사용자 가이드

AWS 애플리케이션 검색 서비스

AWS 애플리케이션 검색 서비스: 사용자 가이드

Table of Contents

AWS Application Discovery Service란 무엇인가요?

AWS Application Discovery Service 는 온프레미스 서버 및 데이터베이스에 대한 사용량 및 구성 데이터를 수집하여 AWS 클라우드로의 마이그레이션을 계획하는 데 도움이 됩니다. Application Discovery Service는 AWS Migration Hub 및 AWS Database Migration Service Fleet Advisor와 통합됩니다. Migration Hub는 마이그레이션 상태 정보를 단일 콘솔로 집계하므로 마이그레이션 추적을 간소화합니다. 검색된 서버를 보고 애플리케이션으로 그룹화한 다음 홈 리전의 Migration Hub 콘솔에서 각 애플리케이션의 마이그레이션 상태를 추적할 수 있습니다. DMS Fleet Advisor를 사용하여 데이터베이스 워크로드의 마이그레이션 옵션을 평가할 수 있습니다.

검색된 모든 데이터는 AWS Migration Hub 홈 리전에 저장됩니다. 따라서 검색 및 마이그레이션 활동을 수행하기 전에 Migration Hub 콘솔에서 또는 CLI 명령을 사용하여 홈 리전을 설정해야 합니다. Microsoft Excel 또는 AWS Amazon Athena 및 Amazon QuickSight와 같은 분석 도구에서 분석을 위해 데이터를 내보낼 수 있습니다.

Application Discovery Service APIs 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 리전에 저장되므로 검색 프로세스를 시작하기 AWS Migration Hub 전에 홈 리전을에 설정해야 합니다. 홈 리전 작업에 대한 자세한 내용은 홈 리전을 참조하세요.

Application Discovery Service는 온프레미스 서버에 대한 검색 및 데이터 수집을 수행하는 세 가지 방법을 제공합니다.

- VMware vCenter를 통해 Application Discovery Service Agentless Collector(Agentless Collector)(OVA 파일)를 배포하여 에이전트 없는 검색을 수행할 수 있습니다. Agentless Collector를 구성한 후에는 vCenter와 연결된 가상 머신(VMs) 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 데이터베이스에 대한 사용률 데이터를 수집하여 CPU, RAM 및 디스크 I/O와 같은 지표의 평균 및 최대 사용률을 제공합니다.

- 에이전트 기반 검색은 각 VMs 및 물리적 서버에 AWS Application Discovery Agent(Discovery Agent)를 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.
- 파일 기반 가져오기를 사용하면 Agentless Collector 또는 Discovery Agent를 사용하지 않고도 온프레미스 환경의 세부 정보를 Migration Hub로 직접 가져올 수 있으므로 가져온 데이터에서 직접 마이그레이션 평가 및 계획을 수행할 수 있습니다. 수집된 데이터는 제공된 데이터에 따라 달라집니다.

Application Discovery Service는 AWS 파트너 네트워크(APN) 파트너의 애플리케이션 검색 솔루션과 통합됩니다. 이러한 타사 솔루션은 에이전트리스 수집기 또는 검색 에이전트를 사용하지 않고도 온프레미스 환경에 대한 세부 정보를 Migration Hub로 직접 가져오는 데 도움이 될 수 있습니다. 타사 애플리케이션 검색 도구는 AWS Application Discovery Service를 쿼리할 수 있으며 퍼블릭 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.

VMware 검색

VMware vCenter 환경에서 실행 중인 가상 머신(VMs)이 있는 경우 Agentless Collector를 사용하여 각 VM에 에이전트를 설치하지 않고도 시스템 정보를 수집할 수 있습니다. 대신이 온프레미스 어플라이언스를 vCenter에 로드하고 모든 호스트와 VMs을 검색할 수 있도록 허용합니다.

Agentless Collector는 사용 중인 운영 체제에 관계없이 vCenter에서 실행되는 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. 따라서이 수준의 세부 정보가 필요하고 마이그레이션 계획을 지원하기 위해 기존 VMs 중 일부를 자세히 살펴보려는 경우 필요에 따라 Discovery Agent를 설치할 수 있습니다.

또한 VMware에서 호스팅되는 VMs의 경우 Agentless Collector와 Discovery Agent를 모두 사용하여 동시에 검색을 수행할 수 있습니다. 각 검색 도구가 수집할 정확한 데이터 유형에 대한 자세한 내용은 섹션을 참조하세요VMware vCenter Agentless Collector 데이터 수집 모듈 사용.

데이터베이스 검색

온프레미스 환경에 데이터베이스 및 분석 서버가 있는 경우 Agentless Collector를 사용하여 이러한 서버를 검색하고 인벤토리를 생성할 수 있습니다. 그런 다음 환경의 각 컴퓨터에 Agentless Collector를 설치할 필요 없이 각 데이터베이스 서버에 대한 성능 지표를 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 모듈은 주기적으로 쿼리를 실행하여 데이터베이스 및 분석 서버의 CPU, 메모리 및 디스크 용량에 대한 실제 사용률 지표를 수집합니다. 수집된 지표에 대한 자세한 내용은 섹션을 참조하세요데이터베이스 및 분석 모듈에서 수집한 데이터.

Agentless Collector가 환경에서 데이터 수집을 완료한 후 AWS DMS 콘솔을 사용하여 추가 분석을 수행하고 마이그레이션을 계획할 수 있습니다. 예를 들어에서 최적의 마이그레이션 대상을 선택하려면 소스 데이터베이스에 대한 대상 권장 사항을 생성할 AWS 클라우드수 있습니다. 자세한 내용은 데이터베이스 및 분석 데이터 수집 모듈 사용 단원을 참조하십시오.

Agentless Collector와 Discovery Agent 비교

다음 표에서는 Application Discovery Service에서 지원하는 데이터 수집 방법을 빠르게 비교합니다.

	에이전트리스 수집기	Discovery Agent	Migration Hub 템플릿	RVTools 내보내기
Supported server types				
VMware 가상 머신	예	예	Yes	Yes
물리적 서버	아니요	예	Yes	Yes
Deployment				
서버 당	아니요	예	N/A	No
vCenter 당	예	아니요	N/A	Yes
동일한 네트워크의 데이터 센터당	아니요	아니요	N/A	아니요
Collected data				
서버 프로파일(정적 구성) 데이터	Yes	Yes	Yes	Yes

	에이전트리스 수집기	Discovery Agent	Migration Hub 템플릿	RVTools 내보내기
Hypervisor의 서버 사용률 지표(CPU, RAM 등)	Yes	Yes	Yes	No
서버의 서버 사용률 지표(CPU, RAM 등)	Yes	Yes	Yes	No
서버 네트워크 연결(TCP만 해당)	Yes	Yes	No	No
실행 중인 프로세스	No	Yes	No	No
수집 간격	-60 minutes	-15 seconds	Single snapshot	Single snapshot
Server data use cases				
Migration Hub에서 서버 데이터 보기	Yes	Yes	Profile only	No
서버 프로파일을 기반으로 Amazon EC2 권장 사항 생성	Yes	Yes	Yes	Yes
사용률 데이터를 기반으로 Amazon EC2 권장 사항 생성	Yes	Yes	Yes	No
최신 사용률 스냅샷 데이터 내보내기	Yes	Yes	Yes	No

	에이전트리스 수집기	Discovery Agent	Migration Hub 템플릿	RVTools 내보내기
시계열 사용률 데이터 내보내기	No	Yes	No	No
Network data use cases				
Migration Hub의 시각화	Yes	Yes	No	No
추가 탐색을 위해 Amazon Athena로 내보내기	No	Yes	No	No
CSV 파일로 내보내기	No	Yes	No	No
Database use cases				
데이터베이스 서버 프로파일(정적 구성) 데이터	Yes	No	No	No
지원되는 데이터베이스 엔진	Oracle, SQL Server, MySQL, PostgreSQL	None	None	None
데이터베이스 스키마 복잡성 및 중복	Yes	No	No	No
데이터베이스 스키마 객체	Yes	No	No	No
Platform support				

	에이전트리스 수집기	Discovery Agent	Migration Hub 템플릿	RVTools 내보내기
지원되는 운영 체제	VMware 센터 v5.5 이상 버전에서 실행되는 모든 OS	모든 Linux 또는 Windows 서버	모든 Linux 또는 Windows 서버	모든 Linux 서버, Windows 서버 또는 VMware v5.5 이상 버전

가정

Application Discovery Service를 사용하려면 다음과 같이 가정합니다.

- 에 가입했습니다 AWS. 자세한 내용은 Application Discovery Service 설정 단원을 참조하십시오.
- Migration Hub 홈 리전을 선택했습니다. 자세한 내용은 홈 리전에 대한 설명서를 참조하세요.

예상되는 결과는 다음과 같습니다.

- Migration Hub 홈 리전은 Application Discovery Service가 검색 및 계획 데이터를 저장하는 유일한 리전입니다.
- 검색 에이전트, 커넥터 및 가져오기는 선택한 Migration Hub 홈 리전에서만 사용할 수 있습니다.
- Application Discovery Service를 사용할 수 있는 AWS 리전 목록은 섹션을 참조하세요Amazon Web Services 일반 참조.

Application Discovery Service 설정

AWS Application Discovery Service 를 처음 사용하기 전에 다음 작업을 완료합니다.

Amazon Web Services 가입

IAM 사용자 생성

Migration Hub 콘솔에 로그인하고 홈 리전 선택

Amazon Web Services 가입

이 없는 경우 다음 단계를 AWS 계정완료하여 생성합니다.

에 가입하려면 AWS 계정

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

   등록 절차 중 전화 또는 텍스트 메시지를 받고 전화 키패드로 확인 코드를 입력하는 과정이 있습니다.

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

IAM 사용자 생성

AWS 계정을 생성하면 계정의 모든 AWS 서비스 및 리소스에 대한 완전한 액세스 권한이 있는 단일 로그인 자격 증명이 생성됩니다. 이 자격 증명을 AWS 계정 루트 사용자라고 합니다. 계정을 생성하는 데 사용한 이메일 주소와 암호를 AWS Management Console 사용하여에 로그인하면 계정의 모든 AWS 리소스에 대한 완전한 액세스 권한을 얻을 수 있습니다.

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

관리 사용자를 생성하는 것 외에도 관리자가 아닌 IAM 사용자를 생성해야 합니다. 다음 주제에서는 두 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

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

IAM 비관리 사용자 생성

비관리형 IAM 사용자를 생성할 때 보안 모범 사례 최소 권한 부여를 따르고 사용자에게 최소 권한을 부여합니다.

IAM 관리형 정책을 사용하여 비관리형 IAM 사용자의 Application Discovery Service에 대한 액세스 수준을 정의합니다. Application Discovery Service 관리형 정책에 대한 자세한 내용은 섹션을 참조하세요AWS 에 대한 관리형 정책 AWS Application Discovery Service.

관리자가 아닌 IAM 사용자를 생성하려면

1. 에서 IAM 콘솔로 AWS Management Console이동합니다.
2. IAM 사용 설명서의 AWS 계정에서 IAM 사용자 생성에 설명된 대로 콘솔을 사용하여 사용자를 생성하는 지침에 따라 관리자가 아닌 IAM 사용자를 생성합니다.

   IAM 사용 설명서의 지침을 따르는 동안:

   - 액세스 유형을 선택하는 단계에서 프로그래밍 방식 액세스를 선택합니다. 권장되지는 않지만 AWS 콘솔에 액세스하는 데 동일한 IAM 사용자 자격 증명을 사용하려는 경우에만 관리 AWS 콘솔 액세스를 선택합니다.

- 권한 설정 페이지의 단계에서 기존 정책을 사용자에게 직접 연결 옵션을 선택합니다. 그런 다음 정책 목록에서 Application Discovery Service에 대한 관리형 IAM 정책을 선택합니다. Application Discovery Service 관리형 정책에 대한 자세한 내용은 섹션을 참조하세요AWS 에 대한 관리형 정책 AWS Application Discovery Service.
- 사용자의 액세스 키(액세IDs 및 보안 액세스 키)를 보는 단계에서는 사용자의 새 액세스 키 ID 및 보안 액세스 키를 안전하고 안전한 장소에 저장하는 방법에 대한 중요 참고 사항의 지침을 따릅니다.

Migration Hub 콘솔에 로그인하고 홈 리전 선택

에 사용 중인 AWS 계정에서 AWS Migration Hub 홈 리전을 선택해야 합니다 AWS Application Discovery Service.

홈 리전을 선택하려면

1. AWS 계정을 사용하여에 로그인 AWS Management Console 하고 https://console.aws.amazon.com/migrationhub/ Migration Hub 콘솔을 엽니다.
2. Migration Hub 콘솔 탐색 창에서 설정을 선택하고 홈 리전을 선택합니다.

   Migration Hub 데이터는 검색, 계획 및 마이그레이션 추적을 위해 홈 리전에 저장됩니다. 자세한 내용은 Migration Hub 홈 리전을 참조하세요.

AWS 애플리케이션 검색 에이전트

AWS Application Discovery Agent(Discovery Agent)는 검색 및 마이그레이션을 대상으로 하는 온프레미스 서버 및 VMs에 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**
>
> Discovery Agent를 배포하기 전에 Migration Hub 홈 리전을 선택해야 합니다. 홈 리전에 에이전트를 등록해야 합니다.

Discovery Agent는 로컬 환경에서 실행되며 루트 권한이 필요합니다. Discovery Agent를 시작하면 홈 리전과 안전하게 연결되고 Application Discovery Service에 등록됩니다.

- 예를 들어 `eu-central-1`가 홈 리전인 경우 Application Discovery Service`arsenal-discovery.`*`eu-central-1`*`.amazonaws.com`에 등록됩니다.
- 또는 필요에 따라 us-west-2를 제외한 다른 모든 리전으로 홈 리전을 대체합니다.
- `us-west-2`가 홈 리전인 경우 Application Discovery Service`arsenal.us-west-2.amazonaws.com`에 등록됩니다.

작동 방법

등록 후 에이전트는 호스트 또는 호스트가 있는 VM에 대한 데이터 수집을 시작합니다. 에이전트는 구성 정보를 위해 15분 간격으로 Application Discovery Service를 ping합니다.

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 포인트는에서 이러한 서버를 실행하는 데 드는 비용을 결정 AWS 하고 마이그레이션을 계획하는 데 도움이 될 수 있습니다.

데이터는 TLS(전송 계층 보안) 암호화를 사용하여 Discovery Agents에서 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 Agent 설치를 다운로드하고 시작하기 전에에서 필요한 모든 사전 조건을 읽어야 합니다. Discovery Agent의 사전 조건

Discovery Agent에서 수집한 데이터

AWS Application Discovery Agent(Discovery Agent)는 온프레미스 서버 및 VMs. Discovery Agent는 시스템 구성, 시계열 사용률 또는 성능 데이터, 프로세스 데이터 및 전송 제어 프로토콜(TCP) 네트워크 연결을 수집합니다. 이 섹션에서는 수집된 데이터에 대해 설명합니다.

Discovery Agent 수집 데이터의 테이블 범례:

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

데이터 필드	설명
agentAssignedProcessId*	에이전트가 검색한 프로세스의 프로세스 ID
agentId	에이전트의 고유 ID
+agentProvidedTimeStamp*	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

데이터 필드	설명
destinationPort*	데이터/요청이 전송되는 포트 번호
패밀리*	라우팅 그룹 프로토콜
freeRAM(MB)	애플리케이션에서 바로 사용할 수 있는 MB 단위의 무료 RAM과 캐시된 RAM
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
totalCpuUsagePct	폴링 기간 동안 호스트의 CPU 사용량(%)

데이터 필드	설명
totalDiskBytesReadPerSecond(Kbps)	모든 디스크에서 초당 읽는 총 킬로비트
totalDiskBytesWrittenPerSecond(Kbps)	모든 디스크에서 초당 기록된 총 킬로비트
totalDiskFreeSize(GB)	사용 가능한 디스크 공간(GB)
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
totalNumLogicalProcessors*	물리적 코어 수 합계와 각 코어에서 실행할 수 있는 스레드의 수를 곱한 값
totalNumNetworkCards	서버의 네트워크 카드 수 합계
totalRAM(MB)	호스트에서 사용할 수 있는 총 RAM
transportProtocol*	사용하고 있는 전송 프로토콜 유형

Discovery Agent의 사전 조건

다음은 AWS Application Discovery Agent(Discovery Agent)를 성공적으로 설치하기 전에 수행해야 하는 사전 조건과 작업입니다.

- Discovery Agent 설치를 시작하기 전에 AWS Migration Hub 홈 리전을 설정해야 합니다.
- 설치된 에이전트의 버전이 1.x이면 제거한 후 최신 버전을 설치해야 합니다.

- 에이전트가 설치 중인 호스트가 Linux를 실행하는 경우 호스트가 최소한 Intel i686 CPU 아키텍처(P6 마이크로 아키텍처라고도 함)를 지원하는지 확인합니다.
- 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 11SP4, 12SP5, 15SP5

  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 인 경우 `eu-central-1`를 사용합니다. `https://arsenal-discovery.eu-central-1.amazonaws.com:443`
- 자동 업그레이드가 작동하려면 홈 리전에서 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**
>
> Discovery Agent에는 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.

Discovery Agent 설치

이 페이지에서는 Linux 및 Microsoft Windows에 Discovery Agent를 설치하는 방법을 다룹니다.

Linux에 Discovery Agent 설치

Linux에서 다음 절차를 완료합니다. 이 절차를 시작하기 전에 Migration Hub 홈 리전이 설정되어 있는지 확인합니다.

> **Note**
>
> 최신이 아닌 Linux 버전을 사용하고 있다면 이전 Linux 플랫폼에 대한 고려 사항를 참조하십시오.

데이터 센터에 AWS Application Discovery Agent를 설치하려면

1. Linux 기반 서버 또는 VM에 로그인하고 에이전트 구성 요소가 포함된 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-region.amazonaws.com/aws-discovery-agent.region/linux/latest/aws-discovery-agent.tar.gz
   ```

   b. Migration Hub 콘솔에서를 다운로드하려면 다음을 수행합니다.

      i. 에 로그인 AWS Management Console 하고 https://console.aws.amazon.com/migrationhub/ Migration Hub 콘솔을 엽니다.

      ii. 왼쪽 탐색 페이지의 검색에서 도구를 선택합니다.

iii. AWS Discovery Agent 상자에서 에이전트 다운로드를 선택한 다음 Linux용 다운로드를 선택합니다. 그러면 즉시 다운로드가 시작됩니다.

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

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

```
curl -o ./discovery.gpg https://s3.region.amazonaws.com/aws-discovery-agent.region/
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
Discovery Agent 설치	에이전트를 설치하려면 다음 예제와 같이 에이전트 설치 명령을 실행합니다. 이 예제에서는 *your-home-region* 을 홈 리전의 이름으로 바꾸고, *aws-access-key-id* 를 액세스 키 ID로 바꾸고, *aws-secret-access-key* 를 보안 액세스 키로 바꿉니다. `sudo bash install -r your-home-region -k aws-access-key-id -s aws-secret-access-key`

원하는 작업	수행할 작업
	기본적으로 에이전트는 업데이트를 사용할 수 있게 되면 자동으로 다운로드하고 적용합니다. 이 기본 구성을 사용하는 것이 좋습니다. 하지만 에이전트가 업데이트를 자동으로 다운로드하고 적용하지 않도록 하려면 에이전트 설치 명령을 실행할 때 `-u false` 파라미터를 포함하세요.
(선택 사항) Discovery Agent 설치 및 투명하지 않은 프록시 구성	투명하지 않은 프록시를 구성하려면 에이전트 설치 명령에 다음 파라미터를 추가합니다. • -e 프록시 암호입니다. • -f 프록시 포트 번호입니다. • -g 프록시 체계입니다. • -i 프록시 사용자 이름입니다. 다음은 투명한 프록시 파라미터를 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 경우 `-e` 및 `-i` 파라미터를 제외합니다. 예제 설치 명령은를 사용하며https, 프록시가 HTTP를 사용하는 경우 `-g` 파라미터 값에 `http`를 지정합니다.

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 인 경우 `eu-central-1`를 사용합니다. `https://arsenal-discovery.eu-central-1.amazonaws.com:443`

이전 Linux 플랫폼에 대한 고려 사항

SUSE 10, CentOS 5 및 RHEL 5와 같은 일부 이전 Linux 플랫폼은 수명이 다 되었거나 최소한의 지원만 받을 수 있습니다. 이러한 플랫폼은 에이전트 업데이트 스크립트가 설치 패키지를 다운로드하지 못하게 하는 out-of-date 암호 제품군으로 인해 어려움을 겪을 수 있습니다.

Curl

Application Discovery 에이전트는 AWS 서버와의 보안 통신을 `curl` 위해가 필요합니다. `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

기존 Linux 시스템은 인터넷 연결을 보호하는 데 중요한 최신이 아닌 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 파라미터가 모두 설치 스크립트로 전달됩니다.

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

Microsoft Windows에 Discovery Agent 설치

Microsoft Windows에 에이전트를 설치하려면 다음 절차를 완료하세요. 이 절차를 시작하기 전에 Migration Hub 홈 리전이 설정되어 있는지 확인합니다.

데이터 센터에 AWS Application Discovery Agent를 설치하려면

1. Windows 에이전트 설치 관리자를 다운로드하되 Windows 내에서 설치 관리자를 실행하려면 두 번 클릭하지 마세요.

   > **Important**
   >
   > Windows 내에서 설치 관리자를 실행하려면 두 번 클릭하지 마십시오. 설치가 실패합니다. 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 관리자가 호스트에서 Visual C++ x86 런타임 버전을 감지하지 못하면 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
Discovery Agent 설치	에이전트를 설치하려면 다음 예제와 같이 에이전트 설치 명령을 실행합니다. 예제에서 *your-home-region* 를 홈 리전의 이름으로,를 액세스 키 ID*aws-access-key-id* 로,를 보안 액세스 키*aws-secret-access-key* 로 바꿉니다. 선택적으로 *C:\install-location* INSTALLLOCATION 파라미터의 폴더 경로를 지정하여 에이전트 설치 위치를 설정할 수 있습니다. 예: `INSTALLLOCATION="` *C:\install-location* ". 결과 폴더 계층 구조는 [INSTALLLOCATION path]\AWS

원하는 작업	수행할 작업
	Discovery입니다. 기본적으로 설치 위치는 `Program Files` 폴더입니다. 선택적으로 `LOGANDCONFIGLOCATION` 를 사용하여 에이전트 로그 폴더 및 구성 파일의 기본 디렉터리(ProgramData)를 재정의할 수 있습니다. 결과 폴더 계층 구조는 입니다[*`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 업데이트를 사용할 수 있게 되면 자동으로 다운로드하고 적용합니다. 이 기본 구성을 사용하는 것이 좋습니다. 그러나 에이전트가 업데이트를 자동으로 다운로드하고 적용하지 않도록 하려면 에이전트 설치 명령을 실행할 때 다음 파라미터를 포함하세요. `AUTO_UPDATE=false` **Warning** 자동 업그레이드를 비활성화하면 최신 보안 패치가 설치되지 않습니다.

원하는 작업	수행할 작업
(선택 사항) Discovery Agent 설치 및 투명하지 않은 프록시 구성	투명하지 않은 프록시를 구성하려면 에이전트 설치 명령에 다음 퍼블릭 속성을 추가합니다. • PROXY_HOST – 프록시 호스트의 이름 • PROXY_SCHEME – 프록시 체계 • PROXY_PORT – 프록시 포트 번호 • PROXY_USER – 프록시 사용자 이름 • PROXY_PASSWORD – 프록시 사용자 암호 다음은 투명한 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 생략합니다. 예제 설치 명령은를 사용합니다https. 프록시가 HTTP를 사용하는 경우 PROXY_SCHEME 값에 http를 지정합니다.

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

   예를 들어 홈 리전이 인 경우 다음을 사용합니다eu-central-1. 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 암호화 방식으로 서명합니다. Windows Server SHA2-signed 자동 업데이트의 경우 호스트에 SHA2 서명 인증을 지원하는 핫픽스가 설치되어 있는지 확인합니다. SP2 Microsoft의 최신 지원 핫픽스는 Windows Server 2008 SP2에서 SHA2 인증을 지원하는 데 도움이 됩니다. SP2

> **Note**
>
> Windows 2003에 대한 SHA256 지원 핫픽스는 더 이상 Microsoft에서 공개적으로 사용할 수 없습니다. 이러한 수정 사항이 Windows 2003 호스트에 아직 설치되지 않은 경우 수동 업그레이드가 필요합니다.

업그레이드를 수동으로 수행하려면

1. Windows Agent Updater를 다운로드합니다.
2. 관리자로 명령 프롬프트를 엽니다.
3. 업데이트 프로그램이 저장된 위치로 이동합니다.
4. 다음 명령을 실행합니다.

```
AWSDiscoveryAgentUpdater.exe /Q
```

Discovery Agent 프로세스 관리

이 페이지에서는 Linux 및 Microsoft Windows에서 Discovery Agent를 관리하는 방법을 다룹니다.

Linux에서 Discovery Agent 프로세스 관리

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

systemd

Application Discovery Agent에 대한 관리 명령

Task	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

Application Discovery Agent에 대한 관리 명령

Task	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

Application Discovery Agent에 대한 관리 명령

Task	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`

Microsoft Windows에서 Discovery Agent 프로세스 관리

Windows Server Manager Services 콘솔을 통해 시스템 수준에서 Discovery Agent의 동작을 관리할 수 있습니다. 다음은 그 방법을 설명하고 있는 테이블입니다.

Task	서비스 이름	서비스 상태/작업
에이전트가 실행 중인지 확인	AWS 검색 에이전트 AWS Discovery Updater	시작됨
에이전트 시작	AWS 검색 에이전트 AWS Discovery Updater	시작을 선택합니다
에이전트 중지	AWS 검색 에이전트 AWS Discovery Updater	중지를 선택합니다.
에이전트 다시 시작	AWS 검색 에이전트 AWS Discovery Updater	다시 시작를 선택합니다.

Discovery Agent 제거

이 페이지에서는 Linux 및 Microsoft Windows에서 Discovery Agent를 제거하는 방법을 다룹니다.

Linux에서 Discovery Agent 제거

이 섹션에서는 Linux에서 Discovery Agent를 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
```

Microsoft Windows에서 Discovery Agent 제거

이 섹션에서는 Microsoft Windows에서 Discovery Agent를 제거하는 방법을 설명합니다.

Windows에서 검색 에이전트 제거

1. Windows에서 제어판을 엽니다.
2. Programs(프로그램)을 선택합니다.
3. Programs and Features(프로그램 및 기능)을 선택합니다.
4. AWS Discovery Agent를 선택합니다.

5. 제거를 선택합니다.

> **Note**
>
> 에이전트를 제거한 후 다시 설치하도록 선택한 경우 /repair 및 /norestart 옵션을 사용하여 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
```

> **Note**
>
> .exe 파일이 서버에 있는 경우 다음 명령을 사용하여 서버에서 에이전트를 완전히 제거할 수 있습니다. 이 명령을 사용하여를 제거하는 경우 에이전트를 다시 설치할 때 /repair 및 /norestart 옵션을 사용할 필요가 없습니다.
>
> ```
> .\AWSDiscoveryAgentInstaller.exe /quiet /uninstall
> ```

Discovery Agent 데이터 수집 시작 및 중지

Discovery Agent를 배포하고 구성한 후 데이터 수집이 중지되면 다시 시작할 수 있습니다. 의 단계에 따라 또는를 통해 API 호출을 수행하여 콘솔을 통해 데이터 수집을 시작AWS Migration Hub 콘솔에서 데이터 수집기 시작 및 중지하거나 중지할 수 있습니다 AWS CLI.

