BlueXP 분류를 배포합니다

BlueXP classification

NetApp
April 03, 2024

This PDF was generated from https://docs.netapp.com/ko-kr/bluexp-classification/task-deploy-overview.html on April 03, 2024. Always check docs.netapp.com for the latest.

목차

BlueXP 분류를 배포합니다 1
어떤 BlueXP 분류 구축을 사용해야 합니까? 1
BlueXP를 사용하여 클라우드에 BlueXP 분류를 배포합니다 1
인터넷에 액세스할 수 있는 호스트에 BlueXP 분류를 설치합니다 11
인터넷에 액세스할 수 없는 Linux 호스트에 BlueXP 분류를 설치합니다 30
Linux 호스트가 BlueXP 분류를 설치할 준비가 되었는지 확인합니다 41

BlueXP 분류를 배포합니다

어떤 BlueXP 분류 구축을 사용해야 합니까?

BlueXP 분류를 다양한 방법으로 구축할 수 있습니다. 어떤 방법이 사용자의 요구를 충족시키는지 알아보십시오.

BlueXP 분류를 다음과 같은 방법으로 구축할 수 있습니다.

- "BlueXP를 사용하여 클라우드에 배포합니다". BlueXP는 BlueXP Connector와 동일한 클라우드 제공업체 네트워크에 BlueXP 분류 인스턴스를 배포합니다.
- "인터넷에 액세스할 수 있는 Linux 호스트에 설치합니다". 네트워크의 Linux 호스트 또는 인터넷에 액세스할 수 있는 클라우드의 Linux 호스트에 BlueXP 분류를 설치합니다. 사내에 있는 BlueXP 분류 인스턴스를 사용하여 온프레미스 ONTAP 시스템을 검사하려는 경우 이러한 설치 유형이 좋은 옵션이 될 수 있지만 반드시 필요한 것은 아닙니다.
- "인터넷 액세스 없이 온-프레미스 사이트에 Linux 호스트에 설치합니다"는 _private 모드라고도 합니다._설치 스크립트를 사용하는 이 유형의 설치는 보안 사이트에 적합합니다.

인터넷에 액세스할 수 있는 Linux 호스트에 설치하고 인터넷에 액세스할 수 없는 Linux 호스트에 온-프레미스 설치 모두 설치 스크립트를 사용합니다. 이 스크립트는 시스템과 환경이 사전 요구 사항을 충족하는지 확인하는 것으로 시작됩니다. 필수 구성 요소가 충족되면 설치가 시작됩니다. BlueXP 분류 설치를 실행하는 것과 별도로 필수 구성 요소를 확인하려면 필수 구성 요소에 대한 테스트만 다운로드할 수 있는 별도의 소프트웨어 패키지가 있습니다.

을 참조하십시오 "Linux 호스트가 BlueXP 분류를 설치할 준비가 되었는지 확인합니다".

BlueXP를 사용하여 클라우드에 BlueXP 분류를 배포합니다

클라우드에 BlueXP 분류를 배포하기 위한 몇 가지 단계를 완료합니다. BlueXP는 BlueXP Connector와 동일한 클라우드 제공업체 네트워크에 BlueXP 분류 인스턴스를 배포합니다.

참고: 또한 이 기능을 사용할 수 있습니다 "인터넷에 액세스할 수 있는 Linux 호스트에 BlueXP 분류를 설치합니다". 이 설치 유형은 사내에 위치한 BlueXP 분류 인스턴스를 사용하여 온프레미스 ONTAP 시스템을 스캔하려는 경우 좋은 옵션이 될 수 있지만 반드시 필요한 것은 아닙니다. 선택한 설치 방법에 관계없이 소프트웨어가 정확히 같은 방식으로 작동합니다.

빠른 시작

다음 단계를 따라 빠르게 시작하거나 나머지 섹션을 아래로 스크롤하여 자세한 내용을 확인하십시오.

1 커넥터를 작성합니다

아직 커넥터가 없으면 지금 연결선을 작성합니다. 을 참조하십시오 "AWS에서 커넥터 생성", "Azure에서 커넥터 만들기", 또는 "GCP에서 커넥터를 생성하는 중입니다".

또한 가능합니다 "Connector On-Premises를 설치합니다" 네트워크의 Linux 호스트 또는 클라우드의 Linux 호스트

2 사전 요구 사항을 검토합니다

환경이 필수 조건을 충족할 수 있는지 확인합니다. 여기에는 인스턴스에 대한 아웃바운드 인터넷 액세스, 포트 443을 통한 커넥터와 BlueXP 분류 간의 연결 등이 포함됩니다. 전체 목록을 참조하십시오.

3 **BlueXP** 분류를 배포합니다

설치 마법사를 시작하여 클라우드에 BlueXP 분류 인스턴스를 배포합니다.

4 **BlueXP** 분류 서비스에 가입합니다

BlueXP의 BlueXP 분류 검사에서 처음 1TB의 데이터는 30일 동안 무료로 제공됩니다. 해당 시점 이후에도 계속해서 데이터를 스캔하려면 클라우드 공급자 마켓플레이스 또는 NetApp의 BYOL 라이센스를 통한 BlueXP 구독이 필요합니다.

커넥터를 작성합니다

Connector가 없는 경우 클라우드 공급자에 Connector를 생성합니다. 을 참조하십시오 "AWS에서 커넥터 생성" 또는 "Azure에서 커넥터 만들기", 또는 "GCP에서 커넥터를 생성하는 중입니다". 대부분의 경우 대부분의 경우 BlueXP 분류를 활성화하기 전에 커넥터가 설정되어 있을 수 있습니다 "BlueXP 기능을 사용하려면 커넥터가 필요합니다"하지만 지금 설정해야 하는 경우도 있습니다.

특정 클라우드 공급자에 배포된 Connector를 사용해야 하는 몇 가지 시나리오가 있습니다.

- AWS의 Cloud Volumes ONTAP, ONTAP용 Amazon FSx 또는 AWS S3 버킷에서 데이터를 스캔할 때는 AWS의 커넥터를 사용합니다.
- Azure 또는 Azure NetApp Files의 Cloud Volumes ONTAP에서 데이터를 스캔할 때 Azure의 커넥터를 사용합니다.
  - Azure NetApp Files의 경우 스캔하려는 볼륨과 동일한 영역에 배포해야 합니다.
- GCP의 Cloud Volumes ONTAP에서 데이터를 스캔할 때 GCP의 커넥터를 사용합니다.

온프레미스 ONTAP 시스템, NetApp이 아닌 파일 공유, 일반 S3 오브젝트 스토리지, 데이터베이스, OneDrive 폴더, SharePoint 계정, Google Drive 계정은 이러한 클라우드 커넥터를 사용할 때 검색할 수 있습니다.

참고: 또한 이 기능을 사용할 수 있습니다 "Connector On-Premises를 설치합니다" 네트워크 또는 클라우드의 Linux 호스트 BlueXP 분류를 사내에서 설치하려는 일부 사용자는 Connector를 내부에 설치할 수도 있습니다.

보시다시피 을 사용해야 하는 몇 가지 상황이 있을 수 있습니다 "다중 커넥터".

정부 지역 지원

정부 지역(AWS GovCloud, Azure Gov 또는 Azure DoD)에 Connector를 구축한 경우 BlueXP 분류가 지원됩니다. 이러한 방식으로 배포된 BlueXP 분류에는 다음과 같은 제한 사항이 있습니다.

- OneDrive 계정, SharePoint 계정 및 Google Drive 계정을 검색할 수 없습니다.
- Microsoft Azure 정보 보호(AIP) 레이블 기능은 통합할 수 없습니다.

"정부 지역에서 커넥터 배포에 대한 자세한 내용은 을 참조하십시오".

사전 요구 사항을 검토합니다

클라우드에 BlueXP 분류를 배포하기 전에 다음 사전 요구 사항을 검토하여 지원되는 구성이 있는지 확인합니다. 클라우드에 BlueXP 분류를 배포할 때 Connector와 동일한 서브넷에 위치합니다.

BlueXP 분류에서 아웃바운드 인터넷 액세스를 활성화합니다

BlueXP 분류에는 아웃바운드 인터넷 액세스가 필요합니다. 가상 또는 물리적 네트워크에서 인터넷 액세스에 프록시 서버를 사용하는 경우 BlueXP 분류 인스턴스에 다음 엔드포인트에 연결할 수 있는 아웃바운드 인터넷 액세스 권한이 있는지 확인합니다. 프록시는 투명하지 않아야 합니다. 현재 투명 프록시를 지원하지 않습니다.

AWS, Azure 또는 GCP에서 BlueXP 분류를 배포하는지 여부에 따라 아래 적절한 표를 검토하십시오.

AWS에 필요한 엔드포인트

엔드포인트	목적
https://api.bluexp.netapp.com 으로 문의하십시오	NetApp 계정을 포함한 BlueXP 서비스와 통신합니다.
https://netapp-cloud-account.auth0.com https://auth0.com 으로 문의하십시오	BlueXP 웹 사이트와 통신하여 중앙 집중식 사용자 인증.
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 및 템플릿에 대한 액세스를 제공합니다.
https://kinesis.us-east-1.amazonaws.com 으로 문의하십시오	NetApp에서 감사 레코드의 데이터를 스트리밍할 수 있습니다.
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	BlueXP 분류를 통해 매니페스트와 템플릿을 액세스 및 다운로드하고 로그 및 메트릭을 전송할 수 있습니다.

Azure에 필요한 엔드포인입니다

엔드포인트	목적
https://api.bluexp.netapp.com 으로 문의하십시오	NetApp 계정을 포함한 BlueXP 서비스와 통신합니다.
https://netapp-cloud-account.auth0.com https://auth0.com 으로 문의하십시오	BlueXP 웹 사이트와 통신하여 중앙 집중식 사용자 인증.
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 액세스하고 로그 및 메트릭을 보낼 수 있습니다.
https://support.compliance.api.bluexp.netapp.com/ 으로 문의하십시오	NetApp에서 감사 레코드의 데이터를 스트리밍할 수 있습니다.

GCP에 필요한 엔드포인입니다

엔드포인트	목적
https://api.bluexp.netapp.com 으로 문의하십시오	NetApp 계정을 포함한 BlueXP 서비스와 통신합니다.
https://netapp-cloud-account.auth0.com https://auth0.com 으로 문의하십시오	BlueXP 웹 사이트와 통신하여 중앙 집중식 사용자 인증.

엔드포인트	목적
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 액세스하고 로그 및 메트릭을 보낼 수 있습니다.
https://support.compliance.api.bluexp.netapp.com/ 으로 문의하십시오	NetApp에서 감사 레코드의 데이터를 스트리밍할 수 있습니다.

BlueXP에 필요한 권한이 있는지 확인합니다

BlueXP에 리소스를 배포하고 BlueXP 분류 인스턴스에 대한 보안 그룹을 만들 수 있는 권한이 있는지 확인합니다. 최신 BlueXP 사용 권한은 에서 확인할 수 있습니다 "NetApp에서 제공하는 정책".

BlueXP 커넥터가 **BlueXP** 분류에 액세스할 수 있는지 확인합니다

Connector와 BlueXP 분류 인스턴스 간의 연결을 확인합니다. Connector의 보안 그룹은 포트 443을 통해 BlueXP 분류 인스턴스 간에 인바운드 및 아웃바운드 트래픽을 허용해야 합니다. 이 연결을 통해 BlueXP 분류 인스턴스를 배포할 수 있으며 규정 준수 및 거버넌스 탭에서 정보를 볼 수 있습니다. BlueXP 분류는 AWS 및 Azure의 정부 지역에서 지원됩니다.

AWS 및 AWS GovCloud 배포에는 추가 인바운드 및 아웃바운드 보안 그룹 규칙이 필요합니다. 을 참조하십시오 "AWS의 커넥터 규칙" 를 참조하십시오.

Azure 및 Azure Government 배포에는 추가 인바운드 및 아웃바운드 보안 그룹 규칙이 필요합니다. 을 참조하십시오 "Azure의 커넥터 규칙" 를 참조하십시오.

BlueXP 분류를 계속 실행할 수 있는지 확인합니다

데이터를 지속적으로 스캔하려면 BlueXP 분류 인스턴스를 계속 사용해야 합니다.

웹 브라우저가 **BlueXP** 분류에 연결되어 있는지 확인합니다

BlueXP 분류를 사용하도록 설정한 후에는 BlueXP 분류 인스턴스에 연결된 호스트에서 BlueXP 인터페이스에 액세스해야 합니다.

BlueXP 분류 인스턴스는 개인 IP 주소를 사용하여 인덱싱된 데이터에 인터넷에서 액세스할 수 없도록 합니다. 따라서 BlueXP에 액세스하는 데 사용하는 웹 브라우저가 해당 개인 IP 주소에 연결되어 있어야 합니다. 이러한 연결은 클라우드 공급자(예: VPN)에 직접 연결되거나 BlueXP 분류 인스턴스와 동일한 네트워크 내에 있는 호스트에서 발생할 수 있습니다.

vCPU 한도를 확인하십시오

클라우드 공급자의 vCPU 제한에 따라 필요한 수의 코어를 사용하여 인스턴스를 구축할 수 있는지 확인합니다. BlueXP가 실행 중인 지역의 관련 인스턴스 제품군에 대한 vCPU 제한을 확인해야 합니다. "필요한 인스턴스 유형을 참조하십시오".

vCPU 제한에 대한 자세한 내용은 다음 링크를 참조하십시오.

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

참고로, AWS 클라우드 환경에서는 CPU가 적고 RAM이 적은 인스턴스에 BlueXP 분류를 배포할 수 있지만 이러한 시스템을 사용할 때는 한계가 있습니다. 을 참조하십시오 "더 작은 인스턴스 유형 사용" 를 참조하십시오.

클라우드에 **BlueXP** 분류를 배포합니다

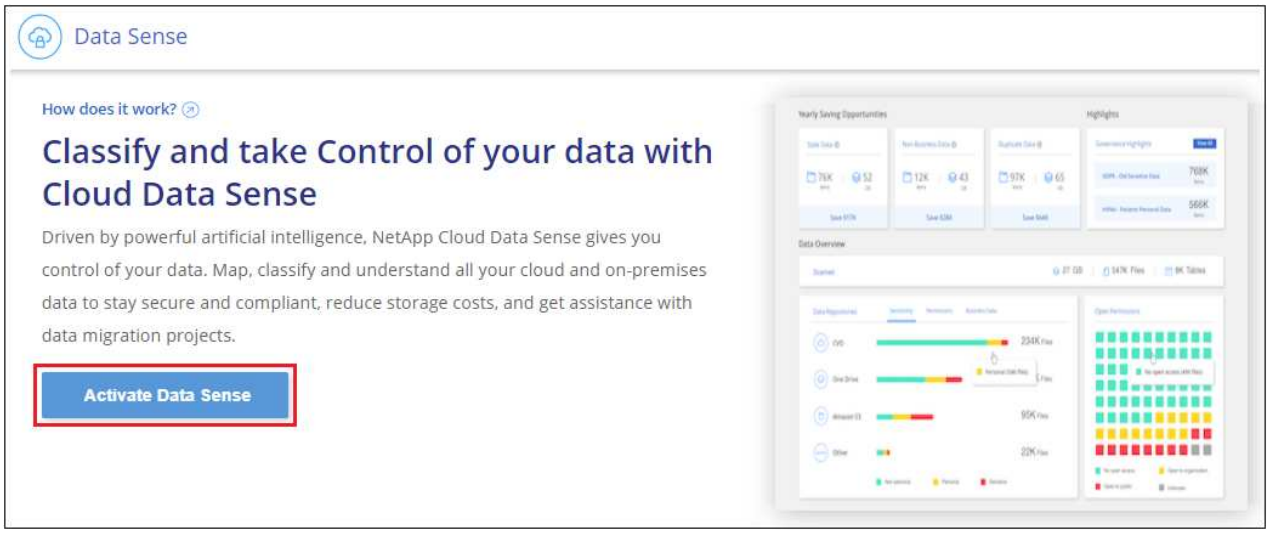
다음 단계에 따라 클라우드에 BlueXP 분류 인스턴스를 배포합니다. Connector는 클라우드에 인스턴스를 배포한 다음 해당 인스턴스에 BlueXP 분류 소프트웨어를 설치합니다.

AWS 환경의 BlueXP Connector에서 BlueXP 분류를 배포할 때 기본 인스턴스 크기를 선택하거나 두 개의 작은 인스턴스 유형 중에서 선택할 수 있습니다. "사용 가능한 인스턴스 유형 및 제한 사항을 참조하십시오". 기본 인스턴스 유형을 사용할 수 없는 지역에서는 BlueXP 분류가 에서 실행됩니다 "대체 인스턴스 유형".

AWS에 구축

단계

1. BlueXP 왼쪽 탐색 메뉴에서 * 거버넌스 > 분류 * 를 클릭합니다.



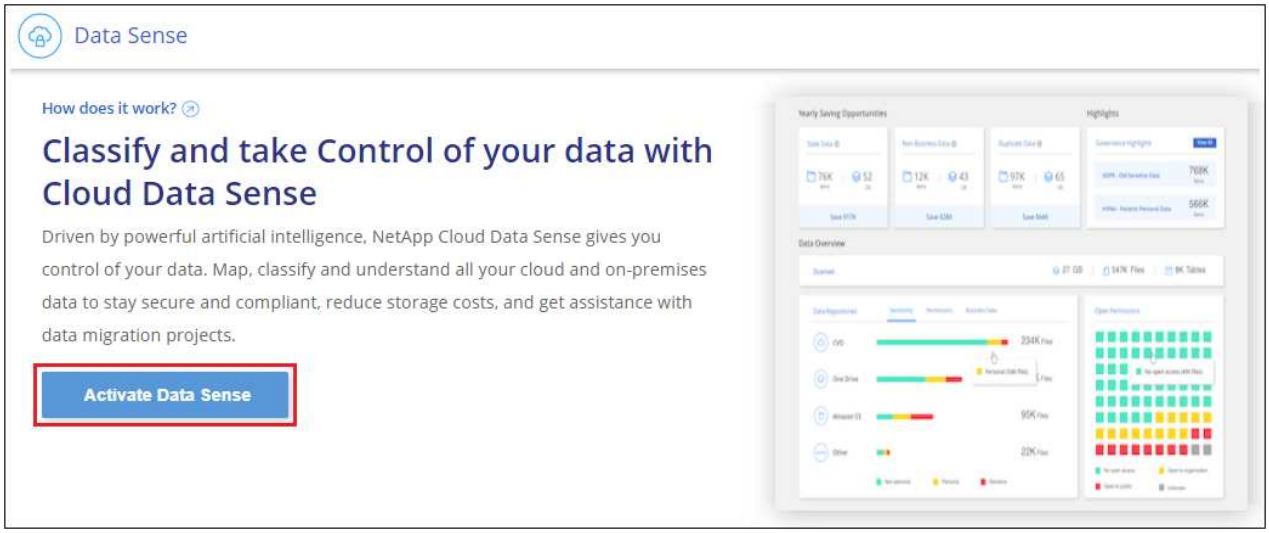
2. Activate Data Sense * 를 클릭합니다.
3. Installation_page에서 * deploy > deploy * 를 클릭하여 "큰" 인스턴스 크기를 사용하고 클라우드 배포 마법사를 시작합니다.
4. 구축 단계를 진행할 때 마법사가 진행률을 표시합니다. 문제가 발생하면 중지하고 입력을 묻는 메시지가 표시됩니다.

5. 인스턴스가 배포되고 BlueXP 분류가 설치되면 * 구성 계속 * 을 클릭하여 _Configuration_페이지로 이동합니다.

