데이터 분류 배포

NetApp Data Classification

NetApp
February 11, 2026

목차

데이터 분류 배포

어떤 NetApp Data Classification 배포를 사용해야 합니까?

NetApp Data Classification 다양한 방법으로 배포할 수 있습니다. 어떤 방법이 귀하의 필요에 맞는지 알아보세요.

데이터 분류는 다음과 같은 방법으로 배포될 수 있습니다.

- "콘솔을 사용하여 클라우드에 배포" . 콘솔은 콘솔 에이전트와 동일한 클라우드 공급자 네트워크에 데이터 분류 인스턴스를 배포합니다.
- "인터넷 접속이 가능한 Linux 호스트에 설치" . 인터넷 접속이 가능한 네트워크의 Linux 호스트나 클라우드의 Linux 호스트에 데이터 분류를 설치합니다. 온프레미스 ONTAP 시스템을 온프레미스에 있는 데이터 분류 인스턴스를 사용하여 스캔하려는 경우 이러한 유형의 설치가 좋은 옵션일 수 있지만, 이는 필수 사항은 아닙니다.
- "인터넷 접속이 불가능한 온프레미스 사이트의 Linux 호스트에 설치"_비공개 모드_라고도 합니다. 설치 스크립트를 사용하는 이 유형의 설치는 콘솔 SaaS 계층에 연결할 수 없습니다.

> BlueXP 개인 모드(레거시 BlueXP 인터페이스)는 일반적으로 인터넷 연결이 없고 AWS Secret Cloud, AWS Top Secret Cloud, Azure IL6를 포함하는 보안 클라우드 지역이 있는 온프레미스 환경에서 사용됩니다. NetApp 기존 BlueXP 인터페이스를 통해 이러한 환경을 계속 지원합니다. 레거시 BlueXP 인터페이스의 개인 모드 설명서는 다음을 참조하세요."BlueXP 개인 모드에 대한 PDF 문서" .

인터넷 접속이 가능한 Linux 호스트에 설치하는 경우와 인터넷 접속이 불가능한 Linux 호스트에 온프레미스로 설치하는 경우 모두 설치 스크립트를 사용합니다. 스크립트는 시스템과 환경이 전제 조건을 충족하는지 확인하는 것으로 시작합니다. 필수 구성 요소가 충족되면 설치가 시작됩니다. 데이터 분류 설치를 실행하지 않고도 전제 조건을 독립적으로 확인하려면 전제 조건만 테스트하는 별도의 소프트웨어 패키지를 다운로드할 수 있습니다.

"Linux 호스트가 데이터 분류를 설치할 준비가 되었는지 확인하세요." .

NetApp Console 사용하여 클라우드에 NetApp Data Classification 배포합니다.

NetApp Console 사용하여 클라우드에 NetApp Data Classification 배포할 수 있습니다. 콘솔은 콘솔 에이전트와 동일한 클라우드 공급자 네트워크에 데이터 분류 인스턴스를 배포합니다.

또한 다음을 수행할 수도 있습니다."인터넷 접속이 가능한 Linux 호스트에 데이터 분류 설치" . 온프레미스 ONTAP 시스템을 온프레미스에 있는 데이터 분류 인스턴스를 사용하여 스캔하려는 경우 이러한 유형의 설치가 좋은 옵션일 수 있지만, 이는 필수 사항은 아닙니다. 어떤 설치 방법을 선택하든 소프트웨어의 기능은 정확히 동일합니다.

빠른 시작

다음 단계에 따라 빠르게 시작하거나, 나머지 섹션으로 스크롤하여 자세한 내용을 확인하세요.

1 콘솔 에이전트 만들기

아직 콘솔 에이전트가 없으면 하나 만드세요. 보다"AWS에서 콘솔 에이전트 만들기" ,"Azure에서 콘솔 에이전트 만들기" , 또는"GCP에서 콘솔 에이전트 만들기" .

당신도 할 수 있습니다"온프레미스에 콘솔 에이전트 설치" 네트워크의 Linux 호스트나 클라우드의 Linux 호스트에서.

2 필수 조건

사용 환경이 필수 요구 사항을 충족하는지 확인하십시오. 여기에는 인스턴스의 아웃바운드 인터넷 액세스, Console 에이전트와 Data Classification 간의 포트 443을 통한 연결 등이 포함됩니다. 전체 목록을 확인하세요.

3 데이터 분류 배포

설치 마법사를 실행하여 클라우드에 데이터 분류 인스턴스를 배포합니다.

콘솔 에이전트 만들기

아직 콘솔 에이전트가 없다면 클라우드 공급자에서 콘솔 에이전트를 만드세요. 보다 "AWS에서 콘솔 에이전트 만들기" 또는 "Azure에서 콘솔 에이전트 만들기" , 또는 "GCP에서 콘솔 에이전트 만들기" . 대부분의 경우 데이터 분류를 활성화하기 전에 콘솔 에이전트를 설정했을 가능성이 높습니다. "콘솔 기능에는 콘솔 에이전트가 필요합니다." 하지만 지금 당장 설정해야 하는 경우도 있습니다.

특정 클라우드 공급자에 배포된 콘솔 에이전트를 사용해야 하는 몇 가지 시나리오가 있습니다.

- AWS의 Cloud Volumes ONTAP 또는 Amazon FSx for ONTAP 버킷에서 데이터를 스캔할 때 AWS의 콘솔 에이전트를 사용합니다.
- Azure의 Cloud Volumes ONTAP 또는 Azure NetApp Files 에서 데이터를 스캔할 때 Azure의 콘솔 에이전트를 사용합니다.
  - Azure NetApp Files 의 경우, 스캔하려는 볼륨과 동일한 지역에 배포해야 합니다.
- GCP에서 Cloud Volumes ONTAP 의 데이터를 스캔할 때 GCP의 콘솔 에이전트를 사용합니다.

이러한 클라우드 콘솔 에이전트를 사용하면 온프레미스 ONTAP 시스템, NetApp 파일 공유 및 데이터베이스를 검사할 수 있습니다.

또한 다음을 수행할 수도 있습니다. "온프레미스에 콘솔 에이전트 설치" 네트워크나 클라우드 내의 Linux 호스트에서. 온프레미스에 데이터 분류를 설치하려는 일부 사용자는 온프레미스에 콘솔 에이전트를 설치하기로 선택할 수도 있습니다.

사용해야 하는 상황이 있을 수 있습니다. "여러 콘솔 에이전트" .

데이터 분류는 스캔할 수 있는 데이터 양에 제한을 두지 않습니다. 각 콘솔 에이전트는 500TiB의 데이터를 스캔하고 표시하는 것을 지원합니다. 500TiB 이상의 데이터를 스캔하려면"다른 콘솔 에이전트를 설치하세요" 그 다음에"다른 데이터 분류 인스턴스 배포" . + 콘솔 UI는 단일 커넥터의 데이터를 표시합니다. 여러 콘솔 에이전트의 데이터를 보는 방법에 대한 팁은 다음을 참조하세요."여러 콘솔 에이전트와 함께 작업" .

정부 지역 지원

콘솔 에이전트가 정부 지역(AWS GovCloud, Azure Gov 또는 Azure DoD)에 배포된 경우 데이터 분류가 지원됩니다. 이런 방식으로 배포할 경우 데이터 분류에는 다음과 같은 제한이 있습니다.

"정부 지역에 콘솔 에이전트를 배포하는 방법에 대해 알아보세요.".

필수 조건

클라우드에 데이터 분류를 배포하기 전에 지원되는 구성이 있는지 확인하려면 다음 필수 구성 요소를 검토하세요. 클라우드에 데이터 분류를 배포하면 콘솔 에이전트와 동일한 서브넷에 위치하게 됩니다.

데이터 분류에서 아웃바운드 인터넷 액세스 활성화

데이터 분류에는 아웃바운드 인터넷 액세스가 필요합니다. 가상 또는 물리적 네트워크에서 인터넷 접속을 위해 프록시 서버를 사용하는 경우, 데이터 분류 인스턴스에 다음 엔드포인트에 연결할 수 있는 아웃바운드 인터넷 접속 권한이 있는지 확인하세요. 프록시는 투명하지 않아야 합니다. 투명 프록시는 현재 지원되지 않습니다.

AWS, Azure 또는 GCP에서 데이터 분류를 배포하는지에 따라 아래 해당 표를 검토하세요.

AWS에 필요한 엔드포인트

엔드포인트	목적
\ https://api.console.netapp.com	NetApp 계정을 포함하는 콘솔 서비스와의 통신입니다.
\ https://netapp-cloud-account.auth0.com \ https://auth0.com	중앙화된 사용자 인증을 위해 콘솔 웹사이트와 통신합니다.
\ https://cloud-compliance-support-netapp.s3.us-west-2.amazonaws.com \ https://hub.docker.com \ https://auth.docker.io \ https://registry-1.docker.io \ https://index.docker.io/ \ https://dseasb33srnrn.cloudfront.net/ \ https://production.cloudflare.docker.com/	소프트웨어 이미지, 매니페스트, 템플릿에 대한 액세스를 제공합니다.
\ https://kinesis.us-east-1.amazonaws.com	NetApp 감사 기록에서 데이터를 스트리밍할 수 있도록 합니다.
\ https://cognito-idp.us-east-1.amazonaws.com \ https://cognito-identity.us-east-1.amazonaws.com \ https://user-feedback-store-prod.s3.us-west-2.amazonaws.com \ https://customer-data-production.s3.us-west-2.amazonaws.com	데이터 분류를 통해 매니페스트와 템플릿에 액세스하고 다운로드하며, 로그와 메트릭을 전송할 수 있습니다.

