aws professional services

Control Tower Hands-on Training Guide

AWS Professional Services

Prerequisite

Prerequisite

- 개인 이메일 계정으로 AWS 서비스 신규 가입 (Gmail 추천)
- 신규 가입 시, 아래와 같은 "+" 기호와 Alias를 조합하여 기존 이메일 계정으로 여러 AWS 계정을 생성할 수 있음
- 향후 Control Tower 실습 종료 후, Alias 형태로 생성된 AWS 계정들을 Suspend 할 예정
- Alias 형식의 이메일은 모두 원래 Email 사서함으로 수신됨 (각종 이메일 인증 및 Notification 등)

< 예시 >

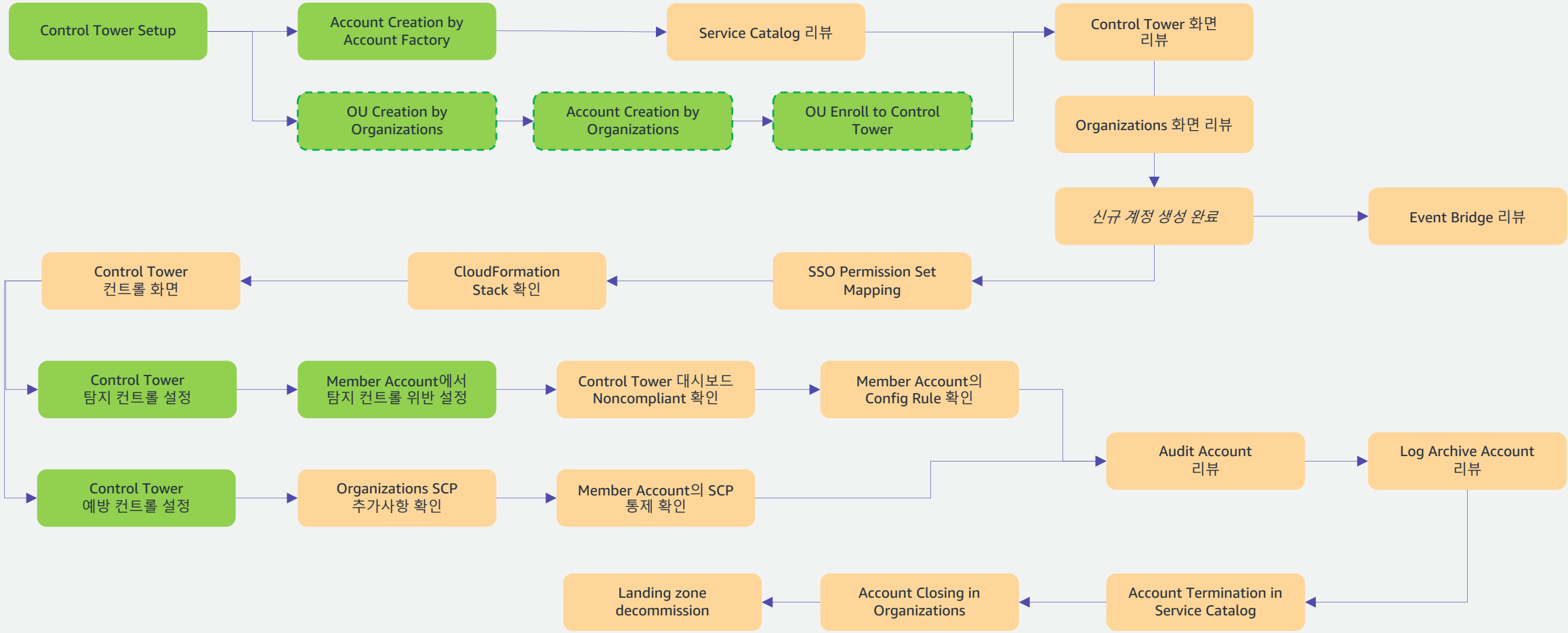
Email 사서함	AWS 계정	용도	생성방법
gildong@gmail.com	gildong+ct1@gmail.com	Control Tower Management 계정	AWS 사이트에서 신규 계정 생성
	gildong+ct1audit@gmail.com	Control Tower Audit 계정	Control Tower Setup 시 자동생성
	gildong+ct1log@gmail.com	Control Tower Log Archive 계정	Control Tower Setup 시 자동생성

Prerequisite

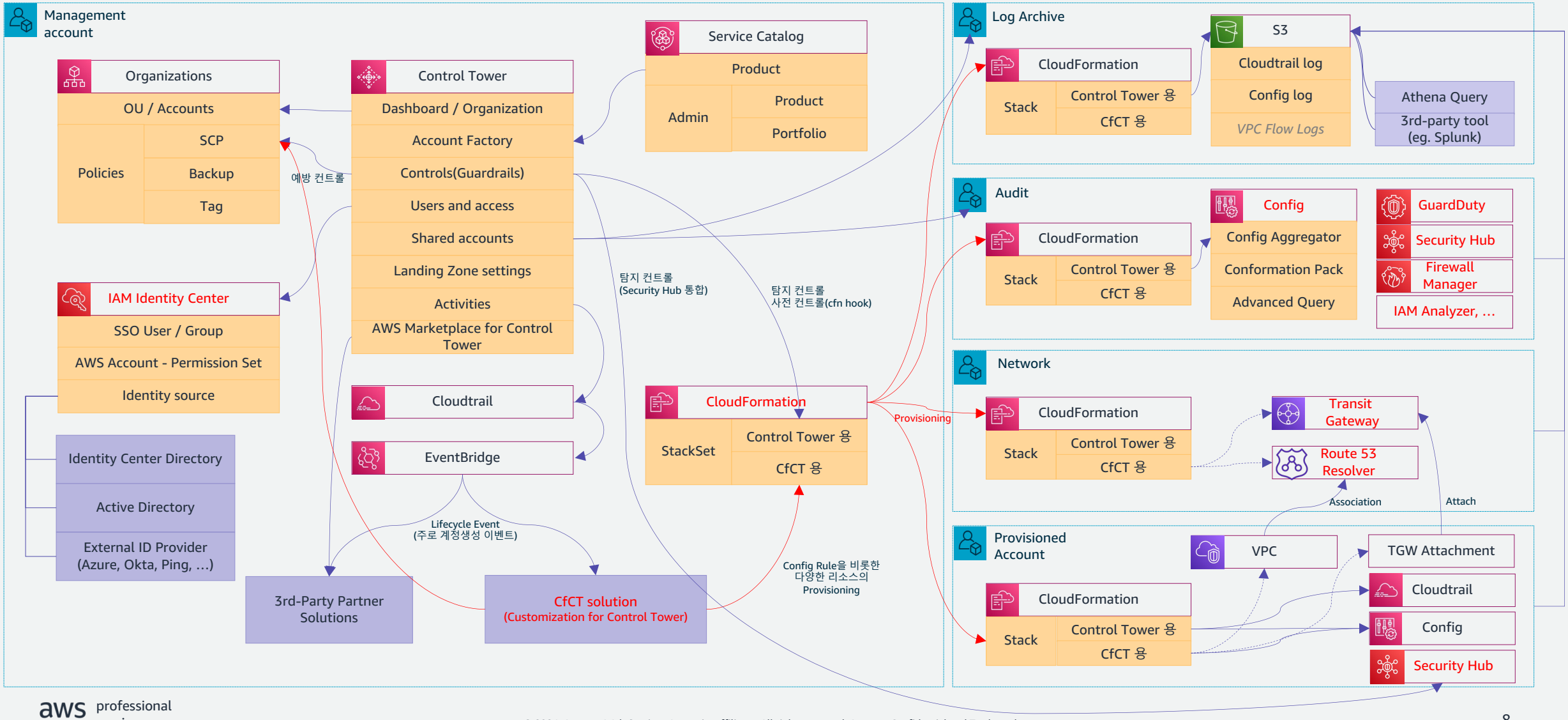
- Control Tower Management 계정에 Root로 로그인 후, AdministratorAccess 권한의 IAM User 생성
- Account 설정으로 이동하여 “결제 정보에 대한 IAM 사용자 및 역할 액세스(IAM User and Role Access to Billing Information)”에서 IAM Access를 활성화 함 → IAM User가 Billing 정보를 조회할 수 있도록 허용
- Root에서 로그아웃 하고, 생성한 IAM User로 로그인
- **Region은 Seoul Region으로 선택 (ap-northeast-2)**
- Budget Report 설정 : Budget 및 Budget Report 설정하여, Daily로 비용정보를 메일로 수신할 수 있도록 함
- Control Tower 자체 실습에 필요한 비용은 몇 천원 수준 (적용하는 가드레일 개수에 따라 다름)

Control Tower Hands-on Scenario

Control Tower hands-on scenario



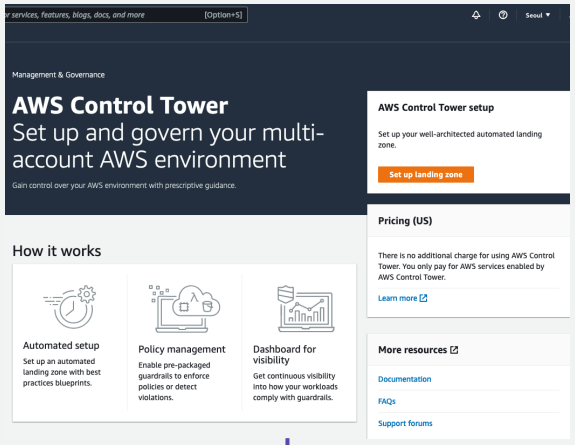
Control Tower Relation Map

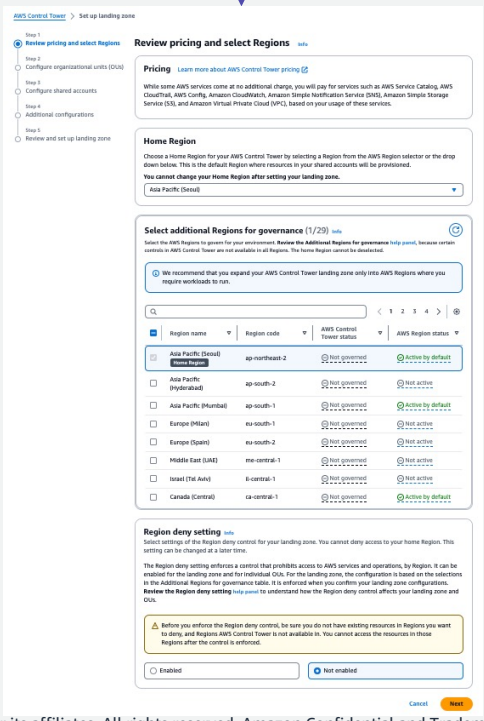


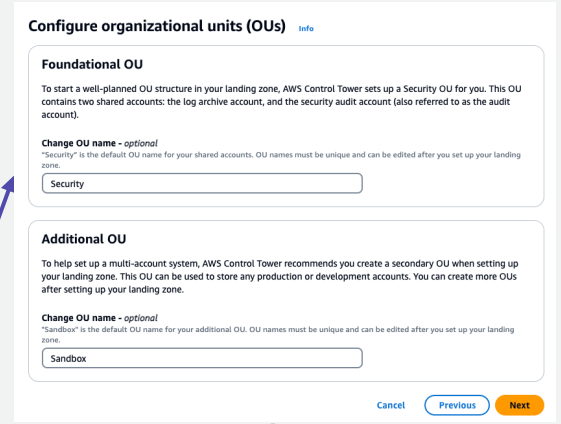
Control Tower Hands-on Start!

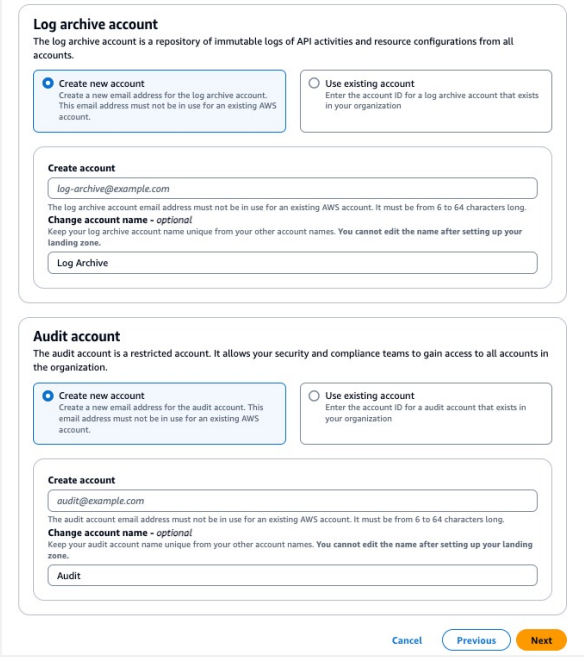
Control Tower Setup

- Home Region 선택
  - Region deny setting은 Home Region 및 Additional Region 외의 모든 Region에 대해서는 접근을 금지하는 옵션으로써, 강력한 Region 거버넌스를 가져갈 경우에 세팅
- OU 구성
  - Security 및 추가 OU(Sandbox 등) 생성
- Shared accounts 구성
  - Log Archive, Audit 계정의 이메일 주소 입력(기존에 AWS에서 사용된 적이 없는 이메일)



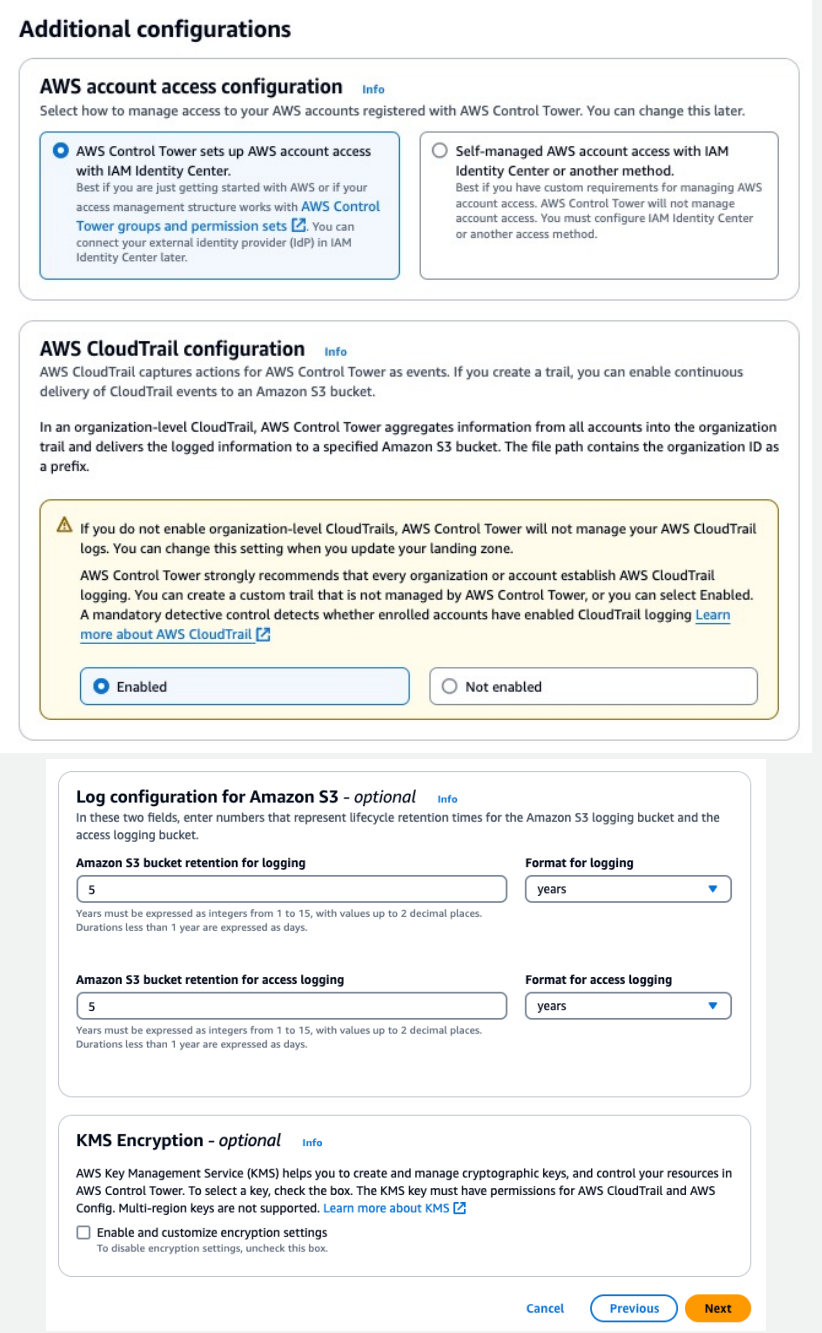






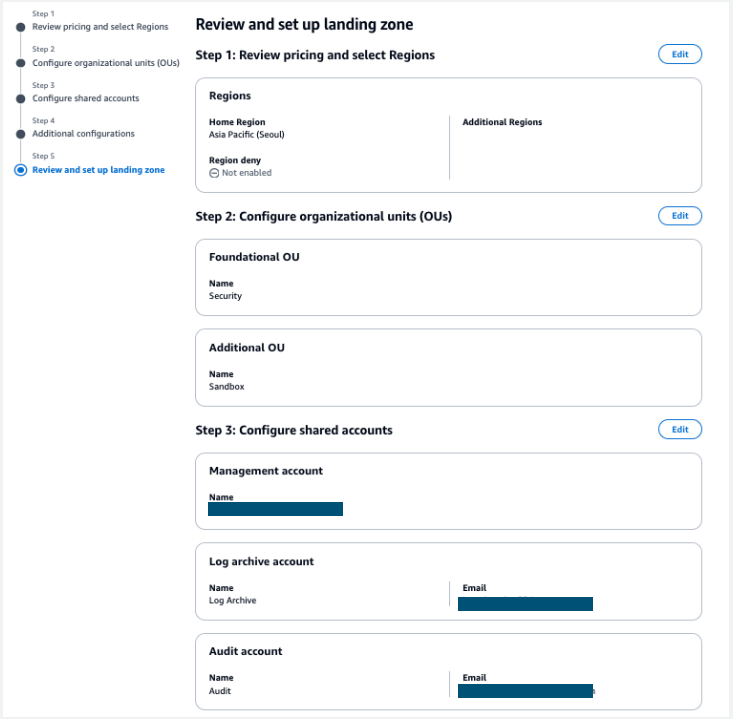
Control Tower Setup

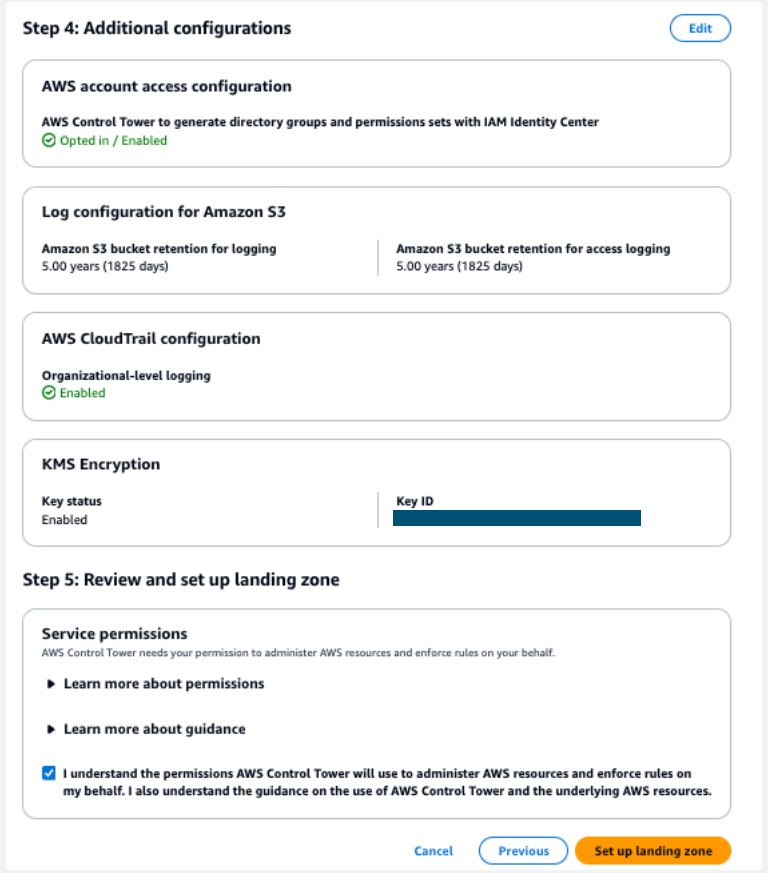
- CloudTrail 및 KMS 암호화 구성
  - Organization-level 활성화를 선택
  - Control Tower 리소스를 Customer KMS로 암호화 할 때 체크 (https://docs.aws.amazon.com/controltower/latest/userguide/configure-kms-keys.html#kms-key-policy-update)



Control Tower Setup

- review checkbox 체크 후 setup landing zone 선택
- 20~30분 소요





Limitation

- https://docs.aws.amazon.com/controltower/latest/userguide/limits.html
- OU 당 5개의 SCP까지 적용 가능
  - Control Tower의 Preventive Control은 Control Tower가 1개의 SCP로 관리
  - 사용자가 추가로 Organization에 SCP를 추가 적용 시 고려해야 함
- Nested OU 깊이는 5개까지 지원 (Root 기준)
  - Ex) RootOU – RegionOU - PrdOU – BusinessOU - WorkloadsOU
- 300개의 Account를 초과하는 OU는 Control Tower에 Register 할 수 없음
- 신규 Account 생성 시, 자동으로 Service Quota를 증가시키거나 Enterprise Support 등록신청이 가능
  - Automate Service Limit Increases
  - Automating Service Limit Increases and Enterprise Support with AWS Control Tower

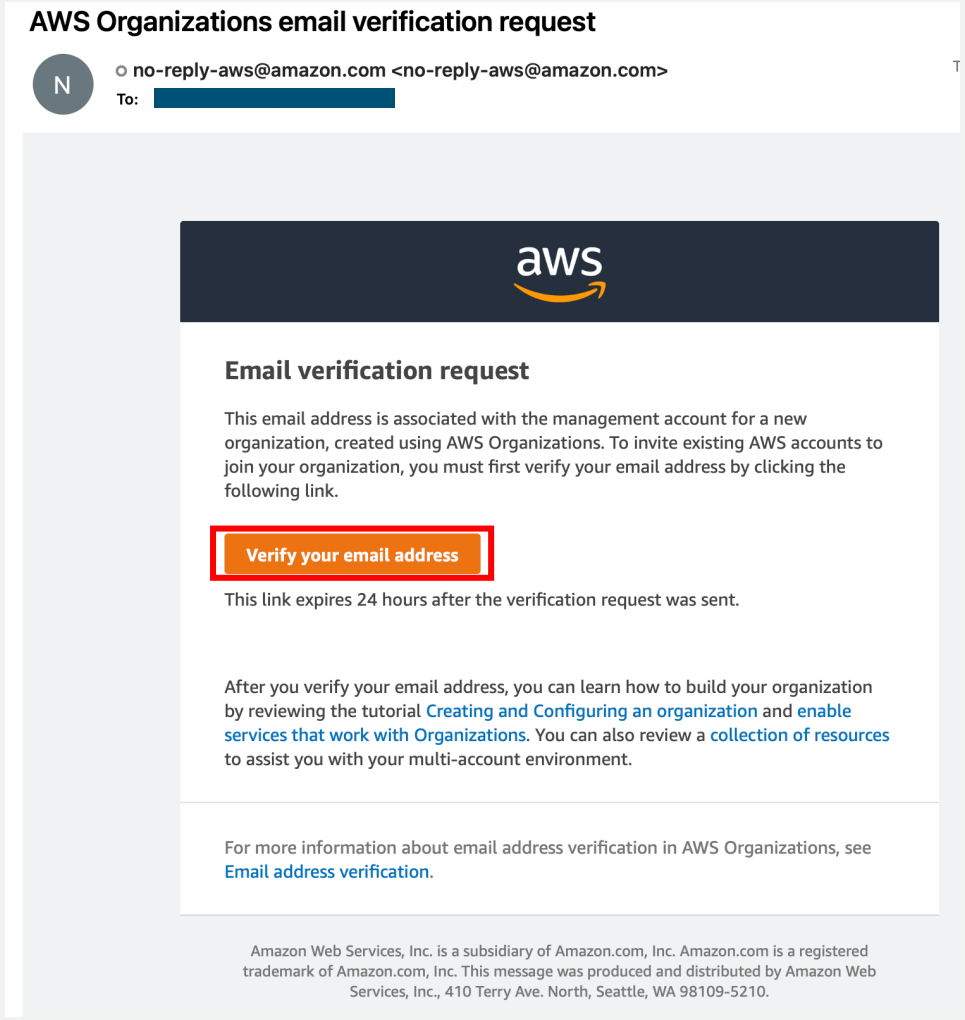
Landing zone setup 시 Administrator를 위한 Tip

- Home Region에서 Setup 하며, Multi Region을 사용할 경우는 가장 워크로드와 로그가 많이 발생하는 Region에 Setup (비용 절감)
- Control Tower에 의해 VPC를 생성할 경우, Control Tower 관리 하에 있는 Region의 Default VPC는 삭제됨. 이 경우 Control Tower로 관리하지 않는 Region은 Control Tower의 Region deny 기능을 사용하거나, Default VPC를 모두 삭제할 것을 권고
- Control Tower에 등록(Enroll)된 OU의 SCP는 수정하지 말고 새로운 SCP를 추가하여 적용할 것
- Control Tower에 등록된 계정은 Organizations에서 OU를 이동하지 말고, Service Catalog의 Product update를 통해 OU 변경 할 것
- Control Tower Account Provisioning 자동화 방법
  - Service Catalog API : Walkthrough: Automated account provisioning in AWS Control Tower
  - Control Tower Account Factory for Terraform(AFT) : Provision accounts with AWS Control Tower Account Factory for Terraform
  - How to automate the creation of multiple accounts in AWS Control Tower

Control Tower Setup과정에서 **AWS Organization**과 **AWS IAM Identity Center SNS** 구성이 진행됩니다.