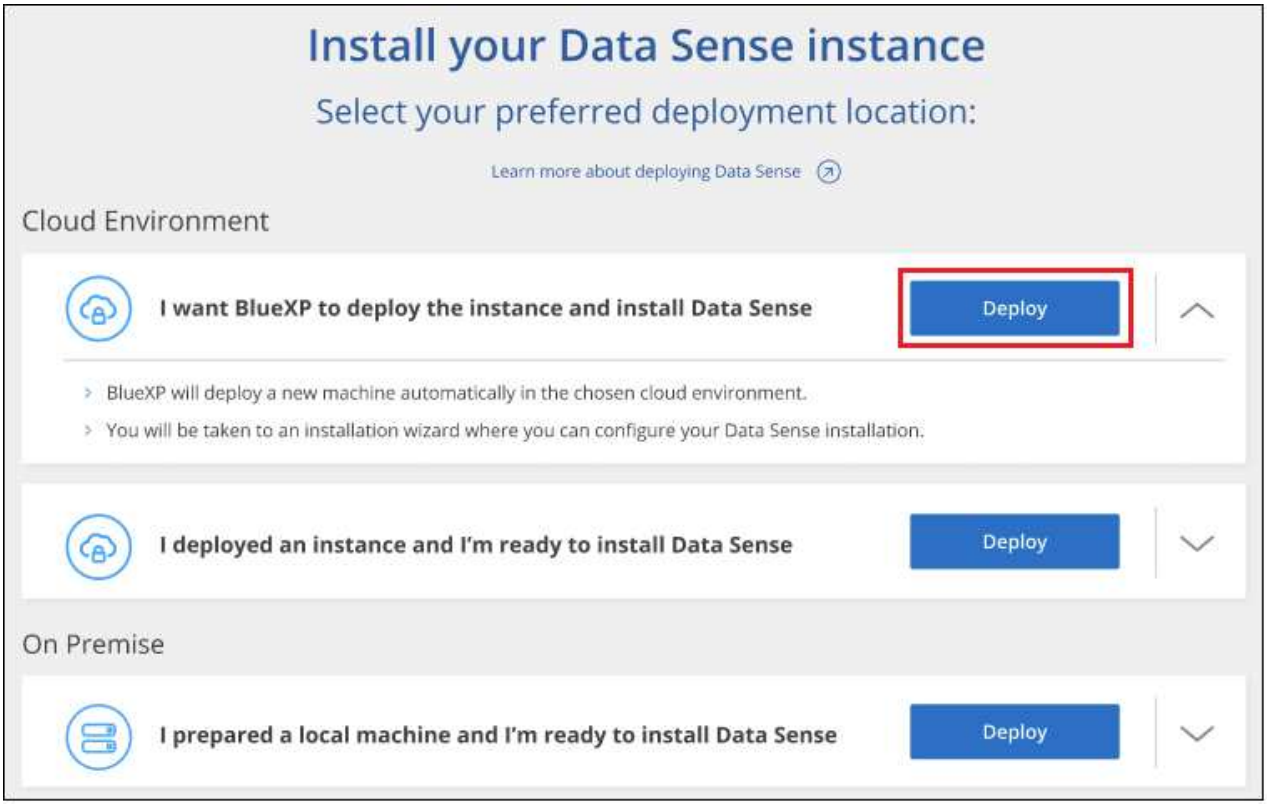
Azure에 구축

단계

1. BlueXP 왼쪽 탐색 메뉴에서 * 거버넌스 > 분류 * 를 클릭합니다.
2. Activate Data Sense * 를 클릭합니다.



3. 클라우드 배포 마법사를 시작하려면 * 배포 * 를 클릭합니다.



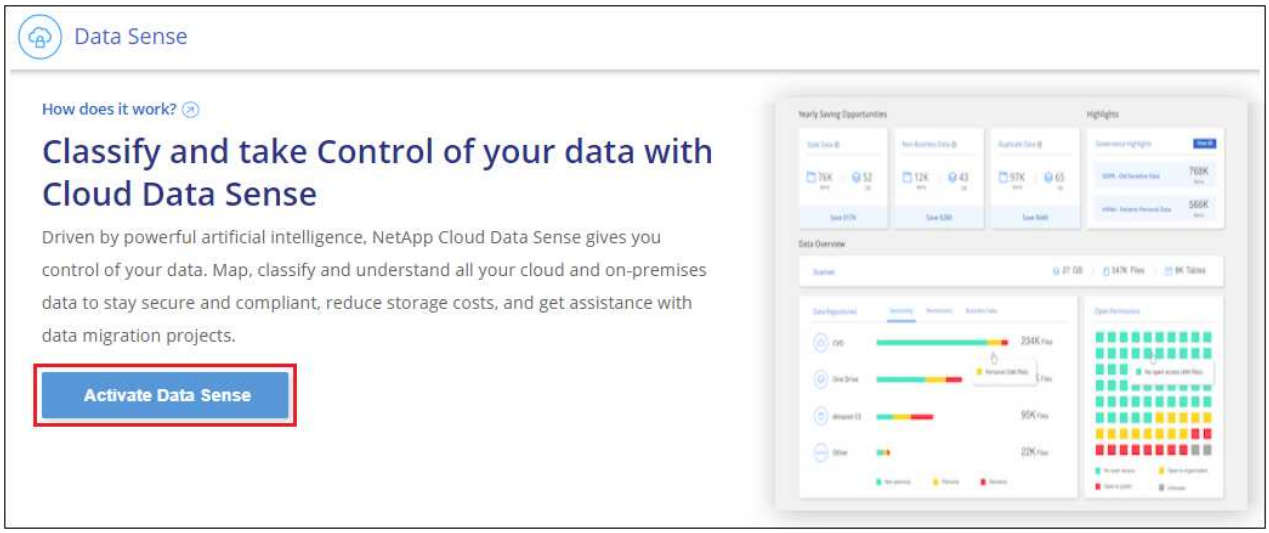
4. 구축 단계를 진행할 때 마법사가 진행률을 표시합니다. 문제가 발생하면 중지하고 입력을 묻는 메시지가 표시됩니다.

5. 인스턴스가 배포되고 BlueXP 분류가 설치되면 * 구성 계속 * 을 클릭하여 _Configuration_페이지로 이동합니다.

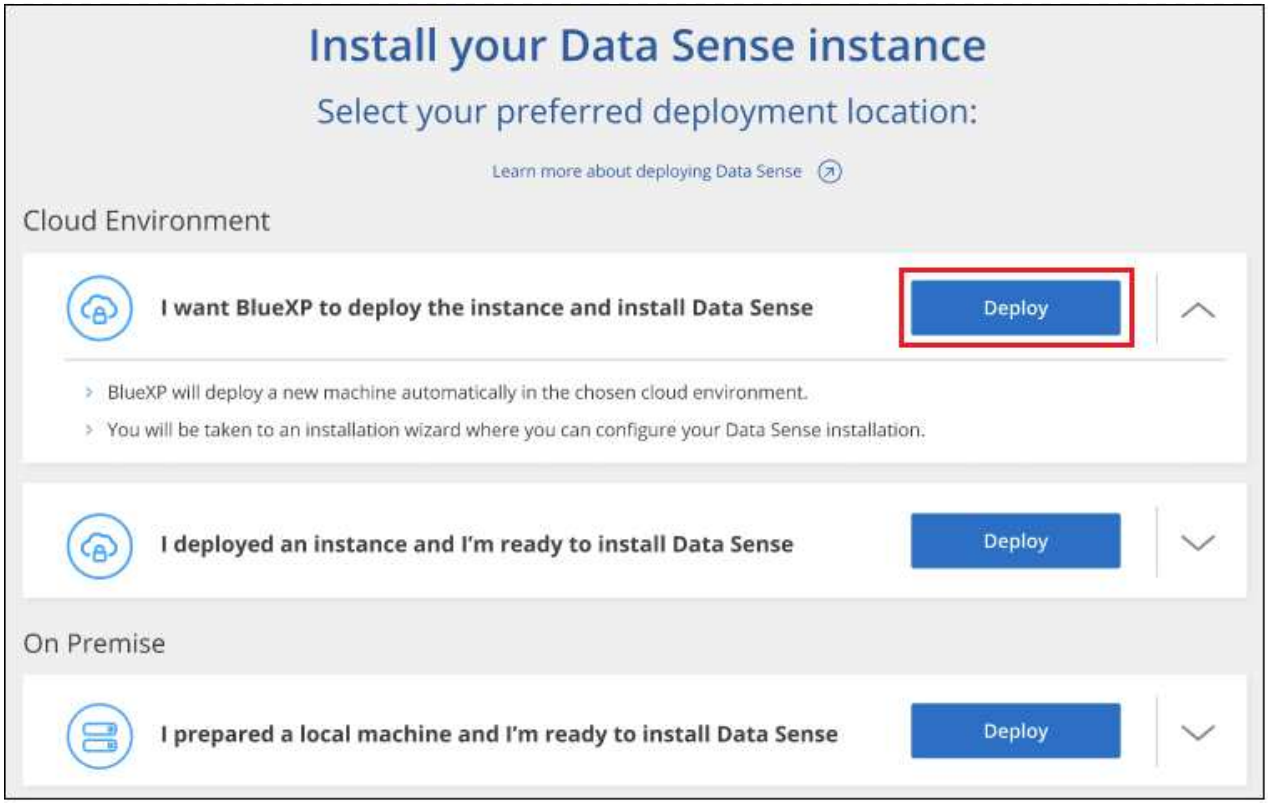
Google Cloud에 배포

단계

1. BlueXP 왼쪽 탐색 메뉴에서 * 거버넌스 > 분류 * 를 클릭합니다.
2. Activate Data Sense * 를 클릭합니다.



3. 클라우드 배포 마법사를 시작하려면 * 배포 * 를 클릭합니다.



4. 구축 단계를 진행할 때 마법사가 진행률을 표시합니다. 문제가 발생하면 중지하고 입력을 묻는 메시지가 표시됩니다.

5. 인스턴스가 배포되고 BlueXP 분류가 설치되면 * 구성 계속 * 을 클릭하여 _Configuration_페이지로 이동합니다.

결과

BlueXP는 클라우드 공급업체에 BlueXP 분류 인스턴스를 배포합니다.

인터넷 연결이 가능한 경우 BlueXP Connector 및 BlueXP 분류 소프트웨어에 대한 업그레이드가 자동화됩니다.

다음 단계

구성 페이지에서 스캔할 데이터 원본을 선택할 수 있습니다.

또한 가능합니다 "BlueXP 분류 라이선스를 설정합니다" 현재. 30일 무료 평가판이 종료될 때까지 요금이 부과되지 않습니다.

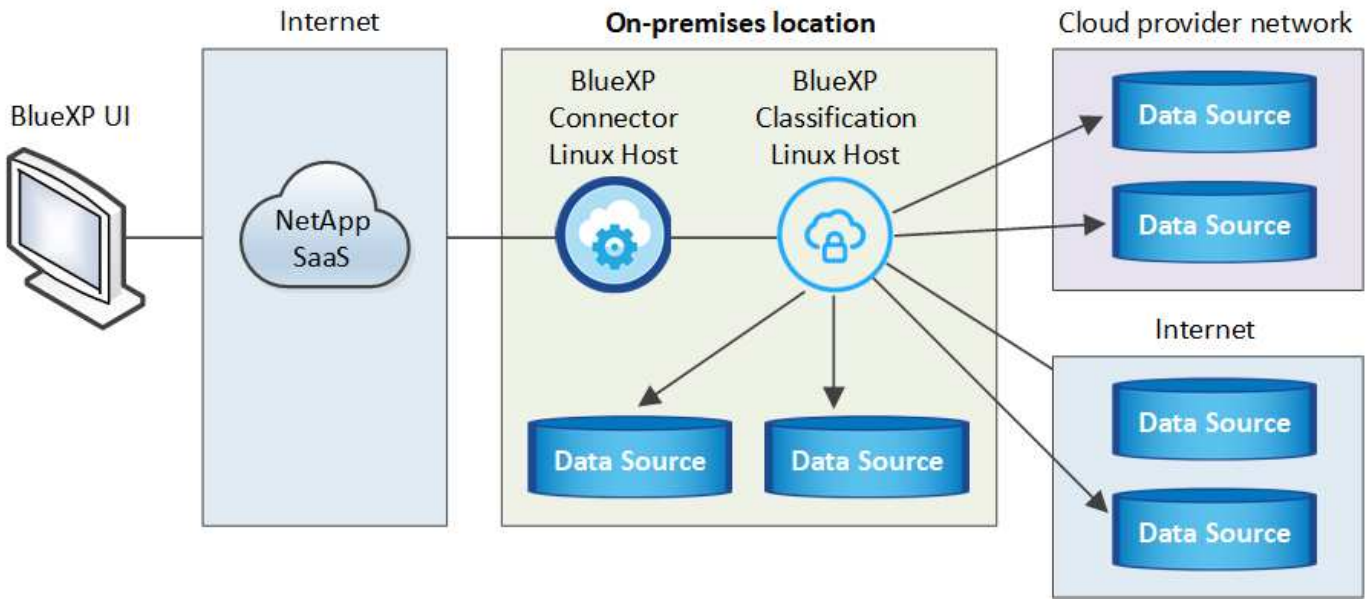
인터넷에 액세스할 수 있는 호스트에 BlueXP 분류를 설치합니다

네트워크의 Linux 호스트 또는 인터넷 액세스가 가능한 클라우드의 Linux 호스트에 BlueXP 분류를 설치하려면 몇 가지 단계를 완료하십시오. 이 설치의 일부로 네트워크 또는 클라우드에 Linux 호스트를 수동으로 배포해야 합니다.

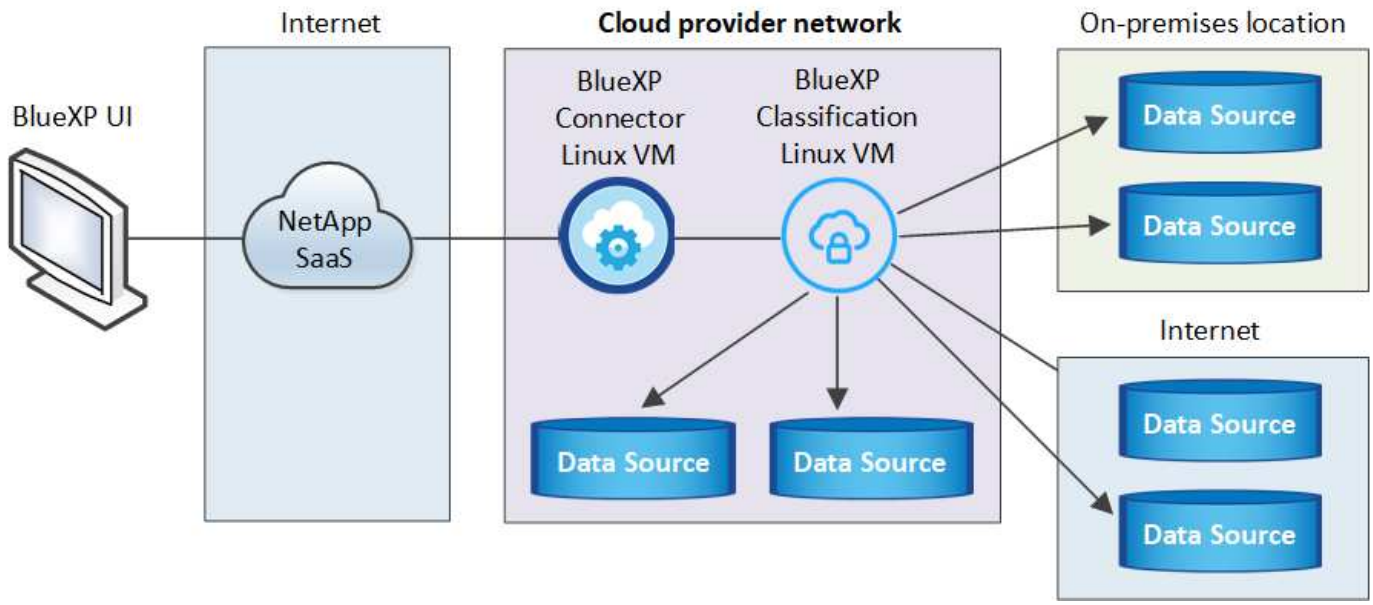
온프레미스에도 위치한 BlueXP 분류 인스턴스를 사용하여 온프레미스 ONTAP 시스템을 스캔하려는 경우 온프레미스 설치가 좋은 옵션이 될 수 있지만, 이는 필수 사항이 아닙니다. 선택한 설치 방법에 관계없이 소프트웨어가 정확히 같은 방식으로 작동합니다.

BlueXP 분류 설치 스크립트는 시스템 및 환경이 필수 전제 조건을 충족하는지 확인하는 것으로 시작됩니다. 필수 구성 요소가 모두 충족되면 설치가 시작됩니다. BlueXP 분류 설치를 실행하는 것과 별도로 필수 구성 요소를 확인하려면 필수 구성 요소에 대한 테스트만 다운로드할 수 있는 별도의 소프트웨어 패키지가 있습니다. "Linux 호스트가 BlueXP 분류를 설치할 준비가 되었는지 확인하는 방법을 참조하십시오".

Linux 호스트 _ 의 일반적인 설치 방법은 다음과 같습니다.



클라우드의 Linux 호스트에 _ 을(를) 설치하는 일반적인 구성 요소와 연결은 다음과 같습니다.



페타바이트 단위의 데이터를 스캐닝할 대규모 구성의 경우 여러 호스트를 포함하여 추가적인 처리 성능을 제공할 수 있습니다. 여러 호스트 시스템을 사용하는 경우 주 시스템을 _Manager node_라고 하며 추가 처리 능력을 제공하는 추가 시스템을 _Scanner nodes_라고 합니다.

참고: 또한 이 기능을 사용할 수 있습니다 "인터넷에 액세스할 수 없는 사내 사이트에 BlueXP 분류를 설치합니다" 완전히 안전한 사이트를 위한 것입니다.

빠른 시작

다음 단계를 따라 빠르게 시작하거나 나머지 섹션을 아래로 스크롤하여 자세한 내용을 확인하십시오.

1 커넥터를 작성합니다

커넥터가 없는 경우 "Connector를 온-프레미스에 배포합니다" 네트워크의 Linux 호스트 또는 클라우드의 Linux 호스트

또한 클라우드 공급자와 커넥터를 생성할 수도 있습니다. 을 참조하십시오 "AWS에서 커넥터 생성", "Azure에서 커넥터 만들기", 또는 "GCP에서 커넥터를 생성하는 중입니다".

2 사전 요구 사항을 검토합니다

환경이 필수 조건을 충족할 수 있는지 확인합니다. 여기에는 인스턴스에 대한 아웃바운드 인터넷 액세스, 포트 443을 통한 커넥터와 BlueXP 분류 간의 연결 등이 포함됩니다. 전체 목록을 참조하십시오.

또한 을 충족하는 Linux 시스템도 필요합니다 따르는 요구사항.

3 **BlueXP** 분류를 다운로드하고 배포합니다

NetApp Support 사이트에서 클라우드 BlueXP 분류 소프트웨어를 다운로드하고 사용할 Linux 호스트에 설치 프로그램 파일을 복사합니다. 그런 다음 설치 마법사를 시작하고 화면의 지시에 따라 BlueXP 분류 인스턴스를 배포합니다.

4 **BlueXP** 분류 서비스에 가입합니다

BlueXP의 BlueXP 분류 검사에서 처음 1TB의 데이터는 30일 동안 무료로 제공됩니다. 해당 시점 이후에도 데이터를 계속 스캔하려면 클라우드 공급자 마켓플레이스 또는 NetApp의 BYOL 라이센스를 구입해야 합니다.

커넥터를 작성합니다

BlueXP 분류를 설치하고 사용하려면 먼저 BlueXP 커넥터가 필요합니다. 대부분의 경우 대부분의 경우 BlueXP 분류를 활성화하기 전에 커넥터가 설정되어 있을 수 있습니다 "BlueXP 기능을 사용하려면 커넥터가 필요합니다"하지만 지금 설정해야 하는 경우도 있습니다.

클라우드 공급자 환경에 하나를 생성하려면 를 참조하십시오 "AWS에서 커넥터 생성", "Azure에서 커넥터 만들기", 또는 "GCP에서 커넥터를 생성하는 중입니다".

특정 클라우드 공급자에 배포된 Connector를 사용해야 하는 몇 가지 시나리오가 있습니다.

- AWS의 Cloud Volumes ONTAP, ONTAP용 Amazon FSx 또는 AWS S3 버킷에서 데이터를 스캔할 때는 AWS의 커넥터를 사용합니다.
- Azure 또는 Azure NetApp Files의 Cloud Volumes ONTAP에서 데이터를 스캔할 때 Azure의 커넥터를 사용합니다.