Azure에 필요한 엔드포인트

엔드포인트	목적
\ https://api.console.netapp.com	NetApp 계정을 포함하는 콘솔 서비스와의 통신입니다.
\ https://netapp-cloud-account.auth0.com \ https://auth0.com	중앙화된 사용자 인증을 위해 콘솔 웹사이트와 통신합니다.
\ https://support.compliance.api.console.netapp.com/ \ https://hub.docker.com \ https://auth.docker.io \ https://registry-1.docker.io \ https://index.docker.io/ \ https://dseasb33srnrn.cloudfront.net/ \ https://production.cloudflare.docker.com/	소프트웨어 이미지, 매니페스트, 템플릿에 대한 액세스를 제공하고 로그와 메트릭을 전송합니다.
\ https://support.compliance.api.console.netapp.com/	NetApp 감사 기록에서 데이터를 스트리밍할 수 있도록 합니다.

GCP에 필요한 엔드포인트

엔드포인트	목적
\ https://api.console.netapp.com	NetApp 계정을 포함하는 콘솔 서비스와의 통신입니다.
\ https://netapp-cloud-account.auth0.com \ https://auth0.com	중앙화된 사용자 인증을 위해 콘솔 웹사이트와 통신합니다.

엔드포인트	목적
\ https://support.compliance.api.console.netapp.com/ \ https://hub.docker.com \ https://auth.docker.io \ https://registry-1.docker.io \ https://index.docker.io/ \ https://dseasb33srnrn.cloudfront.net/ \ https://production.cloudflare.docker.com/	소프트웨어 이미지, 매니페스트, 템플릿에 대한 액세스를 제공하고 로그와 메트릭을 전송합니다.
\ https://support.compliance.api.console.netapp.com/	NetApp 감사 기록에서 데이터를 스트리밍할 수 있도록 합니다.

데이터 분류에 필요한 권한이 있는지 확인하세요.

데이터 분류에 리소스를 배포하고 데이터 분류 인스턴스에 대한 보안 그룹을 생성할 수 있는 권한이 있는지 확인하세요.

- "Google Cloud 권한"
- "AWS 권한"
- "Azure 권한"

콘솔 에이전트가 데이터 분류에 액세스할 수 있는지 확인하세요.

콘솔 에이전트와 데이터 분류 인스턴스 간의 연결을 보장합니다. 콘솔 에이전트의 보안 그룹은 포트 443을 통해 데이터 분류 인스턴스와의 인바운드 및 아웃바운드 트래픽을 허용해야 합니다. 이 연결을 통해 데이터 분류 인스턴스를 배포하고 규정 준수 및 거버넌스 탭에서 정보를 볼 수 있습니다. 데이터 분류는 AWS와 Azure의 정부 지역에서 지원됩니다.

AWS 및 AWS GovCloud 배포에는 추가적인 인바운드 및 아웃바운드 보안 그룹 규칙이 필요합니다. 보다 "AWS의 콘솔 에이전트에 대한 규칙" 자세한 내용은.

Azure 및 Azure Government 배포에는 추가적인 인바운드 및 아웃바운드 보안 그룹 규칙이 필요합니다. 보다 "Azure의 콘솔 에이전트에 대한 규칙" 자세한 내용은.

데이터 분류를 계속 실행할 수 있는지 확인하세요.

데이터 분류 인스턴스는 지속적으로 데이터를 스캔하기 위해 켜져 있어야 합니다.

데이터 분류에 대한 웹 브라우저 연결을 보장합니다.

데이터 분류가 활성화된 후, 사용자가 데이터 분류 인스턴스에 연결된 호스트에서 콘솔 인터페이스에 액세스하는지 확인하세요.

데이터 분류 인스턴스는 개인 IP 주소를 사용하여 인덱싱된 데이터가 인터넷에서 접근되지 않도록 보장합니다. 따라서 콘솔에 접속하는 데 사용하는 웹 브라우저는 해당 개인 IP 주소에 연결되어 있어야 합니다. 해당 연결은 클라우드 공급자(예: VPN)에 대한 직접 연결을 통해 이루어질 수도 있고, 데이터 분류 인스턴스와 동일한 네트워크 내부에 있는 호스트를 통해 이루어질 수도 있습니다.

vCPU 제한을 확인하세요

클라우드 제공업체의 vCPU 한도가 필요한 수의 코어를 갖춘 인스턴스를 배포할 수 있는지 확인하세요. 콘솔이 실행되는 지역에서 해당 인스턴스 패밀리에 대한 vCPU 제한을 확인해야 합니다. "필요한 인스턴스 유형을 확인하세요" .

vCPU 제한에 대한 자세한 내용은 다음 링크를 참조하세요.

- "AWS 설명서: Amazon EC2 서비스 할당량"
- "Azure 설명서: 가상 머신 vCPU 할당량"
- "Google Cloud 문서: 리소스 할당량"

클라우드에 데이터 분류 배포

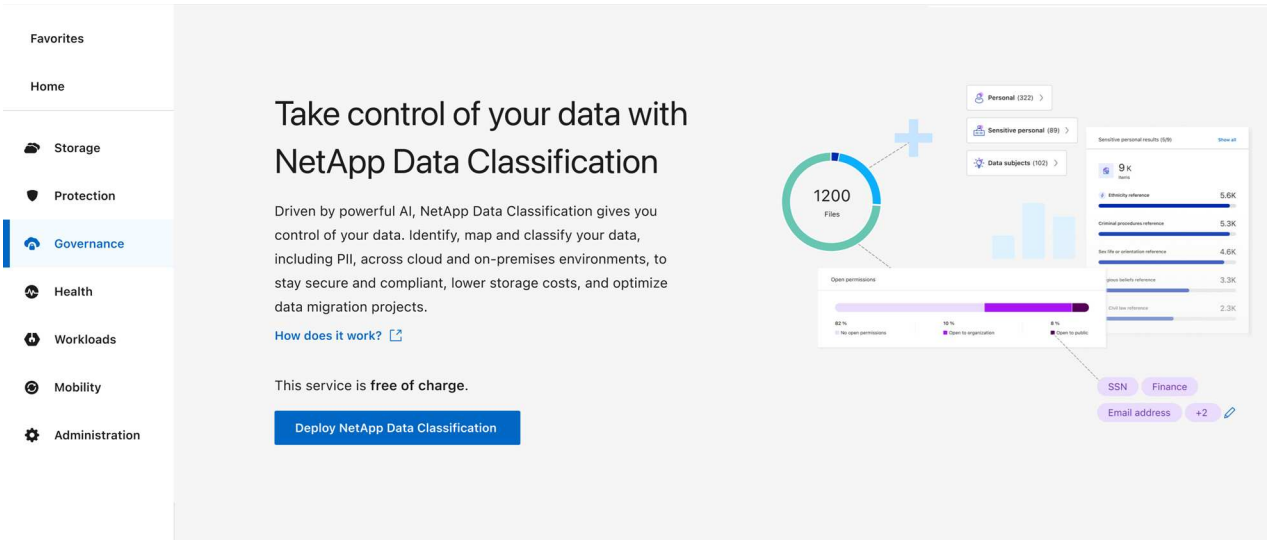
클라우드에 데이터 분류 인스턴스를 배포하려면 다음 단계를 따르세요. 콘솔 에이전트는 클라우드에 인스턴스를 배포한 다음 해당 인스턴스에 데이터 분류 소프트웨어를 설치합니다.

기본 인스턴스 유형을 사용할 수 없는 지역에서는 데이터 분류가 실행됩니다."대체 인스턴스 유형" .

AWS에 배포

단계

1. 데이터 분류의 메인 페이지에서 *온프레미스 또는 클라우드에 분류 배포*를 선택합니다.

