관리자 안내서

Amazon Nimble Studio

Amazon Nimble Studio: 관리자 안내서

Table of Contents

지원 종료 공지: 2024년 10월 22일에는 Amazon Nimble Studio에 대한 지원을 중단할 AWS 예정입니다. 2024년 10월 22일 이후에는 Nimble Studio 콘솔 또는 Nimble Studio 리소스에 더 이상 액세스할 수 없습니다.

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

Amazon Nimble Studio란 무엇인가요?

Nimble Studio는 아티스트가 클라우드에서 시각 효과, 애니메이션 및 게임 콘텐츠를 제작하는 데 사용할 수 있는 애플리케이션 제품군과 서비스를 위한 인프라와 중앙 집중식 관리를 제공합니다.

Nimble Studio에서 사용자 및 그룹 관리에 필수적인 도구를 얻을 수 있습니다. 및 Nimble Studio 파일 전송을 포함한 AWS Thinkbox 애플리케이션을 추가하고 관리할 수도 있습니다.

Nimble Studio는 모든 스튜디오 리소스가 한 곳에 모여 있는 통합 인터페이스를 제공합니다. 사용자를 온보딩하고, 애플리케이션을 할당하고, 직무에 맞는 권한을 연결할 수 있습니다. Nimble Studio에는 AWS 경험이 필요하지 않으며 약 5분 내에 설정할 수 있습니다.

내용

기능 및 이점

Nimble Studio에서 얻을 수 있는 몇 가지 기능 및 이점은 다음과 같습니다.

- Nimble Studio는 무료로 사용할 수 있습니다. 애플리케이션이 사용하는 스튜디오 리소스에 대해서만 비용을 지불하면 됩니다.
- 스튜디오를 중앙에서 관리하고, 상태를 확인하고, 운영에 대한 높은 수준의 인사이트를 얻을 수 있습니다.
- Nimble Studio 애플리케이션, 사용자, 그룹을 추가 및 관리하고 권한을 연결할 수 있습니다.
- AWS Identity and Access Management (IAM) 정책 및 역할을 사용하여 스튜디오 리소스에 대한 액세스를 안전하게 관리합니다.
- AWS IAM Identity Center (IAM Identity Center)를 사용하여 스튜디오 사용자 및 외부 자격 증명 공급자의 로그인 보안을 관리할 수 있습니다.
- 스튜디오 리소스에 태그를 지정하여 스튜디오 리소스를 구성하고 쉽게 찾을 수 있습니다.

관련 애플리케이션

Nimble Studio는 디지털 콘텐츠 제작자가 시각 효과(VFX), 애니메이션, 인터랙티브 콘텐츠 제작을 위한 클라우드 기반 스튜디오를 운영할 수 있는 애플리케이션을 제공합니다.

Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스를 사용하여 로컬 컴퓨터나 클라우드에 이러한 애플리케이션을 설치할 수 있습니다. Amazon Simple Storage Service(Amazon S3)를 사용하여 디지털 미디어 자산을 안전하게 전송 및 저장할 수도 있습니다. 즉, Nimble Studio를 사용하면 물리적 인프라, 장비, 기술 인력 비용을 절감할 수 있습니다.

Nimble Studio가 현재 제공하는 애플리케이션은 다음과 같습니다.

- AWS Thinkbox: Thinkbox 소프트웨어에는 렌더 팜 관리자 Thinkbox Deadline과 3D 플러그인 Thinkbox Krakatoa가 포함되어 있습니다. Thinkbox 소프트웨어를 사용하면 온프레미스에서, Amazon EC2가 있는 클라우드에서, 또는 이 둘의 조합에서 스튜디오의 크리에이티브 결과물을 높일 수 있습니다. 자세한 내용은 AWS Thinkbox 제품을 참조하세요.
- Nimble Studio File Transfer: File Transfer는 Amazon S3와 주고받는 디지털 미디어 자산의 미디어 자산 전송을 가속화합니다. File Transfer는 수천 개의 큰 미디어 파일을 빠르게 이동하는 데 사용할 수 있는 그래픽 사용자 인터페이스를 제공합니다. 자세한 내용은 Nimble Studio File Transfer란 무엇인가요? 페이지를 참조하세요.

Nimble Studio 요금

Nimble Studio는 무료로 설치하고 스튜디오 인프라, 사용자, 보안, 서비스를 관리하는 데 사용할 수 있습니다.

하지만 스튜디오에서 서비스와 애플리케이션을 설정하는 경우 스토리지 및 기타 스튜디오 리소스에 대한 요금이 부과될 수 있습니다. Nimble Studio 애플리케이션 요금에 대한 자세한 내용은 개별 애플리케이션의 요금 페이지를 참조하세요.

AWS 비용 관리에 대한 자세한 내용은 AWS Cost Explorer Service 및 섹션을 참조하세요AWS Budgets.

Nimble Studio 시작하기

Nimble Studio 설치 및 배포에는 약 5분이 소요됩니다.

Nimble Studio 개념 및 용어를 숙지한 후 Amazon Nimble Studio 시작하기를 참조하세요. 여기에서 단계별 스튜디오 배포 지침을 찾을 수 있습니다.

Amazon Nimble Studio 개념 및 용어

이 안내서의 주요 개념 및 용어를 참조하면 Amazon Nimble Studio를 시작하고 작동 방식을 이해하는 데 도움이 됩니다.

주요 기능

Amazon Nimble Studio

Amazon Nimble Studio는 크리에이티브 스튜디오가 스토리보드 스케치부터 최종 결과물에 이르기까지 클라우드에서 시각적 효과, 애니메이션 및 대화형 콘텐츠를 완전히 생성할 수 있도록 AWS 서비스하는 입니다.

Amazon Nimble Studio 콘솔

Nimble Studio 콘솔은 관리자 IT 고객을 위한 전용 AWS Management Console의 일부입니다. 이 콘솔은 관리자가 클라우드 스튜디오를 생성하고 다양한 설정을 관리하는 곳입니다. 예를 들어 Studio 관리자 페이지에서는 리소스를 추가 또는 제거하고, 애플리케이션을 추가하고, 사용자 및 그룹에 권한을 부여할 수 있습니다.

Amazon Nimble Studio 포털

Nimble Studio 포털은 Nimble Studio 애플리케이션 및 서비스와의 일상적인 상호 작용을 위한 사용자 인터페이스를 제공합니다. 사용자는 AWS Management Console과 상호 작용할 필요 없이 사용자 이름과 암호를 사용하여 포털에 직접 로그인합니다.

Nimble Studio File Transfer

File Transfer는 Amazon Simple S3(Amazon S3)와 주고받는 디지털 미디어 자산의 미디어 자산 전송을 가속화합니다. File Transfer는 수천 개의 큰 미디어 파일을 빠르게 이동하는 데 사용할 수 있는 그래픽 사용자 인터페이스를 제공합니다. 자세한 내용은 Nimble Studio File Transfer란 무엇인가요?를 참조하세요.

AWS Thinkbox

Thinkbox 소프트웨어에는 렌더 팜 매니저 Thinkbox Deadline과 3D 플러그인 Thinkbox Krakatoa가 포함되어 있습니다. Thinkbox 소프트웨어를 사용하면 온프레미스에서, Amazon EC2가 있는 클라우드에서, 또는 이 둘의 조합에서 스튜디오의 크리에이티브 결과물을 높일 수 있습니다. 자세한 내용은 AWS Thinkbox 제품을 참조하세요.

주요 개념 및 용어

AWS 관리형 정책

AWS 관리형 정책은에서 생성하고 관리하는 독립 실행형 정책입니다 AWS. 여기에서 독립적인 정책이란 정책 스스로 정책 이름이 포함된 Amazon 리소스 이름(ARN)을 갖고 있다는 것을 의미합니다. 예를 들어 arn:aws:iam::aws:policy/IAMReadOnlyAccess는 AWS 관리형 정책입니다. ARN에 대한 자세한 내용은 IAM ARN 단원을 참조하세요.

AWS 관리형 정책은 일반적인 작업 함수에 권한을 부여하는 데 사용됩니다. 새로운 AWS 서비스 및 API 작업이 도입되면에서 작업 정책이 유지 관리 및 업데이트됩니다. 예를 들어 AdministratorAccess 직무는 AWS의 모든 서비스 및 리소스에 대한 모든 액세스 권한 및 작업 권한을 위임합니다. 반면 AmazonMobileAnalyticsWriteOnlyAccess 및 AmazonEC2ReadOnlyAccess와 같은 부분 액세스 AWS 관리형 정책은 전체 액세스를 허용하지 AWS 서비스 않고에 대한 특정 수준의 액세스를 제공할 수 있습니다. 액세스 정책에 대한 자세한 내용은 정책 요약에서 액세스 수준 요약 이해하기를 참조하세요.

AWS Management Console

AWS Management Console는 관리를 위한 다양한 서비스 콘솔 컬렉션에 대한 액세스를 제공하는 웹 애플리케이션입니다 AWS 서비스.

각 서비스에는 자체 콘솔도 포함되어 있습니다. 이러한 콘솔은 클라우드 컴퓨팅을 위한 다양한 도구를 제공합니다. 결제 및 비용 관리를 도와주는 서비스도 있습니다.

AWS IAM Identity Center (IAM Identity Center)

IAM Identity Center는 여러 AWS 계정 및 비즈니스 애플리케이션에 대한 액세스를 중앙에서 쉽게 관리할 수 있는 AWS 서비스입니다. IAM Identity Center를 사용하면 사용자에게 할당된 모든 계정 및 애플리케이션에 대한 Single Sign-On 액세스를 한 곳에서 제공할 수 있습니다. 또한 AWS Organizations에서 모든 계정에 대한 다중 계정 액세스 및 사용자 권한을 중앙에서 관리할 수 있습니다. 자세한 내용은 AWS IAM Identity Center FAQ에서 알아보세요.

AWS PrivateLink

AWS PrivateLink는 트래픽을 퍼블릭 인터넷에 노출하지 않고 VPCs AWS 서비스와 온프레미스 네트워크 간에 프라이빗 연결을 제공합니다. AWS PrivateLink 를 사용하면 다양한 계정과 VPCs. AWS PrivateLink는에 청구되는 월별 요금으로 사용할 수 있습니다 AWS 계정.

디지털 콘텐츠 제작(DCC)

디지털 콘텐츠 제작(DCC)은 크리에이티브 콘텐츠를 제작하는 데 사용되는 애플리케이션의 범주를 가리킵니다. 여기에는, Blender, Nuke, Maya, Houdini가 포함됩니다.

리전

Nimble Studio는 스튜디오 배포를 선택할 수 있는 11가지 AWS 리전 를 제공합니다. 리전은 데이터와 애플리케이션 같은 필수 스튜디오 인프라가 있는 곳입니다.

리전은 스튜디오 사용자와 가장 가까운 곳에 위치해야 합니다. 그래야 지연이 줄어들고 데이터 전송 속도가 향상됩니다.

스튜디오

스튜디오는 다른 Nimble Studio 관련 리소스의 최상위 컨테이너입니다. 클라우드 스튜디오는 Nimble Studio 웹 포털과 VPC, 사용자 디렉터리, 스토리지 암호화 키 등 AWS 계정 의 필수 리소스에 대한 연결을 관리합니다.

스튜디오 애플리케이션

스튜디오 구성 요소는 고객의 Nimble Studio 내의 구성으로, AWS 계정에 있는 파일 시스템, 라이선스 서버, 렌더 팜 같은 리소스에 액세스하는 방법을 서비스에 알려 줍니다.

Nimble Studio에는 공유 파일 시스템, 컴퓨팅 팜, Active Directory, 라이선스 구성 요소 등 다양한 스튜디오 구성 요소 하위 유형이 포함되어 있습니다. 이러한 하위 유형은 스튜디오에서 사용하려는 리소스를 설명합니다.

스튜디오 리소스

스튜디오 리소스는 스튜디오의 일상 운영에 필요한 것을 요약하는 용어입니다. 클라우드 스튜디오의 인프라에 적합한 리소스를 설명할 때 스튜디오 구성 요소라고 할 수도 있습니다.

태그

태그는 AWS 리소스에 할당하는 레이블입니다. 각 태그는 사용자가 정의하는 키와 선택적 값으로 구성됩니다.

태그를 사용하면 AWS 리소스를 다양한 방식으로 분류할 수 있습니다. 예를 들어, 계정의 Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스에 대해 각 인스턴스의 소유자와 스택 수준을 추적하는 데 도움이 되는 태그 세트를 정의할 수 있습니다. 또한 태그를 사용하면 조직의 공유 파일 시스템 및 렌더 팜을 Nimble Studio와 통합하여 인력을 클라우드로 이동하는 동안 워크플로를 중단 없이 유지할 수 있습니다.

태그를 사용하면 용도, 소유자 또는 환경별로 AWS 리소스를 분류할 수 있습니다. 이 기능은 동일 유형의 리소스가 많을 때 유용합니다. 리소스에 할당한 태그에 따라 특정 리소스를 빠르게 식별할 수 있습니다.

Nimble Studio 설정

이 튜토리얼은 Amazon Nimble Studio를 설정하려는 관리자 사용자를 위한 것입니다.

다음 섹션에서는 Nimble Studio에 스튜디오를 배포하기 전에 완료해야 하는 단계를 안내합니다.

내용

IAM 설정

시작하기 전에 다음 AWS Identity and Access Management (IAM) 설명서를 검토합니다.

- IAM의 보안 모범 사례
- 관리자 AWS 계정 로에 로그인하여 나머지 설정을 완료합니다.

에 가입 AWS 계정

이 없는 경우 다음 단계를 AWS 계정완료하여 생성합니다.

에 가입하려면 AWS 계정

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

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

   에 가입하면 AWS 계정AWS 계정 루트 사용자이 생성됩니다. 루트 사용자에게는 계정의 모든 AWS 서비스 및 리소스에 액세스할 권한이 있습니다. 보안 모범 사례는 사용자에게 관리 액세스 권한을 할당하고, 루트 사용자만 사용하여 루트 사용자 액세스 권한이 필요한 작업을 수행하는 것입니다.

AWS 는 가입 프로세스가 완료된 후 확인 이메일을 보냅니다. 언제든지 https://aws.amazon.com/으로 이동하고 내 계정을 선택하여 현재 계정 활동을 보고 계정을 관리할 수 있습니다.

관리자 액세스 권한이 있는 사용자 생성

에 가입한 후 일상적인 작업에 루트 사용자를 사용하지 않도록 관리 사용자를 AWS 계정보호 AWS IAM Identity Center, AWS 계정 루트 사용자활성화 및 생성합니다.

보안 AWS 계정 루트 사용자

1. 루트 사용자를 선택하고 AWS 계정 이메일 주소를 입력하여 계정 소유자AWS Management Console로에 로그인합니다. 다음 페이지에서 비밀번호를 입력합니다.

   루트 사용자를 사용하여 로그인하는 데 도움이 필요하면 AWS 로그인 User Guide의 루트 사용자로 로그인을 참조하세요.
2. 루트 사용자의 다중 인증(MFA)을 활성화합니다.

   지침은 IAM 사용 설명서의 AWS 계정 루트 사용자(콘솔)에 대한 가상 MFA 디바이스 활성화를 참조하세요.

