

클라우드용 APTARE IT Analytics Data Collector 설 치 설명서

릴리스 **10.5**

클라우드용 APTARE IT Analytics Data Collector 설치 설명서

마지막 업데이트 날짜: 2021-09-01

법적 고지

Copyright © 2021 Veritas Technologies LLC. All rights reserved.

Veritas 및 Veritas 로고는 미국 및 기타 국가에서 Veritas Technologies LLC 또는 그 자회사의 상표 또는 등록 상표입니다. 다른 이름은 해당 회사의 상표일 수 있습니다.

이 제품에는 타사 저작자 표시가 필요한 타사 소프트웨어("타사 프로그램")가 포함될 수 있습니다. 일부 타사 프로그램은 오픈 소스 또는 무료 소프트웨어 라이선스에 따라 사용 가능합니다. 이러한 오픈 소스 또는 무료 소프트웨어 라이선스에 따라 얻은 권리나 책임은 소프트웨어에 첨부된 라이선스 계약에 의해 변경되지 않습니다. 이 베리타스 제품과 함께 제공되거나 다음 위치에서 확인할 수 있는 타사 법적 고지 문서를 참조하시기 바랍니다.

<https://www.veritas.com/about/legal/license-agreements>

이 문서에 설명되어 있는 제품은 사용, 복사, 배포 및 디컴파일/리버스 엔지니어링을 제한하는 라이선스 하에 배포됩니다. 이 문서의 어떤 부분도 Veritas Technologies LLC 및 그 라이선스 제공자의 사전 서면 승인 없이는 어떤 방식, 어떤 형태로도 복제될 수 없습니다.

이 문서는 "있는 그대로" 제공되며, 상품성, 특정 목적 적합성 또는 비침해성에 대한 묵시적 보증을 비롯하여 어떠한 명시적 또는 묵시적인 조건, 진술 및 보증도, 이러한 조건, 진술 및 보증의 배제가 법적으로 무효가 아닌 한, 배제됩니다. Veritas Technologies LLC는 이 문서의 제공, 성능 또는 사용과 관련되는 우발적 손해 또는 결과적 손해에 대해 책임을 지지 않습니다. 이 문서에 포함된 정보는 예고 없이 변경될 수 있습니다.

라이선스가 부여된 소프트웨어 및 문서는 FAR 12.212에서 정한 조건에 따라 상업용 컴퓨터 소프트웨어로 간주되며, 베리타스가 온프레미스 또는 호스트 서비스로 제공하는지 여부와 관계없이, 적용 가능한 경우 FAR 항목 52.227-19 "상업용 컴퓨터 소프트웨어 - 제한된 권리" 및 DFARS 227.7202, 이하 참조 "상업용 컴퓨터 소프트웨어 및 상업용 컴퓨터 소프트웨어 문서" 및 이에 갈음하는 규정에서 정의된 제한된 권리를 따릅니다. 미합중국 정부에 의한 이 소프트웨어의 사용, 수정, 복제 출시, 실행, 표시 또는 공개는 전적으로 이 라이선스 계약의 조건을 따릅니다.

Veritas Technologies LLC
2625 Augustine Drive.
Santa Clara, CA 95054

<http://www.veritas.com>

기술 지원

기술 지원 그룹은 전 세계에 걸쳐 지원 센터를 운영합니다. 모든 지원 서비스는 지원 계약 및 현재 기업의 기술 지원 정책에 따라 제공됩니다. 지원 프로그램에 대한 자세한 내용과 기술 지원에 문의하는 방법은 베리타스 웹 사이트를 참조하십시오.

<https://www.veritas.com/support>

다음 URL에서 베리타스 계정 정보를 관리할 수 있습니다.

<https://my.veritas.com>

기존 지원 계약과 관련하여 궁금한 점이 있는 경우 다음과 같이 해당 지역의 지원 계약 관리 팀에 이메일로 문의하십시오.

전 세계(일본 제외)

CustomerCare@veritas.com

일본

CustomerCare_Japan@veritas.com

문서

문서가 최신 버전인지 확인하십시오. 각 문서의 2페이지에 마지막 업데이트 날짜가 표시됩니다. Veritas 웹 사이트에서 최신 문서를 사용할 수 있습니다.

Veritas SORT(서비스 및 운영 준비 도구)

Veritas SORT(서비스 및 운영 준비 도구)는 시간 소모적인 관리 태스크의 자동화 및 간소화를 위한 정보와 도구를 제공하는 웹 사이트입니다. 제품에 따라 SORT에서 설치 및 업그레이드를 준비하고, 데이터 센터의 위험 요소를 식별하고, 운영 효율성을 개선하는 데 유용한 정보 및 도구를 얻을 수 있습니다. SORT가 제품에 제공하는 서비스 및 도구를 보려면 데이터시트를 참조하십시오.

https://sort.veritas.com/data/support/SORT_Data_Sheet.pdf

목차

1장	Amazon Web Services(AWS)용 사전 설치 설정	6
	Amazon Web Services(AWS)용 사전 설치 설정	6
	Data Collector 추가를 위한 필수 구성 요소(Amazon Web Services)	7
	Amazon Web Services(AWS) 구성을 위한 필수 구성 요소	7
	청구 리포트를 수신하도록 S3 버킷 구성	8
	비용 할당 태그 선택	8
	AWS IAM 사용자 생성	9
	통합된 청구 데이터 수집을 위해 AWS 계정 연결	9
	APTARE IT Analytics 데이터 수집을 위한 역할 생성	10
	IAM 사용자에게 역할 추가	10
	설치 개요(Amazon Web Services - AWS)	11
	Amazon Web Services(AWS) 정책 추가	11
2장	OpenStack Ceilometer용 사전 설치 설정	16
	OpenStack Ceilometer용 사전 설치 설정	16
	Data Collector 추가를 위한 필수 구성 요소(OpenStack Ceilometer)	16
	설치 개요(OpenStack Ceilometer)	17
	OpenStack Ceilometer Data Collector 정책 추가	17
3장	OpenStack Swift용 사전 설치 설정	21
	OpenStack Swift용 사전 설치 설정	21
	Data Collector(OpenStack Swift) 추가를 위한 필수 구성 요소	21
	설치 개요(OpenStack Swift)	22
	OpenStack Swift Data Collector 정책 추가	22
4장	Microsoft Azure용 사전 설치 설정	26
	Microsoft Azure용 사전 설치 설정	26
	Microsoft Azure 데이터 수집을 위한 인증 정보 설정	27
	Windows 시스템에 Azure PowerShell 클라이언트 설치	27
	테넌트 및 구독 ID 찾기	27
	Data Collector에 대한 새 응용 프로그램 등록	28
	주체 생성 및 응용 프로그램에 역할 할당	28
	Data Collector(Microsoft Azure) 추가를 위한 필수 구성 요소	30
	설치 개요(Microsoft Azure)	30

	Microsoft Azure Data Collector 정책 추가	30
5장	Data Collector 소프트웨어 설치	34
	소개	34
	WMI 프록시 서비스 설치(Windows Host Resources만 해당)	34
	WMI 연결 테스트	35
6장	데이터 수집 유효성 검사	38
	유효성 검사 방법	38
	Data Collector: 벤더별 유효성 검사 방법	39
	요청 시 데이터 수집 작업	41
	CLI check install 유틸리티 사용	42
	Data Collector 구성 나열	44
7장	Data Collector 제거	45
	Linux에서 Data Collector 제거	45
	Windows에서 Data Collector 제거	45
8장	Data Collector 수동 시작	46
	소개	46
부록 A	방화벽 구성: 기본 포트	47
	방화벽 구성: 기본 포트	47

Amazon Web Services(AWS)용 사전 설치 설정

이 장의 내용은 다음과 같습니다.

- [Amazon Web Services\(AWS\)용 사전 설치 설정](#)
- [Data Collector](#) 추가를 위한 필수 구성 요소([Amazon Web Services](#))
- [Amazon Web Services\(AWS\)](#) 구성을 위한 필수 구성 요소
- 청구 리포트를 수신하도록 [S3 버킷](#) 구성
- 비용 할당 태그 선택
- [AWS IAM](#) 사용자 생성
- 통합된 청구 데이터 수집을 위해 [AWS 계정 연결](#)
- 설치 개요([Amazon Web Services - AWS](#))
- [Amazon Web Services\(AWS\)](#) 정책 추가

Amazon Web Services(AWS)용 사전 설치 설정

대부분의 경우 [Data Collector](#)의 단일 인스턴스로 원하는 수의 엔터프라이즈 개체를 지원할 수 있습니다. 그러나 각 환경에는 고유한 배포 구성 요구 사항이 있으므로, 설치해야 하는 [Data Collector](#)의 수와 배포에 가장 적합한 서버를 결정할 수 있도록 [Data Collector](#) 소프트웨어를 설치해야 하는 위치를 이해하는 것이 중요합니다.

Data Collector 추가를 위한 필수 구성 요소(Amazon Web Services)

- 64비트 OS. 지원되는 운영 체제는 인증 구성 설명서를 참조하십시오.
- APTARE IT Analytics 시스템으로 벤더 하위 시스템의 데이터를 수집하는 경우 이름/값 쌍은 미국 영어여야 하며 미국 영어 로캘의 관리자가 설치를 완료해야 합니다. 서버의 언어 버전은 미국 영어가 아니어도 됩니다.
- rpm fontconfig가 설치되었는지 확인하십시오. fontconfig는 시스템 전체 글꼴 구성, 사용자 정의 및 응용 프로그램 액세스를 제공하는 라이브러리입니다. rpm fontconfig가 설치되지 않은 경우 설치 프로그램에서 사용자 인터페이스 모드를 로드할 수 없습니다. 이 라이브러리는 새로운 Data Collector 설치에 필요한 사전 요구 사항입니다.
- Amazon Corretto 11을 지원합니다. Amazon Corretto는 OpenJDK(Open Java Development Kit)의 다중 플랫폼 및 프로덕션용 무료 배포판입니다.
- 성능상의 이유로, APTARE IT Analytics 포털과 동일한 서버에 Data Collector를 설치하지 마십시오. 그러나 둘 모두 동일한 서버에 있어야 하는 경우 포털 및 Data Collector 소프트웨어가 동일한 디렉터리에 없음을 확인하십시오.
- 서버(또는 OS 인스턴스)에 Data Collector 하나만 설치하십시오.

Amazon Web Services(AWS) 구성을 위한 필수 구성 요소

Amazon Web Services Data Collector는 다음과 같은 AWS 객체에서 수집할 수 있습니다.

- **S3 버킷(상세 내역 및 사용량)**- 클라우드의 저장소에 대한 S3(Simple Storage Service)
- **EC2 상세 내역** - 가상 서버와 매우 유사한 컴퓨팅 서비스를 위한 EC2(Elastic Cloud Compute)
- **청구 레코드** - 서비스별 사용량 및 해당하는 요금

수집되는 데이터 유형에 대한 자세한 내용은 Data Collector 정책 구성을 참조하십시오.

참고: API 요청 속도의 제한으로 인해 여러 동시 프로세스가 수집을 방해할 수 있습니다. 여러 Amazon Web Services(AWS) 데이터 수집 프로세스와 다른 AWS 스크립트를 동일한 기간에 예약해서는 안 됩니다.

Data Collector가 데이터를 검색할 수 있는 읽기 전용 액세스를 확보할 수 있도록 먼저 다음 단계를 Amazon Web Services(AWS)에서 수행해야 합니다.

