사용자 가이드

AWS Application Discovery 서비스

AWS Application Discovery 서비스: 사용자 가이드

Table of Contents

AWS Application Discovery Service란 무엇인가요?

AWS Application Discovery Service온프레미스 서버와 데이터베이스에 대한 사용 및 구성 데이터를 수집하여AWS 클라우드로의 마이그레이션을 계획하도록 지원합니다. Application Discovery ServiceAWS Database Migration Service FleetAWS Migration Hub Advisor와 통합됩니다. Migration Hub Hub는 마이그레이션 상태 정보를 단일 콘솔로 집계하여 마이그레이션 추적을 간소화합니다. 검색된 서버를 보고 애플리케이션으로 그룹화한 다음 홈 지역의 Migration Hub 콘솔에서 각 애플리케이션의 마이그레이션 상태를 추적할 수 있습니다. DMS Fleet Advisor를 사용하여 데이터베이스 워크로드의 마이그레이션 옵션을 평가할 수 있습니다.

검색된 모든 데이터는AWS Migration Hub 홈 리전에 저장됩니다. 따라서 검색 및 마이그레이션 작업을 수행하기 전에 Migration Hub 콘솔 또는 CLI 명령을 사용하여 홈 지역을 설정해야 합니다. Microsoft Excel 또는 Amazon Athena 및 Amazon과 같은AWS 분석 도구에서 분석을 위해 데이터를 내보낼 수 QuickSight 있습니다.

Application Discovery Service API를 사용하여 검색된 서버의 시스템 성능 및 사용률 데이터를 내보낼 수 있습니다. 이 데이터를 비용 모델에 입력하여 해당 서버를 실행하는 데 드는 비용을 계산합니다 AWS. 또한 서버 간에 존재하는 네트워크 연결에 대한 데이터를 내보낼 수 있습니다. 이 정보는 서버 간 네트워크 종속성을 판단하고 마이그레이션 계획을 위해 애플리케이션으로 그룹화하는 데 도움이 됩니다.

> **Note**
>
> 데이터는 홈 지역에 저장되므로 검색 프로세스를 시작하기AWS Migration Hub 전에 홈 지역을 설정해야 합니다. 홈 리전을 사용하는 방법에 대한 자세한 내용은 홈 리전을 참조하십시오.

Application Discovery Service 온프레미스 서버에 대한 검색 및 데이터 수집을 수행하는 두 가지 방법을 제공합니다.

- VMware vCenter를 통해 Application Discovery Service 에이전트리스 컬렉터 (에이전트리스 컬렉터) (OVA 파일) 를 구축하여 에이전트 없는 검색을 수행할 수 있습니다. 에이전트리스 컬렉터가 구성되면 vCenter와 연결된 가상 시스템 (VM) 및 호스트를 식별합니다. Agentless Collector는 서버 호스트 이름, IP 주소, MAC 주소, 디스크 리소스 할당, 데이터베이스 엔진 버전 및 데이터베이스 스키마와 같은 정적 구성 데이터를 수집합니다. 또한 각 VM 및 데이터베이스의 사용률 데이터를 수집하여 CPU, RAM 및 디스크 I/O와 같은 메트릭의 평균 및 최대 사용률을 제공합니다.

- 에이전트 기반 검색은AWS 애플리케이션 검색 에이전트를 각 VM과 물리적 서버에 배포하여 수행할 수 있습니다. Windows 및 Linux 운영 체제에서 에이전트 설치 관리자를 사용할 수 있습니다. 이는 정적인 구성 데이터, 시계열 시스템 성능 세부 정보, 인바운드(수신) 및 아웃바운드(발신) 네트워크 연결, 실행되는 프로세스에 대한 데이터를 수집합니다.

Application Discovery ServiceAWS 파트너 네트워크 (APN) 파트너의 애플리케이션 검색 솔루션과 통합됩니다. 이러한 타사 솔루션을 사용하면 에이전트 없는 수집기 또는 검색 에이전트를 사용하지 않고도 온프레미스 환경에 대한 세부 정보를 Migration Hub로 직접 가져올 수 있습니다. 타사 애플리케이션 검색 도구는AWS 애플리케이션 검색 서비스를 쿼리하고 공용 API를 사용하여 Application Discovery Service 데이터베이스에 쓸 수 있습니다. 이러한 방식으로 데이터를 Migration Hub로 가져와서 볼 수 있으므로 애플리케이션을 서버와 연결하고 마이그레이션을 추적할 수 있습니다.

VM웨어 Discovery

VMware vCenter 환경에서 실행 중인 가상 시스템 (VM) 이 있는 경우 각 VM에 에이전트를 설치할 필요 없이 에이전트 없는 수집기를 사용하여 시스템 정보를 수집할 수 있습니다. 대신 이 온프레미스 어플라이언스를 vCenter에 로드하여 모든 호스트와 VM을 검색할 수 있도록 합니다.

Agentless Collector는 사용 중인 운영 체제에 관계없이 vCenter에서 실행 중인 각 VM에 대한 시스템 성능 정보 및 리소스 사용률을 캡처합니다. 하지만 각 VM '내부'를 볼 수는 없습니다. 따라서 각 VM에서 실행되는 프로세스나 존재하는 네트워크 연결을 파악할 수 없습니다. 따라서 이러한 수준의 세부 정보가 필요하고 마이그레이션 계획을 지원하기 위해 기존 VM 중 일부를 자세히 살펴보려는 경우 필요에 따라 Discovery Agent를 설치할 수 있습니다.

또한 VMware에서 호스팅되는 VM의 경우 에이전트 없는 수집기와 검색 에이전트를 모두 사용하여 검색을 동시에 수행할 수 있습니다. 각 검색 도구가 수집하는 데이터의 정확한 유형에 대한 자세한 내용은 에이전트리스 컬렉터가 수집한 데이터 및 디스커버리 에이전트에서 수집한 데이터를 참조하십시오.

데이터베이스 검색

온-프레미스 환경에 데이터베이스 및 분석 서버가 있는 경우 Agentless Collector를 사용하여 이러한 서버를 검색하고 인벤토리를 작성할 수 있습니다. 그러면 사용자 환경의 각 컴퓨터에 Agentless Collector를 설치할 필요 없이 각 데이터베이스 서버에 대한 성능 메트릭을 수집할 수 있습니다.

Agentless Collector 데이터베이스 및 분석 데이터 수집 모듈은 데이터 인프라에 대한 통찰력을 제공하는 메타데이터 및 성능 지표를 캡처합니다. 데이터베이스 및 분석 데이터 수집 모듈은 Microsoft Active Directory의 LDAP를 사용하여 네트워크의 OS, 데이터베이스 및 분석 서버에 대한 정보를 수집합니다.

그런 다음 데이터 수집 모듈이 정기적으로 쿼리를 실행하여 데이터베이스 및 분석 서버의 CPU, 메모리 및 디스크 용량에 대한 실제 사용률 지표를 수집합니다. 수집된 지표에 대한 자세한 내용은 을 참조하십시오데이터베이스 및 분석 모듈에서 수집한 데이터.

Agentless Collector가 사용자 환경에서 데이터 수집을 완료한 후AWS DMS 콘솔을 사용하여 추가 분석을 수행하고 마이그레이션을 계획할 수 있습니다. 예를 들어, 에서 최적의 마이그레이션 대상을 선택하려면 원본 데이터베이스에 대한 대상 권장 사항을 생성할 수 있습니다.AWS 클라우드 자세한 정보는 데이터베이스 및 분석 데이터 수집 모듈을 참조하세요.

에이전트리스 콜렉터와 디스커버리 에이전트 비교

다음 표는 Application Discovery Service 데이터 수집 도구를 간략하게 비교한 것입니다.

	에이전트리스 콜렉터	Discovery Agent
Supported server types		
VMware 가상 머신	예	예
물리적 서버	아니요	예
Deployment		
서버 당	아니요	예
vCenter 당	예	아니요
Collected data		
정적 서버 구성 데이터	Yes	Yes
데이터베이스 구성 데이터	Yes	No
VM 사용률 지표	Yes	No
데이터베이스 사용률 지표	Yes	No
시계열 성능 정보	No	Yes (Export only)
네트워크 인바운드(수신)/아웃바운드(발신) 연결	No	Yes (Export only)

	에이전트리스 콜렉터	Discovery Agent
실행 중인 프로세스	No	Yes (Export only)
지원되는 OS	Any OS running in VM웨어 센터 V5.5+	지원되는 Linux 및 Windows 운영 체제 목록은 을 참조하십시오디스커버리 에이전트의 사전 요구 사항.
지원되는 데이터베이스	Oracle, SQL Server, MySQL, and PostgreSQL	없음

가정

Application Discovery Service 사용하려면 다음과 같이 가정해야 합니다.

- 에AWS 가입했습니다. 자세한 정보는 Application Discovery 서비스 설정을 참조하세요.
- Migration Hub 홈 지역을 선택했습니다. 자세한 내용은 홈 리전 단원을 참조하십시오.

예상되는 결과는 다음과 같습니다.

- Migration Hub 홈 리전은 Application Discovery Service 및 계획 데이터를 저장하는 유일한 리전입니다.
- Discovery 에이전트, 커넥터 및 가져오기는 선택한 Migration Hub 홈 지역에서만 사용할 수 있습니다.
- Application Discovery Service 사용할 수 있는AWS 지역 목록은 를 참조하십시오 Amazon Web Services 일반 참조.

Application Discovery 서비스 설정

AWS Application Discovery Service 처음 사용하기 전에 다음 작업을 완료하십시오.

Amazon Web Services에 가입
IAM 사용자 생성
Migration Hub 콘솔에 로그인하고 홈 지역을 선택합니다.

Amazon Web Services에 가입

계정이 AWS 계정없는 경우 다음 단계를 완료하여 새로 만드십시오.

가입하려면 AWS 계정

1. https://portal.aws.amazon.com/billing/signup을 여세요.
2. 온라인 지시 사항을 따르세요.

   등록 절차 중에는 전화를 받고 키패드로 인증 코드를 입력하는 과정이 있습니다.

   에 AWS 계정가입하면 AWS 계정 루트 사용자a가 생성됩니다. 루트 사용자에게는 계정의 모든 AWS 서비스 및 리소스 액세스 권한이 있습니다. 보안 모범 사례로, 사용자에게 관리자 액세스 권한을 할당하고 루트 사용자 액세스가 필요한 작업을 수행할 때는 루트 사용자만 사용하십시오.

IAM 사용자 생성

계정을 생성하면 AWS 계정의 모든 AWS 서비스와 리소스에 완전히 액세스할 수 있는 단일 로그인 ID를 얻게 됩니다. 이 ID를 AWS 계정 루트 사용자라고 합니다. 계정을 만들 때 사용한 이메일 주소와 비밀번호를 AWS Management Console 사용하여 로그인하면 계정의 모든 AWS 리소스에 완전히 액세스할 수 있습니다.

일상적인 작업, 심지어 관리 작업의 경우에도 루트 사용자를 사용하지 않는 것이 좋습니다. 대신 보안 모범 사례인 개별 IAM 사용자 생성 및 AWS Identity and Access Management (IAM) 관리자 사용자 생성을 따르세요. 그런 다음 루트 사용자 자격 증명을 안전하게 보관하고 몇 가지 계정 및 서비스 관리 태스크를 수행할 때만 사용합니다.

관리자 사용자를 생성하는 것 외에도 관리자가 아닌 IAM 사용자도 생성해야 합니다. 다음 항목에서는 두 가지 유형의 IAM 사용자를 생성하는 방법을 설명합니다.

주제

IAM 관리 사용자 생성

기본적으로 관리자 계정은 Application Discovery Service에 액세스하는 데 필요한 모든 정책을 상속합니다.

관리자를 만들려면

- 계정에서 관리자 사용자를 생성하십시오. AWS 관련 지침은 IAM 사용자 가이드의 첫 번째 IAM 사용자 및 관리자 그룹 생성 섹션을 참조하십시오.

IAM 비관리자 사용자 생성

관리자가 아닌 IAM 사용자를 생성할 때는 최소 권한 부여 보안 모범 사례를 따라 사용자에게 최소 권한을 부여하십시오.

IAM 관리형 정책을 사용하여 관리자가 아닌 IAM 사용자가 Application Discovery Service에 액세스하는 수준을 정의할 수 있습니다. Application Discovery Service 관리 정책에 대한 자세한 내용은 을 참조하십시오AWS 에 대한 관리형 정책 AWS Application Discovery Service.

관리자가 아닌 IAM 사용자를 만들려면

1. 에서 AWS Management Console IAM 콘솔로 이동합니다.
2. IAM 사용 설명서의 AWS 계정에 IAM 사용자 생성에 설명된 대로 콘솔을 사용하여 사용자를 생성하는 지침을 따라 관리자가 아닌 IAM 사용자를 생성합니다.

   IAM 사용 설명서의 지침을 따르는 동안:

   - 액세스 유형을 선택하는 단계에서 프로그래밍 액세스를 선택합니다. 참고, 권장되지는 않지만 콘솔에 액세스할 때 동일한 IAM 사용자 자격 증명을 사용하려는 경우에만AWS Management Console 액세스를 선택하십시오. AWS
   - 권한 설정 페이지에 대한 단계에서 기존 정책을 사용자에게 직접 연결하는 옵션을 선택하십시오. 그런 다음 정책 목록에서 Application Discovery Service의 관리형 IAM 정책을 선택합니다. Application Discovery Service 관리 정책에 대한 자세한 내용은 을 참조하십시오AWS 에 대한 관리형 정책 AWS Application Discovery Service.

- 사용자의 액세스 키 (액세스 키 ID 및 보안 액세스 키) 를 보는 단계를 진행하려면 사용자의 새 액세스 키 ID와 보안 액세스 키를 안전한 장소에 저장하는 것에 관한 중요 참고 사항의 지침을 따르십시오.

Migration Hub 콘솔에 로그인하고 홈 지역을 선택합니다.

사용 중인 AWS 계정에서 AWS Migration Hub 거주 지역을 선택해야 합니다 AWS Application Discovery Service.

홈 지역을 선택하려면

1. AWS 계정을 사용하여 https://console.aws.amazon.com/migrationhub/ 에서 Migration Hub 콘솔에 AWS Management Console 로그인하고 여십시오.
2. Migration Hub 콘솔 탐색 창에서 설정을 선택하고 홈 지역을 선택합니다.

   Migration Hub 데이터는 검색, 계획 및 마이그레이션 추적 목적으로 홈 지역에 저장됩니다. 자세한 내용은 Migration Hub 홈 지역을 참조하십시오.

AWS 애플리케이션 검색 에이전트

AWS 응용 프로그램 검색 에이전트 (검색 에이전트) 는 검색 및 마이그레이션 대상으로 온-프레미스 서버 및 VM에 설치하는 소프트웨어입니다. 에이전트는 시스템 구성, 시스템 성능, 실행 중인 프로세스 및 시스템 간 네트워크 연결에 대한 세부 정보 등을 캡처합니다. 에이전트는 대부분의 Linux 및 Windows 운영 체제를 지원하며 물리적 온프레미스 서버, Amazon EC2 인스턴스 및 가상 머신에 배포할 수 있습니다.

> **Note**
>
> 디스커버리 에이전트를 배포하기 전에 Migration Hub 홈 지역을 선택해야 합니다. 홈 리전에 에이전트를 등록해야 합니다.

디스커버리 에이전트는 로컬 환경에서 실행되며 루트 권한이 필요합니다. 디스커버리 에이전트를 시작하면 에이전트가 홈 지역에 안전하게 연결되고 Application Discovery Service에 등록됩니다.

- 예를 들어 홈 `eu-central-1` 지역인 경우 Application Discovery `arsenal-discovery.`*`eu-central-1`*`.amazonaws.com` Service에 등록됩니다.
- 또는 필요에 따라 us-west-2를 제외한 다른 모든 리전을 홈 지역으로 대체합니다.
- 홈 `us-west-2` 지역인 경우 Application Discovery `arsenal.us-west-2.amazonaws.com` Service에 등록됩니다.

작동 방식

등록 후 에이전트는 에이전트가 있는 호스트 또는 VM에 대한 데이터 수집을 시작합니다. 에이전트는 15분 간격으로 Application Discovery Service에 ping을 보내 구성 정보를 요청합니다.

수집된 데이터에는 시스템 사양, 시계열 사용률이나 성능 데이터, 네트워크 연결, 프로세스 데이터가 포함됩니다. 이 정보를 사용하여 IT 자산과 네트워크 종속성을 매핑할 수 있습니다. 이러한 모든 데이터 포인트는 이러한 서버를 실행하는 데 드는 비용을 결정하고 마이그레이션을 계획하는 AWS 데 도움이 됩니다.

데이터는 디스커버리 에이전트에서 TLS (전송 계층 보안) 암호화를 사용하여 Application Discovery Service로 안전하게 전송됩니다. 에이전트는 새 버전을 사용할 수 있게 되면 자동으로 업그레이드하도록 구성되어 있습니다. 원하는 경우 이런 구성을 변경할 수 있습니다.

> **Tip**
>
> Discovery Agent를 다운로드하고 설치를 시작하기 전에 다음 필수 사전 요구 사항을 모두 읽어 보십시오. 디스커버리 에이전트의 사전 요구 사항

주제

디스커버리 에이전트의 사전 요구 사항

다음은 AWS 응용 프로그램 검색 에이전트 (검색 에이전트) 를 성공적으로 설치하기 전에 수행해야 하는 사전 요구 사항 및 작업입니다.

- 디스커버리 에이전트 설치를 시작하기 전에 AWS Migration Hub 홈 지역을 설정해야 합니다.
- 설치된 에이전트의 버전이 1.x이면 제거한 후 최신 버전을 설치해야 합니다.
- 에이전트를 설치할 호스트가 Linux를 실행하는 경우 호스트가 최소한 Intel i686 CPU 아키텍처 (P6 마이크로 아키텍처라고도 함) 를 지원하는지 확인하십시오.
- 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 2003 R2 SP2
  - Windows Server 2008 R1 SP2, 2008 R2 SP1

Windows Server 2012 R1, 2012 R2

Windows Server 2016

Windows Server 2019

Windows Server 2022

- 네트워크로부터의 발신 연결이 제한된 경우 방화벽 설정을 업데이트해야 합니다. 에이전트는 TCP 포트 443을 통해 `arsenal`에 액세스해야 합니다. 인바운드(수신) 포트를 열 필요가 없습니다.

  예를 들어, 홈 리전이 `eu-central-1`인 경우 `https://arsenal-discovery.eu-central-1.amazonaws.com:443`을 사용해야 합니다.
- 자동 업그레이드가 작동하려면 홈 지역의 Amazon S3에 액세스해야 합니다.
- 콘솔에서 AWS Identity and Access Management (IAM) 사용자를 생성하고 기존 `AWSApplicationDiscoveryAgentAccess` IAM 관리형 정책을 연결합니다. 이 정책을 통해 사용자는 사용자를 대신하여 필요한 에이전트 작업을 수행할 수 있습니다. 관리형 정책에 대한 자세한 정보는 AWS 에 대한 관리형 정책 AWS Application Discovery Service단원을 참조하세요.
- NTP(Network Time Protocol) 서버에서 시간차를 확인하고 필요한 경우 수정합니다. 잘못된 시간 동기화로 인해 에이전트 등록 호출이 실패합니다.

> **Note**
>
> 디스커버리 에이전트에는 32비트 및 64비트 운영 체제에서 작동하는 32비트 에이전트 실행 파일이 있습니다. 단일 실행 파일이므로 배포에 필요한 설치 패키지의 수가 줄어듭니다. 이 실행 파일 에이전트는 Linux 및 Windows OS에서 작동합니다. 이 내용은 다음에 나오는 각각의 설치 단원에서 설명합니다.

Linux에 디스커버리 에이전트 설치

Linux에서 다음 절차를 완료합니다. 이 절차를 시작하기 전에 Migration Hub 홈 지역이 설정되었는지 확인하십시오.

> **Note**
>
> 최신이 아닌 Linux 버전을 사용하고 있다면 이전 Linux 플랫폼의 요구 사항를 참조하십시오.

데이터 센터에 AWS 애플리케이션 디스커버리 에이전트를 설치하려면

1. Linux 기반 서버 또는 VM에 로그인하고 에이전트 구성 요소를 포함할 새 디렉터리를 생성합니다.
2. 새 디렉터리로 전환한 후 명령줄이나 콘솔에서 설치 스크립트를 다운로드합니다.

   a. 명령줄에서 다운로드를 하려면 다음 명령을 실행합니다.

   ```
   curl -o ./aws-discovery-agent.tar.gz https://s3-us-west-2.amazonaws.com/aws-discovery-agent.us-west-2/linux/latest/aws-discovery-agent.tar.gz
   ```

   b. Migration Hub 콘솔에서 다운로드하려면 다음과 같이 하십시오.

      i. 콘솔을 열고 검색 도구 페이지로 이동합니다.

      ii. Discovery Agent(검색 에이전트) 상자에서 Download agent(에이전트 다운로드)를 선택한 다음 표시되는 목록 상자에서 Linux를 선택합니다. 그러면 즉시 다운로드가 시작됩니다.

3. 다음 세 가지 명령을 사용하여 설치 패키지의 암호화 서명을 확인합니다.

   ```
   curl -o ./agent.sig https://s3.us-west-2.amazonaws.com/aws-discovery-agent.us-west-2/linux/latest/aws-discovery-agent.tar.gz.sig
   ```

   ```
   curl -o ./discovery.gpg https://s3.us-west-2.amazonaws.com/aws-discovery-agent.us-west-2/linux/latest/discovery.gpg
   ```

   ```
   gpg --no-default-keyring --keyring ./discovery.gpg --verify agent.sig aws-discovery-agent.tar.gz
   ```

   에이전트 퍼블릭 키(discovery.gpg) 지문은 7638 F24C 6717 F97C 4F1B 3BC0 5133 255E 4DF4 2DA2입니다.

4. 다음과 같이 tarball에서 추출합니다.

   ```
   tar -xzf aws-discovery-agent.tar.gz
   ```

5. 에이전트를 설치하려면 다음 설치 방법 중 하나를 선택합니다.

원하는 작업	수행할 작업
디스커버리 에이전트 설치	에이전트를 설치하려면 다음 예와 같이 에이전트 설치 명령을 실행합니다. 예시에서는 거주 지역 이름, *aws-access-key-id* 액세스 키 ID, 보안 액세스 *your-home-region* 키로 대체합니다. *aws-secret-access-key* `sudo bash install -r your-home-region -k aws-access-key-id -s aws-secret-access-key` 기본적으로 상담원은 업데이트가 제공되는 대로 자동으로 다운로드하여 적용합니다. 이 기본 구성을 사용하는 것이 좋습니다. 하지만 에이전트가 업데이트를 자동으로 다운로드하고 적용하지 않도록 하려면 에이전트 설치 명령을 실행할 때 `-u false` 매개 변수를 포함하세요.

원하는 작업	수행할 작업
(선택 사항) Discovery Agent를 설치하고 투명하지 않은 프록시를 구성합니다.	투명하지 않은 프록시를 구성하려면 에이전트 설치 명령에 다음 매개 변수를 추가합니다. • -e 프록시 비밀번호. • -f 프록시 포트 번호. • -g 프록시 스킴. • -i 프록시 사용자 이름. 다음은 투명하지 않은 프록시 매개 변수를 사용하는 에이전트 설치 명령의 예입니다. `sudo bash install -r your-home-region -k aws-access-key-id -s aws-secret-access-key -d myproxy.mycompany.com -e mypassword -f proxy-port-number -g https -i myusername` 프록시에 인증이 필요하지 않은 경우에는 `-e` 및 `-i` 매개 변수를 생략하십시오. 설치 명령 예시에서는 `https` 프록시가 HTTP를 사용하는 경우 `-g` 매개변수 값을 지정합니다`http`.

6. 네트워크로부터의 발신 연결이 제한된 경우 방화벽 설정을 업데이트해야 합니다. 에이전트는 TCP 포트 443을 통해 `arsenal`에 액세스해야 합니다. 인바운드(수신) 포트를 열 필요가 없습니다.

   예를 들어, 홈 리전이 `eu-central-1`인 경우 `https://arsenal-discovery.eu-central-1.amazonaws.com:443`을 사용해야 합니다.

주제

- 이전 Linux 플랫폼의 요구 사항
- Linux의 디스커버리 에이전트 프로세스 관리

- Linux에서 디스커버리 에이전트 제거
- Linux 디스커버리 에이전트 문제 해결

이전 Linux 플랫폼의 요구 사항

SUSE 10, CentOS 5 및 RHEL 5와 같은 일부 이전 Linux 플랫폼은 수명이 다 되었거나 최소한의 지원만 받을 수 있습니다. 이러한 플랫폼에는 에이전트 업데이트 스크립트가 설치 out-of-date 패키지를 다운로드하지 못하도록 하는 암호 제품군이 있을 수 있습니다.

Curl

응용 프로그램 검색 에이전트는 서버와의 보안 통신을 필요로 `curl` 합니다. AWS `curl`의 일부 기존 버전은 최신 웹 서비스로 안전하게 통신할 수 없습니다.

Application Discovery 에이전트에 포함된 `curl`의 버전을 모든 작업에 사용하려면 `-c true` 파라미터로 설치 스크립트를 실행합니다.

인증 기관 번들

구형 Linux 시스템에는 인터넷 통신 보안에 필수적인 out-of-date 인증 기관 (CA) 번들이 있을 수 있습니다.

Application Discovery 에이전트에 포함된 CA 번들을 모든 작업에 사용하려면 `-b true` 파라미터로 설치 스크립트를 실행합니다.

이러한 설치 스크립트 옵션을 함께 사용할 수 있습니다. 다음 예제 명령에서는 두 스크립트 매개 변수가 모두 설치 스크립트에 전달됩니다.

```
sudo bash install -r your-home_region -k aws-access-key-id -s aws-secret-access-key -c
 true -b true
```

Linux의 디스커버리 에이전트 프로세스 관리

`systemd`Upstart, 또는 `System V init` 도구를 사용하여 시스템 수준에서 검색 에이전트의 동작을 관리할 수 있습니다. 다음 탭에서는 각 도구에서 지원되는 작업에 대한 명령을 간략하게 설명합니다.

systemd

Application Discovery Agent에 대한 관리 명령

작업	Command
에이전트가 실행 중인지 확인	`sudo systemctl status aws-discovery-daemon.service`
에이전트 시작	`sudo systemctl start aws-discovery-daemon.service`
에이전트 중지	`sudo systemctl stop aws-discovery-daemon.service`
에이전트 다시 시작	`sudo systemctl restart aws-discovery-daemon.service`

Upstart

애플리케이션 디스커버리 에이전트의 관리 명령

작업	Command
에이전트가 실행 중인지 확인	`sudo initctl status aws-discovery-daemon`
에이전트 시작	`sudo initctl start aws-discovery-daemon`
에이전트 중지	`sudo initctl stop aws-discovery-daemon`
에이전트 다시 시작	`sudo initctl restart aws-discovery-daemon`

System V init

애플리케이션 검색 에이전트의 관리 명령

작업	Command
에이전트가 실행 중인지 확인	`sudo /etc/init.d/aws-discovery-daemon status`
에이전트 시작	`sudo /etc/init.d/aws-discovery-daemon start`
에이전트 중지	`sudo /etc/init.d/aws-discovery-daemon stop`
에이전트 다시 시작	`sudo /etc/init.d/aws-discovery-daemon restart`

Linux에서 디스커버리 에이전트 제거

이 섹션에서는 Linux에서 디스커버리 에이전트를 제거하는 방법을 설명합니다.

yum 패키지 관리자를 사용하는 경우 에이전트를 제거하려면

- yum을 사용하는 경우 다음 명령을 사용하여 에이전트를 제거합니다.

```
rpm -e --nodeps aws-discovery-agent
```

apt-get 패키지 관리자를 사용하는 경우 에이전트를 제거하려면

- apt-get을 사용하는 경우 다음 명령을 사용하여 에이전트를 제거합니다.

```
apt-get remove aws-discovery-agent:i386
```

zypper 패키지 관리자를 사용하는 경우 에이전트를 제거하려면

- zypper를 사용하는 경우 다음 명령을 사용하여 에이전트를 제거합니다.

```
zypper remove aws-discovery-agent
```

Linux 디스커버리 에이전트 문제 해결

Linux에서 디스커버리 에이전트를 설치하거나 사용하는 동안 문제가 발생하는 경우 로깅 및 구성에 대한 다음 지침을 참조하십시오. 에이전트와 관련된 잠재적 문제 또는 Application Discovery Service와의 연결 문제를 해결하는 데 도움을 주기 위해 AWS Support는 종종 이러한 파일을 요청합니다.

- 로그 파일

  검색 에이전트의 로그 파일은 다음 디렉터리에 있습니다.

  ```
  /var/log/aws/discovery/
  ```

  로그 파일은 기본 데몬, 자동 업그레이드 프로그램 또는 설치 프로그램에서 생성되었는지 여부를 나타내기 위해 이름이 지정됩니다.

- 구성 파일

  디스커버리 에이전트 버전 2.0.1617.0 이상의 구성 파일은 다음 디렉터리에 있습니다.

  ```
  /etc/opt/aws/discovery/
  ```

  2.0.1617.0 이전 버전의 디스커버리 에이전트에 대한 구성 파일은 다음 디렉터리에 있습니다.

  ```
  /var/opt/aws/discovery/
  ```

- 이전 버전의 디스커버리 에이전트를 제거하는 방법에 대한 지침은 을 참조하십시오. 디스커버리 에이전트의 사전 요구 사항

Windows에 설치

Windows에 에이전트를 설치하려면 다음 절차를 완료하십시오. 이 절차를 시작하기 전에 Migration Hub 홈 지역이 설정되었는지 확인하십시오.

데이터 센터에 AWS 애플리케이션 디스커버리 에이전트를 설치하려면

1. Windows 에이전트 설치 프로그램을 다운로드하되 Windows 내에서 설치 프로그램을 실행하기 위해 두 번 클릭하지 마십시오.

> **Important**
>
> Windows 내에서 설치 프로그램을 두 번 클릭하여 실행하지 마십시오. 설치에 실패할 수 있습니다. 명령 프롬프트를 사용해서만 에이전트를 설치할 수 있습니다. (설치 관리자를 두 번 클릭했다면 남은 설치 단계를 계속 진행하기 전에 프로그램 추가/제거로 이동해 에이전트를 제거해야 합니다.)
> Windows 에이전트 설치 프로그램이 호스트에서 Visual C++ x86 런타임 버전을 발견하지 못하는 경우 에이전트 소프트웨어를 설치하기 전에 Visual C++ x86 2015-2019 런타임을 자동으로 설치합니다.

2. 명령 프롬프트를 관리자로 열고 설치 패키지를 저장한 위치를 탐색합니다.
3. 에이전트를 설치하려면 다음 설치 방법 중 하나를 선택합니다.

원하는 작업	수행할 작업
디스커버리 에이전트 설치	에이전트를 설치하려면 다음 예와 같이 에이전트 설치 명령을 실행합니다. 예시에서는 거주 지역 이름, *aws-access-key-id* 액세스 키 ID, 보안 액세스 *your-home-region* 키로 대체합니다. *aws-secret-access-key* 선택적으로 INSTALLOCATION 매개 변수의 폴더 경로를 *C:\install-location* 지정하여 에이전트 설치 위치를 설정할 수 있습니다. 예를 들어 INSTALLLOCATION=" *C:\install-location* "입니다. 결과 폴더 계층 구조는 [설치 위치 경로]\AWS Discovery 가 됩니다. 기본적으로 설치 위치는 Program Files 폴더입니다. 선택적으로, 를 LOGANDCONFIGLOCATION 사용하여 에이전트 로그 폴더 및 구성 파일

원하는 작업	수행할 작업
	의 기본 디렉터리 (ProgramData) 를 재정의할 수 있습니다. 결과 폴더 계층 구조는 다음과 같습니다. [*LOGANDCONFIGLOCATION path*]\AWS Discovery `.\AWSDiscoveryAgentInstaller.exe REGION=" your-home-region " KEY_ID="aws-access-key-id " KEY_SECRET=" aws-secret-access-key " /quiet` 기본적으로 에이전트는 업데이트가 제공되는 대로 업데이트를 자동으로 다운로드하여 적용합니다. 이 기본 구성을 사용하는 것이 좋습니다. 하지만 에이전트에서 업데이트를 자동으로 다운로드하고 적용하지 않도록 하려면 에이전트 설치 명령을 실행할 때 다음 매개 변수를 포함하세요. `AUTO_UPDATE=false` **Warning** 자동 업그레이드를 비활성화하면 최신 보안 패치가 설치되지 않습니다.

원하는 작업	수행할 작업
(선택 사항) Discovery Agent를 설치하고 투명하지 않은 프록시를 구성합니다.	투명하지 않은 프록시를 구성하려면 에이전트 설치 명령에 다음 공용 속성을 추가합니다. • PROXY_HOST — 프록시 호스트의 이름 • 프록시_스킴 — 프록시 스킴 • PROXY_PORT — 프록시 포트 번호 • PROXY_USER — 프록시 사용자 이름 • 프록시_비밀번호 — 프록시 사용자 비밀번호 다음은 투명하지 않은 프록시 속성을 사용하는 에이전트 설치 명령의 예입니다. `.\AWSDiscoveryAgentInstaller.exe REGION=" your-home-region " KEY_ID="aws-access-key-id " KEY_SECRET=" aws-secret-access-key " PROXY_HOST=" myproxy.mycompany.com " PROXY_SCHEME="https" PROXY_PORT=" proxy-port-number " PROXY_USER=" myusername " PROXY_PASSWORD=" mypassword " /quiet` 프록시에 인증이 필요하지 않은 경우 PROXY_USER 및 PROXY_PASSWORD 속성을 생략하십시오. 설치 명령 예시에서는 다음을 사용합니다https. 프록시가 HTTP를 사용하는 경우 PROXY_SCHEME 값을 지정하십시오http.

4. 네트워크에서의 아웃바운드 연결이 제한되는 경우 방화벽 설정을 업데이트해야 합니다. 에이전트는 TCP 포트 443을 통해 arsenal에 액세스해야 합니다. 인바운드(수신) 포트를 열 필요가 없습니다.

   예를 들어 거주 지역이 다음과 같은 eu-central-1 경우 다음을 사용합니다. https://arsenal-discovery.*eu-central-1*.amazonaws.com:443

패키지 서명 및 자동 업그레이드

Windows Server 2008 이상의 경우 Amazon은 SHA256 인증서를 사용하여 Application Discovery Service 에이전트 설치 패키지에 암호로 서명합니다. Windows Server 2008 SP2의 SHA2 서명 자동 업데이트의 경우 SHA2 서명 인증을 지원하는 핫픽스가 호스트에 설치되어 있는지 확인하십시오. 마이크로소프트의 최신 지원 핫픽스는 윈도우 서버 2008 SP2에서 SHA2 인증을 지원하는 데 도움이 됩니다.

> **Note**
>
> Windows 2003의 SHA256 지원 핫픽스는 Microsoft에서 더 이상 공개하지 않습니다. Windows 2003 호스트에 이러한 픽스가 아직 설치되지 않은 경우 수동 업그레이드가 필요합니다.

업그레이드를 수동으로 수행하려면

1. Windows 에이전트 업데이터를 다운로드하십시오.
2. 관리자 권한으로 명령 프롬프트를 엽니다.
3. 업데이터가 저장된 위치로 이동합니다.
4. 다음 명령을 실행합니다.

```
AWSDiscoveryAgentUpdater.exe /Q
```

Windows에서 디스커버리 에이전트 프로세스를 관리합니다.

Windows Server 관리자 서비스 콘솔을 통해 시스템 수준에서 검색 에이전트의 동작을 관리할 수 있습니다. 다음은 그 방법을 설명하고 있는 테이블입니다.

작업	서비스 이름	서비스 상태/작업
에이전트가 실행 중인지 확인	AWS 디스커버리 에이전트 AWS 디스커버리 업데이터	시작됨
에이전트 시작	AWS 디스커버리 에이전트 AWS 디스커버리 업데이터	시작을 선택합니다

작업	서비스 이름	서비스 상태/작업
에이전트 중지	AWS 디스커버리 에이전트 AWS 디스커버리 업데이터	중지를 선택합니다.
에이전트 다시 시작	AWS 디스커버리 에이전트 AWS 디스커버리 업데이터	다시 시작를 선택합니다.

Windows에서 검색 에이전트 제거

1. 윈도우에서 제어판을 여십시오.
2. Programs(프로그램)을 선택합니다.
3. Programs and Features(프로그램 및 기능)을 선택합니다.
4. AWS 디스커버리 에이전트를 선택합니다.
5. 제거를 선택합니다.

> **Note**
>
> 에이전트를 제거한 후 다시 설치하도록 선택한 경우 `/repair` 및 `/norestart` 옵션과 함께 다음 명령을 실행합니다.
>
> ```
> .\AWSDiscoveryAgentInstaller.exe REGION="your-home-region" KEY_ID="aws-access-key-id" KEY_SECRET="aws-secret-access-key" /quiet /repair /norestart
> ```

명령줄을 사용하여 Windows에서 검색 에이전트를 제거하려면

1. 시작을 마우스 오른쪽 버튼으로 클릭합니다.
2. 명령 프롬프트를 선택합니다.
3. 다음 명령을 사용하여 Windows에서 검색 에이전트를 제거합니다.

```
wmic product where name='AWS Discovery Agent' call uninstall
```

Windows의 디스커버리 에이전트 문제 해결

Windows에서 AWS 응용 프로그램 검색 에이전트를 설치하거나 사용하는 동안 문제가 발생하는 경우 로깅 및 구성에 대한 다음 지침을 참조하십시오. AWS Support에이전트와 관련된 잠재적 문제 또는 Application Discovery Service와의 연결 문제를 해결하는 데 도움이 될 때 이러한 파일을 요청하는 경우가 많습니다.

- 설치 로깅

  경우에 따라 에이전트 설치 명령이 실패한 것처럼 보일 수 있습니다. 예를 들어, Windows Service Manager에 검색 서비스가 생성되지 않을 것임을 표시하는 결함이 표시될 수 있습니다. 이 경우 /log install.log를 명령에 추가해 verbose 설치 로그를 생성합니다.

- 작업 로깅

  Windows Server 2008 이상에서 에이전트 로그 파일은 다음 디렉터리 아래에서 찾을 수 있습니다.

  ```
  C:\ProgramData\AWS\AWS Discovery\Logs
  ```

  Windows Server 2003의 에이전트 로그 파일은 다음 디렉터리 아래에서 찾을 수 있습니다.

  ```
  C:\Documents and Settings\All Users\Application Data\AWS\AWS Discovery\Logs
  ```

  로그 파일은 기본 서비스, 자동 업그레이드 또는 설치 프로그램에서 생성되었는지 여부를 나타내기 위해 이름이 지정됩니다.

- 구성 파일

  Windows Server 2008 이상에서 에이전트 구성 파일은 다음 위치에서 찾을 수 있습니다.

  ```
  C:\ProgramData\AWS\AWS Discovery\config
  ```

  Windows Server 2003에서 에이전트 구성 파일은 다음 위치에서 찾을 수 있습니다.

  ```
  C:\Documents and Settings\All Users\Application Data\AWS\AWS Discovery\config
  ```

- 이전 버전의 Discovery Agent를 제거하는 방법에 대한 지침은 을 참조하십시오디스커버리 에이전트의 사전 요구 사항.

디스커버리 에이전트에서 수집한 데이터

AWS 애플리케이션 디스커버리 에이전트 (디스커버리 에이전트) 는 온프레미스 서버 및 VM에 설치하는 소프트웨어입니다. 디스커버리 에이전트는 시스템 구성, 시계열 사용률 또는 성능 데이터, 프로세스 데이터, TCP (전송 제어 프로토콜) 네트워크 연결을 수집합니다. 이 섹션에서는 수집되는 데이터에 대해 설명합니다.

디스커버리 에이전트가 수집한 데이터에 대한 표 범례:

- 호스트란 물리적 서버나 VM을 가리킵니다.
- 수집된 데이터는 별도의 명시가 없는 경우에는 KB(Kilobytes)로 측정됩니다.
- Migration Hub 콘솔의 해당 데이터는 메가바이트 (MB) 단위로 보고됩니다.
- 폴링 주기는 약 15초 간격으로 AWS 15분마다 전송됩니다.
- 별표 (*) 로 표시된 데이터 필드는 에이전트의 API 내보내기 기능에서 생성된 `.csv` 파일에서만 사용할 수 있습니다.