AWS Organizations email verification request

- AWS Control Tower 생성 이메일로 확인 요청 메일 수신
- 메일 인증 후 AWS Organizatioin 관리 화면 표시

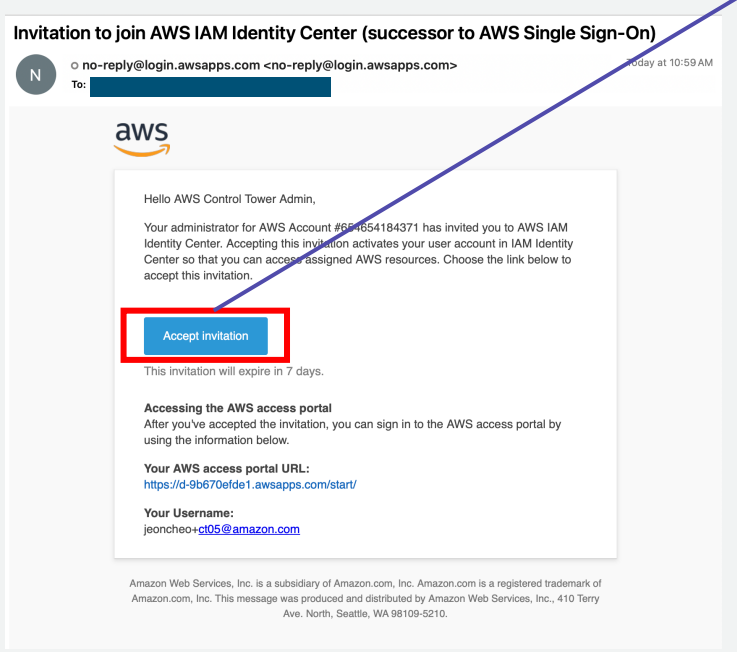


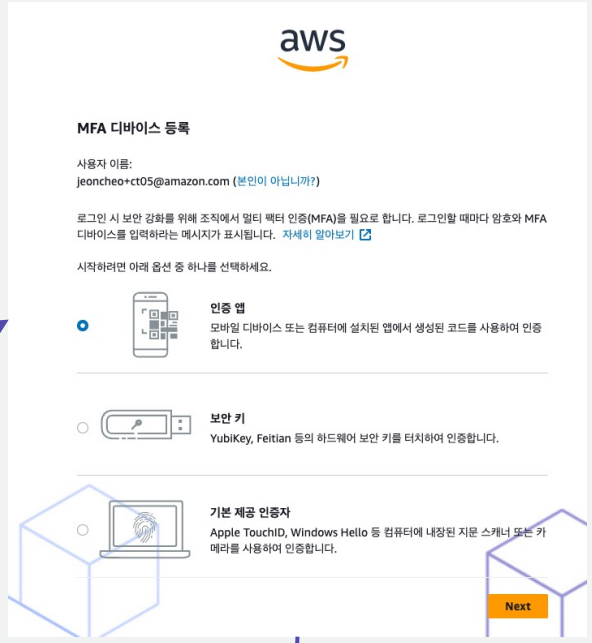
Invitation to join AWS IAM Identity Center

- AWS AWS IAM Identity Center invitation 메일 수신
- “Accept Invitation” 이후 MFA 디바이스 등록 화면 표시됨
- MFA 디바이스 타입 선택 후 등록

Ex) 인증 앱 “google authenticator”다운로드 후

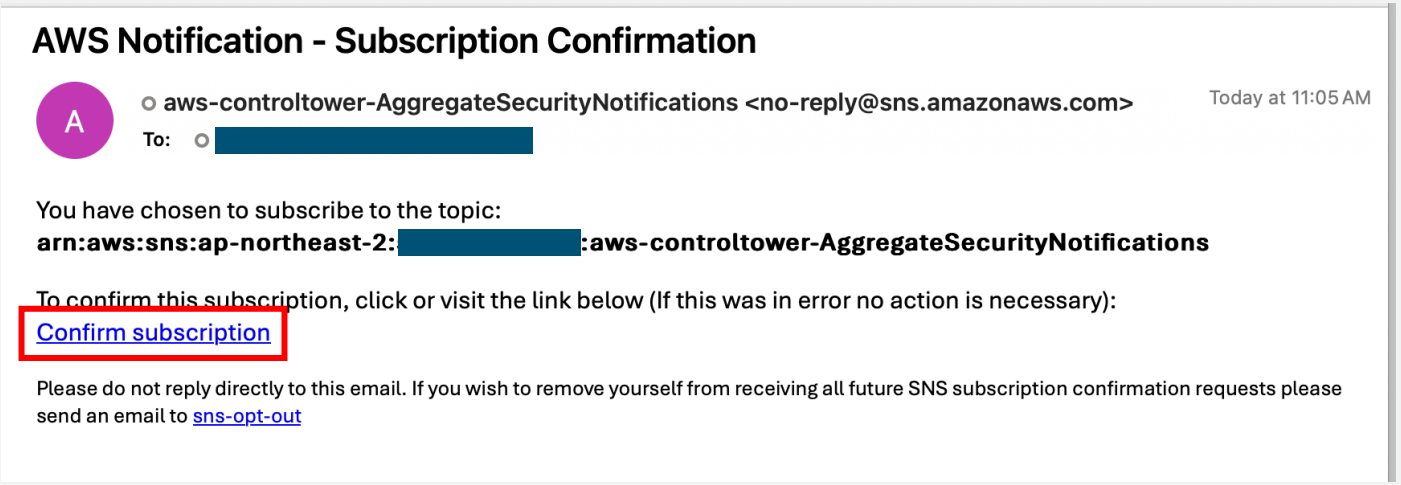
QR 코드 등록

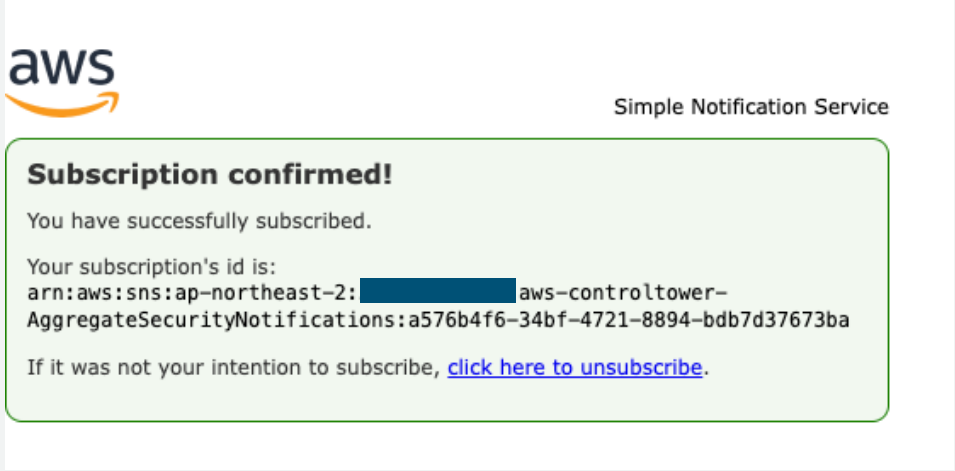




AWS Notification Subscription

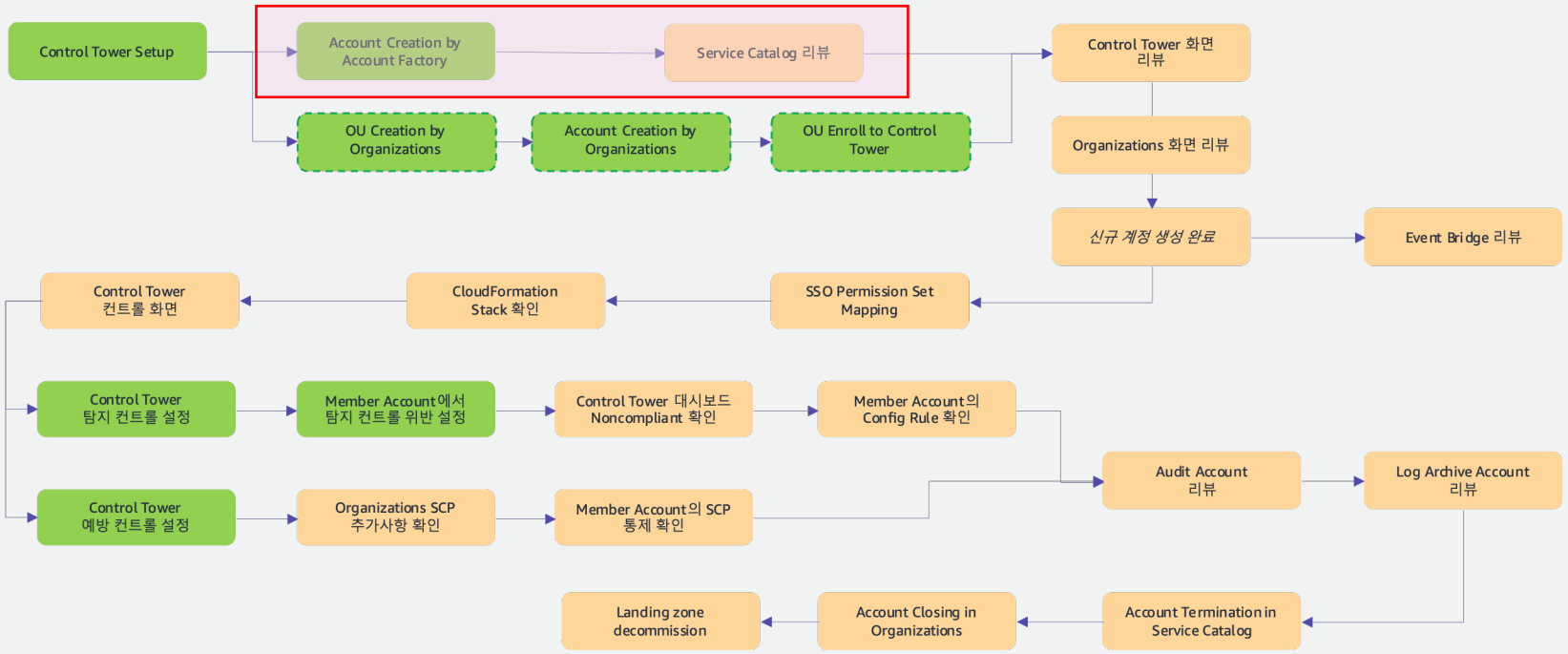
- AWS Control Tower Security Event 수신을 위한 SNS 구독 메일 수신
- " Confirm subscription" 선택





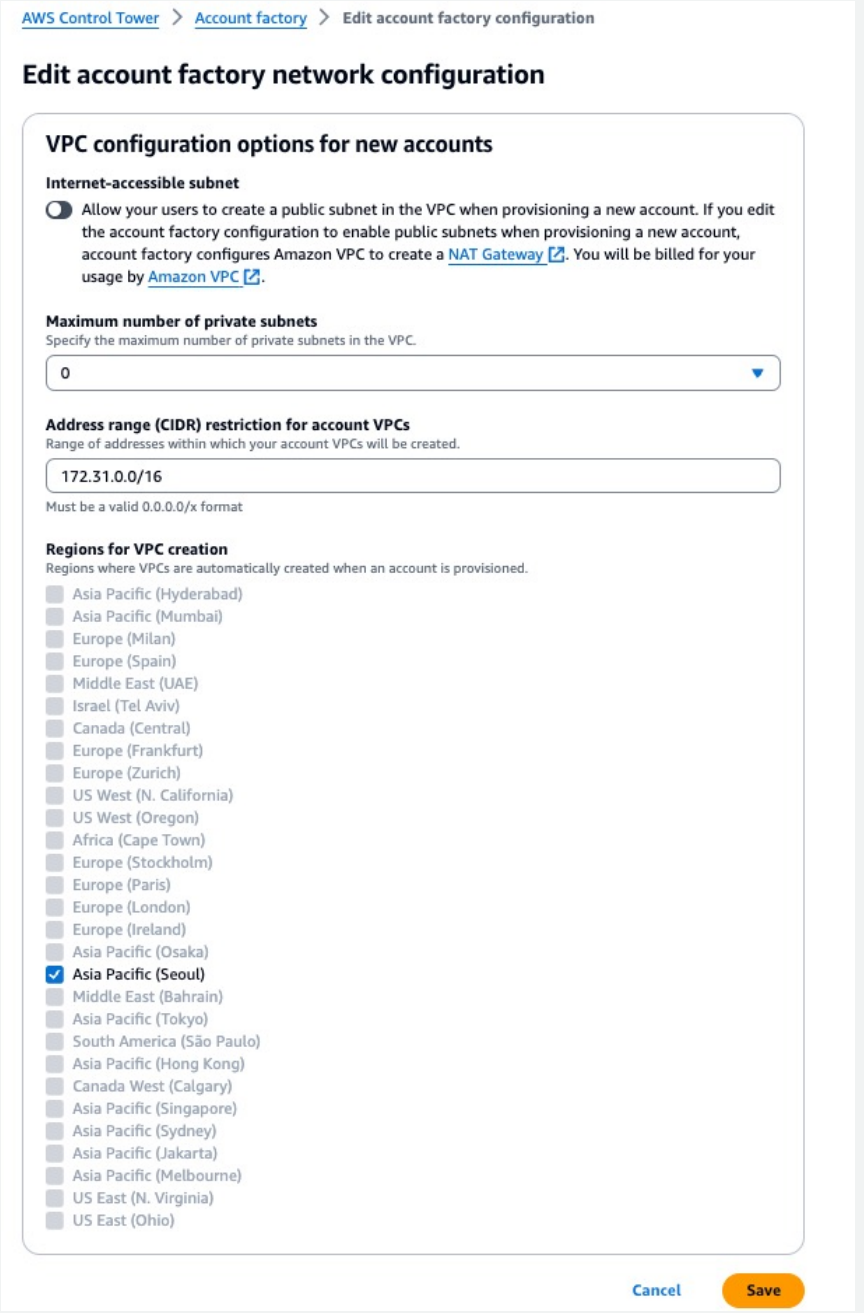
Control Tower Setup이 완료된 후, **AWS Account** 생성을 시작합니다.

Account 생성



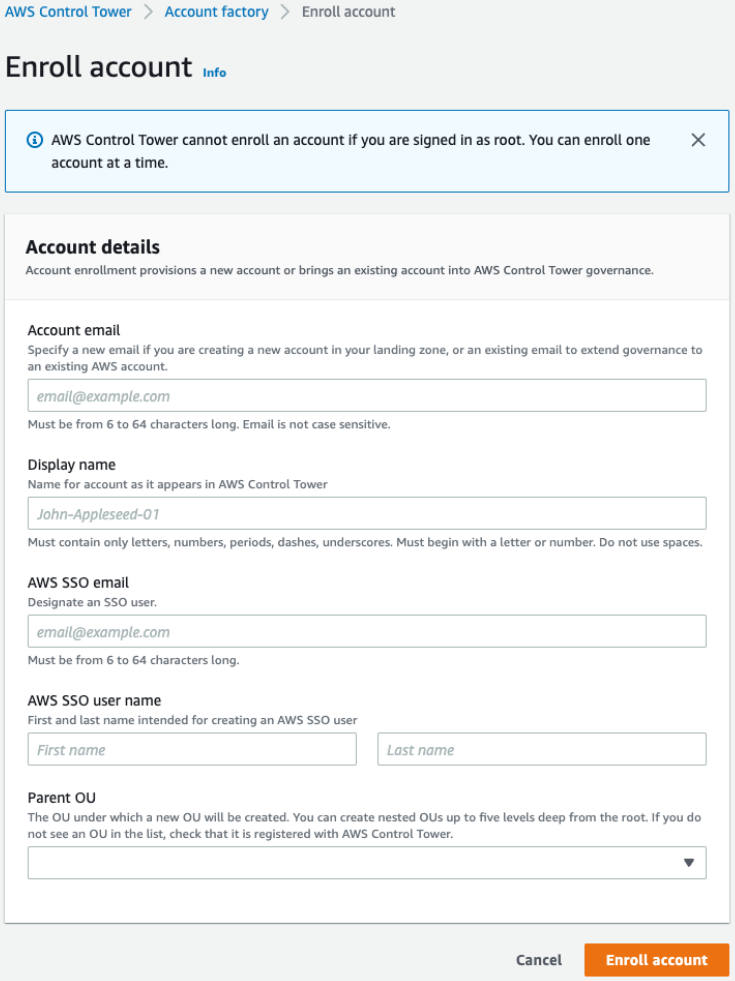
Account Factory - VPC Setting

- Admin이 CIDR을 수작업으로 지정해야 함
- Internet-accessible subnet을 활성화할 경우, NAT Gateway가 생성되므로 비용 부과에 유의
- Control Tower용 Default VPC 생성을 하지 않을 경우에는 Maximum number of private subnets를 0으로 설정하고 모든 Region에 체크를 해제
- TIP : Control Tower Account 생성 시, 모든 Region의 Default VPC를 삭제하고 싶다.
  - https://aws.amazon.com/blogs/mt/customizing-account-configuration-aws-control-tower-lifecycle-events/



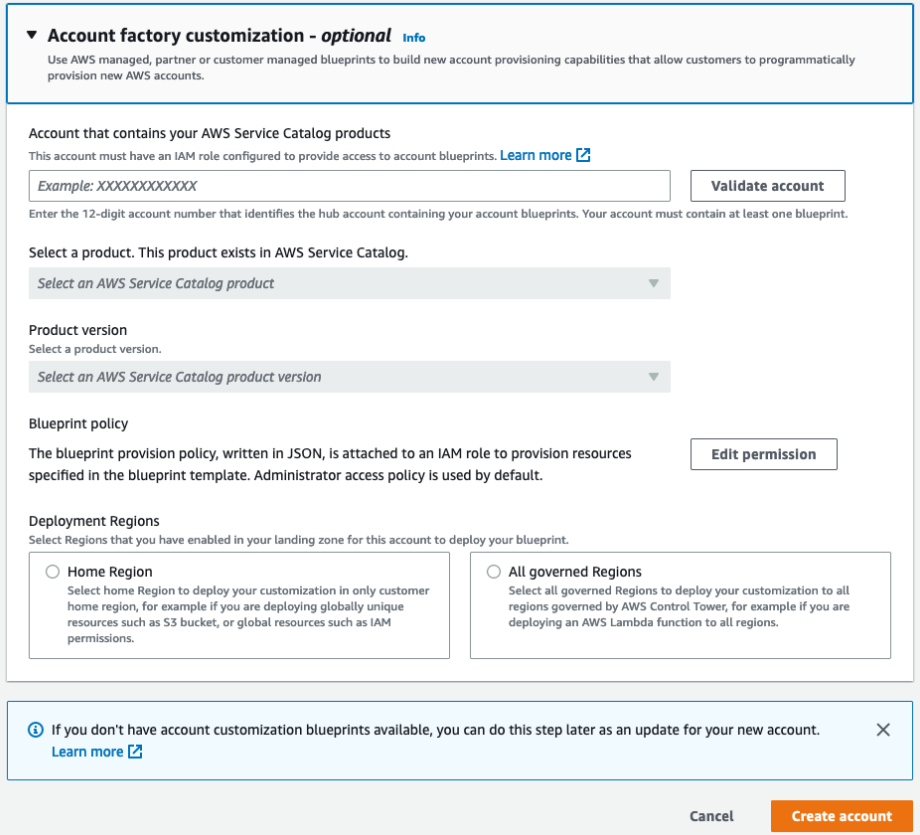
신규 **Account** 생성 - **Account Factory**

- Account Factory - Create account
- 기존에 등록된 적이 없는 Account email 입력
- SSO email, user name은 편의상 Management Account의 이메일을 입력(SSO가 AD 혹은 외부 IdP와 연계되어 있을 경우에는 어떤 값을 넣더라도 무시됨)
- 기존 Organizations에서 생성된 Account Eroll 시 (참고)
  - AWSControlTowerExecution Role을 해당 계정에 먼저 생성 후 Enroll
  - 혹은 OU Register 기능 사용 시, AWSControlTowerExecution Role 자동 생성되며 본 메뉴 사용할 필요 없음
  - email은 정확히 입력해야 하며, 다를 경우 신규 Account 생성됨
  - 기존 계정에서 Cloudtrail을 사용하고 있을 경우, Enroll 후에는 삭제 권고 (Control Tower의 Cloudtrail 추가로 인한 추가 요금 발생)

