사용자 가이드

Amazon Inspector Classic

버전 Latest

Copyright © 2025 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

Amazon Inspector Classic: 사용자 가이드

Copyright © 2025 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

..... viii
Amazon Inspector Classic이란 무엇입니까? 1
Amazon Inspector Classic의 이점 2
Amazon Inspector Classic의 특징 2
Amazon Inspector Classic 평가하기 3
용어 및 개념 3
서비스 한도 5
요금 6
네트워크 연결성 규칙 패키지 요금 6
호스트 평가 규칙 패키지 요금 7
지원 운영 체제 및 리전 8
Amazon Inspector Classic 에이전트에 대해 지원되는 Linux 기반 운영 체제 9
Amazon Inspector Classic 에이전트에 대해 지원되는 Windows 기반 운영 체제 9
지원되는 AWS 리전 9
Amazon Inspector Classic 지원 종료 11
1단계: (선택 사항) 평가 보고서 및 조사 결과 내보내기 12
2단계: Amazon Inspector Classic에서 예정된 모든 평가 실행을 삭제합니다. 13
3단계: 새 Amazon Inspector 활성화 13
시작 14
원클릭 설치 14
고급 설정 15
자습서 17
Amazon Inspector Classic 자습서 - Red Hat Enterprise Linux 17
1단계: Amazon Inspector Classic과 함께 사용할 Amazon EC2 인스턴스를 설정합니다. 17
2단계: Amazon EC2 인스턴스 수정 18
3단계: 평가 대상을 생성하고 EC2 인스턴스에 에이전트 설치 18
4단계: 평가 템플릿 생성 및 실행 19
5단계: 결과 찾기 및 분석 20
6단계: 권장 수정 사항을 평가 대상에 적용 21
Amazon Inspector Classic 자습서 - Ubuntu Server 21
1단계: Amazon Inspector Classic과 함께 사용할 Amazon EC2 인스턴스를 설정합니다. 22
2단계: 평가 대상을 생성하고 EC2 인스턴스에 에이전트 설치 22
3단계: 평가 템플릿 생성 및 실행 23
4단계: 생성된 결과 찾기 및 분석 24

5단계: 권장 수정 사항을 평가 대상에 적용 ... 25
보안 ... 26
데이터 보호 ... 27
저장 데이터 암호화 ... 28
전송 중 암호화 ... 28
ID 및 액세스 관리 ... 28
대상 ... 29
ID를 통한 인증 ... 30
정책을 사용하여 액세스 관리 ... 33
Amazon Inspector Classic에서 IAM을 사용하는 방법 ... 35
예제 2: 사용자가 Amazon Inspector 결과에서만 Describe 및 List 작업을 수행할 수 있도록 허용 ... 38
정책 리소스 ... 39
정책 조건 키 ... 39
ACL ... 40
ABAC ... 40
임시 자격 증명 ... 41
위탁자 권한 ... 41
서비스 역할 ... 42
서비스 연결 역할 ... 42
자격 증명 기반 정책 예제 ... 42
서비스 연결 역할 사용 ... 45
문제 해결 ... 47
로깅 및 모니터링 ... 49
인시던트 대응 ... 50
규정 준수 확인 ... 50
복원성 ... 50
인프라 보안 ... 51
구성 및 취약성 분석 ... 52
보안 모범 사례 ... 52
Amazon Inspector Classic 에이전트 ... 53
Amazon Inspector Classic 에이전트 권한 ... 54
네트워크 및 Amazon Inspector Classic 에이전트 보안 ... 54
Amazon Inspector Classic 에이전트 업데이트 ... 55
원격 측정 데이터 수명 주기 ... 55
Amazon Inspector Classic에서 AWS 계정으로 액세스 제어 ... 55

Amazon Inspector Classic 에이전트 제한 ... 56
Amazon Inspector Classic 에이전트 설치하기 ... 56
Systems Manager Run Command를 사용하여 여러 EC2 인스턴스에 에이전트 설치 ... 56
Linux 기반 EC2 인스턴스에 에이전트 설치 ... 58
Windows 기반 EC2 인스턴스에 에이전트 설치 ... 59
Linux 기반 운영 체제에서 Amazon Inspector Classic 에이전트 작업 ... 60
Amazon Inspector Classic 에이전트가 실행 중인지 확인 ... 61
Amazon Inspector Classic 에이전트 중지 ... 61
Amazon Inspector Classic 에이전트 시작 ... 61
Amazon Inspector Classic 에이전트 설정 수정 ... 62
Amazon Inspector Classic 에이전트에 대한 프록시 지원 구성하기 ... 62
Amazon Inspector Classic 에이전트 설치 제거하기 ... 63
Windows 기반 운영 체제에서 Amazon Inspector Classic 에이전트 작업 ... 64
Amazon Inspector Classic 에이전트를 시작 또는 중지하거나 에이전트가 실행 중인지 확인 ... 65
Amazon Inspector Classic 에이전트 설정 수정하기 ... 65
Amazon Inspector Classic 에이전트에 대한 프록시 지원 구성하기 ... 66
Amazon Inspector Classic 에이전트 설치 제거하기 ... 67
(선택 사항) Linux 기반 운영 체제에서 Amazon Inspector Classic 에이전트 설치 스크립트의 서명을 확인합니다. ... 67
GPG 도구 설치 ... 68
퍼블릭 키 인증 및 가져오기 ... 68
패키지의 서명 확인 ... 70
(선택 사항) Windows 기반 운영 체제에서 Amazon Inspector Classic 에이전트 설치 스크립트의 서명을 확인합니다. ... 71
Amazon Inspector Classic 평가 대상 ... 73
평가 대상을 생성하도록 리소스에 태그 지정 ... 73
Amazon Inspector Classic 평가 대상 제한 ... 74
평가 대상 생성 ... 74
평가 대상 삭제 ... 76
Amazon Inspector Classic 규칙 패키지 및 규칙 ... 77
Amazon Inspector Classic의 규칙 심각도 수준 ... 77
Amazon Inspector Classic 내의 규칙 패키지 ... 78
네트워크 연결성 ... 78
분석된 구성 ... 79
연결성 라우팅 ... 79
결과 유형 ... 80

CVE(일반적인 취약성 및 노출도) ... 82
Center for Internet Security(CIS) 벤치마크 ... 83
Amazon Inspector Classic의 보안 모범 사례 ... 87
SSH를 통해 루트 로그인 비활성화 ... 87
SSH 버전 2만 지원 ... 88
SSH를 통한 암호 인증 비활성화 ... 88
암호 최대 수명 구성 ... 89
암호 최소 길이 구성 ... 89
암호 복잡도 구성 ... 90
ASLR 활성화 ... 91
DEP 활성화 ... 91
시스템 디렉터리에 대한 권한 구성 ... 92
Amazon Inspector Classic 평가 템플릿 및 평가 실행 ... 93
Amazon Inspector Classic 평가 템플릿 ... 93
Amazon Inspector Classic 평가 템플릿 한도 ... 94
평가 템플릿 생성 ... 94
평가 템플릿 삭제 ... 96
평가 실행 ... 96
평가 실행 삭제 ... 97
Amazon Inspector Classic 평가 실행 한도 ... 97
Lambda 함수로 자동 평가 실행 설정 ... 97
Amazon Inspector Classic 알림(콘솔)에 대한 SNS 주제 설정 ... 99
Amazon Inspector Classic 결과 ... 102
조사 결과 작업 ... 102
평가 보고서 ... 105
Amazon Inspector Classic의 제외 사항 ... 107
제외 유형 ... 107
제외 항목 미리 보기 ... 120
사후 평가 제외 항목 보기 ... 121
지원되는 운영 체제의 Amazon Inspector Classic 규칙 패키지 ... 122
를 사용하여 Amazon Inspector Classic API 호출 로깅 AWS CloudTrail ... 128
CloudTrail 내의 Amazon Inspector Classic 정보 ... 128
Amazon Inspector Classic 로그 파일 항목 이해하기 ... 129
Amazon CloudWatch를 사용하여 Amazon Inspector Classic 모니터링하기 ... 131
Amazon Inspector Classic CloudWatch 지표 ... 131
AWS CloudFormation를 사용하여 Amazon Inspector Classic 구성하기 ... 133

Security Hub 통합 134
Amazon Inspector에서 Security Hub로 결과를 보내는 방법 134
Amazon Inspector가 전송하는 조사 결과의 유형 135
조사 결과 전송 지연 시간 135
Security Hub를 사용할 수 없을 때 다시 시도 135
Security Hub에서 기존 조사 결과 업데이트 135
Amazon Inspector가 발견한 일반적인 조사 결과 135
통합 활성화 및 구성 137
결과 전송을 중지하는 방법 138
Amazon Inspector Classic ARNs 139
Amazon Inspector Classic 리소스용 ARN 139
규칙 패키지용 Amazon Inspector Classic ARN 140
미국 동부(오하이오) 141
미국 동부(버지니아 북부) 141
미국 서부(캘리포니아 북부) 142
미국 서부(오리건) 143
아시아 태평양(뭄바이) 143
아시아 태평양(서울) 144
아시아 태평양(시드니) 145
아시아 태평양(도쿄) 146
유럽(프랑크푸르트) 146
유럽(아일랜드) 147
유럽(런던) 148
유럽(스톡홀름) 148
AWS GovCloud(미국 동부) 149
AWS GovCloud(미국 서부) 150
문서 기록 151
AWS 용어집 157

지원 종료 공지: 2026년 5월 20일에 AWS 는 Amazon Inspector Classic에 대한 지원을 종료합니다. 2026년 5월 20일 이후에는 Amazon Inspector Classic 콘솔 또는 Amazon Inspector Classic 리소스에 더 이상 액세스할 수 없습니다. Amazon Inspector Classic은 지난 6개월 동안 평가를 완료하지 않은 새 계정 및 계정에 더 이상 사용할 수 없습니다. 다른 모든 계정의 경우 액세스는 2026년 5월 20일까지 유효하며, 그 이후에는 Amazon Inspector Classic 콘솔 또는 Amazon Inspector Classic 리소스에 더 이상 액세스할 수 없습니다. 자세한 내용은 Amazon Inspector Classic 지원 종료를 참조하세요.

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

Amazon Inspector Classic이란 무엇입니까?

> **Note**
>
> Amazon Inspector Classic을 완전히 리아키텍트하고 재설계한 버전인 새로운 Amazon Inspector를 이제 AWS 리전전반에서 사용할 수 있습니다. 새로운 Amazon Inspector는 EC2 인스턴스 외에도 Amazon Elastic Container Registry(Amazon ECR)에 있는 컨테이너 이미지에 대한 지원을 추가하기 위해 적용 범위를 확대했습니다. 새로운 Amazon Inspector는 와의 통합 AWS Organizations을 통한 다중 계정 지원과 일반적인 취약성 및 노출(CVEs을 기반으로 하는 지속적인 소프트웨어 취약성 및 네트워크 연결성 스캔을 제공합니다. 이러한 기능과 새롭게 개선된 기타 기능을 살펴보고 사용하여 상당히 강화된 보안 가치의 혜택을 누리시기 바랍니다. 새로운 Amazon Inspector의 기능 및 요금에 대한 자세한 내용은 Amazon Inspector를 참조하세요. 새로운 Amazon Inspector로 이전하는 방법에 대한 자세한 내용은 Amazon Inspector Classic 지원 종료 섹션을 참조하십시오.

Amazon Inspector Classic은 Amazon EC2 인스턴스의 네트워크 액세스 가능성과 해당 인스턴스에서 실행되는 애플리케이션의 보안 상태를 테스트합니다. Amazon Inspector Classic은 애플리케이션의 노출, 취약성 및 모범 사례와의 편차를 평가합니다. 평가를 수행한 후, Amazon Inspector Classic은 상세한 보안 평가 결과 목록을 제공하며, 이 목록은 심각도 수준에 따라 구성되어 있습니다.

Amazon Inspector Classic을 사용하면 개발 및 배포 파이프라인 또는 정적 프로덕션 시스템에서 보안 취약성 평가를 자동화할 수 있습니다. 이를 통해 보안 테스트를 개발 및 IT 작업의 정규 부분으로 만들 수 있습니다.

또한, Amazon Inspector Classic은 평가하려는 EC2 인스턴스의 운영 체제에 선택적으로 설치할 수 있는 에이전트라는 사전 정의된 소프트웨어를 제공합니다. 에이전트는 네트워크, 파일 시스템 및 프로세스 활동을 포함한 EC2 인스턴스의 동작을 모니터링합니다. 또한 광범위한 동작 및 구성 데이터를 수집합니다(원격 측정).

> **Important**
>
> AWS 는 제공된 권장 사항을 따르면 모든 잠재적 보안 문제를 해결할 것이라고 보장하지 않습니다. Amazon Inspector Classic에서 생성된 결과는 각 평가 템플릿에 포함된 규칙 패키지 선택, 시스템에 비AWS 구성 요소가 있는지 여부 및 기타 요인에 따라 달라집니다. AWS 서비스에서 실행되는 애플리케이션, 프로세스 및 도구의 보안은 사용자의 책임입니다. 자세한 내용은 보안의 AWS 공동 책임 모델을 참조하십시오.

> **Note**
>
> AWS 는 AWS 클라우드에서 제공되는 서비스를 실행하는 글로벌 인프라를 보호할 책임이 있습니다. 이 인프라는 AWS 서비스를 실행하는 하드웨어, 소프트웨어, 네트워킹 및 시설로 구성됩니다.는 다양한 컴퓨터 보안 표준 및 규정 준수를 확인한 타사 감사자로부터 여러 보고서를 AWS 제공합니다. 자세한 내용은 AWS 클라우드 규정 준수를 참조하십시오.

Amazon Inspector Classic 용어에 대한 자세한 내용은 Amazon Inspector Classic 용어 및 개념을 참고하십시오.

Amazon Inspector Classic의 이점

Amazon Inspector Classic의 몇 가지 주요 이점은 다음과 같습니다.

- 자동화된 보안 검사를 정기적인 배포 및 프로덕션 프로세스에 통합 - 포렌식, 문제 해결 또는 활성 감사 목적으로 AWS 리소스의 보안을 평가합니다. 개발 프로세스 중에 평가를 실행하거나 안정적인 프로덕션 환경에서 평가를 실행합니다.
- 애플리케이션 보안 문제 찾기 – 애플리케이션의 보안 평가를 자동화하고 취약성을 사전에 식별합니다. 이를 사용하여 새로운 애플리케이션을 신속하게 개발 및 반복하고 모범 사례 준수와 정책 준수를 평가할 수 있습니다.
- AWS 리소스에 대한 심층 이해 - Amazon Inspector Classic이 생성하는 조사 결과를 검토하여 AWS 리소스의 활동 및 구성 데이터에 대한 최신 정보를 얻을 수 있습니다.

Amazon Inspector Classic의 특징

Amazon Inspector Classic의 몇 가지 주요 기능은 다음과 같습니다.

- 구성 검색 및 활동 모니터링 엔진 – Amazon Inspector Classic은 시스템 및 리소스 구성을 분석하는 에이전트를 제공합니다. 또한 활동을 모니터링하여 평가 대상의 모양, 작동 방식 및 종속성 구성 요소를 결정합니다. 이 원격 측정을 조합하면 평가 대상 및 잠재적인 보안 또는 규정 준수 문제의 전체적인 그림을 알 수 있습니다.
- 기본 제공되는 콘텐츠 라이브러리 - Amazon Inspector Classic은 규칙 및 보고서의 기본 제공되는 라이브러리를 통합합니다. 여기에는 모범 사례, 공통 규정 준수 표준 및 취약성에 대한 검사가 포함됩니다. 이 검사에는 잠재적인 보안 문제를 해결하기 위한 상세한 권장 단계가 포함됩니다.

- API를 통한 자동화 – Amazon Inspector Classic은 API를 통해 완전히 자동화될 수 있습니다. 이를 통해 보안 테스트를 개발 및 설계 프로세스에 통합하고, 해당 테스트 결과를 선택, 실행 및 보고할 수 있습니다.

Amazon Inspector Classic 평가하기

다음 방법 중 하나를 사용하여 Amazon Inspector Classic 서비스로 작업할 수 있습니다.

Amazon Inspector Classic 콘솔

에 로그인 AWS Management Console 하고 https://console.aws.amazon.com/inspector/ Amazon Inspector Classic 콘솔을 엽니다.

콘솔은 Amazon Inspector Classic 서비스를 액세스 및 사용하는 브라우저 기반 인터페이스입니다.

AWS SDKs

AWS 는 다양한 프로그래밍 언어 및 플랫폼을 위한 라이브러리와 샘플 코드로 구성된 소프트웨어 개발 키트(SDKs)를 제공합니다. 여기에는 Java, Python, Ruby, .NET, iOS, Android 등이 포함됩니다. SDK를 사용하면 편리하게 Amazon Inspector Classic 서비스에 프로그래밍 방식으로 액세스할 수 있습니다. 다운로드 및 설치 방법을 포함하여 AWS SDKs에 대한 자세한 내용은 Amazon Web Services용 도구를 참조하세요.

Amazon Inspector Classic HTTPS API

서비스에 직접 HTTPS 요청을 실행할 수 있는 Amazon Inspector Classic HTTPS API를 사용하여 AWS 프로그래밍 방식으로 Amazon Inspector Classic 및에 액세스할 수 있습니다. 자세한 내용은 Amazon Inspector Classic API 참조를 참조하세요.

AWS 명령줄 도구

AWS 명령줄 도구를 사용하여 시스템의 명령줄에서 명령을 실행하여 Amazon Inspector Classic 작업을 수행할 수 있습니다. 명령줄 도구는 AWS 작업을 수행하는 스크립트를 빌드하려는 경우에도 유용합니다. 자세한 내용은 Amazon Inspector Classic AWS 명령줄 인터페이스를 참조하세요.

Amazon Inspector Classic 용어 및 개념

Amazon Inspector Classic을 시작할 때 핵심 개념을 알아두면 유익합니다.

Amazon Inspector Classic 에이전트

평가 대상에 포함되어 있는 EC2 인스턴스에 설치할 수 있는 소프트웨어 에이전트입니다. 에이전트는 광범위한 구성 데이터 세트(원격 측정)를 수집합니다. 자세한 내용은 Amazon Inspector Classic 에이전트 단원을 참조하십시오.

평가 실행

평가 대상의 구성을 지정된 규칙 패키지에 대해 분석하여 잠재적 보안 문제를 발견하는 프로세스입니다. 평가 실행 중에 Amazon Inspector는 지정된 대상 내의 리소스에서 구성 데이터(원격 측정)를 모니터링, 수집 및 분석합니다. 그런 다음 Amazon Inspector는 데이터를 분석하고 이를 평가 실행하는 동안 사용된 평가 템플릿에 지정되어 있는 보안 규칙 패키지 세트와 비교합니다. 완료된 평가 실행에서 결과(다양한 심각도의 잠재적 보안 문제) 목록을 생성합니다. 자세한 내용은 Amazon Inspector Classic 평가 템플릿 및 평가 실행 단원을 참조하십시오.

평가 대상

Amazon Inspector Classic의 컨텍스트에서는 비즈니스 목표를 달성할 수 있게 도와주는 한 단위로 함께 작동하는 AWS 리소스 모음입니다. Amazon Inspector Classic은 평가 대상을 구성하는 리소스의 보안 상태를 평가합니다.

> **Important**
>
> 현재 Amazon Inspector Classic 평가 대상은 EC2 인스턴스만으로 구성될 수 있습니다. 자세한 내용은 Amazon Inspector Classic 서비스 한도 단원을 참조하세요.

Amazon Inspector Classic 평가 대상을 생성하려면 먼저 EC2 인스턴스를 선택한 키-값 페어로 태그 지정합니다. 그런 다음 공통 키 또는 공통 값을 갖는 태그가 지정된 EC2 인스턴스의 보기를 생성할 수 있습니다. 자세한 내용은 Amazon Inspector Classic 평가 대상 단원을 참조하십시오.

평가 템플릿

평가 실행 중에 사용되는 구성. 템플릿에는 다음 사항이 포함됩니다.

- Amazon Inspector Classic이 평가 대상을 평가하기 위해 사용하는 규칙 패키지
- Amazon Inspector Classic이 평가 실행 상태 및 결과에 대한 알림을 보내는 Amazon SNS 주제
- 평가 실행에 의해 생성된 결과에 지정할 수 있는 태그(키-값 페어)
- 평가 실행 기간

조사 결과

지정된 대상의 평가 실행 중에 Amazon Inspector Classic이 발견한 잠재적인 보안 문제입니다. 결과는 Amazon Inspector Classic 콘솔에 표시되거나 API를 통해 검색됩니다. 여기에는 보안 문제에 대한 자세한 설명과 이를 수정하는 방법에 대한 권장 사항이 모두 포함되어 있습니다. 자세한 내용은 Amazon Inspector Classic 결과 단원을 참조하십시오.

규칙

Amazon Inspector Classic의 컨텍스트에서 평가 실행 중에 수행되는 보안 검사입니다. 규칙에서 잠재적인 보안 문제를 발견하면 Amazon Inspector Classic은 문제를 설명하는 결과를 생성합니다.

규칙 패키지

Amazon Inspector Classic의 맥락에서 살펴본 규칙 모음입니다. 규칙 패키지는 사용자가 설정할 수 있는 보안 목표에 해당합니다. Amazon Inspector Classic 평가 템플릿을 작성할 때 해당하는 규칙 패키지를 선택하여 보안 목표를 지정할 수 있습니다. 자세한 내용은 Amazon Inspector Classic 규칙 패키지 및 규칙 단원을 참조하십시오.

원격 측정

EC2 인스턴스에 대해 설치된 패키지 정보 및 소프트웨어 구성입니다. Amazon Inspector Classic은 평가 실행 중에 데이터를 수집합니다.

Amazon Inspector Classic 서비스 한도

다음 표에는 AWS 계정의 Amazon Inspector Classic 한도가 나와 있습니다.

> **Important**
> 현재 평가 대상은 EC2 인스턴스만으로 구성될 수 있습니다.

다음은 리전별로 AWS 계정당 Amazon Inspector Classic 제한입니다.

리소스	기본 제한	설명
평가를 실행하는 인스턴스	500	리전별로 계정당 실행 중인 모든 평가에 포함될 수 있는 EC2 인스턴스의 최대 수입니다.

리소스	기본 제한	설명
평가 실행	50000	리전별로 계정당 생성할 수 있는 평가 실행의 최대 횟수. 이 실행에 사용된 평가 대상에 중복되는 EC2 인스턴스가 포함되지 않는 한, 여러 평가 실행이 동시에 발생하도록 할 수 있습니다.
평가 템플릿	500	특정 시간에 리전별로 계정당 포함시킬 수 있는 최대 평가 템플릿 수입니다.
평가 대상	50	특정 시간에 리전별로 계정당 포함시킬 수 있는 최대 평가 대상 수입니다.

특별한 언급이 없는 한 한도는 AWS Support 센터에 문의하여 요청 시 높일 수 있습니다.

Amazon Inspector Classic 요금

Amazon Inspector Classic 요금은 각 평가에 포함된 EC2 인스턴스 수와 해당 평가에 사용된 규칙 패키지를 기반으로 합니다.

네트워크 연결성 규칙 패키지 요금

네트워크 연결성 규칙 패키지를 사용한 Amazon Inspector Classic 평가는 매달 평가마다 인스턴스당 (인스턴스-평가) 요금이 부과됩니다. 예를 들어, 인스턴스 1개에 대해 평가를 1회 실행하면 인스턴스-평가가 1회가 됩니다. 인스턴스 10개에 대해 평가를 1회 실행하면 인스턴스-평가가 10회가 됩니다. 요금은 매월 인스턴스-평가당 0.15 USD부터 시작하며, 볼륨 할인을 통해 매월 인스턴스-평가당 최저 0.04 USD까지 낮출 수 있습니다.

무료 평가판 세부 정보

Amazon Inspector Classic을 사용한 첫 90일	인스턴스-평가당 요금
First 250 instance-assessments	$0.00

요금 내역

해당 월에	인스턴스-평가당 요금
First 250 instance-assessments	$0.15
Next 750 instance-assessments	$0.13
Next 4,000 instance-assessments	$0.10
Next 45,000 instance-assessments	$0.07
All other instance-assessments	$0.04

호스트 평가 규칙 패키지 요금

평가에 포함된 일반적인 취약성 및 노출(CVE), 인터넷 보안 센터(CIS) 벤치마크, 보안 모범 사례, 런타임 동작 분석 조합의 경우

Amazon Inspector Classic의 호스트 평가 규칙 패키지는 평가하려는 애플리케이션을 실행하는 Amazon EC2 인스턴스에 배포된 에이전트를 사용합니다. 호스트 규칙 패키지를 사용한 평가는 매달 평가마다 에이전트당(에이전트-평가) 요금이 부과됩니다. 예를 들어, 에이전트 1개에 대해 평가를 1회 실행하면 에이전트-평가가 1회가 됩니다. 에이전트 10개를 대상으로 평가를 1회 실행하면 에이전트-평가가 10회가 됩니다. 요금은 매달 에이전트-평가당 월 0.30 USD부터 시작하며, 볼륨 할인을 통해 에이전트-평가당 월 0.05 USD까지 낮출 수 있습니다.

무료 평가판 세부 정보

Amazon Inspector Classic을 사용한 첫 90일	에이전트-평가당 요금
First 250 agent-assessments	$0.00

요금 내역

해당 월에	에이전트-평가당 요금
First 250 agent-assessments	$0.30
Next 750 agent-assessments	$0.25
Next 4,000 agent-assessments	$0.15
Next 45,000 agent-assessments	$0.10
All other agent-assessments	$0.05

Amazon Inspector Classic이 지원되는 운영 체제 및 리전

이 장에서는 Amazon Inspector Classic에서 지원하는 운영 체제 및 AWS 리전에 대한 정보를 제공합니다.

> **Important**
>
> 현재 Amazon Inspector Classic 평가 대상은 EC2 인스턴스만으로 구성될 수 있습니다. 운영 체제와 상관없이 모든 EC2 인스턴스에서 네트워크 연결성 규칙 패키지를 사용하여 에이전트 없는 평가를 실행할 수 있습니다.

지원되는 운영 체제에서 사용할 수 있는 Amazon Inspector Classic 규칙 패키지에 대한 자세한 내용은 지원되는 운영 체제의 Amazon Inspector Classic 규칙 패키지 섹션을 참조하십시오.

주제

- Amazon Inspector Classic 에이전트에 대해 지원되는 Linux 기반 운영 체제
- Amazon Inspector Classic 에이전트에 대해 지원되는 Windows 기반 운영 체제
- 지원되는 AWS 리전

Amazon Inspector Classic 에이전트에 대해 지원되는 Linux 기반 운영 체제

64-bit x86 및 Arm EC2 인스턴스에서 Amazon Inspector Classic 에이전트를 사용할 수 있습니다. 에이전트는 아래의 Linux 기반 운영 체제 버전과 호환됩니다.

- 64비트 x86 인스턴스
  - Amazon Linux 2
  - Amazon Linux(2018.03, 2017.09, 2017.03, 2016.09, 2016.03, 2015.09, 2015.03, 2014.09, 2014.03, 2013.09, 2013.03, 2012.09, 2012.03)
  - Ubuntu(20.04 LTS, 18.04 LTS, 16.04 LTS, 14.04 LTS)
  - Debian (10.x, 9.0 - 9.5, 8.0 - 8.7)
  - Red Hat Enterprise Linux(8.x, 7.2, 6.2 - 6.9)
  - CentOS(7.2 - 7.x, 6.2 - 6.9)
- Arm 인스턴스
  - Amazon Linux 2
  - Red Hat Enterprise Linux(7.6 - 7.x)
  - Ubuntu(18.04 LTS, 16.04 LTS)

Amazon Inspector Classic 에이전트에 대해 지원되는 Windows 기반 운영 체제

다음 Windows 기반 운영 체제의 64비트 버전을 실행하는 EC2 인스턴스에서만 Amazon Inspector Classic 에이전트를 사용할 수 있습니다.

- Windows Server 2019 Base
- Windows Server 2016 Base
- Windows Server 2012 R2
- Windows Server 2012
- Windows Server 2008 R2

지원되는 AWS 리전

다음과 같은 AWS 리전에서는 Amazon Inspector Classic이 지원됩니다.

- 미국 동부(오하이오) us-east-2
- 미국 동부(버지니아 북부) us-east-1
- 미국 서부(캘리포니아 북부) us-west-1
- 미국 서부(오레곤) us-west-2
- 아시아 태평양(뭄바이) ap-south-1
- 아시아 태평양(서울) ap-northeast-2
- 아시아 태평양(시드니) ap-southeast-2
- 아시아 태평양(도쿄) ap-northeast-1
- EU(프랑크푸르트) eu-central-1
- EU(아일랜드) eu-west-1
- 유럽(런던) eu-west-2
- 유럽(스톡홀름) eu-north-1
- AWS GovCloud(미국 동부) gov-us-east-1
- AWS GovCloud(미국 서부) gov-us-west-1

> **Note**
>
> Network Reachability 규칙 패키지는 AWS GovCloud(미국) 리전에서 사용할 수 없습니다.

Amazon Inspector Classic 지원 종료

신중한 고려 후 2026년 5월 20일부터 Amazon Inspector Classic에 대한 지원을 종료하기로 결정했습니다. Amazon Inspector Classic은 2025년 5월 20일부터 더 이상 신규 고객을 받지 않습니다. 2025년 5월 20일 이전에 서비스에 가입한 계정이 있는 기존 고객은 Amazon Inspector Classic 기능을 계속 사용할 수 있습니다. 2026년 5월 20일 이후에는 Amazon Inspector Classic을 더 이상 사용할 수 없습니다.

이제 새로운 Amazon Inspector를 전세계 AWS 리전에서 사용할 수 있습니다. 새로운 Amazon Inspector는 현재 Amazon Inspector Classic이라고 불리는 기존 Amazon Inspector를 완전히 리아키텍트하고 재설계한 버전입니다. Amazon Inspector의 개선된 주요 기능은 다음과 같습니다.

- 뛰어난 확장성 – 새로운 Amazon Inspector는 확장성과 동적 클라우드 환경에 맞게 구축되었습니다. 계정에서 스캔할 수 있는 인스턴스 또는 이미지 수에 제한이 없습니다.
- 컨테이너 이미지 지원 – 또한, 새로운 Amazon Inspector는 Amazon Elastic Container Registry(Amazon ECR)에 있는 컨테이너 이미지를 스캔하여 소프트웨어 취약성을 찾아냅니다.
- 다중 계정 관리 지원 – 새로운 Amazon Inspector는 Organizations와 통합되었습니다. 이를 통해 조직에서 Amazon Inspector의 관리자 계정을 위임할 수 있습니다. 위임된 관리자 계정은 모든 조사 결과를 통합하고 모든 구성원의 계정을 구성할 수 있는 중앙 집중식 계정입니다.
- AWS Systems Manager 에이전트 사용(SSM 에이전트) - 새 Amazon Inspector를 사용하면 더 이상 모든 EC2 인스턴스에 독립형 Amazon Inspector 에이전트를 설치하고 유지 관리할 필요가 없습니다. 새로운 Amazon Inspector는 널리 배포된 SSM 에이전트를 활용합니다.
- 자동화된 연속 검사 — Amazon Inspector Classic을 사용하면 평가 대상, 평가 템플릿을 수동으로 설정하고 평가 빈도를 구성할 수 있습니다. 하지만, 새 버전의 Amazon Inspector는 새로 시작된 모든 EC2 인스턴스와 Amazon ECR에 푸시된 적격 컨테이너 이미지를 자동으로 감지하고 소프트웨어 취약성 및 의도하지 않은 네트워크 노출 여부를 즉시 스캔합니다. 리소스는 새 EC2 인스턴스 시작, Amazon ECR로 컨테이너 이미지 푸시, EC2 인스턴스에 새 패키지 설치, 패치 설치 또는 리소스에 영향을 미치는 새로운 일반적인 취약성 및 노출(CVE) 게시 등 여러 트리거에 따라 자동으로 다시 스캔됩니다.
- Amazon Inspector 위험 점수 – 새로운 Amazon Inspector는 Amazon Inspector 위험 점수를 계산하여 조사 결과의 우선순위를 정하는 데 도움이 됩니다. 이 위험 점수는 최신 CVE 정보를 네트워크 접근성 및 악용 가능성 정보와 같은 시간적 및 환경적 요인과 상호 연관시켜 계산합니다.
- 추가 통합 - 모든 결과는 새로 설계된 Amazon Inspector 콘솔에서 집계되고 AWS Security Hub 및 Amazon EventBridge로 푸시되어 티켓팅과 같은 워크플로를 자동화합니다. 컨테이너 이미지 관련 조사 결과도 Amazon ECR에 푸시됩니다.

새 Amazon Inspector의 모든 기능 및 요금에 대해 알아보려면 Amazon Inspector 사용 설명서를 참고하십시오.

당분간은 Amazon Inspector Classic을 계속 지원할 예정이므로 고객은 동일한 계정에서 새로운 Amazon Inspector와 Amazon Inspector Classic을 모두 사용할 수 있지만, 새로운 Amazon Inspector로 마이그레이션하는 것을 적극 권장합니다. 다음 섹션에서는 Amazon Inspector Classic에서 새로운 Amazon Inspector로 전환하는 과정을 알려드립니다.

주제

- 1단계: (선택 사항) 평가 보고서 및 조사 결과 내보내기
- 2단계: Amazon Inspector Classic에서 예정된 모든 평가 실행을 삭제합니다.
- 3단계: 새 Amazon Inspector 활성화

1단계: (선택 사항) 평가 보고서 및 조사 결과 내보내기

Amazon Inspector Classic에 평가 보고서와 조사 결과를 저장하려면 평가 보고서를 생성하십시오.

평가 보고서를 생성하려면

1. 평가 실행 페이지에서 보고서를 생성할 평가 실행을 찾습니다. 상태가 분석 완료로 설정되어 있는지 확인합니다.
2. 이 평가 실행에 대한 보고서 열에서 보고서 아이콘을 선택합니다.

> **Important**
>
> 2017년 4월 25일 이후에 수행했거나 수행할 평가 실행에 대해서만 보고서 열에 보고서 아이콘이 표시됩니다. 이는 Amazon Inspector Classic에서 평가 보고서가 사용 가능하게 된 시점입니다.

3. 평가 보고서대화 상자에서 보려는 보고서 유형(결과 보고서 또는 전체 보고서)과 보고서 형식(HTML 또는 PDF)을 선택합니다. 그런 다음 보고서 생성을 선택합니다.

