



개발자 가이드

AWS 네트워크 보안 관리자



AWS 네트워크 보안 관리자: 개발자 가이드

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

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

Table of Contents

AWS Network Security Manager란 무엇입니까?	1
AWS Network Security Manager 작동 방식 한 눈에 보기	1
AWS Network Security Manager의 기능	1
사용 사례	2
관련 서비스	2
AWS Network Security Manager 액세스	3
요금	4
를 처음 사용하십니까?	4
AWS Network Security Manager 작동 방식	5
AWS Network Security Manager 리소스 모델	5
AWS Network Security Manager 리소스 수명 주기, 병합 및 동기화	6
초안 및 활성 수명 주기	6
버전 관리	7
우선순위 기반 정책 병합	8
AWS Config를 사용한 리소스 검색	9
동기화 및 문제 해결	9
관리자 및 멤버 계정	11
서비스 연결 역할	11
AWS Network Security Manager 설정	12
조직 모델 선택	12
단일 계정 사용을 위한 설정	12
AWS Organizations에서 다중 계정 사용을 위한 설정	13
AWS Network Security Manager 관리자 계정 생성	13
AWS Network Security Manager 권한을 사용하여 IAM 자격 증명 생성	15
에 가입 AWS 계정	16
기본적으로 비활성화된 리전에서 AWS Network Security Manager 사용	16
자습서: 첫 번째 네트워크 보안 보호 배포	18
사전 조건	18
1단계: 규칙 생성	19
2단계: 템플릿 생성	20
3단계: 정책 생성	21
4단계: 범위 생성	22
5단계: 배포 생성 및 게시	22
6단계: 동기화 상태 모니터링	23

7단계: 정리	24
다음 단계	25
방화벽 및 보안 서비스 관리	26
AWS WAF용 웹 ACLs 관리	26
AWS WAF 개념	26
AWS WAF용 빠른 생성	30
AWS WAF의 표준 생성 프로세스	33
AWS Shield Advanced에 대한 DDoS 보호 관리	39
AWS Shield Advanced용 빠른 생성	39
AWS Shield Advanced의 표준 생성 프로세스	42
AWS Network Security Manager 및 Firewall Manager	46
AWS Firewall Manager와 공존	46
문제 해결 중 우선 순위	46
AWS Firewall Manager에서 계획된 마이그레이션	46
보안	47
데이터 보호	47
저장된 데이터 암호화	48
전송 중 암호화	49
키 관리	49
ID 및 액세스 관리	49
대상	49
ID를 통한 인증	50
정책을 사용하여 액세스 관리	51
AWS Network Security Manager와 IAM의 작동 방식	52
ID 기반 정책 예시	58
문제 해결	62
서비스 연결 역할	63
서비스 연결 역할 권한	64
서비스 연결 역할 만들기	74
서비스 연결 역할 편집	75
서비스 연결 역할 삭제	75
지원되는 리전:	75
규정 준수 확인	76
복원력	76
인프라 보안	76
보안 모범 사례	77

예방 제어	77
탐지 제어	77
AWS Network Security Manager 모니터링	78
동기화 상태 모니터링	78
동기화 상태 작업	78
동기화 상태 값 이해	78
평가 타임스탬프 이해	79
교차 계정 가시성	79
out-of-sync 리소스 진단	79
CloudTrail 로그	80
AWS CloudTrail의 Network Security Manager 정보	80
예: CreatePolicy 이벤트	82
할당량	84
리소스 할당량	84
리소스 구성 할당량	84
범위 구성 할당량	85
관리자 계정 할당량	85
API 페이지 매김 할당량	85
할당량 조정 가능성	86
문서 기록	87
.....	lxxxviii

AWS Network Security Manager란 무엇입니까?

AWS Network Security Manager를 사용하면 조직의 하나 이상의 계정 및 리소스에 AWS WAF 및 AWS Shield Advanced 규칙과 같은 네트워크 보안 보호를 중앙에서 정의하고 배포할 수 있습니다. 각 리소스를 개별적으로 사용하는 대신 재사용 가능한 정책 객체(규칙, 템플릿 및 정책)를 한 번 정의하고 대규모로 배포하며 정책 드리프트를 감지하고 해결하기 위한 지속적인 모니터링을 제공합니다.

AWS Network Security Manager 작동 방식 한 눈에 보기

계층적 정책 객체 세트를 정의하고 대상 범위에 적용합니다. 가장 낮은 수준의 정책 객체는 규칙입니다. 우선 순위 기반 충돌 해결이 포함된 정책으로 결합할 수 있는 템플릿으로 규칙을 그룹화할 수 있습니다. 그런 다음 범위로 보호할 계정과 리소스를 선택하고 배포를 게시하여 정책을 적용합니다.

배포 후 AWS Network Security Manager는 범위가 지정된 환경 및 배포된 정책을 지속적으로 모니터링하여 의도한 정의와 일치하는지 확인합니다. 그렇지 않은 경우 AWS Network Security Manager는 의도한 구성에서 드리프트되는 리소스를 선택적으로 수정할 수 있습니다. 리소스 모델, 수명 주기 및 아키텍처에 대한 자세한 내용은 섹션을 참조하세요 [AWS Network Security Manager 작동 방식](#).

AWS Network Security Manager의 기능

- 여러 방화벽 유형 지원 - AWS Network Security Manager는 웹 ACL 구성 및 규칙 그룹에 대해 AWS WAF를 지원합니다. 보호되는 리소스 유형에는 Amazon CloudFront 배포, Application Load Balancer 및 Amazon API Gateway 단계가 포함됩니다. AWS Network Security Manager는 Amazon CloudFront 배포, Application Load Balancer, Classic Load Balancer 및 탄력적 IP 주소의 DDoS 보호를 위해 AWS Shield Advanced도 지원합니다.
- 재사용 가능한 보안 구성 - 정책 객체를 규칙으로 한 번 정의하고, 템플릿으로 그룹화하고, 대상 리소스에 대한 범위를 생성합니다. 여러 정책 및 배포에서 규칙, 템플릿 및 범위를 재사용합니다.
- 우선 순위 기반 정책 병합 - 여러 정책이 동일한 리소스를 보호하는 경우 AWS Network Security Manager는 정책 우선 순위에 따라 구성을 병합하여 예측 가능한 충돌 해결을 제공합니다.
- 단일 계정 및 다중 관리자 지원 - 단일 계정에서 AWS Network Security Manager를 사용하거나 각 우선순위 수준이 있는 여러 관리자 계정을 지정합니다. 관리자의 정책이 겹치면 AWS Network Security Manager는 먼저 관리자 우선 순위별로 충돌을 해결한 다음 각 계정 내의 정책 우선 순위별로 충돌을 해결합니다.
- 초안 및 활성 상태 - 규칙, 템플릿, 정책, 범위 및 배포를 포함한 각 AWS Network Security Manager 리소스는 초안 및 활성 상태를 지원합니다. 라이브 보호에 영향을 주지 않고 리소스를 초안으로 저장한 다음 적용할 준비가 되면 게시합니다.

- 버전이 지정된 스냅샷 - 규칙, 템플릿, 정책, 범위 및 배포를 포함한 각 AWS Network Security Manager 리소스는 버전 번호가 지정된 변경 불가능한 스냅샷을 지원합니다. 버전 관리를 사용하여 잘 알려진 AWS Network Security Manager 리소스 구성을 보존합니다.
- 보호된 리소스 동기화 진단 - 범위 내 각 리소스에 대해 동기화되지 않은 설정과 각 구성 필드의 실제 값과 비교한 예상 설정을 정확히 확인합니다.
- 자동 수정 - 선택적으로 AWS Network Security Manager가 out-of-sync 리소스를 자동으로 수정하고 수동 개입 없이 의도한 구성에 맞게 조정할 수 있습니다.
- 자연어 규칙 생성 - GenerateRuleConfiguration 작업을 사용하여 규칙을 일반 언어로 설명하고 Amazon Bedrock으로 구동되는 해당 구성 JSON을 수신합니다.

사용 사례

다음은 AWS Network Security Manager의 일반적인 사용 사례입니다.

- 모든 계정에 기존 AWS WAF 규칙 적용 - 모든 인터넷 연결 애플리케이션이 사용해야 하는 AWS WAF 규칙 그룹 세트를 정의한 다음 전체 조직에 배포합니다. AWS Network Security Manager는 범위가 지정되면 새 범위 내 리소스에 규칙을 자동으로 적용합니다.
- 특정 리소스에서 특정 사용자 지정 또는 예외 AWS WAF 규칙 생성 - 특정 리소스 세트에만 적용되는 AWS WAF 규칙 세트를 정의합니다. 이 세트는 AWS 계정 ID, OU, 태그 또는 Amazon 리소스 이름(ARNs).
- 인터넷 연결 리소스에서 DDoS 보호 확인 - 퍼블릭 리소스 유형으로 범위가 지정된 AWS Shield Advanced 정책을 생성하고 조직 전체에 배포하여 중요한 리소스에 DDoS 보호가 활성화되도록 합니다.
- 구성 드리프트 감지 및 수정 - 동기화 상태 모니터링을 사용하여 방화벽 구성이 의도한 상태에서 드리프트된 리소스를 식별하고 필요에 따라 자동 수정을 활성화하여 규정 준수를 다시 시작합니다.
- 여러 팀에 보안 관리 위임 - 우선순위 수준이 다르고 특정 계정, 조직 단위 또는 방화벽 유형에 대한 범위가 지정된 액세스 권한을 가진 여러 관리자 계정을 지정하여 팀이 정의된 경계 내에서 자체 보안 정책을 관리할 수 있도록 합니다.

관련 서비스

- AWS WAF - AWS WAF를 사용하여 가용성에 영향을 미치거나, 보안을 손상시키거나, 과도한 리소스를 소비할 수 있는 일반적인 웹 악용 및 봇으로부터 웹 애플리케이션 및 APIs를 보호합니다. AWS Network Security Manager는 AWS WAF를 사용하여 단일 계정 또는 조직 내 여러 계정의 리소스에 대한 웹 ACLs 및 규칙 그룹을 생성하고 관리합니다.

- AWS Shield Advanced -에서 실행되는 애플리케이션에 대한 확장된 보호를 제공하는 관리형 DDoS 보호 서비스입니다. AWS Network Security Manager는 Shield Advanced를 사용하여 단일 계정 또는 조직의 여러 계정에 있는 리소스에 대해 DDoS 보호를 제공합니다.
- AWS 조직 - AWS 리소스를 확장하고 확장함에 따라 환경을 중앙에서 관리하고 관리하는 데 도움이 됩니다. AWS Network Security Manager를 사용하려면 AWS Organizations가 멤버 계정 전반에서 보호를 관리해야 합니다.
- AWS Config - AWS 리소스의 구성을 평가, 감사 및 평가할 수 있는 서비스입니다. AWS Network Security Manager는 서비스 연결 AWS Config 레코더를 사용하여 멤버 계정의 리소스를 검색합니다.

AWS Network Security Manager 액세스

다음 인터페이스를 통해 AWS Network Security Manager에 액세스할 수 있습니다.

AWS 관리 콘솔

AWS Network Security Manager 리소스를 관리하기 위한 웹 기반 인터페이스입니다.

<https://console.aws.amazon.com/network-security-manager/> AWS Network Security Manager 콘솔을 엽니다.

AWS 명령줄 인터페이스(CLI)AWS

AWS Network Security Manager 작업에 대한 명령을 제공합니다. 자세한 내용은 [AWS CLI 명령 참조](#)를 참조하세요.

AWS SDKs

AWS는 다양한 프로그래밍 언어 및 플랫폼을 위한 라이브러리 및 샘플 코드로 구성된 SDKs를 제공합니다. SDKs는 AWS Network Security Manager에 프로그래밍 방식으로 액세스할 수 있는 편리한 방법을 제공합니다. 자세한 내용은 [Amazon Web Services용 도구](#)를 참조하세요.

AWS Network Security Manager API

HTTPS를 통해 JSON을 사용하는 REST API입니다. API 엔드포인트 형식은 `network-security-manager.{region}.api.aws`입니다. 자세한 내용은 [AWS Network Security Manager API 참조](#)를 참조하세요.

AWS Network Security Manager를 시작하려면 [AWS Network Security Manager 설정](#) 및 섹션을 참조하세요. [자습서: 첫 번째 네트워크 보안 보호 배포](#).

요금

AWS Network Security Manager가 모니터링하고 보호하는 각 범위 내 리소스에 대해 비용을 지불합니다. AWS WAF 및 AWS Shield Advanced와 같이 배포하는 기본 보안 서비스에 추가 요금이 적용됩니다. 자세한 요금 정보는 AWS 웹 사이트의 [AWS Network Security Manager 요금](#)을 참조하세요.

를 처음 사용하십니까?

AWS Network Security Manager를 처음 사용하는 경우 다음 주제를 순서대로 읽는 것이 좋습니다.

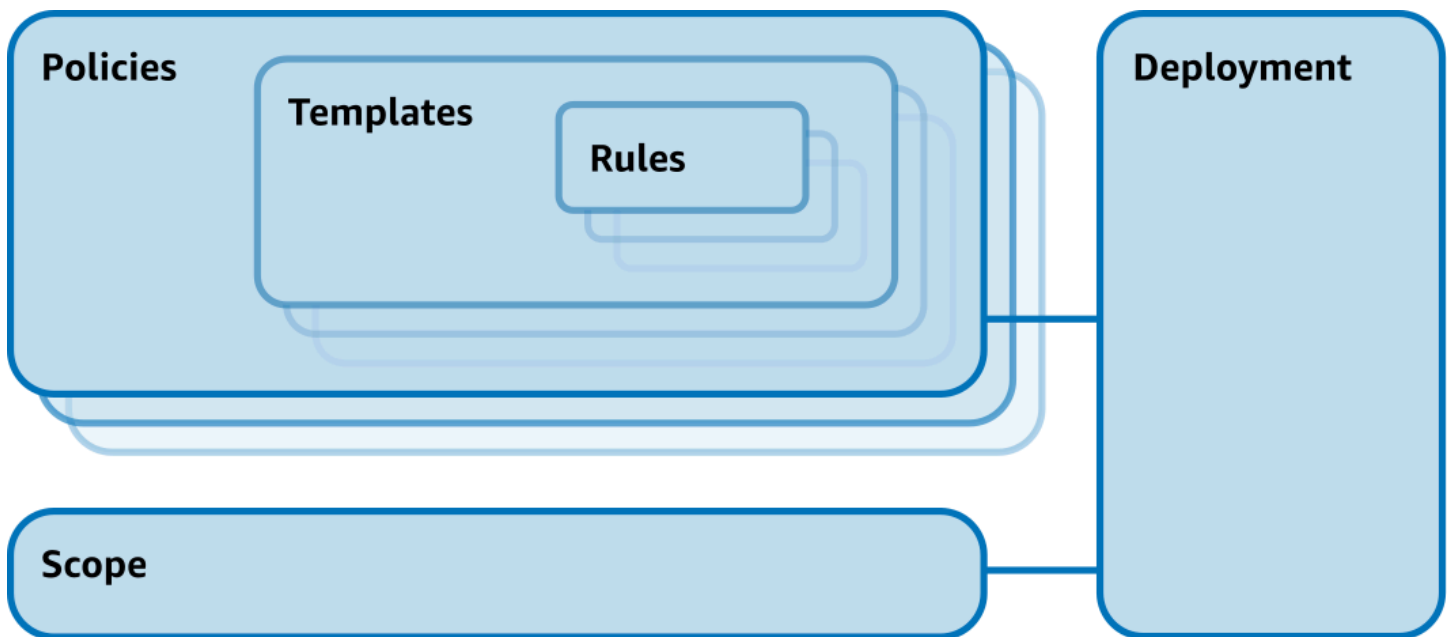
1. [AWS Network Security Manager 작동 방식](#) - 리소스 모델, 수명 주기 상태, 정책 병합 및 동기화에 대해 알아봅니다.
2. [AWS Network Security Manager 설정](#) - AWS Network Security Manager를 사용하기 위한 사전 조건을 완료합니다.
3. [자습서: 첫 번째 네트워크 보안 보호 배포](#) - 첫 번째 배포를 생성하는 end-to-end 자습서를 살펴봅니다.

AWS Network Security Manager 작동 방식

AWS Network Security Manager 리소스 모델을 사용하여 단일 계정 또는 조직의 여러 계정에 있는 리소스에 대한 네트워크 보안 보호를 설계하고 관리합니다. 이 장에서는 다섯 가지 리소스 유형, 계층 구조를 구성하는 방법, 해당 동작을 관리하는 주요 개념을 설명합니다.

AWS Network Security Manager 리소스 모델

AWS Network Security Manager는 구성 계층 구조에 배열된 5가지 리소스 유형을 사용합니다.



리소스는 계층 구조를 통해 서로 위쪽으로 참조합니다. 규칙은 템플릿 및 정책 내에서 사용됩니다. 템플릿, 규칙 또는 둘 다 정책 내에서 사용됩니다. 범위는 정책이 배포 내에서 보호하는 리소스를 참조합니다.

다음 섹션에서는 계층 구조의 각 리소스 유형에 대해 설명합니다.

규칙 - 네트워크 보안 구성의 원자 단위입니다. 규칙에는 트래픽 검사 규칙과 방화벽 구성 규칙이라는 두 가지 유형이 있습니다. 트래픽 검사는 보안 서비스가 트래픽을 처리하는 방법에 중점을 둡니다. 구성 규칙은 트래픽 검사 외부의 시스템 작업을 지정합니다. 규칙의 구조는 방화벽 유형에 따라 다릅니다.

템플릿 - 단일 방화벽 유형에 대한 순서가 지정되고 재사용 가능한 규칙 그룹입니다. 템플릿을 사용하여 관련 규칙을 함께 패키징하고 여러 정책에서 공유할 수 있습니다. 템플릿은 선택 사항입니다.

정책 - 순서가 지정된 템플릿 및 규칙 집합을 방화벽 유형에 대한 적용 설정과 결합합니다. 각 정책에는 우선 순위가 있습니다(숫자가 작을수록 우선 순위가 높음을 나타냄). 여러 정책이 동일한 리소스를 보호하는 경우 우선 순위에 따라 충돌 해결 방법이 결정됩니다. 트래픽 검사 규칙의 경우 우선 순위에 따라 규칙이 집계되는 순서가 결정됩니다. 방화벽 구성 규칙의 경우 우선 순위에 따라 각 리소스에 적용되는 구성과 범위 내 정책이 결정됩니다.

범위 - 보호가 적용되는 선언적 선택입니다. 범위는 보호할 리소스 유형을 지정하며 선택적으로 태그 또는 구성 속성을 기준으로 리소스를 필터링할 수 있습니다. 다중 계정 모드에서 범위는 포함하거나 제외할 계정 또는 OUs도 지정합니다. 단일 계정 모드에서 범위는 계정 자체에 적용됩니다. 범위 모드는 생성할 때 수정됩니다. 한 방향으로만 다중 계정 모드와 단일 계정 모드 간에 범위를 전환할 수 없으므로 다중 계정 범위는 절대 단일 계정 범위가 될 수 없으며 반대의 경우도 될 수 없습니다.

배포 - 하나 이상의 정책을 범위에 바인딩합니다. 배포를 게시하면 적용이 활성화됩니다. AWS Network Security Manager는 범위의 리소스를 검색하고, 의도한 구성을 계산하고, 선택적으로 out-of-sync 리소스를 수정합니다.

리소스 구성 제한은 섹션을 참조하세요 [할당량](#).

AWS Network Security Manager 리소스 수명 주기, 병합 및 동기화

다음 섹션에서는 AWS Network Security Manager 리소스를 생성한 후 리소스가 작동하는 방식을 제어하는 동작과 메커니즘을 설명합니다.

초안 및 활성 수명 주기

규칙, 템플릿, 정책, 범위 및 배포를 포함한 모든 AWS Network Security Manager 리소스의 상태는 초안 또는 활성입니다.

- **활성** - 기본 상태입니다. 리소스가 게시되어 사용할 수 있습니다. 다른 리소스는 이를 참조할 수 있으며, 이를 포함하는 배포는 구성을 적용합니다.
- **초안** - 리소스가 저장되었지만 아직 활성화되지 않았습니다. 초안 리소스는 적용되지 않으며 다른 리소스에서 참조할 수 없습니다. 리소스를 생성하거나 업데이트할 때 초안 저장을 선택하여 초안 상태를 유지합니다.

기본적으로 AWS Network Security Manager는 리소스를 활성으로 생성합니다. API를 사용하여 리소스를 초안으로 생성하려면 생성 또는 업데이트 작업 `false`에서 `isPublished` 파라미터를 `로` 설정합니다.

리소스를 업데이트할 때 다음 시나리오가 적용됩니다.

현재 상태	작업	결과
Draft	초안 저장을 선택합니다.	초안 업데이트(초안으로 유지)
Draft	게시 선택	초안 게시(활성 상태가 됨)
활성	게시 선택	업데이트 및 활성 상태 유지(활성)
활성	초안 저장을 선택합니다.	초안 오버레이 생성(아래에 활성 리소스가 있는 초안이 됨)

hasPublishedVersion 필드가 목록에 나타나고 응답을 가져옵니다. 이 필드는 게시된 활성 리소스가 초안 아래에 존재하는지 여부를 알려줍니다. 리소스의 초안 상태가 및 이면 hasPublishedVersion: true보류 중인 초안이 게시된 라이브 활성 리소스 위에 배치됩니다.

다른 활성 리소스가 참조하는 활성 리소스는 삭제할 수 없습니다.

버전 관리

규칙, 템플릿, 정책, 범위 및 배포를 포함한 모든 AWS Network Security Manager 리소스의 버전을 지정할 수 있습니다. 활성 리소스의 버전을 생성하려면 리소스를 선택하고 작업을 선택한 다음 버전이 지정된 스냅샷 생성을 선택합니다. 업데이트 시마다 버전이 자동으로 생성되는 것은 아닙니다.

AWS CLI 대체

활성 리소스에서 Create{Resource}Snapshot API 작업을 사용하여 버전을 생성할 수도 있습니다.

키 버전 속성:

- 각 버전에는 고유한 숫자(순차 정수)와 버전 검증 ARN(예:)이 있습니다arn:aws:network-security-manager:us-east-1:123456789012:rule:abc123:3.
- 버전은 변경할 수 없습니다. 업데이트할 수 없습니다.
- 리소스당 최대 10개의 버전을 생성할 수 있습니다.

- 버전에는 태그를 지정할 수 있습니다.

버전을 사용하여 원하는 구성 변형을 보존합니다. 리소스를 롤백하려면 버전을 읽은 다음 라이브 리소스를 버전에서 원하는 구성으로 업데이트합니다.

우선순위 기반 정책 병합

여러 정책이 동일한 리소스를 보호하면 AWS Network Security Manager는 구성을 단일 결과로 병합합니다. 우선 순위 번호가 낮을수록 우선 순위가 높음을 나타냅니다(우선 순위 1이 우선 순위 2보다 우선 함). AWS Network Security Manager가 트래픽 검사 규칙이 포함된 정책을 병합하면 우선 순위에 따라 규칙이 집계되는 순서가 결정됩니다. 방화벽 구성 규칙의 경우 우선 순위가 더 높은 정책에 따라 적용되는 구성이 결정됩니다.

