관리 및 모니터링

NetApp Console setup and administration

NetApp
February 11, 2026

목차

관리 및 모니터링

NetApp 지원 계정 담당자

NetApp Console 과 관련된 NSS 자격 증명 관리

NetApp 지원 사이트 계정을 콘솔 조직과 연결하여 스토리지 관리를 위한 주요 워크플로를 활성화하세요. 이러한 NSS 자격증은 조직 전체와 연관되어 있습니다.

콘솔은 사용자 계정당 하나의 NSS 계정을 연결하는 것도 지원합니다. "사용자 수준 자격 증명을 관리하는 방법을 알아보세요" .

개요

다음 작업을 활성화하려면 NetApp 지원 사이트 자격 증명을 특정 콘솔 계정 일련 번호와 연결해야 합니다.

- BYOL(Bring Your Own License)을 사용할 때 Cloud Volumes ONTAP 배포

  콘솔에서 라이선스 키를 업로드하고 구매한 기간 동안 구독을 활성화하려면 NSS 계정을 제공해야 합니다. 여기에는 기간 갱신을 위한 자동 업데이트가 포함됩니다.

- 사용량에 따라 지불하는 Cloud Volumes ONTAP 시스템 등록

  시스템 지원을 활성화하고 NetApp 기술 지원 리소스에 액세스하려면 NSS 계정을 제공해야 합니다.

- Cloud Volumes ONTAP 소프트웨어를 최신 릴리스로 업그레이드

이러한 자격 증명은 특정 콘솔 계정 일련 번호와 연결됩니다. 사용자는 *지원 > NSS 관리*에서 이러한 자격 증명에 액세스할 수 있습니다.

NSS 계정 추가

콘솔 내의 지원 대시보드에서 콘솔에서 사용할 NetApp 지원 사이트 계정을 추가하고 관리할 수 있습니다.

NSS 계정을 추가하면 콘솔은 라이선스 다운로드, 소프트웨어 업그레이드 확인, 향후 지원 등록 등에 이 정보를 사용합니다.

귀하의 조직에 여러 개의 NSS 계정을 연결할 수 있습니다. 그러나 동일한 조직 내에서 고객 계정과 파트너 계정을 가질 수는 없습니다.

NetApp 지원 및 라이선싱에 특화된 인증 서비스를 위한 ID 공급자로 Microsoft Entra ID를 사용합니다.

단계

1. *관리 > 지원*에서.
2. *NSS 관리*를 선택하세요.
3. *NSS 계정 추가*를 선택하세요.
4. *계속*을 선택하면 Microsoft 로그인 페이지로 이동합니다.

5. 로그인 페이지에서 NetApp 지원 사이트에 등록된 이메일 주소와 비밀번호를 입력하세요.

   로그인에 성공하면 NetApp NSS 사용자 이름을 저장합니다.

   이는 귀하의 이메일에 매핑되는 시스템 생성 ID입니다. **NSS** 관리 페이지에서 이메일을 표시할 수 있습니다. ••• 메뉴.

   - 로그인 자격 증명 토큰을 새로 고쳐야 하는 경우 자격 증명 업데이트 옵션도 있습니다. ••• 메뉴.

     이 옵션을 사용하면 다시 로그인하라는 메시지가 표시됩니다. 이 계정의 토큰은 90일 후에 만료됩니다. 이에 대한 알림이 게시됩니다.

다음은 무엇인가요?

이제 사용자는 새로운 Cloud Volumes ONTAP 시스템을 생성할 때와 기존 Cloud Volumes ONTAP 시스템을 등록할 때 계정을 선택할 수 있습니다.

- "AWS에서 Cloud Volumes ONTAP 출시"
- "Azure에서 Cloud Volumes ONTAP 시작"
- "Google Cloud에서 Cloud Volumes ONTAP 출시"
- "선불제 시스템 등록"

NSS 자격 증명 업데이트

보안상의 이유로 NSS 자격 증명은 90일마다 업데이트해야 합니다. NSS 자격 증명이 만료되면 콘솔 알림 센터에서 알림을 받게 됩니다. "알림 센터에 대해 알아보세요" .

만료된 자격 증명으로 인해 다음과 같은 문제가 발생할 수 있습니다(이에 국한되지 않음).

- 라이선스 업데이트로 인해 새로 구매한 용량을 활용할 수 없게 됩니다.
- 지원 사례를 제출하고 추적하는 기능.

또한, 조직과 연결된 NSS 계정을 변경하려는 경우 조직과 연결된 NSS 자격 증명을 업데이트할 수 있습니다. 예를 들어, NSS 계정과 연결된 사람이 회사를 떠난 경우입니다.

단계

1. *관리 > 지원*에서.
2. *NSS 관리*를 선택하세요.
3. 업데이트하려는 NSS 계정에 대해 다음을 선택하세요.••• 그런 다음 *자격 증명 업데이트*를 선택하세요.
4. 메시지가 표시되면 *계속*을 선택하여 Microsoft 로그인 페이지로 이동합니다.

   NetApp 지원 및 라이선싱과 관련된 인증 서비스를 위한 ID 공급자로 Microsoft Entra ID를 사용합니다.

5. 로그인 페이지에서 NetApp 지원 사이트에 등록된 이메일 주소와 비밀번호를 입력하세요.

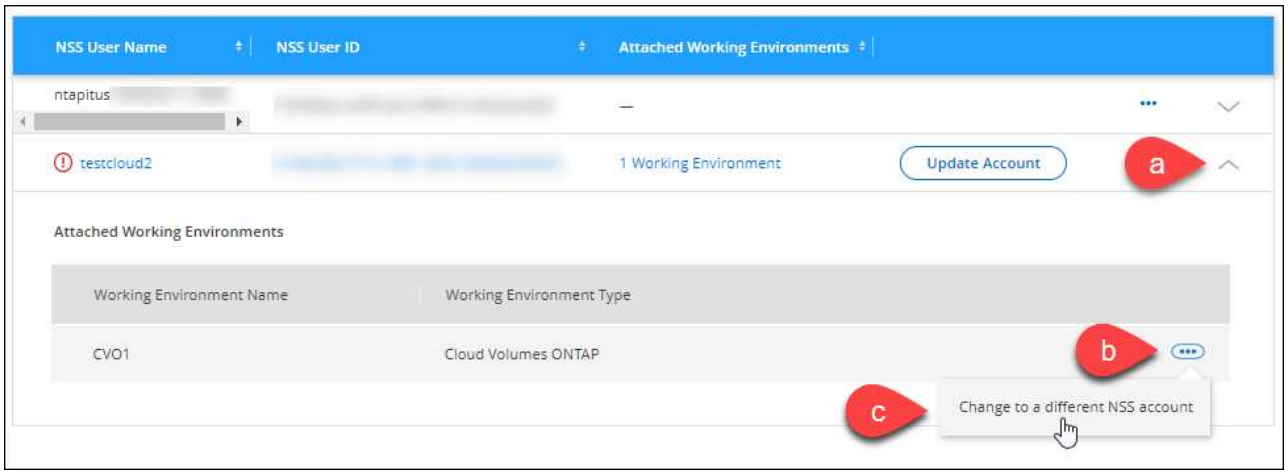
다른 **NSS** 계정에 시스템 연결

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

먼저 계정을 콘솔에 연결해야 합니다.

단계

1. *관리 > 지원*에서.
2. *NSS 관리*를 선택하세요.
3. NSS 계정을 변경하려면 다음 단계를 완료하세요.
   a. 시스템이 현재 연결되어 있는 NetApp 지원 사이트 계정에 대한 행을 확장합니다.
   b. 연결을 변경하려는 시스템에 대해 다음을 선택하세요.•••
   c. *다른 NSS 계정으로 변경*을 선택하세요.



   d. 계정을 선택한 다음 *저장*을 선택하세요.

NSS 계정의 이메일 주소 표시

보안상의 이유로 NSS 계정과 연결된 이메일 주소는 기본적으로 표시되지 않습니다. NSS 계정의 이메일 주소와 관련 사용자 이름을 볼 수 있습니다.

NSS 관리 페이지로 이동하면 콘솔이 표의 각 계정에 대한 토큰을 생성합니다. 해당 토큰에는 연관된 이메일 주소에 대한 정보가 포함되어 있습니다. 페이지를 벗어나면 토큰이 제거됩니다. 해당 정보는 캐시되지 않으므로 개인 정보가 보호됩니다.

단계

1. *관리 > 지원*에서.
2. *NSS 관리*를 선택하세요.
3. 업데이트하려는 NSS 계정에 대해 다음을 선택하세요.••• 그런 다음 *이메일 주소 표시*를 선택하세요. 복사 버튼을 사용하여 이메일 주소를 복사할 수 있습니다.

NSS 계정 제거

더 이상 콘솔에서 사용하지 않을 NSS 계정을 삭제하세요.

현재 Cloud Volumes ONTAP 시스템과 연결된 계정은 삭제할 수 없습니다. 먼저 다음이 필요합니다.해당 시스템을 다른 NSS 계정에 연결합니다. .

단계

1. *관리 > 지원*에서.
2. *NSS 관리*를 선택하세요.
3. 삭제하려는 NSS 계정에 대해 다음을 선택하세요. ••• 그런 다음 *삭제*를 선택하세요.
4. 삭제를 선택하여 확인하세요.

NetApp Console 로그인과 관련된 자격 증명 관리

콘솔에서 수행한 작업에 따라 ONTAP 자격 증명과 NetApp 지원 사이트(NSS) 자격 증명을 사용자 로그인과 연결했을 수 있습니다. 해당 자격 증명을 연결한 후에는 해당 자격 증명을 보고 관리할 수 있습니다. 예를 들어, 이러한 자격 증명의 비밀번호를 변경하는 경우 콘솔에서 비밀번호를 업데이트해야 합니다.

ONTAP 자격 증명

사용자는 콘솔에서 ONTAP 클러스터를 검색하려면 ONTAP 관리자 자격 증명이 필요합니다. 하지만 ONTAP 시스템 관리자 액세스는 콘솔 에이전트를 사용하는지 여부에 따라 달라집니다.

콘솔 에이전트 없이

클러스터의 ONTAP 시스템 관리자에 액세스하려면 사용자에게 ONTAP 자격 증명을 입력하라는 메시지가 표시됩니다. 사용자는 이러한 자격 증명을 콘솔에 저장하도록 선택할 수 있으며, 그렇게 하면 매번 입력하라는 메시지가 표시되지 않습니다. 사용자 자격 증명은 해당 사용자에게만 표시되며 사용자 자격 증명 페이지에서 관리할 수 있습니다.

콘솔 에이전트를 사용하여

기본적으로 사용자는 ONTAP 시스템 관리자에 액세스하기 위해 ONTAP 자격 증명을 입력하라는 메시지를 받지 않습니다. 하지만 콘솔 관리자(조직 관리자 역할 있음)는 사용자에게 ONTAP 자격 증명을 입력하라는 메시지를 표시하도록 콘솔을 구성할 수 있습니다. 이 설정을 활성화하면 사용자는 매번 ONTAP 자격 증명을 입력해야 합니다.

"자세히 알아보세요."

NSS 자격 증명

NetApp Console 로그인과 연결된 NSS 자격 증명을 통해 지원 등록, 사례 관리 및 Digital Advisor 에 액세스할 수 있습니다.

- *지원 > 리소스*에 액세스하여 지원에 등록하면 NSS 자격 증명을 로그인과 연결하라는 메시지가 표시됩니다.

  이렇게 하면 귀하의 조직이나 계정이 지원을 위해 등록되고 지원 자격이 활성화됩니다. 귀하의 조직에서 단 한 명의 사용자만이 NetApp 지원 사이트 계정을 로그인과 연결하여 지원을 등록하고 지원 자격을 활성화해야 합니다. 이 작업이 완료되면 리소스 페이지에 귀하의 계정이 지원을 위해 등록되었다는 메시지가 표시됩니다.

  "지원 등록 방법 알아보기"

- *관리 > 지원 > 사례 관리*에 액세스하면 NSS 자격 증명을 입력하라는 메시지가 표시됩니다(아직 입력하지 않은 경우). 이 페이지에서는 NSS 계정과 회사와 관련된 지원 사례를 만들고 관리할 수 있습니다.
- 콘솔에서 Digital Advisor 에 액세스하면 NSS 자격 증명을 입력하여 Digital Advisor 에 로그인하라는 메시지가 표시됩니다.

로그인과 관련된 NSS 계정에 대해 다음 사항을 참고하세요.

- 계정은 사용자 수준에서 관리되므로 로그인하는 다른 사용자는 계정을 볼 수 없습니다.
- 사용자당 Digital Advisor 및 지원 사례 관리와 연결된 NSS 계정은 하나만 있을 수 있습니다.
- NetApp 지원 사이트 계정을 Cloud Volumes ONTAP 시스템과 연결하려는 경우, 본인이 소속된 조직에 추가된 NSS 계정에서만 선택할 수 있습니다.

  NSS 계정 수준 자격 증명은 로그인과 연결된 NSS 계정과 다릅니다. NSS 계정 수준 자격 증명을 사용하면 BYOL로 Cloud Volumes ONTAP 배포하고, PAYGO 시스템을 등록하고, 소프트웨어를 업그레이드할 수 있습니다.

  "NetApp Console 조직 또는 계정에서 NSS 자격 증명을 사용하는 방법에 대해 자세히 알아보세요." .

사용자 자격 증명을 관리하세요

사용자 이름과 비밀번호를 업데이트하거나 자격 증명을 삭제하여 사용자 자격 증명을 관리하세요.

단계

1. *관리 > 자격 증명*을 선택합니다.
2. *사용자 자격 증명*을 선택하세요.
3. 아직 사용자 자격 증명이 없으면 *NSS 자격 증명 추가*를 선택하여 NetApp 지원 사이트 계정을 추가할 수 있습니다.
4. 다음 옵션을 작업 메뉴에서 선택하여 기존 자격 증명을 관리하세요.
   - 자격 증명 업데이트: 계정의 사용자 이름과 비밀번호를 업데이트합니다.
   - 자격 증명 삭제: 콘솔 로그인과 연결된 NSS 계정을 제거합니다.

콘솔 에이전트

NetApp Console 에이전트에 대해 알아보세요

콘솔 에이전트를 사용하면 NetApp Console 인프라에 연결하고 AWS, Azure, Google Cloud 또는 온프레미스 환경 전반에 걸쳐 스토리지 솔루션을 안전하게 오케스트레이션할 뿐만 아니라 데이터 보호 서비스도 사용할 수 있습니다.

콘솔 에이전트를 사용하면 다음 작업을 수행할 수 있습니다.

- NetApp Console 에서 Cloud Volumes ONTAP 프로비저닝, 스토리지 볼륨 설정, 데이터 분류 사용 등과 같은 스토리지 관리 작업을 오케스트레이션할 수 있습니다.
- 구독 결제 통합을 위해 클라우드 공급업체의 IAM 역할을 사용하여 인증하세요.
- 고급 데이터 서비스(NetApp Backup and Recovery, NetApp Disaster Recovery, NetApp Ransomware Resilience 및 NetApp Cloud Tiering)를 활용하십시오.
- 콘솔을 제한 모드로 사용하십시오.

고급 오케스트레이션이나 데이터 보호 기능이 필요하지 않은 경우 에이전트를 배포하지 않고도 온프레미스 ONTAP 클러스터와 클라우드 네이티브 스토리지 서비스를 중앙에서 관리할 수 있습니다. 모니터링 및 데이터 이동성 도구도 사용할 수 있습니다.

다음 표는 콘솔 에이전트를 사용하거나 사용하지 않고 사용할 수 있는 기능과 서비스를 보여줍니다.

	중개인을 통해 이용 가능합니다.	중개인 없이 구매 가능
지원되는 스토리지 시스템:		
ONTAP 용 Amazon FSx	예 (검색 및 관리 기능)	예 (탐색 전용)
Amazon S3 스토리지	예	아니요
Azure Blob 저장소	예	예
Azure NetApp Files	예	예
Cloud Volumes ONTAP	예	아니요
E-시리즈 시스템	예	아니요
Google Cloud NetApp Volumes	예	예
구글 클라우드 스토리지 버킷	예	아니요
StorageGRID 시스템	예	아니요
온프레미스 ONTAP 클러스터(고급 관리 및 검색)	예 (고급 관리 및 발견)	아니요 (기본적인 탐색만 가능)
이용 가능한 스토리지 관리 서비스:		
알림	예	아니요
자동화 허브	예	예
Digital Advisor (Active IQ)	예	아니요
라이선스 및 구독 관리	예	아니요
경제적 효율성	예	아니요
홈페이지 대시보드 지표	네[2]	아니요
수명주기 계획	예	아니요[1]
지속 가능성	예	아니요

	중개인을 통해 이용 가능합니다.	중개인 없이 구매 가능
소프트웨어 업데이트	예	예
NetApp 워크로드	예	예
이용 가능한 데이터 서비스:		
NetApp Backup and Recovery	예	아니요
데이터 분류	예	아니요
NetApp Cloud Tiering	예	아니요
NetApp Copy and Sync	예	아니요
NetApp Disaster Recovery	예	아니요
NetApp Ransomware Resilience	예	아니요
NetApp Volume Caching	예	아니요

[1] 콘솔 에이전트 없이도 라이프사이클 계획을 볼 수 있지만, 작업을 시작하려면 콘솔 에이전트가 필요합니다.

[2] 홈 페이지에 정확한 메트릭을 표시하려면 적절한 크기와 구성의 콘솔 에이전트가 필요합니다.

콘솔 에이전트는 항상 작동해야 합니다.

콘솔 에이전트는 NetApp Console 의 기본적인 부분입니다. 관련 상담원이 항상 가동되고, 업무를 처리하며, 접근 가능한지 확인하는 것은 고객 여러분의 책임입니다. 콘솔은 짧은 에이전트 중단은 처리할 수 있지만 인프라 장애는 신속하게 해결해야 합니다.

이 문서는 EULA에 따라 관리됩니다. 설명서에 없는 방식으로 제품을 작동하면 제품의 기능과 EULA 권리에 영향을 미칠 수 있습니다.

지원되는 위치

다음 위치에 에이전트를 설치할 수 있습니다.

- 아마존 웹 서비스
- 마이크로소프트 애저

  Cloud Volumes ONTAP 시스템을 관리하는 것과 동일한 지역에 Azure에 콘솔 에이전트를 배포합니다. 또는 다음을 배포합니다. "Azure 지역 쌍" . 이렇게 하면 Cloud Volumes ONTAP 과 연결된 스토리지 계정 간에 Azure Private Link 연결이 사용됩니다. "Cloud Volumes ONTAP Azure Private Link를 사용하는 방법 알아보기"

- 구글 클라우드

Google Cloud에서 콘솔과 데이터 서비스를 사용하려면 Google Cloud에 에이전트를 배포하세요.

- 귀하의 구내에서

클라우드 제공자와의 커뮤니케이션

에이전트는 AWS, Azure, Google Cloud와의 모든 통신에 TLS 1.3을 사용합니다.

제한 모드

제한 모드에서 콘솔을 사용하려면 콘솔 에이전트를 설치하고 콘솔 에이전트에서 로컬로 실행되는 콘솔 인터페이스에 액세스해야 합니다.

"NetApp Console 배포 모드에 대해 알아보세요" .

콘솔 에이전트를 설치하는 방법

콘솔에서 직접 콘솔 에이전트를 설치하거나, 클라우드 공급업체의 마켓플레이스를 이용하거나, 자신의 Linux 호스트나 VCenter 환경에 소프트웨어를 수동으로 설치할 수 있습니다.

- "NetApp Console 배포 모드에 대해 알아보세요"
- "표준 모드에서 NetApp Console 시작하기"
- "제한 모드에서 NetApp Console 시작하기"

클라우드 공급자 권한

NetApp Console 에서 직접 콘솔 에이전트를 생성하려면 특정 권한이 필요하고 콘솔 에이전트 자체에 대한 또 다른 권한 집합이 필요합니다. AWS 또는 Azure에서 콘솔을 통해 직접 콘솔 에이전트를 만드는 경우 콘솔은 필요한 권한을 가진 콘솔 에이전트를 만듭니다.

표준 모드에서 콘솔을 사용하는 경우 권한을 제공하는 방법은 콘솔 에이전트를 만들려는 방법에 따라 달라집니다.

권한을 설정하는 방법을 알아보려면 다음을 참조하세요.

- 표준 모드
  - "AWS의 에이전트 설치 옵션"
  - "Azure의 에이전트 설치 옵션"
  - "Google Cloud의 에이전트 설치 옵션"
  - "온프레미스 배포에 대한 클라우드 권한 설정"
- "제한 모드에 대한 권한 설정"

콘솔 에이전트가 일상 업무를 수행하는 데 필요한 정확한 권한을 보려면 다음 페이지를 참조하세요.

- "콘솔 에이전트가 AWS 권한을 사용하는 방법을 알아보세요."
- "콘솔 에이전트가 Azure 권한을 사용하는 방법 알아보기"
- "콘솔 에이전트가 Google Cloud 권한을 사용하는 방법을 알아보세요."

이후 릴리스에서 새로운 권한이 추가되면 콘솔 에이전트 정책을 업데이트하는 것은 사용자의 책임입니다. 릴리스

노트에는 새로운 권한이 나열되어 있습니다.

에이전트 업그레이드

NetApp 기능을 추가하고 안정성을 개선하기 위해 매달 에이전트 소프트웨어를 업데이트합니다. Cloud Volumes ONTAP 및 온프레미스 ONTAP 클러스터 관리와 같은 일부 콘솔 기능은 콘솔 에이전트 버전 및 설정에 따라 달라집니다.

클라우드에 에이전트를 설치하면 인터넷에 연결되어 있는 경우 콘솔 에이전트가 자동으로 업데이트됩니다.

운영 체제 및 **VM** 유지 관리

콘솔 에이전트 호스트에서 운영 체제를 유지 관리하는 것은 귀하(고객)의 책임입니다. 예를 들어, 귀하(고객)는 회사의 운영 체제 배포에 대한 표준 절차에 따라 콘솔 에이전트 호스트의 운영 체제에 보안 업데이트를 적용해야 합니다.

사소한 보안 업데이트를 적용할 때 고객은 콘솔 호스트에서 어떤 서비스도 중지할 필요가 없습니다.

고객이 콘솔 에이전트 VM을 중지했다가 다시 시작해야 하는 경우, 클라우드 제공업체의 콘솔에서 수행하거나 온프레미스 관리를 위한 표준 절차를 사용해야 합니다.

콘솔 에이전트는 항상 작동해야 합니다. .

다중 시스템 및 에이전트

에이전트는 콘솔에서 여러 시스템을 관리하고 데이터 서비스를 지원할 수 있습니다. 배포 규모와 사용하는 데이터 서비스에 따라 단일 에이전트를 사용하여 여러 시스템을 관리할 수 있습니다.

대규모 배포의 경우 NetApp 담당자와 협력하여 환경 크기를 조정하세요. 문제가 발생하면 NetApp 지원팀에 문의하세요.

에이전트 배포의 몇 가지 예는 다음과 같습니다.

- 멀티클라우드 환경(예: AWS와 Azure)이 있고 AWS에 한 에이전트, Azure에 다른 에이전트를 두는 것을 선호합니다. 각각은 해당 환경에서 실행되는 Cloud Volumes ONTAP 시스템을 관리합니다.
- 서비스 제공자는 한 콘솔 조직을 사용하여 고객에게 서비스를 제공하는 동시에, 다른 조직을 사용하여 사업부 중 하나에 대한 재해 복구를 제공할 수 있습니다. 각 조직에는 자체 에이전트가 필요합니다.

콘솔 에이전트 배포

AWS

AWS의 콘솔 에이전트 설치 옵션

AWS에서 콘솔 에이전트를 만드는 방법에는 여러 가지가 있습니다. 가장 일반적인 방법은 NetApp Console 에서 직접 실행하는 것입니다.

다음과 같은 설치 옵션을 사용할 수 있습니다.

- "콘솔에서 직접 콘솔 에이전트를 만듭니다."(이것은 표준 옵션입니다)

  이 작업을 수행하면 선택한 VPC에서 Linux와 콘솔 에이전트 소프트웨어를 실행하는 EC2 인스턴스가 시작됩니다.

- "AWS Marketplace에서 콘솔 에이전트 만들기"

  이 작업을 수행하면 Linux와 콘솔 에이전트 소프트웨어가 실행되는 EC2 인스턴스가 시작되지만 배포는 콘솔이 아닌 AWS Marketplace에서 직접 시작됩니다.

- "자신의 Linux 호스트에 소프트웨어를 다운로드하고 수동으로 설치하세요."

선택하는 설치 옵션은 설치를 준비하는 방법에 영향을 미칩니다. 여기에는 AWS에서 리소스를 인증하고 관리하는 데 필요한 권한을 콘솔에 제공하는 방법이 포함됩니다.

NetApp Console 에서 **AWS**에 콘솔 에이전트 만들기

NetApp Console 에서 직접 AWS에서 콘솔 에이전트를 만들 수 있습니다. AWS 콘솔에서 콘솔 에이전트를 생성하기 전에 네트워킹을 설정하고 AWS 권한을 준비해야 합니다.

시작하기 전에

- 당신은 ~을 가져야합니다"콘솔 에이전트에 대한 이해" .
- 검토해야 합니다"콘솔 에이전트 제한 사항" .

1단계**: AWS**에 콘솔 에이전트를 배포하기 위한 네트워킹 설정

콘솔 에이전트를 설치하려는 네트워크 위치가 다음 요구 사항을 지원하는지 확인하세요. 이러한 요구 사항을 통해 콘솔 에이전트는 하이브리드 클라우드의 리소스와 프로세스를 관리할 수 있습니다.

VPC 및 서브넷

콘솔 에이전트를 생성할 때는 에이전트가 상주해야 하는 VPC와 서브넷을 지정해야 합니다.

대상 네트워크에 대한 연결

콘솔 에이전트를 사용하려면 시스템을 만들고 관리하려는 위치에 대한 네트워크 연결이 필요합니다. 예를 들어, Cloud Volumes ONTAP 시스템이나 온프레미스 환경의 스토리지 시스템을 만들 계획인 네트워크입니다.

아웃바운드 인터넷 접속

콘솔 에이전트를 배포하는 네트워크 위치에는 특정 엔드포인트에 연결하기 위한 아웃바운드 인터넷 연결이 있어야 합니다.

콘솔 에이전트에서 연락한 엔드포인트

콘솔 에이전트는 일상 업무를 위해 퍼블릭 클라우드 환경 내의 리소스와 프로세스를 관리하기 위해 다음 엔드포인트에 연결하기 위해 아웃바운드 인터넷 액세스가 필요합니다.

아래 나열된 엔드포인트는 모두 CNAME 항목입니다.

엔드포인트	목적
AWS 서비스(amazonaws.com): • 클라우드포메이션 • 탄력적 컴퓨팅 클라우드(EC2) • ID 및 액세스 관리(IAM) • 키 관리 서비스(KMS) • 보안 토큰 서비스(STS) • 간편 보관 서비스(S3)	AWS 리소스를 관리합니다. 엔드포인트는 AWS 지역에 따라 달라집니다. "자세한 내용은 AWS 설명서를 참조하세요."
Amazon FsX for NetApp ONTAP: • api.workloads.netapp.com	웹 기반 콘솔은 이 엔드포인트에 연결하여 Workload Factory API와 상호 작용함으로써 ONTAP 기반 워크로드용 FSx를 관리하고 운영합니다.
\ https://mysupport.netapp.com	라이선스 정보를 얻고 NetApp 지원팀에 AutoSupport 메시지를 보냅니다.
\ https://signin.b2c.netapp.com	NetApp 지원 사이트(NSS) 자격 증명을 업데이트하거나 NetApp Console 에 새로운 NSS 자격 증명을 추가합니다.
\ https://support.netapp.com	라이선스 정보를 얻고 NetApp 지원팀에 AutoSupport 메시지를 보내고 Cloud Volumes ONTAP 에 대한 소프트웨어 업데이트를 받습니다.
\ https://api.bluexp.netapp.com \ https://netapp-cloud-account.auth0.com \ https://netapp-cloud-account.us.auth0.com \ https://console.netapp.com \ https://components.console.bluexp.netapp.com \ https://cdn.auth0.com	NetApp Console 내에서 기능과 서비스를 제공합니다.

엔드포인트	목적
\ https://bluexpinfraprod.eastus2.data.azurecr.io \ https://bluexpinfraprod.azurecr.io	콘솔 에이전트 업그레이드를 위한 이미지를 얻으려면. • 새로운 에이전트를 배포할 때 유효성 검사를 통해 현재 엔드포인트에 대한 연결성을 테스트합니다. 당신이 사용하는 경우"이전 종료점" , 유효성 검사에 실패합니다. 이러한 실패를 방지하려면 유효성 검사를 건너뛰세요. 이전 엔드포인트는 계속 지원되지만 NetApp 가능한 한 빨리 현재 엔드포인트에 맞게 방화벽 규칙을 업데이트할 것을 권장합니다. "엔드포인트 목록을 업데이트하는 방법을 알아보세요" . • 방화벽의 현재 엔드포인트로 업데이트하면 기존 에이전트도 계속 작동합니다.

NetApp 콘솔에서 연결된 엔드포인트

SaaS 계층을 통해 제공되는 웹 기반 NetApp Console 사용하면 여러 엔드포인트에 연결하여 데이터 관리 작업을 완료할 수 있습니다. 여기에는 콘솔에서 콘솔 에이전트를 배포하기 위해 연결된 엔드포인트가 포함됩니다.

"NetApp 콘솔에서 연결된 엔드포인트 목록 보기" .

프록시 서버

NetApp 명시적 프록시 구성과 투명 프록시 구성을 모두 지원합니다. 투명 프록시를 사용하는 경우 프록시 서버에 대한 인증서만 제공하면 됩니다. 명시적 프록시를 사용하는 경우 IP 주소와 자격 증명도 필요합니다.

- IP 주소
- 신임장
- HTTPS 인증서

포트

Cloud Volumes ONTAP 에서 NetApp 지원팀으로 AutoSupport 메시지를 보내기 위한 프록시로 사용되거나 사용자가 시작하지 않는 한 콘솔 에이전트로 들어오는 트래픽이 없습니다.

- HTTP(80) 및 HTTPS(443)는 로컬 UI에 대한 액세스를 제공하며 이는 드문 상황에서 사용됩니다.
- SSH(22)는 문제 해결을 위해 호스트에 연결해야 하는 경우에만 필요합니다.
- 아웃바운드 인터넷 연결을 사용할 수 없는 서브넷에 Cloud Volumes ONTAP 시스템을 배포하는 경우 포트 3128을 통한 인바운드 연결이 필요합니다.

Cloud Volumes ONTAP 시스템에 AutoSupport 메시지를 보낼 아웃바운드 인터넷 연결이 없는 경우 콘솔은 콘솔 에이전트에 포함된 프록시 서버를 사용하도록 해당 시스템을 자동으로 구성합니다. 유일한 요구 사항은 콘솔 에이전트의 보안 그룹이 포트 3128을 통한 인바운드 연결을 허용하는 것입니다. 콘솔 에이전트를 배포한 후 이 포트를 열어야 합니다.

NTP 활성화

NetApp Data Classification 사용하여 회사 데이터 소스를 스캔하려는 경우 콘솔 에이전트와 NetApp Data Classification 시스템 모두에서 NTP(네트워크 시간 프로토콜) 서비스를 활성화하여 시스템 간의 시간을 동기화해야 합니다. "NetApp 데이터 분류에 대해 자세히 알아보세요"

콘솔 에이전트를 만든 후 이 네트워킹 요구 사항을 구현해야 합니다.

2단계**:** 콘솔 에이전트에 대한 **AWS** 권한 설정

VPC에 콘솔 에이전트를 배포하려면 먼저 콘솔이 AWS에서 인증을 받아야 합니다. 다음 인증 방법 중 하나를 선택할 수 있습니다.

- 콘솔이 필요한 권한이 있는 IAM 역할을 가정하도록 합니다.
- 필요한 권한이 있는 IAM 사용자에게 AWS 액세스 키와 비밀 키를 제공합니다.

두 옵션 모두 첫 번째 단계는 IAM 정책을 만드는 것입니다. 이 정책에는 AWS 콘솔에서 콘솔 에이전트를 시작하는 데 필요한 권한만 포함되어 있습니다.

필요한 경우 IAM을 사용하여 IAM 정책을 제한할 수 있습니다. `Condition` 요소. "AWS 설명서: 조건 요소"

단계

1. AWS IAM 콘솔로 이동합니다.
2. *정책 > 정책 만들기*를 선택합니다.
3. *JSON*을 선택하세요.
4. 다음 정책을 복사하여 붙여넣으세요.

   이 정책에는 AWS 콘솔에서 콘솔 에이전트를 시작하는 데 필요한 권한만 포함되어 있습니다. 콘솔이 콘솔 에이전트를 생성하면 콘솔 에이전트가 AWS 리소스를 관리할 수 있도록 하는 새로운 권한 집합이 콘솔 에이전트에 적용됩니다. "콘솔 에이전트 자체에 필요한 권한 보기".

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "iam:CreateRole",
        "iam:DeleteRole",
        "iam:PutRolePolicy",
        "iam:CreateInstanceProfile",
        "iam:DeleteRolePolicy",
        "iam:AddRoleToInstanceProfile",
```

```
        "iam:RemoveRoleFromInstanceProfile",
        "iam:DeleteInstanceProfile",
        "iam:PassRole",
        "iam:ListRoles",
        "ec2:DescribeInstanceStatus",
        "ec2:RunInstances",
        "ec2:ModifyInstanceAttribute",
        "ec2:CreateSecurityGroup",
        "ec2:DeleteSecurityGroup",
        "ec2:DescribeSecurityGroups",
        "ec2:RevokeSecurityGroupEgress",
        "ec2:AuthorizeSecurityGroupEgress",
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:RevokeSecurityGroupIngress",
        "ec2:CreateNetworkInterface",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DeleteNetworkInterface",
        "ec2:ModifyNetworkInterfaceAttribute",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "ec2:DescribeDhcpOptions",
        "ec2:DescribeKeyPairs",
        "ec2:DescribeRegions",
        "ec2:DescribeInstances",
        "ec2:CreateTags",
        "ec2:DescribeImages",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeLaunchTemplates",
        "ec2:CreateLaunchTemplate",
        "cloudformation:CreateStack",
        "cloudformation:DeleteStack",
        "cloudformation:DescribeStacks",
        "cloudformation:DescribeStackEvents",
        "cloudformation:ValidateTemplate",
        "ec2:AssociateIamInstanceProfile",
        "ec2:DescribeIamInstanceProfileAssociations",
        "ec2:DisassociateIamInstanceProfile",
        "iam:GetRole",
        "iam:TagRole",
        "kms:ListAliases",
        "cloudformation:ListStacks"
      ],
      "Resource": "*"
    },
    {
      "Effect": "Allow",
```

```
        "Action": [
          "ec2:TerminateInstances"
        ],
        "Condition": {
          "StringLike": {
            "ec2:ResourceTag/OCCMInstance": "*"
          }
        },
        "Resource": [
          "arn:aws:ec2:*:*:instance/*"
        ]
      }
    ]
}
```

5. *다음*을 선택하고 필요한 경우 태그를 추가합니다.
6. *다음*을 선택하고 이름과 설명을 입력합니다.
7. *정책 만들기*를 선택하세요.
8. 콘솔이 가정할 수 있는 IAM 역할이나 IAM 사용자에게 정책을 연결하여 콘솔에 액세스 키를 제공할 수 있습니다.
   - (옵션 1) 콘솔이 맡을 수 있는 IAM 역할을 설정합니다.
     i. 대상 계정의 AWS IAM 콘솔로 이동합니다.
     ii. 액세스 관리에서 *역할 > 역할 만들기*를 선택하고 단계에 따라 역할을 만듭니다.
     iii. *신뢰할 수 있는 엔터티 유형*에서 *AWS 계정*을 선택합니다.
     iv. *다른 AWS 계정*을 선택하고 콘솔 SaaS 계정의 ID를 입력하세요: 952013314444
     v. 이전 섹션에서 만든 정책을 선택하세요.
     vi. 역할을 만든 후 역할 ARN을 복사하여 콘솔 에이전트를 만들 때 콘솔에 붙여넣을 수 있습니다.
   - (옵션 2) 콘솔에 액세스 키를 제공할 수 있도록 IAM 사용자에 대한 권한을 설정합니다.
     i. AWS IAM 콘솔에서 *사용자*를 선택한 다음 사용자 이름을 선택합니다.
     ii. *권한 추가 > 기존 정책을 직접 첨부*를 선택합니다.
     iii. 생성한 정책을 선택하세요.
     iv. *다음*을 선택한 다음 *권한 추가*를 선택합니다.
     v. IAM 사용자에 대한 액세스 키와 비밀 키가 있는지 확인하세요.

결과

이제 필요한 권한이 있는 IAM 역할이나 필요한 권한이 있는 IAM 사용자가 생겼습니다. 콘솔에서 콘솔 에이전트를 만들 때 역할이나 액세스 키에 대한 정보를 제공할 수 있습니다.

3단계**:** 콘솔 에이전트 만들기

콘솔 웹 기반 콘솔에서 직접 콘솔 에이전트를 만듭니다.

이 작업에 관하여

- 콘솔에서 콘솔 에이전트를 생성하면 기본 구성을 사용하여 AWS에 EC2 인스턴스가 배포됩니다. 콘솔 에이전트를 생성한 후에는 CPU나 RAM이 적은 더 작은 EC2 인스턴스로 전환하지 마세요. "콘솔 에이전트의 기본 구성에 대해 알아보세요" .
- 콘솔에서 콘솔 에이전트를 생성하면 에이전트에 대한 IAM 역할과 프로필이 생성됩니다. 이 역할에는 콘솔 에이전트가 AWS 리소스를 관리할 수 있는 권한이 포함됩니다. 향후 릴리스에서 새로운 권한이 추가되면 역할이 업데이트되도록 하세요. "콘솔 에이전트에 대한 IAM 정책에 대해 자세히 알아보세요.".

시작하기 전에

다음 사항이 있어야 합니다.

- AWS 인증 방법: 필요한 권한이 있는 IAM 사용자에 대한 IAM 역할 또는 액세스 키입니다.
- 네트워킹 요구 사항을 충족하는 VPC 및 서브넷.
- EC2 인스턴스에 대한 키 쌍입니다.
- 콘솔 에이전트에서 인터넷에 접속하는 데 프록시가 필요한 경우 프록시 서버에 대한 세부 정보입니다.
- 설정"네트워킹 요구 사항" .
- 설정"AWS 권한" .

단계

1. *관리 > 에이전트*를 선택하세요.
2. 개요 페이지에서 *에이전트 배포 > AWS*를 선택합니다.
3. 마법사의 단계에 따라 콘솔 에이전트를 만듭니다.
4. 소개 페이지에서 프로세스 개요를 제공합니다.
5. **AWS** 자격 증명 페이지에서 AWS 지역을 지정한 다음 인증 방법을 선택합니다. 인증 방법은 콘솔에서 가정할 수 있는 IAM 역할이나 AWS 액세스 키 및 비밀 키입니다.

   *역할 가정*을 선택하면 콘솔 에이전트 배포 마법사에서 첫 번째 자격 증명 세트를 만들 수 있습니다. 추가 자격 증명 세트는 자격 증명 페이지에서 만들어야 합니다. 그러면 마법사의 드롭다운 목록에서 해당 항목을 사용할 수 있습니다. "추가 자격 증명을 추가하는 방법을 알아보세요" .

6. 세부정보 페이지에서 콘솔 에이전트에 대한 세부정보를 제공합니다.
   - 이름을 입력하세요.
   - 사용자 정의 태그(메타데이터)를 추가합니다.
   - 콘솔에서 필요한 권한이 있는 새 역할을 만들지 아니면 사용자가 설정한 기존 역할을 선택할지 선택합니다. "필요한 권한" .
   - 콘솔 에이전트의 EBS 디스크를 암호화할지 여부를 선택합니다. 기본 암호화 키를 사용하거나 사용자 지정 키를 사용할 수 있습니다.
7. 네트워크 페이지에서 에이전트에 대한 VPC, 서브넷 및 키 쌍을 지정하고, 공용 IP 주소를 활성화할지 여부를 선택하고, 선택적으로 프록시 구성을 지정합니다.

   콘솔 에이전트 가상 머신에 액세스하려면 올바른 키 쌍이 있는지 확인하세요. 키 쌍이 없으면 액세스할 수 없습니다.

8. 보안 그룹 페이지에서 새 보안 그룹을 만들지, 아니면 필요한 인바운드 및 아웃바운드 규칙을 허용하는 기존 보안

그룹을 선택할지 선택합니다.

"AWS에 대한 보안 그룹 규칙 보기" .

9. 선택 사항을 검토하여 설정이 올바른지 확인하세요.

   a. 에이전트 구성 검증 확인란은 배포 시 콘솔에서 네트워크 연결 요구 사항을 검증하도록 기본적으로 선택되어 있습니다. 콘솔에서 에이전트를 배포하지 못하면 문제 해결에 도움이 되는 보고서가 제공됩니다. 배포가 성공하면 보고서는 제공되지 않습니다.

   아직도 사용 중이라면"이전 종료점" 에이전트 업그레이드에 사용되면 유효성 검사가 오류로 인해 실패합니다. 이를 방지하려면 유효성 검사를 건너뛰려면 확인란의 선택을 취소하세요.

10. *추가*를 선택하세요.

    콘솔은 약 10분 안에 에이전트를 배포합니다. 프로세스가 완료될 때까지 페이지에 머물러주세요.

결과

프로세스가 완료되면 콘솔 에이전트를 콘솔에서 사용할 수 있습니다.

배포에 실패하면 콘솔에서 보고서와 로그를 다운로드하여 문제를 해결할 수 있습니다."설치 문제를 해결하는 방법을 알아보세요."

콘솔 에이전트를 생성한 동일한 AWS 계정에 Amazon S3 버킷이 있는 경우, 시스템 페이지에 Amazon S3 작업 환경이 자동으로 표시됩니다. "NetApp Console 에서 S3 버킷을 관리하는 방법을 알아보세요."

AWS Marketplace에서 콘솔 에이전트 만들기

AWS Marketplace에서 직접 AWS에서 콘솔 에이전트를 만들 수 있습니다. AWS Marketplace에서 콘솔 에이전트를 만들려면 네트워킹을 설정하고, AWS 권한을 준비하고, 인스턴스 요구 사항을 검토한 다음 콘솔 에이전트를 만들어야 합니다.

시작하기 전에

- 당신은 ~을 가져야합니다"콘솔 에이전트에 대한 이해" .
- 검토해야 합니다"콘솔 에이전트 제한 사항" .

1단계**:** 네트워킹 설정

하이브리드 클라우드 리소스를 관리하려면 콘솔 에이전트의 네트워크 위치가 다음 요구 사항을 충족하는지 확인하세요.

VPC 및 서브넷

콘솔 에이전트를 생성할 때는 에이전트가 상주해야 하는 VPC와 서브넷을 지정해야 합니다.

대상 네트워크에 대한 연결

콘솔 에이전트를 사용하려면 시스템을 만들고 관리하려는 위치에 대한 네트워크 연결이 필요합니다. 예를 들어, Cloud Volumes ONTAP 시스템이나 온프레미스 환경의 스토리지 시스템을 만들 계획인 네트워크입니다.

아웃바운드 인터넷 접속

콘솔 에이전트를 배포하는 네트워크 위치에는 특정 엔드포인트에 연결하기 위한 아웃바운드 인터넷 연결이 있어야 합니다.

콘솔 에이전트에서 연락한 엔드포인트

콘솔 에이전트는 일상 업무를 위해 퍼블릭 클라우드 환경 내의 리소스와 프로세스를 관리하기 위해 다음 엔드포인트에 연결하기 위해 아웃바운드 인터넷 액세스가 필요합니다.

아래 나열된 엔드포인트는 모두 CNAME 항목입니다.

엔드포인트	목적
AWS 서비스(amazonaws.com): • 클라우드포메이션 • 탄력적 컴퓨팅 클라우드(EC2) • ID 및 액세스 관리(IAM) • 키 관리 서비스(KMS) • 보안 토큰 서비스(STS) • 간편 보관 서비스(S3)	AWS 리소스를 관리합니다. 엔드포인트는 AWS 지역에 따라 달라집니다. "자세한 내용은 AWS 설명서를 참조하세요."
Amazon FsX for NetApp ONTAP: • api.workloads.netapp.com	웹 기반 콘솔은 이 엔드포인트에 연결하여 Workload Factory API와 상호 작용함으로써 ONTAP 기반 워크로드용 FSx를 관리하고 운영합니다.
\ https://mysupport.netapp.com	라이선스 정보를 얻고 NetApp 지원팀에 AutoSupport 메시지를 보냅니다.
\ https://signin.b2c.netapp.com	NetApp 지원 사이트(NSS) 자격 증명을 업데이트하거나 NetApp Console 에 새로운 NSS 자격 증명을 추가합니다.
\ https://support.netapp.com	라이선스 정보를 얻고 NetApp 지원팀에 AutoSupport 메시지를 보내고 Cloud Volumes ONTAP 에 대한 소프트웨어 업데이트를 받습니다.
\ https://api.bluexp.netapp.com \ https://netapp-cloud-account.auth0.com \ https://netapp-cloud-account.us.auth0.com \ https://console.netapp.com \ https://components.console.bluexp.netapp.com \ https://cdn.auth0.com	NetApp Console 내에서 기능과 서비스를 제공합니다.

엔드포인트	목적
\ https://bluexpinfraprod.eastus2.data.azurecr.io \ https://bluexpinfraprod.azurecr.io	콘솔 에이전트 업그레이드를 위한 이미지를 얻으려면. • 새로운 에이전트를 배포할 때 유효성 검사를 통해 현재 엔드포인트에 대한 연결성을 테스트합니다. 당신이 사용하는 경우"이전 종료점" , 유효성 검사에 실패합니다. 이러한 실패를 방지하려면 유효성 검사를 건너뛰세요. 이전 엔드포인트는 계속 지원되지만 NetApp 가능한 한 빨리 현재 엔드포인트에 맞게 방화벽 규칙을 업데이트할 것을 권장합니다. "엔드포인트 목록을 업데이트하는 방법을 알아보세요" . • 방화벽의 현재 엔드포인트로 업데이트하면 기존 에이전트도 계속 작동합니다.

프록시 서버

NetApp 명시적 프록시 구성과 투명 프록시 구성을 모두 지원합니다. 투명 프록시를 사용하는 경우 프록시 서버에 대한 인증서만 제공하면 됩니다. 명시적 프록시를 사용하는 경우 IP 주소와 자격 증명도 필요합니다.

- IP 주소
- 신임장
- HTTPS 인증서

포트

Cloud Volumes ONTAP 에서 NetApp 지원팀으로 AutoSupport 메시지를 보내기 위한 프록시로 사용되거나 사용자가 시작하지 않는 한 콘솔 에이전트로 들어오는 트래픽이 없습니다.

- HTTP(80) 및 HTTPS(443)는 로컬 UI에 대한 액세스를 제공하며 이는 드문 상황에서 사용됩니다.
- SSH(22)는 문제 해결을 위해 호스트에 연결해야 하는 경우에만 필요합니다.
- 아웃바운드 인터넷 연결을 사용할 수 없는 서브넷에 Cloud Volumes ONTAP 시스템을 배포하는 경우 포트 3128을 통한 인바운드 연결이 필요합니다.

  Cloud Volumes ONTAP 시스템에 AutoSupport 메시지를 보낼 아웃바운드 인터넷 연결이 없는 경우 콘솔은 콘솔 에이전트에 포함된 프록시 서버를 사용하도록 해당 시스템을 자동으로 구성합니다. 유일한 요구 사항은 콘솔 에이전트의 보안 그룹이 포트 3128을 통한 인바운드 연결을 허용하는 것입니다. 콘솔 에이전트를 배포한 후 이 포트를 열어야 합니다.

NTP 활성화

NetApp Data Classification 사용하여 회사 데이터 소스를 스캔하려는 경우 콘솔 에이전트와 NetApp Data Classification 시스템 모두에서 NTP(네트워크 시간 프로토콜) 서비스를 활성화하여 시스템 간의 시간을 동기화해야 합니다. "NetApp 데이터 분류에 대해 자세히 알아보세요"

콘솔 에이전트를 만든 후 이 네트워크 액세스를 구현합니다.

2단계**: AWS** 권한 설정

마켓플레이스 배포를 준비하려면 AWS에서 IAM 정책을 만들고 이를 IAM 역할에 연결합니다. AWS Marketplace에서 콘솔 에이전트를 생성하면 해당 IAM 역할을 선택하라는 메시지가 표시됩니다.

단계

1. AWS 콘솔에 로그인하고 IAM 서비스로 이동합니다.
2. 정책을 만듭니다.
   a. *정책 > 정책 만들기*를 선택합니다.
   b. *JSON*을 선택하고 내용을 복사하여 붙여넣습니다."콘솔 에이전트에 대한 IAM 정책" .
   c. 나머지 단계를 완료하여 정책을 만듭니다.

   사용하려는 NetApp 데이터 서비스에 따라 두 번째 정책을 만들어야 할 수도 있습니다. 표준 지역의 경우 권한은 두 가지 정책에 걸쳐 분산됩니다. AWS의 관리형 정책에는 최대 문자 크기 제한이 있으므로 두 개의 정책이 필요합니다. "콘솔 에이전트에 대한 IAM 정책에 대해 자세히 알아보세요." .
3. IAM 역할을 만듭니다.
   a. *역할 > 역할 만들기*를 선택합니다.
   b. *AWS 서비스 > EC2*를 선택합니다.
   c. 방금 만든 정책을 첨부하여 권한을 추가합니다.
   d. 나머지 단계를 완료하여 역할을 만듭니다.

결과

이제 AWS Marketplace에서 배포하는 동안 EC2 인스턴스와 연결할 수 있는 IAM 역할이 생겼습니다.

3단계**:** 인스턴스 요구 사항 검토

콘솔 에이전트를 생성할 때 다음 요구 사항을 충족하는 EC2 인스턴스 유형을 선택해야 합니다.

CPU

8개 코어 또는 8개 vCPU

숫양

32GB

AWS EC2 인스턴스 유형

CPU 및 RAM 요구 사항을 충족하는 인스턴스 유형입니다. NetApp t3.2xlarge를 권장합니다.

4단계**:** 콘솔 에이전트 만들기

AWS Marketplace에서 직접 콘솔 에이전트를 만듭니다.

이 작업에 관하여

AWS Marketplace에서 콘솔 에이전트를 생성하면 기본 구성을 사용하여 AWS에 EC2 인스턴스가 배포됩니다. "콘솔 에이전트의 기본 구성에 대해 알아보세요" .

시작하기 전에

다음 사항이 있어야 합니다.

- 네트워킹 요구 사항을 충족하는 VPC 및 서브넷.
- 콘솔 에이전트에 필요한 권한이 포함된 정책이 첨부된 IAM 역할입니다.
- IAM 사용자가 AWS Marketplace를 구독하고 구독을 취소할 수 있는 권한입니다.
- 인스턴스에 필요한 CPU 및 RAM 요구 사항을 이해합니다.
- EC2 인스턴스에 대한 키 쌍입니다.

단계

1. 로 가다 "AWS Marketplace에 NetApp Console 에이전트 목록이 추가되었습니다."
2. 마켓플레이스 페이지에서 *구독 계속하기*를 선택하세요.
3. 소프트웨어를 구독하려면 *약관 동의*를 선택하세요.

   구독 절차는 몇 분 정도 걸릴 수 있습니다.
4. 구독 프로세스가 완료되면 *구성 계속*을 선택하세요.
5. 이 소프트웨어 구성 페이지에서 올바른 지역을 선택했는지 확인한 다음 *계속 실행*을 선택합니다.
6. 이 소프트웨어 실행 페이지의 *작업 선택*에서 *EC2를 통해 실행*을 선택한 다음 *실행*을 선택합니다.

   EC2 콘솔을 사용하여 인스턴스를 시작하고 IAM 역할을 연결합니다. 웹사이트에서 실행 작업에서는 이 작업이 불가능합니다.
7. 프롬프트에 따라 인스턴스를 구성하고 배포하세요.
   - 이름 및 태그: 인스턴스의 이름과 태그를 입력합니다.
   - 애플리케이션 및 **OS** 이미지: 이 섹션을 건너뜁니다. 콘솔 에이전트 AMI가 이미 선택되었습니다.
   - 인스턴스 유형: 지역별 가용성에 따라 RAM 및 CPU 요구 사항을 충족하는 인스턴스 유형을 선택합니다(t3.2xlarge가 미리 선택되어 권장됨).
   - 키 쌍(로그인): 인스턴스에 안전하게 연결하는 데 사용할 키 쌍을 선택하세요.
   - 네트워크 설정: 필요에 따라 네트워크 설정을 편집하세요.
     - 원하는 VPC와 서브넷을 선택하세요.
     - 인스턴스에 공용 IP 주소가 있어야 하는지 여부를 지정합니다.
     - 콘솔 에이전트 인스턴스에 필요한 연결 방법(SSH, HTTP, HTTPS)을 활성화하는 보안 그룹 설정을 지정합니다.

"AWS에 대한 보안 그룹 규칙 보기" .

- 저장소 구성: 루트 볼륨의 기본 크기와 디스크 유형을 유지합니다.

  루트 볼륨에서 Amazon EBS 암호화를 활성화하려면 *고급*을 선택하고 *볼륨 1*을 확장한 다음 *암호화*를 선택하고 KMS 키를 선택합니다.

- 고급 세부 정보: *IAM 인스턴스 프로필*에서 콘솔 에이전트에 필요한 권한이 포함된 IAM 역할을 선택합니다.
- 요약: 요약을 검토하고 *인스턴스 시작*을 선택합니다.

  AWS는 지정된 설정으로 콘솔 에이전트를 시작하고, 콘솔 에이전트는 약 10분 후에 실행됩니다.

  설치에 실패하면 로그와 보고서를 보고 문제 해결에 도움을 받을 수 있습니다."설치 문제를 해결하는 방법을 알아보세요."

8. 콘솔 에이전트 가상 머신에 연결되어 있고 콘솔 에이전트의 URL이 있는 호스트에서 웹 브라우저를 엽니다.
9. 로그인 후 콘솔 에이전트를 설정하세요.
   a. 콘솔 에이전트와 연결할 콘솔 조직을 지정합니다.
   b. 시스템 이름을 입력하세요.
   c. *보안된 환경에서 실행하고 있습니까?*에서 제한 모드를 비활성화하세요.

      표준 모드에서 콘솔을 사용하려면 제한 모드를 비활성화하세요. 보안 환경이 있고 콘솔 백엔드 서비스에서 이 계정의 연결을 끊으려는 경우에만 제한 모드를 활성화해야 합니다. 그렇다면,"제한 모드에서 NetApp Console 시작하기 위한 단계를 따르세요." .

   d. *시작하기*를 선택하세요.

결과

이제 콘솔 에이전트가 설치되고 콘솔 조직에 설정되었습니다.

웹 브라우저를 열고 이동하세요 "NetApp Console" 콘솔과 함께 콘솔 에이전트를 사용하려면 다음을 수행합니다.

콘솔 에이전트를 생성한 동일한 AWS 계정에 Amazon S3 버킷이 있는 경우, 시스템 페이지에 Amazon S3 작업 환경이 자동으로 표시됩니다. "NetApp Console 에서 S3 버킷을 관리하는 방법을 알아보세요."

AWS에 콘솔 에이전트를 수동으로 설치합니다.

AWS에서 실행되는 Linux 호스트에 콘솔 에이전트를 수동으로 설치할 수 있습니다. Linux 호스트에 콘솔 에이전트를 수동으로 설치하려면 호스트 요구 사항을 검토하고, 네트워킹을 설정하고, AWS 권한을 준비하고, 콘솔 에이전트를 설치한 다음, 준비한 권한을 제공해야 합니다.

시작하기 전에

- 당신은 ~을 가져야합니다"콘솔 에이전트에 대한 이해" .
- 검토해야 합니다"콘솔 에이전트 제한 사항" .

1단계**:** 호스트 요구 사항 검토

콘솔 에이전트 소프트웨어가 실행되는 호스트가 운영 체제, RAM 및 포트 요구 사항을 충족하는지 확인하십시오.

콘솔 에이전트는 UID와 GID 범위를 19000~19200으로 예약합니다. 이 범위는 고정되어 있으며 수정할 수 없습니다. 호스트의 타사 소프트웨어가 이 범위 내의 UID나 GID를 사용하는 경우 에이전트 설치가 실패합니다. NetApp 충돌을 피하기 위해 타사 소프트웨어가 없는 호스트를 사용할 것을 권장합니다.

전담 호스트

콘솔 에이전트를 실행하려면 전용 호스트가 필요합니다. 다음의 크기 요건을 충족하는 모든 아키텍처가 지원됩니다.

- CPU: 8개 코어 또는 8개 vCPU
- 램: 32GB
- 디스크 공간: 호스트에 권장되는 디스크 공간은 165GB이며, 다음 파티션 요구 사항이 적용됩니다.
  - `/opt`: 120GiB의 공간이 사용 가능해야 합니다.

    에이전트는 다음을 사용합니다. `/opt` 설치하려면 `/opt/application/netapp` 디렉토리와 그 내용.
  - `/var`: 40GiB의 공간이 사용 가능해야 합니다.

    콘솔 에이전트는 다음 공간이 필요합니다. `/var` Podman이나 Docker는 컨테이너를 이 디렉터리 내에 생성하도록 설계되었기 때문입니다. 구체적으로, 그들은 컨테이너를 생성할 것입니다. `/var/lib/containers/storage` 디렉토리 및 `/var/lib/docker` Docker용입니다. 이 공간에서는 외부 마운트나 심볼릭 링크가 작동하지 않습니다.

AWS EC2 인스턴스 유형

CPU 및 RAM 요구 사항을 충족하는 인스턴스 유형입니다. NetApp t3.2xlarge를 권장합니다.

하이퍼바이저

지원되는 운영 체제를 실행하도록 인증된 베어 메탈 또는 호스팅 하이퍼바이저가 필요합니다.

운영 체제 및 컨테이너 요구 사항

콘솔 에이전트는 표준 모드 또는 제한 모드에서 콘솔을 사용할 때 다음 운영 체제에서 지원됩니다. 에이전트를 설치하기 전에 컨테이너 오케스트레이션 도구가 필요합니다.

운영 체제	지원되는 **OS** 버전	지원되는 에이전트 버전	필수 컨테이너 도구	셀리눅스
레드햇 엔터프라이즈 리눅스		9.6 • 영어 버전만 제공됩니다. • 호스트는 Red Hat Subscription Management에 등록되어야 합니다. 등록되지 않은 경우 호스트는 에이전트 설치 중에 필요한 타사 소프트웨어를 업데이트하기 위해 저장소에 액세스할 수 없습니다.	4.0.0 이상, 콘솔이 표준 모드 또는 제한 모드인 경우	Podman 버전 5.4.0과 podman-compose 1.5.0. Podman 구성 요구 사항 보기 .
강제 모드 또는 허용 모드에서 지원됨		9.1에서 9.4까지 • 영어 버전만 제공됩니다. • 호스트는 Red Hat Subscription Management에 등록되어야 합니다. 등록되지 않은 경우 호스트는 에이전트 설치 중에 필요한 타사 소프트웨어를 업데이트하기 위해 저장소에 액세스할 수 없습니다.	3.9.50 이상, 콘솔이 표준 모드 또는 제한 모드인 경우	Podman 버전 4.9.4와 podman-compose 1.5.0. Podman 구성 요구 사항 보기 .

운영 체제	지원되는 **OS** 버전	지원되는 에이전트 버전	필수 컨테이너 도구	셀리눅스
강제 모드 또는 허용 모드에서 지원됨		8.6에서 8.10까지 • 영어 버전만 제공됩니다. • 호스트는 Red Hat Subscription Management에 등록되어야 합니다. 등록되지 않은 경우 호스트는 에이전트 설치 중에 필요한 타사 소프트웨어를 업데이트하기 위해 저장소에 액세스할 수 없습니다.	3.9.50 이상, 콘솔이 표준 모드 또는 제한 모드인 경우	Podman 버전 4.6.1 또는 4.9.4와 podman-compose 1.0.6. Podman 구성 요구 사항 보기 .
강제 모드 또는 허용 모드에서 지원됨	우분투		24.04 장기	표준 모드 또는 제한 모드에서 NetApp Console 사용하는 3.9.45 이상
Docker 엔진 23.06~28.0.0.	지원되지 않음		22.04 장기	3.9.50 이상

키 쌍

콘솔 에이전트를 생성할 때 인스턴스와 함께 사용할 EC2 키 쌍을 선택해야 합니다.

IMDSv2를 사용할 때 **PUT** 응답 홉 제한

IMDSv2가 활성화된 경우(새 EC2 인스턴스의 기본값) PUT 응답 홉 제한을 3으로 설정하십시오. 그렇게 하지 않으면 에이전트 설정 중에 시스템에 UI 초기화 오류가 표시됩니다.

- "Amazon EC2 인스턴스에서 IMDSv2 사용 요구"
- "AWS 설명서: PUT 응답 홉 제한 변경"

2단계**: Podman** 또는 **Docker Engine** 설치

운영 체제에 따라 에이전트를 설치하기 전에 Podman 또는 Docker Engine이 필요합니다.

- Red Hat Enterprise Linux 8 및 9에는 Podman이 필요합니다.

  지원되는 Podman 버전 보기 .

- Ubuntu에는 Docker 엔진이 필요합니다.

지원되는 Docker Engine 버전 보기 .

예 **1.** 단계

포드만

Podman을 설치하고 구성하려면 다음 단계를 따르세요.

- podman.socket 서비스를 활성화하고 시작합니다.
- python3 설치
- podman-compose 패키지 버전 1.0.6을 설치하세요
- PATH 환경 변수에 podman-compose를 추가합니다.
- Red Hat Enterprise Linux를 사용하는 경우 Podman 버전이 CNI 대신 Netavark Aardvark DNS를 사용하는지 확인하십시오.

DNS 포트 충돌을 피하기 위해 에이전트를 설치한 후 aardvark-dns 포트(기본값: 53)를 조정하세요. 지침에 따라 포트를 구성하세요.

단계

1. 호스트에 podman-docker 패키지가 설치되어 있다면 제거합니다.

