Amazon Inspector

사용 설명서

버전 Latest

Amazon Inspector: 사용 설명서

Table of Contents

Amazon Inspector란 무엇입니까?

Amazon Inspector는 Amazon EC2 instances의 네트워크 액세스 가능성 및 해당 인스턴스에서 실행되는 애플리케이션의 보안 상태를 테스트합니다. Amazon Inspector는 노출, 취약성 및 모범 사례에서 벗어난 애플리케이션을 평가합니다. 평가를 수행한 후, Amazon Inspector는 상세한 보안 평가 결과 목록을 제공하며, 이 목록은 심각도 수준에 따라 구성되어 있습니다.

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

> **Important**
>
> AWS는 제공된 권장 사항으로 모든 잠재적 보안 문제가 해결됨을 보장하지 않습니다. Amazon Inspector에서 생성한 결과는 각 평가 템플릿에 포함된 규칙 패키지, 시스템에 AWS가 아닌 구성 요소가 있는지 여부 및 기타 요소에 따라 다릅니다. AWS 서비스에서 실행되는 애플리케이션, 프로세스 및 도구의 보안에 대한 책임은 사용자에게 있습니다. 자세한 내용은 보안의 AWS 공동 책임 모델을 참조하십시오.
>
> **Note**
>
> AWS는 AWS 클라우드에 제공된 서비스를 실행하는 글로벌 인프라를 보호해야 합니다. 이 인프라는 AWS 서비스를 실행하는 하드웨어, 소프트웨어, 네트워킹, 시설로 구성됩니다. AWS는 다양한 컴퓨터 보안 표준 및 규정을 준수하는지 확인한 타사 감사자의 여러 보고서를 제공합니다. 자세한 내용은 AWS 클라우드 규정 준수를 참조하십시오.

Amazon Inspector 용어에 대한 자세한 내용은 Amazon Inspector 용어 및 개념 (p. 2) 단원을 참조하십시오.

Amazon Inspector의 이점

Amazon Inspector의 주요 장점은 다음과 같습니다.

- 정기적인 배포 및 프로덕션 프로세스에 자동화된 보안 검사 통합 – 과학수사, 문제 해결 또는 능동적인 감사 목적을 위해 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 더 깊은 이해 – Amazon Inspector가 생성한 결과를 검토하여 AWS 리소스의 활동 및 구성 데이터에 대한 정보를 지속적으로 얻을 수 있습니다.

Amazon Inspector의 기능

Amazon Inspector에서 제공하는 주요 기능 몇 가지는 다음과 같습니다.

- 구성 검색 및 활동 모니터링 엔진 – Amazon Inspector는 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 Inspector는 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 Inspector는 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 요금

Amazon Inspector 요금은 각 평가에 포함된 EC2 인스턴스 수와 해당 평가에 사용된 규칙 패키지를 기반으로 합니다. Amazon Inspector 요금에 대한 자세한 내용은 Amazon Inspector 요금을 참조하십시오.

Amazon Inspector에 액세스

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

Amazon Inspector 콘솔

Sign in to the AWS Management 콘솔 and open the Amazon Inspector console at https://console.aws.amazon.com/inspector/.

콘솔은 Amazon Inspector 서비스를 액세스 및 사용하는 브라우저 기반 인터페이스입니다.

AWS SDK

AWS에서는 다양한 프로그래밍 언어 및 플랫폼을 위한 라이브러리와 샘플 코드로 구성된 소프트웨어 개발 키트(SDK)를 제공합니다. 여기에는 Java, Python, Ruby, .NET, iOS, Android 등이 포함됩니다. SDK를 사용하면 편리하게 Amazon Inspector에 프로그래밍 방식으로 액세스할 수 있습니다. 다운로드 및 설치 방법을 비롯하여 AWS SDK에 대한 자세한 내용은 Amazon Web Services용 도구를 참조하십시오.

Amazon Inspector HTTPS API

서비스로 직접 HTTPS 요청을 실행할 수 있는 Amazon Inspector HTTPS API를 사용하여 프로그래밍 방식으로 Amazon Inspector 및 AWS에 액세스할 수 있습니다. 자세한 내용은 Amazon Inspector API 참조를 참조하십시오.

AWS 명령줄 도구

AWS 명령줄 도구를 통해 시스템 명령줄에서 명령을 실행하여 Amazon Inspector 작업을 수행할 수 있습니다. AWS 작업을 수행하는 스크립트를 작성할 때도 명령줄 도구가 유용합니다. 자세한 내용은 Amazon Inspector AWS 명령줄 인터페이스를 참조하십시오.

Amazon Inspector 용어 및 개념

Amazon Inspector를 시작할 때 핵심 개념을 알아두면 유익합니다.

Amazon Inspector 에이전트

평가 대상에 포함되어 있는 Amazon EC2 instances에 설치할 수 있는 소프트웨어 에이전트입니다. 에이전트는 네트워크, 파일 시스템 및 프로세스 활동을 포함한 EC2 instances의 동작을 모니터링합니다. 또한 광범위한 동작 및 구성 데이터를 수집합니다(원격 측정). 자세한 내용은 Amazon Inspector 에이전트 (p. 20)를 참조하십시오.

평가 실행

평가 대상의 구성 및 동작을 지정된 규칙 패키지에 대해 분석하여 잠재적 보안 문제를 발견하는 프로세스입니다. 평가 실행 중에 Amazon Inspector는 지정된 대상 내 동작 데이터(원격 측정)를 모니터링, 수집

및 분석합니다. 여기에는 보안 채널 사용, 실행 중인 프로세스 간의 네트워크 트래픽 및 AWS 서비스와의 통신 세부 정보가 포함됩니다. 그런 다음 Amazon Inspector는 데이터를 분석하고 이를 평가 실행 중에 사용된 평가 템플릿에 지정된 보안 규칙 패키지 세트와 비교합니다. 완료된 평가 실행에서 결과(다양한 심각도의 잠재적 보안 문제) 목록을 생성합니다. 자세한 내용은 Amazon Inspector 평가 템플릿 및 평가 실행 (p. 50)를 참조하십시오.

평가 대상

Amazon Inspector의 컨텍스트에서는 비즈니스 목표를 달성할 수 있게 도와 주는 한 단위로 함께 작동하는 AWS 리소스 모음입니다. Amazon Inspector는 평가 대상을 지속할 수 있는 리소스 보안 상태를 평가합니다.

Important

현재 Amazon Inspector 평가 대상은 EC2 인스턴스만으로 구성될 수 있습니다. 자세한 내용은 Amazon Inspector 서비스 제한 (p. 3) 단원을 참조하십시오.

Amazon Inspector 평가 대상을 생성하려면 먼저 EC2 instances를 선택한 키-값 페어로 태그 지정합니다. 그런 다음 공통 키 또는 공통 값을 갖는 태그가 지정된 EC2 instances의 보기를 생성할 수 있습니다. 자세한 내용은 Amazon Inspector 평가 대상 (p. 34)를 참조하십시오.

평가 템플릿

평가 실행 중에 사용되는 구성. 템플릿에는 다음 사항이 포함됩니다.

- Amazon Inspector가 평가 대상을 평가하기 위해 사용하는 규칙 패키지
- Amazon Inspector가 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

결과

지정된 대상의 평가 실행 중에 Amazon Inspector가 발견한 잠재적인 보안 문제입니다. 결과는 Amazon Inspector 콘솔에 표시되거나 API를 통해 검색됩니다. 여기에는 보안 문제에 대한 자세한 설명과 이를 수정하는 방법에 대한 권장 사항이 모두 포함되어 있습니다. 자세한 내용은 Amazon Inspector 결과 (p. 56)를 참조하십시오.

규칙

Amazon Inspector의 컨텍스트에서 평가 실행 중에 수행되는 보안 검사입니다. 규칙에서 잠재적인 보안 문제를 발견하면 Amazon Inspector는 문제를 설명하는 결과를 생성합니다.

규칙 패키지

Amazon Inspector의 컨텍스트에서 규칙 모음입니다. 규칙 패키지는 사용자가 설정할 수 있는 보안 목표에 해당합니다. Amazon Inspector 평가 템플릿을 작성할 때 해당하는 규칙 패키지를 선택하여 보안 목표를 지정할 수 있습니다. 자세한 내용은 Amazon Inspector 규칙 패키지 및 규칙 (p. 37)를 참조하십시오.

원격 측정

네트워크 연결 및 프로세스 생성 기록과 같은 EC2 인스턴스 데이터(동작, 구성 등). Amazon Inspector는 평가 실행 중에 데이터를 수집합니다.

Amazon Inspector 서비스 제한

다음 표에는 AWS 계정의 Amazon Inspector 제한이 나와 있습니다.

Important

현재 평가 대상은 EC2 인스턴스만으로 구성될 수 있습니다.

다음은 리전별로 AWS 계정당 Amazon Inspector 제한입니다.

리소스	기본 한도	의견
평가를 실행하는 인스턴스	500	리전별로 계정당 실행 중인 모든 평가에 포함될 수 있는 EC2 instances의 최대 수입니다.
평가 실행	50000	리전별로 계정당 생성할 수 있는 평가 실행의 최대 수입니다. 이 실행에 사용된 평가 대상에 중복되는 EC2 instances가 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 Center에 문의하여 요청 시 높일 수 있습니다.

Amazon Inspector 지원 운영 체제 및 리전

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

> **Important**
>
> 현재 Amazon Inspector 평가 대상은 EC2 인스턴스만으로 구성될 수 있습니다. 운영 체제와 상관없이 모든 EC2 instances에서 네트워크 연결성 (p. 38) 규칙 패키지를 사용하여 에이전트 없는 평가를 실행할 수 있습니다.

지원되는 운영 체제에서 사용할 수 있는 Amazon Inspector 규칙 패키지에 대한 자세한 내용은 지원되는 운영 체제의 Amazon Inspector 규칙 패키지 (p. 65) 단원을 참조하십시오.

주제

- Amazon Inspector 에이전트에 대해 지원되는 Linux 기반 운영 체제 (p. 4)
- Amazon Inspector 에이전트에 대해 지원되는 Windows 기반 운영 체제 (p. 5)
- 지원되는 AWS 리전 (p. 5)

Amazon Inspector 에이전트에 대해 지원되는 Linux 기반 운영 체제

다음 Linux 기반 운영 체제의 64비트 x86 및 Arm 버전을 실행하는 EC2 인스턴스에서 Amazon Inspector 에이전트를 사용할 수 있습니다.

- Amazon Linux 2(LTS, 2017.12)
- 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(18.04 LTS, 16.04 LTS, 14.04 LTS)
- Debian(9.0 - 9.5, 8.0 - 8.7)
- Red Hat Enterprise Linux(7.2 - 7.6, 6.2 - 6.9)
- CentOS(7.2 - 7.6, 6.2 - 6.9)

Important

다음 목록에는 Linux, Ubuntu, Red Hat Enterprise Linux 및 CentOS에서 실행되는 Amazon Inspector 에이전트와 호환 가능한 모든 커널 버전이 포함되어 있습니다. https://s3.amazonaws.com/aws-agent.us-east-1/linux/support/supported_versions.json Linux 기반 OS에서 CVE (p. 40), CIS (p. 41) 또는 보안 모범 사례 (p. 46) 규칙 패키지를 사용하면 EC2 인스턴스에 대한 평가를 실행할 수 있습니다. 인스턴스에 목록에 포함된 커널 버전이 없는 경우에도 평가가 성공적으로 실행됩니다.
실행 시간 행동 분석 (p. 43) 규칙 패키지를 사용하여 Linux 기반 OS가 설치된 EC2 인스턴스의 성공적인 Amazon Inspector 평가를 실행하려면 인스턴스에 이 목록에 포함된 커널 버전이 있어야 합니다. 인스턴스에 에이전트와 호환되지 않는 커널 버전이 있는 경우 실행 시간 동작 분석 규칙 패키지가 하나의 EC2 인스턴스 결과만 평가합니다. 해당 결과는 EC2 인스턴스의 커널 버전이 지원되지 않음을 알려 줍니다.

Amazon Inspector 에이전트에 대해 지원되는 Windows 기반 운영 체제

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

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

지원되는 AWS 리전

Amazon Inspector는 다음 AWS 리전에서 지원됩니다.

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

- AWS GovCloud(US-East)
- AWS GovCloud (US-West)

Note

네트워크 연결성 (p. 38) 규칙 패키지는 AWS GovCloud(US) 리전에서 사용할 수 없습니다.

Amazon Inspector 시작하기

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

Important

Amazon Inspector를 사용하려면 AWS 계정이 있어야 합니다. AWS에 가입하면 Amazon Inspector를 포함한 AWS의 모든 서비스에 계정이 자동으로 등록됩니다. AWS 계정이 없는 경우에는 아래 단계를 수행하여 계정을 만드십시오.

AWS에 가입하려면

1. https://portal.aws.amazon.com/billing/signup을 엽니다.
2. 온라인 지시 사항을 따릅니다.

   등록 절차 중 전화를 받고 전화 키패드를 사용하여 확인 코드를 입력하는 과정이 있습니다.

주제

Amazon Inspector 사용을 위한 사전 조건

Amazon Inspector 콘솔을 처음 시작하는 경우, Get Started를 선택하고 다음 사전 필수 작업을 수행합니다. Amazon Inspector 평가 실행을 실행하기 전에 다음 작업을 완료해야 합니다.

- AWS 환경에서 적어도 하나의 Amazon EC2 인스턴스가 있어야만 Amazon Inspector 평가를 실행할 수 있습니다. EC2 인스턴스 시작에 대한 내용은 Amazon Elastic Compute Cloud 설명서를 참조하십시오.
- 대부분의 경우 Amazon Inspector 에이전트는 평가 대상의 각 EC2 instance에서 실행되어야 합니다. 에이전트 설치에 대한 자세한 내용은 Amazon Inspector 에이전트 설치 (p. 22) 단원을 참조하십시오. 또는 Systems Manager Run Command를 사용하여 Amazon EC2 인스턴스에 에이전트를 설치할 수 있습니다. Amazon Inspector 에이전트에 대한 자세한 내용은 Amazon Inspector 에이전트 (p. 20) 단원을 참조하십시오.

원클릭 설치

다음 절차는 사전 빌드된 템플릿과 사전 정의된 일정 파라미터(주 1회 또는 한 번)를 최근 AWS 계정 및 리전에서 사용 가능한 모든 EC2 인스턴스를 사용하여 자동 평가가 생성되고 실행하는 방법에 대해 보여줍니다.

1. Sign in to the AWS Management 콘솔 and open the Amazon Inspector console at https://console.aws.amazon.com/inspector/.
2. 시작 페이지에서 실행할 평가 유형을 선택합니다. Network Assessments(네트워크 평가)는 AWS 환경의 네트워크 구성에 대한 취약성을 분석하며 Amazon Inspector 에이전트가 필요하지 않습니다. Host Assessments(호스트 평가)는 호스트상의 소프트웨어 및 EC2 instances 구성의 취약성을 분석하며 EC2 instances에 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 역할 (p. 17)을 만들려면

   Note

   Amazon Inspector는 평가 대상에 EC2 인스턴스를 식별할 수 있도록 EC2 인스턴스와 태그를 열거할 필요가 있습니다. Amazon Inspector는 `AWSServiceRoleForAmazonInspector`라는 서비스 연결 역할을 통해 AWS 계정의 이러한 리소스로 액세스할 수 있습니다. 서비스 연결 역할에 대한 자세한 내용은 Amazon Inspector에 서비스 연결 역할 사용 (p. 17) 및 서비스 연결 역할 사용 단원을 참조하십시오.

b. 해당되는 경우 Amazon Inspector 에이전트 (p. 20)를 AWS 계정 및 AWS 리전에 사용 가능한 모든 Amazon EC2 인스턴스에 설치합니다.

   Note

   이 서비스는 AWS Systems Manager Run Command를 허용하는 이러한 EC2 instances에만 Amazon Inspector 에이전트를 설치할 수 있습니다. 이 옵션을 이용하려면 현재 AWS 계정 및 AWS 리전의 모든 EC2 인스턴스에 SSM 에이전트가 설치되어 있고, Run Command를 허용하는 IAM 역할이 지정되어 있어야 합니다. 자세한 내용은 Systems Manager Run Command를 사용하여 여러 EC2 인스턴스에 에이전트 설치 (p. 23) 단원을 참조하십시오.

c. 평가 대상 (p. 34)에 이러한 인스턴스를 추가합니다.

d. 평가 템플릿 (p. 50)에 표준화된 규칙 패키지로 대상을 추가합니다.