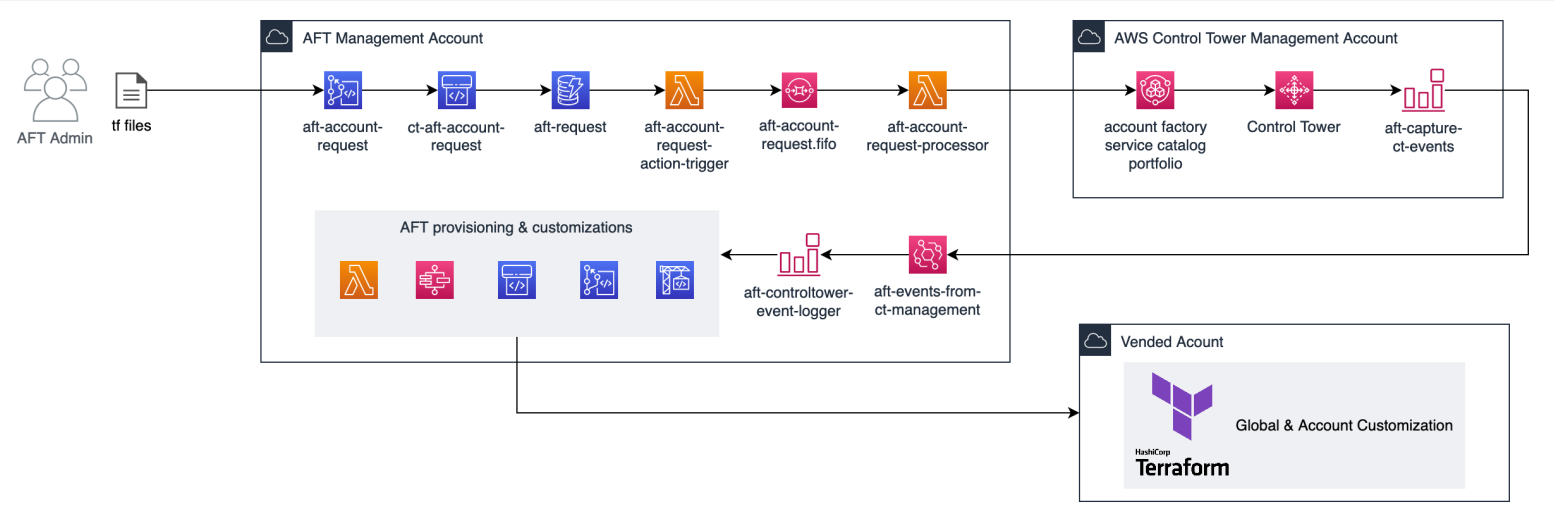


(Optional) Account Factory Customization(AFC)

- AWS Account에 공통 리소스를 배포할 수 있게 해 주는 기능
- 기존 Account에도 Account Factory의 Update 기능 활용하여 배포 가능
- CloudFormation 템플릿으로 정의하여, Service Catalog product 형태로 저장되는 Account Blueprint를 사용
- 사전 정의된 파트너사들의 Blueprint도 활용 가능(Splunk, Datalog 등)
- Management Account보다는 Hub Account 등의 Product를 관리할 수 있는 다른 공용 Account에 Service Catalog 관리권한을 위임하는 것을 권고
- Setup 절차
  - Organizations의 관리자 권한을 최소 권한으로 Hub Account에 위임
  - 관리권한 위임받은 Account(eg. Hub Account)에 Switch Role을 통해 접속 후, AWSControlTowerBlueprintAccess Role 생성 (Switch Role 하지 않으면, Control Tower 필수 예방 컨트롤로 인해 Role 생성이 안됨)
  - Hub Account로 접속하여 Service Catalog의 Product를 새로 생성
  - Account Factory에서 Account Factory customization 영역에 적절한 값(Hub Account, Product, Version 등)을 세팅하여 Account 생성 혹은 업데이트 수행



(Optional) Control Tower Account Factory for Terraform (AFT)



- 테라폼 파이프라인을 이용하여 Account를 생성하고 필요한 리소스를 생성할 수 있는 기능
- AFT Pipeline: (필수) – AFT 프레임워크와 모든 배포를 지원하는 데 필요한 구성 요소
- AFT Feature Options: (선택 사항) – 사전에 정의된 기능 플래그를 선택하고 배포할 수 있음
  - 데이터 이벤트 로깅을 CloudTrail 위한 조직 수준 만들기
  - 계정의 AWS 기본 VPC 삭제
  - 프로비저닝된 계정을 Enterprise AWS Support 플랜에 등록

https://docs.aws.amazon.com/ko_kr/controltower/latest/userguide/aft-overview.html

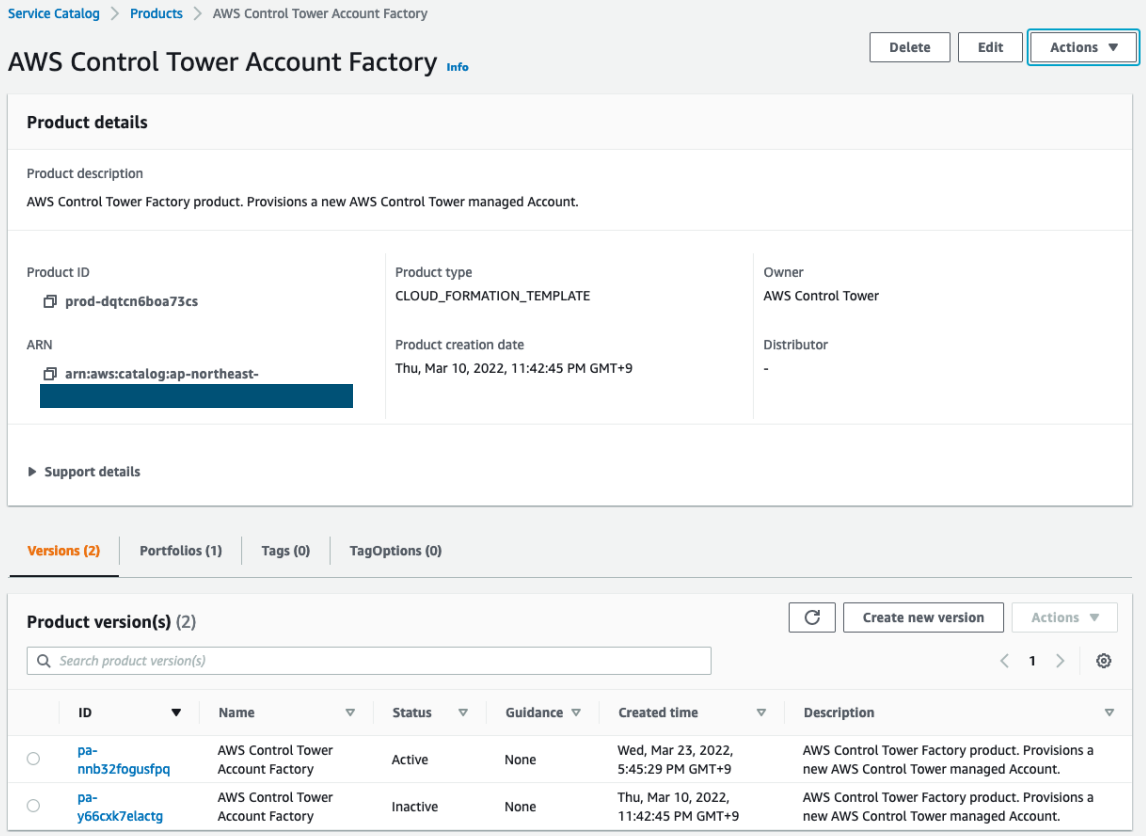
여기서 잠시...

Service Catalog와의 관계는?

Service Catalog Section

Administration - Product

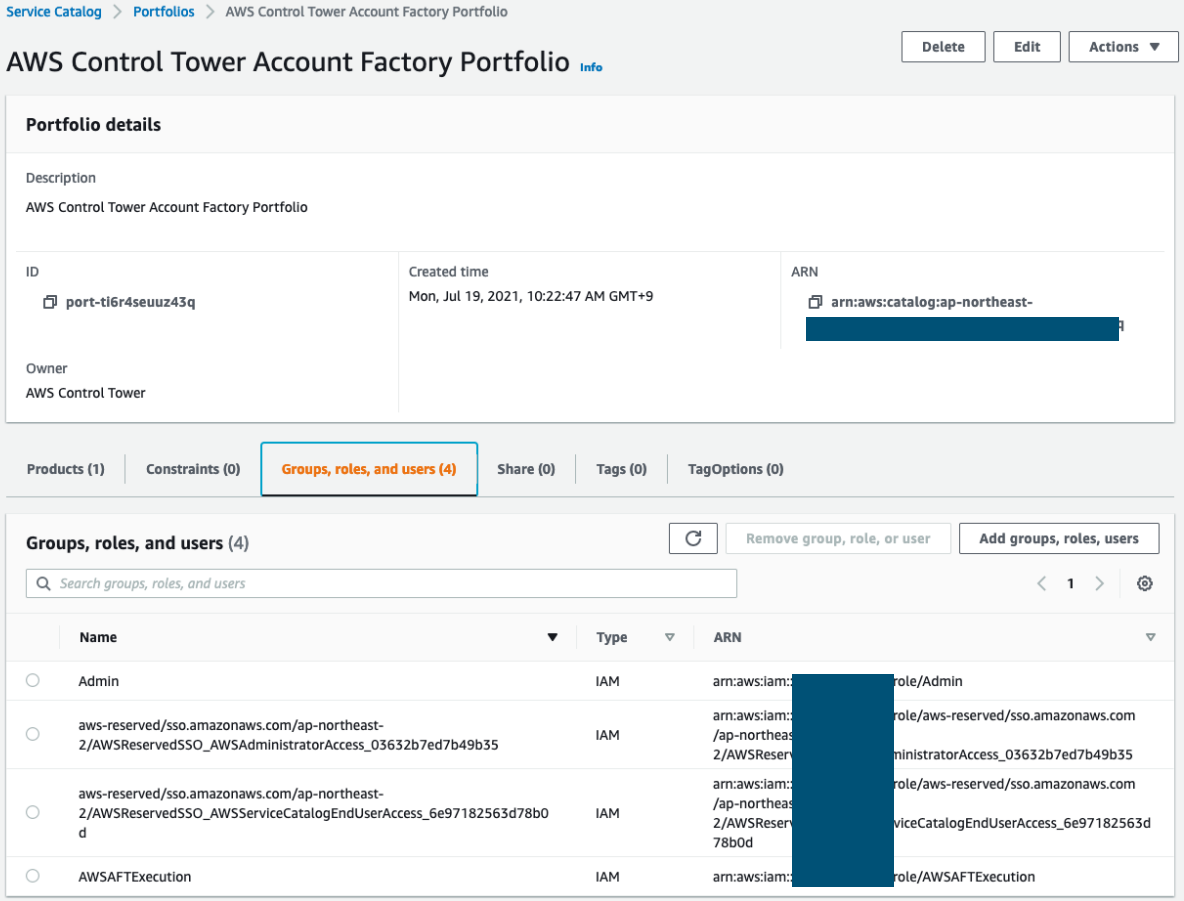
- Account Factory의 Product
- 관리자가 특별히 수정하거나 관리할 부분은 없음



Service Catalog Section

Administration - Portfolios

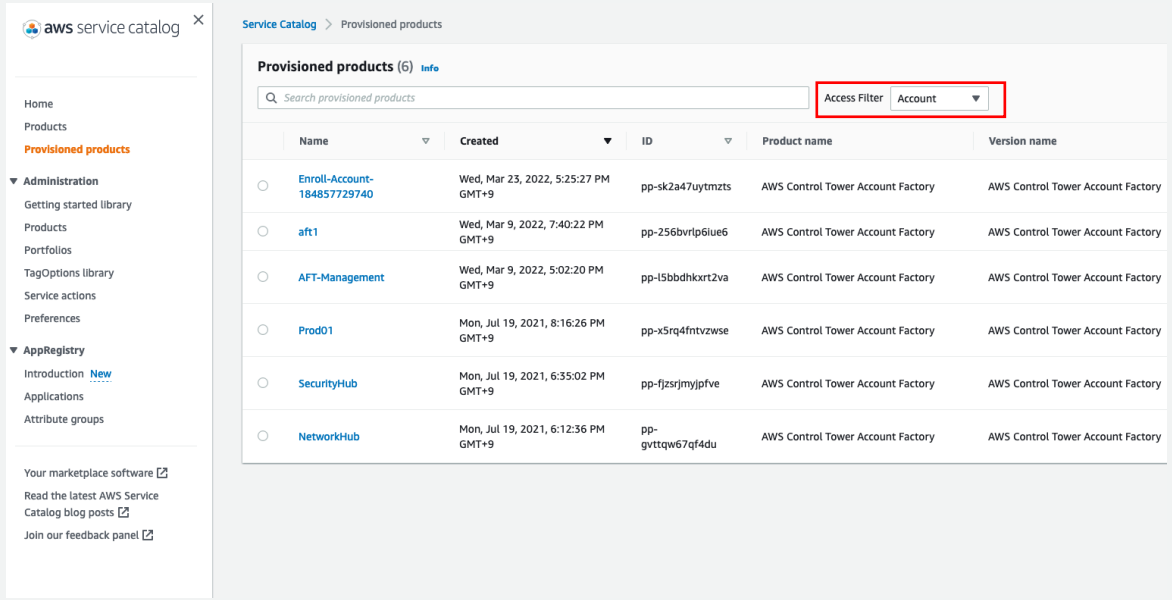
- Account Factory Product의 Portfolios
- Groups, roles and users 메뉴에서 부여된 범위의 사용자만 Account Factory Product를 사용할 수 있음
- Lamdba 함수 등을 통해 Service Catalog API를 사용하여 Account를 생성할 경우, 해당 Role을 여기서 추가함



Service Catalog Section

Account Factory Product and Provisioned Product

- Service Catalog의 Account Factory Product를 Launch 하는 것과 Account Factory를 통해 생성하는 것은 동일함.
- Access Filter를 Account로 변경해야, 다른 Admin 및 Role을 사용해 생성된 Control Tower 계정이 모두 조회됨
- Control Tower 거버넌스에서 제외하거나 계정을 Suspension 할 경우, Provisioned Service Catalog에서 먼저 Terminate 한 후 진행함.
- Terminate 진행 시에는 해당 계정에서 모든 Control Tower 리소스가 삭제되며, Root 하위로 이동하게 됨.



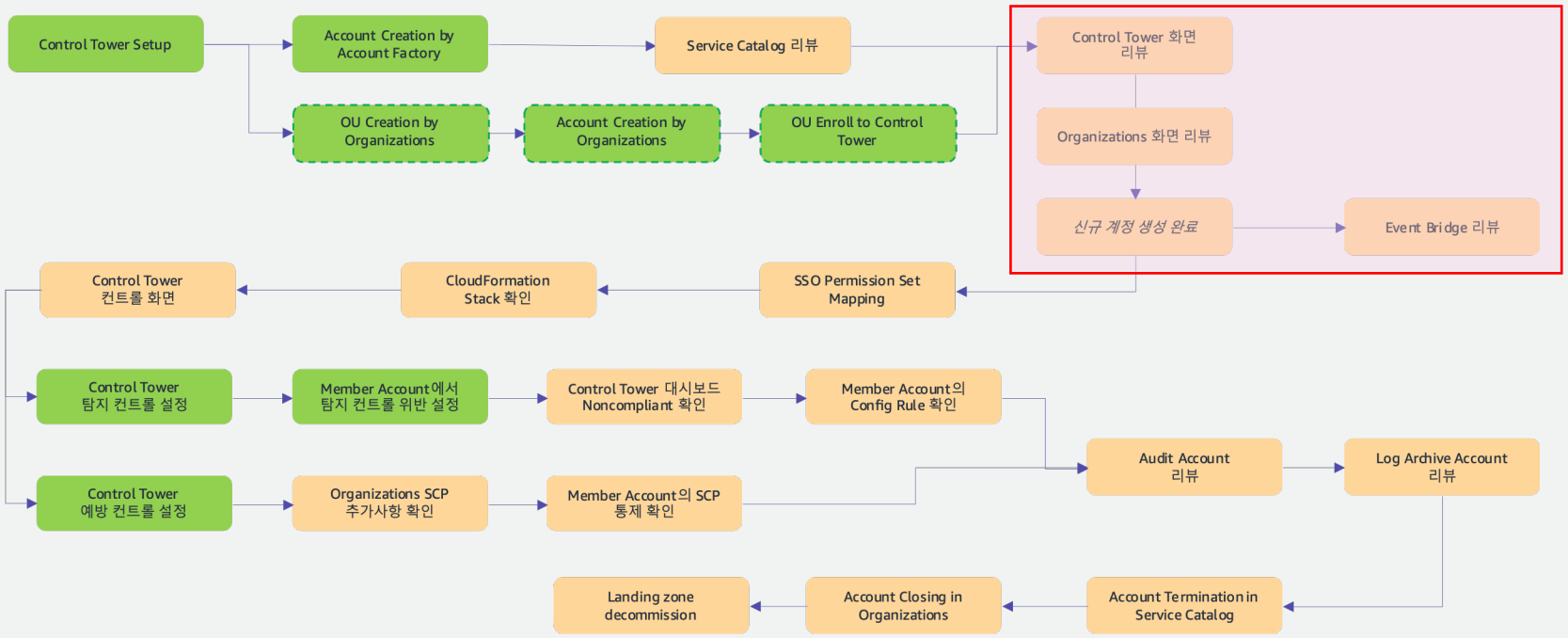
Service Catalog Section

Service Catalog API를 사용한 Account Factory 계정 생성

- Service Catalog API를 통해 계정생성을 자동화 할 수 있음(ProvisionProduct)
- 참조영상 : Programmatically Create an AWS Account with AWS Control Tower
- Using lifecycle events to track AWS Control Tower actions and trigger automated workflows
- Control Tower API를 제공하나 Control enable/disable, list 등 단순한 기능만 지원

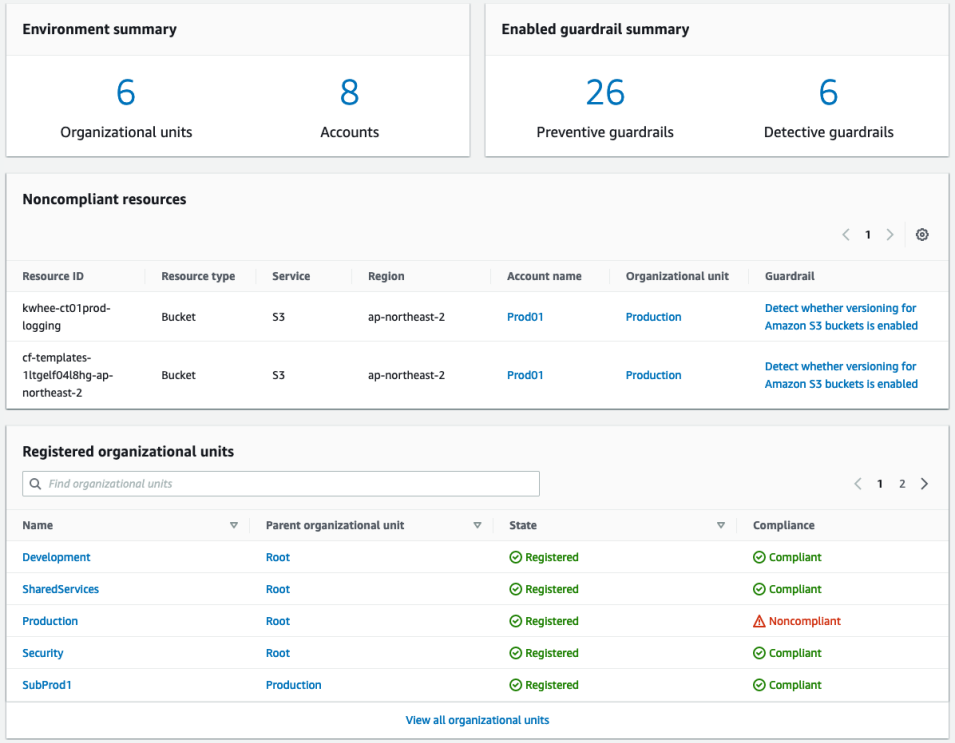
Return to Control Tower

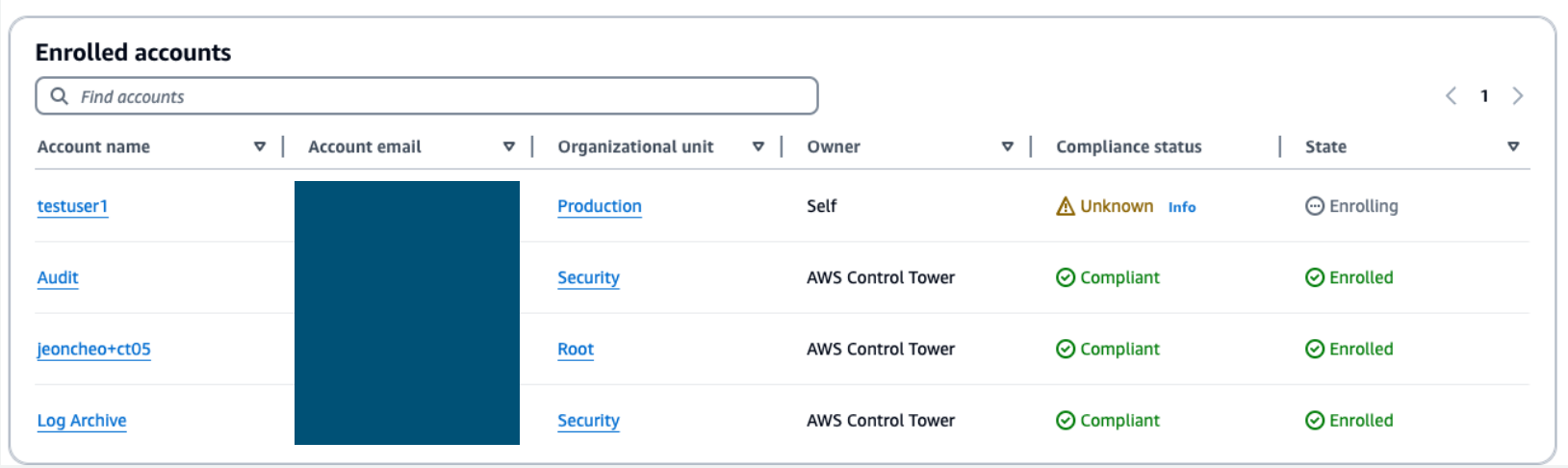
Hands-on Scenario



Dashboard

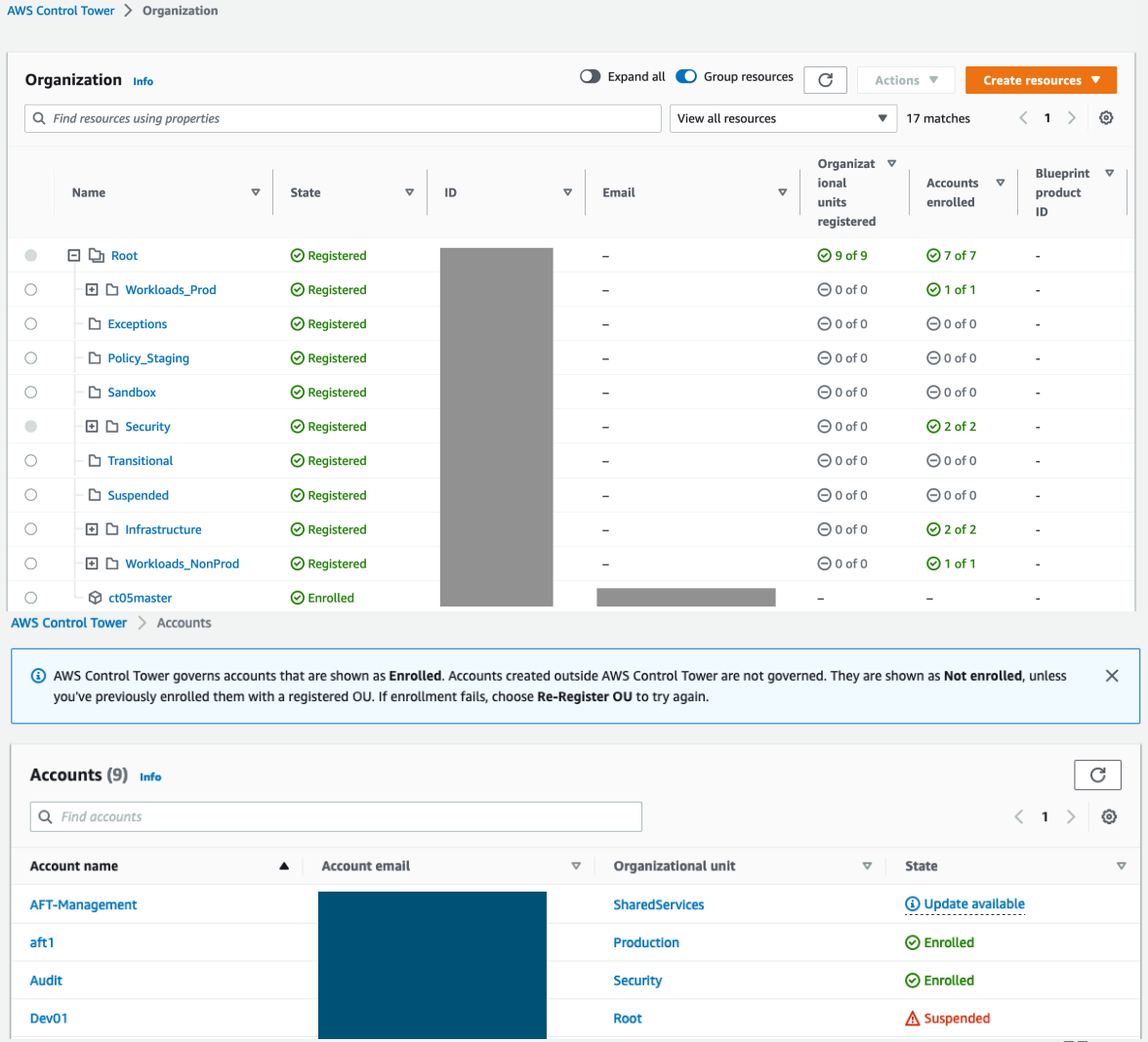
- Noncompliant resources
- Registered organizations units
- Enrolled accounts