관리자 액세스 권한이 있는 사용자 생성

1. IAM Identity Center를 활성화합니다.

   지침은 AWS IAM Identity Center 사용 설명서의 AWS IAM Identity Center설정을 참조하세요.
2. IAM Identity Center에서 사용자에게 관리 액세스 권한을 부여합니다.

   를 자격 증명 소스 IAM Identity Center 디렉터리 로 사용하는 방법에 대한 자습서는 AWS IAM Identity Center 사용 설명서의 기본값으로 사용자 액세스 구성을 IAM Identity Center 디렉터리 참조하세요.

관리 액세스 권한이 있는 사용자로 로그인

- IAM IDentity Center 사용자로 로그인하려면 IAM Identity Center 사용자를 생성할 때 이메일 주소로 전송된 로그인 URL을 사용합니다.

  IAM Identity Center 사용자를 사용하여 로그인하는 데 도움이 필요하면 AWS 로그인 사용 설명서의 AWS 액세스 포털에 로그인을 참조하세요.

추가 사용자에게 액세스 권한 할당

1. IAM Identity Center에서 최소 권한 적용 모범 사례를 따르는 권한 세트를 생성합니다.

지침은AWS IAM Identity Center 사용 설명서의 Create a permission set를 참조하세요.

2. 사용자를 그룹에 할당하고, 그룹에 Single Sign-On 액세스 권한을 할당합니다.

   지침은 AWS IAM Identity Center 사용 설명서의 Add groups를 참조하세요.

관련 리소스

- IAM의 보안 모범 사례
- AWS 서비스 할당량 - AWS 일반 참조

Amazon Nimble Studio 시작하기

이 장에서는 Nimble Studio 콘솔을 사용하여 스튜디오의 인프라를 생성하고,를 확인하고 AWS 리전, 설정을 검토하고, 스튜디오를 생성하는 방법을 보여줍니다. 추가 설정을 사용하여 설정을 사용자 지정할 수도 있습니다.

처음 방문하는 AWS 고객은 Nimble Studio 설정 자습서를 참조하세요.

주제

Nimble Studio 설정

이 안내서에서는 인프라를 구성하고, 설정을 검토하고, 스튜디오를 생성하는 방법을 보여 줍니다. 추가 스튜디오 설정을 사용하여 스튜디오를 사용자 지정할 수도 있습니다.

1단계: 스튜디오 인프라 구성

스튜디오의 인프라는 다음과 같은 구성 요소로 이루어집니다.

- 스튜디오 표시 이름: 스튜디오 표시 이름은 스튜디오를 식별하는 방법입니다(예: AnyCompany Studio). 스튜디오 이름은 스튜디오 포털 URL도 결정합니다. 설정을 완료한 후 언제든지 스튜디오 표시 이름을 변경할 수 있습니다.
- 스튜디오 포털 URL: 스튜디오 포털 URL을 사용하여 스튜디오에 액세스할 수 있습니다. 이 URL은 스튜디오 표시 이름을 기반으로 합니다(예: https://anycompanystudio.awsapps.com). 설정을 완료한 후 언제든지 스튜디오 포털 URL을 변경할 수 있습니다.
- AWS 리전: AWS 리전는 AWS 데이터 센터 모음의 물리적 위치입니다. 스튜디오를 설정하면 기본적으로 사용자와 가장 가까운 위치가 리전으로 지정됩니다. 사용자들과 가장 가까운 곳에 위치하도록 리전을 변경해야 합니다. 이렇게 하면 지연이 줄어들고 데이터 전송 속도가 향상됩니다.

> **Important**
>
> Nimble Studio 설정을 완료한 후에는 리전을 변경할 수 없습니다.

스튜디오 인프라를 구성하려면 이 섹션의 작업을 완료하세요.

스튜디오의 인프라를 구성하려면

1. AWS Management Console에 로그인하고 Nimble Studio 콘솔을 엽니다.
2. Nimble Studio 설정을 선택하고 다음을 선택합니다.
3. 스튜디오 표시 이름을 입력합니다(예: **AnyCompany Studio**).
4. (선택 사항) Studio 포털 이름을 변경하려면 URL 편집을 선택합니다.
5. (선택 사항) 스튜디오 사용자들과 가장 가까운 위치로 AWS 리전을 변경하려면 리전 변경을 선택합니다.

   a. 사용자들과 가장 가까운 리전을 선택합니다.

   b. 리전 적용을 선택합니다.
6. (선택 사항) 스튜디오 설정을 추가로 사용자 지정하려면 추가 스튜디오 설정을 선택합니다.
7. 스튜디오를 생성하기 전에 설정을 검토하려면 다음을 선택합니다.

2단계: 스튜디오 검토 및 생성

스튜디오의 인프라를 구성한 후 스튜디오를 검토하고 변경하고 생성할 수 있습니다.

스튜디오를 검토 및 생성하려면

1. 검토 및 생성 페이지에서 스튜디오 인프라를 검토합니다.
2. AWS 리전이 스튜디오 사용자들과 가장 가까운 위치인지 확인합니다.
3. (선택 사항) 스튜디오 설정을 변경하려면 편집을 선택합니다.
4. 준비가 되었으면 스튜디오 생성을 선택합니다.

추가 스튜디오 설정

Nimble Studio 설정에는 추가 스튜디오 설정이 포함됩니다. 이러한 설정을 사용하면 Nimble Studio 설정에서에 수행하는 모든 변경 사항을 보고 AWS 계정, 스튜디오 사용자 역할을 구성하고, 암호화 키 유형을 변경할 수 있습니다. 스튜디오 리소스에 선택적 태그를 추가할 수도 있습니다.

스튜디오 사용자 역할 구성

AWS 서비스는 서비스 역할을 수임하여 사용자를 대신하여 작업을 수행할 수 있습니다. Nimble Studio가 사용자에게 스튜디오 내 리소스에 대한 액세스 권한을 부여하려면 스튜디오 사용자 역할이 필요합니다.

스튜디오 사용자 역할에 AWS Identity and Access Management (IAM) 관리형 정책을 연결할 수 있습니다. 정책을 통해 사용자는 특정 작업(예: 특정 Nimble Studio 애플리케이션에서 작업 생성)을 수행할 수 있습니다. 애플리케이션은 관리형 정책의 특정 조건에 의존하므로 관리형 정책을 사용하지 않으면 애플리케이션이 예상대로 작동하지 않을 수 있습니다.

설정을 완료한 후 언제든지 스튜디오 사용자 역할을 변경할 수 있습니다. 사용자 역할에 대한 자세한 내용은 IAM 역할을 참조하세요.

다음 탭에는 두 가지 사용 사례에 대한 지침이 포함되어 있습니다. 새 서비스 역할을 생성하고 사용하려면 새 서비스 역할 탭을 선택합니다. 기존 서비스 역할을 사용하려면 기존 서비스 역할 탭을 선택합니다.

New service role

새 서비스 역할을 생성하고 사용하려면

1. 새 서비스 역할 생성 및 사용을 선택합니다.
2. (선택 사항) 서비스 사용자 역할 이름을 입력합니다.
3. 역할에 대한 자세한 내용을 보려면 권한 세부 정보 보기를 선택합니다.

Existing service role

기존 서비스 역할을 사용하려면

1. 기존 서비스 역할 사용을 선택합니다.
2. 드롭다운 목록을 열어 기존 서비스 역할을 선택합니다.
3. (선택 사항) 역할에 대한 자세한 내용을 보려면 IAM 콘솔에서 보기를 선택합니다.

AWS IAM Identity Center

AWS IAM Identity Center 는 사용자 및 그룹을 관리하기 위한 클라우드 기반 Single Sign-On 서비스입니다. IAM Identity Center를 엔터프라이즈 Single Sign-On(SSO) 공급자와 통합하면 사용자가 회사 계정으로 로그인할 수도 있습니다.

Nimble Studio는 기본적으로 IAM Identity Center를 활성화하며, Nimble Studio를 설정하고 사용하려면 IAM Identity Center가 필요합니다. 자세한 내용은 정의 섹션을 참조하세요 AWS IAM Identity Center.

AWS KMS 암호화 키 구성

AWS Key Management Service (AWS KMS) 키는 데이터를 암호화, 복호화 및 재암호화하는 데 사용할 수 있는 KMS 키의 기본 유형입니다.

Nimble Studio에는 다음과 같은 AWS KMS 암호화 키 유형이 포함됩니다.

- AWS 소유 키 - AWS 소유 키는가 AWS 서비스 소유 및 관리하는 KMS 키로 AWS 계정, 여러 AWS 계정. AWS owned 키에서 사용할 수 있습니다.owned 키는에 상주하지 않지만 Nimble Studio는 AWS 소유 키를 사용하여 계정의 리소스를 보호할 수 있습니다.

  를 사용하려면 키 또는 키 정책을 생성하거나 유지 관리할 필요가 AWS KMS없습니다. AWS 소유 키를 사용하는 데는 요금이 부과되지 않으며의 할당량에 AWS KMS 포함되지 않습니다 AWS 계정.
- 고객 관리형 AWS KMS 키 - 고객 관리형 키는 AWS 계정 생성, 소유 및 관리하는의 KMS 키입니다.

  이러한 KMS 키를 완전히 제어할 수 있습니다. 고객 관리형 키에는 월별 요금이 발생합니다. 또한 프리 티어를 AWS KMS 초과하여에 대한 각 API 요청에 대해 요금이 발생합니다. AWS KMS 요금에 대한 자세한 내용은 AWS Key Management Service 요금을 참조하세요.

설정을 완료한 후에는 암호화 키 유형을 변경할 수 없습니다. AWS KMS 및 암호화 키 유형에 대한 자세한 내용은 AWS KMS 설명서를 참조하세요.

다른 암호화 키 유형을 선택하려면

1. 다른 AWS KMS 키 선택(고급)을 선택합니다.
2. AWS KMS 키를 선택하거나 Amazon 리소스 번호(ARN)를 입력합니다.
3. AWS KMS 키 생성을 선택합니다.

태그 구성

태그는 Nimble Studio 리소스를 구성하기 위한 레이블 역할을 합니다. 최대 50개의 태그를 추가하여 리소스를 식별, 구성, 필터링, 검색할 수 있습니다.

각 태그는 사용자가 정의하는 다음 두 부분으로 구성됩니다. 태그 키와 선택적 태그 값입니다(예: 키: `domain` 및 값: `anycompanystudio.com`).

설정을 완료한 후 언제든지 태그를 추가하거나 삭제할 수 있습니다. 태그에 대한 자세한 내용은 AWS 리소스 태그 지정을 참조하세요.

스튜디오 리소스에 태그를 추가려면

1. Add new tag(새 태그 추가가)를 선택합니다.
2. 태그 키를 입력합니다.
3. (선택 사항) 태그 값을 입력합니다.

스튜디오 삭제

더 이상 필요하지 않은 스튜디오는 삭제할 수 있습니다. 스튜디오를 삭제하면 스튜디오 인프라만 삭제됩니다. 사용자 역할, 정책, 애플리케이션 데이터와 같은 다른 AWS 리소스는 그대로 유지됩니다.

> **Important**
>
> 삭제한 스튜디오는 복구할 수 없습니다.

스튜디오를 삭제하려면

1. 에 로그인 AWS Management Console 하고 Nimble Studio 콘솔을 엽니다.
2. 스튜디오 개요를 선택합니다.
3. 작업을 선택한 후 스튜디오 삭제를 선택합니다.
4. **`delete`**를 입력한 다음 삭제를 선택합니다.

Amazon Nimble Studio에서의 보안

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

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

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

> **Important**
>
> Security Pillar - AWS Well-Architected Framework를 읽고 숙지하는 것이 좋습니다. 이 문서에는 AWS 인프라 보안을 위한 주요 원칙이 포함되어 있습니다.

이 설명서는 Nimble Studio 사용 시 공동 책임 모델을 적용하는 방법을 이해하는 데 도움이 됩니다. 다음 주제에서는 보안 및 규정 준수 목표를 충족하도록 Nimble Studio을(를) 구성하는 방법을 보여줍니다. 또한 Nimble Studio 리소스를 모니터링하고 보호하는 데 도움이 되는 다른 AWS 서비스를 사용하는 방법도 알아봅니다.

추가 정보

- 보안 원칙 - AWS Well-Architected Framework
- AWS 클라우드 개발 키트 (AWS CDK) (AWS CDK) 보안
- Amazon Virtual Private Cloud에서의 보안
- AWS 보안 인증 정보
- Amazon EC2의 보안

- Linux
- Windows

AWS 계정 보안 설정

이 가이드에서는 리소스가 손상되었을 때 알림을 AWS 계정 수신하고 특정 AWS 계정 사용자가 액세스할 수 있도록를 설정하는 방법을 보여줍니다. 를 보호하고 리소스를 AWS 계정 추적하려면 다음 단계를 완료하세요.

내용

- 계정의 액세스 키를 삭제합니다.
- 다중 인증 활성화
- 모든에서 CloudTrail 활성화 AWS 리전
- Amazon GuardDuty 및 알림 설정

계정의 액세스 키를 삭제합니다.

AWS Command Line Interface (AWS CLI) 또는 API를 사용하여 AWS 리소스에 대한 프로그래밍 방식 액세스를 허용할 수 있습니다. AWS APIs 그러나는 프로그래밍 방식 액세스를 위해 루트 계정과 연결된 액세스 키를 생성하거나 사용하지 않도록 AWS 권장합니다.

액세스 키가 여전히 있는 경우, 해당 액세스 키를 삭제하고 사용자를 생성하는 것이 좋습니다. 그런 다음 호출하려는 API에 필요한 권한만 해당 사용자에게 부여하세요. 해당 사용자를 사용하여 액세스 키를 발급할 수 있습니다.

자세한 내용은 AWS 일반 참조 안내서의 AWS 계정의 액세스 키 관리를 참조하세요.

다중 인증 활성화

다중 인증(MFA)은 사용자 이름과 암호에 더해 인증 계층을 제공하는 보안 기능입니다.

MFA의 원리는 다음과 같습니다. 사용자 이름과 암호로 로그인한 후에 본인만 물리적으로 액세스할 수 있는 추가 정보도 제공해야 합니다. 이 정보는 전용 MFA 하드웨어 디바이스 또는 휴대 전화의 앱에서 가져올 수 있습니다.

지원되는 MFA 디바이스 목록에서 사용하려는 MFA 디바이스 유형을 선택해야 합니다. 하드웨어 디바이스의 경우 MFA 디바이스를 안전한 위치에 보관하세요.

가상 MFA 디바이스(예: 휴대 전화 앱)를 사용한다면 휴대 전화가 분실되거나 손상되는 경우 어떻게 할지 생각해 둬야 합니다. 한 가지 방법은 사용하는 가상 MFA 디바이스를 안전한 장소에 보관하는 것입니다. 또 다른 옵션은 두 개 이상의 디바이스를 동시에 활성화하거나 디바이스 키 복구에 가상 MFA 옵션을 사용하는 것입니다.

MFA에 대한 자세한 내용은 가상 다중 인증(MFA) 디바이스 활성화를 참조하세요.

