aws

사용자 가이드

Migration Hub Strategy Recommendations

Migration Hub Strategy Recommendations: 사용자 가이드

Table of Contents

Migration Hub Strategy Recommendations란?

Migration Hub Strategy Recommendations는 애플리케이션의 실행 가능한 변환 경로에 대한 마이그레이션 및 현대화 전략 권장 사항을 제공하여 마이그레이션 및 현대화 이니셔티브를 계획하는 데 도움이 됩니다.

Strategy Recommendations는 서버 인벤토리, 런타임 환경, Microsoft IIS, Java Tomcat 및 Jboss 애플리케이션용 애플리케이션 바이너리를 분석하여 안티 패턴 보고서를 생성할 수 있습니다. 또한 Strategy Recommendations가 모든 애플리케이션의 소스 코드 및 데이터베이스 분석을 수행할 수 있도록 소스 코드를 구성할 수 있습니다. Strategy Recommendations는 이 분석을 비즈니스 목표 및 제공한 애플리케이션 및 데이터베이스의 변환 기본 설정과 비교하여 다음을 권장합니다.

- 각 애플리케이션을 위한 가장 효과적인 마이그레이션 전략
- 사용할 수 있는 마이그레이션 및 현대화 도구 또는 서비스
- 특정 옵션에 대해 해결해야 할 애플리케이션 비호환성 및 안티 패턴

Migration Hub Strategy Recommendations는 관련 배포 대상, 도구 및 프로그램을 사용하여 리호스팅, 리플랫포밍 및 리팩터링을 위한 마이그레이션 및 현대화 전략을 권장합니다. 리호스팅, 리플랫포밍, 리팩터링에 대한 자세한 내용은 AWS Prescriptive Guidance 용어집의 Migration terms - 7 Rs를 참조하세요.

Strategy Recommendations는 AWS Application Migration Service(AWS MGN)를 사용하여 Amazon Elastic Compute Cloud(Amazon EC2)에서 리호스팅하는 등 간단한 옵션을 추천할 수 있습니다. 보다 최적화된 권장 사항에는 AWS App2Container를 사용하여 컨테이너로 리플랫포밍하거나 .NET Core 및 PostgreSQL과 같은 오픈 소스 기술로 리팩터링하는 것이 포함될 수 있습니다.

Strategy Recommendations를 처음 사용하시나요?

Strategy Recommendations를 처음 사용하는 경우 먼저 다음 섹션을 읽을 것을 권장합니다.

- Strategy Recommendations 개요
- Strategy Recommendations 설정
- Strategy Recommendations 시작하기

Strategy Recommendations 개요

AWS Migration Hub 콘솔에서 Migration Hub Strategy Recommendations를 사용하여 서버 및 애플리케이션 포트폴리오에 대한 평가를 시작할 수 있습니다. 콘솔을 사용하여 평가를 설정하고 수행할 수 있습니다. 평가 후에는 콘솔을 사용하여 권장 변환 도구와 함께 각 서버 및 애플리케이션에 대한 평가 데이터를 볼 수 있습니다.

리팩터링 권장 사항 및 비호환성 목록을 받으려면 Strategy Recommendations를 사용하여 애플리케이션 소스 코드와 데이터베이스를 평가할 수 있습니다.

Microsoft Excel 파일로 권장 사항 데이터를 다운로드할 수도 있습니다.

관련 서비스

- AWS Migration Hub - AWS Migration Hub 콘솔을 사용하여 Migration Hub Strategy Recommendations 콘솔에 액세스합니다. 데이터를 수집하는 서버에 대한 정보도 표시합니다.
- AWS Application Discovery Service - Strategy Recommendations를 사용하기 전에 Application Discovery Service를 사용하여 AWS Migration Hub 콘솔에서 서버 및 애플리케이션에 대한 데이터를 수집합니다.
- AWS Application Migration Service - AWS Application Migration Service는 로의 lift-and-shift 마이그레이션에 권장되는 기본 마이그레이션 서비스입니다 AWS.
- AWS Database Migration Service - 온프레미스, Amazon Relational Database Service(RDS) DB 인스턴스 또는 Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스의 데이터베이스에서 서비스의 데이터베이스로 데이터를 마이그레이션하는 데 사용할 수 있는 AWS Database Migration Service 웹 서비스입니다 AWS .
- AWS App2Container – AWS App2Container(A2C)는 .NET 및 Java 애플리케이션을 컨테이너화된 애플리케이션으로 현대화하기 위한 명령줄 도구입니다.
- Porting Assistant for .NET – NET 소스 코드 분석에 사용합니다. Porting Assistant for .NET은 Microsoft .NET Framework 애플리케이션을 .NET Core로 이식하는 데 필요한 수동 작업을 줄여주는 호환성 스캐너입니다. Porting Assistant for .NET은 .NET 애플리케이션 소스 코드를 평가하고 호환되지 않는 API와 서드 파티 패키지를 식별합니다.
- Windows Server용 End-of-Support 마이그레이션 프로그램 End-of-Support 마이그레이션 프로그램(EMP)에는 리팩터링 AWS없이 Windows Server 2003, 2008 및 2008 R2에서 지원되는 최신 버전으로 레거시 애플리케이션을 마이그레이션하는 도구가 포함되어 있습니다.

- AWS Schema Conversion Tool - AWS Schema Conversion Tool(AWS SCT)를 사용하여 기존 데이터베이스 스키마를 한 데이터베이스 엔진에서 다른 데이터베이스 엔진으로 변환할 수 있습니다.
- Windows Web Application Migration Assistant – 용 Windows Web Application Migration Assistant AWS Elastic Beanstalk 는 ASP.NET 및 ASP.NET Core 애플리케이션을 온프레미스 IIS Windows 서버에서 Elastic Beanstalk로 마이그레이션하는 대화형 PowerShell 유틸리티입니다.
- Babelfish for Aurora PostgreSQL – Babelfish for Aurora PostgreSQL은 Aurora가 Microsoft SQL 서버용으로 작성된 애플리케이션의 명령을 이해할 수 있게 하는 Amazon Aurora PostgreSQL 호환 버전의 새로운 기능입니다.

Strategy Recommendations 설정

Migration Hub Strategy Recommendations를 처음 사용한다면 먼저 다음 작업을 완료해야 합니다.

주제

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 전화 또는 텍스트 메시지를 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 사용 AWS IAM Identity Center 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.

Strategy Recommendations 사용자 및 역할

Strategy Recommendations에 대한 두 가지 역할을 생성하는 것이 좋습니다.

- 콘솔에 액세스하려면 `AWSMigrationHubFullAccess` 및 `AWSMigrationHubStrategyConsoleFullAccess` 관리형 정책이 연결된 역할을 생성합니다.
- Strategy Recommendations 애플리케이션 데이터 수집기에 액세스하려면 `AWSMigrationHubStrategyCollector` 관리형 정책이 연결된 역할을 생성합니다.

IAM 관리형 정책은 사용자가 서비스에 액세스할 수 있는 수준을 정의합니다. `AWSMigrationHubFullAccess` 관리형 AWS Migration Hub 정책은 Migration Hub 콘솔에 대한 액세스 권한을 부여합니다. 자세한 내용은 Migration Hub 역할 및 정책을 참조하세요. `AWSMigrationHubStrategyConsoleFullAccess` 및 `AWSMigrationHubStrategyCollector` 관리형 정책에 대한 자세한 내용은 AWS Migration Hub Strategy Recommendations에 대한 관리형 정책 섹션을 참조하세요.

액세스 권한을 제공하려면 사용자, 그룹 또는 역할에 권한을 추가하세요:

- 의 사용자 및 그룹 AWS IAM Identity Center:

  권한 세트를 생성합니다. AWS IAM Identity Center 사용 설명서의 권한 세트 생성의 지침을 따릅니다.
- 보안 인증 공급자를 통해 IAM에서 관리되는 사용자:

  ID 페더레이션을 위한 역할을 생성합니다. IAM 사용 설명서의 Create a role for a third-party identity provider (federation)의 지침을 따릅니다.
- IAM 사용자:
  - 사용자가 맡을 수 있는 역할을 생성합니다. IAM 사용 설명서에서 Create a role for an IAM user의 지침을 따릅니다.
  - (권장되지 않음)정책을 사용자에게 직접 연결하거나 사용자를 사용자 그룹에 추가합니다. IAM 사용 설명서에서 사용자(콘솔)에 권한 추가의 지침을 따르세요.

Strategy Recommendations 시작하기

이 섹션에서는 Migration Hub Strategy Recommendations를 시작하는 방법을 설명합니다.

주제

Strategy Recommendations의 사전 조건

다음은 Migration Hub Strategy Recommendations 사용을 위한 사전 조건입니다.

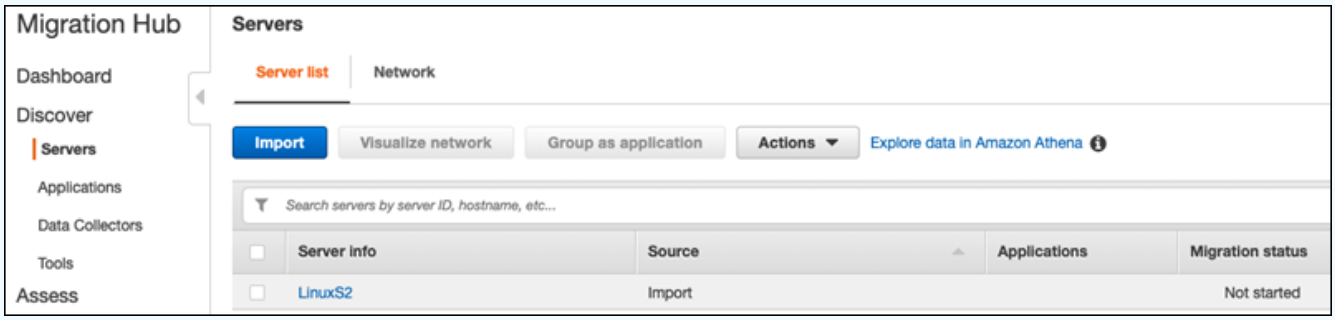
- 하나 이상의 AWS 계정이 있어야 하며 사용자는 이러한 계정에 대해를 설정해야 합니다. 자세한 내용은 Strategy Recommendations 설정 단원을 참조하십시오.
- Strategy Recommendations 애플리케이션 데이터 수집기 클라이언트가 서버에서 원격으로 데이터를 수집할 수 있어야 합니다. 이를 위해서는 모든 Windows 서버에 사용할 수 있는 보안 인증 집합과 모든 Linux 서버에서 작동하는 보안 인증 집합을 사용해야 합니다. 보안 인증에 서버에서 디렉터리를 생성하고 삭제할 수 있는 권한이 있어야 합니다.
- vCenter에 배포된 수집기 버전은 VMware vCenter Server V6.0, V6.5, 6.7 또는 7.0을 지원합니다.

  수집기 AMI를 사용하여 Amazon EC2 인스턴스에 수집기를 배포할 수도 있습니다.
- 운영 체제(OS) 환경이 지원되는지 확인합니다.
  - Linux
    - Amazon Linux 2012.03, 2015.03
    - Amazon Linux 2(2018년 9월 25일 업데이트 이후)
    - Ubuntu 12.04, 14.04, 16.04, 18.04, 20.04
    - Red Hat Enterprise Linux 5.11, 6.10, 7.3, 7.7, 8.1
    - CentOS 5.11, 6.9, 7.3
    - SUSE 11 SP4, 12 SP5

  - Windows
    - Windows Server 2008 R1 SP2, 2008 R2 SP1
    - Windows Server 2012 R1, 2012 R2
    - Windows Server 2016
    - Windows Server 2019
- 소스 코드 분석을 위해 GitHub 및 GitHub Enterprise 리포지토리에는 Strategy Recommendations 수집기 클라이언트와 공유할 수 있는 리포지토리 범위의 개인 액세스 토큰이 있어야 합니다. 리포지토리 범위로 개인용 액세스 토큰을 생성하는 방법에 대한 자세한 내용은 GitHub Docs의 Creating a personal access token을 참조하세요.

  Porting Assistant for .NET 권장 사항에 대해 .NET 리포지토리를 분석하려면 Porting Assistant for .NET 이식 평가 도구로 설정된 Windows 시스템을 제공해야 합니다. 자세한 내용은 Porting Assistant for .NET 설명서의 Getting started with Porting Assistant for .NET을 참조하세요.
- 데이터베이스 분석을 위한 Strategy Recommendations를 활성화하려면 AWS Secrets Manager에 보안 인증 정보를 입력해야 합니다. 자세한 내용은 Strategy Recommendations 데이터베이스 분석 단원을 참조하십시오.
- Strategy Recommendations AWS Application Discovery Service 를 사용하기 전에를 사용하여 AWS Migration Hub 콘솔에서 서버 및 애플리케이션에 대한 데이터를 수집해야 합니다. 다음 방법 중 하나를 사용하여 데이터를 수집할 수 있습니다.
  - Migration Hub 가져오기 - Migration Hub 가져오기를 사용하면 온프레미스 서버 및 애플리케이션에 대한 정보를 Migration Hub로 가져올 수 있습니다. 자세한 내용은 Application Discovery Service 사용 설명서의 Migration Hub Import를 참조하세요.
  - AWS Application Discovery Service Agentless Collector – Agentless Collector는 VMware 가상 머신에 대한 정보를 수집하는 VMware 어플라이언스입니다. 자세한 내용은 Application Discovery Service 사용 설명서의 Agentless Collector를 참조하세요.
  - AWS Application Discovery Agent - Discovery Agent는 시스템 정보 및 시스템 간 네트워크 연결 세부 정보를 캡처하기 위해 온프레미스 서버 및 VMs에 설치하는 AWS 소프트웨어입니다. 자세한 내용은 Application Discovery Service 사용 설명서의 AWS Application Discovery Agent를 참조하세요.
- Strategy Recommendations 데이터 수집기 - 서버가 VMware vCenter에서 호스팅되고 사용자가 액세스 권한을 제공하는 경우 Strategy Recommendations가 서버 인벤토리를 자동으로 가져올 수 있습니다. Strategy Recommendations 콘솔은 수집된 정보를 사용하여 평가를 지원합니다.

> **Note**
>
> Migration Hub 가져오기가 성공적으로 완료되었는지 확인하려면 Migration Hub 콘솔 탐색 창의 검색에서 서버를 선택합니다. 가져온 서버가 모두 나열되어야 합니다.



1단계: Strategy Recommendations 수집기 다운로드

Migration Hub Strategy Recommendations 애플리케이션 데이터 수집기는 온프레미스 VMware 환경에 설치할 수 있는 가상 어플라이언스입니다. Strategy Recommendations 애플리케이션 데이터 수집기는 Amazon Machine Image(AMI)로도 사용할 수 있습니다. 수집기의 AMI 버전을 사용하여 AWS 애플리케이션을 평가하거나 다른 이유로 수집기를 다운로드할 필요가 없습니다. 이 섹션을 건너뛰고 Amazon EC2 인스턴스에 Strategy Recommendations 수집기 배포로 이동할 수 있습니다.

이 섹션에서는 수집기를 VMware 환경에서 가상 머신으로 배포하는 데 사용하는 수집기 OVA(Open Virtualization Archive) 파일을 다운로드하는 방법을 설명합니다.

수집기 OVA 파일 다운로드

1. 에서 생성한 AWS 계정을 사용하여에 Strategy Recommendations 설정로그인 AWS Management Console 하고 https://console.aws.amazon.com/migrationhub/ Migration Hub 콘솔을 엽니다.
2. Migration Hub 콘솔 탐색 창에서 전략을 선택합니다.
3. Migration Hub Strategy Recommendations 페이지에서 데이터 수집기 다운로드를 선택합니다.
4. 애플리케이션 데이터를 가져오려는 경우 가져오기 템플릿 다운로드를 선택할 수도 있습니다. 데이터 가져오기에 대한 자세한 내용은 Strategy Recommendations로 데이터 가져오기 섹션을 참조하세요.
5. 권장 사항 가져오기 버튼을 클릭하고 동의를 선택하여 Migration Hub가 계정에서 서비스 연결 역할(SLR)을 생성할 수 있도록 합니다. Strategy Recommendations를 처음 설정할 때 SLR을 생성해야 합니다. 자세한 내용은 Strategy Recommendations에 대한 서비스 연결 역할 사용 단원을 참조하십시오.

2단계: Strategy Recommendations 수집기 배포

이 섹션에서는 Strategy Recommendations 애플리케이션 데이터 수집기를 배포하는 방법을 설명합니다. 애플리케이션 데이터 수집기는 서버에서 실행 중인 애플리케이션을 식별하고, 소스 코드 분석을 수행하고, 데이터베이스를 분석하는 에이전트 없는 데이터 수집기입니다.

수집기 배포 방법에는 두 가지가 있습니다.

- VMware vCenter Server에 가상 머신으로 배포합니다. 자세한 내용은 vCenter에 Strategy Recommendations 수집기 배포 단원을 참조하십시오.
- 평가하려는 AWS 애플리케이션이 있는 경우 Strategy Recommendations 수집기 Amazon Machine Image(AMI)를 사용할 수 있습니다. 자세한 내용은 Amazon EC2 인스턴스에 Strategy Recommendations 수집기 배포 단원을 참조하십시오.

vCenter에 Strategy Recommendations 수집기 배포

Migration Hub Strategy Recommendations 애플리케이션 데이터 수집기는 온프레미스 VMware 환경에 설치할 수 있는 가상 어플라이언스입니다. 이 섹션에서는 VMware 환경에서 수집기 OVA(Open Virtualization Archive) 파일을 가상 머신으로 배포하는 방법을 설명합니다.