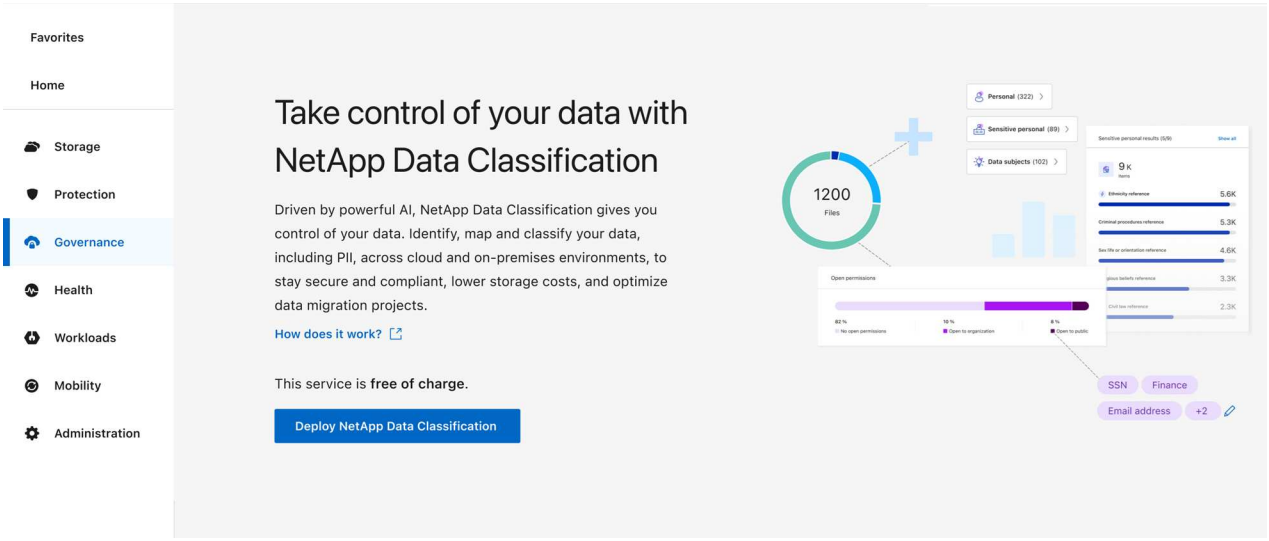


2. 설치 페이지에서 *배포 > 배포*를 선택하여 "대형" 인스턴스 크기를 사용하고 클라우드 배포 마법사를 시작합니다.
3. 마법사는 배포 단계를 진행하면서 진행 상황을 표시합니다. 입력이 필요하거나 문제가 발생하면 메시지가 표시됩니다.
4. 인스턴스가 배포되고 데이터 분류가 설치되면 *구성 계속*을 선택하여 구성 페이지로 이동합니다.

Azure에 배포

단계

1. 데이터 분류의 메인 페이지에서 *온프레미스 또는 클라우드에 분류 배포*를 선택합니다.



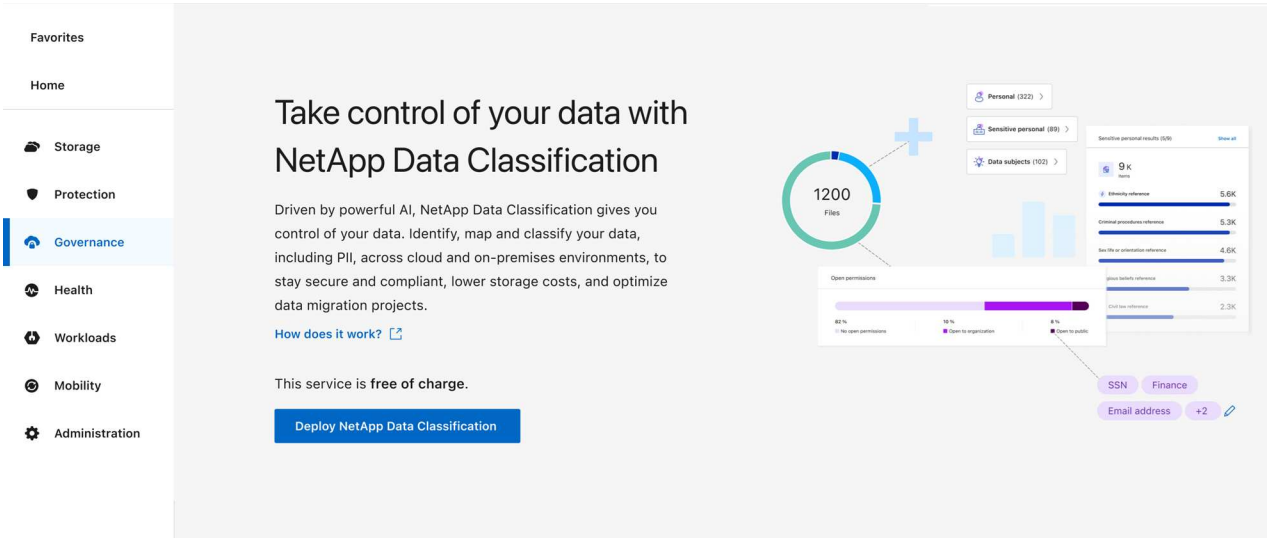
2. 클라우드 배포 마법사를 시작하려면 *배포*를 선택하세요.
3. 마법사는 배포 단계를 진행하면서 진행 상황을 표시합니다. 문제가 발생하면 멈추고 입력을 요청합니다.

4. 인스턴스가 배포되고 데이터 분류가 설치되면 *구성 계속*을 선택하여 구성 페이지로 이동합니다.

Google Cloud에 배포

단계

1. 데이터 분류의 메인 페이지에서 *거버넌스 > 분류*를 선택합니다.
2. *온프레미스 또는 클라우드에 분류 배포*를 선택합니다.



3. 클라우드 배포 마법사를 시작하려면 *배포*를 선택하세요.
4. 마법사는 배포 단계를 진행하면서 진행 상황을 표시합니다. 문제가 발생하면 멈추고 입력을 요청합니다.
5. 인스턴스가 배포되고 데이터 분류가 설치되면 *구성 계속*을 선택하여 구성 페이지로 이동합니다.

결과

콘솔은 클라우드 공급자에 데이터 분류 인스턴스를 배포합니다.

인스턴스가 인터넷에 연결되어 있는 한 콘솔 에이전트와 데이터 분류 소프트웨어의 업그레이드는 자동화됩니다.

다음은 무엇인가

구성 페이지에서 스캔할 데이터 소스를 선택할 수 있습니다.

인터넷 접속이 가능한 호스트에 **NetApp Data Classification** 설치

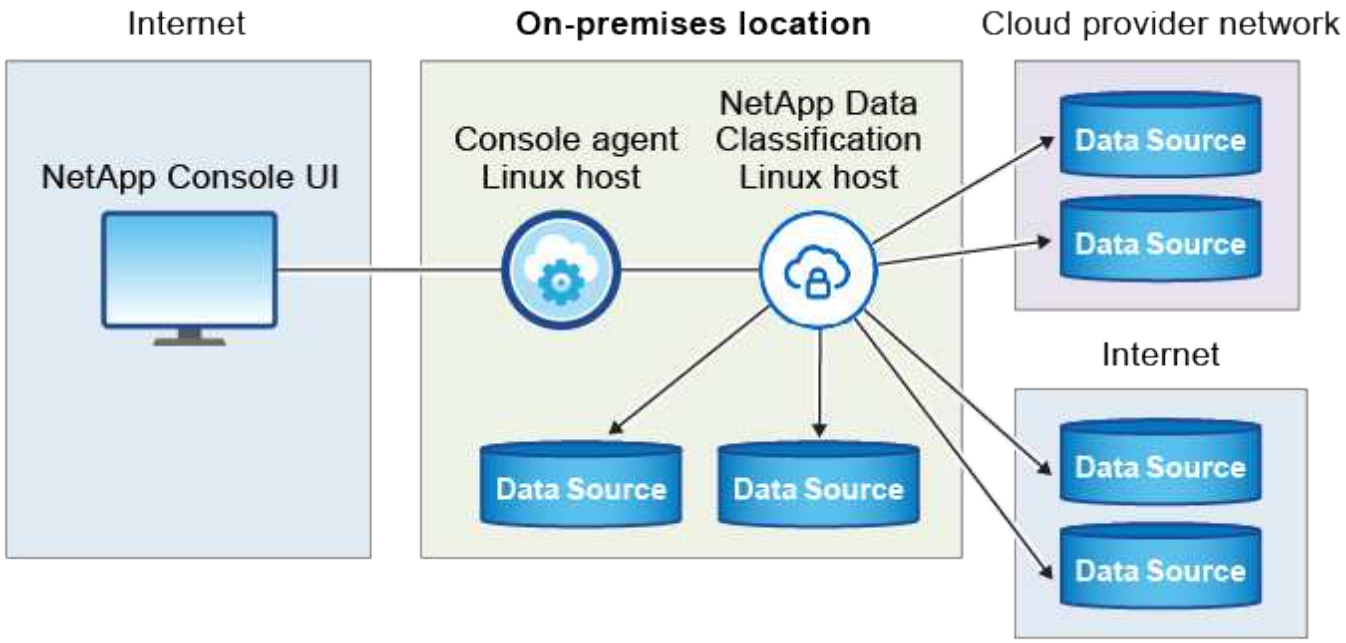
네트워크의 Linux 호스트나 인터넷 접속이 가능한 클라우드의 Linux 호스트에 NetApp Data Classification 배포하려면 네트워크나 클라우드에 Linux 호스트를 수동으로 배포해야 합니다.

온프레미스 설치는 온프레미스에 있는 데이터 분류 인스턴스를 사용하여 온프레미스 ONTAP 시스템을 스캔하는 것을 선호하는 경우에 좋은 옵션입니다. 이것은 필수사항이 아닙니다. 어떤 설치 방법을 선택하든 소프트웨어의 기능은 동일합니다.

