



BlueXP 관리

Setup and administration

NetApp
April 26, 2024

목차

- BlueXP 관리 1
 - BlueXP에서 ID 페더레이션 사용 1
 - BlueXP 계정 6
 - 커넥터 21
 - 자격 증명 및 구독 39

BlueXP 관리

BlueXP에서 ID 페더레이션 사용

ID 페더레이션 사용자가 회사 ID의 자격 증명을 사용하여 로그인할 수 있도록 BlueXP에서 단일 로그인을 활성화합니다. 시작하려면 ID 페더레이션이 BlueXP와 작동하는 방식에 대해 알아보고 설치 프로세스의 개요를 검토하십시오.

NSS 자격 증명을 사용한 ID 페더레이션

NetApp Support 사이트(NSS) 자격 증명을 사용하여 BlueXP에 로그인하는 경우 이 페이지의 지침에 따라 ID 페더레이션을 설정해서는 안 됩니다. 대신 다음을 수행해야 합니다.

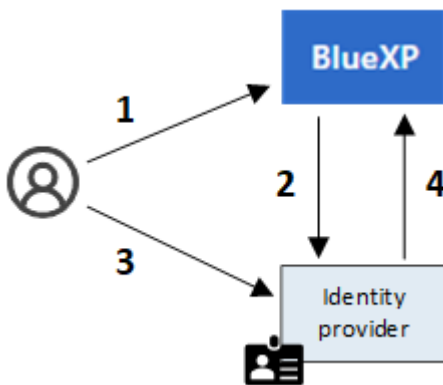
- 를 다운로드하고 완료합니다 "[NetApp 통합 요청 양식](#)"
- 양식에 지정된 이메일 주소로 양식을 제출합니다

NetApp ID 및 액세스 관리 팀에서 요청을 검토합니다.

ID 페더레이션의 작동 방식

ID 페더레이션을 설정하면 BlueXP의 인증 서비스 공급자(auth0)와 사용자 고유의 ID 관리 공급자 간에 트러스트 연결이 만들어집니다.

다음 이미지는 BlueXP에서 ID 페더레이션이 작동하는 방식을 보여 줍니다.



1. 사용자가 BlueXP 로그인 페이지에 이메일 주소를 입력합니다.
2. BlueXP는 전자 메일 도메인이 통합 연결의 일부임을 확인하고 신뢰할 수 있는 연결을 사용하여 인증 요청을 ID 공급자에게 보냅니다.

통합 연결을 설정할 때 BlueXP는 항상 해당 통합 연결을 인증에 사용합니다.

3. 사용자는 회사 디렉터리의 자격 증명을 사용하여 인증합니다.
4. ID 공급자가 사용자의 ID를 인증하고 사용자가 BlueXP에 로그인되어 있습니다.

ID 페더레이션은 SAML(Security Assertion Markup Language 2.0) 및 OIDC(OpenID Connect)와 같은 공개 표준을 사용합니다.

지원되는 ID 공급자

BlueXP는 다음과 같은 ID 공급자를 지원합니다.

- SAML(Security Assertion Markup Language) ID 공급자
- Microsoft Entra ID입니다
- ADFS(Active Directory Federation Services)
- PingFederate(PingFederate)

BlueXP는 서비스 공급업체에서 시작한(SP 시작) SSO만 지원합니다. ID 공급자 시작(IDP 시작) SSO는 지원되지 않습니다.


설치 프로세스 개요


BlueXP와 ID 관리 공급자 간의 연결을 설정하기 전에 그에 따라 준비할 수 있도록 해야 할 단계를 이해해야 합니다.

다음 단계는 NetApp 클라우드 로그인을 사용하여 BlueXP에 로그인하는 사용자를 위한 것입니다. NSS 자격 증명을 사용하여 BlueXP에 로그인하는 경우 [NSS 자격 증명으로 ID 페더레이션을 설정하는 방법에 대해 알아봅니다](#).

SAML ID 공급자


BlueXP와 SAML ID 공급자 간의 페더레이션 연결을 설정하는 단계는 다음과 같습니다.


단계	완료자	설명
1	AD(Active Directory) 관리자	<p>BlueXP에서 ID 페더레이션을 사용하도록 SAML ID 공급자를 구성합니다.</p> <p>SAML ID 공급자에 대한 지침 보기:</p> <ul style="list-style-type: none">• "고급"• "오타"• "OneLogin"• "PingFederate(PingFederate)"• "Salesforce를 참조하십시오"• "사이트 마인더"• "SSOCircle" <p>ID 공급자가 위의 목록에 나타나지 않으면 "다음 일반 지침을 따르십시오"</p> <div> auth0에서 연결을 만드는 방법을 설명하는 단계를 _NOT_ 완료하십시오. 다음 단계에서 해당 연결을 만듭니다.</div>

단계	완료자	설명
2	BlueXP 관리자	<p>로 이동합니다 "NetApp Federation 설정 페이지" 그리고 BlueXP와의 연결을 생성합니다.</p> <p>이 단계를 완료하려면 AD 관리자로부터 ID 공급자에 대한 다음 정보를 얻어야 합니다.</p> <ul style="list-style-type: none"> • 로그인 URL • X509 서명 인증서(PEM 또는 CER 형식) • 로그아웃 URL(선택 사항) <p>이 정보를 사용하여 연결을 만든 후 페더레이션 설정 페이지에는 다음 단계에서 구성을 완료하기 위해 AD 관리자에게 보낼 수 있는 매개 변수가 나열됩니다.</p> <div>  <p>인증서 만료 날짜를 기록해 둡니다. Federation Setup 페이지로 돌아가서 certificate_before_it_expires를 업데이트해야 합니다. 이것은 여러분의 책임입니다. BlueXP는 만료 날짜를 추적하지 않습니다. AD 팀과 함께 시간을 두고 알림을 받는 것이 가장 좋습니다.</p> </div>
3	AD 관리자	2단계를 완료한 후 페더레이션 설정 페이지에 표시된 매개 변수를 사용하여 ID 공급자에 대한 구성을 완료합니다.
4	BlueXP 관리자	<p>에서 연결을 테스트하고 활성화합니다 "NetApp Federation 설정 페이지"</p> <p>연결 테스트와 연결 설정 간에 페이지가 새로 고쳐집니다.</p>

Microsoft Entra ID입니다


BlueXP와 Microsoft Entra ID 간에 페더레이션 연결을 설정하는 단계는 다음과 같습니다.

단계	완료자	설명
1	AD 관리자	<p>BlueXP와 ID 통합을 지원하도록 Microsoft Entra ID를 구성합니다.</p> <p>"Microsoft Entra ID로 응용 프로그램을 등록하는 방법에 대한 지침을 봅니다"</p> <div>  <p>auth0에서 연결을 만드는 방법을 설명하는 단계를 <u>NOT</u> 완료하십시오. 다음 단계에서 해당 연결을 만듭니다.</p> </div>

단계	완료자	설명
2	BlueXP 관리자	<p>로 이동합니다 "NetApp Federation 설정 페이지" 그리고 BlueXP와의 연결을 생성합니다.</p> <p>이 단계를 완료하려면 AD 관리자로부터 다음 정보를 얻어야 합니다.</p> <ul style="list-style-type: none"> • 클라이언트 ID입니다 • 클라이언트 암호 값입니다 • Microsoft Entra ID 도메인입니다 <p>이 정보를 사용하여 연결을 만든 후 페더레이션 설정 페이지에는 다음 단계에서 구성을 완료하기 위해 AD 관리자에게 보낼 수 있는 매개 변수가 나열됩니다.</p> <div>  <p>비밀 키 만료 날짜를 기록해 두십시오. Federation Setup 페이지로 돌아가서 <code>certificate_before_it_expires</code>를 업데이트해야 합니다. 이것은 여러분의 책임입니다. BlueXP는 만료 날짜를 추적하지 않습니다. AD 팀과 함께 시간을 두고 알림을 받는 것이 가장 좋습니다.</p> </div>
3	AD 관리자	2단계를 완료한 후 페더레이션 설정 페이지에 표시된 매개 변수를 사용하여 Microsoft Entra ID에서 구성을 완료합니다.
4	BlueXP 관리자	<p>에서 연결을 테스트하고 활성화합니다 "NetApp Federation 설정 페이지"</p> <p>연결 테스트와 연결 설정 간에 페이지가 새로 고쳐집니다.</p>

고급

BlueXP와 ADFS 간의 통합 연결을 설정하는 단계는 다음과 같습니다.

단계	완료자	설명
1	AD 관리자	<p>BlueXP에서 ID 페더레이션을 사용하도록 ADFS 서버를 구성합니다.</p> <p>"auth0으로 ADFS 서버를 구성하기 위한 지침을 봅니다"</p>
2	BlueXP 관리자	<p>로 이동합니다 "NetApp Federation 설정 페이지" 그리고 BlueXP와의 연결을 생성합니다.</p> <p>이 단계를 완료하려면 AD 관리자로부터 ADFS 서버의 URL 또는 페더레이션 메타데이터 파일을 얻어야 합니다.</p> <p>이 정보를 사용하여 연결을 만든 후 페더레이션 설정 페이지에는 다음 단계에서 구성을 완료하기 위해 AD 관리자에게 보낼 수 있는 매개 변수가 나열됩니다.</p> <div>  <p>인증서 만료 날짜를 기록해 둡니다. Federation Setup 페이지로 돌아가서 <code>certificate_before_it_expires</code>를 업데이트해야 합니다. 이것은 여러분의 책임입니다. BlueXP는 만료 날짜를 추적하지 않습니다. AD 팀과 함께 시간을 두고 알림을 받는 것이 가장 좋습니다.</p> </div>

단계	완료자	설명
3	AD 관리자	2단계를 완료한 후 페더레이션 설정 페이지에 표시된 매개 변수를 사용하여 ADFS 서버의 구성을 완료합니다.
4	BlueXP 관리자	에서 연결을 테스트하고 활성화합니다 "NetApp Federation 설정 페이지" 연결 테스트와 연결 설정 간에 페이지가 새로 고쳐집니다.

PingFederate(PingFederate)

BlueXP와 PingFederate 서버 간의 통합 연결을 설정하는 단계는 다음과 같습니다.

단계	완료자	설명
1	AD 관리자	BlueXP에서 ID 페더레이션을 사용하도록 PingFederate 서버를 구성합니다. "연결 생성에 대한 지침을 봅니다" <div>  <p>auth0에서 연결을 만드는 방법을 설명하는 단계를 _NOT_ 완료하십시오. 다음 단계에서 해당 연결을 만듭니다.</p> </div>
2	BlueXP 관리자	로 이동합니다 "NetApp Federation 설정 페이지" 그리고 BlueXP와의 연결을 생성합니다. 이 단계를 완료하려면 AD 관리자로부터 다음 정보를 얻어야 합니다. <ul style="list-style-type: none"> • PingFederate 서버의 URL입니다 • X509 서명 인증서(PEM 또는 CER 형식) 이 정보를 사용하여 연결을 만든 후 페더레이션 설정 페이지에는 다음 단계에서 구성을 완료하기 위해 AD 관리자에게 보낼 수 있는 매개 변수가 나열됩니다. <div>  <p>인증서 만료 날짜를 기록해 둡니다. Federation Setup 페이지로 돌아가서 certificate_before_it_expires를 업데이트해야 합니다. 이것은 여러분의 책임입니다. BlueXP는 만료 날짜를 추적하지 않습니다. AD 팀과 함께 시간을 두고 알림을 받는 것이 가장 좋습니다.</p> </div>
3	AD 관리자	2단계를 완료한 후 페더레이션 설정 페이지에 표시된 매개 변수를 사용하여 PingFederate 서버의 구성을 완료합니다.
4	BlueXP 관리자	에서 연결을 테스트하고 활성화합니다 "NetApp Federation 설정 페이지" 연결 테스트와 연결 설정 간에 페이지가 새로 고쳐집니다.

통합 연결을 업데이트하는 중입니다

BlueXP 관리자가 연결을 설정한 후 관리자는 에서 언제든지 연결을 업데이트할 수 있습니다 ["NetApp Federation 설정 페이지"](#)

예를 들어 새 인증서를 업로드하여 연결을 업데이트해야 할 수 있습니다.

연결을 만든 BlueXP 관리자는 연결을 업데이트할 수 있는 권한이 있는 유일한 사용자입니다. 관리자를 추가하려면 NetApp Support에 문의하십시오.

BlueXP 계정

BlueXP 계정을 관리합니다

BlueXP 계정을 만들면 단일 관리자 사용자와 작업 영역만 포함됩니다. 사용자를 추가하고, 자동화를 위해 서비스 계정을 만들고, 작업 영역을 추가하는 등의 방법으로 조직의 요구에 맞게 계정을 관리할 수 있습니다.

["BlueXP 계정의 작동 방식에 대해 알아보십시오."](#)

Tenancy API로 계정을 관리합니다

API 요청을 전송하여 계정 설정을 관리하려면 `_Tenancy_API`를 사용해야 합니다. 이 API는 Cloud Volumes ONTAP 작업 환경을 만들고 관리하는 데 사용하는 BlueXP API와 다릅니다.

["Tenancy API에 대한 끝점을 봅니다"](#)

사용자 생성 및 관리

계정의 사용자는 특정 작업 영역의 리소스에 액세스하고 관리할 수 있습니다.

사용자 추가

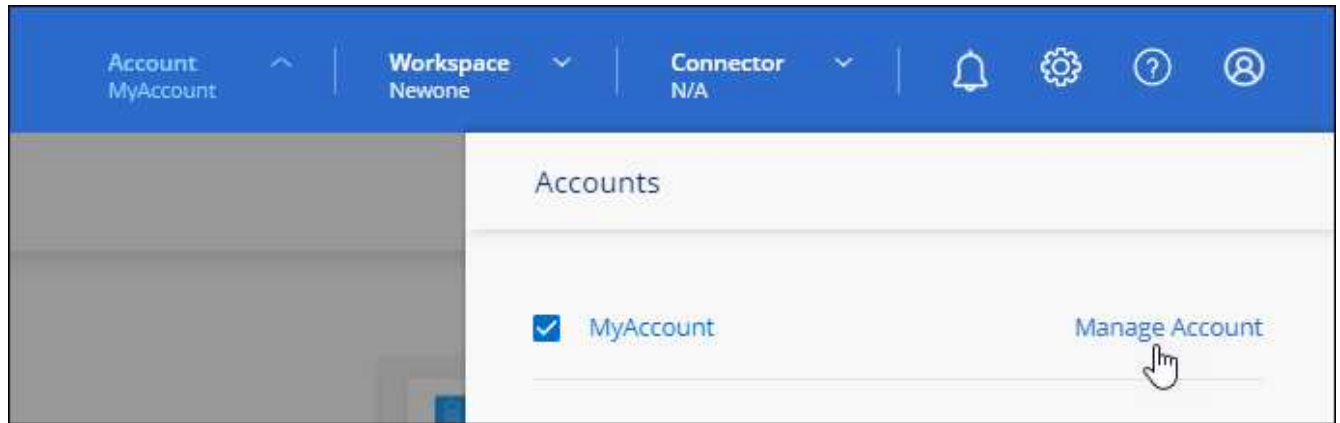
BlueXP 사용자가 BlueXP에서 작업 환경을 만들고 관리할 수 있도록 사용자를 BlueXP 계정과 연결합니다.

단계

1. 사용자가 아직 이 작업을 수행하지 않은 경우 사용자에게 로 이동하라고 요청합니다 ["NetApp BlueXP 웹 사이트"](#)를 클릭합니다.
2. BlueXP 상단에서 * 계정 * 드롭다운을 선택합니다.



3. 현재 선택한 계정 옆에 있는 * 계정 관리 * 를 선택합니다.



4. 구성원 탭에서 * 사용자 연결 * 을 선택합니다.
5. 사용자의 이메일 주소를 입력하고 사용자의 역할을 선택합니다.
 - * 계정 관리자 *: BlueXP에서 모든 작업을 수행할 수 있습니다.
 - * Workspace Admin *: 할당된 작업 영역에서 리소스를 만들고 관리할 수 있습니다.
 - * Compliance Viewer *: BlueXP 분류에 대한 규정 준수 정보만 볼 수 있고 액세스 권한이 있는 작업 영역에 대한 보고서를 생성할 수 있습니다.
6. 작업 영역 관리자 또는 규정 준수 뷰어를 선택한 경우 해당 사용자와 연결할 작업 영역을 하나 이상 선택합니다.



The image shows a web-based dialog box titled "Associate User". At the top, there is a user icon. Below the title, a light blue banner contains the text: "To add a user to your NetApp Cloud Account, that user must already have signed up at [NetApp Cloud Central](#). Enter the email address that they used when signing up with Cloud Central." The main form area has three sections: "User's Email" with a text input field containing "test@netapp.com"; "Role" with a dropdown menu showing "Workspace Admin"; and "Associate User to Workspaces" with a dropdown menu showing "Workspace-1" and a close button (X). At the bottom, there are two buttons: a grey "Cancel" button and a blue "Associate User" button.

7. Associate * 를 선택합니다.

결과

사용자는 NetApp BlueXP의 "Account Association"이라는 제목의 이메일을 받아야 합니다. 이메일에는 BlueXP에 액세스하는 데 필요한 정보가 포함되어 있습니다.

사용자를 제거합니다

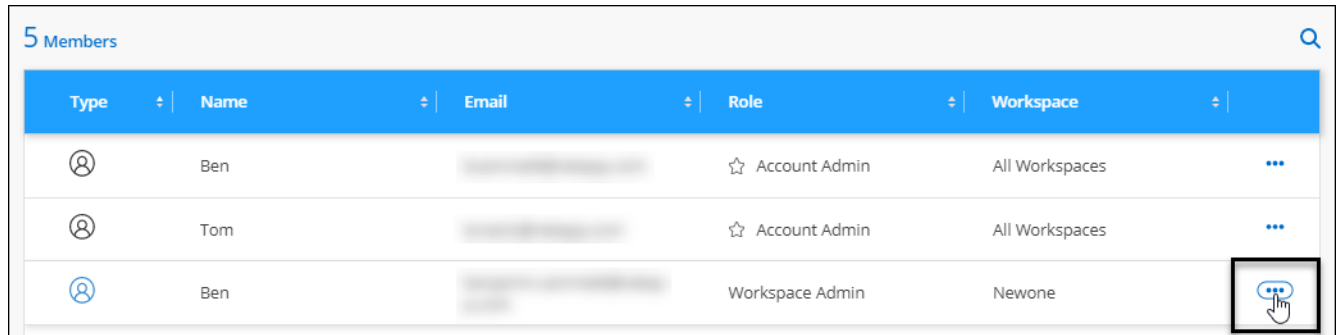
BlueXP 계정의 리소스에 더 이상 액세스할 수 없도록 사용자를 연결 해제합니다.

단계

1. BlueXP 상단에서 * 계정 * 드롭다운을 선택하고 * 계정 관리 * 를 선택합니다.



2. 구성원 탭의 해당 행에 있는 작업 메뉴를 선택합니다.



3. 사용자 연결 해제 * 를 선택하고 * 연결 해제 * 를 선택하여 확인합니다.

결과

사용자는 더 이상 이 BlueXP 계정의 리소스에 액세스할 수 없습니다.

작업 영역 관리자의 작업 영역을 관리합니다

언제든지 Workspace Admins를 작업 영역과 연결 및 연결 해제할 수 있습니다. 사용자를 연결하면 해당 작업 영역에서 작업 환경을 만들고 볼 수 있습니다.



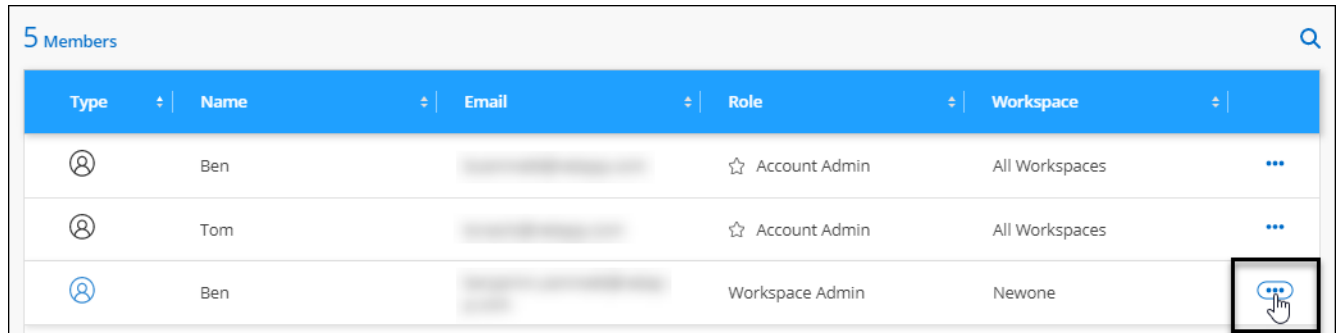
또한 Workspace 관리자가 BlueXP에서 해당 작업 영역에 액세스할 수 있도록 Connector를 작업 영역과 연결해야 합니다. "[Connector의 작업 영역을 관리하는 방법에 대해 알아봅니다](#)".

단계

1. BlueXP 상단에서 * 계정 * 드롭다운을 선택하고 * 계정 관리 * 를 선택합니다.



2. 구성원 탭의 해당 행에 있는 작업 메뉴를 선택합니다.



3. 작업 공간 관리 * 를 선택합니다.

4. 사용자와 연결할 작업 영역을 선택하고 * 적용 * 을 선택합니다.

결과

이제 사용자는 Connector가 작업 영역과 연결되어 있는 한 BlueXP에서 해당 작업 영역에 액세스할 수 있습니다.

서비스 계정 생성 및 관리

서비스 계정은 자동화를 위해 BlueXP에 인증된 API 호출을 수행할 수 있는 "사용자" 역할을 합니다. 따라서 언제든지 퇴사할 수 있는 실제 사용자의 계정을 기반으로 자동화 스크립트를 작성할 필요가 없으므로 자동화를 더욱 쉽게 관리할 수 있습니다.

다른 BlueXP 사용자와 마찬가지로 서비스 계정에 역할을 할당하여 서비스 계정에 권한을 부여합니다. 또한 서비스 계정을 특정 작업 영역에 연결하여 서비스가 액세스할 수 있는 작업 환경(리소스)을 제어할 수도 있습니다.

서비스 계정을 만들 때 BlueXP에서 서비스 계정에 대한 클라이언트 ID 및 클라이언트 암호를 복사하거나 다운로드할 수 있습니다. 이 키 쌍은 BlueXP의 인증에 사용됩니다.

서비스 계정을 사용할 때는 API 작업에 새로 고침 토큰이 필요하지 않습니다. ["토큰 새로 고침 에 대해 알아봅니다"](#)

서비스 계정을 생성합니다

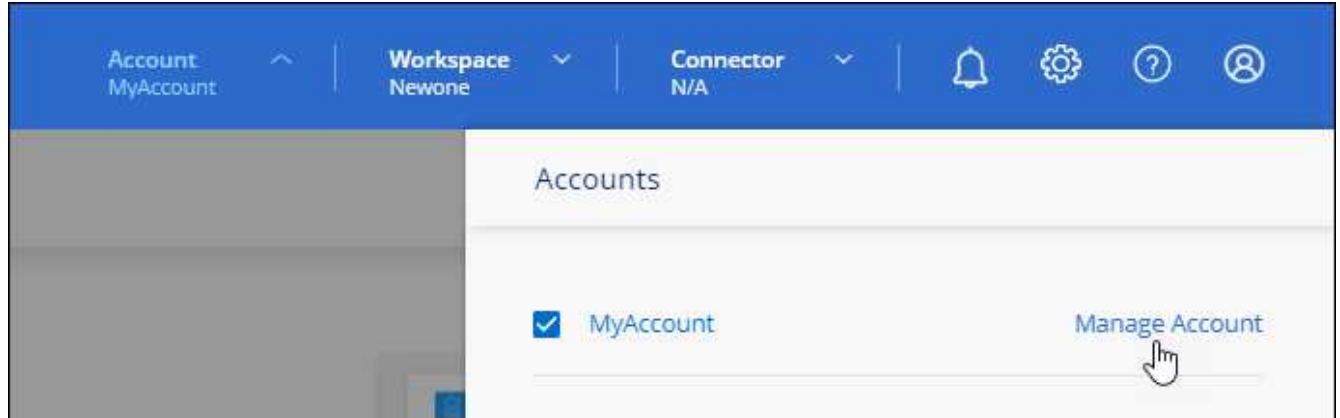
작업 환경의 리소스를 관리하는 데 필요한 만큼 서비스 계정을 만듭니다.

단계

1. BlueXP 상단에서 * 계정 * 드롭다운을 선택합니다.



2. 현재 선택한 계정 옆에 있는 * 계정 관리 * 를 선택합니다.



3. 구성원 탭에서 * 서비스 계정 생성 * 을 선택합니다.
4. 이름을 입력하고 역할을 선택합니다. 계정 관리자 이외의 역할을 선택한 경우 이 서비스 계정과 연결할 작업 영역을 선택합니다.
5. Create * 를 선택합니다.
6. 클라이언트 ID 및 클라이언트 암호를 복사하거나 다운로드합니다.

클라이언트 암호는 한 번만 볼 수 있으며 BlueXP에서 저장할 수 없습니다. 암호를 복사하거나 다운로드한 후 안전하게 보관하십시오.

7. 닫기 * 를 선택합니다.

서비스 계정에 대한 베어러 토큰을 얻습니다

를 API 호출하기 위해 "테넌시 API" 서비스 계정에 대한 베어러 토큰을 얻어야 합니다.

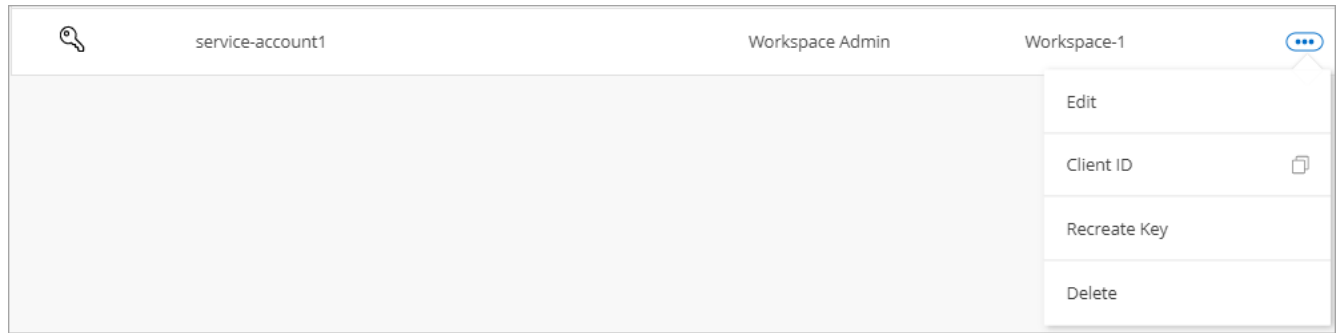
"서비스 계정 토큰을 만드는 방법에 대해 알아보십시오"

클라이언트 ID를 복사합니다

서비스 계정의 클라이언트 ID는 언제든지 복사할 수 있습니다.

단계

1. 구성원 탭의 서비스 계정에 해당하는 행에서 작업 메뉴를 선택합니다.



2. 클라이언트 ID * 를 선택합니다.

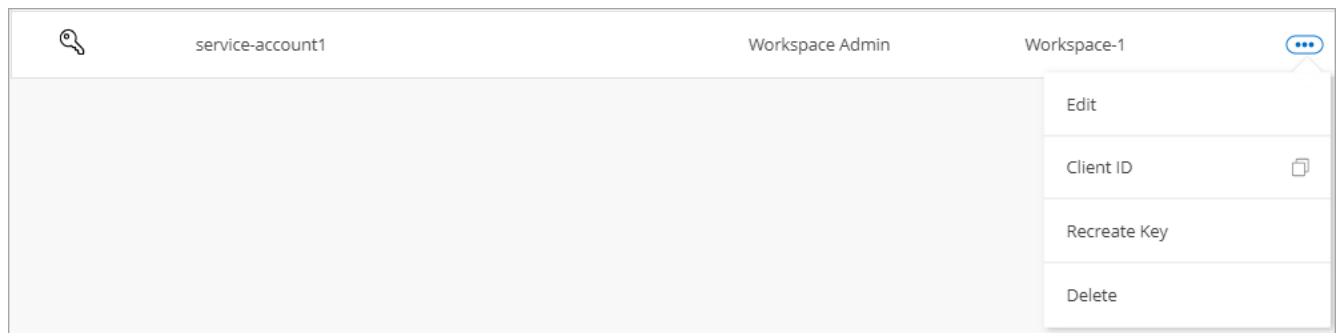
3. ID가 클립보드에 복사됩니다.

키를 다시 생성합니다

키를 다시 생성하면 이 서비스 계정의 기존 키가 삭제되며 새 키가 생성됩니다. 이전 키를 사용할 수 없습니다.

단계

1. 구성원 탭의 서비스 계정에 해당하는 행에서 작업 메뉴를 선택합니다.



2. 키 재생성 * 을 선택합니다.

3. reate * 를 선택하여 확인합니다.

4. 클라이언트 ID 및 클라이언트 암호를 복사하거나 다운로드합니다.

클라이언트 암호는 한 번만 볼 수 있으며 BlueXP에서 저장할 수 없습니다. 암호를 복사하거나 다운로드한 후 안전하게 보관하십시오.

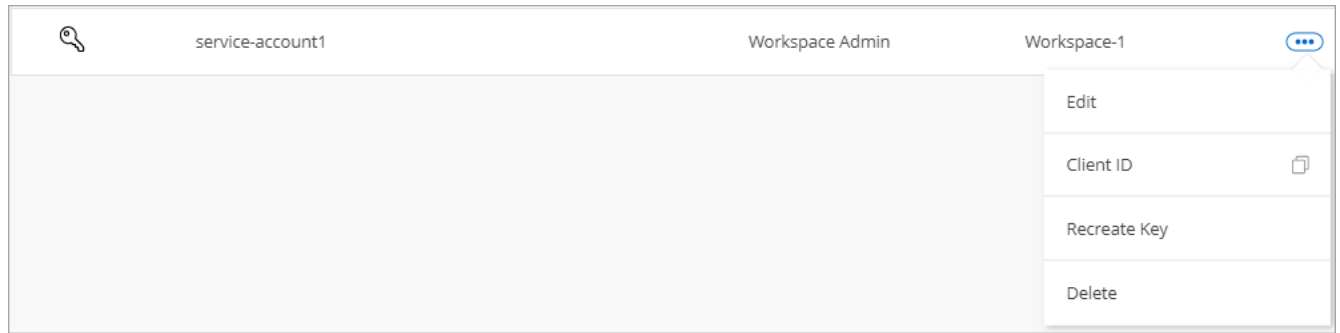
5. 닫기 * 를 선택합니다.

서비스 계정을 삭제합니다

더 이상 사용할 필요가 없는 경우 서비스 계정을 삭제합니다.

단계

1. 구성원 탭의 서비스 계정에 해당하는 행에서 작업 메뉴를 선택합니다.