다음 절차에서는 VMware vCenter Server 환경에서 Strategy Recommendations 수집기를 배포하는 방법을 설명합니다.

vCenter에 수집기 배포

1. vCenter에 VMware 관리자로 로그인합니다.
2. 1단계에서 다운로드한 OVA 파일을 배포합니다. OVA 파일에는 Strategy Recommendations API에 액세스하는 데 사용할 수 있는 수집기와 CLI가 포함되어 있습니다.

   다음 링크에서 OVA 파일을 다운로드할 수도 있습니다.

   https://application-data-collector-release.s3.us-west-2.amazonaws.com/ova/latest/AWSMHubApplicationDataCollector.ova

VM의 권장 사양은 다음과 같습니다.

Strategy Recommendations 수집기 VM 사양

- RAM - 최소 8GB

- CPU - 최소 4개

> **Note**
>
> 새로운 기능과 버그 수정이 모두 포함된 최신 버전의 수집기를 사용하려면 수집기 OVA 파일을 배포한 후 수집기를 업그레이드합니다. 업그레이드 방법에 관한 지침은 Strategy Recommendations 수집기 업그레이드 섹션을 참조하세요.

Amazon EC2 인스턴스에 Strategy Recommendations 수집기 배포

평가하려는 AWS 애플리케이션이 있는 경우 Strategy Recommendations 애플리케이션 데이터 수집기 Amazon Machine Image(AMI)를 사용할 수 있습니다.

다음 절차는 수집기 AMI에서 Amazon EC2 인스턴스를 시작하는 방법을 설명합니다.

수집기 Amazon EC2 인스턴스 배포

1. https://console.aws.amazon.com/ec2/에서 Amazon EC2 콘솔을 엽니다.
2. 화면 상단의 탐색 모음에는 현재 리전이 표시됩니다(예: 미국 동부(오하이오)). Strategy Recommendations에서 사용하는 리전 중에서 필요에 맞는 리전을 선택합니다. 이러한 리전 목록은 AWS 일반 참조의 Strategy Recommendations endpoints를 참조하세요.
3. 탐색 창의 이미지 아래에서 AMI를 선택합니다.
4. 내 소유 드롭다운에서 공개 이미지를 선택합니다.
5. 검색 창을 선택하고 메뉴에서 AMI 이름을 선택합니다.
6. 이름으로 AWSMHubApplicationDataCollector을 입력합니다.
7. 계정 소유자가 703163444405이면 AMI의 소스가 안전한 것입니다.
8. 이 AMI에서 인스턴스를 시작하려면 원하는 인스턴스를 선택한 다음 시작을 선택합니다. 콘솔을 사용하여 인스턴스를 시작하는 방법에 대한 자세한 내용은 Amazon EC2 사용 설명서의 AMI에서 인스턴스 시작을 참조하세요.

   Amazon EC2 인스턴스의 권장 사양은 다음과 같습니다.

   Strategy Recommendations 수집기 Amazon EC2 인스턴스 사양

   - RAM - 최소 8GB
   - CPU - 최소 4개

Strategy Recommendations AMI에는 Strategy Recommendations API에 액세스하는 데 사용할 수 있는 수집기와 CLI가 포함되어 있습니다.

> **Note**
>
> 새로운 기능과 버그 수정이 모두 포함된 최신 버전의 수집기를 사용하고 있는지 확인하려면 Strategy Recommendations 수집기를 Amazon EC2 인스턴스로 배포한 후 수집기를 업그레이드하세요. 업그레이드 방법에 관한 지침은 Strategy Recommendations 수집기 업그레이드 섹션을 참조하세요.

3단계: Strategy Recommendations 수집기에 로그인

이 섹션에서는 배포된 Migration Hub Strategy Recommendations 애플리케이션 데이터 수집기에 로그인하는 방법을 설명합니다. 수집기에 로그인하는 방법은 수집기를 배포한 방식에 따라 달라집니다.

- vCenter 기반 환경에 배포된 수집기에 로그인합니다.
- Amazon EC2 인스턴스로 배포된 수집기에 로그인

vCenter 기반 환경에 배포된 수집기에 로그인합니다.

vCenter 기반 환경에 배포된 Strategy Recommendations 수집기에 로그인하려면

1. 다음 명령을 사용하여 SSH 클라이언트로 수집기에 연결합니다.

   ```
   ssh ec2-user@CollectorIPAddress
   ```

2. 암호를 입력하라는 메시지가 나타나면 기본 암호 aq1@WSde3을 입력합니다. 처음 로그인할 때 암호를 변경해야 합니다.

Amazon EC2 인스턴스로 배포된 수집기에 로그인

Amazon EC2 인스턴스로 배포된 Strategy Recommendations 수집기에 로그인하려면

- 다음 명령을 사용하여 SSH 클라이언트로 수집기에 연결합니다.

  ```
  ssh -i "Keyname.pem" ec2-user@CollectorIPAddress
  ```

Keyname.pem은 수집기 AMI에서 Amazon EC2 인스턴스를 시작할 때 생성된 프라이빗 키입니다.

4단계: Strategy Recommendations 수집기 설정

이 섹션에서는 명령줄 `collector setup` 명령을 사용하여 Migration Hub Strategy Recommendations 애플리케이션 데이터 수집기를 구성하는 방법을 설명합니다. 이러한 구성은 로컬에 저장됩니다.

`collector setup` 명령을 사용하려면 먼저 다음 `docker exec` 명령을 사용하여 수집기 Docker 컨테이너에 bash 쉘 세션을 생성해야 합니다.

```
docker exec -it application-data-collector bash
```

`collector setup` 명령은 다음 명령을 모두 연속으로 실행하지만 각 명령을 개별적으로 실행할 수도 있습니다.

- `collector setup --aws-configurations` - AWS 구성을 설정합니다.
- `collector setup --vcenter-configurations` - vCenter 구성을 설정합니다.

> **Note**
>
> vCenter 구성 설정은 수집기가 vCenter에서 호스팅되는 경우에만 가능합니다. 그러나 명령 `collector setup --vcenter-configurations`를 사용하여 vCenter 구성 설정을 강제로 적용할 수 있습니다.

- `collector setup --remote-server-configurations` - 원격 서버 구성을 설정합니다.
- `collector setup --version-control-configurations` - 버전 관리 구성을 설정합니다.

동시에 모든 수집기 구성 설정

1. 다음 명령을 입력합니다.

   ```
   collector setup
   ```

2. 에 설명된 대로 AWS 구성에 대한 정보를 입력합니다AWS 구성 설정.
3. vCenter 구성 설정에 설명된 대로 vCenter 구성 정보를 입력합니다.
4. 원격 서버 구성 설정에 설명된 대로 원격 서버 구성 정보를 입력합니다.

5. 버전 관리 구성 설정에 설명된 대로 버전 관리 구성 정보를 입력합니다.
6. 데이터 수집을 위해 원격 Windows 및 Linux 서버 준비의 지침에 따라 수집기 데이터를 수집할 수 있도록 Windows 및 Linux 서버를 준비합니다.

AWS 구성 설정

`collector setup` 명령 또는 `collector setup --aws-configurations` 명령을 사용할 때 AWS 구성을 설정하려면

1. Have you setup IAM permissions... 질문에 Y(예)를 입력합니다. Strategy Recommendations 사용자 및 역할의 단계에 따라 `AWSMigrationHubStrategyCollector` 관리형 정책을 사용하여 수집기에 액세스할 사용자를 생성할 때 이러한 권한을 설정합니다.
2. 의 단계에 따라 수집기에 액세스하기 위해 생성한 사용자가 있는 AWS 계정에서 액세스 키와 보안 키를 입력합니다Strategy Recommendations 사용자 및 역할.
3. 리전(예: `us-west-2`)을 입력합니다. Strategy Recommendations에서 사용하는 리전 중에서 필요에 맞는 리전을 선택합니다. 이러한 리전 목록은 AWS 일반 참조의 Strategy Recommendations endpoints를 참조하세요.
4. Upload collector related metrics to migration hub strategy service? 질문에 Y(예)를 입력합니다. 지표 정보는 적절한 지원을 AWS 제공하는 데 도움이 됩니다.
5. Upload collector related logs to migration hub strategy service? 질문에 Y(예)를 입력합니다. 로그의 정보는 적절한 지원을 AWS 제공하는 데 도움이 됩니다.

다음 예에서는 AWS 구성에 대한 예제 항목을 포함하여 표시되는 내용을 보여줍니다.

```
Have you setup IAM permissions in you AWS account as per the user guide? [Y/N]: Y
Choose one of the following options for providing user credentials:
1. Long term AWS credentials
2. Temporary AWS credentials
Enter your options [1-2]: 2
AWS session token:
AWS access key ID [None]:
AWS secret access Key [None]:
AWS region name [us-west-2]:
AWS configurations are saved successfully
Upload collector related metrics to migration hub strategy service? By default
 collector will upload metrics. [Y/N]: Y
```

```
Upload collector related logs to migration hub strategy service? By default collector
 will upload logs. [Y/N]: Y
Application data collector configurations are saved successfully
Start registering application data collector
Application data collector is registered successfully.
```

vCenter 구성 설정

`collector setup` 명령 또는 `collector setup --vcenter-configurations` 명령 사용 시 vCenter 구성 설정

1. VMware vCenter 보안 인증을 사용하여 인증하려는 경우 Would you like to authenticate using VMware vCenter credentials 질문에 Y(예)를 입력합니다.

   > **Note**
   >
   > VMware vCenter 보안 인증을 사용하여 인증하려면 대상 서버에 VMware 도구가 설치되어 있어야 합니다.

   호스트 URL(vCenter IP 주소 또는 URL)을 입력합니다. 그런 다음 VMware vCenter의 사용자 이름과 암호를 입력합니다.
2. Windows 서버를 구성하려는 경우 Do you have Windows machines managed by VMware vCenter 질문에 Y(예)를 입력합니다.

   Windows의 사용자 이름과 암호를 입력합니다.

   > **Note**
   >
   > Windows 원격 서버가 Active Directory 도메인에 속하는 경우 CLI를 사용하여 원격 서버 구성을 제공할 때 사용자 이름을 *domain-name**username*으로 입력해야 합니다. 예를 들어, 도메인 이름이 exampledomain이고 사용자 이름이 Administrator인 경우 CLI에 입력하는 사용자 이름은 exampledomain\Administrator입니다.
3. Linux 서버를 구성하려는 경우 Setup for Linux using VMware vCenter 질문에 Y(예)를 입력합니다.

   Linux의 사용자 이름과 암호를 입력합니다.

4. vCenter 외부 서버에 대한 원격 서버 보안 인증을 설정하려는 경우 Would you like to setup credentials for servers outside vCenter using NTLM for Windows 및 SSH/Cert based for Linux 질문에 Y(예)를 입력합니다.
5. vCenter 외부에서 관리되는 Windows 시스템에 대한 보안 인증이 vCenter Windows 시스템에 대한 보안 인증을 구성할 때 제공된 보안 인증과 동일한 경우 Would you like to use the same Windows credentials used during vCenter setup 질문에 Y(예)를 입력합니다. 그렇지 않으면 N(아니요)을 입력합니다.

   Y(예)로 답하면 다음과 같은 질문이 나타납니다.

   a. Are you okay with collector accepting and locally storing server certificates on your behalf during first interaction with windows servers? 질문에 Y(예)를 입력합니다.
   b. SSH 인증을 구성하려면 Enter your options 질문에 1을 입력합니다.

      SSH 인증을 사용하기로 선택한 경우 생성된 키 보안 인증을 Linux 서버에 복사해야 합니다. 자세한 내용은 Linux 서버에서 키 기반 인증 설정 단원을 참조하십시오.

다음 예에서는 VMware vCenter 구성에 대한 예제 항목을 포함하여 표시되는 내용을 보여줍니다.

```
Your Linux remote server configurations are saved successfully.
collector setup –vcenter-configurations
Start setting up vCenter configurations for remote execution
Note: Authenticating using VMware vCenter credentials requires VMware tools to be
 installed on the target servers
Would you like to authenticate using VMware vCenter credentials? [Y/N]: y

NOTE: Your vSphere user must have Guest Operations privileges enabled.

Host Url for VMware vCenter: domain-name
Username for VMware vCenter: username
Password for VMware vCenter: password
Reenter password for VMware vCenter: password
Successfully stored vCenter credentials...
Do you have Windows machines managed by VMware vCenter? [Y/N]: y

NOTE: For the best experience, we recommend that you create a new Active Directory user
 in the Domain Admins group.

Username for Windows (Domain\User): username
Password for Windows: password
```

```
Reenter password for Windows: password
Successfully stored windows credentials...
You can verify your setup for vCenter windows machines is correct with "collector diag-
check"
Do you have Linux machines managed by VMWare vCenter? [Y/N]: y
Username for Linux: username
Password for Linux: password
Reenter password for Linux: password
Successfully stored linux credentials...
You can verify your setup for vCenter linux machines is correct with "collector diag-
check"
Would you like to setup credentials for servers not managed by vCenter using NTLM for
 windows and SSH/Cert based for Linux? [Y/N]: y
Setting up target server for remote execution:
Would you like to setup credentials for servers not managed by vCenter using NLTM for
 Windows [Y/N]: y
Would you like to use the same Windows credentials used during vCenter setup? [Y/N]: y
Are you okay with collector accepting and locally storing server certificates on your
 behalf during first interaction with windows servers? These certificates will be used
 by collector for secure communication with windows servers [Y/N]: y
Successfully stored windows server credentials...
Please note that all windows server certificates are stored in directory /opt/amazon/
application-data-collector/remote-auth/windows/certs

Please note the IP address of the collector and run the script specified in the user
 documentation on all the windows servers in your inventory
You can verify your setup for remote windows machines is correct with "collector diag-
check"
Would you like to setup credentials for servers not managed by vCenter using SSH/Cert
 based for Linux? [Y/N]: y
Choose one of the following options for remote authentication:
1. SSH based authentication
2. Certificate based authentication
Enter your options [1-2]: 1
Would you like to use the same Linux credentials used during vCenter setup? [Y/N]: y
Generating SSH key on this machine...
Successfully generated SSH key pair

SSH key pair path: /opt/amazon/application-data-collector/remote-auth/linux/keys/
id_rsa_assessment
Please add the public key "id_rsa_assessment.pub" to the "$HOME/.ssh/authorized_keys"
 file in your remote machines.
```

```
You can verify your setup for remote linux machines is correct with "collector diag-
check
```

원격 서버 구성 설정

`collector setup` 명령 또는 `collector setup --remote-server-configurations` 명령 사용 시 원격 서버 구성 설정

1. Windows 서버를 구성하려는 경우 Would you like to setup credentials for servers not managed by vCenter using NLTM for Windows 질문에 Y(예)를 입력합니다.

   WinRM의 사용자 이름과 암호를 입력합니다.

   > **Note**
   >
   > Windows 원격 서버가 Active Directory 도메인에 속하는 경우 CLI를 사용하여 원격 서버 구성을 제공할 때 사용자 이름을 *`domain-name`**`username`*으로 입력해야 합니다. 예를 들어, 도메인 이름이 exampledomain이고 사용자 이름이 Administrator인 경우 CLI에 입력하는 사용자 이름은 exampledomain\Administrator입니다.

   Are you okay with collector accepting and locally storing server certificates on your behalf during first interaction with windows servers? 질문에 Y(예)를 입력합니다. Windows Server 인증서는 디렉터리 `/opt/amazon/application-data-collector/remote-auth/windows/certs`에 저장됩니다.

   생성된 서버 보안 인증을 Windows 서버에 복사해야 합니다. 자세한 내용은 Windows 서버에서 원격 서버 구성 설정 단원을 참조하십시오.
2. Linux 서버를 구성하려는 경우 Setup for Linux using SSH or Cert 질문에 Y(예)를 입력합니다.
3. SSH 키 기반 인증을 구성하려면 Enter your options 질문에 1을 입력합니다.

   SSH 인증을 사용하기로 선택한 경우 생성된 키 보안 인증을 Linux 서버에 복사해야 합니다. 자세한 내용은 Linux 서버에서 키 기반 인증 설정 단원을 참조하십시오.
4. 인증서 기반 인증을 구성하려면 Enter your options 질문에 2를 입력합니다.

   인증서 기반 인증 설정에 대한 자세한 내용은 Linux 서버에서 인증서 기반 인증 설정 섹션을 참조하세요.

다음 예에서는 원격 서버 구성에 대한 예제 항목을 포함하여 표시되는 내용을 보여줍니다.

```
Setting up target server for remote execution
Would you like to setup credentials for servers not managed by vCenter using NLTM for
 Windows [Y/N]: y

NOTE: For the best experience, we recommend that you create a new Active Directory user
 in the Domain Admins group.

Username for WinRM (Domain\User): username
Password for WinRM: password
Reenter password for WinRM: password
Are you okay with collector accepting and locally storing server certificates on your
 behalf during first interaction with windows servers? These certificates will be used
 by collector for secure communication with windows servers [Y/N]: Y
Successfully stored windows server credentials...
Please note that all windows server certificates are stored in directory /opt/amazon/
application-data-collector/remote-auth/windows/certs

Please note the IP address of the collector and run the script specified in the user
 documentation on all the windows servers in your inventory
Would you like to setup credentials for servers not managed by vCenter using SSH/Cert
 based for Linux? [Y/N]: Y
Choose one of the following options for remote authentication:
1. SSH based authentication
2. Certificate based authentication
Enter your options [1-2]: 1
User name for remote server: username
Generating SSH key on this machine...
SSH key pair path: /opt/amazon/application-data-collector/remote-auth/linux/keys/
id_rsa_assessment
Please add the public key "id_rsa_assessment.pub" to the "$HOME/.ssh/authorized_keys"
 file in your remote machines.
Your Linux remote server configurations are saved successfully.
```

버전 관리 구성 설정

`collector setup` 명령 또는 `collector setup --version-control-configurations` 명령 사용 시 버전 관리 구성 설정

1. Set up source code analysis? 질문에 Y(예)를 입력합니다.
2. Git 서버 엔드포인트를 구성하려면 Enter your options 질문에 1을 입력합니다.

GIT 서버 엔드포인트로 github.com을 입력합니다.