1. 청구 리포트를 수신하도록 S3 버킷을 구성하십시오. 8페이지의 “[청구 리포트를 수신하도록 S3 버킷 구성](#)” 참조

2. 비용 할당 태그를 선택하십시오.8페이지의 “비용 할당 태그 선택” 참조
 3. AWS IAM 사용자를 생성하고 액세스 키를 생성하십시오.9페이지의 “AWS IAM 사용자 생성” 참조
 4. 통합된 청구 데이터 수집을 위해 AWS 계정을 연결하십시오.9페이지의 “통합된 청구 데이터 수집을 위해 AWS 계정 연결” 참조
 5. 포털에서 Collector를 설치하십시오.
 6. 포털에서 Data Collector 정책을 추가하십시오.
- 11페이지의 “설치 개요(Amazon Web Services - AWS)” 참조

청구 리포트를 수신하도록 S3 버킷 구성

Amazon Web Services(AWS)에서 리소스 및 태그가 포함된 청구 리포트를 수신하도록 S3 버킷(Simple Storage Service Bucket)을 구성해야 합니다.

1. AWS Data Collector에서 액세스할 청구 레코드를 수집하는 **S3** 버킷을 생성합니다.
2. AWS 청구 및 비용 관리 기본 설정(AWS Billing and Cost Management Preferences)에서 **S3** 버킷을 청구 레코드 수신(Receive Billing Records)으로 구성합니다.
3. AWS에서 제공하는 샘플 정책에서 텍스트를 복사합니다.

이 정책은 AWS 청구를 통해 S3 버킷에 청구 레코드 파일을 생성할 수 있는 권한을 설정합니다.

4. S3 버킷 속성에서 샘플을 정책에 붙여 넣어 버킷 정책을 추가하십시오.
5. S3 버킷을 확인하십시오.
6. 비용 할당 태그를 선택하십시오.

8페이지의 “비용 할당 태그 선택” 참조

비용 할당 태그 선택

1. AWS 리소스에 할당된 비용 할당 태그를 선택하십시오. 그러면, 이러한 태그가 청구 리포트에 나타나고 Data Collector에 의해 수집됩니다. 태그는 사용자가 정의하며 청구 및 보고의 그룹화와 총계 계산을 실행합니다.

사용자 정의 태그는 EC2 및 S3 리소스의 수집에 사용됩니다. 이러한 태그는 EC2 인스턴스 및 S3 버킷의 총 비용에 대한 비용 할당 보고에 필요합니다.

참고: Amazon Web Services는 하루에 한 번 이상 리포트를 생성하며 한 달 동안 매일 총계가 추가됩니다. 따라서 APTARE IT Analytics Data Collector에 의해 수집되는 S3 버킷에 청구 레코드 파일이 나타나려면 최대 24시간이 걸릴 수 있습니다.

2. AWS IAM 사용자를 생성하십시오.

9페이지의 “AWS IAM 사용자 생성” 참조

AWS IAM 사용자 생성

데이터 수집에는 제한적인 권한을 가진 Amazon Web Services(AWS) Identity and Access Management(IAM) 사용자가 필요합니다. 이 사용자에게는 S3 버킷의 청구 레코드를 수집할 수 있을 뿐만 아니라 EC2 리소스 및 모든 S3 버킷에 대한 데이터를 검색하기 위한 AWS API 메서드에 액세스할 수 있는 읽기 전용 권한이 있어야 합니다.

9페이지의 “통합된 청구 데이터 수집을 위해 AWS 계정 연결” 참조

1. Amazon Web Services IAM 관리 콘솔에서 APTARE IT Analytics Data Collector에서 사용하는 IAM 사용자를 생성하십시오.

사용자(Users) > 새 사용자 생성(Create New Users) >을 누르고 사용자 이름을 입력하십시오.

각 사용자에게 대한 액세스 키 생성을 선택했는지 확인하십시오.

이 구성에서는 액세스 키 ID 및 비밀 액세스 키가 다음 보안 인증 정보로 생성됩니다.

2. 나중에 Data Collector 정책을 구성할 때 필요한 인증 정보를 다운로드하십시오.

이러한 인증 정보는 APTARE IT Analytics AWS Data Collector 정책을 구성할 때 필요합니다. 액세스 키 및 비밀 액세스 키는 Data Collector에서 AWS API에 대한 읽기 전용 요청을 수행하는 데 사용됩니다.

3. IAM 창에서 앞서 생성한 IAM 사용자를 선택하고 AWS에서 제공한 ReadOnlyAccess 정책을 첨부하여 권한을 부여하십시오.

이 읽기 전용 정책을 사용하면 Data Collector가 EC2 리소스 및 S3 버킷의 데이터를 검색할 수 있습니다.

4. 예를 들어 민감한 데이터가 있는 버킷에 대한 액세스를 제한하기 위해 사용자 정의 AWS 정책을 생성할 수 있습니다.

5. AWS 계정을 연결하려면 다음을 참조하십시오.

9페이지의 “통합된 청구 데이터 수집을 위해 AWS 계정 연결” 참조

통합된 청구 데이터 수집을 위해 AWS 계정 연결

일부 대규모 조직에서는 서로 다른 비용 센터에 대해 별도의 AWS 계정을 생성한 다음 이러한 계정을 납부자 계정에 연결합니다. 이 경우 이러한 모든 계정에 대한 청구 레코드는 납부자 계정에 대한 청구 레코드에 누적됩니다. 단일 AWS IAM 사용자가 이러한 청구 레코드와 EC2 및 S3 버킷에 대한 다른 모든 정보를 수집하게 하려면 해당 사용자에게

교차 계정 API 액세스 권한을 부여해야 합니다. 계정을 연결하여 계정 간에 신뢰 관계를 설정합니다.

APTARE IT Analytics 데이터 수집을 위한 역할 생성

1. 납부자 계정이 아닌 AWS 계정에 로그인하십시오.
2. AWS IAM 창에서 **역할**을 선택하십시오.
3. **readOnlyAccessForCollection**과 같이 데이터 수집용으로 한정된 역할을 식별하는 역할 이름을 입력하십시오. 역할이 생성된 후에는 입력한 이름을 변경할 수 없습니다.
4. 역할 유형 선택: **교차 계정 액세스를 위한 역할 > 소유한 AWS 계정 간의 액세스 제공**.
5. 납부자 계정의 계정 ID를 사용하여 신뢰 관계를 설정하지만 MFA는 필요하지 않습니다.
6. AWS에서 제공한 **ReadOnlyAccess** 정책을 첨부하십시오.
7. 역할을 생성하기 전에 역할 정보를 검토하여 다음과 같은 정보가 올바른지 확인하십시오.
 - **역할 이름:** APTARE IT Analytics 데이터 수집을 위해 이름이 지정된 역할.
 - **신뢰할 수 있는 객체:** 납부자 계정의 ID.
 - **정책:** **ReadOnlyAccess**.
8. 역할 **ARN**을 클립보드에 복사하십시오. IAM 사용자에게 역할을 추가할 때 이 복사된 ARN(Amazon Resource Name)을 사용합니다.
10페이지의 **“IAM 사용자에게 역할 추가”** 참조
9. 역할 생성을 눌러 계정을 연결하십시오.
10. IAM 사용자에게 역할을 추가하십시오.

IAM 사용자에게 역할 추가

1. AWS 납부자 계정에 로그인하십시오.
2. AWS IAM 창에서 생성한 사용자를 선택하십시오.
9페이지의 **“AWS IAM 사용자 생성”** 참조
3. 사용자의 권한에서 나열된 **ReadOnlyAccess** 정책에 추가로 **인라인 정책**을 생성하십시오.
4. 사용자 정의 정책을 선택하고 **정책 이름**을 입력하십시오.

5. 정책을 편집하여 사용 권한을 사용자 정의하십시오. 아래의 **빨간색**으로 표시된 **Resource** 예를 앞서 클립보드에 복사한 **역할 ARN**을 끝은 따옴표로 묶어서 바꾸십시오.

```
{ "Statement": [
  {
    "Effect": "Allow",
    "Action": "sts:AssumeRole",
    "Resource": "arn:aws:iam::123456789012:role/accessForAPTARECollector"
  }
]
```

6. 이제 AWS 구성이 완료되었습니다. 데이터 수집 구성을 계속하십시오.

설치 개요(Amazon Web Services - AWS)

다음 목록을 사용하여 표시된 순서대로 각 단계를 완료하십시오.

1. 로컬 호스트 파일을 업데이트하십시오. 이렇게 하면 포털에 액세스할 수 있습니다.
2. 포털에서 **Data Collector**를 아직 생성하지 않은 경우 지금 추가하십시오.
3. 포털에서 **Amazon Web Services Policy Data Collector** 정책을 추가하십시오.
4. **Data Collector** 서버에서 **Data Collector** 소프트웨어를 설치하십시오.
5. **Data Collector** 설치의 유효성을 검사하십시오.

Amazon Web Services(AWS) 정책 추가

- 정책 추가 전: **Data Collector** 정책을 추가할 **Data Collector**가 포털에 있어야 합니다. 특정 벤더에 대한 특정 필수 구성 요소 및 지원되는 구성에 대해서는 인증 구성 설명서를 참조하십시오.
- 정책 추가 후: 일부 정책에서 **Collector** 관리 페이지 작업 모음의 **실행** 버튼을 사용하여 요청 시 수집을 실행할 수 있습니다. 실행 버튼은 정책 벤더가 지원되는 경우에만 표시됩니다.

요청 시 수집을 사용하면 수집을 실행할 프로브 및 장치를 선택할 수 있습니다. 이 작업은 예약된 실행과 동일한 데이터를 수집하면서 문제 해결을 위한 로그 정보도 수집합니다. 프로브에 대한 설명은 정책을 참조하십시오.

정책을 추가하려면 다음과 같이 하십시오.

- 1 관리 > 데이터 수집 > **Collector** 관리를 선택하십시오. 현재 구성된 포털 **Data Collector**가 표시됩니다.
- 2 필요한 경우 **Collector**를 검색하십시오.
- 3 목록에서 **Data Collector**를 선택하십시오.
- 4 정책 추가를 누른 다음 메뉴에서 벤더별 항목을 선택하십시오.
- 5 매개 변수를 입력하거나 선택하십시오. 필수 매개 변수는 별표(*)로 표시됩니다.

참고: API 요청 속도의 제한으로 인해 여러 동시 프로세스가 수집을 방해할 수 있습니다. 여러 Amazon Web Services(AWS) 데이터 수집 프로세스와 다른 AWS 스크립트를 동일한 기간에 예약해서는 안 됩니다.