  Azure NetApp Files의 경우 스캔하려는 볼륨과 동일한 영역에 배포해야 합니다.

- GCP의 Cloud Volumes ONTAP에서 데이터를 스캔할 때 GCP의 커넥터를 사용합니다.

온프레미스 ONTAP 시스템, NetApp이 아닌 파일 공유, 일반 S3 오브젝트 스토리지, 데이터베이스, OneDrive 폴더, SharePoint 계정, Google Drive 계정은 이러한 클라우드 커넥터를 사용하여 스캔할 수 있습니다.

참고: 또한 이 기능을 사용할 수 있습니다 "Connector를 온-프레미스에 배포합니다" 네트워크의 Linux 호스트 또는 클라우드의 Linux 호스트 BlueXP 분류를 사내에서 설치하려는 일부 사용자는 Connector를 내부에 설치할 수도 있습니다.

보시다시피 을 사용해야 하는 몇 가지 상황이 있을 수 있습니다 "다중 커넥터".

BlueXP 분류를 설치할 때 커넥터 시스템의 IP 주소 또는 호스트 이름이 필요합니다. 이 정보는 구내에 Connector를 설치한 경우 확인할 수 있습니다. Connector가 클라우드에 배포된 경우 BlueXP 콘솔에서 이 정보를 찾을 수 있습니다. 도움말 아이콘을 클릭하고 * 지원 * 을 선택한 다음 * BlueXP 커넥터 * 를 클릭합니다.

Linux 호스트 시스템을 준비합니다

BlueXP 분류 소프트웨어는 특정 운영 체제 요구 사항, RAM 요구 사항, 소프트웨어 요구 사항 등을 충족하는 호스트에서 실행해야 합니다. Linux 호스트는 네트워크 또는 클라우드에 있을 수 있습니다.

BlueXP 분류를 계속 실행할 수 있는지 확인합니다. 데이터를 지속적으로 스캔하려면 BlueXP 분류 장비가 켜져 있어야 합니다.

- BlueXP 분류는 다른 애플리케이션과 공유되는 호스트에서는 지원되지 않습니다. 호스트는 전용 호스트여야 합니다.
- 구내 호스트 시스템을 구축할 때 BlueXP 분류 검사를 수행할 데이터 세트의 크기에 따라 세 가지 시스템 크기 중에서 선택할 수 있습니다.

시스템 크기	**CPU**	**RAM(**스왑 메모리는 비활성화 상태여야 함**)**	디스크
* 초대형 *	32개의 CPU	128GB RAM	/, 또는 의 1TiB SSD /opt에서 -100GiB를 사용할 수 있습니다 -895GiB는 /var/lib/docker에서 사용할 수 있습니다 /tmp에 -5GiB입니다
* 대형 *	CPU 16개	64GB RAM	500GiB SSD 켜짐/또는 /opt에서 -100GiB를 사용할 수 있습니다 /var/lib/docker에서 사용 가능한 395GiB /tmp에 -5GiB입니다
* 중간 *	CPU 8개	32GB RAM	200GiB SSD 켜짐/또는 /opt에서 -50GiB를 사용할 수 있습니다 /var/lib/docker에서 -145GiB를 사용할 수 있습니다 /tmp에 -5GiB입니다
* 소형 *	CPU 8개	16GB RAM	또는 에서 100GiB SSD /opt에서 -50GiB를 사용할 수 있습니다 /var/lib/docker에서 -45GiB를 사용할 수 있습니다 /tmp에 -5GiB입니다

소형 시스템을 사용할 때는 제한이 있습니다. 을 참조하십시오 "더 작은 인스턴스 유형 사용" 를 참조하십시오.

- BlueXP 분류 설치를 위해 클라우드에 컴퓨팅 인스턴스를 배포할 때는 위의 "대규모" 시스템 요구 사항을 충족하는 시스템을 권장합니다.
  - * AWS EC2 인스턴스 유형 *: "m6i.4xLarge"를 권장합니다. "추가 AWS 인스턴스 유형을 참조하십시오".
  - * Azure VM size *: "Standard_D16s_v3"을 권장합니다. "추가 Azure 인스턴스 유형을 참조하십시오".
  - * GCP 시스템 유형 *: "n2-standard-16"을 권장합니다. "추가 GCP 인스턴스 유형을 참조하십시오".
- UNIX 폴더 권한 *: 다음과 같은 최소 UNIX 권한이 필요합니다.

폴더	최소 권한
/tmp	`rwxrwxrwt`
/opt	`rwxr-xr-x`
/var/lib/docker입니다	`rwx------`
/usr/lib/systemd/system입니다	`rwxr-xr-x`

- * 운영 체제 *:
  - 다음 운영 체제에서는 Docker 컨테이너 엔진을 사용해야 합니다.
    - Red Hat Enterprise Linux 버전 7.8 및 7.9

        - CentOS 버전 7.8 및 7.9
        - Ubuntu 22.04(BlueXP 분류 버전 1.23 이상 필요)
    - 다음 운영 체제에는 Podman 컨테이너 엔진을 사용해야 하며 BlueXP 분류 버전 1.30 이상이 필요합니다.
        - Red Hat Enterprise Linux 버전 8.8, 9.0, 9.1, 9.2 및 9.3

          RHEL 8.x 및 RHEL 9.x를 사용하는 경우 다음 기능은 현재 지원되지 않습니다.

            - 어두운 장소에 설치
            - 분산 스캔, 마스터 스캐너 노드 및 원격 스캐너 노드 사용
- * Red Hat 서브스크립션 관리 *: 호스트는 Red Hat 서브스크립션 관리 에 등록되어 있어야 합니다. 등록되지 않은 경우 설치 중에 시스템에서 필요한 타사 소프트웨어를 업데이트하기 위해 리포지토리에 액세스할 수 없습니다.
- * 추가 소프트웨어 *: BlueXP 분류를 설치하기 전에 호스트에 다음 소프트웨어를 설치해야 합니다.
    - 사용 중인 OS에 따라 컨테이너 엔진 중 하나를 설치해야 합니다.
        - Docker Engine 버전 19.3.1 이상 "설치 지침을 봅니다".

          "이 비디오 시청" CentOS에 Docker를 설치하는 빠른 데모를 보려면

        - Podman 버전 4 이상 Podman을 설치하려면 시스템 패키지를 업데이트하십시오 (`sudo yum update -y`)를 클릭한 다음 Podman을 설치합니다 (`sudo yum install netavark -y`)를 클릭합니다.
- Python 버전 3.6 이상. "설치 지침을 봅니다".
    - * NTP 고려 사항 *: NetApp에서는 NTP(네트워크 시간 프로토콜) 서비스를 사용하도록 BlueXP 분류 시스템을 구성할 것을 권장합니다. BlueXP 분류 시스템과 BlueXP Connector 시스템 간에 시간을 동기화해야 합니다.
    - * Firewalld 고려 사항 *: 사용하려는 경우 `firewalld`BlueXP 분류를 설치하기 전에 활성화하는 것이 좋습니다. 다음 명령을 실행하여 구성합니다 `firewalld` 따라서 BlueXP 분류와 호환됩니다.

      ```
      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 BlueXP 분류 호스트를 스캐너 노드로 사용할 계획이라면 이 규칙을 주 시스템에 추가하십시오.

    ```
    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 활성화 또는 업데이트할 때마다 다시 시작해야 합니다 `firewalld` 설정.

설치 후 BlueXP 분류 호스트 시스템의 IP 주소를 변경할 수 없습니다.

BlueXP 분류에서 아웃바운드 인터넷 액세스를 활성화합니다

BlueXP 분류에는 아웃바운드 인터넷 액세스가 필요합니다. 가상 또는 물리적 네트워크에서 인터넷 액세스에 프록시 서버를 사용하는 경우 BlueXP 분류 인스턴스에 다음 엔드포인트에 연결할 수 있는 아웃바운드 인터넷 액세스 권한이 있는지 확인합니다.

엔드포인트	목적
https://api.bluexp.netapp.com 으로 문의하십시오	NetApp 계정을 포함한 BlueXP 서비스와 통신합니다.
https://netapp-cloud-account.auth0.com https://auth0.com 으로 문의하십시오	BlueXP 웹 사이트와 통신하여 중앙 집중식 사용자 인증.
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 액세스하고 로그 및 메트릭을 보낼 수 있습니다.
https://support.compliance.api.bluexp.netapp.com/ 으로 문의하십시오	NetApp에서 감사 레코드의 데이터를 스트리밍할 수 있습니다.
https://github.com/docker https://download.docker.com 으로 문의하십시오	Docker 설치를 위한 사전 필수 패키지를 제공합니다.
http://mirror.centos.org http://mirrorlist.centos.org http://mirror.centos.org/centos/7/extras/x86_64/Packages/container-selinux-2.107-3.el7.noarch.rpm 를 참조하십시오	CentOS 설치를 위한 필수 패키지를 제공합니다.
http://packages.ubuntu.com/ http://archive.ubuntu.com	Ubuntu 설치를 위한 필수 패키지를 제공합니다.

필요한 모든 포트가 활성화되어 있는지 확인합니다

커넥터, BlueXP 분류, Active Directory 및 데이터 소스 간의 통신에 필요한 모든 포트가 열려 있는지 확인해야 합니다.

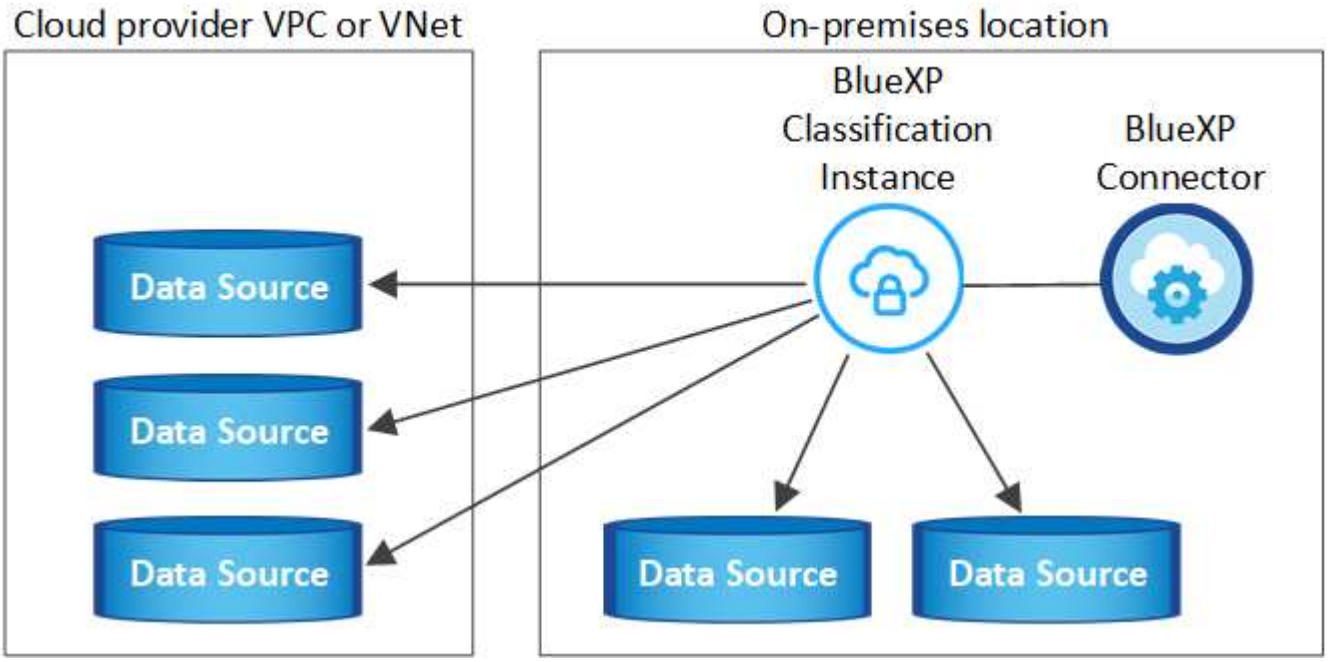
연결 유형	포트	설명
커넥터 <>BlueXP 분류	8080(TCP), 443(TCP) 및 80	Connector의 방화벽 또는 라우팅 규칙은 포트 443을 통해 BlueXP 분류 인스턴스 간에 인바운드 및 아웃바운드 트래픽을 허용해야 합니다. 포트 8080이 열려 있는지 확인하여 BlueXP에서 설치 진행률을 확인합니다.

연결 유형	포트	설명
커넥터 <>ONTAP 클러스터(NAS)	443(TCP)	BlueXP는 HTTPS를 사용하여 ONTAP 클러스터를 검색합니다. 사용자 지정 방화벽 정책을 사용하는 경우 다음 요구 사항을 충족해야 합니다. • 커넥터 호스트는 포트 443을 통한 아웃바운드 HTTPS 액세스를 허용해야 합니다. Connector가 클라우드에 있는 경우 모든 아웃바운드 통신은 사전 정의된 방화벽 또는 라우팅 규칙으로 허용됩니다. • ONTAP 클러스터는 포트 443을 통한 인바운드 HTTPS 액세스를 허용해야 합니다. 기본 "관리" 방화벽 정책은 모든 IP 주소에서 인바운드 HTTPS 액세스를 허용합니다. 이 기본 정책을 수정하거나 자체 방화벽 정책을 만든 경우 HTTPS 프로토콜을 해당 정책에 연결하고 Connector 호스트에서 액세스를 활성화해야 합니다.
BlueXP 분류<>ONTAP 클러스터	• NFS-111(TCP\UDP) 및 2049(TCP\UDP)의 경우 • CIFS-139(TCP\UDP) 및 445(TCP\UDP)의 경우	BlueXP 분류에는 각 Cloud Volumes ONTAP 서브넷 또는 온프레미스 ONTAP 시스템에 대한 네트워크 연결이 필요합니다. Cloud Volumes ONTAP의 방화벽 또는 라우팅 규칙은 BlueXP 분류 인스턴스에서 인바운드 연결을 허용해야 합니다. 이러한 포트가 BlueXP 분류 인스턴스에 열려 있는지 확인합니다. • NFS-111 및 2049용 • CIFS-139 및 445의 경우 NFS 볼륨 내보내기 정책은 BlueXP 분류 인스턴스에서 액세스를 허용해야 합니다.
BlueXP 분류<>Active Directory	389(TCP 및 UDP), 636(TCP), 3268(TCP) 및 3269(TCP)	회사의 사용자에 대해 Active Directory가 이미 설정되어 있어야 합니다. 또한 BlueXP 분류에는 CIFS 볼륨을 스캔하기 위해 Active Directory 자격 증명이 필요합니다. Active Directory에 대한 정보가 있어야 합니다. • DNS 서버 IP 주소 또는 여러 IP 주소 • 서버의 사용자 이름 및 암호 • 도메인 이름(Active Directory 이름) • 보안 LDAP(LDAPS) 사용 여부 • LDAP 서버 포트(일반적으로 LDAP의 경우 389, 보안 LDAP의 경우 636)

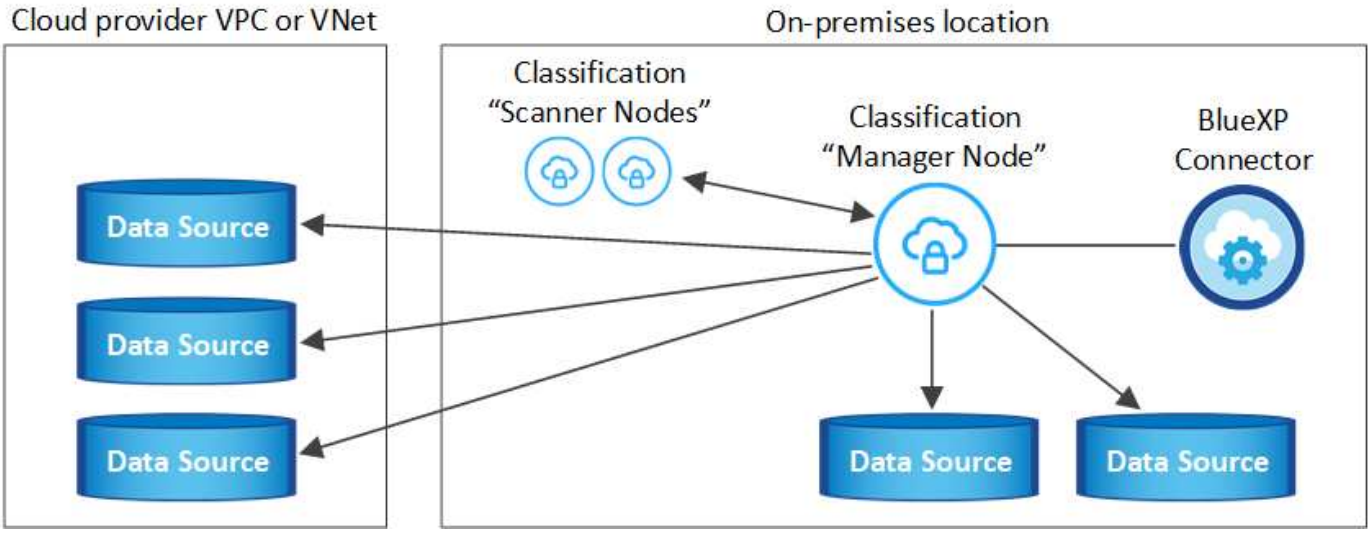
여러 BlueXP 분류 호스트를 사용하여 데이터 소스를 검사하는 추가 처리 기능을 제공하는 경우 추가 포트/프로토콜을 활성화해야 합니다. "추가 포트 요구 사항을 참조하십시오".

Linux 호스트에 BlueXP 분류를 설치합니다

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



페타바이트 단위의 데이터를 스캐닝할 대규모 구성의 경우 여러 호스트를 포함하여 추가적인 처리 성능을 제공할 수 있습니다. 여기에서 해당 단계를 확인하십시오.



을 참조하십시오 Linux 호스트 시스템 준비 및 사전 요구 사항 검토 BlueXP 분류를 배포하기 전에 필요한 전체 목록을 확인하십시오.

인스턴스가 인터넷에 연결되어 있는 경우 BlueXP 분류 소프트웨어로의 업그레이드가 자동화됩니다.

> BlueXP 분류는 소프트웨어가 사내에 설치된 경우 현재 ONTAP용 S3 버킷, Azure NetApp Files 또는 FSx를 스캔할 수 없습니다. 이러한 경우 클라우드 및 에 별도의 Connector 및 BlueXP 분류 인스턴스를 배포해야 합니다 "커넥터 사이를 전환합니다" 다양한 데이터 소스에 대해

일반 구성을 위한 단일 호스트 설치

단일 온-프레미스 호스트에 BlueXP 분류 소프트웨어를 설치할 때 요구 사항을 검토하고 다음 단계를 따르십시오.

"이 비디오 시청" BlueXP 분류 설치 방법을 확인합니다.

모든 설치 작업은 BlueXP 분류를 설치할 때 기록됩니다. 설치 중에 문제가 발생하면 설치 감사 로그의 내용을 볼 수 있습니다. 에 기록됩니다 `/opt/netapp/install_logs/`. "자세한 내용은 여기에서 확인하십시오.".