3. GitHub Enterprise Server를 구성하려면 Enter your options 질문에 2를 입력합니다.

   GIT server endpoint: *git-enterprise-endpoint*와 같이 https:// 없이 엔터프라이즈 엔드포인트를 입력합니다.

4. Git *username*과 개인용 액세스 *token*을 입력합니다.

5. C# 코드를 분석하려는 경우 Do you have any csharp repositories that should be analyzed on a windows machine? 질문에 Y(예)를 입력합니다.

   > **Note**
   >
   > Porting Assistant for .NET 권장 사항에 대해 .NET 리포지토리를 분석하려면 Porting Assistant for .NET 이식 평가 도구로 설정된 Windows 시스템을 제공해야 합니다. 자세한 내용은 Porting Assistant for .NET 설명서의 Getting started with Porting Assistant for .NET을 참조하세요.

6. Would you like to reuse existing windows credentials on this machine? 질문에 대해 C# 소스 코드 분석을 위해 Windows 시스템이 이전에 `--remote-server-configurations` 또는 `--vcenter-configurations` 설정의 일부로 제공된 보안 인증과 동일한 보안 인증을 사용하는 경우 Y(예)를 입력합니다.

   새 보안 인증을 입력하려는 경우 N(아니요)을 입력합니다.

7. VMWare vCenter Windows Machine 보안 인증을 사용하려면 Choose one of the following options for windows credentials에 1을 입력합니다.

8. Windows 시스템의 IP 주소를 입력합니다.

다음 예에서는 버전 관리 구성에 대한 예제 항목을 포함하여 표시되는 내용을 보여줍니다.

```
Set up for source code analysis [Y/N]: y
Choose one of the following options for version control type:
1. GIT
2. GIT Enterprise
3. Azure DevOps - Git
Enter your options [1-3]: 3
Your server endpoint: dev.azure.com (http://dev.azure.com/)
Your DevOps Organization name: <Your organization name>
```

```
Personal access token [None]:
Your version control credentials are saved successfully.
Do you have any csharp repositories that should be analyzed on a windows machine? [Y/
N]: y
Would you like to reuse existing windows credentials on this machine? [Y/N]: y
Choose one of the following options for windows credentials:
1. VMWare vCenter Windows Machine
2. Standard Windows Machine
Enter your options [1-2]:
1
Windows machine IP Address: <Your windows machine IP address>
Using VMWare vCenter Windows Machine credentials
Successfully stored windows server credentials...
```

데이터 수집을 위해 원격 Windows 및 Linux 서버 준비

> **Note**
>
> vCenter 보안 인증을 사용하여 Strategy Recommendations 애플리케이션 데이터 수집기를 설정하는 경우에는 이 단계가 필요 없습니다.

원격 서버 구성을 설정한 후 `collector setup command` 또는 `collector setup --remote-server-configurations` 명령을 사용하는 경우 Strategy Recommendations 애플리케이션 데이터 수집기가 원격 서버에서 데이터를 수집할 수 있도록 원격 서버를 준비해야 합니다.

> **Note**
>
> 프라이빗 IP 주소를 사용하여 서버에 연결할 수 있는지 확인해야 합니다. 원격 실행을 위해의 Virtual Private Cloud(VPC)를 통해 환경을 설정하는 방법에 AWS 대한 자세한 지침은 Amazon Virtual Private Cloud 사용 설명서를 참조하세요.

원격 Linux 서버를 준비하려면 원격 Linux 서버 준비 섹션을 참조하세요.

원격 Windows 서버를 준비하려면 Windows 서버에서 원격 서버 구성 설정 섹션을 참조하세요.

원격 Linux 서버 준비

Linux 서버에서 키 기반 인증 설정

원격 서버 구성을 구성할 때 Linux용 SSH 키 기반 인증을 설정하도록 선택한 경우 Strategy Recommendations 애플리케이션 데이터 수집기에서 데이터를 수집할 수 있게 다음 단계를 수행하여 서버에서 키 기반 인증을 설정해야 합니다.

Linux 서버에서 키 기반 인증 설정

1. 컨테이너의 다음 폴더에서 id_rsa_assessment.pub라는 이름으로 생성된 퍼블릭 키를 복사합니다.

   /opt/amazon/application-data-collector/remote-auth/linux/keys.
2. 복사한 퍼블릭 키를 모든 원격 시스템의 `$HOME/.ssh/authorized_keys` 파일에 추가합니다. 사용할 수 있는 파일이 없는 경우 `touch` 또는 `vim` 명령을 사용하여 생성합니다.
3. 원격 서버의 홈 폴더가 권한 수준 755 이하인지 확인합니다. 777인 경우 작동하지 않습니다. `chmod` 명령을 사용하여 권한을 제한할 수 있습니다.

Linux 서버에서 인증서 기반 인증 설정

원격 서버 구성을 구성할 때 Linux용 인증서 기반 인증을 설정하도록 선택한 경우 Strategy Recommendations 애플리케이션 데이터 수집기에서 데이터를 수집할 수 있게 다음 단계를 수행해야 합니다.

애플리케이션 서버에 대해 인증 기관(CA)이 이미 설정되어 있는 경우 이 옵션을 권장합니다.

Linux 서버에서 인증서 기반 인증 설정

1. 모든 원격 서버에 사용할 수 있는 사용자 이름을 복사합니다.
2. 수집기의 퍼블릭 키를 CA에 복사합니다.

   수집기의 퍼블릭 키는 다음 위치에서 찾을 수 있습니다.

   /opt/amazon/application-data-collector/remote-auth/linux/keys/id_rsa_assessment.pub

   인증서를 생성하려면 이 퍼블릭 키를 CA에 추가해야 합니다.
3. 이전 단계에서 생성한 인증서를 수집기의 다음 위치에 복사합니다.

   /opt/amazon/application-data-collector/remote-auth/linux/keys

인증서의 이름은 id_rsa_assessment-cert.pub여야 합니다.

4. 설정 단계에서 인증서 파일 이름을 입력합니다.

Windows 서버에서 원격 서버 구성 설정

수집기 설정에서 원격 서버 구성을 설정할 때 Windows를 설정하도록 선택한 경우 Strategy Recommendations에서 데이터를 수집할 수 있게 다음 단계를 수행해야 합니다.

> 원격 서버에서 실행되는 PowerShell 스크립트에 대해 자세히 알아보려면 이 노트를 읽으세요.
>
> 이 스크립트는 PowerShell 원격을 활성화하고 협상 이외의 모든 인증 방법을 비활성화합니다. 이는 Windows NT LAN Manager(NTLM)에 사용되며 'AllowUnencrypted' WSMan 프로토콜을 false로 설정하여 새로 생성된 리스너가 암호화된 트래픽만 수락하도록 합니다. Microsoft에서 제공한 스크립트인 `New-SelfSignedCertificateEx.ps1`을 사용하여 자체 서명된 인증서를 생성합니다.
>
> HTTP 리스너가 있는 모든 WSMan 인스턴스는 기존 HTTPS 리스너와 함께 제거됩니다. 그런 다음 새 HTTPS 리스너가 생성됩니다. TCP 포트 5986에 대한 인바운드 방화벽 규칙도 생성됩니다. 마지막 단계에서 WinRM 서비스가 다시 시작됩니다.

Windows 2008 서버에서 원격 연결을 통해 데이터 수집 설정

1. 다음 명령을 사용하여 서버에 설치된 PowerShell의 버전을 확인합니다.

```
$PSVersionTable
```

2. PowerShell 버전이 5.1이 아닌 경우 Microsoft 설명서의 WMF 5.1 설치 및 구성 지침에 따라 WMF 5.1을 다운로드하고 설치합니다.
3. 새 PowerShell 창에서 다음 명령을 사용하여 PowerShell 5.1이 설치되어 있는지 확인합니다.

```
$PSVersionTable
```

4. Windows 2012 이상에서 원격 연결을 통해 데이터 수집을 설정하는 방법을 설명하는 다음 단계를 따릅니다.

Windows 2012 이상의 서버에서 원격 연결을 통해 데이터 수집 설정

1. 다음 URL에서 설치 스크립트를 다운로드합니다.

   https://application-data-collector-release.s3.us-west-2.amazonaws.com/scripts/WinRMSetup.ps1
2. 다음 URL에서 `New-SelfSignedCertificateEx.ps1`을 다운로드하고 `WinRMSetup.ps1`을 다운로드한 동일한 폴더에 스크립트를 붙여넣습니다.

   https://github.com/Azure/azure-libraries-for-net/blob/master/Samples/Asset/New-SelfSignedCertificateEx.ps1
3. 설정을 완료하려면 다운로드한 PowerShell 스크립트를 모든 애플리케이션 서버에서 실행합니다.

```
.\WinRMSetup.ps1
```

> **Note**
>
> Windows Remote Server에서 Windows Remote Management(WinRM)가 제대로 설정되지 않은 경우 해당 서버에서 데이터를 수집하려고 하면 실패합니다. 이 경우 컨테이너의 다음 위치에서 서버에 해당하는 인증서를 삭제해야 합니다.
> /opt/amazon/application-data-collector/remote-auth/windows/certs/***ads-server-id***.cer
> 인증서를 삭제한 후 데이터 수집 프로세스가 다시 시도될 때까지 기다립니다.

수집기와 서버가 데이터 수집을 위해 설정되었는지 확인합니다.

다음 명령을 사용하여 수집기와 서버가 데이터 수집을 위해 설정되었는지 확인합니다.

```
collector diag-check
```

이 명령은 서버 구성에 대한 일련의 진단 검사를 수행하고 실패한 검사에 대한 입력을 제공합니다.

-a 모드에서 명령을 사용하면 검사가 완료된 후 DiagnosticCheckResult.txt 파일에 출력이 표시됩니다.

```
collector diag-check -a
```

해당 서버의 IP 주소를 사용하여 단일 서버의 서버 구성에 대해 진단 검사를 수행할 수 있습니다.

다음 예제는 성공적인 설정의 출력을 보여줍니다.

Linux 서버

```
            Provide your test server IP address: IP address
-------------------------------------------------------------
Start checking connectivity & credentials...
Connectivity and Credential Checks succeeded
-------------------------------------------------------------
Start checking permissions...
Permission Check succeeded
-------------------------------------------------------------
Start checking OS version...
OS version check succeeded
-------------------------------------------------------------
Start checking Linux Bash installation...
Linux Bash installation check succeeded
-------------------------------------------------------------
All diagnostic checks complete successfully.
This server is correctly set up and ready for data collection.
```

Windows 서버

```
            Windows PowerShell Version Check succeeded
Provide your test server IP address: IP address
-------------------------------------------------------------
Start checking connectivity & credentials...
Connectivity and Credential Checks succeeded
-------------------------------------------------------------
Start checking permissions...
Permission Check succeeded
-------------------------------------------------------------
Start checking OS version...
OS version check succeeded
-------------------------------------------------------------
Start checking Windows architecture type...
Windows Architecture Type Check succeeded
-------------------------------------------------------------
All diagnostic checks complete successfully.
This server is correctly set up and ready for data collection.
```

다음 예제는 원격 서버 보안 인증이 잘못된 경우 표시되는 오류 메시지를 보여줍니다.

```
Unable to authenticate the server credentials with IP address ${IPAddress}.
Ensure that your credentials are accurate and the server is configured correctly.
Use the following command to reset incorrect credentials.
collector setup –remote-server-configurations
```

5단계: Migration Hub 콘솔에서 Strategy Recommendations를 사용하여 권장 사항 가져오기

이 섹션에서는 Migration Hub 콘솔에서 Strategy Recommendations를 사용하여 처음으로 마이그레이션 권장 사항을 가져오는 방법을 설명합니다.

추천을 받으려면

1. 에서 생성한 AWS 계정을 사용하여에 Strategy Recommendations 설정로그인 AWS Management Console 하고 https://console.aws.amazon.com/migrationhub/ Migration Hub 콘솔을 엽니다.
2. Migration Hub 콘솔 탐색 창에서 전략을 선택합니다.
3. Migration Hub Strategy Recommendations 페이지에서 권장 사항 가져오기를 선택합니다.
4. Migration Hub가 계정에 서비스 연결 역할(SLR)을 생성할 수 있도록 허용하는 데 동의하면 동의를 선택합니다. SLR에 대한 자세한 내용은 Strategy Recommendations에 대한 서비스 연결 역할 사용 섹션을 참조하세요.
5. 데이터 소스 구성

    a. 데이터 소스 구성 페이지에서 다음 옵션 중에서 분석할 서버의 소스를 선택해야 합니다.

        i. Strategy Recommendations 애플리케이션 데이터 수집기 - Strategy Recommendations 수집기를 사용하여 VMware vCenter에서 호스팅되는 VM에 대한 정보를 자동으로 검색할 수 있습니다. 이 옵션을 사용하면 추가 설정을 수행할 필요가 없습니다.

        ii. 수동 가져오기 - 서버와 애플리케이션에 대한 데이터를 개별적으로 가져오려면 Strategy Recommendations 가져오기 템플릿을 사용합니다. 가져오기 템플릿은 VM에 대한 사용 가능한 정보를 입력할 수 있는 JSON 파일입니다.

        iii. Application Discovery Service - Application Discovery Service를 사용하여 온프레미스 애플리케이션 및 서버에 대한 정보를 수집할 수 있습니다. Migration Hub 콘솔의 도구 섹

션에서 검색 도구 아래의 여러 옵션 중에서 선택할 수 있습니다. 예를 들어, Application Discovery Service Agentless Collector, AWS Discovery Agent 또는 가져오기(CSV 파일의 경우)를 선택할 수 있습니다.

b. 서버 테이블에는 데이터 소스 섹션에서 선택한 사항에 따라 사용 가능한 서버가 모두 나열됩니다.

c. 등록된 애플리케이션 데이터 수집기 아래에는 설정한 애플리케이션 데이터 수집기가 나열됩니다. 데이터 수집기를 설정하지 않은 경우 데이터 수집기를 다운로드한 다음 배포할 수 있습니다. 자세한 내용은 1단계: Strategy Recommendations 수집기 다운로드 및 2단계: Strategy Recommendations 수집기 배포 단원을 참조하세요.

> **Note**
>
> 전략 권장 사항을 가져오려면 최소한 하나의 애플리케이션 데이터 수집기를 설정하거나 애플리케이션 데이터 가져오기를 수행해야 합니다. 수집기를 설정하지 않고 애플리케이션 수준 데이터를 추가하려는 경우 애플리케이션 데이터 가져오기 템플릿을 사용할 수 있습니다. 나중에 데이터 소스를 더 추가할 수 있습니다.

d. 수동 가져오기를 선택한 경우 가져오기 세부 정보에서 새 가져오기 추가를 선택합니다.

e. 가져오기 이름에 가져오기의 이름을 입력합니다.

f. S3 버킷 URI에 업로드할 가져오기 JSON 파일의 S3 버킷 URI를 입력합니다.

> **Important**
>
> S3 버킷 이름은 접두사 **`migrationhub-strategy`**로 시작해서는 안 됩니다.

g. Next(다음)를 선택합니다.

6. 기본 설정 지정

a. 기본 설정 지정 페이지에서 비즈니스 목표 및 마이그레이션 기본 설정을 지정합니다. Strategy Recommendations는 지정한 기본 설정에 따라 애플리케이션과 데이터베이스를 마이그레이션하고 현대화하기 위한 최적의 전략을 권장합니다. 나중에 이 기본 설정을 변경할 수 있습니다.

b. Next(다음)를 선택합니다.

7. 검토 및 제출

a. 구성된 데이터 소스 및 마이그레이션 기본 설정을 검토합니다.

b. 모든 것이 정확해 보이면 데이터 분석 시작을 선택합니다. 그러면 서버 인벤토리 및 런타임 환경과 Microsoft IIS 및 Java 애플리케이션의 애플리케이션 바이너리 분석이 수행됩니다.

> **Note**
>
> 바이너리 분석 상태는 콘솔에 표시되지 않습니다. 분석이 완료되면 안티 패턴 보고서에 대한 링크나 분석이 실패했다는 메시지가 표시됩니다.

Strategy Recommendations 권장 사항

이 섹션에서는 마이그레이션 포트폴리오의 서버 및 애플리케이션에 대한 Strategy Recommendations 마이그레이션 및 현대화 권장 사항을 보는 방법을 설명합니다.

주제

Strategy Recommendations에서 전략 권장 사항 보기

이 섹션에서는 AWS Migration Hub 콘솔에서 Strategy Recommendations를 사용하여 마이그레이션 전략 권장 사항을 보는 방법을 설명합니다.

전략 권장 사항 보기

1. 에서 생성한 AWS 계정을 사용하여에 Strategy Recommendations 설정로그인 AWS Management Console 하고 https://console.aws.amazon.com/migrationhub/ Migration Hub 콘솔을 엽니다.
2. Migration Hub 콘솔 탐색 창에서 전략을 선택한 다음 권장 사항을 선택합니다.
3. 권장 사항 페이지에서 포트폴리오의 요약 권장 사항 및 세부 마이그레이션 'R' 전략 권장 사항을 보고 내보낼 수 있습니다. 또한 마이그레이션 및 현대화 도구 및 대상과 서버 및 애플리케이션 구성 요소에 대한 안티 패턴을 볼 수 있습니다.

   안티 패턴은 포트폴리오에서 발견된 알려진 문제를 심각도별로 분류한 목록입니다. 심각도가 높은 안티 패턴은 해결해야 할 비호환성을 나타내고, 중간 심각도의 안티 패턴은 경고를 나타내고, 심각도가 낮은 안티 패턴은 정보 문제를 나타냅니다. 'R' 전략에 대한 자세한 내용은 AWS Prescriptive Guidance 용어집의 Migration terms - 7 Rs를 참조하세요.