를 설치하고 데이터 수집을 AWS CLI 시작하거나 중지하려면

1. 아직 설치하지 않은 경우 OS 유형(Windows 또는 Mac/Linux)에 AWS CLI 적합한를 설치합니다. 지침은 AWS Command Line Interface 사용 설명서를 참조하세요.
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. 와 같이 기본 리전 이름에 홈 리전을 입력합니다*us-west-2*. (이 예에서는 `us-west-2`가 홈 리전이라고 가정합니다.)
   d. 기본 출력 형식에 `text`를 입력합니다.
3. 데이터 수집을 중지하거나 시작하려는 에이전트의 ID를 찾으려면 다음 명령을 입력합니다.

```
aws discovery describe-agents
```

4. 에이전트가 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>
```

Discovery Agent 문제 해결

이 페이지에서는 Linux 및 Microsoft Windows의 Discovery Agent 문제 해결을 다룹니다.

Linux의 Discovery Agent 문제 해결

Linux에서 Discovery Agent를 설치하거나 사용하는 동안 문제가 발생하면 로깅 및 구성에 대한 다음 지침을 참조하세요. 에이전트 또는 Application Discovery Service에 대한 연결과 관련된 잠재적 문제를 해결하는 데 도움이 되는 경우 AWS Support는 종종 이러한 파일을 요청합니다.

- 로그 파일

  Discovery Agent의 로그 파일은 다음 디렉터리에 있습니다.

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

로그 파일의 이름은 기본 데몬, 자동 업그레이드 프로그램 또는 설치 관리자에 의해 생성되는지 여부를 나타내도록 지정됩니다.

- 구성 파일

  Discovery Agent 버전 2.0.1617.0 이상의 구성 파일은 다음 디렉터리에 있습니다.

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

  2.0.1617.0 이전 버전의 Discovery Agent에 대한 구성 파일은 다음 디렉터리에 있습니다.

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

- 이전 버전의 Discovery Agent를 제거하는 방법에 대한 지침은 섹션을 참조하세요Discovery Agent의 사전 조건.

Microsoft Windows의 Discovery Agent 문제 해결

Microsoft Windows에서 AWS Application Discovery Agent를 설치하거나 사용하는 동안 문제가 발생하는 경우 로깅 및 구성에 대한 다음 지침을 참조하세요.는 에이전트 또는 Application Discovery Service에 대한 연결과 관련된 잠재적 문제를 해결하는 데 도움이 될 때 이러한 파일을 요청하는 경우가 AWS Support많습니다.

- 설치 로깅

  경우에 따라 에이전트 설치 명령이 실패하는 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 파일의 이름은 기본 서비스, 자동 업그레이드 또는 설치 관리자에 의해 생성되었는지 여부를 나타내도록 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 섹션을 참조하세요Discovery Agent의 사전 조건.

Application Discovery Service Agentless Collector

Application Discovery Service Agentless Collector(Agentless Collector)는 서버 프로파일 정보(예: OS, CPUs 수, RAM 양), 데이터베이스 메타데이터, 사용률 지표, 온프레미스 서버 간 네트워크 트래픽에 대한 데이터를 포함하여 온프레미스 환경에 대한 에이전트 없는 방법을 통해 정보를 수집하는 온프레미스 애플리케이션입니다. OVA(Open Virtualization Archive) 파일을 사용하여 Agentless Collector를 VMware vCenter Server 환경의 VM(가상 머신)으로 설치합니다.

Agentless Collector에는 여러 에이전트 없는 수집 방법을 사용할 수 있는 모듈식 아키텍처가 있습니다. Agentless Collector는 VMware VMs 데이터베이스 및 분석 서버에서 데이터를 수집하기 위한 모듈을 제공합니다. 또한 온프레미스 서버 간의 네트워크 트래픽에 대한 데이터를 수집하기 위한 모듈도 제공합니다.

Agentless Collector는 온프레미스 서버 및 데이터베이스에 대한 사용 및 구성 데이터와 온프레미스 서버 간의 네트워크 트래픽에 대한 데이터를 수집하여 AWS Application Discovery Service (Application Discovery Service)에 대한 데이터 수집을 지원합니다.

Application Discovery Service는 마이그레이션 상태 정보를 단일 콘솔로 집계할 때 마이그레이션 추적을 간소화하는 AWS Migration Hub서비스와 통합됩니다. 검색된 서버를 보고, Amazon EC2 권장 사항을 얻고, 네트워크 연결을 시각화하고, 서버를 애플리케이션으로 그룹화한 다음 홈 리전의 Migration Hub 콘솔에서 각 애플리케이션의 마이그레이션 상태를 추적할 수 있습니다.

Agentless Collector 데이터베이스 및 분석 데이터 수집 모듈은 AWS Database Migration Service ()와 통합됩니다AWS DMS. 이 통합은 로의 마이그레이션을 계획하는 데 도움이 됩니다 AWS 클라우드. 데이터베이스 및 분석 데이터 수집 모듈을 사용하여 환경에서 데이터베이스 및 분석 서버를 검색하고 로 마이그레이션하려는 서버 인벤토리를 구축할 수 있습니다 AWS 클라우드. 이 데이터 수집 모듈은 CPU, 메모리 및 디스크 용량의 데이터베이스 메타데이터 및 실제 사용률 지표를 수집합니다. 이러한 지표를 수집한 후 AWS DMS 콘솔을 사용하여 소스 데이터베이스에 대한 대상 권장 사항을 생성할 수 있습니다.

Agentless Collector의 사전 조건

다음은 Application Discovery Service Agentless Collector(Agentless Collector)를 사용하기 위한 사전 조건입니다.

- 하나 이상의 AWS 계정.

- AWS Migration Hub 홈 리전이 설정된 AWS 계정은 섹션을 참조하세요Migration Hub 콘솔에 로그인하고 홈 리전 선택. Migration Hub 데이터는 검색, 계획 및 마이그레이션 추적을 위해 홈 리전에 저장됩니다.
- AWS 관리형 정책를 사용하도록 설정된 AWS 계정 IAM 사용자입니다`AWSApplicationDiscoveryAgentlessCollectorAccess`. 데이터베이스 및 분석 데이터 수집 모듈을 사용하려면이 IAM 사용자가 두 개의 고객 관리형 IAM 정책 `DMSCollectorPolicy` 및 도 사용해야 합니다`FleetAdvisorS3Policy`. 자세한 내용은 Application Discovery Service Agentless Collector 배포 단원을 참조하십시오. IAM 사용자는 Migration Hub 홈 리전이 설정된 AWS 계정에서 생성해야 합니다.
- VMware vCenter Server V5.5, V6, V6.5, 6.7 또는 7.0.

> **Note**
>
> Agentless Collector는 이러한 VMware 버전을 모두 지원 VMware 하지만 현재 버전 6.7 및 7.0을 기준으로 테스트합니다.

- VMware vCenter Server 설정의 경우 시스템 그룹에 설정된 읽기 및 보기 권한으로 vCenter 자격 증명을 제공할 수 있는지 확인합니다.
- Agentless Collector를 사용하려면 TCP 포트 443을 통해 여러 AWS 도메인에 아웃바운드 액세스해야 합니다. 이러한 도메인 목록은 섹션을 참조하세요AWS 도메인에 대한 아웃바운드 액세스를 위한 방화벽 구성.
- 데이터베이스 및 분석 데이터 수집 모듈을 사용하려면 Migration Hub 홈 리전으로 AWS 리전 설정한에서 Amazon S3 버킷을 생성합니다. 데이터베이스 및 분석 데이터 수집 모듈은 인벤토리 메타데이터를이 Amazon S3 버킷에 저장합니다. 자세한 내용은 Amazon S3 사용자 안내서의 버킷 생성을 참조하세요.
- Agentless Collector 버전 2에는 ESXi 6.5 이상이 필요합니다.

AWS 도메인에 대한 아웃바운드 액세스를 위한 방화벽 구성

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 리전이 미국 서부(오레곤) 리전, us-west-2 또는 기타 리전인지에 따라 달라집니다.

AWS 계정 홈 리전이 us-west-2인 경우 다음 도메인은 아웃바운드 액세스가 필요합니다.

- `arsenal-discovery.us-west-2.amazonaws.com` - 수집기는이 도메인을 사용하여 필요한 IAM 사용자 자격 증명으로 구성되어 있는지 확인합니다. 수집기는 홈 리전이 us-west-2이므로 수집된 데이터를 전송하고 저장하는 데도 사용합니다.
- `migrationhub-config.us-west-2.amazonaws.com` - 수집기는이 도메인을 사용하여 제공된 IAM 사용자 자격 증명을 기반으로 수집기가 데이터를 전송하는 홈 리전을 결정합니다.
- `api.ecr-public.us-east-1.amazonaws.com` - 수집기는이 도메인을 사용하여 사용 가능한 업데이트를 검색합니다.
- `public.ecr.aws` - 수집기는이 도메인을 사용하여 업데이트를 다운로드합니다.
- `dms.`*`your-migrationhub-home-region`*`.amazonaws.com` - 수집기는이 도메인을 사용하여 AWS DMS 데이터 수집기에 연결합니다.
- `s3.amazonaws.com` - 수집기는이 도메인을 사용하여 데이터베이스 및 분석 데이터 수집 모듈에서 수집한 데이터를 Amazon S3 버킷에 업로드합니다.
- `sts.amazonaws.com` - 수집기는이 도메인을 사용하여 수집기가 구성된 계정을 이해합니다.

다음 도메인은 AWS 계정 홈 리전이가 아닌 경우 아웃바운드 액세스가 필요합니다. **us-west-2**

- `arsenal-discovery.us-west-2.amazonaws.com` - 수집기는이 도메인을 사용하여 필요한 IAM 사용자 자격 증명으로 구성되어 있는지 확인합니다.
- `arsenal-discovery.`*`your-migrationhub-home-region`*`.amazonaws.com` - 수집기는이 도메인을 사용하여 수집된 데이터를 전송하고 저장합니다.
- `migrationhub-config.us-west-2.amazonaws.com` - 수집기는이 도메인을 사용하여 제공된 IAM 사용자 자격 증명을 기반으로 수집기가 데이터를 전송해야 하는 홈 리전을 결정합니다.
- `api.ecr-public.us-east-1.amazonaws.com` - 수집기는이 도메인을 사용하여 사용 가능한 업데이트를 검색합니다.
- `public.ecr.aws` - 수집기는이 도메인을 사용하여 업데이트를 다운로드합니다.
- `dms.`*`your-migrationhub-home-region`*`.amazonaws.com` - 수집기는이 도메인을 사용하여 AWS DMS 데이터 수집기에 연결합니다.
- `s3.amazonaws.com` - 수집기는이 도메인을 사용하여 데이터베이스 및 분석 데이터 수집 모듈에서 수집한 데이터를 Amazon S3 버킷에 업로드합니다.
- `sts.amazonaws.com` - 수집기는이 도메인을 사용하여 수집기가 구성된 계정을 이해합니다.

Agentless Collector를 설정할 때 설정 실패 - 자격 증명을 확인하고 다시 시도하거나 AWS 연결할 수 없음과 같은 오류가 발생할 수 있습니다. 네트워크 설정을 확인하십시오. 이러한 오류는 아웃바운드 액세스가 필요한 AWS 도메인 중 하나에 HTTPS 연결을 설정하려는 Agentless Collector의 시도 실패로 인해 발생할 수 있습니다.

에 대한 연결을 설정할 수 AWS 없는 경우 Agentless Collector는 온프레미스 환경에서 데이터를 수집할 수 없습니다. 연결을 수정하는 방법에 대한 자세한 내용은 섹션을 AWS참조하세요설정 AWS 중에 에이전트리스 수집기 수정에 도달할 수 없음.

Application Discovery Service Agentless Collector 배포

Application Discovery Service Agentless Collector를 배포하려면 먼저 IAM 사용자를 생성하고 수집기를 다운로드해야 합니다. 이 페이지에서는 수집기를 배포하기 위해 취해야 할 단계를 안내합니다.

Agentless Collector에 대한 IAM 사용자 생성

Agentless Collector를 사용하려면에서 사용한 AWS 계정에서 (IAM) 사용자를 생성Migration Hub 콘솔에 로그인하고 홈 리전 선택 AWS Identity and Access Management 해야 합니다. 그런 다음 다음 AWS 관리형 정책 AWSApplicationDiscoveryAgentlessCollectorAccess를 사용하도록이 IAM 사용자를 설정합니다. IAM 사용자를 생성할 때이 IAM 정책을 연결합니다.

데이터베이스 및 분석 데이터 수집 모듈을 사용하려면 두 개의 고객 관리형 IAM 정책을 생성합니다. 이러한 정책은 Amazon S3 버킷 및 API에 AWS DMS 대한 액세스를 제공합니다. 자세한 내용은 IAM 사용 설명서의 고객 관리형 정책 생성을 참조하세요.

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

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

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

```
{
    "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/*"
            ]
        }
    ]
}
```

앞의 예에서를 사전 조건 단계에서 생성한 Amazon S3 버킷의 이름으로 *bucket_name* 바꿉니다.

Agentless Collector와 함께 사용할 비관리형 IAM 사용자를 생성하는 것이 좋습니다. 비관리형 IAM 사용자를 생성할 때는 보안 모범 사례 최소 권한 부여를 따르고 사용자에게 최소 권한을 부여합니다.

Agentless Collector와 함께 사용할 관리자가 아닌 IAM 사용자를 생성하려면

1. 에서에서 홈 리전을 설정하는 데 사용한 AWS 계정을 사용하여 IAM 콘솔로 AWS Management Console이동합니다Migration Hub 콘솔에 로그인하고 홈 리전 선택.
2. IAM 사용 설명서의 AWS 계정에서 IAM 사용자 생성에 설명된 대로 콘솔을 사용하여 사용자를 생성하는 지침에 따라 관리자가 아닌 IAM 사용자를 생성합니다.

   IAM 사용 설명서의 지침을 따르는 동안:

   - 액세스 유형을 선택하는 단계에서 프로그래밍 방식 액세스를 선택합니다. 권장되지는 않지만 AWS 콘솔에 액세스하는 데 동일한 IAM 사용자 자격 증명을 사용하려는 경우에만 관리 AWS 콘솔 액세스를 선택합니다.

- 권한 설정 페이지의 단계에서 기존 정책을 사용자에게 직접 연결 옵션을 선택합니다. 그런 다음 정책 목록에서 AWSApplicationDiscoveryAgentlessCollectorAccess AWS 관리형 정책을 선택합니다.

  그런 다음 DMSCollectorPolicy 및 FleetAdvisorS3Policy 고객 관리형 IAM 정책을 선택합니다.

- 사용자의 액세스 키(액세IDs 및 보안 액세스 키)를 보는 단계에서는 사용자의 새 액세스 키 ID 및 보안 액세스 키를 안전하고 안전한 장소에 저장하는 방법에 대한 중요 참고 사항의 지침을 따릅니다. 에 이러한 액세스 키가 필요합니다에이전트리스 수집기 구성.

  액세스 키를 교체하는 것이 AWS 보안 모범 사례입니다. 키 교체에 대한 자세한 내용은 IAM 사용 설명서의 장기 보안 인증이 필요한 사용 사례에 대해 정기적으로 액세스 키 교체를 참조하세요.

에이전트리스 수집기 다운로드

Application Discovery Service Agentless Collector(Agentless Collector)를 설정하려면 Agentless Collector OVA(Open Virtualization Archive) 파일을 다운로드하여 배포해야 합니다. Agentless Collector는 온프레미스 VMware 환경에 설치하는 가상 어플라이언스입니다. 이 단계에서는 수집기 OVA 파일을 다운로드하는 방법을 설명하고 다음 단계에서는 이를 배포하는 방법을 설명합니다.

수집기 OVA 파일을 다운로드하고 체크섬을 확인하려면

1. vCenter에 VMware 관리자로 로그인하고 Agentless Collector OVA 파일을 다운로드할 디렉터리로 전환합니다.
2. 다음 URL에서 OVA 파일을 다운로드합니다.

   에이전트 없는 수집기 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
```

에이전트리스 수집기 배포

Application Discovery Service Agentless Collector(Agentless Collector)는 온프레미스 VMware 환경에 설치하는 가상 어플라이언스입니다. 이 섹션에서는 VMware 환경에서 다운로드한 OVA(Open Virtualization Archive) 파일을 배포하는 방법을 설명합니다.

Agentless Collector 가상 머신 사양

Agentless Collector version 2

- 운영 체제 - Amazon Linux 2023
- RAM – 16GB
- CPU - 코어 4개
- VMware 요구 사항 - VMware에서 AL2023을 실행하기 위한 VMware 호스트 요구 사항 참조

Agentless Collector version 1

- 운영 체제 - Amazon Linux 2
- RAM – 16GB
- CPU - 코어 4개

다음 절차에서는 VMware 환경에 Agentless Collector OVA 파일을 배포하는 단계를 안내합니다.

Agentless Collector를 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 수집기 OVA 파일을 선택한 다음 마법사를 완료합니다. 서버 관리 대시보드의 프록시 설정이 올바르게 구성되었는지 확인합니다.
   - 명령줄 사용: 명령줄에서 수집기 OVA 파일을 설치하려면 VMware Open Virtualization Format Tool(ovftool)을 다운로드하여 사용합니다. ovftool을 다운로드하려면 OVF 도구 설명서 페이지에서 릴리스를 선택합니다.

다음은 ovftool 명령줄 도구를 사용하여 수집기 OVA 파일을 설치하는 예제입니다.

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

다음은 예제의 ## ### 값을 설명합니다.

- 이름은 Agentless Collector VM에 사용할 이름입니다.
- 데이터 스토어는 vCenter에 있는 데이터 스토어의 이름입니다.
- OVA 파일 이름은 다운로드한 수집기 OVA 파일의 이름입니다.
- 사용자 이름/암호는 vCenter 자격 증명입니다.
- vcenterurl은 vCenter의 URL입니다.
- vi 경로는 VMware ESXi 호스트의 경로입니다.

3. vCenter에서 배포된 Agentless Collector를 찾습니다. VM을 마우스 오른쪽 버튼으로 클릭한 다음 전원, 전원 켜기를 선택합니다.
4. 몇 분 후 수집기의 IP 주소가 vCenter에 표시됩니다. 이 IP 주소를 사용하여 수집기에 연결합니다.

Agentless Collector 콘솔 액세스

다음 절차에서는 Application Discovery Service Agentless Collector(Agentless Collector) 콘솔에 액세스하는 방법을 설명합니다.

Agentless Collector 콘솔에 액세스하려면

1. 웹 브라우저를 열고 주소 표시줄에 **https://***<ip_address>***/** URL을 입력합니다. 여기서 *<ip_address>*는에서 가져온 수집기의 IP 주소입니다에이전트리스 수집기 배포.
2. Agentless Collector에 처음 액세스할 때 시작하기를 선택합니다. 그런 다음 로그인하라는 메시지가 표시됩니다.

Agentless Collector 콘솔에 처음 액세스하는 경우 다음으로가 됩니다에이전트리스 수집기 구성. 그렇지 않으면 다음으로가 표시됩니다에이전트리스 수집기 대시보드.

에이전트리스 수집기 구성

Application Discovery Service Agentless Collector(Agentless Collector)는 Amazon Linux 2 기반 가상 머신(VM)입니다. 다음 섹션에서는 Agentless Collector 콘솔의 Agentless Collector 구성 페이지에서 수집기 VM을 구성하는 방법을 설명합니다.

에이전트리스 수집기 구성 페이지에서 수집기 VM을 구성하려면

1. 수집기 이름에 수집기를 식별할 이름을 입력합니다. 이름에는 공백이 포함될 수 있지만 특수 문자는 포함될 수 없습니다.
2. 데이터 동기화에서 수집기가 검색한 데이터를 수신할 대상 계정으로 지정할 AWS 계정 IAM 사용자의 AWS 액세스 키와 보안 키를 입력합니다. IAM 사용자의 요구 사항에 대한 자세한 내용은 섹션을 참조하세요Application Discovery Service Agentless Collector 배포.

   a. AWS access-key에 대상 AWS 계정으로 지정하려는 계정 IAM 사용자의 액세스 키를 입력합니다.

   b. AWS secret-key에 대상 AWS 계정으로 지정하려는 계정 IAM 사용자의 보안 키를 입력합니다.

   c. (선택 사항) 네트워크에서 프록시를 사용하여에 액세스해야 하는 경우 프록시 호스트, 프록시 포트 및 선택적으로 기존 프록시 서버로 인증하는 데 필요한 자격 증명을 AWS입력합니다.
3. Agentless Collector 암호에서 Agentless Collector에 대한 액세스를 인증하는 데 사용할 암호를 설정합니다.

   - 암호는 대/소문자를 구분합니다.
   - 암호는 8~64자여야 합니다.
   - 암호는 각각의 다음 네 가지 범주의 문자를 최소 1자씩 포함해야 합니다.
     - 소문자(a~z)
     - 대문자(A-Z)
     - 숫자(0-9)
     - 영숫자가 아닌 문자(@$!#%*?&)
   - 암호는 @$!#%*?& 이외의 특수 문자를 포함할 수 없습니다.

   a. Agentless Collector 암호에 수집기에 대한 액세스를 인증하는 데 사용할 암호를 입력합니다.

   b. Agentless Collector 암호 재입력의 경우 확인을 위해 암호를 다시 입력합니다.
4. 기타 설정에서 라이선스 계약을 읽습니다. 수락에 동의하면 확인란을 선택합니다.

5. Agentless Collector에 대한 자동 업데이트를 활성화하려면 기타 설정에서 Agentless Collector 자동 업데이트를 선택합니다. 이 확인란을 선택하지 않으면에 설명된 대로 Agentless Collector를 수동으로 업데이트해야 합니다Application Discovery Service Agentless Collector 수동 업데이트.
6. 구성 저장을 선택합니다.

다음 주제에서는 선택적 수집기 구성 작업에 대해 설명합니다.

선택적 구성 작업

- (선택 사항) Agentless Collector VM의 고정 IP 주소 구성
- (선택 사항) DHCP를 사용하여 Agentless Collector VM을 로 재설정
- (선택 사항) Kerberos 인증 프로토콜 구성

(선택 사항) Agentless Collector VM의 고정 IP 주소 구성

다음 단계에서는 Application Discovery Service Agentless Collector(Agentless Collector) VM에 대한 고정 IP 주소를 구성하는 방법을 설명합니다. 처음 설치하면 동적 호스트 구성 프로토콜(DHCP)을 사용하도록 수집기 VM이 구성됩니다.

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

Agentless Collector version 2

수집기 VM에 대한 고정 IP 주소를 구성하려면

1. VMware vCenter에서 다음 네트워크 정보를 수집합니다.
   - 정적 IP 주소 - 서브넷의 서명되지 않은 IP 주소입니다. 예: 192.168.1.138.
   - CIDR 넷마스크 - CIDR 넷마스크를 가져오려면 수집기 VM을 호스팅하는 VMware vCenter 호스트의 IP 주소 설정을 확인합니다. 예: /24.
   - 기본 게이트웨이 - 기본 게이트웨이를 가져오려면 수집기 VM을 호스팅하는 VMware vCenter 호스트의 IP 주소 설정을 확인합니다. 예: 192.168.1.1.
   - 기본 DNS - 기본 DNS를 가져오려면 수집기 VM을 호스팅하는 VMware vCenter 호스트의 IP 주소 설정을 확인합니다. 예: 192.168.1.1.

- (선택 사항) 보조 DNS
- (선택 사항) 로컬 도메인 이름 - 이렇게 하면 수집기가 도메인 이름 없이 vCenter 호스트 URL에 도달할 수 있습니다.

2. 다음 예제와 **collector** 같이 수집기의 VM 콘솔을 열고 암호를 **ec2-user** 사용하여 로 로그인합니다.

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

3. 원격 터미널에 다음 명령을 입력하여 네트워크 인터페이스를 비활성화합니다.

```
sudo ip link set ens192 down
```

4. 다음 단계에 따라 인터페이스 구성을 업데이트합니다.

   a. 다음 명령을 사용하여 vi 편집기에서 10-cloud-init-ens192.network를 엽니다.

   ```
   sudo vi /etc/systemd/network/10-cloud-init-ens192.network
   ```

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

   ```
   [Match]
   Name=ens192

   [Network]
   DHCP=no
   Address=static-ip-value/CIDR-netmask
   Gateway=gateway-value
   DNS=dnsserver-value
   ```

5. 다음 단계에 따라 도메인 이름 시스템(DNS)을 업데이트합니다.

   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 예제에서는 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 ip link set ens192 up
```

7. 다음 예제와 같이 VM을 재부팅합니다.

```
sudo reboot
```

8. 다음 단계를 사용하여 네트워크 설정을 확인합니다.

   a. 다음 명령을 입력하여 IP 주소가 올바르게 구성되어 있는지 확인합니다.

```
ifconfig
ip addr show
```

   b. 다음 명령을 입력하여 게이트웨이가 올바르게 추가되었는지 확인합니다.

```
route -n
```

   출력은 다음 예제와 유사해야 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 퍼블릭 URL을 ping할 수 있는지 확인합니다.

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

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

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

Agentless Collector version 1

수집기 VM에 대한 고정 IP 주소를 구성하려면

1. VMware vCenter에서 다음 네트워크 정보를 수집합니다.
   - 정적 IP 주소 - 서브넷의 서명되지 않은 IP 주소입니다. 예: 192.168.1.138.
   - 네트워크 마스크 - 네트워크 마스크를 가져오려면 수집기 VM을 호스팅하는 VMware vCenter 호스트의 IP 주소 설정을 확인합니다. 예: 255.255.255.0.
   - 기본 게이트웨이 - 기본 게이트웨이를 가져오려면 수집기 VM을 호스팅하는 VMware vCenter 호스트의 IP 주소 설정을 확인합니다. 예: 192.168.1.1.
   - 기본 DNS - 기본 DNS를 가져오려면 수집기 VM을 호스팅하는 VMware vCenter 호스트의 IP 주소 설정을 확인합니다. 예: 192.168.1.1.
   - (선택 사항) 보조 DNS
   - (선택 사항) 로컬 도메인 이름 - 이렇게 하면 수집기가 도메인 이름 없이 vCenter 호스트 URL에 도달할 수 있습니다.
2. 다음 예제와 **collector** 같이 수집기의 VM 콘솔을 열고 암호를 **ec2-user** 사용하여 로 로그인합니다.

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

3. 원격 터미널에 다음 명령을 입력하여 네트워크 인터페이스를 비활성화합니다.

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

4. 다음 단계에 따라 인터페이스 eth0 구성을 업데이트합니다.

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

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

b. 다음 예제와 같이 네트워크 정보 수집 단계에서 수집하는 정보로 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 단계에 따라 도메인 이름 시스템(DNS)을 업데이트합니다.

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 예제에서는 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 예제와 같이 VM을 재부팅합니다.

```
sudo reboot
```

8. 다음 단계를 사용하여 네트워크 설정을 확인합니다.

a. 다음 명령을 입력하여 IP 주소가 올바르게 구성되어 있는지 확인합니다.

```
ifconfig
ip addr show
```

b. 다음 명령을 입력하여 게이트웨이가 올바르게 추가되었는지 확인합니다.