필요한 것

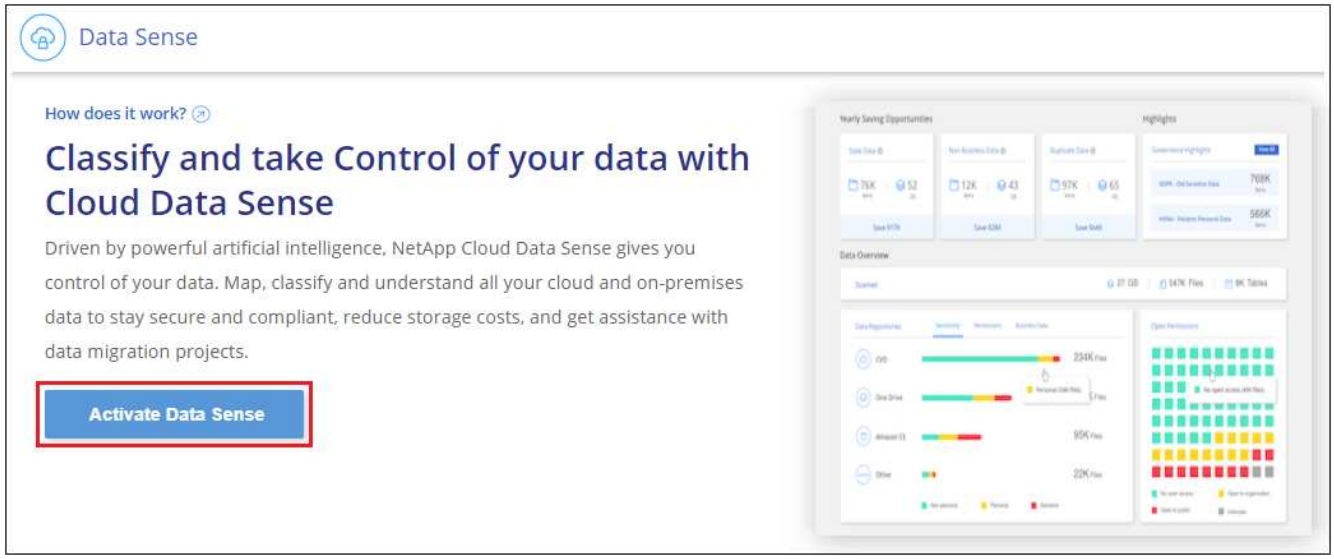
- Linux 시스템이 를 충족하는지 확인합니다 호스트 요구 사항.
- 시스템에 2개의 필수 소프트웨어 패키지(Docker Engine 또는 Podman 및 Python 3)가 설치되어 있는지 확인합니다.
- Linux 시스템에 대한 루트 권한이 있는지 확인합니다.
- 인터넷 액세스에 프록시를 사용하는 경우:
  - 프록시 서버 정보(IP 주소 또는 호스트 이름, 연결 포트, 연결 스키마: https 또는 http, 사용자 이름 및 암호)가 필요합니다.
  - 프록시가 TLS 가로채기를 수행하는 경우 TLS CA 인증서가 저장된 BlueXP 분류 Linux 시스템의 경로를 알아야 합니다.
  - 프록시는 투명하지 않아야 합니다. 현재 투명 프록시를 지원하지 않습니다.
  - 사용자는 로컬 사용자여야 합니다. 도메인 사용자는 지원되지 않습니다.
- 오프라인 환경이 필요한 를 충족하는지 확인합니다 사용 권한 및 연결.

단계

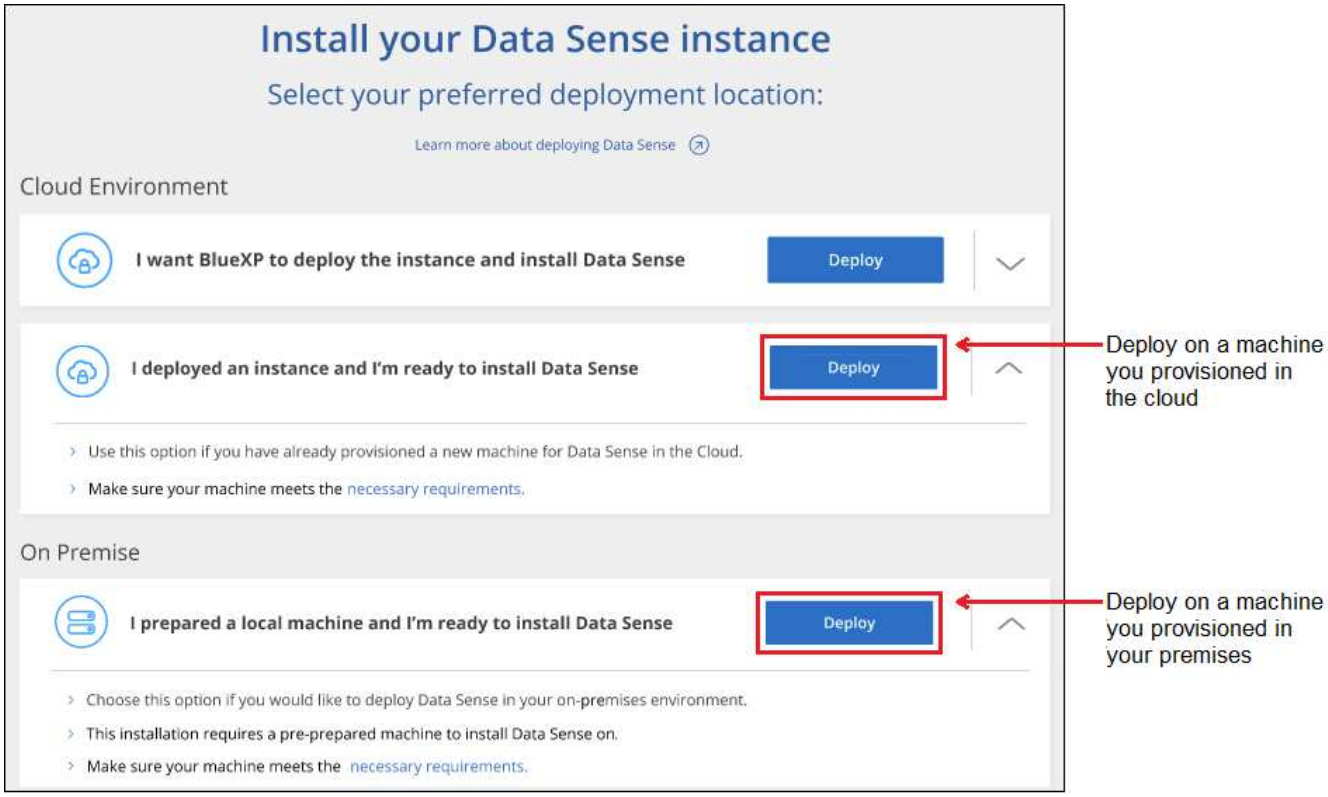
1. 에서 BlueXP 분류 소프트웨어를 다운로드합니다 "NetApp Support 사이트". 선택해야 하는 파일의 이름은 * DATASENSE-INinstaller-<version>.tar.gz * 입니다.
2. 설치 프로그램 파일을 사용하려는 Linux 호스트에 복사합니다(scp 또는 다른 방법 사용).
3. 호스트 시스템에서 설치 프로그램 파일의 압축을 풉니다. 예를 들면 다음과 같습니다.

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

4. BlueXP에서 * 거버넌스 > 분류 * 를 선택합니다.
5. Activate Data Sense * 를 클릭합니다.



6. 클라우드에서 준비한 인스턴스 또는 사내에서 준비한 인스턴스에 BlueXP 분류를 설치할 것인지 여부에 따라 해당 * deploy * 버튼을 클릭하여 BlueXP 분류 설치를 시작합니다.



7. Deploy Data Sense on Premises_대화 상자가 표시됩니다. 제공된 명령을 복사합니다(예: `sudo ./install.sh -a 12345 -c 27AG75 -t 2198qq`)를 사용하여 텍스트 파일에 붙여 넣어 나중에 사용할 수 있습니다. 그런 다음 * 닫기 * 를 클릭하여 대화 상자를 닫습니다.

8. 호스트 시스템에서 복사한 명령을 입력한 다음 일련의 프롬프트를 따르거나 필요한 모든 매개 변수를 명령줄 인수로 포함하여 전체 명령을 제공할 수 있습니다.

   설치 프로그램은 사전 검사를 수행하여 시스템 및 네트워킹 요구 사항이 제대로 설치되어 있는지 확인합니다. "이 비디오 시청" 사전 점검 메시지 및 의미를 이해합니다.

프롬프트가 나타나면 매개 변수를 입력합니다.	전체 명령 입력:
a. 7단계에서 복사한 명령을 붙여 넣습니다. `sudo ./install.sh -a <account_id> -c <client_id> -t <user_token>` 구내에 설치하지 않고 클라우드 인스턴스에 설치하는 경우 를 추가합니다 `--manual-cloud -install <cloud_provider>`. b. BlueXP 분류 호스트 시스템의 IP 주소 또는 호스트 이름을 입력하여 Connector 시스템에서 액세스할 수 있도록 합니다. c. BlueXP 커넥터 호스트 시스템의 IP 주소 또는 호스트 이름을 입력하여 BlueXP 분류 시스템에서 액세스할 수 있습니다. d. 메시지가 나타나면 프록시 세부 정보를 입력합니다. BlueXP Connector가 이미 프록시를 사용하고 있는 경우 BlueXP 분류가 자동으로 Connector에서 사용하는 프록시를 사용하기 때문에 이 정보를 다시 입력할 필요가 없습니다.	또는 필요한 호스트 및 프록시 매개 변수를 제공하여 전체 명령을 미리 생성할 수도 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 ID입니다
- *client_id*=커넥터 클라이언트 ID(클라이언트 ID에 접미어 "clients"가 없으면 추가)
- *USER_TOKEN*= JWT 사용자 액세스 토큰
- *DS_HOST*= BlueXP 분류 Linux 시스템의 IP 주소 또는 호스트 이름입니다.
- *cm_host*= BlueXP 커넥터 시스템의 IP 주소 또는 호스트 이름입니다.
- *cloud_provider*= 클라우드 인스턴스에 설치할 때 클라우드 공급자에 따라 "AWS", "Azure" 또는 "GCP"를 입력하십시오.
- *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 체계: https 또는 http(기본값 http).
- *proxy_user*= 기본 인증이 필요한 경우 프록시 서버에 연결할 인증된 사용자입니다. 사용자는 로컬 사용자여야 합니다. - 도메인 사용자는 지원되지 않습니다.
- *proxy_password*=지정한 사용자 이름의 암호입니다.
- *ca_cert_dir*=추가 TLS CA 인증서 번들을 포함하는 BlueXP 분류 Linux 시스템의 경로입니다. 프록시가 TLS 가로채기를 수행하는 경우에만 필요합니다.

결과

BlueXP 분류 설치 프로그램은 패키지를 설치하고, 설치를 등록하고, BlueXP 분류를 설치합니다. 설치는 10분에서 20분 정도 걸릴 수 있습니다.

호스트 시스템과 커넥터 인스턴스 간에 포트 8080을 통해 연결되어 있는 경우 BlueXP의 BlueXP 분류 탭에서 설치

진행 상황을 확인할 수 있습니다.

다음 단계

구성 페이지에서 스캔할 데이터 원본을 선택할 수 있습니다.

또한 가능합니다 "BlueXP 분류 라이선스를 설정합니다" 현재. 30일 무료 평가판이 종료될 때까지 요금이 부과되지 않습니다.

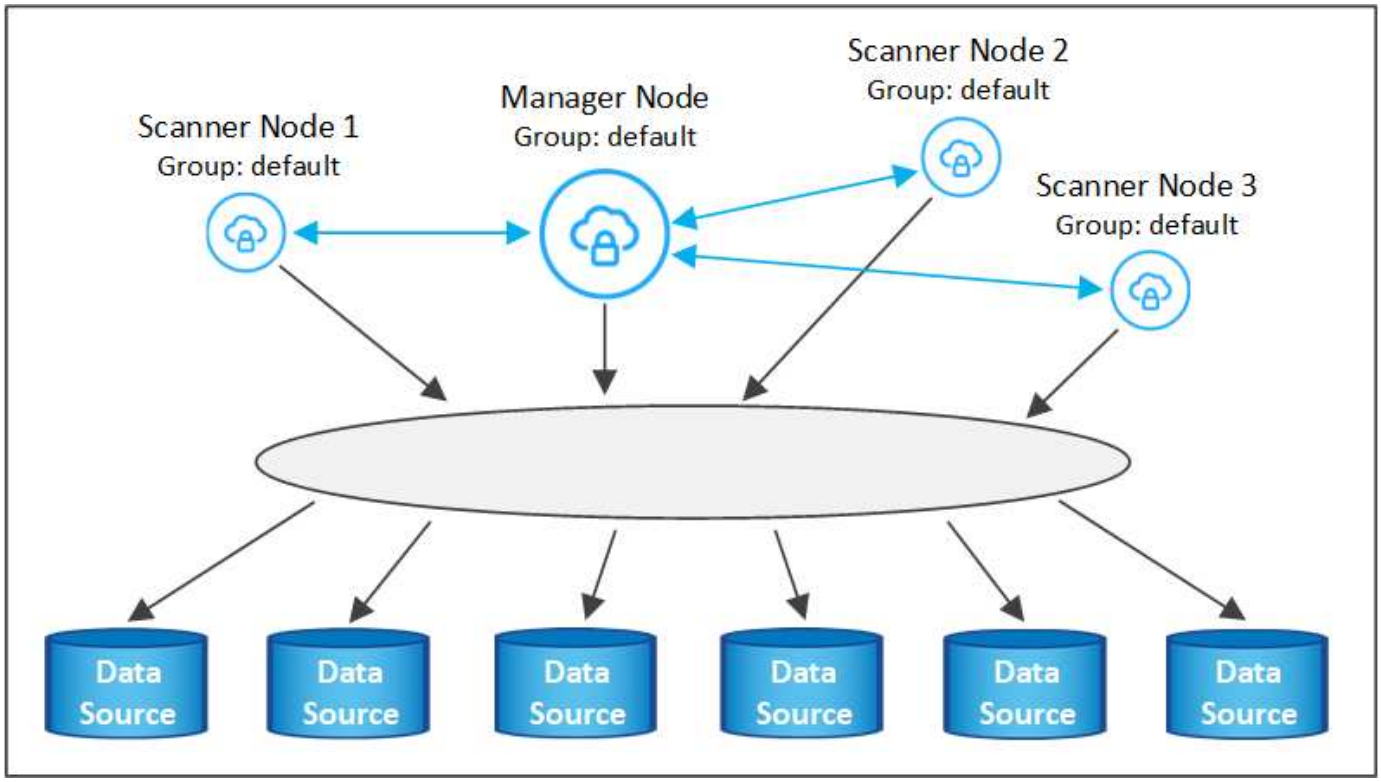
기존 배포에 스캐너 노드를 추가합니다

데이터 원본을 스캔하기 위해 스캔 처리 성능이 더 필요한 경우 스캐너 노드를 더 추가할 수 있습니다. 관리자 노드를 설치한 직후 스캐너 노드를 추가하거나 나중에 스캐너 노드를 추가할 수 있습니다. 예를 들어 데이터 소스 중 하나에 있는 데이터의 양이 6개월 후 두 배 또는 세 배 증가했다는 사실을 알고 있는 경우 데이터 스캔을 지원하기 위해 새 스캐너 노드를 추가할 수 있습니다.

다음 두 가지 방법으로 스캐너 노드를 추가할 수 있습니다.

- 노드를 추가하여 모든 데이터 소스 스캔에 도움을 줍니다
- 특정 데이터 소스 또는 특정 데이터 소스 그룹(일반적으로 위치에 따라 다름)을 스캔하는 데 도움이 되는 노드 추가

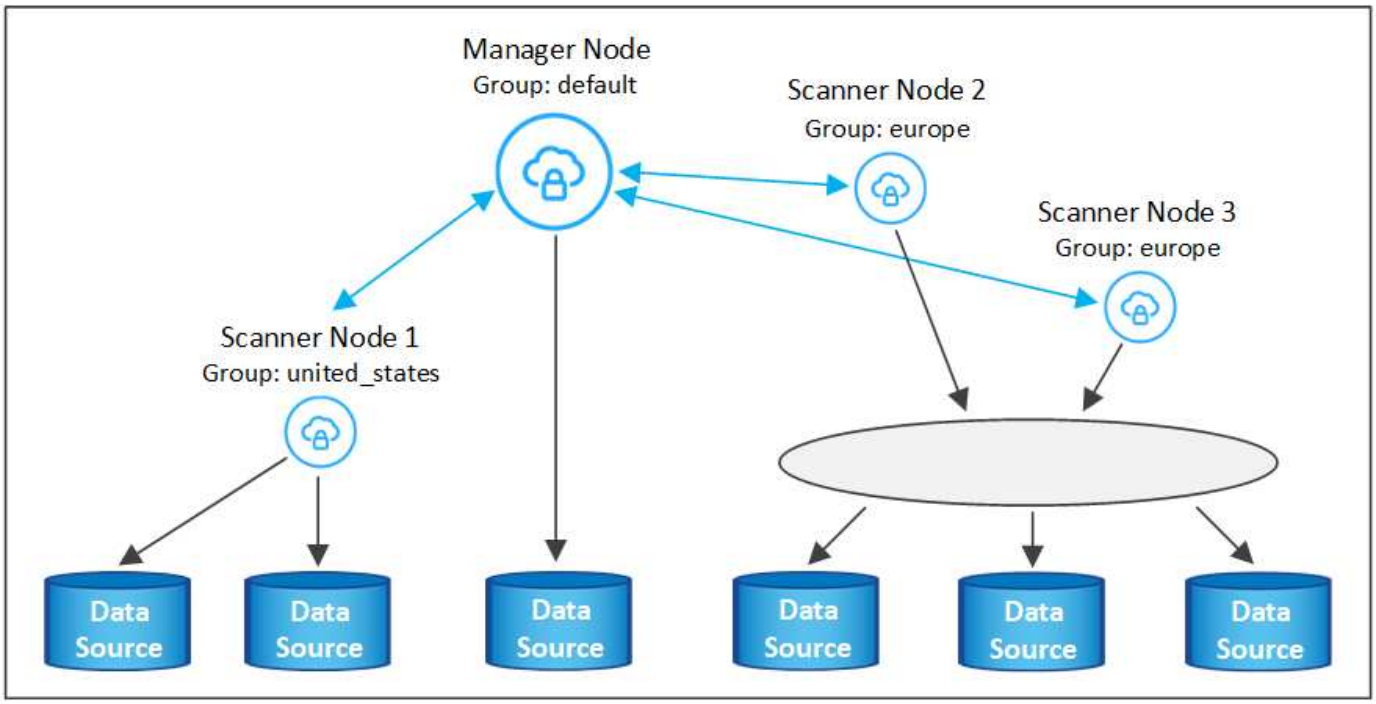
기본적으로 새로 추가한 스캐너 노드는 스캔 리소스의 일반 풀에 추가됩니다. 이를 "기본 스캐너 그룹"이라고 합니다. 아래 이미지의 "기본" 그룹에는 6개 데이터 소스 모두의 스캔 데이터인 1개의 관리자 노드와 3개의 스캐너 노드가 있습니다.



데이터 원본에 물리적으로 가까운 스캐너 노드에서 스캔할 특정 데이터 원본이 있는 경우 스캐너 노드 또는 스캐너 노드 그룹을 정의하여 특정 데이터 원본 또는 데이터 원본 그룹을 스캔할 수 있습니다. 아래 이미지에는 관리자 노드 1개와 스캐너 노드 3개가 있습니다.

- Manager 노드는 "기본" 그룹에 있으며 1개의 데이터 소스를 스캔하고 있습니다

- 스캐너 노드 1은 "United_states" 그룹에 있으며 2개의 데이터 소스를 스캔하고 있습니다
- 스캐너 노드 2와 3은 "유럽" 그룹에 속하며 3개의 데이터 원본에 대한 스캔 작업을 공유합니다



BlueXP 분류 스캐너 그룹은 데이터가 저장되는 별도의 지리적 영역으로 정의할 수 있습니다. 여러 BlueXP 분류 스캐너 노드를 전 세계에 배포하고 각 노드에 대해 스캐너 그룹을 선택할 수 있습니다. 이렇게 하면 각 스캐너 노드가 가장 가까운 데이터를 스캔합니다. 스캐너 노드가 데이터에 가까울수록 데이터 스캔 시 네트워크 대기 시간이 최대한 줄어들기 때문에 성능이 향상됩니다.

BlueXP 분류에 추가할 스캐너 그룹을 선택하고 이름을 선택할 수 있습니다. BlueXP 분류에서는 "유럽"이라는 스캐너 그룹에 매핑된 노드가 유럽에 배치되도록 강제하지 않습니다.

다음 단계에 따라 추가 BlueXP 분류 스캐너 노드를 설치합니다.

