩니다. 또한 AWS Control Tower 외부에서 생성된 기존 OU와 계정이 있는 경우 이를 AWS Control Tower 거버넌스로 가져올 수 있습니다.

기존 AWS Organizations 및 AWS 계정의 경우 대부분의 고객은 계정이 포함된 전체 조직 단위 (OU)를 등록하여 계정 그룹을 등록하는 것을 선호합니다. 계정을 개별적으로 등록할 수도 있습니다. 개별 계정 등록에 대한 자세한 내용은 을 참조하십시오. 기존 등록 AWS 계정

용어

- 기존 조직을 AWS Control Tower로 가져오는 것을 조직 등록 또는 조직으로 거버넌스 확장이라고 합니다.
- AWS 계정을 AWS Control Tower로 가져오는 것을 계정 등록이라고 합니다.

OU 및 계정 보기

AWS Control Tower 조직 페이지에서는 AWS Control Tower에 등록된 OU와 등록되지 않은 OU를 포함하여 귀사의 AWS Organizations모든 OU를 볼 수 있습니다. 계층 구조의 일부로 중첩된 OU를 볼 수 있습니다. 조직 페이지에서 조직 단위를 쉽게 볼 수 있는 방법은 오른쪽 상단의 드롭다운에서 조직 단위만 선택하는 것입니다.

조직 페이지에는 OU 또는 AWS Control Tower의 등록 상태와 상관없이 조직의 모든 계정이 나열됩니다. 조직 페이지에서 계정을 쉽게 볼 수 있는 방법은 오른쪽 상단의 드롭다운에서 계정만을 선택하는 것입니다. 계정이 등록 전제 조건을 충족하는 경우 OU 내에서 개별적으로 계정을 보고, 업데이트하고, 등록할 수 있습니다.

필터링을 선택하지 않으면 조직 페이지에 계정과 OU가 계층 구조로 표시됩니다. 모든 AWS Control Tower 리소스를 모니터링하고 조치를 취할 수 있는 중앙 위치입니다. 조직 페이지에 대한 자세한 내용은 안내 동영상을 참조하십시오.

비디오 안내

이 동영상 (4:01) 은 AWS Control Tower에서 조직 페이지를 사용하는 방법을 설명합니다. 동영상 오른쪽 하단에 있는 아이콘을 선택하여 전체 화면으로 확대하면 더 잘 보입니다. 자막을 사용할 수 있습니다.

AWS Control Tower의 조직 페이지 활용에 대한 동영상 안내

주제

- 기존 조직 단위를 AWS Control Tower에 등록
- 기존 등록 AWS 계정

거버넌스를 기존 조직으로 확장하십시오.

시작하기, 2단계의 AWS Control Tower 사용 설명서에 설명된 대로 랜딩 존 (LZ) 을 설정하여 기존 조직에 AWS Control Tower 거버넌스를 추가할 수 있습니다.

기존 조직에 AWS Control Tower 랜딩 존을 설정할 때 예상되는 사항은 다음과 같습니다.

- AWS Organizations 조직당 하나의 랜딩 존을 가질 수 있습니다.
- AWS Control Tower는 기존 AWS Organizations 조직의 관리 계정을 관리 계정으로 사용합니다. 새 관리 계정은 필요하지 않습니다.
- AWS Control Tower는 등록된 OU에 감사 계정과 로깅 계정이라는 두 개의 새 계정을 설정합니다.
- 조직의 서비스 한도가 이러한 두 개의 추가 계정을 만들 수 있도록 허용해야 합니다.
- 랜딩 존을 시작하거나 OU를 등록한 후에는 AWS Control Tower 컨트롤이 해당 OU에 등록된 모든 계정에 자동으로 적용됩니다.
- AWS Control Tower에서 관리하는 OU에 기존 AWS 계정을 추가로 등록하여 해당 계정에 제어가 적용되도록 할 수 있습니다.
- AWS Control Tower에서 OU를 더 추가하고 기존 OU를 등록할 수 있습니다.

등록 및 등록을 위한 기타 사전 요구 사항을 확인하려면 AWS Control Tower 시작하기를 참조하십시오.

다음은 AWS Control Tower 랜딩 존이 설정되지 않은 AWS 조직의 OU에 AWS Control Tower 컨트롤이 적용되지 않는 방법에 대한 자세한 내용입니다.

- AWS Control Tower Account Factory 외부에서 생성된 새 계정은 등록된 OU의 제어 항목에 구속되지 않습니다.
- AWS Control Tower에 등록되지 않은 OU에서 생성된 새 계정은 AWS Control Tower에 해당 계정을 특별히 등록하지 않는 한 규제 항목의 구속을 받지 않습니다. 계정 등록에 대한 자세한 내용은 기존 등록 AWS 계정 단원을 참조하십시오.

- 추가 기존 조직, 기존 계정, 새 OU 또는 AWS Control Tower 외부에서 생성한 모든 계정은 OU를 별도로 등록하거나 계정을 등록하지 않는 한 AWS Control Tower 제어에 구속되지 않습니다.

기존 OU 및 계정에 AWS Control Tower를 적용하는 방법에 대한 자세한 내용은 을 참조하십시오기존 조직 단위를 AWS Control Tower에 등록.

기존 조직에 AWS Control Tower 랜딩 존을 설정하는 프로세스의 개요는 다음 섹션의 비디오를 참조하십시오.

> **Note**
>
> 설정 중에 AWS Control Tower는 일반적인 문제를 방지하기 위해 사전 점검을 수행합니다. 그러나 현재 Landing Zone 솔루션을 사용하고 있다면 조직에서 AWS Control Tower를 활성화하기 전에 AWS 솔루션스 아키텍트에게 문의하여 AWS Control Tower가 현재 랜딩 존 배포를 방해할 수 있는지 확인하십시오. AWS AWS Organizations또한 한 착륙 지대에서 다른 착륙 지대로 계정을 이동하는 방법에 대한 자세한 내용은 을 참조하십시오계정이 사전 요구 사항을 충족하지 않으면 어떻게 됩니까?.

동영상: 기존 랜딩 존 활성화 AWS Organizations

이 동영상 (7:48) 에서는 기존 AWS Organizations 구조물에 AWS Control Tower 랜딩 존을 설정하고 활성화하는 방법을 설명합니다. 동영상 오른쪽 하단에 있는 아이콘을 선택하여 전체 화면으로 확대하면 더 잘 보입니다. 자막을 사용할 수 있습니다.

기존 조직을 위한 AWS Control Tower 활성화

IAM ID 센터 및 기존 조직에 대한 고려 사항

- AWS IAM Identity Center (IAM ID 센터) 가 이미 설정되어 있는 경우, AWS Control Tower 홈 지역은 IAM 자격 증명 센터 지역과 동일해야 합니다.
- AWS Control Tower는 기존 구성을 삭제하지 않습니다.
- IAM Identity Center가 이미 활성화되어 있고 IAM Identity Center 디렉터리를 사용하는 경우, AWS Control Tower는 권한 집합, 그룹 등과 같은 리소스를 추가하고 평소와 같이 진행합니다.
- 다른 디렉터리 (외부, AD, Managed AD) 가 설정된 경우, AWS Control Tower는 기존 구성을 변경하지 않습니다. 자세한 내용은 AWS IAM Identity Center (IAM ID 센터) 고객을 위한 고려 사항를 참조하세요.

다른 AWS 서비스에 대한 액세스

조직을 AWS Control Tower 거버넌스로 전환한 후에도 AWS Organizations 콘솔과 API를 통해 AWS Organizations제공되는 모든 AWS 서비스에 계속 액세스할 수 있습니다. 자세한 내용은 관련 AWS 서비스을(를) 참조하세요.

AWS Control Tower의 중첩된 OU

이 장에서는 AWS Control Tower에서 중첩된 OU를 사용할 때 알아두어야 할 기대치와 고려 사항을 나열합니다. 대부분의 측면에서 중첩된 OU를 사용하는 것은 플랫 OU 구조를 사용하는 것과 같습니다. 등록 및 재등록 기능은 이 장에 설명된 변경된 동작을 제외하고 중첩된 OU에서 작동합니다.

비디오 안내

이 동영상 (4:46) 은 AWS Control Tower에서 중첩된 OU 배포를 관리하는 방법을 설명합니다. 동영상 오른쪽 하단에 있는 아이콘을 선택하여 전체 화면으로 확대하면 더 잘 보입니다. 자막을 사용할 수 있습니다.

AWS Control Tower의 중첩된 OU 관리에 대한 동영상 설명.

중첩된 OU 및 랜딩 존의 모범 사례에 대한 지침은 AWS Control Tower 랜딩 존을 중첩된 OU로 구성하기 블로그 게시물을 참조하십시오.

플랫 OU 구조에서 중첩된 OU 구조로 확장

플랫 OU 구조로 AWS Control Tower 랜딩 존을 생성한 경우, 이를 중첩된 OU 구조로 확장할 수 있습니다.

이 프로세스에는 네 가지 주요 단계가 있습니다.

1. AWS Control Tower에서 원하는 중첩된 OU 구조를 생성합니다.
2. AWS Organizations 콘솔로 이동하여 대량 이동 기능을 사용하여 계정을 원본 OU (플랫) 에서 대상 OU (중첩) 로 이동합니다. 방법은 다음과 같습니다.
   a. 계정을 옮기려는 OU로 이동합니다.
   b. OU의 모든 계정을 선택합니다.
   c. 이동을 선택합니다.

> **Note**
>
> AWS Control Tower에는 Move 기능이 없으므로 이 단계는 AWS Organizations 콘솔에서 수행해야 합니다.

3. AWS Control Tower의 중첩된 OU로 이동하여 등록하거나 재등록하십시오. 중첩된 OU의 모든 계정이 등록됩니다.
   - AWS Control Tower에서 OU를 생성한 경우 OU를 다시 등록하십시오.
   - 에서 AWS Organizations OU를 생성한 경우 처음으로 OU를 등록하십시오.
4. 계정을 이동하고 등록한 후에는 AWS Organizations 콘솔이나 AWS Control Tower 콘솔에서 비어 있는 최상위 OU를 삭제합니다.

중첩된 OU 등록 사전 검사

중첩된 OU와 해당 멤버 계정을 성공적으로 등록할 수 있도록 AWS Control Tower는 일련의 사전 검사를 수행합니다. 최상위 OU 또는 중첩된 OU를 등록할 때도 이와 동일한 사전 점검이 수행됩니다. 자세한 내용은 등록 또는 재등록 중 발생하는 일반적인 실패 원인을 참조하십시오.

- 모든 사전 점검을 통과하면 AWS Control Tower가 자동으로 OU 등록을 시작합니다.
- 사전 검사에 실패할 경우, AWS Control Tower는 등록 프로세스를 중단하고 OU를 등록하기 전에 수정해야 하는 항목 목록을 제공합니다.

중첩된 OU 및 역할

AWS Control Tower는 대상 OU의 계정과 대상 OU 아래에 중첩된 모든 OU의 계정에 `AWSControlTowerExecution` 역할을 배포합니다. 대상 OU만 등록하려는 경우에도 마찬가지입니다. 이 역할은 관리 계정 관리자의 모든 사용자에게 해당 역할이 있는 모든 계정에 대한 권한을 부여합니다`AWSControlTowerExecution`. 이 역할은 일반적으로 AWS Control Tower 컨트롤에서 허용되지 않는 작업을 수행하는 데 사용할 수 있습니다.

등록할 계획이 없는 미등록 계정에서 이 역할을 삭제할 수 있습니다. 이 역할을 삭제하면 역할을 계정에 복원하지 않는 한 AWS Control Tower에 계정을 등록하거나 직계 상위 OU를 등록할 수 없습니다. 계정에서 `AWSControlTowerExecution` 역할을 삭제하려면 해당 역할로 로그인해야 합니다. 다른 IAM 보안 주체는 AWS Control Tower에서 관리하는 역할을 삭제할 수 없기 때문입니다. `AWSControlTowerExecution`

역할 액세스를 제한하는 방법에 대한 자세한 내용은 역할 신뢰 관계의 선택적 조건을 참조하십시오.

중첩된 OU 및 계정을 등록하고 재등록하면 어떻게 되나요?

중첩된 OU를 등록하거나 재등록하면 AWS Control Tower는 대상 OU의 모든 미등록 계정을 등록하고 등록된 모든 계정을 업데이트합니다. 예상 사항은 다음과 같습니다.

AWS Control Tower는 다음과 같은 작업을 수행합니다.

- 이 OU에 등록되지 않은 모든 계정과 중첩된 OU의 모든 미등록 계정에 `AWSControlTowerExecution` 역할을 추가합니다.
- 등록되지 않은 구성원 계정을 등록합니다.
- 등록된 회원 계정을 재등록합니다.
- 새로 등록한 회원 계정을 위한 IAM ID 센터 로그인을 생성합니다.
- 기존 등록 회원 계정을 업데이트하여 landding Zone 변경 사항을 반영합니다.
- 이 OU 및 해당 구성원 계정에 대해 구성된 컨트롤을 업데이트합니다.

중첩된 OU 등록 고려 사항

- 핵심 OU (보안 OU) 에서는 OU를 등록할 수 없습니다.
- 중첩된 OU는 별도로 등록해야 합니다.
- 상위 OU가 등록되어 있지 않으면 OU를 등록할 수 없습니다.
- 트리의 상위에 있는 모든 OU가 일정 시점에 성공적으로 등록되지 않으면 (일부는 삭제되었을 수 있음) OU를 등록할 수 없습니다.
- 드리프트된 상위 OU에 속하는 OU를 등록할 수는 있지만 해당 작업으로 인한 편차는 복구되지 않습니다.

중첩된 OU 제한

- OU는 루트 아래에 최대 5단계까지 중첩될 수 있습니다.
- 대상 OU 아래의 중첩된 OU는 별도로 등록하거나 다시 등록해야 합니다.
- 대상 OU가 계층 구조에서 레벨 2 이하인 경우, 즉 최상위 OU가 아닌 경우 상위 OU에서 활성화된 예방 제어가 이 OU와 그 아래의 모든 OU에 자동으로 적용됩니다.
- OU 등록 실패는 계층 트리 위로 전파되지 않습니다. 상위 OU 세부 정보 페이지에서 중첩된 OU 상태에 대한 세부 정보를 볼 수 있습니다.

- OU 등록 실패는 계층 구조 트리 아래로 전파되지 않습니다.
- AWS Control Tower는 신규 또는 기존 계정의 VPC 설정을 수정하지 않습니다.

중첩된 OU 및 규정 준수

AWS Control Tower 콘솔에서는 조직 페이지에서 규정을 준수하지 않는 OU 및 계정을 볼 수 있으므로 규정 준수를 더 큰 규모로 이해할 수 있습니다.

중첩된 OU 및 계정의 규정 준수에 대한 고려 사항

- OU의 규정 준수는 OU 아래에 중첩된 OU의 규정 준수를 기반으로 결정되지 않습니다.
- 컨트롤의 규정 준수 상태는 중첩된 OU를 포함하여 컨트롤이 활성화된 모든 OU에서 계산됩니다. OU 및 계정의 AWS Control Tower 규정 준수 상태를 참조하십시오.
- OU가 OU 계층 구조에서 어느 위치에 있든 관계없이 OU에 규정을 준수하지 않는 계정이 있는 경우에만 OU가 비준수로 표시됩니다.
- 중첩된 OU가 규정을 준수하지 않는 경우 상위 OU는 자동으로 비규격으로 간주되지 않습니다.
- OU 세부 정보 또는 계정 세부 정보 페이지에서 OU 또는 계정이 비준수 상태로 표시되는 원인이 될 수 있는 비준수 리소스 목록을 볼 수 있습니다.

중첩된 OU 및 드리프트

특정 상황에서는 드리프트로 인해 중첩된 OU가 등록되지 않을 수 있습니다.

드리프트 및 중첩된 OU에 대한 기대

- 상위 항목이 드리프트된 OU에서는 제어를 활성화할 수 있지만, 드리프트된 OU에서는 직접 제어할 수 없습니다.
- 최상위 드리프트된 OU가 아닌 한, 드리프트된 OU에서 탐지 제어를 활성화할 수 있습니다.
- 필수 제어는 최상위 OU에서만 사용할 수 있습니다. 중첩된 OU를 등록할 때는 필수 컨트롤이 생략됩니다.
- 하나의 필수 컨트롤은 AWS Config 리소스를 보호합니다. 따라서 중첩된 OU를 등록하려면 해당 컨트롤이 비드리프트 상태여야 합니다. 표류하는 경우 AWS Control Tower는 중첩된 OU의 등록을 차단합니다.
- 최상위 OU가 드리프트 상태인 경우 AWS Config 리소스를 보호하는 제어가 유동적일 수 있습니다. 이 상황에서 AWS Control Tower는 탐정 제어 적용을 포함하여 AWS Config 리소스 생성 또는 업데이트가 필요한 모든 작업을 차단합니다.

중첩된 OU 및 제어

등록된 OU에서 컨트롤을 활성화하면 예방 컨트롤과 탐지 컨트롤의 동작이 다릅니다. 중첩된 OU의 경우 사전 예방적 제어는 탐지 제어와 유사하게 작동합니다.

예방적 통제

- 예방적 통제는 중첩된 OU에 적용됩니다.
- 필수 예방 통제는 OU 및 중첩된 OU의 모든 계정에 적용됩니다.
- 예방 통제는 대상 OU에 중첩된 모든 계정과 OU에 영향을 미치며, 해당 계정과 OU가 등록되지 않았더라도 마찬가지입니다.

Detective 및 사전 예방적 제어

- 중첩된 OU는 탐지 제어 또는 사전 예방 제어를 자동으로 상속하지 않으므로 별도로 활성화해야 합니다.
- Detective 및 사전 예방적 제어는 랜딩 존의 운영 지역에 등록된 계정에만 배포됩니다.

제어 상태 및 상속을 활성화했습니다.

OU 세부 정보 페이지에서 각 OU에 대해 상속된 컨트롤을 볼 수 있습니다.

> **Tip**
>
> 제어 상속을 활용하여 OU의 SCP 할당량을 넘지 않도록 할 수 있습니다. 예를 들어 중첩된 OU에 직접 사용하도록 설정하는 대신 OU 계층 구조의 최상위 OU에서 컨트롤을 사용하도록 설정할 수 있습니다.

상속된 상태

- 상속 상태는 컨트롤이 상속을 통해서만 활성화되고 OU에 직접 적용되지는 않았음을 나타냅니다.
- Enabled 상태는 다른 OU의 상태에 관계없이 이 OU에 제어가 적용됨을 의미합니다.
- 실패 상태는 다른 OU의 상태와 상관없이 이 OU에 제어가 적용되지 않음을 의미합니다.

> **Note**
>
> 상속 상태는 컨트롤이 트리의 상위에 있는 OU에 적용되어 이 OU에 적용되었지만 이 OU에 직접 추가되지는 않았음을 나타냅니다.

> **랜딩 존이 최신 버전이 아닌 경우**
>
> 사용 가능 컨트롤 표의 각 행은 개별 OU 하나에 대해 활성화된 컨트롤 하나를 나타냅니다.

중첩된 OU 및 루트

루트는 OU가 아니므로 등록하거나 다시 등록할 수 없습니다. 또한 루트에서 직접 계정을 만들 수 없습니다. 루트는 규정을 준수하지 않거나 등록 또는 변경 중과 같은 수명 주기 상태를 가질 수 없습니다.

하지만 루트는 모든 계정과 OU의 최상위 컨테이너입니다. 중첩된 OU의 경우 이 노드는 다른 모든 OU가 중첩되는 노드입니다.

기존 조직 단위를 AWS Control Tower에 등록

여러 기존 AWS 계정을 AWS Control Tower로 가져오는 효율적인 방법은 AWS Control Tower의 거버넌스를 전체 조직 단위 (OU) 로 확장하는 것입니다.

로 AWS Organizations생성된 기존 OU와 해당 계정에 대한 AWS Control Tower 거버넌스를 활성화하려면 OU를 AWS Control Tower 랜딩 존에 등록하십시오. 최대 300개의 계정을 포함하는 OU를 등록할 수 있습니다. OU에 포함된 계정이 300개가 넘는 경우 AWS Control Tower에 등록할 수 없습니다.

OU를 등록하면 OU의 멤버 계정이 AWS Control Tower 랜딩 존에 등록됩니다. OU에 적용되는 컨트롤에 의해 관리됩니다.

> **Note**
>
> 아직 AWS Control Tower 랜딩 존이 없는 경우 먼저 AWS Control Tower에서 만든 새 조직이나 기존 AWS Organizations 조직에 랜딩 존을 설정하십시오. 착륙 지대를 설정하는 방법에 대한 자세한 내용은 을 참조하십시오AWS Control Tower 시작하기.

OU를 등록하면 내 계정은 어떻게 되나요?

AWS Control Tower에는 조직 내 계정에 스택을 자동으로 AWS CloudFormation 배포할 수 있도록 사용자 간에 AWS CloudFormation 또는 사용자를 대신하여 신뢰할 수 있는 액세스를 설정할 수 있는 권한이 필요합니다. AWS Organizations

- 등록되지 않음 상태인 모든 계정에 `AWSControlTowerExecution` 역할이 추가됩니다.
- OU를 등록하면 OU와 해당 OU의 모든 계정에 기본적으로 필수 제어 기능이 활성화됩니다.

OU를 등록한 후 계정을 부분적으로 등록합니다.

OU를 성공적으로 등록할 수는 있지만 일부 계정은 등록되지 않은 상태로 남아 있을 수 있습니다. 그렇다면 이러한 계정은 등록을 위한 사전 요구 사항 중 일부를 충족하지 못합니다. OU 등록 프로세스의 일부로 계정을 등록하지 못하면 계정 페이지의 계정 상태가 등록 실패로 표시됩니다. OU 페이지의 계정 필드에서 4/5와 같은 계정 정보를 볼 수도 있습니다.

예를 들어 5개 중 4개가 표시되면 OU에 총 5개의 계정이 있고 그 중 4개는 성공적으로 등록되었지만 한 개의 계정은 OU 등록 프로세스 중에 등록에 실패했음을 의미합니다. 계정이 등록 사전 요구 사항을 충족하는지 확인한 후 OU 재등록을 선택하여 계정을 등록할 수 있습니다.

OU 등록을 위한 IAM 사용자 사전 요구 사항

이미 권한이 `Admin` 있더라도 OU 등록 작업을 수행할 때 (IAM) ID (사용자 또는 역할) 또는 IAM Identity Center 사용자 ID가 적절한 Account Factory 포트폴리오에 포함되어야 합니다. AWS Identity and Access Management 그렇지 않으면 등록 중에 프로비저닝된 제품을 생성할 수 없습니다. AWS Control Tower가 OU를 등록할 때 IAM 사용자의 자격 증명 또는 IAM ID 센터 사용자 자격 증명을 사용하기 때문에 오류가 발생합니다.

관련 포트폴리오는 AWS 컨트롤 타워에서 만든 것으로, AWS 컨트롤 타워 어카운트 팩토리 포트폴리오라고 합니다. 서비스 카탈로그 > 어카운트 팩토리 > AWS Control Tower 어카운트 팩토리 포트폴리오를 선택하여 해당 페이지로 이동하십시오. 그런 다음 그룹, 역할 및 사용자라는 탭을 선택하여 IAM 또는 IAM ID 센터 ID를 확인하십시오. 액세스 권한을 부여하는 방법에 대한 자세한 내용은 설명서를 참조하십시오. AWS Service Catalog

기존 OU 등록

AWS Control Tower 콘솔의 조직 페이지에서는 AWS Control Tower에 등록된 OU와 등록되지 않은 OU를 포함하여 조직의 모든 OU 및 계정을 계층 구조로 볼 수 있습니다.

일반적으로 등록되지 않은 OU는 에서 AWS Organizations생성되었으며 다른 랜딩 존의 적용을 받지 않습니다. 최대 300개의 계정을 포함하는 기존 OU를 등록할 수 있습니다. OU에 포함된 계정이 300개가 넘는 경우 AWS Control Tower에 등록할 수 없습니다.

기존 OU를 등록하려면

1. https://console.aws.amazon.com/controltower 에서 AWS 컨트롤 타워 콘솔에 로그인합니다.
2. 왼쪽 창 탐색 메뉴에서 조직을 선택합니다.
3. 조직 페이지에서 등록하려는 OU 옆의 라디오 버튼을 선택한 다음 오른쪽 상단의 작업 드롭다운 메뉴에서 조직 단위 등록을 선택하거나, OU 이름을 선택하여 해당 OU의 OU 세부 정보 페이지를 볼 수 있습니다.
4. OU 세부 정보 페이지의 오른쪽 상단에 있는 작업 드롭다운 메뉴에서 OU 등록을 선택할 수 있습니다.

등록 프로세스는 거버넌스를 OU로 확장하는 데 최소 10분, 추가 계정당 최대 2분이 추가로 소요됩니다.

기존 OU 등록 결과

기존 OU를 등록하면 `AWSControlTowerExecution` 역할을 통해 AWS Control Tower가 거버넌스를 개별 계정으로 확장할 수 있습니다. 가드레일이 적용되고 계정 활동에 대한 정보가 감사 및 로깅 계정에 보고됩니다.

기타 결과는 다음과 같습니다.

- `AWSControlTowerExecution`을 통해 AWS Control Tower 감사 계정이 감사를 수행할 수 있습니다.
- `AWSControlTowerExecution`모든 계정의 모든 로그가 로깅 계정으로 전송되도록 조직의 로깅을 구성하는 데 도움이 됩니다.
- `AWSControlTowerExecution`선택한 AWS Control Tower 제어 항목이 OU의 모든 개별 계정과 AWS Control Tower에서 생성하는 모든 새 계정에 자동으로 적용되도록 합니다.

등록된 OU의 경우, AWS Control Tower 컨트롤에 구현된 감사 및 로깅 기능을 기반으로 규정 준수 및 보안 보고서를 제공할 수 있습니다. 보안 및 규정 준수 팀은 모든 요구 사항이 충족되었는지 그리고 조직 드리프트가 발생하지 않았는지 확인할 수 있습니다. 드리프트에 대한 자세한 내용은 을 참조하십시오. AWS Control Tower의 드리프트 감지 및 해결

> **Note**
>
> AWS Control Tower가 OU와 해당 계정을 표시할 때 한 가지 특이한 상황이 발생할 수 있습니다. 등록된 OU에서 계정을 생성한 후 해당 등록된 계정을 등록되지 않은 다른 OU로 옮기는 경

우, 특히 계정을 AWS Organizations 이전하는 데 사용한 경우 OU 세부 정보 페이지에서 결과 “1 of 0” 계정을 확인할 수 있습니다. 또한 등록되지 않은 OU에 등록되지 않은 다른 계정을 생성했을 수도 있습니다. 등록되지 않은 계정이 있는 경우 콘솔에 해당 OU의 “1/1"이 표시될 수 있습니다. 새로 만든 단일 계정이 등록된 것처럼 보이지만 실제로는 그렇지 않습니다. 새 계정을 등록해야 합니다.

새 OU 생성

AWS 컨트롤 타워에서 새 OU를 만들려면

1. 조직 페이지로 이동합니다.
2. 오른쪽 상단의 리소스 생성 드롭다운 메뉴에서 조직 단위 생성을 선택합니다.
3. OU 이름 필드에 이름을 지정합니다.
4. 상위 OU 드롭다운에서 등록된 OU의 계층 구조를 볼 수 있습니다. 만들고 있는 새 OU의 상위 OU를 선택합니다.
5. 추가를 선택합니다.

Tip

간단한 단계로 중첩된 OU를 추가하려면 조직 페이지의 표에 표시된 상위 OU의 이름을 선택하고 해당 상위 OU의 OU 페이지를 확인한 다음 오른쪽 상단의 작업 드롭다운 메뉴에서 OU 추가를 선택합니다. 새 OU는 선택한 OU 아래에 중첩된 OU로 자동 생성됩니다.

Note

Landing Zone이 최신 상태가 아닌 경우 드롭다운 메뉴에 계층 구조 대신 단순 목록이 표시됩니다. 랜딩 영역에 중첩된 OU가 포함되어 있더라도 L5 OU 아래에 새 OU를 생성할 수 없으므로 드롭다운에 L5 OU가 표시되지 않습니다. AWS Control Tower의 중첩된 OU에 대한 자세한 내용은 을 참조하십시오AWS Control Tower의 중첩된 OU.

등록 또는 재등록 시 발생하는 일반적인 실패 원인

OU 또는 해당 구성원 계정의 등록 (또는 재등록) 이 실패할 경우, 어떤 사전 검사를 통과하지 못했는지를 보여주는 상세 보고서가 들어 있는 파일을 다운로드할 수 있습니다. 등록 영역 오른쪽 상단에 나타나는 다운로드 버튼을 선택하여 다운로드를 완료할 수 있습니다.

이 섹션에는 사전 확인이 실패할 경우 발생할 수 있는 오류 유형과 오류 수정 방법이 나와 있습니다.

일반적으로 OU를 등록하거나 재등록하면 해당 OU 내의 모든 계정이 AWS Control Tower에 등록됩니다. 하지만 OU 전체가 성공적으로 등록되었더라도 일부 계정은 등록에 실패할 수 있습니다. 이러한 경우에는 계정과 관련된 사전 확인 실패를 해결한 다음 해당 계정이나 OU를 다시 등록해 봐야 합니다.

랜딩 존 오류

- 랜딩 존이 준비되지 않았습니다.

  현재 랜딩 존을 재설정하거나 최신 버전으로 업데이트하세요.

OU 오류

- 최대 SCP 수를 초과했습니다.

  OU당 서비스 제어 정책 (SCP) 한도를 초과했거나 다른 할당량에 도달했을 수 있습니다. AWS Control Tower 랜딩 존에 있는 모든 OU에는 OU당 5개의 SCP 제한이 적용됩니다. 할당량이 허용하는 것보다 많은 SCP가 있는 경우 SCP를 삭제하거나 통합해야 합니다.
- 충돌하는 SCP

  기존 SCP를 OU 또는 계정에 적용할 수 있으며, 이로 인해 AWS Control Tower가 계정을 등록하지 못할 수 있습니다. 적용된 SCP에서 AWS Control Tower의 작동을 방해할 수 있는 정책이 있는지 확인하십시오. 계층 구조 상위에 있는 OU로부터 물려받은 SCP를 반드시 확인하십시오.
- 스택 세트 할당량을 초과했습니다.

  스택 세트 할당량이 초과되었을 수 있습니다. 할당량이 허용하는 것보다 많은 인스턴스가 있는 경우 일부 스택 인스턴스를 삭제해야 합니다. 자세한 내용은, AWS CloudFormation 사용 설명서의 AWS CloudFormation 할당량 섹션을 참조하십시오.
- 계정 한도를 초과했습니다.

  AWS Control Tower는 등록 시 각 OU를 300개의 계정으로 제한합니다.

계정 오류

- 계정에 대한 사전 확인 금지

  OU의 기존 SCP는 AWS Control Tower가 OU 멤버 계정에 대한 사전 확인을 수행하지 못하게 합니다. 이 사전 확인 실패를 해결하려면 OU에서 SCP를 업데이트하거나 제거하십시오.

- 이메일 주소 오류

  계정에 지정한 이메일 주소가 이름 지정 표준을 준수하지 않습니다. 다음은 허용되는 문자를 지정하는 정규 표현식 (regex) 입니다. `[A-Z0-9a-z._%+-]+@[A-Za-z0-9.-]+[.]+[A-Za-z]+`

- Config 레코더 또는 전송 채널 사용

  계정에 기존 AWS Config 구성 레코더 또는 전송 채널이 있을 수 있습니다. 계정을 등록하려면 먼저 AWS Control Tower 관리 계정의 리소스가 관리되는 모든 AWS CLI AWS 지역에서 삭제하거나 수정해야 합니다.

- STS는 비활성화되었습니다.

  AWS Security Token Service 계정에서 (AWS STS) 이 비활성화될 수 있습니다. AWS AWS Control Tower에서 지원하는 모든 지역의 계정에서 STS 엔드포인트를 활성화해야 합니다.

- IAM ID 센터 충돌

  AWS Control Tower 홈 지역은 AWS IAM Identity Center (IAM ID 센터) 지역과 동일하지 않습니다. IAM 자격 증명 센터가 이미 설정되어 있는 경우, AWS Control Tower 홈 지역은 IAM 자격 증명 센터 지역과 동일해야 합니다.

- 상충되는 SNS 주제

  계정에는 AWS 컨트롤 타워가 사용해야 하는 아마존 심플 알림 서비스 (Amazon SNS) 주제 이름이 있습니다. AWS Control Tower는 특정 이름을 가진 리소스 (예: SNS 주제) 를 생성합니다. 이러한 이름을 이미 사용한 경우 AWS Control Tower 설정이 실패합니다. 이전에 AWS Control Tower에 등록한 계정을 다시 사용하는 경우 이러한 상황이 발생할 수 있습니다.

- 일시 중단된 계정이 감지되었습니다.

  이 계정은 일시 중지되었습니다. AWS Control Tower에는 등록할 수 없습니다. 이 OU에서 계정을 제거하고 다시 시도하십시오.

- 포트폴리오에 없는 IAM 사용자

  OU를 등록하기 전에 Service Catalog 포트폴리오에 AWS Identity and Access Management (IAM) 사용자를 추가합니다. 이 오류는 관리 계정에만 해당됩니다.

- 계정이 사전 요구 사항을 충족하지 않음

  계정이 계정 등록을 위한 사전 요구 사항을 충족하지 않습니다. 예를 들어, 계정에 계정을 AWS Control Tower에 등록하는 데 필요한 역할 및 권한이 누락되었을 수 있습니다. 역할 추가 지침은 에서 확인할 수 있습니다. 필요한 IAM 역할을 기존 역할에 수동으로 AWS 계정 추가하고 등록하십시오.

다시 말씀드리지만, AWS Control Tower에 계정을 등록하면 모든 AWS 계정에서 자동으로 AWS CloudTrail 활성화됩니다. 등록 전에 계정에서 활성화된 경우 CloudTrail 등록 프로세스를 시작하기 전에 CloudTrail 비활성화하지 않는 한 이중 청구가 발생할 수 있습니다.

조직 업데이트

OU (조직 구성 단위) 를 업데이트하거나 OU 내 여러 계정을 업데이트하는 가장 빠른 방법은 OU를 다시 등록하는 것입니다.

AWS 컨트롤 타워 OU 및 계정 업데이트 시기

Landning Zone 업데이트를 수행할 때는 등록된 계정을 업데이트하여 해당 계정에 새 제어 기능을 적용해야 합니다.

- 재등록 옵션을 사용하여 OU에 속한 모든 계정을 업데이트할 수 있습니다.
- landing Zone에 등록된 OU가 두 개 이상인 경우 모든 OU를 다시 등록하여 모든 계정을 업데이트하십시오.
- 단일 계정을 업데이트하려면 AWS Control Tower 콘솔에서 업데이트하거나 에서 프로비저닝된 제품 업데이트 옵션을 선택할 수 있습니다. AWS Service Catalog콘솔에서 계정 업데이트 섹션을 참조하십시오.

동일한 OU에서 여러 계정을 업데이트하십시오.

한 번의 작업으로 한 OU의 여러 계정을 업데이트하려면

1. https://console.aws.amazon.com/controltower 에서 AWS Control Tower 콘솔에 로그인합니다.
2. 왼쪽 창 탐색 메뉴에서 조직을 선택합니다.
3. 조직 페이지에서 원하는 OU를 선택하여 OU 세부 정보 페이지를 확인합니다.
4. 오른쪽 상단의 작업에서 OU 재등록을 선택합니다.

모든 계정과 OU를 업데이트해야 하는 경우 AWS Control Tower 조직의 각 OU에 대해 이 단계를 반복합니다.

또는 업데이트 가능 상태가 표시된 계정을 선택한 다음 필요한 만큼 계정 업데이트를 선택할 수도 있습니다.

재등록 중에는 어떻게 되나요?

OU를 재등록하는 경우:

- State 필드에는 계정이 현재 AWS Control Tower에 등록되어 있는지 (등록), 계정이 등록된 적이 없는지 (등록되지 않음), 이전에 등록이 실패했는지 (등록 실패) 가 표시됩니다.
- OU를 재등록하면 [등록 안 됨] 또는 [등록 실패] 상태의 모든 계정에 **`AWSControlTowerExecution`** 역할이 추가됩니다.
- AWS Control Tower는 새로 등록된 계정에 대해 싱글 사인온 (IAM ID 센터) 로그인을 생성합니다.
- 등록된 계정은 AWS Control Tower에 재등록됩니다.
- SCP가 기본 정의로 돌아가기 때문에 OU에 적용된 모든 예방 제어에 대한 편차가 수정되었습니다.
- 모든 계정은 최신 landing Zone 변경 사항을 반영하도록 업데이트됩니다.

자세한 설명은 기존 등록 AWS 계정 섹션을 참조하세요.

> **Tip**
>
> OU를 다시 등록하거나 landing zone 버전과 여러 구성원 계정을 업데이트할 때 -를 언급하는 실패 메시지가 표시될 수 있습니다. StackSet AWSControlTowerExecutionRole 등록된 모든 멤버 계정에 AWSControlTowerExecutionIAM 역할이 이미 존재하므로 관리 StackSet 계정에서 이 작업이 실패할 수 있습니다. 이 오류 메시지는 예상된 동작이므로 무시해도 됩니다.

단일 계정 업데이트

AWS Control Tower 콘솔 또는 Service Catalog 콘솔에서 개별 AWS Control Tower 계정을 업데이트할 수 있습니다.

AWS Control Tower 콘솔에서 단일 계정을 업데이트하려면 을 참조하십시오콘솔에서 계정 업데이트.

에서 단일 계정을 업데이트하려면 AWS Service Catalog

1. AWS Service Catalog로 이동합니다.
2. 왼쪽 창 탐색 메뉴에서 프로비저닝된 제품을 선택합니다.
3. 프로비저닝된 제품 페이지에서 업데이트하려는 프로비저닝된 제품 옆에 있는 라디오 버튼을 선택합니다.
4. 오른쪽 상단에서 작업 드롭다운을 선택하여 업데이트합니다.

에서 AWS Service Catalog업데이트하는 방법에 대한 자세한 내용은 Service Catalog 관리자 안내서의 제품 업데이트를 참조하십시오프로비저닝된 제품 업데이트.

통합 서비스

AWS Control Tower는 다른 AWS 서비스를 기반으로 구축된 서비스로, 잘 설계된 환경을 설정하는 데 도움이 됩니다. 이 장에서는 기본 서비스에 대한 구성 정보와 기본 서비스가 AWS Control Tower에서 작동하는 방식을 포함하여 이러한 서비스에 대한 간략한 개요를 제공합니다.

잘 설계된 환경을 측정하는 방법에 대한 자세한 내용은 Well-Architected 도구에 대해 알아보십시오.AWS 관리 및 거버넌스 클라우드 환경 가이드도 참조하십시오.

주제

- 다음을 사용하여 환경을 배포하십시오. AWS CloudFormation
- 를 사용하여 이벤트를 모니터링하십시오. CloudTrail
- 다음을 통해 리소스 및 서비스를 모니터링할 수 있습니다. CloudWatch
- 다음을 사용하여 리소스 구성을 관리하십시오. AWS Config
- IAM으로 엔티티에 대한 권한 관리
- AWS Key Management Service
- Lambda를 사용하여 서버리스 컴퓨팅 함수 실행
- 다음을 통해 계정을 관리합니다. AWS Organizations
- Amazon S3를 사용하여 객체 저장
- Security Hub로 환경을 모니터링하세요
- 다음을 통해 계정을 프로비저닝합니다. AWS Service Catalog
- Amazon 심플 알림 서비스를 통한 알림 추적
- 를 사용하여 분산 애플리케이션을 구축하십시오. AWS Step Functions

다음을 사용하여 환경을 배포하십시오. AWS CloudFormation

AWS CloudFormation 예측 가능하고 반복적으로 AWS 인프라 배포를 생성하고 프로비저닝할 수 있습니다. 이를 통해 기본 인프라 생성 및 구성에 대한 걱정 없이 AWS 제품을 활용하여 클라우드에서 안정성과 확장성이 뛰어나고 비용 효율적인 애플리케이션을 구축할 수 있습니다. AWS AWS CloudFormation 템플릿 파일을 사용하여 리소스 컬렉션을 단일 단위 (스택) 로 만들고 삭제할 수 있습니다. 자세한 내용은 AWS CloudFormation 사용 설명서를 참조하십시오.

AWS Control Tower는 AWS CloudFormation 스택세트를 사용하여 계정에 제어를 적용합니다. AWS Control Tower가 함께 작동하는 방식에 AWS CloudFormation 대한 자세한 내용은 을 참조하십시오 [를 사용하여 AWS Control Tower 리소스 생성 AWS CloudFormation](#).

를 사용하여 이벤트를 모니터링하십시오. CloudTrail

AWS Control Tower는 중앙 집중식 로깅 및 감사를 AWS CloudTrail 활성화하도록 구성합니다. 를 통해 CloudTrail 관리 계정은 회원 계정의 관리 조치 및 라이프사이클 이벤트를 검토할 수 있습니다.

CloudTrail 계정에 대한 AWS API 호출 기록을 보관하여 클라우드에서 AWS 환경을 모니터링할 수 있습니다. 예를 들어, 지원하는 서비스의 AWS API를 호출한 사용자 및 계정 CloudTrail, 호출이 이루어진 소스 IP 주소, 호출이 발생한 시간을 식별할 수 있습니다. API를 사용하여 애플리케이션에 CloudTrail 통합하고, 조직의 트레일 생성을 자동화하고, 트레일의 상태를 확인하고, 관리자의 CloudTrail 로그온 및 비활성화 방식을 제어할 수 있습니다. 자세한 내용은 AWS CloudTrail 사용 설명서를 참조하십시오.

다음을 통해 리소스 및 서비스를 모니터링할 수 있습니다. CloudWatch

CloudWatch Amazon은 몇 분 안에 사용을 시작할 수 있는 안정적이고 확장 가능하며 유연한 모니터링 솔루션을 제공합니다. 따라서 더 이상 자체 모니터링 시스템 및 인프라를 설치, 관리, 확장할 필요가 없습니다. 자세한 내용은 Amazon CloudWatch 사용 설명서를 참조하십시오.

CloudWatch Amazon이 AWS Control Tower와 협력하는 방식에 대한 자세한 내용은 모니터링을 참조하십시오.

다음을 사용하여 리소스 구성을 관리하십시오. AWS Config

AWS Config 구성 방식, 리소스 간의 관계, 시간 경과에 따른 구성 및 관계 변화를 포함하여 AWS 계정과 관련된 리소스를 자세히 볼 수 있습니다. 자세한 정보는 AWS Config 개발자 안내서를 참조하십시오.

AWS Config AWS Control Tower에서 프로비저닝하는 리소스에는 자동으로 태그가 `aws-control-tower` 지정되고 값은 입니다. `managed-by-control-tower`

AWS Control Tower의 리소스를 AWS Config 모니터링하고 기록하는 방법과 이에 대한 요금 청구 방법에 대한 자세한 내용은 을 참조하십시오[다음을 사용하여 리소스 변경을 모니터링합니다. AWS Config](#).

AWS Control Tower는 탐지 제어를 구현하는 AWS Config 규칙 데 사용합니다. 자세한 내용은 AWS Control Tower의 제어에 대한 정보를 참조하십시오.

IAM으로 엔티티에 대한 권한 관리

AWS Identity and Access Management (IAM) 은 다른 AWS 서비스에 대한 액세스를 제어하기 위한 AWS 서비스입니다. IAM을 사용하면 사용자 및 애플리케이션에 액세스 권한을 부여하는 AWS 리소스를 지정하는 사용자, 보안 자격 증명 (예: 액세스 키, 권한) 을 중앙에서 관리할 수 있습니다.

IAM을 ID 공급자로 선택하면 랜딩 존을 설정할 때 여러 그룹이 AWS IAM Identity Center 자동으로 생성될 수 있습니다. 이러한 그룹에는 IAM의 사전 정의된 권한 정책인 권한 집합이 있습니다. 또한 최종 사용자는 IAM을 사용하여 IAM 사용자 및 멤버 계정 내 다른 엔티티의 권한 범위를 정의할 수 있습니다.

AWS Identity and Access Management (IAM) 은 계정 및 비즈니스 애플리케이션에 대한 액세스를 관리하는 방법을 단순화합니다. AWS AWS Control Tower에서 모든 AWS 계정의 IAM ID 센터 액세스 및 사용자 권한을 제어할 수 있습니다.

자세한 내용은 AWS IAM Identity Center 사용 설명서를 참조하십시오.

IAM을 지원하지 AWS 리전 않는 지역에 기반을 두고 있는 경우 다른 ID 공급자를 데려와 사용자 및 그룹을 수동으로 설정하고 유지할 수 있습니다.

AWS Key Management Service

AWS Key Management Service (AWS KMS) 를 사용하면 데이터를 보호하는 키를 만들고 제어할 수 있습니다. AWS Control Tower에서는 선택적으로 AWS KMS 암호화 키로 데이터를 암호화할 수 있습니다. 에 대한 AWS KMS자세한 내용은 AWS KMS 개발자 안내서를 참조하십시오.

AWS Control Tower에서 AWS KMS 키를 설정하는 방법에 대한 자세한 내용은 선택적 AWS KMS 키 구성을 참조하십시오.

Lambda를 사용하여 서버리스 컴퓨팅 함수 실행

를 사용하면 AWS Lambda서버를 프로비저닝하거나 관리하지 않고도 코드를 실행할 수 있습니다. 추가 관리 오버헤드 없이 다양한 유형의 애플리케이션 또는 백엔드 서비스를 위한 코드를 실행할 수 있습니다. 코드를 업로드하면 Lambda는 고가용성으로 코드를 실행하고 확장할 수 있습니다. 다른 AWS 서비스에서 자동으로 트리거되도록 코드를 설정하거나 웹 또는 모바일 앱에서 직접 코드를 호출할 수 있습니다.

예를 들어, Lambda를 사용하여 다른 계정을 검토할 수 있도록 프로그래밍 방식으로 AWS Control Tower 감사 계정의 특정 역할을 맡을 수 있습니다. 또한 AWS Control Tower 수명 주기 이벤트를 사용하여 Lambda 함수를 트리거할 수 있습니다.

다음을 통해 계정을 관리합니다. AWS Organizations

AWS Organizations 여러 계정을 하나의 조직으로 통합하여 사용자가 만들고 중앙에서 관리할 수 있게 해주는 AWS 계정 관리 서비스입니다. Organizations를 사용하면 구성원 계정을 만들고 기존 계정을 조직에 가입하도록 초대할 수 있습니다. 이러한 계정을 그룹으로 구성하고 정책 기반 제어 항목을 연결할 수 있습니다. 자세한 내용은 AWS Organizations 사용 설명서를 참조하십시오.

AWS Control Tower에서 Organizations는 청구를 중앙에서 관리하고, 액세스, 규정 준수 및 보안을 제어하고, 멤버 AWS 계정 전체에서 리소스를 공유할 수 있도록 지원합니다. 계정은 조직 단위(OU)라고 하는 논리 그룹으로 그룹화됩니다. 조직에 대한 자세한 내용은 AWS Organizations 사용 설명서를 참조하십시오.

AWS Control Tower는 다음과 같은 OU를 사용합니다.

- 루트 — 랜딩 존에 있는 모든 계정과 기타 모든 OU의 부모 컨테이너입니다.
- 보안 - 이 OU에는 로그 아카이브 계정, 감사 계정 및 해당 계정이 소유한 리소스가 포함됩니다.
- 샌드박스 — 이 OU는 landing Zone을 설정할 때 생성됩니다. 랜딩 존에 있는 해당 OU와 다른 하위 OU에는 멤버 계정이 포함되어 있습니다. 최종 사용자가 AWS 리소스 관련 작업을 수행하기 위해 액세스하는 계정입니다.

> **Note**
>
> 조직 단위 페이지의 AWS Control Tower 콘솔을 통해 랜딩 존에 OU를 추가할 수 있습니다.

고려 사항

AWS Control Tower를 통해 생성된 OU에 컨트롤을 적용할 수 있습니다. AWS Control Tower 외부에서 만든 OU는 기본적으로 할 수 없습니다. 하지만 이러한 OU는 등록할 수 있습니다. OU를 등록한 후에는 OU와 해당 계정에 제어를 적용할 수 있습니다. OU 등록에 대한 자세한 내용은 AWS Control Tower에 기존 조직 단위 등록을 참조하십시오.

Amazon S3를 사용하여 객체 저장

Amazon Simple Storage Service (Amazon S3)는 인터넷 스토리지 서비스입니다. Amazon S3를 사용하면 인터넷을 통해 언제 어디서든 원하는 양의 데이터를 저장하고 검색할 수 있습니다. AWS Management Console의 간편하고 직관적인 웹 인터페이스를 사용하여 이러한 작업을 수행할 수 있습니다. 자세한 내용은 Amazon Simple Storage Service 사용 설명서를 참조하십시오.

랜딩 존을 설정하면 랜딩 존에 있는 모든 계정의 모든 로그를 포함하는 Amazon S3 버킷이 로그 아카이브 계정에 생성됩니다.

Security Hub로 환경을 모니터링하세요

AWS 컨트롤 타워는 서비스 관리형 표준: AWS Control Tower라는 Security Hub 표준을 통해 보안 허브와 AWS 통합됩니다. 자세한 내용은 Security Hub 표준을 참조하십시오.

다음을 통해 계정을 프로비저닝합니다. AWS Service Catalog

AWS Service Catalog IT 관리자는 승인된 제품 포트폴리오를 만들고 관리하여 최종 사용자에게 배포할 수 있으며, 최종 사용자는 개인화된 포털에서 필요한 제품에 액세스할 수 있습니다. 일반적인 제품에는 리소스를 사용하여 AWS 배포되는 서버, 데이터베이스, 웹 사이트 또는 애플리케이션이 포함됩니다.

특정 제품에 액세스할 수 있는 사용자를 제어할 수 있으므로 조직의 비즈니스 표준을 준수하고, 제품 수명 주기를 관리하고, 사용자가 확신을 가지고 제품을 찾고 출시하도록 지원할 수 있습니다. 자세한 내용은 Service Catalog 관리자 안내서를 참조하십시오.

AWS Control Tower에서는 중앙 클라우드 관리자와 최종 사용자가 “사용자 지정 청사진”이라는 AWS Service Catalog 제품을 사용하여 랜딩 존에서 사용자 지정 계정을 프로비저닝할 수 있습니다. 자세한 내용은 2단계를 참조하십시오. 제품 만들기. AWS Service Catalog

또한 AWS Control Tower는 Service Catalog API를 사용하여 계정 프로비저닝과 업데이트를 더욱 자동화할 수 있습니다. 자세한 내용은 AWS Service Catalog 개발자 안내서를 참조하십시오.

AWS Service Catalog 외부 제품 유형으로 전환

AWS Service Catalog Terraform 오픈 소스 제품 및 프로비저닝된 제품에 대한 지원을 External이라는 새로운 제품 유형으로 변경했습니다. 이 전환에 대해 자세히 알아보려면 관리자 안내서에서 기존

Terraform 오픈 소스 제품 및 프로비저닝된 제품을 외부 제품 유형으로 업데이트하는 것을 참조하세요.AWS Service Catalog

이 변경은 AWS Control Tower 계정 팩토리 사용자 지정을 사용하여 생성하거나 등록한 기존 계정에 영향을 줍니다. 이러한 계정을 외부 제품 유형으로 전환하려면 AWS Control AWS Service Catalog Tower와 AWS Control Tower를 모두 변경해야 합니다.

외부 제품 유형으로 전환하려면

1. 외부 및 Terraform 오픈 소스 제품 유형에 대한 지원을 모두 AWS Service Catalog 포함하도록 기존 Terraform 참조 엔진을 업그레이드하십시오. Terraform 참조 엔진 업데이트에 대한 지침은 리포지토리를 검토하세요.AWS Service Catalog GitHub
2. 에서 AWS Service Catalog기존 Terraform 오픈 소스 제품 (청사진) 을 복제하고 새 외부 제품 유형을 사용하여 복제하십시오. 기존 Terraform 오픈 소스 블루프린트를 종료하지 마십시오.
3. AWS Control Tower에서 Terraform 오픈 소스 블루프린트를 사용하여 각 계정을 업데이트하여 새로운 외부 블루프린트를 사용하십시오.

   a. 블루프린트를 업데이트하려면 먼저 Terraform 오픈 소스 블루프린트를 완전히 제거해야 합니다. 자세한 내용은 계정에서 블루프린트 삭제를 참조하세요.

   b. 새 외부 블루프린트를 같은 계정에 추가하세요. 자세한 내용은 AWS Control Tower 계정에 청사진 추가를 참조하십시오.
4. Terraform 오픈 소스 청사진을 사용하는 모든 계정이 외부 청사진으로 업데이트된 후에는 Terraform 오픈 소스를 제품 유형으로 사용하는 모든 제품으로 AWS Service Catalog 돌아가서 종료하십시오.
5. 앞으로는 AWS Control Tower 계정 팩토리 사용자 지정을 사용하여 생성하거나 등록한 모든 계정은 AWS CloudFormation또는 외부 제품 유형을 사용하는 청사진을 참조해야 합니다.

   외부 제품 유형을 사용하여 생성한 블루프린트의 경우, AWS Control Tower는 Terraform 템플릿과 Terraform 참조 엔진을 사용하는 계정 사용자 지정만 지원합니다. 자세히 알아보려면 사용자 지정을 위한 설정을 참조하십시오.

> **Note**
>
> AWS Control Tower는 새 계정을 생성할 때 제품 유형으로 Terraform 오픈 소스를 지원하지 않습니다. 이러한 변경 사항에 대해 자세히 알아보려면 관리자 안내서에서 기존 Terraform 오픈 소스 제품 및 프로비저닝된 제품을 외부 제품 유형으로 업데이트하는 방법을 참조하십시

오.AWS Service Catalog AWS Service Catalog 필요에 따라 이 제품 유형 전환을 통해 고객을 지원할 예정입니다. 계정 담당자에게 문의하여 지원을 요청하십시오.

Amazon 심플 알림 서비스를 통한 알림 추적

Amazon Simple Notification Service (Amazon SNS) 는 애플리케이션, 최종 사용자 및 디바이스가 클라우드에서 즉시 알림을 보내고 받을 수 있게 해주는 웹 서비스입니다. 자세한 설명은 Amazon Simple Notification Service 개발자 안내서를 참조하세요.

AWS Control Tower는 Amazon SNS를 사용하여 관리 계정 및 감사 계정의 이메일 주소로 프로그래밍 방식의 알림을 보냅니다. 이러한 경고는 착륙 지대 내에서 드리프트를 방지하는 데 도움이 됩니다. 자세한 정보는 AWS Control Tower의 드리프트 감지 및 해결을 참조하세요.

또한 Amazon 심플 알림 서비스를 사용하여 규정 준수 알림을 AWS Config전송합니다.

> **Tip**
>
> AWS Control Tower 제어 규정 준수 알림 (감사 계정) 을 수신하는 가장 좋은 방법 중 하나는 구독하는 `AggregateConfigurationNotifications` 것입니다. 규정 준수를 검사하는 데 도움이 되는 서비스입니다. 규정 준수를 위반하는 AWS Config 규칙에 대한 실제 데이터를 제공합니다. AWS Config OU의 계정 목록을 자동으로 유지 관리합니다.
> 이메일이나 SNS에서 허용하는 모든 유형의 구독을 사용하여 수동으로 구독해야 합니다.
> 명세서는 감사 계정으로 `arn:aws:sns:`*`homeregion`*`:`*`account`*`:aws-controltower-AggregateSecurityNotifications` 연결됩니다.

를 사용하여 분산 애플리케이션을 구축하십시오. AWS Step Functions

AWS Step Functions 시각적 워크플로의 일련의 단계로 분산 애플리케이션의 구성 요소를 쉽게 조정할 수 있습니다. 빠르게 상태 시스템을 빌드하고 실행하여 안정적이고 확장 가능한 방식으로 애플리케이션의 단계를 실행할 수 있습니다. 자세한 정보는 AWS Step Functions 개발자 안내서를 참조하세요.

AWS Control Tower의 자격 증명 및 액세스 관리

Account Factory에서 계정을 프로비저닝하거나 AWS Control Tower 콘솔에서 새 조직 단위 (OU) 를 생성하는 등 랜딩 존에서 작업을 수행하려면 AWS Identity and Access Management (IAM) 하거나 승인된 사용자임을 AWS IAM Identity Center 인증해야 합니다. AWS 예를 들어, AWS Control Tower 콘솔을 사용하는 경우 관리자가 제공한 AWS 자격 증명을 제공하여 ID를 인증합니다.

ID를 인증한 후 IAM은 특정 작업 및 리소스 세트에 대해 정의된 권한 AWS 집합으로 액세스를 제어합니다. 계정 관리자인 경우 IAM을 사용하여 계정과 연결된 리소스에 대한 다른 IAM 사용자의 액세스를 제어할 수 있습니다.

주제

인증

다음과 같은 유형의 AWS ID로 액세스할 수 있습니다.

- AWS 계정 루트 사용자 - 계정을 처음 만들 때는 해당 AWS 계정의 모든 AWS 서비스와 리소스에 대한 완전한 액세스 권한을 가진 ID로 시작합니다. 이 ID를 AWS 계정 루트 사용자라고 합니다. 계정을 만드는 데 사용한 이메일 주소와 암호로 로그인할 때 이 자격 증명에 액세스할 수 있습니다. 일상적인 작업, 심지어 관리 작업의 경우에도 루트 사용자를 사용하지 않을 것을 강력히 권장합니다. 대신 첫 IAM Identity Center 사용자 (권장) 또는 IAM 사용자를 생성할 때만 루트 사용자를 사용하는 모범 사례를 따르세요 (대부분의 사용 사례에서는 모범 사례가 아님). 그런 다음 루트 사용자 자격 증명을 안전하게 보관하고 몇 가지 계정 및 서비스 관리 태스크를 수행할 때만 사용합니다. 자세한 정보는 루트 사용자로 로그인하는 경우을 참조하세요.
- IAM 사용자 — IAM 사용자는 특정 사용자 지정 권한을 가진 AWS 계정 내 자격 증명입니다. IAM 사용자 자격 증명을 사용하여 AWS 관리 콘솔, AWS 토론 포럼 또는 AWS Support Center와 같은 보안 AWS 웹 페이지에 로그인할 수 있습니다. AWS 장기 자격 증명을 보유한 IAM 사용자를 생성하면 보안 위험이 더 커지므로 IAM 사용자 대신 IAM Identity Center 사용자를 생성하는 것이 좋습니다.

특정 목적을 위해 IAM 사용자를 생성해야 하는 경우 로그인 자격 증명 외에도 각 IAM 사용자에 대한 액세스 키를 생성할 수 있습니다. 여러 SDK 중 하나를 통해 또는 CLI (AWS 명령줄 인터페이스) 를 사용하여 프로그래밍 방식으로 AWS 서비스를 호출할 때 이러한 키를 사용할 수 있습니다. SDK 및 CLI 도구는 액세스 키를 사용하여 암호화 방식으로 요청에 서명합니다. AWS 도구를 사용하지 않는 경우 요청에 직접 서명해야 합니다. AWS Control Tower는 인바운드 API 요청을 인증하기 위한 프로토콜인 서명 버전 4를 지원합니다. 요청 인증에 대한 자세한 내용은 일반 참조의 AWS 서명 버전 4 서명 프로세스를 참조하십시오.

- IAM 역할 – IAM 역할은 계정에 만들 수 있는, 특정 권한을 지닌 IAM 자격 증명입니다. IAM 역할은 자격 증명이라는 점에서 IAM 사용자와 비슷하며, AWS 자격 증명이 수행할 수 있는 작업과 수행할 수 없는 작업을 결정하는 권한 정책을 가지고 있습니다. AWS그러나 역할은 한 사람하고만 연관되지 않고 해당 역할이 필요한 사람이라면 누구든지 맡을 수 있어야 합니다. 또한 역할에는 그와 연관된 암호 또는 액세스 키와 같은 표준 장기 자격 증명이 없습니다. 대신에 역할을 맡은 사람에게는 해당 역할 세션을 위한 임시 보안 자격 증명이 제공됩니다. 임시 보안 인증 정보가 있는 IAM 역할은 다음과 같은 상황에서 유용합니다.
  - 연동 사용자 액세스 — IAM 사용자를 생성하는 대신 엔터프라이즈 사용자 디렉토리 또는 웹 ID 공급자의 기존 ID를 사용할 수 있습니다. AWS Directory Service이러한 사용자를 페더레이션 사용자라고 합니다. AWS ID 공급자를 통해 액세스를 요청할 때 연동 사용자에게 역할을 할당합니다. 페더레이션 사용자에 대한 자세한 정보는 IAM 사용 설명서의 페더레이션 사용자 및 역할을 참조하세요.
  - AWS 서비스 액세스 — 서비스 역할은 서비스가 사용자를 대신하여 사용자 계정에서 작업을 수행하는 IAM 역할입니다. 일부 AWS 서비스 환경을 설정할 때는 서비스가 위임할 역할을 정의해야 합니다. 이 서비스 역할에는 서비스가 필요한 AWS 리소스에 액세스하는 데 필요한 모든 권한이 포함되어야 합니다. 서비스 역할은 서비스마다 다르지만 해당 서비스에 대한 문서화된 요구 사항을 충족하는 한 대부분의 경우 권한을 선택할 수 있습니다. 서비스 역할은 해당 계정 내에서만 액세스를 제공하며 다른 계정의 서비스에 대한 액세스를 부여하는 데 사용할 수 없습니다. IAM 내에서 서비스 역할을 만들고, 수정하고, 삭제할 수 있습니다. 예를 들어, Amazon Redshift에서 사용자 대신 Amazon S3 버킷에 액세스하도록 허용하는 역할을 생성한 다음 해당 버킷의 데이터를 Amazon Redshift 클러스터로 로드할 수 있습니다. 자세한 내용은 IAM 사용 설명서의 AWS 서비스에 권한을 위임하기 위한 역할 생성을 참조하십시오.
  - Amazon EC2에서 실행되는 애플리케이션 — IAM 역할을 사용하여 Amazon EC2 인스턴스에서 실행되고 CLI AWS 또는 API 요청을 하는 애플리케이션의 임시 자격 증명을 관리할 수 있습니다. AWS 이는 Amazon EC2 인스턴스 내에 액세스 키를 저장할 때 권장되는 방법입니다. Amazon EC2 인스턴스에 AWS 역할을 할당하고 모든 애플리케이션에서 사용할 수 있게 하려면 인스턴스에 연결된 인스턴스 프로필을 생성합니다. 인스턴스 프로파일에는 역할이 포함되어 있으며 Amazon EC2 인스턴스에서 실행되는 프로그램이 임시 보안 인증 정보를 얻을 수 있습니다. 자세

한 정보는 IAM 사용 설명서의 IAM 역할을 사용하여 Amazon EC2 인스턴스에서 실행되는 애플리케이션에 권한 부여를 참조하세요.