```
route -n
```

출력은 다음 예제와 유사해야 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 퍼블릭 URL을 ping할 수 있는지 확인합니다.

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

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

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

(선택 사항) DHCP를 사용하여 Agentless Collector VM을 로 재설정

다음 단계에서는 DHCP를 사용하도록 Agentless Collector VM을 재구성하는 방법을 설명합니다.

Agentless Collector version 2

DHCP를 사용하도록 수집기 VM을 구성하려면

1. 원격 터미널에서 다음 명령을 실행하여 네트워크 인터페이스를 비활성화합니다.

```
sudo ip link set ens192 down
```

2. 다음 단계에 따라 인터페이스 구성을 업데이트합니다.

   a. 다음 명령을 사용하여 vi 편집기에서 `10-cloud-init-ens192.network` 파일을 엽니다.

   ```
   sudo vi /etc/systemd/network/10-cloud-init-ens192.network
   ```

   b. 다음 예제와 같이 값을 업데이트합니다.

   ```
   [Match]
   Name=ens192

   [Network]
   DHCP=yes

   [DHCP]
   ClientIdentifier=mac
   ```

3. 다음 명령을 입력하여 DNS 설정을 재설정합니다.

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

4. 다음 명령을 입력하여 네트워크 인터페이스를 활성화합니다.

   ```
   sudo ip link set ens192 up
   ```

5. 다음 예제와 같이 수집기 VM을 재부팅합니다.

   ```
   sudo reboot
   ```

Agentless Collector version 1

DHCP를 사용하도록 수집기 VM을 구성하려면

1. 원격 터미널에서 다음 명령을 실행하여 네트워크 인터페이스를 비활성화합니다.

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

2. 다음 단계에 따라 네트워크 구성을 업데이트합니다.

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

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

b. 다음 예제와 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 예제와 같이 수집기 VM을 재부팅합니다.

```
sudo reboot
```

(선택 사항) Kerberos 인증 프로토콜 구성

OS 서버가 Kerberos 인증 프로토콜을 지원하는 경우이 프로토콜을 사용하여 서버에 연결할 수 있습니다. 이렇게 하려면 Application Discovery Service Agentless Collector VM을 구성해야 합니다.

다음 단계에서는 Application Discovery Service Agentless Collector VM에서 Kerberos 인증 프로토콜을 구성하는 방법을 설명합니다.

수집기 VM에서 Kerberos 인증 프로토콜을 구성하려면

1. 다음 예제와 **`collector`** 같이 수집기의 VM 콘솔을 열고 암호를 **`ec2-user`** 사용하여 로 로그인합니다.

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

2. /etc 폴더에서 krb5.conf 구성 파일을 엽니다. 다음 코드 예제를 사용하여 이 작업을 수행할 수 있습니다.

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

3. 다음 정보로 krb5.conf 구성 파일을 업데이트합니다.

```
[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 예제와 같이 수집기 VM을 재부팅합니다.

```
sudo reboot
```

Agentless Collector 네트워크 데이터 수집 모듈 사용

네트워크 데이터 수집 모듈을 사용하면 온프레미스 데이터 센터의 서버 간 종속성을 검색할 수 있습니다. 이 네트워크 데이터는 애플리케이션이 서버 간에 통신하는 방식에 대한 가시성을 제공하여 마이그레이션 계획을 가속화합니다.

Network Data Collection 모듈은 VMware vCenter 모듈이 식별하는 서버에 연결하고 해당 서버의 소스 IP에서 대상 IP/포트 트래픽으로 분석합니다.

주제

네트워크 데이터 수집 모듈 설정

Network Data Collection 모듈은 VMware vCenter 모듈에서 가져온 서버 인벤토리에 대한 네트워크 데이터를 수집합니다. 따라서 네트워크 데이터 수집 모듈을 사용하려면 먼저 VMware vCenter 모듈을 설정합니다. 지침은 다음 주제의 지침을 따르세요.

1. the section called “수집기 배포”
2. the section called “수집기 콘솔에 액세스”
3. the section called “수집기 구성”
4. the section called “VMware 데이터 수집 모듈 사용”

네트워크 데이터 수집 모듈을 설정하려면

1. Agentless Collector 대시보드의 네트워크 데이터 수집 섹션에서 네트워크 연결 보기를 선택합니다.
2. 네트워크 연결 페이지에서 수집기 편집을 선택합니다.
3. 자격 증명 섹션에서 자격 증명 세트를 하나 이상 입력합니다. 최대 10개의 자격 증명 세트를 입력할 수 있습니다. 모듈이 서버에 대한 데이터를 처음 수집하려고 할 때 작동하는 자격 증명 세트를 찾을 때까지 모든 자격 증명을 시도합니다. 그런 다음 해당 세트를 저장하고 이후 시도에서 다시 사용합니다. 자격 증명 설정에 대한 자세한 내용은 섹션을 참조하세요the section called “보안 인증 설정”.

4. 데이터 수집 기본 설정 섹션에서 서버가 재부팅될 때 데이터 수집을 자동으로 시작하려면 데이터 수집 자동 시작을 선택합니다.
5. WinRM 인증서를 설정하지 않은 경우 WinRM 인증서 검사 비활성화를 선택합니다.
6. 저장(Save)을 선택합니다.
7. 수집은 15초마다 서버에서 수행됩니다. 지정된 서버에 대한 수집 시도의 세부 정보를 보려면 서버 테이블에서 서버 왼쪽의 확인란을 선택합니다.

보안 인증 설정

Network Data Collection 모듈은 WinRM을 사용하여 Windows 서버에서 데이터를 수집합니다. SNMPv2 및 SNMPv3를 사용하여 Linux 서버에서 데이터를 수집합니다.

WinRM 자격 증명:

- 다음과 같은 Windows 계정의 사용자 이름과 암호를 지정합니다.
  - `\root\standardcimv2` 네임스페이스에 대한 읽기 액세스
  - `MSFT_NetTCPConnection` 클래스에 대한 읽기 권한
  - 원격 WMI 액세스
- 최소한의 필수 권한으로 전용 서비스 계정을 생성하는 것이 좋습니다.
- 도메인 관리자 또는 로컬 관리자 계정을 사용하지 마세요.
- 포트 5986(HTTPS)은 수집기와 대상 서버 간에 열려 있어야 합니다.
- WinRM 인증서 검사를 비활성화하지 마세요. WinRM 인증서 설정에 대한 자세한 내용은 섹션을 참조하세요the section called “WinRM 인증서 구성 시 자체 서명된 인증 문제 해결”.

SNMPv2 자격 증명:

- 1.3.6.1.2.1.6.13에 액세스할 수 있는 읽기 전용 커뮤니티 문자열을 제공합니다.* OID
- SNMPv3의 보안 개선으로 인해 SNMPv2SNMPv32보다 선호됩니다.
- 포트 161/UDP는 수집기와 대상 서버 간에 열려 있어야 합니다.
- 복잡하고 기본이 아닌 커뮤니티 문자열 사용
- "퍼블릭" 또는 "프라이빗"과 같은 일반적인 문자열은 피합니다.
- 커뮤니티 문자열을 암호처럼 처리

SNMPv3 보안 인증 정보

- 1.3.6.1.2.1.6.13에 액세스할 수 있는 읽기 전용 권한을 가진 사용자 이름/암호 및 인증/프라이버시 세부 정보를 제공합니다.* OID.
- 포트 161/UDP는 수집기와 대상 서버 간에 열려 있어야 합니다.
- 인증 및 개인 정보 보호 모두 활성화
- 강력한 인증 프로토콜 사용(MD5보다 SHA 선호)
- 강력한 암호화 프로토콜 사용(DES보다 AES 선호)
- 인증 및 개인 정보 보호 모두에 복잡한 암호 사용
- 고유한 사용자 이름 사용(일반 이름 피하기)

자격 증명 관리에 대한 일반적인 모범 사례

- 보안 인증 정보 저장
- 모든 자격 증명을 정기적으로 교체
- 암호 관리자 또는 보안 볼트 사용
- 자격 증명 사용량 모니터링
- 최소 권한 원칙을 따르고 필요한 최소 권한만 부여합니다.

네트워크 데이터 수집 시도

새 서버가 검색되면 수집기는 각 IP 주소에 대해 구성된 각 자격 증명을 시도합니다. 수집기가 유효한 자격 증명을 찾은 후에는 해당 자격 증명만 사용합니다. 두 번 연속 실패하면 수집기는 30분, 2시간, 8시간, 24시간 후에 서버의 네트워킹 데이터를 수집하려고 시도합니다. 6회 시도에 실패하면 수집기는 구성된 모든 자격 증명을 매일 한 번 계속 시도합니다. 문제를 해결하려면 현재 자격 증명을 편집하거나 수집기 편집을 선택하여 자격 증명을 추가하거나 모니터링 중인 대상 서버를 변경합니다.

Network Data Collection 모듈의 서버 상태

다음 표에서는 컬렉션 상태 값을 설명합니다.

상태 표시기	의미
수집 또는 수집	네트워크 연결에 대한 마지막 수집 시도가 성공했습니다.

상태 표시기	의미
오류 또는 오류	네트워킹 또는 권한 문제로 인해 네트워크 연결에 대한 마지막 수집 시도가 실패했습니다. 자세한 내용을 알아보려면 오류가 있는 서버 왼쪽의 확인란을 선택합니다.
건너뜀	유효한 자격 증명이 제공되지 않은 서버입니다. 추가 서버 자격 증명을 업데이트하거나 구성합니다.
데이터 없음	서버의 데이터 수집이 시작되지 않았습니다. 데이터 수집을 시작하려면 수집기 시작을 선택합니다.
보류중	수집이 시작되었지만 수집을 시도하지 않았습니다. 몇 분 정도 기다린 다음 목록을 새로 고칩니다.

VMware vCenter Agentless Collector 데이터 수집 모듈 사용

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

주제

- VMware vCenter용 Agentless Collector 데이터 수집 모듈 설정
- VMware 데이터 수집 세부 정보 보기
- vCenter 데이터 수집 범위 제어
- Agentless Collector VMware vCenter 데이터 수집 모듈에서 수집한 데이터

VMware vCenter용 Agentless Collector 데이터 수집 모듈 설정

이 섹션에서는 에이전트리스 컬렉터 VMware vCenter 데이터 수집 모듈을 설정하여 VMware VMs에서 서버 인벤토리, 프로파일 및 사용률 데이터를 수집하는 방법을 설명합니다.

> **Note**
>
> vCenter 설정을 시작하기 전에 시스템 그룹에 대한 읽기 및 보기 권한 세트를 사용하여 vCenter 자격 증명을 제공할 수 있는지 확인합니다.

VMware vCenter 데이터 수집 모듈을 설정하려면

1. Agentless Collector 대시보드 페이지의 데이터 수집에서 VMware vCenter 섹션에서 설정을 선택합니다.
2. VMware vCenter 데이터 수집 설정 페이지에서 다음을 수행합니다.
   a. vCenter 자격 증명에서:
      i. vCenter URL/IP에 VMware vCenter Server 호스트의 IP 주소를 입력합니다.
      ii. vCenter 사용자 이름에 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:
      - 설정 성공 직후 데이터 수집을 자동으로 시작하려면 데이터 수집 자동 시작을 선택합니다.
   c. 설정을 선택합니다.

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

VMware 데이터 수집 세부 정보 보기

VMware 데이터 수집 세부 정보 페이지에는에서 설정한 vCenter에 대한 세부 정보가 표시됩니다VMware vCenter용 Agentless Collector 데이터 수집 모듈 설정.

검색된 vCenter 서버 아래에 설정한 vCenter가 vCenter에 대한 다음 정보와 함께 나열됩니다.

- vCenter 서버의 IP 주소입니다.
- vCenter의 서버 수입니다.
- 데이터 수집의 상태입니다.

- 마지막 업데이트 이후 경과 시간입니다.

vCenter 서버 제거를 선택하여 표시된 vCenter 서버를 제거하고 VMware vCenter 데이터 수집 설정 페이지로 돌아갑니다.

데이터 수집을 자동으로 시작하도록 선택하지 않은 경우이 페이지의 데이터 수집 시작 버튼을 사용하여 데이터 수집을 시작할 수 있습니다. 데이터 수집이 시작되면 시작 버튼이 데이터 수집 중지로 변경됩니다.

수집 상태 열에 수집 중이 표시되면 데이터 수집이 시작된 것입니다.

AWS Migration Hub 콘솔에서 수집된 데이터를 볼 수 있습니다. VMware vCenter 서버 인벤토리에 대한 데이터를 수집하는 경우 데이터 수집을 켠 후 약 15분 후에 콘솔에 표시되는 데이터에 액세스할 수 있습니다.

인터넷 액세스가 차단되지 않은 경우이 페이지에서 Migration Hub의 서버 보기를 선택하여 Migration Hub 콘솔을 열 수 있습니다. 이 버튼을 선택하든 선택하지 않든 Migration Hub 콘솔에 액세스하는 방법에 대한 자세한 내용은 섹션을 참조하세요수집된 데이터 보기.

다음은 마이그레이션 계획 활동에 따라 권장되는 데이터 수집 기간에 대한 지침입니다.

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

vCenter 데이터 수집 범위 제어

vCenter 사용자는 Application Discovery Service를 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 vCenter에 속한 모든 호스트와 VM이 인벤토리에 추가되도록 허용하거나 각 사례별로 권한을 부여할 수 있습니다.

> **Note**
>
> 보안 모범 사례로 Application Discovery Service의 vCenter 사용자에게 불필요한 추가 권한을 부여하지 않는 것이 좋습니다.

다음 절차는 세분화 수준이 가장 낮은 순서에서 높은 순서로 구성 시나리오를 설명합니다. 이 절차는 vSphere Client v6.7.0.2에 대한 것입니다. 사용하는 vSphere 클라이언트 버전에 따라 다른 버전의 클라이언트에 대한 절차가 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. 데이터 센터 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. 하위에 전파를 선택한 다음 확인을 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. 확인을 선택합니다.

> **Note**
>
> [Propagate to children]을 선택한 경우에도 각 사례별로 ESX 호스트와 VM에서 읽기 전용 권한을 제거할 수 있습니다. 이 옵션은 다른 ESX 호스트와 VM에 적용되는 상속된 권한에 영향을 미치지 않습니다.

Agentless Collector VMware vCenter 데이터 수집 모듈에서 수집한 데이터

다음 정보는 Application Discovery Service Agentless Collector(Agentless Collector) VMware vCenter 데이터 수집 모듈에서 수집하는 데이터를 설명합니다. 데이터 수집 설정에 대한 자세한 내용은 섹션을 참조하세요VMware vCenter용 Agentless Collector 데이터 수집 모듈 설정.

Agentless Collector VMware vCenter에서 수집한 데이터에 대한 테이블 범례:

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

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

데이터 필드	설명
applicationConfigurationId*	VM이 그룹화된 마이그레이션 애플리케이션의 ID입니다.
avgCpuUsagePct	폴링 기간 동안의 평균 CPU 사용량 비율입니다.

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 null입니다.
avgDiskWriteOpsPerSecond**	초당 평균 쓰기 I/O 작업 수입니다.
avgFreeRAM	평균 무료 RAM은 MB로 표현됩니다.
avgNetworkBytesReadPerSecond	초당 읽기 바이트의 평균 처리량입니다.
avgNetworkBytesWrittenPerSecond	초당 기록된 평균 처리량 바이트 수입니다.
computerManufacturer	ESXi 호스트에서 보고한 공급업체입니다.
computerModel	ESXi 호스트에서 보고한 컴퓨터 모델입니다.
configId	Application Discovery Service에서 검색된 VM에 할당한 ID입니다.
configType	검색된 리소스 유형입니다.
connectorId	가상 어플라이언스의 ID입니다.
cpuType	VM용 vCPU, 호스트용 실제 모델.
datacenterId	vCenter의 ID입니다.
hostId*	VM 호스트의 ID입니다.
hostName	가상화 소프트웨어를 실행하는 호스트의 이름입니다.
하이퍼바이저	하이퍼바이저 유형입니다.
id	서버의 ID입니다.

데이터 필드	설명
lastModifiedTimeStamp*	데이터 내보내기 전 데이터 수집의 최신 날짜 및 시간입니다.
macAddress	VM의 MAC 주소입니다.
주소	가상화 소프트웨어의 작성자입니다.
maxCpuUsagePct	폴링 기간 중 CPU 사용량의 최대 백분율입니다.
maxDiskBytesReadPerSecond	폴링 기간 동안 디스크에서 읽은 최대 바이트 수입니다.
maxDiskBytesWrittenPerSecond	폴링 기간 동안 디스크에 기록된 최대 바이트 수입니다.
maxDiskReadOpsPerSecond**	초당 최대 읽기 I/O 작업 수입니다.
maxDiskWriteOpsPerSecond**	초당 최대 쓰기 I/O 작업 수입니다.
maxNetworkBytesReadPerSecond	초당 읽기 바이트의 최대 처리량입니다.
maxNetworkBytesWrittenPerSecond	초당 쓰기되는 최대 처리량 바이트 수입니다.
memoryReservation*	VM에서 메모리의 과다 커밋을 방지하기 위해 제한합니다.
moRefId	고유한 vCenter 관리형 객체 참조 ID입니다.
name*	VM 또는 네트워크 이름(사용자 지정).
numCores	VM에 할당된 CPU 코어 수입니다.
numCpus	ESXi 호스트의 CPU 소켓 수입니다.
numDisks**	VM의 디스크 수입니다.
numNetworkCards**	VM의 네트워크 카드 수입니다.
osName	VM의 운영 체제 이름입니다.

데이터 필드	설명
osVersion	VM의 운영 체제 버전.
portGroupId*	VLAN의 멤버 포트 그룹의 ID입니다.
portGroupName*	VLAN의 멤버 포트 그룹 이름입니다.
powerState*	전원 상태입니다.
serverId	Application Discovery Service에서 검색된 VM에 ID를 할당했습니다.
smBiosId*	시스템 관리 BIOS의 ID/버전입니다.
state*	가상 어플라이언스의 상태입니다.
toolsStatus	VMware 도구의 운영 상태
totalDiskFreeSize	MB로 표현되는 여유 디스크 공간입니다. vCenter Server 7.0 이상 버전에서 사용할 수 있습니다.
totalDiskSize	MB로 표현되는 디스크의 총 용량입니다.
totalRAM	VM에서 사용할 수 있는 총 RAM 양은 MB입니다.
type	호스트 유형입니다.
vCenterId	VM의 고유 ID 번호입니다.
vCenterName*	vCenter 호스트의 이름입니다.
virtualSwitchName*	가상 스위치의 이름입니다.
vmFolderPath	VM 파일의 디렉터리 경로입니다.
vmName	가상 머신의 이름입니다.

데이터베이스 및 분석 데이터 수집 모듈 사용

이 섹션에서는 데이터베이스 및 분석 데이터 수집 모듈을 설정, 구성 및 사용하는 방법을 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 섹션을 참조하세요Agentless Collector 데이터베이스 및 분석 데이터 수집 모듈에서 수집한 데이터.

> **Important**
>
> 지원 종료 공지: 2026년 5월 20일에 AWS 는 AWS Database Migration Service Fleet Advisor 에 대한 지원을 종료합니다. 2026년 5월 20일 이후에는 더 이상 AWS DMS Fleet Advisor 콘솔 또는 AWS DMS Fleet Advisor 리소스에 액세스할 수 없습니다. 자세한 내용은 AWS DMS Fleet Advisor 지원 종료를 참조하세요.

데이터베이스 및 분석 데이터 수집 모듈을 사용할 때 상위 수준에서 다음 단계를 수행합니다.

1. 사전 조건 단계를 완료하고, IAM 사용자를 구성하고, 데이터 수집기를 생성합니다 AWS DMS .
2. 데이터 수집 모듈이 수집된 메타데이터 및 성능 지표를 전송할 수 있도록 데이터 전달을 구성합니다 AWS.
3. LDAP 서버를 추가하고 이를 사용하여 데이터 환경에서 OS 서버를 검색합니다. 또는 OS 서버를 수동으로 추가하거나를 사용합니다VMware 데이터 수집 모듈 사용.
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 컬렉션을 실행합니다. 자세한 내용은 데이터베이스 및 분석 데이터 수집 단원을 참조하십시오.
6. AWS DMS 콘솔에서 수집된 데이터를 보고 이를 사용하여 로 마이그레이션하기 위한 대상 권장 사항을 생성합니다 AWS 클라우드. 자세한 내용은 데이터베이스 및 분석 데이터 수집 단원을 참조하십시오.

주제

- Agentless Collector 데이터베이스 및 분석 데이터 수집 모듈에서 수집한 데이터

지원되는 OS, 데이터베이스 및 분석 서버

Agentless Collector의 데이터베이스 및 분석 데이터 수집 모듈은 Microsoft Active Directory LDAP 서버를 지원합니다.

이 데이터 수집 모듈은 다음 OS 서버를 지원합니다.

- Amazon Linux 2
- CentOS Linux 버전 6 이상
- Debian 버전 10 이상
- Red Hat Enterprise Linux 버전 7 이상
- SUSE Linux Enterprise Server 버전 12 이상
- Ubuntu 버전 16.01 이상
- Windows Server 2012 이상
- Windows XP 이상

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

- Microsoft SQL Server 버전 2012 및 2019 이하
- MySQL 버전 5.6 및 8 이하
- Oracle 버전 11g 릴리스 2 및 12c 이하, 19c 및 21c
- PostgreSQL 버전 9.6 및 13 이하

AWS DMS 데이터 수집기 생성

데이터베이스 및 분석 데이터 수집 모듈은 AWS DMS 데이터 수집기를 사용하여 AWS DMS 콘솔과 상호 작용합니다. AWS DMS 콘솔에서 수집된 데이터를 보거나 이를 사용하여 적절한 크기의 AWS 대상 엔진을 결정할 수 있습니다. 자세한 내용은 AWS DMS Fleet Advisor 대상 권장 사항 기능 사용을 참조하세요.

AWS DMS 데이터 수집기를 생성하기 전에 AWS DMS 데이터 수집기가 Amazon S3 버킷에 액세스하는 데 사용하는 IAM 역할을 생성합니다. 에서 사전 조건을 완료하면이 Amazon S3 버킷을 생성했습니다Agentless Collector의 사전 조건.

AWS DMS 데이터 수집기가 Amazon S3에 액세스할 수 있는 IAM 역할을 생성하려면

1. 에 로그인 AWS Management Console 하고 https://console.aws.amazon.com/iam/ IAM 콘솔을 엽니다.
2. 탐색 창에서 역할을 선택한 다음 역할 생성을 선택합니다.
3. 신뢰할 수 있는 엔터티 선택 페이지의 신뢰할 수 있는 엔터티 유형 아래에서 AWS 서비스를 선택합니다. 다른 AWS 서비스의 사용 사례에서 DMS를 선택합니다.
4. DMS 확인란을 선택하고 다음을 선택합니다.
5. 권한 추가 페이지에서 이전에 생성한 FleetAdvisorS3Policy를 선택합니다. 다음을 선택합니다.
6. 이름 지정, 검토 및 생성 페이지에서 역할 이름에 **`FleetAdvisorS3Role`**을 입력하고 역할 생성을 선택합니다.
7. 생성한 역할을 열고 신뢰 관계 탭을 선택합니다. 신뢰 정책 편집을 선택합니다.
8. 신뢰 정책 편집 페이지에서 다음 JSON을 편집기에 붙여넣고 기존 코드를 바꿉니다.

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

9. 정책 업데이트를 선택합니다.

이제 AWS DMS 콘솔에서 데이터 수집기를 생성합니다.

AWS DMS 데이터 수집기를 생성하려면

1. 에 로그인 AWS Management Console 하고 https://console.aws.amazon.com/dms/v2/ AWS DMS 콘솔을 엽니다.

2. Migration Hub 홈 리전으로 AWS 리전 설정한를 선택합니다. 자세한 내용은 Migration Hub에 로그인하고 홈 리전 선택 단원을 참조하십시오.
3. 탐색 창에서 검색 아래에 있는 데이터 수집기를 선택합니다. 데이터 수집기 페이지가 열립니다.
4. 데이터 수집기 생성을 선택합니다. 데이터 수집기 생성 페이지가 열립니다.
5. 일반 구성 섹션의 이름에 데이터 수집기의 이름을 입력합니다.
6. 연결 섹션에서 Browse S3을 선택합니다. 목록에서 이전에 생성한 Amazon S3 버킷을 선택합니다.
7. IAM 역할에서 이전에 생성한 `FleetAdvisorS3Role`를 선택합니다.
8. 데이터 수집기 생성을 선택합니다.

데이터 전달 구성

필요한 AWS 리소스를 생성한 후 데이터베이스 및 분석 데이터 수집 모듈에서 AWS DMS 수집기로의 데이터 전달을 구성합니다.

데이터 전달을 구성하려면

1. Agentless Collector 콘솔을 엽니다. 자세한 내용은 수집기 콘솔에 액세스 단원을 참조하십시오.
2. 데이터베이스 및 분석 수집기 보기를 선택합니다.
3. 대시보드 페이지의 데이터 전달 섹션에서 데이터 전달 구성을 선택합니다.
4. AWS 리전, IAM 액세스 키 ID 및 IAM 보안 액세스 키의 경우 Agentless Collector는 이전에 구성한 값을 사용합니다. 자세한 내용은 Migration Hub에 로그인하고 홈 리전 선택 및 수집기 배포 섹션을 참조하세요.
5. 연결된 DMS 데이터 수집기에서 AWS DMS 콘솔에서 생성한 데이터 수집기를 선택합니다.
6. 저장을 선택합니다.

데이터 전달을 구성한 후 대시보드 페이지에서 데이터 전달 섹션을 확인합니다. 데이터베이스 및 분석 데이터 수집 모듈에 DMS에 대한 액세스 및 S3에

대한 액세스에 연결됨이 표시되는지 확인합니다.

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. LDAP(Lightweight Directory Access

Protocol)는 개방형 표준 애플리케이션 프로토콜입니다. 이 프로토콜을 사용하여 IP 네트워크를 통해 분산 디렉터리 정보 서비스에 액세스하고 유지할 수 있습니다.

데이터베이스 및 분석 데이터 수집 모듈에 기존 LDAP 서버를 추가하여 네트워크의 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. Agentless Collector 콘솔을 엽니다. 자세한 내용은 수집기 콘솔에 액세스 단원을 참조하십시오.
2. 데이터베이스 및 분석 수집기 보기를 선택한 다음 탐색 창의 검색에서 LDAP 서버를 선택합니다.
3. LDAP 서버 추가를 선택합니다. LDAP 서버 추가 페이지가 열립니다.
4. 호스트 이름에 LDAP 서버의 호스트 이름을 입력합니다.
5. 포트에 LDAP 요청에 사용되는 포트 번호를 입력합니다.
6. 사용자 이름에 LDAP 서버에 연결하는 데 사용하는 사용자 이름을 입력합니다.
7. 암호에 LDAP 서버에 연결하는 데 사용하는 암호를 입력합니다.
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 검색의 경우, 도메인 서버가 LDAP 프로토콜을 사용하여 요청을 실행하려면 데이터 수집 모듈에 자격 증명이 필요합니다.

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

또는 OS 서버를 수동으로 추가하거나 쉼표로 구분된 값(CSV) 파일에서 서버 목록을 가져올 수 있습니다. 또한 VMware vCenter Agentless Collector 데이터 수집 모듈을 사용하여 OS 서버를 검색할 수 있습니다. 자세한 내용은 VMware 데이터 수집 모듈 사용 단원을 참조하십시오.

데이터베이스 및 분석 데이터 수집 모듈에 OS 서버를 추가하려면

1. 데이터베이스 및 분석 수집기 페이지의 탐색 창의 검색에서 OS 서버를 선택합니다.