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

3. Confirmation 대화 상자에서 OK를 선택합니다. Amazon Inspector은 자동으로 평가를 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 인스턴스에서 확인란을 선택하여 모든 EC2 instances를 평가 대상의 AWS 계정과 리전에 포함되게 하십시오. 추가할 EC2 instances를 선택하고자 한다면 모든 인스턴스 확인란 선택을 해제하고 대상 EC2 instances과 관련된 키 및 값 태그를 입력합니다. EC2 인스턴스 태그에 대한 자세한 내용은 Amazon EC2 리소스에 태그 지정을 참조하십시오.
4. 에이전트 설치의 경우, 인스턴스가 System Manager Run Command를 허용한다면 기본적으로 확인란을 선택한 상태로 유지할 수 있습니다. 이 서비스는 Systems Manager Run Command를 허용하는 모든 EC2 instances에 Amazon Inspector 에이전트를 설치할 수 있습니다. 이 옵션을 이용하려면 현재 AWS 계정 및 AWS 리전의 모든 EC2 인스턴스에 SSM 에이전트가 설치되어 있고, Run Command를 허용하는 IAM 역할이 지정되어 있어야 합니다. 자세한 내용은 Systems Manager Run Command를 사용하여 여러 EC2 인스턴스에 에이전트 설치 (p. 23) 단원을 참조하십시오. 수동으로 에이전트를 설치하고자 한다면 Installing Amazon Inspector Agents (p. 22)를 참조하십시오.
5. [Next]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 Rules (p. 37)를 참조하십시오.
8. Duration에서 평가 템플릿 실행 기간을 선택합니다.

9. Assessment Schedule에서 반복 평가 실행 일정을 설정할 수 있습니다.
10. [Next]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

    Amazon Inspector는 평가 대상에 EC2 인스턴스를 식별할 수 있도록 EC2 인스턴스와 태그를 열거할 필요가 있습니다. Amazon Inspector는 `AWSServiceRoleForAmazonInspector`라는 서비스 연결 역할을 통해 AWS 계정의 이러한 리소스로 액세스할 수 있습니다. 서비스 연결 역할에 대한 자세한 내용은 Amazon Inspector에 서비스 연결 역할 사용 (p. 17) 및 서비스 연결 역할 사용 단원을 참조하십시오.
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 결과 (p. 56)을 참조하십시오.

Amazon Inspector에 관한 자습서

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

자습서

- 자습서: Red Hat Enterprise Linux와 함께 Amazon Inspector를 사용하기 (p. 10)
- 자습서: Amazon Inspector와 함께 Ubuntu Server 사용 (p. 13)

Amazon Inspector 자습서 - Red Hat Enterprise Linux

이 자습서의 지침을 따르기 전에 Amazon Inspector 용어 및 개념 (p. 2)에 익숙해지는 것이 좋습니다.

이 자습서는 Amazon Inspector를 사용하여 Red Hat Enterprise Linux 7.5 운영 체제를 실행하는 EC2 instance의 동작을 분석하는 방법을 보여줍니다. Amazon Inspector 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 평가를 설계하고 실행하고자 한다면 Creating a Basic Assessment (p. 7)를 참조하십시오.

주제

- 1단계: Amazon Inspector를 이용한 Amazon EC2 인스턴스를 설치합니다. (p. 10)
- 2단계: Amazon EC2 인스턴스 수정 (p. 10)
- 3단계: 평가 대상을 생성하고 EC2 인스턴스에 에이전트를 설치합니다. (p. 11)
- 4단계: 평가 템플릿 생성 및 실행 (p. 11)
- 5단계: 생성된 결과 찾기 및 분석 (p. 12)
- 6단계: 권장 수정 사항을 평가 대상에 적용 (p. 12)

1단계: Amazon Inspector를 이용한 Amazon EC2 인스턴스를 설치합니다.

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

> Note
>
> EC2 instances의 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 instance을 수정합니다. 자세한 내용은 https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-1111와 CVE(일반적인 취약성 및 노출도) (p. 40)를 참조하십시오.

`InspectorEC2InstanceLinux` 인스턴스에 연결하고 다음 명령을 실행합니다.

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

EC2 instance에 연결하는 방법에 대한 지시 사항은 Amazon EC2 사용 설명서에서 Connect to Your Instance를 참조하십시오.

3단계: 평가 대상을 생성하고 EC2 인스턴스에 에이전트를 설치합니다.

Amazon Inspector가 평가 대상을 사용하여 평가하고자하는 AWS 리소스를 설계합니다.

평가 대상을 생성하고 EC2 인스턴스에 에이전트를 설치하려면

1. Sign in to the AWS Management 콘솔 and open the Amazon Inspector console at https://console.aws.amazon.com/inspector/.
2. 탐색 창에서 Assessment targets(평가 대상)를 선택한 후 Create(생성)를 선택합니다.

   다음을 수행합니다.

   a. Name에 평가 대상의 이름을 입력합니다.

      본 자습서에서는 **`MyTargetLinux`**를 입력합니다.

   b. Use Tags에서는 키 및 값 필드에 값을 입력하여 이 평가 대상에 포함할 EC2 instances를 선택합니다.

      이 자습서에서는 Key 필드에 **`Name`**을 Value 필드에 **`InspectorEC2InstanceLinux`**을 입력하여 이전 단계에서 생성한 EC2 인스턴스를 선택합니다.

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

   c. 저장을 선택합니다.

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

      Note

      AWS Systems Manager Run Command (p. 23)를 사용하여 Amazon Inspector 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 에이전트를 설치할 수 있습니다. 자세한 내용은 Amazon Inspector 에이전트 설치 (p. 22)를 참조하십시오.

   e. 저장을 선택합니다.

   Note

   이 시점에서 Amazon Inspector는 `AWSServiceRoleForAmazonInspector`라는 서비스 연결 역할을 생성합니다. 이 역할은 Amazon Inspector에 리소스에 대해 필요한 액세스 권한을 부여합니다. 자세한 내용은 Amazon Inspector에 대한 서비스 연결 역할 생성 (p. 17)를 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. Name 평가 템플릿의 이름을 입력합니다. 본 자습서에서는 **`MyFirstTemplateLinux`**를 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: 생성된 결과 찾기 및 분석

평가 실행이 완료되면 결과 세트 또는 Amazon Inspector가 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 Findings를 선택합니다.

   Instance InspectorEC2InstanceLinux is vulnerable to CVE-2018-1111(Instance InspectorEC2InstanceLinux가 CVE-2018-1111에 취약함)이라는 높음 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 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 단원에서 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: 생성된 결과 찾기 및 분석 (p. 12)의 단계를 수행하여 MyFirstTemplateLinux 템플릿의 후속 실행 결과를 확인합니다.

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

Amazon Inspector 자습서 - Ubuntu Server

이 자습서의 지침을 따르기 전에 Amazon Inspector 용어 및 개념 (p. 2)에 익숙해지는 것이 좋습니다.

이 자습서는 Amazon Inspector를 사용하여 Ubuntu Server 16.04 LTS 운영 체제를 실행하는 EC2 instance의 동작을 분석하는 방법을 보여 줍니다. Amazon Inspector 워크플로 탐색 방법에 대한 단계별 지침을 제공합니다. 여기에는 Amazon EC2 인스턴스 준비, 평가 템플릿 실행 및 평가 결과에서 도출된 권장 보안 해결책 실천이 포함됩니다.

최초 사용자이고 한 번의 클릭으로 Amazon Inspector 평가를 설계하고 실행하고자 한다면 Creating a Basic Assessment (p. 7)를 참조하십시오.

주제

1단계: Amazon Inspector를 이용한 Amazon EC2 인스턴스를 설치합니다.

EC2 인스턴스를 설정하려면

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

  Note

  EC2 instances의 태그 지정에 대한 자세한 내용은 리소스 및 태그를 참조하십시오.

2단계: Amazon EC2 인스턴스 수정

이 자습서에서는 잠재적 보안 문제 CVE-2017-1111에 노출되도록 대상 EC2 instance을 수정합니다. 자세한 내용은 https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-6507와 CVE(일반적인 취약성 및 노출도) (p. 40)를 참조하십시오.

EC2 인스턴스를 수정하려면

- 이전 단원에서 생성한 **InspectorEC2InstanceUbuntu** 인스턴스에 연결하고 다음 명령을 실행합니다.

```
sudo apt-get install apparmor=2.10.95-0ubuntu2.5
```

3단계: 평가 대상을 생성하고 EC2 인스턴스에 에이전트를 설치합니다.

Amazon Inspector가 평가 대상을 사용하여 평가하고자하는 AWS 리소스를 설계합니다.

평가 대상을 생성하고 EC2 instance에 에이전트를 설치하려면

1. Sign in to the AWS Management 콘솔 and open the Amazon Inspector console at https://console.aws.amazon.com/inspector/.
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. Use Tags에서는 키 및 값 필드에 값을 입력하여 이 평가 대상에 포함할 EC2 instances를 선택합니다.

   이 자습서에서는 Key 필드에 **Name**을 Value 필드에 **InspectorEC2InstanceUbuntu**을 입력하여 이전 단계에서 생성한 EC2 인스턴스를 선택합니다.

   모든 인스턴스 확인란을 선택하여 평가 대상의 AWS 계정과 리전이 모든 EC2 인스턴스에 포함되게 하십시오.
5. 태그가 지정된 EC2 인스턴스에 Amazon Inspector 에이전트를 설치합니다. 평가 대상에 포함된 EC2 인스턴스에 에이전트를 설치하려면 Install Agents 확인란을 선택하십시오.

   Note

   Systems Manager Run Command (p. 23)를 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 에이전트 설치 (p. 22) 단원을 참조하십시오.
6. 저장을 선택합니다.

   Note

   이때 `AWSServiceRoleForAmazonInspector`라는 서비스 연결 역할이 생성되어 Amazon Inspector에 리소스에 대한 액세스 권한을 부여합니다. 자세한 내용은 Amazon Inspector에 대한 서비스 연결 역할 생성 (p. 17) 단원을 참조하십시오.

4단계: 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. 본 자습서에서는 **MyFirstTemplateUbuntu**를 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.

5단계: 생성된 결과 찾기 및 분석

평가 실행이 완료되면 결과 세트 또는 Amazon Inspector가 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-2017-6507에 대한 결과를 생성합니다.

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.

   Instance InspectorEC2InstanceUbuntu is vulnerable to CVE-2017-6507(Instance InspectorEC2InstanceUbuntu가 CVE-2017-6507에 취약함)이라는 높음 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 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-2017-6507에 노출되도록 평가 대상을 수정했습니다. 이 절차는 이 문제에 대한 권장 수정 사항을 적용할 수 있습니다.

1. **`InspectorEC2InstanceUbuntu`** 인스턴스에 연결하고 다음 명령을 실행합니다.

   ```
   sudo apt-get install apparmor=2.10.95-0ubuntu2.6
   ```

2. Assessment templates(평가 템플릿) 페이지에서 MyFirstTemplateUbuntu를 선택한 후 Run(실행)을 선택하여 이 템플릿으로 새로운 실행을 시작합니다.
3. 5단계: 생성된 결과 찾기 및 분석 (p. 15)의 단계를 수행하여 MyFirstTemplateUbuntu 템플릿의 후속 실행 결과를 확인합니다.

   보안 문제 CVE-2017-6507을 해결했기 때문에 더 이상 이 문제의 결과가 표시되지 않습니다.

Amazon Inspector에 서비스 연결 역할 사용

Amazon Inspector에서는 AWS Identity and Access Management(IAM) 서비스 연결 역할을 사용합니다. 서비스 연결 역할은 Amazon Inspector에 직접 연결된 고유한 유형의 IAM 역할입니다. 서비스 연결 역할은 Amazon Inspector에서 사전 정의하며 서비스에서 다른 AWS 서비스를 자동으로 호출하기 위해 필요한 모든 권한을 포함합니다.

서비스 연결 역할을 통해 Amazon Inspector 설정이 쉬워지는데 필요한 권한을 수동으로 추가할 필요가 없기 때문입니다. Amazon Inspector에서 서비스 연결 역할 권한을 정의하므로, 달리 정의되지 않은 한 Amazon Inspector에서만 해당 역할을 맡을 수 있습니다. 정의된 권한에는 신뢰 정책과 권한 정책이 포함되며, 이 권한 정책은 다른 IAM 개체에 연결할 수 없습니다.

Amazon Inspector가 실행 중인 모든 리전에 있는 AWS 계정에 대한 평가 대상을 먼저 삭제하지 않으면 서비스 연결 역할을 삭제할 수 없습니다.

서비스 연결 역할을 지원하는 기타 서비스에 대한 자세한 정보는 IAM으로 작업하는 AWS 서비스를 참조하고 서비스 연결 역할 열에 예가 있는 서비스를 찾으십시오. 해당 서비스에 대한 서비스 연결 역할 설명서를 보려면 [Yes] 링크를 선택합니다.

Amazon Inspector에 대한 서비스 연결 역할 권한

Amazon Inspector에서는 `AWSServiceRoleForAmazonInspector`라는 서비스 연결 역할을 사용합니다. `AWSServiceRoleForAmazonInspector` 서비스 연결 역할은 이 역할을 맡을 Amazon Inspector를 신뢰합니다.

역할 권한 정책은 Amazon Inspector가 지정된 리소스에서 다음 작업을 완료하도록 허용합니다.

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

`AWSServiceRoleForAmazonInspector` 역할을 성공적으로 만들려면 Amazon Inspector와 작업할 때 사용하는 IAM 자격 증명(사용자, 역할 또는 그룹)에 필요한 권한이 있어야 합니다. 필수 권한을 부여하려면 `AmazonInspectorFullAccess` 관리형 정책을 IAM 사용자, 그룹 또는 역할에 추가합니다. 관리형 정책에 대한 자세한 내용은 Amazon Inspector에 대한 AWS 관리형(미리 정의된) 정책 (p. 77) 단원을 참조하십시오.

서비스 연결 역할에 대한 자세한 내용은 IAM 사용 설명서의 서비스 연결 역할 권한을 참조하십시오.

Amazon Inspector에 대한 서비스 연결 역할 생성

`AWSServiceRoleForAmazonInspector` 서비스 연결 역할은 수동으로 생성할 필요가 없습니다.

`AWSServiceRoleForAmazonInspector` 서비스 연결 역할은 자동으로 생성되지만 일부 최소 설정을 먼저 수행해야 할 수도 있습니다. 다음 단원에서는 `AWSServiceRoleForAmazonInspector` 서비스 연결 역할 설정 및 사용에 대해 자세히 설명합니다.

Amazon Inspector를 처음 시작하는 경우

- 콘솔에서 시작Amazon Inspector 마법사를 진행하거나 CreateAssessmentTarget API 작업을 실행하면 `AWSServiceRoleForAmazonInspector` 서비스 연결 역할이 자동으로 생성됩니다.

- 현재 로그인되어 있는 리전에 있는 AWS 계정에 대해서만 `AWSServiceRoleForAmazonInspector` 서비스 연결 역할이 생성됩니다. 이 리전에 있는 AWS 계정의 리소스에 대해서만 Amazon Inspector에 액세스 권한을 부여합니다. 이후에 동일한 AWS 계정을 사용해 시작Amazon Inspector 콘솔 마법사를 진행하거나 다른 리전에서 CreateAssessmentTarget API 작업을 실행하면 AWS 계정에서 이미 생성된 동일한 서비스 연결 역할이 다른 리전에서도 적용되며 Amazon Inspector에 이러한 리전에 있는 AWS 계정의 리소스에 대한 액세스 권한을 부여합니다.

AWS 계정에서 이미 Amazon Inspector가 실행 중인 경우

- AWS 계정에서 이미 Amazon Inspector가 실행 중이면 Amazon Inspector에 리소스에 대한 액세스 권한을 부여하는 IAM 역할이 이미 AWS 계정이 있는 것입니다. 이 경우, Amazon Inspector 콘솔 또는 API 작업을 통해 새 평가 대상이나 새 평가 템플릿을 생성하면 `AWSServiceRoleForAmazonInspector` 서비스 연결 역할이 자동으로 생성됩니다. 새로 생성된 이 서비스 연결 역할이 지금까지 Amazon Inspector에 리소스에 대한 액세스 권한을 부여한 이전에 생성된 IAM 역할을 대체합니다.

  Amazon Inspector의 대시보드 페이지에 있는 Accounts Setting(계정 설정) 섹션에서 Manage Amazon Inspector service-linked role 링크를 선택해 수동으로 `AWSServiceRoleForAmazonInspector` 서비스 연결 역할을 생성할 수도 있습니다. 새로 생성된 이 서비스 연결 역할이 지금까지 Amazon Inspector에 리소스에 대한 액세스 권한을 부여한 이전에 생성된 IAM 역할을 대체합니다.

