



AWS Config

Assess, Audit, and Evaluate

Hyeonsang Han(AWS)

AWS Professional Services | Sr. Security Risk and Compliance
Consultant

hanhyeon@amazon.com

Agenda

- ✓ 요구 사항
- ✓ AWS 운영 모델
- ✓ AWS Config 개요
- ✓ AWS Config Use Cases
- ✓ AWS Config 기능
- ✓ Q & A

퍼블릭 클라우드의 필요 사항

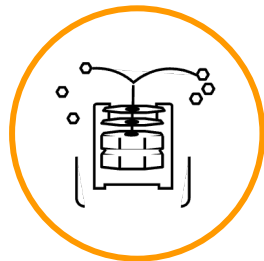
AWS 고객의 챌린지



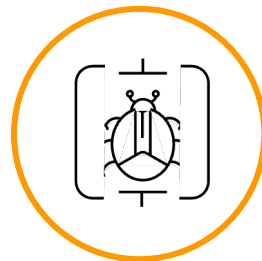
Dynamic



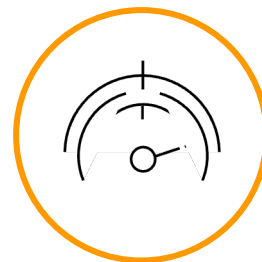
**Volume,
variety, and
velocity**



**글로벌화와
로컬라이징**



**빠르게 변화가
필요한 혁신**



**클라우드에
친화적인 구성**

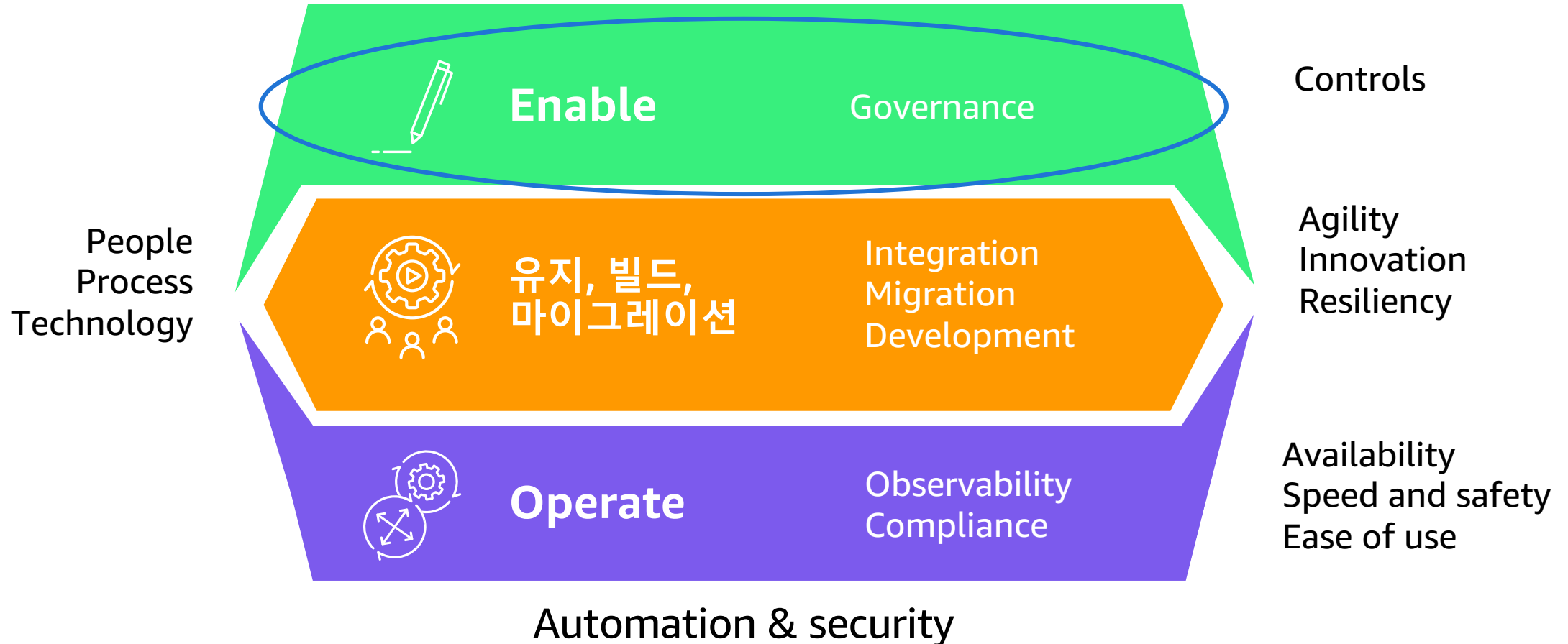


**다양한 규정 준수 및
보안 요구 사항**

AWS Cloud Ops

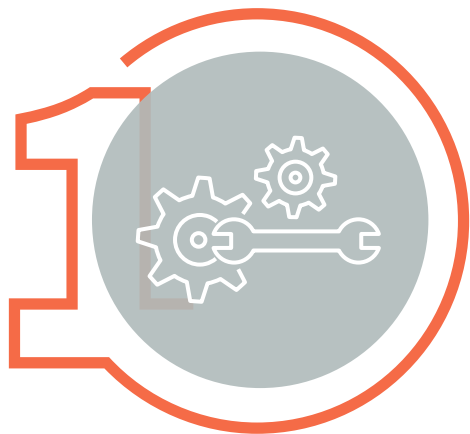