2. OS 서버 추가를 선택합니다. OS 서버 추가 페이지가 열립니다.
3. OS 서버 자격 증명을 제공합니다.

   a. OS 유형에서 서버의 운영 체제를 선택합니다.

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

   c. 포트에 원격 쿼리에 사용되는 포트 번호를 입력합니다.

   d. 인증 유형에서 OS 서버에서 사용하는 인증 유형을 선택합니다.

   e. 사용자 이름에 OS 서버에 연결하는 데 사용하는 사용자 이름을 입력합니다.

   f. 암호에 OS 서버에 연결하는 데 사용하는 암호를 입력합니다.

   g. 확인을 선택하여 OS 서버 자격 증명을 올바르게 추가했는지 확인합니다.
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 서버에 대한 자격 증명을 추가한 후 CSV 파일을 저장합니다.

   d. 찾아보기를 선택한 다음 CSV 파일을 선택합니다.
5. OS 서버 추가를 선택합니다.
6. 모든 OS 서버에 대한 자격 증명을 추가한 후 OS 서버를 선택하고 데이터베이스 서버 검색을 선택합니다.

데이터베이스 서버 검색

이 섹션에서는 운영 체제 및 데이터베이스 서버를 구성하기 위해 수행해야 하는 단계를 안내합니다. 그런 다음 서버를 검색하고 데이터베이스 또는 분석 서버를 수동으로 추가할 수 있습니다.

데이터베이스 검색의 경우 데이터 수집 모듈에 필요한 최소 권한을 가진 소스 데이터베이스 사용자를 생성해야 합니다. 자세한 내용은 AWS DMS 사용 설명서의 AWS DMS Fleet Advisor용 데이터베이스 사용자 생성을 참조하세요.

설정 구성

이전에 추가된 OS 서버에서 실행 중인 데이터베이스를 검색하려면 데이터 수집 모듈에 운영 체제 및 데이터베이스 서버에 대한 액세스 권한이 필요합니다. 이 페이지에서는 연결 설정에서 지정한 포트에서 데이터베이스에 액세스할 수 있도록 하기 위해 수행해야 하는 단계를 간략하게 설명합니다. 또한 데이터베이스 서버에서 원격 인증을 켜고 데이터 수집 모듈에 권한을 제공합니다.

Linux에서 설정 구성

Linux에서 데이터베이스 서버를 검색하도록 설정을 구성하려면 다음 절차를 완료하세요.

데이터베이스 서버를 검색하도록 Linux를 구성하려면

1. `ss` 및 `netstat` 명령에 대한 sudo 액세스 권한을 제공합니다.

   다음 코드 예제에서는 `ss` 및 `netstat` 명령에 대한 sudo 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"
   ```

   앞의 예에서를 OS 서버 연결 자격 증명에 지정한 Linux 사용자의 이름으로 *username* 바꿉니다.

   앞의 예제에서는 `ss` 및 `netstat` 명령의 `/usr/bin/` 경로를 사용합니다. 이 경로는 사용자 환경에서 다를 수 있습니다. `ss` 및 `netstat` 명령의 경로를 확인하려면 `which ss` 및 `which netstat` 명령을 실행합니다.
2. 원격 SSH 스크립트 실행을 허용하고 인터넷 제어 메시지 프로토콜(ICMP) 트래픽을 허용하도록 Linux 서버를 구성합니다.

Microsoft Windows에서 설정 구성

Microsoft Windows에서 데이터베이스 서버를 검색하도록 설정을 구성하려면 다음 절차를 완료하세요.

데이터베이스 서버를 검색하도록 Microsoft Windows를 구성하려면

1. 자격 증명에 권한 부여를 제공하여 Windows Management Instrumentation(WMI) 및 WMI 쿼리 언어(WQL) 쿼리를 실행하고 레지스트리를 읽을 수 있습니다.

2. OS 서버 연결 자격 증명에서 지정한 Windows 사용자를 분산 COM 사용자, 성능 로그 사용자, 성능 모니터 사용자 및 이벤트 로그 리더 그룹에 추가합니다. 이 작업을 수행하려면 다음 코드 예제를 사용합니다.

```
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
```

   앞의 예에서를 OS 서버 연결 자격 증명에 지정한 Windows 사용자의 이름으로 *username* 바꿉니다.

3. OS 서버 연결 자격 증명에서 지정한 Windows 사용자에게 필요한 권한을 부여합니다.

   - Windows 관리 및 계측 속성에서 로컬 시작 및 원격 활성화를 선택합니다.
   - WMI 제어에서 , , 및 WMI 네임스페이스에 대한 방법 실행CIMV2, 계정 활성화, 원격 활성화 DEFAULT StandartCimv2및 읽기 보안 권한을 선택합니다.
   - WMI 플러그인의 경우 winrm configsddl default를 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
```

데이터베이스 서버 검색

콘솔에서 데이터베이스 서버를 검색하고 추가하려면 다음 작업 세트를 완료합니다.

데이터베이스 서버 검색을 시작하려면

1. 데이터베이스 및 분석 수집기 페이지의 탐색 창의 검색에서 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 편집합니다.

    a. 자격 증명이 동일한 단일 서버 또는 여러 서버를 선택한 다음 작업 메뉴에서 편집을 선택합니다. OS 서버 편집 페이지가 열립니다.

    b. 포트에 원격 쿼리에 사용되는 포트 번호를 입력합니다.

    c. 인증 유형에서 OS 서버가 사용하는 인증 유형을 선택합니다.

    d. 사용자 이름에 OS 서버에 연결하는 데 사용하는 사용자 이름을 입력합니다.

    e. 암호에 OS 서버에 연결하는 데 사용하는 암호를 입력합니다.

    f. 연결 확인을 선택하여 OS 서버 자격 증명을 올바르게 업데이트했는지 확인합니다. 그 후 저장을 선택합니다.
4. 모든 OS 서버의 자격 증명을 업데이트한 후 OS 서버를 선택하고 데이터베이스 서버 검색을 선택합니다.

데이터베이스 및 분석 데이터 수집 모듈은 OS 서버에 연결하고 지원되는 데이터베이스 및 분석 서버를 검색합니다. 데이터 수집 모듈이 검색을 완료한 후 데이터베이스 서버 보기를 선택하여 검색된 데이터베이스 및 분석 서버 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 인벤토리에 이미 추가한 경우이 단계를 건너뛸 수 있습니다.

데이터베이스 또는 분석 서버를 수동으로 추가하려면

1. 데이터베이스 및 분석 수집기 페이지의 탐색 창에서 데이터 수집을 선택합니다.
2. 데이터베이스 서버 추가를 선택합니다. 데이터베이스 서버 추가 페이지가 열립니다.
3. 데이터베이스 서버 자격 증명을 제공합니다.

    a. 데이터베이스 엔진에서 서버의 데이터베이스 엔진을 선택합니다. 자세한 내용은 지원되는 OS, 데이터베이스 및 분석 서버 단원을 참조하십시오.

    b. 호스트 이름/IP에 데이터베이스 또는 분석 서버의 호스트 이름 또는 IP 주소를 입력합니다.

    c. 포트에 서버가 실행되는 포트를 입력합니다.

d. 인증 유형에서 데이터베이스 또는 분석 서버가 사용하는 인증 유형을 선택합니다.

e. 사용자 이름에 서버에 연결하는 데 사용하는 사용자 이름을 입력합니다.

f. 암호에 서버에 연결하는 데 사용하는 암호를 입력합니다.

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

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 CSV 파일에 데이터베이스 또는 분석 서버 연결 자격 증명을 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 서버의 자격 증명을 추가한 후 CSV 파일을 저장합니다.

d. 찾아보기를 선택한 다음 CSV 파일을 선택합니다.

5. 데이터베이스 서버 추가를 선택합니다.

6. 모든 OS 서버에 대한 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 연결하고 메타데이터 및 성능 지표를 수집할 수 있습니다.

데이터베이스 및 분석 서버를 인벤토리에 추가하려면

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

2. 메타데이터 및 성능 지표를 수집할 데이터베이스 및 분석 서버를 선택합니다.

3. 인벤토리에 추가를 선택합니다.

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

Agentless Collector 데이터베이스 및 분석 데이터 수집 모듈에서 수집한 데이터

Application Discovery Service Agentless Collector(Agentless Collector) 데이터베이스 및 분석 데이터 수집 모듈은 데이터 환경에서 다음 지표를 수집합니다. 데이터 수집 설정에 대한 자세한 내용은 섹션을 참조하세요데이터베이스 및 분석 데이터 수집 모듈 사용.

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

- OS 서버의 가용 메모리
- OS 서버의 가용 스토리지
- 데이터베이스 버전 및 에디션
- OS 서버의 CPU 수
- 스키마 수
- 저장된 프로시저의 수
- 테이블 수
- 트리거 수
- 조회수
- 스키마 구조

AWS DMS 콘솔에서 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 수집할 때 다음 지표를 캡처합니다.

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

수집된 데이터 보기

> **Important**
>
> 지원 종료 공지: 2026년 5월 20일에 AWS 는 AWS Database Migration Service Fleet Advisor에 대한 지원을 종료합니다. 2026년 5월 20일 이후에는 더 이상 AWS DMS Fleet Advisor 콘솔 또는 AWS DMS Fleet Advisor 리소스에 액세스할 수 없습니다. 자세한 내용은 AWS DMS Fleet Advisor 지원 종료를 참조하세요.

의 단계에 따라 Application Discovery Service Agentless Collector(Agentless Collector)가 Migration Hub 콘솔에서 수집한 데이터를 볼 수 있습니다AWS Migration Hub 콘솔에서 서버 보기.

다음 단계를 수행하여 AWS DMS 콘솔에서 데이터베이스 및 분석 서버에 대해 수집된 지표를 볼 수도 있습니다.

AWS DMS 콘솔에서 데이터베이스 및 분석 데이터 수집 모듈에서 검색한 데이터를 보려면

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

AWS DMS 콘솔을 사용하여 중복 스키마를 식별하고, 마이그레이션 복잡성을 결정하고, 향후 분석을 위해 인벤토리 정보를 내보낼 수 있습니다. 자세한 내용은 Fleet Advisor에서 AWS DMS 분석에 인벤토리 사용을 참조하세요.

에이전트리스 수집기 액세스

이 섹션에서는 Application Discovery Service Agentless Collector(Agentless Collector)를 사용하는 방법을 설명합니다.

주제

- 에이전트리스 수집기 대시보드
- Agentless Collector 설정 편집
- VMware vCenter 자격 증명 편집

에이전트리스 수집기 대시보드

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

주제

- 수집기 상태
- 데이터 수집

수집기 상태

수집기 상태는 수집기에 대한 상태 정보를 제공합니다. 수집기 이름, 수집기의 AWS 연결 상태, Migration Hub 홈 리전 및 버전.

AWS 연결 문제가 있는 경우 Agentless Collector 구성 설정을 편집해야 할 수 있습니다.

수집기 구성 설정을 편집하려면 수집기 설정 편집을 선택하고에 설명된 지침을 따릅니다Agentless Collector 설정 편집.

데이터 수집

데이터 수집에서 데이터 수집 방법을 선택할 수 있습니다. Application Discovery Service Agentless Collector(Agentless Collector)는 현재 VMware VMs과 데이터베이스 및 분석 서버에서 데이터 수집을 지원합니다. 향후 모듈은 추가 가상화 플랫폼에서의 수집과 운영 체제 수준 수집을 지원합니다.

주제

VMware vCenter 데이터 수집

VMware VMs에서 서버 인벤토리, 프로파일 및 사용률 데이터를 수집하려면 vCenter 서버에 대한 연결을 설정합니다. 연결을 설정하려면 VMware vCenter 섹션에서 설정을 선택하고에 설명된 지침을 따릅니다VMware vCenter Agentless Collector 데이터 수집 모듈 사용.

vCenter 데이터 수집을 설정한 후 대시보드에서 다음을 수행할 수 있습니다.

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

> **Note**
>
> 대시보드 페이지의 vCenter 데이터 수집을 설정한 후 VMware vCenter 섹션의 설정 버튼이 데이터 수집 상태 정보, 데이터 수집 중지 버튼 및 보기 및 편집 버튼으로 대체됩니다.

데이터베이스 및 분석 데이터 수집

다음 두 가지 모드에서 데이터베이스 및 분석 데이터 수집 모듈을 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. 이 수집된 정보를 사용하여 AWS DMS 콘솔에서 대상 권장 사항을 계산할 수 있습니다. 소스 데이터베이스가 과다 프로비저닝되거나 과소 프로비저닝되면 대상 권장 사항도 과다 프로비저닝되거나 과소 프로비저닝됩니다.

이것이 기본 모드입니다.

메타데이터, 데이터베이스 용량 및 리소스 사용률

메타데이터 및 데이터베이스 용량 정보 외에도 데이터 수집 모듈은 데이터베이스 및 분석 서버의 CPU, 메모리 및 디스크 용량에 대한 실제 사용률 지표를 수집합니다. 권장 사항은 실제 데이터베이

스 워크로드를 기반으로 하므로이 모드는 기본 모드보다 더 정확한 대상 권장 사항을 제공합니다. 이 모드에서 데이터 수집 모듈은 1분마다 성능 지표를 수집합니다.

데이터베이스 및 분석 서버에서 메타데이터 및 성능 지표 수집을 시작하려면

1. 데이터베이스 및 분석 수집기 페이지의 탐색 창에서 데이터 수집을 선택합니다.
2. 데이터베이스 인벤토리 목록에서 메타데이터 및 성능 지표를 수집할 데이터베이스 및 분석 서버를 선택합니다.
3. 데이터 수집 실행을 선택합니다. 데이터 수집 유형 대화 상자가 열립니다.
4. 분석을 위해 데이터를 수집하는 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. 데이터 수집 상태를 보려면 수집 상태 탭을 선택합니다.

데이터 수집을 완료하면 데이터 수집 모듈이 수집된 데이터를 Amazon S3 버킷에 업로드합니다. 그런 다음에 설명된 대로 수집된이 데이터를 볼 수 있습니다수집된 데이터 보기.

Agentless Collector 설정 편집

에 설명된 대로 Application Discovery Service Agentless Collector(Agentless Collector)를 처음 설정할 때 수집기를 구성했습니다에이전트리스 수집기 구성. 다음 절차에서는 Agentless Collector 구성 설정을 편집하는 방법을 설명합니다.

수집기 구성 설정을 편집하려면

- Agentless Collector 대시보드에서 수집기 설정 편집 버튼을 선택합니다.

  수집기 설정 편집 페이지에서 다음을 수행합니다.

  a. 수집기 이름에 수집기를 식별할 이름을 입력합니다. 이름에는 공백이 포함될 수 있지만 특수 문자는 포함될 수 없습니다.

  b. 검색 데이터의 대상 AWS 계정에서 수집기가 검색한 데이터를 수신할 대상 계정으로 지정할 AWS 계정의 AWS 액세스 키와 보안 키를 입력합니다. IAM 사용자의 요구 사항에 대한 자세한 내용은 섹션을 참조하세요Application Discovery Service Agentless Collector 배포.

i. AWS access-key에 대상 AWS 계정으로 지정하려는 계정 IAM 사용자의 액세스 키를 입력합니다.

ii. AWS Secret-key에 대상 AWS 계정으로 지정하려는 계정 IAM 사용자의 보안 키를 입력합니다.

c. Agentless Collector 암호에서 Agentless Collector에 대한 액세스를 인증하는 데 사용할 암호를 변경합니다.

i. Agentless Collector 암호에 Agentless Collector에 대한 액세스를 인증하는 데 사용할 암호를 입력합니다.

ii. Agentless Collector 암호 재입력의 경우 확인을 위해 암호를 다시 입력합니다.

d. 구성 저장을 선택합니다.

다음으로가 표시됩니다에이전트리스 수집기 대시보드.

VMware vCenter 자격 증명 편집

VMware VMs에서 서버 인벤토리, 프로파일 및 사용률 데이터를 수집하려면 vCenter 서버에 대한 연결을 설정합니다. VMware vCenter 연결 설정에 대한 자세한 내용은 섹션을 참조하세요VMware vCenter Agentless Collector 데이터 수집 모듈 사용.

이 섹션에서는 vCenter 자격 증명을 편집하는 방법을 설명합니다.

> **Note**
>
> vCenter 자격 증명을 편집하기 전에 시스템 그룹에 대한 읽기 및 보기 권한 세트를 사용하여 vCenter 자격 증명을 제공할 수 있는지 확인합니다.

VMware vCenter 자격 증명을 편집하려면

페이지에서 vCenter 서버 편집을 VMware 데이터 수집 세부 정보 보기 선택합니다.

- vCenter 편집 페이지에서 다음을 수행합니다.

  a. vCenter 자격 증명에서:

  i. vCenter URL/IP에 VMware vCenter Server 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. 저장(Save)을 선택합니다.

Application Discovery Service Agentless Collector 수동 업데이트

Application Discovery Service Agentless Collector(Agentless Collector)를 구성할 때에 설명된 대로 자동 업데이트를 활성화하도록 선택할 수 있습니다에이전트리스 수집기 구성. 자동 업데이트를 활성화하지 않으면 Agentless Collector를 수동으로 업데이트해야 합니다.

다음 절차에서는 Agentless Collector를 수동으로 업데이트하는 방법을 설명합니다.

Agentless Collector를 수동으로 업데이트하려면

1. 최신 Agentless Collector Open Virtualization Archive(OVA) 파일을 가져옵니다.
2. (선택 사항) 최신 파일을 배포하기 전에 이전 Agentless Collector OVA 파일을 삭제하는 것이 좋습니다.
3. 의 단계를 따릅니다에이전트리스 수집기 배포.

이전 절차에서는 에이전트리스 수집기만 업데이트합니다. OS를 최신 상태로 유지하는 것은 사용자의 책임입니다.

Amazon EC2 인스턴스를 업데이트하려면

1. VMware vCenter에서 Agentless Collector의 IP 주소를 가져옵니다.
2. 다음 예제와 **`collector`** 같이 수집기의 VM 콘솔을 열고 암호를 **`ec2-user`** 사용하여 로 로그인합니다.

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

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

커널 라이브 패치

Agentless Collector version 2

Agentless Collector 버전 2 가상 머신은에 설명된 대로 Amazon Linux 2023을 사용합니다에이전트리스 수집기 배포.

Amazon Linux 2023용 라이브 패치를 활성화하고 사용하려면 Amazon EC2 사용 설명서의 AL2023의 커널 라이브 패치를 참조하세요. Amazon EC2

Agentless Collector version 1

Agentless Collector 버전 1 가상 머신은에 설명된 대로 Amazon Linux 2를 사용합니다에이전트리스 수집기 배포.

Amazon Linux 2용 라이브 패치를 활성화하고 사용하려면 Amazon EC2 사용 설명서의 AL2의 커널 라이브 패치를 참조하세요.

Agentless Collector 버전 1에서 버전 2로 업그레이드하려면

1. 최신 이미지를 사용하여 새 Agentless Collector OVA를 설치합니다.
2. 보안 인증을 설정합니다.
3. 이전 가상 어플라이언스를 삭제합니다.

에이전트리스 수집기 문제 해결

이 섹션에는 Application Discovery Service Agentless Collector(Agentless Collector)와 관련하여 알려진 문제를 해결하는 데 도움이 되는 주제가 포함되어 있습니다.

주제

- 수정 Unable to retrieve manifest or certificate file error
- WinRM 인증서 구성 시 자체 서명된 인증 문제 해결
- 설정 AWS 중에 에이전트리스 수집기 수정에 도달할 수 없음
- 프록시 호스트에 연결할 때 자체 서명된 인증 문제 해결
- 비정상 수집기 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

- 독립 실행형 ESX 호스트 지원
- Agentless Collector 문제에 대한 AWS 지원 문의

수정 Unable to retrieve manifest or certificate file error

VMware vCenter UI의 Amazon S3 URL에서 OVA를 배포하려고 할 때이 오류가 발생하면 vCenter 서버가 다음 요구 사항을 충족하는지 확인합니다.

- VMware vCenter Server 버전 8.0 업데이트 1 이상
- VMware vCenter Server 7.0 업데이트 3q(ISO 빌드 23788036) 이상

WinRM 인증서 구성 시 자체 서명된 인증 문제 해결

WinRM 인증서 검사를 활성화하면 자체 서명된 인증 기관을 Agentless Collector로 가져와야 할 수 있습니다.

자체 서명된 인증 기관을 가져오려면

1. VMware vCenter에서 수집기의 VM 웹 콘솔을 열고 다음 예제와 `collector` 같이 암호`ec2-user`로 로그인합니다.

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

2. WinRM 인증서에 서명하는 데 사용되는 모든 자체 서명된 CA 인증서가 디렉터리 아래에 있는지 확인합니다`/etc/pki/ca-trust/source/anchors`. 예시:

   ```
   /etc/pki/ca-trust/source/anchors/https-winrm-ca-1.pem
   ```

3. 새 인증서를 설치하려면 다음 명령을 실행합니다.

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

4. 다음 명령을 실행하여 Agentless Collector를 다시 시작합니다.

   ```
   sudo shutdown -r now
   ```

5. (선택 사항) 인증서를 성공적으로 가져왔는지 확인하려면 다음 명령을 실행할 수 있습니다.

```
sudo trust list --filter=ca-anchors | less
```

설정 AWS 중에 에이전트리스 수집기 수정에 도달할 수 없음

Agentless Collector를 사용하려면 TCP 포트 443을 통해 여러 AWS 도메인에 대한 아웃바운드 액세스가 필요합니다. 콘솔에서 Agentless Collector를 구성할 때 다음 오류 메시지가 표시될 수 있습니다.

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

이 오류는 Agentless Collector가 설정 프로세스 중에 수집기가 통신해야 하는 AWS 도메인에 HTTPS 연결을 설정하려는 시도가 실패했기 때문에 발생합니다. 연결을 설정할 수 없는 경우 Agentless Collector 구성이 실패합니다.

에 대한 연결을 수정하려면 AWS

1. IT 관리자에게 문의하여 회사 방화벽이 포트 443에서 아웃바운드 액세스가 필요한 AWS 도메인으로의 아웃바운드 트래픽을 차단하고 있는지 확인합니다. 아웃바운드 액세스가 필요한 AWS 도메인은 홈 리전이 미국 서부(오레곤) 리전, us-west-2 또는 기타 리전인지에 따라 달라집니다.

   AWS 계정 홈 리전이 us-west-2인 경우 다음 도메인에 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`

   다음 도메인은 AWS 계정 홈 리전이가 아닌 경우 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 수집기 구성의 데이터 동기화 섹션에서 프록시 호스트를 구성합니다.

2. 방화벽을 업데이트해도 연결 문제가 해결되지 않는 경우 다음 단계를 사용하여 수집기 가상 머신이 이전 단계에 나열된 도메인에 아웃바운드 네트워크 연결이 되어 있는지 확인합니다.

   a. VMware vCenter에서 Agentless Collector의 IP 주소를 가져옵니다.

   b. 다음 예제와 **`collector`** 같이 수집기의 VM 웹 콘솔을 열고 암호를 **`ec2-user`** 사용하여 로 로그인합니다.

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

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

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

3. 텔넷이 도메인을 확인할 수 없는 경우 Amazon Linux 2에 대한 지침을 사용하여 정적 DNS 서버를 구성해 보세요.
4. 오류가 계속되면 추가 지원은 섹션을 참조하세요Agentless Collector 문제에 대한 AWS 지원 문의.

프록시 호스트에 연결할 때 자체 서명된 인증 문제 해결

선택적으로 제공된 프록시와의 통신이 HTTPS를 통해 이루어지고 프록시에 자체 서명된 인증서가 있는 경우 인증서를 제공해야 할 수 있습니다.

1. VMware vCenter에서 Agentless Collector의 IP 주소를 가져옵니다.
2. 다음 예제와 `collector` 같이 수집기의 VM 웹 콘솔을 열고 암호`ec2-user`로 로그인합니다.

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

3. `-----BEGIN CERTIFICATE-----` 및를 포함하여 보안 프록시와 연결된 인증서의 본문을 `-----END CERTIFICATE-----`다음 파일에 붙여 넣습니다.

   ```
   /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 Agentless Collector를 다시 시작합니다.

```
sudo shutdown -r now
```

비정상 수집기 찾기

모든 수집기의 상태 정보는 AWS Migration Hub (Migration Hub) 콘솔의 데이터 수집기 페이지에 있습니다. 상태가 주의 필요인 수집기를 찾아 문제가 있는 수집기를 식별할 수 있습니다.

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

Agentless Collector 콘솔에 액세스하려면

1. AWS 계정을 사용하여에 로그인 AWS Management Console 하고 https://console.aws.amazon.com/migrationhub/ Migration Hub 콘솔을 엽니다.
2. Migration Hub 콘솔 탐색 창의 검색에서 데이터 수집기를 선택합니다.
3. Agentless 수집기 탭에서 상태가 주의 필요인 각 커넥터의 IP 주소를 기록해 둡니다.
4. Agentless Collector 콘솔을 열려면 웹 브라우저를 엽니다. 그런 다음 주소 표시줄에 **https://***<ip_address>***/** URL을 입력합니다. 여기서 ip_address는 비정상 수집기의 IP 주소입니다.
5. 로그인을 선택한 다음에서 수집기가 구성될 때 설정된 Agentless Collector 암호를 입력합니다에이전트리스 수집기 구성.
6. Agentless Collector 대시보드 페이지의 데이터 수집에서 VMware vCenter 섹션에서 보기 및 편집을 선택합니다.
7. 의 지침에 따라 URL과 자격 증명을 VMware vCenter 자격 증명 편집 수정합니다.

상태 문제를 해결하면 수집기가 vCenter 서버와의 연결을 다시 설정하고 수집기의 상태가 수집 중 상태로 변경됩니다. 문제가 지속되면 섹션을 참조하세요Agentless Collector 문제에 대한 AWS 지원 문의.

비정상 수집기의 가장 일반적인 원인은 IP 주소 및 자격 증명 문제입니다. IP 주소 문제 해결 및는 이러한 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 엔드포인트의 형식이 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.

수집기 IP 주소 문제를 해결하려면

1. VMware vCenter에서 Agentless Collector의 IP 주소를 가져옵니다.
2. 웹 브라우저를 열어 Agentless Collector 콘솔을 연 다음 주소 표시줄에 **`https://`***`<ip_address>`***`/`** URL을 입력합니다. 여기서 ip_address는에서 수집기의 IP 주소입니다에이전트리스 수집기 배포.
3. 로그인을 선택한 다음에서 수집기가 구성될 때 설정된 Agentless Collector 암호를 입력합니다에이전트리스 수집기 구성.
4. Agentless Collector 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` 또는와 같은 별도의 명령줄 도구를 사용하여 연결된 vCenter 서버가 활성 상태이고 수집기 VM에서 IP에 연결할 수 있는지 `traceroute`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 수집기 VM에서 들어오는 연결을 허용하도록 방화벽 설정을 업데이트합니다.

vCenter 자격 증명 문제 해결

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

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

vCenter 자격 증명 편집에 대한 자세한 내용은 섹션을 참조하세요VMware vCenter 자격 증명 편집.

데이터베이스 및 분석 데이터 수집 모듈의 데이터 전달 문제 해결

Agentless Collector의 데이터베이스 및 분석 데이터 수집 모듈의 홈 페이지에는 DMS에 대한 액세스 및 S3에 대한 액세스의 연결 상태가 표시됩니다. DMS 액세스 및 S3 액세스에 대한 액세스 없음이 표시되면 데이터 전달을 구성합니다. 자세한 내용은 데이터 전달 구성 단원을 참조하십시오.

데이터 전달을 구성한 후이 문제가 발생하면 데이터 수집 모듈이 인터넷에 액세스할 수 있는지 확인합니다. 그런 다음 IAM 사용자에게 DMSCollectorPolicy 및 FleetAdvisorS3Policy 정책을 추가했는지 확인합니다. 자세한 내용은 Application Discovery Service Agentless Collector 배포 단원을 참조하십시오.

데이터 수집 모듈이에 연결할 수 없는 AWS경우 다음 도메인에 대한 아웃바운드 액세스를 제공합니다.

- `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 환경에서 OS 서버를 검색합니다. 그런 다음 데이터 수집 모듈은 OS 서버에 연결하여 데이터베이스 및 분석 서버를 검색합니다. 이러한 데이터베이스 서버에서 데이터 수집 모듈은 용량 및 성능 지표를 수집합니다. 데이터 수집 모듈이 이러한 서버에 연결할 수 없는 경우 서버에 연결할 수 있는지 확인합니다.

다음 예제에서는 *## ###* 값을 값으로 바꿉니다.

- LDAP 서버에 연결할 수 있는지 확인하려면 `ldap-util` 패키지를 설치합니다. 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 사용합니다.

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

Windows에서 이전 예제를 관리자로 실행합니다.

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

Linux에서 이전 예제를 실행합니다.

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

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

Windows에서 이전 예제를 관리자로 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]"
```

Linux에서 이전 예제를 실행합니다.