2. 삭제 * 를 선택합니다.
3. 확인하려면 * 삭제 * 를 다시 선택합니다.

작업 영역을 관리합니다

작업 영역을 만들고 이름을 바꾸고 삭제하여 관리합니다. 작업 영역에 자원이 포함된 경우에는 작업 영역을 삭제할 수 없습니다. 비어 있어야 합니다.

단계

1. BlueXP 상단에서 * 계정 * 드롭다운을 선택하고 * 계정 관리 * 를 선택합니다.
2. 작업 공간 * 을 선택합니다.
3. 다음 옵션 중 하나를 선택합니다.
 - 새 작업 공간을 만들려면 * 새 작업 공간 추가 * 를 선택합니다.
 - 작업 공간의 이름을 바꾸려면 * Rename * 을 선택합니다.
 - 작업 공간을 삭제하려면 * 삭제 * 를 선택합니다.

새 작업 영역을 만든 경우 해당 작업 영역에 연결선 을 추가해야 합니다. Connector를 추가하지 않으면 작업 영역 관리자가 작업 영역의 리소스에 액세스할 수 없습니다. 자세한 내용은 다음 섹션을 참조하십시오.

Connector의 작업 영역을 관리합니다

Workspace 관리자가 BlueXP에서 이러한 작업 영역에 액세스할 수 있도록 Connector를 작업 영역에 연결해야 합니다.

Account Admins만 있는 경우에는 Connector를 작업 영역과 연결할 필요가 없습니다. 계정 관리자는 기본적으로 BlueXP의 모든 작업 영역에 액세스할 수 있습니다.

["사용자, 작업 영역 및 커넥터에 대해 자세히 알아보십시오".](#)

단계

1. BlueXP 상단에서 * 계정 * 드롭다운을 선택하고 * 계정 관리 * 를 선택합니다.
2. 커넥터 * 를 선택합니다.
3. 연결하려는 Connector의 * 작업 영역 관리 * 를 선택합니다.
4. 커넥터와 연결할 작업 영역을 선택하고 * 적용 * 을 선택합니다.

계정 이름을 변경합니다

언제든지 계정 이름을 변경하여 사용할 수 있는 의미 있는 내용으로 바꿀 수 있습니다.

단계

1. BlueXP 상단에서 * 계정 * 드롭다운을 선택하고 * 계정 관리 * 를 선택합니다.
2. 개요 * 탭에서 계정 이름 옆에 있는 편집 아이콘을 선택합니다.
3. 새 계정 이름을 입력하고 * 저장 * 을 선택합니다.

개인 미리 보기 허용

BlueXP에서 미리 보기로 사용할 수 있는 새 서비스에 액세스하려면 계정의 개인 미리 보기를 허용합니다.

개인 미리 보기의 서비스는 예상대로 작동하지 않을 뿐만 아니라 중단 및 기능 누락이 발생할 수 있습니다.

단계

1. BlueXP 상단에서 * 계정 * 드롭다운을 선택하고 * 계정 관리 * 를 선택합니다.
2. 개요 * 탭에서 * 개인 미리 보기 허용 * 설정을 활성화합니다.

타사 서비스를 허용합니다

사용자 계정의 타사 서비스가 BlueXP에서 사용 가능한 타사 서비스에 액세스할 수 있도록 허용합니다. 타사 서비스는 NetApp에서 제공하는 서비스와 유사한 클라우드 서비스이지만 타사의 관리 및 지원을 받습니다.

단계

1. BlueXP 상단에서 * 계정 * 드롭다운을 선택하고 * 계정 관리 * 를 선택합니다.
2. 개요 * 탭에서 * 타사 서비스 허용 * 설정을 활성화합니다.

계정의 작업을 모니터링합니다

BlueXP가 수행하는 작업의 상태를 모니터링하여 해결해야 할 문제가 있는지 확인할 수 있습니다. 알림 센터, 시각표에서 상태를 보거나 이메일로 알림을 보낼 수 있습니다.


다음 표에서는 Notification Center와 시간 표시 막대를 비교하여 각 기능이 제공해야 하는 사항을 설명합니다.

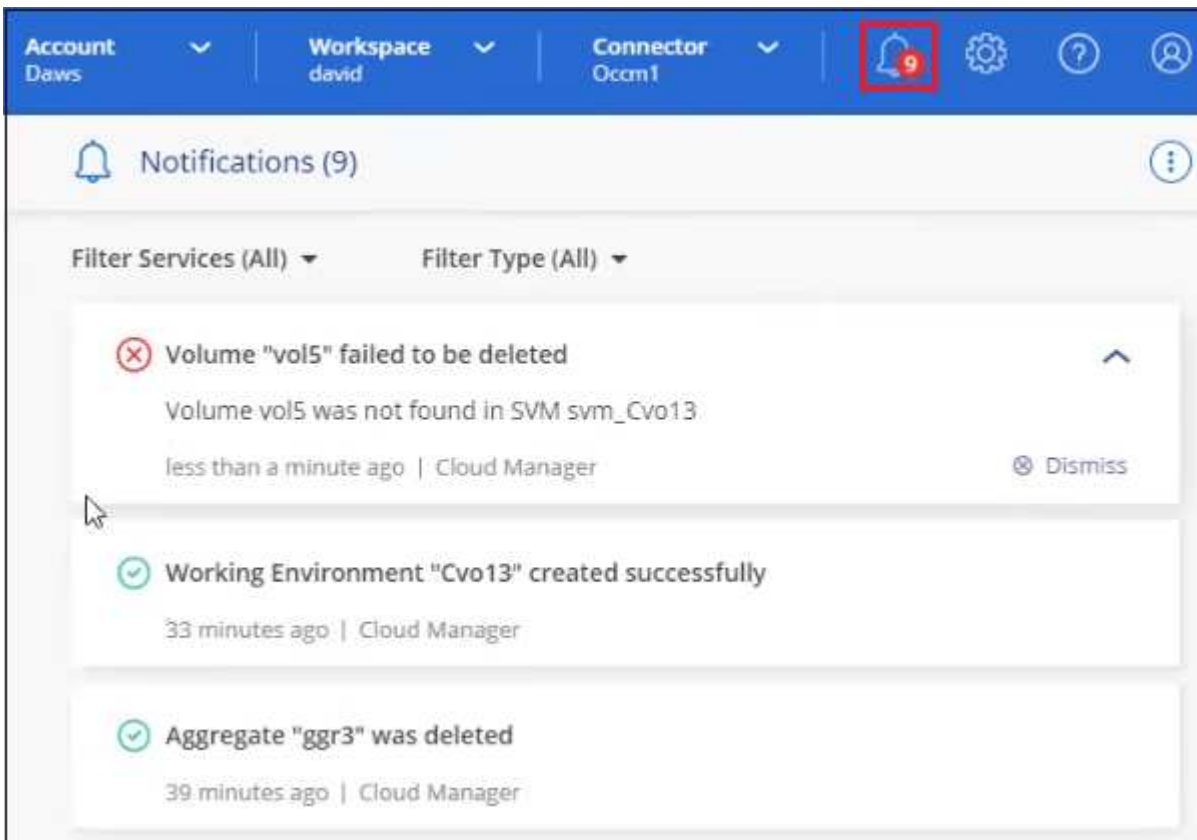
알림 센터	타임라인
이벤트 및 작업에 대한 상위 상태를 표시합니다	추가 조사를 위한 각 이벤트 또는 조치에 대한 세부 정보를 제공합니다
현재 로그인 세션의 상태를 표시합니다(로그오프 후 알림 센터에 정보가 표시되지 않음).	지난 달의 상태를 유지합니다
사용자 인터페이스에서 시작된 작업만 표시합니다	UI 또는 API의 모든 작업을 표시합니다
사용자가 시작한 작업을 표시합니다	사용자가 시작했는지 또는 시스템이 시작되었는지에 관계없이 모든 작업을 표시합니다
중요도에 따라 결과를 필터링합니다	서비스, 작업, 사용자, 상태 등을 기준으로 필터링합니다

알림 센터	타임라인
계정 사용자 및 다른 사용자에게 알림을 이메일로 보낼 수 있는 기능을 제공합니다	이메일 기능이 없습니다

알림 센터를 사용하여 활동을 모니터링합니다

알림은 BlueXP에서 시작한 작업의 진행 상황을 추적하므로 작업의 성공 여부를 확인할 수 있습니다. 이 기능을 사용하면 현재 로그인 세션 중에 시작한 여러 BlueXP 작업의 상태를 볼 수 있습니다. 현재 모든 BlueXP 서비스가 알림 센터에 정보를 보고하는 것은 아닙니다.

알림 벨()를 선택합니다. 벨의 작은 거품의 색상은 활성 상태인 최상위 심각도 알림을 나타냅니다. 따라서 빨간색 기포가 나타나면 확인해야 할 중요한 알림이 있다는 의미입니다.



또한 시스템에 로그인하지 않은 경우에도 중요한 시스템 작업을 알 수 있도록 이메일을 통해 특정 유형의 알림을 보내도록 BlueXP를 구성할 수 있습니다. 이메일은 BlueXP 계정에 속한 모든 사용자 또는 특정 유형의 시스템 작업을 알고 있어야 하는 다른 수신자에게 보낼 수 있습니다. 자세한 내용은 [참조하십시오 이메일 알림 설정을 지정합니다](#).

알림 유형

알림은 다음 범주로 분류됩니다.

알림 유형입니다	설명
심각	수정 조치를 즉시 취하지 않으면 서비스가 중단될 수 있는 문제가 발생했습니다.
오류	조치 또는 프로세스가 실패로 끝나거나 지정 조치가 취해지지 않을 경우 실패로 이어질 수 있습니다.

알림 유형입니다	설명
경고	심각한 심각도에 도달하지 않도록 주의해야 할 문제입니다. 이 심각도에 대한 알림은 서비스 중단을 유발하지 않으며 즉각적인 수정 조치가 필요하지 않을 수 있습니다.
권장 사항	시스템 또는 특정 서비스 개선을 위한 조치를 취할 것을 권장하는 시스템 권장 사항(예: 비용 절감, 새로운 서비스 제안, 권장 보안 구성 등)
정보	작업 또는 프로세스에 대한 추가 정보를 제공하는 메시지입니다.
성공	작업 또는 프로세스가 성공적으로 완료되었습니다.

알림을 필터링합니다

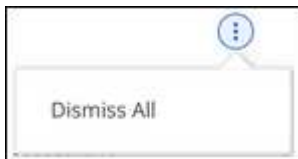
기본적으로 알림 센터에는 모든 활성 알림이 표시됩니다. 표시되는 알림을 필터링하여 중요한 알림만 표시할 수 있습니다. BlueXP "서비스" 및 "유형" 알림별로 필터링할 수 있습니다.

예를 들어, BlueXP 작업에 대한 "오류" 및 "경고" 알림만 표시하려면 해당 항목을 선택하면 해당 유형의 알림만 표시됩니다.

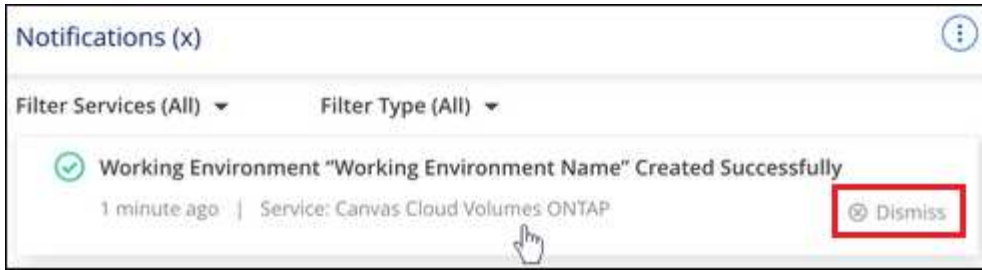
알림을 닫습니다

더 이상 알림을 볼 필요가 없는 경우 페이지에서 알림을 제거할 수 있습니다. 모든 알림을 한 번에 해제하거나 개별 알림을 해제할 수 있습니다.

모든 알림을 해제하려면 알림 센터에서 을 선택합니다 : 를 선택하고 * 모두 해제 * 를 선택합니다.



개별 알림을 해제하려면 알림 위에 커서를 놓고 * Dismiss * 를 선택합니다.



이메일 알림 설정을 지정합니다

이메일을 통해 특정 유형의 알림을 전송할 수 있으므로 BlueXP에 로그인하지 않은 경우에도 중요한 시스템 작업을 알 수 있습니다. 이메일은 BlueXP 계정에 속한 모든 사용자 또는 특정 유형의 시스템 작업을 알고 있어야 하는 다른 수신자에게 보낼 수 있습니다.



- 현재 BlueXP 기능 및 서비스와 같은 BlueXP 기능 및 서비스에 대한 알림은 커넥터, BlueXP 디지털 지갑, BlueXP 복사 및 동기화, BlueXP 백업 및 복구, BlueXP 계층화, BlueXP 마이그레이션 보고서에 대한 이메일로 전송됩니다. 추가 서비스는 향후 릴리즈에서 추가될 예정입니다.
- Connector가 인터넷에 연결되지 않은 사이트에 설치되어 있으면 이메일 알림 전송이 지원되지 않습니다.

알림 센터에서 설정한 필터에 따라 전자 메일로 받을 알림 유형이 결정되지는 않습니다. 기본적으로 BlueXP 계정 관리자는 모든 "중요" 및 "권장 사항" 알림에 대한 이메일을 받게 됩니다. 이러한 알림은 모든 서비스에 걸쳐 제공됩니다. 커넥터 또는 BlueXP 백업 및 복구와 같은 특정 서비스에 대해서만 알림을 받도록 선택할 수는 없습니다.

다른 모든 사용자와 수신자는 알림 이메일을 수신하지 않도록 구성되어 있으므로 추가 사용자에 대한 알림 설정을 구성해야 합니다.

알림 설정을 사용자 지정하려면 계정 관리자여야 합니다.

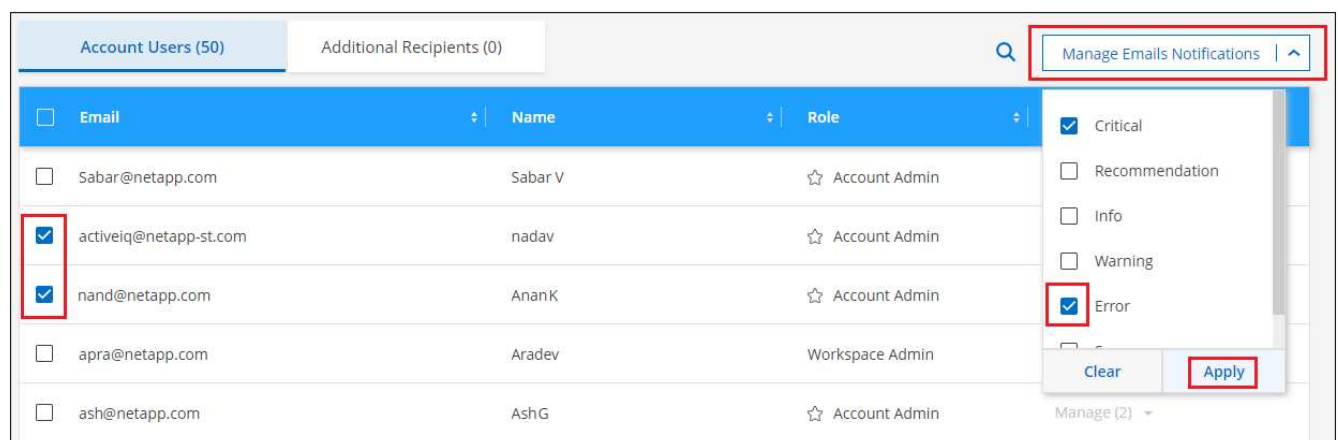
단계

1. BlueXP 메뉴 표시줄에서 * 설정 > 경고 및 알림 설정 * 을 선택합니다.



2. 계정 사용자_탭 또는 _Additional Recipients_tab에서 사용자 또는 여러 사용자를 선택하고 보낼 알림 유형을 선택합니다.

- 단일 사용자를 변경하려면 해당 사용자의 알림 열에서 메뉴를 선택하고 전송할 알림 유형을 선택한 다음 * 적용 * 을 선택합니다.
- 여러 사용자를 변경하려면 각 사용자에 대한 확인란을 선택하고 * 이메일 알림 관리 * 를 선택한 후 전송할 알림 유형을 선택하고 * 적용 * 을 선택합니다.

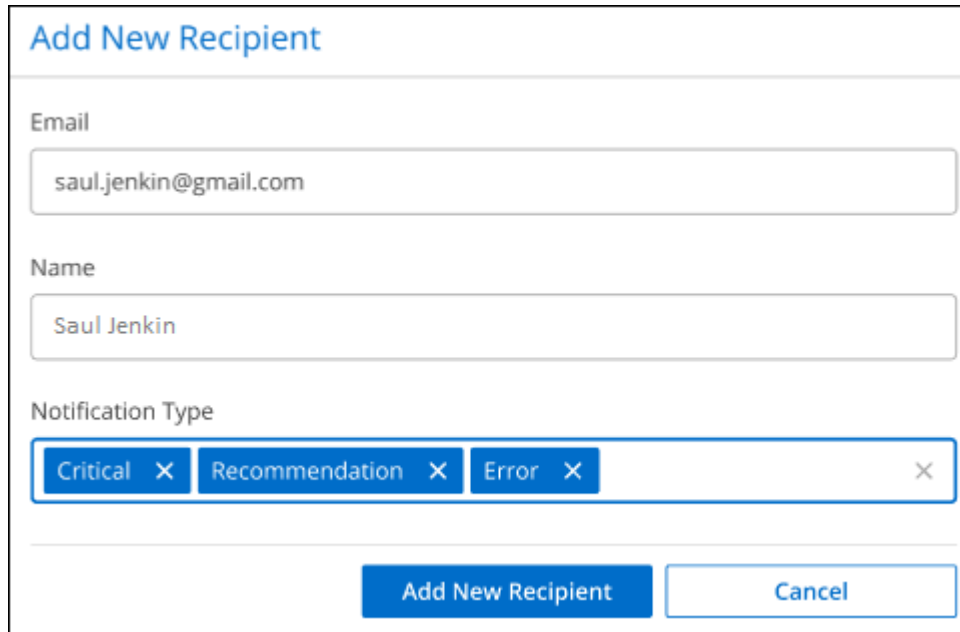


추가 이메일 수신자를 추가합니다

계정 사용자_탭에 나타나는 사용자는 에서 BlueXP 계정의 사용자로부터 자동으로 채워집니다 ("계정 관리 페이지")를 클릭합니다. BlueXP에 액세스할 수 없지만 특정 유형의 경고 및 알림에 대해 알림을 받아야 하는 다른 사람 또는 그룹에 대해서는 _Additional Recipients_tab에서 전자 메일 주소를 추가할 수 있습니다.

단계

1. 알림 및 알림 설정 페이지에서 * 새 수신자 추가 * 를 선택합니다.

A screenshot of a web form titled "Add New Recipient". It contains three input fields: "Email" with the value "saul.jenkin@gmail.com", "Name" with the value "Saul Jenkin", and "Notification Type" which is a multi-select dropdown showing "Critical", "Recommendation", and "Error". At the bottom, there are two buttons: "Add New Recipient" and "Cancel".

2. 이름, 이메일 주소를 입력하고 수신인이 수신할 알림 유형을 선택한 다음 * 새 수신자 추가 * 를 선택합니다.

계정의 사용자 활동을 감사합니다

BlueXP의 시간 표시 막대에는 사용자가 계정 관리를 위해 수행한 작업이 표시됩니다. 여기에는 사용자 연결, 작업 영역 만들기, 커넥터 만들기 등의 관리 작업이 포함됩니다.

특정 작업을 수행한 사람을 확인해야 하거나 작업의 상태를 확인해야 하는 경우 시간 표시 막대를 확인하는 것이 도움이 됩니다.

단계

1. BlueXP 메뉴 모음에서 * 설정 > 타임라인 * 을 선택합니다.
2. 필터 아래에서 * Service * 를 선택하고 * Tenancy * 를 활성화하고 * Apply * 를 선택합니다.

결과

계정 관리 작업이 표시되도록 타임라인이 업데이트됩니다.

다른 **BlueXP** 계정을 만듭니다

BlueXP에 등록하면 조직의 계정을 만들라는 메시지가 표시됩니다. 이 계정만 필요한 경우 여러 계정이 필요한 경우에는 Tenancy API를 사용하여 추가 계정을 만들어야 합니다.

다음 API 호출을 사용하여 BlueXP 계정을 추가로 생성합니다.

게시 /tenancy/account/{accountName}

제한된 모드를 활성화하려면 요청 본문에 다음을 포함해야 합니다.

```
{
  "isSaasDisabled": true
}
```



BlueXP에서 계정을 만든 후에는 제한된 모드 설정을 변경할 수 없습니다. 나중에 제한 모드를 활성화할 수 없으며 나중에 비활성화할 수 없습니다. 계정을 생성할 때 설정해야 합니다.

["이 API 호출을 사용하는 방법에 대해 알아보십시오"](#)

관련 링크

- ["BlueXP 계정에 대해 알아보십시오"](#)
- ["BlueXP 배포 모드에 대해 알아보십시오"](#)

사용자 역할

계정 관리자, 작업 영역 관리자, 규정 준수 뷰어 및 SnapCenter 관리자 역할은 사용자에게 특정 권한을 제공합니다. 새 사용자를 BlueXP 계정에 연결할 때 이러한 역할 중 하나를 할당할 수 있습니다.

Compliance Viewer 역할은 읽기 전용 BlueXP 분류 액세스를 위한 것입니다.

작업	계정 관리자	작업 영역 관리자	규정 준수 뷰어	SnapCenter 관리자
작업 환경 관리	예	예	아니요	아니요
작업 환경에 대한 서비스를 활성화합니다	예	예	아니요	아니요
작업 영역에서 작업 환경을 제거합니다	예	예	아니요	아니요
작업 환경을 삭제합니다	예	예	아니요	아니요
데이터 복제 상태를 봅니다	예	예	아니요	아니요
타임라인을 봅니다	예	예	아니요	아니요
작업 공간 간 전환	예	예	예	아니요
BlueXP 분류 검사 결과를 봅니다	예	예	예	아니요
Cloud Volumes ONTAP 보고서를 받습니다	예	아니요	아니요	아니요
커넥터 작성	예	아니요	아니요	아니요
BlueXP 계정을 관리합니다	예	아니요	아니요	아니요
자격 증명 관리	예	아니요	아니요	아니요
BlueXP 설정을 수정합니다	예	아니요	아니요	아니요
지원 대시보드 보기 및 관리	예	아니요	아니요	아니요

작업	계정 관리자	작업 영역 관리자	규정 준수 뷰어	SnapCenter 관리자
HTTPS 인증서를 설치합니다	예	아니요	아니요	아니요

관련 링크

- ["BlueXP 계정에서 작업 영역 및 사용자를 설정합니다"](#)
- ["BlueXP 계정에서 작업 영역 및 사용자 관리"](#)

커넥터

커넥터의 시스템 ID를 찾습니다

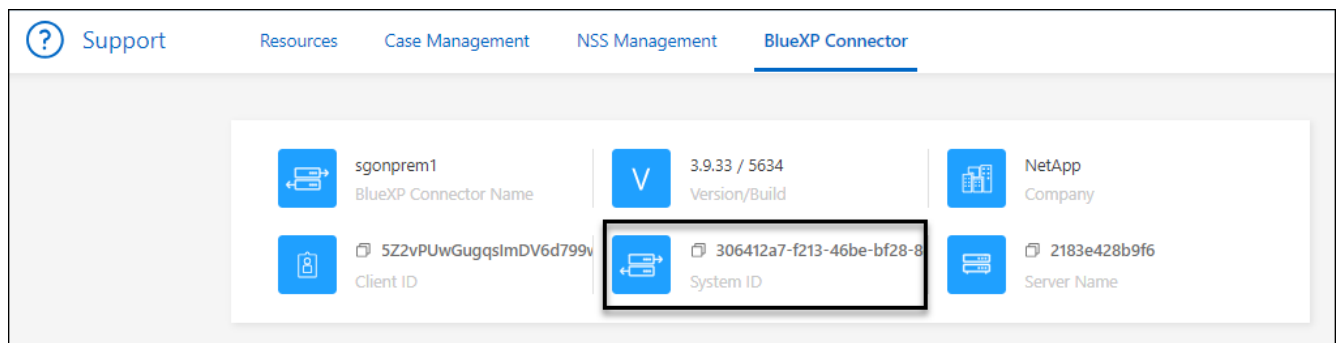
시작하려면 NetApp 담당자가 Connector의 시스템 ID를 물어 볼 수 있습니다. ID는 일반적으로 라이선스 및 문제 해결 목적으로 사용됩니다.

단계

1. BlueXP 콘솔의 오른쪽 상단에서 도움말 아이콘을 선택합니다.
2. Support > BlueXP Connector * 를 선택합니다.

시스템 ID가 페이지 상단에 나타납니다.

◦ 예 *



기존 커넥터 관리

Connector를 만든 후에는 항상 관리해야 할 수 있습니다. 예를 들어, 둘 이상의 커넥터가 있는 경우 커넥터 사이를 전환할 수 있습니다. 또는 비공개 모드에서 BlueXP를 사용할 때 커넥터를 수동으로 업그레이드해야 할 수도 있습니다.

["커넥터 작동 방식에 대해 알아보십시오"](#).



Connector에는 커넥터 호스트에서 액세스할 수 있는 로컬 UI가 포함되어 있습니다. 이 UI는 제한된 모드 또는 프라이빗 모드에서 BlueXP를 사용하는 고객을 위해 제공됩니다. 표준 모드에서 BlueXP를 사용하는 경우 에서 사용자 인터페이스에 액세스해야 합니다 ["BlueXP SaaS 콘솔"](#)

["BlueXP 배포 모드에 대해 알아보십시오"](#).

운영 체제 및 VM 유지 보수

커넥터 호스트에서 운영 체제를 유지 관리하는 것은 사용자의 책임입니다. 예를 들어, 회사의 운영 체제 배포 표준 절차에 따라 Connector 호스트의 운영 체제에 보안 업데이트를 적용해야 합니다.

OS 업데이트를 실행할 때 커넥터 호스트에서 서비스를 중지할 필요가 없습니다.

Connector VM을 중지한 다음 시작해야 하는 경우, 클라우드 공급자의 콘솔에서 또는 온프레미스 관리를 위한 표준 절차를 사용하여 시작해야 합니다.

"커넥터는 항상 작동해야 합니다".

VM 또는 인스턴스 유형입니다

BlueXP에서 Connector를 직접 생성한 경우 BlueXP는 기본 구성을 사용하여 클라우드 공급자에 가상 머신 인스턴스를 구축했습니다. Connector를 생성한 후에는 CPU 또는 RAM이 적은 더 작은 VM 인스턴스로 변경하지 마십시오.

CPU 및 RAM 요구 사항은 다음과 같습니다.

CPU

코어 4개 또는 vCPU 4개

RAM

14GB

"Connector의 기본 설정에 대해 알아봅니다".

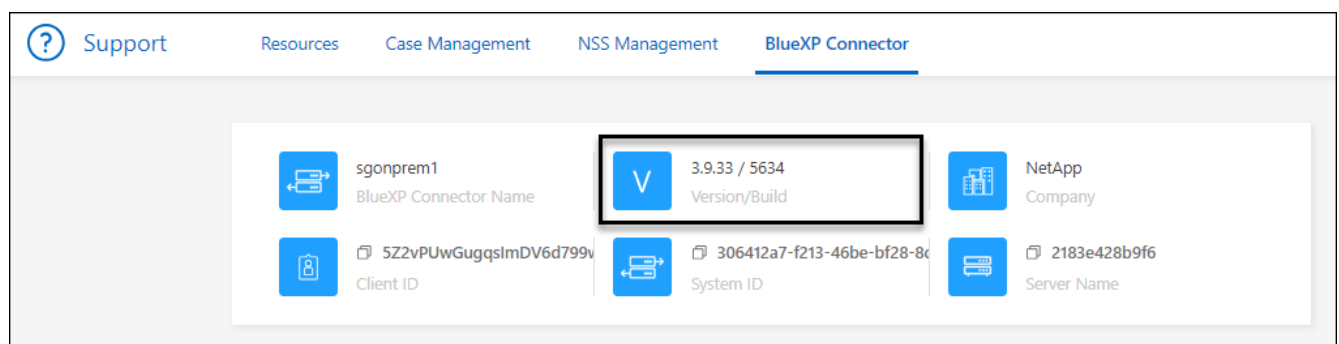
Connector 버전 보기

Connector 버전을 확인하여 커넥터가 최신 릴리즈로 자동 업그레이드되었는지 또는 NetApp 담당자와 공유해야 하는지 확인할 수 있습니다.

단계

1. BlueXP 콘솔의 오른쪽 상단에서 도움말 아이콘을 선택합니다.
2. Support > BlueXP Connector * 를 선택합니다.

버전이 페이지 상단에 표시됩니다.



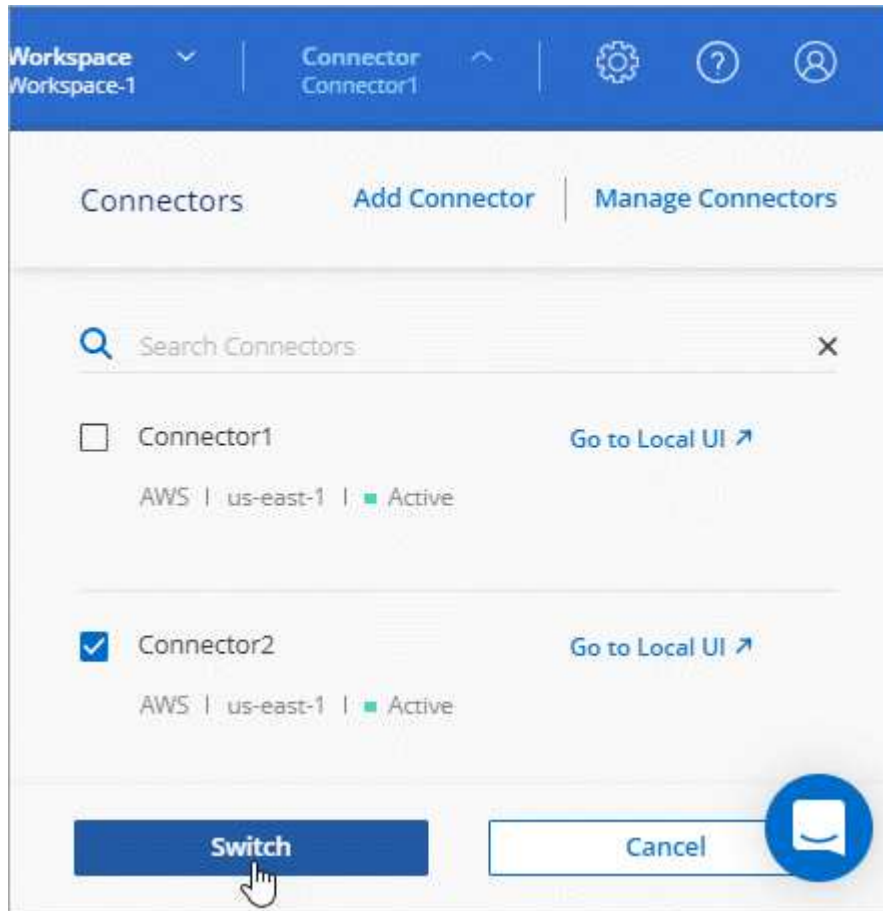
커넥터 사이를 전환합니다

커넥터가 여러 개 있는 경우 커넥터 사이를 전환하여 특정 커넥터와 연결된 작업 환경을 볼 수 있습니다.