클라우드 & 온프레미스 또는 엣지에서 워크로드 사용, 구축, 운영 지원

Cloud financial management

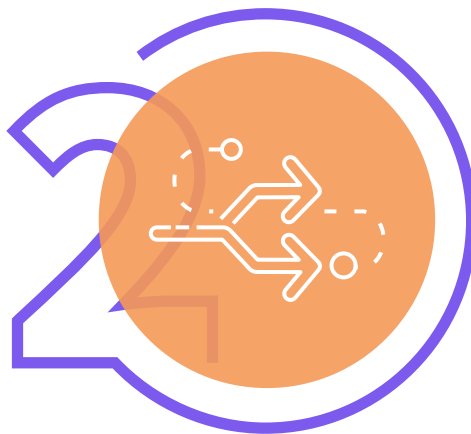


운영에 필요한 고객의 요구사항

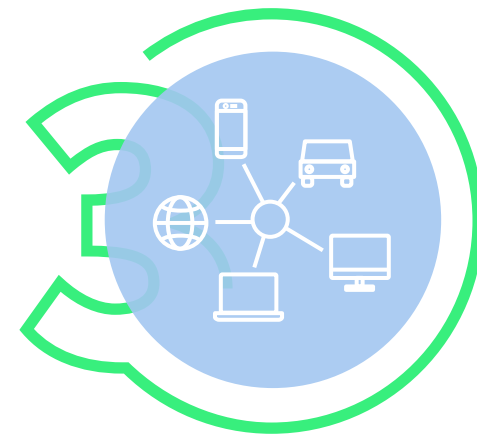
For Security Operation



리소스 규정 준수를 평가하는
방법은 무엇인가요?



대규모로 규정 준수를 관리하는
방법은 무엇인가요?



사용자 오류와 인터럽트를 줄이는
방법은 무엇인가요?

클라우드 운영환경에서 보안감사 시 고려할 사항

Governance and compliance, Inventory and configuration

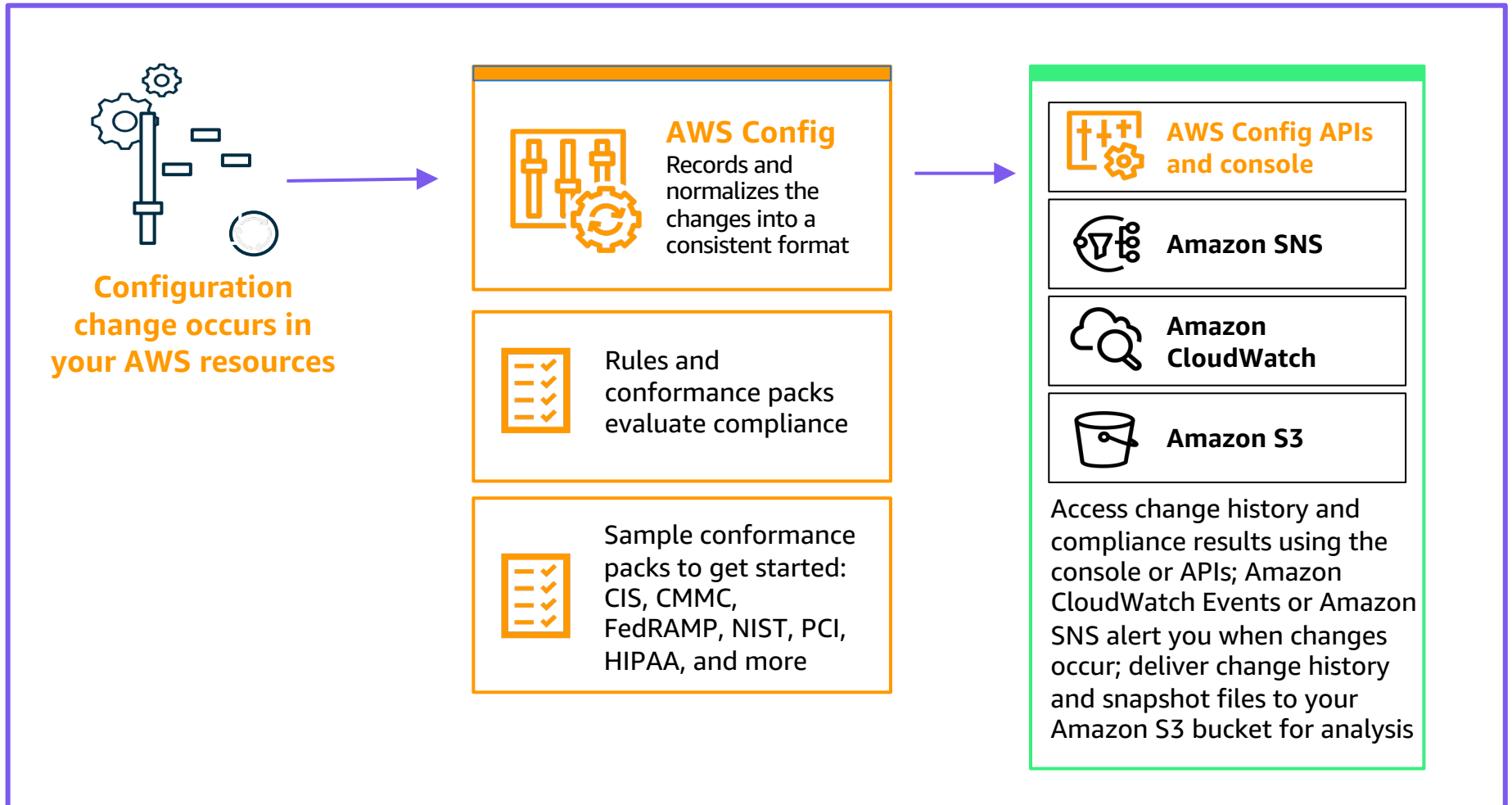
- 현재 구성된 리소스는 무엇이 있습니까?
- 리소스의 최신 구성 상태는 어떻게 됩니까?
- 리소스 간에 어떤 관계가 존재합니까?
- 과거에 발생한 구성 변경 사항은 무엇입니까?
- 규정 준수 정책을 위반한 리소스는 무엇입니까?
- 리소스가 제대로 구성되었습니까?
- 자원이 규제 요구 사항을 준수하는지 여부
- 지속적인 규정 준수를 보장하려면 어떻게 해야 합니까?
- 리소스가 규정을 준수하지 않을 경우 거의 실시간으로 알림을 받으려면 어떻게 해야 합니까?