표 1-1 Amazon Web Services Data Collector 정책

필드	설명
Collector 도메인	Collector 백업 정책이 추가되는 Collector의 도메인. 읽기 전용 필드입니다. 기본적으로 새 정책의 도메인은 Collector의 도메인과 동일합니다. 이 필드는 Collector를 추가할 때 설정됩니다.
정책 도메인	정책 도메인은 Data Collector에 대해 구성되는 정책의 도메인입니다. 정책 도메인은 Collector 도메인과 동일한 값으로 설정되어야 합니다. 도메인은 호스트 그룹 계층의 최상위 수준을 식별합니다. 새로 검색된 모든 호스트는 정책 도메인과 연결된 루트 호스트 그룹에 추가됩니다. 일반적으로 드롭다운 목록에는 정책 도메인 하나만 사용할 수 있습니다. MSP(Managed Services Provider)인 경우 각 고객에게 고유한 호스트 그룹 계층이 있는 고유한 도메인이 있습니다. 도메인 이름을 찾으려면 사용자 계정 메뉴에서 내 프로필 을 선택하십시오.
계정 ID 또는 별칭	AWS 관리 콘솔에 표시된 AWS 계정 ID 번호를 입력하십시오. Amazon 계정의 지불 계정 ID입니다. 계정 별칭이 생성된 경우 계정 ID 대신 사용할 수 있습니다.
액세스 키	AWS IAM 사용자의 액세스 키 ID를 입력하십시오.
보안 키	AWS IAM 사용자의 보안 액세스 키를 입력하십시오.
S3 버킷 청구	APTARE IT Analytics AWS Data Collector 정책에 대한 청구 레코드를 수집하기 위해 특별히 생성된 S3 버킷의 이름입니다.

표 1-1 Amazon Web Services Data Collector 정책 (계속)

필드	설명
EC2 상세 내역	다음과 같은 상세 내역을 포함하여 EC2 인스턴스, EBS 볼륨 및 EBS 볼륨 스냅샷과 해당 개체 간의 관계를 수집합니다. - EC2 인스턴스: 이름, 태그, 지역, 가용성 영역, 시작 날짜, 상태, 유형, 가상화, 모니터링 구성. - EBS 볼륨: 이름, 태그, 지역, 가용성 영역, 생성 날짜, 상태, 유형, 크기. - EBS 볼륨 스냅샷: 이름, 태그, 지역, 생성 시작 날짜, 진행률, 상태, 볼륨 크기.
S3 상세 내역	이름, 태그, 지역, 소유자, 생성 시점 및 버전 정보 같은 S3 버킷 상세 내역을 수집합니다.
	참고: 많은 수의 개체가 있는 버킷의 경우 이 수집에 긴 시간이 걸릴 수 있습니다. 저장소 버킷 사용량 추적은 다음 AWS 지역에서 지원됩니다. - us-east-1 - us-east-2 - us-west-1 - us-west-2 - af-south-1 - ap-east-1 - ap-south-1 - ap-northeast-3 - ap-northeast-2 - ap-southeast-1 - ap-southeast-2 - ap-northeast-1 - ca-central-1 - eu-central-1 - eu-west-1 - eu-west-2 - eu-west-3 - eu-south-1 - eu-north-1 - me-south-1 - sa-east-1 - us-gov-east-1 - us-gov-west-1

표 1-1 Amazon Web Services Data Collector 정책 (계속)

필드	설명
청구 레코드	청구서, 리소스, 납부자, 연결된 계정, 사용 유형 및 비용 같은 리소스와 태그가 있는 상세 청구 리포트의 모든 필드를 수집합니다.
예약	참고: AWS 청구 레코드는 24시간마다 한 번씩 업데이트됩니다. 따라서 APTARE IT Analytics에서 청구 레코드를 사용하려면 이 Data Collector 정책을 구성한 후 24시간이 걸릴 수 있습니다. 예약을 생성하려면 시계 아이콘을 누르십시오. 매분, 매시간, 매일, 매주 및 매월 예약을 생성할 수 있습니다. 기본 CRON 문자열의 고급 용법도 사용할 수 있습니다. CRON 식의 예: */30 **** 30분마다 한 번을 의미합니다. */20 9-18 *** 오전 9시부터 오후 6시까지 20분마다 한 번을 의미합니다. */10 *** 1-5 월요일부터 금요일까지 10분마다 한 번을 의미합니다. 참고: Collector 정책에 대해 설정된 명시적 예약은 Collector 서버의 시간을 기준으로 상대적입니다. 빈도가 있는 예약은 Data Collector가 재시작된 시간을 기준으로 상대적입니다.
참고	Data Collector 정책에 대한 메모를 입력하거나 편집하십시오. 최대 문자 수는 1024자입니다. 정책 메모는 특정 벤더에 대한 정책 정보와 함께 유지되며 Collector 관리 페이지에 열로 표시되고 검색도 가능합니다.
연결 테스트	연결 테스트에서는 정책에 제공된 IP 주소 및 인증 정보를 사용하여 AWS에 연결하는 Data Collector 프로세스가 시작됩니다. 이 유효성 검사 프로세스에서는 성공 메시지 또는 특정 연결 오류 목록이 반환됩니다. 연결 테스트를 수행하려면 에이전트 서비스가 실행 중이어야 합니다. 유효성 검사 요청의 응답 시간에는 여러 요인이 영향을 미치므로 일부 요청은 다른 요청보다 시간이 오래 걸립니다. 예를 들어 AWS에 연결할 때 지연이 발생할 수 있습니다. 마찬가지로, Data Collector에서 실행 중인 다른 처리 스레드로 인해 응답 수신에 지연될 수 있습니다. 또한 관리 > 데이터 수집 > Collector 관리에서 사용할 수 있는 실행 기능을 사용하여 데이터 수집을 테스트할 수 있습니다. 이 요청 시 데이터 수집 실행은 도메인, 호스트 그룹, URL, Data Collector 정책 및 데이터베이스 연결에 대한 확인을 포함하여 개별 정책 수준에서 설치의 개략적 확인을 시작합니다. 수집 실행을 테스트하기 위해 개별 프로브 및 서버를 선택할 수도 있습니다.

참고: 초기 데이터 수집 기간에 대한 자세한 내용은 다음을 참조하십시오.

15페이지의 [“AWS 수집 기간 수정”](#) 참조

AWS 수집 기간 수정

Amazon Web Services(AWS) 청구 데이터를 처음 수집할 때 **Data Collector**는 한 달 분량의 데이터를 수집합니다. 이 기간을 재정의하려면 **AWS_BILLING_LOOKBACK_MONTHS** 고급 매개 변수를 첫 번째 수집 중에 검색해야 하는 청구 기록의 개월 수로 설정하십시오.

참고: 매개 변수를 설정하려면 **관리자 > 고급**으로 이동한 다음 **매개 변수**를 누르십시오. 매개 변수 페이지가 표시됩니다.

The screenshot shows the Veritas APTARE IT Analytics™ Admin interface. The left sidebar contains a navigation menu with items like Users, Domains, Chargeback, Solutions, Data Collection, Reports, Thresholds, NetBackup Discovery, Backup SLA, Master Schedules, Backup Windows, Method Designer, File List, Advanced, and Parameters. The 'Parameters' item is highlighted with a red box and a red arrow. The main content area is titled 'Parameters' and includes buttons for Add, Refresh, and Download. Below these buttons is a table with columns for Domain, Collector, and Parameter. The table contains two rows: one for 'ABCIndustry' with 'FA_CLEAN_UP_TEMPORARY_FILES' as the parameter, and another for 'ABCIndustry' with 'ACCESS_CONTROL_FALLBACK_STRINGS' as the parameter. The 'Admin' button in the top right corner is also highlighted with a red box and a red arrow.

Domain	Collector	Parameter
ABCIndustry		FA_CLEAN_UP_TEMPORARY_FILES
ABCIndustry		ACCESS_CONTROL_FALLBACK_STRINGS

OpenStack Ceilometer용 사전 설치 설정

이 장의 내용은 다음과 같습니다.

- [OpenStack Ceilometer용 사전 설치 설정](#)
- [Data Collector 추가를 위한 필수 구성 요소\(OpenStack Ceilometer\)](#)
- [설치 개요\(OpenStack Ceilometer\)](#)
- [OpenStack Ceilometer Data Collector 정책 추가](#)

OpenStack Ceilometer용 사전 설치 설정

대부분의 경우 **Data Collector**의 단일 인스턴스로 원하는 수의 엔터프라이즈 개체를 지원할 수 있습니다. 그러나 각 환경에는 고유한 배포 구성 요구 사항이 있으므로, 설치해야 하는 **Data Collector**의 수와 배포에 가장 적합한 서버를 결정할 수 있도록 **Data Collector** 소프트웨어를 설치해야 하는 위치를 이해하는 것이 중요합니다.

Data Collector 추가를 위한 필수 구성 요소(OpenStack Ceilometer)

- 64비트 OS. 지원되는 운영 체제는 **Certified Configurations Guide**(영문)를 참조하십시오.
- **APTARE IT Analytics** 시스템으로 벤더 하위 시스템의 데이터를 수집하는 경우 이름/값 쌍은 미국 영어여야 하며 미국 영어 로캘의 관리자가 설치를 완료해야 합니다. 서버의 언어 버전은 미국 영어가 아니어도 됩니다.
- **rpm fontconfig**가 설치되었는지 확인하십시오. **fontconfig**는 시스템 전체 글꼴 구성, 사용자 정의 및 응용 프로그램 액세스를 제공하는 라이브러리입니다. **rpm fontconfig**가

설치되지 않은 경우 설치 프로그램에서 사용자 인터페이스 모드를 로드할 수 없습니다. 이 라이브러리는 새로운 **Data Collector** 설치의 필수 구성 요소입니다.

- **Amazon Corretto 11**을 지원합니다. **Amazon Corretto**는 **OpenJDK(Open Java Development Kit)**의 다중 플랫폼 및 프로덕션용 무료 배포판입니다.
- 성능상의 이유로, **APTARE IT Analytics** 포털과 동일한 서버에 **Data Collector**를 설치하지 마십시오. 그러나 둘 모두 동일한 서버에 있어야 하는 경우 포털 및 **Data Collector** 소프트웨어가 동일한 디렉터리에 없음을 확인하십시오.
- 서버(또는 OS 인스턴스)에 **Data Collector** 하나만 설치하십시오.

설치 개요(OpenStack Ceilometer)

클라우드 기반 데이터 수집 중에 **APTARE IT Analytics**은 **OpenStack Ceilometer**를 지원합니다. **OpenStack Ceilometer**는 **OpenStack** 내의 다양한 다른 프로젝트를 통해 제공되는 메트릭을 일반적인 검색 메커니즘에 노출하여 차지백 청구를 수행할 수 있도록 합니다. 참고로 현재 **APTARE IT Analytics**은 **OpenStack Compute(Nova)**에 대한 메트릭만 캡처합니다. **SQL** 템플릿 디자이너에서 **Ceilometer** 뷰를 사용할 수 있으며 **Data Collector** 정책은 클라우드로 분류됩니다.

다음 목록을 사용하여 표시된 순서대로 각 단계를 완료하십시오.

1. 로컬 호스트 파일을 업데이트하십시오. 이렇게 하면 포털에 액세스할 수 있습니다.
2. 포털에서 **Data Collector**를 아직 생성하지 않은 경우 지금 추가하십시오.
3. 포털에서 **OpenStack Ceilometer Data Collector** 정책을 추가하십시오.
4. **Data Collector** 서버에서 **Data Collector** 소프트웨어를 설치하십시오.
5. **Data Collector** 설치의 유효성을 검사하십시오.