   - 데이터 센터에 변경 사항이 있거나 기본 설정을 업데이트하는 경우 데이터를 다시 분석하는 것이 좋습니다. 데이터를 다시 분석하여 권장 사항을 새로 받으려면 데이터 다시 분석을 선택합니다.

     다시 분석 프로세스가 완료될 때까지 이전 데이터와 새 데이터가 권장 데이터 결과에 혼합될 수 있습니다.

권장 사항이 포함된 보고서 파일을 다운로드하려면 권장 사항 내보내기를 선택합니다.

4. 애플리케이션 구성 요소 탭에서 마이그레이션 포트폴리오의 애플리케이션 구성 요소에 대한 권장 사항을 볼 수 있습니다. 자세한 내용은 Strategy Recommendations 애플리케이션 구성 요소 권장 사항 단원을 참조하십시오.
5. 서버 탭에서 마이그레이션 포트폴리오의 서버에 대한 권장 사항을 볼 수 있습니다. 자세한 내용은 Strategy Recommendations 서버 권장 사항 단원을 참조하십시오.
6. 기본 설정 탭에서 5단계: 추천 받기에서 지정한 기본 설정을 편집할 수 있습니다. 기본 설정 편집에 대한 자세한 내용은 Strategy Recommendations 기본 설정 섹션을 참조하세요.

Strategy Recommendations 애플리케이션 구성 요소 권장 사항

이 섹션에서는 Migration Hub 콘솔에서 Strategy Recommendations를 사용하여 애플리케이션 구성 요소에 대한 마이그레이션 전략 권장 사항을 보고 분석하는 방법을 설명합니다.

주제

- Strategy Recommendations에서 애플리케이션 구성 요소 작업 수행
- Strategy Recommendations 소스 코드 분석
- Strategy Recommendations 데이터베이스 분석
- Strategy Recommendations 바이너리 분석

Strategy Recommendations에서 애플리케이션 구성 요소 작업 수행

이 섹션에서는 Migration Hub 콘솔에서 Migration Hub Strategy Recommendations를 사용하여 마이그레이션 및 현대화 전략 권장 사항을 보고 구성하는 방법을 설명합니다.

주제

- 애플리케이션 구성 요소 권장 사항 보기
- 애플리케이션 구성 요소에 대한 소스 코드 분석 구성
- 애플리케이션 구성 요소에 대한 데이터베이스 분석 구성

애플리케이션 구성 요소 권장 사항 보기

이 섹션에서는 Migration Hub 콘솔에서 Strategy Recommendations를 사용하여 애플리케이션 구성 요소에 대한 마이그레이션 전략 권장 사항을 보는 방법을 설명합니다.

애플리케이션 구성 요소에 대한 권장 사항 세부 정보 보기

1. 에서 생성한 AWS 계정을 사용하여에 Strategy Recommendations 설정로그인 AWS Management Console 하고 https://console.aws.amazon.com/migrationhub/ Migration Hub 콘솔을 엽니다.
2. Migration Hub 콘솔 탐색 창에서 전략을 선택한 다음 권장 사항을 선택합니다.
3. 권장 사항 페이지에서 애플리케이션 구성 요소 탭을 선택합니다.

   a. 애플리케이션 구성 요소 요약 아래에는 서버 포트폴리오에서 실행 중인 다양한 유형의 응용 프로그램 구성 요소에 대한 개요가 나와 있습니다.

   b. 애플리케이션 구성 요소에서 구성 요소 이름, 구성 요소 유형 및 마이그레이션 'R' 전략 권장 사항을 볼 수 있습니다. 서버 포트폴리오에서 실행 중인 다양한 애플리케이션 구성 요소에 사용할 마이그레이션 대상과 마이그레이션 및 현대화 도구도 볼 수 있습니다. 'R' 전략에 대한 자세한 내용은 AWS Prescriptive Guidance 용어집의 Migration terms - 7 Rs를 참조하세요.
4. 애플리케이션 구성 요소의 세부 정보를 보려면 애플리케이션 구성 요소를 선택한 다음 세부 정보 보기를 선택합니다.
5. 애플리케이션 구성 요소 세부 정보 페이지(구성 요소 이름이 제목으로 표시된 페이지)의 권장 사항 요약 아래에서 애플리케이션 구성 요소에 대한 권장 사항을 볼 수 있습니다. 식별된 안티 패턴도 볼 수 있습니다. 안티 패턴은 포트폴리오에서 발견된 알려진 문제를 심각도별로 분류한 목록입니다.
6. 전략 옵션 탭을 선택하여 애플리케이션 구성 요소에 대한 마이그레이션 권장 사항을 봅니다. 다른 전략을 선택한 다음 기본 설정됨을 선택하여 권장 전략을 재정의할 수 있습니다.
7. 보고 있는 애플리케이션 구성 요소의 유형에 따라 소스 구성 또는 데이터베이스 구성 탭이 있습니다. 소스 구성에 대한 자세한 내용은 애플리케이션 구성 요소에 대한 소스 코드 분석 구성 섹션을 참조하세요. 데이터베이스 구성에 대한 자세한 내용은 애플리케이션 구성 요소에 대한 데이터베이스 분석 구성 섹션을 참조하세요.

애플리케이션 구성 요소에 대한 소스 코드 분석 구성

이 섹션에서는 Migration Hub 콘솔에서 Strategy Recommendations를 사용하여 애플리케이션 구성 요소에 대한 소스 코드 분석을 구성하는 방법을 설명합니다.

애플리케이션 구성 요소에 대한 소스 코드 분석 구성

1. Migration Hub 콘솔 탐색 창에서 전략을 선택한 다음 권장 사항을 선택합니다.
2. 권장 사항 페이지에서 애플리케이션 구성 요소 탭을 선택합니다.

3. 애플리케이션 구성 요소 아래의 구성 요소 목록에서 구성 요소 유형이 java, dotnetframework 또는 IIS인 애플리케이션 구성 요소를 선택한 다음 세부 정보 보기를 선택합니다.
4. 애플리케이션 구성 요소 세부 정보 페이지(구성 요소 이름이 제목으로 표시된 페이지)에서 소스 코드 구성 탭을 선택합니다.
5. 소스 코드 구성 세부 정보에서 소스 코드 분석을 선택합니다.
6. 소스 코드 분석 페이지에서 애플리케이션 구성 요소의 소스 코드를 저장하는 리포지토리 이름, 브랜치 이름 및 프로젝트 이름(해당하는 경우)을 입력합니다. 사용할 GitHub 소스 코드 버전 관리의 유형을 선택한 다음 분석을 선택합니다.

   분석이 완료되면 애플리케이션 구성 요소 세부 정보 페이지에서 업데이트된 권장 사항을 볼 수 있습니다.

소스 코드 분석에 대한 자세한 내용은 Strategy Recommendations 소스 코드 분석 섹션을 참조하세요.

애플리케이션 구성 요소에 대한 데이터베이스 분석 구성

이 섹션에서는 Migration Hub 콘솔에서 Strategy Recommendations를 사용하여 애플리케이션 구성 요소에 대한 데이터베이스 분석을 구성하는 방법을 설명합니다.

애플리케이션 구성 요소에 대한 데이터베이스 분석 구성

1. Migration Hub 콘솔 탐색 창에서 전략을 선택한 다음 권장 사항을 선택합니다.
2. 권장 사항 페이지에서 애플리케이션 구성 요소 탭을 선택합니다.
3. 애플리케이션 구성 요소 아래의 구성 요소 목록에서 구성 요소 유형이 SQLServer인 애플리케이션 구성 요소를 선택한 다음 세부 정보 보기를 선택합니다.
4. 애플리케이션 구성 요소 세부 정보 페이지(구성 요소 이름이 제목으로 표시된 페이지)에서 데이터베이스 구성 탭을 선택합니다.
5. 데이터베이스 구성 세부 정보에서 데이터베이스 세부 정보 분석을 선택합니다.
6. AWS Secrets Manager에서 생성한 드롭다운 메뉴에서 데이터베이스 보안 인증에 사용할 보안 암호 이름을 선택하고 분석을 선택합니다.

   분석이 완료되면 애플리케이션 구성 요소 세부 정보 페이지에서 업데이트된 권장 사항을 볼 수 있습니다.

데이터베이스 분석 및 보안 암호 이름 설정에 대한 자세한 내용은 Strategy Recommendations 데이터베이스 분석 섹션을 참조하세요.

Strategy Recommendations 소스 코드 분석

Migration Hub Strategy Recommendations는 자동으로 포트폴리오의 애플리케이션을 식별하고 해당 애플리케이션을 위한 애플리케이션 구성 요소를 생성합니다. 예를 들어, 포트폴리오에 Java 애플리케이션이 있는 경우 해당 애플리케이션은 구성 요소 유형이 java인 애플리케이션 구성 요소로 식별됩니다.

Strategy Recommendations는 애플리케이션 구성 요소의 소스 코드를 분석하도록 구성된 경우 해당 코드를 분석합니다. 소스 코드 분석을 위한 애플리케이션 구성 요소 설정에 대한 자세한 내용은 애플리케이션 구성 요소에 대한 소스 코드 분석 구성 섹션을 참조하세요.

Strategy Recommendations는 Java 및 C# 프로그래밍 언어에 대한 소스 코드 분석을 수행합니다.

Strategy Recommendations 소스 코드 분석 사용을 위한 사전 조건에 대한 자세한 내용은 Strategy Recommendations의 사전 조건 섹션을 참조하세요.

Strategy Recommendations 데이터베이스 분석

Strategy Recommendations는 자동으로 포트폴리오의 데이터베이스 서버를 식별하고 이를 위한 애플리케이션 구성 요소를 생성합니다. 예를 들어 포트폴리오에 SQL Server 데이터베이스가 있는 경우 해당 데이터베이스는 애플리케이션 구성 요소 sqlservr.exe로 식별됩니다.

Strategy Recommendations는 AWS Schema Conversion Tool 사용하여 식별된 SQL Server 애플리케이션 구성 요소인 sqlservr.exe의 개별 데이터베이스를 분석합니다. Strategy Recommendations는 데이터베이스를 Amazon Aurora MySQL 호환 버전, Amazon Aurora PostgreSQL 호환 버전, Amazon RDS for MySQL 및 Amazon RDS for PostgreSQL과 같은 AWS 데이터베이스로 마이그레이션할 때 비호환성을 식별합니다. MySQL

현재 Strategy Recommendations 데이터베이스 분석은 SQL 서버에만 제공됩니다.

데이터베이스를 분석하도록 Strategy Recommendations를 구성하려면 Strategy Recommendations 애플리케이션 데이터 수집기가 데이터베이스에 연결할 수 있게 보안 인증을 제공해야 합니다. 이렇게 하려면 AWS 계정의 AWS Secrets Manager에서 보안 암호를 생성합니다.

제공하는 보안 인증의 권한에 대한 자세한 내용은 AWS Schema Conversion Tool 자격 증명에 필요한 권한 섹션을 참조하세요. 보안 인증을 사용한 보안 암호 생성에 대한 자세한 내용은 Secrets Manager에서 데이터베이스 보안 인증을 위한 보안 암호 생성 섹션을 참조하세요.

자격 증명과 보안 암호를 설정한 후 데이터베이스 서버에서 AWS Schema Conversion Tool 분석을 구성할 수 있습니다. 자세한 내용은 애플리케이션 구성 요소에 대한 데이터베이스 분석 구성 단원을 참조하십시오.

애플리케이션 구성 요소에 대한 데이터베이스 분석을 구성하면 AWS Schema Conversion Tool 인벤토리 작업이 예약됩니다. 이 작업이 완료되면 해당 데이터베이스 서버의 모든 개별 데이터베이스에 대해 새 애플리케이션 구성 요소가 생성되는 것을 볼 수 있습니다. 예를 들어 SQL Server에 두 개의 데이터베이스(exampledbs1 및 exampledbs2)가 있는 경우 각 데이터베이스에 대해 exampledbs1과 exampledbs2라는 애플리케이션 구성 요소가 생성됩니다.

식별된 각 데이터베이스를 데이터베이스로 AWS 마이그레이션할 때 안티 패턴을 보려면 애플리케이션 구성 요소에 대한 데이터베이스 분석 구성의 단계에 따라 각 데이터베이스에 대한 분석을 설정합니다.

AWS Schema Conversion Tool 자격 증명에 필요한 권한

AWS Secrets Manager에 제공하는 로그인 자격 증명에는 `VIEW SERVER STATE` 및 `VIEW ANY DEFINITION` 권한만 필요합니다.

SQL Server 로그인을 생성할 때 원하는 로그인 이름과 암호를 제공할 수 있습니다.

Secrets Manager에서 데이터베이스 보안 인증을 위한 보안 암호 생성

보안 인증 정보를 Strategy Recommendations 애플리케이션 데이터 수집기가 데이터베이스에 연결할 준비가 되면 다음 절차에 설명된 대로 AWS 계정의 AWS Secrets Manager에서 보안 암호를 생성합니다.

AWS 계정에서 AWS Secrets Manager를 사용하여 보안 암호를 생성하려면

1. 에서 생성한 AWS 계정을 사용하여에 Strategy Recommendations 설정로그인 AWS Management Console 하고 https://console.aws.amazon.com/secretsmanager/ AWS Secrets Manager 콘솔을 엽니다.
2. 새 암호 저장을 선택합니다.
3. 보안 암호 유형을 다른 유형의 보안 암호를 선택합니다.
4. 키/값 페어 아래에 다음 정보를 입력합니다.

   사용자 이름 - *your-username*

   그런 다음 + 행 추가를 선택하고 다음 정보를 입력합니다.

   암호 - *your-password*
5. 다음을 선택합니다.
6. migrationhub-strategy- 접두사가 붙은 문자열로 보안 암호 이름을 입력합니다. migrationhub-strategy-one을 예로 들 수 있습니다.

> **Note**
>
> 나중에 사용할 수 있도록 안전한 곳에 보안 암호 이름을 저장합니다.

7. 다음을 선택하고 다음을 다시 선택합니다.
8. 저장(Store)을 선택합니다.

Strategy Recommendations에서 데이터베이스 분석을 설정할 때 데이터베이스 보안 인증을 위해 생성한 보안 암호를 사용할 수 있습니다.

Strategy Recommendations 바이너리 분석

Migration Hub Strategy Recommendations는 포트폴리오의 애플리케이션과 해당 애플리케이션에 속하는 애플리케이션 구성 요소를 자동으로 식별합니다. 예를 들어, 포트폴리오에 Java 애플리케이션이 있는 경우 Strategy Recommendations는 해당 애플리케이션을 구성 요소 유형이 java인 애플리케이션 구성 요소로 식별합니다. 소스 코드에 대한 액세스를 구성하지 않고도 Strategy Recommendations는 Windows의 IIS 애플리케이션 DLL이나 Linux의 애플리케이션 JAR 파일을 검사하여 바이너리 분석을 수행하고 안티 패턴 보고서 또는 비호환성 보고서를 제공할 수 있습니다. 안티 패턴 보고서는 Strategy Recommendations가 포트폴리오에서 발견한 알려진 문제를 심각도별로 분류한 목록입니다. 비호환성 보고서에는 API 호환성, Nuget Package 및 이식 작업과 같은 안티 패턴의 하위 집합이 포함됩니다.

Strategy Recommendations는 Windows IIS, Java Tomcat 및 Jboss 애플리케이션에 대한 분석을 수행합니다. IIS 애플리케이션이 있는 경우 Strategy Recommendations는 기본적으로 비호환성 보고서를 생성합니다. 전체 안티 패턴 보고서를 받으려면 소스 코드 액세스를 구성해야 합니다. Java 애플리케이션이 있는 경우 Strategy Recommendations는 기본적으로 전체 안티 패턴 보고서를 생성합니다.

비호환 보고서 또는 안티 패턴 보고서는 분석이 완료된 후 표시됩니다. 분석에 실패한 경우 버전 관리 구성 설정에 설명된 대로 소스 코드 액세스 권한을 제공하여 소스 코드 분석을 실행해 볼 수 있습니다.

Strategy Recommendations 서버 권장 사항

이 섹션에서는 Migration Hub 콘솔에서 Migration Hub Strategy Recommendations를 사용하여 마이그레이션 포트폴리오의 서버에 대한 마이그레이션 전략 권장 사항을 보는 방법을 설명합니다.

서버 권장 사항 보기

1. 에서 생성한 AWS 계정을 사용하여에 Strategy Recommendations 설정로그인 AWS Management Console 하고 https://console.aws.amazon.com/migrationhub/ Migration Hub 콘솔을 엽니다.

2. Migration Hub 콘솔 탐색 창에서 전략을 선택한 다음 권장 사항을 선택합니다.
3. 권장 사항 페이지에서 서버 탭을 선택합니다.

   a. 서버 요약에서는 포트폴리오에서 실행 중인 다양한 유형의 서버에 대한 개요를 볼 수 있습니다.

   b. 서버에서는 서버 및 운영 체제 세부 정보와 마이그레이션 'R' 전략 권장 사항을 볼 수 있습니다. 또한 권장 사항에 따라 마이그레이션 대상과 서버에서 식별된 안티 패턴 수를 볼 수 있습니다. 'R' 전략에 대한 자세한 내용은 AWS Prescriptive Guidance 용어집의 Migration terms - 7 Rs를 참조하세요.
4. 서버에 대한 심층적인 권장 사항 세부 정보를 보려면 목록에서 서버를 선택한 다음 세부 정보 보기를 선택합니다. 서버에서 실행 중인 애플리케이션 구성 요소를 기반으로 하는 서버 심층 분석 및 권장 사항과 함께 서버에 대해 수집된 메타데이터를 볼 수 있습니다.
5. 서버 세부 정보 페이지(서버 이름이 제목으로 표시된 페이지)의 권장 사항 요약에서 서버에 대한 전략 권장 사항의 개요를 볼 수 있습니다. 식별된 안티 패턴도 볼 수 있습니다. 안티 패턴은 포트폴리오에서 발견된 알려진 문제를 심각도별로 분류한 목록입니다.
6. 전략 옵션 탭을 선택하여 서버에 대한 마이그레이션 권장 사항을 봅니다. 다른 전략을 선택한 다음 기본 설정됨을 선택하여 권장 전략을 재정의할 수 있습니다.
7. 애플리케이션 구성 요소 탭을 선택하여 서버와 관련된 애플리케이션 구성 요소의 목록을 볼 수 있습니다.
8. 애플리케이션 구성 요소에 대한 세부 정보를 보려면 목록에서 구성 요소를 선택하고 세부 정보 보기를 선택합니다. 애플리케이션 구성 요소에 대한 자세한 내용은 애플리케이션 구성 요소 작업 수행 섹션을 참조하세요.