  Note

  이전에 생성된 이 IAM 역할은 삭제되지 않습니다. 온전하게 유지되지만 더 이상 Amazon Inspector에 리소스에 대한 액세스 권한을 부여하는 데 사용되지 않습니다. IAM 콘솔을 사용해 이 IAM 역할을 추가로 관리하거나 삭제할 수 있습니다.
- 현재 로그인되어 있는 리전에 있는 AWS 계정에 대해서만 `AWSServiceRoleForAmazonInspector` 서비스 연결 역할이 생성됩니다. 이 리전에 있는 AWS 계정의 리소스에 대해서만 Amazon Inspector에 액세스 권한을 부여합니다. 동일한 AWS 계정을 사용하여 다른 리전에서 실행 중인 Amazon Inspector 서비스에 대한 평가 대상 또는 평가 템플릿을 만들면 AWS 계정에 이미 생성된 동일한 서비스 연결 역할이 적용됩니다. 이 리전에 있는 AWS 계정의 리소스에 대해 Amazon Inspector에 액세스 권한을 부여합니다.

IAM 콘솔을 사용하여 Inspector 서비스 연결 역할을 생성할 수 있습니다. IAM CLI 또는 IAM API에서 `Amazon Inspector` 서비스 이름의 서비스 연결 역할을 생성합니다. 자세한 내용은 IAM 사용 설명서의 서비스 연결 역할 생성을 참조하십시오.

이 서비스 연결 역할을 삭제한 다음 다시 생성해야 하는 경우 동일한 프로세스를 사용하여 계정에서 역할을 다시 생성할 수 있습니다. Get started with Amazon Inspector again, 시 서비스 연결 역할이 자동으로 생성됩니다.

Amazon Inspector에 대한 서비스 연결 역할 편집

Amazon Inspector에서는 `AWSServiceRoleForAmazonInspector` 서비스 연결 역할을 편집하도록 허용하지 않습니다. 서비스 연결 역할을 생성한 후에는 다양한 개체가 역할을 참조할 수 있기 때문에 역할 이름을 변경할 수 없습니다. 그러나 IAM를 사용하여 역할의 설명을 편집할 수 있습니다. 자세한 내용은 IAM 사용 설명서의 서비스에 연결 역할 편집을 참조하십시오.

Amazon Inspector에 대한 서비스 연결 역할 삭제

서비스 연결 역할이 필요한 기능 또는 서비스가 더 이상 필요 없는 경우에는 해당 역할을 삭제할 것을 권합니다. 따라서 적극적으로 모니터링하거나 유지하지 않는 미사용 개체가 없도록 합니다. 단, 서비스 연결 역할에 대한 리소스를 먼저 정리해야 수동으로 삭제할 수 있습니다.

Note

리소스를 삭제하려 할 때 Amazon Inspector 서비스가 역할을 사용 중이면 삭제에 실패할 수 있습니다. 이 문제가 발생하면 몇 분 기다렸다가 작업을 다시 시도하십시오.

`AWSServiceRoleForAmazonInspector`에서 사용하는 Amazon Inspector 리소스를 삭제하려면

- Amazon Inspector가 실행 중인 모든 리전에서 이 AWS 계정에 대한 평가 대상을 삭제합니다. 자세한 내용은 Amazon Inspector 평가 대상 (p. 34) 단원을 참조하십시오.

IAM을 사용하여 서비스 연결 역할을 수동으로 삭제하려면

IAM 콘솔, IAM CLI 또는 IAM API를 사용하여 `AWSServiceRoleForAmazonInspector` 서비스 연결 역할을 삭제할 수 있습니다. 자세한 정보는 IAM 사용 설명서의 서비스에 연결 역할 삭제 단원을 참조하십시오.

Amazon Inspector 에이전트

Amazon Inspector 에이전트는 Amazon EC2 인스턴스의 동작 데이터(네트워크 구성, 파일 시스템 보안, 프로세스 활동을 포함)를 모니터링하고 수집하는 엔터티입니다. 모든 경우에 요구되진 않지만, 보안성을 완전히 평가하기 위해선 대상 Amazon EC2 인스턴스마다 Amazon Inspector 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 에이전트 작업 (p. 25) 및 Windows 기반 운영 체제에서 Amazon Inspector 에이전트 작업 (p. 27) 단원을 참조하십시오.

> **Note**
>
> Amazon Inspector 에이전트는 네트워크 연결성 (p. 38) 규칙 패키지를 실행하는 데 필수가 아닙니다.

주제

Amazon Inspector 에이전트 권한

Amazon Inspector 에이전트를 설치하려면 관리자 권한이나 루트 권한이 필요합니다. 지원되는 Linux 기반 운영 체제에서 에이전트는 루트 액세스 권한으로 실행되는 사용자 모드 실행 파일과 에이전트가 작동하는 데 필요한 커널 모듈로 구성됩니다. 지원되는 Windows 기반 운영 체제에서 에이전트는 각각 `LocalSystem` 권한이 있는 사용자 모드로 실행되는 업데이터 서비스 및 에이전트 서비스로 구성됩니다. 에이전트에는 해당 에이전트가 작동하는 데 필요한 커널 모드 드라이버도 포함되어 있습니다.

> **Important**
>
> 다음 목록에는 Linux, Ubuntu, Red Hat Enterprise Linux 및 CentOS에서 실행되는 Amazon Inspector 에이전트와 호환 가능한 모든 커널 버전이 포함되어 있습니다. https://s3.amazonaws.com/aws-agent.us-east-1/linux/support/supported_versions.json
> Linux 기반 OS에서 CVE (p. 40), CIS (p. 41) 또는 보안 모범 사례 (p. 46) 규칙 패키지를 사용하면 EC2 instance에 대한 Amazon Inspector 평가를 실행할 수 있습니다. 인스턴스에 목록에 포함된 커널 버전이 없는 경우에도 평가가 성공적으로 실행됩니다.
> 실행 시간 행동 분석 (p. 43) 규칙 패키지를 사용하여 Linux 기반 OS가 설치된 EC2 instance의 성공적인 평가를 실행하려면 인스턴스에 이 목록에 포함된 커널 버전이 있어야 합니다. 인스턴스에 에이전트와 호환되지 않는 커널 버전이 있는 경우 실행 시간 동작 분석 (p. 43) 규칙 패키지가 하나의 EC2 instance 결과만 평가합니다. 해당 결과는 EC2 instance의 커널 버전이 지원되지 않음을 알려 줍니다.

네트워크 및 Amazon Inspector 에이전트 보안

Amazon Inspector 에이전트는 Amazon Inspector 서비스와 대체로 모든 통신을 시작합니다. 이는 에이전트가 엔드포인트에 원격 측정 데이터를 전송할 수 있도록 퍼블릭 엔드포인트에 대한 아웃바운드 네트워크 경로를 가져야 한다는 것을 의미합니다. 예를 들어, 에이전트는 `arsenal.<region>.amazonaws.com`일 수 있고 엔드포인트는 `s3.dualstack.aws-region.amazonaws.com`의 Amazon S3 버킷일 수 있습니다. (`<region>`은 Amazon Inspector를 실행 중인 실제 AWS 리전으로 바꾸십시오.) 자세한 내용은 AWS IP 주소 범위를 참조하십시오. 에이전트의 모든 연결이 아웃바운드로 설정되므로 Amazon Inspector에서 에이전트로 인바운드 통신을 허용하도록 보안 그룹의 포트를 열 필요는 없습니다.

에이전트는 EC2 instance의 역할 또는 인스턴스에 역할이 할당되지 않은 경우 인스턴스 메타데이터 문서와 연결된 AWS 자격 증명을 사용하여 인증된 TLS 보호 채널을 통해 Amazon Inspector와 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 Inspector에 다시 보냅니다. 에이전트는 자신이 데이터를 수집하는 시스템을 변경하지 않습니다. 에이전트는 원격 측정 데이터를 수집한 후 Amazon Inspector에 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 에이전트 업데이트

Amazon Inspector 에이전트에 대한 업데이트를 사용할 수 있게 되면 Amazon S3에서 자동으로 다운로드되어 적용됩니다. 이때 필수 종속성도 업데이트됩니다. 자동 업데이트 기능의 경우 EC2 instances에 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 Inspector로 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 에이전트에서 생성하는 원격 측정 데이터는 JSON 파일로 형식이 지정됩니다. 파일은 TLS를 통해 거의 실시간으로 Amazon Inspector에 전달됩니다. 여기에서 평가별로 실행되는 임시 KMS 파생 키로 암호화됩니다. 그런 다음 Amazon Inspector 전용 Amazon S3 버킷에 안전하게 저장됩니다. Amazon Inspector의 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 데이터에 대한 표준 S3 버킷 수명 주기 정책에 따라 30일 후에 영구적으로 삭제됩니다. 현재 Amazon Inspector는 수집된 원격 측정에 API 또는 S3 버킷 액세스 메커니즘을 제공하지 않습니다.

Amazon Inspector에서 AWS 계정으로의 액세스 제어

보안 서비스로서 Amazon Inspector는 태그를 쿼리하여 평가할 EC2 instances를 찾아야 하는 경우에만 AWS 계정 및 리소스에 액세스합니다. 이 작업은 Amazon Inspector 서비스의 초기 설정 중에 생성된 역할에 의한 표준 IAM 액세스를 통해 수행됩니다. 평가하는 중에 환경과의 모든 통신은 EC2 instances에 로컬로 설치된 Amazon Inspector 에이전트에 의해 시작됩니다. Amazon Inspector 서비스에서 생성한 평가 대상, 평가 템플릿 및 결과 등의 서비스 객체는 Amazon Inspector에서 관리하고 액세스할 수 있는 데이터베이스에만 저장됩니다.

Amazon Inspector 에이전트 한도

Amazon Inspector 에이전트 한도에 대한 자세한 내용은 Amazon Inspector 서비스 제한 (p. 3) 단원을 참조하십시오.

Amazon Inspector 에이전트 퍼블릭 라이선스

Amazon Inspector 에이전트는 커널 모듈(`amznmon64`)을 전체 에이전트의 구성 요소로 사용합니다. 커널 모듈은 일반 퍼블릭 라이선스(GPLv2)를 사용합니다. 모듈 소스 코드 및 라이선스 정보는 여기에서 공개적으로 액세스할 수 있습니다.

- 소스 코드: https://s3.amazonaws.com/aws-agent.us-east-1/linux/support/AwsAgentKernelModule.tar.gz
- 서명 파일: https://s3.amazonaws.com/aws-agent.us-east-1/linux/support/AwsAgentKernelModule.tar.gz.sig

Amazon Inspector 에이전트 설치

여러 인스턴스(Linux 기반 및 Windows 기반 인스턴스 포함)에서 Systems Manager Run Command를 사용하여 Amazon Inspector 에이전트를 설치할 수 있습니다. 또는 각 EC2 instance에 로그인하여 에이전트를 개별적으로 설치할 수 있습니다. 이 장의 절차에 두 방법이 모두 설명되어 있습니다.

또 다른 옵션으로, 콘솔에서 평가 대상 정의 페이지의 에이전트 설치 확인란을 선택하여 평가 대상에 포함된 모든 Amazon EC2 인스턴스에 에이전트를 신속하게 설치할 수 있습니다.

주제

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

Amazon Linux AMI와 Amazon Inspector 에이전트

평가 대상에 포함하려는 Amazon Linux EC2 instances에서 수동 Amazon Inspector 에이전트 설치를 건너뛰기 위해 Amazon Inspector 에이전트가 설치된 Amazon Linux AMI를 사용할 수 있습니다. 이 AMI에는 에

이전트가 사전 설치되어 있으며 에이전트 설치 또는 설정을 위한 추가 단계가 필요하지 않습니다. 이 EC2 instances와 함께 Amazon Inspector 사용을 시작하려면 원하는 평가 대상과 일치하도록 태그를 지정하면 됩니다. Amazon Inspector 에이전트가 설치된 Amazon Linux AMI의 구성은 액세스를 제한하고 소프트웨어 취약점을 줄이겠다는 두 가지 주요 보안 목표에 초점을 두고 보안을 강화합니다.

현재 Amazon Inspector 에이전트가 사전 설치되어 있는 유일한 EC2 instance AMI입니다. Ubuntu Server 또는 Windows Server를 실행하는 EC2 instances의 경우 수동 에이전트 설치 단계를 완료해야 합니다.

Amazon Inspector 에이전트가 설치된 Amazon Linux AMI는 EC2 콘솔과 AWS Marketplace에서 제공됩니다.

Systems Manager Run Command를 사용하여 여러 EC2 인스턴스에 에이전트 설치

Systems Manager Run Command를 사용하여 EC2 instances에 Amazon Inspector에이전트를 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 instance에 SSM 에이전트가 설치되어 있고, Run Command를 허용하는 IAM 역할이 지정되어 있어야 합니다. SSM 에이전트는 Amazon EC2 Windows 인스턴스와 Amazon Linux 인스턴스에 기본적으로 설치됩니다. Amazon EC2 Systems Manager에는 명령을 처리하는 EC2 instances를 위한 IAM 역할과 명령을 실행하는 사용자를 위한 별도의 역할이 필요합니다. 자세한 내용은 Installing and Configuring SSM Agent 및 Configuring Security Roles for System Manager 단원을 참조하십시오.

Systems Manager Run Command를 사용하여 여러 EC2 instances에 에이전트를 설치하려면

1. https://console.aws.amazon.com/ec2/에서 Amazon EC2 콘솔을 엽니다.
2. 탐색 창의 [Systems Manager Services] 아래에서 [Run Command]를 선택합니다.
3. Run a command를 선택합니다.
4. 명령 문서에서 Amazon이 소유한 AmazonInspector-ManageAWSAgent라는 이름의 문서를 선택합니다. 이 문서에는 EC2 instances에 Amazon Inspector 에이전트를 설치하는 데 필요한 스크립트가 들어 있습니다.
5. 다음을 기준으로 대상 선택에서 태그 지정 옵션 또는 수동으로 인스턴스 선택을 선택하여 EC2 instances를 지정합니다. 그런 다음 인스턴스 선택을 선택합니다. 평가 대상의 모든 인스턴스에 에이전트를 설치하려면 평가 대상을 생성할 때 사용한 태그를 그대로 지정하면 됩니다.
6. EC2 콘솔에서 명령 실행의 지침을 사용하여 제공되는 나머지 옵션을 선택한 다음 실행을 선택합니다.

> Note
>
> 평가 대상을 만들 때 여러 EC2 instances(Linux 기반 및 Windows 기반)에 에이전트를 설치하거나 기존 대상에 대해 Run Command를 사용하여 에이전트 설치 버튼을 사용할 수도 있습니다. 자세한 내용은 평가 대상 생성 (p. 34)를 참조하십시오.

Linux 기반 EC2 인스턴스에 에이전트 설치

Linux 기반 EC2 instance에 Amazon Inspector 에이전트를 설치하려면 다음 절차를 수행합니다.

Linux 기반 EC2 instance에 에이전트를 설치하려면

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

   Note

   Amazon Inspector에서 지원하는 운영 체제에 대한 내용은 Amazon Inspector 지원 운영 체제 및 리전 (p. 4) 단원을 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) AWS 에이전트 설치 스크립트가 변경 또는 손상되지 않았는지 확인합니다. 자세한 내용은 (선택 사항) Linux 기반 운영 체제에서 Amazon Inspector 에이전트 설치 스크립트의 서명을 확인합니다. (p. 29) 단원을 참조하십시오.
4. sudo bash install에 에이전트를 설치하려면

   Note

   에이전트에 대한 업데이트를 사용할 수 있게 되면 Amazon S3에서 자동으로 다운로드되어 적용됩니다. 자세한 내용은 Amazon Inspector 에이전트 업데이트 (p. 21) 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)
   - `libpcap0.8`

Windows 기반 EC2 인스턴스에 에이전트 설치

Windows 기반 EC2 instance에 Amazon Inspector 에이전트를 설치하려면 다음 절차를 수행합니다.

Windows 기반 EC2 instance에 에이전트를 설치하려면

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

   Note

   Amazon Inspector에서 지원하는 운영 체제에 대한 자세한 내용은 Amazon Inspector 지원 운영 체제 및 리전 (p. 4) 단원을 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 에이전트 업데이트 (p. 21) 단원을 참조하십시오.
   이 자동 업데이트 프로세스를 건너뛸 경우 에이전트를 설치할 때 다음 명령을 실행합니다.
   AWSAgentInstall.exe AUTOUPDATE=No

Linux 기반 운영 체제에서 Amazon Inspector 에이전트 작업

Amazon Inspector 에이전트를 설치 및 제거, 확인하고, 동작을 수정할 수 있습니다. Linux 기반 운영 체제를 실행하는 Amazon EC2 인스턴스에 로그인하여 다음 절차를 실행합니다. Amazon Inspector에 대해 지원되는 운영 체제에 대한 자세한 내용은 Amazon Inspector 지원 운영 체제 및 리전 (p. 4) 단원을 참조하십시오.

Note

이 단원의 명령은 Amazon Inspector 서비스에서 지원하는 모든 AWS 리전에서 작동합니다.