데이터 필드	설명
agentAssignedProcessId *	에이전트가 검색한 프로세스의 프로세스 ID
agentId	에이전트의 고유 ID
agentProvidedTime스탬프*	에이전트 관찰 날짜 및 시간(mm/dd/yyyy hh:mm:ss am/pm)
cmdLine*	명령줄에 입력된 프로세스
cpuType	호스트에 사용되고 있는 CPU(중앙 처리 장치)의 유형
destinationIp*	패킷이 전송되는 장치의 IP 주소
destinationPort*	데이터/요청이 전송되는 포트 번호
패밀리*	라우팅 그룹 프로토콜
freeRAM(MB)	애플리케이션에서 바로 사용할 수 있는 MB 단위의 무료 RAM과 캐시된 RAM

데이터 필드	설명
gateway*	네트워크의 노드 주소
hostName	데이터가 수집되는 호스트 이름
하이퍼바이저	하이퍼바이저 유형
ipAddress	호스트의 IP 주소
ipVersion*	IP 버전 번호
isSystem*	프로세스를 OS가 소유하고 있는지 여부를 나타내는 부울 속성
macAddress	호스트의 MAC 주소
name*	수집 중인 호스트 이름, 네트워크, 지표 등의 데이터
netMask*	네트워크 호스트가 속한 IP 주소 접두사
osName	호스트의 운영 체제 이름
osVersion	호스트의 운영 체제 버전
경로	명령줄에서 발생하는 명령의 경로
sourceIp*	IP 패킷을 전송하는 장치의 IP 주소
sourcePort*	데이터/요청의 출처인 포트 번호
타임스탬프*	에이전트가 기록한 보고된 속성의 날짜와 시간
totalCpuUsage협정	폴링 기간 동안 호스트의 CPU 사용량(%)
totalDiskBytesReadPerSecond (Kbps)	모든 디스크의 초당 읽기 총 킬로비트
totalDiskBytesWrittenPerSecond (Kbps)	모든 디스크에서 초당 기록된 총 킬로비트
totalDiskFree크기 (GB)	사용 가능한 디스크 공간(GB)

데이터 필드	설명
totalDiskReadOpsPerSecond	초당 읽기 I/O 연산 수 합계
totalDiskSize (GB)	디스크 총 용량(GB)
totalDiskWriteOpsPerSecond	초당 쓰기 I/O 연산 수 합계
totalNetworkBytesReadPerSecond (Kbps)	초당 총 읽기 처리량(바이트)
totalNetworkBytesWrittenPerSecond (Kbps)	초당 총 쓰기 처리량(바이트)
totalNumCores	CPU의 독립 처리 유닛 수 합계
totalNumCpus	중앙 처리 유닛 수 합계
totalNumDisks	호스트의 물리적 하드 디스크 수
totalNumLogical프로세서 *	물리적 코어 수 합계와 각 코어에서 실행할 수 있는 스레드의 수를 곱한 값
totalNumNetwork카드	서버의 네트워크 카드 수 합계
totalRAM(MB)	호스트에서 사용할 수 있는 총 RAM
transportProtocol*	사용하고 있는 전송 프로토콜 유형

디스커버리 에이전트 데이터 수집 시작 또는 중지

디스커버리 에이전트를 배포하고 구성한 후 데이터 수집이 중지되면 다시 시작할 수 있습니다. 콘솔을 통해 또는 를 통해 API를 호출하여 데이터 수집을 시작하거나 중지할 수 AWS CLI있습니다. 두 방법 모두 다음 절차에 설명되어 있습니다.

Using the Migration Hub console

다음 절차는 Migration Hub 콘솔의 데이터 수집기 페이지에서 Discovery Agent 데이터 수집 프로세스를 시작하거나 중지하는 방법을 보여줍니다.

데이터 수집을 시작하거나 중지하려면

1. 탐색 창에서 Data Collectors(데이터 수집기)를 선택합니다.

2. 에이전트 탭을 선택합니다.
3. 시작하거나 중지하려는 에이전트의 확인란을 선택합니다.

> **Tip**
>
> 여러 에이전트를 설치했지만 특정 호스트에서만 데이터 수집을 시작하거나 중지하려는 경우 에이전트 행의 호스트 이름 열은 에이전트가 설치된 호스트를 식별합니다.

4. Start data collection(데이터 수집 시작)이나 Stop data collection(데이터 수집 중지)를 선택합니다.

Using the AWS CLI

에서 Discovery Agent 데이터 수집 프로세스를 시작하거나 중지하려면 먼저 환경에 를 설치한 다음 선택한 Migration Hub 홈 지역을 사용하도록 CLI를 설정해야 합니다. AWS CLI AWS CLI

데이터 수집을 설치 AWS CLI 및 시작 또는 중지하려면

1. 아직 설치하지 않았다면 OS 유형 (Windows 또는 Mac/Linux) 에 맞게 설치하십시오. AWS CLI 지침은 AWS Command Line Interface 사용 설명서를 참조하십시오.
2. 명령 프롬프트(Windows) 또는 터미널(MAC/Linux)을 엽니다.
   a. `aws configure`를 입력하고 Enter 키를 누릅니다.
   b. AWS 액세스 키 ID와 AWS 보안 액세스 키를 입력합니다.
   c. 기본 리전 이름에 홈 리전을 입력합니다(예: *us-west-2*). 이 예에서는 홈 리전을 `us-west-2`로 가정합니다.
   d. 기본 출력 형식에 `text`를 입력합니다.
3. 데이터 수집을 중지하거나 시작하려는 에이전트의 ID를 찾으려면 다음 명령을 입력합니다.

```
aws discovery describe-agents
```

4. 에이전트에서 데이터 수집을 시작하려면 다음 명령을 입력합니다.

```
aws discovery start-data-collection-by-agent-ids --agent-ids <agent ID>
```

에이전트의 데이터 수집을 중지하려면 다음 명령을 입력합니다.

```
aws discovery stop-data-collection-by-agent-ids --agent-ids <agent ID>
```

Application Discovery Service 에이전트리스 컬렉터

Application Discovery Service 에이전트리스 컬렉터 (Agentless Collector) 는 에이전트 없는 방법을 통해 서버 프로필 정보 (예: OS, CPU 수, RAM 용량), 데이터베이스 메타데이터, 사용률 지표 등 온프레미스 환경에 대한 정보를 수집하는 온프레미스 애플리케이션입니다. OVA(Open Virtualization Archive) 파일을 사용하여 Agentless Collector를 VMware vCenter Server 환경의 VM(가상 머신)으로 설치합니다.

에이전트리스 컬렉터는 모듈식 아키텍처를 사용하므로 여러 에이전트 없는 수집 방법을 사용할 수 있습니다. 에이전트리스 컬렉터는 현재 VMware VM과 데이터베이스 및 분석 서버에서 데이터를 수집하기 위한 모듈을 지원합니다. 향후 모듈에서는 네트워크 연결 수집, 추가 가상화 플랫폼에서의 수집, 운영 체제 수준 수집을 지원할 예정입니다.

Agentless Collector는 온-프레미스 서버 및 데이터베이스에 대한 사용 및 구성 데이터를 AWS 클라우드 수집하여 마이그레이션을 계획하는 데 도움이 되는 AWS Application Discovery Service (Application Discovery Service) 에 대한 데이터 수집을 지원합니다.

Application Discovery Service는 와 AWS Migration Hub통합되어 마이그레이션 상태 정보를 단일 콘솔로 집계하므로 마이그레이션 추적을 단순화합니다. 검색된 서버를 보고, Amazon EC2 권장 사항을 얻고, 네트워크 연결을 시각화하고, 서버를 애플리케이션으로 그룹화한 다음, 홈 지역의 Migration Hub 콘솔에서 각 애플리케이션의 마이그레이션 상태를 추적할 수 있습니다.

Agentless Collector 데이터베이스 및 분석 데이터 수집 모듈은 () 와 통합되어 있습니다. AWS Database Migration Service AWS DMS이 통합은 으로의 마이그레이션을 계획하는 데 도움이 됩니다. AWS 클라우드데이터베이스 및 분석 데이터 수집 모듈을 사용하여 사용자 환경의 데이터베이스 및 분석 서버를 검색하고 마이그레이션할 서버의 인벤토리를 구축할 수 AWS 클라우드있습니다. 이 데이터 수집 모듈은 데이터베이스 메타데이터와 CPU, 메모리, 디스크 용량의 실제 사용률 지표를 수집합니다. 이러한 지표를 수집한 후 AWS DMS 콘솔을 사용하여 원본 데이터베이스에 대한 대상 권장 사항을 생성할 수 있습니다.

주제

에이전트리스 컬렉터 시작하기

이 섹션에서는 Application Discovery Service 에이전트리스 컬렉터 (Agentless Collector) 를 사용하여 시작하는 방법에 대해 설명합니다.

토픽

에이전트 없는 컬렉터의 사전 요구 사항

Application Discovery Service 에이전트리스 컬렉터 (에이전트 없는 컬렉터) 를 사용하기 위한 사전 요구 사항은 다음과 같습니다.

- 하나 이상의 계정. AWS
- AWS Migration Hub홈 지역이 설정된 AWS 계정 (참조)Migration Hub 콘솔에 로그인하고 홈 지역을 선택합니다.. Migration Hub 데이터는 검색, 계획 및 마이그레이션 추적 목적으로 홈 지역에 저장됩니다.
- AWS관리형 정책을 `AWSApplicationDiscoveryAgentlessCollectorAccess` 사용하도록 설정된 AWS 계정 IAM 사용자. 데이터베이스 및 분석 데이터 수집 모듈을 사용하려면 이 IAM 사용자는 두 개의 고객 관리형 IAM 정책 및 도 사용해야 합니다. `DMSCollectorPolicy` `FleetAdvisorS3Policy` 자세히 알아보려면 1단계: 에이전트리스 컬렉터용 IAM 사용자 생성의 내용을 참조하세요. IAM 사용자는 Migration Hub 홈 지역이 설정된 AWS 계정에서 생성해야 합니다.
- VMware vCenter Server V5.5, V6, V6.5, 6.7 또는 7.0.

> **Note**
>
> 에이전트리스 컬렉터는 이러한 VMware 버전을 모두 지원하지만 현재는 버전 6.7 및 7.0을 기준으로 테스트하고 있습니다.

- VMware vCenter Server 설정의 경우 시스템 그룹에 대해 설정된 읽기 및 보기 권한으로 vCenter 자격 증명을 제공할 수 있는지 확인하십시오.
- 에이전트가 없는 컬렉터에는 TCP 포트 443을 통해 여러 도메인에 대한 아웃바운드 액세스가 필요합니다. AWS 이러한 도메인 목록은 을 참조하십시오. 도메인에 대한 아웃바운드 액세스를 AWS 위한 방화벽을 구성합니다.
- 데이터베이스 및 분석 데이터 수집 모듈을 사용하려면 Migration Hub 홈 지역으로 설정한 곳에 Amazon S3 버킷을 생성하십시오. AWS 리전 데이터베이스 및 분석 데이터 수집 모듈은 이 Amazon S3 버킷에 인벤토리 메타데이터를 저장합니다. 자세한 내용은 Amazon S3 사용 설명서의 버킷 생성을 참조하십시오.

도메인에 대한 아웃바운드 액세스를 AWS 위한 방화벽을 구성합니다.

네트워크에서의 아웃바운드 연결이 제한되는 경우 Agentless Collector에 필요한 AWS 도메인에 대한 아웃바운드 액세스를 허용하도록 방화벽 설정을 업데이트해야 합니다. 아웃바운드 액세스가 필요한 AWS 도메인은 Migration Hub 홈 지역이 미국 서부 (오레곤) 지역인지, us-west-2 지역인지에 따라 달라집니다.

계정 홈 지역이 us-west-2인 경우 다음 도메인에는 아웃바운드 액세스가 필요합니다. AWS

- `arsenal-discovery.us-west-2.amazonaws.com`— 컬렉터는 이 도메인을 사용하여 필수 IAM 사용자 자격 증명으로 구성되었는지 확인합니다. 홈 지역이 us-west-2이므로 수집기는 수집된 데이터를 전송 및 저장하는 데에도 이를 사용합니다.
- `migrationhub-config.us-west-2.amazonaws.com`— 수집자는 이 도메인을 사용하여 제공된 IAM 사용자 자격 증명을 기반으로 수집기가 데이터를 보내는 홈 지역을 결정합니다.
- `api.ecr-public.us-east-1.amazonaws.com`— 컬렉터는 이 도메인을 사용하여 사용 가능한 업데이트를 검색합니다.
- `public.ecr.aws`— 컬렉터는 이 도메인을 사용하여 업데이트를 다운로드합니다.
- `dms.`*`your-migrationhub-home-region`*`.amazonaws.com`— 수집기는 이 도메인을 사용하여 AWS DMS 데이터 수집기에 연결합니다.

- `s3.amazonaws.com`— 수집기는 이 도메인을 사용하여 데이터베이스 및 분석 데이터 수집 모듈에서 수집한 데이터를 Amazon S3 버킷에 업로드합니다.

AWS계정 홈 지역이 아닌 **`us-west-2`** 경우 다음 도메인에는 아웃바운드 액세스가 필요합니다.

- `arsenal-discovery.us-west-2.amazonaws.com`— 수집기는 이 도메인을 사용하여 필수 IAM 사용자 자격 증명으로 구성되었는지 확인합니다.
- `arsenal-discovery.`*`your-migrationhub-home-region`*`.amazonaws.com`— 수집기는 수집된 데이터를 보내고 저장하는 데 이 도메인을 사용합니다.
- `migrationhub-config.us-west-2.amazonaws.com`— 수집기는 이 도메인을 사용하여 제공된 IAM 사용자 자격 증명을 기반으로 수집자가 데이터를 전송해야 하는 홈 지역을 결정합니다.
- `api.ecr-public.us-east-1.amazonaws.com`— 컬렉터는 이 도메인을 사용하여 사용 가능한 업데이트를 검색합니다.
- `public.ecr.aws`— 컬렉터는 이 도메인을 사용하여 업데이트를 다운로드합니다.
- `dms.`*`your-migrationhub-home-region`*`.amazonaws.com`— 수집기는 이 도메인을 사용하여 AWS DMS 데이터 수집기에 연결합니다.
- `s3.amazonaws.com`— 수집기는 이 도메인을 사용하여 데이터베이스 및 분석 데이터 수집 모듈에서 수집한 데이터를 Amazon S3 버킷에 업로드합니다.

Agentless Collector를 설정할 때 설치 실패 (자격 증명을 확인하고 다시 시도하지 않으면 연결할 수 AWS 없음) 와 같은 오류가 발생할 수 있습니다. 네트워크 설정을 확인하십시오. 이러한 오류는 Agentless Collector가 아웃바운드 액세스가 필요한 AWS 도메인 중 하나에 HTTPS 연결을 설정하지 못했기 때문에 발생할 수 있습니다.

연결을 설정할 AWS 수 없는 경우 Agentless Collector는 온-프레미스 환경에서 데이터를 수집할 수 없습니다. 연결을 수정하는 방법에 대한 자세한 내용은 을 참조하십시오. AWS 설치 중에 에이전트리스 컬렉터에 연결할 수 없는 문제 해결 AWS

1단계: 에이전트리스 컬렉터용 IAM 사용자 생성

에이전트리스 컬렉터를 사용하려면 사용한 AWS 계정에서 (AWS Identity and Access ManagementIAM) Migration Hub 콘솔에 로그인하고 홈 지역을 선택합니다. 사용자를 생성해야 합니다. 그런 다음 이 IAM 사용자가 다음 관리형 정책을 사용하도록 설정합니다. AWS AWSApplicationDiscoveryAgentlessCollectorAccess IAM 사용자를 생성할 때 이 IAM 정책을 연결합니다.

데이터베이스 및 분석 데이터 수집 모듈을 사용하려면 고객 관리형 IAM 정책을 두 개 생성하십시오. 이러한 정책은 Amazon S3 버킷과 AWS DMS API에 대한 액세스를 제공합니다. 자세한 내용은 IAM 사용 설명서의 고객 관리형 정책 생성을 참조하십시오.

- 다음 JSON 코드를 사용하여 정책을 생성합니다. **DMSCollectorPolicy**

```
{
 "Version": "2012-10-17",
 "Statement": [{
  "Effect": "Allow",
  "Action": [
   "dms:DescribeFleetAdvisorCollectors",
   "dms:ModifyFleetAdvisorCollectorStatuses",
   "dms:UploadFileMetadataList"
  ],
  "Resource": "*"
 }]
}
```

- 다음 JSON 코드를 사용하여 정책을 생성합니다. **FleetAdvisorS3Policy**

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "s3:GetObject*",
                "s3:GetBucket*",
                "s3:List*",
                "s3:DeleteObject*",
                "s3:PutObject*"
            ],
            "Resource": [
                "arn:aws:s3:::bucket_name",
                "arn:aws:s3:::bucket_name/*"
            ]
        }
    ]
}
```

위 예제에서는 사전 요구 사항 단계에서 생성한 Amazon S3 버킷의 이름으로 *bucket_name* 대체합니다.

관리자가 아닌 IAM 사용자를 생성하여 에이전트 없는 Collector와 함께 사용하는 것이 좋습니다. 관리자가 아닌 IAM 사용자를 생성할 때는 최소 권한 부여 보안 모범 사례를 따라 사용자에게 최소 권한을 부여하십시오.

에이전트리스 컬렉터와 함께 사용할 비관리자 IAM 사용자를 만들려면

1. 에서 AWS Management Console 홈 지역을 설정하는 데 사용한 AWS 계정을 사용하여 IAM 콘솔로 이동합니다. Migration Hub 콘솔에 로그인하고 홈 지역을 선택합니다.
2. IAM 사용 설명서의 AWS계정에 IAM 사용자 생성에 설명된 대로 콘솔을 사용하여 사용자를 생성하는 지침을 따라 관리자가 아닌 IAM 사용자를 생성합니다.

   IAM 사용 설명서의 지침을 따르는 동안:

   - 액세스 유형을 선택하는 단계에서 프로그래밍 액세스를 선택합니다. 참고, 권장되지는 않지만 콘솔에 액세스할 때 동일한 IAM 사용자 자격 증명을 사용하려는 경우에만 AWS Management Console 액세스를 선택하십시오. AWS
   - 권한 설정 페이지에 대한 단계에서 기존 정책을 사용자에게 직접 연결하는 옵션을 선택하십시오. 그런 다음 정책 목록에서 `AWSApplicationDiscoveryAgentlessCollectorAccess` AWS 관리형 정책을 선택합니다.

     다음으로 `FleetAdvisorS3Policy` 고객 관리형 IAM 정책을 선택합니다. `DMSCollectorPolicy`
   - 사용자의 액세스 키 (액세스 키 ID 및 보안 액세스 키) 를 보는 단계를 진행하려면 사용자의 새 액세스 키 ID와 보안 액세스 키를 안전한 장소에 저장하는 것에 관한 중요 참고 사항의 지침을 따르십시오. 이 액세스 키를 입력해야 합니다5단계: 에이전트리스 컬렉터 구성.

     액세스 키를 교체하는 것이 AWS 보안 모범 사례입니다. 키 교체에 대한 자세한 내용은 IAM User Guide의 장기 자격 증명이 필요한 사용 사례를 위해 정기적으로 액세스 키를 교체하는 내용을 참조하십시오.

2단계: 에이전트리스 컬렉터 다운로드

Application Discovery Service 에이전트 없는 수집기 (에이전트 없는 수집기) 를 설정하려면 에이전트 없는 수집기 OVA (개방형 가상화 아카이브) 파일을 다운로드하여 배포해야 합니다. 에이전트리스 컬

렉터는 온프레미스 VMware 환경에 설치하는 가상 어플라이언스입니다. 이 단계에서는 컬렉터 OVA 파일을 다운로드하는 방법을 설명하고 다음 단계에서는 이를 배포하는 방법을 설명합니다.

컬렉터 OVA 파일을 다운로드하고 체크섬을 확인하려면

1. vCenter에 VMware 관리자로 로그인하고 에이전트리스 컬렉터 OVA 파일을 다운로드할 디렉토리로 전환합니다.
2. 다음 URL에서 OVA 파일을 다운로드합니다.

   에이전트리스 컬렉터 OVA
3. 시스템 환경의 해싱 알고리즘에 따라 MD5나 SHA256을 다운로드해서 체크섬 값이 포함된 파일을 얻습니다. 다운로드한 값을 사용하여 이전 단계에서 다운로드한 `ApplicationDiscoveryServiceAgentlessCollector` 파일을 확인합니다.
4. Linux 버전에 따라 해당 MD5 명령 또는 SHA256 명령을 실행하여 `ApplicationDiscoveryServiceAgentlessCollector.ova` 파일의 암호화 서명이 다운로드한 해당 MD5/SHA256 파일의 값과 일치하는지 확인합니다.

```
$ md5sum ApplicationDiscoveryServiceAgentlessCollector.ova
```

```
$ sha256sum ApplicationDiscoveryServiceAgentlessCollector.ova
```

3단계: 에이전트리스 컬렉터 배포

Application Discovery Service 에이전트리스 컬렉터 (에이전트리스 컬렉터) 는 온프레미스 VMware 환경에 설치하는 가상 어플라이언스입니다. 이 섹션에서는 이전 단계에서 다운로드한 OVA (오픈 가상화 아카이브) 파일을 VMware 환경에 배포하는 방법을 설명합니다.

에이전트리스 컬렉터 가상 시스템 사양

- 운영 체제 — 아마존 리눅스 2
- RAM — 16GB
- CPU — 4코어

다음 절차는 VMware 환경에 에이전트리스 컬렉터 OVA 파일을 배포하는 단계를 안내합니다.

에이전트리스 컬렉터를 배포하려면

1. vCenter에 VMware 관리자로 로그인합니다.
2. 다음 방법 중 하나를 사용하여 OVA 파일을 설치합니다.
   - UI 사용: 파일을 선택하고 OVF 템플릿 배포를 선택한 다음 이전 섹션에서 다운로드한 컬렉터 OVA 파일을 선택한 다음 마법사를 완료하십시오.
   - 명령줄 사용: 명령줄에서 컬렉터 OVA 파일을 설치하려면 VMware 개방형 가상화 형식 도구 (ovftool) 를 다운로드하여 사용하십시오. ovftool을 다운로드하려면 OVF 도구 설명서 페이지에서 릴리스를 선택합니다.

     다음은 ovftool 명령줄 도구를 사용하여 컬렉터 OVA 파일을 설치하는 예제입니다.

     ```
     ovftool --acceptAllEulas --name=AgentlessCollector --datastore=datastore1
      -dm=thin ApplicationDiscoveryServiceAgentlessCollector.ova
      'vi://username:password@vcenterurl/Datacenter/host/esxi/'
     ```

     다음은 예제에서 **## ###** 값을 설명합니다.

     - 이름은 에이전트리스 Collector VM에 사용할 이름입니다.
     - 데이터스토어는 vCenter에 있는 데이터스토어의 이름입니다.
     - OVA 파일 이름은 다운로드한 컬렉터 OVA 파일의 이름입니다.
     - 사용자 이름/암호는 vCenter 자격 증명입니다.
     - vcenterurl은 vCenter의 URL입니다.
     - vi 경로는 VMware ESXi 호스트의 경로입니다.
3. vCenter에서 배포된 에이전트 없는 컬렉터를 찾으십시오. VM을 마우스 오른쪽 버튼으로 클릭한 다음 전원, 전원 켜기를 선택합니다.
4. 몇 분 후 vCenter에 컬렉터의 IP 주소가 표시됩니다. 이 IP 주소를 사용하여 컬렉터에 연결합니다.

4단계: 에이전트리스 컬렉터 콘솔 액세스

다음 절차는 Application Discovery Service 에이전트리스 컬렉터 (Agentless Collector) 콘솔에 액세스하는 방법을 설명합니다.

에이전트리스 컬렉터 콘솔에 액세스하려면

1. 웹 브라우저를 열고 주소 표시줄에 다음 **https://**/URL을 입력합니다. 이 <ip_address><ip_address>URL은 컬렉터의 IP 주소입니다. 3단계: 에이전트리스 컬렉터 배포
2. 에이전트리스 컬렉터에 처음 액세스할 때는 [시작하기] 를 선택합니다. 그러면 로그인하라는 메시지가 표시됩니다.

에이전트리스 컬렉터 콘솔에 처음 액세스하는 경우, 다음으로 접속하세요. 5단계: 에이전트리스 컬렉터 구성 그렇지 않으면 다음에 볼 수 있습니다. 에이전트리스 컬렉터 대시보드

5단계: 에이전트리스 컬렉터 구성

Application Discovery Service 에이전트리스 컬렉터 (Agentless Collector) 는 아마존 리눅스 2 기반 가상 머신 (VM) 입니다. 다음 섹션에서는 에이전트리스 컬렉터 콘솔의 에이전트리스 컬렉터 구성 페이지에서 컬렉터 VM을 구성하는 방법을 설명합니다.

에이전트리스 컬렉터 구성 페이지에서 컬렉터 VM을 구성하려면

1. 컬렉터 이름에는 컬렉터를 식별할 수 있는 컬렉터 이름을 입력합니다. 이름에는 공백이 포함될 수 있지만 특수 문자는 포함할 수 없습니다.
2. 데이터 동기화에서 수집기가 검색한 데이터를 수신할 대상 계정으로 지정할 AWS 계정 IAM 사용자의 AWS 액세스 키와 비밀 키를 입력합니다. IAM 사용자의 요구 사항에 대한 자세한 내용은 을 참조하십시오. 1단계: 에이전트리스 컬렉터용 IAM 사용자 생성

    a. AWSaccess-key에는 대상 계정으로 지정하는 AWS 계정 IAM 사용자의 액세스 키를 입력합니다.

    b. AWSsecret-key의 경우 대상 계정으로 지정하려는 AWS 계정 IAM 사용자의 비밀 키를 입력합니다.

    c. (선택 사항) 네트워크에 액세스하기 위해 프록시를 사용해야 하는 경우 프록시 호스트AWS, 프록시 포트 및 기존 프록시 서버 인증에 필요한 자격 증명 (선택 사항) 을 입력합니다.
3. 에이전트 없는 컬렉터 암호에서 에이전트 없는 Collector에 대한 액세스를 인증하는 데 사용할 비밀번호를 설정합니다.

    - 비밀번호는 대소문자를 구분합니다.
    - 비밀번호는 8~64자 길이여야 합니다.
    - 암호는 각각의 다음 네 가지 범주의 문자를 최소 1자씩 포함해야 합니다.
        - 소문자(a~z)

- 대문자(A-Z)
- 숫자(0-9)
- 영숫자 이외의 문자 (@$! #%*? &)

- 비밀번호는 다음 문자 이외의 특수 문자를 포함할 수 없습니다. @$! #%*? &

a. 에이전트리스 컬렉터 암호의 경우 컬렉터에 대한 액세스를 인증하는 데 사용할 비밀번호를 입력합니다.

b. 에이전트 없는 컬렉터 암호를 다시 입력하려면 암호를 다시 입력하십시오.

4. 기타 설정에서 사용권 계약을 읽어보십시오. 동의하는 경우 확인란을 선택합니다.
5. 에이전트 없는 Collector에 대한 자동 업데이트를 활성화하려면 기타 설정에서 에이전트 없는 Collector의 자동 업데이트를 선택합니다. 이 확인란을 선택하지 않으면 에 설명된 대로 에이전트 없는 Collector를 수동으로 업데이트해야 합니다. 에이전트리스 컬렉터 수동 업데이트
6. 구성 저장을 선택합니다.

다음 항목에서는 선택적 컬렉터 구성 작업에 대해 설명합니다.

선택적 구성 작업

- (선택 사항) 에이전트리스 컬렉터 VM의 고정 IP 주소 구성
- (선택 사항) 에이전트리스 컬렉터 VM을 DHCP를 사용하도록 다시 재설정합니다.
- (선택 사항) Kerberos 인증 프로토콜을 구성합니다.

(선택 사항) 에이전트리스 컬렉터 VM의 고정 IP 주소 구성

다음 단계는 Application Discovery Service 에이전트리스 컬렉터 (에이전트리스 컬렉터) VM의 고정 IP 주소를 구성하는 방법을 설명합니다. 컬렉터 VM은 처음 설치될 때 동적 호스트 구성 프로토콜 (DHCP)을 사용하도록 구성됩니다.

> **Note**
>
> 에이전트리스 컬렉터는 IPv4를 지원합니다. IPv6는 지원하지 않습니다.

컬렉터 VM의 고정 IP 주소를 구성하려면

1. VMware vCenter에서 다음 네트워크 정보를 수집합니다.

- 고정 IP 주소 - 서브넷의 서명되지 않은 IP 주소입니다. 예를 들어 192.168.1.138을 예로 들 수 있습니다.
- 네트워크 마스크 - 컬렉터 VM을 호스팅하는 VMware vCenter 호스트의 IP 주소 설정을 확인하여 확인할 수 있습니다. 예를 들어 255.255.255.0이 이에 해당합니다.
- 기본 게이트웨이 - 컬렉터 VM을 호스팅하는 VMware vCenter 호스트의 IP 주소 설정을 확인하여 확인할 수 있습니다. 예를 들어, 192.168.1.1입니다.
- 기본 DNS - 컬렉터 VM을 호스팅하는 VMware vCenter 호스트의 IP 주소 설정을 확인하여 확인할 수 있습니다. 예를 들면 192.168.1.1입니다.
- (선택 사항) 보조 DNS
- (선택 사항) 로컬 도메인 이름 - 이렇게 하면 수집기가 도메인 이름 없이 vCenter 호스트 URL에 연결할 수 있습니다.

2. 컬렉터의 VM 콘솔을 열고 다음 예와 **`collector`** 같이 암호를 **`ec2-user`** 사용하여 로그인합니다.

```
username: ec2-user
password: collector
```

3. 원격 터미널에 다음 명령을 입력하여 네트워크 인터페이스를 비활성화합니다.

```
sudo /sbin/ifdown eth0
```

4. 다음 단계를 사용하여 인터페이스 eth0 구성을 업데이트합니다.

   a. 다음 명령을 사용하여 vi 편집기에서 ifcfg-eth0을 엽니다.

   ```
   sudo vi /etc/sysconfig/network-scripts/ifcfg-eth0
   ```

   b. 네트워크 정보 수집 단계에서 수집한 정보로 다음 예와 같이 인터페이스 값을 업데이트합니다.

   ```
   DEVICE=eth0
   BOOTPROTO=static
   ONBOOT=yes
   IPADDR=static-ip-value
   NETMASK=netmask-value
   GATEWAY=gateway-value
   TYPE=Ethernet
   ```

```
USERCTL=yes
PEERDNS=no
RES_OPTIONS="timeout:2 attempts:5"
```

5. 다음 단계를 사용하여 도메인 이름 시스템 (DNS) 을 업데이트하십시오.

   a. 다음 명령을 사용하여 vi에서 `resolv.conf` 파일을 엽니다.

   ```
   sudo vi /etc/resolv.conf
   ```

   b. 다음 명령을 사용하여 vi에서 `resolv.conf` 파일을 업데이트합니다.

   ```
   search localdomain-name
   options timeout:2 attempts:5
   nameserver dnsserver-value
   ```

   다음 예제는 편집된 `resolv.conf` 파일을 보여줍니다.

   ```
   search vsphere.local
   options timeout:2 attempts:5
   nameserver 192.168.1.1
   ```

6. 다음 명령을 입력하여 네트워크 인터페이스를 활성화합니다.

   ```
   sudo /sbin/ifup eth0
   ```

7. 다음 예와 같이 VM을 재부팅합니다.

   ```
   sudo reboot
   ```

8. 다음 단계를 사용하여 네트워크 설정을 확인합니다.

   a. 다음 명령을 입력하여 IP 주소가 올바르게 구성되었는지 확인합니다.

   ```
   ifconfig

   ip addr show
   ```

   b. 다음 명령을 입력하여 게이트웨이가 올바르게 추가되었는지 확인합니다.

   ```
   route -n
   ```

출력은 다음 예와 비슷해야 합니다.

```
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
0.0.0.0         192.168.1.1     0.0.0.0         UG    0      0        0 eth0
172.17.0.0      0.0.0.0         255.255.0.0     U     0      0        0 docker0
192.168.1.0     0.0.0.0         255.255.255.0   U     0      0
```

c. 다음 명령을 입력하여 공개 URL을 ping할 수 있는지 확인합니다.

```
ping www.google.com
```

d. 다음 예와 같이 vCenter IP 주소 또는 호스트 이름을 ping할 수 있는지 확인합니다.

```
ping vcenter-host-url
```

(선택 사항) 에이전트리스 컬렉터 VM을 DHCP를 사용하도록 다시 재설정합니다.

다음 단계는 DHCP를 사용하도록 에이전트가 없는 수집기 VM을 재구성하는 방법을 설명합니다.

DHCP를 사용하도록 컬렉터 VM을 구성하려면

1. 원격 터미널에 다음 명령을 입력하여 네트워크 인터페이스를 비활성화합니다.

```
sudo /sbin/ifdown eth0
```

2. 다음 단계를 사용하여 네트워크 구성을 업데이트하십시오.

a. 다음 명령을 사용하여 vi 편집기에서 `ifcfg-eth0` 파일을 엽니다.

```
sudo /sbin/ifdown eth0
```

b. 다음 예와 같이 `ifcfg-eth0` 파일의 값을 업데이트합니다.

```
DEVICE=eth0
BOOTPROTO=dhcp
ONBOOT=yes
TYPE=Ethernet
USERCTL=yes
PEERDNS=yes
```

```
DHCPV6C=yes
DHCPV6C_OPTIONS=-nw
PERSISTENT_DHCLIENT=yes
RES_OPTIONS="timeout:2 attempts:5"
```

3. 다음 명령을 입력하여 DNS 설정을 재설정합니다.

```
echo "" | sudo tee /etc/resolv.conf
```

4. 다음 명령을 입력하여 네트워크 인터페이스를 활성화합니다.

```
sudo /sbin/ifup eth0
```

5. 다음 예와 같이 컬렉터 VM을 재부팅합니다.

```
sudo reboot
```

(선택 사항) Kerberos 인증 프로토콜을 구성합니다.

OS 서버가 Kerberos 인증 프로토콜을 지원하는 경우 이 프로토콜을 사용하여 서버에 연결할 수 있습니다. 이렇게 하려면 Application Discovery Service 에이전트리스 컬렉터 VM을 구성해야 합니다.

다음 단계는 Application Discovery Service 에이전트리스 컬렉터 VM에서 Kerberos 인증 프로토콜을 구성하는 방법을 설명합니다.

컬렉터 VM에 Kerberos 인증 프로토콜을 구성하려면

1. 컬렉터의 VM 콘솔을 열고 다음 예와 **`collector`** 같이 비밀번호를 **`ec2-user`** 사용하여 로그인합니다.

```
username: ec2-user
password: collector
```

2. `/etc`폴더에서 `krb5.conf` 구성 파일을 엽니다. 이렇게 하려면 다음 코드 예제를 사용할 수 있습니다.

```
cd /etc
sudo nano krb5.conf
```

3. 다음 정보로 `krb5.conf` 구성 파일을 업데이트하십시오.

```
[libdefaults]
    forwardable = true
    dns_lookup_realm = true
    dns_lookup_kdc = true
    ticket_lifetime = 24h
    renew_lifetime = 7d
    default_realm = default_Kerberos_realm

[realms]
 default_Kerberos_realm = {
     kdc = KDC_hostname
     server_name = server_hostname
     default_domain = domain_to_expand_hostnames
 }

[domain_realm]
 .domain_name = default_Kerberos_realm
 domain_name = default_Kerberos_realm
```

파일을 저장하고 텍스트 편집기를 종료합니다.

4. 다음 예와 같이 컬렉터 VM을 재부팅합니다.