Strategy Recommendations 기본 설정

이 섹션에서는 Migration Hub 콘솔에서 Migration Hub Strategy Recommendations 기본 설정을 보고 편집하는 방법을 설명합니다.

5단계: 추천 받기에 설명된 대로 Strategy Recommendations를 처음 설정할 때 권장 사항 기본 설정을 선택합니다. 이러한 기본 설정을 편집할 수 있습니다.

권장 사항 기본 설정 편집

1. 에서 생성한 AWS 계정을 사용하여에 Strategy Recommendations 설정로그인 AWS Management Console 하고 https://console.aws.amazon.com/migrationhub/ Migration Hub 콘솔을 엽니다.
2. Migration Hub 콘솔 탐색 창에서 전략을 선택한 다음 권장 사항을 선택합니다.

3. 권장 사항 페이지에서 기본 설정 탭을 선택합니다.
4. 우선순위 비즈니스 목표에서 비즈니스 목표를 끌어서 놓아 재정렬할 수 있습니다.
5. 원하는 애플리케이션 기본 설정과 데이터베이스 기본 설정을 선택한 다음 변경 사항 저장을 선택합니다.

기본 설정을 변경하면 데이터 다시 분석을 선택하라는 내용의 배너가 표시됩니다.

Strategy Recommendations 데이터 소스

이 섹션에서는 Strategy Recommendations에서 사용하는 데이터 소스를 설명합니다.

주제

Strategy Recommendations 데이터 소스 보기

이 섹션에서는에서 Strategy Recommendations 데이터 소스를 보는 방법을 설명합니다 AWS Management Console.

데이터 소스 보기

1. 에서 생성한 AWS 계정을 사용하여에 Strategy Recommendations 설정로그인 AWS Management Console 하고 https://console.aws.amazon.com/migrationhub/ Migration Hub 콘솔을 엽니다.
2. Migration Hub 콘솔 탐색 창에서 전략을 선택한 다음 데이터 소스를 선택합니다.
3. 수집기 탭에서 설정한 Strategy Recommendations 애플리케이션 데이터 수집기를 볼 수 있습니다. 수집기에 대한 자세한 내용은 Strategy Recommendations 애플리케이션 데이터 수집기 섹션을 참조하세요.
4. 가져오기 탭에서 데이터를 가져오고 데이터 가져오기를 볼 수 있습니다. 자세한 내용은 Strategy Recommendations로 데이터 가져오기 단원을 참조하십시오.
5. 도구 탭에서 수집기 및 애플리케이션 가져오기 데이터 템플릿을 다운로드할 수 있습니다.

Strategy Recommendations 애플리케이션 데이터 수집기

이 섹션에서는 Strategy Recommendations 애플리케이션 데이터 수집기를 사용하는 방법을 설명합니다.

애플리케이션 데이터 수집기 다운로드 및 설정에 대한 자세한 내용은 1단계: Strategy Recommendations 수집기 다운로드 섹션을 참조하세요.

주제

Strategy Recommendations 수집기에서 수집하는 데이터

이 섹션에서는 Migration Hub Strategy Recommendations 애플리케이션 데이터 수집기에서 수집하는 데이터 유형을 설명합니다. 애플리케이션 데이터 수집기는 서버에서 실행 중인 애플리케이션을 식별하고, 소스 코드 분석을 수행하고, 데이터베이스를 분석하는 에이전트 없는 데이터 수집기입니다.

데이터 필드	설명
OS 유형	Windows 또는 Linux
OS 버전	특정 버전의 OS입니다. Windows Server 2003, RHEL 5.2를 예로 들 수 있습니다.
OS 아키텍처	32비트 또는 64비트 OS
서버 VM임	서버가 VM 또는 물리적 머신입니다.
가상화 소프트웨어	vCenter, Hyper-V를 예로 들 수 있습니다.
위치	Amazon Elastic Compute Cloud 콘솔(Amazon EC2) 또는 온프레미스를 예로 들 수 있습니다.
dualBoot임	여러 OS로 부팅할 수 있습니다.
펌웨어 유형	BIOS, UEFI
부트 로더	GRUB, GRUB 2
파티션 테이블 유형	MBR, GPT
CPU 속도	CPU 속도(GHz). 예: 2.4GHz
Windows OS data	
Windows 버전	Standard, Data Center, Enterprise

데이터 필드	설명
.NET Framework 버전	설치된 .NET Framework 버전
.NET Core 버전	설치된 .NET 코어 버전
Linux data	
Linux OS 배포판	RHEL, CentOS, SUSE 등
커널 버전	uname -r 출력(예: `4.9.217-0.1.ac.205.84.332.metal1.x86_64`
For each disk volume	
파일 시스템 유형	FAT32, NTFS, ReFS, ext4, jfs 등)
디스크 볼륨 크기	총 디스크 크기
디스크 볼륨 여유 공간	디스크 여유 공간
가상 디스크 이미지 형식	vmdk, vhd, vhdx
디스크 유형(Windows)	기본, 동적
Application level data	
애플리케이션 이름	실행 중인 프로세스의 이름. 예: SQLServr.exe, MSdtsservr.exe 등
애플리케이션 유형	IIS, JBoss, Tomcat 등
프로그래밍 언어 및 버전	C#, Java
JDK 버전	설치된 JDK의 버전
소스 코드 사용 가능 여부	소스 코드 리포지토리를 제공하면 소스 코드를 사용할 수 있음을 나타냅니다.
애플리케이션 비트 크기	16비트, 32비트, 64비트
Windows	

데이터 필드	설명
앱에서 사용하는.NET Framework 버전	애플리케이션용으로 런타임 시 로드되는 .NET Framework DLL의 버전
.NET Core 버전	애플리케이션용으로 런타임 시 로드되는 .NET Core DLL의 버전
WPF 프레임워크 사용 여부	.NET 기반 애플리케이션이 WPF 애플리케이션 유형인지 여부를 결정합니다.
WCF 프레임워크 사용 여부	.NET 기반 애플리케이션이 WCF 애플리케이션 유형인지 여부를 결정합니다.
ASP.NET 버전	ASP.NET의 버전
IIS 버전	Windows 컴퓨터에 설치된 IIS 서버의 버전
애플리케이션 OS 드라이버 비트 크기	32비트, 64비트
Windows 레지스트리 사용	컴퓨터의 레지스트리 키를 쿼리하여 데이터베이스 버전, Java 버전, .NET 버전 등의 정보를 찾습니다.
애플리케이션에서 사용하는 모든 DLL	Windows 프로세스에서 런타임 시 로드한 모든 DLL 목록을 가져옵니다.
PowerShell 버전	컴퓨터에 설치된 PowerShell 버전을 확인합니다. 5.1 이상이어야 합니다.
Linux	
애플리케이션 프레임워크 유형	Tomcat, Spring Boot, JBoss, WebLogic, WebSphere
애플리케이션 프레임워크 버전	애플리케이션 프레임워크의 버전
Database	
데이터베이스 유형	MS SQL, Oracle, MySQL 등

데이터 필드	설명
데이터베이스 버전	데이터베이스의 버전

Strategy Recommendations에서 데이터 제거

Strategy Recommendations에서 데이터를 모두 제거하려면 AWS Support에 연락하여 전체 데이터 삭제를 요청하세요.

Strategy Recommendations 수집기 업그레이드

Migration Hub Strategy Recommendations 애플리케이션 데이터 수집기는 자동으로 업그레이드됩니다. 필요한 경우 다음 절차를 사용하여 수동으로 수집기를 업그레이드할 수 있습니다.

Strategy Recommendations 수집기 업그레이드

1. 다음 명령을 사용하여 SSH 클라이언트로 수집기 VM에 연결합니다.

```
ssh ec2-user@CollectorIPAddress
```

2. 다음 예제와 같이 수집기 VM의 업그레이드 디렉터리로 변경합니다.

```
cd  /home/ec2-user/collector/upgrades
```

3. 다음 명령을 사용하여 업그레이드 스크립트를 실행합니다.

```
sudo bash application-data-collector-upgrade
```

Strategy Recommendations로 데이터 가져오기

애플리케이션 데이터 수집기를 사용하는 대신 마이그레이션 및 현대화 권장사항을 원하는 애플리케이션 및 서버에 대한 정보를 가져올 수 있습니다.

데이터를 가져올 때 권장 사항은 데이터 수집기를 사용할 때만큼 심층적이지 않습니다. 예를 들어, 가져온 데이터에는 소스 코드 분석을 사용할 수 없습니다.

이 섹션에서는 애플리케이션 가져오기 템플릿을 사용하여 Migration Hub 콘솔에서 Strategy Recommendations로 데이터를 가져오는 방법을 설명합니다.

데이터 가져오기

1. 에서 생성한 AWS 계정을 사용하여에 Strategy Recommendations 설정로그인 AWS Management Console 하고 https://console.aws.amazon.com/migrationhub/ Migration Hub 콘솔을 엽니다.
2. Migration Hub 콘솔 탐색 창에서 전략을 선택한 다음 데이터 소스를 선택합니다.
3. 가져오기 탭을 선택합니다.
4. 가져오기 템플릿 다운로드를 선택하여 애플리케이션 가져오기 템플릿을 다운로드합니다.
5. 템플릿을 작성하여 Amazon S3 버킷에 업로드합니다. 버킷 이름이 접두사 `migrationhub-strategy`로 시작하는지 확인합니다.
6. 가져오기 탭으로 돌아가서 가져오기를 선택합니다.
7. 가져오기 이름을 입력하고, 작성한 데이터 템플릿의 Amazon S3 객체 URI를 입력한 다음 가져오기 시작을 선택합니다.

Strategy Recommendations 가져오기 템플릿

다운로드하는 가져오기 템플릿은 다음 예제와 같은 `.json` 파일입니다.

```
{
    "ImportFormatVersion": 1,
    "Resources": [
        {
            "ResourceType": "SERVER",
            "ResourceName": "",
            "ResourceId": "",
            "IpAddress": "",
            "OSDistribution": "",
            "OSType": "",
            "HostName": "",
            "OSVersion": "",
            "CPUArchitecture": ""
        },
        {
            "ResourceType": "PROCESS",
            "ResourceName": "",
            "ResourceId": "",
            "ApplicationType": "",
            "DotNetFrameworkVersion": "",
            "ApplicationVersion": "",
            "DotNetCoreVersion": "",
```

```
            "JdkVersion": "",
            "ProgrammingLanguage": "",
            "DatabaseType": "",
            "DatabaseVersion": "",
            "DatabaseEdition": "",
            "AssociatedServerIds": []
        }
    ]
}
```

가져오기 템플릿을 작성하는 데 도움이 되도록 데이터 필드의 유효한 값이 다음 표에 나열되어 있습니다.

서버에 대한 필수 필드는 다음 표에 나열되어 있습니다.

명칭	설명	형식	필수	유효값
ResourceId	요청에 대한 고유 ID	String	예	모든 고유 문자열
ResourceName	리소스의 이름	String	예	모든 문자열
ResourceType	가져올 리소스의 유형	String	예	"Server", "Process"
OSDistribution	Windows, Windows Server, Ubuntu	String	예	Windows: "Windows PC" , "Windows Server" Linux: "Ubuntu", "RHEL", "Amazon Linux", "DEBIAN", "SLES", "CENT_OS" , "ORACLE_LINUX", "FEDORA", "KALI"
OSType	운영 체제 유형	String	예	"Windows", "Linux"
OSVersion	커널 버전	String	예	설명서의 HTML 버전을 참조하세요.

명칭	설명	형식	필수	유효값
CPUArchitecture	CPU 아키텍처	String	No	"32bit", "64bit"
IpAddress	서버의 IP 주소	Array	아니요	xxx.xxx.xxx.xxx 형식
MacAddresses	서버와 연결된 Mac 주소	Array	아니요	xx:xx:xx:xx:xx:xx 형식
Hostname	호스트의 이름	String	No	모든 문자열

프로세스에 대한 필수 필드는 다음 표에 나열되어 있습니다.

명칭	설명	형식	필수	유효값
ResourceId	요청에 대한 고유 ID	String	예	모든 고유 문자열
ResourceName	리소스의 이름	String	예	모든 문자열
ResourceType	가져올 리소스의 유형	String	예	"Server", "Process"
AssociatedServerIds	프로세스가 실행 중인 서버 ID의 목록	String	예	정의한 “"ResourceType": "SERVER"의 ResourceId
ApplicationType	애플리케이션 유형	String	예	"Tomcat", "JBoss", "Spring", "IIS", "Mongo DB", "DB2", "Maria DB", "MySQL", "Oracle", "SQLServer", "Sybase", "PostgreSQLServer", "Cassandra",

명칭	설명	형식	필수	유효값
				"IBM WebSphere", "Oracle WebLogic", "Java Generic"
ApplicationVersion	애플리케이션의 버전	String	예	"IIS 1.0", "IIS 2.0", "IIS 3.0", "IIS 4.0", "IIS 5.0", "IIS 5.1", "IIS 6.0", "IIS 7.0", "IIS 7.5", "IIS 8.0", "IIS 8.5", "IIS 10.0"
ProgrammingLanguage	애플리케이션을 위한 프로그래밍 언어	String	No	"Java", "CSharp"

명칭	설명	형식	필수	유효값
DotNetFrameworkVersion	애플리케이션이 .NET Framework 기반인 경우 .NET Framework 버전	String	No	"DotnetFramework 1.0", "DotnetFramework 1.0 SP1", "DotnetFramework 1.0 SP2", "DotnetFramework 1.0 SP3", "DotnetFramework 1.1", "DotnetFramework 1.1 SP1", "DotnetFramework 2.0", "DotnetFramework 2.0 SP1", "DotnetFramework 2.0 SP2", "DotnetFramework 3.0", "DotnetFramework 3.0 SP1", "DotnetFramework 3.0 SP2", "DotnetFramework 3.5", "DotnetFramework 3.5 SP1", "DotnetFramework 4.0", "DotnetFramework 4.5", "DotnetFramework 4.5.1", "DotnetFramework 4.5.2", "DotnetFramework 4.6", "DotnetFramework 4.6.1", "DotnetFramework 4.6.2", "DotnetFramework 4.7", "DotnetFramework 4.7.1", "DotnetFramework 4.7.2", "DotnetFramework 4.8"
DotNetCoreVersion	애플리케이션이 .NET Core 기반인 경우 .NET Core 버전	String	No	".NET Core 1.0", ".NET Core 1.1", ".NET Core 2.0", ".NET Core 2.1", ".NET Core 2.2", ".NET Core 3.0", ".NET Core 3.1"

명칭	설명	형식	필수	유효값
JdkVersion	애플리케이션에서 JDK를 사용하는 경우 JDK 버전	String	No	"JDK1.0", "JDK2.0", "JDK3.0", …, "JDK11.0"
DatabaseType	유형 데이터베이스	String	No	"SQLServer", "Oracle", "Sybase", "Mongo DB", "Maria DB", "Apache Cassandra", "MySQL", "IBM DB2", "PostgreSQLServer"
DatabaseEdition	데이터베이스 버전	String	No	
DatabaseVersion	데이터베이스의 버전	String	No	설명서의 HTML 버전을 참조하세요.

Strategy Recommendations에서 데이터 제거

Migration Hub Strategy Recommendations에서 모든 데이터를 제거하려면 AWS Support에 문의하세요.

Migration Hub Strategy Recommendations의 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 또한는 안전하게 사용할 수 있는 서비스를 제공합니다. 타사 감사자는 규정 AWS 준수 프로그램 일환으로 보안의 효과를 정기적으로 테스트하고 확인합니다. Migration Hub Strategy Recommendations에 적용되는 규정 준수 프로그램에 대한 자세한 내용은 규정 준수 AWS 프로그램 제공 범위 내 서비스규정 준수 .
- 클라우드의 보안 - 사용자의 책임은 사용하는 AWS 서비스에 따라 결정됩니다. 또한 귀하는 귀사의 데이터 민감도, 귀사의 요구 사항, 관련 법률 및 규정을 비롯한 기타 요소에 대해서도 책임이 있습니다.

이 설명서는 Strategy Recommendations 사용 시 책임 분담 모델을 적용하는 방법을 이해하는 데 도움이 됩니다. 다음 항목에서는 보안 및 규정 준수 목표를 충족하도록 Strategy Recommendations를 구성하는 방법을 보여줍니다. 또한 Strategy Recommendations 리소스를 모니터링하고 보호하는 데 도움이 되는 다른 AWS 서비스를 사용하는 방법도 알아봅니다.