- IAM ID 센터 사용자 포털에 대한 IAM ID 센터 사용자 인증은 IAM ID 센터에 연결된 디렉터리에 의해 제어됩니다. 하지만 사용자 포털 내에서 최종 사용자가 사용할 수 있는 AWS 계정에 대한 권한 부여는 다음 두 가지 요소에 의해 결정됩니다.
  - AWS IAM Identity Center 콘솔에서 해당 AWS 계정에 대한 액세스 권한을 할당받은 사용자 자세한 내용은 사용 설명서의 싱글 사인온 액세스를 참조하십시오.AWS IAM Identity Center
  - AWS IAM Identity Center 콘솔에서 최종 사용자에게 해당 계정에 대한 적절한 액세스를 허용할 수 있는 권한 수준은 어느 정도입니까? AWS 자세한 내용은 사용 설명서의 권한 세트를 참조하십시오.AWS IAM Identity Center

액세스 제어

랜딩 존에서 AWS Control Tower 리소스 또는 기타 AWS 리소스를 생성, 업데이트, 삭제 또는 나열하려면 작업을 수행할 수 있는 권한과 해당 리소스에 액세스할 수 있는 권한이 필요합니다. 또한 프로그래밍 방식으로 작업을 수행하려면 유효한 액세스 키가 필요합니다.

다음 섹션에서는 AWS Control Tower의 권한을 관리하는 방법을 설명합니다.

주제

- AWS Control Tower 리소스에 대한 액세스 권한 관리 개요
- AWS Control Tower에 대한 자격 증명 기반 정책 (IAM 정책) 사용

AWS IAM 아이덴티티 센터 및 AWS 컨트롤 타워와의 협력

AWS Control Tower에서는 IAM Identity Center를 통해 중앙 클라우드 관리자와 최종 사용자가 여러 AWS 계정 및 비즈니스 애플리케이션에 대한 액세스를 관리할 수 있습니다. 자격 증명 및 액세스 제어를 자체 관리하는 옵션을 선택하지 않은 한, AWS Control Tower는 기본적으로 이 서비스를 사용하여 Account Factory를 통해 생성된 계정에 대한 액세스를 설정하고 관리합니다.

자격 증명 공급자 선택에 대한 자세한 내용은 을 참조하십시오. IAM ID 센터 지침

AWS Control Tower에서 IAM ID 센터 사용자 및 권한을 설정하는 방법에 대한 간단한 자습서는 이 비디오 (6:23) 를 참조하십시오. 동영상 오른쪽 하단에 있는 아이콘을 선택하여 전체 화면으로 확대하면 더 잘 보입니다. 자막을 사용할 수 있습니다.

AWS Control Tower에서 AWS IAM 자격 증명 센터를 설정하는 방법에 대한 동영상 안내.

IAM 자격 증명 센터를 통한 AWS Control Tower 설정에 대한 정보

AWS Control Tower를 처음 설정할 때는 루트 사용자 사용자 및 올바른 권한을 가진 IAM 사용자만 IAM Identity Center 사용자를 추가할 수 있습니다. 하지만 AWSAccountFactory그룹에 최종 사용자를 추가한 후에는 Account Factory 마법사에서 새 IAM Identity Center 사용자를 생성할 수 있습니다. 자세한 설명은 Account Factory를 통한 계정 제공 및 관리 섹션을 참조하세요.

권장 기본값을 선택하면 AWS Control Tower는 사용자 ID 및 Single Sign-On을 관리하는 데 도움이 되는 사전 구성된 디렉터리로 랜딩 존을 설정하여 사용자가 여러 계정에 걸쳐 페더레이션된 액세스를 갖도록 합니다. landing Zone을 설정하면 사용자 그룹 및 권한 집합을 포함하도록 이 기본 디렉터리가 생성됩니다.

> **Note**
>
> IAM Identity AWS IAM Identity Center Center의 위임된 관리자 기능을 사용하여 조직 내 관리를 관리 계정이 아닌 다른 계정에 위임할 수 있습니다. 이 기능을 사용하기로 선택한 경우 그룹 멤버십을 관리할 수 있는 액세스 권한이 있는 관리자는 관리 계정에 할당된 그룹도 관리할 수 있다는 점에 유의하십시오. 자세한 내용은 “AWS SSO 위임 관리 시작하기”라는 제목의 이 블로그 게시물을 참조하십시오.

사용자 그룹, 역할 및 권한 집합

사용자 그룹은 공유 계정 내에 정의된 특수 역할을 관리합니다. 역할은 함께 속한 권한 세트를 설정합니다. 그룹의 모든 멤버는 해당 그룹과 연결된 권한 세트 또는 역할을 상속합니다. 멤버 계정의 최종 사용자를 위한 새 그룹을 만들어 그룹이 수행하는 특정 작업에 필요한 역할만 사용자 지정하여 할당할 수 있습니다.

사용 가능한 권한 집합에는 읽기 전용 액세스, AWS Control Tower 관리 액세스, Service Catalog 액세스 등 다양한 사용자 권한 요구 사항이 포함됩니다. 이러한 권한 집합을 통해 최종 사용자는 기업 지침에 따라 랜딩 존에서 자신의 AWS 계정을 신속하게 프로비저닝할 수 있습니다.

사용자, 그룹 및 권한 할당을 계획하는 방법에 대한 팁은 그룹, 역할, 정책 설정을 위한 권장 사항 단원을 참조하십시오.

AWS Control Tower의 맥락에서 이 서비스를 사용하는 방법에 대한 자세한 내용은 사용 AWS IAM Identity Center 설명서의 다음 주제를 참조하십시오.

- 사용자를 추가하려면 사용자 추가를 참조하십시오.

- 그룹에 사용자를 추가하려면 그룹에 사용자 추가를 참조하십시오.
- 사용자 속성을 편집하려면사용자 속성 편집을 참조하십시오.
- 그룹을 추가하려면 그룹 추가를 참조하십시오.

> **Warning**
>
> AWS Control Tower는 홈 리전에 IAM ID 센터 디렉터리를 설정합니다. 다른 지역에 랜딩 존을 설정한 다음 IAM Identity Center 콘솔로 이동하는 경우 지역을 홈 지역으로 변경해야 합니다. 홈 지역에서 IAM ID 센터 구성을 삭제하지 마십시오.

IAM 자격 증명 센터 계정 및 AWS Control Tower에 대해 알아야 할 사항

다음은 AWS Control Tower에서 IAM Identity Center 사용자 계정을 사용할 때 알아두면 좋은 몇 가지 사항입니다.

- AWS IAM ID 센터 사용자 계정이 비활성화된 경우 Account Factory에서 새 계정을 프로비저닝하려고 하면 오류 메시지가 표시됩니다. IAM ID 센터 콘솔에서 IAM ID 센터 사용자를 다시 활성화할 수 있습니다.
- Account Factory에서 판매한 계정과 연결된 프로비저닝된 제품을 업데이트할 때 새 IAM ID 센터 사용자 이메일 주소를 지정하면 AWS Control Tower는 새 IAM ID 센터 사용자 계정을 생성합니다. 이전에 만든 사용자 계정은 제거되지 않습니다. IAM Identity Center에서 이전 IAM Identity Center 사용자 이메일 주소를 제거하려는 경우 사용자 AWS 비활성화를 참조하십시오.
- AWS IAM Identity Center는 Azure 액티브 디렉터리와 통합되었으며, 기존 Azure 액티브 디렉터리를 AWS 컨트롤 타워에 연결할 수 있습니다.
- AWS Control Tower의 동작이 AWS IAM Identity Center 및 다양한 자격 증명 소스와 상호 작용하는 방식에 대한 자세한 내용은 AWS IAM ID 센터 설명서의 자격 증명 소스 변경 고려 사항을 참조하십시오.

AWS 컨트롤 타워용 IAM 자격 증명 센터 그룹

AWS Control Tower는 계정에서 특정 작업을 수행하는 사용자를 구성할 수 있도록 사전 구성된 그룹을 제공합니다. IAM Identity Center에서 사용자를 추가하고 이러한 그룹에 직접 배정할 수 있습니다. 이렇게 하면 권한 세트가 계정 내의 그룹에 있는 사용자에게 적용됩니다. 랜딩 존을 설정할 때 생성되는 그룹은 다음과 같습니다.

AWSAccountFactory

계정	권한 세트	설명
관리 계정	AWSServiceCatalogEndUserAccess	이 그룹은 Account Factory를 사용하여 새 계정을 프로비저닝할 때만 이 계정에서 사용됩니다.

AWSServiceCatalogAdmins

계정	권한 세트	설명
관리 계정	AWSServiceCatalogAdminFullAccess	이 그룹은 이 계정에서 Account Factory를 관리적으로 변경하는 데만 사용됩니다. 이 그룹의 사용자는 그룹에 속해 있지 않는 한 새 계정을 AWSAccountFactory프로비전할 수 없습니다.

AWSControlTowerAdmins

계정	권한 세트	설명
관리 계정	AWSAdministratorAccess	이 계정에서 이 그룹의 사용자만 AWS Control Tower 콘솔에 액세스할 수 있습니다.
로그 아카이브 계정	AWSAdministratorAccess	사용자는 이 계정에서 관리자 액세스 권한을 갖습니다.
감사 계정	AWSAdministratorAccess	사용자는 이 계정에서 관리자 액세스 권한을 갖습니다.
멤버 계정	AWSOrganizationsFullAccess	사용자는 이 계정에서 Organizations에 대한 전체 액세스 권한을 가집니다.

AWSSecurityAuditPowerUsers

계정	권한 세트	설명
관리 계정	AWSPowerUserAccess	사용자는 애플리케이션 개발 작업을 수행하고 AWS 인식 가능한 애플리케이션 개발을 지원하는 리소스와 서비스를 만들고 구성할 수 있습니다.
로그 아카이브 계정	AWSPowerUserAccess	사용자는 애플리케이션 개발 작업을 수행하고 AWS 인식 가능한 애플리케이션 개발을 지원하는 리소스와 서비스를 만들고 구성할 수 있습니다.
감사 계정	AWSPowerUserAccess	사용자는 애플리케이션 개발 작업을 수행하고 AWS 인식 가능한 애플리케이션 개발을 지원하는 리소스와 서비스를 만들고 구성할 수 있습니다.
멤버 계정	AWSPowerUserAccess	사용자는 애플리케이션 개발 작업을 수행하고 AWS 인식 가능한 애플리케이션 개발을 지원하는 리소스와 서비스를 만들고 구성할 수 있습니다.

AWSSecurityAuditors

계정	권한 세트	설명
관리 계정	AWSReadOnlyAccess	사용자는 이 계정의 모든 AWS 서비스와 리소스에 대한 읽기 전용 액세스 권한을 가집니다.

계정	권한 세트	설명
로그 아카이브 계정	AWSReadOnlyAccess	사용자는 이 계정의 모든 AWS 서비스와 리소스에 대한 읽기 전용 액세스 권한을 가집니다.
감사 계정	AWSReadOnlyAccess	사용자는 이 계정의 모든 AWS 서비스와 리소스에 대한 읽기 전용 액세스 권한을 가집니다.
멤버 계정	AWSReadOnlyAccess	사용자는 이 계정의 모든 AWS 서비스와 리소스에 대한 읽기 전용 액세스 권한을 가집니다.

AWSLogArchiveAdmins

계정	권한 세트	설명
로그 아카이브 계정	AWSAdministratorAccess	사용자는 이 계정에서 관리자 액세스 권한을 갖습니다.

AWSLogArchiveViewers

계정	권한 세트	설명
로그 아카이브 계정	AWSReadOnlyAccess	사용자는 이 계정의 모든 AWS 서비스와 리소스에 대한 읽기 전용 액세스 권한을 가집니다.

AWSAuditAccountAdmins

계정	권한 세트	설명
감사 계정	AWSAdministratorAccess	사용자는 이 계정에서 관리자 액세스 권한을 갖습니다.

AWS Control Tower 리소스에 대한 액세스 권한 관리 개요

모든 AWS 리소스는 에서 AWS 계정소유하며 리소스를 생성하거나 리소스를 액세스할 수 있는 권한은 권한 정책에 따라 관리됩니다. 계정 관리자는 IAM 자격 증명(사용자, 그룹 및 역할)에 권한 정책을 연결할 수 있습니다. 일부 서비스 (예: AWS Lambda) 는 리소스에 권한 정책을 연결하는 것도 지원합니다.

> **Note**
>
> 계정 관리자 또는 관리자는 관리자 권한이 있는 사용자입니다. 자세한 설명은 IAM 사용자 가이드의 IAM 모범 사례 섹션을 참조하십시오.

사용자 또는 역할에 권한을 부여할 책임이 있는 경우 권한이 필요한 사용자 및 역할, 각 사용자 및 역할에 권한이 필요한 리소스, 해당 리소스를 운영하기 위해 허용되어야 하는 특정 작업을 파악하고 추적해야 합니다.

주제

- AWS Control 타워 리소스 및 운영
- 리소스 소유권 정보
- 리소스에 대한 액세스를 관리합니다.
- 정책 요소 지정: 조치, 효과, 원칙
- 정책에서 조건 지정

AWS Control 타워 리소스 및 운영

AWS Control Tower에서 기본 리소스는 랜딩 존입니다. 또한 AWS Control Tower는 가드레일이라고도 하는 추가 리소스 유형인 컨트롤을 지원합니다. 하지만 AWS Control Tower의 경우 기존 착륙 지대의 상황에서만 제어를 관리할 수 있습니다. 컨트롤은 하위 리소스라고 할 수 있습니다.

의 리소스와 하위 AWS 리소스에는 다음 예와 같이 고유한 Amazon 리소스 이름 (ARN) 이 연결되어 있습니다.

AWS 컨트롤 타워는 AWS 컨트롤 타워 리소스를 사용할 수 있는 일련의 API 작업을 제공합니다. 사용 가능한 작업 목록은 AWS 컨트롤 타워, AWS 컨트롤 타워 API 레퍼런스를 참조하십시오.

AWS Control Tower의 AWS CloudFormation 리소스에 대한 자세한 내용은 AWS CloudFormation 사용 설명서를 참조하십시오.

리소스 소유권 정보

누가 리소스를 만들었든 상관없이 계정에서 생성된 리소스는 계정을 소유합니다. AWS 구체적으로, 리소스 소유자는 리소스 생성 요청을 인증하는 보안 주체 (즉, AWS 계정 루트 사용자, IAM Identity Center 사용자, IAM 사용자 또는 IAM 역할) 의 AWS 계정입니다. 다음 예에서는 이러한 작동 방식을 설명합니다.

- AWS 계정의 계정 루트 사용자 자격 증명을 사용하여 landing Zone을 설정하는 경우 해당 AWS 계정이 리소스의 소유자가 됩니다. AWS
- AWS 계정에서 IAM 사용자를 생성하고 해당 사용자에게 랜딩 존 설정 권한을 부여하는 경우 해당 사용자는 계정이 사전 요구 사항을 충족하는 한 랜딩 존을 설정할 수 있습니다. 하지만 사용자가 속한 AWS 계정이 landing zone 리소스를 소유합니다.
- AWS 계정에 랜딩 존을 설정할 권한이 있는 IAM 역할을 생성하는 경우, 해당 역할을 수임할 수 있는 사람은 누구나 랜딩 존을 설정할 수 있습니다. 역할이 속한 사용자 AWS 계정은 landing zone 리소스를 소유합니다.

리소스에 대한 액세스를 관리합니다.

권한 정책은 누가 무엇에 액세스할 수 있는지를 나타냅니다. 다음 섹션에서는 권한 정책을 만드는 데 사용 가능한 옵션에 대해 설명합니다.

> **Note**
>
> 이 섹션에서는 AWS Control Tower의 맥락에서 IAM을 사용하는 방법을 설명합니다. IAM 서비스에 대한 자세한 정보는 다루지 않습니다. IAM 설명서 전체 내용은 IAM 사용 설명서의 IAM이란 무엇입니까? 섹션을 참조하세요. IAM 정책 구문과 설명에 대한 자세한 내용은 IAM 사용 설명서의 AWS IAM 정책 참조 섹션을 참조하세요.

IAM 자격 증명에 연결된 정책을 자격 증명 기반 정책 (IAM 정책) 이라고 합니다. 리소스에 연결된 정책을 리소스 기반 정책이라고 합니다.

> **Note**
>
> AWS Control Tower는 자격 증명 기반 정책 (IAM 정책) 만 지원합니다.

주제

- 자격 증명 기반 정책 (IAM 정책) 에 대한 정보
- 역할 생성 및 권한 할당
- 리소스 기반 정책

자격 증명 기반 정책 (IAM 정책) 에 대한 정보

정책을 IAM ID에 연계할 수 있습니다. 예를 들면, 다음을 수행할 수 있습니다:

- 계정 내 사용자 또는 그룹에 권한 정책 연결 — 사용자에게 AWS Control Tower 리소스를 생성할 수 있는 권한 (예: landing zone 설정) 을 부여하려면 사용자가 속한 사용자 또는 그룹에 권한 정책을 연결할 수 있습니다.
- 역할에 권한 정책 연결(교차 계정 권한 부여) – ID 기반 권한 정책을 IAM 역할에 연결하여 교차 계정 권한을 부여할 수 있습니다. 예를 들어 한 AWS 계정의 관리자 (계정 A) 가 다른 계정 (계정 B) 에 AWS 계정 간 권한을 부여하는 역할을 만들거나 관리자가 다른 AWS 서비스에 권한을 부여하는 역할을 만들 수 있습니다.
  1. 계정 A 관리자는 IAM 역할을 생성하고 계정 A의 리소스를 관리할 권한을 부여하는 역할에 권한 정책을 연결합니다.
  2. 계정 A 관리자는 신뢰 정책을 역할에 연결합니다. 이 정책은 역할을 담당할 수 있는 보안 주체로 계정 B를 식별합니다.
  3. 계정 B 관리자는 계정 B의 모든 사용자에게 역할을 수임할 수 있는 권한을 부여할 수 있습니다. 이 역할을 맡으면 계정 B의 사용자는 계정 A의 리소스를 생성하거나 해당 리소스에 대한 액세스 권한을 얻을 수 있습니다.
  4. AWS 서비스에 역할을 수임할 수 있는 권한 (권한) 을 부여하려면 신뢰 정책에서 지정하는 보안 주체를 AWS 서비스라고 할 수 있습니다.

역할 생성 및 권한 할당

역할 및 권한을 통해 AWS Control Tower 및 기타 AWS 서비스 (프로그래밍 방식의 리소스 액세스 포함) 에 있는 리소스에 액세스할 수 있습니다.

액세스 권한을 제공하려면 사용자, 그룹 또는 역할에 권한을 추가하세요:

- 다음 지역의 AWS IAM Identity Center사용자 및 그룹:

  권한 세트를 생성합니다. AWS IAM Identity Center 사용 설명서의 권한 세트 생성의 지침을 따르세요.

- ID 제공자를 통해 IAM에서 관리되는 사용자:

  ID 페더레이션을 위한 역할을 생성합니다. IAM 사용 설명서의 서드 파티 자격 증명 공급자의 역할 만들기(연합)의 지침을 따르세요.

- IAM 사용자:
  - 사용자가 맡을 수 있는 역할을 생성합니다. IAM 사용 설명서에서 IAM 사용자의 역할 생성의 지침을 따르세요.
  - (권장되지 않음)정책을 사용자에게 직접 연결하거나 사용자를 사용자 그룹에 추가합니다. IAM 사용 설명서에서 사용자(콘솔)에 권한 추가의 지침을 따르세요.

IAM을 사용하여 권한을 위임하는 방법에 대한 자세한 설명은 IAM 사용자 가이드의 액세스 관리 섹션을 참조하십시오.

> **Note**
>
> AWS Control Tower 랜딩 존을 설정할 때는 AdministratorAccess관리형 정책을 사용하는 사용자 또는 역할이 필요합니다. (arn:AWS:iam: :AWS:policy/) AdministratorAccess

(IAM 콘솔) 역할을 만들려면 AWS 서비스

1. https://console.aws.amazon.com/iam/ 에서 AWS Management Console 로그인하고 IAM 콘솔을 엽니다.
2. IAM 콘솔의 탐색 창에서 역할을 선택하고 역할 생성을 선택합니다.
3. 신뢰할 수 있는 엔터티 유형에 AWS 서비스를 선택합니다.
4. 서비스 또는 사용 사례의 경우 서비스를 선택한 다음, 사용 사례를 선택합니다. 사용 사례는 서비스에 필요한 신뢰 정책을 포함하기 위해 서비스에서 정합니다.
5. 다음을 선택합니다.
6. 권한 정책의 경우 선택한 사용 사례에 따라 옵션이 달라집니다.
   - 서비스가 역할에 대한 권한을 정의하는 경우 권한 정책을 선택할 수 없습니다.
   - 제한된 권한 정책 세트에서 선택합니다.
   - 모든 권한 정책에서 선택합니다.
   - 권한 정책 없음을 선택하고 역할이 생성된 후 정책을 생성한 다음, 정책을 역할에 연결합니다.

7. (선택 사항) 권한 경계를 선택합니다. 이는 서비스 역할에서 가능한 고급 기능이며 서비스 링크된 역할은 아닙니다.

   a. 권한 경계 설정 섹션을 열고 최대 역할 권한을 관리하기 위한 권한 경계 사용을 선택합니다.

      IAM에는 계정의 AWS 관리형 및 고객 관리형 정책 목록이 포함되어 있습니다.

   b. 정책을 선택하여 권한 경계를 사용하세요.

8. 다음을 선택합니다.

9. 역할 이름의 경우 옵션은 서비스에 따라 달라집니다.

   - 서비스에서 역할 이름을 정의하는 경우 이 역할 이름을 편집할 수 없습니다.
   - 서비스에서 역할 이름에 대한 접두사를 정의하는 경우 사용자가 선택적 접미사를 입력할 수 있습니다.
   - 서비스에서 역할 이름을 정의하지 않는 경우 역할 이름을 지정할 수 있습니다.

   > **Important**
   >
   > 역할 이름을 지정할 때는 다음 사항에 유의하세요.
   >
   > - 역할 이름은 사용자 내에서 고유해야 AWS 계정하며 대소문자를 구분하여 고유할 수 없습니다.
   >
   >   예를 들어, 이름이 **PRODROLE**과 **prodrole**, 두 가지로 지정된 역할을 만들지 마십시오. 역할 이름이 정책 또는 ARN의 일부로 사용되는 경우 역할 이름은 대소문자를 구분합니다. 그러나 로그인 프로세스와 같이 콘솔에서 역할 이름이 고객에게 표시되는 경우에는 역할 이름이 대소문자를 구분하지 않습니다.
   > - 다른 엔터티가 역할을 참조할 수 있기 때문에 역할이 생성된 후에는 역할 이름을 편집할 수 없습니다.

10. (선택 사항)설명에 역할에 대한 설명을 입력합니다.

11. (선택 사항) 역할에 대한 사용 사례와 권한을 편집하려면 1단계: 신뢰할 수 있는 엔터티 선택 또는 2단계: 권한 추가 섹션에서 편집을 선택합니다.

12. (선택 사항) 태그를 키-값 페어로 연결하여 역할을 식별, 구성 또는 검색합니다. IAM에서 태그 사용에 대한 자세한 내용을 알아보려면 IAM 사용 설명서의 IAM 리소스에 태그 지정을 참조하세요.

13. 역할을 검토한 다음 역할 생성을 선택합니다.

JSON 정책 편집기를 사용하여 정책을 생성하려면

1. 에 AWS Management Console 로그인하고 https://console.aws.amazon.com/iam/ 에서 IAM 콘솔을 엽니다.
2. 왼쪽의 탐색 창에서 정책을 선택합니다.

   정책을 처음으로 선택하는 경우 관리형 정책 소개 페이지가 나타납니다. 시작하기를 선택합니다.
3. 페이지 상단에서 정책 생성을 선택합니다.
4. 정책 편집기 섹션에서 JSON 옵션을 선택합니다.
5. JSON 정책 문서를 입력하거나 붙여 넣습니다. IAM 정책 언어에 대한 자세한 내용은 IAM JSON 정책 참조를 참조하세요.
6. 정책 검증 동안 생성된 모든 보안 경고, 오류 또는 일반 경고를 해결하고 다음을 선택합니다.

   > **Note**
   >
   > 언제든지 시각적 편집기 옵션과 JSON 편집기 옵션을 서로 전환할 수 있습니다. 그러나 변경을 적용하거나 시각적 편집기에서 다음을 선택한 경우 IAM은 시각적 편집기에 최적화되도록 정책을 재구성할 수 있습니다. 자세한 내용은 IAM 사용 설명서의 정책 재구성을 참조하십시오.
7. (선택 사항) 에서 정책을 만들거나 편집할 때 템플릿에서 사용할 수 있는 JSON 또는 YAML 정책 템플릿을 생성할 수 있습니다. AWS Management Console AWS CloudFormation

   이렇게 하려면 정책 편집기에서 작업을 선택한 다음 템플릿 생성을 CloudFormation 선택합니다. 자세히 AWS CloudFormation알아보려면 AWS CloudFormation 사용 설명서의 AWS Identity and Access Management 리소스 유형 참조를 참조하십시오.
8. 정책에 권한 추가를 완료했으면 다음을 선택합니다.
9. 검토 및 생성 페이지에서 생성하는 정책의 정책 이름과 설명(선택 사항)을 입력합니다. 이 정책에 정의된 권한을 검토하여 정책이 부여한 권한을 확인합니다.
10. (선택 사항) 태그를 키 값 페어로 연결하여 메타데이터를 정책에 추가합니다. IAM에서 태그 사용에 대한 자세한 내용을 알아보려면 IAM 사용 설명서의 IAM 리소스에 태그 지정을 참조하세요.
11. 정책 생성을 선택하고 새로운 정책을 저장합니다.

시각적 편집기를 사용하여 정책을 생성하려면

1. https://console.aws.amazon.com/iam/ 에서 IAM 콘솔에 AWS Management Console 로그인하고 엽니다.
2. 왼쪽의 탐색 창에서 정책을 선택합니다.

   정책을 처음으로 선택하는 경우 관리형 정책 소개 페이지가 나타납니다. 시작하기(Get Started)를 선택합니다.
3. 정책 생성(Create policy)을 선택합니다.
4. 정책 편집기 섹션에서 서비스 선택 섹션을 찾은 다음 하나를 선택합니다. AWS 서비스상단의 검색 상자를 사용하여 서비스 목록 결과를 제한할 수 있습니다. 시각적 편집기 권한 블록 내에서 하나의 서비스만 선택할 수 있습니다. 둘 이상의 서비스에 액세스 권한을 부여하려면 더 많은 권한 추가를 선택하여 여러 개의 권한 블록을 추가합니다.
5. 허용된 작업에서 정책에 추가할 작업을 선택합니다. 작업을 선택하는 방법은 다음과 같습니다.

   - 모든 작업에 대한 확인란을 선택합니다.
   - 작업 추가를 선택하여 특정 작업의 이름을 입력합니다. 와일드카드 문자 (*) 를 사용하여 여러 동작을 지정할 수 있습니다.
   - 액세스 수준 그룹 중 하나를 선택하여 액세스 수준에 대한 모든 작업(예: 읽기, 쓰기 또는 목록)을 선택합니다.
   - 각 액세스 레벨 그룹을 확장하여 개별 작업을 선택합니다.

   기본적으로 생성되는 정책은 사용자가 선택하는 작업을 허용합니다. 대신 선택한 작업을 거부하려면 Switch to deny permissions(권한 거부로 전환)을 선택합니다. 기본적으로 IAM은 거부하기 때문에, 보안 모범 사례로 사용자에게 필요한 작업과 리소스에만 권한을 허용하는 것이 좋습니다. 다른 명령문이나 정책에서 별도로 허용한 권한을 재정의하려는 경우에만 권한을 거부하는 JSON 문을 만드십시오. 권한 거부의 수가 늘어나면 권한 문제를 해결하기가 더 어려워질 수 있기 때문에 그 수를 최소한으로 제한하는 것이 좋습니다.
6. 리소스에서 이전 단계에서 선택한 서비스 및 작업이 특정 리소스 선택을 지원하지 않는 경우에는 모든 리소스가 허용되며 이 섹션을 편집할 수 없습니다.

   리소스 수준 권한을 지원하는 작업을 하나 이상 선택하면 시각적 편집기에 해당 리소스가 나열됩니다. 그러면 리소스를 확장하여 정책에 대한 리소스를 지정할 수 있습니다.

   다음과 같은 방법으로 리소스를 지정할 수 있습니다.

- ARN 추가를 선택하여 Amazon 리소스 이름(ARN)별로 리소스를 지정합니다. 시각적 ARN 편집기를 사용하거나 ARN을 수동으로 나열할 수 있습니다. ARN 구문에 대한 자세한 내용은 IAM 사용 설명서의 Amazon 리소스 이름 (ARN) 을 참조하십시오. 정책 *Resource* 요소에서 ARN을 사용하는 방법에 대한 자세한 내용은 IAM 사용 설명서의 IAM JSON 정책 요소: 리소스를 참조하십시오.
- 리소스 옆의 이 계정에서 모두를 선택하여 해당 유형의 모든 리소스에 권한을 부여합니다.
- 모두를 선택하여 해당 서비스에 대한 모든 리소스를 선택합니다.

7. (선택 사항) 요청 조건 - 선택 사항을 선택하여 생성하는 정책에 조건을 추가합니다. 조건은 JSON 정책 문의 효과를 제한합니다. 예를 들어 특정 시간 범위 내에 사용자의 요청이 발생하는 경우에만 사용자가 리소스에 대한 작업을 수행할 수 있도록 지정할 수 있습니다. 또한 일반적으로 사용되는 조건을 사용하여 다중 요소 인증 (MFA) 디바이스를 사용하여 사용자를 인증해야 하는지 여부를 제한할 수 있습니다. 또는 요청이 특정 IP 주소 범위에서 발생하도록 요구할 수 있습니다. 정책 조건에서 사용할 수 있는 모든 컨텍스트 키 목록은 서비스 권한 부여 참조의 AWS 서비스에 대한 작업, 리소스 및 조건 키를 참조하십시오.

   조건을 선택하는 방법은 다음과 같습니다.

   - 확인란을 사용하여 일반적으로 사용되는 조건을 선택합니다.
   - 다른 조건 추가를 선택하여 다른 조건을 지정합니다. 조건의 조건 키, 한정자 및 운영자를 선택한 다음 값을 입력합니다. 값을 두 개 이상 추가하려면 추가를 선택합니다. 값이 논리 OR 연산자로 연결된 것으로 간주할 수 있습니다. 마치면 조건 추가를 선택합니다.

   조건을 두 개 이상 추가하려면 다시 다른 조건 추가를 선택합니다. 필요에 따라 반복합니다. 각 조건은 이 시각적 편집기 권한 블록 하나에만 적용됩니다. 권한 블록이 일치하는 것으로 간주되려면 모든 조건이 true여야 합니다. 즉, 조건을 논리 AND 연산자로 연결한다고 가정해 보겠습니다.

   조건 요소에 대한 자세한 내용은 IAM 사용 설명서의 IAM JSON 정책 요소: 조건을 참조하십시오.

8. 더 많은 권한 블록을 추가하려면 더 많은 권한 추가를 선택합니다. 각 블록에 대해 2~5단계를 반복합니다.

> **Note**
>
> 언제든지 시각적 편집기 옵션과 JSON 편집기 옵션을 서로 전환할 수 있습니다. 그러나 변경을 적용하거나 시각적 편집기에서 다음을 선택한 경우 IAM은 시각적 편집기에 최적화

되도록 정책을 재구성할 수 있습니다. 자세한 내용은 IAM 사용 설명서의 정책 재구성을 참조하십시오.

9. (선택 사항) 에서 정책을 생성하거나 편집할 때 템플릿에서 사용할 수 있는 JSON 또는 YAML 정책 템플릿을 생성할 수 있습니다. AWS Management Console AWS CloudFormation

   이렇게 하려면 정책 편집기에서 작업을 선택한 다음 템플릿 생성을 CloudFormation 선택합니다. 자세히 AWS CloudFormation알아보려면 AWS CloudFormation 사용 설명서의 AWS Identity and Access Management 리소스 유형 참조를 참조하십시오.
10. 정책에 권한 추가를 완료했으면 다음을 선택합니다.
11. 검토 및 생성 페이지에서 생성하는 정책의 정책 이름과 설명(선택 사항)을 입력합니다. 이 정책에 정의된 권한을 검토하여 의도한 권한을 부여했는지 확인합니다.
12. (선택 사항) 태그를 키 값 페어로 연결하여 메타데이터를 정책에 추가합니다. IAM에서 태그 사용에 대한 자세한 내용을 알아보려면 IAM 사용 설명서의 IAM 리소스에 태그 지정을 참조하세요.
13. 정책 생성을 선택하고 새로운 정책을 저장합니다.

프로그래밍 방식으로 액세스 권한을 부여하려면

사용자가 AWS 외부 사용자와 상호 작용하려는 경우 프로그래밍 방식의 액세스가 필요합니다. AWS Management Console프로그래밍 방식의 액세스 권한을 부여하는 방법은 액세스하는 사용자 유형에 따라 다릅니다. AWS

사용자에게 프로그래밍 방식 액세스 권한을 부여하려면 다음 옵션 중 하나를 선택합니다.

프로그래밍 방식 액세스가 필요한 사용자는 누구인가요?	To	액세스 권한을 부여하는 사용자
작업 인력 ID (IAM Identity Center가 관리하는 사용자)	임시 자격 증명을 사용하여 AWS CLI, AWS SDK 또는 API에 대한 프로그래밍 요청에 서명할 수 있습니다. AWS	사용하고자 하는 인터페이스에 대한 지침을 따릅니다. • AWS CLI 에 대한 내용은 사용 설명서의 AWS CLI사용을 AWS IAM Identity Center위한 구성을 참조하십시오.AWS Command Line Interface • AWS SDK, 도구 및 AWS API의 경우 AWS SDK 및 도

프로그래밍 방식 액세스가 필요한 사용자는 누구인가요?	To	액세스 권한을 부여하는 사용자
		구 참조 안내서의 IAM ID 센터 인증을 참조하십시오.
IAM	임시 자격 증명을 사용하여 AWS CLI, AWS SDK 또는 API에 대한 프로그래밍 방식 요청에 서명할 수 있습니다. AWS	IAM 사용 설명서의 AWS 리소스와 함께 임시 자격 증명 사용의 지침을 따르십시오.
IAM	(권장되지 않음) 장기 자격 증명을 사용하여 AWS CLI, AWS SDK 또는 API에 대한 프로그래밍 요청에 서명하십시오. AWS	사용하고자 하는 인터페이스에 대한 지침을 따릅니다. • 에 대한 내용은 사용 설명서의 IAM 사용자 자격 증명을 사용한 인증을 참조하십시오. AWS CLIAWS Command Line Interface • AWS SDK 및 도구의 경우 SDK 및 도구 참조 안내서의 장기 자격 증명을 사용한 인증을 참조하십시오.AWS • AWS API의 경우 IAM 사용 설명서의 IAM 사용자의 액세스 키 관리를 참조하십시오.

공격자로부터 보호

다른 AWS 서비스 주체에게 권한을 부여할 때 공격자로부터 보호하는 방법에 대한 자세한 내용은 역할 신뢰 관계의 선택적 조건을 참조하십시오. 정책에 특정 조건을 추가하면 특정 유형의 공격 (혼동 대리 공격) 을 방지하는 데 도움이 될 수 있습니다. 이러한 공격은 특정 주체가 서비스 간 사칭 등의 작업을 수행하도록 강요할 때 발생하는 혼동 보조 공격입니다. 정책 조건에 대한 일반적인 내용은 을 참조하십시오. 정책에서 조건 지정

AWS Control Tower에서 자격 증명 기반 정책을 사용하는 방법에 대한 자세한 내용은 을 참조하십시오. AWS Control Tower에 대한 자격 증명 기반 정책 (IAM 정책) 사용 사용자, 그룹, 역할 및 권한에 대한 자세한 내용은 IAM 사용 설명서의 자격 증명(사용자, 그룹 및 역할)을 참조하세요.

리소스 기반 정책

Amazon S3과 같은 다른 서비스도 리소스 기반 권한 정책을 지원합니다. 예를 들어, 정책을 S3 버킷에 연결하여 해당 버킷에 대한 액세스 권한을 관리할 수 있습니다. AWS Control Tower는 리소스 기반 정책을 지원하지 않습니다.

정책 요소 지정: 조치, 효과, 원칙

AWS Control Tower 콘솔 또는 랜딩 존 API를 통해 랜딩 존을 설정하고 관리할 수 있습니다. 랜딩 존을 설정하려면 IAM 정책에 정의된 관리 권한을 가진 IAM 사용자여야 합니다.

정책에서 식별할 수 있는 가장 기본적인 요소는 다음과 같습니다.

- 리소스 – 정책에서 Amazon 리소스 이름(ARN)을 사용하여 정책을 적용할 리소스를 식별합니다. 자세한 정보는 AWS Control 타워 리소스 및 운영을 참조하세요.
- 조치 – 조치 키워드를 사용하여 허용 또는 거부할 리소스 작업을 식별합니다. 수행할 수 있는 작업 유형에 대한 자세한 내용은 AWS Control Tower에서 정의한 작업을 참조하십시오.
- 결과 – 사용자가 특정 작업을 요청하는 경우의 결과를 지정합니다. 이는 허용 또는 거부 중에 하나가 될 수 있습니다. 명시적으로 리소스에 대한 액세스 권한을 부여(허용)하지 않는 경우, 액세스는 묵시적으로 거부됩니다. 다른 정책에서 액세스 권한을 부여하는 경우라도 사용자가 해당 리소스에 액세스할 수 없도록 하기 위해 리소스에 대한 권한을 명시적으로 거부할 수도 있습니다.
- 보안 주체 — 자격 증명 기반 정책 (IAM 정책) 에서는 정책이 연결된 사용자가 암시적 보안 주체입니다. 리소스 기반 정책의 경우, 사용자, 계정, 서비스 또는 권한의 수신자인 기타 개체를 지정합니다 (리소스 기반 정책에만 해당). AWS Control Tower는 리소스 기반 정책을 지원하지 않습니다.

IAM 정책 구문과 설명에 대한 자세한 내용은 IAM 사용 설명서의 AWS IAM 정책 참조를 참조하십시오.

정책에서 조건 지정

권한을 부여할 때 IAM 정책 언어를 사용하여 정책이 적용되는 조건을 지정할 수 있습니다. 예를 들어, 특정 날짜 이후에만 정책을 적용할 수 있습니다. 정책 언어에서의 조건 지정에 관한 자세한 설명은 IAM 사용자 가이드의 조건을 참조하십시오.

조건을 표현하기 위해 사전 정의된 조건 키를 사용할 수 있습니다. AWS Control Tower에만 적용되는 조건 키는 없습니다. 하지만 필요에 따라 사용할 수 있는 AWS-wide 조건 키가 있습니다. AWS-wide 키의 전체 목록은 IAM 사용 설명서의 조건에 사용할 수 있는 키를 참조하십시오.

서비스 간 사칭 방지

에서 AWS, 크로스 서비스 사칭은 대리인 혼동을 야기할 수 있습니다. 한 서비스가 다른 서비스를 호출할 때 서비스 간 사칭은 한 서비스가 다른 서비스를 조작하여 다른 방식으로는 허용되지 않는 방식으로 권한을 사용하여 고객의 리소스에 대해 조치를 취하는 경우 발생합니다. 이 공격을 방지하기 위해 에서는 합법적인 권한을 가진 서비스만 계정의 리소스에 액세스할 수 있도록 데이터를 보호하는 데 도움이 되는 도구를 AWS 제공합니다.

정책의 `aws:SourceArn` 및 `aws:SourceAccount` 조건을 사용하여 AWS Control Tower가 리소스에 액세스할 수 있도록 다른 서비스에 부여하는 권한을 제한하는 것이 좋습니다.

- 서비스 간 액세스에 리소스를 하나만 연결하려는 `aws:SourceArn` 경우에 사용하십시오.
- `aws:SourceAccount`해당 계정의 모든 리소스를 서비스 간 사용에 연결할 수 있도록 허용하려는 경우에 사용합니다.
- `aws:SourceArn`값에 계정 ID (예: Amazon S3 버킷의 ARN) 가 포함되어 있지 않은 경우 두 조건을 모두 사용하여 권한을 제한해야 합니다.
- 두 조건을 모두 사용하고 `aws:SourceArn` 값에 계정 ID가 포함된 경우 동일한 정책 설명에서 사용할 때 `aws:SourceArn` 값의 값과 계정이 동일한 계정 ID를 표시해야 합니다. `aws:SourceAccount`

자세한 정보와 지침은 https://docs.aws.amazon.com/controltower/latest/userguide/conditions-for-role-trust.html을 참조하세요.

AWS Control Tower에 대한 자격 증명 기반 정책 (IAM 정책) 사용

이 주제에서는 계정 관리자가 IAM ID (즉, 사용자, 그룹, 역할) 에 권한 정책을 연결하여 AWS Control Tower 리소스에서 작업을 수행할 수 있는 권한을 부여하는 방법을 보여주는 ID 기반 정책의 예를 제공합니다.

> **Important**
>
> 먼저 AWS Control Tower 리소스에 대한 액세스를 관리하는 데 사용할 수 있는 기본 개념과 옵션을 설명하는 소개 주제를 검토하는 것이 좋습니다. 자세한 정보는 AWS Control Tower 리소스에 대한 액세스 권한 관리 개요을 참조하세요.

AWS Control Tower 콘솔 사용에 필요한 권한

AWS Control Tower는 랜딩 존을 설정할 때 자동으로 세 가지 역할을 생성합니다. 콘솔 액세스를 허용하려면 세 가지 역할 모두 필요합니다. AWS Control Tower는 최소 작업 및 리소스 세트에 대한 액세스를 제한하는 모범 사례로서 권한을 세 가지 역할로 분할합니다.

세 가지 필수 역할

- AWS ControlTowerAdmin 역할
- AWS ControlTowerStackSetRole
- AWS ControlTowerCloudTrailRole

이러한 역할에 대한 역할 신뢰 정책에 대한 액세스를 제한하는 것이 좋습니다. 자세한 내용은 역할 신뢰 관계의 선택적 조건을 참조하십시오.

AWS ControlTowerAdmin 역할

이 역할을 통해 AWS Control Tower는 착륙 지대를 유지하는 데 중요한 인프라에 액세스할 수 있습니다. `AWS ControlTowerAdmin`역할에는 연결된 관리형 정책과 IAM 역할을 위한 역할 신뢰 정책이 필요합니다. 역할 신뢰 정책은 역할을 수임할 수 있는 보안 주체를 지정하는 리소스 기반 정책입니다.

다음은 이 역할 신뢰 정책의 예제 코드입니다.

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

CLI에서 이 역할을 생성하여 이라는 파일에 넣는 AWS CLI `trust.json` 명령 예는 다음과 같습니다.

```
aws iam create-role --role-name AWSControlTowerAdmin --path /service-role/ --assume-
role-policy-document file://trust.json
```

이 역할에는 두 개의 IAM 정책이 필요합니다.

1. 인라인 정책, 예:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "ec2:DescribeAvailabilityZones",
            "Resource": "*"
        }
    ]
}
```

2. 다음에 나오는 관리형 정책은 다음과 같습니다. `AWS ControlTowerServiceRolePolicy`

AWS ControlTowerServiceRolePolicy

AWS ControlTowerServiceRolePolicy이 정책은 AWS CloudFormation 스택세트와 스택 인스턴스, AWS CloudTrail 로그 파일, AWS Control Tower의 구성 애그리게이터, AWS Control Tower에서 관리하는 AWS Organizations 계정 및 조직 단위 (OU) 와 같은 AWS Control Tower 리소스를 생성하고 관리할 권한을 정의하는 AWS관리형 정책입니다.

이 관리형 정책에 대한 업데이트는 표에 요약되어 있습니다. AWS Control Tower의 관리형 정책

자세한 내용은 `AWSControlTowerServiceRolePolicy`AWS 관리형 정책 참조 안내서를 참조하십시오.

관리형 정책 이름: `AWS ControlTowerServiceRolePolicy`

의 JSON `AWS ControlTowerServiceRolePolicy` 아티팩트는 다음과 같습니다.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "cloudformation:CreateStack",
                "cloudformation:CreateStackInstances",
                "cloudformation:CreateStackSet",
```

```
                "cloudformation:DeleteStack",
                "cloudformation:DeleteStackInstances",
                "cloudformation:DeleteStackSet",
                "cloudformation:DescribeStackInstance",
                "cloudformation:DescribeStacks",
                "cloudformation:DescribeStackSet",
                "cloudformation:DescribeStackSetOperation",
                "cloudformation:ListStackInstances",
                "cloudformation:UpdateStack",
                "cloudformation:UpdateStackInstances",
                "cloudformation:UpdateStackSet"
            ],
            "Resource": [
                "arn:aws:cloudformation:*:*:type/resource/AWS-IAM-Role"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "account:EnableRegion",
                "account:ListRegions",
                "account:GetRegionOptStatus"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "cloudformation:CreateStack",
                "cloudformation:CreateStackInstances",
                "cloudformation:CreateStackSet",
                "cloudformation:DeleteStack",
                "cloudformation:DeleteStackInstances",
                "cloudformation:DeleteStackSet",
                "cloudformation:DescribeStackInstance",
                "cloudformation:DescribeStacks",
                "cloudformation:DescribeStackSet",
                "cloudformation:DescribeStackSetOperation",
                "cloudformation:GetTemplate",
                "cloudformation:ListStackInstances",
                "cloudformation:UpdateStack",
                "cloudformation:UpdateStackInstances",
                "cloudformation:UpdateStackSet"
            ],
```

```
            "Resource": [
                "arn:aws:cloudformation:*:*:stack/AWSControlTower*/*",
                "arn:aws:cloudformation:*:*:stack/StackSet-AWSControlTower*/*",
                "arn:aws:cloudformation:*:*:stackset/AWSControlTower*:*",
                "arn:aws:cloudformation:*:*:stackset-target/AWSControlTower*/*"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "cloudtrail:CreateTrail",
                "cloudtrail:DeleteTrail",
                "cloudtrail:GetTrailStatus",
                "cloudtrail:StartLogging",
                "cloudtrail:StopLogging",
                "cloudtrail:UpdateTrail",
                "cloudtrail:PutEventSelectors",
                "logs:CreateLogStream",
                "logs:PutLogEvents",
                "logs:PutRetentionPolicy"
            ],
            "Resource": [
                "arn:aws:logs:*:*:log-group:aws-controltower/CloudTrailLogs:*",
                "arn:aws:cloudtrail:*:*:trail/aws-controltower*"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "s3:GetObject"
            ],
            "Resource": [
                "arn:aws:s3:::aws-controltower*/*"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "sts:AssumeRole"
            ],
            "Resource": [
                "arn:aws:iam::*:role/AWSControlTowerExecution",
                "arn:aws:iam::*:role/AWSControlTowerBlueprintAccess"
            ]
```

```
        },
        {
            "Effect": "Allow",
            "Action": [
                "cloudtrail:DescribeTrails",
                "ec2:DescribeAvailabilityZones",
                "iam:ListRoles",
                "logs:CreateLogGroup",
                "logs:DescribeLogGroups",
                "organizations:CreateAccount",
                "organizations:DescribeAccount",
                "organizations:DescribeCreateAccountStatus",
                "organizations:DescribeOrganization",
                "organizations:DescribeOrganizationalUnit",
                "organizations:DescribePolicy",
                "organizations:ListAccounts",
                "organizations:ListAccountsForParent",
                "organizations:ListAWSServiceAccessForOrganization",
                "organizations:ListChildren",
                "organizations:ListOrganizationalUnitsForParent",
                "organizations:ListParents",
                "organizations:ListPoliciesForTarget",
                "organizations:ListTargetsForPolicy",
                "organizations:ListRoots",
                "organizations:MoveAccount",
                "servicecatalog:AssociatePrincipalWithPortfolio"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "iam:GetRole",
                "iam:GetUser",
                "iam:ListAttachedRolePolicies",
                "iam:GetRolePolicy"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "iam:PassRole"
            ],
```

```
            "Resource": [
                "arn:aws:iam::*:role/service-role/AWSControlTowerStackSetRole",
                "arn:aws:iam::*:role/service-role/AWSControlTowerCloudTrailRole",
                "arn:aws:iam::*:role/service-role/
AWSControlTowerConfigAggregatorRoleForOrganizations"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "config:DeleteConfigurationAggregator",
                "config:PutConfigurationAggregator",
                "config:TagResource"
            ],
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "aws:ResourceTag/aws-control-tower": "managed-by-control-tower"
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": [
                "organizations:EnableAWSServiceAccess",
                "organizations:DisableAWSServiceAccess"
            ],
            "Resource": "*",
            "Condition": {
                "StringLike": {
                    "organizations:ServicePrincipal": [
                        "config.amazonaws.com",
                        "cloudtrail.amazonaws.com"
                    ]
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": "iam:CreateServiceLinkedRole",
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "iam:AWSServiceName": "cloudtrail.amazonaws.com"
```

```
                }
            }
        }
    ]
}
```

역할 신뢰 정책:

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

인라인 정책은 다음과 같습니다. AWSControlTowerAdminPolicy

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": "ec2:DescribeAvailabilityZones",
            "Resource": "*",
            "Effect": "Allow"
        }
    ]
}
```

AWS ControlTowerStackSetRole

AWS CloudFormation 이 역할을 맡아 AWS Control Tower에서 생성한 계정에 스택 세트를 배포합니다. 인라인 정책:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": [
                "sts:AssumeRole"
            ],
            "Resource": [
                "arn:aws:iam::*:role/AWSControlTowerExecution"
            ],
            "Effect": "Allow"
        }
    ]
}
```

신뢰 정책

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

AWS ControlTowerCloudTrailRole

AWS Control Tower는 모범 CloudTrail 사례로서 활성화하고 이 역할을 제공합니다 CloudTrail. CloudTrail이 역할을 맡아 CloudTrail 로그를 생성하고 게시합니다. 인라인 정책:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": "logs:CreateLogStream",
            "Resource": "arn:aws:logs:*:*:log-group:aws-controltower/CloudTrailLogs:*",
```

```
            "Effect": "Allow"
        },
        {
            "Action": "logs:PutLogEvents",
            "Resource": "arn:aws:logs:*:*:log-group:aws-controltower/CloudTrailLogs:*",
            "Effect": "Allow"
        }
    ]
}
```

신뢰 정책

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

AWSControlTowerBlueprintAccess 역할 요구 사항

AWS Control Tower에서는 동일한 조직 내의 지정된 블루프린트 허브 계정에서 `AWSControlTowerBlueprintAccess` 역할을 생성해야 합니다.

역할 이름

역할 이름은 `AWSControlTowerBlueprintAccess`이어야 합니다.

역할 신뢰 정책

다음 주체를 신뢰하도록 역할을 설정해야 합니다.

- 관리 계정에서 AWS Control Tower를 사용하는 주체
- 관리 계정에서의 `AWSControlTowerAdmin` 역할.

다음 예는 최소 권한 신뢰 정책을 보여줍니다. 자체 정책을 만들 때는 *YourManagementAccountId*용어를 AWS Control Tower 관리 계정의 실제 계정 *YourControlTowerUserRole*ID로 바꾸고, 이 용어는 관리 계정의 IAM 역할 식별자로 바꾸십시오.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "AWS": [
                    "arn:aws:iam::YourManagementAccountId:role/service-role/
AWSControlTowerAdmin",

 "arn:aws:iam::YourManagementAccountId:role/YourControlTowerUserRole"
                ]
            },
            "Action": "sts:AssumeRole",
            "Condition": {}
        }
    ]
}
```

역할 권한

관리형 정책을 역할에 AWSServiceCatalogAdminFullAccess연결해야 합니다.

AWSServiceRoleForAWSControlTower

이 역할을 통해 AWS Control Tower는 Log Archive 계정, 감사 계정 및 멤버 계정에 대한 액세스 권한을 부여하여 드리프트 리소스 알림 등 랜딩 존 유지 관리에 중요한 작업을 수행할 수 있습니다.

이 `AWSServiceRoleForAWSControlTower` 역할에는 IAM 역할을 위한 연결된 관리형 정책과 역할 신뢰 정책이 필요합니다.

이 역할의 관리형 정책: `AWSControlTowerAccountServiceRolePolicy`

역할 신뢰 정책:

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

```
            "Effect": "Allow",
            "Principal": {
                "Service": "controltower.amazonaws.com"
            },
            "Action": "sts:AssumeRole"
        }
    ]
}
```

AWSControlTowerAccountServiceRolePolicy

이 AWS관리형 정책을 통해 AWS Control Tower는 사용자를 대신하여 자동화된 계정 구성 및 중앙 집중식 거버넌스를 제공하는 AWS 서비스를 호출할 수 있습니다.

이 정책에는 Security Hub 서비스 관리형 표준: AWS Control Tower의 일부인 Security Hub 컨트롤에서 관리하는 리소스에 대한 AWS Security Hub 결과 전달을 구현할 수 있는 AWS Control Tower의 최소 권한이 포함되어 있으며, 고객 계정 관리 기능을 제한하는 변경을 방지합니다. 이는 고객이 직접 시작하지 않는 백그라운드 AWS Security Hub 드리프트 탐지 프로세스의 일부입니다.

이 정책은 각 멤버 계정에서 Security Hub 컨트롤에 대한 Amazon EventBridge 규칙을 생성할 수 있는 권한을 부여하며, 이러한 규칙은 정확한 규칙을 지정해야 합니다 EventPattern. 또한 규칙은 서비스 주체가 관리하는 규칙에서만 작동할 수 있습니다.

서비스 주체: `controltower.amazonaws.com`

의 JSON `AWSControlTowerAccountServiceRolePolicy` 아티팩트는 다음과 같습니다.

```
{
 "Version": "2012-10-17",
 "Statement": [
  {
  //For creating the managed rule
   "Sid": "AllowPutRuleOnSpecificSourcesAndDetailTypes",
   "Effect": "Allow",
   "Action": "events:PutRule",
   "Resource": "arn:aws:events:*:*:rule/*ControlTower*",
   "Condition": {
    "ForAnyValue:StringEquals": {
     "events:source": "aws.securityhub"
    },
    "Null": {
     "events:detail-type": "false"
    },
```

```
    "StringEquals": {
     "events:ManagedBy": "controltower.amazonaws.com",
     "events:detail-type": "Security Hub Findings - Imported"
    }
   }
  },
  // Other operations to manage the managed rule
  {
   "Sid": "AllowOtherOperationsOnRulesManagedByControlTower",
   "Effect": "Allow",
   "Action": [
    "events:DeleteRule",
    "events:EnableRule",
    "events:DisableRule",
    "events:PutTargets",
    "events:RemoveTargets"
   ],
   "Resource": "arn:aws:events:*:*:rule/*ControlTower*",
   "Condition": {
    "StringEquals": {
     "events:ManagedBy": "controltower.amazonaws.com"
    }
   }
  },
  // More managed rule permissions
  {
   "Sid": "AllowDescribeOperationsOnRulesManagedByControlTower",
   "Effect": "Allow",
   "Action": [
    "events:DescribeRule",
    "events:ListTargetsByRule"
   ],
   "Resource": "arn:aws:events:*:*:rule/*ControlTower*"
  },
  // Add permission to publish the security notifications to SNS
  {
   "Sid": "AllowControlTowerToPublishSecurityNotifications",
   "Effect": "Allow",
   "Action": "sns:publish",
   "Resource": "arn:aws:sns:*:*:aws-controltower-AggregateSecurityNotifications",
   "Condition": {
    "StringEquals": {
     "aws:PrincipalAccount": "${aws:ResourceAccount}"
    }
```

```
    }
   },
   // For drift verification
   {
    "Sid": "AllowActionsForSecurityHubIntegration",
    "Effect": "Allow",
    "Action": [
     "securityhub:DescribeStandardsControls",
     "securityhub:GetEnabledStandards"
    ],
    "Resource": "arn:aws:securityhub:*:*:hub/default"
   }
  ]
}
```

이 관리형 정책에 대한 업데이트는 표에 요약되어 있습니다. AWS Control Tower의 관리형 정책

AWS Control Tower의 관리형 정책

AWS 에서 생성하고 관리하는 독립형 IAM 정책을 제공하여 많은 일반적인 사용 사례를 해결합니다. AWS관리형 정책은 사용자가 필요한 권한을 조사할 필요가 없도록 일반 사용 사례에 필요한 권한을 부여합니다. 자세한 내용은 IAM 사용 설명서의 AWS 관리형 정책을 참조하세요.

변경 사항	설명	날짜
AWSControlTowerAccountServiceRolePolicy— 새 정책	AWS Control Tower는 AWS Control Tower가 이벤트 규칙을 생성 및 관리하고, 해당 규칙을 기반으로 Security Hub와 관련된 제어에 대한 드리프트 감지를 관리할 수 있도록 하는 새로운 서비스 연결 역할을 추가했습니다. 이러한 변경은 리소스가 Security Hub 서비스 관리형 표준: AWS Control Tower의 일부인 Security Hub 컨트롤과 관련된 경우 고객이 콘솔에서 드리	2023년 5월 22일

변경 사항	설명	날짜
	프트된 리소스를 볼 수 있도록 하기 위해 필요합니다.	
AWS ControlTowerServiceRolePolicy-기존 정책 업데이트	AWS Control Tower는 랜딩 존에 있는 고객 계정 (관리 AWS 계정 `EnableRegion` `ListRegions` , 로그 아카이브 계정, 감사 계정, OU 회원 계정) 에 옵트인을 AWS 리전 사용할 수 있도록 AWS Control Tower가, 계정 관리 서비스로 구현된 API를 호출할 수 있는 새로운 권한을 추가했습니다. `GetRegionOptStatus` 고객이 AWS Control Tower의 지역 거버넌스를 옵트인 지역으로 확장할 수 있도록 하려면 이러한 변경이 필요합니다.	2023년 4월 6일

변경 사항	설명	날짜
AWS ControlTowerServiceRolePolicy-기존 정책 업데이트	AWS Control Tower는 하나 이상의 Service Catalog 제품에 저장된 사전 정의된 블루프린트를 포함하는 조직의 전용 계정인 블루프린트 (허브) 계정에서 AWS Control Tower가 `AWSControlTowerBlueprintAccess` 역할을 맡을 수 있도록 하는 새로운 권한을 추가했습니다. AWS Control Tower는 Service Catalog 포트폴리오 생성, 요청된 청사진 제품 추가, 계정 프로비저닝 시 요청된 회원 계정과 포트폴리오 공유라는 세 가지 작업을 수행하는 `AWSControlTowerBlueprintAccess` 역할을 맡습니다. 고객이 AWS Control Tower Account Factory를 통해 사용자 지정 계정을 프로비저닝할 수 있으려면 이러한 변경이 필요합니다.	2022년 10월 28일

변경 사항	설명	날짜
AWS ControlTowerServiceRolePolicy-기존 정책 업데이트	AWS Control Tower는 고객이 Landing Zone 버전 3.0부터 조직 수준의 AWS CloudTrail 트레일을 설정할 수 있는 새로운 권한을 추가했습니다. 조직 기반 CloudTrail 기능을 사용하려면 고객이 CloudTrail 서비스에 대한 신뢰할 수 있는 액세스를 활성화해야 하며, IAM 사용자 또는 역할은 관리 계정에서 조직 수준 추적을 생성할 권한이 있어야 합니다.	2022년 6월 20일
AWS ControlTowerServiceRolePolicy-기존 정책 업데이트	AWS Control Tower는 고객이 KMS 키 암호화를 사용할 수 있는 새로운 권한을 추가했습니다. KMS 기능을 사용하면 고객이 자신의 KMS 키를 제공하여 로그를 암호화할 수 있습니다. CloudTrail 고객은 또한 landing zone 업데이트 또는 수리 중에 KMS 키를 변경할 수 있습니다. KMS 키를 업데이트할 때는 API를 호출할 권한이 AWS CloudFormation 필요합니다. AWS CloudTrail `PutEventSelector` 정책 변경은 AWS ControlTowerAdmin역할이 AWS CloudTrail `PutEventSelector` API를 호출할 수 있도록 허용하는 것입니다.	2021년 7월 28일

변경 사항	설명	날짜
AWS Control Tower는 변경 사항 추적을 시작했습니다.	AWS Control Tower는 AWS 관리형 정책의 변경 사항을 추적하기 시작했습니다.	2021년 5월 27일

AWS Control Tower의 보안

클라우드 AWS 보안이 최우선 과제입니다. AWS 고객은 가장 보안에 민감한 조직의 요구 사항을 충족하도록 구축된 데이터 센터 및 네트워크 아키텍처의 혜택을 누릴 수 있습니다.

보안은 기업과 기업 간의 AWS 공동 책임입니다. 공동 책임 모델은 이 사항을 클라우드 내 보안 및 클라우드의 보안으로 설명합니다.