OpenStack Ceilometer Data Collector 정책 추가

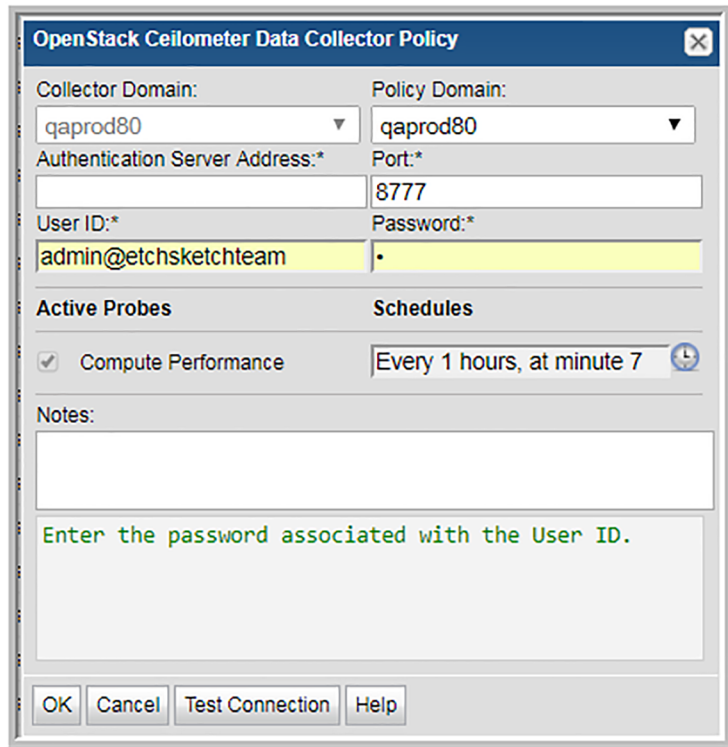
- 정책 추가 전: **Data Collector** 정책을 추가할 **Data Collector**가 포털에 있어야 합니다. 특정 벤더에 대한 특정 필수 구성 요소 및 지원되는 구성에 대해서는 인증 구성 설명서를 참조하십시오.
- 정책 추가 후: 일부 정책에서 **Collector** 관리 페이지 작업 모음의 실행 버튼을 사용하여 요청 시 수집을 실행할 수 있습니다. 실행 버튼은 정책 벤더가 지원되는 경우에만 표시됩니다.

요청 시 수집을 사용하면 수집을 실행할 프로브 및 장치를 선택할 수 있습니다. 이 작업은 예약된 실행과 동일한 데이터를 수집하면서 문제 해결을 위한 로그 정보도 수집합니다. 프로브에 대한 설명은 정책을 참조하십시오.

정책을 추가하려면 다음과 같이 하십시오.

- 1 관리 > 데이터 수집 > **Collector** 관리를 선택하십시오. 현재 구성된 포털 Data Collector가 표시됩니다.
- 2 필요한 경우 Collector를 검색하십시오.
- 3 목록에서 Data Collector를 선택하십시오.

- 4 정책을 추가를 누른 다음 메뉴에서 벤더별 항목을 선택하십시오.



The image shows a configuration window titled "OpenStack Ceilometer Data Collector Policy". It contains several input fields and sections for configuring the data collector policy.

Collector Domain:	Policy Domain:
qaprod80	qaprod80

Authentication Server Address:*	Port:*
	8777

User ID:*	Password:*
admin@etchsketchteam	*

Active Probes	Schedules
☒ Compute Performance	Every 1 hours, at minute 7

Notes:

Enter the password associated with the User ID.

Buttons: OK, Cancel, Test Connection, Help

5 매개 변수를 입력하거나 선택하십시오. 필수 매개 변수는 별표(*)로 표시됩니다.

필드	설명
Collector 도메인	Collector 백업 정책이 추가되는 Collector의 도메인. 읽기 전용 필드입니다. 기본적으로 새 정책의 도메인은 Collector의 도메인과 동일합니다. 이 필드는 Collector를 추가할 때 설정됩니다.
정책 도메인	정책 도메인은 Data Collector에 대해 구성되는 정책의 도메인입니다. 정책 도메인은 Collector 도메인과 동일한 값으로 설정되어야 합니다. 도메인은 호스트 그룹 계층의 최상위 수준을 식별합니다. 새로 검색된 모든 호스트는 정책 도메인과 연결된 루트 호스트 그룹에 추가됩니다. 일반적으로 트러블슈팅 목록에는 정책 도메인 하나만 사용할 수 있습니다. MSP(Managed Services Provider)인 경우 각 고객에게 고유한 호스트 그룹 계층이 있는 고유한 도메인이 있습니다. 도메인 이름을 찾으려면 로그인 이름을 누르고 메뉴에서 내 프로필을 선택하십시오. 도메인 이름이 프로필 설정에 표시됩니다.
인증 서버 주소*	ID 서비스를 포함하는 서버의 IP 주소와 포트 번호를 <ip address>:<port number> 형식으로 입력하십시오. 기본 포트인 35357에서 실행한다면 포트 번호가 필요하지 않습니다. 그러나 기본값과 다른 포트에서 실행하는 경우 포트 번호를 지정해야 합니다.
포트	Ceilometer API 서비스 포트.
사용자 ID*	테넌트/프로젝트에 대한 액세스 권한이 있는 사용자 ID를 입력하십시오. 이 사용자에게 모든 프로젝트에 액세스할 수 있는 관리자 역할이 있어야 합니다.
암호*	사용자 ID에 연결된 암호를 입력하십시오.
컴퓨팅 성능	마지막 수집 주기 이후의 시간을 기준으로 최대 1시간까지 메트릭을 수집하십시오. 시간당 수집 하나가 권장 기간입니다.
참고	Data Collector 정책에 대한 메모를 입력하거나 편집하십시오. 최대 문자 수는 1024자입니다. 정책 메모는 특정 벤더에 대한 정책 정보와 함께 유지되며 Collector 관리 페이지에 열로 표시되고 검색도 가능합니다.
연결 테스트	연결 테스트에서는 정책에 제공된 IP 주소 및 인증 정보를 사용하여 하위 시스템에 연결하는 Data Collector 프로세스가 시작됩니다. 이 유효성 검사 프로세스에서는 성공 메시지 또는 특정 연결 오류 목록이 반환됩니다. 연결 테스트를 수행하려면 에이전트 서비스가 실행 중이어야 합니다. 유효성 검사 요청의 응답 시간에는 여러 요인이 영향을 미치므로 일부 요청은 다른 요청보다 시간이 오래 걸립니다. 예를 들어 하위 시스템에 연결할 때 지연이 발생할 수 있습니다. 마찬가지로, Data Collector에서 실행 중인 다른 처리 스레드로 인해 응답 수신이 지연될 수 있습니다. 또한 관리 > 데이터 수집 > Collector 관리에서 사용할 수 있는 실행 기능을 사용하여 데이터 수집을 테스트할 수 있습니다. 이 요청 시 데이터 수집 실행은 도메인, 호스트 그룹, URL, Data Collector 정책 및 데이터베이스 연결에 대한 확인을 포함하여 개별 정책 수준에서 설치의 개략적 확인을 시작합니다. 수집 실행을 테스트하기 위해 개별 프로브 및 서버를 선택할 수도 있습니다.

OpenStack Swift용 사전 설치 설정

이 장의 내용은 다음과 같습니다.

- [OpenStack Swift용 사전 설치 설정](#)
- [Data Collector\(OpenStack Swift\) 추가를 위한 필수 구성 요소](#)
- [설치 개요\(OpenStack Swift\)](#)
- [OpenStack Swift Data Collector 정책 추가](#)

OpenStack Swift용 사전 설치 설정

대부분의 경우 **Data Collector**의 단일 인스턴스로 원하는 수의 엔터프라이즈 개체를 지원할 수 있습니다. 그러나 각 환경에는 고유한 배포 구성 요구 사항이 있으므로, 설치해야 하는 **Data Collector**의 수와 배포에 가장 적합한 서버를 결정할 수 있도록 **Data Collector** 소프트웨어를 설치해야 하는 위치를 이해하는 것이 중요합니다.

Data Collector(OpenStack Swift) 추가를 위한 필수 구성 요소

- 64비트 OS. 지원되는 운영 체제는 인증 구성 설명서를 참조하십시오.
- **APTARE IT Analytics** 시스템으로 벤더 하위 시스템의 데이터를 수집하는 경우 이름/값 쌍은 미국 영어여야 하며 미국 영어 로캘의 관리자가 설치를 완료해야 합니다. 서버의 언어 버전은 미국 영어가 아니어도 됩니다.
- **rpm fontconfig**가 설치되었는지 확인하십시오. **fontconfig**는 시스템 전체 글꼴 구성, 사용자 정의 및 응용 프로그램 액세스를 제공하는 라이브러리입니다. **rpm fontconfig**가

설치되지 않은 경우 설치 프로그램에서 사용자 인터페이스 모드를 로드할 수 없습니다. 이 라이브러리는 새로운 **Data Collector** 설치에 필요한 사전 요구 사항입니다.

- **Amazon Corretto 11**을 지원합니다. **Amazon Corretto**는 **OpenJDK(Open Java Development Kit)**의 다중 플랫폼 및 프로덕션용 무료 배포판입니다.
- 성능상의 이유로, **APTARE IT Analytics** 포털과 동일한 서버에 **Data Collector**를 설치하지 마십시오. 그러나 둘 모두 동일한 서버에 있어야 하는 경우 포털 및 **Data Collector** 소프트웨어가 동일한 디렉터리에 없음을 확인하십시오.
- 서버(또는 OS 인스턴스)에 **Data Collector** 하나만 설치하십시오.

설치 개요(OpenStack Swift)

다음 목록을 사용하여 표시된 순서대로 각 단계를 완료하십시오.

1. 로컬 호스트 파일을 업데이트하십시오. 이렇게 하면 포털에 액세스할 수 있습니다.
2. 포털에서 **Data Collector**를 아직 생성하지 않은 경우 지금 추가하십시오.
3. 포털에서 **OpenStack Swift Data Collector** 정책을 추가하십시오.
4. **Data Collector** 서버에서 **Data Collector** 소프트웨어를 설치하십시오.
5. **Data Collector** 설치의 유효성을 검사하십시오.

OpenStack Swift Data Collector 정책 추가

- 정책 추가 전: **Data Collector** 정책을 추가할 **Data Collector**가 포털에 있어야 합니다. 특정 벤더에 대한 특정 필수 구성 요소 및 지원되는 구성에 대해서는 인증 구성 설명서를 참조하십시오.
- 정책 추가 후: 일부 정책에서 **Collector** 관리 페이지 작업 모음의 실행 버튼을 사용하여 요청 시 수집을 실행할 수 있습니다. 실행 버튼은 정책 벤더가 지원되는 경우에만 표시됩니다.
요청 시 수집을 사용하면 수집을 실행할 프로브 및 장치를 선택할 수 있습니다. 이 작업은 예약된 실행과 동일한 데이터를 수집하면서 문제 해결을 위한 로그 정보도 수집합니다. 프로브에 대한 설명은 정책을 참조하십시오.

정책을 추가하려면 다음과 같이 하십시오.

1. **관리 > 데이터 수집 > Collector** 관리를 선택하십시오. 현재 구성된 포털 **Data Collector**가 표시됩니다.
2. 필요한 경우 **Collector**를 검색하십시오.
3. 목록에서 **Data Collector**를 선택하십시오.

- 4 정책 추가를 누른 다음 메뉴에서 벤더별 항목을 선택하십시오.

OpenStack Swift Data Collector Policy

✕

Collector Domain:

1-domain-for-pat

Policy Domain:

1-domain-for-pat

Authentication Server:*

Public Port:

5000

User ID:*

Password:*

Proxy Address:*

Proxy Path:*

/etc/swift

User ID:*

Password:*

Get Nodes

Active Probes

Schedules

☒ Swift Details

Every 8 hours, at minute 40

🕒

Node Details

Configure

Node	Collection State	Status

Notes:

OK

Cancel

Help

Privacy Policy

5 매개 변수를 입력하거나 선택하십시오. 필수 매개 변수는 별표(*)로 표시됩니다.