AWS Network Security Manager는 다음 순서에 따라 두 수준에서 우선 순위를 평가합니다.

1. 관리자 우선 순위 - AWS Network Security Manager는 관리자 우선 순위를 먼저 평가합니다. 예 설명된 대로 각 조직 관리자에게 우선 순위가 할당됩니다 [the section called “관리자 및 멤버 계정”](#). AWS Network Security Manager는 정책을 병합할 때 멤버 계정의 자체 단일 계정 정책보다 높은 관리자 정책의 순위를 매깁니다. 관리자 정책과 멤버 계정의 단일 계정 정책이 모두 리소스에 적용되고 충돌하는 경우 관리자 정책의 구성이 성공합니다. 멤버 계정은 관리자 정책을 옵트아웃, 재정의 또는 제외할 수 없습니다.
2. 정책 우선 순위 - 각 계정 내에서 AWS Network Security Manager는 정책 우선 순위를 사용하여 나머지 충돌을 해결합니다. 정책 우선 순위 값은 1부터 시작하는 정수이며 계정별로 고유해야 합니다.

PutAdminAccount 작업의 필수 priority 필드인 1~10의 정수로 관리자 우선 순위를 설정합니다. 우선 순위 값은 고유하므로 두 관리자가 우선 순위를 공유하지 않으며 타이 브레이크가 필요하지 않습니다. 자세한 내용은 [AWS Network Security Manager API 참조](#)를 참조하세요.

리소스에 적용 가능한 모든 정책의 병합 결과는 효과적인 방화벽 구성입니다. AWS Network Security Manager는 이 구성을 계산하여 리소스의 실제 구성과 비교하고 모든 차이를 동기화 상태로 보고합니다.

정책이 충돌하면 AWS Network Security Manager는 각 속성을 비교하고 우선 순위가 높은 정책의 값을 적용합니다. 우선 순위가 높은 정책이 속성을 정의하지 않으면 우선 순위가 낮은 정책 값이 적용됩니다. 유효 구성과 일치하는 리소스는 IN_SYNC입니다. 우선 순위가 낮은 정책으로 보호되는 리소스로, 우선 순위가 높은 정책에서 설정이 우선 순위가 낮은 배포에 대해 OUT_OF_SYNC로 재정의됩니다. 이는 장애가 아닌 예상되는 동작입니다.

AWS Config를 사용한 리소스 검색

AWS Network Security Manager는 서비스 연결 AWS Config 구성 레코더를 사용하여 계정에서 보호된 리소스를 검색합니다. 이 레코더는 해당 계정이 배포 범위에 들어갈 때 각 계정에 자동으로 생성됩니다. AWS Firewall Manager와 달리 추가 설정을 수행할 필요가 없습니다. AWS Network Security Manager의 AWS 구성 사용은 AWS Network Security Manager 고객에게 청구되지 않습니다.

서비스 연결 레코더의 주요 특성:

- 이 역할은 `AWSConfigurationRecorderForNetworkSecurityManager`로 명명됩니다.
- 계정의 고객 관리형 구성 레코더와는 별개입니다.
- 활성 범위 및 배포와 관련된 리소스 유형만 기록합니다.
- AWS Config를 설정하거나 구성 레코더를 생성할 필요가 없습니다. AWS Network Security Manager는 이를 자동으로 관리합니다. AWS Network Security Manager의 AWS 구성 사용은 고객에게 청구되지 않습니다.
- 레코더가 사용 중인 동안에는 레코더를 수정하거나 삭제할 수 없습니다. AWS Network Security Manager는 수명 주기를 자동으로 관리합니다.

AWS Network Security Manager가 작동하려면 AWS Config를 수동으로 활성화하거나 구성할 필요가 없습니다. 이 서비스는 배포를 게시한 후 리소스 검색을 자동으로 처리합니다.

동기화 및 문제 해결

AWS Network Security Manager의 적용은 비동기식이며 최종적으로 일관됩니다. 배포를 게시한 후 또는 리소스가 변경되면 다음 단계가 발생합니다.

1. 리소스 검색 - AWS Network Security Manager는 서비스 연결 AWS Config 레코더를 사용하여 범위 내 리소스를 검색합니다.
2. 구성 계산 - 검색된 각 리소스에 대해 AWS Network Security Manager는 우선 순위별로 적용 가능한 모든 정책을 병합하여 효과적인 방화벽 구성을 계산합니다.
3. 동기화 평가 - AWS Network Security Manager는 유효 구성을 리소스의 실제 구성과 비교하고 동기화 상태를 기록합니다.
4. 문제 해결(선택 사항) - 정책에 `remediationEnabled`를 설정한 경우 AWS Network Security Manager는 out-of-sync 리소스를 수정합니다.

각 단계는 비동기식입니다. 워크플로의 결과:

- 배포 게시와 리소스 보호 사이에는 지연이 있습니다.
- 범위에 새 리소스를 생성하는 것과 보호되는 사이에 지연이 있습니다.
- 동기화 상태 항목의 Last Checked 타임스탬프는 AWS Network Security Manager가 리소스를 마지막으로 평가한 시기를 알려줍니다.

문제 해결 및 리소스 정리는 정책 수준 설정입니다. `policyConfiguration` 객체의 정책당 각각을 구성합니다.

`remediationEnabled`

AWS Network Security Manager가 규정 미준수 리소스를 자동으로 수정할지 여부를 지정합니다. 이 설정을 활성화하면 AWS Network Security Manager는 효과적인 구성과 일치하도록 out-of-sync 리소스를 수정합니다.

`resourcesCleanUp`

AWS Network Security Manager가 더 이상 필요하지 않을 때 생성한 리소스를 자동으로 제거할지 여부를 지정합니다. AWS Network Security Manager는 배포를 제거할 때 또는 계정 또는 리소스가 범위를 벗어날 때 생성한 방화벽을 삭제합니다.

`remediationEnabled` 및 `resourcesCleanUp` 설정 모두 기본값은 `false`입니다. AWS Network Security Manager는 이러한 설정을 활성화할 때까지 리소스를 수정하거나 정리하지 않습니다. `policyConfiguration` 객체에는 AWS WAF 정책에 `wafConfig` 적용되는 도 들어 있습니다. 자세한 내용은 [AWS Network Security Manager API](#) 참조를 참조하세요.

리소스가 동기화되지 않은 경우 동기화 상태에는 실제 값과 비교하여 예상 값을 표시하는 설정별 세부 정보가 포함된 out-of-sync 이유가 포함됩니다. 이유는 다음과 같은 범주로 구성됩니다.

- `missingFirewall` - 리소스와 연결된 방화벽 보호가 없습니다.
- `invalidFirewall` - 방화벽이 존재하지만 해당 구성이 유효 구성과 다릅니다. 여기에는 , `incorrectSingleValueConfigurations`, `missingAppendableConfigurationValues`, `unexpectedAppendableConfigurationValues` 및의 6가지 세부 버킷 `incorrectAppendableConfigurationOrder` `missingMergeableConfigurationValues`이 포함됩니다 `unexpectedMergeableConfigurationValues`.

문제 해결이 활성화되었지만 AWS Network Security Manager가 리소스를 수정할 수 없는 경우 `remediationIssues` 필드는 , 문제를 `issueType` message 설명하는 및 문제 해결 방법을 `correctiveAction` 제안하는를 제공합니다.

AWS Network Security Manager는 관리하지 않는 설정을 평가하지 않습니다. 필드가 기여 규칙에 표시되지 않으면 AWS Network Security Manager는 동기화 평가 중에 필드를 무시합니다.

관리자 및 멤버 계정

AWS Network Security Manager는 AWS Organizations를 기반으로 구축된 교차 계정 관리 모델을 사용합니다.

- 관리자 계정 - AWS Network Security Manager 리소스(규칙, 템플릿, 정책, 범위 및 배포)를 생성하고 관리하는 계정입니다. 관리자 계정을 하나 이상 지정합니다. 각 계정의 우선 순위는 1~10입니다.
- 멤버 계정 - AWS Network Security Manager가 리소스를 검색하고, 동기화 상태를 평가하고, 선택적으로 out-of-sync 구성을 수정하는 계정입니다. AWS Network Security Manager는 서비스 연결 역할을 통해 멤버 계정에서 작동합니다. 자세한 내용은 [the section called “서비스 연결 역할”](#) 섹션을 참조하세요.

필요에 따라 각 관리자의 범위를 계정, OUs 및 방화벽 유형의 하위 집합으로 지정할 수 있습니다. 이 기능을 사용하여 특정 영역의 관리를 다른 팀에 위임합니다.

AWS Network Security Manager는 리전 서비스입니다. 리전 간 종속성 없이 리전당 리소스 및 배포를 생성합니다.

서비스 연결 역할

AWS Network Security Manager는 라는 IAM 서비스 연결 역할을

AWSServiceRoleForNetworkSecurityManager 사용하여 사용자를 대신하여 조직의 멤버 계정에서 작업합니다. 이 역할은 `network-security-manager.amazonaws.com` 서비스 보안 주체를 신뢰합니다. NetworkSecurityManagerServiceRolePolicy AWS 관리형 정책을 사용합니다.

AWS Network Security Manager는 서비스를 활성화할 때 이 역할을 자동으로 생성하므로 수동 설정이 없습니다. 이 역할을 통해 AWS Network Security Manager는 AWS WAF 및 AWS Shield Advanced 보호를 관리하고, AWS Config를 통해 보호된 리소스를 검색하고, 교차 계정 작업을 수행할 수 있습니다. 자세한 내용은 [the section called “서비스 연결 역할”](#) 섹션을 참조하세요.

AWS Network Security Manager 설정

AWS Network Security Manager를 사용하면 두 가지 조직 모델에서 작업할 수 있습니다. 단일 계정에서 직접 사용하거나 AWS Organizations와 함께 사용하여 여러 계정에서 보호를 관리합니다. 설정 단계는 선택한 모델에 따라 다릅니다.

주제

- [조직 모델 선택](#)
- [단일 계정 사용을 위한 설정](#)
- [AWS Organizations에서 다중 계정 사용을 위한 설정](#)
- [AWS Network Security Manager 관리자 계정 생성](#)
- [AWS Network Security Manager 권한을 사용하여 IAM 자격 증명 생성](#)
- [기본적으로 비활성화된 리전에서 AWS Network Security Manager 사용](#)

조직 모델 선택

다음 조직 모델 중에서 선택합니다.

- 단일 계정 - AWS Network Security Manager를 사용하여 한 계정의 리소스를 보호합니다. AWS Organizations 또는 관리자 계정은 필요하지 않습니다. AWS Network Security Manager 권한으로 IAM 자격 증명을 생성하고 서비스를 직접 사용하기 시작합니다. AWS Network Security Manager는 계정에 서비스 연결 역할을 자동으로 생성합니다.
- 다중 계정 - Organizations와 함께 AWS Network Security Manager를 사용하여 여러 계정의 리소스를 보호합니다. 이 모드에서는 AWS Organizations를 설정하고, 신뢰할 수 있는 액세스를 활성화하고, 관리자 계정을 생성해야 합니다.

단일 계정 사용을 위한 설정

단일 계정에서 AWS Network Security Manager를 사용하려면 적절한 권한을 가진 IAM 자격 증명을 생성하고 서비스를 직접 사용하기 시작합니다. 관리자 계정을 생성할 필요가 없습니다. AWS Network Security Manager는 백그라운드에서 계정에 서비스 연결 역할을 자동으로 생성합니다. [the section called “AWS Network Security Manager 권한을 사용하여 IAM 자격 증명 생성”](#)로 이동하세요.

AWS Organizations에서 다중 계정 사용을 위한 설정

여러 계정에서 보호를 관리하려면 필요한 AWS Organizations 멤버십 및 구성을 설정합니다.

1. 조직의 AWS Network Security Manager 관리자로 사용할 계정 선택 - Network AWS Security Manager 리소스를 생성하고 관리하는 계정입니다.
2. 조직 멤버십 확인 - 선택한 계정이 아직 조직의 멤버가 아닌 경우 가입하도록 합니다. AWS Organizations 사용 설명서의 [계정에 가입 AWS 초대](#)의 지침을 따르세요.
3. 조직의 모든 기능 활성화 - AWS Organizations에는 통합 결제 기능과 모든 기능의 두 가지 기능 세트가 있습니다. AWS Network Security Manager를 사용하려면 모든 기능에 대해 조직을 활성화해야 합니다. 조직이 통합 결제용으로만 구성된 경우 조직 사용 설명서의 [조직 내 모든 기능 활성화](#)의 지침을 따르세요. AWS
4. AWS Network Security Manager에 대한 신뢰할 수 있는 액세스 활성화 - AWS Organizations에서 AWS Network Security Manager에 대한 신뢰할 수 있는 액세스를 활성화합니다. 신뢰할 수 있는 액세스를 활성화하면 AWS Network Security Manager가 멤버 계정에서 서비스 연결 역할을 생성하고 대신 리소스를 관리할 수 있습니다.
5. 위임된 관리자 계정 등록 - 선택한 계정을 AWS Organizations의 AWS Network Security Manager에 대한 위임된 관리자로 등록합니다. Organizations 관리 계정을 사용하여이 단계를 완료합니다.

신뢰할 수 있는 액세스를 끌 때 다중 계정 보호 비활성화

AWS Organizations에서 AWS Network Security Manager에 대한 신뢰할 수 있는 액세스를 끄거나 위임된 관리자 계정의 등록을 취소하는 경우 AWS Network Security Manager는 다중 계정 범위 및 배포를 DISABLED 상태로 설정하고 관리하는 보호를 정리합니다.

AWS Network Security Manager 관리자 계정 생성

이 단계는 다중 계정 모드에만 적용됩니다. 조직의 관리 계정만 AWS Network Security Manager 관리자 계정을 생성할 수 있습니다.

Organizations 설정을 완료한 후 계정을 AWS Network Security Manager 관리자로 등록합니다. 콘솔 또는 AWS 명령줄 인터페이스(AWS CLI)에서이 작업을 수행할 수 있습니다.

관리자 계정을 생성하면 AWS Network Security Manager는 조직의 모든 계정에 서비스 연결 역할을 자동으로 생성합니다. 이 역할을 사용하면 AWS Network Security Manager가 리소스를 검색하고 멤버 계정의 보호를 관리합니다.

AWS Network Security Manager를 사용하면 조직의 방화벽 리소스를 관리하는 여러 관리자가 있을 수 있습니다. 조직에서 여러 관리자를 사용하려는 경우 각 관리자에게 관리 범위 조건을 적용하여 관리할 수 있는 리소스를 정의할 수 있습니다. 이렇게 하면 조직 내에서 다양한 관리자 역할을 가질 수 있는 유연성과 최소 권한 액세스 원칙을 유지할 수 있습니다. 예를 들어 한 관리자가 조직 단위(OU), 다른 관리자는 특정 정책 유형만 관리할 수 있습니다.

조직당 지정할 수 있는 관리자의 최대수는 [할당량](#)을 참조하세요.

리전 등록

단일 AWS 리전에 AWS Network Security Manager 관리자 계정을 등록합니다. 추가 리전에서 AWS Network Security Manager를 사용하려면 각 리전에서이 단계를 반복합니다.

콘솔을 사용하여 관리자 계정을 생성하려면

1. <https://console.aws.amazon.com/network-security-manager/> AWS Network Security Manager 콘솔을 엽니다.
2. 탐색 창에서 설정을 선택합니다.
3. 관리자 추가를 선택합니다.
4. 계정을 선택하고 우선 순위 값(1~10)을 입력합니다.
5. 관리자 추가를 선택하여 확인합니다.

AWS CLI를 사용하여 관리자 계정을 생성하려면

PutAdminAccount 작업을 직접적으로 호출합니다. 우선 순위 값(1~10)을 제공해야 합니다.

다음 AWS CLI 예제에서는 우선 순위가 1인 AWS Network Security Manager 관리자로 계정을 등록합니다.

```
aws network-security-manager put-admin-account \  
  --account-id 123456789012 \  
  --priority 1
```

각각 우선순위가 다른 여러 관리자 계정을 지정할 수 있습니다. 선택적으로 adminScope 파라미터를 제공하여 각 관리자를 특정 계정, OUs 또는 방화벽 유형으로 제한할 수 있습니다.

콘솔을 사용하여 관리자 계정을 제거하려면

⚠ 관리자 제거 시 다중 계정 보호 비활성화

관리자 계정을 제거하면 AWS Network Security Manager는 다중 계정 범위 및 배포를 DISABLED 상태로 설정하고 관리하는 보호를 정리합니다.

1. <https://console.aws.amazon.com/network-security-manager/> AWS Network Security Manager 콘솔을 엽니다.
2. 탐색 창에서 설정을 선택합니다.
3. 제거할 관리자 계정을 선택합니다.
4. Remove administrator(관리자 제거)를 선택합니다.
5. 확인하려면 관리자 삭제 확인을 선택합니다.

AWS Network Security Manager 권한을 사용하여 IAM 자격 증명 생성

AWS Network Security Manager를 사용하려면 AWS Network Security Manager 작업을 호출할 권한이 있는 IAM 자격 증명(사용자 또는 역할)이 필요합니다. IAM 작업은 접두사를 사용합니다network-security-manager.

다음 예제 IAM 정책에는 세 개의 문이 포함되어 있습니다. 첫 번째 문은 모든 AWS Network Security Manager 작업에 대한 전체 액세스 권한을 부여합니다. 두 번째 문은 AWS Network Security Manager에 필요한 추가 AWS Organizations 및 AWS WAF 권한을 부여합니다. AWS Network Security Manager는 이러한 권한을 사용하여 조직의 계정 및 조직 단위(OU)를 식별하고 사용 가능한 WAF 규칙 그룹 및 관리형 제품을 나열합니다. 또한 이러한 권한을 통해 AWS Network Security Manager는 신뢰할 수 있는 액세스를 활성화하고 Organizations에 AWS 위임된 관리자를 등록할 수 있습니다. 세 번째 문은 AWS Network Security Manager가 단일 계정 및 다중 계정 사용 모두에 필요한 서비스 연결 역할을 생성하는 데 필요한 iam:CreateServiceLinkedRole 권한을 부여합니다.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
```

```

        "Effect": "Allow",
        "Action": "network-security-manager:*",
        "Resource": "*"
    },
    {
        "Effect": "Allow",
        "Action": [
            "organizations:DescribeOrganization",
            "organizations:ListAccounts",
            "organizations:ListRoots",
            "organizations:ListOrganizationalUnitsForParent",
            "organizations:ListAccountsForParent",
            "organizations:EnableAWSServiceAccess",
            "organizations:RegisterDelegatedAdministrator",
            "wafv2:ListRuleGroups",
            "wafv2:ListAvailableManagedRuleGroups",
            "wafv2:DescribeAllManagedProducts"
        ],
        "Resource": "*"
    },
    {
        "Effect": "Allow",
        "Action": "iam:CreateServiceLinkedRole",
        "Resource": "*"
    }
]
}

```

프로덕션 용도로는 필요한 최소 권한만 부여하는 것이 좋습니다. 자세한 내용은 [the section called “ID 및 액세스 관리”](#) 섹션을 참조하세요.

에 가입 AWS 계정

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

기본적으로 비활성화된 리전에서 AWS Network Security Manager 사용

기본적으로 비활성화된 리전에서 AWS Network Security Manager를 사용하려면 조직의 관리 계정과 AWS Network Security Manager 관리자 계정 모두에 대해 리전을 활성화해야 합니다. 기본적으로 비

활성화된 리전과 이를 활성화하는 방법에 대한 자세한 내용은 일반 참조의 [AWS 리전 관리](#)를 참조하세요. AWS

비활성화된 리전을 활성화하려면

Organizations 관리 계정과 AWS Network Security Manager 관리자 계정 모두에 대해 AWS 일반 참조의 [리전 활성화](#) 지침을 따릅니다.

첫 번째 네트워크 보안 보호 배포

이 자습서에서는 AWS Network Security Manager 콘솔을 사용하여 AWS WAF 웹 ACL을 배포하는 방법을 안내합니다. 다음 단계를 완료합니다.

1. 규칙 생성
2. 템플릿 생성
3. 정책 생성
4. 범위 생성
5. 배포 생성 및 게시
6. 동기화 상태 모니터링

이 자습서에서는 선택한 계정에서 Application Load Balancer를 보호하는 AWS WAF 웹 ACL을 생성합니다. 이 프로세스는 AWS Network Security Manager에서 지원하는 모든 보안 서비스 및 방화벽에 대해 거의 동일합니다.

완료 시간: 약 10분

비용: 이 자습서에서는 요금이 발생할 수 있는 AWS 서비스를 사용합니다. 현재 요금은 AWS 웹 사이트의 [AWS Network Security Manager 요금](#)을 참조하세요.

사전 조건

시작하기 전에 다음 요구 사항을 충족하는지 확인합니다.

- 에 설명된 대로 설정 단계를 완료했습니다 [AWS Network Security Manager 설정](#).
- AWS Network Security Manager 권한이 있는 AWS Identity and Access Management(IAM) 자격 증명입니다.
- 모든 기능이 활성화된 AWS Organizations 조직 및 지정된 AWS Network Security Manager 관리자 계정(다중 계정 배포에 필요).
- AWS Network Security Manager 콘솔에 대한 액세스.

1단계: 규칙 생성

규칙은 보안 구성의 구성 요소입니다. 이 단계에서는 두 개의 AWS WAF 규칙을 생성합니다. 하나는 기본 작업을 설정하고 다른 하나는 가시성 구성을 설정합니다. 기본 작업 및 VisibilityConfig는 AWS WAF 웹 ACL의 필수 필드입니다.

기본 작업 규칙을 생성하려면 다음 단계를 따릅니다.

1. <https://console.aws.amazon.com/network-security-manager/> AWS Network Security Manager 콘솔을 엽니다.
2. 탐색 창에서 개요를 선택합니다.
3. 개요 페이지에서 규칙 생성을 선택합니다.
4. 규칙 이름에와 같이 설명이 포함된 이름을 입력합니다my-default-action-rule.
5. 규칙 정의 섹션의 방화벽 유형에서 AWS WAF를 선택합니다.
6. 규칙 유형 선택에서 구성을 선택합니다.
7. 구성 유형 삽입을 선택한 다음 기본 작업을 선택합니다. JSON 편집기가 기본 구성과 함께 나타납니다.
8. JSON 편집기에서 Block 섹션을 제거하고 Allow 섹션만 유지합니다.
9. 규칙 생성을 선택합니다.

VisibilityConfig 규칙을 생성하려면 다음 단계를 따릅니다.

1. 탐색 창에서 개요를 선택합니다.
2. 개요 페이지에서 규칙 생성을 선택합니다.
3. 규칙 이름에와 같이 설명이 포함된 이름을 입력합니다my-visibility-config-rule.
4. 규칙 정의 섹션의 방화벽 유형에서 AWS WAF를 선택합니다.
5. 규칙 유형 선택에서 구성을 선택합니다.
6. 구성 유형 삽입을 선택한 다음 VisibilityConfig를 선택합니다. JSON 편집기가 기본 구성과 함께 나타납니다.
7. 규칙 생성을 선택합니다.

AWS CLI 대체

AWS CLI를 사용하여 규칙을 생성할 수도 있습니다.