주제

Amazon Inspector 에이전트가 실행 중인지 확인

- 에이전트가 설치되고 실행 중인지 확인하려면 EC2 instance에 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 에이전트 중지

- 에이전트를 중지하려면 다음 명령을 실행합니다.

  sudo /etc/init.d/awsagent stop

Amazon Inspector 에이전트 시작

- 에이전트를 시작하려면 다음 명령을 실행합니다.

  sudo /etc/init.d/awsagent start

Amazon Inspector 에이전트 설정 수정

EC2 instance에 Amazon Inspector 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 에이전트에 대한 프록시 지원 구성

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 instance에 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 (p. 23) 절차의 단계를 수행하여 Amazon Inspector 에이전트를 설치합니다.

실행 중인 에이전트를 사용하여 EC2 instance에서 프록시 지원을 구성하려면

1. 프록시 지원을 구성하려면 EC2 instance에서 실행 중인 에이전트 버전이 1.0.800.1 이상이어야 합니다. 에이전트에 대한 자동 업데이트 프로세스를 활성화한 경우 Amazon Inspector 에이전트가 실행 중인지 확인 (p. 25) 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 (p. 23) 절차를 수행하여 이 EC2 instance에 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 에이전트 제거

에이전트를 제거하려면

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

   Note

   Amazon Inspector에 대해 지원되는 운영 체제에 대한 자세한 내용은 Amazon Inspector 지원 운영 체제 및 리전 (p. 4) 단원을 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 에이전트 작업

Amazon Inspector 에이전트를 시작, 중지하고, 동작을 수정할 수 있습니다. Windows 기반 운영 체제를 실행하는 EC2 instance에 로그인하고 이 장의 절차를 실행합니다. Amazon Inspector에 대해 지원되는 운영 체제에 대한 자세한 내용은 Amazon Inspector 지원 운영 체제 및 리전 (p. 4) 단원을 참조하십시오.

Note

이 장의 명령은 Amazon Inspector 서비스에서 지원하는 모든 AWS 리전에서 작동합니다.

주제

Amazon Inspector 에이전트를 시작 또는 중지하거나 에이전트가 실행 중인지 확인

에이전트를 시작, 중지 또는 확인하려면

1. EC2 instance에서 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 instance에 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 에이전트 설정 수정

EC2 instance에 Amazon Inspector 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 에이전트에 대한 프록시 지원 구성

Windows 기반 운영 체제에서 에이전트에 대한 프록시 지원을 받으려면 `WinHTTP` 프록시를 사용합니다. `netsh` 유틸리티를 사용하여 `WinHTTP` 프록시를 설정하려면 https://technet.microsoft.com/en-us/library/cc731131%28v=ws.10%29.aspx를 참조하십시오.

> Important
>
> Windows 기반 인스턴스에는 HTTPS 프록시만 지원됩니다.

다음 절차 중 하나를 완료합니다.

프록시 서버를 사용하는 EC2 instance에 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 instance에서 프록시 지원을 구성하려면

1. 프록시 지원을 구성하려면 EC2 instance에서 실행 중인 Amazon Inspector 에이전트 버전이 1.0.0.59 이상이어야 합니다. 에이전트에 대한 자동 업데이트 프로세스를 활성화한 경우 Amazon Inspector 에이전트를 시작 또는 중지하거나 에이전트가 실행 중인지 확인 (p. 27) 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 (p. 24) 절차를 수행하여 이 EC2 instance에 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 Agent Service(AWS 에이전트 서비스)와 AWS Agent Updater Service(AWS 에이전트 업데이터 서비스)를 찾은 후 각 프로세스를 시작합니다. 두 프로세스가 모두 성공적으로 재시작되면 `AWSAgentStatus.exe` 파일을 실행합니다(Amazon Inspector 에이전트를 시작 또는 중지하거나 에이전트가 실행 중인지 확인 (p. 27)의 5단계 참조). 에이전트의 상태를 보고 구성된 프록시를 사용 중인지 확인합니다.

Amazon Inspector 에이전트 제거

에이전트를 제거하려면

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

   Note

   Amazon Inspector에 대해 지원되는 운영 체제에 대한 자세한 내용은 Amazon Inspector 지원 운영 체제 및 리전 (p. 4) 단원을 참조하십시오.
2. EC2 instance의 제어판, 프로그램 추가/제거로 이동합니다.
3. 설치된 프로그램 목록에서 AWS 에이전트를 선택한 다음, 제거를 선택합니다.

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

이 주제에서는 Linux 기반 운영 체제에서 Amazon Inspector 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 에이전트의 소프트웨어가 변경 또는 손상된 것을 확인한 경우 설치 파일을 실행하지 마십시오. 대신, AWS Support에 문의하십시오.

Linux 기반 운영 체제용 Amazon Inspector 에이전트 파일은 보안 디지털 서명을 위한 Pretty Good Privacy 표준의 오픈 소스 구현(OpenPGP)인 `GnuPG`를 사용하여 서명됩니다. `GnuPG`(`GPG`라고도 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 참조하십시오.

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

주제

GPG 도구 설치

Linux 또는 Unix 운영 체제를 사용하는 경우 일반적으로 GPG 도구가 이미 설치되어 있습니다. 시스템에 도구가 설치되어 있는지 테스트하려면 명령 프롬프트에 gpg를 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 퍼블릭 키를 인증하고 이를 신뢰할 수 있는 키로 GPG 인증 키에 추가하는 것입니다.

Amazon Inspector 퍼블릭 키 인증 및 가져오기

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.key라는 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.key를 저장한 디렉터리의 명령 프롬프트에서 다음 명령을 사용하여 Amazon Inspector 퍼블릭 키를 인증 키에 가져옵니다.

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

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 `58360418`입니다.

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`과 동일해야 합니다. 반환된 키 지문을 이 페이지에 게시된 지문과 비교합니다. 두 지문이 일치해야 합니다. 일치하지 않을 경우 Amazon Inspector 에이전트 설치 스크립트를 설치하지 말고 AWS Support에 문의하십시오.