필드	설명
Collector 도메인	Collector 백업 정책이 추가되는 Collector의 도메인. 읽기 전용 필드입니다. 기본적으로 새 정책의 도메인은 Collector의 도메인과 동일합니다. 이 필드는 Collector를 추가할 때 설정됩니다.
정책 도메인	정책 도메인은 Data Collector에 대해 구성되는 정책의 도메인입니다. 정책 도메인은 Collector 도메인과 동일한 값으로 설정되어야 합니다. 도메인은 호스트 그룹 계층의 최상위 수준을 식별합니다. 새로 검색된 모든 호스트는 정책 도메인과 연결된 루트 호스트 그룹에 추가됩니다. 일반적으로 트러블슈팅 목록에는 정책 도메인 하나만 사용할 수 있습니다. MSP(Managed Services Provider)인 경우 각 고객에게 고유한 호스트 그룹 계층이 있는 고유한 도메인이 있습니다. 도메인 이름을 찾으려면 로그인 이름을 누르고 메뉴에서 내 프로필을 선택하십시오. 도메인 이름이 프로필 설정에 표시됩니다.
인증 서버*	인증 서버의 IP 주소와 포트 번호를 <ip address>:<port_number> 형식으로 입력하십시오. V1의 경우 기본 포트에서 실행한다면 포트 번호가 필요하지 않습니다. 그러나 기본값과 다른 포트에서 실행하는 경우 포트 번호를 지정해야 합니다. V2 인증을 사용하는 경우 이 포트 번호는 기본값이 35757인 인증 서버의 관리 포트입니다.
공용 포트	V2 인증을 위한 공용 포트입니다. 일반적으로 기본값은 5000입니다.
사용자 ID*	테넌트/프로젝트에 대한 액세스 권한이 있는 사용자 ID를 입력하십시오. 이 사용자에게 모든 프로젝트에 액세스할 수 있는 관리자 역할이 있어야 합니다. 노드 가져오기를 누르면 유효한 사용자인지 확인하기 위해 인증 정보가 확인됩니다.
암호*	사용자 ID에 연결된 암호를 입력하십시오.
프록시 IP*	OpenStack 프록시 서버에 대한 IP 주소 또는 호스트 이름을 입력하십시오. 이 주소/이름은 컨트롤러에 구성된 것과 동일할 수 있습니다.
프록시 경로*	이 경로는 OpenStack Swift 구성 파일의 위치를 식별합니다. 기본값은 /etc/swift입니다.
사용자 ID*	Swift 프록시 서버에 대한 사용자 ID를 입력하십시오. 이 사용자에게는 슈퍼 사용자 루트 권한(sudo, sesudo 및 pbrun이 지원됨)이 있어야 합니다. 노드 가져오기를 누르면 프록시 서버에 대한 SSH 연결이 설정되고 노드 IP 주소 목록이 반환됩니다.
암호*	프록시 사용자 ID와 연결된 암호를 입력하십시오.
노드 가져오기	노드 가져오기를 누르면 인증 서버 인증 정보가 확인됩니다. 다음으로, 테이블에 나열되는 노드 IP 주소 목록을 반환하기 위해 프록시 서버에 대한 SSH 연결이 설정됩니다. 이 프로세스는 완료에 최대 1분이 걸릴 수 있습니다. 이 프로세스가 완료되면 상세 내역 링크를 눌러 상태 및 노드 목록의 수집을 방해하는 인증 실패와 같은 모든 오류를 나열하십시오. 노드 가져오기를 수행하려면 에이전트 서비스가 실행 중이어야 합니다.

필드	설명
구성	구성을 누르면 Data Collector 정책이 저장되고 호스트 인벤토리 창이 표시되므로, 나열된 노드에 대해 수집을 실행하기 전에 인증 정보 관리, 경로 관리 및 액세스 제어 관리 같은 작업을 수행할 수 있습니다. 참고: 노드 목록이 식별되었더라도 호스트 인벤토리 창에서 모든 구성이 설정되고 수집이 활성화되기 전에는 노드 수집이 완료되지 않습니다. 구성이 올바르지 않은 경우 메타데이터 로그 파일에 “Could not find a host for this IP address: <ip_address>” 메시지가 나타날 수 있습니다.
활성 프로브	
예약	예약을 생성하려면 시계 아이콘을 누르십시오. 기본적으로 8시간마다 수집됩니다. 매분, 매시간, 매일, 매주 및 매월 예약을 생성할 수 있습니다. 기본 CRON 문자열의 고급 용법도 사용할 수 있습니다. CRON 식의 예: * / 30 * * * * 30분마다 한 번을 의미합니다. * / 20 9-18 * * * 오전 9시부터 오후 6시까지 20분마다 한 번을 의미합니다. * / 10 * * * 1-5 월요일부터 금요일까지 10분마다 한 번을 의미합니다. 참고: Collector 정책에 대해 설정된 명시적 예약은 Collector 서버의 시간을 기준으로 상대적입니다. 빈도가 있는 예약은 Data Collector가 재시작된 시간을 기준으로 상대적입니다.
수집 상태	저장소 노드에 대해 나열된 값은 호스트의 주 용량 프로브 상태(On, Off 또는 N/A)를 나타냅니다. 초기 노드 가져오기 작업 후에는 구성 단계를 수행해야 데이터 수집을 시도할 수 있기 때문에 이 상태는 항상 N/A입니다.
상태	저장소 노드에 대해 나열된 값은 호스트에 대한 모든 프로브의 상태(Error, Success 또는 N/A)를 나타냅니다. 초기 노드 가져오기 작업 후에는 구성 단계를 수행해야 데이터 수집을 시도할 수 있기 때문에 이 상태는 항상 N/A입니다.
참고	Data Collector 정책에 대한 메모를 입력하거나 편집하십시오. 최대 문자 수는 1024자입니다. 정책 메모는 특정 밴더에 대한 정책 정보와 함께 유지되며 Collector 관리 페이지에 열로 표시되고 검색도 가능합니다.

Microsoft Azure용 사전 설치 설정

이 장의 내용은 다음과 같습니다.

- [Microsoft Azure용 사전 설치 설정](#)
- [Microsoft Azure 데이터 수집을 위한 인증 정보 설정](#)
- [Windows 시스템에 Azure PowerShell 클라이언트 설치](#)
- [테넌트 및 구독 ID 찾기](#)
- [Data Collector에 대한 새 응용 프로그램 등록](#)
- [주체 생성 및 응용 프로그램에 역할 할당](#)
- [Data Collector\(Microsoft Azure\) 추가를 위한 필수 구성 요소](#)
- [설치 개요\(Microsoft Azure\)](#)
- [Microsoft Azure Data Collector 정책 추가](#)

Microsoft Azure용 사전 설치 설정

대부분의 경우 Data Collector의 단일 인스턴스로 원하는 수의 엔터프라이즈 개체를 지원할 수 있습니다. 그러나 각 환경에는 고유한 배포 구성 요구 사항이 있으므로, 설치해야 하는 Data Collector의 수와 배포에 가장 적합한 서버를 결정할 수 있도록 Data Collector 소프트웨어를 설치해야 하는 위치를 이해하는 것이 중요합니다.

클라우드 기반 데이터 수집의 일부로 Microsoft Azure를 APTARE IT Analytics 지원합니다. 정책은 Azure 리소스에 대한 백업, 저장소 계정, 청구 및 VM을 식별합니다. Azure로 작업하려면 하나 이상의 Azure 구독이 필요합니다. 청구, 용량 및 가상 시스템에 대해 Azure 리포트를 사용할 수 있습니다. Azure 데이터베이스 보기는 SQL 템플릿 디자이너

에서 사용자 정의 리포트를 생성하는 데 사용할 수 있습니다. Azure 엔터프라이즈 개체는 동적 템플릿 디자이너에서도 정의됩니다.

참고: Data Collector는 리소스 관리자 모델과 함께 배포된 Azure 리소스만 지원합니다.

Microsoft Azure 데이터 수집을 위한 인증 정보 설정

Azure 데이터 수집을 위한 인증 정보 설정:

1. 27페이지의 “Windows 시스템에 Azure PowerShell 클라이언트 설치” 참조
2. 27페이지의 “테넌트 및 구독 ID 찾기” 참조
3. 28페이지의 “Data Collector에 대한 새 응용 프로그램 등록” 참조
4. 28페이지의 “주체 생성 및 응용 프로그램에 역할 할당” 참조

Windows 시스템에 Azure PowerShell 클라이언트 설치

Azure에서 Windows PowerShell을 사용하여 데이터 수집에 필요한 정보에 액세스하십시오. Windows PowerShell을 관리자로 실행해야 합니다.

Azure 클라이언트에 Windows PowerShell을 설치하려면 다음과 같이 하십시오.

- 1 <http://go.microsoft.com/fwlink/p/?linkid=320376&clcid=0x409>로 이동하십시오.
- 2 설치하고 프롬프트에서 다음을 입력하여 모듈을 가져오십시오.

```
Install and at the prompt enter the following to import modules:
Install-Module PowerShellGet -Force
Install-Module -Name AzureRM -AllowClobber
Import-Module -Name AzureRM
```

테넌트 및 구독 ID 찾기

1. Azure Windows PowerShell을 관리자로 실행하십시오.
2. Azure 계정에 로그인하십시오.

```
Login-AzureRMAccount
```

3. 출력에서 테넌트 ID 및 구독 ID를 확인하십시오.

```
Get-AzureRmSubscription
```

Data Collector에 대한 새 응용 프로그램 등록

Azure와 상호 작용할 수 있으려면 먼저 Azure에 새 응용 프로그램을 등록해야 합니다.

Data Collector에 대한 새 응용 프로그램을 등록하려면 다음과 같이 하십시오.

Azure Windows PowerShell 내에서 계정에 로그인해야 합니다. 다음 단계는 Microsoft Azure PowerShell 프롬프트에서 수행합니다.

- 1 다음을 입력하여 테넌트 ID 및 구독 ID를 사용하여 컨텍스트를 설정하십시오.

```
Set-AzureRMContext -SubscriptionId <SUBSCRIPTIONID> -TenantId <TENANTID>
```

- 2 SecureString에서 암호를 설정하십시오.

```
$securePwd = ConvertTo-SecureString "<PASSWORD>" -AsPlainText -Force
```

- 3 DisplayName, Hostname 및 Azure 기본 디렉터리를 수정하십시오. 다음을 복사하여 프롬프트에 붙여 넣으십시오.

참고: Azure 기본 디렉터리는 Azure 계정의 구독 > 개요에서 찾을 수 있습니다.

```
$azureAdApplication = New-AzureRmADApplication -DisplayName  
"<DISPLAYNAME>" -HomePage "https://<HOSTNAME>.<AZURE-DEFAULT-DIRECTORY>"  
-IdentifierUri "https://<HOSTNAME>.<AZURE-DEFAULT-DIRECTORY>" -Password  
$securePwd -AvailableToOtherTenants $true
```

- 4 다음을 입력하여 응용 프로그램 매개 변수를 표시하십시오.

```
$azureAdApplication
```

- 5 선택한 구독 ID, 테넌트 ID, 응용 프로그램 ID 및 암호를 기록하십시오. 응용 프로그램 ID는 출력에 표시됩니다. Data Collector에는 이러한 네 가지 매개 변수가 필요합니다.