예를 들어, 멀티클라우드 환경에서 일하고 있다고 가정해 보겠습니다. AWS에 Connector가 있고 Google Cloud에 Connector가 있을 수 있습니다. 이러한 클라우드에서 실행되는 Cloud Volumes ONTAP 시스템을 관리하려면 이러한 커넥터 사이를 전환해야 합니다.

단계

1. 커넥터 * 드롭다운을 선택하고 다른 커넥터를 선택한 다음 * 스위치 * 를 선택합니다.



결과

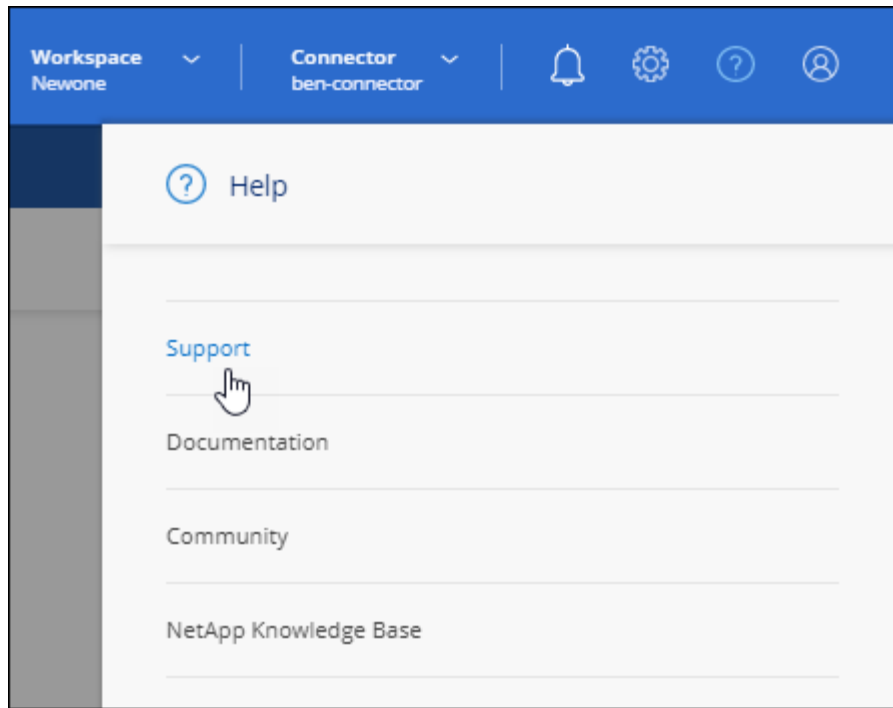
BlueXP는 선택한 커넥터와 연결된 작업 환경을 새로 고치고 표시합니다.

AutoSupport 메시지를 다운로드하거나 보냅니다

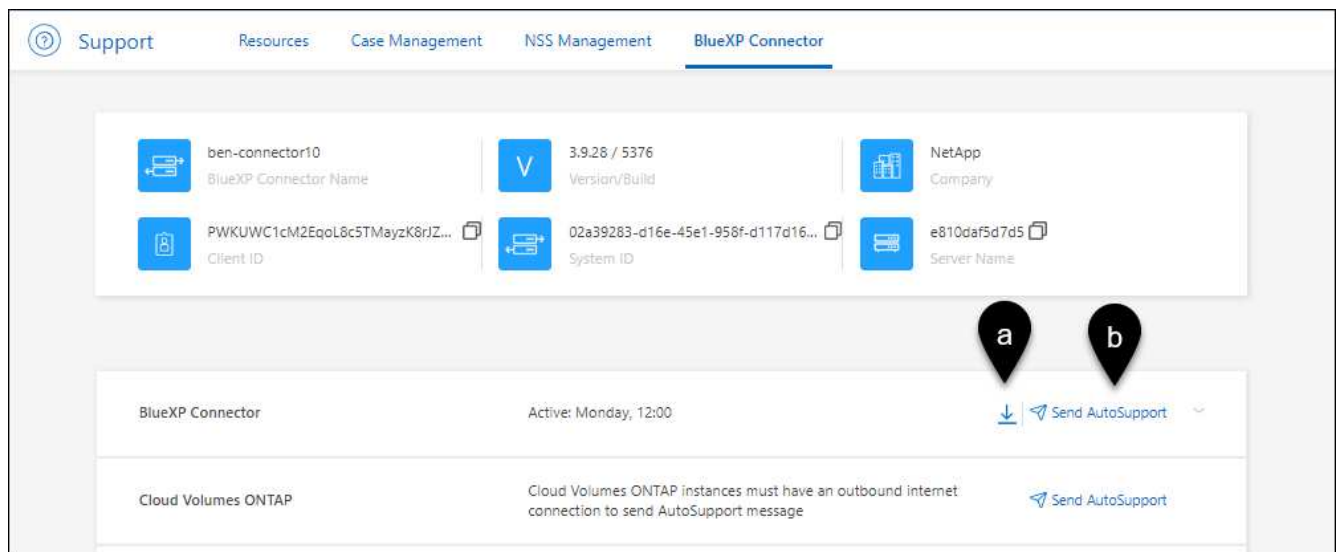
문제가 있는 경우 NetApp 직원이 문제 해결을 위해 NetApp 지원에 AutoSupport 메시지를 보내도록 요청할 수 있습니다.

단계

1. BlueXP 콘솔의 오른쪽 상단에서 도움말 아이콘을 선택하고 * 지원 * 을 선택합니다.



2. BlueXP 커넥터 * 를 선택합니다.
3. NetApp 지원에 정보를 보내는 방법에 따라 다음 옵션 중 하나를 선택합니다.
 - a. 로컬 컴퓨터에 AutoSupport 메시지를 다운로드하는 옵션을 선택합니다. 그런 다음 원하는 방법을 사용하여 NetApp Support로 보낼 수 있습니다.
 - b. 메시지를 NetApp 지원으로 직접 보내려면 * Send AutoSupport * 를 선택합니다.



Linux VM에 연결합니다

Connector가 실행되는 Linux VM에 연결해야 하는 경우 클라우드 공급자에서 제공하는 연결 옵션을 사용하여 연결할 수 있습니다.

설치하고

AWS에서 Connector 인스턴스를 생성한 경우 AWS 액세스 키와 암호 키를 제공했습니다. 이 키 쌍을 사용하여 인스턴스에 SSH를 사용할 수 있습니다. EC2 Linux 인스턴스의 사용자 이름은 Ubuntu입니다(2023년 5월 이전에 생성된 커넥터의 경우 사용자 이름은 EC2-user입니다).

["AWS Docs: Linux 인스턴스에 연결합니다"](#)

Azure를 지원합니다

Azure에서 Connector VM을 생성할 때 사용자 이름을 지정하고 암호 또는 SSH 공개 키로 인증하도록 선택했습니다. VM에 연결하도록 선택한 인증 방법을 사용합니다.

["Azure Docs: VM에 SSH를 연결합니다"](#)

Google 클라우드

Google Cloud에서 Connector를 만들 때는 인증 방법을 지정할 수 없습니다. 그러나 Google Cloud Console 또는 Google Cloud CLI(gcloud)를 사용하여 Linux VM 인스턴스에 연결할 수 있습니다.

["Google Cloud Docs: Linux VM에 연결합니다"](#)

Amazon EC2 인스턴스에서 IMDSv2를 사용해야 합니다

2024년부터 BlueXP는 이제 커넥터 및 Cloud Volumes ONTAP(HA 구축을 위한 중재자 포함)를 통해 Amazon EC2 인스턴스 메타데이터 서비스 버전 2(IMDSv2)를 지원합니다. 대부분의 경우 IMDSv2는 새 EC2 인스턴스에 자동으로 구성됩니다. IMDSv1은 2024년 3월 이전에 활성화되었습니다. 보안 정책에서 요구하는 경우 EC2 인스턴스에 IMDSv2를 수동으로 구성해야 할 수 있습니다.

이 작업에 대해

IMDSv2는 취약성에 대한 향상된 보호 기능을 제공합니다. ["IMDSv2에 대한 자세한 내용은 AWS 보안 블로그를 참조하십시오"](#)

EC2 인스턴스에 대해 IMDS(인스턴스 메타데이터 서비스)가 다음과 같이 활성화됩니다.

- BlueXP에서 또는 를 사용하여 새로운 Connector를 구축하는 경우 ["Terraform 스크립트"](#), IMDSv2는 EC2 인스턴스에서 기본적으로 사용하도록 설정됩니다.
- AWS에서 새 EC2 인스턴스를 시작한 다음 Connector 소프트웨어를 수동으로 설치하면 IMDSv2도 기본적으로 사용하도록 설정됩니다.
- AWS Marketplace에서 Connector를 실행하면 IMDSv1이 기본적으로 활성화됩니다. EC2 인스턴스에 IMDSv2를 수동으로 구성할 수 있습니다.
- 기존 커넥터의 경우 IMDSv1은 계속 지원되지만 원하는 경우 EC2 인스턴스에서 IMDSv2를 수동으로 구성할 수 있습니다.
- Cloud Volumes ONTAP의 경우 새 인스턴스와 기존 인스턴스에서 IMDSv1이 기본적으로 사용됩니다. 원하는 경우 EC2 인스턴스에 IMDSv2를 수동으로 구성할 수 있습니다.

시작하기 전에

- Connector 버전은 3.9.38 이상이어야 합니다.
- Cloud Volumes ONTAP에서 다음 버전 중 하나를 실행해야 합니다.
 - 9.12.1 P2(또는 후속 패치)

- 9.13.0 P4(또는 후속 패치)
- 9.13.1 또는 이 릴리스 이후의 모든 버전

• 이 변경 사항을 적용하려면 Cloud Volumes ONTAP 인스턴스를 다시 시작해야 합니다.

이 작업에 대해

응답 홉 제한을 3으로 변경해야 하므로 다음 단계를 수행하려면 AWS CLI를 사용해야 합니다.

단계

1. 커넥터 인스턴스에서 IMDSv2를 사용해야 합니다.

a. 커넥터용 Linux VM에 연결합니다.

AWS에서 Connector 인스턴스를 생성한 경우 AWS 액세스 키와 암호 키를 제공했습니다. 이 키 쌍을 사용하여 인스턴스에 SSH를 사용할 수 있습니다. EC2 Linux 인스턴스의 사용자 이름은 Ubuntu입니다(2023년 5월 이전에 생성된 커넥터의 경우 사용자 이름은 EC2-user입니다).

["AWS Docs: Linux 인스턴스에 연결합니다"](#)

b. AWS CLI를 설치합니다.

["AWS 문서: 최신 버전의 AWS CLI를 설치하거나 업데이트합니다"](#)

c. 를 사용합니다 `aws ec2 modify-instance-metadata-options` IMDSv2의 사용을 요구하고 PUT 응답 홉 제한을 3으로 변경하는 명령어이다.

▪ 예 *

```
aws ec2 modify-instance-metadata-options \
  --instance-id <instance-id> \
  --http-put-response-hop-limit 3 \
  --http-tokens required \
  --http-endpoint enabled
```



를 클릭합니다 `http-tokens` 매개 변수는 IMDSv2를 Required 로 설정합니다. 시기 `http-tokens` 이 필수 요소이며 도 설정해야 합니다 `http-endpoint` 를 활성화합니다.

2. Cloud Volumes ONTAP 인스턴스에서 IMDSv2를 사용해야 합니다.

a. 로 이동합니다 ["Amazon EC2 콘솔"](#)

b. 탐색 창에서 * 인스턴스 * 를 선택합니다.

c. Cloud Volumes ONTAP 인스턴스를 선택합니다.

d. 조치 > 인스턴스 설정 > 인스턴스 메타데이터 옵션 수정 * 을 선택합니다.

e. 인스턴스 메타데이터 수정 옵션 * 대화 상자에서 다음을 선택합니다.

- 인스턴스 메타데이터 서비스 * 의 경우 * 활성화 * 를 선택합니다.
- IMDSv2 * 의 경우 * 필수 * 를 선택합니다.

- 저장 * 을 선택합니다.
- f. HA 중재자를 포함하여 다른 Cloud Volumes ONTAP 인스턴스에 대해 이 단계를 반복합니다.
- g. ["Cloud Volumes ONTAP 인스턴스를 중지하고 시작합니다"](#)

결과

이제 커넥터 인스턴스 및 Cloud Volumes ONTAP 인스턴스가 IMDSv2를 사용하도록 구성되었습니다.

비공개 모드를 사용할 경우 커넥터를 업그레이드합니다

비공개 모드에서 BlueXP를 사용하는 경우 NetApp Support 사이트에서 최신 버전을 사용할 수 있는 경우 커넥터를 업그레이드할 수 있습니다.

업그레이드 프로세스 중에 Connector를 다시 시작해야 업그레이드 중에 웹 기반 콘솔을 사용할 수 없게 됩니다.



표준 모드 또는 제한된 모드에서 BlueXP를 사용할 경우, 소프트웨어 업데이트를 받을 수 있도록 아웃바운드 인터넷에 액세스할 수 있는 경우 Connector에서 소프트웨어를 자동으로 최신 버전으로 업데이트합니다.

단계

1. 에서 Connector 소프트웨어를 다운로드합니다 ["NetApp Support 사이트"](#).

인터넷 액세스 없이 개인 네트워크용 오프라인 설치 프로그램을 다운로드해야 합니다.

2. Linux 호스트에 설치 프로그램을 복사합니다.
3. 스크립트를 실행할 권한을 할당합니다.

```
chmod +x /path/BlueXP-Connector-offline-<version>
```

여기서 <version>는 다운로드한 커넥터 버전입니다.

4. 설치 스크립트를 실행합니다.

```
sudo /path/BlueXP-Connector-offline-<version>
```

여기서 <version>는 다운로드한 커넥터 버전입니다.

5. 업그레이드가 완료되면 * 도움말 > 지원 > 커넥터 * 로 이동하여 커넥터 버전을 확인할 수 있습니다.

커넥터의 IP 주소를 변경합니다

비즈니스에 필요한 경우 클라우드 공급자가 자동으로 할당하는 Connector 인스턴스의 내부 IP 주소와 공용 IP 주소를 변경할 수 있습니다.

단계

1. 클라우드 공급자의 지침에 따라 Connector 인스턴스의 로컬 IP 주소 또는 공용 IP 주소(또는 둘 다)를 변경합니다.

2. 공용 IP 주소를 변경한 경우 Connector에서 실행 중인 로컬 사용자 인터페이스에 연결해야 하는 경우 Connector 인스턴스를 다시 시작하여 새 IP 주소를 BlueXP에 등록합니다.
3. 전용 IP 주소를 변경한 경우 백업이 커넥터의 새 전용 IP 주소로 전송되도록 Cloud Volumes ONTAP 구성 파일의 백업 위치를 업데이트합니다.

각 Cloud Volumes ONTAP 시스템의 백업 위치를 업데이트해야 합니다.

- a. Cloud Volumes ONTAP CLI에서 다음 명령을 실행하여 현재 백업 타겟을 표시합니다.

```
system configuration backup show
```

- b. 다음 명령을 실행하여 백업 대상의 IP 주소를 업데이트합니다.

```
system configuration backup settings modify -destination <target-location>
```

Connector의 URI를 편집합니다

Connector 의 URI(Uniform Resource Identifier)를 추가하고 제거합니다.

단계

1. BlueXP 헤더에서 * 커넥터 * 드롭다운을 선택합니다.
2. 커넥터 관리 * 를 선택합니다.
3. Connector에 대한 작업 메뉴를 선택하고 * URI 편집 * 을 선택합니다.
4. URI를 추가 및 제거한 다음 * 적용 * 을 선택합니다.

Google Cloud NAT 게이트웨이를 사용할 때 다운로드 오류를 수정합니다

커넥터는 Cloud Volumes ONTAP용 소프트웨어 업데이트를 자동으로 다운로드합니다. 구성에서 Google Cloud NAT 게이트웨이를 사용하는 경우 다운로드가 실패할 수 있습니다. 소프트웨어 이미지를 분할하는 부품 수를 제한하여 이 문제를 해결할 수 있습니다. 이 단계는 BlueXP API를 사용하여 완료해야 합니다.

단계

1. 다음과 같은 JSON을 본문으로 /occm/config에 PUT 요청을 제출합니다.

```
{
  "maxDownloadSessions": 32
}
```

maxDownloadSessions_ 값은 1이거나 1보다 큰 정수일 수 있습니다. 값이 1이면 다운로드한 이미지는 분할되지 않습니다.

32는 예제 값입니다. 사용할 값은 NAT 구성과 동시에 사용할 수 있는 세션 수에 따라 다릅니다.

["/occm/config API 호출에 대해 자세히 알아보십시오"](#)

BlueXP에서 커넥터를 제거합니다

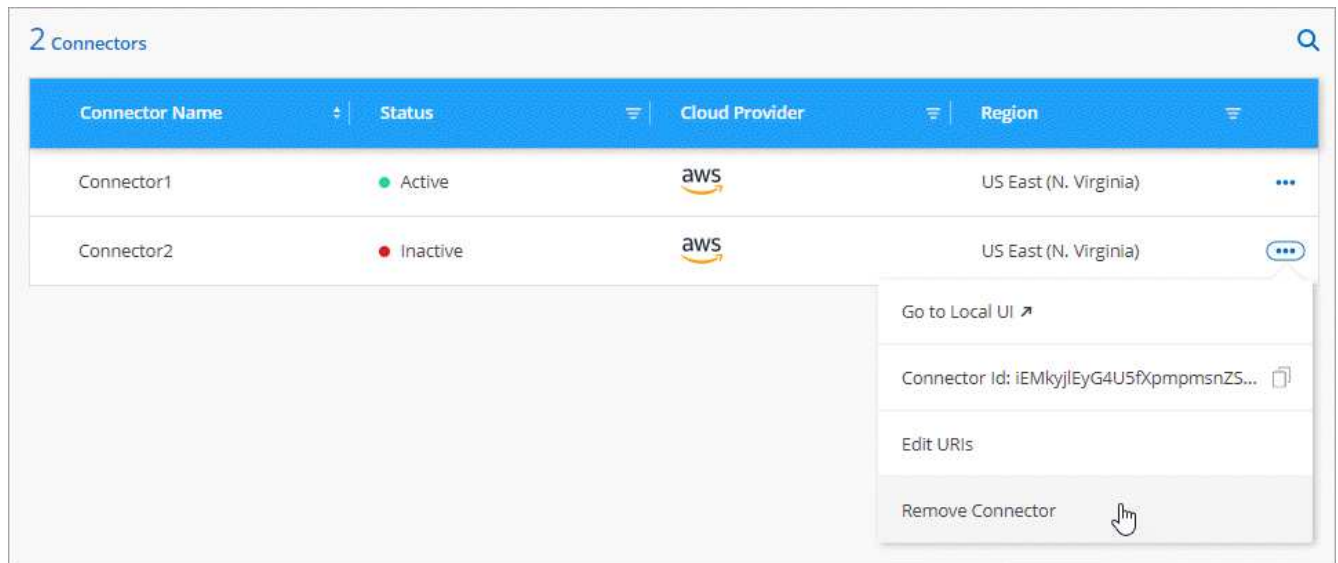
커넥터가 비활성 상태인 경우 BlueXP의 커넥터 목록에서 제거할 수 있습니다. Connector 가상 시스템을 삭제하거나 Connector 소프트웨어를 제거한 경우 이 작업을 수행할 수 있습니다.

커넥터 분리에 대한 내용은 다음과 같습니다.

- 이 작업은 가상 머신을 삭제하지 않습니다.
- 이 작업은 되돌릴 수 없습니다. BlueXP에서 커넥터를 제거한 후에는 다시 추가할 수 없습니다.

단계

1. BlueXP 헤더에서 * 커넥터 * 드롭다운을 선택합니다.
2. 커넥터 관리 * 를 선택합니다.
3. 비활성 커넥터의 작업 메뉴를 선택하고 * 커넥터 제거 * 를 선택합니다.



4. 확인할 커넥터 이름을 입력한 다음 * 제거 * 를 선택합니다.

결과

BlueXP는 커넥터에서 커넥터를 제거합니다.

Connector 소프트웨어를 제거합니다

커넥터 소프트웨어를 제거하여 문제를 해결하거나 호스트에서 소프트웨어를 영구적으로 제거합니다. 사용해야 하는 단계는 인터넷 액세스(표준 모드 또는 제한된 모드)가 있는 호스트에 커넥터를 설치했는지, 인터넷 액세스가 없는 네트워크에 있는 호스트(개인 모드)에 커넥터를 설치했는지에 따라 다릅니다.

표준 모드 또는 제한 모드를 사용하는 경우 를 제거합니다

아래 단계를 사용하여 표준 모드 또는 제한된 모드에서 BlueXP를 사용할 때 Connector 소프트웨어를 제거할 수 있습니다.

단계

1. 커넥터용 Linux VM에 연결합니다.
2. Linux 호스트에서 제거 스크립트를 실행합니다.

```
/opt/application/netapp/service-manager-2/uninstall.sh [silent]
```

_silent_는 확인 메시지를 표시하지 않고 스크립트를 실행합니다.

비공개 모드를 사용하는 경우 를 제거합니다

아래 단계를 수행하여 인터넷에 액세스할 수 없는 비공개 모드에서 BlueXP를 사용할 때 Connector 소프트웨어를 제거할 수 있습니다.

단계

1. 커넥터용 Linux VM에 연결합니다.
2. Linux 호스트에서 다음 명령을 실행합니다.

```
./opt/application/netapp/ds/cleanup.sh  
rm -rf /opt/application/netapp/ds
```

보안 액세스를 위해 HTTPS 인증서를 설치합니다

기본적으로 BlueXP는 웹 콘솔에 대한 HTTPS 액세스를 위해 자체 서명된 인증서를 사용합니다. 회사에서 요구하는 경우 CA(인증 기관)에서 서명한 인증서를 설치할 수 있으므로 자체 서명된 인증서보다 보안 보호가 향상됩니다.

시작하기 전에

BlueXP 설정을 변경하려면 먼저 커넥터를 만들어야 합니다. ["자세히 알아보기"](#).

HTTPS 인증서를 설치합니다

보안 액세스를 위해 CA에서 서명한 인증서를 설치합니다.

단계

1. BlueXP 콘솔의 오른쪽 상단에서 설정 아이콘을 선택하고 * HTTPS 설정 * 을 선택합니다.

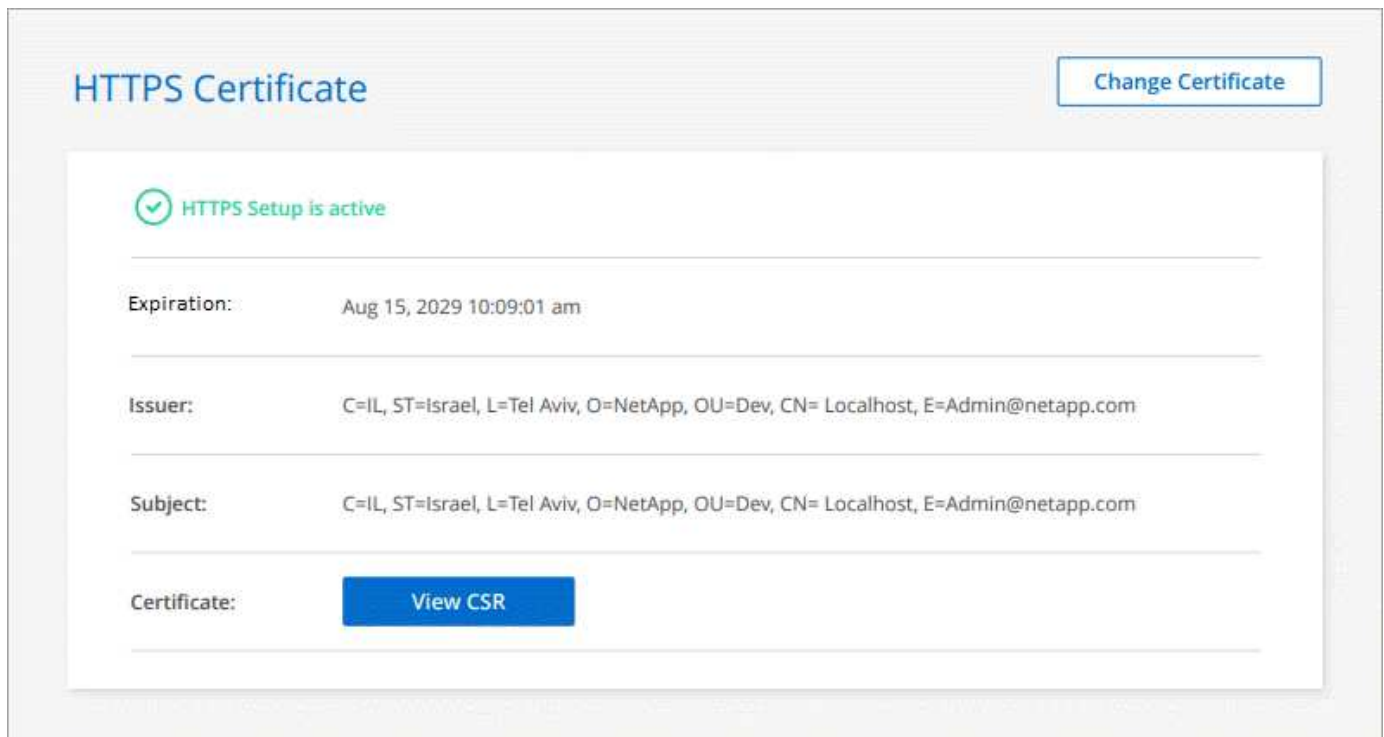


2. HTTPS 설정 페이지에서 인증서 서명 요청(CSR)을 생성하거나 고유한 CA 서명 인증서를 설치하여 인증서를 설치합니다.

옵션을 선택합니다	설명
CSR을 생성합니다	<p>a. 커넥터 호스트의 호스트 이름 또는 DNS(공통 이름)를 입력한 다음 * CSR 생성 * 을 선택합니다.</p> <p>BlueXP는 인증서 서명 요청을 표시합니다.</p> <p>b. CSR을 사용하여 CA에 SSL 인증서 요청을 제출합니다.</p> <p>인증서는 PEM(Privacy Enhanced Mail) Base-64로 인코딩된 X.509 형식을 사용해야 합니다.</p> <p>c. 인증서 파일을 업로드한 다음 * 설치 * 를 선택합니다.</p>
고유한 CA 서명 인증서를 설치합니다	<p>a. CA 서명 인증서 설치 * 를 선택합니다.</p> <p>b. 인증서 파일과 개인 키를 모두 로드한 다음 * 설치 * 를 선택합니다.</p> <p>인증서는 PEM(Privacy Enhanced Mail) Base-64로 인코딩된 X.509 형식을 사용해야 합니다.</p>

결과

BlueXP는 이제 CA 서명 인증서를 사용하여 안전한 HTTPS 액세스를 제공합니다. 다음 이미지는 보안 액세스를 위해 구성된 BlueXP 계정을 보여줍니다.



BlueXP HTTPS 인증서를 갱신합니다

BlueXP 콘솔에 안전하게 액세스하려면 만료되기 전에 BlueXP HTTPS 인증서를 갱신해야 합니다. 인증서가 만료되기 전에 갱신하지 않으면 사용자가 HTTPS를 사용하여 웹 콘솔에 액세스할 때 경고가 나타납니다.

단계

1. BlueXP 콘솔의 오른쪽 상단에서 설정 아이콘을 선택하고 * HTTPS 설정 * 을 선택합니다.

만료 날짜를 포함하여 BlueXP 인증서에 대한 세부 정보가 표시됩니다.

2. 인증서 변경 * 을 선택하고 단계에 따라 CSR을 생성하거나 고유한 CA 서명 인증서를 설치합니다.

결과

BlueXP는 새로운 CA 서명 인증서를 사용하여 안전한 HTTPS 액세스를 제공합니다.

프록시 서버를 사용하도록 **Connector**를 구성합니다

회사 정책에 따라 인터넷에 대한 모든 통신에 프록시 서버를 사용해야 하는 경우 해당 프록시 서버를 사용하도록 커넥터를 구성해야 합니다. 설치하는 동안 프록시 서버를 사용하도록 **Connector**를 구성하지 않은 경우 언제든지 해당 프록시 서버를 사용하도록 **Connector**를 구성할 수 있습니다.

프록시 서버를 사용하도록 **Connector**를 구성하면 공용 IP 주소 또는 NAT 게이트웨이를 사용할 수 없는 경우 아웃바운드 인터넷 액세스를 제공합니다. 이 프록시 서버는 아웃바운드 연결이 있는 커넥터만 제공합니다. Cloud Volumes ONTAP 시스템에 대한 연결은 제공하지 않습니다.

Cloud Volumes ONTAP 시스템에 AutoSupport 메시지를 보내기 위한 아웃바운드 인터넷 연결이 없는 경우 BlueXP는 자동으로 해당 Cloud Volumes ONTAP 시스템이 커넥터에 포함된 프록시 서버를 사용하도록 구성합니다. 유일한 요구 사항은 커넥터 보안 그룹이 포트 3128을 통한 인바운드 연결을 허용하는지 확인하는 것입니다. **Connector**를 배포한 후 이 포트를 열어야 합니다.

지원되는 구성

- BlueXP는 HTTP 및 HTTPS를 지원합니다.
- 프록시 서버는 클라우드 또는 네트워크에 있을 수 있습니다.
- BlueXP는 투명한 프록시 서버를 지원하지 않습니다.

Connector에서 프록시를 활성화합니다

커넥터가 관리하는 프록시 서버(HA 중개자 포함)와 Cloud Volumes ONTAP 시스템을 사용하도록 커넥터를 구성하는 경우 모두 프록시 서버를 사용합니다.

이 작업은 **Connector**를 다시 시작합니다. 계속하기 전에 커넥터가 어떠한 작업도 수행하지 않는지 확인하십시오.