```
dnf remove podman-docker
rm /var/run/docker.sock
```

2. Podman을 설치하세요.

   공식 Red Hat Enterprise Linux 저장소에서 Podman을 다운로드할 수 있습니다.

   a. Red Hat Enterprise Linux 9.6의 경우:

   ```
   sudo dnf install podman-5:<version>
   ```

   여기서 <버전>은 설치하려는 Podman의 지원되는 버전입니다. 지원되는 Podman 버전 보기 .

   b. Red Hat Enterprise Linux 9.1~9.4 버전의 경우:

   ```
   sudo dnf install podman-4:<version>
   ```

   여기서 <버전>은 설치하려는 Podman의 지원되는 버전입니다. 지원되는 Podman 버전 보기 .

   c. Red Hat Enterprise Linux 8의 경우:

   ```
   sudo dnf install podman-4:<version>
   ```

   여기서 <버전>은 설치하려는 Podman의 지원되는 버전입니다. 지원되는 Podman 버전 보기 .

3. podman.socket 서비스를 활성화하고 시작합니다.

```
sudo systemctl enable --now podman.socket
```

4. python3를 설치합니다.

```
sudo dnf install python3
```

5. 시스템에 EPEL 저장소 패키지가 아직 없으면 설치하세요.

   이 단계는 podman-compose가 EPEL(Enterprise Linux용 추가 패키지) 저장소에서 사용 가능하기 때문에 필요합니다.

6. Red Hat Enterprise 9를 사용하는 경우:

   a. EPEL 저장소 패키지를 설치하세요.

```
sudo dnf install https://dl.fedoraproject.org/pub/epel/epel-release-latest-9.noarch.rpm
```

   +

   a. podman-compose 패키지 1.5.0을 설치합니다.

```
sudo dnf install podman-compose-1.5.0
```

7. Red Hat Enterprise Linux 8을 사용하는 경우:

   a. EPEL 저장소 패키지를 설치하세요.

```
sudo dnf install https://dl.fedoraproject.org/pub/epel/epel-release-latest-8.noarch.rpm
```

   b. podman-compose 패키지 1.0.6을 설치합니다.

```
sudo dnf install podman-compose-1.0.6
```

> ⓘ 를 사용하여 `dnf install` 명령은 PATH 환경 변수에 podman-compose를 추가하는 요구 사항을 충족합니다. 설치 명령은 이미 포함되어 있는 /usr/bin에 podman-compose를 추가합니다. `secure_path` 호스트의 옵션.

   c. Red Hat Enterprise Linux 8을 사용하는 경우 Podman 버전이 CNI 대신 Aardvark DNS와 함께 NetAvark를 사용하는지 확인하세요.

i. 다음 명령을 실행하여 networkBackend가 CNI로 설정되어 있는지 확인하세요.

```
podman info | grep networkBackend
```

ii. networkBackend가 설정된 경우 `CNI` , 당신은 그것을 변경해야 합니다 `netavark` .

iii. 설치하다 `netavark` 그리고 `aardvark-dns` 다음 명령을 사용합니다.

```
dnf install aardvark-dns netavark
```

iv. 열기 `/etc/containers/containers.conf` 파일을 열고 network_backend 옵션을 "cni" 대신 "netavark"를 사용하도록 수정합니다.

만약에 `/etc/containers/containers.conf` 존재하지 않습니다. 구성을 변경하세요. `/usr/share/containers/containers.conf` .

v. Podman을 다시 시작하세요.

```
systemctl restart podman
```

vi. 다음 명령을 사용하여 networkBackend가 이제 "netavark"로 변경되었는지 확인하세요.

```
podman info | grep networkBackend
```

도커 엔진

Docker Engine을 설치하려면 Docker 설명서를 따르세요.

단계

1. "Docker에서 설치 지침 보기"

   지원되는 Docker Engine 버전을 설치하려면 다음 단계를 따르세요. 콘솔에서 지원되지 않으므로 최신 버전을 설치하지 마세요.

2. Docker가 활성화되어 실행 중인지 확인하세요.

```
sudo systemctl enable docker && sudo systemctl start docker
```

3단계**:** 네트워킹 설정

콘솔 에이전트가 하이브리드 클라우드의 리소스를 관리할 수 있도록 네트워크 위치가 다음 요구 사항을 충족하는지 확인하십시오.

대상 네트워크에 대한 연결

콘솔 에이전트를 사용하려면 시스템을 만들고 관리하려는 위치에 대한 네트워크 연결이 필요합니다. 예를 들어, Cloud Volumes ONTAP 시스템이나 온프레미스 환경의 스토리지 시스템을 만들 계획인 네트워크입니다.

아웃바운드 인터넷 접속

콘솔 에이전트를 배포하는 네트워크 위치에는 특정 엔드포인트에 연결하기 위한 아웃바운드 인터넷 연결이 있어야 합니다.

웹 기반 **NetApp Console** 사용할 때 컴퓨터에서 연결된 엔드포인트

웹 브라우저에서 콘솔에 액세스하는 컴퓨터는 여러 엔드포인트에 접속할 수 있어야 합니다. 콘솔 에이전트를 설정하고 콘솔을 일상적으로 사용하려면 콘솔을 사용해야 합니다.

"NetApp 콘솔을 위한 네트워킹 준비" .

콘솔 에이전트에서 연락한 엔드포인트

콘솔 에이전트는 일상 업무를 위해 퍼블릭 클라우드 환경 내의 리소스와 프로세스를 관리하기 위해 다음 엔드포인트에 연결하기 위해 아웃바운드 인터넷 액세스가 필요합니다.

아래 나열된 엔드포인트는 모두 CNAME 항목입니다.

엔드포인트	목적
AWS 서비스(amazonaws.com): • 클라우드포메이션 • 탄력적 컴퓨팅 클라우드(EC2) • ID 및 액세스 관리(IAM) • 키 관리 서비스(KMS) • 보안 토큰 서비스(STS) • 간편 보관 서비스(S3)	AWS 리소스를 관리합니다. 엔드포인트는 AWS 지역에 따라 달라집니다. "자세한 내용은 AWS 설명서를 참조하세요."
Amazon FsX for NetApp ONTAP: • api.workloads.netapp.com	웹 기반 콘솔은 이 엔드포인트에 연결하여 Workload Factory API와 상호 작용함으로써 ONTAP 기반 워크로드용 FSx를 관리하고 운영합니다.
\ https://mysupport.netapp.com	라이선스 정보를 얻고 NetApp 지원팀에 AutoSupport 메시지를 보냅니다.
\ https://signin.b2c.netapp.com	NetApp 지원 사이트(NSS) 자격 증명을 업데이트하거나 NetApp Console 에 새로운 NSS 자격 증명을 추가합니다.

엔드포인트	목적
\ https://support.netapp.com	라이선스 정보를 얻고 NetApp 지원팀에 AutoSupport 메시지를 보내고 Cloud Volumes ONTAP 에 대한 소프트웨어 업데이트를 받습니다.
\ https://api.bluexp.netapp.com \ https://netapp-cloud-account.auth0.com \ https://netapp-cloud-account.us.auth0.com \ https://console.netapp.com \ https://components.console.bluexp.netapp.com \ https://cdn.auth0.com	NetApp Console 내에서 기능과 서비스를 제공합니다.
\ https://bluexpinfraprod.eastus2.data.azurecr.io \ https://bluexpinfraprod.azurecr.io	콘솔 에이전트 업그레이드를 위한 이미지를 얻으려면. • 새로운 에이전트를 배포할 때 유효성 검사를 통해 현재 엔드포인트에 대한 연결성을 테스트합니다. 당신이 사용하는 경우"이전 종료점" , 유효성 검사에 실패합니다. 이러한 실패를 방지하려면 유효성 검사를 건너뛰세요. 이전 엔드포인트는 계속 지원되지만 NetApp 가능한 한 빨리 현재 엔드포인트에 맞게 방화벽 규칙을 업데이트할 것을 권장합니다. "엔드포인트 목록을 업데이트하는 방법을 알아보세요" . • 방화벽의 현재 엔드포인트로 업데이트하면 기존 에이전트도 계속 작동합니다.

프록시 서버

NetApp 명시적 프록시 구성과 투명 프록시 구성을 모두 지원합니다. 투명 프록시를 사용하는 경우 프록시 서버에 대한 인증서만 제공하면 됩니다. 명시적 프록시를 사용하는 경우 IP 주소와 자격 증명도 필요합니다.

- IP 주소
- 신임장
- HTTPS 인증서

포트

Cloud Volumes ONTAP 에서 NetApp 지원팀으로 AutoSupport 메시지를 보내기 위한 프록시로 사용되거나 사용자가 시작하지 않는 한 콘솔 에이전트로 들어오는 트래픽이 없습니다.

- HTTP(80) 및 HTTPS(443)는 로컬 UI에 대한 액세스를 제공하며 이는 드문 상황에서 사용됩니다.
- SSH(22)는 문제 해결을 위해 호스트에 연결해야 하는 경우에만 필요합니다.
- 아웃바운드 인터넷 연결을 사용할 수 없는 서브넷에 Cloud Volumes ONTAP 시스템을 배포하는 경우 포트 3128을 통한 인바운드 연결이 필요합니다.

  Cloud Volumes ONTAP 시스템에 AutoSupport 메시지를 보낼 아웃바운드 인터넷 연결이 없는 경우 콘솔은 콘솔 에이전트에 포함된 프록시 서버를 사용하도록 해당 시스템을 자동으로 구성합니다. 유일한 요구 사항은 콘솔 에이전트의 보안 그룹이 포트 3128을 통한 인바운드 연결을 허용하는 것입니다. 콘솔 에이전트를 배포한 후 이 포트를 열어야 합니다.

NTP 활성화

NetApp Data Classification 사용하여 회사 데이터 소스를 스캔하려는 경우 콘솔 에이전트와 NetApp Data Classification 시스템 모두에서 NTP(네트워크 시간 프로토콜) 서비스를 활성화하여 시스템 간의 시간을 동기화해야 합니다. "NetApp 데이터 분류에 대해 자세히 알아보세요"

4단계**:** 콘솔에 대한 **AWS** 권한 설정

다음 옵션 중 하나를 사용하여 NetApp Console 에 AWS 권한을 부여하십시오.

- 옵션 1: IAM 정책을 만들고 EC2 인스턴스와 연결할 수 있는 IAM 역할에 정책을 연결합니다.
- 옵션 2: 필요한 권한이 있는 IAM 사용자의 AWS 액세스 키를 콘솔에 제공합니다.

콘솔에 대한 권한을 준비하려면 다음 단계를 따르세요.

IAM 역할

단계

1. AWS 콘솔에 로그인하고 IAM 서비스로 이동합니다.
2. 정책을 만듭니다.
   a. *정책 > 정책 만들기*를 선택합니다.
   b. *JSON*을 선택하고 내용을 복사하여 붙여넣습니다."콘솔 에이전트에 대한 IAM 정책" .
   c. 나머지 단계를 완료하여 정책을 만듭니다.

      사용하려는 NetApp 데이터 서비스에 따라 두 번째 정책을 만들어야 할 수도 있습니다. 표준 지역의 경우 권한은 두 가지 정책에 걸쳐 분산됩니다. AWS의 관리형 정책에는 최대 문자 크기 제한이 있으므로 두 개의 정책이 필요합니다. "콘솔 에이전트에 대한 IAM 정책에 대해 자세히 알아보세요." .
3. IAM 역할을 만듭니다.
   a. *역할 > 역할 만들기*를 선택합니다.
   b. *AWS 서비스 > EC2*를 선택합니다.
   c. 방금 만든 정책을 첨부하여 권한을 추가합니다.
   d. 나머지 단계를 완료하여 역할을 만듭니다.

결과

콘솔 에이전트를 설치한 후 이제 EC2 인스턴스와 연결할 수 있는 IAM 역할이 생겼습니다.

AWS 액세스 키

단계

1. AWS 콘솔에 로그인하고 IAM 서비스로 이동합니다.
2. 정책을 만듭니다.
   a. *정책 > 정책 만들기*를 선택합니다.
   b. *JSON*을 선택하고 내용을 복사하여 붙여넣습니다."콘솔 에이전트에 대한 IAM 정책" .
   c. 나머지 단계를 완료하여 정책을 만듭니다.

      사용하려는 NetApp 데이터 서비스에 따라 두 번째 정책을 만들어야 할 수도 있습니다.

   표준 지역의 경우 권한은 두 가지 정책에 걸쳐 분산됩니다. AWS의 관리형 정책에는 최대 문자 크기 제한이 있으므로 두 개의 정책이 필요합니다. "콘솔 에이전트에 대한 IAM 정책에 대해 자세히 알아보세요." .
3. IAM 사용자에게 정책을 연결합니다.
   - "AWS 설명서: IAM 역할 생성"
   - "AWS 설명서: IAM 정책 추가 및 제거"
4. 콘솔 에이전트를 설치한 후 NetApp Console 에 추가할 수 있는 액세스 키가 사용자에게 있는지 확인하세요.

결과

이제 필요한 권한이 있는 IAM 사용자와 콘솔에 제공할 수 있는 액세스 키가 생겼습니다.

5단계**:** 콘솔 에이전트 설치

필수 조건을 모두 충족한 후에는 Linux 호스트에 소프트웨어를 수동으로 설치하십시오.

시작하기 전에

다음 사항이 있어야 합니다.

- 콘솔 에이전트를 설치하려면 루트 권한이 필요합니다.
- 콘솔 에이전트에서 인터넷에 접속하는 데 프록시가 필요한 경우 프록시 서버에 대한 세부 정보입니다.

  설치 후 프록시 서버를 구성할 수 있지만, 그렇게 하려면 콘솔 에이전트를 다시 시작해야 합니다.

- 프록시 서버가 HTTPS를 사용하거나 프록시가 가로채기 프록시인 경우 CA 서명 인증서가 필요합니다.

콘솔 에이전트를 수동으로 설치하는 경우 투명 프록시 서버에 대한 인증서를 설정할 수 없습니다. 투명 프록시 서버에 대한 인증서를 설정해야 하는 경우 설치 후 유지 관리 콘솔을 사용해야 합니다. 자세히 알아보세요"에이전트 유지 관리 콘솔" .

이 작업에 관하여

설치 후, 새로운 버전이 나오면 콘솔 에이전트가 자동으로 업데이트됩니다.

단계

1. 호스트에 *http_proxy* 또는 *https_proxy* 시스템 변수가 설정되어 있으면 제거합니다.

   ```
   unset http_proxy
   unset https_proxy
   ```

   이러한 시스템 변수를 제거하지 않으면 설치가 실패합니다.

2. 콘솔 에이전트 소프트웨어를 다운로드한 다음 Linux 호스트에 복사하십시오. NetApp Console 또는 NetApp 지원 사이트에서 다운로드할 수 있습니다.
   - NetApp Console: *에이전트 > 관리 > 에이전트 배포 > 온프레미스 > 수동 설치*로 이동합니다.

     에이전트 설치 파일 다운로드 또는 파일 URL 다운로드를 선택하십시오.

   - NetApp 지원 사이트 (콘솔에 대한 액세스 권한이 없는 경우 필요) "NetApp 지원 사이트" ,
3. 스크립트를 실행할 수 있는 권한을 할당합니다.

   ```
   chmod +x NetApp_Console_Agent_Cloud_<version>
   ```

   여기서 <버전>은 다운로드한 콘솔 에이전트의 버전입니다.

4. 정부 클라우드 환경에 설치하는 경우 구성 검사를 비활성화하세요."수동 설치에 대한 구성 검사를 비활성화하는 방법을 알아보세요."
5. 설치 스크립트를 실행합니다.

```
./NetApp_Console_Agent_Cloud_<version> --proxy <HTTP or HTTPS proxy
server> --cacert <path and file name of a CA-signed certificate>
```

네트워크에서 인터넷 접속을 위해 프록시가 필요한 경우 프록시 정보를 추가해야 합니다. 설치 중에 명시적 프록시를 추가할 수 있습니다. `--proxy` 및 `--cacert` 매개변수는 선택 사항이며 추가하라는 메시지가 표시되지 않습니다. 명시적 프록시 서버가 있는 경우 표시된 대로 매개변수를 입력해야 합니다.

투명 프록시를 구성하려면 설치 후에 구성하면 됩니다. "에이전트 유지 관리 콘솔에 대해 알아보세요"

+

다음은 CA 서명 인증서로 명시적 프록시 서버를 구성하는 예입니다.

+

```
./NetApp_Console_Agent_Cloud_v4.0.0--proxy
https://user:password@10.0.0.30:8080/ --cacert /tmp/cacert/certificate.cer
```

+
`--proxy` 다음 형식 중 하나를 사용하여 Console 에이전트가 HTTP 또는 HTTPS 프록시 서버를 사용하도록 구성합니다.

+ * http://address:port * http://user-name:password@address:port * http://domain-name%92user-name:password@address:port * https://address:port * https://user-name:password@address:port * https://domain-name%92user-name:password@address:port

+ 다음 사항에 유의하십시오:

+ 사용자는 로컬 사용자 또는 도메인 사용자일 수 있습니다. 도메인 사용자의 경우 위와 같이 \의 ASCII 코드를 사용해야 합니다. **Console** 에이전트는 **@** 문자가 포함된 사용자 이름이나 암호를 지원하지 않습니다. 암호에 다음 특수 문자(& 또는 !)가 포함된 경우 백슬래시를 앞에 붙여 해당 특수 문자를 이스케이프해야 합니다.

+ 예를 들면:

+ http://bxpproxyuser:netapp1\!@address:3128

1. Podman을 사용한 경우 aardvark-dns 포트를 조정해야 합니다.

   a. 콘솔 에이전트 가상 머신에 SSH를 실행합니다.

   b. podman */usr/share/containers/containers.conf* 파일을 열고 Aardvark DNS 서비스에 대해 선택한 포트를 수정합니다. 예를 들어, 54로 변경합니다.

      ```
      vi /usr/share/containers/containers.conf
      ```

      예를 들어:

```
# Port to use for dns forwarding daemon with netavark in rootful bridge
# mode and dns enabled.
# Using an alternate port might be useful if other DNS services should
# run on the machine.
#
dns_bind_port = 54
```

a. 콘솔 에이전트 가상 머신을 재부팅합니다.

2. 설치가 완료될 때까지 기다리세요.

설치가 끝나면 프록시 서버를 지정한 경우 콘솔 에이전트 서비스(occm)가 두 번 다시 시작됩니다.

설치에 실패하면 설치 보고서와 로그를 보고 문제를 해결하는 데 도움이 됩니다."설치 문제를 해결하는 방법을 알아보세요."

1. 콘솔 에이전트 가상 머신에 연결된 호스트에서 웹 브라우저를 열고 다음 URL을 입력합니다.

https://ipaddress

2. 로그인 후 콘솔 에이전트를 설정하세요.

a. 콘솔 에이전트와 연결할 조직을 지정합니다.

b. 시스템 이름을 입력하세요.

c. *보안된 환경에서 실행하고 있습니까?*에서 제한 모드를 비활성화하세요.

이 단계에서는 표준 모드에서 콘솔을 사용하는 방법을 설명하므로 제한 모드를 비활성화해야 합니다. 보안 환경이 있고 백엔드 서비스에서 이 계정의 연결을 끊으려는 경우에만 제한 모드를 활성화해야 합니다. 그렇다면 ,"제한 모드에서 NetApp Console 시작하기 위한 단계를 따르세요." .

d. *시작하기*를 선택하세요.

콘솔 에이전트를 생성한 동일한 AWS 계정에 Amazon S3 버킷이 있는 경우, 시스템 페이지에 Amazon S3 스토리지 시스템이 자동으로 표시됩니다. "NetApp ConsoleP에서 S3 버킷을 관리하는 방법을 알아보세요."

6단계**: NetApp Console** 에 권한 제공

콘솔 에이전트를 설치한 후에는 콘솔 에이전트가 AWS에서 데이터 및 스토리지 인프라를 관리할 수 있도록 설정한 AWS 권한을 제공해야 합니다.

IAM 역할

생성한 IAM 역할을 콘솔 에이전트 EC2 인스턴스에 연결합니다.

단계

1. Amazon EC2 콘솔로 이동합니다.
2. *인스턴스*를 선택하세요.
3. 콘솔 에이전트 인스턴스를 선택합니다.
4. *작업 > 보안 > IAM 역할 수정*을 선택합니다.
5. IAM 역할을 선택하고 *IAM 역할 업데이트*를 선택합니다.

로 가다 "NetApp Console" 콘솔 에이전트를 사용하려면.

AWS 액세스 키

필요한 권한이 있는 IAM 사용자의 AWS 액세스 키를 콘솔에 제공합니다.

단계

1. 콘솔에서 현재 올바른 콘솔 에이전트가 선택되어 있는지 확인하세요.
2. *관리 > 자격 증명*을 선택합니다.
3. *조직 자격 증명*을 선택하세요.
4. *자격 증명 추가*를 선택하고 마법사의 단계를 따르세요.
   a. 자격 증명 위치: *Amazon Web Services > 에이전트를 선택하세요.
   b. 자격 증명 정의: AWS 액세스 키와 비밀 키를 입력합니다.
   c. 마켓플레이스 구독: 지금 구독하거나 기존 구독을 선택하여 마켓플레이스 구독을 이러한 자격 증명과 연결합니다.
   d. 검토: 새로운 자격 증명에 대한 세부 정보를 확인하고 *추가*를 선택합니다.

로 가다 "NetApp Console" 콘솔 에이전트를 사용하려면.

하늘빛

Azure의 콘솔 에이전트 설치 옵션

Azure에서 콘솔 에이전트를 만드는 방법에는 여러 가지가 있습니다. 가장 일반적인 방법은 NetApp Console 에서 직접 실행하는 것입니다.

다음과 같은 설치 옵션을 사용할 수 있습니다.

- "NetApp Console 에서 직접 콘솔 에이전트를 만듭니다."(이것은 표준 옵션입니다)

  이 작업을 수행하면 선택한 VNet에서 Linux와 콘솔 에이전트 소프트웨어를 실행하는 VM이 시작됩니다.

- "Azure Marketplace에서 콘솔 에이전트 만들기"

이 작업을 수행하면 Linux와 콘솔 에이전트 소프트웨어가 실행되는 VM도 시작되지만 배포는 콘솔이 아닌 Azure Marketplace에서 직접 시작됩니다.

- "자신의 Linux 호스트에 소프트웨어를 다운로드하고 수동으로 설치하세요."

선택하는 설치 옵션은 설치를 준비하는 방법에 영향을 미칩니다. 여기에는 Azure에서 리소스를 인증하고 관리하는 데 필요한 권한을 콘솔 에이전트에 제공하는 방법이 포함됩니다.

NetApp Console 에서 **Azure**에 콘솔 에이전트 만들기

NetApp Console 에서 Azure에 콘솔 에이전트를 만들려면 네트워킹을 설정하고, Azure 권한을 준비한 다음 콘솔 에이전트를 만들어야 합니다.

시작하기 전에

- 당신은 ~을 가져야합니다"콘솔 에이전트에 대한 이해" .
- 검토해야 합니다"콘솔 에이전트 제한 사항" .

1단계**:** 네트워킹 설정

콘솔 에이전트를 설치하려는 네트워크 위치가 다음 요구 사항을 지원하는지 확인하세요. 이러한 요구 사항을 통해 콘솔 에이전트는 하이브리드 클라우드 리소스를 관리할 수 있습니다.

Azure 지역

Cloud Volumes ONTAP 사용하는 경우 콘솔 에이전트는 관리하는 Cloud Volumes ONTAP 시스템과 동일한 Azure 지역이나 "Azure 지역 쌍" Cloud Volumes ONTAP 시스템용. 이 요구 사항은 Cloud Volumes ONTAP 과 연결된 스토리지 계정 간에 Azure Private Link 연결이 사용되도록 보장합니다.

"Cloud Volumes ONTAP Azure Private Link를 사용하는 방법 알아보기"

VNet 및 서브넷

콘솔 에이전트를 만들 때는 에이전트가 상주해야 하는 VNet과 서브넷을 지정해야 합니다.

대상 네트워크에 대한 연결

콘솔 에이전트를 사용하려면 시스템을 만들고 관리하려는 위치에 대한 네트워크 연결이 필요합니다. 예를 들어, Cloud Volumes ONTAP 시스템이나 온프레미스 환경의 스토리지 시스템을 만들 계획인 네트워크입니다.

아웃바운드 인터넷 접속

콘솔 에이전트를 배포하는 네트워크 위치에는 특정 엔드포인트에 연결하기 위한 아웃바운드 인터넷 연결이 있어야 합니다.

콘솔 에이전트에서 연락한 엔드포인트

콘솔 에이전트는 일상 업무를 위해 퍼블릭 클라우드 환경 내의 리소스와 프로세스를 관리하기 위해 다음 엔드포인트에 연결하기 위해 아웃바운드 인터넷 액세스가 필요합니다.

아래 나열된 엔드포인트는 모두 CNAME 항목입니다.

엔드포인트	목적
\ https://management.azure.com \ https://login.microsoftonline.com \ https://blob.core.windows.net \ https://core.windows.net	Azure 공용 지역의 리소스를 관리합니다.
\ https://management.chinacloudapi.cn \ https://login.chinacloudapi.cn \ https://blob.core.chinacloudapi.cn \ https://core.chinacloudapi.cn	Azure China 지역의 리소스를 관리합니다.
\ https://mysupport.netapp.com	라이선스 정보를 얻고 NetApp 지원팀에 AutoSupport 메시지를 보냅니다.
\ https://signin.b2c.netapp.com	NetApp 지원 사이트(NSS) 자격 증명을 업데이트하거나 NetApp Console 에 새로운 NSS 자격 증명을 추가합니다.
\ https://support.netapp.com	라이선스 정보를 얻고 NetApp 지원팀에 AutoSupport 메시지를 보내고 Cloud Volumes ONTAP 에 대한 소프트웨어 업데이트를 받습니다.
\ https://api.bluexp.netapp.com \ https://netapp-cloud-account.auth0.com \ https://netapp-cloud-account.us.auth0.com \ https://console.netapp.com \ https://components.console.bluexp.netapp.com \ https://cdn.auth0.com	NetApp Console 내에서 기능과 서비스를 제공합니다.

엔드포인트	목적
\ https://bluexpinfraprod.eastus2.data.azurecr.io \ https://bluexpinfraprod.azurecr.io	콘솔 에이전트 업그레이드를 위한 이미지를 얻으려면. • 새로운 에이전트를 배포할 때 유효성 검사를 통해 현재 엔드포인트에 대한 연결성을 테스트합니다. 당신이 사용하는 경우"이전 종료점" , 유효성 검사에 실패합니다. 이러한 실패를 방지하려면 유효성 검사를 건너뛰세요. 이전 엔드포인트는 계속 지원되지만 NetApp 가능한 한 빨리 현재 엔드포인트에 맞게 방화벽 규칙을 업데이트할 것을 권장합니다. "엔드포인트 목록을 업데이트하는 방법을 알아보세요" . • 방화벽의 현재 엔드포인트로 업데이트하면 기존 에이전트도 계속 작동합니다.

NetApp 콘솔에서 연결된 엔드포인트

SaaS 계층을 통해 제공되는 웹 기반 NetApp Console 사용하면 여러 엔드포인트에 연결하여 데이터 관리 작업을 완료할 수 있습니다. 여기에는 콘솔에서 콘솔 에이전트를 배포하기 위해 연결된 엔드포인트가 포함됩니다.

"NetApp 콘솔에서 연결된 엔드포인트 목록 보기" .

프록시 서버

NetApp 명시적 프록시 구성과 투명 프록시 구성을 모두 지원합니다. 투명 프록시를 사용하는 경우 프록시 서버에 대한 인증서만 제공하면 됩니다. 명시적 프록시를 사용하는 경우 IP 주소와 자격 증명도 필요합니다.

- IP 주소
- 신임장
- HTTPS 인증서

포트

Cloud Volumes ONTAP 에서 NetApp 지원팀으로 AutoSupport 메시지를 보내기 위한 프록시로 사용되거나 사용자가 시작하지 않는 한 콘솔 에이전트로 들어오는 트래픽이 없습니다.

- HTTP(80) 및 HTTPS(443)는 로컬 UI에 대한 액세스를 제공하며 이는 드문 상황에서 사용됩니다.
- SSH(22)는 문제 해결을 위해 호스트에 연결해야 하는 경우에만 필요합니다.
- 아웃바운드 인터넷 연결을 사용할 수 없는 서브넷에 Cloud Volumes ONTAP 시스템을 배포하는 경우 포트 3128을 통한 인바운드 연결이 필요합니다.

Cloud Volumes ONTAP 시스템에 AutoSupport 메시지를 보낼 아웃바운드 인터넷 연결이 없는 경우 콘솔은 콘솔 에이전트에 포함된 프록시 서버를 사용하도록 해당 시스템을 자동으로 구성합니다. 유일한 요구 사항은 콘솔 에이전트의 보안 그룹이 포트 3128을 통한 인바운드 연결을 허용하는 것입니다. 콘솔 에이전트를 배포한 후 이 포트를 열어야 합니다.

NTP 활성화

NetApp Data Classification 사용하여 회사 데이터 소스를 스캔하려는 경우 콘솔 에이전트와 NetApp Data Classification 시스템 모두에서 NTP(네트워크 시간 프로토콜) 서비스를 활성화하여 시스템 간의 시간을 동기화해야 합니다. "NetApp 데이터 분류에 대해 자세히 알아보세요"

콘솔 에이전트를 만든 후 이 네트워킹 요구 사항을 구현해야 합니다.

2단계**:** 콘솔 에이전트 배포 정책**(**사용자 지정 역할**)** 만들기

Azure에서 콘솔 에이전트를 배포할 수 있는 권한이 있는 사용자 지정 역할을 만들어야 합니다.

Azure 계정이나 Microsoft Entra 서비스 주체에 할당할 수 있는 Azure 사용자 지정 역할을 만듭니다. 콘솔은 Azure에 인증하고 이러한 권한을 사용하여 사용자를 대신하여 콘솔 에이전트를 만듭니다.

콘솔은 Azure에 콘솔 에이전트 VM을 배포하고 다음을 활성화합니다. "시스템 할당 관리 ID" , 필요한 역할을 생성하고 이를 VM에 할당합니다. "콘솔이 권한을 사용하는 방식을 검토하세요." .

Azure Portal, Azure PowerShell, Azure CLI 또는 REST API를 사용하여 Azure 사용자 지정 역할을 만들 수 있습니다. 다음 단계에서는 Azure CLI를 사용하여 역할을 만드는 방법을 보여줍니다. 다른 방법을 사용하려면 다음을 참조하세요. "Azure 설명서"

단계

1. Azure에서 새로운 사용자 지정 역할에 필요한 권한을 복사하여 JSON 파일에 저장합니다.

이 사용자 지정 역할에는 콘솔에서 Azure의 콘솔 에이전트 VM을 시작하는 데 필요한 권한만 포함되어 있습니다. 다른 상황에서는 이 정책을 사용하지 마세요. 콘솔에서 콘솔 에이전트를 만들면 콘솔 에이전트 VM에 새로운 권한 집합이 적용되어 콘솔 에이전트가 Azure 리소스를 관리할 수 있게 됩니다.

```
{
  "Name": "Azure SetupAsService",
  "Actions": [
    "Microsoft.Compute/disks/delete",
    "Microsoft.Compute/disks/read",
    "Microsoft.Compute/disks/write",
    "Microsoft.Compute/locations/operations/read",
    "Microsoft.Compute/operations/read",
    "Microsoft.Compute/virtualMachines/instanceView/read",
    "Microsoft.Compute/virtualMachines/read",
    "Microsoft.Compute/virtualMachines/write",
    "Microsoft.Compute/virtualMachines/delete",
    "Microsoft.Compute/virtualMachines/extensions/write",
    "Microsoft.Compute/virtualMachines/extensions/read",
    "Microsoft.Compute/availabilitySets/read",
```

```
    "Microsoft.Network/locations/operationResults/read",
    "Microsoft.Network/locations/operations/read",
    "Microsoft.Network/networkInterfaces/join/action",
    "Microsoft.Network/networkInterfaces/read",
    "Microsoft.Network/networkInterfaces/write",
    "Microsoft.Network/networkInterfaces/delete",
    "Microsoft.Network/networkSecurityGroups/join/action",
    "Microsoft.Network/networkSecurityGroups/read",
    "Microsoft.Network/networkSecurityGroups/write",
    "Microsoft.Network/virtualNetworks/checkIpAddressAvailability/read",
    "Microsoft.Network/virtualNetworks/read",
    "Microsoft.Network/virtualNetworks/subnets/join/action",
    "Microsoft.Network/virtualNetworks/subnets/read",
    "Microsoft.Network/virtualNetworks/subnets/virtualMachines/read",
    "Microsoft.Network/virtualNetworks/virtualMachines/read",
    "Microsoft.Network/publicIPAddresses/write",
    "Microsoft.Network/publicIPAddresses/read",
    "Microsoft.Network/publicIPAddresses/delete",
    "Microsoft.Network/networkSecurityGroups/securityRules/read",
    "Microsoft.Network/networkSecurityGroups/securityRules/write",
    "Microsoft.Network/networkSecurityGroups/securityRules/delete",
    "Microsoft.Network/publicIPAddresses/join/action",

"Microsoft.Network/locations/virtualNetworkAvailableEndpointServices/rea
d",
    "Microsoft.Network/networkInterfaces/ipConfigurations/read",
    "Microsoft.Resources/deployments/operations/read",
    "Microsoft.Resources/deployments/read",
    "Microsoft.Resources/deployments/delete",
    "Microsoft.Resources/deployments/cancel/action",
    "Microsoft.Resources/deployments/validate/action",
    "Microsoft.Resources/resources/read",
    "Microsoft.Resources/subscriptions/operationresults/read",
    "Microsoft.Resources/subscriptions/resourceGroups/delete",
    "Microsoft.Resources/subscriptions/resourceGroups/read",
    "Microsoft.Resources/subscriptions/resourcegroups/resources/read",
    "Microsoft.Resources/subscriptions/resourceGroups/write",
    "Microsoft.Authorization/roleDefinitions/write",
    "Microsoft.Authorization/roleAssignments/write",

"Microsoft.MarketplaceOrdering/offertypes/publishers/offers/plans/agreem
ents/read",

"Microsoft.MarketplaceOrdering/offertypes/publishers/offers/plans/agreem
ents/write",
    "Microsoft.Network/networkSecurityGroups/delete",
```