```
sudo reboot
```

6단계: 에이전트리스 컬렉터 데이터 수집 모듈 설정

Application Discovery Service 에이전트리스 컬렉터 (Agentless Collector) 콘솔 대시보드 페이지의 데이터 수집에서 서버의 인벤토리, 프로필 및 사용률 데이터를 수집하도록 데이터 수집 모듈을 설정합니다.

에이전트리스 컬렉터는 현재 VMware VM과 데이터베이스 및 분석 서버에서의 데이터 수집을 지원합니다. 향후 모듈에서는 추가 가상화 플랫폼에서의 수집 및 운영 체제 수준 수집을 지원할 예정입니다.

토픽

- VMware vCenter 에이전트리스 컬렉터 데이터 수집 모듈
- 데이터베이스 및 분석 데이터 수집 모듈

VMware vCenter 에이전트리스 컬렉터 데이터 수집 모듈

이 섹션에서는 VMware VM에서 서버 인벤토리, 프로필 및 사용률 데이터를 수집하는 데 사용되는 Application Discovery Service 에이전트리스 컬렉터 (Agentless Collector) VMware vCenter 데이터 수집 모듈에 대해 설명합니다.

주제

VMware vCenter용 에이전트리스 컬렉터 데이터 수집 모듈을 설정하는 방법

이 섹션에서는 VMware VM에서 서버 인벤토리, 프로필 및 사용률 데이터를 수집하도록 에이전트리스 Collector VMware vCenter 데이터 수집 모듈을 설정하는 방법을 설명합니다.

> **Note**
>
> vCenter 설정을 시작하기 전에 시스템 그룹에 설정된 읽기 및 보기 권한이 있는 vCenter 자격 증명을 제공할 수 있는지 확인하십시오.

VMware vCenter 데이터 수집 모듈을 설정하려면

1. 에이전트리스 컬렉터 대시보드 페이지의 데이터 수집에서 VMware vCenter 섹션에서 설정을 선택합니다.
2. VMware vCenter 데이터 수집 설정 페이지에서 다음을 수행하십시오.
   a. vCenter 자격 증명 아래에서:
      i. vCenter URL/IP의 경우 VMware vCenter 서버 호스트의 IP 주소를 입력합니다.
      ii. vCenter 사용자 이름에는 수집기가 vCenter와 통신하는 데 사용하는 로컬 또는 도메인 사용자의 이름을 입력합니다. 도메인 사용자의 경우 domain\username 또는 username@domain 형식을 사용합니다.
      iii. vCenter 암호에 로컬 또는 도메인 사용자 암호를 입력합니다.
   b. 데이터 수집 기본 설정에서:

- 성공적으로 설정한 후 즉시 자동으로 데이터 수집을 시작하려면 자동으로 데이터 수집 시작을 선택합니다.

c. Set up(설정)을 선택합니다.

다음으로 다음 항목에서 설명하는 VMware 데이터 수집 세부 정보 페이지가 표시됩니다.

VM웨어 데이터 수집 세부 정보 데이터 수집 데이터 수집 세부 정보 중지

VMware 데이터 수집 세부 정보 페이지에는 설정한 vCenter에 대한 세부 정보가 표시됩니다VMware vCenter용 에이전트리스 컬렉터 데이터 수집 모듈을 설정하는 방법.

검색된 vCenter 서버에는 설정한 vCenter가 vCenter에 대한 다음 정보와 함께 나열됩니다.

- vCenter 서버의 IP 서버의 IP 서버의 IP IP 서버의 IP IP IP 서버의 IP IP IP IP
- vCenter의 서버 수입니다.
- 데이터 수집 상태입니다.
- 마지막 업데이트 이후 얼마나 지났어요.

표시된 vCenter 서버를 제거하고 VMware vCenter 데이터 수집 설정 페이지로 돌아가려면 vCenter 서버 제거를 선택합니다.

데이터 수집을 자동으로 시작하도록 선택하지 않은 경우 이 페이지의 데이터 수집 시작 단추를 사용하여 데이터 수집을 시작할 수 있습니다. 데이터 수집이 시작되면 시작 버튼이 데이터 수집 중지로 바뀝니다.

컬렉션 상태 열에 수집이 표시되면 데이터 수집이 시작된 것입니다.

수집된 데이터는AWS Migration Hub 콘솔에서 볼 수 있습니다. VMware vCenter Server 인벤토리에 대한 데이터를 수집하는 경우 데이터 수집을 설정한 후 약 15분 후에 콘솔에 나타나는 데이터에 액세스할 수 있습니다.

인터넷 액세스가 차단되지 않은 경우 이 페이지에서 Migration Hub에서 서버 보기를 선택하여 Migration Hub 콘솔을 열 수 있습니다. 이 버튼의 선택 여부에 관계없이 Migration Hub 콘솔에 액세스하는 방법에 대한 자세한 내용은 을 참조하십시오7단계: 수집된 데이터 보기.

다음은 마이그레이션 계획 활동에 따른 권장 데이터 수집 기간에 대한 지침입니다.

- TCO (총 소유 비용) - 2~4주
- 마이그레이션 계획 - 2~6주

vCenter 데이터 수집 범위 제어

vCenter 사용자는 Application Discovery Service 사용하여 인벤토리를 작성하려면 각 ESX 호스트 또는 VM에 대한 읽기 전용 권한이 필요합니다. 권한 설정을 이용해 데이터 수집에 어떤 호스트와 VM을 포함시킬지 제어할 수 있습니다. 현재 vCenter의 모든 호스트 및 VM의 인벤토리를 허용하거나 권한을 case-by-case 기준으로 부여할 수 있습니다.

> **Note**
>
> 보안의 모범 사례로 Application Discovery Service vCenter 사용자에게 불필요한 추가 권한을 부여하지 않는 것이 가장 좋습니다.

다음 절차는 세분화 수준이 가장 낮은 순서에서 높은 순서로 구성 시나리오를 설명합니다. 이러한 절차는 vSphere 클라이언트 v6.7.0.2에 대한 것입니다. 다른 버전의 클라이언트에 대한 절차는 사용 중인 vSphere Client의 버전에 따라 다를 수 있습니다.

현재 vCenter에 속한 모든 ESX 호스트와 VM에 대한 데이터를 검색하려면

1. VMware vSphere 클라이언트에서 [vCenter]를 선택한 후 [Hosts and Clusters] 또는 [VMs and Templates]를 선택합니다.
2. 데이터센터 리소스를 선택한 다음 권한을 선택합니다.
3. vCenter 사용자를 선택한 다음 사용자 역할을 추가, 편집 또는 제거할 기호를 선택합니다.
4. 역할 메뉴에서 읽기 전용을 선택합니다.
5. [자녀에게 전달] 을 선택한 다음 [확인] 을 선택합니다.

특정 ESX 호스트와 모든 하위 객체에 대한 데이터를 검색하려면

1. VMware vSphere 클라이언트에서 [vCenter]를 선택한 후 [Hosts and Clusters] 또는 [VMs and Templates]를 선택합니다.
2. [Related Objects], [Hosts]를 선택합니다.
3. 호스트 이름에 대한 컨텍스트(오른쪽 클릭) 메뉴를 열고 [All vCenter Actions], [Add Permission]을 선택합니다.
4. [Add Permission]에서 호스트에 vCenter 사용자를 추가합니다. [Assigned Role]에서 [Read-only]를 선택합니다.
5. [Propagate to children], [OK]를 선택합니다.

특정 ESX 호스트 또는 하위 VM에 대한 데이터를 검색하려면

1. VMware vSphere 클라이언트에서 [vCenter]를 선택한 후 [Hosts and Clusters] 또는 [VMs and Templates]를 선택합니다.
2. [Related Objects]를 선택합니다.
3. [Hosts](vCenter에 알려진 ESX 호스트 목록 표시) 또는 [Virtual Machines](모든 ESX 호스트에 걸친 VM 목록 표시)를 선택합니다.
4. 호스트 또는 VM 이름에 대한 컨텍스트(오른쪽 클릭) 메뉴를 열고 [All vCenter Actions], [Add Permission]을 선택합니다.
5. [Add Permission]에서 호스트 또는 VM에 vCenter 사용자를 추가합니다. [Assigned Role]에서 [Read-only]를 선택합니다.
6. 확인(OK)을 선택합니다.

> **Note**
>
> [하위 항목으로 전파] 를 선택한 경우에도 ESX 호스트 및 VM에서 읽기 전용 권한을case-by-case 개별적으로 제거할 수 있습니다. 이 옵션은 다른 ESX 호스트와 VM에 적용되는 상속된 권한에 영향을 미치지 않습니다.

데이터베이스 및 분석 데이터 수집 모듈

이 단원에서는 데이터베이스 및 분석 데이터 수집 모듈을 설정, 구성 및 사용하는 방법에 대해 설명합니다. 이 데이터 수집 모듈을 사용하여 데이터 환경에 연결하고 온프레미스 데이터베이스 및 분석 서버에서 메타데이터 및 성능 지표를 수집할 수 있습니다. 이 모듈에서 수집할 수 있는 지표에 대한 자세한 내용은 단원을 참조하세요Agentless Collector 데이터베이스 및 분석 데이터 수집 모듈에서 수집한 데이터.

데이터베이스 및 분석 데이터 수집 모듈을 사용할 때는 상위 수준에서 다음 단계를 수행해야 합니다.

1. 필수 단계를 완료하고, IAM 사용자를 구성하고,AWS DMS 데이터 수집기를 생성합니다.
2. 데이터 수집 모듈이 수집된 메타데이터 및 성능 메트릭을 로 전송할 수 있도록 데이터 전달을 구성하세요AWS.
3. LDAP 서버를 추가하고 이를 사용하여 데이터 환경에서 OS 서버를 검색합니다. 또는 OS 서버를 수동으로 추가하거나 를 사용하십시오VM웨어 데이터 수집 데이터 수집 모듈 데이터 수집 모듈 데이터 수집 모듈.

4. OS 서버에 대한 연결 자격 증명을 구성한 다음 이를 사용하여 데이터베이스 서버를 검색합니다.
5. 데이터베이스 및 분석 서버에 대한 연결 자격 증명을 구성한 다음 데이터 수집을 실행합니다. 자세한 정보는 데이터베이스 및 분석 데이터 수집을 참조하세요.
6. AWS DMS콘솔에서 수집된 데이터를 보고 이를 사용하여 마이그레이션을 위한 대상 권장 사항을 생성합니다AWS 클라우드. 자세한 정보는 데이터베이스 및 분석 데이터 수집을 참조하세요.

주제

- 지원되는 OS, 데이터베이스 및 분석 서버
- AWS DMS데이터 수집기 만들기
- 데이터 포워딩 설정
- LDAP 및 OS 서버 추가
- 데이터베이스 서버 살펴보기

지원되는 OS, 데이터베이스 및 분석 서버

에이전트리스 컬렉터의 데이터베이스 및 분석 데이터 수집 모듈은 Microsoft Active Directory LDAP 서버를 지원합니다.

이 데이터 수집 모듈은 다음 OS 서버를 지원합니다.

- Amazon Linux 2
- CentOS 리눅스 버전 6 이상
- De비안 안 안 안 안 안
- Red Hat Hat Hat Hat Hat Hat Hat을
- SUSE E E E USE E E E USE E E E E E E
- 우분투 버전 16.01 이상
- Windows Server ver ver ver ver ver ver ver ver
- 윈도우 XP 이상

또한 데이터베이스 및 분석 데이터 수집 모듈은 다음 데이터베이스 서버를 지원합니다.

- 마이크로소프트 SQL 서버 버전 2012 및 2019년까지
- MySQL SQL SQL
- 오라클 버전 11g 릴리스 2 및 최대 12c, 19c 및 21c

- PostgreSQL

AWS DMS데이터 수집기 만들기

데이터베이스 및 분석 데이터 수집 모듈은AWS DMS 데이터 수집기를 사용하여AWS DMS 콘솔과 상호 작용합니다. 수집된 데이터를AWS DMS 콘솔에서 보거나 이를 사용하여 적절한 크기의AWS 대상 엔진을 결정할 수 있습니다. 자세한 내용은 AWS DMSFleet Advisor 대상 권장 사항 기능 사용을 참조하십시오.

데이터 수집기를 생성하기 전에AWS DMS 데이터 수집기가 Amazon S3 버킷에 액세스하는 데 사용하는 IAM 역할을 생성하십시오.AWS DMS 에서 사전 요구 사항을 완료했을 때 이 Amazon S3 버킷을에이전트 없는 컬렉터의 사전 요구 사항 생성했습니다.

AWS DMS데이터 수집기가 Amazon S3에 액세스할 수 있도록 IAM 역할을 생성하려면

1. AWS Management Console에 로그인하여 https://console.aws.amazon.com/iam/에서 IAM 콘솔을 엽니다.
2. 탐색 창에서 역할을 선택한 후 역할 생성을 선택합니다.
3. 신뢰할 수 있는 엔티티 선택 페이지에서 신뢰할 수 있는 엔티티 유형에서AWS 서비스를 선택합니다. 다른AWS 서비스의 사용 사례에서 DMS를 선택합니다.
4. DMS 확인란을 선택하고 다음을 선택합니다.
5. 권한 추가 페이지에서 이전에 생성한 FleetAdvisorS3Policy를 선택합니다. 다음을 선택합니다.
6. 이름, 검토 및 생성 페이지에서 역할 이름을 입력한**`FleetAdvisorS3Role`** 다음 역할 생성을 선택합니다.
7. 생성한 역할을 열고 신뢰 관계 탭을 선택합니다. 신뢰 정책 편집(Edit trust policy)을 선택합니다.
8. 신뢰 정책 편집 페이지에서 다음 JSON을 편집기에 붙여넣고 기존 코드를 대체합니다.

```
{
 "Version": "2012-10-17",
 "Statement": [{
  "Sid": "",
  "Effect": "Allow",
  "Principal": {
   "Service": [
    "dms.amazonaws.com",
    "dms-fleet-advisor.amazonaws.com"
   ]
  },
```

```
  "Action": "sts:AssumeRole"
 }]
}
```

9. 정책 업데이트(Update policy)를 선택합니다.

이제AWS DMS 콘솔에서 데이터 수집기를 생성합니다.

AWS DMS데이터 수집기를 만들려면

1. AWS Management Console로그인하고 https://console.aws.amazon.com/dms/v2/ 에서AWS DMS 콘솔을 엽니다.
2. AWS 리전Migration Hub 홈 지역으로 설정한 지역을 선택합니다. 자세한 정보는 Migration Hub에 로그인하고 거주 지역을 선택하세요을 참조하세요.
3. 탐색 창의 디스커버에서 데이터 수집기를 선택합니다. 데이터 수집기 페이지가 열립니다.
4. 데이터 수집기 생성을 선택합니다. 데이터 수집기 만들기 페이지가 열립니다.
5. 일반 구성 섹션의 이름에 데이터 수집기의 이름을 입력합니다.
6. 연결 섹션에서 S3 찾아보기를 선택합니다. 이전에 만든 Amazon S3 버킷을 선택합니다.
7. IAM 역할의 경우 이전에`FleetAdvisorS3Role` 생성한 역할을 선택합니다.
8. 데이터 수집기 생성을 선택합니다.

데이터 포워딩 설정

필요한AWS 리소스를 생성한 후 데이터베이스 및 분석 데이터 수집 모듈에서AWS DMS 수집기로 데이터를 전달하도록 구성하십시오.

데이터 전달을 구성하려면

1. 에이전트리스 컬렉터 콘솔을 엽니다. 자세한 정보는 4단계: 컬렉터 콘솔 액세스을 참조하세요.
2. 데이터베이스 및 분석 컬렉터 보기를 선택합니다.
3. 대시보드 페이지의 데이터 전달 섹션에서 데이터 전달 구성을 선택합니다.
4. IAM 액세스 키 ID 및 IAM 보안 액세스 키의 경우 에이전트리스 컬렉터는 이전에 구성한 값을 사용합니다. AWS 리전 자세한 내용은 Migration Hub에 로그인하고 거주 지역을 선택하세요 및 1단계: IAM 사용자 생성 단원을 참조하세요.
5. Connected DMS 데이터 수집기의 경우AWS DMS 콘솔에서 생성한 데이터 수집기를 선택합니다.
6. 저장을 선택합니다.

데이터 전달을 구성한 후 대시보드 페이지의 데이터 전달 섹션을 확인하십시
오. 데이터베이스 및 분석 데이터 수집 모듈에 DMS 액세스 및 S3 액세스를 위한

연

결됨이 표시되는지 확인하십시오.

LDAP 및 OS 서버 추가

데이터베이스 및 분석 데이터 수집 모듈은 Microsoft Active Directory의 LDAP를 사용하여 네트워크의 OS, 데이터베이스 및 분석 서버에 대한 정보를 수집합니다. 경량 디렉터리 액세스 프로토콜 (LDAP) 은 개방형 표준 애플리케이션 프로토콜입니다. 이 프로토콜을 사용하여 IP 네트워크를 통해 분산 디렉터리 정보 서비스에 액세스하고 유지 관리할 수 있습니다.

기존 LDAP 서버를 데이터베이스 및 분석 데이터 수집 모듈에 추가하여 네트워크에서 OS 서버를 자동으로 검색할 수 있습니다. LDAP를 사용하지 않는 경우 OS 서버를 수동으로 추가할 수 있습니다.

데이터베이스 및 분석 데이터 수집 모듈에 LDAP 서버를 추가하려면

1. 에이전트리스 컬렉터 콘솔을 엽니다. 자세한 정보는 4단계: 컬렉터 콘솔 액세스을 참조하세요.
2. 데이터베이스 및 분석 컬렉터 보기를 선택한 다음 탐색 창의 Discovery에서 LDAP 서버를 선택합니다.
3. LDAP 서버 추가를 선택합니다. LDAP 서버 추가 페이지가 열립니다.
4. 호스트 이름에 LDAP 서버의 호스트 이름을 입력합니다.
5. 포트에 사용되는 포트 번호를 입력합니다.
6. 사용자 이름에 사용합니다.
7. 암호에 사용합니다.
8. (선택 사항) 연결 확인을 선택하여 LDAP 서버 자격 증명을 올바르게 추가했는지 확인합니다. 또는 나중에 LDAP 서버 페이지의 목록에서 LDAP 서버 연결 자격 증명을 확인할 수 있습니다.
9. LDAP 서버 추가를 선택합니다.
10. LDAP 서버 페이지의 목록에서 LDAP 서버를 선택하고 OS 서버 검색을 선택합니다.

> **Important**
>
> OS 검색을 위해서는 LDAP 프로토콜을 사용하여 요청을 실행할 도메인 서버의 데이터 수집 모듈에 대한 자격 증명이 필요합니다.

데이터베이스 및 분석 데이터 수집 모듈은 LDAP 서버에 연결하여 OS 서버를 검색합니다. 데이터 수집 모듈에서 OS 서버 검색을 완료한 후 OS 서버 보기를 선택하여 검색된 OS 서버 목록을 볼 수 있습니다.

또는 OS Server 을 직접 추가하거나 CSV (쉼표로 구분된 값) 파일에서 서버 목록을 가져올 수 있습니다. 또한 VMware vCenter 에이전트리스 컬렉터 데이터 수집 모듈을 사용하여 OS 서버를 검색할 수 있습니다. 자세한 정보는 VM웨어 데이터 수집 데이터 수집 모듈 데이터 수집 모듈 데이터 수집 모듈을 참조하세요.

데이터베이스 및 분석 데이터 수집 모듈에 OS 서버를 추가하려면

1. 데이터베이스 및 분석 컬렉터 페이지의 탐색 창의 Discovery에서 OS 서버를 선택합니다.
2. OS 서버 추가를 선택합니다. OS 서버 추가 페이지가 열립니다.
3. OS 서버 자격 증명을 입력합니다.

   a. OS 유형에서 서버의 운영 체제를 선택합니다.

   b. 호스트 이름/IP에 OS 서버의 호스트 이름 또는 IP 주소를 입력합니다.

   c. 포트에 사용되는 포트 번호를 입력합니다.

   d. 인증 유형에서 OS 서버에서 사용하는 인증 유형을 선택합니다.

   e. 사용자 이름에 사용합니다.

   f. 암호에 사용하는 암호를 입력합니다.

   g. 확인을 선택하여 OS 서버 자격 증명을 올바르게 추가했는지 확인하십시오.
4. (선택 사항) CSV 파일에서 여러 OS 서버를 추가합니다.

   a. CSV에서 OS 서버 대량 가져오기를 선택합니다.

   b. 템플릿 다운로드를 선택하여 사용자 지정할 수 있는 템플릿이 포함된 CSV 파일을 저장합니다.

   c. 템플릿에 따라 OS 서버의 연결 자격 증명을 파일에 입력합니다. 다음 예제에서는 CSV 파일에 OS 서버 연결 자격 증명을 제공하는 방법을 보여줍니다.

   ```
   OS type,Hostname/IP,Port,Authentication type,Username,Password
   Linux,192.0.2.0,22,Key-based authentication,USER-EXAMPLE,ANPAJ2UCCR6DPCEXAMPLE
   Windows,203.0.113.0,,NTLM,USER2-EXAMPLE,AKIAIOSFODNN7EXAMPLE
   ```

   모든 OS 서버의 자격 증명을 추가한 후 CSV 파일을 저장합니다.

   d. 찾아보기를 선택한 다음 CSV 파일을 선택합니다.
5. OS 서버 추가를 선택합니다.

6. 모든 OS 서버의 자격 증명을 추가한 후 OS 서버를 선택하고 데이터베이스 서버 검색을 선택합니다.

데이터베이스 서버 살펴보기

데이터베이스 검색을 위해서는 데이터 수집 모듈에 필요한 최소 권한으로 원본 데이터베이스의 사용자를 생성하십시오. 자세한 내용은 사용 설명서의 AWS DMSFleet Advisor용 데이터베이스AWS DMS 사용자 생성을 참조하십시오.

이전에 추가한 OS 서버에서 실행 중인 데이터베이스를 검색하려면 데이터 수집 모듈에서 운영 체제 및 데이터베이스 서버에 액세스할 수 있어야 합니다. 연결 설정에서 지정한 포트에서 데이터베이스에 액세스할 수 있는지 확인합니다. 그런 다음 데이터베이스 서버에서 원격 인증을 켜십시오. 이 외에도 데이터 수집 모듈에 다음과 같은 권한을 제공하십시오.

Windows에서 데이터베이스 서버를 검색하려면

1. Windows 관리 기기 (WMI) 및 WMI 쿼리 언어 (WQL) 쿼리를 실행하고 레지스트리를 읽을 수 있는 권한이 포함된 자격 증명을 제공합니다.
2. OS 서버 연결 자격 증명에 지정한 Windows 사용자를 분산 COM 사용자, 성능 로그 사용자, 성능 모니터 사용자 및 이벤트 로그 판독기 그룹에 추가합니다. 그러기 위해서는 다음 코드 예제를 사용하세요.

```
net localgroup "Distributed COM Users" username /ADD
net localgroup "Performance Log Users" username /ADD
net localgroup "Performance Monitor Users" username /ADD
net localgroup "Event Log Readers" username /ADD
```

   위 예에서 Windows Server ver ver ver ver 에 지정한 Windows Server 사용자 이름으로*username* 바꿉니다.
3. OS 서버 연결 자격 증명에 지정한 Windows 사용자에게 필요한 권한을 부여합니다.
   - Windows 관리 및 기기 속성에서 로컬 실행 및 원격 활성화를 선택합니다.
   - WMI Control의 경우, 및`WMI` 네임스페이스에 대한 실행 방법, 계정 활성화**`CIMV2`** **`DEFAULTStandartCimv2`**, 원격 사용 및 보안 읽기 권한을 선택합니다.
   - WMI 플러그인의 경우`winrm configsddl default` 실행한 다음 읽기 및 실행을 선택합니다.
4. 다음 코드 예제를 사용하여 Windows 호스트를 구성합니다.

```
netsh advfirewall firewall add rule name="Open Ports for WinRM incoming traffic"
 dir=in action=allow protocol=TCP localport=5985, 5986 # Opens ports for WinRM
netsh advfirewall firewall add rule name="All ICMP V4" protocol=icmpv4:any,any
 dir=in action=allow # Allows ICPM traffic

Enable-PSRemoting -Force # Enables WinRM
Set-Service WinRM -StartMode Automatic # Allows WinRM service to run on host
 startup
Set-Item WSMan:\localhost\Client\TrustedHosts -Value {IP} -Force # Sets the
 specific IP from which the access to WinRM is allowed

winrm set winrm/config/service '@{Negotiation="true"}' # Allow Negosiate auth usage
winrm set winrm/config/service '@{AllowUnencrypted="true"}' # Allow unencrypted
 connection
```

Linux에서 데이터베이스 서버를 검색하려면

1. ss및netstat 명령에 sudo 액세스를 제공합니다.

   다음 코드 예제는ss 및netstat 명령에 sudo에 대한 액세스 권한을 부여합니다.

   ```
   sudo bash -c "cat << EOF >> /etc/sudoers.d/username
   username ALL=(ALL) NOPASSWD: /usr/bin/ss
   username ALL=(ALL) NOPASSWD: /usr/bin/netstat
   EOF"
   ```

   위 예에서 에서 지정한 Linux 사용자 이름으로*username* 바꿉니다.

   위 예제에서는ss 및netstat 명령의/usr/bin/ 경로를 사용합니다. 이 경로는 환경에 따라 다를 수 있습니다. 및 명령의 경로를 확인하려면sswhich ss 및netstatwhich netstat 명령을 실행합니다.
2. 원격 SSH 스크립트 실행을 허용하고 ICMP (인터넷 제어 메시지 프로토콜) 트래픽을 허용하도록 Linux 서버를 구성합니다.

데이터베이스 서버 검색을 시작하려면

1. 데이터베이스 및 분석 컬렉터 페이지의 탐색 창의 Discovery에서 OS 서버를 선택합니다.

2. 데이터베이스 및 분석 서버가 포함된 OS 서버를 선택한 다음 작업 메뉴에서 연결 확인을 선택합니다.
3. 연결 상태가 실패인 서버의 경우 연결 자격 증명을 편집하십시오.
   a. 자격 증명이 동일한 경우 단일 서버 또는 여러 서버를 선택한 다음 작업 메뉴에서 편집을 선택합니다. OS 서버 편집 페이지가 열립니다.
   b. 포트에 사용되는 포트 번호를 입력합니다.
   c. 인증 유형에서 OS 서버에서 사용하는 인증 유형을 선택합니다.
   d. 사용자 이름에 사용합니다.
   e. 암호에 사용하는 암호를 입력합니다.
   f. 연결 확인을 선택하여 OS 서버 자격 증명을 올바르게 업데이트했는지 확인하십시오. 그런 다음 [Save] 를 선택합니다.
4. 모든 OS 서버의 자격 증명을 업데이트한 후 OS 서버를 선택하고 데이터베이스 서버 검색을 선택합니다.

데이터베이스 및 분석 데이터 수집 모듈은 OS 서버에 연결하여 지원되는 데이터베이스 및 분석 서버를 검색합니다. 데이터 수집 모듈에서 검색을 완료한 후 데이터베이스 서버 보기를 선택하여 검색된 데이터베이스 및 분석 서버의 목록을 볼 수 있습니다.

또는 데이터베이스 및 분석 서버를 인벤토리에 수동으로 추가할 수 있습니다. 또한 CSV 파일에서 서버 목록을 가져올 수 있습니다. 모든 데이터베이스 및 분석 서버를 이미 인벤토리에 추가한 경우에는 이 단계를 건너뛸 수 있습니다.

데이터베이스 또는 분석 서버를 수동으로 추가하려면

1. 데이터베이스 및 분석 컬렉터 페이지의 탐색 창에서 데이터 수집을 선택합니다.
2. 데이터베이스 서버 추가를 선택합니다. 데이터베이스 서버 추가 페이지가 열립니다.
3. 데이터베이스 서버 자격 증명을 입력합니다.
   a. 데이터베이스 엔진에서 서버의 데이터베이스 엔진을 선택합니다. 자세한 정보는 지원되는 OS, 데이터베이스 및 분석 서버을 참조하세요.
   b. Hostname/IP에 데이터베이스 또는 분석 서버의 호스트 이름 또는 IP 주소를 입력합니다.
   c. Port에 서버가 실행되는 포트를 입력합니다.
   d. 인증 유형에서 데이터베이스 또는 분석 서버가 사용하는 인증 유형을 선택합니다.
   e. 사용자 이름에 사용합니다.

f. 암호에 사용하는 암호를 입력합니다.

g. 확인을 선택하여 데이터베이스 또는 분석 서버 자격 증명을 올바르게 추가했는지 확인하십시오.

4. (선택 사항) CSV 파일에서 여러 서버를 추가합니다.

a. CSV에서 데이터베이스 서버 대량 가져오기를 선택합니다.

b. 템플릿 다운로드를 선택하여 사용자 지정할 수 있는 템플릿이 포함된 CSV 파일을 저장합니다.

c. 템플릿에 따라 데이터베이스 및 분석 서버의 연결 자격 증명을 파일에 입력합니다. 다음 예제에서는 데이터베이스 또는 분석 서버 연결 자격 증명을 CSV 파일로 제공하는 방법을 보여줍니다.

```
Database engine,Hostname/IP,Port,Authentication type,Username,Password,Oracle
 service name,Database,Allow public key retrieval,Use SSL,Trust server
 certificate
Oracle,192.0.2.1,1521,Login/Password authentication,USER-
EXAMPLE,AKIAI44QH8DHBEXAMPLE,orcl,,,,
PostgreSQL,198.51.100.1,1533,Login/Password authentication,USER2-
EXAMPLE,bPxRfiCYEXAMPLE,,postgre,,TRUE,
MSSQL,203.0.113.1,1433,Login/Password authentication,USER3-
EXAMPLE,h3yCo8nvbEXAMPLE,,,,,TRUE
MySQL,2001:db8:4006:812:ffff:200e,8080,Login/Password authentication,USER4-
EXAMPLE,APKAEIVFHP46CEXAMPLE,,mysql,TRUE,TRUE,
```

모든 데이터베이스 및 분석 서버에 자격 증명을 추가한 후 CSV 파일을 저장합니다.

d. 찾아보기를 선택한 다음 CSV 파일을 선택합니다.

5. 데이터베이스 서버 추가를 선택합니다.

6. 모든 OS 서버의 자격 증명을 추가한 후 OS 서버를 선택하고 데이터베이스 서버 검색을 선택합니다.

모든 데이터베이스 및 분석 서버를 데이터 수집 모듈에 추가한 후 인벤토리에 추가합니다. 데이터베이스 및 분석 데이터 수집 모듈은 인벤토리에서 서버에 연결하여 메타데이터 및 성능 메트릭을 수집할 수 있습니다.

데이터베이스 및 분석 서버를 인벤토리에 추가하려면

1. 데이터베이스 및 분석 컬렉터 페이지의 탐색 창의 검색에서 데이터베이스 서버를 선택합니다.

2. 메타데이터 및 성능 메트릭을 수집하려는 데이터베이스 및 분석 서버를 선택합니다.

3. 인벤토리에 추가를 선택합니다.

모든 데이터베이스 및 분석 서버를 인벤토리에 추가한 후 메타데이터 및 성능 지표 수집을 시작할 수 있습니다. 자세한 정보는 데이터베이스 및 분석 데이터 수집 단원을 참조하세요.

7단계: 수집된 데이터 보기

Application Discovery Service 에이전트리스 컬렉터 (에이전트 없는 컬렉터) 가 수집한 데이터를 Migration Hub 콘솔에서 볼 수 있습니다. 콘솔에서 데이터베이스 및 분석 서버에 대해 수집된 지표를 볼 수 있습니다. AWS DMS

VMware vCenter 에이전트리스 컬렉터 데이터 수집 모듈에서 검색된 데이터를 보려면

1. AWS Management Console로그인하고 https://console.aws.amazon.com/migrationhub/ 에서 Migration Hub 콘솔을 엽니다. 이 작업을 수행하려면 생성한 IAM 사용자와 다른 IAM 사용자 계정을 사용하여 Agentless Collector를 설정하고 액세스하는 것이 좋습니다.
2. Migration Hub 콘솔 탐색 창의 디스커버에서 서버를 선택합니다.
3. 서버에 대한 세부 정보를 보려면 서버 정보 열에서 서버의 호스트 이름을 선택합니다. 서버의 세부 정보 페이지에는 호스트 이름, IP 주소, 성능 지표 등과 같은 서버 관련 정보가 표시됩니다.

데이터베이스 및 분석 데이터 수집 모듈에서 검색된 데이터를 보려면

1. https://console.aws.amazon.com/dms/v2/ 에서 AWS Management Console 로그인하고 AWS DMS 콘솔을 엽니다.
2. 디스커버에서 인벤토리를 선택합니다. 인벤토리 페이지가 열립니다.
3. 인벤토리 분석을 선택하여 유사성 및 복잡성과 같은 데이터베이스 스키마 속성을 확인합니다.
4. 스키마 탭을 선택하여 분석 결과를 확인합니다.

AWS DMS콘솔을 사용하여 중복 스키마를 식별하고, 마이그레이션 복잡성을 확인하고, 향후 분석을 위해 인벤토리 정보를 내보낼 수 있습니다. 자세한 내용은 AWS DMSFleet Advisor의 분석을 위한 인벤토리 사용을 참조하십시오.

에이전트리스 컬렉터가 수집한 데이터

Application Discovery Service 에이전트리스 컬렉터 (Agentless Collector) 데이터 수집 모듈을 설정하여 서버에서 인벤토리, 프로필 및 사용률 데이터를 수집합니다.

에이전트리스 컬렉터는 현재 VMware VM과 데이터베이스 및 분석 서버에서의 데이터 수집을 지원합니다. 향후 모듈에서는 추가 가상화 플랫폼에서의 수집 및 운영 체제 수준 수집을 지원할 예정입니다.

데이터 수집 설정에 대한 자세한 내용은 을 참조하십시오6단계: 에이전트리스 컬렉터 데이터 수집 모듈 설정.

다음 항목에서는 Application Discovery Service 에이전트 없는 수집기 (에이전트 없는 수집기) 데이터 수집 모듈에서 수집한 데이터에 대해 설명합니다.

토픽

- 에이전트리스 컬렉터 VMware vCenter 데이터 수집 모듈에서 수집한 데이터
- Agentless Collector 데이터베이스 및 분석 데이터 수집 모듈에서 수집한 데이터

에이전트리스 컬렉터 VMware vCenter 데이터 수집 모듈에서 수집한 데이터

다음 정보는 Application Discovery Service 에이전트 없는 수집기 (에이전트 없는 수집기) VMware vCenter 데이터 수집 모듈에서 수집한 데이터를 설명합니다. 데이터 수집 설정에 대한 자세한 내용은 을 참조하십시오. VMware vCenter용 에이전트리스 컬렉터 데이터 수집 모듈을 설정하는 방법

에이전트리스 컬렉터에 대한 표 범례: VMware vCenter 수집 데이터:

- 수집된 데이터는 별도의 명시가 없는 경우에는 KB(Kilobytes)로 측정됩니다.
- Migration Hub 콘솔의 해당 데이터는 메가바이트 (MB) 단위로 보고됩니다.
- 별표 (*) 로 표시된 데이터 필드는 Application Discovery Service API 내보내기 기능을 통해 생성된.csv 파일에서만 사용할 수 있습니다.

  에이전트리스 컬렉터는 AWS CLI를 사용한 데이터 내보내기를 지원합니다. AWS CLI를 사용하여 수집된 데이터를 내보내려면 Application Discovery Service 사용 설명서의 수집된 데이터 내보내기 페이지에서 모든 서버의 시스템 성능 데이터 내보내기에 설명된 지침을 따르십시오.
- 폴링 기간의 간격은 약 60분입니다.
- 현재 이중 별표(**)로 표시된 데이터 필드는 null 값을 반환합니다.

데이터 필드	설명
applicationConfigurationId*	VM이 그룹화된 마이그레이션 애플리케이션의 ID.
avgCpuUsagePct	폴링 기간 동안의 평균 CPU 사용률

데이터 필드	설명
avgDiskBytesReadPerSecond	폴링 기간 동안 디스크에서 읽은 평균 바이트 수입니다.
avgDiskBytesWrittenPerSecond	폴링 기간 동안 디스크에 기록된 평균 바이트 수입니다.
avgDiskReadOpsPerSecond**	초당 평균 읽기 I/O 작업 수 null.
avgDiskWriteOpsPerSecond**	초당 평균 쓰기 I/O 작업 수입니다.
avgFreeRAM	평균 여유 RAM은 MB 단위로 표시됩니다.
avgNetworkBytesReadPerSecond	초당 읽은 평균 바이트 처리량.
avgNetworkBytesWrittenPerSecond	초당 기록된 바이트의 평균 처리량.
컴퓨터 제조업체	ESXi 호스트가 보고한 공급업체입니다.
컴퓨터 모델	ESXi 호스트에서 보고한 컴퓨터 모델입니다.
configId	Application Discovery Service에서 검색된 VM에 할당한 ID입니다.
configType	검색된 리소스 유형.
connectorId	가상 어플라이언스의 ID.
cpuType	VM의 vCPU, 호스트의 실제 모델.
datacenterId	v센터의 ID입니다.
hostId*	VM 호스트의 ID입니다.
hostName	가상화 소프트웨어를 실행하는 호스트의 이름.
하이퍼바이저	하이퍼바이저 유형.
id	서버 ID.

데이터 필드	설명
lastModifiedTime스탬프*	데이터 내보내기 전 데이터 수집의 최신 날짜 및 시간
macAddress	VM의 MAC 주소.
주소	가상화 소프트웨어 제조업체.
maxCpuUsagePct	폴링 기간 동안의 최대 CPU 사용률
maxDiskBytesReadPerSecond	폴링 기간 동안 디스크에서 읽은 최대 바이트 수
maxDiskBytesWrittenPerSecond	폴링 기간 동안 디스크에 기록된 최대 바이트 수입니다.
maxDiskReadOpsPerSecond**	초당 최대 읽기 I/O 작업 수
maxDiskWriteOpsPerSecond**	초당 최대 쓰기 I/O 작업 수
maxNetworkBytesReadPerSecond	초당 읽은 최대 바이트 처리량
maxNetworkBytesWrittenPerSecond	초당 기록된 최대 바이트 처리량
memoryReservation*	VM의 메모리 오버커밋을 방지하기 위한 제한입니다.
moRefId	고유한 vCenter 관리 객체 참조 ID
name*	VM 또는 네트워크 이름 (사용자 지정)
numCores	VM에 할당된 CPU 코어 수입니다.
numCpus	ESXi 호스트의 CPU 소켓 수입니다.
numDisks**	VM의 디스크 수
numNetworkCards**	VM에 있는 네트워크 카드 수
osName	VM의 운영 체제 이름.
osVersion	VM의 운영 체제 버전.

데이터 필드	설명
portGroupId*	VLAN의 멤버 포트 그룹 ID.
portGroupName*	VLAN의 멤버 포트 그룹 이름.
powerState*	전원 상태.
serverId	Application Discovery Service에서 검색된 VM에 ID를 할당했습니다.
smBiosId*	시스템 관리 BIOS의 ID/버전
state*	가상 어플라이언스의 상태.
toolsStatus	VMware 툴의 작동 상태
totalDiskFree크기	여유 디스크 공간 (MB) vCenter Server 7.0 이상 버전에서 사용할 수 있습니다.
totalDiskSize	디스크의 총 용량은 MB 단위로 표시됩니다.
totalRAM	VM에서 사용할 수 있는 총 RAM 크기 (MB)
유형	호스트 유형.
vCenterId	VM의 고유 ID 번호입니다.
vCenterName*	vCenter 호스트의 이름입니다.
virtualSwitchName*	가상 스위치의 이름.
vmFolderPath	VM 파일의 디렉터리 경로.
vmName	가상 머신의 이름.

Agentless Collector 데이터베이스 및 분석 데이터 수집 모듈에서 수집한 데이터

Application Discovery Service 에이전트리스 컬렉터 (Agentless Collector) 데이터베이스 및 분석 데이터 수집 모듈은 데이터 환경에서 다음과 같은 메트릭을 수집합니다. 데이터 수집 설정에 대한 자세한 내용은 단원을 참조하세요데이터베이스 및 분석 데이터 수집 모듈.

데이터베이스 및 분석 데이터 수집 모듈을 사용하여 메타데이터 및 데이터베이스 용량을 수집하면 다음과 같은 지표를 캡처합니다.

- OS 서버의 사용 가능한 메모리
- OS 서버의 사용 가능한 스토리지
- 데이터베이스 버전 및 에디션
- OS 서버의 CPU 수
- 스키마 수
- 저장 프로시저 수
- 테이블 수
- 트리거 수 (트리거 수) 입니다
- 조회수
- 스키마 구조

AWS DMS콘솔에서 스키마 분석을 시작하면 데이터 수집 모듈이 다음 지표를 분석하고 표시합니다.

- 데이터베이스 지원 날짜
- 코드 줄 수
- 스키마 복잡성
- 스키마의 유사성

데이터베이스 및 분석 데이터 수집 모듈을 사용하여 메타데이터, 데이터베이스 용량 및 리소스 사용률을 수집하면 다음과 같은 지표를 캡처합니다.

- 데이터베이스 서버의 I/O 처리량
- 데이터베이스 서버의 초당 입출력 작업 처리량 (IOPS) 입니다.
- OS 서버에서 사용하는 CPU 수

- OS 서버의 메모리 사용량
- OS 서버의 스토리지 사용량

데이터베이스 및 분석 데이터 수집 모듈을 사용하여 Oracle 및 SQL Server 데이터베이스에서 메타데이터, 용량 및 사용률 지표를 수집할 수 있습니다. 동시에 PostgreSQL 및 MySQL 데이터베이스의 경우 데이터 수집 모듈은 메타데이터만 수집할 수 있습니다.

에이전트리스 컬렉터 콘솔 사용

이 섹션에서는 Application Discovery Service 에이전트리스 컬렉터 (에이전트리스 컬렉터) 콘솔을 사용하는 방법을 설명합니다.

주제

- 에이전트리스 컬렉터 대시보드
- 에이전트리스 컬렉터 설정 편집
- VM웨어 vCenter 자격 증명 편집

에이전트리스 컬렉터 대시보드

Application Discovery Service 에이전트리스 컬렉터 (Agentless Collector) 대시보드 페이지에서 컬렉터 상태를 확인하고 다음 항목에 설명된 대로 데이터 수집 방법을 선택할 수 있습니다.

주제

- 수집가 상태
- 데이터 수집

수집가 상태

컬렉터 상태는 컬렉터에 대한 상태 정보를 제공합니다. 컬렉터 이름, 컬렉터의 AWS 연결 상태, Migration Hub 홈 리전 및 버전.

AWS연결 문제가 있으면 에이전트리스 컬렉터 구성 설정을 편집해야 할 수 있습니다.

컬렉터 구성 설정을 편집하려면 컬렉터 설정 편집을 선택하고 에 설명된 지침을 따르십시오에이전트리스 컬렉터 설정 편집.

데이터 수집

데이터 수집에서 데이터 수집 방법을 선택할 수 있습니다. Application Discovery Service 에이전트리스 컬렉터 (Agentless Collector) 는 현재 VMware VM과 데이터베이스 및 분석 서버에서의 데이터 수집을 지원합니다. 향후 모듈에서는 추가 가상화 플랫폼에서의 수집 및 운영 체제 수준 수집을 지원할 예정입니다.

주제

VM웨어 vCenter 데이터 수집

VMware VM에서 서버 인벤토리, 프로필 및 사용률 데이터를 수집하려면 vCenter 서버에 대한 연결을 설정하십시오. 연결을 설정하려면 VMware vCenter 섹션에서 설정을 선택하고 에 설명된 지침을 따르십시오6단계: 에이전트리스 컬렉터 데이터 수집 모듈 설정.

vCenter 데이터 수집을 설정한 후 대시보드에서 다음을 수행할 수 있습니다.

- 데이터 수집 상태 보기
- 데이터 수집 시작
- 데이터 수집 중지

> **Note**
>
> 대시보드 페이지에서 vCenter 데이터 수집을 설정하면 VMware vCenter 섹션의 설정 버튼이 데이터 수집 상태 정보, 데이터 수집 중지 버튼, 보기 및 편집 버튼으로 바뀝니다.

데이터베이스 및 분석 데이터 수집

데이터베이스 및 분석 데이터 수집 모듈을 다음 두 가지 모드로 실행할 수 있습니다.

메타데이터 및 데이터베이스 용량

데이터 수집 모듈은 데이터베이스 및 분석 서버에서 스키마, 버전, 에디션, CPU, 메모리 및 디스크 용량과 같은 정보를 수집합니다. 이렇게 수집된 정보를 사용하여AWS DMS 콘솔에서 대상 권장 사

항을 계산할 수 있습니다. 원본 데이터베이스가 오버프로비저닝 또는 언더프로비저닝된 경우 대상 권장 사항도 오버프로비저닝 또는 언더프로비저닝됩니다.

이것이 기본 모드입니다.

메타데이터, 데이터베이스 용량 및 리소스 사용률

데이터 수집 모듈은 메타데이터 및 데이터베이스 용량 정보 외에도 데이터베이스 및 분석 서버의 CPU, 메모리 및 디스크 용량에 대한 실제 사용률 지표를 수집합니다. 이 모드는 권장 사항이 실제 데이터베이스 워크로드를 기반으로 하므로 기본 모드보다 더 정확한 대상 권장 사항을 제공합니다. 이 모드에서는 데이터 수집 모듈이 1분마다 성능 지표를 수집합니다.

데이터베이스 및 분석 서버에서 메타데이터 및 성능 지표 수집을 시작하려면

1. 데이터베이스 및 분석 컬렉터 페이지의 탐색 창에서 데이터 수집을 선택합니다.
2. 데이터베이스 인벤토리 목록에서 메타데이터 및 성능 메트릭을 수집하려는 데이터베이스 및 분석 서버를 선택합니다.
3. 데이터 수집 실행을 선택합니다. 데이터 수집 유형 대화 상자가 열립니다.
4. 분석을 위한 데이터 수집 방법을 선택합니다.

   메타데이터, 데이터베이스 용량 및 리소스 사용률 옵션을 선택한 경우 데이터 수집 기간을 설정합니다. 다음 7일 동안 데이터를 수집하거나 사용자 지정 범위를 1~60일로 설정할 수 있습니다.
5. 데이터 수집 실행을 선택합니다. 데이터 수집 페이지가 열립니다.
6. 컬렉션 상태 탭을 선택하여 데이터 수집 상태를 확인합니다.

데이터 수집을 완료하면 데이터 수집 모듈이 수집된 데이터를 Amazon S3 버킷에 업로드합니다. 그러면 에 설명된 대로 수집된 데이터를 볼 수7단계: 수집된 데이터 보기 있습니다.

에이전트리스 컬렉터 설정 편집

에 설명된 대로 Application Discovery Service 에이전트리스 컬렉터 (에이전트리스 컬렉터) 를 처음 설정할 때 컬렉터를5단계: 에이전트리스 컬렉터 구성 구성했습니다. 다음 절차에서는 에이전트 없는 수집기 구성 설정을 편집하는 방법을 설명합니다.

컬렉터 구성 설정을 편집하려면

- 에이전트 없는 컬렉터 대시보드에서 컬렉터 설정 편집 버튼을 선택합니다.

  컬렉터 설정 편집 페이지에서 다음 작업을 수행합니다.

a. 컬렉터 이름에 컬렉터를 식별할 이름을 입력합니다. 이름은 공백을 포함할 수 있지만 특수 문자를 포함할 수 없습니다.

b. 검색 데이터의 대상AWS 계정에서 컬렉터가 검색한 데이터를 받을 대상AWS 계정으로 지정할 계정의AWS 액세스 키와 비밀 키를 입력합니다. IAM 사용자의 요구 사항에 대한 자세한 내용은 을 참조하십시오1단계: 에이전트리스 컬렉터용 IAM 사용자 생성.

   i. 액세스 AWS키에는 대상 계정으로 지정하는AWS 계정 IAM 사용자의 액세스 키를 입력합니다.

   ii. 비밀 AWS키에는 대상 계정으로 지정하는AWS 계정 IAM 사용자의 비밀 키를 입력합니다.

c. 에이전트리스 컬렉터 비밀번호에서 에이전트리스 컬렉터에 대한 액세스를 인증하는 데 사용할 비밀번호를 변경합니다.

   i. 에이전트 없는 컬렉터 암호의 경우 에이전트리스 컬렉터에 대한 액세스를 인증하는 데 사용할 암호를 입력합니다.

   ii. Agentless Collector 암호를 다시 입력하려면 확인을 위해 암호를 다시 입력하십시오.

d. 구성 저장을 선택합니다.

다음으로 보게 될 것입니다에이전트리스 컬렉터 대시보드.

VM웨어 vCenter 자격 증명 편집

VMware VM에서 서버 인벤토리, 프로필 및 사용률 데이터를 수집하려면 vCenter 서버에 대한 연결을 설정하십시오. VMware vCenter 연결 설정에 대한 자세한 내용은 을 참조하십시오6단계: 에이전트리스 컬렉터 데이터 수집 모듈 설정.

이 섹션에서는 vCenter 자격 증명을 편집하는 방법을 설명합니다.

> **Note**
>
> vCenter 자격 증명을 편집하기 전에 시스템 그룹에 설정된 읽기 및 보기 권한이 있는 vCenter 자격 증명을 제공할 수 있는지 확인하십시오.

VMware vCenter 자격 증명을 편집하려면

VM웨어 데이터 수집 세부 정보 데이터 수집 데이터 수집 세부 정보 중지페이지에서 vCenter 서버 편집을 선택합니다.

- vCenter 편집 페이지에서 다음을 수행합니다.

  a. vCenter 자격 증명 아래에서:

     i. vCenter URL/IP의 경우 VMware vCenter 서버 호스트의 IP 주소를 입력합니다.

     ii. vCenter 사용자 이름에 커넥터가 vCenter와 통신하기 위해 사용하는 로컬 또는 도메인 사용자의 이름을 입력합니다. 도메인 사용자의 경우 domain\username 또는 username@domain 형식을 사용합니다.

     iii. vCenter 암호에 로컬 또는 도메인 사용자 암호를 입력합니다.

  b. 저장을 선택합니다.

에이전트리스 컬렉터 수동 업데이트

Application Discovery Service 에이전트 없는 수집기 (에이전트 없는 수집기) 를 구성할 때 에 설명된 대로 자동 업데이트를 활성화하도록 선택할 수 있습니다. 5단계: 에이전트리스 컬렉터 구성 자동 업데이트를 활성화하지 않는 경우 에이전트리스 컬렉터를 수동으로 업데이트해야 합니다.

다음 절차는 에이전트리스 컬렉터를 수동으로 업데이트하는 방법을 설명합니다.

에이전트리스 컬렉터를 수동으로 업데이트하려면

1. 최신 에이전트리스 컬렉터 오픈 가상화 아카이브 (OVA) 파일을 구하십시오.
2. (선택 사항) 최신 파일을 배포하기 전에 이전 에이전트리스 컬렉터 OVA 파일을 삭제하는 것이 좋습니다.
3. 에이전트리스 컬렉터 시작하기섹션에서 단계를 따라 진행하세요. 3단계: 에이전트리스 컬렉터 배포 6단계: 에이전트리스 컬렉터 데이터 수집 모듈 설정

이전 절차는 에이전트 없는 컬렉터만 업데이트합니다. OS를 최신 상태로 유지하는 것은 사용자의 책임입니다.

Amazon EC2 인스턴스를 업데이트하려면

1. VMware vCenter에서 에이전트리스 컬렉터의 IP 주소를 가져옵니다.

2. 컬렉터의 VM 콘솔을 열고 다음 예와 **collector** 같이 비밀번호를 **ec2-user** 사용하여 로그인합니다.