AWS Config

평가, 감사 및 평가

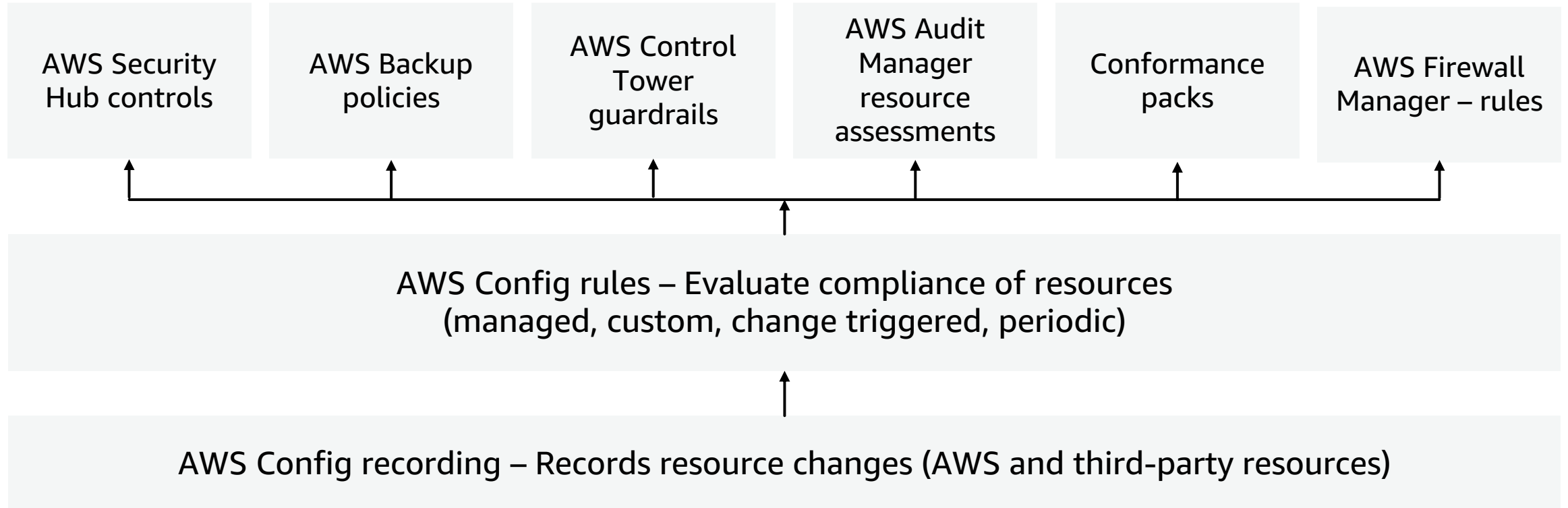


Assess, audit,
and evaluate



AWS Config

규정 준수 평가를 위한 핵심



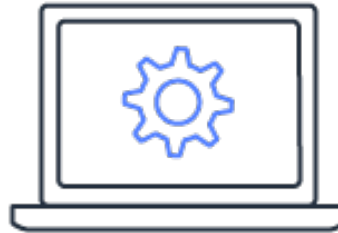
AWS Config 사용 이점



지속적인 모니터링



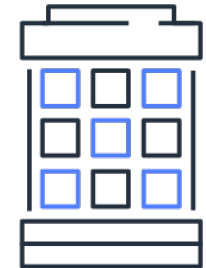
지속적인 평가 수행



변경사항
관리

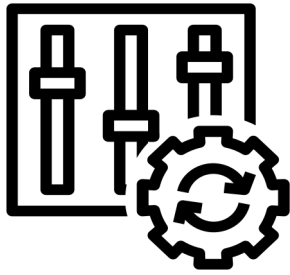


운영 이슈 식별
관리

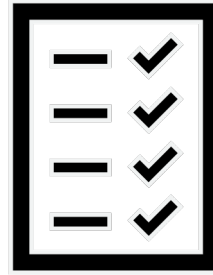


3rd 리소스를 연동
& 컴플라이언스
모니터링

AWS Config 유즈케이스



**AWS 리소스별 구성
내역에 대한 히스토리**
(3rd party and on
Premises resources)



컴플라이언스



구성 변경에 대한 가시성

AWS Config 유즈케이스

Configuration history of AWS resources

AWS Config를 사용하면 AWS, 온프레미스 및 기타 클라우드에서 리소스의 구성 및 관계의 변경 사항을 검토하고, 리소스 구성 이력을 탐색하고, 규칙을 사용하여 규정 준수를 결정할 수 있습니다.

Compliance

리소스 구성과 리소스 변경이 기본 제공 또는 사용자 지정 규칙을 준수하는지 평가하고, 규정을 준수하지 않는 리소스를 자동으로 수정할 수 있는 전략을 계획하고, 단일 계정, 리전 또는 AWS 조직을 통해 조직 전체에 배포할 수 있는 여러 규칙 및 수정 작업으로 구성된 규정 준수 팩을 사용할 수 있습니다.

Visualization of Configuration changes

구성은 리소스 인벤토리 및 규정 준수에 대한 중앙 집중식 보기를 제공하며, 집계된 데이터에 대해 고급 쿼리를 실행할 수 있습니다. 이 기능을 사용하면 유연성이 향상되고 여러 팀이 관리 계정에 액세스하여 조직 전체의 데이터를 사용할 필요가 없습니다.

AWS Config 기능

features



AWS 리소스의 구성 내역

AWS 리소스의 변경 사항에 대한 세부 정보를 기록하여 구성 기록 타임라인을 제공합니다.
과거의 어느 시점에서든 리소스 구성이 어떻게 생겼는지에 대한 세부 정보 얻기

소프트웨어 구성 기록 (SSM 에이전트 필요)

Amazon EC2 인스턴스 및 온프레미스 또는 다른 클라우드 공급자를 실행하는 서버 내에서 소프트웨어 구성 변경 사항을 기록합니다.