관련 리소스

- 다중 인증 시작하기
- MFA를 AWS 사용하여에 대한 액세스 보호

모든에서 CloudTrail 활성화 AWS 리전

를 사용하여 AWS 리소스의 모든 활동을 추적할 수 있습니다AWS CloudTrail. 지금 CloudTrail을 켜는 것을 권장합니다. 이렇게 하면 지원 와 AWS 솔루션 아키텍트가 나중에 보안 또는 구성 문제를 해결하는 데 도움이 될 수 있습니다.

모든에서 CloudTrail 로깅을 활성화하려면 업데이트 - 모든 리전에서 켜기 및 여러 추적 사용을 AWS 리전참조하세요. AWS CloudTrail

CloudTrail에 대한 자세한 내용은 에서 CloudTrail 켜기: API 활동 로깅을 참조하세요 AWS 계정. CloudTrail이 Nimble Studio를 모니터링하는 방법을 알아보려면 를 사용하여 Nimble Studio 호출 로깅 AWS CloudTrail을 참조하세요.

Amazon GuardDuty 및 알림 설정

Amazon GuardDuty는 다음을 분석하고 처리하는 지속적 보안 모니터링 서비스입니다.

- 데이터 소스
- Amazon VPC 흐름 로그
- AWS CloudTrail 관리 이벤트 로그
- CloudTrail S3 데이터 이벤트 로그
- DNS 로그

Amazon GuardDuty는 사용자 AWS 환경 내에서 예기치 않고 잠재적으로 승인되지 않은 악의적인 활동을 식별합니다. 악의적 활동에는 권한 에스컬레이션, 노출된 보안 인증 정보 사용 또는 악의적인

IP 주소나 도메인과의 통신 같은 문제가 포함될 수 있습니다. GuardDuty는 이러한 활동을 식별하기 위해 악성 IP 주소 및 도메인 목록 같은 위협 인텔리전스 피드와 기계 학습을 사용합니다. 예를 들어 GuardDuty는 맬웨어에 서비스를 제공하거나 비트코인을 채굴하는 손상된 Amazon EC2 인스턴스를 탐지할 수 있습니다.

또한 GuardDuty는 AWS 계정 액세스 동작에서 손상 징후를 모니터링합니다. 여기에는 사용된 적이 없는에 배포 AWS 리전 된 인스턴스와 같은 무단 인프라 배포가 포함됩니다. 또한 암호 강도를 줄이기 위한 암호 정책 변경과 같은 특이한 API 직접 호출도 포함됩니다.

GuardDuty는 보안 조사 결과를 생성하여 AWS 환경의 상태를 알려줍니다. 이러한 조사 결과는 GuardDuty 콘솔이나 Amazon CloudWatch 이벤트를 통해 볼 수 있습니다.

Amazon SNS 주제 및 엔드포인트 설정

Amazon SNS 설정 주제 및 엔드포인트 설정 자습서의 지침을 따르세요.

GuardDuty 조사 결과를 위한 EventBridge 이벤트 설정

GuardDuty가 생성하는 모든 조사 결과를 위한 이벤트를 전송하는 EventBridge 규칙을 생성하세요.

GuardDuty 조사 결과를 위한 EventBridge 이벤트를 생성하려면

1. Amazon EventBridge 콘솔(https://console.aws.amazon.com/events/)에 로그인합니다.
2. 탐색 창에서 규칙을 선택합니다. 그런 다음 규칙 생성을 선택합니다.
3. 새 규칙의 이름과 설명을 입력합니다. 그런 다음 다음을 선택합니다.
4. 이벤트 소스에서 AWS 이벤트 또는 EventBridge 파트너 이벤트가 선택된 상태로 둡니다.
5. 이벤트 패턴에서 이벤트 소스로 AWS 서비스를 선택합니다. 그런 다음 AWS 서비스에서 GuardDuty를 선택하고, 이벤트 유형에서 GuardDuty 결과를 선택합니다. 이것은 Amazon SNS 주제 및 엔드포인트 설정에서 생성한 주제입니다.
6. Next(다음)를 선택합니다.
7. 대상 1에서 AWS 서비스를 선택합니다. 대상 선택 드롭다운에서 SNS 주제를 선택합니다. 그런 다음 GuardDuty_to_Email 주제를 선택합니다.
8. 추가 설정 섹션에서 대상 입력 구성 드롭다운을 사용하여 입력 변환기를 선택합니다. 입력 변환기 구성을 선택합니다.
9. 대상 입력 변환기 섹션의 입력 경로 필드에 다음 코드를 입력합니다.

```
{
```

```
    "severity": "$.detail.severity",
    "Account_ID": "$.detail.accountId",
    "Finding_ID": "$.detail.id",
    "Finding_Type": "$.detail.type",
    "region": "$.region",
    "Finding_description": "$.detail.description"
}
```

10. 이메일의 형식을 지정하려면 템플릿 필드에 다음 코드를 입력합니다.

```
"AWS <Account_ID> has a severity <severity> GuardDuty finding type <Finding_Type>
 in the <region> region."
"Finding Description:"
"<Finding_description>. "
"For more details open the GuardDuty console at https://console.aws.amazon.com/
guardduty/home?region=<region>#/findings?search=id=<Finding_ID>"
```

11. 생성(Create)을 선택합니다. 그런 다음 다음을 선택합니다.
12. (선택 사항) 태그를 사용하여 AWS 리소스를 추적하는 경우 태그를 추가합니다.
13. Next(다음)를 선택합니다.
14. 규칙을 검토합니다. 그런 다음 규칙 생성을 선택합니다.

이제 AWS 계정 보안을 설정했으므로 특정 사용자에게 액세스 권한을 부여하고 리소스가 손상되면 알림을 받을 수 있습니다.

Amazon Nimble Studio 데이터 보호

AWS 공동 책임 모델의 데이터 보호에 적용됩니다Amazon Nimble Studio. 이 모델에 설명된 대로 AWS 는 모든를 실행하는 글로벌 인프라를 보호할 책임이 있습니다 AWS 클라우드. 사용자는 인프라에서 호스팅되는 콘텐츠를 관리해야 합니다. 사용하는 AWS 서비스 의 보안 구성과 관리 태스크에 대한 책임도 사용자에게 있습니다. 데이터 프라이버시에 대한 자세한 내용은 데이터 프라이버시 FAQ를 참조하세요. 유럽의 데이터 보호에 대한 자세한 내용은 AWS 보안 블로그의 AWS 공동 책임 모델 및 GDPR 블로그 게시물을 참조하세요.

데이터 보호를 위해 자격 증명을 보호하고 AWS 계정 AWS IAM Identity Center 또는 AWS Identity and Access Management (IAM)를 사용하여 개별 사용자를 설정하는 것이 좋습니다. 이렇게 하면 개별 사용자에게 자신의 직무를 충실히 이행하는 데 필요한 권한만 부여됩니다. 또한 다음과 같은 방법으로 데이터를 보호하는 것이 좋습니다.

- 각 계정에 다중 인증(MFA)을 사용하세요.
- SSL/TLS를 사용하여 AWS 리소스와 통신합니다. TLS 1.2는 필수이며 TLS 1.3을 권장합니다.
- 를 사용하여 API 및 사용자 활동 로깅을 설정합니다 AWS CloudTrail. CloudTrail 추적을 사용하여 AWS 활동을 캡처하는 방법에 대한 자세한 내용은 AWS CloudTrail 사용 설명서의 CloudTrail 추적 작업을 참조하세요.
- AWS 암호화 솔루션과 내부의 모든 기본 보안 제어를 사용합니다 AWS 서비스.
- Amazon S3에 저장된 민감한 데이터를 검색하고 보호하는 데 도움이 되는 Amazon Macie와 같은 고급 관리형 보안 서비스를 사용하세요.
- 명령줄 인터페이스 또는 API를 AWS 통해에 액세스할 때 FIPS 140-3 검증 암호화 모듈이 필요한 경우 FIPS 엔드포인트를 사용합니다. 사용 가능한 FIPS 엔드포인트에 대한 자세한 내용은 Federal Information Processing Standard(FIPS) 140-3을 참조하세요.

고객의 이메일 주소와 같은 기밀 정보나 중요한 정보는 태그나 이름 필드와 같은 자유 형식 텍스트 필드에 입력하지 않는 것이 좋습니다. 여기에는 콘솔, API AWS CLI또는 AWS SDKs를 사용하여 Nimble Studio 또는 다른 AWS 서비스 로 작업하는 경우가 포함됩니다. 이름에 사용되는 태그 또는 자유 형식 텍스트 필드에 입력하는 모든 데이터는 청구 또는 진단 로그에 사용될 수 있습니다. 외부 서버에 URL을 제공할 때 해당 서버에 대한 요청을 검증하기 위해 자격 증명을 URL에 포함해서는 안 됩니다.

AWS 공동 책임 모델은 Amazon Nimble Studio의 데이터 보호에 적용됩니다. 이 모델에 설명된 대로 AWS 는 모든를 실행하는 글로벌 인프라를 보호할 책임이 있습니다 AWS 클라우드. 이 인프라에서 호스팅되는 콘텐츠에 대한 제어를 유지하는 것은 사용자의 책임입니다. 이 콘텐츠에는 사용하는에 대한 보안 구성 및 관리 작업이 포함되어 AWS 서비스 있습니다.

데이터 프라이버시에 대한 자세한 내용은 데이터 프라이버시 FAQ를 참조하세요. 유럽 연합의 데이터 보호에 대한 자세한 내용은 GDPR 센터를 참조하세요.

저장 시 암호화

Nimble Studio는 AWS Key Management Service (AWS KMS)에 저장된 암호화 키를 사용한 저장 데이터 암호화를 통해 민감한 스튜디오 데이터를 보호합니다. 저장 시 암호화는 Nimble Studio를 사용할 수 AWS 리전 있는 모든에서 사용할 수 있습니다. 암호화되는 스튜디오 데이터에는 모든 리소스 유형의 이름과 설명은 물론 스튜디오 구성 요소 스크립트, 스크립트 파라미터, 마운트 지점, 공유 이름 및 기타 데이터가 포함됩니다.

데이터를 암호화하면 유효한 키 없이는 어떤 사용자나 애플리케이션도 디스크에 저장된 민감한 데이터를 읽을 수 없습니다. 암호화된 데이터는 안전하게 저장될 수 있으며 관리형 키에 대한 액세스가 승인된 당사자만 복호화할 수 있습니다.

Nimble Studio가 저장 데이터 암호화에를 사용하는 방법에 AWS KMS 대한 자세한 내용은 섹션을 참조하세요Amazon Nimble Studio의 키 관리.

AWS KMS 키와 함께 권한 부여 사용

권한 부여는 AWS 보안 주체가 암호화 작업에서 AWS KMS 키를 사용하도록 허용하는 정책 도구입니다. 또한 `DescribeKey` 명령을 사용하여 KMS 키를 보고 권한 부여를 생성 및 관리하도록 할 수 있습니다.

권한 부여는와 통합 AWS 서비스 되는에서 저장 데이터를 암호화하는 AWS KMS 데 일반적으로 사용됩니다. 서비스는 계정의 사용자를 대신하여 권한 부여를 만들고, 권한을 사용하고, 작업이 완료되는 즉시 권한 부여를 폐기합니다.

Nimble Studio가 스튜디오를 생성하면 사용자 역할과 관리자 역할이라는 두 가지 역할이 Nimble Studio 포털 사용자에게 제공됩니다. Nimble Studio는 이러한 역할의 고객 관리형 키에 대한 권한 부여를 생성하여 이 역할에 스튜디오에서 암호화된 데이터에 대한 액세스 권한을 제공합니다.

> **Important**
>
> 권한 부여를 삭제하면 관리자가 새 권한 부여를 생성할 때까지 사용자는 Nimble Studio 포털을 사용할 수 없게 됩니다.

권한 부여 AWS 서비스 사용 방법에 대한 자세한 내용은 서비스 사용 설명서 또는 개발자 안내서의 AWS 서비스 사용 AWS KMS 방법 또는 저장 시 암호화 주제를 참조하세요.

전송 중 암호화

다음 표는 전송 중 데이터가 암호화되는 방법에 대한 정보를 제공합니다. 해당하는 경우 Nimble Studio의 다른 데이터 보호 방법도 나열됩니다.

Data	네트워크 경로	보호
이미지 및 JavaScript 파일과 같은 웹 자산	네트워크 경로는 Nimble Studio 사용자와 Nimble Studio 간 경로입니다.	데이터 암호화는 TLS 1.2 이상을 사용합니다.
픽셀 및 관련 스트리밍 트래픽	네트워크 경로는 Nimble Studio 사용자와 Nimble Studio 간 경로입니다.	256비트 Advanced Encryption Standard(AES-256)를 사용하

		여 암호화되고 TLS 1.2 이상을 사용하여 전송.
API 트래픽	경로는 Nimble Studio 사용자와 Nimble Studio 간 경로입니다.	TLS 1.2 이상을 사용하여 암호화. 연결 생성 요청은 SigV4를 사용하여 서명됩니다.

Amazon Nimble Studio의 키 관리

새 테이블을 생성할 때 다음 키 중 하나를 선택하여 스튜디오 데이터를 암호화할 수 있습니다.

- AWS 소유 KMS 키 - 기본 암호화 유형입니다. 키는 Nimble Studio가 소유합니다(추가 비용 없음).
- 고객 관리형 KMS 키 - 키는 사용자의 계정에 저장되며 사용자가 생성, 소유, 관리합니다. key. AWS KMS charges를 완전히 제어할 수 있습니다.

AWS Key Management Service (AWS KMS)에서 고객 관리형 KMS 키를 삭제하면 파괴적이고 위험할 수 있습니다. 이렇게 하면 키와 연결된 키 구성 요소와 모든 메타데이터가 되돌릴 수 없는 방식으로 삭제됩니다. 고객 관리형 KMS 키가 삭제된 후에는 해당 키로 암호화된 데이터를 더 이상 복호화할 수 없습니다. 즉, 데이터를 복구할 수 없게 됩니다.

따라서는 고객에게 키를 삭제하기 전에 최대 30일의 대기 기간을 AWS KMS 제공합니다. 기본 대기 기간은 30일입니다.

대기 기간에 대해

고객 관리형 KMS 키를 삭제하는 것은 안전하지 않으며 위험할 수 있기 때문에 대기 기간을 7~30일로 설정해야 합니다. 기본 대기 기간은 30일입니다.

그러나 실제 대기 기간은 예약한 대기 기간보다 최대 24시간 더 길어질 수 있습니다. 키가 삭제될 실제 날짜 및 시간을 가져오려면 DescribeKey 작업을 사용하세요. AWS KMS 콘솔의 키 세부 정보 페이지에 있는 일반 구성 섹션에서 예약된 삭제 날짜를 확인할 수도 있습니다. 시간대를 확인하세요.

대기 기간 동안 고객 관리형 키의 상태 및 키 상태는 삭제 대기 중입니다.

- 삭제 대기 중인 고객 관리형 KMS 키는 어떠한 암호화 작업에도 사용할 수 없습니다.
- AWS KMS 는 삭제 보류 중인 고객 관리형 키의 백업 키를 교체하지 않습니다. AWS KMS

고객 관리형 AWS KMS 키 삭제에 대한 자세한 내용은 고객 마스터 키 삭제를 참조하세요.