패키지의 서명 확인

GPG 도구를 설치하고, Amazon Inspector 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://d1wk0tztpsntt1.cloudfront.net/linux/latest/install.sig
```

2. `install.sig` 및 Amazon Inspector 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 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 Inspector에 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 참조하십시오.

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

이 주제에서는 Windows 기반 운영 체제에서 Amazon Inspector 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 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.

5C 2C B5 5A 9A B9 B1 D6 3F F4 1B 0D A2 76 F2 A9 2B 09 A8 6A

이 값을 확인하려면 다음 절차를 수행합니다.

1. 다운로드한 `AWSAgentInstall.exe`를 마우스 오른쪽 버튼으로 클릭하고 속성 창을 엽니다.
2. 디지털 서명 탭을 선택합니다.
3. 서명 목록에서 Amazon Services LLC를 선택한 후 세부 정보를 선택합니다.
4. 일반 탭이 선택되어 있지 않으면 이 탭을 선택한 후 인증서 보기를 선택합니다.
5. 아직 선택하지 않은 경우 세부 정보 탭을 선택한 후 표시 드롭다운 목록에서 모두를 선택합니다.
6. 지문 필드가 보일 때까지 아래로 스크롤한 후 지문을 선택합니다. 그러면 아래 창에 전체 지문 값이 표시됩니다.

   - 아래 창의 지문 값이 다음과 값과 동일한지 확인합니다.

     5C 2C B5 5A 9A B9 B1 D6 3F F4 1B 0D A2 76 F2 A9 2B 09 A8 6A

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 평가 대상

Amazon Inspector를 사용하여 AWS 평가 대상(AWS 리소스 모음)에 해결해야 할 잠재적인 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 Amazon Inspector 서비스 제한 (p. 3) 단원을 참조하십시오.

> Note
>
> EC2 instances 시작에 대한 자세한 내용은 Amazon Elastic Compute Cloud 설명서를 참조하십시오.

주제

평가 대상을 생성하도록 리소스에 태그 지정

평가할 Amazon Inspector에 대한 평가 대상을 생성하려면 대상에 포함할 EC2 instances에 태그를 지정하여 시작합니다. 태그는 인스턴스 및 기타 AWS 리소스를 식별하고 구성하기 위한 메타데이터 역할을 하는 단어 또는 구입니다. Amazon Inspector는 태그를 사용하여 대상에 속한 인스턴스를 식별합니다.

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

평가 대상을 빌드하기 위해 EC2 instances에 태그를 지정할 경우 사용자 지정 태그 키를 만들거나 동일한 AWS 계정에서 다른 사용자가 만든 태그 키를 사용할 수 있습니다. AWS가 자동으로 생성하는 태그 키를 사용할 수도 있습니다. 예를 들어, AWS는 시작하는 EC2 instances의 Name 태그 키를 자동으로 만듭니다.

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

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

Amazon Inspector 평가 대상 제한

AWS 계정당 최대 50개의 평가 대상을 생성할 수 있습니다. 자세한 내용은 Amazon Inspector 서비스 제한 (p. 3) 단원을 참조하십시오.

평가 대상 생성

Amazon Inspector 콘솔을 사용하여 평가 대상을 만들 수 있습니다.

평가 대상을 생성하려면

1. Sign in to the AWS Management 콘솔 and open the Amazon Inspector console at https://console.aws.amazon.com/inspector/.
2. 탐색 창에서 [Assessment Targets]를 선택한 후 [Create]를 선택합니다.
3. 이름에 평가 대상의 이름을 입력합니다.
4. 다음 중 하나를 수행하십시오.
   - 이 AWS 계정에 모든 EC2 instances를 포함하고 이 평가 대상에 리전을 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 서비스 제한 (p. 3) 단원을 참조하십시오.
   - 이 평가 대상에 포함할 EC2 instances를 선택하려면 태그 사용에 태그 키 이름과 키-값 페어를 입력합니다.
5. (선택 사항) 대상을 생성할 때 에이전트 설치 확인란을 선택하여 이 대상의 모든 EC2 instances 에 에이전트를 설치할 수 있습니다. 이 옵션을 사용하려면 EC2 instances에 SSM 에이전트가 설치되어 있고, Run Command를 허용하는 IAM 역할이 지정되어 있어야 합니다. SSM 에이전트는 Amazon EC2 Windows 인스턴스와 Amazon Linux 인스턴스에 기본적으로 설치됩니다. Amazon EC2 Systems Manager에는 명령을 처리하는 EC2 instances를 위한 IAM 역할과 명령을 실행하는 사용자를 위한 별도의 역할이 필요합니다. 자세한 내용은 Installing and Configuring SSM Agent 및 Configuring Security Roles for System Manager 단원을 참조하십시오.

   Important

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

   Note

   기존의 평가 대상에 대해 Run Command를 사용하여 에이전트 설치 버튼을 선택하여 이 대상의 모든 EC2 instances에 에이전트를 설치할 수 있습니다.

   Note

   Systems Manager Run Command를 사용하여 여러 EC2 instances에 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 설치하려면 (p. 23)을 참조하십시오.
6. 저장을 선택합니다.

   Note

   Assessment Targets(평가 대상) 페이지에 있는 Preview Target(대상 미리 보기) 버튼을 사용하여 평가 대상에 포함되어 있는 모든 EC2 instances를 검토할 수 있습니다. 각 EC2 instance에 대해 호스트 이름, 인스턴스 ID, IP 주소 및 해당되는 경우 에이전트의 상태를 검토할 수 있습니다. 에이전트 상태는 HEALTHY, UNHEALTHY 및 UNKNOWN 값을 가질 수 있습니다. Amazon Inspector는 EC2 instance에서 실행 중인 에이전트가 있는지 여부를 판단할 수 없을 때 UNKNOWN 상태를 표시합니다.

평가 대상 삭제

평가 대상을 삭제하려면 다음 절차를 수행하십시오.

평가 대상을 삭제하려면

- 평가 대상 페이지에서 삭제할 대상을 선택한 후 삭제를 선택합니다. 확인 메시지가 표시되면 [Yes]를 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 규칙 패키지 및 규칙

Amazon Inspector을 사용하여 잠재적 보안 문제 및 취약점에 대한 평가 대상(AWS 리소스 모음)에 액세스할 수 있습니다. Amazon Inspector는 평가 대상의 행동 및 보안 구성과 선택된 보안 규칙 패키지를 비교합니다. Amazon Inspector의 컨텍스트에서 규칙은 평가 실행 중에 Amazon Inspector가 수행하는 보안 검사입니다.

Amazon Inspector에서 규칙은 범주, 심각도 또는 요금별로 고유한 규칙 패키지로 함께 그룹화됩니다. 이렇게 하면 다양한 종류의 분석을 수행할 수 있습니다. 예를 들어, Amazon Inspector는 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 Inspector의 규칙에 대한 심각도 수준

각 Amazon Inspector 규칙에는 심각도 수준이 할당되어 있습니다. 이 경우 분석에서 규칙의 우선 순위를 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. Informational 수준은 단순히 평가 대상의 보안 구성 세부 정보를 강조 표시합니다. 다음은 각각에 대응하는 권장 방법입니다.

- 높음 – 평가 대상 내 정보 기밀성, 무결성 및 가용성이 손상될 수 있는 보안 문제를 설명합니다. 이 보안 문제는 긴급으로 처리하고 즉각적으로 해결하는 것이 좋습니다.
- 중간 – 평가 대상 내 정보 기밀성, 무결성 및 가용성이 손상될 수 있는 보안 문제를 설명합니다. 가능한 다음 기회(예: 다음 서비스 업데이트)에 이 문제를 해결하는 것이 좋습니다.
- 낮음 – 평가 대상 내 정보 기밀성, 무결성 및 가용성이 손상될 수 있는 보안 문제를 설명합니다. 이후 서비스 업데이트 시 이 문제를 해결하는 것이 좋습니다.
- 정보 – 평가 대상의 특정 보안 구성 세부 정보를 설명합니다. 비즈니스 및 조직 목표에 따라 이 정보를 기록해 두거나 이 정보를 사용하여 평가 대상의 보안을 강화할 수 있습니다.

Amazon Inspector의 규칙 패키지

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

네트워크 평가:

호스트 평가:

- Center for Internet Security(CIS) 벤치마크 (p. 41)
- Amazon Inspector 보안 모범 사례 (p. 46)
- 실행 시간 행동 분석 (p. 43)

네트워크 연결성

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

네트워크 연결성 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 instance에 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 에이전트는 이 규칙 패키지를 통해 EC2 instance를 평가하는 데 필요하지 않습니다. 하지만 설치된 에이전트는 포트에서 수신하는 프로세스의 존재 여부에 대한 정보를 제공할 수 있습니다.

> **Important**
>
> 이 규칙 패키지는 Amazon EC2 Classic 네트워크를 지원하지 않습니다.

자세한 내용은 지원되는 운영 체제의 Amazon Inspector 규칙 패키지 (p. 65) 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

Important

네트워크 연결성 규칙 패키지는 인바운드 액세스를 허용하거나 제한하는 다른 설명을 고려하지 않습니다.

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 포함 된 평가는 각 연결성 라우팅에 대해 다음 유형의 결과를 반환할 수 있습니다.

- `RecognizedPort` (p. 39)
- `UnrecognizedPortWithListener` (p. 40)
- `NetworkExposure` (p. 40)

RecognizedPort

잘 알려진 서비스에 일반적으로 사용되는 포트에 연결 가능합니다. 대상 EC2 instance에 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.

서비스	TCP 포트	UDP 포트
SMB	445	445
NetBIOS	137, 139	137, 138
LDAP	389	389
LDAP over TLS	636	
글로벌 카탈로그 LDAP	3268	
글로벌 카탈로그 LDAP over TLS	3269	

서비스	TCP 포트	UDP 포트
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
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 instance에 설치된 경우에만 생성될 수 있습니다. 이 유형의 결과에는 낮음 심각도가 부여됩니다.

NetworkExposure

이 유형의 결과는 EC2 instance에서 연결할 수 있는 포트에 대한 집계 정보를 표시합니다. 이러한 결과는 탄력적 네트워크 인터페이스와 EC2 instance의 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 instances가 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 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.

이 패키지에 포함된 규칙은 EC2 instances가 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 규칙 패키지 (p. 65) 단원을 참조하십시오.

Center for Internet Security(CIS) 벤치마크

CIS 보안 벤치 마크 프로그램은 조직이 보안을 평가하고 개선하는 데 도움이 되는 잘 정의되고 편향되지 않으며 합의된 업계 모범 사례를 제공합니다. AWS는 CIS 보안 벤치마크 회원 회사입니다. Amazon Inspector 인증 목록을 보려면 CIS 웹 사이트의 Amazon Web Services 페이지를 참조하십시오.

Amazon Inspector는 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 7 Benchmark v2.0.2 Level 2 Server
- CIS Benchmark for CentOS Linux 7 Benchmark v2.0.2 Level 1 Workstation
- CIS Benchmark for CentOS Linux 7 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 7 Benchmark v2.0.2 Level 2 Server
- CIS Benchmark for Red Hat Enterprise Linux 7 Benchmark v2.0.2. Level 1 Workstation
- CIS Benchmark for Red Hat Enterprise Linux 7 Benchmark v2.0.2 Level 2 Workstation

Ubuntu

- 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 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)
- 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 1 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 1 Domain Controller Profile)

Amazon Inspector 평가 실행에서 생성한 결과에 특정 CIS 벤치마크가 표시될 경우 벤치마크에 대한 상세한 PDF 설명을 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 규칙 패키지 (p. 65) 단원을 참조하십시오.

실행 시간 행동 분석

실행 시간 동작 분석 규칙 패키지의 규칙은 평가 실행 중 인스턴스의 동작을 분석합니다. 또한 EC2 instances를 더 안전하게 만드는 방법에 대한 지침을 제공합니다.

자세한 내용은 지원되는 운영 체제의 Amazon Inspector 규칙 패키지 (p. 65) 단원을 참조하십시오.

주제

보안되지 않은 클라이언트 프로토콜(로그인)

이 규칙은 클라이언트가 보안되지 않은 프로토콜을 사용하여 원격 시스템에 로그인하는 것을 감지합니다.

> Important
>
> 현재 Linux 기반 또는 Windows 기반 운영 체제를 실행하는 EC2 instances를 평가 대상에 포함시킬 수 있습니다.
> 이 규칙은 Linux 또는 Windows 기반 운영 체제를 실행하는 EC2 instances에 대한 결과를 생성합니다.

심각도: 중간 (p. 37)

결과

평가 대상의 EC2 instance가 보안되지 않은 프로토콜로 원격 호스트에 연결하여 로그인합니다. 이러한 프로토콜은 자격 증명을 안전하게 보안하지 않으므로 자격 증명의 도난 위험이 높습니다.

해결 방법

이러한 보안되지 않은 프로토콜을 보안이 우수한 프로토콜(예: SSH)로 바꾸는 것이 좋습니다.

보안되지 않은 클라이언트 프로토콜(일반)

이 규칙은 클라이언트의 보안되지 않은 프로토콜 사용을 감지합니다.

> Important
>
> 현재 Linux 기반 또는 Windows 기반 운영 체제를 실행하는 EC2 instances를 평가 대상에 포함시킬 수 있습니다.

이 규칙은 Linux 또는 Windows 기반 운영 체제를 실행하는 EC2 instances에 대한 결과를 생성합니다.

심각도: 낮음 (p. 37)

결과

평가 대상의 EC2 instance가 보안되지 않은 프로토콜을 사용하여 원격 호스트에 연결합니다. 이러한 프로토콜은 트래픽을 보안하지 않으므로 트래픽 가로채기 공격이 성공할 위험이 높습니다.

해결 방법

이러한 보안되지 않은 프로토콜을 암호화된 버전으로 바꾸는 것이 좋습니다.

사용하지 않은 수신 TCP 포트

이 규칙은 평가 대상에 필요하지 않은 수신 TCP 포트를 감지합니다.

Important

현재 Linux 기반 또는 Windows 기반 운영 체제를 실행하는 EC2 instances를 평가 대상에 포함시킬 수 있습니다.
이 규칙은 Linux 또는 Windows 기반 운영 체제를 실행하는 EC2 instances에 대한 결과를 생성합니다.

심각도: 정보 (p. 37)

결과

평가 대상의 EC2 instance가 TCP 포트에서 수신 중이지만 Amazon Inspector는 평가 실행 중에 이러한 포트에 대한 트래픽을 발견하지 못했습니다.

해결 방법

배포의 공격 대상 영역을 줄이기 위해 사용하지 않는 네트워크 서비스는 비활성화하는 것이 좋습니다. 네트워크 서비스가 필요한 경우 VPC ACL, EC2 보안 그룹 및 방화벽 등의 네트워크 제어 메커니즘을 사용하여 해당 서비스의 노출을 제한하는 것이 좋습니다.

보안되지 않은 서버 프로토콜

이 규칙을 통해 EC2 instances가 FTP, Telnet, HTTP, IMAP, POP 버전 3, SMTP, SNMP 버전 1 및 2, RSH 및 `rlogin` 등의 보안 및 암호화되지 않은 포트/서비스 지원을 허용하는지 여부를 확인할 수 있습니다.

Important

현재 Linux 기반 또는 Windows 기반 운영 체제를 실행하는 EC2 instances를 평가 대상에 포함시킬 수 있습니다.
이 규칙은 Linux 또는 Windows 기반 운영 체제를 실행하는 EC2 instances에 대한 결과를 생성합니다.

심각도: 정보 (p. 37)

결과

평가 대상의 EC2 instance가 보안되지 않은 프로토콜을 지원하도록 구성되어 있습니다.

해결 방법

평가 대상의 EC2 instance에서 지원되는 보안되지 않은 프로토콜을 비활성화하고, 이를 아래와 같은 보안이 더 우수한 프로토콜로 바꾸는 것이 좋습니다.

- Telnet, RSH 및 `rlogin`을 비활성화하고 이를 SSH로 바꿉니다. 가능하지 않은 경우 보안되지 않은 서비스가 VPC 네트워크 ACL 및 EC2 보안 그룹과 같은 적절한 네트워크 액세스 제어로 보호되도록 해야 합니다.
- 가능한 경우 FTP를 SCP 또는 SFTP로 바꿉니다. 가능하지 않은 경우 FTP 서버가 VPC 네트워크 ACL 및 EC2 보안 그룹과 같은 적절한 네트워크 액세스 제어로 보호되도록 해야 합니다.
- 가능한 경우 HTTP를 HTTPS로 바꿉니다. 문제의 웹 서버와 관련된 자세한 내용은 `http://nginx.org/en/docs/http/configuring_https_servers.html` 및 `http://httpd.apache.org/docs/2.4/ssl/ssl_howto.html` 단원을 참조하십시오.
- 필요하지 않은 경우 IMAP, POP3 및 SMTP 서비스를 비활성화합니다. 필요한 경우 이러한 이메일 프로토콜을 TLS와 같은 암호화된 프로토콜과 함께 사용하는 것이 좋습니다.
- 필요하지 않은 경우 SNMP 서비스를 비활성화합니다. 필요한 경우 SNMP v1 및 v2를 암호화된 통신을 사용하는 더 안전한 SNMP v3로 바꿉니다.

데이터 실행 방지(DEP) 기능이 없는 소프트웨어

이 규칙은 데이터 실행 방지(DEP) 지원 없이 컴파일된 타사 소프트웨어가 있는지 감지합니다. DEP는 스택 기반 버퍼 오버플로우 및 기타 메모리 손상 공격으로부터 보호하여 시스템 보안을 개선합니다.

> **Important**
>
> 현재 Linux 기반 또는 Windows 기반 운영 체제를 실행하는 EC2 instances를 평가 대상에 포함시킬 수 있습니다.
> 평가 실행 중에 이 규칙은 Linux 기반 운영 체제를 실행하는 EC2 instances에 대한 결과만 생성합니다. 이 규칙은 Windows 기반 운영 체제를 실행하는 EC2 instances에 대한 결과는 생성하지 않습니다.

심각도: 중간 (p. 37)

결과

평가 대상의 EC2 instance에 DEP를 지원하지 않는 실행 파일이 있습니다.

해결 방법

DEP를 사용하지 않는 경우 평가 대상에서 이 소프트웨어를 제거하거나 공급업체에 문의하여 DEP가 활성화된 이 소프트웨어의 업데이트된 버전을 받는 것이 좋습니다.

보안되지 않은 권한이 포함된 루트 프로세스

이 규칙을 통해 권한이 없는 사용자가 수정할 수 있는 모듈을 로드하는 루트 프로세스를 감지할 수 있습니다.

> **Important**
>
> 현재 Linux 기반 또는 Windows 기반 운영 체제를 실행하는 EC2 instances를 평가 대상에 포함시킬 수 있습니다.
> 평가 실행 중에 이 규칙은 Linux 기반 운영 체제를 실행하는 EC2 instances에 대한 결과만 생성합니다. 이 규칙은 Windows 기반 운영 체제를 실행하는 EC2 instances에 대한 결과는 생성하지 않습니다.

심각도: 높음 (p. 37)

결과

무단 수정에 취약한 공유 객체를 사용하는 하나 이상의 루트 소유 프로세스를 포함하는 인스턴스가 평가 대상에 있습니다. 이러한 공유 객체에는 부적절한 권한/소유권이 있기 때문에 훼손에 취약합니다.

해결 방법

평가 대상의 보안을 강화하기 위해 루트 사용자만 쓸 수 있도록 관련 모듈에 대한 권한을 수정하는 것이 좋습니다.

Amazon Inspector 보안 모범 사례

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

> **Important**
>
> 현재 Linux 기반 또는 Windows 기반 운영 체제를 실행하는 EC2 instances를 평가 대상에 포함시킬 수 있습니다.
> 평가를 실행하는 중에 이 단원에서 설명하는 규칙은 Linux 기반 운영 체제를 실행하는 EC2 instances에 대한 결과만 생성합니다. 이 규칙은 Windows 기반 운영 체제를 실행하는 EC2 instances에 대한 결과는 생성하지 않습니다.
> 자세한 내용은 지원되는 운영 체제의 Amazon Inspector 규칙 패키지 (p. 65) 단원을 참조하십시오.

주제

SSH를 통해 루트 로그인 비활성화

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

심각도: 중간 (p. 37)

결과

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

해결 방법

SSH를 통한 루트 계정 로그인을 방지하도록 EC2 instance를 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 instances가 SSH 프로토콜 버전 1을 지원하도록 구성되어 있는지 확인할 수 있습니다.

심각도: 중간 (p. 37)

결과

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

해결 방법

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

SSH를 통한 암호 인증 비활성화

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

심각도: 중간 (p. 37)

결과

평가 대상의 EC2 instance가 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 instances에서 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 instances에 암호의 최대 수명이 구성되어 있는지 확인할 수 있습니다.

심각도 - 중간 (p. 37)

결과

평가 대상의 EC2 instance에 암호의 최대 수명이 구성되어 있지 않습니다.

해결 방법

암호를 사용하는 경우 평가 대상의 모든 EC2 instances에 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 instances에 암호의 최소 길이가 구성되어 있는지 확인할 수 있습니다.

심각도: 중간 (p. 37)

결과

평가 대상의 EC2 instance에 암호의 최소 길이가 구성되어 있지 않습니다.

해결 방법

암호를 사용하는 경우 평가 대상의 모든 EC2 instances에 암호의 최소 길이를 구성하는 것이 좋습니다. 최소 암호 길이를 적용하면 암호 추측 공격이 성공할 위험이 줄어듭니다. 최소 암호 길이를 적용하려면 PAM 구성에서 `pam_cracklib.so`의 `minlen` 파라미터를 설정합니다. 자세한 내용은 `man pam_cracklib`를 참조하십시오.

암호 복잡도 구성

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

심각도: 중간 (p. 37)

결과

평가 대상의 EC2 instances에 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 instances를 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 `pam_cracklib.so` 모듈을 사용하여 `lcredit`, `ucredit`, `dcredit` 및 `ocredit` 옵션을 설정할 수 있습니다. 자세한 내용은 `man pam_cracklib` 단원을 참조하십시오.

ASLR 활성화

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

심각도: 중간 (p. 37)

결과

평가 대상의 EC2 instance에 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 instances의 운영 체제에서 ASLR을 활성화하는 것이 좋습니다.

DEP 활성화

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

심각도: 중간 (p. 37)

결과

평가 대상의 EC2 instance에 ASLR이 활성화되어 있지 않습니다.

해결 방법

평가 대상에 있는 모든 EC2 instances의 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 (p. 37)

결과

평가 대상의 EC2 instance에 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 instances의 모든 시스템 디렉터리를 루트 계정 자격 증명을 사용하여 로그인하는 사용자만 쓸 수 있도록 구성합니다.

Amazon Inspector 평가 템플릿 및 평가 실행

Amazon Inspector에서 AWS 리소스를 분석하는 보안 규칙을 사용하여 잠재적인 보안 문제를 발견할 수 있습니다. Amazon Inspector에서는 리소스에 대한 동작 데이터(원격 측정)를 모니터링 및 수집합니다. 이 데이터에는 보안 채널 사용, 실행 중인 프로세스 간의 네트워크 트래픽 및 AWS 서비스와의 통신에 대한 정보가 포함됩니다. 그런 다음 Amazon Inspector는 보안 규칙 패키지 세트에 대한 데이터를 분석 및 비교합니다. 마지막으로 Amazon Inspector는 다양한 심각도의 잠재적인 보안 문제를 식별하는 결과 목록을 생성합니다.

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

주제

Amazon Inspector 평가 템플릿

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

- Amazon Inspector가 평가 대상을 평가하기 위해 사용하는 규칙 패키지
- 평가 실행 기간

  Note

  사용 가능한 다음 값으로 기간을 설정할 수 있습니다.
  - 15분
  - 1시간(권장)
  - 8시간
  - 12시간
  - 24시간

  실행 중인 평가 템플릿의 기간이 길수록, Amazon Inspector가 수집 및 분석할 수 있는 원격 측정 세트가 더 철저하고 완벽합니다. 즉, 분석이 더 길어지면 Amazon Inspector는 평가 대상의 동작을 더 자세히 관찰하고 더 많은 결과 세트를 생성할 수 있습니다. 마찬가지로 평가 실행 중에 대상에 포함된 AWS 리소스를 더 철저하게 사용할수록, Amazon Inspector가 수집 및 분석하는 원격 측정 세트가 더 철저하고 완벽합니다.
- Amazon Inspector가 평가 실행 상태 및 결과에 대한 알림을 보내는 Amazon SNS 주제

- 이 평가 템플릿을 사용하는 평가 실행에서 생성한 결과에 할당할 수 있는 Amazon Inspector 속성(키-값 페어)

Amazon Inspector에서 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 Inspector는 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 평가 템플릿 제한

각 AWS 계정당 최대 500개의 평가 템플릿을 생성할 수 있습니다.

자세한 내용은 Amazon Inspector 서비스 제한 (p. 3) 단원을 참조하십시오.

평가 템플릿 생성

평가 템플릿을 생성하려면

1. Sign in to the AWS Management 콘솔 and open the Amazon Inspector console at https://console.aws.amazon.com/inspector/.
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 Assessment Templates(평가 템플릿) 페이지에 있는 대상 미리 보기 버튼을 사용하여 평가 대상에 포함되어 있는 모든 EC2 instances를 검토할 수 있습니다. 각 EC2 instance에 대해 호스트 이름, 인스턴스 ID, IP 주소 및 해당되는 경우 에이전트의 상태를 검토할 수 있습니다. 에이전트 상태는 HEALTHY, UNHEALTHY 및 UNKNOWN 값을 가질 수 있습니다. Amazon Inspector는 EC2 instance에서 실행 중인 에이전트가 있는지 여부를 판단할 수 없을 때 UNKNOWN 상태를 표시합니다.
   Assessment Templates(평가 템플릿) 페이지에 있는 대상 미리 보기 버튼을 사용하여 이전에 생성된 템플릿에 포함되어 있는 평가 대상을 구성하는 EC2 instances를 검토할 수도 있습니다.
5. [Rules packages]에서 평가 템플릿에 포함시킬 하나 이상의 규칙 패키지를 선택합니다.
6. [Duration]에서 평가 템플릿의 기간을 지정합니다.
7. SNS 주제에서 Amazon Inspector가 평가 실행 상태 및 결과에 대한 알림을 보낼 SNS 주제를 지정합니다. Amazon Inspector는 다음 이벤트에 관하여 SNS 알림을 보냅니다.

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

   SNS 주제 설정에 대한 자세한 내용은 Amazon Inspector 알림에 대한 SNS 주제 설정 (p. 54) 단원을 참조하십시오.

8. (선택 사항) 태그에서 키 및 값 값을 입력합니다. 평가 템플릿에 여러 태그를 추가할 수 있습니다.
9. (선택 사항) 결과에 추가된 속성에 대해 키 및 값의 값을 입력합니다. Amazon Inspector는 평가 템플릿에 의해 생성된 모든 결과에 속성을 적용합니다. 평가 템플릿에 여러 속성을 추가할 수 있습니다. 결과 및 결과 태그 지정에 대한 자세한 내용은 Amazon Inspector 결과 (p. 56)를 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 선택하면 Amazon Inspector에서 설정 중인 평가 실행 일정에 대한 Amazon CloudWatch Events 규칙을 자동으로 생성해 줍니다. Amazon Inspector는 `AWS_InspectorEvents_Invoke_Assessment_Template`이라는 IAM 역할을 자동으로 생성합니다. CloudWatch 이벤트는 이 역할을 통해 Amazon Inspector 리소스를 API로 호출할 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 (p. 53) 단원을 참조하십시오.
11. [Create and run] 또는 [Create]를 선택합니다.

평가 템플릿 삭제

평가 템플릿을 삭제하려면 다음 절차를 수행하십시오.

평가 템플릿을 삭제하려면

- Assessment Templates(평가 템플릿) 페이지에서 삭제할 템플릿을 선택한 후 삭제를 선택합니다. 확인 메시지가 표시되면 [Yes]를 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. AWS 계정별 평가 실행 제한 내에 있는 한, 동일한 템플릿을 사용하여 여러 평가 실행을 시작할 수 있습니다. 자세한 내용은 Amazon Inspector 평가 실행 제한 (p. 53) 단원을 참조하십시오.

Amazon Inspector 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 실행을 위해 [Assessment templates] 페이지 또는 [Assessment runs] 페이지에서 [Run], [Cancel], [Delete] 버튼을 차례로 선택합니다.

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 평가 실행 제한

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

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

자세한 내용은 Amazon Inspector 서비스 제한 (p. 3) 단원을 참조하십시오.

Lambda 함수로 자동 평가 실행 설정

평가에 대한 반복 일정을 설정할 경우 AWS Lambda 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. AWS Management 콘솔에 로그인한 다음 AWS Lambda 콘솔을 엽니다.
2. 탐색 창에서 대시보드 또는 함수를 선택한 후 Create a Lambda Function(Lambda 함수 생성)을 선택합니다.
3. [Select blueprint] 페이지에서 [inspector-scheduled-run] 블루프린트를 선택합니다. 필터 필드에 **`inspector`**를 입력하여 이 블루프린트를 찾을 수 있습니다.
4. 트리거 구성 페이지에서 함수를 트리거하는 CloudWatch 이벤트를 지정하여 자동화된 실행에 대한 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 Amazon CloudWatch Events란 무엇입니까?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.
5. [Configure function] 페이지에서 다음을 지정합니다.
   - 이름에 함수의 이름을 입력합니다.
   - (선택 사항) 설명에 나중에 함수를 식별하는 데 도움이 되는 설명을 입력합니다.

- 실행 시간에서 기본값 **`Node.js 8.10`**을 유지합니다. AWS Lambda는 **`Node.js 8.10`** 실행 시간의 경우에만 inspector-scheduled-run 블루프린트를 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 단원을 참조하십시오.

  이 함수를 실행하려면 AWS Lambda가 실행을 시작하고 오류를 포함한 실행에 대한 로그 메시지를 Amazon CloudWatch Logs에 쓸 수 있게 해주는 IAM 역할이 필요합니다. AWS Lambda는 모든 자동화된 반복 평가 실행에 대해 이 역할을 맡습니다. 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": "*"
    }
  ]
}
```