EC2 인스턴스에 대해 기록된 인프라 구성 변경 사항과 함께 OS 및 시스템 수준 구성 변경 내역 제공

구성 스냅샷

모든 리소스 및 해당 구성에 대한 시점 캡처 제공

구성 및 사용자 정의 가능한 규칙

기본 제공 또는 사용자 지정 규칙에 대한 규정 준수를 위해 리소스 구성 및 리소스 변경 사항을 평가하고 비준수 리소스의 문제 해결을 자동화합니다.

AWS Lambda에서 사전 구축된 규칙을 사용자 지정하거나 리소스 구성에 대한 내부 모범 사례 및 지침을 정의하는 사용자 지정 규칙을 생성합니다.

AWS Config 기능

features



리소스 관계 추적

계정에서 AWS 리소스 관계를 검색, 매핑 및 추적합니다.

예를 들어 새 Amazon EC2 보안 그룹이 Amazon EC2 인스턴스와 연결된 경우 Config는 Amazon EC2 보안 그룹과 Amazon EC2 인스턴스 모두의 업데이트된 구성을 기록합니다.

적합성 팩

AWS Config 규칙 및 수정 작업 모음을 단일 엔터티로 패키징하여 단일 계정 또는 전체 조직에 배포합니다.

다중 계정, 다중 리전 데이터 집계

리소스 및 Config 규칙 준수 상태에 대한 전사적 보기를 제공하여 중앙 집중식 감사 및 거버넌스를 지원합니다.

클라우드 거버넌스

비준수 리소스를 신속하게 찾아내고 적절한 조치를 취할 수 있도록 시각적 대시보드를 제공합니다.

기본 구성 컴포넌트

Config 의 구성 항목



리소스 구성 품목

계정에 있는 지원되는 AWS 리소스의 다양한 속성에 대한 특정 시점 보기를 나타냄
메타데이터, 속성, 관계, 현재 구성 및 관련 이벤트 포함

AWS Config는 기록 중인 리소스 유형에 대한 변경을 감지할 때마다 변경 사항 추적 생성

구성 히스토리

일정 기간 동안 지정된 리소스에 대한 구성 항목의 모음

리소스를 처음 만든 시간, 지난 달 동안 리소스가 구성된 방법, 변경 사항 확인 기능 지원
타임라인을 사용하여 API 또는 콘솔에서 리소스에 대한 기록 구성 항목에 액세스

구성 레코더

계정에서 지원되는 리소스의 구성을 저장

기본적으로 AWS Config가 실행 중인 리전에서 지원되는 모든 리소스를 기록

지정한 리소스 유형만 기록하는 사용자 지정 구성 레코더를 생성 지원

AWS 리소스

Resource check

The screenshot displays the AWS Config console interface for a specific resource. The left sidebar shows the navigation menu with 'Resources' selected. The main content area shows the details for the resource **i-0a0ff3ee031d01d26**. The 'Details' tab is active, showing a list of attributes. Four orange arrows point to specific elements: the 'Resource type' (AWS::EC2::Instance), the 'Resource ID' (i-0a0ff3ee031d01d26), the 'Amazon Resource Name' (arn:aws:ec2:ap-northeast-2:088985876653:instance/i-0a0ff3ee031d01d26), and the 'Resource Timeline' button in the top right corner. The 'Resource Timeline' button is also highlighted with an orange box.

Attribute	Value
Resource name	i-0a0ff3ee031d01d26
Resource type	AWS::EC2::Instance
Resource ID	i-0a0ff3ee031d01d26
Amazon Resource Name	arn:aws:ec2:ap-northeast-2:088985876653:instance/i-0a0ff3ee031d01d26
Availability zone	ap-northeast-2a
Created on	November 13, 2023 10:45 AM
Instance Type	t3.medium
Instance state	stopped
Private DNS	ip-10-0-0-124.ap-northeast-2.compute.internal
Private Ips	10.0.0.124
Public DNS	-
AMI ID	ami-0f0cc846201190547
Platform	-
Launch time	2023-11-13T01:45:17.000Z
Lifecycle	-
Monitoring	enabled

AWS 리소스

Timeline change check

Events

All times are in Asia/Seoul (UTC+09:00)

Start date

2023/11/20

Event type

Now

All event types

November 20, 2023

14:03:16

Configuration change

7 field change(s)

JSON diff - 7 field change(s)

From

```
{
  Configuration.NetworkInterfaces.0: {
    "association": {
      "ipOwnerId": "amazon",
      "publicDnsName": "ec2-13-124-89-120.ap-northeast-2.compute.amazonaws.com",
      "publicIp": "13.124.89.120",
      "attachment": {
        "attachTime": "2023-11-13T01:45:17.000Z",
        "deleteOnTermination": true,
        "deviceIndex": 0,
        "status": "attached",
        "networkCardIndex": 0,
        "description": "",
        "groups": [
          {
            "groupName": "IR-test-hhs-ForensicInstanceSecurityGroup-A42L00FPP5J6",
            "groupId": "sg-03dc99e10f88144eb"
          }
        ],
        "ipv6Addresses": [],
        "macAddress": "02:9d:a0:aa:ca:e2",
        "networkInterfaceId": "eni-08060ac10a58bfb8d",
        "ownerId": "088985876653",
        "privateDnsName": "ip-10-0-0-124.ap-northeast-2.compute.internal",
        "privateIpAddress": "10.0.0.124",
        "privateIpAddresses": [
          {
            "association": {
              "ipOwnerId": "amazon",
              "publicDnsName": "ec2-13-124-89-120.ap-northeast-2.compute.amazonaws.com",
              "publicIp": "13.124.89.120",
              "primary": true,
              "privateDnsName": "ip-10-0-0-124.ap-northeast-2.compute.internal",
              "privateIpAddress": "10.0.0.124"
            },
            "sourceDestCheck": true,
            "status": "in-use",
            "subnetId": "subnet-0c42ec51e9227657d",
            "vpcId": "vpc-06300f120900a81a8",
            "interfaceType": "interface"
          }
        ]
      }
    }
  }
}
```