2단계: Amazon Inspector Classic에서 예정된 모든 평가 실행을 삭제합니다.

Amazon Inspector Classic을 비활성화하려면 활성 상태인 모든 AWS 리전에 있는 계정에서 평가 템플릿을 모두 삭제하십시오. 평가 템플릿을 삭제하면 앞으로 예정된 평가 실행이 모두 중지됩니다.

평가 템플릿 삭제

- Assessment Templates(평가 템플릿) 페이지에서 삭제할 템플릿을 선택한 후 삭제를 선택합니다. 확인 메시지가 표시되면 예를 선택합니다.

> **Important**
>
> 평가 템플릿을 삭제하면 이 템플릿과 연결된 모든 평가 템플릿, 평가 실행, 결과 및 모든 버전의 보고서가 삭제됩니다.

3단계: 새 Amazon Inspector 활성화

AWS Management Console 또는 새 Amazon Inspector API를 사용하여 새 Amazon Inspector를 활성화할 수 있습니다. APIs 새로운 Amazon Inspector를 시작하려면 Amazon Inspector 사용 설명서의 시작하기를 참고하십시오.

Amazon Inspector Classic 시작하기

이 자습서에서는 첫 번째 평가를 생성하고 실행하여 Amazon Inspector Classic을 설치하고 시작하는 방법을 보여 줍니다.

원클릭 설치

다음 절차에서는 현재 및에서 사용 가능한 모든 Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스에서 사전 빌드된 템플릿 AWS 계정 과 사전 정의된 예약 파라미터(주 1회 또는 1회만)를 사용하여 자동 평가를 생성하고 실행하는 방법을 보여줍니다 AWS 리전.

1. 에 로그인 AWS Management Console 하고 https://console.aws.amazon.com/inspector/ Amazon Inspector Classic 콘솔을 엽니다.
2. 시작 페이지에서 실행할 평가 유형을 선택합니다. 네트워크 평가는 AWS 환경의 네트워크 구성에 취약성이 있는지 분석하며 Amazon Inspector Classic 에이전트가 필요하지 않습니다. 호스트 평가는 호스트상의 소프트웨어 및 EC2 인스턴스 구성의 취약성을 분석하며 EC2 인스턴스에 에이전트를 설치하도록 요구합니다.

   Run weekly(주별 실행)(권장) 또는 Run once(한 번 실행) 중 하나를 선택합니다. 선택하는 대로 서비스는 자동으로 평가를 생성합니다. 특히 이 서비스는 다음을 수행합니다.

   a. 서비스 연결 역할을 만들려면

   > **Note**
   >
   > 평가 대상에 지정된 EC2 인스턴스를 식별하려면 Amazon Inspector Classic 에서 EC2 인스턴스와 태그를 열거해야 합니다. Amazon Inspector Classic은 `AWSServiceRoleForAmazonInspector`라는 서비스 연결 역할을 통해 사용자의 AWS 계정 에 있는 이러한 리소스에 액세스할 수 있습니다. 서비스 연결 역할에 대한 자세한 내용은 Amazon Inspector Classic에 대해 서비스 연결 역할 사용 및 서비스 연결 역할 사용 섹션을 참조하십시오.

   b. 해당하는 경우는 AWS 계정 및 리전에서 사용 가능한 모든 EC2 인스턴스에 Amazon Inspector Classic 에이전트를 설치합니다.

> **Note**
>
> 서비스는 AWS Systems Manager Run Command를 허용하는 EC2 인스턴스에만 Amazon Inspector Classic 에이전트를 설치합니다. 이 옵션을 사용하려면 현재의 모든 EC2 인스턴스 AWS 계정 와 SSM 에이전트 AWS 리전 가 설치되어 있고 Run Command를 허용하는 IAM 역할이 있는지 확인합니다. 자세한 내용은 Systems Manager Run Command를 사용하여 여러 EC2 인스턴스에 에이전트 설치 단원을 참조하십시오.

c. 평가 대상에 이러한 인스턴스를 추가합니다.

d. 평가 템플릿에 표준화된 규칙 패키지로 대상을 추가합니다.

e. Run weekly(recommended) 또는 Run once 중 선택 여부에 따라 주마다 혹은 단 한 번 평가를 실행합니다.

3. 확인 대화 상자에서 OK를 선택합니다. Amazon Inspector Classic은 평가를 자동으로 실행합니다.

고급 설정

다음 절차는 특정 Amazon EC2 인스턴스, 규칙 패키지 및 일정 파라미터를 선택하여 평가 대상 및 템플릿을 추가하는 방법에 대해 보여줍니다.

1. Welcome 페이지에서 Advanced setup을 선택합니다.
2. Define an assessment target 페이지에서 평가 대상의 이름을 입력합니다.
3. 모든 인스턴스의 경우 확인란을 선택한 상태로 유지하여 AWS 계정 및 리전의 모든 EC2 인스턴스를 평가 대상에 포함할 수 있습니다. 포함할 EC2 인스턴스를 선택하려면, 모든 인스턴스 확인란의 선택을 취소하고 대상 EC2 인스턴스와 연결된 키 및 값 태그를 입력합니다. EC2 인스턴스 태그에 대한 자세한 내용은 Amazon EC2 리소스에 태그 지정을 참조하십시오.
4. 에이전트 설치의 경우, 인스턴스가 System Manager 명령 실행을 허용한다면 기본적으로 확인란을 선택한 상태로 유지할 수 있습니다. 이 서비스는가 허용하는 평가 대상의 모든 EC2 인스턴스에 Amazon Inspector Classic 에이전트를 설치합니다 AWS Systems Manager. 이 옵션을 사용하려면 현재의 모든 EC2 인스턴스 AWS 계정 와 SSM 에이전트 AWS 리전 가 설치되어 있고 Run Command를 허용하는 IAM 역할이 있는지 확인합니다. 자세한 내용은 Systems Manager Run Command를 사용하여 여러 EC2 인스턴스에 에이전트 설치 단원을 참조하십시오. 수동으로 에이전트를 설치하고자 한다면 Installing Amazon Inspector Agents를 참조하십시오.
5. Next(다음)를 선택합니다.

6. Define an assessment template 페이지에서 평가 템플릿의 이름을 입력합니다.
7. Rules packages에서 평가 템플릿에 포함시킬 규칙 패키지를 선택합니다. 규칙 패키지에 대한 자세한 내용은 Amazon Inspector Rules Packages and Rules를 참조하십시오.
8. Duration에서 평가 템플릿 실행 기간을 선택합니다.
9. (선택 사항) 평가 일정에서 반복 평가 실행 일정을 설정할 수 있습니다.
10. Next(다음)를 선택합니다.
11. Review 페이지에서 평가 대상 및 템플릿 선택에 대하여 검토합니다. 구성이 만족스러우면 Create을 선택합니다. 평가 템플릿의 평가 일정을 설정하는 경우 생성을 선택하면 자동으로 평가가 실행됩니다.

> **Note**
>
> 평가 대상에 지정된 EC2 인스턴스를 식별하려면 Amazon Inspector Classic에서 EC2 인스턴스와 태그를 열거해야 합니다. Amazon Inspector Classic은 라는 서비스 연결 역할을 AWS 계정 통해의 이러한 리소스에 액세스할 수 있습니다`AWSServiceRoleForAmazonInspector`. Amazon Inspector Classic에서 서비스 연결 역할 사용에 대한 자세한 내용은 Amazon Inspector Classic에 대해 서비스 연결 역할 사용 섹션을 참조하세요. 서비스 연결 역할에 대한 자세한 내용은 AWS Identity and Access Management 사용 설명서의 서비스 연결 역할 사용을 참조하세요

12. 평가 일정을 설정하지 않으면 평가 템플릿을 콘솔을 통해 탐색하고 실행을 선택합니다.
13. 평가 실행 절차를 추적하기 위해서는 콘솔 탐색 창에서 Assessment runs를 선택한 다음 Findings를 선택합니다. 결과에 대한 자세한 내용은 Amazon Inspector Classic 결과을 참조하십시오.

Amazon Inspector Classic 자습서

다음 자습서는 Amazon Inspector Classic 평가가 Red Hat Enterprise Linux 및 Ubuntu 작업 시스템에서 실행하는 방법에 대해 보여줍니다.

자습서

- 자습서: Red Hat Enterprise Linux에서 Amazon Inspector Classic 사용하기
- 자습서: Ubuntu Server에서 Amazon Inspector Classic 사용하기

Amazon Inspector Classic 자습서 - Red Hat Enterprise Linux

이 자습서의 지침을 따르기 전에 Amazon Inspector Classic 용어 및 개념에 익숙해지는 것이 좋습니다.

이 자습서는 Amazon Inspector Classic을 사용하여 Red Hat Enterprise Linux 7.5 운영 체제를 실행하는 EC2 인스턴스의 동작을 분석하는 방법을 보여줍니다. Amazon Inspector Classic 워크플로 탐색 방법에 대한 단계별 지침을 제공합니다. 워크플로는 Amazon EC2 인스턴스 준비, 평가 템플릿 실행 및 평가 결과에서 도출된 권장 보안 해결책 실천을 포함합니다. 최초 사용자이고 한 번의 클릭으로 Amazon Inspector Classic 평가를 설계하고 실행하고자 한다면 Creating a Basic Assessment를 참조하십시오.

주제

- 1단계: Amazon Inspector Classic과 함께 사용할 Amazon EC2 인스턴스를 설정합니다.
- 2단계: Amazon EC2 인스턴스 수정
- 3단계: 평가 대상을 생성하고 EC2 인스턴스에 에이전트 설치
- 4단계: 평가 템플릿 생성 및 실행
- 5단계: 결과 찾기 및 분석
- 6단계: 권장 수정 사항을 평가 대상에 적용

1단계: Amazon Inspector Classic과 함께 사용할 Amazon EC2 인스턴스를 설정합니다.

이 자습서에서는 Red Hat Enterprise Linux 7.5를 실행하는 EC2 인스턴스를 하나 생성하고 Name 키 및 **`InspectorEC2InstanceLinux`** 값을 사용하여 이를 태그합니다.

> **Note**
>
> EC2 인스턴스의 태그 지정에 대한 자세한 내용은 리소스 및 태그를 참조하십시오.

2단계: Amazon EC2 인스턴스 수정

이 자습서에서는 잠재적 보안 문제 CVE-2018-1111에 노출되도록 대상 EC2 인스턴스를 수정합니다. 자세한 내용은 https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-1111와 CVE(일반적인 취약성 및 노출도)를 참조하십시오.

`InspectorEC2InstanceLinux` 인스턴스에 연결하고 다음 명령을 실행합니다.

```
sudo yum install dhclient-12:4.2.5-68.el7
```

EC2 인스턴스 연결 방법에 관한 지침은 Amazon EC2 사용 설명서의 인스턴스에 연결을 참조하세요.

3단계: 평가 대상을 생성하고 EC2 인스턴스에 에이전트 설치

Amazon Inspector Classic이 평가 대상을 사용하여 평가하고자 하는 AWS 리소스를 설계합니다.

평가 대상을 생성하고 EC2 인스턴스에 에이전트를 설치하려면

1. 에 로그인 AWS Management Console 하고 https://console.aws.amazon.com/inspector/ Amazon Inspector Classic 콘솔을 엽니다.
2. 탐색 창에서 Assessment targets(평가 대상)를 선택한 후 Create(생성)를 선택합니다.

   다음을 수행합니다.

   a. Name에 평가 대상의 이름을 입력합니다.

      이 자습서에서는 **`MyTargetLinux`**을 입력합니다.

   b. 태그 사용의 경우, 키 및 값 필드에 값을 입력하여 이 평가 대상에 포함하려는 EC2 인스턴스를 선택합니다.

      이 자습서의 경우, 키 필드에 **`Name`**을 입력하고 값 필드에 **`InspectorEC2InstanceLinux`**를 입력하여 이전 단계에서 만든 EC2 인스턴스를 선택합니다.

      모든 인스턴스 확인란을 선택하여 모든 EC2 인스턴스를 평가 대상의 AWS 계정과 리전에 포함되게 합니다.

c. 저장(Save)을 선택합니다.

d. 태그가 지정된 EC2 인스턴스에 Amazon Inspector Classic 에이전트를 설치합니다. 평가 대상에 포함된 EC2 인스턴스에 에이전트를 설치하려면 에이전트 설치 확인란을 선택합니다.

> **Note**
>
> AWS Systems Manager 명령 실행을 사용하여 Amazon Inspector Classic 에이전트를 설치할 수도 있습니다. 평가 대상의 모든 인스턴스에 에이전트를 설치하려면 평가 대상을 생성할 때 사용한 태그를 그대로 지정하면 됩니다. 또는 수동으로 EC2 인스턴스에 Amazon Inspector Classic 에이전트를 설치할 수 있습니다. 자세한 내용은 Amazon Inspector Classic 에이전트 설치하기 단원을 참조하십시오.

e. 저장(Save)을 선택합니다.

> **Note**
>
> 이 시점에서 Amazon Inspector Classic은 `AWSServiceRoleForAmazonInspector`라는 서비스 연결 역할을 생성합니다. 이 역할은 Amazon Inspector Classic에 리소스에 대해 필요한 액세스 권한을 부여합니다. 자세한 내용은 Amazon Inspector Classic에 대한 서비스 연결 역할 생성 단원을 참조하십시오.

4단계: 평가 템플릿 생성 및 실행

템플릿을 생성하고 실행하려면

1. 탐색 창에서 Assessment Templates(평가 템플릿)를 선택한 후 Create(생성)를 선택합니다.
2. Name에 평가 템플릿의 이름을 입력합니다. 이 자습서에서는 **`MyFirstTemplateLinux`**을 입력합니다.
3. Target name에, 위에서 생성한 평가 대상인 **`MyTargetLinux`**를 선택합니다.
4. Rules packages에서 이 평가 템플릿에서 사용할 규칙 패키지를 선택합니다.

   이 자습서에서는 Common Vulnerabilities and Exposures-1.1를 선택합니다.
5. [Duration]에서 평가 템플릿의 기간을 지정합니다.

   이 자습서에서는 15 minutes를 선택합니다.

6. [Create and run]을 선택합니다.

5단계: 결과 찾기 및 분석

평가 실행이 완료되면 결과 세트 또는 Amazon Inspector Classic이 평가 대상에서 발견한 잠재적인 보안 문제가 생성됩니다. 결과를 검토하고 권장 단계에 따라 잠재적인 보안 문제를 해결할 수 있습니다.

이 자습서는 이전 단계를 완료하면 평가 실행 시 일반적인 취약성 CVE-2018-1111에 대한 결과를 생성합니다.

결과를 찾고 분석하려면

1. 탐색 창에서 Assessment runs(평가 실행)를 선택합니다. MyFirstTemplateLinux라는 평가 템플릿의 실행 상태가 Collecting data로 있는지 확인합니다. 이는 평가 실행이 현재 진행 중이고, 대상의 원격 측정 데이터가 수집되어 선택된 규칙 패키지에 대해 분석되고 있음을 나타냅니다.
2. 평가 실행이 진행 중일 때는 평가 실행에서 생성되는 결과를 볼 수 없습니다. 평가가 모두 완료될 때까지 기다립니다. 그러나 이 자습서에서는 몇 분 후에 실행을 중지할 수 있습니다.

   MyFirstTemplateLinux의 상태는 처음에 Stopping으로 바뀌었다가 몇 분 후에 Analyzing으로 바뀐 후 마지막으로 Analysis complete으로 됩니다. 이 상태 변경을 보려면 Refresh 아이콘 선택합니다.
3. 탐색 창에서 결과를 선택합니다.

   InspectorEC2InstanceLinux 인스턴스가 CVE-2018-1111에 취약함이라는 높은 심각도의 새 결과가 표시될 수 있습니다.

   > **Note**
   > 새 결과가 표시되지 않으면 Refresh 아이콘을 선택합니다.

   보기를 확장하여 이 결과의 세부 정보를 표시하려면 결과 왼쪽에 있는 화살표를 선택합니다. 결과 세부 정보에는 다음이 포함됩니다.

   - 결과 ARN
   - 이 결과를 생성한 평가 실행의 이름
   - 이 결과를 생성한 평가 대상의 이름
   - 이 결과를 생성한 평가 템플릿의 이름
   - 평가 실행 시작 시간

- 평가 실행 종료 시간
- 평가 실행 상태
- 이 결과를 트리거한 규칙을 포함하는 규칙 패키지의 이름
- Amazon Inspector Classic 에이전트 ID
- 결과의 이름
- 결과의 심각도
- 결과에 대한 설명
- 결과에서 설명하는 잠재적 보안 문제를 해결하기 위해 수행할 수 있는 권장하는 수정 단계

6단계: 권장 수정 사항을 평가 대상에 적용

이 자습서에서는 잠재적 보안 문제 CVE-2018-1111에 노출되도록 평가 대상을 수정했습니다. 이 절차는 이 문제에 대한 권장 수정 사항을 적용할 수 있습니다.

수정 사항을 대상에 적용하려면

1. 이전 섹션에서 생성한 **`InspectorEC2InstanceLinux`** 인스턴스에 연결하고 다음 명령을 실행합니다.

   ```
   sudo yum update dhclient-12:4.2.5-68.el7
   ```

2. Amazon templates 페이지에서 MyFirstTemplateLinux를 선택한 후 Run을 선택하여 이 템플릿으로 새로운 평가 실행을 시작합니다.
3. 5단계: 결과 찾기 및 분석의 단계를 수행하여 MyFirstTemplateLinux 템플릿의 후속 실행 결과를 확인합니다.

   보안 문제 CVE-2018-1111을 해결했기 때문에 더 이상 이 문제의 결과가 표시되지 않습니다.

Amazon Inspector Classic 자습서 - Ubuntu Server

이 자습서의 지침을 따르기 전에 Amazon Inspector Classic 용어 및 개념에 익숙해지는 것이 좋습니다.

이 자습서는 Amazon Inspector Classic을 사용하여 Ubuntu Server 16.04 LTS 운영 체제를 실행하는 EC2 인스턴스의 동작을 분석하는 방법을 보여 줍니다. Amazon Inspector Classic 워크플로 탐색 방법에 대한 단계별 지침을 제공합니다.

최초 사용자이고 한 번의 클릭으로 Amazon Inspector Classic 평가를 설계하고 실행하고자 한다면 Creating a Basic Assessment를 참조하십시오.

주제

- 1단계: Amazon Inspector Classic과 함께 사용할 Amazon EC2 인스턴스를 설정합니다.
- 2단계: 평가 대상을 생성하고 EC2 인스턴스에 에이전트 설치
- 3단계: 평가 템플릿 생성 및 실행
- 4단계: 생성된 결과 찾기 및 분석
- 5단계: 권장 수정 사항을 평가 대상에 적용

1단계: Amazon Inspector Classic과 함께 사용할 Amazon EC2 인스턴스를 설정합니다.

EC2 인스턴스를 설정하려면

- 이 자습서에서는 Ubuntu Server 16.04 LTS를 실행하는 EC2 인스턴스를 하나 생성하고 Name 키 및 **`InspectorEC2InstanceUbuntu`** 값을 사용하여 태그를 지정합니다.

> **Note**
>
> EC2 인스턴스의 태그 지정에 대한 자세한 내용은 리소스 및 태그를 참조하십시오.

2단계: 평가 대상을 생성하고 EC2 인스턴스에 에이전트 설치

Amazon Inspector Classic이 평가 대상을 사용하여 평가하고자 하는 AWS 리소스를 설계합니다.

평가 대상을 생성하고 EC2 인스턴스에 에이전트를 설치하려면

1. 에 로그인 AWS Management Console 하고 https://console.aws.amazon.com/inspector/ Amazon Inspector Classic 콘솔을 엽니다.
2. 탐색 창에서 Assessment targets(평가 대상)를 선택한 후 Create(생성)를 선택합니다.
3. Name에 평가 대상의 이름을 입력합니다.

   본 자습서에서는 **`MyTargetUbuntu`**을 입력하겠습니다.

4. 태그 사용의 경우 키 및 값 필드에 값을 입력하여 이 평가 대상에 포함하려는 EC2 인스턴스를 선택합니다.

   이 자습서의 경우, 키 필드에 **Name**을 입력하고 값 필드에 **InspectorEC2InstanceUbuntu**를 입력하여 이전 단계에서 만든 EC2 인스턴스를 선택합니다.

   모든 인스턴스 확인란을 선택하여 평가 대상의 AWS 계정과 리전이 모든 EC2 인스턴스에 포함되게 하십시오.

5. 태그가 지정된 EC2 인스턴스에 Amazon Inspector Classic 에이전트를 설치합니다. 평가 대상에 포함된 EC2 인스턴스에 에이전트를 설치하려면 Install Agents 확인란을 선택하십시오.

   > **Note**
   >
   > Systems Manager Run Command를 사용하여 Amazon Inspector Agent를 설치할 수도 있습니다. 평가 대상의 모든 인스턴스에 에이전트를 설치하려면 평가 대상을 생성할 때 사용한 태그를 그대로 지정하면 됩니다. 또는 수동으로 EC2 인스턴스에 Amazon Inspector 에이전트를 설치할 수 있습니다. 자세한 내용은 Amazon Inspector Classic 에이전트 설치하기 단원을 참조하십시오.

6. 저장(Save)을 선택합니다.

> **Note**
>
> 이때 `AWSServiceRoleForAmazonInspector`라는 서비스 연결 역할이 생성되어 Amazon Inspector Classic에 리소스에 대한 액세스 권한을 부여합니다. 자세한 내용은 Amazon Inspector Classic에 대한 서비스 연결 역할 생성 단원을 참조하십시오.

3단계: 평가 템플릿 생성 및 실행

템플릿을 생성하고 실행하려면

1. Advanced setup(고급 설정)을 사용하면 Define an assessment template(평가 템플릿 정의) 페이지로 이동합니다. 또는 Assessment templates(평가 템플릿) 페이지로 이동한 다음 생성을 선택합니다.
2. Name에 평가 템플릿의 이름을 입력합니다. 이 자습서에서는 **MyFirstTemplateUbuntu**을 입력합니다.

3. Target name에, 위에서 생성한 평가 대상인 **`MyTargetUbuntu`**를 선택합니다.
4. Rules packages(규칙 패키지)에서 드롭다운 메뉴를 사용하여 이 평가 템플릿에서 사용할 규칙 패키지를 선택합니다.

   이 자습서에서는 Common Vulnerabilities and Exposures-1.1를 선택합니다.
5. [Duration]에서 평가 템플릿의 기간을 지정합니다.

   이 자습서에서는 15 minutes(15분)를 선택합니다.
6. Advanced setup을 사용하면 Next를 선택합니다. 다음 Review 페이지에서 Create을 선택합니다. 또는 Create and run(생성 및 실행)을 선택합니다.

4단계: 생성된 결과 찾기 및 분석

평가 실행이 완료되면 결과 세트 또는 Amazon Inspector Classic이 평가 대상에서 발견한 잠재적인 보안 문제가 생성됩니다. 결과를 검토하고 권장 단계에 따라 잠재적인 보안 문제를 해결할 수 있습니다.

1. Assessment Runs(평가 실행) 페이지로 이동합니다. 이전 단계에서 생성한 MyFirstTemplateUbuntu라는 평가 템플릿의 실행 상태가 Collecting data(데이터 수집)로 설정되어 있는지 확인합니다. 이는 평가 실행이 현재 진행 중이고, 대상의 원격 측정 데이터가 수집되어 선택된 규칙 패키지에 대해 분석되고 있음을 나타냅니다.
2. 평가 실행이 진행 중일 때는 평가 실행에서 생성되는 결과를 볼 수 없습니다. 평가가 모두 완료될 때까지 기다립니다.

   MyFirstTemplateUbuntu의 상태는 처음에 Stopping(중지 중)으로 바뀌었다가 몇 분 후에 Analyzing(분석 중)으로 바뀐 후 마지막으로 Analysis complete(분석 완료)로 됩니다. 이 상태 변경을 보려면 Refresh 아이콘 선택합니다.
3. Findings(결과) 페이지로 이동합니다.

   보기를 확장하여 이 결과의 세부 정보를 표시하려면 결과 왼쪽에 있는 화살표를 선택합니다. 결과 세부 정보에는 다음이 포함됩니다.

   - 결과 ARN
   - 이 결과를 생성한 평가 실행의 이름
   - 이 결과를 생성한 평가 대상의 이름
   - 이 결과를 생성한 평가 템플릿의 이름
   - 평가 실행 시작 시간

- 평가 실행 종료 시간
- 평가 실행 상태
- 이 결과를 트리거한 규칙을 포함하는 규칙 패키지의 이름
- Amazon Inspector Classic 에이전트 ID
- 결과의 이름
- 결과의 심각도
- 결과에 대한 설명
- 결과에서 설명하는 잠재적 보안 문제를 해결하기 위해 수행할 수 있는 권장하는 수정 단계

5단계: 권장 수정 사항을 평가 대상에 적용

이 절차에서는 업데이트를 적용하여 발견된 문제를 해결합니다.

1. 인스턴스 **`InspectorEC2InstanceUbuntu`**에 연결하고 패키지 업데이트를 수행합니다.
2. Assessment templates(평가 템플릿) 페이지에서 MyFirstTemplateUbuntu를 선택한 후 Run(실행)을 선택하여 이 템플릿으로 새로운 실행을 시작합니다.
3. 4단계: 생성된 결과 찾기 및 분석의 단계를 수행하여 MyFirstTemplateUbuntu 템플릿의 후속 실행 결과를 확인합니다.

   이 패키지 업데이트는 템플릿을 처음 실행했을 때 발견된 조사 결과를 해결해야 합니다.

Amazon Inspector Classic에서의 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 AWS 와 사용자 간의 공동 책임입니다. 공동 책임 모델은 이 사항을 클라우드의 보안 및 클라우드 내 보안으로 설명합니다.

- 클라우드 보안 - AWS 는 AWS 클라우드에서 AWS 서비스를 실행하는 인프라를 보호할 책임이 있습니다. AWS 또한는 안전하게 사용할 수 있는 서비스를 제공합니다. 타사 감사자는 AWS 규정 준수 프로그램 일환으로 보안의 효과를 정기적으로 테스트하고 확인합니다. Amazon Inspector Classic에 적용되는 규정 준수 프로그램에 대한 자세한 내용은 규정 준수 프로그램의 범위에 속하는 AWS 서비스 를 참조하세요.
- 클라우드의 보안 - 사용자의 책임은 사용하는 AWS 서비스에 따라 결정됩니다. 또한 귀하는 귀사의 데이터 민감도, 귀사의 요구 사항, 관련 법률 및 규정을 비롯한 기타 요소에 대해서도 책임이 있습니다.

이 설명서는 Amazon Inspector Classic을 사용할 때 공동 책임 모델을 적용하는 방법을 이해하는 데 도움이 됩니다. 다음 주제에서는 보안 및 규정 준수 목적에 맞게 Amazon Inspector Classic을 구성하는 방법을 보여줍니다. 또한 Amazon Inspector Classic 리소스를 모니터링하고 보호하는 데 도움이 되는 다른 AWS 서비스를 사용하는 방법을 알아봅니다.

주제

- Amazon Inspector Classic에서의 데이터 보호
- Amazon Inspector Classic용 ID 및 액세스 관리
- Amazon Inspector Classic 로깅 및 모니터링
- Amazon Inspector Classic의 인시던트 대응
- Amazon Inspector Classic의 규정 준수 확인
- Amazon Inspector Classic의 복원성
- Amazon Inspector Classic의 인프라 보안
- Amazon Inspector Classic의 구성 및 취약성 분석
- Amazon Inspector Classic의 보안 모범 사례

Amazon Inspector Classic에서의 데이터 보호

AWS 공동 책임 모델 Amazon Inspector Classic의 데이터 보호에 적용됩니다. 이 모델에 설명된 대로 AWS 는 모든를 실행하는 글로벌 인프라를 보호할 책임이 있습니다 AWS 클라우드. 사용자는 인프라에서 호스팅되는 콘텐츠를 관리해야 합니다. 사용하는 AWS 서비스 의 보안 구성과 관리 태스크에 대한 책임도 사용자에게 있습니다. 데이터 프라이버시에 대한 자세한 내용은 데이터 프라이버시 FAQ를 참조하세요. 유럽의 데이터 보호에 대한 자세한 내용은 AWS 보안 블로그의 AWS 공동 책임 모델 및 GDPR 블로그 게시물을 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 사용하세요.
- 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 사용하세요.
- 명령줄 인터페이스 또는 API를 AWS 통해에 액세스할 때 FIPS 140-3 검증 암호화 모듈이 필요한 경우 FIPS 엔드포인트를 사용합니다. 사용 가능한 FIPS 엔드포인트에 대한 자세한 내용은 Federal Information Processing Standard(FIPS) 140-3을 참조하세요.

고객의 이메일 주소와 같은 기밀 정보나 중요한 정보는 태그나 이름 필드와 같은 자유 형식 텍스트 필드에 입력하지 않는 것이 좋습니다. 여기에는 Amazon Inspector Classic 또는 기타 AWS 서비스 에서 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 자격 증명을 URL에 포함해서는 안 됩니다.

주제

- 저장 데이터의 암호화
- 전송 중 데이터 암호화

저장 데이터의 암호화

평가 실행 중에 Amazon Inspector Classic 에이전트에서 생성하는 원격 측정 데이터는 JSON 파일로 형식이 지정됩니다. 이러한 파일은 TLS를 통해 near-real-time Amazon Inspector Classic으로 전송되며, 여기서 per-assessment-run 임시 AWS KMS파생 키로 암호화됩니다.

그런 다음 Amazon Inspector Classic 전용 S3 버킷에 안전하게 저장됩니다. Amazon Inspector Classic의 규칙 엔진은 다음 사항을 수행합니다.

- S3 버킷의 암호화된 원격 측정 데이터에 액세스
- 메모리에서 해당 데이터 해독
- 구성된 평가 규칙에 따라 해당 데이터를 처리하여 결과 생성

전송 중 데이터 암호화

관리형 서비스인 Amazon Inspector Classic은 AWS 글로벌 네트워크 보안으로 보호됩니다. AWS 보안 서비스 및가 인프라를 AWS 보호하는 방법에 대한 자세한 내용은 AWS 클라우드 보안을 참조하세요. 인프라 보안 모범 사례를 사용하여 AWS 환경을 설계하려면 보안 원칙 AWS Well-Architected Framework의 인프라 보호를 참조하세요.

AWS 에서 게시한 API 호출을 사용하여 네트워크를 통해 Amazon Inspector Classic에 액세스합니다. 고객은 다음을 지원해야 합니다.

- Transport Layer Security(TLS) TLS 1.2는 필수이며 TLS 1.3을 권장합니다.
- DHE(Ephemeral Diffie-Hellman) 또는 ECDHE(Elliptic Curve Ephemeral Diffie-Hellman)와 같은 완전 전송 보안(PFS)이 포함된 암호 제품군 Java 7 이상의 최신 시스템은 대부분 이러한 모드를 지원합니다.

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

Amazon Inspector Classic용 ID 및 액세스 관리

AWS Identity and Access Management (IAM)는 관리자가 AWS 리소스에 대한 액세스를 안전하게 제어하는 데 도움이 AWS 서비스 되는 입니다. IAM 관리자는 인증(로그인) 및 권한 부여(권한 보유)를 통

해 Amazon Inspector 리소스를 사용할 수 있는 사용자를 제어합니다. IAM은 추가 비용 없이 사용할 수 AWS 서비스 있는 입니다.

주제

- 대상
- ID를 통한 인증
- 정책을 사용하여 액세스 관리
- Amazon Inspector Classic에서 IAM을 사용하는 방법
- 예제 2: 사용자가 Amazon Inspector 결과에서만 Describe 및 List 작업을 수행할 수 있도록 허용
- Amazon Inspector에 대한 정책 리소스
- Amazon Inspector에 사용되는 정책 조건 키
- Amazon Inspector의 ACL
- Amazon Inspector를 사용한 ABAC
- Amazon Inspector에서 임시 보안 인증 정보 사용
- Amazon Inspector에 대한 교차 서비스 보안 주체 권한
- Amazon Inspector의 서비스 역할
- Amazon Inspector의 서비스 연결 역할
- Amazon Inspector Classic의 자격 증명 기반 정책 예
- Amazon Inspector Classic에 대해 서비스 연결 역할 사용
- Amazon Inspector Classic ID 및 액세스 문제 해결

대상

AWS Identity and Access Management (IAM)를 사용하는 방법은 Amazon Inspector에서 수행하는 작업에 따라 다릅니다.

서비스 사용자 – Amazon Inspector 서비스를 사용하여 작업을 수행하는 경우 필요한 보안 인증 정보와 권한을 관리자가 제공합니다. 더 많은 Amazon SNS 기능을 사용하여 작업을 수행한다면 추가 권한이 필요할 수 있습니다. 액세스 권한 관리 방법을 이해하면 관리자에게 올바른 권한을 요청하는 데 도움이 됩니다. Amazon Inspector의 기능에 액세스할 수 없다면 Amazon Inspector Classic ID 및 액세스 문제 해결 섹션을 참조하세요.

서비스 관리자 – 회사에서 Amazon Inspector 리소스를 책임지고 있다면 Amazon Inspector에 대한 완전한 액세스 권한이 있을 것입니다. 서비스 관리자는 서비스 사용자가 액세스해야 하는 Amazon

Inspector 기능과 리소스를 결정합니다. 그런 다음 IAM 관리자에게 요청을 제출하여 서비스 사용자의 권한을 변경해야 합니다. 이 페이지의 정보를 검토하여 IAM의 기본 개념을 이해하세요. 회사가 Amazon Inspector에서 IAM을 사용하는 방법에 대해 자세히 알아보려면 Amazon Inspector Classic에서 IAM을 사용하는 방법 섹션을 참조하세요.

IAM 관리자 - IAM 관리자라면 Amazon Inspector에 대한 액세스 관리 정책 작성 방법을 자세히 알고 싶을 수도 있습니다. IAM에서 사용할 수 있는 Amazon Inspector 자격 증명 기반 정책 예제를 보려면 Amazon Inspector Classic의 자격 증명 기반 정책 예 섹션을 참조하세요.

ID를 통한 인증

인증은 자격 증명 자격 증명을 AWS 사용하여에 로그인하는 방법입니다. IAM 사용자 또는 AWS 계정 루트 사용자 IAM 역할을 수임하여 로 인증(로그인 AWS)되어야 합니다.