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

Amazon Inspector 알림에 대한 SNS 주제 설정

Amazon Simple Notification Service(Amazon SNS)는 구독 엔드포인트 또는 클라이언트에 메시지를 보내는 웹 서비스입니다. Amazon SNS를 사용하여 Amazon Inspector에 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. Define who can publish messages to the topic(주제에 메시지를 게시할 수 있는 사람 정의)에서 Only the specified AWS accounts(지정된 AWS 계정만)를 선택한 후 주제를 생성할 리전의 계정에 대한 ARN을 입력합니다.

      - `## ##(####)` - arn:aws:iam::646659390643:root
      - `## ##(#### ##)` - arn:aws:iam::316112463485:root
      - `## ##(##### ## ##)` - arn:aws:iam::166987590008:root
      - `## ##(###)` - arn:aws:iam::758058086616:root
      - `### ###(###)` - arn:aws:iam::162588757376:root
      - `### ###(##)` - arn:aws:iam::526946625049:root
      - `### ###(###)` - arn:aws:iam::454640832652:root
      - `### ###(##)` - arn:aws:iam::406045910587:root

- `EU(######)` - arn:aws:iam::537503971621:root
- `EU(####)` - arn:aws:iam::357557129151:root
- `EU(##)` - arn:aws:iam::146838936955:root
- `EU(####)` - 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. Define who can subscribe to this topic(이 주제를 구독할 수 있는 사람 정의)에서 Only the specified AWS accounts(지정된 AWS 계정만)를 선택한 후 주제를 생성할 리전의 계정에 대한 ARN을 입력합니다.

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

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

Amazon Inspector 결과

결과는 평가 대상을 평가하는 동안 Amazon Inspector에서 발견할 수 있는 잠재적인 보안 문제입니다. 결과는 Amazon Inspector 콘솔에 표시되거나 API를 통해 검색됩니다. 결과에는 보안 문제 및 이를 해결하기 위한 권장 사항에 대한 자세한 설명이 포함되어 있습니다.

Amazon Inspector에서 결과를 생성하면 Amazon Inspector 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.

결과 작업

생성된 Amazon Inspector 결과에서 다음 절차를 수행합니다.

속성을 찾고, 분석하고, 결과에 할당

1. Sign in to the AWS Management 콘솔 and open the Amazon Inspector console at https://console.aws.amazon.com/inspector/.
2. 평가를 실행한 후 Amazon Inspector 콘솔에서 Findings 페이지로 이동하여 결과를 볼 수 있습니다.

   Amazon Inspector 콘솔의 Dashboard 페이지에 있는 Notable Findings 섹션에서 결과를 볼 수도 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 환경에서는 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 instance를 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.

- CIS(Center of Internet Security)의 기본 심각도 세부 정보. 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. Tags for findings from this assessment(이 평가의 결과 태그) 필드의 키 및 값 필드를 사용할 수 있습니다. 자세한 내용은 Amazon Inspector 평가 템플릿 및 평가 실행 (p. 50) 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.
6. 생성된 결과의 열을 표시하거나 숨기고, 생성된 결과를 필터링하려면 Findings(결과) 페이지의 오른쪽 상단 모서리에 있는 설정 아이콘을 선택합니다.
7. 결과를 삭제하려면 평가 실행 페이지로 가서 결과를 삭제할 실행을 선택합니다. 그런 다음 [Delete]를 선택합니다. 확인 메시지가 표시되면 [Yes]를 선택합니다.

   Important

   Amazon Inspector에서는 개별 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 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 Inspector에서 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**
   >
   > 2017년 4월 25일 이후에 수행했거나 수행할 평가 실행에 대해서만 보고서 열에 보고서 아이콘이 표시됩니다. 이는 Amazon Inspector에서 평가 보고서를 제공한 시점입니다.
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 [Yes]를 선택합니다.

  > **Important**
  >
  > Amazon Inspector에서는 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 Inspector의 제외

제외 항목은 Amazon Inspector 평가 실행의 출력입니다. 제외 항목은 사용자가 완료할 수 없는 보안 검사 및 해당 문제를 해결하는 방법을 보여 줍니다. 예를 들어 지정된 대상의 EC2 instance에 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 (p. 64) 단원을 참조하십시오.

불필요한 AWS 수수료 발생을 방지하기 위해 Amazon Inspector는 평가를 실행하기 전에 제외 항목을 미리 볼 수 있게 해 줍니다. 콘솔의 Assessment templates(평가 템플릿) 페이지에서 미리 보기를 확인할 수 있습니다. 자세한 내용은 제외 항목 미리 보기 (p. 63)를 참조하십시오.

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

주제

제외 유형

Amazon Inspector는 다음과 같은 제외 유형을 생성할 수 있습니다.

제외 유형	설명	권장 사항								
대상에 인스턴스 없음	평가 대상에 지정된 태그를 가진 EC2 instances가 없습니다.	평가 대상의 태그가 대상 EC2 인스턴스의 태그와 일치하는지 확인합니다.								
에이전트가 실행 중임	이미 대상EC2 instance에서 평가 실행이 진행 중입니다.	대상 EC2 instance에서 현재 평가 실행이 완료될 때까지 기다립니다.								
에이전트를 찾을 수 없음	대상 EC2 instance에서 Amazon Inspector 에이전트를 찾을 수 없습니다.	대상 EC2 instance에 Amazon Inspector 에이전트를 설치 또는 재설치합니다. 자세한 내용								

제외 유형	설명	권장 사항								
		은 Amazon Inspector 에이전트 설치 (p. 22)를 참조하십시오.								
에이전트에 이상이 있음	대상 EC2 instance의 Amazon Inspector 에이전트가 이상이 있는 상태입니다.	이 인스턴스에서 Amazon Inspector 에이전트의 상태를 확인하고 필요한 작업을 수행합니다. 자세한 내용은 Inspector 에이전트 단원을 참조하십시오.								
커널 모듈 사용 불가	대상 EC2 instance의 Amazon Inspector 에이전트에서 커널 모듈을 사용할 수 없습니다.	지원되는 커널 버전 목록은 Amazon Inspector 지원 운영 체제 및 리전을 참조하십시오.								
지원되지 않는 OS 버전	대상 EC2 instance의 운영 체제가 Amazon Inspector 평가를 지원하지 않습니다.	평가 대상에서 대상 EC2 instance를 제거하거나 이 인스턴스가 포함되지 않은 대상을 생성합니다. 지원되는 운영 체제 목록은 Amazon Inspector지원 운영 체제 및 리전을 참조하십시오.								
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 instance의 운영 체제가 평가 템플릿에 포함된 규칙 패키지에서 지원되지 않습니다.	충돌하는 규칙 패키지 없이 평가 템플릿을 생성하거나 평가 템플릿에서 대상 EC2 instance를 제거합니다. 운영 체제에서 지원되는 규칙 패키지 목록은 지원되는 운영 체제의 규칙 패키지 가용성을 참조하십시오.								
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.								
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 Balancer를 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.								
네트워크 연결성 오류 – Elastic Load Balancing 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.								
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 Connect	내부 오류로 인해 네트워크 연결성 평가가 AWS Direct Connect를 통해 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.								
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 Inspector에서는 평가를 실행하기 전에 잠재적인 제외 항목을 미리 볼 수 있게 해 줍니다.

평가 제외 항목을 미리 보려면

1. Sign in to the AWS Management 콘솔 and open the Amazon Inspector console at https://console.aws.amazon.com/inspector/.
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. Sign in to the AWS Management 콘솔 and open the Amazon Inspector console at https://console.aws.amazon.com/inspector/.
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 규칙 패키지

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

Important

운영 체제와 상관없이 모든 EC2 instance에서 네트워크 연결성 (p. 38) 규칙 패키지를 사용하여 에이전트 없는 평가를 실행할 수 있습니다.

Note

지원되는 운영 체제에 대한 자세한 내용은 Amazon Inspector 지원 운영 체제 및 리전 (p. 4) 단원을 참조하십시오.

지원되는 운영 체제	CVE(일반적인 취약성 및 노출도)	CIS 벤치마크	네트워크 연결성	보안 모범 사례	실행 시간 행동 분석
Amazon Linux 2 LTS, 2017.12	지원	지원	지원	지원	지원
Amazon Linux 2018.03	지원	지원	지원	지원	지원
Amazon Linux 2017.09	지원	지원	지원	지원	지원
Amazon Linux 2017.03	지원	지원	지원	지원	지원
Amazon Linux 2016.09	지원	지원	지원	지원	지원
Amazon Linux 2016.03	지원	지원	지원	지원	지원
Amazon Linux 2015.09	지원	지원	지원	지원	지원
Amazon Linux 2015.03	지원	지원	지원	지원	지원

지원되는 운영 체제	CVE(일반적인 취약성 및 노출도)	CIS 벤치마크	네트워크 연결성	보안 모범 사례	실행 시간 행동 분석
Amazon Linux 2014.09	지원		지원	지원	
Amazon Linux 2014.03	지원		지원	지원	
Amazon Linux 2013.09	지원		지원	지원	
Amazon Linux 2013.03	지원		지원	지원	
Amazon Linux 2012.09	지원		지원	지원	
Amazon Linux 2012.03	지원		지원	지원	
Ubuntu 18.04 LTS	지원		지원	지원	지원
Ubuntu 16.04 LTS	지원	지원	지원	지원	지원
Ubuntu 14.04 LTS	지원	지원	지원	지원	지원
Debian 9.0-9.5, 8.0-8.7	지원		지원	지원	
RHEL 7.6	지원	지원	지원	지원	
RHEL 6.2 - 6.9, 7.2 - 7.5	지원	지원	지원	지원	지원
CentOS 7.6	지원	지원	지원	지원	

지원되는 운영 체제	CVE(일반적인 취약성 및 노출도)	CIS 벤치마크	네트워크 연결성	보안 모범 사례	실행 시간 행동 분석
CentOS 6.2-6.9, 7.2-7.5	지원	지원	지원	지원	지원
Windows Server 2012 R2	지원	지원	지원		지원
Windows Server 2012	지원	지원	지원		지원
Windows Server 2008 R2	지원	지원	지원		지원
Windows Server 2016 Base	지원		지원		지원

AWS CloudTrail을 사용하여 Amazon Inspector API 호출 로깅

Amazon Inspector는 Amazon Inspector의 사용자, 역할 또는 AWS 서비스가 수행한 작업에 대한 레코드를 제공하는 서비스인 AWS CloudTrail과 통합됩니다. CloudTrail은 Amazon Inspector 콘솔의 호출 및 Amazon Inspector API 코드 호출 등 Amazon Inspector에 대한 모든 API 작업 호출을 이벤트로 캡처합니다. 추적을 생성하면 Amazon Inspector 이벤트를 비롯하여 CloudTrail 이벤트를 Amazon S3 버킷으로 지속적으로 배포할 수 있습니다. 추적을 구성하지 않은 경우 이벤트 기록에서 CloudTrail 콘솔의 최신 이벤트를 볼 수도 있습니다. CloudTrail에서 수집하는 정보를 사용하여 Amazon Inspector에 어떤 요청이 이루어졌는지, 어떤 IP 주소에서 요청했는지, 누가 언제 요청했는지 등을 확인할 수 있습니다.

CloudTrail에 대한 자세한 내용은 AWS CloudTrail User Guide을 참조하십시오. Amazon Inspector API 작업의 전체 목록은 Amazon InspectorAPI 참조에서 작업을 참조하십시오.

CloudTrail의 Amazon Inspector 정보

CloudTrail은 계정 생성 시 AWS 계정에서 활성화됩니다. Amazon Inspector에서 활동이 수행되면 해당 활동은 이벤트 기록에서 다른 AWS 서비스 이벤트와 함께 CloudTrail 이벤트에 기록됩니다. AWS 계정에서 최신 이벤트를 확인, 검색 및 다운로드할 수 있습니다. 자세한 내용은 CloudTrail 이벤트 기록에서 이벤트 보기를 참조하십시오.

Amazon Inspector 이벤트를 비롯하여 AWS 계정의 이벤트 기록을 보유하려면 추적을 생성하십시오. 추적은 CloudTrail이 Amazon S3 버킷으로 로그 파일을 전송할 수 있도록 합니다. 콘솔에서 추적을 생성하면 기본적으로 모든 AWS 리전에 추적이 적용됩니다. 추적은 AWS 파티션에 있는 모든 리전의 이벤트를 로깅하고 지정한 Amazon S3 버킷으로 로그 파일을 전송합니다. 또는 CloudTrail 로그에서 수집된 이벤트 데이터를 추가 분석 및 처리하도록 다른 AWS 서비스를 구성할 수 있습니다. 자세한 정보는 다음을 참조하십시오.

- 추적 생성 개요
- CloudTrail 지원 서비스 및 통합
- CloudTrail에 대한 Amazon SNS 알림 구성
- 여러 리전에서 CloudTrail 로그 파일 받기 및 여러 계정에서 CloudTrail 로그 파일 받기

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

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

모든 이벤트 및 로그 항목에는 요청을 생성한 사용자에 대한 정보가 들어 있습니다. 자격 증명 정보를 이용하면 다음을 쉽게 판단할 수 있습니다.

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

자세한 내용은 CloudTrail userIdentity 요소를 참조하십시오.

Amazon Inspector 로그 파일 항목 이해

추적은 지정한 Amazon S3 버킷에 이벤트를 로그 파일로 제공할 수 있도록 해 주는 구성입니다. CloudTrail 로그 파일에는 하나 이상의 로그 항목이 포함됩니다. 이벤트는 어떤 소스로부터의 단일 요청을 나타내며 요청된 작업, 작업 날짜와 시간, 요청 파라미터 등에 대한 정보가 들어 있습니다. CloudTrail 로그 파일은 퍼블릭 API 호출의 주문 스택 추적이 아니기 때문에 특정 순서로 표시되지 않습니다.