```
aws network-security-manager create-rule \  
  --rule-name "my-default-action-rule" \  
  --firewall-type WAF \  
  --rule-type CONFIGURATION \  
  --configuration '{"DefaultAction": {"Allow": {}}}' \  
  --is-published true  
  
aws network-security-manager create-rule \  
  --rule-name "my-visibility-config-rule" \  
  --firewall-type WAF \  
  --rule-type CONFIGURATION \  
  --configuration '{"VisibilityConfig": {"SampledRequestsEnabled": true, \  
    "CloudWatchMetricsEnabled": true, "MetricName": "my-web-acl-metric"}}' \  
  --is-published true
```

2단계: 템플릿 생성

템플릿은 정책 간에 재사용할 규칙을 하나 이상 그룹화합니다. 이 단계에서는 1단계의 규칙을 포함하는 템플릿을 생성합니다.

1. 탐색 창에서 개요를 선택합니다.
2. 개요 페이지에서 템플릿 생성을 선택합니다.
3. 템플릿 이름에와 같이 설명이 포함된 이름을 입력합니다my-waf-template.
4. 방화벽 유형에서 AWS WAF를 선택합니다.
5. 규칙 섹션에서 규칙 추가를 선택하고 1단계에서 생성한 규칙을 선택합니다.
6. 템플릿 생성을 선택합니다.

AWS CLI 대체

AWS CLI를 사용하여 템플릿을 생성할 수도 있습니다.

```
aws network-security-manager create-template \  
  --template-name "my-waf-template" \  
  --firewall-type WAF \  
  --associated-rule-list '["ruleIdentifier": "rule-arn-from-step-1"]' \  
  --is-published true
```

```
--is-published true
```

3단계: 정책 생성

정책은 템플릿과 적용 설정을 결합합니다. 이 단계에서는 템플릿을 참조하고 자동 수정을 활성화하는 정책을 생성합니다.

1. 탐색 창에서 개요를 선택합니다.
2. 개요 페이지에서 정책 생성을 선택합니다.
3. 정책 이름에 설명이 포함된 이름을 입력합니다(예: my-waf-policy).
4. 방화벽 유형에서 AWS WAF를 선택합니다.
5. 정책 우선 순위 섹션에 기존 정책과 해당 우선 순위가 표시됩니다. 새 정책의 우선 순위를 검토합니다. 조정해야 하는 경우 우선 순위 필드를 선택하고 값을 1 또는 사용하지 않는 우선 순위 번호로 변경합니다.
6. 템플릿 및 규칙 섹션에서 템플릿 추가를 선택하고 2단계에서 생성한 템플릿을 선택합니다.
7. 수정에서 활성화됨을 선택합니다.
8. 기존 고객 웹 ACL 확인에서 문제 해결 없음을 선택합니다.
9. 정책 생성을 선택합니다.

AWS CLI 대체

AWS CLI를 사용하여 정책을 생성할 수도 있습니다.

```
aws network-security-manager create-policy \  
  --policy-name "my-waf-policy" \  
  --firewall-type WAF \  
  --priority 1 \  
  --associated-template-and-rule-list '["templateIdentifier": "template-arn-  
from-step-2"]]' \  
  --policy-configuration '{"remediationEnabled": true, "resourcesCleanUp":  
false, "wafConfig": {"existingCustomerWebACLResolution": "NO_REMEDIATION"}}' \  
  --is-published true
```

4단계: 범위 생성

범위는 보호가 적용되는 위치를 정의합니다. 이 단계에서는 계정의 Application Load Balancer를 대상으로 하는 범위를 생성합니다.

1. 탐색 창에서 개요를 선택합니다.
2. 개요 페이지에서 범위 생성을 선택합니다.
3. 범위 이름에와 같이 설명이 포함된 이름을 입력합니다my-alb-scope.
4. (선택 사항) 계정 및 조직 단위 선택 섹션의 관리 범위 제어 방법 선택에서 전체 AWS 조직(모든 OUs 및 계정)으로 범위를 선택합니다. 단일 계정 배포의 경우이 단계를 건너뜁니다.
5. 리소스 섹션의 리소스 유형에서 Application Load Balancer를 선택합니다.
6. 범위 생성(Create scope)을 선택합니다.

AWS CLI 대체

AWS CLI를 사용하여 범위를 생성할 수도 있습니다.

```
aws network-security-manager create-scope \
  --scope-name "my-alb-scope" \
  --scope-configuration '{
    "accountFilter": {"includeAll": {}},
    "resourceScopes": {
      "AWS::ElasticLoadBalancingV2::LoadBalancer::application": {
        "includeAll": true
      }
    }
  }' \
  --is-published true
```

5단계: 배포 생성 및 게시

배포는 정책을 범위에 바인딩하고 적용을 활성화합니다. 배포를 생성하고 게시하려면:

1. 탐색 창에서 개요를 선택합니다.
2. 개요 페이지에서 배포 생성을 선택합니다.

3. 배포 이름에와 같이 설명이 포함된 이름을 입력합니다my-first-deployment.
4. 정책 섹션에서 정책 추가를 선택하고 3단계에서 생성한 정책을 선택합니다.
5. 범위 섹션에서 범위 추가를 선택하고 4단계에서 생성한 범위를 선택합니다.
6. 배포 만들기를 선택합니다.

AWS Network Security Manager는 리소스를 검색하고 보호를 적용하기 시작합니다. 이 프로세스는 비 동기식이며 완료하는 데 몇 분 정도 걸릴 수 있습니다.

AWS CLI 대체

AWS CLI를 사용하여 배포를 생성하고 게시할 수도 있습니다.

```
aws network-security-manager create-deployment \
  --deployment-name "my-first-deployment" \
  --associated-policy-list '["policyIdentifier": "policy-arn-from-step-3"]]' \
  \
  --associated-scope-list '["scopeIdentifier": "scope-arn-from-step-4"]]' \
  --deployment-configuration '{"enableCrossAccountVisibility": true}' \
  --is-published true
```

6단계: 동기화 상태 모니터링

배포를 게시한 후 AWS Network Security Manager는 리소스를 검색하고 해당 구성을 동기화합니다. 각 리소스의 상태를 모니터링하려면:

1. 탐색 창에서 개요를 선택합니다.
2. 배포 탭을 선택합니다.
3. 5단계에서 생성한 배포를 선택합니다.
4. 동기화 탭을 선택합니다.
5. 각 리소스의 동기화 상태를 검토합니다.
 - IN_SYNC - 리소스 구성이 의도한 보호 설정과 일치합니다.
 - OUT_OF_SYNC - 리소스 구성이 일치하지 않습니다. AWS Network Security Manager는 문제 해결이 활성화되면 이를 자동으로 해결합니다.
 - NOT_APPLICABLE - 리소스가 범위 내에 있지만이 배포로 평가할 수 없습니다.

i AWS CLI 대체

AWS CLI를 사용하여 동기화 상태를 확인할 수도 있습니다.

```
aws network-security-manager list-resource-synchronization-statuses \
  --deployment-identifier "deployment-arn-from-step-5"
```

7단계: 정리

생성한 리소스가 더 이상 필요하지 않은 경우 해당 리소스를 역순으로 삭제하여 적용을 중지하고 범위 내 리소스에서 보호를 제거합니다.

이러한 리소스는 서로를 참조하기 때문에 역순이 중요합니다. 리소스를 삭제하기 전에 리소스와 연결된 항목을 확인하려면 해당 리소스의 ARN을 ListResourceAssociations 사용하여 호출합니다. 연결된 각 리소스의 ARN 및 리소스 유형을 반환합니다. 자세한 내용은 [AWS Network Security Manager API](#) 참조를 참조하세요.

1. 탐색 창에서 개요를 선택합니다. 배포 탭을 선택합니다. 배포를 선택하고 작업을 선택한 다음 삭제를 선택합니다.
2. 범위 탭을 선택합니다. 범위를 선택하고 작업을 선택한 다음 삭제를 선택합니다.
3. 정책 탭을 선택합니다. 정책을 선택하고 작업을 선택한 다음 삭제를 선택합니다.
4. 템플릿 탭을 선택합니다. 템플릿을 선택하고 작업을 선택한 다음 삭제를 선택합니다.
5. [Rules] 탭을 선택합니다. 규칙을 선택하고 작업을 선택한 다음 삭제를 선택합니다.

i AWS CLI 대체

리소스를 삭제하기 전에 연결을 확인하여 삭제 순서를 계획합니다.

```
aws network-security-manager list-resource-associations \
  --resource-arn "resource-arn"
```

리소스에 여전히 연결이 있는 경우 먼저 연결된 리소스를 제거하거나 삭제합니다. AWS CLI를 사용하여 리소스를 역순으로 삭제할 수 있습니다.

```
aws network-security-manager delete-deployment \
  --deployment-identifier "deployment-arn"
```

```
aws network-security-manager delete-scope \  
  --scope-identifier "scope-arn"  
  
aws network-security-manager delete-policy \  
  --policy-identifier "policy-arn"  
  
aws network-security-manager delete-template \  
  --template-identifier "template-arn"  
  
aws network-security-manager delete-rule \  
  --rule-identifier "rule-arn"
```

다음 단계

이제 제대로 배포되었으므로 네트워크 보안 보호를 확장하는 다음 방법을 살펴보세요.

- 의 리소스 모델 및 수명 주기에 대해 알아보십시오 [AWS Network Security Manager 작동 방식](#).
- 초안/게시 워크플로를 사용하여 변경 사항이 적용되기 전에 스테이징합니다. 자세한 내용은 [the section called “초안 및 활성 수명 주기”](#) 섹션을 참조하세요.
- 스냅샷을 생성하여 잘 알려진 구성을 보존합니다. 자세한 내용은 [the section called “버전 관리”](#) 섹션을 참조하세요.
- GenerateRuleConfiguration를 사용하여 자연어 설명에서 규칙을 생성합니다. 자세한 내용은 [AWS Network Security Manager API 참조](#)를 참조하세요.
- 조직 전체에서 AWS WAF 및 AWS Shield Advanced 보호를 관리하는 방법을 알아보십시오. 자세한 내용은 [방화벽 및 보안 서비스 관리](#) 섹션을 참조하세요.

방화벽 및 보안 서비스 관리

AWS Network Security Manager를 사용하면 여러 방화벽 및 보안 서비스에 대한 보안 정책을 정의하고 배포할 수 있습니다. 공통 요소는 AWS 네트워크 보안 포트폴리오에 걸쳐 있지만 AWS Network Security Manager 내에서 해결해야 하는 중요한 변형이 있습니다.

지원되는 각 네트워크 보안 서비스에 대해 다음 하위 섹션에서는 빠른 생성 및 표준 세부 생성 프로세스의 고유한 요소와 단계를 설명합니다.

AWS WAF용 웹 ACLs 관리

AWS Network Security Manager를 사용하면 조직의 계정 및 리소스에 AWS WAF 웹 액세스 제어 목록(웹 ACLs) 중앙에서 구성하고 배포할 수 있습니다. AWS WAF에 대한 AWS Network Security Manager 규칙을 정의하고, 이를 보호 템플릿으로 그룹화하고, AWS Network Security Manager 정책 및 배포를 통해 대규모로 적용할 수 있습니다.

AWS WAF 개념

다음 개념은 AWS Network Security Manager를 AWS WAF와 함께 사용할 때에만 적용됩니다. AWS Network Security Manager의 작동 방식에 대한 자세한 내용은 섹션을 참조하세요 [AWS Network Security Manager 작동 방식](#).

AWS WAF 규칙 유형

AWS WAF의 경우 규칙은 다음 두 가지 유형 중 하나입니다.

- 검사 - PreProcessFirewallManagerRuleGroups (고객 정의 규칙보다 먼저 실행되는 규칙) 또는 PostProcessFirewallManagerRuleGroups (다음에 실행되는 규칙)을 사용하여 규칙 그룹 정의를 포함합니다.
- 구성 - 단일 웹 ACL 구성 설정을 포함합니다. 구성 JSON에는 지원되는 설정과 일치하는 최상위 키가 정확히 하나 포함되어야 합니다(예: , Description, DefaultActionVisibilityConfig, LoggingConfiguration, CaptchaConfig, , ChallengeConfig, CustomResponseBodies, DataProtectionConfigAssociationConfig, 또는 OnSourceDDoSProtectionConfig TokenDomainsMonetizationConfig).

대부분의 웹 ACL 구성 설정은 AWS WAF CreateWebACL 작업의 파라미터에 해당합니다. 이러한 설정 및 정의에 대한 자세한 내용은 WAF API 참조의 [CreateWebACL](#)을 참조하세요. AWS

예외는 별도로 LoggingConfiguration 구성하는 입니다. 자세한 내용은 [the section called “로깅”](#) 섹션을 참조하세요.

AWS WAF 정책 병합

AWS WAF의 경우 각 구성 설정은 다음 병합 전략 중 하나를 사용합니다.

SingleValue

값을 하나만 가질 수 있는 설정입니다. 우선 순위가 가장 높은 정책이 성공합니다. 우선 순위 값은 고유하므로 두 정책이 동일한 우선 순위에서 다른 값을 정의할 수 없습니다. AWS Network Security Manager의 우선 순위 해결 방법에 대한 자세한 내용은 섹션을 참조하세요 [the section called “우선순위 기반 정책 병합”](#). 다음 설정은 SingleValue를 사용합니다. DefaultAction, VisibilityConfig, CaptchaConfig, ChallengeConfig, OnSourceDDoSProtectionConfig, LoggingConfiguration, 및 MonetizationConfigDescription.

추가(및 AppendAndSort)

모든 정책의 항목은 우선 순위에 따라 목록에 추가됩니다. TokenDomains 및는 추가를 DataProtectionConfig.DataProtections 사용합니다. PreProcessFirewallManagerRuleGroups 및는 모든 정책의 규칙 그룹을 추가하고 우선 순위에 따라 정렬하는 AppendAndSort를 PostProcessFirewallManagerRuleGroups 사용합니다. AWS WAF는 규칙 그룹을 순차적으로 평가하기 때문에 순서가 중요합니다.

병합

모든 정책의 항목은 우선 순위에 관계없이 단일 세트로 병합됩니다. CustomResponseBodies 및는 병합을 AssociationConfig.RequestBody 사용합니다.

추가, AppendAndSort 및 병합 전략은 중복 항목을 제거합니다. 두 정책이 동일한 구성에 기여하면 AWS Network Security Manager는 우선 순위가 더 높은 정책에서 항목을 유지합니다. 따라서 유효 구성에는 기여 정책당 사본 하나가 아니라 해당 항목의 사본 하나가 포함됩니다.

기존 웹 ACL 해상도

AWS WAF 정책의 existingCustomerWebACLResolution 설정을 사용하여 AWS Network Security Manager가 고객 관리형 웹 ACL이 이미 있는 리소스를 처리하는 방법을 지정합니다.

- RETROFIT - 유효 구성에 맞게 기존 웹 ACL을 업데이트합니다.

- `OVERRIDE_ASSOCIATION` - AWS Network Security Manager에서 관리하는 웹 ACL을 대신 리소스와 연결합니다.
- `NO_REMEDIATION` - 웹 ACL이 있는 경우 수정하지 마십시오.

웹 ACL 트래픽 로깅

정책의 `LoggingConfiguration` 설정을 사용하여 웹 ACL 로깅을 제어합니다. AWS Network Security Manager는 AWS WAF `PutLoggingConfiguration` 작업을 사용하여이 설정을 적용합니다. 웹 ACL당 하나의 로깅 대상을 정의할 수 있습니다. 자세한 내용은 WAF API 참조의 [PutLoggingConfiguration](#)을 참조하세요. AWS

정책이 관리하는 모든 범위 내 웹 ACL은 정책이 지정하는 대상으로 로그를 보냅니다. 이를 통해 조직의 계정에 대한 중앙 집중식 로깅을 수행할 수 있습니다. 이를 사용하여 웹 ACLs 조직 전체에서 분석하는 트래픽에 대한 자세한 정보를 얻을 수 있습니다.

여러 계정에 대한 중앙 집중식 로깅의 경우 Amazon S3 버킷 또는 Amazon Data Firehose 전송 스트림으로 로그를 전송할 수 있습니다. 각 대상 유형에는 추가 구성이 필요하며, AWS Network Security Manager가 범위 내 리소스 및 계정에서 AWS WAF 로깅을 관리하기 전에 이를 완료해야 합니다. 대상 이름은 로 시작해야 합니다 `aws-waf-logs-`.

Amazon Data Firehose

다음과 같은 특성을 가진 전송 스트림을 생성합니다.

- AWS Network Security Manager 관리자 계정을 사용하여 생성됨
- 예를 들어 `aws-waf-logs-`로 시작하는 이름입니다. `aws-waf-logs-network-security-manager-central`
- PUT 소스
- 사용자가 운영하는 리전 또는 Amazon CloudFront에 대한 로그를 캡처하는 경우 미국 동부(버지니아 북부) 리전에서 생성됩니다.

전송 스트림을 사용하기 전에 테스트하여 조직의 로그에 대한 처리량이 충분한지 확인합니다. 자세한 내용은 [Amazon Data Firehose 개발자 안내서의 Amazon Data Firehose 전송 스트림 생성](#)을 참조하세요.

Amazon S3

AWS WAF 개발자 안내서의 Amazon S3 지침에 따라 버킷을 생성합니다. 또한 로그 전송이 버킷에 쓸 수 있도록 허용하는 권한으로 버킷을 구성해야 합니다. 다음 버킷 정책은 이러한 권한을 부여합니다.