```
username: ec2-user
password: collector
```

3. Amazon Linux 2 사용 설명서의 AL2 인스턴스에서 인스턴스 소프트웨어 업데이트의 지침을 따르십시오.

아마존 리눅스 2에서의 커널 라이브 패칭

에이전트리스 컬렉터 가상 머신은 에 설명된 대로 Amazon Linux 2를 사용합니다. 3단계: 에이전트리스 컬렉터 배포

Amazon Linux 2에서 라이브 패치를 활성화하고 사용하려면 Amazon EC2 사용 설명서의 Amazon Linux 2에서의 커널 라이브 패칭을 참조하십시오.

에이전트리스 컬렉터 문제 해결

이 섹션에는 Application Discovery Service 에이전트리스 컬렉터 (에이전트리스 컬렉터) 와 관련된 알려진 문제를 해결하는 데 도움이 되는 항목이 포함되어 있습니다.

주제

- 설치 중에 에이전트리스 컬렉터에 연결할 수 없는 문제 해결 AWS
- 프록시 호스트에 연결할 때 자체 서명된 인증 문제 해결
- 비정상 컬렉터 찾기
- IP 주소 문제 해결
- vCenter 자격 증명 문제 해결
- 데이터베이스 및 분석 데이터 수집 모듈의 데이터 전달 문제 해결
- 데이터베이스 및 분석 데이터 수집 모듈의 연결 문제 해결
- 독립형 ESX 호스트 지원
- 에이전트 없는 AWS 컬렉터 문제에 대한 지원 문의

설치 중에 에이전트리스 컬렉터에 연결할 수 없는 문제 해결 AWS

에이전트리스 컬렉터에는 TCP 포트 443을 통해 여러 도메인에 대한 아웃바운드 액세스가 필요합니다. AWS 콘솔에서 에이전트리스 컬렉터를 구성할 때 다음과 같은 오류 메시지가 표시될 수 있습니다.

> 연결할 수 없습니다. AWS
>
> AWS 연결할 수 없습니다. 네트워크 설정을 확인하십시오.

이 오류는 Agentless Collector가 설정 프로세스 중에 컬렉터가 통신해야 하는 AWS 도메인에 HTTPS 연결을 설정하지 못했기 때문에 발생합니다. 연결을 설정할 수 없는 경우 에이전트리스 컬렉터 구성이 실패합니다.

연결을 수정하려면 AWS

1. IT 관리자에게 문의하여 회사 방화벽이 포트 443에서 아웃바운드 액세스가 필요한 AWS 도메인으로 향하는 아웃바운드 트래픽을 차단하고 있는지 확인하십시오. 아웃바운드 액세스가 필요한 AWS 도메인은 홈 지역이 미국 서부 (오레곤) 지역인지, us-west-2인지, 기타 지역인지에 따라 달라집니다.

   AWS 계정 홈 지역이 us-west-2인 경우 다음 도메인에는 아웃바운드 액세스가 필요합니다.

   - `arsenal-discovery.us-west-2.amazonaws.com`
   - `migrationhub-config.us-west-2.amazonaws.com`
   - `api.ecr-public.us-east-1.amazonaws.com`
   - `public.ecr.aws`

   AWS 계정 홈 지역이 아닌 경우 다음 도메인에는 아웃바운드 액세스가 필요합니다. **us-west-2**

   - `arsenal-discovery.us-west-2.amazonaws.com`
   - `arsenal-discovery.`*`your-home-region`*`.amazonaws.com`
   - `migrationhub-config.us-west-2.amazonaws.com`
   - `api.ecr-public.us-east-1.amazonaws.com`
   - `public.ecr.aws`

방화벽이 Agentless Collector가 통신해야 하는 AWS 도메인에 대한 아웃바운드 액세스를 차단하는 경우 Collector 구성 아래의 데이터 동기화 섹션에서 프록시 호스트를 구성하십시오.

2. 방화벽을 업데이트해도 연결 문제가 해결되지 않는 경우 다음 단계를 사용하여 Collector 가상 시스템이 이전 단계에 나열된 도메인에 대한 아웃바운드 네트워크 연결을 가지고 있는지 확인하십시오.

   a. VMware vCenter에서 에이전트리스 컬렉터의 IP 주소를 가져옵니다.

   b. 컬렉터의 VM 콘솔을 열고 다음 예와 **`collector`** 같이 비밀번호를 **`ec2-user`** 사용하여 로그인합니다.

   ```
   username: ec2-user
   password: collector
   ```

   c. 다음 예와 같이 포트 443에서 텔넷을 실행하여 나열된 도메인에 대한 연결을 테스트합니다.

   ```
   telnet migrationhub-config.us-west-2.amazonaws.com 443
   ```

3. 텔넷으로 도메인을 확인할 수 없는 경우 Amazon Linux 2 지침을 사용하여 정적 DNS 서버를 구성해 보십시오.

4. 오류가 계속되는 경우 추가 지원이 필요하면 을 참조하십시오에이전트 없는 AWS 컬렉터 문제에 대한 지원 문의.

프록시 호스트에 연결할 때 자체 서명된 인증 문제 해결

선택적으로 제공된 프록시와 HTTPS를 통해 통신하고 프록시에 자체 서명된 인증서가 있는 경우 인증서를 제공해야 할 수 있습니다.

1. VMware vCenter에서 에이전트리스 컬렉터의 IP 주소를 가져옵니다.

2. 컬렉터의 VM 콘솔을 열고 다음 `ec2-user` 예와 `collector` 같이 암호를 사용하여 로그인합니다.

   ```
   username: ec2-user
   password: collector
   ```

3. `-----BEGIN CERTIFICATE-----`및 `-----END CERTIFICATE-----` 를 포함하여 보안 프록시와 연결된 인증서 본문을 다음 파일에 붙여넣습니다.

```
/etc/pki/ca-trust/source/anchors/https-proxy-ca.pem
```

4. 새 인증서를 설치하려면 다음 명령을 실행합니다.

```
sudo update-ca-trust
```

5. 다음 명령을 실행하여 에이전트 없는 Collector를 다시 시작합니다.

```
sudo shutdown -r now
```

비정상 컬렉터 찾기

모든 수집기의 상태 정보는 AWS Migration Hub (Migration Hub) 콘솔의 데이터 수집기 페이지에서 찾을 수 있습니다. 주의 필요 상태인 수집자를 찾으면 문제가 있는 수집자를 식별할 수 있습니다.

다음 절차는 Agentless Collector 콘솔에 액세스하여 상태 문제를 식별하는 방법을 설명합니다.

에이전트리스 컬렉터 콘솔에 액세스하려면

1. AWS 계정을 사용하여 https://console.aws.amazon.com/migrationhub/ 에서 Migration Hub 콘솔에 AWS Management Console 로그인하고 여십시오.
2. Migration Hub 콘솔 탐색 창의 디스커버에서 데이터 수집기를 선택합니다.
3. 에이전트리스 컬렉터 탭에서 상태가 주의 필요인 각 커넥터의 IP 주소를 기록해 둡니다.
4. 에이전트리스 컬렉터 콘솔을 열려면 웹 브라우저를 여십시오. 그런 다음 주소 표시줄에 다음 **https://**/URL을 입력합니다. <ip_address>여기서 ip_address는 비정상 컬렉터의 IP 주소입니다.
5. [로그인] 을 선택한 다음 컬렉터가 구성될 때 설정된 에이전트리스 컬렉터 암호를 입력합니다. 5단계: 에이전트리스 컬렉터 구성
6. 에이전트리스 컬렉터 대시보드 페이지의 데이터 수집에서 VMware vCenter 섹션에서 보기 및 편집을 선택합니다.
7. 의 지침에 따라 URL과 자격 VM웨어 vCenter 자격 증명 편집 증명을 수정하십시오.

상태 문제를 해결한 후 수집기는 vCenter Server와의 연결을 다시 설정하고 수집기의 상태는 수집 중 상태로 변경됩니다. 문제가 계속되는 경우 을 참조하십시오. 에이전트 없는 AWS 컬렉터 문제에 대한 지원 문의

비정상 수집기의 가장 일반적인 원인은 IP 주소 및 자격 증명 문제입니다. IP 주소 문제 해결이러한 문제를 해결하고 수집기를 정상 상태로 되돌리는 데 도움이 될 vCenter 자격 증명 문제 해결 수 있습니다.

IP 주소 문제 해결

수집기 설정 중에 제공된 vCenter 엔드포인트가 잘못되었거나 유효하지 않거나 vCenter 서버가 현재 다운되어 연결할 수 없는 경우 수집기가 비정상 상태가 될 수 있습니다. 이 경우 연결 오류 메시지가 표시됩니다.

다음 절차는 IP 주소 문제를 해결하도록 도움을 줄 수 있습니다.

컬렉터 IP 주소 문제를 해결하려면

1. VMware vCenter에서 에이전트리스 컬렉터의 IP 주소를 가져옵니다.
2. 웹 브라우저를 열어 에이전트리스 컬렉터 콘솔을 열고 주소 표시줄에 다음 **https://**/URL을 입력합니다. <ip_address>여기서 ip_address는 컬렉터의 IP 주소입니다. 3단계: 에이전트리스 컬렉터 배포
3. 로그인을 선택한 다음 Agentless Collector 암호를 입력합니다. 이 암호는 컬렉터가 구성될 때 설정되었습니다. 5단계: 에이전트리스 컬렉터 구성
4. 에이전트리스 컬렉터 대시보드 페이지의 데이터 수집에서 VMware vCenter 섹션에서 보기 및 편집을 선택합니다.
5. VMware 데이터 수집 세부 정보 페이지의 검색된 vCenter 서버에서 vCenter 열의 IP 주소를 기록해 둡니다.
6. `ping`또는 `traceroute` 같은 별도의 명령줄 도구를 사용하여 연결된 vCenter 서버가 활성 상태이고 수집기 VM에서 IP에 연결할 수 있는지 확인합니다.

   - IP 주소가 올바르지 않고 vCenter 서비스가 활성 상태인 경우 수집기 콘솔에서 IP 주소를 업데이트하고 다음을 선택합니다.
   - IP 주소가 정확하지만 vCenter 서버가 비활성 상태라면 활성화하십시오.
   - IP 주소가 정확하지만 vCenter 서버가 활성 상태라면, 방화벽 문제로 인해 수신 네트워크 연결이 차단되는지 확인합니다. 그렇다면 Collector VM에서 들어오는 연결을 허용하도록 방화벽 설정을 업데이트하십시오.

vCenter 자격 증명 문제 해결

수집기를 구성할 때 제공한 vCenter 사용자 자격 증명이 유효하지 않거나 vCenter 읽기 및 보기 계정 권한이 없는 경우 수집기는 비정상 상태가 될 수 있습니다.

vCenter 자격 증명과 관련된 문제가 발생하는 경우 시스템 그룹에 vCenter 읽기 및 보기 권한이 설정되어 있는지 확인하십시오.

vCenter 자격 증명을 편집하는 방법에 대한 자세한 내용은 을 참조하십시오. VM웨어 vCenter 자격 증명 편집

데이터베이스 및 분석 데이터 수집 모듈의 데이터 전달 문제 해결

Agentless Collector의 데이터베이스 및 분석 데이터 수집 모듈 홈 페이지에는 DMS 액세스 및 S3 액세스에 대한 연결 상태가 표시됩니다. DMS에 대한 액세스 및 S3에 대한 액세스에 액세스 불가능이 표시되면 데이터 전달을 구성하십시오. 자세한 정보는 데이터 포워딩 설정을 참조하세요.

데이터 전달을 구성한 후 이 문제가 발생하는 경우 데이터 수집 모듈이 인터넷에 액세스할 수 있는지 확인하십시오. 그런 다음 IAM 사용자에게 DMS CollectorPolicy 및 FleetAdvisorS3Policy 정책을 추가했는지 확인하세요. 자세한 정보는 1단계: 에이전트리스 컬렉터용 IAM 사용자 생성을 참조하세요.

데이터 수집 모듈을 연결할 수 없는 AWS경우 다음 도메인에 아웃바운드 액세스를 제공하십시오.

- `dms.your-home-region.amazonaws.com`
- `s3.amazonaws.com`

데이터베이스 및 분석 데이터 수집 모듈의 연결 문제 해결

Agentless Collector의 데이터베이스 및 분석 데이터 수집 모듈은 LDAP 서버에 연결하여 데이터 환경의 OS 서버를 검색합니다. 그런 다음 데이터 수집 모듈을 OS 서버에 연결하여 데이터베이스 및 분석 서버를 검색합니다. 데이터 수집 모듈은 이러한 데이터베이스 서버에서 용량 및 성능 메트릭을 수집합니다. 데이터 수집 모듈을 이러한 서버에 연결할 수 없는 경우 서버에 연결할 수 있는지 확인하십시오.

다음 예시에서는 *## ###* 값을 사용자 값으로 바꾸십시오.

- LDAP 서버에 연결할 수 있는지 확인하려면 패키지를 설치하십시오. `ldap-util` 이렇게 하려면 다음 명령을 실행합니다.

  ```
  sudo apt-get install ldap-util
  ```

  그리고 다음 명령을 실행합니다.

  ```
  ldapsearch -x -D "CN=user,CN=Users,DC=example,DC=com" -w "password" -b
   "dc=example,dc=com" -h
  ```

- Linux OS 서버에 연결할 수 있는지 확인하려면 다음 명령을 사용하십시오.

```
ssh -i C:\Users\user\private_key.pem -p 22 username@my-linux-host.domain.com
```

Windows에서 관리자 권한으로 이전 예제를 실행합니다.

```
ssh username@my-linux-host.domain.com
```

이전 예제를 Linux에서 실행합니다.

- Windows OS 서버에 연결할 수 있는지 확인하려면 다음 명령을 사용하십시오.

```
winrs -r:[hostname or ip] -u:username -p:password cmd
```

Windows에서 관리자 권한으로 이전 예제를 실행합니다.

```
sudo apt install -y winrm
winrm --user=username --password=password [http or https]://[hostname or ip]:[port]
 "[cmd.exe or any other CLI command]"
```

이전 예제를 Linux에서 실행합니다.

- SQL Server 데이터베이스에 연결할 수 있는지 확인하려면 다음 명령을 사용하십시오.

```
sqlcmd -S [hostname or IP] -U username -P 'password'
SELECT GETDATE() AS sysdate
```

- MySQL 데이터베이스에 연결할 수 있는지 확인하려면 다음 명령을 사용하십시오.

```
mysql -u username -p 'password' -h [hostname or IP] -P [port]
SELECT NOW() FROM DUAL
```

- Oracle 데이터베이스에 연결할 수 있는지 확인하려면 다음 명령을 사용하십시오.

```
sqlplus username/password@[hostname or IP]:port/servicename
SELECT SYSDATE FROM DUAL
```

- PostgreSQL 데이터베이스에 연결할 수 있는지 확인하려면 다음 명령을 사용하십시오.

```
psql -U username -h [hostname or IP] -p port -d database
```

```
SELECT CURRENT_TIMESTAMP AS sysdate
```

데이터베이스 및 분석 서버에 연결할 수 없는 경우 필요한 권한을 제공해야 합니다. 자세한 정보는 데이터베이스 서버 살펴보기을 참조하세요.

독립형 ESX 호스트 지원

에이전트리스 컬렉터는 독립형 ESX 호스트를 지원하지 않습니다. ESX 호스트는 vCenter Server 인스턴스의 일부여야 합니다.

에이전트 없는 AWS 컬렉터 문제에 대한 지원 문의

Application Discovery Service 에이전트 없는 수집기 (Agentless Collector) 에서 문제가 발생하여 도움이 필요한 경우 AWS 지원팀에 문의하십시오. 그러면 연락이 오고 수집기 로그를 전송하라는 메시지가 표시될 수 있습니다.

에이전트리스 컬렉터 로그를 가져오려면

1. VMware vCenter에서 에이전트리스 컬렉터의 IP 주소를 가져옵니다.
2. 컬렉터의 VM 콘솔을 열고 다음 예와 **collector** 같이 비밀번호를 **ec2-user** 사용하여 로그인합니다.

   ```
   username: ec2-user
   password: collector
   ```
3. 다음 명령을 사용하여 로그 폴더로 이동합니다.

   ```
   cd /var/log/aws/collector
   ```
4. 다음 명령을 사용하여 로그 파일을 압축합니다.

   ```
   sudo cp /local/agentless_collector/compose.log .
   docker inspect $(docker ps --format {{.Names}}) | sudo tee docker_inspect.log >/
   dev/null
   sudo tar czf logs_$(date '+%d-%m-%Y_%H.%M.%S').tar.gz * --exclude='db.mv*'
   ```
5. 에이전트리스 컬렉터 VM에서 로그 파일을 복사합니다.

   ```
   scp logs*.tar.gz targetuser@targetaddress
   ```

6. 이 `tar.gz` 파일을 AWS 기업 지원 부서에 제출하십시오.

Migration Hub

AWS Migration Hub(Migration Hub) 가져오기를 사용하면 Application Discovery Agent Connector (에이전트 없는 수집기) 를 사용하지 않고 Migration Hub 로 직접 가져올 수 있습니다.AWSApplication Discovery (Discovery Agent) - 가져온 데이터에서 직접 마이그레이션 평가 및 계획을 수행할 수 있습니다. 디바이스를 애플리케이션으로 그룹화하고 해당 마이그레이션 상태를 추적할 수도 있습니다.

가져오기 요청을 시작하려면

- 특수 형식의 CSV(쉼표로 구분된 값) 가져오기 템플릿을 다운로드합니다.
- 기존의 온프레미스 서버 데이터로 채웁니다.
- Migration Hub 콘솔을 사용하여 마이그레이션 허브에 업로드합니다.AWS CLI또는 다음 중 하나를 AWSSDK.

여러 가져오기 요청을 제출할 수 있습니다. 각 요청은 순차적으로 처리됩니다. 콘솔이나 가져오기 API를 통해 언제든지 가져오기 요청 상태를 확인할 수 있습니다.

가져오기 요청이 완료되면 가져온 개별 레코드의 세부 정보를 볼 수 있습니다. Migration Hub 콘솔에서 직접 사용률 데이터, 태그, 애플리케이션 매핑을 볼 수 있습니다. 가져오는 동안 오류가 발생할 경우 성공한 레코드와 실패한 레코드 수 및 실패한 각 레코드에 대한 오류 세부 정보를 검토할 수 있습니다.

오류: 오류 로그와 실패한 레코드 파일을 압축된 아카이브의 CSV 파일로 다운로드할 수 있는 링크가 제공됩니다. 이러한 파일을 사용하여 오류 수정 후 가져오기 요청을 다시 제출합니다.

가져온 레코드, 가져온 서버, 삭제한 레코드를 보관할 수 있는 수는 제한됩니다. 자세한 정보는 AWS Application Discovery Service 할당량을 참조하세요.

지원되는 가져오기 파일 필드

Migration Hub 가져오기를 사용하면 모든 소스에서 데이터를 가져올 수 있습니다. 제공된 데이터는 CSV 파일에 대해 지원되는 형식이어야 하며, 데이터에는 해당 필드에 대해 지원되는 범위가 있는 지원되는 필드만 포함되어야 합니다.

다음 표에서 별표가 표시된 가져오기 필드는 필수 필드입니다. 가져오기 파일의 각 레코드는 서버 또는 애플리케이션을 고유하게 식별하기 위해 값을 채운 이러한 필수 필드를 한 개 이상 가져야 합니다. 그렇지 않을 경우 필수 필드가 없는 레코드를 가져올 때 실패합니다.

> **Note**
>
> VMware 중 하나를 사용하는 경우MoRefId 또는 VMware.vCenterId, 레코드를 식별하려면 동일한 레코드에 두 필드가 있어야 합니다.

가져오기 필드 이름	설명	예
ExternalId*	각 레코드를 고유하게 표시할 수 있는 사용자 정의 식별자입니다. 예,ExternalId은 데이터 센터에 있는 서버의 인벤토리 ID일 수 있습니다.	Inventory Id 1 Server 2 CMBD Id 3
SMBiosId	시스템 관리 BIOS(SMBIOS) ID.	
IPAddress*	따옴표로 묶은 서버 IP 주소의 쉼표 구분 목록.	192.0.0.2 "10.12.31.233, 10.12.32.11"
MACAddress*	따옴표로 묶은 서버 MAC 주소의 쉼표 구분 목록.	00:1B:44:11:3A:B7 "00-15-E9-2B-99-3C, 00-14-22-01-23-45"
HostName*	서버의 호스트 이름입니다. 이 값에 정규화된 도메인 이름(FQDN)을 사용할 것을 권장합니다.	ip-1-2-3-4 localhost.domain
VMware.MoRefId*	관리되는 객체 참조 ID. VMware.V를 제공해야 합니다.CenterId.	
VMware.vCenterId*	가상 머신 고유 식별자. VMware를 제공해야 합니다.MoRefId.	

가져오기 필드 이름	설명	예
CPU.NumberOfProcessors	CPU 수입니다.	4
CPU.NumberOfCores	물리적 코어 총수	8
CPU.NumberOfLogicalCores	서버의 모든 CPU에서 동시에 실행할 수 있는 총 스레드 수입니다. 일부 CPU는 단일 CPU 코어에서 동시에 실행할 수 있는 여러 스레드를 지원합니다. 이 경우 이 숫자는 물리적(또는 가상) 코어의 수보다 더 많습니다.	16
OS.Name	운영 체제 이름.	Linux Windows.Hat
OS.Version	운영 체제 버전.	16.04.3 NT 6.2.8
VMware.VMName	가상 머신의 이름.	Corp1
RAM.TotalSizeInMB	서버에서 사용 가능한 총 RAM(MB)	64 128
RAM.UsedSizeInMB.avg	서버에서 사용된 평균 RAM 양(MB)	64 128
RAM.UsedSizeInMB.max	서버에서 사용 가능한 최대 RAM 양(MB)	64 128
CPU.UsagePct.Ag	검색 도구가 데이터를 수집할 때의 평균 CPU 사용률.	45 23.9

가져오기 필드 이름	설명	예
CPU.UsagePct.Max	검색 도구가 데이터를 수집할 때의 최대 CPU 사용률.	55.34 24
DiskReadsPerSecondInKB.avg	초당 평균 디스크 읽기 수(KB).	1159 84506
DiskWritesPerSecondInKB.avg	초당 평균 디스크 쓰기 수(KB).	199 6197
DiskReadsPerSecondInKB.max	초당 최대 디스크 읽기 수(KB).	37892 869962
DiskWritesPerSecondInKB.max	초당 최대 디스크 쓰기 수(KB).	18436 1808
DiskReadsOpsPerSecond.Ag	초당 평균 디스크 I/O 연산 수.	45 28
DiskWritesOpsPerSecond.Ag	초당 평균 디스크 쓰기 연산 수	8 3
DiskReadsOpsPerSecond.Max	초당 최대 디스크 읽기 작업 수.	1083 176
DiskWritesOpsPerSecond.Max	초당 최대 디스크 쓰기 작업 수.	535 71
NetworkReadsPerSecondInKB.avg	초당 평균 네트워크 읽기 작업 수(KB)	45 28

가져오기 필드 이름	설명	예
NetworkWritesPerSecondInKB.avg	초당 평균 네트워크 쓰기 작업 수(KB)	8 3
NetworkReadsPerSecondInKB.max	초당 최대 네트워크 읽기 작업 수(KB)	1083 176
NetworkWritesPerSecondInKB.max	초당 최대 네트워크 쓰기 작업 수(KB)	535 71
애플리케이션	이 서버를 포함하는 애플리케이션의 쉼표 구분 목록(따옴표로 묶음). 이 값에는 기존 애플리케이션 및/또는 가져올 때 생성되는 새 애플리케이션이 포함될 수 있습니다.	Application1 "Application2, Application3"
태그	이름:값 형식의 태그를 쉼표로 구분한 목록. **Important** 태그에 민감한 정보(예: 개인 데이터)를 저장하지 마십시오.	"zone:1, critical:yes" "zone:3, critical:no, zone:1"

각 레코드에 적어도 한 개의 필수 필드가 있으면, 가져오기 템플릿에 정의된 일부 필드에 데이터가 없어도 데이터를 가져올 수 있습니다. 중복은 외부 또는 내부 일치 키를 사용하여 여러 가져오기 요청에서 관리됩니다. 자체 일치 키 `External ID`를 입력할 경우 이 필드는 레코드를 고유하게 식별하고 가져오는 데 사용됩니다. 일치 키를 지정하지 않으면 가져오기에서 가져오기 템플릿에 있는 일부 열에서 파생된 내부 생성 일치 키를 사용합니다. 이 일치에 대한 자세한 내용은 검색된 서버 및 애플리케이션을 위한 매칭 로직 단원을 참조하십시오.

> **Note**
>
> Migration Hub 가져오기는 가져오기 템플릿에 정의된 필드 외의 다른 필드를 지원하지 않습니다. 제공한 사용자 지정 필드는 무시되며 가져오지 않습니다.

가져오기 권한 설정

데이터를 가져오려면 IAM 사용자에게 업로드하는 데 필요한 Amazon S3 권한 () 이 있어야 합니다.`s3:PutObject`) 파일을 Amazon S3로 가져오고 객체를 읽으려면 (`s3:GetObject`). 또한 프로그래밍 방식 액세스를 설정해야 합니다.AWS CLI) 또는 IAM 정책을 생성하고 가져오기를 수행하는 IAM 사용자에게 연결하여 콘솔에 액세스합니다.AWS계정.

Console Permissions

다음 절차를 통해 가져오기 요청을 수행할 IAM 사용자에 대한 권한 정책을 편집합니다.AWS콘솔을 사용하여 계정을 생성합니다.

사용자의 연결된 관리형 정책을 편집하려면

1. AWS Management Console에 로그인하여 https://console.aws.amazon.com/iam/에서 IAM 콘솔을 엽니다.
2. 탐색 창에서 사용자를 선택합니다.
3. 권한 정책을 변경하려는 사용자의 이름을 선택합니다.
4. 권한 탭을 선택한 후 권한 추가를 선택합니다.
5. 기존 정책 직접 연결을 선택한 후 정책 생성을 선택합니다.

    a. 정책 생성 페이지에서 JSON을 선택하고 다음 정책에 붙여 넣습니다. 버킷 이름을 IAM 사용자가 가져오기 파일을 업로드할 버킷의 실제 이름으로 바꿉니다.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "s3:GetBucketLocation",
        "s3:ListAllMyBuckets"
      ],
```

```
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": ["s3:ListBucket"],
      "Resource": ["arn:aws:s3:::importBucket"]
    },
    {
      "Effect": "Allow",
      "Action": [
        "s3:PutObject",
        "s3:GetObject",
        "s3:DeleteObject"
      ],
      "Resource": ["arn:aws:s3:::importBucket/*"]
    }
  ]
}
```

b. 정책 검토(Review policy)를 선택합니다.

c. 정책 요약을 검토하기 전에 이름에 새 정책 이름을 지정하고, 필요한 경우 설명을 입력합니다.

d. Create policy(정책 생성)를 선택합니다.

6. 로 돌아갑니다권한가져오기 요청을 수행할 사용자의 IAM 콘솔 페이지입니다.AWS계정.
7. 정책 테이블을 새로 고치고 방금 생성한 정책의 이름을 검색합니다.
8. [다음: 권한(Next: Review)]를 선택합니다.
9. 권한 추가(Add permissions)를 선택합니다.

IAM 사용자에게 정책을 추가했으며 이제 가져오기 프로세스를 시작할 수 있습니다.

AWS CLI Permissions

다음 절차에 따라 IAM 사용자에게 다음을 사용하여 데이터 가져오기를 요청할 수 있는 권한을 부여하는 데 필요한 관리형 정책을 생성합니다.AWS CLI.

관리형 정책을 생성하여 연결하려면

1. 사용`aws iam create-policy` AWS CLI명령을 사용하여 다음 권한을 갖는 IAM 정책을 생성합니다. 버킷 이름을 IAM 사용자가 가져오기 파일을 업로드할 버킷의 실제 이름으로 바꿉니다.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": ["s3:ListBucket"],
      "Resource": ["arn:aws:s3:::importBucket"]
    },
    {
      "Effect": "Allow",
      "Action": [
        "s3:PutObject",
        "s3:GetObject",
        "s3:DeleteObject"
      ],
      "Resource": ["arn:aws:s3:::importBucket/*"]
    }
  ]
}
```

이 명령의 사용에 대한 자세한 내용은 단원을 참조하십시오.create-policy의AWS CLI명령 참조.

2. 사용aws iam create-policy AWS CLI명령을 사용하여 다음 권한을 갖는 IAM 정책을 생성합니다.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "discovery:ListConfigurations",
                "discovery:CreateApplication",
                "discovery:UpdateApplication",
                "discovery:AssociateConfigurationItemsToApplication",
                "discovery:DisassociateConfigurationItemsFromApplication",
                "discovery:GetDiscoverySummary",
                "discovery:StartImportTask",
                "discovery:DescribeImportTasks",
                "discovery:BatchDeleteImportData"
            ],
```

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

3. 사용aws iam attach-user-policy AWS CLI이전 두 단계에서 생성한 정책을 명령을 사용하여 가져오기 요청을 수행할 IAM 사용자에게 연결합니다.AWS를 사용하는 계정AWS CLI. 이 명령의 사용에 대한 자세한 내용은 단원을 참조하십시오.attach-user-policy의AWS CLI명령 참조.

IAM 사용자에게 정책을 추가했으며 이제 가져오기 프로세스를 시작할 수 있습니다.

지정된 Amazon S3 버킷에 객체를 업로드할 경우, 객체에 대해 설정된 기본 권한을 그대로 유지해야 사용자가 객체를 읽을 수 있습니다.

Amazon S3로 가져오기 파일 업로드

그런 다음 CSV 형식의 가져오기 파일을 Amazon S3로 업로드해야 가져올 수 있습니다. 시작하기 전에 생성하거나 선택한 가져오기 파일을 보관할 Amazon S3 버킷이 있어야 합니다.

Console S3 Upload

Amazon S3로 가져오기 파일을 업로드하려면

1. AWS Management Console에 로그인한 후 https://console.aws.amazon.com/s3/에서 Amazon S3 콘솔을 엽니다.
2. 버킷 이름 목록에서 객체를 업로드하려는 버킷 이름을 선택합니다.
3. 업로드를 선택합니다.
4. 업로드 대화 상자에서 파일 추가를 선택한 후 업로드할 파일을 선택합니다.
5. 업로드할 파일을 선택한 후 열기를 선택합니다.
6. 업로드를 선택합니다.
7. 파일을 업로드한 후 버킷 대시보드에서 데이터 파일 객체 이름을 선택합니다.
8. 객체 세부 정보 페이지의 개요 탭에서 객체 URL을 복사합니다. 이 URL은 가져오기 요청을 생성할 때 필요합니다.
9. 위치로 이동합니다가져오기에 설명된 대로 Migration Hub 콘솔의 페이지데이터 가져오기. 그런 다음 객체 URL을Amazon S3 객체 URL필드.

AWS CLI S3 Upload

Amazon S3로 가져오기 파일을 업로드하려면

1. 터미널 창을 열고 가져오기 파일이 저장된 디렉터리로 이동합니다.
2. 다음 명령을 입력합니다.

```
aws s3 cp ImportFile.csv s3://BucketName/ImportFile.csv
```

3. 그러면 다음 결과가 반환됩니다.

```
upload: .\ImportFile.csv to s3://BucketName/ImportFile.csv
```

4. 반환된 전체 Amazon S3 객체 경로를 복사합니다. 이 URL은 가져오기 요청을 생성할 때 필요합니다.

데이터 가져오기

Migration Hub 콘솔에서 가져오기 템플릿을 다운로드하여 기존 온프레미스 서버 데이터로 채우면 Migration Hub 로 데이터 가져오기를 시작할 수 있습니다. 다음 지침에서는 콘솔을 사용하거나, 를 통한 API 호출을 사용하는 방법이 여기에 해당됩니다.AWS CLI.

Console Import

에서 데이터 가져오기 시작도구Migration Hub 콘솔의 페이지입니다.

데이터 가져오기를 시작하려면

1. 탐색 창의 검색에서 도구를 선택합니다.
2. 가져오기 템플릿을 아직 작성하지 않은 경우 가져오기 상자에서 템플릿 가져오기를 선택하여 템플릿을 다운로드할 수 있습니다. 다운로드한 템플릿을 열고 기존 온프레미스 서버 데이터로 채웁니다. 또한 Amazon S3 버킷에서 가져오기 템플릿을 다운로드할 수도 있습니다.https://s3.us-west-2.amazonaws.com/templates-7cffcf56-bd96-4b1c-b45b-a5b42f282e46/import_template.csv
3. 를 열려면가져오기페이지가져오기의가져오기상자.
4. 언더을 가져옵니다에서 가져오기 이름을 지정합니다.

5. 을 입력합니다Amazon S3 객체 URL필드. 이 단계를 수행하려면 가져오기 데이터 파일을 Amazon S3로 업로드해야 합니다. 자세한 정보는 Amazon S3로 가져오기 파일 업로드을 참조하세요.
6. 하단 오른쪽 부분에서 가져오기를 선택합니다. 그러면 가져오기 페이지가 열립니다. 이 페이지의 표에서 가져오기와 해당 상태를 볼 수 있습니다.

데이터 가져오기를 시작하기 위한 선행 절차를 수행하면, 가져오기 페이지에 진행 상태, 완료 시간, 성공 또는 실패한 레코드 수를 비롯하여 각 가져오기 요청의 세부 정보가 표시되고 해당 레코드를 다운로드할 수 있는 기능이 제공됩니다. 이 화면에서 서버 페이지의 검색으로 이동하여 실제 가져온 데이터를 볼 수도 있습니다.

서버 페이지에서 검색된 모든 서버(디바이스) 목록과 가져오기 이름을 볼 수 있습니다. 다음 위치에서 탐색할 때가져오기(가져오기 기록) 페이지에 나열된 가져오기 이름을 선택하여이름열에 이동하게 됩니다.서버선택한 가져오기의 데이터 세트를 기반으로 필터가 적용되는 페이지입니다. 그러면 해당 가져오기에 속한 데이터만 볼 수 있습니다.

아카이브는 .zip 형식이며, `errors-file` 파일과 `failed-entries-file` 파일이 들어 있습니다. 오류 파일에는 각 실패한 각 행과 연결된 오류 메시지 및 가져오기에 실패한 데이터 파일의 관련 열 이름이 들어 있습니다. 이 파일을 사용하여 문제가 발생한 위치를 빠르게 식별할 수 있습니다. 실패한 항목 파일에는 각 행과 실패한 모든 열이 포함되어 있습니다. 이 파일의 오류 파일에서 호출된 내용을 변경하고 수정된 정보로 파일을 다시 가져오십시오.

AWS CLI Import

AWS CLI에서 데이터 가져오기 프로세스를 시작하려면 먼저 환경에 AWS CLI를 설치해야 합니다. 자세한 내용은 단원을 참조하십시오.다음 설치AWSCommand Line Interface의AWS Command Line Interface사용 설명서.

> **Note**
>
> 가져오기 템플릿 파일을 아직 작성하지 않은 경우 Amazon S3 버킷에서 가져오기 템플릿을 다운로드할 수 있습니다.https://s3.us-west-2.amazonaws.com/templates-7cffcf56-bd96-4b1c-b45b-a5b42f282e46/import_template.csv

데이터 가져오기를 시작하려면

1. 터미널 창을 열고 다음 명령을 입력합니다.

```
aws discovery start-import-task --import-url s3://BucketName/ImportFile.csv --
name ImportName
```

2. 그러면 가져오기 작업이 생성되고 다음 상태 정보가 반환됩니다.

```
{
    "task": {
        "status": "IMPORT_IN_PROGRESS",
        "applicationImportSuccess": 0,
        "serverImportFailure": 0,
        "serverImportSuccess": 0,
        "name": "ImportName",
        "importRequestTime": 1547682819.801,
        "applicationImportFailure": 0,
        "clientRequestToken": "EXAMPLE1-abcd-1234-abcd-EXAMPLE1234",
        "importUrl": "s3://BucketName/ImportFile.csv",
        "importTaskId": "import-task-EXAMPLE1229949eabfEXAMPLE03862c0"
    }
}
```

Migration Hub 가져오기 요청 추적

콘솔을 사용하여 Migration Hub 가져오기 요청의 상태를 추적할 수 있습니다.AWS CLI또는 다음 중 하나를 수행합니다.AWSSDK.

Console Tracking

에서가져오기Migration Hub 콘솔의 대시보드에서 다음 요소를 찾을 수 있습니다.

- 이름— 가져오기 요청의 이름입니다.
- 가져오기 ID— 가져오기 요청의 고유 ID입니다.
- 을 가져옵니다— 가져오기 요청이 생성된 날짜와 시간입니다.
- 을 가져옵니다— 가져오기 요청의 상태입니다. 다음 값 중 하나일 수 있습니다.
  - 가져오는 중— 이 데이터 파일을 현재 가져오는 중입니다.
  - 을 가져옵니다— 전체 데이터 파일을 성공적으로 가져왔습니다.
  - 오류와 함께 가져옴— 데이터 파일의 레코드 중 한 개 이상을 가져오는 데 실패했습니다. 실패한 레코드를 해결하려면 가져오기 작업에 대해 레코드를 다운로드하지 못함을 선택하고 실패한 항목 csv 파일의 오류를 해결한 후 다시 가져오기를 수행합니다.