Control Tower Organizations

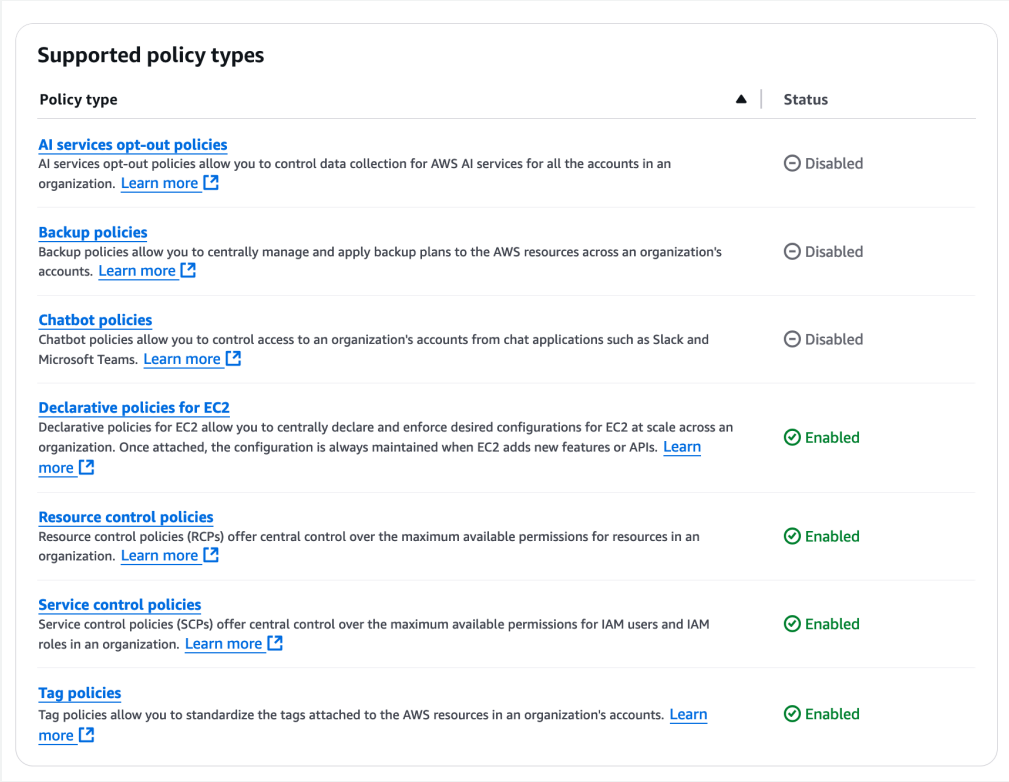
- Preventive Guardrail은 Register 여부와 상관없이 Nested OU로 상속
- Detective Guardrail은 적용 당시의 Register 여부에 따름
- OU Register 시 OU 내에 Enroll 되지 않은 모든 Account는 병렬로 Enroll이 수행됨
- OU Re-Register 시 OU 내의 모든 Account의 Enroll이 다시 병렬로 수행되며, Drift 상태의 Account들이 Fix 됨



Organizations Section

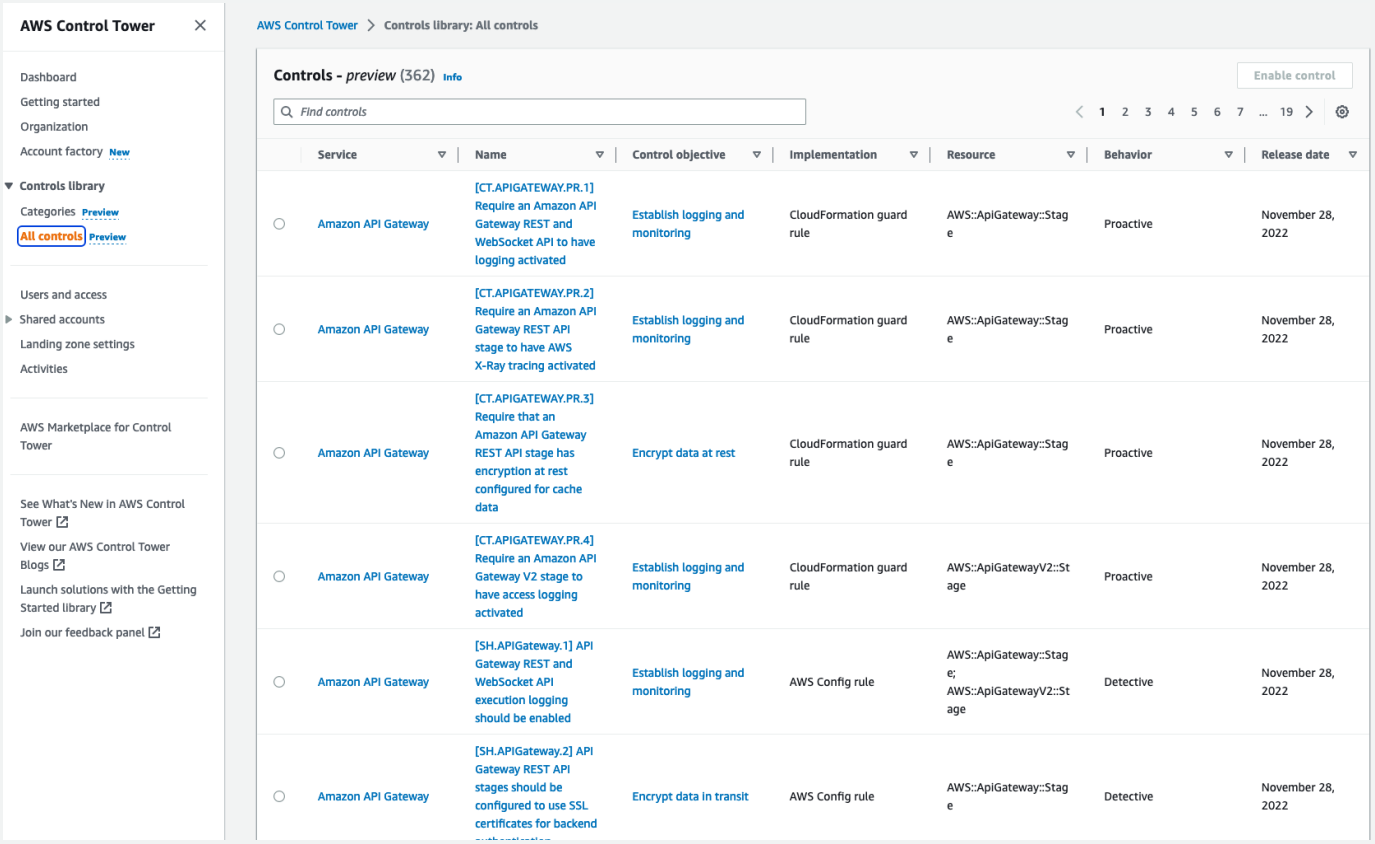
Organizations with Control Tower

- Control Tower에 Enroll된 OU와 Account는 Organizations에서 조작(Move, Rename 등)을 자제
- Policies
  - SCP는 Control Tower의 컨트롤과 연결되어 있으며, Backup 및 Tag 정책은 Control Tower와 직접적인 연관은 없으나 거버넌스 측면의 정책을 수립하여 적용
  - Declarative policy
    - SCP (Service Control Policies)
    - RCP (Resource Control Policies)
    - Declarative policies for EC2
  - Backup policies : OU/Account 별 Backup 정책 적용
  - Tag policies : OU/Account 별 Tag 정책 적용
- 필독문서
  - Best Practices for Organizational Units with AWS Organizations
  - Whitepaper : Organizing Your AWS Environment Using Multiple Accounts



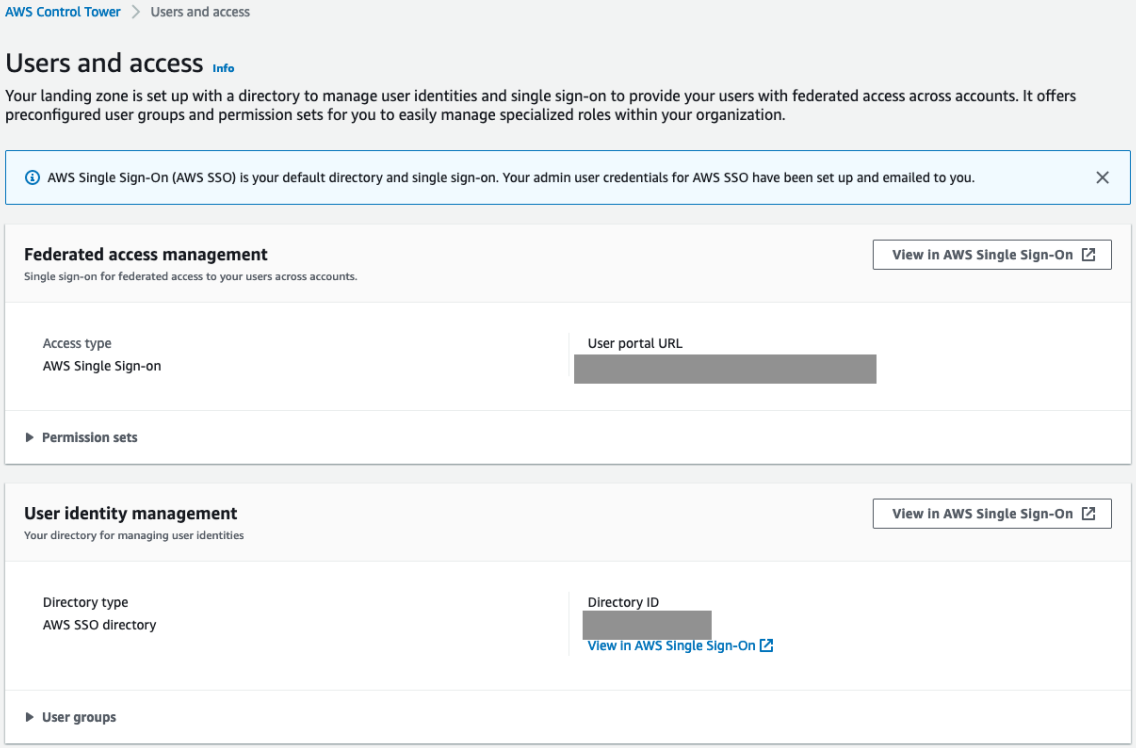
Controls Library

- 컨트롤 적용 시에 설명 예정



Users and access

- ControlTower는 AWS SSO를 기본적으로 활성화 시킴
- 기존에 SSO가 이미 활성화되어 On-prem AD 혹은 3rd-party Identity Provider와 Integration 되어 있을 경우에는 SSO 설정을 전혀 변경하지 않음



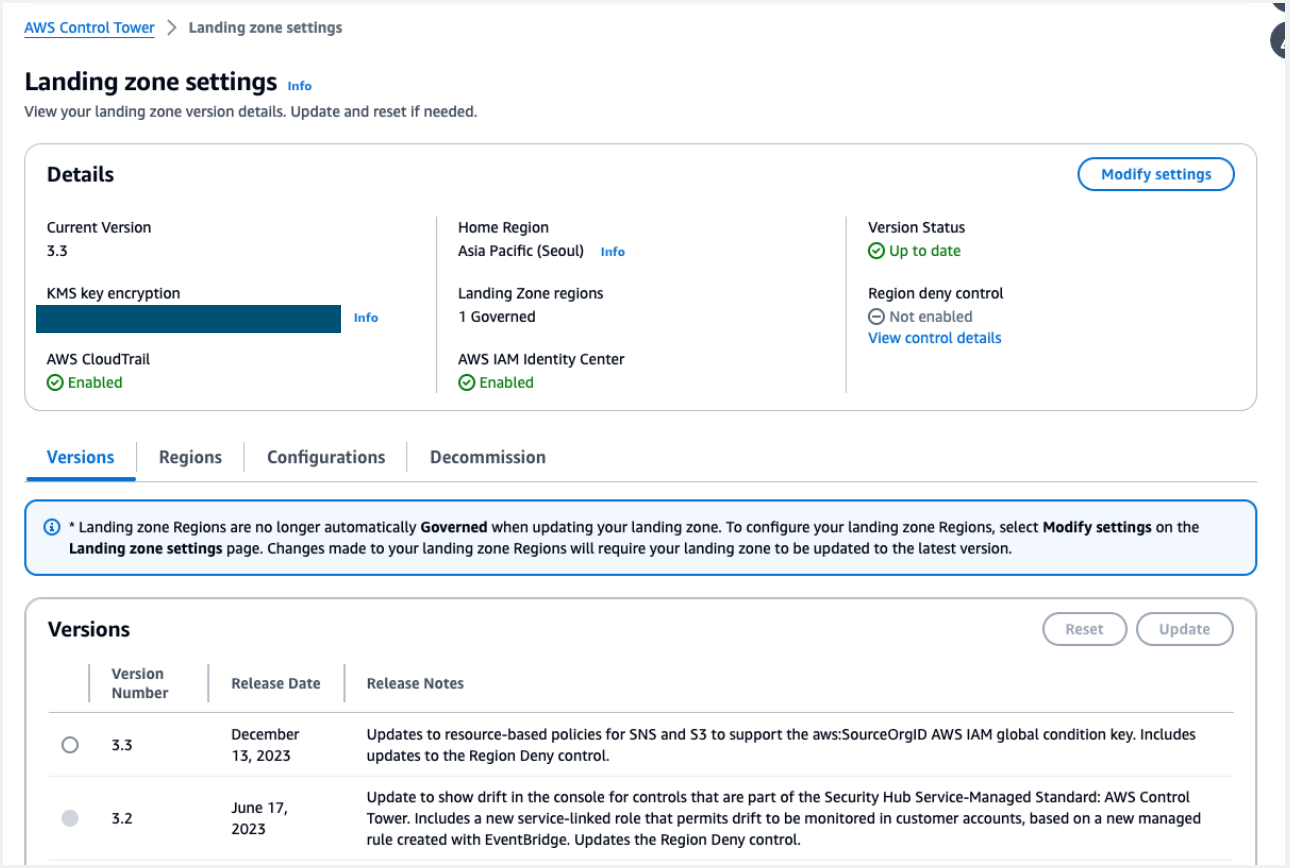
Control w/ Accounts

- Management 계정은 Control Tower의 거버넌스 및 컨트롤이 적용되지 않음 (CloudTrail만 적용됨)
- Security OU는 Control Tower에서 관리하므로, CfCT의 SCP는 반드시 필요한 것만 주의하여 적용

OU	Account List	Control Tower 제공 컨트롤			Customized 컨트롤(CfCT)		
		CloudTrail	Config Rule	SCP	Config Rule	SCP	기타 리소스 (Role/Policy/ lambda/VPC/...)
Root	**Management Account**	적용	**적용 X**	**적용 X**	**적용 X**	**적용 X**	**적용 X**
Security	**Audit Log Archive**	적용	적용	적용	적용	**주의하여 적용**	선택적 적용
Infrastructure	Network Shared services	적용	적용	적용	적용	적용	선택적 적용
Sandbox	AWS Sandbox 계정	적용	적용	적용	적용	적용	선택적 적용
Workloads OUs	AWS 업무 계정	적용	적용	적용	적용	적용	선택적 적용

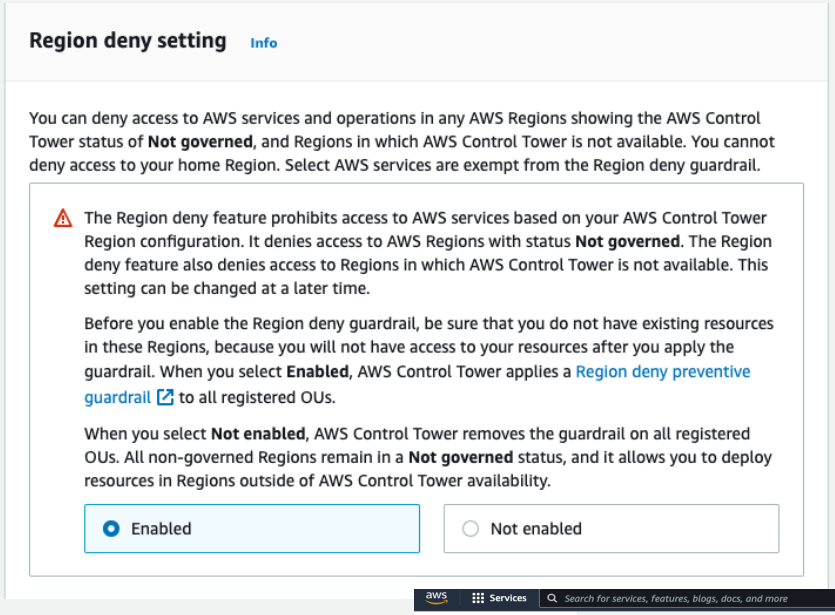
Landing zone settings

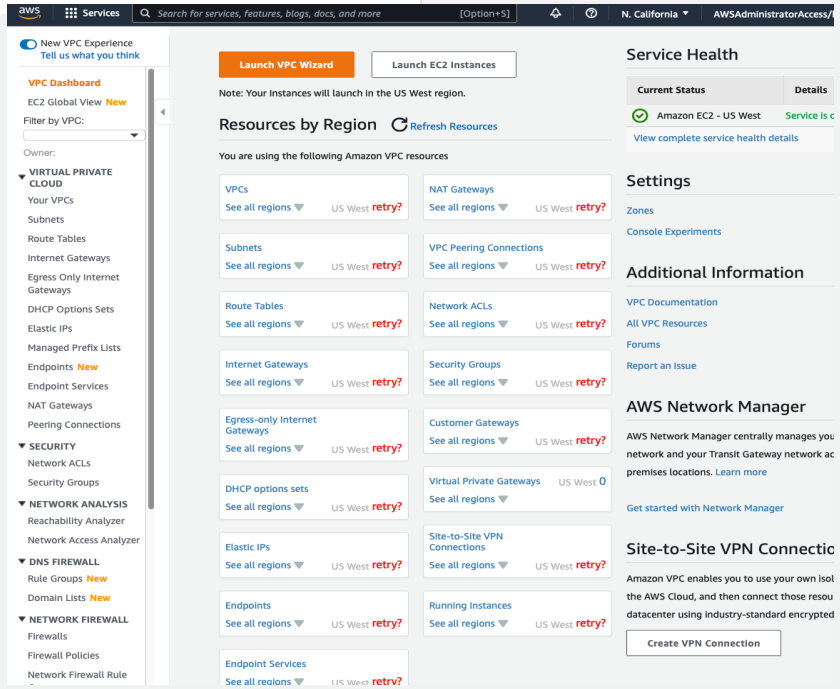
- Versions
  - 새로운 버전이 Release 되면, Update를 통해 Landing zone 업그레이드를 수행하며, 이후 모든 OU에 대해서 개별적으로 Update를 수행
  - Landing zone에 Drift가 발생했을 경우 Repair를 통해 해결 가능
- Regions
  - 관리되는 Region 현황
- Configurations
  - KMS Encryption 현황
- Decommision
  - 랜딩존 삭제 시



Region Deny setting

- Control Tower에서 관리하는 Region 외의 다른 모든 Region에 대한 사용 금지 정책
- Control Tower Setup 시 설정하며, 이후에도 변경 가능
- 강력한 Enterprise Region 거버넌스 적용 시에 사용
- 모든 OU에 공통으로 적용됨
- Global 서비스들에 대해서는 예외처리가 되어 있어, us-east-1이 Deny Region으로 되어 있을 경우에도 대부분은 정상적이나, 일부 경우에 오류가 발생할 수 있음. (Route53 Health Check, SSO Admin delegation 등)





Drift 발생 유형 및 조치 사항

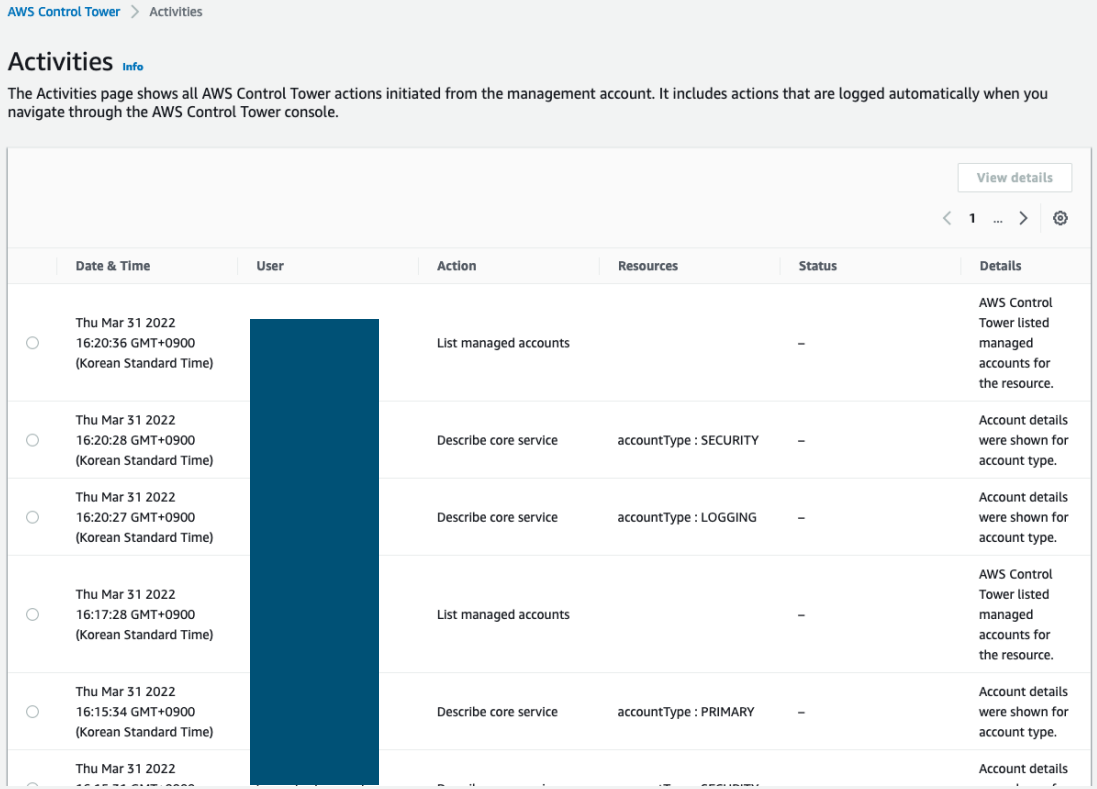
- Account Drift
  - Moved Member Account, Added Member Account, Removed Member Account
- Policy Drift
  - Unplanned Update to Managed SCP, SCP Attached to Managed OU, SCP Detached from Managed OU, SCP Attached to Member Account, Deleted Foundational OU