다음 예제는 Amazon Inspector `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 사용한 Amazon Inspector 모니터링

원시 데이터를 수집하고 읽을 수 있는 실시간 지표로 처리하는 Amazon CloudWatch를 사용하여 Amazon Inspector를 모니터링할 수 있습니다. 기본적으로 Amazon Inspector는 지표 데이터를 5분 내에 CloudWatch에 보냅니다. AWS Management 콘솔, AWS CLI 또는 API를 사용하여 Amazon Inspector가 CloudWatch에 전송하는 지표를 볼 수 있습니다.

Amazon CloudWatch에 대한 자세한 내용은 Amazon CloudWatch 사용 설명서를 참조하십시오.

Amazon Inspector CloudWatch 지표

Amazon Inspector 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			
`TotalAssessmentRunFindings`	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			
`TotalAssessmentRunFindings`	이 템플릿에 대한 결과 수			

집계 지표

지표	설명			
`TotalAssessmentRuns`	이 AWS 계정의 평가 실행 수			

AWS CloudFormation을 사용하여 Amazon Inspector 구성

AWS CloudFormation에서 지원하는 Amazon Inspector 리소스에 대한 참조 정보는 다음 주제를 참조하십시오.

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

> **Important**
>
> 지원되는 AWS 리전에 있는 Amazon Inspector 규칙 패키지의 ARM 목록은 규칙 패키지의 Amazon Inspector ARN (p. 80) 단원을 참조하십시오.

Amazon Inspector에 대한 인증 및 액세스 제어

Amazon Inspector에 액세스하려면 AWS가 요청을 인증하는 데 사용할 수 있는 자격 증명이 필요합니다. 이 자격 증명에는 Amazon Inspector 평가 대상, 평가 템플릿 또는 결과와 같은 AWS 리소스에 액세스할 수 있는 권한이 있습니다. 다음 단원에서는 리소스에 액세스할 수 있는 대상을 제어하여 리소스를 보호할 수 있도록 AWS Identity and Access Management(IAM) 및 Amazon Inspector를 사용하는 방법에 대한 세부 정보를 제공합니다.

인증

다음과 같은 ID 유형으로 AWS에 액세스할 수 있습니다.

- AWS 계정 루트 사용자 – AWS 계정을 처음 생성할 때는 해당 계정의 모든 AWS 서비스 및 리소스에 대한 완전한 액세스 권한이 있는 SSO(Single Sign-In) ID로 시작합니다. 이 자격 증명은 AWS 계정 루트 사용자라고 하며, 계정을 생성할 때 사용한 이메일 주소와 암호로 로그인하여 액세스합니다. 일상적인 작업은 물론 관리 작업에도 루트 사용자를 사용하지 않는 것이 좋습니다. 대신 IAM 사용자를 처음 생성할 때만 루트 사용자를 사용하는 모범 사례를 준수하십시오. 그런 다음 루트 사용자 자격 증명을 안전하게 보관해 두고 몇 가지 계정 및 서비스 관리 작업을 수행할 때만 해당 자격 증명을 사용합니다.
- IAM 사용자 – IAM 사용자는 특정 사용자 지정 권한(예: AWS Directory Service에서 a directory을 생성할 권한)이 있는 AWS 계정 내 자격 증명입니다. IAM 사용자 이름과 암호를 사용하여 AWS Management 콘솔, AWS 토론 포럼 또는 AWS Support Center 같은 보안 AWS 웹 페이지에 로그인할 수 있습니다.

  사용자 이름과 암호 외에도 각 사용자에 대해 액세스 키를 생성할 수 있습니다. 여러 SDK 중 하나를 통해 또는 AWS Command Line Interface(CLI)를 사용하여 AWS 제품에 프로그래밍 방식으로 액세스할 때 이러한 키를 사용할 수 있습니다. SDK 및 CLI 도구는 액세스 키를 사용하여 암호화 방식으로 요청에 서명합니다. AWS 도구를 사용하지 않는 경우 요청에 직접 서명해야 합니다. AWS Directory Service supports는 인바운드 API 요청을 인증하기 위한 프로토콜인 서명 버전 4를 지원합니다. 요청 인증에 대한 자세한 내용은 AWS General Reference의 서명 버전 4 서명 프로세스 단원을 참조하십시오.

- IAM 역할 – IAM 역할은 특정 권한을 가진 계정에서 생성할 수 있는 IAM 자격 증명입니다. IAM 역할은 AWS에서 자격 증명으로 할 수 있는 것과 할 수 없는 것을 결정하는 권한 정책을 포함하는 AWS 자격 증명이라는 점에서 IAM 사용자와 유사합니다. 그러나 역할은 한 사람과만 연관되지 않고 해당 역할이 필요한 사람이라면 누구든지 맡을 수 있어야 합니다. 또한 역할에는 그와 연관된 암호 또는 액세스 키와 같은 표준 장기 자격 증명이 없습니다. 대신에 역할을 수임한 사람에게는 해당 역할 세션을 위한 임시 보안 자격 증명이 제공됩니다. 임시 자격 증명이 있는 IAM 역할은 다음과 같은 상황에서 유용합니다.

  - 연합된 사용자 액세스 – IAM 사용자를 생성하는 대신 AWS Directory Service의 기존 ID, 엔터프라이즈 사용자 디렉터리 또는 웹 ID 공급자를 사용할 수 있습니다. 이 사용자를 연합된 사용자라고 합니다. AWS에서는 ID 공급자를 통해 액세스가 요청되면 연합된 사용자에게 역할을 할당합니다. 연합된 사용자에 대한 자세한 내용은 IAM 사용 설명서의 연합된 사용자 및 역할을 참조하십시오.

- AWS 서비스 액세스 – 서비스 역할은 서비스가 사용자를 대신하여 사용자 계정에서 작업을 수행하기 위해 수임하는 IAM 역할입니다. 일부 AWS 서비스 환경을 설정할 때 서비스에서 맡을 역할을 정의해야 합니다. 이 서비스 역할에는 서비스가 AWS 리소스에 액세스하는 데 필요한 모든 권한이 포함되어야 합니다. 서비스 역할은 서비스마다 다르지만 해당 서비스에 대한 문서화된 요구 사항을 충족하는 한 대부분의 경우 권한을 선택할 수 있습니다. 서비스 역할은 해당 계정 내 액세스 권한만 제공하며 다른 계정의 서비스에 대한 액세스 권한을 부여하는 데 사용될 수 없습니다. IAM 내에서 서비스 역할을 생성, 수정 및 삭제할 수 있습니다. 예를 들어 Amazon Redshift에서 사용자 대신 Amazon S3 버킷에 액세스하도록 허용하는 역할을 생성한 후 해당 버킷에 있는 데이터를 Amazon Redshift 클러스터로 로드할 수 있습니다. 자세한 내용은 IAM 사용 설명서의 AWS 서비스에 대한 권한을 위임할 역할 생성을 참조하십시오.

- Amazon EC2에서 실행 중인 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 해당 역할을 모든 애플리케이션에서 사용할 수 있도록 하려면 인스턴스에 연결된 인스턴스 프로파일을 생성합니다. 인스턴스 프로파일에는 역할이 포함되어 있으며 EC2 인스턴스에서 실행되는 프로그램이 임시 자격 증명을 얻을 수 있습니다. 자세한 내용은 IAM 사용 설명서의 IAM 역할을 사용하여 Amazon EC2 인스턴스에서 실행되는 애플리케이션에 권한 부여를 참조하십시오.

액세스 제어

요청을 인증할 수 있는 유효한 자격 증명이 있더라도 권한이 없다면 Amazon Inspector 리소스를 생성하거나 액세스할 수 없습니다. 예를 들어 Amazon Inspector 평가 대상 및 평가 템플릿을 생성하여 평가를 실행할 수 있는 권한이 있어야 합니다.

다음 단원에서는 Amazon Inspector에 대한 권한을 관리하는 방법을 설명합니다. 먼저 개요를 읽어 보면 도움이 됩니다.

Amazon Inspector 리소스에 대한 액세스 권한 관리 개요

모든 AWS 리소스는 AWS 계정의 소유이고, 리소스 생성 또는 리소스 액세스 권한은 AWS Identity and Access Management(IAM) 권한 정책에 따라 결정됩니다. 계정 관리자는 IAM 자격 증명(사용자, 그룹 및 역할)에 권한 정책을 연결할 수 있습니다. AWS Lambda 같은 일부 서비스에서도 권한 정책을 리소스에 연결할 수 있습니다.

> Note
>
> 계정 관리자 또는 관리자 사용자는 관리자 권한이 있는 IAM 사용자입니다. 자세한 내용은 IAM 사용 설명서의 IAM 모범 사례를 참조하십시오.

권한을 부여하려면 권한을 부여 받을 사용자, 권한 대상이 되는 리소스, 해당 리소스에 허용되는 특정 작업을 결정합니다.

주제

Amazon Inspector 리소스 및 작업

Amazon Inspector에서 주 리소스는 리소스 그룹, 평가 대상, 평가 템플릿, 평가 실행 및 결과입니다. 다음 표에서처럼 이러한 리소스에는 고유한 Amazon Resource Name(ARN)이 연결됩니다.

리소스 유형	ARN 형식
리소스 그룹	`arn:aws:inspector:region:account-id:resourcegroup/ID`
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`
결과	`arn:aws:inspector:region:account-id:target/ID/template/ID/run/ID/finding/ID`

Amazon Inspector은(는) Amazon Inspector 리소스를 처리하기 위한 작업을 제공합니다. 사용 가능한 작업 목록은 작업을(를) 참조하십시오.

리소스 소유권 이해

리소스 소유자는 리소스를 생성하는 AWS 계정입니다. 즉, 리소스 소유자는 리소스를 생성하는 요청을 인증하는 보안 주체 엔터티(루트 계정, IAM 사용자 또는 IAM 역할)의 AWS 계정입니다. 다음 예에서는 이 계정의 작동 방식을 설명합니다.

- AWS 계정의 루트 계정 자격 증명을 사용하여 Amazon Inspector 평가 대상을 생성하는 경우, AWS 계정이 이 리소스 소유자가 됩니다.
- AWS 계정에서 IAM 사용자를 생성하고 해당 사용자에게 평가 대상을 생성할 수 있는 권한을 부여하는 경우 이 사용자가 평가 대상을 생성할 수 있습니다. 하지만 평가 대상 리소스는 해당 사용자가 속한 AWS 계정이 소유합니다.
- 평가 대상을 생성할 권한이 있는 AWS 계정에서 IAM 역할을 생성하는 경우 해당 역할을 담당할 수 있는 사람은 누구나 평가 대상을 생성할 수 있습니다. 하지만 Amazon Inspector 평가 대상 리소스는 해당 역할이 속한 AWS 계정이 소유합니다.

리소스 액세스 관리

권한 정책은 누가 무엇에 액세스 할 수 있는지를 나타냅니다. 다음 단원에서는 권한 정책을 만드는 데 사용 가능한 옵션에 대해 설명합니다.

> **Note**
>
> 이 단원에서는 Amazon Inspector의 맥락에서 IAM을 사용하는 방법에 대해 설명하며, IAM 서비스에 대한 자세한 내용은 다루지 않습니다. 전체 IAM 설명서는 IAM 사용 설명서의 IAM이란 무엇인가?를

참조하십시오. IAM 정책 구문과 설명에 대한 자세한 내용은 IAM 사용 설명서의 AWS IAM 정책 참조를 참조하십시오.

IAM 자격 증명에 연결된 정책은 자격 증명 기반 정책(IAM 정책)이라고 합니다. 리소스에 연결된 정책은 리소스 기반 정책 이라고 합니다. Amazon Inspector는 자격 증명 기반 정책만 지원합니다.

주제

자격 증명 기반 정책(IAM 정책)

정책을 IAM 자격 증명에 연결할 수 있습니다. 예를 들면,

- 계정 내 사용자 또는 그룹에 권한 정책 연결 – 계정 관리자는 IAM 사용자에 연결된 권한 정책을 사용하여 해당 사용자에게 평가 대상 생성 권한을 부여할 수 있습니다.
- 역할에 권한 정책 연결(교차 계정 권한 부여) – 자격 증명 기반 권한 정책을 IAM 역할에 연결하여 교차 계정 권한을 부여할 수 있습니다. 예를 들어, 계정 A의 관리자는 다음과 같이 다른 AWS 계정(예: 계정 B) 또는 AWS 서비스에 교차 계정 권한을 부여할 역할을 생성할 수 있습니다.
  - 계정 A 관리자는 IAM 역할을 생성하고 계정 A의 리소스에 대한 권한을 부여하는 권한 정책을 역할에 연결합니다.
  - 계정 A 관리자는 계정 B를 역할을 수임할 보안 주체로 식별하는 역할에 신뢰 정책을 연결합니다.
  - 계정 B 관리자는 계정 B의 사용자에게 역할을 수임할 권한을 위임할 수 있습니다. 그러면 계정 B의 사용자가 계정 A에서 리소스를 생성하거나 액세스할 수 있습니다. AWS 서비스에 역할 수임 권한을 부여할 경우, 신뢰 정책의 보안 주체가 AWS 서비스 보안 주체이기도 합니다.

  IAM을 사용하여 권한을 위임하는 방법에 대한 자세한 내용은 IAM 사용 설명서의 액세스 관리를 참조하십시오.

다음은 모든 리소스의 `inspector:ListFindings` 작업에 대한 권한을 부여하는 정책의 예시입니다.

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

Amazon Inspector에서 자격 증명 기반 정책을 사용하는 방법에 대한 자세한 내용은 Amazon Inspector에 대한 자격 증명 기반 정책(IAM 정책) 사용 (p. 76) 단원을 참조하십시오. 사용자, 그룹, 역할 및 권한에 대한 자세한 내용은 IAM 사용 설명서의 자격 증명(사용자, 그룹 및 역할)을 참조하십시오.

리소스 기반 정책

Amazon S3와 같은 다른 서비스도 리소스 기반 권한 정책을 지원합니다. 예를 들어, 정책을 S3 버킷에 연결하여 해당 버킷에 대한 액세스 권한을 관리할 수 있습니다. Amazon Inspector는 리소스 기반 정책을 지원하지 않습니다.

정책 요소 지정: 작업, 효과, 리소스, 보안 주체

각 Amazon Inspector 리소스(Amazon Inspector 리소스 및 작업 (p. 74) 참조)에 대해 서비스는 API 작업을 정의합니다(작업 참조). 이러한 API 작업에 대한 권한을 부여하기 위해 Amazon Inspector에서는 정책에서 지정할 수 있는 작업을 정의합니다. API 작업을 실시하려면 둘 이상의 작업에 대한 권한이 필요할 수 있습니다. 특정 작업에 대한 권한을 부여할 때 해당 작업이 허용되거나 거부되는 리소스도 식별합니다.

다음은 가장 기본적인 정책 요소입니다.

- 리소스 – 정책에서 Amazon 리소스 이름(ARN)을 사용하여 정책을 적용할 리소스를 식별합니다. 자세한 내용은 Amazon Inspector 리소스 및 작업 (p. 74) 단원을 참조하십시오.
- 작업 – 작업 키워드를 사용하여 허용 또는 거부할 리소스 작업을 식별합니다. 예를 들어, `inspector:ListFindings` 권한은 사용자에게 Amazon Inspector `ListFindings` 작업 수행 권한을 허용합니다.
- 효과 – 사용자가 특정 작업을 요청할 때 결과를 지정합니다. 효과는 거부 또는 허용일 수 있습니다. 리소스를 허용하기 위한 액세스 권한을 명시적으로 부여하지 않으면 액세스가 암시적으로 거부됩니다. 리소스에 대한 액세스를 명시적으로 거부할 수도 있습니다. 다른 정책에서 액세스 권한을 부여하더라도 사용자가 해당 리소스에 액세스할 수 없도록 하려고 할 때 이러한 작업을 수행할 수 있습니다.
- 보안 주체 – 자격 증명 기반 정책(IAM 정책)에서 정책이 연결되는 사용자는 암시적인 보안 주체입니다.

IAM 정책 구문과 설명에 대한 자세한 내용은 IAM 사용 설명서의 AWS IAM 정책 참조를 참조하십시오.

모든 Amazon Inspector API 작업과 해당 작업이 적용되는 리소스를 보여주는 표는 Amazon Inspector API 권한: 작업, 리소스 및 조건 참조 (p. 78) 단원을 참조하십시오.

정책에서 조건 지정

권한을 부여할 때 IAM 정책 언어를 사용하여 정책을 시행하기 위해 충족해야 하는 조건을 지정할 수 있습니다. 예를 들어, 특정 날짜 이후에만 정책을 적용할 수 있습니다. 정책 언어에서의 조건 지정에 관한 자세한 내용은 IAM 사용 설명서의 조건을 참조하십시오.

조건을 표시하려면 미리 정의된 조건 키를 사용합니다. Amazon Inspector에 특정한 조건 키는 없습니다. 하지만 필요에 따라 사용할 수 있는 AWS 조건 키는 있습니다. AWS 키의 전체 목록은 IAM 사용 설명서의 사용 가능한 조건 키를 참조하십시오.