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

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

- MySQL 데이터베이스에 연결할 수 있는지 확인하려면 다음 명령을 사용합니다.

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

- Oracle 데이터베이스에 연결할 수 있는지 확인하려면 다음 명령을 사용합니다.

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

- PostgreSQL 데이터베이스에 연결할 수 있는지 확인하려면 다음 명령을 사용합니다.

```
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 내용은 데이터베이스 서버 검색 단원을 참조하십시오.

독립 실행형 ESX 호스트 지원

Agentless Collector는 독립 실행형 ESX 호스트를 지원하지 않습니다. ESX 호스트는 vCenter Server 인스턴스의 일부여야 합니다.

Agentless Collector 문제에 대한 AWS 지원 문의

Application Discovery Service Agentless Collector(Agentless Collector)에 문제가 발생하여 도움이 필요한 경우 AWS Support에 문의하세요. 연락이 되면 수집기 로그를 보내라는 메시지가 표시될 수 있습니다.

Agentless Collector 로그를 가져오려면

1. VMware vCenter에서 Agentless Collector의 IP 주소를 가져옵니다.
2. 다음 예제와 **`collector`** 같이 수집기의 VM 웹 콘솔을 열고 암호를 **`ec2-user`** 사용하여 로 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. Agentless Collector VM에서 로그 파일을 복사합니다.

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

6. AWS Enterprise Support에 `tar.gz` 파일을 제공합니다.

Migration Hub로 데이터 가져오기

AWS Migration Hub (Migration Hub) 가져오기를 사용하면 Application Discovery Service Agentless Collector(Agentless Collector) 또는 AWS Application Discovery Agent(Discovery Agent)를 사용하지 않고도 온프레미스 환경의 세부 정보를 Migration Hub로 직접 가져올 수 있으므로 가져온 데이터에서 직접 마이그레이션 평가 및 계획을 수행할 수 있습니다. 디바이스를 애플리케이션으로 그룹화하고 해당 마이그레이션 상태를 추적할 수도 있습니다.

이 페이지에서는 가져오기 요청을 완료하는 단계를 설명합니다. 먼저 다음 두 옵션 중 하나를 사용하여 온프레미스 서버 데이터를 준비합니다.

- 일반적인 타사 도구를 사용하여 온프레미스 서버 데이터가 포함된 파일을 생성합니다.
- CSV(쉼표로 구분된 값) 가져오기 템플릿을 다운로드하여 온프레미스 서버 데이터로 채웁니다.

앞서 설명한 두 가지 방법 중 하나를 사용하여 온프레미스 데이터 파일을 생성한 후 Migration Hub 콘솔 AWS CLI또는 SDK 중 하나를 사용하여 Migration Hub에 AWS 파일을 업로드합니다. SDKs 두 옵션에 대한 자세한 내용은 단원을 참조하십시오the section called “지원되는 가져오기 형식”.

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 콘솔 내에서 직접 사용률 데이터, 태그 및 애플리케이션 매핑을 봅니다. 가져오는 동안 오류가 발생할 경우 성공한 레코드와 실패한 레코드 수 및 실패한 각 레코드에 대한 오류 세부 정보를 검토할 수 있습니다.

오류 처리: 압축된 아카이브에서 오류 로그와 실패한 레코드 파일을 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 내용은 AWS Application Discovery Service 할당량 단원을 참조하십시오.

지원되는 가져오기 형식

Migration Hub는 다음과 같은 가져오기 형식을 지원합니다.

- RVTools
- Migration Hub 가져오기 템플릿

RVTools

Migration Hub는 RVTools를 통해 VMware vSphere의 내보내기 가져오기를 지원합니다. RVTools에서 데이터를 저장할 때 먼저 모두 csv로 내보내기 옵션 또는 모두 Excel로 내보내기 옵션을 선택한 다음 폴더를 ZIP하고 ZIP 파일을 Migration Hub로 가져옵니다. ZIP에는 vInfo, vNetwork, vCpu, vMemory, vDisk, vPartition, vSource, vTools, vHost, vNic, vSC_VMK 파일이 필요합니다.

Migration Hub 가져오기 템플릿

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 표의 가져오기 필드 이름 옆에 있는 별표(*)는 필수 필드임을 나타냅니다. 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.

다음 표의 가져오기 파일 이름 옆에 있는 캐럿(^)은 serverId가 제공된 경우 읽기 전용임을 나타냅니다.

> **Note**
>
> 레코드를 식별하기 위해 VMware.MoRefId 또는 VMware.VCenterId를 사용할 경우 동일한 레코드에 두 필드가 있어야 합니다.

가져오기 필드 이름	설명	예시
ExternalId*^	각 레코드를 고유하게 표시할 수 있는 사용자 정의 식별자입니다. 예를 들어 ExternalId는 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"

가져오기 필드 이름	설명	예시
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.VCenterId를 제공해야 합니다.	
VMware.VCenterId*^	가상 머신 고유 식별자. VMware.MoRefId를 제공해야 합니다.	
CPU.NumberOfProcessors^	CPU 수입니다.	4
CPU.NumberOfCores^	물리적 코어 총수	8
CPU.NumberOfLogicalCores^	서버의 모든 CPUs에서 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

가져오기 필드 이름	설명	예시
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.Avg^	검색 도구가 데이터를 수집할 때의 평균 CPU 사용률.	45 23.9
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

가져오기 필드 이름	설명	예시
DiskReadsOpsPerSecond.Avg^	초당 평균 디스크 I/O 연산 수.	45 28
DiskWritesOpsPerSecond.Avg^	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
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
Applications	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"

가져오기 필드 이름	설명	예시
ApplicationWave	이 서버의 마이그레이션 웨이브입니다.	
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"
ServerId	Migration Hub 서버 목록에 표시된 서버 식별자입니다.	`d-server-01kk9i6ywwaxmp`

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 애플리케이션에 대한 일치 로직 단원을 참조하십시오.

Note

Migration Hub 가져오기는 가져오기 템플릿에 정의된 필드 이외의 필드는 지원하지 않습니다. 제공한 사용자 지정 필드는 무시되며 가져오지 않습니다.

가져오기 권한 설정

데이터를 가져오기 전에 IAM 사용자에게 가져오기 파일을 Amazon S3에 업로드(`s3:PutObject`)하고 객체()를 읽는 데 필요한 Amazon S3 권한이 있는지 확인합니다`s3:GetObject`. 또한 IAM 정책을 생성하고 AWS 계정에서 가져오기를 수행하는 IAM 사용자에게 연결하여 프로그래밍 방식 액세스(용 AWS CLI) 또는 콘솔 액세스를 설정해야 합니다.

Console Permissions

다음 절차에 따라 콘솔을 사용하여 AWS 계정에서 가져오기 요청을 수행할 IAM 사용자의 권한 정책을 편집합니다.

사용자의 연결된 관리형 정책을 편집하려면

1. 에 로그인 AWS Management Console 하고 https://console.aws.amazon.com/iam/://https://https://https://https://https://://https://://https://://https://://https://https://://https
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 검토를 선택합니다.

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

d. 정책 생성을 선택합니다.

6. 계정 AWS 에서 가져오기 요청을 할 사용자의 권한 부여 IAM 콘솔 페이지로 돌아갑니다.
7. 정책 테이블을 새로 고치고 방금 생성한 정책의 이름을 검색합니다.
8. 다음: 검토를 선택합니다.
9. 권한 추가를 선택합니다.

IAM 사용자에게 정책을 추가했으므로 이제 가져오기 프로세스를 시작할 준비가 되었습니다.

AWS CLI Permissions

다음 절차에 따라 IAM 사용자에게를 사용하여 데이터 가져오기 요청을 수행할 수 있는 권한을 부여하는 데 필요한 관리형 정책을 생성합니다 AWS CLI.

관리형 정책을 생성하고 연결하려면

1. `aws iam create-policy` AWS CLI 명령을 사용하여 다음 권한이 있는 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 명령 사용에 대한 자세한 내용은 명령 참조의 create-policy를 AWS CLI 참조하세요.

2. `aws iam create-policy` AWS CLI 명령을 사용하여 다음 권한을 가진 추가 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. `aws iam attach-user-policy` AWS CLI 명령을 사용하여를 사용하여 계정 AWS 에서 가져오기 요청을 수행할 IAM 사용자에게 이전 두 단계에서 생성한 정책을 연결합니다 AWS CLI. 이 명령 사용에 대한 자세한 내용은 명령 참조의 attach-user-policy를 AWS CLI 참조하세요.

IAM 사용자에게 정책을 추가했으므로 이제 가져오기 프로세스를 시작할 준비가 되었습니다.

IAM 사용자가 지정한 Amazon S3 버킷에 객체를 업로드할 때 사용자가 객체를 읽을 수 있도록 설정된 객체에 대한 기본 권한을 그대로 두어야 합니다.

Amazon S3에 가져오기 파일 업로드

다음으로 CSV 형식의 가져오기 파일을 Amazon S3에 업로드해야 가져올 수 있습니다. 시작하기 전에 미리 생성 및/또는 선택한 가져오기 파일을 보관할 Amazon S3 버킷이 있어야 합니다.

Console S3 Upload

Amazon S3에 가져오기 파일을 업로드하려면

1. 에 로그인 AWS Management Console 하고 https://console.aws.amazon.com/s3/://https://https://https://://https://://https://://https://://https://://httpsAmazon S3://://://https://://://https://://://://https
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. 에 설명된 대로 Migration Hub 콘솔의 가져오기 페이지로 이동합니다데이터 가져오기. 그런 다음 Amazon S3 객체 URL 필드에 객체 URL을 붙여 넣습니다.

AWS CLI S3 Upload

Amazon S3에 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. 가져오기 요청을 생성할 때이 정보가 필요합니다.

데이터 가져오기

Migration Hub 콘솔에서 가져오기 템플릿을 다운로드하고 기존 온프레미스 서버 데이터로 채운 후에는 데이터를 Migration Hub로 가져올 준비가 된 것입니다. 다음 지침에서는 콘솔을 사용하거나를 통해 API를 호출하여 이를 수행하는 두 가지 방법을 설명합니다 AWS CLI.

Console Import

Migration Hub 콘솔의 도구 페이지에서 데이터 가져오기를 시작합니다.

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 버킷의 가져오기 템플릿을 https://s3.us-west-2.amazonaws.com/templates-7cffcf56-bd96-4b1c-b45b-a5b42f282e46/import_template.csv://https://https://https://https://https://https://https://https://https://https://https://https://
3. 가져오기 페이지를 열려면 가져오기 상자에서 가져오기를 선택합니다.
4. 가져오기 이름에서 가져오기 이름을 지정합니다.
5. Amazon S3 객체 URL 필드를 작성합니다. 이 단계를 수행하려면 가져오기 데이터 파일을 Amazon S3에 업로드해야 합니다. 자세한 내용은 Amazon S3에 가져오기 파일 업로드 단원을 참조하십시오.
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. 이름 열에 나열된 가져오기 이름을 선택하여 가져오기(가져오기 기록) 페이지에서 이동하면 선택한 가져오기의 데이터 세트를 기반으로 필터가 적용되는 서버 페이지로 이동합니다. 그러면 해당 특정 가져오기에 속한 데이터만 표시됩니다.

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

에서 데이터 가져오기 프로세스를 시작하려면 먼저 환경에 AWS CLI를 설치해야 AWS CLI 합니다. 자세한 내용은 AWS Command Line Interface 사용 설명서의 AWS 명령줄 인터페이스 설치를 참조하세요.

> **Note**
>
> 아직 가져오기 템플릿을 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

콘솔 AWS CLI또는 AWS SDKs.

Console Tracking

Migration Hub 콘솔의 가져오기 대시보드에서 다음 요소를 찾을 수 있습니다.

- 이름 - 가져오기 요청의 이름입니다.
- 가져오기 ID - 가져오기 요청의 고유 ID입니다.
- 가져오기 시간 - 가져오기 요청이 생성된 날짜 및 시간입니다.
- 가져오기 상태 - 가져오기 요청의 상태입니다. 다음 값 중 하나일 수 있습니다:
  - 가져오기 -이 데이터 파일을 현재 가져오고 있습니다.
  - 가져오기 - 전체 데이터 파일을 성공적으로 가져왔습니다.
  - 오류와 함께 가져오기 - 데이터 파일의 레코드 중 하나 이상을 가져오지 못했습니다. 실패한 레코드를 해결하려면 가져오기 작업에 대해 레코드를 다운로드하지 못함을 선택하고 실패한 항목 csv 파일의 오류를 해결한 후 다시 가져오기를 수행합니다.
  - 가져오기 실패 - 가져온 데이터 파일의 레코드가 없습니다. 실패한 레코드를 해결하려면 가져오기 작업에 대해 레코드를 다운로드하지 못함을 선택하고 실패한 항목 csv 파일의 오류를 해결한 후 다시 가져오기를 수행합니다.
- 가져온 레코드 - 성공적으로 가져온 특정 데이터 파일의 레코드 수입니다.
- 실패한 레코드 - 가져오지 않은 특정 데이터 파일의 레코드 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 실패한 가져오기 레코드 문제 해결 단원을 참조하십시오.

검색된 데이터 보기 및 탐색

Application Discovery Service Agentless Collector(Agentless Collector)와 AWS Discovery Agent(Discovery Agent)는 모두 평균 및 최대 사용률을 기반으로 시스템 성능 데이터를 제공합니다. 수집된 시스템 성능 데이터를 사용하여 높은 수준의 총 소유 비용(TCO)을 수행할 수 있습니다. Discovery Agents는 시스템 성능 정보, 인바운드 및 아웃바운드 네트워크 연결, 서버에서 실행되는 프로세스에 대한 시계열 데이터를 포함하여 더 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 모두에서 Agentless Collector 및 Discovery Agent가 검색한 데이터를 보고 작업하는 방법에 대한 지침을 제공합니다 AWS CLI.

주제

- Migration Hub 콘솔을 사용하여 수집된 데이터 보기
- Amazon Athena에서 데이터 탐색

Migration Hub 콘솔을 사용하여 수집된 데이터 보기

Application Discovery Service Agentless Collector(Agentless Collector)와 AWS Discovery Agent(Discovery Agent) 모두에서 데이터 수집 프로세스가 시작된 후 콘솔을 사용하여 서버 및 VMs에 대해 수집된 데이터를 볼 수 있습니다. 데이터는 데이터 수집이 시작된 후 약 15분 후에 콘솔에 표시됩니다. 를 사용하여 API를 호출하여 수집된 데이터를 내보내면이 데이터를 CSV 형식으로 볼 수도 있습니다 AWS CLI.

콘솔에서 검색된 서버에 대해 수집된 데이터를 보려면의 단계를 따릅니다AWS Migration Hub 콘솔에서 서버 보기. 콘솔을 사용하여 Agentless Collectors 또는 Discovery Agents에서 검색한 서버를 보고, 정렬하고, 태그를 지정하는 방법에 대한 자세한 내용은 섹션을 참조하세요AWS Migration Hub 콘솔을 사용하여 데이터 검색.

Agentless Collector 데이터베이스 및 분석 데이터 수집 모듈은 수집된 데이터를 Amazon S3 버킷에 업로드합니다. AWS DMS 콘솔에서이 버킷의 데이터를 볼 수 있습니다. 검색된 데이터베이스 및 분석 서버에 대해 수집된 데이터를 보려면의 단계를 따릅니다수집된 데이터 보기.

검색된 서버 및 애플리케이션에 대한 일치 로직

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

이 매칭 로직은 (Migration Hub) 가져오기, Application Discovery Service Agentless Collector(Agentless Collector), AWS Application Discovery Agent(Discovery Agent) 및 기타 마이그레이션 도구를 포함한 AWS Migration Hub 여러 소스의 중복 서버를 처리합니다. Migration Hub 가져오기에 대한 자세한 내용은 Migration Hub 가져오기를 참조하세요.

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 콘솔에서이 서버를 볼 때 서버에 대한 고유한 항목 하나만 찾을 수 있습니다.

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.

일치하는 필드

다음 필드는 검색 도구 사용 시 서버를 일치시키는 데 사용됩니다.

- ExternalId - 서버를 일치시키는 데 사용되는 기본 필드입니다. 이 필드의 값이 `ExternalId` 다른 항목의 값과 동일한 경우 Application Discovery Service는 다른 필드의 일치 여부에 관계없이 두 항목을 일치시킵니다.
- IPAddress
- HostName
- MacAddress
- VMware.MoRefId 및 VMware.vCenterId - Application Discovery Service가 일치를 수행하려면이 두 값이 다른 항목의 각 필드와 동일해야 합니다.

Amazon Athena에서 데이터 탐색

Amazon Athena에서 데이터를 탐색하면 Discovery Agent가 검색한 모든 온프레미스 서버에서 수집한 데이터를 한 곳에서 분석할 수 있습니다. Amazon Athena의 데이터 탐색이 Migration Hub 콘솔에서 활성화되고(또는 StartContinousExport API를 사용하여) 에이전트에 대한 데이터 수집이 활성화되면 에이전트가 수집한 데이터는 정기적으로 S3 버킷에 자동으로 저장됩니다. 자세한 내용은 Amazon Athena에서 데이터 탐색 단원을 참조하십시오.

Amazon Athena에서 데이터를 탐색하면 Discovery Agents가 검색한 모든 온프레미스 서버에서 수집한 데이터를 한 곳에서 분석할 수 있습니다. Amazon Athena에서 데이터 탐색이 Migration Hub 콘솔에서 활성화되고(또는 StartContinousExport API를 사용하여) 에이전트에 대한 데이터 수집이 활성화되면 에이전트가 수집한 데이터가 정기적으로 S3 버킷에 자동으로 저장됩니다.

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

이 섹션의 주제에서는 Athena에서 데이터를 사용하여 로컬 환경을 평가하고 마이그레이션할 계획을 세우는 방법을 설명합니다 AWS.

Amazon Athena에서 데이터 탐색 켜기

Amazon Athena의 데이터 탐색은 Migration Hub 콘솔 또는의 API 직접 호출을 사용하여 연속 내보내기를 켜면 활성화됩니다 AWS CLI. Amazon Athena에서 검색된 데이터를 보고 탐색을 시작하려면 먼저 데이터 탐색을 켜야 합니다.

지속적 내보내기를 켜면 계정에서 서비스 연결 역할`AWSServiceRoleForApplicationDiscoveryServiceContinuousExport`이 자동으로 사용됩니다. 이 서비스 연결 역할에 대한 자세한 내용은 Application Discovery Service에 대한 서비스 연결 역할 권한 단원을 참조하십시오.

다음 지침은 콘솔 및를 사용하여 Amazon Athena에서 데이터 탐색을 활성화하는 방법을 보여줍니다 AWS CLI.

Turn on with the console

"데이터 수집 시작"Amazon Athena 선택하거나 Migration Hub 콘솔의 Data Collectors 페이지에서 "Amazon Athena의 데이터 탐색"이라는 레이블이 지정된 토글을 클릭하면 암시적으로 연속 내보내기를 켜면 Amazon Athena의 데이터 탐색이 활성화됩니다.

콘솔에서 Amazon Athena의 데이터 탐색을 켜려면

1. 탐색 창에서 Data Collectors(데이터 수집기)를 선택합니다.
2. 에이전트 탭을 선택합니다.
3. 데이터 수집 시작을 선택하거나 데이터 수집이 이미 켜져 있는 경우 Amazon Athena에서 데이터 탐색 토글을 클릭합니다.
4. 이전 단계에서 생성된 대화 상자에서 관련 비용에 대해 동의하는 확인란을 클릭하고 계속 또는 활성화를 선택합니다.

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

Enable with the AWS CLI

Amazon Athena의 데이터 탐색은의 API 호출을 통해 명시적으로 설정된 Continuous Export를 통해 활성화됩니다 AWS CLI. 이렇게 하려면 먼저 환경에를 설치해야 AWS CLI 합니다.

Amazon Athena에서를 설치하고 데이터 탐색을 AWS CLI 켜려면

1. 운영 체제(Linux, macOS 또는 Windows) AWS CLI 용를 설치합니다. 지침은 AWS Command Line Interface 사용 설명서를 참조하세요.
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 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 실행되어 Amazon Athena에서 검색된 데이터를 보고 작업할 수 있습니다. 이 기능을 처음 활성화하면 데이터가 Amazon Athena에 표시되는 데 최대 30분이 걸릴 수 있습니다.

Amazon Athena에서 직접 데이터 탐색

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

다음 지침에서는 Athena 콘솔에서 직접 에이전트 데이터를 탐색하는 방법을 설명합니다. Athena에 데이터가 없거나 Amazon Athena에서 데이터 탐색을 활성화하지 않은 경우에 설명된 대로 Amazon Athena에서 데이터 탐색을 활성화하라는 대화 상자가 표시됩니다Amazon Athena에서 데이터 탐색 켜기.

Athena에서 에이전트가 검색한 데이터를 직접 탐색하려면

1. AWS Migration Hub 콘솔의 탐색 창에서 서버를 선택합니다.
2. Amazon Athena 콘솔을 열려면 Amazon Athena에서 데이터 탐색을 선택합니다.
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 Amazon Athena에서 사전 정의된 쿼리 사용 단원을 참조하십시오.

Amazon Athena 데이터 시각화

데이터를 시각화하기 위해 Amazon QuickSight와 같은 시각화 프로그램이나 사이토스케이프, yEd 또는 Gelphi와 같은 기타 오픈 소스 시각화 도구로 쿼리를 포팅할 수 있습니다. 이러한 도구를 사용하여 네트워크 다이어그램, 요약 차트 및 기타 그래픽을 렌더링할 수 있습니다. 이 방법을 사용하면 수집된 데이터에 소스로 액세스하여 시각화를 생성할 수 있도록 시각화 프로그램을 통해 Athena에 연결합니다.

QuickSight를 사용하여 Amazon Athena 데이터를 시각화하려면

1. Amazon QuickSight에 로그인합니다.
2. Connect to another data source or upload a file(다른 데이터 원본에 연결 또는 파일 업로드)을 선택합니다.
3. Athena를 선택합니다. 새 Athena 데이터 소스 대화 상자가 표시됩니다.
4. Data source name(데이터 원본 이름) 필드에 이름을 입력합니다.
5. 데이터 소스 생성을 선택합니다.
6. 테이블 선택 대화 상자에서 Agents-servers-os 테이블을 선택한 후 선택을 선택합니다.
7. 데이터 세트 생성 완료 대화 상자에서 더 빠른 분석을 위해 SPICE로 가져오기를 선택한 다음 시각화를 선택합니다.

   시각화가 렌더링됩니다.

Amazon Athena에서 사전 정의된 쿼리 사용

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 콘솔의 탐색 창에서 서버를 선택합니다.
2. Amazon Athena 콘솔을 열려면 Amazon Athena에서 데이터 탐색을 선택합니다.
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. 뷰를 생성하는 방법에 대한 자세한 내용은 Amazon Athena 사용 설명서의 CREATE VIEW를 참조하세요.

```
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 데이터 분석

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 통신 추적

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 가져오기 테이블 생성 단원을 참조하십시오.

iana_service_ports_import 테이블이 생성되었으면 아웃바운드 트래픽을 추적하기 위한 두 가지 보기 헬퍼 함수를 생성합니다. 뷰를 생성하는 방법에 대한 자세한 내용은 Amazon Athena 사용 설명서의 CREATE VIEW를 참조하세요.