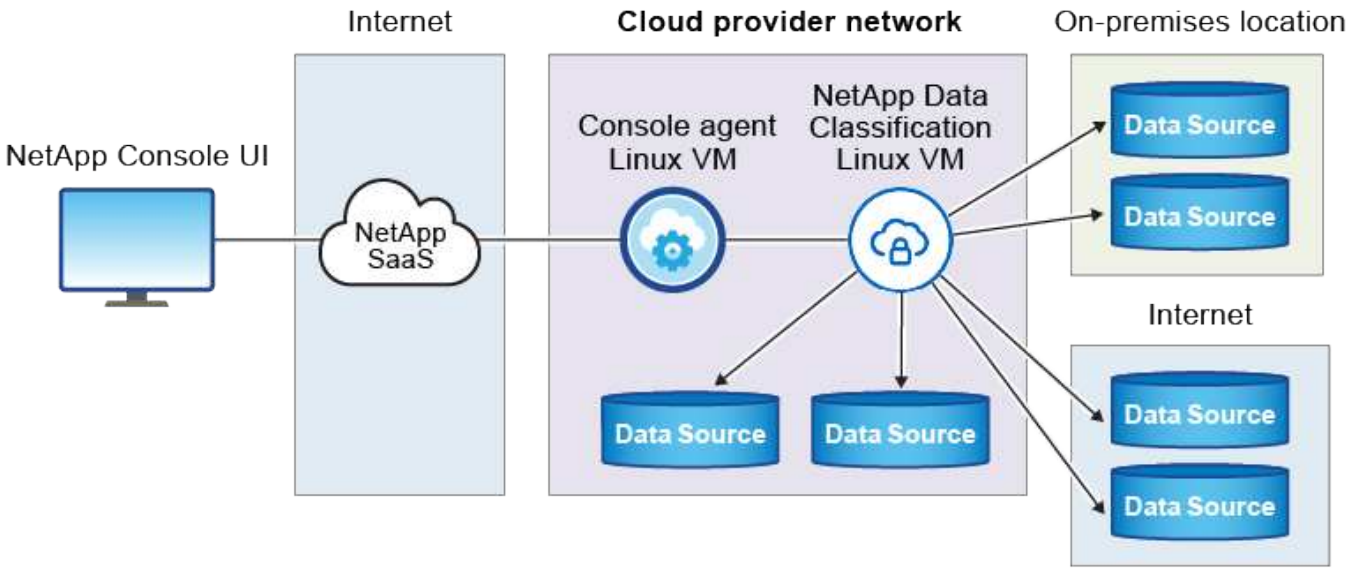
데이터 분류 설치 스크립트는 시스템과 환경이 필수 전제 조건을 충족하는지 확인하는 것으로 시작됩니다. 모든 전제 조건이 충족되면 설치가 시작됩니다. 데이터 분류 설치를 실행하지 않고도 전제 조건을 독립적으로 확인하려면 전제 조건만 테스트하는 별도의 소프트웨어 패키지를 다운로드할 수 있습니다. "Linux 호스트가 데이터 분류를 설치할 준비가

되었는지 확인하는 방법을 알아보세요." .

귀사 구내의 Linux 호스트에 일반적으로 설치되는 구성 요소와 연결은 다음과 같습니다.



클라우드에 있는 Linux 호스트에 일반적으로 설치되는 구성 요소와 연결은 다음과 같습니다.



빠른 시작

다음 단계에 따라 빠르게 시작하거나, 나머지 섹션으로 스크롤하여 자세한 내용을 확인하세요.

1 콘솔 에이전트 만들기

아직 콘솔 에이전트가 없는 경우 "온프레미스에 콘솔 에이전트 배포" 네트워크의 Linux 호스트나 클라우드의 Linux 호스트에서.

클라우드 공급자를 사용하여 콘솔 에이전트를 생성할 수도 있습니다. 보다 "AWS에서 콘솔 에이전트 만들기" , "Azure에서 콘솔 에이전트 만들기" , 또는 "GCP에서 콘솔 에이전트 만들기" .

2 필수 조건 검토

귀하의 환경이 전제 조건을 충족하는지 확인하세요. 여기에는 인스턴스에 대한 아웃바운드 인터넷 액세스, 포트 443을 통한 콘솔 에이전트와 데이터 분류 간의 연결 등이 포함됩니다. 전체 목록을 확인하세요 .

또한 다음을 충족하는 Linux 시스템이 필요합니다.다음 요구 사항 .

3 데이터 분류 다운로드 및 배포

NetApp 지원 사이트에서 클라우드 데이터 분류 소프트웨어를 다운로드하고 사용하려는 Linux 호스트에 설치 프로그램 파일을 복사합니다. 그런 다음 설치 마법사를 실행하고 메시지에 따라 데이터 분류 인스턴스를 배포합니다.

콘솔 에이전트 만들기

데이터 분류를 설치하고 사용하려면 콘솔 에이전트가 필요합니다. 대부분의 경우 데이터 분류를 활성화하기 전에 콘솔 에이전트를 설정했을 가능성이 높습니다. "콘솔 기능에는 콘솔 에이전트가 필요합니다." 하지만 지금 당장 설정해야 하는 경우도 있습니다.

클라우드 공급자 환경에서 하나를 생성하려면 다음을 참조하세요. "AWS에서 콘솔 에이전트 만들기" , "Azure에서 콘솔 에이전트 만들기" , 또는 "GCP에서 콘솔 에이전트 만들기" .

특정 클라우드 공급자에 배포된 콘솔 에이전트를 사용해야 하는 몇 가지 시나리오가 있습니다.

- AWS의 Cloud Volumes ONTAP 또는 Amazon FSx for ONTAP 에서 데이터를 스캔할 때 AWS의 콘솔 에이전트를 사용합니다.
- Azure의 Cloud Volumes ONTAP 또는 Azure NetApp Files 에서 데이터를 스캔할 때 Azure의 콘솔 에이전트를 사용합니다.

  Azure NetApp Files 의 경우, 스캔하려는 볼륨과 동일한 지역에 배포해야 합니다.

- GCP에서 Cloud Volumes ONTAP 의 데이터를 스캔할 때 GCP의 콘솔 에이전트를 사용합니다.

온프레미스 ONTAP 시스템, NetApp 파일 공유 및 데이터베이스 계정은 이러한 클라우드 콘솔 에이전트를 사용하여 스캔할 수 있습니다.

또한 다음을 수행할 수도 있습니다. "온프레미스에 콘솔 에이전트 배포" 네트워크의 Linux 호스트나 클라우드의 Linux 호스트에서. 온프레미스에 데이터 분류를 설치하려는 일부 사용자는 콘솔 에이전트도 온프레미스에 설치하기로 선택할 수도 있습니다.

데이터 분류를 설치할 때 콘솔 에이전트 시스템의 IP 주소나 호스트 이름이 필요합니다. 사내에 콘솔 에이전트를 설치한 경우 이 정보를 얻을 수 있습니다. 콘솔 에이전트가 클라우드에 배포된 경우 콘솔에서 다음 정보를 찾을 수 있습니다. 도움말 아이콘을 선택한 다음 *지원*을 선택하고 콘솔 에이전트를 선택합니다.

Linux 호스트 시스템 준비

데이터 분류 소프트웨어는 특정 운영 체제 요구 사항, RAM 요구 사항, 소프트웨어 요구 사항 등을 충족하는 호스트에서 실행되어야 합니다. Linux 호스트는 네트워크에 있을 수도 있고 클라우드에 있을 수도 있습니다.

데이터 분류를 계속 실행할 수 있는지 확인하세요. 데이터 분류 머신은 지속적으로 데이터를 스캔하기 위해 계속 켜져 있어야 합니다.

- 데이터 분류는 전용 호스트에서 수행되어야 합니다. 호스트는 다른 애플리케이션이나 바이러스 백신과 같은 타사 소프트웨어와 공유할 수 없습니다.
- 데이터 분류를 통해 스캔할 데이터 세트에 맞는 크기를 선택하십시오.

시스템 크기	**CPU**	**RAM(**스왑 메모리를 비활성화해야 함**)**	디스크
특대	32개의 CPU	128GB 램	• /에 1TiB SSD, 또는 /opt에 100GiB 사용 가능 • /var/lib/docker에서 895GiB 사용 가능 • /tmp에 5GiB • **Podman**의 경우 **/var/tmp**에 **30GB**
크기가 큰	16개의 CPU	64GB 램	• /에 500GiB SSD, 또는 /opt에 100GiB 사용 가능 • /var/lib/docker 또는 Podman /var/lib/containers에서 400GiB 사용 가능 • /tmp에 5GiB • **Podman**의 경우 **/var/tmp**에 **30GB**

- 데이터 분류 설치를 위해 클라우드에 컴퓨팅 인스턴스를 배포할 때 위의 "대규모" 시스템 요구 사항을 충족하는 시스템을 사용하는 것이 좋습니다.
  - **Amazon Elastic Compute Cloud(Amazon EC2)** 인스턴스 유형: "m6i.4xlarge". "추가 AWS 인스턴스 유형 보기" .
  - **Azure VM** 크기: "Standard_D16s_v3". "추가 Azure 인스턴스 유형 보기" .
  - **GCP** 머신 유형: "n2-standard-16". "추가 GCP 인스턴스 유형을 참조하세요." .
- **UNIX** 폴더 권한: 다음과 같은 최소 UNIX 권한이 필요합니다.