- 클라우드 보안 - AWS 클라우드에서 AWS 서비스를 실행하는 인프라를 보호하는 역할을 합니다. AWS AWS 또한 안전하게 사용할 수 있는 서비스를 제공합니다. 서드 파티 감사자는 정기적으로 AWS 규정 준수 프로그램의 일환으로 보안 효과를 테스트하고 검증합니다. AWS Control Tower에 적용되는 규정 준수 프로그램에 대해 자세히 알아보려면 규정 준수 프로그램별 범위 내AWS 서비스를 참조하십시오.
- 클라우드에서의 보안 — 귀하의 책임은 사용하는 AWS 서비스에 따라 결정됩니다. 또한 데이터의 민감도, 조직의 요구 사항, 관련 법률 및 규정을 비롯한 기타 요소에 대해서도 책임이 있습니다.

이 설명서는 AWS Control Tower를 사용할 때 공동 책임 모델을 적용하는 방법을 이해하는 데 도움이 됩니다. 다음 주제에서는 보안 및 규정 준수 목표를 충족하도록 AWS Control Tower를 구성하는 방법을 보여줍니다. 또한 AWS Control Tower 리소스를 모니터링하고 보호하는 데 도움이 되는 다른 AWS 서비스를 사용하는 방법도 배웁니다.

AWS Control Tower에서의 데이터 보호

AWS 공동 책임 모델 AWS Control Tower의 데이터 보호에 적용됩니다. 이 모델에 설명된 대로, AWS는 모든 것을 실행하는 글로벌 인프라를 보호할 책임이 AWS 클라우드있습니다. 사용자는 인프라에서 호스팅되는 콘텐츠를 관리해야 합니다. 사용하는 AWS 서비스 의 보안 구성과 관리 작업에 대한 책임도 사용자에게 있습니다. 데이터 프라이버시에 대한 자세한 내용은 데이터 프라이버시 FAQ를 참조하세요. 유럽의 데이터 보호에 대한 자세한 내용은 AWS 보안 블로그의 AWS 공동 책임 모델 및 GDPR 블로그 게시물을 참조하십시오.

데이터 보호를 위해 AWS 계정 자격 증명을 보호하고 AWS IAM Identity Center OR AWS Identity and Access Management (IAM) 을 사용하여 개별 사용자를 설정하는 것이 좋습니다. 이렇게 하면 개별 사용자에게 자신의 직무를 충실히 이행하는 데 필요한 권한만 부여됩니다. 또한 다음과 같은 방법으로 데이터를 보호하는 것이 좋습니다.

- 각 계정에 멀티 팩터 인증 설정(MFA)을 사용하세요.

- SSL/TLS를 사용하여 리소스와 통신할 수 있습니다. AWS TLS 1.2는 필수이며 TLS 1.3를 권장합니다.
- 를 사용하여 API 및 사용자 활동 로깅을 설정합니다. AWS CloudTrail
- 포함된 모든 기본 보안 제어와 함께 AWS 암호화 솔루션을 사용하십시오 AWS 서비스.
- Amazon S3에 저장된 민감한 데이터를 검색하고 보호하는 데 도움이 되는 Amazon Macie와 같은 고급 관리형 보안 서비스를 사용하세요.
- 명령줄 인터페이스 또는 API를 AWS 통해 액세스할 때 FIPS 140-2로 검증된 암호화 모듈이 필요한 경우 FIPS 엔드포인트를 사용하십시오. 사용 가능한 FIPS 엔드포인트에 대한 자세한 내용은 Federal Information Processing Standard(FIPS) 140-2를 참조하십시오.

고객의 이메일 주소와 같은 기밀 정보나 중요한 정보는 태그나 이름 필드와 같은 자유 양식 필드에 입력하지 않는 것이 좋습니다. 여기에는 AWS Control Tower 또는 다른 곳에서 콘솔 AWS CLI, API 또는 AWS SDK를 AWS 서비스 사용하여 작업하는 경우가 포함됩니다. 이름에 사용되는 태그 또는 자유 형식 텍스트 필드에 입력하는 모든 데이터는 청구 또는 진단 로그에 사용될 수 있습니다. 외부 서버에 URL을 제공할 때 해당 서버에 대한 요청을 검증하기 위해 보안 인증 정보를 URL에 포함시켜서는 안 됩니다.

> **Note**
>
> 를 사용한 사용자 활동 AWS CloudTrail 로깅은 랜딩 존을 설정할 때 AWS Control Tower에서 자동으로 처리됩니다.

데이터 보호에 대한 자세한 내용은 AWS 보안 블로그의 AWS 공동 책임 모델 및 GDPR 블로그 게시물을 참조하십시오. AWS Control Tower는 랜딩 존에 있는 콘텐츠를 보호하는 데 사용할 수 있는 다음과 같은 옵션을 제공합니다.

주제

- 유휴 데이터 암호화
- 전송 중 데이터 암호화
- 콘텐츠에 대한 액세스 제한

유휴 데이터 암호화

AWS Control Tower는 Amazon S3 버킷과 Amazon DynamoDB 데이터베이스를 사용합니다. 이 데이터베이스는 Amazon S3 관리형 키 (SSE-S3) 를 사용하여 저장 시 암호화되어 랜딩 존을 지원합니다. 이 암호화는 landing Zone을 설정할 때 기본적으로 구성됩니다. 선택적으로 KMS 암호화 키로 리소스를 암호화하도록 landding Zone을 구성할 수 있습니다. 또한 랜딩 존에서 사용하는 서비스를 지원하는 서비스에 대해 저장 중 암호화를 설정할 수 있습니다. 자세한 내용은 해당 서비스 온라인 설명서의 보안 장을 참조하십시오.

전송 중 데이터 암호화

AWS Control Tower는 랜딩 존을 지원하기 위해 전송 계층 보안 (TLS) 및 클라이언트 측 암호화를 사용하여 전송 중 암호화를 수행합니다. 또한 AWS Control Tower에 액세스하려면 HTTPS 엔드포인트를 통해서만 액세스할 수 있는 콘솔을 사용해야 합니다. 이 암호화는 landing Zone을 설정할 때 기본적으로 구성됩니다.

콘텐츠에 대한 액세스 제한

가장 좋은 방법은 적절한 사용자 하위 집합에 대한 액세스를 제한하는 것입니다. AWS Control Tower를 사용하면 중앙 클라우드 관리자와 최종 사용자에게 올바른 IAM 권한이 있는지 확인하거나, IAM Identity Center 사용자의 경우 올바른 그룹에 속해 있는지 확인함으로써 이 작업을 수행할 수 있습니다.

- IAM 엔티티의 역할 및 정책에 대한 자세한 내용은 IAM 사용 설명서를 참조하세요.
- 랜딩 존을 설정할 때 생성되는 IAM Identity Center 그룹에 대한 자세한 내용은 을 참조하십시오AWS 컨트롤 타워용 IAM 자격 증명 센터 그룹.

AWS Control Tower의 규정 준수 검증

AWS Control Tower는 조직이 규제 및 모범 사례를 통해 규정 준수 요구 사항을 충족하도록 지원하는 잘 설계된 서비스입니다. 또한 타사 감사자는 여러 규정 AWS 준수 프로그램의 일환으로 랜딩 존에서 사용할 수 있는 여러 서비스의 보안 및 규정 준수를 평가합니다. 여기에는 SOC, PCI, FedRAMP, HIPAA 등이 포함됩니다.

특정 규정 준수 프로그램 범위 내 AWS 서비스 목록은 규정 준수 프로그램별 범위 내AWS 서비스를 참조하십시오. 일반 정보는 AWS 규정 준수 프로그램을 참조하십시오.

를 사용하여 타사 감사 보고서를 다운로드할 수 AWS Artifact있습니다. 자세한 내용은 사용 AWS Artifact 안내서의 AWS Artifact에서 보고서 다운로드를 참조하십시오.

AWS Control Tower를 사용할 때의 규정 준수 책임은 데이터의 민감도, 회사의 규정 준수 목표, 관련 법률 및 규정에 따라 결정됩니다. AWS 규정 준수에 도움이 되는 다음 리소스를 제공합니다.

- 보안 및 규정 준수 퀵 스타트 가이드 - 이 배포 가이드에서는 아키텍처 고려 사항을 설명하고 보안 및 규정 준수에 중점을 둔 기본 환경을 배포하기 위한 단계를 제공합니다. AWS
- Amazon Web Services의 HIPAA 보안 및 규정 준수를 위한 설계 — 이 백서에서는 기업이 HIPAA 준수 애플리케이션을 만드는 AWS 데 사용할 수 있는 방법을 설명합니다.
- AWS 규정 준수 리소스 — 이 워크북 및 가이드 모음은 해당 산업 및 지역에 적용될 수 있습니다.
- AWS Config— 이 AWS 서비스는 리소스 구성이 내부 관행, 업계 지침 및 규정을 얼마나 잘 준수하는지 평가합니다.
- AWS Security Hub— 이 AWS 서비스는 보안 업계 표준 및 모범 사례를 준수하는지 확인하는 데 도움이 AWS 되는 보안 상태를 종합적으로 보여줍니다.

AWS Control Tower의 레질리언스

AWS 글로벌 인프라는 AWS 지역 및 가용 영역을 중심으로 구축됩니다.

AWS 지역은 물리적으로 분리되고 격리된 여러 가용 영역을 제공하며, 이러한 가용 영역은 지연 시간이 짧고 처리량이 높으며 중복성이 높은 네트워킹을 통해 연결됩니다. 가용 영역으로 중단 없이 가용 영역 간에 자동으로 장애 조치가 이루어지는 애플리케이션 및 데이터베이스를 설계하고 운영할 수 있습니다. 가용 영역은 기존의 단일 또는 복수 데이터 센터 인프라보다 가용성, 내결함성, 확장성이 뛰어납니다.

AWS Control Tower를 사용할 수 AWS 리전 있는 곳의 목록은 을 참조하십시오AWS 지역별로 AWS Control Tower를 활용하는 방법.

홈 리전은 랜딩 존이 설정된 AWS 지역으로 정의됩니다.

AWS 지역 및 가용 영역에 대한 자세한 내용은 AWS 글로벌 인프라를 참조하십시오.

AWS Control Tower의 인프라 보안

AWS Control Tower는 Amazon Web Services: 보안 프로세스 개요 백서에 설명된 AWS 글로벌 네트워크 보안 절차에 따라 보호됩니다.

AWS 게시된 API 호출을 사용하여 네트워크를 통해 랜딩 영역 내의 AWS 서비스 및 리소스에 액세스할 수 있습니다. 전송 계층 보안 (TLS) 1.2가 필요하며 전송 계층 보안 (TLS) 1.3 이상을 권장합니다. 클

라이언트는 Ephemeral Diffie-Hellman(DHE) 또는 Elliptic Curve Ephemeral Diffie-Hellman(ECDHE)과 같은 PFS(전달 완전 보안, Perfect Forward Secrecy)가 포함된 암호 제품군도 지원해야 합니다. Java 7 이상의 최신 시스템은 대부분 이러한 모드를 지원합니다.

또한 요청은 액세스 키 ID 및 IAM 주체와 관련된 비밀 액세스 키를 사용하여 서명해야 합니다. 또는 AWS Security Token Service(AWS STS)를 사용하여 임시 보안 인증을 생성하여 요청에 서명할 수 있습니다.

보안 그룹을 설정하여 AWS Control Tower 랜딩 존 워크로드에 추가 네트워크 인프라 보안을 제공할 수 있습니다. 자세한 내용은 둘러보기: AWS 방화벽 관리자를 사용하여 AWS 컨트롤 타워에 보안 그룹 설정을(를) 참조하세요.

AWS Control Tower에서의 로깅 및 모니터링

모니터링을 통해 잠재적 인시던트를 대비 및 대응할 수 있습니다. 모니터링 활동의 결과는 로그 파일에 저장됩니다. 따라서 로깅과 모니터링은 밀접하게 관련된 개념이며, AWS Control Tower의 체계적인 아키텍처에서 중요한 부분을 차지합니다.

landing Zone을 설정할 때 생성되는 공유 계정 중 하나가 로그 아카이브 계정입니다. 모든 공유 및 회원 계정의 로그를 포함하여 모든 로그를 중앙에서 수집하는 데 사용됩니다. 로그 파일은 Amazon S3 버킷에 저장됩니다. 관리자와 감사자는 이러한 로그 파일을 통해 발생한 작업 및 이벤트를 검토할 수 있습니다.

가장 좋은 방법은 AWS 설정의 모든 부분에서 모니터링 데이터를 로그로 수집하여 다중 지점 장애가 발생할 경우 이를 더 쉽게 디버깅할 수 있도록 하는 것입니다. AWS landing Zone의 리소스 및 활동을 모니터링하기 위한 여러 도구를 제공합니다.

예를 들어, 제어 상태는 지속적으로 모니터링됩니다. AWS Control Tower 콘솔에서 상태를 한 눈에 보거나 AWS Control Tower API를 사용하여 프로그래밍 방식으로 확인할 수 있습니다. Account Factory에서 프로비저닝한 계정의 상태 및 상태도 지속적으로 모니터링됩니다.

활동 페이지에서 기록된 작업을 볼 수 있습니다.

AWS Control Tower 콘솔의 활동 페이지는 AWS Control Tower 관리 계정 작업에 대한 개요를 제공합니다. AWS Control Tower 활동 페이지로 이동하려면 왼쪽 탐색 메뉴에서 활동을 선택하십시오.

활동 페이지에 표시된 활동은 AWS Control Tower의 AWS CloudTrail 이벤트 로그에 보고된 활동과 동일하지만 표 형식으로 표시됩니다. 특정 활동에 대한 자세한 내용은 테이블에서 활동을 선택한 다음 세부 정보 보기를 선택합니다.

로그 아카이브 파일에서 회원 계정 활동 및 이벤트를 볼 수 있습니다.

다음 섹션에서는 AWS Control Tower에서의 모니터링 및 로깅에 대해 보다 자세히 설명합니다.

주제

AWS Control Tower 로그인 정보

AWS Control Tower는 및 와의 통합을 통해 자동으로 작업 AWS CloudTrail 및 AWS Config이벤트를 기록하고 이를 기록합니다. CloudWatch AWS Control Tower 관리 계정 및 조직의 회원 계정에서 발생한 작업을 포함하여 모든 작업이 기록됩니다. 관리 계정 작업 및 이벤트는 콘솔의 활동 페이지에서 확인할 수 있습니다. 로그 아카이브 파일에서 멤버 계정 작업 및 이벤트를 볼 수 있습니다.

조직 수준 트레일

AWS Control Tower는 랜딩 존을 설정할 때 새로운 CloudTrail 트레일을 설정합니다. 조직 수준의 추적이므로 관리 계정과 조직 내 모든 구성원 계정에 대한 모든 이벤트를 기록합니다. 이 기능은 신뢰할 수 있는 액세스를 기반으로 관리 계정에 모든 구성원 계정에 대한 트레일을 생성할 수 있는 권한을 부여합니다.

AWS Control Tower 및 CloudTrail 조직 추적에 대한 자세한 내용은 조직 추적 생성을 참조하십시오.

> **Note**
>
> 랜딩 존 버전 3.0 이전의 AWS Control Tower 릴리스에서는 AWS Control Tower가 각 계정에 회원 계정 트레일을 생성했습니다. 릴리스 3.0으로 업데이트하면 트레일이 조직 CloudTrail 트레일이 됩니다. 트레일 간 이동에 대한 모범 사례는 CloudTrail 사용 설명서의 트레일 변경 모범 사례를 참조하십시오.

계정을 AWS Control Tower에 등록하면 해당 계정은 AWS Control Tower 조직의 AWS CloudTrail 트레일에 따라 관리됩니다. 해당 계정에 CloudTrail 트레일을 기존에 배포한 경우, AWS Control Tower에 등록하기 전에 해당 계정의 기존 트레일을 삭제하지 않는 한 요금이 중복될 수 있습니다.

> **Note**
>
> 랜딩 존 버전 3.0으로 업데이트하면 AWS Control Tower가 사용자를 대신하여 등록된 계정의 계정 수준 트레일 (AWS Control Tower가 생성한) 을 삭제합니다. 기존 계정 수준 로그 파일은 Amazon S3 버킷에 보존됩니다.

감사 계정의 Amazon S3 버킷 정책

AWS Control Tower에서는 요청이 조직 또는 조직 단위 (OU) 에서 시작된 경우에만 AWS 서비스가 리소스에 액세스할 수 있습니다. 모든 쓰기 권한에 대한 `aws:SourceOrgID` 조건이 충족되어야 합니다.

Amazon S3 버킷 정책의 `aws:SourceOrgID` 조건 요소에서 조건 키를 사용하고 조직 ID에 값을 설정할 수 있습니다. 이 조건은 조직 내 계정을 대신하여 S3 버킷에 CloudTrail 로그만 쓸 수 있도록 하고, 조직 외부의 CloudTrail 로그가 AWS Control Tower S3 버킷에 기록하는 것을 방지합니다.

이 정책은 기존 워크로드의 기능에는 영향을 미치지 않습니다. 정책은 다음 예제에 나와 있습니다.

```
S3AuditBucketPolicy:
    Type: AWS::S3::BucketPolicy
    Properties:
      Bucket: !Ref S3AuditBucket
      PolicyDocument:
        Version: 2012-10-17
        Statement:
          - Sid: AllowSSLRequestsOnly
            Effect: Deny
            Principal: '*'
            Action: s3:*
            Resource:
             - !Sub "arn:${AWS::Partition}:s3:::${S3AuditBucket}"
             - !Sub "arn:${AWS::Partition}:s3:::${S3AuditBucket}/*"
            Condition:
              Bool:
                aws:SecureTransport: false
          - Sid: AWSBucketPermissionsCheck
            Effect: Allow
            Principal:
              Service:
                - cloudtrail.amazonaws.com
                - config.amazonaws.com
            Action: s3:GetBucketAcl
            Resource:
              - !Sub "arn:${AWS::Partition}:s3:::${S3AuditBucket}"
          - Sid: AWSConfigBucketExistenceCheck
            Effect: Allow
            Principal:
              Service:
                - cloudtrail.amazonaws.com
                - config.amazonaws.com
            Action: s3:ListBucket
            Resource:
              - !Sub "arn:${AWS::Partition}:s3:::${S3AuditBucket}"
          - Sid: AWSBucketDeliveryForConfig
            Effect: Allow
```

```
            Principal:
              Service:
                - config.amazonaws.com
            Action: s3:PutObject
            Resource:
              - Fn::Join:
                  - ""
                  -
                    - !Sub "arn:${AWS::Partition}:s3:::"
                    - !Ref "S3AuditBucket"
                    - !Sub "/${AWSLogsS3KeyPrefix}/AWSLogs/*/*"
            Condition:
              StringEquals:
                aws:SourceOrgID: !Ref OrganizationId
          - Sid: AWSBucketDeliveryForOrganizationTrail
            Effect: Allow
            Principal:
              Service:
                - cloudtrail.amazonaws.com
            Action: s3:PutObject
            Resource: !If [IsAccountLevelBucketPermissionRequiredForCloudTrail,
                [!Sub "arn:${AWS::Partition}:s3:::${S3AuditBucket}/
${AWSLogsS3KeyPrefix}/AWSLogs/${Namespace}/*", !Sub "arn:${AWS::Partition}:s3:::
${S3AuditBucket}/${AWSLogsS3KeyPrefix}/AWSLogs/${OrganizationId}/*"],
                !Sub "arn:${AWS::Partition}:s3:::${S3AuditBucket}/
${AWSLogsS3KeyPrefix}/AWSLogs/*/*"]
            Condition:
              StringEquals:
            aws:SourceOrgID: !Ref OrganizationId
```

이 조건 키에 대한 자세한 내용은 IAM 설명서 및 “리소스에 액세스하는 AWS 서비스를 위한 확장 가능한 제어 사용”이라는 제목의 IAM 블로그 게시물을 참조하십시오.

모니터링을 위한 통합 도구

모니터링은 AWS Control Tower 및 기타 AWS 솔루션의 안정성, 가용성 및 성능을 유지하는 데 있어 중요한 부분입니다. AWS 는 AWS Control Tower를 관찰하고, 문제 발생 시 보고하고, 적절한 경우 자동 조치를 취할 수 있는 다음과 같은 모니터링 도구를 제공합니다.

- Amazon은 실행 중인 AWS 리소스와 애플리케이션을 AWS 실시간으로 CloudWatch 모니터링합니다. 지표를 수집 및 추적하고, 맞춤 대시보드를 생성할 수 있으며, 지정된 지표가 지정한 임계값에 도달하면 사용자에게 알리거나 조치를 취하도록 경보를 설정할 수 있습니다. 예를 들어 Amazon EC2

인스턴스의 CPU 사용량 또는 기타 지표를 CloudWatch 추적하고 필요할 때 새 인스턴스를 자동으로 시작할 수 있습니다. 자세한 내용은 Amazon CloudWatch 사용 설명서를 참조하십시오.

- Amazon CloudWatch Events는 AWS 리소스 변경을 설명하는 시스템 이벤트의 스트림을 거의 실시간으로 제공합니다. CloudWatch 이벤트를 사용하면 특정 이벤트를 감시하고 이러한 이벤트가 발생할 때 다른 AWS 서비스에서 자동화된 작업을 트리거하는 규칙을 작성할 수 있으므로 자동화된 이벤트 기반 컴퓨팅이 가능합니다. 자세한 내용은 Amazon CloudWatch Events 사용 설명서를 참조하십시오.
- Amazon CloudWatch Logs를 사용하면 Amazon EC2 인스턴스 및 기타 소스에서 로그 파일을 모니터링 CloudTrail, 저장 및 액세스할 수 있습니다. CloudWatch 로그는 로그 파일의 정보를 모니터링하고 특정 임계값이 충족되면 알려줄 수 있습니다. 또한 매우 내구력 있는 스토리지에 로그 데이터를 저장할 수 있습니다. 자세한 내용은 Amazon CloudWatch Logs 사용 설명서를 참조하십시오.
- AWS CloudTrail계정에서 또는 AWS 계정을 대신하여 이루어진 API 호출 및 관련 이벤트를 캡처하고 지정한 Amazon S3 버킷으로 로그 파일을 전송합니다. 어떤 사용자와 계정이 전화를 걸었는지 AWS, 어떤 소스 IP 주소에서 호출이 이루어졌는지, 언제 호출이 발생했는지 식별할 수 있습니다.

팁: CloudWatch 로그 및 CloudWatch 로그 인사이트를 통해 계정의 CloudTrail 활동을 보고 쿼리할 수 있습니다. 이 활동에는 AWS Control Tower 수명 주기 이벤트가 포함됩니다. CloudWatch로그 기능을 사용하면 일반적으로 사용할 수 있는 것보다 더 세밀하고 정확한 쿼리를 수행할 수 있습니다. CloudTrail

자세한 내용은 를 사용하여 AWS Control Tower 작업 로깅 AWS CloudTrail을(를) 참조하세요.

를 사용하여 AWS Control Tower 작업 로깅 AWS CloudTrail

AWS Control Tower는 AWS Control Tower의 사용자, 역할 또는 AWS 서비스가 취한 조치를 기록해 주는 서비스와 통합되어 있습니다. AWS CloudTrailCloudTrail AWS Control Tower의 작업을 이벤트로 캡처합니다. 트레일을 생성하면 AWS Control Tower의 CloudTrail 이벤트를 포함하여 Amazon S3 버킷으로 이벤트를 지속적으로 전송할 수 있습니다.

트레일을 구성하지 않아도 CloudTrail 콘솔의 이벤트 기록에서 가장 최근 이벤트를 계속 볼 수 있습니다. 에서 수집한 CloudTrail 정보를 사용하여 AWS Control Tower에 이루어진 요청, 요청이 이루어진 IP 주소, 요청한 사람, 요청 시기 및 추가 세부 정보를 확인할 수 있습니다.

구성 및 활성화 방법을 CloudTrail 포함하여 자세한 내용은 사용 AWS CloudTrail 설명서를 참조하십시오.

AWS Control 타워 정보 CloudTrail

CloudTrail 계정을 생성하면 AWS 계정에서 활성화됩니다. 지원되는 이벤트 활동이 AWS Control Tower에서 발생하면 해당 활동이 CloudTrail 이벤트 기록의 다른 AWS 서비스 이벤트와 함께 이벤트에 기록됩니다. AWS 계정에서 최근 이벤트를 보고, 검색하고, 다운로드할 수 있습니다. 자세한 내용은 이벤트 기록으로 CloudTrail 이벤트 보기를 참조하십시오.

> **Note**
>
> 랜딩 존 버전 3.0 이전의 AWS Control Tower 릴리스에서는 AWS Control Tower가 회원 계정 트레일을 생성했습니다. 릴리스 3.0으로 업데이트하면 CloudTrail 트레일이 조직 트레일이 되도록 업데이트됩니다. 트레일 간 이동에 대한 모범 사례는 CloudTrail 사용 설명서의 조직 트레일 만들기를 참조하십시오.

권장 사항: 트레일 만들기

AWS Control Tower의 이벤트를 포함하여 AWS 계정에서 진행 중인 이벤트 기록을 보려면 트레일을 생성하십시오. 트레일을 사용하면 CloudTrail Amazon S3 버킷으로 로그 파일을 전송할 수 있습니다. 콘솔에서 추적을 생성하면 기본적으로 모든 AWS 지역에 추적이 적용됩니다. 트레일은 AWS 파티션에 있는 모든 지역의 이벤트를 기록하고 지정한 Amazon S3 버킷으로 로그 파일을 전송합니다. 또한 CloudTrail 로그에서 수집된 이벤트 데이터를 추가로 분석하고 이에 따라 조치를 취하도록 다른 AWS 서비스를 구성할 수 있습니다. 자세한 내용은 다음 자료를 참조하십시오.

- 추적 생성 개요
- 트레일 생성을 준비하세요.
- CloudTrail 비용 관리
- CloudTrail 지원되는 서비스 및 통합
- 에 대한 Amazon SNS 알림 구성 CloudTrail
- 여러 지역에서 CloudTrail 로그 파일 수신 및 여러 계정으로부터 CloudTrail 로그 파일 수신

AWS Control Tower는 다음과 같은 작업을 CloudTrail 로그 파일에 이벤트로 기록합니다.

퍼블릭 API

- `DisableControl`
- `EnableControl`

- GetControlOperation
- ListEnabledControls

기타 API

- SetupLandingZone
- UpdateAccountFactoryConfig
- ManageOrganizationalUnit
- CreateManagedAccount
- EnableGuardrail
- GetLandingZoneStatus
- GetHomeRegion
- ListManagedAccounts
- DescribeManagedAccount
- DescribeAccountFactoryConfig
- DescribeGuardrailForTarget
- DescribeManagedOrganizationalUnit
- ListEnabledGuardrails
- ListGuardrailViolations
- ListGuardrails
- ListGuardrailsForTarget
- ListManagedAccountsForGuardrail
- ListManagedAccountsForParent
- ListManagedOrganizationalUnits
- ListManagedOrganizationalUnitsForGuardrail
- GetGuardrailComplianceStatus
- DescribeGuardrail
- ListDirectoryGroups
- DescribeSingleSignOn

- `DescribeCoreService`
- `GetAvailableUpdates`

모든 이벤트 및 로그 항목에는 요청을 생성한 사용자에 대한 정보가 들어 있습니다. 보안 인증 정보를 이용하면 다음을 쉽게 판단할 수 있습니다.

- 요청이 루트 또는 AWS Identity and Access Management (IAM) 사용자 자격 증명으로 이루어졌는지 여부
- 역할 또는 페더레이션 사용자에 대한 임시 보안 보안 인증을 사용하여 요청이 생성되었는지 여부.
- 다른 AWS 서비스에서 요청했는지 여부.
- 요청이 액세스 거부로 거부되었는지 또는 성공적으로 처리되었는지 여부.

자세한 내용은 CloudTrail userIdentity 요소를 참조하세요.

예: AWS Control Tower 로그 파일 항목

트레일은 지정한 Amazon S3 버킷에 이벤트를 로그 파일로 전송할 수 있는 구성입니다. CloudTrail 로그 파일에는 하나 이상의 로그 항목이 포함되어 있습니다. 이벤트는 모든 소스의 단일 요청을 나타내며 요청된 작업, 작업 날짜 및 시간, 요청 매개 변수 등에 대한 정보를 포함합니다. CloudTrail 이벤트는 로그 파일에 특정 순서로 표시되지 않습니다.

다음 예제는 작업을 시작한 사용자의 ID 기록을 포함하여 `SetupLandingZone` AWS Control Tower 이벤트에 대한 일반적인 로그 파일 항목의 구조를 보여주는 로그 항목을 보여줍니다. CloudTrail

```
{
  "eventVersion": "1.05",
  "userIdentity": {
    "type": "AssumedRole",
    "principalId": "AIDACKCEVSQ6C2EXAMPLE:backend-test-assume-role-session",
    "arn": "arn:aws:sts::76543EXAMPLE;:assumed-role/AWSControlTowerTestAdmin/backend-
test-assume-role-session",
    "accountId": "76543EXAMPLE",
    "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
    "sessionContext": {
      "attributes": {
        "mfaAuthenticated": "false",
        "creationDate": "2018-11-20T19:36:11Z"
      },
```

```
      "sessionIssuer": {
        "type": "Role",
        "principalId": "AIDACKCEVSQ6C2EXAMPLE",
        "arn": "arn:aws:iam::AKIAIOSFODNN7EXAMPLE:role/AWSControlTowerTestAdmin",
        "accountId": "AIDACKCEVSQ6C2EXAMPLE",
        "userName": "AWSControlTowerTestAdmin"
      }
    }
  },
  "eventTime": "2018-11-20T19:36:15Z",
  "eventSource": "controltower.amazonaws.com",
  "eventName": "SetupLandingZone",
  "awsRegion": "us-east-1",
  "sourceIPAddress": "AWS Internal",
  "userAgent": "Coral/Netty4",
  "errorCode": "InvalidParametersException",
  "errorMessage": "Home region EU_CENTRAL_1 is unsupported",
  "requestParameters": {
    "homeRegion": "EU_CENTRAL_1",
    "logAccountEmail": "HIDDEN_DUE_TO_SECURITY_REASONS",
    "sharedServiceAccountEmail": "HIDDEN_DUE_TO_SECURITY_REASONS",
    "securityAccountEmail": "HIDDEN_DUE_TO_SECURITY_REASONS",
    "securityNotificationEmail": "HIDDEN_DUE_TO_SECURITY_REASONS"
  },
  "responseElements": null,
  "requestID": "96f47b68-ed5f-4268-931c-807cd1f89a96",
  "eventID": "4ef5cf08-39e5-4fdf-9ea2-b07ced506851",
  "eventType": "AwsApiCall",
  "recipientAccountId": "76543EXAMPLE"
}
```


다음을 사용하여 리소스 변경을 모니터링합니다. AWS Config

AWS Control Tower는 등록된 모든 AWS Config 계정에서 이를 활성화하므로 탐지 제어를 통해 규정 준수를 모니터링하고, 리소스 변경을 기록하고, 리소스 변경 로그를 로그 아카이브 계정에 전달할 수 있습니다.

Landing Zone 버전이 3.0 이전인 경우: 등록된 계정의 경우 계정이 운영되는 모든 지역의 리소스에 대한 모든 변경 사항을 AWS Config 기록합니다. 각 변경 사항은 리소스 식별자, 지역, 각 변경 내용이 기록된 날짜, 변경 내용이 알려진 리소스와 관련이 있는지 또는 새로 발견된 리소스와 관련이 있는지 여부와 같은 정보가 포함된 구성 항목 (CI) 으로 모델링됩니다.

랜딩 존 버전이 3.0 이상인 경우: AWS Control Tower는 IAM 사용자, 그룹, 역할 및 고객 관리형 정책과 같은 글로벌 리소스에 대한 기록을 홈 지역으로만 제한합니다. 글로벌 리소스 변경 사본이 모든 지역에 저장되는 것은 아닙니다. 리소스 기록의 이러한 제한은 AWS Config 모범 사례를 준수합니다. 글로벌 리소스의 전체 목록은 AWS Config 설명서에서 확인할 수 있습니다.

- 자세한 AWS Config내용은 AWS Config 작동 방식을 참조하십시오.
- 지원할 AWS Config 수 있는 리소스 목록은 지원되는 리소스 유형을 참조하십시오.
- AWS Control Tower 환경에서 리소스 추적을 사용자 지정하는 방법에 대해 알아보려면 AWS Control Tower의 AWS Config 리소스 추적 사용자 지정이라는 제목의 블로그 게시물을 참조하십시오.

AWS Control Tower는 등록된 모든 계정에 AWS Config 전송 채널을 설정합니다. 이 전송 채널을 통해 로그 아카이브 계정에 기록된 모든 변경 사항을 기록하여 AWS Config Amazon Simple Storage Service 버킷의 폴더에 저장합니다.

AWS Control Tower의 AWS Config 비용 관리

이 섹션에서는 AWS Control Tower 계정의 리소스 변경 사항을 AWS Config 기록하고 요금을 청구하는 방법을 설명합니다. 이 정보는 AWS Control Tower를 사용할 때 이와 관련된 AWS Config비용을 관리하는 방법을 이해하는 데 도움이 될 수 있습니다. AWS Control Tower는 추가 비용을 추가하지 않습니다.

> **Note**
>
> 랜딩 존 버전이 3.0 이상인 경우: AWS Control Tower는 IAM 사용자, 그룹, 역할 및 고객 관리형 정책과 같은 글로벌 리소스에 대한 AWS Config 기록을 홈 지역으로만 제한합니다. 따라서 이 섹션의 일부 정보는 착륙 지대에 적용되지 않을 수 있습니다.

AWS Config 계정이 운영되는 각 지역의 각 리소스에 대한 각 변경 사항을 구성 항목 (CI) 으로 기록하도록 설계되었습니다. AWS Config 생성된 각 구성 항목에 대해 요금이 청구됩니다.

AWS Config 작동 방식

AWS Config 각 지역의 리소스를 개별적으로 기록합니다. IAM 역할과 같은 일부 글로벌 리소스는 지역당 한 번씩 기록됩니다. 예를 들어 5개 지역에서 운영되는 등록 계정에서 새 IAM 역할을 AWS Config 생성하는 경우 각 지역에 하나씩 총 5개의 CI가 생성됩니다. Route 53 호스팅 영역과 같은 기타 글로벌 리소스는 모든 지역에서 한 번만 기록됩니다. 예를 들어, 등록된 계정에서 새 Route 53 호스팅 영역을

AWS Config 생성하면 해당 계정에 대해 선택한 지역 수에 관계없이 하나의 CI가 생성됩니다. 이러한 유형의 리소스를 구분하는 데 도움이 되는 목록은 을 참조하십시오동일한 리소스가 여러 번 기록됩니다..

> **Note**
>
> AWS Control Tower와 협력하는 경우 AWS Config, AWS Control Tower의 지배를 받거나 관리되지 않는 지역이 있을 수 있으며, 계정이 해당 지역에서 운영되는 경우 변경 사항을 AWS Config 계속 기록할 수 있습니다.

AWS Config 리소스에서 두 가지 유형의 관계를 탐지합니다.

AWS Config 리소스 간의 직접 관계와 간접 관계를 구분합니다. 다른 리소스의 Describe API 호출에서 리소스가 반환되는 경우 해당 리소스는 직접적인 관계로 기록됩니다. 다른 리소스와의 직접적인 관계에서 리소스를 변경하는 경우 는 두 리소스에 대한 CI를 만들지 AWS Config 않습니다.

예를 들어 Amazon EC2 인스턴스를 생성하고 API에서 네트워크 인터페이스를 생성하도록 요구하는 경우 Amazon EC2 인스턴스는 네트워크 인터페이스와 직접적인 관계가 있는 AWS Config 것으로 간주합니다. 따라서 CI는 하나만 AWS Config 생성됩니다.

AWS Config 간접 관계인 리소스 관계에 대해 별도의 변경 사항을 기록합니다. 예를 들어, 보안 그룹을 AWS Config 생성하고 보안 그룹에 속하는 관련 Amazon EC2 인스턴스를 추가하면 두 개의 CI를 생성합니다.

직접 및 간접 관계에 대한 자세한 내용은 리소스와 관련된 직접 및 간접 관계란 무엇입니까? 를 참조하십시오.

AWS Config 설명서에서 리소스 관계 목록을 찾을 수 있습니다.

등록된 계정의 AWS Config 레코더 데이터 보기

AWS Config 와 CloudWatch 통합되어 대시보드에서 AWS Config CI를 볼 수 있습니다. 자세한 내용은 Amazon CloudWatch 지표AWS Config 지원이라는 제목의 블로그 게시물을 참조하십시오.

프로그래밍 방식으로 AWS Config 데이터를 보려면 AWS CLI를 사용하거나 다른 도구를 사용할 수 있습니다. AWS

특정 리소스의 AWS Config 레코더 데이터를 쿼리하십시오.

AWS CLI를 사용하여 리소스의 최신 변경 목록을 검색할 수 있습니다.

리소스 기록 명령:

- `aws configservice get-resource-config-history --resource-type RESOURCE-TYPE --resource-id RESOURCE-ID --region REGION`

자세한 내용은 의 API 설명서를 참조하십시오 `get-config-history`.

Amazon으로 AWS Config 데이터를 시각화하세요 QuickSight

조직 AWS Config 전체에서 기록한 리소스를 시각화하고 쿼리할 수 있습니다. 자세한 내용은 Amazon Athena와 Amazon을 사용한 AWS Config 데이터 시각화를 참조하십시오. QuickSight

AWS Control AWS Config Tower에서의 문제 해결

이 섹션에서는 AWS Control AWS Config Tower와 함께 사용할 때 발생할 수 있는 몇 가지 문제에 대한 정보를 제공합니다.

높은 AWS Config 비용

워크플로에 리소스를 자주 생성, 업데이트 또는 삭제하는 프로세스가 포함되어 있거나 리소스를 많이 처리하는 경우 해당 워크플로우에서 많은 수의 CI가 생성될 수 있습니다. 비프로덕션 계정에서 이러한 프로세스를 실행하는 경우 계정 등록을 취소해 보세요. 해당 계정의 AWS Config 레코더를 수동으로 비활성화해야 할 수도 있습니다.

> **Note**
>
> 계정을 등록 취소하면 AWS Control Tower는 해당 계정의 리소스에 대해 탐지 제어를 적용하거나 AWS Config 활동 등의 계정 이벤트를 기록할 수 없습니다.

자세한 내용은 등록된 계정 관리 취소를 참조하십시오. 레코더를 비활성화하는 방법을 알아보려면 구성 AWS Config 레코더 관리를 참조하십시오.

동일한 리소스가 여러 번 기록됩니다.

리소스가 글로벌 리소스인지 확인하세요. 버전 3.0 이전의 AWS Control Tower 랜딩 존의 AWS Config 경우, 운영 중인 각 리전에 대해 특정 글로벌 리소스를 한 번 기록할 AWS Config 수 있습니다. 예를 들어, 8개 지역에서 활성화된 경우 AWS Config 각 역할은 8번 기록됩니다.

다음 리소스는 운영 중인 각 지역에 대해 한 번씩 AWS Config 기록됩니다.

- `AWS::IAM::Group`
- `AWS::IAM::Policy`
- `AWS::IAM::Role`
- `AWS::IAM::User`

기타 글로벌 리소스는 한 번만 기록됩니다. 다음은 한 번 기록되는 리소스의 몇 가지 예입니다.

- `AWS::Route53::HostedZone`
- `AWS::Route53::HealthCheck`
- `AWS::ECR::PublicRepository`
- `AWS::GlobalAccelerator::Listener`
- `AWS::GlobalAccelerator::EndpointGroup`
- `AWS::GlobalAccelerator::Accelerator`

AWS Config 리소스를 기록하지 않았습니다.

특정 리소스는 다른 리소스와 종속성 관계가 있습니다. 이러한 관계는 직접적이거나 간접적일 수 있습니다. FAQ에서 더 이상 사용되지 않는 간접 관계 목록을 찾을 수 있습니다. AWS Config

AWS Control Tower의 라이프사이클 이벤트

AWS Control Tower에서 기록하는 일부 이벤트는 수명 주기 이벤트입니다. 수명 주기 이벤트의 목적은 리소스 상태를 변경하는 특정 AWS Control Tower 작업의 완료를 표시하는 것입니다. 수명 주기 이벤트는 조직 단위 (OU), 계정, 제어 등 AWS Control Tower가 생성하거나 관리하는 리소스에 적용됩니다.

AWS Control Tower 수명 주기 이벤트의 특징

- 각 수명 주기 이벤트에 대해 이벤트 로그는 원래 Control Tower 작업이 성공적으로 완료되었는지 또는 실패했는지 여부를 표시합니다.
- AWS CloudTrail 각 수명 주기 이벤트를 비 API AWS 서비스 이벤트로 자동 기록합니다. 자세한 내용은 AWS CloudTrail 사용 설명서를 참조하십시오.
- 각 라이프사이클 이벤트는 Amazon EventBridge 및 Amazon CloudWatch 이벤트 서비스에도 전달됩니다.

AWS Control Tower의 라이프사이클 이벤트는 다음과 같은 두 가지 주요 이점을 제공합니다.

- 수명 주기 이벤트는 AWS Control Tower 작업의 완료를 등록하므로 수명 주기 CloudWatch 이벤트의 상태에 따라 자동화 워크플로의 다음 단계를 트리거할 수 있는 Amazon EventBridge 규칙 또는 Amazon Events 규칙을 생성할 수 있습니다.
- 로그는 관리자 및 감사자가 조직의 특정 활동 유형을 검토하는 데 도움이 되는 추가 세부 정보를 제공합니다.

수명 주기 이벤트 작동 방식

AWS Control Tower는 여러 서비스를 사용하여 조치를 구현합니다. 따라서 각 수명 주기 이벤트는 일련의 작업이 완료된 후에만 기록됩니다. 예를 들어 OU에서 컨트롤을 활성화하면 AWS Control Tower는 요청을 구현하는 일련의 하위 단계를 시작합니다. 전체 하위 단계의 최종 결과는 수명 주기 이벤트의 상태로 로그에 기록됩니다.

- 모든 기본 하위 단계가 성공적으로 완료되면 수명 주기 이벤트 상태가 성공으로 기록됩니다.
- 기본 하위 단계 중 하나라도 성공적으로 완료되지 않은 경우 수명 주기 이벤트 상태는 실패함으로 기록됩니다.

각 수명 주기 이벤트에는 AWS Control Tower 작업이 시작된 시기를 보여주는 로깅된 타임스탬프와 수명 주기 이벤트가 완료되어 성공 또는 실패를 표시하는 또 다른 타임스탬프가 포함됩니다.

Control Tower에서 수명 주기 이벤트 보기

AWS Control Tower 대시보드의 활동 페이지에서 수명 주기 이벤트를 볼 수 있습니다.

- 활동 페이지로 이동하려면 왼쪽 탐색 창에서 활동을 선택합니다.
- 특정 이벤트에 대한 세부 정보를 보려면 이벤트를 선택한 다음 오른쪽 상단의 세부 정보 보기 버튼을 선택합니다.

AWS Control Tower 수명 주기 이벤트를 워크플로에 통합하는 방법에 대한 자세한 내용은 이 블로그 게시물인 수명 주기 이벤트를 사용하여 AWS Control Tower 작업을 추적하고 자동화된 워크플로를 트리거하는 방법을 참조하십시오.

예상 동작 CreateManagedAccount 및 UpdateManagedAccount 수명 주기 이벤트

계정을 만들거나 AWS Control Tower에 계정을 등록하면 이 두 작업이 동일한 내부 API를 호출합니다. 프로세스 중에 오류가 발생하는 경우 일반적으로 계정이 생성되었지만 완전히 프로비저닝되지 않은

후에 오류가 발생합니다. 오류가 발생한 후 계정을 다시 생성하거나 프로비저닝된 제품을 업데이트하려고 하면 AWS Control Tower는 계정이 이미 존재한다고 판단합니다.

계정이 존재하므로 AWS Control Tower는 재시도 요청 종료 시 `CreateManagedAccount` 수명 `UpdateManagedAccount` 주기 이벤트 대신 수명 주기 이벤트를 기록합니다. 오류로 인해 다른 `CreateManagedAccount` 이벤트가 발생할 것으로 예상했을 수 있습니다. 하지만 `UpdateManagedAccount` 라이프사이클 이벤트는 예상되고 바람직한 동작입니다.

자동화된 방법을 사용하여 계정을 생성하거나 AWS Control Tower에 등록하려는 경우 수명 주기 이벤트뿐 아니라 수명 주기 이벤트도 UpdateManagedAccount찾도록 Lambda 함수를 프로그래밍하십시오. CreateManagedAccount

수명 주기 이벤트 이름

각 수명 주기 이벤트는 원래 AWS Control Tower 작업에 해당하도록 이름이 지정되며, 이 작업도 CloudTrail AWS에서 기록합니다. 따라서 예를 들어, AWS Control Tower 이벤트에서 시작된 수명 주기 `CreateManagedAccount` CloudTrail 이벤트는 이름이 `CreateManagedAccount` 지정됩니다.

다음 목록의 각 이름은 `JSON` 형식으로 기록된 세부 정보 예제에 대한 링크입니다. 이 예제에 표시된 추가 세부 정보는 Amazon CloudWatch 이벤트 로그에서 가져온 것입니다.

`JSON`에서는 주석을 지원하지 않지만 설명용으로 예제에 몇 가지 주석이 추가되었습니다. 주석은 앞에 “//”가 붙고 예제의 오른쪽에 표시됩니다.

이들 예제에서는 일부 계정 이름과 조직 이름이 가려져 있습니다. `accountId`는 항상 12자리 숫자 시퀀스이며, 예제에서 이 시퀀스는 “xxxxxxxxxx”로 대체됩니다. `organizationalUnitID`는 문자 및 숫자의 고유한 문자열입니다. 예제에서는 그 형태가 보존되어 있습니다.

- `CreateManagedAccount`: 로그에는 AWS Control Tower가 어카운트 팩토리를 사용하여 새 계정을 생성하고 프로비저닝하는 모든 작업을 성공적으로 완료했는지 여부가 기록됩니다.
- `UpdateManagedAccount`: 로그에는 AWS Control Tower가 이전에 계정 팩토리를 사용하여 생성한 계정과 연결된 프로비저닝된 제품을 업데이트하기 위한 모든 작업을 성공적으로 완료했는지 여부가 기록됩니다.
- `EnableGuardrail`: 로그에는 AWS Control Tower가 AWS Control Tower에서 생성한 OU에서 제어를 활성화하기 위한 모든 작업을 AWS Control Tower가 성공적으로 완료했는지 여부가 기록됩니다.
- `DisableGuardrail`: 로그에는 AWS Control Tower가 AWS Control Tower에서 생성한 OU에서 제어를 비활성화하는 모든 작업을 AWS Control Tower가 성공적으로 완료했는지 여부가 기록됩니다.

- SetupLandingZone: 로그에는 AWS Control Tower가 랜딩 존 설정을 위한 모든 작업을 성공적으로 완료했는지 여부가 기록됩니다.
- UpdateLandingZone: 로그에는 AWS Control Tower가 기존 착륙 지대를 업데이트하기 위한 모든 작업을 성공적으로 완료했는지 여부가 기록됩니다.
- RegisterOrganizationalUnit: 로그에는 AWS Control Tower가 OU에서 거버넌스 기능을 활성화하기 위한 모든 작업을 성공적으로 완료했는지 여부가 기록됩니다.
- DeregisterOrganizationalUnit: 로그에는 AWS Control Tower가 OU에서 거버넌스 기능을 비활성화하는 모든 작업을 성공적으로 완료했는지 여부가 기록됩니다.
- PrecheckOrganizationalUnit: 로그에는 AWS Control Tower가 거버넌스 확장 작업을 성공적으로 완료하는 데 방해가 되는 리소스를 감지했는지 여부가 기록됩니다.

다음 섹션에서는 각 유형의 수명 주기 이벤트에 대해 기록된 세부 정보의 예와 함께 AWS Control Tower 수명 주기 이벤트 목록을 제공합니다.

CreateManagedAccount

이 수명 주기 이벤트는 AWS Control Tower가 어카운트 팩토리를 사용하여 새 계정을 성공적으로 생성하고 프로비저닝했는지 여부를 기록합니다. 이 이벤트는 AWS Control Tower CreateManagedAccount CloudTrail 이벤트에 해당합니다. 수명 주기 이벤트 로그에는 새로 만든 계정의 accountName 및 accountId와 계정이 배치된 OU의 organizationalUnitName 및 organizationalUnitId가 포함됩니다.

```
{
    "version": "0",
    "id": "999cccaa-eaaa-0000-1111-123456789012",
    "detail-type": "AWS Service Event via CloudTrail",
    "source": "aws.controltower",
    "account": "XXXXXXXXXXXX",                                    // Management account
 ID.
    "time": "2018-08-30T21:42:18Z",                               // Format: yyyy-MM-
dd'T'hh:mm:ssZ
    "region": "us-east-1",                                        // AWS Control Tower
 home region.
    "resources": [ ],
    "detail": {
        "eventVersion": "1.05",
        "userIdentity": {
            "accountId": "XXXXXXXXXXXX",
            "invokedBy": "AWS Internal"
```

```
        },
        "eventTime": "2018-08-30T21:42:18Z",                    // Timestamp when call
 was made. Format: yyyy-MM-dd'T'hh:mm:ssZ.
        "eventSource": "controltower.amazonaws.com",
        "eventName": "CreateManagedAccount",
        "awsRegion": "us-east-1",
        "sourceIPAddress": "AWS Internal",
        "userAgent": "AWS Internal",
        "eventID": "0000000-0000-0000-1111-123456789012",
        "readOnly": false,
        "eventType": "AwsServiceEvent",
        "serviceEventDetails": {
            "createManagedAccountStatus": {
                "organizationalUnit":{
                    "organizationalUnitName":"Custom",
                    "organizationalUnitId":"ou-XXXX-l3zc8b3h"

                    },
                "account":{
                    "accountName":"LifeCycle1",
                    "accountId":"XXXXXXXXXXXX"
                    },
                "state":"SUCCEEDED",
                "message":"AWS Control Tower successfully created a managed account.",
                "requestedTimestamp":"2019-11-15T11:45:18+0000",
                "completedTimestamp":"2019-11-16T12:09:32+0000"}
        }
    }
}
```

UpdateManagedAccount

이 수명 주기 이벤트는 AWS Control Tower가 이전에 어카운트 팩토리를 사용하여 생성한 계정과 연결된 프로비저닝된 제품을 성공적으로 업데이트했는지 여부를 기록합니다. 이 이벤트는 AWS Control Tower `UpdateManagedAccount` CloudTrail 이벤트에 해당합니다. 수명 주기 이벤트 로그에는 연결된 계정의 `accountName` 및 `accountId`와 업데이트된 계정이 배치된 OU의 `organizationalUnitName` 및 `organizationalUnitId`가 포함됩니다.

```
{
    "version": "0",
    "id": "999cccaa-eaaa-0000-1111-123456789012",
    "detail-type": "AWS Service Event via CloudTrail",
```

```
    "source": "aws.controltower",
    "account": "XXXXXXXXXXXX",                                    // AWS Control Tower
 organization management account.
    "time": "2018-08-30T21:42:18Z",                               // Format: yyyy-MM-
dd'T'hh:mm:ssZ
    "region": "us-east-1",                                        // AWS Control Tower
 home region.
    "resources": [],
    "detail": {
        "eventVersion": "1.05",
        "userIdentity": {
            "accountId": "XXXXXXXXX",
            "invokedBy": "AWS Internal"
        },
        "eventTime": "2018-08-30T21:42:18Z",                      // Timestamp when call
 was made. Format: yyyy-MM-dd'T'hh:mm:ssZ.
        "eventSource": "controltower.amazonaws.com",
        "eventName": "UpdateManagedAccount",
        "awsRegion": "us-east-1",
        "sourceIPAddress": "AWS Internal",
        "userAgent": "AWS Internal",
        "eventID": "0000000-0000-0000-1111-123456789012",
        "readOnly": false,
        "eventType": "AwsServiceEvent",
        "serviceEventDetails": {
            "updateManagedAccountStatus": {
                "organizationalUnit":{
                    "organizationalUnitName":"Custom",
                    "organizationalUnitId":"ou-XXXX-l3zc8b3h"
                    },
                "account":{
                    "accountName":"LifeCycle1",
                    "accountId":"624281831893"
                    },
                "state":"SUCCEEDED",
                "message":"AWS Control Tower successfully updated a managed account.",
                "requestedTimestamp":"2019-11-15T11:45:18+0000",
                "completedTimestamp":"2019-11-16T12:09:32+0000"}
        }
    }
}
```

EnableGuardrail

이 수명 주기 이벤트는 AWS Control Tower에서 관리하는 OU에 대한 제어를 AWS Control Tower가 성공적으로 활성화했는지 여부를 기록합니다. 이 이벤트는 AWS Control Tower EnableGuardrail CloudTrail 이벤트에 해당합니다. 수명 주기 이벤트 로그에는 guardrailBehavior 컨트롤의 OU와 컨트롤이 organizationalUnitName 활성화된 organizationalUnitId OU의 OU가 포함됩니다. guardrailId

```
{
    "version": "0",
    "id": "999cccaa-eaaa-0000-1111-123456789012",
    "detail-type": "AWS Service Event via CloudTrail",
    "source": "aws.controltower",
    "account": "XXXXXXXXXXXX",
    "time": "2018-08-30T21:42:18Z",                                    // End-time of action.
 Format: yyyy-MM-dd'T'hh:mm:ssZ
    "region": "us-east-1",                                             // AWS Control Tower
 home region.
    "resources": [ ],
    "detail": {
        "eventVersion": "1.05",
        "userIdentity": {
            "accountId": "XXXXXXXXXXXX",
            "invokedBy": "AWS Internal"
        },
        "eventTime": "2018-08-30T21:42:18Z",
        "eventSource": "controltower.amazonaws.com",
        "eventName": "EnableGuardrail",
        "awsRegion": "us-east-1",
        "sourceIPAddress": "AWS Internal",
        "userAgent": "AWS Internal",
        "eventID": "0000000-0000-0000-1111-123456789012",
        "readOnly": false,
        "eventType": "AwsServiceEvent",
        "serviceEventDetails": {
            "enableGuardrailStatus": {
                "organizationalUnits": [
                    {
                      "organizationalUnitName": "Custom",
                      "organizationalUnitId": "ou-vwxy-18vy4yro"
                    }
                  ],
```

```
                  "guardrails": [
                    {
                      "guardrailId": "AWS-GR_RDS_INSTANCE_PUBLIC_ACCESS_CHECK",
                      "guardrailBehavior": "DETECTIVE"
                    }
                  ],
                  "state": "SUCCEEDED",
                  "message": "AWS Control Tower successfully enabled a guardrail on an
 organizational unit.",
                  "requestTimestamp": "2019-11-12T09:01:07+0000",
                  "completedTimestamp": "2019-11-12T09:01:54+0000"
                }
        }
    }
}
```

DisableGuardrail

이 수명 주기 이벤트는 AWS Control Tower에서 관리하는 OU의 제어를 AWS Control Tower가 성공적으로 비활성화했는지 여부를 기록합니다. 이 이벤트는 AWS Control Tower `DisableGuardrail` CloudTrail 이벤트에 해당합니다. 수명 주기 이벤트 로그에는 `guardrailBehavior` 컨트롤의 O와 컨트롤이 `organizationalUnitName` 비활성화된 `organizationalUnitId` OU의 OU가 포함됩니다. `guardrailId`

```
{
    "version": "0",
    "id": "999cccaa-eaaa-0000-1111-123456789012",
    "detail-type": "AWS Service Event via CloudTrail",
    "source": "aws.controltower",
    "account": "XXXXXXXXXXXX",
    "time": "2018-08-30T21:42:18Z",
    "region": "us-east-1",
    "resources": [ ],
    "detail": {
        "eventVersion": "1.05",
        "userIdentity": {
            "accountId": "XXXXXXXXXXXX",
            "invokedBy": "AWS Internal"
        },
        "eventTime": "2018-08-30T21:42:18Z",
        "eventSource": "controltower.amazonaws.com",
        "eventName": "DisableGuardrail",
```

```
        "awsRegion": "us-east-1",
        "sourceIPAddress": "AWS Internal",
        "userAgent": "AWS Internal",
        "eventID": "0000000-0000-0000-1111-123456789012",
        "readOnly": false,
        "eventType": "AwsServiceEvent",
        "serviceEventDetails": {
            "disableGuardrailStatus": {
                   "organizationalUnits": [
                    {
                      "organizationalUnitName": "Custom",
                      "organizationalUnitId": "ou-vwxy-18vy4yro"
                    }
                  ],
                  "guardrails": [
                    {
                      "guardrailId": "AWS-GR_RDS_INSTANCE_PUBLIC_ACCESS_CHECK",
                      "guardrailBehavior": "DETECTIVE"
                    }
                  ],
                  "state": "SUCCEEDED",
                  "message": "AWS Control Tower successfully disabled a guardrail on an
 organizational unit.",
                  "requestTimestamp": "2019-11-12T09:01:07+0000",
                  "completedTimestamp": "2019-11-12T09:01:54+0000"
                }
            }
        }
    }
```

SetupLandingZone

이 수명 주기 이벤트는 AWS Control Tower가 성공적으로 랜딩 존을 설정했는지 여부를 기록합니다. 이 이벤트는 AWS Control Tower SetupLandingZone CloudTrail 이벤트에 해당합니다. 수명 주기 이벤트 로그에는 AWS Control Tower가 관리 계정에서 생성하는 조직의 ID인 가 포함됩니다. rootOrganizationalId 로그 항목에는 AWS Control Tower가 랜딩 존을 설정할 때 생성되는 각 accountId OU에 대한 accountName 및 및 각 계정에 대한 및 도 포함됩니다. organizationalUnitName organizationalUnitId

```
{
    "version": "0",
    "id": "999cccaa-eaaa-0000-1111-123456789012",               // Request ID.
```

```
   "detail-type": "AWS Service Event via CloudTrail",
   "source": "aws.controltower",
   "account": "XXXXXXXXXXXX",                                    // Management account
ID.
   "time": "2018-08-30T21:42:18Z",                               // Event time from
CloudTrail.
   "region": "us-east-1",                                        // Management account
CloudTrail region.
   "resources": [ ],
   "detail": {
       "eventVersion": "1.05",
       "userIdentity": {
           "accountId": "XXXXXXXXXXXX",                          // Management-account
ID.
           "invokedBy": "AWS Internal"
       },
       "eventTime": "2018-08-30T21:42:18Z",                      // Timestamp when call
was made. Format: yyyy-MM-dd'T'hh:mm:ssZ.
       "eventSource": "controltower.amazonaws.com",
       "eventName": "SetupLandingZone",
       "awsRegion": "us-east-1",                                 // AWS Control Tower
home region.
       "sourceIPAddress": "AWS Internal",
       "userAgent": "AWS Internal",
       "eventID": "CloudTrail_event_ID",                         // This value is
generated by CloudTrail.
       "readOnly": false,
       "eventType": "AwsServiceEvent",
       "serviceEventDetails": {
           "setupLandingZoneStatus": {
               "state": "SUCCEEDED",                              // Status of entire
lifecycle operation.
               "message": "AWS Control Tower successfully set up a new landing zone.",

               "rootOrganizationalId" : "r-1234",
               "organizationalUnits" : [                          // Use a list.
                 {
                   "organizationalUnitName": "Security",             // Security OU
name.
                   "organizationalUnitId": "ou-adpf-302pk332"    // Security OU ID.
                 },
                 {
                   "organizationalUnitName": "Custom",           // Custom OU name.
                   "organizationalUnitId": "ou-adpf-302pk332"    // Custom OU ID.
```

```
                },
              ],
              "accounts": [                                          // All created
 accounts are here. Use a list of "account" objects.

                {
                  "accountName": "Audit",
                  "accountId": "XXXXXXXXXXXX"
                },
                {
                  "accountName": "Log archive",
                  "accountId": "XXXXXXXXXXXX"
                }
            ],
            "requestedTimestamp": "2018-08-30T21:42:18Z",
            "completedTimestamp": "2018-08-30T21:42:18Z"
          }
        }
    }
}
```

UpdateLandingZone

이 수명 주기 이벤트는 AWS Control Tower가 기존 랜딩 존을 성공적으로 업데이트했는지 여부를 기록합니다. 이 이벤트는 AWS Control Tower UpdateLandingZone CloudTrail 이벤트에 해당합니다. 수명 주기 이벤트 로그에는 AWS Control Tower에서 관리하는 (업데이트된) 조직의 ID인 가 포함됩니다. rootOrganizationalId 로그 항목에는 각 organizationalUnitId OU에 대한 organizationalUnitName 및, 이전에 AWS Control Tower가 랜딩 존을 처음 설정할 때 생성된 각 계정에 accountId 대한 accountName 및 도 포함됩니다.

```
{
    "version": "0",
    "id": "999cccaa-eaaa-0000-1111-123456789012",                 // Request ID.
    "detail-type": "AWS Service Event via CloudTrail",
    "source": "aws.controltower",
    "account": "XXXXXXXXXXXX",                                   // Management account
 ID.
    "time": "2018-08-30T21:42:18Z",                              // Event time from
 CloudTrail.
    "region": "us-east-1",                                       // Management account
 CloudTrail region.
    "resources": [ ],
```

```
   "detail": {
       "eventVersion": "1.05",
       "userIdentity": {
           "accountId": "XXXXXXXXXXXX",                          // Management account
ID.
           "invokedBy": "AWS Internal"
       },
       "eventTime": "2018-08-30T21:42:18Z",                      // Timestamp when call
was made. Format: yyyy-MM-dd'T'hh:mm:ssZ.
       "eventSource": "controltower.amazonaws.com",
       "eventName": "UpdateLandingZone",
       "awsRegion": "us-east-1",                                 // AWS Control Tower
home region.
       "sourceIPAddress": "AWS Internal",
       "userAgent": "AWS Internal",
       "eventID": "CloudTrail_event_ID",                         // This value is
generated by CloudTrail.

       "readOnly": false,
       "eventType": "AwsServiceEvent",
       "serviceEventDetails": {
           "updateLandingZoneStatus": {
               "state": "SUCCEEDED",                             // Status of entire
operation.
               "message": "AWS Control Tower successfully updated a landing zone.",


               "rootOrganizationalId" : "r-1234",
               "organizationalUnits" : [                          // Use a list.
                 {
                   "organizationalUnitName": "Security",            // Security OU
name.
                   "organizationalUnitId": "ou-adpf-302pk332"    // Security OU ID.
                 },
                 {
                   "organizationalUnitName": "Custom",             // Custom OU name.
                   "organizationalUnitId": "ou-adpf-302pk332"     // Custom OU ID.
                 },
               ],
              "accounts": [                                       // All created
accounts are here. Use a list of "account" objects.

                 {
                   "accountName": "Audit",
```

```
                    "accountId": "XXXXXXXXXXXX"
                  },
                  {
                    "accountName": "Log archive",
                    "accountId": "XXXXXXXXXX"
                  }
              ],
              "requestedTimestamp": "2018-08-30T21:42:18Z",
              "completedTimestamp": "2018-08-30T21:42:18Z"
            }
        }
    }
}
```

RegisterOrganizationalUnit

이 수명 주기 이벤트는 AWS Control Tower가 OU에서 거버넌스 기능을 성공적으로 활성화했는지 여부를 기록합니다. 이 이벤트는 AWS Control Tower `RegisterOrganizationalUnit` CloudTrail 이벤트에 해당합니다. 수명 주기 이벤트 로그에는 AWS Control Tower가 거버넌스 하에 설정한 `organizationalUnitId` OU의 OU가 포함됩니다. `organizationalUnitName`

```
{
    "version": "0",
    "id": "999cccaa-eaaa-0000-1111-123456789012",
    "detail-type": "AWS Service Event via CloudTrail",
    "source": "aws.controltower",
    "account": "123456789012",
    "time": "2018-08-30T21:42:18Z",
    "region": "us-east-1",
    "resources": [ ],
    "detail": {
        "eventVersion": "1.05",
        "userIdentity": {
            "accountId": "XXXXXXXXXXXX",
            "invokedBy": "AWS Internal"
        },
        "eventTime": "2018-08-30T21:42:18Z",
        "eventSource": "controltower.amazonaws.com",
        "eventName": "RegisterOrganizationalUnit",
        "awsRegion": "us-east-1",
        "sourceIPAddress": "AWS Internal",
        "userAgent": "AWS Internal",
        "eventID": "0000000-0000-0000-1111-123456789012",
```

```
        "readOnly": false,
        "eventType": "AwsServiceEvent",
        "serviceEventDetails": {
            "registerOrganizationalUnitStatus": {
                "state": "SUCCEEDED",

                "message": "AWS Control Tower successfully registered an organizational
 unit.",

                "organizationalUnit" :
                  {
                    "organizationalUnitName": "Test",
                    "organizationalUnitId": "ou-adpf-302pk332"
                  }
                "requestedTimestamp": "2018-08-30T21:42:18Z",
                "completedTimestamp": "2018-08-30T21:42:18Z"
            }
        }
    }
}
```

DeregisterOrganizationalUnit

이 수명 주기 이벤트는 AWS Control Tower가 OU의 거버넌스 기능을 성공적으로 비활성화했는지 여부를 기록합니다. 이 이벤트는 AWS Control Tower `DeregisterOrganizationalUnit` CloudTrail 이벤트에 해당합니다. 수명 주기 이벤트 로그는 AWS Control Tower가 거버넌스 기능을 비활성화한 `organizationalUnitId` OU의 종료를 포함합니다. `organizationalUnitName`

```
{
    "version": "0",
    "id": "999cccaa-eaaa-0000-1111-123456789012",
    "detail-type": "AWS Service Event via CloudTrail",
    "source": "aws.controltower",
    "account": "XXXXXXXXXXXX",
    "time": "2018-08-30T21:42:18Z",
    "region": "us-east-1",
    "resources": [ ],
    "detail": {
        "eventVersion": "1.05",
        "userIdentity": {
            "accountId": "XXXXXXXXXXXX",
            "invokedBy": "AWS Internal"
        },
```

```
        "eventTime": "2018-08-30T21:42:18Z",
        "eventSource": "controltower.amazonaws.com",
        "eventName": "DeregisterOrganizationalUnit",
        "awsRegion": "us-east-1",
        "sourceIPAddress": "AWS Internal",
        "userAgent": "AWS Internal",
        "eventID": "0000000-0000-0000-1111-123456789012",
        "readOnly": false,
        "eventType": "AwsServiceEvent",
        "serviceEventDetails": {
            "deregisterOrganizationalUnitStatus": {
                "state": "SUCCEEDED",
                "message": "AWS Control Tower successfully deregistered an
organizational unit, and enabled mandatory guardrails on the new organizational
unit.",
                "organizationalUnit" :
                  {
                    "organizationalUnitName": "Test",                    // Foundational
OU name.
                    "organizationalUnitId": "ou-adpf-302pk332"           // Foundational
OU ID.
                  },
                "requestedTimestamp": "2018-08-30T21:42:18Z",
                "completedTimestamp": "2018-08-30T21:42:18Z"
            }
            }
        }
    }
```

PrecheckOrganizationalUnit

이 수명 주기 이벤트는 AWS Control Tower가 OU에 대한 사전 검사를 성공적으로 수행했는지 여부를 기록합니다. 이 이벤트는 AWS Control Tower `PrecheckOrganizationalUnit` CloudTrail 이벤트에 해당합니다. 수명 주기 이벤트 로그에는 AWS Control Tower가 OU 등록 프로세스 중에 사전 점검을 수행한 각 리소스의 `IdName`, 및 `failedPrechecks` 값에 대한 필드가 포함되어 있습니다.