```
{
  "Version": "2012-10-17",
  "Id": "AWSLogDeliveryForNetworkSecurityManager",
  "Statement": [
    {
      "Sid": "AWSLogDeliveryAclCheckNetworkSecurityManager",
      "Effect": "Allow",
      "Principal": {
        "Service": "delivery.logs.amazonaws.com"
      },
      "Action": "s3:GetBucketAcl",
      "Resource": "arn:aws:s3:::aws-waf-logs-bucket-suffix"
    },
    {
      "Sid": "AWSLogDeliveryWriteNetworkSecurityManager",
      "Effect": "Allow",
      "Principal": {
        "Service": "delivery.logs.amazonaws.com"
      },
      "Action": "s3:PutObject",
      "Resource": "arn:aws:s3:::aws-waf-logs-bucket-suffix/policy-id/AWSLogs/*",
      "Condition": {
        "StringEquals": {
          "s3:x-amz-acl": "bucket-owner-full-control"
        }
      }
    }
  ]
}
```

*bucket-suffix*를 자체 버킷 이름 접미사로 바꾸고 *policy-id*를 정책 ID로 바꿉니다.

 CloudWatch Logs는 단일 계정 사용만 지원합니다.

여러 계정에서 AWS Network Security Manager를 사용하는 경우 Amazon CloudWatch Logs 로그 그룹을 로깅 대상으로 사용할 수 없습니다. 로그 그룹은 웹 ACL과 동일한 AWS 계정 및 동일한 리전에 있어야 합니다. 다중 계정 배포의 경우 Amazon S3 버킷 또는 Amazon Data Firehose 전송 스트림을 대신 사용합니다.

AWS WAF용 빠른 생성

빠른 생성을 사용하면 단일 안내 워크플로에서 AWS WAF 보호를 정의하고 배포할 수 있습니다. 빠른 생성을 사용하면 한 세션에서 배포를 통해 규칙에 대한 완전한 웹 ACL 보호를 설정할 수 있습니다.

빠른 생성을 사용하여 AWS WAF 보호를 정의하고 배포하려면 다음 절차를 순서대로 완료하세요.

정책을 생성하고 보호를 추가하려면

1. <https://console.aws.amazon.com/network-security-manager/> AWS Network Security Manager 콘솔을 엽니다.
2. 탐색 창에서 개요를 선택합니다.
3. 개요 페이지의 오른쪽 상단에서 빠른 생성 및 배포를 선택합니다. 빠른 생성 및 배포 페이지가 여러 창과 함께 나타납니다.
4. 정책 세부 정보 창의 이름에 정책 이름을 입력합니다. (선택 사항) 설명에 설명을 입력합니다.
5. 보호 정의 창에서 작업할 방화벽 유형을 선택합니다. AWS WAF를 선택합니다. 규칙 또는 템플릿을 추가할 수 있는 템플릿 및 규칙 하위 창이 나타납니다.
6. 규칙을 추가하려면 규칙 추가 또는 관리를 선택합니다. 표시되는 창에서 규칙 유형 선택에서 다음 중 하나를 선택합니다.
 - AWS 관리형 규칙 - 표에는 AWS WAF가 지원하는 모든 AWS 관리형 규칙이 표시됩니다.
 - 규칙 - 테이블에는 AWS 관리형 규칙 이외의 소유한 AWS WAF 규칙 그룹이 표시됩니다.

정책에 추가할 규칙의 확인란을 선택합니다. 그런 다음 규칙 추가를 선택합니다.

7. 템플릿을 추가하려면 템플릿 추가를 선택합니다. 템플릿 추가 창이 나타나면 테이블에 사용 가능한 템플릿이 표시됩니다. 정책에 포함할 버전과 함께 원하는 템플릿을 선택합니다. 그런 다음 템플릿 추가를 선택합니다.

정책을 구성하려면

1. 템플릿 및 규칙 테이블에서 선택 사항을 검토합니다. 위치 열의 정수에 따라 규칙 및 템플릿의 평가 순서가 결정됩니다. 평가 순서를 변경하려면 위치 열에서 위치 값을 선택합니다. 화살표를 사용하여 값을 변경합니다. 변경 사항을 수락하려면 확인을 선택합니다. 변경 사항을 되돌리려면 취소를 선택합니다.
2. 보호 정의 창의 정책 구성에서 AWS Network Security Manager가 대상 범위에서 수행하는 자동화된 작업을 결정합니다.

- 문제 해결은 AWS Network Security Manager에 설명된 원하는 상태와 보안 상태가 동기화되지 않은 모든 리소스에 정의된 정책을 적용합니다.
 - 리소스 정리는 배포가 제거되거나 계정 또는 리소스가 범위를 벗어날 때 AWS Network Security Manager가 리소스에 대해 생성한 방화벽을 삭제합니다.
 - 기존 고객 WebACL 해결은 정의 중인 정책과 이미 배포된 정책 간의 충돌을 해결하는 방법을 결정합니다. 메뉴에서 다음 옵션 중 하나를 선택합니다.
 - 문제 해결 없음은 이미 웹 ACL이 있는 리소스에 대한 문제 해결을 건너뛵니다.
 - 연결 재정의를 기존 웹 ACL을 AWS Network Security Manager에서 생성한 웹 ACL로 대체합니다.
 - Retrofit은 기존 웹 ACL마다 규칙을 새로 고치고 웹 ACL을 리소스와 연결된 상태로 유지합니다.
3. 정책 우선 순위 창에서 우선 순위를 설정합니다. AWS Network Security Manager는 우선 순위에 따라 정책을 평가하여 충돌을 해결합니다. 낮은 위치(낮은 정수)는 우선 순위가 높습니다. 우선 순위를 편집하려면 위치 값을 선택합니다. 그런 다음 화살표로 늘리거나 값을 직접 입력합니다. 선택을 확인하려면 확인을 선택합니다. 변경 사항을 취소하려면 취소를 선택합니다.

범위를 설정하려면

1. 범위 설정 창에서 정책이 적용되는 자산 세트를 정의합니다. 범위 이름에 이름을 입력합니다. (선택 사항) 설명에 설명을 입력합니다.

2.

다중 계정 모드만 해당

이 단계는 다중 계정 모드에만 적용됩니다. 다중 계정 모드에서 계정 및 조직 단위 선택 하위 창을 사용하여 포함하거나 제외할 계정 또는 OUs 선택합니다. 단일 계정 모드에서는 이 하위 창이 콘솔에 표시되지 않으므로 이 단계를 건너뛵니다.

계정 및 조직 단위 선택 하위 창에서 다음 옵션 중 하나를 선택합니다.

- 전체 AWS 조직으로 범위를 지정합니다. 추가 정의는 필요하지 않습니다.
- 전체 AWS 조직으로 범위를 지정하되 특정 OUs. 조직 단위 하위 창과 계정 하위 창이 나타납니다. 조직 단위를 제외하려면 OUs 선택합니다. 조직 트리에서 조직 단위를 선택한 다음 OUs 선택합니다. 개별 계정을 제외하려면 계정 추가를 선택합니다. 조직 트리에서 계정을 선택한 다음 계정 추가를 선택합니다.
- 전체 AWS 조직으로 범위를 지정하지 말고 특정 OUs 및 계정만 포함합니다. 원하는 조직 단위와 계정을 포함하려면 동일한 OUs 추가 및 계정 추가 메커니즘을 사용합니다.

3. 리소스 하위 창의 리소스 유형에서 모든 또는 특정 AWS WAF 리소스 유형을 선택합니다. 옵션은 다음 중 하나 이상입니다.

- Application Load Balancer
- Amazon API Gateway REST API
- CloudFront 배포

CloudFront 리전 요구 사항

CloudFront 배포 리소스를 보호하려면 미국 동부(버지니아 북부) 리전()을 사용합니다.us-east-1

글로벌 및 리전 리소스 유형

글로벌 리소스 유형(CloudFront Distribution) 또는 리전 리소스 유형(Application Load Balancer 및 Amazon API Gateway REST API)을 선택할 수 있지만 둘 다 선택할 수는 없습니다. 리소스 유형을 선택한 후에는 구성을 업데이트할 때 CloudFront 배포와 리전 리소스 유형 간에 전환할 수 없습니다.

비관리형 CloudFront 리소스

AWS Network Security Manager는 CloudFront 정액 요금제 또는 CloudFront 스테이징 배포를 사용하는 CloudFront 배포를 관리하지 않습니다. 이러한 리소스는 동기화되지 않습니다.

4. 선택한 각 리소스 유형에 대해 다음 상호 배타적 옵션 중 하나를 선택합니다.

- 모든 리소스 포함
- 특정 리소스 포함
- 특정 리소스 제외

5. 특정 리소스 포함을 선택한 경우 다음 표현식 유형 중 하나를 선택한 다음 태그 또는 ARNs.

- 단일 기준
- 모든 기준 일치(AND)
- 모든 기준과 일치(OR)
- NOT

모든 리소스 유형에는 태그 및 ARN 포함 기준이 있습니다. 태그를 선택하는 경우 키와 선택적 값을 입력합니다. 여러 태그를 식별할 수 있습니다. 리소스 유형이 Application Load Balancer인 경우 추가 구성 기준이 나타납니다. 구성에서 인터넷 연결 또는 내부 옵션이 있는 스키마를 선택합니다.

정책을 검토하고 배포하려면

1. 검토 및 배포 창의 배포 이름에 이름을 입력합니다. (선택 사항) 설명에 설명을 입력합니다. 배포의 콘텐츠가 조직의 다른 계정에 표시되는지 확인하려면 이 배포에 대한 교차 계정 가시성 활성화를 선택합니다.
2. (선택 사항) 리소스에 태그를 추가하려면 새 태그 추가를 선택한 다음 키와 선택적 값 조합을 입력합니다.
3. 정의한 내용을 실행하려면 생성 및 배포를 선택합니다. 프로세스가 완료되면 배포 페이지가 나타나고 생성된 항목의 세부 정보를 볼 수 있습니다.

⚠ 배포 시 요금이 발생할 수 있습니다.

배포는 네트워크 보안 서비스를 생성하여 보호된 리소스에 연결합니다. AWS Network Security Manager는 보호된 리소스에 대해 요금을 부과합니다. 보안 서비스 자체는 리소스를 보호하므로 추가 요금이 발생합니다. 배포하기 전에 [AWS Network Security Manager 요금 페이지](#)와 [AWS WAF 요금 페이지](#)를 검토하세요.

AWS WAF의 표준 생성 프로세스

표준 생성 프로세스를 사용하면 전체 제어를 위해 규칙, 템플릿, 정책, 범위 및 배포와 같은 각 AWS WAF 구성 요소를 개별적으로 생성합니다. 재사용 가능한 구성 요소를 생성하고 필요에 따라 결합하려는 경우 이 접근 방식을 사용합니다.

AWS Network Security Manager AWS WAF 정책에는 규칙과 템플릿이 포함될 수 있습니다. 정책을 적용하면 AWS Network Security Manager는 각 범위 내 계정에 웹 ACL을 생성합니다.

규칙을 생성하는 방법(콘솔)

1. AWS Network Security Manager 관리자 계정을 사용하여 AWS Management Console에 로그인한 다음 <https://console.aws.amazon.com/network-security-manager/> AWS Network Security Manager 콘솔을 엽니다.

관리자 계정 설정

AWS Network Security Manager 관리자 계정 설정에 대한 자세한 내용은 섹션을 참조하세요 [AWS Network Security Manager 설정](#).

2. 탐색 창에서 AWS Network Security Manager를 선택한 다음 개요를 선택합니다.
3. 개요 창에서 규칙 생성을 선택합니다. 설명이 포함된 이름을 입력한 다음 선택적 설명을 입력합니다.
4. 규칙 정의 창의 방화벽 유형에서 AWS WAF를 선택합니다.
5. 규칙 유형에서 검사 또는 구성을 선택합니다.

검사를 선택하면 규칙 그룹 참조 정의라는 JSON 편집기 창이 다음 옵션과 함께 나타납니다.

- 템플릿 삽입 - 첫 번째(사전 처리) 규칙 또는 마지막(사후 처리) 규칙에 대한 JSON 템플릿을 선택합니다. 선택할 때 AWS Network Security Manager는 템플릿을 완료하는 데 입력이 필요한 경우 경고 아이콘과 함께 해당 JSON을 편집기에 삽입합니다.
- 규칙 그룹 삽입 - 다음 세 가지 옵션으로 구동되는 선택 목록을 제공합니다.
 - AWS 관리형 규칙(AMR) 규칙 그룹
 - 기존 사용자 지정 규칙 그룹
 - AWS Marketplace 규칙 그룹

AWS Network Security Manager는 선택한와 연결된 규칙 그룹을 표시하며 포함할 단일 인스턴스를 선택할 수 있습니다. 선택한 후 규칙 그룹 선택을 선택합니다. AWS Network Security Manager는 올바른 구문으로 검사 규칙에 대한 참조를 JSON 편집기에 삽입합니다.

- AI로 삽입 - AI 구성 생성기라는 오버레이 창을 엽니다. 이 도구를 사용하여 규칙을 일반 언어로 설명하면 AWS Network Security Manager가 편집기에서 연결된 JSON을 생성합니다. 그런 다음 생성된 코드를 검토하고 출력을 수락, 수정 또는 삭제하도록 선택할 수 있습니다.
6. (선택 사항) JSON 규칙 정의가 완료되면 태그를 규칙과 연결할 수 있습니다. 이렇게 하려면 태그 추가(Add new tag)를 선택한 다음 키(Key) 및 선택 사항인 값(Value)을 입력합니다.
 7. 정의를 마치면 초안 저장을 선택하여 비활성, 잠재적으로 불완전한 객체를 저장하거나 규칙 생성을 선택합니다.

⚠ 웹 ACL 이름은 영구적입니다.

웹 ACL 이름을 생성한 후에는 변경할 수 없습니다. 정책 이름을 업데이트하는 경우 AWS Network Security Manager는 연결된 웹 ACL 이름을 업데이트하지 않습니다. AWS Network Security Manager가 다른 이름의 웹 ACL을 생성하도록 하려면 새 정책을 생성해야 합니다.

템플릿을 생성하려면(콘솔)

템플릿은 정책 내에서 평가를 위해 우선 순위에 따라 규칙을 수집합니다. 규칙 유형을 보안 목표에 맞는 그룹화로 구성할 수 있습니다. 또한 여러 팀이 책임과 기술에 맞는 보안 제어 문을 구축하도록 할 수 있습니다.

1. 개요 페이지의 개요 창에서 템플릿 생성을 선택합니다. 템플릿 생성 페이지에서 템플릿 이름을 입력하고 선택적 설명을 입력한 다음 방화벽 유형(이 경우 AWS WAF)을 선택합니다.
2. 방화벽 유형을 선택하면 규칙 창이 나타납니다. 두 규칙 추가 버튼 중 하나를 선택하여 사용 가능한 규칙 목록을 엽니다. 규칙 이름 왼쪽에 있는 확인란을 선택하여 템플릿에 추가합니다. 규칙의 특정 버전을 선택하려면 규칙의 버전 필드를 선택합니다. 여러 버전을 사용할 수 있는 경우 원하는 버전을 선택한 다음 확인을 선택합니다.
3. (선택 사항) 템플릿에 대한 태그를 생성합니다. 완료되면 초안 저장 또는 템플릿 생성을 선택합니다. 정책을 계속 생성하려면 템플릿 생성을 선택합니다.

정책을 생성하려면(콘솔)

이는 정책 정의 및 배포 준비의 마지막 단계입니다.

1. 개요 페이지의 개요 창에서 정책 생성을 선택합니다. 정책 생성 페이지에서 이름과 선택적 설명을 입력한 다음 방화벽 유형(이 경우 AWS WAF)을 선택합니다.
2. 정책 우선 순위 창에서 우선 순위를 설정합니다. AWS Network Security Manager는 우선 순위에 따라 정책을 평가하여 충돌을 해결합니다. 낮은 위치(낮은 정수)는 우선 순위가 높습니다. 우선 순위를 편집하려면 위치 값을 선택합니다. 그런 다음 화살표로 늘리거나 값을 직접 입력합니다. 선택을 확인하려면 확인을 선택합니다. 변경 사항을 취소하려면 취소를 선택합니다.
3. 정책 구성 창에서 AWS Network Security Manager가 대상 범위에서 수행하는 자동화된 작업을 결정합니다.

- 문제 해결은 AWS Network Security Manager에 설명된 원하는 상태와 보안 상태가 동기화되지 않은 모든 리소스에 정의된 정책을 적용합니다.
 - 리소스 정리는 배포가 제거되거나 계정 또는 리소스가 범위를 벗어날 때 AWS Network Security Manager가 리소스에 대해 생성한 방화벽을 삭제합니다.
 - 기존 고객 WebACL 해결은 정의 중인 정책과 이미 배포된 정책 간의 충돌을 해결하는 방법을 결정합니다. 메뉴에서 다음 옵션 중 하나를 선택합니다.
 - 문제 해결 없음은 이미 웹 ACL이 있는 리소스에 대한 문제 해결을 건너뛸니다.
 - 연결을 재정의하면 기존 웹 ACL이 AWS Network Security Manager에서 생성한 웹 ACL로 대체됩니다.
 - Retrofit은 규칙을 각 기존 웹 ACL에 새로 고치고 웹 ACL을 리소스와 연결된 상태로 유지합니다.
4. 이러한 구성 설정이 완료되면 정책에 추가할 규칙과 템플릿을 선택합니다. 템플릿 및 규칙 창에서 규칙 추가 또는 템플릿 추가를 선택하여 정책을 채웁니다. 두 프로세스 모두가 섹션의 앞부분에서 설명한 규칙 선택 프로세스와 동일한 방식으로 작동하는 창을 엽니다.

범위를 생성하려면(콘솔)

1. 개요 페이지 또는 도구 내의 다른 영역에서이 단계를 시작할 수 있습니다. 범위 세부 정보 창에서 범위 이름과 선택적 설명을 입력합니다.

2.

다중 계정 모드만 해당

이 단계는 다중 계정 모드에만 적용됩니다. 다중 계정 모드에서 계정 및 조직 단위 선택 하위 창을 사용하여 포함하거나 제외할 계정 또는 OUs 선택합니다. 단일 계정 모드에서는이 하위 창이 콘솔에 표시되지 않으므로이 단계를 건너뛸니다.

계정 및 조직 단위 선택 창에서 관리 범위를 제어하는 세 가지 방법 중 하나를 선택합니다.

- 전체 AWS 조직(모든 OUs 및 계정) 범위 - 추가 정의가 필요하지 않습니다.
- 전체 AWS 조직으로 범위를 지정하되 특정 OUs 및 계정 제외 - 조직 단위와 계정의 하위 창 2개가 나타납니다. OUs 선택하여 OUs 추가 창을 열고 조직 트리에서 필요한 조직 단위를 선택한 다음 OUs 선택합니다. 개별 계정을 추가하려면 계정 하위 창에서 계정 추가를 선택하고 조직 트리에서 계정을 선택한 다음 계정 추가를 선택합니다.
- 전체 AWS 조직으로 범위를 지정하지 않고 특정 OUs 및 계정만 포함 - 동일한 하위 창을 사용하여 이전 옵션에 대해 설명된 것과 동일한 메커니즘을 가진 OUs 또는 계정을 추가합니다.

3. 그런 다음 리소스 하위 창에서 리소스를 선택합니다. 리소스 유형 선택 상자에서 모든 또는 특정 AWS WAF 리소스 유형을 선택합니다. AWS WAF의 경우 옵션은 다음 중 일부 또는 전부입니다.

- Application Load Balancer
- Amazon API Gateway REST API
- CloudFront 배포

CloudFront 리전 요구 사항

CloudFront Distribution 리소스를 보호하려면 미국 동부(버지니아 북부) 리전()을 사용합니다.us-east-1

글로벌 및 리전 리소스 유형

글로벌 리소스 유형(CloudFront Distribution) 또는 리전 리소스 유형(Application Load Balancer 및 Amazon API Gateway REST API)을 선택할 수 있지만 둘 다 선택할 수는 없습니다. 리소스 유형을 선택한 후에는 구성을 업데이트할 때 CloudFront 배포와 리전 리소스 유형 간에 전환할 수 없습니다.

비관리형 CloudFront 리소스

AWS Network Security Manager는 CloudFront 정액 요금제 또는 CloudFront 스테이징 배포를 사용하는 CloudFront 배포를 관리하지 않습니다. 이러한 리소스는 동기화되지 않습니다.

4. 선택한 각 리소스 유형에 대해 다음 상호 배타적 옵션 중 하나를 선택합니다.

- 모든 리소스 포함
- 특정 리소스 포함
- 특정 리소스 제외

5. 특정 리소스 포함을 선택한 경우 다음 표현식 유형 중 하나를 선택합니다.

- 단일 기준
- 모든 기준 일치(AND)
- 모든 기준과 일치(OR)
- NOT

6. 각 표현식 유형은 단일 또는 다중 포함 기준과 ARNs 지원하므로 태그 또는 ARNs. 모든 리소스 유형은 태그 및 ARN 포함 기준을 지원합니다. 태그를 선택하는 경우 키와 선택적 값을 식별합니다. 여러 태그를 식별할 수 있습니다.
7. Application Load Balancer의 경우 추가 구성 기준이 나타납니다. 구성 내에서 인터넷 경계 또는 내부 옵션을 사용하여 스키마를 설정할 수 있습니다.

배포를 생성하려면(콘솔)

배포는 정책을 범위에 바인딩하고 적용을 활성화하여 AWS Network Security Manager가 범위 내 리소스에 AWS WAF 규칙을 적용하도록 합니다.

1. 개요 페이지의 개요 창에서 배포 생성을 선택합니다. 도구 내의 다른 영역에서도 이 단계를 시작할 수 있습니다.
2. 배포할 정책을 선택합니다.
3. AWS Network Security Manager가 정책을 적용하는 계정 및 리소스를 정의하는 범위를 선택합니다.
4. 배포 이름에 이름을 입력합니다. (선택 사항) 설명에 설명을 입력합니다.
5. (선택 사항) 배포를 조직의 다른 계정에 표시하려면 이 배포에 대한 교차 계정 가시성 활성화를 선택합니다.
6. (선택 사항) 태그를 추가하려면 새 태그 추가를 선택한 다음 키와 선택적 값 조합을 입력합니다.
7. 생성 및 배포를 선택합니다. AWS Network Security Manager가 생성한 세부 정보를 볼 수 있는 배포 페이지가 나타납니다.

배포 시 요금이 발생할 수 있습니다.

배포는 네트워크 보안 서비스를 생성하여 보호된 리소스에 연결합니다. AWS Network Security Manager는 보호된 리소스에 대해 요금을 부과합니다. 보안 서비스 자체는 리소스를 보호하므로 추가 요금이 발생합니다. 배포하기 전에 [AWS Network Security Manager 요금 페이지](#)와 [AWS WAF 요금 페이지](#)를 검토하세요.

AWS Shield Advanced에 대한 DDoS 보호 관리

AWS Network Security Manager를 사용하면 조직의 계정 및 리소스에 걸쳐 AWS Shield Advanced 보호를 중앙에서 구성하고 배포할 수 있습니다. AWS Network Security Manager 정책 및 배포를 통해 DDoS 보호 정책을 정의하고 대규모로 적용할 수 있습니다.

 AWS Network Security Manager는 별도로 청구됩니다.

AWS Network Security Manager는 AWS Shield Advanced 제안의 일부가 아닙니다. 요금에 대한 자세한 내용은 [AWS Network Security Manager 요금](#) 및 [AWS Shield Advanced 요금](#)을 참조하세요.

 AWS Shield Advanced 구독

활성 배포에 해당 범위의 계정이 포함된 경우 AWS Network Security Manager는 해당 계정을 AWS Shield Advanced에 구독합니다. AWS Network Security Manager는 계정이 범위를 벗어나거나 배포를 제거할 때 구독을 취소하지 않습니다. AWS Shield Advanced 구독을 취소하려면 AWS WAF 개발자 안내서의 [AWS Shield Advanced 구독](#)을 참조하세요.

AWS Shield Advanced용 빠른 생성

빠른 생성을 사용하면 단일 안내 워크플로에서 AWS Shield Advanced 보호를 정의하고 배포할 수 있습니다. 한 세션에서 배포를 통해 정책으로부터 DDoS 보호를 설정하려는 경우 빠른 생성을 사용합니다.

빠른 생성을 사용하여 AWS Shield Advanced 보호를 정의하고 배포하려면 다음 절차를 순서대로 완료하세요.

정책을 생성하고 보호를 구성하려면

다음 단계를 완료합니다.

1. <https://console.aws.amazon.com/network-security-manager/> AWS Network Security Manager 콘솔을 엽니다.
2. 탐색 창에서 개요를 선택합니다.

3. 개요 페이지에서 빠른 생성 및 배포를 선택합니다. 빠른 생성 및 배포 페이지가 여러 창과 함께 나타납니다.
4. 정책 세부 정보 창의 이름에 정책 이름을 입력합니다. (선택 사항) 설명에 설명을 입력합니다.
5. 보호 정의 창에서 작업할 방화벽 유형을 선택합니다. AWS Shield Advanced를 선택합니다.
6. 보호 정의 창의 정책 구성에서 AWS Network Security Manager가 대상 범위에서 수행하는 자동화된 작업을 결정합니다.
 - 문제 해결은 AWS Network Security Manager가 설명하는 원하는 상태와 보안 상태가 일치하지 않는 모든 리소스에 정의된 정책을 적용합니다.
 - 리소스 정리는 배포가 제거되거나 계정 또는 리소스가 범위를 벗어날 때 AWS Network Security Manager가 리소스에 대해 생성한 DDoS 보호를 삭제합니다.
 - 기존 고객 DDoS 해결은 정의 중인 정책과 이미 배포된 정책 간의 충돌을 해결하는 방법을 결정합니다. 메뉴에서 다음 옵션 중 하나를 선택합니다.
 - 문제 해결 없음은 이미 DDoS 보호 기능이 있는 리소스에 대한 문제 해결을 건너뛵니다.
 - 연결 재정의를 기존 DDoS 보호를 AWS Network Security Manager에서 생성한 DDoS 보호로 대체합니다.
 - Retrofit은 기존 DDoS 보호 각각에 규칙을 새로 고치고 리소스와 연결된 DDoS 보호를 유지합니다.
7. 정책 우선 순위 창에서 우선 순위를 설정합니다. AWS Network Security Manager는 우선 순위에 따라 정책을 평가하여 충돌을 해결합니다. 낮은 위치(낮은 정수)는 우선 순위가 높습니다.

우선 순위를 편집하려면 위치 값을 선택합니다. 그런 다음 화살표로 늘리거나 값을 직접 입력합니다. 선택을 확인하려면 확인을 선택합니다. 변경 사항을 취소하려면 취소를 선택합니다.

범위를 설정하려면

다음 단계를 완료합니다.

1. 범위 설정 창에서 정책이 적용되는 자산 세트를 정의합니다. 범위 이름에 이름을 입력합니다. (선택 사항) 설명에 설명을 입력합니다.

2.

다중 계정 모드만 해당

이 단계는 다중 계정 모드에만 적용됩니다. 다중 계정 모드에서 계정 및 조직 단위 선택 하위 창을 사용하여 포함하거나 제외할 계정 또는 OUs 선택합니다. 단일 계정 모드에서는이 하위 창이 콘솔에 표시되지 않으므로이 단계를 건너뛵니다.

계정 및 조직 단위 선택 하위 창에서 다음 옵션 중 하나를 선택합니다.

- 전체 AWS 조직으로 범위를 지정합니다. 추가 정의는 필요하지 않습니다.
 - 전체 AWS 조직으로 범위를 지정하되 특정 OUs. 조직 단위 하위 창과 계정 하위 창이 나타납니다. 조직 단위를 제외하려면 OUs 선택합니다. 조직 트리에서 조직 단위를 선택한 다음 OUs 선택합니다. 개별 계정을 제외하려면 계정 추가를 선택합니다. 조직 트리에서 계정을 선택한 다음 계정 추가를 선택합니다.
 - 전체 AWS 조직으로 범위를 지정하지 말고 특정 OUs 및 계정만 포함합니다. 원하는 조직 단위와 계정을 포함하려면 동일한 OUs 추가 및 계정 추가 메커니즘을 사용합니다.
3. 리소스 하위 창의 리소스 유형에서 모든 또는 특정 AWS Shield Advanced 리소스 유형을 선택합니다. 옵션은 다음 중 하나 이상입니다.
- Application Load Balancer
 - CloudFront 배포
 - Classic Load Balancer
 - 탄력적 IP 주소
4. 선택한 각 리소스 유형에 대해 다음 상호 배타적 옵션 중 하나를 선택합니다.
- 모든 리소스 포함
 - 특정 리소스 포함
 - 특정 리소스 제외
5. 특정 리소스 포함을 선택한 경우 다음 표현식 유형 중 하나를 선택한 다음 태그 또는 ARNs.
- 단일 기준
 - 모든 기준 일치(AND)
 - 모든 기준과 일치(OR)
 - NOT

모든 리소스 유형에는 태그 및 ARN 포함 기준이 있습니다. 태그를 선택하는 경우 키와 선택적 값을 입력합니다. 여러 태그를 식별할 수 있습니다.

CloudFront 리전 요구 사항

CloudFront 배포 리소스를 보호하려면 미국 동부(버지니아 북부) 리전()을 사용합니다.us-east-1

정책을 검토하고 배포하려면

다음 단계를 완료합니다.

1. 검토 및 배포 창의 배포 이름에 이름을 입력합니다. (선택 사항) 설명에 설명을 입력합니다. 배포의 콘텐츠가 조직의 다른 계정에 표시되는지 확인하려면 이 배포에 대한 교차 계정 가시성 활성화를 선택합니다.
2. (선택 사항) 리소스에 태그를 추가하려면 새 태그 추가를 선택한 다음 키 및 선택적 값 조합을 입력합니다.
3. 정책 및 범위를 생성하고 배포하려면 생성 및 배포를 선택합니다. 프로세스가 완료되면 AWS Network Security Manager가 생성한 세부 정보를 볼 수 있는 배포 페이지가 나타납니다.

 배포 시 요금이 발생할 수 있습니다.