To

```
{
  Configuration.NetworkInterfaces.1: {
    "attachment": {
      "attachTime": "2023-11-13T01:45:17.000Z",
      "deleteOnTermination": true,
      "deviceIndex": 0,
      "status": "attached",
      "networkCardIndex": 0,
      "description": "",
      "groups": [
        {
          "groupName": "IR-test-hhs-ForensicInstanceSecurityGroup-A42L00FPP5J6",
          "groupId": "sg-03dc99e10f88144eb"
        }
      ],
      "ipv6Addresses": [],
      "macAddress": "02:9d:a0:aa:ca:e2",
      "networkInterfaceId": "eni-08060ac10a58bfb8d",
      "ownerId": "088985876653",
      "privateDnsName": "ip-10-0-0-124.ap-northeast-2.compute.internal",
      "privateIpAddress": "10.0.0.124",
      "privateIpAddresses": [
        {
          "primary": true,
          "privateDnsName": "ip-10-0-0-124.ap-northeast-2.compute.internal",
          "privateIpAddress": "10.0.0.124"
        }
      ],
      "sourceDestCheck": true,
      "status": "in-use",
      "subnetId": "subnet-0c42ec51e9227657d",
      "vpcId": "vpc-06300f120900a81a8",
      "interfaceType": "interface"
    }
  }
}
```

Configuration.State.Name: "running"

Configuration.PublicIp.Address: "13.124.89.120"

Configuration.State.Reason: ""

Configuration.PublicIp.Name: "ec2-13-124-89-120.ap-northeast-2.compute.amazonaws.com"

Configuration.State.Name: "stopped"

Configuration.State.Reason: "User initiated (2023-11-20 05:02:26 GMT)"

Configuration.PublicIp.Name: ""

Configuration.State.Reason: "Client.UserInitiatedShutdown: User initiated shutdown"

View full record

AWS Config Rules

Detective controls

- **AWS Config rules**
 - ✓ 지속적인 규정 준수
 - ✓ 정기 감사
- **Conformance pack**
 - ✓ 시나리오 기반 배포
 - ✓ 전반적인 컴플라이언스 준수 상태를 위한 구성 항목
 - ✓ Security Hub standards vs conformance packs

기본 컴포넌트

Config Rule



AWS Config Rule

특정 AWS 리소스 또는 전체 AWS 계정에 대해 원하는 구성 설정을 확인

리소스가 규칙을 위반하는 경우 AWS Config는 리소스와 규칙을 준수하지 않는 것으로 플래그를 지정

AWS Config는 사용자 지정 가능한 사전 정의된 규칙을 제공하여 시작하는 데 도움이 되지만 사용자 지정 규칙을 생성 가능

Evaluation Triggers

AWS Config는 리소스 구성 변경 사항을 지속적으로 추적하지만 이러한 변경 사항이 규칙의 조건을 위반하는지 여부를 확인

규칙을 활성화하면 AWS Config가 리소스를 규칙의 조건과 비교하며 초기 평가 이후 AWS Config는 평가가 트리거될 때마다 평가를 계속 실행

평가 트리거는 규칙의 일부로 정의되며 다음의 유형이 포함

- 구성 변경: 규칙의 범위와 일치하는 리소스가 구성에서 변경되면 평가를 트리거
- 주기적: 선택한 빈도 (예: 24시간마다) 로 규칙에 대한 평가를 실행

AWS Config Rules



지속적인 리소스 모니터링을 통해
효과적인 거버넌스 프레임워크를 구축하기 위한 서비스

구성 변경 사항 분석

AWS 에서 제공하는 347 Managed Rule

AWS Lambda 를 활용한 사용자 정책 적용가능

GitHub repo: Community sourced rules

Aggregate compliance into a central account

Compliance history

AWS Config Rules

매니지드 룰

Specify rule type

Step 1: Specify rule type
Step 2: Configure rule
Step 3: Review and create

Select rule type

- ☒ Add AWS managed rule
Customize any of the following rules to suit your needs.

securityhub-iam-support-policy-in-use-2fe8df89

Rule details

Description: Checks that the 'AWSSupportAccess' managed policy is attached to any IAM user, group, or role.

Enabled evaluation mode: **DETECTIVE**

Last successful detective evaluation: **November 20, 2023 3:52 AM**

Config rule ARN: **arn:aws:config:ap-northeast-2:592238680800:config-rule/aws-service-rule/securityhub.amazonaws.com/config-rule-6xsh03**

Detective evaluation trigger type: Periodic: 12 hours

Scope of changes: -

Parameters

Key	Type	Value	Description
policyARN	String	arn:aws:iam::aws:policy/AWSSupportAccess	An IAM policy ARN to be checked.
policyUsageType	String	ANY	Specify whether you expect the policy to be attached to an IAM user, group or role. Valid values are IAM_USER, IAM_GROUP, IAM_ROLE,

Resources in scope

Noncompliant

ID	Type	Status	Annotation	Compliance
592238680800	Account	-	-	Noncompliant

AWS Config Rules

매니지드 룰

Timeline

The resource timeline allows you to view all the configuration items captured over time for a specific resource and the compliance status changes. For accurate reporting on the compliance status, you must record the AWS Config ResourceCompliance resource type.