이벤트 로그에는,, 필드를 포함하여 사전 점검이 수행된 중첩 계정에 대한 정보도 포함되어 있습니다. `accountName` `accountId` `failedPrechecks`

`failedPrechecks`값이 비어 있으면 해당 리소스에 대한 모든 사전 검사가 성공적으로 통과되었음을 의미합니다.

- 이 이벤트는 사전 검사에 실패한 경우에만 발생합니다.
- 빈 OU를 등록하는 경우에는 이 이벤트가 발생하지 않습니다.

이벤트 예:


```
{
  "eventVersion": "1.08",
  "userIdentity": {
    "accountId": "XXXXXXXXXXXX",
    "invokedBy": "AWS Internal"
  },
  "eventTime": "2021-09-20T22:45:43Z",
  "eventSource": "controltower.amazonaws.com",
  "eventName": "PrecheckOrganizationalUnit",
  "awsRegion": "us-west-2",
  "sourceIPAddress": "AWS Internal",
  "userAgent": "AWS Internal",
  "eventID": "b41a9d67-0da4-4dc5-a87a-25fa19dc5305",
  "readOnly": false,
  "eventType": "AwsServiceEvent",
  "managementEvent": true,
  "recipientAccountId": "XXXXXXXXXXXX",
  "serviceEventDetails": {
    "precheckOrganizationalUnitStatus": {
      "organizationalUnit": {
        "organizationalUnitName": "Ou-123",
        "organizationalUnitId": "ou-abcd-123456",
        "failedPrechecks": [
            "SCP_CONFLICT"
          ]
      },
      "accounts": [
        {
          "accountName": "Child Account 1",
          "accountId": "XXXXXXXXXXXX",
          "failedPrechecks": [
            "FAILED_TO_ASSUME_ROLE"
          ]
        },
        {
          "accountName": "Child Account 2",
          "accountId": "XXXXXXXXXXXX",
```

```
          "failedPrechecks": [
            "FAILED_TO_ASSUME_ROLE"
          ]
        },
        {
          "accountName": "Management Account",
          "accountId": "XXXXXXXXXXXX",
          "failedPrechecks": [
            "MISSING_PERMISSIONS_AF_PRODUCT"
          ]
        },
        {
          "accountName": "Child Account 3",
          "accountId": "XXXXXXXXXXXX",
          "failedPrechecks": []
        },
        ...
      ],
      "state": "FAILED",
      "message": "AWS Control Tower failed to register an organizational unit due to
 pre-check failures. Go to the OU details page to download a list of failed pre-checks
 for the OU and accounts within.",
      "requestedTimestamp": "2021-09-20T22:44:02+0000",
      "completedTimestamp": "2021-09-20T22:45:43+0000"
    }
  },
  "eventCategory": "Management"
}
```

에서 AWS 사용자 알림 사용 AWS Control Tower

AWS 사용자 알림을 사용하여 AWS Control Tower 이벤트 알림을 받을 전송 채널을 설정할 수 있습니다. 이벤트가 지정한 규칙과 일치하면 알림을 받습니다. 이메일, AWS Chatbot채팅 알림, AWS 콘솔 모바일 앱 푸시 알림 등 여러 채널을 통해 이벤트 알림을 받을 수 있습니다. 콘솔 알림 센터에서도 알림을 볼 수 있습니다.

AWS 사용자 알림은 집계를 지원하므로 특정 이벤트 중에 받는 알림 수를 줄일 수 있습니다. 알림은 콘솔 알림 센터에서도 볼 수 있습니다.

대신 AWS 사용자 알림을 통해 알림을 구독하면 EventBridge 다음과 같은 이점이 있습니다.

- 더 친숙한 사용자 인터페이스 (UI).

- 글로벌 내비게이션 바의 벨/알림 영역에서 AWS 콘솔과 통합됩니다.
- 이메일 알림이 기본적으로 지원되므로 Amazon SNS를 설정할 필요가 없습니다.
- 가장 눈에 띄는 것은 AWS 사용자 알림 전용 모바일 푸시 알림 지원입니다.

예를 들어 Security Hub의 중요하고 심각도가 높은 것으로 확인되는 경우를 예로 들 수 있습니다. 알림 구독을 설정하는 JSON의 코드 스니펫은 다음과 같을 수 있습니다.

```
{
  "detail": {
    "findings": {
      "Compliance": {
        "Status": ["FAILED", "WARNING", "NOT_AVAILABLE"]
      },
      "RecordState": ["ACTIVE"],
      "Severity": {
        "Label": ["CRITICAL", "HIGH"]
      },
      "Workflow": {
        "Status": ["NEW", "NOTIFIED"]
      }
    }
  }
}
```

이벤트 필터링

- AWS 사용자 알림 콘솔에서 사용할 수 있는 필터를 사용하여 서비스 및 이름별로 이벤트를 필터링할 수 있습니다.
- JSON 코드로 필터를 직접 만들면 특정 속성별로 이벤트를 EventBridge 필터링할 수 있습니다.

예제 이벤트 AWS Control Tower

다음은 에 대한 일반화된 예제 이벤트입니다. AWS Control Tower

- EventBridge 이벤트입니다.
- AWS 사용자 알림을 사용하여 EventBridge 이벤트 (예: 이 이벤트) 를 구독할 수 있습니다.

```
{
```

```
    "version": "0",
    "id": "<id>", // alphanumeric string
    "detail-type": "AWS Service Event via CloudTrail",
    "source": "aws.controltower",
    "account": "<account ID>", // Management account ID.
    "time": "<date>", // Format: yyyy-MM-dd'T'hh:mm:ssZ
    "region": "<region>", // AWS Control Tower home region.
    "resources": [],
    "detail": {
        "eventVersion": "1.05",
        "userIdentity": {
            "accountId": "121212121212",
            "invokedBy": "AWS Internal"
        },
        "eventTime": "2018-08-30T21:42:18Z", // Timestamp when call was made. Format:
 yyyy-MM-dd'T'hh:mm:ssZ.
        "eventSource": "controltower.amazonaws.com",
        "eventName": "<event name>", // one of the 9 event names in https://
docs.aws.amazon.com/controltower/latest/userguide/lifecycle-events.html
        "awsRegion": "<region>",
        "sourceIPAddress": "AWS Internal",
        "userAgent": "AWS Internal",
        "eventID": "<id>",
        "readOnly": false,
        "eventType": "AwsServiceEvent",
        "serviceEventDetails": {
            // the contents of this object vary depending on the event subtype and
 event state
        }
    }
}
```

연습

이 장에는 AWS Control Tower를 사용하는 데 도움이 될 수 있는 단계별 절차가 포함되어 있습니다.

주제

둘러보기: ALZ에서 AWS 컨트롤 타워로 이동

많은 AWS 고객이 AWS Landing Zone 솔루션 (ALZ) 을 채택하여 안전하고 규정을 준수하는 다중 AWS 계정 환경을 구축했습니다. 랜딩 존 관리 부담을 줄이기 위해 AWS Control Tower라는 관리형 서비스를 AWS 만들었습니다.

ALZ에는 추가 기능이 예정되어 있지 않으며 장기적으로만 지원될 예정입니다. 따라서 ALZ에서 AWS Control Tower 서비스로 이동하는 것이 좋습니다. 이 장에 링크된 블로그에서는 이러한 이동에 대한 다양한 고려 사항을 안내하고 ALZ에서 AWS Control Tower로의 성공적인 마이그레이션을 계획할 수 있는 방법을 설명합니다.

블로그: AWS 랜딩 존 솔루션을 AWS Control Tower로 마이그레이션

AWS 규범적 지침은 ALZ에서 AWS Control Tower로 전환하는 단계를 포함하여 보다 광범위한 설명서를 제공합니다. 기본적으로 여러 사전 요구 사항에 따라 ALZ를 실행하는 기존 조직에서 AWS Control Tower 거버넌스를 활성화합니다. 자세한 내용은 AWS 랜딩 존에서 AWS Control Tower로의 전환을 참조하십시오.

둘러보기: Service Catalog API를 이용한 AWS Control Tower의 계정 프로비저닝 자동화

AWS Control Tower는 다음과 같은 여러 다른 AWS 서비스와 통합되어 AWS Service Catalog있습니다. API를 사용하여 AWS Control Tower에서 회원 계정을 생성하고 프로비저닝할 수 있습니다.

이 동영상은 AWS Service Catalog API를 호출하여 자동화된 일괄 처리 방식으로 계정을 프로비저닝하는 방법을 보여줍니다. 프로비저닝의 경우 AWS 명령줄 인터페이스 (CLI) 에서 ProvisionProductAPI를 호출하고 설정하려는 각 계정의 파라미터가 포함된 JSON 파일을 지정합니다. 이 동영상은 AWS Cloud9 개발 환경을 설치하고 사용하여 이 작업을 수행하는 방법을 보여줍니다. AWS Cloud9 대신 클라우드셸을 사용하는 경우에도 CLI 명령은 동일합니다. AWS

> **Note**
>
> 또한 각 계정의 API를 호출하여 계정 업데이트 자동화에 이 접근 방식을 적용할 수 있습니다. UpdateProvisionedProduct AWS Service Catalog 계정을 하나씩 업데이트하는 스크립트를 작성할 수 있습니다.

완전히 다른 자동화 방법으로, Terraform에 익숙하다면 AWS Control Tower Account Factory for Terraform (AFT) 으로 계정을 프로비저닝할 수 있습니다.

자동화 관리 역할 예시

다음은 관리 계정에서 자동화 관리 역할을 구성하는 데 사용할 수 있는 샘플 템플릿입니다. 대상 계정에서 관리자 액세스를 사용하여 자동화를 수행할 수 있도록 관리 계정에서 이 역할을 구성해야 합니다.

```
AWSTemplateFormatVersion: 2010-09-09
Description: Configure the SampleAutoAdminRole

Resources:
  AdministrationRole:
    Type: AWS::IAM::Role
    Properties:
      RoleName: SampleAutoAdminRole
      AssumeRolePolicyDocument:
        Version: 2012-10-17
        Statement:
          - Effect: Allow
            Principal:
              Service: cloudformation.amazonaws.com
            Action:
              - sts:AssumeRole
      Path: /
      Policies:
        - PolicyName: AssumeSampleAutoAdminRole
          PolicyDocument:
```

```
            Version: 2012-10-17
            Statement:
              - Effect: Allow
                Action:
                  - sts:AssumeRole
                Resource:
                  - "arn:aws:iam::*:role/SampleAutomationExecutionRole"
```

샘플 자동화 실행 역할

다음은 자동화 실행 역할을 설정하는 데 사용할 수 있는 샘플 템플릿입니다. 대상 계정에서 이 역할을 구성할 수 있습니다.

```
AWSTemplateFormatVersion: "2010-09-09"
Description: "Create automation execution role for creating Sample Additional Role."

Parameters:
  AdminAccountId:
    Type: "String"
    Description: "Account ID for the administrator account (typically management,
 security or shared services)."
  AdminRoleName:
    Type: "String"
    Description: "Role name for automation administrator access."
    Default: "SampleAutomationAdministrationRole"
  ExecutionRoleName:
    Type: "String"
    Description: "Role name for automation execution."
    Default: "SampleAutomationExecutionRole"
  SessionDurationInSecs:
    Type: "Number"
    Description: "Maximum session duration in seconds."
    Default: 14400

Resources:
  # This needs to run after AdminRoleName exists.
  ExecutionRole:
    Type: "AWS::IAM::Role"
    Properties:
      RoleName: !Ref ExecutionRoleName
      MaxSessionDuration: !Ref SessionDurationInSecs
      AssumeRolePolicyDocument:
        Version: "2012-10-17"
```

```
        Statement:
          - Effect: "Allow"
            Principal:
              AWS:
                - !Sub "arn:aws:iam::${AdminAccountId}:role/${AdminRoleName}"
            Action:
              - "sts:AssumeRole"
      Path: "/"
      ManagedPolicyArns:
        - "arn:aws:iam::aws:policy/AdministratorAccess"
```

이러한 역할을 구성한 후에는 AWS Service Catalog API를 호출하여 자동화된 작업을 수행합니다. CLI 명령은 비디오에 나와 있습니다.

Service Catalog API의 샘플 프로비저닝 입력

다음은 API를 사용하여 AWS Control Tower 계정을 프로비저닝하는 경우 Service Catalog `ProvisionProduct` API에 제공할 수 있는 입력의 샘플입니다.

```
{
  pathId: "lpv2-7n2o3nudljh4e",
  productId: "prod-y422ydgjge2rs",
  provisionedProductName: "Example product 1",
  provisioningArtifactId: "pa-2mmz36cfpj2p4",
  provisioningParameters: [
    {
      key: "AccountEmail",
      value: "abc@amazon.com"
    },
    {
      key: "AccountName",
      value: "ABC"
    },
    {
      key: "ManagedOrganizationalUnit",
      value: "Custom (ou-xfe5-a8hb8ml8)"
    },
    {
      key: "SSOUserEmail",
      value: "abc@amazon.com"
    },
    {
      key: "SSOUserFirstName",
```

```
      value: "John"
    },
    {
      key: "SSOUserLastName",
      value: "Smith"
    }
  ],
  provisionToken: "c3c795a1-9824-4fb2-a4c2-4b1841be4068"
}
```

자세한 내용은 Service Catalog의 API 참조를 참조하십시오.

> **Note**
>
> 값의 입력 문자열 형식이 에서 OU_NAME 로 ManagedOrganizationalUnit 변경되었음을 알 수 OU_NAME (OU_ID) 있습니다. 다음 비디오에서는 이러한 변경 사항에 대해 언급하지 않습니다.

비디오 안내

이 동영상 (6:58) 은 AWS Control Tower에서 계정 배포를 자동화하는 방법을 설명합니다. 동영상 오른쪽 하단에 있는 아이콘을 선택하여 전체 화면으로 확대하면 더 잘 보입니다. 자막을 사용할 수 있습니다.

AWS Control Tower의 자동 계정 프로비저닝에 대한 동영상 설명.

둘러보기: VPC 없이 AWS 컨트롤 타워 구성

이 주제에서는 VPC 없이 AWS Control Tower 계정을 구성하는 방법을 안내합니다.

워크로드에 VPC가 필요하지 않은 경우 다음을 수행할 수 있습니다.

- AWS Control Tower 가상 사설 클라우드 (VPC) 를 삭제할 수 있습니다. 이 VPC는 랜딩 존을 설정할 때 생성됩니다.
- 연결된 VPC 없이 새 AWS Control Tower 계정을 생성하도록 Account Factory 설정을 변경할 수 있습니다.

> **Important**
>
> VPC 인터넷 액세스 설정이 활성화된 상태에서 Account Factory 계정을 프로비저닝하는 경우, 해당 Account Factory 설정은 고객이 관리하는 Amazon VPC 인스턴스에 대한 인터넷 액세스 허용 안 함 제어보다 우선합니다. 새로 프로비전된 계정에 대한 인터넷 액세스를 활성화하지 않으려면 Account Factory에서 설정을 변경해야 합니다.

AWS Control Tower VPC를 삭제합니다.

AWS Control Tower 외부에서 모든 AWS 고객은 기본 VPC를 가지고 있으며, Amazon VPC (가상 사설 클라우드) 콘솔 https://console.aws.amazon.com/vpc/ 에서 기본 VPC를 확인할 수 있습니다. 기본 VPC의 이름에는 이름 끝 부분에 항상 (default)라는 단어가 포함되므로 기본 VPC를 인식할 수 있습니다.

AWS Control Tower 랜딩 존을 설정하면 AWS Control Tower는 AWS 기본 VPC를 삭제하고 새 AWS Control Tower 기본 VPC를 생성합니다. 새 VPC는 AWS Control Tower 관리 계정과 연결되어 있습니다. 이 주제에서는 새 VPC를 Control Tower VPC라고 부릅니다.

Amazon VPC 콘솔에서 AWS 컨트롤 타워 VPC를 볼 때는 이름 끝에 (기본값) 이라는 단어가 표시되지 않습니다. VPC가 두 개 이상인 경우 할당된 CIDR 범위를 사용하여 올바른 AWS Control Tower VPC를 식별해야 합니다.

AWS 컨트롤 타워 VPC를 삭제할 수 있지만, 나중에 AWS Control Tower에서 VPC가 필요할 경우 직접 생성해야 합니다.

AWS 컨트롤 타워 VPC를 삭제하려면

1. https://console.aws.amazon.com/vpc/에서 Amazon VPC 콘솔을 여세요.
2. Service Catalog 옵션에서 VPC를 **VPC** 검색하거나 선택합니다. 그러면 VPC 대시보드가 표시됩니다.
3. 왼쪽 메뉴에서 VPC를 선택합니다. 그러면 모든 VPC가 나와 있는 목록이 표시됩니다.
4. CIDR 범위로 AWS 컨트롤 타워 VPC를 식별하십시오.
5. VPC를 삭제하려면 작업을 선택한 다음 VPC 삭제를 선택합니다.

AWS Control Tower 관리 계정을 위한 AWS (기본) VPC는 이미 모든 지역에 있습니다. 보안 모범 사례를 따르려면 AWS Control Tower VPC를 삭제하기로 선택한 경우 모든 지역의 관리 계정과 연결된 기

본 AWS VPC도 삭제하는 것이 가장 좋습니다. AWS 따라서 관리 계정을 보호하려면 각 지역에서 기본 VPC를 제거하고, AWS Control Tower 홈 지역의 Control Tower에서 생성한 VPC도 제거해야 합니다.

VPC 없이 AWS Control Tower에서 계정 생성

최종 사용자 워크로드에 VPC가 필요하지 않은 경우 이 방법을 사용하여 VPC가 자동으로 생성되지 않는 최종 사용자 계정을 설정할 수 있습니다.

AWS Control Tower 대시보드에서 네트워크 구성 설정을 보고 편집할 수 있습니다. 관련 VPC 없이 AWS Control Tower 계정이 생성되도록 설정을 변경하면 설정을 다시 변경할 때까지 모든 새 계정이 VPC 없이 생성됩니다.

VPC 없이 계정을 생성하도록 Account Factory를 구성하려면

1. 웹 브라우저를 열고 https://console.aws.amazon.com/controltower 에서 AWS Control Tower 콘솔로 이동합니다.
2. 왼쪽 메뉴에서 Account Factory를 선택합니다.
3. 그러면 네트워크 구성 섹션이 있는 Account Factory 페이지가 표시됩니다.
4. 나중에 복원하려는 경우 현재 설정을 기록해 두십시오.
5. 네트워크 구성 섹션에서 편집 버튼을 선택합니다.
6. Account Factory 네트워크 구성 편집 페이지에서 VPC Configuration options for new accounts 섹션으로 이동합니다.

   옵션 1이나 옵션 2 또는 둘 다를 따라 AWS Control Tower가 계정을 프로비저닝할 때 VPC를 생성하지 않도록 할 수 있습니다.

   a. 옵션 1 — 서브넷 제거

      - Internet-accessible subnet 토글 스위치를 끕니다.
      - Maximum number of private subnets 값을 0으로 설정합니다.

   b. 옵션 2 — 지역 제거 AWS

      - Regions for VPC creation 열의 모든 확인란을 선택 취소합니다.
7. 저장을 선택합니다.

가능한 오류

AWS Control Tower VPC를 삭제하거나 VPC가 없는 계정을 생성하도록 Account Factory를 재구성할 때 발생할 수 있는 이러한 오류에 유의하십시오.

- 기존 관리 계정의 AWS Control Tower VPC에 종속성이나 리소스가 있을 수 있으며, 이로 인해 삭제 실패 오류가 발생할 수 있습니다.
- VPC 없이 새 계정을 시작하도록 설정할 때 기본 CIDR을 그대로 두면 요청이 실패하고 CIDR이 유효하지 않습니다 오류가 표시됩니다.

둘러보기: AWS 방화벽 관리자를 사용하여 AWS 컨트롤 타워에 보안 그룹 설정

이 동영상은 AWS Firewall Manager 서비스를 사용하여 AWS Control Tower의 네트워크 보안을 개선하는 방법을 보여줍니다. 보안 그룹을 설정할 수 있는 보안 관리자 계정을 지정할 수 있습니다. AWS Control Tower 조직에 보안 정책을 구성하고 보안 규칙을 적용하는 방법과 정책을 자동으로 적용하여 규정을 준수하지 않는 리소스를 수정하는 방법을 알아봅니다. 조직의 각 계정 및 리소스 (예: Amazon EC2 인스턴스) 에 적용되는 보안 그룹을 볼 수 있습니다.

자체 방화벽 정책을 생성하거나 신뢰할 수 있는 공급업체의 규칙을 구독할 수 있습니다.

AWS 방화벽 관리자를 사용하여 보안 그룹 설정

이 동영상 (8:02) 은 AWS Control Tower의 리소스 및 워크로드에 더 나은 네트워크 인프라 보안을 설정하는 방법을 설명합니다. 동영상 오른쪽 하단에 있는 아이콘을 선택하여 전체 화면으로 확대하면 더 잘 보입니다. 자막을 사용할 수 있습니다.

AWS Control Tower의 방화벽 설정 안내 동영상.

자세한 내용은 WAF 설정 AWS 방법에 대한 설명서를 참조하십시오.

둘러보기: AWS Control Tower 랜딩 존 해체

AWS Control Tower를 사용하면 랜딩 존이라고 하는 안전한 다중 계정 AWS 환경을 설정하고 관리할 수 있습니다. AWS Control Tower에서 할당한 모든 리소스를 정리하는 프로세스를 랜딩 존 해체라고 합니다.

더 이상 AWS Control Tower를 사용하지 않으려는 경우, 자동 폐기 도구가 AWS Control Tower에서 할당한 리소스를 정리합니다. 자동 해체 프로세스를 시작하려면 랜딩 존 설정 페이지로 이동하여 서비스 해제 탭을 선택한 다음 서비스 해제 랜딩 존을 선택합니다.

서비스 해제 중에 수행된 작업 목록은 을 참조하십시오. 폐기 프로세스 개요

> **Warning**
>
> 모든 AWS Control Tower 리소스를 수동으로 삭제하는 것은 서비스 해제와 다릅니다. 새 착륙 지대를 설정할 수 없습니다.

해체 과정에서 AWS Organizations 다음과 같은 방식으로 사용자 데이터와 기존 데이터가 변경되지 않습니다.

- AWS Organizations는 데이터를 제거하지 않고 생성한 랜딩 영역의 요소만 제거합니다.
- 폐기 프로세스가 완료된 후에도 Amazon S3 버킷 및 CloudWatch Amazon Logs 로그 그룹과 같은 몇 가지 리소스 아티팩트가 남아 있습니다. 다른 랜딩 영역을 설정하기 전에 이러한 리소스를 수동으로 삭제하여 특정 리소스를 유지 관리하는 데 따른 비용이 발생하지 않도록 해야 합니다.
- 자동 폐기를 사용하여 부분적으로 설정된 랜딩 존을 제거할 수 없습니다. 랜딩 존 설정 프로세스가 실패할 경우, 실패 상태를 해결하고 자동 폐기를 가능하게 하기 위해 모든 방법을 설정해야 합니다. 그렇지 않으면 리소스를 개별적으로 수동으로 삭제해야 합니다.

랜딩 영역을 폐기하는 것은 중대한 결과를 초래하는 프로세스이며 실행 취소할 수 없습니다. AWS Control Tower에서 취한 폐기 조치와 해체 후 남아 있는 아티팩트는 다음 섹션에 설명되어 있습니다.

> **Important**
>
> 랜딩 영역 사용을 중지하려는 경우에만 이 폐기 프로세스를 수행하는 것이 좋습니다. 기존 랜딩 영역을 폐기한 후에는 다시 생성할 수 없습니다.

폐기 프로세스 개요

랜딩 존 해제를 요청하면 AWS Control Tower는 다음과 같은 조치를 취합니다.

- landing zone에서 활성화된 각 탐정 제어를 비활성화합니다. AWS Control Tower는 제어를 지원하는 AWS CloudFormation 리소스를 삭제합니다.

- 에서 서비스 제어 정책 (SCP) 을 제거하여 각 예방 제어를 비활성화합니다. AWS Organizations정책이 비어 있는 경우 (AWS Control Tower에서 관리하는 모든 SCP를 제거한 후여야 함), AWS Control Tower는 정책을 분리하고 완전히 삭제합니다.
- 로 배포된 모든 블루프린트를 삭제합니다. AWS CloudFormation StackSets
- 모든 지역에 CloudFormation 스택으로 배포된 모든 블루프린트를 삭제합니다.
- 프로비저닝된 각 계정에 대해 AWS Control Tower는 서비스 종료 프로세스 중에 다음과 같은 작업을 수행합니다.
  - 각 Account Factory 계정의 레코드를 삭제합니다.
  - AWS Control Tower에서 생성한 IAM 역할을 제거하고 (추가 정책이 추가되지 않은 경우) 표준 IAM 역할을 다시 생성하여 계정에 대한 AWS Control Tower 권한을 취소합니다. `OrganizationsFullAccessRole`
  - 에서 계정 기록을 제거합니다. AWS Service Catalog
  - AWS Service Catalog에서 Account Factory 제품 및 포트폴리오를 제거합니다.
- 공유 (감사 및 로그 아카이브) 계정의 블루프린트를 삭제합니다.
- AWS Control Tower에서 생성한 IAM 역할을 제거하고 (추가 정책이 추가되지 않은 경우) IAM 역할을 다시 생성하여 공유 계정에서 AWS Control Tower 권한을 취소합니다. `OrganizationsFullAccessRole`
- 공유 계정과 관련된 레코드를 삭제합니다.
- 고객이 생성한 OU와 관련된 레코드를 삭제합니다.
- 홈 리전을 식별하는 내부 레코드를 삭제합니다.

> **Note**
>
> 폐기 후 VPC가 비어 있지 않은 경우 Account Factory VPC 블루프린트 (`BP_ACCOUNT_FACTORY_VPC`)를 제거하여 경로와 NAT 게이트웨이를 정리할 수 있습니다.

해체 중에 리소스가 제거되지 않음

랜딩 존을 폐기한다고 해서 AWS Control Tower 설치 프로세스를 완전히 되돌릴 수는 없습니다. 특정 리소스는 남아 있으며 수동으로 제거할 수 있습니다.

AWS Organizations

기존 AWS Organizations 조직이 없는 고객의 경우, AWS Control Tower는 보안과 샌드박스라는 두 개의 조직 단위 (OU) 로 구성된 조직을 구성합니다. 랜딩 영역을 폐기하는 경우 다음과 같이 조직의 계층이 유지됩니다.

- AWS Control Tower 콘솔에서 생성한 조직 단위 (OU) 는 제거되지 않습니다.
- 보안 및 샌드박스 OU는 제거되지 않습니다.
- 조직은 AWS Organizations삭제되지 않습니다.
- 공유, 프로비저닝 또는 관리 계정의 어떤 계정도 이동되거나 제거되지 않습니다. AWS Organizations

AWS IAM Identity Center (SSO)

기존 IAM ID 센터 디렉터리가 없는 고객의 경우, AWS Control Tower는 IAM ID 센터를 설정하고 초기 디렉터리를 구성합니다. 랜딩 존을 해제해도 AWS Control Tower는 IAM ID 센터를 변경하지 않습니다. 필요한 경우 관리 계정에 저장된 IAM ID 센터 정보를 수동으로 삭제할 수 있습니다. 특히 다음 영역은 폐기를 통해 변경되지 않습니다.

- Account Factory로 생성한 사용자는 제거되지 않습니다.
- AWS Control Tower 설치로 생성된 그룹은 제거되지 않습니다.
- AWS Control Tower에서 생성한 권한 집합은 제거되지 않습니다.
- AWS 계정과 IAM ID 센터 권한 집합 간의 연결은 제거되지 않습니다.
- IAM ID 센터 디렉터리는 변경되지 않습니다.

역할

설정 중에 콘솔을 사용하는 경우 AWS Control Tower가 특정 역할을 생성하거나, API를 통해 landing Zone을 설정하는 경우 이러한 역할을 생성하도록 요청합니다. landing Zone을 사용 중지해도 다음 역할은 제거되지 않습니다.

- `AWSControlTowerAdmin`
- `AWSControlTowerCloudTrailRole`
- `AWSControlTowerStackSetRole`
- `AWSControlTowerConfigAggregatorRoleForOrganizations`

Amazon S3 버킷

설정 중에 AWS Control Tower는 로깅 계정에 로깅 및 로깅 액세스를 위한 버킷을 생성합니다. 랜딩 영역을 폐기할 때 다음 리소스는 제거되지 않습니다.

- 로깅 계정의 로깅 및 로깅 액세스 S3 버킷은 제거되지 않습니다.
- 로깅 및 로깅 액세스 버킷의 내용은 제거되지 않습니다.

공유 계정

AWS Control Tower 설치 중에 보안 OU에 두 개의 공유 계정 (감사 및 로그 아카이브) 이 생성됩니다. 랜딩 영역을 폐기하는 경우 다음과 같은 결과가 발생합니다.

- AWS Control Tower 설치 중에 생성된 공유 계정은 폐쇄되지 않습니다.
- `OrganizationAccountAccessRole`IAM 역할은 표준 구성에 맞게 다시 생성됩니다. AWS Organizations
- `AWSControlTowerExecution` 역할은 제거됩니다.

프로비저닝된 계정

AWS Control Tower 고객은 어카운트 팩토리를 사용하여 새 AWS 계정을 생성할 수 있습니다. 랜딩 영역을 폐기하는 경우 다음과 같은 결과가 발생합니다.

- Account Factory로 생성한 프로비저닝된 계정은 해지되지 않습니다.
- 에서 프로비저닝된 AWS Service Catalog 제품은 제거되지 않습니다. 해당 계정을 종료하여 정리하면 해당 계정이 루트 OU로 이동됩니다.
- AWS Control Tower가 생성한 VPC는 제거되지 않으며, 관련 AWS CloudFormation 스택 세트 (`BP_ACCOUNT_FACTORY_VPC`) 도 제거되지 않습니다.
- `OrganizationAccountAccessRole`IAM 역할은 표준 구성에 맞게 다시 생성되었습니다. AWS Organizations
- `AWSControlTowerExecution` 역할은 제거됩니다.

CloudWatch 로그 로그 그룹

라는 이름의 `AWSControlTowerBP-BASELINE-CLOUDTRAIL-MANAGEMENT` 블루프린트의 일부로 CloudWatch 로그 로그 그룹`aws-controltower/CloudTrailLogs`, 이 생성됩니다. 이 로그 그룹은 제거되지 않습니다. 대신 청사진이 삭제되며 리소스는 유지됩니다.

- 다른 랜딩 영역을 설정하기 전에 이 로그 그룹을 수동으로 삭제해야 합니다.

> **Note**
>
> Landzone 3.0 이상을 사용하는 고객은 등록된 개별 계정의 로그 및 로그 역할을 삭제할 필요가 없습니다. 이러한 CloudTrail CloudTrail 로그 및 로그 역할은 조직 수준 추적을 위해 관리 계정에서만 생성되기 때문입니다.
>
> AWS Control Tower는 랜딩 존 버전 3.2부터 라는 아마존 EventBridge 규칙을 생성합니다`AWSControlTowerManagedRule`. 이 규칙은 모든 관리 지역에 대해 각 회원 계정에 생성됩니다. 이 규칙은 서비스 해제 중에 자동으로 삭제되지 않으므로 새 지역에 랜딩 존을 설정하려면 먼저 모든 관리 지역의 공유 및 멤버 계정에서 규칙을 수동으로 삭제해야 합니다.

AWS Control Tower 리소스를 삭제하는 방법에 대한 절차는 에 나와 AWS Control 타워 리소스 관리 있습니다.

AWS Control 타워 리소스 관리

이 문서에서는 정기적인 유지 관리 및 관리 작업의 일환으로 AWS Control Tower 리소스를 개별적으로 제거하는 방법에 대한 지침을 제공합니다. 이 장에 제공된 절차는 필요한 경우 개별 리소스 또는 일부 리소스를 제거하는 데만 사용됩니다. 랜딩 존을 해체하는 것과는 다릅니다.

다음과 같은 두 가지 유형의 작업을 수행하려면 리소스를 제거해야 할 수 있습니다.

- 일반적인 상황에서 랜딩 영역을 관리할 때 리소스를 삭제하려는 경우
- 자동 폐기 후 남아 있는 리소스를 정리하기 위함입니다.

> **Warning**
>
> 리소스를 수동으로 제거하면 새 랜딩 존을 설정할 수 없습니다. 해체하는 것과는 다릅니다. AWS Control Tower 랜딩 존을 폐기하려는 경우 이 장에 설명된 조치를 둘러보기: AWS Control Tower 랜딩 존 해체 취하기 전에 의 지침을 따르십시오. 이 장의 지침은 자동 해제가 완료된 후 남아 있는 리소스를 정리하는 데 도움이 될 수 있습니다. 모든 랜딩 존 리소스를 수동으로 삭제하더라도 랜딩 존을 해체하는 것과는 다르며 예상치 못한 요금이 발생할 수 있습니다.

AWS Control Tower에서 계정을 제거해야 하는 경우 다음 섹션을 참조하여 계정을 폐쇄하십시오.

- 계정 관리 취소
- Account Factory에서 생성한 계정 폐쇄

삭제하는 대신 서비스 해제가 필요한가요?

기업용 AWS Control Tower를 더 이상 사용할 계획이 없거나 조직 리소스의 대대적인 재배포가 필요한 경우, 처음 landing Zone을 설정할 때 생성한 리소스를 사용 중지하는 것이 좋습니다.

- 폐기 프로세스가 완료된 후에도 Amazon S3 버킷 및 CloudWatch Amazon Logs 로그 그룹과 같은 몇 가지 리소스 아티팩트가 남아 있습니다.
- 다른 랜딩 존 (Landing Zone) 을 설정하기 전에 계정의 나머지 리소스를 수동으로 정리하여 예상치 못한 요금이 부과되지 않도록 해야 합니다. 자세한 설명은 해체 중에 리소스가 제거되지 않음 섹션을 참조하세요.

> **Warning**
>
> Landing Zone 사용을 중단하려는 경우에만 해체 프로세스를 수행하는 것이 좋습니다. 이 프로세스는 실행 취소할 수 없습니다.

AWS Control Tower 리소스 제거에 대한 정보

이 장의 개별 절차는 AWS Control Tower 리소스를 수동으로 제거하는 방법을 안내합니다. 이 절차는 Landing Zone에서 특정 리소스를 삭제해야 할 때 따를 수 있습니다.

이 절차를 수행하기 전에 달리 명시되지 않는 한, 랜딩 존의 홈 리전에 로그인하고 랜딩 존이 포함된 관리 계정에 대한 관리자 권한을 가진 IAM 사용자 또는 IAM Identity Center의 사용자로 로그인해야 합니다. AWS Management Console

> **Warning**
>
> 이는 AWS Control Tower 설정에 거버넌스 드리프트를 도입할 수 있는 파괴적인 조치입니다. 이는 실행 취소할 수 없습니다.

주제

- SCP 삭제

- 삭제 StackSets 및 스택
- 로그 아카이브 계정에서 Amazon S3 버킷을 삭제합니다.
- Account Factory 포트폴리오 및 제품 제거
- AWS Control Tower 역할 및 정책 제거
- AWS Control 타워 리소스 도움말

SCP 삭제

AWS Control Tower는 제어를 위해 서비스 제어 정책 (SCP) 을 사용합니다. 이 절차는 특히 AWS Control Tower와 관련된 SCP를 삭제하는 방법을 안내합니다.

SCP를 AWS Organizations 삭제하려면

1. https://console.aws.amazon.com/organizations/에서 Organizations 콘솔을 엽니다.
2. 정책 탭을 열고 접두사 aws-guardrails-가 있는 서비스 제어 정책(SCP)을 찾아 각 SCP에 대해 다음을 수행합니다.
   a. 연결된 OU에서 SCP를 분리합니다.
   b. SCP를 삭제합니다.

삭제 StackSets 및 스택

AWS Control Tower는 랜딩 존에 AWS Config 규칙 컨트롤과 관련된 배포를 위해 StackSets 및 스택을 사용합니다. 다음 절차는 이러한 특정 리소스를 삭제하는 방법을 설명합니다.

삭제하려면 AWS CloudFormation StackSets

1. https://console.aws.amazon.com/cloudformation 에서 AWS CloudFormation 콘솔을 엽니다.
2. 왼쪽 탐색 메뉴에서 선택합니다 StackSets.
3. 접두사가 StackSet AWSControlTower있는 각각에 대해 다음을 수행하십시오. StackSeta에 계정이 여러 개 있는 경우 시간이 좀 걸릴 수 있습니다.
   a. 대시보드의 표에서 특정 StackSet 항목을 선택합니다. 그러면 해당 속성 페이지가 열립니다 StackSet.
   b. 페이지 하단의 Stacks 테이블에서 테이블에 있는 모든 AWS 계정의 계정 ID를 기록합니다. 모든 계정 목록을 복사합니다.

c. 작업에서 스택 삭제를 선택합니다. StackSet

d. 배포 옵션 설정의 배포 위치에서 계정에 스택 배포를 선택합니다.

e. 텍스트 필드에 3.b단계에서 기록한 AWS 계정 ID를 쉼표로 구분하여 입력합니다. 예를 들면 *123456789012*, *098765431098* 등입니다.

f. Specify regions(리전 지정)에서 Add all(모두 추가)을 선택하고 페이지의 나머지 파라미터를 기본값으로 설정하고 다음을 선택합니다.

g. 검토 페이지에서 선택 사항을 검토한 다음 Delete stacks(스택 삭제)를 선택합니다.

h. StackSet 속성 페이지에서 상대방을 위해 이 절차를 다시 시작할 수 있습니다. StackSets

4. 여러 StackSets 속성 페이지의 스택 테이블에 있는 레코드가 비어 있으면 프로세스가 완료됩니다.
5. 스택 테이블의 레코드가 비어 있으면 삭제를 선택합니다. StackSet

스택을 AWS CloudFormation 삭제하려면

1. https://console.aws.amazon.com/cloudformation 에서 AWS CloudFormation 콘솔을 엽니다.
2. 스택 대시보드에서 접두사가 있는 모든 스택을 검색합니다. AWSControlTower
3. 테이블의 각 스택에 대해 다음을 수행합니다.

   a. 스택 이름 옆의 확인란을 선택합니다.

   b. 작업 메뉴에서 Delete Stack(스택 삭제)을 선택합니다.

   c. 열린 대화 상자에서 정보를 검토하여 정보가 정확한지 확인하고 예, 삭제를 선택합니다.

로그 아카이브 계정에서 Amazon S3 버킷을 삭제합니다.

다음 절차는 AWSControlTowerExecution그룹의 IAM Identity Center 사용자로 로그 아카이브 계정에 로그인한 다음 로그 아카이브 계정에서 Amazon S3 버킷을 삭제하는 방법을 안내합니다.

올바른 권한으로 로그 아카이브 계정에 로그인하려면

1. https://console.aws.amazon.com/organizations/에서 Organizations 콘솔을 엽니다.
2. 계정 탭에서 로그 아카이브 계정을 찾습니다.
3. 열린 오른쪽 창에서 로그 아카이브 계정 번호를 기록해 둡니다.
4. 탐색 모음에서 계정 이름을 선택한 다음 계정 메뉴를 엽니다.
5. 역할 전환을 선택합니다.
6. 열린 페이지에서 계정에 로그 아카이브 계정의 계정 번호를 입력합니다.

7. 역할에 다음을 입력합니다. AWSControlTowerExecution
8. 표시 이름은 텍스트로 채워져 있습니다.
9. 원하는 색상을 선택합니다.
10. 역할 전환을 선택합니다.

Amazon S3 버킷을 삭제하려면

1. https://console.aws.amazon.com/s3/ 에서 Amazon S3 콘솔을 엽니다.
2. aws-controltower가 포함된 버킷 이름을 검색합니다.
3. 테이블의 각 버킷에 대해 다음을 수행합니다.
   a. 테이블의 버킷에 대한 확인란을 선택합니다.
   b. 삭제를 선택합니다.
   c. 열린 대화 상자에서 정보를 검토하여 정보가 정확한지 확인하고 버킷의 이름을 입력하여 확인한 다음 확인을 선택합니다.

Account Factory 포트폴리오 및 제품 제거

다음 절차는 AWSServiceCatalogAdmins그룹에서 IAM Identity Center 사용자로 로그인한 다음 Account Factory 포트폴리오 및 제품을 정리하는 방법을 안내합니다.

적절한 권한으로 관리 계정에 로그인하는 방법

1. 사용자 포털 URL *directory-id*.awsapps.com/start로 이동합니다.
2. AWS 계정에서 관리 계정을 찾으세요.
3. 에서 AWSServiceCatalogAdminFullAccess관리 콘솔을 선택하여 이 AWS Management Console 역할로 로그인합니다.

Account Factory를 정리하려면

1. Service Quotas 콘솔(https://console.aws.amazon.com/servicecatalog/)을 엽니다.
2. 왼쪽 탐색 메뉴에서 Portfolios list(포트폴리오 목록)를 선택합니다.
3. 로컬 포트폴리오 테이블에서AWS Control Tower Account Factory 포트폴리오라는 이름의 포트폴리오를 검색하십시오.
4. 해당 포트폴리오의 이름을 선택하여 세부 정보 페이지로 이동합니다.

5. 페이지의 제약 조건 섹션을 확장하고 제품 이름이 AWS Control Tower Account Factory인 제약 조건의 라디오 버튼을 선택합니다.
6. 제약 조건 제거를 선택합니다.
7. 열린 대화 상자에서 정보를 검토하여 정보가 정확한지 확인하고 계속을 선택합니다.
8. 페이지의 제품 섹션에서 AWS Control Tower Account Factory라는 이름의 제품에 대한 라디오 버튼을 선택합니다.
9. 제품 제거를 선택합니다.
10. 열린 대화 상자에서 정보를 검토하여 정보가 정확한지 확인하고 계속을 선택합니다.
11. 페이지의 Users, Groups, and Roles(사용자, 그룹 및 역할) 섹션을 확장하고 이 테이블의 모든 레코드에 대한 확인란을 선택합니다.
12. REMOVE USERS, GROUP OR ROLE(사용자, 그룹 또는 역할 제거)을 선택합니다.
13. 열린 대화 상자에서 정보를 검토하여 정보가 정확한지 확인하고 계속을 선택합니다.
14. 왼쪽 탐색 메뉴에서 Portfolios list(포트폴리오 목록)를 선택합니다.
15. 로컬 포트폴리오 테이블에서AWS Control Tower Account Factory 포트폴리오라는 이름의 포트폴리오를 검색하십시오.
16. 해당 포트폴리오의 라디오 버튼을 선택한 다음 포트폴리오 삭제를 선택합니다.
17. 열린 대화 상자에서 정보를 검토하여 정보가 정확한지 확인하고 계속을 선택합니다.
18. 왼쪽 탐색 메뉴에서 Product list(제품 목록)를 선택합니다.
19. 관리자 제품 페이지에서 AWS Control Tower Account Factory라는 제품을 검색하십시오.
20. 제품을 선택하여 Admin product details(관리자 제품 세부 정보) 페이지를 엽니다.
21. 작업에서 Delete product(제품 삭제)를 선택합니다.
22. 열린 대화 상자에서 정보를 검토하여 정보가 정확한지 확인하고 계속을 선택합니다.

AWS Control Tower 역할 및 정책 제거

이 절차는 랜딩 존이 설정되었을 때 또는 이후에 AWS Control Tower가 생성한 역할 및 정책을 정리하는 방법을 안내합니다.

IAM ID 센터 AWSServiceCatalogEndUserAccess 역할을 삭제하려면

1. https://console.aws.amazon.com/singlesignon/ 에서 AWS IAM Identity Center 콘솔을 엽니다.
2. 지역을 홈 AWS 지역, 즉 AWS Control Tower를 처음 설치한 지역으로 변경하십시오.

3. 왼쪽 탐색 메뉴에서 AWS 계정을 선택합니다.
4. 관리 계정 링크를 선택합니다.
5. 권한 세트의 드롭다운을 선택하고 선택한 다음 제거를 선택합니다 AWSServiceCatalogEndUserAccess.
6. 왼쪽 패널에서 AWS 계정을 선택합니다.
7. Permission sets(권한 세트) 탭을 엽니다.
8. AWSServiceCatalogEndUserAccess선택하고 삭제합니다.

IAM 역할을 삭제하려면

1. https://console.aws.amazon.com/iam/에서 IAM 콘솔을 엽니다.
2. 왼쪽 탐색 메뉴에서 역할을 선택합니다.
3. 테이블에서 이름이 AWSControlTower있는 역할을 검색합니다.
4. 테이블의 각 역할에 대해 다음을 수행합니다.
    a. 역할에 대한 확인란을 선택합니다.
    b. 역할 삭제(Delete role)를 선택합니다.
    c. 열린 대화 상자에서 정보를 검토하여 정보가 정확한지 확인하고 예, 삭제를 선택합니다.

IAM 정책을 삭제하려면

1. https://console.aws.amazon.com/iam/에서 IAM 콘솔을 엽니다.
2. 왼쪽 탐색 메뉴에서 정책을 선택합니다.
3. 테이블에서 이름이 AWSControlTower지정된 정책을 검색합니다.
4. 테이블의 각 정책에 대해 다음을 수행합니다.
    a. 정책에 대한 확인란을 선택합니다.
    b. 드롭다운 메뉴에서 Policy actions(정책 작업) 및 삭제를 차례로 선택합니다.
    c. 열린 대화 상자에서 정보를 검토하여 정보가 정확한지 확인하고 삭제를 선택합니다.

AWS Control 타워 리소스 도움말

AWS Control Tower 리소스를 제거해도 해결할 수 없는 문제가 발생하는 경우 AWS Support에 문의하십시오.

착륙 지대를 해체하는 방법

AWS Control Tower 랜딩 존을 폐기하려면 여기에 나와 있는 절차를 따르십시오.

> **Note**
>
> 해지하기 전에 등록된 계정을 관리 취소하는 것이 좋습니다.

1. AWS Control Tower 콘솔에서 랜딩 존 설정 페이지로 이동합니다.
2. Decommission your landing zone(랜딩 영역 폐기) 섹션에서 Decommission your landing zone(랜딩 영역 폐기)을 선택합니다.
3. 필요한 확인 프로세스와 함께 수행할 작업을 설명하는 대화 상자가 나타납니다. 폐기한다는 의도를 확인하려면 모든 확인란을 선택하고 요청에 따라 확인 내용을 입력해야 합니다.

   > **Important**
   >
   > 폐기 프로세스는 실행 취소할 수 없습니다.

4. 랜딩 존을 폐기하겠다는 의사를 확인하면 서비스 해제가 진행되는 동안 AWS Control Tower 홈 페이지로 리디렉션됩니다. 폐기 프로세스는 최대 2시간이 소요될 수 있습니다.
5. 해체에 성공하면 AWS Control Tower 콘솔에서 새 랜딩 존을 설정하기 전에 남은 리소스를 수동으로 삭제해야 합니다. 이러한 나머지 리소스에는 일부 특정 Amazon S3 버킷, 조직 및 로그 CloudWatch 로그 그룹이 포함됩니다.

   > **Note**
   >
   > 이러한 조치는 청구 및 규정 준수 활동에 중대한 영향을 미칠 수 있습니다. 예를 들어 이러한 리소스를 삭제하지 않으면 예상치 못한 요금이 부과될 수 있습니다.

   리소스를 수동으로 삭제하는 방법에 대한 자세한 내용은 AWS Control Tower 리소스 제거에 대한 정보 단원을 참조하십시오.
6. 새 AWS 지역에 새 착륙 지대를 설정하려면 이 추가 단계를 따르세요. CLI를 통해 다음 명령을 입력합니다.

```
aws organizations disable-aws-service-access --service-principal
 controltower.amazonaws.com
```

해체 후 수동 정리 작업이 필요함

- 랜딩 존을 해제한 후 새 랜딩 존을 만들거나 기존 로그 아카이브 또는 감사 계정을 가져오는 절차를 따르는 경우 로그 아카이브 및 감사 계정에 대해 다른 이메일 주소를 지정해야 합니다.
- 다른 랜딩 존을 설정하기 전에 CloudWatch 로그 로그 그룹 을 수동으로 삭제해야 합니다. `aws-controltower/CloudTrailLogs`
- 로그용으로 예약된 이름을 가진 두 개의 Amazon S3 버킷을 수동으로 제거하거나 이름을 변경해야 합니다.
- 기존 보안 및 샌드박스 조직 단위를 수동으로 삭제하거나 이름을 변경해야 합니다.

> **Note**
>
> AWS Control Tower Security OU 조직을 삭제하려면 먼저 로깅 및 감사 계정을 삭제해야 하지만 관리 계정은 삭제하지 않아야 합니다. 이러한 계정을 삭제하려면 감사 계정과 로깅 계정에 루트 사용자로 로그인하는 경우하여 각 계정을 개별적으로 삭제해야 합니다.

- AWS Control Tower의 AWS IAM Identity Center (IAM ID 센터) 구성을 수동으로 삭제하고 싶을 수도 있지만 기존 IAM ID 센터 구성을 계속 진행할 수 있습니다.
- AWS Control Tower에서 생성한 VPC를 제거하고 관련 AWS CloudFormation 스택 세트를 제거할 수 있습니다.
- 새 AWS 지역에 새 착륙 지대를 설정하려면 먼저 다음 추가 단계를 따라야 합니다.
  - CLI를 통해 다음 명령을 입력합니다.

```
aws organizations disable-aws-service-access --service-principal
 controltower.amazonaws.com
```

  - 모든 관리 지역의 공유 및 멤버 계정에서 나머지 관리 규칙 (호출`AWSControlTowerManagedRule`) 을 삭제합니다. `AWSControlTowerManagedRule`아마존 EventBridge 규칙입니다.

landing Zone을 해체한 후의 설정

랜딩 영역을 폐기한 후에는 수동 정리가 완료될 때까지 설정을 다시 실행할 수 없습니다. 또한 남아 있는 리소스를 수동으로 정리하지 않으면 예기치 않은 결제 요금이 발생할 수 있습니다. 다음 사항에 유의해야 합니다.

- AWS 컨트롤 타워 관리 계정은 AWS 컨트롤 타워 루트 OU의 일부입니다. 관리 계정에서 다음과 같은 IAM 역할 및 IAM 정책이 제거되었는지 확인하십시오.
  - 역할:
    - `AWSControlTowerAdmin`
    - `AWSControlTowerCloudTrailRole`
    - `AWSControlTowerStackSetRole`
  - 정책:
    - `AWSControlTowerAdminPolicy`
    - `AWSControlTowerCloudTrailRolePolicy`
    - `AWSControlTowerStackSetRolePolicy`
- 랜딩 존을 다시 시작하기 전에 AWS Control Tower의 기존 IAM Identity Center 구성을 삭제하거나 업데이트하고 싶을 수도 있지만 반드시 삭제할 필요는 없습니다.
- AWS Control Tower에서 생성한 VPC를 제거하고 싶을 수도 있습니다.
- 로깅 또는 감사 계정에 지정된 이메일 주소가 기존 AWS 계정과 연결된 경우 설치가 실패합니다. AWS 계정을 폐쇄하거나 다른 이메일 주소를 사용하여 랜딩 존을 다시 설정할 수 있습니다. 또는 자신의 로깅 및 감사 계정을 가져올 수 있는 기능을 사용하여 기존 공유 계정을 재사용할 수도 있습니다. 자세한 정보는 기존 보안 또는 로깅 계정을 가져올 때 고려할 사항을 참조하세요.
- 다음과 같은 예약된 이름을 가진 Amazon S3 버킷이 로깅 계정에 이미 있는 경우 설치가 실패합니다.
  - `aws-controltower-logs-{accountId}-{region}`(로깅 버킷에 사용)
  - `aws-controltower-s3-access-logs-{accountId}-{region}`(로깅 액세스 버킷에 사용)

  이러한 버킷의 이름을 변경하거나 이러한 버킷을 제거하거나 로깅 계정에 다른 계정을 사용해야 합니다.

- 관리 계정에 CloudWatch Logs에 기존 로그 그룹인aws-controltower/CloudTrailLogs, 가 있는 경우 설치가 실패합니다. 로그 그룹의 이름을 변경하거나 로그 그룹을 제거해야 합니다.

새 계정을 설정하기 전 AWS 리전

새 AWS 지역에 새 착륙 지대를 설정하려면 다음 추가 단계를 따르세요.

- CLI를 통해 다음 명령을 입력합니다.

```
aws organizations disable-aws-service-access --service-principal
 controltower.amazonaws.com
```

- 모든 관리 지역의 공유 및 멤버 계정에서 나머지 관리 규칙 (이라는AWSControlTowerManagedRule) 을 삭제합니다.

> **Note**
>
> Security 또는 Sandbox라는 최상위 OU가 있는 조직에서는 새 랜딩 존을 설정할 수 없습니다. 랜딩 영역을 다시 설정하려면 이러한 OU의 이름을 바꾸거나 OU를 제거해야 합니다.

문제 해결

AWS Control Tower를 사용하는 동안 문제가 발생하는 경우 다음 정보를 사용하여 모범 사례에 따라 문제를 해결할 수 있습니다. 발생한 문제가 다음 정보의 범위를 벗어나거나 해결을 시도한 후에도 문제가 지속되면 AWS Support에 문의하십시오.

랜딩 영역 시작 실패

랜딩 영역 시작 실패의 일반적인 원인:

- 확인 이메일 메시지에 응답하지 않음
- AWS CloudFormation StackSet 실패.

확인 이메일 메시지: 관리 계정이 한 시간 미만인 경우 추가 계정을 만들 때 문제가 발생할 수 있습니다.

취할 조치

이 문제가 발생하는 경우 이메일을 확인하십시오. 응답을 대기하는 확인 이메일이 전송되었을 수 있습니다. 또는 한 시간 정도 기다렸다가 다시 시도하는 것이 좋습니다. 문제가 지속되면 AWS Support에 문의하세요.

실패 StackSets: landing Zone 시작 실패의 또 다른 가능한 원인은 AWS CloudFormation StackSet 실패입니다. AWS 프로비저닝이 성공하려면 AWS Control Tower가 관리하는 모든 AWS 지역의 관리 계정에서 보안 토큰 서비스 (STS) 지역을 활성화해야 합니다. 그렇지 않으면 스택 세트를 시작할 수 없습니다.

취할 조치

AWS Control Tower를 시작하기 전에 필요한 AWS 보안 토큰 서비스 (STS) 엔드포인트 지역을 모두 활성화해야 합니다.

AWS Control AWS 리전 Tower가 지원하는 목록을 보려면 을 참조하십시오AWS 지역별로 AWS Control Tower를 활용하는 방법.

랜딩 존이 최신 상태가 아님 오류

최근에 랜딩 존을 업데이트하지 않은 경우, AWS Control Tower에 다시 액세스하려고 할 때 오류가 발생할 수 있습니다. 다음과 비슷한 오류 메시지가 표시될 수 있습니다.

`Unable to access Control Tower`

계정이 너무 오랫동안 비활성 상태였습니다. 비활성 상태이므로 AWS Control Tower에 액세스하려면 랜딩 존을 업데이트해야 합니다.

하지만, Landing Zone 업데이트가 실패할 수 있습니다.

취해야 할 조치

조직의 관리 계정에 로그인하고 루트 사용자로 로그인합니다. IAM 사용자 또는 IAM ID 센터의 사용자는 AWS Control Tower 관리자 권한을 가지고 있어야 하며 그룹에 속해야 합니다. AWSControlTowerAdmins 그런 다음 업데이트를 다시 시도해 보십시오.

새 계정 프로비저닝 실패

이 문제가 발생하면 이러한 일반적인 원인을 확인하십시오.

계정 프로비저닝 양식을 작성할 때 다음과 같은 내용이 있을 수 있습니다.

- 지정된 tagOptions
- 활성화된 SNS 알림
- 활성화된 프로비저닝된 제품 알림

이러한 옵션을 지정하지 않고 다시 계정을 프로비저닝합니다. 자세한 정보는 Account Factory를 통한 AWS Service Catalog 계정 프로비저닝 을 참조하세요.

실패의 다른 일반적인 원인:

- 리소스 변경 내용을 보기 위해 프로비저닝된 제품 계획을 만든 경우 계정 프로비저닝이 계속 진행 중 상태로 유지될 수 있습니다.
- 다른 AWS Control Tower 구성 변경이 진행 중인 동안에는 Account Factory에서 새 계정을 생성할 수 없습니다. 예를 들어 OU에 컨트롤을 추가하는 프로세스를 실행하는 동안 계정을 프로비저닝하려고 하면 Account Factory에 오류 메시지가 표시됩니다.

AWS Control Tower에서 이전 작업의 상태를 확인하려면

- AWS CloudFormation >로 이동합니다. StackSets
- AWS Control Tower (접두사: "AWSControlTower“) 와 관련된 각 스택 세트를 확인합니다.
- 아직 실행 중인 AWS CloudFormation StackSets 작업을 찾아보십시오.