1. 스캐너 노드로 사용할 Linux 호스트 시스템을 준비합니다
2. 이 Linux 시스템에 Data Sense 소프트웨어를 다운로드하십시오
3. Manager 노드에서 명령을 실행하여 스캐너 노드를 식별합니다
4. 스캐너 노드에 소프트웨어를 배포하려면 다음 단계를 따르십시오(특정 스캐너 노드에 대해 "스캐너 그룹"을 선택적으로 정의).
5. 스캐너 그룹을 정의한 경우 관리자 노드에서 다음을 수행합니다.
   a. "working_environment_to_scanner_group_config.yml" 파일을 열고 각 스캐너 그룹이 스캔할 작업 환경을 정의합니다
   b. 다음 스크립트를 실행하여 이 매핑 정보를 모든 스캐너 노드에 등록합니다.
   `update_we_scanner_group_from_config_file.sh`

필요한 것

- 스캐너 노드의 모든 Linux 시스템이 을 충족하는지 확인합니다 호스트 요구 사항.
- 시스템에 두 가지 필수 소프트웨어 패키지(Docker Engine 또는 Podman 및 Python 3)가 설치되어 있는지 확인합니다.

- Linux 시스템에 대한 루트 권한이 있는지 확인합니다.
- 사용 환경이 필요한 를 충족하는지 확인합니다 사용 권한 및 연결.
- 추가하려는 스캐너 노드 호스트의 IP 주소가 있어야 합니다.
- BlueXP 분류 관리자 노드 호스트 시스템의 IP 주소가 있어야 합니다
- 커넥터 시스템의 IP 주소 또는 호스트 이름, NetApp 계정 ID, 커넥터 클라이언트 ID 및 사용자 액세스 토큰이 있어야 합니다. 스캐너 그룹을 사용하려는 경우 계정의 각 데이터 원본에 대한 작업 환경 ID를 알아야 합니다. 이 정보를 보려면 아래의 *필수 단계 * 를 참조하십시오.
- 모든 호스트에서 다음 포트 및 프로토콜을 활성화해야 합니다.

포트	프로토콜	설명
2377	TCP	클러스터 관리 통신
7946	TCP, UDP	노드 간 통신
4789	UDP입니다	오버레이 네트워크 트래픽
50	ESP	암호화된 IPsec 오버레이 네트워크(ESP) 트래픽
111	TCP, UDP	호스트 간 파일 공유를 위한 NFS 서버(각 스캐너 노드에서 관리자 노드로 필요)
2049	TCP, UDP	호스트 간 파일 공유를 위한 NFS 서버(각 스캐너 노드에서 관리자 노드로 필요)

- 를 사용하는 경우 `firewalld` BlueXP 분류 시스템에서 BlueXP 분류를 설치하기 전에 활성화하는 것이 좋습니다. 다음 명령을 실행하여 구성합니다 `firewalld` 따라서 BlueXP 분류와 호환됩니다.

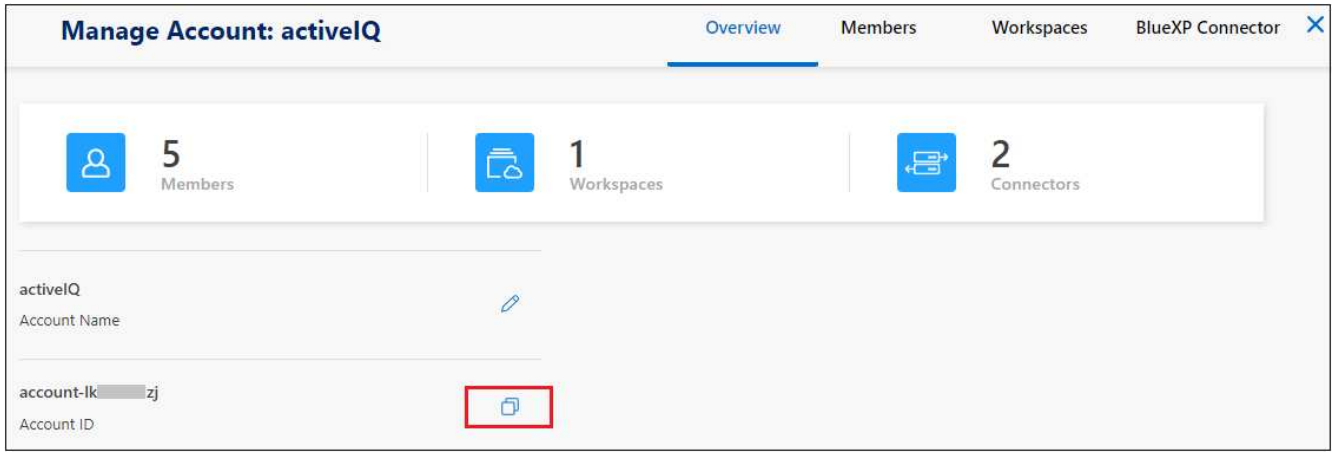
```
firewall-cmd --permanent --add-service=http
firewall-cmd --permanent --add-service=https
firewall-cmd --permanent --add-port=80/tcp
firewall-cmd --permanent --add-port=8080/tcp
firewall-cmd --permanent --add-port=443/tcp
firewall-cmd --permanent --add-port=2377/tcp
firewall-cmd --permanent --add-port=7946/udp
firewall-cmd --permanent --add-port=7946/tcp
firewall-cmd --permanent --add-port=4789/udp
firewall-cmd --reload
```

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

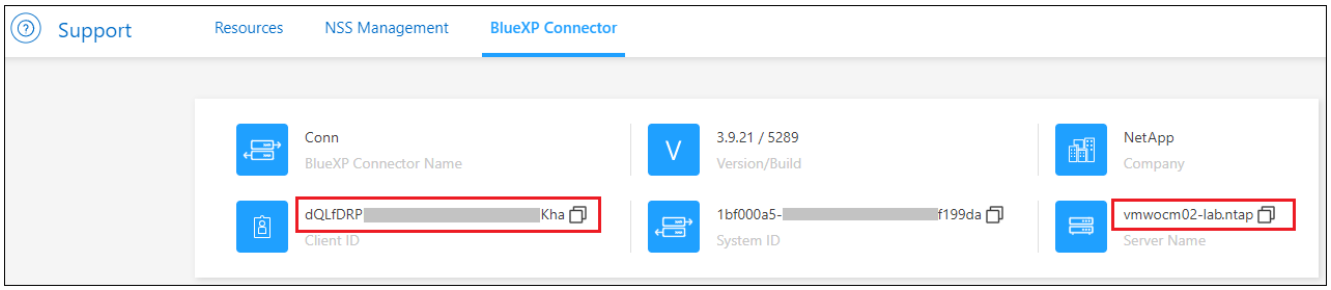
필수 단계

다음 단계에 따라 스캐너 노드를 추가하는 데 필요한 NetApp 계정 ID, 커넥터 클라이언트 ID, 커넥터 서버 이름 및 사용자 액세스 토큰을 얻습니다.

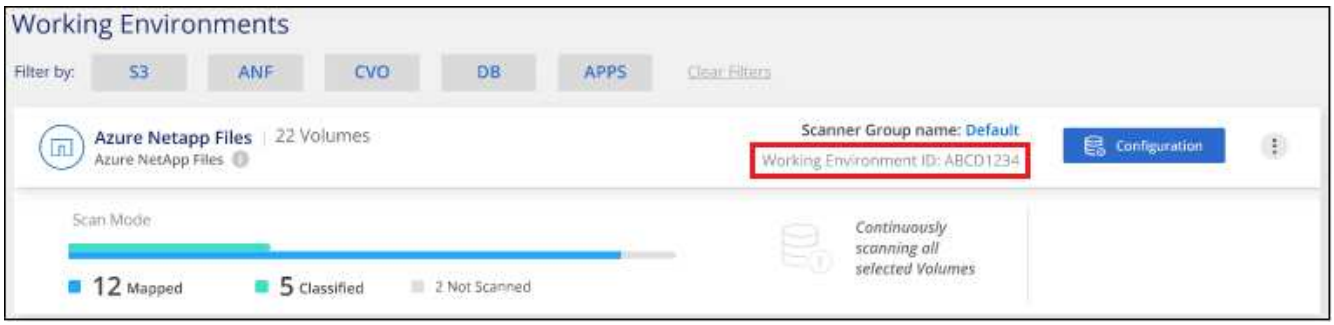
1. BlueXP 메뉴 표시줄에서 * 계정 > 계정 관리 * 를 클릭합니다.



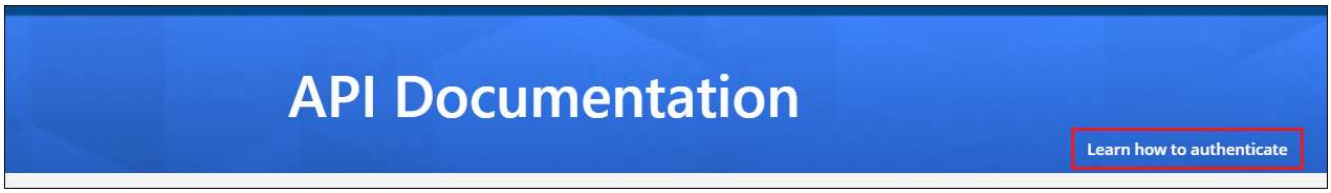
2. 계정 ID _ 을(를) 복사합니다.
3. BlueXP 메뉴 모음에서 * 도움말 > 지원 > BlueXP 커넥터 * 를 클릭합니다.



4. 커넥터_클라이언트 ID_ 및 _서버 이름_을 복사합니다.
5. 스캐너 그룹을 사용하려는 경우 BlueXP 분류 구성 탭에서 스캐너 그룹에 추가할 각 작업 환경의 작업 환경 ID를 복사합니다.



6. 로 이동합니다 "API 설명서 개발자 허브" 를 클릭하고 * 인증 방법 알아보기 * 를 클릭합니다.



7. "사용자 이름" 및 "암호" 매개 변수에서 계정 관리자의 사용자 이름과 암호를 사용하여 인증 지침을 따릅니다.
8. 그런 다음 응답에서 _ACCESS TOKEN_을 복사합니다.

단계

1. BlueXP 분류 관리자 노드에서 "add_scanner_node.sh" 스크립트를 실행합니다. 예를 들어, 이 명령은 두 개의 스캐너 노드를 추가합니다.

   ```
   sudo ./add_scanner_node.sh -a <account_id> -c <client_id> -m <cm_host> -h
   <ds_manager_ip> -n <node_private_ip_1,node_private_ip_2> -t <user_token>
   ```

   변수 값:

   - *ACCOUNT_ID*= NetApp 계정 ID입니다
   - *client_id*=커넥터 클라이언트 ID(필수 조건 단계에서 복사한 클라이언트 ID에 접미사 "clients" 추가)
   - *cm_host*= 커넥터 시스템의 IP 주소 또는 호스트 이름입니다
   - *DS_MANAGER_IP*= BlueXP 분류 관리자 노드 시스템의 전용 IP 주소입니다
   - *node_private_ip*= BlueXP 분류 스캐너 노드 시스템의 IP 주소(여러 스캐너 노드 IP는 쉼표로 구분)
   - *USER_TOKEN*= JWT 사용자 액세스 토큰

2. add_scanner_node 스크립트가 완료되기 전에 스캐너 노드에 필요한 설치 명령이 대화 상자에 표시됩니다. 명령을 복사합니다(예: `sudo ./node_install.sh -m 10.11.12.13 -t ABCDEF1s35212 -u red95467j`)를 입력하고 텍스트 파일에 저장합니다.

3. 켜짐 * 각 * 스캐너 노드 호스트:

   a. 데이터 감지 설치 프로그램 파일(* DATASENSE-INinstaller-<version>.tar.gz*)을 호스트 컴퓨터('scp' 또는 다른 방법 사용)에 복사합니다.

   b. 설치 프로그램 파일의 압축을 풉니다.

   c. 2단계에서 복사한 명령을 붙여 넣고 실행합니다.

   d. 스캐너 노드를 "scanner group"에 추가하려면 * -r <scanner_group_name> * 매개 변수를 명령에 추가합니다. 그렇지 않으면 스캐너 노드가 "기본" 그룹에 추가됩니다.

      모든 스캐너 노드에서 설치가 완료되고 관리자 노드에 연결된 경우 "add_scanner_node.sh" 스크립트도 완료됩니다. 설치하는 데 10-20분이 소요될 수 있습니다.

4. 스캐너 그룹에 스캐너 노드를 추가한 경우 관리자 노드로 돌아가 다음 두 가지 작업을 수행합니다.

   a. "/opt/netapp/config/custom_configuration/working_environment_to_scanner_group_config.yml" 파일을 열고 특정 작업 환경을 스캔할 스캐너 그룹의 매핑을 입력합니다. 각 데이터 소스에 대해 _Working Environment ID_가 있어야 합니다. 예를 들어 다음 항목은 "유럽" 스캐너 그룹에 작업 환경 2개를 추가하고 "United_states" 스캐너 그룹에 작업 환경 2개를 추가합니다.

```
scanner_groups:
 europe:
   working_environments:
     - "working_environment_id1"
     - "working_environment_id2"
 united_states:
   working_environments:
     - "working_environment_id3"
     - "working_environment_id4"
```

목록에 추가되지 않은 모든 작업 환경은 "기본" 그룹에 의해 스캔됩니다. "기본" 그룹에 하나 이상의 관리자 또는 스캐너 노드가 있어야 합니다.

b. 다음 스크립트를 실행하여 이 매핑 정보를 모든 스캐너 노드에 등록합니다.
`/opt/netapp/Datasense/tools/update_we_scanner_group_from_config_file.sh`

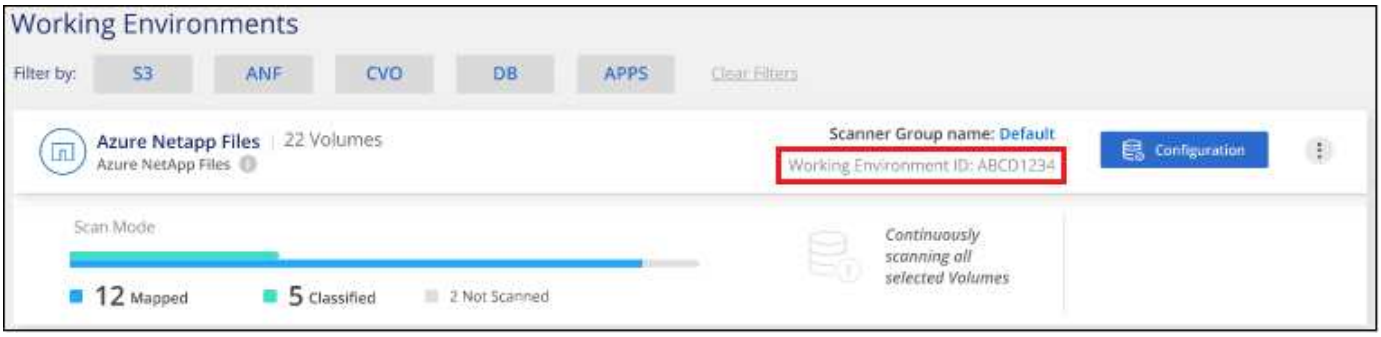
결과

BlueXP 분류는 모든 데이터 소스를 스캔하기 위해 관리자 및 스캐너 노드와 함께 설정됩니다.

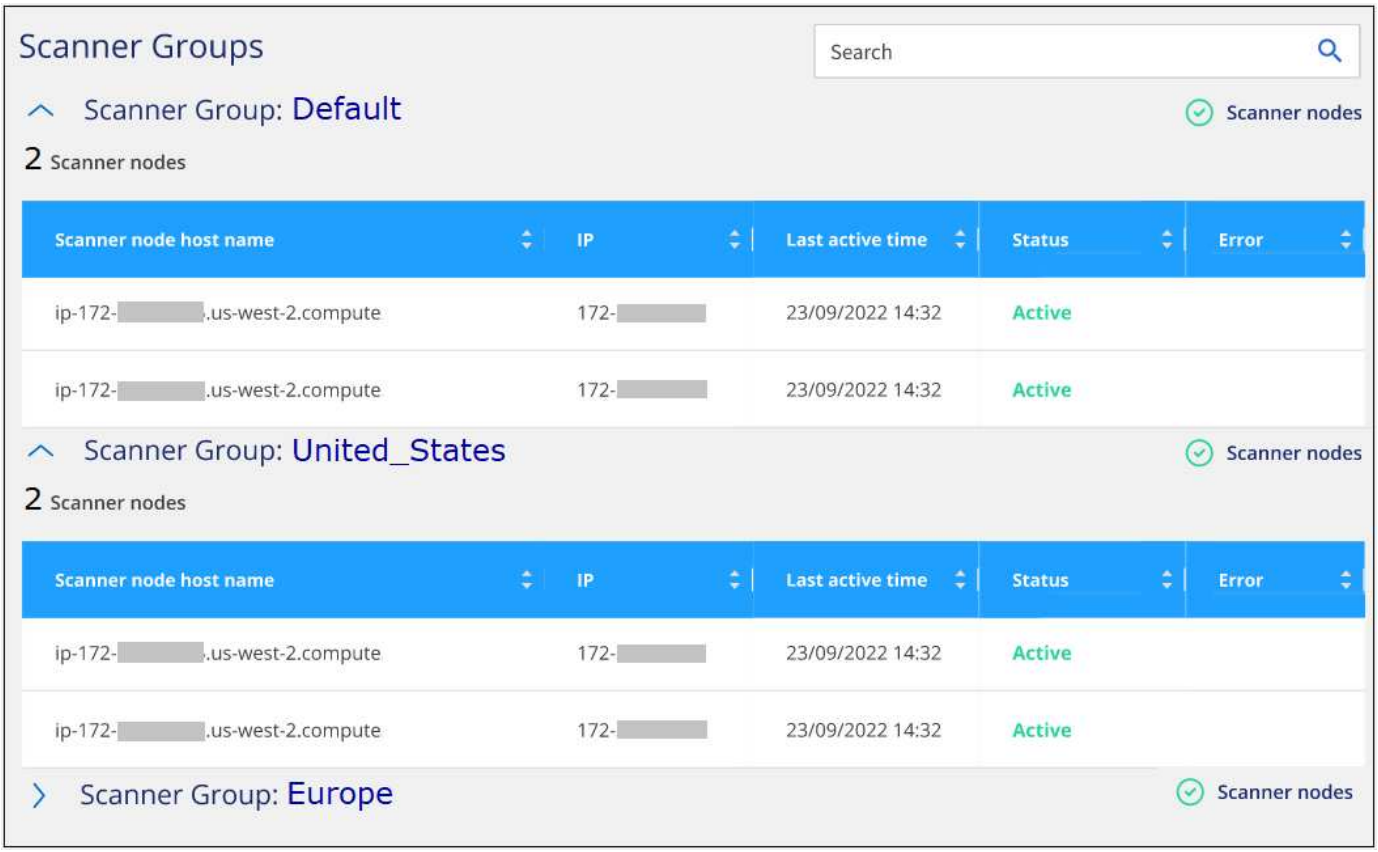
다음 단계

아직 선택하지 않은 경우 구성 페이지에서 스캔할 데이터 원본을 선택할 수 있습니다. 스캐너 그룹을 생성한 경우 각 데이터 소스는 해당 그룹의 스캐너 노드에 의해 스캔됩니다.

구성 페이지에서 각 작업 환경에 대한 스캐너 그룹 이름을 볼 수 있습니다.



또한 구성 페이지 아래쪽에 있는 그룹의 각 스캐너 노드에 대한 IP 주소 및 상태와 함께 모든 스캐너 그룹 목록을 볼 수 있습니다.



가능합니다 "BlueXP 분류 라이선스를 설정합니다" 현재. 30일 무료 평가판이 종료될 때까지 요금이 부과되지 않습니다.

대규모 구성을 위한 다중 호스트 설치

페타바이트 단위의 데이터를 스캐닝할 대규모 구성의 경우 여러 호스트를 포함하여 추가적인 처리 성능을 제공할 수 있습니다. 여러 호스트 시스템을 사용하는 경우 주 시스템을 _Manager node_라고 하며 추가 처리 능력을 제공하는 추가 시스템을 _Scanner nodes_라고 합니다.

여러 온-프레미스 호스트에 BlueXP 분류 소프트웨어를 동시에 설치할 경우 다음 단계를 따르십시오. 이러한 방식으로 여러 호스트를 배포할 때는 "스캐너 그룹"을 사용할 수 없습니다.