```
        "Microsoft.Storage/storageAccounts/delete",
        "Microsoft.Storage/storageAccounts/write",
        "Microsoft.Resources/deployments/write",
        "Microsoft.Resources/deployments/operationStatuses/read",
        "Microsoft.Authorization/roleAssignments/read"
    ],
    "NotActions": [],
    "AssignableScopes": [],
    "Description": "Azure SetupAsService",
    "IsCustom": "true"
}
```

2. 할당 가능한 범위에 Azure 구독 ID를 추가하여 JSON을 수정합니다.

   예

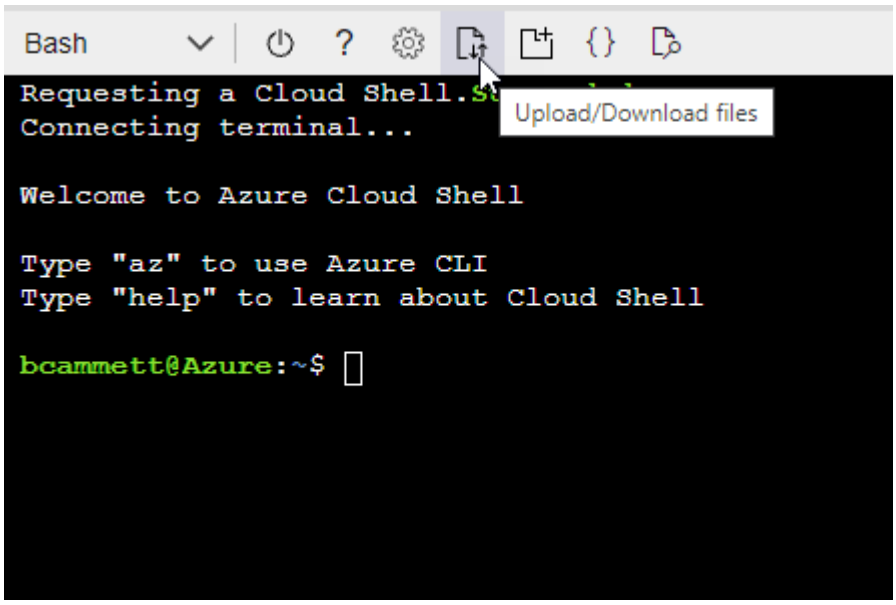
```
"AssignableScopes": [
"/subscriptions/d333af45-0d07-4154-943d-c25fbzzzzzzz"
]
```

3. JSON 파일을 사용하여 Azure에서 사용자 지정 역할을 만듭니다.

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

   a. 시작 "Azure 클라우드 셸" Bash 환경을 선택하세요.

   b. JSON 파일을 업로드합니다.



   c. 다음 Azure CLI 명령을 입력하세요.

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

이제 _Azure SetupAsService_라는 사용자 지정 역할이 생겼습니다. 이 사용자 지정 역할은 사용자 계정이나 서비스 주체에 적용할 수 있습니다.

3단계**:** 인증 설정

콘솔에서 콘솔 에이전트를 만들 때 콘솔이 Azure에 인증하고 VM을 배포할 수 있도록 하는 로그인을 제공해야 합니다. 두 가지 옵션이 있습니다.

1. 메시지가 표시되면 Azure 계정으로 Sign in . 이 계정에는 특정 Azure 권한이 있어야 합니다. 이는 기본 옵션입니다.
2. Microsoft Entra 서비스 주체에 대한 세부 정보를 제공합니다. 이 서비스 주체에도 특정 권한이 필요합니다.

콘솔에서 사용할 인증 방법 중 하나를 준비하려면 다음 단계를 따르세요.

Azure 계정

콘솔에서 콘솔 에이전트를 배포할 사용자에게 사용자 지정 역할을 할당합니다.

단계

1. Azure Portal에서 구독 서비스를 열고 사용자의 구독을 선택합니다.
2. *액세스 제어(IAM)*를 클릭합니다.
3. 추가 > *역할 할당 추가*를 클릭한 다음 권한을 추가합니다.
   a. **Azure SetupAsService** 역할을 선택하고 *다음*을 클릭합니다.

      Azure SetupAsService는 Azure의 콘솔 에이전트 배포 정책에 제공된 기본 이름입니다. 역할에 다른 이름을 선택한 경우 해당 이름을 대신 선택하세요.

   b. *사용자, 그룹 또는 서비스 주체*를 선택된 상태로 유지합니다.
   c. *멤버 선택*을 클릭하고 사용자 계정을 선택한 후 *선택*을 클릭합니다.
   d. *다음*을 클릭하세요.
   e. *검토 + 할당*을 클릭하세요.

서비스 주체

Azure 계정으로 로그인하는 대신, 필요한 권한이 있는 Azure 서비스 주체의 자격 증명을 콘솔에 제공할 수 있습니다.

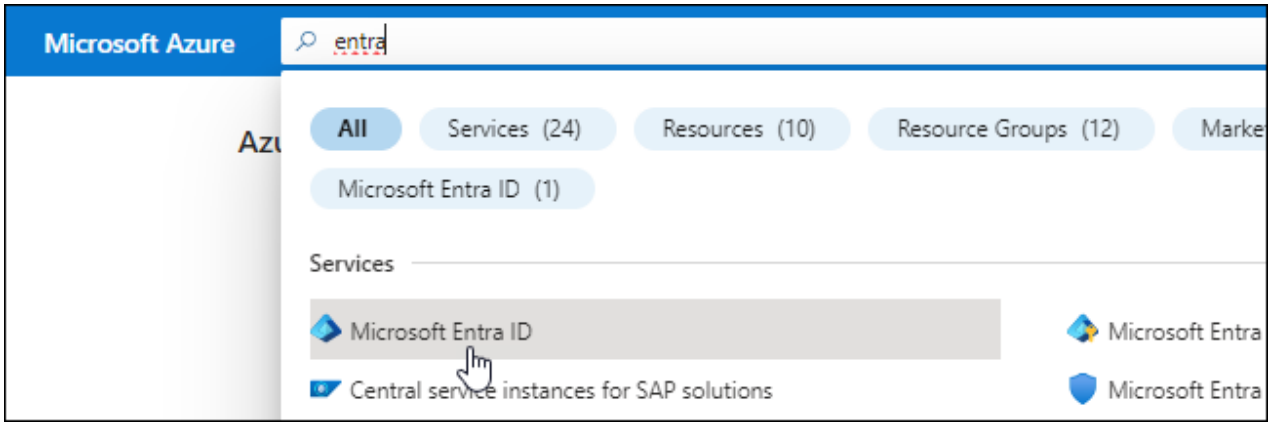
Microsoft Entra ID에서 서비스 주체를 만들고 설정하고 콘솔에 필요한 Azure 자격 증명을 얻습니다.

역할 기반 액세스 제어를 위한 **Microsoft Entra** 애플리케이션 만들기

1. Azure에서 Active Directory 애플리케이션을 만들고 해당 애플리케이션에 역할을 할당할 수 있는 권한이 있는지 확인하세요.

   자세한 내용은 다음을 참조하세요. "Microsoft Azure 설명서: 필요한 권한"

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



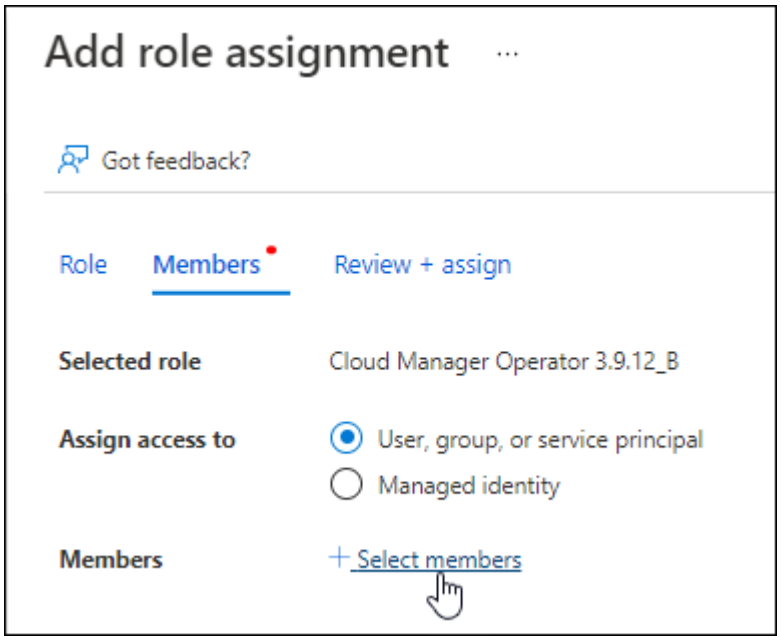
3. 메뉴에서 *앱 등록*을 선택하세요.
4. *신규 등록*을 선택하세요.

5. 신청서에 대한 세부 사항을 지정하세요:
   - 이름: 애플리케이션의 이름을 입력하세요.
   - 계정 유형: 계정 유형을 선택하세요(모든 계정 유형이 NetApp Console 에서 작동합니다).
   - 리디렉션 **URI**: 이 필드는 비워두어도 됩니다.
6. *등록*을 선택하세요.

   AD 애플리케이션과 서비스 주체를 생성했습니다.

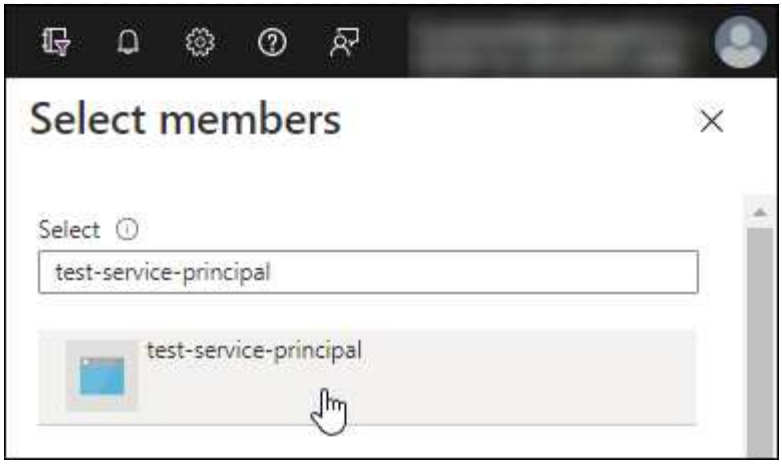
애플리케이션에 사용자 정의 역할 할당

1. Azure Portal에서 구독 서비스를 엽니다.
2. 구독을 선택하세요.
3. *액세스 제어(IAM) > 추가 > 역할 할당 추가*를 클릭합니다.
4. 역할 탭에서 콘솔 운영자 역할을 선택하고 *다음*을 클릭합니다.
5. 멤버 탭에서 다음 단계를 완료하세요.
   a. *사용자, 그룹 또는 서비스 주체*를 선택된 상태로 유지합니다.
   b. *멤버 선택*을 클릭하세요.



   c. 애플리케이션 이름을 검색하세요.

      예를 들면 다음과 같습니다.



a. 해당 애플리케이션을 선택하고 *선택*을 클릭하세요.

b. *다음*을 클릭하세요.

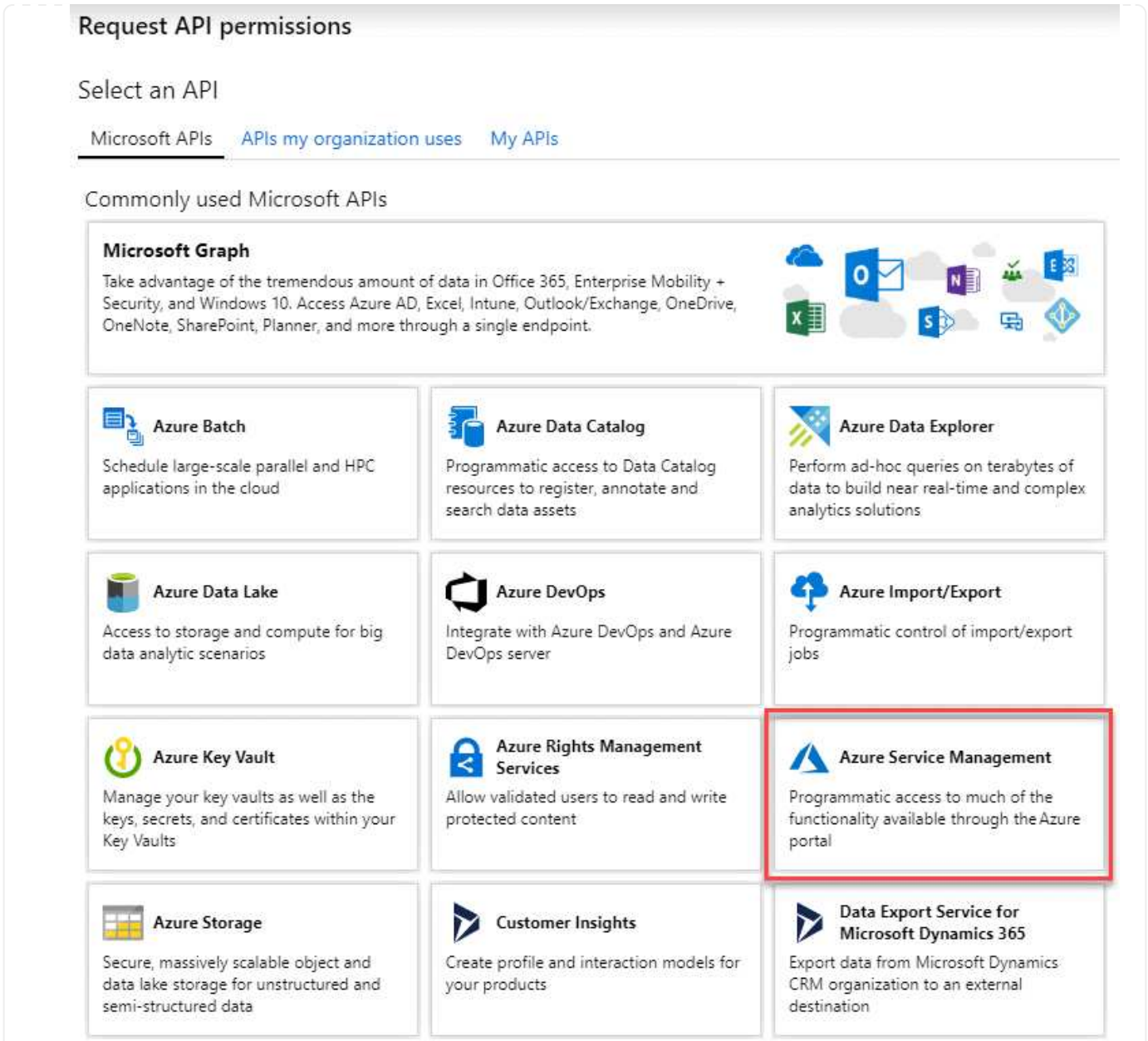
6. *검토 + 할당*을 클릭하세요.

   이제 서비스 주체는 콘솔 에이전트를 배포하는 데 필요한 Azure 권한을 갖게 되었습니다.

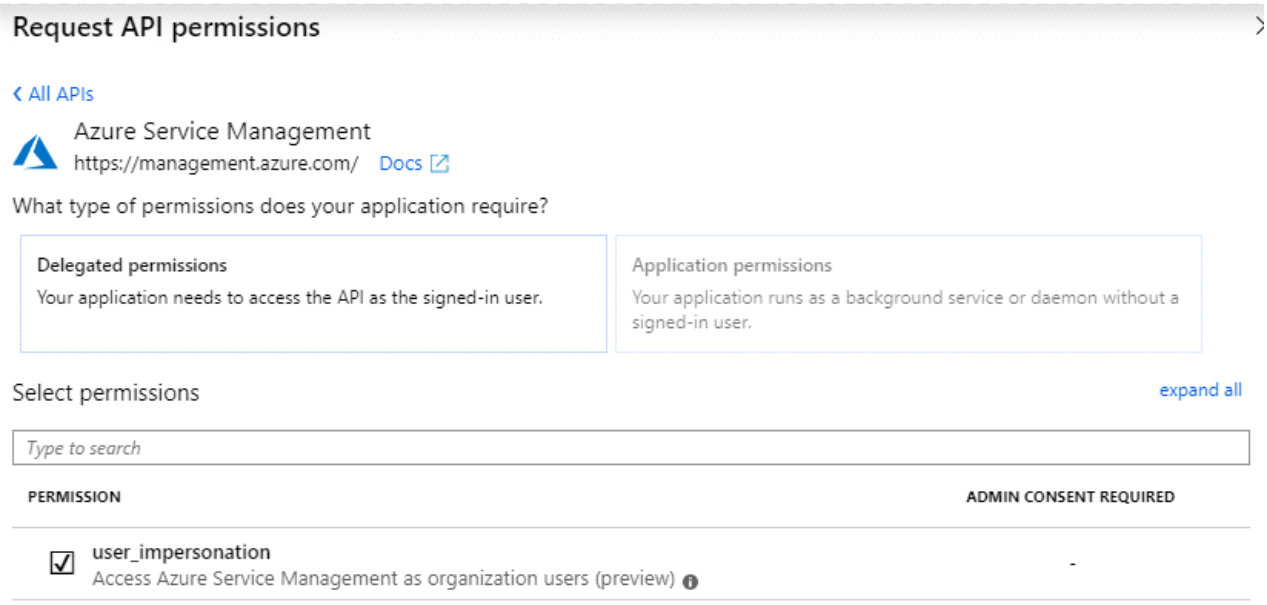
   여러 Azure 구독의 리소스를 관리하려면 각 구독에 서비스 주체를 바인딩해야 합니다. 예를 들어, 콘솔을 사용하면 Cloud Volumes ONTAP 배포할 때 사용할 구독을 선택할 수 있습니다.

Windows Azure 서비스 관리 **API** 권한 추가

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.

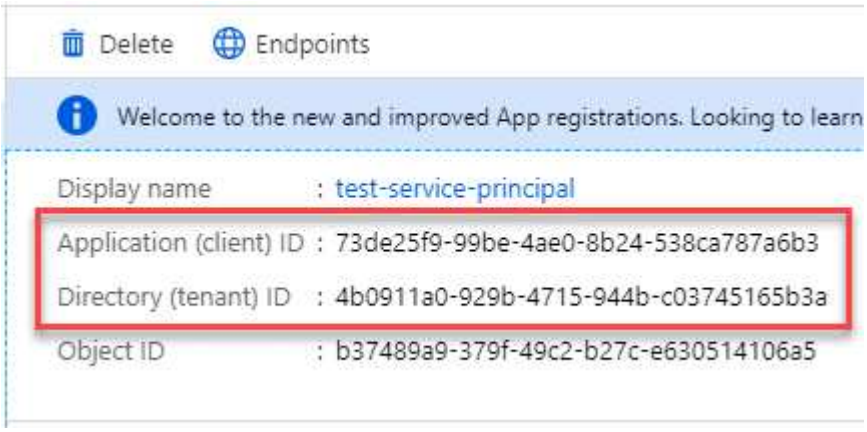


4. *조직 사용자로 Azure Service Management에 액세스*를 선택한 다음 *권한 추가*를 선택합니다.



애플리케이션의 애플리케이션 **ID**와 디렉토리 **ID**를 가져옵니다**.**

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



콘솔에 Azure 계정을 추가하는 경우 애플리케이션(클라이언트) ID와 애플리케이션의 디렉터리(테넌트) ID를 제공해야 합니다. 콘솔은 ID를 사용하여 프로그래밍 방식으로 로그인합니다.

클라이언트 비밀을 생성하세요

1. **Microsoft Entra ID** 서비스를 엽니다.
2. *앱 등록*을 선택하고 애플리케이션을 선택하세요.
3. *인증서 및 비밀번호 > 새 클라이언트 비밀번호*를 선택합니다.
4. 비밀에 대한 설명과 기간을 제공하세요.
5. *추가*를 선택하세요.
6. 클라이언트 비밀번호 값을 복사합니다.

결과

이제 서비스 주체가 설정되었고 애플리케이션(클라이언트) ID, 디렉토리(테넌트) ID 및 클라이언트 비밀번호 값을 복사했어야 합니다. 콘솔 에이전트를 생성할 때 콘솔에 이 정보를 입력해야 합니다.

4단계: 콘솔 에이전트 만들기

NetApp Console 에서 직접 콘솔 에이전트를 만듭니다.

이 작업에 관하여

- 콘솔에서 콘솔 에이전트를 만들면 기본 구성을 사용하여 Azure에 가상 머신이 배포됩니다. 콘솔 에이전트를 만든 후에는 CPU나 RAM이 적은 더 작은 VM 인스턴스로 전환하지 마세요. "콘솔 에이전트의 기본 구성에 대해 알아보세요" .
- 콘솔이 콘솔 에이전트를 배포하면 사용자 지정 역할을 만들고 이를 콘솔 에이전트 VM에 할당합니다. 이 역할에는 콘솔 에이전트가 Azure 리소스를 관리할 수 있는 권한이 포함되어 있습니다. 이후 릴리스에서 새로운 권한이 추가되므로 역할이 최신 상태로 유지되도록 해야 합니다. "콘솔 에이전트의 사용자 정의 역할에 대해 자세히 알아보세요." .

시작하기 전에

다음 사항이 있어야 합니다.

- Azure 구독.
- 선택한 Azure 지역의 VNet 및 서브넷.
- 조직에서 모든 발신 인터넷 트래픽에 프록시가 필요한 경우 프록시 서버에 대한 세부 정보:
  - IP 주소
  - 신임장
  - HTTPS 인증서
- 콘솔 에이전트 가상 머신에 대한 인증 방법을 사용하려면 SSH 공개 키가 필요합니다. 인증 방법에 대한 또 다른 옵션은 비밀번호를 사용하는 것입니다.

  "Azure에서 Linux VM에 연결하는 방법에 대해 알아보세요."

- 콘솔에서 콘솔 에이전트에 대한 Azure 역할을 자동으로 생성하지 않으려면 직접 만들어야 합니다."이 페이지의 정책을 사용하여" .

  이러한 권한은 콘솔 에이전트 자체에 대한 것입니다. 이는 이전에 콘솔 에이전트 VM을 배포하기 위해 설정한 것과 다른 권한 집합입니다.

단계

1. *관리 > 에이전트*를 선택하세요.
2. 개요 페이지에서 *에이전트 배포 > Azure*를 선택합니다.
3. 검토 페이지에서 에이전트 배포에 필요한 요구 사항을 검토합니다. 해당 요구 사항도 이 페이지의 위에 자세히 설명되어 있습니다.
4. 가상 머신 인증 페이지에서 Azure 권한을 설정하는 방법과 일치하는 인증 옵션을 선택합니다.
   - Microsoft 계정에 로그인하려면 *로그인*을 선택하세요. 이 계정에는 필요한 권한이 있어야 합니다.

     이 양식은 Microsoft에서 소유하고 호스팅합니다. 귀하의 자격 증명은 NetApp 에 제공되지 않습니다.

     이미 Azure 계정에 로그인한 경우 콘솔은 자동으로 해당 계정을 사용합니다. 여러 개의 계정이 있는 경우 먼저 로그아웃하여 올바른 계정을 사용하고 있는지 확인해야 할 수도 있습니다.
   - 필수 권한을 부여하는 Microsoft Entra 서비스 주체에 대한 정보를 입력하려면 *Active Directory 서비스 주체*를 선택하세요.
     - 애플리케이션(클라이언트) ID
     - 디렉토리(테넌트) ID
     - 클라이언트 비밀번호

   서비스 주체에 대한 이러한 값을 얻는 방법을 알아보세요. .
5. 가상 머신 인증 페이지에서 Azure 구독, 위치, 새 리소스 그룹 또는 기존 리소스 그룹을 선택한 다음, 만들고 있는 콘솔 에이전트 가상 머신에 대한 인증 방법을 선택합니다.

   가상 머신의 인증 방법은 비밀번호나 SSH 공개 키가 될 수 있습니다.

   "Azure에서 Linux VM에 연결하는 방법에 대해 알아보세요."
6. 세부 정보 페이지에서 에이전트의 이름을 입력하고 태그를 지정하고 콘솔에서 필요한 권한이 있는 새 역할을 생성할지 아니면 설정한 기존 역할을 선택할지 선택합니다."필요한 권한" .

   이 역할과 연결된 Azure 구독을 선택할 수 있습니다. 선택한 각 구독은 해당 구독의 리소스를 관리할 수 있는 콘솔 에이전트 권한을 제공합니다(예: Cloud Volumes ONTAP).
7. 네트워크 페이지에서 VNet과 서브넷을 선택하고, 공용 IP 주소를 활성화할지 여부를 지정하고, 선택적으로 프록시 구성을 지정합니다.
   - 보안 그룹 페이지에서 새 보안 그룹을 만들지, 아니면 필요한 인바운드 및 아웃바운드 규칙을 허용하는 기존 보안 그룹을 선택할지 선택합니다.

     "Azure에 대한 보안 그룹 규칙 보기" .
8. 선택 사항을 검토하여 설정이 올바른지 확인하세요.
   a. 에이전트 구성 검증 확인란은 배포 시 콘솔에서 네트워크 연결 요구 사항을 검증하도록 기본적으로 선택되어 있습니다. 콘솔에서 에이전트를 배포하지 못하면 문제 해결에 도움이 되는 보고서가 제공됩니다. 배포가 성공하면 보고서는 제공되지 않습니다.

아직도 사용 중이라면"이전 종료점" 에이전트 업그레이드에 사용되면 유효성 검사가 오류로 인해 실패합니다. 이를 방지하려면 유효성 검사를 건너뛰려면 확인란의 선택을 취소하세요.

9. *추가*를 선택하세요.

콘솔은 약 10분 안에 에이전트를 준비합니다. 프로세스가 완료될 때까지 페이지에 머물러주세요.

결과

프로세스가 완료되면 콘솔 에이전트를 콘솔에서 사용할 수 있습니다.

배포에 실패하면 콘솔에서 보고서와 로그를 다운로드하여 문제를 해결할 수 있습니다."설치 문제를 해결하는 방법을 알아보세요."

콘솔 에이전트를 만든 동일한 Azure 계정에 Azure Blob Storage가 있는 경우 Azure Blob Storage가 시스템 페이지에 자동으로 표시됩니다. "NetApp Console 에서 Azure Blob 스토리지를 관리하는 방법을 알아보세요."

Azure Marketplace에서 콘솔 에이전트 만들기

Azure Marketplace에서 직접 Azure에서 콘솔 에이전트를 만들 수 있습니다. Azure Marketplace에서 콘솔 에이전트를 만들려면 네트워킹을 설정하고, Azure 권한을 준비하고, 인스턴스 요구 사항을 검토한 다음 콘솔 에이전트를 만들어야 합니다.

시작하기 전에

- 당신은 ~을 가져야합니다"콘솔 에이전트에 대한 이해" .
- 검토"콘솔 에이전트 제한 사항" .

1단계**:** 네트워킹 설정

콘솔 에이전트를 설치하려는 네트워크 위치가 다음 요구 사항을 지원하는지 확인하세요. 이러한 요구 사항을 충족하면 콘솔 에이전트가 하이브리드 클라우드의 리소스를 관리할 수 있습니다.

Azure 지역

Cloud Volumes ONTAP 사용하는 경우 콘솔 에이전트는 관리하는 Cloud Volumes ONTAP 시스템과 동일한 Azure 지역이나 "Azure 지역 쌍" Cloud Volumes ONTAP 시스템용. 이 요구 사항은 Cloud Volumes ONTAP 과 연결된 스토리지 계정 간에 Azure Private Link 연결이 사용되도록 보장합니다.

"Cloud Volumes ONTAP Azure Private Link를 사용하는 방법 알아보기"

VNet 및 서브넷

콘솔 에이전트를 만들 때는 에이전트가 상주해야 하는 VNet과 서브넷을 지정해야 합니다.

대상 네트워크에 대한 연결

콘솔 에이전트를 사용하려면 시스템을 만들고 관리하려는 위치에 대한 네트워크 연결이 필요합니다. 예를 들어, Cloud Volumes ONTAP 시스템이나 온프레미스 환경의 스토리지 시스템을 만들 계획인 네트워크입니다.

아웃바운드 인터넷 접속

콘솔 에이전트를 배포하는 네트워크 위치에는 특정 엔드포인트에 연결하기 위한 아웃바운드 인터넷 연결이 있어야 합니다.

콘솔 에이전트에서 연락한 엔드포인트

콘솔 에이전트는 일상 업무를 위해 퍼블릭 클라우드 환경 내의 리소스와 프로세스를 관리하기 위해 다음 엔드포인트에 연결하기 위해 아웃바운드 인터넷 액세스가 필요합니다.

아래 나열된 엔드포인트는 모두 CNAME 항목입니다.

엔드포인트	목적
\ https://management.azure.com \ https://login.microsoftonline.com \ https://blob.core.windows.net \ https://core.windows.net	Azure 공용 지역의 리소스를 관리합니다.
\ https://management.chinacloudapi.cn \ https://login.chinacloudapi.cn \ https://blob.core.chinacloudapi.cn \ https://core.chinacloudapi.cn	Azure China 지역의 리소스를 관리합니다.
\ https://mysupport.netapp.com	라이선스 정보를 얻고 NetApp 지원팀에 AutoSupport 메시지를 보냅니다.
\ https://signin.b2c.netapp.com	NetApp 지원 사이트(NSS) 자격 증명을 업데이트하거나 NetApp Console 에 새로운 NSS 자격 증명을 추가합니다.
\ https://support.netapp.com	라이선스 정보를 얻고 NetApp 지원팀에 AutoSupport 메시지를 보내고 Cloud Volumes ONTAP 에 대한 소프트웨어 업데이트를 받습니다.
\ https://api.bluexp.netapp.com \ https://netapp-cloud-account.auth0.com \ https://netapp-cloud-account.us.auth0.com \ https://console.netapp.com \ https://components.console.bluexp.netapp.com \ https://cdn.auth0.com	NetApp Console 내에서 기능과 서비스를 제공합니다.

엔드포인트	목적
\ https://bluexpinfraprod.eastus2.data.azurecr.io \ https://bluexpinfraprod.azurecr.io	콘솔 에이전트 업그레이드를 위한 이미지를 얻으려면. • 새로운 에이전트를 배포할 때 유효성 검사를 통해 현재 엔드포인트에 대한 연결성을 테스트합니다. 당신이 사용하는 경우"이전 종료점" , 유효성 검사에 실패합니다. 이러한 실패를 방지하려면 유효성 검사를 건너뛰세요. 이전 엔드포인트는 계속 지원되지만 NetApp 가능한 한 빨리 현재 엔드포인트에 맞게 방화벽 규칙을 업데이트할 것을 권장합니다. "엔드포인트 목록을 업데이트하는 방법을 알아보세요" . • 방화벽의 현재 엔드포인트로 업데이트하면 기존 에이전트도 계속 작동합니다.

프록시 서버

NetApp 명시적 프록시 구성과 투명 프록시 구성을 모두 지원합니다. 투명 프록시를 사용하는 경우 프록시 서버에 대한 인증서만 제공하면 됩니다. 명시적 프록시를 사용하는 경우 IP 주소와 자격 증명도 필요합니다.

- IP 주소
- 신임장
- HTTPS 인증서

포트

Cloud Volumes ONTAP 에서 NetApp 지원팀으로 AutoSupport 메시지를 보내기 위한 프록시로 사용되거나 사용자가 시작하지 않는 한 콘솔 에이전트로 들어오는 트래픽이 없습니다.

- HTTP(80) 및 HTTPS(443)는 로컬 UI에 대한 액세스를 제공하며 이는 드문 상황에서 사용됩니다.
- SSH(22)는 문제 해결을 위해 호스트에 연결해야 하는 경우에만 필요합니다.
- 아웃바운드 인터넷 연결을 사용할 수 없는 서브넷에 Cloud Volumes ONTAP 시스템을 배포하는 경우 포트 3128을 통한 인바운드 연결이 필요합니다.

  Cloud Volumes ONTAP 시스템에 AutoSupport 메시지를 보낼 아웃바운드 인터넷 연결이 없는 경우 콘솔은 콘솔 에이전트에 포함된 프록시 서버를 사용하도록 해당 시스템을 자동으로 구성합니다. 유일한 요구 사항은 콘솔 에이전트의 보안 그룹이 포트 3128을 통한 인바운드 연결을 허용하는 것입니다. 콘솔 에이전트를 배포한 후 이 포트를 열어야 합니다.

NTP 활성화

NetApp Data Classification 사용하여 회사 데이터 소스를 스캔하려는 경우 콘솔 에이전트와 NetApp Data Classification 시스템 모두에서 NTP(네트워크 시간 프로토콜) 서비스를 활성화하여 시스템 간의 시간을 동기화해야 합니다. "NetApp 데이터 분류에 대해 자세히 알아보세요"

콘솔 에이전트를 만든 후 네트워킹 요구 사항을 구현합니다.

2단계**: VM** 요구 사항 검토

콘솔 에이전트를 생성할 때 다음 요구 사항을 충족하는 가상 머신 유형을 선택하세요.

CPU

8개 코어 또는 8개 vCPU

숫양

32GB

Azure VM 크기

CPU 및 RAM 요구 사항을 충족하는 인스턴스 유형입니다. NetApp Standard_D8s_v3를 권장합니다.

3단계**:** 권한 설정

다음과 같은 방법으로 권한을 부여할 수 있습니다.

- 옵션 1: 시스템에서 할당한 관리 ID를 사용하여 Azure VM에 사용자 지정 역할을 할당합니다.
- 옵션 2: 필요한 권한이 있는 Azure 서비스 주체에 대한 자격 증명을 콘솔에 제공합니다.

콘솔에 대한 권한을 설정하려면 다음 단계를 따르세요.

사용자 정의 역할

Azure Portal, Azure PowerShell, Azure CLI 또는 REST API를 사용하여 Azure 사용자 지정 역할을 만들 수 있습니다. 다음 단계에서는 Azure CLI를 사용하여 역할을 만드는 방법을 보여줍니다. 다른 방법을 사용하려면 다음을 참조하세요. "Azure 설명서"

단계

1. 자체 호스트에 소프트웨어를 수동으로 설치하려는 경우 VM에서 시스템이 할당한 관리 ID를 활성화하여 사용자 지정 역할을 통해 필요한 Azure 권한을 제공할 수 있습니다.

   "Microsoft Azure 설명서: Azure Portal을 사용하여 VM의 Azure 리소스에 대한 관리 ID 구성"

2. 내용을 복사하세요"커넥터에 대한 사용자 정의 역할 권한" JSON 파일에 저장합니다.
3. 할당 가능한 범위에 Azure 구독 ID를 추가하여 JSON 파일을 수정합니다.

   NetApp Console 과 함께 사용하려는 각 Azure 구독에 대한 ID를 추가해야 합니다.

   예

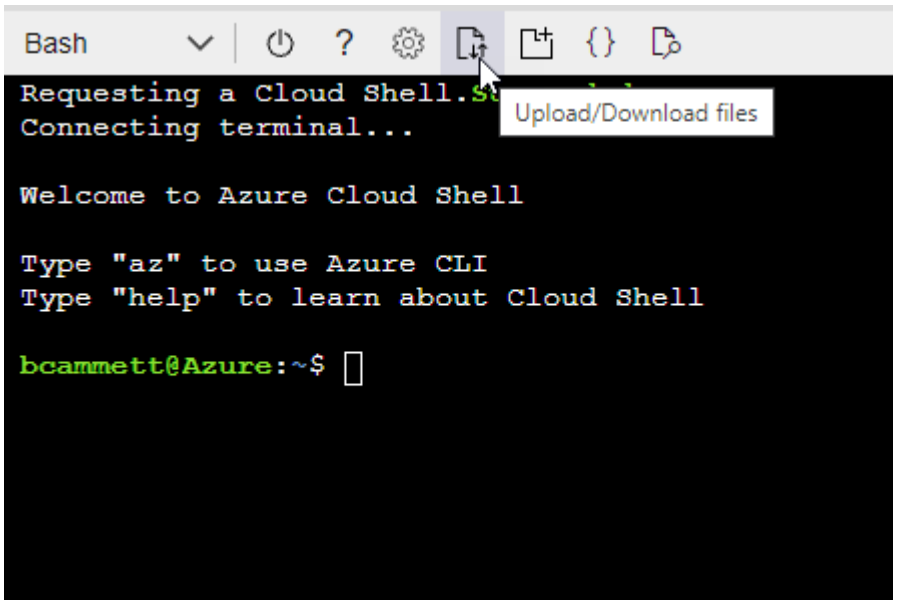
   ```
   "AssignableScopes": [
   "/subscriptions/d333af45-0d07-4154-943d-c25fbzzzzzzz",
   "/subscriptions/54b91999-b3e6-4599-908e-416e0zzzzzzz",
   "/subscriptions/398e471c-3b42-4ae7-9b59-ce5bbzzzzzzz"
   ]
   ```

4. JSON 파일을 사용하여 Azure에서 사용자 지정 역할을 만듭니다.

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

   a. 시작 "Azure 클라우드 셸" Bash 환경을 선택하세요.

   b. JSON 파일을 업로드합니다.



c. Azure CLI를 사용하여 사용자 지정 역할을 만듭니다.

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

서비스 주체

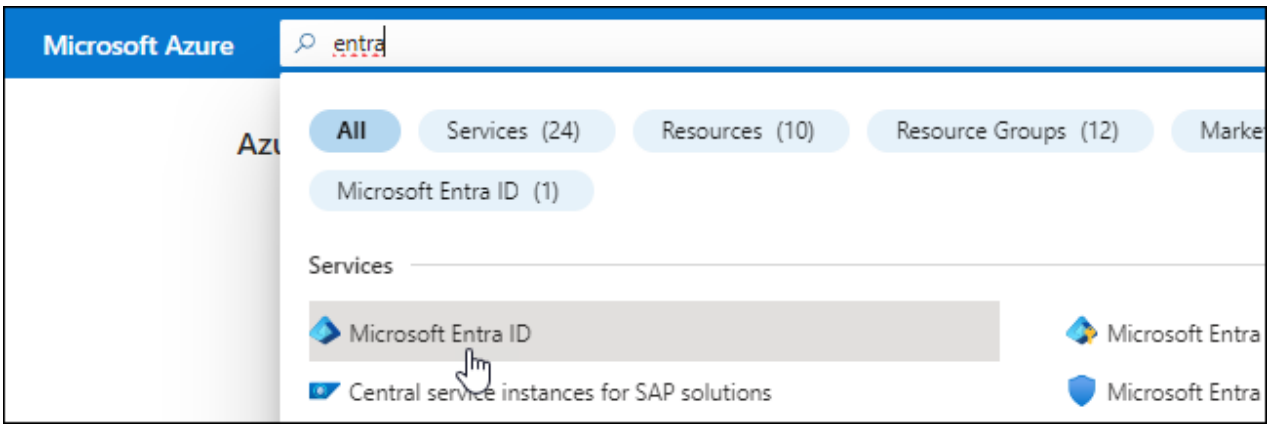
Microsoft Entra ID에서 서비스 주체를 만들고 설정하고 콘솔에 필요한 Azure 자격 증명을 얻습니다.

역할 기반 액세스 제어를 위한 **Microsoft Entra** 애플리케이션 만들기

1. Azure에서 Active Directory 애플리케이션을 만들고 해당 애플리케이션에 역할을 할당할 수 있는 권한이 있는지 확인하세요.

   자세한 내용은 다음을 참조하세요. "Microsoft Azure 설명서: 필요한 권한"

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



3. 메뉴에서 *앱 등록*을 선택하세요.
4. *신규 등록*을 선택하세요.
5. 신청서에 대한 세부 사항을 지정하세요:
   - 이름: 애플리케이션의 이름을 입력하세요.
   - 계정 유형: 계정 유형을 선택하세요(모든 계정 유형이 NetApp Console 에서 작동합니다).
   - 리디렉션 **URI**: 이 필드는 비워두어도 됩니다.
6. *등록*을 선택하세요.

   AD 애플리케이션과 서비스 주체를 생성했습니다.

역할에 애플리케이션 할당

1. 사용자 정의 역할 만들기:

   Azure Portal, Azure PowerShell, Azure CLI 또는 REST API를 사용하여 Azure 사용자 지정 역할을 만들 수 있습니다. 다음 단계에서는 Azure CLI를 사용하여 역할을 만드는 방법을 보여줍니다. 다른 방법을 사용하려면 다음을 참조하세요. "Azure 설명서"

   a. 내용을 복사하세요"콘솔 에이전트에 대한 사용자 정의 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.

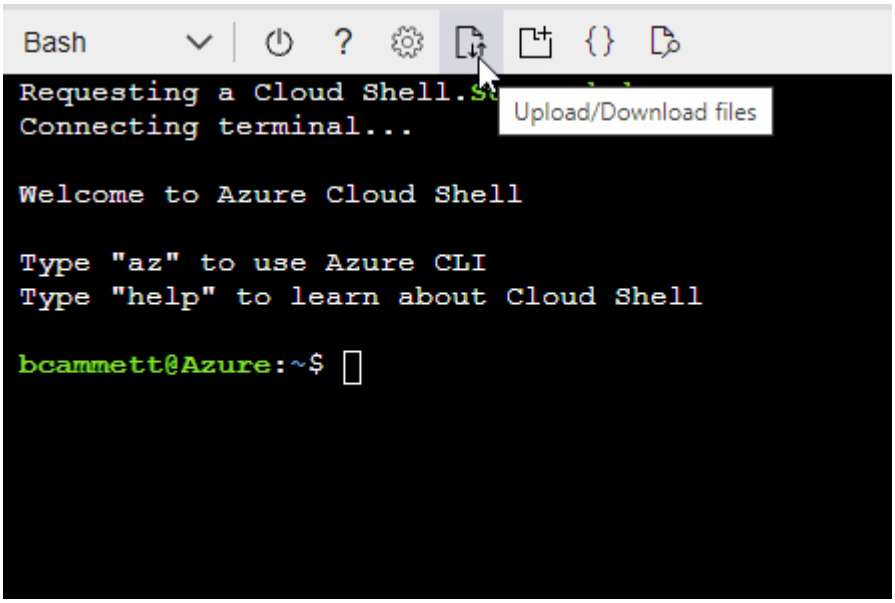
예

```
"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 만듭니다.

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

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



- Azure CLI를 사용하여 사용자 지정 역할을 만듭니다.

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

이제 콘솔 에이전트 가상 머신에 할당할 수 있는 콘솔 운영자라는 사용자 지정 역할이 생겼습니다.

2. 역할에 애플리케이션을 할당합니다.

a. Azure Portal에서 구독 서비스를 엽니다.

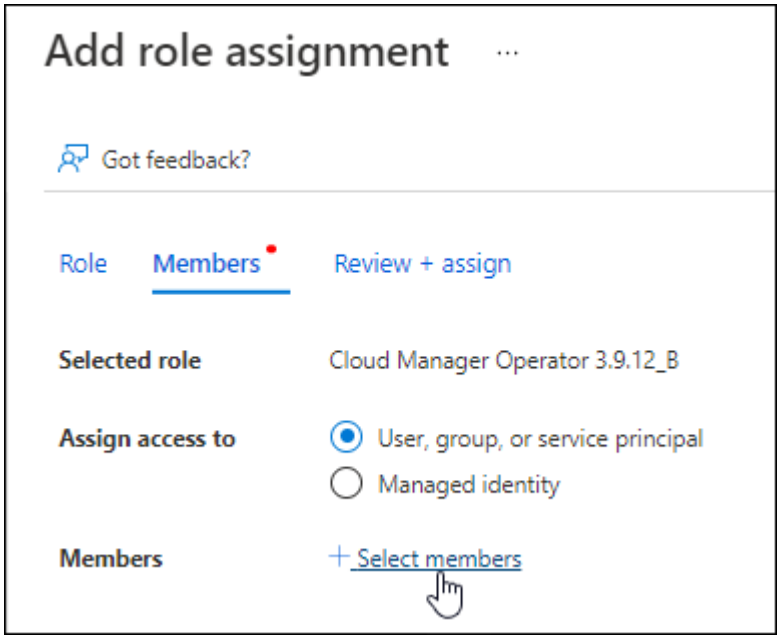
b. 구독을 선택하세요.

c. *액세스 제어(IAM) > 추가 > 역할 할당 추가*를 선택합니다.

d. 역할 탭에서 콘솔 운영자 역할을 선택하고 *다음*을 선택합니다.

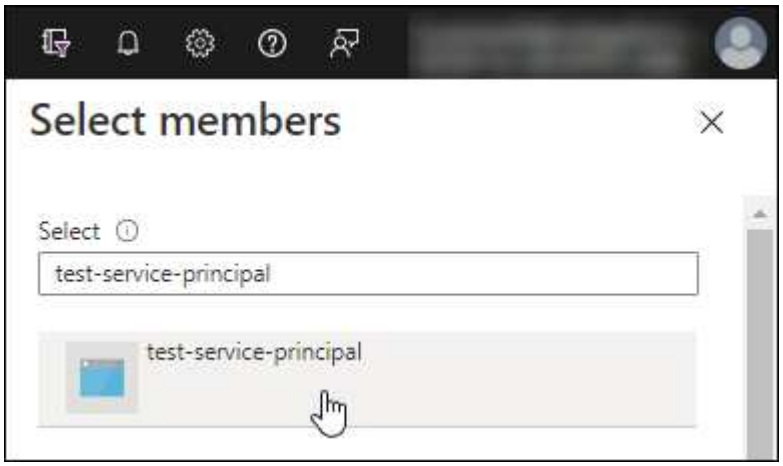
e. 멤버 탭에서 다음 단계를 완료하세요.

- *사용자, 그룹 또는 서비스 주체*를 선택된 상태로 유지합니다.
- *멤버 선택*을 선택하세요.



- 애플리케이션 이름을 검색하세요.

  예를 들면 다음과 같습니다.



- 애플리케이션을 선택하고 *선택*을 선택하세요.
- *다음*을 선택하세요.

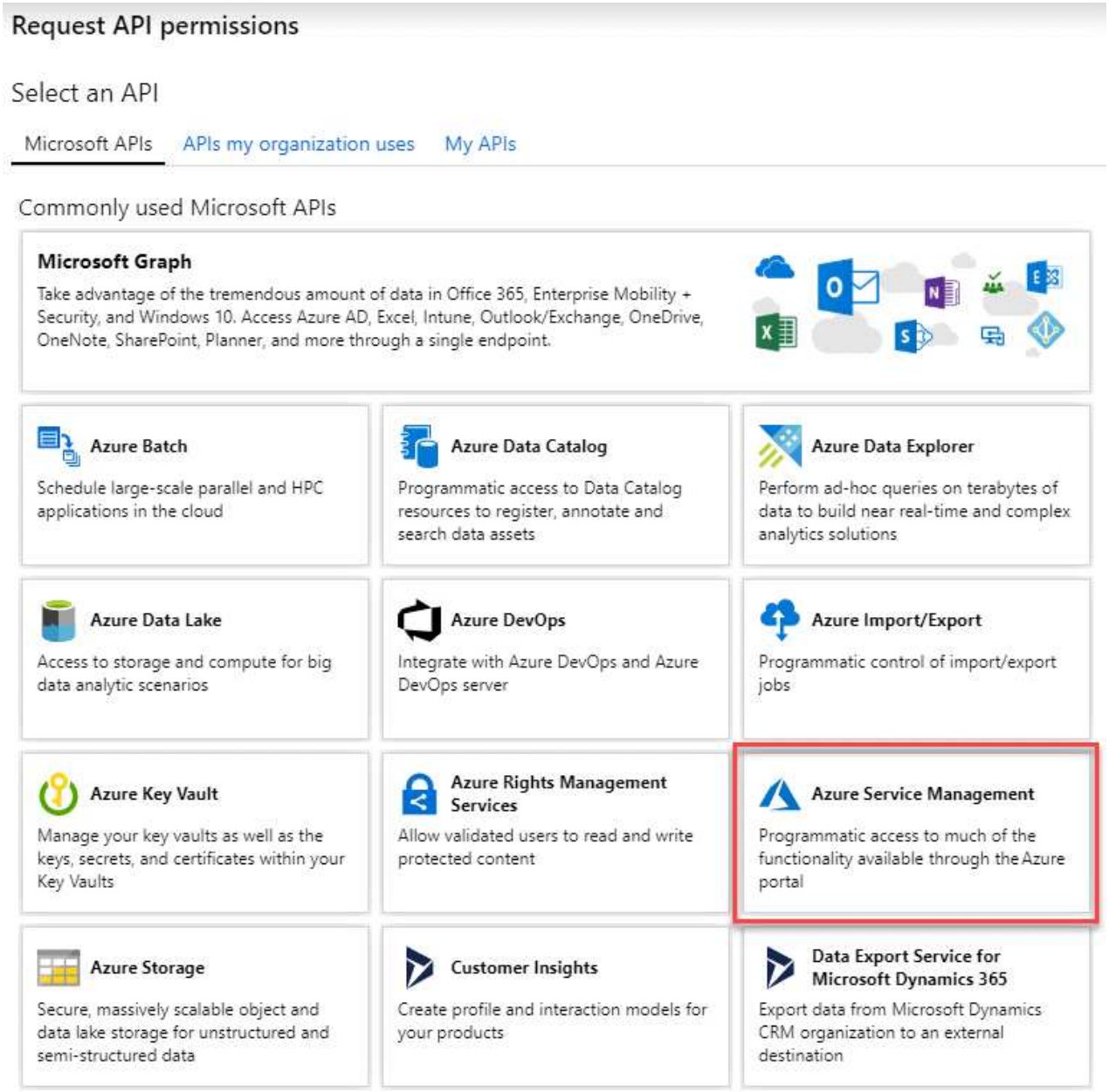
f. *검토 + 할당*을 선택하세요.

이제 서비스 주체는 콘솔 에이전트를 배포하는 데 필요한 Azure 권한을 갖게 되었습니다.

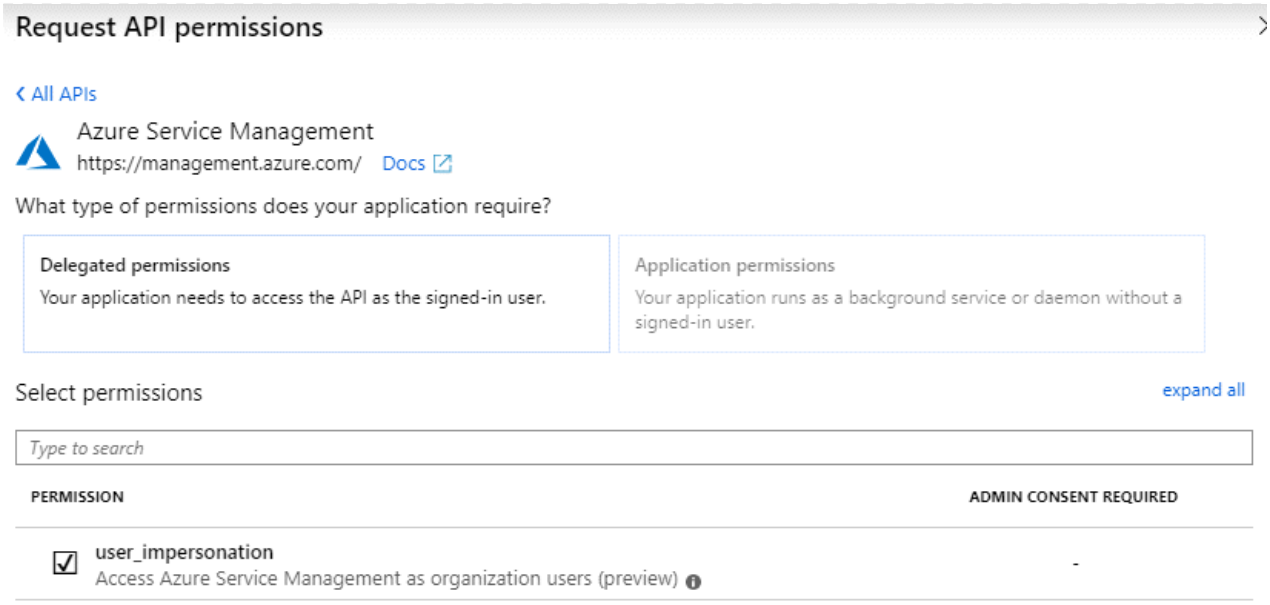
여러 Azure 구독에서 Cloud Volumes ONTAP 배포하려면 각 구독에 서비스 주체를 바인딩해야 합니다. NetApp Console 에서 Cloud Volumes ONTAP 배포할 때 사용할 구독을 선택할 수 있습니다.

Windows Azure 서비스 관리 **API** 권한 추가

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.

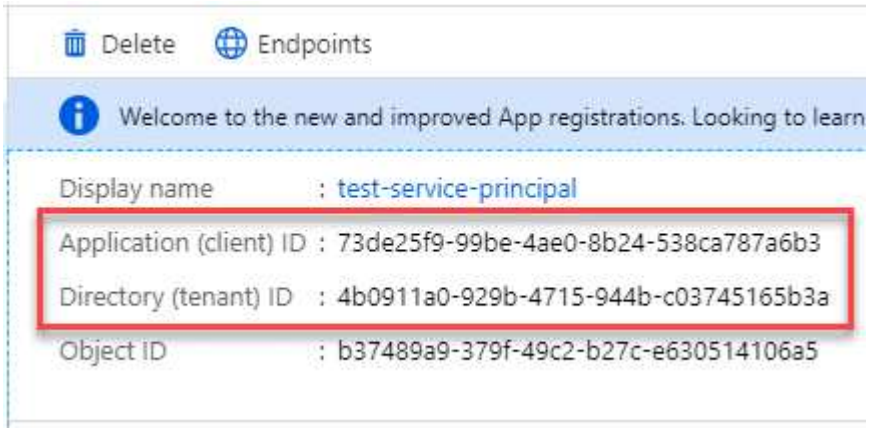


4. *조직 사용자로 Azure Service Management에 액세스*를 선택한 다음 *권한 추가*를 선택합니다.



애플리케이션의 애플리케이션 **ID**와 디렉토리 **ID**를 가져옵니다**.**

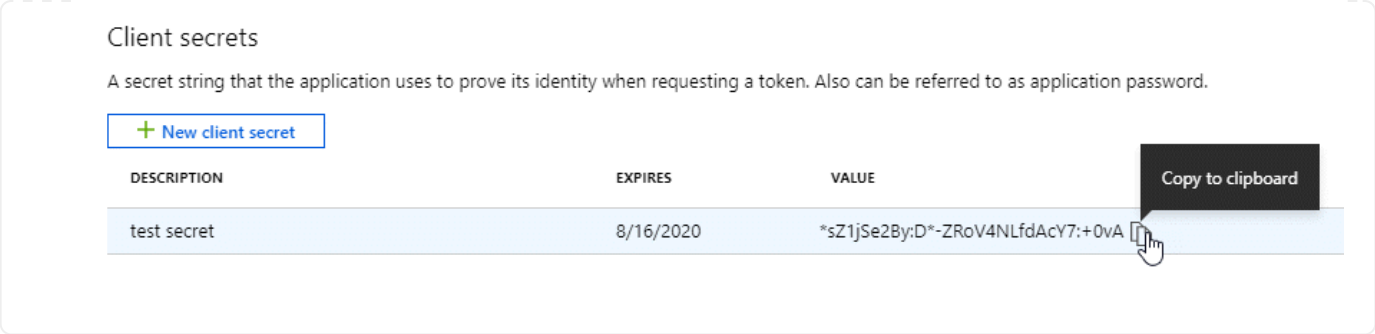
1. **Microsoft Entra ID** 서비스에서 *앱 등록*을 선택하고 애플리케이션을 선택합니다.
2. *애플리케이션(클라이언트) ID*와 *디렉토리(테넌트) ID*를 복사합니다.