자격 증명 소스를 통해 제공된 자격 증명을 사용하여 페더레이션 자격 증명 AWS 으로에 로그인할 수 있습니다. AWS IAM Identity Center (IAM Identity Center) 사용자, 회사의 Single Sign-On 인증 및 Google 또는 Facebook 자격 증명은 페더레이션 자격 증명의 예입니다. 페더레이션형 ID로 로그인할 때 관리자가 이전에 IAM 역할을 사용하여 ID 페더레이션을 설정했습니다. 페더레이션을 사용하여 AWS 에 액세스하면 간접적으로 역할을 수임하게 됩니다.

사용자 유형에 따라 AWS Management Console 또는 AWS 액세스 포털에 로그인할 수 있습니다. 로그인에 대한 자세한 내용은 AWS 로그인 사용 설명서의에 로그인하는 방법을 AWS참조하세요. AWS 계정

AWS 프로그래밍 방식으로에 액세스하는 경우는 자격 증명을 사용하여 요청에 암호화 방식으로 서명할 수 있는 소프트웨어 개발 키트(SDK)와 명령줄 인터페이스(CLI)를 AWS 제공합니다. AWS 도구를 사용하지 않는 경우 요청에 직접 서명해야 합니다. 권장 방법을 사용하여 요청에 직접 서명하는 자세한 방법은 IAM 사용 설명서에서 API 요청용AWS Signature Version 4를 참조하세요.

사용하는 인증 방법에 상관없이 추가 보안 정보를 제공해야 할 수도 있습니다. 예를 들어, 다중 인증(MFA)을 사용하여 계정의 보안을 강화하는 것이 AWS 좋습니다. 자세한 내용은 AWS IAM Identity Center 사용 설명서에서 다중 인증 및 IAM 사용 설명서에서 IAM의AWS 다중 인증을 참조하세요.

AWS 계정 루트 사용자

를 생성할 때 계정의 모든 AWS 서비스 및 리소스에 대한 완전한 액세스 권한이 있는 하나의 로그인 자격 증명으로 AWS 계정시작합니다. 이 자격 증명을 AWS 계정 루트 사용자라고 하며 계정을 생성하는 데 사용한 이메일 주소와 암호로 로그인하여 액세스합니다. 일상적인 작업에 루트 사용자를 사용하지 않을 것을 강력히 권장합니다. 루트 사용자 자격 증명을 보호하고 루트 사용자만 수행할 수 있는 작업

을 수행하는 데 사용합니다. 루트 사용자로 로그인해야 하는 전체 작업 목록은 IAM 사용 설명서의 루트 사용자 보안 인증이 필요한 작업을 참조하세요.

페더레이션 자격 증명

가장 좋은 방법은 관리자 액세스가 필요한 사용자를 포함한 인간 사용자에게 자격 증명 공급자와의 페더레이션을 사용하여 임시 자격 증명을 사용하여 AWS 서비스 에 액세스하도록 요구하는 것입니다.

페더레이션 자격 증명은 엔터프라이즈 사용자 디렉터리, 웹 자격 증명 공급자, AWS Directory Service, Identity Center 디렉터리 또는 자격 증명 소스를 통해 제공된 자격 증명을 사용하여 AWS 서비스 에 액세스하는 모든 사용자의 사용자입니다. 페더레이션 자격 증명에 액세스할 때 역할을 AWS 계정수임하고 역할은 임시 자격 증명을 제공합니다.

중앙 집중식 액세스 관리를 위해 AWS IAM Identity Center을(를) 사용하는 것이 좋습니다. IAM Identity Center에서 사용자 및 그룹을 생성하거나 모든 및 애플리케이션에서 사용할 수 있도록 자체 ID 소스의 사용자 AWS 계정 및 그룹 집합에 연결하고 동기화할 수 있습니다. IAM Identity Center에 대한 자세한 내용은 AWS IAM Identity Center 사용 설명서에서 IAM Identity Center란 무엇인가요?를 참조하세요.

IAM 사용자 및 그룹

IAM 사용자는 단일 사용자 또는 애플리케이션에 대한 특정 권한이 AWS 계정 있는 내의 자격 증명입니다. 가능하면 암호 및 액세스 키와 같은 장기 자격 증명이 있는 IAM 사용자를 생성하는 대신 임시 자격 증명을 사용하는 것이 좋습니다. 하지만 IAM 사용자의 장기 자격 증명이 필요한 특정 사용 사례가 있는 경우, 액세스 키를 교체하는 것이 좋습니다. 자세한 내용은 IAM 사용 설명서의 장기 보안 인증이 필요한 사용 사례의 경우, 정기적으로 액세스 키 교체를 참조하세요.

IAM 그룹은 IAM 사용자 컬렉션을 지정하는 자격 증명입니다. 사용자는 그룹으로 로그인할 수 없습니다. 그룹을 사용하여 여러 사용자의 권한을 한 번에 지정할 수 있습니다. 그룹을 사용하면 대규모 사용자 집합의 권한을 더 쉽게 관리할 수 있습니다. 예를 들어, IAMAdmins라는 그룹이 있고 이 그룹에 IAM 리소스를 관리할 권한을 부여할 수 있습니다.

사용자는 역할과 다릅니다. 사용자는 한 사람 또는 애플리케이션과 고유하게 연결되지만, 역할은 해당 역할이 필요한 사람이라면 누구나 수임할 수 있습니다. 사용자는 영구적인 장기 자격 증명을 가지고 있지만, 역할은 임시 보안 인증만 제공합니다. 자세한 내용은 IAM 사용 설명서에서 IAM 사용자 사용 사례를 참조하세요.

IAM 역할

IAM 역할은 특정 권한이 AWS 계정 있는 내의 자격 증명입니다. IAM 사용자와 유사하지만, 특정 개인과 연결되지 않습니다. 에서 IAM 역할을 일시적으로 수임하려면 사용자에서 IAM 역할(콘솔)로 전환할 AWS Management Console수 있습니다. https://docs.aws.amazon.com/IAM/latest/UserGuide/

id_roles_use_switch-role-console.html 또는 AWS API 작업을 호출하거나 사용자 지정 URL을 AWS CLI 사용하여 역할을 수임할 수 있습니다. 역할 사용 방법에 대한 자세한 내용은 IAM 사용 설명서의 역할 수임 방법을 참조하세요.

임시 보안 인증이 있는 IAM 역할은 다음과 같은 상황에서 유용합니다.

- 페더레이션 사용자 액세스 - 페더레이션 ID에 권한을 부여하려면 역할을 생성하고 해당 역할의 권한을 정의합니다. 페더레이션 ID가 인증되면 역할이 연결되고 역할에 정의된 권한이 부여됩니다. 페더레이션 관련 역할에 대한 자세한 내용은 IAM 사용 설명서의 Create a role for a third-party identity provider (federation)를 참조하세요. IAM Identity Center를 사용하는 경우, 권한 집합을 구성합니다. 인증 후 ID가 액세스할 수 있는 항목을 제어하기 위해 IAM Identity Center는 권한 집합을 IAM의 역할과 연관짓습니다. 권한 집합에 대한 자세한 내용은 AWS IAM Identity Center 사용 설명서의 권한 집합을 참조하세요.
- 임시 IAM 사용자 권한 - IAM 사용자 또는 역할은 IAM 역할을 수임하여 특정 작업에 대한 다양한 권한을 임시로 받을 수 있습니다.
- 교차 계정 액세스 - IAM 역할을 사용하여 다른 계정의 사용자(신뢰할 수 있는 보안 주체)가 내 계정의 리소스에 액세스하도록 허용할 수 있습니다. 역할은 계정 간 액세스를 부여하는 기본적인 방법입니다. 그러나 일부 에서는 정책을 리소스에 직접 연결할 AWS 서비스수 있습니다(역할을 프록시로 사용하는 대신). 교차 계정 액세스에 대한 역할과 리소스 기반 정책의 차이점을 알아보려면 IAM 사용 설명서의 IAM의 교차 계정 리소스 액세스를 참조하세요.
- 교차 서비스 액세스 - 일부는 다른에서 기능을 AWS 서비스 사용합니다 AWS 서비스. 예를 들어, 서비스에서 호출하면 일반적으로 해당 서비스는 Amazon EC2에서 애플리케이션을 실행하거나 Amazon S3에 객체를 저장합니다. 서비스는 직접적으로 호출하는 위탁자의 권한을 사용하거나, 서비스 역할을 사용하거나, 또는 서비스 연결 역할을 사용하여 이 작업을 수행할 수 있습니다.
  - 전달 액세스 세션(FAS) - IAM 사용자 또는 역할을 사용하여에서 작업을 수행하는 경우 AWS보안 주체로 간주됩니다. 일부 서비스를 사용하는 경우, 다른 서비스에서 다른 작업을 시작하는 작업을 수행할 수 있습니다. FAS는를 호출하는 보안 주체의 권한을 다운스트림 서비스에 AWS 서비스 대한 요청과 AWS 서비스함께 사용합니다. FAS 요청은 서비스가 완료하기 위해 다른 AWS 서비스 또는 리소스와의 상호 작용이 필요한 요청을 수신할 때만 이루어집니다. 이 경우, 두 작업을 모두 수행할 수 있는 권한이 있어야 합니다. FAS 요청 시 정책 세부 정보는 전달 액세스 세션을 참조하세요.
  - 서비스 역할 - 서비스 역할은 서비스가 사용자를 대신하여 작업을 수행하기 위해 맡는 IAM 역할입니다. IAM 관리자는 IAM 내에서 서비스 역할을 생성, 수정 및 삭제할 수 있습니다. 자세한 정보는 IAM 사용 설명서의 Create a role to delegate permissions to an AWS 서비스를 참조하세요.
  - 서비스 연결 역할 - 서비스 연결 역할은에 연결된 서비스 역할의 한 유형입니다 AWS 서비스. 서비스는 사용자를 대신하여 작업을 수행하기 위해 역할을 수임할 수 있습니다. 서비스 연결 역할은에

나타나 AWS 계정 며 서비스가 소유합니다. IAM 관리자는 서비스 링크 역할의 권한을 볼 수 있지만 편집은 할 수 없습니다.

- Amazon EC2에서 실행되는 애플리케이션 - IAM 역할을 사용하여 EC2 인스턴스에서 실행되고 AWS CLI 또는 AWS API 요청을 수행하는 애플리케이션의 임시 자격 증명을 관리할 수 있습니다. 이는 EC2 인스턴스 내에 액세스 키를 저장할 때 권장되는 방법입니다. EC2 인스턴스에 AWS 역할을 할당하고 모든 애플리케이션에서 사용할 수 있도록 하려면 인스턴스에 연결된 인스턴스 프로파일을 생성합니다. 인스턴스 프로필에는 역할이 포함되어 있으며 EC2 인스턴스에서 실행되는 프로그램이 임시 보안 인증을 얻을 수 있습니다. 자세한 정보는 IAM 사용 설명서의 IAM 역할을 사용하여 Amazon EC2 인스턴스에서 실행되는 애플리케이션에 권한 부여를 참조하세요.

정책을 사용하여 액세스 관리

정책을 AWS 생성하고 자격 증명 또는 리소스에 연결하여 AWS 에서 액세스를 제어합니다. 정책은 자격 증명 또는 리소스와 연결된 AWS 경우 권한을 정의하는의 객체입니다.는 보안 주체(사용자, 루트 사용자 또는 역할 세션)가 요청할 때 이러한 정책을 AWS 평가합니다. 정책에서 권한은 요청이 허용되거나 거부되는 지를 결정합니다. 대부분의 정책은에 JSON 문서 AWS 로 저장됩니다. JSON 정책 문서의 구조와 콘텐츠에 대한 자세한 정보는 IAM 사용 설명서의 JSON 정책 개요를 참조하세요.

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.

기본적으로, 사용자 및 역할에는 어떠한 권한도 없습니다. 사용자에게 사용자가 필요한 리소스에서 작업을 수행할 권한을 부여하려면 IAM 관리자가 IAM 정책을 생성하면 됩니다. 그런 다음 관리자가 IAM 정책을 역할에 추가하고, 사용자가 역할을 수임할 수 있습니다.

IAM 정책은 작업을 수행하기 위해 사용하는 방법과 상관없이 작업에 대한 권한을 정의합니다. 예를 들어, `iam:GetRole` 작업을 허용하는 정책이 있다고 가정합니다. 해당 정책이 있는 사용자는 AWS Management Console AWS CLI, 또는 API에서 역할 정보를 가져올 수 있습니다 AWS .

ID 기반 정책

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 정의를 참조하세요.

ID 기반 정책은 인라인 정책 또는 관리형 정책으로 한층 더 분류할 수 있습니다. 인라인 정책은 단일 사용자, 그룹 또는 역할에 직접 포함됩니다. 관리형 정책은의 여러 사용자, 그룹 및 역할에 연결할 수 있는

독립 실행형 정책입니다 AWS 계정. 관리형 정책에는 AWS 관리형 정책 및 고객 관리형 정책이 포함됩니다. 관리형 정책 또는 인라인 정책을 선택하는 방법을 알아보려면 IAM 사용 설명서의 관리형 정책 및 인라인 정책 중에서 선택을 참조하세요.

리소스 기반 정책

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 위탁자가 해당 리소스와 어떤 조건에서 어떤 작업을 수행할 수 있는지를 정의합니다. 리소스 기반 정책에서 위탁자를 지정해야 합니다. 보안 주체에는 계정, 사용자, 역할, 페더레이션 사용자 또는가 포함될 수 있습니다 AWS 서비스.

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

액세스 제어 목록(ACL)

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.

Amazon S3 AWS WAF및 Amazon VPC는 ACLs. ACL에 관한 자세한 내용은 Amazon Simple Storage Service 개발자 가이드의 액세스 제어 목록(ACL) 개요를 참조하세요.

기타 정책 타입

AWS 는 덜 일반적인 추가 정책 유형을 지원합니다. 이러한 정책 타입은 더 일반적인 정책 유형에 따라 사용자에게 부여되는 최대 권한을 설정할 수 있습니다.

- 권한 경계 – 권한 경계는 ID 기반 정책에 따라 IAM 엔터티(IAM 사용자 또는 역할)에 부여할 수 있는 최대 권한을 설정하는 고급 기능입니다. 개체에 대한 권한 경계를 설정할 수 있습니다. 그 결과로 얻는 권한은 객체의 ID 기반 정책과 그 권한 경계의 교집합입니다. `Principal` 필드에서 사용자나 역할을 지정하는 리소스 기반 정책은 권한 경계를 통해 제한되지 않습니다. 이러한 정책 중 하나에 포함된 명시적 거부는 허용을 재정의합니다. 권한 경계에 대한 자세한 정보는 IAM 사용 설명서의 IAM 엔티티에 대한 권한 경계를 참조하세요.
- 서비스 제어 정책(SCPs) - SCPs는의 조직 또는 조직 단위(OU)에 대한 최대 권한을 지정하는 JSON 정책입니다 AWS Organizations. AWS Organizations 는 AWS 계정 기업이 소유한 여러을 그룹화하고 중앙에서 관리하기 위한 서비스입니다. 조직에서 모든 기능을 활성화할 경우, 서비스 제어 정책(SCP)을 임의의 또는 모든 계정에 적용할 수 있습니다. SCP는 각각을 포함하여 멤버 계정의 엔

터티에 대한 권한을 제한합니다 AWS 계정 루트 사용자. 조직 및 SCP에 대한 자세한 내용은 AWS Organizations 사용 설명서에서 Service control policies을 참조하세요.

- 리소스 제어 정책(RCP) - RCP는 소유한 각 리소스에 연결된 IAM 정책을 업데이트하지 않고 계정의 리소스에 대해 사용 가능한 최대 권한을 설정하는 데 사용할 수 있는 JSON 정책입니다. RCP는 멤버 계정의 리소스에 대한 권한을 제한하며 조직에 속하는지 여부에 AWS 계정 루트 사용자관계없이를 포함한 자격 증명에 대한 유효 권한에 영향을 미칠 수 있습니다. RCP를 AWS 서비스 지원하는 목록을 포함하여 조직 및 RCPs에 대한 자세한 내용은 AWS Organizations 사용 설명서의 리소스 제어 정책(RCPs)을 참조하세요.
- 세션 정책 – 세션 정책은 역할 또는 페더레이션 사용자에 대해 임시 세션을 프로그래밍 방식으로 생성할 때 파라미터로 전달하는 고급 정책입니다. 결과적으로 얻는 세션의 권한은 사용자 또는 역할의 ID 기반 정책의 교차와 세션 정책입니다. 또한 권한을 리소스 기반 정책에서 가져올 수도 있습니다. 이러한 정책 중 하나에 포함된 명시적 거부는 허용을 재정의합니다. 자세한 정보는 IAM 사용 설명서의 세션 정책을 참조하세요.

여러 정책 유형

여러 정책 유형이 요청에 적용되는 경우, 결과 권한은 이해하기가 더 복잡합니다. 에서 여러 정책 유형이 관련될 때 요청을 허용할지 여부를 AWS 결정하는 방법을 알아보려면 IAM 사용 설명서의 정책 평가 로직을 참조하세요.

Amazon Inspector Classic에서 IAM을 사용하는 방법

IAM을 사용하여 Amazon Inspector에 대한 액세스를 관리하기 전에 Amazon Inspector에서 사용할 수 있는 IAM 기능에 대해 알아봅니다.

Amazon Inspector Classic에서 사용할 수 있는 IAM 기능

IAM 기능	Amazon Inspector 지원
ID 기반 정책	예
리소스 기반 정책	아니요
정책 작업	예
정책 리소스	예
정책 조건 키(서비스별)	예

IAM 기능	Amazon Inspector 지원
ACLs	아니요
ABAC(정책 내 태그)	부분
임시 자격 증명	예
보안 주체 권한	예
서비스 역할	아니요
서비스 링크 역할	예

Amazon Inspector 및 기타 AWS 서비스에서 대부분의 IAM 기능을 사용하는 방법을 전체적으로 알아보려면 IAM 사용 설명서의 AWS IAM으로 작업하는 서비스를 참조하세요.

Amazon Inspector의 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 정의를 참조하세요.

IAM ID 기반 정책을 사용하면 허용되거나 거부되는 작업과 리소스뿐 아니라 작업이 허용되거나 거부되는 조건을 지정할 수 있습니다. ID 기반 정책에서는 위탁자가 연결된 사용자 또는 역할에 적용되므로 위탁자를 지정할 수 없습니다. JSON 정책에서 사용하는 모든 요소에 대해 알아보려면 IAM 사용 설명서의 IAM JSON 정책 요소 참조를 참조하세요.

Amazon Inspector의 자격 증명 기반 정책 예

Amazon Inspector 자격 증명 기반 정책 예제를 보려면 Amazon Inspector Classic의 자격 증명 기반 정책 예 섹션을 참조하세요.

Amazon Inspector 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 위탁자가 해당 리소스와 어떤 조건에서 어떤 작업을 수행할 수 있는지를 정의합니다. 리소스 기반 정책에서 위탁자를 지정해야 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 위탁자로 지정할 수 있습니다. 리소스 기반 정책에 크로스 계정 보안 주체를 추가하는 것은 트러스트 관계 설정의 절반밖에 되지 않는다는 것을 유념하세요. 보안 주체와 리소스가 다른 경우 신뢰할 수 AWS 계정있는 계정의 IAM 관리자는 보안 주체 엔터티(사용자 또는 역할)에게 리소스에 액세스할 수 있는 권한도 부여해야 합니다. 엔터티에 ID 기반 정책을 연결하여 권한을 부여합니다. 하지만 리소스 기반 정책이 동일 계정의 위탁자에 액세스를 부여하는 경우, 추가 자격 증명 기반 정책이 필요하지 않습니다. 자세한 내용은 IAM 사용 설명서의 교차 계정 리소스 액세스를 참조하세요.

Amazon Inspector에 대한 정책 작업

정책 작업 지원: 예

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

JSON 정책의 `Action` 요소는 정책에서 액세스를 허용하거나 거부하는 데 사용할 수 있는 작업을 설명합니다. 정책 작업은 일반적으로 연결된 AWS API 작업과 이름이 동일합니다. 일치하는 API 작업이 없는 권한 전용 작업 같은 몇 가지 예외도 있습니다. 정책에서 여러 작업이 필요한 몇 가지 작업도 있습니다. 이러한 추가 작업을 일컬어 종속 작업이라고 합니다.

연결된 작업을 수행할 수 있는 권한을 부여하기 위한 정책에 작업을 포함하세요.

Amazon Inspector 작업 목록을 보려면 서비스 승인 참조의 Amazon Inspector Classic에서 정의한 작업을 참조하세요.

Amazon Inspector의 정책 작업은 작업 앞에 다음 접두사를 사용합니다.

```
inspector
```

단일 문에서 여러 작업을 지정하려면 다음과 같이 쉼표로 구분합니다.

```
"Action": [
```

```
      "inspector:action1",
      "inspector:action2"
         ]
```

다음 권한 정책은 사용자에게 `Describe` 및 `List`로 시작하는 모든 작업을 실행할 수 있는 권한을 부여합니다. 이러한 작업은 평가 대상 또는 결과와 같은 Amazon Inspector 리소스에 대한 정보를 보여 줍니다. `Resource` 요소에 와일드카드 문자(*)가 있으면 계정이 소유한 모든 Amazon Inspector 리소스에 작업이 허용됩니다.

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Effect":"Allow",
         "Action": [
            "inspector:Describe*",
            "inspector:List*"
            ],
         "Resource":"*"
      }
   ]
}
```

예제 2: 사용자가 Amazon Inspector 결과에서만 Describe 및 List 작업을 수행할 수 있도록 허용

다음 권한 정책은 사용자에게 `ListFindings` 및 `DescribeFindings` 작업만 실행할 수 있는 권한을 부여합니다. 이러한 작업은 Amazon Inspector 결과에 대한 정보를 보여 줍니다. `Resource` 요소에 와일드카드 문자(*)가 있으면 계정이 소유한 모든 Amazon Inspector 리소스에 작업이 허용됩니다.

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Effect":"Allow",
         "Action": [
                  "inspector:DescribeFindings",
                  "inspector:ListFindings"
         ],
```

```
            "Resource":"*"
        }
    ]
}
```

Amazon Inspector ID 기반 정책 예제를 보려면 Amazon Inspector Classic의 자격 증명 기반 정책 예 섹션을 참조하세요.

Amazon Inspector에 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. 문에는 `Resource`또는 `NotResource`요소가 반드시 추가되어야 합니다. 모범 사례에 따라 Amazon 리소스 이름(ARN)을 사용하여 리소스를 지정합니다. 리소스 수준 권한이라고 하는 특정 리소스 유형을 지원하는 작업에 대해 이를 수행할 수 있습니다.

작업 나열과 같이 리소스 수준 권한을 지원하지 않는 작업의 경우, 와일드카드(*)를 사용하여 해당 문이 모든 리소스에 적용됨을 나타냅니다.

```
"Resource": "*"
```

Amazon Inspector 리소스 유형 및 해당 ARN의 목록을 보려면 서비스 권한 부여 참조에서 Amazon Inspector Classic에서 정의한 리소스를 참조하세요. 각 리소스의 ARN을 지정할 수 있는 작업을 알아보려면 Amazon Inspector Classic에서 정의한 작업을 참조하세요.

Amazon Inspector ID 기반 정책 예제를 보려면 Amazon Inspector Classic의 자격 증명 기반 정책 예 섹션을 참조하세요.

Amazon Inspector에 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` 요소(또는 `Condition` 블록)를 사용하면 정책이 발효되는 조건을 지정할 수 있습니다. `Condition` 요소는 옵션입니다. 같거나 작음과 같은 조건 연산자를 사용하여 정책의 조건을 요청의 값과 일치시키는 조건식을 생성할 수 있습니다.

한 문에서 여러 `Condition` 요소를 지정하거나 단일 `Condition` 요소에서 여러 키를 지정하는 경우, AWS 는 논리적 `AND` 작업을 사용하여 평가합니다. 단일 조건 키에 여러 값을 지정하는 경우는 논리적 `OR` 작업을 사용하여 조건을 AWS 평가합니다. 문의 권한을 부여하기 전에 모든 조건을 충족해야 합니다.

조건을 지정할 때 자리 표시자 변수를 사용할 수도 있습니다. 예를 들어, IAM 사용자에게 IAM 사용자 이름으로 태그가 지정된 경우에만 리소스에 액세스할 수 있는 권한을 부여할 수 있습니다. 자세한 내용은 IAM 사용 설명서의 IAM 정책 요소: 변수 및 태그를 참조하세요.

AWS 는 전역 조건 키와 서비스별 조건 키를 지원합니다. 모든 AWS 전역 조건 키를 보려면 IAM 사용 설명서의 AWS 전역 조건 컨텍스트 키를 참조하세요.

Amazon Inspector 조건 키 목록을 보려면 서비스 승인 참조의 Amazon Inspector Classic에 사용되는 조건 키를 참조하세요. 조건 키를 사용할 수 있는 작업과 리소스를 알아보려면 Amazon Inspector Classic에서 정의한 작업을 참조하세요.

Amazon Inspector ID 기반 정책 예제를 보려면 Amazon Inspector Classic의 자격 증명 기반 정책 예 섹션을 참조하세요.

Amazon Inspector의 ACL

ACL 지원: 아니요

액세스 제어 목록(ACL)은 어떤 위탁자(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.

Amazon Inspector를 사용한 ABAC

ABAC 지원(정책의 태그): 부분적

속성 기반 액세스 제어(ABAC)는 속성에 근거하여 권한을 정의하는 권한 부여 전략입니다. 에서는 AWS이러한 속성을 태그라고 합니다. IAM 엔터티(사용자 또는 역할) 및 많은 AWS 리소스에 태그를 연결할 수 있습니다. ABAC의 첫 번째 단계로 개체 및 리소스에 태그를 지정합니다. 그런 다음 위탁자의 태그가 액세스하려는 리소스의 태그와 일치할 때 작업을 허용하도록 ABAC 정책을 설계합니다.

ABAC는 빠르게 성장하는 환경에서 유용하며 정책 관리가 번거로운 상황에 도움이 됩니다.

태그에 근거하여 액세스를 제어하려면 `aws:ResourceTag/key-name`, `aws:RequestTag/key-name` 또는 `aws:TagKeys` 조건 키를 사용하여 정책의 조건 요소에 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 정의를 참조하세요. ABAC 설정 단계가 포함된 자습서를 보려면 IAM 사용 설명서의 속성 기반 액세스 제어(ABAC) 사용을 참조하세요.

Amazon Inspector에서 임시 보안 인증 정보 사용

임시 자격 증명 지원: 예

일부 AWS 서비스 는 임시 자격 증명을 사용하여 로그인할 때 작동하지 않습니다. 임시 자격 증명으로 AWS 서비스 작업하는를 비롯한 추가 정보는 AWS 서비스 IAM 사용 설명서의 IAM으로 작업하는 섹션을 참조하세요.

사용자 이름 및 암호를 제외한 방법을 AWS Management Console 사용하여에 로그인하는 경우 임시 자격 증명을 사용합니다. 예를 들어 회사의 SSO(Single Sign-On) 링크를 AWS 사용하여에 액세스하면 해당 프로세스가 임시 자격 증명을 자동으로 생성합니다. 또한 콘솔에 사용자로 로그인한 다음 역할을 전환할 때 임시 자격 증명을 자동으로 생성합니다. 역할 전환에 대한 자세한 내용은 IAM 사용 설명서의 사용자에서 IAM 역할로 전환(콘솔)을 참조하세요.

AWS CLI 또는 AWS API를 사용하여 임시 자격 증명을 수동으로 생성할 수 있습니다. 그런 다음 이러한 임시 자격 증명을 사용하여 장기 액세스 키를 사용하는 대신 임시 자격 증명을 동적으로 생성하는 access AWS. AWS recommends에 액세스할 수 있습니다. 자세한 정보는 IAM의 임시 보안 자격 증명 섹션을 참조하세요.

Amazon Inspector에 대한 교차 서비스 보안 주체 권한

전달 액세스 세션(FAS) 지원: 예

IAM 사용자 또는 역할을 사용하여에서 작업을 수행하는 경우 AWS보안 주체로 간주됩니다. 일부 서비스를 사용하는 경우, 다른 서비스에서 다른 작업을 시작하는 작업을 수행할 수 있습니다. FAS는를 호출하는 보안 주체의 권한을 다운스트림 서비스에 AWS 서비스 대한 요청과 AWS 서비스함께 사용합니다. FAS 요청은 서비스가 완료하기 위해 다른 AWS 서비스 또는 리소스와의 상호 작용이 필요한 요청을 수신할 때만 이루어집니다. 이 경우, 두 작업을 모두 수행할 수 있는 권한이 있어야 합니다. FAS 요청 시 정책 세부 정보는 전달 액세스 세션을 참조하세요.

Amazon Inspector의 서비스 역할

서비스 역할 지원: 아니요

서비스 역할은 서비스가 사용자를 대신하여 작업을 수행하는 것으로 가정하는 IAM 역할입니다. IAM 관리자는 IAM 내에서 서비스 역할을 생성, 수정 및 삭제할 수 있습니다. 자세한 정보는 IAM 사용 설명서의 Create a role to delegate permissions to an AWS 서비스를 참조하세요.

> **Warning**
> 서비스 역할에 대한 권한을 변경하면 Amazon Inspector 기능이 중단될 수 있습니다. Amazon Inspector에서 관련 지침을 제공하는 경우에만 서비스 역할을 편집합니다.

Amazon Inspector의 서비스 연결 역할

서비스 링크 역할 지원: 예

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

Amazon Inspector 서비스 연결 역할 생성 또는 관리에 대한 자세한 정보는 Amazon Inspector Classic에 대해 서비스 연결 역할 사용 섹션을 참조하세요.

Amazon Inspector Classic의 자격 증명 기반 정책 예

기본적으로 사용자 및 역할은 Amazon Inspector 리소스를 생성하거나 수정할 수 있는 권한이 없습니다. 또한 AWS Management Console, AWS Command Line Interface (AWS CLI) 또는 AWS API를 사용하여 작업을 수행할 수 없습니다. 사용자에게 사용자가 필요한 리소스에서 작업을 수행할 권한을 부여하려면 IAM 관리자가 IAM 정책을 생성하면 됩니다. 그런 다음 관리자가 IAM 정책을 역할에 추가하고, 사용자가 역할을 맡을 수 있습니다.

이러한 예제 JSON 정책 문서를 사용하여 IAM 자격 증명 기반 정책을 생성하는 방법을 알아보려면 IAM 사용 설명서의 IAM 정책 생성(콘솔)을 참조하세요.

각 리소스 유형에 대한 ARN 형식을 비롯하여 Amazon Inspector에서 정의되는 작업 및 리소스 유형에 대한 자세한 내용은 서비스 승인 참조의 Amazon Inspector Classic에 사용되는 작업, 리소스 및 조건 키를 참조하세요.

주제

- 정책 모범 사례
- Amazon Inspector 콘솔 사용
- 사용자가 자신의 고유한 권한을 볼 수 있도록 허용
- 사용자가 Amazon Inspector 결과에서만 Describe 및 List 작업을 수행할 수 있도록 허용

정책 모범 사례

자격 증명 기반 정책에 따라 계정에서 사용자가 Amazon Inspector 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 따릅니다.

- 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 정보는 IAM 사용 설명서의 AWS 관리형 정책 또는 AWS 직무에 대한 관리형 정책을 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 권한을 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 특정를 통해 사용되는 경우 조건을 사용하여 서비스 작업에 대한 액세스 권한을 부여할 수도 있습니다 AWS CloudFormation. 자세한 정보는 IAM 사용 설명서의 IAM JSON 정책 요소: 조건을 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 검증을 참조하세요.
- 다중 인증(MFA) 필요 -에서 IAM 사용자 또는 루트 사용자가 필요한 시나리오가 있는 경우 추가 보안을 위해 MFA를 AWS 계정켭니다. API 작업을 직접 호출할 때 MFA가 필요하면 정책에 MFA 조건을 추가합니다. 자세한 내용은 IAM 사용 설명서의 MFA를 통한 보안 API 액세스를 참조하세요.

IAM의 모범 사례에 대한 자세한 내용은 IAM 사용 설명서의 IAM의 보안 모범 사례를 참조하세요.

Amazon Inspector 콘솔 사용

Amazon Inspector Classic 콘솔에 액세스하려면 최소한의 권한 집합이 있어야 합니다. 이러한 권한은 AWS 계정에서 Amazon Inspector 리소스에 대한 세부 정보를 나열하고 볼 수 있도록 허용해야 합니다. 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.

사용자와 역할이 여전히 Amazon Inspector 콘솔을 사용할 수 있도록 하려면 Amazon Inspector *ConsoleAccess* 또는 *ReadOnly* AWS 관리형 정책도 엔터티에 연결합니다. 자세한 내용은 IAM 사용 설명서의 사용자에게 권한 추가를 참조하세요.

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": "*"
        }
    ]
}
```

사용자가 Amazon Inspector 결과에서만 Describe 및 List 작업을 수행할 수 있도록 허용

다음 권한 정책은 사용자에게 `ListFindings` 및 `DescribeFindings` 작업만 실행할 수 있는 권한을 부여합니다. 이러한 작업은 Amazon Inspector 결과에 대한 정보를 보여 줍니다. `Resource` 요소에 와일드카드 문자(*)가 있으면 계정이 소유한 모든 Amazon Inspector 리소스에 작업이 허용됩니다.

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Effect":"Allow",
         "Action": [
                  "inspector:DescribeFindings",
                  "inspector:ListFindings"
         ],
         "Resource":"*"
      }
   ]
}
```

Amazon Inspector Classic에 대해 서비스 연결 역할 사용

Amazon Inspector Classic은 AWS Identity and Access Management (IAM) 서비스 연결 역할을 사용합니다. 서비스 연결 역할은 Amazon Inspector Classic에 직접 연결되는 고유한 유형의 IAM 역할입니다. 서비스 연결 역할은 Amazon Inspector Classic에 의해 사전 정의되며 서비스가 사용자를 대신하여 다른 AWS 서비스 를 호출하는 데 필요한 모든 권한을 포함합니다.

필요한 권한을 수동으로 추가할 필요가 없으므로 서비스 연결 역할로 Amazon Inspector Classic을 더 쉽게 설정할 수 있습니다. Amazon Inspector Classic에서 서비스 연결 역할의 권한을 정의하므로 다르

게 정의되지 않은 한, Amazon Inspector Classic만 해당 역할을 수임할 수 있습니다. 정의된 권한에는 신뢰 정책과 권한 정책이 포함되며 이 권한 정책은 다른 IAM 엔티티에 연결할 수 없습니다.