- 을 가져옵니다— 가져온 데이터 파일의 레코드를 가져오지 못했습니다. 실패한 레코드를 해결하려면 가져오기 작업에 대해 레코드를 다운로드하지 못함을 선택하고 실패한 항목 csv 파일의 오류를 해결한 후 다시 가져오기를 수행합니다.
- 가져온 레코드— 특정 데이터 파일에서 성공적으로 가져온 레코드의 수입니다.
- 실패한 레코드— 특정 데이터 파일에서 가져오지 못한 레코드의 수입니다.

CLI Tracking

`aws discovery describe-import-tasks` AWS CLI 명령을 사용하여 가져오기 작업의 상태를 추적할 수 있습니다.

1. 터미널 창을 열고 다음 명령을 입력합니다.

   ```
   aws discovery describe-import-tasks
   ```

2. 이렇게 하면 모든 가져오기 작업의 목록이 JSON 형식으로 반환되며, 상태 및 기타 관련 정보가 함께 제공됩니다. 결과를 필터링하여 가져오기 작업의 하위 집합을 반환할 수도 있습니다(선택 사항).

가져오기 작업을 추적할 경우 반환된 `serverImportFailure` 값이 0보다 큰 것을 볼 수 있습니다. 이 경우 가져오기 파일에 가져오지 못한 항목이 한 개 이상 있는 것입니다. 이 문제는 실패한 레코드 아카이브를 다운로드하고, 내부의 파일을 검토하며, 수정된 failure-entries.csv 파일로 다른 가져오기 요청을 수행하여 해결할 수 있습니다.

가져오기 작업을 생성한 후 추가 작업을 수행하여 데이터 마이그레이션을 관리하고 추적할 수 있습니다. 예를 들어 특정 요청에 대해 실패한 레코드의 아카이브를 다운로드할 수 있습니다. 실패한 레코드 아카이브를 사용하여 가져오기 문제를 해결하는 방법은 레코드 가져오기 실패 문제 해결 단원을 참조하십시오.

검색된 데이터 보기, 내보내기 및 탐색

Application Discovery Service 에이전트 없는 컬렉터 (에이전트 없는 컬렉터) 및AWS디스커버리 에이전트 (디스커버리 에이전트) 는 평균 및 최대 사용률을 기준으로 시스템 성능 데이터를 제공합니다. 수집된 시스템 성능 데이터를 사용하여 높은 수준의 총 소유 비용 (TCO) 을 수행할 수 있습니다. Discovery Agent는 시스템 성능 정보, 인바운드 및 아웃바운드 네트워크 연결, 서버에서 실행되는 프로세스에 대한 시계열 데이터를 비롯한 보다 자세한 데이터를 수집합니다. 서버 간 네트워크 종속성을 이해하고 마이그레이션 계획을 위한 애플리케이션으로 관련 서비스를 그룹화 하는 데 이 데이터를 사용할 수 있습니다.

이 섹션에서는 콘솔과 콘솔에서 에이전트리스 컬렉터 및 디스커버리 에이전트가 검색한 데이터를 보고 사용하는 방법에 대한 지침을 찾을 수 있습니다.AWS CLI.

주제

- Migration Hub 콘솔을 사용하여 수집된 데이터 보기
- 수집된 데이터 내보내기
- Amazon Athena 데이터 탐색

Migration Hub 콘솔을 사용하여 수집된 데이터 보기

Application Discovery Service 에이전트리스 컬렉터 (에이전트리스 컬렉터) 와AWS 검색 에이전트 (Discovery Agent) 모두 데이터 수집 프로세스가 시작된 후 콘솔을 사용하여 서버 및 VM에 대해 수집된 데이터를 볼 수 있습니다. 데이터는 데이터 수집이 시작된 후 약 15분 후에 콘솔에 표시됩니다. 를 사용하여 API를 호출하여 수집된 데이터를 내보내 이 데이터를 CSV 형식으로 볼 수도AWS CLI 있습니다. 수집된 데이터를 내보내는 방법은 다음 섹션에서 다룹니다수집된 데이터 내보내기.

검색된 서버에 대해 수집된 데이터 보기

1. 콘솔 탐색 창에서 Servers(서버)를 선택합니다. 검색된 서버가 서버 목록으로 표시됩니다.
2. 수집된 데이터로 구성된 세부 정보는 Server info(서버 정보) 열의 서버 이름 링크를 선택합니다. 그러면 시스템 정보, 성능 지표 같은 상세 정보를 설명하는 화면이 표시됩니다.

콘솔을 사용하여 에이전트 없는 Collector 또는 Discovery Agent가 검색한 서버를 보고, 정렬하고, 태그를 지정하는 방법에 대한 자세한 내용은 을 참조하십시오AWS Application Discovery Service콘솔 안내.

에이전트 없는 수집기 데이터베이스 및 분석 데이터 수집 모듈은 수집된 데이터를 Amazon S3 버킷에 업로드합니다. AWSDMS 콘솔에서 이 버킷의 데이터를 볼 수 있습니다.

검색된 데이터베이스 및 분석 서버에 대해 수집된 데이터를 보려면

1. AWS Management Console로그인하고 https://console.aws.amazon.com/dms/v2/ 에서AWS DMS 콘솔을 엽니다.
2. 디스커버에서 인벤토리를 선택합니다. 인벤토리 페이지가 열리고 검색된 데이터베이스 및 분석 서버의 목록이 표시됩니다.

검색된 서버 및 애플리케이션을 위한 매칭 로직

AWS Application Discovery Service(Application Discovery Service) 에는 검색한 서버가 기존 항목과 일치하는지 식별하는 매칭 로직이 내장되어 있습니다. 이 로직에서 일치를 찾으면 기존의 검색된 서버의 정보를 새 값으로 업데이트합니다.

이 매칭 로직은AWS Migration Hub (Migration Hub) 가져오기, Application Discovery Service 에이전트리스 컬렉터 (Agentless Collector),AWS 애플리케이션 검색 에이전트 (Discovery Agent) 및 기타 마이그레이션 도구를 비롯한 여러 소스의 중복 서버를 처리합니다. Migration Hub 가져오기에 대한 자세한 내용은 Migration Hub 가져오기를 참조하십시오.

서버 검색이 이루어지면 각 항목은 가져온 서버가 이미 존재하지 않음을 확인하기 위해 이전에 가져온 레코드와 교차 검사됩니다. 일치하는 항목이 없으면 새 레코드가 생성되고 새 고유 서버 식별자가 할당됩니다. 일치하는 항목이 발견될 경우 새 항목은 계속 생성되지만 기존 서버와 동일한 고유 서버 식별자가 할당됩니다. Migration Hub 콘솔에서 이 서버를 볼 때 해당 서버의 고유한 항목이 하나뿐입니다.

이 항목과 관련된 서버 속성은 병합되어 이전에 사용 가능한 레코드와 새로 가져온 레코드의 속성 값을 표시합니다. 여러 소스의 특정 서버 속성에 대해 값이 두 개 이상 있는 경우(예: 가져오기를 사용하여 검색된 특정 서버 및 검색 에이전트에서 검색된 `Total RAM`에 대해 서로 다른 두 개의 값이 있는 경우) 가장 최근에 업데이트된 값이 서버에 대한 일치 레코드에 표시됩니다.

매칭 필드

다음 필드는 검색 도구 사용 시 서버를 일치시키는 데 사용됩니다.

- ExternalId— 서버를 매칭하는 데 사용되는 기본 필드입니다. 이 필드의 값이 다른`ExternalId` 항목의 값과 동일하면 Application Discovery Service Service는 다른 필드의 일치 여부에 관계없이 두 항목을 일치시킵니다.

- IPAddress
- HostName
- MacAddress
- VM웨어. MoRefId및 VM웨어. vCenterId— Application Discovery Service Service가 일치를 수행하려면 이 두 값이 모두 다른 항목의 해당 필드와 동일해야 합니다.

수집된 데이터 내보내기

Application Discovery Service 에이전트리스 컬렉터 (에이전트리스 컬렉터) 와AWS 애플리케이션 검색 에이전트 (Discovery Agent) 모두 데이터 수집 프로세스가 시작된 후 서버와 VM에 대해 수집된 데이터를 내보낼 수 있습니다. 이 데이터는 데이터를 수집하는 데 사용한 검색 도구에 따라 콘솔과 상호 작용하거나 를 통해 API를 호출하여 내보낼 수 있습니다.AWS CLI

선택 방법을 넓힐 수 있도록, 아래에서 두 방법에 대한 지침을 제공하고 있습니다.

를 사용하여 모든 서버에 대해 수집된 데이터를 내보냅니다.AWS CLI

호스트 및 VM에서 실행되는 모든 에이전트 없는 수집기 및 검색 에이전트에서 수집된 데이터는AWS Command Line Interface (AWS CLI) 를 사용하여 대량으로 내보낼 수 있습니다. 데이터를 내보내기 전에 사용자 환경에AWS CLI 설치해야 합니다.

AWS CLI 설치 및 수집된 데이터 내보내기

1. 아직 설치하지 않은 경우, OS 유형(Windows 또는 Mac/Linux)에 맞는 AWS CLI를 설치합니다. 설치 지침은 사용 AWS Command Line Interface설명서를 참조하십시오.
2. 명령 프롬프트(Windows) 또는 터미널(MAC/Linux)을 엽니다.
   a. `aws configure`를 입력하고 Enter 키를 누릅니다.
   b. AWS액세스 키 ID와AWS 보안 액세스 키를 입력합니다.
   c. 기본 리전 이름에 `us-west-2`를 입력합니다.
   d. 기본 출력 형식에 `text`를 입력합니다.
3. 다음 명령을 입력해 내보내기 ID를 생성합니다.

```
aws discovery start-export-task
```

4. 이전 단계에서 생성한 내보내기 ID를 사용, 다음 명령을 입력해 파라미터 `"configurationsDownloadUrl"`의 값인 S3 URL을 생성합니다.

```
aws discovery describe-export-tasks --export-ids <export ID>
```

5. 이전 단계에서 생성한 URL을 복사해 브라우저에 붙여넣어 검색된 서버에 대해 수집된 데이터를 zip 파일로 다운로드합니다.

콘솔을 사용하여 상담원이 수집한 데이터 내보내기

콘솔에서 에이전트가 수집한 데이터를 내보내는 작업은 특정 서버의 세부 정보 페이지에서 에이전트 한 개로 제한됩니다. 세부 정보 페이지에서 화면 하단의 내보내기 아래에 서버의 내보내기 작업이 나열되어 있습니다. 내보내기 작업이 없으면 테이블은 비어 있습니다. 한 번에 최대 5회의 서버 데이터 내보내기를 실행할 수 있습니다.

발견된 서버에 대해 수집된 데이터 내보내기

1. 탐색 창에서 Servers(서버)를 선택합니다.
2. 서버 정보 열에서 데이터를 내보낼 대상 서버의 링크를 선택합니다.
3. 화면 맨 아래 내보내기 섹션에서 Export server details(서버 세부 정보 내보내기)를 선택합니다.
4. Export server details(서버 세부 정보 내보내기)에서 시작일 및 시간을 입력합니다.

> **Note**
>
> 시작 시간은 현재 시간에서 72시간 이내여야 합니다.

5. [Export]를 선택해 작업을 시작합니다. 최초 상태는 In-progress(진행 중)이며, 상태를 업데이트하려면 내보내기 섹션에서 새로 고침 아이콘을 클릭합니다.
6. 내보내기 작업이 완료되면 다운로드를 선택하고 .zip 파일을 저장합니다.
7. 저장된 파일의 압축을 풉니다. .csv 파일 세트에는 내보내기 데이터가 들어 있습니다.

   Microsoft Excel에서 .csv 파일을 열고 내보낸 서버 데이터를 검토할 수 있습니다.

   파일 중에 내보내기 작업과 그 결과에 대한 데이터가 포함된 JSON 파일이 있습니다.

> **Note**
>
> AWS Migration Hub콘솔에서 Amazon Elastic Compute Cloud (Amazon EC2) 인스턴스 권장 사항을 생성하고 내보내는 방법에 대한 자세한 내용은 AWS Migration Hub사용 설명서의 Amazon EC2 인스턴스 권장 사항을 참조하십시오.

Amazon Athena 데이터 탐색

Amazon Athena 데이터 탐색을 사용하면 Discovery Agent가 검색한 모든 온프레미스 서버에서 수집한 데이터를 한 곳에서 분석할 수 있습니다. Amazon Athena에서 데이터 탐색이 활성화되면 Migration Hub 콘솔에서 (또는 StartContinousExport API) 및 에이전트에 대한 데이터 수집이 켜지면 에이전트에서 수집한 데이터가 정기적으로 S3 버킷에 자동으로 저장됩니다.

그런 다음 Amazon Athena를 방문하여 사전 정의된 쿼리를 실행하여 각 서버의 시계열 시스템 성능, 각 서버에서 실행되는 프로세스 유형 및 서로 다른 서버 간의 네트워크 종속성을 분석할 수 있습니다. 또한 Amazon Athena를 사용하여 사용자 지정 쿼리를 작성하고, 구성 관리 데이터베이스 (CMDB) 내보내기와 같은 기존 데이터 소스를 추가로 업로드하고, 검색된 서버를 실제 비즈니스 애플리케이션과 연결할 수 있습니다. Athena 데이터베이스를 Amazon과 통합할 수도 있습니다. QuickSight 쿼리 출력을 시각화하고 추가 분석을 수행할 수 있습니다.

Steps

1. Amazon Athena에서 데이터 탐색 지원
2. Amazon Athena에서 데이터 탐색 작업

Amazon Athena에서 데이터 탐색 지원

Amazon Athena에서의 데이터 탐색은 Migration Hub 콘솔이나 에서 API 호출을 사용하여 연속 내보내기를 켜면 활성화됩니다.AWS CLI. Amazon Athena에서 검색된 데이터를 보고 탐색을 시작하려면 먼저 데이터 탐색을 켜야 합니다.

[연속 내보내기] 에서 서비스 연결 역할`AWSServiceRoleForApplicationDiscoveryServiceContinuousExport`사용자 계정에서 자동으로 사용됩니다. 이 서비스 연결 역할에 대한 자세한 내용은 Application Discovery 서비스에 대한 서비스 연결 역할 권한 단원을 참조하십시오.

다음 지침은 콘솔과 콘솔을 사용하여 Amazon Athena에서 데이터 탐색을 활성화하는 방법을 보여줍니다.AWS CLI.

Enable with the console

Amazon Athena의 데이터 탐색은 “데이터 수집 시작”을 선택하거나 “Amazon Athena에서의 데이터 탐색”이라고 표시된 토글을 클릭하면 묵시적으로 연속 내보내기가 활성화되어 활성화됩니다.데이터 수집기Migration Hub 콘솔의 페이지입니다.

콘솔에서 Amazon Athena에서 데이터 탐색을 활성화하려면

1. 탐색 창에서 Data Collectors(데이터 수집기)를 선택합니다.
2. 에이전트 탭을 선택합니다.
3. 선택해데이터 수집 시작또는 이미 데이터 수집이 켜져 있는 경우Amazon Athena 데이터 탐색비장.
4. 이전 단계에서 생성된 대화 상자에서 관련 비용에 대해 동의하는 확인란을 클릭하고 계속 또는 활성화를 선택합니다.

> **Note**
>
> 이제 에이전트가 “연속 내보내기” 모드로 실행되므로 Amazon Athena에서 검색된 데이터를 보고 작업할 수 있습니다. 처음 활성화하면 데이터가 Amazon Athena에 표시되는 데 최대 30분이 걸릴 수 있습니다.

Enable with the AWS CLI

Amazon Athena에서의 데이터 탐색은 API 호출을 통해 연속 내보내기가 명시적으로 활성화되어 있으므로 활성화됩니다.AWS CLI. 이렇게 하려면 먼저 환경에 AWS CLI가 설치되어 있어야 합니다.

를 설치하려면AWS CLIAmazon Athena에서 데이터 탐색을 활성화합니다.

1. 운영 체제(Linux, macOS, Windows)에 맞는 AWS CLI를 설치합니다. 다음을 참조:AWS Command Line Interface사용 설명서지침을 위해.
2. 명령 프롬프트(Windows) 또는 터미널(Linux나 macOS)을 엽니다.
   a. `aws configure`를 입력하고 Enter 키를 누릅니다.
   b. 귀하의 정보를 입력하십시오AWS액세스 키 ID 및AWS보안 액세스 키.

c. 기본 리전 이름에 `us-west-2`를 입력합니다.

d. 기본 출력 형식에 `text`를 입력합니다.

3. 다음 명령을 입력합니다.

```
aws discovery start-continuous-export
```

> **Note**
>
> 이제 에이전트가 "연속 내보내기" 모드로 실행되므로 Amazon Athena에서 검색된 데이터를 보고 작업할 수 있습니다. 처음 활성화하면 데이터가 Amazon Athena에 표시되는 데 최대 30분이 걸릴 수 있습니다.

Amazon Athena에서 데이터 탐색 작업

Amazon Athena에서 데이터 탐색을 활성화한 후에는 Athena에서 직접 데이터를 쿼리하여 에이전트가 검색한 상세한 최신 데이터를 탐색하고 작업할 수 있습니다. 데이터를 사용하여 스프레드시트를 생성하고, 비용 분석을 실행하며, 시각화 프로그램으로 쿼리를 이식하고, 네트워크 종속성을 다이어그램으로 표시할 수 있습니다.

이 섹션의 항목에서는 Athena 데이터를 사용하여 로컬 환경을 다음으로 마이그레이션하기 위한 평가 및 계획을 수립하는 방법을 설명합니다.AWS.

주제

- Amazon Athena에서 직접 데이터 탐색
- Amazon Athena 데이터 시각화
- Athena에서 사용할 사전 정의된 쿼리

Amazon Athena에서 직접 데이터 탐색

다음 지침에서는 Athena 콘솔에서 직접 Athena 데이터를 탐색하는 방법을 설명합니다. Athena에 데이터가 없거나 Amazon Athena에서 데이터 탐색을 활성화하지 않은 경우 에 설명된 대로 Amazon Athena에서 데이터 탐색을 활성화하라는 대화 상자가 표시됩니다.Amazon Athena에서 데이터 탐색 지원.

Athena에서 에이전트가 발견한 데이터를 직접 탐색하려면

1. AWS Migration Hub 콘솔을 열고, 탐색 창에서 Servers(서버)를 선택합니다.
2. Amazon Athena 콘솔을 열려면 다음을 선택하십시오.Amazon Athena에서 데이터 탐색.
3. 쿼리 편집기 페이지에서 탐색 창의 데이터베이스 아래에 application_discovery_service_database가 선택되어 있는지 확인합니다.

   > **Note**
   >
   > 테이블 아래에 있는 다음 테이블은 에이전트로 그룹화된 데이터 세트를 나타냅니다.
   >
   > - os_info_agent
   > - network_interface_agent
   > - sys_performance_agent
   > - processes_agent
   > - inbound_connection_agent
   > - outbound_connection_agent
   > - id_mapping_agent

4. Athena 쿼리 편집기에서 SQL 쿼리를 작성하고 실행하여 Amazon Athena 콘솔에서 데이터를 쿼리합니다. 예를 들어, 검색된 모든 서버 IP 주소를 보려면 다음 쿼리를 사용할 수 있습니다.

   ```
   SELECT * FROM network_interface_agent;
   ```

   더 많은 예제 쿼리는 Athena에서 사용할 사전 정의된 쿼리 단원을 참조하십시오.

Amazon Athena 데이터 시각화

데이터를 시각화하기 위해 Amazon 같은 시각화 프로그램에 쿼리를 포팅할 수 있습니다. QuickSight 또는 사이토스케이프, Yed 또는 Gelphi와 같은 기타 오픈 소스 시각화 도구. 이러한 도구를 사용하여 네트워크 다이어그램, 요약 차트 및 기타 그래픽을 렌더링할 수 있습니다. 이 방법을 사용하면 시각화 프로그램을 통해 Athena에 연결하면 Athena가 수집된 데이터에 원본으로 액세스하여 시각화를 생성할 수 있습니다.

Amazon을 사용하여 Amazon Athena 데이터를 시각화하려면 QuickSight

1. 에 로그인합니다.아마존 QuickSight.

2. Connect to another data source or upload a file(다른 데이터 원본에 연결 또는 파일 업로드)을 선택합니다.
3. 선택해Athena. 이새 Athena 데이터 원본대화 상자가 표시됩니다.
4. Data source name(데이터 원본 이름) 필드에 이름을 입력합니다.
5. [Create data source]를 선택합니다.
6. 단원을 선택합니다Agents-servers-os의 테이블테이블을 선택하세요대화 상자 및 선택Select.
7. 데이터 세트 생성 완료 대화 상자에서 더 빠른 분석을 위해 SPICE로 가져오기를 선택한 다음 시각화를 선택합니다.

   시각화가 렌더링됩니다.

Athena에서 사용할 사전 정의된 쿼리

이 단원에는 TCO 분석 및 네트워크 시각화와 같은 일반 사용 사례에 대한 미리 정의된 쿼리가 포함되어 있습니다. 이러한 쿼리를 있는 그대로 사용하거나 필요한 대로 수정할 수 있습니다.

사전 정의된 쿼리를 사용하려면 다음을 수행합니다.

1. AWS Migration Hub 콘솔을 열고, 탐색 창에서 Servers(서버)를 선택합니다.
2. Amazon Athena 콘솔을 열려면 다음을 선택하십시오.Amazon Athena에서 데이터 탐색.
3. 쿼리 편집기 페이지에서 탐색 창의 데이터베이스 아래에 application_discovery_service_database가 선택되어 있는지 확인합니다.
4. Query Editor(쿼리 편집기)에서 더하기(+) 기호를 선택하여 새 쿼리를 위한 탭을 생성합니다.
5. 사전 정의된 쿼리에서 쿼리 중 하나를 복사합니다.
6. 방금 생성한 새 쿼리 탭의 쿼리 창에 쿼리를 붙여 넣습니다.
7. 쿼리 실행(Run Query)을 선택합니다.

사전 정의된 쿼리

쿼리에 대한 정보를 보려면 해당 제목을 선택합니다.

서버의 IP 주소 및 호스트 이름 가져오기

이 보기 헬퍼 함수는 특정 서버의 IP 주소와 호스트 이름을 검색합니다. 다른 쿼리에서 이 보기를 사용할 수 있습니다. 뷰 생성에 대한 자세한 내용은 단원을 참조하십시오.뷰 생성에서Amazon Athena 사용 설명서.

```
CREATE OR REPLACE VIEW hostname_ip_helper AS
SELECT DISTINCT
  "os"."host_name"
, "nic"."agent_id"
, "nic"."ip_address"
FROM
  os_info_agent os
, network_interface_agent nic
WHERE ("os"."agent_id" = "nic"."agent_id");
```

에이전트가 있거나 없는 서버 식별

이 쿼리는 데이터의 유효성을 검증하는 데 도움이 됩니다. 네트워크의 여러 서버에 에이전트를 배포한 경우 이 쿼리를 사용하여 네트워크에 에이전트를 배포하지 않은 다른 서버가 있는지 확인할 수 있습니다. 이 쿼리에서는 인바운드 및 아웃바운드 네트워크 트래픽을 조회하고 프라이빗 IP 주소에 대해서만 트래픽을 필터링합니다. 즉, 192, 10 또는 172로 시작하는 IP 주소입니다.

```
SELECT DISTINCT "destination_ip" "IP Address" ,
         (CASE
    WHEN (
    (SELECT "count"(*)
    FROM network_interface_agent
    WHERE ("ip_address" = "destination_ip") ) = 0) THEN
        'no'
        WHEN (
        (SELECT "count"(*)
        FROM network_interface_agent
        WHERE ("ip_address" = "destination_ip") ) > 0) THEN
            'yes' END) "agent_running"
    FROM outbound_connection_agent
WHERE ((("destination_ip" LIKE '192.%')
        OR ("destination_ip" LIKE '10.%'))
        OR ("destination_ip" LIKE '172.%'))
UNION
SELECT DISTINCT "source_ip" "IP ADDRESS" ,
         (CASE
    WHEN (
    (SELECT "count"(*)
    FROM network_interface_agent
    WHERE ("ip_address" = "source_ip") ) = 0) THEN
        'no'
        WHEN (
```

```
        (SELECT "count"(*)
        FROM network_interface_agent
        WHERE ("ip_address" = "source_ip") ) > 0) THEN
            'yes' END) "agent_running"
    FROM inbound_connection_agent
WHERE ((("source_ip" LIKE '192.%')
        OR ("source_ip" LIKE '10.%'))
        OR ("source_ip" LIKE '172.%'));
```

에이전트가 있는 서버의 시스템 성능 데이터를 분석합니다.

이 쿼리를 사용하여 에이전트가 설치된 온프레미스의 시스템 성능 및 사용률 패턴 데이터를 분석할 수 있습니다. 이 쿼리는 각 서버의 호스트 이름을 식별하기 위해 system_performance_agent 테이블을 os_info_agent 테이블과 결합합니다. 이 쿼리는 에이전트가 실행 중인 모든 서버에 대해 시계열 사용률 데이터(15분 간격)를 반환합니다.

```
SELECT "OS"."os_name" "OS Name" ,
    "OS"."os_version" "OS Version" ,
    "OS"."host_name" "Host Name" ,
     "SP"."agent_id" ,
     "SP"."total_num_cores" "Number of Cores" ,
     "SP"."total_num_cpus" "Number of CPU" ,
     "SP"."total_cpu_usage_pct" "CPU Percentage" ,
     "SP"."total_disk_size_in_gb" "Total Storage (GB)" ,
     "SP"."total_disk_free_size_in_gb" "Free Storage (GB)" ,
     ("SP"."total_disk_size_in_gb" - "SP"."total_disk_free_size_in_gb") "Used
 Storage" ,
     "SP"."total_ram_in_mb" "Total RAM (MB)" ,
     ("SP"."total_ram_in_mb" - "SP"."free_ram_in_mb") "Used RAM (MB)" ,
     "SP"."free_ram_in_mb" "Free RAM (MB)" ,
     "SP"."total_disk_read_ops_per_sec" "Disk Read IOPS" ,
     "SP"."total_disk_bytes_written_per_sec_in_kbps" "Disk Write IOPS" ,
     "SP"."total_network_bytes_read_per_sec_in_kbps" "Network Reads (kbps)" ,
     "SP"."total_network_bytes_written_per_sec_in_kbps" "Network Write (kbps)"
FROM "sys_performance_agent" "SP" , "OS_INFO_agent" "OS"
WHERE ("SP"."agent_id" = "OS"."agent_id") limit 10;
```

포트 번호 및 프로세스 세부 정보를 기반으로 서버 간 아웃바운드 통신을 추적합니다.

이 쿼리는 포트 번호 및 프로세스 세부 정보와 함께 각 서비스의 아웃바운드 트래픽에 대한 세부 정보를 가져옵니다.

IANA에서 다운로드한 IANA 포트 레지스트리 데이터베이스가 포함된 `iana_service_ports_import` 테이블을 아직 생성하지 않았다면 쿼리를 실행하기 전에 이 테이블을 생성해야 합니다. 이 테이블 생성 방법에 대한 자세한 내용은 IANA 포트 레지스트리 임포트 테이블 생성 단원을 참조하십시오.

`iana_service_ports_import` 테이블이 생성되었으면 아웃바운드 트래픽을 추적하기 위한 두 가지 보기 헬퍼 함수를 생성합니다. 뷰 생성에 대한 자세한 내용은 단원을 참조하십시오.뷰 생성에서Amazon Athena 사용 설명서.

아웃바운드 추적 헬퍼 함수를 생성하려면

1. https://console.aws.amazon.com/athena/에서 Athena 콘솔을 엽니다.
2. 생성`valid_outbound_ips_helper`보기: 고유한 아웃바운드 대상 IP 주소를 모두 나열하는 다음 도우미 함수를 사용합니다.

```
CREATE OR REPLACE VIEW valid_outbound_ips_helper AS
SELECT DISTINCT "destination_ip"
FROM outbound_connection_agent;
```

3. 아웃바운드 트래픽에 대한 통신 빈도를 결정하는 다음 헬퍼 함수를 사용하여 `outbound_query_helper` 보기를 생성합니다.

```
CREATE OR REPLACE VIEW outbound_query_helper AS
SELECT "agent_id" ,
         "source_ip" ,
         "destination_ip" ,
         "destination_port" ,
         "agent_assigned_process_id" ,
         "count"(*) "frequency"
FROM outbound_connection_agent
WHERE (("ip_version" = 'IPv4')
        AND ("destination_ip" IN
    (SELECT *
    FROM valid_outbound_ips_helper )))
GROUP BY  "agent_id", "source_ip", "destination_ip", "destination_port",
 "agent_assigned_process_id";
```

4. `iana_service_ports_import` 테이블과 두 가지 헬퍼 함수를 생성한 후에는 다음 쿼리를 실행하여 포트 번호 및 프로세스 세부 정보와 함께 각 서비스의 아웃바운드 트래픽에 대한 세부 정보를 얻을 수 있습니다.

```
SELECT hip1.host_name "Source Host Name",
         outbound_connections_results0.source_ip "Source IP Address",
         hip2.host_name "Destination Host Name",
         outbound_connections_results0.destination_ip "Destination IP Address",
         outbound_connections_results0.frequency "Connection Frequency",
         outbound_connections_results0.destination_port "Destination Communication
 Port",
         outbound_connections_results0.servicename "Process Service Name",
         outbound_connections_results0.description "Process Service Description"
FROM
    (SELECT DISTINCT o.source_ip,
         o.destination_ip,
         o.frequency,
         o.destination_port,
         ianap.servicename,
         ianap.description
    FROM outbound_query_helper o, iana_service_ports_import ianap
    WHERE o.destination_port = TRY_CAST(ianap.portnumber AS integer)) AS
 outbound_connections_results0 LEFT OUTER
JOIN hostname_ip_helper hip1
    ON outbound_connections_results0.source_ip = hip1.ip_address LEFT OUTER
JOIN hostname_ip_helper hip2
    ON outbound_connections_results0.destination_ip = hip2.ip_address
```

포트 번호 및 프로세스 세부 정보를 기반으로 서버 간 인바운드 통신을 추적합니다.

이 쿼리는 포트 번호 및 프로세스 세부 정보와 함께 각 서비스의 인바운드 트래픽에 대한 정보를 가져옵니다.

IANA에서 다운로드한 IANA 포트 레지스트리 데이터베이스가 포함된 `iana_service_ports_import` 테이블을 아직 생성하지 않았다면 쿼리를 실행하기 전에 이 테이블을 생성해야 합니다. 이 테이블 생성 방법에 대한 자세한 내용은 IANA 포트 레지스트리 임포트 테이블 생성 단원을 참조하십시오.

`iana_service_ports_import` 테이블이 생성되었으면 인바운드 트래픽을 추적하기 위한 두 가지 보기 헬퍼 함수를 생성합니다. 뷰 생성에 대한 자세한 내용은 단원을 참조하십시오.뷰 생성에서Amazon Athena 사용 설명서.

가져오기 추적 헬퍼 함수를 생성하려면

1. https://console.aws.amazon.com/athena/에서 Athena 콘솔을 엽니다.

2. 모든 고유한 인바운드 소스 IP 주소를 나열하는 다음 헬퍼 함수를 사용하여 `valid_inbound_ips_helper` 보기를 생성합니다.

```
CREATE OR REPLACE VIEW valid_inbound_ips_helper AS
SELECT DISTINCT "source_ip"
FROM inbound_connection_agent;
```

3. 인바운드 트래픽에 대한 통신 빈도를 결정하는 다음 헬퍼 함수를 사용하여 `inbound_query_helper` 보기를 생성합니다.

```
CREATE OR REPLACE VIEW inbound_query_helper AS
SELECT "agent_id" ,
         "source_ip" ,
         "destination_ip" ,
         "destination_port" ,
         "agent_assigned_process_id" ,
         "count"(*) "frequency"
FROM inbound_connection_agent
WHERE (("ip_version" = 'IPv4')
        AND ("source_ip" IN
    (SELECT *
    FROM valid_inbound_ips_helper )))
GROUP BY  "agent_id", "source_ip", "destination_ip", "destination_port",
 "agent_assigned_process_id";
```

4. `iana_service_ports_import` 테이블과 두 가지 헬퍼 함수를 생성한 후에는 다음 쿼리를 실행하여 포트 번호 및 프로세스 세부 정보와 함께 각 서비스의 인바운드 트래픽에 대한 세부 정보를 얻을 수 있습니다.

```
SELECT hip1.host_name "Source Host Name",
         inbound_connections_results0.source_ip "Source IP Address",
         hip2.host_name "Destination Host Name",
         inbound_connections_results0.destination_ip "Destination IP Address",
         inbound_connections_results0.frequency "Connection Frequency",
         inbound_connections_results0.destination_port "Destination Communication
 Port",
         inbound_connections_results0.servicename "Process Service Name",
         inbound_connections_results0.description "Process Service Description"
FROM
    (SELECT DISTINCT i.source_ip,
         i.destination_ip,
         i.frequency,
```

```
        i.destination_port,
        ianap.servicename,
        ianap.description
    FROM inbound_query_helper i, iana_service_ports_import ianap
    WHERE i.destination_port = TRY_CAST(ianap.portnumber AS integer)) AS
 inbound_connections_results0 LEFT OUTER
JOIN hostname_ip_helper hip1
    ON inbound_connections_results0.source_ip = hip1.ip_address LEFT OUTER
JOIN hostname_ip_helper hip2
    ON inbound_connections_results0.destination_ip = hip2.ip_address
```

포트 번호에서 실행 중인 소프트웨어 식별

이 쿼리는 포트 번호를 기준으로 실행 중인 소프트웨어를 식별합니다.

IANA에서 다운로드한 IANA 포트 레지스트리 데이터베이스가 포함된 `iana_service_ports_import` 테이블을 아직 생성하지 않았다면 쿼리를 실행하기 전에 이 테이블을 생성해야 합니다. 이 테이블 생성 방법에 대한 자세한 내용은 IANA 포트 레지스트리 임포트 테이블 생성 단원을 참조하십시오.

다음 쿼리를 실행하여 포트 번호를 기준으로 실행 중인 소프트웨어를 식별합니다.

```
SELECT o.host_name "Host Name",
       ianap.servicename "Service",
       ianap.description "Description",
       con.destination_port,
       con.cnt_dest_port "Destination Port Count"
FROM   (SELECT agent_id,
               destination_ip,
               destination_port,
               Count(destination_port) cnt_dest_port
        FROM   inbound_connection_agent
        GROUP  BY agent_id,
                  destination_ip,
                  destination_port) con,
       (SELECT agent_id,
               host_name,
               Max("timestamp")
        FROM   os_info_agent
        GROUP  BY agent_id,
                  host_name) o,
       iana_service_ports_import ianap
```

```
WHERE  ianap.transportprotocol = 'tcp'
       AND con.destination_ip NOT LIKE '172%'
       AND con.destination_port = ianap.portnumber
       AND con.agent_id = o.agent_id
ORDER BY cnt_dest_port DESC;
```

IANA 포트 레지스트리 임포트 테이블 생성

미리 정의된 쿼리 중 일부에는 IANA(Internet Assigned Numbers Authority)에서 다운로드한 정보가 포함된 `iana_service_ports_import` 테이블이 필요합니다.

iana_service_ports_import 테이블을 생성하려면

1. IANA 포트 레지스트리 데이터베이스 다운로드CSV파일 원본서비스 이름 및 전송 프로토콜 포트 번호 레지스트리...에iana.org.
2. Amazon S3 S3로 파일을 업로드합니다. 자세한 내용은 S3 버킷에 파일 및 폴더를 업로드하려면 어떻게 해야 합니까?를 참조하십시오.
3. Athena에서 라는 이름의 새 테이블 만들기`iana_service_ports_import`. 지침은 단원을 참조하십시오.테이블 생성에서Amazon Athena 사용 설명서. 다음 예제에서는 `my_bucket_name`을 이전 단계에서 CSV 파일을 업로드한 S3 버킷의 이름으로 대치해야 합니다.

```
CREATE EXTERNAL TABLE IF NOT EXISTS iana_service_ports_import (
          ServiceName STRING,
          PortNumber INT,
          TransportProtocol STRING,
          Description STRING,
          Assignee STRING,
          Contact STRING,
          RegistrationDate STRING,
          ModificationDate STRING,
          Reference STRING,
          ServiceCode STRING,
          UnauthorizedUseReported STRING,
          AssignmentNotes STRING
)
ROW FORMAT SERDE 'org.apache.hadoop.hive.serde2.lazy.LazySimpleSerDe'
WITH SERDEPROPERTIES (
  'serialization.format' = ',',
  'quoteChar' = '"',
  'field.delim' = ','
) LOCATION 's3://my_bucket_name/'
```

```
TBLPROPERTIES ('has_encrypted_data'='false',"skip.header.line.count"="1");
```

AWS Application Discovery Service콘솔 안내

AWS Application Discovery Service(Application Discovery Service) 는 다음과 통합되었습니다.AWS Migration Hub(Migration Hub) 및 고객은 Migration Hub 내에서 데이터 수집기, 서버 및 애플리케이션을 보고 관리할 수 있습니다. Application Discovery Service 콘솔을 사용하면 Migration Hub 콘솔로 리디렉션됩니다. Migration Hub 콘솔로 작업하려면 별도의 단계나 설정이 필요하지 않습니다.

이 섹션에서는 Application Discovery Service Agentless Collector (Agentless Collector) 를 관리 및 모니터링하는 방법에 대해서 살펴보겠습니다.AWS콘솔을 사용하는 애플리케이션 검색 에이전트 (검색 에이전트).

주제

기본 대시보드

기본 대시보드를 보려면 다음을 선택합니다.대시보드(사용)AWS Migration Hub(Migration Hub) 콘솔 탐색 창. Migration Hub 기본 대시보드에서는 Application Discovery Service 에이전트리스 컬렉터 (에이전트 없는 컬렉터) 와 같은 서버, 애플리케이션 및 데이터 수집기에 대한 상위 수준의 통계를 볼 수 있습니다.AWS애플리케이션 검색 에이전트 (디스커버리 에이전트).

기본 대시보드

기본 대시보드는 중앙의 Discover(검색) 및 Migrate(마이그레이션) 대시보드에서 데이터를 수집합니다. 네 개의 상태 및 정보 창으로 구성되어 있고, 빠른 액세스를 위한 링크 목록이 있습니다. 이 창을 사용해 가장 최근 업데이트된 애플리케이션에 대한 요약된 상태를 확인할 수 있습니다. 또 애플리케이션에 빠르게 액세스하고, 여러 상태의 애플리케이션에 대한 개요 정보를 얻고, 시간에 따른 마이그레이션 진행 상황을 추적할 수 있습니다.

기본 대시보드를 보려면 다음을 선택합니다.대시보드Migration Hub 콘솔 홈 페이지의 왼쪽에 있는 탐색 창에서

데이터 수집 도구

Application Discovery Service 에이전트 없는 컬렉터 (에이전트 없는 컬렉터) 및AWS애플리케이션 검색 에이전트 (디스커버리 에이전트) 는 다음과 같은 데이터 수집 툴입니다.AWS Application Discovery Service(Application Discovery Service) 는 기존 인프라를 검색하는 데 사용됩니다. 다음 주제에서는 이러한 검색 데이터 수집 도구를 다운로드하고 배포하는 방법에 대해서 살펴봅니다.에이전트리스 컬렉터 시작하기과AWS 애플리케이션 검색 에이전트.

이러한 데이터 수집 툴은 각 서버와 해당 서버에서 실행되는 프로세스에 대한 세부 정보를 제공하는 Application Discovery Service의 리포지토리에 데이터를 저장합니다. 이러한 도구 중 하나를 배포하면에서 수집된 데이터를 시작, 중지 및 볼 수 있습니다.AWS Migration Hub(Migration Hub) 콘솔.

주제

- 데이터 수집기 시작 및 중지
- 데이터 수집기 보기 및 정렬

데이터 수집기 시작 및 중지

사용AWS애플리케이션 검색 에이전트 (Discovery Agent) 가 배포되면 에서 데이터 수집 프로세스를 시작하거나 중지할 수 있습니다.데이터 수집기페이지AWS Migration Hub(Migration Hub) 콘솔.

데이터 수집 도구 시작 및 중지

1. 사용AWS계정, 로그인AWS Management Console그런 다음 에서 Migration Hub 콘솔을 여십시오.https://console.aws.amazon.com/migrationhub/.
2. Migration Hub 콘솔 탐색 창에서발견하기, 선택데이터 수집기.
3. 에이전트 탭을 선택합니다.
4. 시작 또는 중지할 수집 도구의 확인란을 선택합니다.
5. Start data collection(데이터 수집 시작)이나 Stop data collection(데이터 수집 중지)를 선택합니다.