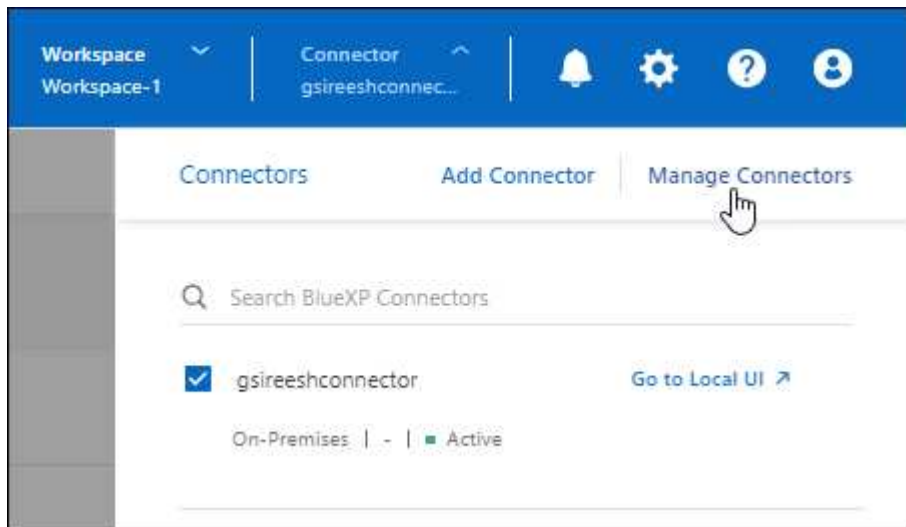
단계

1. BlueXP 커넥터 편집 * 페이지로 이동합니다.

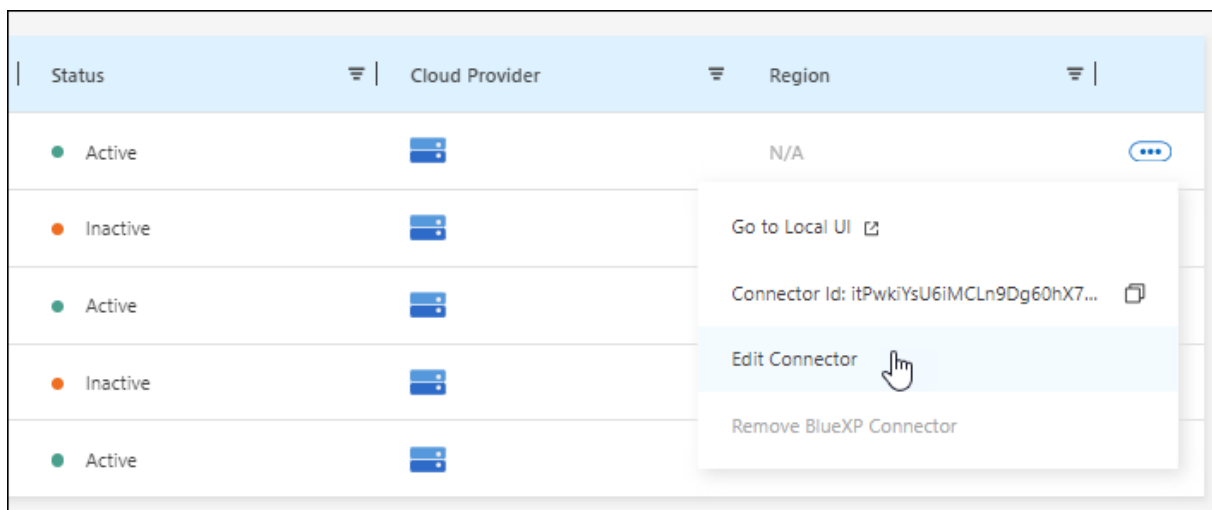
탐색 방법은 표준 모드에서 BlueXP를 사용(SaaS 웹 사이트에서 BlueXP 인터페이스에 액세스) 하는지, 제한된 모드나 프라이빗 모드(커넥터 호스트에서 로컬로 BlueXP 인터페이스에 액세스)로 BlueXP를 사용 중인지 여부에 따라 달라집니다.

표준 모드

- BlueXP 헤더에서 * 커넥터 * 드롭다운을 선택합니다.
- 커넥터 관리 * 를 선택합니다.

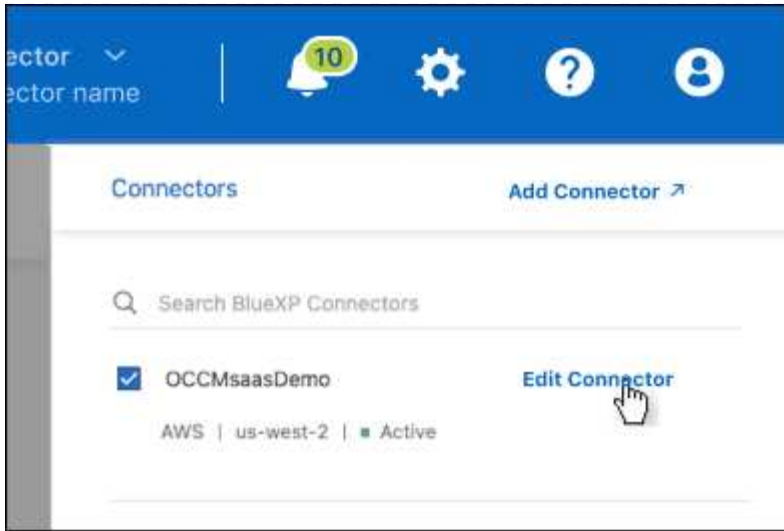


- 커넥터의 작업 메뉴를 선택하고 * 커넥터 편집 * 을 선택합니다.



제한 또는 비공개 모드

- BlueXP 헤더에서 * 커넥터 * 드롭다운을 선택합니다.
- 커넥터 편집 * 을 선택합니다.



2. HTTP 프록시 구성 * 을 선택합니다.

3. 프록시 설정:

- a. 프록시 사용 * 을 선택합니다.
- b. 구문을 사용하여 서버를 지정합니다 `http://address:port` 또는 `https://address:port`
- c. 서버에 대한 기본 인증이 필요한 경우 사용자 이름과 암호를 지정합니다.

다음 사항에 유의하십시오.

- 사용자는 로컬 사용자 또는 도메인 사용자일 수 있습니다.
- 도메인 사용자의 경우 도메인-이름 %92user-name과 같이 \에 대한 ASCII 코드를 입력해야 합니다

예: NetApp%92proxy

- BlueXP는 @ 문자를 포함하는 암호를 지원하지 않습니다.

d. 저장 * 을 선택합니다.

직접 **API** 트래픽을 활성화합니다

Connector가 프록시 서버를 사용하도록 구성한 경우 프록시를 거치지 않고 API 호출을 클라우드 공급자 서비스로 직접 전송하기 위해 Connector에서 직접 API 트래픽을 활성화할 수 있습니다. 이 옵션은 AWS, Azure 또는 Google Cloud에서 실행되는 커넥터에서 지원됩니다.

Cloud Volumes ONTAP에서 Azure 개인 링크 사용을 비활성화했으며 서비스 끝점을 대신 사용하는 경우 직접 API 트래픽을 활성화해야 합니다. 그렇지 않으면 트래픽이 제대로 라우팅되지 않습니다.

"Cloud Volumes ONTAP에서 Azure 전용 링크 또는 서비스 끝점을 사용하는 방법에 대해 자세히 알아보십시오"

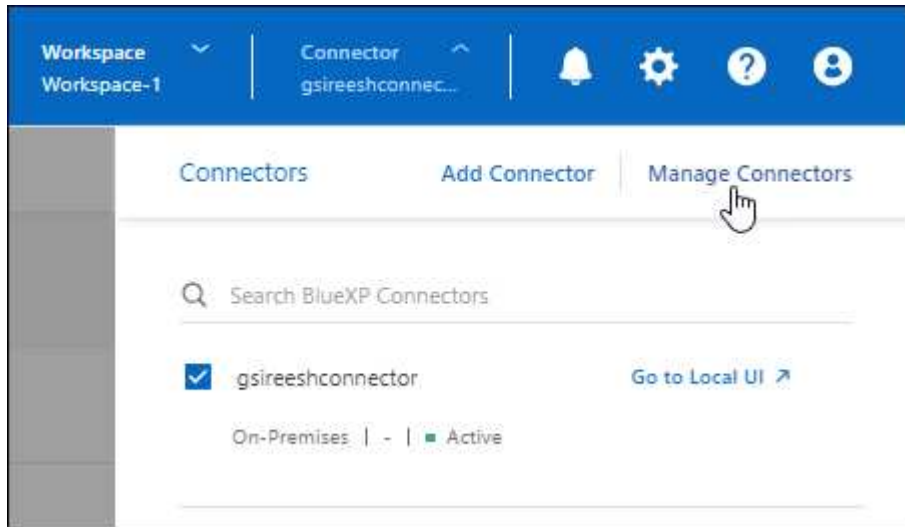
단계

1. BlueXP Connector 편집 * 페이지로 이동합니다.

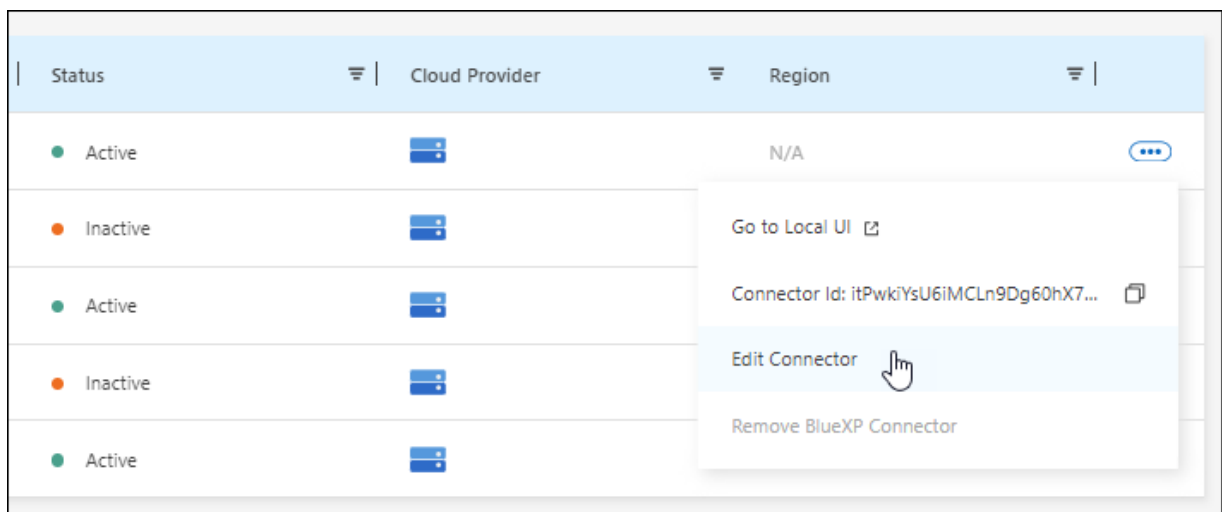
탐색 방법은 표준 모드에서 BlueXP를 사용(SaaS 웹 사이트에서 BlueXP 인터페이스에 액세스) 하는지, 제한된 모드나 프라이빗 모드(커넥터 호스트에서 로컬로 BlueXP 인터페이스에 액세스)로 BlueXP를 사용 중인지 여부에 따라 달라집니다.

표준 모드

- BlueXP 헤더에서 * 커넥터 * 드롭다운을 선택합니다.
- 커넥터 관리 * 를 선택합니다.

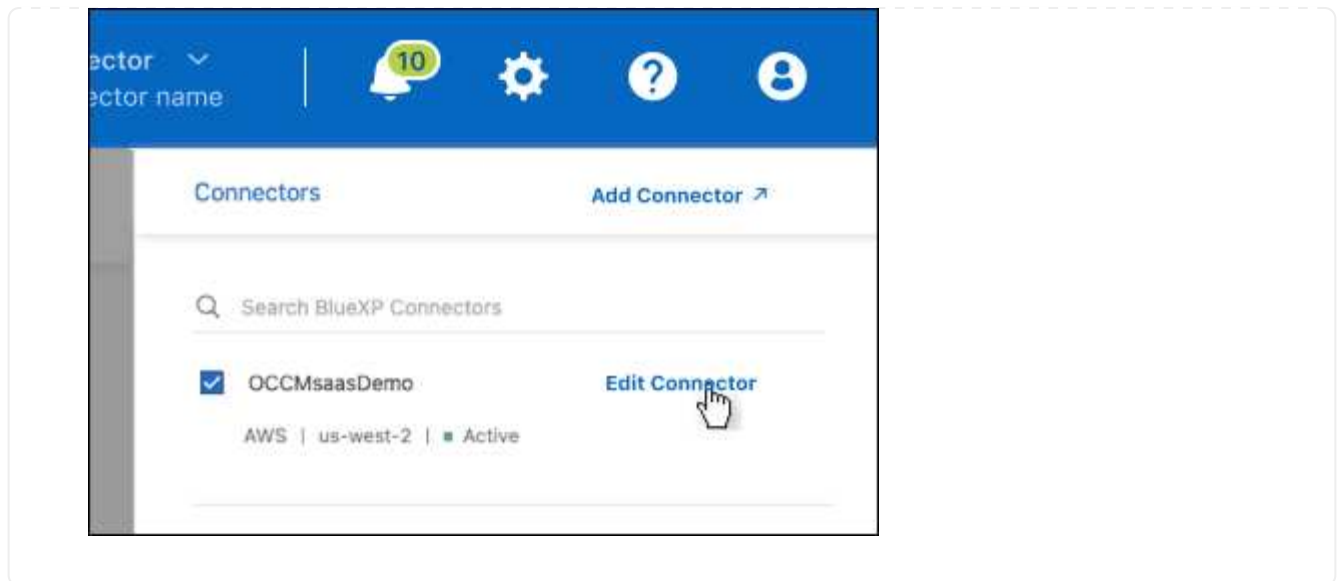


- 커넥터의 작업 메뉴를 선택하고 * 커넥터 편집 * 을 선택합니다.



제한 또는 비공개 모드

- BlueXP 헤더에서 * 커넥터 * 드롭다운을 선택합니다.
- 커넥터 편집 * 을 선택합니다.



2. Support Direct API Traffic * 을 선택합니다.
3. 확인란을 선택하여 옵션을 활성화한 다음 * Save * 를 선택합니다.

Connector의 기본 설정

커넥터 구성을 배포하기 전에 또는 문제를 해결해야 하는 경우에 대해 자세히 알아볼 수 있습니다.

인터넷 액세스가 가능한 기본 구성

BlueXP에서 Connector를 배포했거나 클라우드 공급업체의 마켓플레이스에서 커넥터를 배포했거나 인터넷에 액세스할 수 있는 온프레미스 Linux 호스트에 수동으로 설치한 경우 다음 구성 세부 정보가 적용됩니다.

AWS 세부 정보

BlueXP 또는 클라우드 제공업체의 마켓플레이스에서 Connector를 배포한 경우 다음 사항에 유의하십시오.

- EC2 인스턴스 유형은 T3.xLarge입니다.
- 이미지의 운영 체제는 Ubuntu 22.04 LTS입니다.

운영 체제에는 GUI가 포함되어 있지 않습니다. 시스템에 액세스하려면 터미널을 사용해야 합니다.

- EC2 Linux 인스턴스의 사용자 이름은 Ubuntu입니다(2023년 5월 이전에 생성된 커넥터의 경우 사용자 이름은 EC2-user입니다).
- 기본 시스템 디스크는 100GiB GP2 디스크입니다.

Azure 세부 정보

BlueXP 또는 클라우드 제공업체의 마켓플레이스에서 Connector를 배포한 경우 다음 사항에 유의하십시오.

- VM 유형은 DS3 v2입니다.
- 이미지의 운영 체제는 Ubuntu 22.04 LTS입니다.

운영 체제에는 GUI가 포함되어 있지 않습니다. 시스템에 액세스하려면 터미널을 사용해야 합니다.

- 기본 시스템 디스크는 100GiB 프리미엄 SSD 디스크입니다.

Google Cloud 세부 정보

BlueXP에서 커넥터를 배포한 경우 다음 사항에 유의하십시오.

- VM 인스턴스는 n2-standard-4입니다.
- 이미지의 운영 체제는 Ubuntu 22.04 LTS입니다.

운영 체제에는 GUI가 포함되어 있지 않습니다. 시스템에 액세스하려면 터미널을 사용해야 합니다.

- 기본 시스템 디스크는 100GiB SSD 영구 디스크입니다.

설치 폴더

Connector 설치 폴더는 다음 위치에 있습니다.

`/opt/application/netapp/cloudmanager`입니다

로그 파일

로그 파일은 다음 폴더에 들어 있습니다.

- `/opt/application/netapp/cloudmanager/log`입니다
또는
- `/opt/application/netapp/service-manager-2/로그`(새로운 3.9.23 설치부터 시작)

이러한 폴더의 로그에는 Connector 및 Docker 이미지에 대한 세부 정보가 나와 있습니다.

- `/opt/application/netapp/cloudmanager/docker/데이터/로그`

이 폴더의 로그에는 Connector에서 실행되는 클라우드 서비스 및 BlueXP 서비스에 대한 세부 정보가 나와 있습니다.

커넥터 서비스

- BlueXP 서비스의 이름은 `occm`입니다.
- `occm` 서비스는 MySQL 서비스에 따라 달라진다.

MySQL 서비스가 다운되면 `occm` 서비스도 다운됩니다.

포트

커넥터는 Linux 호스트에서 다음 포트를 사용합니다.

- HTTP 액세스용 80
- HTTPS 액세스용 443

인터넷 액세스가 없는 기본 구성

인터넷 액세스가 없는 온프레미스 Linux 호스트에 커넥터를 수동으로 설치한 경우 다음 구성이 적용됩니다. ["이 설치 옵션에 대해 자세히 알아보십시오"](#).

- Connector 설치 폴더는 다음 위치에 있습니다.

`/opt/application/netapp/DS`

- 로그 파일은 다음 폴더에 들어 있습니다.

`/var/lib/docker/volumes/DS_occmpdata/_data/log`

이 폴더의 로그에는 Connector 및 Docker 이미지에 대한 세부 정보가 나와 있습니다.

- 모든 서비스가 Docker 컨테이너 내부에서 실행 중입니다

서비스는 실행 중인 Docker 런타임 서비스에 따라 다릅니다

- 커넥터는 Linux 호스트에서 다음 포트를 사용합니다.

- HTTP 액세스용 80
- HTTPS 액세스용 443

자격 증명 및 구독

설치하고

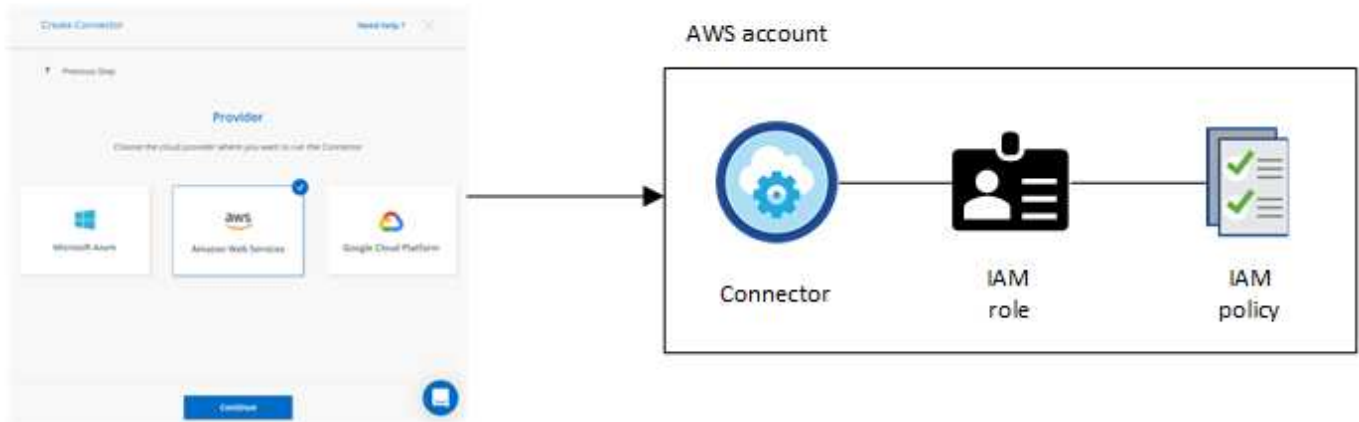
AWS 자격 증명 및 권한에 대해 알아보십시오

BlueXP가 AWS 자격 증명을 사용하여 대신 작업을 수행하는 방법과 해당 자격 증명이 마켓플레이스 구독과 어떻게 연관되는지 알아보십시오. BlueXP에서 하나 이상의 AWS 계정에 대한 자격 증명을 관리할 때 이러한 세부 정보를 이해하는 것이 도움이 될 수 있습니다. 예를 들어, BlueXP에 AWS 자격 증명을 추가해야 하는 시기를 알 수 있습니다.


초기 **AWS** 자격 증명

BlueXP에서 커넥터를 배포할 때는 IAM 사용자의 ARN 또는 액세스 키를 제공해야 합니다. 사용하는 인증 방법에는 Connector 인스턴스를 AWS에 구축하는 데 필요한 권한이 있어야 합니다. 필요한 권한이 에 나열됩니다 ["AWS의 커넥터 구축 정책"](#).

BlueXP가 AWS에서 Connector 인스턴스를 시작하면 IAM 역할과 해당 인스턴스에 대한 인스턴스 프로필이 생성됩니다. 또한 Connector에 해당 AWS 계정 내의 리소스 및 프로세스를 관리할 수 있는 권한을 제공하는 정책을 첨부합니다. ["BlueXP에서 사용 권한을 사용하는 방법을 검토합니다"](#).



Cloud Volumes ONTAP에 대한 새 작업 환경을 생성하는 경우 BlueXP는 기본적으로 다음 AWS 자격 증명을 선택합니다.

Details & Credentials			
Instance Profile Credentials	 Account ID	QA Subscription Marketplace Subscription	Edit Credentials

초기 AWS 자격 증명을 사용하여 모든 Cloud Volumes ONTAP 시스템을 구축하거나 추가 자격 증명을 추가할 수 있습니다.

추가 **AWS** 자격 증명

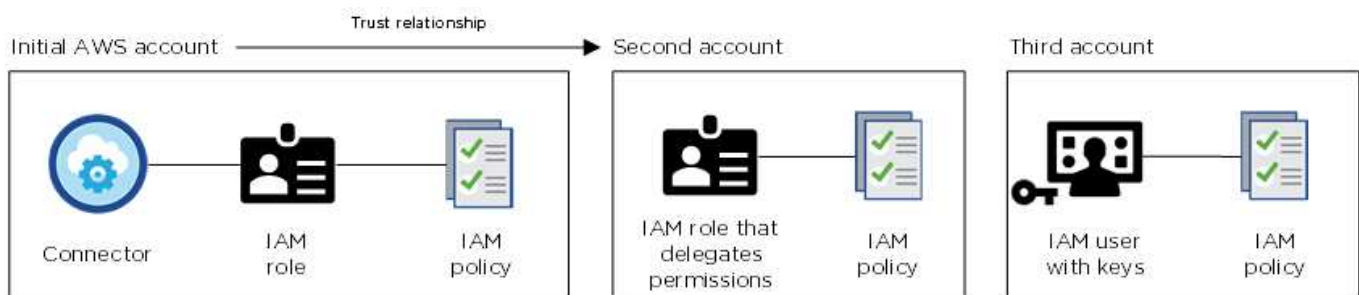
다음 두 가지 방법으로 AWS 자격 증명을 추가할 수 있습니다.

- 기존 Connector에 AWS 자격 증명을 추가할 수 있습니다
- AWS 자격 증명을 BlueXP에 직접 추가할 수 있습니다

자세한 내용은 아래 섹션을 참조하십시오.

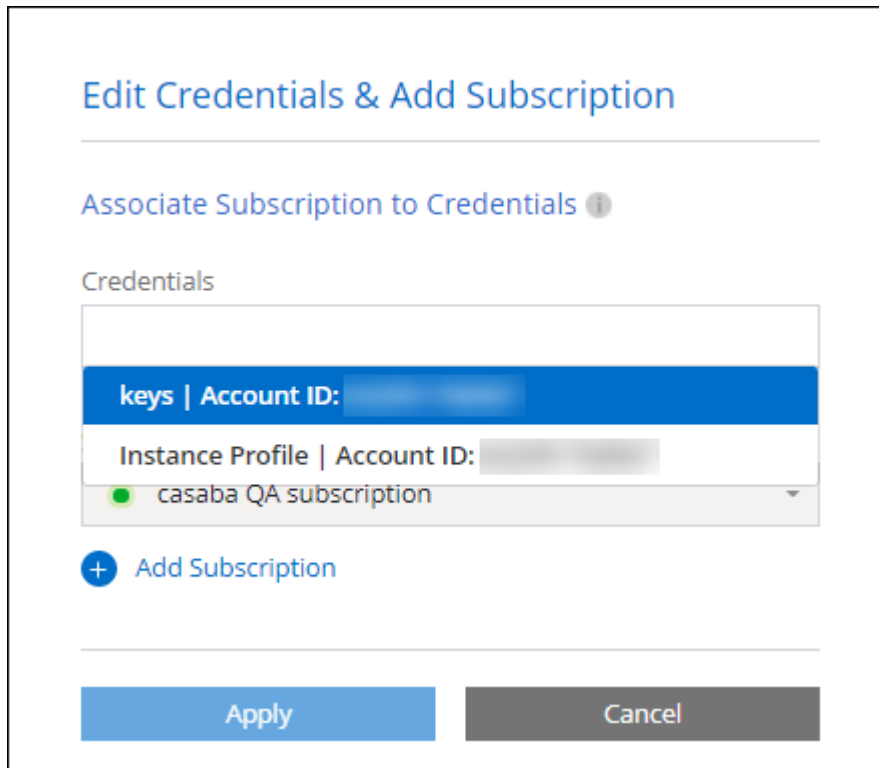
기존 커넥터에 **AWS** 자격 증명을 추가합니다

추가 AWS 계정과 함께 BlueXP를 사용하려면 IAM 사용자를 위한 AWS 키 또는 신뢰할 수 있는 계정에서 역할의 ARN을 제공할 수 있습니다. 다음 이미지는 두 개의 추가 계정을 보여 줍니다. 하나는 신뢰할 수 있는 계정에서 IAM 역할을 통해 권한을 제공하고 다른 하나는 IAM 사용자의 AWS 키를 통해 권한을 제공합니다.



그런 다음 IAM 역할의 ARN(Amazon Resource Name)이나 IAM 사용자의 AWS 키를 지정하여 BlueXP에 계정 자격 증명을 추가합니다.

예를 들어, 새 Cloud Volumes ONTAP 작업 환경을 생성할 때 자격 증명 간에 전환할 수 있습니다.



The screenshot shows a web interface titled "Edit Credentials & Add Subscription". Below the title is a section "Associate Subscription to Credentials" with an information icon. Underneath is a "Credentials" section containing a list of credentials. The first credential is highlighted with a blue bar and labeled "keys | Account ID:". Below this, there is a section for "Instance Profile | Account ID:" with a greyed-out input field. A green dot and the text "casaba QA subscription" are visible below the instance profile section. At the bottom of the dialog are two buttons: "Apply" (blue) and "Cancel" (grey).

"기존 커넥터에 AWS 자격 증명을 추가하는 방법에 대해 알아보십시오."

BlueXP에 AWS 자격 증명을 직접 추가합니다

BlueXP에 새 AWS 자격 증명을 추가하면 ONTAP 작업 환경에 대한 FSx를 생성 및 관리하거나 커넥터를 생성하는 데 필요한 권한이 제공됩니다.

- "ONTAP용 Amazon FSx용 BlueXP에 AWS 자격 증명을 추가하는 방법에 대해 알아보십시오"
- "Connector를 생성하기 위해 BlueXP에 AWS 자격 증명을 추가하는 방법에 대해 알아보십시오"

자격 증명 및 마켓플레이스 구독

커넥터에 추가하는 자격 증명은 AWS Marketplace 구독과 연결되어 시간 단위(PAYGO) 또는 연간 계약을 통해 Cloud Volumes ONTAP에 대한 비용을 지불하고 다른 BlueXP 서비스를 사용할 수 있어야 합니다.

"AWS 구독을 연결하는 방법을 알아보십시오".

AWS 자격 증명 및 마켓플레이스 구독에 대해서는 다음을 참조하십시오.

- AWS Marketplace 구독은 하나의 AWS 자격 증명 집합과 연결할 수 있습니다
- 기존 마켓플레이스 구독을 새 구독으로 바꿀 수 있습니다

FAQ 를 참조하십시오

다음은 자격 증명 및 구독과 관련된 질문입니다.

AWS 자격 증명을 안전하게 회전하려면 어떻게 해야 하나요?

위 섹션에서 설명한 것처럼 BlueXP를 이용하면 커넥터 인스턴스와 연결된 IAM 역할이나 신뢰할 수 있는 계정에서 IAM 역할을 가정하거나 AWS 액세스 키를 제공하는 등 몇 가지 방법으로 AWS 자격 증명을 제공할 수 있습니다.

처음 두 가지 옵션을 사용할 경우 BlueXP는 AWS 보안 토큰 서비스를 사용하여 지속적으로 회전하는 임시 자격 증명을 얻습니다. 이 프로세스는 자동 및 안전의 모범 사례입니다.

BlueXP에 AWS 액세스 키를 제공하는 경우 정기적으로 BlueXP에서 키를 업데이트하여 키를 회전해야 합니다. 이는 완전히 수동으로 진행되는 프로세스입니다.

Cloud Volumes ONTAP 작업 환경에 대한 **AWS Marketplace** 구독을 변경할 수 있습니까?

예, 가능합니다. 자격 증명 세트와 연결된 AWS 마켓플레이스 가입을 변경하면 모든 기존 및 신규 Cloud Volumes ONTAP 작업 환경이 새 구독에 대해 요금이 청구됩니다.

["AWS 구독을 연결하는 방법을 알아보십시오"](#).

마켓플레이스 구독이 서로 다른 여러 **AWS** 자격 증명을 추가할 수 있습니까?

동일한 AWS 계정에 속한 모든 AWS 자격 증명은 동일한 AWS 마켓플레이스 구독에 연결됩니다.

서로 다른 AWS 계정에 속하는 여러 AWS 자격 증명이 있는 경우 해당 자격 증명을 동일한 AWS Marketplace 구독 또는 다른 구독에 연결할 수 있습니다.

기존 **Cloud Volumes ONTAP** 작업 환경을 다른 **AWS** 계정으로 이동할 수 있습니까?

아니요, Cloud Volumes ONTAP 작업 환경에 연결된 AWS 리소스를 다른 AWS 계정으로 이동할 수 없습니다.

마켓플레이스 배포 및 온프레미스 배포에 자격 증명이 어떻게 작동하나요?

위 섹션에서는 BlueXP의 커넥터에 권장되는 배포 방법에 대해 설명합니다. AWS Marketplace에서 Connector를 AWS에 구축할 수도 있고, 자신의 Linux 호스트에 Connector 소프트웨어를 수동으로 설치할 수도 있습니다.

Marketplace를 사용하는 경우 사용 권한이 동일한 방식으로 제공됩니다. IAM 역할을 수동으로 생성 및 설정한 다음 추가 계정에 대한 권한을 제공하면 됩니다.

온-프레미스 배포의 경우 BlueXP 시스템에 대해 IAM 역할을 설정할 수 없지만 AWS 액세스 키를 사용하여 권한을 제공할 수 있습니다.

사용 권한을 설정하는 방법은 다음 페이지를 참조하십시오.