필요한 것

- Manager 및 Scanner 노드의 모든 Linux 시스템이 을 충족하는지 확인합니다 호스트 요구 사항.
- 시스템에 두 가지 필수 소프트웨어 패키지(Docker 또는 Podman Engine 및 Python 3)가 설치되어 있는지 확인합니다.
- Linux 시스템에 대한 루트 권한이 있는지 확인합니다.
- 사용 환경이 필요한 를 충족하는지 확인합니다 사용 권한 및 연결.
- 사용하려는 스캐너 노드 호스트의 IP 주소가 있어야 합니다.
- 모든 호스트에서 다음 포트 및 프로토콜을 활성화해야 합니다.

포트	프로토콜	설명
2377	TCP	클러스터 관리 통신
7946	TCP, UDP	노드 간 통신

포트	프로토콜	설명
4789	UDP입니다	오버레이 네트워크 트래픽
50	ESP	암호화된 IPsec 오버레이 네트워크(ESP) 트래픽
111	TCP, UDP	호스트 간 파일 공유를 위한 NFS 서버(각 스캐너 노드에서 관리자 노드로 필요)
2049	TCP, UDP	호스트 간 파일 공유를 위한 NFS 서버(각 스캐너 노드에서 관리자 노드로 필요)

단계

1. 에서 1단계부터 7단계까지 수행합니다 단일 호스트 설치 관리자 노드에서.
2. 8단계에서 설명한 것처럼 설치 프로그램에서 메시지를 표시하면 일련의 프롬프트에 필요한 값을 입력하거나 설치 프로그램에 명령줄 인수로 필요한 매개 변수를 제공할 수 있습니다.

   단일 호스트 설치에 사용할 수 있는 변수 외에도 새 옵션 * -n<node_ip> * 를 사용하여 스캐너 노드의 IP 주소를 지정할 수 있습니다. 여러 스캐너 노드 IP는 쉼표로 구분됩니다.

   예를 들어, 이 명령은 다음과 같이 3개의 스캐너 노드를 추가합니다.
   ```
   sudo ./install.sh -a <account_id> -c <client_id> -t <user_token> --host
   <ds_host> --manager-host <cm_host> -n <node_ip1>,<node_ip2>,<node_ip3> --proxy
   -host <proxy_host> --proxy-port <proxy_port> --proxy-scheme <proxy_scheme>
   --proxy-user <proxy_user> --proxy-password <proxy_password>
   ```
3. 관리자 노드 설치가 완료되기 전에 스캐너 노드에 필요한 설치 명령이 대화 상자에 표시됩니다. 명령을 복사합니다(예: `sudo ./node_install.sh -m 10.11.12.13 -t ABCDEF-1-3u69m1-1s35212`)를 입력하고 텍스트 파일에 저장합니다.
4. 켜짐 * 각 * 스캐너 노드 호스트:
   a. 데이터 감지 설치 프로그램 파일(* DATASENSE-INinstaller-<version>.tar.gz*)을 호스트 컴퓨터('scp' 또는 다른 방법 사용)에 복사합니다.
   b. 설치 프로그램 파일의 압축을 풉니다.
   c. 3단계에서 복사한 명령을 붙여 넣고 실행합니다.

      모든 스캐너 노드에서 설치가 완료되고 관리자 노드에 연결되었으면 관리자 노드 설치도 완료됩니다.

결과

BlueXP 분류 설치 프로그램이 패키지 설치를 완료하고 설치를 등록합니다. 설치는 10분에서 20분 정도 걸릴 수 있습니다.

다음 단계

구성 페이지에서 스캔할 데이터 원본을 선택할 수 있습니다.

또한 가능합니다 "BlueXP 분류 라이선스를 설정합니다" 현재. 30일 무료 평가판이 종료될 때까지 요금이 부과되지 않습니다.

인터넷에 액세스할 수 없는 Linux 호스트에 BlueXP 분류를 설치합니다

인터넷에 액세스할 수 없는 온프레미스 사이트의 Linux 호스트에 BlueXP 분류를 설치하려면 몇 단계를 완료하십시오. _ private mode _ 라고도 합니다. 이러한 유형의 설치는 보안 사이트에 적합합니다.

"BlueXP Connector 및 BlueXP 분류의 다양한 배포 모드에 대해 알아보십시오".

참고: 또한 이 기능을 사용할 수 있습니다 "인터넷에 액세스할 수 있는 사내 사이트에 BlueXP 분류를 배포합니다".

BlueXP 분류 설치 스크립트는 시스템 및 환경이 필수 전제 조건을 충족하는지 확인하는 것으로 시작됩니다. 필수 구성 요소가 모두 충족되면 설치가 시작됩니다. BlueXP 분류 설치를 실행하는 것과 별도로 필수 구성 요소를 확인하려면 필수 구성 요소에 대한 테스트만 다운로드할 수 있는 별도의 소프트웨어 패키지가 있습니다. "Linux 호스트가 BlueXP 분류를 설치할 준비가 되었는지 확인하는 방법을 참조하십시오".

지원되는 데이터 소스

비공개 모드("오프라인" 또는 "다크" 사이트라고도 함)를 설치할 경우 BlueXP 분류는 사내 사이트에 로컬인 데이터 소스에서만 데이터를 스캔할 수 있습니다. 현재 BlueXP 분류는 다음 * 로컬 * 데이터 소스를 검사할 수 있습니다.

- 온프레미스 ONTAP 시스템
- 데이터베이스 스키마
- SharePoint 사내 계정(SharePoint Server)
- 비NetApp NFS 또는 CIFS 파일 공유
- S3(Simple Storage Service) 프로토콜을 사용하는 오브젝트 스토리지

현재 Cloud Volumes ONTAP, Azure NetApp Files, FSx for ONTAP, AWS S3 또는 Google Drive 스캔을 지원하지 않습니다. BlueXP 분류가 개인 모드로 배포되는 경우 OneDrive 또는 SharePoint Online 계정

제한 사항

대부분의 BlueXP 분류 기능은 인터넷에 액세스할 수 없는 사이트에 배포할 때 작동합니다. 그러나 인터넷 액세스가 필요한 특정 기능은 지원되지 않습니다. 예를 들면 다음과 같습니다.

- Microsoft Azure 정보 보호(AIP) 레이블 관리
- 특정 중요 정책이 결과를 반환할 때 BlueXP 사용자에게 전자 메일 알림을 보냅니다
- 여러 사용자에 대한 BlueXP 역할 설정(예: 계정 관리자 또는 규정 준수 뷰어)
- BlueXP 복사 및 동기화를 사용하여 소스 파일 복사 및 동기화
- 사용자 피드백을 받는 중입니다
- BlueXP에서 소프트웨어 자동 업그레이드

  BlueXP 커넥터와 BlueXP 분류 모두 새로운 기능을 사용하려면 정기적인 수동 업그레이드가 필요합니다. BlueXP 분류 UI 페이지 하단에서 BlueXP 분류 버전을 확인할 수 있습니다. 를 확인하십시오 "BlueXP 분류 릴리스 정보" 각 릴리스의 새로운 기능과 해당 기능을 원하는지 여부를 확인합니다. 그런 다음 의 단계를 수행할 수 있습니다 "BlueXP 커넥터를 업그레이드합니다" 및 BlueXP 분류 소프트웨어를 업그레이드합니다.

빠른 시작

다음 단계를 따라 빠르게 시작하거나 나머지 섹션을 아래로 스크롤하여 자세한 내용을 확인하십시오.

1 **BlueXP** 커넥터를 설치합니다

아직 비공개 모드로 커넥터가 설치되어 있지 않은 경우 "커넥터를 배포합니다" 이제 Linux 호스트에서

2 **BlueXP** 분류 사전 요구 사항을 검토합니다

Linux 시스템이 를 충족하는지 확인합니다 호스트 요구 사항필요한 모든 소프트웨어가 설치되어 있고 오프라인 환경이 필요한 를 충족한다는 것을 나타냅니다 사용 권한 및 연결.

3 **BlueXP** 분류를 다운로드하고 배포합니다

NetApp Support 사이트에서 BlueXP 분류 소프트웨어를 다운로드하고 사용할 Linux 호스트에 설치 프로그램 파일을 복사합니다. 그런 다음 설치 마법사를 시작하고 화면의 지시에 따라 BlueXP 분류 인스턴스를 배포합니다.

4 **BlueXP** 분류 서비스에 가입합니다

BlueXP의 BlueXP 분류 검사에서 처음 1TB의 데이터는 30일 동안 무료로 제공됩니다. 이 시점 이후에 데이터를 계속 스캔하려면 NetApp의 BYOL 라이센스가 필요합니다.

BlueXP 커넥터를 설치합니다

BlueXP 커넥터가 아직 비공개 모드로 설치되어 있지 않은 경우 "커넥터를 배포합니다" 오프라인 사이트의 Linux 호스트

Linux 호스트 시스템을 준비합니다

BlueXP 분류 소프트웨어는 특정 운영 체제 요구 사항, RAM 요구 사항, 소프트웨어 요구 사항 등을 충족하는 호스트에서 실행해야 합니다.

- BlueXP 분류는 다른 애플리케이션과 공유되는 호스트에서는 지원되지 않습니다. 호스트는 전용 호스트여야 합니다.
- 구내 호스트 시스템을 구축할 때 BlueXP 분류 검사를 수행할 데이터 세트의 크기에 따라 세 가지 시스템 크기 중에서 선택할 수 있습니다.

시스템 크기	**CPU**	**RAM(**스왑 메모리는 비활성화 상태여야 함**)**	디스크
* 초대형 *	32개의 CPU	128GB RAM	/, 또는 의 1TiB SSD /opt에서 -100GiB를 사용할 수 있습니다 -895GiB는 /var/lib/docker에서 사용할 수 있습니다 /tmp에 -5GiB입니다

시스템 크기	**CPU**	**RAM(**스왑 메모리는 비활성화 상태여야 함**)**	디스크
* 대형 *	CPU 16개	64GB RAM	500GiB SSD 켜짐/또는 /opt에서 -100GiB를 사용할 수 있습니다 /var/lib/docker에서 사용 가능한 395GiB /tmp에 -5GiB입니다
* 중간 *	CPU 8개	32GB RAM	200GiB SSD 켜짐/또는 /opt에서 -50GiB를 사용할 수 있습니다 /var/lib/docker에서 -145GiB를 사용할 수 있습니다 /tmp에 -5GiB입니다
* 소형 *	CPU 8개	16GB RAM	또는 에서 100GiB SSD /opt에서 -50GiB를 사용할 수 있습니다 /var/lib/docker에서 -45GiB를 사용할 수 있습니다 /tmp에 -5GiB입니다

소형 시스템을 사용할 때는 제한이 있습니다. 을 참조하십시오 "더 작은 인스턴스 유형 사용" 를 참조하십시오.

- BlueXP 분류 설치를 위해 클라우드에 컴퓨팅 인스턴스를 배포할 때는 위의 "대규모" 시스템 요구 사항을 충족하는 시스템을 권장합니다.
  - * AWS EC2 인스턴스 유형 *: "m6i.4xLarge"를 권장합니다. "추가 AWS 인스턴스 유형을 참조하십시오".
  - * Azure VM size *: "Standard_D16s_v3"을 권장합니다. "추가 Azure 인스턴스 유형을 참조하십시오".
  - * GCP 시스템 유형 *: "n2-standard-16"을 권장합니다. "추가 GCP 인스턴스 유형을 참조하십시오".
- UNIX 폴더 권한 *: 다음과 같은 최소 UNIX 권한이 필요합니다.

폴더	최소 권한
/tmp	`rwxrwxrwt`
/opt	`rwxr-xr-x`
/var/lib/docker입니다	`rwx------`
/usr/lib/systemd/system입니다	`rwxr-xr-x`

- * 운영 체제 *:
  - 다음 운영 체제에서는 Docker 컨테이너 엔진을 사용해야 합니다.
    - Red Hat Enterprise Linux 버전 7.8 및 7.9
    - CentOS 버전 7.8 및 7.9
    - Ubuntu 22.04(BlueXP 분류 버전 1.23 이상 필요)
  - 다음 운영 체제에는 Podman 컨테이너 엔진을 사용해야 하며 BlueXP 분류 버전 1.30 이상이 필요합니다.
    - Red Hat Enterprise Linux 버전 8.8, 9.0, 9.1, 9.2 및 9.3

RHEL 8.x 및 RHEL 9.x를 사용하는 경우 다음 기능은 현재 지원되지 않습니다.

  - 어두운 장소에 설치
  - 분산 스캔, 마스터 스캐너 노드 및 원격 스캐너 노드 사용

- * Red Hat 서브스크립션 관리 *: 호스트는 Red Hat 서브스크립션 관리 에 등록되어 있어야 합니다. 등록되지 않은 경우 설치 중에 시스템에서 필요한 타사 소프트웨어를 업데이트하기 위해 리포지토리에 액세스할 수 없습니다.
- * 추가 소프트웨어 *: BlueXP 분류를 설치하기 전에 호스트에 다음 소프트웨어를 설치해야 합니다.
  - 사용 중인 OS에 따라 컨테이너 엔진 중 하나를 설치해야 합니다.
    - Docker Engine 버전 19.3.1 이상 "설치 지침을 봅니다".

      "이 비디오 시청" CentOS에 Docker를 설치하는 빠른 데모를 보려면

    - Podman 버전 4 이상 Podman을 설치하려면 시스템 패키지를 업데이트하십시오 (`sudo yum update -y`)를 클릭한 다음 Podman을 설치합니다 (`sudo yum install netavark -y`)를 클릭합니다.
- Python 버전 3.6 이상. "설치 지침을 봅니다".
  - * NTP 고려 사항 *: NetApp에서는 NTP(네트워크 시간 프로토콜) 서비스를 사용하도록 BlueXP 분류 시스템을 구성할 것을 권장합니다. BlueXP 분류 시스템과 BlueXP Connector 시스템 간에 시간을 동기화해야 합니다.
  - * Firewalld 고려 사항 *: 사용하려는 경우 `firewalld`BlueXP 분류를 설치하기 전에 활성화하는 것이 좋습니다. 다음 명령을 실행하여 구성합니다 `firewalld` 따라서 BlueXP 분류와 호환됩니다.

```
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
```

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

설치 후 BlueXP 분류 호스트 시스템의 IP 주소를 변경할 수 없습니다.

BlueXP 및 BlueXP 분류 사전 요구 사항을 확인합니다

BlueXP 분류를 배포하기 전에 다음 전제 조건을 검토하여 지원되는 구성이 있는지 확인합니다.

- Connector에 리소스를 배포하고 BlueXP 분류 인스턴스에 대한 보안 그룹을 만들 수 있는 권한이 있는지 확인합니다. 최신 BlueXP 사용 권한은 에서 확인할 수 있습니다 "NetApp에서 제공하는 정책".
- BlueXP 분류를 계속 실행할 수 있는지 확인합니다. 데이터를 지속적으로 스캔하려면 BlueXP 분류 인스턴스를 계속 사용해야 합니다.
- 웹 브라우저가 BlueXP 분류에 연결되어 있는지 확인합니다. BlueXP 분류를 사용하도록 설정한 후에는 BlueXP 분류 인스턴스에 연결된 호스트에서 BlueXP 인터페이스에 액세스해야 합니다.

  BlueXP 분류 인스턴스는 개인 IP 주소를 사용하여 인덱싱된 데이터에 다른 사용자가 액세스할 수 없도록 합니다.

따라서 BlueXP에 액세스하는 데 사용하는 웹 브라우저가 해당 개인 IP 주소에 연결되어 있어야 합니다. 이러한 연결은 BlueXP 분류 인스턴스와 동일한 네트워크 내에 있는 호스트에서 발생할 수 있습니다.

필요한 모든 포트가 활성화되어 있는지 확인합니다

커넥터, BlueXP 분류, Active Directory 및 데이터 소스 간의 통신에 필요한 모든 포트가 열려 있는지 확인해야 합니다.

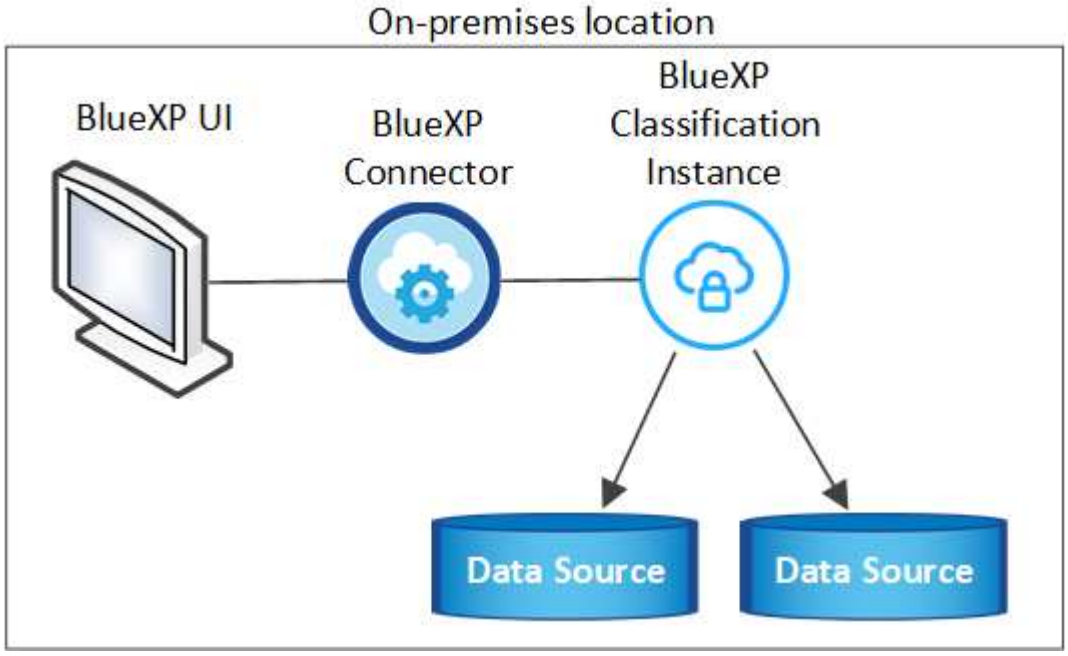
연결 유형	포트	설명
커넥터 <>BlueXP 분류	8080(TCP), 6000(TCP), 443(TCP) 및 80	Connector의 보안 그룹은 포트 6000 및 443을 통해 BlueXP 분류 인스턴스 간에 인바운드 및 아웃바운드 트래픽을 허용해야 합니다. • BlueXP 분류 BYOL 라이센스가 다크 사이트에서 작동하도록 하려면 포트 6000이 필요합니다. • BlueXP에서 설치 진행률을 확인할 수 있도록 포트 8080이 열려 있어야 합니다.
커넥터 <>ONTAP 클러스터(NAS)	443(TCP)	BlueXP는 HTTPS를 사용하여 ONTAP 클러스터를 검색합니다. 사용자 지정 방화벽 정책을 사용하는 경우 다음 요구 사항을 충족해야 합니다. • 커넥터 호스트는 포트 443을 통한 아웃바운드 HTTPS 액세스를 허용해야 합니다. Connector가 클라우드에 있는 경우 모든 아웃바운드 통신은 미리 정의된 보안 그룹에서 허용됩니다. • ONTAP 클러스터는 포트 443을 통한 인바운드 HTTPS 액세스를 허용해야 합니다. 기본 "관리" 방화벽 정책은 모든 IP 주소에서 인바운드 HTTPS 액세스를 허용합니다. 이 기본 정책을 수정하거나 자체 방화벽 정책을 만든 경우 HTTPS 프로토콜을 해당 정책에 연결하고 Connector 호스트에서 액세스를 활성화해야 합니다.
BlueXP 분류<>ONTAP 클러스터	• NFS-111(TCP\UDP) 및 2049(TCP\UDP)의 경우 • CIFS-139(TCP\UDP) 및 445(TCP\UDP)의 경우	BlueXP 분류에는 각 Cloud Volumes ONTAP 서브넷 또는 온프레미스 ONTAP 시스템에 대한 네트워크 연결이 필요합니다. Cloud Volumes ONTAP의 보안 그룹은 BlueXP 분류 인스턴스에서 인바운드 연결을 허용해야 합니다. 이러한 포트가 BlueXP 분류 인스턴스에 열려 있는지 확인합니다. • NFS-111 및 2049용 • CIFS-139 및 445의 경우 NFS 볼륨 내보내기 정책은 BlueXP 분류 인스턴스에서 액세스를 허용해야 합니다.