데이터 보안 조치

데이터 보호를 위해 자격 AWS 계정 증명을 보호하고 AWS Identity and Access Management (IAM)을 사용하여 개별 계정을 설정하는 것이 좋습니다. 이렇게 하면 개별 사용자에게 자신의 직무를 충실히 이행하는 데 필요한 권한만 부여됩니다. 또한 다음과 같은 방법으로 데이터를 보호하는 것이 좋습니다.

- 각 계정에 다중 인증(MFA)을 사용하세요.
- SSL/TLS를 사용하여 AWS 리소스와 통신합니다. TLS 1.2 이상을 권장합니다.
- 를 사용하여 API 및 사용자 활동 로깅을 설정합니다 AWS CloudTrail.
- AWS 암호화 솔루션과 내의 모든 기본 보안 제어를 사용합니다 AWS 서비스.
- 명령행 인터페이스 또는 API를 통해 AWS 에 액세스할 때 FIPS 140-2 검증된 암호화 모듈이 필요한 경우, FIPS 엔드포인트를 사용합니다. 사용 가능한 FIPS 엔드포인트에 대한 자세한 내용은 Federal Information Processing Standard(FIPS) 140-2를 참조하세요.

이름 필드와 같은 자유 형식 필드에 고객 계정 번호 같은 민감한 식별 정보를 절대 입력하지 마세요. 여기에는 Amazon Nimble Studio 또는 기타에서 콘솔, API AWS CLI, 또는 AWS SDKs를 AWS 서비스 사용하여 작업하는 경우가 포함됩니다. Amazon Nimble Studio 또는 기타 서비스에 입력하는 데이터는 캡처되어 진단 로그에 포함될 수 있습니다. 외부 서버에 URL을 제공할 때 해당 서버에 대한 요청을 검증하기 위해 자격 증명 정보를 URL에 포함하지 마십시오.

진단 데이터 및 지표

StudioBuilder를 배포 및 삭제하는 동안 Amazon Nimble Studio는 문제를 진단하고 Nimble Studio의 기능 및 사용자 경험을 개선하는 데 사용하는 특정 지표를 수집합니다.

수집되는 지표의 유형

- 사용 정보 - 실행되는 일반 명령 및 하위 명령.
- 오류 및 진단 정보 - 종료 코드, 내부 예외 이름, 실패 등 실행되는 명령의 상태 및 기간.
- 시스템 및 환경 정보 - Python 버전, 운영 체제(Windows, Linux 또는macOS), StudioBuilder가 실행되는 환경.

Amazon Nimble Studio의 Identity and Access Management

AWS Identity and Access Management (IAM)는 관리자가 AWS 리소스에 대한 액세스를 안전하게 제어할 수 AWS 서비스 있도록 도와주는 입니다. 관리자는 어떤 사용자가 Amazon Nimble Studio 리소스

를 사용할 수 있도록 인증(로그인) 및 권한 부여(권한 있음)될 수 있는지 제어합니다. IAM은 추가 비용 없이 사용할 수 AWS 서비스 있는 입니다.

주제

대상

사용 방법 AWS Identity and Access Management (IAM)은 Nimble Studio에서 수행하는 작업에 따라 다릅니다.

서비스 사용자 - Nimble Studio 서비스를 사용하여 작업을 수행한다면 서비스 사용자입니다. 이 경우 할당된 리소스에 액세스하는 데 필요한 보안 인증 정보와 권한을 관리자가 제공합니다. 더 많은 Nimble Studio 기능을 사용하여 작업을 수행하게 되면 추가 권한이 필요할 수 있습니다. 액세스 권한 관리 방법을 이해하면 관리자에게 올바른 권한을 요청하는 데 도움이 됩니다. Nimble Studio의 기능에 액세스할 수 없는 경우 Amazon Nimble Studio 자격 증명 및 액세스 문제 해결을 참조하세요.

서비스 관리자 - 회사에서 Nimble Studio 리소스를 책임지고 있다면 Nimble Studio에 대한 전체 액세스 권한을 가지고 있을 것입니다. 서비스 관리자는 직원이 액세스해야 하는 Nimble Studio 기능과 리소스를 결정합니다. 그런 다음 관리자에게 요청을 제출하여 서비스 사용자의 권한을 변경합니다. 이 페이지의 정보를 검토하여 IAM의 기본 개념을 이해하세요. 회사가 Nimble Studio에서 IAM을 사용하는 방법에 대해 자세히 알아보려면 Amazon Nimble Studio에서 IAM을 사용하는 방법을 참조하세요.

ID를 통한 인증

인증은 AWS 자격 증명으로에 로그인하는 방법입니다. 를 사용하여 로그인하는 방법에 대한 자세한 내용은 IAM 사용 설명서의 IAM 사용자 또는 루트 사용자 AWS Management Console 로에 로그인을 AWS Management Console참조하세요.

AWS 계정 루트 사용자, 사용자 또는 IAM 역할을 수임하여 인증(로그인 AWS)되어야 합니다. 회사의 Single Sign-On(SSO) 인증을 사용하거나 Google 또는 Facebook을 사용하여 로그인할 수도 있습니다. 이러한 경우 관리자는 이전에 IAM 역할을 사용하여 자격 증명 연동을 설정한 것입니다. 다른 회사의 자격 증명을 AWS 사용하여에 액세스할 때 역할을 간접적으로 수임합니다.

AWS Management Console에 직접 로그인하려면 루트 사용자 이메일 주소 또는 사용자 이름과 암호를 사용하세요. 루트 사용자 또는 사용자 액세스 키를 사용하여 프로그래밍 방식으로 AWS 에 액세스할 수 있습니다.

AWS 는 자격 증명을 사용하여 요청에 암호화 방식으로 서명할 수 있는 SDK 및 명령줄 도구를 제공합니다. AWS 도구를 사용하지 않는 경우 직접 요청에 서명하세요. 이렇게 하려면 인바운드 API 요청을 인증하기 위한 프로토콜인 서명 버전 4를 사용합니다. 요청 인증에 대한 자세한 내용은 AWS 일반 참조의 서명 버전 4 서명 프로세스를 참조하세요.

사용하는 인증 방법에 상관 없이 추가 보안 정보를 제공해야 할 수도 있습니다. 예를 들어는 다중 인증(MFA)을 사용하여 계정의 보안을 강화할 것을 AWS 권장합니다. 자세한 내용은 IAM 사용 설명서의 AWS에서 다중 인증(MFA) 사용을 참조하세요.

AWS 계정 루트 사용자

를 처음 생성할 때 계정의 모든 AWS 서비스 및 리소스에 대한 완전한 액세스 권한이 있는 단일 로그인 자격 증명으로 AWS 계정시작합니다. 이 자격 증명을 테 AWS 계정 루트 사용자라고 하며 계정을 생성하는 데 사용한 이메일 주소와 암호로 로그인하여 액세스합니다. 일상적인 작업, 심지어 관리 작업의 경우에도 루트 사용자를 사용하지 않는 것이 좋습니다. 대신, IAM 사용자를 처음 생성할 때만 루트 사용자를 사용하는 모범 사례를 준수합니다. 그런 다음 루트 사용자 자격 증명을 안전하게 보관하고 몇 가지 계정 및 서비스 관리 태스크를 수행할 때만 사용합니다.

사용자 및 그룹

사용자는 한 사람 또는 애플리케이션에 대한 특정 권한이 AWS 계정 있는 내 자격 증명입니다. 사용자에게는 장기 보안 인증 정보 또는 액세스 키 세트가 있을 수 있습니다. 액세스 키를 생성하는 방법은 IAM 사용 설명서의 IAM 사용자의 액세스 키 관리를 참조하세요. 사용자의 액세스 키를 생성할 때는 키 페어를 확인하고 안전하게 저장하세요. 비밀 액세스 키는 향후에 복구할 수 없습니다. 그 대신 새 액세스 키 페어를 생성하세요.

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

사용자는 역할과 다릅니다. 사용자는 한 사람 또는 애플리케이션과 고유하게 연결되지만, 역할은 해당 역할이 필요한 사람이라면 누구나 수임할 수 있습니다. 사용자는 영구적인 장기 자격 증명을 가지고 있지만, 역할은 임시 보안 인증만 제공합니다. 자세한 내용은 IAM 사용 설명서의 IAM 사용자(역할이 아님)를 생성해야 하는 경우를 참조하세요.

IAM 역할

IAM 역할은 특정 권한이 AWS 계정 있는 내 자격 증명입니다. 이 역할은 사용자와 비슷하지만, 특정 개인과 연결되지 않습니다. 역할을 전환 AWS Management Console 하여에서 IAM 역할을 일시적으로 수임할 수 있습니다. AWS CLI 또는 AWS API 작업을 호출하거나 사용자 지정 URL을 사용하여 역할을 수임할 수 있습니다. 역할 사용 방법에 대한 자세한 정보는 IAM 사용 설명서의 IAM 역할 사용을 참조하세요.

임시 자격 증명이 있는 IAM 역할은 다음과 같은 상황에서 유용합니다.

- 임시 사용자 권한 - 사용자는 IAM 역할을 수임하여 특정 작업에 대한 다양한 권한을 임시로 받을 수 있습니다.
- 페더레이션 사용자 액세스 - 사용자를 생성하는 대신의 기존 자격 증명 AWS Directory Service, 엔터프라이즈 사용자 디렉터리 또는 웹 자격 증명 공급자를 사용할 수 있습니다. 이 사용자를 페더레이션 사용자라고 합니다. AWS 에서는 자격 증명 공급자를 통해 액세스가 요청되면 페더레이션 사용자에게 역할을 할당합니다. 페더레이션 사용자에 대한 자세한 내용은 IAM 사용 설명서의 페더레이션 사용자 및 역할을 참조하세요.
  - 멤버십 - Nimble Studio는 '멤버십'이라는 개념을 사용하여 특정 시작 프로파일에 대한 액세스 권한을 사용자에게 제공합니다. 스튜디오 관리자는 IAM 정책을 작성하거나 이해할 필요 없이 멤버십을 통해 사용자에게 리소스 액세스 권한을 위임할 수 있습니다. Nimble Studio 관리자가 시작 프로파일에서 사용자의 멤버십을 생성하면 사용자는 시작 프로파일을 사용하는 데 필요한 IAM 작업(예: 해당 시작 프로파일을 사용하여 속성 보기 및 스트리밍 세션 시작)을 수행할 권한이 부여됩니다.
  - 서비스 역할 - 서비스 역할은 서비스가 사용자를 대신하여 작업을 수행하기 위해 맡는 IAM 역할입니다. 서비스 역할은 해당 계정 내에서만 액세스를 제공하며 다른 계정의 서비스에 대한 액세스를 부여하는 데 사용할 수 없습니다. 관리자는 IAM 내에서 서비스 역할을 생성, 수정, 삭제할 수 있습니다. 자세한 내용은 IAM 사용 설명서의 AWS 서비스에 대한 권한을 위임할 역할 생성을 참조하세요.
  - 서비스 연결 역할 - 서비스 연결 역할은에 연결된 서비스 역할의 한 유형입니다 AWS 서비스. 서비스는 사용자를 대신하여 작업을 수행하기 위해 역할을 수임할 수 있습니다. Nimble Studio는 서비스 연결 역할을 지원하지 않습니다.

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

IAM 역할을 사용할지 또는 사용자를 사용할지를 알아보려면 IAM 사용 설명서의 IAM 역할(사용자가 아님)을 만들어야 하는 경우를 참조하세요.

정책을 사용하여 액세스 관리

정책을 AWS 생성하고 IAM 자격 증명 또는 AWS 리소스에 연결하여의 액세스를 제어합니다. 정책은 자격 증명 또는 리소스와 연결된 AWS 경우 해당 권한을 정의하는의 객체입니다. 루트 사용자 또는 사용자로 로그인하거나 IAM 역할을 수임할 수 있습니다. 그런 다음 요청을 수행하면는 관련 자격 증명 기반 또는 리소스 기반 정책을 AWS 평가합니다. 정책에서 권한은 요청이 허용되거나 거부되는 지를 결정합니다. 대부분의 정책은에 JSON 문서 AWS 로 저장됩니다. JSON 정책 문서의 구조와 콘텐츠에 대한 자세한 정보는 IAM 사용 설명서의 JSON 정책 개요를 참조하세요.

관리자는 AWS JSON 정책을 사용하여 누가 무엇을 액세스할 수 있는지 지정할 수 있습니다. 즉, 어떤 보안 주체가 어떤 리소스에서 어떤 조건으로 작업을 수행할 수 있는지 지정할 수 있습니다.

모든 IAM 개체(사용자 또는 역할)는 처음에는 권한이 없습니다. 다시 말해, 기본적으로 사용자는 아무 작업도 수행할 수 없으며, 자신의 암호를 변경할 수도 없습니다. 사용자에게 태스크를 수행할 권한을 부여하기 위해 관리자는 사용자에게 권한 정책을 연결해야 합니다. 또한 관리자는 의도한 권한을 가지고 있는 그룹에 사용자를 추가할 수 있습니다. 관리자가 그룹에 권한을 부여하면 그룹의 모든 사용자가 해당 권한을 받습니다.

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

ID 기반 정책

자격 증명 기반 정책은 사용자, 사용자 그룹 또는 역할과 같은 자격 증명에 연결할 수 있는 JSON 권한 정책 문서입니다. 이러한 정책은 사용자와 역할이 어떤 리소스에서 어떤 조건으로 어떤 작업을 수행할 수 있는지 제어합니다. 자격 증명 기반 정책을 생성하는 방법을 알아보려면 IAM 사용 설명서의 IAM 정책 생성을 참조하세요.

보안 인증 기반 정책은 인라인 정책 또는 관리형 정책으로 한층 더 분류할 수 있습니다. 인라인 정책은 단일 사용자, 그룹 또는 역할에 직접 포함됩니다. 관리형 정책은의 여러 사용자, 그룹 및 역할에 연결할 수 있는 독립 실행형 정책입니다 AWS 계정. 관리형 정책에는 AWS 관리형 정책 및 고객 관리형 정책이 포함됩니다. 관리형 정책 또는 인라인 정책을 선택하는 방법을 알아보려면 IAM 사용 설명서의 관리형 정책과 인라인 정책을 참조하세요.

리소스 기반 정책

리소스 기반 정책은 리소스에 연결하는 JSON 정책 설명서입니다. 리소스 기반 정책의 예제는 IAM 역할 신뢰 정책과 Amazon S3 버킷 정책입니다. 리소스 기반 정책을 지원하는 서비스에서 서비스 관리자는 이러한 정책을 사용하여 특정 리소스에 대한 액세스를 통제할 수 있습니다. 정책이 연결된 리소스의 경우 정책은 지정된 보안 주체가 해당 리소스에서 어떤 조건으로 어떤 작업을 수행할 수 있는지 정의합니다. 리소스 기반 정책에서 보안 주체를 지정합니다. 보안 주체에는 계정, 사용자, 역할, 페더레이션 사용자 또는가 포함될 수 있습니다 AWS 서비스.