접는 사람	최소 권한
/임시	`rwxrwxrwt`
/고르다	`rwxr-xr-x`
/var/lib/도커	`rwx------`
/usr/lib/systemd/시스템	`rwxr-xr-x`

- 운영체제:

- 다음 운영 체제에서는 Docker 컨테이너 엔진을 사용해야 합니다.
  - Red Hat Enterprise Linux 버전 7.8 및 7.9
  - Ubuntu 22.04(데이터 분류 버전 1.23 이상 필요)
  - Ubuntu 24.04(데이터 분류 버전 1.23 이상 필요)
- 다음 운영 체제에서는 Podman 컨테이너 엔진을 사용해야 하며, Data Classification 버전 1.30 이상이 필요합니다.
  - Red Hat Enterprise Linux 버전 8.8, 8.10, 9.0, 9.1, 9.2, 9.3, 9.4, 9.5 및 9.6.
- 호스트 시스템에서 고급 벡터 확장(AVX2)을 활성화해야 합니다.

- **Red Hat Subscription Management**: 호스트는 Red Hat Subscription Management에 등록되어야 합니다. 등록되지 않은 경우, 설치 중에 시스템은 저장소에 접근하여 필요한 타사 소프트웨어를 업데이트할 수 없습니다.
- 추가 소프트웨어: 데이터 분류를 설치하기 전에 호스트에 다음 소프트웨어를 설치해야 합니다.
  - 사용 중인 운영체제에 따라 컨테이너 엔진 중 하나를 설치해야 합니다.
    - Docker Engine 버전 19.3.1 이상. "설치 지침 보기" .
    - Podman 버전 4 이상. Podman을 설치하려면 다음을 입력하세요.(`sudo yum install podman netavark -y`).
- Python 버전 3.6 이상. "설치 지침 보기" .
  - **NTP** 고려 사항: NetApp 데이터 분류 시스템을 구성하여 NTP(네트워크 시간 프로토콜) 서비스를 사용할 것을 권장합니다. 데이터 분류 시스템과 콘솔 에이전트 시스템 간의 시간은 동기화되어야 합니다.
- 방화벽 고려 사항: 방화벽을 사용하려는 경우 `firewalld` 데이터 분류를 설치하기 전에 해당 기능을 활성화하는 것이 좋습니다. 다음 명령을 실행하여 구성하세요. `firewalld` 데이터 분류와 호환되도록:

```
firewall-cmd --permanent --add-service=http
firewall-cmd --permanent --add-service=https
firewall-cmd --permanent --add-port=80/tcp
firewall-cmd --permanent --add-port=8080/tcp
firewall-cmd --permanent --add-port=443/tcp
firewall-cmd --reload
```

추가 데이터 분류 호스트를 스캐너 노드로 사용할 계획이라면 지금 바로 기본 시스템에 다음 규칙을 추가하세요.

```
firewall-cmd --permanent --add-port=2377/tcp
firewall-cmd --permanent --add-port=7946/udp
firewall-cmd --permanent --add-port=7946/tcp
firewall-cmd --permanent --add-port=4789/udp
```

Docker 또는 Podman을 활성화하거나 업데이트할 때마다 다시 시작해야 합니다. `firewalld` 설정.

데이터 분류 호스트 시스템의 IP 주소는 설치 후 변경할 수 없습니다.

데이터 분류에서 아웃바운드 인터넷 액세스 활성화

데이터 분류에는 아웃바운드 인터넷 액세스가 필요합니다. 가상 또는 물리적 네트워크에서 인터넷 접속을 위해 프록시 서버를 사용하는 경우, 데이터 분류 인스턴스에 다음 엔드포인트에 연결할 수 있는 아웃바운드 인터넷 접속 권한이 있는지 확인하세요.

엔드포인트	목적
\ https://api.console.netapp.com	NetApp 계정을 포함한 콘솔과의 통신.
\ https://netapp-cloud-account.auth0.com \ https://auth0.com	중앙화된 사용자 인증을 위해 콘솔 웹사이트와 통신합니다.
\ https://support.compliance.api.bluexp.netapp.com/ \ https://hub.docker.com \ https://auth.docker.io \ https://registry-1.docker.io \ https://index.docker.io/ \ https://dseasb33srnrn.cloudfront.net/ \ https://production.cloudflare.docker.com/	소프트웨어 이미지, 매니페스트, 템플릿에 대한 액세스를 제공하고 로그와 메트릭을 전송합니다.
\ https://support.compliance.api.bluexp.netapp.com/	NetApp 감사 기록에서 데이터를 스트리밍할 수 있도록 합니다.
\ https://github.com/docker \ https://download.docker.com	Docker 설치를 위한 필수 패키지를 제공합니다.
\ http://packages.ubuntu.com/ \ http://archive.ubuntu.com	Ubuntu 설치를 위한 필수 패키지를 제공합니다.

모든 필수 포트가 활성화되어 있는지 확인하세요

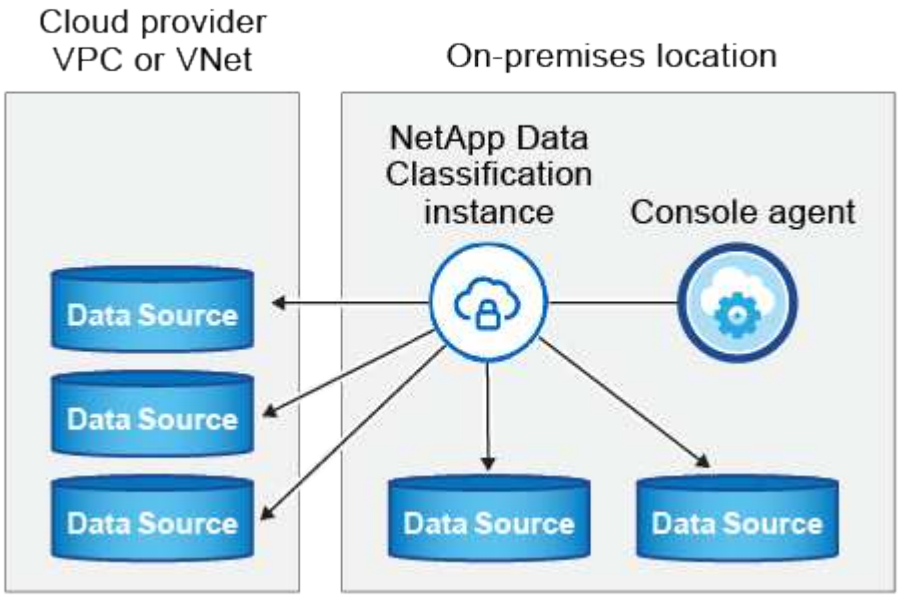
콘솔 에이전트, 데이터 분류, Active Directory 및 데이터 소스 간 통신에 필요한 모든 포트가 열려 있는지 확인해야 합니다.

연결 유형	포트	설명
콘솔 에이전트 <> 데이터 분류	8080(TCP), 443(TCP), 80. 9000	콘솔 에이전트의 방화벽 또는 라우팅 규칙은 포트 443을 통해 데이터 분류 인스턴스로의 인바운드 및 아웃바운드 트래픽을 허용해야 합니다. 콘솔에서 설치 진행 상황을 볼 수 있도록 포트 8080이 열려 있는지 확인하세요. Linux 호스트에서 방화벽을 사용하는 경우 Ubuntu 서버 내의 내부 프로세스에는 포트 9000이 필요합니다.