- 대부분의 Drift는 SCP를 원복, Re-register OU 및 landing zone Repair(Landing zone setting)를 통해 해결
- Control Tower에 Enroll된 OU 및 Account는 Organizations에서 조작하는 것을 피해야 Drift를 방지할 수 있음

https://docs.aws.amazon.com/controltower/latest/userguide/governance-drift.html

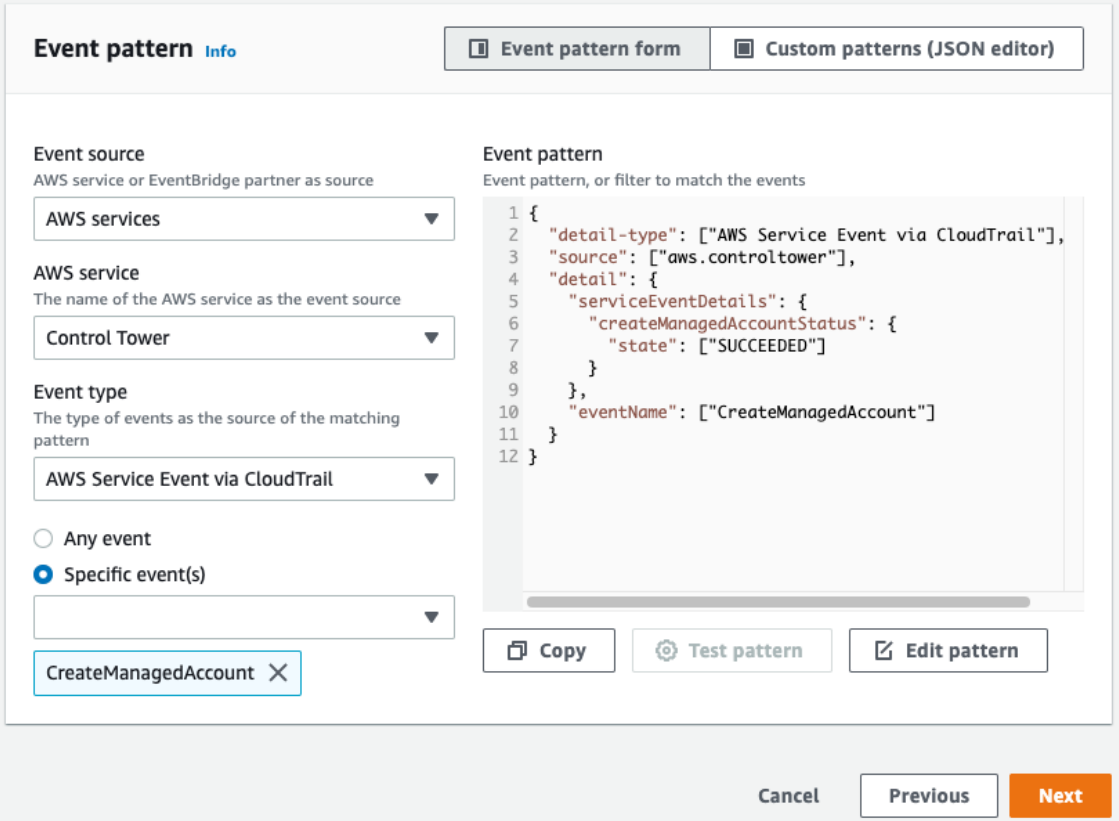
Activities

- Control Tower의 모든 이벤트 조회가 가능하며, CloudTrail로 전송됨
- Cloudtrail Event Console에서도 조회 가능
- Lifecycle 이벤트에 대한 조회 가능
  - https://docs.aws.amazon.com/controltower/latest/userguide/lifecycle-events.html



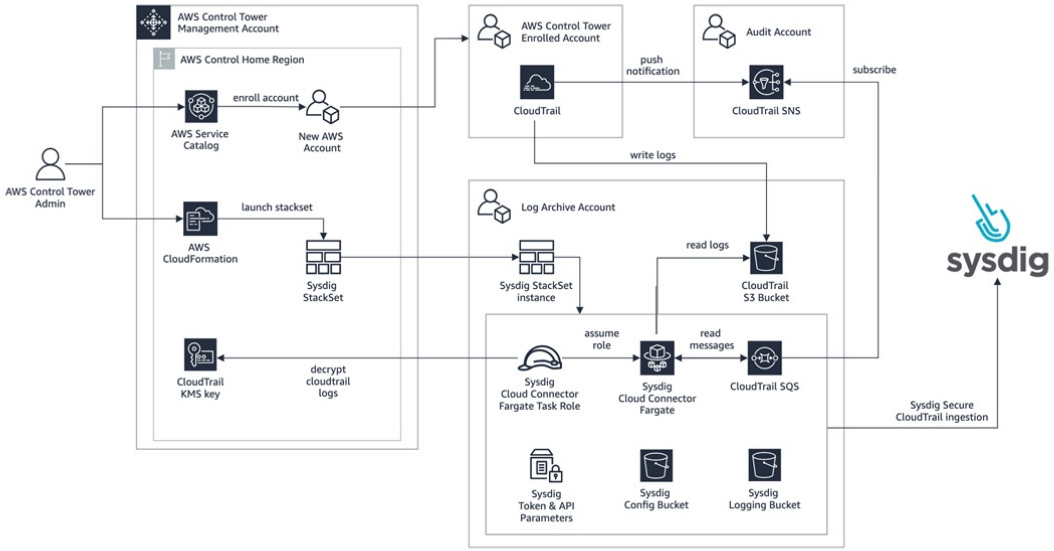
Option) Control Tower Lifecycle 연계 - Event Bridge

- Control Tower의 Lifecycle Event를 연계하기 위해서는 Amazon Event Bridge를 사용함
- Events > Rules > Create rule 선택하여 Control Tower의 Lifecycle에 해당하는 이벤트를 연계하여 다양한 Automation을 구현할 수 있음



AWS Marketplace for Control Tower

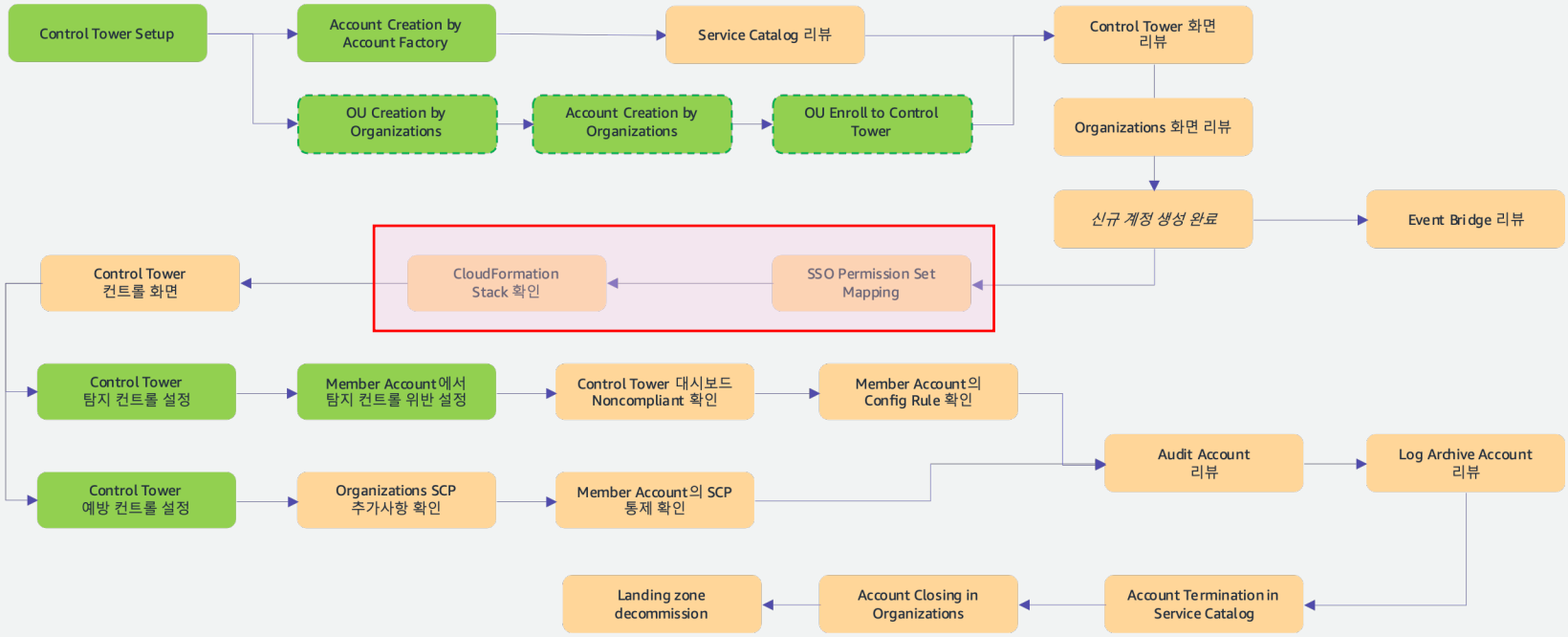
- Control Tower의 Lifecycle 이벤트 혹은 Organizations OU 등과 연계하여, 다양한 Third-party 소프트웨어와 연계가 가능함
- Solutions for AWS Control Tower in AWS Marketplace
- Sysdig의 연계 사례



계정생성이 완료되었나요?

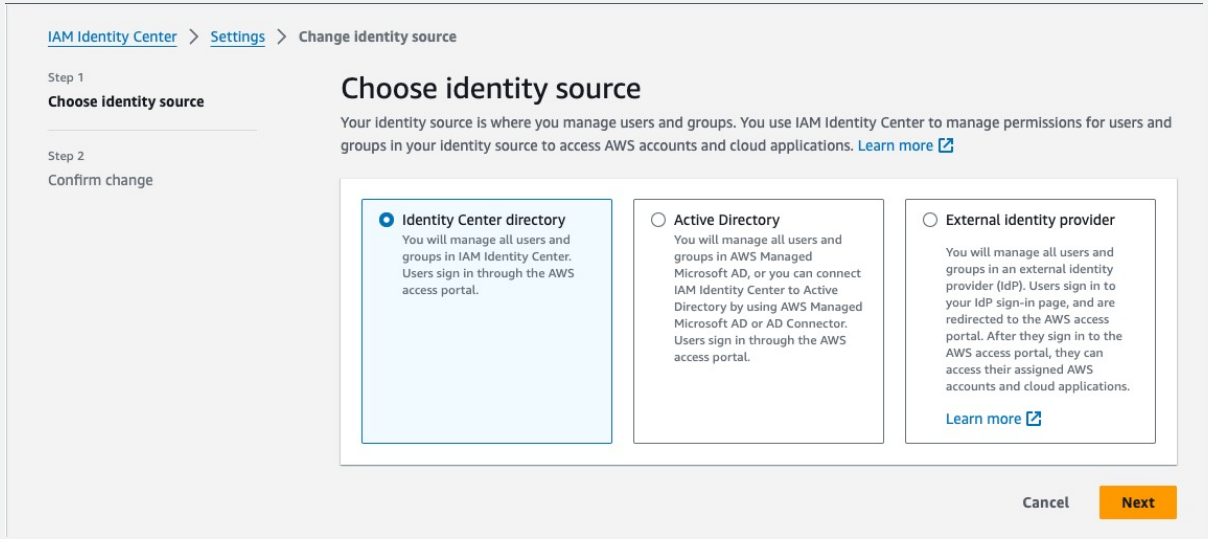
신규계정에 접속하기 위한 **IAM Identity Center(구 SSO)**에 대해 알아봅니다.

Hands-on Scenario



SSO Identity Source

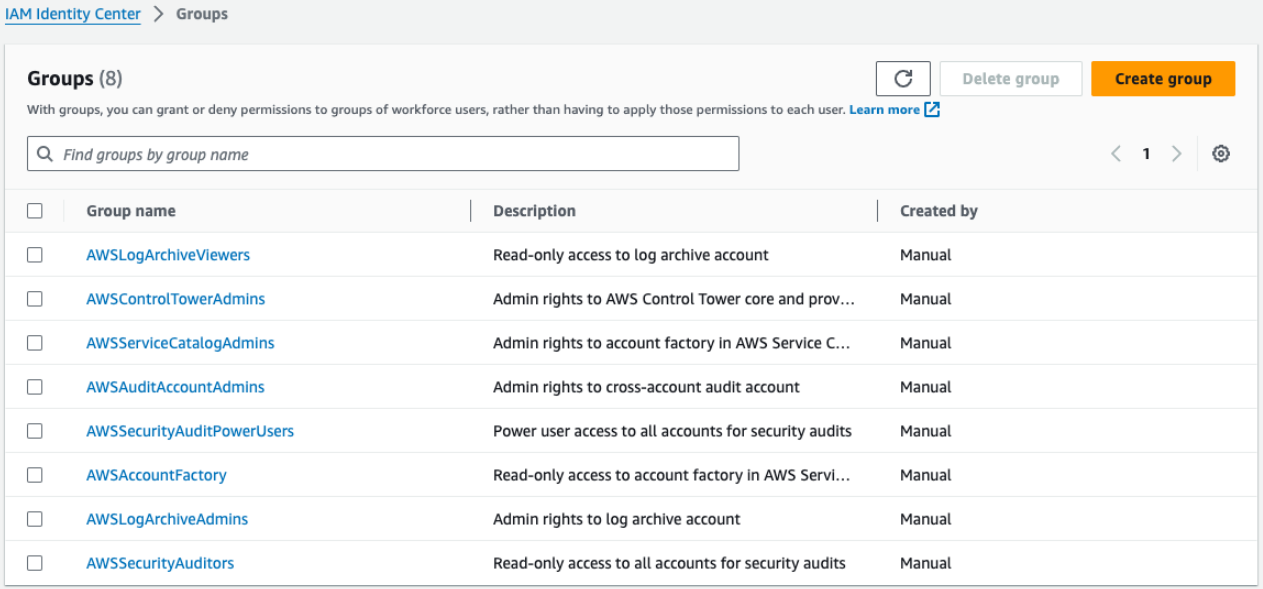
- 일반적인 Enterprise 고객사는 On-premise의 Active Directory와 연동하는 경우가 많음
- Control Tower Setup 시
  - SSO를 사용하고 있지 않다면, AWS SSO 자체 identity source로 설정되고 Default SSO user 및 group이 생성됨
  - SSO가 AD 혹은 외부 IdP와 연동되어 있다면, 그 설정은 그대로 유지되며 변경사항 없음



IAM Identity Center (SSO) Section

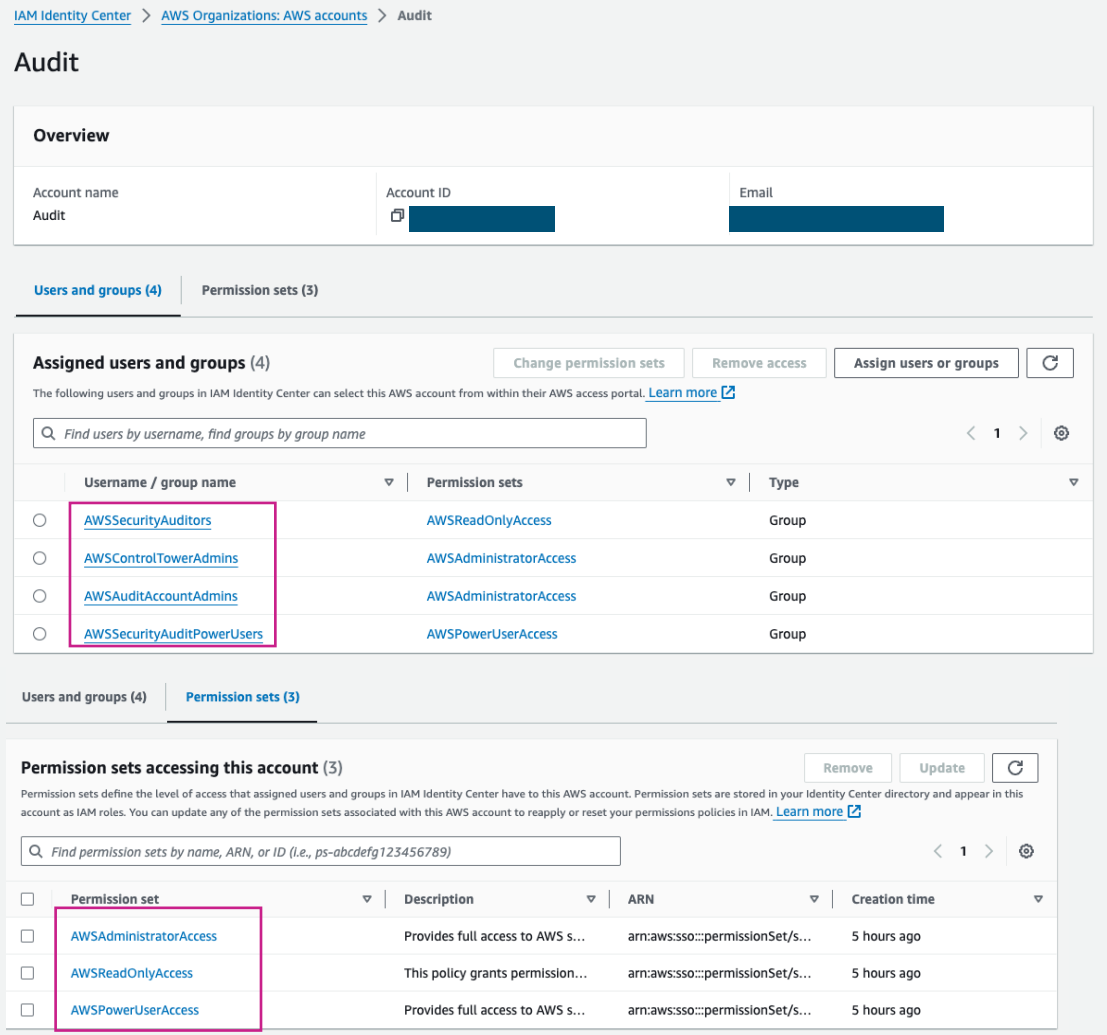
SSO Users / Groups

- 여러 AWS Account에 동일한 ID와 비밀번호로 접속하기 위한 별도의 AWS SSO User
- On-premise의 Active Directory와 연계되어 있는 경우 AD의 User와 Group이 조회됨.
- 여러 시스템에 접속할 수 있는 사번의 개념으로 이해하면 됨.
- 보통 Group에 접속할 수 있는 AWS Account와 적절한 권한의 Permission Set을 매핑하기를 권고
- AWS SSO 자체 identity resource를 사용하고 있을 경우, 생성되는 Default Control Tower 관련 그룹
  - https://docs.aws.amazon.com/controltower/latest/userguide/sso.html



Permission Set

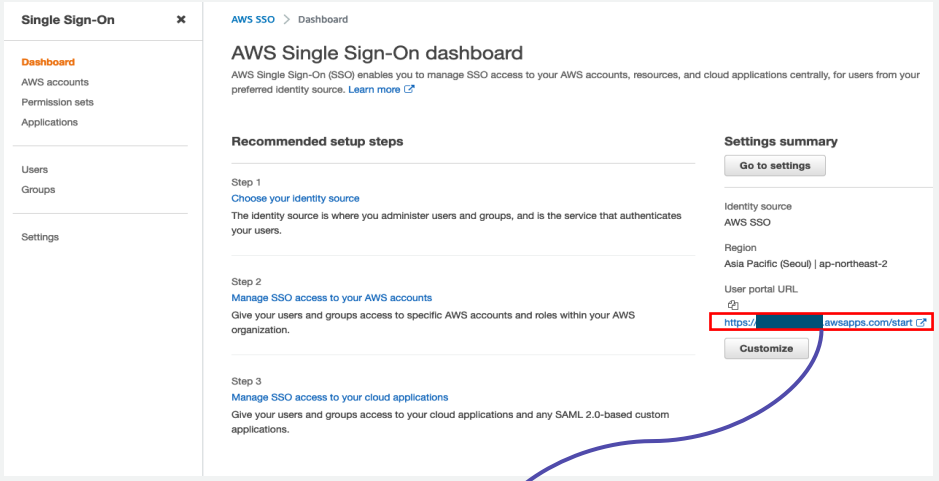
- Control Tower의 Account Factory를 통해 Member Account가 생성이 되면, 이 Account에 접속할 수 있는 SSO User/Group을 필요한 Permission Set으로 매핑해 줘야 함
- 일반적으로 Group과 Permission Set을 매핑하기를 권고
- 본 실습 시에는 기존에 생성된 SSO User를 모두 삭제하고, 새롭게 생성하도록 함
  - User : ctadmin
  - email : 수강생 개인 이메일
  - 생성 시 Group은 AWSControlTowerAdmins로 지정
- AWSControlTowerAdmins 그룹이 모든 AWS Account에서 AWSAdministratorAccess 퍼미션셋을 가지도록 설정함