배포는 네트워크 보안 서비스를 생성하여 보호된 리소스에 연결합니다. AWS Network Security Manager는 보호된 리소스에 대해 요금을 부과합니다. 보안 서비스 자체는 리소스를 보호하므로 추가 요금이 발생합니다. 배포하기 전에 [AWS Network Security Manager 요금 페이지](#)와 [AWS Shield Advanced 요금 페이지](#)를 검토하세요.

AWS Shield Advanced의 표준 생성 프로세스

표준 생성 프로세스를 사용하면 전체 제어를 위해 정책, 범위 및 배포와 같은 각 AWS Shield Advanced 구성 요소를 개별적으로 설정할 수 있습니다. 재사용 가능한 구성 요소를 생성하고 필요에 따라 결합하려는 경우가 접근 방식을 사용합니다.

AWS Shield Advanced 정책은 간단하며 규칙, 규칙 그룹 또는 템플릿을 포함하지 않습니다. 정책을 적용하면 AWS Network Security Manager는 각 범위 내 계정에 AWS Shield Advanced DDoS 보호를 생성합니다. AWS Network Security Manager의 작동 방식에 대한 자세한 내용은 섹션을 참조하세요 [AWS Network Security Manager 작동 방식](#).

정책을 생성하려면(콘솔)

다음 단계를 완료합니다.

1. AWS Network Security Manager 관리자 계정을 사용하여 AWS Management Console에 로그인한 다음 <https://console.aws.amazon.com/network-security-manager/> AWS Network Security Manager 콘솔을 엽니다.

관리자 계정 설정

AWS Network Security Manager 관리자 계정 설정에 대한 자세한 내용은 섹션을 참조하세요 [AWS Network Security Manager 설정](#).

2. 탐색 창에서 AWS Network Security Manager를 선택한 다음 개요를 선택합니다.
3. 개요 창에서 정책 생성을 선택합니다. 이름과 선택적 설명을 입력한 다음 방화벽 유형(이 경우 AWS Shield Advanced)을 선택합니다.
4. 정책 우선 순위 창에서 우선 순위를 설정합니다. AWS Network Security Manager는 우선 순위에 따라 정책을 평가하여 충돌을 해결합니다. 낮은 위치(낮은 정수)는 우선 순위가 높습니다.

우선 순위를 편집하려면 위치 값을 선택합니다. 그런 다음 화살표로 늘리거나 값을 직접 입력합니다. 선택을 확인하려면 확인을 선택합니다. 변경 사항을 취소하려면 취소를 선택합니다.

5. 정책 구성 창에서 AWS Network Security Manager가 대상 범위에서 수행하는 자동화된 작업을 결정합니다.
 - 해결은 AWS Network Security Manager가 설명하는 원하는 상태와 보안 상태가 일치하지 않는 모든 리소스에 정의된 정책을 적용합니다.
 - 리소스 정리는 배포가 제거되거나 계정 또는 리소스의 범위가 벗어날 때 AWS Network Security Manager가 리소스에 대해 생성한 DDoS 보호를 삭제합니다.
 - 기존 고객 DDoS 해결은 정의 중인 정책과 이미 배포된 정책 간의 충돌을 해결하는 방법을 결정합니다. 메뉴에서 다음 옵션 중 하나를 선택합니다.
 - 문제 해결 없음은 이미 DDoS 보호 기능이 있는 리소스에 대한 문제 해결을 건너뛵니다.
 - 연결 재정의를 기존 DDoS 보호를 AWS Network Security Manager에서 생성한 DDoS 보호로 대체합니다.
 - Retrofit은 기존 DDoS 보호 각각에 규칙을 새로 고치고 리소스와 연결된 DDoS 보호를 유지합니다.

범위를 생성하려면(콘솔)

다음 단계를 완료합니다.

1. 범위 세부 정보 창에서 범위 이름과 선택적 설명을 입력합니다.

2.

 다중 계정 모드만 해당

이 단계는 다중 계정 모드에만 적용됩니다. 다중 계정 모드에서 계정 및 조직 단위 선택 하위 창을 사용하여 포함하거나 제외할 계정 또는 OUs 선택합니다. 단일 계정 모드에서는 이 하위 창이 콘솔에 표시되지 않으므로 이 단계를 건너뛰니다.

계정 및 조직 단위 선택 창에서 관리 범위를 제어하는 세 가지 방법 중 하나를 선택합니다.

- 전체 AWS 조직(모든 OUs 및 계정) 범위 - 추가 정의가 필요하지 않습니다.
- 전체 AWS 조직으로 범위를 지정하되 특정 OUs 및 계정 제외 - 조직 단위와 계정의 하위 창 두 개가 나타납니다. OUs 선택하여 OUs 추가 창을 열고 필요한 조직 단위를 선택한 다음 OUs 선택합니다. 개별 계정을 추가하려면 계정 하위 창에서 계정 추가를 선택하고 계정을 선택한 다음 계정 추가를 선택합니다.
- 전체 AWS 조직으로 범위를 지정하지 않고 특정 OUs 및 계정만 포함 - 동일한 하위 창을 사용하여 OUs 또는 계정을 추가합니다.

3. 그런 다음 리소스 하위 창에서 리소스를 선택합니다. 리소스 유형 선택 상자에서 모든 또는 특정 AWS Shield Advanced 리소스 유형을 선택합니다. AWS Shield Advanced의 경우 옵션은 다음 중 일부 또는 전부입니다.

- Application Load Balancer
- CloudFront 배포
- Classic Load Balancer
- 탄력적 IP 주소

4. 선택한 각 리소스 유형에 대해 다음 상호 배타적 옵션 중 하나를 선택합니다.

- 모든 리소스 포함
- 특정 리소스 포함
- 특정 리소스 제외

5. 특정 리소스 포함을 선택한 경우 다음 표현식 유형 중 하나를 선택합니다.

- 단일 기준
- 모든 기준 일치(AND)
- 모든 기준과 일치(OR)
- NOT

6. 각 표현식 유형은 단일 또는 다중 포함 기준과 ARNs 지원하므로 태그 또는 ARNs. 모든 리소스 유형은 태그 및 ARN 포함 기준을 지원합니다. 태그를 선택하는 경우 키와 선택적 값을 식별합니다. 여러 태그를 식별할 수 있습니다.

CloudFront 리전 요구 사항

CloudFront Distribution 리소스를 보호하려면 미국 동부(버지니아 북부) 리전()을 사용합니
다.us-east-1

배포를 생성하려면(콘솔)

배포는 정책을 범위에 바인딩하고 적용을 활성화합니다. 그런 다음 AWS Network Security Manager는 범위 내 리소스에 AWS Shield Advanced DDoS 보호를 적용합니다.

다음 단계를 완료합니다.

1. 개요 페이지의 개요 창에서 배포 생성을 선택합니다.
2. 배포할 정책을 선택합니다.
3. AWS Network Security Manager가 정책을 적용하는 계정 및 리소스를 정의하는 범위를 선택합니다.
4. 배포 이름에 이름을 입력합니다. (선택 사항) 설명에 설명을 입력합니다.
5. (선택 사항) 배포를 조직의 다른 계정에 표시하려면 이 배포에 대한 교차 계정 가시성 활성화를 선택합니다.
6. (선택 사항) 태그를 추가하려면 새 태그 추가를 선택한 다음 키와 선택적 값 조합을 입력합니다.
7. 생성 및 배포를 선택합니다. AWS Network Security Manager가 생성한 세부 정보를 볼 수 있는 배포 페이지가 나타납니다.

배포 시 요금이 발생할 수 있습니다.

배포는 네트워크 보안 서비스를 생성하여 보호된 리소스에 연결합니다. AWS Network Security Manager는 보호된 리소스에 대해 요금을 부과합니다. 보안 서비스 자체는 리소스를 보호하므로 추가 요금이 발생합니다. 배포하기 전에 [AWS Network Security Manager 요금 페이지](#)와 [AWS Shield Advanced 요금 페이지](#)를 검토하세요.

AWS Network Security Manager 및 AWS Firewall Manager

AWS Network Security Manager는 AWS Firewall Manager를 대체하는 서비스입니다. 두 서비스는 완전히 분리되어 있으며, 각각 고유한 기능과 다른 요금 모델을 갖추고 있습니다. 현재 AWS Firewall Manager를 사용하는 경우 별도의 조치를 취할 필요가 없습니다. 기존 방화벽과 정책은 계속 작동합니다. 이 장에서는 두 서비스가 공존하는 방식, 둘 다 사용할 때 우선 순위가 작동하는 방식, 마이그레이션이 사용 가능해질 때 마이그레이션이 작동하는 방식을 설명합니다.

AWS Network Security Manager와 AWS Firewall Manager는 서로 나란히 독립적으로 작동합니다. 어느 시점에서 AWS Firewall Manager는 판매를 중지한 다음 작동을 중지합니다.

AWS Firewall Manager와 공존

AWS Network Security Manager는 변경 작업을 시작하지 않는 한 Firewall Manager로 생성한 AWS 방화벽에 영향을 주지 않습니다. Firewall Manager로 AWS 생성한 방화벽 및 정책은 종료하지 않는 한 계속 작동합니다. 이는 AWS Firewall Manager가 사용 중지된 후에도 마찬가지입니다.

문제 해결 중 우선 순위

두 서비스가 모두 작동하는 동안 AWS Firewall Manager로 생성한 방화벽에 영향을 미치는 작업을 수행할 수 있습니다. AWS Network Security Manager 정책을 생성할 때 대상 리소스 집합인 범위에 적용합니다. 이 범위에 AWS Firewall Manager 정책이 이미 처리하는 리소스가 포함된 경우 문제 해결 중에 AWS Network Security Manager가 우선합니다. 이 경우 AWS Network Security Manager 정책 및 범위는 기존 AWS Firewall Manager 방화벽 및 정책을 재정의합니다. 특정 동작은 선택한 해결 옵션에 따라 달라집니다.

AWS Firewall Manager에서 계획된 마이그레이션

AWS Firewall Manager에서 AWS Network Security Manager로 마이그레이션하면 방화벽 관리가 단일 서비스로 통합되고 기능을 사용할 수 있습니다. 마이그레이션이 계획되었지만 아직 사용할 수 없습니다. 마이그레이션을 사용할 수 있게 되면 AWS Firewall Manager 정책을 AWS Network Security Manager로 이동할 수 있습니다. 마이그레이션하려면 아직 준비되지 않은 두 서비스 모두에서 새로운 작업이 필요합니다.

계획된 프로세스는 AWS Firewall Manager에서 선택한 정책을 복사하여 AWS Network Security Manager로 전송하고 새 정책 구조로 변환합니다. 이 프로세스는 Firewall AWS Manager의 원래 정책 또는 연결된 방화벽에 영향을 주지 않습니다.

AWS Network Security Manager의 보안

의 클라우드 보안 AWS 이 최우선 순위입니다. AWS 고객은 보안에 가장 민감한 조직의 요구 사항을 충족하도록 구축된 데이터 센터 및 네트워크 아키텍처의 이점을 누릴 수 있습니다.

보안은 AWS와 사용자 간의 공동 책임입니다. [공동 책임 모델](#)에서는 이 사항을 클라우드의 보안 및 클라우드 내 보안으로 설명합니다.

- 클라우드 보안 - AWS 는에서 AWS 서비스를 실행하는 인프라를 보호할 책임이 있습니다 AWS 클라우드. AWS 또한 안전하게 사용할 수 있는 서비스를 제공합니다. 타사 감사자는 [AWS 규정 준수 프로그램](#) 일환으로 보안의 효과를 정기적으로 테스트하고 확인합니다. AWS Network Security Manager에 적용되는 규정 준수 프로그램에 대한 자세한 내용은 규정 준수 프로그램 [AWS 제공 범위 내 서비스](#) 규정 준수 프로그램 .
- 클라우드의 보안 - 사용자의 책임은 사용하는 AWS 서비스에 따라 결정됩니다. 또한 귀하는 데이터의 민감도, 회사 요구 사항, 관련 법률 및 규정을 비롯한 기타 요소에 대해서도 책임이 있습니다.

이 설명서는 AWS Network Security Manager를 사용할 때 공동 책임 모델을 적용하는 방법을 이해하는 데 도움이 됩니다. 다음 주제에서는 보안 및 규정 준수 목표에 맞게 AWS Network Security Manager를 구성하는 방법을 보여줍니다. 또한 AWS Network Security Manager 리소스를 모니터링하고 보호하는 데 도움이 되는 다른 AWS 서비스를 사용하는 방법을 알아봅니다.

주제

- [AWS Network Security Manager의 데이터 보호](#)
- [AWS Network Security Manager의 ID 및 액세스 관리](#)
- [AWS Network Security Manager에 서비스 연결 역할 사용](#)
- [AWS Network Security Manager에 대한 규정 준수 검증](#)
- [AWS Network Security Manager의 복원력](#)
- [AWS Network Security Manager의 인프라 보안](#)
- [AWS Network Security Manager의 보안 모범 사례](#)

AWS Network Security Manager의 데이터 보호

AWS [공동 책임 모델](#) AWS Network Security Manager의 데이터 보호에 적용됩니다. 이 모델에 설명된 대로 AWS 는 모든를 실행하는 글로벌 인프라를 보호할 책임이 있습니다 AWS 클라우드. 사용자는 이

인프라에 호스팅되는 콘텐츠에 대한 통제 권한을 유지할 책임이 있습니다. 사용하는 AWS 서비스의 보안 구성과 관리 태스크에 대한 책임도 사용자에게 있습니다. 데이터 프라이버시에 대한 자세한 내용은 [데이터 프라이버시 FAQ](#) 참조하세요. 유럽의 데이터 보호에 대한 자세한 내용은 [일반 데이터 보호 규정\(GDPR\) 센터](#)를 참조하세요.

데이터 보호를 위해 자격 증명을 보호하고 AWS 계정 AWS IAM Identity Center 또는 AWS Identity and Access Management (IAM)를 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 다중 인증(MFA)을 사용합니다.
- SSL/TLS를 사용하여 AWS 리소스와 통신합니다. TLS 1.2는 필수이며 TLS 1.3을 권장합니다.
- 를 사용하여 API 및 사용자 활동 로깅을 설정합니다 AWS CloudTrail. CloudTrail 추적을 사용하여 AWS 활동을 캡처하는 방법에 대한 자세한 내용은 AWS CloudTrail 사용 설명서의 [CloudTrail 추적 작업을 참조하세요](#).
- 내부의 모든 기본 보안 제어와 함께 AWS 암호화 솔루션을 사용합니다 AWS 서비스.
- Amazon S3에 저장된 민감한 데이터를 검색하고 보호하는 데 도움이 되는 Amazon Macie와 같은 고급 관리형 보안 서비스를 사용합니다.
- 명령줄 인터페이스 또는 API를 AWS 통해 액세스할 때 FIPS 140-3 검증 암호화 모듈이 필요한 경우 FIPS 엔드포인트를 사용합니다. 사용 가능한 FIPS 엔드포인트에 대한 자세한 내용은 [연방 정보 처리 표준\(FIPS\) 140-3](#)을 참조하세요.

고객의 이메일 주소와 같은 기밀 정보나 중요한 정보는 태그나 이름 필드와 같은 자유 형식 텍스트 필드에 입력하지 않는 것이 좋습니다. 여기에는 AWS Network Security Manager 또는 기타 AWS 서비스에서 콘솔 AWS CLI, API 또는 AWS SDKs를 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.

저장된 데이터 암호화

AWS Network Security Manager는 AWS Key Management Service(AWS KMS) 키를 사용하여 저장된 모든 데이터를 암호화합니다. 서비스 관리형 KMS 키는 리소스 구성, 배포 상태 및 동기화 데이터를 보호합니다. 이러한 키는 구성하거나 관리할 필요가 없습니다.

전송 중 암호화

AWS Network Security Manager는 전송 계층 보안(TLS)을 사용하여 전송 중인 모든 데이터를 암호화합니다. 모든 API 요청에는 TLS 1.2 이상이 필요합니다. AWS Network Security Manager API 엔드포인트에 대한 연결은 HTTPS만 사용합니다.

키 관리

AWS Network Security Manager는 서비스 관리형 AWS KMS 키를 저장 시 암호화에 사용합니다. 지금은 자체 KMS 키를 제공할 수 없습니다.

AWS Network Security Manager의 ID 및 액세스 관리

AWS Identity and Access Management (IAM)는 관리자가 AWS 리소스에 대한 액세스를 안전하게 제어하는 데 도움이 되는 서비스입니다. IAM 관리자는 AWS Network Security Manager 리소스를 사용할 수 있는 인증(로그인) 및 권한(권한 있음)을 받을 수 있는 사용자를 제어합니다. IAM은 추가 비용 없이 사용할 수 있는 AWS 서비스입니다.

주제

- [대상](#)
- [ID를 통한 인증](#)
- [정책을 사용하여 액세스 관리](#)
- [AWS Network Security Manager와 IAM의 작동 방식](#)
- [AWS Network Security Manager의 자격 증명 기반 정책 예제](#)
- [AWS Network Security Manager 자격 증명 및 액세스 문제 해결](#)

대상

AWS Identity and Access Management (IAM)를 사용하는 방법은 역할에 따라 다릅니다.

- 서비스 사용자 - 기능에 액세스할 수 없는 경우 관리자에게 권한 요청([참조 AWS Network Security Manager 자격 증명 및 액세스 문제 해결](#))
- 서비스 관리자 - 사용자 액세스 결정 및 권한 요청 제출([AWS Network Security Manager와 IAM의 작동 방식](#) 참조)
- IAM 관리자 - 액세스를 관리하기 위한 정책 작성([AWS Network Security Manager의 자격 증명 기반 정책 예제](#) 참조)

ID를 통한 인증

인증은 AWS 자격 증명으로 로그인하는 방법입니다. AWS 계정 루트 사용자, IAM 사용자 또는 IAM 역할을 수임하여 인증되어야 합니다.

AWS IAM Identity Center (IAM Identity Center), Single Sign-On 인증 또는 Google/Facebook 자격 증명과 같은 자격 증명 소스의 자격 증명을 사용하여 페더레이션 자격 증명으로 로그인할 수 있습니다. 로그인하는 방법에 대한 자세한 내용은 AWS 로그인 사용 설명서의 [AWS 계정에 로그인하는 방법](#) 섹션을 참조하세요.

프로그래밍 방식 액세스를 위해서는 요청에 암호화 방식으로 서명할 수 있는 SDK 및 CLI를 AWS 제공합니다. 자세한 내용은 IAM 사용 설명서의 [API 요청용 AWS Signature Version 4](#) 섹션을 참조하세요.

AWS 계정 루트 사용자

를 생성할 때 모든 AWS 서비스 및 리소스에 대한 완전한 액세스 권한이 있는 AWS 계정 theroot 사용자라는 하나의 로그인 자격 증명으로 AWS 계정시작합니다. 일상적인 태스크에 루트 사용자를 사용하지 않을 것을 강력히 권장합니다. 루트 사용자 자격 증명이 필요한 작업은 IAM 사용 설명서의 [루트 사용자 자격 증명이 필요한 작업](#) 섹션을 참조하세요.

페더레이션 ID

가장 좋은 방법은 인간 사용자에게 자격 증명 공급자와의 페더레이션을 사용하여 임시 자격 증명을 AWS 서비스 사용하여 액세스하도록 요구하는 것입니다.

페더레이션 자격 증명은 엔터프라이즈 디렉터리, 웹 자격 증명 공급자 또는 자격 증명 소스의 자격 증명을 AWS 서비스 사용하여 Directory Service 에 액세스하는 사용자입니다. 페더레이션 ID는 임시 자격 증명을 제공하는 역할을 수임합니다.

중앙 집중식 액세스 관리를 위해 AWS IAM Identity Center를 추천합니다. 자세한 정보는 AWS IAM Identity Center 사용 설명서의 [What is IAM Identity Center?](#)를 참조하세요.

IAM 사용자 및 그룹

[IAM 사용자](#)는 단일 개인 또는 애플리케이션에 대한 특정 권한을 가진 ID입니다. 장기 자격 증명에 있는 IAM 사용자 대신 임시 자격 증명을 사용하는 것이 좋습니다. 자세한 내용은 IAM 사용 설명서의 [자격 증명 공급자와의 페더레이션을 사용하여 임시 자격 증명을 AWS 사용하여 액세스하도록 인간 사용자에게 요구하기](#)를 참조하세요.

[IAM 그룹](#)은 IAM 사용자 모음을 지정하고 대규모 사용자 집합에 대한 관리 권한을 더 쉽게 만듭니다. 자세한 내용은 IAM 사용 설명서의 [IAM 사용자 사용 사례](#) 섹션을 참조하세요.

IAM 역할

[IAM 역할](#)은 임시 자격 증명을 제공하는 특정 권한이 있는 자격 증명입니다. [사용자에서 IAM 역할\(콘솔\)로 전환하거나 또는 API 작업을 호출하여 역할을](#) 수임할 수 있습니다. AWS CLI AWS 자세한 내용은 IAM 사용 설명서의 [역할 수임 방법](#)을 참조하세요.

IAM 역할은 페더레이션 사용자 액세스, 임시 IAM 사용자 권한, 교차 계정 액세스, 교차 서비스 액세스 및 Amazon EC2에서 실행되는 애플리케이션에 유용합니다. 자세한 내용은 IAM 사용 설명서의 [교차 계정 리소스 액세스](#)를 참조하세요.

정책을 사용하여 액세스 관리

정책을 AWS 생성하고 자격 증명 또는 리소스에 연결하여 AWS 에서 액세스를 제어합니다. 정책은 자격 증명 또는 리소스와 연결될 때 권한을 정의합니다.는 보안 주체가 요청할 때 이러한 정책을 AWS 평가합니다. 대부분의 정책은 JSON 문서 AWS 로 저장됩니다. JSON 정책 문서에 대한 자세한 내용은 IAM 사용 설명서의 [JSON 정책 개요](#) 섹션을 참조하세요.

정책을 사용하여 관리자는 어떤 보안 주체가 어떤 리소스에 대해 어떤 조건에서 작업을 수행할 수 있는지 정의하여 누가 무엇을 액세스할 수 있는지 지정합니다.

기본적으로 사용자 및 역할에는 어떠한 권한도 없습니다. IAM 관리자는 IAM 정책을 생성하고 사용자가 수임할 수 있는 역할에 추가합니다. IAM 정책은 작업을 수행하기 위해 사용하는 방법과 관계없이 작업에 대한 권한을 정의합니다.

ID 기반 정책

ID 기반 정책은 ID(사용자, 사용자 그룹 또는 역할)에 연결하는 JSON 권한 정책 문서입니다. 이러한 정책은 자격 증명이 수행할 수 있는 작업, 대상 리소스 및 이에 관한 조건을 제어합니다. ID 기반 정책을 생성하는 방법을 알아보려면 IAM 사용 설명서에서 [고객 관리형 정책으로 사용자 지정 IAM 권한 정의](#)를 참조하세요.

ID 기반 정책은 인라인 정책(단일 ID에 직접 포함) 또는 관리형 정책(여러 ID에 연결된 독립 실행형 정책)일 수 있습니다. 관리형 정책 또는 인라인 정책을 선택하는 방법을 알아보려면 IAM 사용 설명서의 [관리형 정책 및 인라인 정책 중에서 선택](#) 섹션을 참조하세요.

리소스 기반 정책

리소스 기반 정책은 리소스에 연결하는 JSON 정책 설명서입니다. 예를 들어 IAM 역할 신뢰 정책 및 Amazon S3 버킷 정책이 있습니다. 리소스 기반 정책을 지원하는 서비스에서 서비스 관리자는 이러한 정책을 사용하여 특정 리소스에 대한 액세스를 통제할 수 있습니다. 리소스 기반 정책에서 [보안 주체를 지정](#)해야 합니다.

리소스 기반 정책은 해당 서비스에 있는 인라인 정책입니다. 리소스 기반 정책에서는 IAM의 AWS 관리형 정책을 사용할 수 없습니다.

기타 정책 유형

AWS는 보다 일반적인 정책 유형에서 부여한 최대 권한을 설정할 수 있는 추가 정책 유형을 지원합니다.

- 권한 경계 - ID 기반 정책에서 IAM 엔터티에 부여할 수 있는 최대 권한을 설정합니다. 자세한 정보는 IAM 사용 설명서의 [IAM 엔터티의 권한 범위](#)를 참조하세요.
- 서비스 제어 정책(SCP) - AWS Organizations내 조직 또는 조직 단위에 대한 최대 권한을 지정합니다. 자세한 내용은 AWS Organizations 사용 설명서의 [서비스 제어 정책](#)을 참조하세요.
- 리소스 제어 정책(RCP) - 계정의 리소스에 사용할 수 있는 최대 권한을 설정합니다. 자세한 내용은 AWS Organizations 사용 설명서의 [리소스 제어 정책\(RCP\)](#)을 참조하세요.
- 세션 정책 - 역할 또는 페더레이션 사용자에게 대해 임시 세션을 프로그래밍 방식으로 생성할 때 파라미터로 전달하는 고급 정책입니다. 자세한 내용은 IAM 사용 설명서의 [세션 정책](#)을 참조하세요.

여러 정책 유형

여러 정책 유형이 요청에 적용되는 경우, 결과 권한은 이해하기가 더 복잡합니다. 여러 정책 유형이 관련될 때 요청을 허용할지 여부를 AWS 결정하는 방법을 알아보려면 IAM 사용 설명서의 [정책 평가 로직](#)을 참조하세요.

AWS Network Security Manager와 IAM의 작동 방식

IAM을 사용하여 AWS Network Security Manager에 대한 액세스를 관리하기 전에 AWS Network Security Manager에서 사용할 수 있는 IAM 기능에 대해 알아봅니다.

IAM 특성	AWS Network Security Manager 지원
자격 증명 기반 정책	예
리소스 기반 정책	아니요
정책 작업	예
정책 리소스	예
정책 조건 키	예

IAM 특성	AWS Network Security Manager 지원
ACL	아니요
ABAC(정책의 태그)	예
임시 보안 인증	예
엔터티 권한	예
서비스 역할	예
서비스 연결 역할	예

AWS Network Security Manager 및 기타 AWS 서비스가 대부분의 IAM 기능과 작동하는 방식을 전체적으로 알아보려면 IAM 사용 설명서의 [AWS IAM으로 작업하는 서비스](#)를 참조하세요.

AWS Network Security Manager에 대한 자격 증명 기반 정책

ID 기반 정책 지원: 예

ID 기반 정책은 IAM 사용자, 사용자 그룹 또는 역할과 같은 ID에 연결할 수 있는 JSON 권한 정책 문서입니다. 이러한 정책은 사용자 및 역할이 어떤 리소스와 어떤 조건에서 어떤 작업을 수행할 수 있는지를 제어합니다. 자격 증명 기반 정책을 생성하는 방법을 알아보려면 IAM 사용 설명서에서 [고객 관리형 정책으로 사용자 지정 IAM 권한 정의](#)를 참조하세요.

IAM ID 기반 정책을 사용하면 허용되거나 거부되는 작업과 리소스뿐 아니라 작업이 허용되거나 거부되는 조건을 지정할 수 있습니다. JSON 정책에서 사용할 수 있는 모든 요소에 대해 알아보려면 IAM 사용 설명서의 [IAM JSON 정책 요소 참조](#)를 참조하세요.

AWS Network Security Manager 내의 리소스 기반 정책

리소스 기반 정책 지원: 아니요

리소스 기반 정책은 리소스에 연결하는 JSON 정책 설명서입니다. 리소스 기반 정책의 예제는 IAM 역할 신뢰 정책과 Amazon S3 버킷 정책입니다. 리소스 기반 정책을 지원하는 서비스에서 서비스 관리자는 이러한 정책을 사용하여 특정 리소스에 대한 액세스를 통제할 수 있습니다. 정책이 연결된 리소스의 경우 정책은 지정된 보안 주체가 해당 리소스와 어떤 조건에서 어떤 작업을 수행할 수 있는지를 정의합니다. 리소스 기반 정책에서 [보안 주체를 지정](#)해야 합니다. 보안 주체에는 계정, 사용자, 역할, 페더레이션 사용자 또는가 포함될 수 있습니다 AWS 서비스.

교차 계정 액세스를 활성화하려는 경우, 전체 계정이나 다른 계정의 IAM 개체를 리소스 기반 정책의 보안 주체로 지정할 수 있습니다. 자세한 내용은 IAM 사용 설명서의 [IAM에서 교차 계정 리소스 액세스](#)를 참조하세요.

AWS Network Security Manager는 리소스 기반 정책을 지원하지 않습니다.

AWS Network Security Manager에 대한 정책 작업

정책 작업 지원: 예

관리자는 AWS JSON 정책을 사용하여 누가 무엇에 액세스할 수 있는지 지정할 수 있습니다. 즉, 어떤 보안 주체가 어떤 리소스와 어떤 조건에서 작업을 수행할 수 있는지를 지정할 수 있습니다.

JSON 정책의 Action요소는 정책에서 액세스를 허용하거나 거부하는 데 사용할 수 있는 작업을 설명합니다. 연결된 작업을 수행할 수 있는 권한을 부여하기 위한 정책에 작업을 포함하세요.

AWS Network Security Manager 작업 목록을 보려면 서비스 승인 참조의 [AWS Network Security Manager에서 정의한 작업을](#) 참조하세요.

AWS Network Security Manager의 정책 작업은 작업 앞에 다음 접두사를 사용합니다.