계정 프로비저닝이 1시간 이상 걸리는 경우 프로비저닝 프로세스를 종료하고 다시 시도하는 것이 좋습니다.

기존 계정 등록 실패

기존 AWS 계정을 등록하려고 한 번 시도했지만 등록이 실패하는 경우 두 번째로 시도하면 스택 세트가 존재한다는 오류 메시지가 표시될 수 있습니다. 계속하려면 Account Factory에서 프로비저닝된 제품을 제거해야 합니다.

첫 번째 등록 실패의 이유가 계정에서 `AWSControlTowerExecution` 역할을 미리 생성하지 않았기 때문인 경우, 오류 메시지에 이 역할을 생성하라는 메시지가 표시됩니다. 그러나 이 역할을 생성하려고 하면 AWS Control Tower에서 역할을 생성할 수 없다는 또 다른 오류 메시지가 나타날 수 있습니다. 이 오류는 프로세스가 부분적으로 완료되었기 때문에 발생합니다.

이 경우 기존 계정 등록을 진행하기 전에 두 가지 복구 단계를 수행해야 합니다. 먼저 콘솔을 통해 Account Factory가 제공하는 제품을 종료해야 합니다 AWS Service Catalog . 그런 다음 AWS Organizations 콘솔을 사용하여 계정을 OU 밖으로 수동으로 이동하고 루트로 다시 이동해야 합니다. 이 작업이 완료되면 계정에서 `AWSControlTowerExecution` 역할을 생성한 다음 계정 등록 양식을 다시 작성합니다.

등록 실패의 또 다른 가능한 원인은 계정에 기존 Config AWS 리소스가 있기 때문입니다. 이 경우 기존 리소스를 수정하는 방법에 대한 지침은 기존 AWS Config 리소스가 있는 계정 등록을 참조하세요.

Account Factory 계정을 업데이트할 수 없음

계정이 일관되지 않은 상태인 경우 Account Factory 또는 AWS Service Catalog에서 성공적으로 업데이트할 수 없습니다.

사례 1: 다음과 비슷한 오류 메시지가 표시될 수 있습니다.

```
AWS Control Tower could not baseline VPC in the managed account because of existing resource dependencies.
```

일반적인 원인: AWS Control Tower는 초기 프로비저닝 중에 항상 AWS 기본 VPC를 제거합니다. 계정에 AWS 기본 VPC를 사용하려면 계정 생성 후 기본 VPC를 추가해야 합니다. 실제 설명과 같이 Account Factory를 설정하지 않는 한, AWS Control Tower에는 기본 AWS VPC를 대체하는 자체 기본 VPC가 있습니다. 따라서 AWS Control Tower는 VPC를 전혀 프로비저닝하지 않습니다. 따라서 계정에 VPC가 없게 됩니다. 기본 VPC를 사용하려면 AWS 기본 VPC를 다시 추가해야 합니다.

하지만 AWS Control Tower는 AWS 기본 VPC를 지원하지 않습니다. 계정을 배포하면 계정이 상태로 전환됩니다. `Tainted` 해당 상태에서는 계정을 업데이트할 수 없습니다. AWS Service Catalog

취할 조치: 추가한 기본 VPC를 삭제해야 합니다. 그러면 계정을 업데이트할 수 있습니다.

> **Note**
>
> `Tainted`상태로 인해 다음과 같은 문제가 발생합니다. 계정이 업데이트되지 않으면 계정이 속한 OU에서 제어를 활성화하지 못할 수 있습니다.

사례 2: 다음과 비슷한 오류 메시지가 표시될 수 있습니다.

```
AWS Control Tower detects that your enrolled account has been moved to a
new organizational unit.
```

일반적인 원인: 등록된 OU에서 다른 OU로 계정을 이동하려고 했지만 이전 AWS Config 규칙은 그대로 남아 있습니다. 계정이 일관되지 않은 상태입니다.

취해야 할 조치:

계정 이동이 의도된 경우:

- Service Catalog에서 계정을 종료합니다.
- 다시 등록하세요.
- 컨텍스트/영향: 배포된 AWS Config 규칙이 대상 OU에서 지정한 구성과 일치하지 않습니다.
- AWS Config 규칙이 이전 OU에 그대로 남아 있어 의도하지 않은 지출이 발생할 수 있습니다.
- 계정을 재등록하거나 업데이트하려는 시도는 리소스 이름 충돌로 인해 실패합니다.

의도하지 않은 계정 이동인 경우:

- 계정을 원래 OU로 되돌립니다.
- Service Catalog에서 계정을 업데이트합니다.
- 시작 매개 변수에 해당 계정이 원래 속했던 OU를 입력합니다.
- 컨텍스트/영향: 계정을 원래 OU로 되돌리지 않으면 계정 상태가 새 OU에서 지정하는 컨트롤과 일치하지 않게 됩니다.
- 계정 업데이트는 이전 OU와 관련된 규칙을 삭제하지 않으므로 유효한 수정 방법이 아닙니다. AWS Config

랜딩 존을 업데이트할 수 없습니다.

AWS Control Tower는 업데이트가 실패할 경우 이전 랜딩 존 버전으로 롤백하지 않습니다. 착륙 지대가 불확실한 상태일 수 있습니다. 그렇다면 지원팀에 문의하세요 AWS .

랜딩 존 업데이트는 여러 가지 이유로 실패할 수 있습니다.

- 사전 요구 사항이 충족되지 않음
- AWS Config 특정 계정에 리소스가 있습니다.
- 폐쇄된 계정이 존재합니다.

사전 요구 사항이 충족되지 않음

랜딩 존 업데이트는 랜딩 존 설정과 동일한 사전 요구 사항을 충족해야 합니다. 업데이트하기 전에 사전 출시 검사를 검토하세요.

AWS Config 보안 OU 계정에 리소스가 있습니다.

감사 및 로그 아카이브 계정에는 AWS Config 리소스를 추가하지 마십시오. 이러한 리소스가 있는 상태에서는 Landing Zone 업데이트 프로세스를 완료할 수 없습니다. 이러한 제한은 계정을 등록하거나 처음으로 landing Zone을 설정하는 경우와 유사합니다. 자세한 내용은 기존 AWS Config 리소스가 있는 계정 등록을 참조하십시오.

폐쇄된 계정이 존재합니다.

계정이 폐쇄됨 또는 일시 중단된 상태인 경우, landing Zone을 업데이트하려고 할 때 문제가 발생할 수 있습니다. Landing Zone을 업데이트하기 전에 폐쇄된 모든 계정에서 프로비저닝된 제품을 삭제해야 합니다.

AWS Service Catalog 프로비저닝된 제품 페이지에서 다음과 유사한 오류 메시지가 표시될 수 있습니다.

```
AWSControlTowerExecution role can't be assumed on the account.
```

일반적인 원인: 프로비저닝된 제품을 삭제하지 않고 계정을 일시 중지했습니다.

취해야 할 조치: 이 오류가 표시되는 경우 다음 두 가지 옵션이 있습니다.

1. AWS Support에 문의하여 계정을 다시 열고 프로비저닝된 제품을 삭제한 다음 계정을 다시 닫으십시오.

2. 계정 폐쇄로 인해 연결이 끊긴 리소스를 에서 제거하십시오. StackSets (이 옵션은 현재 상태의 인스턴스 중 제거하지 않을 인스턴스가 StackSets 있는 경우에만 사용할 수 있습니다.)

에서 리소스를 제거하려면 폐쇄된 StackSets 각 계정에 대해 다음과 같이 하십시오.

- 각 AWS Control StackSets Tower로 이동하여 모든 지역에서 폐쇄된 계정의 계정을 제거하십시오. StackInstances
- 중요: Retain Stack 옵션을 선택하면 스택 인스턴스만 StackSet 제거됩니다. StackSet 폐쇄된 계정에서는 역할을 수임할 수 없으므로 `AWSControlTowerExecution` 역할을 맡으려고 하면 실패하고, 이로 인해 오류 메시지가 표시됩니다.

다음과 같은 실패 오류가 발생했습니다. AWS Config

AWS Config 가 AWS Control Tower에서 지원하는 모든 AWS 지역에서 활성화된 경우 사전 확인이 실패했기 때문에 오류 메시지가 표시될 수 있습니다. 의 일부 기본 동작으로 인해 메시지가 문제를 적절하게 설명하지 못하는 것처럼 보일 수 있습니다. AWS Config

다음 중 하나와 유사한 오류 메시지가 나타날 수 있습니다.

- `AWS Control Tower cannot create an AWS Config delivery channel because one already exists. To continue, delete the existing delivery channel and try again .`
- `AWS Control Tower cannot create an AWS Config configuration recorder because one already exists. To continue, delete the existing delivery channel and try again .`

일반적인 원인: AWS 계정에서 AWS Config 서비스를 사용하도록 설정하면 기본 이름을 사용하여 구성 레코더와 전송 채널이 만들어집니다. 콘솔을 통해 AWS Config 서비스를 비활성화하면 컨피그레이션 레코더 또는 전송 채널이 삭제되지 않습니다. CLI를 통해 삭제하거나 AWS Control Tower에서 사용할 수 있도록 수정해야 합니다. AWS Control Tower가 지원하는 지역 중 하나에서 AWS Config 서비스를 활성화하면 이 오류가 발생할 수 있습니다.

계정에 기존 AWS Config 리소스가 있는 경우 기존 리소스를 수정하는 방법에 대한 지침은 기존 AWS Config 리소스가 있는 계정 등록을 참조하세요.

취할 조치: 지원되는 모든 리전에서 구성 레코더 및 전송 채널을 삭제합니다. AWS Config를 비활성화하는 것만으로는 충분하지 않습니다. CLI를 통해 컨피그레이션 레코더와 전송 채널을 삭제해야 합니다. CLI에서 구성 레코더 및 전송 채널을 삭제한 후 다시 AWS Control Tower를 시작하고 계정을 등록해 볼 수 있습니다.

프로비저닝된 제품을 배포하는 중이라면 재시도하기 전에 프로비저닝된 제품을 삭제해야 합니다. 그렇지 않으면 다음과 비슷한 오류 메시지가 표시될 수 있습니다.

- `An error occurred (InvalidParametersException) when calling the ProvisionProduct operation: A stack named Stackname already exists.`

메시지에서 스택의 이름을 *Stackname*지정합니다.

다음은 컨피그레이션 레코더 및 전송 채널의 상태를 확인하는 데 사용할 수 있는 몇 가지 예제 AWS Config CLI 명령입니다.

보기 명령:

- `aws configservice describe-delivery-channels`
- `aws configservice describe-delivery-channel-status`
- `aws configservice describe-configuration-recorders`
- `The normal response is something like "name": "default"`

삭제 명령:

- `aws configservice stop-configuration-recorder --configuration-recorder-name NAME-FROM-DESCRIBE-OUTPUT`
- `aws configservice delete-delivery-channel --delivery-channel-name NAME-FROM-DESCRIBE-OUTPUT`
- `aws configservice delete-configuration-recorder --configuration-recorder-name NAME-FROM-DESCRIBE-OUTPUT`

자세한 내용은 설명서를 참조하십시오. AWS Config

- 구성 레코더 (AWS CLI) 관리
- 전송 채널 관리

시작 경로를 찾을 수 없음 오류

새 계정을 생성하려고 할 때 다음과 유사한 오류 메시지가 나타날 수 있습니다.

```
No launch paths found for resource: prod-dpqqfywxxxx
```

이 오류 메시지는 AWS Control Tower에서 계정을 프로비저닝하는 데 도움이 되는 통합 서비스인 에서 생성됩니다. AWS Service Catalog

일반적인 원인:

- 루트로 로그인했을 수 있습니다. AWS Control Tower는 루트 사용자로 로그인한 경우 계정 생성을 지원하지 않습니다.
- IAM Identity Center 사용자가 적절한 권한 그룹에 추가되지 않았습니다. IAM Identity Center 사용자를 다음 권한 그룹 (최종 사용자 액세스용) 또는 AWSAccountFactoryAWSServiceCatalogAdmins(관리자 액세스용) 중 하나에 추가해야 할 수 있습니다.
- IAM 사용자로 인증된 경우 올바른 권한을 갖도록 AWS Service Catalog 포트폴리오에 추가해야 합니다.
- 이 문제는 올바른 권한을 가지고 있지만 AWS Control Tower 드리프트가 감지되어 드리프트 복구가 필요한 경우에도 발생합니다. 대부분의 유형의 드리프트를 복구하려면 랜딩 존 설정 페이지에서 Reset을 선택하십시오.

권한 부족 오류를 수신했습니다.

계정에 특정 작업을 수행하는 데 필요한 권한이 없을 수 있습니다. AWS Organizations다음과 같은 유형의 오류가 발생하는 경우 IAM 또는 IAM Identity Center 권한과 같은 모든 권한 영역을 확인하여 해당 위치에서 권한이 거부되지 않았는지 확인하십시오.

```
You have insufficient permissions to perform AWS Organizations API actions.
```

작업에 시도하려는 조치가 필요하다고 생각되지만 관련 제한 사항을 찾을 수 없는 경우 시스템 관리자 또는 AWS Support에 문의하세요.

Detective 컨트롤은 계정에 적용되지 않습니다

최근에 AWS Control Tower 배포를 새 AWS 지역으로 확장한 경우, AWS Control Tower가 관리하는 OU 내의 개별 계정이 업데이트되기 전까지는 어떤 지역에서든 새로 생성한 계정에 새로 적용된 탐지 제어 항목이 적용되지 않습니다. 기존 계정에 대한 기존 탐지 제어는 여전히 유효합니다.

계정을 업데이트하기 전에 탐지 제어를 활성화하려고 하면 다음과 비슷한 오류 메시지가 표시될 수 있습니다.

```
AWS Control Tower can't enable the selected control on this OU. AWS Control Tower cannot apply the control on the OU ou-xxx-xxxxxxxx, because child accounts have dependencies that are missing. Update all child accounts under the OU, then try again.
```

취할 조치: 계정 업데이트.

AWS Control Tower 콘솔에서 계정을 업데이트하려면 을 참조하십시오AWS 컨트롤 타워 OU 및 계정 업데이트 시기.

프로그래밍 방식으로 여러 개별 계정을 업데이트하려면 의 AWS Service Catalog API와 AWS CLI를 사용하여 업데이트를 자동화할 수 있습니다. 이 업데이트 프로세스 방법에 대한 자세한 내용은 이 비디오 안내을 참조하십시오. 동영상에 표시된 UpdateProvisionedProductAPI를 API로 ProvisionProduct대체할 수 있습니다.

계정에서 탐지 제어를 활성화하는 데 문제가 더 있는 경우 AWS Support에 문의하세요.

API에서 속도 초과 오류가 반환되었습니다. AWS Organizations

가능한 원인

AWS Control Tower가 SCP의 드리프트 여부를 확인하기 위해 일일 스캔을 실행하는 동안 워크로드가 실행되고 있었습니다.

따라야 할 단계

API 스로틀링 또는 `rate exceeded` 오류가 발생하는 경우 다음 단계를 시도해 보세요.

- 워크로드를 다른 시간에 실행하세요. (AWS Control Tower에서 감사 스캔을 실행하는 시기를 알아보려면 지역별 AWS Control Tower SCP 불변량 스캔 일정을 참조하십시오.)
- HTTP를 통해 API를 직접 호출하는 경우: 실패한 작업을 자동으로 재시도하는 AWS SDK를 사용하십시오.
- Service AWS Quotas 및 Support를 통해 한도 증가를 요청하십시오.

Elastic Beanstalk의 API 스로틀링에 대한 문제 해결 지침의 예는 다음에서 찾을 수 있습니다. `https://aws.amazon.com/premiumsupport/knowledge-center/elastic-beanstalk-api-throttling-errors/`

Account Factory 계정을 한 AWS 컨트롤 타워 랜딩 존에서 다른 AWS 컨트롤 타워 랜딩 존으로 직접 이전하지 못함

> **Warning**
>
> 적격 계정은 동일한 전체 AWS 조직에 속해야 하고 각 조직에는 하나의 랜딩 존만 있을 수 있기 때문에 이 방법은 적격 계정 등록의 전제 조건을 충족하지 않습니다. 이 작업을 시도했지만 오류 메시지가 여러 번 표시되는 경우 도움이 될 수 있는 몇 가지 정보가 있습니다.

Account Factory를 통해 프로비저닝한 계정을 다른 관리 계정 아래의 AWS Control Tower에서 관리하는 다른 랜딩 존으로 이동하려면 원래 OU에서 해당 계정과 관련된 모든 IAM 역할 및 스택을 제거해야 합니다. 계정이 배포된 모든 지역에서 이러한 리소스를 제거하십시오.

> **Note**
>
> 리소스를 제거하는 가장 좋은 방법은 계정을 이동하기 전에 원래 OU에서 계정 프로비저닝을 해제하는 것입니다.

리소스를 제거하지 않으면 새 OU에 등록이 실패하는 경우가 종종 있습니다. 하나 이상의 오류 메시지가 발생할 수 있으며, 계정이 배포된 모든 지역에서 나머지 역할 및 스택이 제거될 때까지 비슷한 오류 메시지가 계속 표시됩니다.

오류 메시지를 받을 때마다 새 OU에서 계정을 제거하고 오류 메시지의 대상인 이전 리소스를 삭제한 다음 계정을 새 OU로 다시 이동해 봐야 합니다. 남아 있는 모든 리소스, 즉 계정이 배포된 모든 지역에 대해 이 프로세스를 10~20회 정도 removing-and-deleting 반복해야 합니다. 이러한 오류가 반복해서 발생하는 이유는 IAM 역할 삭제를 방지하는 SCP가 있는 OU에 계정이 프로비저닝되었기 때문입니다. 재시도하기 전에 계정의 리소스를 모두 삭제하여 복구 프로세스를 더 짧게 만들 수 있습니다.

아래 예는 삭제되지 않은 역할 및 스택이 남아 있는 경우 받을 수 있는 실패 메시지 유형을 나타냅니다. 오래된 리소스가 남아 있는 한, 계정을 등록하려고 할 때마다 이러한 메시지가 한 번에 하나씩 표시될 가능성이 큽니다.

예제의 리소스 ID 문자열 값이 수정되었습니다. 오류 메시지가 표시될 경우 해당 값이 동일하지 않을 수 있습니다. 다음 예와 비슷한 메시지가 표시될 수 있습니다.

- AWS Control Tower cannot create the IAM role *aws-controltower-AdministratorExecutionRole* because the role already exists. To continue, delete the existing IAM role and try again.
- AWS Control Tower cannot create the IAM role *aws-controltower-ConfigRecorderRole* because the role already exists. To continue, delete the existing IAM role and try again.
- AWS Control Tower cannot create the IAM role *aws-controltower-ForwardSnsNotificationRole* because the role already exists. To continue, delete the existing IAM role and try again.

또는 다음과 비슷한 스택 세트 실패에 대한 오류 메시지가 표시될 수 있습니다.

```
"Error\":\"StackSetFailState\",
\"Cause\":\"StackSetOperation on AWSControlTowerBP-BASELINE-CLOUDWATCH
with id 8aXXXXf5-e0XX-4XXa-bc4XX-dXXXXXee31
has reached SUCCEEDED state but has 1 NON-CURRENT stack instances;
here is the summary :{ StackSet Id:
AWSControlTowerBP-BASELINE-CLOUDWATCH:40XXXbf2-Xead-46a1-XXXa-eXXXXecb2ee2,
Stack instance Id:
arn:aws:cloudformation:eu-west-1:1X23456789XX:
            stack/StackSet-AWSControlTowerBP-BASELINE-CLOUDWATCH-4feXXXXXX-ecXX-XXc6-
bXXX-4ae678/4feXXXXXX-ecX-4ae123458,
Status: OUTDATED,
Status Reason: ResourceLogicalId:ForwardSnsNotification,
ResourceType:AWS::Lambda::Function,
ResourceStatusReason:aws-controltower-NotificationForwarder already exists in stack
arn:aws:cloudformation:eu-west-1:1X23456789XX:
            stack/StackSet-AWSControlTowerBP-BASELINE-CLOUDWATCH-4feXXXXXX-ecXX-XXc6-
bXXX-4ae678/4feXXXXXX-ecX-4ae123458.
```

첫 번째 OU에서 나머지 리소스가 모두 제거되면 계정을 새 OU에 성공적으로 초대, 프로비저닝 또는 등록할 수 있습니다.

AWS Support

기존 구성원 계정을 다른 지원 플랜으로 이동하려는 경우 루트 계정 자격 증명으로 각 계정에 로그인하고, 플랜을 비교하고, 원하는 지원 수준을 설정할 수 있습니다.

지원 플랜을 변경할 때는 MFA 및 계정 보안 연락처를 업데이트하는 것이 좋습니다.

베이스라인 유형

AWS Control Tower의 기준은 대상에 적용할 수 있는 리소스 및 특정 구성 그룹입니다. 가장 일반적인 기준 대상은 조직 단위 (OU) 일 수 있습니다. 예를 들어 OU를 대상으로 선택한 베이스라인을 활성화하여 해당 OU를 AWS Control Tower에 등록할 수 있습니다.

랜딩 존 설정 시 기준 타겟은 공유 계정 또는 랜딩 존 전체가 될 수 있습니다. 특정 베이스라인은 사용자의 landing zone 설정 및 구성에 따라 활성화 및 업데이트될 수 있습니다. AWS Control Tower는 베이스라인에서 지정하는 방식으로 리소스를 생성하여 대상에 배포합니다.

대상에 대한 베이스라인을 활성화하면 베이스라인은 리소스라고 하는 AWS CloudFormation 리소스로 표시됩니다. `EnabledBaseline`

AWS Control Tower에는 네 가지 필수 유형의 기준이 있습니다.

- 한 가지 유형은 AWS Control Tower에 등록된 OU 또는 기준을 적용하여 등록하려는 OU에 적용할 수 있습니다.
- 초기 설정 또는 랜딩 존 업데이트 중에 Landing Zone 또는 공유 계정에 세 가지 기본 유형을 적용할 수 있습니다.

OU 등록 및 업데이트를 위해 OU 수준에서 적용되는 기준 유형

- 이름: `AWSControlTowerBaseline`

  설명: AWS Control Tower 거버넌스에 필요한 대상 OU 내 멤버 계정에 대한 리소스 및 필수 제어를 설정합니다.

  고려 사항: 이 베이스라인은 landing zone 지역 거부 제어의 설정을 유지합니다. 즉, 랜딩 영역 수준에서 지역이 허용되지 않는 경우 `EnableBaseline` API를 호출하여 OU를 등록할 때 해당 지역은 해당 OU에 허용되지 않습니다.

  > **Note**
  >
  > OU 수준 지역 거부 제어는 landding zone 지역 거부 제어에서 허용하지 않는 지역을 허용할 방법이 없습니다.

  자세한 내용은 문서의 SCP가 거부를 처리하는 방법을 참조하십시오. AWS Organizations

권장 사항: OU용 `EnableBaseline` API를 호출하기 전에 대상 OU에서 워크로드를 실행할 수 있는 지역을 확인하고, 랜딩 존 지역 거부 제어와 비교하여 결과를 확인하는 것이 좋습니다. 그렇지 않으면 특정 지역의 리소스에 액세스할 수 없게 될 수 있습니다.

> **Note**
>
> 랜딩 존 기준선은 OU 수준 기준선과 다르게 작동합니다.

AWS Control Tower는 랜딩 존 설정 및 업데이트 프로세스의 일환으로 랜딩 존 수준에서 자동으로 적용되는 기준을 활성화합니다. 랜딩 존 설정을 변경하면 랜딩 존의 베이스라인이 변경될 수 있습니다. 예를 들어, IAM Identity Center를 옵트인하면 AWS Control Tower는 랜딩 존에서 `IdentityCenterBaseline` 베이스라인의 최신 버전을 활성화할 수 있습니다.

`ListEnabledBaselines`API 호출을 통해 landing zone에 대해 활성화된 베이스라인을 볼 수 있습니다.

Landing Zone 또는 공유 계정에 적용할 수 있는 기준 유형

- 이름: `AuditBaseline`

  설명: 조직 내 계정의 보안 및 규정 준수를 모니터링하기 위한 리소스를 설정합니다. 이 기준은 AWS Control Tower에서 배포하므로 변경할 수 없습니다.

- 이름: `LogArchiveBaseline`

  설명: 조직 내 계정의 API 활동 및 리소스 구성 로그를 저장할 중앙 리포지토리를 설정합니다. 이 기준은 AWS Control Tower에서 배포하므로 변경할 수 없습니다.

- 이름: `IdentityCenterBaseline`

  설명: IAM Identity Center의 공유 리소스를 설정하여 계정에 대한 ID 센터 `AWSControlTowerBaseline` 액세스를 설정할 수 있도록 준비합니다.

  고려 사항: 이 기준은 처음 랜딩 존을 설정할 때 IAM Identity Center를 ID 공급자로 선택한 경우 또는 이후에 랜딩 존에 IAM Identity Center를 활성화하도록 랜딩 존 설정을 변경하는 경우에만 유효합니다. 다른 ID 공급자를 사용하는 경우 이 기준을 활성화할 수 있는 액세스 권한이 없습니다.

계정의 부분 등록

베이스라인에 따라 작업할 때는 계정을 부분 등록이라는 상태로 만들 수 있습니다.

AWS Control Tower는 대상 OU의 계정에 필수 리소스만 적용하기 때문에 `ResetEnabledBaseline` API를 호출하여 OU를 재등록하는 경우 이 상태가 발생할 수 있습니다. 상위 OU의 선택적 리소스 (컨트롤) 가 누락된 계정은 부분 등록으로 표시됩니다.

등록되지 않은 계정을 등록된 OU로 이동한 다음 OU의 `ResetEnabledBaseline` API를 호출하여 해당 계정을 등록하면, AWS Control Tower는 계정과 연결된 리소스를 새로 등록된 계정에 적용합니다. `AWSControlTowerBaseline` 하지만 이 OU에 대해 활성화된 선택적 컨트롤은 계정에 적용되지 않습니다. 계정은 부분 등록 상태로 유지됩니다.

계정을 완전히 등록하려면 콘솔에서 계정 재등록 또는 업데이트를 선택합니다. 콘솔에서 이러한 작업을 선택하면 AWS Control Tower는 해당 OU에 대해 활성화된 선택적 제어를 포함하여 해당 OU의 모든 리소스를 새로 등록한 계정에 적용합니다.

AWS Control Tower 콘솔과 기준 API 간의 운영 차이

OU의 거버넌스 상태를 변경하면 기준선 API를 통해 거버넌스를 변경하는 것에 비해 AWS Control Tower 콘솔이 자동으로 더 많은 작업을 수행합니다.

차이

- 제품 등록 및 프로비저닝

  콘솔을 통해 OU를 등록하면 AWS Control Tower는 각 계정 등록의 일환으로 OU 멤버 계정에 대한 Service Catalog 제품을 생성합니다. `EnableBaseline`API와 를 사용하여 OU를 등록하는 경우`AWSControlTowerBaseline`, AWS Control Tower는 OU의 멤버 계정에 대해 프로비저닝된 제품을 생성하지 않습니다.
- OU 등록 취소

  OU 등록을 취소할 때마다 먼저 모든 구성원 계정과 중첩된 OU를 제거해야 합니다. 그러면 AWS Control Tower는 OU에 적용되는 모든 제어를 제거합니다.
  - 콘솔에서 OU 삭제를 선택하면 AWS Control Tower가 등록을 취소한 다음 조직에서 OU를 삭제합니다.
  - 하지만 `DisableBaseline` API를 호출하여 OU를 `AWSControlTowerBaseline` OU에서 제거하여 OU를 등록 취소하는 경우, AWS Control Tower는 조직에서 OU를 삭제하지 않으며, OU는 여전히 조직에 존재하며 등록되지 않은 상태로 남아 있습니다.

기준 및 버전 관리 기본값

AWS Control Tower 랜딩 존이 이미 설정되어 있고 랜딩 존 베이스라인을 활성화하기로 선택한 경우, AWS Control Tower는 랜딩 존 버전과 호환되는 최신 버전의 베이스라인을 활성화합니다. AWS Control Tower에 아직 등록되지 않은 OU에 베이스라인을 활성화하기로 선택한 경우, AWS Control Tower는 해당 OU에 호환되는 최신 버전의 베이스라인을 자동으로 제공합니다.

OU 기준 및 랜딩 존 버전의 호환성

AWS Control Tower 기준을 사용하면 비즈니스에 필요한 경우 랜딩 존 수준이 아닌 OU 수준에서 거버넌스 표준을 설정할 수 있습니다. `AWSControlTowerBaseline`라는 기준을 사용하여 OU를 AWS Control Tower에 등록하는 데 도움이 됩니다.

> **Note**
>
> 기준선은 랜딩 존 내에 안정적인 거버넌스 환경을 구축하기 위해 함께 작동하는 제어 및 리소스 그룹입니다.

OU에 베이스라인을 활성화하려면 AWS Control Tower에서 `EnableBaseline` API를 호출하여 현재 AWS Control Tower 랜딩 존 버전과 호환되는 기준 버전을 지정해야 합니다. 기준을 지정한 후에는 OU의 모든 구성원 계정이 OU에 대해 지정된 기준을 따릅니다. 즉, 새 계정에는 업데이트된 기준선이 제공되고 기존 구성원 계정은 새 기준선에 따라 관리됩니다.

기존 OU 및 계정에 대한 기준을 선택하지 않은 경우 기본적으로 landing Zone 버전에 따라 전체 거버넌스 상태가 결정됩니다. 하지만 랜딩 존에 등록된 각 OU에는 기본 버전이 할당되며, 이는 현재 랜딩 존 버전과 호환되는 최신 베이스라인입니다. 따라서 기준선을 구체적으로 할당하지 않았더라도 각 OU와 등록된 구성원 계정에는 관련 기준선이 있습니다.

OU 수준 기준의 경우 다음 표는 기준선과 AWS Control Tower 랜딩 존 버전의 호환성을 보여줍니다. `AWSControlTowerBaseline`

베이스라인 버전	랜딩 존 버전	포함된 청사진	포함된 컨트롤	이전 베이스라인과의 변경	
1.0	2.0에서 2.7로	BP_베이스라인_클라우드	모든 필수 제어	None	

베이스라인 버전	랜딩 존 버전	포함된 청사진	포함된 컨트롤	이전 베이스라인과의 변경	
		트레일, BP_베이스라인_클라우드워치, BP_베이스라인_구성, BP_베이스라인_역할, BP_베이스라인_서비스_역할, IAM 리소스			
2.0	2.8 - 2.9	BP_BASELINE_CLOUDTRAIL, BP_BASELINE_CLOUDWATCH, BP_베이스라인_구성, BP_베이스라인_역할, BP_BASELINE_SERVICE_ROLES, 구성 SLR, IAM 리소스	모든 필수 제어	SLR을 AWS Config 사용하기 위한 서비스 연결 역할(SLR) 및 새로운 Config 블루프린트가 추가되었습니다.	

베이스라인 버전	랜딩 존 버전	포함된 청사진	포함된 컨트롤	이전 베이스라인과의 변경	
3.0	3.0에서 3.1까지	BP_BASELINE_CLOUDWATCH, BP_베이스라인_구성, BP_베이스라인_역할, BP_BASELINE_SERVICE_ROLES, 구성 SLR, IAM 리소스	모든 필수 제어	새 AWS Config 청사진. 글로벌 리소스를 홈 지역에만 기록하도록 변경하십시오. CloudTrail 블루프린트가 삭제되었습니다.	
4.0	3.2에서 3.3까지	BP_BASELINE_CLOUDWATCH, BP_BASELINE_CONFIG, BP_BASELINE_SERVICE_ROLE, BP_BASELINE_SERVICE_ROLE, 구성 SLR, IAM 리소스	모든 필수 제어	새로운 SLR 블루프린트	

landing Zone을 설정할 때 계정에서 생성되는 특정 리소스에 대한 자세한 내용은 공유 계정에서 생성되는 리소스를 참조하십시오.

새로운 기본 버전을 지원하는 버전으로 랜딩 존을 업데이트하고 새 랜딩 존 버전이 기존 **AWSControlTowerBaseline** 기본 버전과 호환되는 경우 OU 상태가 업데이트 가능으로 변경됩니다.

- 2.x에서 3.x로 landing Zone을 업데이트하는 경우를 제외하고 OU 기준을 즉시 업데이트하지 않고도 어카운트 팩토리 및 기타 기능을 계속 사용할 수 있습니다.
- 이 OU에 등록된 새 계정은 기본 버전이 업데이트될 때까지 (콘솔의 관리 확장 기능 또는 API를 통해) 기존 기준 버전을 기반으로 리소스를 받습니다. `UpdateEnabledBaseline`
- 기본 버전을 업데이트하면 해당 OU 내의 모든 계정에 새 기본 버전에 기반한 리소스가 제공됩니다.

> **Note**
>
> AWS Control Tower 랜딩 존을 버전 2.X에서 원하는 버전 3.X로 업데이트하는 경우, 계정 수준에서 조직 수준 트레일로 변경되었으므로 OU의 기본 버전도 업데이트해야 합니다. AWS CloudTrail 콘솔에서 OU에는 업데이트 필요 상태가 표시됩니다.

기준 고려 사항

- OU에 기본 업데이트가 필요한 경우 새 계정을 프로비전하거나 기존 계정을 해당 OU에 등록할 수 없습니다.
- Landing Zone 업데이트 후 OU 기준선도 업데이트하려는 경우 OU를 다시 등록하거나 프로그래밍 방식으로 OU 기준 버전을 업데이트해야 합니다.
- 사용 중인 랜딩 존 버전에서 호환되는 가장 높은 베이스라인으로 업데이트하여 랜딩 존과 베이스라인을 결합하여 제공하는 모든 이점을 얻을 수 있도록 하는 것이 좋습니다. 예를 들어, landing zone 버전 3.3으로 업데이트하면 기본 3.0을 계속 사용할 수 있지만 기본 4.0으로 업데이트하지 않는 한 landing Zone 버전 3.3의 모든 이점을 얻을 수는 없습니다.
- 베이스라인 업데이트는 롤백할 수 없습니다.
- 기본 활성화는 한 번에 하나의 OU를 대상으로 합니다. 따라서 부모 OU가 업데이트될 때 중첩된 OU는 자동으로 업데이트되지 않습니다. 중첩된 OU를 업데이트하기 전에 상위 OU를 업데이트하는 것이 좋습니다.
- `UpdateEnabledBaseline`API를 호출하거나 콘솔에서 OU를 재등록하는 경우 OU는 기본 업데이트 이전에 활성화된 모든 컨트롤을 유지합니다.
- 여러 베이스라인 버전이 랜딩 존 버전과 호환되는 경우, 관리되지 않는 OU에서 베이스라인을 활성화하는 경우 최신 베이스라인 버전을 사용해야 합니다.

예: API로만 AWS 컨트롤 타워 OU 등록

이 예제 안내는 첨부 문서입니다. 설명, 주의 사항 및 자세한 내용은 을 참조하십시오. 베이스라인 유형

사전 조건

AWS Control Tower에 등록되지 않은 기존 OU가 있고 등록하려는 OU가 있어야 합니다. 또는 업데이트를 위해 재등록하려는 등록된 OU가 있어야 합니다.

OU 등록

1. landing zone에 `IdentityCenterBaseline` 이 (가) 활성화되어 있는지 확인합니다. 그렇다면 Identity Center 활성화 베이스라인 식별자를 가져오십시오.

```
aws controltower list-baselines --query 'baselines[?name==`IdentityCenterBaseline`].
[arn]'
```

```
aws controltower list-enabled-baselines --query 'enabledBaselines[?
baselineIdentifier==`<Identity Center Baseline Arn>`].[arn]'
```

2. 대상 OU의 ARN을 가져옵니다.

```
aws organizations describe-organizational-unit --organizational-unit-id
 <Organizational Unit ID> --query 'OrganizationalUnit.[Arn]'
```

3. 베이스라인의 ARN을 가져옵니다. `AWSControlTowerBaseline`

```
aws controltower list-baselines --query 'baselines[?name==`AWSControlTowerBaseline`].
[arn]'
```

4. 대상 OU에 `AWSControlTowerBaseline` 기준선을 생성합니다.

   ID 센터 베이스라인이 활성화된 경우:

```
aws controltower enable-baseline --baseline-identifier <AWSControlTowerBaseline ARN>
 --baseline-version <BASELINE VERSION> --target-identifier <OU ARN> --parameters
 '[{"key":"IdentityCenterEnabledBaselineArn","value":"<Identity Center Enabled
 Baseline ARN>"}]'
```

   Identity Center 베이스라인이 활성화되지 않은 경우 다음과 같이 *`parameters`* 플래그를 생략하십시오.

```
aws controltower enable-baseline --baseline-identifier <AWSControlTowerBaseline ARN>
 --baseline-version <BASELINE VERSION> --target-identifier <OU ARN>
```

OU 재등록

랜딩 존 설정을 업데이트하거나 랜딩 존 버전을 업데이트한 후에는 OU를 다시 등록하여 최신 변경 사항을 적용해야 합니다. 다음 단계에 따라 관련 리소스를 재설정하여 프로그래밍 방식으로 OU를 재등록하십시오. EnabledBaseline

1. 재등록할 대상 OU의 ARN을 가져옵니다.

```
aws organizations describe-organizational-unit --organizational-unit-id <OU ID> --
query 'OrganizationalUnit.[Arn]'
```

2. 대상 OU에 대한 EnabledBaseline 리소스의 ARN을 가져옵니다.

```
aws controltower list-enabled-baselines --query 'enabledBaselines[?
targetIdentifier==`<OUARN>`].[arn]'
```

3. 활성화 베이스라인을 재설정합니다.

```
aws controltower reset-enabled-baseline --enabled-baseline-
identifier <EnabledBaselineArn>
```

기준 API 사용 예시

이 섹션에는 AWS Control Tower 기준 API의 입력 및 출력 파라미터 예제가 수록되어 있습니다.

DisableBaseline

이 API 작업에 대한 자세한 내용은 을 참조하십시오. DisableBaseline

DisableBaseline입력:

```
{
    "enabledBaselineIdentifier": "arn:aws:controltower:us-
west-2:123456789012:enabledbaseline/AB12CD34EF56GH789"
}
```

DisableBaseline출력:

```
{
    "operationIdentifier": "58f12232-26be-4735-a3e9-dd30d90f021f"
}
```

DisableBaselineCLI 예제:

```
aws controltower disable-baseline \
    --enabled-baseline-identifier arn:aws:controltower:us-
west-2:123456789012:enabledbaseline/AB12CD34EF56GH789 \
    --region us-west-2
```

EnableBaseline

이 API 작업에 대한 자세한 내용은 을 참조하십시오 EnableBaseline.

EnableBaseline입력:

```
{
    "baselineIdentifier": "arn:aws:controltower:us-west-2::baseline:17BSJV3IGJ2QSGA2",
    "targetIdentifier": "arn:aws:organizations::123456789012:ou/o-kgj0txdhpa/ou-
r9mj-4j3mzjql",
    "baselineVersion": "3.0",
    "parameters": [
        {
            "key": "IdentityCenterEnabledBaselineArn",
            "value": "arn:aws:controltower:us-west-2:123456789012:enabledbaseline/
XAHCR4CJTSI4W07MZ"
        }
    ]
}
```

EnableBaseline출력:

```
{
    "operationIdentifier": "58f12232-26be-4735-a3e9-dd30d90f021f",
    "arn": "arn:aws:controltower:us-west-2:123456789012:enabledbaseline/
XAHCR4CJTSI4W07MZ"
}
```

EnableBaselineCLI 예제:

이 예시는 랜딩 존이 옵트인된 AWS Organizations 조직이 AWS Control Tower에서 관리하는 AWS IAM Identity Center 액세스를 허용하도록 기준을 설정하는 방법을 보여줍니다. ID 센터 EnabledBaseline 식별자를 검색하려면 ID 센터 기준에 따라 필터링하여 ListEnabledBaselines API를 호출할 수 있습니다. (arn:aws:controltower:*Region*::baseline/LN25R72TTG6IGPTQ)

```
aws controltower list-enabled-baselines \
    --filter baselineIdentifiers=arn:aws:controltower:us-west-2::baseline/
LN25R72TTG6IGPTQ \
    --region us-west-2
```

응답에는 식별자를 보여주는 EnabledBaseline 세부 정보가 표시됩니다.

```
{
    "enabledBaselines": [
        {
            "arn": "arn:aws:controltower:us-west-2:123456789012:enabledbaseline/
XAHXS7P6C4I453EZC",
            "baselineIdentifier": "arn:aws:controltower:us-west-2::baseline/
LN25R72TTG6IGPTQ",
            "targetIdentifier": "arn:aws:organizations::123456789012:account/o-
aq21sw43de5/123456789012",
            "statusSummary": {
                "status": "SUCCEEDED"
            }
        }
    ]
}
```

> **Note**
>
> 응답의 ARN 값을 기록하고 이 값을 파라미터로 전달하여 기본 기준을 활성화합니다.

```
aws controltower enable-baseline \
    --baseline-identifier arn:aws:controltower:us-west-2::baseline/17BSJV3IGJ2QSGA2 \
    --baseline-version 3.0 \
    --target-identifier arn:aws:organizations::123456789012:ou/o-aq21sw43de5/ou-po90-
lk87jh65 \
```

```
    --parameters
 '[{"key":"IdentityCenterEnabledBaselineArn","value":"arn:aws:controltower:us-
west-2:123456789012:enabledbaseline/XAHXS7P6C4I453EZC"}]' \
    --region us-west-2
```

IAM Identity Center의 AWS Control Tower 관리에서 랜딩 존을 옵트아웃한 조직의 경우 파라미터 없이 베이스라인을 활성화하십시오.

```
aws controltower enable-baseline \
    --baseline-identifier arn:aws:controltower:us-west-2::baseline/17BSJV3IGJ2QSGA2 \
    --baseline-version 3.0 \
    --target-identifier arn:aws:organizations::123456789012:ou/o-aq21sw43de5/ou-po90-
lk87jh65 \
    --region us-west-2
```

GetBaseline

이 API 작업에 대한 자세한 내용은 을 참조하십시오. GetBaseline

GetBaseline입력:

```
{
    "baselineIdentifier": "arn:aws:controltower:us-west-2::baseline/17BSJV3IGJ2QSGA2"
}
```

GetBaseline출력:

```
{
    "arn": "arn:aws:controltower:us-west-2::baseline/17BSJV3IGJ2QSGA2",
    "name": "AWSControlTowerBaseline",
    "description": "Sets up resources and mandatory controls for member accounts within
 the target OU, required for AWS Control Tower governance.",
}
```

GetBaselineCLI 예제:

```
aws controltower get-baseline \
    --baseline-identifier arn:aws:controltower:us-west-2::baseline/17BSJV3IGJ2QSGA2 \
    --region us-west-2
```

GetBaselineOperation

이 API 작업에 대한 자세한 내용은 을 참조하십시오 GetBaselineOperation.

GetBaselineOperation입력:

```
{
    "operationIdentifier": "58f12232-26be-4735-a3e9-dd30d90f021f"
}
```

GetBaselineOperation출력:

```
{
    "baselineOperation": {
        "operationIdentifier": "58f12232-26be-4735-a3e9-dd30d90f021f",
        "operationType": "DISABLE_BASELINE",
        "status": "FAILED",
        "startTime": "2023-01-12T19:05:00Z",
        "endTime": "2023-01-12T19:45:00Z",
        "statusMessage": "Can't perform DisableBaseline on a parent target with
 governed child OUs"
    }
}
```

GetBaselineOperationCLI 예제:

```
aws controltower get-baseline-operation \
    --operation-identifier 58f12232-26be-4735-a3e9-dd30d90f021f \
    --region us-west-2
```

GetEnabledBaseline

이 API 작업에 대한 자세한 내용은 을 참조하십시오 GetEnabledBaseline.

GetEnabledBaseline입력:

```
{
    "enabledBaselineIdentifier": "arn:aws:controltower:us-
west-2:123456789012:enabledbaseline/XAHCR4CJTSI4W07MZ"
}
```

GetEnabledBaseline출력:

```
{
    "enabledBaselineDetails": {
        "arn": "arn:aws:controltower:us-west-2:123456789012:enabledbaseline/
XAHCR4CJTSI4W07MZ",
        "baselineIdentifier": "arn:aws:controltower:us-
west-2::baseline:17BSJV3IGJ2QSGA2",
        "baselineVersion": "3.0",
        "targetIdentifier": "arn:aws:organizations::123456789012:ou/o-kgj0txdhpa/ou-
r9mj-4j3mzjql",
        "statusSummary": {
            "status": "SUCCEEDED",
            "lastOperationIdentifier": "58f12232-26be-4735-a3e9-dd30d90f021f"
        },
        "parameters": [
            {
                "key": "IdentityCenterEnabledBaselineArn",
                "value": "arn:aws:controltower:us-west-2:123456789012:enabledbaseline/
XAHCR4CJTSI4W07MZ"
            }
        ]
    }
}
```

GetEnabledBaselineCLI 예제:

```
aws controltower get-enabled-baseline \
    --enabled-baseline-identifier arn:aws:controltower:us-
west-2:123456789012:enabledbaseline/XAHXS7P6C4I453EZC \
    --region us-west-2
```

ListBaselines

이 API 작업에 대한 자세한 내용은 을 참조하십시오 ListBaselines.

ListBaselines입력 (선택적 입력 사용):

```
{
    "nextToken": "AbCd1234",
    "maxResults": "4"
```

```
}
```

ListBaselines출력:

```
{
    "baselines": [
        {
            "arn": "arn:aws:controltower:us-west-1::baseline/4T4HA1KMO10S6311",
            "name": "AuditBaseline",
            "description": "Sets up resources to monitor security and compliance of
 accounts in your organization."
        },
        {
            "arn": "arn:aws:controltower:us-west-1::baseline/J8HX46AHS5MIKQPD",
            "name": "LogArchiveBaseline",
            "description": "Sets up a central repository for logs of API activities and
 resource configurations from accounts in your organization."
        },
        {
            "arn": "arn:aws:controltower:us-west-1::baseline/LN25R72TTG6IGPTQ",
            "name": "IdentityCenterBaseline",
            "description": "Sets up shared resources for AWS Identity Center, which
 prepares the AWSControlTowerBaseline to set up Identity Center access for accounts."
        },
        {
            "arn": "arn:aws:controltower:us-west-1::baseline/17BSJV3IGJ2QSGA2",
            "name": "AWSControlTowerBaseline",
            "description": "Sets up resources and mandatory controls for member
 accounts within the target OU, required for AWS Control Tower governance."
        }
    ]
}
```

ListBaselinesCLI 예제:

```
aws controltower list-baselines \
    --region us-west-2
```

ListEnabledBaselines

이 API 작업에 대한 자세한 내용은 을 참조하십시오 ListEnabledBaselines.

ListEnabledBaselines입력 (필터 없음):

```
{
    "nextToken": "bde7-XX0c6fXXXXXX",
    "maxResults": 5
}
```

ListEnabledBaselines입력 (baselineIdentifiers필터 전용):

```
{
    "filter": {
        "baselineIdentifiers": ['arn:aws:controltower:us-
east-1::baseline/17BSJV3IGJ2QSGA2', 'arn:aws:controltower:us-
east-1::baseline/12GZU8CKZKVMS2AW']
    },
    "nextToken": "bde7-XX0c6fXXXXXX",
    "maxResults": 5
}
```

ListEnabledBaselines입력 (targetIdentifiers필터 전용):

```
{
    "filter": {
        "targetIdentifiers": ['arn:aws:organizations::123456789012:ou/o-s9511vn103/ou-
xqj7-fex1u317', 'arn:aws:organizations::123456789012:ou/o-s9511vn103/ou-xqj7-11q6n2cf']
    },
    "nextToken": "bde7-XX0c6fXXXXXX",
    "maxResults": 2
}
```

ListEnabledBaselines입력 (baselineIdentifiers및 targetIdentifiers 필터):

```
{
    "filter": {
        "baselineIdentifiers": ['arn:aws:controltower:us-
east-1::baseline/17BSJV3IGJ2QSGA2']
        "targetIdentifiers": ['arn:aws:organizations::123456789012:ou/o-s9511vn103/ou-
xqj7-fex1u317']
    },
    "nextToken": "bde7-XX0c6fXXXXXX",
    "maxResults": 5
}
```

ListEnabledBaselines출력:

```
{
    "enabledBaselines": [
        {
            "arn": "arn:aws:controltower:us-east-1:123456789012:enabledbaseline/
XAHCR4CJTSI4W07MZ",
            "baselineIdentifier": "arn:aws:controltower:us-
east-1::baseline:17BSJV3IGJ2QSGA2",
            "baselineVersion": "3.0",
            "targetIdentifier": "arn:aws:organizations::123456789012:ou/o-kgj0txdhpa/
ou-r9mj-4j3mzjql",
            "statusSummary": {
                "status": "SUCCEEDED",
                "lastOperationIdentifier": "58f12232-26be-4735-a3e9-dd30d90f021f"
            }
        },
        {
            "arn": "arn:aws:controltower:us-east-1:123456789012:enabledbaseline/
XAJ9NKW88AA4W9CLL",
            "baselineIdentifier": "arn:aws:controltower:us-
east-1::baseline:17BSJV3IGJ2QSGA2",
            "baselineVersion": "4.0",
            "targetIdentifier": "arn:aws:organizations::123456789012:ou/o-s9511vn103/
ou-xqj7-fex1u317",
            "statusSummary": {
            "status": "FAILED",
                "lastOperationIdentifier": "81e02df1-2b4d-48f0-838f-3833b93dcdc0"
            }
        }
    ],
    "nextToken": "e2bXXXXX6cab"
}
```

한 가지 유형의 필터 (baselineIdentifiers필터) 를 사용하는 CLI 예제:

```
aws controltower list-enabled-baselines \
    --filter baselineIdentifiers=arn:aws:controltower:us-
west-2::baseline/17BSJV3IGJ2QSGA2,arn:aws:controltower:us-west-2::baseline/
LN25R72TTG6IGPTQ \
    --region us-west-2
```

다중 필터 (baselineIdentifiers및 targetIdentifiers 필터) 를 사용하는 CLI 예제:

```
aws controltower list-enabled-baselines \
    --filter targetIdentifiers=arn:aws:organizations::123456789012:ou/o-
aq21sw43de5/ou-po90-lk87jh65,baselineIdentifiers=arn:aws:controltower:us-
west-2::baseline/17BSJV3IGJ2QSGA2 \
    --region us-west-2
```

ResetEnabledBaseline

이 API 작업에 대한 자세한 내용은 을 참조하십시오 ResetEnabledBaseline.

ResetEnabledbaseline입력:

```
{
    "enabledBaselineIdentifier": "arn:aws:controltower:us-
west-2:123456789012:enabledbaseline/XAJ9NKW88AA4W9CLL"
}
```

ResetEnabledBaseline출력:

```
{
    "operationIdentifier": "81e02df1-2b4d-48f0-838f-3833b93dcdc0"
}
```

ResetEnabledBaselineCLI 예제:

```
aws controltower reset-enabled-baseline \
    --enabled-baseline-identifier arn:aws:controltower:us-
west-2:123456789012:enabledbaseline/XAHXS7P6C4I453EZC \
    --region us-west-2
```

UpdateEnabledBaseline

이 API 작업에 대한 자세한 내용은 을 참조하십시오 UpdateEnabledBaseline.

UpdateEnabledBaseline입력:

```
{
    "enabledBaselineIdentifier": "arn:aws:controltower:us-
east-1:123456789012:enabledbaseline/XAJ9NKW88AA4W9CLL",
    "baselineVersion": "4.0",
```

```
    "parameters": [
        {
            "key": "IdentityCenterEnabledBaselineArn",
            "value": "arn:aws:controltower:us-east-1:123456789012:enabledbaseline/
XAHCR4CJTSI4W07MZ"
        }
    ]
}
```

UpdateEnabledBaseline출력:

```
{
    "operationIdentifier": "81e02df1-2b4d-48f0-838f-3833b93dcdc0"
}
```

UpdateEnabledBaselineCLI 예제:

```
aws controltower update-enabled-baseline \
    --enabled-baseline-identifier arn:aws:controltower:us-
west-2:123456789012:enabledbaseline/XAHXS7P6C4I453EZC \
    --baseline-version 4.0
    --parameters
 '[{"key":"IdentityCenterEnabledBaselineArn","value":"arn:aws:controltower:us-
west-2:123456789012:enabledbaseline/XAHXS7P6C4I453EZC"}]' \
    --region us-west-2
```

관련 정보

이 주제에서는 AWS Control Tower 기능과 추가 개선 사항에 대한 일반적인 사용 사례 및 모범 사례를 나열합니다. 이 주제에는 AWS Control Tower를 사용할 때 도움이 될 수 있는 관련 블로그 게시물, 기술 설명서 및 관련 리소스에 대한 링크도 포함되어 있습니다.

자습서 및 실습

- AWS Control Tower 실습 — 이 실습에서는 AWS Control Tower와 관련된 일반적인 작업에 대한 높은 수준의 개요를 제공합니다.
- 사용 사례를 염두에 두고 있지만 어디서부터 시작해야 할지 잘 모르겠으면 AWS Control Tower 대시보드에서 맞춤형 안내 받기를 선택하십시오.
- AWS Control Tower 기능을 사용하는 방법을 자세히 설명하는 엄선된 YouTube 동영상 목록을 방문해 보십시오.

네트워킹

에서 네트워크에 대해 반복 가능하고 관리 가능한 패턴을 설정하십시오. AWS고객이 일반적으로 사용하는 설계, 자동화 및 어플라이언스에 대해 자세히 알아보십시오.

- AWS Quick Start VPC 아키텍처 — 이 퀵 스타트 가이드는 AWS 클라우드 인프라 AWS 모범 사례를 기반으로 네트워킹 기반을 제공합니다. AWS 서비스 및 기타 리소스를 시작할 수 있는 퍼블릭 및 프라이빗 서브넷이 있는 AWS Virtual Private Network 환경을 구축합니다.
- AWS Service Catalog를 사용하는 AWS Control Tower의 셀프 서비스 VPC — 이 블로그 게시물에서는 사용자 지정 VPC로 계정을 프로비저닝할 수 있도록 Account Factory를 설정하는 방법을 설명합니다.
- AWS Control Tower에서 서버리스 트랜짓 네트워크 오케스트레이터 (STNO) 구현 — 이 블로그 게시물에서는 계정 간 네트워크 연결 액세스를 자동화하는 방법을 보여줍니다. 이 블로그는 AWS Control Tower 관리자 또는 해당 AWS 환경 내 네트워크 관리를 담당하는 관리자를 대상으로 합니다.

보안, 자격 증명 및 로깅

보안 태세를 확장하고, 외부 또는 기존 ID 공급자와 통합하고, 로깅 시스템을 중앙 집중화하십시오.

보안

- AWS Control Tower 수명 주기 이벤트를 통한 AWS Security Hub 알림 자동화 — 이 블로그 게시물에서는 기존 계정과 새 계정의 AWS Control Tower 다중 계정 환경에서 Security Hub 활성화 및 구성을 자동화하는 방법을 설명합니다.
- 활성화 AWS Identity and Access Management — 이 블로그 게시물에서는 IAM Access Analyzer 결과를 활성화하고 중앙 집중화하여 조직의 보안 가시성을 높이는 방법을 설명합니다.
- AWS Systems Manager Parameter Store는 구성 데이터 관리 및 암호 관리를 위한 안전한 계층적 스토리지를 제공합니다. 이를 사용하여 AWS Systems Manager와 AWS에서 사용할 수 있도록 안전한 위치에서 구성 정보를 공유할 수 CloudFormation 있습니다. 예를 들어, 적합성 팩을 배포하려는 지역 목록을 저장할 수 있습니다.

ID

- Azure AD 사용자 ID를 싱글 사인온을 위한 AWS 계정 및 애플리케이션에 연결 — 이 블로그 게시물에서는 IAM ID 센터 및 AWS Control Tower와 함께 Azure AD를 사용하는 방법을 설명합니다.
- 다음을 사용하여 Okta 사용자의 AWS 액세스를 중앙에서 관리합니다. AWS IAM Identity Center— 이 블로그 게시물에서는 IAM Identity Center 및 AWS Control Tower와 함께 Okta를 사용하는 방법을 설명합니다.

로깅

- AWS 중앙 집중식 로깅 솔루션 — 이 솔루션 게시물에서는 조직이 여러 계정 및 AWS 지역에 걸쳐 로그를 수집, 분석 및 표시할 수 있도록 하는 중앙 집중식 로깅 솔루션에 대해 설명합니다. AWS

리소스 배포 및 워크로드 관리

리소스와 워크로드를 배포하고 관리합니다.

- 시작하기 라이브러리 통합 — 이 블로그 게시물에서는 사용할 수 있는 시작하기 포트폴리오에 대해 설명합니다.
- AWS Control Tower에 클라우드 커스토디언의 지속적인 배포

기존 조직 및 계정과의 협력

기존 AWS 조직 및 계정과 함께 작업하세요.

- 계정 등록 — 이 사용 설명서 주제에서는 기존 AWS 계정을 AWS Control Tower에 등록하는 방법을 설명합니다.
- AWS Control Tower에 계정 가져오기 — 이 블로그 게시물에서는 기존 AWS 조직에 AWS Control Tower를 배포하는 방법을 설명합니다.
- AWS Config 규정 준수 팩을 사용하여 AWS Control Tower 거버넌스 확장 — 이 블로그 게시물에서는 기존 계정 및 조직을 AWS AWS Config Control Tower의 거버넌스로 전환하는 데 도움이 되는 규정 준수 팩을 배포하는 방법을 설명합니다.
- AWS Control Tower를 사용하여 가드레일 위반을 탐지하고 완화하는 방법 — 이 블로그 게시물에서는 제어 항목을 추가하는 방법과 규제 준수 위반에 대해 이메일로 알림을 받을 수 있도록 SNS 알림을 구독하는 방법을 설명합니다.

자동화 및 통합

계정 생성을 자동화하고 수명 주기 이벤트를 AWS Control Tower와 통합하십시오.

- 수명 주기 이벤트 — 이 블로그 게시물에서는 AWS Control Tower에서 수명 주기 이벤트를 사용하는 방법을 설명합니다.
- 계정 생성 자동화 — 이 블로그 게시물에서는 AWS Control Tower에서 자동 계정 생성을 설정하는 방법을 설명합니다.
- Amazon VPC 흐름 로그 자동화 — 이 블로그 게시물에서는 다중 계정 환경에서 Amazon VPC 흐름 로그를 자동화하고 중앙 집중화하는 방법을 설명합니다.
- AWS Control Tower 수명 주기 이벤트를 통한 VPC 태깅 자동화 — 이 블로그 게시물에서는 AWS Control Tower의 수명 주기 이벤트를 통해 VPC의 리소스 태깅을 자동화하는 방법을 설명합니다.
- 자동 계정 관리 — 이 블로그 게시물에서는 AWS Control Tower 환경을 설정한 후 계정 관리 작업을 자동화하는 방법을 설명합니다.

워크로드 마이그레이션

AWS Control Tower의 다른 AWS 서비스를 사용하여 워크로드 마이그레이션을 지원하십시오.

- CloudEndure 마이그레이션 — 이 블로그 게시물에서는 워크로드 마이그레이션을 지원하기 위해 AWS Control CloudEndure Tower와 기타 AWS 서비스를 결합하는 방법을 설명합니다.

관련 AWS 서비스

AWS Control Tower는 의 오케스트레이션 계층 역할을 합니다. AWS Organizations따라서 AWS Organizations 콘솔 및 API를 통해 AWS 컨트롤 타워와 연동되는 20개 이상의 다른 AWS 서비스에 액세스할 수 있습니다. 이러한 추가 서비스는 AWS Control Tower 콘솔을 통해 직접 액세스할 수 없습니다.

- AWS Organizations를 통해 AWS Control Tower에 사용할 수 있는 전체 서비스 목록은 AWS Organizations와 함께 사용할 수 있는 AWS 서비스를 참조하십시오.
- 이러한 관련 AWS 서비스에 다중 계정 기능을 사용하려면 신뢰할 수 있는 액세스를 활성화해야 합니다. 자세한 내용은 기타 AWS 서비스와 AWS Organizations 사용을 참조하세요.

  > **Note**
  >
  > AWS IAM ID 센터는 AWS Control Tower에 AWS CloudTrail 설치되며 완전히 통합되어 있다는 점을 기억하십시오. AWS Config이러한 서비스에 대한 신뢰할 수 있는 액세스 또는 위임 관리 설정은 수정할 필요가 없습니다.

- 를 통해 제공되는 일부 AWS 서비스는 AWS Systems Manager 및 AWS Firewall Manager를 비롯한 위임 관리를 사용할 AWS Organizations 수 있습니다. 자세한 내용은 위임된 관리자 구성 및 Firewall Manager의 위임된 관리자 계정 활성화를 참조하십시오. AWS Firewall Manager를 사용하여 보안 그룹을 설정하는 이 동영상도 참조하십시오.

AWS Marketplace 솔루션

에서 솔루션을 찾아보세요 AWS Marketplace.

- AWS Control Tower Marketplace — 타사 소프트웨어를 통합하는 데 도움이 되는 AWS Control Tower용 광범위한 솔루션을 AWS Marketplace 제공합니다. 이러한 솔루션은 ID 관리, 다중 계정 환경을 위한 보안, 중앙 집중식 네트워킹, 운영 인텔리전스, 보안 정보 및 이벤트 관리 (SIEM) 를 비롯한 주요 인프라 및 운영 사용 사례를 해결하는 데 도움이 됩니다.

AWS Control 타워 출시 노트

다음 섹션에서는 AWS Control Tower 랜딩 존에 대한 업데이트가 필요한 AWS Control Tower 릴리스와 서비스에 자동으로 통합되는 릴리스에 대한 세부 정보를 보여줍니다.

기능 및 릴리스는 공식적으로 대중에게 발표된 날짜를 기준으로 연대순 (가장 최근부터) 으로 나열됩니다. 기능 또는 릴리스가 문서화된 시점과 공식적으로 발표되는 시점 사이에 지연이 있을 수 있으므로 여기에 나열된 기능 또는 릴리스 날짜는 에 나와 있는 날짜와 약간 다를 수 있습니다. 문서 이력

2024년 1월 - 현재

2024년 1월부터 AWS Control Tower는 다음과 같은 업데이트를 출시했습니다.