주체 생성 및 응용 프로그램에 역할 할당

이 단계를 통해 구독에 대한 액세스 권한을 새로 등록된 응용 프로그램에 부여할 수 있습니다.

구독에 대한 액세스 권한을 실행하려면 기여자 역할을 생성하거나 응용 프로그램에 대한 판독기 및 사용자 정의 역할의 조합을 생성할 수 있습니다. 판독기 및 사용자 정의 역할은 기여자 역할에 비해 제한된 권한을 가지고 있으므로, 기여자 역할을 통해 제공된 권한이 조직 정책을 준수하지 않는 경우 해당 권한을 응용 프로그램에 할당하도록 선택할 수 있습니다.

주체를 생성하고 기여자 역할을 할당하려면 다음과 같이 하십시오.

1. 응용 프로그램에 대한 주체 생성:

```
New-AzureRmADServicePrincipal -ApplicationId <APPLICATIONID>
```

2. 기여자 역할 생성:

```
New-AzureRmRoleAssignment -RoleDefinitionName Contributor  
-ServicePrincipalName <APPLICATIONID>
```

주체를 생성하고 판독기 및 사용자 정의 역할을 할당하려면 다음과 같이 하십시오.

1. 응용 프로그램에 대한 주체 생성:

```
New-AzureRmADServicePrincipal -ApplicationId <APPLICATIONID>
```

2. 판독기 역할 생성:

```
New-AzureRmRoleAssignment -RoleDefinitionName Reader  
-ServicePrincipalName <APPLICATIONID>
```

3. 응용 프로그램에 판독기 역할 할당:

```
New-AzureRmRoleAssignment -RoleDefinitionName Reader  
-ServicePrincipalName <APPLICATIONID>
```

4. JSON 템플릿을 사용하여 사용자 정의 역할을 생성하십시오.

예를 들어 다음을 사용하여 customrole.json 파일을 생성하십시오.

```
{ "Name": "<Role-Name>", "Id": null, "IsCustom": true,  
  "Description": "<Role Description>", "Actions":  
  [ "Microsoft.Storage/storageAccounts/listkeys/action" ],  
  "NotActions": [], "DataActions": [], "NotDataActions": [],  
  "AssignableScopes": [ "/subscriptions/<Subscription ID>" ] }
```

5. 사용자 정의 역할 생성:

```
New-AzRoleDefinition -InputFile "C:\CustomRoles\customrole.json"
```

6. 응용 프로그램에 사용자 정의 역할 할당:

```
New-AzureRmRoleAssignment -RoleDefinitionName <customRoleName>  
-ServicePrincipalName <APPLICATIONID>
```

Data Collector(Microsoft Azure) 추가를 위한 필수 구성 요소

- 64비트 OS. 지원되는 운영 체제는 **Certified Configurations Guide**(영문)를 참조하십시오.
- **APTARE IT Analytics** 시스템으로 벤더 하위 시스템의 데이터를 수집하는 경우 이름/값 쌍은 미국 영어여야 하며 미국 영어 로캘의 관리자가 설치를 완료해야 합니다. 서버의 언어 버전은 미국 영어가 아니어도 됩니다.
- **Amazon Corretto 11**을 지원합니다. **Amazon Corretto**는 **OpenJDK**(Open Java Development Kit)의 다중 플랫폼 및 프로덕션용 무료 배포판입니다.
- **rpm fontconfig**가 설치되었는지 확인하십시오. **fontconfig**는 시스템 전체 글꼴 구성, 사용자 정의 및 응용 프로그램 액세스를 제공하는 라이브러리입니다. **rpm fontconfig**가 설치되지 않은 경우 설치 프로그램에서 사용자 인터페이스 모드를 로드할 수 없습니다.
- 성능상의 이유로, **APTARE IT Analytics** 포털과 동일한 서버에 **Data Collector**를 설치하지 마십시오. 그러나 둘 모두 동일한 서버에 있어야 하는 경우 포털 및 **Data Collector** 소프트웨어가 동일한 디렉터리에 없음을 확인하십시오.
- 서버(또는 OS 인스턴스)에 **Data Collector** 하나만 설치하십시오.
- 포트 443이 필요합니다.

설치 개요(Microsoft Azure)

다음 목록을 사용하여 표시된 순서대로 각 단계를 완료하십시오.

1. 로컬 호스트 파일을 업데이트하십시오. 이렇게 하면 포털에 액세스할 수 있습니다.
2. 포털에서 **Data Collector**를 아직 생성하지 않은 경우 지금 추가하십시오.
3. 포털에서 **Microsoft Azure Data Collector** 정책을 추가하십시오.
4. **Data Collector** 서버에서 **Data Collector** 소프트웨어를 설치하십시오.
5. **Data Collector** 설치의 유효성을 검사하십시오.

Microsoft Azure Data Collector 정책 추가

- 정책 추가 전: **Data Collector** 정책을 추가할 **Data Collector**가 포털에 있어야 합니다. 특정 벤더에 대한 특정 필수 구성 요소 및 지원되는 구성에 대해서는 인증 구성 설명서를 참조하십시오.

- 정책 추가 후: 일부 정책에서 **Collector** 관리 페이지 작업 모음의 **실행** 버튼을 사용하여 요청 시 수집을 실행할 수 있습니다. **실행** 버튼은 정책 벤더가 지원되는 경우에만 표시됩니다.

요청 시 수집을 사용하면 수집을 실행할 프로브 및 장치를 선택할 수 있습니다. 이 작업은 예약된 실행과 동일한 데이터를 수집하면서 문제 해결을 위한 로그 정보도 수집합니다. 프로브에 대한 설명은 정책을 참조하십시오.

정책을 추가하려면 다음과 같이 하십시오.

- 1 **관리 > 데이터 수집 > Collector** 관리를 선택하십시오. 현재 구성된 포털 **Data Collector**가 표시됩니다.
- 2 필요한 경우 **Collector**를 검색하십시오.
- 3 목록에서 **Data Collector**를 선택하십시오.
- 4 **정책 추가**를 누른 다음 메뉴에서 벤더별 항목을 선택하십시오.

5 매개 변수를 입력하거나 선택하십시오. 필수 매개 변수는 별표(*)로 표시됩니다.

필드	설명
Collector 도메인	Collector 백업 정책이 추가되는 Collector의 도메인. 읽기 전용 필드입니다. 기본적으로 새 정책의 도메인은 Collector의 도메인과 동일합니다. 이 필드는 Collector를 추가할 때 설정됩니다.
정책 도메인	정책 도메인은 Data Collector에 대해 구성되는 정책의 도메인입니다. 정책 도메인은 Collector 도메인과 동일한 값으로 설정되어야 합니다. 도메인은 호스트 그룹 계층의 최상위 수준을 식별합니다. 새로 검색된 모든 호스트는 정책 도메인과 연결된 루트 호스트 그룹에 추가됩니다. 일반적으로 드롭다운 목록에는 정책 도메인 하나만 사용할 수 있습니다. MSP(Managed Services Provider)인 경우 각 고객에게 고유한 호스트 그룹 계층이 있는 고유한 도메인이 있습니다. 도메인 이름을 찾으려면 로그인 이름을 누르고 메뉴에서 내 프로필을 선택하십시오. 도메인 이름이 프로필 설정에 표시됩니다.
구독 ID*	Microsoft Azure Cloud 계정의 구독 ID입니다.
제공 ID*	Microsoft Azure Cloud 구독의 제공 ID입니다. 제안 ID를 찾으려면 Azure 포털에 로그인하고 제공 ID가 구독 서비스 아래 매개 변수로 나열됩니다.
테넌트 ID*	Microsoft Azure Cloud 계정의 테넌트 ID입니다. GUID라고도 합니다.
응용 프로그램 ID*	등록된 Microsoft Azure 응용 프로그램과 연결된 응용 프로그램 ID입니다. Azure를 사용하려면 Data Collector가 상호 작용할 수 있는 응용 프로그램이 필요합니다. 참고: 28페이지의 "Data Collector에 대한 새 응용 프로그램을 등록하려면 다음과 같이 하십시오." 참조
암호*	응용 프로그램 ID(등록된 Microsoft Azure 응용 프로그램)와 연결된 암호입니다.
가상 시스템	Azure 가상 시스템의 수집 예약을 설정하려면 선택하십시오.
저장소 계정	Azure Storage 계정의 수집 예약을 설정하려면 선택하십시오.
청구	Azure 청구의 수집 예약을 설정하려면 선택하십시오.
Azure 백업	Azure 백업의 수집 예약을 설정하려면 선택하십시오.
참고	Data Collector 정책에 대한 메모를 입력하거나 편집하십시오. 최대 문자 수는 1024자입니다. 정책 메모는 특정 벤더에 대한 정책 정보와 함께 유지되며 Collector 관리 페이지에 열로 표시되고 검색도 가능합니다.

필드

연결 테스트

설명

연결 테스트에서는 정책에 제공된 IP 주소 및 인증 정보를 사용하여 하위 시스템에 연결하는 Data Collector 프로세스가 시작됩니다. 이 유효성 검사 프로세스에서는 성공 메시지 또는 특정 연결 오류 목록이 반환됩니다. 연결 테스트를 수행하려면 에이전트 서비스가 실행 중이어야 합니다.

유효성 검사 요청의 응답 시간에는 여러 요인이 영향을 미치므로 일부 요청은 다른 요청보다 시간이 오래 걸립니다. 예를 들어 하위 시스템에 연결할 때 지연이 발생할 수 있습니다. 마찬가지로, Data Collector에서 실행 중인 다른 처리 스레드로 인해 응답 수신에 지연될 수 있습니다.

또한 **관리 > 데이터 수집 > Collector** 관리에서 사용할 수 있는 **실행** 기능을 사용하여 데이터 수집을 테스트할 수 있습니다. 이 요청 시 데이터 수집 실행은 도메인, 호스트 그룹, URL, Data Collector 정책 및 데이터베이스 연결에 대한 확인을 포함하여 개별 정책 수준에서 설치의 개략적 확인을 시작합니다. 수집 실행을 테스트하기 위해 개별 프로브 및 서버를 선택할 수도 있습니다.

Data Collector 소프트웨어 설치

이 장의 내용은 다음과 같습니다.

- 소개
- WMI 프록시 서비스 설치(Windows Host Resources만 해당)
- WMI 연결 테스트

소개

APTARE IT Analytics 시스템으로 벤더 하위 시스템의 데이터를 수집하는 경우 이름/값 쌍은 미국 영어여야 하며 미국 영어 로캘의 관리자가 설치를 완료해야 합니다. 서버의 언어 버전은 미국 영어가 아니어도 됩니다.

참고: 이 설치에 필요한 권한을 부여하려면 로컬 관리자로 로그인하십시오.

WMI 프록시 서비스 설치(Windows Host Resources만 해당)

Windows 호스트에서 데이터를 수집하려면 WMI 프록시를 설치할 Windows 호스트를 선택하십시오.