Amazon Inspector에 대한 자격 증명 기반 정책(IAM 정책) 사용

이 장에서는 IAM 정책이라고도 알려진 자격 증명 기반 권한 정책의 예를 제공합니다. 계정 관리자는 IAM 자격 증명(사용자, 그룹 및 역할)에 이러한 권한 정책을 연결할 수 있습니다.

> **Important**
>
> Amazon Inspector 리소스에 대한 액세스 관리를 위해 제공되는 기본 개념과 옵션 설명에 대한 소개 주제 부분을 우선 읽어 보는 것이 좋습니다. 자세한 내용은 Amazon Inspector 리소스에 대한 액세스 권한 관리 개요 (p. 73) 단원을 참조하십시오.

이 장의 단원에서는 다음 내용을 학습합니다.

- Amazon Inspector 콘솔 사용에 필요한 권한 (p. 77)
- Amazon Inspector에 대한 AWS 관리형(미리 정의된) 정책 (p. 77)
- 고객 관리형 정책 예 (p. 77)

다음은 권한 정책의 예제입니다.

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

이 예제 정책은 Amazon Inspector 결과를 나열할 수 있는 권한을 부여하는 명령문을 포함합니다. Amazon Inspector는 리소스 수준에서 이 특정 작업에 대한 권한을 지원하지 않습니다. 따라서 정책은 와일드카드 문자(*)를 `Resource` 값으로 지정합니다.

Amazon Inspector 콘솔 사용에 필요한 권한

Amazon Inspector 콘솔을 사용하려면 사용자는 Amazon Inspector에 대한 AWS 관리형 (미리 정의된) 정책 (p. 77)에 설명되어 있는 `AmazonInspectorFullAccess` 또는 `AmazonInspectorReadOnlyAccess` 정책이 부여한 권한을 가지고 있어야 합니다. 이러한 정책(예: 앞의 예제 정책)에 나온 최소 필수 권한보다 더 제한적인 IAM 정책을 만들면 콘솔은 해당 정책에 연결된 사용자에 대해 의도대로 작동하지 않습니다.

> **Note**
>
> 앞의 예제 정책과 연결된 IAM 사용자는 `ListFindings` API 작업 또는 `list-findings` CLI 명령을 호출하여 Amazon Inspector 결과를 성공적으로 나열할 수 있습니다.

Amazon Inspector에 대한 AWS 관리형(미리 정의된) 정책

AWS는 AWS에서 생성하고 관리하는 독립형 IAM 정책을 제공하여 많은 일반 사용 사례를 처리합니다. 이러한 관리형 정책은 사용자가 필요한 권한을 조사할 필요가 없도록 일반 사용 사례에 필요한 권한을 부여합니다. 자세한 내용은 IAM 사용 설명서의 AWS 관리형 정책을 참조하십시오.

계정의 IAM 사용자에게 연결할 수 있는 다음 AWS 관리형 정책은 Amazon Inspector에 대해 고유합니다.

- `AmazonInspectorFullAccess` – Amazon Inspector에 대한 모든 액세스 권한을 제공합니다.
- `AmazonInspectorReadOnlyAccess` – Amazon Inspector에 대한 읽기 전용 액세스 권한을 제공합니다.

사용자에게 필요한 API 작업 및 리소스에 액세스하도록 허용하는 사용자 지정 IAM 정책을 생성할 수도 있습니다. 해당 권한이 필요한 IAM 사용자 또는 그룹에 이러한 사용자 지정 정책을 연결할 수 있습니다.

고객 관리형 정책 예

이 단원에서는 다양한 Amazon Inspector 작업에 대한 권한을 부여하는 사용자 정책의 예를 제공합니다.

> **Note**
>
> 모든 예에서는 미국 서부(오리건) 리전(`us-west-2`)을 사용하며 가상의 계정 ID를 포함합니다.

예제

예제 1: 사용자가 모든 Amazon Inspector 리소스에서 Describe 및 List 작업을 수행할 수 있도록 허용

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 API 권한: 작업, 리소스 및 조건 참조

다음 표에는 Amazon Inspector API 작업이 각각 나열되어 있습니다. 또한 작업을 수행할 권한을 부여하는 데 사용하는 해당 작업 및 권한을 부여할 수 있는 AWS 리소스가 나열되어 있습니다. IAM 자격 증명에 연결할

수 있는 액세스 제어 (p. 73) 및 쓰기 권한 정책(자격 증명 기반 정책)을 설정할 때 다음 표를 참조로 사용합니다. 정책의 `Action` 필드에서 작업을 지정하고 정책의 `Resource` 필드에서 리소스 값을 지정합니다.

Amazon Inspector 정책에서 AWS 조건 키를 사용하여 조건을 표시할 수 있습니다. AWS 키의 전체 목록은 IAM 사용 설명서의 사용 가능한 조건 키를 참조하십시오.

Note

작업을 지정하려면 `inspector:` 접두사 다음에 API 작업 이름을 사용합니다(예: `inspector:CreateResourceGroup`).

규칙 패키지의 Amazon Inspector ARN

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

주제

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
실행 시간 행동 분석	arn:aws:inspector:us-east-2:646659390643:rulespackage/0-UCYZFKPV

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-1:316112463485: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
실행 시간 행동 분석	arn:aws:inspector:us-east-1:316112463485:rulespackage/0-gBONHN9h

미국 서부(캘리포니아 북부 지역)

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-1:166987590008:rulespackage/0-byoQRFYm
실행 시간 행동 분석	arn:aws:inspector:us-west-1:166987590008:rulespackage/0-yeYxlt0x

미국 서부(오레곤)

규칙 패키지 이름	ARN
CVE(일반적인 취약성 및 노출도)	arn:aws:inspector:us-west-2:758058086616:rulespackage/0-9
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
실행 시간 행동 분석	arn:aws:inspector:us-west-2:758058086616:rulespackage/0-vg5GGHSD

아시아 태평양(뭄바이)

규칙 패키지 이름	ARN
CVE(일반적인 취약성 및 노출도)	arn:aws:inspector:ap-south-1:162588757376: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
실행 시간 행동 분석	arn:aws:inspector:ap-south-1:162588757376:rulespackage/0-EhMQZy6C

아시아 태평양(서울)

규칙 패키지 이름	ARN
CVE(일반적인 취약성 및 노출도)	arn:aws:inspector:ap-northeast-2:526946625049:rulespackag PoGHMznc
CIS 운영 체제 보안 구성 벤치마크	arn:aws:inspector:ap-northeast-2:526946625049:rulespackag T9srhg1z
네트워크 연결성	arn:aws:inspector:ap-northeast-2:526946625049:rulespackag s3OmLzhL
보안 모범 사례	arn:aws:inspector:ap-northeast-2:526946625049:rulespackag
실행 시간 행동 분석	arn:aws:inspector:ap-northeast-2:526946625049:rulespackag PoYq7lI7

아시아 태평양(시드니)

규칙 패키지 이름	ARN
CVE(일반적인 취약성 및 노출도)	arn:aws:inspector:ap-southeast-2:454640832652:rulespackag D5TGAxiR
CIS 운영 체제 보안 구성 벤치마크	arn:aws:inspector:ap-southeast-2:454640832652:rulespackag Vkd2Vxjq
네트워크 연결성	arn:aws:inspector:ap-southeast-2:454640832652:rulespackag FLcuV4Gz
보안 모범 사례	arn:aws:inspector:ap-southeast-2:454640832652:rulespackag asL6HRgN
실행 시간 행동 분석	arn:aws:inspector:ap-southeast-2:454640832652:rulespackag P8Tel2Xj

아시아 태평양(도쿄)

규칙 패키지 이름	ARN
CVE(일반적인 취약성 및 노출도)	arn:aws:inspector:ap-northeast-1:406045910587:rulespackag gHP9oWNT
CIS 운영 체제 보안 구성 벤치마크	arn:aws:inspector:ap-northeast-1:406045910587:rulespackag
네트워크 연결성	arn:aws:inspector:ap-northeast-1:406045910587:rulespackag YI95DVd7
보안 모범 사례	arn:aws:inspector:ap-northeast-1:406045910587:rulespackag bBUQnxMq
실행 시간 행동 분석	arn:aws:inspector:ap-northeast-1:406045910587:rulespackag knGBhqEu

EU(프랑크푸르트)

규칙 패키지 이름	ARN
CVE(일반적인 취약성 및 노출도)	arn:aws:inspector:eu-central-1:537503971621:rulespackage/ wNqHa8M9
CIS 운영 체제 보안 구성 벤치마크	arn:aws:inspector:eu-central-1:537503971621:rulespackage/ nZrAVuv8
네트워크 연결성	arn:aws:inspector:eu-central-1:537503971621:rulespackage/
보안 모범 사례	arn:aws:inspector:eu-central-1:537503971621:rulespackage/ ZujVHEPB
실행 시간 행동 분석	arn:aws:inspector:eu-central-1:537503971621:rulespackage/

EU(아일랜드)

규칙 패키지 이름	ARN
CVE(일반적인 취약성 및 노출도)	arn:aws:inspector:eu-west-1:357557129151:rulespackage/0- ubA5XvBh

규칙 패키지 이름	ARN
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-1:357557129151:rulespackage/0-SnojL3Z6
실행 시간 행동 분석	arn:aws:inspector:eu-west-1:357557129151:rulespackage/0-lLmwe1zd

EU(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
실행 시간 행동 분석	arn:aws:inspector:eu-west-2:146838936955:rulespackage/0-S8t0UlXB

EU(스톡홀름)

규칙 패키지 이름	ARN
CVE(일반적인 취약성 및 노출도)	arn:aws:inspector:eu-north-1:453420244670:rulespackage/0-IgdgIewd
CIS 운영 체제 보안 구성 벤치마크	arn:aws:inspector:eu-north-1:453420244670:rulespackage/0-Yn8jlX7f

규칙 패키지 이름	ARN
네트워크 연결성	arn:aws:inspector:eu-north-1:453420244670:rulespackage/0-
보안 모범 사례	arn:aws:inspector:eu-north-1:453420244670:rulespackage/0-HfBQSbSf
실행 시간 행동 분석	arn:aws:inspector:eu-north-1:453420244670:rulespackage/0-bwwFfRbF

AWS GovCloud(US-East)

규칙 패키지 이름	ARN
CVE(일반적인 취약성 및 노출도)	arn:aws-us-gov:inspector:us-gov-east-1:206278770380:rulespackage/0-3
CIS 운영 체제 보안 구성 벤치마크	arn:aws-us-gov:inspector:us-gov-east-1:206278770380:rulespackage/0-pTLCdIww
보안 모범 사례	arn:aws-us-gov:inspector:us-gov-east-1:206278770380:rulespackage/0-vlgEGcVD
실행 시간 행동 분석	arn:aws-us-gov:inspector:us-gov-east-1:206278770380:rulespackage/0-8

AWS GovCloud (US-West)

규칙 패키지 이름	ARN
CVE(일반적인 취약성 및 노출도)	arn:aws-us-gov:inspector:us-gov-west-1:850862329162:rulespackage/0-4
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

규칙 패키지 이름	ARN
실행 시간 행동 분석	`arn:aws-us-gov:inspector:us-gov-west-1:850862329162:rulespackage/0-JMyjuzoW`

문서 기록

설명서 최종 업데이트: 2018년 11월 12일

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

update-history-change	update-history-description	update-history-date
추가된 OS 지원 (p. 88)	CentOS 7.6에 대한 Amazon Inspector 지원이 추가되었습니다. 자세한 내용은 Amazon Inspector 지원 운영 체제 및 리전 및 지원되는 운영 체제의 규칙 패키지 가용성을 참조하십시오.	December 3, 2018
새 콘텐츠 (p. 88)	Amazon Inspector 네트워크 연결성 규칙 패키지가 추가되어 사용자가 에이전트 없이 보안 취약성에 대한 네트워크 구성을 분석하는 평가를 실행할 수 있습니다. 자세한 내용은 Network Reachability 단원을 참조하십시오.	November 9, 2018
추가된 OS 지원 (p. 88)	RHEL 7.6에 대한 Amazon Inspector 지원이 추가되었습니다. 자세한 내용은 Amazon Inspector 지원 운영 체제 및 리전 및 지원되는 운영 체제의 규칙 패키지 가용성을 참조하십시오.	October 30, 2018
추가된 OS 지원 (p. 88)	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.	August 13, 2018
추가된 리전 지원 (p. 88)	`AWS GovCloud (US)`에 대한 리전 지원이 추가되었습니다.	June 13, 2018

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

변경 사항	설명	날짜
새 콘텐츠	계정의 모든 Amazon EC2 인스턴스를 대상으로 할 수 있는 기능이 추가되었습니다. 자세한 내용은 Amazon Inspector 평가 대상 (p. 34) 단원을 참조하십시오.	2018년 5월 24일
추가된 OS 지원	Amazon Linux 2018.03 및 Ubuntu 18.04에 대해 Amazon Inspector 지원이 추가되었습니다.	2018년 5월 15일

변경 사항	설명	날짜
새 콘텐츠	반복적인 Amazon Inspector 평가를 설정하는 기능이 추가되었습니다.	2018년 30월 4일
새 콘텐츠	콘솔을 통해 Amazon Inspector 에이전트를 설치할 수 있는 기능이 추가되었습니다.	2018년 30월 4일
추가된 OS 지원	Amazon Linux에 대한 Amazon Inspector 지원 추가.	2018년 3월 13일
추가된 OS 지원	Windows Server 2016 Base에 대한 Amazon Inspector 평가 지원이 추가되었습니다.	2018년 2월 20일
추가된 리전 지원	`US East (Ohio)` 리전에 대한 Amazon Inspector 지원이 추가되었습니다.	2018년 2월 7일
새 콘텐츠	이제 커널 모듈을 사용할 수 없을 때 Amazon Inspector 평가가 실행될 수 있습니다.	2018년 1월 11일
추가된 리전 지원	`EU (Frankfurt)` 리전에 대한 Amazon Inspector 지원이 추가되었습니다.	2017년 12월 19일
새 콘텐츠	Amazon Inspector API 및 콘솔을 통해 Amazon Inspector 에이전트 상태를 점검할 수 있는 기능이 추가되었습니다.	2017년 12월 15일
새 콘텐츠	다음 기능을 추가했습니다. • 서비스 연결 역할 사용 • AWS Marketplace에서 사용 가능한 Amazon Inspector 에이전트 AMI • Amazon Inspector AWS CloudFormation 템플릿	2017년 12월 5일
추가된 OS 지원	CentOS 7.4에 대해 Amazon Inspector 평가 지원이 추가되었습니다.	2017년 11월 9일
추가된 OS 지원	Amazon Linux 2017.09에 대해 Amazon Inspector 평가 지원이 추가되었습니다.	2017년 10월 11일
추가된 OS 지원	RHEL 7.4에 대해 Amazon Inspector 평가 지원이 추가되었습니다.	2018년 2월 20일
추가된 HIPAA 자격	Amazon Inspector은 이제 HIPAA 자격이 있습니다.	2017년 7월 31일

변경 사항	설명	날짜
새 콘텐츠	Amazon CloudWatch 이벤트를 사용하여 자동으로 Amazon Inspector 보안 평가를 트리거할 수 있는 기능이 추가되었습니다.	2017년 7월 27일
추가된 리전 지원	`US West (N. California)` 리전에 대한 Amazon Inspector 지원이 추가되었습니다.	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 평가 지원이 추가되었습니다.	2017년 5월 23일
추가된 OS 지원	Amazon Linux 2017.03에 대해 Amazon Inspector 평가 지원이 추가되었습니다.	2017년 4월 25일
새로운 콘텐츠 및 추가된 OS 지원	추가된 내용: • Ubuntu 16.04에 대한 Amazon Inspector 지원이 추가되었습니다. • Amazon Inspector 작업 자동화를 위한 Lambda 블루프린트의 가용성입니다.	2017년 1월 5일
새로운 OS 지원	Microsoft Windows에 대한 Amazon Inspector 지원이 추가되었습니다.	2016년 8월 26일
추가된 리전 지원	`Asia Pacific (Seoul)` 리전에 대한 Amazon Inspector 지원이 추가되었습니다.	2016년 8월 26일
추가된 리전 지원	`Asia Pacific (Mumbai)` 리전에 대한 Amazon Inspector 지원이 추가되었습니다.	2016년 4월 25일
추가된 리전 지원	`Asia Pacific (Sydney)` 리전에 대한 Amazon Inspector 지원이 추가되었습니다.	2016년 4월 25일
검색 시작	Amazon Inspector 서비스가 시작되었습니다.	2015년 10월 7일

AWS Glossary

For the latest AWS terminology, see the AWS Glossary in the AWS General Reference.