연결 유형	포트	설명
콘솔 에이전트 <> ONTAP 클러스터(NAS)	443(TCP)	콘솔은 HTTPS를 사용하여 ONTAP 클러스터를 검색합니다. 사용자 지정 방화벽 정책을 사용하는 경우 다음 요구 사항을 충족해야 합니다. • 콘솔 에이전트 호스트는 포트 443을 통해 아웃바운드 HTTPS 액세스를 허용해야 합니다. 콘솔 에이전트가 클라우드에 있는 경우 모든 아웃바운드 통신은 사전 정의된 방화벽이나 라우팅 규칙에 따라 허용됩니다. • ONTAP 클러스터는 포트 443을 통해 인바운드 HTTPS 액세스를 허용해야 합니다. 기본 "mgmt" 방화벽 정책은 모든 IP 주소에서 인바운드 HTTPS 액세스를 허용합니다. 이 기본 정책을 수정했거나 사용자 고유의 방화벽 정책을 만든 경우 HTTPS 프로토콜을 해당 정책과 연결하고 콘솔 에이전트 호스트에서 액세스를 활성화해야 합니다.
데이터 분류 <> ONTAP 클러스터	• NFS의 경우 - 111(TCP\UDP) 및 2049(TCP\UDP) • CIFS의 경우 - 139(TCP\UDP) 및 445(TCP\UDP)	데이터 분류에는 각 Cloud Volumes ONTAP 서브넷이나 온프레미스 ONTAP 시스템에 대한 네트워크 연결이 필요합니다. Cloud Volumes ONTAP 의 방화벽이나 라우팅 규칙은 데이터 분류 인스턴스에서 인바운드 연결을 허용해야 합니다. 다음 포트가 데이터 분류 인스턴스에 열려 있는지 확인하세요. • NFS - 111 및 2049의 경우 • CIFS - 139 및 445의 경우 NFS 볼륨 내보내기 정책은 데이터 분류 인스턴스에서의 액세스를 허용해야 합니다.
데이터 분류 <> Active Directory	389(TCP 및 UDP), 636(TCP), 3268(TCP), 3269(TCP)	회사 사용자를 위해 Active Directory가 이미 설정되어 있어야 합니다. 또한, 데이터 분류에는 CIFS 볼륨을 스캔하기 위한 Active Directory 자격 증명이 필요합니다. Active Directory에 대한 정보가 있어야 합니다. • DNS 서버 IP 주소 또는 여러 IP 주소 • 서버의 사용자 이름 및 비밀번호 • 도메인 이름(Active Directory 이름) • 보안 LDAP(LDAPS)를 사용하든 사용하지 않든 • LDAP 서버 포트(일반적으로 LDAP의 경우 389, 보안 LDAP의 경우 636)

Linux 호스트에 데이터 분류 설치

일반적인 구성의 경우 단일 호스트 시스템에 소프트웨어를 설치합니다. 여기에서 해당 단계를 확인하세요 .



보다Linux 호스트 시스템 준비 그리고필수 조건 검토 데이터 분류를 배포하기 전에 필요한 전체 요구 사항 목록을 확인하세요.

인스턴스에 인터넷 연결이 있는 한 데이터 분류 소프트웨어 업그레이드는 자동으로 수행됩니다.

현재 데이터 분류 기능은 온프레미스에 소프트웨어가 설치된 경우 S3 버킷, Azure NetApp Files 또는 FSx for ONTAP 검색할 수 없습니다. 이러한 경우 클라우드에 별도의 콘솔 에이전트와 데이터 분류 인스턴스를 배포해야 합니다. "커넥터 간 전환" 다양한 데이터 소스에 대해.

일반적인 구성을 위한 단일 호스트 설치

단일 온프레미스 호스트에 데이터 분류 소프트웨어를 설치할 때 요구 사항을 검토하고 다음 단계를 따르세요.

"이 영상을 시청하세요"데이터 분류를 설치하는 방법을 알아보세요.

데이터 분류를 설치할 때 모든 설치 활동이 기록됩니다. 설치 중에 문제가 발생하면 설치 감사 로그의 내용을 볼 수 있습니다. 에 쓰여있다 `/opt/netapp/install_logs/` .

시작하기 전에

- Linux 시스템이 다음 사항을 충족하는지 확인하십시오.호스트 요구 사항 .
- 시스템에 두 가지 필수 소프트웨어 패키지(Docker Engine 또는 Podman, Python 3)가 설치되어 있는지 확인합니다.
- Linux 시스템에서 루트 권한이 있는지 확인하세요.
- 인터넷에 접속하기 위해 프록시를 사용하는 경우:
  - 프록시 서버 정보(IP 주소 또는 호스트 이름, 연결 포트, 연결 방식: https 또는 http, 사용자 이름 및 비밀번호)가 필요합니다.
  - 프록시가 TLS 가로채기를 수행하는 경우 TLS CA 인증서가 저장된 Data Classification Linux 시스템의

경로를 알아야 합니다.

- 프록시는 투명하지 않아야 합니다. 데이터 분류는 현재 투명 프록시를 지원하지 않습니다.
- 사용자는 로컬 사용자여야 합니다. 도메인 사용자는 지원되지 않습니다.

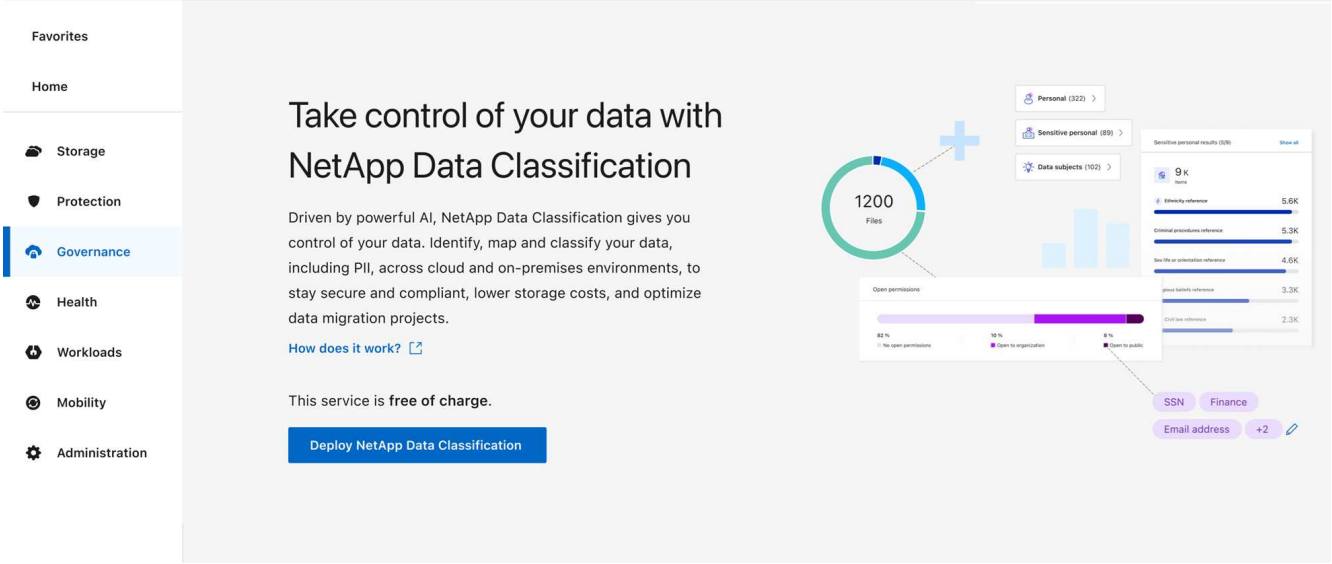
- 오프라인 환경이 요구 사항을 충족하는지 확인하세요.권한 및 연결 .

단계

1. 데이터 분류 소프트웨어를 다운로드하세요. "NetApp 지원 사이트" . 선택해야 하는 파일의 이름은 *DATASENSE-INSTALLER-<버전>.tar.gz*입니다.
2. 사용하려는 Linux 호스트에 설치 프로그램 파일을 복사합니다(사용 `scp` 또는 다른 방법).
3. 호스트 컴퓨터에서 설치 프로그램 파일의 압축을 풉니다. 예:

```
tar -xzf DATASENSE-INSTALLER-V1.25.0.tar.gz
```

4. 콘솔에서 *거버넌스 > 분류*를 선택합니다.
5. *온프레미스 또는 클라우드에 분류 배포*를 선택합니다.



6. 클라우드에서 준비한 인스턴스에 데이터 분류를 설치하는지, 아니면 사내에서 준비한 인스턴스에 데이터 분류를 설치하는지에 따라 적절한 배포 옵션을 선택하여 데이터 분류 설치를 시작합니다.
7. 온프레미스에 데이터 분류 배포 대화 상자가 표시됩니다. 제공된 명령을 복사합니다(예: `sudo ./install.sh -a 12345 -c 27AG75 -t 2198qq`)을 텍스트 파일에 붙여넣어 나중에 사용할 수 있습니다. 그런 다음 *닫기*를 선택하여 대화 상자를 닫습니다.
8. 호스트 머신에서 복사한 명령을 입력한 다음 일련의 프롬프트를 따르거나 모든 필수 매개변수를 포함한 전체 명령을 명령줄 인수로 제공할 수 있습니다.

   설치 프로그램은 성공적인 설치를 위해 시스템 및 네트워킹 요구 사항이 충족되는지 사전 점검을 수행합니다. "이 영상을 시청하세요" 사전 확인 메시지와 그 의미를 이해합니다.