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

Nimble Studio의 액세스 제어 목록(ACL)

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

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

기타 정책 타입

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

- 권한 경계 – 권한 경계는 자격 증명 기반 정책에 따라 IAM 엔터티(IAM 사용자 또는 역할)에 부여할 수 있는 최대 권한을 설정하는 고급 기능입니다. 개체에 대한 권한 경계를 설정할 수 있습니다. 그 결과로 얻는 권한은 엔터티의 자격 증명 기반 정책과 그 권한 경계의 교집합입니다. `Principal` 필드에서 사용자나 역할을 지정하는 리소스 기반 정책은 권한 경계에 의해 제한되지 않습니다. 이러한 정책 중 하나에 포함된 명시적 거부는 허용을 재정의합니다. 권한 경계에 대한 자세한 내용은 IAM 사용 설명서의 IAM 엔터티의 권한 범위를 참조하세요.
- 서비스 제어 정책(SCP) – SCP는 Organizations에서 조직 또는 조직 단위(OU)에 대한 최대 권한을 지정하는 JSON 정책입니다. Organizations는 비즈니스가 소유하는 여러 AWS 계정 을 그룹화하

고 중앙에서 관리할 수 있는 서비스입니다. 조직에서 모든 기능을 활성화할 경우, 서비스 제어 정책(SCP)을 임의의 또는 모든 계정에 적용할 수 있습니다. SCP는 각 AWS 계정 루트 사용자를 포함하여 멤버 계정의 엔터티에 대한 권한을 제한합니다. 조직 및 SCPs에 대한 자세한 내용은 AWS Organizations 사용 설명서의 SCPs 작동 방식을 참조하세요.

- 세션 정책 – 세션 정책은 역할 또는 페더레이션 사용자에 대해 임시 세션을 프로그래밍 방식으로 생성할 때 파라미터로 전달하는 고급 정책입니다. 결과적으로 얻는 세션의 권한은 사용자 또는 역할의 자격 증명 기반 정책과 세션 정책의 교집합입니다. 또한 권한을 리소스 기반 정책에서 가져올 수도 있습니다. 이러한 정책 중 하나에 포함된 명시적 거부는 허용을 재정의합니다. 자세한 정보는 IAM 사용 설명서의 세션 정책을 참조하세요.

여러 정책 유형

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

Amazon Nimble Studio에서 IAM을 사용하는 방법

IAM을 사용하여 Nimble Studio에 대한 액세스를 관리하기 전에 Nimble Studio에서 사용할 수 있는 IAM 기능을 알아보세요.

Amazon Nimble Studio에서 사용할 수 있는 IAM 기능

IAM 기능	Nimble Studio 지원
Nimble Studio의 정책 작업	예
Nimble Studio의 정책 리소스	예
Amazon Nimble Studio의 정책 조건 키	예
Nimble Studio의 액세스 제어 목록(ACL)	아니요
Nimble Studio에서 속성 기반 액세스 제어(ABAC)	예
Nimble Studio에서 임시 보안 인증 정보 사용	예
Nimble Studio의 서비스 간 보안 주체 권한	예

IAM 기능	Nimble Studio 지원
Nimble Studio의 서비스 역할	예
Nimble Studio의 서비스 연결 역할	아니요

Nimble Studio 및 기타에서 대부분의 IAM 기능을 AWS 서비스 사용하는 방법을 개괄적으로 알아보려면 IAM 사용 설명서의 AWS 서비스 IAM으로 작업하는 섹션을 참조하세요.

Nimble Studio 자격 증명 기반 정책

보안 인증 기반 정책 지원	예

자격 증명 기반 정책은 사용자, 사용자 그룹 또는 역할과 같은 자격 증명에 연결할 수 있는 JSON 권한 정책 문서입니다. 이러한 정책은 사용자와 역할이 어떤 리소스에서 어떤 조건으로 어떤 작업을 수행할 수 있는지 제어합니다. 자격 증명 기반 정책을 생성하는 방법을 알아보려면 IAM 사용 설명서의 IAM 정책 생성을 참조하세요.

IAM 자격 증명 기반 정책을 사용하면 허용되거나 거부되는 작업과 리소스뿐 아니라 작업이 허용되거나 거부되는 조건도 지정할 수 있습니다. 자격 증명 기반 정책은 연결된 사용자 또는 역할에 적용되므로 자격 증명 정책에서는 보안 주체를 지정할 수 없습니다. JSON 정책에서 사용할 수 있는 모든 요소에 대해 알아보려면 IAM 사용 설명서의 IAM JSON 정책 요소 참조를 참조하세요.

Amazon Nimble Studio의 자격 증명 기반 정책 예제

Nimble Studio 자격 증명 기반 정책 예제를 보려면 Amazon Nimble Studio의 자격 증명 기반 정책 예제를 참조하세요.

Nimble Studio 내 리소스 기반 정책

리소스 기반 정책 지원	아니요

Nimble Studio는 리소스 기반 정책이나 크로스 계정 액세스를 지원하지 않습니다. 리소스 기반 정책은 리소스에 연결하는 JSON 정책 설명서입니다. 리소스 기반 정책의 예제는 IAM 역할 신뢰 정책과 Amazon S3 버킷 정책입니다. 리소스 기반 정책을 지원하는 서비스에서 서비스 관리자는 이러한 정책을 사용하여 특정 리소스에 대한 액세스를 통제할 수 있습니다. 정책이 연결된 리소스의 경우 정책은

지정된 보안 주체가 해당 리소스에서 어떤 조건으로 어떤 작업을 수행할 수 있는지 정의합니다. 리소스 기반 정책에서 보안 주체를 지정합니다. 보안 주체에는 계정, 사용자, 역할, 페더레이션 사용자 또는가 포함될 수 있습니다 AWS 서비스.

Nimble Studio의 정책 작업

정책 작업 지원	예

관리자는 AWS JSON 정책을 사용하여 누가 무엇을 액세스할 수 있는지 지정할 수 있습니다. 즉, 어떤 보안 주체가 어떤 리소스에서 어떤 조건으로 작업을 수행할 수 있는지 지정할 수 있습니다.

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

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

Nimble Studio 작업 목록을 보려면 서비스 승인 참조의 Amazon Nimble Studio에서 정의한 작업을 참조하세요.

Nimble Studio의 정책 작업은 작업 앞에 다음 접두사를 사용합니다.

```
nimble
```

단일 문에서 여러 작업을 지정하려면 다음과 같이 쉼표로 구분합니다.

```
"Action": [
      "nimble:action1",
      "nimble:action2"
         ]
```

Nimble Studio 자격 증명 기반 정책 예제를 보려면 Amazon Nimble Studio의 자격 증명 기반 정책 예제를 참조하세요.

Nimble Studio의 정책 리소스

정책 리소스 지원	예

관리자는 AWS JSON 정책을 사용하여 누가 무엇을 액세스할 수 있는지 지정할 수 있습니다. 즉, 어떤 보안 주체가 어떤 리소스에서 어떤 조건으로 작업을 수행할 수 있는지 지정할 수 있습니다.

`Resource` JSON 정책 요소는 작업이 적용되는 하나 이상의 객체를 지정합니다. 문에는 `Resource`또는 `NotResource`요소가 반드시 추가되어야 합니다. 모범 사례에 따라 Amazon 리소스 이름(ARN)을 사용하여 리소스를 지정합니다. 리소스 수준 권한이라고 하는 특정 리소스 유형을 지원하는 작업에 대해 이를 수행할 수 있습니다.

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

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

Nimble Studio 자격 증명 기반 정책 예제를 보려면 Amazon Nimble Studio의 자격 증명 기반 정책 예제를 참조하세요.

Amazon Nimble Studio의 정책 조건 키

정책 조건 키 지원	예

관리자는 AWS JSON 정책을 사용하여 누가 무엇을 액세스할 수 있는지 지정할 수 있습니다. 즉, 어떤 보안 주체가 어떤 리소스에서 어떤 조건으로 작업을 수행할 수 있는지 지정할 수 있습니다.

`Condition` 요소(또는 `Condition`**`block`**`) lets you specify conditions in which a statement is in effect. The `Condition` 요소는 선택 사항입니다. 같거나 작음과 같은 조건 연산자를 사용하여 정책의 조건을 요청의 값과 일치시키는 조건식을 생성할 수 있습니다.

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

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

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

Nimble Studio 자격 증명 기반 정책 예제를 보려면 Amazon Nimble Studio의 자격 증명 기반 정책 예제를 참조하세요.

Nimble Studio의 액세스 제어 목록(ACL)

ACL 지원	아니요

Nimble Studio는 액세스 제어 목록(ACL)을 지원하지 않습니다. ACL은 어떤 보안 주체(계정 멤버, 사용자 또는 역할)가 리소스에 액세스할 수 있는 권한을 가지고 있는지 제어합니다. ACL은 리소스 기반 정책과 유사하지만 JSON 정책 문서 형식을 사용하지 않습니다.

Nimble Studio에서 속성 기반 액세스 제어(ABAC)

ABAC 지원(정책의 태그)	예

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

태그에 근거하여 액세스를 제어하려면 `aws:ResourceTag/key-name`, `aws:RequestTag/key-name` 또는 `aws:TagKeys` 조건 키를 사용하여 정책의 조건 요소에 태그 정보를 제공합니다.

ABAC에 대한 자세한 정보는 IAM 사용 설명서의 AWS용 ABAC란 무엇입니까?를 참조하세요. ABAC 설정 단계가 포함된 자습서를 보려면 IAM 사용 설명서의 속성 기반 액세스 제어(ABAC) 사용을 참조하세요.

Nimble Studio에서 임시 보안 인증 정보 사용

임시 보안 인증 지원	예

임시 자격 증명을 사용하여 로그인할 때 작동하지 AWS 서비스 않는 경우도 있습니다. 임시 자격 증명으로 AWS 서비스 작업하는을 비롯한 추가 정보는 AWS 서비스 IAM 사용 설명서의 IAM으로 작업하는를 참조하세요.

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

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

Nimble Studio의 서비스 간 보안 주체 권한

보안 주체 권한 지원	예

Nimble Studio의 서비스 역할

서비스 역할 지원	예

서비스 역할은 서비스가 사용자를 대신하여 작업을 수행하는 것으로 가정하는 IAM 역할입니다. 서비스 역할은 해당 계정 내에서만 액세스를 제공하며 다른 계정의 서비스에 대한 액세스를 부여하는 데 사용할 수 없습니다. 관리자는 IAM 내에서 서비스 역할을 생성, 수정, 삭제할 수 있습니다. 자세한 내용은 IAM 사용 설명서의 AWS 서비스에 대한 권한을 위임할 역할 생성을 참조하세요.

> **Warning**
>
> 서비스 역할의 권한을 변경하면 Nimble Studio 기능이 중단될 수 있습니다. Nimble Studio가 관련 지침을 제공하는 경우에만 서비스 역할을 편집하세요.

Nimble Studio의 서비스 연결 역할

서비스 연결 역할 지원	아니요

Nimble Studio는 서비스 연결 역할을 지원하지 않습니다. 서비스 연결 역할은에 연결된 서비스 역할의 한 유형입니다 AWS 서비스. 서비스는 사용자를 대신하여 태스크를 수행하기 위해 역할을 수임할 수 있습니다. 서비스 연결 역할은 IAM 계정에 표시되고, 서비스가 소유합니다. 관리자는 서비스 연결 역할의 권한을 볼 수 있지만 편집은 할 수 없습니다.

서비스 연결 역할 생성 또는 관리에 대한 자세한 내용은 AWS 서비스 IAM으로 작업하는 서비스를 참조하세요. 서비스 연결 역할 열에서 Yes가 포함된 서비스를 테이블에서 찾습니다. 해당 서비스에 대한 서비스 연결 역할 설명서를 보려면 예 링크를 선택합니다.

Amazon Nimble Studio의 자격 증명 기반 정책 예제

기본적으로 사용자 및 역할에는 Nimble Studio 리소스를 생성하거나 수정할 수 있는 권한이 없습니다. 또한 AWS Management Console AWS CLI또는 AWS API를 사용하여 작업을 수행할 수 없습니다. 관리자는 리소스에서 작업을 수행할 수 있는 권한을 사용자와 역할에게 부여하는 IAM 정책을 생성해야 합니다. 그런 다음 관리자는 해당 권한이 필요한 사용자 또는 그룹에 이러한 정책을 연결해야 합니다.

이러한 예제 JSON 정책 문서를 사용하여 IAM 자격 증명 기반 정책을 생성하는 방법을 알아보려면 IAM 사용 설명서의 IAM 정책 생성을 참조하세요.

주제

- 정책 모범 사례

정책 모범 사례

자격 증명 기반 정책은 매우 강력합니다. 이 정책은 계정에서 사용자가 Nimble Studio 리소스를 생성, 액세스 또는 삭제할 수 있는지 여부를 결정합니다. 이 작업으로 인해 AWS 계정에 비용이 발생할 수 있습니다. ID 기반 정책을 생성하거나 편집할 때는 다음 지침과 권장 사항을 따릅니다.

- AWS 관리형 정책 사용 시작하기 - Nimble Studio를 빠르게 사용하려면 AWS 관리형 정책을 사용하여 직원에게 필요한 권한을 부여하세요. 이 정책은 이미 계정에서 사용할 수 있으며 AWS에 의해 유지 관리 및 업데이트됩니다. 자세한 내용은 IAM 사용 설명서의 AWS 관리형 정책으로 권한 사용 시작하기를 참조하세요.
- 최소 권한 부여 - 사용자 지정 정책을 생성할 때 태스크를 수행하는 데 필요한 권한만 부여합니다. 최소한의 권한 조합으로 시작하여 필요에 따라 추가 권한을 부여합니다. 처음부터 권한을 많이 부여한 후 나중에 줄이는 방법보다 이 방법이 안전합니다. 자세한 정보는 IAM 사용 설명서의 최소 권한 부여를 참조하십시오.

- 중요한 작업에 대해 MFA 활성화 - 보안을 강화하기 위해 IAM 사용자가 중요한 리소스 또는 API 작업에 액세스할 때 다중 인증(MFA)을 사용하도록 합니다. 자세한 정보는 IAM 사용 설명서의 AWS에서 다중 인증(MFA) 사용을 참조하세요.
- 보안 강화를 위해 정책 조건 사용 – 실제로 가능한 경우 자격 증명 기반 정책이 리소스에 대한 액세스를 허용하는 조건을 정의합니다. 예를 들어 요청을 할 수 있는 IP 주소의 범위를 지정하도록 조건을 작성할 수 있습니다. 지정된 날짜 또는 시간 범위 내에서만 요청을 허용하거나, SSL 또는 MFA를 사용해야 하는 조건을 작성할 수도 있습니다. 자세한 내용은 IAM 사용 설명서의 IAM JSON 정책 요소: 조건을 참조하세요.

AWS Amazon Nimble Studio에 대한 관리형 정책

사용자, 그룹 및 역할에 권한을 추가하려면 직접 정책을 작성하는 것보다 AWS 관리형 정책을 사용하는 것이 더 쉽습니다. 팀에 필요한 권한만 제공하는 IAM 고객 관리형 정책을 생성하기 위해서는 시간과 전문 지식이 필요합니다. 빠르게 시작하려면 AWS 관리형 정책을 사용할 수 있습니다. 이 정책은 일반적인 사용 사례를 다루며 사용자의 AWS 계정에서 사용할 수 있습니다. AWS 관리형 정책에 대한 자세한 내용은 IAM 사용 설명서의 AWS 관리형 정책을 참조하세요.