먼저 관련 리소스를 삭제해야만 서비스 연결 역할을 삭제할 수 있습니다. 이렇게 하면 리소스에 대한 액세스 권한을 실수로 삭제할 수 없기 때문에 Amazon Inspector Classic 리소스가 보호됩니다.

서비스 연결 역할을 지원하는 다른 서비스에 대한 자세한 내용은 AWS IAM으로 작업하는 서비스를 참조하고 서비스 연결 역할 열에서 예인 서비스를 찾습니다. 해당 서비스에 대한 서비스 연결 역할 설명서를 보려면 예 링크를 선택합니다.

Amazon Inspector Classic에 대한 서비스 연결 역할 권한

Amazon Inspector Classic은 AWSServiceRoleForAmazonInspector – ServiceLinkedRoleDescription 라는 서비스 연결 역할을 사용합니다.

AWSServiceRoleForAmazonInspector 서비스 연결 역할은 역할을 수임하기 위해 다음 서비스를 신뢰합니다.

- `inspector.amazonaws.com`

AmazonInspectorServiceRolePolicy라는 역할 권한 정책은 Amazon Inspector Classic이 지정된 리소스에 대해 다음 작업을 완료하도록 허용합니다.

- 작업: `arn:aws:iam::*:role/aws-service-role/inspector.amazonaws.com/AWSServiceRoleForAmazonInspector`에 대한 `iam:CreateServiceLinkedRole`

IAM 엔터티(IAM 사용자, 그룹, 역할 등)가 서비스 연결 역할을 작성하고 편집하거나 삭제할 수 있도록 권한을 구성해야 합니다. 자세한 내용은 IAM 사용 설명서의 서비스 연결 역할 권한을 참조하세요.

Amazon Inspector Classic에 대한 서비스 연결 역할 생성

서비스 링크 역할은 수동으로 생성할 필요가 없습니다. AWS Management Console AWS CLI, 또는 AWS API에서 CompleteThisCreateActionInThisService를 완료하면 Amazon Inspector Classic이 서비스 연결 역할을 생성합니다.

Amazon Inspector Classic에 대한 서비스 연결 역할 편집

Amazon Inspector Classic은 AWSServiceRoleForAmazonInspector 서비스 연결 역할을 편집하도록 허용하지 않습니다. 서비스 링크 역할을 생성한 후에는 다양한 개체가 역할을 참조할 수 있기 때문에

역할 이름을 변경할 수 없습니다. 하지만 IAM을 사용하여 역할의 설명을 편집할 수 있습니다. 자세한 내용은 IAM 사용 설명서의 서비스 연결 역할 편집을 참조하세요.

Amazon Inspector Classic에 대한 서비스 연결 역할 삭제

서비스 연결 역할이 필요한 기능 또는 서비스가 더 이상 필요 없는 경우에는 해당 역할을 삭제하는 것이 좋습니다. 이렇게 하면 적극적으로 모니터링하거나 유지 관리하지 않는 미사용 개체가 없게 됩니다. 단, 서비스 링크 역할에 대한 리소스를 먼저 정리해야 수동으로 삭제할 수 있습니다.

> **Note**
>
> 리소스를 삭제하려고 할 때 Amazon Inspector Classic 서비스가 역할을 사용 중이면 삭제에 실패할 수 있습니다. 이 문제가 발생하면 몇 분 기다렸다가 작업을 다시 시도하세요.

`AWSServiceRoleForAmazonInspector`에서 사용하는 Amazon Inspector Classic 리소스를 삭제하려면,

- Amazon Inspector Classic이 AWS 리전 실행 중인 모든 AWS 계정 에서 이에 대한 평가 대상을 삭제합니다. 자세한 내용은 Amazon Inspector Classic 평가 대상 단원을 참조하십시오.

IAM을 사용하여 수동으로 서비스 연결 역할을 삭제하려면 다음을 수행하세요.

IAM 콘솔 AWS CLI, 또는 AWS API를 사용하여 AWSServiceRoleForAmazonInspector 서비스 연결 역할을 삭제합니다. 자세한 내용은 IAM 사용 설명서의 서비스 연결 역할 삭제를 참조하십시오.

Amazon Inspector Classic 서비스 연결 역할이 지원되는 리전

Amazon Inspector Classic은 서비스가 제공되는 모든 리전에서 서비스 연결 역할 사용을 지원합니다. 자세한 내용을 알아보려면 AWS 리전 및 엔드포인트를 참조하세요.

Amazon Inspector Classic ID 및 액세스 문제 해결

다음 정보를 사용하여 Amazon Inspector 및 IAM으로 작업할 때 발생할 수 있는 일반적인 문제를 진단하고 수정할 수 있습니다.

주제

- Amazon Inspector에서 작업을 수행할 권한이 없음

- iam:PassRole을 수행하도록 인증되지 않음
- 내 외부의 사람이 내 Amazon Inspector 리소스 AWS 계정 에 액세스하도록 허용하고 싶습니다.

Amazon Inspector에서 작업을 수행할 권한이 없음

작업을 수행할 권한이 없다는 오류가 수신되면, 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 `inspector:`*`GetWidget`* 권한이 없을 때 발생합니다.

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

이 경우, `inspector:`*`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 수 있는 권한이 없다는 오류가 수신되면 Amazon Inspector에 역할을 전달할 수 있도록 정책을 업데이트해야 합니다.

일부 AWS 서비스 에서는 새 서비스 역할 또는 서비스 연결 역할을 생성하는 대신 기존 역할을 해당 서비스에 전달할 수 있습니다. 이렇게 하려면 사용자가 서비스에 역할을 전달할 수 있는 권한을 가지고 있어야 합니다.

다음 예제 오류는 `marymajor`라는 IAM 사용자가 콘솔을 사용하여 Amazon Inspector에서 태스크를 수행하려고 하는 경우에 발생합니다. 하지만 작업을 수행하려면 서비스 역할이 부여한 권한이 서비스에 있어야 합니다. Mary는 서비스에 역할을 전달할 수 있는 권한을 가지고 있지 않습니다.

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

이 경우, Mary가 `iam:PassRole` 작업을 수행할 수 있도록 Mary의 정책을 업데이트해야 합니다.

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

내 외부의 사람이 내 Amazon Inspector 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.

자세히 알아보려면 다음을 참조하세요.

- Amazon Inspector에서 이러한 기능을 지원하는지 여부를 알아보려면 Amazon Inspector Classic에서 IAM을 사용하는 방법 섹션을 참조하세요.
- 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.
- 타사에 리소스에 대한 액세스 권한을 제공하는 방법을 알아보려면 IAM 사용 설명서의 타사가 AWS 계정 소유한에 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 액세스를 참조하세요.

Amazon Inspector Classic 로깅 및 모니터링

Amazon Inspector Classic은 Amazon Inspector Classic에서 사용자 AWS CloudTrail, 역할 또는 서비스가 수행한 작업에 대한 레코드를 제공하는 AWS 서비스와 통합됩니다. CloudTrail은 Amazon Inspector Classic 콘솔의 호출과 Amazon Inspector Classic API 작업에 대한 코드 호출을 포함하여 Amazon Inspector Classic에 대한 모든 API 호출을 이벤트로 캡처합니다.

Amazon Inspector Classic에서 CloudTrail 로깅을 사용하는 방법에 대한 자세한 내용은 를 사용하여 Amazon Inspector Classic API 호출 로깅 AWS CloudTrail을 참조하십시오.

원시 데이터를 수집하여 읽기 가능하며 실시간에 가까운 지표로 처리하는 Amazon CloudWatch를 통해 Amazon Inspector Classic을 모니터링할 수 있습니다. Amazon Inspector Classic은 기본적으로 측정치 데이터를 5분 동안 CloudWatch에 전송합니다.

Amazon Inspector Classic과 함께 CloudWatch를 사용하는 방법에 대한 자세한 내용은 Amazon CloudWatch를 사용하여 Amazon Inspector Classic 모니터링하기을 참조하십시오.

Amazon Inspector Classic의 인시던트 대응

Amazon Inspector Classic에 대한 인시던트 대응은 AWS 책임입니다. AWS 에는 인시던트 대응을 관리하는 공식적이고 문서화된 정책 및 프로그램이 있습니다.

AWS 광범위한 영향을 미치는 운영 문제는 AWS 서비스 상태 대시보드에 게시됩니다.

AWS Health Dashboard를 통해 개별 계정에도 운영 문제가 게시됩니다. 사용 방법에 대한 자세한 내용은 AWS Health 사용 설명서를 AWS Health Dashboard참조하세요.

Amazon Inspector Classic의 규정 준수 확인

타사 감사자는 여러 규정 준수 프로그램의 일환으로 Amazon Inspector Classic의 보안 및 AWS 규정 준수를 평가합니다. 여기에는 SOC, PCI, FedRAMP, HIPAA 등이 포함됩니다.

특정 규정 준수 프로그램 범위의 AWS 서비스 목록은 규정 준수 프로그램 제공 범위 내 AWS 서비스규정 준수 프로그램 참조하세요. 일반 정보는 AWS 규정 준수 프로그램.

를 사용하여 타사 감사 보고서를 다운로드할 수 있습니다 AWS Artifact. 자세한 내용은 AWS Artifact에서 보고서 다운로드를 참조하세요.

Amazon Inspector Classic 사용 시 규정 준수 책임은 데이터의 민감도, 회사의 규정 준수 목표 및 관련 법률과 규정에 따라 결정됩니다.는 규정 준수를 지원하기 위해 다음 리소스를 AWS 제공합니다.

- 보안 및 규정 준수 빠른 시작 안내서: 이 배포 안내서에서는 아키텍처 고려 사항에 관해 설명하고 AWS에서 보안 및 규정 준수에 중점을 둔 기본 환경을 배포하기 위한 단계를 제공합니다.
- Amazon Web Services의 HIPAA 보안 및 규정 준수를 위한 설계 -이 백서에서는 기업이 AWS 를 사용하여 HIPAA 준수 애플리케이션을 생성하는 방법을 설명합니다.
- AWS 규정 준수 리소스 -이 워크북 및 가이드 모음은 산업 및 위치에 적용될 수 있습니다.
- AWS Config 개발자 안내서의 규칙을 사용하여 리소스 평가 -이 AWS Config 서비스는 리소스 구성이 내부 관행, 업계 지침 및 규정을 얼마나 잘 준수하는지 평가합니다.
- AWS Security Hub -이 AWS 서비스는 보안 업계 표준 및 모범 사례 준수 여부를 확인하는 데 도움이 AWS 되는 내 보안 상태에 대한 포괄적인 보기를 제공합니다.

Amazon Inspector Classic의 복원성

AWS 글로벌 인프라는 AWS 리전 및 가용 영역을 중심으로 구축됩니다. AWS 리전은 물리적으로 분리되고 격리된 여러 가용 영역을 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.

Amazon Inspector Classic은 가용성이 높으며 여러 가용 영역에서 컴퓨팅 리소스를 사용하여 쿼리를 실행합니다. 특정 가용 영역에 연결할 수 없는 경우 쿼리를 자동으로 적절하게 라우팅합니다.

Amazon Inspector Classic은 Amazon S3를 기본 데이터 저장소로 사용하기 때문에 데이터의 가용성과 내구성이 높습니다. Amazon S3는 중요한 데이터를 저장할 수 있도록 견고한 인프라를 제공합니다. 99.999999999%의 객체 내구성을 제공하도록 설계되었습니다. 데이터가 여러 시설과 각 시설의 여러 디바이스에 중복 저장됩니다.

Amazon Inspector Classic의 인프라 보안

관리형 서비스인 Amazon Inspector Classic은 AWS 글로벌 네트워크 보안으로 보호됩니다. AWS 보안 서비스 및가 인프라를 AWS 보호하는 방법에 대한 자세한 내용은 AWS 클라우드 보안을 참조하세요. 인프라 보안 모범 사례를 사용하여 AWS 환경을 설계하려면 보안 원칙 AWS Well-Architected Framework의 인프라 보호를 참조하세요.

AWS 에서 게시한 API 호출을 사용하여 네트워크를 통해 Amazon Inspector Classic에 액세스합니다. 고객은 다음을 지원해야 합니다.

- Transport Layer Security(TLS) TLS 1.2는 필수이며 TLS 1.3을 권장합니다.
- DHE(Ephemeral Diffie-Hellman) 또는 ECDHE(Elliptic Curve Ephemeral Diffie-Hellman)와 같은 완전 전송 보안(PFS)이 포함된 암호 제품군 Java 7 이상의 최신 시스템은 대부분 이러한 모드를 지원합니다.

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

Amazon Inspector Classic 네트워크 및 에이전트 보안에 대한 자세한 내용은 the section called “네트워크 및 Amazon Inspector Classic 에이전트 보안” 섹션을 참조하십시오.

Amazon Inspector Classic의 구성 및 취약성 분석

Amazon Inspector Classic은 평가하려는 EC2 인스턴스의 운영 체제에 선택적으로 설치할 수 있는 에이전트라는 사전 정의된 소프트웨어를 제공합니다. 에이전트는 원격 측정이라는 광범위한 구성 데이터 세트를 수집합니다. Amazon Inspector Classic 에이전트에 대한 자세한 내용은 Amazon Inspector Classic 에이전트 섹션을 참조하십시오.

Amazon Inspector Classic의 보안 모범 사례

Amazon Inspector Classic은 자체 보안 정책을 개발하고 구현할 때 고려해야 할 여러 보안 기능을 제공합니다. 다음 모범 사례는 일반적인 지침이며 완벽한 보안 솔루션을 나타내지는 않습니다. 이러한 모범 사례는 환경에 적절하지 않거나 충분하지 않을 수 있으므로 참고용으로만 사용하세요.

Amazon Inspector Classic의 보안 모범 사례 목록은 the section called “Amazon Inspector Classic의 보안 모범 사례” 섹션을 참조하십시오.

Amazon Inspector Classic 에이전트

Amazon Inspector Classic 에이전트는 Amazon EC2 인스턴스에 대해 설치된 패키지 정보 및 소프트웨어 구성을 수집하는 엔터티입니다. 모든 경우에 요구되진 않지만, 보안성을 완전히 평가하기 위해선 대상 Amazon EC2 인스턴스마다 Amazon Inspector Classic 에이전트를 설치해야 합니다.

에이전트를 설치, 제거 및 다시 설치하는 방법, 설치된 에이전트가 실행 중인지 확인하는 방법 및 에이전트에 대한 프록시 지원을 구성하는 방법에 대한 자세한 내용은 Linux 기반 운영 체제에서 Amazon Inspector Classic 에이전트 작업 및 Windows 기반 운영 체제에서 Amazon Inspector Classic 에이전트 작업 섹션을 참조하십시오.

> **Note**
>
> Amazon Inspector Classic 에이전트는 네트워크 연결성 규칙 패키지를 실행하는 데 필수가 아닙니다.

> **Important**
>
> Amazon Inspector Classic 에이전트는 올바르게 작동하기 위해 Amazon EC2 인스턴스 메타데이터를 사용합니다. 인스턴스 메타데이터 서비스 버전 1 또는 버전 2(IMDSv1 또는 IMDSv2)를 사용하여 인스턴스 메타데이터에 액세스합니다. EC2 인스턴스 메타데이터와 액세스 방법에 대한 자세한 내용은 인스턴스 메타데이터 및 사용자 데이터를 참조하십시오.

주제

- Amazon Inspector Classic 에이전트 권한
- 네트워크 및 Amazon Inspector Classic 에이전트 보안
- Amazon Inspector Classic 에이전트 업데이트
- 원격 측정 데이터 수명 주기
- Amazon Inspector Classic에서 AWS 계정으로 액세스 제어
- Amazon Inspector Classic 에이전트 제한
- Amazon Inspector Classic 에이전트 설치하기
- Linux 기반 운영 체제에서 Amazon Inspector Classic 에이전트 작업

- Windows 기반 운영 체제에서 Amazon Inspector Classic 에이전트 작업
- (선택 사항) Linux 기반 운영 체제에서 Amazon Inspector Classic 에이전트 설치 스크립트의 서명을 확인합니다.
- (선택 사항) Windows 기반 운영 체제에서 Amazon Inspector Classic 에이전트 설치 스크립트의 서명을 확인합니다.

Amazon Inspector Classic 에이전트 권한

Amazon Inspector Classic 에이전트를 설치하려면 관리자 권한이나 루트 권한이 필요합니다. 지원되는 Linux 기반 운영 체제에서 에이전트는 루트 액세스 권한으로 실행되는 사용자 모드 실행 파일로 구성됩니다. 지원되는 Windows 기반 운영 체제에서 에이전트는 각각 `LocalSystem` 권한이 있는 사용자 모드로 실행되는 업데이터 서비스 및 에이전트 서비스로 구성됩니다.

네트워크 및 Amazon Inspector Classic 에이전트 보안

Amazon Inspector Classic 에이전트는 Amazon Inspector Classic 서비스와의 모든 통신을 시작합니다. 이는 에이전트가 원격 측정 데이터를 전송할 수 있도록 퍼블릭 엔드포인트에 대한 아웃바운드 네트워크 경로를 가져야 한다는 것을 의미합니다. 예를 들어, 에이전트가 `arsenal.<region>.amazonaws.com`에 연결할 수 있거나 엔드포인트가 `s3.dualstack.<region>.amazonaws.com`의 Amazon S3 버킷일 수 있습니다. 를 Amazon Inspector Classic을 실행 중인 실제 AWS 리전`<region>`으로 바꿔야 합니다. 자세한 내용은 AWS IP 주소 범위를 참조하십시오. 에이전트의 모든 연결이 아웃바운드로 설정되므로 Amazon Inspector Classic에서 에이전트로 인바운드 통신을 허용하도록 보안 그룹의 포트를 열 필요는 없습니다.

에이전트는 EC2 인스턴스의 역할과 연결된 AWS 자격 증명을 사용하거나 역할이 할당되지 않은 경우 인스턴스의 메타데이터 문서를 사용하여 인증된 TLS 보호 채널을 통해 Amazon Inspector Classic과 주기적으로 통신합니다. 에이전트가 인증되면 에이전트는 서비스에 하트비트 메시지를 보내고 그에 대한 응답으로 서비스에서 명령을 받습니다. 평가가 예약된 경우 에이전트는 해당 평가에 대한 명령을 받습니다. 이 명령은 구조화된 JSON 파일이며 에이전트에서 미리 구성된 특정 센서를 활성화 또는 비활성화하도록 에이전트에 지시합니다. 각 명령 작업은 에이전트 내에서 미리 정의됩니다. 임의의 명령은 실행할 수 없습니다.

평가 중에 에이전트는 시스템에서 원격 측정 데이터를 수집하여 TLS로 보호된 채널을 통해 Amazon Inspector Classic에 다시 보냅니다. 에이전트는 자신이 데이터를 수집하는 시스템을 변경하지 않습니다. 에이전트는 원격 측정 데이터를 수집한 후 Amazon Inspector Classic에 원격 측정 데이터를 다시 보내서 처리합니다. 에이전트가 생성하는 원격 측정 데이터 이외에 에이전트는 평가하는 시스템 또는

평가 대상에 대한 다른 데이터를 수집하거나 전송할 수 없습니다. 현재 에이전트에서 원격 측정 데이터를 가로채서 검사하기 위해 노출된 메서드는 없습니다.

Amazon Inspector Classic 에이전트 업데이트

Amazon Inspector Classic 에이전트에 대한 업데이트를 사용할 수 있게 되면 Amazon S3에서 자동으로 다운로드되어 적용됩니다. 이때 필수 종속성도 업데이트됩니다. 자동 업데이트 기능의 경우 EC2 인스턴스에 설치한 에이전트를 추적하거나 해당 에이전트의 버전 관리를 수동으로 유지할 필요가 없습니다. 모든 업데이트는 관련 보안 표준을 준수하기 위해 감사된 Amazon 변경 제어 프로세스의 적용을 받습니다.

에이전트의 보안을 강화하기 위해 에이전트와 자동 업데이트 릴리스 사이트(S3) 사이의 모든 통신은 TLS 연결을 통해 수행되며 서버는 인증됩니다. 자동 업데이트 프로세스와 관련된 모든 바이너리는 디지털 서명되며 서명은 설치 전에 업데이터가 확인합니다. 자동 업데이트 프로세스는 평가 기간이 아닌 동안에만 실행됩니다. 오류가 감지되면 업데이트 프로세스가 롤백하여 업데이트를 다시 시도할 수 있습니다. 마지막으로, 에이전트 업데이트 프로세스는 에이전트 기능만 업그레이드하는 역할을 합니다. 어떤 특정 정보도 업데이트 워크플로의 일부로 에이전트에서 Amazon Inspector Classic으로 전송되지 않습니다. 업데이트 프로세스의 일부로 전달되는 유일한 정보는 기본 설치 성공/실패 원격 측정이며, 해당되는 경우 업데이트 실패 진단 정보가 전달됩니다.

원격 측정 데이터 수명 주기

평가 실행 중에 Amazon Inspector Classic 에이전트에서 생성하는 원격 측정 데이터는 JSON 파일로 형식이 지정됩니다. 파일은 TLS를 통해 거의 실시간으로 Amazon Inspector Classic에 전달됩니다. 여기에서 평가별로 실행되는 임시 KMS 파생 키로 암호화됩니다. 그런 다음 Amazon Inspector Classic 전용 Amazon S3 버킷에 안전하게 저장됩니다. Amazon Inspector Classic의 규칙 엔진은 S3 버킷의 암호화된 원격 측정 데이터에 액세스하고, 메모리에서 암호를 해독하며, 구성된 평가 규칙에 따라 데이터를 처리하여 결과를 생성합니다. S3에 저장된 원격 측정 데이터는 지원 요청을 지원하는 용도로만 보관됩니다. Amazon에서 다른 용도를 위해 사용하거나 집계하지 않습니다. 원격 측정 데이터는 Amazon Inspector Classic 데이터에 대한 표준 S3 버킷 수명 주기 정책에 따라 30일 후에 영구적으로 삭제됩니다. 현재 Amazon Inspector Classic은 수집된 원격 측정에 API 또는 S3 버킷 액세스 메커니즘을 제공하지 않습니다.

Amazon Inspector Classic에서 AWS 계정으로 액세스 제어

보안 서비스인 Amazon Inspector Classic은 태그를 쿼리하여 평가할 EC2 인스턴스를 찾아야 하는 경우에만 AWS 계정과 리소스에 액세스합니다. 이 작업은 Amazon Inspector Classic 서비스의 초기 설

정 중에 생성된 역할에 의한 표준 IAM 액세스를 통해 수행됩니다. 평가하는 중에 환경과의 모든 통신은 EC2 인스턴스에 로컬로 설치된 Amazon Inspector Classic 에이전트에 의해 시작됩니다. Amazon Inspector Classic 서비스에서 생성한 평가 대상, 평가 템플릿 및 결과 등의 서비스 객체는 Amazon Inspector Classic에서 관리하고 액세스할 수 있는 데이터베이스에만 저장됩니다.

Amazon Inspector Classic 에이전트 제한

Amazon Inspector Classic 에이전트 제한에 대한 자세한 내용은 Amazon Inspector Classic 서비스 한도 섹션을 참조하십시오.

Amazon Inspector Classic 에이전트 설치하기

Systems Manager 명령 실행을 사용하여 여러 인스턴스(Linux 기반 인스턴스와 Windows 기반 인스턴스 모두 포함)에 Amazon Inspector Classic 에이전트를 설치할 수 있습니다. 또는 각 EC2 인스턴스에 로그인하여 에이전트를 개별적으로 설치할 수 있습니다. 이 장의 절차에 두 방법이 모두 설명되어 있습니다.

또 다른 옵션으로, 콘솔의 평가 대상 정의 페이지에서 에이전트 설치 확인란을 선택하여 평가 대상에 포함된 모든 Amazon EC2 인스턴스에 에이전트를 빠르게 설치할 수 있습니다.

주제

- Systems Manager Run Command를 사용하여 여러 EC2 인스턴스에 에이전트 설치
- Linux 기반 EC2 인스턴스에 에이전트 설치
- Windows 기반 EC2 인스턴스에 에이전트 설치

> **Note**
>
> 이 장의 절차는 Amazon Inspector Classic에서 지원하는 모든 AWS 리전에 적용됩니다.

Systems Manager Run Command를 사용하여 여러 EC2 인스턴스에 에이전트 설치

Systems Manager 명령 실행을 사용하여 EC2 인스턴스에 Amazon Inspector Classic 에이전트를 설치할 수 있습니다. 이 방법을 이용하면 원격으로 동시에 여러 인스턴스에 에이전트를 설치할 수 있습니다(한 명령으로 Linux 기반 및 Windows 기반 인스턴스 모두 가능).

> **Important**
>
> Systems Manager Run Command를 사용한 에이전트 설치는 현재 Debian 운영 체제에서 지원되지 않습니다.

> **Important**
>
> 이 옵션을 이용하려면 EC2 인스턴스에 SSM 에이전트가 설치되어 있고, 명령 실행을 허용하는 IAM 역할이 지정되어 있어야 합니다. SSM 에이전트는 Amazon EC2 Windows 인스턴스와 Amazon Linux 인스턴스에 기본적으로 설치됩니다. Amazon EC2 Systems Manager에는 명령을 처리하는 EC2 인스턴스를 위한 IAM 역할과 명령을 실행하는 사용자를 위한 별도의 역할이 필요합니다. 자세한 내용은 SSM 에이전트 설치 및 구성 및 SSM에 대한 보안 역할 구성 섹션을 참조하십시오.

Systems Manager 명령 실행을 사용하여 여러 EC2 인스턴스에 에이전트 설치하려면

1. https://console.aws.amazon.com/systems-manager/ AWS Systems Manager 콘솔을 엽니다.
2. 탐색 창의 노드 도구에서 명령 실행을 선택합니다.
3. Run a command를 선택합니다.
4. 명령 문서의 경우 Amazon이 소유한 AmazonInspector-ManageAWSAgent라는 이름의 문서를 선택합니다. 이 문서에는 EC2 인스턴스에 Amazon Inspector Classic 에이전트를 설치하는 데 필요한 스크립트가 들어 있습니다.
5. 대상의 경우 다른 방법을 사용하여 EC2 인스턴스를 선택할 수 있습니다. 평가 대상의 모든 인스턴스에 에이전트를 설치하려면 평가 대상을 생성할 때 사용한 태그를 지정하면 됩니다.
6. 콘솔에서 명령 실행의 지침을 사용하여 제공되는 나머지 옵션을 선택한 다음 실행을 선택합니다.

> **Note**
>
> 평가 대상을 만들 때 여러 EC2 인스턴스(Linux 기반 및 Windows 기반)에 에이전트를 설치하거나 기존 대상에 대해 명령 실행을 사용하여 에이전트 설치 버튼을 사용할 수도 있습니다. 자세한 내용은 평가 대상 생성 단원을 참조하십시오.

Linux 기반 EC2 인스턴스에 에이전트 설치

Linux 기반 EC2 인스턴스에 Amazon Inspector Classic 에이전트를 설치하려면 다음 절차를 수행합니다.

Linux 기반 EC2 인스턴스에 에이전트를 설치하려면

1. Linux 기반 운영 체제를 실행 중인 EC2 인스턴스(Amazon Inspector Classic 에이전트를 설치할 인스턴스)에 로그인합니다.

   > **Note**
   >
   > Amazon Inspector Classic이 지원하는 운영 체제에 대한 자세한 내용은 Amazon Inspector Classic이 지원되는 운영 체제 및 리전 섹션을 참조하십시오.

2. 다음 명령 중 하나를 실행하여 에이전트 설치 스크립트를 다운로드합니다.

   - wget https://inspector-agent.amazonaws.com/linux/latest/install
   - curl -O https://inspector-agent.amazonaws.com/linux/latest/install

3. (선택 사항) 에이전트 설치 스크립트가 변경 또는 손상되지 않았는지 확인합니다. 자세한 내용은 (선택 사항) Linux 기반 운영 체제에서 Amazon Inspector Classic 에이전트 설치 스크립트의 서명을 확인합니다. 단원을 참조하십시오.

4. sudo bash install에 에이전트를 설치하려면

   > **Note**
   >
   > SELinux 환경에 에이전트를 설치하는 경우 Amazon Inspector Classic이 무제한 데몬으로 감지될 수 있습니다. 이는 에이전트 프로세스의 도메인을 기본값 `initrc_t`에서 `bin_t`로 변경하여 방지할 수 있습니다. SELinux용 에이전트를 설치하기 전에 다음 명령을 사용하여 Amazon Inspector Classic 실행 스크립트에 `bin_t` 컨텍스트를 할당하십시오.
   >
   > sudo semanage fcontext -a -t bin_t /etc/rc\.d/init\.d/awsagent
   > sudo semanage fcontext -a -t bin_t /etc/init\.d/awsagent

> **Note**
>
> 에이전트에 대한 업데이트를 사용할 수 있게 되면 Amazon S3에서 자동으로 다운로드되어 적용됩니다. 자세한 내용은 Amazon Inspector Classic 에이전트 업데이트 단원을 참조하십시오.
>
> 이 자동 업데이트 프로세스를 건너뛸 경우 에이전트를 설치할 때 다음 명령을 실행합니다.
>
> sudo bash install -u false

> **Note**
>
> (선택 사항) 에이전트 설치 스크립트를 제거하려면 rm install을 실행합니다.

5. 에이전트를 설치하는 데 필요한 다음 파일과 기능이 제대로 설치되어 있는지 확인합니다.
   - `libcurl4`(Ubuntu 18.04에 에이전트를 설치해야 함)
   - `libcurl3`
   - `libgcc1`
   - `libc6`
   - `libstdc++6`
   - `libssl1.0.1`
   - `libssl1.0.2`(Debian 9에 에이전트를 설치해야 함)
   - `libssl1.1`(Ubuntu 20.04 LTS에 에이전트를 설치해야 함)
   - `libpcap0.8`

Windows 기반 EC2 인스턴스에 에이전트 설치

Windows 기반 EC2 인스턴스에 Amazon Inspector Classic 에이전트를 설치하려면 다음 절차를 수행합니다.

Windows 기반 EC2 인스턴스에 에이전트를 설치하려면

1. Windows 기반 운영 체제를 실행 중인 EC2 인스턴스(에이전트를 설치할 인스턴스)에 로그인합니다.

> **Note**
>
> Amazon Inspector Classic이 지원하는 운영 체제에 대한 자세한 내용은 Amazon Inspector Classic이 지원되는 운영 체제 및 리전 섹션을 참조하십시오.

2. 다음 .exe 파일을 다운로드합니다.

   `https://inspector-agent.amazonaws.com/windows/installer/latest/AWSAgentInstall.exe`

3. 관리자 권한으로 명령 프롬프트 창을 열고, 다운로드한 `AWSAgentInstall.exe`를 저장한 위치로 이동한 다음, .exe 파일을 실행하여 에이전트를 설치합니다.

> **Note**
>
> 에이전트에 대한 업데이트를 사용할 수 있게 되면 Amazon S3에서 자동으로 다운로드되어 적용됩니다. 자세한 내용은 Amazon Inspector Classic 에이전트 업데이트 단원을 참조하십시오.
>
> 이 자동 업데이트 프로세스를 건너뛸 경우 에이전트를 설치할 때 다음 명령을 실행합니다.
>
> AWSAgentInstall.exe AUTOUPDATE=No

Linux 기반 운영 체제에서 Amazon Inspector Classic 에이전트 작업

Amazon Inspector Classic 에이전트를 설치 및 제거, 확인하고, 동작을 수정할 수 있습니다. Linux 기반 운영 체제를 실행하는 Amazon EC2 인스턴스에 로그인하여 다음 절차를 실행합니다. Amazon Inspector Classic에 대해 지원되는 운영 체제에 대한 자세한 내용은 Amazon Inspector Classic이 지원되는 운영 체제 및 리전 섹션을 참조하십시오.

> **Important**
>
> Amazon Inspector Classic 에이전트는 올바르게 작동하기 위해 Amazon EC2 인스턴스 메타데이터를 사용합니다. 인스턴스 메타데이터 서비스 버전 1 또는 버전 2(IMDSv1 또는 IMDSv2)를 사용하여 인스턴스 메타데이터에 액세스합니다. EC2 인스턴스 메타데이터와 액세스 방법에 대한 자세한 내용은 인스턴스 메타데이터 및 사용자 데이터를 참조하십시오.

> **Note**
> 이 섹션의 명령은 Amazon Inspector Classic에서 지원하는 모든 AWS 리전에서 작동합니다.

주제

- Amazon Inspector Classic 에이전트가 실행 중인지 확인
- Amazon Inspector Classic 에이전트 중지
- Amazon Inspector Classic 에이전트 시작
- Amazon Inspector Classic 에이전트 설정 수정
- Amazon Inspector Classic 에이전트에 대한 프록시 지원 구성하기
- Amazon Inspector Classic 에이전트 설치 제거하기

Amazon Inspector Classic 에이전트가 실행 중인지 확인

- 에이전트가 설치되고 실행 중인지 확인하려면 EC2 인스턴스에 로그인하여 다음 명령을 실행합니다.

  ```
  sudo /opt/aws/awsagent/bin/awsagent status
  ```

  이 명령은 현재 실행 중인 에이전트의 상태 또는 에이전트에 연결할 수 없음을 설명하는 오류를 반환합니다.

Amazon Inspector Classic 에이전트 중지

- 에이전트를 중지하려면 다음 명령을 실행합니다.

  ```
  sudo /etc/init.d/awsagent stop
  ```

Amazon Inspector Classic 에이전트 시작

- 에이전트를 시작하려면 다음 명령을 실행합니다.

  ```
  sudo /etc/init.d/awsagent start
  ```

Amazon Inspector Classic 에이전트 설정 수정

EC2 인스턴스에 Amazon Inspector Classic 에이전트가 설치되어 실행 중이면 `agent.cfg` 파일의 설정을 수정하여 에이전트의 동작을 변경할 수 있습니다. Linux 기반 운영 체제에서 `agent.cfg` 파일은 `/opt/aws/awsagent/etc` 디렉터리에 위치합니다. `agent.cfg` 파일을 수정 및 저장한 후 변경 사항을 적용하려면 에이전트를 중지했다 시작해야 합니다.

> **Important**
>
> AWS Support의 지침에 따라서만 `agent.cfg` 파일을 수정하는 것이 좋습니다.