데이터 수집기 보기 및 정렬

여러 데이터 수집기를 배포한 경우 다음과 같이 표시된 배포된 수집기 목록을 정렬할 수 있습니다.데이터 수집기콘솔 페이지 검색줄에 필터를 적용하여 목록을 정렬합니다. Data Collectors(데이터 수집기) 목록에서 정의한 기준 대부분에 대해 검색 및 필터링을 할 수 있습니다.

다음 표에는 사용할 수 있는 검색 기준이 나와 있습니다.에이전트연산자, 값 및 값 정의를 포함합니다.

검색 기준	연산자	값: 정의
에이전트 ID	==	수집 도구가 설치된 미리 채워진 목록에서 선택한 모든 에이전트 ID.
Hostname	== !=	에이전트의 경우, 에이전트가 설치된 호스트의 미리 채워진 목록에서 선택한 호스트 이름입니다.
수집 상태	== !=	시작 데이터를 수집하여 Application Discovery Service 전송 중입니다. 시작 예정: 데이터 수집이 시작될 예정입니다. 데이터는 다음 ping 시 Application Discovery Service 전송되며 상태는 다음과 같이 변경됩니다.시작됨. 중지 데이터가 수집되거나 Application Discovery Service 전송되지 않습니다. 중지 데이터 수집은 중단될 예정입니다. 다음 ping 시 Application Discovery Service 데이터 전송이 중단되고 상태가 다음과 같이 변경됩니다.중지.
상태	== !=	Healthy 데이터 수집이 켜져 있지 않습니다. 도구는 정상 작동하고 있습니다.

검색 기준	연산자	값: 정의
		Unhealthy: 도구가 오류 상태입니다. 데이터 수집 및 보고가 되지 않습니다. 알 수 없음 한 시간 넘게 연결이 설정되지 않았습니다. 종료 이 도구는 시스템, 서비스 또는 데몬 종료로 인해 마지막으로 “종료 중”이라는 메시지를 보냈습니다. 재부팅이나 도구 업그레이드의 경우, 상태가 첫 보고 주기에 다른 상태로 변경됩니다. 실행 데이터 수집이 켜져 있습니다. 도구는 정상 작동하고 있습니다.
IP 주소	== !=	수집 도구가 설치된 미리 채워진 목록에서 선택한 IP 주소입니다.

다음 표에는 사용할 수 있는 검색 기준이 나와 있습니다.에이전트 없는 수집기연산자, 값 및 값 정의를 포함합니다.

검색 기준	연산자	값: 정의
ID	==	컬렉션 도구가 설치되어 있는 미리 채워진 목록에서 선택한 에이전트 없는 모든 컬렉터 ID.
Hostname	== !=	에이전트 없는 수집기의 경우 에이전트 없는 수집기가 설치된 미리 채워진 호스트 목록에

검색 기준	연산자	값: 정의
		서 선택한 모든 호스트 이름입니다.
상태	== !=	데이터 수집 데이터 수집이 켜져 있습니다. 도구는 정상 작동하고 있습니다. 구성 준비 완료 - 데이터 수집이 켜져 있지 않습니다. 도구는 정상 작동하고 있습니다. 주의 사항 - 도구가 오류 상태이므로 주의가 필요합니다. 알 수 없음 한 시간 넘게 연결이 설정되지 않았습니다. 종료: 이 도구는 시스템, 서비스 또는 데몬 종료로 인해 마지막으로 “종료 중”이라는 메시지를 보냈습니다. 재부팅이나 도구 업그레이드의 경우, 상태가 첫 보고 주기에 다른 상태로 변경됩니다.
IP 주소	== !=	수집 도구가 설치된 미리 채워진 목록에서 선택한 IP 주소입니다.

검색 필터를 적용해 데이터 수집기를 정렬

1. 사용AWS계정, 로그인AWS Management Console그런 다음 에서 Migration Hub 콘솔을 여십시오.https://console.aws.amazon.com/migrationhub/.
2. Migration Hub 콘솔 탐색 창에서발견하기, 선택데이터 수집기.
3. 다음 중 하나를 선택하세요에이전트 없는 수집기또는에이전트탭.
4. 검색 창 안을 클릭한 다음 목록에서 검색 기준을 선택합니다.

5. 다음 목록에서 연산자를 선택합니다.
6. 마지막 목록에서 값을 선택합니다.

서버 데이터 보기, 내보내기 및 탐색

Servers(서버) 페이지는 데이터 수집 도구에 알려진 각 서버 인스턴스에 대한 시스템 구성 및 성능 데이터를 제공합니다. 서버 정보를 보고, 필터로 서버를 정렬하고, 키 값 쌍으로 서버에 태그를 지정하고, 서버 및 시스템에 대한 세부 정보를 내보낼 수 있습니다.

주제

서버 보기 및 정렬

데이터 수집 도구가 검색한 서버에 대한 정보를 보고, 필터를 사용해 서버를 정렬할 수 있습니다.

서버 보기

데이터 수집 도구가 검색한 서버에 대한 일반 보기 및 세부 보기를 가져올 수 있습니다.

검색된 서버 보기

1. 사용AWS계정, 로그인AWS Management Console그런 다음 에서 Migration Hub 콘솔을 여십시오.https://console.aws.amazon.com/migrationhub/.
2. Migration Hub 콘솔 탐색 창에서발견하기, 선택서버. 검색된 서버가 서버 목록으로 표시됩니다.
3. 서버에 대한 세부 정보는 Server info(서버 정보) 열의 서버 링크를 선택합니다. 그러면 서버에 대해 설명하고 있는 화면이 표시됩니다.

이 서버 세부 정보 화면에는 시스템 정보와 성능 지표가 표시됩니다. 또 네트워크 종속성과 프로세스 정보를 내보내기 하는 단추가 있습니다. 서버 세부 정보를 내보내려면 서버 데이터 내보내기를 참조하십시오.

검색 필터로 서버 정렬

특정 서버를 쉽게 찾으려면 검색 필터를 적용해 수집 도구가 검색한 전체 서버를 정렬합니다. 여러 기준으로 검색 및 필터링을 할 수 있습니다.

검색 필터를 적용해 서버를 정렬

1. 사용AWS계정, 로그인AWS Management Console그런 다음 에서 Migration Hub 콘솔을 여십시오.https://console.aws.amazon.com/migrationhub/.
2. Migration Hub 콘솔 탐색 창에서발견하기, 선택서버.
3. 검색 창 안을 클릭한 다음 목록에서 검색 기준을 선택합니다.
4. 다음 목록에서 연산자를 선택합니다.
5. 선택한 기준에 대해 대/소문자를 구분하는 값을 입력한 다음 Enter를 누릅니다.
6. 2-4단계를 반복해서 여러 필터를 적용할 수 있습니다.

태깅 서버

마이그레이션 계획을 지원하고 체계적으로 관리를 하기 위해 각 서버에 여러 태그를 생성해 지정할 수 있습니다. 태그는 서버에 대한 사용자 지정 데이터나 메타데이터를 저장할 수 있는 사용자 정의 키 값 쌍입니다. 한 번의 작업으로 개별 서버 또는 여러 서버에 태그를 지정할 수 있습니다.AWS Application Discovery Service (Application Discovery Service) 태그는 다음과 유사합니다.AWS태그이지만 두 가지 유형의 태그는 서로 바꿔서 사용할 수 없습니다.

기본 서버 페이지에서 1개 이상의 서버에 여러 개의 태그를 추가하거나 제거할 수 있습니다. 서버 세부 정보 페이지에서 선택한 서버에 하나 이상의 태그를 추가하거나 제거할 수 있습니다. 단 한 번의 작업으로 여러 서버에 대해 태그 지정 작업을 수행하거나 태그를 지정할 수 있습니다. 또 태그를 제거할 수도 있습니다.

하나 이상의 서버에 태그 추가

1. 사용AWS계정, 로그인AWS Management Console그런 다음 에서 Migration Hub 콘솔을 여십시오.https://console.aws.amazon.com/migrationhub/.
2. Migration Hub 콘솔 탐색 창에서발견하기, 선택서버.
3. Server info(서버 정보) 열에서 태그를 추가할 서버에 대한 서버 링크를 선택합니다. 동시에 하나 이상의 서버에 대해 태그를 추가하려면 여러 서버의 확인란을 모두 클릭합니다.
4. 선택해태그 추가를 선택한새 태그 추가.
5. 대화 상자에서 키를 입력합니다.Key필드 및 선택적으로 의 값값필드.

선택하여 더 많은 태그 추가새 태그 추가그리고 더 많은 정보를 추가합니다.

6. 저장(Save)을 선택합니다.

하나 이상의 서버에서 태그 제거

1. 사용AWS계정, 로그인AWS Management Console그런 다음 에서 Migration Hub 콘솔을 여십시오.https://console.aws.amazon.com/migrationhub/.
2. Migration Hub 콘솔 탐색 창에서발견하기, 선택서버.
3. Server info(서버 정보) 열에서 태그를 제거할 서버에 대한 서버 링크를 선택합니다. 여러 서버의 확인란을 선택하여 한 번에 둘 이상의 서버에서 태그를 제거합니다.
4. 선택해태그 제거.
5. 제거할 각 태그를 선택합니다.
6. [Confirm]을 선택합니다.

서버 데이터 내보내기

서버 세부 정보 화면을 사용해 하나의 서버에 대한 네트워크 종속성과 프로세스 정보를 내보내기 할 수 있습니다. 서버 세부 정보 화면의 내보내기 섹션에 위치한 테이블에서 서버에 대한 내보내기 작업을 찾을 수 있습니다. 내보내기 작업이 없는 경우 테이블이 비어 있습니다. 동시에 최대 다섯 개의 데이터 모음을 내보낼 수 있습니다.

> **Note**
>
> 콘솔에서 서버 데이터를 내보내는 것은 해당 서버에서 실행 중인 에이전트가 수집한 데이터에만 사용할 수 있습니다. 에이전트가 설치된 모든 서버의 데이터를 대량으로 내보내려면 을 참조하십시오.Amazon Athena 데이터 탐색.

서버에 대한 세부 데이터 내보내기

1. 사용AWS계정, 로그인AWS Management Console그런 다음 에서 Migration Hub 콘솔을 여십시오.https://console.aws.amazon.com/migrationhub/.
2. Migration Hub 콘솔 탐색 창에서발견하기, 선택서버.
3. Server info(서버 정보) 열에서 데이터를 내보내기 원하는 서버 ID를 선택합니다.
4. 화면 맨 아래 내보내기 섹션에서 Export server details(서버 세부 정보 내보내기)를 선택합니다.

5. Export server details(서버 세부 정보 내보내기)에서 시작일 및 시간을 입력합니다.

> **Note**
>
> 시작 시간은 현재 시간에서 72시간 이내여야 합니다.

6. [Export]를 선택해 작업을 시작합니다. 최초 상태는 In-progress(진행 중)이며, 상태를 업데이트하려면 내보내기 섹션에서 새로 고침 아이콘을 클릭합니다.
7. 내보내기 작업이 완료되면 다운로드를 선택하고 .zip 파일을 저장합니다.
8. 저장된 파일의 압축을 풉니다. .csv 파일 세트에는 다음과 유사한 내보내기 데이터가 포함됩니다.

   - *<AWS## ID>*_destinationProcessConnection.csv
   - *<AWS## ID>*_networkInterface.csv
   - *<AWS## ID>*_osInfo.csv
   - *<AWS## ID>*_process.csv
   - *<AWS## ID>*_sourceProcessConnection.csv
   - *<AWS## ID>*_systemPerformance.csv

   Microsoft Excel에서 .csv 파일을 열고 내보낸 서버 데이터를 검토할 수 있습니다.

   파일 중에 내보내기 작업과 그 결과에 대한 데이터가 포함된 JSON 파일이 있습니다.

Athena의 데이터 탐색

Amazon Athena 데이터 탐색을 사용하면 Discovery Agent가 검색한 모든 온프레미스 서버에서 수집한 데이터를 한 곳에서 분석할 수 있습니다. Amazon Athena에서 데이터 탐색이 활성화되면 Migration Hub 콘솔에서 (또는 StartContinousExport API) 및 에이전트에 대한 데이터 수집이 켜지면 에이전트에서 수집한 데이터가 정기적으로 S3 버킷에 자동으로 저장됩니다. 자세한 정보는 Amazon Athena 데이터 탐색을 참조하세요.

애플리케이션

기능을 유지하기 위해 검색된 서버 가운데 일부를 함께 마이그레이션 해야 할 수도 있습니다. 이 경우, 검색된 서버를 애플리케이션으로 논리적으로 정의해 그룹화 할 수 있습니다.

그룹화 프로세스의 일부로 검색, 필터링, 태그 추가를 할 수 있습니다.

서버를 새 애플리케이션이나 기존 애플리케이션으로 그룹화

1. 사용AWS계정, 로그인AWS Management Console그런 다음 에서 Migration Hub 콘솔을 여십시오.https://console.aws.amazon.com/migrationhub/.
2. Migration Hub 콘솔 탐색 창에서발견하기, 선택서버.
3. 서버 목록에서 새 애플리케이션이나 기존 애플리케이션으로 그룹화 할 각 서버를 선택합니다.

   그룹에 포함시킬 서버를 선택하기 위해 서버 목록에서 지정한 기준으로 검색 및 필터링을 할 수 있습니다. 검색 창 안을 클릭한 다음 목록에서 항목을 선택합니다. 그리고 다음 목록에서 연산자를 선택한 다음 기준을 입력합니다.
4. 선택 선택한 각 서버에서 를 선택합니다.태그 추가, 값을 입력합니다.Key를 누른 다음 필요에 따라 값을 입력합니다.값.
5. Group as application(애플리케이션으로 그룹화)를 선택해 애플리케이션을 생성하거나 기존 애플리케이션 그룹에 추가합니다.
6. Group as application(애플리케이션으로 그룹화) 대화 상자에서 Group as a new application(새 애플리케이션으로 그룹화) 또는 Add to an existing application(기존 애플리케이션에 추가)를 선택합니다.

   a. Group as a new application(새 애플리케이션으로 그룹화)을 선택한 경우 애플리케이션 이름에 이름을 입력합니다. 선택적으로 Application description(애플리케이션 설명)에 설명을 입력할 수 있습니다.

   b. Add to an existing application(기존 애플리케이션에 추가)를 선택한 경우 목록으로 추가할 애플리케이션의 이름을 선택합니다.
7. 저장(Save)을 선택합니다.

Application Discovery Service API를 사용하여 검색된 구성 항목 쿼리

구성 항목은 에이전트나 가져오기를 통해 데이터 센터에서 발견한 IT 자산입니다. AWS Application Discovery Service (Application Discovery Service) 를 사용하는 경우 API를 사용하여 필터를 지정하고 서버, 애플리케이션, 프로세스 및 연결 자산에 대한 특정 구성 항목을 쿼리합니다. API에 대한 자세한 내용은 Application Discovery Service API 참조를 참조하십시오.

다음 섹션의 표에는 두 가지 Application Discovery Service 작업에 사용할 수 있는 입력 필터 및 출력 정렬 옵션이 나열되어 있습니다.

- `DescribeConfigurations`
- `ListConfigurations`

필터링 및 정렬 옵션은 적용되는 자산 유형(서버, 애플리케이션, 프로세스 또는 연결)별로 구성됩니다.

> **Important**
>
> 에서 반환한 `DescribeConfigurations` `ListConfigurations` 결과이며 최근 업데이트가 포함되지 `StartExportTask` 않을 수 있습니다. 자세한 정보는 최종 일관성을 참조하세요.

`DescribeConfigurations`액션 사용

`DescribeConfigurations` 작업은 구성 ID의 목록에 대한 속성을 가져옵니다. 제공된 ID가 모두 동일한 자산 유형(서버, 애플리케이션, 프로세스 또는 연결)이어야 합니다. 출력 필드는 선택된 자산 유형에 고유해야 합니다. 예를 들어, 서버 구성 항목에 대한 출력은 호스트 이름, 운영 체제 및 네트워크 카드 수 등 서버에 대한 속성 목록을 포함합니다. 명령 구문에 대한 자세한 내용은 을 참조하십시오 DescribeConfigurations.

`DescribeConfigurations` 작업은 필터링을 지원하지 않습니다.

`DescribeConfigurations`의 출력 필드

다음 표에는 `DescribeConfigurations` 작업에 지원되는 출력 필드의 목록이 자산 유형별로 나열되어 있습니다. 필수로 표시된 항목은 항상 출력에 포함됩니다.

서버 자산

필드	필수
server.agentId	
server.applications	
server.applications.hasMore Values	
server.configurationId	x
server.cpuType	
server.hostName	
server.hypervisor	
server.networkInterfaceInfo	
server.networkInterfaceInfo .hasMoreValues	
server.osName	
server.osVersion	
server.tags	
server.tags.hasMoreValues	
server.timeOfCreation	x
server.type	
server.performance.avgCpuUs agePct	
server.performance.avgDiskR eadIOPS	

필드	필수
server.performance.avgDiskReadsPerSecondInKB	
server.performance.avgDiskWriteIOPS	
server.performance.avgDiskWritesPerSecondInKB	
server.performance.avgFreeRAMInKB	
server.performance.avgNetworkReadsPerSecondInKB	
server.performance.avgNetworkWritesPerSecondInKB	
server.performance.maxCpuUsagePct	
server.performance.maxDiskReadIOPS	
server.performance.maxDiskReadsPerSecondInKB	
server.performance.maxDiskWriteIOPS	
server.performance.maxDiskWritesPerSecondInKB	
server.performance.maxNetworkReadsPerSecondInKB	
server.performance.maxNetworkWritesPerSecondInKB	

필드	필수
server.performance.minFreeRAMInKB	
server.performance.numCores	
server.performance.numCpus	
server.performance.numDisks	
server.performance.numNetworkCards	
server.performance.totalRAMInKB	

프로세스 자산

필드	필수
process.commandLine	
process.configurationId	x
process.name	
process.path	
process.timeOfCreation	x

애플리케이션 자산

필드	필수
application.configurationId	x
application.description	

필드	필수
application.lastModifiedTime	x
application.name	x
application.serverCount	x
application.timeOfCreation	x

ListConfigurations액션 사용

ListConfigurations 작업은 필터에 지정하는 기준에 따라 구성 항목의 목록을 가져옵니다. 명령 구문에 대한 자세한 내용은 을 참조하십시오 ListConfigurations.

ListConfigurations의 출력 필드

다음 표에는 ListConfigurations 작업에 지원되는 출력 필드의 목록이 자산 유형별로 나열되어 있습니다. 필수로 표시된 항목은 항상 출력에 포함됩니다.

서버 자산

필드	필수
server.configurationId	x
server.agentId	
server.hostName	
server.osName	
server.osVersion	
server.timeOfCreation	x
server.type	

프로세스 자산

필드	필수
process.commandLine	
process.configurationId	x
process.name	
process.path	
process.timeOfCreation	x
server.agentId	
server.configurationId	x

애플리케이션 자산

필드	필수
application.configurationId	x
application.description	
application.name	x
application.serverCount	x
application.timeOfCreation	x
application.lastModifiedTime	x

연결 자산

필드	필수
connection.destinationIp	x

필드	필수
connection.destinationPort	x
connection.ipVersion	x
connection.latestTimestamp	x
connection.occurrence	x
connection.sourceIp	x
connection.transportProtocol	
destinationProcess.configurationId	
destinationProcess.name	
destinationServer.configurationId	
destinationServer.hostName	
sourceProcess.configurationId	
sourceProcess.name	
sourceServer.configurationId	
sourceServer.hostName	

ListConfigurations에 지원되는 필터

다음 표에는 ListConfigurations 작업에 지원되는 필터가 자산 유형별로 나열되어 있습니다. 필터 및 값은 지원되는 논리적 조건 중 하나에 의해 정의된 키/값 관계에 있습니다. 표시된 필터의 출력을 정렬할 수 있습니다.

서버 자산

필터	지원되는 조건	지원되는 값	지원되는 정렬
server.configurationId	• EQUALS • NOT_EQUALS • EQ • NE	• 유효한 서버 구성 ID	None
server.hostName	• EQUALS • NOT_EQUALS • EQ • NE • CONTAINS • NOT_CONTAINS	• String	• ASC • DESC
server.osName	• EQUALS • NOT_EQUALS • EQ • NE • CONTAINS • NOT_CONTAINS	• String	• ASC • DESC
server.osVersion	• EQUALS • NOT_EQUALS • EQ • NE • CONTAINS • NOT_CONTAINS	• String	• ASC • DESC
server.agentId	• EQUALS • NOT_EQUALS • EQ • NE	• String	None

필터	지원되는 조건	지원되는 값	지원되는 정렬
server.connectorId	• EQUALS • NOT_EQUALS • EQ • NE	• String	None
server.type	• EQUALS • NOT_EQUALS • EQ • NE	다음 값 중 하나를 가진 문자열: • EC2 • 기타 • VMWARE_VM • VMWARE_HOST • VMWARE_VM_TEMPLATE	None
server.vmWareInfo.morefId	• EQUALS • NOT_EQUALS • EQ • NE • CONTAINS • NOT_CONTAINS	• String	None
server.vmWareInfo.vcenterId	• EQUALS • NOT_EQUALS • EQ • NE • CONTAINS • NOT_CONTAINS	• String	None

필터	지원되는 조건	지원되는 값	지원되는 정렬
server.vmWareInfo.hostId	• EQUALS • NOT_EQUALS • EQ • NE • CONTAINS • NOT_CONTAINS	• String	None
server.networkInterfaceInfo.portGroupId	• EQUALS • NOT_EQUALS • EQ • NE • CONTAINS • NOT_CONTAINS	• String	None
server.networkInterfaceInfo.portGroupName	• EQUALS • NOT_EQUALS • EQ • NE • CONTAINS • NOT_CONTAINS	• String	None
server.networkInterfaceInfo.virtualSwitchName	• EQUALS • NOT_EQUALS • EQ • NE • CONTAINS • NOT_CONTAINS	• String	None

필터	지원되는 조건	지원되는 값	지원되는 정렬
server.networkInterfaceInfo.ipAddress	• EQUALS • NOT_EQUALS • EQ • NE • CONTAINS • NOT_CONTAINS	• String	None
server.networkInterfaceInfo.macAddress	• EQUALS • NOT_EQUALS • EQ • NE • CONTAINS • NOT_CONTAINS	• String	None
server.performance.avgCpuUsagePct	• GE • LE • GT • LT	• 백분율	None
server.performance.totalDiskFreeSizeInKB	• GE • LE • GT • LT	• Double	None
server.performance.avgFreeRAMInKB	• GE • LE • GT • LT	• Double	None

필터	지원되는 조건	지원되는 값	지원되는 정렬
server.tag.value	• EQUALS • NOT_EQUALS • EQ • NE • CONTAINS • NOT_CONTAINS	• String	None
server.tag.key	• EQUALS • NOT_EQUALS • EQ • NE • CONTAINS • NOT_CONTAINS	• String	None
server.application.name	• EQUALS • NOT_EQUALS • EQ • NE • CONTAINS • NOT_CONTAINS	• String	None
server.application.description	• EQUALS • NOT_EQUALS • EQ • NE • CONTAINS • NOT_CONTAINS	• String	None

필터	지원되는 조건	지원되는 값	지원되는 정렬
server.application.configurationId	• EQUALS • NOT_EQUALS • EQ • NE	• 유효한 애플리케이션 구성 ID	None
server.process.configurationId	• EQUALS • NOT_EQUALS • EQ • NE	• ProcessId	None
server.process.name	• EQUALS • NOT_EQUALS • EQ • NE • CONTAINS • NOT_CONTAINS	• String	None
server.process.commandLine	• EQUALS • NOT_EQUALS • EQ • NE • CONTAINS • NOT_CONTAINS	• String	None

애플리케이션 자산

필터	지원되는 조건	지원되는 값	지원되는 정렬
application.configurationId	• EQUALS • NOT_EQUALS • EQ	• ApplicationId	None

필터	지원되는 조건	지원되는 값	지원되는 정렬
	• NE		
application.name	• EQUALS • NOT_EQUALS • EQ • NE • CONTAINS • NOT_CONTAINS	• String	• ASC • DESC
application.description	• EQUALS • NOT_EQUALS • EQ • NE • CONTAINS • NOT_CONTAINS	• String	• ASC • DESC
application.serverCount	필터링이 지원되지 않습니다.	필터링이 지원되지 않습니다.	• ASC • DESC
application.timeOfCreation	필터링이 지원되지 않습니다.	필터링이 지원되지 않습니다.	• ASC • DESC
application.lastModifiedTime	필터링이 지원되지 않습니다.	필터링이 지원되지 않습니다.	• ASC • DESC

필터	지원되는 조건	지원되는 값	지원되는 정렬
server.configurationId	• EQUALS • NOT_EQUALS • EQ • NE	• ServerId	None

프로세스 자산

필터	지원되는 조건	지원되는 값	지원되는 정렬
process.configurationId	• EQUALS • NOT_EQUALS • EQ • NE	• ProcessId	
process.name	• EQUALS • NOT_EQUALS • EQ • NE • CONTAINS • NOT_CONTAINS	• String	• ASC • DESC
process.commandLine	• EQUALS • NOT_EQUALS • EQ • NE • CONTAINS • NOT_CONTAINS	• String	• ASC • DESC
server.configurationId	• EQUALS • NOT_EQUALS • EQ	• ServerId	

필터	지원되는 조건	지원되는 값	지원되는 정렬
	• NE		
server.hostName	• EQUALS • NOT_EQUALS • EQ • NE • CONTAINS • NOT_CONTAINS	• String	• ASC • DESC
server.osName	• EQUALS • NOT_EQUALS • EQ • NE • CONTAINS • NOT_CONTAINS	• String	• ASC • DESC
server.os Version	• EQUALS • NOT_EQUALS • EQ • NE • CONTAINS • NOT_CONTAINS	• String	• ASC • DESC
server.agentId	• EQUALS • NOT_EQUALS • EQ • NE • CONTAINS • NOT_CONTAINS	• String	

연결 자산

필터	지원되는 조건	지원되는 값	지원되는 정렬
connection.sourceIp	• EQUALS • NOT_EQUALS • EQ • NE • CONTAINS • NOT_CONTAINS	• IP	• ASC • DESC
connection.destinationIp	• EQUALS • NOT_EQUALS • EQ • NE • CONTAINS • NOT_CONTAINS	• IP	• ASC • DESC
connection.destinationPort	• EQUALS • NOT_EQUALS • EQ • NE	• Integer	• ASC • DESC
sourceServer.configurationId	• EQUALS • NOT_EQUALS • EQ • NE	• ServerId	
sourceServer.hostName	• EQUALS • NOT_EQUALS • EQ • NE • CONTAINS • NOT_CONTAINS	• String	• ASC • DESC

필터	지원되는 조건	지원되는 값	지원되는 정렬
destinationServer.osName	• EQUALS • NOT_EQUALS • EQ • NE • CONTAINS • NOT_CONTAINS	• String	• ASC • DESC
destinationServer.osVersion	• EQUALS • NOT_EQUALS • EQ • NE • CONTAINS • NOT_CONTAINS	• String	• ASC • DESC
destinationServer.agentId	• EQUALS • NOT_EQUALS • EQ • NE • CONTAINS • NOT_CONTAINS	• String	
sourceProcess.configurationId	• EQUALS • NOT_EQUALS • EQ • NE	• ProcessId	

필터	지원되는 조건	지원되는 값	지원되는 정렬
sourceProcess.name	• EQUALS • NOT_EQUALS • EQ • NE • CONTAINS • NOT_CONTAINS	• String	• ASC • DESC
sourceProcess.commandLine	• EQUALS • NOT_EQUALS • EQ • NE • CONTAINS • NOT_CONTAINS	• String	• ASC • DESC
destinationProcess.configurationId	• EQUALS • NOT_EQUALS • EQ • NE	• ProcessId	
destinationProcess.name	• EQUALS • NOT_EQUALS • EQ • NE • CONTAINS • NOT_CONTAINS	• String	• ASC • DESC

필터	지원되는 조건	지원되는 값	지원되는 정렬
`destinationprocess.commandLine`	• EQUALS • NOT_EQUALS • EQ • NE • CONTAINS • NOT_CONTAINS	• String	• ASC • DESC

API의 AWS Application Discovery Service 최종 일관성

다음 업데이트 작업은 최종적으로 일관됩니다. StartExportTask DescribeConfigurations, 및 읽기 작업에 업데이트가 즉시 표시되지 않을 수 ListConfigurations있습니다.

- AssociateConfigurationItemsTo애플리케이션
- CreateTags
- DeleteApplications
- DeleteTags
- DescribeBatchDeleteConfiguration태스크
- DescribeImport태스크
- DisassociateConfigurationItemsFrom애플리케이션
- UpdateApplication

최종 일관성 관리를 위한 제안:

- 읽기 작업 StartExportTask DescribeConfigurations, 또는 ListConfigurations(또는 해당 AWS CLI 명령) 을 호출할 때는 지수 백오프 알고리즘을 사용하여 이전 업데이트 작업이 시스템에 전파되는 데 충분한 시간을 허용하십시오. 이렇게 하려면 2초의 대기 시간부터 시작하여 점차 최대 5분까지 늘려 읽기 작업을 반복해서 실행하십시오.
- 업데이트 작업에서 200 - OK 응답이 반환되더라도 후속 작업 사이에 대기 시간을 추가하십시오. 몇 초의 대기 시간으로 시작하는 지수 백오프 알고리즘을 적용하고 대기 시간을 약 5분까지 점차 늘리십시오.

AWS Application Discovery Service의 보안

AWS에서 클라우드 보안을 가장 중요하게 생각합니다. AWS 고객은 보안에 가장 보안에 민감한 조직의 요구 사항에 부합하도록 구축된 데이터 센터 및 네트워크 아키텍처의 혜택을 누릴 수 있습니다.

보안은 AWS와 귀하의 공동 책임입니다. 공동 책임 모델은 이 사항을 클라우드 내 보안 및 클라우드의 보안으로 설명합니다.

- 클라우드의 보안 - AWS는 AWS 클라우드에서 AWS 서비스를 실행하는 인프라를 보호합니다. AWS는 또한 안전하게 사용할 수 있는 서비스를 제공합니다. 서드 파티 감사자는 정기적으로 AWS 규정 준수 프로그램의 일환으로 보안 효과를 테스트하고 검증합니다.
- 클라우드 내 보안 – 귀하의 책임은 귀하가 사용하는 AWS 서비스에 의해 결정됩니다. 또한 데이터의 민감도, 조직의 요구 사항 및 관련 법률 및 규정을 비롯한 기타 요소에 대해서도 책임이 있습니다.

AWS애플리케이션 검색 에이전트 또는 Application Discovery Service Agentless Collector를 사용하려면 계정에 대한 액세스 키를 제공해야 합니다. AWS 그러면 이 정보가 로컬 인프라에 저장됩니다. 공동 책임 모델의 일환으로 인프라에 대한 액세스를 보호할 책임은 귀하에게 있습니다.

이 설명서는 Application Discovery Service를 사용할 때 공동 책임 모델을 적용하는 방법을 이해하는 데 도움이 됩니다. 다음 항목에서는 보안 및 규정 준수 목표를 충족하도록 Application Discovery Service를 구성하는 방법을 보여줍니다. 또한 Application Discovery Service 리소스를 모니터링하고 보호하는 데 도움이 되는 다른 AWS 서비스를 사용하는 방법도 알아봅니다.

주제

Identity 및 Access Management에 대한 AWS Application Discovery Service

AWS Identity and Access Management (IAM) 은 관리자가 리소스에 대한 액세스를 안전하게 제어할 수 AWS 서비스 있도록 AWS 도와줍니다. IAM 관리자는 Application Discovery Service 리소스를 사용할 수 있는 인증 (로그인) 및 권한 부여 (권한 보유) 를 받을 수 있는 사용자를 제어합니다. IAM은 추가 AWS 서비스 비용 없이 사용할 수 있습니다.

주제

고객

사용 방법 AWS Identity and Access Management (IAM) 은 Application Discovery Service에서 수행하는 작업에 따라 다릅니다.

서비스 사용자 - Application Discovery Service 서비스를 사용하여 작업을 수행하는 경우 관리자가 필요한 자격 증명과 권한을 제공합니다. 더 많은 Application Discovery Service 기능을 사용하여 작업을 수행함에 따라 추가 권한이 필요할 수 있습니다. 액세스 권한 관리 방식을 이해하면 적절한 권한을 관리자에게 요청할 수 있습니다. Application Discovery Service의 기능에 액세스할 수 없는 경우 을 참조하십시오AWS Application Discovery Service ID 및 액세스 문제 해결.

서비스 관리자 — 회사에서 Application Discovery Service 리소스를 담당하는 경우 Application Discovery Service에 대한 전체 액세스 권한을 가지고 있을 것입니다. 서비스 사용자가 액세스해야 하는 Application Discovery Service 기능 및 리소스를 결정하는 것은 여러분의 몫입니다. 그런 다음, IAM 관리자에게 요청을 제출하여 서비스 사용자의 권한을 변경해야 합니다. 이 페이지의 정보를 검토하여 IAM의 기본 개념을 이해합니다. 회사에서 Application Discovery Service와 함께 IAM을 사용하는 방법에 대한 자세한 내용은 을 참조하십시오IAM의 AWS Application Discovery Service 작동 방식.

IAM 관리자 - IAM 관리자인 경우 Application Discovery Service에 대한 액세스를 관리하기 위한 정책을 작성하는 방법에 대해 자세히 알아보는 것이 좋습니다. IAM에서 사용할 수 있는 Application Discovery Service ID 기반 정책의 예를 보려면 을 참조하십시오. AWS Application Discovery Service ID 기반 정책 예제

자격 증명을 통한 인증

인증은 ID 자격 증명을 AWS 사용하여 로그인하는 방법입니다. IAM 사용자로 인증 (로그인 AWS) 하거나 IAM 역할을 맡아 인증 (로그인) 해야 합니다. AWS 계정 루트 사용자

ID 소스를 통해 제공된 자격 증명을 사용하여 페더레이션 ID로 로그인할 수 있습니다. AWS AWS IAM Identity Center (IAM ID 센터) 사용자, 회사의 싱글 사인온 인증, Google 또는 Facebook 자격 증명이 페더레이션 ID의 예입니다. 페더레이션형 ID로 로그인할 때 관리자가 이전에 IAM 역할을 사용하여 ID 페더레이션을 설정했습니다. 페더레이션을 사용하여 액세스하는 경우 AWS 간접적으로 역할을 맡게 됩니다.

사용자 유형에 따라 AWS Management Console 또는 AWS 액세스 포털에 로그인할 수 있습니다. 로그인에 대한 자세한 내용은 AWS 로그인 사용 설명서의 내 로그인 방법을 참조하십시오. AWS AWS 계정

AWS 프로그래밍 방식으로 액세스하는 경우 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 직접 요청에 서명하는 방법에 대한 자세한 내용은 IAM 사용 설명서의 AWS API 요청 서명을 참조하십시오.

사용하는 인증 방법에 상관없이 추가 보안 정보를 제공해야 할 수도 있습니다. 예를 들어, AWS 계정의 보안을 강화하기 위해 다단계 인증 (MFA) 을 사용할 것을 권장합니다. 자세한 내용은AWS IAM Identity Center 사용 설명서의 다중 인증 및 IAM 사용 설명서의 AWS에서 다중 인증(MFA) 사용을 참조하세요.

AWS 계정 루트 사용자

계정을 AWS 계정만들 때는 먼저 계정의 모든 AWS 서비스 리소스에 대한 완전한 액세스 권한을 가진 하나의 로그인 ID로 시작합니다. 이 ID를 AWS 계정 루트 사용자라고 하며, 계정을 만들 때 사용한 이메일 주소와 비밀번호로 로그인하여 액세스할 수 있습니다. 일상적인 작업에 루트 사용자를 사용하지 않을 것을 강력히 권장합니다. 루트 사용자 보안 인증 정보를 보호하고 루트 사용자만 수행할 수 있는 태스크를 수행하는 데 사용하세요. 루트 사용자로 로그인해야 하는 전체 작업 목록은 IAM 사용 설명서의 루트 사용자 보안 인증이 필요한 태스크를 참조하세요.

IAM 사용자 및 그룹

IAM 사용자는 단일 사용자 또는 애플리케이션에 대한 특정 권한을 가진 사용자 내의 자격 증명입니다. AWS 계정 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 정보는 IAM 사용 설명서의 IAM 사용자를 만들어야 하는 경우(역할이 아님)를 참조하세요.

IAM 역할

IAM 역할은 특정 권한을 가진 사용자 AWS 계정 내의 자격 증명입니다. IAM 사용자와 유사하지만, 특정 개인과 연결되지 않습니다. 역할을 AWS Management Console 전환하여 에서 일시적으로 IAM 역할을 맡을 수 있습니다. AWS CLI 또는 AWS API 작업을 호출하거나 사용자 지정 URL을 사용하여 역할을 수임할 수 있습니다. 역할 사용 방법에 대한 자세한 정보는 IAM 사용 설명서의 IAM 역할 사용을 참조하세요.

임시 보안 인증 정보가 있는 IAM 역할은 다음과 같은 상황에서 유용합니다.

- 페더레이션 사용자 액세스 - 페더레이션 아이덴티티에 권한을 부여하려면 역할을 생성하고 해당 역할의 권한을 정의합니다. 연동 자격 증명이 인증되면 역할이 연결되고 역할에 정의된 권한이 부여됩니다. 페더레이션 역할에 대한 자세한 내용은 IAM 사용 설명서의 타사 자격 증명 공급자의 역할 만들기를 참조하세요. IAM Identity Center를 사용하는 경우 권한 세트를 구성합니다. 인증 후 자격 증명이 액세스할 수 있는 항목을 제어하기 위해 IAM Identity Center는 권한 세트를 IAM의 역할과 연관짓습니다. 권한 세트에 대한 자세한 내용은AWS IAM Identity Center 사용 설명서의 권한 세트를 참조하세요.
- 임시 IAM 사용자 권한 - IAM 사용자 또는 역할은 IAM 역할을 수임하여 특정 태스크에 대한 다양한 권한을 임시로 받을 수 있습니다.
- 크로스 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 AWS 서비스경우에는 역할을 프록시로 사용하는 대신 정책을 리소스에 직접 연결할 수 있습니다. 크로스 계정 액세스를 위한 역할과 리소스 기반 정책의 차이점을 알아보려면 IAM 사용 설명서의 IAM 역할과 리소스 기반 정책의 차이를 참조하세요.
- 서비스 간 액세스 — 일부는 다른 AWS 서비스서비스의 기능을 AWS 서비스 사용합니다. 예를 들어 서비스에서 직접 호출을 수행하면 일반적으로 해당 서비스는 EC2에서 애플리케이션을 실행하거나 Amazon S3에 개체를 저장합니다. 서비스는 호출하는 보안 주체의 권한을 사용하거나, 서비스 역할을 사용하거나, 또는 서비스 연결 역할을 사용하여 이 작업을 수행할 수 있습니다.
  - 순방향 액세스 세션 (FAS) — IAM 사용자 또는 역할을 사용하여 작업을 수행하는 경우 보안 AWS 주체로 간주됩니다. 일부 서비스를 사용하는 경우 다른 서비스에서 다른 작업을 시작하는 작업을 수행할 수 있습니다. FAS는 전화를 거는 주체의 권한을 다운스트림 AWS 서비스서비스에 AWS 서비스 요청하기 위한 요청과 결합하여 사용합니다. FAS 요청은 다른 서비스 AWS 서비스 또는

리소스와의 상호 작용이 필요한 요청을 서비스가 수신한 경우에만 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 태스크를 수행하기 위해 맡는 IAM 역할입니다. IAM 관리자는 IAM 내에서 서비스 역할을 생성, 수정 및 삭제할 수 있습니다. 자세한 정보는 IAM 사용 설명서의 AWS 서비스에 대한 권한을 위임할 역할 생성을 참조하세요.
- 서비스 연결 역할 — 서비스 연결 역할은 에 연결된 서비스 역할의 한 유형입니다. AWS 서비스서비스는 사용자를 대신하여 작업을 수행하기 위해 역할을 수임할 수 있습니다. 서비스 연결 역할은 사용자에게 AWS 계정 표시되며 해당 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 API 요청을 AWS CLI 하는 애플리케이션의 임시 자격 증명을 관리할 수 있습니다. AWS 이는 EC2 인스턴스 내에 액세스 키를 저장할 때 권장되는 방법입니다. EC2 인스턴스에 AWS 역할을 할당하고 모든 애플리케이션에서 사용할 수 있게 하려면 인스턴스에 연결된 인스턴스 프로필을 생성합니다. 인스턴스 프로파일에는 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.

IAM 역할을 사용할지 또는 IAM 사용자를 사용할지를 알아보려면 IAM 사용 설명서의 IAM 역할(사용자 대신)을 생성하는 경우를 참조하세요.

정책을 사용하여 액세스 관리

정책을 생성하고 이를 AWS ID 또는 리소스에 AWS 연결하여 액세스를 제어할 수 있습니다. 정책은 ID 또는 리소스와 연결될 때 AWS 해당 권한을 정의하는 객체입니다. AWS 주도자 (사용자, 루트 사용자 또는 역할 세션) 가 요청할 때 이러한 정책을 평가합니다. 정책에서 권한은 요청이 허용되거나 거부되는 지를 결정합니다. 대부분의 정책은 JSON 문서로 AWS 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, 사용자와 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`태스크를 허용하는 정책이 있다고 가정합니다. 해당 정책을 사용하는 사용자는 AWS Management Console, AWS CLI, 또는 AWS API에서 역할 정보를 가져올 수 있습니다.