- AWS Control Tower는 최대 100개의 동시 제어 작업을 지원합니다.
- AWS Control Tower는 AWS 캐나다 서부 (캘거리) 에서 사용 가능
- AWS Control Tower는 셀프 서비스 할당량 조정을 지원합니다.
- AWS Control Tower, 규제 참조 가이드 출시
- AWS Control Tower는 두 개의 사전 예방적 제어를 업데이트하고 이름을 변경합니다.
- 더 이상 사용되지 않는 제어 기능은 더 이상 사용할 수 없습니다.
- AWS Control Tower는 다음의 `EnabledControl` 리소스 태깅을 지원합니다. AWS CloudFormation
- AWS Control Tower는 OU 등록 및 기준에 따른 구성을 위한 API를 지원합니다.

AWS Control Tower는 최대 100개의 동시 제어 작업을 지원합니다.

2024년 5월 20일

(AWS Control Tower 랜딩 존은 업데이트가 필요하지 않습니다.)

AWS Control Tower는 이제 더 높은 동시성으로 여러 제어 작업을 지원합니다. 콘솔에서 또는 API를 사용하여 여러 조직 단위 (OU) 에서 동시에 최대 100개의 AWS Control Tower 제어 작업을 제출할 수 있습니다. 최대 10개의 작업을 동시에 실행할 수 있으며 추가 작업은 대기열에 보관됩니다. 이렇게 하면 반복적인 제어 작업으로 인한 운영 부담 없이 여러 AWS 계정항목에 대해 보다 표준화된 구성을 설정할 수 있습니다.

진행 중인 제어 작업과 대기 중인 제어 작업의 상태를 모니터링하려면 AWS Control Tower 콘솔의 새로운 최근 작업 페이지로 이동하거나 새 `ListControlOperations`API를 호출할 수 있습니다.

AWS Control Tower 라이브러리에는 다양한 규제 목표, 프레임워크 및 서비스에 매핑되는 500개 이상의 제어 항목이 포함되어 있습니다. 저장된 데이터 암호화와 같은 특정 규제 목표의 경우 단일 제어 작업으로 여러 제어를 활성화하여 목표를 달성하는 데 도움이 될 수 있습니다. 이 기능을 사용하면 개발을 가속화하고, 모범 사례 제어를 더 빠르게 채택하고, 운영 복잡성을 완화할 수 있습니다.

AWS Control Tower는 AWS 캐나다 서부 (캘거리) 에서 사용 가능

2024년 5월 3일

(AWS Control Tower 랜딩 존은 업데이트가 필요하지 않습니다.)

오늘부터 캐나다 서부 (캘거리) 지역에서 AWS Control Tower를 활성화할 수 있습니다. 이미 AWS Control Tower를 배포했고 거버넌스 기능을 이 지역으로 확장하려는 경우, AWS Control Tower 랜딩 존 API를 사용하면 됩니다. 또는 콘솔에서 AWS Control Tower 대시보드의 설정 페이지로 이동하여 지역을 선택하고 랜딩 존을 업데이트하십시오.

캐나다 서부 (캘거리) 지역은 지원하지 않습니다. AWS Service Catalog이러한 이유로 AWS Control Tower의 일부 기능은 다릅니다. 가장 눈에 띄는 기능 변경은 Account Factory를 사용할 수 없다는 것입니다. 캐나다 서부 (캘거리) 를 홈 지역으로 선택하는 경우 계정 업데이트, 계정 자동화 설정 및 Service Catalog와 관련된 기타 프로세스의 절차는 다른 지역과 다릅니다.

프로비저닝 계정

캐나다 서부 (캘거리) 지역에서 새 계정을 생성하고 프로비저닝하려면 AWS Control Tower 외부에서 계정을 생성한 다음 등록된 OU에 등록하는 것이 좋습니다. 자세한 내용은 기존 계정 등록 및 계정 등록 단계를 참조하십시오.

Service Catalog API는 캐나다 서부 (캘거리) 지역에서 사용할 수 없습니다. Service Catalog API를 통한 AWS Control Tower의 자동 계정 프로비저닝에 나와 있는 예제 스크립트는 사용할 수 없습니다.

AWS Control Tower에 대한 다른 기본 종속성이 없기 때문에 캐나다 서부 (캘거리) 에서는 AFC (어카운트 팩토리 사용자 지정), AFC (테라폼용 어카운트 팩토리), AWS 컨트롤 타워 사용자 지정 (cFCT) 을 사용할 수 없습니다. 거버넌스를 캐나다 서부 (캘거리) 지역으로 확장하는 경우, 거주 지역에서 Service Catalog를 사용할 수 있는 한, AWS Control Tower가 지원하는 모든 지역의 AFC 블루프린트를 계속 관리할 수 있습니다.

규제 항목

AWS Security Hub 서비스 관리형 표준: AWS Control Tower에 대한 사전 예방적 제어 및 제어는 캐나다 서부 (캘거리) 지역에서 사용할 수 없습니다. 예방 `CT.CLOUDFORMATION.PR.1` 제어는 후크 기반 사전 예방 제어를 활성화하는 데만 필요하므로 캐나다 서부 (캘거리) 에서는 사용할 수 없습니다. 에 기반한 특정 탐정 통제는 사용할 수 없습니다. AWS Config 자세한 내용은 관리 제한단원을 참조하세요.

ID 제공업체

IAM ID 센터는 캐나다 서부 (캘거리) 에서 사용할 수 없습니다. 모범 사례 권장 사항은 IAM Identity Center를 사용할 수 있는 지역에 랜딩 존을 설정하는 것입니다. 또는 캐나다 서부 (캘거리) 의 외부 ID 공급자를 사용하는 경우 계정 액세스 구성을 자체 관리할 수도 있습니다.

캐나다 서부 (캘거리) 지역에서 Service Catalog를 사용할 수 없더라도 AWS Control Tower에서 지원하는 다른 지역에는 영향을 미치지 않습니다. 이러한 차이는 거주 지역이 캐나다 서부 (캘거리) 인 경우에만 적용됩니다.

AWS Control Tower를 사용할 수 있는 AWS 지역의 전체 목록은 지역 표를 참조하십시오.

AWS Control Tower는 셀프 서비스 할당량 조정을 지원합니다.

2024년 4월 25일

(AWS Control Tower 랜딩 존은 업데이트가 필요하지 않습니다.)

AWS Control Tower는 이제 Service Quotas 콘솔을 통해 셀프 서비스 할당량 조정을 지원합니다. 자세한 정보는 할당량 증가 요청을 참조하세요.

AWS Control Tower, 규제 참조 가이드 출시

2024년 4월 21일

(AWS Control Tower 랜딩 존은 업데이트가 필요하지 않습니다.)

AWS Control Tower는 AWS Control Tower 환경과 관련된 규제 항목에 대한 세부 정보를 찾을 수 있는 새 문서인 규제 참조 안내서를 발표했습니다. 이전에는 이 자료가 AWS Control Tower 사용 설명

서에 포함되었습니다. 규제 참조 안내서는 확장된 형식의 규제 항목을 다룹니다. 자세한 내용은 AWS Control Tower 규제 참조 안내서를 참조하십시오.

AWS Control Tower는 두 개의 사전 예방적 제어를 업데이트하고 이름을 변경합니다.

2024년 3월 26일

(AWS Control Tower 랜딩 존은 업데이트가 필요하지 않습니다.)

AWS Control Tower는 Amazon Service의 업데이트에 맞춰 두 개의 사전 예방적 제어 항목의 이름을 변경했습니다. OpenSearch

- [CT.OPENSEARCH.PR.8] TLSv1.2를 사용하려면 엘라스틱서치 서비스 도메인이 필요합니다.
- [CT.OPENSEARCH.PR.16] TLSv1.2를 사용하려면 Amazon OpenSearch 서비스 도메인이 필요합니다.

Amazon Service의 최신 릴리스에 맞춰 이 두 컨트롤의 컨트롤 이름과 아티팩트를 업데이트했습니다. Amazon OpenSearch Service는 이제 도메인 엔드포인트 보안을 위한 전송 보안 옵션 중 전송 계층 보안 (TLS) 버전 1.3을 지원합니다.

이러한 컨트롤에 대한 TLSv1.3 지원을 추가하기 위해 컨트롤의 의도를 반영하도록 컨트롤의 아티팩트와 이름을 업데이트했습니다. 이제 서비스 도메인의 최소 TLS 버전을 평가합니다. 사용자 환경에서 이 업데이트를 수행하려면 컨트롤을 비활성화 및 활성화하여 최신 아티팩트를 배포해야 합니다.

다른 사전 예방적 제어는 이 변경의 영향을 받지 않습니다. 이러한 규제 항목을 검토하여 규제 목표를 충족하는지 확인하는 것이 좋습니다.

질문이나 문제가 있으면 AWS Support에 문의하십시오.

더 이상 사용되지 않는 제어 기능은 더 이상 사용할 수 없습니다.

2024년 3월 12일

(AWS Control Tower 랜딩 존은 업데이트가 필요하지 않습니다.)

AWS Control Tower는 일부 제어 기능을 지원 중단했습니다. 이러한 컨트롤은 더 이상 사용할 수 없습니다.

- CT.ATHENA.PR.1

- CT.CODEBUILD.PR.4
- CT.AUTOSCALING.PR.3
- SH.Athena.1
- SH.Codebuild.5
- SH.AutoScaling.4
- SH.SNS.1
- SH.SNS.2

AWS Control Tower는 다음의 **EnabledControl** 리소스 태깅을 지원합니다. AWS CloudFormation

2024년 2월 22일

(AWS Control Tower 랜딩 존은 업데이트가 필요하지 않습니다.)

이번 AWS Control Tower 릴리스에서는 `EnabledControl` 리소스의 동작을 업데이트하여 구성 가능한 제어에 더 잘 맞추고 자동화를 통해 AWS Control Tower 환경을 관리하는 기능을 개선합니다. 이번 릴리스에서는 템플릿을 사용하여 구성 가능한 `EnabledControl` 리소스에 태그를 추가할 수 있습니다. AWS CloudFormation 이전에는 AWS Control Tower 콘솔 및 API를 통해서만 태그를 추가할 수 있었습니다.

AWS Control Tower `GetEnabledControl` 및 `ListTagsforResource` API 운영은 `EnabledControl` 리소스 기능에 의존하기 때문에 이번 릴리스에서 업데이트되었습니다. `EnableControl`

자세한 내용은 AWS Control Tower 및 `EnabledControl`AWS CloudFormation사용 설명서의 *`EnabledControl`* 리소스 태깅을 참조하십시오.

AWS Control Tower는 OU 등록 및 기준에 따른 구성을 위한 API를 지원합니다.

2024년 2월 14일

(AWS Control Tower 랜딩 존은 업데이트가 필요하지 않습니다.)

이러한 API는 통화를 통한 프로그래밍 방식의 OU 등록을 지원합니다. `EnableBaseline` OU에서 베이스라인을 활성화하면 OU 내 멤버 계정이 AWS Control Tower 거버넌스에 등록됩니다. 특정 주의 사

항이 적용될 수 있습니다. 예를 들어, AWS Control Tower 콘솔을 통한 OU 등록은 필수 제어뿐 아니라 선택적 제어도 사용할 수 있습니다. API를 호출할 때 선택적 제어를 활성화하기 위해 추가 단계를 완료해야 할 수 있습니다.

AWS Control Tower 기준선은 OU 및 회원 계정의 AWS Control Tower 거버넌스에 대한 모범 사례를 구현합니다. 예를 들어 OU에 베이스라인을 활성화하면 OU 내 멤버 계정은 IAM Identity Center 및 필수 IAM 역할을 비롯한 AWS CloudTrail정의된 리소스 그룹을 받게 됩니다. AWS Config AWS

특정 베이스라인은 특정 AWS Control Tower 랜딩 존 버전과 호환됩니다. AWS Control Tower는 랜딩 존 설정을 변경할 때 호환되는 최신 베이스라인을 랜딩 존에 적용할 수 있습니다. 자세한 정보는 OU 기준 및 랜딩 존 버전의 호환성을 참조하세요.

이번 릴리스에는 네 가지 필수 요소가 포함되어 있습니다. 베이스라인 유형

- `AWSControlTowerBaseline`
- `AuditBaseline`
- `LogArchiveBaseline`
- `IdentityCenterBaseline`

새 API와 정의된 기준을 사용하여 OU를 등록하고 OU 프로비저닝 워크플로를 자동화할 수 있습니다. 또한 API는 이미 AWS Control Tower 거버넌스 하에 있는 OU를 관리할 수 있으므로 랜딩 존 업데이트 후 OU를 재등록할 수 있습니다. API에는 IaC (코드형 인프라) 로 OU를 관리할 수 있는 AWS CloudFormation `EnabledBaseline` 리소스 지원이 포함되어 있습니다.

베이스라인 API

- EnableBaseline, UpdateEnabledBaseline, DisableBaseline: OU의 기준에 따라 조치를 취하십시오.
- GetEnabledBaseline, ListEnabledBaselines: 활성화된 기준선의 구성을 검색하십시오.
- GetBaselineOperation: 특정 기본 작업의 상태를 볼 수 있습니다.
- ResetEnabledBaseline: 베이스라인을 활성화하여 OU의 리소스 드리프트를 해결합니다 (중첩된 OU 및 필수 제어 드리프트 포함). 또한 지역 거부 제어의 편차를 해결합니다. landing-zone-level
- GetBaseline, ListBaselines: AWS Control Tower 기준의 콘텐츠를 확인해 보십시오.

이러한 API에 대해 자세히 알아보려면 AWS Control Tower 사용 설명서의 기준 및 API 참조를 검토하십시오. 새 API는 GovCloud (미국) 지역을 제외하고 AWS Control Tower를 사용할 수 AWS 리전 있는 곳에서만 사용할 수 있습니다. AWS Control Tower를 사용할 수 AWS 리전 있는 곳의 목록은 AWS 리전 표를 참조하십시오.

2023년 1월 - 현재

2023년 1월부터 AWS Control Tower는 다음과 같은 업데이트를 출시했습니다.

- 새 AWS Service Catalog 외부 제품 유형으로의 전환 (3단계)
- AWS 컨트롤 타워 랜딩 존 버전 3.3
- 새 AWS Service Catalog 외부 제품 유형으로 전환 (2단계)
- AWS Control Tower, 디지털 주권을 지원하는 규제 항목 발표
- AWS Control Tower는 랜딩 존 API를 지원합니다.
- AWS Control Tower는 활성화된 컨트롤에 대한 태그 지정을 지원합니다.
- AWS Control Tower는 아시아 태평양 (멜버른) 지역에서 사용 가능
- 새 AWS Service Catalog 외부 제품 유형으로의 전환 (1단계)
- 새 제어 API 사용 가능
- AWS Control Tower는 추가 규제 항목을 추가합니다.
- 보고된 새 드리프트 유형: 신뢰할 수 있는 액세스 비활성화
- 네 가지 추가 AWS 리전
- 텔아비브 지역에서 사용 가능한 AWS Control Tower
- AWS Control Tower, 28개의 새로운 사전 예방 제어 기능 출시
- AWS Control Tower는 두 가지 규제 항목을 더 이상 사용하지 않습니다.
- AWS 컨트롤 타워 랜딩 존 버전 3.2
- AWS Control Tower는 ID를 기반으로 계정을 처리합니다.
- AWS Control Tower 제어 라이브러리에서 제공되는 추가 Security Hub 탐지 제어 항목
- AWS Control Tower는 제어 메타데이터 테이블을 게시합니다.
- Account Factory 커스터마이징을 위한 테라폼 지원
- AWS 랜딩 존에 IAM 아이덴티티 센터 자체 관리 기능 사용 가능
- AWS Control Tower는 OU의 복합 거버넌스를 해결합니다.
- 추가 사전 예방 제어 기능을 사용할 수 있습니다.
- Amazon EC2 사전 예방 제어 업데이트
- 7개의 추가 사용 가능 AWS 리전
- Account Factory for Terraform (AFT) 계정 사용자 지정 요청 추적

- AWS 컨트롤 타워 랜딩 존 버전 3.1
- 사전 예방적 통제가 일반적으로 이용 가능

새 AWS Service Catalog 외부 제품 유형으로의 전환 (3단계)

2023년 12월 14일

(AWS Control Tower 랜딩 존은 업데이트가 필요하지 않습니다.)

AWS Control Tower는 더 이상 새로 만들 때 제품 유형 (청사진) 으로 Terraform 오픈 소스를 지원하지 않습니다. AWS 계정계정 청사진 업데이트에 대한 자세한 내용 및 지침은 외부 제품 유형으로의 전환을 참조하십시오. AWS Service Catalog

외부 제품 유형을 사용하도록 계정 블루프린트를 업데이트하지 않는 경우 Terraform 오픈 소스 블루프린트를 사용하여 프로비저닝한 계정만 업데이트하거나 종료할 수 있습니다.

AWS 컨트롤 타워 랜딩 존 버전 3.3

2023년 12월 14일

(AWS Control Tower landzone을 버전 3.3으로 업데이트하려면 업데이트가 필요합니다. 자세한 내용은 참조랜딩 영역 업데이트).

AWS Control Tower 감사 계정의 S3 버킷 정책 업데이트

모든 쓰기 권한에 대한 `aws:SourceOrgID` 조건이 충족되어야 하도록 AWS Control Tower가 계정에 배포하는 Amazon S3 Audit 버킷 정책을 수정했습니다. 이번 릴리스부터 AWS 서비스는 조직 또는 조직 단위 (OU) 에서 요청이 시작된 경우에만 리소스에 액세스할 수 있습니다.

`aws:SourceOrgID`조건 키를 사용하고 S3 버킷 정책의 조건 요소에 있는 조직 ID에 값을 설정할 수 있습니다. 이 조건은 조직 내 계정을 대신하여 S3 버킷에 CloudTrail 로그만 쓸 수 있도록 하고, 조직 외부의 CloudTrail 로그가 AWS Control Tower S3 버킷에 기록하는 것을 방지합니다.

기존 워크로드의 기능에는 영향을 주지 않으면서 잠재적인 보안 취약성을 개선하기 위해 이러한 변경을 적용했습니다. 업데이트된 정책을 보려면 을 참조하십시오. 감사 계정의 Amazon S3 버킷 정책

새 조건 키에 대한 자세한 내용은 IAM 설명서 및 “리소스에 액세스하는 AWS 서비스를 위한 확장 가능한 제어 사용”이라는 제목의 IAM 블로그 게시물을 참조하십시오.

SNS 주제의 정책 업데이트 AWS Config

SNS 주제 정책에 새 `aws:SourceOrgID` 조건 키를 추가했습니다. 업데이트된 정책을 보려면 AWS Config AWS Config SNS 주제 정책을 참조하십시오.

착륙 지대 지역 제어 거부 업데이트

- 제거되었습니다. `discovery-marketplace:` 이 조치는 `aws-marketplace:*` 면제 적용 대상입니다.
- `quicksight:DescribeAccountSubscription` 추가됨

업데이트된 템플릿 AWS CloudFormation

AWS KMS 암호화를 사용하지 않을 때 드리프트가 표시되지 `BASELINE-CLOUDTRAIL-MASTER` 않도록 이름이 지정된 스택의 AWS CloudFormation 템플릿을 업데이트했습니다.

새 AWS Service Catalog 외부 제품 유형으로 전환 (2단계)

2023년 12월 7일

(AWS Control Tower 랜딩 존은 업데이트가 필요하지 않습니다.)

HashiCorp Terraform 라이선스를 업데이트했습니다. 그 결과 Terraform 오픈 소스 제품 및 프로비저닝된 제품에 대한 지원을 External이라는 새로운 제품 유형으로 AWS Service Catalog 변경했습니다.

계정의 기존 워크로드 및 AWS 리소스가 중단되지 않도록 하려면 2023년 12월 14일까지 AWS Service Catalog 외부 제품 유형으로 전환의 AWS Control Tower 전환 단계를 따르십시오.

AWS Control Tower, 디지털 주권을 지원하는 규제 항목 발표

2023년 11월 27일

(AWS Control Tower 랜딩 존은 업데이트가 필요하지 않습니다.)

AWS Control Tower는 디지털 주권 요구 사항을 충족하는 데 도움이 되는 65개의 새로운 AWS관리형 제어를 발표했습니다. 이번 릴리스부터 AWS Control Tower 콘솔의 새로운 디지털 주권 그룹에서 이러한 규제 항목을 찾아볼 수 있습니다. 이러한 제어를 사용하여 데이터 레지던시, 세분화된 액세스 제한, 암호화 및 복원력 기능과 관련된 조치를 방지하고 리소스 변경을 탐지하는 데 도움이 될 수 있습니다. 이러한 제어는 대규모 요구 사항을 보다 쉽게 해결할 수 있도록 설계되었습니다. 디지털 주권 통제에 대한 자세한 내용은 디지털 주권 보호를 강화하는 통제를 참조하십시오.

예를 들어, AWS AppSync API 캐시에 전송 중 암호화를 활성화하도록 요구하거나 여러 가용 영역에 AWS Network Firewall을 배포해야 하는 등 암호화 및 복원력 전략을 적용하는 데 도움이 되는 제어를

활성화하도록 선택할 수 있습니다. 또한 AWS Control Tower 지역 거부 제어를 사용자 지정하여 고유한 비즈니스 요구 사항에 가장 적합한 지역별 제한을 적용할 수 있습니다.

이번 릴리스에서는 더욱 향상된 AWS Control Tower 지역 거부 기능이 제공됩니다. OU 수준에서 새로운 매개 변수화된 지역 거부 제어를 적용하여 거버넌스의 세분성을 높이는 동시에 착륙 영역 수준에서 추가 지역 거버넌스를 유지할 수 있습니다. 이 사용자 지정 가능한 지역 거부 제어를 통해 고유한 비즈니스 요구 사항에 가장 적합한 지역 제한을 적용할 수 있습니다. 구성 가능한 새로운 지역 거부 제어에 대한 자세한 내용은 OU에 적용된 지역 거부 제어를 참조하십시오.

새로운 지역 거부 개선 사항의 새로운 도구인 이번 릴리스에는 활성화된 제어를 기본 설정으로 재설정할 수 있는 새 API가 포함되어 있습니다. `UpdateEnabledControl` 이 API는 드리프트를 빠르게 해결해야 하거나 컨트롤이 드리프트 상태에 있지 않음을 프로그래밍 방식으로 보장해야 하는 사용 사례에 특히 유용합니다. 새 API에 대한 자세한 내용은 AWS Control Tower API 레퍼런스를 참조하십시오.

새로운 사전 예방 제어

- CT.APIGATEWAY.PR.6: 최소 TLS 프로토콜 버전의 TLSv1.2를 지정하는 보안 정책을 사용하려면 Amazon API Gateway REST 도메인이 필요합니다.
- CT.APPSYNC.PR.2: 프라이빗 가시성을 AWS AppSync 사용하도록 GraphQL API를 구성해야 합니다.
- CT.APPSYNC.PR.3: AWS AppSync GraphQL API가 API 키로 인증되지 않도록 요구
- CT.APPSYNC.PR.4: 전송 중 암호화를 AWS AppSync 활성화하려면 GraphQL API 캐시가 필요합니다.
- CT.APPSYNC.PR.5: 저장 중 암호화를 AWS AppSync 활성화하려면 GraphQL API 캐시가 필요합니다.
- CT.AUTOSCALING.PR.9: 저장된 데이터를 암호화하려면 Amazon EC2 Auto Scaling 시작 구성을 통해 구성된 Amazon EBS 볼륨이 필요합니다.
- CT.AUTOSCALING.PR.10: Amazon EC2 Auto Scaling 그룹이 시작 템플릿을 재정의할 때 AWS Nitro 인스턴스 유형만 사용하도록 요구
- CT.AUTOSCALING.PR.11: 시작 템플릿을 재정의할 때는 인스턴스 간 네트워크 트래픽 암호화를 지원하는 AWS Nitro 인스턴스 유형만 Amazon EC2 Auto Scaling 그룹에 추가해야 합니다.
- CT.DAX.PR.3: 전송 계층 보안 (TLS) 을 사용하여 전송 데이터를 암호화하려면 DynamoDB 액셀러레이터 클러스터가 필요합니다.
- CT.DMS.PR.2: 소스 및 대상 엔드포인트의 연결을 암호화하려면 DMS (AWS Database Migration Service) 엔드포인트가 필요합니다.

- CT.EC2.PR.15: Amazon EC2 인스턴스가 리소스 유형에서 생성할 때 AWS Nitro 인스턴스 유형을 사용하도록 요구 `AWS::EC2::LaunchTemplate`
- CT.EC2.PR.16: Amazon EC2 인스턴스를 리소스 유형으로 생성할 때는 AWS Nitro 인스턴스 유형을 사용해야 합니다. `AWS::EC2::Instance`
- CT.EC2.PR.17: AWS Nitro 인스턴스 유형을 사용하려면 Amazon EC2 전용 호스트가 필요합니다.
- CT.EC2.PR.18: Amazon EC2 플릿이 Nitro 인스턴스 유형의 시작 템플릿만 재정의하도록 요구합니다. AWS
- CT.EC2.PR.19: Amazon EC2 인스턴스를 리소스 유형을 사용하여 생성한 경우 인스턴스 간 전송 중 암호화를 지원하는 니트로 인스턴스 유형을 사용하도록 요구 `AWS::EC2::Instance`
- CT.EC2.PR.20: Amazon EC2 플릿은 인스턴스 간 전송 시 암호화를 지원하는 AWS Nitro 인스턴스 유형의 시작 템플릿만 재정의하도록 요구합니다.
- CT.ELASTICACHE.PR.8: 최신 버전의 Redis Amazon ElastiCache 복제 그룹에 RBAC 인증을 활성화해야 합니다.
- CT.MQ.PR.1: 고가용성을 위해 Amazon MQ ActiveMQ 브로커가 액티브/스탠바이 배포 모드를 사용하도록 요구합니다.
- CT.MQ.PR.2: 고가용성을 위해 Amazon MQ Rabbit MQ 브로커가 다중 AZ 클러스터 모드를 사용하도록 요구합니다.
- CT.MSK.PR.1: 클러스터 브로커 노드 간 전송 시 암호화를 적용하려면 Amazon 관리형 스트리밍 for Apache Kafka Kafka (MSK) 클러스터가 필요합니다.
- CT.MSK.PR.2: Apache Kafka용 Amazon 관리형 스트리밍 (MSK) 클러스터를 비활성화된 상태로 구성해야 합니다. PublicAccess
- CT.NETWORK-FIREWALL.PR.5: 여러 가용 영역에 AWS Network Firewall 방화벽을 배포해야 합니다.
- CT.RDS.PR.26: 전송 계층 보안 (TLS) 연결을 요구하려면 Amazon RDS DB 프록시가 필요합니다.
- CT.RDS.PR.27: 지원되는 엔진 유형에 대한 전송 계층 보안 (TLS) 연결을 요구하려면 Amazon RDS DB 클러스터 파라미터 그룹이 필요합니다.
- CT.RDS.PR.28: 지원되는 엔진 유형에 대한 전송 계층 보안 (TLS) 연결을 요구하려면 Amazon RDS DB 파라미터 그룹이 필요합니다.
- CT.RDS.PR.29: 'PubliclyAccessible' 속성을 통해 공개적으로 액세스할 수 있도록 Amazon RDS 클러스터를 구성하지 않아야 합니다.
- CT.RDS.PR.30: Amazon RDS 데이터베이스 인스턴스에 지원되는 엔진 유형에 대해 지정한 KMS 키를 사용하도록 구성된 유휴 암호화가 있어야 합니다.

- CT.S3.PR.12: Amazon S3 액세스 포인트에 모든 옵션이 true로 설정된 블록 퍼블릭 액세스 (BPA) 구성이 있어야 합니다.

새로운 예방 제어

- CT.APPSYNC.PV.1 AWS AppSync GraphQL API가 프라이빗 가시성을 사용하도록 구성되어 있어야 합니다.
- CT.EC2.PV.1암호화된 EC2 볼륨에서 Amazon EBS 스냅샷을 생성해야 합니다.
- CT.EC2.PV.2연결된 Amazon EBS 볼륨이 저장된 데이터를 암호화하도록 구성되어 있어야 합니다.
- CT.EC2.PV.3Amazon EBS 스냅샷을 공개적으로 복원할 수 없도록 요구
- CT.EC2.PV.4Amazon EBS 다이렉트 API가 호출되지 않도록 요구
- CT.EC2.PV.5Amazon EC2 VM 가져오기 및 내보내기 사용을 금지합니다.
- CT.EC2.PV.6더 이상 사용되지 않는 Amazon EC2 및 API 작업의 사용을 금지합니다. RequestSpotFleet RequestSpotInstances
- CT.KMS.PV.1서비스에 대한 AWS KMS 보조금 생성을 제한하는 설명을 키 정책에 포함하도록 요구하십시오. AWS KMS AWS
- CT.KMS.PV.2암호화에 RSA 키 자료를 사용하는 AWS KMS 비대칭 키의 키 길이는 2048비트가 아니어야 합니다.
- CT.KMS.PV.3바이패스 정책 잠금 안전 검사가 활성화된 상태로 AWS KMS 키를 구성해야 합니다.
- CT.KMS.PV.4CloudHSM에서 가져온 키 구성 요소로 CMK (AWS KMS 고객 관리 키) 를 구성해야 함 AWS
- CT.KMS.PV.5가져온 키 구성 요소로 AWS KMS 고객 관리 키 (CMK) 를 구성해야 합니다.
- CT.KMS.PV.6외부 키 저장소 (XKS) 에서 가져온 키 구성 요소로 CMK (AWS KMS 고객 관리 키) 를 구성해야 합니다.
- CT.LAMBDA.PV.1IAM 기반 인증을 사용하려면 AWS Lambda 함수 URL이 필요합니다. AWS
- CT.LAMBDA.PV.2내부 보안 주체만 액세스할 수 있도록 AWS Lambda 함수 URL을 구성해야 합니다. AWS 계정
- CT.MULTISERVICE.PV.1: 조직 구성 단위에 대한 요청에 따라 액세스를 거부합니다. AWS AWS 리전

디지털 주권 거버넌스 태세를 강화하는 새로운 탐지 제어 기능은 서비스 관리형 AWS Security Hub 표준 AWS Control Tower의 일부입니다.

새로운 탐정 규제

- SH.ACM.2: ACM에서 관리하는 RSA 인증서는 최소 2,048비트의 키 길이를 사용해야 합니다.
- SH.AppSync.5: AWS AppSync GraphQL API는 API 키로 인증해서는 안 됩니다.
- SH.CloudTrail.6: CloudTrail 로그를 저장하는 데 사용되는 S3 버킷에 공개적으로 액세스할 수 없는지 확인하십시오.
- SH.DMS.9: DMS 엔드포인트는 SSL을 사용해야 합니다.
- SH.DocumentDB.3: Amazon DocumentDB 수동 클러스터 스냅샷은 공개해서는 안 됩니다.
- SH.DynamoDB.3: DynamoDB 액셀러레이터 (DAX) 클러스터는 유휴 상태에서 암호화되어야 합니다.
- SH.EC2.23: EC2 트랜짓 게이트웨이는 VPC 연결 요청을 자동으로 수락하지 않아야 합니다.
- SH.EKS.1: EKS 클러스터 엔드포인트는 공개적으로 액세스할 수 없어야 합니다.
- SH.ElastiCache.3: ElastiCache 복제 그룹에는 자동 장애 조치가 활성화되어 있어야 합니다.
- SH.ElastiCache.4: ElastiCache 복제 그룹이 활성화되어 있어야 encryption-at-rest 합니다.
- SH.ElastiCache.5: ElastiCache 복제 그룹이 encryption-in-transit 활성화되어 있어야 합니다.
- SH.ElastiCache.6: 이전 Redis 버전의 ElastiCache 복제 그룹에는 Redis AUTH가 활성화되어 있어야 합니다.
- SH.EventBridge.3: EventBridge 사용자 지정 이벤트 버스에는 리소스 기반 정책이 첨부되어야 합니다.
- SH.KMS.4: AWS KMS 키 로테이션을 활성화해야 합니다.
- SH.Lambda.3: Lambda 함수는 VPC에 있어야 합니다.
- SH.MQ.5: ActiveMQ 브로커는 액티브/스탠바이 배포 모드를 사용해야 합니다.
- SH.MQ.6: RabbitMQ 브로커는 클러스터 배포 모드를 사용해야 합니다.
- SH.MSK.1: MSK 클러스터는 브로커 노드 간 전송 시 암호화되어야 합니다.
- SH.RDS.12: RDS 클러스터에 대해 IAM 인증을 구성해야 합니다.
- SH.RDS.15: RDS DB 클러스터는 여러 가용 영역에 맞게 구성해야 합니다.
- SH.S3.17: S3 버킷은 유휴 상태에서 키를 사용하여 암호화해야 합니다. AWS KMS

AWS Security Hub 서비스 관리형 표준 AWS Control Tower에 추가된 규제 항목에 대한 자세한 내용은 설명서에서 서비스 관리형 표준: AWS Control Tower에 적용되는 제어를 참조하십시오. AWS Security Hub

AWS Security Hub 서비스 관리형 표준 AWS Control Tower의 일부인 특정 제어를 지원하지 AWS 리전 않는 항목의 목록은 지원되지 않는 지역을 참조하십시오.

OU 수준에서 지역 거부를 위한 구성 가능한 새로운 제어

CT.MULTISERVICE.PV.1: 이 컨트롤은 파라미터를 수락하여 전체 AWS Control Tower 랜딩 존이 아닌 OU 수준에서 허용되는 면제 지역, IAM 보안 주체 및 작업을 지정합니다. 이는 서비스 제어 정책 (SCP) 에 의해 구현되는 예방적 제어입니다.

자세한 내용은 OU에 적용된 지역 거부 제어를 참조하십시오.

`UpdateEnabledControl` API

이번 AWS Control Tower 릴리스에는 제어에 대한 다음과 같은 API 지원이 추가되었습니다.

- 업데이트된 `EnableControl` API는 구성 가능한 제어를 구성할 수 있습니다.
- 업데이트된 `GetEnabledControl` API는 활성화된 컨트롤에 구성된 매개변수를 표시합니다.
- 새 `UpdateEnabledControl` API는 활성화된 컨트롤의 매개변수를 변경할 수 있습니다.

자세한 내용은 AWS Control Tower API 레퍼런스를 참조하십시오.

AWS Control Tower는 랜딩 존 API를 지원합니다.

2023년 11월 26일

(AWS Control Tower 랜딩 존은 업데이트가 필요하지 않습니다.)

AWS Control Tower는 이제 API를 사용한 랜딩 존 구성 및 시작을 지원합니다. API를 사용하여 랜딩 존을 생성, 업데이트, 가져오기, 나열, 재설정 및 삭제할 수 있습니다.

다음 API를 사용하면 AWS CloudFormation 또는 를 사용하여 프로그래밍 방식으로 랜딩 존을 설정하고 관리할 수 있습니다. AWS CLI

AWS Control Tower는 랜딩 존에 대해 다음과 같은 API를 지원합니다.

- `CreateLandingZone`—이 API 호출은 랜딩 존 버전과 매니페스트 파일을 사용하여 랜딩 존을 생성합니다.
- `GetLandingZoneOperation`—이 API 호출은 지정된 landding Zone 작업의 상태를 반환합니다.
- `GetLandingZone`—이 API 호출은 버전, 매니페스트 파일, 상태를 포함하여 지정된 landding Zone에 대한 세부 정보를 반환합니다.

- `UpdateLandingZone`—이 API 호출은 landding Zone 버전 또는 매니페스트 파일을 업데이트합니다.
- `ListLandingZone`—이 API 호출은 관리 계정의 랜딩 존 설정에 대해 하나의 랜딩 존 식별자 (ARN)를 반환합니다.
- `ResetLandingZone`—이 API 호출은 랜딩 존을 최신 업데이트에 지정된 매개변수로 재설정하여 드리프트를 복구할 수 있습니다. 랜딩 존이 업데이트되지 않은 경우 이 호출은 랜딩 존을 생성 시 지정된 파라미터로 재설정합니다.
- `DeleteLandingZone`—이 API 호출은 랜딩 존을 해제합니다.

landding zone API를 시작하려면 를 참조하십시오. API를 사용하여 AWS 컨트롤 타워 시작하기

AWS Control Tower는 활성화된 컨트롤에 대한 태그 지정을 지원합니다.

2023년 11월 10일

(AWS Control Tower 랜딩 존은 업데이트가 필요하지 않습니다.)

AWS Control Tower는 이제 AWS Control Tower 콘솔에서 또는 API를 통해 활성화된 제어에 대한 리소스 태깅을 지원합니다. 활성화된 컨트롤의 태그를 추가, 제거 또는 나열할 수 있습니다.

다음 API가 출시됨에 따라 AWS Control Tower에서 활성화하는 컨트롤에 대한 태그를 구성할 수 있습니다. 태그를 사용하면 리소스를 손쉽게 관리, 식별, 정리, 검색 및 필터링할 수 있습니다. 태그를 생성하여 용도, 소유자, 환경 또는 기타 기준으로 리소스를 분류할 수 있습니다.

AWS Control Tower는 컨트롤 태깅을 위해 다음과 같은 API를 지원합니다.

- `TagResource`—이 API 호출은 AWS Control Tower에서 활성화된 컨트롤에 태그를 추가합니다.
- `UntagResource`—이 API 호출은 AWS Control Tower에서 활성화된 컨트롤에서 태그를 제거합니다.
- `ListTagsForResource`—이 API 호출은 AWS Control Tower에서 활성화된 컨트롤에 대한 태그를 반환합니다.

AWS 컨트롤 타워 제어 API는 AWS 컨트롤 타워가 제공되는 AWS 리전 곳에서 사용할 수 있습니다. 사용 가능한 AWS Control AWS 리전 Tower의 전체 목록은 AWS 지역 표를 참조하십시오. AWS 컨트롤 타워 API의 전체 목록은 API 참조를 참조하십시오.

AWS Control Tower는 아시아 태평양 (멜버른) 지역에서 사용 가능

2023년 11월 3일

(AWS Control Tower 랜딩 존은 업데이트가 필요하지 않습니다.)

AWS Control Tower는 아시아 태평양 (멜버른) 지역에서 사용할 수 있습니다.

이미 AWS Control Tower를 사용 중이고 계정의 이 지역으로 거버넌스 기능을 확장하려는 경우, AWS Control Tower 대시보드의 설정 페이지로 이동하여 지역을 선택한 다음 랜딩 존을 업데이트하십시오. 랜딩 존 업데이트 후에는 AWS Control Tower가 관리하는 모든 계정을 업데이트하여 새 리전에서 계정과 OU를 거버넌스 하에 두어야 합니다. 자세한 내용은 업데이트 정보를 참조하십시오.

AWS Control Tower를 사용할 수 있는 지역의 전체 목록은 AWS 리전 표를 참조하십시오.

새 AWS Service Catalog 외부 제품 유형으로의 전환 (1단계)

2023년 10월 31일

(AWS Control Tower 랜딩 존은 업데이트가 필요하지 않습니다.)

HashiCorp Terraform 라이선스를 업데이트했습니다. 그 결과 Terraform 오픈 소스 제품에 대한 지원이 AWS Service Catalog 업데이트되고 제품이 External이라는 새로운 제품 유형으로 프로비저닝되었습니다.

AWS Control Tower는 AWS Service Catalog 외부 제품 유형에 의존하는 Account Factory 사용자 지정을 지원하지 않습니다. 계정의 기존 워크로드 및 AWS 리소스가 중단되지 않도록 하려면 2023년 12월 14일까지 AWS Control Tower 전환 단계를 다음 권장 순서대로 따르십시오.

1. 외부 및 Terraform 오픈 소스 제품 유형에 대한 지원을 AWS Service Catalog 포함하도록 기존 Terraform 참조 엔진을 업그레이드하십시오. Terraform 참조 엔진 업데이트에 대한 지침은 리포지토리를 검토하세요.AWS Service Catalog GitHub
2. 기존 Terraform 오픈 소스 블루프린트로 AWS Service Catalog 이동하여 복제하여 새 외부 제품 유형을 사용하세요. 기존 Terraform 오픈 소스 블루프린트를 종료하지 마십시오.
3. 기존 Terraform 오픈 소스 블루프린트를 계속 사용하여 AWS Control Tower에서 계정을 생성하거나 업데이트하십시오.

새 제어 API 사용 가능

2023년 10월 14일

(AWS Control Tower 랜딩 존은 업데이트가 필요하지 않습니다.)

AWS Control Tower는 이제 AWS Control Tower 컨트롤을 대규모로 배포하고 관리하는 데 사용할 수 있는 추가 API를 지원합니다. AWS Control Tower 제어 API에 대한 자세한 내용은 API 참조를 참조하십시오.

AWS Control Tower는 새로운 제어 API를 추가했습니다.

- `GetEnabledControl`—API 호출은 활성화된 제어에 대한 세부 정보를 제공합니다.

이 API도 업데이트되었습니다.

`ListEnabledControls`—이 API 호출은 지정된 조직 단위에서 AWS Control Tower가 활성화한 컨트롤과 여기에 포함된 계정을 나열합니다. 이제 `EnabledControlSummary` 객체에 추가 정보가 반환됩니다.

이러한 API를 사용하면 몇 가지 일반적인 작업을 프로그래밍 방식으로 수행할 수 있습니다. 예:

- AWS Control Tower 제어 라이브러리에서 활성화한 모든 컨트롤의 목록을 가져올 수 있습니다.
- 활성화된 모든 컨트롤에 대해 컨트롤이 지원되는 지역, 컨트롤 식별자 (ARN), 컨트롤의 드리프트 상태, 컨트롤의 상태 요약에 대한 정보를 얻을 수 있습니다.

AWS 컨트롤 타워 제어 API는 AWS 컨트롤 타워가 제공되는 AWS 리전 곳에서 사용할 수 있습니다. 사용 가능한 AWS Control AWS 리전 Tower의 전체 목록은 AWS 지역 표를 참조하십시오. AWS 컨트롤 타워 API의 전체 목록은 API 참조를 참조하십시오.

AWS Control Tower는 추가 규제 항목을 추가합니다.

2023년 10월 5일

(AWS Control Tower 랜딩 존은 업데이트가 필요하지 않습니다.)

AWS Control Tower는 새로운 사전 예방 및 탐지 제어를 발표했습니다.

AWS Control Tower의 사전 예방적 제어는 규정을 준수하지 않는 리소스를 프로비저닝하기 전에 AWS CloudFormation 식별하여 차단하는 AWS CloudFormation Hook을 통해 구현됩니다. 사전 예방적 제어는 AWS Control Tower의 기존 예방 및 탐지 제어 기능을 보완합니다.

새로운 사전 예방 제어

- [CT.ATHENA.PR.1] Amazon Athena 워크그룹이 저장된 Athena 쿼리 결과를 암호화하도록 요구

- [CT.ATHENA.PR.2] Amazon Athena 워크그룹이 저장 중인 Athena 쿼리 결과를 (KMS) 키로 암호화하도록 요구 AWS Key Management Service
- [CT.CLOUDTRAIL.PR.4] 키를 사용하여 저장 중 암호화를 활성화하려면 AWS CloudTrail Lake 이벤트 데이터 스토어가 필요합니다. AWS KMS
- [CT.DAX.PR.2] 최소 3개의 가용 영역에 노드를 배포하려면 Amazon DAX 클러스터가 필요합니다.
- [CT.EC2.PR.14] 저장된 데이터를 암호화하려면 Amazon EC2 시작 템플릿을 통해 구성된 Amazon EBS 볼륨이 필요합니다.
- [CT.EKS.PR.2] Amazon EKS 클러스터를 KMS (AWS 키 관리 서비스) 키를 사용한 비밀 암호화로 구성해야 함
- [CT.ELASTICLOADBALANCING.PR.14] 영역 간 로드 밸런싱을 활성화하려면 Network Load Balancer가 필요합니다.
- [CT.ELASTICLOADBALANCING.PR.15] Elastic Load Balancing v2 대상 그룹이 영역 간 로드 밸런싱을 명시적으로 비활성화하지 않도록 설정해야 합니다.
- [CT.EMR.PR.1] Amazon S3에 저장된 데이터를 암호화하도록 Amazon EMR (EMR) 보안 구성을 구성해야 합니다.
- [CT.EMR.PR.2] Amazon EMR (EMR) 보안 구성이 Amazon S3에 저장된 데이터를 키로 암호화하도록 구성되어 있어야 합니다. AWS KMS
- [CT.EMR.PR.3] Amazon EMR (EMR) 보안 구성이 키를 사용한 EBS 볼륨 로컬 디스크 암호화로 구성되어 있어야 합니다. AWS KMS
- [CT.EMR.PR.4] 전송 데이터를 암호화하도록 Amazon EMR (EMR) 보안 구성을 구성해야 합니다.
- [CT.GLUE.PR.1] AWS Glue 작업에 관련 보안 구성이 있어야 합니다.
- [CT.GLUE.PR.2] AWS KMS 키를 사용하여 Amazon S3 대상의 데이터를 암호화하려면 AWS Glue 보안 구성이 필요합니다.
- [CT.KMS.PR.2] 암호화에 RSA 키 자료를 사용하는 AWS KMS 비대칭 키의 키 길이는 2048비트보다 커야 합니다.
- [CT.KMS.PR.3] 서비스에 대한 권한 AWS KMS 부여를 제한하는 설명을 키 정책에 포함해야 합니다. AWS KMS AWS
- [CT.LAMBDA.PR.4] AWS 조직 또는 특정 AWS 계정에 액세스 권한을 부여하려면 AWS Lambda 계층 권한이 필요합니다.
- [CT.LAMBDA.PR.5] AWS IAM 기반 인증을 사용하려면 AWS Lambda 함수 URL이 필요합니다.
- [CT.LAMBDA.PR.6] 특정 출처에 대한 액세스를 제한하려면 AWS Lambda 함수 URL CORS 정책이 필요합니다.

- [CT.NEPTUNE.PR.4] 감사 로그에 대한 Amazon 로그 내보내기를 활성화하려면 CloudWatch Amazon Neptune DB 클러스터가 필요합니다.
- [CT.NEPTUNE.PR.5] Amazon Neptune DB 클러스터에서 백업 보존 기간을 7일 이상으로 설정하도록 요구
- [CT.REDSHIFT.PR.9] Amazon Redshift 클러스터 파라미터 그룹이 전송 데이터를 암호화하는 데 보안 소켓 계층 (SSL) 을 사용하도록 구성되어 있어야 합니다.

이러한 새로운 사전 예방적 제어 기능은 AWS Control Tower가 제공되는 AWS 리전 곳에서 상업적으로 사용할 수 있습니다. 이러한 제어에 대한 자세한 내용은 사전 제어를 참조하십시오. 제어 기능을 사용할 수 있는 위치에 대한 자세한 내용은 제어 제한을 참조하십시오.

새로운 탐정 제어

Security Hub 서비스 관리형 표준인 AWS Control Tower에 새로운 제어 기능이 추가되었습니다. 이러한 제어는 거버넌스 태세를 강화하는 데 도움이 됩니다. 특정 OU에서 활성화한 후에는 Security Hub 서비스 관리형 표준인 AWS Control Tower의 일부로 작동합니다.

- [SH.Athena.1] Athena 워크그룹은 유휴 상태에서 암호화되어야 합니다.
- [SH.Neptune.1] Neptune DB 클러스터는 유휴 상태에서 암호화되어야 합니다.
- [SH.Neptune.2] Neptune DB 클러스터는 감사 로그를 로그에 게시해야 합니다. CloudWatch
- [SH.Neptune.3] Neptune DB 클러스터 스냅샷은 퍼블릭이 아니어야 합니다.
- [SH.Neptune.4] Neptune DB 클러스터에는 삭제 방지 기능이 활성화되어 있어야 합니다.
- [SH.Neptune.5] Neptune DB 클러스터에는 자동 백업이 활성화되어 있어야 합니다.
- [SH.Neptune.6] Neptune DB 클러스터 스냅샷은 유휴 상태에서 암호화해야 합니다.
- [SH.Neptune.7] Neptune DB 클러스터에는 IAM 데이터베이스 인증이 활성화되어 있어야 합니다.
- [SH.Neptune.8] 태그를 스냅샷에 복사하도록 Neptune DB 클러스터를 구성해야 합니다.
- [SH.RDS.27] RDS DB 클러스터는 유휴 상태에서 암호화해야 합니다.

새로운 AWS Security Hub 탐지 컨트롤은 AWS Control AWS 리전 Tower가 있는 대부분의 지역에서 사용할 수 있습니다. 이러한 규제 항목에 대한 자세한 내용은 서비스 관리형 표준에 적용되는 규제: AWS Control Tower를 참조하십시오. 제어 항목을 사용할 수 있는 위치에 대한 자세한 내용은 을 참조하십시오. 관리 제한

보고된 새 드리프트 유형: 신뢰할 수 있는 액세스 비활성화

2023년 9월 21일

(AWS Control Tower 랜딩 존은 업데이트가 필요하지 않습니다.)

AWS Control Tower 랜딩 존을 설정한 후에는 에서 AWS Control Tower에 대한 신뢰할 수 있는 액세스를 비활성화할 수 AWS Organizations있습니다. 하지만 그렇게 하면 드리프트가 발생합니다.

신뢰할 수 있는 액세스가 비활성화된 드리프트 유형에서는 이러한 유형의 드리프트가 발생하면 AWS Control Tower에서 알림을 보내므로 AWS Control Tower 랜딩 존을 복구할 수 있습니다. 자세한 내용은 거버넌스 드리프트 유형을 참조하십시오.

네 가지 추가 AWS 리전

2023년 9월 13일

(AWS Control Tower 랜딩 존은 업데이트가 필요하지 않습니다.)

AWS Control Tower는 이제 아시아 태평양 (하이데라바드), 유럽 (스페인 및 취리히), 중동 (UAE) 에서 사용할 수 있습니다.

이미 AWS Control Tower를 사용 중이고 계정의 이 지역으로 거버넌스 기능을 확장하려는 경우, AWS Control Tower 대시보드의 설정 페이지로 이동하여 지역을 선택한 다음 랜딩 존을 업데이트하십시오. 랜딩 존 업데이트 후에는 AWS Control Tower가 관리하는 모든 계정을 업데이트하여 새 리전에서 계정과 OU를 거버넌스 하에 두어야 합니다. 자세한 내용은 업데이트 정보를 참조하십시오.

AWS Control Tower를 사용할 수 있는 지역의 전체 목록은 AWS 리전 표를 참조하십시오.

텔아비브 지역에서 사용 가능한 AWS Control Tower

2023년 8월 28일

(AWS Control Tower 랜딩 존은 업데이트가 필요하지 않습니다.)

AWS Control Tower는 이스라엘 (텔아비브) 지역에서의 가용성을 발표했습니다.

이미 AWS Control Tower를 사용 중이고 계정의 이 지역으로 거버넌스 기능을 확장하려는 경우, AWS Control Tower 대시보드의 설정 페이지로 이동하여 지역을 선택한 다음 랜딩 존을 업데이트하십시오. 랜딩 존 업데이트 후에는 AWS Control Tower가 관리하는 모든 계정을 업데이트하여 새 리전에서 계정과 OU를 거버넌스 하에 두어야 합니다. 자세한 내용은 업데이트 정보를 참조하십시오.

AWS Control Tower를 사용할 수 있는 지역의 전체 목록은 AWS 리전 표를 참조하십시오.

AWS Control Tower, 28개의 새로운 사전 예방 제어 기능 출시

2023년 7월 24일

(AWS Control Tower 랜딩 존은 업데이트가 필요하지 않습니다.)

AWS Control Tower는 AWS 환경 관리를 지원하기 위해 28개의 새로운 사전 예방 제어를 추가하고 있습니다.

사전 예방적 제어는 규정을 준수하지 않는 리소스를 프로비저닝하기 전에 차단함으로써 다중 계정 AWS 환경 전반에서 AWS Control Tower의 거버넌스 기능을 강화합니다. 이러한 컨트롤은 Amazon, Amazon Neptune CloudWatch, ElastiCache Amazon 및 Amazon DocumentDB와 같은 AWS 서비스를 관리하는 데 도움이 됩니다. AWS Step Functions새로운 제어 기능은 로깅 및 모니터링 설정, 저장된 데이터 암호화 또는 복원력 향상과 같은 제어 목표를 달성하는 데 도움이 됩니다.

새 컨트롤의 전체 목록은 다음과 같습니다.

- [CT.APPSYNC.PR.1] GraphQL API에서 로깅을 AWS AppSync 활성화해야 합니다.
- [CT.CLOUDWATCH.PR.1] CloudWatch Amazon 경보에 경보 상태에 대한 작업이 구성되어 있어야 합니다.
- [CT.CLOUDWATCH.PR.2] CloudWatch 아마존 로그 그룹을 최소 1년 동안 보존하도록 요구
- [CT.CLOUDWATCH.PR.3] CloudWatch Amazon 로그 그룹을 유휴 상태에서 KMS 키를 사용하여 암호화하도록 요구 AWS
- [CT.CLOUDWATCH.PR.4] 아마존 알람 액션을 활성화해야 합니다 CloudWatch
- [CT.DOCUMENTDB.PR.1] Amazon DocumentDB 클러스터를 유휴 상태에서 암호화해야 함
- [CT.DOCUMENTDB.PR.2] Amazon DocumentDB 클러스터에 자동 백업이 활성화되어 있어야 합니다.
- [CT.DYNAMODB.PR.2] Amazon DynamoDB 테이블을 유휴 상태에서 키를 사용하여 암호화하도록 요구 AWS KMS
- [CT.EC2.PR.13] Amazon EC2 인스턴스에 세부 모니터링이 활성화되어 있어야 합니다.
- [CT.EKS.PR.1] 클러스터 쿠버네티스 API 서버 엔드포인트에 대한 퍼블릭 액세스를 비활성화하도록 Amazon EKS 클러스터를 구성해야 합니다.
- [CT.ELASTICACHE.PR.1] Redis용 ElastiCache Amazon 클러스터에 자동 백업이 활성화되어 있어야 합니다.
- [CT.ELASTICACHE.PR.2] Redis용 ElastiCache Amazon 클러스터에 자동 마이너 버전 업그레이드가 활성화되어 있어야 합니다.

- [CT.ELASTICACHE.PR.3] Redis용 ElastiCache Amazon 복제 그룹에 자동 장애 조치가 활성화되어 있어야 합니다.
- [CT.ELASTICACHE.PR.4] Amazon ElastiCache 복제 그룹에 저장 중 암호화가 활성화되어 있어야 합니다.
- [CT.ELASTICACHE.PR.5] Redis용 ElastiCache Amazon 복제 그룹에 전송 중 암호화가 활성화되어 있어야 합니다.
- [CT.ELASTICACHE.PR.6] 사용자 지정 서브넷 그룹을 사용하려면 Amazon ElastiCache 캐시 클러스터가 필요합니다.
- [CT.ELASTICACHE.PR.7] 이전 Redis 버전의 ElastiCache Amazon 복제 그룹에 Redis 인증 필요
- [CT.ELASTICBEANSTALK.PR.3] 로깅 구성을 갖추려면 Elastic Beanstalk 환경이 필요합니다 AWS
- [CT.LAMBDA.PR.3] 고객 관리형 아마존 가상 사설 클라우드 (VPC) 에 AWS Lambda 함수가 있어야 함
- [CT.NEPTUNE.PR.1] Amazon Neptune DB 클러스터에 (IAM) 데이터베이스 인증 필요 AWS Identity and Access Management
- [CT.NEPTUNE.PR.2] Amazon Neptune DB 클러스터에 삭제 방지 기능이 활성화되어 있어야 합니다.
- [CT.NEPTUNE.PR.3] Amazon Neptune DB 클러스터에 스토리지 암호화가 활성화되어 있어야 합니다.
- [CT.REDSHIFT.PR.8] Amazon Redshift 클러스터를 암호화해야 합니다.
- [CT.S3.PR.9] Amazon S3 버킷에 S3 오브젝트 잠금이 활성화되어 있어야 합니다.
- [CT.S3.PR.10] Amazon S3 버킷에는 키를 사용하여 서버 측 암호화가 구성되어 있어야 합니다. AWS KMS
- [CT.S3.PR.11] Amazon S3 버킷에 버전 관리를 활성화해야 합니다.
- [CT.STEPFUNCTIONS.PR.1] 상태 시스템에 로깅이 활성화되어 있어야 합니다. AWS Step Functions
- [CT.STEPFUNCTIONS.PR.2] 스테이트 머신에 추적 기능이 활성화되어 있어야 합니다. AWS Step Functions AWS X-Ray

AWS Control Tower의 사전 예방적 제어는 규정을 준수하지 않는 리소스를 프로비저닝하기 전에 AWS CloudFormation 식별하여 차단하는 AWS CloudFormation Hook을 통해 구현됩니다. 사전 예방적 제어는 AWS Control Tower의 기존 예방 및 탐지 제어 기능을 보완합니다.

이러한 새로운 사전 예방 제어 기능은 AWS Control Tower가 제공되는 모든 AWS 리전 곳에서 사용할 수 있습니다. 이러한 제어에 대한 자세한 내용은 사전 제어를 참조하십시오.

AWS Control Tower는 두 가지 규제 항목을 더 이상 사용하지 않습니다.

2023년 7월 18일

(AWS Control Tower 랜딩 존은 업데이트가 필요하지 않습니다.)

AWS Control Tower는 보안 규제 항목이 최신 상태이고 여전히 모범 사례로 간주되는지 확인하기 위해 정기적으로 검토합니다. 다음 두 규제 항목은 2023년 7월 18일부터 사용이 중단되었으며, 2023년 8월 18일부터 규제 라이브러리에서 제거될 예정입니다. 더 이상 어떤 조직 단위에서도 이러한 컨트롤을 활성화할 수 없습니다. 제거 날짜 이전에 이러한 컨트롤을 비활성화하도록 선택할 수 있습니다.

- [SH.S3.4] S3 버킷에는 서버 측 암호화가 활성화되어 있어야 합니다.
- [CT.S3.PR.7] Amazon S3 버킷에 서버 측 암호화가 구성되어 있어야 합니다.

지원 중단 이유

2023년 1월부터 Amazon S3는 암호화되지 않은 모든 신규 및 기존 버킷에 기본 암호화를 구성하여 해당 버킷에 업로드된 새 객체에 대해 S3 관리 키 (SSE-S3) 를 기본 암호화 수준으로 사용하는 서버 측 암호화를 적용합니다. 이미 SSE-S3 또는 AWS 키 관리 서비스 (KMS) 키를 사용한 서버 측 암호화 (AWS SSE-KMS) 가 구성된 기존 버킷의 기본 암호화 구성은 변경되지 않았습니다.

AWS 컨트롤 타워 랜딩 존 버전 3.2

2023년 6월 16일

(AWS Control Tower landzone을 버전 3.2로 업데이트하려면 업데이트가 필요합니다. 자세한 내용은 참조랜딩 영역 업데이트).

AWS Control Tower 랜딩 존 버전 3.2에서는 AWS Security Hub 서비스 관리형 표준: AWS Control Tower의 일부인 제어 기능을 일반 버전으로 제공합니다. 이 표준의 일부인 컨트롤의 드리프트 상태를 AWS Control Tower 콘솔에서 볼 수 있는 기능을 소개합니다.

이 업데이트에는 라는 새로운 서비스 연결 역할 (SLR) 이 포함되어 있습니다. AWSServiceRoleForAWSControlTower 이 역할은 각 멤버 AWSControlTowerManagedRule계정에서 라는 EventBridge 관리형 규칙을 생성하여 AWS Control Tower를 지원합니다. 이 관리형 규칙은 AWS Control Tower에서 제어 드리프트를 확인할 수 있는 AWS Security Hub 찾기 이벤트를 수집합니다.

이 규칙은 AWS Control Tower에서 만든 첫 번째 관리형 규칙입니다. 규칙은 스택으로 배포되지 않고 EventBridge API에서 직접 배포됩니다. 규칙은 EventBridge 콘솔에서 또는 EventBridge API를 통해 볼 수 있습니다. `managed-by`필드가 채워지면 AWS Control Tower 서비스 보안 주체가 표시됩니다.

이전에는 AWS Control Tower가 회원 계정에서 작업을 수행하는 AWSControlTowerExecution역할을 맡았습니다. 이 새로운 역할과 규칙은 다중 계정 환경에서 작업을 수행할 때 최소 권한을 허용한다는 모범 사례 원칙에 더 잘 부합합니다. AWS 새 역할은 회원 계정에서 관리형 규칙 생성, 관리형 규칙 유지 관리, SNS를 통한 보안 알림 게시, 드리프트 확인 등을 구체적으로 허용하는 범위 축소된 권한을 제공합니다. 자세한 정보는 AWSServiceRoleForAWSControlTower을 참조하세요.

Landzone 3.2 업데이트에는 처음에 서비스 연결 역할을 배포하는 관리 계정의 새 StackSet 리소스도 포함되어 있습니다. `BP_BASELINE_SERVICE_LINKED_ROLE`

Security Hub 제어 드리프트 (랜딩 존 3.2 이상) 를 보고하면 AWS Control Tower는 Security Hub로부터 일일 상태 업데이트를 받습니다. 모든 관리 대상 지역에서 제어 기능이 활성화되어 있지만, AWS Control Tower는 AWS Control Tower 홈 지역에만 AWS Security Hub Finding 이벤트를 전송합니다. 자세한 내용은 Security Hub 제어 드리프트 보고를 참조하십시오.

지역 거부 제어 업데이트

이 랜딩 존 버전에는 지역 거부 컨트롤에 대한 업데이트도 포함되어 있습니다.