아웃바운드 추적 헬퍼 함수를 생성하려면

1. https://console.aws.amazon.com/athena/에서 Athena 콘솔을 엽니다.
2. 모든 개별 아웃바운드 대상 IP 주소를 나열하는 다음 헬퍼 함수를 사용하여 `valid_outbound_ips_helper` 뷰를 생성합니다.

```
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 통신 추적

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 가져오기 테이블 생성 단원을 참조하십시오.

`iana_service_ports_import` 테이블이 생성되었으면 인바운드 트래픽을 추적하기 위한 두 가지 보기 헬퍼 함수를 생성합니다. 뷰를 생성하는 방법에 대한 자세한 내용은 Amazon Athena 사용 설명서의 CREATE VIEW를 참조하세요.

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 가져오기 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 가져오기 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.org 서비스 이름 및 전송 프로토콜 포트 번호 레지스트리에서 IANA 포트 레지스트리 데이터베이스 CSV 파일을 다운로드합니다.
2. Amazon S3로 파일을 업로드합니다. 자세한 내용은 S3 버킷에 파일 및 폴더를 업로드하려면 어떻게 해야 합니까?를 참조하십시오.
3. Athena에서 라는 새 테이블을 생성합니다`iana_service_ports_import`. 지침은 Amazon Athena 사용 설명서의 테이블 생성을 참조하세요. 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 Migration Hub 콘솔을 사용하여 데이터 검색

AWS Application Discovery Service (Application Discovery Service)는 AWS Migration Hub (Migration Hub)와 통합되며 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 작업하는 경우 추가 단계나 설정이 필요하지 않습니다.

이 섹션에서는 콘솔을 사용하여 Application Discovery Service Agentless Collector(Agentless Collector) 및 AWS Application Discovery Agent(Discovery Agent)를 관리하고 모니터링하는 방법을 찾을 수 있습니다.

주제

AWS Migration Hub 콘솔 대시보드에서 데이터 보기

기본 대시보드를 보려면 (Migration Hub) 콘솔 탐색 창에서 대시보드를 AWS Migration Hub 선택합니다. Migration Hub 기본 대시보드에서 Application Discovery Service Agentless Collector(Agentless Collector) 및 Application Discovery Agent(Discovery Agent)와 같은 서버, AWS 애플리케이션 및 데이터 수집기에 대한 상위 수준 통계를 볼 수 있습니다.

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 Migration Hub 콘솔 홈페이지 왼쪽에 있는 탐색 창에서 대시보드를 선택합니다.

AWS Migration Hub 콘솔에서 데이터 수집기 시작 및 중지

Application Discovery Service Agentless Collector(Agentless Collector) 및 AWS Application Discovery Agent(Discovery Agent)는 AWS Application Discovery Service (Application Discovery Service)가 기존 인프라를 검색하는 데 사용하는 데이터 수집 도구입니다. 다음 단계에서는 이러한 검색 데이터 수집 도구 에이전트리스 수집기 배포 및를 다운로드하고 배포하는 방법을 설명합니다AWS 애플리케이션 검색 에이전트.

이러한 데이터 수집 도구는 Application Discovery Service의 리포지토리에 데이터를 저장하여 각 서버와 해당 서버에서 실행되는 프로세스에 대한 세부 정보를 제공합니다. 이러한 도구 중 하나가 배포되면 AWS Migration Hub (Migration Hub) 콘솔에서 수집된 데이터를 시작, 중지 및 볼 수 있습니다.

AWS Application Discovery Agent(Discovery Agent)가 배포된 후 (Migration Hub) 콘솔의 Data Collectors 페이지에서 데이터 수집 프로세스를 시작하거나 중지할 AWS Migration Hub 수 있습니다.

데이터 수집 도구 시작 및 중지

1. AWS 계정을 사용하여에 로그인 AWS Management Console 하고 https://console.aws.amazon.com/migrationhub/ Migration Hub 콘솔을 엽니다.
2. Migration Hub 콘솔 탐색 창의 검색에서 데이터 수집기를 선택합니다.
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.

콘솔에서 AWS Migration Hub 데이터 수집기 정렬

많은 데이터 수집기를 배포한 경우 콘솔의 데이터 수집기 페이지에서 배포된 수집기의 표시된 목록을 정렬할 수 있습니다. 검색 창에 필터를 적용하여 목록을 정렬합니다. Data Collectors(데이터 수집기) 목록에서 정의한 기준 대부분에 대해 검색 및 필터링을 할 수 있습니다.

다음 표에는 연산자, 값 및 값 정의를 포함하여 에이전트에 사용할 수 있는 검색 기준이 나와 있습니다.

검색 기준	연산자	값: 정의
에이전트 ID	==	컬렉션 도구가 설치된 미리 채워진 목록에서 선택한 모든 에이전트 ID입니다.

검색 기준	연산자	값: 정의
Hostname	== !=	에이전트의 경우, 에이전트가 설치된 호스트의 미리 채워진 목록에서 선택한 호스트 이름입니다.
수집 상태	== !=	시작됨: 데이터를 수집하여 Application Discovery Service로 전송 중 예약된 시작: 데이터 수집 시작이 예약되었습니다. 데이터는 다음 ping 시 Application Discovery Service로 전송되고 상태가 시작됨으로 변경됩니다. 중지됨: 데이터가 수집되지 않거나 Application Discovery Service로 전송되지 않습니다. 예약된 중지: 데이터 수집 중지가 예약되었습니다. 데이터는 다음 ping 시 Application Discovery Service로 전송되지 않으며 상태가 중지됨으로 변경됩니다.

검색 기준	연산자	값: 정의
상태	== !=	정상: 데이터 수집이 활성화되어 있지 않습니다. 도구는 정상 작동하고 있습니다. 이상 있음: 도구가 오류 상태입니다. 데이터 수집 및 보고가 되지 않습니다. 알 수 없음: 한 시간 이상 연결이 수립되지 않았습니다. 종료: 도구가 시스템 서비스나 데몬 종료 때문에 '종료'를 통신했습니다. 재부팅이나 도구 업그레이드의 경우, 상태가 첫 보고 주기에 다른 상태로 변경됩니다. 실행: 데이터 수집이 활성화되어 있습니다. 도구는 정상 작동하고 있습니다.
IP 주소	== !=	수집 도구가 설치된 미리 채워진 목록에서 선택한 IP 주소입니다.

다음 표에는 연산자, 값 및 값 정의를 포함하여 Agentless 수집기에 사용할 수 있는 검색 기준이 나와 있습니다.

검색 기준	연산자	값: 정의
ID	==	수집 도구가 설치된 미리 채워진 목록에서 선택한 에이전트 없는 수집기 ID입니다.

검색 기준	연산자	값: 정의
Hostname	== !=	에이전트리스 수집기의 경우 에이전트리스 수집기가 설치된 호스트의 미리 채워진 목록에서 선택한 모든 호스트 이름입니다.
상태 표시기	== !=	데이터 수집: 데이터 수집이 켜져 있습니다. 도구는 정상 작동하고 있습니다. 구성 준비 완료 - 데이터 수집이 켜져 있지 않습니다. 도구는 정상 작동하고 있습니다. 주의 필요 - 도구가 오류 상태이고 주의가 필요합니다. 알 수 없음: 한 시간 이상 연결이 수립되지 않았습니다. 종료: 도구에서 시스템, 서비스 또는 데몬 종료로 인해 마지막으로 "종료"를 전달했습니다. 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. AWS 계정을 사용하여에 로그인 AWS Management Console 하고 https://console.aws.amazon.com/migrationhub/ Migration Hub 콘솔을 엽니다.
2. Migration Hub 콘솔 탐색 창의 검색에서 데이터 수집기를 선택합니다.

3. 에이전트리스 수집기 또는 에이전트 탭을 선택합니다.
4. 검색 창 안을 클릭한 다음 목록에서 검색 기준을 선택합니다.
5. 다음 목록에서 연산자를 선택합니다.
6. 마지막 목록에서 값을 선택합니다.

AWS Migration Hub 콘솔에서 서버 보기

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.

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

검색된 서버 보기

1. AWS 계정을 사용하여에 로그인 AWS Management Console 하고 https://console.aws.amazon.com/migrationhub/ Migration Hub 콘솔을 엽니다.
2. Migration Hub 콘솔 탐색 창의 검색에서 서버를 선택합니다. 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 AWS Migration Hub 를 사용하여 서버 데이터 내보내기를 참조하십시오.

AWS Migration Hub 콘솔에서 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. AWS 계정을 사용하여에 로그인 AWS Management Console 하고 https://console.aws.amazon.com/migrationhub/ Migration Hub 콘솔을 엽니다.
2. Migration Hub 콘솔 탐색 창의 검색에서 서버를 선택합니다.

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.

AWS Migration Hub 콘솔에서 서버 태그 지정

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. 단일 작업으로 개별 서버 또는 여러 서버에 태그를 지정할 수 있습니다 AWS Application Discovery Service (Application Discovery Service) 태그는 AWS 태그와 유사하지만 두 가지 유형의 태그를 서로 바꿔 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. AWS 계정을 사용하여에 로그인 AWS Management Console 하고 https://console.aws.amazon.com/migrationhub/ Migration Hub 콘솔을 엽니다.
2. Migration Hub 콘솔 탐색 창의 검색에서 서버를 선택합니다.
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. 태그 추가를 선택한 다음 새 태그 추가를 선택합니다.
5. 대화 상자에서 키 필드에 키를 입력하고 선택적으로 값 필드에 값을 입력합니다.

   새 태그 추가를 선택하고 추가 정보를 추가하여 태그를 더 추가합니다.
6. 저장(Save)을 선택합니다.

하나 이상의 서버에서 태그 제거

1. AWS 계정을 사용하여에 로그인 AWS Management Console 하고 https://console.aws.amazon.com/migrationhub/ Migration Hub 콘솔을 엽니다.

2. Migration Hub 콘솔 탐색 창의 검색에서 서버를 선택합니다.
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. 태그 제거를 선택합니다.
5. 제거할 각 태그를 선택합니다.
6. 확인을 선택합니다.

AWS Migration Hub 를 사용하여 서버 데이터 내보내기

이 주제에서는 AWS Management Console AWS Command Line Interface, 또는 API를 사용하여 서버 데이터를 내보내는 방법을 설명합니다.

AWS Management Console 를 사용하여 모든 서버의 서버 데이터를 내보내려면

1. 에 로그인 AWS Management Console 하고 https://console.aws.amazon.com/migrationhub/ Migration Hub 콘솔을 엽니다.
2. 왼쪽 탐색 창의 검색에서 서버를 선택합니다.
3. 작업을 선택한 다음 검색 데이터 내보내기를 선택합니다.
4. 화면 맨 아래 내보내기 섹션에서 Export server details(서버 세부 정보 내보내기)를 선택합니다. 이 작업은 다음 표에 설명된 .csv 파일이 포함된 .zip 파일을 생성합니다.

파일 이름	설명
{account_id}_Application.csv	서버 수, 이름 및 설명을 포함한 각 애플리케이션의 세부 정보입니다.
{account_id}_ApplicationResourceAssociation.csv	서버와 애플리케이션 간의 관계입니다.
{account_id}_ImportTemplate	각 서버의 애플리케이션 및 태그에 대한 요약입니다. 이 파일을 수정하고 다시 가져와서 서버와 연결된 애플리케이션을 업데이트할 수 있습니다.
{account_id}_NetworkInterface.csv	연결된 서버, 주소 및 스위치를 포함한 각 네트워크 인터페이스의 세부 정보입니다.

파일 이름	설명
{account_id}_Server.csv	운영 체제, 호스트 이름 및 하이퍼바이저를 포함한 각 서버의 세부 정보입니다.
{account_id}_SystemPerformance.csv	CPU, 메모리 및 스토리지 구성, 성능을 포함한 각 서버의 세부 정보입니다.
{account_id}_Tags.csv	서버와 연결된 각 태그의 세부 정보입니다.
{account_id}_VMwareInfo.csv	moRef, vmName 및 vCenter를 포함한 각 VMware 구성의 세부 정보입니다.

AWS Management Console 를 사용하여 특정 서버의 에이전트 데이터를 내보내려면

1. 에 로그인 AWS Management Console 하고 https://console.aws.amazon.com/migrationhub/ Migration Hub 콘솔을 엽니다.
2. 왼쪽 탐색 창의 검색에서 서버를 선택합니다.
3. 서버 아래의 검색 필드에 커서를 놓습니다. 드롭다운 목록이 나타납니다. 해당 목록의 속성에서 소스를 선택한 다음 = 연산자를 선택하고 소스 = 에이전트를 선택합니다.
4. 검색 결과에서 데이터를 내보낼 서버의 이름을 선택합니다. 이 작업을 수행하면 해당 서버의 세부 정보 페이지로 이동합니다.
5. 시작 시간과 종료 시간을 입력한 다음 내보내기를 선택합니다. 내보낸 .zip 파일에는 다음 표에 설명된 .csv 파일이 포함됩니다.

{account_id}_destinationProcessConnection.csv	서버로의 인바운드 연결에 대한 세부 정보입니다.
{account_id}_networkInterface.csv	주소, 마스크 및 이름을 포함한 각 네트워크 인터페이스의 세부 정보
{account_id}_osInfo.csv	CPU 유형, 하이퍼바이저 및 운영 체제 이름을 포함한 운영 체제의 세부 정보입니다.

{account_id}_process.csv	서버에서 실행되는 프로세스의 세부 정보입니다.
{account_id}_sourceProcessConnection.csv	서버에서 시작된 아웃바운드 연결의 세부 정보입니다.
{account_id}_systemPerformance.csv	서버의 CPU, 메모리 및 스토리지 구성 및 성능에 대한 세부 정보입니다.

AWS Command Line Interface 또는 API를 사용하여 서버 데이터를 내보내려면

1. start-export-task를 실행합니다. 해당 API 작업은 StartExportTask입니다.
2. describe-export-tasks 실행합니다. 해당 API 작업은 DescribeExportTasks.

AWS Migration Hub 콘솔에서 서버 그룹화

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. AWS 계정을 사용하여에 로그인 AWS Management Console 하고 https://console.aws.amazon.com/migrationhub/ Migration Hub 콘솔을 엽니다.
2. Migration Hub 콘솔 탐색 창의 검색에서 서버를 선택합니다.
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 사항: 선택한 각 서버에서 태그 추가를 선택하고 키에 값을 입력합니다. 이후 선택적으로 값에 값을 입력합니다.
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 에이전트 또는 가져오기에 의해 데이터 센터에서 검색된 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 참조하세요.

다음 섹션의 표에는 두 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**
>
> `DescribeConfigurations`, `ListConfigurations`및에서 반환한 결과에는 최근 업데이트가 포함되어 있지 않을 `StartExportTask` 수 있습니다. 자세한 내용은 the section called "최종 일관성" 단원을 참조하십시오.

`DescribeConfigurations` 작업 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 DescribeConfigurations를 참조하십시오.

`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

ListConfigurations 작업 사용

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

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	없음
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	없음

필터	지원되는 조건	지원되는 값	지원되는 정렬
server.connectorId	• EQUALS • NOT_EQUALS • EQ • NE	• String	없음
server.type	• EQUALS • NOT_EQUALS • EQ • NE	다음 값 중 하나를 가진 문자열: • EC2 • 기타 • VMWARE_VM • VMWARE_HOST • VMWARE_VM_TEMPLATE	없음
server.vmWareInfo.morefId	• EQUALS • NOT_EQUALS • EQ • NE • CONTAINS • NOT_CONTAINS	• String	없음
server.vmWareInfo.vcenterId	• EQUALS • NOT_EQUALS • EQ • NE • CONTAINS • NOT_CONTAINS	• String	없음

필터	지원되는 조건	지원되는 값	지원되는 정렬
server.vmWareInfo.hostId	• EQUALS • NOT_EQUALS • EQ • NE • CONTAINS • NOT_CONTAINS	• String	없음
server.networkInterfaceInfo.portGroupId	• EQUALS • NOT_EQUALS • EQ • NE • CONTAINS • NOT_CONTAINS	• String	없음
server.networkInterfaceInfo.portGroupName	• EQUALS • NOT_EQUALS • EQ • NE • CONTAINS • NOT_CONTAINS	• String	없음
server.networkInterfaceInfo.virtualSwitchName	• EQUALS • NOT_EQUALS • EQ • NE • CONTAINS • NOT_CONTAINS	• String	없음

필터	지원되는 조건	지원되는 값	지원되는 정렬
server.networkInterfaceInfo.ipAddress	• EQUALS • NOT_EQUALS • EQ • NE • CONTAINS • NOT_CONTAINS	• String	없음
server.networkInterfaceInfo.macAddress	• EQUALS • NOT_EQUALS • EQ • NE • CONTAINS • NOT_CONTAINS	• String	없음
server.performance.avgCpuUsagePct	• GE • LE • GT • LT	• 백분율	없음
server.performance.totalDiskFreeSizeInKB	• GE • LE • GT • LT	• 배정밀도 실수	없음
server.performance.avgFreeRAMInKB	• GE • LE • GT • LT	• 배정밀도 실수	없음

필터	지원되는 조건	지원되는 값	지원되는 정렬
server.tag.value	• EQUALS • NOT_EQUALS • EQ • NE • CONTAINS • NOT_CONTAINS	• String	없음
server.tag.key	• EQUALS • NOT_EQUALS • EQ • NE • CONTAINS • NOT_CONTAINS	• String	없음
server.application.name	• EQUALS • NOT_EQUALS • EQ • NE • CONTAINS • NOT_CONTAINS	• String	없음
server.application.description	• EQUALS • NOT_EQUALS • EQ • NE • CONTAINS • NOT_CONTAINS	• String	없음

필터	지원되는 조건	지원되는 값	지원되는 정렬
server.application.configurationId	• EQUALS • NOT_EQUALS • EQ • NE	• 유효한 애플리케이션 구성 ID	없음
server.process.configurationId	• EQUALS • NOT_EQUALS • EQ • NE	• ProcessId	없음
server.process.name	• EQUALS • NOT_EQUALS • EQ • NE • CONTAINS • NOT_CONTAINS	• String	없음
server.process.commandLine	• EQUALS • NOT_EQUALS • EQ • NE • CONTAINS • NOT_CONTAINS	• String	없음

애플리케이션 자산

필터	지원되는 조건	지원되는 값	지원되는 정렬
application.configurationId	• EQUALS • NOT_EQUALS • EQ	• ApplicationId	없음

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	없음

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

AWS Application Discovery Service API의 최종 일관성

다음 업데이트 작업은 최종적으로 일관됩니다. 업데이트는 읽기 작업 StartExportTask, DescribeConfigurations 및 ListConfigurations에 즉시 표시되지 않을 수 있습니다.

- AssociateConfigurationItemsToApplication
- CreateTags
- DeleteApplications
- DeleteTags
- DescribeBatchDeleteConfigurationTask
- DescribeImportTasks
- DisassociateConfigurationItemsFromApplication
- UpdateApplication

최종 일관성 관리를 위한 제안 사항:

- 읽기 작업 StartExportTask, DescribeConfigurations 또는 ListConfigurations(또는 해당 AWS CLI 명령)를 호출할 때 지수 백오프 알고리즘을 사용하여 이전 업데이트 작업이 시스템을 통해 전파될 때까지 충분한 시간을 확보합니다. 이렇게 하려면 2초 대기 시간부터 시작하여 최대 5분의 대기 시간까지 읽기 작업을 반복적으로 실행합니다.
- 업데이트 작업이 200 - OK 응답을 반환하더라도 후속 작업 사이에 대기 시간을 추가합니다. 몇 초의 대기 시간으로 시작하는 지수 백오프 알고리즘을 적용하고 대기 시간을 약 5분까지 점진적으로 늘립니다.

인터페이스 엔드포인트를 AWS Application Discovery Service 사용한 액세스(AWS PrivateLink)

AWS PrivateLink 를 사용하여 VPC와 간에 프라이빗 연결을 생성할 수 있습니다 AWS Application Discovery Service. 인터넷 게이트웨이, NAT 디바이스, VPN 연결 또는 AWS Direct Connect 연결을 사용하지 않고 VPC에 있는 것처럼 Application Discovery Service에 액세스할 수 있습니다. VPC의 인스턴스는 Application Discovery Service에 액세스하는 데 퍼블릭 IP 주소가 필요하지 않습니다.

AWS PrivateLink에서 제공되는 인터페이스 엔드포인트를 생성하여 이 프라이빗 연결을 설정합니다. 인터페이스 엔드포인트에 대해 사용 설정하는 각 서브넷에서 엔드포인트 네트워크 인터페이스를 생성합니다. 이는 Application Discovery Service로 향하는 트래픽의 진입점 역할을 하는 요청자 관리형 네트워크 인터페이스입니다.

자세한 내용은AWS PrivateLink 가이드의 AWS PrivateLink를 통해 AWS 서비스 에 액세스를 참조하세요.

Application Discovery Service 고려 사항

Application Discovery Service에 대한 인터페이스 엔드포인트를 설정하기 전에 AWS PrivateLink 가이드의 인터페이스 VPC 엔드포인트를 사용하여 AWS 서비스 액세스를 검토합니다.

Application Discovery Service는 두 가지 인터페이스를 지원합니다. 하나는 모든 API 작업을 호출하기 위한 인터페이스이고, 다른 하나는 에이전트리스 수집기 및 AWS Application Discovery Agent가 검색 데이터를 전송하기 위한 인터페이스입니다.

인터페이스 엔드포인트 생성

Amazon VPC 콘솔 또는 AWS Command Line Interface (AWS CLI)를 사용하여 인터페이스 엔드포인트를 생성할 수 있습니다. 자세한 내용은 AWS PrivateLink 가이드의 인터페이스 VPC 엔드포인트를 사용하여 AWS 서비스 액세스를 참조하세요.

For Application Discovery Service

다음 서비스 이름을 사용하여 Application Discovery Service에 대한 인터페이스 엔드포인트를 생성합니다.

```
com.amazonaws.region.discovery
```

인터페이스 엔드포인트에 대해 프라이빗 DNS를 활성화하면 기본 리전 DNS 이름을 사용하여 Application Discovery Service에 API 요청을 할 수 있습니다. 예: `discovery.us-east-1.amazonaws.com`.

For Agentless Collector and AWS Application Discovery Agent

다음 서비스 이름을 사용하여 인터페이스 엔드포인트를 생성합니다.

```
com.amazonaws.region.arsenal-discovery
```

인터페이스 엔드포인트에 대해 프라이빗 DNS를 활성화하면 기본 리전 DNS 이름을 사용하여 Application Discovery Arsenal에 API 요청을 할 수 있습니다. 예: `arsenal-discovery.us-east-1.amazonaws.com`.

엔드포인트의 엔드포인트 정책 생성

엔드포인트 정책은 인터페이스 인터페이스 엔드포인트에 연결할 수 있는 IAM 리소스입니다. 기본 엔드포인트 정책은 인터페이스 엔드포인트를 통해 AWS 서비스에 대한 전체 액세스를 허용합니다. VPC에서 AWS 서비스에 허용되는 액세스를 제어하려면 인터페이스 엔드포인트에 사용자 지정 엔드포인트 정책을 연결합니다.

엔드포인트 정책은 다음 정보를 지정합니다.

- 작업을 수행할 수 있는 보안 주체 (AWS 계정, IAM 사용자, IAM 역할)
- 수행할 수 있는 작업.

자세한 내용은AWS PrivateLink 가이드의 엔드포인트 정책을 사용하여 서비스에 대한 액세스 제어를 참조하세요.

예: VPC 엔드포인트 정책

다음은 사용자 지정 엔드포인트 정책의 예입니다. 이 정책은 인터페이스 엔드포인트에 연결될 때 모든 리소스의 모든 보안 주체에 대한 액세스 권한을 나열된 작업에 부여합니다.

Example policy for Application Discovery Service

```
{
   "Statement": [
      {
         "Principal": "*",
```

```
         "Effect": "Allow",
         "Action": [
            "discovery:action-1",
            "discovery:action-2",
            "discovery:action-3"
         ],
         "Resource":"*"
      }
   ]
}
```

Example policy for the Agentless Collector and AWS Application Discovery Agent