연결 유형	포트	설명
BlueXP 분류<>Active Directory	389(TCP 및 UDP), 636(TCP), 3268(TCP) 및 3269(TCP)	회사의 사용자에 대해 Active Directory가 이미 설정되어 있어야 합니다. 또한 BlueXP 분류에는 CIFS 볼륨을 스캔하기 위해 Active Directory 자격 증명이 필요합니다. Active Directory에 대한 정보가 있어야 합니다. • DNS 서버 IP 주소 또는 여러 IP 주소 • 서버의 사용자 이름 및 암호 • 도메인 이름(Active Directory 이름) • 보안 LDAP(LDAPS) 사용 여부 • LDAP 서버 포트(일반적으로 LDAP의 경우 389, 보안 LDAP의 경우 636)

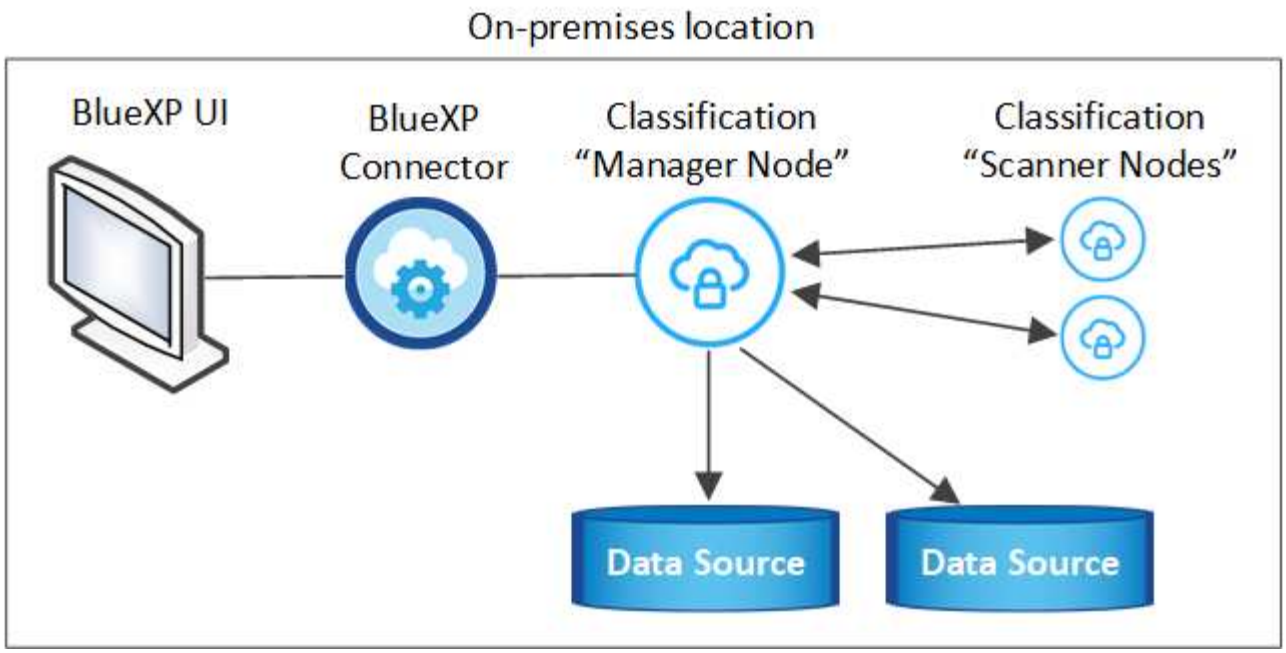
여러 BlueXP 분류 호스트를 사용하여 데이터 소스를 검사하는 추가 처리 기능을 제공하는 경우 추가 포트/프로토콜을 활성화해야 합니다. "추가 포트 요구 사항을 참조하십시오".

사내 **Linux** 호스트에 **BlueXP** 분류를 설치합니다

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



페타바이트 단위의 데이터를 스캐닝할 대규모 구성의 경우 여러 호스트를 포함하여 추가적인 처리 성능을 제공할 수 있습니다. "여기에서 해당 단계를 확인하십시오".



일반 구성을 위한 단일 호스트 설치

오프라인 환경의 단일 사내 호스트에 BlueXP 분류 소프트웨어를 설치할 때는 다음 단계를 따르십시오.

모든 설치 작업은 BlueXP 분류를 설치할 때 기록됩니다. 설치 중에 문제가 발생하면 설치 감사 로그의 내용을 볼 수 있습니다. 에 기록됩니다 `/opt/netapp/install_logs/`. "자세한 내용은 여기에서 확인하십시오.".

필요한 것

- Linux 시스템이 를 충족하는지 확인합니다 호스트 요구 사항.
- 두 가지 필수 소프트웨어 패키지(Docker Engine 또는 Podman 및 Python 3)를 설치했는지 확인합니다.
- Linux 시스템에 대한 루트 권한이 있는지 확인합니다.
- 오프라인 환경이 필요한 를 충족하는지 확인합니다 사용 권한 및 연결.

단계

1. 인터넷 구성 시스템의 경우 에서 BlueXP 분류 소프트웨어를 다운로드합니다 "NetApp Support 사이트". 선택해야 하는 파일의 이름은 * DataSense-offline-bundle-<version>.tar.gz * 입니다.
2. 개인 모드에서 사용할 Linux 호스트에 설치 프로그램 번들을 복사합니다.
3. 호스트 시스템에서 설치 프로그램 번들의 압축을 풉니다. 예를 들면 다음과 같습니다.

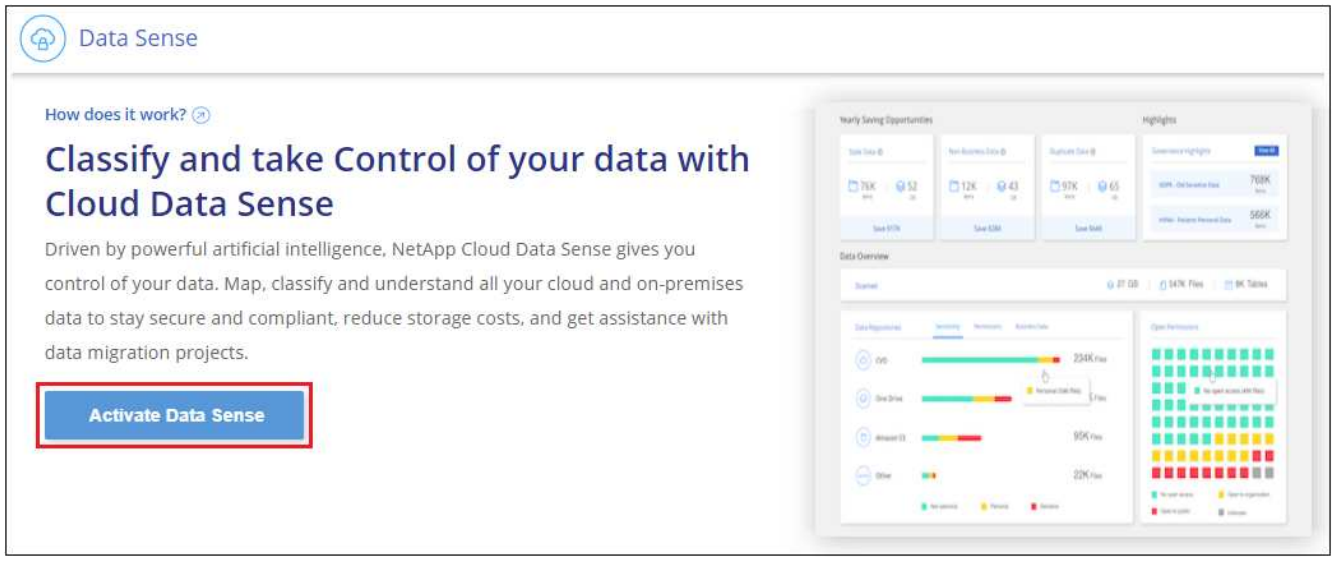
   ```
   tar -xzf DataSense-offline-bundle-v1.25.0.tar.gz
   ```

   필요한 소프트웨어와 실제 설치 파일 * cc_onprem_installer.tar.gz * 를 추출합니다.

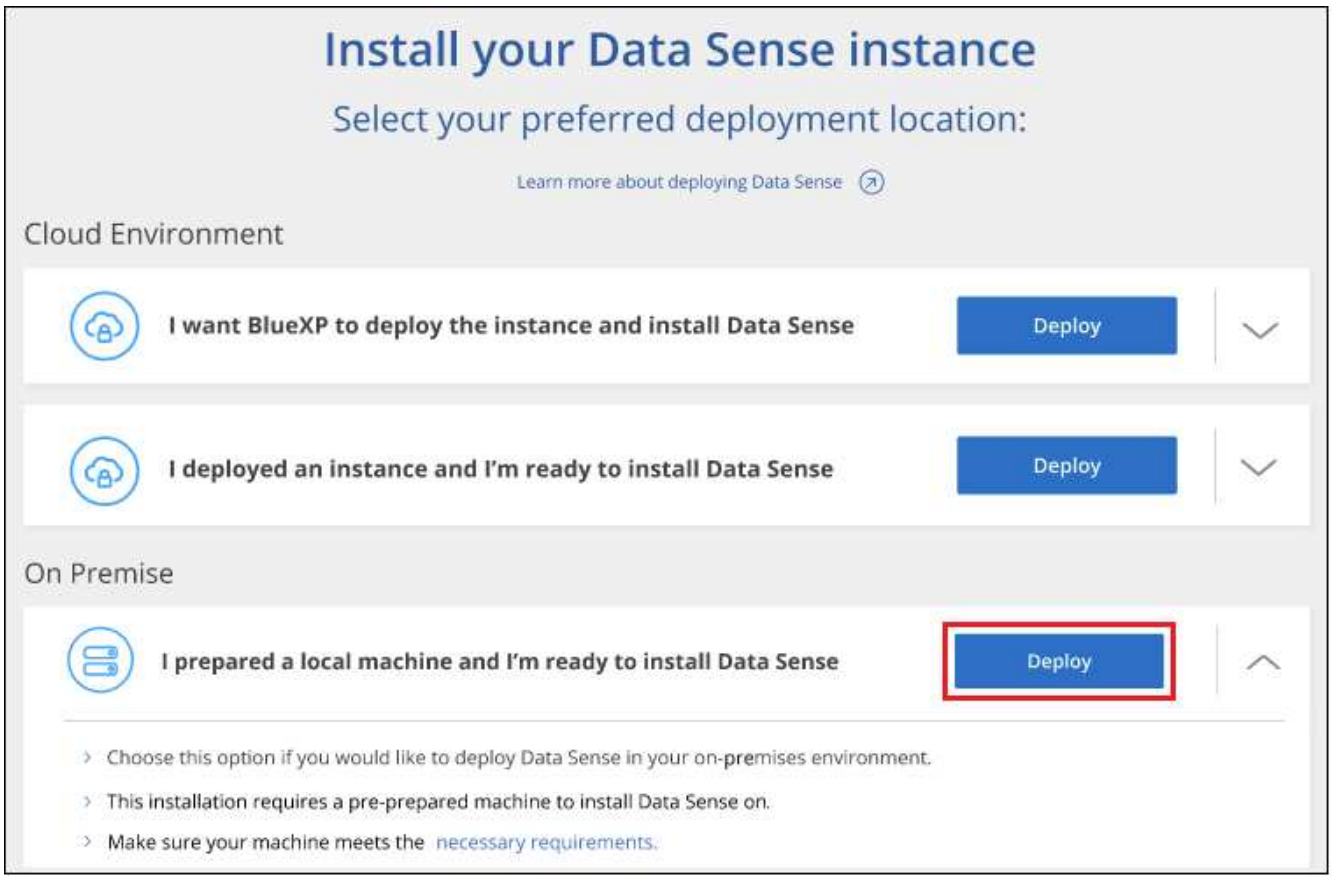
4. 호스트 시스템에서 설치 파일의 압축을 풉니다. 예를 들면 다음과 같습니다.

   ```
   tar -xzf cc_onprem_installer.tar.gz
   ```

5. BlueXP를 시작하고 * Governance > Classification * 을 선택합니다.
6. Activate Data Sense * 를 클릭합니다.



7. 사내 설치를 시작하려면 * deploy * 를 클릭합니다.



8. Deploy Data Sense on Premises_대화 상자가 표시됩니다. 제공된 명령을 복사합니다(예: `sudo ./install.sh -a 12345 -c 27AG75 -t 2198qq --darksite`)를 사용하여 텍스트 파일에 붙여 넣어 나중에 사용할 수 있습니다. 그런 다음 * 닫기 * 를 클릭하여 대화 상자를 닫습니다.
9. 호스트 시스템에서 복사한 명령을 입력한 다음 일련의 프롬프트를 따르거나 필요한 모든 매개 변수를 명령줄 인수로

포함하여 전체 명령을 제공할 수 있습니다.

설치 프로그램은 사전 검사를 수행하여 시스템 및 네트워킹 요구 사항이 제대로 설치되어 있는지 확인합니다.

프롬프트가 나타나면 매개 변수를 입력합니다.	전체 명령 입력:
a. 8단계에서 복사한 정보를 붙여 넣습니다. `sudo ./install.sh -a <account_id> -c <client_id> -t <user_token> --darksite` b. BlueXP 분류 호스트 시스템의 IP 주소 또는 호스트 이름을 입력하여 Connector 시스템에서 액세스할 수 있도록 합니다. c. BlueXP 커넥터 호스트 시스템의 IP 주소 또는 호스트 이름을 입력하여 BlueXP 분류 시스템에서 액세스할 수 있습니다.	또는 필요한 호스트 매개 변수를 제공하여 전체 명령을 미리 생성할 수도 있습니다. `sudo ./install.sh -a <account_id> -c <client_id> -t <user_token> --host <ds_host> --manager-host <cm_host> --no-proxy --darksite`

변수 값:

- *ACCOUNT_ID*= NetApp 계정 ID입니다
- *client_id*=커넥터 클라이언트 ID(클라이언트 ID에 접미어 "clients"가 없으면 추가)
- *USER_TOKEN*= JWT 사용자 액세스 토큰
- *DS_HOST*= BlueXP 분류 시스템의 IP 주소 또는 호스트 이름입니다.
- *cm_host*= BlueXP 커넥터 시스템의 IP 주소 또는 호스트 이름입니다.

결과

BlueXP 분류 설치 프로그램은 패키지를 설치하고, 설치를 등록하고, BlueXP 분류를 설치합니다. 설치는 10분에서 20분 정도 걸릴 수 있습니다.

호스트 시스템과 커넥터 인스턴스 간에 포트 8080을 통해 연결되어 있는 경우 BlueXP의 BlueXP 분류 탭에서 설치 진행 상황을 확인할 수 있습니다.

다음 단계

구성 페이지에서 로컬 을 선택할 수 있습니다 "온프레미스 ONTAP 클러스터" 및 "데이터베이스를 지원합니다" 선택합니다.

또한 가능합니다 "BlueXP 분류에 대한 BYOL 라이센스 설정" 현재 BlueXP 디지털 전자지갑에서 30일 무료 평가판이 종료될 때까지 요금이 부과되지 않습니다.

대규모 구성을 위한 다중 호스트 설치

페타바이트 단위의 데이터를 스캐닝할 대규모 구성의 경우 여러 호스트를 포함하여 추가적인 처리 성능을 제공할 수 있습니다. 여러 호스트 시스템을 사용하는 경우 주 시스템을 _Manager node_라고 하며 추가 처리 능력을 제공하는 추가 시스템을 _Scanner nodes_라고 합니다.

오프라인 환경의 여러 사내 호스트에 BlueXP 분류 소프트웨어를 설치할 때는 다음 단계를 따르십시오.

필요한 것

- Manager 및 Scanner 노드의 모든 Linux 시스템이 을 충족하는지 확인합니다 호스트 요구 사항.
- 두 가지 필수 소프트웨어 패키지(Docker Engine 또는 Podman 및 Python 3)를 설치했는지 확인합니다.
- Linux 시스템에 대한 루트 권한이 있는지 확인합니다.
- 오프라인 환경이 필요한 를 충족하는지 확인합니다 사용 권한 및 연결.
- 사용하려는 스캐너 노드 호스트의 IP 주소가 있어야 합니다.
- 모든 호스트에서 다음 포트 및 프로토콜을 활성화해야 합니다.

포트	프로토콜	설명
2377	TCP	클러스터 관리 통신
7946	TCP, UDP	노드 간 통신
4789	UDP입니다	오버레이 네트워크 트래픽
50	ESP	암호화된 IPsec 오버레이 네트워크(ESP) 트래픽
111	TCP, UDP	호스트 간 파일 공유를 위한 NFS 서버(각 스캐너 노드에서 관리자 노드로 필요)
2049	TCP, UDP	호스트 간 파일 공유를 위한 NFS 서버(각 스캐너 노드에서 관리자 노드로 필요)

단계

1. 에서 1단계부터 8단계까지 수행합니다 "단일 호스트 설치" 관리자 노드에서.
2. 9단계에서 설명한 것처럼 설치 관리자가 메시지를 표시하면 일련의 프롬프트에 필요한 값을 입력하거나 설치 프로그램에 명령줄 인수로 필요한 매개 변수를 제공할 수 있습니다.

   단일 호스트 설치에 사용할 수 있는 변수 외에도 새 옵션 * -n<node_ip> * 를 사용하여 스캐너 노드의 IP 주소를 지정할 수 있습니다. 여러 노드 IP는 쉼표로 구분됩니다.

   예를 들어, 이 명령은 다음과 같이 3개의 스캐너 노드를 추가합니다.
   ```
   sudo ./install.sh -a <account_id> -c <client_id> -t <user_token> --host
   <ds_host> --manager-host <cm_host> -n <node_ip1>,<node_ip2>,<node_ip3> --no
   -proxy --darksite
   ```
3. 관리자 노드 설치가 완료되기 전에 스캐너 노드에 필요한 설치 명령이 대화 상자에 표시됩니다. 명령을 복사합니다(예: `sudo ./node_install.sh -m 10.11.12.13 -t ABCDEF-1-3u69m1-1s35212`)를 입력하고 텍스트 파일에 저장합니다.
4. 켜짐 * 각 * 스캐너 노드 호스트:
   a. Data Sense 설치 프로그램 파일(* cc_onpremise_installer.tar.gz *)을 호스트 컴퓨터에 복사합니다.
   b. 설치 프로그램 파일의 압축을 풉니다.
   c. 3단계에서 복사한 명령을 붙여 넣고 실행합니다.

      모든 스캐너 노드에서 설치가 완료되고 관리자 노드에 연결되었으면 관리자 노드 설치도 완료됩니다.

결과

BlueXP 분류 설치 프로그램이 패키지 설치를 완료하고 설치를 등록합니다. 설치에는 15 ~ 25분이 소요될 수 있습니다.

다음 단계

구성 페이지에서 로컬 을 선택할 수 있습니다 "온프레미스 ONTAP 클러스터" 및 로컬 "데이터베이스를 지원합니다" 선택합니다.

또한 가능합니다 "BlueXP 분류에 대한 BYOL 라이센스 설정" 현재 BlueXP 디지털 전자지갑에서 30일 무료 평가판이 종료될 때까지 요금이 부과되지 않습니다.

BlueXP 분류 소프트웨어를 업그레이드합니다

BlueXP 분류 소프트웨어는 정기적으로 새로운 기능으로 업데이트되므로 정기적으로 새로운 버전을 확인하여 최신 소프트웨어와 기능을 사용하고 있는지 확인해야 합니다. 업그레이드를 자동으로 수행하기 위한 인터넷 연결이 없기 때문에 BlueXP 분류 소프트웨어를 수동으로 업그레이드해야 합니다.