글로벌 서비스 및 API 추가

- AWS Billing and Cost Management (`billing:*`)
- AWS CloudTrail (`cloudtrail:LookupEvents`) 를 사용하면 멤버 계정의 글로벌 이벤트를 확인할 수 있습니다.
- AWS 통합 결제 () `consolidatedbilling:*`
- AWS 관리 콘솔 모바일 애플리케이션 (`consoleapp:*`)
- AWS 프리 티어 (`freetier:*`)
- AWS 인보이스 발행 (`invoicing:*`)
- AWS IQ () `iq:*`
- AWS 사용자 알림 () `notifications:*`
- AWS 사용자 알림 연락처 (`notifications-contacts:*`)
- Amazon Payments (`payments:*`)
- AWS 세금 설정 (`tax:*`)

글로벌 서비스 및 API 제거됨

- 유효한 조치가 `s3:GetAccountPublic` 아니기 때문에 제거되었습니다.
- 유효한 동작이 `s3:PutAccountPublic` 아니므로 제거되었습니다.

AWS Control Tower는 ID를 기반으로 계정을 처리합니다.

2023년 6월 14일

(AWS Control Tower 랜딩 존은 업데이트가 필요하지 않습니다.)

이제 AWS Control Tower는 계정 이메일 주소가 아닌 AWS 계정 ID를 추적하여 Account Factory에서 생성한 계정을 생성하고 관리합니다.

계정을 프로비저닝할 때 계정 요청자는 항상 `CreateAccount` 및 권한을 가지고 있어야 합니다. `DescribeCreateAccountStatus` 이 권한 집합은 관리자 역할의 일부이며 요청자가 관리자 역할을 맡으면 자동으로 부여됩니다. 계정을 프로비저닝할 권한을 위임하는 경우 계정 요청자를 위해 이러한 권한을 직접 추가해야 할 수 있습니다.

AWS Control Tower 제어 라이브러리에서 제공되는 추가 Security Hub 탐지 제어 항목

2023년 6월 12일

(AWS Control Tower 랜딩 존은 업데이트가 필요하지 않습니다.)

AWS Control Tower는 AWS Control Tower 제어 라이브러리에 10개의 새로운 AWS Security Hub 탐지 제어 항목을 추가했습니다. 이러한 새로운 제어 기능은 API Gateway, Amazon Elastic Compute Cloud (EC2) AWS CodeBuild, 아마존 Elastic Load Balancer, Amazon Redshift, Amazon 등과 같은 서비스를 대상으로 합니다. SageMaker AWS WAF이러한 새로운 제어 기능은 로깅 및 모니터링 설정, 네트워크 액세스 제한, 저장된 데이터 암호화와 같은 제어 목표를 충족하여 거버넌스 태세를 강화하는 데 도움이 됩니다.

이러한 제어 기능은 특정 OU에서 활성화하면 Security Hub 서비스 관리형 표준인 AWS Control Tower의 일부로 작동합니다.

- [sh.Account.1] 다음을 위한 보안 연락처 정보를 제공해야 합니다. AWS 계정
- [sh.APIGateway.8] API Gateway 경로는 권한 부여 유형을 지정해야 합니다.
- [sh.APIGateway.9] API Gateway V2 스테이지에 대한 액세스 로깅을 구성해야 합니다.
- [SH. CodeBuild.3] CodeBuild S3 로그는 암호화되어야 합니다.
- [SH.EC2.25] EC2 시작 템플릿은 네트워크 인터페이스에 퍼블릭 IP를 할당해서는 안 됩니다.
- [SH.ELB.1] 모든 HTTP 요청을 HTTPS로 리디렉션하도록 애플리케이션 로드 밸런서를 구성해야 합니다.
- [sh.Redshift.10] Redshift 클러스터는 유휴 상태에서 암호화되어야 합니다

- [SH. SageMaker.2] SageMaker 노트북 인스턴스는 커스텀 VPC에서 시작해야 합니다.
- [SH. SageMaker.3] 사용자에게 SageMaker 노트북 인스턴스에 대한 루트 액세스 권한이 없어야 합니다.
- [SH.WAF.10] WAFV2 웹 ACL에는 하나 이상의 규칙 또는 규칙 그룹이 있어야 합니다.

새로운 AWS Security Hub 탐지 제어 기능은 AWS Control Tower가 제공되는 모든 AWS 리전 곳에서 사용할 수 있습니다. 이러한 규제 항목에 대한 자세한 내용은 서비스 관리형 표준에 적용되는 규제: AWS Control Tower를 참조하십시오.

AWS Control Tower는 제어 메타데이터 테이블을 게시합니다.

2023년 6월 7일

(AWS Control Tower 랜딩 존은 업데이트가 필요하지 않습니다.)

AWS Control Tower는 이제 게시된 설명서의 일부로 제어 메타데이터의 전체 표를 제공합니다. 제어 API로 작업할 때 각 컨트롤의 API ControlIdentifier를 조회할 수 있으며, 이는 각 컨트롤과 관련된 고유한 ARN입니다. AWS 리전표에는 각 컨트롤이 다루는 프레임워크와 규제 목표가 포함되어 있습니다. 이전에는 이 정보를 콘솔에서만 사용할 수 있었습니다.

이 표에는 AWS Security Hub 서비스 관리형 표준:AWS Control Tower의 일부인 Security Hub 컨트롤에 대한 메타데이터도 포함되어 있습니다. 자세한 내용은 제어 메타데이터 표를 참조하십시오.

제어 식별자의 간략한 목록과 일부 사용 예는 API 및 컨트롤의 리소스 식별자를 참조하십시오.

Account Factory 커스터마이징을 위한 테라폼 지원

2023년 6월 6일

(AWS Control Tower 랜딩 존은 업데이트가 필요하지 않습니다.)

AWS Control Tower는 AFC (어카운트 팩토리 사용자 지정) 를 통해 Terraform에 대한 단일 리전 지원을 제공합니다. 이번 릴리스부터 AWS Control Tower와 Service Catalog를 함께 사용하여 Terraform 오픈 소스에서 AFC 계정 블루프린트를 정의할 수 있습니다. AWS Control Tower에서 리소스를 프로비저닝하기 전에 새 리소스와 기존 AWS 계정리소스를 사용자 지정할 수 있습니다. 기본적으로 이 기능을 사용하면 AWS Control Tower 홈 리전에서 Terraform을 사용하여 계정을 배포하고 업데이트할 수 있습니다.

계정 청사진은 프로비저닝 시 필요한 특정 리소스 및 구성을 설명합니다. AWS 계정 블루프린트를 템플릿으로 사용하여 대규모로 여러 개를 만들 수 있습니다. AWS 계정

시작하려면 Terraform 참조 엔진을 켜서 사용하세요. GitHub 참조 엔진은 Terraform 오픈 소스 엔진이 Service Catalog와 함께 작동하는 데 필요한 코드 및 인프라를 구성합니다. 이 일회성 설정 프로세스는 몇 분 정도 걸립니다. 그런 다음 Terraform에서 사용자 지정 계정 요구 사항을 정의한 다음 잘 정의된 AWS Control Tower 계정 팩토리 워크플로를 사용하여 계정을 배포할 수 있습니다. Terraform을 선호하는 고객은 AFC를 통해 대규모로 AWS Control Tower 계정 사용자 지정을 활용하고 프로비저닝된 후 각 계정에 즉시 액세스할 수 있습니다.

이러한 사용자 지정을 만드는 방법을 알아보려면 Service Catalog 설명서에서 제품 만들기 및 Terraform 오픈 소스 시작하기를 참조하십시오. 이 기능은 AWS Control Tower가 제공되는 모든 AWS 리전 곳에서 사용할 수 있습니다.

AWS 랜딩 존에 IAM 아이덴티티 센터 자체 관리 기능 사용 가능

2023년 6월 6일

(AWS Control Tower 랜딩 존은 업데이트가 필요하지 않습니다.)

이제 AWS Control Tower는 설치 또는 업데이트 중에 구성할 수 있는 AWS Control Tower 랜딩 존에 대한 선택적 자격 증명 공급자 선택을 지원합니다. 다중 계정을 사용한 환경 구성에 정의된 모범 사례 지침에 따라 기본적으로 landing Zone은 AWS IAM Identity Center를 사용하도록 설정되어 있습니다 AWS. 이제 세 가지 대안이 있습니다.

- 기본 설정을 그대로 사용하고 AWS Control Tower에서 AWS IAM ID 센터를 설치하고 관리하도록 허용할 수 있습니다.
- 특정 비즈니스 요구 사항을 반영하여 AWS IAM ID 센터를 자체 관리하도록 선택할 수 있습니다.
- 필요한 경우 IAM Identity Center를 통해 연결하여 타사 ID 공급자를 가져와 자체 관리할 수도 있습니다. 규제 환경에 따라 특정 공급자를 사용해야 하거나 AWS IAM Identity Center를 사용할 수 AWS 리전 없는 곳에서 사업을 운영하는 경우 ID 공급자 옵션을 사용해야 합니다.

자세한 정보는 IAM ID 센터 지침을 참조하세요.

계정 수준에서 ID 제공자를 선택하는 것은 지원되지 않습니다. 이 기능은 전체 착륙 지대에만 적용됩니다. AWS Control Tower 자격 증명 공급자 옵션은 AWS Control AWS 리전 Tower가 있는 모든 곳에서 이용할 수 있습니다.

AWS Control Tower는 OU의 복합 거버넌스를 해결합니다.

2023년 6월 1일

(AWS Control Tower 랜딩 존은 업데이트가 필요하지 않습니다.)

이번 릴리스부터 AWS Control Tower는 OU가 복합 거버넌스 상태인 경우 제어 항목이 조직 단위 (OU)에 배포되는 것을 방지합니다. AWS Control Tower가 거버넌스를 새로운 AWS 리전것으로 확장하거나 거버넌스를 제거한 후 계정이 업데이트되지 않으면 OU에서 혼합 거버넌스가 발생합니다. 이 릴리스는 해당 OU의 회원 계정을 일관된 규정 준수를 유지하는 데 도움이 됩니다. 자세한 정보는 지역을 구성할 때 복합 거버넌스를 피하세요.을 참조하세요.

추가 사전 예방 제어 기능을 사용할 수 있습니다.

2023년 5월 19일

(AWS Control Tower 랜딩 존은 업데이트가 필요하지 않습니다.)

AWS Control Tower는 다중 계정 환경을 관리하고 저장된 데이터 암호화 또는 네트워크 액세스 제한과 같은 특정 규제 목표를 충족하는 데 도움이 되는 28개의 새로운 사전 예방 제어를 추가하고 있습니다. 리소스를 프로비저닝하기 전에 리소스를 확인하는 AWS CloudFormation 후크를 통해 사전 예방적 제어가 구현됩니다. 새로운 제어 기능은 아마존 AWS 서비스, 아마존 EC2 Auto Scaling, 아마존, 아마존 API Gateway, SageMaker 아마존 관계형 데이터베이스 OpenSearch 서비스 (RDS) 와 같은 서비스를 관리하는 데 도움이 될 수 있습니다.

사전 예방적 제어는 AWS Control AWS 리전 Tower가 제공되는 모든 상업에서 지원됩니다.

아마존 OpenSearch 서비스

- [CT.OPENSEARCH.PR.1] 저장된 데이터를 암호화하려면 Elasticsearch 도메인이 필요합니다.
- [CT.OPENSEARCH.PR.2] 사용자 지정 아마존 VPC에서 엘라스틱서치 도메인을 생성해야 함
- [CT.OPENSEARCH.PR.3] 노드 간에 전송되는 데이터를 암호화하려면 Elasticsearch 도메인이 필요합니다.
- [CT.OPENSEARCH.PR.4] 오류 로그를 Amazon Logs로 보내려면 Elasticsearch 도메인이 필요합니다 CloudWatch
- [CT.OPENSEARCH.PR.5] 감사 로그를 Amazon Logs로 전송하려면 Elasticsearch 도메인이 필요합니다. CloudWatch
- [CT.OPENSEARCH.PR.6] 영역 인식 기능을 갖추려면 Elasticsearch 도메인에 최소 3개의 데이터 노드가 있어야 합니다.
- [CT.OPENSEARCH.PR.7] Elasticsearch 도메인에 최소 세 개의 전용 마스터 노드가 있어야 합니다.
- [CT.OPENSEARCH.PR.8] TLSv1.2를 사용하려면 엘라스틱서치 서비스 도메인이 필요합니다
- [CT.OPENSEARCH.PR.9] 저장된 데이터를 암호화하려면 Amazon OpenSearch 서비스 도메인이 필요합니다.

- [CT.OPENSEARCH.PR.10] 사용자가 지정한 아마존 VPC에서 OpenSearch 아마존 서비스 도메인을 생성하도록 요구
- [CT.OPENSEARCH.PR.11] 노드 간에 전송되는 데이터를 암호화하려면 OpenSearch Amazon 서비스 도메인이 필요합니다.
- [CT.OPENSEARCH.PR.12] 아마존 로그에 오류 로그를 보내려면 OpenSearch 아마존 서비스 도메인이 필요합니다. CloudWatch
- [CT.OPENSEARCH.PR.13] Amazon Logs에 감사 로그를 보내려면 OpenSearch 아마존 서비스 도메인이 필요합니다. CloudWatch
- [CT.OPENSEARCH.PR.14] OpenSearch Amazon 서비스 도메인에 영역 인식 및 최소 세 개의 데이터 노드가 있어야 함
- [CT.OPENSEARCH.PR.15] 세분화된 액세스 제어를 사용하려면 Amazon OpenSearch 서비스 도메인이 필요합니다.
- [CT.OPENSEARCH.PR.16] TLSv1.2를 사용하려면 아마존 서비스 도메인이 필요합니다 OpenSearch

Amazon EC2 Auto Scaling

- [CT.AUTOSCALING.PR.1] Amazon EC2 Auto Scaling 그룹에 여러 가용 영역이 있어야 함
- [CT.AUTOSCALING.PR.2] IMDSv2용으로 Amazon EC2 인스턴스를 구성하려면 Amazon EC2 Auto Scaling 그룹 시작 구성이 필요합니다.
- [CT.AUTOSCALING.PR.3] Amazon EC2 Auto Scaling 시작 구성에는 단일 홉 메타데이터 응답 제한이 있어야 합니다.
- [CT.AUTOSCALING.PR.4] Amazon Elastic Load Balancing (ELB) 과 연결된 Amazon EC2 Auto Scaling 그룹에 ELB 상태 확인을 활성화해야 합니다.
- [CT.AUTOSCALING.PR.5] Amazon EC2 Auto Scaling 그룹 시작 구성에는 퍼블릭 IP 주소를 가진 Amazon EC2 인스턴스가 없어야 합니다.
- [CT.AUTOSCALING.PR.6] 모든 Amazon EC2 Auto Scaling 그룹에는 여러 인스턴스 유형을 사용해야 합니다.
- [CT.AUTOSCALING.PR.8] Amazon EC2 Auto Scaling 그룹에 EC2 시작 템플릿을 구성해야 함

아마존 SageMaker

- [CT.SAGEMAKER.PR.1] 인터넷에 직접 액세스하지 못하도록 Amazon SageMaker 노트북 인스턴스가 필요합니다.

- [CT.SAGEMAKER.PR.2] 사용자 지정 아마존 VPC 내에 SageMaker 아마존 노트북 인스턴스를 배포해야 함
- [CT.SAGEMAKER.PR.3] Amazon 노트북 인스턴스에 루트 액세스가 허용되지 않도록 요구 SageMaker

Amazon API Gateway

- [CT.APIGATEWAY.PR.5] 인증 유형을 지정하려면 Amazon API Gateway V2 웹 소켓 및 HTTP 경로가 필요합니다.

Amazon Relational Database Service(RDS)

- [CT.RDS.PR.25] Amazon RDS 데이터베이스 클러스터에 로깅이 구성되어 있어야 합니다.

자세한 내용은 사전 제어를 참조하십시오.

Amazon EC2 사전 예방 제어 업데이트

2023년 5월 2일

(AWS Control Tower 랜딩 존은 업데이트가 필요하지 않습니다.)

AWS Control Tower는 두 가지 사전 예방 제어 항목, 즉, CT.EC2.PR.3 을 CT.EC2.PR.4 업데이트했습니다.

업데이트된 CT.EC2.PR.3 컨트롤의 경우, 포트 80 또는 443을 제외한 보안 그룹 리소스의 접두사 목록을 참조하는 모든 AWS CloudFormation 배포는 배포가 차단됩니다.

업데이트된 CT.EC2.PR.4 컨트롤의 경우 포트가 3389, 20, 23, 110, 143, 3306, 8080, 1433, 9200, 9300, 25, 445, 135, 21, 1434, 4333, 5432, 5500, 5601, 22, 3000, 5000, 8088, 8888이면 보안 그룹 리소스의 접두사 목록을 참조하는 모든 AWS CloudFormation 배포가 차단됩니다.

7개의 추가 사용 가능 AWS 리전

2023년 4월 19일

(AWS Control Tower 랜딩 존은 업데이트가 필요하지 않습니다.)

이제 AWS Control Tower를 캘리포니아 북부 (샌프란시스코), 아시아 태평양 (홍콩, 자카르타, 오사카), 유럽 (밀라노), 중동 (바레인), 아프리카 (케이프타운) 등 7개 지역에서 추가로 사용할 수 AWS 리전있습

니다. 옵트인 지역이라고 하는 AWS Control Tower의 이러한 추가 지역은 기본적으로 활성화되지 않습니다. 단, 기본적으로 활성화되는 미국 서부 (캘리포니아 북부) 지역은 예외입니다.

AWS Control Tower의 일부 컨트롤은 AWS Control Tower가 제공되는 추가 AWS 리전 지역 중 일부에서는 작동하지 않습니다. 해당 지역은 필수 기본 기능을 지원하지 않기 때문입니다. 자세한 내용은 관리 제한단원을 참조하세요.

이러한 새 지역 중 아시아 태평양 (자카르타 및 오사카) 에서는 cFCT를 사용할 수 없습니다. 다른 지역의 이용 가능 여부는 변함이 없습니다 AWS 리전 .

AWS Control Tower가 지역 및 규제 항목의 제한을 관리하는 방법에 대한 자세한 내용은 을 참조하십시오옵트인 지역 활성화 AWS 고려 사항.

AFT에서 요구하는 VPCE 엔드포인트는 중동 (바레인) 지역에서는 사용할 수 없습니다. 이 지역에 AFT를 배포하는 고객은 매개변수를 사용하여 배포해야 합니다. `aft_vpc_endpoints=false` 자세한 내용은 README 파일의 매개변수를 참조하십시오.

Amazon EC2의 제한으로 인해 AWS Control Tower VPC는 미국 서부 (캘리포니아 북부) 지역에 두 개의 가용 영역을 보유하고 있습니다. `us-west-1` 미국 서부 (캘리포니아 북부) 에서는 6개의 서브넷이 두 가용 영역에 분산되어 있습니다. 자세한 정보는 AWS Control 타워 및 VPC의 개요을 참조하세요.

AWS Control `GetRegionOptStatus` Tower는 AWS Control Tower가 AWS 계정 관리 서비스를 통해 구현된 API 및 API를 호출할 수 `AWSControlTowerServiceRolePolicy` 있도록 하는 새로운 권한을 추가하여, 랜딩 존의 공유 계정 (Management 계정, 로그 아카이브 계정, 감사 계정) 및 OU 회원 계정에서 이러한 추가 기능을 AWS 리전 사용할 수 있도록 했습니다. `EnableRegion` `ListRegions` 자세한 정보는 AWS Control Tower의 관리형 정책을 참조하세요.

Account Factory for Terraform (AFT) 계정 사용자 지정 요청 추적

2023년 2월 16일

AFT는 계정 사용자 지정 요청 추적을 지원합니다. 계정 사용자 지정 요청을 제출할 때마다 AFT는 AFT 사용자 지정 AWS Step Functions 상태 시스템을 통과하는 고유한 추적 토큰을 생성하며, 이 시스템은 실행의 일부로 토큰을 기록합니다. Amazon CloudWatch Logs 인사이트 쿼리를 사용하여 타임스탬프 범위를 검색하고 요청 토큰을 검색할 수 있습니다. 따라서 토큰과 함께 제공되는 페이로드를 확인할 수 있으므로 전체 AFT 워크플로에서 계정 사용자 지정 요청을 추적할 수 있습니다. AFT에 대한 자세한 내용은 Terraform용 AWS Control Tower 어카운트 팩토리 개요를 참조하십시오. CloudWatch 로그 및 Step Functions에 대한 자세한 내용은 다음을 참조하십시오.

- 아마존 CloudWatch 로그란 무엇입니까? Amazon CloudWatch Logs 사용 설명서에서

- 무엇입니까 AWS Step Functions? AWS Step Functions 개발자 안내서에서

AWS 컨트롤 타워 랜딩 존 버전 3.1

2023년 2월 9일

(AWS Control Tower landzone을 버전 3.1로 업데이트하려면 업데이트가 필요합니다. 자세한 내용은 참조랜딩 영역 업데이트)

AWS Control Tower 랜딩 존 버전 3.1에는 다음과 같은 업데이트가 포함되어 있습니다.

- 이번 릴리스부터 AWS Control Tower는 액세스 로깅 버킷 (Log Archive 계정에 액세스 로그가 저장되는 Amazon S3 버킷) 에 대한 불필요한 액세스 로깅을 비활성화하는 동시에 S3 버킷에 대한 서버 액세스 로깅을 계속 활성화합니다. 또한 이번 릴리스에는 플랜 및 같은 글로벌 서비스에 대한 추가 작업을 허용하는 지역 거부 제어에 대한 업데이트도 포함되어 있습니다. AWS Support AWS Artifact
- AWS Control Tower 액세스 로깅 버킷에 대한 서버 액세스 로깅을 비활성화하면 Security Hub가 Log Archive 계정의 액세스 로깅 버킷에 대한 검색 결과를 생성합니다. AWS Security Hub 규칙에 따라 [S3.9] S3 버킷 서버 액세스 로깅이 활성화되어야 합니다. Security Hub에 따라 이 규칙의 Security Hub 설명에 명시된 대로 이 특정 검색 결과를 숨기는 것이 좋습니다. 자세한 내용은 숨겨진 검색 결과에 대한 정보를 참조하십시오.
- Log Archive 계정의 (일반) 로깅 버킷에 대한 액세스 로깅은 버전 3.1에서 변경되지 않았습니다. 모범 사례에 따라 해당 버킷의 액세스 이벤트는 액세스 로깅 버킷에 로그 항목으로 기록됩니다. 액세스 로깅에 대한 자세한 내용은 Amazon S3 설명서의 서버 액세스 로깅을 사용한 요청 로깅을 참조하십시오.
- 지역 거부 제어를 업데이트했습니다. 이 업데이트를 통해 더 많은 글로벌 서비스에서 조치를 취할 수 있습니다. 이 SCP에 대한 자세한 내용은 요청에 AWS 따른 액세스 거부 AWS 리전 및 데이터 상주 보호를 강화하는 제어를 참조하십시오.

  글로벌 서비스 추가:

  - AWS Account Management (`account:*`)
  - AWS 활성화 (`activate:*`)
  - AWS Artifact (`artifact:*`)
  - AWS Billing Conductor (`billingconductor:*`)
  - AWS Compute Optimizer (`compute-optimizer:*`)
  - AWS Data Pipeline (`datapipeline:GetAccountLimits`)
  - AWS Device Farm(`devicefarm:*`)

- AWS Marketplace (`discovery-marketplace:*`)
- 아마존 ECR () `ecr-public:*`
- AWS License Manager (`license-manager:ListReceivedLicenses`)
- AWS `lightsail:Get*`Lightsail ()
- AWS 리소스 탐색기 (`resource-explorer-2:*`)
- 아마존 S3 (`s3:CreateMultiRegionAccessPoint,s3:GetBucketPolicyStatus,s3:PutMultiRegionAcc`
- AWS Savings Plan (`savingsplans:*`)
- IAM 아이덴티티 센터 () `sso:*`
- AWS Support App (`supportapp:*`)
- AWS Support 플랜 () `supportplans:*`
- AWS 지속가능성 (`sustainability:*`)
- AWS Resource Groups Tagging API (`tag:GetResources`)
- AWS Marketplace 공급업체 인사이트 (`vendor-insights:ListEntitledSecurityProfiles`)

사전 예방적 통제가 일반적으로 이용 가능

2023년 1월 24일

(AWS Control Tower 랜딩 존은 업데이트가 필요하지 않습니다.)

이전에 미리 보기 상태로 발표되었던 선택적 사전 예방 제어를 이제 정식 버전으로 사용할 수 있습니다. 이러한 컨트롤은 리소스를 배포하기 전에 리소스를 점검하여 새 리소스가 사용자 환경에서 활성화된 제어를 준수하는지 확인하기 때문에 사전 예방적이라고 합니다. 자세한 정보는 포괄적인 제어는 AWS 리소스 공급 및 관리를 지원합니다.을 참조하세요.

2022년 1월 - 12월

2022년에 AWS Control Tower는 다음과 같은 업데이트를 발표했습니다.

- 동시 계정 운영
- 어카운트 팩토리 커스터마이징 (AFC)
- 포괄적인 제어는 AWS 리소스 공급 및 관리를 지원합니다.

- 모든 AWS Config 규칙의 규정 준수 상태를 볼 수 있습니다.
- 제어용 API 및 새 리소스 AWS CloudFormation
- CFCT는 스택 세트 삭제를 지원합니다.
- 맞춤형 로그 보존
- 롤 드리프트 수리 가능
- AWS 컨트롤 타워 랜딩 존 버전 3.0
- 조직 페이지는 OU와 계정의 관점을 통합합니다.
- 개별 회원 계정의 등록 및 업데이트가 더 쉬워졌습니다.
- AFT는 공유 AWS Control Tower 계정에 대한 자동 사용자 지정을 지원합니다.
- 모든 선택적 컨트롤에 대한 동시 작업
- 기존 보안 및 로깅 계정
- AWS 컨트롤 타워 랜딩 존 버전 2.9
- AWS 컨트롤 타워 랜딩 존 버전 2.8

동시 계정 운영

2022년 12월 16일

(AWS Control Tower 랜딩 존은 업데이트가 필요하지 않습니다.)

AWS Control Tower는 이제 어카운트 팩토리에서의 동시 작업을 지원합니다. 한 번에 최대 5개의 계정을 생성, 업데이트 또는 등록할 수 있습니다. 백그라운드에서 계정 구축이 완료되는 동안 최대 5개의 작업을 연속으로 제출하고 각 요청의 완료 상태를 확인할 수 있습니다. 예를 들어, 더 이상 다른 계정을 업데이트하거나 전체 OU (조직 구성 단위) 를 다시 등록하기 전에 각 프로세스가 완료될 때까지 기다릴 필요가 없습니다.

어카운트 팩토리 커스터마이징 (AFC)

2022년 11월 28일

(AWS Control Tower 랜딩 존은 업데이트가 필요하지 않습니다.)

계정 팩토리 사용자 지정을 사용하면 AWS Control Tower 콘솔 내에서 신규 및 기존 계정을 사용자 지정할 수 있습니다. 이러한 새로운 사용자 지정 기능을 사용하면 전문 Service Catalog 제품에 포함된 AWS CloudFormation 템플릿인 계정 블루프린트를 유연하게 정의할 수 있습니다. 블루프린트는 완전

히 커스터마이징된 리소스와 구성을 제공합니다. 특정 사용 사례에 맞게 계정을 사용자 지정하는 데 도움이 되는 AWS 파트너가 구축하고 관리하는 사전 정의된 블루프린트를 사용할 수도 있습니다.

이전에는 AWS Control Tower 어카운트 팩토리가 콘솔에서의 계정 사용자 지정을 지원하지 않았습니다. 이번 어카운트 팩토리 업데이트를 통해 계정 요구 사항을 미리 정의하고 이를 잘 정의된 워크플로의 일부로 구현할 수 있습니다. 블루프린트를 적용하여 새 계정을 만들고, 다른 AWS 계정을 AWS Control Tower에 등록하고, 기존 AWS Control Tower 계정을 업데이트할 수 있습니다.

어카운트 팩토리에서 계정을 프로비저닝, 등록 또는 업데이트할 때 배포할 블루프린트를 선택하게 됩니다. 블루프린트에 지정된 리소스는 계정에 프로비저닝됩니다. 계정 구축이 완료되면 모든 사용자 지정 구성을 즉시 사용할 수 있습니다.

계정 사용자 지정을 시작하려면 Service Catalog 제품에서 원하는 사용 사례에 맞는 리소스를 정의하면 됩니다. AWS 시작 라이브러리에서 파트너 관리형 솔루션을 선택할 수도 있습니다. 자세한 정보는 AFC (Account Factory Customize) 로 계정을 사용자 지정하세요을 참조하세요.

포괄적인 제어는 AWS 리소스 공급 및 관리를 지원합니다.

2022년 11월 28일

(AWS Control Tower 랜딩 존은 업데이트가 필요하지 않습니다.)

AWS Control Tower는 이제 AWS CloudFormation 후크를 통해 구현되는 새롭고 선택적인 사전 예방 제어를 포함하여 포괄적인 제어 관리를 지원합니다. 이러한 컨트롤은 리소스를 배포하기 전에 리소스를 점검하여 새 리소스가 사용자 환경에서 활성화된 제어를 준수하는지 여부를 결정하기 때문에 사전 예방적이라고 합니다.

130개 이상의 새로운 사전 예방 제어를 통해 AWS Control Tower 환경의 특정 정책 목표를 달성하고, 업계 표준 규정 준수 프레임워크의 요구 사항을 충족하고, 20개 이상의 다른 서비스에 걸친 AWS Control Tower 상호 작용을 관리할 수 있습니다. AWS

AWS Control Tower 규제 라이브러리는 관련 AWS 서비스 및 리소스에 따라 이러한 제어를 분류합니다. 자세한 내용은 사전 예방적 제어를 참조하십시오.

이번 릴리스에서 AWS Control Tower는 AWS 기본 보안 모범 사례 (FSBP) 표준을 지원하는 새로운 Security Hub 서비스 관리형 표준인 AWS Control Tower와도 AWS Security Hub통합됩니다. 콘솔에서 160개 이상의 Security Hub 제어 항목을 AWS Control Tower 컨트롤과 함께 볼 수 있으며, AWS Control Tower 환경에 대한 Security Hub 보안 점수를 받을 수 있습니다. 자세한 내용은 Security Hub 컨트롤을 참조하십시오.

모든 AWS Config 규칙의 규정 준수 상태를 볼 수 있습니다.

2022년 11월 18일

(AWS Control Tower 랜딩 존은 업데이트가 필요하지 않습니다.)

이제 AWS Control Tower는 AWS Control Tower에 등록된 조직 단위에 배포된 모든 AWS Config 규칙의 규정 준수 상태를 표시합니다. AWS Control Tower 콘솔 외부로 이동하지 않고도 등록 여부에 관계없이 AWS Control Tower에서 계정에 영향을 미치는 모든 AWS Config 규칙의 규정 준수 상태를 확인할 수 있습니다. 고객은 AWS Control Tower에서 탐지 제어라고 하는 Config 규칙을 설정하거나 서비스를 통해 직접 설정할 수 있습니다. AWS Config 에서 배포한 AWS Config 규칙이 AWS Control Tower에서 배포한 규칙과 함께 표시됩니다.

이전에는 AWS Config 서비스를 통해 배포된 AWS Config 규칙이 AWS Control Tower 콘솔에 표시되지 않았습니다. 고객은 AWS Config 서비스를 탐색하여 규정을 준수하지 않는 AWS Config 규칙을 식별해야 했습니다. 이제 AWS Control Tower 콘솔에서 규정을 준수하지 않는 AWS Config 규칙을 식별할 수 있습니다. 모든 Config 규칙의 규정 준수 상태를 보려면 AWS Control Tower 콘솔의 계정 세부 정보 페이지로 이동하십시오. AWS Control Tower에서 관리하는 컨트롤의 규정 준수 상태와 AWS Control Tower 외부에 배포된 Config 규칙을 보여주는 목록이 표시됩니다.

제어용 API 및 새 리소스 AWS CloudFormation

2022년 9월 1일

(AWS Control Tower 랜딩 존은 업데이트가 필요하지 않습니다.)

AWS Control Tower는 이제 일련의 API 호출을 통해 가드레일이라고도 하는 프로그래밍 방식의 제어 관리를 지원합니다. 새 AWS CloudFormation 리소스는 제어를 위한 API 기능을 지원합니다. 자세한 내용은 AWS Control Tower에서의 작업 자동화 및 를 사용하여 AWS Control Tower 리소스 생성 AWS CloudFormation 단원을 참조하세요.

이러한 API를 사용하면 AWS Control Tower 라이브러리에서 제어를 활성화 및 비활성화하고 적용 상태를 확인할 수 있습니다. API에는 에 대한 AWS CloudFormation지원이 포함되어 있으므로 infrastructure-as-code (IaC) 으로 AWS 리소스를 관리할 수 있습니다. AWS Control Tower는 전체 조직 단위 (OU) 및 OU 내 모든 AWS 계정에 대한 정책 의도를 표현하는 선택적 예방 및 탐지 제어를 제공합니다. 이러한 규칙은 새 계정을 생성하거나 기존 계정을 변경할 때도 계속 유효합니다.

이번 릴리스에 포함된 API

- EnableControl— 이 API 호출은 컨트롤을 활성화합니다. 지정된 조직 구성 단위와 여기에 포함된 계정에 AWS 리소스를 만드는 비동기 작업을 시작합니다.

- DisableControl— 이 API 호출은 컨트롤을 끕니다. 지정된 조직 단위의 AWS 리소스와 해당 조직 단위에 포함된 계정을 삭제하는 비동기 작업을 시작합니다.
- GetControlOperation— 특정 OR 작업의 상태를 반환합니다. EnableControlDisableControl
- ListEnabledControls— 지정된 조직 구성 단위에서 AWS Control Tower가 활성화한 컨트롤과 해당 구성 단위에 포함된 계정을 나열합니다.

선택적 컨트롤의 컨트롤 이름 목록을 보려면 AWS Control Tower 사용 설명서의 API 및 컨트롤용 리소스 식별자를 참조하십시오.

CFCT는 스택 세트 삭제를 지원합니다.

2022년 8월 26일

(AWS Control Tower 랜딩 존은 업데이트가 필요하지 않습니다.)

AWS Control Tower (cFCT) 에 대한 사용자 지정은 이제 파일에 파라미터를 설정하여 스택 세트 삭제를 지원합니다. `manifest.yaml` 자세한 정보는 스택 세트 삭제을 참조하세요.

> **Important**
>
> 처음에 값을 `enable_stack_set_deletion` ~로 `true` 설정하면 다음에 cFCT를 호출할 때 접두사로 `CustomControlTower-` 시작하고 관련 키 태그가 `Key:AWS_Solutions, Value: CustomControlTowerStackSet` 있지만 매니페스트 파일에 선언되지 않은 모든 리소스가 삭제 스테이징됩니다.

맞춤형 로그 보존

2022년 8월 15일

(AWS Control Tower 랜딩 존에는 업데이트가 필요합니다. 자세한 내용은 참조랜딩 영역 업데이트)

AWS Control Tower는 이제 AWS Control Tower CloudTrail 로그를 저장하는 Amazon S3 버킷의 보존 정책을 사용자 지정하는 기능을 제공합니다. Amazon S3 로그 보존 정책을 일 또는 년 단위로 최대 15년까지 사용자 지정할 수 있습니다.

로그 보존을 사용자 지정하지 않기로 선택한 경우 기본 설정은 표준 계정 로깅의 경우 1년, 액세스 로깅의 경우 10년입니다.

이 기능은 랜딩 존을 업데이트하거나 복구할 때 AWS Control Tower를 통해 기존 고객이 사용할 수 있고, 신규 고객은 AWS Control Tower 설치 프로세스를 통해 사용할 수 있습니다.

롤 드리프트 수리 가능

2022년 8월 11일

(AWS Control Tower 랜딩 존은 업데이트가 필요하지 않습니다.)

AWS Control Tower는 이제 역할 드리프트에 대한 복구를 지원합니다. landing Zone을 완전히 복구하지 않고도 필요한 역할을 복원할 수 있습니다. 이러한 유형의 드리프트 복구가 필요한 경우 콘솔 오류 페이지에 역할을 복원하는 단계가 제공되므로 랜딩 존을 다시 사용할 수 있습니다.

AWS 컨트롤 타워 랜딩 존 버전 3.0

2022년 7월 29일

(AWS Control Tower 랜딩 존을 버전 3.0으로 업데이트하려면 업데이트가 필요합니다. 자세한 내용은 참조랜딩 영역 업데이트)

AWS Control Tower 랜딩 존 버전 3.0에는 다음과 같은 업데이트가 포함되어 있습니다.

- 조직 수준의 AWS CloudTrail 트레일을 선택하거나 AWS Control Tower에서 관리하는 트레일을 CloudTrail 옵트아웃할 수 있는 옵션입니다.
- 계정에서의 로그 활동 여부를 AWS CloudTrail 판단하기 위한 두 가지 새로운 탐지 제어 기능.
- 거주 지역의 글로벌 리소스에 대한 AWS Config 정보만 집계하는 옵션입니다.
- 지역 거부 제어에 대한 업데이트.
- 관리형 정책 업데이트, AWSControlTowerServiceRolePolicy.
- 등록된 각 `aws-controltower/CloudTrailLogs` 계정에서 더 이상 IAM `aws-controltower-CloudWatchLogsRole` 역할과 CloudWatch 로그 그룹을 생성하지 않습니다. 이전에는 계정 추적을 위해 각 계정에서 이러한 계정을 생성했습니다. 조직 트레일의 경우 관리 계정에는 하나의 트레일만 생성합니다.

다음 섹션에서는 각각의 새로운 기능에 대한 자세한 내용을 제공합니다.

AWS Control Tower의 조직 수준 CloudTrail 트레일

Landing Zone 버전 3.0을 통해 AWS Control Tower는 이제 조직 수준의 트레일을 AWS CloudTrail 지원합니다.

AWS Control Tower 랜딩 존을 버전 3.0으로 업데이트하면 조직 수준의 AWS CloudTrail 트레일을 로깅 기본 설정으로 선택하거나 AWS Control Tower에서 관리하는 CloudTrail 트레일을 옵트아웃할 수 있습니다. 버전 3.0으로 업데이트하면 AWS Control Tower는 24시간의 대기 기간 후에 등록된 계정의 기존 계정 수준 트레일을 삭제합니다. AWS Control Tower는 등록되지 않은 계정의 계정 수준 트레일을 삭제하지 않습니다. 드물긴 하지만 랜딩 존 업데이트가 성공하지 못했지만 AWS Control Tower가 이미 조직 수준의 트레일을 생성한 이후에 오류가 발생하는 경우, 업데이트 작업이 성공적으로 완료될 때까지 조직 수준 및 계정 수준 트레일에 대해 중복 요금이 발생할 수 있습니다.

랜딩 존 3.0부터 AWS Control Tower는 관리하는 계정 수준의 트레일을 더 이상 지원하지 않습니다. AWS 대신 AWS Control Tower는 선택에 따라 활성 또는 비활성 상태의 조직 수준 트레일을 생성합니다.

> **Note**
>
> 버전 3.0 이상으로 업데이트한 후에는 AWS Control Tower에서 관리하는 계정 수준 CloudTrail 트레일을 계속 사용할 수 없습니다.

로그가 저장된 기존 Amazon S3 버킷에 남아 있기 때문에 집계된 계정 로그에서는 로깅 데이터가 손실되지 않습니다. 트레일만 삭제되고 기존 로그는 삭제되지 않습니다. 조직 수준 트레일을 추가하는 옵션을 선택하면 AWS Control Tower는 Amazon S3 버킷 내 새 폴더의 새 경로를 열고 해당 위치로 로깅 정보를 계속 전송합니다. AWS Control Tower에서 관리하는 트레일을 옵트아웃하는 경우 기존 로그는 변경되지 않고 버킷에 남아 있습니다.

로그 스토리지의 경로 명명 규칙

- 계정 추적 로그는 다음 형식의 경로로 저장됩니다. `/org id/AWSLogs/…`
- 조직 추적 로그는 다음 형식의 경로와 함께 저장됩니다. `/org id/AWSLogs/org id/…`

AWS Control Tower가 조직 수준 CloudTrail 트레일에 대해 생성하는 경로는 다음과 같은 형식을 갖는 수동으로 생성한 조직 수준 트레일의 기본 경로와 다릅니다.

- `/AWSLogs/org id/…`

경로 이름 지정에 대한 자세한 내용은 로그 파일 찾기를 참조하십시오. CloudTrail CloudTrail

> **Tip**
>
> 계정 수준의 트레일을 직접 생성하고 관리할 계획이라면 AWS Control Tower landing zone 버전 3.0으로 업데이트를 완료하기 전에 새 트레일을 생성하여 즉시 로깅을 시작하는 것이 좋습니다.

언제든지 계정 수준 또는 조직 CloudTrail 수준의 새 트레일을 생성하고 직접 관리할 수 있습니다. AWS Control Tower에서 관리하는 조직 수준의 CloudTrail 트레일을 선택할 수 있는 옵션은 랜딩 존을 버전 3.0 이상으로 업데이트하는 동안 사용할 수 있습니다. landing Zone을 업데이트할 때마다 조직 수준의 트레일을 옵트인하거나 옵트아웃할 수 있습니다.

타사 서비스에서 로그를 관리하는 경우 서비스에 새 경로 이름을 지정해야 합니다.

> **Note**
>
> 버전 3.0 이상의 랜딩 존의 경우, AWS Control Tower는 계정 수준 AWS CloudTrail 트레일을 지원하지 않습니다. 언제든지 자체 계정 수준 트레일을 생성 및 유지 관리할 수 있으며, AWS Control Tower에서 관리하는 조직 수준 트레일을 선택할 수도 있습니다.

홈 리전의 리소스만 기록하십시오. AWS Config

Landing Zone 버전 3.0에서 AWS Control Tower는 홈 지역에만 글로벌 리소스를 기록하도록 기준 구성을 업데이트했습니다. AWS Config 버전 3.0으로 업데이트한 후에는 글로벌 리소스에 대한 리소스 기록이 홈 지역에서만 활성화됩니다.

이 구성은 모범 사례로 간주됩니다. AWS Security Hub 및 에서 권장하는 방식이며 AWS Config, 글로벌 리소스를 생성, 수정 또는 삭제할 때 생성되는 구성 항목의 수를 줄여 비용을 절감할 수 있습니다. 이전에는 고객이나 AWS 서비스에 의해 글로벌 리소스가 생성, 업데이트 또는 삭제될 때마다 각 관리 지역의 각 항목에 대해 구성 항목이 생성되었습니다.

로깅을 위한 두 가지 새로운 탐지 제어 AWS CloudTrail

조직 수준 AWS CloudTrail 추적 변경의 일환으로 AWS Control Tower는 활성화 여부를 확인하는 두 개의 새로운 탐지 제어 기능을 도입합니다. CloudTrail 첫 번째 컨트롤에는 필수 지침이 있으며 3.0 이상의 설치 또는 랜딩 존 업데이트 중에 보안 OU에서 활성화됩니다. 두 번째 컨트롤에는 강력히 권장되는 지침이 포함되어 있으며, 이미 필수 제어 보호가 시행되고 있는 보안 OU 이외의 모든 OU에도 선택적으로 적용할 수 있습니다.

필수 제어: 보안 조직 단위의 공유 계정에 Lake가 활성화되었는지 AWS CloudTrail 또는 CloudTrail Lake가 활성화되었는지 여부를 감지합니다.

강력히 권장되는 제어: 계정이 활성화되었는지 AWS CloudTrail 또는 CloudTrail Lake가 활성화되었는지 여부를 감지합니다.

새 제어 항목에 대한 자세한 내용은 AWS Control Tower 제어 라이브러리를 참조하십시오.

지역 거부 제어에 대한 업데이트

아래 나열된 일부 추가 서비스의 조치를 포함하도록 지역 거부 제어의 NotAction목록을 업데이트했습니다.

```
        “chatbot:*”,
        "s3:GetAccountPublic",
        "s3:DeleteMultiRegionAccessPoint",
        "s3:DescribeMultiRegionAccessPointOperation",
        "s3:GetMultiRegionAccessPoint",
        "s3:GetMultiRegionAccessPointPolicy",
        "s3:GetMultiRegionAccessPointPolicyStatus",
        "s3:ListMultiRegionAccessPoints",
        "s3:GetStorageLensConfiguration",
        “s3:GetStorageLensDashboard",
        “s3:ListStorageLensConfigurations”
        “s3:GetAccountPublicAccessBlock“,,
        “s3:PutAccountPublic",
        “s3:PutAccountPublicAccessBlock“,
```

비디오 안내

이 동영상 (3:07) 은 기존 AWS Control Tower 랜딩 존을 버전 3으로 업데이트하는 방법을 설명합니다. 동영상 오른쪽 하단에 있는 아이콘을 선택하여 전체 화면으로 확대하면 더 잘 보입니다. 자막을 사용할 수 있습니다.

기존 AWS Control Tower 랜딩 존을 랜딩 존 3으로 업데이트하는 방법에 대한 동영상 안내.

조직 페이지는 OU와 계정의 관점을 통합합니다.

2022년 7월 18일

(AWS Control Tower 랜딩 존은 업데이트 필요 없음)

AWS Control Tower의 새 조직 페이지에는 모든 조직 단위 (OU) 및 계정의 계층적 보기가 표시됩니다. 이전에 존재했던 OU 및 계정 페이지의 정보를 결합합니다.

새 페이지에서 상위 OU와 중첩된 OU 및 계정 간의 관계를 볼 수 있습니다. 리소스 그룹화에 대한 조치를 취할 수 있습니다. 페이지 보기를 구성할 수 있습니다. 예를 들어 계층적 보기를 확장 또는 축소하거나, 계정 또는 OU만 표시하도록 보기를 필터링하거나, 등록된 계정 및 등록된 OU만 보도록 선택하거나, 관련 리소스 그룹을 볼 수 있습니다. 전체 조직이 제대로 업데이트되었는지 확인하는 것이 더 쉽습니다.

개별 회원 계정의 등록 및 업데이트가 더 쉬워졌습니다.

2022년 5월 31일

(AWS Control Tower 랜딩 존은 업데이트 필요 없음)

AWS Control Tower는 이제 회원 계정을 개별적으로 업데이트하고 등록할 수 있는 향상된 기능을 제공합니다. 각 계정에는 업데이트가 가능한 시기가 표시되므로 회원 계정에 최신 구성이 포함되어 있는지 보다 쉽게 확인할 수 있습니다. 몇 가지 간소화된 단계를 통해 landing Zone을 업데이트하거나, 계정 드리프트를 해결하거나, 계정을 등록된 OU에 등록할 수 있습니다.

계정을 업데이트할 때 각 업데이트 작업에 계정의 전체 OU (Organization Unit) 를 포함할 필요가 없습니다. 따라서 개별 계정을 업데이트하는 데 필요한 시간이 크게 줄어듭니다.

AWS 컨트롤 타워 콘솔의 추가 지원을 받아 계정을 AWS 컨트롤 타워 OU에 등록할 수 있습니다. AWS Control Tower에 등록한 기존 계정은 여전히 계정 사전 요구 사항을 충족해야 하며 역할을 추가해야 합니다. `AWSControlTowerExecution` 그런 다음 등록된 OU를 선택하고 등록 버튼을 선택하여 해당 OU에 계정을 등록할 수 있습니다.

유사한 프로세스를 더욱 구분하고 계정 정보를 입력할 때 설정 오류가 발생하지 않도록 계정 등록 기능을 계정 팩토리의 계정 생성 워크플로우와 분리했습니다.

AFT는 공유 AWS Control Tower 계정에 대한 자동 사용자 지정을 지원합니다.

2022년 5월 27일

(AWS Control Tower 랜딩 존은 업데이트 필요 없음)

Account Factory for Terraform (AFT) 은 이제 등록된 계정과 함께 관리 계정, 감사 계정, 로그 아카이브 계정 등 AWS Control Tower에서 관리하는 모든 계정을 프로그래밍 방식으로 사용자 지정하고 업데이

트할 수 있습니다. 작업을 수행하는 역할의 범위를 지정하므로 계정 구성의 보안을 보호하는 동시에 계정 사용자 지정 및 업데이트 관리를 중앙 집중화할 수 있습니다.

기존 AWSAFTExecution역할은 이제 모든 계정에 사용자 지정을 배포합니다. 비즈니스 및 보안 요구 사항에 따라 AWSAFTExecution역할 액세스를 제한하는 경계를 설정하여 IAM 권한을 설정할 수 있습니다. 또한 신뢰할 수 있는 사용자를 위해 해당 역할에서 승인된 사용자 지정 권한을 프로그래밍 방식으로 위임할 수 있습니다. 가장 좋은 방법은 필요한 사용자 지정을 배포하는 데 필요한 권한으로 권한을 제한하는 것입니다.

이제 AFT는 공유 계정 및 관리 계정을 포함한 모든 관리 계정에 AFT 리소스를 배포하기 위한 새 AWSAFTService역할을 생성합니다. 이전에는 리소스가 역할별로 배포되었습니다. AWSAFTExecution

AWS Control Tower 공유 및 관리 계정은 어카운트 팩토리를 통해 프로비저닝되지 않으므로 해당 계정에는 프로비저닝된 해당 제품이 없습니다. AWS Service Catalog따라서 Service Catalog에서 공유 및 관리 계정을 업데이트할 수 없습니다.

모든 선택적 컨트롤에 대한 동시 작업

2022년 5월 18일

(AWS Control Tower 랜딩 존은 업데이트 필요 없음)

AWS Control Tower는 이제 예방 제어와 탐지 제어를 위한 동시 작업을 지원합니다.

이 새로운 기능을 통해 이제 모든 선택적 제어를 동시에 적용하거나 제거할 수 있으므로 모든 선택적 제어의 사용 편의성과 성능이 개선됩니다. 개별 제어 작업이 완료될 때까지 기다릴 필요 없이 여러 개의 선택적 제어를 활성화할 수 있습니다. 유일한 제한 시간은 AWS Control Tower가 랜딩 존 설정 중이거나 거버넌스를 새 조직으로 확장하는 동안입니다.

예방 제어를 위해 지원되는 기능:

- 동일한 OU에 다양한 예방 제어를 적용하고 제거합니다.
- 여러 OU에 서로 다른 예방 관리를 동시에 적용하고 제거하십시오.
- 여러 OU에 동일한 예방 제어를 동시에 적용하고 제거하십시오.
- 예방 및 탐지 제어를 동시에 적용하고 제거할 수 있습니다.

출시된 모든 AWS Control Tower 버전에서 이러한 제어 동시성 개선을 경험할 수 있습니다.

중첩된 OU에 예방 제어를 적용하면 대상 OU에 중첩된 모든 계정 및 OU에 영향을 미치며, 해당 계정과 OU가 AWS Control Tower에 등록되지 않은 경우에도 마찬가지입니다. 예방 제어는 의 일부인 서비스 제어 정책 (SCP) 을 사용하여 구현됩니다. AWS Organizations Detective 컨트롤은 규칙을 사용하여 AWS Config 구현됩니다. 가드레일은 새 계정을 만들거나 기존 계정을 변경할 때도 유효하며, AWS Control Tower는 각 계정이 활성화된 정책을 어떻게 준수하는지에 대한 요약 보고서를 제공합니다. 사용 가능한 컨트롤의 전체 목록은 AWS Control Tower 제어 라이브러리를 참조하십시오.

기존 보안 및 로깅 계정

2022년 5월 16일

(초기 설정 중에 사용 가능)

이제 AWS Control Tower는 초기 랜딩 존 설정 프로세스 중에 기존 AWS 계정을 AWS Control Tower 보안 또는 로깅 계정으로 지정할 수 있는 옵션을 제공합니다. 이 옵션을 사용하면 AWS Control Tower가 새로운 공유 계정을 생성할 필요가 없습니다. 기본적으로 감사 계정이라고 하는 보안 계정은 보안 및 규정 준수 팀이 랜딩 존의 모든 계정에 액세스할 수 있도록 하는 제한된 계정입니다. 기본적으로 Log Archive 계정이라고 하는 로깅 계정은 리포지토리로 작동합니다. 랜딩 존에 있는 모든 계정의 API 활동 및 리소스 구성 로그를 저장합니다.

기존 보안 및 로깅 계정을 가져오면 AWS Control Tower 거버넌스를 기존 조직으로 확장하거나 대체 랜딩 존에서 AWS Control Tower로 이전하는 것이 더 쉬워집니다. 기존 계정을 사용할 수 있는 옵션은 초기 landding zone 설정 중에 표시됩니다. 여기에는 성공적인 배포를 보장하기 위한 설치 프로세스 중의 점검이 포함됩니다. AWS Control Tower는 기존 계정에 필요한 역할과 제어를 구현합니다. 이러한 계정에 있는 기존 리소스 또는 데이터를 제거하거나 병합하지는 않습니다.

제한: 기존 AWS 계정을 감사 및 로그 아카이브 계정으로 AWS Control Tower에 가져오고 해당 계정에 기존 AWS Config 리소스가 있는 경우, 계정을 AWS Control Tower에 등록하려면 먼저 기존 AWS Config 리소스를 삭제해야 합니다.

AWS 컨트롤 타워 랜딩 존 버전 2.9

2022년 4월 22일

(AWS Control Tower 랜딩 존을 버전 2.9로 업데이트하려면 업데이트가 필요합니다. 자세한 내용은 참조랜딩 영역 업데이트)

AWS Control Tower 랜딩 존 버전 2.9는 Python 버전 3.9 런타임을 사용하도록 알림 전달자 Lambda를 업데이트합니다. 이 업데이트는 2022년 7월에 예정된 Python 버전 3.6의 지원 중단을 해결합니다. 최신 정보는 Python 지원 중단 페이지를 참조하십시오.

AWS 컨트롤 타워 랜딩 존 버전 2.8

2022년 2월 10일

(AWS Control Tower 랜딩 존을 버전 2.8로 업데이트하려면 업데이트가 필요합니다. 자세한 내용은 참조랜딩 영역 업데이트)

AWS Control Tower 랜딩 존 버전 2.8에는 AWS 기본 보안 모범 사례의 최신 업데이트에 부합하는 기능이 추가되었습니다.

이번 릴리스에서:

- 기존 S3 액세스 로그 버킷에 대한 액세스를 추적할 수 있도록 Log Archive 계정의 액세스 로그 버킷에 대한 액세스 로깅이 구성됩니다.
- 수명 주기 정책에 대한 지원이 추가되었습니다. 기존 S3 액세스 로그 버킷의 액세스 로그는 기본 보존 기간인 10년으로 설정되어 있습니다.
- 또한 이번 릴리스는 AWS Control Tower가 모든 관리 계정 (관리 계정 제외) 에서 제공하는 AWS AWS Config서비스 연결 역할 (SLR) 을 사용하도록 업데이트하므로, 모범 사례에 AWS Config 맞게 Config 규칙을 설정하고 관리할 수 있습니다. 업그레이드하지 않은 고객은 기존 역할을 계속 사용하게 됩니다.
- 이 릴리스는 AWS Config 데이터 암호화를 위한 AWS Control Tower KMS 구성 프로세스를 간소화하고 관련 상태 메시징을 개선합니다. CloudTrail
- 이 릴리스에는 해당 기능을 사용할 수 있도록 지역 거부 제어에 대한 업데이트가 포함되어 있습니다. `route53-application-recovery` `us-west-2`
- 업데이트: 2022년 2월 15일에 AWS Lambda 함수의 데드레터 대기열을 제거했습니다.

추가 세부 정보:

- 랜딩 존을 해제해도 AWS Control Tower는 AWS Config 서비스 연결 역할을 제거하지 않습니다.
- Account Factory 계정을 프로비저닝 해제해도 AWS Control Tower는 AWS Config 서비스 연결 역할을 제거하지 않습니다.

랜딩 존을 2.8로 업데이트하려면 랜딩 존 설정 페이지로 이동하여 2.8 버전을 선택한 다음 업데이트를 선택합니다. 랜딩 존을 업데이트한 후에는 에 나와 있는 대로 AWS Control Tower가 관리하는 모든 계정을 업데이트해야 합니다. AWS Control Tower에서의 구성 업데이트 관리

2021년 1월 - 12월

2021년에 AWS Control Tower는 다음과 같은 업데이트를 발표했습니다.

- 지역 거부 기능
- 데이터 레지던시 기능
- AWS Control Tower는 Terraform 계정 프로비저닝 및 사용자 지정을 소개합니다
- 새로운 라이프사이클 이벤트 제공
- AWS Control Tower는 중첩된 OU를 지원합니다.
- Detective Control 동시성
- 두 개의 새 지역을 이용할 수 있습니다.
- 지역 선택 취소
- AWS Control Tower는 AWS 키 관리 시스템과 함께 작동합니다.
- 컨트롤의 이름이 변경되었고 기능은 변경되지 않았습니다.
- AWS Control Tower는 매일 SCP를 스캔하여 드리프트를 확인합니다.
- OU 및 계정의 사용자 지정 이름
- AWS 컨트롤 타워 랜딩 존 버전 2.7
- 세 개의 새 AWS 지역을 사용할 수 있습니다.
- 일부 지역만 관리하세요.
- AWS Control Tower는 이제 거버넌스를 조직의 기존 OU로 확장합니다. AWS
- AWS Control Tower는 대량 계정 업데이트를 제공합니다.

지역 거부 기능

2021년 11월 30일

(AWS Control Tower 랜딩 존은 업데이트가 필요하지 않습니다.)

AWS Control Tower는 이제 AWS Control Tower 환경에 등록된 계정의 AWS 서비스 및 운영에 대한 액세스를 제한하는 데 도움이 되는 지역 거부 기능을 제공합니다. 지역 거부 기능은 AWS Control Tower의 기존 지역 선택 및 지역 선택 취소 기능을 보완합니다. 이러한 기능을 함께 사용하면 규정 준수 및 규제 문제를 해결하는 동시에 추가 지역으로의 확장과 관련된 비용의 균형을 맞출 수 있습니다.

예를 들어 독일 AWS 고객은 프랑크푸르트 지역 외 지역의 AWS 서비스 액세스를 거부할 수 있습니다. AWS Control Tower 설정 프로세스 중에 또는 랜딩 존 설정 페이지에서 제한 지역을 선택할 수 있습

니다. 지역 거부 기능은 AWS Control Tower 랜딩 존 버전을 업데이트할 때 사용할 수 있습니다. 일부 AWS 서비스는 지역 거부 기능에서 제외됩니다. 자세히 알아보려면 지역 거부 제어 구성을 참조하십시오.

데이터 레지던시 기능

2021년 11월 30일

(AWS Control Tower 랜딩 존은 업데이트 필요 없음)

이제 AWS Control Tower는 AWS 서비스에 업로드하는 모든 고객 데이터가 지정된 AWS 지역에만 위치하도록 하기 위해 특별히 구축된 제어 기능을 제공합니다. 고객 데이터가 저장되고 처리되는 AWS 지역 또는 지역을 선택할 수 있습니다. AWS Control Tower를 사용할 수 있는 AWS AWS 지역의 전체 목록은 지역 표를 참조하십시오.

세분화된 제어를 위해 Amazon VPN (가상 사설망) 연결 금지 또는 Amazon VPC 인스턴스의 인터넷 액세스 금지 등의 추가 제어를 적용할 수 있습니다. AWS Control Tower 콘솔에서 제어 항목의 규정 준수 상태를 확인할 수 있습니다. 사용 가능한 컨트롤의 전체 목록은 AWS Control Tower 제어 라이브러리를 참조하십시오.

AWS Control Tower는 Terraform 계정 프로비저닝 및 사용자 지정을 소개합니다

2021년 11월 29일

(AWS Control Tower 랜딩 존에 대한 선택적 업데이트)

이제 Terraform을 사용하여 AWS Control Tower Account Factory for Terraform (AFT) 을 통해 AWS 컨트롤 타워를 통해 사용자 지정 계정을 프로비저닝하고 업데이트할 수 있습니다.

AFT는 AWS Control Tower에서 관리하는 계정을 프로비저닝하는 단일 Terraform IaC (코드형 인프라) 파이프라인을 제공합니다. 프로비저닝 중에 사용자 지정하면 최종 사용자에게 계정을 제공하기 전에 비즈니스 및 보안 정책을 충족하는 데 도움이 됩니다.

AFT 자동 계정 생성 파이프라인은 계정 프로비저닝이 완료될 때까지 모니터링한 다음 계속하여 필요한 사용자 지정으로 계정을 향상시키는 추가 Terraform 모듈을 트리거합니다. 사용자 지정 프로세스의 추가 부분으로 자체 사용자 지정 Terraform 모듈을 설치하도록 파이프라인을 구성하고 일반 사용자 지정을 위해 에서 제공하는 AFT 기능 옵션을 추가하도록 선택할 수 있습니다. AWS

AWS Control Tower 사용 설명서에 제공된 단계를 따르고 Terraform 인스턴스용 AFT를 다운로드하여 Terraform용 AWS Control Tower Account Factory를 시작하십시오. 테라폼용 AWS Control Tower 어

카운트 팩토리 (AFT) 배포 AFT는 테라폼 클라우드, 테라폼 엔터프라이즈 및 테라폼 오픈 소스 배포판을 지원합니다.

새로운 라이프사이클 이벤트 제공

2021년 11월 18일

(AWS Control Tower 랜딩 존은 업데이트 필요 없음)

`PrecheckOrganizationalUnit`이벤트는 중첩된 OU의 리소스를 포함하여 거버넌스 확장 작업의 성공을 가로막는 리소스가 있는지 여부를 기록합니다. 자세한 정보는 `PrecheckOrganizationalUnit`을 참조하세요.

AWS Control Tower는 중첩된 OU를 지원합니다.

2021년 11월 16일

(AWS Control Tower 랜딩 존은 업데이트 필요 없음)

이제 AWS Control Tower를 사용하면 중첩된 OU를 랜딩 존의 일부로 포함할 수 있습니다.

AWS Control Tower는 중첩된 조직 단위 (OU) 에 대한 지원을 제공하므로 계정을 여러 계층 수준으로 구성하고 예방 제어를 계층적으로 적용할 수 있습니다. 중첩된 OU를 포함하는 OU를 등록하고, 상위 OU 아래에 OU를 생성 및 등록하고, 깊이에 상관없이 등록된 모든 OU에서 제어를 활성화할 수 있습니다. 이 기능을 지원하기 위해 콘솔에는 관리되는 계정 및 OU 수가 표시됩니다.