주제

- Migration Hub Strategy Recommendations의 데이터 보호
- Migration Hub Strategy Recommendations에 대한 자격 증명 및 액세스 관리
- Migration Hub Strategy Recommendations에 대한 규정 준수 검증

Migration Hub Strategy Recommendations의 데이터 보호

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

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

- 각 계정에 다중 인증(MFA)을 사용하세요.
- SSL/TLS를 사용하여 AWS 리소스와 통신합니다. TLS 1.2는 필수이며 TLS 1.3을 권장합니다.
- 를 사용하여 API 및 사용자 활동 로깅을 설정합니다 AWS CloudTrail. CloudTrail 추적을 사용하여 AWS 활동을 캡처하는 방법에 대한 자세한 내용은 AWS CloudTrail 사용 설명서의 CloudTrail 추적 작업을 참조하세요.
- 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 Strategy Recommendations 또는 기타 AWS 서비스 콘솔, API AWS CLI또는 AWS SDKs를 사용하여 작업하는 경우가 포함됩니다. 이름에 사용되는 태그 또는 자유 형식 텍스트 필드에 입력하는 모든 데이터는 청구 또는 진단 로그에 사용될 수 있습니다. 외부 서버에 URL을 제공할 때 해당 서버에 대한 요청을 검증하기 위해 보안 인증 정보를 URL에 포함시켜서는 안 됩니다.

저장된 데이터 암호화

Strategy Recommendations의 데이터베이스에 저장되는 모든 데이터는 암호화됩니다.

전송 중 암호화

Strategy Recommendations 인터네트워크 통신은 모든 구성 요소와 클라이언트 간의 TLS 1.2 암호화를 지원합니다.

Migration Hub Strategy Recommendations에 대한 자격 증명 및 액세스 관리

AWS Identity and Access Management (IAM)는 관리자가 AWS 리소스에 대한 액세스를 안전하게 제어하는 데 도움이 AWS 서비스 되는 입니다. IAM 관리자는 어떤 사용자가 Strategy Recommendations 리소스를 사용할 수 있는 인증(로그인) 및 승인(권한 있음)을 받을 수 있는지 제어합니다. IAM은 추가 비용 없이 사용할 수 AWS 서비스 있는 입니다.

주제

대상

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

서비스 사용자 - Strategy Recommendations 서비스를 사용하여 작업을 수행하는 경우 필요한 보안 인증과 권한을 관리자가 제공합니다. 더 많은 Strategy Recommendations 기능을 사용하여 작업을 수행하게 되면 추가 권한이 필요할 수 있습니다. 액세스 권한 관리 방법을 이해하면 관리자에게 올바른 권한을 요청하는 데 도움이 됩니다. Strategy Recommendations의 기능에 액세스할 수 없는 경우 Migration Hub Strategy Recommendations 자격 증명 및 액세스 문제 해결 섹션을 참조하세요.

서비스 관리자 - 회사에서 Strategy Recommendations 리소스를 책임지고 있는 경우 Strategy Recommendations에 대한 전체 액세스 권한을 가지고 있을 것입니다. 서비스 관리자는 서비스 사용자

가 액세스해야 하는 Strategy Recommendations 기능과 리소스를 결정합니다. 그런 다음 IAM 관리자에게 요청을 제출하여 서비스 사용자의 권한을 변경해야 합니다. 이 페이지의 정보를 검토하여 IAM의 기본 개념을 이해하세요. 회사가 Strategy Recommendations에서 IAM을 사용하는 방법에 대해 자세히 알아보려면 Migration Hub Strategy Recommendations가 IAM에서 작동하는 방식 섹션을 참조하세요.

IAM 관리자 - IAM 관리자라면 Strategy Recommendations에 대한 액세스 권한 관리 정책 작성 방법을 자세히 알고 싶을 것입니다. IAM에서 사용할 수 있는 Strategy Recommendations ID 기반 정책 예제를 보려면 Migration Hub Strategy Recommendations의 ID 기반 정책 예제 섹션을 참조하세요.

ID를 통한 인증

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

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

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

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

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

AWS 계정 루트 사용자

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

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

페더레이션 자격 증명

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

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

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

IAM 사용자 및 그룹

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

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

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

IAM 역할

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

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

임시 보안 인증이 있는 IAM 역할은 다음과 같은 상황에서 유용합니다.

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

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

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

정책을 사용하여 액세스 관리

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

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

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

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

ID 기반 정책

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

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

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

리소스 기반 정책

리소스 기반 정책은 리소스에 연결하는 JSON 정책 설명서입니다. 리소스 기반 정책의 예제는 IAM 역할 신뢰 정책과 Amazon S3 버킷 정책입니다. 리소스 기반 정책을 지원하는 서비스에서 서비스 관리자는 이러한 정책을 사용하여 특정 리소스에 대한 액세스를 통제할 수 있습니다. 정책이 연결된 리소스의 경우 정책은 지정된 위탁자가 해당 리소스와 어떤 조건에서 어떤 작업을 수행할 수 있는지를 정의합니다. 리소스 기반 정책에서 위탁자를 지정해야 합니다. 보안 주체에는 계정, 사용자, 역할, 페더레이션 사용자 또는이 포함될 수 있습니다 AWS 서비스.

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

액세스 제어 목록(ACL)

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

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

기타 정책 타입

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

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

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

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

여러 정책 유형

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

Migration Hub Strategy Recommendations가 IAM에서 작동하는 방식

IAM을 사용하여 Strategy Recommendations에 대한 액세스를 관리하기 전에 Strategy Recommendations에서 사용할 수 있는 IAM 기능을 알아보세요.

Migration Hub Strategy Recommendations에서 사용할 수 있는 IAM 기능

IAM 기능	Strategy Recommendations 지원
ID 기반 정책	예
리소스 기반 정책	아니요
정책 작업	예
정책 리소스	아니요
정책 조건 키	아니요

IAM 기능	Strategy Recommendations 지원
ACL	아니요
ABAC(정책 내 태그)	아니요
임시 보안 인증	예
보안 주체 권한	예
서비스 역할	아니요
서비스 링크 역할	예

Strategy Recommendations 및 기타 AWS 서비스가 대부분의 IAM 기능과 작동하는 방식을 전체적으로 알아보려면 IAM 사용 설명서의 AWS IAM으로 작업하는 서비스를 참조하세요.

Strategy Recommendations의 ID 기반 정책

ID 기반 정책 지원: 예

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

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

Strategy Recommendations의 ID 기반 정책 예제

Strategy Recommendations ID 기반 정책의 예제를 보려면 Migration Hub Strategy Recommendations의 ID 기반 정책 예제 섹션을 참조하세요.

Strategy Recommendations 내의 리소스 기반 정책

리소스 기반 정책 지원: 아니요

리소스 기반 정책은 리소스에 연결하는 JSON 정책 설명서입니다. 리소스 기반 정책의 예제는 IAM 역할 신뢰 정책과 Amazon S3 버킷 정책입니다. 리소스 기반 정책을 지원하는 서비스에서 서비스 관리자는 이러한 정책을 사용하여 특정 리소스에 대한 액세스를 통제할 수 있습니다. 정책이 연결된 리소스의 경우 정책은 지정된 위탁자가 해당 리소스와 어떤 조건에서 어떤 작업을 수행할 수 있는지를 정의합니다. 리소스 기반 정책에서 위탁자를 지정해야 합니다. 보안 주체에는 계정, 사용자, 역할, 페더레이션 사용자 또는이 포함될 수 있습니다 AWS 서비스.

교차 계정 액세스를 활성화하려는 경우, 전체 계정이나 다른 계정의 IAM 개체를 리소스 기반 정책의 위탁자로 지정할 수 있습니다. 리소스 기반 정책에 크로스 계정 보안 주체를 추가하는 것은 트러스트 관계 설정의 절반밖에 되지 않는다는 것을 유념하세요. 보안 주체와 리소스가 다른 경우 신뢰할 수 AWS 계정있는 계정의 IAM 관리자는 보안 주체 엔터티(사용자 또는 역할)에게 리소스에 액세스할 수 있는 권한도 부여해야 합니다. 엔터티에 ID 기반 정책을 연결하여 권한을 부여합니다. 하지만 리소스 기반 정책이 동일 계정의 위탁자에 액세스를 부여하는 경우, 추가 자격 증명 기반 정책이 필요하지 않습니다. 자세한 내용은 IAM 사용 설명서의 교차 계정 리소스 액세스를 참조하세요.

Strategy Recommendations를 위한 정책 작업

정책 작업 지원: 예

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

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

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

Strategy Recommendations 작업 목록을 보려면 서비스 승인 참조의 Migration Hub Strategy Recommendations 사항에서 정의한 작업을 참조하세요.

Strategy Recommendations의 정책 작업은 작업 앞에 다음 접두사를 사용합니다.

```
migrationhub-strategy
```

단일 문에서 여러 작업을 지정하려면 다음과 같이 쉼표로 구분합니다.

```
"Action": [
```

```
      "migrationhub-strategy:action1",
      "migrationhub-strategy:action2"
         ]
```

Strategy Recommendations ID 기반 정책의 예제를 보려면 Migration Hub Strategy Recommendations의 ID 기반 정책 예제 섹션을 참조하세요.

Strategy Recommendations를 위한 정책 리소스

정책 리소스 지원: 아니요

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

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

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

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

Strategy Recommendations 리소스 유형 및 해당 ARN의 목록을 보려면 서비스 권한 부여 참조의 Migration Hub Strategy Recommendations에서 정의한 리소스를 참조하세요. 각 리소스의 ARN을 지정할 수 있는 작업을 알아보려면 Migration Hub Strategy Recommendations가 정의한 작업을 참조하세요.

Strategy Recommendations ID 기반 정책의 예제를 보려면 Migration Hub Strategy Recommendations의 ID 기반 정책 예제 섹션을 참조하세요.

Strategy Recommendations에 사용되는 정책 조건 키

서비스별 정책 조건 키 지원: 아니요

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

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

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

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

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

Strategy Recommendations 조건 키 목록을 보려면 서비스 승인 참조의 Migration Hub Strategy Recommendations 사항에 사용되는 조건 키를 참조하세요. 조건 키를 사용할 수 있는 작업과 리소스를 알아보려면 Migration Hub Strategy Recommendations가 정의한 작업을 참조하세요.

Strategy Recommendations ID 기반 정책의 예제를 보려면 Migration Hub Strategy Recommendations의 ID 기반 정책 예제 섹션을 참조하세요.

Strategy Recommendations의 액세스 제어 목록(ACL)

ACL 지원: 아니요

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

Strategy Recommendations 사항을 포함한 ABAC(속성 기반 액세스 제어)

ABAC 지원(정책의 태그): 아니요

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

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

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

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

ABAC에 대한 자세한 내용은 IAM 사용 설명서의 ABAC 권한 부여를 통한 권한 정의를 참조하세요. ABAC 설정 단계가 포함된 자습서를 보려면 IAM 사용 설명서의 속성 기반 액세스 제어(ABAC) 사용을 참조하세요.

Strategy Recommendations에서 임시 보안 인증 정보 사용

임시 자격 증명 지원: 예

일부 AWS 서비스 는 임시 자격 증명을 사용하여 로그인할 때 작동하지 않습니다. 임시 자격 증명으로 AWS 서비스 작업하는를 포함한 추가 정보는 AWS 서비스 IAM 사용 설명서의 IAM으로 작업하는 섹션을 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 자격 증명을 자동으로 생성합니다. 역할 전환에 대한 자세한 내용은 IAM 사용 설명서의 사용자에서 IAM 역할로 전환(콘솔)을 참조하세요.

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

Strategy Recommendations의 교차 서비스 보안 주체 권한

전달 액세스 세션(FAS) 지원: 예

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

Strategy Recommendations의 서비스 역할

서비스 역할 지원: 아니요

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

> **Warning**
> 서비스 역할에 대한 권한을 변경하면 Strategy Recommendations 기능이 중단될 수 있습니다. Strategy Recommendations가 관련 지침을 제공하는 경우에만 서비스 역할을 편집하세요.

Strategy Recommendations에 대한 서비스 연결 역할

서비스 링크 역할 지원: 예

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

Strategy Recommendations 서비스 연결 역할을 생성 또는 관리하는 방법에 대한 자세한 내용은 Strategy Recommendations에 대한 서비스 연결 역할 사용 섹션을 참조하세요.

AWS Migration Hub Strategy Recommendations에 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. 서비스는 관리 AWS 형 정책에 새로운 기능을 지원하는 추가 권한을 가끔 추가합니다. 이 유형의 업데이트는 정책이 연결된 모든 ID(사용자, 그룹 및 역할)에 적용됩니다. 서비스는 새 기능이 시작되거나 새 작업을 사용할 수 있게 되면 AWS 관리형 정책을 업데이트할 가능성이 높습니다. 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. 서비스가 새 기능을 시작하면는 새 작업 및 리소스에 대한 읽기 전용 권한을 AWS 추가합니다. 직무 정책의 목록과 설명은 IAM 사용 설명서의 직무에 관한AWS 관리형 정책을 참조하세요.

AWS 관리형 정책: AWSMigrationHubStrategyConsoleFullAccess

`AWSMigrationHubStrategyConsoleFullAccess` 정책을 IAM 보안 인증에 연결할 수 있습니다.

`AWSMigrationHubStrategyConsoleFullAccess` 정책은 사용자에게 AWS Management Console을 통해 Strategy Recommendations 서비스에 대한 전체 액세스 권한을 부여합니다.

권한 세부 정보

이 정책에는 다음 권한이 포함되어 있습니다.

- `discovery` - Application Discovery Service에서 검색 요약을 얻을 수 있는 액세스 권한을 사용자에게 부여합니다.
- `iam` - 전략 권장 사항을 사용하기 위한 요구 사항인 사용자를 위한 서비스 연결 역할을 생성할 수 있습니다.
- `migrationhub-strategy` - 사용자에게 Strategy Recommendations에 대한 전체 액세스 권한을 부여합니다.
- `s3` - Strategy Recommendations에서 사용하는 S3 버킷을 생성하고 읽을 수 있도록 합니다.
- `secretsmanager` - Secrets Manager에서 보안 암호 액세스를 나열할 수 있도록 합니다.

이 정책에 대한 권한을 보려면 AWS 관리형 정책 참조 안내서AWSMigrationHubStrategyConsoleFullAccess의 섹션을 참조하세요.

AWS 관리형 정책: AWSMigrationHubStrategyCollector

`AWSMigrationHubStrategyCollector` 정책을 IAM 보안 인증에 연결할 수 있습니다.

권한 세부 정보

이 정책에는 다음 권한이 포함되어 있습니다.

- `application-transformation` - 애플리케이션 변환 작업에 대한 로그 및 지표 데이터를 업로드하고 이식 호환성 평가 및 권장 사항을 사용할 수 있는 권한을 부여합니다.
- `execute-api` - Amazon API Gateway에 액세스하여 AWS에 로그와 지표를 업로드할 수 있도록 합니다.
- `migrationhub-strategy` - 사용자에게 메시지를 등록하고, 메시지를 보내고, 로그 데이터를 업로드하고, 지표 데이터를 Strategy Recommendations에 업로드할 수 있는 액세스 권한을 부여합니다.
- `s3` - 사용자에게 버킷 및 해당 위치를 나열할 수 있는 액세스 권한을 부여합니다. 또한 사용자에게 Strategy Recommendations에서 사용하는 S3 버킷에 대한 쓰기, 객체 검색, 객체 추가,의 액세스 제어 목록(ACL) 반환, 생성, 액세스, 암호화 구성, `PublicAccessBlock` 구성 수정, 버전 관리 상태 설정, 수명 주기 구성 생성 또는 교체에 대한 액세스 권한이 부여됩니다.
- `secretsmanager` - Strategy Recommendations에서 사용하는 Secrets Manager의 보안 암호에 액세스할 수 있도록 합니다.

이 정책에 대한 권한을 보려면 AWS 관리형 정책 참조 안내서AWSMigrationHubStrategyCollector의 섹션을 참조하세요.

AWS 관리형 정책에 대한 Strategy Recommendations 업데이트

이 서비스가 이러한 변경 사항을 추적하기 시작한 이후 Strategy Recommendations의 AWS 관리형 정책 업데이트에 대한 세부 정보를 봅니다. 이 페이지의 변경 사항에 대한 자동 알림을 받으려면 Strategy Recommendations 문서 기록 페이지에서 RSS 피드를 구독하세요.