콘솔에 Azure 계정을 추가하는 경우 애플리케이션(클라이언트) ID와 애플리케이션의 디렉터리(테넌트) ID를 제공해야 합니다. 콘솔은 ID를 사용하여 프로그래밍 방식으로 로그인합니다.

클라이언트 비밀을 생성하세요

1. **Microsoft Entra ID** 서비스를 엽니다.
2. *앱 등록*을 선택하고 애플리케이션을 선택하세요.
3. *인증서 및 비밀번호 > 새 클라이언트 비밀번호*를 선택합니다.
4. 비밀에 대한 설명과 기간을 제공하세요.
5. *추가*를 선택하세요.
6. 클라이언트 비밀번호 값을 복사합니다.



4단계**:** 콘솔 에이전트 만들기

Azure Marketplace에서 직접 콘솔 에이전트를 시작합니다.

이 작업에 관하여

Azure Marketplace에서 콘솔 에이전트를 만들면 기본 구성으로 가상 머신이 설정됩니다. "콘솔 에이전트의 기본 구성에 대해 알아보세요" .

시작하기 전에

다음 사항이 있어야 합니다.

- Azure 구독.
- 선택한 Azure 지역의 VNet 및 서브넷.
- 조직에서 모든 발신 인터넷 트래픽에 프록시가 필요한 경우 프록시 서버에 대한 세부 정보:
  - IP 주소
  - 신임장
  - HTTPS 인증서
- 콘솔 에이전트 가상 머신에 대한 인증 방법을 사용하려면 SSH 공개 키가 필요합니다. 인증 방법에 대한 또 다른 옵션은 비밀번호를 사용하는 것입니다.

  "Azure에서 Linux VM에 연결하는 방법에 대해 알아보세요."

- 콘솔에서 콘솔 에이전트에 대한 Azure 역할을 자동으로 생성하지 않으려면 직접 만들어야 합니다."이 페이지의 정책을 사용하여" .

  이러한 권한은 콘솔 에이전트 인스턴스 자체에 대한 것입니다. 이는 이전에 콘솔 에이전트 VM을 배포하기 위해 설정한 것과 다른 권한 집합입니다.

단계

1. Azure Marketplace의 NetApp Console 에이전트 VM 페이지로 이동합니다.

   "상업 지역을 위한 Azure Marketplace 페이지"

2. *지금 받기*를 선택한 다음 *계속*을 선택하세요.
3. Azure Portal에서 *만들기*를 선택하고 단계에 따라 가상 머신을 구성합니다.

   VM을 구성할 때 다음 사항에 유의하세요.

- **VM** 크기: CPU 및 RAM 요구 사항을 충족하는 VM 크기를 선택하세요. Standard_D8s_v3을 권장합니다.
- 디스크: 콘솔 에이전트는 HDD 또는 SSD 디스크를 사용하면 최적의 성능을 발휘할 수 있습니다.
- 네트워크 보안 그룹: 콘솔 에이전트에는 SSH, HTTP, HTTPS를 사용하는 인바운드 연결이 필요합니다.

  "Azure에 대한 보안 그룹 규칙 보기" .

- ID*: *관리*에서 *시스템에서 할당한 관리 ID 사용*을 선택합니다.

  이 설정은 관리되는 ID를 통해 콘솔 에이전트 가상 머신이 자격 증명을 제공하지 않고도 Microsoft Entra ID로 자신을 식별할 수 있기 때문에 중요합니다. "Azure 리소스에 대한 관리 ID에 대해 자세히 알아보세요." .

4. 검토 **+** 생성 페이지에서 선택 사항을 검토하고 *생성*을 선택하여 배포를 시작합니다.

   Azure는 지정된 설정으로 가상 머신을 배포합니다. 약 10분 안에 가상 머신과 콘솔 에이전트 소프트웨어가 실행되는 것을 볼 수 있습니다.

   설치에 실패하면 로그와 보고서를 보고 문제 해결에 도움을 받을 수 있습니다."설치 문제를 해결하는 방법을 알아보세요."

5. 콘솔 에이전트 가상 머신에 연결된 호스트에서 웹 브라우저를 열고 다음 URL을 입력합니다.

   https://ipaddress

6. 로그인 후 콘솔 에이전트를 설정하세요.
   a. 콘솔 에이전트와 연결할 콘솔 조직을 지정합니다.
   b. 시스템 이름을 입력하세요.
   c. *보안된 환경에서 실행하고 있습니까?*에서 제한 모드를 비활성화하세요.

      표준 모드에서 콘솔을 사용하려면 제한 모드를 비활성화하세요. 보안 환경이 있고 콘솔 백엔드 서비스에서 이 계정의 연결을 끊으려는 경우에만 제한 모드를 활성화해야 합니다. 그렇다면,"제한 모드에서 콘솔을 시작하려면 다음 단계를 따르세요." .

   d. *시작하기*를 선택하세요.

결과

이제 콘솔 에이전트를 설치하고 콘솔 조직에 맞게 설정했습니다.

콘솔 에이전트를 만든 동일한 Azure 구독에 Azure Blob 저장소가 있는 경우 시스템 페이지에 Azure Blob 저장소 시스템이 자동으로 표시됩니다. "콘솔에서 Azure Blob 저장소를 관리하는 방법을 알아보세요."

5단계**:** 콘솔 에이전트에 권한 제공

이제 콘솔 에이전트를 만들었으므로 이전에 설정한 권한을 제공해야 합니다. 권한을 제공하면 콘솔 에이전트가 Azure에서 데이터 및 스토리지 인프라를 관리할 수 있습니다.

사용자 정의 역할

Azure Portal로 이동하여 하나 이상의 구독에 대한 콘솔 에이전트 가상 머신에 Azure 사용자 지정 역할을 할당합니다.

단계

1. Azure Portal에서 구독 서비스를 열고 구독을 선택합니다.

   구독 서비스에서 역할을 할당하는 것이 중요한 이유는 이를 통해 구독 수준에서 역할 할당의 범위가 지정되기 때문입니다. _scope_는 액세스가 적용되는 리소스 집합을 정의합니다. 다른 수준(예: 가상 머신 수준)에서 범위를 지정하는 경우 NetApp Console 내에서 작업을 완료하는 기능에 영향을 미칩니다.

   "Microsoft Azure 설명서: Azure RBAC 범위 이해"

2. 액세스 제어**(IAM)** > 추가 > *역할 할당 추가*를 선택합니다.
3. 역할 탭에서 콘솔 운영자 역할을 선택하고 *다음*을 선택합니다.

   콘솔 운영자는 정책에 제공된 기본 이름입니다. 역할에 다른 이름을 선택한 경우 해당 이름을 대신 선택하세요.

4. 멤버 탭에서 다음 단계를 완료하세요.
   a. *관리되는 ID*에 대한 액세스 권한을 할당합니다.
   b. *멤버 선택*을 선택하고, 콘솔 에이전트 가상 머신이 생성된 구독을 선택하고, *관리 ID*에서 *가상 머신*을 선택한 다음, 콘솔 에이전트 가상 머신을 선택합니다.
   c. *선택*을 선택하세요.
   d. *다음*을 선택하세요.
   e. *검토 + 할당*을 선택하세요.
   f. 추가 Azure 구독의 리소스를 관리하려면 해당 구독으로 전환한 다음 이러한 단계를 반복합니다.

다음은 무엇인가요**?**

로 가다 "NetApp Console" 콘솔 에이전트를 사용하려면.

서비스 주체

단계

1. *관리 > 자격 증명*을 선택합니다.
2. *자격 증명 추가*를 선택하고 마법사의 단계를 따르세요.
   a. 자격 증명 위치: *Microsoft Azure > 에이전트*를 선택합니다.
   b. 자격 증명 정의: 필요한 권한을 부여하는 Microsoft Entra 서비스 주체에 대한 정보를 입력합니다.
      - 애플리케이션(클라이언트) ID
      - 디렉토리(테넌트) ID
      - 클라이언트 비밀번호
   c. 마켓플레이스 구독: 지금 구독하거나 기존 구독을 선택하여 마켓플레이스 구독을 이러한 자격 증명과 연결합니다.

d. 검토: 새로운 자격 증명에 대한 세부 정보를 확인하고 *추가*를 선택합니다.

결과

이제 콘솔에는 Azure에서 사용자를 대신하여 작업을 수행하는 데 필요한 권한이 있습니다.

Azure에 콘솔 에이전트를 수동으로 설치합니다.

자신의 Linux 호스트에 콘솔 에이전트를 수동으로 설치하려면 호스트 요구 사항을 검토하고, 네트워킹을 설정하고, Azure 권한을 준비하고, 콘솔 에이전트를 설치한 다음, 준비한 권한을 제공해야 합니다.

시작하기 전에

- 당신은 ~을 가져야합니다"콘솔 에이전트에 대한 이해" .
- 검토해야 합니다"콘솔 에이전트 제한 사항" .

1단계**:** 호스트 요구 사항 검토

콘솔 에이전트 소프트웨어는 특정 운영 체제 요구 사항, RAM 요구 사항, 포트 요구 사항 등을 충족하는 호스트에서 실행되어야 합니다.

콘솔 에이전트는 UID와 GID 범위를 19000~19200으로 예약합니다. 이 범위는 고정되어 있으며 수정할 수 없습니다. 호스트의 타사 소프트웨어가 이 범위 내의 UID나 GID를 사용하는 경우 에이전트 설치가 실패합니다. NetApp 충돌을 피하기 위해 타사 소프트웨어가 없는 호스트를 사용할 것을 권장합니다.

전담 호스트

콘솔 에이전트를 실행하려면 전용 호스트가 필요합니다. 다음의 크기 요건을 충족하는 모든 아키텍처가 지원됩니다.

- CPU: 8개 코어 또는 8개 vCPU
- 램: 32GB
- 디스크 공간: 호스트에 권장되는 디스크 공간은 165GB이며, 다음 파티션 요구 사항이 적용됩니다.
  - `/opt`: 120GiB의 공간이 사용 가능해야 합니다.

    에이전트는 다음을 사용합니다. `/opt` 설치하려면 `/opt/application/netapp` 디렉토리와 그 내용.
  - `/var`: 40GiB의 공간이 사용 가능해야 합니다.

    콘솔 에이전트는 다음 공간이 필요합니다. `/var` Podman이나 Docker는 컨테이너를 이 디렉터리 내에 생성하도록 설계되었기 때문입니다. 구체적으로, 그들은 컨테이너를 생성할 것입니다. `/var/lib/containers/storage` 디렉토리 및 `/var/lib/docker` Docker용입니다. 이 공간에서는 외부 마운트나 심볼릭 링크가 작동하지 않습니다.

Azure VM 크기

CPU 및 RAM 요구 사항을 충족하는 인스턴스 유형입니다. NetApp Standard_D8s_v3를 권장합니다.

하이퍼바이저

지원되는 운영 체제를 실행하도록 인증된 베어 메탈 또는 호스팅 하이퍼바이저가 필요합니다.

운영 체제 및 컨테이너 요구 사항

콘솔 에이전트는 표준 모드 또는 제한 모드에서 콘솔을 사용할 때 다음 운영 체제에서 지원됩니다. 에이전트를 설치하기 전에 컨테이너 오케스트레이션 도구가 필요합니다.

운영 체제	지원되는 **OS** 버전	지원되는 에이전트 버전	필수 컨테이너 도구	셀리눅스
레드햇 엔터프라이즈 리눅스		9.6 • 영어 버전만 제공됩니다. • 호스트는 Red Hat Subscription Management에 등록되어야 합니다. 등록되지 않은 경우 호스트는 에이전트 설치 중에 필요한 타사 소프트웨어를 업데이트하기 위해 저장소에 액세스할 수 없습니다.	4.0.0 이상, 콘솔이 표준 모드 또는 제한 모드인 경우	Podman 버전 5.4.0과 podman-compose 1.5.0. Podman 구성 요구 사항 보기 .
강제 모드 또는 허용 모드에서 지원됨		9.1에서 9.4까지 • 영어 버전만 제공됩니다. • 호스트는 Red Hat Subscription Management에 등록되어야 합니다. 등록되지 않은 경우 호스트는 에이전트 설치 중에 필요한 타사 소프트웨어를 업데이트하기 위해 저장소에 액세스할 수 없습니다.	3.9.50 이상, 콘솔이 표준 모드 또는 제한 모드인 경우	Podman 버전 4.9.4와 podman-compose 1.5.0. Podman 구성 요구 사항 보기 .

운영 체제	지원되는 **OS** 버전	지원되는 에이전트 버전	필수 컨테이너 도구	셀리눅스
강제 모드 또는 허용 모드에서 지원됨		8.6에서 8.10까지 • 영어 버전만 제공됩니다. • 호스트는 Red Hat Subscription Management에 등록되어야 합니다. 등록되지 않은 경우 호스트는 에이전트 설치 중에 필요한 타사 소프트웨어를 업데이트하기 위해 저장소에 액세스할 수 없습니다.	3.9.50 이상, 콘솔이 표준 모드 또는 제한 모드인 경우	Podman 버전 4.6.1 또는 4.9.4와 podman-compose 1.0.6. Podman 구성 요구 사항 보기 .
강제 모드 또는 허용 모드에서 지원됨	우분투		24.04 장기	표준 모드 또는 제한 모드에서 NetApp Console 사용하는 3.9.45 이상
Docker 엔진 23.06~28.0.0.	지원되지 않음		22.04 장기	3.9.50 이상

2단계**: Podman** 또는 **Docker Engine** 설치

운영 체제에 따라 에이전트를 설치하기 전에 Podman 또는 Docker Engine이 필요합니다.

- Red Hat Enterprise Linux 8 및 9에는 Podman이 필요합니다.

  지원되는 Podman 버전 보기 .

- Ubuntu에는 Docker 엔진이 필요합니다.

  지원되는 Docker Engine 버전 보기 .

예 **2.** 단계

포드만

Podman을 설치하고 구성하려면 다음 단계를 따르세요.

- podman.socket 서비스를 활성화하고 시작합니다.
- python3 설치
- podman-compose 패키지 버전 1.0.6을 설치하세요
- PATH 환경 변수에 podman-compose를 추가합니다.
- Red Hat Enterprise Linux를 사용하는 경우 Podman 버전이 CNI 대신 Netavark Aardvark DNS를 사용하는지 확인하십시오.

DNS 포트 충돌을 피하기 위해 에이전트를 설치한 후 aardvark-dns 포트(기본값: 53)를 조정하세요. 지침에 따라 포트를 구성하세요.

단계

1. 호스트에 podman-docker 패키지가 설치되어 있다면 제거합니다.

```
dnf remove podman-docker
rm /var/run/docker.sock
```

2. Podman을 설치하세요.

   공식 Red Hat Enterprise Linux 저장소에서 Podman을 다운로드할 수 있습니다.

   a. Red Hat Enterprise Linux 9.6의 경우:

   ```
   sudo dnf install podman-5:<version>
   ```

   여기서 <버전>은 설치하려는 Podman의 지원되는 버전입니다. 지원되는 Podman 버전 보기 .

   b. Red Hat Enterprise Linux 9.1~9.4 버전의 경우:

   ```
   sudo dnf install podman-4:<version>
   ```

   여기서 <버전>은 설치하려는 Podman의 지원되는 버전입니다. 지원되는 Podman 버전 보기 .

   c. Red Hat Enterprise Linux 8의 경우:

   ```
   sudo dnf install podman-4:<version>
   ```

   여기서 <버전>은 설치하려는 Podman의 지원되는 버전입니다. 지원되는 Podman 버전 보기 .

3. podman.socket 서비스를 활성화하고 시작합니다.

```
sudo systemctl enable --now podman.socket
```

4. python3를 설치합니다.

```
sudo dnf install python3
```

5. 시스템에 EPEL 저장소 패키지가 아직 없으면 설치하세요.

   이 단계는 podman-compose가 EPEL(Enterprise Linux용 추가 패키지) 저장소에서 사용 가능하기 때문에 필요합니다.

6. Red Hat Enterprise 9를 사용하는 경우:

   a. EPEL 저장소 패키지를 설치하세요.

```
sudo dnf install https://dl.fedoraproject.org/pub/epel/epel-release-latest-9.noarch.rpm
```

   +

   a. podman-compose 패키지 1.5.0을 설치합니다.

```
sudo dnf install podman-compose-1.5.0
```

7. Red Hat Enterprise Linux 8을 사용하는 경우:

   a. EPEL 저장소 패키지를 설치하세요.

```
sudo dnf install https://dl.fedoraproject.org/pub/epel/epel-release-latest-8.noarch.rpm
```

   b. podman-compose 패키지 1.0.6을 설치합니다.

```
sudo dnf install podman-compose-1.0.6
```

> ⓘ 를 사용하여 `dnf install` 명령은 PATH 환경 변수에 podman-compose를 추가하는 요구 사항을 충족합니다. 설치 명령은 이미 포함되어 있는 /usr/bin에 podman-compose를 추가합니다. `secure_path` 호스트의 옵션.

   c. Red Hat Enterprise Linux 8을 사용하는 경우 Podman 버전이 CNI 대신 Aardvark DNS와 함께 NetAvark를 사용하는지 확인하세요.

i. 다음 명령을 실행하여 networkBackend가 CNI로 설정되어 있는지 확인하세요.

```
podman info | grep networkBackend
```

ii. networkBackend가 설정된 경우 `CNI` , 당신은 그것을 변경해야 합니다 `netavark` .

iii. 설치하다 `netavark` 그리고 `aardvark-dns` 다음 명령을 사용합니다.

```
dnf install aardvark-dns netavark
```

iv. 열기 `/etc/containers/containers.conf` 파일을 열고 network_backend 옵션을 "cni" 대신 "netavark"를 사용하도록 수정합니다.

만약에 `/etc/containers/containers.conf` 존재하지 않습니다. 구성을 변경하세요. `/usr/share/containers/containers.conf` .

v. Podman을 다시 시작하세요.

```
systemctl restart podman
```

vi. 다음 명령을 사용하여 networkBackend가 이제 "netavark"로 변경되었는지 확인하세요.

```
podman info | grep networkBackend
```

도커 엔진

Docker Engine을 설치하려면 Docker 설명서를 따르세요.

단계

1. "Docker에서 설치 지침 보기"

   지원되는 Docker Engine 버전을 설치하려면 다음 단계를 따르세요. 콘솔에서 지원되지 않으므로 최신 버전을 설치하지 마세요.

2. Docker가 활성화되어 실행 중인지 확인하세요.

```
sudo systemctl enable docker && sudo systemctl start docker
```

3단계**:** 네트워킹 설정

콘솔 에이전트를 설치하려는 네트워크 위치가 다음 요구 사항을 지원하는지 확인하세요. 이러한 요구 사항을 충족하면 콘솔 에이전트가 하이브리드 클라우드 환경 내의 리소스와 프로세스를 관리할 수 있습니다.

Azure 지역

Cloud Volumes ONTAP 사용하는 경우 콘솔 에이전트는 관리하는 Cloud Volumes ONTAP 시스템과 동일한 Azure 지역이나 "Azure 지역 쌍" Cloud Volumes ONTAP 시스템용. 이 요구 사항은 Cloud Volumes ONTAP 과 연결된 스토리지 계정 간에 Azure Private Link 연결이 사용되도록 보장합니다.

"Cloud Volumes ONTAP Azure Private Link를 사용하는 방법 알아보기"

대상 네트워크에 대한 연결

콘솔 에이전트를 사용하려면 시스템을 만들고 관리하려는 위치에 대한 네트워크 연결이 필요합니다. 예를 들어, Cloud Volumes ONTAP 시스템이나 온프레미스 환경의 스토리지 시스템을 만들 계획인 네트워크입니다.

아웃바운드 인터넷 접속

콘솔 에이전트를 배포하는 네트워크 위치에는 특정 엔드포인트에 연결하기 위한 아웃바운드 인터넷 연결이 있어야 합니다.

웹 기반 **NetApp Console** 사용할 때 컴퓨터에서 연결된 엔드포인트

웹 브라우저에서 콘솔에 액세스하는 컴퓨터는 여러 엔드포인트에 접속할 수 있어야 합니다. 콘솔 에이전트를 설정하고 콘솔을 일상적으로 사용하려면 콘솔을 사용해야 합니다.

"NetApp 콘솔을 위한 네트워킹 준비" .

콘솔 에이전트에서 연락한 엔드포인트

콘솔 에이전트는 일상 업무를 위해 퍼블릭 클라우드 환경 내의 리소스와 프로세스를 관리하기 위해 다음 엔드포인트에 연결하기 위해 아웃바운드 인터넷 액세스가 필요합니다.

아래 나열된 엔드포인트는 모두 CNAME 항목입니다.

엔드포인트	목적
\ https://management.azure.com \ https://login.microsoftonline.com \ https://blob.core.windows.net \ https://core.windows.net	Azure 공용 지역의 리소스를 관리합니다.
\ https://management.chinacloudapi.cn \ https://login.chinacloudapi.cn \ https://blob.core.chinacloudapi.cn \ https://core.chinacloudapi.cn	Azure China 지역의 리소스를 관리합니다.
\ https://mysupport.netapp.com	라이선스 정보를 얻고 NetApp 지원팀에 AutoSupport 메시지를 보냅니다.
\ https://signin.b2c.netapp.com	NetApp 지원 사이트(NSS) 자격 증명을 업데이트하거나 NetApp Console 에 새로운 NSS 자격 증명을 추가합니다.
\ https://support.netapp.com	라이선스 정보를 얻고 NetApp 지원팀에 AutoSupport 메시지를 보내고 Cloud Volumes ONTAP 에 대한 소프트웨어 업데이트를 받습니다.

엔드포인트	목적
\ https://api.bluexp.netapp.com \ https://netapp-cloud-account.auth0.com \ https://netapp-cloud-account.us.auth0.com \ https://console.netapp.com \ https://components.console.bluexp.netapp.com \ https://cdn.auth0.com	NetApp Console 내에서 기능과 서비스를 제공합니다.
\ https://bluexpinfraprod.eastus2.data.azurecr.io \ https://bluexpinfraprod.azurecr.io	콘솔 에이전트 업그레이드를 위한 이미지를 얻으려면. • 새로운 에이전트를 배포할 때 유효성 검사를 통해 현재 엔드포인트에 대한 연결성을 테스트합니다. 당신이 사용하는 경우"이전 종료점" , 유효성 검사에 실패합니다. 이러한 실패를 방지하려면 유효성 검사를 건너뛰세요. 이전 엔드포인트는 계속 지원되지만 NetApp 가능한 한 빨리 현재 엔드포인트에 맞게 방화벽 규칙을 업데이트할 것을 권장합니다. "엔드포인트 목록을 업데이트하는 방법을 알아보세요" . • 방화벽의 현재 엔드포인트로 업데이트하면 기존 에이전트도 계속 작동합니다.

프록시 서버

NetApp 명시적 프록시 구성과 투명 프록시 구성을 모두 지원합니다. 투명 프록시를 사용하는 경우 프록시 서버에 대한 인증서만 제공하면 됩니다. 명시적 프록시를 사용하는 경우 IP 주소와 자격 증명도 필요합니다.

- IP 주소
- 신임장
- HTTPS 인증서

포트

Cloud Volumes ONTAP 에서 NetApp 지원팀으로 AutoSupport 메시지를 보내기 위한 프록시로 사용되거나 사용자가 시작하지 않는 한 콘솔 에이전트로 들어오는 트래픽이 없습니다.

- HTTP(80) 및 HTTPS(443)는 로컬 UI에 대한 액세스를 제공하며 이는 드문 상황에서 사용됩니다.
- SSH(22)는 문제 해결을 위해 호스트에 연결해야 하는 경우에만 필요합니다.
- 아웃바운드 인터넷 연결을 사용할 수 없는 서브넷에 Cloud Volumes ONTAP 시스템을 배포하는 경우 포트 3128을 통한 인바운드 연결이 필요합니다.

Cloud Volumes ONTAP 시스템에 AutoSupport 메시지를 보낼 아웃바운드 인터넷 연결이 없는 경우 콘솔은 콘솔 에이전트에 포함된 프록시 서버를 사용하도록 해당 시스템을 자동으로 구성합니다. 유일한 요구 사항은 콘솔 에이전트의 보안 그룹이 포트 3128을 통한 인바운드 연결을 허용하는 것입니다. 콘솔 에이전트를 배포한 후 이 포트를 열어야 합니다.

NTP 활성화

NetApp Data Classification 사용하여 회사 데이터 소스를 스캔하려는 경우 콘솔 에이전트와 NetApp Data Classification 시스템 모두에서 NTP(네트워크 시간 프로토콜) 서비스를 활성화하여 시스템 간의 시간을 동기화해야 합니다. "NetApp 데이터 분류에 대해 자세히 알아보세요"

4단계**:** 콘솔 에이전트 배포 권한 설정

다음 옵션 중 하나를 사용하여 콘솔 에이전트에 Azure 권한을 제공해야 합니다.

- 옵션 1: 시스템에서 할당한 관리 ID를 사용하여 Azure VM에 사용자 지정 역할을 할당합니다.
- 옵션 2: 필요한 권한이 있는 Azure 서비스 주체에 대한 자격 증명을 콘솔 에이전트에 제공합니다.

콘솔 에이전트에 대한 권한을 준비하려면 다음 단계를 따르세요.

콘솔 에이전트 배포를 위한 사용자 지정 역할 만들기

Azure Portal, Azure PowerShell, Azure CLI 또는 REST API를 사용하여 Azure 사용자 지정 역할을 만들 수 있습니다. 다음 단계에서는 Azure CLI를 사용하여 역할을 만드는 방법을 보여줍니다. 다른 방법을 사용하려면 다음을 참조하세요. "Azure 설명서"

단계

1. 자체 호스트에 소프트웨어를 수동으로 설치하려는 경우 VM에서 시스템이 할당한 관리 ID를 활성화하여 사용자 지정 역할을 통해 필요한 Azure 권한을 제공할 수 있습니다.

   "Microsoft Azure 설명서: Azure Portal을 사용하여 VM의 Azure 리소스에 대한 관리 ID 구성"

2. 내용을 복사하세요"커넥터에 대한 사용자 정의 역할 권한" JSON 파일에 저장합니다.
3. 할당 가능한 범위에 Azure 구독 ID를 추가하여 JSON 파일을 수정합니다.

   NetApp Console 과 함께 사용하려는 각 Azure 구독에 대한 ID를 추가해야 합니다.

   예

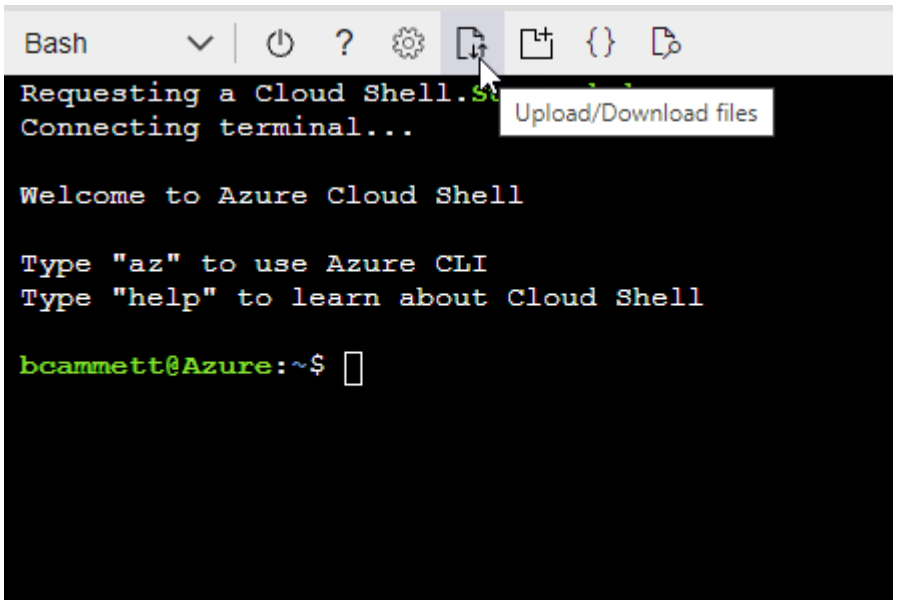
   ```
   "AssignableScopes": [
   "/subscriptions/d333af45-0d07-4154-943d-c25fbzzzzzzz",
   "/subscriptions/54b91999-b3e6-4599-908e-416e0zzzzzzz",
   "/subscriptions/398e471c-3b42-4ae7-9b59-ce5bbzzzzzzz"
   ]
   ```

4. JSON 파일을 사용하여 Azure에서 사용자 지정 역할을 만듭니다.

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

   a. 시작 "Azure 클라우드 셸" Bash 환경을 선택하세요.

   b. JSON 파일을 업로드합니다.



c. Azure CLI를 사용하여 사용자 지정 역할을 만듭니다.

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

서비스 주체

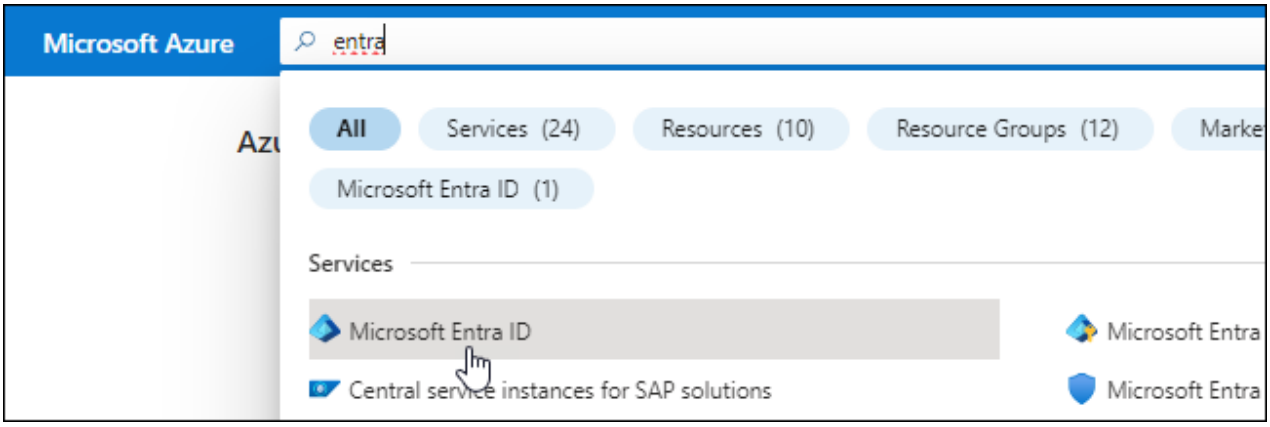
Microsoft Entra ID에서 서비스 주체를 만들고 설정하고 콘솔 에이전트에 필요한 Azure 자격 증명을 얻습니다.

역할 기반 액세스 제어를 위한 **Microsoft Entra** 애플리케이션 만들기

1. Azure에서 Active Directory 애플리케이션을 만들고 해당 애플리케이션에 역할을 할당할 수 있는 권한이 있는지 확인하세요.

   자세한 내용은 다음을 참조하세요. "Microsoft Azure 설명서: 필요한 권한"

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



3. 메뉴에서 *앱 등록*을 선택하세요.
4. *신규 등록*을 선택하세요.
5. 신청서에 대한 세부 사항을 지정하세요:
   - 이름: 애플리케이션의 이름을 입력하세요.
   - 계정 유형: 계정 유형을 선택하세요(모든 계정 유형이 NetApp Console 에서 작동합니다).
   - 리디렉션 **URI**: 이 필드는 비워두어도 됩니다.
6. *등록*을 선택하세요.

   AD 애플리케이션과 서비스 주체를 생성했습니다.

역할에 애플리케이션 할당

1. 사용자 정의 역할 만들기:

   Azure Portal, Azure PowerShell, Azure CLI 또는 REST API를 사용하여 Azure 사용자 지정 역할을 만들 수 있습니다. 다음 단계에서는 Azure CLI를 사용하여 역할을 만드는 방법을 보여줍니다. 다른 방법을 사용하려면 다음을 참조하세요. "Azure 설명서"

   a. 내용을 복사하세요"콘솔 에이전트에 대한 사용자 정의 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.

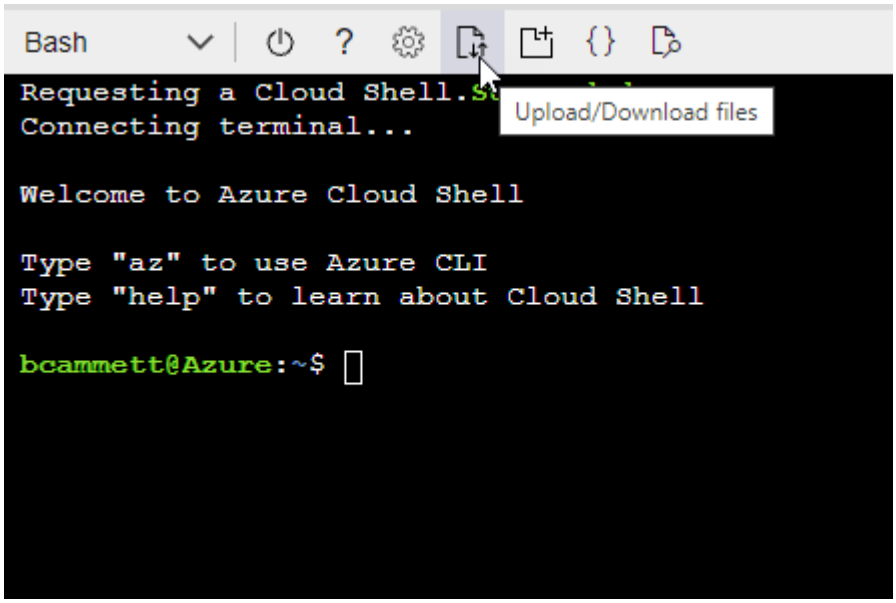
예

```
"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 만듭니다.

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

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



- Azure CLI를 사용하여 사용자 지정 역할을 만듭니다.

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

이제 콘솔 에이전트 가상 머신에 할당할 수 있는 콘솔 운영자라는 사용자 지정 역할이 생겼습니다.

2. 역할에 애플리케이션을 할당합니다.

a. Azure Portal에서 구독 서비스를 엽니다.

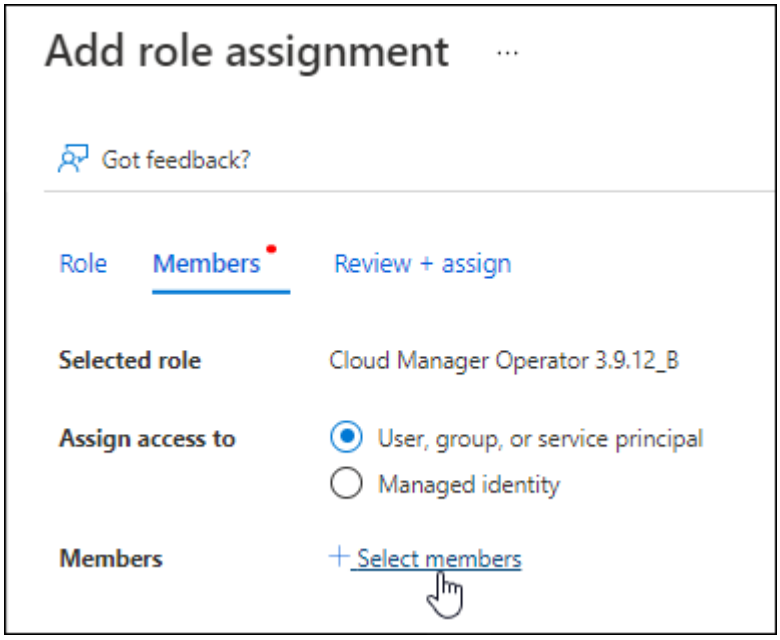
b. 구독을 선택하세요.

c. *액세스 제어(IAM) > 추가 > 역할 할당 추가*를 선택합니다.

d. 역할 탭에서 콘솔 운영자 역할을 선택하고 *다음*을 선택합니다.

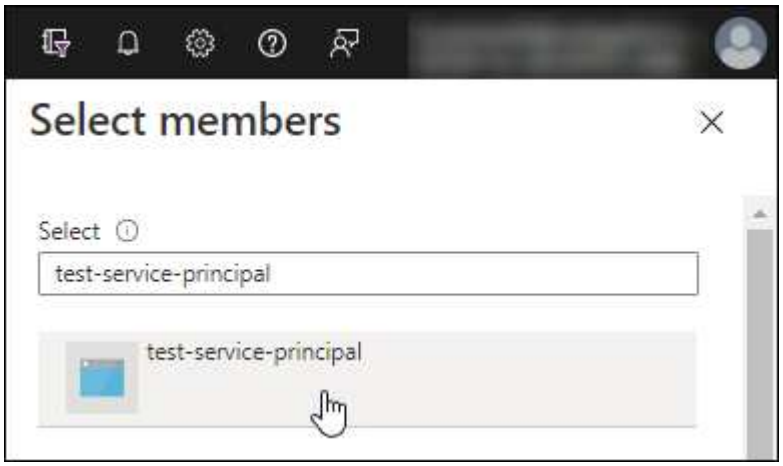
e. 멤버 탭에서 다음 단계를 완료하세요.

- *사용자, 그룹 또는 서비스 주체*를 선택된 상태로 유지합니다.
- *멤버 선택*을 선택하세요.



- 애플리케이션 이름을 검색하세요.

  예를 들면 다음과 같습니다.



- 애플리케이션을 선택하고 *선택*을 선택하세요.
- *다음*을 선택하세요.

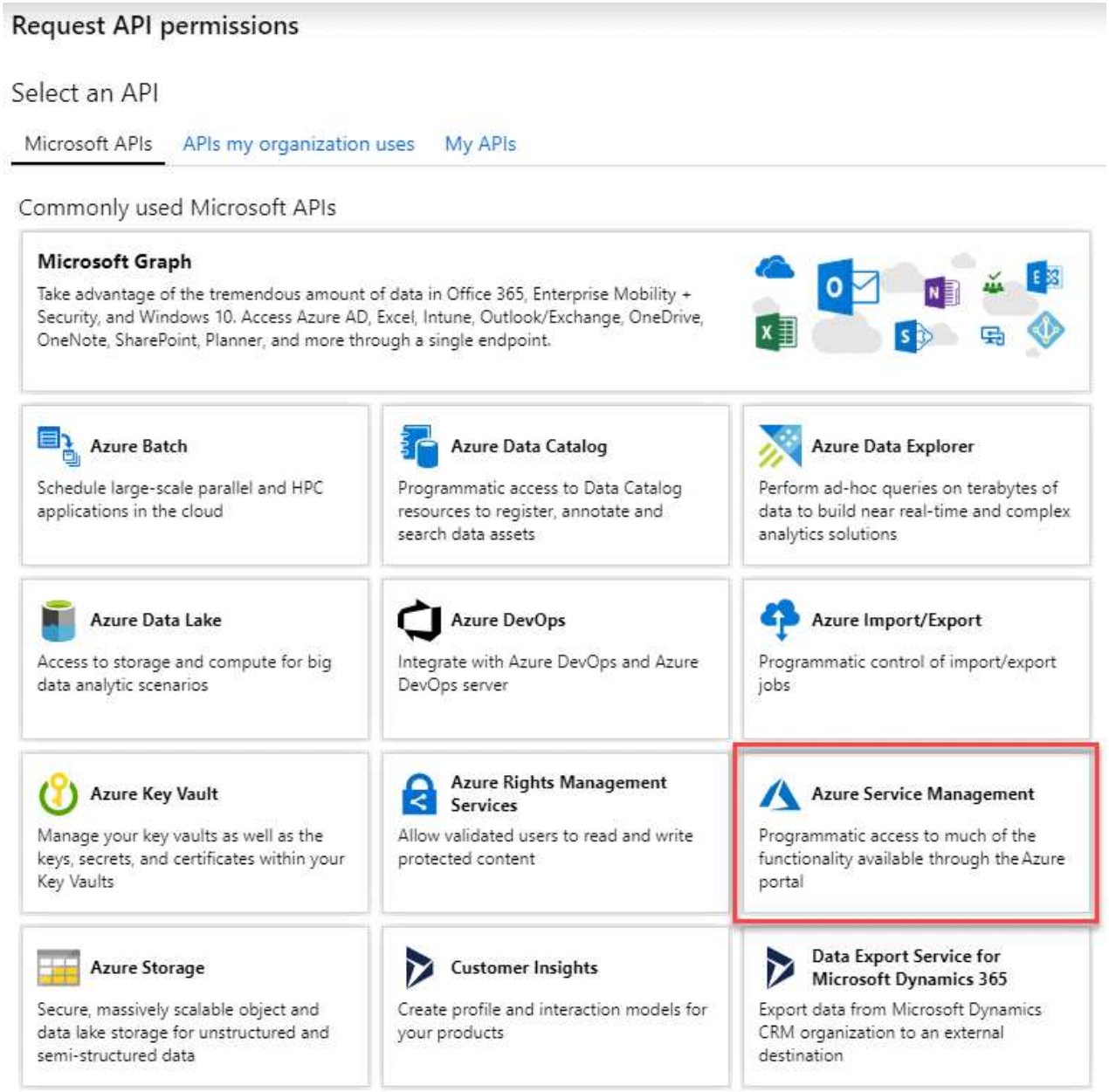
f. *검토 + 할당*을 선택하세요.

이제 서비스 주체는 콘솔 에이전트를 배포하는 데 필요한 Azure 권한을 갖게 되었습니다.

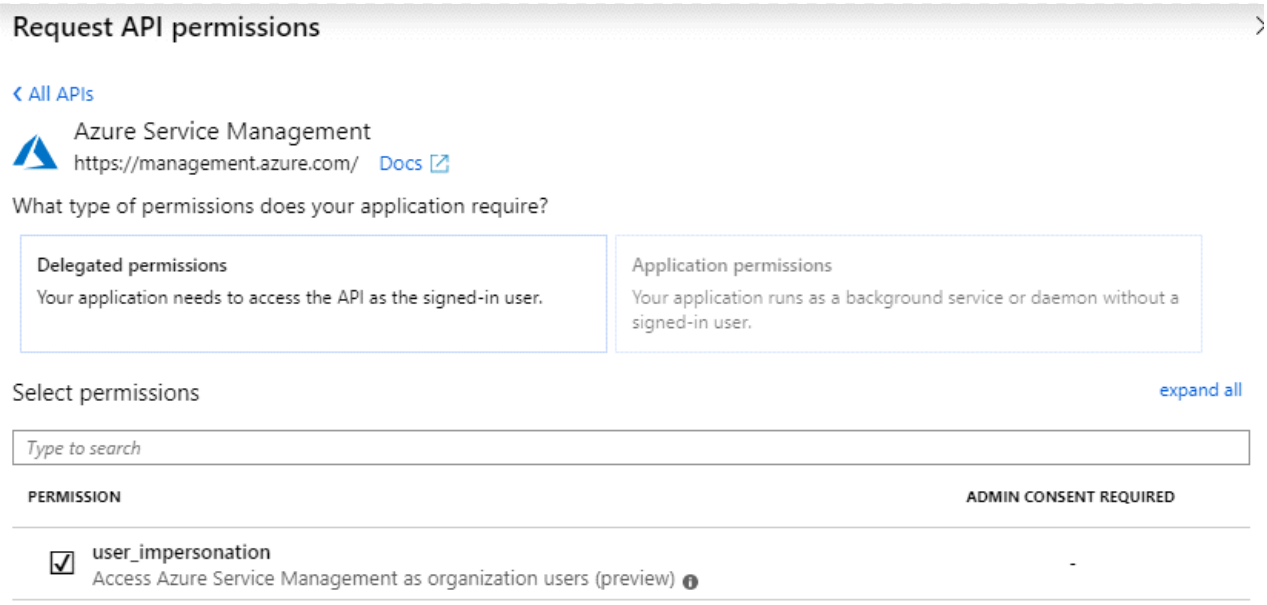
여러 Azure 구독에서 Cloud Volumes ONTAP 배포하려면 각 구독에 서비스 주체를 바인딩해야 합니다. NetApp Console 에서 Cloud Volumes ONTAP 배포할 때 사용할 구독을 선택할 수 있습니다.

Windows Azure 서비스 관리 **API** 권한 추가

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.

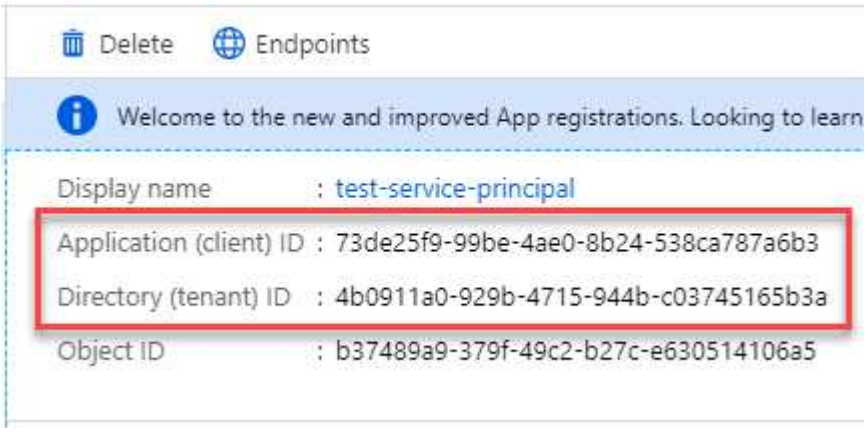


4. *조직 사용자로 Azure Service Management에 액세스*를 선택한 다음 *권한 추가*를 선택합니다.



애플리케이션의 애플리케이션 **ID**와 디렉토리 **ID**를 가져옵니다**.**

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



콘솔에 Azure 계정을 추가하는 경우 애플리케이션(클라이언트) ID와 애플리케이션의 디렉터리(테넌트) ID를 제공해야 합니다. 콘솔은 ID를 사용하여 프로그래밍 방식으로 로그인합니다.

클라이언트 비밀을 생성하세요

1. **Microsoft Entra ID** 서비스를 엽니다.
2. *앱 등록*을 선택하고 애플리케이션을 선택하세요.
3. *인증서 및 비밀번호 > 새 클라이언트 비밀번호*를 선택합니다.
4. 비밀에 대한 설명과 기간을 제공하세요.
5. *추가*를 선택하세요.
6. 클라이언트 비밀번호 값을 복사합니다.

결과

이제 서비스 주체가 설정되었고 애플리케이션(클라이언트) ID, 디렉토리(테넌트) ID 및 클라이언트 비밀번호 값을 복사했어야 합니다. Azure 계정을 추가할 때 콘솔에 이 정보를 입력해야 합니다.

5단계**:** 콘솔 에이전트 설치

필수 구성 요소를 모두 완료한 후에는 Linux 호스트에 소프트웨어를 수동으로 설치할 수 있습니다.

시작하기 전에

다음 사항이 있어야 합니다.

- 콘솔 에이전트를 설치하려면 루트 권한이 필요합니다.
- 콘솔 에이전트에서 인터넷에 접속하는 데 프록시가 필요한 경우 프록시 서버에 대한 세부 정보입니다.

  설치 후 프록시 서버를 구성할 수 있지만, 그렇게 하려면 콘솔 에이전트를 다시 시작해야 합니다.

- 프록시 서버가 HTTPS를 사용하거나 프록시가 가로채기 프록시인 경우 CA 서명 인증서가 필요합니다.

> ⓘ 콘솔 에이전트를 수동으로 설치하는 경우 투명 프록시 서버에 대한 인증서를 설정할 수 없습니다. 투명 프록시 서버에 대한 인증서를 설정해야 하는 경우 설치 후 유지 관리 콘솔을 사용해야 합니다. 자세히 알아보세요"에이전트 유지 관리 콘솔" .

- 사용자 지정 역할을 통해 필요한 Azure 권한을 제공할 수 있도록 Azure의 VM에서 관리되는 ID를 활성화합니다.

  "Microsoft Azure 설명서: Azure Portal을 사용하여 VM의 Azure 리소스에 대한 관리 ID 구성"

이 작업에 관하여

설치 후, 새로운 버전이 나오면 콘솔 에이전트가 자동으로 업데이트됩니다.

단계

1. 호스트에 *http_proxy* 또는 *https_proxy* 시스템 변수가 설정되어 있으면 제거합니다.

   ```
   unset http_proxy
   unset https_proxy
   ```

   이러한 시스템 변수를 제거하지 않으면 설치가 실패합니다.

2. 콘솔 에이전트 소프트웨어를 다운로드한 다음 Linux 호스트에 복사하십시오. NetApp Console 또는 NetApp 지원 사이트에서 다운로드할 수 있습니다.
   - NetApp Console: *에이전트 > 관리 > 에이전트 배포 > 온프레미스 > 수동 설치*로 이동합니다.

     에이전트 설치 파일 다운로드 또는 파일 URL 다운로드를 선택하십시오.

   - NetApp 지원 사이트 (콘솔에 대한 액세스 권한이 없는 경우 필요) "NetApp 지원 사이트" ,
3. 스크립트를 실행할 수 있는 권한을 할당합니다.

```
chmod +x NetApp_Console_Agent_Cloud_<version>
```

   여기서 <버전>은 다운로드한 콘솔 에이전트의 버전입니다.

4. 정부 클라우드 환경에 설치하는 경우 구성 검사를 비활성화하세요."수동 설치에 대한 구성 검사를 비활성화하는 방법을 알아보세요."
5. 설치 스크립트를 실행합니다.

```
./NetApp_Console_Agent_Cloud_<version> --proxy <HTTP or HTTPS proxy
server> --cacert <path and file name of a CA-signed certificate>
```

   네트워크에서 인터넷 접속을 위해 프록시가 필요한 경우 프록시 정보를 추가해야 합니다. 설치 중에 명시적 프록시를 추가할 수 있습니다. `--proxy` 및 `--cacert` 매개변수는 선택 사항이며 추가하라는 메시지가 표시되지 않습니다. 명시적 프록시 서버가 있는 경우 표시된 대로 매개변수를 입력해야 합니다.

   투명 프록시를 구성하려면 설치 후에 구성하면 됩니다. "에이전트 유지 관리 콘솔에 대해 알아보세요"

+

다음은 CA 서명 인증서로 명시적 프록시 서버를 구성하는 예입니다.