Amazon Inspector Classic 에이전트에 대한 프록시 지원 구성하기

Linux 기반 운영 체제에서 에이전트에 대한 프록시 지원을 받으려면 특정 환경 변수가 포함된 에이전트 관련 구성 파일을 사용합니다. 자세한 내용은 https://wiki.archlinux.org/index.php/proxy_settings를 참조하십시오.

다음 절차 중 하나를 완료합니다.

프록시 서버를 사용하는 EC2 인스턴스에 에이전트를 설치하려면

1. `awsagent.env`라는 파일을 생성하고 `/etc/init.d/` 디렉터리에 저장합니다.
2. 다음 형식의 환경 변수를 포함하도록 `awsagent.env`를 편집합니다.

   - `export https_proxy=hostname:port`
   - `export http_proxy=hostname:port`
   - `export no_proxy=169.254.169.254`

   > **Note**
   >
   > 이전 예제 값을 반드시 유효한 호스트 이름과 포트 번호의 조합으로 대체하십시오. `no_proxy` 변수에 대한 인스턴스 메타데이터 엔드포인트(169.254.169.254)의 IP 주소를 지정합니다.

3. Linux 기반 EC2 인스턴스에 에이전트 설치 절차의 단계를 수행하여 Amazon Inspector Classic 에이전트를 설치합니다.

실행 중인 에이전트를 사용하여 EC2 인스턴스에서 프록시 지원을 구성하려면

1. 프록시 지원을 구성하려면 EC2 인스턴스에서 실행 중인 에이전트 버전이 1.0.800.1 이상이어야 합니다. 에이전트에 대한 자동 업데이트 프로세스를 활성화한 경우 Amazon Inspector Classic 에이전트가 실행 중인지 확인 절차를 사용하여 에이전트 버전이 1.0.800.1 이상인지 확인할 수 있습니다. 에이전트에 대한 자동 업데이트 프로세스를 활성화하지 않은 경우 Linux 기반 EC2 인스턴스에 에이전트 설치 절차를 수행하여 이 EC2 인스턴스에 에이전트를 다시 설치해야 합니다.
2. `awsagent.env`라는 파일을 생성하고 `/etc/init.d/` 디렉터리에 저장합니다.
3. 다음 형식의 환경 변수를 포함하도록 `awsagent.env`를 편집합니다.

   - `export https_proxy=hostname:port`
   - `export http_proxy=hostname:port`
   - `export no_proxy=169.254.169.254`

   > **Note**
   > 이전 예제 값을 반드시 유효한 호스트 이름과 포트 번호의 조합으로 대체하십시오. `no_proxy` 변수에 대한 인스턴스 메타데이터 엔드포인트(169.254.169.254)의 IP 주소를 지정합니다.

4. 다음 명령을 사용하여 에이전트를 처음 중지한 후 다시 시작합니다.

   ```
   sudo /etc/init.d/awsagent restart
   ```

   에이전트 및 자동 업데이트 프로세스 모두에서 프록시 설정을 선택 및 사용합니다.

Amazon Inspector Classic 에이전트 설치 제거하기

에이전트를 제거하려면

1. Linux 기반 운영 체제를 실행 중인 EC2 인스턴스(에이전트를 제거할 인스턴스)에 로그인합니다.

   > **Note**
   > Amazon Inspector Classic에 대해 지원되는 운영 체제에 대한 자세한 내용은 Amazon Inspector Classic이 지원되는 운영 체제 및 리전 섹션을 참조하십시오.

2. 에이전트를 제거하려면 다음 명령 중 하나를 사용합니다.

   - Amazon Linux, CentOS, 및 Red Hat의 경우, 다음 명령을 실행하십시오.

     ```
     sudo yum remove 'AwsAgent*'
     ```

   - Ubuntu 서버의 경우 다음 명령을 실행합니다.

     ```
     sudo apt-get purge 'awsagent*'
     ```

Windows 기반 운영 체제에서 Amazon Inspector Classic 에이전트 작업

Amazon Inspector Classic 에이전트를 시작, 중지하고, 동작을 수정할 수 있습니다. Windows 기반 운영 체제를 실행하는 EC2 인스턴스에 로그인하고 이 장의 절차를 실행합니다. Amazon Inspector Classic에 대해 지원되는 운영 체제에 대한 자세한 내용은 Amazon Inspector Classic이 지원되는 운영 체제 및 리전 섹션을 참조하십시오.

> **Important**
>
> Amazon Inspector Classic 에이전트는 올바르게 작동하기 위해 Amazon EC2 인스턴스 메타데이터를 사용합니다. 인스턴스 메타데이터 서비스 버전 1 또는 버전 2(IMDSv1 또는 IMDSv2)를 사용하여 인스턴스 메타데이터에 액세스합니다. EC2 인스턴스 메타데이터와 액세스 방법에 대한 자세한 내용은 인스턴스 메타데이터 및 사용자 데이터를 참조하십시오.

> **Note**
>
> 이 장의 명령은 Amazon Inspector Classic에서 지원하는 모든 AWS 리전에서 작동합니다.

주제

- Amazon Inspector Classic 에이전트를 시작 또는 중지하거나 에이전트가 실행 중인지 확인
- Amazon Inspector Classic 에이전트 설정 수정하기
- Amazon Inspector Classic 에이전트에 대한 프록시 지원 구성하기
- Amazon Inspector Classic 에이전트 설치 제거하기

Amazon Inspector Classic 에이전트를 시작 또는 중지하거나 에이전트가 실행 중인지 확인

에이전트를 시작, 중지 또는 확인하려면

1. EC2 인스턴스에서 시작, 실행을 차례로 선택한 다음, **`services.msc`**를 입력합니다.
2. 에이전트가 실행 중인 경우 상태가 시작됨 또는 실행 중으로 설정된 두 개의 서비스가 서비스 창, AWS Agent Service(AWS 에이전트 서비스) 및 AWS Agent Updater Service(AWS 에이전트 업데이터 서비스)에 나열됩니다.
3. 에이전트를 시작하려면 AWS Agent Service(AWS 에이전트 서비스)를 마우스 오른쪽 버튼으로 클릭한 다음 시작을 선택합니다. 서비스가 시작되면 상태가 시작됨 또는 실행 중으로 업데이트됩니다.
4. 에이전트를 중지하려면 AWS Agent Service(AWS 에이전트 서비스)를 마우스 오른쪽 버튼으로 클릭하고 중지을 선택합니다. 서비스가 중지된 경우 상태가 지워집니다(공백으로 표시됨). AWS Agent Updater Service(AWS 에이전트 업데이터 서비스)를 중지하면 모든 향후 개선 사항 및 수정 사항이 에이전트에 설치되지 않기 때문에 권장하지 않습니다.
5. 에이전트가 설치되고 실행 중인지 확인하려면 관리 권한을 사용하여 EC2 인스턴스에 로그인하고 명령 프롬프트를 엽니다. `C:\Program Files\Amazon Web Services\AWS Agent`로 이동하여 다음 명령을 실행합니다.

   AWSAgentStatus.exe

   이 명령은 현재 실행 중인 에이전트의 상태 또는 에이전트에 연결할 수 없음을 설명하는 오류를 반환합니다.

Amazon Inspector Classic 에이전트 설정 수정하기

EC2 인스턴스에 Amazon Inspector Classic 에이전트가 설치되어 실행 중이면 `agent.cfg` 파일의 설정을 수정하여 에이전트의 동작을 변경할 수 있습니다. Windows 기반 운영 체제에서 해당 파일은 `C:\ProgramData\Amazon Web Services\AWS Agent` 디렉터리에 위치합니다. `agent.cfg` 파일을 수정 및 저장한 후 변경 사항을 적용하려면 에이전트를 중지했다 시작해야 합니다.

> **Important**
>
> AWS Support의 지침에 따라서만 `agent.cfg` 파일을 수정하는 것이 좋습니다.

Amazon Inspector Classic 에이전트에 대한 프록시 지원 구성하기

Windows 기반 운영 체제에서 에이전트에 대한 프록시 지원을 받으려면 `WinHTTP` 프록시를 사용합니다. `netsh` 유틸리티를 사용하여 `WinHTTP` 프록시를 설정하려면 Windows Hypertext Transfer Protocol(WINHTTP)용 Netsh 명령을 참조하십시오.

> **Important**
>
> Windows 기반 인스턴스에는 HTTPS 프록시만 지원됩니다.

다음 절차 중 하나를 완료합니다.

프록시 서버를 사용하는 EC2 인스턴스에 에이전트를 설치하려면

1. .exe 파일 `https://d1wk0tztpsntt1.cloudfront.net/windows/installer/latest/AWSAgentInstall.exe`를 다운로드합니다.
2. 명령 프롬프트 창이나 PowerShell 창을 엽니다(관리 권한 사용). 다운로드한 `AWSAgentInstall.exe`를 저장한 위치로 이동한 후 다음 명령을 실행합니다.

   ```
   .\AWSAgentInstall.exe /install USEPROXY=1
   ```

실행 중인 에이전트를 사용하여 EC2 인스턴스에서 프록시 지원을 구성하려면

1. 프록시 지원을 구성하려면 EC2 에이전트에서 실행 중인 Amazon Inspector Classic 에이전트 버전이 1.0.0.59 이상이어야 합니다. 에이전트에 대한 자동 업데이트 프로세스를 활성화한 경우 Amazon Inspector Classic 에이전트를 시작 또는 중지하거나 에이전트가 실행 중인지 확인 절차를 사용하여 에이전트 버전이 1.0.0.59 이상인지 확인할 수 있습니다. 에이전트에 대한 자동 업데이트 프로세스를 활성화하지 않은 경우 Windows 기반 EC2 인스턴스에 에이전트 설치 절차를 수행하여 이 EC2 인스턴스에 에이전트를 다시 설치해야 합니다.
2. 레지스트리 편집기를 엽니다(`regedit.exe`).
3. 레지스트리 키 `"HKEY_LOCAL_MACHINE/SOFTWARE/Amazon Web Services/AWS Agent Updater"`로 이동합니다.
4. 이 레지스트리 키 내에 `"UseProxy"`라는 레지스트리 `DWORD(32bit)` 값을 생성합니다.
5. 값을 두 번 클릭하여 값을 1로 설정합니다.
6. **`services.msc`**를 입력하고, 서비스 창에서 AWS 에이전트 서비스와 AWS 업데이터 서비스를 찾은 후에 각 프로세스를 다시 시작합니다. 두 프로세스가 모두 성공적으로 재시작되면

`AWSAgentStatus.exe` 파일을 실행합니다(Amazon Inspector Classic 에이전트를 시작 또는 중지하거나 에이전트가 실행 중인지 확인의 5단계 참조). 에이전트의 상태를 보고 구성된 프록시를 사용 중인지 확인합니다.

Amazon Inspector Classic 에이전트 설치 제거하기

에이전트를 제거하려면

1. Windows 기반 운영 체제를 실행 중인 EC2 인스턴스(Amazon Inspector Classic 에이전트를 제거할 인스턴스)에 로그인합니다.

   > **Note**
   >
   > Amazon Inspector Classic에 대해 지원되는 운영 체제에 대한 자세한 내용은 Amazon Inspector Classic이 지원되는 운영 체제 및 리전 섹션을 참조하십시오.

2. EC2 인스턴스에서 [제어판], [프로그램 추가/제거]로 이동합니다.
3. 설치된 프로그램 목록에서 AWS 에이전트를 선택한 다음, 제거를 선택합니다.

(선택 사항) Linux 기반 운영 체제에서 Amazon Inspector Classic 에이전트 설치 스크립트의 서명을 확인합니다.

이 주제에서는 Linux 기반 운영 체제에서 Amazon Inspector Classic 에이전트 설치 스크립트의 유효성을 확인하는 권장 프로세스에 대해 설명합니다.

인터넷에서 애플리케이션을 다운로드할 때마다 소프트웨어 게시자의 자격 증명을 인증하고 애플리케이션이 게시된 이후 변경되거나 손상되지 않았는지 확인하는 것이 좋습니다. 이를 통해 바이러스나 기타 악성 코드가 포함된 애플리케이션 버전을 설치하는 것을 방지할 수 있습니다.

이 주제의 단계를 실행한 후에 Amazon Inspector Classic 에이전트의 소프트웨어가 변경 또는 손상된 것을 확인한 경우 설치 파일을 실행하지 마십시오. 대신, AWS Support에 문의하십시오.

Linux 기반 운영 체제용 Amazon Inspector Classic 에이전트 파일은 보안 디지털 서명을 위한 Pretty Good Privacy 표준의 오픈 소스 구현(OpenPGP)인 GnuPG를 사용하여 서명됩니다. GnuPG(GPG라고도 함)는 디지털 서명을 통해 인증 및 무결성 검사를 제공합니다. Amazon EC2는 다운로드한 Amazon EC2 CLI 도구를 확인하는 데 사용할 수 있는 퍼블릭 키 및 서명을 게시합니다. PGP 및 GnuPG(GPG)에 대한 자세한 내용은 http://www.gnupg.org를 참조하세요.

첫 번째 단계는 소프트웨어 게시자와 신뢰를 구축하는 것입니다. 소프트웨어 게시자의 퍼블릭 키를 다운로드하고, 퍼블릭 키의 소유자가 정당한 소유자인지 확인한 다음, 퍼블릭 키를 키링에 추가합니다. 키링은 알려진 퍼블릭 키의 모음입니다. 퍼블릭 키의 신뢰성을 설정한 후, 이를 사용하여 애플리케이션의 서명을 확인할 수 있습니다.

주제

- GPG 도구 설치
- 퍼블릭 키 인증 및 가져오기
- 패키지의 서명 확인

GPG 도구 설치

Linux 또는 Unix 운영 체제를 사용하는 경우 일반적으로 GPG 도구가 이미 설치되어 있습니다. 시스템에 도구가 설치되어 있는지 테스트하려면 명령 프롬프트에 gpg(을)를 입력합니다. GPG 도구가 설치되어 있는 경우, GPG 명령 프롬프트가 표시됩니다. GPG 도구가 설치되어 있지 않은 경우 명령을 찾을 수 없다는 오류가 표시됩니다. 리포지토리에서 GnuPG 패키지를 설치할 수 있습니다.

Debian 기반 Linux에서 GPG 도구를 설치하려면

- 터미널에서 apt-get install gnupg 명령을 실행합니다.

Red Hat 기반 Linux에서 GPG 도구를 설치하려면

- 터미널에서 yum install gnupg 명령을 실행합니다.

퍼블릭 키 인증 및 가져오기

프로세스의 다음 단계는 Amazon Inspector Classic 퍼블릭 키를 인증하고 이를 신뢰할 수 있는 키로 GPG 인증 키에 추가하는 것입니다.

Amazon Inspector Classic 퍼블릭 키를 인증하고 가져오려면.

1. 다음 중 하나를 수행하여 퍼블릭 GPG 빌드 키 사본을 가져옵니다.
   - https://d1wk0tztpsntt1.cloudfront.net/linux/latest/inspector.gpg에서 다운로드합니다.
   - 다음 텍스트에서 키를 복사하여 `inspector.gpg`라는 파일에 붙여 넣습니다. 다음의 모든 항목을 포함해야 합니다.

```
-----BEGIN PGP PUBLIC KEY BLOCK-----
Version: GnuPG v2.0.18 (GNU/Linux)

mQINBFYDlfEBEADFpfNt/mdCtsmfDoga+PfHY9bdXAD68yhp2m9NyH3BOzle/MXI
8siNfoRgzDwuWnIaezHwwLWkDw2paRxp1NMQ9qRe8Phq0ewheLrQu95dwDgMcw90
gf9m1iKVHjdVQ9qNHlB2OFknPDxMDRHcrmlJYDKYCX3+MODEHnlK25tIH2KWezXP
FPSU+TkwjLRzSMYH1L8IwjFUIIi78jQS9a31R/cOl4zuC5fOVghYlSomLI8irfoD
JSa3csVRujSmOAf9o3beiMR/kNDMpgDOxgiQTu/Kh39cl6o8AKe+QKK48kqO7hra
h1dpzLbfeZEVU6dWMZtlUksG/zKxuzD6d8vXYH7Z+x09POPFALQCQQMC3WisIKgj
zJEFhXMCCQ3NLC3CeyMq3vP7MbVRBYE7t3d2uDREkZBgIf+mbUYfYPhrzy0qT9Tr
PgwcnUvDZuazxuuPzucZGOJ5kbptat3DcUpstjdkMGAId3JawBbps77qRZdA+swr
o9o3jbowgmf0y5ZS6KwvZnC6XyTAkXy2io7mSrAIRECrANrzYzfp5v7uD7w8Dk0X
1OrfOm1VufMzAyTu0YQGBWaQKzSB8tCkvFw54PrRuUTcV826XU7SIJNzmNQo58uL
bKyLVBSCVabfs0lkECIesq8PT9xMYfQJ421uATHyYUnFTU2TYrCQEab7oQARAQAB
tCdBbWF6b24gSW5zcGVjdG9yIDxpbnNwZWN0b3JAYW1hem9uLmNvbT6JAjgEEwEC
ACIFAlYDlfECGwMGCwkIBwMCBhUIAgkKCwQWAgMBAh4BAheAAAoJECR0CWBYNgQY
8yUP/2GpIl40f3mKBUiSTe0XQLvwiBCHmY+V9fOuKqDTinxssjEMCnz0vsKeCZF/
L35pwNa/oW0OJa8D7sCkKG+8LuyMpcPDyqptLrYPprUWtz2+qLCHgpWsrku7ateF
x4hWS0jUVeHPaBzI9V1NTHsCx9+nbpWQ5Fk+7VJI8hbMDY7NQx6fcse8WTlP/0r/
HIkKzzqQQaaOf5t9zc5DKwi+dFmJbRUyaq22xs8C81UODjHunhjHdZ21cnsgk91S
fviuaum9aR4/uVIYOTVWnjC5J3+VlczyUt5FaYrrQ5ov0dM+biTUXwve3X8Q85Nu
DPnO/+zxb7Jz3QCHXnuTbxZTjvvl60Oi8//uRTnPXjz4wZLwQfibgHmk1++hzND7
wOYA02Js6v5FZQlLQAod7q2wuA1pq4MroLXzziDfy/9ea8B+tzyxlmNVRpVZY4Ll
DOHyqGQhpkyV3drjjNZlEofwbfu7m6ODwsgMl5ynzhKklJzwPJFfB3mMc7qLi+qX
MJtEX8KJ/iVUQStHHAG7daL1bxpWSI3BRuaHsWbBGQ/mcHBgUUOQJyEp5LAdg9Fs
VP55gWtF7pIqifiqlcfgG0Ov+A3NmVbmiGKSZvfrc5KsF/k43rCGqDx1RV6gZvyI
LfO9+3sEIlNrsMib0KRLDeBt3EuDsaBZgOkqjDhgJUesqiCy
=iEhB
-----END PGP PUBLIC KEY BLOCK-----
```

2. inspector.gpg를 저장한 디렉터리의 명령 프롬프트에서 다음 명령을 사용하여 Amazon Inspector Classic 퍼블릭 키를 인증 키로 가져옵니다.

```
gpg --import inspector.gpg
```

이 명령은 다음과 같은 결과를 반환합니다.

```
gpg: key 58360418: public key "Amazon Inspector <inspector@amazon.com>" imported
                    gpg: Total number processed: 1
                    gpg:               imported: 1  (RSA: 1)
```

다음 단계에서 필요하므로 키 값을 적어 둡니다. 이전 예제에서 키 값은 58360418입니다.

3. 키-값을 이전 단계의 값으로 대체하고 다음 명령을 실행하여 지문을 확인합니다.

```
gpg --fingerprint key-value
```

이 명령에서 다음과 비슷한 결과를 반환합니다.

```
pub   4096R/58360418 2015-09-24
                Key fingerprint = DDA0 D4C5 10AE 3C20 6F46  6DC0 2474 0960 5836
 0418
                uid                  Amazon Inspector <inspector@amazon.com>
```

또한 지문 문자열은 이전 예제에 표시된 `DDA0 D4C5 10AE 3C20 6F46 6DC0 2474 0960 5836 0418`(와)과 동일해야 합니다. 반환된 키 지문을 이 페이지에 게시된 지문과 비교합니다. 두 지문이 일치해야 합니다. 일치하지 않을 경우 Amazon Inspector Classic 에이전트 설치 스크립트를 설치하지 말고 AWS Support에 문의하십시오.

패키지의 서명 확인

GPG 도구를 설치하고, Amazon Inspector Classic 퍼블릭 키를 인증 및 가져오고, 퍼블릭 키가 신뢰할 수 있는지 확인하면 설치 스크립트의 서명을 확인할 준비가 된 것입니다.

설치 스크립트 서명을 확인하려면

1. 명령 프롬프트에서 다음 명령을 실행하여 설치 스크립트용 서명 파일을 다운로드합니다.

```
curl -O https://inspector-agent.amazonaws.com/linux/latest/install.sig
```

2. `install.sig` 및 Amazon Inspector Classic 설치 파일을 저장한 디렉터리의 명령 프롬프트에서 다음 명령을 실행하여 서명을 확인합니다. 두 파일이 모두 있어야 합니다.

```
gpg --verify ./install.sig
```

출력은 다음과 같아야 합니다.

```
gpg: Signature made Thu 24 Sep 2015 03:19:09 PM UTC using RSA key ID 58360418
gpg: Good signature from "Amazon Inspector <inspector@amazon.com>" [unknown]
gpg: WARNING: This key is not certified with a trusted signature!
```

```
gpg:          There is no indication that the signature belongs to the owner.
Primary key fingerprint: DDA0 D4C5 10AE 3C20 6F46  6DC0 2474 0960 5836 0418
```

출력에 `Good signature from "Amazon Inspector <inspector@amazon.com>"` 문구가 포함된 경우 서명을 확인했고 Amazon Inspector Classic 설치 스크립트 실행을 계속할 수 있음을 의미합니다.

출력에 `BAD signature` 문구가 포함된 경우, 절차를 올바르게 수행했는지 확인합니다. 계속해서 이 응답을 받게 되면 이전에 다운로드한 설치 파일을 실행하지 말고 AWS Support에 문의하십시오.

다음은 표시될 수 있는 경고에 대한 세부 정보입니다.

- 경고: 이 키는 신뢰할 수 있는 서명으로 인증되지 않았습니다. 서명이 소유자에게 속한다는 표시가 없습니다. 이는 사용자가 Amazon Inspector Classic에 대한 신뢰할 수 있는 퍼블릭 키를 소유하고 있다는 개인적인 신뢰 수준을 가리킬 뿐입니다. AWS 사무실을 방문하여 직접 키를 받는 것이 이상적입니다. 그러나 대부분의 경우 웹 사이트에서 다운로드합니다. 이 경우 웹 사이트는 AWS 웹 사이트입니다.
- gpg: 궁극적으로 신뢰할 수 있는 키를 찾을 수 없습니다. 이는 사용자(또는 사용자가 신뢰하는 다른 사용자)가 특정 키를 "궁극적으로 신뢰"하지 않음을 뜻합니다.

자세한 내용은 http://www.gnupg.org를 참조하세요.

(선택 사항) Windows 기반 운영 체제에서 Amazon Inspector Classic 에이전트 설치 스크립트의 서명을 확인합니다.

이 주제에서는 Windows 기반 운영 체제에서 Amazon Inspector Classic 에이전트 설치 스크립트의 유효성을 확인하는 권장 프로세스에 대해 설명합니다.

인터넷에서 애플리케이션을 다운로드할 때마다 소프트웨어 게시자의 자격 증명을 인증하고 애플리케이션이 게시된 이후 변경되거나 손상되지 않았는지 확인하는 것이 좋습니다. 이를 통해 바이러스나 기타 악성 코드가 포함된 애플리케이션 버전을 설치하는 것을 방지할 수 있습니다.

이 주제의 단계를 실행한 후에 Amazon Inspector Classic 에이전트의 소프트웨어가 변경 또는 손상된 것을 확인한 경우 설치 파일을 실행하지 마십시오. 대신, AWS Support에 문의하십시오.

Windows 기반 운영 체제에서 다운로드된 에이전트 설치 스크립트의 유효성을 확인하려면 Amazon Services LLC 서명자 인증서의 지문이 다음 값과 동일한지 확인해야 합니다.

E8 83 C5 3A F7 8C BA 7C F5 A2 47 E9 B8 86 FC E9 68 EE 0B 36

이 값을 확인하려면 다음 절차를 수행합니다.

1. 다운로드한 `AWSAgentInstall.exe`(을)를 마우스 오른쪽 버튼으로 클릭하고 속성(Properties) 창을 엽니다.
2. 디지털 서명(Digital Signatures) 탭을 선택합니다.
3. 서명 목록에서 Amazon Services Web Services, Inc.를 선택한 후 세부 정보를 선택합니다.
4. 일반 탭이 선택되어 있지 않으면 이 탭을 선택한 후 인증서 보기(View Certificate)를 선택합니다.
5. 세부 정보 탭을 선택한 다음, 선택되어 있지 않은 경우 표시 드롭다운 목록에서 모두(All)를 선택합니다.
6. 지문(Thumbprint) 필드가 보일 때까지 아래로 스크롤한 후 지문(Thumbprint)을 선택합니다. 그러면 아래 창에 전체 지문 값이 표시됩니다.

   - 아래 창의 지문 값이 다음과 값과 동일한지 확인합니다.

     E8 83 C5 3A F7 8C BA 7C F5 A2 47 E9 B8 86 FC E9 68 EE 0B 36

     동일하다면, 다운로드한 에이전트 설치 스크립트가 정품이므로 안전하게 설치할 수 있습니다.
   - 아래 세부 정보 창의 지문 값이 위의 값과 동일하지 않을 경우 `AWSAgentInstall.exe`를 실행하지 마십시오.

Amazon Inspector Classic 평가 대상

Amazon Inspector Classic을 사용하여 AWS 평가 대상(AWS 리소스 모음)에 해결해야 할 잠재적 보안 문제가 있는지 평가할 수 있습니다.

> **Important**
>
> 현재 평가 대상은 지원되는 운영 체제에서 실행되는 EC2 인스턴스로만 구성될 수 있습니다. 지원되는 운영 체제 및 지원되는 AWS 리전에 대한 자세한 내용은 the section called "지원 운영 체제 및 리전" 섹션을 참조하십시오.

> **Note**
>
> EC2 인스턴스 시작에 대한 내용은 Amazon Elastic Compute Cloud 설명서를 참조하십시오.

주제

- 평가 대상을 생성하도록 리소스에 태그 지정
- Amazon Inspector Classic 평가 대상 제한
- 평가 대상 생성
- 평가 대상 삭제

평가 대상을 생성하도록 리소스에 태그 지정

평가할 Amazon Inspector Classic에 대한 평가 대상을 생성하려면 대상에 포함할 EC2 인스턴스에 태그를 지정하여 시작합니다. 태그는 인스턴스 및 기타 AWS 리소스를 식별하고 구성하기 위한 메타데이터 역할을 하는 단어 또는 구문입니다. Amazon Inspector Classic은 생성한 태그를 사용하여 대상에 속한 인스턴스를 식별합니다.

모든 AWS 태그는 선택한 키와 값 페어로 구성됩니다. 예를 들어, 키 "Name" 및 값 "MyFirstInstance"의 이름을 지정할 수 있습니다. 인스턴스에 태그를 지정한 후 Amazon Inspector Classic 콘솔을 사용하여 평가 대상에 인스턴스를 추가합니다. 인스턴스가 두 개 이상의 태그 키-값 페어와 일치할 필요는 없습니다.

EC2 인스턴스에 태그를 지정하여 평가 대상을 빌드할 때 사용자 지정 태그 키를 생성하거나 동일한 AWS 계정의 다른 사용자가 생성한 태그 키를 사용할 수 있습니다. 에서 AWS 자동으로 생성하는 태그 키를 사용할 수도 있습니다. 예를 들어는 시작하는 EC2 인스턴스에 대한 이름 태그 키를 AWS 자동으로 생성합니다.

태그를 만들 때 EC2 인스턴스에 태그를 추가하거나 각 EC2 인스턴스의 콘솔 페이지에서 태그를 한 번에 하나씩 추가, 변경 또는 제거할 수 있습니다. 태그 편집기를 사용하여 한 번에 여러 EC2 인스턴스에 태그를 추가할 수도 있습니다.

자세한 내용은 태그 편집기를 참조하십시오. EC2 인스턴스의 태그 지정에 대한 자세한 내용은 리소스 및 태그를 참조하십시오.

Amazon Inspector Classic 평가 대상 제한

AWS 계정당 최대 50개의 평가 대상을 생성할 수 있습니다. 자세한 내용은 Amazon Inspector Classic 서비스 한도 단원을 참조하십시오.

평가 대상 생성

Amazon Inspector Classic 콘솔을 사용하여 평가 대상을 생성할 수 있습니다.

평가 대상 생성

1. 에 로그인 AWS Management Console 하고 https://console.aws.amazon.com/inspector/ Amazon Inspector Classic 콘솔을 엽니다.
2. 탐색 창에서 [Assessment Targets]를 선택한 후 [Create]를 선택합니다.
3. 이름에 평가 대상의 이름을 입력합니다.
4. 다음 중 하나를 수행합니다.

   - 이 AWS 계정 및 리전의 모든 EC2 인스턴스를이 평가 대상에 포함하려면 모든 인스턴스 확인란을 선택합니다.

     > **Note**
     >
     > 평가 실행에 포함할 수 있는 최대 에이전트 수에 대한 제한은 이 옵션을 사용할 때 적용됩니다. 자세한 내용은 Amazon Inspector Classic 서비스 한도 단원을 참조하십시오.

   - 이 평가 대상에 포함할 EC2 인스턴스를 선택하려면 태그 사용에 태그 키 이름과 키-값 페어를 입력합니다.

5. (선택 사항) 대상을 생성할 때 에이전트 설치 확인란을 선택하여 이 대상의 모든 EC2 인스턴스에 에이전트를 설치할 수 있습니다. 이 옵션을 사용하려면 EC2 인스턴스에 SSM 에이전트가 설치되어 있고, 명령 실행을 허용하는 IAM 역할이 지정되어 있어야 합니다. SSM 에이전트는 Amazon EC2 Windows 인스턴스와 Amazon Linux 인스턴스에 기본적으로 설치됩니다. Amazon EC2 Systems Manager에는 명령을 처리하는 EC2 인스턴스를 위한 IAM 역할과 명령을 실행하는 사용자를 위한 별도의 역할이 필요합니다. 자세한 내용은 Installing and Configuring SSM Agent 및 Configuring Security Roles for System Manager 섹션을 참조하십시오.

> **Important**
>
> 이미 에이전트를 실행 중인 EC2 인스턴스가 있는 경우, 이 옵션을 사용하면 현재 그 인스턴스에서 실행 중인 에이전트가 최신 에이전트 버전으로 대체됩니다.

> **Note**
>
> 기존의 평가 대상에 대해 명령 실행을 사용하여 에이전트 설치 버튼을 선택하여 이 대상의 모든 EC2 인스턴스에 에이전트를 설치할 수 있습니다.

> **Note**
>
> Systems Manager 명령 실행을 사용하여 여러 EC2 인스턴스에 원격으로 에이전트를 설치할 수도 있습니다(Linux 기반 인스턴스 및 Windows 기반 인스턴스 모두 동일한 명령으로 가능). 자세한 내용은 Systems Manager Run Command를 사용하여 여러 EC2 인스턴스에 Amazon Inspector 에이전트를 설치하려면을 참조하십시오.

6. 저장(Save)을 선택합니다.

> **Note**
>
> 평가 대상 페이지의 대상 미리 보기 버튼을 사용하여 평가 대상에 포함된 모든 EC2 인스턴스를 검토할 수 있습니다. 각 EC2 에이전트에 대해 호스트 이름, 인스턴스 ID, IP 주소 및 해당되는 경우 에이전트의 상태를 검토할 수 있습니다. 에이전트 상태는 정상, 비정상, 알 수 없음의 값을 가질 수 있습니다. Amazon Inspector Classic은 EC2 인스턴스에서 실행 중인 에이전트가 있는지 여부를 확인할 수 없는 경우 상태를 알 수 없음으로 표시합니다.

평가 대상 삭제

평가 대상을 삭제하려면 다음 절차를 수행하십시오.

평가 대상 삭제

- 평가 대상 페이지에서 삭제할 대상을 선택한 후 삭제를 선택합니다. 확인 메시지가 표시되면 예를 선택합니다.

> **Important**
>
> 평가 대상을 삭제하면 해당 대상과 연결된 모든 평가 템플릿, 평가 실행, 결과 및 모든 버전의 보고서가 삭제됩니다.

`DeleteAssessmentTarget` API를 사용하여 평가 대상을 삭제할 수도 있습니다.

Amazon Inspector Classic 규칙 패키지 및 규칙

Amazon Inspector Classic을 사용하여 평가 대상(AWS 리소스 모음)의 잠재적인 보안 문제 및 취약성을 평가할 수 있습니다. Amazon Inspector Classic은 평가 대상의 동작 및 보안 구성을 선택된 보안 규칙 패키지에 비교합니다. Amazon Inspector Classic의 컨텍스트에서 규칙은 평가 실행 중에 Amazon Inspector Classic이 수행하는 보안 검사입니다.

Amazon Inspector Classic에서 규칙은 범주, 심각도 또는 요금별로 고유한 규칙 패키지로 함께 그룹화됩니다. 이렇게 하면 다양한 종류의 분석을 수행할 수 있습니다. 예를 들어, Amazon Inspector Classic은 애플리케이션을 평가하는 데 사용할 수 있는 많은 수의 규칙을 제공합니다. 그러나 특정 영역의 문제를 대상으로 하거나 특정한 보안 문제를 발견하기 위해 더 작은 하위 세트의 사용 가능한 규칙을 포함하고자 할 수도 있습니다. 대규모 IT 부서가 있는 회사는 이 애플리케이션이 보안 위협에 노출되는지 확인하고자 합니다. 반면, 심각도 수준이 높음인 문제에만 집중하고자 하는 회사도 있습니다.

- Amazon Inspector Classic의 규칙 심각도 수준
- Amazon Inspector Classic 내의 규칙 패키지

Amazon Inspector Classic의 규칙 심각도 수준

각 Amazon Inspector Classic 규칙에는 심각도 수준이 할당되어 있습니다. 이 경우 분석에서 규칙의 우선순위를 지정할 필요가 줄어듭니다. 또한 규칙이 잠재적인 문제를 강조 표시할 때 응답을 결정하는 데 도움이 될 수도 있습니다.

High, Medium, Low 수준은 모두 평가 대상 내 정보 기밀, 무결성 및 가용성이 손상될 수 있는 보안 문제를 나타냅니다. 수준은 문제로 인해 손상이 발생할 가능성과 문제 해결이 시급한 정도에 따라 구분됩니다.