변경 사항	설명	날짜
AWSMigrationHubStrategyCollector – 기존 정책 업데이트	이 정책은 애플리케이션 `GetPortingRecommendationAssessment` 변환 서비스가 로그`StartPortingRecommendationAssessment` 와 지표를 서비스에 전송할 수 있도록 `PutLogData` , `StartPortingCompatibilityAs`	2024년 4월 1일

변경 사항	설명	날짜
	`sessment GetPortingCompatibilityAssessment` , 및 애플리케이션 변환 작업을 포함하도록 업데이트되었습니다. 로그 및 지표 업로드를 지원하기 위해 Amazon Simple Storage Service(Amazon S3)에 `ListBucket` 및가 `GetBucketLocation` 추가되었습니다. Strategy Recommendations 수집기가 로그와 지표를 서비스의 엔드포인트로 전송할 수 있도록 `PutLogData` 및 `PutMetricData` 도 추가되었습니다.	
AWSMigrationHubStrategyCollector – 기존 정책 업데이트	이 정책은 `PutMetricData` 및 `PutLogData` 작업으로 업데이트됩니다. 이러한 작업은 애플리케이션 변환 작업에 대한 로그 및 지표 데이터를 업로드하는 권한을 부여합니다. 또한이 업데이트에는 `aws:ResourceAccount` 가 포함된 Amazon Simple Storage Service 및 AWS Secrets Manager 작업을 사용할 수 있는 권한에 `aws:PrincipalAccount` 대한와 동일한지 확인하는 조건이 추가됩니다.	2024년 2월 5일

변경 사항	설명	날짜
AWSMigrationHubStrategyCollector – 기존 정책 업데이트	이 정책은 Amazon S3 API `CreateBucket` , `PutEncryptionConfiguration` , `PutBucketPublicAccessBlock` , `PutBucketPolicy` , `PutBucketVersioning` 및 `PutLifecycleConfiguration` 으로 업데이트됩니다.	2023년 9월 15일
AWSMigrationHubStrategyCollector – 기존 정책 업데이트	이 정책 업데이트는 소스 코드를 분석할 수 있는 권한을 부여합니다.	2023년 3월 8일
AWSMigrationHubStrategyConsoleFullAccess – 기존 정책 업데이트	이 정책은 `DescribeConfigurations` , 및 `DescribeTags` 의 세 가지 AWS Application Discovery Service APIs로 업데이트됩니다`ListConfigurations` .	2022년 11월 10일
AWSMigrationHubStrategyCollector – 기존 정책 업데이트	이 정책은 `UpdateCollectorConfiguration` 작업으로 업데이트됩니다. 이 작업은 쉽게 검색할 수 있도록 수집기 구성을 저장합니다.	2022년 9월 7일
AWSMigrationHubStrategyConsoleFullAccess – 출시 시 사용 가능한 새 정책	`AWSMigrationHubStrategyConsoleFullAccess` 는 AWS Management Console을 통해 사용자에게 Strategy Recommendations 서비스에 대한 전체 액세스 권한을 부여합니다.	2021년 10월 25일

변경 사항	설명	날짜
AWSMigrationHubStrategyCollector – 출시 시 사용 가능한 새 정책	`AWSMigrationHubStrategyCollector` 는 사용자에게 Strategy Recommendations 서비스에 대한 액세스 권한과 서비스와 관련된 S3 버킷에 대한 읽기/쓰기 액세스 권한을 부여합니다. 또한 Amazon API Gateway에 로그 및 지표를 업로드할 수 있는 액세스 권한 AWS과 AWS Secrets Manager에 보안 인증을 가져올 수 있는 액세스 권한을 부여합니다.	2021년 10월 25일
AWSMigrationHubStrategyServiceRolePolicy – 출시 시 사용 가능한 새 정책	`AWSMigrationHubStrategyServiceRolePolicy` 서비스 연결 역할 정책은 AWS Migration Hub 및에 대한 액세스를 제공합니다 AWS Application Discovery Service. 이 정책에서는 Amazon Simple Storage Service(S3)에 보고서를 저장할 수 있는 권한도 부여합니다.	2021년 10월 25일
Strategy Recommendations에서 변경 사항 추적 시작	Strategy Recommendations는 AWS 관리형 정책에 대한 변경 사항을 추적하기 시작했습니다.	2021년 10월 25일

Migration Hub Strategy Recommendations의 ID 기반 정책 예제

기본적으로 사용자 및 역할은 Strategy Recommendations 리소스를 생성하거나 수정할 수 있는 권한이 없습니다. 또한 AWS Management Console, AWS Command Line Interface (AWS CLI) 또는 AWS

API를 사용하여 작업을 수행할 수 없습니다. 사용자에게 사용자가 필요한 리소스에서 작업을 수행할 권한을 부여하려면 IAM 관리자가 IAM 정책을 생성하면 됩니다. 그런 다음 관리자가 IAM 정책을 역할에 추가하고, 사용자가 역할을 맡을 수 있습니다.

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

각 리소스 유형에 대한 ARN 형식을 비롯하여 Strategy Recommendations에서 정의되는 작업 및 리소스 유형에 대한 자세한 내용은 서비스 승인 참조의 Migration Hub Strategy Recommendations에 사용되는 작업, 리소스 및 조건 키를 참조하세요.

주제

- 정책 모범 사례
- Strategy Recommendations 콘솔 사용
- 사용자가 자신의 고유한 권한을 볼 수 있도록 허용
- 하나의 Amazon S3 버킷에 액세스

정책 모범 사례

ID 기반 정책에 따라 계정에서 사용자가 Strategy Recommendations 리소스를 생성, 액세스 또는 삭제할 수 있는지 여부가 결정됩니다. 이 작업으로 인해 AWS 계정에 비용이 발생할 수 있습니다. ID 기반 정책을 생성하거나 편집할 때는 다음 지침과 권장 사항을 따릅니다.

- AWS 관리형 정책을 시작하고 최소 권한으로 전환 - 사용자 및 워크로드에 권한 부여를 시작하려면 많은 일반적인 사용 사례에 대한 권한을 부여하는 AWS 관리형 정책을 사용합니다. 에서 사용할 수 있습니다 AWS 계정. 사용 사례에 맞는 AWS 고객 관리형 정책을 정의하여 권한을 추가로 줄이는 것이 좋습니다. 자세한 정보는 IAM 사용 설명서의 AWS 관리형 정책 또는 AWS 직무에 대한 관리형 정책을 참조하세요.
- 최소 권한 적용 – IAM 정책을 사용하여 권한을 설정하는 경우, 작업을 수행하는 데 필요한 권한만 부여합니다. 이렇게 하려면 최소 권한으로 알려진 특정 조건에서 특정 리소스에 대해 수행할 수 있는 작업을 정의합니다. IAM을 사용하여 권한을 적용하는 방법에 대한 자세한 정보는 IAM 사용 설명서에 있는 IAM의 정책 및 권한을 참조하세요.
- IAM 정책의 조건을 사용하여 액세스 추가 제한 – 정책에 조건을 추가하여 작업 및 리소스에 대한 액세스를 제한할 수 있습니다. 예를 들어, SSL을 사용하여 모든 요청을 전송해야 한다고 지정하는 정책 조건을 작성할 수 있습니다. AWS 서비스와 같은 특정를 통해 사용되는 경우 조건을 사용하여 서비스 작업에 대한 액세스 권한을 부여할 수도 있습니다 AWS CloudFormation. 자세한 정보는 IAM 사용 설명서의 IAM JSON 정책 요소: 조건을 참조하세요.

- IAM Access Analyzer를 통해 IAM 정책을 확인하여 안전하고 기능적인 권한 보장 - IAM Access Analyzer에서는 IAM 정책 언어(JSON)와 모범 사례가 정책에서 준수되도록 새로운 및 기존 정책을 확인합니다. IAM Access Analyzer는 100개 이상의 정책 확인 항목과 실행 가능한 추천을 제공하여 안전하고 기능적인 정책을 작성하도록 돕습니다. 자세한 내용은 IAM 사용 설명서의 IAM Access Analyzer에서 정책 검증을 참조하세요.
- 다중 인증(MFA) 필요 -에서 IAM 사용자 또는 루트 사용자가 필요한 시나리오가 있는 경우 추가 보안을 위해 MFA를 AWS 계정합니다. API 작업을 직접 호출할 때 MFA가 필요하면 정책에 MFA 조건을 추가합니다. 자세한 내용은 IAM 사용 설명서의 MFA를 통한 보안 API 액세스를 참조하세요.

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

Strategy Recommendations 콘솔 사용

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

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

사용자와 역할이 Strategy Recommendations 콘솔을 계속 사용할 수 있도록 하려면 Strategy Recommendations `ConsoleAccess` 또는 `ReadOnly` AWS 관리형 정책도 엔터티에 연결합니다. 자세한 내용은 IAM 사용 설명서의 사용자에게 권한 추가를 참조하세요.

사용자가 자신의 고유한 권한을 볼 수 있도록 허용

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

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "ViewOwnUserInfo",
            "Effect": "Allow",
            "Action": [
                "iam:GetUserPolicy",
```

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

하나의 Amazon S3 버킷에 액세스

이 예제에서는의 IAM 사용자에게 Amazon S3 버킷 중 하나인에 대한 AWS 계정 액세스 권한을 부여하려고 합니다`amzn-s3-demo-bucket`. 또한 사용자가 객체를 추가, 업데이트 및 삭제하도록 허용하려고 합니다.

이 정책에서는 `s3:PutObject`, `s3:GetObject` 및 `s3:DeleteObject` 권한을 사용자에게 부여할 뿐만 아니라 `s3:ListAllMyBuckets`, `s3:GetBucketLocation` 및 `s3:ListBucket` 권한도 부여합니다. 이러한 권한은 콘솔에 필요한 추가 권한입니다. 또한 콘솔에서 객체를 복사, 자르기 및 붙여넣기를 할 수 있으려면 `s3:PutObjectAcl` 및 `s3:GetObjectAcl` 작업이 필요합니다. 사용자에게 권한을 부여하고 콘솔을 사용하여 권한을 테스트하는 예제 연습은 예제 연습: 사용자 정책을 사용하여 버킷에 대한 액세스 제어를 참조하세요.

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

```
            "Sid":"ListBucketsInConsole",
            "Effect":"Allow",
            "Action":[
               "s3:ListAllMyBuckets"
            ],
            "Resource":"arn:aws:s3:::*"
         },
         {
            "Sid":"ViewSpecificBucketInfo",
            "Effect":"Allow",
            "Action":[
               "s3:ListBucket",
               "s3:GetBucketLocation"
            ],
            "Resource":"arn:aws:s3:::amzn-s3-demo-bucket"
         },
         {
            "Sid":"ManageBucketContents",
            "Effect":"Allow",
            "Action":[
               "s3:PutObject",
               "s3:PutObjectAcl",
               "s3:GetObject",
               "s3:GetObjectAcl",
               "s3:DeleteObject"
            ],
            "Resource":"arn:aws:s3:::amzn-s3-demo-bucket/*"
         }
      ]
   }
```

Migration Hub Strategy Recommendations 자격 증명 및 액세스 문제 해결

다음 정보를 사용하여 Strategy Recommendations와 IAM에서 작업할 때 발생할 수 있는 공통적인 문제를 진단하고 수정할 수 있습니다.

주제

- Strategy Recommendations에서 작업을 수행할 권한이 없음
- iam:PassRole을 수행하도록 인증되지 않음

- 액세스 키를 보아야 합니다.
- 관리자인데, 다른 사용자가 Strategy Recommendations에 액세스하도록 허용하기를 원함
- 내 외부의 사람이 내 Strategy Recommendations 리소스에 액세스 AWS 계정 하도록 허용하고 싶습니다.

Strategy Recommendations에서 작업을 수행할 권한이 없음

에서 작업을 수행할 권한이 없다는 AWS Management Console 메시지가 표시되면 관리자에게 문의하여 도움을 받아야 합니다. 관리자는 사용자 이름과 비밀번호를 제공한 사람입니다.

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

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

이 경우, Mateo는 *`my-example-widget`* 작업을 사용하여 `migrationhub-strategy:`*`GetWidget`* 리소스에 액세스하도록 허용하는 정책을 업데이트하라고 관리자에게 요청합니다.

iam:PassRole을 수행하도록 인증되지 않음

`iam:PassRole` 작업을 수행할 수 있는 권한이 없다는 오류가 수신되면 Strategy Recommendations에 역할을 전달할 수 있도록 정책을 업데이트해야 합니다.

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

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

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

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

도움이 필요한 경우 AWS 관리자에게 문의하세요. 관리자는 로그인 보안 인증 정보를 제공한 사람입니다.

액세스 키를 보아야 합니다.

IAM 사용자 액세스 키를 생성한 후에는 언제든지 액세스 키 ID를 볼 수 있습니다. 하지만 보안 액세스 키는 다시 볼 수 없습니다. 보안 액세스 키를 잃어버린 경우 새로운 액세스 키 페어를 생성해야 합니다.

액세스 키는 액세스 키 ID(예: `AKIAIOSFODNN7EXAMPLE`)와 보안 액세스 키(예: `wJalrXUtnFEMI/K7MDENG/bPxRfiCYEXAMPLEKEY`)의 두 가지 부분으로 구성됩니다. 사용자 이름 및 암호와 같이 액세스 키 ID와 보안 액세스 키를 함께 사용하여 요청을 인증해야 합니다. 사용자 이름과 암호를 관리하는 것처럼 안전하게 액세스 키를 관리합니다.

> **Important**
>
> 정식 사용자 ID를 찾는 데 도움이 되더라도 액세스 키를 타사에 제공하지 마시기 바랍니다. 이렇게 하면 누군가에게에 대한 영구 액세스 권한을 부여할 수 있습니다 AWS 계정.

액세스 키 페어를 생성할 때는 액세스 키 ID와 보안 액세스 키를 안전한 위치에 저장하라는 메시지가 나타납니다. 보안 액세스 키는 생성할 때만 사용할 수 있습니다. 하지만 보안 액세스 키를 잃어버린 경우 새로운 액세스 키를 IAM 사용자에게 추가해야 합니다. 최대 두 개의 액세스 키를 가질 수 있습니다. 이미 두 개가 있는 경우 새로 생성하려면 먼저 키 페어 하나를 삭제해야 합니다. 지침을 보려면 IAM 사용 설명서의 액세스 키 관리를 참조하십시오.

관리자인데, 다른 사용자가 Strategy Recommendations에 액세스하도록 허용하기를 원함

다른 사용자가 Strategy Recommendations에 액세스하도록 허용하려면 액세스 권한이 필요한 사용자 또는 애플리케이션에 권한을 부여해야 합니다. AWS IAM Identity Center 를 사용하여 사용자 및 애플리케이션을 관리하는 경우 사용자 또는 그룹에 권한 세트를 할당하여 액세스 수준을 정의합니다. 권한 세트는 IAM 정책을 자동으로 생성하고 사용자 또는 애플리케이션과 연결된 IAM 역할에 할당합니다. 자세한 내용은 AWS IAM Identity Center 사용 설명서에서 권한 세트를 참조하세요.

IAM Identity Center를 사용하지 않는 경우 액세스가 필요한 사용자 또는 애플리케이션에 대한 IAM 엔터티(사용자 또는 역할)를 생성해야 합니다. 그런 다음 Strategy Recommendations에서 올바른 권한을 부여하는 정책을 엔터티에 연결해야 합니다. 권한이 부여되면 사용자 또는 애플리케이션 개발자에게 자격 증명을 제공합니다. 이들은 이 자격 증명을 사용하여 AWS에 액세스합니다. IAM 사용자, 그룹, 정책, 권한 생성에 대한 자세한 내용은 IAM 사용 설명서의 IAM ID 및 IAM 정책과 권한을 참조하세요.

내 외부의 사람이 내 Strategy Recommendations 리소스에 액세스 AWS 계정 하도록 허용하고 싶습니다.

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

자세히 알아보려면 다음을 참조하세요.

- Strategy Recommendations에서 이러한 기능을 지원하는지 여부를 알아보려면 Migration Hub Strategy Recommendations가 IAM에서 작동하는 방식 섹션을 참조하세요.
- 소유 AWS 계정 한의 리소스에 대한 액세스 권한을 제공하는 방법을 알아보려면 IAM 사용 설명서의 소유한 다른의 IAM 사용자에게 액세스 권한 제공을 참조 AWS 계정 하세요.
- 타사에 리소스에 대한 액세스 권한을 제공하는 방법을 알아보려면 IAM 사용 설명서의 타사가 AWS 계정 소유한에 대한 액세스 권한 제공을 AWS 계정참조하세요.
- ID 페더레이션을 통해 액세스 권한을 제공하는 방법을 알아보려면 IAM 사용 설명서의 외부에서 인증된 사용자에게 액세스 권한 제공(ID 페더레이션)을 참조하세요.
- 크로스 계정 액세스에 대한 역할과 리소스 기반 정책 사용의 차이점을 알아보려면 IAM 사용 설명서의 IAM의 크로스 계정 리소스 액세스를 참조하세요.

Strategy Recommendations에 대한 서비스 연결 역할 사용

Migration Hub Strategy Recommendations는 AWS Identity and Access Management (IAM) 서비스 연결 역할을 사용합니다. 서비스 연결 역할은 Strategy Recommendations에 직접 연결된 고유한 유형의 IAM 역할입니다. 서비스 연결 역할은 Strategy Recommendations에서 사전 정의하며 서비스에서 사용자를 대신하여 다른 AWS 서비스를 호출하는 데 필요한 모든 권한을 포함합니다.

서비스 연결 역할을 사용하면 필요한 권한을 수동으로 추가할 필요가 없으므로 Strategy Recommendations를 더 쉽게 설정할 수 있습니다. Strategy Recommendations에서 서비스 연결 역할의 권한을 정의하므로 다르게 정의되지 않은 한, Strategy Recommendations만 해당 역할을 수임할 수 있습니다. 정의된 권한에는 신뢰 정책과 권한 정책이 포함되며 이 권한 정책은 다른 IAM 엔티티에 연결할 수 없습니다.

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

Strategy Recommendations에 대한 서비스 연결 역할 권한

Strategy Recommendations는 AWSServiceRoleForMigrationHubStrategy라는 서비스 연결 역할을 사용하고 이를 AWSMigrationHubStrategyServiceRolePolicy IAM 정책 - AWS Migration Hub 및에 대한 액세스를 제공합니다 AWS Application Discovery Service. 이 정책에서는 Amazon Simple Storage Service(S3)에 보고서를 저장할 수 있는 권한도 부여합니다.

AWSServiceRoleForMigrationHubStrategy 서비스 연결 역할은 역할을 수임하기 위해 다음 서비스를 신뢰합니다.

- `migrationhub-strategy.amazonaws.com`

역할 권한 정책을 통해 Strategy Recommendations는 다음 작업을 완료할 수 있습니다.

AWS Application Discovery Service 작업