프롬프트에 따라 매개변수를 입력하세요.	전체 명령을 입력하세요:
a. 7단계에서 복사한 명령을 붙여넣습니다. `sudo ./install.sh -a <account_id> -c <client_id> -t <user_token>` 클라우드 인스턴스(사내가 아닌)에 설치하는 경우 다음을 추가하세요. `--manual-cloud-install <cloud_provider>` . b. 콘솔 에이전트 시스템에서 액세스할 수 있도록 데이터 분류 호스트 머신의 IP 주소 또는 호스트 이름을 입력하세요. c. 데이터 분류 시스템에서 액세스할 수 있도록 콘솔 에이전트 호스트 머신의 IP 주소 또는 호스트 이름을 입력하세요. d. 지시에 따라 프록시 세부 정보를 입력하세요. 콘솔 에이전트가 이미 프록시를 사용하는 경우 데이터 분류가 자동으로 콘솔 에이전트에서 사용하는 프록시를 사용하므로 여기에 다시 정보를 입력할 필요가 없습니다.	또는 필요한 호스트 및 프록시 매개변수를 제공하여 전체 명령을 미리 만들 수 있습니다. `sudo ./install.sh -a <account_id> -c <client_id> -t <user_token> --host <ds_host> --manager-host <cm_host> --manual-cloud-install <cloud_provider> --proxy-host <proxy_host> --proxy-port <proxy_port> --proxy-scheme <proxy_scheme> --proxy -user <proxy_user> --proxy-password <proxy_password> --cacert-folder-path <ca_cert_dir>`

변수 값:

- *account_id* = NetApp 계정 ID
- *client_id* = 콘솔 에이전트 클라이언트 ID(클라이언트 ID에 접미사 "clients"가 없으면 추가)
- *user_token* = JWT 사용자 액세스 토큰
- *ds_host* = 데이터 분류 Linux 시스템의 IP 주소 또는 호스트 이름입니다.
- *cm_host* = 콘솔 에이전트 시스템의 IP 주소 또는 호스트 이름입니다.
- *cloud_provider* = 클라우드 인스턴스에 설치하는 경우 클라우드 공급자에 따라 "AWS", "Azure" 또는 "Gcp"를 입력하세요.
- *proxy_host* = 호스트가 프록시 서버 뒤에 있는 경우 프록시 서버의 IP 또는 호스트 이름입니다.
- *proxy_port* = 프록시 서버에 연결할 포트(기본값 80).
- *proxy_scheme* = 연결 방식: https 또는 http(기본값은 http).
- *proxy_user* = 기본 인증이 필요한 경우 프록시 서버에 연결하는 인증된 사용자입니다. 사용자는 로컬 사용자여야 합니다. 도메인 사용자는 지원되지 않습니다.
- *proxy_password* = 지정한 사용자 이름에 대한 비밀번호입니다.
- *ca_cert_dir* = 추가 TLS CA 인증서 번들이 포함된 Data Classification Linux 시스템의 경로입니다. 프록시가 TLS 가로채기를 수행하는 경우에만 필요합니다.

결과

데이터 분류 설치 프로그램은 패키지를 설치하고, 설치를 등록하고, 데이터 분류를 설치합니다. 설치하는 데 10~20분이 걸릴 수 있습니다.

호스트 머신과 콘솔 에이전트 인스턴스 사이에 포트 8080을 통해 연결이 있는 경우 콘솔의 데이터 분류 탭에서 설치

진행률을 볼 수 있습니다.

다음은 무엇인가

구성 페이지에서 스캔할 데이터 소스를 선택할 수 있습니다.

인터넷 접속이 없는 Linux 호스트에 NetApp Data Classification 설치

인터넷 접속이 불가능한 온프레미스 사이트의 Linux 호스트에 NetApp Data Classification 설치하는 것을 _개인 모드_라고 합니다. 설치 스크립트를 사용하는 이 유형의 설치는 NetApp Console SaaS 계층에 연결되지 않습니다.

BlueXP 개인 모드(레거시 BlueXP 인터페이스)는 일반적으로 인터넷 연결이 없고 AWS Secret Cloud, AWS Top Secret Cloud, Azure IL6를 포함하는 보안 클라우드 지역이 있는 온프레미스 환경에서 사용됩니다. NetApp 기존 BlueXP 인터페이스를 통해 이러한 환경을 계속 지원합니다. 레거시 BlueXP 인터페이스의 개인 모드 설명서는 다음을 참조하세요."BlueXP 개인 모드에 대한 PDF 문서" .

Linux 호스트가 NetApp Data Classification 설치할 준비가 되었는지 확인하세요.

Linux 호스트에 NetApp Data Classification 수동으로 설치하기 전에 호스트에서 스크립트를 실행하여 Data Classification을 설치하는 데 필요한 모든 전제 조건이 충족되었는지 확인합니다. 이 스크립트는 네트워크의 Linux 호스트나 클라우드의 Linux 호스트에서 실행할 수 있습니다. 호스트는 인터넷에 연결되어 있을 수도 있고, 인터넷에 접속할 수 없는 사이트(다크 사이트)에 있을 수도 있습니다.

데이터 분류 설치 스크립트에는 환경이 요구 사항을 충족하는지 확인하는 테스트 스크립트가 포함되어 있습니다. 설치 스크립트를 실행하기 전에 Linux 호스트의 준비 상태를 확인하기 위해 이 스크립트를 별도로 실행할 수 있습니다.

시작하기

다음 작업을 수행하게 됩니다.

- 선택적으로, 콘솔 에이전트가 설치되어 있지 않으면 설치하세요. 콘솔 에이전트를 설치하지 않고도 테스트 스크립트를 실행할 수 있지만, 스크립트는 콘솔 에이전트와 데이터 분류 호스트 머신 간의 연결을 확인합니다. 따라서 콘솔 에이전트를 설치하는 것이 좋습니다.
- 호스트 머신을 준비하고 모든 요구 사항을 충족하는지 확인하세요.
- 데이터 분류 호스트 머신에서 아웃바운드 인터넷 액세스를 활성화합니다.
- 모든 시스템에서 필요한 포트가 모두 활성화되어 있는지 확인하세요.
- 필수 테스트 스크립트를 다운로드하여 실행하세요.

콘솔 에이전트 만들기

데이터 분류를 설치하고 사용하려면 콘솔 에이전트가 필요합니다. 하지만 콘솔 에이전트 없이도 필수 구성 요소 스크립트를 실행할 수 있습니다.

당신은 할 수 있습니다 "온프레미스에 콘솔 에이전트 설치" 네트워크 내의 Linux 호스트 또는 클라우드의 Linux 호스트에서 실행할 수 있습니다. 콘솔 에이전트가 온프레미스에 설치되어 있는 경우 데이터 분류 기능도 온프레미스에 설치할 수 있습니다.

클라우드 공급자 환경에서 콘솔 에이전트를 생성하려면 다음을 참조하세요.

- "AWS에서 콘솔 에이전트 만들기"
- "Azure에서 콘솔 에이전트 만들기"
- "GCP에서 콘솔 에이전트 만들기"

필수 조건 스크립트를 실행하려면 콘솔 에이전트 시스템의 IP 주소 또는 호스트 이름이 필요합니다. 콘솔 에이전트를 사내에 설치한 경우 이 정보를 확인할 수 있습니다. 콘솔 에이전트가 클라우드에 배포된 경우 콘솔에서 이 정보를 확인할 수 있습니다. 도움말 아이콘을 선택한 다음 *지원*을 선택하고, 에이전트 및 감사 섹션에서 *에이전트로 이동*을 선택하세요.

호스트 요구 사항 확인

데이터 분류 소프트웨어는 특정 운영 체제 요구 사항, RAM 요구 사항 및 소프트웨어 요구 사항을 충족하는 호스트에서 실행되어야 합니다.

- 데이터 분류는 전용 호스트에서 수행되어야 합니다. 호스트는 다른 애플리케이션이나 바이러스 백신과 같은 타사 소프트웨어와 공유할 수 없습니다.
- 데이터 분류를 통해 스캔할 데이터 세트에 맞는 크기를 선택하십시오.

시스템 크기	**CPU**	**RAM(**스왑 메모리를 비활성화해야 함**)**	디스크
특대	32개의 CPU	128GB 램	• /에 1TiB SSD, 또는 /opt에 100GiB 사용 가능 • /var/lib/docker에서 895GiB 사용 가능 • /tmp에 5GiB • **Podman**의 경우 **/var/tmp**에 **30GB**
크기가 큰	16개의 CPU	64GB 램	• /에 500GiB SSD, 또는 /opt에 100GiB 사용 가능 • /var/lib/docker 또는 Podman /var/lib/containers에서 400GiB 사용 가능 • /tmp에 5GiB • **Podman**의 경우 **/var/tmp**에 **30GB**

- 데이터 분류 설치를 위해 클라우드에 컴퓨팅 인스턴스를 배포할 때 위의 "대규모" 시스템 요구 사항을 충족하는 시스템을 사용하는 것이 좋습니다.

- **Amazon Elastic Compute Cloud(Amazon EC2)** 인스턴스 유형: "m6i.4xlarge". "추가 AWS 인스턴스 유형 보기" .
- **Azure VM** 크기: "Standard_D16s_v3". "추가 Azure 인스턴스 유형 보기" .
- **GCP** 머신 유형: "n2-standard-16". "추가 GCP 인스턴스 유형을 참조하세요." .

- **UNIX** 폴더 권한: 다음과 같은 최소 UNIX 권한이 필요합니다.