AWS 서비스는 AWS 관리형 정책을 유지 관리하고 업데이트합니다. AWS 관리형 정책에서는 권한을 변경할 수 없습니다. 서비스에서 때때로 추가 권한을 AWS 관리형 정책에 추가하여 새로운 기능을 지원합니다. 이 유형의 업데이트는 정책이 연결된 모든 ID(사용자, 그룹 및 역할)에 적용됩니다. 서비스는 새로운 기능이 시작되거나 새 작업을 사용할 수 있을 때 AWS 관리형 정책에 업데이트됩니다. 서비스는 AWS 관리형 정책에서 권한을 제거하지 않으므로 정책 업데이트가 기존 권한을 손상시키지 않습니다.

또한 여러 서비스에 걸쳐 있는 직무에 대한 관리형 정책을 AWS 지원합니다. 예를 들어 ReadOnlyAccess AWS 관리형 정책은 모든 AWS 서비스 및 리소스에 대한 읽기 전용 액세스를 제공합니다. 서비스에서 새 기능을 시작하면 AWS (이)가 새 작업 및 리소스에 대한 읽기 전용 권한을 추가합니다. 직무 정책의 목록과 설명은 IAM 사용 설명서의 직무에 관한AWS 관리형 정책을 참조하세요.

최종 사용자는 주로 Nimble Studio 포털을 사용하여 Amazon Nimble Studio에 액세스합니다. StudioBuilder 또는 Nimble Studio 콘솔을 사용하여 스튜디오를 생성할 때 스튜디오 페르소나마다 하나씩 IAM 역할(스튜디오 관리자 및 스튜디오 사용자)이 생성됩니다. 각각에는 해당 IAM 관리형 정책이 연결되어 있습니다. Nimble Studio 포털은 사용자가 액세스 권한이 있는 리소스만 나열하고 사용할 수 있는 경험을 제공합니다.

Nimble Studio 포털은 사용자가 액세스 권한이 있는 리소스만 나열하고 사용할 수 있는 경험을 제공하며, 포털의 올바른 운영은 이러한 정책의 내용에 따라 결정됩니다. Nimble Studio 최종 사용자는 포털을 사용하여 클라우드 스튜디오에 액세스합니다. 따라서 관리자가 StudioBuilder를 사용하여 스튜디오

를 생성하면 스튜디오에 액세스해야 하는 사용자당 하나의 IAM 역할이 생성됩니다. 여기에는 스튜디오 관리자와 스튜디오 사용자가 포함되며, 각 역할에는 해당 IAM 관리형 정책이 연결되어 있습니다.

직무 정책의 목록과 설명은 IAM 사용 설명서의 직무에 관한AWS 관리형 정책을 참조하세요.

AWS 관리형 정책: **AmazonNimbleStudio-LaunchProfileWorker**

AmazonNimbleStudio-LaunchProfileWorker 정책을 IAM 보안 인증에 연결할 수 있습니다.

이 정책을 Nimble Studio Builder에서 생성한 EC2 인스턴스에 연결하여 Nimble Studio 시작 프로파일 작업자에게 필요한 리소스에 대한 액세스 권한을 부여합니다.

권한 세부 정보

이 정책에는 다음 권한이 포함되어 있습니다.

- ds - LaunchProfile 작업자가 LaunchProfile에 연결된 AWS Managed Microsoft AD 에 대한 연결 정보를 검색할 수 있도록 합니다.
- ec2 - LaunchProfile 작업자가 LaunchProfile에 연결하기 위한 보안 그룹 및 서브넷 정보를 검색할 수 있도록 합니다.
- fsx - LaunchProfile 작업자가 LaunchProfile에 연결된 Amazon FSx 볼륨에 대한 연결 정보를 검색할 수 있도록 합니다.

```
{
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeSecurityGroups",
        "fsx:DescribeFileSystems",
        "ds:DescribeDirectories"
      ],
      "Resource": [
        "*"
      ],
      "Condition": {
        "StringEquals": {
          "aws:CalledViaLast": "nimble.amazonaws.com"
        }
      },
```

```
      "Sid": "GetLaunchProfileInitializationDependencies"
    }
  ],
  "Version": "2012-10-17"
}
```

AWS 관리형 정책: **AmazonNimbleStudio-StudioAdmin**

AmazonNimbleStudio-StudioAdmin 정책을 IAM 보안 인증에 연결할 수 있습니다.

이 정책을 스튜디오와 연결된 관리자 역할에 연결하여 스튜디오 관리자와 연결된 Amazon Nimble Studio 리소스 및 다른 서비스의 관련 스튜디오 리소스에 대한 액세스 권한을 부여합니다.

권한 세부 정보

이 정책에는 다음 권한이 포함되어 있습니다.

- nimble - 스튜디오 사용자가 StudioAdmins가 위임한 Nimble 리소스에 액세스할 수 있도록 합니다.
- sso - 스튜디오 사용자가 스튜디오에 있는 다른 사용자의 이름을 볼 수 있도록 합니다.
- identitystore - 스튜디오 사용자가 스튜디오에 있는 다른 사용자의 이름을 볼 수 있도록 합니다.
- ds - Nimble Studio가 스튜디오와 AWS Managed Microsoft AD 연결된에 가상 워크스테이션을 추가할 수 있도록 허용합니다.
- ec2 - Nimble Studio가 구성된 VPC에 가상 워크스테이션을 연결할 수 있도록 합니다.
- fsx - Nimble Studio가 구성된 Amazon FSx 볼륨에 가상 워크스테이션을 연결할 수 있도록 합니다.
- cloudwatch - Nimble Studio가 CloudWatch 지표를 검색할 수 있도록 합니다.

```
{
  "Statement": [
    {
      "Sid": "StudioAdminFullAccess",
      "Effect": "Allow",
      "Action": [
        "nimble:CreateStreamingSession",
        "nimble:GetStreamingSession",
        "nimble:StartStreamingSession",
        "nimble:StopStreamingSession",
        "nimble:CreateStreamingSessionStream",
        "nimble:GetStreamingSessionStream",
        "nimble:DeleteStreamingSession",
        "nimble:ListStreamingSessionBackups",
```

```
        "nimble:GetStreamingSessionBackup",
        "nimble:ListEulas",
        "nimble:ListEulaAcceptances",
        "nimble:GetEula",
        "nimble:AcceptEulas",
        "nimble:ListStudioMembers",
        "nimble:GetStudioMember",
        "nimble:ListStreamingSessions",
        "nimble:GetStreamingImage",
        "nimble:ListStreamingImages",
        "nimble:GetLaunchProfileInitialization",
        "nimble:GetLaunchProfileDetails",
        "nimble:GetFeatureMap",
        "nimble:PutStudioLogEvents",
        "nimble:ListLaunchProfiles",
        "nimble:GetLaunchProfile",
        "nimble:GetLaunchProfileMember",
        "nimble:ListLaunchProfileMembers",
        "nimble:PutLaunchProfileMembers",
        "nimble:UpdateLaunchProfileMember",
        "nimble:DeleteLaunchProfileMember"
      ],
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": [
        "sso-directory:DescribeUsers",
        "sso-directory:SearchUsers",
        "identitystore:DescribeUser",
        "identitystore:ListUsers"
      ],
      "Resource": [
        "*"
      ]
    },
    {
      "Effect": "Allow",
      "Action": [
        "ds:CreateComputer",
        "ds:DescribeDirectories",
        "ec2:DescribeSubnets",
        "ec2:CreateNetworkInterface",
        "ec2:DescribeNetworkInterfaces",
```

```
        "ec2:DeleteNetworkInterface",
        "ec2:CreateNetworkInterfacePermission",
        "ec2:DeleteNetworkInterfacePermission",
        "ec2:DescribeSecurityGroups",
        "fsx:DescribeFileSystems"
      ],
      "Resource": [
        "*"
      ],
      "Condition": {
        "StringEquals": {
          "aws:CalledViaLast": "nimble.amazonaws.com"
        }
      }
    },
    {
      "Effect": "Allow",
      "Action": "cloudwatch:GetMetricData",
      "Resource": "*",
      "Condition": {
        "StringEquals": {
          "cloudwatch:namespace": "AWS/NimbleStudio"
        }
      }
    }
  ],
  "Version": "2012-10-17"
}
```

AWS 관리형 정책: **AmazonNimbleStudio-StudioUser**

AmazonNimbleStudio-StudioUser 정책을 IAM 보안 인증에 연결할 수 있습니다.

이 정책을 스튜디오와 관련된 사용자 역할에 연결하여 스튜디오 사용자와 연결된 Amazon Nimble Studio 리소스 및 다른 서비스의 관련 스튜디오 리소스에 대한 액세스 권한을 부여합니다.

권한 세부 정보

이 정책에는 다음 권한이 포함되어 있습니다.

- nimble - 스튜디오 사용자가 StudioAdmins가 위임한 Nimble 리소스에 액세스할 수 있도록 합니다.
- sso - 스튜디오 사용자가 스튜디오에 있는 다른 사용자의 이름을 볼 수 있도록 합니다.

- identitystore - 스튜디오 사용자가 스튜디오에 있는 다른 사용자의 이름을 볼 수 있도록 합니다.
- ds - Nimble Studio가 스튜디오와 AWS Managed Microsoft AD 연결된에 가상 워크스테이션을 추가할 수 있도록 허용합니다.
- ec2 - Nimble Studio가 구성된 VPC에 가상 워크스테이션을 연결할 수 있도록 합니다.
- fsx - Nimble Studio가 구성된 Amazon FSx 볼륨에 가상 워크스테이션을 연결할 수 있도록 합니다.

```
{
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "ds:CreateComputer",
        "ec2:DescribeSubnets",
        "ec2:CreateNetworkInterfacePermission",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DeleteNetworkInterfacePermission",
        "ec2:DeleteNetworkInterface",
        "ec2:CreateNetworkInterface",
        "ec2:DescribeSecurityGroups",
        "fsx:DescribeFileSystems",
        "ds:DescribeDirectories"
      ],
      "Resource": [
        "*"
      ],
      "Condition": {
        "StringEquals": {
          "aws:CalledViaLast": "nimble.amazonaws.com"
        }
      }
    },
    {
      "Effect": "Allow",
      "Action": [
        "sso-directory:DescribeUsers",
        "sso-directory:SearchUsers",
        "identitystore:DescribeUser",
        "identitystore:ListUsers"
      ],
      "Resource": [
        "*"
```

```
      ]
    },
    {
      "Effect": "Allow",
      "Action": [
        "nimble:ListLaunchProfiles"
      ],
      "Resource": "*",
      "Condition": {
        "StringEquals": {
          "nimble:requesterPrincipalId": "${nimble:principalId}"
        }
      }
    },
    {
      "Effect": "Allow",
      "Action": [
        "nimble:ListStudioMembers",
        "nimble:GetStudioMember",
        "nimble:ListEulas",
        "nimble:ListEulaAcceptances",
        "nimble:GetFeatureMap",
        "nimble:PutStudioLogEvents"
      ],
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": [
        "nimble:StartStreamingSession",
        "nimble:StopStreamingSession",
        "nimble:DeleteStreamingSession",
        "nimble:GetStreamingSession",
        "nimble:CreateStreamingSessionStream",
        "nimble:GetStreamingSessionStream",
        "nimble:ListStreamingSessions"
        "nimble:ListStreamingSessionBackups",
        "nimble:GetStreamingSessionBackup"
      ],
      "Resource": "*",
      "Condition": {
        "StringEquals": {
          "nimble:ownedBy": "${nimble:requesterPrincipalId}"
        }
```

```
      }
    }
  ],
  "Version": "2012-10-17"
}
```

AWS 관리형 정책에 대한 Nimble Studio 업데이트

이 서비스가 이러한 변경 사항을 추적하기 시작한 이후 Amazon Nimble Studio의 AWS 관리형 정책 업데이트에 대한 세부 정보를 봅니다.

변경 사항	설명	날짜
AWS 관리형 정책: AmazonNimbleStudio-StudioUser - 정책 업데이트	최신 버전의 자격 증명 스토어 서비스를 사용하도록 Amazon Nimble Studio가 정책을 업데이트했습니다.	2023년 9월 22일
AWS 관리형 정책: AmazonNimbleStudio-StudioAdmin - 정책 업데이트	최신 버전의 자격 증명 스토어 서비스를 사용하도록 Amazon Nimble Studio가 정책을 업데이트했습니다.	2023년 9월 22일
AWS 관리형 정책: AmazonNimbleStudio-StudioUser - 정책 업데이트	스튜디오 사용자가 워크스테이션 백업을 볼 수 있도록 Amazon Nimble Studio가 정책을 업데이트했습니다.	2022년 12월 20일
AWS 관리형 정책: AmazonNimbleStudio-StudioAdmin - 정책 업데이트	스튜디오 관리자가 워크스테이션 백업을 볼 수 있도록 Amazon Nimble Studio가 정책을 업데이트했습니다.	2022년 12월 20일
AWS 관리형 정책: AmazonNimbleStudio-StudioUser - 정책 업데이트	스튜디오 관리자가 CloudWatch 지표를 검색할 수 있도록 Amazon Nimble Studio가 정책을 업데이트했습니다.	2021년 11월 11일

변경 사항	설명	날짜
AWS 관리형 정책: AmazonNimbleStudio-StudioUser - 정책 업데이트	스튜디오 사용자가 워크스테이션을 시작하고 중지할 수 있도록 Amazon Nimble Studio가 정책을 업데이트했습니다.	2021년 11월 1일
AWS 관리형 정책: AmazonNimbleStudio-StudioAdmin - 정책 업데이트	스튜디오 관리자가 워크스테이션을 시작하고 중지할 수 있도록 Amazon Nimble Studio가 정책을 업데이트했습니다.	2021년 11월 1일
AWS 관리형 정책: AmazonNimbleStudio-StudioUser - 정책 업데이트	`nimble:createdBy` 대신 `nimble:ownedBy` 에 기반하여 스트리밍 세션 리소스에 대한 액세스를 조건부로 허용하도록 Amazon Nimble Studio가 정책을 업데이트했습니다.	2021년 8월 16일
AWS 관리형 정책: AmazonNimbleStudio-StudioUser - 새 정책	Amazon Nimble Studio가 스튜디오 사용자와 연결된 리소스 및 다른 서비스의 관련 스튜디오 리소스에 대한 액세스를 허용하는 새 정책을 추가했습니다.	2021년 4월 28일
AWS 관리형 정책: AmazonNimbleStudio-StudioAdmin - 새 정책	Amazon Nimble Studio가 스튜디오 관리자와 연결된 리소스 및 다른 서비스의 관련 스튜디오 리소스에 대한 액세스를 허용하는 새 정책을 추가했습니다.	2021년 4월 28일
AWS 관리형 정책: AmazonNimbleStudio-LaunchProfileWorker - 새 정책	Amazon Nimble Studio가 Nimble Studio 시작 프로파일 작업자에게 필요한 리소스에 대한 액세스를 허용하는 새 정책을 추가했습니다.	2021년 4월 28일

변경 사항	설명	날짜
Amazon Nimble Studio가 변경 사항 추적 시작	Amazon Nimble Studio는 AWS 관리형 정책에 대한 변경 사항 추적을 시작했습니다.	2021년 4월 28일

교차 서비스 혼동된 대리자 방지

혼동된 대리자 문제는 작업을 수행할 권한이 없는 엔터티가 권한이 더 많은 엔터티에게 작업을 수행하도록 강요할 수 있는 보안 문제입니다. 에서 AWS교차 서비스 위장은 혼동된 대리자 문제를 초래할 수 있습니다. 교차 서비스 가장은 한 서비스(호출하는 서비스)가 다른 서비스(호출되는 서비스)를 직접적으로 호출할 때 발생할 수 있습니다. 호출하는 서비스가 액세스 권한이 없는 다른 고객의 리소스에서 그 권한을 사용하여 허용되지 않는 작업을 하도록 조작될 수 있습니다. 이를 방지하기 위해 AWS 에서는 계정의 리소스에 대한 액세스 권한이 부여된 서비스 보안 주체를 사용하여 모든 서비스에 대한 데이터를 보호하는 데 도움이 되는 도구를 제공합니다.