자격 증명 기반 정책

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

자격 증명 기반 정책은 인라인 정책 또는 관리형 정책으로 한층 더 분류할 수 있습니다. 인라인 정책은 단일 사용자, 그룹 또는 역할에 직접 포함됩니다. 관리형 정책은 내 여러 사용자, 그룹 및 역할에 연결할 수 있는 독립형 정책입니다. AWS 계정관리형 정책에는 AWS 관리형 정책과 고객 관리형 정책이 포함됩니다. 관리형 정책 또는 인라인 정책을 선택하는 방법을 알아보려면 IAM 사용 설명서의 관리형 정책과 인라인 정책의 선택을 참조하세요.

리소스 기반 정책

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

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

액세스 제어 목록(ACL)

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

ACL을 지원하는 서비스의 예로는 아마존 S3와 아마존 VPC가 있습니다. AWS WAF ACL에 대해 자세히 알아보려면 Amazon Simple Storage Service 개발자 안내서의 ACL(액세스 제어 목록) 개요를 참조하세요.

기타 정책 유형

AWS 일반적이지 않은 추가 정책 유형을 지원합니다. 이러한 정책 타입은 더 일반적인 정책 타입에 따라 사용자에게 부여되는 최대 권한을 설정할 수 있습니다.

- 권한 경계 – 권한 경계는 보안 인증 기반 정책에 따라 IAM 엔터티(IAM 사용자 또는 역할)에 부여할 수 있는 최대 권한을 설정하는 고급 기능입니다. 개체에 대한 권한 경계를 설정할 수 있습니다. 그 결과로 얻는 권한은 엔터티의 자격 증명 기반 정책과 그 권한 경계의 교집합입니다. `Principal` 필드에서 사용자나 역할을 보안 주체로 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 엔터티에 대한 권한 경계를 참조하세요.
- 서비스 제어 정책 (SCP) - SCP는 조직 또는 조직 단위 (OU) 에 대한 최대 권한을 지정하는 JSON 정책입니다. AWS Organizations AWS Organizations 사업체가 소유한 여러 AWS 계정 개를 그룹화하고 중앙에서 관리하는 서비스입니다. 조직에서 모든 기능을 활성화할 경우 서비스 제어 정책 (SCP)을 임의의 또는 모든 계정에 적용할 수 있습니다. SCP는 구성원 계정의 엔티티 (각 엔티티 포함) 에 대한 권한을 제한합니다. AWS 계정 루트 사용자조직 및 SCP에 대한 자세한 정보는AWS Organizations 사용 설명서의 SCP 작동 방식을 참조하세요.
- 세션 정책 – 세션 정책은 역할 또는 연합된 사용자에 대해 임시 세션을 프로그래밍 방식으로 생성할 때 파라미터로 전달하는 고급 정책입니다. 결과적으로 얻는 세션의 권한은 사용자 또는 역할 자격 증명 기반 정책의 교차 및 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 타입이 요청에 적용되는 경우 결과 권한은 이해하기가 더 복잡합니다. 여러 정책 유형이 관련되어 있을 때 요청을 허용할지 여부를 AWS 결정하는 방법을 알아보려면 IAM 사용 설명서의 정책 평가 로직을 참조하십시오.

IAM의 AWS Application Discovery Service 작동 방식

IAM을 사용하여 Application Discovery Service에 대한 액세스를 관리하려면 먼저 Application Discovery Service에서 사용할 수 있는 IAM 기능이 무엇인지 이해해야 합니다. Application Discovery Service 및 기타 AWS 서비스가 IAM과 어떻게 연동되는지 자세히 알아보려면 IAM 사용 설명서의 IAM과 연동되는AWS 서비스를 참조하십시오.

주제

- Application Discovery 서비스 ID 기반 정책
- Application Discovery 서비스 리소스 기반 정책
- Application Discovery 서비스 태그를 기반으로 한 권한 부여
- Application Discovery 서비스 IAM 역할

Application Discovery 서비스 ID 기반 정책

IAM 자격 증명 기반 정책을 사용하면 허용되거나 거부되는 작업와 리소스뿐 아니라 작업이 허용되거나 거부되는 조건을 지정할 수 있습니다. Application Discovery Service는 특정 작업, 리소스 및 조건 키를 지원합니다. JSON 정책에서 사용하는 모든 요소에 대해 알고 싶다면 IAM 사용 설명서의 IAM JSON 정책 요소 참조를 참조하세요.

작업

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

JSON 정책의 `Action`요소는 정책에서 액세스를 허용하거나 거부하는 데 사용할 수 있는 태스크를 설명합니다. 정책 작업은 일반적으로 관련 AWS API 작업과 이름이 같습니다. 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 포함하십시오.

Application Discovery Service의 정책 작업은 작업 앞에 다음 접두사를 사용합니다. `discovery:` 정책 문에는 `Action` 또는 `NotAction` 요소가 포함되어야 합니다. Application Discovery Service는 이 서비스로 수행할 수 있는 작업을 설명하는 자체 작업 세트를 정의합니다.

명령문 하나에 여러 태스크를 지정하려면 다음과 같이 쉼표로 구분합니다.

```
"Action": [
      "discovery:action1",
      "discovery:action2"
```

와일드카드(*)를 사용하여 여러 작업을 지정할 수 있습니다. 예를 들어, `Describe`라는 단어로 시작하는 모든 태스크를 지정하려면 다음 태스크를 포함합니다.

```
"Action": "discovery:Describe*"
```

Application Discovery Service 작업 목록을 보려면 IAM 사용 설명서에 정의된 작업을 참조하십시오. AWS Application Discovery Service

리소스

Application Discovery Service는 정책에 리소스 ARN을 지정하는 것을 지원하지 않습니다. 액세스를 분리하려면 별도로 생성하여 사용하십시오. AWS 계정

조건 키

Application Discovery Service는 서비스별 조건 키를 제공하지 않지만 일부 글로벌 조건 키 사용은 지원합니다. 모든 AWS 글로벌 조건 키를 보려면 IAM 사용 AWS 설명서의 글로벌 조건 컨텍스트 키를 참조하십시오.

예제

Application Discovery Service ID 기반 정책의 예를 보려면 을 참조하십시오. AWS Application Discovery Service ID 기반 정책 예제

Application Discovery 서비스 리소스 기반 정책

Application Discovery Service는 리소스 기반 정책을 지원하지 않습니다.

Application Discovery 서비스 태그를 기반으로 한 권한 부여

Application Discovery Service는 리소스에 태그를 지정하거나 태그를 기반으로 액세스를 제어하는 기능을 지원하지 않습니다.

Application Discovery 서비스 IAM 역할

IAM 역할은 AWS 계정 내에서 특정 권한을 가진 엔티티입니다.

Application Discovery Service에서 임시 자격 증명 사용

Application Discovery Service는 임시 자격 증명 사용을 지원하지 않습니다.

서비스 연결 역할

서비스 연결 역할을 사용하면 AWS 서비스가 다른 서비스의 리소스에 액세스하여 사용자를 대신하여 작업을 완료할 수 있습니다. 서비스 연결 역할은 IAM 계정에 나타나고 서비스가 소유합니다. IAM 관리자는 서비스 연결 역할의 권한을 볼 수 있지만 편집할 수 없습니다.

Application Discovery Service는 서비스 연결 역할을 지원합니다. Application Discovery Service 서비스 연결 역할을 만들거나 관리하는 방법에 대한 자세한 내용은 을 참조하십시오. Application Discovery 서비스에 대한 서비스 연결 역할 사용

서비스 역할

이 기능을 사용하면 서비스가 사용자를 대신하여 서비스 역할을 수임할 수 있습니다. 이 역할을 사용하면 서비스가 다른 서비스의 리소스에 액세스해 사용자를 대신해 작업을 완료할 수 있습니다. 서비스 역할은 IAM 계정에 나타나고, 해당 계정이 소유합니다. 즉, IAM 관리자가 이 역할에 대한 권한을 변경할 수 있습니다. 그러나 권한을 변경하면 서비스의 기능이 손상될 수 있습니다.

Application Discovery Service는 서비스 역할을 지원합니다.

AWS 에 대한 관리형 정책 AWS Application Discovery Service

사용자, 그룹 및 역할에 권한을 추가하려면 정책을 직접 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 참조하십시오.

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

또한 여러 서비스에 걸친 작업 기능에 대한 관리형 정책을 AWS 지원합니다. 예를 들어, ReadOnlyAccess AWS 관리형 정책은 모든 AWS 서비스와 리소스에 대한 읽기 전용 액세스를 제공합니다. 서비스가 새 기능을 출시하면 새 작업 및 리소스에 대한 읽기 전용 권한이 AWS 추가됩니다. 직무 정책의 목록과 설명은 IAM 사용 설명서의 직무에 관한 AWS 관리형 정책을 참조하세요.

AWS 관리형 정책: AWSApplicationDiscoveryServiceFullAccess

이 AWSApplicationDiscoveryServiceFullAccess 정책은 IAM 사용자 계정에 Application Discovery Service 및 Migration Hub API에 대한 액세스 권한을 부여합니다.

이 정책이 연결된 IAM 사용자 계정은 Application Discovery Service를 구성하고, 에이전트를 시작 및 중지하고, 에이전트 없는 검색을 시작 및 중지하고, 검색 서비스 데이터베이스에서 데이터를 쿼리할 수 있습니다. AWS 이 정책의 예는 Application Discovery Service에 대한 전체 액세스 권한 부여 단원을 참조하십시오.

AWS 관리형 정책: AWSApplicationDiscoveryAgentlessCollectorAccess

AWSApplicationDiscoveryAgentlessCollectorAccess관리형 정책은 Application Discovery Service 에이전트 없는 수집기 (Agentless Collector) 에게 Application Discovery Service에 등록 및 통신하고 다른 서비스와 통신할 수 있는 액세스 권한을 부여합니다. AWS

에이전트리스 컬렉터를 구성하는 데 사용되는 자격 증명을 가진 IAM 사용자에게 이 정책을 연결해야 합니다.

권한 세부 정보

이 정책에는 다음 권한이 포함되어 있습니다.

- arsenal— 수집기가 Application Discovery Service 애플리케이션에 등록할 수 있습니다. 이렇게 해야 수집된 데이터를 다시 보낼 수 AWS 있습니다.
- ecr-public— 컬렉터가 Amazon Elastic 컨테이너 레지스트리 퍼블릭 (Amazon ECR Public) 을 호출하여 컬렉터에 대한 최신 업데이트를 찾을 수 있도록 합니다.
- mgh— 컬렉터가 콜렉터 구성에 사용된 계정의 홈 리전을 AWS Migration Hub 호출하여 검색할 수 있도록 허용합니다. 이는 수집된 데이터를 어느 지역으로 전송해야 하는지를 파악하는 데 필요합니다.
- sts— 수집자가 Amazon ECR Public을 호출하여 최신 업데이트를 받을 수 있도록 서비스 베어러 토큰을 검색할 수 있습니다.

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

```
                "arsenal:RegisterOnPremisesAgent"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "ecr-public:DescribeImages"
            ],
            "Resource": "arn:aws:ecr-
public::446372222237:repository/6e5498e4-8c31-4f57-9991-13b4b992ff7b"
        },
        {
            "Effect": "Allow",
            "Action": [
                "ecr-public:GetAuthorizationToken"

            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "mgh:GetHomeRegion"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "sts:GetServiceBearerToken"
            ],
            "Resource": "*"
        }
    ]
}
```

AWS 관리형 정책: AWSApplicationDiscoveryAgentAccess

이 `AWSApplicationDiscoveryAgentAccess` 정책은 애플리케이션 검색 에이전트에게 Application Discovery Service에 등록하고 통신할 수 있는 액세스 권한을 부여합니다.

응용 프로그램 검색 에이전트에서 사용하는 자격 증명을 가진 모든 사용자에게 이 정책을 연결합니다.

또한 이 정책은 사용자에게 Arsenal에 대한 액세스 권한을 부여합니다. Arsenal은 에서 관리하고 AWS 호스팅하는 에이전트 서비스입니다. Arsenal은 클라우드의 Application Discovery Service로 데이터를 전달합니다. 이 정책의 예는 디스커버리 에이전트에 액세스 권한 부여 단원을 참조하십시오.

AWS 관리형 정책: AWSAgentlessDiscoveryService

이 `AWSAgentlessDiscoveryService` 정책은 VMware vCenter Server에서 실행 중인 AWS 에이전트 없는 검색 커넥터에 Application Discovery Service에 커넥터 상태 메트릭을 등록, 통신 및 공유할 수 있는 액세스 권한을 부여합니다.

이 정책을 커넥터가 자격 증명을 사용하는 사용자에게 연결합니다.

AWS 관리형 정책: 정책 ApplicationDiscoveryServiceContinuousExportServiceRole

IAM 계정에 `AWSApplicationDiscoveryServiceFullAccess` 정책이 연결되어 있는 경우 Amazon Athena에서 데이터 탐색을 활성화하면 계정에 자동으로 연결됩니다. `ApplicationDiscoveryServiceContinuousExportServiceRolePolicy`

이 정책을 사용하면 Amazon Data Firehose 스트림을 AWS Application Discovery Service 생성하여 AWS Application Discovery Service 에이전트가 수집한 데이터를 변환하여 계정의 Amazon S3 버킷으로 전송할 수 AWS 있습니다.

또한 이 정책은 application_discovery_service_database라는 새 데이터베이스와 에이전트가 수집한 데이터를 매핑하기 위한 테이블 스키마를 포함하는 데이터베이스를 생성합니다. AWS Glue Data Catalog 이 정책의 예는 상담원 데이터 수집 권한 부여 단원을 참조하십시오.

AWS 관리형 정책: AWSDiscoveryContinuousExportFirehosePolicy

Amazon Athena에서 데이터 탐색을 사용하려면 `AWSDiscoveryContinuousExportFirehosePolicy` 정책이 필요합니다. 이를 통해 Amazon Data Firehose는 Application Discovery Service에서 수집한 데이터를 Amazon S3에 쓸 수 있습니다. 이 정책 사용에 대한 자세한 내용은 역할 생성 AWSApplicationDiscoveryServiceFirehose 단원을 참조하십시오. 이 정책의 예는 데이터 탐색 권한 부여 단원을 참조하십시오.

역할 생성 AWSApplicationDiscoveryServiceFirehose

관리자가 IAM 사용자 계정에 관리형 정책을 연결합니다. `AWSDiscoveryContinuousExportFirehosePolicy`정책을 사용할 때 관리자는 먼저 다음 절차에 나와 AWSApplicationDiscoveryServiceFirehose있는 것처럼 Firehose를 신뢰할 수 있는 개체로 사용하

여 이름을 지정한 다음 `AWSDiscoveryContinuousExportFirehosePolicy` 정책을 역할에 연결해야 합니다.

AWSApplicationDiscoveryServiceFirehose IAM 역할을 생성하려면

1. IAM 콘솔의 탐색 창에서 [Roles] 를 선택합니다.
2. Create Role(역할 생성)을 선택합니다.
3. Kinesis를 선택합니다.
4. 사용 사례로 Kinesis Firehose를 선택합니다.
5. 다음: 권한을 선택합니다.
6. 필터 정책에서 를 검색합니다. AWSDiscoveryContinuousExportFirehosePolicy
7. 옆에 있는 AWSDiscoveryContinuousExportFirehosePolicy상자를 선택한 후 다음: 검토를 선택합니다.
8. 역할 AWSApplicationDiscoveryServiceFirehose이름으로 입력한 다음 역할 만들기를 선택합니다.

Application Discovery Service의 AWS 관리형 정책 업데이트

이 서비스가 이러한 변경 사항을 추적하기 시작한 이후 Application Discovery Service의 AWS 관리형 정책 업데이트에 대한 세부 정보를 확인하십시오. 이 페이지의 변경 사항에 대한 자동 알림을 받아보려면 AWS Application Discovery Service 문서 기록 페이지에서 RSS 피드를 구독합니다.

변경 사항	설명	날짜
AWSApplicationDiscoveryAgentlessCollectorAccess— 에이전트리스 컬렉터 출시와 함께 새로운 정책이 제공되었습니다.	Application Discovery Service는 에이전트 없는 수집기에 Application Discovery Service에 등록 및 통신하고 다른 AWS 서비스와 통신할 수 있는 액세스 권한을 부여하는 새로운 관리형 정책을 `AWSApplicationDiscoveryAgentlessCollectorAccess` 추가했습니다.	2022년 8월 16일

변경 사항	설명	날짜
Application Discovery Service가 변경 사항 추적을 시작했습니다.	Application Discovery Service는 AWS 관리형 정책의 변경 사항을 추적하기 시작했습니다.	2021년 3월 1일

AWS Application Discovery Service ID 기반 정책 예제

기본적으로 IAM 사용자 및 역할에는 Application Discovery Service 리소스를 만들거나 수정할 권한이 없습니다. 또한 AWS Management Console AWS CLI, 또는 AWS API를 사용하여 작업을 수행할 수 없습니다. IAM 관리자는 지정된 리소스에서 특정 API 작업을 수행할 수 있는 권한을 사용자와 역할에게 부여하는 IAM 정책을 생성해야 합니다. 그런 다음 관리자는 해당 권한이 필요한 IAM 사용자 또는 그룹에 이러한 정책을 연결해야 합니다.

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

주제

- 정책 모범 사례
- Application Discovery Service에 대한 전체 액세스 권한 부여
- 디스커버리 에이전트에 액세스 권한 부여
- 상담원 데이터 수집 권한 부여
- 데이터 탐색 권한 부여
- Migration Hub 콘솔 네트워크 다이어그램 사용 권한 부여

정책 모범 사례

ID 기반 정책은 누군가가 사용자 계정에서 Application Discovery Service 리소스를 생성, 액세스 또는 삭제할 수 있는지 여부를 결정합니다. 이 작업으로 인해 AWS 계정에 비용이 발생할 수 있습니다. ID 기반 정책을 생성하거나 편집할 때는 다음 지침과 권장 사항을 따르세요.

- AWS 관리형 정책으로 시작하여 최소 권한 권한으로 이동 — 사용자와 워크로드에 권한을 부여하려면 여러 일반적인 사용 사례에 권한을 부여하는 AWS 관리형 정책을 사용하십시오. 에서 사용할 수 있습니다. AWS 계정사용 사례에 맞는 AWS 고객 관리형 정책을 정의하여 권한을 더 줄이는 것이 좋습니다. 자세한 정보는 IAM 사용 설명서의 AWS managed policies(관리형 정책) 또는 AWS managed policies for job functions(직무에 대한 관리형 정책)를 참조하세요.

- 최소 권한 적용 – IAM 정책을 사용하여 권한을 설정하는 경우 태스크를 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 Policies and permissions in IAM(IAM의 정책 및 권한)을 참조하세요.
- IAM 정책의 조건을 사용하여 액세스 추가 제한 – 정책에 조건을 추가하여 작업 및 리소스에 대한 액세스를 제한할 수 있습니다. 예를 들어 SSL을 사용하여 모든 요청을 전송해야 한다고 지정하는 정책 조건을 작성할 수 있습니다. 예를 AWS 서비스들어 특정 작업을 통해 서비스 작업을 사용하는 경우 조건을 사용하여 서비스 작업에 대한 액세스 권한을 부여할 수도 AWS CloudFormation있습니다. 자세한 정보는 IAM 사용 설명서의 IAM JSON 정책 요소: 조건을 참조하세요.
- IAM Access Analyzer를 통해 IAM 정책을 검증하여 안전하고 기능적인 권한 보장 – IAM Access Analyzer에서는 IAM 정책 언어(JSON)와 모범 사례가 정책에서 준수되도록 신규 및 기존 정책을 검증합니다. IAM Access Analyzer는 100개 이상의 정책 확인 항목과 실행 가능한 추천을 제공하여 안전하고 기능적인 정책을 작성하도록 돕습니다. 자세한 정보는 IAM 사용 설명서의 IAM Access Analyzer 정책 검증을 참조하tpdy.
- 멀티 팩터 인증 (MFA) 필요 - IAM 사용자 또는 루트 사용자가 필요한 시나리오가 있는 경우 추가 보안을 위해 AWS 계정 MFA를 활성화하십시오. API 작업을 직접 호출할 때 MFA가 필요하면 정책에 MFA 조건을 추가합니다. 자세한 정보는 IAM 사용 설명서의 Configuring MFA-protected API access(MFA 보호 API 액세스 구성)를 참조하세요.

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

Application Discovery Service에 대한 전체 액세스 권한 부여

AWSApplicationDiscoveryServiceFullAccess 관리형 정책은 IAM 사용자 계정에 Application Discovery Service 및 Migration Hub API에 대한 액세스 권한을 부여합니다.

이 정책을 계정에 연결한 IAM 사용자는 Application Discovery Service를 구성하고, 에이전트를 시작 및 중지하고, 에이전트 없는 검색을 시작 및 중지하고, 검색 서비스 데이터베이스에서 데이터를 쿼리할 수 있습니다. AWS 이 정책에 대한 자세한 내용은 AWS 에 대한 관리형 정책 AWS Application Discovery Service 단원을 참조하십시오.

Example AWSApplicationDiscoveryServiceFullAccess 정책

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

```
                "mgh:*",
                "discovery:*"
            ],
            "Effect": "Allow",
            "Resource": "*"
        },
        {
            "Action": [
                "iam:GetRole"
            ],
            "Effect": "Allow",
            "Resource": "*"
        }
    ]
}
```

디스커버리 에이전트에 액세스 권한 부여

AWSApplicationDiscoveryAgentAccess 관리형 정책은 애플리케이션 검색 에이전트가 Application Discovery Service에 등록하고 통신할 수 있는 액세스 권한을 부여합니다. 이 정책에 대한 자세한 내용은 AWS 에 대한 관리형 정책 AWS Application Discovery Service 단원을 참조하십시오.

응용 프로그램 검색 에이전트에서 사용하는 자격 증명을 가진 모든 사용자에게 이 정책을 연결하십시오.

또한 이 정책은 사용자에게 Arsenal에 대한 액세스 권한을 부여합니다. Arsenal은 에서 관리하고 AWS 호스팅하는 에이전트 서비스입니다. Arsenal은 클라우드의 Application Discovery Service로 데이터를 전달합니다.

Example AWSApplicationDiscoveryAgentAccess 정책

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

```
}
```

상담원 데이터 수집 권한 부여

ApplicationDiscoveryServiceContinuousExportServiceRolePolicy 관리형 정책을 사용하면 Amazon Data Firehose 스트림을 AWS Application Discovery Service 생성하여 Application Discovery Service 에이전트가 수집한 데이터를 변환하여 계정의 Amazon S3 버킷으로 전송할 수 AWS 있습니다.

또한 이 정책은 에이전트가 수집한 AWS Glue 데이터를 매핑하기 위한 테이블 `application_discovery_service_database` 스키마와 라는 새 데이터베이스를 포함하는 데이터 카탈로그를 생성합니다.

이 정책 사용에 대한 자세한 내용은 AWS 에 대한 관리형 정책 AWS Application Discovery Service 단원을 참조하십시오.

Example ApplicationDiscoveryServiceContinuousExportServiceRolePolicy

```
{
   "Version": "2012-10-17",
    "Statement": [
        {
            "Action": [
                "glue:CreateDatabase",
                "glue:UpdateDatabase",
                "glue:CreateTable",
                "glue:UpdateTable",
                "firehose:CreateDeliveryStream",
                "firehose:DescribeDeliveryStream",
                "logs:CreateLogGroup"
            ],
            "Effect": "Allow",
            "Resource": "*"
        },
        {
            "Action": [
                "firehose:DeleteDeliveryStream",
                "firehose:PutRecord",
                "firehose:PutRecordBatch",
                "firehose:UpdateDestination"
            ],
            "Effect": "Allow",
            "Resource": "arn:aws:firehose:*:*:deliverystream/aws-application-discovery-
service*"
```

```
        },
        {
            "Action": [
                "s3:CreateBucket",
                "s3:ListBucket",
                "s3:PutBucketLogging",
                "s3:PutEncryptionConfiguration"
            ],
            "Effect": "Allow",
            "Resource": "arn:aws:s3:::aws-application-discovery-service*"
        },
        {
            "Action": [
                "s3:GetObject"
            ],
            "Effect": "Allow",
            "Resource": "arn:aws:s3:::aws-application-discovery-service*/*"
        },
        {
            "Action": [
                "logs:CreateLogStream",
                "logs:PutRetentionPolicy"
            ],
            "Effect": "Allow",
            "Resource": "arn:aws:logs:*:*:log-group:/aws/application-discovery-service/
firehose*"
        },
        {
            "Action": [
                "iam:PassRole"
            ],
            "Effect": "Allow",
            "Resource": "arn:aws:iam::*:role/AWSApplicationDiscoveryServiceFirehose",
            "Condition": {
                "StringLike": {
                    "iam:PassedToService": "firehose.amazonaws.com"
                }
            }
        },
        {
            "Action": [
                "iam:PassRole"
            ],
            "Effect": "Allow",
```

```
            "Resource": "arn:aws:iam::*:role/service-role/
AWSApplicationDiscoveryServiceFirehose",
            "Condition": {
                "StringLike": {
                    "iam:PassedToService": "firehose.amazonaws.com"
                }
            }
        }
    ]
}
```

데이터 탐색 권한 부여

Amazon Athena에서 데이터 탐색을 사용하려면 AWSDiscoveryContinuousExportFirehosePolicy 정책이 필요합니다. 이를 통해 Amazon Data Firehose는 Application Discovery Service에서 수집한 데이터를 Amazon S3에 쓸 수 있습니다. 이 정책 사용에 대한 자세한 내용은 역할 생성 AWSApplicationDiscoveryServiceFirehose 단원을 참조하십시오.

Example AWSDiscoveryContinuousExportFirehosePolicy

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "glue:GetTableVersions"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "s3:AbortMultipartUpload",
                "s3:GetBucketLocation",
                "s3:GetObject",
                "s3:ListBucket",
                "s3:ListBucketMultipartUploads",
                "s3:PutObject"
            ],
            "Resource": [
                "arn:aws:s3:::aws-application-discovery-service-*",
                "arn:aws:s3:::aws-application-discovery-service-*/*"
```

```
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "logs:PutLogEvents"
            ],
            "Resource": [
                "arn:aws:logs:*:*:log-group:/aws/application-discovery-service/
firehose:log-stream:*"
            ]
        }
    ]
}
```

Migration Hub 콘솔 네트워크 다이어그램 사용 권한 부여

Application Discovery Service 또는 Migration Hub에 대한 액세스를 허용하거나 거부하는 ID 기반 정책을 생성할 때 AWS Migration Hub 콘솔 네트워크 다이어그램에 대한 액세스 권한을 부여하려면 정책에 `discovery:GetNetworkConnectionGraph` 작업을 추가해야 할 수 있습니다.

정책에 다음 두 가지가 모두 해당하는 경우 새 정책에서 `discovery:GetNetworkConnectionGraph` 작업을 사용하거나 이전 정책을 업데이트해야 합니다.

- 이 정책은 Application Discovery Service 또는 Migration Hub에 대한 액세스를 허용하거나 거부합니다.
- 정책은 `discovery:`*`action-name`* 보다 `discovery:*` 구체적인 검색 작업 (예:) 을 하나 더 사용하여 액세스 권한을 부여합니다.

다음 예는 IAM 정책에서 `discovery:GetNetworkConnectionGraph` 작업을 사용하는 방법을 보여줍니다.

Example

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": ["discovery:GetNetworkConnectionGraph"],
            "Resource": "*"
```

```
        }
    ]
}
```

Migration Hub 네트워크 다이어그램에 대한 자세한 내용은 Migration Hub에서 네트워크 연결 보기를 참조하십시오.

Application Discovery 서비스에 대한 서비스 연결 역할 사용

AWS Application Discovery Service은 AWS Identity and Access Management(IAM) 서비스 연결 역할을 사용합니다. 서비스 연결 역할은 Application Discovery Service에 직접 연결된 고유한 유형의 IAM 역할입니다. 서비스 연결 역할은 Application Discovery Service에서 사전 정의하며 서비스에서 다른 역할을 호출하기 위해 필요한 모든 권한을 포함합니다.AWS사용자를 대신하여 서비스를 제공합니다.

필요한 권한을 수동으로 추가할 필요가 없으므로 서비스 연결 역할은 Application Discovery Service를 더 쉽게 설정할 수 있습니다. Application Discovery Service에서 서비스 연결 역할의 권한을 정의합니다. 달리 정의되어 있지 않는 한, Application Discovery Service Service만 역할을 수임 정의된 권한에는 신뢰 정책과 권한 정책이 포함되며, 이 권한 정책은 다른 IAM 엔터티에 연결할 수 없습니다.

먼저 관련 리소스를 삭제한 후에만 서비스 연결 역할을 삭제할 수 있습니다. 이렇게 하면 리소스에 대한 액세스 권한을 부주의로 삭제할 수 없기 때문에 Application Discovery Service Service가 보호됩니다.

주제

- Application Discovery 서비스에 대한 서비스 연결 역할 권한
- Application Discovery 서비스에 대한 서비스 연결 역할 생성
- Application Discovery 서비스에 대한 서비스 연결 역할 삭제

서비스 연결 역할을 지원하는 기타 서비스에 대한 자세한 내용은 IAM으로 작업하는 AWS 서비스를 참조해 서비스 연결 역할(Service-Linked Role) 열이 예(Yes)인 서비스를 찾으세요. 해당 서비스에 대한 서비스 연결 역할 설명서를 보려면 예(Yes) 링크를 선택합니다.

Application Discovery 서비스에 대한 서비스 연결 역할 권한

Application Service에서는 인 서비스 연결 역할을 사용합니다.AWSServiceRoleForApplicationDiscoveryServiceContinuousExport— 다음에 액세스할 수 있습니다.AWS사용 또는 관리되는 서비스 및 리소스AWS Application Discovery Service.

이 AWSServiceRoleForApplicationDiscoveryServiceContinuousExport 서비스 연결 역할은 역할을 수임하기 위해 다음 서비스를 신뢰합니다.

- continuousexport.discovery.amazonaws.com

역할 권한 정책은 Application Discovery Service 다음 작업을 완료하도록 허용합니다.

글루

  CreateDatabase

  UpdateDatabase

  CreateTable

  UpdateTable

firehose

  CreateDeliveryStream

  DeleteDeliveryStream

  DescribeDeliveryStream

  PutRecord

  PutRecordBatch

  UpdateDestination

s3

  CreateBucket

  ListBucket

  GetObject

로그

  CreateLogGroup

  CreateLogStream

  PutRetentionPolicy

iam

`PassRole`

다음은 위의 작업이 적용되는 리소스를 보여 주는 전체 정책입니다.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": [
                "glue:CreateDatabase",
                "glue:UpdateDatabase",
                "glue:CreateTable",
                "glue:UpdateTable",
                "firehose:CreateDeliveryStream",
                "firehose:DescribeDeliveryStream",
                "logs:CreateLogGroup"
            ],
            "Effect": "Allow",
            "Resource": "*"
        },
        {
            "Action": [
                "firehose:DeleteDeliveryStream",
                "firehose:PutRecord",
                "firehose:PutRecordBatch",
                "firehose:UpdateDestination"
            ],
            "Effect": "Allow",
            "Resource": "arn:aws:firehose:*:*:deliverystream/aws-application-discovery-
service*"
        },
        {
            "Action": [
                "s3:CreateBucket",
                "s3:ListBucket",
                "s3:PutBucketLogging",
                "s3:PutEncryptionConfiguration"
            ],
            "Effect": "Allow",
            "Resource": "arn:aws:s3:::aws-application-discovery-service*"
        },
```

```
        {
            "Action": [
                "s3:GetObject"
            ],
            "Effect": "Allow",
            "Resource": "arn:aws:s3:::aws-application-discovery-service*/*"
        },
        {
            "Action": [
                "logs:CreateLogStream",
                "logs:PutRetentionPolicy"
            ],
            "Effect": "Allow",
            "Resource": "arn:aws:logs:*:*:log-group:/aws/application-discovery-service/
firehose*"
        },
        {
            "Action": [
                "iam:PassRole"
            ],
            "Effect": "Allow",
            "Resource": "arn:aws:iam::*:role/AWSApplicationDiscoveryServiceFirehose",
            "Condition": {
                "StringLike": {
                    "iam:PassedToService": "firehose.amazonaws.com"
                }
            }
        },
        {
            "Action": [
                "iam:PassRole"
            ],
            "Effect": "Allow",
            "Resource": "arn:aws:iam::*:role/service-role/
AWSApplicationDiscoveryServiceFirehose",
            "Condition": {
                "StringLike": {
                    "iam:PassedToService": "firehose.amazonaws.com"
                }
            }
        }
    ]
}
```

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

Application Discovery 서비스에 대한 서비스 연결 역할 생성

서비스 연결 역할은 수동으로 생성할 필요가 없습니다. 이 AWSServiceRoleForApplicationDiscoveryServiceContinuousExport 서비스 연결 역할은 a) “데이터 수집 시작”을 선택한 후 데이터 수집기 페이지에서 제공되는 대화 상자에서 옵션을 확인하거나 “Athena에서의 데이터 탐색”이라는 슬라이더를 클릭하여 연속 내보내기가 암시적으로 켜진 경우 또는 b) StartContinuousExport 를 사용하는 APIAWSCLI.

> **Important**
>
> 이 서비스 연결 역할은 이 역할이 지원하는 기능을 사용하는 다른 서비스에서 작업을 완료했을 경우 계정에 나타날 수 있습니다. 자세한 내용은 내 IAM 계정에 표시되는 새 역할을 참조하세요.

Migration Hub 콘솔에서 서비스 연결 역할 생성

Migration Hub 콘솔을 사용하여 AWSServiceRoleForApplicationDiscoveryServiceContinuousExport 서비스 연결 역할

서비스 연결 역할을 생성하려면 다음을 수행합니다(콘솔).

1. 탐색 창에서 Data Collectors(데이터 수집기)를 선택합니다.
2. 에이전트 탭을 선택합니다.
3. 토글Athena의 데이터 탐색슬라이더를 On 위치로 이동합니다.
4. 이전 단계에서 생성된 대화 상자에서 관련 비용에 대해 동의하는 확인란을 클릭하고 계속 또는 활성화를 선택합니다.

에서 서비스 연결 역할 생성AWS CLI

에서 Application Discovery Service 명령을 사용할 수 있습니다.AWS Command Line Interface를 만들려면 AWSServiceRoleForApplicationDiscoveryServiceContinuousExport서비스 연결 역할

이 서비스 연결 역할은 에서 연속 내보내기를 시작할 때 자동으로 생성됩니다.AWS CLI(그AWS CLI먼저 사용자 환경에 설치해야 합니다.)

에서 연속 내보내기를 시작하여 서비스 연결 역할을 만드는 방법 (CLI)AWS CLI

1. 운영 체제(Linux, macOS, Windows)에 맞는 AWS CLI를 설치합니다. 다음을 참조:AWS Command Line Interface사용 설명서자세한 내용은 단원을 참조하세요
2. 명령 프롬프트(Windows) 또는 터미널(Linux나 macOS)을 엽니다.
   a. `aws configure`를 입력하고 Enter 키를 누릅니다.
   b. 귀하의 정보를 입력하십시오AWS액세스 키 ID 및AWS보안 액세스 키.
   c. 기본 리전 이름에 `us-west-2`를 입력합니다.
   d. 기본 출력 형식에 `text`를 입력합니다.
3. 다음 명령을 입력합니다.

```
aws discovery start-continuous-export
```

또한 IAM 콘솔을 사용해 다음과 같은 서비스 연결 역할을 생성할 수도 있습니다.디스커버리 서비스 - 연속 내보내기사용 사례. IAM CLI 또는 IAM API에서 `continuousexport.discovery.amazonaws.com` 서비스 이름의 서비스 연결 역할을 생성합니다. 자세한 내용은 IAM 사용 설명서의 서비스 연결 역할 생성 섹션을 참조하세요. 이 서비스 연결 역할을 삭제한 후에는 동일한 프로세스를 사용하여 역할을 다시 생성할 수 있습니다.

Application Discovery 서비스에 대한 서비스 연결 역할 삭제

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

서비스 연결 역할 정리

IAM을 사용하여 서비스 연결 역할을 삭제하기 전에 먼저 역할에서 사용되는 리소스를 삭제해야 합니다.

> **Note**
>
> 리소스를 삭제하려 할 때 Application Discovery Service 역할을 사용 중이면 삭제에 실패할 수 있습니다. 이 문제가 발생하면 몇 분 기다렸다가 작업을 다시 시도하세요.

에서 사용하는 Application Discovery Service 리소스를 삭제하려면 AWSServiceRoleForApplicationDiscoveryServiceContinuousExport Migration Hub 콘솔의 서비스 연결 역할

1. 탐색 창에서 Data Collectors(데이터 수집기)를 선택합니다.
2. 에이전트 탭을 선택합니다.
3. 토글Athena의 데이터 탐색슬라이더를 Off 위치로 이동합니다.

에서 사용하는 Application Discovery Service 리소스를 삭제하려면 AWSServiceRoleForApplicationDiscoveryServiceContinuousExport 의 서비스 연결 역할은AWS CLI

1. 운영 체제(Linux, macOS, Windows)에 맞는 AWS CLI를 설치합니다. 다음을 참조:AWS Command Line Interface사용 설명서자세한 내용은 단원을 참조하세요
2. 명령 프롬프트(Windows) 또는 터미널(Linux나 macOS)을 엽니다.
   a. `aws configure`를 입력하고 Enter 키를 누릅니다.
   b. 귀하의 정보를 입력하십시오AWS액세스 키 ID 및AWS보안 액세스 키.
   c. 기본 리전 이름에 `us-west-2`를 입력합니다.
   d. 기본 출력 형식에 `text`를 입력합니다.
3. 다음 명령을 입력합니다.

```
aws discovery stop-continuous-export --export-id <export ID>
```

   - 중지하려는 연속 내보내기의 내보내기 ID를 모르는 경우 다음 명령을 입력하여 연속 내보내기의 ID를 확인합니다.

```
aws discovery describe-continuous-exports
```

4. 다음 명령을 입력하여 반환 상태가 “비활성”인지 확인하여 연속 내보내기가 중지되었는지 확인합니다.

```
aws discovery describe-continuous-export
```

수동으로 서비스 연결 역할 삭제

삭제할 수 있음 AWSServiceRoleForApplicationDiscoveryServiceContinuousExport IAM 콘솔, AWS CLI 또는 IAM API를 사용하여 서비스 연결 역할을 사용합니다. 이 서비스 연결 역할이 필요한 Discovery Service - 연속 내보내기 기능을 더 이상 사용하지 않을 경우에는 해당 역할을 삭제하는 것이 좋습니다. 따라서 적극적으로 모니터링하거나 유지하지 않는 미사용 엔터티가 없도록 합니다. 자세한 내용은 IAM 사용 설명서의 서비스 연결 역할 삭제 섹션을 참조하세요.

> **Note**
>
> 삭제하기 전에 먼저 서비스 연결 역할을 정리해야 합니다. 서비스 연결 역할 정리을 참조하세요.

AWS Application Discovery Service ID 및 액세스 문제 해결

다음 정보를 사용하면 Application Discovery Service 및 IAM을 사용할 때 발생할 수 있는 일반적인 문제를 진단하고 해결하는 데 도움이 됩니다.

주제

- 저는 IAM을 수행할 권한이 없습니다. PassRole

저는 IAM을 수행할 권한이 없습니다. PassRole

작업을 수행할 권한이 없다는 오류 메시지가 표시되는 경우 Application Discovery Service에 역할을 전달할 수 있도록 정책을 업데이트해야 합니다. `iam:PassRole`

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

다음 예제 오류는 이라는 IAM 사용자가 Application Discovery Service에서 콘솔을 사용하여 작업을 `marymajor` 수행하려고 할 때 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 필요하면 AWS 관리자에게 문의하세요. 관리자는 로그인 자격 증명을 제공한 사람입니다.

AWS Application Discovery Service의 로깅 및 모니터링

AWS Application Discovery Service는 AWS CloudTrail에 통합됩니다. 이 CloudTrail 문제 해결 및 감사 목적으로 계정 활동을 기록하고 지속적으로 모니터링하고 유지합니다. CloudTrail 에 대한 이벤트 기록을 제공합니다.AWS계정 활동 (다음을 통해 수행된 작업 포함)AWSManagement ConsoleAWSSDK 및 명령줄 도구 이 단원의 주제에서는 사용 방법을 설명합니다. CloudTrail 애플리케이션 Discovery Service

주제

- 을 사용하여 Application Discovery Service API 호출 로깅AWS CloudTrail

을 사용하여 Application Discovery Service API 호출 로깅AWS CloudTrail

AWS Application Discovery Service와 와 통합AWS CloudTrail, 사용자, 역할 또는AWSApplication Discovery Service CloudTrail 는 Application Discovery Service 에 대한 API 호출을 이벤트로 캡처 캡처되는 호출에는 Application Discovery Service 콘솔로부터의 호출과 Application Discovery Service API 작업에 대한 코드 호출이

추적을 생성하면 에 대한 지속적인 배포를 활성화할 수 있습니다. CloudTrail Application Discovery Service 에 대한 이벤트를 포함하여 Amazon S3 버킷에 대한 이벤트 추적을 구성하지 않은 경우 에서 최신 이벤트를 볼 수도 있습니다. CloudTrail 콘솔 인이벤트 기록. 에서 수집하는 정보 사용 CloudTrail 에서 Application Discovery Service 에 수행된 요청, 요청이 수행된 IP 주소, 요청을 수행한 사람, 요청이 수행된 시간 및 추가 세부 정보를 확인할 수 있습니다.

알아볼 내용 CloudTrail섹션을 참조하세요.AWS CloudTrail사용 설명서.

의 Application Discovery Service CloudTrail

CloudTrail 에서 활성화되었습니다AWS계정 생성 시 Application Discovery Service 에서 활동이 이루어지면 CloudTrail 다른 사람과 함께 하는 이벤트AWS에서 서비스 이벤트이벤트 기록. AWS 계정에서

최신 이벤트를 확인, 검색 및 다운로드할 수 있습니다. 자세한 내용을 알아보려면 다음 섹션을 참조하세요.에서 에서 이벤트 보기 CloudTrail 이벤트 기록.

에서 이벤트를 지속적으로 기록하려면AWSApplication Discovery Service 에 대한 이벤트를 포함하는 계정이 추적을 생성합니다. A트레일가능하게 하다 CloudTrail Amazon S3 버킷으로 로그 파일을 전송하려면 콘솔에서 추적을 생성하면 기본적으로 모든 AWS 리전에 추적이 적용됩니다. 추적은 AWS 파티션에 있는 모든 리전의 이벤트를 로깅하고 지정된 Amazon S3 버킷으로 로그 파일을 전송합니다. 또한 다른 항목을 구성할 수 있습니다.AWS에서 수집된 이벤트 데이터를 추가 분석 및 처리하기 위한 서비스 CloudTrail 로그. 자세한 내용은 다음 자료를 참조하세요.

- 추적 생성 개요
- CloudTrail 지원 서비스 및 통합
- 에 대한 Amazon SNS 알림 구성 CloudTrail
- 수신 CloudTrail 여러 리전에서 로그 파일과수신 CloudTrail 여러 계정의 로그 파일

모든 Application Discovery Service CloudTrail 에 문서화되어 있습니다.Application Discovery Service. 예를 들어 에 대한 호출은`CreateTags`,`DescribeTags`, 및`GetDiscoverySummary`작업은 에서 항목을 생성합니다. CloudTrail 로그 파일

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

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

자세한 내용은 CloudTrail userIdentity 요소를 참조하십시오.

Application Discovery Service 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 호출에 대한 순서 지정된 스택 기록이 아니기 때문에 특정 순서로 표시되지 않습니다.

다음 예제에서는 CloudTrail 를 보여 주는 로그 항목DescribeTags작업.