Informational 수준은 단순히 평가 대상의 보안 구성 세부 정보를 강조 표시합니다.

심각도에 따라 문제를 해결하는 데 권장되는 대응 방법은 다음과 같습니다.

- 높음 – 심각도가 높음인 문제는 매우 시급한 문제입니다. Amazon Inspector Classic은 이 보안 문제를 긴급으로 처리하고 즉각적으로 해결하는 것을 권장합니다.
- 중간 – 심각도가 중간인 문제는 다소 시급한 문제입니다. Amazon Inspector Classic은 가능한 다음 기회(예: 다음 서비스 업데이트)에 이 문제를 해결하는 것을 권장합니다.
- 낮음 – 심각도가 낮음인 문제는 덜 시급한 문제입니다. Amazon Inspector Classic은 이후 서비스 업데이트 시 이 문제를 해결하는 것을 권장합니다.

- 정보성 – 이 문제는 순전히 정보용입니다. 비즈니스 및 조직 목표에 따라 이 정보를 기록해 두거나 이 정보를 사용하여 평가 대상의 보안을 강화할 수 있습니다.

Amazon Inspector Classic 내의 규칙 패키지

Amazon Inspector 평가에서는 다음 규칙 패키지의 모든 조합을 사용할 수 있습니다.

네트워크 평가:

- 네트워크 연결성

호스트 평가:

- CVE(일반적인 취약성 및 노출도)
- Center for Internet Security(CIS) 벤치마크
- Amazon Inspector Classic의 보안 모범 사례

네트워크 연결성

네트워크 연결성 패키지의 규칙은 네트워크 구성을 분석하여 EC2 인스턴스의 보안 취약성을 찾습니다. Amazon Inspector가 생성하는 결과는 안전하지 않은 액세스 제한에 대한 지침도 제공합니다.

Network Reachability 규칙 패키지는 AWS Provable Security 이니셔티브의 최신 기술을 사용합니다.

이 규칙에 의해 생성된 결과는 포트가 인터넷 게이트웨이(Application Load Balancer 또는 Classic Load Balancer 뒤에 있는 인스턴스 포함), VPC 피어링 연결 또는 가상 게이트웨이를 통한 VPN을 통해 인터넷에서 연결될 수 있는지 여부를 나타냅니다. 또한 이러한 결과는 잘못 관리되는 보안 그룹, ACL, IGW 등과 같이 악의적인 액세스를 허용하는 네트워크 구성을 강조합니다.

이러한 규칙은 AWS 네트워크의 모니터링을 자동화하고 EC2 인스턴스에 대한 네트워크 액세스가 잘못 구성되었을 수 있음을 식별하는 데 도움이 됩니다. 이 패키지를 평가 실행에 포함하면 특히 VPC 피어링 연결 및 VPN에서 유지하기 복잡하고 비용이 많이 드는 스캐너를 설치하거나 패킷을 보내지 않고도 자세한 네트워크 보안 검사를 구현할 수 있습니다.

> **Important**
>
> Amazon Inspector Classic 에이전트는 이 규칙 패키지를 통해 EC2 인스턴스를 평가하는 데 필요하지 않습니다. 하지만 설치된 에이전트는 포트에서 수신하는 프로세스의 존재 여부에 대한

정보를 제공할 수 있습니다. Amazon Inspector Classic에서 지원하지 않는 운영 체제에는 에이전트를 설치하지 마십시오. 지원되지 않는 운영 체제를 실행하는 인스턴스에 에이전트가 있는 경우 네트워크 연결 가능성 규칙 패키지가 해당 인스턴스에서 작동하지 않습니다.

자세한 내용은 지원되는 운영 체제의 Amazon Inspector Classic 규칙 패키지 단원을 참조하십시오.

분석된 구성

네트워크 연결성 규칙은 취약성에 대한 다음 엔터티의 구성을 분석합니다.

- Amazon EC2 인스턴스
- Application Load Balancers
- Direct Connect
- Elastic Load Balancer
- 탄력적 네트워크 인터페이스
- 인터넷 게이트웨이(IGW)
- 네트워크 액세스 제어 목록(ACL)
- 라우팅 테이블
- 보안 그룹(SG)
- 서브넷
- Virtual Private Cloud(VPC)
- 가상 프라이빗 게이트웨이(VGW)
- VPC 피어링 연결

연결성 라우팅

네트워크 연결성 규칙은 VPC 외부에서 포트에 액세스할 수 있는 방법에 해당하는 다음 연결성 라우팅을 확인합니다.

- **`Internet`** - 인터넷 게이트웨이(Application Load Balancer 및 Classic Load Balancer 포함)
- **`PeeredVPC`** - VPC 피어링 연결
- **`VGW`** - 가상 프라이빗 게이트웨이

결과 유형

네트워크 연결성 규칙 패키지가 포함된 평가는 각 연결성 라우팅에 대해 다음 유형의 결과를 반환할 수 있습니다.

- RecognizedPort
- UnrecognizedPortWithListener
- NetworkExposure

RecognizedPort

잘 알려진 서비스에 일반적으로 사용되는 포트에 연결 가능합니다. 대상 EC2 인스턴스에 에이전트가 있는 경우 생성된 검색 결과는 포트에 활성 수신 프로세스가 있는지 여부도 나타냅니다. 이러한 결과 유형은 잘 알려진 서비스의 보안 영향에 따라 심각도가 지정됩니다.

- **RecognizedPortWithListener** – 인식된 포트는 특정 네트워킹 구성 요소를 통해 퍼블릭 인터넷에서 외부로 연결할 수 있으며 프로세스는 포트에서 수신 대기합니다.
- **RecognizedPortNoListener** – 인식된 포트는 특정 네트워킹 구성 요소를 통해 퍼블릭 인터넷에서 외부로 연결할 수 있으며 포트에 대해 수신하는 프로세스가 없습니다.
- **RecognizedPortNoAgent** – 인식된 포트는 특정 네트워킹 구성 요소를 통해 퍼블릭 인터넷에서 외부로 연결할 수 있습니다. 대상 인스턴스에 에이전트를 설치하지 않은 상태에서는 포트에서 수신하는 프로세스가 있는지 여부를 확인할 수 없습니다.

다음 표는 인식된 포트 목록을 보여 줍니다.

Service	TCP 포트	UDP 포트
SMB	445	445
NetBIOS	137, 139	137, 138
LDAP	389	389
LDAP over TLS	636	
글로벌 카탈로그 LDAP	3268	

Service	TCP 포트	UDP 포트
글로벌 카탈로그 LDAP over TLS	3269	
NFS	111, 2049, 4045, 1110	111, 2049, 4045, 1110
Kerberos	88, 464, 543, 544, 749, 751	88, 464, 749, 750, 751, 752
RPC	111, 135, 530	111, 135, 530
WINS	1512, 42	1512, 42
DHCP	67, 68, 546, 547	67, 68, 546, 547
Syslog	601	514
인쇄 서비스	515	
Telnet	23	23
FTP	21	21
SSH	22	22
RDP	3389	3389
MongoDB	27017, 27018, 27019, 28017	
SQL 서버	1433	1434
MySQL	3306	
PostgreSQL	5432	
Oracle	1521, 1630	
Elasticsearch	9300, 9200	
HTTP	80	80

Service	TCP 포트	UDP 포트
HTTPS	443	443

`UnrecogizedPortWithListener`

앞의 표에 나열되지 않은 포트는 연결 가능하며 활성 수신 프로세스가 있습니다. 이 유형의 결과는 수신 프로세스에 대한 정보를 표시하므로 Amazon Inspector 에이전트가 대상 EC2 인스턴스에 설치된 경우에만 생성될 수 있습니다. 이 유형의 결과에는 낮음 심각도가 부여됩니다.

`NetworkExposure`

이 유형의 결과는 EC2 인스턴스에서 연결할 수 있는 포트에 대한 집계 정보를 표시합니다. 이러한 결과는 탄력적 네트워크 인터페이스와 EC2 인스턴스의 보안 그룹을 조합할 때 TCP 및 UDP 포트 범위의 연결 가능한 집합을 보여 줍니다. 이 유형의 결과는 정보 심각도를 갖습니다.

CVE(일반적인 취약성 및 노출도)

이 패키지의 규칙을 통해 평가 대상의 EC2 인스턴스가 CVE(일반적인 취약성 및 노출도)에 노출되는지 여부를 확인할 수 있습니다. 공격은 패칭되지 않은 취약성을 악용하여 서비스 또는 데이터의 기밀성, 무결성 또는 가용성을 손상시킬 수 있습니다. CVE 시스템은 공개적으로 알려진 정보 보안 취약성 및 노출도에 대한 참조 방법을 제공합니다. 자세한 내용은 https://cve.mitre.org/를 참조하십시오.

Amazon Inspector Classic 평가에서 생성한 결과에 특정 CVE가 표시될 경우 https://cve.mitre.org/에서 CVE의 ID를 검색할 수 있습니다(예: **`CVE-2009-0021`**). 검색 결과에서 이 CVE, 해당 심각도 및 완화 방법에 대한 상세 정보를 제공할 수 있습니다.

일반적인 취약성 및 악용(CVE) 규칙 패키지에 대해 Amazon Inspector는 다음과 같이 제공된 CVSS 기본 점수 및 ALAS 심각도 수준을 매핑했습니다.

Amazon Inspector 심각도	CVSS 기본 점수	ALAS 심각도 (CVSS가 점수를 매기지 않은 경우)
High	>= 5	Critical or Important
Medium	< 5 and >= 2.1	Medium
Low	< 2.1 and >= 0.8	Low

Informational	< 0.8	N/A

이 패키지에 포함된 규칙은 EC2 인스턴스가 다음의 리전 목록에서 CVE에 노출되는지 여부를 평가하는 데 도움이 됩니다.

- 미국 동부(버지니아 북부)
- 미국 동부(오하이오)
- 미국 서부(캘리포니아 북부)
- 미국 서부(오리건)
- EU(아일랜드)
- EU(프랑크푸르트)
- EU(런던)
- EU(스톡홀름)
- 아시아 태평양(도쿄)
- 아시아 태평양(서울)
- 아시아 태평양(뭄바이)
- 아시아 태평양(시드니)
- AWS GovCloud 서부(미국)
- AWS GovCloud 동부(미국)

CVE 규칙 패키지는 정기적으로 업데이트됩니다. 이 목록을 검색하는 시점에 동시에 발생하는 평가 실행에 포함된 CVE가 이 목록에 포함됩니다.

자세한 내용은 지원되는 운영 체제의 Amazon Inspector Classic 규칙 패키지 단원을 참조하십시오.

Center for Internet Security(CIS) 벤치마크

CIS Security Benchmarks 프로그램은 조직이 보안을 평가하고 개선하는 데 도움이 되는 잘 정의되고 편향되지 않은 합의 기반 업계 모범 사례를 제공합니다. AWS 는 CIS Security Benchmarks 멤버 회사입니다. Amazon Inspector Classic 인증 목록을 보려면 CIS 웹 사이트의 Amazon Web Services 페이지를 참조하십시오.

Amazon Inspector Classic은 현재 다음 운영 체제에 대한 보안 구성 태세를 설정하는 데 도움이 되는 다음 CIS 인증 규칙 패키지를 제공합니다.

Amazon Linux

- CIS Benchmark for Amazon Linux 2 Benchmark v1.0.0 Level 1
- CIS Benchmark for Amazon Linux 2 Benchmark v1.0.0 Level 2
- CIS Benchmark for Amazon Linux Benchmark v2.1.0 Level 1
- CIS Benchmark for Amazon Linux Benchmark v2.1.0 Level 2
- CIS Benchmark for Amazon Linux 2014.09-2015.03 v1.1.0 Level 1

CentOS Linux

- CIS Benchmark for CentOS Linux 7 Benchmark v2.2.0 Level 1 Server
- CIS Benchmark for CentOS Linux 7 Benchmark v2.2.0 Level 2 Server
- CIS Benchmark for CentOS Linux 7 Benchmark v2.2.0 Level 1 Workstation
- CIS Benchmark for CentOS Linux 7 Benchmark v2.2.0 Level 2 Workstation
- CIS Benchmark for CentOS Linux 6 Benchmark v2.0.2 Level 1 Server
- CIS Benchmark for CentOS Linux 6 Benchmark v2.0.2 Level 2 Server
- CIS Benchmark for CentOS Linux 6 Benchmark v2.0.2 Level 1 Workstation
- CIS Benchmark for CentOS Linux 6 Benchmark v2.0.2 Level 2 Workstation

Red Hat Enterprise Linux

- CIS Benchmark for Red Hat Enterprise Linux 7 Benchmark v2.1.1 Level 1 Server
- CIS Benchmark for Red Hat Enterprise Linux 7 Benchmark v2.1.1 Level 2 Server
- CIS Benchmark for Red Hat Enterprise Linux 7 Benchmark v2.1.1 Level 1 Workstation
- CIS Benchmark for Red Hat Enterprise Linux 7 Benchmark v2.1.1 Level 2 Workstation
- CIS Benchmark for Red Hat Enterprise Linux 6 Benchmark v2.0.2 Level 1 Server
- CIS Benchmark for Red Hat Enterprise Linux 6 Benchmark v2.0.2 Level 2 Server

- CIS Benchmark for Red Hat Enterprise Linux 6 Benchmark v2.0.2. Level 1 Workstation
- CIS Benchmark for Red Hat Enterprise Linux 6 Benchmark v2.0.2 Level 2 Workstation

Ubuntu

- CIS Benchmark for Ubuntu Linux 18.04 LTS Benchmark v1.0.0 Level 1 Server
- CIS Benchmark for Ubuntu Linux 18.04 LTS Benchmark v1.0.0 Level 2 Server
- CIS Benchmark for Ubuntu Linux 18.04 LTS Benchmark v1.0.0 Level 1 Workstation
- CIS Benchmark for Ubuntu Linux 18.04 LTS Benchmark v1.0.0 Level 2 Workstation
- CIS Benchmark for Ubuntu Linux 16.04 LTS Benchmark v1.1.0 Level 1 Server
- CIS Benchmark for Ubuntu Linux 16.04 LTS Benchmark v1.1.0 Level 2 Server
- CIS Benchmark for Ubuntu Linux 16.04 LTS Benchmark v1.1.0 Level 1 Workstation
- CIS Benchmark for Ubuntu Linux 16.04 LTS Benchmark v1.1.0 Level 2 Workstation
- CIS Benchmark for Ubuntu Linux 14.04 LTS Benchmark v2.0.0 Level 1 Server
- CIS Benchmark for Ubuntu Linux 14.04 LTS Benchmark v2.0.0 Level 2 Server
- CIS Benchmark for Ubuntu Linux 14.04 LTS Benchmark v2.0.0 Level 1 Workstation
- CIS Benchmark for Ubuntu Linux 14.04 LTS Benchmark v2.0.0 Level 2 Workstation

Windows

- Windows Server 2016 (CIS Benchmark for Microsoft Windows 2016 RTM (Release 1607), v1.1.0, Level 1 Member Server Profile)
- Windows Server 2016 (CIS Benchmark for Microsoft Windows 2016 RTM (Release 1607), v1.1.0, Level 2 Member Server Profile)

- Windows Server 2016 (CIS Benchmark for Microsoft Windows 2016 RTM (Release 1607), v1.1.0, Level 1 Domain Controller Profile)
- Windows Server 2016 (CIS Benchmark for Microsoft Windows 2016 RTM (Release 1607), v1.1.0, Level 2 Domain Controller Profile)
- Windows Server 2016 (CIS Benchmark for Microsoft Windows 2016 RTM (Release 1607), v1.1.0, Next Generation Windows Security Profile)
- Windows Server 2012 R2 (CIS Benchmark for Microsoft Windows 2012 R2, v2.2.0, Level 1 Domain Controller Profile)
- Windows Server 2012 R2 (CIS Benchmark for Microsoft Windows 2012 R2, v2.2.0, Level 2 Domain Controller Profile)
- Windows Server 2012 R2 (CIS Benchmark for Microsoft Windows 2012 R2, v2.2.0, Level 1 Member Server Profile)
- Windows Server 2012 R2 (CIS Benchmark for Microsoft Windows 2012 R2, v2.2.0, Level 2 Member Server Profile)
- Windows Server 2012 (CIS Benchmark for Microsoft Windows 2012 non-R2, v2.0.0, Level 1 Member Server Profile)
- Windows Server 2012 (CIS Benchmark for Microsoft Windows 2012 non-R2, v2.0.0, Level 2 Member Server Profile)
- Windows Server 2012 (CIS Benchmark for Microsoft Windows 2012 non-R2, v2.0.0, Level 1 Domain Controller Profile)
- Windows Server 2012 (CIS Benchmark for Microsoft Windows 2012 non-R2, v2.0.0, Level 2 Domain Controller Profile)
- Windows Server 2008 R2 (CIS Benchmark for Microsoft Windows 2008 R2, v3.0.0, Level 1 Domain Controller Profile)
- Windows Server 2008 R2 (CIS Benchmark for Microsoft Windows 2008 R2, v3.0.0, Level 1 Member Server Profile)

Amazon Inspector Classic 평가 실행에서 생성한 결과에 특정 CIS 벤치마크가 표시될 경우 벤치마크에 대한 상세한 PDF 설명은 https://benchmarks.cisecurity.org/에서 다운로드할 수 있습니다(무료 등록 필요). 벤치마크 문서에 이 CIS 벤치마크, 해당 심각도 및 완화 방법에 대한 상세 정보가 나와 있습니다.

자세한 내용은 지원되는 운영 체제의 Amazon Inspector Classic 규칙 패키지 단원을 참조하십시오.

Amazon Inspector Classic의 보안 모범 사례

Amazon Inspector Classic 규칙을 사용하여 시스템이 안전하게 구성되어 있는지 확인할 수 있습니다.

> **Important**
>
> 현재 Linux 기반 또는 Windows 기반 운영 체제를 실행하는 EC2 인스턴스를 평가 대상에 포함시킬 수 있습니다.
> 평가를 실행하는 중에 이 섹션에서 설명하는 규칙은 Linux 기반 운영 체제를 실행하는 EC2 인스턴스에 대한 결과만 생성합니다. 이 규칙은 Windows 기반 운영 체제를 실행하는 EC2 인스턴스에 대한 결과는 생성하지 않습니다.
> 자세한 내용은 지원되는 운영 체제의 Amazon Inspector Classic 규칙 패키지 단원을 참조하십시오.

주제

- SSH를 통해 루트 로그인 비활성화
- SSH 버전 2만 지원
- SSH를 통한 암호 인증 비활성화
- 암호 최대 수명 구성
- 암호 최소 길이 구성
- 암호 복잡도 구성
- ASLR 활성화
- DEP 활성화
- 시스템 디렉터리에 대한 권한 구성

SSH를 통해 루트 로그인 비활성화

이 규칙을 통해 SSH 데몬이 EC2 인스턴스에 루트로 로그인하는 것을 허용하도록 구성되어 있는지 확인할 수 있습니다.

심각도

Medium

결과

사용자가 SSH를 통해 루트 자격 증명을 사용하여 로그인할 수 있도록 구성된 EC2 인스턴스가 평가 대상에 있습니다. 이 경우 Brute-Force 공격이 성공할 가능성이 높아집니다.

해결 방법

SSH를 통한 루트 계정 로그인을 방지하도록 EC2 인스턴스를 구성하는 것이 좋습니다. 대신 필요한 경우 루트 이외의 사용자로 로그인하고 `sudo`를 사용하여 권한을 에스컬레이션합니다. SSH 루트 계정 로그인을 비활성화하려면 `/etc/ssh/sshd_config` 파일에서 `PermitRootLogin`을 `no`로 설정하고 `sshd`를 다시 시작합니다.

SSH 버전 2만 지원

이 규칙을 통해 EC2 인스턴스가 SSH 프로토콜 버전 1을 지원하도록 구성되어 있는지 확인할 수 있습니다.

심각도

Medium

결과

평가 대상의 EC2 인스턴스가 SSH 1을 지원하도록 구성되어 있습니다. SSH 1에는 보안을 크게 저하시키는 설계 결함이 내재되어 있습니다.

해결 방법

SSH 2 이상만 지원하도록 평가 대상의 EC2 인스턴스를 구성하는 것이 좋습니다. OpenSSH의 경우 `Protocol 2`를 `/etc/ssh/sshd_config` 파일에서 설정하여 이를 수행할 수 있습니다. 자세한 내용은 `man sshd_config` 단원을 참조하십시오.

SSH를 통한 암호 인증 비활성화

이 규칙을 통해 EC2 인스턴스가 SSH 프로토콜을 통한 암호 인증을 지원하도록 구성되어 있는지 확인할 수 있습니다.

심각도

Medium

결과

평가 대상의 EC2 인스턴스가 SSH를 통한 암호 인증을 지원하도록 구성되어 있습니다. 암호 인증은 Brute-Force 공격에 취약하기 때문에 가능한 경우 키 기반 인증을 사용하기 위해 암호 인증을 비활성화해야 합니다.

해결 방법

EC2 인스턴스에서 SSH를 통한 암호 인증을 비활성화하고 대신 키 기반 인증 지원을 활성화하는 것이 좋습니다. 그러면 Brute-Force 공격의 성공 가능성을 크게 낮출 수 있습니다. 자세한 내용은 https://aws.amazon.com/articles/1233/을 참조하십시오. 암호 인증이 지원되는 경우 SSH 서버에 대한 액세스를 신뢰할 수 있는 IP 주소로 제한해야 합니다.

암호 최대 수명 구성

이 규칙을 통해 EC2 인스턴스에 암호의 최대 수명이 구성되어 있는지 확인할 수 있습니다.

심각도

Medium

결과

평가 대상의 EC2 인스턴스에 암호의 최대 수명이 구성되어 있지 않습니다.

해결 방법

암호를 사용하는 경우 평가 대상의 모든 EC2 인스턴스에 암호의 최대 수명을 구성하는 것이 좋습니다. 이를 위해 사용자는 암호를 정기적으로 변경해야 합니다. 그러면 암호 추측 공격이 성공할 가능성을 낮출 수 있습니다. 기존 사용자에 대해 이 문제를 해결하려면 chage 명령을 사용합니다. 모든 향후 사용자에 대한 암호의 최대 수명을 구성하려면 `/etc/login.defs` 파일의 `PASS_MAX_DAYS` 필드를 편집합니다.

암호 최소 길이 구성

이 규칙을 통해 EC2 인스턴스에 암호의 최소 길이가 구성되어 있는지 확인할 수 있습니다.

심각도

Medium

결과

평가 대상의 EC2 인스턴스에 암호의 최소 길이가 구성되어 있지 않습니다.

해결 방법

암호를 사용하는 경우 평가 대상의 모든 EC2 인스턴스에 암호의 최소 길이를 구성하는 것이 좋습니다. 최소 암호 길이를 적용하면 암호 추측 공격이 성공할 위험이 줄어듭니다. `pwquality.conf` 파일에서 `minlen` 옵션을 사용하여 이 작업을 수행할 수 있습니다. 자세한 내용은 https://linux.die.net/man/5/pwquality.conf를 참조하십시오.

인스턴스에서 `pwquality.conf`를 사용할 수 없는 경우 `minlen` 모듈을 사용하여 `pam_cracklib.so` 옵션을 설정할 수 있습니다. 자세한 내용은 `man pam_cracklib` 단원을 참조하십시오.

`minlen` 옵션은 14 이상으로 설정해야 합니다.

암호 복잡도 구성

이 규칙을 통해 EC2 인스턴스에 암호 복잡도 메커니즘이 구성되어 있는지 확인할 수 있습니다.

심각도

Medium

결과

평가 대상의 EC2 인스턴스에 암호 복잡도 메커니즘 또는 제한이 구성되어 있지 않습니다. 이 경우 사용자가 단순한 암호를 설정할 수 있고, 그렇게 되면 권한 없는 사용자가 액세스 권한을 얻어 계정을 오용할 가능성이 커집니다.

해결 방법

암호를 사용하는 경우 암호 복잡도 수준을 요구하도록 평가 대상의 모든 EC2 인스턴스를 구성하는 것이 좋습니다. `pwquality.conf` 파일에서 `lcredit`, `ucredit`, `dcredit`, `ocredit` 옵션을 사용하여 이 작업을 수행할 수 있습니다. 자세한 내용은 https://linux.die.net/man/5/pwquality.conf를 참조하십시오.

인스턴스에서 `pwquality.conf`를 사용할 수 없는 경우 `lcredit` 모듈을 사용하여 `ucredit`, `dcredit`, `ocredit` 및 `pam_cracklib.so` 옵션을 설정할 수 있습니다. 자세한 내용은 `man pam_cracklib` 단원을 참조하십시오.

이러한 각 옵션에 대한 예상 값은 아래와 같이 -1보다 작거나 같습니다.

```
lcredit <= -1, ucredit <= -1, dcredit<= -1, ocredit <= -1
```

또한 이 `remember` 옵션을 12 이상으로 설정해야 합니다. 자세한 내용은 `man pam_unix` 단원을 참조하십시오.

ASLR 활성화

이 규칙을 통해 평가 대상에 있는 EC2 인스턴스의 운영 체제에서 주소 공간 레이아웃 무작위화(ASLR)가 활성화되어 있는지 확인할 수 있습니다.

심각도

Medium

결과

평가 대상의 EC2 인스턴스에 ASLR이 활성화되어 있지 않습니다.

해결 방법

평가 대상의 보안을 강화하기 위해 echo 2 | sudo tee /proc/sys/kernel/randomize_va_space를 실행하여 평가 대상에 있는 모든 EC2 인스턴스의 운영 체제에서 ASLR을 활성화하는 것이 좋습니다.

DEP 활성화

이 규칙을 통해 평가 대상에 있는 EC2 인스턴스의 운영 체제에서 데이터 실행 방지(DEP)가 활성화되어 있는지 확인할 수 있습니다.

> **Note**
>
> 이 규칙은 ARM 프로세서가 있는 EC2 인스턴스에 대해서는 지원되지 않습니다.

심각도

Medium

결과

평가 대상의 EC2 인스턴스에 DEP가 활성화되어 있지 않습니다.

해결 방법

평가 대상에 있는 모든 EC2 인스턴스의 운영 체제에서 DEP를 활성화하는 것이 좋습니다. DEP를 활성화하면 버퍼 오버플로우 기술을 사용하여 보안 손상으로부터 인스턴스를 보호할 수 있습니다.

시스템 디렉터리에 대한 권한 구성

이 규칙은 바이너리 및 시스템 구성 정보가 들어 있는 시스템 디렉터리에 대한 권한을 확인합니다. 루트 사용자(루트 계정 자격 증명을 사용하여 로그인한 사용자)만 이 디렉터리에 대한 쓰기 권한을 갖고 있는지 확인합니다.

심각도

높음

결과

평가 대상의 EC2 인스턴스에 루트 이외의 사용자가 쓸 수 있는 시스템 디렉터리가 포함되어 있습니다.

해결 방법

평가 대상의 보안을 강화하고 악의적인 로컬 사용자의 권한 에스컬레이션을 방지하려면 대상에 있는 모든 EC2 인스턴스의 모든 시스템 디렉터리를 루트 계정 자격 증명을 사용하여 로그인하는 사용자만 쓸 수 있도록 구성합니다.

Amazon Inspector Classic 평가 템플릿 및 평가 실행

Amazon Inspector Classic을 사용하면 보안 규칙을 사용하여 AWS 리소스를 분석하여 잠재적 보안 문제를 발견할 수 있습니다. Amazon Inspector Classic은 리소스에 관한 동작 데이터(텔레메트리)를 모니터링하고 수집합니다. 데이터에는 보안 채널 사용, 실행 중인 프로세스 간의 네트워크 트래픽, AWS 서비스와의 통신에 대한 세부 정보가 포함됩니다. 그런 다음 Amazon Inspector Classic은 보안 규칙 패키지 세트에 대한 데이터를 분석 및 비교합니다. 마지막으로 Amazon Inspector Classic은 다양한 심각도의 잠재적인 보안 문제를 식별하는 결과 목록을 생성합니다.

시작하려면 평가 대상(Amazon Inspector Classic이 분석하도록 할 AWS 리소스 모음)을 만듭니다. 그 다음, 평가 템플릿(평가를 구성하는 데 사용하는 청사진)을 만듭니다. 템플릿을 사용하여 결과 세트를 생성하는 평가 실행, 모니터링 및 분석 프로세스를 시작합니다.

주제

- Amazon Inspector Classic 평가 템플릿
- Amazon Inspector Classic 평가 템플릿 한도
- 평가 템플릿 생성
- 평가 템플릿 삭제
- 평가 실행
- Amazon Inspector Classic 평가 실행 한도
- Lambda 함수로 자동 평가 실행 설정
- Amazon Inspector Classic 알림(콘솔)에 대한 SNS 주제 설정

Amazon Inspector Classic 평가 템플릿

평가 템플릿을 사용하면 다음과 같은 평가 실행의 구성을 지정할 수 있습니다.

- Amazon Inspector Classic이 평가 대상을 평가하기 위해 사용하는 규칙 패키지
- 평가 실행 기간 - 평가 실행 기간을 3분에서 24시간 사이로 설정할 수 있습니다. 평가 실행 기간은 1시간으로 설정하는 것이 좋습니다.
- Amazon Inspector Classic이 평가 실행 상태 및 결과에 대한 알림을 보내는 Amazon SNS 주제
- Amazon Inspector Classic이 평가 템플릿을 사용하는 평가 실행에서 생성한 결과에 할당할 수 있는 속성(키-값 페어)

Amazon Inspector Classic에서 평가 템플릿을 생성한 후 다른 AWS 리소스처럼 이 템플릿에 태그를 지정할 수 있습니다. 자세한 내용은 태그 편집기를 참조하십시오. 평가 템플릿에 태그를 지정하면 해당 템플릿을 구성할 수 있으며 보안 전략을 더 효율적으로 관리할 수 있습니다. 예를 들어, Amazon Inspector Classic은 평가 대상을 평가하는 데 사용할 수 있는 많은 수의 규칙을 제공합니다. 특정 영역을 대상으로 하거나 특정한 보안 문제를 발견하기 위해 평가 템플릿에 더 작은 하위 세트의 사용 가능한 규칙을 포함하고자 할 수도 있습니다. 평가 템플릿에 태그를 지정하면 보안 전략 및 목표에 따라 언제든지 신속하게 템플릿을 찾아서 실행할 수 있습니다.

> **Important**
>
> 평가 템플릿을 생성한 후에는 수정할 수 없습니다.

Amazon Inspector Classic 평가 템플릿 한도

각 AWS 계정에 대해 최대 500개의 평가 템플릿을 생성할 수 있습니다.

자세한 내용은 Amazon Inspector Classic 서비스 한도 단원을 참조하십시오.

평가 템플릿 생성

평가 템플릿 생성

1. 에 로그인 AWS Management Console 하고 https://console.aws.amazon.com/inspector/ Amazon Inspector Classic 콘솔을 엽니다.
2. 탐색 창에서 Assessment Templates(평가 템플릿)를 선택한 후 Create(생성)를 선택합니다.
3. 이름에 평가 템플릿의 이름을 입력합니다.
4. [Target name]에서 분석할 평가 대상을 선택합니다.

> **Note**
>
> 평가 템플릿을 생성할 때 평가 템플릿 페이지의 대상 미리 보기 버튼을 사용하여 평가 대상에 포함된 모든 EC2 인스턴스를 검토할 수 있습니다. 각 EC2 에이전트에 대해 호스트 이름, 인스턴스 ID, IP 주소 및 해당되는 경우 에이전트의 상태를 검토할 수 있습니다. 에이전트 상태는 정상, 비정상, 알 수 없음의 값을 가질 수 있습니다. Amazon Inspector Classic은 EC2 인스턴스에서 실행 중인 에이전트가 있는지 여부를 확인할 수 없는 경우 상태를 알 수 없음으로 표시합니다.

평가 템플릿 페이지의 대상 미리 보기 버튼을 사용하여 이전에 만든 템플릿에 포함된 평가 대상을 구성하는 EC2 인스턴스를 검토할 수도 있습니다.

5. [Rules packages]에서 평가 템플릿에 포함시킬 하나 이상의 규칙 패키지를 선택합니다.
6. [Duration]에서 평가 템플릿의 기간을 지정합니다.
7. (선택 사항) SNS 주제의 경우, Amazon Inspector Classic이 평가 실행 상태 및 결과에 대한 알림을 보내는 SNS 주제를 구체화하세요. Amazon Inspector Classic은 다음 이벤트에 대한 SNS 알림을 보낼 수 있습니다.

   - 평가 실행이 시작됨
   - 평가 실행이 종료됨
   - 평가 실행 상태가 변경됨
   - 결과가 생성됨

   SNS 주제 설정에 대한 자세한 내용은 Amazon Inspector Classic 알림(콘솔)에 대한 SNS 주제 설정 섹션을 참조하십시오.
8. (선택 사항) 태그에서 키 및 값 값을 입력합니다. 평가 템플릿에 여러 태그를 추가할 수 있습니다.
9. (선택 사항) 검색 결과에 추가된 속성의 경우 키 및 값에 대한 값을 입력합니다. Amazon Inspector Classic은 평가 템플릿에서 생성한 모든 결과에 속성을 적용합니다. 평가 템플릿에 여러 속성을 추가할 수 있습니다. 결과 및 결과 태그 지정에 대한 자세한 내용은 Amazon Inspector Classic 결과 섹션을 참조하십시오.
10. (선택 사항) 이 템플릿을 사용하여 평가 실행 일정을 설정하려면 Set up recurring assessment runs once every <number_of_days>, starting now (지금부터 <number_of_days>당 반복 평가 실행 설정) 확인란을 선택하고 위쪽 및 아래쪽 화살표로 반복 패턴(일수)을 지정하면 됩니다.

> **Note**
>
> 이 확인란을 사용하면 Amazon Inspector Classic이 사용자가 설정 중인 평가 실행 일정에 대한 Amazon CloudWatch Events 규칙을 자동으로 생성합니다. 그러고 나면 Amazon Inspector Classic이 이름이 `AWS_InspectorEvents_Invoke_Assessment_Template`으로 지정된 IAM 역할도 자동으로 생성합니다. 이 역할을 통해 CloudWatch Events는 Amazon Inspector Classic 리소스에 대해 API 호출을 수행할 수 있습니다. CloudWatch 이벤트 및 개념에 대한 자세한 내용은 What is Amazon CloudWatch Events? 및 Using Resource-Based Policies for CloudWatch Events를 참조하십시오.