General details

Resource ID	Resource type	Resource name
592238680800	AWS::::Account	-

Events

All times are in Asia/Seoul (UTC+09:00)

Start date

2023/11/20

Now

Event type

All event types

October 19, 2023

15:52:53

Rule compliance

7 Noncompliant rule(s)

10 rule(s) applied

15:52:52

Rule compliance

6 Noncompliant rule(s)

8 rule(s) applied

15:52:52

Rule compliance

5 Noncompliant rule(s)

7 rule(s) applied

15:52:51

Rule compliance

3 Noncompliant rule(s)

5 rule(s) applied

May 16, 2023

14:10:16

Rule compliance

All compliant

1 rule(s) applied

14:10:15

Rule compliance

4 Noncompliant rule(s)

5 rule(s) applied

14:10:13



Rule compliance

4 Noncompliant rule(s)

6 rule(s) applied

AWS Config Rules

규정 준수 변경 사항

General details			
Resource ID 592238680800	Resource type AWS::Account	Date May 16, 2023 2:10 PM	Compliance  Compliant
Rules			
Rule name	Compliance status	Amazon resource name	
AWSControlTower_AWS-GR_DETECT_CLOUDTRAIL_ENABLED_ON_SHARED_ACCOUNTS	 Compliant	arn:aws:config:ap-northeast-2:592238680800:config-rule/config-rule-uhomsa	
JSON diff - 5 field change(s)			
From	To		
<pre>{ Configuration.configRuleList.1: {"configRuleArn":"arn:aws:config:ap-northeast-2:592238680800:config-rule/aws-service-rule/securityhub.amazonaws.com/config-rule-z0vs0c","configRuleId":"config-rule-z0vs0c","configRuleName":"securityhub-ec2-ebs-encryption-by-default-3d3cdba3","complianceType":"NON_COMPLIANT"} Configuration.configRuleList.0: {"configRuleArn":"arn:aws:config:ap-northeast-2:592238680800:config-rule/aws-service-rule/securityhub.amazonaws.com/config-rule-xskqa6","configRuleId":"config-rule-xskqa6","configRuleName":"securityhub-root-account-lambda-mfa-enabled-04e10b5a","complianceType":"NON_COMPLIANT"} Configuration.complianceType: "NON_COMPLIANT" Configuration.configRuleList.2: {"configRuleArn":"arn:aws:config:ap-northeast-2:592238680800:config-rule/aws-service-rule/securityhub.amazonaws.com/config-rule-a5hhsb","configRuleId":"config-rule-a5hhsb","configRuleName":"securityhub-iam-password-policy-prevent-reuse-check-c9c0d06f","complianceType":"NON_COMPLIANT"} Configuration.configRuleList.2: {"configRuleArn":"arn:aws:config:ap-northeast-2:592238680800:config-rule/aws-service-rule/securityhub.amazonaws.com/config-rule-vxuero","configRuleId":"config-rule-vxuero","configRuleName":"securityhub-root-account-mfa-enabled-fdfbfea6","complianceType":"NON_COMPLIANT"} }</pre>	<pre>{ Configuration.configRuleList.1: {"configRuleArn":"arn:aws:config:ap-northeast-2:592238680800:config-rule/aws-service-rule/securityhub.amazonaws.com/config-rule-z0vs0c","configRuleId":"config-rule-z0vs0c","configRuleName":"securityhub-ec2-ebs-encryption-by-default-3d3cdba3","complianceType":"NON_COMPLIANT"} Configuration.configRuleList.0: {"configRuleArn":"arn:aws:config:ap-northeast-2:592238680800:config-rule/aws-service-rule/securityhub.amazonaws.com/config-rule-xskqa6","configRuleId":"config-rule-xskqa6","configRuleName":"securityhub-root-account-lambda-mfa-enabled-04e10b5a","complianceType":"NON_COMPLIANT"} Configuration.complianceType: "COMPLIANT" Configuration.configRuleList.2: {"configRuleArn":"arn:aws:config:ap-northeast-2:592238680800:config-rule/aws-service-rule/securityhub.amazonaws.com/config-rule-a5hhsb","configRuleId":"config-rule-a5hhsb","configRuleName":"securityhub-iam-password-policy-prevent-reuse-check-c9c0d06f","complianceType":"NON_COMPLIANT"} Configuration.configRuleList.2: {"configRuleArn":"arn:aws:config:ap-northeast-2:592238680800:config-rule/aws-service-rule/securityhub.amazonaws.com/config-rule-vxuero","configRuleId":"config-rule-vxuero","configRuleName":"securityhub-root-account-mfa-enabled-fdfbfea6","complianceType":"NON_COMPLIANT"} }</pre>		

AWS Config Conformance Pack



구성 규정 준수 공통 프레임워크

단일 엔터티로서 AWS Config 규칙 및 수정 작업 모음
단일 계정 및 리전 또는 AWS 조직의 조직 전체에 배포

Immutable

개별 규칙은 액세스 권한이나 계정 권한에 관계없이 변경불가
기관의 마스터 계정에 의해 배포되는 경우 기관의 구성원 계정으로 수정불가

샘플 템플릿

PCI-DSS, AWS 모범 사례 (S3, DynamoDB 및 IAM) 와 같은 다양한 운영 모범 사례에 사용할 수 있는 샘플 적합성 팩 템플릿
K-ISMS 적합성 팩 적용 가능

샘플 템플릿은 사용자 지정 적합성 팩을 개발하는 데 도움이 되는 시작 지점을 제공

AWS Config Conformance Pack

Step 1

Specify template

Step 2

Specify conformance pack details

Step 3

Review and deploy

Specify template

Template details

Conformance pack template

Every conformance pack is based on a template. A template is a YAML file that contains configuration information about AWS accounts and regions where you want to deploy AWS Config rules and remediation actions.

☒ Use sample template

☐ Template is ready

Sample template

Select a sample template

This collection of sample templates will help you get started with conformance packs and quickly build your own template.