Identity and Access Management(IAM)가 Amazon Nimble Studio에 제공하는 리소스 액세스 권한을 제한하려면 리소스 정책에서 `aws:SourceArn` 및 `aws:SourceAccount` 글로벌 조건 컨텍스트 키를 사용하는 것이 좋습니다. 두 글로벌 조건 컨텍스트 키를 모두 사용하는 경우 `aws:SourceAccount` 값과 `aws:SourceArn` 값의 계정은 동일한 정책 문에서 사용될 때 동일한 계정 ID를 사용해야 합니다.

`aws:SourceArn`의 값은 스튜디오의 ARN이어야 하고, `aws:SourceAccount`는 계정 ID여야 합니다. 스튜디오는 Nimble Studio에서 생성되기 때문에 생성되기 전까지는 스튜디오 ID가 무엇인지 알 수 없습니다. 스튜디오가 생성되면 최종 스튜디오 ID를 `aws:SourceArn`으로 설정하여 신뢰 정책을 업데이트할 수 있습니다.

혼동된 대리인 문제로부터 보호하는 가장 효과적인 방법은 리소스의 전체 ARN이 포함된 `aws:SourceArn` 글로벌 조건 컨텍스트 키를 사용하는 것입니다. 리소스의 전체 ARN을 모르거나 여러 리소스를 지정하는 경우, ARN의 알 수 없는 부분에 와일드카드(*)를 포함한 `aws:SourceArn` 글로벌 조건 컨텍스트 키를 사용합니다. 예: `arn:aws:nimble::123456789012:*`.

최종 사용자는 Nimble Studio 포털에 로그인하면 스튜디오 역할을 수임합니다. 스튜디오를 생성할 때는 역할을 AWS 구성하고 정책 평가를 수행합니다.는 사용자 중 한 명이 Nimble Studio 포털에 로그인할 때마다 정책을 AWS 평가합니다. 스튜디오를 생성할 때 `aws:SourceArn`을 수정할 수 없습니다. 스튜디오 생성을 완료한 후 studioARN을 `aws:SourceArn`에 사용할 수 있습니다.

다음 예제는 Nimble Studio에서 `aws:SourceArn` 및 `aws:SourceAccount` 전역 조건 컨텍스트 키를 사용하여 혼동된 대리자 문제를 방지하는 방법을 보여 주는 역할 수임 정책입니다.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "identity.nimble.amazonaws.com"
      },
      "Action": [
        "sts:AssumeRole",
        "sts:TagSession"
      ],
      "Condition": {
        "StringEquals": {
          "aws:SourceAccount": "123456789012"
        },
        "StringLike": {
          "aws:SourceArn": "arn:aws:nimble:us-west-2:123456789012:studio/*"
        }
      }
    }
  ]
}
```

Amazon Nimble Studio 자격 증명 및 액세스 문제 해결

다음 정보를 사용하여 Nimble Studio 및 IAM 작업 시 발생할 수 있는 공통적인 문제를 진단하고 수정할 수 있습니다.

주제

- Nimble Studio에서 작업을 수행할 권한이 없습니다.
- iam:PassRole을 수행할 권한이 없습니다.
- 액세스 키를 확인하고자 합니다.
- 관리자인데, 다른 사용자의 Nimble Studio 액세스를 허용하려고 합니다.
- 내 외부의 사람이 내 Nimble Studio 리소스에 액세스 AWS 계정 하도록 허용하려고 합니다.

Nimble Studio에서 작업을 수행할 권한이 없습니다.

작업을 수행할 권한이 없다는 오류가 수신되면, 작업을 수행할 수 있도록 정책을 업데이트해야 합니다.

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

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

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

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

iam:PassRole을 수행할 권한이 없습니다.

iam:PassRole 작업을 수행할 권한이 없다는 오류가 수신되면 관리자에게 문의하여 도움을 받으세요. 역할을 Nimble Studio로 전달하도록 허용하는 정책을 업데이트하도록 요청합니다.

일부 AWS 서비스 에서는 새 서비스 역할 또는 서비스 연결 역할을 생성하는 대신 기존 역할을 해당 서비스에 전달할 수 있습니다. 이렇게 하려면 서비스에 역할을 전달할 수 있는 권한이 필요합니다.

다음 예제 오류는 johndoe라는 사용자가 콘솔을 사용하여 Nimble Studio에서 작업을 수행하려고 하는 경우에 발생합니다. 하지만 태스크를 수행하려면 서비스에 서비스 역할이 부여한 권한이 있어야 합니다. John은 서비스에 역할을 전달할 수 있는 권한을 가지고 있지 않습니다.

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

이 경우 John은 iam:PassRole 작업을 수행할 권한을 부여하도록 정책을 업데이트할 것을 관리자에게 요청합니다.

액세스 키를 확인하고자 합니다.

Amazon Nimble Studio는 액세스 키를 제공하지 않습니다. 비밀 액세스 키에 대한 자세한 내용은 IAM 사용 설명서의 액세스 키 관리를 참조하세요.

> **Important**
>
> 정식 사용자 ID 찾기를 돕기 위해서라고 하더라도 액세스 키를 제3자에게 제공하지 마세요. 이로 인해 다른 사람에게 계정에 대한 영구 액세스를 제공하게 될 수 있습니다.

액세스 키 페어를 생성할 때 액세스 키 ID와 비밀 액세스 키를 안전한 위치에 저장하라는 메시지가 표시됩니다. 보안 액세스 키는 생성할 때만 사용할 수 있습니다. 비밀 액세스 키를 잃어버린 경우 새로운

액세스 키를 사용자에게 추가하세요. 최대 두 개의 액세스 키를 가질 수 있습니다. 이미 두 개가 있는 경우 새로 생성하려면 먼저 키 페어 하나를 삭제합니다. 지침을 보려면 IAM 사용 설명서의 액세스 키 관리를 참조하세요.

관리자인데, 다른 사용자의 Nimble Studio 액세스를 허용하려고 합니다.

다른 사용자가 Nimble Studio에 액세스하도록 허용하려면 액세스 권한이 필요한 사용자나 애플리케이션에 대한 IAM 엔터티(사용자 또는 역할)를 생성하세요. 다른 사용자들은 해당 엔터티에 대한 보안 인증을 사용해 AWS에 액세스합니다. 그런 다음 올바른 권한을 부여하는 정책을 엔터티에 연결합니다.

Nimble Studio는 AWS Management Console에서 `AmazonNimbleStudio-StudioUser`를 제공합니다. 콘솔을 관리하는 IT 관리자는 이 정책을 사용하여 다른 사용자에게 스튜디오 액세스 권한을 부여합니다.

관리자 정책 사용에 대한 자습서는 Nimble Studio 설정 안내서를 참조하세요. 사용자 및 시작 프로파일 정책과 같은 기존 정책을 사용자에 연결하는 방법을 알아보려면 IAM 사용자 생성(콘솔)을 참조하세요.

정책 가져오기에 대한 자세한 내용은 IAM 사용 설명서의 IAM 위임 사용자 및 그룹 처음 생성을 참조하세요.

내 외부의 사람이 내 Nimble Studio 리소스에 액세스 AWS 계정 하도록 허용하려고 합니다.

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

자세히 알아보려면 다음을 참조하세요.

- Nimble Studio에서 이러한 기능을 지원하는지 알아보려면 Amazon Nimble Studio에서 IAM을 사용하는 방법 단원을 참조하세요.
- 소유 AWS 계정 한의 리소스에 대한 액세스 권한을 제공하는 방법을 알아보려면 IAM 사용 설명서의 소유 AWS 계정 한 다른의 IAM 사용자에게 액세스 권한 제공을 참조하세요.
- 타사에 리소스에 대한 액세스 권한을 제공하는 방법을 알아보려면 IAM 사용 설명서의 타사 AWS 계정 소유에 대한 액세스 권한 제공을 AWS 계정참조하세요.
- ID 페더레이션을 통해 액세스 권한을 제공하는 방법을 알아보려면 IAM 사용 설명서의 외부에서 인증된 사용자에게 액세스 권한 제공(ID 페더레이션)을 참조하세요.

- 크로스 계정 액세스를 위한 역할과 리소스 기반 정책 사용의 차이점을 알아보려면 IAM 사용 설명서의 IAM 역할과 리소스 기반 정책의 차이를 참조하세요.

Nimble Studio의 보안 이벤트 로깅 및 모니터링

모니터링은 Amazon Nimble Studio 및 AWS 솔루션의 안정성, 가용성 및 성능을 유지하는 데 중요한 부분입니다. AWS 솔루션의 모든 부분에서 모니터링 데이터를 수집하여 다중 지점 장애가 발생할 경우 더 쉽게 디버깅할 수 있습니다.

AWS 및 Nimble Studio는 를 사용하여 Nimble Studio 호출 로깅 AWS CloudTrail 및 AWS CloudFormation 사용 설명서를 포함하여 리소스를 모니터링하고 잠재적 인시던트에 대응할 수 있는 도구를 제공합니다.

JSON 및 YAML 템플릿의 예를 AWS CloudFormation포함하여 Amazon Nimble Studio가 작동하는 방식에 대한 자세한 내용은 AWS CloudFormation 사용 설명서의 Amazon Nimble Studio 리소스 및 속성 참조를 참조하세요. CloudFormation 템플릿을 사용하는 방법을 이해하려면 AWS CloudFormation 개념을 참조하세요.

주제

- 를 사용하여 Nimble Studio 호출 로깅 AWS CloudTrail

를 사용하여 Nimble Studio 호출 로깅 AWS CloudTrail

Amazon Nimble Studio는 Nimble Studio AWS 서비스 에서 사용자 AWS CloudTrail, 역할 또는가 수행한 작업에 대한 레코드를 제공하는 서비스와 통합됩니다. CloudTrail은 Nimble Studio에 대한 모든 API 직접 호출을 이벤트로 캡처합니다. 캡처되는 호출에는 Nimble Studio 콘솔로부터의 호출과 Amazon Nimble Studio 작업에 대한 코드 호출이 포함됩니다.

추적을 생성하면 Nimble Studio 이벤트를 포함한 CloudTrail 이벤트를 지속적으로 Amazon S3 버킷에 배포할 수 있습니다. 추적을 구성하지 않은 경우에도 CloudTrail 콘솔의 이벤트 기록에서 최신 이벤트를 볼 수 있습니다. CloudTrail에서 수집한 정보를 사용하여 Nimble Studio에 수행된 요청, 요청이 수행된 IP 주소, 요청을 수행한 사람, 요청이 수행된 시간 및 추가 세부 정보를 확인할 수 있습니다.

CloudTrail의 Nimble Studio 정보

CloudTrail은 계정을 생성할 AWS 계정 때에서 활성화됩니다. Nimble Studio에서 활동이 발생하면, 해당 활동은 이벤트 기록의 다른 AWS 서비스 이벤트와 함께 CloudTrail 이벤트 로그에 기록됩니다. 에서

최근 이벤트를 보고 검색하고 다운로드할 수 있습니다 AWS 계정. 자세한 정보는 CloudTrail 이벤트 기록을 사용하여 이벤트 보기를 참조하세요.

Nimble Studio에 대한 이벤트를 AWS 계정포함하여에서 이벤트를 지속적으로 기록하려면 추적을 생성합니다. CloudTrail은 추적을 사용하여 Amazon S3 버킷으로 로그 파일을 전송할 수 있습니다. 콘솔에서 추적을 생성하면 기본적으로 모든 AWS 리전에 추적이 적용됩니다. 추적은 AWS 파티션의 모든 리전에서 이벤트를 로깅하고 지정한 Amazon S3 버킷으로 로그 파일을 전송합니다. 또한 CloudTrail 로그에서 수집된 이벤트 데이터를 추가로 분석하고 조치를 취 AWS 서비스 하도록 다른를 구성할 수 있습니다.

자세한 내용은 다음 자료를 참조하세요.

추적 생성 개요

CloudTrail 지원 서비스 및 통합

CloudTrail에 대한 Amazon SNS 알림 구성

여러 리전에서 CloudTrail 로그 파일 수신

여러 계정에서 CloudTrail 로그 파일 수신

Nimble Studio 작업은 CloudTrail에서 로깅되고 Amazon Nimble Studio API 참조에 기록됩니다. 예를 들어, CreateStudio, GetStudio, DeleteStudio 작업 호출은 CloudTrail 로그 파일에 항목을 생성합니다.

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

- 요청이 루트 또는 AWS Identity and Access Management (IAM) 사용자 자격 증명으로 이루어졌는지 여부입니다.
- 역할 또는 페더레이션 사용자에 대한 임시 보안 인증을 사용하여 요청이 생성되었는지 여부.
- 다른 서비스에서 요청했는지.

자세한 내용은 CloudTrail userIdentity 요소를 참조하세요.

Nimble Studio 로그 파일 항목 이해

추적이란 지정한 Amazon S3 버킷에 이벤트를 로그 파일로 입력할 수 있게 하는 구성입니다. CloudTrail 로그 파일에는 하나 이상의 로그 항목이 포함될 수 있습니다. 이벤트는 모든 소스로부터의 단일 요청을 나타내며 요청 작업, 작업 날짜와 시간, 요청 파라미터 등에 대한 정보가 들어 있습니다.

CloudTrail 로그 파일은 퍼블릭 API 직접 호출에 대한 순서가 지정된 스택 추적이 아니므로 특정 순서로 표시되지 않습니다.

이 JSON 예제는 세 가지 작업을 보여 줍니다.

- ACTION_1: CreateStudio
- ACTION_2: GetStudio
- ACTION_3: DeleteStudio


```
{
    "eventVersion": "0",
    "userIdentity": {
        "type": "AssumedRole",
        "principalId": "EXAMPLE-PrincipalID:EXAMPLE-Session",
        "arn": "arn:aws:sts::111122223333:assumed-role/EXAMPLE-UserName/EXAMPLE-
Session",
        "accountId": "111122223333",
        "accessKeyId": "EXAMPLE-accessKeyId",
        "sessionContext": {
            "sessionIssuer": {
                "type": "Role",
                "principalId": "EXAMPLE-PrincipalID",
                "arn": "arn:aws:iam::111122223333:role/EXAMPLE-UserName",
                "accountId": "111122223333",
                "userName": "EXAMPLE-UserName"
            },
            "webIdFederationData": {},
            "attributes": {
                "mfaAuthenticated": "false",
                "creationDate": "2021-03-08T23:25:49Z"
            }
        }
    },
    "eventTime": "2021-03-08T23:25:49Z",
    "eventSource": "nimble.amazonaws.com",
    "eventName": "CreateStudio",
    "awsRegion": "us-west-2",
    "sourceIPAddress": "192.0.2.0",
    "userAgent": "EXAMPLE-userAgent",
    "requestParameters": {
        "displayName": "Studio Name",
        "studioName": "EXAMPLE-studioName",
```