> **Note**
>
> AWS Lambda 함수로 자동 평가 실행을 설정할 수도 있습니다. 자세한 내용은 Lambda 함수로 자동 평가 실행 설정 단원을 참조하십시오.

11. [Create and run] 또는 [Create]를 선택합니다.

평가 템플릿 삭제

평가 템플릿을 삭제하려면 다음 절차를 수행하십시오.

평가 템플릿 삭제

- Assessment Templates(평가 템플릿) 페이지에서 삭제할 템플릿을 선택한 후 삭제를 선택합니다. 확인 메시지가 표시되면 예를 선택합니다.

> **Important**
>
> 평가 템플릿을 삭제하면 이 템플릿과 연결된 모든 평가 템플릿, 평가 실행, 결과 및 모든 버전의 보고서가 삭제됩니다.

`DeleteAssessmentTemplate` API를 사용하여 평가 템플릿을 삭제할 수도 있습니다.

평가 실행

평가 템플릿을 만든 후 이를 사용하여 평가 실행을 시작할 수 있습니다. 각 AWS 계정의 실행 한도 내에 있는 한 동일한 템플릿을 사용하여 여러 실행을 시작할 수 있습니다. 자세한 내용은 Amazon Inspector Classic 평가 실행 한도 단원을 참조하십시오.

Amazon Inspector Classic 콘솔을 사용하는 경우 Assessment templates 페이지에서 새 평가 템플릿의 최초 실행을 시작해야 합니다. 실행을 시작한 후 [Assessment runs] 페이지를 사용하여 실행 진행 상태를 모니터링할 수 있습니다. [Run], [Cancel] 및 [Delete] 버튼을 사용하여 실행을 시작, 취소 또는 삭제할 수 있습니다. 또한 실행의 ARN, 실행을 위해 선택한 규칙 패키지, 실행에 적용한 태그 및 속성을 포함한 실행의 세부 정보를 확인할 수 있습니다.

평가 템플릿의 후속 실행에서는 평가 템플릿 페이지 또는 평가 실행 페이지의 실행, 취소, 삭제 버튼을 사용할 수 있습니다.

평가 실행 삭제

평가 실행을 삭제하려면 다음 절차를 수행하십시오.

실행을 삭제하려면

- 평가 실행 페이지에서 삭제할 실행을 선택한 후 삭제를 선택합니다. 확인 메시지가 표시되면 예를 선택합니다.

> **Important**
> 실행을 삭제하면 해당 실행의 모든 결과 및 보고서 버전도 모두 삭제됩니다.

`DeleteAssessmentRun` API를 사용하여 실행을 삭제할 수도 있습니다.

Amazon Inspector Classic 평가 실행 한도

각 AWS 계정에 대해 최대 50,000개의 평가 실행을 생성할 수 있습니다.

이 실행에 사용된 대상에 중복되는 EC2 인스턴스가 포함되지 않는 한, 여러 실행이 동시에 발생하도록 할 수 있습니다.

자세한 내용은 Amazon Inspector Classic 서비스 한도 단원을 참조하십시오.

Lambda 함수로 자동 평가 실행 설정

평가에 대한 반복 일정을 설정할 경우 콘솔을 통해 Lambda 함수를 생성하여 평가 템플릿이 자동으로 실행되도록 구성할 수 있습니다. 자세한 내용은 Lambda 함수를 참조하십시오.

AWS Lambda 콘솔을 사용하여 자동 평가 실행을 설정하려면 다음 절차를 수행합니다.

Lambda 함수를 통해 자동 실행을 설정하려면

1. 에 로그인 AWS Management Console하고 AWS Lambda 콘솔을 엽니다.
2. 탐색 창에서 대시보드 또는 함수를 선택한 후 Lambda 함수 생성)을 선택합니다.

3. 함수 생성 페이지에서 Browse serverless app repository(서버리스 앱 리포지토리 찾아보기)를 선택한 다음 검색 필드에 **inspector**를 입력합니다.
4. inspector-scheduled-run 청사진를 선택합니다.
5. 검토, 구성 및 배포 페이지에서 함수를 트리거하는 CloudWatch 이벤트를 지정하여 자동화된 실행의 반복 일정을 설정합니다. 이를 수행하려면 규칙 이름 및 설명을 입력한 다음, 예약 표현식을 선택합니다. 예약 표현식에서 실행이 발생하는 빈도를 결정합니다. 예를 들어, 15분마다 또는 하루 한 번입니다. CloudWatch 이벤트 및 개념에 대한 자세한 내용은 What is Amazon CloudWatch Events?를 참조하십시오.

   트리거 활성화 확인란을 선택한 경우 함수 생성을 마치면 즉시 실행이 시작됩니다. 자동화된 후속 실행에서는 예약 표현식 필드에 지정한 반복 패턴을 따릅니다. 함수를 생성하는 동안 [Enable trigger] 확인란을 선택하지 않은 경우 나중에 함수를 편집하여 이 트리거를 활성화할 수 있습니다.
6. [Configure function] 페이지에서 다음을 지정합니다.

   - 이름에 함수의 이름을 입력합니다.
   - (선택 사항) 설명에 나중에 함수를 식별하는 데 도움이 되는 설명을 입력합니다.
   - 런타임의 경우 기본값를 유지합니다**Node.js 8.10**.는 **Node.js 8.10** 런타임에 대해서만 inspector-scheduled-run 블루프린트를 AWS Lambda 지원합니다.
   - 이 함수를 사용하여 자동으로 실행할 평가 템플릿입니다. [assessmentTemplateArn]이라는 환경 변수 값을 제공하여 이를 수행합니다.
   - 기본값인 **index.handler**로 설정된 핸들러를 유지합니다.
   - [Role] 필드를 사용한 함수에 대한 권한입니다. 자세한 내용은 AWS Lambda 권한 모델 섹션을 참조하십시오.

     이 함수를 실행하려면 AWS Lambda 가 실행을 시작하고 오류를 포함하여 실행에 대한 로그 메시지를 Amazon CloudWatch Logs. AWS Lambda assumes에 기록할 수 있는 IAM 역할이 필요합니다. 예를 들어, 이 IAM 역할에 다음 샘플 정책을 연결할 수 있습니다.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "inspector:StartAssessmentRun",
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
```

```
        "logs:PutLogEvents"
      ],
      "Resource": "*"
    }
  ]
}
```

7. 선택 사항을 검토한 후 [Create function]을 선택합니다.

Amazon Inspector Classic 알림(콘솔)에 대한 SNS 주제 설정

Amazon Simple Notification Service(Amazon SNS)는 구독 엔드포인트 또는 클라이언트에 메시지를 보내는 웹 서비스입니다. Amazon SNS를 사용하여 Amazon Inspector Classic에 대한 알림을 설정할 수 있습니다.

알림에 대한 SNS 주제를 설정하려면

1. SNS 주제를 생성합니다. 자습서: Amazon SNS 주제 생성을 참조하십시오. 주제를 생성한 경우 Access policy - optional(액세스 정책 - 선택 사항) 섹션을 확장합니다. 확장한 후 다음을 수행하여 주제에 메시지를 전송하는 평가를 허용합니다.

   a. Choose method(방법 선택)에서 기본을 선택합니다.

   b. 주제에 메시지를 게시할 수 있는 사용자 정의에서 지정된 AWS 계정만 선택한 다음 주제를 생성하려는 리전의 계정에 대한 ARN을 입력합니다.

      - `US East (Ohio)` - arn:aws:iam::646659390643:root
      - `US East (N. Virginia)` - arn:aws:iam::316112463485:root
      - `US West (N. California)` - arn:aws:iam::166987590008:root
      - `US West (Oregon)` - arn:aws:iam::758058086616:root
      - `Asia Pacific (Mumbai)` - arn:aws:iam::162588757376:root
      - `Asia Pacific (Seoul)` - arn:aws:iam::526946625049:root
      - `Asia Pacific (Sydney)` - arn:aws:iam::454640832652:root
      - `Asia Pacific (Tokyo)` - arn:aws:iam::406045910587:root
      - `Europe (Frankfurt)` - arn:aws:iam::537503971621:root
      - `Europe (Ireland)` - arn:aws:iam::357557129151:root
      - `Europe (London)` - arn:aws:iam::146838936955:root

- `Europe (Stockholm)` - arn:aws:iam::453420244670:root
- `AWS GovCloud (US-East)` - arn:aws-us-gov:iam::206278770380:root
- `AWS GovCloud (US-West)` - arn:aws-us-gov:iam::850862329162:root

c. 이 주제를 구독할 수 있는 사용자 정의에서 지정된 AWS 계정만 선택한 다음 주제를 생성하려는 리전의 계정에 대한 ARN을 입력합니다.

d. IAM 사용 설명서에서 혼동된 대리자 문제에 설명된 대로 Inspector가 혼동된 대리자로 사용되는 것을 방지하려면 다음과 같이 하십시오.

i. 고급을 선택합니다. 이렇게 하면 JSON 편집기로 이동하게 됩니다.

ii. 다음 조건을 추가합니다.

```
"Condition": {
   "StringEquals": {
     "aws:SourceAccount": <your account Id here>,
     "aws:SourceArn": "arn:aws:inspector:*:*:*"
   }
 }
```

e. (선택 사항) aws:SourceAccount 및 aws:SourceArn에 대한 추가 정보는 IAM 사용 설명서의 전역 조건 컨텍스트 키를 참고하십시오.

f. 필요에 따라 주제에 대한 기타 설정을 업데이트한 후 주제 생성을 선택합니다.

2. (선택 사항) 암호화된 SNS 주제를 생성하려면 SNS 개발자 설명서의 저장된 암호화를 참고하십시오.

3. Inspector가 KMS 키의 혼동된 대리자로 사용되는 것을 방지할 수 있도록 아래의 추가 단계를 수행합니다.

a. KMS 콘솔에서 CMK로 이동합니다.

b. 편집을 선택합니다.

c. 다음 조건을 추가합니다.

```
"Condition": {
   "StringEquals": {
     "aws:SourceAccount": <your account Id here>,
     "aws:SourceArn": "arn:aws:sns:*:*:*"
   }
```

```
        }
```

4. 생성한 주제에 대한 구독을 생성합니다. 자세한 내용은 자습서: 엔드포인트를 Amazon SNS 주제에 구독 설정을 참조하십시오.
5. 구독이 올바르게 구성되었는지 확인하려면 주제에 메시지를 게시하십시오. 자세한 내용은 자습서: Amazon SNS 주제에 메시지 게시를 참조하십시오.

Amazon Inspector Classic 결과

결과는 평가 대상을 평가하는 동안 Amazon Inspector Classic에서 발견할 수 있는 잠재적인 보안 문제입니다. 결과는 Amazon Inspector Classic 콘솔 또는 API를 통해 표시됩니다. 결과에는 보안 문제 및 이를 해결하기 위한 권장 사항에 대한 자세한 설명이 포함되어 있습니다.

Amazon Inspector에서 결과를 생성하면 Amazon Inspector Classic 관련 속성을 결과에 할당하여 결과를 추적할 수 있습니다. 이 속성은 키-값 페어로 구성됩니다.

속성을 사용하여 결과를 추적하는 것은 보안 전략의 워크플로를 관리하는 데 매우 유용할 수 있습니다. 예를 들어, 평가를 생성 및 실행한 후 사용자 보안 목표 및 접근 방식에 기반한 다양한 심각도, 긴급도 및 사용자 관심의 결과 목록이 생성됩니다. 결과의 권장 사항 단계 하나를 즉시 수행하여 잠재적으로 긴급한 보안 문제를 해결하고자 할 수 있습니다. 또는 다음에 서비스 업데이트가 제공될 때까지 다른 결과의 해결을 연기하고자 할 수도 있습니다. 예를 들어, 즉시 해결할 결과를 추적하려면 **`Status`** / **`Urgent`**의 키-값 페어를 가진 속성을 생성하여 결과에 할당할 수 있습니다. 또한 속성을 사용하여 잠재적 보안 문제를 해결하는 워크로드를 분산할 수 있습니다. 예를 들어, 팀의 보안 엔지니어인 Bob에게 결과를 해결할 작업을 제공하기 위해 **`Assigned Engineer`** / **`Bob`**의 키-값 페어를 가진 속성을 결과에 할당할 수 있습니다.

조사 결과 작업

생성된 Amazon Inspector Classic 결과에서 다음 절차를 수행합니다.

속성을 찾고, 분석하고, 결과에 할당

1. 에 로그인 AWS Management Console 하고 https://console.aws.amazon.com/inspector/ Amazon Inspector Classic 콘솔을 엽니다.
2. 평가를 실행한 후 Amazon Inspector Classic 콘솔에서 결과 페이지로 이동하여 결과를 볼 수 있습니다.

   또한, Amazon Inspector Classic 콘솔의 대시보드 페이지에 있는 주목할 만한 조사 결과 섹션에서 조사 결과를 확인할 수 있습니다.

   > **Note**
   >
   > 평가 실행이 진행 중일 때는 평가 실행에서 생성되는 결과를 볼 수 없습니다. 그러나 기간이 완료되기 전에 평가를 중지한 경우 결과의 하위 세트를 볼 수 있습니다. 프로덕션 환경

에서는 전체 결과 세트를 생성할 수 있도록 모든 평가가 전체 기간 동안 실행되도록 하는 것이 좋습니다.

3. 특정 결과에 대한 세부 정보를 보려면 해당 결과 옆의 확장 위젯을 선택합니다. 결과 세부 정보에는 다음이 포함됩니다.

   - 이 결과가 등록된 EC2 인스턴스를 포함하는 평가 대상의 이름
   - 이 결과를 생성하는 데 사용된 평가 템플릿의 이름.
   - 평가 실행 시작 시간.
   - 평가 실행 종료 시간.
   - 평가 실행 상태.
   - 이 결과를 트리거한 규칙을 포함하는 규칙 패키지의 이름.
   - 결과의 이름.
   - 결과의 심각도.
   - CVSS(공통 취약성 평가 시스템)의 기본 심각도 세부 정보. 여기에는 CVE(일반적인 취약성 및 노출도) 규칙 패키지의 규칙에 의해 생성된 결과의 CVSS 벡터 및 CVSS 점수 지표(CVSS 버전 2.0 및 3.0 포함)가 포함됩니다. CVSS에 대한 자세한 내용은 https://www.first.org/cvss/를 참조하십시오.
   - 인터넷 보안 센터(CIS)의 기본 심각도 세부 정보입니다. 여기에는 CIS 벤치마크 패키지의 규칙을 통해 생성된 결과의 CIS 가중 지표가 포함됩니다. CIS 가중 지표에 대한 자세한 내용은 https://www.cisecurity.org/를 참조하십시오.
   - 결과에 대한 설명.
   - 결과에서 설명하는 잠재적 보안 문제를 해결하기 위해 수행할 수 있는 권장 단계.

4. 결과에 속성을 할당하려면 결과를 선택한 후 [Add/Edit Attributes]를 선택합니다.

   평가 템플릿을 만들 때 결과에 속성을 할당할 수도 있습니다. 이를 수행하기 위해 평가 실행에 의해 생성된 모든 결과에 속성을 자동으로 할당하도록 새 템플릿을 구성합니다. 이 평가의 조사 결과를 위한 태그 필드에서 키 및 값 필드를 사용할 수 있습니다. 자세한 내용은 Amazon Inspector Classic 평가 템플릿 및 평가 실행 단원을 참조하십시오.

5. 결과를 스프레드시트로 내보내려면 Findings(결과) 페이지의 오른쪽 상단 모서리에 있는 아래쪽 화살표를 선택합니다. 대화 상자에서 모든 열 내보내기 또는 표시된 열 내보내기를 선택합니다.

   내보낸 내용에서 모든 datetime 값은 Epoch 타임스탬프입니다.

6. 현재 조사 결과를 필터링하려면, 조사 결과 테이블 위에 있는 필터 표시줄에 인스턴스 ID 또는 CVE 번호와 같이 필터링하려는 단일 문자열을 입력합니다. 추가 정보 열을 표시하거나 숨기려면 조사 결과 페이지의 오른쪽 상단에 있는 설정 아이콘을 선택합니다.
7. 결과를 삭제하려면 평가 실행 페이지로 가서 결과를 삭제할 실행을 선택합니다. 그런 다음 삭제를 선택합니다. 확인 메시지가 표시되면 예를 선택합니다.

> **Important**
>
> Amazon Inspector Classic에서는 개별 조사 결과를 삭제할 수 없습니다. 평가 실행을 삭제하면 해당 실행의 모든 결과와 모든 버전의 보고서가 삭제됩니다.

DeleteAssessmentRun API를 사용하여 평가 실행을 삭제할 수도 있습니다.

평가 보고서

Amazon Inspector Classic 평가 보고서는 평가 실행에서 테스트한 항목과 평가 결과를 자세히 보여 주는 문서입니다. 보고서를 저장하고 팀과 수정 작업을 공유하거나 규정 준수 감사 데이터를 보완하는 데 사용할 수 있습니다. 실행을 성공적으로 완료한 후 평가 실행에 대한 보고서를 생성할 수 있습니다.

> **Note**
>
> Amazon Inspector Classic에서 평가 보고서 기능을 제공한 2017년 4월 25일 이후에 수행된 평가 실행에 대해서만 보고서를 생성할 수 있습니다.

다음과 같은 종류의 평가 보고서를 볼 수 있습니다.

- 결과 보고서 – 이 보고서에는 다음과 같은 내용이 포함됩니다.
  - 평가에 대한 요약
  - 평가 실행 중 평가된 EC2 인스턴스
  - 평가 실행에 포함된 규칙 패키지
  - 각 결과에 대한 자세한 내용(결과를 보유한 모든 EC2 인스턴스 포함)
- 전체 보고서 – 이 보고서에는 결과 보고서에 포함되는 모든 내용이 포함되며, 평가 대상의 인스턴스에 대해 확인된 규칙 목록이 추가로 제공됩니다.

평가 보고서를 생성하려면

1. 평가 실행 페이지에서 보고서를 생성할 평가 실행을 찾습니다. 상태가 Analysis complete(분석 완료)로 설정되어 있는지 확인합니다.
2. 이 평가 실행에 대한 보고서 열에서 보고서 아이콘을 선택합니다.

   > **Important**
   >
   > 2025년 3월 24일부터 평가 보고서에는 네트워크 연결성 조사 결과에 대한 심각도 정보가 더 이상 포함되지 않습니다. 이 정보는 Amazon Inspector 콘솔에서 확인할 수 있습니다.

3. 평가 보고서)대화 상자에서 보려는 보고서 유형(결과 또는 전체 보고서)과 보고서 형식(HTML 또는 PDF)을 선택합니다. 그런 다음 보고서 생성을 선택합니다.

GetAssessmentReport API를 통해 평가 보고서를 생성할 수도 있습니다.

평가 보고서를 삭제하려면 다음 절차를 수행하십시오.

보고서를 삭제하려면

- 평가 실행 페이지에서 삭제하려는 보고서의 대상인 실행을 선택한 후 삭제를 선택합니다. 확인 메시지가 표시되면 예를 선택합니다.

  > **Important**
  >
  > Amazon Inspector Classic에서는 개별 보고서를 삭제할 수 없습니다. 평가 실행을 삭제하면 해당 실행의 모든 버전의 보고서와 결과도 모두 삭제됩니다.

  DeleteAssessmentRun API를 사용하여 평가 실행을 삭제할 수도 있습니다.

Amazon Inspector Classic의 제외 사항

제외 항목은 Amazon Inspector Classic 평가 실행의 출력입니다. 제외 항목은 사용자가 완료할 수 없는 보안 검사 및 해당 문제를 해결하는 방법을 보여 줍니다. 예를 들어 지정된 대상의 EC2 인스턴스에 에이전트가 없거나, 지원되지 않는 운영 체제를 사용하거나, 예기치 않은 오류로 인해 문제가 발생할 수 있습니다.

콘솔의 평가 실행 페이지에서 제외 항목을 볼 수 있습니다. 자세한 내용은 사후 평가 제외 항목 보기 단원을 참조하십시오.

불필요한 AWS 요금이 발생하지 않도록 Amazon Inspector Classic을 사용하면 평가를 실행하기 전에 제외 항목을 미리 볼 수 있습니다. 콘솔의 Assessment templates(평가 템플릿) 페이지에서 미리 보기를 확인할 수 있습니다. 자세한 내용은 제외 항목 미리 보기 단원을 참조하십시오.

> **Note**
>
> 2018년 6월 25일 이후에 실행한 경우에만 사후 평가 제외 항목을 생성할 수 있습니다. 이는 Amazon Inspector Classic에서 제외 항목이 사용 가능하게 된 시점입니다. 하지만 제외 항목 미리 보기는 날짜와 관계없이 모든 평가 템플릿에서 사용할 수 있습니다.

주제

- 제외 유형
- 제외 항목 미리 보기
- 사후 평가 제외 항목 보기

제외 유형

Amazon Inspector Classic은 다음과 같은 제외 유형을 발생시킬 수 있습니다.

제외 유형	설명	권장 사항
대상	평가 대상에 지정된	평가 대상의 태그가

제외 유형	설명	권장 사항
에이전트 인스턴스 없음	태그를 가진 EC2 인스턴스가 없습니다.	대상 EC2 인스턴스의 태그와 일치하는지 확인합니다.
에이전트가 실행 중임	이미 대상 EC2 인스턴스에서 평가 실행이 진행 중입니다.	대상 EC2 인스턴스에서 현재 평가 실행이 완료될 때까지 기다립니다.

제외 유형	설명	권장 사항
에이전트를 찾을 수 없음	대상 EC2 인스턴스에서 Amazon Inspector Classic 에이전트를 찾을 수 없습니다.	대상 EC2 인스턴스에 Amazon Inspector Classic 에이전트를 설치하거나 다시 설치하십시오. 자세한 내용은 Amazon Inspector Classic 에이전트 설치하기 단원을 참조하십시오.

제외 유형	설명	권장 사항
에이전트 에이상이 있음	대상 EC2 인스턴스의 Amazon Inspector Classic 에이전트가 비정상 상태입니다.	이 인스턴스에서 Amazon Inspector Classic 에이전트의 상태를 확인하고 필요한 작업을 수행합니다. 자세한 내용은 Inspector 에이전트 섹션을 참조하십시오.

제외 유형	설명	권장 사항
지원되지 않는 OS 버전	대상 EC2 인스턴스의 운영 체제가 Amazon Inspector Classic 평가를 지원하지 않습니다.	평가 대상에서 대상 EC2 인스턴스를 제거하거나 이 인스턴스가 포함되지 않은 대상을 생성합니다. 지원되는 운영 체제 목록은 Amazon Inspector Classic 지원 운영 체제 및 리전을 참조하십시오.

제외 유형	설명	권장 사항
사용되지 않는 규칙 패키지	평가 템플릿에 더 이상 사용되지 않는 규칙 패키지가 포함되어 있습니다.	사용되지 않는 규칙 패키지 없이 평가 템플릿을 생성한 다음 이를 향후 평가 실행에 사용합니다.

제외 유형	설명	권장 사항
OS에서 지원되지 않는 규칙 패키지	대상 EC2 인스턴스의 운영 체제가 평가 템플릿에 포함된 규칙 패키지에서 지원되지 않습니다.	충돌하는 규칙 패키지 없이 평가 템플릿을 생성하거나 평가 템플릿에서 대상 EC2 인스턴스를 제거합니다. 운영 체제에서 지원되는 규칙 패키지 목록은 지원되는 운영 체제의 규칙 패키지 가용성을 참조하십시오.

제외 유형	설명	권장 사항
단일 인스턴스에 대한 규칙 평가 오류	내부 오류로 인해 이 인스턴스에 대한 규칙 평가에 장애가 발생했습니다.	평가를 다시 시도합니다. 평가를 다시 실행할 때 제외가 지속되면 Support에 문의하십시오.
규칙 평가 오류	내부 오류로 인해 평가에 대한 규칙 평가에 장애가 발생했습니다.	평가를 다시 시도합니다. 평가를 다시 실행할 때 제외가 지속되면 Support에 문의하십시오.

제외 유형	설명	권장 사항
네트워크 연결성 오류 - 인터넷	내부 오류로 인해 네트워크 연결성 평가가 인터넷에서 연결할 수 있는 포트를 확인하는 데 실패했습니다. 다른 네트워크 연결성 유형에 대한 결과를 얻을 수 있습니다.	평가를 다시 시도합니다. 평가를 다시 실행할 때 제외가 지속되면 Support에 문의하십시오.

제외 유형	설명	권장 사항
네트워크 연결성 오류 - Application Load Balan를 통한 인터넷	내부 오류로 인해 네트워크 연결성 평가가 Application Load Balancer를 통해 인터넷에서 연결할 수 있는 포트를 확인하는 데 실패했습니다. 다른 네트워크 연결성 유형에 대한 결과를 얻을 수 있습니다.	평가를 다시 시도합니다. 평가를 다시 실행할 때 제외가 지속되면 Support에 문의하십시오.

제외 유형	설명	권장 사항
네트워크 연결성 오류 - Elastic Load Balan 로드 밸런서를 통한 인터넷	내부 오류로 인해 네트워크 연결성 평가가 Elastic Load Balancing 로드 밸런서를 통해 인터넷에서 연결할 수 있는 포트를 확인하는 데 실패했습니다. 다른 네트워크 연결성 유형에 대한 결과를 얻을 수 있습니다.	평가를 다시 시도합니다. 평가를 다시 실행할 때 제외가 지속되면 Support에 문의하십시오.

제외 유형	설명	권장 사항
네트워크 연결성 오류 - VPN	내부 오류로 인해 네트워크 연결성 평가가 VPN에서 연결할 수 있는 포트를 확인하는 데 실패했습니다. 다른 네트워크 연결성 유형에 대한 결과를 얻을 수 있습니다.	평가를 다시 시도합니다. 평가를 다시 실행할 때 제외가 지속되면 Support에 문의하십시오.

제외 유형	설명	권장 사항
네트워크 연결성 오류 - AWS Direct Conne	내부 오류로 인해를 통해 연결할 수 있는 포트에 대한 검사에서 네트워크 연결성 평가가 실패했습니다 AWS Direct Connect. 다른 네트워크 연결성 유형에 대한 결과를 얻을 수 있습니다.	평가를 다시 시도합니다. 평가를 다시 실행할 때 제외가 지속되면 Support에 문의하십시오.

제외 유형	설명	권장 사항
네트워크 연결성 오류 – VPC 피어링	내부 오류로 인해 네트워크 연결성 평가가 피어링된 VPC에서 연결할 수 있는 포트를 확인하는 데 실패했습니다. 다른 네트워크 연결성 유형에 대한 결과를 얻을 수 있습니다.	평가를 다시 시도합니다. 평가를 다시 실행할 때 제외가 지속되면 Support에 문의하십시오.

제외 항목 미리 보기

Amazon Inspector Classic에서는 평가를 실행하기 전에 잠재적인 제외 항목을 미리 볼 수 있게 해 줍니다.

평가 제외 항목을 미리 보려면

1. 에 로그인 AWS Management Console 하고 https://console.aws.amazon.com/inspector/ Amazon Inspector Classic 콘솔을 엽니다.
2. 탐색 창에서 Assessment templates(평가 템플릿)를 선택합니다.
3. 평가 템플릿을 확장하고 Assessment templates(평가 템플릿) 섹션에서 Preview exclusions(제외 항목 미리 보기)를 선택합니다.

4. 감지된 모든 제외 항목에 대한 설명 및 이를 해결하기 위한 권장 사항을 검토합니다.

   `ListExclusions` 및 `DescribeExclusions` 작업을 사용하여 제외 항목을 나열 및 설명할 수도 있습니다.

사후 평가 제외 항목 보기

평가 실행 후 모든 제외 항목에 대한 세부 정보를 볼 수 있습니다.

제외 항목에 대한 세부 정보를 보려면

1. 에 로그인 AWS Management Console 하고 https://console.aws.amazon.com/inspector/ Amazon Inspector Classic 콘솔을 엽니다.
2. 탐색 창에서 Assessment runs(평가 실행)를 선택합니다.
3. Exclusions(제외 항목) 열에서 평가 실행과 연결된 활성 링크를 선택합니다.
4. 감지된 모든 제외 항목에 대한 설명 및 이를 해결하기 위한 권장 사항을 검토합니다.

   `ListExclusions` 및 `DescribeExclusions` 작업을 사용하여 제외 항목을 나열 및 설명할 수도 있습니다.

지원되는 운영 체제의 Amazon Inspector Classic 규칙 패키지

평가 대상에 포함된 EC2 인스턴스에서 Amazon Inspector Classic 규칙 패키지를 실행할 수 있습니다. 다음 표는 지원되는 운영 체제에 대한 규칙 패키지의 가용성을 보여 줍니다.

> **Important**
>
> 운영 체제와 상관없이 모든 EC2 인스턴스에서 네트워크 연결성 규칙 패키지를 사용하여 에이전트 없는 평가를 실행할 수 있습니다.

> **Note**
>
> 지원되는 운영 체제에 대한 자세한 내용은 Amazon Inspector Classic이 지원되는 운영 체제 및 리전 섹션을 참조하십시오.

지원되는 운영 체제	CVE(일반적인 취약성 및 노출도)	CIS 벤치마크	네트워크 연결성	보안 모범 사례	실행 시간 행동 분석
Amaz Linux 2	지원	지원	지원	지원	Deprecated
Amaz Linux 2018.	지원	지원	지원	지원	Deprecated
Amaz Linux 2017.	지원	지원	지원	지원	Deprecated

지원되는 운영체제	CVE(일반적인 취약성 및 노출도)	CIS 벤치마크	네트워크 연결성	보안 모범 사례	실행 시간 행동 분석
Amaz Linux 2017.	지원	지원	지원	지원	Deprecated
Amaz Linux 2016.	지원	지원	지원	지원	Deprecated
Amaz Linux 2016.	지원	지원	지원	지원	Deprecated
Amaz Linux 2015.	지원	지원	지원	지원	Deprecated
Amaz Linux 2015.	지원	지원	지원	지원	Deprecated
Amaz Linux 2014.	지원		지원	지원	
Amaz Linux 2014.	지원		지원	지원	

지원되는 운영체제	CVE(일반적인 취약성 및 노출도)	CIS 벤치마크	네트워크 연결성	보안 모범 사례	실행 시간 행동 분석
Amaz Linux 2013.	지원		지원	지원	
Amaz Linux 2013.	지원		지원	지원	
Amaz Linux 2012.	지원		지원	지원	
Amaz Linux 2012.	지원		지원	지원	
Ubun 20.04 LTS	지원		지원	지원	
Ubun 18.04 LTS	지원	지원	지원	지원	Deprecated
Ubun 16.04 LTS	지원	지원	지원	지원	Deprecated

지원되는 운영 체제	CVE(일반적인 취약성 및 노출도)	CIS 벤치마크	네트워크 연결성	보안 모범 사례	실행 시간 행동 분석
Ubun 14.04 LTS	지원	지원	지원	지원	Deprecated
Debia 10.x, 9.0 - 9.5, 8.0 - 8.7	지원		지원	지원	
RHEL 8.x	지원		지원	지원	
RHEL 7.6 - 7.x	지원	지원	지원	지원	
RHEL 6.2 - 6.9, 7.2 - 7.5	지원	지원	지원	지원	Deprecated

지원되는 운영 체제	CVE(일반적인 취약성 및 노출도)	CIS 벤치마크	네트워크 연결성	보안 모범 사례	실행 시간 행동 분석
Cent(7.6 - 7.X	지원	지원	지원	지원	
Cent(6.2-6. 7.2-7.	지원	지원	지원	지원	Deprecated
Wind Serve 2019 Base	지원		지원		
Wind Serve 2016 Base	지원	지원	지원		Deprecated
Wind Serve 2012 R2	지원	지원	지원		Deprecated
Wind Serve 2012	지원	지원	지원		Deprecated

지원되는 운영 체제	CVE(일반적인 취약성 및 노출도)	CIS 벤치마크	네트워크 연결성	보안 모범 사례	실행 시간 행동 분석
Windows Server 2008 R2	지원	지원	지원		Deprecated

를 사용하여 Amazon Inspector Classic API 호출 로깅 AWS CloudTrail

Amazon Inspector Classic은 Amazon Inspector Classic에서 사용자, 역할 또는 AWS CloudTrail서비스가 수행한 작업에 대한 레코드를 제공하는 AWS 서비스와 통합됩니다. CloudTrail은 Amazon Inspector Classic 콘솔의 호출과 Amazon Inspector Classic API 작업에 대한 코드 호출을 포함하여 Amazon Inspector Classic에 대한 모든 API 호출을 이벤트로 캡처합니다. 추적을 생성하면 Amazon Inspector Classic 이벤트를 포함한 CloudTrail 이벤트를 지속적으로 Amazon S3 버킷에 배포할 수 있습니다. 추적을 구성하지 않은 경우에도 CloudTrail 콘솔의 이벤트 기록에서 최신 이벤트를 볼 수 있습니다. CloudTrail에서 수집한 정보를 사용하여 Amazon Inspector Classic에 수행된 요청, 요청이 수행된 IP 주소, 요청을 수행한 사람, 요청이 수행된 시간 및 기타 자세한 사항을 확인할 수 있습니다.

CloudTrail에 대한 자세한 내용은 AWS CloudTrail 사용 설명서를 참조하세요. Amazon Inspector Classic API 작업의 전체 목록은 Amazon Inspector Classic API 참조의 작업을 참고하십시오.

CloudTrail 내의 Amazon Inspector Classic 정보

AWS 계정을 생성할 때 계정에서 CloudTrail이 활성화됩니다. Amazon Inspector Classic에서 활동이 발생하면 해당 활동이 이벤트 기록의 다른 AWS 서비스 이벤트와 함께 CloudTrail 이벤트에 기록됩니다. AWS 계정에서 최신 이벤트를 확인, 검색 및 다운로드할 수 있습니다. 자세한 내용은 CloudTrail 이벤트 기록을 사용하여 이벤트 보기에서 참조하세요.

Amazon Inspector Classic에 대한 이벤트를 포함하여 AWS 계정의 이벤트를 지속적으로 기록하려면 추적을 생성합니다. CloudTrail은 추적을 사용하여 Amazon S3 버킷으로 로그 파일을 전송할 수 있습니다. 콘솔에서 추적을 생성하면 기본적으로 모든 AWS 리전에 추적이 적용됩니다. 추적은 AWS 파티션의 모든 리전에서 이벤트를 로깅하고 지정한 Amazon S3 버킷으로 로그 파일을 전송합니다. 또한 CloudTrail 로그에서 수집된 이벤트 데이터를 추가로 분석하고 조치를 취하도록 다른 AWS 서비스를 구성할 수 있습니다. 자세한 내용은 다음 자료를 참조하세요.

- 트레일 생성 개요
- CloudTrail 지원 서비스 및 통합
- CloudTrail에서 Amazon SNS 알림 구성
- 여러 리전으로부터 CloudTrail 로그 파일 받기 및 여러 계정으로부터 CloudTrail 로그 파일 받기

CloudTrail은 `AddAttributesToFindings` 및 `DescribeAssessmentTargets` 같은 읽기 전용 작업과 `ListAssessmentRuns` 및 `CreateAssessmentTemplate` 같은 관리 작업을 포함한 모든 Amazon Inspector Classic 작업을 기록합니다.

> **Note**
>
> CloudTrail은 Amazon Inspector Classic 읽기 전용 작업의 요청 정보만 기록합니다. 요청 및 응답 정보는 다른 모든 Amazon Inspector Classic 작업에 대해 기록됩니다.

모든 이벤트 또는 로그 항목에는 요청을 생성했던 사용자에 대한 정보가 포함됩니다. 자격 증명을 이용하면 다음을 쉽게 판단할 수 있습니다.

- 요청이 루트 또는 AWS Identity and Access Management (IAM) 사용자 자격 증명으로 이루어졌는지 여부
- 역할 또는 페더레이션 사용자에 대한 임시 보안 자격 증명을 사용하여 요청이 생성되었는지 여부
- 다른 AWS 서비스에서 요청을 했는지 여부

자세한 내용은 CloudTrail userIdentity 요소 섹션을 참조하세요.

Amazon Inspector Classic 로그 파일 항목 이해하기

추적이란 지정한 Amazon S3 버킷에 이벤트를 로그 파일로 입력할 수 있게 하는 구성입니다. CloudTrail 로그 파일에는 하나 이상의 로그 항목이 포함될 수 있습니다. 이벤트는 모든 소스로부터의 단일 요청을 나타내며 요청 작업, 작업 날짜와 시간, 기타 요청 파라미터에 관한 정보가 들어 있습니다. CloudTrail 로그 파일은 퍼블릭 API 직접 호출의 주문 스택 트레이스가 아니므로 특정 순서로 표시되지 않습니다.

다음 예제는 Amazon Inspector Classic `CreateResourceGroup` 작업을 보여주는 CloudTrail 로그 항목입니다.