시작하기 전에

- BlueXP Connector 소프트웨어를 최신 버전으로 업그레이드하는 것이 좋습니다. "커넥터 업그레이드 단계를 참조하십시오".
- BlueXP 분류 버전 1.24부터 향후 모든 소프트웨어 버전으로 업그레이드할 수 있습니다.

  BlueXP 분류 소프트웨어가 1.24 이전 버전을 실행 중인 경우 한 번에 하나의 주요 버전만 업그레이드할 수 있습니다. 예를 들어, 버전 1.21.x가 설치되어 있는 경우 1.22.x로 업그레이드할 수 있습니다 몇 가지 주요 버전이 뒤쳐지면 소프트웨어를 여러 번 업그레이드해야 합니다.

단계

1. 인터넷 구성 시스템의 경우 에서 BlueXP 분류 소프트웨어를 다운로드합니다 "NetApp Support 사이트". 선택해야 하는 파일의 이름은 * DataSense-offline-bundle-<version>.tar.gz * 입니다.
2. 소프트웨어 번들을 Linux 호스트에 복사하면 BlueXP 분류가 다크 사이트에 설치됩니다.
3. 호스트 시스템에서 소프트웨어 번들의 압축을 풉니다. 예를 들면 다음과 같습니다.

   ```
   tar -xvf DataSense-offline-bundle-v1.25.0.tar.gz
   ```

   그러면 설치 파일 * cc_onpremise_installer.tar.gz * 가 추출됩니다.

4. 호스트 시스템에서 설치 파일의 압축을 풉니다. 예를 들면 다음과 같습니다.

   ```
   tar -xzf cc_onprem_installer.tar.gz
   ```

   그러면 업그레이드 스크립트 * start_darsite_upgrade.sh * 와 필요한 타사 소프트웨어가 추출됩니다.

5. 호스트 시스템에서 업그레이드 스크립트를 실행합니다. 예를 들면 다음과 같습니다.

   ```
   start_darksite_upgrade.sh
   ```

결과

BlueXP 분류 소프트웨어가 호스트에서 업그레이드됩니다. 업데이트는 5분에서 10분 정도 소요될 수 있습니다.

대규모 구성을 스캔하기 위해 여러 호스트 시스템에 BlueXP 분류를 배포한 경우에는 스캐너 노드에 업그레이드가 필요하지 않습니다.

BlueXP 분류 UI 페이지 하단에 있는 버전을 확인하여 소프트웨어가 업데이트되었는지 확인할 수 있습니다.

Linux 호스트가 BlueXP 분류를 설치할 준비가 되었는지 확인합니다

Linux 호스트에 수동으로 BlueXP 분류를 설치하기 전에 호스트에서 스크립트를 실행하여 BlueXP 분류를 설치하기 위한 모든 필수 구성 요소가 준비되어 있는지 확인할 수 있습니다. 이 스크립트는 네트워크의 Linux 호스트 또는 클라우드의 Linux 호스트에서 실행할 수 있습니다. 호스트를 인터넷에 연결하거나 호스트가 인터넷에 액세스할 수 없는 사이트(A_Dark site_)에 상주할 수 있습니다.

BlueXP 분류 설치 스크립트의 일부인 필수 테스트 스크립트도 있습니다. 여기에 설명된 스크립트는 BlueXP 분류 설치 스크립트를 실행하는 것과 독립적으로 Linux 호스트를 확인하려는 사용자를 위해 특별히 설계되었습니다.

시작하기

다음 작업을 수행합니다.

1. BlueXP 커넥터가 아직 설치되지 않은 경우 설치할 수도 있습니다. Connector를 설치하지 않고 테스트 스크립트를 실행할 수 있지만 스크립트는 Connector와 BlueXP 분류 호스트 시스템 간의 연결을 검사하므로 Connector를 사용하는 것이 좋습니다.
2. 호스트 시스템을 준비하고 모든 요구 사항을 충족하는지 확인합니다.
3. BlueXP 분류 호스트 시스템에서 아웃바운드 인터넷 액세스를 활성화합니다.
4. 모든 시스템에서 필요한 포트가 활성화되어 있는지 확인합니다.
5. 사전 필수 테스트 스크립트를 다운로드하고 실행합니다.

커넥터를 작성합니다

BlueXP 분류를 설치하고 사용하려면 먼저 BlueXP 커넥터가 필요합니다. 그러나 커넥터 없이 필수 구성 요소 스크립트를 실행할 수 있습니다.

가능합니다 "Connector On-Premises를 설치합니다" 네트워크의 Linux 호스트 또는 클라우드의 Linux 호스트 BlueXP 분류를 사내에서 설치하려는 일부 사용자는 Connector를 내부에 설치할 수도 있습니다.

클라우드 공급자 환경에 Connector를 만들려면 를 참조하십시오 "AWS에서 커넥터 생성", "Azure에서 커넥터 만들기", 또는 "GCP에서 커넥터를 생성하는 중입니다".

필수 구성 요소 스크립트를 실행할 때는 커넥터 시스템의 IP 주소 또는 호스트 이름이 필요합니다. 이 정보는 구내에 Connector를 설치한 경우 확인할 수 있습니다. Connector가 클라우드에 배포된 경우 BlueXP 콘솔에서 이 정보를 찾을 수 있습니다. 도움말 아이콘을 클릭하고 * 지원 * 을 선택한 다음 * BlueXP 커넥터 * 를 클릭합니다.

호스트 요구 사항을 확인합니다

BlueXP 분류 소프트웨어는 특정 운영 체제 요구 사항, RAM 요구 사항, 소프트웨어 요구 사항 등을 충족하는 호스트에서 실행해야 합니다.

- BlueXP 분류는 다른 애플리케이션과 공유되는 호스트에서는 지원되지 않습니다. 호스트는 전용 호스트여야 합니다.
- 구내 호스트 시스템을 구축할 때 BlueXP 분류 검사를 수행할 데이터 세트의 크기에 따라 세 가지 시스템 크기 중에서 선택할 수 있습니다.

시스템 크기	**CPU**	**RAM(**스왑 메모리는 비활성화 상태여야 함**)**	디스크
* 초대형 *	32개의 CPU	128GB RAM	/, 또는 의 1TiB SSD /opt에서 -100GiB를 사용할 수 있습니다 -895GiB는 /var/lib/docker에서 사용할 수 있습니다 /tmp에 -5GiB입니다
* 대형 *	CPU 16개	64GB RAM	500GiB SSD 켜짐/또는 /opt에서 -100GiB를 사용할 수 있습니다 /var/lib/docker에서 사용 가능한 395GiB /tmp에 -5GiB입니다
* 중간 *	CPU 8개	32GB RAM	200GiB SSD 켜짐/또는 /opt에서 -50GiB를 사용할 수 있습니다 /var/lib/docker에서 -145GiB를 사용할 수 있습니다 /tmp에 -5GiB입니다
* 소형 *	CPU 8개	16GB RAM	또는 에서 100GiB SSD /opt에서 -50GiB를 사용할 수 있습니다 /var/lib/docker에서 -45GiB를 사용할 수 있습니다 /tmp에 -5GiB입니다

소형 시스템을 사용할 때는 제한이 있습니다. 을 참조하십시오 "더 작은 인스턴스 유형 사용" 를 참조하십시오.

- BlueXP 분류 설치를 위해 클라우드에 컴퓨팅 인스턴스를 배포할 때는 위의 "대규모" 시스템 요구 사항을 충족하는 시스템을 권장합니다.
  - * AWS EC2 인스턴스 유형 *: "m6i.4xLarge"를 권장합니다. "추가 AWS 인스턴스 유형을 참조하십시오".
  - * Azure VM size *: "Standard_D16s_v3"을 권장합니다. "추가 Azure 인스턴스 유형을 참조하십시오".
  - * GCP 시스템 유형 *: "n2-standard-16"을 권장합니다. "추가 GCP 인스턴스 유형을 참조하십시오".
- UNIX 폴더 권한 *: 다음과 같은 최소 UNIX 권한이 필요합니다.

폴더	최소 권한
/tmp	`rwxrwxrwt`
/opt	`rwxr-xr-x`
/var/lib/docker입니다	`rwx------`

폴더	최소 권한
/usr/lib/systemd/system입니다	`rwxr-xr-x`

- * 운영 체제 *:
  - 다음 운영 체제에서는 Docker 컨테이너 엔진을 사용해야 합니다.
    - Red Hat Enterprise Linux 버전 7.8 및 7.9
    - CentOS 버전 7.8 및 7.9
    - Ubuntu 22.04(BlueXP 분류 버전 1.23 이상 필요)
  - 다음 운영 체제에는 Podman 컨테이너 엔진을 사용해야 하며 BlueXP 분류 버전 1.30 이상이 필요합니다.
    - Red Hat Enterprise Linux 버전 8.8, 9.0, 9.1, 9.2 및 9.3

      RHEL 8.x 및 RHEL 9.x를 사용하는 경우 다음 기능은 현재 지원되지 않습니다.

      - 어두운 장소에 설치
      - 분산 스캔, 마스터 스캐너 노드 및 원격 스캐너 노드 사용
- * Red Hat 서브스크립션 관리 *: 호스트는 Red Hat 서브스크립션 관리 에 등록되어 있어야 합니다. 등록되지 않은 경우 설치 중에 시스템에서 필요한 타사 소프트웨어를 업데이트하기 위해 리포지토리에 액세스할 수 없습니다.
- * 추가 소프트웨어 *: BlueXP 분류를 설치하기 전에 호스트에 다음 소프트웨어를 설치해야 합니다.
  - 사용 중인 OS에 따라 컨테이너 엔진 중 하나를 설치해야 합니다.
    - Docker Engine 버전 19.3.1 이상 "설치 지침을 봅니다".

      "이 비디오 시청" CentOS에 Docker를 설치하는 빠른 데모를 보려면

    - Podman 버전 4 이상 Podman을 설치하려면 시스템 패키지를 업데이트하십시오 (`sudo yum update -y`)를 클릭한 다음 Podman을 설치합니다 (`sudo yum install netavark -y`)를 클릭합니다.
- Python 버전 3.6 이상. "설치 지침을 봅니다".
  - * NTP 고려 사항 *: NetApp에서는 NTP(네트워크 시간 프로토콜) 서비스를 사용하도록 BlueXP 분류 시스템을 구성할 것을 권장합니다. BlueXP 분류 시스템과 BlueXP Connector 시스템 간에 시간을 동기화해야 합니다.
  - * Firewalld 고려 사항 *: 사용하려는 경우 `firewalld`BlueXP 분류를 설치하기 전에 활성화하는 것이 좋습니다. 다음 명령을 실행하여 구성합니다 `firewalld` 따라서 BlueXP 분류와 호환됩니다.

    ```
    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 BlueXP 분류 호스트를 스캐너 노드(분산 모델)로 사용할 계획이라면 이 규칙을 주 시스템에 추가하십시오.

```
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 활성화 또는 업데이트할 때마다 다시 시작해야 합니다 `firewalld` 설정.

BlueXP 분류에서 아웃바운드 인터넷 액세스를 활성화합니다

BlueXP 분류에는 아웃바운드 인터넷 액세스가 필요합니다. 가상 또는 물리적 네트워크에서 인터넷 액세스에 프록시 서버를 사용하는 경우 BlueXP 분류 인스턴스에 다음 엔드포인트에 연결할 수 있는 아웃바운드 인터넷 액세스 권한이 있는지 확인합니다.

인터넷에 연결되지 않은 사이트에 설치된 호스트 시스템에는 이 섹션이 필요하지 않습니다.

엔드포인트	목적
https://api.bluexp.netapp.com 으로 문의하십시오	NetApp 계정을 포함한 BlueXP 서비스와 통신합니다.
https://netapp-cloud-account.auth0.com https://auth0.com 으로 문의하십시오	BlueXP 웹 사이트와 통신하여 중앙 집중식 사용자 인증.
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 액세스하고 로그 및 메트릭을 보낼 수 있습니다.
https://support.compliance.api.bluexp.netapp.com/ 으로 문의하십시오	NetApp에서 감사 레코드의 데이터를 스트리밍할 수 있습니다.
https://github.com/docker https://download.docker.com 으로 문의하십시오	Docker 설치를 위한 사전 필수 패키지를 제공합니다.
http://mirror.centos.org http://mirrorlist.centos.org http://mirror.centos.org/centos/7/extras/x86_64/Packages/container-selinux-2.107-3.el7.noarch.rpm 를 참조하십시오	CentOS 설치를 위한 필수 패키지를 제공합니다.
http://packages.ubuntu.com/ http://archive.ubuntu.com	Ubuntu 설치를 위한 필수 패키지를 제공합니다.

필요한 모든 포트가 활성화되어 있는지 확인합니다

커넥터, BlueXP 분류, Active Directory 및 데이터 소스 간의 통신에 필요한 모든 포트가 열려 있는지 확인해야 합니다.

연결 유형	포트	설명
커넥터 <>BlueXP 분류	8080(TCP), 443(TCP) 및 80	Connector의 방화벽 또는 라우팅 규칙은 포트 443을 통해 BlueXP 분류 인스턴스 간에 인바운드 및 아웃바운드 트래픽을 허용해야 합니다. 포트 8080이 열려 있는지 확인하여 BlueXP에서 설치 진행률을 확인합니다.
커넥터 <>ONTAP 클러스터(NAS)	443(TCP)	BlueXP는 HTTPS를 사용하여 ONTAP 클러스터를 검색합니다. 사용자 지정 방화벽 정책을 사용하는 경우 커넥터 호스트는 포트 443을 통한 아웃바운드 HTTPS 액세스를 허용해야 합니다. Connector가 클라우드에 있는 경우 모든 아웃바운드 통신은 사전 정의된 방화벽 또는 라우팅 규칙으로 허용됩니다.

BlueXP 분류 필수 구성 요소 스크립트를 실행합니다

다음 단계에 따라 BlueXP 분류 전제 조건 스크립트를 실행합니다.

"이 비디오 시청" 필수 구성 요소 스크립트를 실행하고 결과를 해석하는 방법을 확인합니다.

필요한 것

- Linux 시스템이 를 충족하는지 확인합니다 호스트 요구 사항.
- 시스템에 2개의 필수 소프트웨어 패키지(Docker Engine 또는 Podman 및 Python 3)가 설치되어 있는지 확인합니다.
- Linux 시스템에 대한 루트 권한이 있는지 확인합니다.

단계

1. 에서 BlueXP 분류 필수 구성 요소 스크립트를 다운로드합니다 "NetApp Support 사이트". 선택해야 하는 파일의 이름은 * standalone-pre-requised-tester-<version> * 입니다.
2. 사용할 Linux 호스트에 파일을 복사합니다(사용) `scp` 또는 다른 방법 참조).
3. 스크립트를 실행할 권한을 할당합니다.

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

4. 다음 명령을 사용하여 스크립트를 실행합니다.

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

   인터넷 액세스가 없는 호스트에서 스크립트를 실행하는 경우에만 "--car사이트" 옵션을 추가합니다. 호스트가 인터넷에 연결되어 있지 않으면 특정 필수 구성 요소 테스트를 건너뜁니다.

5. 이 스크립트는 BlueXP 분류 호스트 시스템의 IP 주소를 묻는 메시지를 표시합니다.
   - IP 주소 또는 호스트 이름을 입력합니다.
6. 이 스크립트에는 BlueXP Connector가 설치되어 있는지 여부를 묻는 메시지가 표시됩니다.

- 커넥터가 설치되어 있지 않으면 * N * 을 입력하십시오.
- 커넥터가 설치된 경우 * Y * 를 입력합니다. 그런 다음 테스트 스크립트가 이 연결을 테스트할 수 있도록 BlueXP Connector의 IP 주소 또는 호스트 이름을 입력합니다.

7. 이 스크립트는 시스템에서 다양한 테스트를 실행하고 진행되면서 결과를 표시합니다. 작업이 완료되면 세션 로그를 라는 파일에 씁니다 `prerequisites-test-<timestamp>.log` 디렉토리에 있습니다 `/opt/netapp/install_logs`.

결과

모든 필수 구성 요소 테스트가 성공적으로 실행된 경우 준비가 되면 호스트에 BlueXP 분류를 설치할 수 있습니다.

발견된 문제가 있는 경우 "권장" 또는 "필수"로 분류하여 해결합니다. 권장 문제는 일반적으로 BlueXP 분류 검사 및 분류 작업의 실행 속도를 느리게 만드는 항목입니다. 이러한 항목은 수정할 필요가 없지만, 이를 해결할 수 있습니다.

"필수" 문제가 있는 경우 문제를 해결하고 사전 요구 사항 테스트 스크립트를 다시 실행해야 합니다.

저작권 정보

Copyright © 2024 NetApp, Inc. All Rights Reserved. 미국에서 인쇄된 본 문서의 어떠한 부분도 저작권 소유자의 사전 서면 승인 없이는 어떠한 형식이나 수단(복사, 녹음, 녹화 또는 전자 검색 시스템에 저장하는 것을 비롯한 그래픽, 전자적 또는 기계적 방법)으로도 복제될 수 없습니다.

NetApp이 저작권을 가진 자료에 있는 소프트웨어에는 아래의 라이센스와 고지사항이 적용됩니다.

본 소프트웨어는 NetApp에 의해 '있는 그대로' 제공되며 상품성 및 특정 목적에의 적합성에 대한 명시적 또는 묵시적 보증을 포함하여(이에 제한되지 않음) 어떠한 보증도 하지 않습니다. NetApp은 대체품 또는 대체 서비스의 조달, 사용 불능, 데이터 손실, 이익 손실, 영업 중단을 포함하여(이에 국한되지 않음), 이 소프트웨어의 사용으로 인해 발생하는 모든 직접 및 간접 손해, 우발적 손해, 특별 손해, 징벌적 손해, 결과적 손해의 발생에 대하여 그 발생 이유, 책임론, 계약 여부, 엄격한 책임, 불법 행위(과실 또는 그렇지 않은 경우)와 관계없이 어떠한 책임도 지지 않으며, 이와 같은 손실의 발생 가능성이 통지되었다 하더라도 마찬가지입니다.

NetApp은 본 문서에 설명된 제품을 언제든지 예고 없이 변경할 권리를 보유합니다. NetApp은 NetApp의 명시적인 서면 동의를 받은 경우를 제외하고 본 문서에 설명된 제품을 사용하여 발생하는 어떠한 문제에도 책임을 지지 않습니다. 본 제품의 사용 또는 구매의 경우 NetApp에서는 어떠한 특허권, 상표권 또는 기타 지적 재산권이 적용되는 라이센스도 제공하지 않습니다.

본 설명서에 설명된 제품은 하나 이상의 미국 특허, 해외 특허 또는 출원 중인 특허로 보호됩니다.

제한적 권리 표시: 정부에 의한 사용, 복제 또는 공개에는 DFARS 252.227-7013(2014년 2월) 및 FAR 52.227-19(2007년 12월)의 기술 데이터-비상업적 품목에 대한 권리(Rights in Technical Data -Noncommercial Items) 조항의 하위 조항 (b)(3)에 설명된 제한사항이 적용됩니다.

여기에 포함된 데이터는 상업용 제품 및/또는 상업용 서비스(FAR 2.101에 정의)에 해당하며 NetApp, Inc.의 독점 자산입니다. 본 계약에 따라 제공되는 모든 NetApp 기술 데이터 및 컴퓨터 소프트웨어는 본질적으로 상업용이며 개인 비용만으로 개발되었습니다. 미국 정부는 데이터가 제공된 미국 계약과 관련하여 해당 계약을 지원하는 데에만 데이터에 대한 전 세계적으로 비독점적이고 양도할 수 없으며 재사용이 불가능하며 취소 불가능한 라이센스를 제한적으로 가집니다. 여기에 제공된 경우를 제외하고 NetApp, Inc.의 사전 서면 승인 없이는 이 데이터를 사용, 공개, 재생산, 수정, 수행 또는 표시할 수 없습니다. 미국 국방부에 대한 정부 라이센스는 DFARS 조항 252.227-7015(b)(2014년 2월)에 명시된 권한으로 제한됩니다.

상표 정보

NETAPP, NETAPP 로고 및 http://www.netapp.com/TM에 나열된 마크는 NetApp, Inc.의 상표입니다. 기타 회사 및 제품 이름은 해당 소유자의 상표일 수 있습니다.