중첩된 OU를 사용하면 AWS Control Tower OU를 AWS 다중 계정 전략에 맞게 조정할 수 있으며, 상위 OU 수준에서 제어를 적용함으로써 여러 OU에서 제어를 활성화하는 데 필요한 시간을 줄일 수 있습니다.

주요 고려 사항

1. 최상위 OU부터 시작하여 트리 아래로 진행하면서 한 번에 한 OU씩 기존 다단계 OU를 AWS Control Tower에 등록할 수 있습니다. 자세한 정보는 플랫 OU 구조에서 중첩된 OU 구조로 확장을 참조하세요.
2. 등록된 OU 바로 아래에 있는 계정은 자동으로 등록됩니다. 트리 아래에 있는 계정은 직계 부모 OU를 등록하여 등록할 수 있습니다.
3. 예방 통제 (SCP) 는 자동으로 계층 아래로 상속되며, 부모에 적용된 SCP는 모든 중첩된 OU에 상속됩니다.

4. Detective 컨트롤 (AWS Config 규칙) 은 자동으로 상속되지 않습니다.
5. 탐지 제어 규정 준수는 각 OU에서 보고합니다.
6. OU의 SCP 드리프트는 해당 OU에 속한 모든 계정과 OU에 영향을 미칩니다.
7. 보안 OU (Core OU) 아래에 중첩된 새 OU를 만들 수는 없습니다.

Detective Control 동시성

2021년 11월 5일

(AWS Control Tower 랜딩 존에 대한 선택적 업데이트)

AWS Control Tower 탐지 제어는 이제 탐지 제어의 동시 작업을 지원하여 사용 편의성과 성능을 개선합니다. 개별 제어 작업이 완료될 때까지 기다릴 필요 없이 여러 탐지 제어를 활성화할 수 있습니다.

지원되는 기능:

- 동일한 OU에서 다양한 탐지 제어를 활성화합니다 (예: 루트 사용자의 MFA 활성화 여부 감지 및 Amazon S3 버킷에 대한 퍼블릭 쓰기 액세스 허용 여부 감지).
- 여러 OU에서 다양한 탐지 제어를 동시에 활성화하십시오.
- 지원되는 제어 동시 실행 작업에 대한 추가 지침을 제공하기 위해 가드레일 오류 메시지가 개선되었습니다.

이번 릴리즈에서는 지원되지 않음:

- 여러 OU에서 동일한 탐지 제어를 동시에 활성화하는 것은 지원되지 않습니다.
- 예방 제어 동시성은 지원되지 않습니다.

모든 버전의 AWS Control Tower에서 탐지 제어 동시성 개선을 경험할 수 있습니다. 현재 버전 2.7을 사용하지 않는 고객은 Landing Zone 업데이트를 수행하여 최신 버전에서 사용할 수 있는 지역 선택 및 선택 취소와 같은 다른 기능을 활용하는 것이 좋습니다.

두 개의 새 지역을 이용할 수 있습니다.

2021년 7월 29일

(AWS Control Tower 랜딩 존에는 업데이트 필요)

이제 AWS Control Tower를 남미 (상파울루) 와 유럽 (파리) 의 두 AWS 지역에서 추가로 사용할 수 있습니다. 이 업데이트는 AWS Control Tower의 가용성을 15개 AWS 지역으로 확대합니다.

AWS Control Tower를 처음 사용하는 경우 지원되는 모든 지역에서 바로 시작할 수 있습니다. 출시 과정에서 AWS Control Tower에서 다중 계정 환경을 구축하고 관리할 지역을 선택할 수 있습니다.

이미 AWS Control Tower 환경이 있고 하나 이상의 지원되는 지역에서 AWS Control Tower 거버넌스 기능을 확장하거나 제거하려는 경우, AWS Control Tower 대시보드의 랜딩 영역 설정 페이지로 이동한 다음 지역을 선택합니다. 랜딩 존을 업데이트한 후에는 AWS Control Tower가 관리하는 모든 계정을 업데이트해야 합니다.

지역 선택 취소

2021년 7월 29일

(AWS Control Tower 랜딩 존에 대한 선택적 업데이트)

AWS Control Tower 지역 선택 취소로 AWS Control Tower 리소스의 지리적 위치를 관리하는 능력이 향상됩니다. 더 이상 AWS Control Tower에서 관리하지 않으려는 지역은 선택 취소할 수 있습니다. 이 기능을 사용하면 규정 준수 및 규제 문제를 해결하는 동시에 추가 지역으로의 확장과 관련된 비용의 균형을 맞출 수 있습니다.

지역 선택 취소는 AWS Control Tower 랜딩 존 버전을 업데이트할 때 사용할 수 있습니다.

Account Factory를 사용하여 새 계정을 만들거나 기존 회원 계정을 등록하거나 Extend Governance (Extend Governance) 를 선택하여 기존 조직 단위에 계정을 등록하는 경우, AWS Control Tower는 계정 내 선택한 지역에 중앙 집중식 로깅, 모니터링 및 제어를 포함하는 거버넌스 기능을 배포합니다. 지역을 선택 취소하고 해당 지역에서 AWS Control Tower 거버넌스를 제거하면 해당 거버넌스 기능은 제거되지만, AWS 리소스나 워크로드를 해당 지역에 배포하는 사용자의 능력을 저해하지는 않습니다.

AWS Control Tower는 AWS 키 관리 시스템과 함께 작동합니다.

2021년 7월 28일

(AWS Control Tower 랜딩 존에 대한 선택적 업데이트)

AWS Control Tower는 AWS 키 관리 서비스 (AWS KMS) 키를 사용할 수 있는 옵션을 제공합니다. 키는 AWS Control Tower가 배포하는 서비스 (및 관련 Amazon S3 데이터 포함 AWS CloudTrail) 를 보호하기 위해 사용자가 제공하고 관리합니다. AWS Config AWS KMS 암호화는 AWS Control Tower가 기본적으로 사용하는 SSE-S3 암호화보다 향상된 수준의 암호화입니다.

AWS KMS 지원을 AWS Control Tower에 통합하는 것은 민감한 로그 파일에 대한 AWS 추가 보안 계층을 권장하는 기본 보안 모범 사례와 일치합니다. 저장 중 암호화에는 AWS KMS 관리형 키 (SSE-KMS) 를 사용해야 합니다. AWS KMS 암호화 지원은 새 랜딩 존을 설정하거나 기존 AWS Control Tower 랜딩 존을 업데이트할 때 이용할 수 있습니다.

이 기능을 구성하려면 초기 랜딩 존 설정 중에 KMS 키 구성을 선택하면 됩니다. 기존 KMS 키를 선택하거나 AWS KMS 콘솔로 이동하는 버튼을 선택하여 새 키를 생성할 수 있습니다. 또한 기본 암호화에서 SSE-KMS 또는 다른 SSE-KMS 키로 유연하게 변경할 수 있습니다.

기존 AWS Control Tower 랜딩 존의 경우 업데이트를 수행하여 AWS KMS 키 사용을 시작할 수 있습니다.

컨트롤의 이름이 변경되었고 기능은 변경되지 않았습니다.

2021년 7월 26일

(AWS Control Tower 랜딩 존은 업데이트 필요 없음)

AWS Control Tower는 규제 항목의 정책 의도를 더 잘 반영하기 위해 특정 규제 이름 및 설명을 수정하고 있습니다. 수정된 이름 및 설명은 컨트롤이 계정의 정책을 구현하는 방식을 보다 직관적으로 이해하는 데 도움이 됩니다. 예를 들어 탐정 제어 항목 자체가 특정 작업을 중지하지 않고 정책 위반만 탐지하고 대시보드를 통해 경고를 제공하기 때문에 탐정 제어 항목의 이름을 “Disallow”에서 “Detect”로 일부 변경했습니다.

제어 기능, 지침 및 구현은 변경되지 않았습니다. 컨트롤 이름과 설명만 수정되었습니다.

AWS Control Tower는 매일 SCP를 스캔하여 드리프트를 확인합니다.

2021년 5월 11일

(AWS Control Tower 랜딩 존은 업데이트 필요 없음)

이제 AWS Control Tower는 관리형 SCP를 매일 자동 스캔하여 해당 제어가 올바르게 적용되고 표류하지 않았는지 확인합니다. 스캔 결과 드리프트가 발견되면 알림을 받게 됩니다. AWS Control Tower는 드리프트 문제당 하나의 알림만 전송하므로, 랜딩 존이 이미 드리프트 상태에 있는 경우 새 드리프트 항목이 발견되지 않는 한 추가 알림을 받지 않습니다.

OU 및 계정의 사용자 지정 이름

2021년 4월 16일

(AWS Control Tower 랜딩 존은 업데이트 필요 없음)

이제 AWS Control Tower에서 랜딩 존 이름을 사용자 지정할 수 있습니다. AWS Control Tower가 조직 단위 (OU) 및 핵심 계정에 대해 권장하는 이름을 유지하거나 초기 landing Zone 설정 프로세스 중에 이러한 이름을 수정할 수 있습니다.

AWS Control Tower가 OU 및 핵심 계정에 제공하는 기본 이름은 AWS 다중 계정 모범 사례 지침과 일치합니다. 그러나 회사에 특정 이름 지정 정책이 있거나 동일한 권장 이름을 가진 기존 OU 또는 계정이 이미 있는 경우 새 OU 및 계정 이름 지정 기능을 사용하면 이러한 제약 조건을 유연하게 해결할 수 있습니다.

설치 중 워크플로가 변경되는 것과는 별개로 이전에 Core OU로 알려졌던 OU는 이제 보안 OU라고 하며, 이전에 사용자 지정 OU로 알려졌던 OU는 이제 샌드박스 OU라고 합니다. 이름 지정에 대한 전반적인 AWS 모범 사례 지침에 맞게 조정하기 위해 이러한 변경을 적용했습니다.

신규 고객에게는 이러한 새 OU 이름이 표시됩니다. 기존 고객에게는 이러한 OU의 원래 이름이 계속 표시됩니다. 설명서를 새 이름으로 업데이트하는 동안 OU 이름 지정에 일부 불일치가 발생할 수 있습니다.

AWS 관리 콘솔에서 AWS Control Tower를 시작하려면 AWS Control Tower 콘솔로 이동하여 오른쪽 상단에서 랜딩 존 설정을 선택하십시오. 자세한 내용은 AWS Control Tower 랜딩 존 계획에 대해 읽어 보십시오.

AWS 컨트롤 타워 랜딩 존 버전 2.7

2021년 4월 8일

(AWS Control Tower 랜딩 존을 버전 2.7로 업데이트하려면 업데이트가 필요합니다. 자세한 내용은 을 참조하십시오랜딩 영역 업데이트.

AWS Control Tower 버전 2.7부터 AWS Control Tower는 AWS Control Tower 리소스에만 정책을 구현하는 4개의 새로운 필수 예방적 로그 아카이브 제어 항목을 도입했습니다. 기존 Log Archive 제어 항목 4개에 대한 지침을 필수에서 선택으로 조정했는데, 이는 AWS Control Tower 외부 리소스에 대한 정책을 설정했기 때문입니다. 이 제어 변경 및 확장은 AWS Control Tower 내 리소스에 대한 Log Archive 거버넌스를 AWS Control Tower 외부의 리소스 거버넌스와 분리할 수 있는 기능을 제공합니다.

변경된 네 가지 제어 항목을 새로운 필수 제어 항목과 함께 사용하여 더 광범위한 AWS 로그 아카이브 집합에 거버넌스를 제공할 수 있습니다. 기존 AWS Control Tower 환경에서는 환경 일관성을 위해 이러한 네 가지 변경된 제어를 자동으로 활성화하지만 이제 이러한 선택적 제어를 비활성화할 수 있습니

다. 새로운 AWS Control Tower 환경에서는 모든 선택적 제어를 활성화해야 합니다. 기존 환경에서는 AWS Control Tower에서 배포하지 않은 Amazon S3 버킷에 암호화를 추가하기 전에 이전의 필수 제어를 비활성화해야 합니다.

새로운 필수 제어 항목:

- 로그 아카이브에 있는 AWS Control Tower 생성 S3 버킷의 암호화 구성 변경을 허용하지 않음
- 로그 아카이브에 있는 AWS Control Tower 생성 S3 버킷의 로깅 구성 변경을 허용하지 않음
- 로그 아카이브에 있는 AWS Control Tower 생성 S3 버킷에 대한 버킷 정책 변경을 허용하지 않음
- 로그 아카이브에 있는 AWS Control Tower 생성 S3 버킷의 수명 주기 구성 변경을 허용하지 않음

지침이 필수에서 선택으로 변경되었습니다.

- 모든 Amazon S3 버킷의 암호화 구성 변경 금지 [이전: 로그 아카이브에 대해 저장 중 암호화 활성화]
- 모든 Amazon S3 버킷의 로깅 구성 변경 금지 [이전: 로그 아카이브에 대한 액세스 로깅 활성화]
- 모든 Amazon S3 버킷에 대한 버킷 정책 변경 금지 [이전: 로그 아카이브에 대한 정책 변경 금지]
- 모든 Amazon S3 버킷의 수명 주기 구성 변경 금지 [이전: 로그 아카이브에 대한 보존 정책 설정]

AWS Control Tower 버전 2.7에는 2.7로 업그레이드한 후 이전 버전과 호환되지 않을 수 있는 AWS Control Tower 랜딩 존 블루프린트에 대한 변경 사항이 포함되어 있습니다.

- 특히, AWS Control Tower 버전 2.7은 AWS Control Tower에서 배포한 S3 버킷에서 `BlockPublicAccess` 자동으로 활성화됩니다. 워크로드에 계정 간 액세스가 필요한 경우 이 기본값을 해제할 수 있습니다. `BlockPublicaccess`활성화된 상태에서 어떤 일이 발생하는지에 대한 자세한 내용은 Amazon S3 스토리지에 대한 퍼블릭 액세스 차단을 참조하십시오.
- AWS Control Tower 버전 2.7에는 HTTPS에 대한 요구 사항이 포함되어 있습니다. AWS Control Tower에서 배포한 S3 버킷으로 전송되는 모든 요청은 보안 소켓 계층 (SSL) 을 사용해야 합니다. HTTPS 요청만 전달할 수 있습니다. HTTP (SSL 제외) 를 엔드포인트로 사용하여 요청을 보내는 경우 이 변경으로 인해 액세스 거부 오류가 발생하여 워크플로가 중단될 수 있습니다. 이 변경 사항은 landing Zone을 2.7로 업데이트한 후에는 되돌릴 수 없습니다.

  HTTP 대신 TLS를 사용하도록 요청을 변경하는 것이 좋습니다.

세 개의 새 AWS 지역을 사용할 수 있습니다.

2021년 4월 8일

(AWS Control Tower 랜딩 존에는 업데이트 필요)

AWS Control Tower는 아시아 태평양 (도쿄) 지역, 아시아 태평양 (서울) 지역, 아시아 태평양 (뭄바이) 지역 등 세 개의 추가 AWS 지역에서 사용할 수 있습니다. 이러한 지역으로 거버넌스를 확장하려면 Landing Zone을 버전 2.7로 업데이트해야 합니다.

버전 2.7로 업데이트할 때 랜딩 존이 해당 지역으로 자동으로 확장되지 않으므로 포함하려면 Regions 테이블에서 랜딩 존을 확인하고 선택해야 합니다.

일부 지역만 관리하세요.

2021년 2월 19일

(AWS Control Tower 랜딩 존은 업데이트 필요 없음)

AWS Control Tower 지역 선택은 AWS Control Tower 리소스의 지리적 위치를 더 잘 관리할 수 있는 기능을 제공합니다. 규정 준수, 규제, 비용 또는 기타 이유로 AWS 리소스 또는 워크로드를 호스팅하는 지역의 수를 늘리기 위해 이제 관리할 추가 지역을 선택할 수 있습니다.

새 랜딩 존을 설정하거나 AWS Control Tower 랜딩 존 버전을 업데이트할 때 리전을 선택할 수 있습니다. Account Factory를 사용하여 새 계정을 만들거나 기존 회원 계정을 등록하거나 Extend Governance를 사용하여 기존 조직 단위에 계정을 등록하는 경우, AWS Control Tower는 계정 내 선택한 지역에 중앙 집중식 로깅, 모니터링 및 제어를 위한 거버넌스 기능을 배포합니다. 지역 선택에 대한 자세한 내용은 을 참조하십시오. AWS 컨트롤 타워 지역 구성

AWS Control Tower는 이제 거버넌스를 조직의 기존 OU로 확장합니다. AWS

2021년 1월 28일

(AWS Control Tower 랜딩 존은 업데이트 필요 없음)

AWS Control Tower 콘솔 내에서 기존 조직 단위 (OU) (AWS Control Tower에 속하지 않는 조직) 로 거버넌스를 확장하십시오. 이 기능을 사용하면 AWS Control Tower 거버넌스에 따라 최상위 OU와 포함된 계정을 가져올 수 있습니다. 거버넌스를 OU 전체로 확장하는 방법에 대한 자세한 내용은 을 참조하십시오. 기존 조직 단위를 AWS Control Tower에 등록

OU를 등록하면 AWS Control Tower는 OU 내에서 거버넌스를 성공적으로 확장하고 계정을 등록할 수 있도록 일련의 검사를 수행합니다. OU의 초기 등록과 관련된 일반적인 문제에 대한 자세한 내용은 을 참조하십시오. 등록 또는 재등록 시 발생하는 일반적인 실패 원인

AWS Control Tower 제품 웹 페이지를 방문하거나 를 방문하여 AWS Control Tower를 시작하는 방법에 대한 이 동영상을 YouTube 시청할 수도 있습니다. AWS Organizations

AWS Control Tower는 대량 계정 업데이트를 제공합니다.

2021년 1월 28일

(AWS Control Tower 랜딩 존은 업데이트 필요 없음)

대량 업데이트 기능을 사용하면 이제 AWS Control Tower 대시보드에서 클릭 한 번으로 최대 300개의 계정을 포함하는 등록된 AWS Organizations 조직 구성 단위 (OU) 의 모든 계정을 업데이트할 수 있습니다. 이는 AWS Control Tower 랜딩 존을 업데이트하고 등록된 계정을 현재 랜딩 존 버전에 맞게 업데이트해야 하는 경우에 특히 유용합니다.

또한 이 기능을 사용하면 AWS Control Tower 랜딩 존을 업데이트하여 새 지역으로 확장하거나 OU를 재등록하여 해당 OU의 모든 계정에 최신 제어 기능이 적용되도록 할 때 계정을 최신 상태로 유지할 수 있습니다. 대량 계정 업데이트를 사용하면 한 번에 한 계정씩 업데이트하거나 외부 스크립트를 사용하여 여러 계정에서 업데이트를 수행할 필요가 없습니다.

착륙 영역 업데이트에 대한 자세한 내용은 을 참조하십시오랜딩 영역 업데이트.

OU 등록 또는 재등록에 대한 자세한 내용은 을 참조하십시오기존 조직 단위를 AWS Control Tower에 등록.

2020년 1월 - 12월

2020년에 AWS Control Tower는 다음과 같은 업데이트를 발표했습니다.

- 이제 AWS Control Tower 콘솔이 외부 AWS Config 규칙에 연결됩니다.
- 이제 AWS Control Tower를 다른 지역에서도 사용할 수 있습니다.
- 가드레일 업데이트
- AWS Control Tower 콘솔에는 OU 및 계정에 대한 자세한 정보가 나와 있습니다.
- AWS Control Tower를 사용하여 새로운 다중 계정 AWS 환경을 설정할 수 있습니다. AWS Organizations
- AWS Control Tower 솔루션의 사용자 지정
- AWS 컨트롤 타워 버전 2.3의 일반 출시

- AWS Control Tower의 단일 단계 계정 프로비저닝
- AWS Control 타워 폐기 도구
- AWS Control Tower 수명 주기 이벤트 알림

이제 AWS Control Tower 콘솔이 외부 AWS Config 규칙에 연결됩니다.

2020년 12월 29일

(AWS Control Tower 랜딩 존을 버전 2.6으로 업데이트하려면 업데이트가 필요합니다. 자세한 내용은 참조랜딩 영역 업데이트)

AWS Control Tower에는 이제 외부 Config 규칙을 탐지하는 데 도움이 되는 조직 수준의 애그리게이터가 포함됩니다. AWS 이를 통해 AWS Control Tower 콘솔에서 AWS Control Tower에서 생성한 Config 규칙 외에 외부에서 생성한 AWS Config 규칙의 존재 여부를 확인할 수 있습니다. AWS 애그리게이터를 사용하면 AWS Control Tower가 관리되지 않는 계정에 액세스할 필요 없이 AWS Control Tower가 외부 규칙을 탐지하고 AWS Config 콘솔로 연결되는 링크를 제공할 수 있습니다.

이 기능을 사용하면 이제 계정에 적용된 탐지 제어를 통합적으로 볼 수 있으므로 규정 준수를 추적하고 계정에 추가 제어가 필요한지 판단할 수 있습니다. 자세한 내용은 AWS Control Tower가 비관리형 OU 및 계정의 AWS Config 규칙을 집계하는 방법을 참조하십시오.

이제 AWS Control Tower를 다른 지역에서도 사용할 수 있습니다.

2020년 11월 18일

(AWS Control Tower landzone을 버전 2.5로 업데이트하려면 업데이트가 필요합니다. 자세한 내용은 참조랜딩 영역 업데이트)

이제 AWS Control Tower를 5개의 추가 AWS 리전에서 사용할 수 있습니다.

- 아시아 태평양(싱가포르) 리전
- Europe (Frankfurt) Region
- Europe (London) Region
- Europe (Stockholm) Region
- 캐나다(중부) 리전

이 5개 AWS 지역의 추가는 AWS Control Tower 버전 2.5에 도입된 유일한 변경 사항입니다.

AWS Control Tower는 미국 동부 (버지니아 북부) 지역, 미국 동부 (오하이오) 지역, 미국 서부 (오레곤) 지역, 유럽 (아일랜드) 지역, 아시아 태평양 (시드니) 지역에서도 사용할 수 있습니다. 이번 출시로 이제 AWS Control Tower를 10개 AWS 지역에서 사용할 수 있습니다.

이 landing Zone 업데이트에는 나열된 모든 지역이 포함되며 취소할 수 없습니다. 랜딩 존을 버전 2.5로 업데이트한 후에는 지원되는 AWS 10개 지역을 관리하도록 AWS Control Tower에 등록된 모든 계정을 수동으로 업데이트해야 합니다. 자세한 내용은 AWS 컨트롤 타워 지역 구성을 참조하세요.

가드레일 업데이트

2020년 10월 8일

(AWS Control Tower 랜딩 존은 업데이트 필요 없음)

필수 제어를 위한 업데이트된 버전이 출시되었습니다`AWS-GR_IAM_ROLE_CHANGE_PROHIBITED`.

AWS Control Tower에 자동으로 등록되는 계정에는 `AWSControlTowerExecution` 역할이 활성화되어 있어야 하기 때문에 이러한 제어 변경은 필수입니다. 이전 버전의 컨트롤에서는 이 역할을 생성할 수 없습니다.

자세한 내용은 AWS Control AWS CloudFormation Tower에서 설정한 AWS IAM 역할 변경 금지 및 AWS Control Tower 규제 참조 안내서를 참조하십시오.

AWS Control Tower 콘솔에는 OU 및 계정에 대한 자세한 정보가 나와 있습니다.

2020년 7월 22일

(AWS Control Tower 랜딩 존은 업데이트 필요 없음)

등록된 조직 및 계정과 함께 AWS Control Tower에 등록되지 않은 조직 및 계정을 볼 수 있습니다.

AWS Control Tower 콘솔에서 AWS 계정 및 조직 단위 (OU) 에 대한 세부 정보를 볼 수 있습니다. 이제 계정 페이지에는 OU 또는 AWS Control Tower의 등록 상태와 상관없이 조직의 모든 계정이 나열됩니다. 이제 모든 테이블을 검색, 정렬 및 필터링할 수 있습니다.

AWS Control Tower를 사용하여 새로운 다중 계정 AWS 환경을 설정할 수 있습니다. AWS Organizations

2020년 4월 22일

(AWS Control Tower 랜딩 존은 업데이트 필요 없음)

AWS Organizations 이제 고객은 다음과 같은 새로운 기능을 활용하여 AWS Control Tower를 사용하여 새로 생성된 조직 단위 (OU) 및 계정을 관리할 수 있습니다.

- 기존 AWS Organizations 고객은 이제 기존 관리 계정에서 새 조직 단위 (OU) 를 위한 새 랜딩 존을 설정할 수 있습니다. AWS Control Tower에서 새 OU를 생성하고 AWS Control Tower 거버넌스를 통해 해당 OU에 새 계정을 생성할 수 있습니다.
- AWS Organizations 고객은 계정 등록 프로세스나 스크립팅을 사용하여 기존 계정을 등록할 수 있습니다.

AWS Control Tower는 다른 서비스를 사용하는 오케스트레이션 AWS 서비스를 제공합니다. 여러 계정을 보유한 조직과 신규 또는 기존 다중 계정 AWS 환경을 설정하고 대규모로 관리하는 가장 쉬운 방법을 찾는 팀을 위해 설계되었습니다. AWS Control Tower가 관리하는 조직의 경우 클라우드 관리자는 조직의 계정이 정해진 정책을 준수한다는 사실을 알고 있습니다. 빌더는 규정 준수에 대한 과도한 우려 없이 새 AWS 계정을 신속하게 프로비저닝할 수 있어 이점이 있습니다.

착륙 영역 설정에 대한 자세한 내용은 을 참조하십시오AWS Control Tower 랜딩 존을 계획하십시오.. AWS Control Tower 제품 웹 페이지를 방문하거나 를 방문하여 AWS Control Tower를 시작하는 방법에 대한 이 동영상을 YouTube 시청할 수도 있습니다. AWS Organizations

이 변경 사항 외에도 AWS Control Tower의 빠른 계정 프로비저닝 기능은 계정 등록으로 이름이 변경되었습니다. 이제 기존 AWS 계정을 등록하고 새 계정을 생성할 수 있습니다. 자세한 정보는 기존 계정 등록을 참조하세요.

AWS Control Tower 솔루션의 사용자 지정

2020년 3월 17일

(AWS Control Tower 랜딩 존은 업데이트 필요 없음)

이제 AWS Control Tower에는 사용자 지정 템플릿과 정책을 AWS Control Tower 랜딩 존에 쉽게 적용할 수 있는 새로운 참조 구현이 포함되어 있습니다.

AWS Control Tower의 사용자 지정을 사용하면 AWS CloudFormation 템플릿을 사용하여 조직 내 기존 및 새 계정에 새 리소스를 배포할 수 있습니다. 또한 AWS Control Tower에서 이미 제공한 SCP 외에도 해당 계정에 사용자 지정 서비스 제어 정책 (SCP) 을 적용할 수 있습니다. AWS Control Tower 파이프라인의 사용자 지정은 AWS Control Tower 수명 주기 이벤트 및 알림 (AWS Control Tower의 라이프사이클 이벤트) 과 통합되어 리소스 배포가 랜딩 존과 동기화된 상태를 유지하도록 합니다.

이 AWS Control Tower 솔루션 아키텍처에 대한 배포 설명서는 AWS 솔루션 웹 페이지를 통해 제공됩니다.

AWS 컨트롤 타워 버전 2.3의 일반 출시

2020년 3월 5일

(AWS Control Tower 랜딩 존에는 업데이트가 필요합니다. 자세한 내용은 을 참조하십시오랜딩 영역 업데이트.

AWS Control Tower는 이제 미국 동부 (오하이오), 미국 동부 (버지니아 북부), 미국 서부 (오레곤), 유럽 (아일랜드) AWS 지역 외에도 아시아 태평양 (시드니) 지역에서도 사용할 수 있습니다. 아시아 태평양 (시드니) 지역의 추가는 AWS Control Tower 버전 2.3에 도입된 유일한 변경 사항입니다.

이전에 AWS Control Tower를 사용한 적이 없다면, 지원되는 모든 지역에서 오늘 시작할 수 있습니다. 이미 AWS Control Tower를 사용 중이고 계정의 아시아 태평양 (시드니) 지역으로 거버넌스 기능을 확장하려는 경우, AWS Control Tower 대시보드의 설정 페이지로 이동하십시오. 여기에서 landing zone을 최신 릴리스로 업데이트하세요. 그런 다음 계정을 개별적으로 업데이트하세요.

> **Note**
>
> Landing Zone을 업데이트해도 계정이 자동으로 업데이트되지는 않습니다. 계정이 몇 개 이상인 경우 필수 업데이트에 시간이 많이 걸릴 수 있습니다. 따라서 AWS Control Tower 랜딩 존을 워크로드를 실행할 필요가 없는 지역으로 확장하지 않는 것이 좋습니다.

새 지역으로의 배포로 인한 탐지 컨트롤의 예상 동작에 대한 자세한 내용은 AWS Control Tower 지역 구성을 참조하십시오.

AWS Control Tower의 단일 단계 계정 프로비저닝

2020년 3월 2일

(AWS Control Tower 랜딩 존은 업데이트 필요 없음)

AWS Control Tower는 이제 AWS Control Tower 콘솔을 통한 단일 단계 계정 프로비저닝을 지원합니다. 이 기능을 사용하면 AWS Control Tower 콘솔 내에서 새 계정을 프로비저닝할 수 있습니다.

간소화된 양식을 사용하려면 AWS Control Tower 콘솔에서 Account Factory로 이동한 다음 빠른 계정 프로비저닝을 선택하십시오. AWS Control Tower는 프로비저닝된 계정과 해당 계정에 대해 생성된 싱글 사인온 (IAM Identity Center) 사용자에게 동일한 이메일 주소를 할당합니다. 이 두 이메일 주소를 다르게 설정하려면 Service Catalog를 통해 계정을 프로비저닝해야 합니다.

다른 계정에 대한 업데이트와 마찬가지로 Service Catalog와 AWS Control Tower 계정 팩토리를 사용하여 빠른 계정 프로비저닝을 통해 생성한 계정을 업데이트하십시오.

> **Note**
>
> 2020년 4월, 빠른 계정 프로비저닝 기능은 계정 등록으로 이름이 변경되었습니다. 2022년 6월에는 AWS Control Tower 콘솔에서 계정을 생성하고 업데이트하는 기능과 AWS 계정을 등록하는 기능이 분리되었습니다. 자세한 정보는 기존 계정 등록을 참조하세요.

AWS Control 타워 폐기 도구

2020년 2월 28일

(AWS Control Tower 랜딩 존은 업데이트 필요 없음)

AWS Control Tower는 이제 AWS Control Tower에서 할당한 리소스를 정리하는 데 도움이 되는 자동 폐기 도구를 지원합니다. 기업용 AWS Control Tower를 더 이상 사용할 계획이 없거나 조직 리소스를 대대적으로 재배포해야 하는 경우, 처음 landing Zone을 설정할 때 생성된 리소스를 정리하는 것이 좋습니다.

대부분 자동화된 프로세스를 사용하여 Landing Zone을 AWS Support 해체하려면 필요한 추가 단계에 대한 지원을 받으려면 문의하세요. 해체에 대한 자세한 내용은 을 참조하십시오. 둘러보기: AWS Control Tower 랜딩 존 해체

AWS Control Tower 수명 주기 이벤트 알림

2020년 1월 22일

(AWS Control Tower 랜딩 존은 업데이트 필요 없음)

AWS Control Tower는 수명 주기 이벤트 알림의 가용성을 발표합니다. 수명 주기 이벤트는 AWS Control Tower에서 생성 및 관리하는 조직 단위 (OU), 계정, 규제 항목과 같은 리소스의 상태를 변경할 수 있는 AWS Control Tower 작업이 완료되었음을 나타냅니다. 라이프사이클 이벤트는 이벤트로 기록되고 AWS CloudTrail EventBridge 이벤트로 Amazon에 전달됩니다.

AWS Control Tower는 서비스를 사용하여 수행할 수 있는 작업 (랜딩 존 생성 또는 업데이트, OU 생성 또는 삭제, OU에 대한 제어 활성화 또는 비활성화, 계정 팩토리를 사용하여 새 계정 생성 또는 다른 OU로 계정 이동) 이 완료되면 수명 주기 이벤트를 기록합니다.

AWS Control Tower는 여러 AWS 서비스를 사용하여 모범 사례 다중 계정 AWS 환경을 구축하고 관리합니다. AWS Control Tower 작업이 완료되는 데 몇 분 정도 걸릴 수 있습니다. CloudTrail 로그에서 수명 주기 이벤트를 추적하여 원래 AWS Control Tower 작업이 성공적으로 완료되었는지 확인할 수 있습니다. 수명 주기 이벤트가 CloudTrail 기록될 때 이를 알리거나 자동화 워크플로의 다음 단계를 자동으로 트리거하는 EventBridge 규칙을 생성할 수 있습니다.

2019년 1월 - 12월

2019년 1월 1일부터 12월 31일까지 AWS 컨트롤 타워는 다음과 같은 업데이트를 발표했습니다.

- AWS 컨트롤 타워 버전 2.2의 일반 출시
- AWS Control Tower의 새로운 선택적 제어
- AWS Control Tower의 새로운 탐지 제어
- AWS Control Tower는 관리 계정과 도메인이 다른 공유 계정의 이메일 주소를 수락합니다.
- AWS 컨트롤 타워 버전 2.1의 일반 출시

AWS 컨트롤 타워 버전 2.2의 일반 출시

2019년 11월 13일

(AWS Control Tower 랜딩 존에는 업데이트가 필요합니다. 자세한 내용은 을 참조하십시오랜딩 영역 업데이트.

AWS Control Tower 버전 2.2는 계정 변동을 방지하는 세 가지 새로운 예방 제어 기능을 제공합니다.

- AWS Control Tower에서 설정한 Amazon CloudWatch 로그 로그 그룹 변경 금지
- AWS Control Tower에서 생성한 AWS Config 집계 권한 삭제 금지
- 로그 아카이브 삭제 금지

제어는 전체 AWS 환경에 대한 지속적인 거버넌스를 제공하는 높은 수준의 규칙입니다. AWS Control Tower 랜딩 존을 생성하면 랜딩 존과 모든 조직 단위 (OU), 계정 및 리소스는 선택한 컨트롤에서 적용하는 거버넌스 규칙을 준수합니다. 사용자 및 조직 구성원이 landing Zone을 사용할 때 이 규정 준수 상태가 우발적이든 의도적이든 변경될 수 있습니다. 드리프트 감지를 통해 편차를 해결하기 위해 변경 또는 구성 업데이트가 필요한 리소스를 식별할 수 있습니다. 자세한 정보는 AWS Control Tower의 드리프트 감지 및 해결을 참조하세요.

AWS Control Tower의 새로운 선택적 제어

2019년 9월 5일

(AWS Control Tower 랜딩 존은 업데이트 필요 없음)

AWS Control Tower에는 이제 다음과 같은 네 가지 새로운 선택적 제어 항목이 포함됩니다.

- MFA가 없는 Amazon S3 버킷에서의 삭제 작업 허용 안 함
- Amazon S3 버킷의 복제 구성 변경을 허용하지 않음
- 루트 사용자로서의 작업 허용 안 함
- 루트 사용자의 액세스 키 생성 금지

컨트롤은 전체 AWS 환경에 대한 지속적인 거버넌스를 제공하는 높은 수준의 규칙입니다. 가드레일을 사용하면 정책 의도를 표현할 수 있습니다. 자세한 내용은 AWS Control Tower의 제어에 대한 정보를 참조하십시오.

AWS Control Tower의 새로운 탐지 제어

2019년 8월 25일

(AWS Control Tower 랜딩 존은 업데이트 필요 없음)

AWS Control Tower에는 이제 다음과 같은 8개의 새로운 탐지 제어 항목이 포함됩니다.

- Amazon S3 버킷의 버전 관리가 활성화되었는지 여부 감지
- 콘솔의 IAM 사용자에 대해 MFA가 활성화되었는지 여부 감지 AWS
- IAM 사용자에 대한 MFA 활성화 여부 감지
- Amazon EC2 인스턴스에 대해 Amazon EBS 최적화가 활성화되었는지 여부를 감지합니다.
- Amazon EBS 볼륨이 Amazon EC2 인스턴스에 연결되어 있는지 여부를 감지합니다.
- Amazon RDS 데이터베이스 인스턴스에 대한 퍼블릭 액세스가 활성화되었는지 여부 감지
- Amazon RDS 데이터베이스 스냅샷에 대한 퍼블릭 액세스가 활성화되었는지 여부 감지
- Amazon RDS 데이터베이스 인스턴스에 스토리지 암호화가 활성화되어 있는지 여부를 감지합니다.

제어는 전체 AWS 환경에 대한 지속적인 거버넌스를 제공하는 높은 수준의 규칙입니다. 탐지 컨트롤은 정책 위반과 같은 계정 내 리소스 비준수를 탐지하고 대시보드를 통해 알림을 제공합니다. 자세한 내용은 AWS Control Tower의 제어에 대한 정보를 참조하십시오.

AWS Control Tower는 관리 계정과 도메인이 다른 공유 계정의 이메일 주소를 수락합니다.

2019년 8월 1일

(AWS Control Tower 랜딩 존은 업데이트 필요 없음)

AWS Control Tower에서는 이제 도메인이 관리 계정의 이메일 주소와 다른 공유 계정 (로그 아카이브 및 감사 구성원) 및 하위 계정 (계정 팩토리를 사용하여 판매) 의 이메일 주소를 제출할 수 있습니다. 이 기능은 새 landing Zone을 생성하고 새 자녀 계정을 프로비전할 때만 사용할 수 있습니다.

AWS 컨트롤 타워 버전 2.1의 일반 출시

2019년 6월 24일

(AWS Control Tower 랜딩 존에는 업데이트가 필요합니다. 자세한 내용은 랜딩 존 업데이트를 참조하십시오.

AWS Control Tower는 이제 정식 버전으로 제공되고 프로덕션 용도로 지원됩니다. AWS Control Tower는 새로운 다중 계정 AWS 환경을 설정하고 대규모로 관리하는 가장 쉬운 방법을 찾고 있는 여러 계정과 팀을 보유한 조직을 대상으로 합니다. AWS Control Tower를 사용하면 조직의 계정이 정해진 정책을 준수하도록 할 수 있습니다. 분산된 팀의 최종 사용자는 새 AWS 계정을 빠르게 프로비저닝할 수 있습니다.

AWS Control Tower를 사용하면 다중 계정 구조를 구성하고, 사용자 자격 증명과 페더레이션된 액세스를 관리하고 AWS Organizations, Service Catalog를 통한 계정 프로비저닝 활성화 AWS IAM Identity Center, 및 를 사용하여 중앙 집중식 로그 아카이브를 생성하는 등의 모범 사례를 적용하는 랜딩 존을 설정할 수 있습니다. AWS CloudTrail AWS Config

지속적인 거버넌스를 위해 보안, 운영 및 규정 준수에 대해 명확하게 정의된 규칙인 사전 구성된 제어를 활성화할 수 있습니다. 가드레일을 사용하면 정책을 준수하지 않는 리소스가 배포되는 것을 방지하고 배포된 리소스의 비준수 여부를 지속적으로 모니터링할 수 있습니다. AWS Control Tower 대시보드는 프로비저닝된 계정, 활성화된 제어, 계정의 규정 준수 상태를 비롯한 AWS 환경에 대한 중앙 집중식 가시성을 제공합니다.

AWS Control Tower 콘솔에서 클릭 한 번으로 새로운 다중 계정 환경을 설정할 수 있습니다. AWS Control Tower를 사용하기 위한 추가 요금이나 선결제 약정은 없습니다. Landing Zone을 설정하고 선택된 제어를 구현하도록 설정한 AWS 서비스에 대해서만 비용을 지불하면 됩니다.

문서 이력

- 최신 설명서 업데이트: 2024년 5월 20일

다음 표에는 AWS Control Tower 사용 설명서의 중요한 변경 사항이 설명되어 있습니다. 설명서 업데이트에 대한 알림을 받으려면 RSS 피드를 구독하시면 됩니다.

변경 사항	설명	날짜
AWS Control Tower는 최대 100개의 동시 제어 작업을 지원합니다.	동시 제어 작업 할당량을 100으로 늘렸습니다.	2024년 5월 20일
AWS Control Tower는 AWS 캘거리 서부 (캐나다) 지역에서 사용 가능	AWS Control Tower는 캐나다 서부 (캘거리) 지역에서 사용할 수 있습니다.	2024년 5월 3일
AWS Control Tower는 셀프 서비스 할당량 조정을 지원합니다	AWS Control Tower는 콘솔의 AWS Service Quotas와 통합되어 있습니다.	2024년 4월 25일
제어 관련 설명서를 새 가이드로 옮겼습니다.	AWS Control Tower는 규제 참조 안내서를 게시했습니다.	2024년 4월 21일
리소스에 태그 지정하기 `EnabledControl` AWS CloudFormation	AWS Control Tower는 AWS CloudFormation 템플릿을 통해 `EnabledControl` 리소스에 태그를 추가할 수 있도록 지원합니다.	2024년 2월 22일
베이스라인 API 사용 가능	AWS Control Tower는 프로그래밍 방식으로 OU를 등록하기 위한 새로운 API를 출시했습니다.	2024년 2월 14일
AWS 컨트롤 타워 랜딩 존 버전 3.3	AWS Control Tower 랜딩 존 버전 3.3을 사용할 수 있습니다.	2023년 12월 14일

AWS Control Tower, 디지털 주권을 지원하는 규제 항목 발표	AWS Control Tower는 디지털 주권 요구 사항을 가진 고객을 지원하기 위해 제어 그룹을 출시했습니다.	2023년 11월 27일
AWS Control Tower는 랜딩 존 API를 지원합니다.	AWS Control Tower는 새 API를 사용하여 랜딩 존을 구성하고 시작할 수 있도록 지원합니다.	2023년 11월 26일
AWS Control Tower는 태깅이 가능한 컨트롤을 지원합니다.	AWS Control Tower는 콘솔 및 새 API에서 태깅이 가능한 컨트롤을 지원합니다.	2023년 11월 10일
AWS Control Tower는 아시아 태평양 (멜버른) 에서 사용 가능 AWS 리전	아시아 태평양 (멜버른) 지역에서 사용할 수 있습니다.	2023년 11월 3일
새 제어 API 사용 가능	AWS Control Tower는 새로운 제어 API를 출시했습니다.	2023년 10월 14일
AWS Control Tower, 새로운 규제 항목 출시	AWS Control Tower는 새로운 사전 예방 및 탐지 제어를 출시했습니다.	2023년 10월 5일
AWS Control Tower는 신뢰할 수 있는 액세스를 비활성화하는 데 따른 드리프트를 보고했습니다.	고객이 AWS Control Tower에 대한 신뢰할 수 있는 액세스를 차단한 경우, AWS Control Tower는 드리프트가 발생하면 이를 고객에게 알립니다. AWS Organizations	2023년 9월 21일
AWS Control Tower는 네 가지 추가 버전으로 제공됩니다. AWS 리전	아시아 태평양 (하이데라바드), 유럽 (스페인 및 취리히), 중동 (UAE) 에서 사용할 수 있습니다.	2023년 9월 13일

텔아비브 지역에서 사용 가능한 AWS Control Tower	AWS Control Tower는 텔아비브 지역 il-central-1에서 사용할 수 있습니다.	2023년 8월 28일
AWS Control Tower, 28개의 새로운 사전 예방 제어 기능 출시	AWS Control Tower는 28개의 새로운 사전 예방 제어를 출시했습니다.	2023년 7월 24일
AWS Control Tower는 규제 항목 2개를 더 이상 사용하지 않습니다.	AWS Control Tower는 2023년 8월 18일부터 제어 라이브러리에서 두 개의 컨트롤을 제거합니다.	2023년 7월 18일
AWS Control Tower 랜딩 존 3.2 이용 가능	AWS Control Tower 랜딩 존 버전 3.2를 사용할 수 있습니다.	2023년 6월 16일
AWS Control Tower는 ID를 기반으로 계정을 처리합니다.	AWS Control Tower는 AWS 계정의 이메일 주소가 아닌 계정 ID를 추적합니다.	2023년 6월 14일
추가 Security Hub 탐지 제어 기능 사용 가능	AWS Control Tower는 Security Hub 서비스 관리형 표준인 AWS Control Tower를 위해 제어 라이브러리에 10개의 새로운 제어 항목을 추가합니다.	2023년 6월 12일
AWS Control Tower는 제어 메타데이터 테이블을 게시합니다.	AWS Control Tower는 이제 게시된 설명서의 일부로 제어 메타데이터 테이블을 제공합니다.	2023년 6월 7일
Account Factory 커스터마이징을 위한 테라폼 지원	AFC의 Terraform 오픈 소스 블루프린트에 대한 단일 지역 지원.	2023년 6월 6일

AWS 랜딩 존에 사용할 수 있는 IAM 자체 관리	AWS Control Tower는 이제 고객이 랜딩 존으로 사용할 ID 공급자를 선택할 수 있도록 지원합니다.	2023년 6월 6일
새 역할 추가	AWS Control Tower는 새로운 서비스 연결 역할 및 관련 정책을 추가했습니다. AWSServiceRoleForAWSControlTowerAWSControlTowerAccountServiceRolePolicy	2023년 6월 1일
복합 거버넌스 업데이트	복합 거버넌스에 대해 고객에게 알리기 위한 업데이트.	2023년 6월 1일
추가 사전 예방 제어 기능 사용 가능	새로운 사전 예방 제어를 통해 다중 계정 환경을 관리하고 특정 규제 목표를 충족할 수 있습니다.	2023년 5월 19일
7개의 추가 지역 사용 가능	이제 AWS Control Tower를 캘리포니아 북부 (샌프란시스코), 아시아 태평양 (홍콩, 자카르타, 오사카), 유럽 (밀라노), 중동 (바레인), 아프리카 (케이프타운) 등 7개 지역에서 추가로 사용할 수 AWS 리전있습니다.	2023년 4월 19일
관리형 정책으로 변경	AWS Control Tower가 AWS 계정 관리 서비스에 의해 구현된 `EnableRegion` `ListRegions` ,, `GetRegionOptStatus` API를 호출할 수 AWSControlTowerServiceRolePolicy있도록 변경했습니다.	2023년 4월 6일

계정 사용자 지정 요청 추적은 일반적으로 사용할 수 있습니다.	AWS Control Tower는 이제 Account Factory for Terraform (AFT) 워크플로를 사용하여 계정 사용자 지정 요청을 추적하는 기능을 지원합니다.	2023년 2월 16일
IAM 모범 사례 업데이트	IAM 모범 사례 권장 사항에 맞게 가이드가 업데이트되었습니다. 자세한 내용은 IAM의 보안 모범 사례를 참조하세요.	2023년 2월 15일
AWS Control Tower 랜딩 존 3.1 이용 가능	AWS Control Tower 랜딩 존 3.1을 사용할 수 있습니다.	2023년 2월 9일
사전 예방적 제어는 일반적으로 사용 가능합니다.	사전 예방적 제어는 미리 보기 상태부터 일반 공급까지 시작됩니다.	2023년 1월 24일
동시 계정 운영	AWS Control Tower는 이제 어카운트 팩토리에서 최대 5개의 동시 작업을 지원합니다. 한 번에 최대 5개의 계정을 생성, 업데이트 또는 등록할 수 있습니다.	2022년 12월 16일
사전 예방적 제어는 리소스 프로비저닝을 지원합니다.	AWS Control Tower는 이제 AWS CloudFormation 후크를 통해 구현되는 사전 예방적 제어를 지원합니다.	2022년 11월 28일
어카운트 팩토리 사용자 지정 가능	AWS Control Tower는 이제 AWS Control Tower 콘솔에서 직접 블루프린트라고 하는 사용자 지정 가능한 계정 템플릿을 사용하여 계정 프로비저닝을 지원합니다.	2022년 11월 28일

모든 규칙의 규정 준수 상태를 볼 수 있습니다. AWS Config	이제 AWS Control Tower는 AWS Control Tower에 등록된 조직 단위에 배포된 모든 AWS Config 규칙의 규정 준수 상태를 표시합니다.	2022년 11월 18일
관리형 정책으로 변경	Account Factory 사용자 지정에 필요한 `AWSControlTowerBlueprintAccess` 역할을 AWS Control Tower가 맡을 수 AWSControlTowerServiceRolePolicy있도록 변경했습니다.	2022년 10월 28일
제어, 리소스용 API AWS CloudFormation	AWS Control Tower는 이제 일련의 API 호출과 새로운 AWS CloudFormation 리소스를 통해 컨트롤의 활성화 및 비활성화를 지원합니다.	2022년 9월 1일
CFCT는 스택 세트 삭제를 지원합니다.	CFCT는 매니페스트 파일에 매개변수를 설정하여 스택 세트 삭제를 지원합니다.	2022년 8월 26일
맞춤형 로그 보존	AWS Control Tower CloudTrail 로그를 저장하는 Amazon S3 버킷의 보존 정책을 일 또는 년 단위로 최대 15년까지 사용자 지정할 수 있습니다.	2022년 8월 15일
역할 드리프트 복구가 가능합니다.	AWS Control Tower는 착륙 지대를 완전히 수리하지 않고도 역할 드리프트에 대한 수리를 지원합니다.	2022년 8월 11일

버전 3.0 사용 가능	AWS Control Tower landing Zone 버전 3.0은 계정 기반 AWS CloudTrail 트레일에서 조직 기반 트레일로 변경되며, 조직 수준의 트레일을 활성화하도록 관리형 정책을 업데이트합니다. 이를 통해 거주 지역에서만 정보를 집계할 수 있습니다. AWS Config 버전 3.0에는 지역 거부 제어에 대한 업데이트와 두 개의 새로운 탐지 제어 기능도 포함되어 있습니다.	2022년 7월 29일
조직 페이지에는 OU와 계정의 뷰가 결합되어 있습니다.	AWS Control Tower의 새 조직 페이지에는 모든 조직 단위(OU) 및 계정의 계층적 보기가 표시됩니다.	2022년 7월 18일
관리형 정책으로 변경	고객이 조직 수준의 AWS CloudTrail 트레일을 사용하여 로그를 집계할 수 AWSControlTowerServiceRolePolicy있도록 변경했습니다. AWS CloudTrail	2022년 6월 20일
회원 계정 등록 및 업데이트가 더 쉬워졌습니다.	이제 AWS Control Tower는 랜딩 존 내에서 회원 계정을 개별적으로 등록하고 업데이트할 수 있는 기능을 제공합니다. 각 계정에는 업데이트가 가능한 시기가 표시됩니다. 계정 등록 버튼을 Account Factory의 계정 생성 워크플로와 분리했습니다.	2022년 5월 31일

AFT는 공유 계정의 사용자 지정을 지원합니다.	Terraform용 AWS Control Tower Account Factory는 이제 AWS Control Tower 관리 계정, 로그 아카이브 및 감사 계정에 대한 사용자 지정을 지원합니다.	2022년 5월 27일
모든 선택적 제어에 대한 동시 운영	AWS Control Tower에서는 이제 선택적 예방 가데일과 탐지 제어를 동시에 적용 및 제거할 수 있습니다.	2022년 5월 18일
기존 보안 및 로깅 계정	AWS Control Tower는 이제 착륙 영역 설정 중에 새 계정을 생성하는 대신 기존 보안 및 로깅 계정을 가져오는 기능을 지원합니다.	2022년 5월 16일
버전 2.9를 사용할 수 있습니다.	AWS Control Tower 랜딩 존 버전 2.9는 Python 버전 3.9 런타임을 사용하도록 알림 전달자 Lambda를 업데이트합니다.	2022년 4월 22일
AWS 모범 사례에 대한 지원이 업데이트되어 버전 2.8이 제공됩니다.	AWS Control Tower 랜딩 존 버전 2.8은 워크로드와 AWS 계정이 AWS 모범 사례에 부합하도록 하기 위한 추가 지원을 제공합니다.	2022년 2월 10일
지역 거부 제어	AWS Control Tower에는 이제 AWS 지역에 대한 액세스를 제한하고 규정 준수 및 규제 문제를 해결하는 데 도움이 되는 제어 기능이 포함되어 있습니다.	2021년 11월 30일

데이터 레지던시 제어	AWS Control Tower는 이제 세분화된 제어를 통해 데이터 레지던시를 관리하는 데 도움이 되는 제어를 지원합니다.	2021년 11월 30일
테라폼용 AWS Control Tower 어카운트 팩토리	AWS Control Tower는 이제 자동화된 계정 프로비저닝 및 업데이트를 위해 Terraform을 지원합니다.	2021년 11월 29일
새 수명 주기 이벤트 제공	`PrecheckOrganizationalUnit` 이벤트는 중첩된 OU의 리소스를 포함하여 거버넌스 확장 작업의 성공을 가로막는 리소스가 있는지 여부를 기록합니다.	2021년 11월 18일
중첩된 OU 사용 가능	AWS Control Tower는 이제 랜딩 존에 중첩된 OU 구조를 포함할 수 있도록 지원합니다.	2021년 11월 16일
Detective Control 동시성	AWS Control Tower 탐지 제어는 이제 동시 활성화 및 비활성화 작업을 지원합니다.	2021년 11월 5일
두 개의 새로운 리전을 이용할 수 있습니다.	AWS Control Tower는 이제 두 개의 새로운 AWS 지역, 즉 유럽 (파리) 지역과 남아메리카 (상파울루) 지역에서 사용할 수 있습니다.	2021년 7월 29일
지역 선택 취소	AWS Control Tower를 통해 더 이상 관리하지 않으려는 AWS 지역의 선택을 취소할 수 있습니다.	2021년 7월 29일

KMS 키를 사용할 수 있습니다.	원하는 경우 관리하는 KMS 키를 만들거나 선택하여 데이터와 리소스를 암호화할 수 있습니다.	2021년 7월 28일
관리형 정책으로 변경	고객이 자신의 KMS 암호화 키를 AWS CloudTrail 로그에 사용할 수 AWSControlTowerServiceRolePolicy있도록 변경했습니다.	2021년 7월 28일
컨트롤 이름은 변경되었지만 기능은 변경되지 않았습니다.	일부 컨트롤 이름 및 설명은 기능 변경 없이 컨트롤의 정책 의도를 더 잘 반영하도록 업데이트되었습니다.	2021년 7월 26일
관리 대상 SCP의 자동 스캔	AWS Control Tower는 관리형 SCP를 매일 자동 스캔하여 드리프트를 확인합니다.	2021년 5월 11일
OU 및 계정의 사용자 지정 이름	AWS Control Tower를 사용하면 랜딩 존 설정 프로세스 중에 드리프트를 생성하지 않고도 필수 OU 및 계정에 대한 사용자 지정 이름을 제공할 수 있습니다.	2021년 4월 16일
랜딩 존 해체는 셀프 서비스입니다.	이제 AWS Control Tower를 사용하면 지원 부서에 AWS 문의하지 않고도 랜딩 존을 해제할 수 있습니다. 해제는 취소할 수 없는 반자동 프로세스입니다. 모든 AWS Control Tower 리소스를 수동으로 삭제하는 것과는 다릅니다.	2021년 4월 9일

세 개의 추가 지역	이제 AWS Control Tower를 아시아 태평양 (도쿄) 지역, 아시아 태평양 (서울) 지역, 아시아 태평양 (뭄바이) 지역의 3개 추가 AWS 지역에서 사용할 수 있습니다.	2021년 4월 8일
새로운 로그 아카이브 컨트롤, landing Zone 버전 2.7 사용 가능	새로운 Log Archive 제어 항목 4개는 AWS Control Tower 외부의 리소스 거버넌스와는 별도로 AWS Control Tower 리소스에 대한 Log Archive 거버넌스를 제공합니다. 기존 규제 항목 4개에 대한 지침이 필수 항목에서 선택 항목으로 변경되었습니다. AWS Control Tower 랜딩 존 버전 2.7에는 업데이트 후에는 취소할 수 없는 HTTPS 요구 사항이 포함되어 있습니다.	2021년 4월 8일
지역 선택	AWS Control Tower 지역 선택은 AWS Control Tower 리소스의 지리적 위치를 더 잘 관리할 수 있는 기능을 제공합니다. 규정 준수, 규제, 비용 또는 기타 이유로 AWS 리소스 또는 워크로드를 호스팅하는 지역의 수를 늘리기 위해 이제 관리할 추가 지역을 선택할 수 있습니다.	2021년 2월 19일
OU를 등록하면 AWS Control Tower의 모든 계정을 한 번에 관리할 수 있습니다.	AWS Control Tower는 OU를 등록하는 기능을 추가하는데, 이는 여러 계정을 동시에 거버넌스로 전환하는 방법입니다.	2021년 1월 28일

등록된 OU의 여러 계정 업데이트	이제 AWS Control Tower 대시보드에서 클릭 한 번으로 최대 300개의 계정을 포함하는 등록된 AWS Organizations 조직 단위 (OU) 의 모든 계정을 업데이트할 수 있습니다. 대량 업데이트라고도 하는 다중 계정 업데이트 기능을 사용하면 한 번에 하나의 계정을 업데이트하거나 외부 스크립트를 사용하여 여러 계정에서 업데이트를 동시에 수행할 필요가 없습니다.	2021년 1월 28일
관리되지 않는 OU 및 계정을 집계하기 위한 새로운 역할	새 역할은 외부 AWS Config 규칙을 탐지하는 데 도움이 되므로 AWS Control Tower는 관리되지 않는 계정에 대한 액세스 권한을 얻을 필요가 없습니다.	2020년 12월 29일
AWS Control Tower는 더 많은 AWS 지역에서 사용할 수 있습니다.	이제 AWS Control Tower를 아시아 태평양 (싱가포르) 지역, 유럽 (프랑크푸르트) 지역, 유럽 (런던) 지역, 유럽 (스톡홀름) 지역, 캐나다 (중부) 지역에 배포할 수 있습니다. 이번 출시로 이제 AWS Control Tower를 10개 AWS 지역에서 사용할 수 있습니다. 이 Landing Zone 업데이트에는 나열된 모든 지역이 포함되며 취소할 수 없습니다. 랜딩 존을 버전 2.5로 업데이트한 후에는 지원되는 AWS 10개 지역을 관리하도록 AWS Control Tower에 등록된 모든 계정을 수동으로 업데이트해야 합니다.	2020년 11월 18일

컨트롤 업데이트	필수 제어를 위한 업데이트 버전이 출시되었습니다`AWS-GR_IAM_ROLE_CHANGE_PROHIBITED` . 업데이트된 컨트롤을 사용하면 계정을 더 쉽게 자동으로 등록할 수 있습니다.	2020년 10월 8일
이제 AWS Control Tower에서 관련 정보 페이지를 사용할 수 있습니다.	관련 정보 페이지를 사용하면 AWS Control Tower 랜딩 존을 설정한 후 도움이 될 수 있는 일반적인 작업을 더 쉽게 찾을 수 있습니다.	2020년 9월 18일
AWS Control Tower 콘솔에는 OU 및 계정에 대한 자세한 정보가 나와 있습니다.	AWS Control Tower 콘솔에서 AWS 계정 및 조직 단위 (OU)에 대한 세부 정보를 볼 수 있습니다. 이제 '계정' 페이지에는 OU 또는 AWS Control Tower의 등록 상태와 상관없이 조직의 모든 계정이 나열됩니다. 이제 모든 테이블을 검색, 정렬 및 필터링할 수 있습니다.	2020년 7월 22일
AWS Control Tower를 사용하면 기존 조직이 랜딩 존을 설정할 수 있습니다.	이제 기존 조직에 AWS Control Tower의 랜딩 존을 설치하여 조직을 거버넌스로 전환할 수 있습니다. AWS Control Tower의 Quick 계정 프로비저닝 기능은 Enroll 계정으로 이름이 변경되었으며, 이제 기존 AWS 계정을 등록하고 새 계정을 생성할 수 있습니다.	2020년 4월 16일

AWS Control Tower는 이제 아시아 태평양 지역에서 사용할 수 있습니다.	이제 AWS Control Tower를 아시아 태평양 (시드니) AWS 지역에 배포할 수 있습니다. 이번 릴리스에는 벤더 계정을 수동으로 업데이트해야 하며, 아시아 태평양 (시드니) 에서 워크로드를 실행하려는 경우에만 업데이트해야 합니다.	2020년 3월 3일
AWS Control Tower 랜딩 존을 폐기할 수 있습니다.	AWS Support는 수동 정리가 필요하지만 조직을 보존하는 대부분 자동화된 프로세스를 통해 랜딩 존을 영구적으로 비활성화할 수 있도록 지원합니다.	2020년 2월 27일
AWS Control Tower에서 빠른 계정 프로비저닝을 사용할 수 있습니다.	빠른 계정 프로비저닝을 통해 랜딩 영역이 최신 상태일 때 계정 등록 기능을 사용하여 새 멤버 계정을 쉽게 시작할 수 있습니다.	2020년 2월 20일
수명 주기 이벤트는 AWS Control Tower에서 추적됩니다.	수명 주기 이벤트는 일부 워크플로 자동화를 더 쉽게 하기 위해 특정 AWS Control Tower 이벤트에 대한 추가 세부 정보를 제공합니다.	2019년 12월 12일
설정 및 활동 페이지는 AWS Control Tower에서 사용할 수 있습니다.	설정 및 활동 페이지를 사용하면 랜딩 존 업데이트 및 기록된 이벤트 확인을 보다 쉽게 수행할 수 있습니다.	2019년 11월 30일
AWS Control Tower에는 추가 예방 제어 기능을 사용할 수 있습니다.	AWS Control Tower의 예방 제어를 통해 조직과 리소스를 환경에 맞게 조정할 수 있습니다.	2019년 9월 6일

AWS Control Tower에는 추가 탐지 제어 기능을 사용할 수 있습니다.	AWS Control Tower의 Detective 컨트롤은 조직 및 리소스 상태에 대한 정보를 제공합니다.	2019년 8월 27일
AWS Control Tower는 이제 정식 버전으로 제공됩니다.	AWS Control Tower는 다중 계정 AWS 환경을 대규모로 설정하고 관리할 수 있는 가장 쉬운 방법을 제공하는 서비스입니다.	2019년 6월 24일

AWS 용어집

최신 AWS 용어는 참조의 AWS 용어집을 참조하십시오.AWS 용어집

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