- 표준 모드
 - ["AWS Marketplace 구축에 대한 사용 권한을 설정합니다"](#)
 - ["온프레미스 배포에 대한 권한을 설정합니다"](#)
- ["제한된 모드에 대한 권한을 설정합니다"](#)

- ["비공개 모드에 대한 권한을 설정합니다"](#)

BlueXP의 AWS 자격 증명 및 마켓플레이스 가입을 관리합니다

BlueXP에서 AWS 계정에 클라우드 리소스를 배포하고 관리하는 데 필요한 권한을 갖도록 AWS 자격 증명을 추가 및 관리합니다. 여러 AWS Marketplace 구독을 관리하는 경우 자격 증명 페이지에서 각 구독을 서로 다른 AWS 자격 증명에 할당할 수 있습니다.

개요

기존 커넥터 또는 BlueXP에 AWS 자격 증명을 추가할 수 있습니다.

- 기존 커넥터에 AWS 자격 증명을 추가합니다

기존 Connector에 AWS 자격 증명을 추가하면 퍼블릭 클라우드 환경 내의 리소스 및 프로세스를 관리하는 데 필요한 권한이 제공됩니다. [Connector에 AWS 자격 증명을 추가하는 방법에 대해 알아보십시오.](#)

- Connector 생성을 위해 BlueXP에 AWS 자격 증명을 추가합니다

BlueXP에 새 AWS 자격 증명을 추가하면 BlueXP에서 커넥터를 생성하는 데 필요한 권한을 얻을 수 있습니다. [BlueXP에 AWS 자격 증명을 추가하는 방법에 대해 알아보십시오.](#)

- ONTAP용 FSx용 BlueXP에 AWS 자격 증명을 추가합니다

BlueXP에 새로운 AWS 자격 증명을 추가하면 ONTAP용 FSx를 생성 및 관리하는 데 필요한 권한이 BlueXP에 부여됩니다. ["ONTAP용 FSx에 대한 사용 권한을 설정하는 방법에 대해 알아보십시오"](#)

자격 증명을 회전하는 방법

BlueXP를 사용하면 Connector 인스턴스와 연관된 IAM 역할, 신뢰할 수 있는 계정에서 IAM 역할을 가정하거나 AWS 액세스 키를 제공하여 AWS 자격 증명을 제공할 수 있습니다. ["AWS 자격 증명 및 권한에 대해 자세히 알아보십시오"](#).

처음 두 가지 옵션을 사용할 경우 BlueXP는 AWS 보안 토큰 서비스를 사용하여 지속적으로 회전하는 임시 자격 증명을 얻습니다. 이 프로세스는 자동적이며 안전하기 때문에 가장 좋은 방법입니다.

BlueXP에 AWS 액세스 키를 제공하는 경우 정기적으로 BlueXP에서 키를 업데이트하여 키를 회전해야 합니다. 이는 완전히 수동으로 진행되는 프로세스입니다.

Connector에 추가 자격 증명을 추가합니다

Connector에 추가 AWS 자격 증명을 추가하여 퍼블릭 클라우드 환경 내에서 리소스 및 프로세스를 관리하는 데 필요한 권한을 부여합니다. 다른 계정에서 IAM 역할의 ARN을 제공하거나 AWS 액세스 키를 제공할 수 있습니다.

BlueXP를 처음 사용하는 경우 ["BlueXP에서 AWS 자격 증명과 사용 권한을 사용하는 방법에 대해 알아보십시오"](#).

권한을 부여합니다

Connector에 AWS 자격 증명을 추가하기 전에 필요한 권한을 제공해야 합니다. 권한을 통해 BlueXP는 해당 AWS 계정 내의 리소스와 프로세스를 관리할 수 있습니다. 사용 권한을 제공하는 방법은 BlueXP에서 신뢰할 수 있는 계정 또는 AWS 키의 역할을 ARN으로 제공할지 여부에 따라 달라집니다.



BlueXP에서 커넥터를 배포한 경우, BlueXP는 Connector를 배포한 계정에 대해 AWS 자격 증명을 자동으로 추가했습니다. AWS Marketplace에서 Connector를 배포했거나 기존 시스템에 Connector 소프트웨어를 수동으로 설치한 경우에는 이 초기 계정이 추가되지 않습니다. ["AWS 자격 증명 및 권한에 대해 알아보십시오"](#).

- 선택 *
- [다른 계정에서 IAM 역할을 가정하여 권한을 부여합니다](#)
- [AWS 키를 제공하여 권한을 부여합니다](#)

다른 계정에서 **IAM** 역할을 가정하여 권한을 부여합니다

IAM 역할을 사용하여 Connector 인스턴스를 구축한 소스 AWS 계정과 다른 AWS 계정 간에 신뢰 관계를 설정할 수 있습니다. 그런 다음 신뢰할 수 있는 계정의 IAM 역할 ARN을 BlueXP에 제공합니다.

Connector가 구내에 설치되어 있으면 이 인증 방법을 사용할 수 없습니다. AWS 키를 사용해야 합니다.

단계

1. Connector에 권한을 제공하려는 대상 계정의 IAM 콘솔로 이동합니다.
2. 액세스 관리에서 * 역할 > 역할 만들기 * 를 선택하고 단계를 따라 역할을 만듭니다.

다음을 수행하십시오.

- 신뢰할 수 있는 엔터티 유형 * 에서 * AWS 계정 * 을 선택합니다.
- 다른 AWS 계정 * 을 선택하고 Connector 인스턴스가 있는 계정의 ID를 입력합니다.
- 의 내용을 복사하여 붙여 넣어 필요한 정책을 만듭니다 ["Connector에 대한 IAM 정책"](#).

3. 나중에 BlueXP에 붙여넣을 수 있도록 IAM 역할의 역할 ARN을 복사합니다.

결과

이제 계정에 필요한 권한이 있습니다. [이제 Connector에 자격 증명을 추가할 수 있습니다](#).

AWS 키를 제공하여 권한을 부여합니다

BlueXP에 IAM 사용자를 위한 AWS 키를 제공하려면 해당 사용자에게 필요한 권한을 부여해야 합니다. BlueXP IAM 정책은 BlueXP에서 사용할 수 있는 AWS 작업 및 리소스를 정의합니다.

Connector가 구내에 설치된 경우 이 인증 방법을 사용해야 합니다. IAM 역할을 사용할 수 없습니다.

단계

1. IAM 콘솔에서 의 내용을 복사하여 붙여 넣어 정책을 생성합니다 ["Connector에 대한 IAM 정책"](#).

["AWS 설명서: IAM 정책 생성"](#)

2. IAM 역할 또는 IAM 사용자에게 정책을 연결합니다.

- ["AWS 설명서: IAM 역할 생성"](#)
- ["AWS 설명서: IAM 정책 추가 및 제거"](#)

결과

이제 계정에 필요한 권한이 있습니다. [이제 Connector에 자격 증명을 추가할 수 있습니다.](#)

자격 증명을 추가합니다

필요한 권한이 있는 AWS 계정을 제공한 후 해당 계정의 자격 증명을 기존 Connector에 추가할 수 있습니다. 이렇게 하면 동일한 커넥터를 사용하여 해당 계정에서 Cloud Volumes ONTAP 시스템을 시작할 수 있습니다.

시작하기 전에

클라우드 공급자에서 이러한 자격 증명을 만든 경우 사용할 수 있을 때까지 몇 분 정도 걸릴 수 있습니다. BlueXP에 자격 증명을 추가하기 전에 몇 분 정도 기다립니다.

단계

1. 현재 BlueXP에서 올바른 커넥터가 선택되어 있는지 확인합니다.
2. BlueXP 콘솔의 오른쪽 상단에서 설정 아이콘을 선택하고 * 자격 증명 * 을 선택합니다.



3. 계정 자격 증명 * 페이지에서 * 자격 증명 추가 * 를 선택하고 마법사의 단계를 따릅니다.
 - a. * 자격 증명 위치 *: * Amazon Web Services > Connector * 를 선택합니다.
 - b. * 자격 증명 정의 *: 신뢰할 수 있는 IAM 역할의 ARN(Amazon Resource Name)을 제공하거나 AWS 액세스 키와 비밀 키를 입력합니다.
 - c. * Marketplace 구독 *: 지금 가입하거나 기존 구독을 선택하여 마켓플레이스 구독을 이러한 자격 증명과 연결합니다.

PAYGO(시간별 비용) 또는 연간 계약으로 BlueXP 서비스에 대한 비용을 지불하려면 AWS Marketplace 구독과 AWS 자격 증명이 연결되어 있어야 합니다.
 - d. * 검토 *: 새 자격 증명에 대한 세부 정보를 확인하고 * 추가 * 를 선택합니다.

결과

이제 새 작업 환경을 만들 때 세부 정보 및 자격 증명 페이지에서 다른 자격 증명 세트로 전환할 수 있습니다.

Connector 생성을 위해 **BlueXP**에 자격 증명을 추가합니다

BlueXP에 Connector 생성에 필요한 권한을 제공하는 IAM 역할의 ARN을 제공하여 BlueXP에 AWS 자격 증명을 추가합니다. 새 Connector를 만들 때 이러한 자격 증명을 선택할 수 있습니다.

IAM 역할을 설정합니다

BlueXP SaaS 계층이 역할을 맡을 수 있도록 IAM 역할을 설정합니다.

단계

1. 대상 계정에서 IAM 콘솔로 이동합니다.
2. 액세스 관리에서 * 역할 > 역할 만들기 * 를 선택하고 단계를 따라 역할을 만듭니다.

다음을 수행하십시오.

- 신뢰할 수 있는 엔터티 유형 * 에서 * AWS 계정 * 을 선택합니다.
- 다른 AWS 계정 * 을 선택하고 BlueXP SaaS ID:952013314444를 입력합니다
- Connector를 만드는 데 필요한 권한을 포함하는 정책을 만듭니다.
 - "ONTAP용 FSx에 필요한 권한을 봅니다"
 - "Connector 배포 정책을 봅니다"

3. 다음 단계에서 BlueXP에 붙여넣을 수 있도록 IAM 역할의 역할 ARN을 복사합니다.

결과

이제 IAM 역할에 필요한 권한이 있습니다. 이제 **BlueXP**에 추가할 수 있습니다.

자격 증명을 추가합니다

필요한 권한을 IAM 역할에 제공한 후 ARN 역할을 BlueXP에 추가합니다.

시작하기 전에

방금 IAM 역할을 생성한 경우 사용할 수 있을 때까지 몇 분 정도 걸릴 수 있습니다. BlueXP에 자격 증명을 추가하기 전에 몇 분 정도 기다립니다.

단계

1. BlueXP 콘솔의 오른쪽 상단에서 설정 아이콘을 선택하고 * 자격 증명 * 을 선택합니다.



2. 계정 자격 증명 * 페이지에서 * 자격 증명 추가 * 를 선택하고 마법사의 단계를 따릅니다.
 - a. * 자격 증명 위치 *: * Amazon Web Services > BlueXP * 를 선택합니다.
 - b. * 자격 증명 정의 *: IAM 역할의 ARN(Amazon Resource Name)을 제공합니다.
 - c. * 검토 *: 새 자격 증명에 대한 세부 정보를 확인하고 * 추가 * 를 선택합니다.

결과

이제 새 커넥터를 만들 때 자격 증명을 사용할 수 있습니다.

ONTAP용 Amazon FSx용 BlueXP에 자격 증명을 추가합니다

자세한 내용은 를 참조하십시오 ["ONTAP용 Amazon FSx에 대한 BlueXP 문서"](#)

AWS 구독을 연결합니다

BlueXP에 AWS 자격 증명을 추가한 후 AWS Marketplace 구독을 해당 자격 증명과 연결할 수 있습니다. 이 구독을 통해 PAYGO(hourly rate)로 Cloud Volumes ONTAP를 결제하거나 연간 계약을 통해 다른 BlueXP 서비스를 사용할 수 있습니다.

BlueXP에 자격 증명을 추가한 후 AWS Marketplace 구독을 연결할 수 있는 두 가지 시나리오가 있습니다.

- 처음에 BlueXP에 자격 증명을 추가할 때 구독을 연결하지 않았습니다.
- AWS 자격 증명과 연결된 AWS Marketplace 구독을 변경하려고 합니다.

현재 마켓플레이스 구독을 새 구독으로 교체하면 기존 Cloud Volumes ONTAP 작업 환경과 모든 새로운 작업 환경에 대한 마켓플레이스 구독이 변경됩니다.

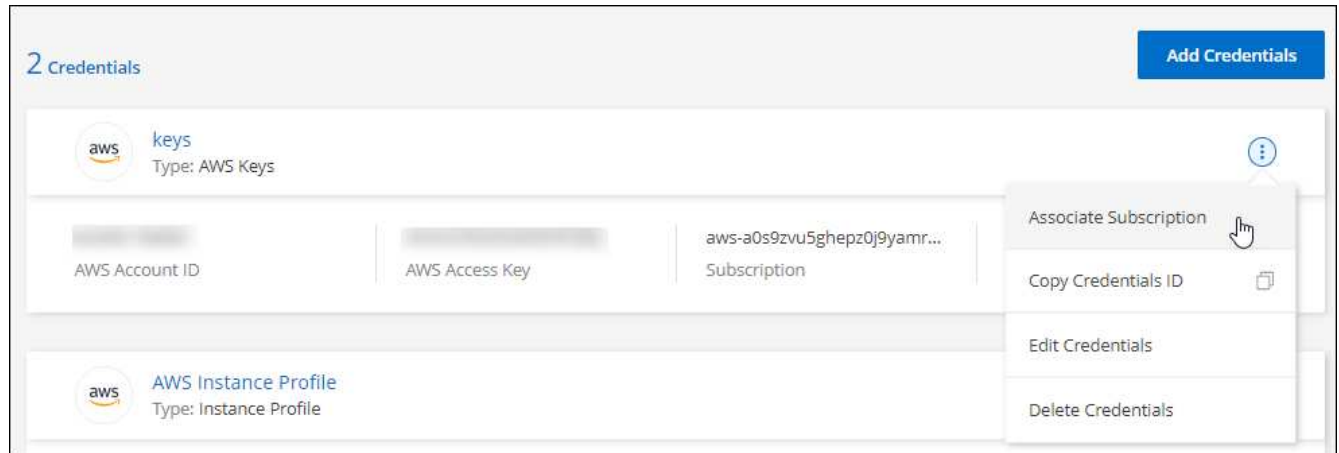
시작하기 전에

BlueXP 설정을 변경하려면 먼저 커넥터를 만들어야 합니다. ["커넥터를 만드는 방법에 대해 알아봅니다"](#).

단계

1. BlueXP 콘솔의 오른쪽 상단에서 설정 아이콘을 선택하고 * 자격 증명 * 을 선택합니다.
2. 자격 증명 집합에 대한 작업 메뉴를 선택한 다음 * 가입 연결 * 을 선택합니다.

Connector와 연결된 자격 증명을 선택해야 합니다. BlueXP와 연결된 자격 증명과 마켓플레이스 구독을 연결할 수 없습니다.



3. 자격 증명을 기존 구독과 연결하려면 드롭다운 목록에서 구독을 선택하고 * Associate * 를 선택합니다.

4. 자격 증명을 새 구독과 연결하려면 * 구독 추가 > 계속 * 을 선택하고 AWS 마켓플레이스의 단계를 따릅니다.

a. 구매 옵션 보기 * 를 선택합니다.

b. 가입 * 을 선택합니다.

c. 계정 설정 * 을 선택합니다.

BlueXP 웹 사이트로 이동합니다.

d. [구독 할당 *] 페이지에서:

- 이 구독을 연결할 BlueXP 계정을 선택합니다.
- 기존 구독 바꾸기 * 필드에서 하나의 계정에 대한 기존 구독을 이 새 구독으로 자동 대체할지 여부를 선택합니다.

BlueXP는 계정의 모든 자격 증명에 대한 기존 구독을 이 새 구독으로 대체합니다. 자격 증명 집합이 구독과 연결되지 않은 경우 이 새 구독은 해당 자격 증명과 연결되지 않습니다.

다른 모든 계정의 경우 이 단계를 반복하여 구독을 수동으로 연결해야 합니다.

- 저장 * 을 선택합니다.

다음 비디오에서는 AWS 마켓플레이스를 구독하는 단계를 보여줍니다.

AWS 마켓플레이스에서 BlueXP를 구독하십시오

기존 구독을 계정에 연결합니다

AWS 마켓플레이스에서 BlueXP를 구독하는 경우 프로세스의 마지막 단계는 BlueXP 웹 사이트의 구독과 BlueXP 계정을 연결하는 것입니다. 이 단계를 완료하지 않은 경우 BlueXP 계정에 가입을 사용할 수 없습니다.

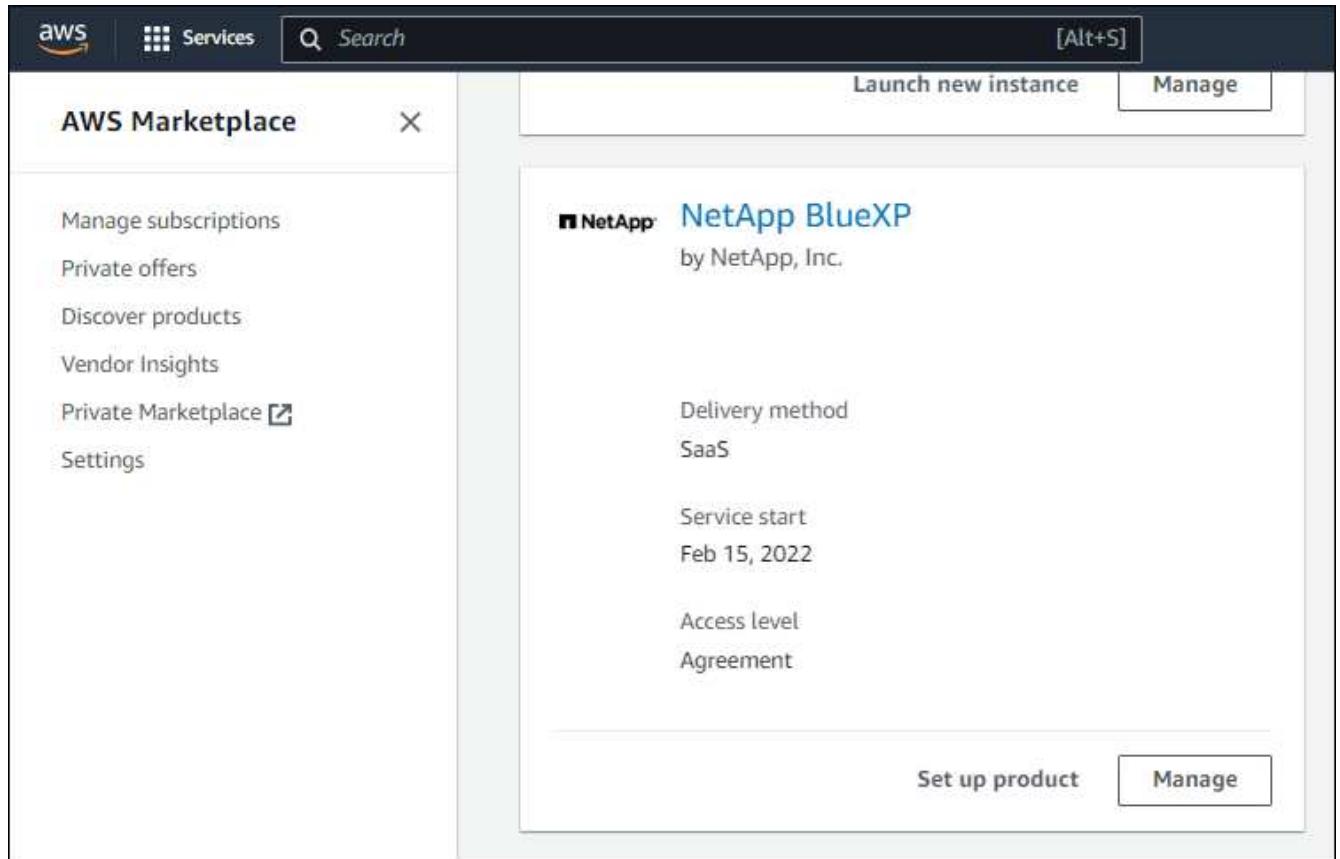
AWS 마켓플레이스에서 BlueXP를 구독했지만 구독과 계정을 연결하는 단계를 놓친 경우 아래 단계를 따르십시오.

단계

1. BlueXP 디지털 지갑으로 이동하여 구독 요금과 BlueXP 계정의 연결이 아닌지 확인합니다.
 - a. BlueXP 탐색 메뉴에서 * Governance > Digital Wallet * 을 선택합니다.
 - b. 구독 * 을 선택합니다.
 - c. BlueXP 구독이 나타나지 않는지 확인합니다.

현재 보고 있는 계정과 연결된 구독만 표시됩니다. 구독이 표시되지 않으면 다음 단계를 진행합니다.

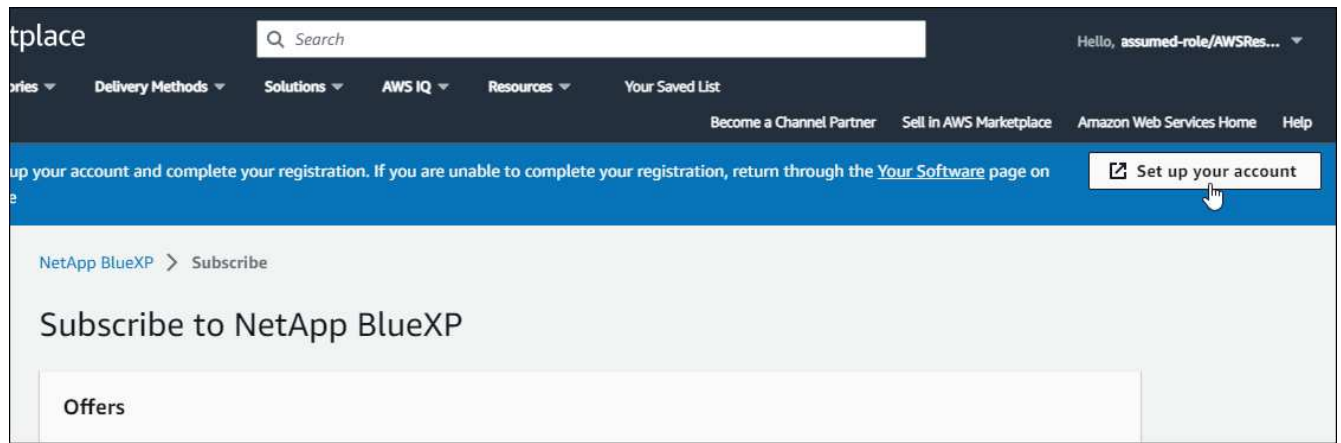
2. AWS 콘솔에 로그인하고 * AWS Marketplace 구독 * 으로 이동합니다.
3. NetApp BlueXP 구독을 찾을 수 있습니다.



4. 제품 설정 * 을 선택합니다.

구독 제안 페이지는 새 브라우저 탭 또는 창에 로드되어야 합니다.

5. 계정 설정 * 을 선택합니다.



netapp.com 의 * 구독 할당 * 페이지가 새 브라우저 탭 또는 창에 로드되어야 합니다.

먼저 BlueXP에 로그인하라는 메시지가 표시될 수 있습니다.

6. [구독 할당 *] 페이지에서:

- 이 구독을 연결할 BlueXP 계정을 선택합니다.
- 기존 구독 바꾸기 * 필드에서 하나의 계정에 대한 기존 구독을 이 새 구독으로 자동 대체할지 여부를 선택합니다.

BlueXP는 계정의 모든 자격 증명에 대한 기존 구독을 이 새 구독으로 대체합니다. 자격 증명 집합이 구독과 연결되지 않은 경우 이 새 구독은 해당 자격 증명과 연결되지 않습니다.

다른 모든 계정의 경우 이 단계를 반복하여 구독을 수동으로 연결해야 합니다.

Subscription Assignment

✓
Your subscription to BlueXP / Cloud Volumes ONTAP from the AWS Marketplace was created successfully.

Subscription name
PayAsYouGo

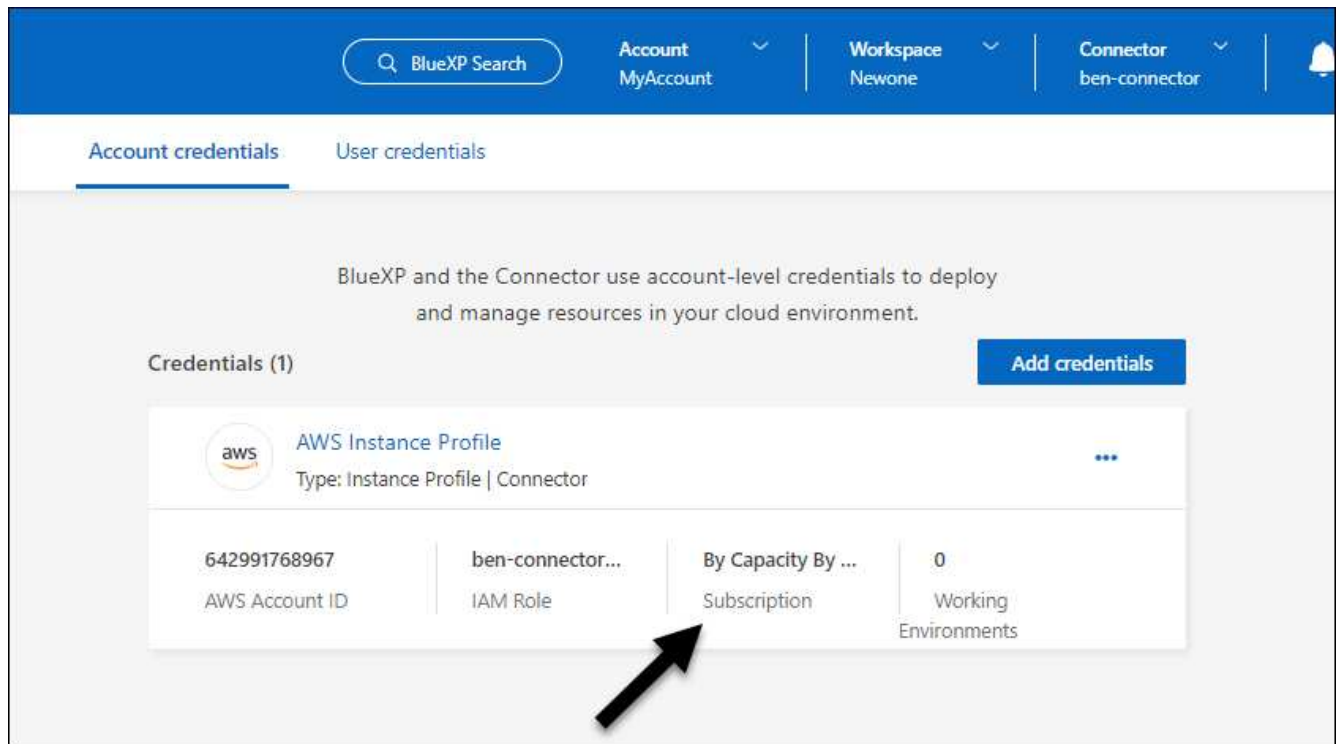
Select the NetApp accounts that you'd like to associate this subscription with.
You can automatically replace the existing subscription for one account with this new subscription.

NetApp account	Replace existing subscription
<input checked="" type="checkbox"/> cloudTiering_undefined	<input type="checkbox"/>
<input checked="" type="checkbox"/> CS-HhewH	<input type="checkbox"/>
<input checked="" type="checkbox"/> benAccount	<input checked="" type="checkbox"/>

Save

7. BlueXP 디지털 지갑으로 이동하여 구독이 BlueXP 계정과 연결되어 있는지 확인합니다.
 - a. BlueXP 탐색 메뉴에서 * Governance > Digital Wallet * 을 선택합니다.
 - b. 구독 * 을 선택합니다.
 - c. BlueXP 구독이 나타나는지 확인합니다.
8. 구독이 AWS 자격 증명과 연결되어 있는지 확인합니다.
 - a. BlueXP 콘솔의 오른쪽 상단에서 설정 아이콘을 선택하고 * 자격 증명 * 을 선택합니다.
 - b. 계정 자격 증명 * 페이지에서 구독이 AWS 자격 증명과 연결되어 있는지 확인합니다.

예를 들어,



자격 증명을 편집합니다

계정 유형(AWS 키 또는 역할 담당)을 변경하거나, 이름을 편집하거나, 자격 증명(키 또는 ARN 역할)을 업데이트하여 BlueXP에서 AWS 자격 증명을 편집합니다.



Connector 인스턴스와 연결된 인스턴스 프로파일의 자격 증명은 편집할 수 없습니다.

단계

1. BlueXP 콘솔의 오른쪽 상단에서 설정 아이콘을 선택하고 * 자격 증명 * 을 선택합니다.
2. 계정 자격 증명 * 페이지에서 자격 증명 세트의 작업 메뉴를 선택한 다음 * 자격 증명 편집 * 을 선택합니다.
3. 필요한 내용을 변경한 다음 * Apply * 를 선택합니다.

자격 증명을 삭제합니다

더 이상 자격 증명 세트가 필요하지 않으면 BlueXP에서 삭제할 수 있습니다. 작업 환경과 연결되지 않은 자격 증명만 삭제할 수 있습니다.



Connector 인스턴스와 연결된 인스턴스 프로파일의 자격 증명은 삭제할 수 없습니다.

단계

1. BlueXP 콘솔의 오른쪽 상단에서 설정 아이콘을 선택하고 * 자격 증명 * 을 선택합니다.
2. 계정 자격 증명 * 페이지에서 자격 증명 세트의 작업 메뉴를 선택한 다음 * 자격 증명 삭제 * 를 선택합니다.
3. 삭제하려면 * 삭제 * 를 선택합니다.