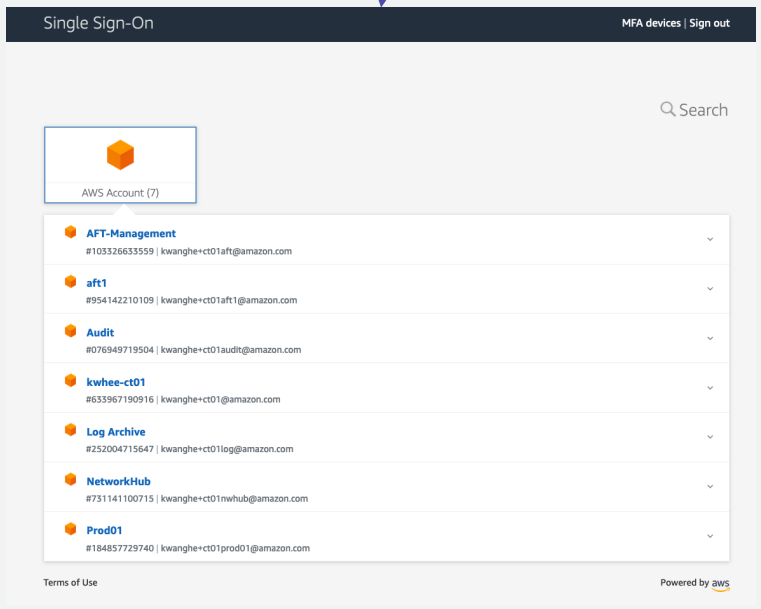


IAM Identity Center (SSO) Section

SSO Portal

- SSO Dashboard에 있는 Portal URL로 접속
- 로그인 시 MFA를 사용하도록 강제됨





IAM Identity Center (SSO) Section

신규로 생성된 **Member Account**의 리소스 리뷰

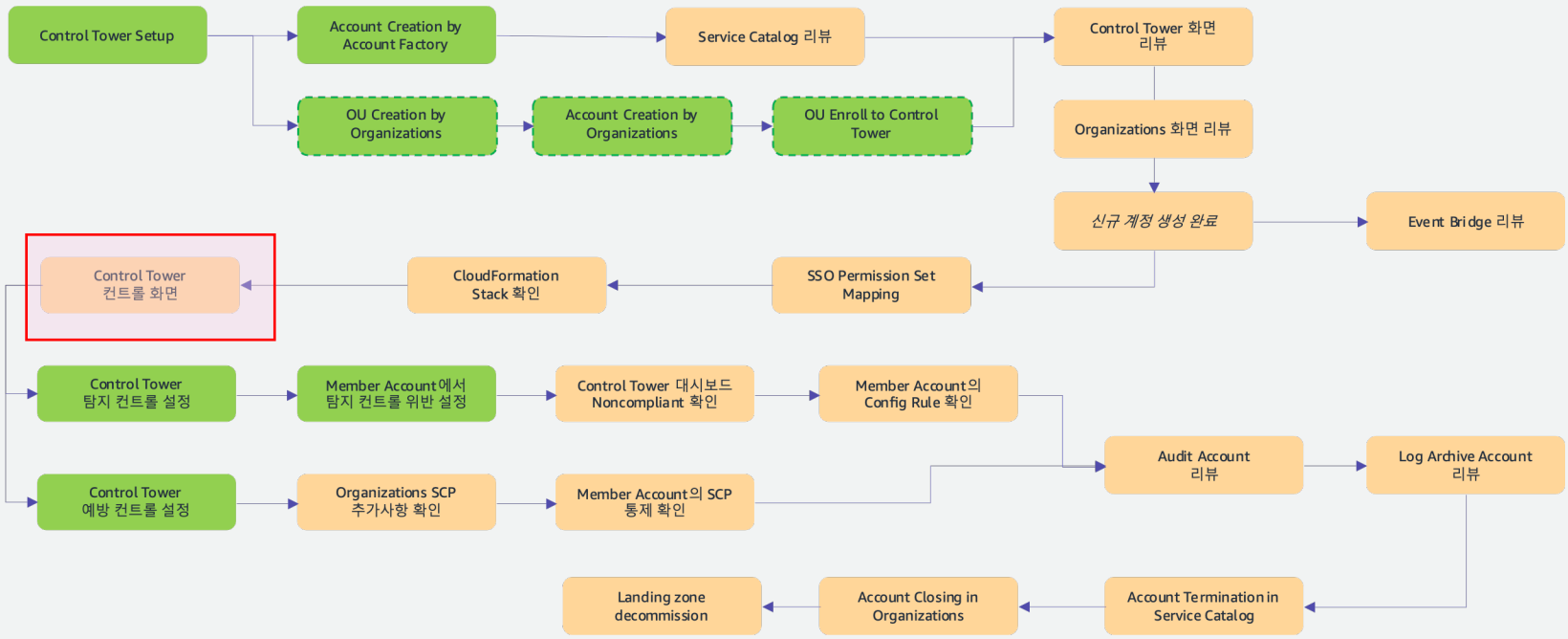
- SSO Portal을 통해 신규로 생성된 Account에 접속
- CloudFormation Stack 조회
- Control Tower 보호정책(SCP)에 의해 본 리소스는 Member Account의 Admin 혹은 root 권한으로도 삭제할 수 없음

AWS service	Resource type	Resource name
AWS CloudFormation	Stacks	StackSet-AWSControlTowerBP-BASELINE-CLOUDTRAIL-* StackSet-AWSControlTowerBP-BASELINE-CLOUDWATCH-* StackSet-AWSControlTowerBP-BASELINE-CONFIG-* StackSet-AWSControlTowerBP-BASELINE-ROLES-* StackSet-AWSControlTowerBP-BASELINE-SERVICE-ROLES-*
AWS CloudTrail	Trail	aws-controltower-BaselineCloudTrail
Amazon CloudWatch	CloudWatch Event Rules	aws-controltower-ConfigComplianceChangeEventRule
Amazon CloudWatch	CloudWatch Logs	aws-controltower/CloudTrailLogs /aws/lambda/aws-controltower-NotificationForwarder
AWS Identity and Access Management	Roles	aws-controltower-AdministratorExecutionRole aws-controltower-CloudWatchLogsRole aws-controltower-ConfigRecorderRole aws-controltower-ForwardSnsNotificationRole aws-controltower-ReadOnlyExecutionRole AWSControlTowerExecution
AWS Identity and Access Management	Policies	AWSControlTowerServiceRolePolicy
Amazon Simple Notification Service	Topics	aws-controltower-SecurityNotifications
AWS Lambda	Applications	StackSet-AWSControlTowerBP-BASELINE-CLOUDWATCH-*
AWS Lambda	Functions	aws-controltower-NotificationForwarder

https://docs.aws.amazon.com/controltower/latest/userguide/account-factory-considerations.html

신규 계정에 적용되는 컨트롤을 확인합니다.

Hands-on Scenario



Controls(구 Guardrails)

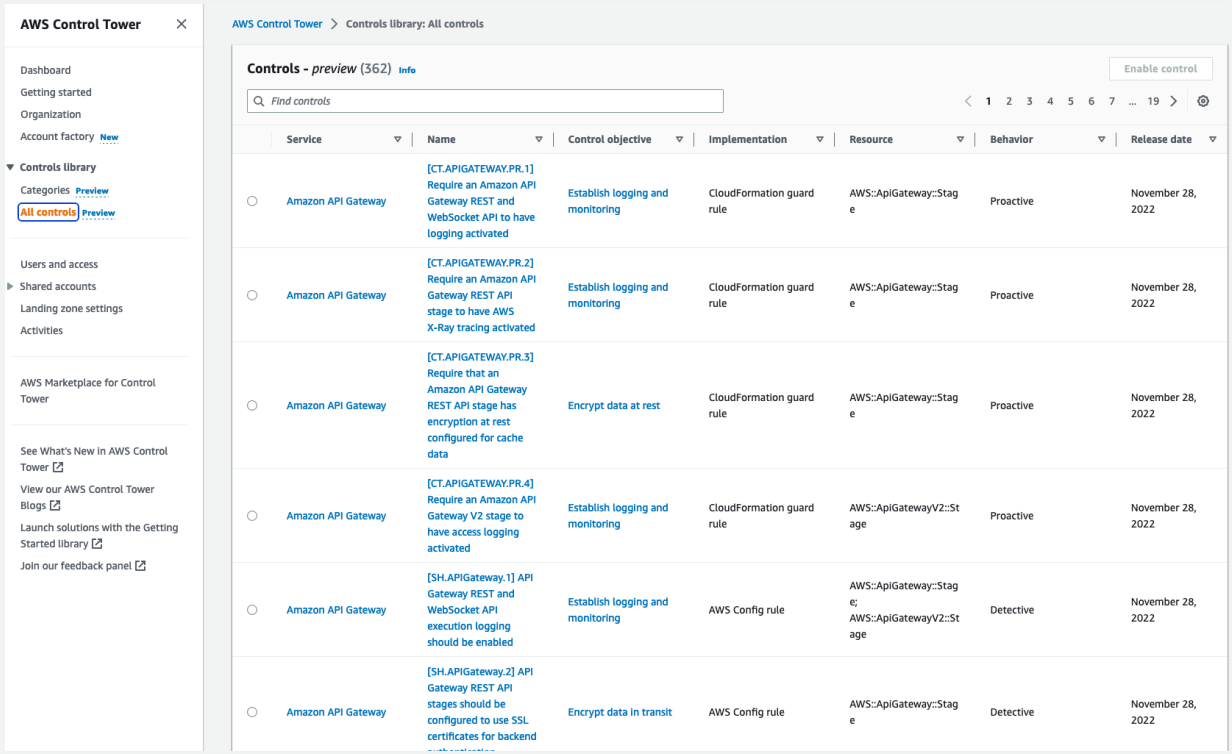
- Control Behavior (동작)
  - Detective : 탐지 컨트롤(Config rules)
  - Preventive : 예방 컨트롤(SCP)
  - Proactive : 사전(선제적) 컨트롤(CloudFormation hooks)

- Guidance(지침)
  - Control Tower에서 제공하는 컨트롤에 주로 해당됨
  - Mandatory : Control Tower 자체 리소스 보호 정책
  - Strongly Recommended : 고객에게 강력히 권고
  - Elective : 고객의 상황에 따른 선택적 적용

- Control Categories는 Control Objectives, Services, Frameworks 등으로 분류됨

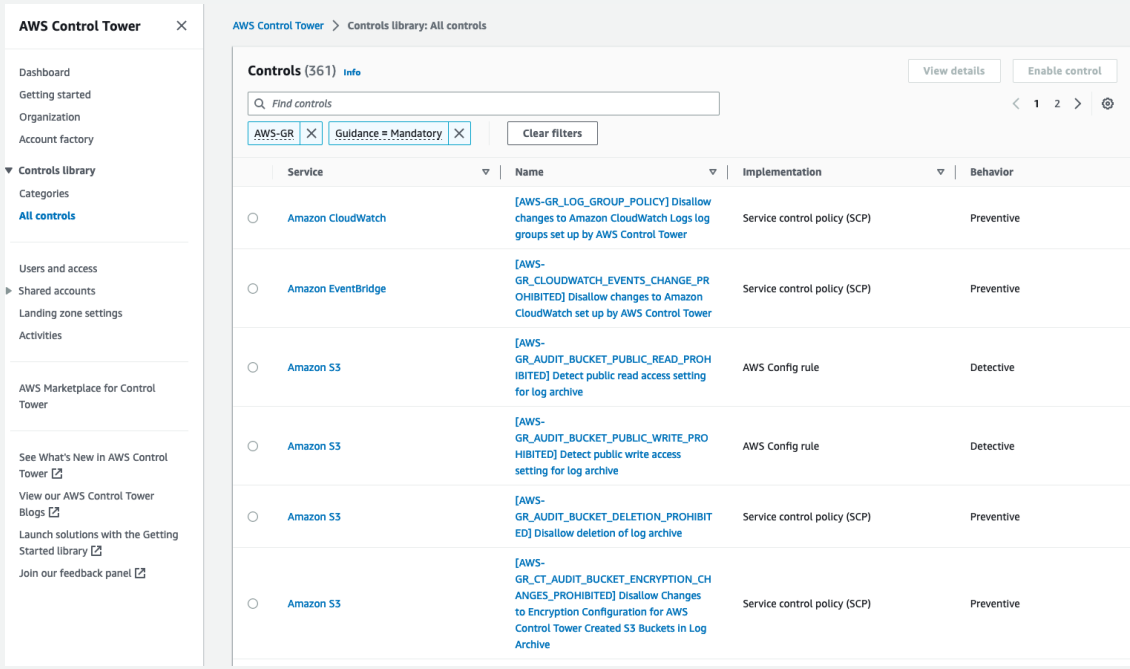
- Preventive Control는 Enroll/Unenroll OU 모두 적용되고, Detective Control는 Enroll OU만 적용됨

- 개별 컨트롤은 OU 단위로 Enable/Disable을 병렬로 수행 가능



Controls Owned by Control Tower

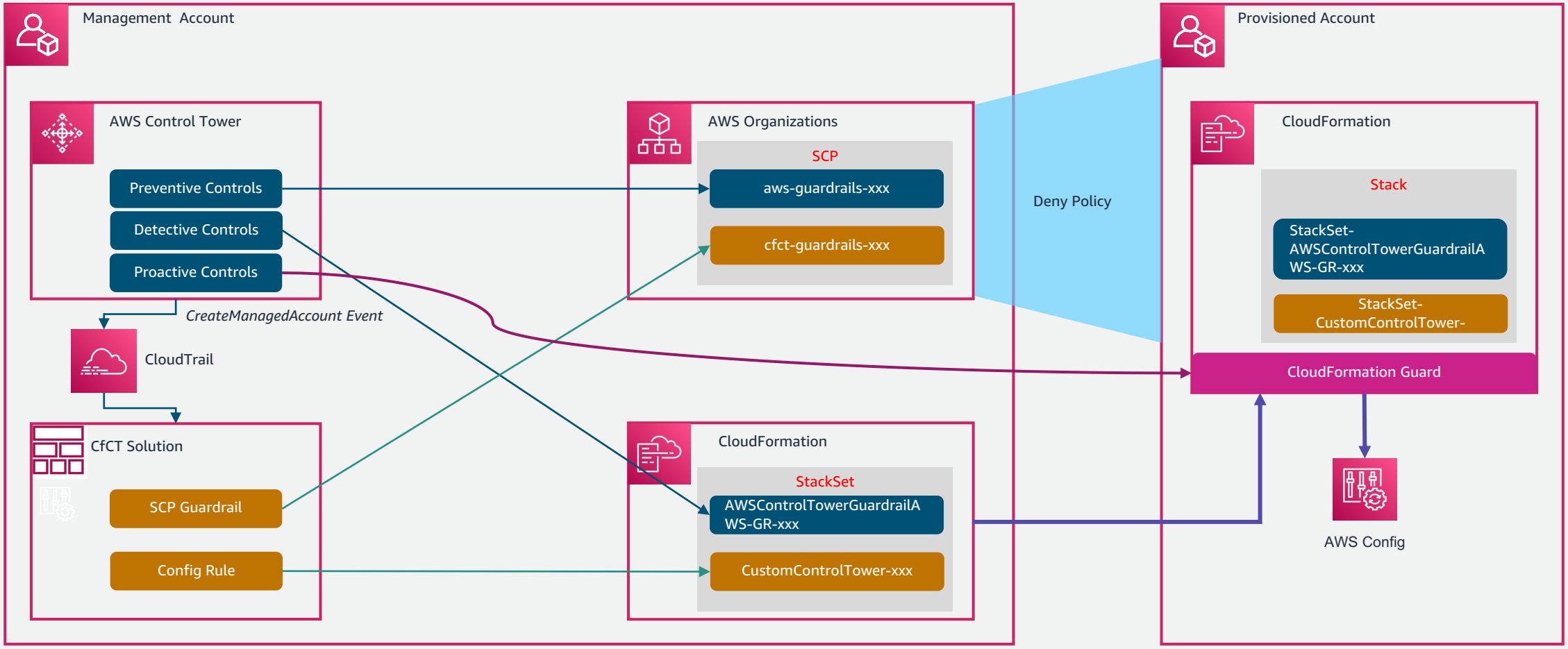
- Control Tower 서비스 초기부터 제공되고 있는 탐지 및 예방 가드레일
- "[AWS-GR"의 접두어로 구분됨
- Mandatory Controls (필수 컨트롤)
  - 필터조건 : 'AWS-GR' and 'Guidance = Mandatory'
- Data Residency Controls (데이터 저장 컨트롤)
  - 필터조건 : 'AWS-GR' and 'Guidance = Elective' 중에 포함
- Optional Controls - Strongly Recommended Controls (권고 컨트롤)
  - 필터조건 : 'AWS-GR' and 'Guidance = Strongly Recommended'
- Optional Controls - Elective Controls (선택적 컨트롤)
  - 필터조건 : 'AWS-GR' and 'Guidance = Elective' 중 Data Residency Control을 제외한 나머지
- Guradrail check list로 전체 유형 및 종류를 전반적으로 파악 필요



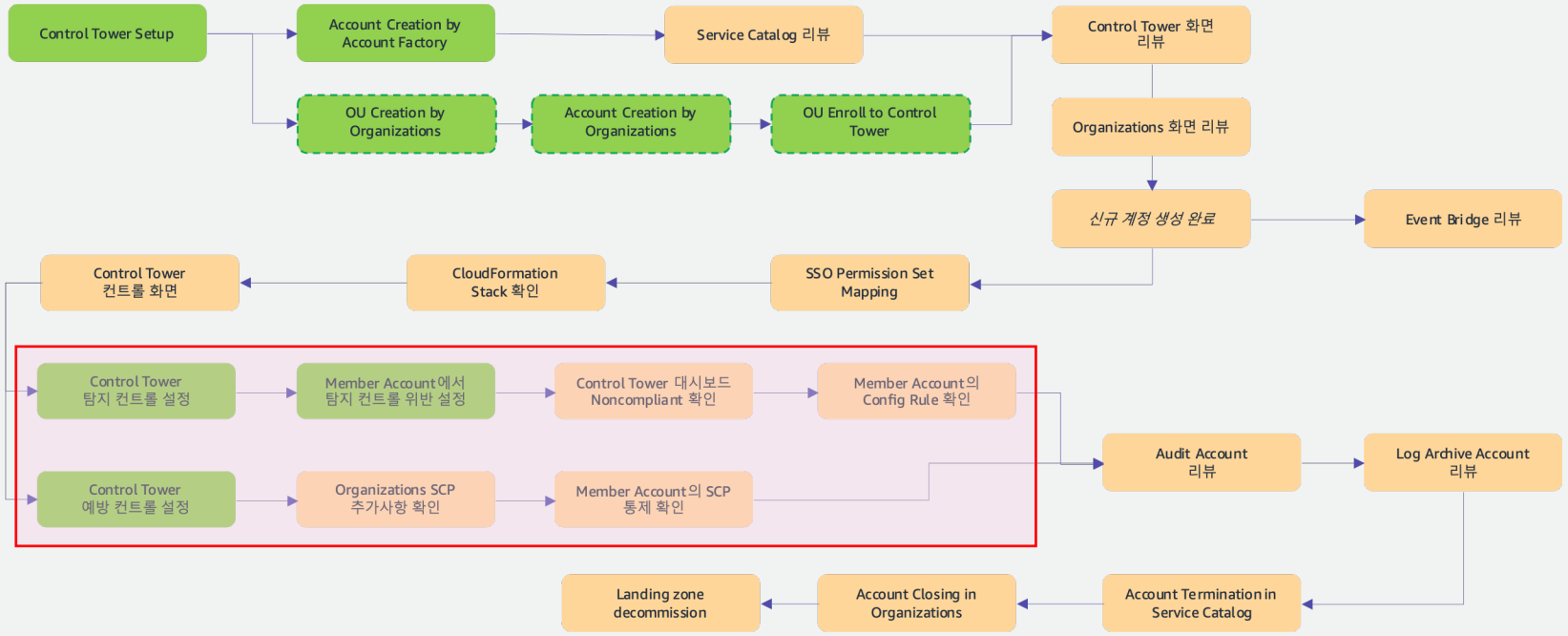
Control Tower 기본 컨트롤 외 추가 컨트롤 정보

- Control Tower의 컨트롤은 고객의 니즈에 따라 지속적으로 추가될 계획이나, 고객이 직접 컨트롤을 추가할 수 있음.
- 탐지 컨트롤은 Config Rule을, 예방 컨트롤은 SCP의 다양한 케이스를 적용
- 다양한 OU 및 Account에 배포하기 위해서는 CfCT(Customizations for Control Tower) 솔루션을 활용
- 탐지 컨트롤 참고
  - AWS Config Managed Rules
- 예방 컨트롤 참고
  - Best Practices for AWS Organizations Service Control Policies in a Multi-Account Environment
  - AWS IAM Permission Guradrails
  - Example service control policies

Controls

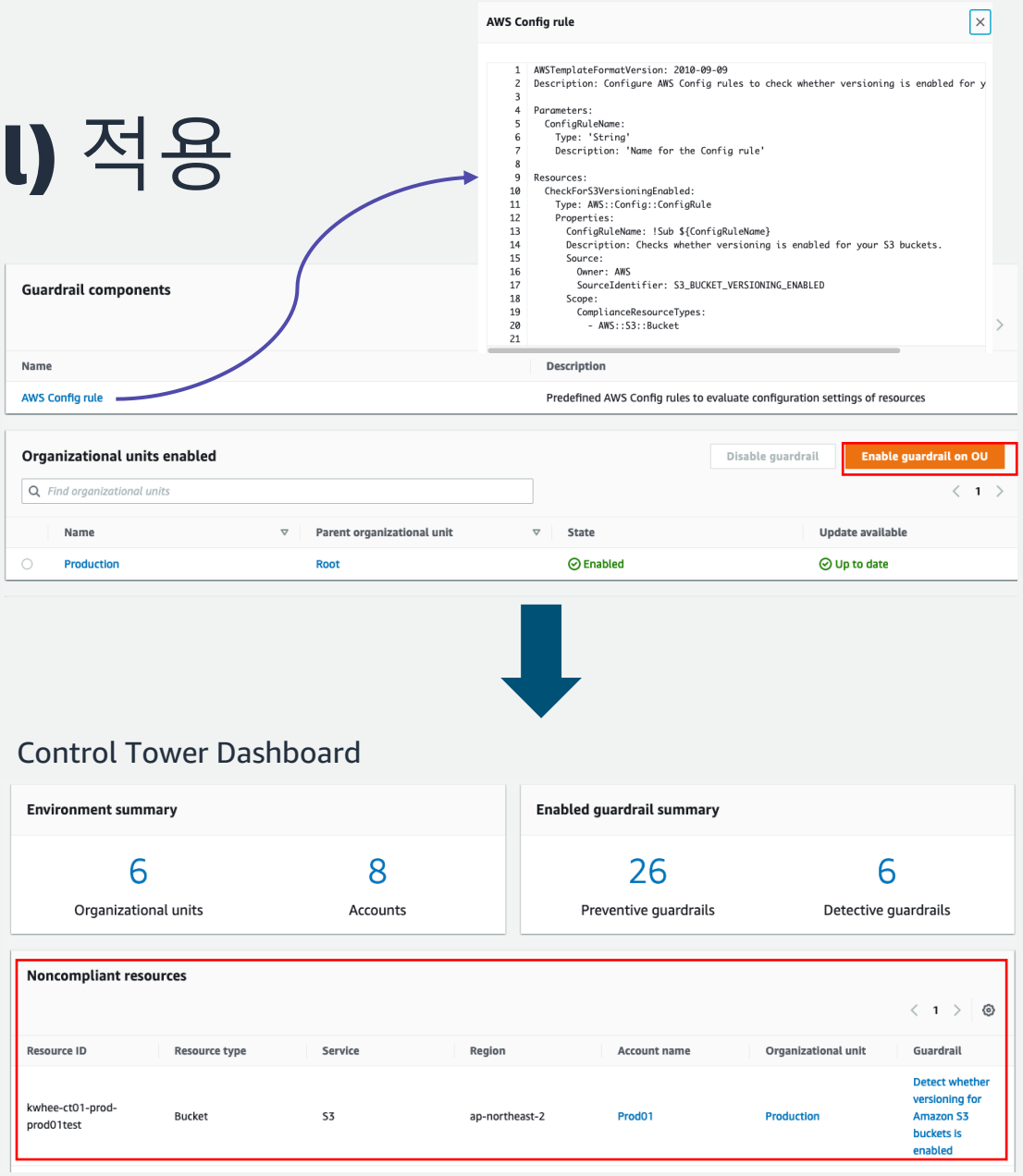


Hands-on Scenario



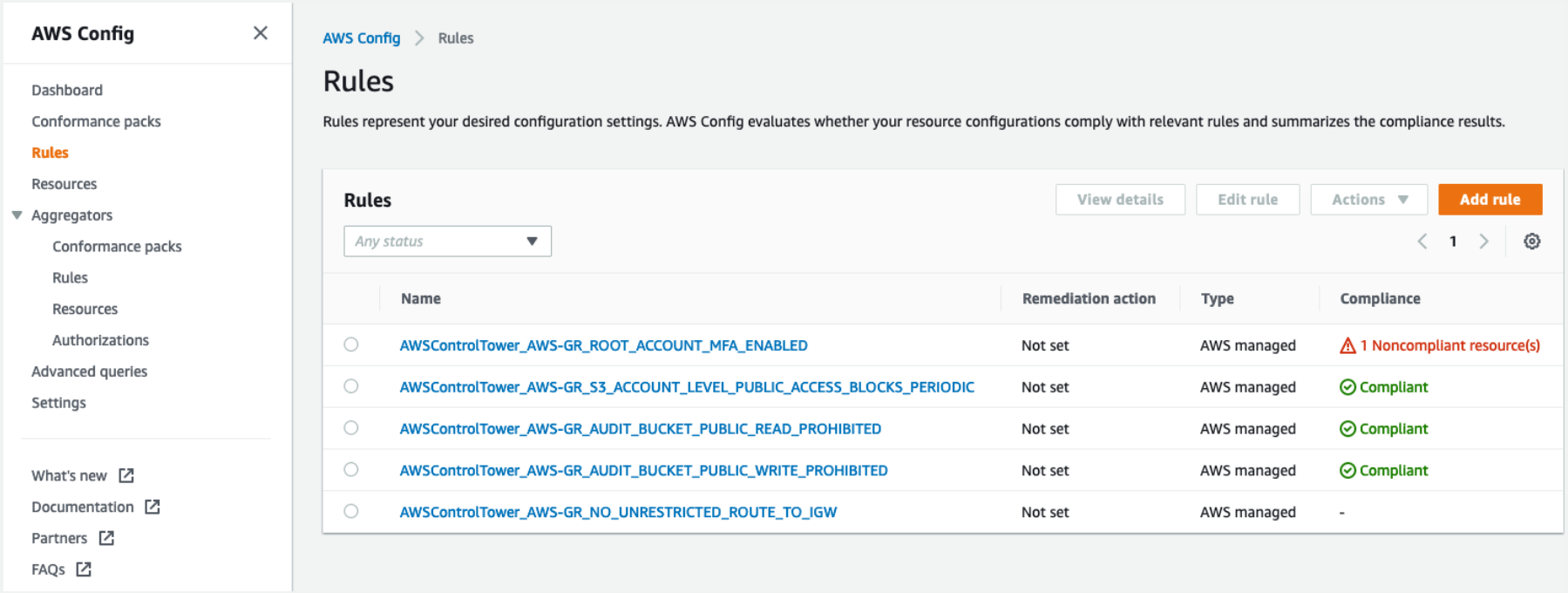
탐지 컨트롤(Detective Guardrail) 적용

- 적용 시나리오
  - Management Account 탐지 컨트롤 설정
    - Detect whether versioning for Amazon S3 buckets is enable로 이동
    - Guardrail components - AWS Config rule의 내용 확인
    - Organizational units enabled에서 “Enable guardrail on OU”를 통해 적용
    - CloudFormation - StackSet으로 이동하여 “AWSControlTowerGuardrailAWS-GR-S3-VERSIONING-ENABLED” 생성 과정 조회
  - 신규 Member Account
    - 신규 S3 Bucket 생성 : Default 상태인 Bucket Version의 “Disable” 상태로 생성
    - CloudFormation - Stack으로 이동하여, “StackSet-AWSControlTowerGuardrailAWS-GR-S3-VERSIONING-ENABLED-***” 형식의 Stack 조회 (Resource 탭)
    - AWS Config - Rules로 이동하여, “AWSControlTower_AWS-GR_S3_VERSIONING_ENABLED”의 상세내용 조회
  - Management Account
    - Control Tower Dashboard에서 Noncompliant resources 탐지 확인
    - 탐지되는데 약 5분~10분 소요되므로 예방 컨트롤 적용 후에 결과 확인