접는 사람	최소 권한
/임시	`rwxrwxrwt`
/고르다	`rwxr-xr-x`
/var/lib/도커	`rwx------`
/usr/lib/systemd/시스템	`rwxr-xr-x`

- 운영체제:
  - 다음 운영 체제에서는 Docker 컨테이너 엔진을 사용해야 합니다.
    - Red Hat Enterprise Linux 버전 7.8 및 7.9
    - Ubuntu 22.04(데이터 분류 버전 1.23 이상 필요)
    - Ubuntu 24.04(데이터 분류 버전 1.23 이상 필요)
  - 다음 운영 체제에서는 Podman 컨테이너 엔진을 사용해야 하며, Data Classification 버전 1.30 이상이 필요합니다.
    - Red Hat Enterprise Linux 버전 8.8, 8.10, 9.0, 9.1, 9.2, 9.3, 9.4, 9.5 및 9.6.
  - 호스트 시스템에서 고급 벡터 확장(AVX2)을 활성화해야 합니다.
- **Red Hat Subscription Management**: 호스트는 Red Hat Subscription Management에 등록되어야 합니다. 등록되지 않은 경우, 설치 중에 시스템은 저장소에 접근하여 필요한 타사 소프트웨어를 업데이트할 수 없습니다.
- 추가 소프트웨어: 데이터 분류를 설치하기 전에 호스트에 다음 소프트웨어를 설치해야 합니다.
  - 사용 중인 운영체제에 따라 컨테이너 엔진 중 하나를 설치해야 합니다.
    - Docker Engine 버전 19.3.1 이상. "설치 지침 보기" .
    - Podman 버전 4 이상. Podman을 설치하려면 다음을 입력하세요.(`sudo yum install podman netavark -y`).
- Python 버전 3.6 이상. "설치 지침 보기" .
  - **NTP** 고려 사항: NetApp 데이터 분류 시스템을 구성하여 NTP(네트워크 시간 프로토콜) 서비스를 사용할 것을 권장합니다. 데이터 분류 시스템과 콘솔 에이전트 시스템 간의 시간은 동기화되어야 합니다.
- 방화벽 고려 사항: 방화벽을 사용하려는 경우 `firewalld` 데이터 분류를 설치하기 전에 해당 기능을 활성화하는 것이 좋습니다. 다음 명령을 실행하여 구성하세요. `firewalld` 데이터 분류와 호환되도록:

```
firewall-cmd --permanent --add-service=http
firewall-cmd --permanent --add-service=https
firewall-cmd --permanent --add-port=80/tcp
firewall-cmd --permanent --add-port=8080/tcp
firewall-cmd --permanent --add-port=443/tcp
firewall-cmd --reload
```

추가 데이터 분류 호스트를 스캐너 노드로 사용하려는 경우(분산 모델에서), 이때 다음 규칙을 기본 시스템에 추가하세요.

```
firewall-cmd --permanent --add-port=2377/tcp
firewall-cmd --permanent --add-port=7946/udp
firewall-cmd --permanent --add-port=7946/tcp
firewall-cmd --permanent --add-port=4789/udp
```

Docker 또는 Podman을 활성화하거나 업데이트할 때마다 다시 시작해야 합니다. `firewalld` 설정.

데이터 분류에서 아웃바운드 인터넷 액세스 활성화

데이터 분류에는 아웃바운드 인터넷 액세스가 필요합니다. 가상 또는 물리적 네트워크에서 인터넷 접속을 위해 프록시 서버를 사용하는 경우, 데이터 분류 인스턴스에 다음 엔드포인트에 연결할 수 있는 아웃바운드 인터넷 접속 권한이 있는지 확인하세요.

인터넷 연결이 없는 사이트에 설치된 호스트 시스템에는 이 섹션이 필요하지 않습니다.

엔드포인트	목적
\ https://api.console.netapp.com	NetApp 계정을 포함하는 콘솔 서비스와의 통신입니다.
\ https://netapp-cloud-account.auth0.com \ https://auth0.com	중앙화된 사용자 인증을 위해 콘솔 웹사이트와 통신합니다.
\ https://support.compliance.api.console.netapp.com/ \ https://hub.docker.com \ https://auth.docker.io \ https://registry-1.docker.io \ https://index.docker.io/ \ https://dseasb33srnrn.cloudfront.net/ \ https://production.cloudflare.docker.com/	소프트웨어 이미지, 매니페스트, 템플릿에 대한 액세스를 제공하고 로그와 메트릭을 전송합니다.
\ https://support.compliance.api.console.netapp.com/	NetApp 감사 기록에서 데이터를 스트리밍할 수 있도록 합니다.
\ https://github.com/docker \ https://download.docker.com	Docker 설치를 위한 필수 패키지를 제공합니다.
\ http://packages.ubuntu.com/ \ http://archive.ubuntu.com	Ubuntu 설치를 위한 필수 패키지를 제공합니다.

모든 필수 포트가 활성화되어 있는지 확인하세요

콘솔 에이전트, 데이터 분류, Active Directory 및 데이터 소스 간 통신에 필요한 모든 포트가 열려 있는지 확인해야 합니다.

연결 유형	포트	설명
콘솔 에이전트 <> 데이터 분류	8080(TCP), 443(TCP), 80. 9000	콘솔 에이전트의 방화벽 또는 라우팅 규칙은 포트 443을 통해 데이터 분류 인스턴스로의 인바운드 및 아웃바운드 트래픽을 허용해야 합니다. 콘솔에서 설치 진행 상황을 볼 수 있도록 포트 8080이 열려 있는지 확인하세요. Linux 호스트에서 방화벽을 사용하는 경우 Ubuntu 서버 내의 내부 프로세스에는 포트 9000이 필요합니다.
콘솔 에이전트 <> ONTAP 클러스터(NAS)	443(TCP)	콘솔은 HTTPS를 사용하여 ONTAP 클러스터를 검색합니다. 사용자 지정 방화벽 정책을 사용하는 경우 콘솔 에이전트 호스트는 포트 443을 통한 아웃바운드 HTTPS 액세스를 허용해야 합니다. 콘솔 에이전트가 클라우드에 있는 경우 모든 아웃바운드 통신은 사전 정의된 방화벽이나 라우팅 규칙에 따라 허용됩니다.

데이터 분류 필수 조건 스크립트 실행

데이터 분류 필수 조건 스크립트를 실행하려면 다음 단계를 따르세요.

"이 영상을 시청하세요"필수 구성 요소 스크립트를 실행하고 결과를 해석하는 방법을 알아보세요.

시작하기 전에

- Linux 시스템이 다음 사항을 충족하는지 확인하십시오.호스트 요구 사항 .
- 시스템에 두 가지 필수 소프트웨어 패키지(Docker Engine 또는 Podman, Python 3)가 설치되어 있는지 확인합니다.
- Linux 시스템에서 루트 권한이 있는지 확인하세요.

단계

1. 데이터 분류 전제 조건 스크립트를 다운로드하세요. "NetApp 지원 사이트" . 선택해야 하는 파일의 이름은 *standalone-pre-requisite-tester-<version>*입니다.
2. 사용하려는 Linux 호스트에 파일을 복사합니다(사용 `scp` 또는 다른 방법).
3. 스크립트를 실행할 수 있는 권한을 할당합니다.

```
chmod +x standalone-pre-requisite-tester-v1.25.0
```

4. 다음 명령을 사용하여 스크립트를 실행하세요.

```
./standalone-pre-requisite-tester-v1.25.0 <--darksite>
```

인터넷 접속이 불가능한 호스트에서 스크립트를 실행하는 경우에만 "--darksite" 옵션을 추가하세요. 호스트가

인터넷에 연결되어 있지 않으면 특정 필수 테스트가 건너뜁니다.

5. 스크립트는 데이터 분류 호스트 머신의 IP 주소를 입력하라는 메시지를 표시합니다.
   - IP 주소나 호스트 이름을 입력하세요.
6. 스크립트는 콘솔 에이전트가 설치되어 있는지 여부를 묻습니다.
   - 콘솔 에이전트가 설치되어 있지 않으면 *N*을 입력하세요.
   - 콘솔 에이전트가 설치되어 있는 경우 *Y*를 입력하세요. 그런 다음 테스트 스크립트가 이 연결성을 테스트할 수 있도록 콘솔 에이전트의 IP 주소나 호스트 이름을 입력합니다.
7. 스크립트는 시스템에서 다양한 테스트를 실행하고 진행 상황에 따라 결과를 표시합니다. 완료되면 세션 로그를 다음 이름의 파일에 기록합니다. `prerequisites-test-<timestamp>.log` 디렉토리에서 `/opt/netapp/install_logs` .

결과

모든 필수 테스트가 성공적으로 실행되었다면 준비가 되면 호스트에 데이터 분류를 설치할 수 있습니다.

문제가 발견되면 "권장" 또는 "필수"로 분류하여 수정합니다. 권장되는 문제는 일반적으로 데이터 분류 스캐닝 및 분류 작업의 실행 속도를 느리게 만드는 항목입니다. 이러한 항목은 수정할 필요가 없지만 해결하는 것이 좋습니다.

"필수" 문제가 있는 경우 문제를 해결하고 필수 구성 요소 테스트 스크립트를 다시 실행해야 합니다.