```
discovery:ListConfigurations

discovery:DescribeConfigurations
```

AWS Migration Hub 작업

```
mgh:GetHomeRegion
```

Amazon S3 작업

```
s3:GetBucketAcl

s3:GetBucketLocation

s3:GetObject

s3:ListAllMyBuckets

s3:ListBucket

s3:PutObject

s3:PutObjectAcl
```

이 정책에 대한 권한을 보려면 AWS 관리형 정책 참조 안내서AWSMigrationHubStrategyServiceRolePolicy의 섹션을 참조하세요.

이 정책의 업데이트 기록을 보려면 AWS 관리형 정책에 대한 Strategy Recommendations 업데이트을 참조하세요.

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

Strategy Recommendations에 대한 서비스 연결 역할 생성

서비스 링크 역할은 수동으로 생성할 필요가 없습니다. Migration Hub가의 계정에 서비스 연결 역할(SLR)을 생성하도록 허용하는 데 동의하면 AWS Management Console Strategy Recommendations가 서비스 연결 역할을 생성합니다.

이 서비스 연결 역할을 삭제했다가 다시 생성해야 하는 경우 동일한 프로세스를 사용하여 계정에서 역할을 다시 생성할 수 있습니다. Migration Hub가 계정에 서비스 연결 역할(SLR)을 생성하도록 허용하는 데 동의하면 Strategy Recommendations가 서비스 연결 역할을 다시 생성합니다.

Strategy Recommendations에 대한 서비스 연결 역할 편집

Strategy Recommendations는 AWSServiceRoleForMigrationHubStrategy 서비스 연결 역할을 편집하도록 허용하지 않습니다. 서비스 링크 역할을 생성한 후에는 다양한 개체가 역할을 참조할 수 있기 때문에 역할 이름을 변경할 수 없습니다. 단, Strategy Recommendations 콘솔, CLI 또는 API를 사용하여 역할에 대한 설명을 편집할 수 있습니다.

Strategy Recommendations에 대한 서비스 연결 역할 삭제

IAM을 사용하여 수동으로 서비스 연결 역할을 삭제하려면 다음을 수행하세요.

IAM 콘솔 AWS CLI, 또는 AWS API를 사용하여 AWSServiceRoleForMigrationHubStrategy 서비스 연결 역할을 삭제합니다. 자세한 내용은 IAM 사용 설명서의 서비스 연결 역할 삭제 섹션을 참조하십시오.

AWSServiceRoleForMigrationHubStrategy SLR에서 사용하는 Strategy Recommendations 리소스를 삭제할 때는 실행 중인 평가(권장 사항 생성 작업)가 없어야 합니다. 백그라운드 평가도 실행할 수 없습니다. 평가가 실행 중인 경우 IAM 콘솔에서 SLR 삭제가 실패합니다. SLR 삭제가 실패할 경우 모든 백그라운드 작업이 완료된 후 삭제를 재시도할 수 있습니다. SLR을 삭제하기 전에 생성된 리소스를 정리할 필요는 없습니다.

Strategy Recommendations 서비스 연결 역할이 지원되는 리전

Strategy Recommendations에서는 서비스를 사용할 수 있는 모든 리전에서 서비스 연결 역할 사용을 지원합니다. 자세한 내용은 AWS 리전 및 엔드포인트 섹션을 참조하십시오.

Migration Hub Strategy Recommendations 및 인터페이스 VPC 엔드포인트 (AWS PrivateLink)

인터페이스 VPC 엔드포인트를 생성하여 VPC와 Migration Hub Strategy Recommendations 간에 프라이빗 연결을 설정할 수 있습니다. 인터페이스 엔드포인트는 로 구동됩니다 AWS PrivateLink를 사용하면 인터넷 게이트웨이 AWS PrivateLink, NAT 디바이스, VPN 연결 또는 AWS Direct Connect 연결 없이 Strategy Recommendations API 작업에 비공개로 액세스할 수 있습니다. VPC의 인스턴스는 Strategy Recommendations API와 통신하는 데 퍼블릭 IP 주소를 필요로 하지 않습니다. VPC와 Strategy Recommendations 간의 트래픽은 Amazon 네트워크 내에서 벗어나지 않습니다.

각 인터페이스 엔드포인트는 서브넷에서 하나 이상의 탄력적 네트워크 인터페이스로 표현됩니다.

자세한 내용은 Amazon VPC 사용 설명서의 인터페이스 VPC 엔드포인트(AWS PrivateLink)를 참조하세요.

Strategy Recommendations VPC 엔드포인트 고려 사항

Strategy Recommendations에 대한 인터페이스 VPC 엔드포인트를 설정하기 전에 Amazon VPC 사용 설명서에서 인터페이스 엔드포인트 속성 및 제한 사항과 AWS PrivateLink 할당량을 검토해야 합니다.

Strategy Recommendations는 VPC에서 모든 API 작업에 대한 호출 수행을 지원합니다. Strategy Recommendations를 모두 사용하려면 VPC 엔드포인트를 생성해야 합니다.

Strategy Recommendations에 대한 인터페이스 VPC 엔드포인트 생성

Amazon VPC 콘솔 또는 AWS Command Line Interface (AWS CLI)을 사용하여 Strategy Recommendations에 대한 VPC 엔드포인트를 생성할 수 있습니다. 자세한 내용은 Amazon VPC 사용 설명서의 인터페이스 엔드포인트 생성을 참조하세요.

다음 서비스 이름을 사용하여 Strategy Recommendations용 VPC 엔드포인트를 생성합니다.

- `com.amazonaws.region.migrationhub-strategy`

엔드포인트에 프라이빗 DNS를 사용하는 경우, 리전에 대한 기본 DNS 이름을 사용하여 Strategy Recommendations에 대한 API 요청을 수행할 수 있습니다. 예를 들어 이름 `migrationhub-strategy.us-east-1.amazonaws.com`을 사용할 수 있습니다.

자세한 내용은 Amazon VPC 사용 설명서의 인터페이스 엔드포인트를 통해 서비스 액세스를 참조하세요.

Strategy Recommendations에 대한 VPC 엔드포인트 정책 생성

Strategy Recommendations에 대한 액세스를 제어하는 VPC 엔드포인트에 엔드포인트 정책을 연결할 수 있습니다. 이 정책은 다음 정보를 지정합니다.

- 작업을 수행할 수 있는 위탁자.
- 수행할 수 있는 작업.
- 이러한 작업을 수행할 수 있는 리소스입니다.

자세한 정보는 Amazon VPC 사용 설명서의 VPC 엔드포인트를 통해 서비스에 대한 액세스 제어를 참조하세요.

예제: Strategy Recommendations 작업에 대한 VPC 엔드포인트 정책

다음은 Strategy Recommendations에 대한 엔드포인트 정책의 예입니다. 이 정책은 엔드포인트에 연결될 때 모든 리소스의 모든 보안 주체에 대한 액세스 권한을 나열된 Strategy Recommendations 작업에 부여합니다.

```
{
   "Statement":[
      {
         "Principal":"*",
         "Effect":"Allow",
         "Action":[
            "migrationhub-strategy:ListContacts",
         ],
         "Resource":"*"
      }
   ]
}
```

Migration Hub Strategy Recommendations에 대한 규정 준수 검증

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 참조하세요.

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 규정 준수 및 거버넌스 - 이러한 솔루션 구현 가이드에서는 아키텍처 고려 사항을 설명하고 보안 및 규정 준수 기능을 배포하는 단계를 제공합니다.
- HIPAA 적격 서비스 참조 - HIPAA 적격 서비스가 나열되어 있습니다. 모든가 HIPAA에 적합한 AWS 서비스 것은 아닙니다.
- 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), 결제카드 산업 보안 표준 위원회(PCI), 국제표준화기구(ISO))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.

다른 서비스와 함께 사용

이 섹션에서는 Migration Hub Strategy Recommendations와 상호 작용하는 다른 AWS 서비스에 대해 설명합니다.

주제

를 사용하여 Strategy Recommendations API 호출 로깅 AWS CloudTrail

Migration Hub Strategy Recommendations는 Strategy Recommendations에서 사용자, 역할 또는 AWS CloudTrail서비스가 수행한 작업에 대한 레코드를 제공하는 AWS 서비스와 통합됩니다. CloudTrail은 Strategy Recommendations에 대한 API 호출을 이벤트로 캡처합니다. 캡처되는 호출에는 Strategy Recommendations 콘솔로부터의 호출과 Strategy Recommendations API 작업에 대한 코드 호출이 포함됩니다.

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

CloudTrail에 대한 자세한 내용은 AWS CloudTrail 사용 설명서를 참조하세요.

CloudTrail의 Strategy Recommendations 정보

CloudTrail은 계정을 생성할 AWS 계정 때에서 활성화됩니다. Strategy Recommendations에서 활동이 발생하면 해당 활동은 이벤트 기록의 다른 AWS 서비스 이벤트와 함께 CloudTrail 이벤트에 기록됩니다. AWS 계정에서 최신 이벤트를 확인, 검색 및 다운로드할 수 있습니다. 자세한 내용은 CloudTrail 이벤트 기록을 사용하여 이벤트 보기를 참조하세요.

Strategy Recommendations에 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. 추가

적으로, CloudTrail 로그에서 수집된 이벤트 데이터를 추가 분석 및 처리하도록 다른 AWS 서비스를 구성할 수 있습니다. 자세한 내용은 다음 자료를 참조하세요.

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

Strategy Recommendations는 CloudTrail 로그 파일에 다음 작업을 이벤트로 로깅합니다.

- GetApplicationComponentStrategies
- GetApplicationComponentDetails
- GetAssesment
- GetImportFileTask
- GetPortfolioPreferences
- GetPortfolioSummary
- GetServerDetails
- GetServerStrategies
- ListApplicationComponents
- ListCollectors
- ListImportFileTask
- ListServers
- PutPortfolioPreferences
- StartAssessment
- StartImportFileTask
- StopAssessment
- UpdateApplicationComponetConfig
- UpdateServerConfig

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

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

자세한 내용은 CloudTrail userIdentity 요소를 참조하세요.

Strategy Recommendations 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 호출의 주문 스택 트레이스가 아니므로 특정 순서로 표시되지 않습니다.

다음은 GetServerDetails 작업을 보여주는 CloudTrail 로그 항목이 나타낸 예제입니다.


```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "AssumedRole",
        "principalId": "777777777777",
        "arn": "arn:aws:sts::111122223333:assumed-role/myUserName/...",
        "accountId": "111122223333",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "sessionContext": {
            "sessionIssuer": {
                "type": "Role",
                "principalId": "777777777777",
                "arn": "arn:aws:iam::111122223333:role/myUserName",
                "accountId": "111122223333",
                "userName": "myUserName"
            },
            "webIdFederationData": {},
            "attributes": {
                "creationDate": "2021-09-20T01:07:16Z",
                "mfaAuthenticated": "false"
            }
        }
    },
    "eventTime": "2021-09-20T01:07:43Z",
```

```
    "eventSource": "migrationhub-strategy.amazonaws.com",
    "eventName": "GetServerDetails",
    "awsRegion": "us-west-2",
    "sourceIPAddress": "",
    "userAgent": "",
    "requestParameters": {
        "serverId": "ads-server-006"
    },
    "responseElements": null,
    "requestID": "07D681279BD94AED",
    "eventID": "cdc4b7ed-e171-4cef-975a-ad829d4123e8",
    "readOnly": true,
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "111122223333",
    "eventCategory": "Management"
}
```

Migration Hub Strategy Recommendations 할당량

AWS 계정에는 각 AWS 서비스에 대해 이전에 제한이라고 하는 기본 할당량이 있습니다. 다르게 표시되지 않는 한 리전별로 각 할당량이 적용됩니다. 일부 할당량에 대한 증가를 요청할 수 있으며 다른 할당량은 늘릴 수 없습니다.

Migration Hub Strategy Recommendations의 할당량 목록을 보려면 Strategy Recommendations service quotas를 참조하세요.

Service Quotas 콘솔을 열어 Strategy Recommendations의 할당량을 볼 수도 있습니다. 탐색 창에서 AWS 서비스를 선택하고 Migration Hub Strategy Recommendations를 선택합니다.

할당량 증가를 요청하려면 Service Quotas 사용 설명서의 할당량 증가 요청을 참조하십시오. Service Quotas에서 아직 할당량을 사용할 수 없는 경우 한도 증가 양식을 사용합니다.

릴리스 정보

주제

2023년 11월 17일

새로운 기능

- 수집기 v1.1.47
- .NET 8 애플리케이션을 지원합니다.

2023년 10월 12일

새로운 기능

- 수집기 v1.1.45

- 다중 데이터 소스 지원.

2023년 4월 17일

새로운 기능

- Collector v1.1.22
- 업그레이드 스크립트 향상. 이를 위해서는 최신 버전의 수집기가 필요합니다.

2023년 3월 17일

새 기능

소스 코드 없이도 안티패턴 및 비호환성 탐지를 제공하는 바이너리 분석이 추가되었습니다.

2022년 11월 7일

새 기능

- 애플리케이션을 위한 애플리케이션 필터링
- AWS Application Discovery Service 태그별 서버 필터링

2022년 9월 27일

새 기능

- Collector v1.1.12
  - SCT 버전 667
  - EMPAnalyzer 2.2.0.368
- 서버 인사이트에 대한 `diag check` 명령이 추가되었습니다.
- 잠재적 권장 사항에 대한 지원이 추가되었습니다.
- 구성 및 평가 상태 확인을 위한 사용자 인터페이스가 향상되었습니다.

버그 수정

- Porting Assistant 변환기 및 기타 수정 사항.

2022년 6월 30일

새 기능

- Collector v1.1.11
  - VMware API 지원이 추가되었습니다.
  - A2C에서 바이너리 파일을 다운로드하는 동안 사용자 헤더를 추가하도록 변경을 요청했습니다.
  - Linux 홈 경로, 기본 쉘 및 모든 쉘의 원격 종료가 추가되었습니다.
- A2C v1.17 퍼블릭 바이너리
  - Azure DevOps에 대한 지원이 파이프라인 배포 대상으로 추가되었습니다.

2022년 4월 18일

새 기능

- Collector v1.1.7
- 퍼블릭 URL에서 A2C 바이너리를 동적으로 다운로드하는 기능이 추가되었습니다.

버그 수정

- A2C v1.1.5

2022년 2월 25일

버그 수정

- SCT v5.6.9
- A2C v1.1.2
- Collector v1.1.4

2022년 2월 10일

버그 수정

- SCT v5.6.8

- A2C v1.1.1
  - Linux에서 tar 명령에 대한 검사가 추가되었습니다.
  - Amazon ECR에서 애플리케이션 이미지를 확인하는 문제가 수정되었습니다.
  - 사전 검증을 위해 컨테이너를 제거해야 하는 문제가 수정되었습니다.
- Collector v1.1.3
  - 원격 32비트 시스템의 4xx 오류가 수정되었습니다.
  - A2C 오류 코드가 업데이트되었습니다.
  - 원격 시스템의 소스 코드 분석을 위해 C#에서 IP 주소가 검증되었습니다.

2022년 1월 28일

새 기능

- Collector v1.1.2
- 소스 코드 분석을 위한 Azure DevOps Git 리포지토리 지원이 추가되었습니다.

2022년 1월 14일

새 기능

- Collector v1.1.1
- SQL 데이터베이스에 대한 Babelfish 권장 사항이 추가되었습니다.

2021년 12월 21일

해결된 문제

- Collector v1.1.0
- 데이터베이스 분석이 복원되었습니다.

2021년 12월 15일

알려진 문제

- Collector v1.0.4
- 데이터베이스 분석은 현재 지원되지 않습니다(CVE-2021-44228).

2021년 10월 25일

새 기능

- Collector v1.0.0
- Migration Hub Strategy Recommendations 사용 설명서의 첫 번째 릴리스입니다.

문서 및 버전 기록

다음 표에서는 Strategy Recommendations에 대한 문서 릴리스를 소개합니다. 자세한 내용은 릴리스 정보 단원을 참조하십시오.

변경 사항	설명	날짜
AWS 관리형 정책 업데이트 - AWSMigrationHubStrategyCollector로 업데이트	새 `s3`, `application-transformation` 및 `migrationhub-strategy` 작업을 포함하도록 AWSMigrationHubStrategyCollector 정책을 업데이트했습니다.	2024년 4월 1일
AWS 관리형 정책 업데이트 - AWSMigrationHubStrategyCollector로 업데이트	새 `application-transformation` 작업을 포함하도록 AWSMigrationHubStrategyCollector 정책을 업데이트했습니다. 또한이 업데이트는가와 같아`aws:ResourceAccount` 야 하는 다양한 작업을 제한하는 조건을 추가합니다`aws:PrincipalAccount` .	2024년 2월 5일
새 기능	Strategy Recommendations 애플리케이션 데이터 수집기 클라이언트 v1.1.47는 .NET 8 애플리케이션을 지원하는에서 사용할 수 있습니다.	2023년 11월 17일
새 기능	Strategy Recommendations 애플리케이션 데이터 수집기 클라이언트 v1.1.45은 여러 데이	2023년 10월 12일

	터 소스를 지원하는에서 사용할 수 있습니다.	
AWS 관리형 정책 업데이트 - AWSMigrationHubStrategyCollector로 업데이트	새 Amazon S3 API를 포함하도록 AWSMigrationHubStrategyCollector 정책을 업데이트했습니다. APIs	2023년 9월 15일
AWS 관리형 정책 업데이트 - AWSMigrationHubStrategyCollector로 업데이트	소스 코드에 대한 새 분석기를 포함하도록 AWSMigrationHubStrategyCollector 정책을 업데이트했습니다.	2023년 3월 8일
IAM 모범 사례 업데이트	자세한 내용은 IAM의 보안 모범 사례를 참조하세요.	2023년 2월 25일
AWS 관리형 정책 업데이트 - 기존 정책으로 업데이트	Migration Hub Strategy Recommendations는 기존 정책에 3개의 AWS Application Discovery Service APIs 추가했습니다.	2022년 11월 10일
보안 업데이트	인터페이스 VPC 엔드포인트와 프라이빗 연결을 설정합니다.	2022년 3월 7일
새 기능	소스 코드 분석을 위한 Azure DevOps Git 리포지토리 지원이 추가되었습니다.	2022년 1월 28일
새 기능	SQL 데이터베이스에 대한 Babelfish 권장 사항이 추가되었습니다.	2022년 1월 14일
초기 릴리스	Migration Hub Strategy Recommendations 사용 설명서의 첫 번째 릴리스입니다.	2021년 10월 25일

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