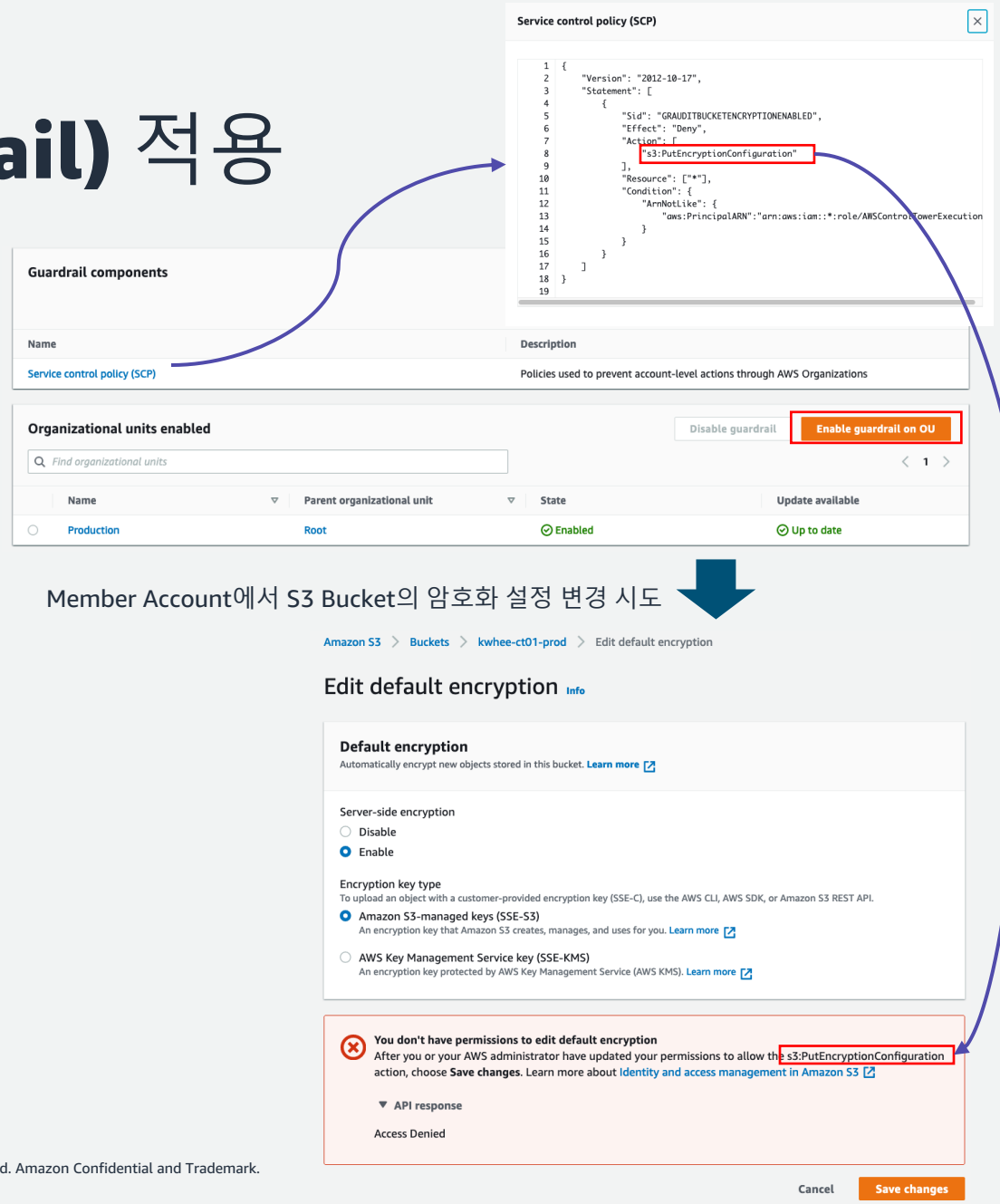
탐지 컨트롤 적용 후, **Member Account**의 **Config** 조회

- 탐지 컨트롤이 적용되면 CloudFormation StackSet을 통해 대상 Account에 배포됨
- 대상 Account의 CloudFormation Stack에서 새로 생성된 컨트롤 Stack 확인
- 대상 Account의 Config에서 새롭게 생성된 Config Rule 확인



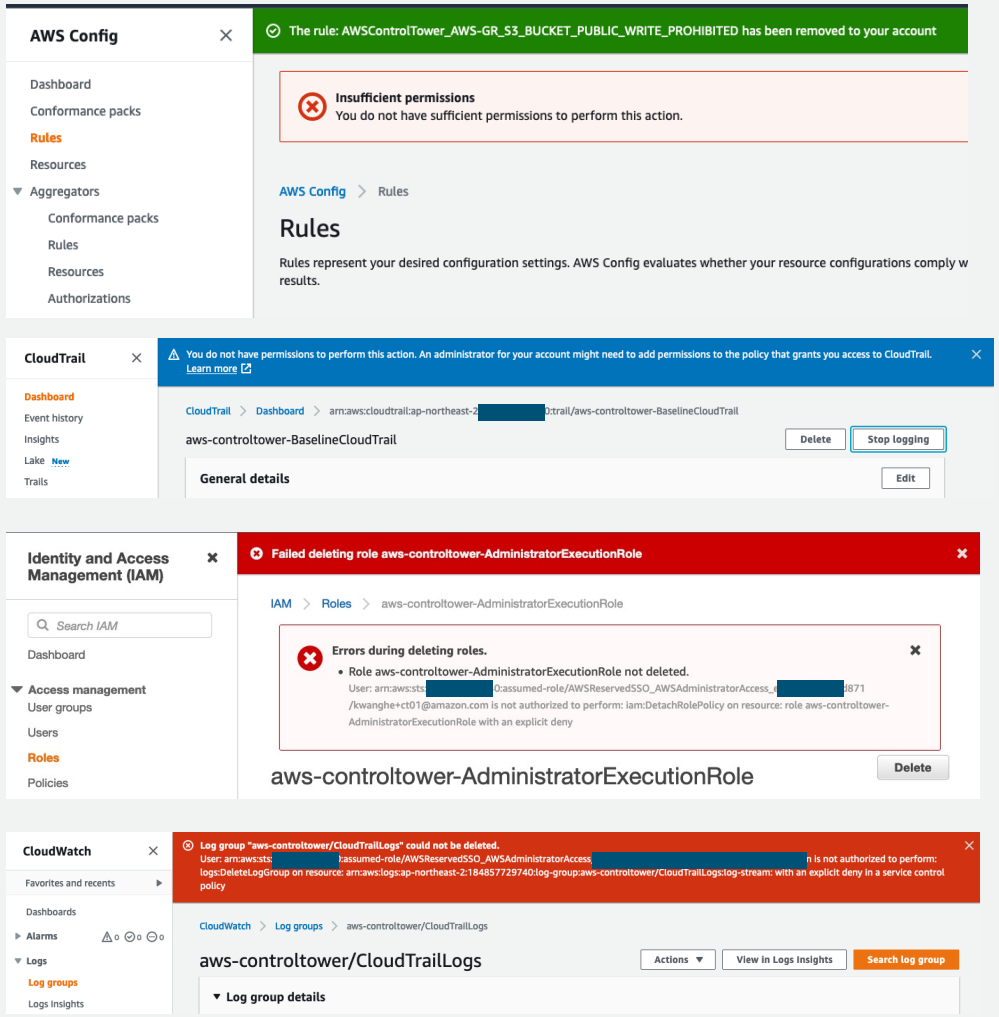
예방 컨트롤(Preventive Guardrail) 적용

- 적용 시나리오
  - Management Account 예방 컨트롤 설정
    - Disallow Changes to Encryption Configuration for Amazon S3 Buckets로 이동
    - Guardrail components - SCP의 내용 확인
    - Organizational units enabled에서 “Enable guardrail on OU”를 통해 적용
    - Organizations에서 해당 OU에 추가된 SCP 정책 확인
  - 신규 Member Account
    - 테스트로 생성한 S3 Bucket의 Properties에서 Default Encryption 설정 변경 시도
    - Permission 오류와 함께, “s3:PutEncryptionConfiguration”이 금지된 내용 확인



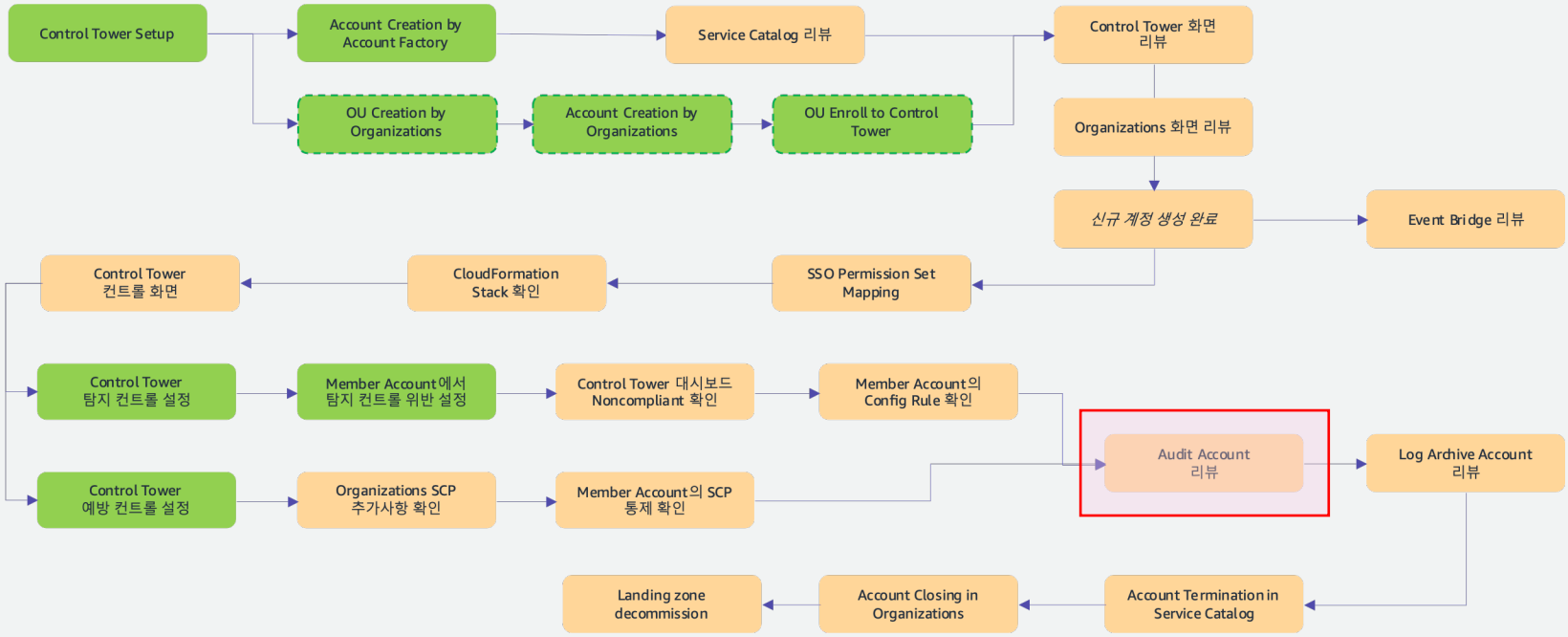
Control Tower 리소스 보호확인 - Mandatory Guardrail

- 필수(Mandatory) 컨트롤은 Control Tower 자체 리소스를 보호하기 위한 정책
- 주로 리소스의 Naming Rule(aws-controltower-*) 혹은 Tag를 통한 SCP 보호 정책이 적용되어 있음
- Member Account에서 각종 삭제 시도 시나리오
  - Control Tower 탐지 컨트롤 삭제
  - Control Tower CloudTrail Disable 시도
  - Control Tower IAM Role 삭제
  - Control Tower CloudWatch Log Group 삭제 시도



Audit Account Review

Hands-on Scenario

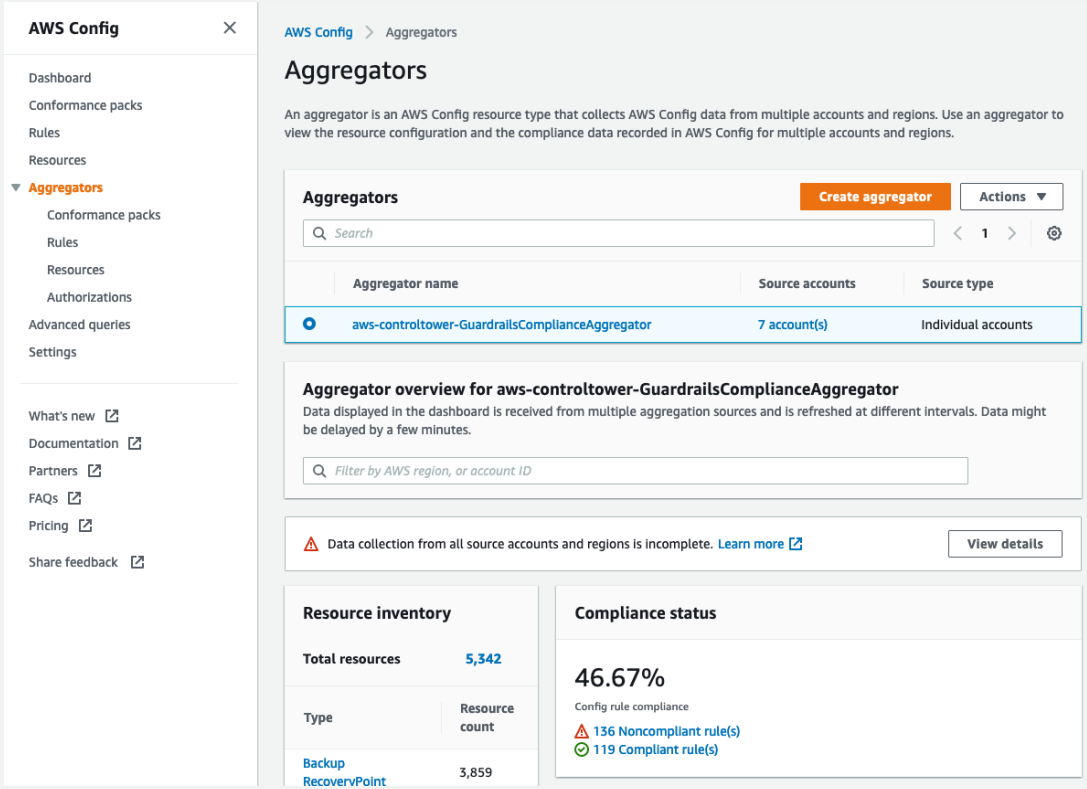


Audit 계정 리뷰

- Audit 계정은 보안팀과 감사 목적의 컴플라이언스 팀만 사용할 수 있도록 함
- Config Rule 및 GuardDuty, Security Hub 등의 관리 역할을 담당하고 자동화 된 보안조치(Remediation action) 등의 기능도 구현할 수 있음
- Control Tower 관련 리소스는 모두 CloudFormation Stack에서 확인 가능
- Audit 계정에서 운영되는 주요 서비스
  - Config Aggregator
  - GuardDuty
  - Inspector
  - Firewall Manager : WAF, Shield, Network Firewall, Security Group 등의 중앙집중형관리
  - Security Hub
  - Macie
  - Detective

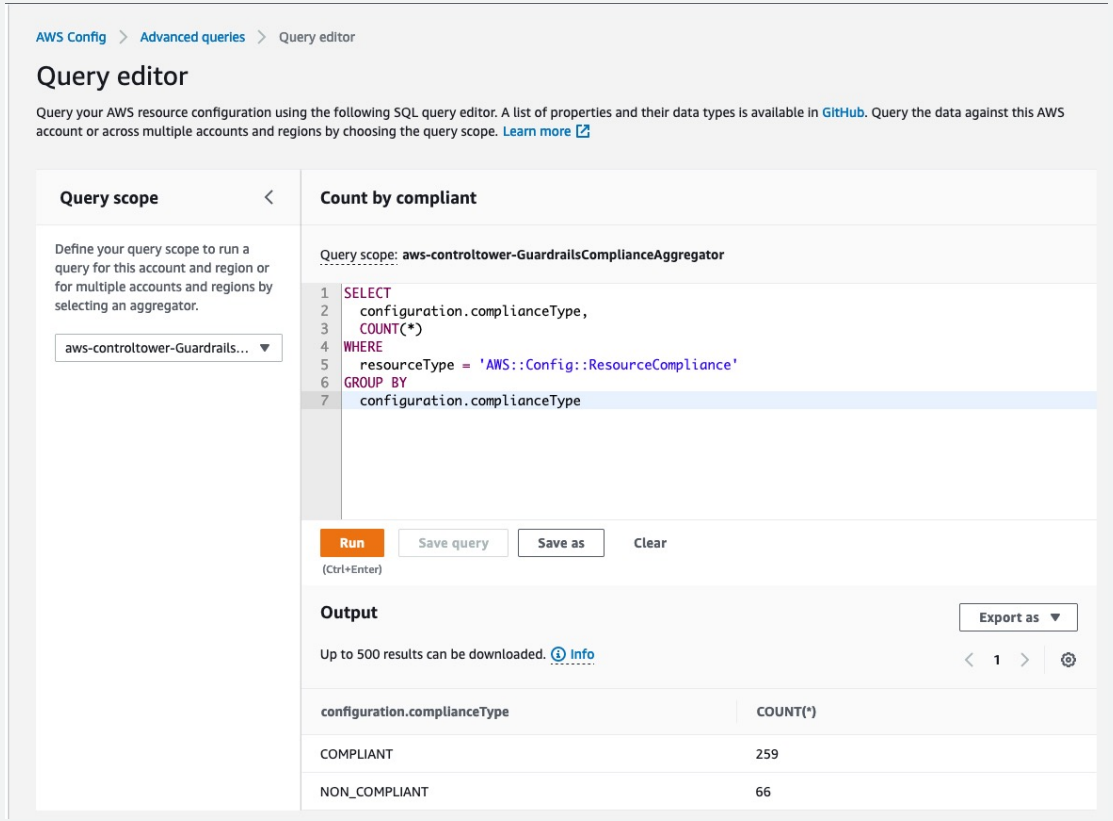
Config Aggregator

- Control Tower에서 관리하는 Account들에 대한 Config Rule 부합여부를 중앙에서 모니터링
- Control Tower에 의해 생성된 Aggregator를 통해 모든 Account의 Config Rule의 Compliance status가 수집됨



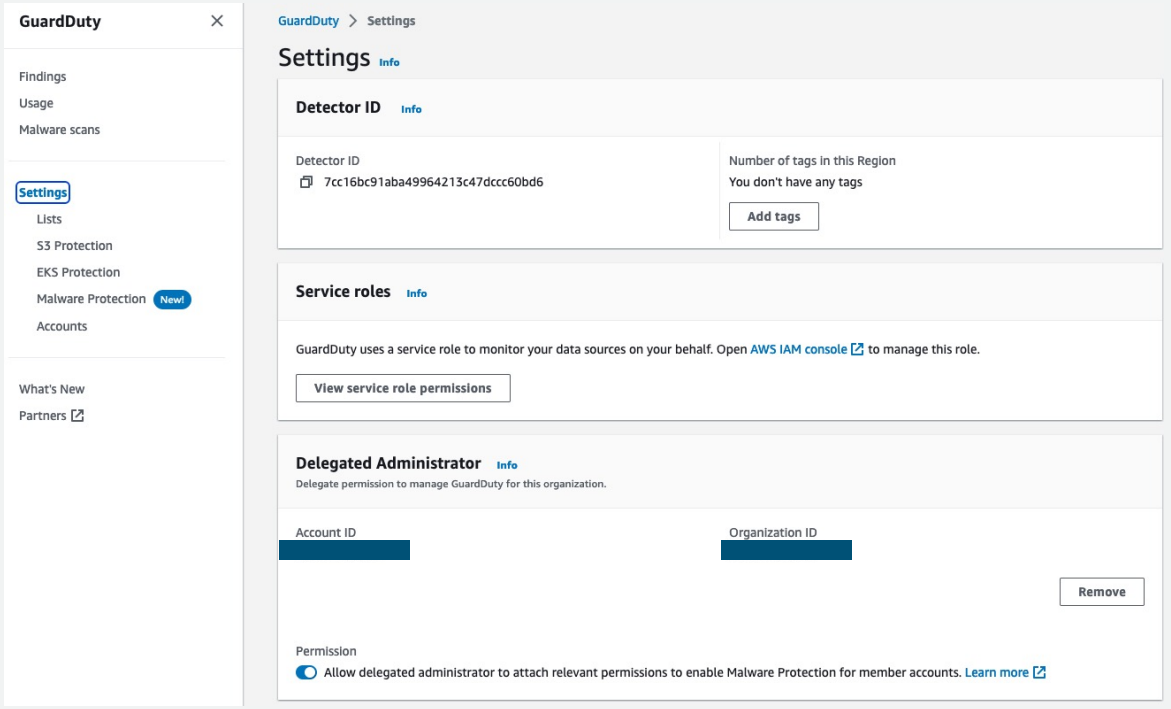
Config Advanced Query

- Config Aggregator를 통해 모든 Member Account의 Resource Configuration 정보를 조회할 수 있음.
- Organizations 내의 모든 Account 내의 인벤토리 정보를 확인하는데 유용
- Sample Query를 사용하여 손쉽게 응용 가능
- Resource Schema가 정의된 GitHub : https://github.com/awslabs/aws-config-resource-schema