+

```
./NetApp_Console_Agent_Cloud_v4.0.0--proxy
https://user:password@10.0.0.30:8080/ --cacert /tmp/cacert/certificate.cer
```

+
`--proxy` 다음 형식 중 하나를 사용하여 Console 에이전트가 HTTP 또는 HTTPS 프록시 서버를 사용하도록 구성합니다.

+ * http://address:port * http://user-name:password@address:port * http://domain-name%92user-name:password@address:port * https://address:port * https://user-name:password@address:port * https://domain-name%92user-name:password@address:port

+ 다음 사항에 유의하십시오:

+ 사용자는 로컬 사용자 또는 도메인 사용자일 수 있습니다. 도메인 사용자의 경우 위와 같이 \의 ASCII 코드를 사용해야 합니다. **Console** 에이전트는 @ 문자가 포함된 사용자 이름이나 암호를 지원하지 않습니다. 암호에 다음 특수 문자(& 또는 !)가 포함된 경우 백슬래시를 앞에 붙여 해당 특수 문자를 이스케이프해야 합니다.

+ 예를 들면:

+ http://bxpproxyuser:netapp1\!@address:3128

1. Podman을 사용한 경우 aardvark-dns 포트를 조정해야 합니다.

   a. 콘솔 에이전트 가상 머신에 SSH를 실행합니다.

   b. podman */usr/share/containers/containers.conf* 파일을 열고 Aardvark DNS 서비스에 대해 선택한 포트를 수정합니다. 예를 들어, 54로 변경합니다.

   ```
   vi /usr/share/containers/containers.conf
   ```

   예를 들어:

   ```
   # Port to use for dns forwarding daemon with netavark in rootful bridge
   # mode and dns enabled.
   # Using an alternate port might be useful if other DNS services should
   # run on the machine.
   #
   dns_bind_port = 54
   ```

   a. 콘솔 에이전트 가상 머신을 재부팅합니다.

2. 설치가 완료될 때까지 기다리세요.

   설치가 끝나면 프록시 서버를 지정한 경우 콘솔 에이전트 서비스(occm)가 두 번 다시 시작됩니다.

   설치에 실패하면 설치 보고서와 로그를 보고 문제를 해결하는 데 도움이 됩니다."설치 문제를 해결하는 방법을 알아보세요."

1. 콘솔 에이전트 가상 머신에 연결된 호스트에서 웹 브라우저를 열고 다음 URL을 입력합니다.

   https://ipaddress

2. 로그인 후 콘솔 에이전트를 설정하세요.

   a. 콘솔 에이전트와 연결할 조직을 지정합니다.

   b. 시스템 이름을 입력하세요.

   c. *보안된 환경에서 실행하고 있습니까?*에서 제한 모드를 비활성화하세요.

      이 단계에서는 표준 모드에서 콘솔을 사용하는 방법을 설명하므로 제한 모드를 비활성화해야 합니다. 보안 환경이 있고 백엔드 서비스에서 이 계정의 연결을 끊으려는 경우에만 제한 모드를 활성화해야 합니다. 그렇다면 ,"제한 모드에서 NetApp Console 시작하기 위한 단계를 따르세요." .

d. *시작하기*를 선택하세요.

콘솔 에이전트를 만든 동일한 Azure 구독에 Azure Blob 저장소가 있는 경우 시스템 페이지에 Azure Blob 저장소 시스템이 자동으로 표시됩니다. "NetApp Console 에서 Azure Blob 스토리지를 관리하는 방법을 알아보세요."

6단계**: NetApp Console** 에 권한 제공

이제 콘솔 에이전트를 설치했으므로 이전에 설정한 Azure 권한을 콘솔 에이전트에 제공해야 합니다. 권한을 제공하면 콘솔에서 Azure의 데이터 및 스토리지 인프라를 관리할 수 있습니다.

사용자 정의 역할

Azure Portal로 이동하여 하나 이상의 구독에 대한 콘솔 에이전트 가상 머신에 Azure 사용자 지정 역할을 할당합니다.

단계

1. Azure Portal에서 구독 서비스를 열고 구독을 선택합니다.

   구독 서비스에서 역할을 할당하는 것이 중요한 이유는 이를 통해 구독 수준에서 역할 할당의 범위가 지정되기 때문입니다. _scope_는 액세스가 적용되는 리소스 집합을 정의합니다. 다른 수준(예: 가상 머신 수준)에서 범위를 지정하는 경우 NetApp Console 내에서 작업을 완료하는 기능에 영향을 미칩니다.

   "Microsoft Azure 설명서: Azure RBAC 범위 이해"

2. 액세스 제어**(IAM)** > 추가 > *역할 할당 추가*를 선택합니다.
3. 역할 탭에서 콘솔 운영자 역할을 선택하고 *다음*을 선택합니다.

   콘솔 운영자는 정책에 제공된 기본 이름입니다. 역할에 다른 이름을 선택한 경우 해당 이름을 대신 선택하세요.

4. 멤버 탭에서 다음 단계를 완료하세요.
   a. *관리되는 ID*에 대한 액세스 권한을 할당합니다.
   b. *멤버 선택*을 선택하고, 콘솔 에이전트 가상 머신이 생성된 구독을 선택하고, *관리 ID*에서 *가상 머신*을 선택한 다음, 콘솔 에이전트 가상 머신을 선택합니다.
   c. *선택*을 선택하세요.
   d. *다음*을 선택하세요.
   e. *검토 + 할당*을 선택하세요.
   f. 추가 Azure 구독의 리소스를 관리하려면 해당 구독으로 전환한 다음 이러한 단계를 반복합니다.

다음은 무엇인가요**?**

로 가다 "NetApp Console" 콘솔 에이전트를 사용하려면.

서비스 주체

단계

1. *관리 > 자격 증명*을 선택합니다.
2. *자격 증명 추가*를 선택하고 마법사의 단계를 따르세요.
   a. 자격 증명 위치: *Microsoft Azure > 에이전트*를 선택합니다.
   b. 자격 증명 정의: 필요한 권한을 부여하는 Microsoft Entra 서비스 주체에 대한 정보를 입력합니다.
      - 애플리케이션(클라이언트) ID
      - 디렉토리(테넌트) ID
      - 클라이언트 비밀번호
   c. 마켓플레이스 구독: 지금 구독하거나 기존 구독을 선택하여 마켓플레이스 구독을 이러한 자격 증명과 연결합니다.

d. 검토: 새로운 자격 증명에 대한 세부 정보를 확인하고 *추가*를 선택합니다.

결과

이제 콘솔 에이전트는 Azure에서 사용자를 대신하여 작업을 수행하는 데 필요한 권한을 갖게 되었습니다.

구글 클라우드

Google Cloud의 콘솔 에이전트 설치 옵션

Google Cloud에서 콘솔 에이전트를 만드는 방법에는 여러 가지가 있습니다. 가장 일반적인 방법은 NetApp Console 에서 직접 실행하는 것입니다.

다음과 같은 설치 옵션을 사용할 수 있습니다.

- "콘솔에서 직접 콘솔 에이전트를 만듭니다."(이것은 표준 옵션입니다)

  이 작업을 수행하면 선택한 VPC에서 Linux와 콘솔 에이전트 소프트웨어를 실행하는 VM 인스턴스가 시작됩니다.

- "Google Platform을 사용하여 콘솔 에이전트 만들기"

  이 작업을 수행하면 Linux와 콘솔 에이전트 소프트웨어가 실행되는 VM 인스턴스가 시작되지만 배포는 콘솔이 아닌 Google Cloud에서 직접 시작됩니다.

- "자신의 Linux 호스트에 소프트웨어를 다운로드하고 수동으로 설치하세요."

선택하는 설치 옵션은 설치를 준비하는 방법에 영향을 미칩니다. 여기에는 Google Cloud에서 리소스를 인증하고 관리하는 데 필요한 권한을 콘솔에 제공하는 방법이 포함됩니다.

NetApp Console 에서 **Google Cloud**에 콘솔 에이전트 만들기

Google Cloud 콘솔에서 콘솔 에이전트를 만들 수 있습니다. 네트워킹을 설정하고, Google Cloud 권한을 준비하고, Google Cloud API를 활성화한 다음 콘솔 에이전트를 만들어야 합니다.

시작하기 전에

- 당신은 ~을 가져야합니다"콘솔 에이전트에 대한 이해" .
- 검토해야 합니다"콘솔 에이전트 제한 사항" .

1단계**:** 네트워킹 설정

콘솔 에이전트가 대상 네트워크에 연결하고 아웃바운드 인터넷에 접속하여 리소스를 관리할 수 있도록 네트워킹을 설정합니다.

VPC 및 서브넷

콘솔 에이전트를 생성할 때는 에이전트가 상주해야 하는 VPC와 서브넷을 지정해야 합니다.

대상 네트워크에 대한 연결

콘솔 에이전트를 사용하려면 시스템을 만들고 관리하려는 위치에 대한 네트워크 연결이 필요합니다. 예를 들어, Cloud Volumes ONTAP 시스템이나 온프레미스 환경의 스토리지 시스템을 만들 계획인 네트워크입니다.

아웃바운드 인터넷 접속

콘솔 에이전트를 배포하는 네트워크 위치에는 특정 엔드포인트에 연결하기 위한 아웃바운드 인터넷 연결이 있어야 합니다.

콘솔 에이전트에서 연락한 엔드포인트

콘솔 에이전트는 일상 업무를 위해 퍼블릭 클라우드 환경 내의 리소스와 프로세스를 관리하기 위해 다음 엔드포인트에 연결하기 위해 아웃바운드 인터넷 액세스가 필요합니다.

아래 나열된 엔드포인트는 모두 CNAME 항목입니다.

엔드포인트	목적
https://www.googleapis.com/compute/v1/ https://compute.googleapis.com/compute/v1 https://cloudresourcemanager.googleapis.com/v1/projects https://www.googleapis.com/compute/beta https://storage.googleapis.com/storage/v1 https://www.googleapis.com/storage/v1 https://iam.googleapis.com/v1 https://cloudkms.googleapis.com/v1 https://config.googleapis.com/v1/projects	Google Cloud에서 리소스를 관리합니다.
\ https://mysupport.netapp.com	라이선스 정보를 얻고 NetApp 지원팀에 AutoSupport 메시지를 보냅니다.
\ https://signin.b2c.netapp.com	NetApp 지원 사이트(NSS) 자격 증명을 업데이트하거나 NetApp Console 에 새로운 NSS 자격 증명을 추가합니다.
\ https://support.netapp.com	라이선스 정보를 얻고 NetApp 지원팀에 AutoSupport 메시지를 보내고 Cloud Volumes ONTAP 에 대한 소프트웨어 업데이트를 받습니다.
\ https://api.bluexp.netapp.com \ https://netapp-cloud-account.auth0.com \ https://netapp-cloud-account.us.auth0.com \ https://console.netapp.com \ https://components.console.bluexp.netapp.com \ https://cdn.auth0.com	NetApp Console 내에서 기능과 서비스를 제공합니다.

엔드포인트	목적
\ https://bluexpinfraprod.eastus2.data.azurecr.io \ https://bluexpinfraprod.azurecr.io	콘솔 에이전트 업그레이드를 위한 이미지를 얻으려면. • 새로운 에이전트를 배포할 때 유효성 검사를 통해 현재 엔드포인트에 대한 연결성을 테스트합니다. 당신이 사용하는 경우"이전 종료점" , 유효성 검사에 실패합니다. 이러한 실패를 방지하려면 유효성 검사를 건너뛰세요. 이전 엔드포인트는 계속 지원되지만 NetApp 가능한 한 빨리 현재 엔드포인트에 맞게 방화벽 규칙을 업데이트할 것을 권장합니다. "엔드포인트 목록을 업데이트하는 방법을 알아보세요" . • 방화벽의 현재 엔드포인트로 업데이트하면 기존 에이전트도 계속 작동합니다.

NetApp 콘솔에서 연결된 엔드포인트

SaaS 계층을 통해 제공되는 웹 기반 NetApp Console 사용하면 여러 엔드포인트에 연결하여 데이터 관리 작업을 완료할 수 있습니다. 여기에는 콘솔에서 콘솔 에이전트를 배포하기 위해 연결된 엔드포인트가 포함됩니다.

"NetApp 콘솔에서 연결된 엔드포인트 목록 보기" .

프록시 서버

NetApp 명시적 프록시 구성과 투명 프록시 구성을 모두 지원합니다. 투명 프록시를 사용하는 경우 프록시 서버에 대한 인증서만 제공하면 됩니다. 명시적 프록시를 사용하는 경우 IP 주소와 자격 증명도 필요합니다.

- IP 주소
- 신임장
- HTTPS 인증서

포트

Cloud Volumes ONTAP 에서 NetApp 지원팀으로 AutoSupport 메시지를 보내기 위한 프록시로 사용되거나 사용자가 시작하지 않는 한 콘솔 에이전트로 들어오는 트래픽이 없습니다.

- HTTP(80) 및 HTTPS(443)는 로컬 UI에 대한 액세스를 제공하며 이는 드문 상황에서 사용됩니다.
- SSH(22)는 문제 해결을 위해 호스트에 연결해야 하는 경우에만 필요합니다.
- 아웃바운드 인터넷 연결을 사용할 수 없는 서브넷에 Cloud Volumes ONTAP 시스템을 배포하는 경우 포트 3128을 통한 인바운드 연결이 필요합니다.

Cloud Volumes ONTAP 시스템에 AutoSupport 메시지를 보낼 아웃바운드 인터넷 연결이 없는 경우 콘솔은 콘솔 에이전트에 포함된 프록시 서버를 사용하도록 해당 시스템을 자동으로 구성합니다. 유일한 요구 사항은 콘솔 에이전트의 보안 그룹이 포트 3128을 통한 인바운드 연결을 허용하는 것입니다. 콘솔 에이전트를 배포한 후 이 포트를 열어야 합니다.

NTP 활성화

NetApp Data Classification 사용하여 회사 데이터 소스를 스캔하려는 경우 콘솔 에이전트와 NetApp Data Classification 시스템 모두에서 NTP(네트워크 시간 프로토콜) 서비스를 활성화하여 시스템 간의 시간을 동기화해야 합니다. "NetApp 데이터 분류에 대해 자세히 알아보세요"

콘솔 에이전트를 만든 후 이 네트워킹 요구 사항을 구현합니다.

2단계**:** 콘솔 에이전트를 생성하기 위한 권한 설정

콘솔에서 콘솔 에이전트를 배포하려면 먼저 콘솔 에이전트 VM을 배포하는 Google 플랫폼 사용자의 권한을 설정해야 합니다.

단계

1. Google 플랫폼에서 사용자 지정 역할을 만듭니다.

   a. 다음 권한을 포함하는 YAML 파일을 만듭니다.

```
title: Console agent deployment policy
description: Permissions for the user who deploys the Console agent
stage: GA
includedPermissions:

- cloudbuild.builds.get
- compute.disks.create
- compute.disks.get
- compute.disks.list
- compute.disks.setLabels
- compute.disks.use
- compute.firewalls.create
- compute.firewalls.delete
- compute.firewalls.get
- compute.firewalls.list
- compute.globalOperations.get
- compute.images.get
- compute.images.getFromFamily
- compute.images.list
- compute.images.useReadOnly
- compute.instances.attachDisk
- compute.instances.create
- compute.instances.get
- compute.instances.list
- compute.instances.setDeletionProtection
```

```
- compute.instances.setLabels
- compute.instances.setMachineType
- compute.instances.setMetadata
- compute.instances.setTags
- compute.instances.start
- compute.instances.updateDisplayDevice
- compute.machineTypes.get
- compute.networks.get
- compute.networks.list
- compute.networks.updatePolicy
- compute.projects.get
- compute.regions.get
- compute.regions.list
- compute.subnetworks.get
- compute.subnetworks.list
- compute.zoneOperations.get
- compute.zones.get
- compute.zones.list
- config.deployments.create
- config.operations.get
- config.deployments.delete
- config.deployments.deleteState
- config.deployments.get
- config.deployments.getState
- config.deployments.list
- config.deployments.update
- config.deployments.updateState
- config.previews.get
- config.previews.list
- config.revisions.get
- config.resources.list
- deploymentmanager.compositeTypes.get
- deploymentmanager.compositeTypes.list
- deploymentmanager.deployments.create
- deploymentmanager.deployments.delete
- deploymentmanager.deployments.get
- deploymentmanager.deployments.list
- deploymentmanager.manifests.get
- deploymentmanager.manifests.list
- deploymentmanager.operations.get
- deploymentmanager.operations.list
- deploymentmanager.resources.get
- deploymentmanager.resources.list
- deploymentmanager.typeProviders.get
- deploymentmanager.typeProviders.list
- deploymentmanager.types.get
```

```
- deploymentmanager.types.list
- resourcemanager.projects.get
- compute.instances.setServiceAccount
- iam.serviceAccounts.actAs
- iam.serviceAccounts.create
- iam.serviceAccounts.list
- iam.serviceAccountKeys.create
- storage.buckets.create
- storage.buckets.get
- storage.objects.create
- storage.folders.create
- storage.objects.list
```

b. Google Cloud에서 Cloud Shell을 활성화합니다.

c. 필요한 권한이 포함된 YAML 파일을 업로드합니다.

d. 다음을 사용하여 사용자 정의 역할을 만듭니다. `gcloud iam roles create` 명령.

다음 예제는 프로젝트 수준에서 "agentDeployment"라는 이름의 역할을 생성합니다.

gcloud iam roles create connectorDeployment --project=myproject --file=agent-deployment.yaml

"Google Cloud 문서: 사용자 지정 역할 만들기 및 관리"

2. 콘솔이나 gcloud를 사용하여 콘솔 에이전트를 배포할 사용자에게 이 사용자 지정 역할을 할당합니다.

"Google Cloud 문서: 단일 역할 부여"

3단계**:** 에이전트와 함께 사용할 **Google Cloud** 서비스 계정을 생성합니다**.**

Google Cloud 서비스 계정은 콘솔 에이전트에 Google Cloud의 리소스를 관리하는 데 필요한 권한을 제공하는 데 필요합니다. 콘솔 에이전트를 만들 때 이 서비스 계정을 콘솔 에이전트 VM과 연결해야 합니다.

이후 릴리스에서 새로운 권한이 추가되면 사용자 지정 역할을 업데이트하는 것은 사용자의 책임입니다. 새로운 권한이 필요한 경우 릴리스 노트에 나열됩니다.

단계

1. Google Cloud에서 사용자 지정 역할을 만듭니다.

a. 내용을 포함하는 YAML 파일을 만듭니다."콘솔 에이전트에 대한 서비스 계정 권한" .

b. Google Cloud에서 Cloud Shell을 활성화합니다.

c. 필요한 권한이 포함된 YAML 파일을 업로드합니다.

d. 다음을 사용하여 사용자 정의 역할을 만듭니다. `gcloud iam roles create` 명령.

다음 예제는 프로젝트 수준에서 "agent"라는 이름의 역할을 생성합니다.

```
gcloud iam roles create connector --project=myproject --file=agent.yaml
```

"Google Cloud 문서: 사용자 지정 역할 만들기 및 관리"

2. Google Cloud에서 서비스 계정을 만들고 서비스 계정에 역할을 할당합니다.
   a. IAM 및 관리 서비스에서 *서비스 계정 > 서비스 계정 만들기*를 선택합니다.
   b. 서비스 계정 세부 정보를 입력하고 *만들기 및 계속*을 선택하세요.
   c. 방금 만든 역할을 선택하세요.
   d. 나머지 단계를 완료하여 역할을 만듭니다.

      "Google Cloud 문서: 서비스 계정 만들기"

3. 콘솔 에이전트가 있는 프로젝트와 다른 프로젝트에 Cloud Volumes ONTAP 시스템을 배포하려는 경우 콘솔 에이전트의 서비스 계정에 해당 프로젝트에 대한 액세스 권한을 제공해야 합니다.

   예를 들어, 콘솔 에이전트가 프로젝트 1에 있고 프로젝트 2에 Cloud Volumes ONTAP 시스템을 만들고 싶다고 가정해 보겠습니다. 프로젝트 2에서 서비스 계정에 대한 액세스 권한을 부여해야 합니다.

   a. IAM 및 관리 서비스에서 Cloud Volumes ONTAP 시스템을 만들려는 Google Cloud 프로젝트를 선택합니다.
   b. **IAM** 페이지에서 *액세스 권한 부여*를 선택하고 필요한 세부 정보를 제공합니다.
      - 콘솔 에이전트 서비스 계정의 이메일을 입력하세요.
      - 콘솔 에이전트의 사용자 지정 역할을 선택합니다.
      - *저장*을 선택하세요.

   자세한 내용은 다음을 참조하세요. "Google Cloud 문서"

4단계**:** 공유 **VPC** 권한 설정

공유 VPC를 사용하여 서비스 프로젝트에 리소스를 배포하는 경우 권한을 준비해야 합니다.

이 표는 참조용이며 IAM 구성이 완료되면 사용자 환경에 권한 표가 반영되어야 합니다.

공유 **VPC** 권한 보기

신원	창조자	호스팅됨	서비스 프로젝트 권한	호스트 프로젝트 권한	목적
에이전트를 배포하기 위한 Google 계정	관습	봉사 프로젝트	"에이전트 배포 정책"	컴퓨팅.네트워크사용자	서비스 프로젝트에 에이전트 배포
에이전트 서비스 계정	관습	봉사 프로젝트	"에이전트 서비스 계정 정책"	compute.network User 배포 관리자 .편집기	서비스 프로젝트에서 Cloud Volumes ONTAP 및 서비스 배포 및 유지 관리
Cloud Volumes ONTAP 서비스 계정	관습	봉사 프로젝트	storage.admin 멤버: NetApp Console 서비스 계정(serviceAccount.user)	해당 없음	(선택 사항) NetApp Cloud Tiering 및 NetApp Backup and Recovery
Google API 서비스 에이전트	구글 클라우드	봉사 프로젝트	(기본값) 편집기	컴퓨팅.네트워크사용자	배포를 대신하여 Google Cloud API와 상호 작용합니다. 콘솔이 공유 네트워크를 사용할 수 있도록 합니다.
Google Compute Engine 기본 서비스 계정	구글 클라우드	봉사 프로젝트	(기본값) 편집기	컴퓨팅.네트워크사용자	배포를 대신하여 Google Cloud 인스턴스와 컴퓨팅 인프라를 배포합니다. 콘솔이 공유 네트워크를 사용할 수 있도록 합니다.

참고사항:

1. deploymentmanager.editor는 배포에 방화벽 규칙을 전달하지 않고 콘솔에서 규칙을 생성하도록 선택한 경우에만 호스트 프로젝트에서 필요합니다. 규칙이 지정되지 않으면 NetApp Console 호스트 프로젝트에 VPC0 방화벽 규칙을 포함하는 배포를 생성합니다.
2. firewall.create와 firewall.delete는 배포에 방화벽 규칙을 전달하지 않고 콘솔에서 해당 규칙을 생성하도록 선택한 경우에만 필요합니다. 이러한 권한은 콘솔 계정의 .yaml 파일에 있습니다. 공유 VPC를 사용하여 HA 쌍을 배포하는 경우 이러한 권한은 VPC1, 2, 3에 대한 방화벽 규칙을 만드는 데 사용됩니다. 다른 모든 배포의 경우 이러한 권한은 VPC0에 대한 규칙을 만드는 데에도 사용됩니다.
3. 클라우드 계층화의 경우 계층화 서비스 계정에는 프로젝트 수준뿐만 아니라 서비스 계정에 대한 serviceAccount.user 역할이 있어야 합니다. 현재 프로젝트 수준에서 serviceAccount.user를 할당하는 경우 getIAMPolicy로 서비스 계정을 쿼리할 때 권한이 표시되지 않습니다.

5단계**: Google Cloud API** 활성화

콘솔 에이전트와 Cloud Volumes ONTAP 배포하기 전에 여러 Google Cloud API를 활성화해야 합니다.

단계

1. 프로젝트에서 다음 Google Cloud API를 활성화하세요.

- 클라우드 배포 관리자 V2 API
- 클라우드 인프라 관리자 API
- 클라우드 로깅 API
- 클라우드 리소스 관리자 API
- 컴퓨트 엔진 API
- ID 및 액세스 관리(IAM) API
- Cloud Key Management Service(KMS) API(NetApp Backup and Recovery를 고객 관리 암호화 키(CMEK)와 함께 사용할 계획인 경우에만 필요)
- Cloud Quotas API(Infrastructure Manager를 사용하는 Cloud Volumes ONTAP 배포에 필요)

"Google Cloud 문서: API 활성화"

6단계**:** 콘솔 에이전트 만들기

콘솔에서 직접 콘솔 에이전트를 만듭니다.

콘솔 에이전트를 생성하면 기본 구성을 사용하여 Google Cloud에 가상 머신 인스턴스가 배포됩니다. 콘솔 에이전트를 만든 후에는 CPU나 RAM이 적은 더 작은 VM 인스턴스로 전환하지 마세요. "콘솔 에이전트의 기본 구성에 대해 알아보세요" .

Google Cloud에 에이전트를 배포하면 에이전트가 배포 파일을 저장할 버킷을 생성합니다.

시작하기 전에

다음 사항이 있어야 합니다.

- 콘솔 에이전트와 콘솔 에이전트 VM에 대한 서비스 계정을 생성하는 데 필요한 Google Cloud 권한입니다.
- 네트워킹 요구 사항을 충족하는 VPC 및 서브넷.
- 콘솔 에이전트에서 인터넷에 접속하는 데 프록시가 필요한 경우 프록시 서버에 대한 세부 정보입니다.

단계

1. *관리 > 에이전트*를 선택하세요.
2. 개요 페이지에서 *에이전트 배포 > Google Cloud*를 선택합니다.
3. 에이전트 배치 페이지에서 필요한 사항에 대한 세부 정보를 검토하세요. 두 가지 옵션이 있습니다.
   a. 제품 내 가이드를 사용하여 배포를 준비하려면 *계속*을 선택하세요. 제품 내 가이드의 각 단계에는 이 문서 페이지에 포함된 정보가 포함되어 있습니다.
   b. 이 페이지의 단계에 따라 이미 준비가 되었다면 *배포로 건너뛰기*를 선택하세요.
4. 마법사의 단계에 따라 콘솔 에이전트를 만듭니다.
   - 메시지가 표시되면 가상 머신 인스턴스를 만드는 데 필요한 권한이 있는 Google 계정에 로그인하세요.

     이 양식은 Google에서 소유하고 호스팅합니다. 귀하의 자격 증명은 NetApp 에 제공되지 않습니다.

   - 세부 정보: 가상 머신 인스턴스의 이름을 입력하고, 태그를 지정하고, 프로젝트를 선택한 다음, 필요한 권한이 있는 서비스 계정을 선택합니다(자세한 내용은 위 섹션을 참조하세요).

- 위치: 인스턴스에 대한 지역, 영역, VPC 및 서브넷을 지정합니다.
- 네트워크: 공용 IP 주소를 사용할지 여부를 선택하고, 선택적으로 프록시 구성을 지정합니다.
- 네트워크 태그: 투명 프록시를 사용하는 경우 콘솔 에이전트 인스턴스에 네트워크 태그를 추가합니다. 네트워크 태그는 소문자로 시작해야 하며 소문자, 숫자, 하이픈을 포함할 수 있습니다. 태그는 소문자나 숫자로 끝나야 합니다. 예를 들어, "console-agent-proxy" 태그를 사용할 수 있습니다.
- 방화벽 정책: 새로운 방화벽 정책을 만들지, 아니면 필요한 인바운드 및 아웃바운드 규칙을 허용하는 기존 방화벽 정책을 선택할지 선택합니다.

  "Google Cloud의 방화벽 규칙"

5. 선택 사항을 검토하여 설정이 올바른지 확인하세요.

   a. 에이전트 구성 검증 확인란은 배포 시 콘솔에서 네트워크 연결 요구 사항을 검증하도록 기본적으로 선택되어 있습니다. 콘솔에서 에이전트를 배포하지 못하면 문제 해결에 도움이 되는 보고서가 제공됩니다. 배포가 성공하면 보고서는 제공되지 않습니다.

   아직도 사용 중이라면"이전 종료점" 에이전트 업그레이드에 사용되면 유효성 검사가 오류로 인해 실패합니다. 이를 방지하려면 유효성 검사를 건너뛰려면 확인란의 선택을 취소하세요.

6. *추가*를 선택하세요.

   에이전트는 약 10분 안에 준비됩니다. 프로세스가 완료될 때까지 페이지에 머물러 주세요.

결과

프로세스가 완료되면 콘솔 에이전트를 사용할 수 있습니다.

배포에 실패하면 콘솔에서 보고서와 로그를 다운로드하여 문제를 해결할 수 있습니다."설치 문제를 해결하는 방법을 알아보세요."

콘솔 에이전트를 생성한 동일한 Google Cloud 계정에 Google Cloud Storage 버킷이 있는 경우, 시스템 페이지에 Google Cloud Storage 시스템이 자동으로 표시됩니다. "콘솔에서 Google Cloud Storage를 관리하는 방법을 알아보세요."

Google Cloud에서 콘솔 에이전트 만들기

Google Cloud를 사용하여 Google Cloud에서 콘솔 에이전트를 만들려면 네트워킹을 설정하고, Google Cloud 권한을 준비하고, Google Cloud API를 활성화한 다음 콘솔 에이전트를 만들어야 합니다.

시작하기 전에

- 당신은 ~을 가져야합니다"콘솔 에이전트에 대한 이해" .
- 검토해야 합니다"콘솔 에이전트 제한 사항" .

1단계**:** 네트워킹 설정

콘솔 에이전트가 리소스를 관리하고 대상 네트워크와 인터넷에 연결할 수 있도록 네트워킹을 설정합니다.

VPC 및 서브넷

콘솔 에이전트를 생성할 때는 에이전트가 상주해야 하는 VPC와 서브넷을 지정해야 합니다.

대상 네트워크에 대한 연결

콘솔 에이전트를 사용하려면 시스템을 만들고 관리하려는 위치에 대한 네트워크 연결이 필요합니다. 예를 들어, Cloud Volumes ONTAP 시스템이나 온프레미스 환경의 스토리지 시스템을 만들 계획인 네트워크입니다.

아웃바운드 인터넷 접속

콘솔 에이전트를 배포하는 네트워크 위치에는 특정 엔드포인트에 연결하기 위한 아웃바운드 인터넷 연결이 있어야 합니다.

콘솔 에이전트에서 연락한 엔드포인트

콘솔 에이전트는 일상 업무를 위해 퍼블릭 클라우드 환경 내의 리소스와 프로세스를 관리하기 위해 다음 엔드포인트에 연결하기 위해 아웃바운드 인터넷 액세스가 필요합니다.

아래 나열된 엔드포인트는 모두 CNAME 항목입니다.

엔드포인트	목적
https://www.googleapis.com/compute/v1/ https://compute.googleapis.com/compute/v1 https://cloudresourcemanager.googleapis.com/v1/projects https://www.googleapis.com/compute/beta https://storage.googleapis.com/storage/v1 https://www.googleapis.com/storage/v1 https://iam.googleapis.com/v1 https://cloudkms.googleapis.com/v1 https://config.googleapis.com/v1/projects	Google Cloud에서 리소스를 관리합니다.
\ https://mysupport.netapp.com	라이선스 정보를 얻고 NetApp 지원팀에 AutoSupport 메시지를 보냅니다.
\ https://signin.b2c.netapp.com	NetApp 지원 사이트(NSS) 자격 증명을 업데이트하거나 NetApp Console 에 새로운 NSS 자격 증명을 추가합니다.
\ https://support.netapp.com	라이선스 정보를 얻고 NetApp 지원팀에 AutoSupport 메시지를 보내고 Cloud Volumes ONTAP 에 대한 소프트웨어 업데이트를 받습니다.
\ https://api.bluexp.netapp.com \ https://netapp-cloud-account.auth0.com \ https://netapp-cloud-account.us.auth0.com \ https://console.netapp.com \ https://components.console.bluexp.netapp.com \ https://cdn.auth0.com	NetApp Console 내에서 기능과 서비스를 제공합니다.

엔드포인트	목적
\ https://bluexpinfraprod.eastus2.data.azurecr.io \ https://bluexpinfraprod.azurecr.io	콘솔 에이전트 업그레이드를 위한 이미지를 얻으려면. • 새로운 에이전트를 배포할 때 유효성 검사를 통해 현재 엔드포인트에 대한 연결성을 테스트합니다. 당신이 사용하는 경우"이전 종료점" , 유효성 검사에 실패합니다. 이러한 실패를 방지하려면 유효성 검사를 건너뛰세요. 이전 엔드포인트는 계속 지원되지만 NetApp 가능한 한 빨리 현재 엔드포인트에 맞게 방화벽 규칙을 업데이트할 것을 권장합니다. "엔드포인트 목록을 업데이트하는 방법을 알아보세요" . • 방화벽의 현재 엔드포인트로 업데이트하면 기존 에이전트도 계속 작동합니다.

NetApp 콘솔에서 연결된 엔드포인트

SaaS 계층을 통해 제공되는 웹 기반 NetApp Console 사용하면 여러 엔드포인트에 연결하여 데이터 관리 작업을 완료할 수 있습니다. 여기에는 콘솔에서 콘솔 에이전트를 배포하기 위해 연결된 엔드포인트가 포함됩니다.

"NetApp 콘솔에서 연결된 엔드포인트 목록 보기" .

프록시 서버

NetApp 명시적 프록시 구성과 투명 프록시 구성을 모두 지원합니다. 투명 프록시를 사용하는 경우 프록시 서버에 대한 인증서만 제공하면 됩니다. 명시적 프록시를 사용하는 경우 IP 주소와 자격 증명도 필요합니다.

- IP 주소
- 신임장
- HTTPS 인증서

포트

Cloud Volumes ONTAP 에서 NetApp 지원팀으로 AutoSupport 메시지를 보내기 위한 프록시로 사용되거나 사용자가 시작하지 않는 한 콘솔 에이전트로 들어오는 트래픽이 없습니다.

- HTTP(80) 및 HTTPS(443)는 로컬 UI에 대한 액세스를 제공하며 이는 드문 상황에서 사용됩니다.
- SSH(22)는 문제 해결을 위해 호스트에 연결해야 하는 경우에만 필요합니다.
- 아웃바운드 인터넷 연결을 사용할 수 없는 서브넷에 Cloud Volumes ONTAP 시스템을 배포하는 경우 포트 3128을 통한 인바운드 연결이 필요합니다.

Cloud Volumes ONTAP 시스템에 AutoSupport 메시지를 보낼 아웃바운드 인터넷 연결이 없는 경우 콘솔은 콘솔 에이전트에 포함된 프록시 서버를 사용하도록 해당 시스템을 자동으로 구성합니다. 유일한 요구 사항은 콘솔 에이전트의 보안 그룹이 포트 3128을 통한 인바운드 연결을 허용하는 것입니다. 콘솔 에이전트를 배포한 후 이 포트를 열어야 합니다.

NTP 활성화

NetApp Data Classification 사용하여 회사 데이터 소스를 스캔하려는 경우 콘솔 에이전트와 NetApp Data Classification 시스템 모두에서 NTP(네트워크 시간 프로토콜) 서비스를 활성화하여 시스템 간의 시간을 동기화해야 합니다. "NetApp 데이터 분류에 대해 자세히 알아보세요"

콘솔 에이전트를 만든 후 이 네트워킹 요구 사항을 구현합니다.

2단계**:** 콘솔 에이전트를 생성하기 위한 권한 설정

Google Cloud 사용자가 Google Cloud에서 콘솔 에이전트 VM을 배포할 수 있는 권한을 설정합니다.

단계

1. Google 플랫폼에서 사용자 지정 역할을 만듭니다.

   a. 다음 권한을 포함하는 YAML 파일을 만듭니다.

```
title: Console agent deployment policy
description: Permissions for the user who deploys the Console
agent
stage: GA
includedPermissions:

- cloudbuild.builds.get
- compute.disks.create
- compute.disks.get
- compute.disks.list
- compute.disks.setLabels
- compute.disks.use
- compute.firewalls.create
- compute.firewalls.delete
- compute.firewalls.get
- compute.firewalls.list
- compute.globalOperations.get
- compute.images.get
- compute.images.getFromFamily
- compute.images.list
- compute.images.useReadOnly
- compute.instances.attachDisk
- compute.instances.create
- compute.instances.get
- compute.instances.list
- compute.instances.setDeletionProtection
- compute.instances.setLabels
- compute.instances.setMachineType
- compute.instances.setMetadata
- compute.instances.setTags
- compute.instances.start
- compute.instances.updateDisplayDevice
- compute.machineTypes.get
- compute.networks.get
- compute.networks.list
- compute.networks.updatePolicy
- compute.projects.get
- compute.regions.get
- compute.regions.list
- compute.subnetworks.get
- compute.subnetworks.list
- compute.zoneOperations.get
- compute.zones.get
- compute.zones.list
- config.deployments.create
```

```
- config.operations.get
- config.deployments.delete
- config.deployments.deleteState
- config.deployments.get
- config.deployments.getState
- config.deployments.list
- config.deployments.update
- config.deployments.updateState
- config.previews.get
- config.previews.list
- config.revisions.get
- config.resources.list
- deploymentmanager.compositeTypes.get
- deploymentmanager.compositeTypes.list
- deploymentmanager.deployments.create
- deploymentmanager.deployments.delete
- deploymentmanager.deployments.get
- deploymentmanager.deployments.list
- deploymentmanager.manifests.get
- deploymentmanager.manifests.list
- deploymentmanager.operations.get
- deploymentmanager.operations.list
- deploymentmanager.resources.get
- deploymentmanager.resources.list
- deploymentmanager.typeProviders.get
- deploymentmanager.typeProviders.list
- deploymentmanager.types.get
- deploymentmanager.types.list
- resourcemanager.projects.get
- compute.instances.setServiceAccount
- iam.serviceAccounts.actAs
- iam.serviceAccounts.create
- iam.serviceAccounts.list
- iam.serviceAccountKeys.create
- storage.buckets.create
- storage.buckets.get
- storage.objects.create
- storage.folders.create
- storage.objects.list
```

b. Google Cloud에서 Cloud Shell을 활성화합니다.

c. 필요한 권한이 포함된 YAML 파일을 업로드합니다.

d. 다음을 사용하여 사용자 정의 역할을 만듭니다. `gcloud iam roles create` 명령.

다음 예제에서는 프로젝트 수준에서 "connectorDeployment"라는 역할을 만듭니다.

gcloud iam 역할 커넥터 배포 생성 --project=myproject --file=connector-deployment.yaml

"Google Cloud 문서: 사용자 지정 역할 만들기 및 관리"

2. Google Cloud에서 콘솔 에이전트를 배포하는 사용자에게 이 사용자 지정 역할을 할당합니다.

"Google Cloud 문서: 단일 역할 부여"

3단계**:** 콘솔 에이전트 작업에 대한 권한 설정

Google Cloud 서비스 계정은 콘솔 에이전트에 Google Cloud의 리소스를 관리하는 데 필요한 권한을 제공하는 데 필요합니다. 콘솔 에이전트를 만들 때 이 서비스 계정을 콘솔 에이전트 VM과 연결해야 합니다.

이후 릴리스에서 새로운 권한이 추가되면 사용자 지정 역할을 업데이트하는 것은 사용자의 책임입니다. 새로운 권한이 필요한 경우 릴리스 노트에 나열됩니다.

단계

1. Google Cloud에서 사용자 지정 역할을 만듭니다.

   a. 내용을 포함하는 YAML 파일을 만듭니다."콘솔 에이전트에 대한 서비스 계정 권한" .

   b. Google Cloud에서 Cloud Shell을 활성화합니다.

   c. 필요한 권한이 포함된 YAML 파일을 업로드합니다.

   d. 다음을 사용하여 사용자 정의 역할을 만듭니다. `gcloud iam roles create` 명령.

   다음 예제는 프로젝트 수준에서 "agent"라는 이름의 역할을 생성합니다.

   ```
   gcloud iam roles create connector --project=myproject --file=agent.yaml
   ```

"Google Cloud 문서: 사용자 지정 역할 만들기 및 관리"

2. Google Cloud에서 서비스 계정을 만들고 서비스 계정에 역할을 할당합니다.

   a. IAM 및 관리 서비스에서 *서비스 계정 > 서비스 계정 만들기*를 선택합니다.

   b. 서비스 계정 세부 정보를 입력하고 *만들기 및 계속*을 선택하세요.

   c. 방금 만든 역할을 선택하세요.

   d. 나머지 단계를 완료하여 역할을 만듭니다.

   "Google Cloud 문서: 서비스 계정 만들기"

3. 콘솔 에이전트가 있는 프로젝트와 다른 프로젝트에 Cloud Volumes ONTAP 시스템을 배포하려는 경우 콘솔 에이전트의 서비스 계정에 해당 프로젝트에 대한 액세스 권한을 제공해야 합니다.

   예를 들어, 콘솔 에이전트가 프로젝트 1에 있고 프로젝트 2에 Cloud Volumes ONTAP 시스템을 만들고 싶다고 가정해 보겠습니다. 프로젝트 2에서 서비스 계정에 대한 액세스 권한을 부여해야 합니다.

   a. IAM 및 관리 서비스에서 Cloud Volumes ONTAP 시스템을 만들려는 Google Cloud 프로젝트를 선택합니다.

   b. **IAM** 페이지에서 *액세스 권한 부여*를 선택하고 필요한 세부 정보를 제공합니다.

- 콘솔 에이전트 서비스 계정의 이메일을 입력하세요.
- 콘솔 에이전트의 사용자 지정 역할을 선택합니다.
- *저장*을 선택하세요.

자세한 내용은 다음을 참조하세요. "Google Cloud 문서"

4단계**:** 공유 **VPC** 권한 설정

공유 VPC를 사용하여 서비스 프로젝트에 리소스를 배포하는 경우 권한을 준비해야 합니다.

이 표는 참조용이며 IAM 구성이 완료되면 사용자 환경에 권한 표가 반영되어야 합니다.

공유 **VPC** 권한 보기

신원	창조자	호스팅됨	서비스 프로젝트 권한	호스트 프로젝트 권한	목적
에이전트를 배포하기 위한 Google 계정	관습	봉사 프로젝트	"에이전트 배포 정책"	컴퓨팅.네트워크사용자	서비스 프로젝트에 에이전트 배포
에이전트 서비스 계정	관습	봉사 프로젝트	"에이전트 서비스 계정 정책"	compute.network User 배포 관리자 .편집기	서비스 프로젝트에서 Cloud Volumes ONTAP 및 서비스 배포 및 유지 관리
Cloud Volumes ONTAP 서비스 계정	관습	봉사 프로젝트	storage.admin 멤버: NetApp Console 서비스 계정(serviceAccount.user)	해당 없음	(선택 사항) NetApp Cloud Tiering 및 NetApp Backup and Recovery
Google API 서비스 에이전트	구글 클라우드	봉사 프로젝트	(기본값) 편집기	컴퓨팅.네트워크사용자	배포를 대신하여 Google Cloud API와 상호 작용합니다. 콘솔이 공유 네트워크를 사용할 수 있도록 합니다.
Google Compute Engine 기본 서비스 계정	구글 클라우드	봉사 프로젝트	(기본값) 편집기	컴퓨팅.네트워크사용자	배포를 대신하여 Google Cloud 인스턴스와 컴퓨팅 인프라를 배포합니다. 콘솔이 공유 네트워크를 사용할 수 있도록 합니다.

참고사항:

1. deploymentmanager.editor는 배포에 방화벽 규칙을 전달하지 않고 콘솔에서 규칙을 생성하도록 선택한 경우에만 호스트 프로젝트에서 필요합니다. 규칙이 지정되지 않으면 NetApp Console 호스트 프로젝트에 VPC0 방화벽 규칙을 포함하는 배포를 생성합니다.
2. firewall.create와 firewall.delete는 배포에 방화벽 규칙을 전달하지 않고 콘솔에서 해당 규칙을 생성하도록 선택한 경우에만 필요합니다. 이러한 권한은 콘솔 계정의 .yaml 파일에 있습니다. 공유 VPC를 사용하여 HA 쌍을 배포하는 경우 이러한 권한은 VPC1, 2, 3에 대한 방화벽 규칙을 만드는 데 사용됩니다. 다른 모든 배포의 경우 이러한 권한은 VPC0에 대한 규칙을 만드는 데에도 사용됩니다.
3. 클라우드 계층화의 경우 계층화 서비스 계정에는 프로젝트 수준뿐만 아니라 서비스 계정에 대한 serviceAccount.user 역할이 있어야 합니다. 현재 프로젝트 수준에서 serviceAccount.user를 할당하는 경우 getIAMPolicy로 서비스 계정을 쿼리할 때 권한이 표시되지 않습니다.

5단계**: Google Cloud API** 활성화

콘솔 에이전트와 Cloud Volumes ONTAP 배포하기 전에 여러 Google Cloud API를 활성화합니다.

단계

1. 프로젝트에서 다음 Google Cloud API를 활성화하세요.

- 클라우드 배포 관리자 V2 API
- 클라우드 인프라 관리자 API
- 클라우드 로깅 API
- 클라우드 리소스 관리자 API
- 컴퓨트 엔진 API
- ID 및 액세스 관리(IAM) API
- Cloud Key Management Service(KMS) API(NetApp Backup and Recovery를 고객 관리 암호화 키(CMEK)와 함께 사용할 계획인 경우에만 필요)
- Cloud Quotas API(Infrastructure Manager를 사용하는 Cloud Volumes ONTAP 배포에 필요)

"Google Cloud 문서: API 활성화"

6단계**:** 콘솔 에이전트 만들기

Google Cloud를 사용하여 콘솔 에이전트를 만듭니다.

콘솔 에이전트를 생성하면 기본 구성으로 Google Cloud에 VM 인스턴스가 배포됩니다. 콘솔 에이전트를 만든 후에는 CPU나 RAM이 적은 더 작은 VM 인스턴스로 전환하지 마세요. "콘솔 에이전트의 기본 구성에 대해 알아보세요" .

시작하기 전에

다음 사항이 있어야 합니다.

- 콘솔 에이전트와 콘솔 에이전트 VM에 대한 서비스 계정을 생성하는 데 필요한 Google Cloud 권한입니다.
- 네트워킹 요구 사항을 충족하는 VPC 및 서브넷.
- VM 인스턴스 요구 사항에 대한 이해.
  - **CPU**: 8개 코어 또는 8개 vCPU
  - 램: 32GB
  - 기계 유형: n2-standard-8을 권장합니다.

    콘솔 에이전트는 보호된 VM 기능을 지원하는 OS가 있는 VM 인스턴스의 Google Cloud에서 지원됩니다.

단계

1. 원하는 방법을 사용하여 Google Cloud SDK에 로그인하세요.

   이 예제에서는 gcloud SDK가 설치된 로컬 셸을 사용하지만 Google Cloud Shell을 사용할 수도 있습니다.

   Google Cloud SDK에 대한 자세한 내용은 다음을 참조하세요."Google Cloud SDK 문서 페이지" .

2. 위 섹션에 정의된 필수 권한이 있는 사용자로 로그인했는지 확인하세요.

   ```
   gcloud auth list
   ```

   출력에는 다음과 같은 내용이 표시되어야 합니다. 여기서 * 사용자 계정은 로그인에 사용할 사용자 계정입니다.