```
network-security-manager
```

단일 문에서 여러 작업을 지정하려면 쉼표로 구분합니다.

```
"Action": [  
    "network-security-manager:action1",  
    "network-security-manager:action2"  
]
```

AWS Network Security Manager는 리소스 유형 전반에 걸쳐 IAM 작업을 정의합니다. 여기에는 스냅샷, 태그 지정, 관리, 동기화 상태 및 리소스 연결 작업과 함께 규칙, 템플릿, 정책, 범위 및 배포에 대한 CRUD(생성, 읽기, 업데이트 및 삭제) 작업이 포함됩니다.

AWS Network Security Manager에 대한 정책 리소스

정책 리소스 지원: 예

관리자는 AWS JSON 정책을 사용하여 누가 무엇에 액세스할 수 있는지 지정할 수 있습니다. 즉, 어떤 보안 주체가 어떤 리소스와 어떤 조건에서 작업을 수행할 수 있는지를 지정할 수 있습니다.

Resource JSON 정책 요소는 작업이 적용되는 하나 이상의 객체를 지정합니다. 모범 사례에 따라 [Amazon 리소스 이름\(ARN\)](#)을 사용하여 리소스를 지정합니다. 리소스 수준 권한을 지원하지 않는 작업의 경우, 와일드카드(*)를 사용하여 해당 문이 모든 리소스에 적용됨을 나타냅니다.

```
"Resource": "*"

```

AWS Network Security Manager 리소스 유형 및 해당 ARNs 목록을 보려면 서비스 권한 부여 참조의 [AWS Network Security Manager에서 정의한 리소스](#)를 참조하세요. 각 리소스의 ARN을 지정할 수 있는 작업을 알아보려면 [AWS Network Security Manager에서 정의한 작업](#)을 참조하세요.

AWS Network Security Manager는 각 리소스(규칙, 템플릿, 정책, 범위 및 배포)에 대한 IAM 리소스 유형과 각 리소스에 대한 스냅샷 유형(예:)을 정의합니다 rule-snapshot. ARN 형식은 다음과 같습니다.

```
arn:aws:network-security-manager:{region}:{account}:{resource-type}:{resource-id}

```

초안 ARNs이 추가:DRAFT되고 스냅샷 ARNs 버전 번호(예: :3)를 추가합니다.

초안은 별도의 IAM 리소스 유형이 아닙니다. 권한 부여를 위해 초안은 상위인 활성 리소스의 하위 항목으로 처리됩니다. 정규화:DRAFT된 ARN은 활성 리소스에 대해 권한을 부여하므로 초안에 대한 작업 권한은 해당 활성 리소스에 대한 작업 권한에서 가져옵니다.

스냅샷은 초안과 다릅니다. 각 스냅샷은 고유한 IAM 리소스 유형이므로 버전 검증 ARN은 상위 활성 리소스가 아닌 해당 스냅샷 리소스 유형에 대해 직접 권한을 부여합니다.

AWS Network Security Manager에 사용되는 정책 조건 키

서비스별 정책 조건 키 지원: 예

관리자는 AWS JSON 정책을 사용하여 누가 무엇에 액세스할 수 있는지 지정할 수 있습니다. 즉, 어떤 보안 주체가 어떤 리소스와 어떤 조건에서 작업을 수행할 수 있는지를 지정할 수 있습니다.

Condition 요소는 정의된 기준에 따라 문이 실행되는 시기를 지정합니다. 같음(equals) 또는 미만(less than)과 같은 [조건 연산자](#)를 사용하여 정책의 조건을 요청의 값과 일치시키는 조건식을 생성할 수 있습니다. 모든 AWS 전역 조건 키를 보려면 IAM 사용 설명서의 [AWS 전역 조건 컨텍스트 키](#)를 참조하세요.

AWS Network Security Manager 조건 키 목록을 보려면 서비스 권한 부여 참조의 [AWS Network Security Manager에 사용되는 조건 키](#)를 참조하세요. 조건 키를 사용할 수 있는 작업과 리소스를 알아보려면 [AWS Network Security Manager에서 정의한 작업](#)을 참조하세요.

AWS Network Security Manager는 속성 기반 액세스 제어(ABAC)를 위해 다음과 같은 AWS 전역 태그 조건 키를 지원합니다.

- `aws:ResourceTag/${TagKey}`
- `aws:RequestTag/${TagKey}`
- `aws:TagKeys`

태그 기반 조건 키는 활성 리소스 및 스냅샷에 적용됩니다. 초안 리소스에는 태그를 지정할 수 없으며 `aws:ResourceTag` 조건을 지원하지 않습니다.

AWS Network Security Manager ACLs

ACL 지원: 아니요

액세스 제어 목록(ACL)은 어떤 보안 주체(계정 멤버, 사용자 또는 역할)가 리소스에 액세스할 수 있는 권한을 가지고 있는지를 제어합니다. ACL은 JSON 정책 문서 형식을 사용하지 않지만 리소스 기반 정책과 유사합니다.

AWS Network Security Manager는 ACLs 제어 목록)을 지원하지 않습니다.

AWS Network Security Manager를 사용한 ABAC

ABAC 지원(정책의 태그): 예

속성 기반 액세스 제어(ABAC)는 태그라고 불리는 속성을 기반으로 권한을 정의하는 권한 부여 전략입니다. IAM 엔터티 및 AWS 리소스에 태그를 연결한 다음 보안 주체의 태그가 리소스의 태그와 일치할 때 작업을 허용하는 ABAC 정책을 설계할 수 있습니다.

태그에 근거하여 액세스를 제어하려면 `aws:ResourceTag/key-name`, `aws:RequestTag/key-name` 또는 `aws:TagKeys` 조건 키를 사용하여 정책의 [조건 요소](#)에 태그 정보를 제공합니다.

서비스가 모든 리소스 유형에 대해 세 가지 조건 키를 모두 지원하는 경우, 값은 서비스에 대해 예입니다. 서비스가 일부 리소스 유형에 대해서만 세 가지 조건 키를 모두 지원하는 경우, 값은 부분적입니다.

ABAC에 대한 자세한 내용은 IAM 사용 설명서의 [ABAC 권한 부여를 통한 권한 정의](#)를 참조하세요. ABAC 설정 단계가 포함된 자습서를 보려면 IAM 사용 설명서의 [속성 기반 액세스 제어\(ABAC\) 사용](#)을 참조하세요.

AWS Network Security Manager는 세 개의 AWS 글로벌 태그 조건 키를 모두 사용하여 속성 기반 액세스 제어를 지원합니다. 해당 리소스에 연결된 태그를 기반으로 AWS Network Security Manager 리소스에 대한 액세스를 제한할 수 있습니다.

AWS Network Security Manager에서 임시 자격 증명 사용

임시 자격 증명 지원: 예

임시 자격 증명은 AWS 리소스에 대한 단기 액세스를 제공하며 페더레이션을 사용하거나 역할을 전환할 때 자동으로 생성됩니다. 장기 액세스 키를 사용하는 대신 임시 자격 증명을 동적으로 생성하는 것이 AWS 좋습니다. 자세한 내용은 IAM 사용 설명서의 [IAM의 임시 보안 자격 증명](#) 및 [IAM으로 작업하는 AWS 서비스](#) 섹션을 참조하세요.

AWS Network Security Manager에 대한 교차 서비스 보안 주체 권한

전달 액세스 세션(FAS) 지원: 예

전달 액세스 세션(FAS)은 호출하는 보안 주체의 권한을 다운스트림 서비스에 AWS 서비스 대한 요청과 AWS 서비스 함께 사용합니다. FAS 요청 시 정책 세부 정보는 [전달 액세스 세션](#)을 참조하세요.

AWS Network Security Manager의 서비스 역할

서비스 역할 지원: 예

서비스 역할은 서비스가 사용자를 대신하여 작업을 수행하는 것으로 가정하는 [IAM 역할](#)입니다. IAM 관리자는 IAM 내에서 서비스 역할을 생성, 수정 및 삭제할 수 있습니다. 자세한 내용은 IAM 사용 설명서의 [AWS 서비스 AWS에 권한을 위임할 역할 생성](#)을 참조하세요.

Warning

서비스 역할에 대한 권한을 변경하면 AWS Network Security Manager 기능이 중단될 수 있습니다. AWS Network Security Manager가 관련 지침을 제공하는 경우에만 서비스 역할을 편집합니다.

AWS Network Security Manager의 서비스 연결 역할

서비스 연결 역할 지원: 예

서비스 연결 역할은 연결된 서비스 역할의 한 유형입니다. 서비스는 사용자를 대신하여 작업을 수행하기 위해 역할을 수입할 수 있습니다. 서비스 연결 역할은 표시 AWS 계정 되며 서비스가 소유합니다. IAM 관리자는 서비스 연결 역할의 권한을 볼 수 있지만 편집은 할 수 없습니다.

AWS Network Security Manager는 서비스 연결 역할을 사용하여 조직의 멤버 계정에서 작동합니다. AWS Network Security Manager는 서비스를 활성화하면 서비스 연결 역할을 자동으로 생성합니다. 역

할은 AWS Network Security Manager에 AWS WAF 및 AWS Shield Advanced 리소스를 관리할 수 있는 권한을 부여합니다. 또한이 역할은 리소스 검색을 위한 AWS Config에 대한 액세스 권한과 교차 계정 작업을 수행할 수 있는 권한을 부여합니다.

AWS Network Security Manager 서비스 연결 역할 생성 및 관리에 대한 자세한 내용은 섹션을 참조하세요 [the section called “서비스 연결 역할”](#).

AWS Network Security Manager의 자격 증명 기반 정책 예제

기본적으로 사용자 및 역할에는 AWS Network Security Manager 리소스를 생성하거나 수정할 수 있는 권한이 없습니다. 사용자에게 사용자가 필요한 리소스에서 작업을 수행할 권한을 부여하려면 IAM 관리자가 IAM 정책을 생성하면 됩니다.

이러한 예제 JSON 정책 문서를 사용하여 IAM ID 기반 정책을 생성하는 방법을 알아보려면 IAM 사용 설명서의 [IAM 정책 생성\(콘솔\)](#)을 참조하세요.

각 리소스 유형에 대한 ARNs 형식을 포함하여 AWS Network Security Manager에서 정의한 작업 및 리소스 유형에 대한 자세한 내용은 서비스 권한 부여 참조의 [AWS Network Security Manager에 사용되는 작업, 리소스 및 조건 키를 참조하세요](#).

주제

- [정책 모범 사례](#)
- [AWS Network Security Manager 콘솔 사용](#)
- [사용자가 자신의 고유한 권한을 볼 수 있도록 허용](#)
- [AWS Network Security Manager에 대한 읽기 전용 액세스](#)
- [규칙 및 템플릿만 관리](#)

정책 모범 사례

자격 증명 기반 정책에 따라 계정에서 사용자가 AWS Network Security Manager 리소스를 생성, 액세스 또는 삭제할 수 있는지 여부가 결정됩니다. 이 작업으로 인해 AWS 계정에 비용이 발생할 수 있습니다. ID 기반 정책을 생성하거나 편집할 때는 다음 지침과 권장 사항을 따르세요.

- AWS 관리형 정책을 시작하고 최소 권한으로 전환 - 사용자 및 워크로드에 권한 부여를 시작하려면 많은 일반적인 사용 사례에 대한 권한을 부여하는 AWS 관리형 정책을 사용합니다. 에서 사용할 수 있습니다 AWS 계정. 사용 사례에 맞는 AWS 고객 관리형 정책을 정의하여 권한을 추가로 줄이는 것이 좋습니다. 자세한 내용은 IAM 사용 설명서의 [AWS 관리형 정책](#) 또는 [AWS 직무에 대한 관리형 정책](#)을 참조하세요.

- 최소 권한 적용 – IAM 정책을 사용하여 권한을 설정하는 경우, 작업을 수행하는 데 필요한 권한만 부여합니다. 이렇게 하려면 최소 권한으로 알려진 특정 조건에서 특정 리소스에 대해 수행할 수 있는 작업을 정의합니다. IAM을 사용하여 권한을 적용하는 방법에 대한 자세한 정보는 IAM 사용 설명서에 있는 [IAM의 정책 및 권한](#)을 참조하세요.
- IAM 정책의 조건을 사용하여 액세스 추가 제한 – 정책에 조건을 추가하여 작업 및 리소스에 대한 액세스를 제한할 수 있습니다. 예를 들어, SSL을 사용하여 모든 요청을 전송해야 한다고 지정하는 정책 조건을 작성할 수 있습니다. AWS 서비스와 같은 특정을 통해 사용되는 경우 조건을 사용하여 서비스 작업에 대한 액세스 권한을 부여할 수도 있습니다 CloudFormation. 자세한 내용은 IAM 사용 설명서의 [IAM JSON 정책 요소: 조건](#)을 참조하세요.
- IAM Access Analyzer를 통해 IAM 정책을 확인하여 안전하고 기능적인 권한 보장 - IAM Access Analyzer에서는 IAM 정책 언어(JSON)와 모범 사례가 정책에서 준수되도록 새로운 및 기존 정책을 확인합니다. IAM Access Analyzer는 100개 이상의 정책 확인 항목과 실행 가능한 추천을 제공하여 안전하고 기능적인 정책을 작성하도록 돕습니다. 자세한 내용은 IAM 사용 설명서의 [IAM Access Analyzer에서 정책 검증](#)을 참조하세요.
- 다중 인증(MFA) 필요 -에서 IAM 사용자 또는 루트 사용자가 필요한 시나리오가 있는 경우 추가 보안을 위해 MFA를 AWS 계정칩니다. API 작업을 직접적으로 호출할 때 MFA가 필요하다면 정책에 MFA 조건을 추가합니다. 자세한 내용은 IAM 사용 설명서의 [MFA를 통한 보안 API 액세스](#)를 참조하세요.

IAM의 모범 사례에 대한 자세한 내용은 IAM 사용 설명서의 [IAM의 보안 모범 사례](#)를 참조하세요.

AWS Network Security Manager 콘솔 사용

AWS Network Security Manager 콘솔에 액세스하려면 최소 권한 집합이 있어야 합니다. 이러한 권한은에서 AWS Network Security Manager 리소스에 대한 세부 정보를 나열하고 볼 수 있도록 허용해야 합니다 AWS 계정. 최소 필수 권한보다 더 제한적인 ID 기반 정책을 생성하는 경우, 콘솔이 해당 정책에 연결된 엔티티(사용자 또는 역할)에 대해 의도대로 작동하지 않습니다.

AWS CLI 또는 AWS API만 호출하는 사용자에게는 최소 콘솔 권한을 허용할 필요가 없습니다. 대신, 수행하려는 API 작업과 일치하는 작업에만 액세스할 수 있도록 합니다.

AWS Network Security Manager 콘솔에 액세스하려면 보안 주체에게 `network-security-manager:List*` 및 `network-security-manager:Get*` 작업에 대한 최소 권한이 필요합니다.

사용자가 자신의 고유한 권한을 볼 수 있도록 허용

이 예제는 IAM 사용자가 자신의 사용자 ID에 연결된 인라인 및 관리형 정책을 볼 수 있도록 허용하는 정책을 생성하는 방법을 보여줍니다. 이 정책에는 콘솔에서 또는 AWS CLI 또는 AWS API를 사용하여 프로그래밍 방식으로이 작업을 완료할 수 있는 권한이 포함됩니다.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "ViewOwnUserInfo",
      "Effect": "Allow",
      "Action": [
        "iam:GetUserPolicy",
        "iam:ListGroupsForUser",
        "iam:ListAttachedUserPolicies",
        "iam:ListUserPolicies",
        "iam:GetUser"
      ],
      "Resource": ["arn:aws:iam::*:user/${aws:username}"]
    },
    {
      "Sid": "NavigateInConsole",
      "Effect": "Allow",
      "Action": [
        "iam:GetGroupPolicy",
        "iam:GetPolicyVersion",
        "iam:GetPolicy",
        "iam:ListAttachedGroupPolicies",
        "iam:ListGroupPolicies",
        "iam:ListPolicyVersions",
        "iam:ListPolicies",
        "iam:ListUsers"
      ],
      "Resource": "*"
    }
  ]
}
```

AWS Network Security Manager에 대한 읽기 전용 액세스

다음 정책은 보안 주체에게 모든 AWS Network Security Manager 리소스에 대한 읽기 전용 액세스 권한을 부여합니다. 이는 변경하지 않고 구성 및 동기화 상태를 확인해야 하는 감사자 또는 모니터링 역할에 유용합니다.

```
{
  "Version": "2012-10-17",
  "Statement": [
```

```

    {
      "Effect": "Allow",
      "Action": [
        "network-security-manager:Get*",
        "network-security-manager:List*"
      ],
      "Resource": "*"
    }
  ]
}

```

규칙 및 템플릿만 관리

다음 정책은 보안 주체가 정책, 범위 또는 배포에 대한 액세스 권한을 부여하지 않고 규칙 및 템플릿을 생성, 업데이트 및 삭제할 수 있도록 허용합니다. 이는 보안 구성을 작성하지만 적용을 제어하지 않는 팀에 유용합니다.