Azure를 지원합니다

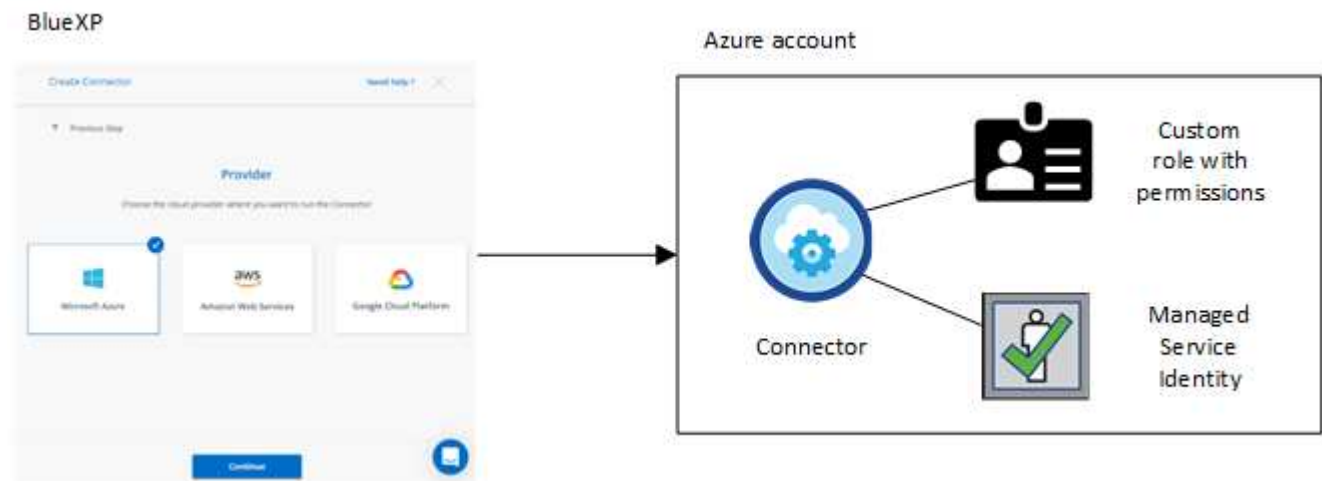
Azure 자격 증명 및 권한에 대해 알아보십시오

BlueXP가 Azure 자격 증명을 사용하여 사용자를 대신하여 작업을 수행하는 방법과 해당 자격 증명이 마켓플레이스 구독과 어떻게 연관되는지 알아보십시오. 이러한 세부 정보를 이해하면 하나 이상의 Azure 구독에 대한 자격 증명을 관리하는 데 도움이 됩니다. 예를 들어, BlueXP에 Azure 자격 증명을 추가해야 하는 시기를 알 수 있습니다.

초기 Azure 자격 증명

BlueXP에서 Connector를 배포하는 경우 Connector 가상 시스템을 배포할 수 있는 권한이 있는 Azure 계정 또는 서비스 보안 주체를 사용해야 합니다. 필요한 권한이 에 나열됩니다 ["Azure용 커넥터 배포 정책"](#).

BlueXP가 Azure에 Connector 가상 시스템을 배포하면 가 활성화됩니다 ["시스템에서 할당한 관리 ID입니다"](#) 가상 머신에서 사용자 지정 역할을 생성하고 가상 머신에 할당합니다. BlueXP는 이 역할을 통해 Azure 가입 내에서 리소스와 프로세스를 관리하는 데 필요한 권한을 얻을 수 있습니다. ["BlueXP에서 사용 권한을 사용하는 방법을 검토합니다"](#).



Cloud Volumes ONTAP에 대한 새 작업 환경을 생성하는 경우 BlueXP는 기본적으로 다음과 같은 Azure 자격 증명을 선택합니다.

Details & Credentials			
Managed Service Ide...	OCCM QA1	ⓘ No subscription is associated	Edit Credentials
Credential Name	Azure Subscription	Marketplace Subscription	

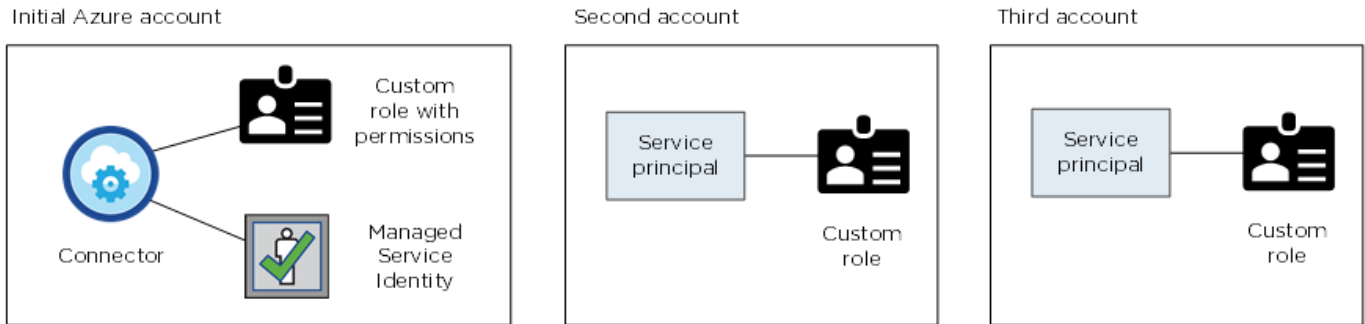
초기 Azure 자격 증명을 사용하여 모든 Cloud Volumes ONTAP 시스템을 배포하거나 추가 자격 증명을 추가할 수 있습니다.

관리되는 ID에 대한 추가 Azure 구독

Connector VM에 할당된 시스템 할당 관리 ID는 Connector를 시작한 구독과 연결됩니다. 다른 Azure 구독을 선택하려면 를 수행해야 합니다 ["관리되는 ID를 해당 구독과 연결합니다"](#).

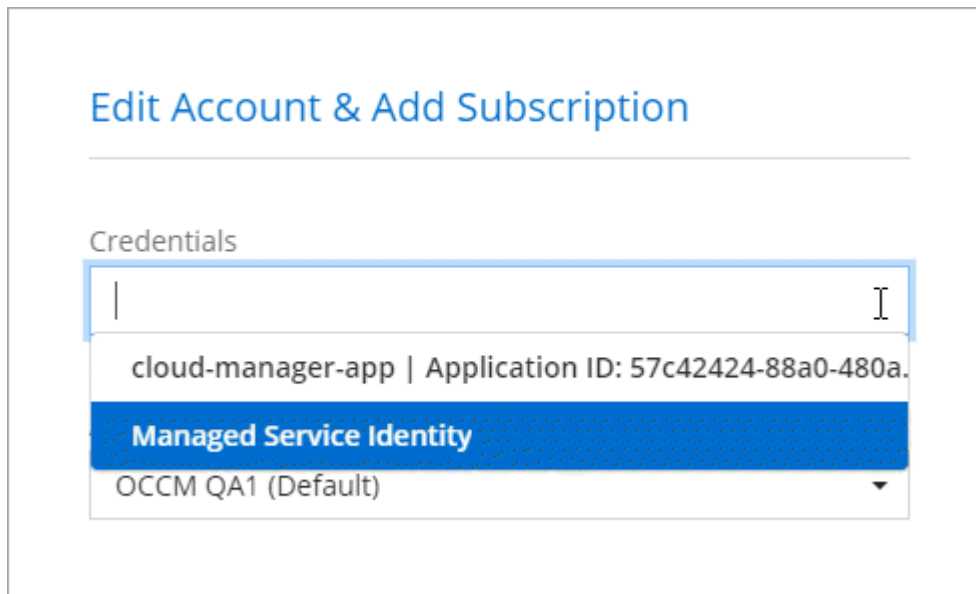
추가 Azure 자격 증명

BlueXP에서 다른 Azure 자격 증명을 사용하려면 에서 필요한 권한을 부여해야 합니다 ["Microsoft Entra ID에서 서비스 보안 주체 만들기 및 설정"](#) 각 Azure 계정에 대해. 다음 그림에서는 두 개의 추가 계정을 보여 줍니다. 각 계정에는 권한을 제공하는 서비스 보안 주체와 사용자 지정 역할이 설정되어 있습니다.



그러면 됩니다 ["계정 자격 증명을 BlueXP에 추가합니다"](#) AD 서비스 보안 주체에 대한 세부 정보를 제공합니다.

예를 들어, 새 Cloud Volumes ONTAP 작업 환경을 생성할 때 자격 증명 간에 전환할 수 있습니다.



자격 증명 및 마켓플레이스 구독

커넥터에 추가하는 자격 증명은 Azure Marketplace 구독과 연결되어 시간 단위(PAYGO) 또는 연간 계약을 통해 Cloud Volumes ONTAP에 대한 비용을 지불하고 다른 BlueXP 서비스를 사용할 수 있어야 합니다.

["Azure 구독을 연결하는 방법에 대해 알아봅니다"](#).

Azure 자격 증명 및 마켓플레이스 구독에 대해서는 다음을 참고하십시오.

- 하나의 Azure Marketplace 구독만 Azure 자격 증명 세트와 연결할 수 있습니다
- 기존 마켓플레이스 구독을 새 구독으로 바꿀 수 있습니다

FAQ 를 참조하십시오

다음 질문은 자격 증명 및 구독과 관련이 있습니다.

Cloud Volumes ONTAP 작업 환경에 대한 **Azure** 마켓플레이스 가입을 변경할 수 있습니까?

예, 가능합니다. Azure 자격 증명 세트와 연결된 Azure 마켓플레이스 구독을 변경하면 기존 및 새 Cloud Volumes ONTAP 작업 환경이 새 구독에 대해 요금이 청구됩니다.

["Azure 구독을 연결하는 방법에 대해 알아봅니다."](#)

마켓플레이스 구독이 서로 다른 여러 **Azure** 자격 증명을 추가할 수 있습니까?

동일한 Azure 구독에 속하는 모든 Azure 자격 증명은 동일한 Azure 마켓플레이스 구독에 연결됩니다.

서로 다른 Azure 구독에 속하는 여러 Azure 자격 증명이 있는 경우 해당 자격 증명을 동일한 Azure Marketplace 구독 또는 다른 마켓플레이스 구독에 연결할 수 있습니다.

기존 **Cloud Volumes ONTAP** 작업 환경을 다른 **Azure** 구독으로 이동할 수 있습니까?

아니요, Cloud Volumes ONTAP 작업 환경에 연결된 Azure 리소스를 다른 Azure 구독으로 이동할 수 없습니다.

마켓플레이스 배포 및 온프레미스 배포에 자격 증명이 어떻게 작동합니까?

위 섹션에서는 BlueXP의 커넥터에 권장되는 배포 방법에 대해 설명합니다. Azure Marketplace에서 Connector를 배포할 수도 있고, 자신의 Linux 호스트에 Connector 소프트웨어를 설치할 수도 있습니다.

마켓플레이스를 사용하는 경우 Connector VM 및 시스템에서 할당한 관리 ID에 사용자 지정 역할을 할당하여 사용 권한을 제공하거나 Microsoft Entra 서비스 보안 주체를 사용할 수 있습니다.

온-프레미스 배포의 경우 Connector에 대해 관리되는 ID를 설정할 수 없지만 서비스 보안 주체를 사용하여 권한을 제공할 수 있습니다.

사용 권한을 설정하는 방법은 다음 페이지를 참조하십시오.

- 표준 모드
 - ["Azure Marketplace 배포에 대한 사용 권한을 설정합니다"](#)
 - ["온프레미스 배포에 대한 권한을 설정합니다"](#)
- "제한된 모드에 대한 권한을 설정합니다"
- ["비공개 모드에 대한 권한을 설정합니다"](#)

BlueXP의 **Azure** 자격 증명 및 마켓플레이스 가입을 관리합니다

Azure 자격 증명을 추가 및 관리하여 BlueXP가 Azure 구독에서 클라우드 리소스를 배포하고 관리하는 데 필요한 권한을 갖도록 합니다. 여러 Azure Marketplace 구독을 관리하는 경우 자격 증명 페이지에서 각 구독을 서로 다른 Azure 자격 증명에 할당할 수 있습니다.

Cloud Volumes ONTAP에 대해 여러 Azure 자격 증명 또는 여러 Azure 마켓플레이스 구독을 사용해야 하는 경우 이 페이지의 단계를 따릅니다.

개요

BlueXP에서 Azure 구독 및 자격 증명을 추가하는 방법에는 두 가지가 있습니다.

1. Azure 구독과 Azure 관리 ID를 추가로 연결합니다.
2. 다른 Azure 자격 증명을 사용하여 Cloud Volumes ONTAP를 배포하려는 경우 서비스 보안 주체를 사용하여 Azure 권한을 부여하고 해당 자격 증명을 BlueXP에 추가합니다.

추가 **Azure** 구독을 관리되는 ID와 연결합니다

BlueXP를 사용하면 Cloud Volumes ONTAP를 배포할 Azure 자격 증명 및 Azure 구독을 선택할 수 있습니다. 를 연결하지 않으면 관리 ID 프로필에 대해 다른 Azure 구독을 선택할 수 없습니다 "**관리 ID**" 있습니다.

이 작업에 대해

관리되는 ID는 입니다 "**초기 Azure 계정입니다**" BlueXP에서 커넥터를 배포하는 경우 Connector를 배포하면 BlueXP 운영자 역할이 생성되어 Connector 가상 머신에 할당됩니다.

단계

1. Azure 포털에 로그인합니다.
2. Subscriptions * 서비스를 연 다음 Cloud Volumes ONTAP를 배포할 구독을 선택합니다.
3. IAM(액세스 컨트롤) * 을 선택합니다.
 - a. Add * > * Add role assignment * 를 선택한 후 권한을 추가합니다.

- BlueXP Operator * 역할을 선택합니다.



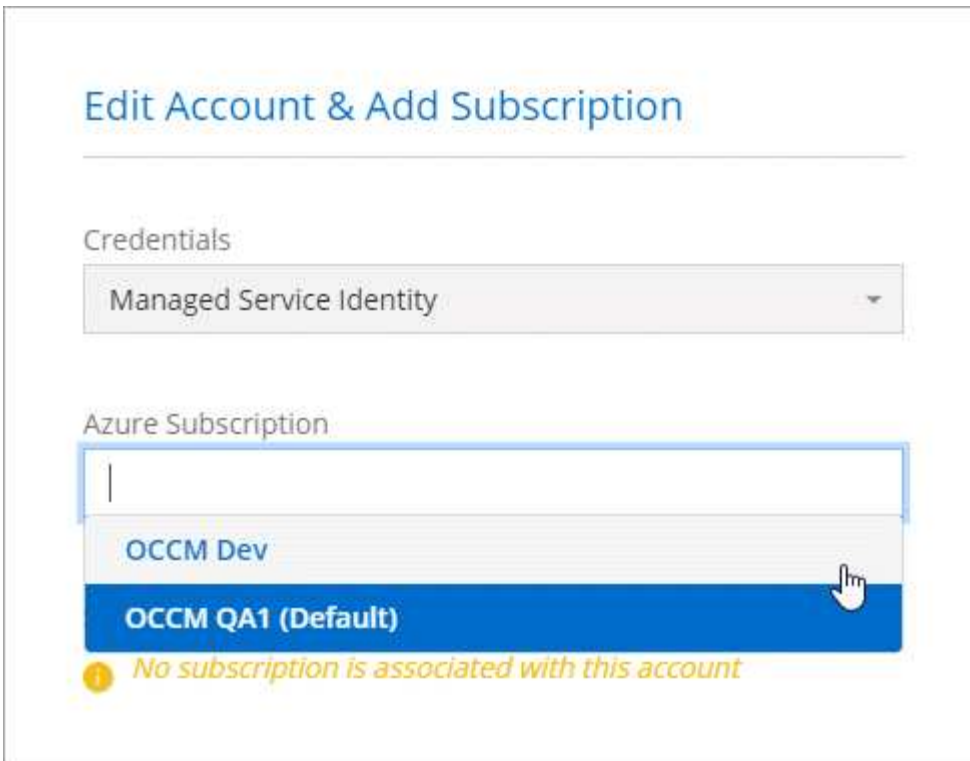
BlueXP 오퍼레이터는 커넥터 정책에 제공된 기본 이름입니다. 역할에 다른 이름을 선택한 경우 대신 해당 이름을 선택합니다.

- Virtual Machine * 에 대한 액세스 권한을 할당합니다.
- Connector 가상 머신이 생성된 서브스크립션을 선택합니다.
- Connector 가상 머신을 선택합니다.
- 저장 * 을 선택합니다.

4. 추가 구독에 대해 이 단계를 반복합니다.

결과

새 작업 환경을 만들 때 이제 관리되는 ID 프로필에 대해 여러 Azure 구독에서 선택할 수 있습니다.



BlueXP에 Azure 자격 증명을 추가합니다

BlueXP에서 커넥터를 배포할 때 BlueXP는 필요한 권한이 있는 가상 시스템에서 시스템에 할당된 관리 ID를 활성화합니다. BlueXP는 Cloud Volumes ONTAP의 새 작업 환경을 만들 때 기본적으로 이러한 Azure 자격 증명을 선택합니다.



기존 시스템에 Connector 소프트웨어를 수동으로 설치한 경우 초기 자격 증명 세트가 추가되지 않습니다. ["Azure 자격 증명 및 권한에 대해 알아보십시오"](#).

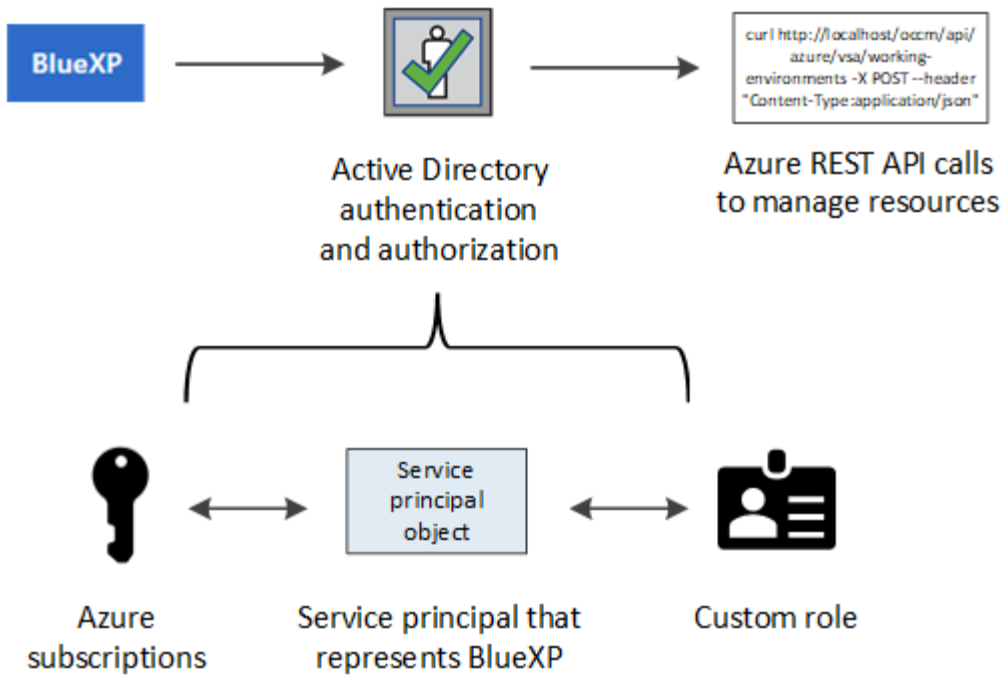
Cloud Volumes ONTAP를 different Azure 자격 증명을 사용하여 배포하려면 각 Azure 계정에 대해 Microsoft Entra ID에서 서비스 보안 주체를 만들고 설정하여 필요한 권한을 부여해야 합니다. 그런 다음 새 자격 증명을 BlueXP에 추가할 수 있습니다.

서비스 보안 주체를 사용하여 **Azure** 사용 권한을 부여합니다

BlueXP에는 Azure에서 작업을 수행할 수 있는 권한이 필요합니다. Microsoft Entra ID에서 서비스 주체를 생성 및 설정하고 BlueXP에 필요한 Azure 자격 증명을 획득하여 Azure 계정에 필요한 권한을 부여할 수 있습니다.

이 작업에 대해

다음 이미지는 BlueXP가 Azure에서 작업을 수행할 수 있는 권한을 얻는 방법을 보여 줍니다. 하나 이상의 Azure 구독에 연결되는 서비스 사용자 지정 개체는 Microsoft Entra ID의 BlueXP를 나타내며 필요한 권한을 허용하는 사용자 지정 역할에 할당됩니다.



단계

1. [Microsoft Entra 응용 프로그램을 만듭니다.](#)
2. [애플리케이션에 역할을 할당합니다.](#)
3. [Windows Azure 서비스 관리 API 권한을 추가합니다.](#)
4. [애플리케이션 ID 및 디렉토리 ID를 가져옵니다.](#)
5. [클라이언트 암호를 생성합니다.](#)

Microsoft Entra 응용 프로그램을 만듭니다

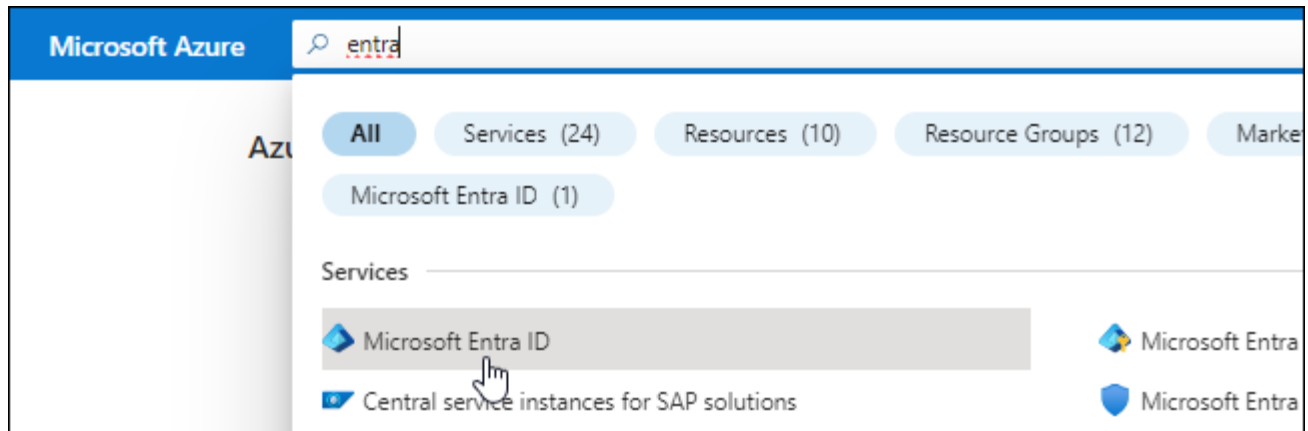
BlueXP가 역할 기반 액세스 제어에 사용할 수 있는 Microsoft Entra 애플리케이션 및 서비스 보안 주체를 생성합니다.

단계

1. Azure에서 Active Directory 응용 프로그램을 만들고 응용 프로그램을 역할에 할당할 수 있는 권한이 있는지 확인합니다.

자세한 내용은 을 참조하십시오 "[Microsoft Azure 문서: 필요한 권한](#)"

2. Azure 포털에서 * Microsoft Entra ID * 서비스를 엽니다.



3. 메뉴에서 * 앱 등록 * 을 선택합니다.
4. 새 등록 * 을 선택합니다.
5. 응용 프로그램에 대한 세부 정보를 지정합니다.
 - * 이름 *: 응용 프로그램의 이름을 입력합니다.
 - * 계정 유형 *: 계정 유형을 선택합니다(모두 BlueXP에서 사용 가능).
 - * URI 리디렉션 *: 이 필드는 비워 둘 수 있습니다.
6. Register * 를 선택합니다.

AD 응용 프로그램 및 서비스 보안 주체를 만들었습니다.

결과

AD 응용 프로그램 및 서비스 보안 주체를 만들었습니다.

애플리케이션에 역할을 할당합니다

서비스 보안 주체를 하나 이상의 Azure 구독에 바인딩하고 BlueXP에서 권한을 갖도록 사용자 지정 "BlueXP 운영자" 역할을 할당해야 합니다.

단계

1. 사용자 지정 역할 만들기:

Azure 포털, Azure PowerShell, Azure CLI 또는 REST API를 사용하여 Azure 사용자 지정 역할을 생성할 수 있습니다. 다음 단계에서는 Azure CLI를 사용하여 역할을 생성하는 방법을 보여 줍니다. 다른 방법을 사용하려면 을 참조하십시오 ["Azure 문서"](#)

- a. 의 내용을 복사합니다 ["Connector에 대한 사용자 지정 역할 권한"](#) JSON 파일에 저장합니다.
- b. 할당 가능한 범위에 Azure 구독 ID를 추가하여 JSON 파일을 수정합니다.

사용자가 Cloud Volumes ONTAP 시스템을 생성할 각 Azure 구독에 대한 ID를 추가해야 합니다.

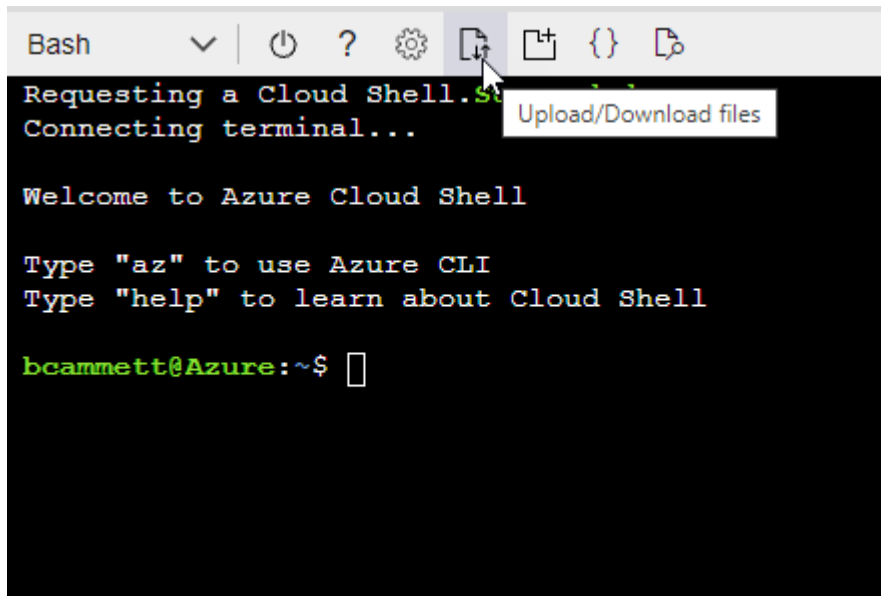
▪ 예 *

```
"AssignableScopes": [
  "/subscriptions/d333af45-0d07-4154-943d-c25fbzzzzzzz",
  "/subscriptions/54b91999-b3e6-4599-908e-416e0zzzzzzz",
  "/subscriptions/398e471c-3b42-4ae7-9b59-ce5bbzzzzzzz"
```

c. JSON 파일을 사용하여 Azure에서 사용자 지정 역할을 생성합니다.

다음 단계에서는 Azure Cloud Shell에서 Bash를 사용하여 역할을 생성하는 방법을 설명합니다.

- 시작 "Azure 클라우드 셸" Bash 환경을 선택하십시오.
- JSON 파일을 업로드합니다.



- Azure CLI를 사용하여 사용자 지정 역할을 생성합니다.

```
az role definition create --role-definition Connector_Policy.json
```

이제 Connector 가상 머신에 할당할 수 있는 BlueXP Operator라는 사용자 지정 역할이 있어야 합니다.

2. 역할에 응용 프로그램을 할당합니다.

- Azure 포털에서 * Subscriptions * 서비스를 엽니다.
- 구독을 선택합니다.
- 액세스 제어(IAM) > 추가 > 역할 할당 추가 * 를 선택합니다.
- Role * 탭에서 * BlueXP Operator * 역할을 선택하고 * Next * 를 선택합니다.
- Members* 탭에서 다음 단계를 완료합니다.
 - 사용자, 그룹 또는 서비스 보안 주체 * 를 선택한 상태로 유지합니다.
 - 구성원 선택 * 을 선택합니다.

Add role assignment ...

Got feedback?

Role **Members** Review + assign

Selected role Cloud Manager Operator 3.9.12_B

Assign access to ☒ User, group, or service principal
☐ Managed identity

Members [+ Select members](#)

- 응용 프로그램의 이름을 검색합니다.

예를 들면 다음과 같습니다.

Select members X

Select ⓘ

test-service-principal

test-service-principal

- 응용 프로그램을 선택하고 * 선택 * 을 선택합니다.
 - 다음 * 을 선택합니다.
- f. 검토 + 할당 * 을 선택합니다.

이제 서비스 보안 주체에 Connector를 배포하는 데 필요한 Azure 권한이 있습니다.

여러 Azure 구독에서 Cloud Volumes ONTAP를 배포하려면 서비스 보안 주체를 해당 구독 각각에 바인딩해야 합니다. BlueXP를 사용하면 Cloud Volumes ONTAP를 배포할 때 사용할 구독을 선택할 수 있습니다.

Windows Azure 서비스 관리 **API** 권한을 추가합니다

서비스 보안 주체는 "Windows Azure Service Management API" 권한이 있어야 합니다.

단계


1. Microsoft Entra ID * 서비스에서 * 앱 등록 * 을 선택하고 애플리케이션을 선택합니다.
2. API 권한 > 권한 추가 * 를 선택합니다.
3. Microsoft API * 에서 * Azure Service Management * 를 선택합니다.

Request API permissions













Select an API

Microsoft APIs **APIs my organization uses** My APIs

Commonly used Microsoft APIs



Microsoft Graph
Take advantage of the tremendous amount of data in Office 365, Enterprise Mobility + Security, and Windows 10. Access Azure AD, Excel, Intune, Outlook/Exchange, OneDrive, OneNote, SharePoint, Planner, and more through a single endpoint.

 <p>Azure Batch Schedule large-scale parallel and HPC applications in the cloud</p>	 <p>Azure Data Catalog Programmatic access to Data Catalog resources to register, annotate and search data assets</p>	 <p>Azure Data Explorer Perform ad-hoc queries on terabytes of data to build near real-time and complex analytics solutions</p>
 <p>Azure Data Lake Access to storage and compute for big data analytic scenarios</p>	 <p>Azure DevOps Integrate with Azure DevOps and Azure DevOps server</p>	 <p>Azure Import/Export Programmatic control of import/export jobs</p>
 <p>Azure Key Vault Manage your key vaults as well as the keys, secrets, and certificates within your Key Vaults</p>	 <p>Azure Rights Management Services Allow validated users to read and write protected content</p>	 <p>Azure Service Management Programmatic access to much of the functionality available through the Azure portal</p>
 <p>Azure Storage Secure, massively scalable object and data lake storage for unstructured and semi-structured data</p>	 <p>Customer Insights Create profile and interaction models for your products</p>	 <p>Data Export Service for Microsoft Dynamics 365 Export data from Microsoft Dynamics CRM organization to an external destination</p>

4. Access Azure Service Management as organization users * 를 선택한 다음 * Add permissions * 를 선택합니다.

Request API permissions

< All APIs



Azure Service Management

<https://management.azure.com/> [Docs](#)

What type of permissions does your application require?

Delegated permissions

Your application needs to access the API as the signed-in user.

Application permissions

Your application runs as a background service or daemon without a signed-in user.

Select permissions

[expand all](#)

Type to search

PERMISSION

ADMIN CONSENT REQUIRED



user_impersonation

Access Azure Service Management as organization users (preview) ⓘ

애플리케이션 ID 및 디렉토리 ID를 가져옵니다

Azure 계정을 BlueXP에 추가하는 경우 응용 프로그램의 응용 프로그램(클라이언트) ID와 디렉터리(테넌트) ID를 제공해야 합니다. BlueXP는 ID를 사용하여 프로그래밍 방식으로 로그인합니다.

단계

1. Microsoft Entra ID * 서비스에서 * 앱 등록 * 을 선택하고 애플리케이션을 선택합니다.
2. 응용 프로그램(클라이언트) ID * 와 * 디렉터리(테넌트) ID * 를 복사합니다.



Azure 계정을 BlueXP에 추가하는 경우 응용 프로그램의 응용 프로그램(클라이언트) ID와 디렉터리(테넌트) ID를 제공해야 합니다. BlueXP는 ID를 사용하여 프로그래밍 방식으로 로그인합니다.