```
        "userRoleArn": "arn:aws:iam::111122223333:role/EXAMPLE-ServiceRole-User",
        "adminRoleArn": "arn:aws:iam::111122223333:role/EXAMPLE-ServiceRole-Admin"
    },
    "responseElements": {},
    "requestID": "EXAMPLE-requestID",
    "eventID": "EXAMPLE-eventID",
    "readOnly": false,
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "eventCategory": "Management",
    "recipientAccountId": "111122223333"
},
{
    "eventVersion": "0",
    "userIdentity": {
        "type": "AssumedRole",
        "principalId": "EXAMPLE-PrincipalID:EXAMPLE-Session",
        "arn": "arn:aws:sts::111122223333:assumed-role/EXAMPLE-UserName/EXAMPLE-
Session",
        "accountId": "111122223333",
        "accessKeyId": "EXAMPLE-accessKeyId",
        "sessionContext": {
            "sessionIssuer": {
                "type": "Role",
                "principalId": "EXAMPLE-PrincipalID",
                "arn": "arn:aws:iam::111122223333:role/EXAMPLE-UserName",
                "accountId": "111122223333",
                "userName": "EXAMPLE-UserName"
            },
            "webIdFederationData": {},
            "attributes": {
                "mfaAuthenticated": "false",
                "creationDate": "2021-03-08T23:44:25Z"
            }
        }
    },
    "eventTime": "2021-03-08T23:44:25Z",
    "eventSource": "nimble.amazonaws.com",
    "eventName": "GetStudio",
    "awsRegion": "us-west-2",
    "sourceIPAddress": "192.0.2.0",
    "userAgent": "EXAMPLE-userAgent",
    "requestParameters": {
        "studioId": "us-west-2-EXAMPLE-studioId"
```

```
    },
    "responseElements": null,
    "requestID": "EXAMPLE-requestID",
    "eventID": "EXAMPLE-eventID",
    "readOnly": true,
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "eventCategory": "Management",
    "recipientAccountId": "111122223333"
},
{
    "eventVersion": "0",
    "userIdentity": {
        "type": "AssumedRole",
        "principalId": "EXAMPLE-PrincipalID:EXAMPLE-Session",
        "arn": "arn:aws:sts::111122223333:assumed-role/EXAMPLE-UserName/EXAMPLE-
Session",
        "accountId": "111122223333",
        "accessKeyId": "EXAMPLE-accessKeyId",
        "sessionContext": {
            "sessionIssuer": {
                "type": "Role",
                "principalId": "EXAMPLE-PrincipalID",
                "arn": "arn:aws:iam::111122223333:role/EXAMPLE-UserName",
                "accountId": "111122223333",
                "userName": "EXAMPLE-UserName"
            },
            "webIdFederationData": {},
            "attributes": {
                "mfaAuthenticated": "false",
                "creationDate": "2021-03-08T23:45:14Z"
            }
        }
    },
    "eventTime": "2021-03-08T23:44:14Z",
    "eventSource": "nimble.amazonaws.com",
    "eventName": "DeleteStudio",
    "awsRegion": "us-west-2",
    "sourceIPAddress": "192.0.2.0",
    "userAgent": "EXAMPLE-userAgent",
    "requestParameters": {
        "studioId": "us-west-2-EXAMPLE-studioId"
    },
    "responseElements": {
```

```
        "studio": {
            "adminRoleArn": "arn:aws:iam::111122223333:role/EXAMPLE-ServiceRole-Admin",
            "displayName": "My New Studio Name",
            "homeRegion": "us-west-2",
            "ssoClientId": "EXAMPLE-ssoClientId",
            "state": "DELETING",
            "statusCode": "DELETING_STUDIO",
            "statusMessage": "Deleting studio",
            "studioEncryptionConfiguration": {
                "keyType": "AWS_OWNED_CMK"
            },
            "studioId": "us-west-2-EXAMPLE-studioId",
            "studioName": "EXAMPLE-studioName",
            "studioUrl": "https://sso111122223333.us-
west-2.portal.nimble.amazonaws.com",
            "tags": {},
            "userRoleArn": "arn:aws:iam::111122223333:role/EXAMPLE-ServiceRole-User"
        }
    },
    "requestID": "EXAMPLE-requestID",
    "eventID": "EXAMPLE-eventID",
    "readOnly": false,
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "eventCategory": "Management",
    "recipientAccountId": "111122223333"
}
```


이 예제에서 리전과 IP 주소, “UserroLearn”과 “AdminroLearn” 등 이벤트 식별에 도움이 되는 기타 “requestParameters”가 이벤트에 표시되는 것을 볼 수 있습니다. “creationDate”에서 시간과 날짜를 확인할 수 있으며, 요청이 시작된 소스는 “eventSource”: “nimble.amazonaws.com”으로 표시됩니다.

CloudTrail은 계정을 생성할 AWS 계정 때에서 활성화됩니다. IAM 또는 AWS STS에서 활동이 발생하면 해당 활동이 이벤트 기록의 다른 이벤트와 함께 CloudTrail AWS 서비스 이벤트에 기록됩니다. 에서 최근 이벤트를 보고 검색하고 다운로드할 수 있습니다 AWS 계정.

AWS CloudTrail 는 콘솔 및 API 호출의 호출을 포함하여 IAM 및 AWS Security Token Service (AWS STS)에 대한 모든 API 호출을 이벤트로 캡처합니다. IAM 및에서 CloudTrail을 사용하는 방법에 대한 자세한 내용은 를 사용하여 IAM 및 AWS STS API 호출 로깅 AWS CloudTrail을 AWS STS참조하세요.

CloudTrail에 대한 자세한 내용은 AWS CloudTrail 사용 설명서를 참조하세요.

Amazon에서 제공하는 기타 모니터링 서비스에 대한 자세한 내용은 Amazon CloudWatch 사용 설명서를 참조하세요.

Amazon Nimble Studio 규정 준수 검증

Amazon Nimble Studio는 공동 책임 모델을 따르며, 규정 준수는 AWS 와 고객 간에 공유됩니다.

AWS 서비스 가 특정 규정 준수 프로그램의 범위 내에 있는지 알아보려면 규정 준수 AWS 서비스 프로그램 범위규정 준수 섹션을 참조하고 관심 있는 규정 준수 프로그램을 선택합니다. 일반 정보는 AWS 규정 준수 프로그램.

를 사용하여 타사 감사 보고서를 다운로드할 수 있습니다 AWS Artifact. 자세한 내용은 Downloading Reports inDownloading AWS Artifact 참조하세요.

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

- 보안 및 규정 준수 빠른 시작 안내서 -이 배포 안내서에서는 아키텍처 고려 사항에 대해 설명하고 보안 및 규정 준수에 중점을 둔에 기준 환경을 배포 AWS 하기 위한 단계를 제공합니다.
- Amazon Web Services의 HIPAA 보안 및 규정 준수를 위한 설계 -이 백서에서는 기업이 AWS 를 사용하여 HIPAA 적격 애플리케이션을 생성하는 방법을 설명합니다.

> **Note**
>
> 모든가 HIPAA에 적합한 AWS 서비스 것은 아닙니다. 자세한 내용은 HIPAA 적격 서비스 참조를 참조하세요.

- AWS 규정 준수 리소스 -이 워크북 및 가이드 모음은 업계 및 위치에 적용될 수 있습니다.
- AWS 고객 규정 준수 가이드 - 규정 준수의 관점에서 공동 책임 모델을 이해합니다. 이 가이드에는 여러 프레임워크(미국 국립표준기술연구소(NIST), 결제 카드 산업 보안 표준 위원회(PCI), 국제표준화기구(ISO) 포함)의 보안 제어에 대한 지침을 보호하고 AWS 서비스 매핑하는 모범 사례가 요약되어 있습니다.
- AWS Config 개발자 안내서의 규칙을 사용하여 리소스 평가 -이 AWS Config 서비스는 리소스 구성이 내부 관행, 업계 지침 및 규정을 얼마나 잘 준수하는지 평가합니다.
- AWS Security Hub - 이를 AWS 서비스 통해 내 보안 상태를 포괄적으로 볼 수 있습니다 AWS. Security Hub는 보안 컨트롤을 사용하여 AWS 리소스를 평가하고 보안 업계 표준 및 모범 사례에 대한 규정 준수를 확인합니다. 지원되는 서비스 및 제어 목록은 Security Hub 제어 참조를 참조하세요.

- Amazon GuardDuty - 의심스러운 악의적인 활동이 있는지 환경을 모니터링하여 사용자, AWS 계정 워크로드, 컨테이너 및 데이터에 대한 잠재적 위협을 AWS 서비스 탐지합니다. GuardDuty는 특정 규정 준수 프레임워크에서 요구하는 침입 탐지 요구 사항을 충족하여 PCI DSS와 같은 다양한 규정 준수 요구 사항을 따르는 데 도움을 줄 수 있습니다.
- AWS Audit Manager - 이를 AWS 서비스 통해 AWS 사용량을 지속적으로 감사하여 위험과 규정 및 업계 표준 준수를 관리하는 방법을 간소화할 수 있습니다.

Amazon Nimble Studio의 인프라 보안

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

AWS 게시된 API 호출을 사용하여 네트워크를 통해 Nimble Studio에 액세스합니다. 고객은 다음을 지원해야 합니다.

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

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

Nimble Studio의 보안 모범 사례

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

모니터링

모니터링은 Nimble Studio 및 AWS 솔루션의 안정성, 가용성 및 성능을 유지하는 데 중요한 부분입니다. 이벤트 모니터링 및 응답에 대한 자세한 내용은 Nimble Studio의 보안 이벤트 로깅 및 모니터링 단원을 참조하세요.

데이터 보호

데이터 보호를 위해 자격 AWS 계정 증명을 보호하고 AWS Identity and Access Management (IAM)을 사용하여 개별 계정을 설정하는 것이 좋습니다. 이렇게 하면 개별 사용자에게 자신의 직무를 충실히 이행하는 데 필요한 권한만 부여됩니다. 또한 다음과 같은 방법으로 데이터를 보호하는 것이 좋습니다.

- 각 계정에 다중 인증(MFA)을 사용하세요.
- SSL/TLS를 사용하여 AWS 리소스와 통신합니다. TLS 1.2 이상을 권장합니다.
- 를 사용하여 API 및 사용자 활동 로깅을 설정합니다 AWS CloudTrail.
- AWS 암호화 솔루션과 내의 모든 기본 보안 제어를 사용합니다 AWS 서비스.
- Amazon S3에 저장된 개인 데이터를 검색하고 보호하는 데 도움이 되는 Amazon Macie와 같은 고급 관리형 보안 서비스를 사용합니다.
- 명령줄 인터페이스 또는 API를 통해 AWS 에 액세스할 때 FIPS 140-2 검증된 암호화 모듈이 필요한 경우 FIPS 엔드포인트를 사용합니다. 사용 가능한 FIPS 엔드포인트에 대한 자세한 내용은 Federal Information Processing Standard(FIPS) 140-2 섹션을 참조하세요.

명칭 필드와 같은 자유 형식 필드에 고객 계정 번호와 같은 중요 식별 정보를 절대 입력하지 마세요. 여기에는 Amazon Nimble Studio 또는 기타에서 콘솔, API AWS CLI또는 AWS SDKs를 AWS 서비스 사용하여 작업하는 경우가 포함됩니다. Amazon Nimble Studio 또는 기타 서비스에 입력하는 데이터는 캡처되어 진단 로그에 포함될 수 있습니다. 외부 서버에 URL을 제공할 때 해당 서버에 대한 요청을 검증하기 위해 자격 증명 정보를 URL에 포함하지 마십시오.

권한

사용자, IAM 역할을 사용하고 사용자에게 최소 권한을 부여하여 AWS 리소스에 대한 액세스를 관리합니다. AWS 액세스 자격 증명을 생성, 배포, 교체 및 취소하기 위한 자격 증명 관리 정책 및 절차를 수립합니다. 자세한 내용은 IAM 사용 설명서의 IAM 모범 사례 섹션을 참조하십시오.

Nimble Studio 지원

이 섹션에는 서비스 및 관련 애플리케이션을 배포하거나 사용하는 동안 도움을 받는 방법 등 Nimble Studio의 다양한 지원 옵션이 나와 있습니다.

내용

Nimble Studio 포럼

Nimble Studio에 대해 궁금한 점이 있다면 Nimble Studio 포럼을 방문할 수 있습니다. 여기에서 커뮤니티 및 AWS 포럼 중재자로부터 Nimble Studio 기능, 기술 문제 및 문제 해결 도움말에 대한 답변을 얻을 수 있습니다.

애플리케이션 지원

Nimble Studio는 다음 애플리케이션에 대한 추가 설명서를 제공합니다.

AWSThinkboxDeadline

렌더 팜에 대한 도움이 필요하거나 Deadline 작동 방식을 알아보려면 AWSThinkboxDeadline 설명서를 참조하세요.

Nimble Studio File Transfer

File Transfer의 작동 방식을 알아보려면 Nimble Studio File Transfer 사용 설명서를 참조하세요.

지원 센터

지원 Center는 지원 사례를 생성하고 관리하는 허브입니다. 결제 및 기술 솔루션, 지식 센터, 지식 센터 비디오, AWS 문서, 교육 및 인증을 비롯한 다양한 리소스에 대한 액세스를 제공합니다.

지원 계획

지원 계획을 통해 성능을 최적화하고, 보안을 유지하고, 가동 중지 시간을 방지하고, 비용을 제어할 수 있습니다. 지원 플랜에 대한 자세한 내용은 지원 플랜 비교를 참조하세요.

AWS 가 사용자를 지원하는 방법에 대한 자세한 내용은 문의하기 페이지를 참조하세요.

문서 이력

- API 버전: 최신
- 최종 설명서 업데이트: 2024년 10월 2일

다음 표에서는 Nimble Studio 관리자 안내서의 각 릴리스에서 변경된 중요 사항에 대해 설명합니다.

변경 사항	설명	
지원 종료 알림	지원 종료 공지: 2024 AWS 년 10월 22일에는 Amazon Nimble Studio에 대한 지원을 중단할 예정입니다. 2024년 10월 22일 이후에는 Nimble Studio 콘솔 또는 Nimble Studio 리소스에 더 이상 액세스할 수 없습니다.	2024년 10월 2일
AWS 관리형 정책 업데이트	최신 버전의 AWS IAM Identity Center 서비스를 사용하도록 `AmazonNimbleStudio-StudioUser` 및 `AmazonNimbleStudio-StudioAdmin` 정책을 업데이트했습니다.	2023년 9월 22일
새로운 서비스 및 가이드	이것은 Amazon Nimble Studio와 Amazon Nimble Studio 관리자 안내서의 첫 번째 릴리스입니다.	2023년 6월 19일

AWS 용어집

최신 AWS 용어는 AWS 용어집 참조의 AWS 용어집을 참조하세요.