Choose sample template

Q

AWS Control Tower Detective Guardrails

Operational Best Practices For NIST 800 181

Operational Best Practices For Networking and Content Delivery Services

Operational Best Practices For Security Identity and Compliance Services

Operational Best Practices for 800 53 rev 4

Operational Best Practices for ABS CCIGv2 Material

Operational Best Practices for ABS CCIGv2 Standard

Operational Best Practices for ACSC Essential8

Operational Best Practices for ACSC ISM

Operational Best Practices for AI and ML

Operational Best Practices for API Gateway

Operational Best Practices for APRA CPG 234

Operational Best Practices for AWS Backup

Operational Best Practices for AWS Identity and Access Management

Operational Best Practices for AWS Well Architected Reliability Pillar

Operational Best Practices for AWS Well Architected Security Pillar

Operational Best Practices for Amazon DynamoDB

Cancel

Next

Step 1

Specify template

Step 2

Specify conformance pack details

Step 3

Review and deploy

Specify template

Template details

Conformance pack template

Every conformance pack is based on a template. A template is a YAML file that contains configuration information about AWS accounts and regions where you want to deploy AWS Config rules and remediation actions.

☒ Use sample template

☐ Template is ready

Sample template

Select a sample template

This collection of sample templates will help you get started with conformance packs and quickly build your own template.

Operational Best Practices for KISMS cpack

Cancel

Next

AWS Config Aggregate



애그리게이터

여러 소스 계정 및 리전에서 AWS Config 구성 및 규정 준수 데이터를 수집하는 AWS Config의 리소스 유형

애그리게이터 계정

하나 이상의 애그리게이터를 소유한 AWS 관리 계정

소스 계정

AWS Config 리소스 구성 및 규정 준수 데이터를 집계하려는 AWS 계정

소스 계정은 개별 계정 또는 AWS 조직의 조직일 수 있습니다.

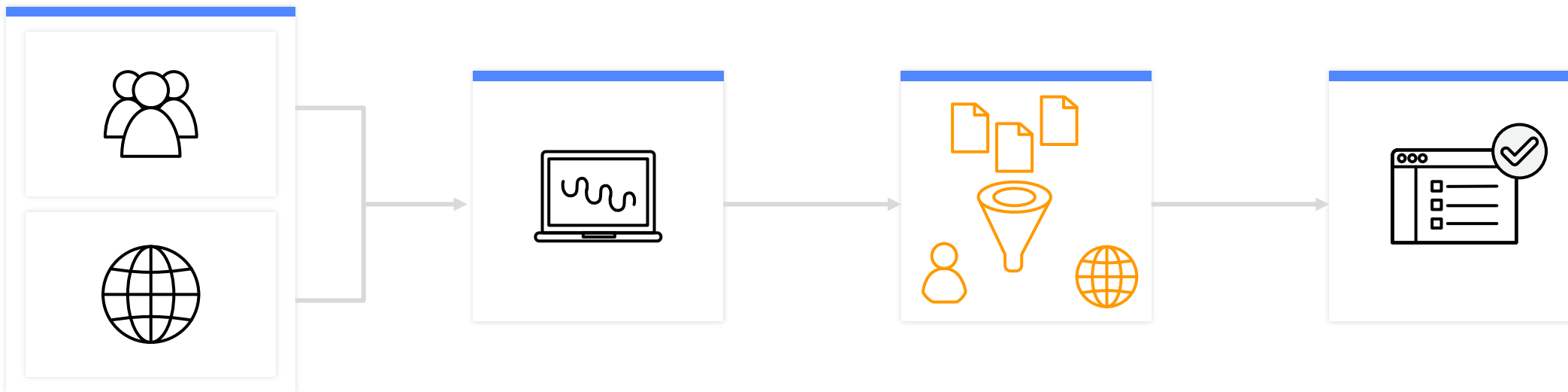
소스 계정을 개별적으로 제공하거나 AWS Organization 을 통해 지정 가능

권한 부여

소스 계정 소유자는 AWS Config 구성 및 규정 준수 데이터를 수집하기 위해 애그리 게이터 계정 및 리전에 부여하는 권한을 의미
AWS 조직의 일부인 소스 계정을 집계하는 경우에는 승인이 필요하지 않음

AWS Config Aggregate

다중 계정, 다중 지역 데이터 집계 기능



계정 및 지역

AWS Config 데이터를 수집할 소스 계정 및 리전을 선택합니다.

AWS Config data

여러 소스 계정 및 리전에서 AWS Config 데이터 수집

애그리게이터

AWS Config에 기록된 리소스 구성 정보 및 규정 준수 데이터를 포함합니다.

집계된 뷰

각 집계자에 대한 모든 준수 및 비준수 규칙 및 리소스 보기

AWS Config Aggregate

AWS Config

Dashboard

Conformance packs

Rules

Resources

Aggregators

Compliance Dashboard New

Conformance packs

Rules

Inventory Dashboard New

Resources

Authorizations

Advanced queries

Settings

What's new

Documentation

Partners

FAQs

Pricing

AWS Config > Aggregators > Resources

Resources

Search multi-account multi-region aggregator resources recorded by AWS Config. To view the details for each resource click the specific resource ID.

Resources


View details

Select aggregator

aws-controltower-GuardrailsComplianceAgg... ▼

Account:

Account	Resource type	Region	Account
Account: 592238680800			
Account: 822151173718 IRFK	IAM Role	ap-northeast-2	100566362651
Account: 420919311495 RPRX	IAM Role	ap-northeast-2	100566362651
Account: 868770922179 ZXMH	IAM Role	ap-northeast-2	100566362651
Account: 774643770299 2GCD	IAM Role	ap-northeast-2	100566362651
Account: 391366672259 RH6Q	IAM Role	ap-northeast-2	100566362651
Account: 921444970065 JVV4D	IAM Role	ap-northeast-2	100566362651
Account: 834656587780 XRGZ	IAM Role	ap-northeast-2	100566362651
Account: 100566362651	IAM Role	ap-northeast-2	100566362651
Account: 997404792226	IAM Role	ap-northeast-2	100566362651
Account: 340247219775	IAM Role	ap-northeast-2	100566362651
AROARO2RY5IN4P5CW1FB	IAM Role	ap-northeast-2	100566362651
AROARO2RY5IN4NQYNJBFY	IAM Role	ap-northeast-2	100566362651
AROARO2RY5IN4YHWZ3JDT	IAM Role	ap-northeast-2	100566362651
AROARO2RY5IN54PXWZP26	IAM Role	ap-northeast-2	100566362651



AWS Config Aggregate

적용 필터

AWS Config

Dashboard

Conformance packs

Rules

Resources

▼ Aggregators

Compliance Dashboard New

Conformance packs

Rules

Inventory Dashboard

Resources

Authorizations

Advanced queries

Settings

What's new

Documentation

Partners

FAQs

Pricing

AWS Config > Aggregators > Resources

Resources

Search multi-account multi-region aggregator resources recorded by AWS Config. To view the details for each resource click the specific resource ID.