클라이언트 암호를 생성합니다

클라이언트 암호를 생성한 다음 BlueXP에 해당 암호를 사용하여 Microsoft Entra ID를 통해 인증할 수 있도록 BlueXP에 해당 암호를 제공해야 합니다.

단계

1. Microsoft Entra ID * 서비스를 엽니다.
2. 앱 등록 * 을 선택하고 응용 프로그램을 선택합니다.
3. 인증서 및 비밀 > 새 클라이언트 비밀 * 을 선택합니다.
4. 비밀과 기간에 대한 설명을 제공하십시오.
5. 추가 * 를 선택합니다.
6. 클라이언트 암호 값을 복사합니다.

Client secrets

A secret string that the application uses to prove its identity when requesting a token. Also can be referred to as application password.

+ New client secret		
DESCRIPTION	EXPIRES	VALUE
test secret	8/16/2020	*sZ1jSe2By:D*-ZRoV4NLfdAcY7:+0vA

Copy to clipboard

이제 BlueXP에서 Microsoft Entra ID를 사용하여 인증하는 클라이언트 암호가 있습니다.

결과

이제 서비스 보안 주체가 설정되었으므로 응용 프로그램(클라이언트) ID, 디렉터리(테넌트) ID 및 클라이언트 암호 값을 복사해야 합니다. Azure 계정을 추가할 때 BlueXP에 이 정보를 입력해야 합니다.

BlueXP에 자격 증명을 추가합니다

필요한 권한이 있는 Azure 계정을 제공한 후 해당 계정에 대한 자격 증명을 BlueXP에 추가할 수 있습니다. 이 단계를 완료하면 다른 Azure 자격 증명을 사용하여 Cloud Volumes ONTAP를 시작할 수 있습니다.

시작하기 전에

클라우드 공급자에서 이러한 자격 증명을 만든 경우 사용할 수 있을 때까지 몇 분 정도 걸릴 수 있습니다. BlueXP에 자격 증명을 추가하기 전에 몇 분 정도 기다립니다.

시작하기 전에

BlueXP 설정을 변경하려면 먼저 커넥터를 만들어야 합니다. ["커넥터를 만드는 방법에 대해 알아봅니다"](#).

단계

1. BlueXP 콘솔의 오른쪽 상단에서 설정 아이콘을 선택하고 * 자격 증명 * 을 선택합니다.

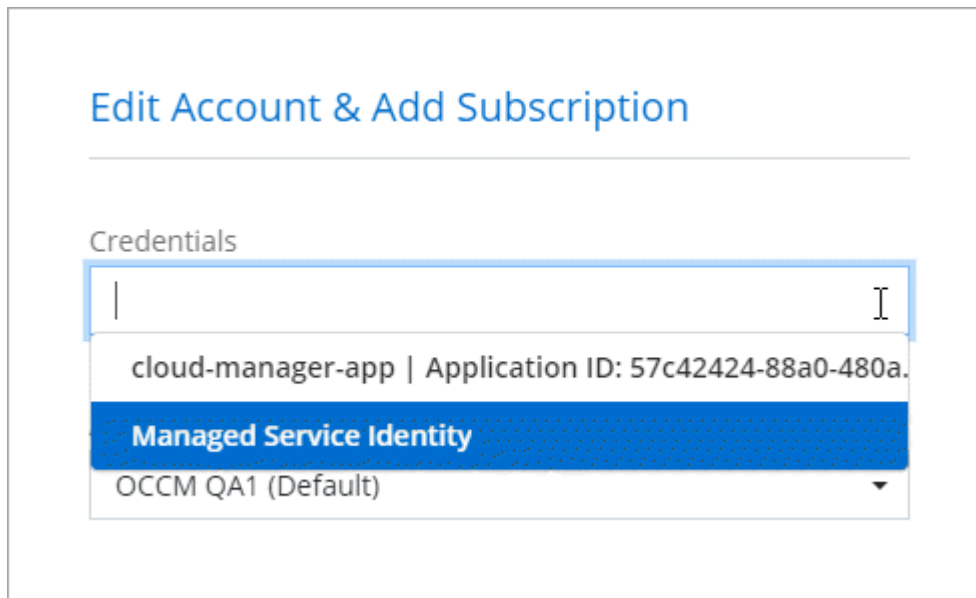


2. 자격 증명 추가 * 를 선택하고 마법사의 단계를 따릅니다.
 - a. * 자격 증명 위치 *: * Microsoft Azure > 커넥터 * 를 선택합니다.
 - b. * 자격 증명 정의 *: 필요한 권한을 부여하는 Microsoft Entra 서비스 보안 주체에 대한 정보를 입력합니다.
 - 애플리케이션(클라이언트) ID입니다

- 디렉토리(테넌트) ID입니다
 - 클라이언트 암호
- c. * Marketplace 구독 *: 지금 가입하거나 기존 구독을 선택하여 마켓플레이스 구독을 이러한 자격 증명과 연결합니다.
- d. * 검토 *: 새 자격 증명에 대한 세부 정보를 확인하고 * 추가 * 를 선택합니다.

결과

이제 세부 정보 및 자격 증명 페이지에서 다른 자격 증명 집합으로 전환할 수 있습니다 ["새 작업 환경을 만들 때"](#)



기존 자격 증명을 관리합니다

Marketplace 구독을 연결하고 자격 증명을 편집하고 삭제하여 BlueXP에 이미 추가한 Azure 자격 증명을 관리합니다.

Azure Marketplace 구독을 자격 증명에 연결합니다

Azure 자격 증명을 BlueXP에 추가한 후 Azure Marketplace 구독을 해당 자격 증명에 연결할 수 있습니다. 이 구독을 통해 선불 종량제 Cloud Volumes ONTAP 시스템을 생성하고 다른 BlueXP 서비스를 사용할 수 있습니다.

BlueXP에 자격 증명을 추가한 후 Azure Marketplace 구독을 연결할 수 있는 두 가지 시나리오가 있습니다.

- 처음에 BlueXP에 자격 증명을 추가할 때 구독을 연결하지 않았습니다.
- Azure 자격 증명과 연결된 Azure Marketplace 구독을 변경하려고 합니다.

현재 마켓플레이스 구독을 새 구독으로 교체하면 기존 Cloud Volumes ONTAP 작업 환경과 모든 새로운 작업 환경에 대한 마켓플레이스 구독이 변경됩니다.

시작하기 전에

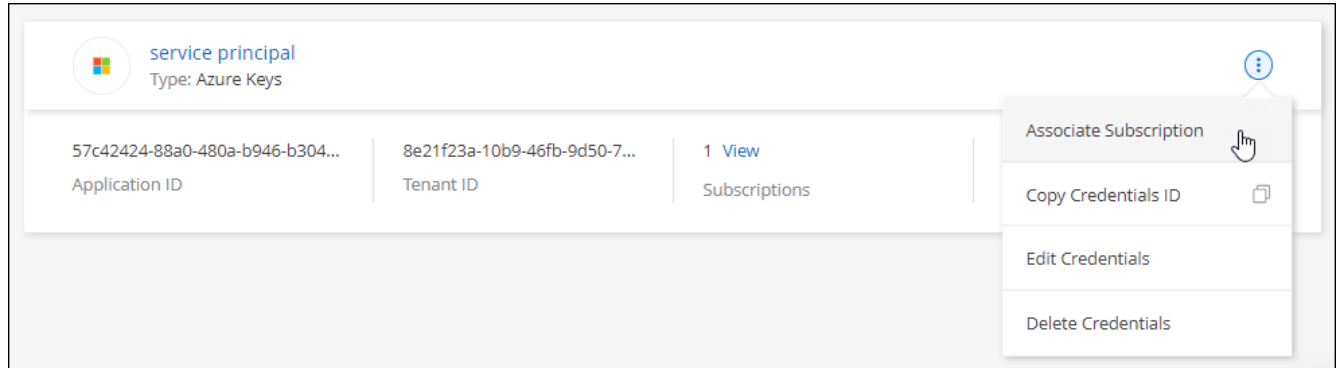
BlueXP 설정을 변경하려면 먼저 커넥터를 만들어야 합니다. ["자세히 알아보기"](#).

단계

1. BlueXP 콘솔의 오른쪽 상단에서 설정 아이콘을 선택하고 * 자격 증명 * 을 선택합니다.

2. 자격 증명 집합에 대한 작업 메뉴를 선택한 다음 * 가입 연결 * 을 선택합니다.

Connector와 연결된 자격 증명을 선택해야 합니다. BlueXP와 연결된 자격 증명과 마켓플레이스 구독을 연결할 수 없습니다.



3. 자격 증명을 기존 구독과 연결하려면 드롭다운 목록에서 구독을 선택하고 * Associate * 를 선택합니다.

4. 자격 증명을 새 구독과 연결하려면 * 구독 추가 > 계속 * 을 선택하고 Azure 마켓플레이스의 단계를 따릅니다.

- 메시지가 표시되면 Azure 계정에 로그인합니다.
- 가입 * 을 선택합니다.
- 양식을 작성하고 * Subscribe * 를 선택합니다.
- 가입 프로세스가 완료되면 * 지금 계정 구성 * 을 선택합니다.

BlueXP 웹 사이트로 이동합니다.

e. [구독 할당 *] 페이지에서:

- 이 구독을 연결할 BlueXP 계정을 선택합니다.
- 기존 구독 바꾸기 * 필드에서 하나의 계정에 대한 기존 구독을 이 새 구독으로 자동 대체할지 여부를 선택합니다.

BlueXP는 계정의 모든 자격 증명에 대한 기존 구독을 이 새 구독으로 대체합니다. 자격 증명 집합이 구독과 연결되지 않은 경우 이 새 구독은 해당 자격 증명과 연결되지 않습니다.

다른 모든 계정의 경우 이 단계를 반복하여 구독을 수동으로 연결해야 합니다.

- 저장 * 을 선택합니다.

다음 비디오에서는 Azure 마켓플레이스에서 구독하는 단계를 보여 줍니다.

[Azure 마켓플레이스에서 BlueXP를 구독하십시오](#)

자격 증명을 편집합니다

Azure 서비스 자격 증명에 대한 세부 정보를 수정하여 BlueXP에서 Azure 자격 증명을 편집합니다. 예를 들어, 서비스 보안 주체 응용 프로그램에 대해 새 암호가 만들어진 경우 클라이언트 암호를 업데이트해야 할 수 있습니다.

단계

1. BlueXP 콘솔의 오른쪽 상단에서 설정 아이콘을 선택하고 * 자격 증명 * 을 선택합니다.
2. 계정 자격 증명 * 페이지에서 자격 증명 세트의 작업 메뉴를 선택한 다음 * 자격 증명 편집 * 을 선택합니다.
3. 필요한 내용을 변경한 다음 * Apply * 를 선택합니다.

자격 증명을 삭제합니다

더 이상 자격 증명 세트가 필요하지 않으면 BlueXP에서 삭제할 수 있습니다. 작업 환경과 연결되지 않은 자격 증명만 삭제할 수 있습니다.

단계

1. BlueXP 콘솔의 오른쪽 상단에서 설정 아이콘을 선택하고 * 자격 증명 * 을 선택합니다.
2. 계정 자격 증명 * 페이지에서 자격 증명 세트의 작업 메뉴를 선택한 다음 * 자격 증명 삭제 * 를 선택합니다.
3. 삭제하려면 * 삭제 * 를 선택합니다.

Google 클라우드

Google Cloud 프로젝트 및 권한에 대해 자세히 알아보십시오

BlueXP가 Google Cloud 자격 증명을 사용하여 대신 작업을 수행하는 방법과 해당 자격 증명이 마켓플레이스 구독과 어떻게 연관되는지 알아보십시오. 이러한 세부 정보를 이해하면 하나 이상의 Google Cloud 프로젝트에 대한 자격 증명을 관리하는 데 도움이 될 수 있습니다. 예를 들어 Connector VM과 연결된 서비스 계정에 대해 자세히 알아볼 수 있습니다.

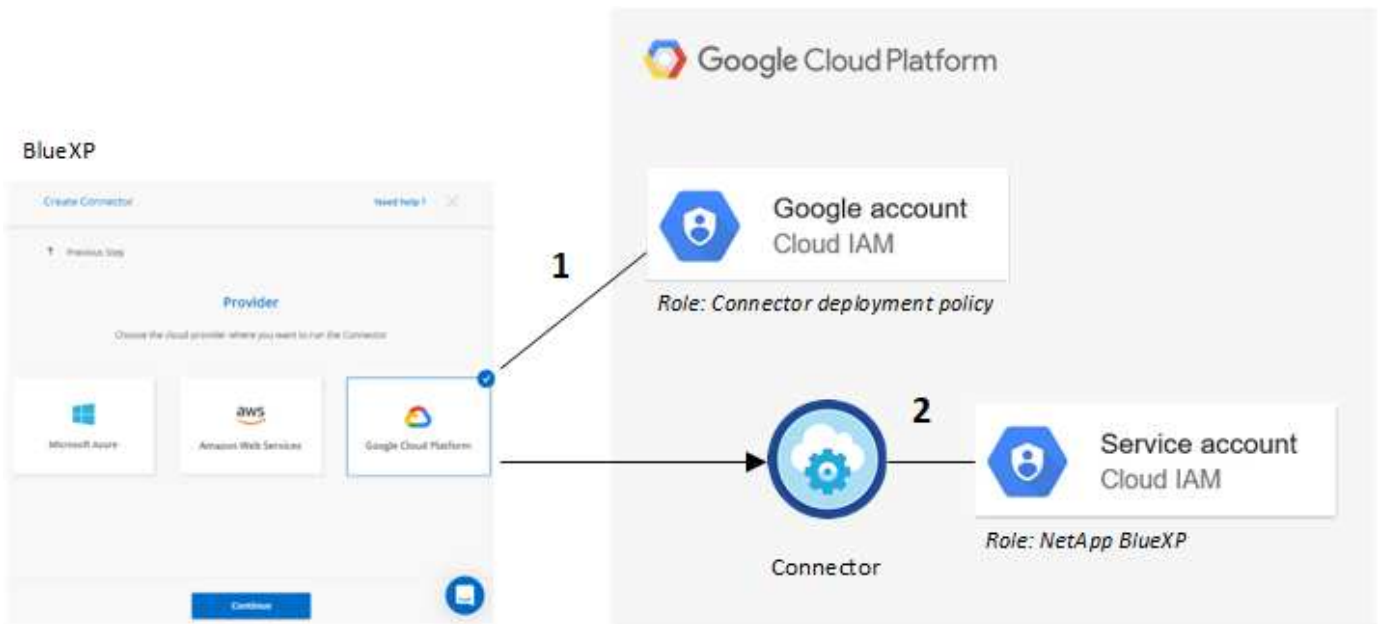
BlueXP의 프로젝트 및 권한

BlueXP를 사용하여 Google Cloud 프로젝트의 리소스를 관리하려면 먼저 Connector를 배포해야 합니다. Connector는 사내 또는 다른 클라우드 공급자에서 실행할 수 없습니다.

BlueXP에서 직접 커넥터를 배포하기 전에 두 가지 권한 세트가 있어야 합니다.

1. BlueXP에서 Connector VM 인스턴스를 시작할 수 있는 권한이 있는 Google 계정을 사용하여 Connector를 배포해야 합니다.
2. 커넥터를 배포할 때 를 선택하라는 메시지가 나타납니다 **"서비스 계정"** VM 인스턴스의 경우. BlueXP는 서비스 계정에서 Cloud Volumes ONTAP 시스템을 생성 및 관리하고 BlueXP 백업 및 복구를 사용하여 백업을 관리하는 권한을 얻습니다. 권한은 서비스 계정에 사용자 지정 역할을 첨부하여 제공됩니다.

다음 이미지는 위의 숫자 1과 2에 설명된 사용 권한 요구 사항을 보여 줍니다.



사용 권한을 설정하는 방법은 다음 페이지를 참조하십시오.

- ["표준 모드에 대한 Google Cloud 권한을 설정합니다"](#)
- ["제한된 모드에 대한 권한을 설정합니다"](#)
- ["비공개 모드에 대한 권한을 설정합니다"](#)

자격 증명 및 마켓플레이스 구독

Google Cloud에 Connector를 구축하면 BlueXP는 Connector가 상주하는 프로젝트에서 Google Cloud 서비스 계정에 대한 기본 자격 증명 세트를 생성합니다. Cloud Volumes ONTAP를 시간당 요금(PAYGO)으로 지불하고 다른 BlueXP 서비스를 사용할 수 있도록 자격 증명이 Google Cloud Marketplace 구독에 연결되어 있어야 합니다.

["Google Cloud Marketplace 구독을 연결하는 방법에 대해 알아보십시오"](#).

Google Cloud 자격 증명 및 마켓플레이스 구독에 대해서는 다음을 참고하십시오.

- 하나의 Google Cloud 자격 증명 세트만 Connector에 연결할 수 있습니다
- 하나의 Google Cloud Marketplace 구독만 자격 증명에 연결할 수 있습니다
- 기존 마켓플레이스 구독을 새 구독으로 바꿀 수 있습니다

Cloud Volumes ONTAP 프로젝트

Cloud Volumes ONTAP는 Connector와 같은 프로젝트나 다른 프로젝트에 상주할 수 있습니다. 다른 프로젝트에 Cloud Volumes ONTAP를 배포하려면 먼저 해당 프로젝트에 Connector 서비스 계정 및 역할을 추가해야 합니다.

- ["서비스 계정 설정 방법에 대해 알아보십시오"](#)
- ["Google Cloud에서 Cloud Volumes ONTAP를 배포하고 프로젝트를 선택하는 방법에 대해 알아보십시오"](#)

BlueXP용 Google Cloud 자격 증명 및 구독을 관리합니다

마켓플레이스 가입을 연결하고 가입 프로세스를 해결하여 Connector VM 인스턴스와 연결된

Google Cloud 자격 증명을 관리할 수 있습니다. 이러한 두 가지 작업을 통해 마켓플레이스 가입을 통해 BlueXP 서비스 비용을 지불할 수 있습니다.

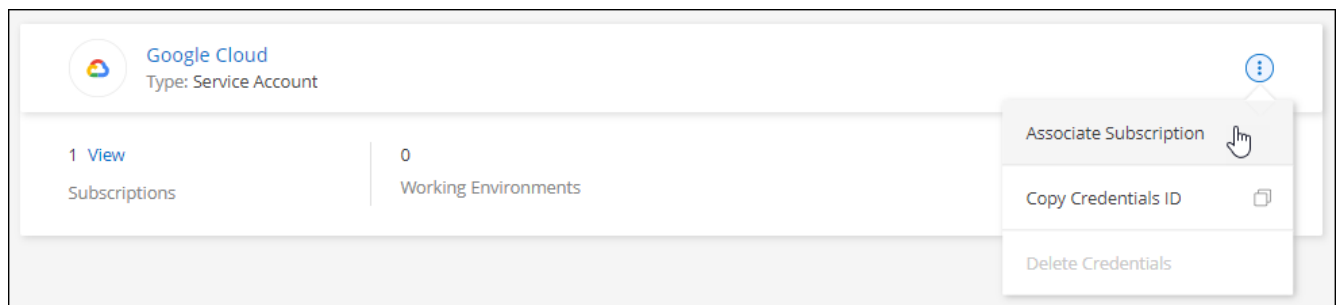
마켓플레이스 구독을 **Google Cloud** 자격 증명과 연결합니다

Google Cloud에서 Connector를 배포하면 BlueXP는 Connector VM 인스턴스와 연결된 기본 자격 증명 집합을 만듭니다. 언제든지 이러한 자격 증명과 연결된 Google Cloud Marketplace 구독을 변경할 수 있습니다. 이 구독을 통해 선불 종량제 Cloud Volumes ONTAP 시스템을 생성하고 다른 BlueXP 서비스를 사용할 수 있습니다.

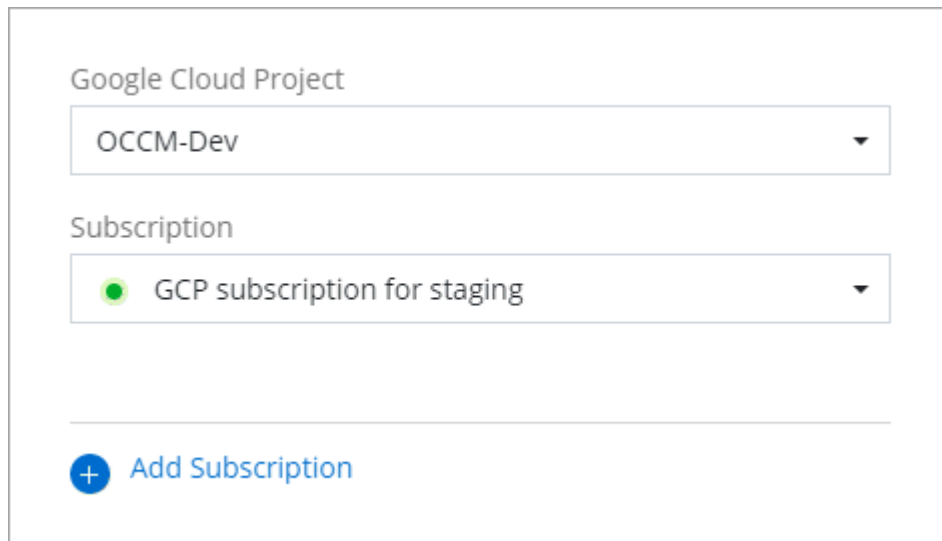
현재 마켓플레이스 구독을 새 구독으로 교체하면 기존 Cloud Volumes ONTAP 작업 환경과 모든 새로운 작업 환경에 대한 마켓플레이스 구독이 변경됩니다.

단계

1. BlueXP 콘솔의 오른쪽 상단에서 설정 아이콘을 선택하고 * 자격 증명 * 을 선택합니다.
2. 자격 증명 집합에 대한 작업 메뉴를 선택한 다음 * 가입 연결 * 을 선택합니다.



3. 자격 증명을 기존 구독과 연결하려면 아래 목록에서 Google Cloud 프로젝트 및 구독을 선택한 다음 * Associate * 를 선택합니다.



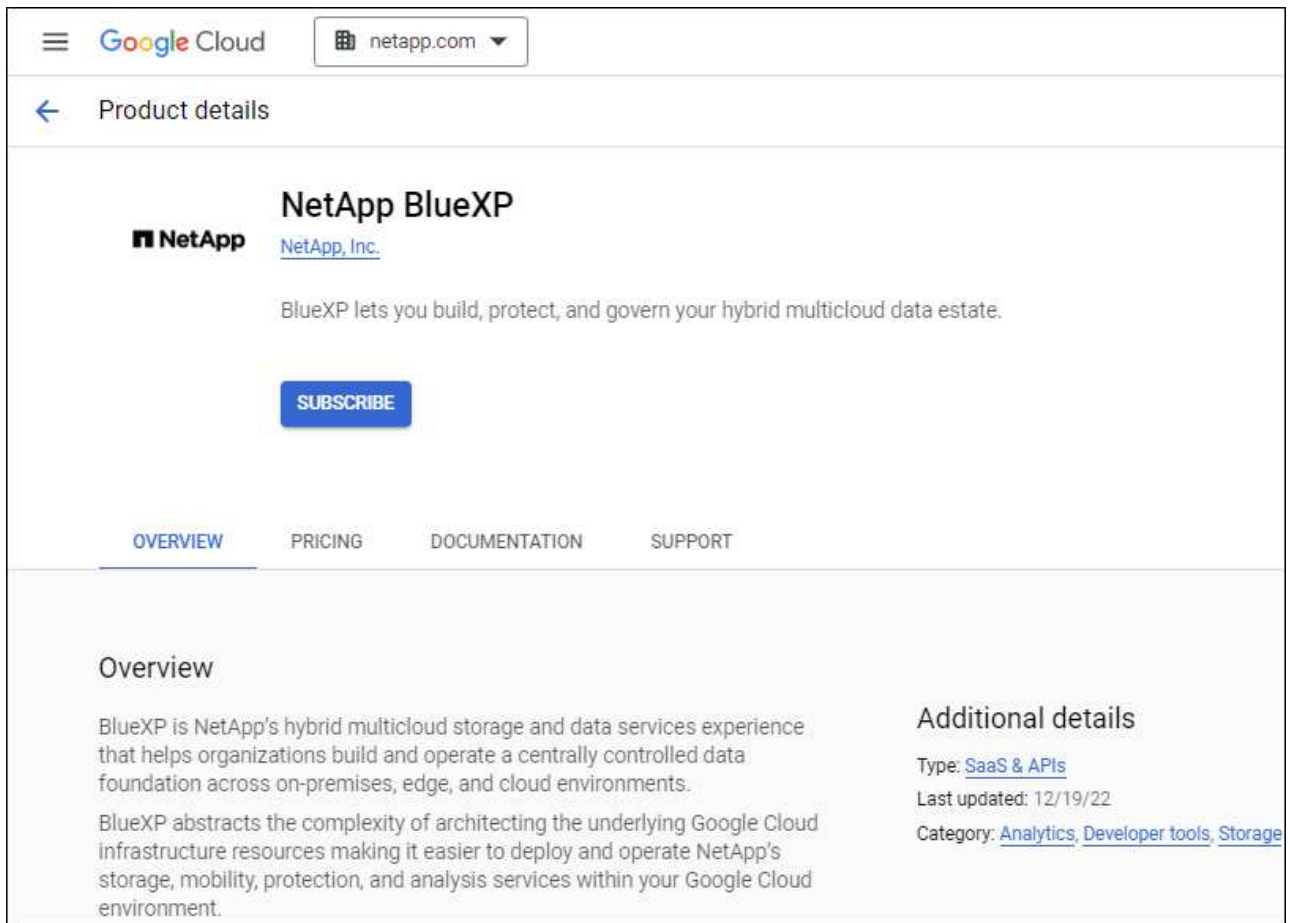
4. 아직 구독이 없는 경우 * 구독 추가 > 계속 * 을 선택하고 Google Cloud Marketplace의 단계를 따릅니다.



다음 단계를 완료하기 전에 Google Cloud 계정과 BlueXP 로그인에 Billing Admin 권한이 모두 있는지 확인하십시오.

- a. 로 리디렉션된 후 "[Google Cloud 마켓플레이스의 NetApp BlueXP 페이지](#)"상단 탐색 메뉴에서 올바른

프로젝트가 선택되어 있는지 확인합니다.

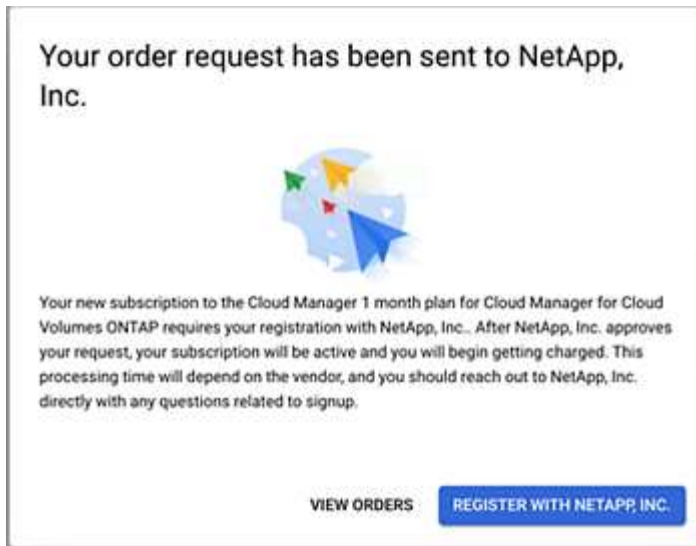


- b. 가입 * 을 선택합니다.
- c. 적절한 청구 계정을 선택하고 이용 약관에 동의합니다.
- d. 가입 * 을 선택합니다.

이 단계에서는 전송 요청을 NetApp에 전송합니다.

- e. 팝업 대화 상자에서 * Register with NetApp, Inc. * 를 선택합니다

Google Cloud 구독을 BlueXP 계정에 연결하려면 이 단계를 완료해야 합니다. 이 페이지에서 리디렉션된 다음 BlueXP에 로그인할 때까지 가입 연결 프로세스가 완료되지 않습니다.



f. 구독 할당 * 페이지의 단계를 완료합니다.



조직의 누군가가 청구 계정에서 NetApp BlueXP 구독을 이미 구독한 경우 으로 리디렉션됩니다 "[BlueXP 웹 사이트의 Cloud Volumes ONTAP 페이지](#)" 대신 예기치 않은 상황인 경우 NetApp 세일즈 팀에 문의하십시오. Google은 Google 청구 계정당 하나의 가입만 활성화합니다.

- 이 구독을 연결할 BlueXP 계정을 선택합니다.
- 기존 구독 바꾸기 * 필드에서 하나의 계정에 대한 기존 구독을 이 새 구독으로 자동 대체할지 여부를 선택합니다.

BlueXP는 계정의 모든 자격 증명에 대한 기존 구독을 이 새 구독으로 대체합니다. 자격 증명 집합이 구독과 연결되지 않은 경우 이 새 구독은 해당 자격 증명과 연결되지 않습니다.

다른 모든 계정의 경우 이 단계를 반복하여 구독을 수동으로 연결해야 합니다.

- 저장 * 을 선택합니다.

다음 비디오에서는 Google Cloud Marketplace를 구독하는 단계를 보여줍니다.


[Google Cloud 마켓플레이스에서 BlueXP를 구독하십시오](#)


- a. 이 프로세스가 완료되면 BlueXP의 자격 증명 페이지로 돌아가서 이 새 구독을 선택합니다.

Google Cloud Project

OCCM-Dev

Subscription

 GCP subscription for staging



마켓플레이스 가입 프로세스 문제 해결

때로는 Google Cloud Marketplace를 통해 BlueXP를 구독하는 경우 권한이 잘못되거나 BlueXP 웹 사이트로 리디렉션되는 것을 실제로 수행하지 않기 때문에 조각화될 수 있습니다. 이 경우 다음 단계를 사용하여 구독 프로세스를 완료합니다.

단계

- 로 이동합니다 "[Google Cloud 마켓플레이스의 NetApp BlueXP 페이지](#)" 주문 상태를 확인합니다. 페이지에 * 공급자 * 에서 관리 * 가 표시되면 아래로 스크롤하여 * 주문 관리 * 를 선택합니다.

Pricing




The product was purchased on 12/9/20.

[MANAGE ORDERS](#)

- 주문에 녹색 확인 표시가 있고 예상치 못한 경우 동일한 대금 청구 계정을 사용하는 조직의 다른 사용자가 이미 구독 중인 것일 수 있습니다. 예기치 않은 요청이거나 이 구독에 대한 자세한 정보가 필요한 경우 NetApp 세일즈 팀에 문의하십시오.

Filter Enter property name or value										
Status	Order number	Plan	Discount	Start date ↓	Plan duration	End date	Payment Schedule	Auto-renew	Next plan	
	2eebbc...	Cloud Manager	-	10/21/21	1 month	-	Postpay	N/A	N/A	⋮

- 주문에 시계 및 * 보류 * 상태가 표시되면 마켓플레이스 페이지로 돌아가서 * 공급자 관리 * 를 선택하여 위에 설명된 프로세스를 완료합니다.