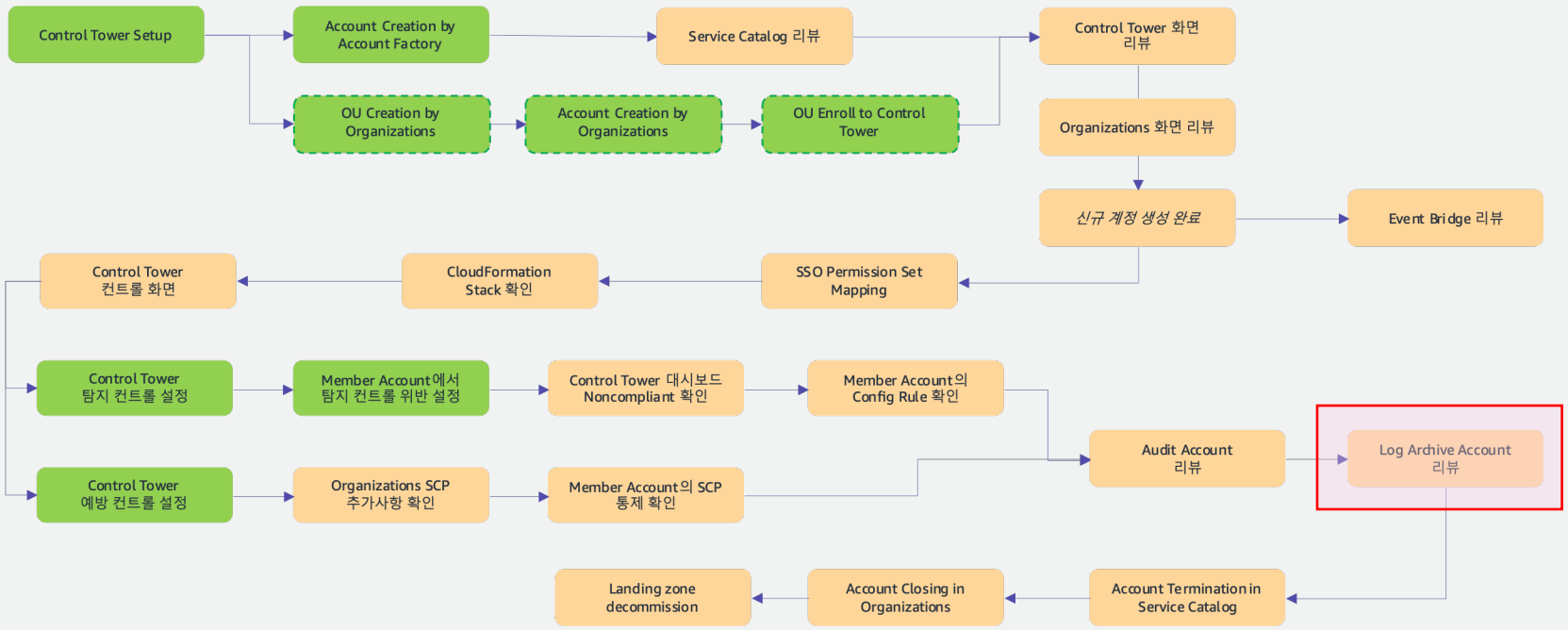
관리자 권한 위임(Delegated Administrator)

- Control Tower의 Management 계정에서 각 보안서비스의 관리자 권한을 Audit 계정으로 위임하도록 권고
- GuardDuty, Security Hub, Inspector, Macie, Detective, Firewall Manager 등 대부분의 보안 서비스는 설정 화면에서 Delegated Administrator를 지정할 수 있음



Log Archive Account Review

Hands-on Scenario



Log Archive 계정 리뷰

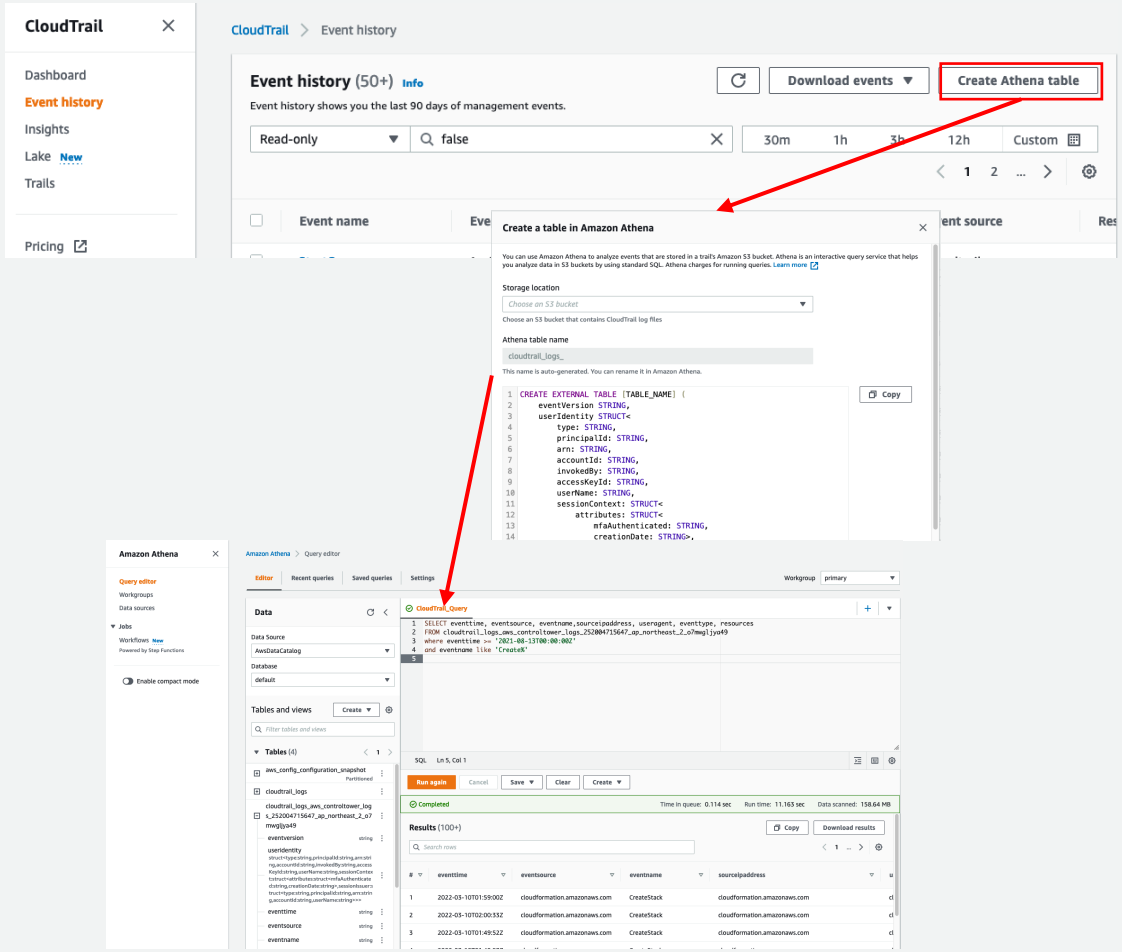
- Control Tower로 관리되는 모든 Account의 Cloudtrail, Config Log의 중앙 저장소로써, 반드시 컴플라이언스 및 보안 담당자만 접근할 수 있도록 함
- Control Tower 관련 리소스는 모두 CloudFormation Stack에서 확인 가능
- S3 Bucket 둘러보기
  - aws-controltower-logs-***
    - Bucket Hierarchy
    - Management의 Lifecycle rule : RetentionRule 1년으로 되어 있으며, 고객사 로그보관 정책에 따라 변경 필요
    - 변경 시에는 Management 계정의 Landing zone settting에서 변경하여 업데이트 수행
  - aws-controltower-s3-access-logs-***
    - aws-controltower-logs-*** Bucket의 Server Access Log

(참고) Log Archive의 CloudTrail Athena Query

- Athena Query를 사용하여, 전체 계정의 Cloudtrail을 일괄로 조회할 수 있음
  - https://docs.aws.amazon.com/athena/latest/ug/cloudtrail-logs.html

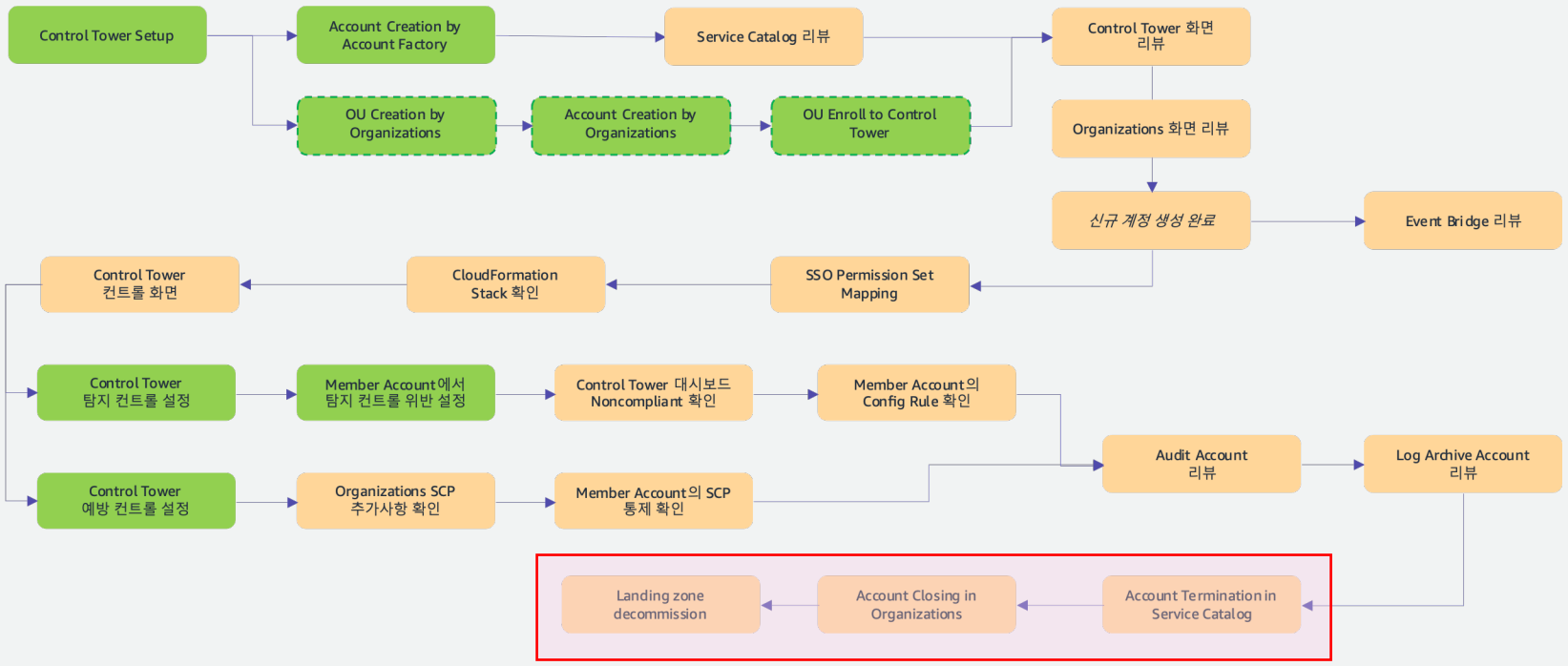
- Bucket 크기가 너무 커서, Scan 데이터를 특정 Account의 특정 기간으로 한정할 시 파티션 테이블 사용
  - https://www.gorillastack.com/blog/real-time-events/cloudtrail-athena-query

- 참고) Management Account에서 CloudTrail Lake를 통해서도 CloudTrail 로그 Query 가능
  - https://docs.aws.amazon.com/awscloudtrail/latest/userguide/cloudtrail-lake.html?icmpid=docs_console_unmapped



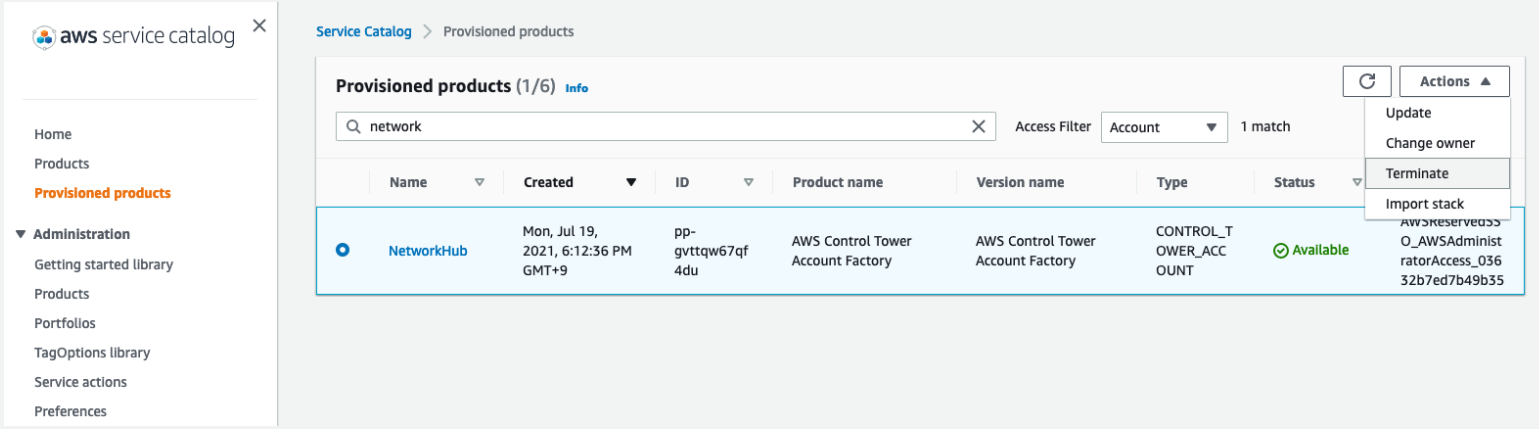
Control Tower에서 계정을 제외시켜 봅시다.

Hands-on Scenario



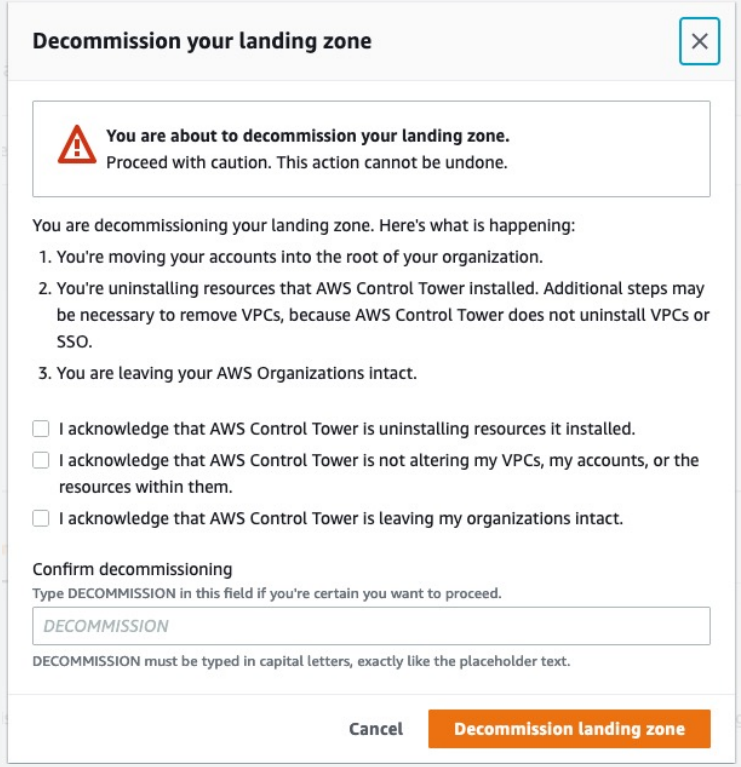
Account Termination in Service Catalog

- Member Account를 Control Tower의 Governance에서 제외하기 위해서는 Service Catalog의 Provisioned Product에서 Terminate 합니다. (몇 분 걸림)
- Terminate된 Account는 Control Tower에서 생성한 CloudFormation Stack 및 리소스를 삭제한 후, Root OU 밑으로 이동됩니다. 이때, CloudWatch Logs, SNS Topic 등의 일부 리소스는 삭제되지 않습니다.
- Service Catalog에서 Account를 Terminate 한다고 해서 완전히 Close되지는 않습니다. Organizations에서 해당 계정을 Close 할 수 있습니다. (계정 폐쇄 확인 메일 수신)
  - https://aws.amazon.com/blogs/mt/aws-organizations-now-provides-a-simple-scalable-and-more-secure-way-to-close-your-member-accounts/



Landing zone Decommission

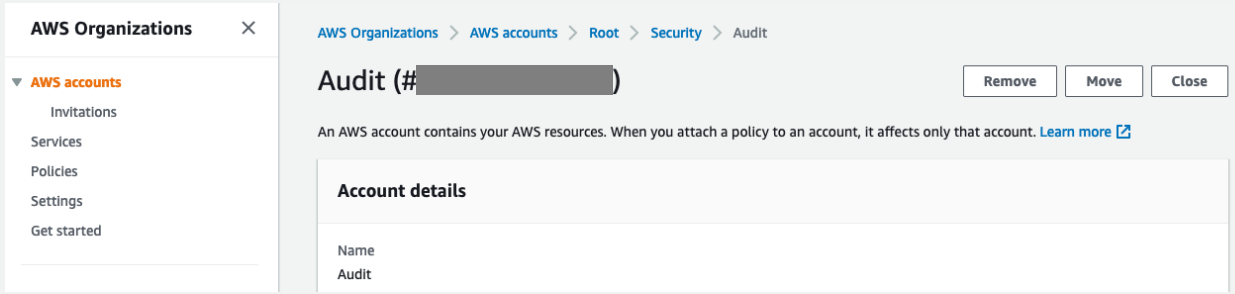
- CheckRide 후 삭제예정
- Control Tower의 Landing Zone Settings > Decommission your landing zone 선택
- Decommission에는 약 2시간 정도 소요
- Decommission 후에도 특정 S3 bucket, Organizations, CloudWatch Logs log group은 삭제되지 않으므로 수작업으로 삭제 필요
  - Control Tower 리소스 수작업 정리



Audit, Log Archive, Management Account Closing

- Organizations에서 Audit 및 Log Archive 계정을 Close 합니다. 단, Organizations에서는 전체 계정 개수의 월 10% 한도 내에서 삭제할 수 있기 때문에, 아래 방법으로 나머지 Account를 Closing 합니다.

- Management Account를 더 이상 사용하지 않을 경우 root로 로그인하여 Account를 Close 합니다.
  - https://docs.aws.amazon.com/organizations/latest/userguide/orgs_manage_accounts_close.html



Cleansing

Cleansing - Option1. Control Tower 환경 유지

- Control Tower 실습 후, Control Tower 환경을 일정기간 더 유지하면서 개인 학습을 원하실 경우, 아래와 같은 비교적 비용이 많이 발생할 수 있는 리소스 중 사용하지 않는 것들은 우선적으로 정리합니다.
  - GuardDuty, Inspector, SecurityHub 등 30일 무료체험 기간 후 유료전환 서비스
  - Network Firewall, WAF, Firewall Manager, Transit Gateway, NAT Gateway 등
  - Control Tower 탐지 가드레일(Config Rule)

- GuardDuty, Inspector, Security Hub 등은 Audit 계정에서 Member Account들을 모두 할당 해제 후, 개별 Account에서 각각 모두 서비스를 Suspend 및 Disable 처리함

- Network Firewall, WAF, Firewall Manager, Transit Gateway, NAT Gateway 등은 모든 리소스 및 정책을 의존성을 체크해 가면서 순차적으로 삭제

- Control Tower 가드레일은 Control Tower Console에서 활성화한 가드레일을 Disable 처리함

Cleansing - Option2. Control Tower 환경 제거

- Control Tower 실습 후, 모든 Control Tower 환경 정리 시에는 AWS계정들을 Suspend 합니다.
- Control Tower를 통해 생성한 계정을 먼저 Suspend 한 후, Audit, Log Archive 계정을 Suspend
- AWS Console 로그인 창으로 이동하여 Root 사용자로 로그인 선택 후, Suspend 할 이메일 계정 입력
- Forgot password(비밀번호 찾기) 기능을 통해 해당 계정의 Root 패스워드를 설정
- 새롭게 설정한 Root 패스워드로 Suspend할 계정에 로그인
- 브라우저 우측 상단의 계정(Account) 메뉴로 이동하여, 가장 하단의 ”계정 해지(Close Account)”를 클릭하여 Suspend 함
- Management 계정을 제외한 모든 계정에 대해 본 절차로 계정 해지절차를 진행하고, 최종 Billing 까지 확인 및 내부 청구가 완료되면 Management 계정도 해지 절차 진행

Reference

참조

Control Tower 한글 워크샵
https://catalog.us-east-1.prod.workshops.aws/workshops/1242b940-6f02-4d39-8ef2-2796370be864/ko-KR/

Control Tower 추가 워크샵(영문)
https://catalog.workshops.aws/control-tower/en-US

수고하셨습니다.

Appendix

Useful Link

- GitHub
  - AWS Samples (Control Tower 연동 샘플 다수) : https://github.com/orgs/aws-samples/repositories?language=&q=control+tower&sort=&type=all
  - awslabs (Control Tower는 아니만 Cloudformation 등 여러가지 샘플 코드 제공) : https://github.com/awslabs
  - aws-ia (AFT 솔루션, Terraform 위주의 자동화) : https://github.com/aws-ia
  - aws solution (CfCT, centralized-logging 등의 솔루션 소스코드) : https://github.com/aws-solutions

- AWS Blog 등 공개자료
  - Cloud Operation and Migrations - control tower : https://aws.amazon.com/blogs/mt/category/management-tools/aws-control-tower/
  - Infrastructure and automation - control tower : https://aws.amazon.com/blogs/infrastructure-and-automation/category/management-tools/aws-control-tower/
  - Architecture - control tower : https://aws.amazon.com/blogs/architecture/category/management-tools/aws-control-tower/
  - AWS Prescriptive Guidance - control tower : https://aws.amazon.com/prescriptive-guidance/?apg-all-cards.sort-by=item.additionalF[…]&apg-all-cards.q=control%2Btower&apg-all-cards.q_operator=AND

Useful Control Tower related solutions

- AWS Control Tower Design 모범지침
- Customizing account configuration with AWS Control Tower lifecycle events : 신규 계정 생성 시, Default VPC 삭제, Shared VPC 공유 및 Firewall Manager의 Security Group 적용 자동화
- Automating DNS infrastructure using Route 53 Resolver endpoints : Route 53 Resolver
- Migrate AWS Landing Zone solution to AWS Control Tower : AWS Landing Zone Solution을 Control Tower로 Migration 하는 방법
- Securely scale multi-account architecture with AWS Network Firewall and AWS Control Tower : Control Tower의 신규 계정이 Service Catalog를 사용한 Network Firewall 자동 적용
- Self-service VPCs in AWS Control Tower using AWS Service Catalog : Service Catalog를 사용하여, Member Account 사용자가 VPC 생성 및 TGW Attach를 Self-service로 작업