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "network-security-manager:CreateRule",
        "network-security-manager:GetRule",
        "network-security-manager:UpdateRule",
        "network-security-manager>DeleteRule",
        "network-security-manager:ListRules",
        "network-security-manager:CreateRuleSnapshot",
        "network-security-manager:ListRuleSnapshots",
        "network-security-manager:CreateTemplate",
        "network-security-manager:GetTemplate",
        "network-security-manager:UpdateTemplate",
        "network-security-manager>DeleteTemplate",
        "network-security-manager:ListTemplates",
        "network-security-manager:CreateTemplateSnapshot",
        "network-security-manager:ListTemplateSnapshots",
        "network-security-manager:TagResource",
        "network-security-manager:UntagResource",
        "network-security-manager:ListTagsForResource"
      ],
      "Resource": "*"
    }
  ]
}

```

```
    ]
}
```

AWS Network Security Manager 자격 증명 및 액세스 문제 해결

다음 정보를 사용하여 AWS Network Security Manager 및 IAM으로 작업할 때 발생할 수 있는 일반적인 문제를 진단하고 수정할 수 있습니다.

주제

- [AWS Network Security Manager에서 작업을 수행할 권한이 없음](#)
- [iam:PassRole을 수행하도록 인증되지 않음](#)
- [내 외부의 사람이 내 AWS Network Security Manager 리소스 AWS 계정 에 액세스하도록 허용하고 싶습니다.](#)

AWS Network Security Manager에서 작업을 수행할 권한이 없음

작업을 수행할 권한이 없다는 오류가 표시되면 작업을 수행할 수 있도록 정책을 업데이트해야 합니다.

다음의 예제 오류는 mateojackson IAM 사용자가 콘솔을 사용하여 가상 *my-example-widget* 리소스에 대한 세부 정보를 보려고 하지만 가상 network-security-manager:*GetWidget* 권한이 없을 때 발생합니다.

```
User: arn:aws:iam::123456789012:user/mateojackson is not authorized to perform:
network-security-manager:GetWidget on resource: my-example-widget
```

이 경우, network-security-manager:*GetWidget* 작업을 사용하여 *my-example-widget* 리소스에 액세스할 수 있도록 mateojackson 사용자 정책을 업데이트해야 합니다.

도움이 필요한 경우 AWS 관리자에게 문의하세요. 관리자는 로그인 자격 증명을 제공한 사람입니다.

iam:PassRole을 수행하도록 인증되지 않음

iam:PassRole 작업을 수행할 권한이 없다는 오류가 수신되면 AWS Network Security Manager에 역할을 전달할 수 있도록 정책을 업데이트해야 합니다.

일부 AWS 서비스에서는 새 서비스 역할 또는 서비스 연결 역할을 생성하는 대신 기존 역할을 해당 서비스에 전달할 수 있습니다. 이렇게 하려면 역할을 서비스에 전달할 권한이 있어야 합니다.

다음 예제 오류는 라는 IAM 사용자가 콘솔을 사용하여 AWS Network Security Manager에서 작업을 수행하려고 marymajor 할 때 발생합니다. 하지만 작업을 수행하려면 서비스 역할이 부여한 권한이 서비스에 있어야 합니다. Mary는 서비스에 역할을 전달할 권한이 없습니다.

```
User: arn:aws:iam::123456789012:user/marymajor is not authorized to perform:
iam:PassRole
```

이 경우, Mary가 iam:PassRole작업을 수행할 수 있도록 Mary의 정책을 업데이트해야 합니다.

도움이 필요한 경우 AWS 관리자에게 문의하세요. 관리자는 로그인 자격 증명을 제공한 사람입니다.

내 외부의 사람이 내 AWS Network Security Manager 리소스 AWS 계정 에 액세스하도록 허용하고 싶습니다.

다른 계정의 사용자 또는 조직 외부의 사람이 리소스에 액세스할 때 사용할 수 있는 역할을 생성할 수 있습니다. 역할을 수임할 신뢰할 수 있는 사람을 지정할 수 있습니다. 리소스 기반 정책 또는 액세스 제어 목록(ACL)을 지원하는 서비스의 경우, 이러한 정책을 사용하여 다른 사람에게 리소스에 대한 액세스 권한을 부여할 수 있습니다.

자세한 내용은 다음을 참조하세요.

- AWS Network Security Manager가 이러한 기능을 지원하는지 여부를 알아보려면 섹션을 참조하세요 [AWS Network Security Manager와 IAM의 작동 방식](#).
- 소유 AWS 계정 한의 리소스에 대한 액세스 권한을 제공하는 방법을 알아보려면 [IAM 사용 설명서의 소유한 다른의 IAM 사용자에게 액세스 권한 제공을 참조 AWS 계정 하세요](#).
- 리소스에 대한 액세스 권한을 타사에 제공하는 방법을 알아보려면 IAM 사용 설명서의 [타사 AWS 계정 소유에 대한 액세스 권한 제공을](#) AWS 계정참조하세요.
- ID 페더레이션을 통해 액세스 권한을 제공하는 방법을 알아보려면 IAM 사용 설명서의 [외부에서 인증된 사용자에게 액세스 권한 제공\(ID 페더레이션\)](#)을 참조하세요.
- 크로스 계정 액세스에 대한 역할과 리소스 기반 정책 사용의 차이점을 알아보려면 IAM 사용 설명서의 [IAM의 크로스 계정 리소스 액세스](#)를 참조하세요.

AWS Network Security Manager에 서비스 연결 역할 사용

AWS Network Security Manager는 IAM [서비스 연결 역할](#)을 사용합니다. 서비스 연결 역할은 AWS Network Security Manager에 직접 연결된 고유한 유형의 IAM 역할입니다. 서비스 연결 역할은 AWS

Network Security Manager에서 사전 정의하며 서비스가 사용자를 대신하여 다른 AWS 서비스를 호출하는 데 필요한 모든 권한을 포함합니다.

서비스 연결 역할을 사용하면 필요한 권한을 수동으로 추가할 필요가 없으므로 AWS Network Security Manager를 더 쉽게 설정할 수 있습니다. AWS Network Security Manager는 서비스 연결 역할의 권한을 정의합니다. 달리 정의되지 않은 한 AWS Network Security Manager만 해당 역할을 수임할 수 있습니다. 정의된 권한에는 신뢰 정책과 권한 정책이 포함됩니다. 다른 IAM 엔터티에는 해당 권한 정책을 연결할 수 없습니다.

관련 리소스를 처음 삭제한 후에만 서비스 연결 역할을 삭제할 수 있습니다. 이렇게 하면 리소스에 대한 액세스 권한을 실수로 제거할 수 없기 때문에 AWS Network Security Manager 리소스가 보호됩니다.

서비스 연결 역할을 지원하는 다른 서비스에 대한 자세한 내용은 [AWS IAM으로 작업하는 서비스를 참조](#)하고 서비스 연결 역할 열에서 예를 포함하는 서비스를 찾습니다. 해당 서비스에 대한 서비스 연결 역할 설명서를 보려면 예(Yes) 링크를 선택합니다.

AWS Network Security Manager에 대한 서비스 연결 역할 권한

AWS Network Security Manager는 라는 서비스 연결 역할을 사용합니다 `AWSServiceRoleForNetworkSecurityManager`. 이 서비스 연결 역할은 `network-security-manager.amazonaws.com` 서비스 보안 주체가 역할을 수임하도록 신뢰합니다.

라는 역할 권한 정책은 AWS Network Security Manager가 지정된 리소스에 대한 작업을 완료할 수 있도록 허용하는 관리형 AWS 정책 `NetworkSecurityManagerServiceRolePolicy`입니다.

다음 신뢰 정책은 `network-security-manager.amazonaws.com` 서비스 보안 주체가 역할을 수임하도록 허용합니다.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "network-security-manager.amazonaws.com"
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

}

Note

IAM 엔터티(사용자, 그룹, 역할 등)가 서비스 연결 역할을 생성하고 편집하거나 삭제할 수 있도록 권한을 구성할 수 있습니다. 자세한 내용은 IAM 사용 설명서의 [서비스 연결 역할 권한](#)을 참조하세요.

권한 세부 정보

AWS Network Security Manager는 계정 및 조직 전체에서 리소스를 보호하고 검색하려면 각 권한 그룹이 필요합니다. NetworkSecurityManagerServiceRolePolicy 관리형 정책은 서비스별로 그룹화된 다음 권한을 부여합니다.

- **wafv2** - 웹 ACLs. 웹 ACLs와 연결 및 연결 해제합니다. 웹 ACL 로깅 구성 및 규칙 그룹 권한 정책을 관리합니다. 리소스 태그 지정 및 해제 AWS Network Security Manager 웹 ACL 및 규칙 구성을 검증합니다.
- **shield** - AWS Shield Advanced 보호를 생성, 설명, 나열 및 삭제합니다. AWS Shield Advanced 구독을 생성하고 설명합니다.
- **elasticloadbalancing** - Application Load Balancer 및 태그를 설명합니다. Application Load Balancer에서 웹 ACL 연결을 생성, 삭제 및 설정합니다.
- **cloudfront** - Amazon CloudFront 배포, 구성 및 태그를 가져오고 나열합니다. 배포 웹 ACLs. VPC 오리진을 읽습니다.
- **apigateway** - Amazon API Gateway REST APIs. API 단계에서 웹 ACL을 설정합니다.
- **ec2** - Amazon EC2 Verified Access 인스턴스 웹 ACLs 및 연결을 읽습니다. AWS Shield Advanced 보호를 위한 탄력적 IP 주소를 설명합니다.
- **cognito-idp, apprunner, amplify, 및 appsyncbedrock-agentcore** - AWS Network Security Manager가 보호된 리소스를 검색할 수 있도록 Amazon Cognito 사용자 풀, AWS App Runner 서비스, AWS AppSync GraphQL APIs, AWS Amplify 앱 및 Amazon Bedrock AgentCore 게이트웨이에 대한 웹 ACL 연결을 읽습니다.
- **config** - 리소스 구성을 선택하고 AWS Network Security Manager가 범위 내 리소스를 검색하는데 사용하는 서비스 연결 AWS Config 구성 레코더를 관리합니다.
- **organizations** - AWS Network Security Manager가 조직 전체에서 운영할 수 있도록 조직, 계정, 루트, 조직 단위 및 위임된 관리자를 읽습니다.
- **logs** - 웹 ACL 로깅을 위한 로그 전송을 생성, 읽기, 업데이트, 삭제 및 나열합니다.

- s3 - 웹 ACL 로그를 전송할 수 aws-waf-logs- 있도록 이름이 로 시작하는 Amazon S3 버킷에 버킷 정책을 가져오고 배치합니다.
- iam - iam:AWSServiceName 조건 키로 범위가 지정된 AWS Shield Advanced AWS Config 및 AWS WAF에 필요한 서비스 연결 역할을 생성합니다.

다음 JSON은 전체 NetworkSecurityManagerServiceRolePolicy 권한 정책을 보여줍니다.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "LogsGeneral",
      "Effect": "Allow",
      "Action": [
        "logs:ListLogDeliveries",
        "logs:CreateLogDelivery",
        "logs:GetLogDelivery",
        "logs:UpdateLogDelivery",
        "logs>DeleteLogDelivery"
      ],
      "Resource": "*"
    },
    {
      "Sid": "S3LogBucketGeneral",
      "Effect": "Allow",
      "Action": [
        "s3:GetBucketPolicy",
        "s3:PutBucketPolicy"
      ],
      "Resource": "arn:aws:s3:::aws-waf-logs-*"
    },
    {
      "Sid": "CloudfrontVpcOriginAccess",
      "Effect": "Allow",
      "Action": [
        "cloudfront:GetVpcOrigin"
      ],
      "Resource": "arn:aws:cloudfront::*:vpccorigin/*"
    },
    {
      "Sid": "ConfigUnscoped",
      "Effect": "Allow",

```

```

    "Action": [
      "config:SelectResourceConfig"
    ],
    "Resource": "*"
  },
  {
    "Sid": "DescribeOrganizationUnScoped",
    "Effect": "Allow",
    "Action": [
      "organizations:DescribeOrganization",
      "organizations:ListAccounts",
      "organizations:ListChildren",
      "organizations:ListRoots",
      "organizations:ListParents",
      "organizations:ListOrganizationalUnitsForParent",
      "organizations:ListAWSServiceAccessForOrganization"
    ],
    "Resource": "*"
  },
  {
    "Sid": "DescribeAccountScoped",
    "Effect": "Allow",
    "Action": "organizations:DescribeAccount",
    "Resource": "arn:aws:organizations::*:account/o-*/*"
  },
  {
    "Sid": "DescribeOrganizationUnitScoped",
    "Effect": "Allow",
    "Action": "organizations:DescribeOrganizationalUnit",
    "Resource": "arn:aws:organizations::*:ou/o-*/ou-*"
  },
  {
    "Sid": "ListDelegatedAdministratorsScoped",
    "Effect": "Allow",
    "Action": "organizations:ListDelegatedAdministrators",
    "Resource": "*",
    "Condition": {
      "StringEquals": {
        "organizations:ServicePrincipal": [
          "network-security-manager.amazonaws.com"
        ]
      }
    }
  }
],

```

```

{
  "Sid": "LoadBalancerNonMutationApiAccess",
  "Effect": "Allow",
  "Action": [
    "elasticloadbalancing:DescribeLoadBalancers",
    "elasticloadbalancing:DescribeTags",
    "elasticloadbalancing:DescribeWebACLAssociation"
  ],
  "Resource": "*"
},
{
  "Sid": "LoadBalancerGetWebACLScoped",
  "Effect": "Allow",
  "Action": "elasticloadbalancing:GetLoadBalancerWebACL",
  "Resource": "arn:aws:elasticloadbalancing:*:*:loadbalancer/app/*/*"
},
{
  "Sid": "CloudFrontDistributionNonMutationApiAccess",
  "Effect": "Allow",
  "Action": [
    "cloudfront:GetDistribution",
    "cloudfront:GetDistributionConfig",
    "cloudfront:ListTagsForResource"
  ],
  "Resource": "arn:aws:cloudfront:*:*:distribution/*"
},
{
  "Sid": "ApiGatewayStageNonMutationApiAccess",
  "Effect": "Allow",
  "Action": "apigateway:GET",
  "Resource": [
    "arn:aws:apigateway:*:*/restapis",
    "arn:aws:apigateway:*:*/restapis/*/stages",
    "arn:aws:apigateway:*:*/restapis/*/stages/*",
    "arn:aws:apigateway:*:*/tags/*"
  ]
},
{
  "Sid": "Wafv2General",
  "Effect": "Allow",
  "Action": [
    "wafv2:TagResource",
    "wafv2:ListResourcesForWebACL",
    "wafv2:AssociateWebACL",

```

```

        "wafv2:ListTagsForResource",
        "wafv2:UntagResource",
        "wafv2:GetWebACL",
        "wafv2:DisassociateFirewallManager",
        "wafv2:DeleteWebACL",
        "wafv2:DisassociateWebACL",
        "wafv2:ValidateNetworkSecurityManagerWebACLConfiguration",
        "wafv2:ValidateNetworkSecurityManagerRuleConfiguration"
    ],
    "Resource": "arn:aws:wafv2:*:*:*/*webacl/*"
},
{
    "Sid": "Wafv2WebAclAndRuleGroupMutation",
    "Effect": "Allow",
    "Action": [
        "wafv2:UpdateWebACL",
        "wafv2:CreateWebACL",
        "wafv2:DeleteFirewallManagerRuleGroups",
        "wafv2:PutFirewallManagerRuleGroups"
    ],
    "Resource": [
        "arn:aws:wafv2:*:*:*/*webacl/*",
        "arn:aws:wafv2:*:*:*global/rulegroup/*",
        "arn:aws:wafv2:*:*:*regional/rulegroup/*",
        "arn:aws:wafv2:*:*:*global/managedruleset/*",
        "arn:aws:wafv2:*:*:*regional/managedruleset/*",
        "arn:aws:wafv2:*:*:*global/ipset/*",
        "arn:aws:wafv2:*:*:*regional/ipset/*",
        "arn:aws:wafv2:*:*:*global/regexpatternset/*",
        "arn:aws:wafv2:*:*:*regional/regexpatternset/*"
    ]
},
{
    "Sid": "Wafv2Logging",
    "Effect": "Allow",
    "Action": [
        "wafv2:PutLoggingConfiguration",
        "wafv2:GetLoggingConfiguration",
        "wafv2>DeleteLoggingConfiguration"
    ],
    "Resource": "arn:aws:wafv2:*:*:*/*webacl/*"
},
{
    "Sid": "Wafv2ListLogging",

```

```

    "Effect": "Allow",
    "Action": "wafv2:ListLoggingConfigurations",
    "Resource": "*"
  },
  {
    "Sid": "Wafv2ListWebACLs",
    "Effect": "Allow",
    "Action": "wafv2:ListWebACLs",
    "Resource": "*"
  },
  {
    "Sid": "Wafv2PermissionPolicy",
    "Effect": "Allow",
    "Action": [
      "wafv2:PutPermissionPolicy",
      "wafv2:GetPermissionPolicy",
      "wafv2>DeletePermissionPolicy"
    ],
    "Resource": [
      "arn:aws:wafv2:*:*:global/rulegroup/*",
      "arn:aws:wafv2:*:*:regional/rulegroup/*"
    ]
  },
  {
    "Sid": "Wafv2WebaclDescribe",
    "Effect": "Allow",
    "Action": "wafv2:GetWebACLForResource",
    "Resource": "arn:aws:wafv2:*:*:*/*webacl/*"
  },
  {
    "Sid": "CloudFrontListDistributions",
    "Effect": "Allow",
    "Action": [
      "cloudfront:ListDistributionsByWebACLId",
      "cloudfront:ListDistributions"
    ],
    "Resource": "*"
  },
  {
    "Sid": "CloudFrontDistributionMutation",
    "Effect": "Allow",
    "Action": [
      "cloudfront:AssociateDistributionWebACL",
      "cloudfront:DisassociateDistributionWebACL"
    ]
  }

```

```

    ],
    "Resource": "arn:aws:cloudfront::*:distribution/*"
  },
  {
    "Sid": "ElbWebAclRemediationScoped",
    "Effect": "Allow",
    "Action": [
      "elasticloadbalancing:CreateWebACLAssociation",
      "elasticloadbalancing>DeleteWebACLAssociation"
    ],
    "Resource": "arn:aws:elasticloadbalancing::*:loadbalancer/app/*/*"
  },
  {
    "Sid": "ElbSetWebAcl",
    "Effect": "Allow",
    "Action": "elasticloadbalancing:SetWebACL",
    "Resource": "*"
  },
  {
    "Sid": "ApiGatewayWebAclRemediation",
    "Effect": "Allow",
    "Action": "apigateway:SetWebACL",
    "Resource": "arn:aws:apigateway::*/restapis/*/stages/*"
  },
  {
    "Sid": "CognitoWebAclIntegration",
    "Effect": "Allow",
    "Action": [
      "cognito-idp:GetWebACLForResource",
      "cognito-idp:ListResourcesForWebACL"
    ],
    "Resource": "*"
  },
  {
    "Sid": "AppRunnerWebAclIntegration",
    "Effect": "Allow",
    "Action": [
      "apprunner:DescribeWebAclForService",
      "apprunner:ListAssociatedServicesForWebAcl"
    ],
    "Resource": "*"
  },
  {
    "Sid": "VerifiedAccessWebAclIntegration",

```

```

    "Effect": "Allow",
    "Action": [
        "ec2:GetVerifiedAccessInstanceWebAcl",
        "ec2:DescribeVerifiedAccessInstanceWebAclAssociations"
    ],
    "Resource": "*"
},
{
    "Sid": "AppSyncWebAclIntegration",
    "Effect": "Allow",
    "Action": [
        "appsync:GetWebACLForResource",
        "appsync:ListResourcesForWebACL"
    ],
    "Resource": "*"
},
{
    "Sid": "AmplifyWebAclIntegration",
    "Effect": "Allow",
    "Action": [
        "amplify:GetWebACLForResource",
        "amplify:ListResourcesForWebACL"
    ],
    "Resource": "*"
},
{
    "Sid": "ShieldGeneral",
    "Effect": "Allow",
    "Action": [
        "shield:CreateProtection",
        "shield:DeleteProtection",
        "shield:DescribeProtection",
        "shield:ListProtections",
        "shield:CreateSubscription",
        "shield:DescribeSubscription",
        "shield:GetSubscriptionState",
        "ec2:DescribeAddresses",
        "elasticloadbalancing:DescribeLoadBalancers",
        "elasticloadbalancing:DescribeTags"
    ],
    "Resource": "*"
},
{
    "Sid": "ShieldSlrCreation",

```

```

    "Effect": "Allow",
    "Action": "iam:CreateServiceLinkedRole",
    "Resource": "arn:aws:iam::*:role/aws-service-role/shield.amazonaws.com/*",
    "Condition": {
      "StringEquals": {
        "iam:AWSServiceName": "shield.amazonaws.com"
      }
    }
  },
  {
    "Sid": "AllowConfigRecorderList",
    "Effect": "Allow",
    "Action": "config:ListConfigurationRecorders",
    "Resource": "*"
  },
  {
    "Sid": "AllowPutServiceLinkedConfigRecorder",
    "Effect": "Allow",
    "Action": "config:PutServiceLinkedConfigurationRecorder",
    "Resource": "*"
  },
  {
    "Sid": "AllowConfigRecorderScopedAccess",
    "Effect": "Allow",
    "Action": [
      "config:DescribeConfigurationRecorders",
      "config:DescribeConfigurationRecorderStatus",
      "config>DeleteServiceLinkedConfigurationRecorder",
      "config:AssociateResourceTypes",
      "config:DisassociateResourceTypes"
    ],
    "Resource": "arn:aws:config::*:configuration-recorder/*"
  },
  {
    "Sid": "AllowCreateConfigServiceLinkedRole",
    "Effect": "Allow",
    "Action": "iam:CreateServiceLinkedRole",
    "Resource": "arn:aws:iam::*:role/aws-service-role/config.amazonaws.com/*",
    "Condition": {
      "StringEquals": {
        "iam:AWSServiceName": "config.amazonaws.com"
      }
    }
  }
},

```

```

{
  "Sid": "AllowListActionsForAgentCoreGateway",
  "Effect": "Allow",
  "Action": [
    "bedrock-agentcore:GatewayListResourcesForWebACL"
  ],
  "Resource": "*"
},
{
  "Sid": "AllowGetActionForAgentCoreGateway",
  "Effect": "Allow",
  "Action": [
    "bedrock-agentcore:GatewayGetWebACLForResource"
  ],
  "Resource": "arn:aws:bedrock-agentcore:*:*:gateway/*"
},
{
  "Sid": "WafV2LoggingSlrCreation",
  "Effect": "Allow",
  "Action": "iam:CreateServiceLinkedRole",
  "Resource": "arn:aws:iam:*:*:role/aws-service-role/wafv2.amazonaws.com/*",
  "Condition": {
    "StringEquals": {
      "iam:AWSServiceName": "wafv2.amazonaws.com"
    }
  }
}
]
}

```

AWS Network Security Manager에 대한 서비스 연결 역할 생성

서비스 연결 역할은 수동으로 생성할 필요가 없습니다. AWS Network Security Manager를 활성화하면 AWS Network Security Manager가 서비스 연결 역할을 생성합니다. 수행할 수동 단계는 없습니다.