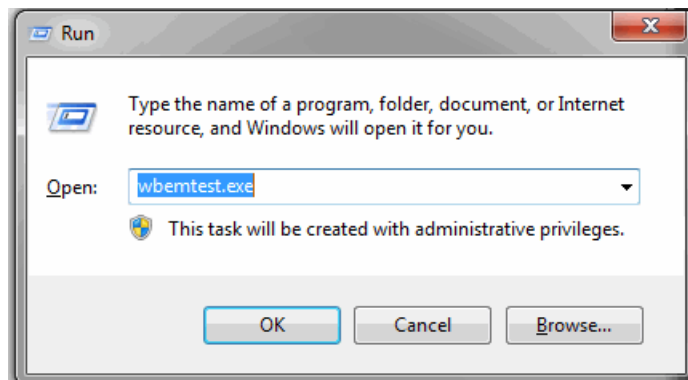
- 이는 Windows Host Resources에서 데이터를 수집하는 경우에만 필요합니다.
- WMI 프록시는 하나의 Windows 호스트에만 설치되어야 합니다.
- Data Collector가 Linux 서버에 있는 경우 WMI 프록시 서비스를 설치할 Windows 서버를 식별해야 합니다.

WMI 연결 테스트

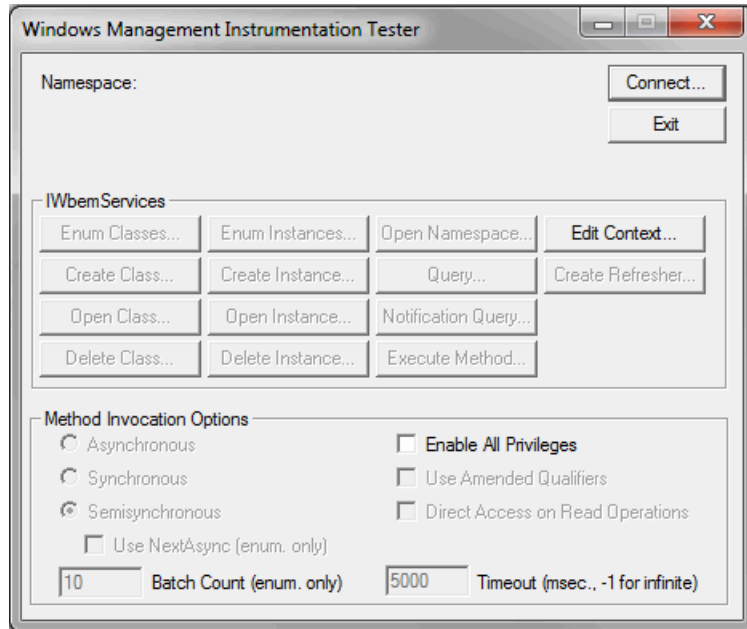
WMI(Windows Management Instrumentation) 프로록시는 APTARE IT Analytics에서 Windows 호스트의 데이터를 수집하는 데 사용됩니다. 연결 문제가 있는 경우 다음 단계를 수행하여 연결을 테스트하고 문제를 해결할 수 있습니다.

WMI가 올바르게 작동하는지 확인하려면 다음 단계를 수행하십시오.

1. Data Collector 서버에 관리자로 로그인하십시오.
2. Windows 시작 메뉴에서 검색 상자에 실행을 입력하여 다음 창을 시작하고 **wbemtest.exe**를 입력한 다음 **확인**을 누르십시오.



3. Windows Management Instrumentation 테스터 창에서 **연결**을 누르십시오.



4. 연결 창에서 다음 형식으로 대상 원격 서버의 IP 주소 또는 호스트 이름을 네임스페이스 항목 앞에 입력하십시오.

\\<IP Address>\root\cimv2

The image shows a 'Connect' dialog box with the following sections:

- Namespace:** A text box containing 'root\cimv2'. To its right are 'Connect' and 'Cancel' buttons.
- Connection:** A section containing:
 - 'Using:' dropdown menu with 'IWbemLocator (Namespaces)' selected.
 - 'Returning:' dropdown menu with 'IWbemServices' selected.
 - 'Completion:' dropdown menu with 'Synchronous' selected.
- Credentials:** A section containing three text boxes labeled 'User:', 'Password:', and 'Authority:'.
- Locale:** A text box.
- How to interpret empty password:** Two radio buttons: 'NULL' (selected) and 'Blank'.
- Impersonation level:** Three radio buttons: 'Identify', 'Impersonate' (selected), and 'Delegate'.
- Authentication level:** Six radio buttons: 'None', 'Packet' (selected), 'Connection', 'Packet integrity', 'Call', and 'Packet privacy'.

5. 연결 창에서 다음 필드를 입력한 다음 **연결**을 누르십시오.
 - 사용자 - 원격 시스템 액세스를 위한 인증 정보를 입력하십시오. 원격 시스템에서 **RPC**(원격 프로시저 호출 프로토콜)를 실행해야 할 수 있습니다.
 - 암호
 - 권한: **NTLMDOMAIN:<NameOfDomain>** 입력
여기서 **NameOfDomain**은 사용자 필드에 지정된 사용자 계정의 도메인입니다.
6. **클래스 열거**를 누르십시오.
7. 슈퍼클래스 정보 창에서 **모든 클래스** 라디오 버튼을 선택하고 슈퍼클래스 이름은 입력하지 마십시오. 그런 다음 **확인**을 누르십시오.
8. WMI 테스터가 클래스 목록을 생성합니다. 이 목록이 표시되지 않으면 **Microsoft Developer Network** 웹 사이트로 이동하여 문제 해결 도움말을 참조하십시오.

<http://msdn.microsoft.com/en-us/library/ms735120.aspx>

데이터 수집 유효성 검사

이 장의 내용은 다음과 같습니다.

- 유효성 검사 방법
- **Data Collector**: 벤더별 유효성 검사 방법
- 요청 시 데이터 수집 작업
- **CLI check install** 유틸리티 사용
- **Data Collector** 구성 나열

유효성 검사 방법

유효성 검사 방법은 **Data Collector** 정책과 연결된 하위 시스템 벤더에 따라 다르게 시작되지만 본질적으로 동일한 기능을 수행합니다. 벤더별 유효성 검사 방법에 대해서는 다음 표를 참조하십시오.

- 연결 테스트 - 정책에 제공된 IP 주소 및 인증 정보를 사용하여 하위 시스템에 연결을 시도하는 **Data Collector** 정책 화면에서 직접 연결 시도를 시작합니다. 이 유효성 검사 프로세스에서는 성공 메시지 또는 특정 연결 오류 목록이 반환됩니다.
- 요청 시 데이터 수집 실행 - 예약된 시작을 기다리지 않고 포털에서 수집 프로세스의 즉각적인 중단간 실행을 시작합니다. 또한 이 요청 시 실행은 연결 테스트와 동일하게 정책 및 해당 값의 유효성을 검사하는 역할을 하며 도메인, 호스트 그룹, URL, **Data Collector** 정책 및 데이터베이스 연결에 대한 확인을 포함하여 개별 정책 수준에서 설치에 대한 개략적 확인을 수행합니다. 실행은 **관리 > 데이터 수집 > Collector** 관리의 정책 수준에서 시작됩니다.

41페이지의 “**요청 시 데이터 수집 작업**” 참조

- **CLI Checkinstall** 유틸리티 - 이 레거시 명령줄 유틸리티는 **Data Collector** 서버에서 연결 테스트 기능 및 요청 시 데이터 수집 실행을 모두 수행합니다.

42페이지의 “**CLI check install 유틸리티 사용**” 참조

참고: APTARE IT Analytics에서는 요청 시 실행을 지원하는 Data Collector 하위 시스템 벤더에 대해 CLI Checkinstall 유틸리티를 사용하는 것을 권장하지 않습니다.

Data Collector: 벤더별 유효성 검사 방법

표 6-1 벤더별 유효성 검사 요구 사항.

벤더 이름	연결 테스트	요청 시	CLI Checkinstall 유틸리티
Amazon Web Services(AWS)	x	x	
Brocade 스위치		x	
Brocade 영역 별칭	x	x	
Cisco 스위치		x	
Cisco 영역 별칭	x	x	
Cohesity DataProtect	x	x	
Commvault Simpana			x
Dell Compellent			x
Dell EMC Elastic Cloud Storage(ECS)	x	x	
Dell EMC NetWorker Backup & Recovery	x		
Dell EMC Unity	x	x	
EMC Avamar		x	
EMC Data Domain Backup	x	x	
EMC Data Domain Storage	x	x	
EMC Isilon		x	
EMC NetWorker			x
EMC Symmetrix	x	x	
EMC VNX CLARiON	x	x	
EMC VNX Celerra			x
EMC VPLEX			x

표 6-1 벤더별 유효성 검사 요구 사항. (계속)

벤더 이름	연결 테스트	요청 시	CLI Checkinstall 유틸리티
EMC XtremIO	x	x	
HDS HCP	x	x	
HDS HNAS		x	
HP 3PAR			x
HP Data Protector			x
HP EVA			x
HPE Nimble Storage	x	x	
Hitachi Block			x
Hitachi Content Platform(HCP)	x	x	
Hitachi NAS	x	x	
Huawei OceanStor	x	x	
IBM Enterprise			x
IBM SVC			x
IBM Spectrum Protect(TSM)		x	
IBM VIO	x	x	
IBM XIV			x
INFINIDAT Infinibox	x	x	
Microsoft Azure	x	x	
Microsoft Hyper-V	x	x	
Microsoft Windows Server	x	x	
NAKIVO Backup & Replication	x	x	
NetApp E Series			x
Netapp		x	
Netapp Cluster Mode		x	

표 6-1 벤더별 유효성 검사 요구 사항. (계속)

벤더 이름	연결 테스트	요청 시	CLI Checkinstall 유틸리티
OpenStack Ceilometer	x	x	
OpenStack Swift	x 연결 테스트는 노드 가져오기 기능에 포함되어 있습니다.	x	
Oracle Recovery Manager(RMAN)	x	x	
Pure FlashArray	x	x	
Rubrik Cloud Data Management	x	x	
VMWare			x
Veeam Backup & Replication	x	x	
Veritas Backup Exec			x
Veritas NetBackup	x	x	
Veritas NetBackup Appliance	X	x	

요청 시 데이터 수집 작업

수집은 작업 모음의 **실행** 버튼을 사용하여 예약 또는 요청 시 실행할 수 있습니다. 요청 시 수집을 사용하면 실행할 프로브 및 장치를 선택할 수 있습니다. 요청 시 실행은 예약된 실행과 같은 데이터를 수집하지만 문제 해결을 위해 추가로 로깅 정보를 수집합니다. 정책이 지정된 벤더 중 하나에 할당되었고 **Collector**가 온라인인 경우 중지된 정책은 여전히 요청 시 수집 실행을 허용합니다.

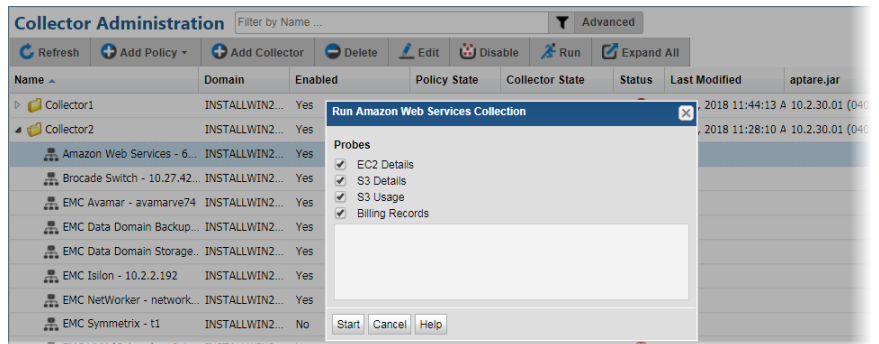
참고: 요청 시 데이터 수집은 일부 정책에 사용할 수 없습니다.