```
{
    "eventVersion": "1.05",
    "userIdentity": {
        "type": "AssumedRole",
        "principalId": "AROAJBHMC4H6EKEXAMPLE:sample-user",
        "arn": "arn:aws:sts::444455556666:assumed-role/ReadOnly/sample-user",
        "accountId": "123456789012",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "sessionContext": {
            "sessionIssuer": {
                "type": "Role",
                "principalId": "AIDAJQABLZS4A3QDU576Q",
                "arn": "arn:aws:iam::444455556666:role/ReadOnly",
                "accountId": "444455556666",
                "userName": "sampleAdmin"
            },
            "webIdFederationData": {},
            "attributes": {
                "mfaAuthenticated": "false",
                "creationDate": "2020-05-05T15:19:03Z"
            }
        }
    },
    "eventTime": "2020-05-05T17:02:40Z",
    "eventSource": "discovery.amazonaws.com",
    "eventName": "DescribeTags",
    "awsRegion": "us-west-2",
    "sourceIPAddress": "20.22.33.44",
    "userAgent": "Coral/Netty4",
    "requestParameters": {
        "maxResults": 0,
        "filters": [
            {
                "values": [
                    "d-server-0315rfdjreyqsq"
                ],
                "name": "configurationId"
            }
        ]
    },
    "responseElements": null,
    "requestID": "mgh-console-eb1cf315-e2b4-4696-93e5-b3a3b9346b4b",
```

```
    "eventID": "7b32b778-91c9-4c75-9cb0-6c852791b2eb",
    "eventType": "AwsApiCall",
    "recipientAccountId": "111122223333"
}
```

AWS Application Discovery Service 할당량

Service Quotas 콘솔은 AWS Application Discovery Service 할당량에 대한 정보를 제공합니다. Service Quotas 콘솔을 사용하면 기본 Service Quotas 콘솔을 사용하거나요청 할당량 증가할당량 조정 가능.

현재 늘릴 수 있는 유일한 할당량은 다음과 같습니다.계정당 가져온 서버.

Application Discovery Service 에는 다음 기본 할당량이

- 계정당 애플리케이션 1,000개

  이 할당량에 도달한 경우 새 애플리케이션을 가져오려면 를 사용하여 기존 애플리케이션을 삭제하면 됩니다.`DeleteApplications`API 작업. 자세한 내용은 단원을 참조하십시오.DeleteApplications의Application Discovery Service API Reference.
- 가져오기 각 가져오기 파일의 최대 파일 크기는 10MB입니다.
- 계정당 가져온 서버 레코드 25,000개
- 가져오기 레코드 삭제 25,000.
- 계정당 10,000개의 가져온 서버 (이 할당량 증가를 요청할 수 있음).
- 1,000개의 활성 에이전트. 데이터를 수집하고 Application Discovery Service 로 전송하는 에이전트.
- 10,000개의 비활성 에이전트. 응답하지만 데이터를 수집하지 않는 에이전트.
- 애플리케이션당 서버 400개
- 서버당 30개의 태그

문제 해결 AWS Application Discovery Service

이 단원에서는 AWS Application Discovery Service에서 일반적으로 발생하는 문제를 해결하는 방법에 대한 정보를 확인할 수 있습니다.

주제

데이터 탐색을 통한 데이터 수집 중지

데이터 탐색을 중지하려면 Migration Hub 콘솔의 검색 > 데이터 수집기 > 에이전트 탭에서 토글 스위치를 끄거나 API를 호출할 수 있습니다. `StopContinuousExport` 데이터 수집을 중지하는 데 최대 30분이 소요될 수 있으며, 이 단계에서 콘솔의 토글 스위치와 `DescribeContinuousExport` API 호출 시 데이터 탐색 상태가 “Stop In Progress”로 표시됩니다.

> **Note**
>
> 콘솔 페이지를 새로 고친 후 토글이 꺼지지 않고 오류 메시지가 발생하거나 `DescribeContinuousExport` API가 "Stop_Failed" 상태로 돌아가는 경우 토글 스위치를 끄거나 `StopContinuousExport` API를 호출하여 다시 시도할 수 있습니다. '데이터 탐색'에 여전히 오류가 표시되고 성공적으로 중지되지 않으면 지원팀에 문의하세요. AWS

또는 다음 단계에 설명된 대로 수동으로 데이터 수집을 중지할 수 있습니다.

옵션 1: 에이전트 데이터 수집 중지

ADS 에이전트를 사용하여 이미 검색을 완료했으며 더 이상 ADS 데이터베이스 리포지토리에서 추가 데이터를 수집하지 않으려면 다음을 수행합니다.

1. Migration Hub 콘솔에서 검색 > 데이터 수집기 > 에이전트 탭을 선택합니다.
2. 실행 중인 기존 에이전트를 모두 선택한 다음 Stop Data Collection(데이터 수집 중지)을 선택합니다.

이렇게 하면 ADS 데이터 리포지토리 및 S3 버킷 모두에서 에이전트가 새 데이터를 수집하지 않습니다. 기존 데이터에는 액세스할 수 있습니다.

옵션 2: 데이터 탐색의 Amazon Kinesis Data Streams 삭제

ADS 데이터 리포지토리에서 에이전트가 데이터를 계속 수집하고 싶지만 데이터 탐색을 사용하여 Amazon S3 버킷의 데이터를 수집하고 싶지 않은 경우 데이터 탐색으로 생성된 Amazon Data Firehose 스트림을 수동으로 삭제할 수 있습니다.

1. AWS 콘솔에서 Amazon Kinesis에 로그인하고 탐색 창에서 Data Firehose를 선택합니다.
2. 데이터 탐색 기능으로 생성한 다음 스트림을 삭제하십시오.

   - `aws-application-discovery-service-id_mapping_agent`
   - `aws-application-discovery-service-inbound_connection_agent`
   - `aws-application-discovery-service-network_interface_agent`
   - `aws-application-discovery-service-os_info_agent`
   - `aws-application-discovery-service-outbound_connection_agent`
   - `aws-application-discovery-service-processes_agent`
   - `aws-application-discovery-service-sys_performance_agent`

데이터 탐색을 통해 수집된 데이터를 제거합니다.

데이터 탐색을 통해 수집된 데이터를 제거하려면

1. Amazon S3에 저장된 검색 에이전트 데이터를 제거합니다.

   AWS Application Discovery Service (ADS) 에서 수집한 데이터는 라는 S3 버킷에 저장됩니다`aws-application-discover-discovery-service-`*`uniqueid`*.

   > **Note**
   >
   > Amazon Athena에서 데이터 탐색이 활성화된 상태에서 Amazon S3 버킷 또는 버킷에 있는 객체를 삭제하면 오류가 발생합니다. 계속해서 새로운 디스커버리 에이전트 데이터를 S3로 전송합니다. Athena에서도 삭제된 데이터에 더 이상 액세스할 수 없습니다.

2. 제거 AWS Glue Data Catalog.

Amazon Athena에서 데이터 탐색을 활성화하면 계정에 Amazon S3 버킷이 생성되어 ADS 에이전트가 수집한 데이터를 일정 시간 간격으로 저장합니다. 또한 Amazon AWS Glue Data Catalog Athena에서 Amazon S3 버킷에 저장된 데이터를 쿼리할 수 있는 채널도 생성합니다. Amazon Athena에서 데이터 탐색을 비활성화하면 Amazon S3 버킷에 새 데이터가 저장되지 않지만 이전에 수집된 데이터는 계속 유지됩니다. 이 데이터가 더 이상 필요하지 않고 Amazon Athena에서 데이터 탐색이 활성화되기 전의 상태로 계정을 반환하려는 경우

a. AWS 콘솔에서 Amazon S3로 이동하여 이름이 “aws-application-discover-discover-discover-service-unique id”인 버킷을 수동으로 삭제합니다.
b. 애플리케이션-검색-서비스-데이터베이스 데이터베이스와 다음 테이블을 모두 삭제하여 데이터 탐색 AWS Glue Data Catalog를 수동으로 제거할 수 있습니다.

- `os_info_agent`
- `network_interface_agent`
- `sys_performance_agent`
- `processes_agent`
- `inbound_connection_agent`
- `outbound_connection_agent`
- `id_mapping_agent`

에서 데이터 제거 AWS Application Discovery Service

Application Discovery Service에서 모든 데이터를 제거하려면 AWS 지원팀에 문의하여 전체 데이터 삭제를 요청하십시오.

Amazon Athena의 데이터 탐색과 관련된 일반적인 문제 해결

이 섹션에서는 Amazon Athena의 데이터 탐색과 관련된 일반적인 문제를 해결하는 방법에 대한 정보를 찾을 수 있습니다.

주제

- 서비스 연결 역할 및 필수 AWS 리소스를 생성할 수 없기 때문에 Amazon Athena에서의 데이터 탐색이 시작되지 않음
- Amazon Athena에 새 에이전트 데이터가 표시되지 않음
- Amazon S3, Amazon Data Firehose에 액세스할 수 있는 권한이 충분하지 않거나 AWS Glue

서비스 연결 역할 및 필수 AWS 리소스를 생성할 수 없기 때문에 Amazon Athena에서의 데이터 탐색이 시작되지 않음

Amazon Athena에서 데이터 탐색을 활성화하면 계정에 서비스 연결 역할이 생성됩니다. 이 역할을 통해 에이전트가 Amazon S3 버킷`AWSServiceRoleForApplicationDiscoveryServiceContinuousExport`, Amazon Kinesis 스트림 등을 포함하여 Amazon Athena에서 수집한 데이터에 액세스할 수 있도록 하는 데 필요한 AWS 리소스를 생성할 수 있습니다. AWS Glue Data Catalog계정에 Amazon Athena에서 이 역할을 생성할 수 있는 적절한 데이터 탐색 권한이 없는 경우, 계정 초기화에 실패합니다. 자세한 내용은 AWS 에 대한 관리형 정책 AWS Application Discovery Service 항목을 참조하세요.

Amazon Athena에 새 에이전트 데이터가 표시되지 않음

새 데이터가 Athena로 유입되지 않고 에이전트가 시작된 지 30분이 넘었고 데이터 탐색 상태가 활성인 경우 아래 나열된 솔루션을 확인하십시오.

- AWS 디스커버리 에이전트

  에이전트의 수집 상태가 시작 상태로 표시되고 상태가 실행 중으로 표시되는지 확인합니다.

- Kinesis 역할

  계정에 `AWSApplicationDiscoveryServiceFirehose` 역할이 있는지 확인합니다.

- Firehose 상태

  다음 Firehose 전송 스트림이 제대로 작동하는지 확인하세요.

  - `aws-application-discovery-service/os_info_agent`
  - `aws-application-discovery-service-network_interface_agent`
  - `aws-application-discovery-service-sys_performance_agent`
  - `aws-application-discovery-service-processes_agent`
  - `aws-application-discovery-service-inbound_connection_agent`
  - `aws-application-discovery-service-outbound_connection_agent`
  - `aws-application-discovery-service-id_mapping_agent`

- AWS Glue Data Catalog

`application-discovery-service-database`데이터베이스가 안에 AWS Glue있는지 확인하세요. 다음 테이블이 AWS Glue에 있는지 확인합니다.

- `os_info_agent`
- `network_interface_agent`
- `sys_performance_agent`
- `processes_agent`
- `inbound_connection_agent`
- `outbound_connection_agent`
- `id_mapping_agent`

- Amazon S3 버킷

  계정에 이름이 지정된 Amazon S3 `aws-application-discovery-service-`*`uniqueid`* 버킷이 있는지 확인하십시오. 버킷의 객체가 이동되거나 삭제된 경우 Athena에 해당 객체가 제대로 표시되지 않습니다.

- 온프레미스 서버

  에이전트가 데이터를 수집하고 AWS Application Discovery Service로 전송할 수 있도록 서버가 실행 중인지 확인합니다.

Amazon S3, Amazon Data Firehose에 액세스할 수 있는 권한이 충분하지 않거나 AWS Glue

Amazon Athena를 사용하고 AWS Organizations있는데 데이터 탐색을 위한 초기화가 실패한다면 Amazon S3, Amazon Data Firehose, Athena 등에 액세스할 수 있는 권한이 없기 때문일 수 있습니다. AWS Glue

이러한 서비스에 대한 액세스 권한을 부여하려면 관리자 권한이 있는 IAM 사용자가 필요합니다. 관리자는 본인의 계정을 사용하여 이러한 액세스 권한을 부여할 수 있습니다. AWS 에 대한 관리형 정책 AWS Application Discovery Service를 참조하세요.

Amazon Athena에서의 데이터 탐색이 제대로 작동하도록 하려면 Amazon S3 버킷, Amazon Data Firehose 스트림 등을 포함하여 Amazon Athena에서 데이터 탐색을 통해 생성된 AWS 리소스를 수정하거나 삭제하지 마십시오. AWS Glue Data Catalog실수로 이러한 리소스를 삭제하거나 수정한 경우

데이터 탐색을 중지한 후 시작합니다. 그러면 이러한 리소스가 자동으로 다시 생성됩니다. 데이터 탐색으로 생성된 Amazon S3 버킷을 삭제하면 버킷에서 수집된 데이터가 손실될 수 있습니다.

레코드 가져오기 실패 문제 해결

Migration Hub 가져오기를 사용하면 디스커버리 커넥터 또는 디스커버리 에이전트를 사용하지 않고도 온-프레미스 환경의 세부 정보를 Migration Hub로 직접 가져올 수 있습니다. 이때 가져온 데이터에서 직접 마이그레이션 평가 및 계획을 수행할 수 있는 옵션이 제공됩니다. 디바이스를 애플리케이션으로 그룹화하고, 마이그레이션 상태를 추적할 수도 있습니다.

데이터를 가져올 때 오류가 발생할 수 있습니다. 일반적으로 이러한 오류의 원인은 다음 중 하나일 수 있습니다.

- 가져오기 관련 할당량에 도달함 - 가져오기 작업과 관련된 할당량이 있습니다. 할당량을 초과하는 가져오기 작업을 요청하면 요청이 실패하고 오류가 반환됩니다. 자세한 정보는 AWS Application Discovery Service 할당량을 참조하세요.
- 가져오기 파일에 쉼표 (,) 가 추가로 삽입되었습니다. —.CSV 파일의 쉼표는 한 필드를 다음 필드와 구분하는 데 사용됩니다. 쉼표는 필드를 구분하는 데 사용되기 때문에 필드 내에 쉼표를 사용하는 것은 지원되지 않습니다. 이것은 포맷 오류의 연쇄적인 원인이 될 수 있습니다. 쉼표는 필드 간에만 사용하고, 가져오기 파일의 다른 부분에는 사용하지 마십시오.
- 필드의 값이 지원되는 범위를 벗어났습니다. — 예를 들어 일부 필드에는 지원하는 값 범위가 `CPU.NumberOfCores` 있어야 합니다. 지원되는 범위보다 크거나 작은 값이 있으면 레코드 가져오기가 실패합니다.

가져오기 요청에 오류가 발생하면 가져오기 작업에서 실패한 레코드를 다운로드하여 해결하고, 실패한 항목 CSV 파일의 오류를 해결한 후 가져오기를 다시 수행하십시오.

Console

실패한 레코드 아카이브를 다운로드하려면

1. 에 AWS Management Console로그인하고 에서 Migration Hub 콘솔을 엽니다https://console.aws.amazon.com/migrationhub.
2. 왼쪽 탐색 창의 검색에서 도구를 선택합니다.
3. 검색 도구에서 가져오기 보기를 선택합니다.
4. 가져오기 대시보드에서 실패한 레코드 수가 있는 가져오기 요청에 대한 라디오 버튼을 선택합니다.

5. 대시보드에서 테이블 위의 레코드를 다운로드하지 못함을 선택합니다. 그러면 아카이브 파일을 다운로드할 수 있는 브라우저의 대화 상자가 열립니다.

AWS CLI

실패한 레코드 아카이브를 다운로드하려면

1. 터미널 창을 열고 다음 명령을 입력합니다. *ImportName* is the name of the import task with the failed entries that you want to correct.:

```
aws discovery describe-import-tasks - -name ImportName
```

2. 출력에서 errorsAndFailedEntriesZip에 대해 반환된 값의 전체 내용을 따옴표를 제외하고 복사합니다.
3. 웹 브라우저를 열고 URL 입력란에 내용을 붙여 넣은 후 ENTER를 누릅니다. 그러면 실패한 레코드 아카이브가 압축된 zip 형식으로 다운로드됩니다.

실패한 레코드 아카이브를 다운로드했으므로 이제 두 개의 파일을 추출하여 오류를 수정할 수 있습니다. 오류가 서비스 기반 한도로 인한 것일 경우, 한도 증가를 요청하십시오 또는 관련 리소스를 충분히 삭제하여 계정을 한도 이내로 유지하십시오. 아카이브에는 다음 파일이 있습니다.

- errors-file.csv - 이 파일은 오류 로그이며, 실패한 각 항목의 각 실패 레코드에 대한 줄ExternalId, 열 이름 및 설명이 포함된 오류 메시지를 추적합니다.
- failed-entries-file.csv — 이 파일에는 원본 가져오기 파일의 실패한 항목만 들어 있습니다.

발생한 non-limit-based 오류를 수정하려면 를 사용하여 파일의 errors-file.csv 문제를 수정한 다음 해당 failed-entries-file.csv 파일을 가져오십시오. 파일 가져오기에 대한 지침은 데이터 가져오기 단원을 참조하십시오.

AWS Application Discovery Service 문서 기록

최신 사용자 가이드 문서 업데이트: 2023년 5월 16일

다음 표는 2019년 1월 이후 사용 설명서 에서 변경된 중요 사항을 설명합니다. 설명서 업데이트에 대한 알림을 받으려면 RSS 피드를 구독하시면 됩니다.

변경 사항	설명	날짜
에이전트리스 컬렉터 데이터베이스 및 분석 데이터 수집 모듈 소개	데이터베이스 및 분석 데이터 수집 모듈은 Application Discovery Service 에이전트리스 컬렉터 (Agentless Collector) 의 새로운 모듈입니다. 이 데이터 수집 모듈을 사용하여 환경에 연결하고 온프레미스 데이터베이스 및 분석 서버에서 메타데이터 및 성능 지표를 수집할 수 있습니다. 자세한 내용은 데이터베이스 및 분석 데이터 수집 모듈을 참조하십시오.	2023년 5월 16일
Application Discovery Service 에이전트리스 컬렉터 소개	Application Discovery Service 에이전트리스 컬렉터 (Agentless Collector) 는 AWS Application Discovery Service 온프레미스 환경에 대한 에이전트 없는 방법을 통해 정보를 수집하여 해당 환경으로의 마이그레이션을 효과적으로 계획할 수 있도록 도와주는 새로운 온-프레미스 애플리케이션입니다. AWS 클라우드 자세한 내용은 에이전트리스 컬렉터를 섹션을 참조하세요.	2022년 8월 16일

IAM 업데이트	이제 ID 기반 정책을 생성할 때 AWS Migration Hub 콘솔 네트워크 다이어그램에 대한 액세스 권한을 부여하는 데 AWS Identity and Access Management (IAM) `discovery:GetNetworkConnectionGraph` 작업을 사용할 수 있습니다. 자세한 내용은 네트워크 다이어그램 사용 권한 부여를 참조하십시오.	2022년 5월 24일
홈 지역 소개	Migration Hub 홈 리전은 전체 포트폴리오에 대한 검색 및 마이그레이션 계획 정보가 담긴 단일 리포지토리와 여러 AWS 지역으로의 마이그레이션을 한눈에 볼 수 있는 단일 리포지토리를 제공합니다.	2019년 11월 20일
Migration Hub 가져오기 기능 소개	Migration Hub 가져오기를 사용하면 서버 사양 및 사용률 데이터를 포함하여 온프레미스 서버 및 애플리케이션에 대한 정보를 Migration Hub Hub로 가져올 수 있습니다. 이 데이터를 사용하여 애플리케이션 마이그레이션 상태를 추적할 수도 있습니다. 자세한 내용은 Migration Hub 가져오기를 섹션을 참조하세요.	2019년 1월 18일

다음 표에서는 2019년 1월 18일 이전에 발표된 Application Discovery Service 사용 설명서에 대한 설명서를 설명합니다.

변경 사항	설명	날짜
새로운 기능	Amazon Athena에서 데이터 탐색을 지원하도록 문서를 업데이트하고 문제 해결 장을 추가했습니다.	2018년 8월 09일
주요 내용 개정	사용 및 출력에 대한 세부 정보를 다시 작성하고, 전체 문서를 재구성했습니다.	2018년 5월 25일
Discovery Agent 2.0	새롭고 개선된 Application Discovery Agent가 출시되었습니다.	2017년 10월 19일
콘솔	AWS Management Console이 추가되었습니다.	2016년 19월 12일
에이전트 없는 검색	이 릴리스는 에이전트가 없는 검색을 설정하고 구성하는 방법에 대해 설명합니다.	2016년 7월 28일
Microsoft Windows Server에 대한 새로운 세부 정보 및 명령 관련 문제 해결	이 업데이트에는 Microsoft Windows Server에 대한 세부 정보가 추가되었습니다. 또한 다양한 명령 관련 문제에 대한 수정이 포함되어 있습니다.	2016년 5월 20일
최초 게시	이 설명서는 Application Discovery Service '사용 설명서'에서 변경된 중요 사항을 기술한 것입니다.	2016년 5월 12일

AWS 용어집

최신 AWS 용어는 AWS 용어집 참조서의 AWS 용어집을 참조하세요.

부록

이 섹션에는 에 대한 추가 정보가 포함되어 있습니다. AWS Application Discovery Service

주제

부록: 디스커버리 커넥터에서 에이전트 없는 컬렉터로의 전환

이 섹션에서는 AWS 에이전트 없는 검색 커넥터 (검색 커넥터) 에서 Application Discovery Service 에이전트 없는 수집기 (에이전트 없는 수집기) 로 전환하는 방법에 대해 설명합니다.

현재 디스커버리 커넥터를 사용하고 있는 고객은 새로운 에이전트 없는 컬렉터로 전환하는 것이 좋습니다.

에이전트 없는 컬렉터 사용을 시작하는 방법을 알아보려면 을 참조하십시오. 에이전트리스 컬렉터 시작하기

에이전트리스 컬렉터를 배포한 후에는 디스커버리 커넥터 가상 컴퓨터를 삭제할 수 있습니다. 이전에 수집된 모든 데이터는 AWS Migration Hub (Migration Hub) 에서 계속 사용할 수 있습니다.

부록: AWS 에이전트리스 디스커버리 커넥터

> **Important**
>
> 현재 디스커버리 커넥터를 사용 중인 고객은 새로운 에이전트리스 컬렉터로 전환하는 것이 좋습니다. 자세한 설명은 부록: 디스커버리 커넥터에서 에이전트 없는 컬렉터로의 전환 섹션을 참조하세요.

주제

디스커버리 커넥터에서 수집한 데이터

디스커버리 커넥터는 VMware vCenter Server 호스트 및 VM에 대한 정보를 수집합니다. 하지만 VMware vCenter Server 도구가 설치된 경우에만 이런 데이터를 캡처할 수 있습니다. 사용 중인 AWS 계정에 이 작업에 필요한 권한이 있는지 확인하려면 을 참조하십시오. AWS 에 대한 관리형 정책 AWS Application Discovery Service

다음에서 디스커버리 커넥터에서 수집한 정보의 인벤토리를 찾을 수 있습니다.

디스커버리 커넥터가 수집한 데이터에 대한 표 범례:

- 수집된 데이터는 별도의 명시가 없는 경우에는 KB(Kilobytes)로 측정됩니다.
- Migration Hub 콘솔의 해당 데이터는 메가바이트 (MB) 단위로 보고됩니다.
- 별표 (*) 로 표시된 데이터 필드는 커넥터의 API 내보내기 기능에서 생성된.csv 파일에서만 사용할 수 있습니다.
- 폴링 기간의 간격은 약 60분입니다.
- 현재 이중 별표(**)로 표시된 데이터 필드는 null 값을 반환합니다.

데이터 필드	설명
applicationConfigurationId*	VM이 그룹으로 속한 마이그레이션 애플리케이션의 ID
avgCpuUsagePct	폴링 기간의 평균 CPU 사용량(%)
avgDiskBytesReadPerSecond	폴링 기간에 디스크에서 읽은 평균 바이트 수
avgDiskBytesWrittenPerSecond	폴링 기간에 디스크에 쓴 평균 바이트 수
avgDiskReadOpsPerSecond**	초당 평균 읽기 I/O 연산 수 null
avgDiskWriteOpsPerSecond**	초당 평균 쓰기 I/O 연산 수
avgFreeRAM	평균적으로 사용 가능한 RAM(MB)
avgNetworkBytesReadPerSecond	초당 평균 읽기 처리량(바이트)
avgNetworkBytesWrittenPerSecond	초당 평균 쓰기 처리량(바이트)

데이터 필드	설명
configId	Application Discovery Service에서 검색된 VM에 ID를 할당했습니다.
configType	검색된 리소스의 유형
connectorId	검색 커넥터 가상 어플라이언스의 ID
cpuType	VM의 경우 vCPU, 호스트의 경우 실제 모델
datacenterId	vCenter ID
hostId*	VM 호스트 ID
hostName	가상 소프트웨어를 실행하는 호스트의 이름
하이퍼바이저	하이퍼바이저 유형
id	서버 ID
lastModifiedTime스탬프*	데이터를 내보내기 전 마지막으로 데이터를 수집한 날짜와 시간
macAddress	VM 제조업체의 MAC
주소	가상 소프트웨어 제조사
maxCpuUsage팩트	폴링 기간 동안 CPU 최대 사용량(%)
maxDiskBytesReadPerSecond	폴링 기간에 디스크에서 읽은 최대 바이트 수
maxDiskBytesWrittenPerSecond	폴링 기간에 디스크에 쓴 최대 바이트 수
maxDiskReadOpsPerSecond**	초당 최대 읽기 I/O 연산 수
maxDiskWriteOpsPerSecond**	초당 최대 쓰기 I/O 연산 수
maxNetworkBytesReadPerSecond	초당 최대 읽기 처리량(바이트)
maxNetworkBytesWrittenPerSecond	초당 최대 쓰기 처리량(바이트)

데이터 필드	설명
memoryReservation*	VM에 메모리가 초과 커밋되지 않도록 제한
moRefId	고유한 vCenter 관리 객체 참조 ID
name*	네트워크나 VM의 이름(사용자 지정)
numCores	CPU의 독립 처리 유닛 수
numCpus	VM의 중앙 처리 유닛 수
numDisks**	VM의 디스크 수
numNetworkCards**	VM의 네트워크 카드 수
osName	VM의 운영 체제 이름
osVersion	VM의 운영 체제 버전
portGroupId*	VLAN의 구성 포트 그룹 ID
portGroupName*	VLAN의 구성 포트 그룹 이름
powerState*	전력(Power) 상태
serverId	Application Discovery Service에서 검색된 VM에 ID를 할당했습니다.
smBiosId*	시스템 관리 BIOS의 ID/버전
state*	검색 커넥터 가상 어플라이언스의 상태
toolsStatus	VMware 도구들의 운영 상태(전체 목록은 데이터 수집기 보기 및 정렬를 참조)
totalDiskSize	디스크 총 용량(MB)
totalRAM	VM에서 사용할 수 있는 총 RAM(MB)
유형	호스트 유형

데이터 필드	설명
vCenterId	VM의 고유 ID 번호
vCenterName*	vCenter 호스트 이름
virtualSwitchName*	가상 스위치의 수
vmFolderPath	VM 파일의 디렉터리 경로.
vmName	가상 머신의 수

디스커버리 커넥터 데이터 수집

검색 커넥터를 VMware 환경에 배포하고 구성한 후 데이터 수집이 중지되면 다시 시작할 수 있습니다. 콘솔을 통해 또는 를 통해 API를 호출하여 데이터 수집을 시작하거나 중지할 수 있습니다. AWS CLI두 방법 모두 다음 절차에 설명되어 있습니다.

Using the Migration Hub Console

다음 절차는 Migration Hub 콘솔의 데이터 수집기 페이지에서 Discovery Connector 데이터 수집 프로세스를 시작하거나 중지하는 방법을 보여줍니다.

데이터 수집을 시작 또는 중지하려면

1. 탐색 창에서 Data Collectors(데이터 수집기)를 선택합니다.
2. Connectors(커넥터) 탭을 선택합니다.
3. 시작하거나 중지하려는 커넥터의 확인란을 선택합니다.
4. Start data collection(데이터 수집 시작)이나 Stop data collection(데이터 수집 중지)를 선택합니다.

> **Note**
>
> 커넥터를 사용하여 데이터 수집을 시작한 후 인벤토리 정보가 표시되지 않으면 vCenter Server를 사용하여 커넥터를 등록했는지 확인합니다.

Using the AWS CLI

에서 Discovery Connector 데이터 수집 프로세스를 시작하려면 먼저 환경에 를 설치한 다음 선택한 Migration Hub 홈 지역을 사용하도록 CLI를 설정해야 합니다. AWS CLI AWS CLI

데이터 수집을 AWS CLI 설치하고 시작하려면

1. 운영 체제 (리눅스, macOS 또는 윈도우) AWS CLI 에 맞게 설치합니다. 지침은 AWS Command Line Interface 사용 설명서를 참조하십시오.
2. 명령 프롬프트(Windows) 또는 터미널(Linux나 macOS)을 엽니다.
   a. `aws configure`를 입력하고 Enter 키를 누릅니다.
   b. AWS 액세스 키 ID와 AWS 보안 액세스 키를 입력합니다.
   c. 기본 지역 이름에 거주 지역을 입력합니다. 예를 들어 `us-west-2`입니다.
   d. 기본 출력 형식에 `text`를 입력합니다.
3. 데이터 수집을 시작하거나 중지하려는 커넥터의 ID를 찾으려면 다음 명령을 입력하여 커넥터의 ID를 확인하십시오.

```
aws discovery describe-agents --filters
 condition=EQUALS,name=hostName,values=connector
```

4. 커넥터에서 데이터 수집을 시작하려면 다음 명령을 입력합니다.

```
aws discovery start-data-collection-by-agent-ids --agent-ids <connector ID>
```

> **Note**
> 커넥터를 사용하여 데이터 수집을 시작한 후 인벤토리 정보가 표시되지 않으면 vCenter Server를 사용하여 커넥터를 등록했는지 확인합니다.

커넥터를 통한 데이터 수집을 중지하려면 다음 명령을 입력합니다.

```
aws discovery stop-data-collection-by-agent-ids --agent-ids <connector ID>
```

디스커버리 커넥터 문제 해결

이 섹션에는 Application Discovery Service 검색 커넥터와 관련된 알려진 문제를 해결하는 데 도움이 되는 항목이 포함되어 있습니다.

설치 AWS 중에 검색 커넥터를 수정할 수 없는 문제를 해결할 수 없습니다.

콘솔에서 AWS 에이전트 없는 검색 커넥터를 구성할 때 다음과 같은 오류 메시지가 표시될 수 있습니다.

> 연결할 수 없습니다. AWS
>
> AWS 연결할 수 없습니다 (연결 재설정). 네트워크 및 프록시 설정을 확인하십시오.

이 오류는 설치 프로세스 중에 커넥터가 통신해야 하는 AWS 도메인에 대해 검색 커넥터가 HTTPS 연결을 설정하지 못했기 때문에 발생합니다. 연결을 설정할 수 없는 경우 검색 커넥터 구성이 실패합니다.

연결을 수정하려면 AWS

1. IT 관리자에게 문의하여 회사 방화벽이 포트 443에서 아웃바운드 액세스가 필요한 AWS 도메인으로 향하는 송신 트래픽을 차단하고 있는지 확인하십시오.

   아웃바운드 액세스가 필요한 AWS 도메인은 다음과 같습니다.

   - `awsconnector.`*`Migration Hub home Region`*`.amazonaws.com`
   - `sns.`*`Migration Hub home Region`*`.amazonaws.com`
   - `arsenal-discovery.`*`Migration Hub home Region`*`.amazonaws.com`
   - `iam.amazonaws.com`
   - `aws.amazon.com`
   - `ec2.amazonaws.com`

   방화벽이 송신 트래픽을 차단하는 경우 차단을 해제하세요. 방화벽을 업데이트한 후 커넥터를 재구성하십시오.
2. 방화벽을 업데이트해도 연결 문제가 해결되지 않으면 커넥터 가상 시스템에 나열된 도메인에 대한 아웃바운드 네트워크 연결이 있는지 확인하십시오. 가상 시스템이 아웃바운드 연결을 사용하

는 경우 다음 예와 같이 포트 443에서 텔넷을 실행하여 나열된 도메인과의 연결을 테스트하십시오.

```
telnet ec2.amazonaws.com 443
```

3. 가상 시스템으로부터의 아웃바운드 연결이 활성화된 경우 추가 문제 해결을 위해 AWS Support에 문의해야 합니다.

비정상 커넥터 수정

모든 디스커버리 커넥터의 상태 정보는 Migration Hub 콘솔의 데이터 수집기 페이지에서 찾을 수 있습니다. Health 상태가 비정상인 커넥터를 찾아 문제가 있는 커넥터를 식별할 수 있습니다. 다음 절차에서는 상태 문제를 식별하기 위해 커넥터 콘솔에 액세스하는 방법을 요약합니다.

커넥터 콘솔에 액세스

1. 웹 브라우저에서 Migration Hub 콘솔을 열고 왼쪽 탐색 메뉴에서 데이터 수집기를 선택합니다.
2. 커넥터 탭에서 상태가 비정상인 각 커넥터의 IP 주소를 기록해 둡니다.
3. 커넥터 가상 컴퓨터에 연결할 수 있는 컴퓨터에서 브라우저를 열고 커넥터 콘솔의 URL을 입력합니다. 여기서 `ip_address_of_connector` 은 비정상 커넥터의 IP 주소입니다. `https://ip_address_of_connector`
4. 커넥터를 구성했을 때 설정된 커넥터 관리 콘솔 암호를 입력합니다.

커넥터 콘솔에 액세스하면 비정상 상태를 해결하기 위한 조치를 취할 수 있습니다. 여기서 vCenter 연결에 대한 정보 보기를 선택하면 진단 메시지가 포함된 대화 상자가 나타납니다. 정보 보기 링크는 1.0.3.12 이상 버전의 커넥터에서만 사용 가능합니다.

상태 문제를 교정한 후, 커넥터와 vCenter 서버가 다시 연결되고, 커넥터 상태가 정상 상태로 변경됩니다. 문제가 지속되면 AWS Support에 문의하십시오.

가장 일반적인 비정상 커넥터의 원인은 IP 주소 문제와 자격 증명 문제입니다. 다음 섹션에서는 이러한 문제를 해결하고 커넥터를 정상 상태로 회복하도록 도움을 줄 수 있습니다.

주제

- IP 주소 문제
- 자격 증명 문제

IP 주소 문제

커넥터는 커넥터 설정 중 제공된 vCenter 엔드포인트 형식이 잘못되거나 유효하지 않을 경우, vCenter 서버가 현재 중지되고 연결되지 않을 경우 비정상 상태가 될 수 있습니다. 이 경우 vCenter 연결에 대한 정보 보기를 선택하면 “vCenter Server의 작동 상태를 확인하거나 설정 편집을 선택하여 vCenter 엔드포인트를 업데이트하십시오”라는 메시지가 포함된 대화 상자가 나타납니다.

다음 절차는 IP 주소 문제를 해결하도록 도움을 줄 수 있습니다.

1. 커넥터 콘솔에서(`https://`*`ip_address_of_connector`*), 설정 편집을 선택합니다.
2. 왼쪽 탐색 창에서 5단계: 검색 커넥터 설정을 선택합니다.
3. vCenter 자격 증명 구성에서 vCenter 호스트 IP 주소를 기록합니다.
4. `ping`또는 `traceroute` 같은 별도의 명령줄 도구를 사용하여 연결된 vCenter 서버가 활성 상태이고 커넥터 VM에서 IP에 연결할 수 있는지 확인합니다.
   - IP 주소가 잘못되었고 vCenter 서비스가 활성 상태라면, IP 주소를 커넥터 콘솔에서 업데이트한 뒤 다음을 선택합니다.
   - IP 주소가 정확하지만 vCenter 서버가 비활성 상태라면 활성화하십시오.
   - IP 주소가 정확하지만 vCenter 서버가 활성 상태라면, 방화벽 문제로 인해 수신 네트워크 연결이 차단되는지 확인합니다. 그렇다면 방화벽 설정을 업데이트해 커넥터 VM의 수신 연결을 허용합니다.

자격 증명 문제

커넥터는 커넥터 설정 중 제공된 vCenter 사용자 자격 증명이 유효하지 않거나 vCenter 읽기 및 보기 계정 권한이 없는 경우 비정상 상태가 될 수 있습니다. 이 경우 vCenter 연결에 대한 정보 보기를 선택하면 “읽기 및 보기 권한이 있는 계정의 vCenter 사용자 이름과 암호를 업데이트하려면 설정 편집을 선택하십시오.” 라는 메시지가 포함된 대화 상자가 나타납니다.

다음 절차는 자격 증명 문제를 해결하도록 도움을 줄 수 있습니다. 사전 조건으로 vCenter 서버 상에서 읽기 및 보기 계정 권한이 있는 vCenter 사용자가 생성되었는지 확인합니다.

1. 커넥터 콘솔에서(`https://`*`ip_address_of_connector`*), 설정 편집을 선택합니다.
2. 왼쪽 탐색 창에서 5단계: 검색 커넥터 설정을 선택합니다.
3. vCenter 자격 증명 구성에서, 읽기 및 보기 권한이 있는 자격 증명을 제공함으로써 vCenter 사용자 이름 및 vCenter 암호를 업데이트합니다.
4. 다음을 선택해 설정을 완료합니다.

독립형 ESX 호스트 지원

디스커버리 커넥터는 독립형 ESX 호스트를 지원하지 않습니다. ESX 호스트는 vCenter Server 인스턴스의 일부여야 합니다.

커넥터 문제에 대한 추가 지원 받기

문제가 발생하여 도움이 필요한 경우 AWS Support에 문의하세요. 연락을 받거나, 커넥터 로그를 보내달라는 요청을 받게 될 것입니다. 다음 방법으로 로그를 입수할 수 있습니다.

- AWS 에이전트리스 디스커버리 커넥터 콘솔에 다시 로그인하고 로그 번들 다운로드를 선택합니다.
- 로그 번들 다운로드가 완료되면, AWS Support의 지시에 따라 보냅니다.

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