```
Credentialed Accounts
ACTIVE  ACCOUNT
     some_user_account@domain.com
*    desired_user_account@domain.com
To set the active account, run:
 $ gcloud config set account `ACCOUNT`
Updates are available for some Cloud SDK components. To install them,
please run:
$ gcloud components update
```

3. 실행하다 `gcloud compute instances create` 명령:

```
gcloud compute instances create <instance-name>
  --machine-type=n2-standard-8
  --image-project=netapp-cloudmanager
  --image-family=cloudmanager
  --scopes=cloud-platform
  --project=<project>
  --service-account=<service-account>
  --zone=<zone>
  --no-address
  --tags <network-tag>
  --network <network-path>
  --subnet <subnet-path>
  --boot-disk-kms-key <kms-key-path>
```

인스턴스 이름
: VM 인스턴스에 대한 원하는 인스턴스 이름입니다.

프로젝트
: (선택 사항) VM을 배포할 프로젝트입니다.

서비스 계정
: 2단계의 출력에 지정된 서비스 계정입니다.

존
: VM을 배포하려는 영역

주소 없음
: (선택 사항) 외부 IP 주소가 사용되지 않습니다(트래픽을 공용 인터넷으로 라우팅하려면 클라우드 NAT 또는 프록시가 필요함)

네트워크 태그
: (선택 사항) 태그를 사용하여 방화벽 규칙을 콘솔 에이전트 인스턴스에 연결하기 위해 네트워크 태그를 추가합니다.

네트워크 경로

(선택 사항) 콘솔 에이전트를 배포할 네트워크 이름을 추가합니다(공유 VPC의 경우 전체 경로가 필요함)

서브넷 경로

(선택 사항) 콘솔 에이전트를 배포할 서브넷 이름을 추가합니다(공유 VPC의 경우 전체 경로가 필요함)

kms-키**-**경로

(선택 사항) 콘솔 에이전트의 디스크를 암호화하기 위해 KMS 키를 추가합니다(IAM 권한도 적용해야 함)

이러한 플래그에 대한 자세한 내용은 다음을 방문하세요."Google Cloud Compute SDK 문서" .

명령을 실행하면 콘솔 에이전트가 배포됩니다. 콘솔 에이전트 인스턴스와 소프트웨어는 약 5분 안에 실행될 것입니다.

4. 웹 브라우저를 열고 콘솔 에이전트 호스트 URL을 입력하세요.

   콘솔 호스트 URL은 호스트 구성에 따라 로컬호스트, 개인 IP 주소 또는 공용 IP 주소가 될 수 있습니다. 예를 들어, 콘솔 에이전트가 공용 IP 주소가 없는 퍼블릭 클라우드에 있는 경우 콘솔 에이전트 호스트에 연결된 호스트의 개인 IP 주소를 입력해야 합니다.

5. 로그인 후 콘솔 에이전트를 설정하세요.

   a. 콘솔 에이전트와 연결할 콘솔 조직을 지정합니다.

      "ID 및 액세스 관리에 대해 알아보세요" .

   b. 시스템 이름을 입력하세요.

결과

이제 콘솔 에이전트가 설치되고 콘솔 조직에 설정되었습니다.

웹 브라우저를 열고 이동하세요 "NetApp Console" 콘솔 에이전트를 사용하려면.

Google Cloud에 콘솔 에이전트를 수동으로 설치합니다**.**

Linux 호스트에 콘솔 에이전트를 수동으로 설치하려면 호스트 요구 사항을 검토하고, 네트워킹을 설정하고, Google Cloud 권한을 준비하고, Google Cloud API를 활성화하고, 콘솔을 설치한 다음, 준비한 권한을 제공해야 합니다.

시작하기 전에

- 당신은 ~을 가져야합니다"콘솔 에이전트에 대한 이해" .
- 검토해야 합니다"콘솔 에이전트 제한 사항" .

1단계**:** 호스트 요구 사항 검토

콘솔 에이전트 소프트웨어는 특정 운영 체제 요구 사항, RAM 요구 사항, 포트 요구 사항 등을 충족하는 호스트에서 실행되어야 합니다.

콘솔 에이전트는 UID와 GID 범위를 19000~19200으로 예약합니다. 이 범위는 고정되어 있으며 수정할 수 없습니다. 호스트의 타사 소프트웨어가 이 범위 내의 UID나 GID를 사용하는 경우 에이전트 설치가 실패합니다. NetApp 충돌을 피하기 위해 타사 소프트웨어가 없는 호스트를 사용할 것을 권장합니다.

전담 호스트

콘솔 에이전트를 실행하려면 전용 호스트가 필요합니다. 다음의 크기 요건을 충족하는 모든 아키텍처가 지원됩니다.

- CPU: 8개 코어 또는 8개 vCPU
- 램: 32GB
- 디스크 공간: 호스트에 권장되는 디스크 공간은 165GB이며, 다음 파티션 요구 사항이 적용됩니다.
  - `/opt`: 120GiB의 공간이 사용 가능해야 합니다.

    에이전트는 다음을 사용합니다. `/opt` 설치하려면 `/opt/application/netapp` 디렉토리와 그 내용.
  - `/var`: 40GiB의 공간이 사용 가능해야 합니다.

    콘솔 에이전트는 다음 공간이 필요합니다. `/var` Podman이나 Docker는 컨테이너를 이 디렉터리 내에 생성하도록 설계되었기 때문입니다. 구체적으로, 그들은 컨테이너를 생성할 것입니다. `/var/lib/containers/storage` 디렉토리 및 `/var/lib/docker` Docker용입니다. 이 공간에서는 외부 마운트나 심볼릭 링크가 작동하지 않습니다.

Google Cloud 머신 유형

CPU 및 RAM 요구 사항을 충족하는 인스턴스 유형입니다. NetApp n2-standard-8을 권장합니다.

콘솔 에이전트는 OS가 있는 VM 인스턴스의 Google Cloud에서 지원됩니다. "보호된 VM 기능"

하이퍼바이저

지원되는 운영 체제를 실행하도록 인증된 베어 메탈 또는 호스팅 하이퍼바이저가 필요합니다.

운영 체제 및 컨테이너 요구 사항

콘솔 에이전트는 표준 모드 또는 제한 모드에서 콘솔을 사용할 때 다음 운영 체제에서 지원됩니다. 에이전트를 설치하기 전에 컨테이너 오케스트레이션 도구가 필요합니다.

운영 체제	지원되는 **OS** 버전	지원되는 에이전트 버전	필수 컨테이너 도구	셀리눅스
레드햇 엔터프라이즈 리눅스		9.6 • 영어 버전만 제공됩니다. • 호스트는 Red Hat Subscription Management에 등록되어야 합니다. 등록되지 않은 경우 호스트는 에이전트 설치 중에 필요한 타사 소프트웨어를 업데이트하기 위해 저장소에 액세스할 수 없습니다.	4.0.0 이상, 콘솔이 표준 모드 또는 제한 모드인 경우	Podman 버전 5.4.0과 podman-compose 1.5.0. Podman 구성 요구 사항 보기 .
강제 모드 또는 허용 모드에서 지원됨		9.1에서 9.4까지 • 영어 버전만 제공됩니다. • 호스트는 Red Hat Subscription Management에 등록되어야 합니다. 등록되지 않은 경우 호스트는 에이전트 설치 중에 필요한 타사 소프트웨어를 업데이트하기 위해 저장소에 액세스할 수 없습니다.	3.9.50 이상, 콘솔이 표준 모드 또는 제한 모드인 경우	Podman 버전 4.9.4와 podman-compose 1.5.0. Podman 구성 요구 사항 보기 .

운영 체제	지원되는 **OS** 버전	지원되는 에이전트 버전	필수 컨테이너 도구	셀리눅스
강제 모드 또는 허용 모드에서 지원됨		8.6에서 8.10까지 • 영어 버전만 제공됩니다. • 호스트는 Red Hat Subscription Management에 등록되어야 합니다. 등록되지 않은 경우 호스트는 에이전트 설치 중에 필요한 타사 소프트웨어를 업데이트하기 위해 저장소에 액세스할 수 없습니다.	3.9.50 이상, 콘솔이 표준 모드 또는 제한 모드인 경우	Podman 버전 4.6.1 또는 4.9.4와 podman-compose 1.0.6. Podman 구성 요구 사항 보기 .
강제 모드 또는 허용 모드에서 지원됨	우분투		24.04 장기	표준 모드 또는 제한 모드에서 NetApp Console 사용하는 3.9.45 이상
Docker 엔진 23.06~28.0.0.	지원되지 않음		22.04 장기	3.9.50 이상

Google Cloud 머신 유형

CPU 및 RAM 요구 사항을 충족하는 인스턴스 유형입니다. NetApp n2-standard-8을 권장합니다.

콘솔 에이전트는 OS가 있는 VM 인스턴스의 Google Cloud에서 지원됩니다. "보호된 VM 기능"

2단계**: Podman** 또는 **Docker Engine** 설치

운영 체제에 따라 에이전트를 설치하기 전에 Podman 또는 Docker Engine이 필요합니다.

- Red Hat Enterprise Linux 8 및 9에는 Podman이 필요합니다.

  지원되는 Podman 버전 보기 .

- Ubuntu에는 Docker 엔진이 필요합니다.

  지원되는 Docker Engine 버전 보기 .

예 **3.** 단계

포드만

Podman을 설치하고 구성하려면 다음 단계를 따르세요.

- podman.socket 서비스를 활성화하고 시작합니다.
- python3 설치
- podman-compose 패키지 버전 1.0.6을 설치하세요
- PATH 환경 변수에 podman-compose를 추가합니다.
- Red Hat Enterprise Linux를 사용하는 경우 Podman 버전이 CNI 대신 Netavark Aardvark DNS를 사용하는지 확인하십시오.

DNS 포트 충돌을 피하기 위해 에이전트를 설치한 후 aardvark-dns 포트(기본값: 53)를 조정하세요. 지침에 따라 포트를 구성하세요.

단계

1. 호스트에 podman-docker 패키지가 설치되어 있다면 제거합니다.

```
dnf remove podman-docker
rm /var/run/docker.sock
```

2. Podman을 설치하세요.

   공식 Red Hat Enterprise Linux 저장소에서 Podman을 다운로드할 수 있습니다.

   a. Red Hat Enterprise Linux 9.6의 경우:

   ```
   sudo dnf install podman-5:<version>
   ```

   여기서 <버전>은 설치하려는 Podman의 지원되는 버전입니다. 지원되는 Podman 버전 보기 .

   b. Red Hat Enterprise Linux 9.1~9.4 버전의 경우:

   ```
   sudo dnf install podman-4:<version>
   ```

   여기서 <버전>은 설치하려는 Podman의 지원되는 버전입니다. 지원되는 Podman 버전 보기 .

   c. Red Hat Enterprise Linux 8의 경우:

   ```
   sudo dnf install podman-4:<version>
   ```

   여기서 <버전>은 설치하려는 Podman의 지원되는 버전입니다. 지원되는 Podman 버전 보기 .

3. podman.socket 서비스를 활성화하고 시작합니다.

```
sudo systemctl enable --now podman.socket
```

4. python3를 설치합니다.

```
sudo dnf install python3
```

5. 시스템에 EPEL 저장소 패키지가 아직 없으면 설치하세요.

   이 단계는 podman-compose가 EPEL(Enterprise Linux용 추가 패키지) 저장소에서 사용 가능하기 때문에 필요합니다.

6. Red Hat Enterprise 9를 사용하는 경우:

   a. EPEL 저장소 패키지를 설치하세요.

```
sudo dnf install https://dl.fedoraproject.org/pub/epel/epel-release-latest-9.noarch.rpm
```

   +

   a. podman-compose 패키지 1.5.0을 설치합니다.

```
sudo dnf install podman-compose-1.5.0
```

7. Red Hat Enterprise Linux 8을 사용하는 경우:

   a. EPEL 저장소 패키지를 설치하세요.

```
sudo dnf install https://dl.fedoraproject.org/pub/epel/epel-release-latest-8.noarch.rpm
```

   b. podman-compose 패키지 1.0.6을 설치합니다.

```
sudo dnf install podman-compose-1.0.6
```

> ⓘ 를 사용하여 `dnf install` 명령은 PATH 환경 변수에 podman-compose를 추가하는 요구 사항을 충족합니다. 설치 명령은 이미 포함되어 있는 /usr/bin에 podman-compose를 추가합니다. `secure_path` 호스트의 옵션.

   c. Red Hat Enterprise Linux 8을 사용하는 경우 Podman 버전이 CNI 대신 Aardvark DNS와 함께 NetAvark를 사용하는지 확인하세요.

i. 다음 명령을 실행하여 networkBackend가 CNI로 설정되어 있는지 확인하세요.

```
podman info | grep networkBackend
```

ii. networkBackend가 설정된 경우 `CNI` , 당신은 그것을 변경해야 합니다 `netavark` .

iii. 설치하다 `netavark` 그리고 `aardvark-dns` 다음 명령을 사용합니다.

```
dnf install aardvark-dns netavark
```

iv. 열기 `/etc/containers/containers.conf` 파일을 열고 network_backend 옵션을 "cni" 대신 "netavark"를 사용하도록 수정합니다.

만약에 `/etc/containers/containers.conf` 존재하지 않습니다. 구성을 변경하세요. `/usr/share/containers/containers.conf` .

v. Podman을 다시 시작하세요.

```
systemctl restart podman
```

vi. 다음 명령을 사용하여 networkBackend가 이제 "netavark"로 변경되었는지 확인하세요.

```
podman info | grep networkBackend
```

도커 엔진

Docker Engine을 설치하려면 Docker 설명서를 따르세요.

단계

1. "Docker에서 설치 지침 보기"

   지원되는 Docker Engine 버전을 설치하려면 다음 단계를 따르세요. 콘솔에서 지원되지 않으므로 최신 버전을 설치하지 마세요.

2. Docker가 활성화되어 실행 중인지 확인하세요.

```
sudo systemctl enable docker && sudo systemctl start docker
```

3단계**:** 네트워킹 설정

하이브리드 클라우드 환경 내에서 콘솔 에이전트가 리소스와 프로세스를 관리할 수 있도록 네트워킹을 설정합니다. 예를 들어, 대상 네트워크에 연결이 가능한지, 아웃바운드 인터넷 접속이 가능한지 확인해야 합니다.

대상 네트워크에 대한 연결

콘솔 에이전트를 사용하려면 시스템을 만들고 관리하려는 위치에 대한 네트워크 연결이 필요합니다. 예를 들어, Cloud Volumes ONTAP 시스템이나 온프레미스 환경의 스토리지 시스템을 만들 계획인 네트워크입니다.

아웃바운드 인터넷 접속

콘솔 에이전트를 배포하는 네트워크 위치에는 특정 엔드포인트에 연결하기 위한 아웃바운드 인터넷 연결이 있어야 합니다.

웹 기반 **NetApp Console** 사용할 때 컴퓨터에서 연결된 엔드포인트

웹 브라우저에서 콘솔에 액세스하는 컴퓨터는 여러 엔드포인트에 접속할 수 있어야 합니다. 콘솔 에이전트를 설정하고 콘솔을 일상적으로 사용하려면 콘솔을 사용해야 합니다.

"NetApp 콘솔을 위한 네트워킹 준비" .

콘솔 에이전트에서 연락한 엔드포인트

콘솔 에이전트는 일상 업무를 위해 퍼블릭 클라우드 환경 내의 리소스와 프로세스를 관리하기 위해 다음 엔드포인트에 연결하기 위해 아웃바운드 인터넷 액세스가 필요합니다.

아래 나열된 엔드포인트는 모두 CNAME 항목입니다.

엔드포인트	목적
https://www.googleapis.com/compute/v1/ https://compute.googleapis.com/compute/v1 https://cloudresourcemanager.googleapis.com/v1/projects https://www.googleapis.com/compute/beta https://storage.googleapis.com/storage/v1 https://www.googleapis.com/storage/v1 https://iam.googleapis.com/v1 https://cloudkms.googleapis.com/v1 https://config.googleapis.com/v1/projects	Google Cloud에서 리소스를 관리합니다.
\ https://mysupport.netapp.com	라이선스 정보를 얻고 NetApp 지원팀에 AutoSupport 메시지를 보냅니다.
\ https://signin.b2c.netapp.com	NetApp 지원 사이트(NSS) 자격 증명을 업데이트하거나 NetApp Console 에 새로운 NSS 자격 증명을 추가합니다.
\ https://support.netapp.com	라이선스 정보를 얻고 NetApp 지원팀에 AutoSupport 메시지를 보내고 Cloud Volumes ONTAP 에 대한 소프트웨어 업데이트를 받습니다.

엔드포인트	목적
\ https://api.bluexp.netapp.com \ https://netapp-cloud-account.auth0.com \ https://netapp-cloud-account.us.auth0.com \ https://console.netapp.com \ https://components.console.bluexp.netapp.com \ https://cdn.auth0.com	NetApp Console 내에서 기능과 서비스를 제공합니다.
\ https://bluexpinfraprod.eastus2.data.azurecr.io \ https://bluexpinfraprod.azurecr.io	콘솔 에이전트 업그레이드를 위한 이미지를 얻으려면. • 새로운 에이전트를 배포할 때 유효성 검사를 통해 현재 엔드포인트에 대한 연결성을 테스트합니다. 당신이 사용하는 경우"이전 종료점" , 유효성 검사에 실패합니다. 이러한 실패를 방지하려면 유효성 검사를 건너뛰세요. 이전 엔드포인트는 계속 지원되지만 NetApp 가능한 한 빨리 현재 엔드포인트에 맞게 방화벽 규칙을 업데이트할 것을 권장합니다. "엔드포인트 목록을 업데이트하는 방법을 알아보세요" . • 방화벽의 현재 엔드포인트로 업데이트하면 기존 에이전트도 계속 작동합니다.

프록시 서버

NetApp 명시적 프록시 구성과 투명 프록시 구성을 모두 지원합니다. 투명 프록시를 사용하는 경우 프록시 서버에 대한 인증서만 제공하면 됩니다. 명시적 프록시를 사용하는 경우 IP 주소와 자격 증명도 필요합니다.

- IP 주소
- 신임장
- HTTPS 인증서

포트

Cloud Volumes ONTAP 에서 NetApp 지원팀으로 AutoSupport 메시지를 보내기 위한 프록시로 사용되거나 사용자가 시작하지 않는 한 콘솔 에이전트로 들어오는 트래픽이 없습니다.

- HTTP(80) 및 HTTPS(443)는 로컬 UI에 대한 액세스를 제공하며 이는 드문 상황에서 사용됩니다.
- SSH(22)는 문제 해결을 위해 호스트에 연결해야 하는 경우에만 필요합니다.
- 아웃바운드 인터넷 연결을 사용할 수 없는 서브넷에 Cloud Volumes ONTAP 시스템을 배포하는 경우 포트 3128을 통한 인바운드 연결이 필요합니다.

Cloud Volumes ONTAP 시스템에 AutoSupport 메시지를 보낼 아웃바운드 인터넷 연결이 없는 경우 콘솔은 콘솔 에이전트에 포함된 프록시 서버를 사용하도록 해당 시스템을 자동으로 구성합니다. 유일한 요구 사항은 콘솔 에이전트의 보안 그룹이 포트 3128을 통한 인바운드 연결을 허용하는 것입니다. 콘솔 에이전트를 배포한 후 이 포트를 열어야 합니다.

NTP 활성화

NetApp Data Classification 사용하여 회사 데이터 소스를 스캔하려는 경우 콘솔 에이전트와 NetApp Data Classification 시스템 모두에서 NTP(네트워크 시간 프로토콜) 서비스를 활성화하여 시스템 간의 시간을 동기화해야 합니다. "NetApp 데이터 분류에 대해 자세히 알아보세요"

4단계**:** 콘솔 에이전트에 대한 권한 설정

Google Cloud 서비스 계정은 콘솔 에이전트에 Google Cloud의 리소스를 관리하는 데 필요한 권한을 제공하는 데 필요합니다. 콘솔 에이전트를 만들 때 이 서비스 계정을 콘솔 에이전트 VM과 연결해야 합니다.

이후 릴리스에서 새로운 권한이 추가되면 사용자 지정 역할을 업데이트하는 것은 사용자의 책임입니다. 새로운 권한이 필요한 경우 릴리스 노트에 나열됩니다.

단계

1. Google Cloud에서 사용자 지정 역할을 만듭니다.

   a. 내용을 포함하는 YAML 파일을 만듭니다."콘솔 에이전트에 대한 서비스 계정 권한" .

   b. Google Cloud에서 Cloud Shell을 활성화합니다.

   c. 필요한 권한이 포함된 YAML 파일을 업로드합니다.

   d. 다음을 사용하여 사용자 정의 역할을 만듭니다. `gcloud iam roles create` 명령.

      다음 예제는 프로젝트 수준에서 "agent"라는 이름의 역할을 생성합니다.

      ```
      gcloud iam roles create connector --project=myproject --file=agent.yaml
      ```

   "Google Cloud 문서: 사용자 지정 역할 만들기 및 관리"

2. Google Cloud에서 서비스 계정을 만들고 서비스 계정에 역할을 할당합니다.

   a. IAM 및 관리 서비스에서 *서비스 계정 > 서비스 계정 만들기*를 선택합니다.

   b. 서비스 계정 세부 정보를 입력하고 *만들기 및 계속*을 선택하세요.

   c. 방금 만든 역할을 선택하세요.

   d. 나머지 단계를 완료하여 역할을 만듭니다.

      "Google Cloud 문서: 서비스 계정 만들기"

3. 콘솔 에이전트가 있는 프로젝트와 다른 프로젝트에 Cloud Volumes ONTAP 시스템을 배포하려는 경우 콘솔 에이전트의 서비스 계정에 해당 프로젝트에 대한 액세스 권한을 제공해야 합니다.

   예를 들어, 콘솔 에이전트가 프로젝트 1에 있고 프로젝트 2에 Cloud Volumes ONTAP 시스템을 만들고 싶다고 가정해 보겠습니다. 프로젝트 2에서 서비스 계정에 대한 액세스 권한을 부여해야 합니다.

   a. IAM 및 관리 서비스에서 Cloud Volumes ONTAP 시스템을 만들려는 Google Cloud 프로젝트를 선택합니다.

b. **IAM** 페이지에서 *액세스 권한 부여*를 선택하고 필요한 세부 정보를 제공합니다.
   - 콘솔 에이전트 서비스 계정의 이메일을 입력하세요.
   - 콘솔 에이전트의 사용자 지정 역할을 선택합니다.
   - *저장*을 선택하세요.

자세한 내용은 다음을 참조하세요. "Google Cloud 문서"

5단계**:** 공유 **VPC** 권한 설정

공유 VPC를 사용하여 서비스 프로젝트에 리소스를 배포하는 경우 권한을 준비해야 합니다.

이 표는 참조용이며 IAM 구성이 완료되면 사용자 환경에 권한 표가 반영되어야 합니다.

공유 **VPC** 권한 보기

신원	창조자	호스팅됨	서비스 프로젝트 권한	호스트 프로젝트 권한	목적
에이전트를 배포하기 위한 Google 계정	관습	봉사 프로젝트	"에이전트 배포 정책"	컴퓨팅.네트워크사용자	서비스 프로젝트에 에이전트 배포
에이전트 서비스 계정	관습	봉사 프로젝트	"에이전트 서비스 계정 정책"	compute.network User 배포 관리자 .편집기	서비스 프로젝트에서 Cloud Volumes ONTAP 및 서비스 배포 및 유지 관리
Cloud Volumes ONTAP 서비스 계정	관습	봉사 프로젝트	storage.admin 멤버: NetApp Console 서비스 계정(serviceAccount.user)	해당 없음	(선택 사항) NetApp Cloud Tiering 및 NetApp Backup and Recovery
Google API 서비스 에이전트	구글 클라우드	봉사 프로젝트	(기본값) 편집기	컴퓨팅.네트워크사용자	배포를 대신하여 Google Cloud API와 상호 작용합니다. 콘솔이 공유 네트워크를 사용할 수 있도록 합니다.
Google Compute Engine 기본 서비스 계정	구글 클라우드	봉사 프로젝트	(기본값) 편집기	컴퓨팅.네트워크사용자	배포를 대신하여 Google Cloud 인스턴스와 컴퓨팅 인프라를 배포합니다. 콘솔이 공유 네트워크를 사용할 수 있도록 합니다.

참고사항:

1. deploymentmanager.editor는 배포에 방화벽 규칙을 전달하지 않고 콘솔에서 규칙을 생성하도록 선택한 경우에만 호스트 프로젝트에서 필요합니다. 규칙이 지정되지 않으면 NetApp Console 호스트 프로젝트에 VPC0 방화벽 규칙을 포함하는 배포를 생성합니다.
2. firewall.create와 firewall.delete는 배포에 방화벽 규칙을 전달하지 않고 콘솔에서 해당 규칙을 생성하도록 선택한 경우에만 필요합니다. 이러한 권한은 콘솔 계정의 .yaml 파일에 있습니다. 공유 VPC를 사용하여 HA 쌍을 배포하는 경우 이러한 권한은 VPC1, 2, 3에 대한 방화벽 규칙을 만드는 데 사용됩니다. 다른 모든 배포의 경우 이러한 권한은 VPC0에 대한 규칙을 만드는 데에도 사용됩니다.
3. 클라우드 계층화의 경우 계층화 서비스 계정에는 프로젝트 수준뿐만 아니라 서비스 계정에 대한 serviceAccount.user 역할이 있어야 합니다. 현재 프로젝트 수준에서 serviceAccount.user를 할당하는 경우 getIAMPolicy로 서비스 계정을 쿼리할 때 권한이 표시되지 않습니다.

6단계**: Google Cloud API** 활성화

Google Cloud에 콘솔 에이전트를 배포하려면 먼저 몇 가지 Google Cloud API를 사용 설정해야 합니다.

단계

1. 프로젝트에서 다음 Google Cloud API를 활성화하세요.

- 클라우드 배포 관리자 V2 API
- 클라우드 인프라 관리자 API
- 클라우드 로깅 API
- 클라우드 리소스 관리자 API
- 컴퓨트 엔진 API
- ID 및 액세스 관리(IAM) API
- Cloud Key Management Service(KMS) API(NetApp Backup and Recovery를 고객 관리 암호화 키(CMEK)와 함께 사용할 계획인 경우에만 필요)
- Cloud Quotas API(Infrastructure Manager를 사용하는 Cloud Volumes ONTAP 배포에 필요)

"Google Cloud 문서: API 활성화"

7단계**:** 콘솔 에이전트 설치

필수 구성 요소를 모두 완료한 후에는 Linux 호스트에 소프트웨어를 수동으로 설치할 수 있습니다.

에이전트를 배포하면 시스템에서 배포 파일을 저장할 Google Cloud 버킷도 생성합니다.

시작하기 전에

다음 사항이 있어야 합니다.

- 콘솔 에이전트를 설치하려면 루트 권한이 필요합니다.
- 콘솔 에이전트에서 인터넷에 접속하는 데 프록시가 필요한 경우 프록시 서버에 대한 세부 정보입니다.

  설치 후 프록시 서버를 구성할 수 있지만, 그렇게 하려면 콘솔 에이전트를 다시 시작해야 합니다.

- 프록시 서버가 HTTPS를 사용하거나 프록시가 가로채기 프록시인 경우 CA 서명 인증서가 필요합니다.

> 콘솔 에이전트를 수동으로 설치하는 경우 투명 프록시 서버에 대한 인증서를 설정할 수 없습니다. 투명 프록시 서버에 대한 인증서를 설정해야 하는 경우 설치 후 유지 관리 콘솔을 사용해야 합니다. 자세히 알아보세요"에이전트 유지 관리 콘솔" .

이 작업에 관하여

설치 후, 새로운 버전이 나오면 콘솔 에이전트가 자동으로 업데이트됩니다.

단계

1. 호스트에 *http_proxy* 또는 *https_proxy* 시스템 변수가 설정되어 있으면 제거합니다.

   ```
   unset http_proxy
   unset https_proxy
   ```

   이러한 시스템 변수를 제거하지 않으면 설치가 실패합니다.

2. 콘솔 에이전트 소프트웨어를 다운로드한 다음 Linux 호스트에 복사하십시오. NetApp Console 또는 NetApp 지원 사이트에서 다운로드할 수 있습니다.

- NetApp Console: *에이전트 > 관리 > 에이전트 배포 > 온프레미스 > 수동 설치*로 이동합니다.

  에이전트 설치 파일 다운로드 또는 파일 URL 다운로드를 선택하십시오.

- NetApp 지원 사이트 (콘솔에 대한 액세스 권한이 없는 경우 필요) "NetApp 지원 사이트" ,

3. 스크립트를 실행할 수 있는 권한을 할당합니다.

```
chmod +x NetApp_Console_Agent_Cloud_<version>
```

여기서 <버전>은 다운로드한 콘솔 에이전트의 버전입니다.

4. 정부 클라우드 환경에 설치하는 경우 구성 검사를 비활성화하세요."수동 설치에 대한 구성 검사를 비활성화하는 방법을 알아보세요."
5. 설치 스크립트를 실행합니다.

```
./NetApp_Console_Agent_Cloud_<version> --proxy <HTTP or HTTPS proxy
server> --cacert <path and file name of a CA-signed certificate>
```

네트워크에서 인터넷 접속을 위해 프록시가 필요한 경우 프록시 정보를 추가해야 합니다. 설치 중에 명시적 프록시를 추가할 수 있습니다. `--proxy` 및 `--cacert` 매개변수는 선택 사항이며 추가하라는 메시지가 표시되지 않습니다. 명시적 프록시 서버가 있는 경우 표시된 대로 매개변수를 입력해야 합니다.

투명 프록시를 구성하려면 설치 후에 구성하면 됩니다. "에이전트 유지 관리 콘솔에 대해 알아보세요"

+

다음은 CA 서명 인증서로 명시적 프록시 서버를 구성하는 예입니다.

+

```
./NetApp_Console_Agent_Cloud_v4.0.0--proxy
https://user:password@10.0.0.30:8080/ --cacert /tmp/cacert/certificate.cer
```

+
`--proxy` 다음 형식 중 하나를 사용하여 Console 에이전트가 HTTP 또는 HTTPS 프록시 서버를 사용하도록 구성합니다.

+ * http://address:port * http://user-name:password@address:port * http://domain-name%92user-name:password@address:port * https://address:port * https://user-name:password@address:port * https://domain-name%92user-name:password@address:port

+ 다음 사항에 유의하십시오:

+ 사용자는 로컬 사용자 또는 도메인 사용자일 수 있습니다. 도메인 사용자의 경우 위와 같이 \의 ASCII 코드를 사용해야 합니다. **Console** 에이전트는 **@** 문자가 포함된 사용자 이름이나 암호를 지원하지 않습니다. 암호에 다음 특수 문자(& 또는 !)가 포함된 경우 백슬래시를 앞에 붙여 해당 특수 문자를 이스케이프해야 합니다.

+ 예를 들면:

+ http://bxpproxyuser:netapp1\!@address:3128

1. Podman을 사용한 경우 aardvark-dns 포트를 조정해야 합니다.

   a. 콘솔 에이전트 가상 머신에 SSH를 실행합니다.

   b. podman */usr/share/containers/containers.conf* 파일을 열고 Aardvark DNS 서비스에 대해 선택한 포트를 수정합니다. 예를 들어, 54로 변경합니다.

   ```
   vi /usr/share/containers/containers.conf
   ```

   예를 들어:

   ```
   # Port to use for dns forwarding daemon with netavark in rootful bridge
   # mode and dns enabled.
   # Using an alternate port might be useful if other DNS services should
   # run on the machine.
   #
   dns_bind_port = 54
   ```

   a. 콘솔 에이전트 가상 머신을 재부팅합니다.

2. 설치가 완료될 때까지 기다리세요.

   설치가 끝나면 프록시 서버를 지정한 경우 콘솔 에이전트 서비스(occm)가 두 번 다시 시작됩니다.

   설치에 실패하면 설치 보고서와 로그를 보고 문제를 해결하는 데 도움이 됩니다."설치 문제를 해결하는 방법을 알아보세요."

1. 콘솔 에이전트 가상 머신에 연결된 호스트에서 웹 브라우저를 열고 다음 URL을 입력합니다.

   https://ipaddress

2. 로그인 후 콘솔 에이전트를 설정하세요.

   a. 콘솔 에이전트와 연결할 조직을 지정합니다.

   b. 시스템 이름을 입력하세요.

   c. *보안된 환경에서 실행하고 있습니까?*에서 제한 모드를 비활성화하세요.

      이 단계에서는 표준 모드에서 콘솔을 사용하는 방법을 설명하므로 제한 모드를 비활성화해야 합니다. 보안 환경이 있고 백엔드 서비스에서 이 계정의 연결을 끊으려는 경우에만 제한 모드를 활성화해야 합니다. 그렇다면 ,"제한 모드에서 NetApp Console 시작하기 위한 단계를 따르세요." .

   d. *시작하기*를 선택하세요.

설치에 실패하면 로그와 보고서를 보고 문제 해결에 도움을 받을 수 있습니다."설치 문제를 해결하는 방법을 알아보세요."

콘솔 에이전트를 생성한 동일한 Google Cloud 계정에 Google Cloud Storage 버킷이 있는 경우, 시스템 페이지에 Google Cloud Storage 시스템이 자동으로 표시됩니다. "NetApp Console 에서 Google Cloud Storage를 관리하는 방법을 알아보세요."

8단계**:** 콘솔 에이전트에 권한 제공

이전에 설정한 Google Cloud 권한을 콘솔 에이전트에 제공해야 합니다. 권한을 제공하면 콘솔 에이전트가 Google Cloud에서 데이터 및 스토리지 인프라를 관리할 수 있습니다.

단계

1. Google Cloud 포털로 이동하여 콘솔 에이전트 VM 인스턴스에 서비스 계정을 할당합니다.

   "Google Cloud 문서: 인스턴스의 서비스 계정 및 액세스 범위 변경"

2. 다른 Google Cloud 프로젝트의 리소스를 관리하려면 해당 프로젝트에 콘솔 에이전트 역할이 있는 서비스 계정을 추가하여 액세스 권한을 부여하세요. 각 프로젝트마다 이 단계를 반복해야 합니다.

온프레미스에 에이전트 설치

온프레미스에 콘솔 에이전트를 수동으로 설치합니다.

온프레미스에 콘솔 에이전트를 설치한 다음 로그인하여 콘솔 조직에서 작동하도록 설정합니다.

VMWare 사용자인 경우 OVA를 사용하여 VCenter에 콘솔 에이전트를 설치할 수 있습니다."VCenter에 에이전트를 설치하는 방법에 대해 자세히 알아보세요."

설치하기 전에 호스트(VM 또는 Linux 호스트)가 요구 사항을 충족하는지 확인하고 콘솔 에이전트가 인터넷과 대상 네트워크에 아웃바운드 액세스할 수 있는지 확인해야 합니다. NetApp 데이터 서비스나 Cloud Volumes ONTAP 과 같은 클라우드 스토리지 옵션을 사용할 계획이라면 콘솔에 추가할 클라우드 공급자에서 자격 증명을 만들어야 합니다. 이렇게 하면 콘솔 에이전트가 사용자를 대신하여 클라우드에서 작업을 수행할 수 있습니다.

콘솔 에이전트 설치를 준비하세요

콘솔 에이전트를 설치하기 전에 설치 요구 사항을 충족하는 호스트 머신이 있는지 확인해야 합니다. 또한 네트워크 관리자와 협력하여 콘솔 에이전트가 필요한 엔드포인트에 대한 아웃바운드 액세스 권한과 대상 네트워크에 대한 연결 권한을 가지고 있는지 확인해야 합니다.

콘솔 에이전트 호스트 요구 사항 검토

운영 체제, RAM 및 포트 요구 사항을 충족하는 x86 호스트에서 콘솔 에이전트를 실행합니다. 콘솔 에이전트를 설치하기 전에 호스트가 이러한 요구 사항을 충족하는지 확인하세요.

콘솔 에이전트는 UID와 GID 범위를 19000~19200으로 예약합니다. 이 범위는 고정되어 있으며 수정할 수 없습니다. 호스트의 타사 소프트웨어가 이 범위 내의 UID나 GID를 사용하는 경우 에이전트 설치가 실패합니다. NetApp 충돌을 피하기 위해 타사 소프트웨어가 없는 호스트를 사용할 것을 권장합니다.

전담 호스트

콘솔 에이전트를 실행하려면 전용 호스트가 필요합니다. 다음의 크기 요건을 충족하는 모든 아키텍처가 지원됩니다.

- CPU: 8개 코어 또는 8개 vCPU
- 램: 32GB
- 디스크 공간: 호스트에 권장되는 디스크 공간은 165GB이며, 다음 파티션 요구 사항이 적용됩니다.
  - `/opt`: 120GiB의 공간이 사용 가능해야 합니다.

    에이전트는 다음을 사용합니다. `/opt` 설치하려면 `/opt/application/netapp` 디렉토리와 그 내용.
  - `/var`: 40GiB의 공간이 사용 가능해야 합니다.

    콘솔 에이전트는 다음 공간이 필요합니다. `/var` Podman이나 Docker는 컨테이너를 이 디렉터리 내에 생성하도록 설계되었기 때문입니다. 구체적으로, 그들은 컨테이너를 생성할 것입니다. `/var/lib/containers/storage` 디렉토리 및 `/var/lib/docker` Docker용입니다. 이 공간에서는 외부 마운트나 심볼릭 링크가 작동하지 않습니다.

하이퍼바이저

지원되는 운영 체제를 실행하도록 인증된 베어 메탈 또는 호스팅 하이퍼바이저가 필요합니다.

운영 체제 및 컨테이너 요구 사항

콘솔 에이전트는 표준 모드 또는 제한 모드에서 콘솔을 사용할 때 다음 운영 체제에서 지원됩니다. 에이전트를 설치하기 전에 컨테이너 오케스트레이션 도구가 필요합니다.

운영 체제	지원되는 **OS** 버전	지원되는 에이전트 버전	필수 컨테이너 도구	셀리눅스
레드햇 엔터프라이즈 리눅스		9.6 • 영어 버전만 제공됩니다. • 호스트는 Red Hat Subscription Management에 등록되어야 합니다. 등록되지 않은 경우 호스트는 에이전트 설치 중에 필요한 타사 소프트웨어를 업데이트하기 위해 저장소에 액세스할 수 없습니다.	4.0.0 이상, 콘솔이 표준 모드 또는 제한 모드인 경우	Podman 버전 5.4.0과 podman-compose 1.5.0. Podman 구성 요구 사항 보기 .

운영 체제	지원되는 **OS** 버전	지원되는 에이전트 버전	필수 컨테이너 도구	셀리눅스
강제 모드 또는 허용 모드에서 지원됨		9.1에서 9.4까지 • 영어 버전만 제공됩니다. • 호스트는 Red Hat Subscription Management에 등록되어야 합니다. 등록되지 않은 경우 호스트는 에이전트 설치 중에 필요한 타사 소프트웨어를 업데이트하기 위해 저장소에 액세스할 수 없습니다.	3.9.50 이상, 콘솔이 표준 모드 또는 제한 모드인 경우	Podman 버전 4.9.4와 podman-compose 1.5.0. Podman 구성 요구 사항 보기 .
강제 모드 또는 허용 모드에서 지원됨		8.6에서 8.10까지 • 영어 버전만 제공됩니다. • 호스트는 Red Hat Subscription Management에 등록되어야 합니다. 등록되지 않은 경우 호스트는 에이전트 설치 중에 필요한 타사 소프트웨어를 업데이트하기 위해 저장소에 액세스할 수 없습니다.	3.9.50 이상, 콘솔이 표준 모드 또는 제한 모드인 경우	Podman 버전 4.6.1 또는 4.9.4와 podman-compose 1.0.6. Podman 구성 요구 사항 보기 .
강제 모드 또는 허용 모드에서 지원됨	우분투		24.04 장기	표준 모드 또는 제한 모드에서 NetApp Console 사용하는 3.9.45 이상
Docker 엔진 23.06~28.0.0.	지원되지 않음		22.04 장기	3.9.50 이상

콘솔 에이전트에 대한 네트워크 액세스 설정

콘솔 에이전트가 리소스를 관리할 수 있도록 네트워크 액세스를 설정합니다. 대상 네트워크에 연결하고 특정 엔드포인트에 대한 아웃바운드 인터넷 액세스가 필요합니다.

대상 네트워크에 대한 연결

콘솔 에이전트를 사용하려면 시스템을 만들고 관리하려는 위치에 대한 네트워크 연결이 필요합니다. 예를 들어, Cloud Volumes ONTAP 시스템이나 온프레미스 환경의 스토리지 시스템을 만들 계획인 네트워크입니다.

아웃바운드 인터넷 접속

콘솔 에이전트를 배포하는 네트워크 위치에는 특정 엔드포인트에 연결하기 위한 아웃바운드 인터넷 연결이 있어야 합니다.

웹 기반 **NetApp Console** 사용할 때 컴퓨터에서 연결된 엔드포인트

웹 브라우저에서 콘솔에 액세스하는 컴퓨터는 여러 엔드포인트에 접속할 수 있어야 합니다. 콘솔 에이전트를 설정하고 콘솔을 일상적으로 사용하려면 콘솔을 사용해야 합니다.

"NetApp 콘솔을 위한 네트워킹 준비" .

콘솔 에이전트에서 연락한 엔드포인트

콘솔 에이전트는 일상 업무를 위해 퍼블릭 클라우드 환경 내의 리소스와 프로세스를 관리하기 위해 다음 엔드포인트에 연결하기 위해 아웃바운드 인터넷 액세스가 필요합니다.

아래 나열된 엔드포인트는 모두 CNAME 항목입니다.

사내에 설치된 콘솔 에이전트는 Google Cloud의 리소스를 관리할 수 없습니다. Google Cloud 리소스를 관리하려면 Google Cloud에 에이전트를 설치해야 합니다.

AWS

콘솔 에이전트가 온프레미스에 설치된 경우 AWS에 배포된 NetApp 시스템(예: Cloud Volumes ONTAP)을 관리하기 위해 다음 AWS 엔드포인트에 대한 네트워크 액세스가 필요합니다.

콘솔 에이전트에서 연락한 엔드포인트

콘솔 에이전트는 일상 업무를 위해 퍼블릭 클라우드 환경 내의 리소스와 프로세스를 관리하기 위해 다음 엔드포인트에 연결하기 위해 아웃바운드 인터넷 액세스가 필요합니다.

아래 나열된 엔드포인트는 모두 CNAME 항목입니다.

엔드포인트	목적
AWS 서비스(amazonaws.com): • 클라우드포메이션 • 탄력적 컴퓨팅 클라우드(EC2) • ID 및 액세스 관리(IAM) • 키 관리 서비스(KMS) • 보안 토큰 서비스(STS) • 간편 보관 서비스(S3)	AWS 리소스를 관리합니다. 엔드포인트는 AWS 지역에 따라 달라집니다. "자세한 내용은 AWS 설명서를 참조하세요."
Amazon FsX for NetApp ONTAP: • api.workloads.netapp.com	웹 기반 콘솔은 이 엔드포인트에 연결하여 Workload Factory API와 상호 작용함으로써 ONTAP 기반 워크로드용 FSx를 관리하고 운영합니다.
\ https://mysupport.netapp.com	라이선스 정보를 얻고 NetApp 지원팀에 AutoSupport 메시지를 보냅니다.
\ https://signin.b2c.netapp.com	NetApp 지원 사이트(NSS) 자격 증명을 업데이트하거나 NetApp Console 에 새로운 NSS 자격 증명을 추가합니다.
\ https://support.netapp.com	라이선스 정보를 얻고 NetApp 지원팀에 AutoSupport 메시지를 보내고 Cloud Volumes ONTAP 에 대한 소프트웨어 업데이트를 받습니다.

엔드포인트	목적
\ https://api.bluexp.netapp.com \ https://netapp-cloud-account.auth0.com \ https://netapp-cloud-account.us.auth0.com \ https://console.netapp.com \ https://components.console.bluexp.netapp.com \ https://cdn.auth0.com	NetApp Console 내에서 기능과 서비스를 제공합니다.
\ https://bluexpinfraprod.eastus2.data.azurecr.io \ https://bluexpinfraprod.azurecr.io	콘솔 에이전트 업그레이드를 위한 이미지를 얻으려면. • 새로운 에이전트를 배포할 때 유효성 검사를 통해 현재 엔드포인트에 대한 연결성을 테스트합니다. 당신이 사용하는 경우"이전 종료점" , 유효성 검사에 실패합니다. 이러한 실패를 방지하려면 유효성 검사를 건너뛰세요. 이전 엔드포인트는 계속 지원되지만 NetApp 가능한 한 빨리 현재 엔드포인트에 맞게 방화벽 규칙을 업데이트할 것을 권장합니다. "엔드포인트 목록을 업데이트하는 방법을 알아보세요" . • 방화벽의 현재 엔드포인트로 업데이트하면 기존 에이전트도 계속 작동합니다.

하늘빛

콘솔 에이전트가 온프레미스에 설치된 경우 Azure에 배포된 NetApp 시스템(예: Cloud Volumes ONTAP)을 관리하기 위해 다음 Azure 엔드포인트에 대한 네트워크 액세스가 필요합니다.

엔드포인트	목적
\ https://management.azure.com \ https://login.microsoftonline.com \ https://blob.core.windows.net \ https://core.windows.net	Azure 공용 지역의 리소스를 관리합니다.
\ https://management.chinacloudapi.cn \ https://login.chinacloudapi.cn \ https://blob.core.chinacloudapi.cn \ https://core.chinacloudapi.cn	Azure China 지역의 리소스를 관리합니다.
\ https://mysupport.netapp.com	라이선스 정보를 얻고 NetApp 지원팀에 AutoSupport 메시지를 보냅니다.

엔드포인트	목적
\ https://signin.b2c.netapp.com	NetApp 지원 사이트(NSS) 자격 증명을 업데이트하거나 NetApp Console 에 새로운 NSS 자격 증명을 추가합니다.
\ https://support.netapp.com	라이선스 정보를 얻고 NetApp 지원팀에 AutoSupport 메시지를 보내고 Cloud Volumes ONTAP 에 대한 소프트웨어 업데이트를 받습니다.
\ https://api.bluexp.netapp.com \ https://netapp-cloud-account.auth0.com \ https://netapp-cloud-account.us.auth0.com \ https://console.netapp.com \ https://components.console.bluexp.netapp.com \ https://cdn.auth0.com	NetApp Console 내에서 기능과 서비스를 제공합니다.
\ https://bluexpinfraprod.eastus2.data.azurecr.io \ https://bluexpinfraprod.azurecr.io	콘솔 에이전트 업그레이드를 위한 이미지를 얻으려면. • 새로운 에이전트를 배포할 때 유효성 검사를 통해 현재 엔드포인트에 대한 연결성을 테스트합니다. 당신이 사용하는 경우"이전 종료점" , 유효성 검사에 실패합니다. 이러한 실패를 방지하려면 유효성 검사를 건너뛰세요. 이전 엔드포인트는 계속 지원되지만 NetApp 가능한 한 빨리 현재 엔드포인트에 맞게 방화벽 규칙을 업데이트할 것을 권장합니다. "엔드포인트 목록을 업데이트하는 방법을 알아보세요" . • 방화벽의 현재 엔드포인트로 업데이트하면 기존 에이전트도 계속 작동합니다.

프록시 서버

NetApp 명시적 프록시 구성과 투명 프록시 구성을 모두 지원합니다. 투명 프록시를 사용하는 경우 프록시 서버에 대한 인증서만 제공하면 됩니다. 명시적 프록시를 사용하는 경우 IP 주소와 자격 증명도 필요합니다.

- IP 주소
- 신임장

- HTTPS 인증서

포트

Cloud Volumes ONTAP 에서 NetApp 지원팀으로 AutoSupport 메시지를 보내기 위한 프록시로 사용되거나 사용자가 시작하지 않는 한 콘솔 에이전트로 들어오는 트래픽이 없습니다.

- HTTP(80) 및 HTTPS(443)는 로컬 UI에 대한 액세스를 제공하며 이는 드문 상황에서 사용됩니다.
- SSH(22)는 문제 해결을 위해 호스트에 연결해야 하는 경우에만 필요합니다.
- 아웃바운드 인터넷 연결을 사용할 수 없는 서브넷에 Cloud Volumes ONTAP 시스템을 배포하는 경우 포트 3128을 통한 인바운드 연결이 필요합니다.

  Cloud Volumes ONTAP 시스템에 AutoSupport 메시지를 보낼 아웃바운드 인터넷 연결이 없는 경우 콘솔은 콘솔 에이전트에 포함된 프록시 서버를 사용하도록 해당 시스템을 자동으로 구성합니다. 유일한 요구 사항은 콘솔 에이전트의 보안 그룹이 포트 3128을 통한 인바운드 연결을 허용하는 것입니다. 콘솔 에이전트를 배포한 후 이 포트를 열어야 합니다.

NTP 활성화

NetApp Data Classification 사용하여 회사 데이터 소스를 스캔하려는 경우 콘솔 에이전트와 NetApp Data Classification 시스템 모두에서 NTP(네트워크 시간 프로토콜) 서비스를 활성화하여 시스템 간의 시간을 동기화해야 합니다. "NetApp 데이터 분류에 대해 자세히 알아보세요"

AWS 또는 **Azure**에 대한 콘솔 에이전트 클라우드 권한 만들기

온프레미스 콘솔 에이전트와 함께 AWS 또는 Azure에서 NetApp 데이터 서비스를 사용하려면 클라우드 공급자에서 권한을 설정한 다음, 콘솔 에이전트를 설치한 후 자격 증명을 추가해야 합니다.

Google Cloud에 있는 모든 리소스를 관리하려면 콘솔 에이전트를 설치해야 합니다.

AWS

온프레미스에 콘솔 에이전트를 설치하는 경우 필요한 권한이 있는 IAM 사용자의 액세스 키를 추가하여 콘솔에 AWS 권한을 제공해야 합니다.

콘솔 에이전트가 온프레미스에 설치된 경우 이 인증 방법을 사용해야 합니다. IAM 역할을 사용할 수 없습니다.

단계

1. AWS 콘솔에 로그인하고 IAM 서비스로 이동합니다.
2. 정책을 만듭니다.

   a. *정책 > 정책 만들기*를 선택합니다.

   b. *JSON*을 선택하고 내용을 복사하여 붙여넣습니다."콘솔 에이전트에 대한 IAM 정책" .

   c. 나머지 단계를 완료하여 정책을 만듭니다.

      사용하려는 NetApp 데이터 서비스에 따라 두 번째 정책을 만들어야 할 수도 있습니다.

   표준 지역의 경우 권한은 두 가지 정책에 걸쳐 분산됩니다. AWS의 관리형 정책에는 최대 문자 크기 제한이 있으므로 두 개의 정책이 필요합니다. "콘솔 에이전트에 대한 IAM 정책에 대해 자세히 알아보세요." .

3. IAM 사용자에게 정책을 연결합니다.
   - "AWS 설명서: IAM 역할 생성"
   - "AWS 설명서: IAM 정책 추가 및 제거"
4. 콘솔 에이전트를 설치한 후 NetApp Console 에 추가할 수 있는 액세스 키가 사용자에게 있는지 확인하세요.

결과

이제 필요한 권한이 있는 IAM 사용자에 대한 액세스 키가 생겼습니다. 콘솔 에이전트를 설치한 후 콘솔에서 이러한 자격 증명을 콘솔 에이전트와 연결합니다.

하늘빛

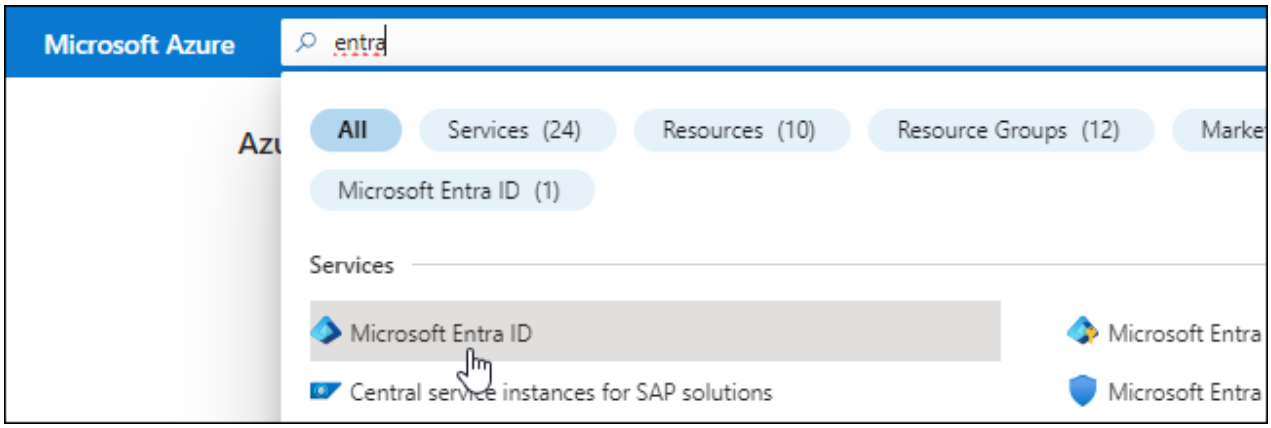
온프레미스에 콘솔 에이전트를 설치하는 경우 Microsoft Entra ID에서 서비스 주체를 설정하고 콘솔 에이전트에 필요한 Azure 자격 증명을 얻어 콘솔 에이전트에 Azure 권한을 제공해야 합니다.

역할 기반 액세스 제어를 위한 **Microsoft Entra** 애플리케이션 만들기

1. Azure에서 Active Directory 애플리케이션을 만들고 해당 애플리케이션에 역할을 할당할 수 있는 권한이 있는지 확인하세요.

   자세한 내용은 다음을 참조하세요. "Microsoft Azure 설명서: 필요한 권한"

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



3. 메뉴에서 *앱 등록*을 선택하세요.
4. *신규 등록*을 선택하세요.
5. 신청서에 대한 세부 사항을 지정하세요:
   - 이름: 애플리케이션의 이름을 입력하세요.
   - 계정 유형: 계정 유형을 선택하세요(모든 계정 유형이 NetApp Console 에서 작동합니다).
   - 리디렉션 **URI**: 이 필드는 비워두어도 됩니다.
6. *등록*을 선택하세요.

   AD 애플리케이션과 서비스 주체를 생성했습니다.

역할에 애플리케이션 할당

1. 사용자 정의 역할 만들기:

   Azure Portal, Azure PowerShell, Azure CLI 또는 REST API를 사용하여 Azure 사용자 지정 역할을 만들 수 있습니다. 다음 단계에서는 Azure CLI를 사용하여 역할을 만드는 방법을 보여줍니다. 다른 방법을 사용하려면 다음을 참조하세요. "Azure 설명서"

   a. 내용을 복사하세요"콘솔 에이전트에 대한 사용자 정의 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.

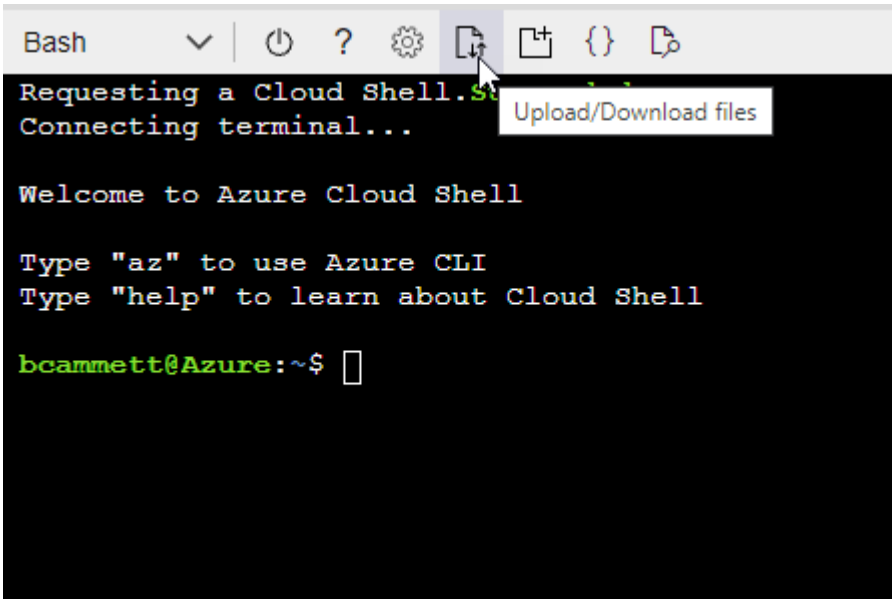
      예

      ```
      "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 만듭니다.

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

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

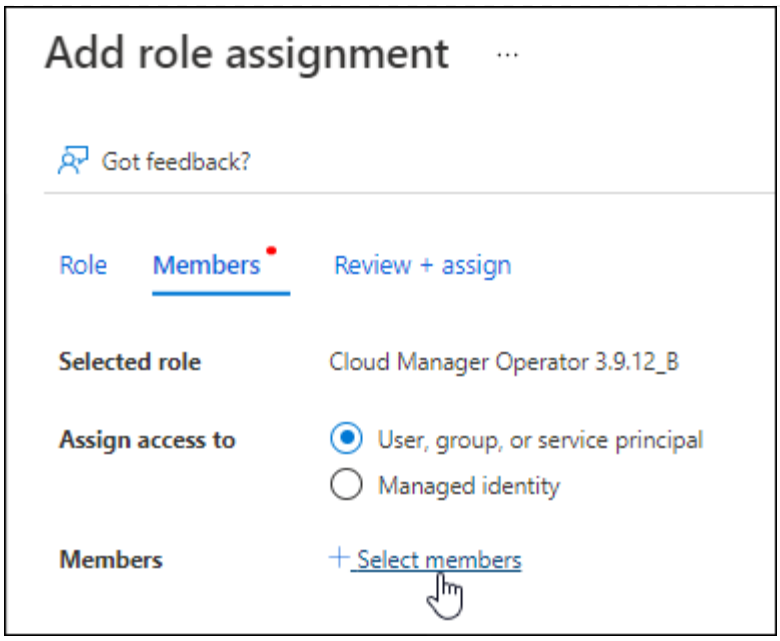


- Azure CLI를 사용하여 사용자 지정 역할을 만듭니다.

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

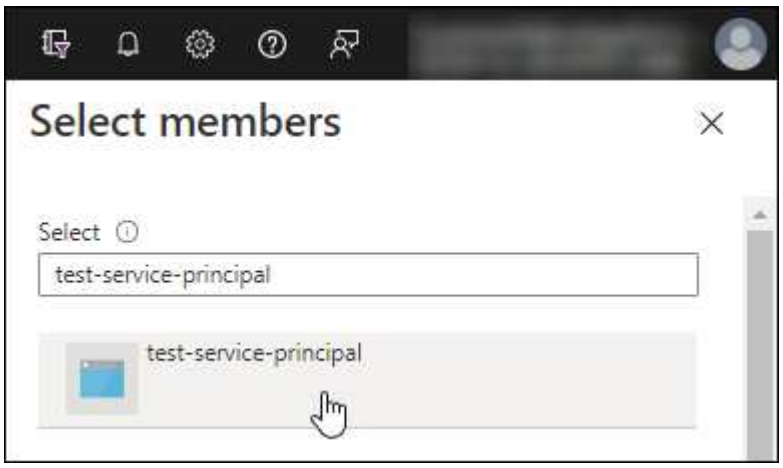
이제 콘솔 에이전트 가상 머신에 할당할 수 있는 콘솔 운영자라는 사용자 지정 역할이 생겼습니다.

2. 역할에 애플리케이션을 할당합니다.
   a. Azure Portal에서 구독 서비스를 엽니다.
   b. 구독을 선택하세요.
   c. *액세스 제어(IAM) > 추가 > 역할 할당 추가*를 선택합니다.
   d. 역할 탭에서 콘솔 운영자 역할을 선택하고 *다음*을 선택합니다.
   e. 멤버 탭에서 다음 단계를 완료하세요.
      - *사용자, 그룹 또는 서비스 주체*를 선택된 상태로 유지합니다.
      - *멤버 선택*을 선택하세요.



- 애플리케이션 이름을 검색하세요.

  예를 들면 다음과 같습니다.



- 애플리케이션을 선택하고 *선택*을 선택하세요.
- *다음*을 선택하세요.

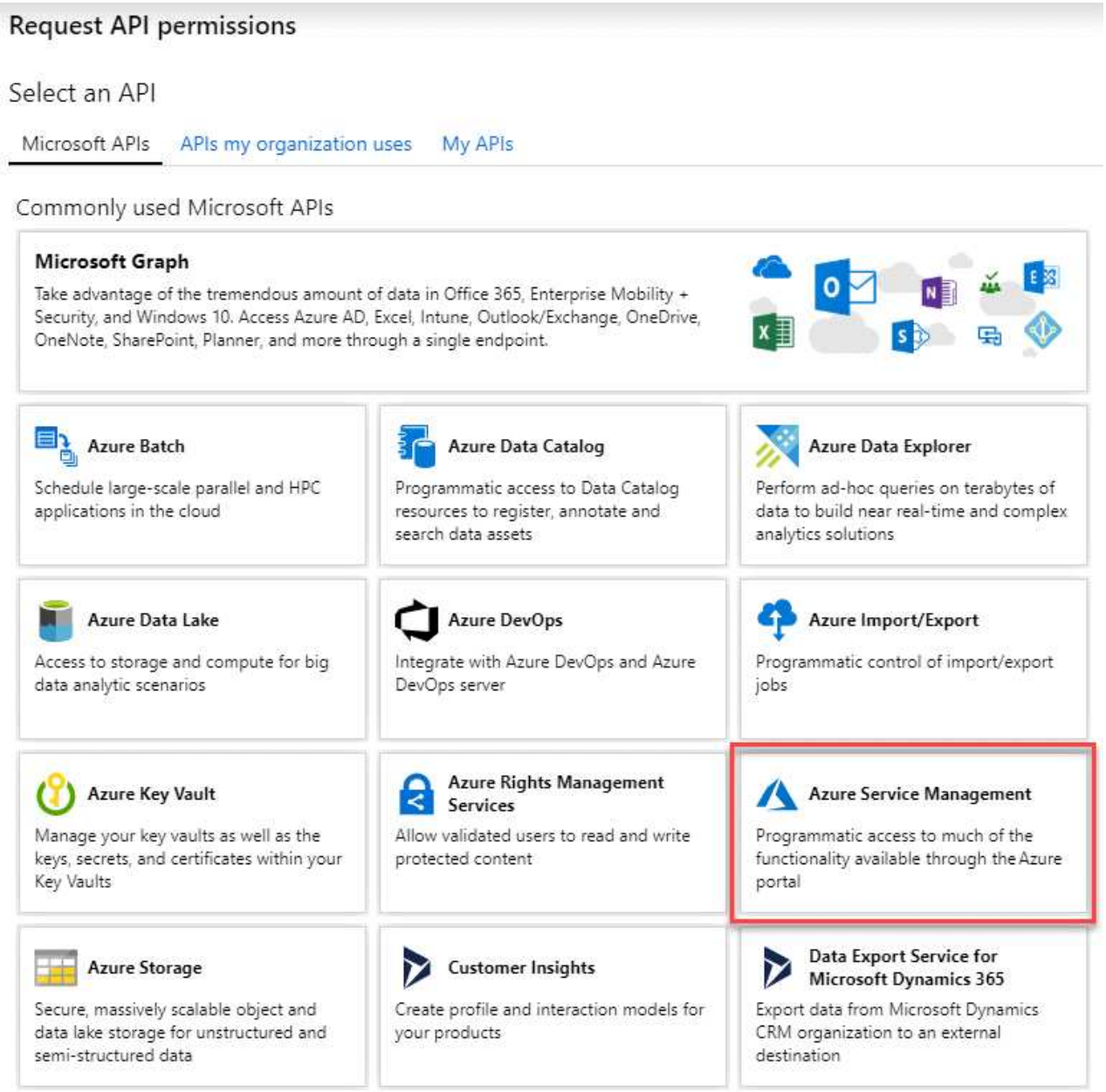
f. *검토 + 할당*을 선택하세요.

이제 서비스 주체는 콘솔 에이전트를 배포하는 데 필요한 Azure 권한을 갖게 되었습니다.

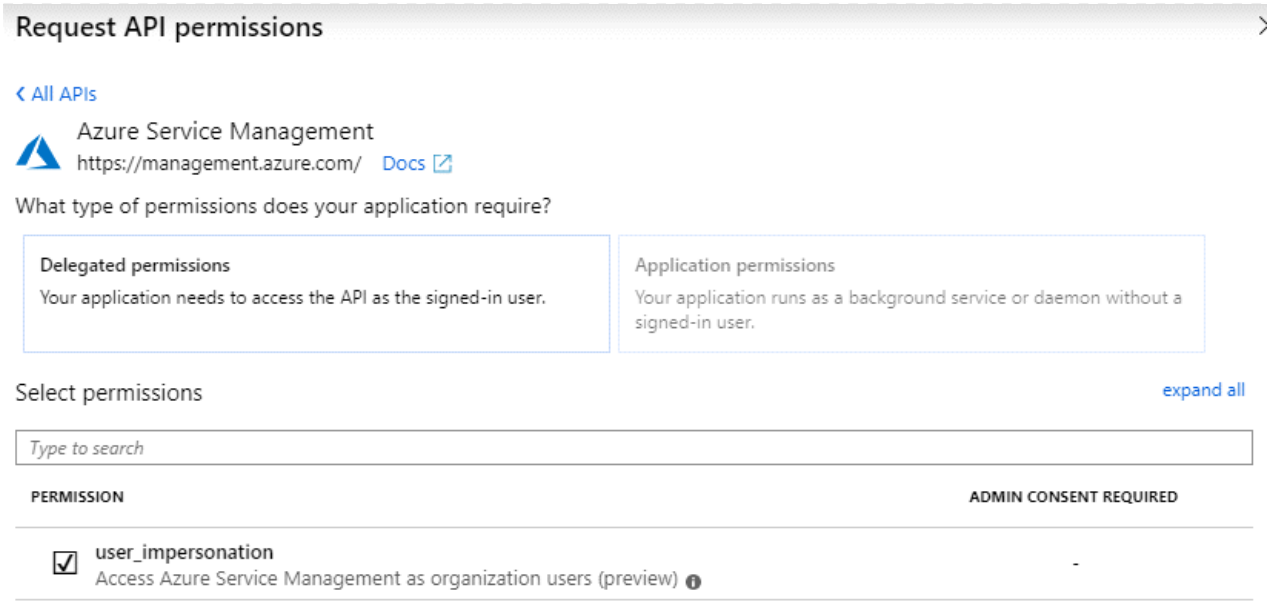
여러 Azure 구독에서 Cloud Volumes ONTAP 배포하려면 각 구독에 서비스 주체를 바인딩해야 합니다. NetApp Console 에서 Cloud Volumes ONTAP 배포할 때 사용할 구독을 선택할 수 있습니다.

Windows Azure 서비스 관리 **API** 권한 추가

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.

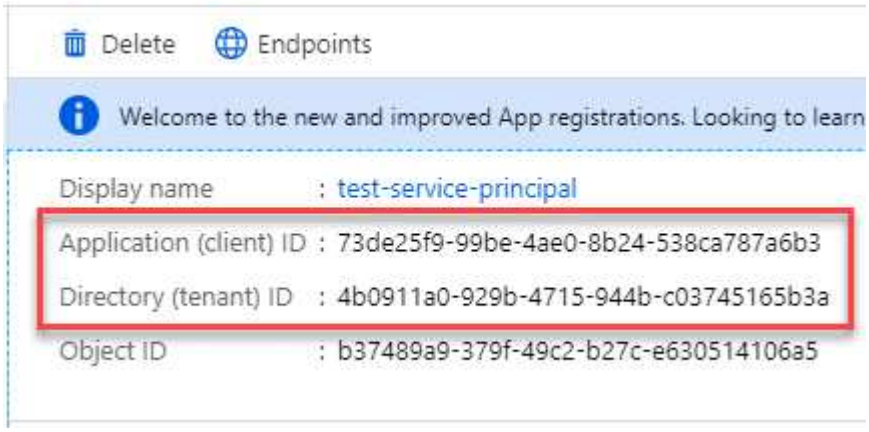


4. *조직 사용자로 Azure Service Management에 액세스*를 선택한 다음 *권한 추가*를 선택합니다.



애플리케이션의 애플리케이션 **ID**와 디렉토리 **ID**를 가져옵니다**.**

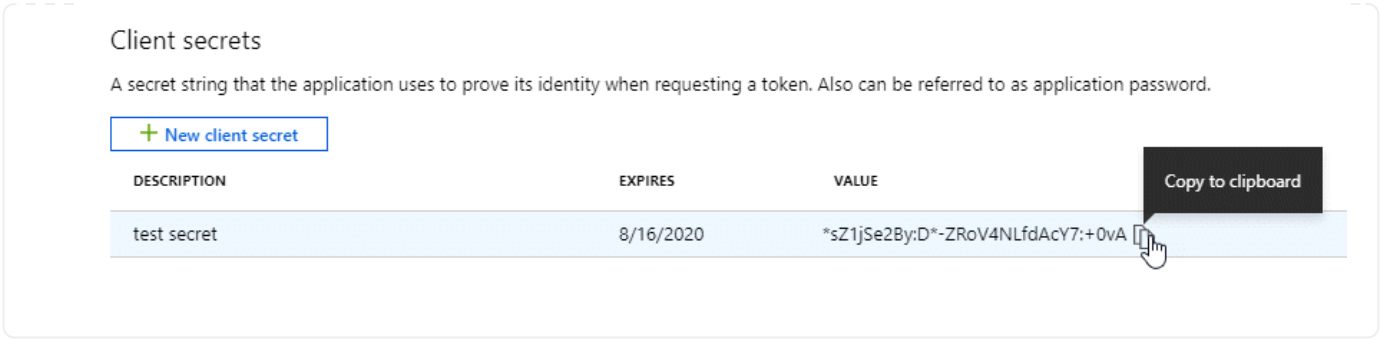
1. **Microsoft Entra ID** 서비스에서 *앱 등록*을 선택하고 애플리케이션을 선택합니다.
2. *애플리케이션(클라이언트) ID*와 *디렉토리(테넌트) ID*를 복사합니다.



콘솔에 Azure 계정을 추가하는 경우 애플리케이션(클라이언트) ID와 애플리케이션의 디렉터리(테넌트) ID를 제공해야 합니다. 콘솔은 ID를 사용하여 프로그래밍 방식으로 로그인합니다.

클라이언트 비밀을 생성하세요

1. **Microsoft Entra ID** 서비스를 엽니다.
2. *앱 등록*을 선택하고 애플리케이션을 선택하세요.
3. *인증서 및 비밀번호 > 새 클라이언트 비밀번호*를 선택합니다.
4. 비밀에 대한 설명과 기간을 제공하세요.
5. *추가*를 선택하세요.
6. 클라이언트 비밀번호 값을 복사합니다.



콘솔 에이전트를 수동으로 설치합니다.

콘솔 에이전트를 수동으로 설치하는 경우 요구 사항을 충족하도록 컴퓨터 환경을 준비해야 합니다. Linux 컴퓨터가 필요하며, Linux 운영 체제에 따라 Podman이나 Docker를 설치해야 합니다.

Podman 또는 Docker Engine 설치

운영 체제에 따라 에이전트를 설치하기 전에 Podman 또는 Docker Engine이 필요합니다.

- Red Hat Enterprise Linux 8 및 9에는 Podman이 필요합니다.

  지원되는 Podman 버전 보기 .

- Ubuntu에는 Docker 엔진이 필요합니다.

  지원되는 Docker Engine 버전 보기 .

예 **4.** 단계

포드만

Podman을 설치하고 구성하려면 다음 단계를 따르세요.

- podman.socket 서비스를 활성화하고 시작합니다.
- python3 설치
- podman-compose 패키지 버전 1.0.6을 설치하세요
- PATH 환경 변수에 podman-compose를 추가합니다.
- Red Hat Enterprise Linux를 사용하는 경우 Podman 버전이 CNI 대신 Netavark Aardvark DNS를 사용하는지 확인하십시오.

DNS 포트 충돌을 피하기 위해 에이전트를 설치한 후 aardvark-dns 포트(기본값: 53)를 조정하세요. 지침에 따라 포트를 구성하세요.

단계

1. 호스트에 podman-docker 패키지가 설치되어 있다면 제거합니다.