이 서비스 연결 역할을 삭제한 다음 다시 생성해야 하는 경우 다음에 서비스를 사용할 때 AWS Network Security Manager가 역할을 다시 생성합니다. 별도의 조치를 취하지 않아도 됩니다.

자세한 내용은 IAM 사용자 설명서의 [서비스 연결 역할 생성](#) 섹션을 참조하세요.

AWS Network Security Manager에 대한 서비스 연결 역할 편집

AWSServiceRoleForNetworkSecurityManager 서비스 연결 역할의 권한은 변경할 수 없습니다. 서비스 연결 역할을 생성한 후에는 다양한 엔터티가 역할을 참조할 수 있기 때문에 역할 이름을 변경할 수 없습니다. 하지만 IAM을 사용하여 역할의 설명을 편집할 수 있습니다.

자세한 내용은 IAM 사용자 설명서의 [서비스 연결 역할 편집](#)을 참조하세요.

AWS Network Security Manager에 대한 서비스 연결 역할 삭제

AWS Network Security Manager를 더 이상 사용할 필요가 없는 경우

AWSServiceRoleForNetworkSecurityManager 서비스 연결 역할을 삭제하는 것이 좋습니다.

서비스 연결 역할을 삭제하기 전에 AWS Network Security Manager가 관리하는 리소스를 정리합니다. AWS Network Security Manager를 비활성화하고 AWS Network Security Manager가 관리하는 리소스가 계정에 남아 있지 않도록 정책 및 범위를 제거합니다. 그런 다음 역할을 수동으로 삭제할 수 있습니다.

Note

리소스를 삭제하려고 할 때 AWS Network Security Manager가 역할을 사용하는 경우 삭제에 실패할 수 있습니다. 이 문제가 발생하면 몇 분 기다렸다가 작업을 다시 시도하세요.

IAM을 사용하여 수동으로 서비스 연결 역할을 삭제하려면 다음을 수행하세요.

1. IAM 콘솔(<https://console.aws.amazon.com/iam/>)을 엽니다.
2. 탐색 창에서 역할을 선택합니다.
3. 검색 상자에 AWSServiceRoleForNetworkSecurityManager를 입력한 다음 역할을 선택합니다.
4. 삭제를 선택합니다.
5. 삭제를 확인하려면 역할 이름을 입력한 다음 삭제를 선택합니다.

자세한 내용은 IAM 사용 설명서의 [서비스 연결 역할 삭제](#)를 참조하세요.

AWS Network Security Manager 서비스 연결 역할에 지원되는 리전

AWS Network Security Manager는 AWS Network Security Manager를 사용할 수 있는 모든 AWS 리전에서 서비스 연결 역할 사용을 지원합니다.

AWS Network Security Manager에 대한 규정 준수 검증

새로운 AWS 가입 환경은 규제 워크로드용으로 설계되지 않았습니다. 새로운 AWS 가입 환경을 사용하고 있지만 규제 대상 워크로드 AWS 에를 사용하려는 경우 AWS 환경에 대한 고급 기능에 [가입 AWS \(고급\)](https://docs.aws.amazon.com/accounts/latest/reference/activate-advanced-features.html)하거나 활성화할 수 있습니다. <https://docs.aws.amazon.com/accounts/latest/reference/activate-advanced-features.html>

AWS 서비스 가 특정 규정 준수 프로그램의 범위 내에 있는지 알아보려면 [AWS 서비스 규정 준수 프로그램 범위 내](#)를 참조하고 관심 있는 규정 준수 프로그램을 선택합니다. 일반 정보는 [AWS 규정 준수 프로그램](#).

를 사용하여 타사 감사 보고서를 다운로드할 수 있습니다 AWS Artifact. 자세한 내용은 [에서 보고서 다운로드 AWS Artifact](#)에서 .

사용 시 규정 준수 책임은 데이터의 민감도, 회사의 규정 준수 목표 및 관련 법률과 규정에 따라 AWS 서비스 결정됩니다. 사용 시 규정 준수 책임에 대한 자세한 내용은 [AWS 보안 설명서를](#) AWS 서비스 참조하세요.

AWS Network Security Manager의 복원력

AWS 글로벌 인프라는 AWS 리전 및 가용 영역을 중심으로 구축됩니다.는 물리적으로 분리되고 격리된 여러 가용 영역을 AWS 리전 제공하며,이 가용 영역은 지연 시간이 짧고 처리량이 높으며 중복성이 높은 네트워킹과 연결됩니다. 가용 영역을 사용하면 중단 없이 영역 간에 자동으로 장애 극복 조치가 이루어지는 애플리케이션 및 데이터베이스를 설계하고 운영할 수 있습니다. 가용 영역은 기존의 단일 또는 다중 데이터 센터 인프라보다 가용성, 내결함성, 확장성이 뛰어납니다.

AWS 리전 및 가용 영역에 대한 자세한 내용은 [AWS 글로벌 인프라를](#) 참조하세요.

AWS 글로벌 인프라 외에도 AWS Network Security Manager는 데이터 복원성과 백업 요구 사항을 지원하는 데 도움이 되는 몇 가지 기능을 제공합니다.

AWS Network Security Manager의 인프라 보안

관리형 서비스인 AWS Network Security Manager는 [Amazon Web Services: 보안 프로세스 개요](#) 백서에 설명된 AWS 글로벌 네트워크 보안 절차로 보호됩니다.

AWS 게시된 API 호출을 사용하여 네트워크를 통해 AWS Network Security Manager에 액세스합니다. 클라이언트가 전송 계층 보안(TLS) 1.0 이상을 지원해야 합니다. TLS 1.2 이상을 권장합니다. 클라이언

언트는 DHE(Ephemeral Diffie-Hellman) 또는 ECDHE(Elliptic Curve Ephemeral Diffie-Hellman)와 같은 완전 전송 보안(PFS)이 포함된 암호 제품군도 지원해야 합니다. Java 7 이상의 최신 시스템은 대부분 이러한 모드를 지원합니다.

또한 요청은 액세스 키 ID 및 IAM 위탁자와 관련된 시크릿 액세스 키를 사용하여 서명해야 합니다. 또는 [AWS Security Token Service](#)(AWS STS)를 사용하여 임시 보안 자격 증명을 생성하여 요청에 서명할 수 있습니다.

AWS Network Security Manager의 보안 모범 사례

다음 모범 사례는 안전한 AWS Network Security Manager 구성을 유지하는 데 도움이 됩니다.

예방 제어

- IAM 최소 권한 사용 - 각 사용자 또는 역할이 AWS Network Security Manager 작업을 수행하는 데 필요한 권한만 부여합니다. 가능하면 IAM 조건 키를 사용하여 특정 리소스에 대한 액세스를 제한합니다.
- 서비스 연결 역할 사용 - AWS Network Security Manager는 서비스 연결 역할을 사용하여 사용자를 대신하여 작업을 수행합니다. 이러한 역할에는 필요한 최소 액세스 범위로 사전 정의된 권한이 있습니다.
- 범위를 신중하게 구성 - 보호가 필요한 계정 및 리소스 유형만 대상으로 하는 범위 구성을 정의합니다. 범위가 너무 넓으면 의도하지 않은 적용이 발생할 수 있습니다.

탐지 제어

- AWS CloudTrail 로깅 활성화 -- CloudTrail은 모든 AWS Network Security Manager API 호출을 기록합니다. 이러한 로그를 검토하여 보안 구성을 변경한 사람과 시기를 감사합니다.
- 동기화 상태 모니터링 - 배포의 동기화 상태를 정기적으로 확인하여 의도한 보안 태세와 동기화되지 않은 리소스를 식별합니다.

AWS Network Security Manager 모니터링

AWS Network Security Manager를 모니터링하면 리소스가 의도한 대로 보호되는지 여부를 이해하는데 도움이 됩니다. AWS Network Security Manager는 다음과 같은 모니터링 기능을 제공합니다.

- 동기화 상태 APIs - 배포 전반에 걸쳐 개별 리소스의 보호 상태를 쿼리합니다.
- AWS CloudTrail - 감사, 규정 준수 및 운영 문제 해결을 위한 모든 AWS Network Security Manager API 호출을 기록합니다.

동기화 상태 모니터링

리소스 보호 여부를 모니터링하는 주요 방법은 동기화 상태 APIs를 통하는 것입니다. AWS Network Security Manager는 범위 내 각 리소스를 평가하고 실제 방화벽 구성이 의도한 구성과 일치하는지 여부를 기록합니다.

동기화 상태 작업

AWS Network Security Manager는 동기화 상태를 쿼리하기 위한 두 가지 작업을 제공합니다.

ListResourceSynchronizationStatuses

특정 배포에 대한 리소스당 상태를 반환합니다. `deploymentIdentifier` 파라미터가 필요합니다. 선택적으로 `synchronizationStatus` (IN_SYNC, OUT_OF_SYNC 또는 NOT_APPLICABLE)을 기준으로 필터링합니다.

ListAggregateResourceSynchronizationStatuses

모든 배포에서 리소스별 집계 상태를 반환합니다. 선택적으로를 기준으로 필터링합니다 `synchronizationStatus`. 이 작업은 각 리소스에 적용되는 모든 정책의 결합된 결과를 보여줍니다.

두 작업 모두 `maxResults` (1~100) 및를 사용한 페이지 매김을 지원합니다 `nextToken`.

동기화 상태 값 이해

IN_SYNC

리소스의 실제 방화벽 구성은 적용 가능한 모든 정책에서 계산된 유효 구성과 일치합니다.

OUT_OF_SYNC

리소스의 실제 구성은 유효 구성과 다릅니다. `outOfSyncReasons` 필드는 예상 값과 실제 값을 비교하여 설정별 세부 정보를 제공합니다.

NOT_APPLICABLE

리소스의 계정 및 리소스 유형이 범위 내에 있지만 리소스 자체가 범위 필터와 일치하지 않습니다 (예: 태그 필터에서 제외). 별도의 작업은 필요없습니다.

리소스가 결과에 전혀 나타나지 않는 경우 계정 또는 리소스 유형은 배포 범위에 포함되지 않습니다. 범위 구성을 확인합니다.

평가 타임스탬프 이해

각 동기화 상태 항목에는 두 개의 타임스탬프가 포함됩니다.

- `evaluatedAt` - Network AWS Security Manager가 리소스의 구성을 마지막으로 평가한 시간입니다. 기한 경과 `evaluatedAt` 값은 최근 변경 사항에 대한 평가가 아직 실행되지 않았음을 나타냅니다.
- `updatedAt` - 동기화 상태 레코드 자체가 마지막으로 변경된 시간입니다. `updatedAt`가 보다 오래된 경우 마지막 평가 이후 `evaluatedAt` 상태가 안정적이었습니다.

교차 계정 가시성

여러 관리자가 동일한 리소스를 보호하는 경우 집계 동기화 상태에 대한 가시성은 각 배포의 `enableCrossAccountVisibility` 설정에 따라 달라집니다.

- 리소스를 포함하는 모든 배포에 교차 계정 가시성이 활성화된 경우 모든 관리자는 전체 집계 상태와 out-of-sync 이유를 볼 수 있습니다.
- 배포에 교차 계정 가시성이 비활성화된 경우 다른 관리자에게는 자세한 이유 대신 `NOT_VISIBLE` 마커가 표시됩니다. 이는 다른 관리자가 리소스를 보호하지만 가시성을 공유하지 않았음을 나타냅니다.

out-of-sync 리소스 진단

리소스가 `OUT_OF_SYNC`를 보고하면 `outOfSyncReasons` 필드는 특정 구성 차이를 식별합니다. 최상위 이유는 다음 중 하나입니다.

- `missingFirewall` -- 리소스와 연결된 방화벽 보호가 없습니다.
- `invalidFirewall` -- 방화벽이 존재하지만 구성이 기대치와 일치하지 않습니다. 특정 차이점은 분류된 버킷에 나열되어 있습니다.

문제 해결이 활성화되었지만 리소스를 수정할 수 없는 경우 `remediationIssues` 필드는 문제를 수동으로 해결하는 방법에 대한 지침을 `correctiveAction`에 제공합니다. 문제 해결은 기본적으로 꺼져 있는 정책 수준 설정입니다. 자세한 내용은 [the section called “동기화 및 문제 해결”](#) 섹션을 참조하세요.

구성이 다른 여러 배포는 동일한 리소스를 대상으로 할 수 있습니다. 이 경우 배포당 동기화 상태는 `OUT_OF_SYNC`이고 집계 동기화 상태는 `IN_SYNC`일 수 있습니다. 이는 장애가 아닌 예상되는 동작입니다. 병합하는 동안 우선 순위가 더 높은 정책의 설정이 우선했습니다. 따라서 리소스는 우선 순위가 낮은 배포의 구성과 일치하지 않더라도 유효 구성과 일치합니다.

를 사용하여 AWS Network Security Manager API 호출 로깅 AWS CloudTrail

AWS Network Security Manager는 사용자 AWS CloudTrail, 역할 또는 서비스가 수행한 작업에 대한 레코드를 제공하는 AWS 서비스와 통합됩니다. CloudTrail은 AWS Network Security Manager에 대한 모든 API 호출을 관리 이벤트로 캡처합니다. 캡처되는 호출에는 AWS Network Security Manager 콘솔의 호출과 AWS Network Security Manager API 작업에 대한 프로그래밍 방식의 호출이 포함됩니다.

추적을 생성하면 AWS Network Security Manager에 대한 이벤트를 포함하여 CloudTrail 이벤트를 지속적으로 Amazon S3 버킷에 배포할 수 있습니다. 트레일을 구성하지 않은 경우에도 CloudTrail 콘솔의 이벤트 기록에서 최신 이벤트를 볼 수 있습니다. 자세한 정보는 [AWS CloudTrail 사용 설명서](#)를 참조하세요.

AWS CloudTrail의 Network Security Manager 정보

CloudTrail은 계정을 생성할 AWS 계정 때에서 활성화됩니다. AWS Network Security Manager에서 활동이 발생하면 해당 활동이 이벤트 기록의 다른 AWS 서비스 이벤트와 함께 CloudTrail 이벤트에 기록됩니다. 에서 최근 이벤트를 보고 검색하고 다운로드할 수 있습니다 AWS 계정. 자세한 내용은 [CloudTrail 이벤트 기록을 사용하여 이벤트 보기](#)를 참조하세요.

AWS Network Security Manager에 대한 이벤트를 AWS 계정포함하여에 이벤트를 지속적으로 기록하려면 추적을 생성합니다. CloudTrail은 추적을 사용하여 Amazon S3 버킷으로 로그 파일을 전송할 수

있습니다. 콘솔에서 트레일을 생성하면 기본적으로 모든 AWS 리전에 트레일이 적용됩니다. 추적은 파티션에 있는 모든 리전의 AWS 이벤트를 로깅합니다. 지정한 Amazon S3 버킷으로 로그 파일을 전송합니다. CloudTrail 로그에서 수집된 이벤트 데이터를 추가로 분석하고 조치를 취하도록 다른 AWS 서비스를 구성할 수 있습니다. 자세한 내용은 다음 자료를 참조하세요.

- [추적 생성 개요](#)
- [CloudTrail 지원 서비스 및 통합](#)
- [CloudTrail에 대한 Amazon SNS 알림 구성](#)

모든 AWS Network Security Manager 작업은 CloudTrail에서 로깅됩니다. 퍼블릭 작업에는 다음이 포함됩니다.

- 규칙, 템플릿, 정책, 범위 및 배포에 대한 CRUD(CruD) 작업 생성, 읽기, 업데이트 및 삭제
- 스냅샷 작업
- 태그 지정 작업
- 관리자 계정 작업
- 동기화 상태 작업
- 리소스 연결 작업
- 규칙 생성 작업

모든 이벤트 항목에는 다음 정보가 포함됩니다.

- 이벤트 소스: `network-security-manager.amazonaws.com`
- 이벤트 이름, 즉 API 작업 이름(예: `CreatePolicy` 또는 `ListDeployments`)
- 영향을 받는 리소스, ARN 및 리소스 유형으로 식별됨

읽기 전용 작업(예: `GetPolicy`, `ListRules` 및 `ListResourceSynchronizationStatuses`)은와 함께 로깅 `readOnly: true`되며 응답 요소를 포함하지 않습니다. 변형 작업에는 요청 파라미터 및 응답 요소가 포함됩니다.

Note

CloudTrail은 이벤트 레코드에서 민감한 필드를 수정합니다. 예를 들어 CloudTrail은 `GenerateRuleConfiguration` 작업에서 `prompt` 파라미터를 수정합니다.

예: CreatePolicy 이벤트

다음 예제는 CreatePolicy 작업에 대한 CloudTrail 로그 항목을 보여줍니다.

```
{
  "eventVersion": "1.09",
  "userIdentity": {
    "type": "AssumedRole",
    "principalId": "AROEXAMPLEID:my-session",
    "arn": "arn:aws:sts::123456789012:assumed-role/AdminRole/my-session",
    "accountId": "123456789012",
    "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
    "sessionContext": {
      "sessionIssuer": {
        "type": "Role",
        "principalId": "AROEXAMPLEID",
        "arn": "arn:aws:iam::123456789012:role/AdminRole",
        "accountId": "123456789012",
        "userName": "AdminRole"
      },
      "attributes": {
        "creationDate": "2026-08-10T18:22:41Z",
        "mfaAuthenticated": "false"
      }
    }
  },
  "eventTime": "2026-08-10T18:24:03Z",
  "eventSource": "network-security-manager.amazonaws.com",
  "eventName": "CreatePolicy",
  "awsRegion": "us-east-1",
  "sourceIPAddress": "192.0.2.44",
  "userAgent": "aws-cli/2.17.0 Python/3.12.4 Darwin/24.6.0",
  "requestParameters": {
    "clientToken": "550e8400-e29b-41d4-a716-446655440001",
    "policyName": "production-web-acl-policy",
    "firewallType": "WAF",
    "priority": 1,
    "associatedTemplateAndRuleList": [
      {
        "templateIdentifier": "arn:aws:network-security-manager:us-east-1:123456789012:template:t1a2b3c4d5"
      }
    ]
  },
}
```

```

    "policyConfiguration": {
      "remediationEnabled": true,
      "resourcesCleanUp": false,
      "wafConfig": {
        "existingCustomerWebACLResolution": "RETROFIT",
        "conflictResolution": "MERGE_WHERE_APPLICABLE"
      }
    },
    "isPublished": true
  },
  "responseElements": {
    "policyId": "p9z8y7x6w5v4u3t2",
    "policyArn": "arn:aws:network-security-manager:us-east-1:123456789012:policy:p9z8y7x6w5v4u3t2",
    "policyName": "production-web-acl-policy",
    "status": "ACTIVE",
    "version": "1"
  },
  "requestID": "b1c2d3e4-5f67-4890-a1b2-c3d4e5f6a7b8",
  "eventID": "f0e1d2c3-b4a5-4968-8776-5a4b3c2d1e0f",
  "readOnly": false,
  "resources": [
    {
      "accountId": "123456789012",
      "type": "AWS::NetworkSecurityManager::Policy",
      "ARN": "arn:aws:network-security-manager:us-east-1:123456789012:policy:p9z8y7x6w5v4u3t2"
    }
  ],
  "eventType": "AwsApiCall",
  "managementEvent": true,
  "recipientAccountId": "123456789012",
  "eventCategory": "Management"
}

```

AWS Network Security Manager 할당량

AWS 계정에는 AWS Network Security Manager에 대한 다음과 같은 기본 할당량이 있습니다. 달리 명시되지 않는 한 각 할당량은 계정당, 리전당입니다.

리소스 할당량

다음 표에는 각 리전에서 계정당 생성할 수 있는 최대 AWS Network Security Manager 리소스 수가 나와 있습니다.

Resource	기본 할당량	조정 가능
계정당 규칙	200	아니요
계정당 템플릿	100	아니요
계정당 정책	100	아니요
계정당 범위	100	아니요
계정당 배포 수	100	아니요
리소스당 스냅샷	10	아니요

리소스 구성 할당량

다음 표에는 AWS Network Security Manager 리소스가 리소스 계층 구조 내에서 서로를 참조하는 방법에 대한 할당량이 나열되어 있습니다.

할당량	값
템플릿당 규칙	1~50
AWS WAF 정책당 템플릿	1 ~ 2
AWS WAF 정책에 따라 결합된 규칙 및 템플릿	1~100

할당량	값
AWS Shield Advanced 정책에 따른 템플릿 또는 규칙	0(비어 있어야 함)
배포당 정책	1 ~ 2
배포당 범위	1(정확히 하나)

범위 구성 할당량

다음 표에는 범위 구성 표현식의 할당량이 나열되어 있습니다.

할당량	값
범위당 리소스 유형 범위	20
범위 표현식 깊이(중첩 수준)	2
범위 표현식 너비(레벨당 기준)	20

관리자 계정 할당량

다음 표에는 AWS Network Security Manager 관리자 계정 우선 순위 수준에 대한 할당량이 나열되어 있습니다.

할당량	값
관리자 우선 순위 수준	1~10

API 페이지 매김 할당량

다음 표에는 목록 작업에 대한 페이지 매김 제한이 나열되어 있습니다.

할당량	값
페이지당 최대 결과 수(maxResults)	100
페이지당 최소 결과(maxResults)	1

할당량 조정 가능성

이전 섹션에 나열된 할당량은 고정되며 지금은 늘릴 수 없습니다.

AWS Network Security Manager 개발자 안내서의 문서 기록

다음 표에서는 AWS Network Security Manager의 설명서 릴리스를 설명합니다.

변경 사항	설명	날짜
최초 릴리스	AWS Network Security Manager 개발자 안내서의 최초 릴리스입니다.	2026년 8월 1일

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