```
{
   "Statement": [
      {
         "Principal": "*",
         "Effect": "Allow",
         "Action": [
            "arsenal:RegisterOnPremisesAgent"
         ],
         "Resource":"*"
      }
   ]
}
```

Agentless Collector 및 AWS Application Discovery Agent에 VPC 엔드포인트 사용

Agentless Collector 및 AWS Application Discovery Agent는 구성 가능한 엔드포인트를 지원하지 않습니다. 대신 `arsenal-discovery` Amazon VPC 엔드포인트에 프라이빗 DNS 기능을 사용합니다.

- 프라이빗 AWS IP 주소를 VPC로 라우팅하도록 AWS Direct Connect 라우팅 테이블을 설정합니다. 예를 들어, 대상 = 10.0.0.0/8 및 대상 = 로컬입니다. 이 설정을 수행하려면 Amazon `arsenal-discovery` VPC 엔드포인트 프라이빗 IP 주소를 VPC로 라우팅해야 합니다.
- Agentless Collector는 구성 가능한 Arsenal 엔드포인트를 지원하지 않으므로 `arsenal-discovery` Amazon VPC 엔드포인트 프라이빗 DNS 기능을 사용합니다.
- AWS Direct Connect 트래픽을 라우팅할 VPC가 동일한 프라이빗 서브넷에 `arsenal-discovery` Amazon VPC 엔드포인트를 설정합니다.

- VPC 내에서 인바운드 트래픽을 활성화하는 보안 그룹(예: 10.0.0.0/8)으로 `arsenal-discovery` Amazon VPC 엔드포인트를 설정합니다.
- Amazon Route 53 인바운드 해석기를 설정하여 `arsenal-discovery` Amazon VPC 엔드포인트 프라이빗 DNS 이름에 대한 DNS 확인을 라우팅합니다. 그러면 VPC 엔드포인트의 프라이빗 IP로 확인됩니다. 이렇게 하지 않으면 수집기는 온프레미스 해석기를 사용하여 DNS 확인을 수행하고 퍼블릭 Arsenal 엔드포인트를 사용하며 트래픽은 VPC를 통과하지 않습니다.
- 모든 퍼블릭 트래픽을 비활성화한 경우 자동 업데이트 기능이 실패합니다. 이는 Agentless Collector가 Amazon ECR 엔드포인트로 요청을 전송하여 업데이트를 검색하기 때문입니다. 퍼블릭 인터넷을 통해 요청을 보내지 않고 자동 업데이트 기능을 작동하려면 Amazon ECR 서비스에 대한 VPC 엔드포인트를 설정하고이 엔드포인트에 대한 프라이빗 DNS 기능을 활성화합니다.

의 보안 AWS Application Discovery Service

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

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

- 클라우드 보안 - AWS 는 클라우드에서 AWS AWS 서비스를 실행하는 인프라를 보호할 책임이 있습니다. AWS 또한는 안전하게 사용할 수 있는 서비스를 제공합니다. 서드 파티 감사자는 정기적으로 AWS 규정 준수 프로그램의 일환으로 보안 효과를 테스트하고 검증합니다.
- 클라우드의 보안 - 사용자의 책임은 사용하는 AWS 서비스에 따라 결정됩니다. 또한 데이터의 민감도, 조직의 요건 및 관련 법률 및 규정을 비롯한 기타 요소에 대해서도 책임이 있습니다.

AWS Application Discovery Agent 또는 Application Discovery Service Agentless Collector를 사용하려면 AWS 계정에 액세스 키를 제공해야 합니다. 그러면이 정보가 로컬 인프라에 저장됩니다. 공동 책임 모델의 일환으로 인프라에 대한 액세스를 보호할 책임은 사용자에게 있습니다.

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

주제

- 에 대한 자격 증명 및 액세스 관리 AWS Application Discovery Service
- 를 사용하여 Application Discovery Service API 호출 로깅 AWS CloudTrail

에 대한 자격 증명 및 액세스 관리 AWS Application Discovery Service

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

주제

대상

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 필요한 자격 증명과 권한을 관리자가 제공합니다. 더 많은 Application Discovery Service 기능을 사용하여 작업을 수행하게 되면 추가 권한이 필요할 수 있습니다. 액세스 권한 관리 방법을 이해하면 관리자에게 올바른 권한을 요청하는 데 도움이 됩니다. Application Discovery Service의 기능에 액세스할 수 없는 경우 섹션을 참조하세요AWS Application Discovery Service 자격 증명 및 액세스 문제 해결.

서비스 관리자 - 회사에서 Application Discovery Service 리소스를 책임지고 있는 경우 Application Discovery Service에 대한 전체 액세스 권한을 가지고 있을 것입니다. 서비스 사용자가 액세스해야 하는 Application Discovery Service 기능과 리소스를 결정하는 것은 사용자의 작업입니다. 그런 다음 IAM 관리자에게 요청을 제출하여 서비스 사용자의 권한을 변경해야 합니다. 이 페이지의 정보를 검토하여 IAM의 기본 개념을 이해하세요. 회사가 Application Discovery Service에서 IAM을 사용하는 방법에 대한 자세한 내용은 섹션을 참조하세요가 IAM에서 AWS Application Discovery Service 작동하는 방식.

IAM 관리자 - IAM 관리자인 경우 Application Discovery Service에 대한 액세스를 관리하는 정책을 작성하는 방법에 대한 세부 정보를 알고 싶을 수 있습니다. IAM에서 사용할 수 있는 Application Discovery Service 자격 증명 기반 정책 예제를 보려면 섹션을 참조하세요AWS Application Discovery Service 자격 증명 기반 정책 예제.

ID를 통한 인증

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

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

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

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

사용하는 인증 방법에 상관없이 추가 보안 정보를 제공해야 할 수도 있습니다. 예를 들어는 다중 인증(MFA)을 사용하여 계정의 보안을 강화할 것을 AWS 권장합니다. 자세한 내용은 AWS IAM Identity Center 사용 설명서에서 다중 인증 및 IAM 사용 설명서에서 IAM의AWS 다중 인증을 참조하세요.

AWS 계정 루트 사용자

를 생성할 때 계정의 모든 AWS 서비스 및 리소스에 대한 완전한 액세스 권한이 있는 하나의 로그인 자격 증명으로 AWS 계정시작합니다. 이 자격 증명을 AWS 계정 테루트 사용자라고 하며 계정을 생성하는 데 사용한 이메일 주소와 암호로 로그인하여 액세스합니다. 일상적인 작업에 루트 사용자를 사용하지 않을 것을 강력히 권장합니다. 루트 사용자 자격 증명을 보호하고 루트 사용자만 수행할 수 있는 작업을 수행하는 데 사용합니다. 루트 사용자로 로그인해야 하는 전체 작업 목록은 IAM 사용 설명서의 루트 사용자 자격 증명이 필요한 작업을 참조하세요.

IAM 사용자 및 그룹

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

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

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

IAM 역할

IAM 역할은 특정 권한이 AWS 계정 있는 내 자격 증명입니다. IAM 사용자와 유사하지만, 특정 개인과 연결되지 않습니다. 에서 IAM 역할을 일시적으로 수임하려면 사용자에서 IAM 역할(콘솔)로 전환할 AWS Management Console수 있습니다. https://docs.aws.amazon.com/IAM/latest/UserGuide/id_roles_use_switch-role-console.html 또는 AWS API 작업을 호출하거나 사용자 지정 URL을 AWS CLI 사용하여 역할을 수임할 수 있습니다. 역할 사용 방법에 대한 자세한 내용은 IAM 사용 설명서의 역할 수임 방법을 참조하세요.

임시 보안 인증이 있는 IAM 역할은 다음과 같은 상황에서 유용합니다.

- 페더레이션 사용자 액세스 - 페더레이션 ID에 권한을 부여하려면 역할을 생성하고 해당 역할의 권한을 정의합니다. 페더레이션 ID가 인증되면 역할이 연결되고 역할에 정의된 권한이 부여됩니다. 페더레이션 관련 역할에 대한 자세한 내용은 IAM 사용 설명서의 Create a role for a third-party identity provider (federation)를 참조하세요. IAM Identity Center를 사용하는 경우, 권한 집합을 구성합니다. 인증 후 ID가 액세스할 수 있는 항목을 제어하기 위해 IAM Identity Center는 권한 집합을 IAM의 역할과 연관짓습니다. 권한 집합에 대한 자세한 내용은 AWS IAM Identity Center 사용 설명서의 권한 집합을 참조하세요.
- 임시 IAM 사용자 권한 - IAM 사용자 또는 역할은 IAM 역할을 수임하여 특정 작업에 대한 다양한 권한을 임시로 받을 수 있습니다.
- 교차 계정 액세스 - IAM 역할을 사용하여 다른 계정의 사용자(신뢰할 수 있는 보안 주체)가 내 계정의 리소스에 액세스하도록 허용할 수 있습니다. 역할은 계정 간 액세스를 부여하는 기본적인 방법입니다. 그러나 일부 에서는 (역할을 프록시로 사용하는 대신) 정책을 리소스에 직접 연결할 AWS 서비스 수 있습니다. 교차 계정 액세스에 대한 역할과 리소스 기반 정책의 차이점을 알아보려면 IAM 사용 설명서의 IAM의 교차 계정 리소스 액세스를 참조하세요.
- 교차 서비스 액세스 - 일부는 다른에서 기능을 AWS 서비스 사용합니다 AWS 서비스. 예를 들어, 서비스에서 호출하면 일반적으로 해당 서비스는 Amazon EC2에서 애플리케이션을 실행하거나 Amazon S3에 객체를 저장합니다. 서비스는 직접적으로 호출하는 위탁자의 권한을 사용하거나, 서비스 역할을 사용하거나, 또는 서비스 연결 역할을 사용하여 이 작업을 수행할 수 있습니다.
  - 전달 액세스 세션(FAS) - IAM 사용자 또는 역할을 사용하여에서 작업을 수행하는 경우 AWS보안 주체로 간주됩니다. 일부 서비스를 사용하는 경우, 다른 서비스에서 다른 작업을 시작하는 작업을 수행할 수 있습니다. FAS는를 호출하는 보안 주체의 권한을 다운스트림 서비스에 AWS 서비스 대

한 요청과 AWS 서비스함께 사용합니다. FAS 요청은 서비스가 다른 AWS 서비스 또는 리소스와의 상호 작용을 완료해야 하는 요청을 수신할 때만 수행됩니다. 이 경우, 두 작업을 모두 수행할 수 있는 권한이 있어야 합니다. FAS 요청 시 정책 세부 정보는 전달 액세스 세션을 참조하세요.

- 서비스 역할 - 서비스 역할은 서비스가 사용자를 대신하여 작업을 수행하기 위해 맡는 IAM 역할입니다. IAM 관리자는 IAM 내에서 서비스 역할을 생성, 수정 및 삭제할 수 있습니다. 자세한 정보는 IAM 사용 설명서의 Create a role to delegate permissions to an AWS 서비스를 참조하세요.
- 서비스 연결 역할 - 서비스 연결 역할은에 연결된 서비스 역할의 한 유형입니다 AWS 서비스. 서비스는 사용자를 대신하여 작업을 수행하기 위해 역할을 수임할 수 있습니다. 서비스 연결 역할은에 표시 AWS 계정 되며 서비스가 소유합니다. IAM 관리자는 서비스 링크 역할의 권한을 볼 수 있지만 편집은 할 수 없습니다.

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

정책을 사용하여 액세스 관리

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

관리자는 AWS JSON 정책을 사용하여 대상에 액세스할 수 있는 사용자를 지정할 수 있습니다. 즉, 어떤 보안 주체가 어떤 리소스와 어떤 조건에서 작업을 수행할 수 있는지를 지정할 수 있습니다.

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

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

ID 기반 정책

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

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

리소스 기반 정책

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

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

액세스 제어 목록(ACL)

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

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

기타 정책 타입

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

- 권한 경계 – 권한 경계는 ID 기반 정책에 따라 IAM 엔터티(IAM 사용자 또는 역할)에 부여할 수 있는 최대 권한을 설정하는 고급 기능입니다. 개체에 대한 권한 경계를 설정할 수 있습니다. 그 결과로 얻

는 권한은 객체의 ID 기반 정책과 그 권한 경계의 교집합입니다. `Principal` 필드에서 사용자나 역할을 지정하는 리소스 기반 정책은 권한 경계를 통해 제한되지 않습니다. 이러한 정책 중 하나에 포함된 명시적 거부는 허용을 재정의합니다. 권한 경계에 대한 자세한 정보는 IAM 사용 설명서의 IAM 엔티티에 대한 권한 경계를 참조하세요.

- 서비스 제어 정책(SCPs) - SCPs는의 조직 또는 조직 단위(OU)에 대한 최대 권한을 지정하는 JSON 정책입니다 AWS Organizations. AWS Organizations 는 비즈니스가 소유 AWS 계정 한 여러를 그룹화하고 중앙에서 관리하기 위한 서비스입니다. 조직에서 모든 기능을 활성화할 경우, 서비스 제어 정책(SCP)을 임의의 또는 모든 계정에 적용할 수 있습니다. SCP는 각각을 포함하여 멤버 계정의 엔터티에 대한 권한을 제한합니다 AWS 계정 루트 사용자. 조직 및 SCP에 대한 자세한 내용은 AWS Organizations 사용 설명서에서 Service control policies을 참조하세요.
- 리소스 제어 정책(RCP) - RCP는 소유한 각 리소스에 연결된 IAM 정책을 업데이트하지 않고 계정의 리소스에 대해 사용 가능한 최대 권한을 설정하는 데 사용할 수 있는 JSON 정책입니다. RCP는 멤버 계정의 리소스에 대한 권한을 제한하며 조직에 속하는지 여부에 AWS 계정 루트 사용자관계없이를 포함한 자격 증명에 대한 유효 권한에 영향을 미칠 수 있습니다. RCP를 AWS 서비스 지원하는 목록을 포함하여 조직 및 RCPs에 대한 자세한 내용은 AWS Organizations 사용 설명서의 리소스 제어 정책(RCPs)을 참조하세요.
- 세션 정책 – 세션 정책은 역할 또는 페더레이션 사용자에 대해 임시 세션을 프로그래밍 방식으로 생성할 때 파라미터로 전달하는 고급 정책입니다. 결과적으로 얻는 세션의 권한은 사용자 또는 역할의 ID 기반 정책의 교차와 세션 정책입니다. 또한 권한을 리소스 기반 정책에서 가져올 수도 있습니다. 이러한 정책 중 하나에 포함된 명시적 거부는 허용을 재정의합니다. 자세한 정보는 IAM 사용 설명서의 세션 정책을 참조하세요.

여러 정책 유형

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

가 IAM에서 AWS Application Discovery Service 작동하는 방식

IAM을 사용하여 Application Discovery Service에 대한 액세스를 관리하기 전에 Application Discovery Service에서 사용할 수 있는 IAM 기능을 이해해야 합니다. Application Discovery Service 및 기타 AWS 서비스가 IAM과 작동하는 방식을 전체적으로 알아보려면 IAM 사용 설명서의 AWS IAM으로 작업하는 서비스를 참조하세요.

주제

- Application Discovery Service 자격 증명 기반 정책

- Application Discovery Service 리소스 기반 정책
- Application Discovery Service 태그 기반 권한 부여
- Application Discovery Service IAM 역할

Application Discovery Service 자격 증명 기반 정책

IAM ID 기반 정책을 사용하면 허용되거나 거부되는 작업과 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 대상에 액세스할 수 있는 사용자를 지정할 수 있습니다. 즉, 어떤 위탁자가 어떤 리소스와 어떤 조건에서 작업을 수행할 수 있는지를 지정할 수 있습니다.

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

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

Application Discovery Service의 정책 작업은 작업 앞에 접두사를 사용합니다`discovery:`. 정책 문에는 `Action` 또는 `NotAction` 요소가 포함되어야 합니다. Application Discovery Service는이 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 설명서의 에서 정의한 작업을 AWS Application Discovery Service 참조하세요.

리소스

Application Discovery Service는 정책에서 리소스 ARNs 지정을 지원하지 않습니다. 액세스를 분리하려면를 생성하고 별도로 사용합니다 AWS 계정.

조건 키

Application Discovery Service는 서비스별 조건 키를 제공하지 않지만 일부 전역 조건 키 사용을 지원합니다. 모든 AWS 전역 조건 키를 보려면 IAM 사용 설명서의 AWS 전역 조건 컨텍스트 키를 참조하세요.

예시

Application Discovery Service 자격 증명 기반 정책의 예를 보려면 섹션을 참조하세요AWS Application Discovery Service 자격 증명 기반 정책 예제.

Application Discovery Service 리소스 기반 정책

Application Discovery Service는 리소스 기반 정책을 지원하지 않습니다.

Application Discovery Service 태그 기반 권한 부여

Application Discovery Service는 리소스에 태그 지정 또는 태그 기반 액세스 제어를 지원하지 않습니다.

Application Discovery Service IAM 역할

IAM 역할은 AWS 계정 내에서 특정 권한이 있는 엔터티입니다.

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 역할 생성 또는 관리에 대한 자세한 내용은 섹션을 참조하세요Application Discovery Service에 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 직접 정책을 작성하는 것보다 AWS 관리형 정책을 사용하는 것이 더 쉽습니다. 팀에 필요한 권한만 제공하는 IAM 고객 관리형 정책을 생성하기 위해서는 시간과 전문 지식이 필요합니다. 빠르게 시작하려면 AWS 관리형 정책을 사용할 수 있습니다. 이 정책은 일반적인 사용 사례를 다루며 사용자의 AWS 계정에서 사용할 수 있습니다. AWS 관리형 정책에 대한 자세한 내용은 IAM 사용 설명서의 AWS 관리형 정책을 참조하세요.

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

또한는 여러 서비스에 걸쳐 있는 직무에 대한 관리형 정책을 AWS 지원합니다. 예를 들어 ReadOnlyAccess AWS 관리형 정책은 모든 AWS 서비스 및 리소스에 대한 읽기 전용 액세스를 제공합니다. 서비스가 새 기능을 시작하면는 새 작업 및 리소스에 대한 읽기 전용 권한을 AWS 추가합니다. 직무 정책의 목록과 설명은 IAM 사용 설명서의 직무에 관한AWS 관리형 정책을 참조하세요.

AWS 관리형 정책: AWSApplicationDiscoveryServiceFullAccess

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

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

AWS 관리형 정책: AWSApplicationDiscoveryAgentlessCollectorAccess

`AWSApplicationDiscoveryAgentlessCollectorAccess` 관리형 정책은 Application Discovery Service Agentless Collector(Agentless Collector)에 Application Discovery Service를 등록 및 통신하고 다른 AWS 서비스와 통신할 수 있는 액세스 권한을 부여합니다.

이 정책은 Agentless Collector를 구성하는 데 자격 증명이 사용되는 IAM 사용자에게 연결되어야 합니다.

권한 세부 정보

이 정책에는 다음 권한이 포함되어 있습니다.

- `arsenal` - 수집기가 Application Discovery Service 애플리케이션에 등록할 수 있도록 허용합니다. 이렇게 하면 수집된 데이터를 로 다시 보낼 수 있습니다 AWS.
- `ecr-public` - 수집기가 Amazon Elastic Container Registry Public(Amazon ECR Public)을 호출하여 수집기에 대한 최신 업데이트를 찾을 수 있도록 허용합니다.
- `mgh` - 수집기가를 호출 AWS Migration Hub 하여 수집기를 구성하는 데 사용되는 계정의 홈 리전을 검색할 수 있습니다. 이는 수집된 데이터를 전송해야 하는 리전을 파악하는 데 필요합니다.
- `sts` - 수집기가 서비스 보유자 토큰을 검색하도록 허용하여 수집기가 Amazon ECR Public에 최신 업데이트를 호출할 수 있도록 합니다.

```
{
    "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

`AWSApplicationDiscoveryAgentAccess` 정책은 Application Discovery Service에 등록하고 통신할 수 있는 액세스 권한을 Application Discovery Agent에 부여합니다.

Application Discovery Agent에서 자격 증명을 사용하는 모든 사용자에게이 정책을 연결합니다.

또한 이 정책은 사용자에게 Arsenal에 대한 액세스 권한을 부여합니다. Arsenal은에서 관리 및 호스팅하는 에이전트 서비스입니다 AWS. Arsenal은 클라우드의 Application Discovery Service에 데이터를 전달합니다. 이 정책의 예는 검색 에이전트에 대한 액세스 권한 부여 단원을 참조하십시오.

AWS 관리형 정책: AWSAgentlessDiscoveryService

이 `AWSAgentlessDiscoveryService` 정책은 VMware vCenter Server에서 실행 중인 AWS Agentless Discovery Connector에 Application Discovery Service와 커넥터 상태 지표를 등록, 통신 및 공유할 수 있는 액세스 권한을 부여합니다.

이 정책을 커넥터가 자격 증명을 사용하는 사용자에게 연결합니다.

AWS 관리형 정책: ApplicationDiscoveryServiceContinuousExportServiceRolePolicy

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

이 정책은 AWS Application Discovery Service 가 Amazon Data Firehose 스트림을 생성하여 AWS Application Discovery Service 에이전트가 수집한 데이터를 변환하고 AWS 계정의 Amazon S3 버킷으로 전송할 수 있도록 허용합니다.

또한이 정책은 에이전트가 수집한 데이터를 매핑하기 위해 application_discovery_service_database라는 새 데이터베이스와 테이블 스키마를 AWS Glue Data Catalog 사용하여를 생성합니다. 이 정책의 예는 에이전트 데이터 수집에 대한 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 AWSApplicationDiscoveryServiceFirehose 역할 생성 단원을 참조하십시오. 이 정책의 예는 데이터 탐색에 대한 권한 부여 단원을 참조하십시오.

AWSApplicationDiscoveryServiceFirehose 역할 생성

관리자는 관리형 정책을 IAM 사용자 계정에 연결합니다. `AWSDiscoveryContinuousExportFirehosePolicy` 정책을 사용할 때 관리자는 먼저 Firehose를 신뢰할 수 있는 엔터티로 사용하여 AWSApplicationDiscoveryServiceFirehose라는 역할을 생성한 다음

다음 다음 절차에 표시된 대로 해당 역할에 `AWSDiscoveryContinuousExportFirehosePolicy` 정책을 연결해야 합니다.

AWSApplicationDiscoveryServiceFirehose IAM 역할을 생성하려면

1. IAM 콘솔의 탐색 창에서 역할을 선택합니다.
2. 역할 생성을 선택합니다.
3. Kinesis를 선택합니다.
4. 사용 사례로 Kinesis Firehose를 선택합니다.
5. 다음: 권한을 선택합니다.
6. Filter Policies(필터 정책)에서 AWSDiscoveryContinuousExportFirehosePolicy를 검색합니다.
7. AWSDiscoveryContinuousExportFirehosePolicy 옆에 있는 확인란을 선택한 다음 다음: 검토를 선택합니다.
8. 역할 이름으로 AWSApplicationDiscoveryServiceFirehose를 입력한 다음 역할 생성을 선택합니다.

AWS 관리형 정책에 대한 Application Discovery Service 업데이트

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

변경 사항	설명	날짜
AWSApplicationDiscoveryAgentlessCollectorAccess - Agentless Collector 시작 시 사용할 수 있는 새 정책	Application Discovery Service는 Agentless Collector에 Application Discovery Service를 등록 및 통신하고 다른 AWS 서비스와 통신할 수 있는 액세스 권한을 `AWSApplicationDiscoveryAgentlessCollectorAccess` 부여하는 새로운 관리형 정책을 추가했습니다.	2022년 8월 16일

변경 사항	설명	날짜
Application Discovery Service에서 변경 사항 추적 시작	Application Discovery Service는 AWS 관리형 정책에 대한 변경 사항 추적을 시작했습니다.	2021년 3월 1일

AWS Application Discovery Service 자격 증명 기반 정책 예제

기본적으로 IAM 사용자 및 역할은 Application Discovery Service 리소스를 생성하거나 수정할 권한이 없습니다. 또한 AWS Management Console AWS CLI또는 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
- 검색 에이전트에 대한 액세스 권한 부여
- 에이전트 데이터 수집에 대한 권한 부여
- 데이터 탐색에 대한 권한 부여
- Migration Hub 콘솔 네트워크 다이어그램을 사용할 수 있는 권한 부여

정책 모범 사례

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

- AWS 관리형 정책을 시작하고 최소 권한으로 전환 - 사용자 및 워크로드에 권한 부여를 시작하려면 많은 일반적인 사용 사례에 대한 권한을 부여하는 AWS 관리형 정책을 사용합니다. 에서 사용할 수 있습니다 AWS 계정. 사용 사례에 맞는 AWS 고객 관리형 정책을 정의하여 권한을 추가로 줄이는 것이 좋습니다. 자세한 정보는 IAM 사용 설명서의 AWS 관리형 정책 또는 AWS 직무에 대한 관리형 정책을 참조하세요.

- 최소 권한 적용 – IAM 정책을 사용하여 권한을 설정하는 경우, 작업을 수행하는 데 필요한 권한만 부여합니다. 이렇게 하려면 최소 권한으로 알려진 특정 조건에서 특정 리소스에 대해 수행할 수 있는 작업을 정의합니다. IAM을 사용하여 권한을 적용하는 방법에 대한 자세한 정보는 IAM 사용 설명서에 있는 IAM의 정책 및 권한을 참조하세요.
- IAM 정책의 조건을 사용하여 액세스 추가 제한 – 정책에 조건을 추가하여 작업 및 리소스에 대한 액세스를 제한할 수 있습니다. 예를 들어, SSL을 사용하여 모든 요청을 전송해야 한다고 지정하는 정책 조건을 작성할 수 있습니다. 조건을 사용하여 AWS 서비스와 같은 특정를 통해 사용되는 경우 서비스 작업에 대한 액세스 권한을 부여할 수도 있습니다 AWS CloudFormation. 자세한 정보는 IAM 사용 설명서의 IAM JSON 정책 요소: 조건을 참조하세요.
- IAM Access Analyzer를 통해 IAM 정책을 확인하여 안전하고 기능적인 권한 보장 - IAM Access Analyzer에서는 IAM 정책 언어(JSON)와 모범 사례가 정책에서 준수되도록 새로운 및 기존 정책을 확인합니다. IAM Access Analyzer는 100개 이상의 정책 확인 항목과 실행 가능한 추천을 제공하여 안전하고 기능적인 정책을 작성하도록 돕습니다. 자세한 내용은 IAM 사용 설명서의 IAM Access Analyzer에서 정책 검증을 참조하세요.
- 다중 인증(MFA) 필요 -에서 IAM 사용자 또는 루트 사용자가 필요한 시나리오가 있는 경우 추가 보안을 위해 MFA를 AWS 계정켭니다. API 작업을 직접 호출할 때 MFA가 필요하면 정책에 MFA 조건을 추가합니다. 자세한 내용은 IAM 사용 설명서의 MFA를 통한 보안 API 액세스를 참조하세요.

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

Application Discovery Service에 대한 전체 액세스 권한 부여

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

계정에이 정책이 연결된 IAM 사용자는 Application Discovery Service를 구성하고, 에이전트를 시작 및 중지하고, 에이전트 없는 검색을 시작 및 중지하고, Discovery Service 데이터베이스에서 데이터를 쿼리할 AWS 수 있습니다. 이 정책에 대한 자세한 내용은 AWS 에 대한 관리형 정책 AWS Application Discovery Service 단원을 참조하세요.

Example AWSApplicationDiscoveryServiceFullAccess 정책

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

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

검색 에이전트에 대한 액세스 권한 부여

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

Application Discovery Agent에서 자격 증명을 사용하는 모든 사용자에게이 정책을 연결합니다.

또한 이 정책은 사용자에게 Arsenal에 대한 액세스 권한을 부여합니다. Arsenal은에서 관리 및 호스팅하는 에이전트 서비스입니다 AWS. Arsenal은 클라우드의 Application Discovery Service에 데이터를 전달합니다.

Example AWSApplicationDiscoveryAgentAccess Policy

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

에이전트 데이터 수집에 대한 권한 부여

ApplicationDiscoveryServiceContinuousExportServiceRolePolicy 관리형 정책을 사용하면가 Amazon Data Firehose 스트림 AWS Application Discovery Service 을 생성하여 Application Discovery Service 에이전트가 수집한 데이터를 변환하고 AWS 계정의 Amazon S3 버킷으로 전송할 수 있습니다.

또한이 정책은 에이전트가 수집한 AWS Glue 데이터를 매핑하기 위해 `application_discovery_service_database` 및 테이블 스키마라는 새 데이터베이스를 사용하여 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 탐색에 대한 권한 부여

Amazon Athena에서 데이터 탐색을 사용하려면 AWSDiscoveryContinuousExportFirehosePolicy 정책이 필요합니다. 이를 통해 Amazon Data Firehose는 Application Discovery Service 에서 수집한 데이터를 Amazon S3에 쓸 수 있습니다. 이 정책 사용에 대한 자세한 내용은 AWSApplicationDiscoveryServiceFirehose 역할 생성 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 다이어그램을 사용할 수 있는 권한 부여

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

정책에 대해 다음 사항이 모두 적용되는 경우 새 정책에서 `discovery:GetNetworkConnectionGraph` 작업을 사용하거나 이전 정책을 업데이트해야 합니다.

- 정책은 Application Discovery Service 또는 Migration Hub에 대한 액세스를 허용하거나 거부합니다.
- 이 정책은 `discovery:`*`action-name`* 대신와 같은 하나 이상의 특정 검색 작업을 사용하여 액세스 권한을 부여합니다`discovery:*`.

다음 예제에서는 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 참조하세요.

Application Discovery Service에 서비스 연결 역할 사용

AWS Application Discovery Service 는 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 서비스가 사용자를 대신하여 다른 AWS 서비스를 호출하는 데 필요한 모든 권한을 포함합니다.

서비스 연결 역할을 사용하면 필요한 권한을 수동으로 추가할 필요가 없으므로 Application Discovery Service를 더 쉽게 설정할 수 있습니다. Application Discovery Service는 서비스 연결 역할의 권한을 정의하며, 달리 정의되지 않은 한 Application Discovery Service만 해당 역할을 수임할 수 있습니다. 정의된 권한에는 신뢰 정책과 권한 정책이 포함되며 이 권한 정책은 다른 IAM 엔티티에 연결할 수 없습니다.

먼저 관련 리소스를 삭제한 후에만 서비스 연결 역할을 삭제할 수 있습니다. 이렇게 하면 리소스에 대한 액세스 권한을 실수로 제거할 수 없으므로 Application Discovery Service 리소스가 보호됩니다.

주제

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

서비스 연결 역할을 지원하는 기타 서비스에 대해 자세히 알아보려면 IAM으로 작업하는AWS 서비스를 참조하여 서비스 연결 역할 열이 예인 서비스를 찾습니다. 해당 서비스에 대한 서비스 연결 역할 설명서를 보려면 링크가 있는 예를 선택합니다.

Application Discovery Service에 대한 서비스 연결 역할 권한

Application Discovery Service는 AWSServiceRoleForApplicationDiscoveryServiceContinuousExport라는 서비스 연결 역할을 사용합니다.에서 사용하거나 관리하는 AWS 서비스 및 리소스에 대한 액세스를 활성화합니다 AWS Application Discovery Service.

AWSServiceRoleForApplicationDiscoveryServiceContinuousExport 서비스 연결 역할은 다음 서비스를 신뢰하여 역할을 수임합니다.

- `continuousexport.discovery.amazonaws.com`

역할 권한 정책은 Application Discovery Service가 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 링크 역할을 생성하고 편집하거나 삭제할 수 있도록 권한을 구성할 수 있습니다. 자세한 내용은 IAM 사용 설명서의 서비스 연결 역할 권한 단원을 참조하세요.

Application Discovery Service에 대한 서비스 연결 역할 생성

서비스 링크 역할은 수동으로 생성할 필요가 없습니다.
AWSServiceRoleForApplicationDiscoveryServiceContinuousExport 서비스 연결 역할은 a) '데이터 수집 시작'을 선택한 후 Data Collectors 페이지에 표시된 대화 상자에서 옵션을 확인하거나 'Athena의 데이터 탐색'이라는 슬라이더를 클릭하거나 b) AWS CLI를 사용하여 StartContinuousExport API를 호출할 때 암시적으로 설정된 경우 자동으로 생성됩니다.

> **Important**
>
> 이러한 서비스 연결 역할은 해당 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 역할을 생성할 수 있습니다.

서비스 연결 역할을 생성하려면 다음을 수행합니다(콘솔).

1. 탐색 창에서 Data Collectors(데이터 수집기)를 선택합니다.
2. 에이전트 탭을 선택합니다.
3. Athena 슬라이더의 데이터 탐색을 켜짐 위치로 전환합니다.
4. 이전 단계에서 생성된 대화 상자에서 관련 비용에 대해 동의하는 확인란을 클릭하고 계속 또는 활성화를 선택합니다.

에서 서비스 연결 역할 생성 AWS CLI

의 Application Discovery Service 명령을 사용하여 AWSServiceRoleForApplicationDiscoveryServiceContinuousExport 서비스 연결 역할을 AWS Command Line Interface 생성할 수 있습니다.

이 서비스 연결 역할은에서 연속 내보내기를 AWS CLI 시작할 때 자동으로 생성됩니다(먼저 환경에 설치해야 AWS CLI 함).

에서 지속적 내보내기를 시작하여 서비스 연결 역할(CLI)을 생성하려면 AWS CLI

1. 운영 체제(Linux, macOS 또는 Windows) AWS CLI 용를 설치합니다. 지침은 AWS Command Line Interface 사용 설명서를 참조하세요.
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 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 사용하여 Discovery Service - Continuous Export 사용 사례에서 서비스 연결 역할을 생성할 수 있습니다. 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 삭제하면 동일한 프로세스를 사용하여 역할을 다시 생성할 수 있습니다.