Resources

View details

Select aggregator

aws-controltower-GuardrailsComplianceAgg... ▼

Filter by resource type, resource identifier, AWS region, or account ID

Filter by

AWS Resource type

Resource identifier

Region


Account

ier

:5JJ7HRFK

:7B4GRPRX

	Resource type	Region	Account
<input type="radio"/>	IAM Role	ap-northeast-2	100566362651
<input type="radio"/>	IAM Role	ap-northeast-2	100566362651
<input type="radio"/>	IAM Role	ap-northeast-2	100566362651
<input type="radio"/>	IAM Role	ap-northeast-2	100566362651
<input type="radio"/>	IAM Role	ap-northeast-2	100566362651
<input type="radio"/>	IAM Role	ap-northeast-2	100566362651
<input type="radio"/>	IAM Role	ap-northeast-2	100566362651
<input type="radio"/>	IAM Role	ap-northeast-2	100566362651
<input type="radio"/>	IAM Role	ap-northeast-2	100566362651
<input type="radio"/>	IAM Role	ap-northeast-2	100566362651



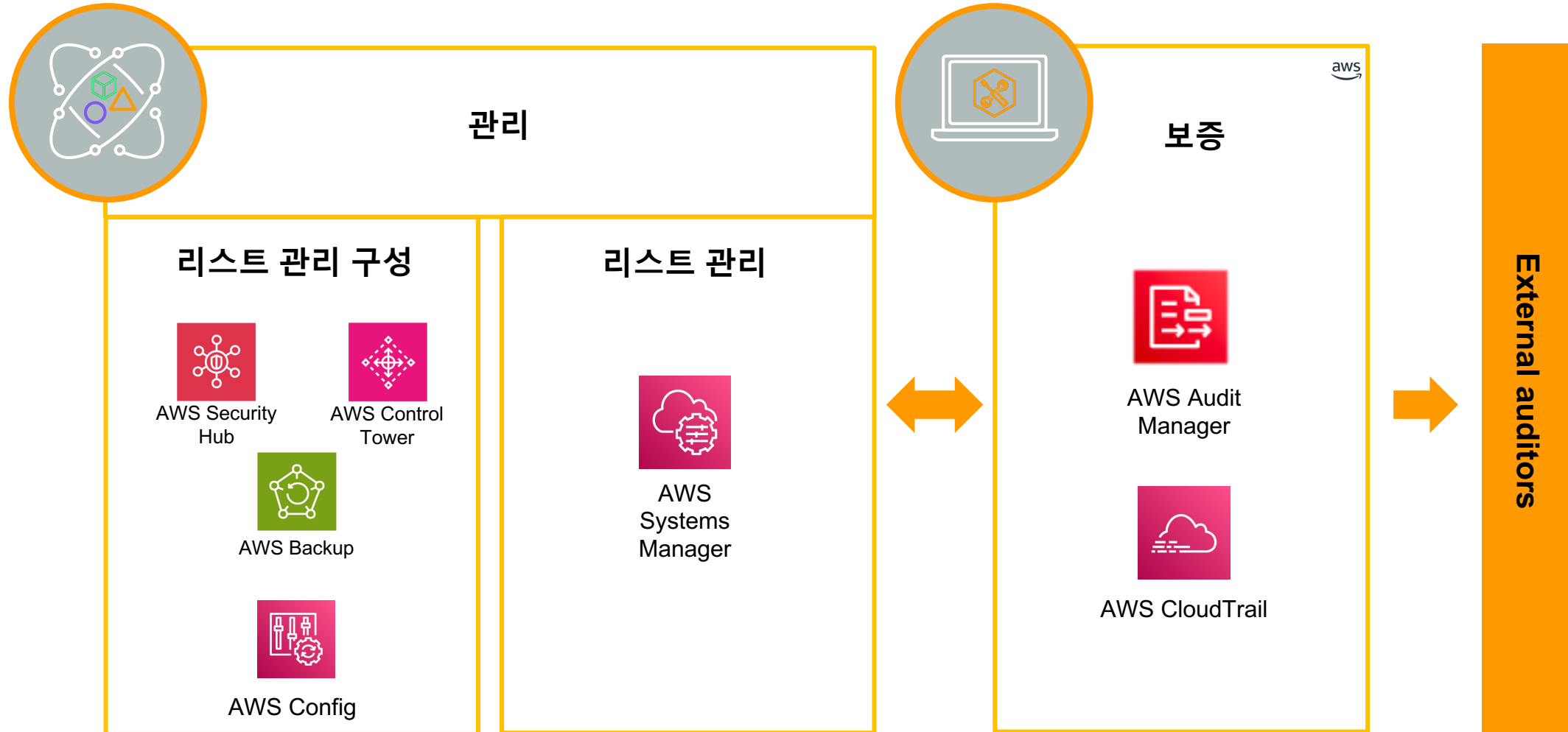
aws professional services

© 2023, Amazon Web Services, Inc. or its affiliates. All rights reserved. Amazon Confidential and Trademark.

클라우드 규정 준수 및 보증 지원

The IIA's three lines model

IIA = Institute of Internal Auditors





감사합니다.