요청 시 데이터 수집은 여러 용도로 사용됩니다. 이를 사용하여 다음을 수행할 수 있습니다.

- **Data Collector** 정책을 생성할 때 수집 프로세스가 중단간 작업인지 유효성 검사
- 예약된 실행을 기다리지 않고 수집 프로세스 즉시 실행 시작
- 새 데이터로 데이터베이스 채우기

요청 시 데이터 수집을 시작하려면 다음과 같이 하십시오.

- 1 관리 > 데이터 수집 > **Collector** 관리를 선택하십시오. 모든 **Data Collector**가 표시됩니다.
- 2 모두 **확장**을 눌러 정책을 찾아보거나 **검색**을 사용하십시오.
- 3 목록에서 **Data Collector** 정책을 선택하십시오. 벤더가 지원되는 경우 작업 모음에 **실행** 버튼이 표시됩니다.
- 4 **실행**을 누르십시오. 수집 실행을 테스트하기 위해 서버 및 개별 프로브를 선택할 수 있는 대화 상자가 표시됩니다. 다음 예에서는 **Amazon Web Services** 대화 상자를 보여 줍니다. 프로브 및 서버에 대한 자세한 내용은 벤더별 콘텐츠를 참조하십시오.



- 5 **시작**을 누르십시오. 예약된 실행과 같은 데이터를 수집하지만 문제 해결을 위해 추가로 로깅 정보를 수집합니다. 일단 시작되면 완료될 때까지 실행 상태를 모니터링할 수 있습니다.

참고: 시작을 누를 때 현재 진행 중인 다른 데이터 수집 실행이 있는 경우 요청 시 실행은 진행 중인 실행이 완료될 때까지 시작을 대기합니다.

CLI check install 유틸리티 사용

이 레거시 유틸리티는 **Data Collector** 서버에서 시작되는 명령줄 인터페이스에서 연결 테스트 기능 및 요청 시 데이터 수집 실행을 모두 수행합니다.

참고: APTARE IT Analytics에서는 요청 시 실행을 지원하는 **Data Collector** 하위 시스템 벤더에 대해 CLI Checkinstall 유틸리티를 사용하는 것을 권장하지 않습니다.

다음 지침에서는 **Data Collector** 파일이 기본 위치에 설치되어 있다고 가정합니다.

Windows의 경우 C:\Program Files\Aptare이고, Linux의 경우 /opt/aptare입니다.

다른 디렉터리에 파일을 설치한 경우 다음 지침에 따라 필요한 경로를 변환하십시오.

참고: 다음 명령 중 일부는 엔터프라이즈의 규모에 따라 최대 몇 시간이 걸릴 수 있습니다.

Checkinstall을 실행하려면 다음과 같이 하십시오.

- 1 Data Collector 서버에서 세션을 여십시오.

Windows: 명령 프롬프트 창을 여십시오.

Linux: **Data Collector** 서버에 루트로 로그인한 텔넷 세션을 여십시오.

- 2 유효성 검사 스크립트를 실행할 디렉터리로 변경하십시오.

Windows: 명령 프롬프트에서 다음을 입력하십시오.

```
cd C:\Program Files\Aptare\mbs\bin <enter>
```

Linux: 텔넷 세션에서 다음을 입력하십시오.

```
cd /opt/aptare/mbs/bin <enter>
```

- 3 유효성 검사 스크립트를 실행하십시오.

Windows: 명령 프롬프트에서 다음을 입력하십시오. `checkinstall.bat <enter>`

Linux: 텔넷 세션에서 다음을 입력하십시오. `./checkinstall.sh <enter>`

checkinstall 유틸리티는 도메인, 호스트 그룹 및 URL, Data Collector 정책 및 데이터베이스 연결에 대한 확인을 포함하여 설치의 개략적 확인을 수행합니다. 포털에 Data Collector 정책이 구성되어 있지 않으면 이 유틸리티가 실패합니다. 구성 요소 확인, 특히 Host Resources에 대한 확인의 경우 **hostresourcedetail.sh|bat** 유틸리티를 실행하십시오.

Checkinstall에는 하나 이상의 특정 장치에 대해 프로브를 실행하는 옵션이 포함되어 있습니다. 일부 Data Collector에서는 장치를 개별적으로 선택할 수 없습니다. 일반적으로 이러한 Collector는 단일 텍스트 상자에 여러 서버 주소 또는 주소 범위를 입력할 수 있습니다. 이러한 Collector에는 Cisco Switch, EMC CLARiON, EMC Data Domain, EMC VNX 어레이, HP 3PAR, IBM 미드레인지 어레이, IBM XIV 어레이 및 VMWare가 포함됩니다. 관리 서버에 연결된 모든 장치를 검색하는 Data Collector도 장치를 개별적으로 선택할 수 없습니다. 여기에는 EMC Symmetric, File Analytics, Hitachi 어레이 및 IBM VIO가 포함됩니다.

- 4 이전 단계의 출력에 **FAILED** 단어가 포함된 경우 지원 부서에 문의하고 다음 파일을 검토할 수 있도록 준비하십시오. `/opt/aptare/mbs/logs/validation/`

```
C:\Program Files\Aptare\mbs\logs\validation\
```

Data Collector 구성 나열

Data Collector 구성 내에 캡슐화된 다양한 하위 스크립트 및 해당 구성을 나열하려면 이 유틸리티를 사용하십시오. 이 유틸리티는 **checkinstall.[sh|bat]** 같은 다른 스크립트와 함께 사용할 수 있습니다.

Linux의 경우: **./listcollectors.sh**

Windows의 경우: **listcollectors.bat**

Data Collector 제거

이 장의 내용은 다음과 같습니다.

- [Linux에서 Data Collector 제거](#)
- [Windows에서 Data Collector 제거](#)

Linux에서 Data Collector 제거

이 제거 프로세스에서는 표준 설치 프로세스를 사용하여 **Data Collector**를 설치했다고 가정합니다.

Windows에서 Data Collector 제거

이 제거 프로세스에서는 표준 설치 프로세스를 사용하여 **Data Collector**를 설치했다고 가정합니다.

참고: 제거 관리자가 전체 **Data Collector** 디렉터리 구조를 삭제하지 않을 수도 있습니다. 설치 후 생성된 새 파일과 해당 상위 디렉터리가 제거되지 않는 경우도 있습니다. 제거 관리자가 완료된 후 루트 설치 폴더(기본적으로 C:\Program Files\Aptare) 및 해당 하위 폴더를 수동으로 제거해야 할 수도 있습니다.

Data Collector 수동 시작

이 장의 내용은 다음과 같습니다.

- 소개

소개

설치 관리자는 **Data Collector**를 자동으로 시작되도록 구성하지만 설치를 완료한 후 먼저 사용자가 설치 유효성을 검사해야 하기 때문에 실제로 **Data Collector**가 시작되지 않습니다.

Data Collector 서비스를 수동으로 시작하려면 관련 운영 체제에 대한 다음과 같은 단계를 수행하십시오.

Windows의 경우

설치 관리자가 **Data Collector** 프로세스를 서비스로 구성합니다.

Data Collector 상태를 보려면 다음과 같이 하십시오.

1. 시작 > 설정 > 제어판을 누르십시오.
2. 관리 도구를 누르십시오.
3. 서비스를 누르십시오. Microsoft 서비스 대화 상자가 표시됩니다. **APTARE 에이전트**에 대한 항목이 포함되어 있어야 합니다. 이 서비스가 실행되고 있지 않은 경우 지금 시작하십시오.

Linux의 경우

설치 관리자가 벤더 운영 체제에 따라 적절한 디렉터리에 **Data Collector** "시작" 및 "중지" 스크립트를 자동으로 복사합니다.

Data Collector를 시작하려면 다음 명령을 사용하십시오.

```
etc/init.d/aptare_agent start
```

방화벽 구성: 기본 포트

이 부록의 내용은 다음과 같습니다.

- 방화벽 구성: 기본 포트

방화벽 구성: 기본 포트

다음 표에서는 포트 서버, **Data Collector** 서버 및 모든 포함된 타사 소프트웨어 제품에서 표준 "기본 제공" 설치의 일부로 사용하는 표준 포트에 대해 설명합니다.

표 A-1 구성 요소: 기본 포트

구성 요소	기본 포트
Apache 웹 서버	http 80 https 443
Linux 호스트	SSH 22, 텔넷 23
관리되는 응용 프로그램	Oracle ASM 1521 MS Exchange 389 MS SQL 1433 File Analytics CIFS 137, 139
Oracle Oracle TNS 수신기 포트	1521
Tomcat - 데이터 리시버 Tomcat의 데이터 리시버 인스턴스용 Apache 커넥터 포트 및 종료 포트	8011, 8017

표 A-1 구성 요소: 기본 포트 (계속)

구성 요소	기본 포트
Tomcat - 포털 Tomcat의 포털 인스턴스용 Apache 커넥터 포트 및 종료 포트	8009, 8015
Windows 호스트	TCP/IP 1248 WMI 135 DCOM TCP/UDP > 1023 SMB TCP 445

표 A-2 데이터 보호: 기본 포트

데이터 보호 벤더	기본 포트 및 참고
Cohesity DataProtect	REST API - 포트 80 또는 443
Commvault Simpana	1433, 135(건너편 파일) 445(TCP를 통한 CIFS) DCOM >1023
Dell EMC NetWorker Backup & Recovery	Dell EMC NetWorker REST API 연결에 사용되는 포트. 기본값: 9090.
EMC Avamar	5555 SSH 22
EMC Data Domain Backup	SSH 22
EMC NetWorker	■ NSRADMIN TCP 7937-7940 ■ WMI 프로시 포트 범위 ■ SSH 22(Linux)
HP Data Protector	5555 WMI 포트 SSH 22(Linux)
IBM Spectrum Protect(TSM)	1500
NAKIVO Backup & Replication	Director Web UI 포트(기본값: 4443)
Oracle Recovery Manager(RMAN)	1521
Rubrik Cloud Data Management	REST API 443
Veeam Backup & Replication	9392
Veritas Backup Exec	1433

표 A-2 데이터 보호: 기본 포트 (계속)

데이터 보호 벤더	기본 포트 및 참고
Veritas NetBackup	1556, 13724 WMI 포트 SSH 22(Linux)

표 A-3 네트워크 및 패브릭: 기본 포트

네트워크 및 패브릭 벤더	기본 포트 및 참고
Brocade 스위치	SMI-S 5988/5989
Cisco 스위치	SMI-S 5988/5989

표 A-4 가상화 벤더: 기본 포트

가상화 벤더	기본 포트 및 참고
IBM VIO	SSH 22, 텔넷 23
Microsoft Hyper-V	WMI 135 DCOM TCP/UDP > 1023
VMware ESX 또는 ESXi, vCenter, vSphere	vSphere VI SDK https TCP 443

표 A-5 복제 벤더: 기본 포트

복제 벤더	기본 포트 및 참고
NetApp ONTAP 7-Mode	ONTAP API 80/443

표 A-6 클라우드 벤더: 기본 포트

클라우드 벤더	기본 포트 및 참고
Amazon Web Services	https 443
Microsoft Azure	https 443
OpenStack Cellometer	8774, 8777 Keystone Admin 3537 Keystone Public 5000
OpenStack Swift	Keystone Admin 35357 Keystone Public 5000 SSH 22