```
{
    "eventVersion": "1.03",
    "userIdentity": {
        "type": "AssumedRole",
        "principalId": "AIDACKCEVSQ6C2EXAMPLE",
        "arn": "arn:aws:iam::444455556666:user/Alice",
        "accountId": "444455556666",
```

```
        "accessKeyId": "AKIAI44QH8DHBEXAMPLE",
        "sessionContext": {
            "attributes": {
                "mfaAuthenticated": "false",
                "creationDate": "2016-04-14T17:05:54Z"
            },
            "sessionIssuer": {
                "type": "Role",
                "principalId": "AIDACKCEVSQ6C2EXAMPLE",
                "arn": "arn:aws:iam::444455556666:user/Alice",
                "accountId": "444455556666",
                "userName": "Alice"
            }
        }
    },
    "eventTime": "2016-04-14T17:12:34Z",
    "eventSource": "inspector.amazonaws.com",
    "eventName": "CreateResourceGroup",
    "awsRegion": "us-west-2",
    "sourceIPAddress": "205.251.233.179",
    "userAgent": "console.amazonaws.com",
    "requestParameters": {
        "resourceGroupTags": [
            {
                "key": "Name",
                "value": "ExampleEC2Instance"
            }
        ]
    },
    "responseElements": {
        "resourceGroupArn": "arn:aws:inspector:us-west-2:444455556666:resourcegroup/0-
oclRMp8B"
    },
    "requestID": "148256d2-0264-11e6-a9b5-b98a7d3b840f",
    "eventID": "e5ea533e-eede-46cc-94f6-0d08e6306ff0",
    "eventType": "AwsApiCall",
    "apiVersion": "v20160216",
    "recipientAccountId": "444455556666"
}
```

Amazon CloudWatch를 사용하여 Amazon Inspector Classic 모니터링하기

원시 데이터를 수집하여 읽기 가능하며 실시간에 가까운 지표로 처리하는 Amazon CloudWatch를 통해 Amazon Inspector Classic을 모니터링할 수 있습니다. Amazon Inspector Classic은 기본적으로 측정치 데이터를 5분 동안 CloudWatch에 전송합니다. AWS Management Console, AWS CLI또는 API를 사용하여 Amazon Inspector Classic이 CloudWatch로 보내는 지표를 볼 수 있습니다.

Amazon CloudWatch에 대한 자세한 내용은 Amazon CloudWatch 사용 설명서를 참조하십시오.

Amazon Inspector Classic CloudWatch 지표

Amazon Inspector Classic 네임스페이스에는 다음 지표가 포함되어 있습니다.

`AssessmentTargetARN` 지표:

지표	설명
`TotalMatchingAgents`	이 대상에 일치하는 에이전트 수
`TotalHealthyAgents`	이 대상에 일치하는 정상적인 에이전트 수
`TotalAssessmentRuns`	이 대상에 대한 평가 실행 수
`TotalAssessmentRun Findings`	이 대상에 대한 결과 수

`AssessmentTemplateARN` 지표:

지표	설명
`TotalMatchingAgents`	이 템플릿에 일치하는 에이전트 수
`TotalHealthyAgents`	이 템플릿에 일치하는 정상적인 에이전트 수
`TotalAssessmentRuns`	이 템플릿에 대한 평가 실행 수

지표	설명
`TotalAssessmentRunFindings`	이 템플릿에 대한 결과 수

집계 지표

지표	설명
`TotalAssessmentRuns`	이 AWS 계정의 평가 실행 수

AWS CloudFormation를 사용하여 Amazon Inspector Classic 구성하기

에서 지원하는 Amazon Inspector Classic 리소스에 대한 참조 정보는 다음 주제를 AWS CloudFormation참조하세요.

- `AWS::Inspector::AssessmentTarget`
- `AWS::Inspector::AssessmentTemplate`
- `AWS::Inspector::ResourceGroup`

> **Important**
>
> 지원되는 AWS 리전에 있는 Amazon Inspector Classic 규칙 패키지의 ARNs 목록은 섹션을 참조하세요규칙 패키지용 Amazon Inspector Classic ARN.

와 통합 AWS Security Hub

AWS Security Hub는에서 보안 상태를 포괄적으로 볼 수 있도록 AWS 하고 보안 업계 표준 및 모범 사례를 기준으로 환경을 확인하는 데 도움이 됩니다. Security Hub는 여러 AWS 계정, 서비스 및 지원되는 타사 파트너 제품에서 보안 데이터를 수집하고 보안 추세를 분석하고 우선 순위가 가장 높은 보안 문제를 식별하는 데 도움이 됩니다.

Security Hub와의 Amazon Inspector 통합을 활용하면 Amazon Inspector에서 Security Hub로 조사 결과를 전송할 수 있습니다. 그러면 Security Hub의 보안 태세 분석에 이러한 결과가 포함됩니다.

목차

- Amazon Inspector에서 Security Hub로 결과를 보내는 방법
  - Amazon Inspector가 전송하는 조사 결과의 유형
  - 조사 결과 전송 지연 시간
  - Security Hub를 사용할 수 없을 때 다시 시도
  - Security Hub에서 기존 조사 결과 업데이트
- Amazon Inspector가 발견한 일반적인 조사 결과
- 통합 활성화 및 구성
- 결과 전송을 중지하는 방법

Amazon Inspector에서 Security Hub로 결과를 보내는 방법

Security Hub의 경우, 보안 문제를 조사 결과와 같이 추적합니다. 일부 결과는 다른 AWS 서비스 또는 타사 파트너가 감지한 문제에서 비롯됩니다. Security Hub에는 보안 문제를 감지하고 조사 결과를 생성하는 데 사용하는 규칙 집합도 있습니다.

Security Hub는 이러한 모든 출처를 총망라하여 조사 결과를 관리할 도구를 제공합니다. 사용자는 조사 결과 목록을 조회하고 필터링할 수 있으며 주어진 조사 결과의 세부 정보를 조회할 수도 있습니다. AWS Security Hub 사용 설명서에서 결과 보기를 참조하세요. 또한 주어진 조사 결과에 대한 조사 상태를 추적할 수도 있습니다. AWS Security Hub 사용 설명서에서 결과에 대한 작업 수행을 참조하세요.

Security Hub의 모든 결과는 AWS Security Finding Format(ASFF)이라는 표준 JSON 형식을 사용합니다. ASFF에는 문제의 출처, 영향을 받은 리소스와 결과의 현재 상태 등에 관한 세부 정보가 포함됩니다. AWS Security Hub 사용 설명서에서 AWS Security Finding 형식(ASFF)을 참조하세요.

Amazon Inspector는 Security Hub로 조사 결과를 전송하는 AWS 서비스 중 하나입니다.

Amazon Inspector가 전송하는 조사 결과의 유형

Amazon Inspector는 생성한 모든 조사 결과를 Security Hub로 보냅니다.

Amazon Inspector는 AWS Security Finding Format(ASFF)을 사용하여 결과를 Security Hub로 보냅니다. ASFF의 경우, `Types` 필드가 결과 유형을 제공합니다. Amazon Inspector의 결과는 `Types`의 값이 다음과 같을 수 있습니다.

- 소프트웨어와 구성 점검 및 취약성, CVE
- 소프트웨어 및 구성 점검/AWS 보안 모범 사례/네트워크 연결성
- 소프트웨어 및 구성 검사/산업 및 규제 표준/CIS 호스트 강화 벤치마크

조사 결과 전송 지연 시간

Amazon Inspector가 새 결과를 생성하면 보통 5분 안에 Security Hub로 전송됩니다.

Security Hub를 사용할 수 없을 때 다시 시도

Security Hub를 사용할 수 없는 경우, Amazon Inspector는 결과가 수신될 때까지 조사 결과 전송을 재시도합니다.

Security Hub에서 기존 조사 결과 업데이트

결과를 Security Hub, Amazon Inspector로 보낸 다음 업데이트를 전송하여 결과 활동의 추가적인 관찰 결과를 반영합니다. 이는 Amazon Inspector에서 발견한 것보다 Security Hub에 있는 Amazon Inspector의 조사 결과가 더 적어지는 결과를 낳게 합니다.

Amazon Inspector가 발견한 일반적인 조사 결과

Amazon Inspector는 AWS Security Finding Format(ASFF)을 사용하여 결과를 Security Hub로 보냅니다.

다음은 Amazon Inspector의 일반적인 결과를 예시로 나타낸 것입니다.

```
{
  "SchemaVersion": "2018-10-08",
  "Id": "inspector/us-east-1/111122223333/629ff13fbbb44c872f7bba3e7f79f60cb6d443d8",
  "ProductArn": "arn:aws:securityhub:us-east-1::product/aws/inspector",
  "GeneratorId": "arn:aws:inspector:us-east-1:316112463485:rulespackage/0-PmNV0Tcd",
```

```
  "AwsAccountId": "111122223333",
  "Types": [
    "Software and Configuration Checks/AWS Security Best Practices/Network Reachability
 - Recognized port reachable from internet"
  ],
  "CreatedAt": "2020-08-19T17:36:22.169Z",
  "UpdatedAt": "2020-11-04T16:36:06.064Z",
  "Severity": {
    "Label": "MEDIUM",
    "Normalized": 40,
    "Original": "6.0"
  },
  "Confidence": 10,
  "Title": "On instance i-0c10c2c7863d1a356, TCP port 22 which is associated with 'SSH'
 is reachable from the internet",
  "Description": "On this instance, TCP port 22, which is associated with SSH, is
 reachable from the internet. You can install the Inspector agent on this instance
 and re-run the assessment to check for any process listening on this port. The
 instance i-0c10c2c7863d1a356 is located in VPC vpc-a0c2d7c7 and has an attached ENI
 eni-078eac9d6ad9b20d1 which uses network ACL acl-154b8273. The port is reachable from
 the internet through Security Group sg-0af64c8a5eb30ca75 and IGW igw-e209d785",
  "Remediation": {
    "Recommendation": {
      "Text": "You can edit the Security Group sg-0af64c8a5eb30ca75 to remove access
 from the internet on port 22"
    }
  },
  "ProductFields": {
    "attributes/VPC": "vpc-a0c2d7c7",
    "aws/inspector/id": "Recognized port reachable from internet",
    "serviceAttributes/schemaVersion": "1",
    "aws/inspector/arn": "arn:aws:inspector:us-east-1:111122223333:target/0-8zh1cWkg/
template/0-rqtRV0u0/run/0-Ck2F6tY9/finding/0-B458MQWe",
    "attributes/ACL": "acl-154b8273",
    "serviceAttributes/assessmentRunArn": "arn:aws:inspector:us-
east-1:111122223333:target/0-8zh1cWkg/template/0-rqtRV0u0/run/0-Ck2F6tY9",
    "attributes/PROTOCOL": "TCP",
    "attributes/RULE_TYPE": "RecognizedPortNoAgent",
    "aws/inspector/RulesPackageName": "Network Reachability",
    "attributes/INSTANCE_ID": "i-0c10c2c7863d1a356",
    "attributes/PORT_GROUP_NAME": "SSH",
    "attributes/IGW": "igw-e209d785",
    "serviceAttributes/rulesPackageArn": "arn:aws:inspector:us-
east-1:111122223333:rulespackage/0-PmNV0Tcd",
```

```
    "attributes/SECURITY_GROUP": "sg-0af64c8a5eb30ca75",
    "attributes/ENI": "eni-078eac9d6ad9b20d1",
    "attributes/REACHABILITY_TYPE": "Internet",
    "attributes/PORT": "22",
    "aws/securityhub/FindingId": "arn:aws:securityhub:us-east-1::product/aws/inspector/
inspector/us-east-1/111122223333/629ff13fbbb44c872f7bba3e7f79f60cb6d443d8",
    "aws/securityhub/ProductName": "Inspector",
    "aws/securityhub/CompanyName": "Amazon"
  },
  "Resources": [
    {
      "Type": "AwsEc2Instance",
      "Id": "arn:aws:ec2:us-east-1:193043430472:instance/i-0c10c2c7863d1a356",
      "Partition": "aws",
      "Region": "us-east-1",
      "Tags": {
        "Name": "kubectl"
      },
      "Details": {
        "AwsEc2Instance": {
          "ImageId": "ami-02354e95b39ca8dec",
          "IpV4Addresses": [
            "172.31.43.6"
          ],
          "VpcId": "vpc-a0c2d7c7",
          "SubnetId": "subnet-4975b475"
        }
      }
    }
  ],
  "WorkflowState": "NEW",
  "Workflow": {
    "Status": "NEW"
  },
  "RecordState": "ACTIVE"
}
```


통합 활성화 및 구성

Security Hub와의 통합을 사용하려면 Security Hub를 활성화해야 합니다. Security Hub를 활성화하는 방법에 대한 자세한 내용은 AWS Security Hub 사용 설명서의 Security Hub 설정을 참조하세요.

Amazon Inspector와 Security Hub를 둘 다 활성화하면 통합이 자동으로 활성화됩니다. Amazon Inspector가 Security Hub로 조사 결과를 전송하기 시작합니다.

결과 전송을 중지하는 방법

Security Hub로 결과를 전송하는 작업을 중지하려면 Security Hub 콘솔 또는 API를 사용하면 됩니다.

AWS Security Hub 사용 설명서에서 통합에서 결과 흐름 활성화 및 비활성화(콘솔) 또는 통합에서 결과 흐름 비활성화(Security Hub API, AWS CLI)를 참조하세요.

Amazon Inspector Classic ARNs

Amazon Inspector Classic의 각 리소스 유형 및 규칙 패키지에는 고유 Amazon 리소스 이름(ARN)이 연결되어 있습니다.

목차

- Amazon Inspector Classic 리소스용 ARN
- 규칙 패키지용 Amazon Inspector Classic ARN
  - 미국 동부(오하이오)
  - 미국 동부(버지니아 북부)
  - 미국 서부(캘리포니아 북부)
  - 미국 서부(오리건)
  - 아시아 태평양(뭄바이)
  - 아시아 태평양(서울)
  - 아시아 태평양(시드니)
  - 아시아 태평양(도쿄)
  - 유럽(프랑크푸르트)
  - 유럽(아일랜드)
  - 유럽(런던)
  - 유럽(스톡홀름)
  - AWS GovCloud(미국 동부)
  - AWS GovCloud(미국 서부)

Amazon Inspector Classic 리소스용 ARN

Amazon Inspector Classic에서 주 리소스는 리소스 그룹, 평가 대상, 평가 템플릿, 평가 실행 및 결과입니다. 다음 표에서처럼 이러한 리소스에는 고유한 Amazon 리소스 이름(ARN)이 연계됩니다.

리소스 유형	ARN 형식
리소스 그룹	`arn:aws:inspector:` *`region`*`:`*`account-id`* `:resource group/` *`ID`*

리소스 유형	ARN 형식
평가 대상	`arn:aws:inspector:` *region*`:`*account-id* `:target/`*ID*
평가 템플릿	`arn:aws:inspector:` *region*`:`*account-id* `:target/`*ID*`:template:` *ID*
평가 실행	`arn:aws:inspector:` *region*`:`*account-id* `:target/`*ID*`/template/` *ID*`/run/`*ID*
조사 결과	`arn:aws:inspector:` *region*`:`*account-id* `:target/`*ID*`/template/` *ID*`/run/`*ID*`/finding/` *ID*

규칙 패키지용 Amazon Inspector Classic ARN

다음 표는 지원되는 모든 리전에 있는 Amazon Inspector Classic 규칙 패키지에 대한 ARN을 보여 줍니다.

주제

- 미국 동부(오하이오)
- 미국 동부(버지니아 북부)
- 미국 서부(캘리포니아 북부)
- 미국 서부(오리건)
- 아시아 태평양(뭄바이)
- 아시아 태평양(서울)
- 아시아 태평양(시드니)
- 아시아 태평양(도쿄)
- 유럽(프랑크푸르트)
- 유럽(아일랜드)
- 유럽(런던)
- 유럽(스톡홀름)
- AWS GovCloud(미국 동부)
- AWS GovCloud(미국 서부)

미국 동부(오하이오)

규칙 패키지 이름	ARN
CVE(일반적인 취약성 및 노출도)	arn:aws:inspector:us-east-2:646659390643:rulespackage/0-JnA8Zp85
CIS 운영 체제 보안 구성 벤치마크	arn:aws:inspector:us-east-2:646659390643:rulespackage/0-m8r61nnh
네트워크 연결성	arn:aws:inspector:us-east-2:646659390643:rulespackage/0-cE4kTR30
보안 모범 사례	arn:aws:inspector:us-east-2:646659390643:rulespackage/0-AxKmMHPX

미국 동부(버지니아 북부)

규칙 패키지 이름	ARN
CVE(일반적인 취약성 및 노출도)	arn:aws:inspector:us-east-1:316112463485:rulespackage/0-gEjTy7T7
CIS 운영 체제 보안 구성 벤치마크	arn:aws:inspector:us-east-1:31611246

규칙 패키지 이름	ARN
	3485:rulespackage/0-rExsr2X8
네트워크 연결성	arn:aws:inspector:us-east-1:316112463485:rulespackage/0-PmNV0Tcd
보안 모범 사례	arn:aws:inspector:us-east-1:316112463485:rulespackage/0-R01qwB5Q

미국 서부(캘리포니아 북부)

규칙 패키지 이름	ARN
CVE(일반적인 취약성 및 노출도)	arn:aws:inspector:us-west-1:166987590008:rulespackage/0-TKgzoVOa
CIS 운영 체제 보안 구성 벤치마크	arn:aws:inspector:us-west-1:166987590008:rulespackage/0-xUY8iRqX
네트워크 연결성	arn:aws:inspector:us-west-1:166987590008:rulespackage/0-TxmXimXF
보안 모범 사례	arn:aws:inspector:us-west-1:16698759

규칙 패키지 이름	ARN
	0008:rulespackage/0-byoQRFYm

미국 서부(오리건)

규칙 패키지 이름	ARN
CVE(일반적인 취약성 및 노출도)	arn:aws:inspector:us-west-2:758058086616:rulespackage/0-9hgA516p
CIS 운영 체제 보안 구성 벤치마크	arn:aws:inspector:us-west-2:758058086616:rulespackage/0-H5hpSawc
네트워크 연결성	arn:aws:inspector:us-west-2:758058086616:rulespackage/0-rD1z6dpl
보안 모범 사례	arn:aws:inspector:us-west-2:758058086616:rulespackage/0-JJOtZiqQ

아시아 태평양(뭄바이)

규칙 패키지 이름	ARN
CVE(일반적인 취약성 및 노출도)	arn:aws:inspector:ap-south-1:1625887

규칙 패키지 이름	ARN
	57376:rulespackage/0-LqnJE9dO
CIS 운영 체제 보안 구성 벤치마크	arn:aws:inspector:ap-south-1:162588757376:rulespackage/0-PSUlX14m
네트워크 연결성	arn:aws:inspector:ap-south-1:162588757376:rulespackage/0-YxKfjFu1
보안 모범 사례	arn:aws:inspector:ap-south-1:162588757376:rulespackage/0-fs0IZZBj

아시아 태평양(서울)

규칙 패키지 이름	ARN
CVE(일반적인 취약성 및 노출도)	arn:aws:inspector:ap-northeast-2:526946625049:rulespackage/0-PoGHMznc
CIS 운영 체제 보안 구성 벤치마크	arn:aws:inspector:ap-northeast-2:526946625049:rulespackage/0-T9srhg1z
네트워크 연결성	arn:aws:inspector:ap-northeast-2:526

규칙 패키지 이름	ARN
	946625049:rulespackage/0-s3OmLzhL
보안 모범 사례	arn:aws:inspector:ap-northeast-2:526946625049:rulespackage/0-2WRpmi4n

아시아 태평양(시드니)

규칙 패키지 이름	ARN
CVE(일반적인 취약성 및 노출도)	arn:aws:inspector:ap-southeast-2:454640832652:rulespackage/0-D5TGAxiR
CIS 운영 체제 보안 구성 벤치마크	arn:aws:inspector:ap-southeast-2:454640832652:rulespackage/0-Vkd2Vxjq
네트워크 연결성	arn:aws:inspector:ap-southeast-2:454640832652:rulespackage/0-FLcuV4Gz
보안 모범 사례	arn:aws:inspector:ap-southeast-2:454640832652:rulespackage/0-asL6HRgN

아시아 태평양(도쿄)

규칙 패키지 이름	ARN
CVE(일반적인 취약성 및 노출도)	arn:aws:inspector:ap-northeast-1:406045910587:rulespackage/0-gHP9oWNT
CIS 운영 체제 보안 구성 벤치마크	arn:aws:inspector:ap-northeast-1:406045910587:rulespackage/0-7WNjqgGu
네트워크 연결성	arn:aws:inspector:ap-northeast-1:406045910587:rulespackage/0-YI95DVd7
보안 모범 사례	arn:aws:inspector:ap-northeast-1:406045910587:rulespackage/0-bBUQnxMq

유럽(프랑크푸르트)

규칙 패키지 이름	ARN
CVE(일반적인 취약성 및 노출도)	arn:aws:inspector:eu-central-1:537503971621:rulespackage/0-wNqHa8M9
CIS 운영 체제 보안 구성 벤치마크	arn:aws:inspector:eu-central-1:53750

규칙 패키지 이름	ARN
	3971621:rulespackage/0-nZrAVuv8
네트워크 연결성	arn:aws:inspector:eu-central-1:537503971621:rulespackage/0-6yunpJ91
보안 모범 사례	arn:aws:inspector:eu-central-1:537503971621:rulespackage/0-ZujVHEPB

유럽(아일랜드)

규칙 패키지 이름	ARN
CVE(일반적인 취약성 및 노출도)	arn:aws:inspector:eu-west-1:357557129151:rulespackage/0-ubA5XvBh
CIS 운영 체제 보안 구성 벤치마크	arn:aws:inspector:eu-west-1:357557129151:rulespackage/0-sJBhCr0F
네트워크 연결성	arn:aws:inspector:eu-west-1:357557129151:rulespackage/0-SPzU33xe
보안 모범 사례	arn:aws:inspector:eu-west-1:35755712

규칙 패키지 이름	ARN
	9151:rulespackage/0-SnojL3Z6

유럽(런던)

규칙 패키지 이름	ARN
CVE(일반적인 취약성 및 노출도)	arn:aws:inspector:eu-west-2:146838936955:rulespackage/0-kZGCqcE1
CIS 운영 체제 보안 구성 벤치마크	arn:aws:inspector:eu-west-2:146838936955:rulespackage/0-IeCjwf1W
네트워크 연결성	arn:aws:inspector:eu-west-2:146838936955:rulespackage/0-AizSYyNq
보안 모범 사례	arn:aws:inspector:eu-west-2:146838936955:rulespackage/0-XApUiSaP

유럽(스톡홀름)

규칙 패키지 이름	ARN
CVE(일반적인 취약성 및 노출도)	arn:aws:inspector:eu-north-1:4534202

규칙 패키지 이름	ARN
	44670:rulespackage/0-IgdgIewd
CIS 운영 체제 보안 구성 벤치마크	arn:aws:inspector:eu-north-1:453420244670:rulespackage/0-Yn8jlX7f
네트워크 연결성	arn:aws:inspector:eu-north-1:453420244670:rulespackage/0-52Sn74uu
보안 모범 사례	arn:aws:inspector:eu-north-1:453420244670:rulespackage/0-HfBQSbSf

AWS GovCloud(미국 동부)

규칙 패키지 이름	ARN
CVE(일반적인 취약성 및 노출도)	arn:aws-us-gov:inspector:us-gov-east-1:206278770380:rulespackage/0-3IFKFuOb
CIS 운영 체제 보안 구성 벤치마크	arn:aws-us-gov:inspector:us-gov-east-1:206278770380:rulespackage/0-pTLCdIww

규칙 패키지 이름	ARN
보안 모범 사례	arn:aws-us-gov:inspector:us-gov-east-1:206278770380:rulespackage/0-vlgEGcVD

AWS GovCloud(미국 서부)

규칙 패키지 이름	ARN
CVE(일반적인 취약성 및 노출도)	arn:aws-us-gov:inspector:us-gov-west-1:850862329162:rulespackage/0-4oQgcI4G
CIS 운영 체제 보안 구성 벤치마크	arn:aws-us-gov:inspector:us-gov-west-1:850862329162:rulespackage/0-Ac4CFOuc
보안 모범 사례	arn:aws-us-gov:inspector:us-gov-west-1:850862329162:rulespackage/0-rOTGqe5G

문서 기록

다음 표는 2018년 5월 이후 Amazon Inspector Classic의 문서 릴리스 기록에 대해 설명합니다.

변경 사항	설명	날짜
지원 종료 알림	지원 종료 알림: 2026년 5월 20일에 Amazon Inspector Classic에 대한 지원이 AWS 종료됩니다. 2026년 5월 20일 이후에는 Amazon Inspector Classic 콘솔 또는 Amazon Inspector Classic 리소스에 더 이상 액세스할 수 없습니다. 자세한 내용은 Amazon Inspector Classic 지원 종료를 참조하세요.	2025년 5월 20일
비밀번호에 대한 보안 모범 사례 업데이트됨	EC2 인스턴스 비밀번호 길이 및 비밀번호 복잡성에 대한 Amazon Inspector Classic 보안 모범 사례 요구 사항이 업데이트되었습니다. 비밀번호 최소 길이 구성 및 비밀번호 복잡성 구성을 참고하십시오.	2021년 3월 8일
최신 운영 체제 버전에 대한 지원 추가됨	Amazon Inspector Classic은 이제 Ubuntu 20.4 LTS, Debian 10.x, RHEL 8.x 및 Windows Server 2019 Base 운영 체제 버전을 지원합니다.	2020년 10월 15일
새로운 보안 장으로 통합된 보안 정보	자격 증명 및 액세스 관리의 관리 정보를 비롯한 Amazon Inspector Classic 보안 정보가 보안 장으로 통합됩니다.	2020년 4월 7일

	Amazon Inspector Classic에서의 보안을 참고하십시오.	
실행 시간 동작 분석 규칙 패키지에 대한 지원이 제거되어 문서가 업데이트되었습니다.	더 이상 지원되지 않는 실행 시간 동작 분석 규칙 패키지에 대한 정보가 제거되어 여러 주제가 업데이트되었습니다.	2019년 9월 5일
추가된 OS 지원	CentOS 7.6에 대한 Amazon Inspector Classic 지원 추가됨 자세한 내용은 Amazon Inspector Classic 지원 운영 체제 및 리전 및 지원되는 운영 체제의 규칙 패키지 가용성을 참조하십시오.	2018년 12월 3일
새로운 내용	Amazon Inspector Classic 네트워크 연결성 규칙 패키지가 추가되어 사용자가 에이전트 없이 보안 취약성에 대한 네트워크 구성을 분석하는 평가를 실행할 수 있습니다. 자세한 내용은 Network Reachability 단원을 참조하십시오.	2018년 11월 9일
추가된 OS 지원	RHEL 7.6에 대한 Amazon Inspector Classic 지원 추가됨 자세한 내용은 Amazon Inspector Classic 지원 운영 체제 및 리전 및 지원되는 운영 체제의 규칙 패키지 가용성을 참조하십시오.	2018년 10월 30일

추가된 OS 지원	CIS Benchmark 규칙 페이지에서 다양한 운영 체제를 실행하는 데에 대한 추가된 지원입니다. 자세한 내용은 Center for Internet Security(CIS) Benchmarks와 Rules Packages Availability Across Supported Operating Systems를 참조하십시오.	2018년 8월 13일
리전 지원 추가	AWS GovCloud (US)에 대한 리전 지원이 추가되었습니다.	2018년 13월 6일

다음 표는 2018년 6월 이전 Amazon Inspector Classic의 문서 릴리스 기록에 대해 설명합니다.

변경 사항	설명	날짜
새로운 내용	계정의 모든 Amazon EC2 인스턴스를 대상으로 할 수 있는 기능이 추가되었습니다. 자세한 내용은 Amazon Inspector Classic 평가 대상 단원을 참조하십시오.	2018년 5월 24일
추가된 OS 지원	Amazon Linux 2018.03 및 Ubuntu 18.04에 대한 Amazon Inspector Classic 지원 추가됨	2018년 5월 15일
새로운 내용	반복적인 Amazon Inspector Classic 평가를 설정하는 기능이 추가되었습니다.	2018년 4월 30일
새로운 내용	콘솔을 통해 Amazon Inspector Classic 에이전트를 설치할 수 있는 기능이 추가되었습니다.	2018년 4월 30일

변경 사항	설명	날짜
추가된 OS 지원	Amazon Linux 2에 대한 Amazon Inspector Classic 지원 추가됨	2018년 3월 13일
추가된 OS 지원	Windows Server 2016 Base에 대한 Amazon Inspector Classic 평가 지원이 추가되었습니다.	2018년 2월 20일
리전 지원 추가	`US East (Ohio)` 리전에 대한 Amazon Inspector Classic 지원 추가됨	2018년 2월 7일
새로운 내용	이제 커널 모듈을 사용할 수 없을 때 Amazon Inspector Classic 평가가 실행될 수 있습니다.	2018년 1월 11일
리전 지원 추가	`EU (Frankfurt)` 리전에 대한 Amazon Inspector Classic 지원 추가됨	2017년 12월 19일
새로운 내용	Amazon Inspector Classic API 및 콘솔을 사용하여 Amazon Inspector Classic 에이전트 상태를 확인하는 기능 추가됨	2017년 12월 15일
새로운 내용	다음 기능을 추가했습니다. • 서비스 연결 역할 사용 • AWS Marketplace에서 Amazon Inspector Classic 에이전트 AMI 사용 가능 • Amazon Inspector Classic AWS CloudFormation 템플릿	2017년 12월 5일

변경 사항	설명	날짜
추가된 OS 지원	CentOS 7.4에 대한 Amazon Inspector Classic 평가 지원 추가됨	2017년 11월 9일
추가된 OS 지원	Amazon Linux 2017.09에 대한 Amazon Inspector Classic 평가 지원 추가됨	2017년 10월 11일
추가된 OS 지원	RHEL 7.4에 대한 Amazon Inspector Classic 평가 지원 추가됨	2018년 2월 20일
추가된 HIPAA 자격	Amazon Inspector Classic은 이제 HIPAA 자격을 획득했습니다.	2017년 7월 31일
새로운 내용	Amazon CloudWatch Events를 사용하여 자동으로 Amazon Inspector Classic 보안 평가를 트리거할 수 있는 기능이 추가되었습니다.	2017년 7월 27일
리전 지원 추가	`US West (N. California)` 리전에 대한 Amazon Inspector Classic 지원 추가됨	2018년 6월 6일
추가된 OS 지원	RHEL 6.2-6.9, RHEL 7.2-7.3, CentOS 6.9 및 CentOS 7.2-7.3에 대해 Amazon Inspector Classic 평가 지원이 추가되었습니다.	2017년 5월 23일
추가된 OS 지원	Amazon Linux 2017.03에 대한 Amazon Inspector Classic 평가 지원 추가됨	2017년 4월 25일

변경 사항	설명	날짜
새로운 콘텐츠 및 추가된 OS 지원	추가된 내용: • Ubuntu 16.04에 대한 Amazon Inspector Classic 지원 • Amazon Inspector Classic 작업 자동화를 위한 Lambda 청사진의 가용성입니다.	2017년 1월 5일
새로운 OS 지원	Microsoft Windows에 대한 Amazon Inspector Classic 지원 추가됨	2016년 8월 26일
리전 지원 추가	`Asia Pacific (Seoul)` 리전에 대한 Amazon Inspector Classic 지원 추가됨	2016년 8월 26일
리전 지원 추가	`Asia Pacific (Mumbai)` 리전에 대한 Amazon Inspector Classic 지원 추가됨	2016년 4월 25일
리전 지원 추가	`Asia Pacific (Sydney)` 리전에 대한 Amazon Inspector Classic 지원 추가됨	2016년 4월 25일
서비스 시작	Amazon Inspector Classic 서비스가 시작되었습니다.	2015년 10월 7일

AWS 용어집

최신 AWS 용어는 AWS 용어집 참조의 AWS 용어집을 참조하세요.