Filter Enter property name or value										
Status	Order number	Plan	Discount	Start date ↓	Plan duration	End date	Payment Schedule	Auto-renew	Next plan	
	d56c66...	Cloud Manager	-	Pending	1 month	Pending	Postpay	N/A	N/A	⋮

BlueXP 계정과 연결된 NSS 자격 증명을 관리합니다

NetApp Support 사이트 계정을 BlueXP 계정과 연결하여 Cloud Volumes ONTAP의 주요 워크플로를 활성화합니다. 이러한 NSS 자격 증명은 전체 BlueXP 계정과 연결되어 있습니다.



또한 BlueXP에서는 BlueXP 사용자당 하나의 NSS 계정을 연결할 수 있습니다. "[사용자 수준 자격 증명을 관리하는 방법에 대해 알아봅니다](#)".

개요

BlueXP에서 다음 작업을 사용하려면 특정 BlueXP 계정 ID와 NetApp Support 사이트 자격 증명을 연결해야 합니다.

- BYOL(Bring Your Own License) 방식으로 Cloud Volumes ONTAP 구축

BlueXP에서 사용권 키를 업로드하고 구입한 용어에 대한 구독을 활성화하려면 NSS 계정을 제공해야 합니다. 여기에는 기간 갱신을 위한 자동 업데이트가 포함됩니다.

- 선불 종량제 Cloud Volumes ONTAP 시스템을 등록합니다

NSS 계정을 제공하면 시스템에 대한 지원을 활성화하고 NetApp 기술 지원 리소스에 액세스할 수 있습니다.

- Cloud Volumes ONTAP 소프트웨어를 최신 릴리즈로 업그레이드하는 중입니다

이러한 자격 증명은 특정 BlueXP 계정 ID와 연결됩니다. BlueXP 계정에 속한 사용자는 * 지원 > NSS 관리 * 에서 이러한 자격 증명에 액세스할 수 있습니다.

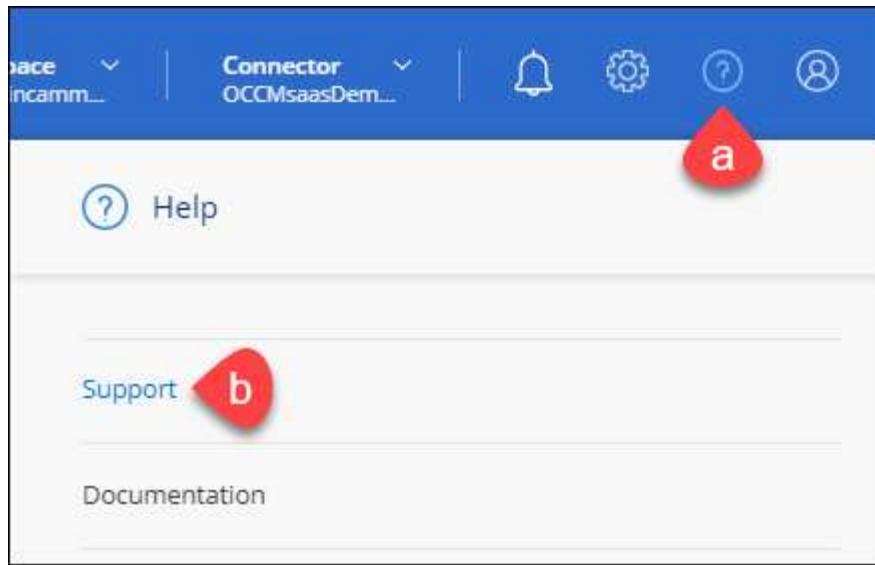
NSS 계정을 추가합니다

지원 대시보드를 사용하면 BlueXP 계정 수준에서 BlueXP에 사용할 NetApp Support 사이트 계정을 추가하고 관리할 수 있습니다.

- 고객 수준 계정이 있는 경우 하나 이상의 NSS 계정을 추가할 수 있습니다.
- 파트너 또는 리셀러 계정이 있는 경우 NSS 계정을 하나 이상 추가할 수 있지만 고객 수준 계정과 함께 추가할 수는 없습니다.

단계

1. BlueXP 콘솔의 오른쪽 상단에서 도움말 아이콘을 선택하고 * 지원 * 을 선택합니다.



2. NSS 관리 > NSS 계정 추가 * 를 선택합니다.
3. 메시지가 표시되면 * 계속 * 을 선택하여 Microsoft 로그인 페이지로 리디렉션합니다.

NetApp는 지원 및 라이선스와 관련된 인증 서비스의 ID 공급자로 Microsoft Entra ID를 사용합니다.

4. 로그인 페이지에서 인증 프로세스를 수행할 수 있도록 NetApp Support 사이트의 등록 이메일 주소와 암호를 제공합니다.

이러한 작업을 통해 BlueXP는 NSS 계정을 사용하여 라이선스 다운로드, 소프트웨어 업그레이드 확인 및 향후 지원 등록과 같은 작업을 수행할 수 있습니다.

다음 사항에 유의하십시오.

- NSS 계정은 고객 수준 계정이어야 합니다(게스트 또는 임시 계정이 아님). 여러 개의 고객 수준 NSS 계정을 가질 수 있습니다.
- NSS 계정은 파트너 수준 계정인 경우 하나만 있을 수 있습니다. 고객 수준 NSS 계정을 추가하려고 하면 파트너 수준 계정이 있으면 다음 오류 메시지가 나타납니다.

"NSS 고객 유형은 이미 다른 유형의 NSS 사용자가 있으므로 이 계정에 허용되지 않습니다."

기존 고객 수준 NSS 계정이 있는 경우에도 마찬가지이며 파트너 수준 계정을 추가하려고 합니다.

- 로그인에 성공하면 NetApp은 NSS 사용자 이름을 저장합니다.

이 ID는 이메일에 매핑되는 시스템 생성 ID입니다. NSS 관리 * 페이지의 에서 이메일을 표시할 수 있습니다 ... 메뉴.

- 로그인 자격 증명 토큰을 새로 고쳐야 하는 경우 에 * 자격 증명 업데이트 * 옵션이 있습니다 ... 메뉴.

이 옵션을 사용하면 다시 로그인하라는 메시지가 표시됩니다. 이러한 계정의 토큰은 90일 후에 만료됩니다. 이를 알리는 알림이 게시됩니다.

다음 단계

이제 사용자는 새 Cloud Volumes ONTAP 시스템을 생성할 때와 기존 Cloud Volumes ONTAP 시스템을 등록할 때

계정을 선택할 수 있습니다.

- "AWS에서 Cloud Volumes ONTAP 실행"
- "Azure에서 Cloud Volumes ONTAP 실행"
- "Google Cloud에서 Cloud Volumes ONTAP 실행"
- "선불 종량제 시스템을 등록하는 중입니다"

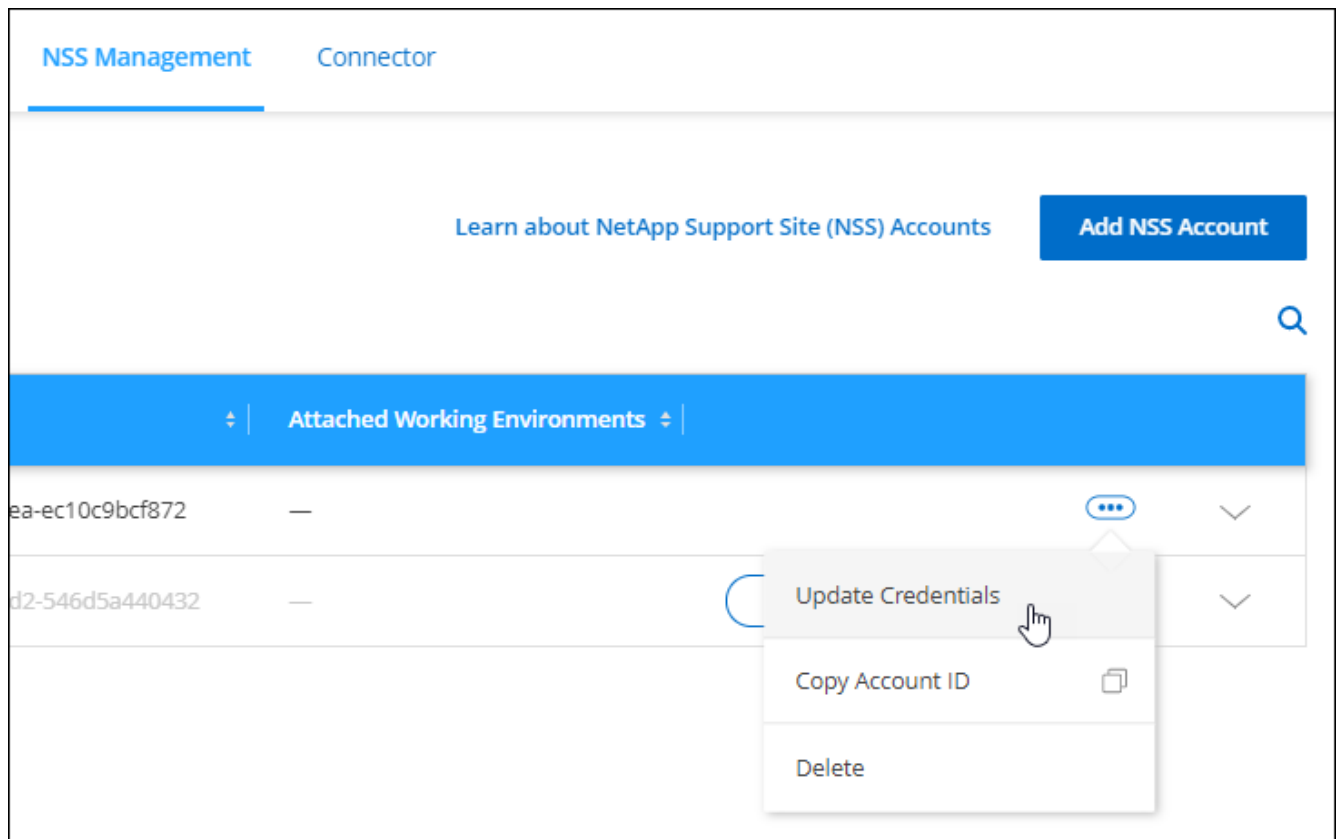
NSS 자격 증명을 업데이트합니다

다음 중 하나가 발생할 경우 BlueXP의 NSS 계정에 대한 자격 증명을 업데이트해야 합니다.

- 계정의 자격 증명을 변경합니다
- 계정에 연결된 새로 고침 토큰이 3개월 후에 만료됩니다

단계

1. BlueXP 콘솔의 오른쪽 상단에서 도움말 아이콘을 선택하고 * 지원 * 을 선택합니다.
2. NSS 관리 * 를 선택합니다.
3. 업데이트할 NSS 계정의 경우 를 선택합니다 ... 그런 다음 * 자격 증명 업데이트 * 를 선택합니다.



4. 메시지가 표시되면 * 계속 * 을 선택하여 Microsoft 로그인 페이지로 리디렉션합니다.

NetApp는 지원 및 라이선스와 관련된 인증 서비스의 ID 공급자로 Microsoft Entra ID를 사용합니다.

5. 로그인 페이지에서 인증 프로세스를 수행할 수 있도록 NetApp Support 사이트의 등록 이메일 주소와 암호를

제공합니다.

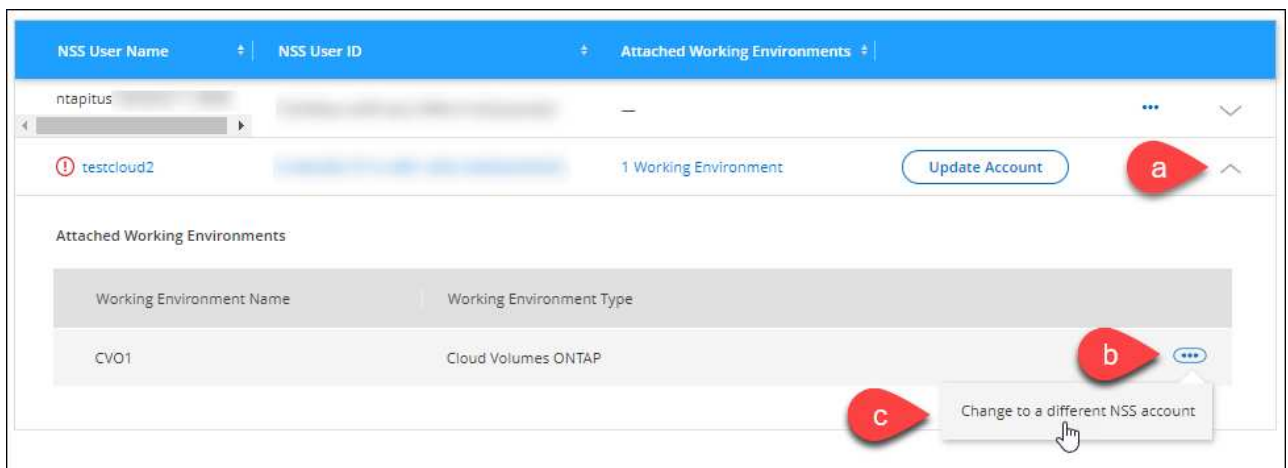
작업 환경을 다른 **NSS** 계정에 연결합니다

조직에 여러 NetApp Support 사이트 계정이 있는 경우 Cloud Volumes ONTAP 시스템과 연결된 계정을 변경할 수 있습니다.

이 기능은 ID 관리를 위해 NetApp에서 채택한 Microsoft Entra ID를 사용하도록 구성된 NSS 계정에서만 지원됩니다. 이 기능을 사용하려면 * NSS 계정 추가 * 또는 * 계정 업데이트 * 를 선택해야 합니다.

단계

1. BlueXP 콘솔의 오른쪽 상단에서 도움말 아이콘을 선택하고 * 지원 * 을 선택합니다.
2. NSS 관리 * 를 선택합니다.
3. NSS 계정을 변경하려면 다음 단계를 수행하십시오.
 - a. 작업 환경이 현재 연결되어 있는 NetApp Support 사이트 계정의 행을 확장합니다.
 - b. 연결을 변경할 작업 환경의 경우 을 선택합니다 ...
 - c. 다른 NSS 계정으로 변경 * 을 선택합니다.



- d. 계정을 선택한 다음 * 저장 * 을 선택합니다.

NSS 계정의 이메일 주소를 표시합니다

이제 NetApp Support 사이트 계정에서 인증 서비스에 Microsoft Entra ID를 사용했으므로 BlueXP에 표시되는 NSS 사용자 이름은 일반적으로 Microsoft Entra에서 생성되는 식별자입니다. 따라서 해당 계정과 연결된 전자 메일 주소를 즉시 알지 못할 수 있습니다. 그러나 BlueXP에는 관련 이메일 주소를 표시하는 옵션이 있습니다.

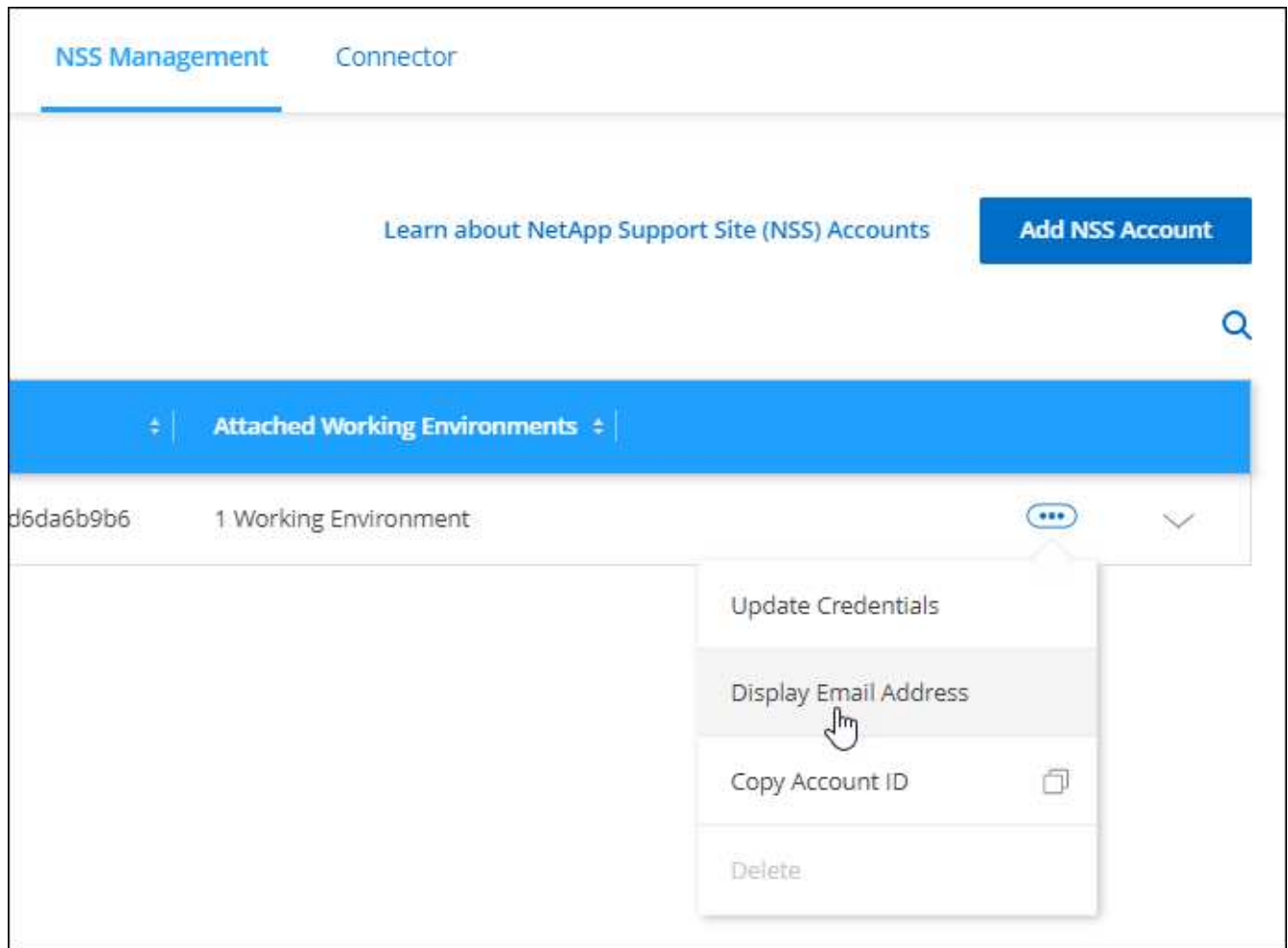


NSS 관리 페이지로 이동하면 BlueXP에서 표의 각 계정에 대한 토큰을 생성합니다. 이 토큰에는 연결된 이메일 주소에 대한 정보가 포함됩니다. 그런 다음 페이지를 나갈 때 토큰이 제거됩니다. 정보는 캐싱되지 않으며 개인 정보를 보호하는 데 도움이 됩니다.

단계

1. BlueXP 콘솔의 오른쪽 상단에서 도움말 아이콘을 선택하고 * 지원 * 을 선택합니다.
2. NSS 관리 * 를 선택합니다.

3. 업데이트할 NSS 계정의 경우 를 선택합니다 ... 그런 다음 * 이메일 주소 표시 * 를 선택합니다.



결과

BlueXP는 NetApp Support 사이트 사용자 이름과 관련 이메일 주소를 표시합니다. 복사 버튼을 사용하여 이메일 주소를 복사할 수 있습니다.

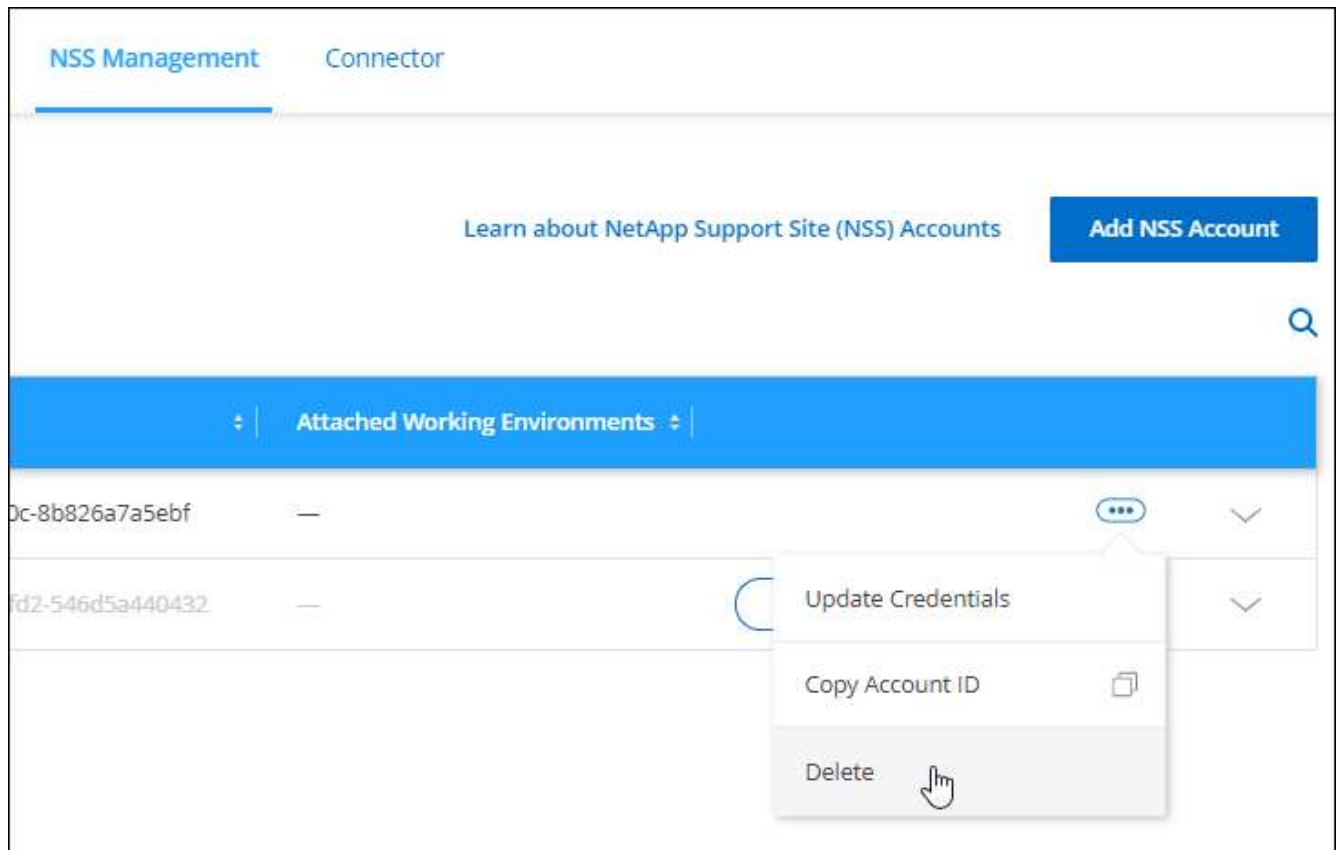
NSS 계정을 제거합니다

BlueXP에서 더 이상 사용하지 않을 NSS 계정을 삭제합니다.

현재 Cloud Volumes ONTAP 작업 환경과 연결된 계정은 삭제할 수 없습니다. 먼저 해야 할 일 [이러한 작업 환경을 다른 NSS 계정에 연결합니다](#).

단계

1. BlueXP 콘솔의 오른쪽 상단에서 도움말 아이콘을 선택하고 * 지원 * 을 선택합니다.
2. NSS 관리 * 를 선택합니다.
3. 삭제할 NSS 계정의 경우 을 선택합니다 ... 그런 다음 * 삭제 * 를 선택합니다.



4. 삭제하려면 * 삭제 * 를 선택합니다.

BlueXP 로그인과 관련된 자격 증명을 관리합니다

BlueXP에서 수행한 작업에 따라 ONTAP 자격 증명 및 NSS(NetApp Support 사이트) 자격 증명을 BlueXP 사용자 로그인에 연결할 수 있습니다. 연결한 후 BlueXP에서 이러한 자격 증명을 보고 관리할 수 있습니다. 예를 들어 이러한 자격 증명의 암호를 변경하는 경우 BlueXP에서 암호를 업데이트해야 합니다.

ONTAP 자격 증명

커넥터를 사용하지 않고 사내 ONTAP 클러스터를 직접 검색할 경우 클러스터에 대한 ONTAP 자격 증명을 입력하라는 메시지가 표시됩니다. 이러한 자격 증명은 사용자 수준에서 관리되므로 로그인하는 다른 사용자가 볼 수 없습니다.

NSS 자격 증명

BlueXP 로그인과 관련된 NSS 자격 증명을 통해 등록, 케이스 관리 및 Digital Advisor에 액세스할 수 있습니다.

- 지원 > 리소스 * 에 액세스하여 지원을 등록하면 NSS 자격 증명을 BlueXP 로그인에 연결하라는 메시지가 표시됩니다.

그러면 지원을 위해 BlueXP 계정이 등록되고 지원 권한이 활성화됩니다. BlueXP 계정에 있는 한 명의 사용자만 NetApp Support 사이트 계정을 BlueXP 로그인에 연결하여 지원을 등록하고 지원 권한을 활성화해야 합니다. 이 작업이 완료되면 * 리소스 * 페이지에 계정이 지원을 위해 등록되었다는 내용이 표시됩니다.

["지원 등록 방법을 알아보십시오"](#)

- 지원 > 케이스 관리 * 에 액세스하면 NSS 자격 증명을 입력하라는 메시지가 표시됩니다(아직 입력하지 않은 경우). 이 페이지에서는 NSS 계정 및 회사와 관련된 지원 사례를 만들고 관리할 수 있습니다.
- BlueXP의 Digital Advisor에 액세스하면 NSS 자격 증명을 입력하여 Digital Advisor에 로그인하라는 메시지가 표시됩니다.

BlueXP 로그인과 관련된 NSS 계정은 다음과 같습니다.

- 계정은 사용자 수준에서 관리되므로 로그인한 다른 사용자가 볼 수 없습니다.
- 사용자당 Digital Advisor 및 지원 케이스 관리와 연결된 NSS 계정은 하나만 있을 수 있습니다.
- NetApp Support 사이트 계정을 Cloud Volumes ONTAP 작업 환경과 연결하려는 경우, BlueXP 계정에 추가한 NSS 계정에서만 사용자가 구성원으로 속해 있는 계정을 선택할 수 있습니다.

NSS 계정 수준 자격 증명은 BlueXP 로그인과 연결된 NSS 계정과 다릅니다. NSS 계정 수준 자격 증명을 사용하면 BYOL(Bring Your Own License), PAYGO 시스템 등록 및 Cloud Volumes ONTAP 소프트웨어 업그레이드 시 Cloud Volumes ONTAP를 구축할 수 있습니다.

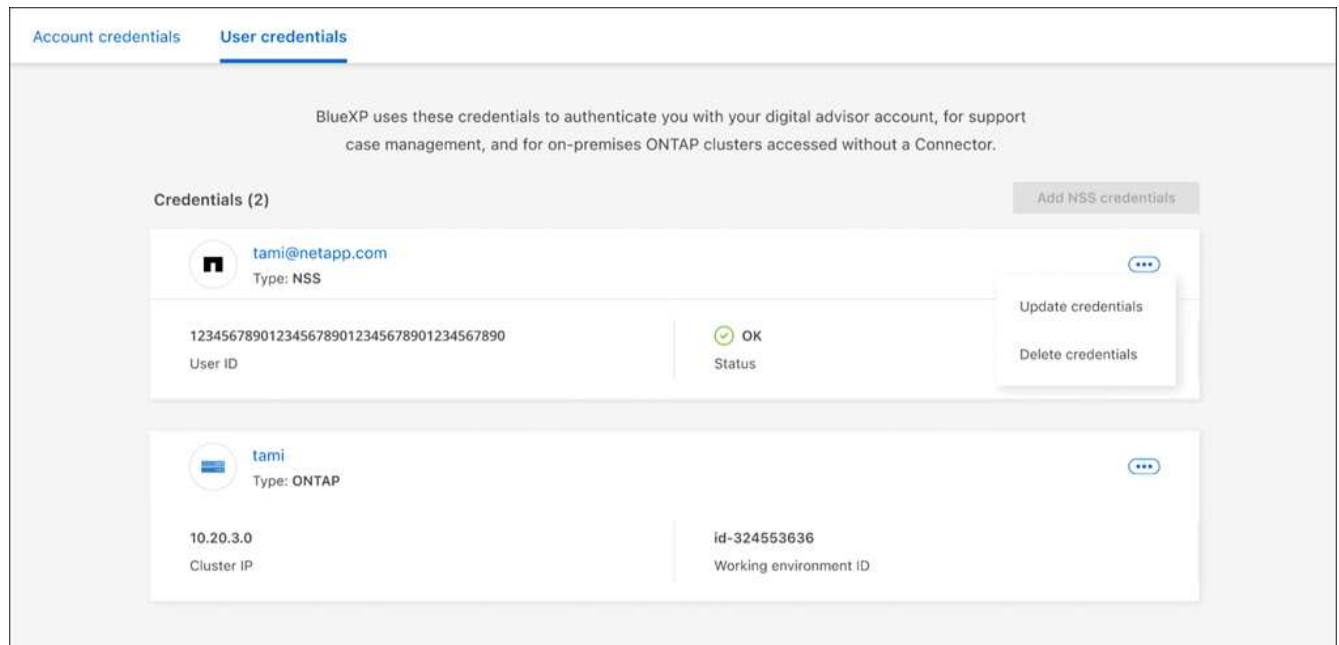
["BlueXP 계정에서 NSS 자격 증명을 사용하는 방법에 대해 자세히 알아보십시오".](#)

사용자 자격 증명을 관리합니다

사용자 이름과 암호를 업데이트하거나 자격 증명을 삭제하여 사용자 자격 증명을 관리합니다.

단계

1. BlueXP 콘솔의 오른쪽 상단에서 설정 아이콘을 선택하고 * 자격 증명 * 을 선택합니다.
2. 사용자 자격 증명 * 을 선택합니다.
3. 아직 사용자 자격 증명이 없는 경우 * NSS 자격 증명 추가 * 를 선택하여 NetApp Support 사이트 계정을 추가할 수 있습니다.
4. 다음 옵션을 선택하여 기존 자격 증명을 관리합니다.
 - * 자격 증명 업데이트 *: 계정의 사용자 이름과 암호를 업데이트합니다.
 - * 자격 증명 삭제 *: BlueXP 사용자 계정과 연결된 계정을 제거합니다.



결과

BlueXP에서 자격 증명을 업데이트합니다. 변경 사항은 ONTAP 클러스터, 디지털 어드바이저 또는 케이스 관리 페이지에 액세스할 때 반영됩니다.

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 라이선스와 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 라이선스도 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 라이선스를 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 라이선스는 DFARS 조항 252.227-7015(b)(2014년 2월)에 명시된 권한으로 제한됩니다.

상표 정보

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