Application Discovery Service에 대한 서비스 연결 역할 삭제

서비스 연결 역할이 필요한 기능 또는 서비스가 더 이상 필요 없는 경우에는 해당 역할을 삭제하는 것이 좋습니다. 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 삭제하려고 할 때 Application Discovery Service에서 역할을 사용하는 경우 삭제에 실패할 수 있습니다. 이 문제가 발생하면 몇 분 기다렸다가 작업을 다시 시도하세요.

마이그레이션 허브 콘솔에서 AWSServiceRoleForApplicationDiscoveryServiceContinuousExport 서비스 연결 역할에서 사용하는 Application Discovery Service 리소스를 삭제하려면

1. 탐색 창에서 Data Collectors(데이터 수집기)를 선택합니다.
2. 에이전트 탭을 선택합니다.
3. Athena 슬라이더의 데이터 탐색을 Off 위치로 전환합니다.

에서 AWSServiceRoleForApplicationDiscoveryServiceContinuousExport 서비스 연결 역할이 사용하는 Application Discovery Service 리소스를 삭제하려면 AWS CLI

1. 운영 체제(Linux, macOS 또는 Windows) AWS CLI 용를 설치합니다. 지침은 AWS Command Line Interface 사용 설명서를 참조하세요.
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 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 "INACTIVE"인지 확인하여 연속 내보내기가 중지되었는지 확인합니다.

```
aws discovery describe-continuous-export
```

수동으로 서비스 연결 역할 삭제

IAM 콘솔, IAM CLI 또는 IAM API를 사용하여 AWSServiceRoleForApplicationDiscoveryServiceContinuousExport 서비스 연결 역할을 삭제할 수 있

습니다. 이 서비스 연결 역할이 필요한 Discovery Service - Continuous Export 기능을 더 이상 사용할 필요가 없는 경우 해당 역할을 삭제하는 것이 좋습니다. 따라서 적극적으로 모니터링하거나 유지하지 않는 미사용 엔터티가 없도록 합니다. 자세한 내용은 IAM 사용 설명서의 서비스 연결 역할 삭제 섹션을 참조하십시오.

> **Note**
>
> 삭제하기 전에 먼저 서비스 연결 역할을 정리해야 합니다. 서비스 연결 역할 정리을(를) 참조하세요.

AWS Application Discovery Service 자격 증명 및 액세스 문제 해결

다음 정보를 사용하여 Application Discovery Service 및 IAM 작업 시 발생할 수 있는 일반적인 문제를 진단하고 수정할 수 있습니다.

주제

- iam:PassRole을 수행할 권한이 없음

iam:PassRole을 수행할 권한이 없음

`iam:PassRole` 작업을 수행할 권한이 없다는 오류가 수신되면 Application Discovery Service에 역할을 전달할 수 있도록 정책을 업데이트해야 합니다.

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

다음 예제 오류는 라는 IAM 사용자가 콘솔을 사용하여 Application Discovery Service에서 작업을 수행`marymajor`하려고 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 필요한 경우 AWS 관리자에게 문의하십시오. 관리자는 로그인 자격 증명을 제공한 사람입니다.

를 사용하여 Application Discovery Service API 호출 로깅 AWS CloudTrail

AWS Application Discovery Service 는 Application Discovery Service에서 사용자 AWS CloudTrail, 역할 또는 서비스가 수행한 작업에 대한 레코드를 제공하는 AWS 서비스와 통합됩니다. CloudTrail을 사용하여 문제 해결 및 감사 목적으로 계정 활동을 로깅, 지속적인 모니터링 및 유지할 수 있습니다. CloudTrail은 AWS 관리 콘솔, AWS SDKs 및 명령줄 도구를 통해 수행된 작업을 포함하여 AWS 계정 활동의 이벤트 기록을 제공합니다.

CloudTrail은 Application Discovery Service에 대한 모든 API 호출을 이벤트로 캡처합니다. 캡처된 호출에는 Application Discovery Service 콘솔의 호출과 Application Discovery Service API 작업에 대한 코드 호출이 포함됩니다.

추적을 생성하면 Application Discovery Service 이벤트를 포함하여 CloudTrail 이벤트를 Amazon S3 버킷으로 지속적으로 전송할 수 있습니다. 트레일을 구성하지 않은 경우에도 CloudTrail 콘솔의 이벤트 기록에서 최신 이벤트를 볼 수 있습니다. CloudTrail에서 수집한 정보를 사용하여 Application Discovery Service에 수행된 요청, 요청이 수행된 IP 주소, 요청을 수행한 사람, 요청이 수행된 시간 및 추가 세부 정보를 확인할 수 있습니다.

CloudTrail에 대한 자세한 내용은 AWS CloudTrail 사용 설명서를 참조하세요.

CloudTrail의 Application Discovery Service 정보

AWS 계정을 생성할 때 계정에서 CloudTrail이 활성화됩니다. Application Discovery Service에서 활동이 발생하면 해당 활동이 이벤트 기록의 다른 AWS 서비스 이벤트와 함께 CloudTrail 이벤트에 기록됩니다. AWS 계정에서 최근 이벤트를 보고 검색하고 다운로드할 수 있습니다. 자세한 정보는 CloudTrail 이벤트 기록을 사용하여 이벤트 보기를 참조하세요.

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

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

모든 Application Discovery Service 작업은 CloudTrail에서 로깅되며 Application Discovery Service API 참조에 문서화됩니다. 예를 들어 `CreateTags`, `DescribeTags` 및 `GetDiscoverySummary` 작업을 직접적으로 호출하면 CloudTrail 로그 파일에 항목이 생성됩니다.

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

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

자세한 설명은 CloudTrail userIdentity 요소를 참조하세요.

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 직접 호출의 주문 스택 트레이스가 아니므로 특정 순서로 표시되지 않습니다.

다음은 `DescribeTags` 작업을 보여주는 CloudTrail 로그 항목이 나타낸 예시입니다.

```
{
    "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 ARN 형식

Amazon 리소스 이름(ARN)은 AWS 리소스를 고유하게 식별하는 문자열입니다.는 모든 리소스에서 리소스를 명확하게 지정하려는 경우 ARN이 AWS 필요합니다 AWS.는 다음 ARNs을 AWS Application Discovery Service 정의합니다.

- Discovery Agent: `arn:aws:discovery:`*`region`*`:`*`account`*`:agent/discovery-agent/`*`agentId`*
- 에이전트리스 수집기: `arn:aws:discovery:`*`region`*`:`*`account`*`:agent/agentless-collector/`*`agentId`*
- 마이그레이션 평가자 수집기: `arn:aws:discovery:`*`region`*`:`*`account`*`:agent/migration-evaluator-collector/`*`agentId`*
- 검색 커넥터: `arn:aws:discovery:`*`region`*`:`*`account`*`:agent/discovery-connector/`*`agentId`*

AWS Application Discovery Service 할당량

Service Quotas 콘솔은 AWS Application Discovery Service 할당량에 대한 정보를 제공합니다. Service Quotas 콘솔을 사용하면 기본 서비스 할당량을 확인하고 조정 가능한 할당량에 대한 할당량 증가를 요청할 수 있습니다.

현재 늘릴 수 있는 유일한 할당량은 계정당 가져온 서버입니다.

Application Discovery Service에는 다음과 같은 기본 할당량이 있습니다.

- 계정당 애플리케이션 1,000개.

  이 할당량에 도달하고 새 애플리케이션을 가져오려는 경우 `DeleteApplications` API 작업을 사용하여 기존 애플리케이션을 삭제할 수 있습니다. 자세한 내용은 Application Discovery Service API 참조의 DeleteApplications를 참조하세요.
- 각 가져오기 파일의 최대 파일 크기는 10MB입니다.
- 계정당 가져온 서버 레코드 25,000개.
- 하루에 가져오기 레코드 25,000개 삭제.
- 계정당 10,000개의 가져온 서버(이 할당량 증가를 요청할 수 있음).
- Application Discovery Service로 데이터를 수집하고 전송하는 1,000명의 활성 에이전트.
- 응답하지만 데이터를 수집하지 않는 비활성 에이전트 10,000명.
- 애플리케이션당 서버 400개
- 서버당 태그 30개.

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 `StopContinuousExport` API를 호출할 수 있습니다. 데이터 수집을 중지하는 데 최대 30분이 걸릴 수 있으며,이 단계에서 콘솔의 토글 스위치와 `DescribeContinuousExport` API 호출은 데이터 탐색 상태를 "진행 중 중지"로 표시합니다.

> **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 않는 경우 AWS 지원팀에 문의하십시오.

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 버킷에서 데이터를 수집하지 않으려면 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 생성된 다음 스트림을 삭제합니다.

   - `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 탐색에서 수집한 데이터 제거

데이터 탐색으로 수집된 데이터를 제거하려면

1. Amazon S3에 저장된 검색 에이전트 데이터를 제거합니다.

   AWS Application Discovery Service (ADS)에서 수집하는 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. Amazon Athena S3로 새 검색 에이전트 데이터를 계속 전송합니다. 삭제된 데이터는 더 이상 Athena에서도 액세스할 수 없습니다.

2. 를 제거합니다 AWS Glue Data Catalog.

Amazon Athena에서 데이터 탐색을 활성화하면 계정에 Amazon S3 버킷이 생성되어 ADS 에이전트가 정기적으로 수집한 데이터를 저장합니다. 또한 Amazon Athena에서 Amazon S3 버킷에 저장된 데이터를 쿼리할 수 AWS Glue Data Catalog 있는 도 생성합니다. Amazon Athena에서 데이터 탐색을 끄면 Amazon S3 버킷에 새 데이터가 저장되지 않지만 이전에 수집된 데이터는 유지됩니다. 이 데이터가 더 이상 필요하지 않고 Amazon Athena에서 데이터 탐색이 활성화되기 전에 계정을 상태로 되돌리려는 경우.

a. AWS 콘솔에서 Amazon S3를 방문하여 "aws-application-discover-discovery-service-uniqueid"라는 이름으로 버킷을 수동으로 삭제합니다.

b. application-discovery-service-database 데이터베이스와 다음 테이블을 모두 삭제하여 데이터 탐색 AWS Glue 데이터 카탈로그를 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 Support에 문의하여 전체 데이터 삭제를 요청하세요.

Amazon Athena에서 데이터 탐색과 관련된 일반적인 문제 해결

이 섹션에서는 Amazon Athena에서 데이터 탐색과 관련된 일반적인 문제를 해결하는 방법에 대한 정보를 찾을 수 있습니다.

주제

- 서비스 연결 역할 및 필요한 AWS 리소스를 생성할 수 없으므로 Amazon Athena에서 데이터 탐색이 시작되지 않음
- 새 에이전트 데이터가 Amazon Athena에 표시되지 않음

- Amazon S3, Amazon Data Firehose 또는에 액세스할 수 있는 권한이 충분하지 않습니다. AWS Glue

서비스 연결 역할 및 필요한 AWS 리소스를 생성할 수 없으므로 Amazon Athena에서 데이터 탐색이 시작되지 않음

Amazon Athena에서 데이터 탐색을 켜면 Amazon S3 버킷`AWSServiceRoleForApplicationDiscoveryServiceContinuousExport`, Amazon Kinesis 스트림 및를 포함하여 에이전트가 Amazon Athena에서 수집된 데이터에 액세스할 수 있도록 하는 데 필요한 AWS 리소스를 생성할 수 있는 서비스 연결 역할가 계정에 생성됩니다 AWS Glue Data Catalog. 계정에 Amazon Athena에서이 역할을 생성할 수 있는 적절한 데이터 탐색 권한이 없는 경우 초기화되지 않습니다. 자세한 내용은 AWS 에 대한 관리형 정책 AWS Application Discovery Service 항목을 참조하세요.

새 에이전트 데이터가 Amazon Athena에 표시되지 않음

새 데이터가 Athena로 흐르지 않고 에이전트가 시작된 지 30분 이상 지났으며 데이터 탐색 상태가 활성인 경우 아래 나열된 솔루션을 확인하세요.

- AWS 검색 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 올바르게 작동하는지 확인합니다.

  - `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` 데이터베이스가에 있는지 확인합니다 AWS Glue. 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

  `aws-application-discovery-service-`*`uniqueid`* 계정에 이름이 인 Amazon S3 버킷이 있는지 확인합니다. 버킷의 객체가 이동 또는 삭제된 경우 Athena에 제대로 표시되지 않습니다.

- 온프레미스 서버

  에이전트가 데이터를 수집하고 AWS Application Discovery Service로 전송할 수 있도록 서버가 실행 중인지 확인합니다.

Amazon S3, Amazon Data Firehose 또는에 액세스할 수 있는 권한이 충분하지 않습니다. AWS Glue

를 사용하고 AWS Organizations있고 Amazon Athena에서 데이터 탐색을 위한 초기화가 실패하는 경우 Amazon S3, Amazon Data Firehose, Athena 또는에 액세스할 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 Service을(를) 참조하세요.

Amazon Athena에서 데이터 탐색이 올바르게 작동하도록 하려면 Amazon S3 버킷, Amazon Data Firehose Streams 및를 포함하여 Amazon Athena에서 데이터 탐색으로 생성된 AWS 리소스를 수정하거나 삭제하지 마세요 AWS Glue Data Catalog. 실수로 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.

실패한 가져오기 레코드 문제 해결

Migration Hub 가져오기를 사용하면 Discovery Connector 또는 Discovery Agent를 사용하지 않고도 온프레미스 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 연결된 할당량이 있습니다. 할당량을 초과하는 가져오기 작업 요청을 수행하면 요청이 실패하고 오류가 반환됩니다. 자세한 내용은 AWS Application Discovery Service 할당량 단원을 참조하십시오.
- 가져오기 파일에 추가 쉼표(,)가 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 벗어남 -와 같은 일부 필드는 지원하는 값의 범위를 가져야 `CPU.NumberOfCores` 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 로그인 AWS Management Console하고에서 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 실패한 각 레코드에 대한 줄, 열 이름ExternalId, 및 설명 오류 메시지를 추적합니다.
- failed-entries-file.csv -이 파일에는 원래 가져오기 파일에서 실패한 항목만 포함됩니다.

한도 기반 오류가 아닌 다른 오류를 수정하려면 errors-file.csv를 사용하여 failed-entries-file.csv 파일에서 문제를 수정한 후 해당 파일을 가져오십시오. 파일 가져오기에 대한 지침은 데이터 가져오기 단원을 참조하십시오.

에 대한 문서 기록 AWS Application Discovery Service

최신 사용 설명서 업데이트: 2023년 5월 16일

다음 표에서는 2019년 1월 18일 이후 Application Discovery Service 사용 설명서의 중요한 변경 사항을 설명합니다. 설명서 업데이트에 대한 알림을 받으려면 RSS 피드를 구독하시면 됩니다.

변경 사항	설명	날짜
Discovery Connector에서 Agentless Collector로 전환	현재 Discovery Connector를 사용하는 고객은 새 Agentless Collector로 전환하는 것이 좋습니다. 2025 AWS Application Discovery Service 년 11월 17일부터는 Discovery Connector에서 새 데이터 수락을 중지합니다. 자세한 내용은 Discovery Connector를 참조하세요.	2024년 11월 12일
에이전트리스 수집기 네트워크 데이터 수집 모듈 릴리스	네트워크 데이터 수집 모듈을 사용하면 온프레미스 데이터 센터의 서버 간 종속성을 검색할 수 있습니다. 자세한 내용은 Agentless Collector 네트워크 데이터 수집 모듈 사용을 참조하세요.	2024년 11월 8일
종속성 매핑을 위한 에이전트리스 컬렉션 지원	자세한 내용은 VMware vCenter Agentless Collector 데이터 수집 모듈 사용을 참조하세요.	2024년 10월 24일
Amazon Linux 2023 기반 Agentless Collector 버전 2 릴리스	자세한 내용은 Agentless Collector의 사전 조건을 참조하세요.	2024년 9월 26일

Agentless Collector 사전 조건 업데이트	자세한 내용은 Agentless Collector의 사전 조건을 참조하세요.	2024년 9월 9일
API의 최종 일관성	자세한 내용은 AWS Application Discovery Service API의 최종 일관성을 참조하세요.	2024년 6월 20일
에이전트리스 수집기 업데이트	아웃바운드 액세스`sts.amazonaws.com` 가 필요한 도메인 목록에를 추가했습니다. 자세한 내용은 AWS 도메인에 대한 아웃바운드 액세스를 위한 방화벽 구성을 참조하세요.	2024년 6월 20일
액세스를 분리하려면 별도의 AWS 계정을 생성하고 사용합니다.	자세한 내용은 AWS Application Discovery Service의 작업, 리소스 및 조건 키를 참조하세요.	2024년 4월 5일
Agentless Collector 데이터베이스 및 분석 데이터 수집 모듈 소개	데이터베이스 및 분석 데이터 수집 모듈은 Application Discovery Service Agentless Collector(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 참조하세요.	2023년 5월 16일

Application Discovery Service Agentless Collector 소개	Application Discovery Service Agentless Collector(Agentless Collector)는 AWS Application Discovery Service 온프레미스 환경에 대한 에이전트 없는 방법을 통해 정보를 수집하여 로의 마이그레이션을 효과적으로 계획하는 데 도움이 되는 새로운 온프레미스 애플리케이션입니다 AWS 클라우드. 자세한 내용은 에이전트리스 수집기를 참조하세요.	2022년 8월 16일
IAM 업데이트	이제 자격 증명 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 다이어그램을 사용할 수 있는 권한 부여를 참조하세요.	2022년 5월 24일
홈 리전 소개	Migration Hub 홈 리전은 전체 포트폴리오에 대한 검색 및 마이그레이션 계획 정보의 단일 리포지토리와 여러 AWS 리전으로의 마이그레이션에 대한 단일 보기를 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 Hub로 가져올 수 있습니다. 이 데이터를 사용하여 애플리케이션 마이그레이션 상태를 추적할 수도 있습니다. 자세한 내용은 Migration Hub Import를 참조하세요.	2019년 1월 18일

다음 표에서는 2019년 1월 18일 이전의 Application Discovery Service 사용 설명서 릴리스에 대해 설명합니다.

변경 사항	설명	날짜
새 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 Console 이 추가되었습니다.	2016년 19월 12일
에이전트 없는 검색	이 릴리스는 에이전트가 없는 검색을 설정하고 구성하는 방법에 대해 설명합니다.	2016년 7월 28일

변경 사항	설명	날짜
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	Application Discovery Service 사용 설명서의 첫 번째 릴리스입니다.	2016년 5월 12일

AWS 용어집

최신 AWS 용어는 AWS 용어집 참조의 AWS 용어집을 참조하세요.

Discovery Connector

> **Important**
>
> 현재 Discovery Connector를 사용하는 고객은 새 Agentless Collector로 전환하는 것이 좋습니다. 2025년 11월 17일부터 Discovery Connectors에서 새 데이터 수락을 AWS Application Discovery Service 중지합니다.

이 섹션에서는 AWS 에이전트리스 검색 커넥터(검색 커넥터)에서 Application Discovery Service 에이전트리스 수집기(에이전트리스 수집기)로 전환하는 방법을 설명합니다.

현재 Discovery Connector를 사용하는 고객은 새 Agentless Collector로 전환하는 것이 좋습니다.

Agentless Collector 사용을 시작하는 방법을 알아보려면 섹션을 참조하세요Application Discovery Service Agentless Collector.

Agentless Collector를 배포한 후 Discovery Connector 가상 머신을 삭제할 수 있습니다. 이전에 수집된 모든 데이터는 (Migration Hub)에서 AWS Migration Hub 계속 사용할 수 있습니다.

Discovery Connector를 사용하여 데이터 수집

> **Important**
>
> 현재 Discovery Connector를 사용하는 고객은 새 Agentless Collector로 전환하는 것이 좋습니다. 2025년 11월 17일부터 Discovery Connectors에서 새 데이터 수락을 AWS Application Discovery Service 중지합니다. 자세한 내용은 Discovery Connector 단원을 참조하십시오.

Discovery Connector는 VMware vCenter Server 호스트 및 VMs에 대한 정보를 수집합니다. 하지만 VMware vCenter Server 도구가 설치된 경우에만 이런 데이터를 캡처할 수 있습니다. 사용 중인 AWS 계정에이 작업에 필요한 권한이 있는지 확인하려면 섹션을 참조하세요AWS 에 대한 관리형 정책 AWS Application Discovery Service.

아래에서 Discovery Connector에서 수집한 정보의 인벤토리를 찾을 수 있습니다.

Discovery Connector에서 수집한 데이터에 대한 테이블 범례:

- 수집된 데이터는 별도의 명시가 없는 경우에는 KB(Kilobytes)로 측정됩니다.

- Migration Hub 콘솔의 동등한 데이터는 메가바이트(MB) 단위로 보고됩니다.
- 별표(*)로 표시된 데이터 필드는 커넥터의 API 내보내기 함수에서 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)
configId	Application Discovery Service에서 검색된 VM에 ID 할당
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

데이터 필드	설명
hostName	가상 소프트웨어를 실행하는 호스트의 이름
하이퍼바이저	하이퍼바이저 유형
id	서버 ID
lastModifiedTimeStamp*	데이터를 내보내기 전 마지막으로 데이터를 수집한 날짜와 시간
macAddress	VM 제조업체의 MAC
주소	가상 소프트웨어 제조사
maxCpuUsagePct	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)
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

데이터 필드	설명
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 ID 할당
smBiosId*	시스템 관리 BIOS의 ID/버전
state*	검색 커넥터 가상 어플라이언스의 상태
toolsStatus	VMware 도구들의 운영 상태(전체 목록은 콘솔에서 AWS Migration Hub 데이터 수집기 정렬를 참조)
totalDiskSize	디스크 총 용량(MB)
totalRAM	VM에서 사용할 수 있는 총 RAM(MB)
type	호스트 유형
vCenterId	VM의 고유 ID 번호
vCenterName*	vCenter 호스트 이름
virtualSwitchName*	가상 스위치의 수
vmFolderPath	VM 파일의 디렉터리 경로.
vmName	가상 머신의 수

Discovery Connector 데이터 수집

VMware 환경에서 Discovery Connector를 배포하고 구성한 후 중지되면 데이터 컬렉션을 다시 시작할 수 있습니다. 콘솔을 통해 또는를 통해 API 호출을 수행하여 데이터 수집을 시작하거나 중지할 수 있습니다 AWS CLI. 이 두 방법 모두 다음 절차에 설명되어 있습니다.

Using the Migration Hub Console

다음 절차에서는 Migration Hub 콘솔의 Data Collectors 페이지에서 Discovery Connector 데이터 수집 프로세스를 시작하거나 중지하는 방법을 보여줍니다.

데이터 수집을 시작하거나 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 AWS CLI를 설치 AWS CLI 한 다음 선택한 Migration Hub 홈 리전을 사용하도록 CLI를 설정해야 합니다.

를 설치하고 데이터 수집을 AWS CLI 시작하려면

1. 운영 체제(Linux, macOS 또는 Windows) AWS CLI 용를 설치합니다. 지침은 AWS Command Line Interface 사용 설명서를 참조하세요.
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 리전 이름에 홈 리전을 입력합니다. 예: `us-west-2`.

d. 기본 출력 형식에 `text`를 입력합니다.

3. 데이터 수집을 시작하거나 중지하려는 커넥터의 ID를 찾으려면 다음 명령을 입력하여 커넥터의 ID를 확인합니다.

```
aws discovery describe-agents --filters
 condition=EQUALS,name=hostName,values=connector
```

4. 커넥터로 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.

커넥터로 데이터 수집을 중지하려면 다음 명령을 입력합니다.

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

Discovery Connector 문제 해결

> **Important**
>
> 현재 Discovery Connector를 사용하는 고객은 새 Agentless Collector로 전환하는 것이 좋습니다. 2025년 11월 17일부터 Discovery Connectors에서 새 데이터 수락을 AWS Application Discovery Service 중지합니다. 자세한 내용은 Discovery Connector 단원을 참조하십시오.

이 섹션에는 Application Discovery Service Discovery Connector에서 알려진 문제를 해결하는 데 도움이 되는 주제가 포함되어 있습니다.

설정 AWS 중에 Discovery Connector에 도달할 수 없는 문제 해결

콘솔에서 AWS 에이전트리스 검색 커넥터를 구성할 때 다음 오류 메시지가 표시될 수 있습니다.

> **연결할 수 없음 AWS**
>
> AWS 에 연결할 수 없습니다(연결 재설정). 네트워크 및 프록시 설정을 확인하십시오.

이 오류는 설정 프로세스 중에 커넥터가 통신해야 하는 AWS 도메인에 대한 HTTPS 연결을 설정하려는 Discovery Connector의 시도가 실패했기 때문에 발생합니다. 연결을 설정할 수 없는 경우 Discovery Connector 구성이 실패합니다.

에 대한 연결을 수정하려면 AWS

1. IT 관리자에게 문의하여 회사 방화벽이 포트 443에서 아웃바운드 액세스 AWS 가 필요한 도메인으로의 송신 트래픽을 차단하고 있는지 확인합니다.

   다음 AWS 도메인에는 아웃바운드 액세스가 필요합니다.

   - `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 해제합니다. 방화벽을 업데이트한 후 커넥터를 다시 구성합니다.
2. 방화벽을 업데이트해도 연결 문제가 해결되지 않는 경우 커넥터 가상 머신에 나열된 도메인에 대한 아웃바운드 네트워크 연결이 있는지 확인합니다. 가상 머신에 아웃바운드 연결이 있는 경우 다음 예제와 같이 포트 443에서 텔넷을 실행하여 나열된 도메인에 대한 연결을 테스트합니다.

   ```
   telnet ec2.amazonaws.com 443
   ```
3. 가상 머신의 아웃바운드 연결이 활성화된 경우 추가 문제 해결을 위해 AWS Support에 문의해야 합니다.

비정상 커넥터 수정

모든 Discovery Connector의 상태 정보는 Migration Hub 콘솔의 Data Collectors 페이지에서 확인할 수 있습니다. 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 창에서 데이터 수집기를 선택합니다.
2. 커넥터 탭에서 상태 상태가 비정상인 각 커넥터의 IP 주소를 기록해 둡니다.
3. 커넥터 가상 머신에 연결할 수 있는 컴퓨터에서 브라우저를 열고 커넥터 콘솔의 URL을 입력합니다. `https://ip_address_of_connector`여기서 `ip_address_of_connector`는 비정상 커넥터의 IP 주소입니다.
4. 커넥터를 구성했을 때 설정된 커넥터 관리 콘솔 암호를 입력합니다.

커넥터 콘솔에 액세스하면 비정상 상태를 해결하기 위한 조치를 취할 수 있습니다. 여기에서 vCenter 연결에 대한 정보 보기를 선택할 수 있으며 진단 메시지가 포함된 대화 상자가 표시됩니다. 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 문의하세요.

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 서버의 운영 상태를 확인하거나 설정 편집을 선택하여 vCenter 엔드포인트를 업데이트"라는 메시지가 포함된 대화 상자가 표시됩니다.

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` 또는와 같은 별도의 명령줄 도구를 사용하여 연결된 vCenter 서버가 활성 상태이고 커넥터 VM에서 IP에 연결할 수 있는지 `traceroute`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 " 편집 설정을 선택하여 읽기 및 보기 권한으로 계정의 vCenter 사용자 이름과 암호를 업데이트합니다."라는 메시지가 포함된 대화 상자가 표시됩니다.

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.

독립 실행형 ESX 호스트 지원

Discovery Connector는 독립 실행형 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 보내 달라는 요청을 받게 될 것입니다. 다음 방법으로 로그를 입수할 수 있습니다.

- AWS Agentless Discovery Connector 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.