```
dnf remove podman-docker
rm /var/run/docker.sock
```

2. Podman을 설치하세요.

   공식 Red Hat Enterprise Linux 저장소에서 Podman을 다운로드할 수 있습니다.

   a. Red Hat Enterprise Linux 9.6의 경우:

   ```
   sudo dnf install podman-5:<version>
   ```

   여기서 <버전>은 설치하려는 Podman의 지원되는 버전입니다. 지원되는 Podman 버전 보기 .

   b. Red Hat Enterprise Linux 9.1~9.4 버전의 경우:

   ```
   sudo dnf install podman-4:<version>
   ```

   여기서 <버전>은 설치하려는 Podman의 지원되는 버전입니다. 지원되는 Podman 버전 보기 .

   c. Red Hat Enterprise Linux 8의 경우:

   ```
   sudo dnf install podman-4:<version>
   ```

   여기서 <버전>은 설치하려는 Podman의 지원되는 버전입니다. 지원되는 Podman 버전 보기 .

3. podman.socket 서비스를 활성화하고 시작합니다.

```
sudo systemctl enable --now podman.socket
```

4. python3를 설치합니다.

```
sudo dnf install python3
```

5. 시스템에 EPEL 저장소 패키지가 아직 없으면 설치하세요.

   이 단계는 podman-compose가 EPEL(Enterprise Linux용 추가 패키지) 저장소에서 사용 가능하기 때문에 필요합니다.

6. Red Hat Enterprise 9를 사용하는 경우:

   a. EPEL 저장소 패키지를 설치하세요.

```
sudo dnf install https://dl.fedoraproject.org/pub/epel/epel-release-latest-9.noarch.rpm
```

   +

   a. podman-compose 패키지 1.5.0을 설치합니다.

```
sudo dnf install podman-compose-1.5.0
```

7. Red Hat Enterprise Linux 8을 사용하는 경우:

   a. EPEL 저장소 패키지를 설치하세요.

```
sudo dnf install https://dl.fedoraproject.org/pub/epel/epel-release-latest-8.noarch.rpm
```

   b. podman-compose 패키지 1.0.6을 설치합니다.

```
sudo dnf install podman-compose-1.0.6
```

> ⓘ 를 사용하여 `dnf install` 명령은 PATH 환경 변수에 podman-compose를 추가하는 요구 사항을 충족합니다. 설치 명령은 이미 포함되어 있는 /usr/bin에 podman-compose를 추가합니다. `secure_path` 호스트의 옵션.

   c. Red Hat Enterprise Linux 8을 사용하는 경우 Podman 버전이 CNI 대신 Aardvark DNS와 함께 NetAvark를 사용하는지 확인하세요.

i. 다음 명령을 실행하여 networkBackend가 CNI로 설정되어 있는지 확인하세요.

```
podman info | grep networkBackend
```

ii. networkBackend가 설정된 경우 `CNI` , 당신은 그것을 변경해야 합니다 `netavark` .

iii. 설치하다 `netavark` 그리고 `aardvark-dns` 다음 명령을 사용합니다.

```
dnf install aardvark-dns netavark
```

iv. 열기 `/etc/containers/containers.conf` 파일을 열고 network_backend 옵션을 "cni" 대신 "netavark"를 사용하도록 수정합니다.

만약에 `/etc/containers/containers.conf` 존재하지 않습니다. 구성을 변경하세요. `/usr/share/containers/containers.conf` .

v. Podman을 다시 시작하세요.

```
systemctl restart podman
```

vi. 다음 명령을 사용하여 networkBackend가 이제 "netavark"로 변경되었는지 확인하세요.

```
podman info | grep networkBackend
```

도커 엔진

Docker Engine을 설치하려면 Docker 설명서를 따르세요.

단계

1. "Docker에서 설치 지침 보기"

   지원되는 Docker Engine 버전을 설치하려면 다음 단계를 따르세요. 콘솔에서 지원되지 않으므로 최신 버전을 설치하지 마세요.

2. Docker가 활성화되어 실행 중인지 확인하세요.

```
sudo systemctl enable docker && sudo systemctl start docker
```

콘솔 에이전트를 수동으로 설치합니다.

기존 온프레미스 Linux 호스트에 콘솔 에이전트 소프트웨어를 다운로드하여 설치합니다.

시작하기 전에

다음 사항이 있어야 합니다.

- 콘솔 에이전트를 설치하려면 루트 권한이 필요합니다.
- 콘솔 에이전트에서 인터넷에 접속하는 데 프록시가 필요한 경우 프록시 서버에 대한 세부 정보입니다.

  설치 후 프록시 서버를 구성할 수 있지만, 그렇게 하려면 콘솔 에이전트를 다시 시작해야 합니다.

- 프록시 서버가 HTTPS를 사용하거나 프록시가 가로채기 프록시인 경우 CA 서명 인증서가 필요합니다.

> ⓘ 콘솔 에이전트를 수동으로 설치하는 경우 투명 프록시 서버에 대한 인증서를 설정할 수 없습니다. 투명 프록시 서버에 대한 인증서를 설정해야 하는 경우 설치 후 유지 관리 콘솔을 사용해야 합니다. 자세히 알아보세요"에이전트 유지 관리 콘솔" .

이 작업에 관하여

설치 후, 새로운 버전이 나오면 콘솔 에이전트가 자동으로 업데이트됩니다.

단계

1. 호스트에 *http_proxy* 또는 *https_proxy* 시스템 변수가 설정되어 있으면 제거합니다.

```
unset http_proxy
unset https_proxy
```

   이러한 시스템 변수를 제거하지 않으면 설치가 실패합니다.

2. 콘솔 에이전트 소프트웨어를 다운로드한 다음 Linux 호스트에 복사하십시오. NetApp Console 또는 NetApp 지원 사이트에서 다운로드할 수 있습니다.
   - NetApp Console: *에이전트 > 관리 > 에이전트 배포 > 온프레미스 > 수동 설치*로 이동합니다.

     에이전트 설치 파일 다운로드 또는 파일 URL 다운로드를 선택하십시오.

   - NetApp 지원 사이트 (콘솔에 대한 액세스 권한이 없는 경우 필요) "NetApp 지원 사이트" ,
3. 스크립트를 실행할 수 있는 권한을 할당합니다.

```
chmod +x NetApp_Console_Agent_Cloud_<version>
```

   여기서 <버전>은 다운로드한 콘솔 에이전트의 버전입니다.

4. 정부 클라우드 환경에 설치하는 경우 구성 검사를 비활성화하세요."수동 설치에 대한 구성 검사를 비활성화하는 방법을 알아보세요."
5. 설치 스크립트를 실행합니다.

```
./NetApp_Console_Agent_Cloud_<version> --proxy <HTTP or HTTPS proxy
server> --cacert <path and file name of a CA-signed certificate>
```

네트워크에서 인터넷 접속을 위해 프록시가 필요한 경우 프록시 정보를 추가해야 합니다. 설치 중에 명시적 프록시를 추가할 수 있습니다. `--proxy` 및 `--cacert` 매개변수는 선택 사항이며 추가하라는 메시지가 표시되지 않습니다. 명시적 프록시 서버가 있는 경우 표시된 대로 매개변수를 입력해야 합니다.

투명 프록시를 구성하려면 설치 후에 구성하면 됩니다. "에이전트 유지 관리 콘솔에 대해 알아보세요"

+

다음은 CA 서명 인증서로 명시적 프록시 서버를 구성하는 예입니다.

+

```
./NetApp_Console_Agent_Cloud_v4.0.0--proxy
https://user:password@10.0.0.30:8080/ --cacert /tmp/cacert/certificate.cer
```

+
`--proxy` 다음 형식 중 하나를 사용하여 Console 에이전트가 HTTP 또는 HTTPS 프록시 서버를 사용하도록 구성합니다.

+ * http://address:port * http://user-name:password@address:port * http://domain-name%92user-name:password@address:port * https://address:port * https://user-name:password@address:port * https://domain-name%92user-name:password@address:port

+ 다음 사항에 유의하십시오:

+ 사용자는 로컬 사용자 또는 도메인 사용자일 수 있습니다. 도메인 사용자의 경우 위와 같이 \의 ASCII 코드를 사용해야 합니다. **Console** 에이전트는 **@** 문자가 포함된 사용자 이름이나 암호를 지원하지 않습니다. 암호에 다음 특수 문자(& 또는 !)가 포함된 경우 백슬래시를 앞에 붙여 해당 특수 문자를 이스케이프해야 합니다.

+ 예를 들면:

+ http://bxpproxyuser:netapp1\!@address:3128

1. Podman을 사용한 경우 aardvark-dns 포트를 조정해야 합니다.

   a. 콘솔 에이전트 가상 머신에 SSH를 실행합니다.

   b. podman */usr/share/containers/containers.conf* 파일을 열고 Aardvark DNS 서비스에 대해 선택한 포트를 수정합니다. 예를 들어, 54로 변경합니다.

      ```
      vi /usr/share/containers/containers.conf
      ```

      예를 들어:

```
# Port to use for dns forwarding daemon with netavark in rootful bridge
# mode and dns enabled.
# Using an alternate port might be useful if other DNS services should
# run on the machine.
#
dns_bind_port = 54
```

a. 콘솔 에이전트 가상 머신을 재부팅합니다.

다음은 무엇인가요?

NetApp Console 내에서 콘솔 에이전트를 등록해야 합니다.

NetApp Console 에 콘솔 에이전트 등록

콘솔에 로그인하고 콘솔 에이전트를 조직과 연결합니다. 로그인 방법은 콘솔을 사용하는 모드에 따라 달라집니다. 표준 모드로 콘솔을 사용하는 경우 SaaS 웹사이트를 통해 로그인합니다. 제한 모드에서 콘솔을 사용하는 경우 콘솔 에이전트 호스트에서 로컬로 로그인합니다.

단계

1. 웹 브라우저를 열고 콘솔 에이전트 호스트 URL을 입력하세요.

   콘솔 호스트 URL은 호스트 구성에 따라 로컬호스트, 개인 IP 주소 또는 공용 IP 주소가 될 수 있습니다. 예를 들어, 콘솔 에이전트가 공용 IP 주소가 없는 퍼블릭 클라우드에 있는 경우 콘솔 에이전트 호스트에 연결된 호스트의 개인 IP 주소를 입력해야 합니다.

2. 가입하거나 로그인하세요.
3. 로그인 후 콘솔을 설정하세요.
   a. 콘솔 에이전트와 연결할 콘솔 조직을 지정합니다.
   b. 시스템 이름을 입력하세요.
   c. *보안된 환경에서 실행하고 있습니까?*에서 제한 모드를 비활성화하세요.

      콘솔 에이전트가 온프레미스에 설치된 경우 제한 모드는 지원되지 않습니다.

   d. *시작하기*를 선택하세요.

NetApp Console 에 클라우드 공급자 자격 증명 제공

콘솔 에이전트를 설치하고 설정한 후 클라우드 자격 증명을 추가하여 콘솔 에이전트가 AWS 또는 Azure에서 작업을 수행하는 데 필요한 권한을 갖도록 합니다.

AWS

시작하기 전에

AWS 자격 증명을 방금 만든 경우 사용할 수 있게 되는 데 몇 분이 걸릴 수 있습니다. 콘솔에 자격 증명을 추가하기 전에 몇 분 정도 기다리세요.

단계

1. *관리 > 자격 증명*을 선택합니다.
2. *조직 자격 증명*을 선택하세요.
3. *자격 증명 추가*를 선택하고 마법사의 단계를 따르세요.
   a. 자격 증명 위치: *Amazon Web Services > 에이전트를 선택하세요.
   b. 자격 증명 정의: AWS 액세스 키와 비밀 키를 입력합니다.
   c. 마켓플레이스 구독: 지금 구독하거나 기존 구독을 선택하여 마켓플레이스 구독을 이러한 자격 증명과 연결합니다.
   d. 검토: 새로운 자격 증명에 대한 세부 정보를 확인하고 *추가*를 선택합니다.

이제 다음으로 이동할 수 있습니다. "NetApp Console" 콘솔 에이전트를 사용하려면.

하늘빛

시작하기 전에

Azure 자격 증명을 방금 만든 경우 사용 가능해지는 데 몇 분 정도 걸릴 수 있습니다. 콘솔 에이전트에 자격 증명을 추가하기 전에 몇 분 정도 기다리세요.

단계

1. *관리 > 자격 증명*을 선택합니다.
2. *자격 증명 추가*를 선택하고 마법사의 단계를 따르세요.
   a. 자격 증명 위치: *Microsoft Azure > 에이전트*를 선택합니다.
   b. 자격 증명 정의: 필요한 권한을 부여하는 Microsoft Entra 서비스 주체에 대한 정보를 입력합니다.
      - 애플리케이션(클라이언트) ID
      - 디렉토리(테넌트) ID
      - 클라이언트 비밀번호
   c. 마켓플레이스 구독: 지금 구독하거나 기존 구독을 선택하여 마켓플레이스 구독을 이러한 자격 증명과 연결합니다.
   d. 검토: 새로운 자격 증명에 대한 세부 정보를 확인하고 *추가*를 선택합니다.

결과

이제 콘솔 에이전트는 Azure에서 사용자를 대신하여 작업을 수행하는 데 필요한 권한을 갖게 되었습니다. 이제 다음으로 이동할 수 있습니다. "NetApp Console" 콘솔 에이전트를 사용하려면.

VCenter를 사용하여 온프레미스에 콘솔 에이전트 설치

VMWare 사용자인 경우 OVA를 사용하여 VCenter에 콘솔 에이전트를 설치할 수 있습니다.

OVA 다운로드 또는 URL은 NetApp Console 통해 이용할 수 있습니다.

VCenter 도구와 함께 콘솔 에이전트를 설치하면 VM 웹 콘솔을 사용하여 유지 관리 작업을 수행할 수 있습니다."에이전트의 VM 콘솔에 대해 자세히 알아보세요."

콘솔 에이전트 설치를 준비하세요

설치하기 전에 VM 호스트가 요구 사항을 충족하는지, 콘솔 에이전트가 인터넷과 대상 네트워크에 액세스할 수 있는지 확인하세요. NetApp 데이터 서비스 또는 Cloud Volumes ONTAP 사용하려면 콘솔 에이전트가 사용자를 대신하여 작업을 수행할 수 있도록 클라우드 공급자 자격 증명을 생성하세요.

콘솔 에이전트 호스트 요구 사항 검토

콘솔 에이전트를 설치하기 전에 호스트 머신이 설치 요구 사항을 충족하는지 확인하세요.

- CPU: 8개 코어 또는 8개 vCPU
- 램: 32GB
- 디스크 공간: 165GB(두꺼운 프로비저닝)
- vSphere 7.0 이상
- ESXi 호스트 7.03 이상

ESXi 호스트에 직접 설치하는 대신 vCenter 환경에 에이전트를 설치하세요.

콘솔 에이전트에 대한 네트워크 액세스 설정

네트워크 관리자와 협력하여 콘솔 에이전트가 필요한 엔드포인트에 대한 아웃바운드 액세스 권한과 대상 네트워크에 대한 연결을 가지고 있는지 확인하세요.

대상 네트워크에 대한 연결

콘솔 에이전트를 사용하려면 시스템을 만들고 관리하려는 위치에 대한 네트워크 연결이 필요합니다. 예를 들어, Cloud Volumes ONTAP 시스템이나 온프레미스 환경의 스토리지 시스템을 만들 계획인 네트워크입니다.

아웃바운드 인터넷 접속

콘솔 에이전트를 배포하는 네트워크 위치에는 특정 엔드포인트에 연결하기 위한 아웃바운드 인터넷 연결이 있어야 합니다.

웹 기반 **NetApp Console** 사용할 때 컴퓨터에서 연결된 엔드포인트

웹 브라우저에서 콘솔에 액세스하는 컴퓨터는 여러 엔드포인트에 접속할 수 있어야 합니다. 콘솔 에이전트를 설정하고 콘솔을 일상적으로 사용하려면 콘솔을 사용해야 합니다.

"NetApp 콘솔을 위한 네트워킹 준비" .

콘솔 에이전트에서 연락한 엔드포인트

콘솔 에이전트는 일상 업무를 위해 퍼블릭 클라우드 환경 내의 리소스와 프로세스를 관리하기 위해 다음 엔드포인트에 연결하기 위해 아웃바운드 인터넷 액세스가 필요합니다.

아래 나열된 엔드포인트는 모두 CNAME 항목입니다.

사내에 설치된 콘솔 에이전트로는 Google Cloud의 리소스를 관리할 수 없습니다. Google Cloud 리소스를 관리하려면 Google Cloud에 에이전트를 설치하세요.

AWS

콘솔 에이전트가 온프레미스에 설치된 경우 AWS에 배포된 NetApp 시스템(예: Cloud Volumes ONTAP)을 관리하기 위해 다음 AWS 엔드포인트에 대한 네트워크 액세스가 필요합니다.

콘솔 에이전트에서 연락한 엔드포인트

콘솔 에이전트는 일상 업무를 위해 퍼블릭 클라우드 환경 내의 리소스와 프로세스를 관리하기 위해 다음 엔드포인트에 연결하기 위해 아웃바운드 인터넷 액세스가 필요합니다.

아래 나열된 엔드포인트는 모두 CNAME 항목입니다.

엔드포인트	목적
AWS 서비스(amazonaws.com): • 클라우드포메이션 • 탄력적 컴퓨팅 클라우드(EC2) • ID 및 액세스 관리(IAM) • 키 관리 서비스(KMS) • 보안 토큰 서비스(STS) • 간편 보관 서비스(S3)	AWS 리소스를 관리합니다. 엔드포인트는 AWS 지역에 따라 달라집니다. "자세한 내용은 AWS 설명서를 참조하세요."
Amazon FsX for NetApp ONTAP: • api.workloads.netapp.com	웹 기반 콘솔은 이 엔드포인트에 연결하여 Workload Factory API와 상호 작용함으로써 ONTAP 기반 워크로드용 FSx를 관리하고 운영합니다.
\ https://mysupport.netapp.com	라이선스 정보를 얻고 NetApp 지원팀에 AutoSupport 메시지를 보냅니다.
\ https://signin.b2c.netapp.com	NetApp 지원 사이트(NSS) 자격 증명을 업데이트하거나 NetApp Console 에 새로운 NSS 자격 증명을 추가합니다.
\ https://support.netapp.com	라이선스 정보를 얻고 NetApp 지원팀에 AutoSupport 메시지를 보내고 Cloud Volumes ONTAP 에 대한 소프트웨어 업데이트를 받습니다.

엔드포인트	목적
\ https://api.bluexp.netapp.com \ https://netapp-cloud-account.auth0.com \ https://netapp-cloud-account.us.auth0.com \ https://console.netapp.com \ https://components.console.bluexp.netapp.com \ https://cdn.auth0.com	NetApp Console 내에서 기능과 서비스를 제공합니다.
\ https://bluexpinfraprod.eastus2.data.azurecr.io \ https://bluexpinfraprod.azurecr.io	콘솔 에이전트 업그레이드를 위한 이미지를 얻으려면. • 새로운 에이전트를 배포할 때 유효성 검사를 통해 현재 엔드포인트에 대한 연결성을 테스트합니다. 당신이 사용하는 경우"이전 종료점" , 유효성 검사에 실패합니다. 이러한 실패를 방지하려면 유효성 검사를 건너뛰세요. 이전 엔드포인트는 계속 지원되지만 NetApp 가능한 한 빨리 현재 엔드포인트에 맞게 방화벽 규칙을 업데이트할 것을 권장합니다. "엔드포인트 목록을 업데이트하는 방법을 알아보세요" . • 방화벽의 현재 엔드포인트로 업데이트하면 기존 에이전트도 계속 작동합니다.

하늘빛

콘솔 에이전트가 온프레미스에 설치된 경우 Azure에 배포된 NetApp 시스템(예: Cloud Volumes ONTAP)을 관리하기 위해 다음 Azure 엔드포인트에 대한 네트워크 액세스가 필요합니다.

엔드포인트	목적
\ https://management.azure.com \ https://login.microsoftonline.com \ https://blob.core.windows.net \ https://core.windows.net	Azure 공용 지역의 리소스를 관리합니다.
\ https://management.chinacloudapi.cn \ https://login.chinacloudapi.cn \ https://blob.core.chinacloudapi.cn \ https://core.chinacloudapi.cn	Azure China 지역의 리소스를 관리합니다.
\ https://mysupport.netapp.com	라이선스 정보를 얻고 NetApp 지원팀에 AutoSupport 메시지를 보냅니다.

엔드포인트	목적
\ https://signin.b2c.netapp.com	NetApp 지원 사이트(NSS) 자격 증명을 업데이트하거나 NetApp Console 에 새로운 NSS 자격 증명을 추가합니다.
\ https://support.netapp.com	라이선스 정보를 얻고 NetApp 지원팀에 AutoSupport 메시지를 보내고 Cloud Volumes ONTAP 에 대한 소프트웨어 업데이트를 받습니다.
\ https://api.bluexp.netapp.com \ https://netapp-cloud-account.auth0.com \ https://netapp-cloud-account.us.auth0.com \ https://console.netapp.com \ https://components.console.bluexp.netapp.com \ https://cdn.auth0.com	NetApp Console 내에서 기능과 서비스를 제공합니다.
\ https://bluexpinfraprod.eastus2.data.azurecr.io \ https://bluexpinfraprod.azurecr.io	콘솔 에이전트 업그레이드를 위한 이미지를 얻으려면. • 새로운 에이전트를 배포할 때 유효성 검사를 통해 현재 엔드포인트에 대한 연결성을 테스트합니다. 당신이 사용하는 경우"이전 종료점" , 유효성 검사에 실패합니다. 이러한 실패를 방지하려면 유효성 검사를 건너뛰세요. 이전 엔드포인트는 계속 지원되지만 NetApp 가능한 한 빨리 현재 엔드포인트에 맞게 방화벽 규칙을 업데이트할 것을 권장합니다. "엔드포인트 목록을 업데이트하는 방법을 알아보세요" . • 방화벽의 현재 엔드포인트로 업데이트하면 기존 에이전트도 계속 작동합니다.

프록시 서버

NetApp 명시적 프록시 구성과 투명 프록시 구성을 모두 지원합니다. 투명 프록시를 사용하는 경우 프록시 서버에 대한 인증서만 제공하면 됩니다. 명시적 프록시를 사용하는 경우 IP 주소와 자격 증명도 필요합니다.

- IP 주소
- 신임장

- HTTPS 인증서

포트

Cloud Volumes ONTAP 에서 NetApp 지원팀으로 AutoSupport 메시지를 보내기 위한 프록시로 사용되거나 사용자가 시작하지 않는 한 콘솔 에이전트로 들어오는 트래픽이 없습니다.

- HTTP(80) 및 HTTPS(443)는 로컬 UI에 대한 액세스를 제공하며 이는 드문 상황에서 사용됩니다.
- SSH(22)는 문제 해결을 위해 호스트에 연결해야 하는 경우에만 필요합니다.
- 아웃바운드 인터넷 연결을 사용할 수 없는 서브넷에 Cloud Volumes ONTAP 시스템을 배포하는 경우 포트 3128을 통한 인바운드 연결이 필요합니다.

  Cloud Volumes ONTAP 시스템에 AutoSupport 메시지를 보낼 아웃바운드 인터넷 연결이 없는 경우 콘솔은 콘솔 에이전트에 포함된 프록시 서버를 사용하도록 해당 시스템을 자동으로 구성합니다. 유일한 요구 사항은 콘솔 에이전트의 보안 그룹이 포트 3128을 통한 인바운드 연결을 허용하는 것입니다. 콘솔 에이전트를 배포한 후 이 포트를 열어야 합니다.

NTP 활성화

NetApp Data Classification 사용하여 회사 데이터 소스를 스캔하려는 경우 콘솔 에이전트와 NetApp Data Classification 시스템 모두에서 NTP(네트워크 시간 프로토콜) 서비스를 활성화하여 시스템 간의 시간을 동기화해야 합니다. "NetApp 데이터 분류에 대해 자세히 알아보세요"

AWS 또는 **Azure**에 대한 콘솔 에이전트 클라우드 권한 만들기

온프레미스 콘솔 에이전트와 함께 AWS 또는 Azure에서 NetApp 데이터 서비스를 사용하려면 클라우드 공급자에서 권한을 설정해야 합니다. 그래야 콘솔 에이전트를 설치한 후 자격 증명을 추가할 수 있습니다.

사내에 설치된 콘솔 에이전트로는 Google Cloud의 리소스를 관리할 수 없습니다. Google Cloud 리소스를 관리하려면 Google Cloud에 에이전트를 설치해야 합니다.

AWS

온프레미스 콘솔 에이전트의 경우 IAM 사용자 액세스 키를 추가하여 AWS 권한을 제공합니다.

온프레미스 콘솔 에이전트에는 IAM 사용자 액세스 키를 사용하세요. 온프레미스 콘솔 에이전트에서는 IAM 역할이 지원되지 않습니다.

단계

1. AWS 콘솔에 로그인하고 IAM 서비스로 이동합니다.
2. 정책을 만듭니다.

   a. *정책 > 정책 만들기*를 선택합니다.

   b. *JSON*을 선택하고 내용을 복사하여 붙여넣습니다."콘솔 에이전트에 대한 IAM 정책" .

   c. 나머지 단계를 완료하여 정책을 만듭니다.

      사용하려는 NetApp 데이터 서비스에 따라 두 번째 정책을 만들어야 할 수도 있습니다.

   표준 지역의 경우 권한은 두 가지 정책에 걸쳐 분산됩니다. AWS의 관리형 정책에는 최대 문자 크기 제한이 있으므로 두 개의 정책이 필요합니다. "콘솔 에이전트에 대한 IAM 정책에 대해 자세히 알아보세요." .

3. IAM 사용자에게 정책을 연결합니다.
   - "AWS 설명서: IAM 역할 생성"
   - "AWS 설명서: IAM 정책 추가 및 제거"
4. 콘솔 에이전트를 설치한 후 NetApp Console 에 추가할 수 있는 액세스 키가 사용자에게 있는지 확인하세요.

결과

이제 필요한 권한이 있는 IAM 사용자 액세스 키가 있어야 합니다. 콘솔 에이전트를 설치한 후 콘솔에서 이러한 자격 증명을 콘솔 에이전트와 연결합니다.

하늘빛

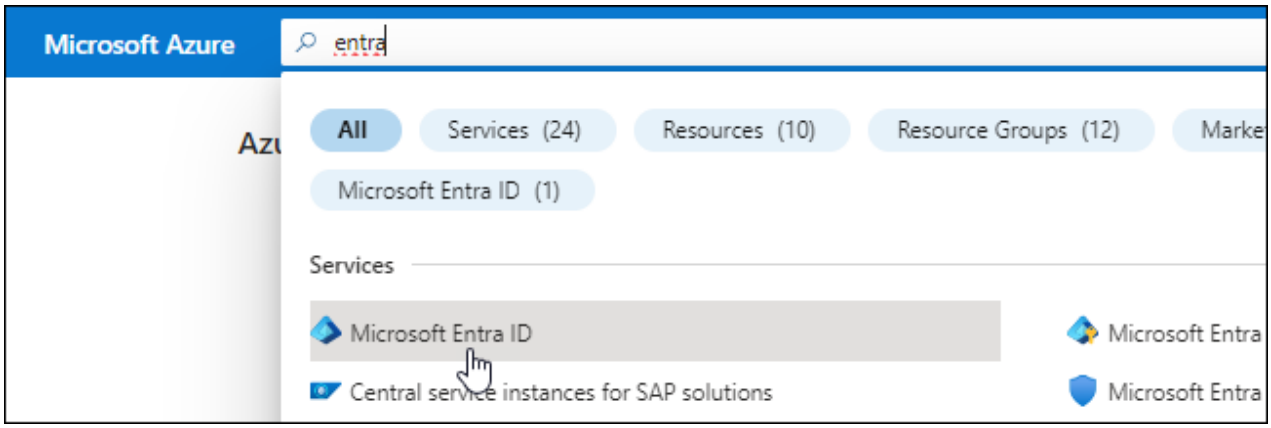
온프레미스에 콘솔 에이전트를 설치하는 경우 Microsoft Entra ID에서 서비스 주체를 설정하고 콘솔 에이전트에 필요한 Azure 자격 증명을 가져와서 콘솔 에이전트에 Azure 권한을 부여해야 합니다.

역할 기반 액세스 제어를 위한 **Microsoft Entra** 애플리케이션 만들기

1. Azure에서 Active Directory 애플리케이션을 만들고 해당 애플리케이션에 역할을 할당할 수 있는 권한이 있는지 확인하세요.

   자세한 내용은 다음을 참조하세요. "Microsoft Azure 설명서: 필요한 권한"

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



3. 메뉴에서 *앱 등록*을 선택하세요.
4. *신규 등록*을 선택하세요.
5. 신청서에 대한 세부 사항을 지정하세요:
   - 이름: 애플리케이션의 이름을 입력하세요.
   - 계정 유형: 계정 유형을 선택하세요(모든 계정 유형이 NetApp Console 에서 작동합니다).
   - 리디렉션 **URI**: 이 필드는 비워두어도 됩니다.
6. *등록*을 선택하세요.

   AD 애플리케이션과 서비스 주체를 생성했습니다.

역할에 애플리케이션 할당

1. 사용자 정의 역할 만들기:

   Azure Portal, Azure PowerShell, Azure CLI 또는 REST API를 사용하여 Azure 사용자 지정 역할을 만들 수 있습니다. 다음 단계에서는 Azure CLI를 사용하여 역할을 만드는 방법을 보여줍니다. 다른 방법을 사용하려면 다음을 참조하세요. "Azure 설명서"

   a. 내용을 복사하세요"콘솔 에이전트에 대한 사용자 정의 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.

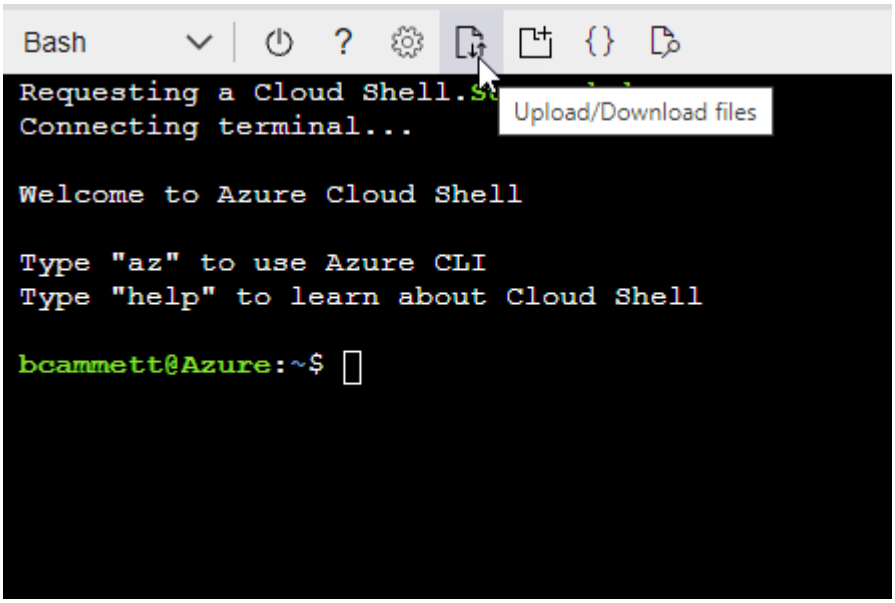
      예

      ```
      "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 만듭니다.

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

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



- Azure CLI를 사용하여 사용자 지정 역할을 만듭니다.

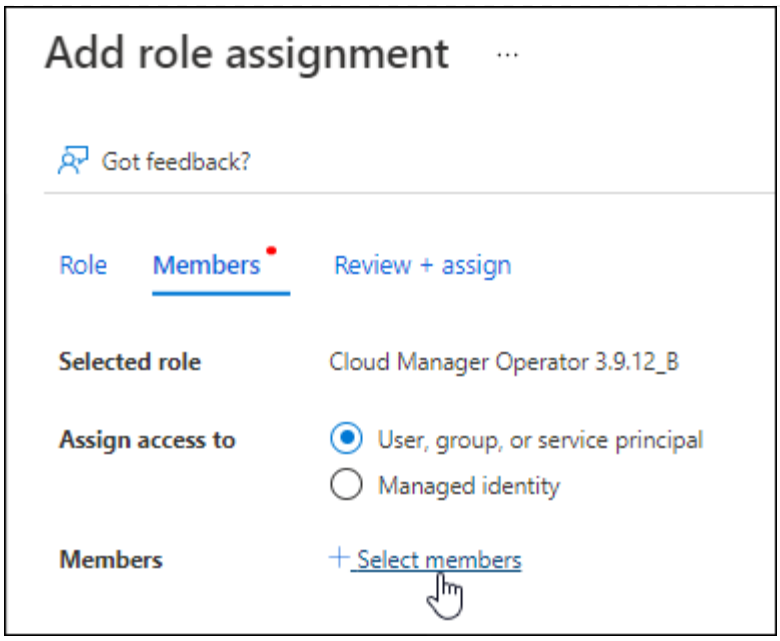
```
az role definition create --role-definition agent_Policy.json
```

이제 콘솔 에이전트 가상 머신에 할당할 수 있는 콘솔 운영자라는 사용자 지정 역할이 생겼습니다.

2. 역할에 애플리케이션을 할당합니다.

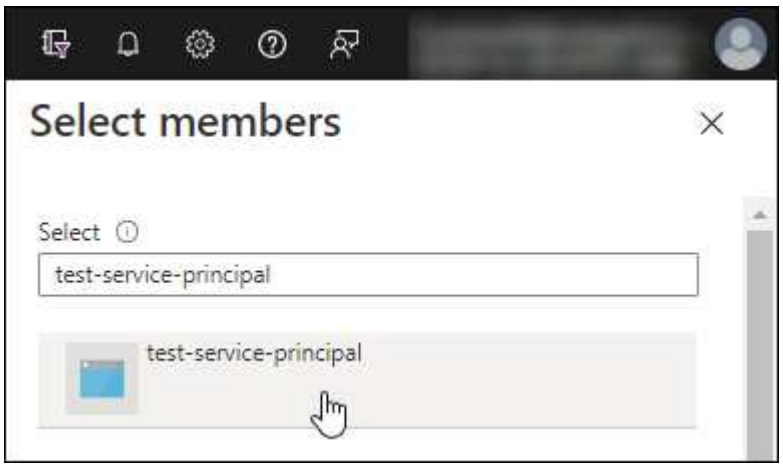
   a. Azure Portal에서 구독 서비스를 엽니다.
   b. 구독을 선택하세요.
   c. *액세스 제어(IAM) > 추가 > 역할 할당 추가*를 선택합니다.
   d. 역할 탭에서 콘솔 운영자 역할을 선택하고 *다음*을 선택합니다.
   e. 멤버 탭에서 다음 단계를 완료하세요.

      - *사용자, 그룹 또는 서비스 주체*를 선택된 상태로 유지합니다.
      - *멤버 선택*을 선택하세요.



- 애플리케이션 이름을 검색하세요.

  예를 들면 다음과 같습니다.



- 애플리케이션을 선택하고 *선택*을 선택하세요.
- *다음*을 선택하세요.

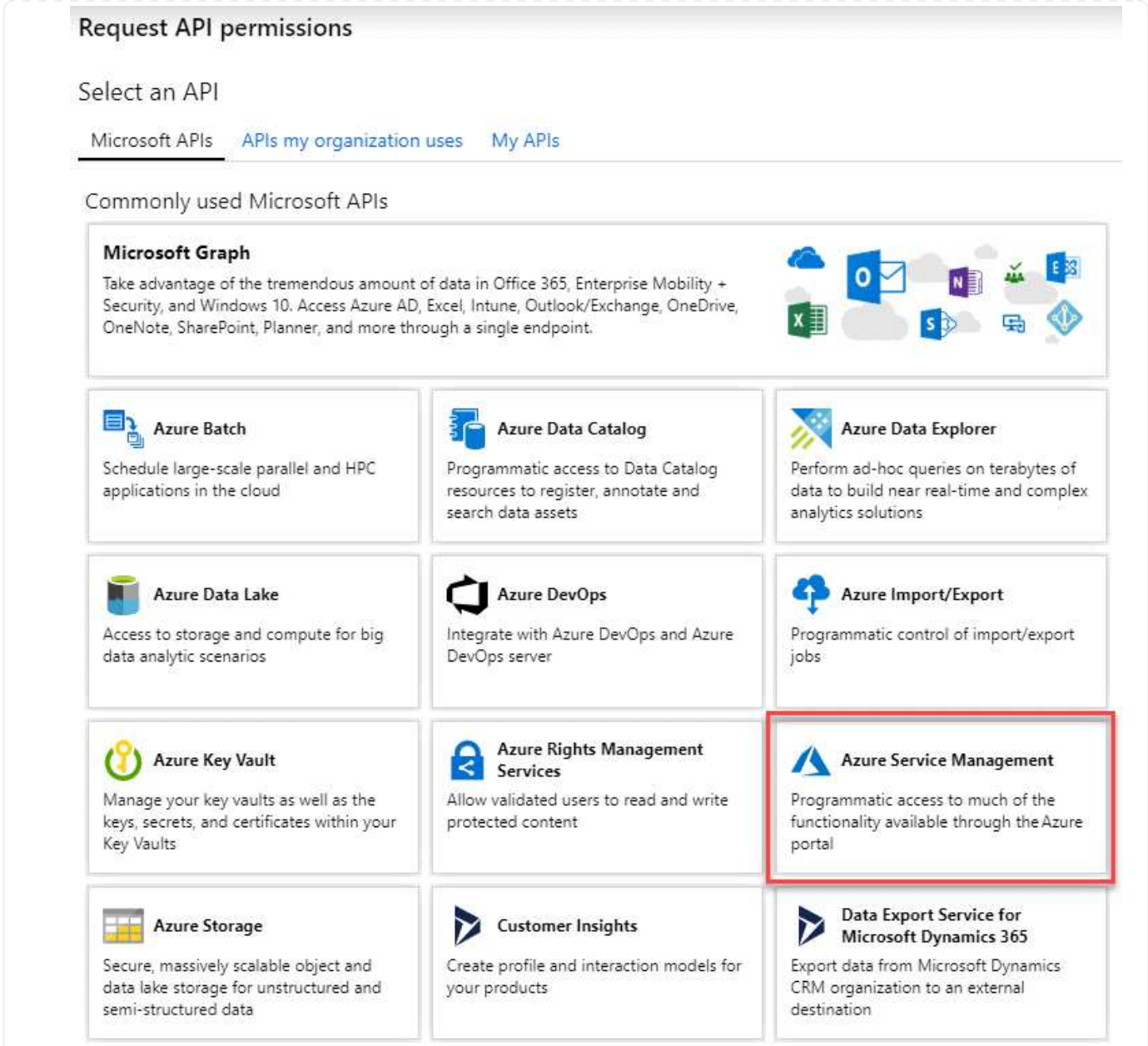
f. *검토 + 할당*을 선택하세요.

이제 서비스 주체는 콘솔 에이전트를 배포하는 데 필요한 Azure 권한을 갖게 되었습니다.

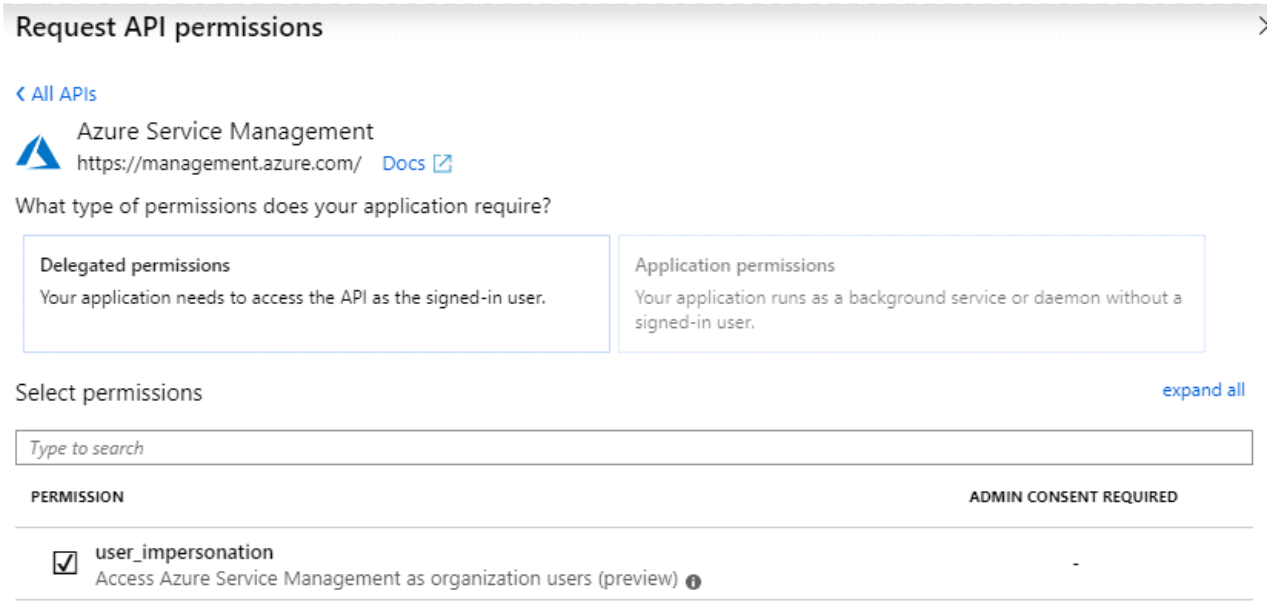
여러 Azure 구독에서 Cloud Volumes ONTAP 배포하려면 각 구독에 서비스 주체를 바인딩해야 합니다. NetApp Console 에서 Cloud Volumes ONTAP 배포할 때 사용할 구독을 선택할 수 있습니다.

Windows Azure 서비스 관리 **API** 권한 추가

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.

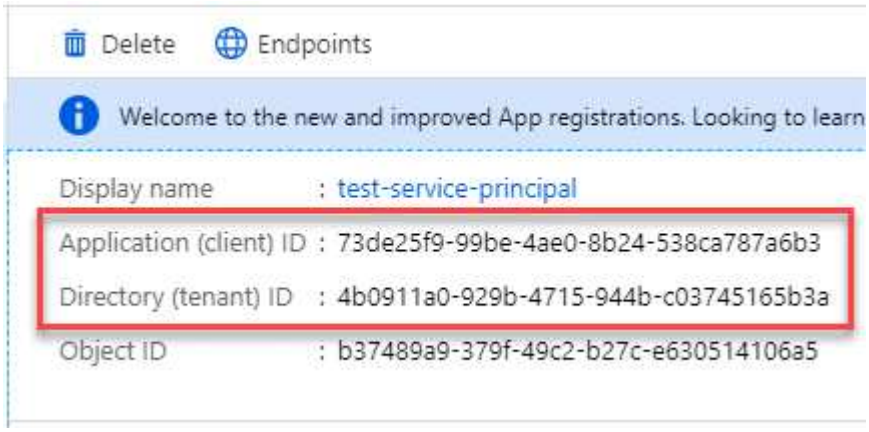


4. *조직 사용자로 Azure Service Management에 액세스*를 선택한 다음 *권한 추가*를 선택합니다.



애플리케이션의 애플리케이션 **ID**와 디렉토리 **ID**를 가져옵니다**.**

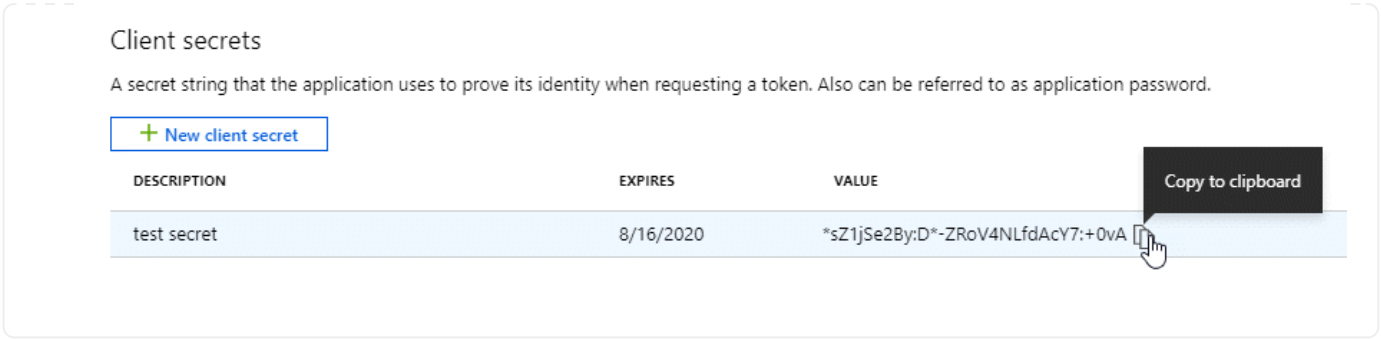
1. **Microsoft Entra ID** 서비스에서 *앱 등록*을 선택하고 애플리케이션을 선택합니다.
2. *애플리케이션(클라이언트) ID*와 *디렉토리(테넌트) ID*를 복사합니다.



콘솔에 Azure 계정을 추가하는 경우 애플리케이션(클라이언트) ID와 애플리케이션의 디렉터리(테넌트) ID를 제공해야 합니다. 콘솔은 ID를 사용하여 프로그래밍 방식으로 로그인합니다.

클라이언트 비밀을 생성하세요

1. **Microsoft Entra ID** 서비스를 엽니다.
2. *앱 등록*을 선택하고 애플리케이션을 선택하세요.
3. *인증서 및 비밀번호 > 새 클라이언트 비밀번호*를 선택합니다.
4. 비밀에 대한 설명과 기간을 제공하세요.
5. *추가*를 선택하세요.
6. 클라이언트 비밀번호 값을 복사합니다.



VCenter 환경에 콘솔 에이전트 설치

NetApp VCenter 환경에 콘솔 에이전트를 설치하는 것을 지원합니다. OVA 파일에는 VMware 환경에 배포할 수 있는 미리 구성된 VM 이미지가 포함되어 있습니다. 파일 다운로드나 URL 배포는 NetApp Console 에서 직접 사용할 수 있습니다. 여기에는 콘솔 에이전트 소프트웨어와 자체 서명 인증서가 포함됩니다.

OVA를 다운로드하거나 **URL**을 복사하세요

OVA를 다운로드하거나 NetApp Console 에서 OVA URL을 직접 복사하세요.

1. *관리 > 에이전트*를 선택하세요.
2. 개요 페이지에서 *에이전트 배포 > 온프레미스*를 선택합니다.
3. *OVA 포함*을 선택하세요.
4. OVA를 다운로드하거나 URL을 복사하여 VCenter에서 사용하세요.

VCenter에 에이전트를 배포하세요

에이전트를 배포하려면 VCenter 환경에 로그인하세요.

단계

1. 환경에 필요한 경우 신뢰할 수 있는 인증서에 자체 서명된 인증서를 업로드하세요. 설치 후 이 인증서를 교체합니다 ."자체 서명 인증서를 교체하는 방법을 알아보세요."
2. 콘텐츠 라이브러리나 로컬 시스템에서 OVA를 배포합니다.

로컬 시스템에서	콘텐츠 라이브러리에서
a. 마우스 오른쪽 버튼을 클릭하고 *OVF 템플릿 배포…*를 선택합니다. b. URL에서 OVA 파일을 선택하거나 해당 위치를 찾은 후 *다음*을 선택합니다.	a. 콘텐츠 라이브러리로 이동하여 콘솔 에이전트 OVA를 선택합니다. b. 작업 > *이 템플릿에서 새 VM*을 선택합니다.

3. OVF 템플릿 배포 마법사를 완료하여 콘솔 에이전트를 배포합니다.
4. VM의 이름과 폴더를 선택한 후 *다음*을 선택합니다.
5. 컴퓨팅 리소스를 선택한 후 *다음*을 선택합니다.
6. 템플릿의 세부 정보를 검토한 후 *다음*을 선택하세요.
7. 라이센스 계약에 동의한 후 *다음*을 선택하세요.
8. 사용할 프록시 구성 유형을 선택하세요: 명시적 프록시, 투명 프록시 또는 프록시 없음.

9. VM을 배포할 데이터 저장소를 선택한 후 *다음*을 선택합니다. 호스트 요구 사항을 충족하는지 확인하세요.
10. VM을 연결할 네트워크를 선택한 후 *다음*을 선택합니다. 네트워크가 IPv4이고 필요한 엔드포인트에 대한 아웃바운드 인터넷 액세스가 가능한지 확인하세요.
11. 템플릿 사용자 지정 창에서 다음 필드를 완료하세요.
    - 프록시 정보
      - 명시적 프록시를 선택한 경우 프록시 서버 호스트 이름이나 IP 주소, 포트 번호, 사용자 이름, 비밀번호를 입력하세요.
      - 투명 프록시를 선택한 경우 해당 인증서를 업로드하세요.
    - 가상 머신 구성
      - 구성 확인 건너뛰기: 이 확인란은 기본적으로 선택 해제되어 있으며, 이는 에이전트가 네트워크 액세스를 검증하기 위해 구성 확인을 실행한다는 것을 의미합니다.
        - NetApp 에이전트의 구성 검사를 설치 과정에 포함하도록 이 상자를 선택하지 않을 것을 권장합니다. 구성 검사는 에이전트가 필요한 엔드포인트에 대한 네트워크 액세스 권한이 있는지 확인합니다. 연결 문제로 인해 배포에 실패하면 에이전트 호스트에서 유효성 검사 보고서와 로그에 액세스할 수 있습니다. 어떤 경우에는 에이전트가 네트워크에 접속할 수 있다고 확신하는 경우 검사를 건너뛸 수 있습니다. 예를 들어, 여전히 다음을 사용하고 있는 경우"이전 종료점" 에이전트 업그레이드에 사용되면 유효성 검사가 오류로 인해 실패합니다. 이를 방지하려면 유효성 검사 없이 설치하려면 확인란을 선택하세요. "엔드포인트 목록을 업데이트하는 방법을 알아보세요" .
      - 유지관리 비밀번호 : 비밀번호를 설정하세요. `maint` 에이전트 유지 관리 콘솔에 액세스할 수 있는 사용자입니다.
      - **NTP** 서버: 시간 동기화를 위해 하나 이상의 NTP 서버를 지정합니다.
      - 호스트 이름: 이 VM의 호스트 이름을 설정합니다. 검색 도메인을 포함하면 안 됩니다. 예를 들어, console10.searchdomain.company.com의 FQDN은 console10으로 입력해야 합니다.
      - 기본 **DNS**: 이름 확인에 사용할 기본 DNS 서버를 지정합니다.
      - 보조 **DNS**: 이름 확인에 사용할 보조 DNS 서버를 지정합니다.
      - 검색 도메인: 호스트 이름을 확인할 때 사용할 검색 도메인 이름을 지정합니다. 예를 들어, FQDN이 console10.searchdomain.company.com이면 searchdomain.company.com을 입력합니다.
      - **IPv4** 주소: 호스트 이름에 매핑된 IP 주소입니다.
      - **IPv4** 서브넷 마스크: IPv4 주소의 서브넷 마스크입니다.
      - **IPv4** 게이트웨이 주소: IPv4 주소에 대한 게이트웨이 주소입니다.
12. *다음*을 선택하세요.
13. 완료 준비 창에서 세부 정보를 검토하고 *마침*을 선택하세요.

    vSphere 작업 표시줄에는 콘솔 에이전트가 배포됨에 따라 진행 상황이 표시됩니다.
14. VM의 전원을 켭니다.

> 배포에 실패하면 에이전트 호스트에서 검증 보고서와 로그에 액세스할 수 있습니다."설치 문제를 해결하는 방법을 알아보세요."

NetApp Console 에 콘솔 에이전트 등록

콘솔에 로그인하고 콘솔 에이전트를 조직과 연결합니다. 로그인 방법은 콘솔을 사용하는 모드에 따라 달라집니다. 표준 모드로 콘솔을 사용하는 경우 SaaS 웹사이트를 통해 로그인합니다. 제한 모드나 비공개 모드로 콘솔을 사용하는 경우 콘솔 에이전트 호스트에서 로컬로 로그인합니다.

단계

1. 웹 브라우저를 열고 콘솔 에이전트 호스트 URL을 입력하세요.

   콘솔 호스트 URL은 호스트 구성에 따라 로컬호스트, 개인 IP 주소 또는 공용 IP 주소가 될 수 있습니다. 예를 들어, 콘솔 에이전트가 공용 IP 주소가 없는 퍼블릭 클라우드에 있는 경우 콘솔 에이전트 호스트에 연결된 호스트의 개인 IP 주소를 입력해야 합니다.

2. 가입하거나 로그인하세요.
3. 로그인 후 콘솔을 설정하세요.
   a. 콘솔 에이전트와 연결할 콘솔 조직을 지정합니다.
   b. 시스템 이름을 입력하세요.
   c. *보안된 환경에서 실행하고 있습니까?*에서 제한 모드를 비활성화하세요.

      콘솔 에이전트가 온프레미스에 설치된 경우 제한 모드는 지원되지 않습니다.

   d. *시작하기*를 선택하세요.

콘솔에 클라우드 공급자 자격 증명 추가

콘솔 에이전트를 설치하고 설정한 후 클라우드 자격 증명을 추가하여 콘솔 에이전트가 AWS 또는 Azure에서 작업을 수행하는 데 필요한 권한을 갖도록 합니다.

AWS

시작하기 전에

AWS 자격 증명을 방금 만든 경우 사용할 수 있게 되는 데 몇 분이 걸릴 수 있습니다. 콘솔에 자격 증명을 추가하기 전에 몇 분 정도 기다리세요.

단계

1. *관리 > 자격 증명*을 선택합니다.
2. *조직 자격 증명*을 선택하세요.
3. *자격 증명 추가*를 선택하고 마법사의 단계를 따르세요.
   a. 자격 증명 위치: *Amazon Web Services > 에이전트를 선택하세요.
   b. 자격 증명 정의: AWS 액세스 키와 비밀 키를 입력합니다.
   c. 마켓플레이스 구독: 지금 구독하거나 기존 구독을 선택하여 마켓플레이스 구독을 이러한 자격 증명과 연결합니다.
   d. 검토: 새로운 자격 증명에 대한 세부 정보를 확인하고 *추가*를 선택합니다.

이제 다음으로 이동할 수 있습니다. "NetApp Console" 콘솔 에이전트를 사용하려면.

하늘빛

시작하기 전에

Azure 자격 증명을 방금 만든 경우 사용 가능해지는 데 몇 분 정도 걸릴 수 있습니다. 콘솔 에이전트에 자격 증명을 추가하기 전에 몇 분 정도 기다리세요.

단계

1. *관리 > 자격 증명*을 선택합니다.
2. *자격 증명 추가*를 선택하고 마법사의 단계를 따르세요.
   a. 자격 증명 위치: *Microsoft Azure > 에이전트*를 선택합니다.
   b. 자격 증명 정의: 필요한 권한을 부여하는 Microsoft Entra 서비스 주체에 대한 정보를 입력합니다.
      - 애플리케이션(클라이언트) ID
      - 디렉토리(테넌트) ID
      - 클라이언트 비밀번호
   c. 마켓플레이스 구독: 지금 구독하거나 기존 구독을 선택하여 마켓플레이스 구독을 이러한 자격 증명과 연결합니다.
   d. 검토: 새로운 자격 증명에 대한 세부 정보를 확인하고 *추가*를 선택합니다.

결과

이제 콘솔 에이전트는 Azure에서 사용자를 대신하여 작업을 수행하는 데 필요한 권한을 갖게 되었습니다. 이제 다음으로 이동할 수 있습니다. "NetApp Console" 콘솔 에이전트를 사용하려면.

온프레미스 콘솔 에이전트용 포트

콘솔 에이전트는 온프레미스 Linux 호스트에 수동으로 설치되는 경우 인바운드 포트를

사용합니다. 계획 목적으로 다음 항구를 참조하세요.

이러한 인바운드 규칙은 모든 NetApp Console 배포 모드에 적용됩니다.

규약	포트	목적
HTTP	80	• 클라이언트 웹 브라우저에서 로컬 사용자 인터페이스로 HTTP 액세스를 제공합니다. • Cloud Volumes ONTAP 업그레이드 프로세스 중에 사용됨
HTTPS	443	클라이언트 웹 브라우저에서 로컬 사용자 인터페이스로 HTTPS 액세스를 제공합니다.

콘솔 에이전트를 유지 관리합니다.

콘솔 에이전트에 대한 **VCenter** 또는 **ESXi** 호스트 유지 관리

콘솔 에이전트를 배포한 후 기존 VCenter 또는 ESXi 호스트를 변경할 수 있습니다. 예를 들어, 콘솔 에이전트를 호스팅하는 VM 인스턴스의 CPU나 RAM을 늘릴 수 있습니다.

VM 웹 콘솔을 사용하여 다음 유지 관리 작업을 수행합니다.

- 디스크 크기 늘리기
- 에이전트를 다시 시작하세요
- 정적 경로 업데이트
- 검색 도메인 업데이트

제한 사항

콘솔을 통해 에이전트를 업그레이드하는 기능은 아직 지원되지 않습니다. 또한 IP 주소, DNS, 게이트웨이에 대한 정보만 볼 수 있습니다.

VM 유지 관리 콘솔에 액세스

VSphere 클라이언트에서 유지 관리 콘솔에 액세스할 수 있습니다.

단계

1. VSphere 클라이언트를 열고 VCenter에 로그인합니다.
2. 콘솔 에이전트를 호스팅하는 VM 인스턴스를 선택합니다.
3. *웹 콘솔 실행*을 선택하세요.
4. VM 인스턴스를 생성할 때 지정한 사용자 이름과 비밀번호를 사용하여 VM 인스턴스에 로그인합니다. 사용자 이름은 `maint` 비밀번호는 VM 인스턴스를 생성할 때 지정한 비밀번호입니다.

메인트 사용자 비밀번호 변경

비밀번호를 변경할 수 있습니다. `maint` 사용자.

단계

1. VSphere 클라이언트를 열고 VCenter에 로그인합니다.

2. 콘솔 에이전트를 호스팅하는 VM 인스턴스를 선택합니다.
3. *웹 콘솔 실행*을 선택하세요.
4. VM 인스턴스를 생성할 때 지정한 사용자 이름과 비밀번호를 사용하여 VM 인스턴스에 로그인합니다. 사용자 이름은 `maint` 비밀번호는 VM 인스턴스를 생성할 때 지정한 비밀번호입니다.
5. 입력하다 `1` 보려면 `System Configuration` 메뉴.
6. 입력하다 `1` 유지 관리 사용자 비밀번호를 변경하고 화면의 지시를 따르세요.

VM 인스턴스의 CPU 또는 RAM을 늘리세요

콘솔 에이전트를 호스팅하는 VM 인스턴스의 CPU 또는 RAM을 늘릴 수 있습니다.

VCenter 또는 ESXi 호스트에서 VM 인스턴스 설정을 편집한 다음 유지 관리 콘솔을 사용하여 변경 사항을 적용합니다.

VSphere 클라이언트의 단계

1. VSphere 클라이언트를 열고 VCenter에 로그인합니다.
2. 콘솔 에이전트를 호스팅하는 VM 인스턴스를 선택합니다.
3. VM 인스턴스를 마우스 오른쪽 버튼으로 클릭하고 *설정 편집*을 선택합니다.
4. /opt 또는 /var 파티션에 사용되는 하드 드라이브 공간을 늘립니다.
   a. /opt에 사용되는 하드 드라이브 공간을 늘리려면 *하드 디스크 2*를 선택하세요.
   b. /var에 사용되는 하드 드라이브 공간을 늘리려면 *하드 디스크 3*을 선택하세요.
5. 변경 사항을 저장합니다.

유지 관리 콘솔의 단계

1. VSphere 클라이언트를 열고 VCenter에 로그인합니다.
2. 콘솔 에이전트를 호스팅하는 VM 인스턴스를 선택합니다.
3. *웹 콘솔 실행*을 선택하세요.
4. VM 인스턴스를 생성할 때 지정한 사용자 이름과 비밀번호를 사용하여 VM 인스턴스에 로그인합니다. 사용자 이름은 `maint` 비밀번호는 VM 인스턴스를 생성할 때 지정한 비밀번호입니다.
5. 입력하다 `1 to view the `System Configuration` 메뉴.
6. 입력하다 `2` 화면의 지시를 따르세요. 콘솔은 새로운 설정을 스캔하고 파티션 크기를 늘립니다.

에이전트 VM에 대한 네트워크 설정 보기

VSphere 클라이언트에서 에이전트 VM의 네트워크 설정을 보고 네트워크 문제를 확인하거나 해결합니다. 다음 네트워크 설정은 볼 수만 있고 업데이트할 수는 없습니다: IP 주소 및 DNS 세부 정보.

단계

1. VSphere 클라이언트를 열고 VCenter에 로그인합니다.
2. 콘솔 에이전트를 호스팅하는 VM 인스턴스를 선택합니다.
3. *웹 콘솔 실행*을 선택하세요.
4. VM 인스턴스를 생성할 때 지정한 사용자 이름과 비밀번호를 사용하여 VM 인스턴스에 로그인합니다. 사용자 이름은

`maint` 비밀번호는 VM 인스턴스를 생성할 때 지정한 비밀번호입니다.

5. 입력하다 `2` 보려면 `Network Configuration` 메뉴.
6. 1~6 사이의 숫자를 입력하면 해당 네트워크 설정을 볼 수 있습니다.

에이전트 **VM**에 대한 정적 경로를 업데이트합니다**.**

필요에 따라 에이전트 VM에 대한 정적 경로를 추가, 업데이트 또는 제거합니다.

단계

1. VSphere 클라이언트를 열고 VCenter에 로그인합니다.
2. 콘솔 에이전트를 호스팅하는 VM 인스턴스를 선택합니다.
3. *웹 콘솔 실행*을 선택하세요.
4. VM 인스턴스를 생성할 때 지정한 사용자 이름과 비밀번호를 사용하여 VM 인스턴스에 로그인합니다. 사용자 이름은 `maint` 비밀번호는 VM 인스턴스를 생성할 때 지정한 비밀번호입니다.
5. 입력하다 `2` 보려면 `Network Configuration` 메뉴.
6. 입력하다 `7` 정적 경로를 업데이트하고 화면의 지시를 따르세요.
7. Enter 키를 누르세요.
8. 선택적으로 추가 변경을 할 수 있습니다.
9. 입력하다 `9` 변경 사항을 커밋합니다.

에이전트 **VM**에 대한 도메인 검색 설정 업데이트

에이전트 VM에 대한 검색 도메인 설정을 업데이트할 수 있습니다.

단계

1. VSphere 클라이언트를 열고 VCenter에 로그인합니다.
2. 콘솔 에이전트를 호스팅하는 VM 인스턴스를 선택합니다.
3. *웹 콘솔 실행*을 선택하세요.
4. VM 인스턴스를 생성할 때 지정한 사용자 이름과 비밀번호를 사용하여 VM 인스턴스에 로그인합니다. 사용자 이름은 `maint` 비밀번호는 VM 인스턴스를 생성할 때 지정한 비밀번호입니다.
5. 입력하다 `2`` 보려면 `Network Configuration` 메뉴.
6. 입력하다 `8` 도메인 검색 설정을 업데이트하고 화면의 지시를 따르세요.
7. Enter 키를 누르세요.
8. 선택적으로 추가 변경을 할 수 있습니다.
9. 입력하다 `9` 변경 사항을 커밋합니다.

에이전트 진단 도구에 액세스하세요

콘솔 에이전트의 문제를 해결하기 위해 진단 도구에 액세스합니다. NetApp 지원팀에서 문제를 해결할 때 이를 요청할 수 있습니다.

단계

1. VSphere 클라이언트를 열고 VCenter에 로그인합니다.
2. 콘솔 에이전트를 호스팅하는 VM 인스턴스를 선택합니다.
3. *웹 콘솔 실행*을 선택하세요.
4. VM 인스턴스를 생성할 때 지정한 사용자 이름과 비밀번호를 사용하여 VM 인스턴스에 로그인합니다. 사용자 이름은 `maint` 비밀번호는 VM 인스턴스를 생성할 때 지정한 비밀번호입니다.
5. 입력하다 `3` 지원 및 진단 메뉴를 보려면.
6. 입력하다 `1` 진단 도구에 접근하고 화면의 지시를 따르세요. + 예를 들어, 모든 에이전트 서비스가 실행 중인지 확인할 수 있습니다. "콘솔 에이전트 상태 확인" .

원격으로 에이전트 진단 도구에 액세스하세요

Putty와 같은 도구를 사용하면 원격으로 진단 도구에 액세스할 수 있습니다. 일회용 비밀번호를 할당하여 에이전트 VM에 대한 SSH 액세스를 활성화합니다.

SSH 접속을 통해 복사 및 붙여넣기 같은 고급 터미널 기능을 사용할 수 있습니다.

단계

1. VSphere 클라이언트를 열고 VCenter에 로그인합니다.
2. 콘솔 에이전트를 호스팅하는 VM 인스턴스를 선택합니다.
3. *웹 콘솔 실행*을 선택하세요.
4. VM 인스턴스를 생성할 때 지정한 사용자 이름과 비밀번호를 사용하여 VM 인스턴스에 로그인합니다. 사용자 이름은 `maint` 비밀번호는 VM 인스턴스를 생성할 때 지정한 비밀번호입니다.
5. 입력하다 `3` 보려면 `Support and Diagnostics` 메뉴.
6. 입력하다 `2` 진단 도구에 액세스하고 화면의 지시에 따라 24시간 후에 만료되는 일회용 비밀번호를 구성합니다.
7. Putty와 같은 SSH 도구를 사용하여 사용자 이름을 사용하여 에이전트 VM에 연결합니다. `diag` 그리고 귀하가 구성한 일회용 비밀번호.

웹 기반 콘솔 액세스를 위한 **CA** 서명 인증서 설치

제한 모드에서 NetApp Console 사용하면 클라우드 지역이나 온프레미스에 배포된 콘솔 에이전트 가상 머신에서 사용자 인터페이스에 액세스할 수 있습니다. 기본적으로 콘솔은 자체 서명된 SSL 인증서를 사용하여 콘솔 에이전트에서 실행되는 웹 기반 콘솔에 대한 안전한 HTTPS 액세스를 제공합니다.

회사에 필요한 경우 인증 기관(CA)에서 서명한 인증서를 설치할 수 있습니다. 이는 자체 서명 인증서보다 더 강력한 보안 기능을 제공합니다. 인증서를 설치한 후, 사용자가 웹 기반 콘솔에 액세스할 때 콘솔은 CA 서명 인증서를 사용합니다.

HTTPS 인증서 설치

콘솔 에이전트에서 실행되는 웹 기반 콘솔에 대한 보안 액세스를 위해 CA에서 서명한 인증서를 설치합니다.

이 작업에 관하여

다음 옵션 중 하나를 사용하여 인증서를 설치할 수 있습니다.

- 콘솔에서 인증서 서명 요청(CSR)을 생성하고, CA에 인증서 요청을 제출한 다음 콘솔 에이전트에 CA 서명 인증서를 설치합니다.

  콘솔이 CSR을 생성하는 데 사용하는 키 쌍은 콘솔 에이전트에 내부적으로 저장됩니다. 콘솔 에이전트에 인증서를 설치하면 콘솔은 자동으로 동일한 키 쌍(개인 키)을 검색합니다.

- 이미 가지고 있는 CA 서명 인증서를 설치하세요.

  이 옵션을 사용하면 CSR이 콘솔을 통해 생성되지 않습니다. CSR을 별도로 생성하고 개인 키는 외부에 저장합니다. 인증서를 설치할 때 콘솔에 개인 키를 제공합니다.

단계

1. *관리 > 에이전트*를 선택하세요.
2. 개요 페이지에서 콘솔 에이전트의 작업 메뉴를 선택하고 *HTTPS 설정*을 선택합니다.

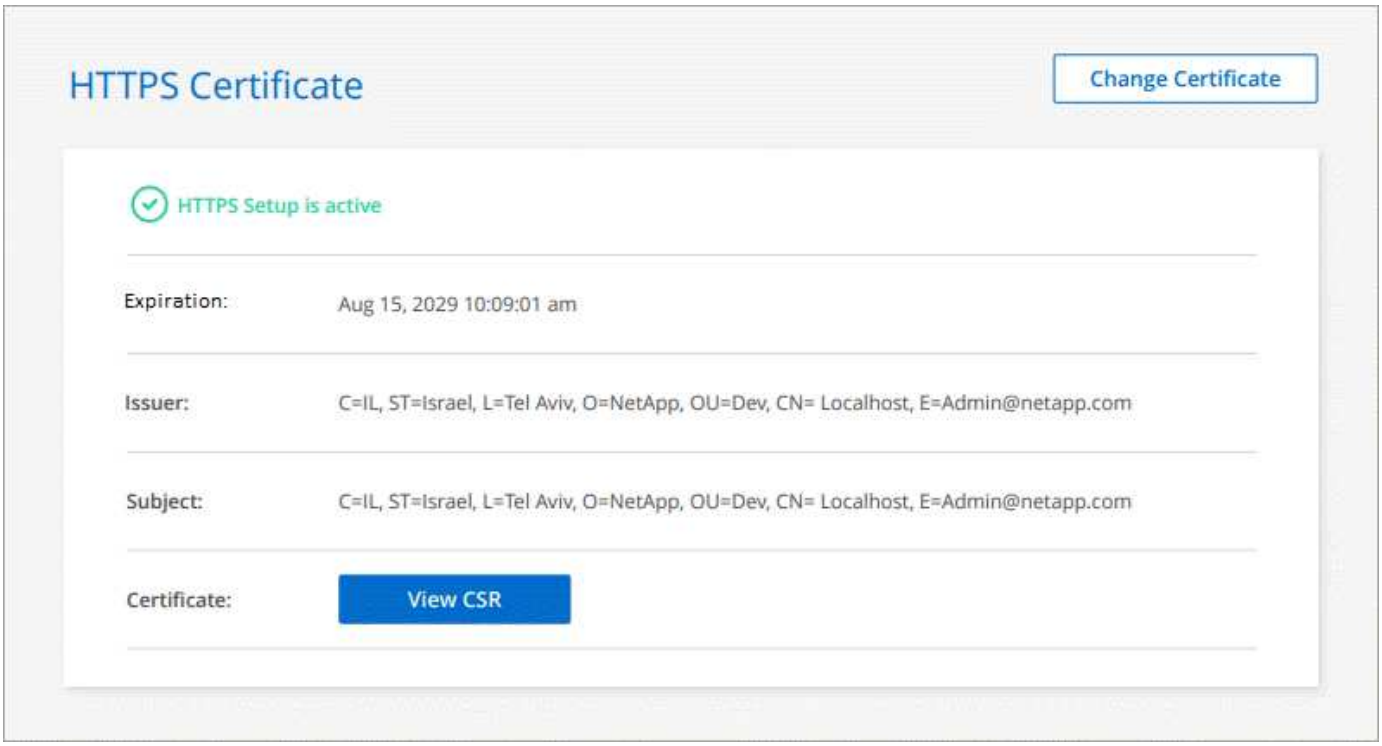
   콘솔 에이전트를 연결해야 편집할 수 있습니다.

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

옵션	설명
CSR 생성	a. 콘솔 에이전트 호스트의 호스트 이름이나 DNS(일반 이름)를 입력한 다음 *CSR 생성*을 선택합니다. 콘솔에 인증서 서명 요청이 표시됩니다. b. CSR을 사용하여 CA에 SSL 인증서 요청을 제출합니다. 인증서는 PEM(Privacy Enhanced Mail) Base-64 인코딩된 X.509 형식을 사용해야 합니다. c. 인증서 파일을 업로드한 다음 *설치*를 선택합니다.
CA 서명 인증서를 직접 설치하세요	a. *CA 서명 인증서 설치*를 선택합니다. b. 인증서 파일과 개인 키를 모두 로드한 다음 *설치*를 선택합니다. 인증서는 PEM(Privacy Enhanced Mail) Base-64 인코딩된 X.509 형식을 사용해야 합니다.

결과

콘솔 에이전트는 이제 CA 서명 인증서를 사용하여 안전한 HTTPS 액세스를 제공합니다. 다음 이미지는 보안 액세스를 위해 구성된 에이전트를 보여줍니다.



콘솔 **HTTPS** 인증서 갱신

보안 액세스를 보장하려면 에이전트의 HTTPS 인증서가 만료되기 전에 갱신해야 합니다. 인증서가 만료되기 전에 갱신하지 않으면 사용자가 HTTPS를 사용하여 웹 콘솔에 액세스할 때 경고가 나타납니다.

단계

1. *관리 > 에이전트*를 선택하세요.
2. 개요 페이지에서 콘솔 에이전트의 작업 메뉴를 선택하고 *HTTPS 설정*을 선택합니다.

   만료일을 포함한 인증서에 대한 세부 정보가 표시됩니다.

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

프록시 서버를 사용하도록 콘솔 에이전트 구성

회사 정책에 따라 모든 인터넷 통신에 프록시 서버를 사용해야 하는 경우 해당 프록시 서버를 사용하도록 에이전트를 구성해야 합니다. 설치 중에 콘솔 에이전트가 프록시 서버를 사용하도록 구성하지 않은 경우 언제든지 콘솔 에이전트가 해당 프록시 서버를 사용하도록 구성할 수 있습니다.

에이전트의 프록시 서버는 공용 IP나 NAT 게이트웨이 없이도 아웃바운드 인터넷 액세스를 가능하게 합니다. 프록시 서버는 Cloud Volumes ONTAP 시스템이 아닌 콘솔 에이전트에 대한 아웃바운드 연결만 제공합니다.

Cloud Volumes ONTAP 시스템에 아웃바운드 인터넷 액세스가 불가능한 경우 콘솔은 콘솔 에이전트의 프록시 서버를 사용하도록 구성합니다. 콘솔 에이전트의 보안 그룹이 포트 3128을 통한 인바운드 연결을 허용하는지 확인해야 합니다. 콘솔 에이전트를 배포한 후 이 포트를 엽니다.

콘솔 에이전트 자체에 아웃바운드 인터넷 연결이 없으면 Cloud Volumes ONTAP 시스템은 구성된 프록시 서버를 사용할 수 없습니다.

지원되는 구성

- Cloud Volumes ONTAP 시스템을 서비스하는 에이전트의 경우 투명 프록시 서버가 지원됩니다. Cloud Volumes ONTAP 과 함께 NetApp 데이터 서비스를 사용하는 경우 투명 프록시 서버를 사용할 수 있는 Cloud Volumes ONTAP 용 전용 에이전트를 만듭니다.
- 명시적 프록시 서버는 Cloud Volumes ONTAP 시스템을 관리하는 에이전트와 NetApp 데이터 서비스를 관리하는 에이전트를 포함한 모든 에이전트에서 지원됩니다.
- HTTP와 HTTPS.
- 프록시 서버는 클라우드나 네트워크에 있을 수 있습니다.

프록시를 구성한 후에는 프록시 유형을 변경할 수 없습니다. 프록시 유형을 변경해야 하는 경우 콘솔 에이전트를 제거하고 새 프록시 유형을 사용하여 새 에이전트를 추가합니다.

콘솔 에이전트에서 명시적 프록시 활성화

콘솔 에이전트가 프록시 서버를 사용하도록 구성하면 해당 에이전트와 해당 에이전트가 관리하는 Cloud Volumes ONTAP 시스템(HA 중재자 포함)은 모두 프록시 서버를 사용합니다.

이 작업을 수행하면 콘솔 에이전트가 다시 시작됩니다. 계속하기 전에 콘솔 에이전트가 유휴 상태인지 확인하세요.

단계

1. *관리 > 에이전트*를 선택하세요.
2. 개요 페이지에서 콘솔 에이전트의 작업 메뉴를 선택하고 *에이전트 편집*을 선택합니다.

   편집하려면 콘솔 에이전트가 활성화되어 있어야 합니다.

3. *HTTP 프록시 구성*을 선택하세요.
4. 구성 유형 필드에서 *명시적 프록시*를 선택합니다.
5. *프록시 사용*을 선택하세요.
6. 구문을 사용하여 서버를 지정하세요 http://address:port 또는 https://address:port
7. 서버에 기본 인증이 필요한 경우 사용자 이름과 비밀번호를 지정하세요.

   다음 사항에 유의하세요.

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

     예: netapp%92proxy

   - 콘솔은 @ 문자가 포함된 비밀번호를 지원하지 않습니다.
8. *저장*을 선택하세요.

콘솔 에이전트에 투명 프록시 활성화

Cloud Volumes ONTAP 만이 콘솔 에이전트에서 투명 프록시 사용을 지원합니다. Cloud Volumes ONTAP 외에

NetApp 데이터 서비스를 사용하는 경우 데이터 서비스나 Cloud Volumes ONTAP 에 사용할 별도의 에이전트를 만들어야 합니다.

투명 프록시를 활성화하기 전에 다음 요구 사항을 충족하는지 확인하세요.

- 에이전트는 투명 프록시 서버와 동일한 네트워크에 설치됩니다.
- 프록시 서버에서 TLS 검사가 활성화되어 있습니다.
- 투명 프록시 서버에서 사용되는 인증서와 일치하는 PEM 형식의 인증서가 있습니다.
- Cloud Volumes ONTAP 이외의 NetApp 데이터 서비스에는 콘솔 에이전트를 사용하지 마세요.

기존 에이전트가 투명 프록시 서버를 사용하도록 구성하려면 콘솔 에이전트 호스트의 명령줄을 통해 사용할 수 있는 콘솔 에이전트 유지 관리 도구를 사용합니다.

프록시 서버를 구성하면 콘솔 에이전트가 다시 시작됩니다. 계속하기 전에 콘솔 에이전트가 유휴 상태인지 확인하세요.

단계

프록시 서버에 대한 PEM 형식의 인증서 파일이 있는지 확인하세요. 인증서가 없으면 네트워크 관리자에게 문의하여 인증서를 받으세요.

1. 콘솔 에이전트 호스트에서 명령줄 인터페이스를 엽니다.
2. 콘솔 에이전트 유지 관리 도구 디렉토리로 이동합니다. `/opt/application/netapp/service-manager-2/agent-maint-console`
3. 투명 프록시를 활성화하려면 다음 명령을 실행하세요. `/home/ubuntu/<certificate-file>.pem` 프록시 서버에 대한 디렉토리 및 이름 인증서 파일입니다.

   ```
   ./agent-maint-console proxy add -c /home/ubuntu/<certificate-file>.pem
   ```

   인증서 파일이 PEM 형식이고 명령과 같은 디렉토리에 있는지 확인하거나 인증서 파일의 전체 경로를 지정하세요.

   ```
   ./agent-maint-console proxy add -c /home/ubuntu/<certificate-file>.pem
   ```

콘솔 에이전트에 대한 투명 프록시 수정

콘솔 에이전트의 기존 투명 프록시 서버는 다음 방법을 사용하여 업데이트할 수 있습니다. `proxy update` 명령어를 사용하거나 투명 프록시 서버를 제거하려면 다음 방법을 사용하십시오. `proxy remove` 명령. 더 자세한 내용은 관련 문서를 참조하십시오."에이전트 유지 관리 콘솔" .

> 프록시를 구성한 후에는 프록시 유형을 변경할 수 없습니다. 프록시 유형을 변경해야 하는 경우 콘솔 에이전트를 제거하고 새 프록시 유형을 사용하여 새 에이전트를 추가합니다.

인터넷에 액세스할 수 없게 되면 콘솔 에이전트 프록시를 업데이트합니다.

네트워크의 프록시 구성이 변경되면 에이전트가 인터넷에 액세스할 수 없게 될 수 있습니다. 예를 들어, 누군가가 프록시 서버의 비밀번호를 변경하거나 인증서를 업데이트하는 경우입니다. 이 경우 콘솔 에이전트 호스트에서 직접 UI에 액세스하여 설정을 업데이트해야 합니다. 콘솔 에이전트 호스트에 대한 네트워크 액세스가 가능하고 콘솔에 로그인할 수

있는지 확인하세요.

직접 API 트래픽 활성화

프록시 서버를 사용하도록 콘솔 에이전트를 구성한 경우 프록시를 거치지 않고 클라우드 공급자 서비스로 API 호출을 직접 보내기 위해 콘솔 에이전트에서 직접 API 트래픽을 활성화할 수 있습니다. AWS, Azure 또는 Google Cloud에서 실행되는 에이전트는 이 옵션을 지원합니다.

Cloud Volumes ONTAP 사용하여 Azure Private Links를 비활성화하고 서비스 엔드포인트를 사용하는 경우 직접 API 트래픽을 활성화합니다. 그렇지 않으면 트래픽이 제대로 라우팅되지 않습니다.

"Cloud Volumes ONTAP 에서 Azure Private Link 또는 서비스 엔드포인트를 사용하는 방법에 대해 자세히 알아보세요."

단계

1. *관리 > 에이전트*를 선택하세요.
2. 개요 페이지에서 콘솔 에이전트의 작업 메뉴를 선택하고 *에이전트 편집*을 선택합니다.

   편집하려면 콘솔 에이전트가 활성화되어 있어야 합니다.

3. *직접 API 트래픽 지원*을 선택하세요.
4. 옵션을 활성화하려면 확인란을 선택한 다음 *저장*을 선택하세요.

콘솔 에이전트 문제 해결

콘솔 에이전트의 문제를 해결하려면 직접 문제를 확인하거나 NetApp 지원팀에 문의하여 시스템 ID, 에이전트 버전 또는 최신 AutoSupport 메시지를 요청할 수 있습니다.

NetApp 지원 사이트 계정이 있는 경우 다음을 볼 수도 있습니다."NetApp 지식 기반."

일반적인 오류 메시지 및 해결 방법

이 표는 일반적인 오류 메시지와 해결 방법을 보여줍니다.

오류 메시지	설명	무엇을 해야 할까
콘솔 에이전트 UI를 로드할 수 없습니다.	에이전트 설치에 실패했습니다	• 서비스 관리자 서비스가 활성화되어 있는지 확인하세요. • 모든 컨테이너가 실행 중인지 확인하세요. • 방화벽이 포트 8888에서 서비스에 대한 액세스를 허용하는지 확인하세요. • 문제가 계속 발생하면 고객 지원팀에 문의하십시오.

오류 메시지	설명	무엇을 해야 할까
NetApp 에이전트 UI에 액세스할 수 없습니다.	이 메시지는 에이전트의 IP 주소에 접근하려고 할 때 나타납니다. 에이전트가 올바른 네트워크 액세스 권한이 없거나 불안정한 경우 초기화에 실패할 수 있습니다.	• 콘솔 에이전트에 연결합니다. • 서비스 관리자 서비스를 확인하세요 • 에이전트가 필요한 네트워크 접근 권한을 가지고 있는지 확인하세요. "필수 네트워크 액세스 엔드포인트에 대해 자세히 알아보세요."
에이전트 설정을 로드할 수 없습니다.	에이전트 설정 페이지에 접근하려고 하면 콘솔에 이 메시지가 표시됩니다.	• OCCM 컨테이너가 실행 중이고 제대로 작동하는지 확인하세요. • 문제가 지속되면 지원팀에 문의하세요.
에이전트에 대한 지원 정보를 로드할 수 없습니다.	이 메시지는 상담원이 귀하의 지원 계정에 액세스할 수 없는 경우 표시됩니다.	• 에이전트가 필요한 엔드포인트에 대한 아웃바운드 액세스 권한을 가지고 있는지 확인하십시오."필수 네트워크 액세스 엔드포인트에 대해 자세히 알아보세요."

콘솔 에이전트 상태 확인

다음 명령 중 하나를 사용하여 콘솔 에이전트를 확인하세요. 모든 서비스의 상태는 _실행중_이어야 합니다. 그렇지 않은 경우 NetApp 지원팀에 문의하세요.

콘솔 에이전트 진단에 액세스하는 방법에 대한 자세한 내용은 다음 항목을 참조하세요.

- "콘솔 에이전트 상태 확인(Linux 호스트 배포용)"
- "콘솔 에이전트 상태 확인(VCenter 배포용)"

Docker(Ubuntu 및 VCenter 배포용)

```
docker ps -a
```

Podman(RedHat Enterprise Linux 배포용)

```
podman ps -a
```

콘솔 에이전트 버전 보기

업그레이드를 확인하려면 콘솔 에이전트 버전을 확인하거나 NetApp 담당자와 공유하세요.

단계

1. *관리 > 지원 > 에이전트*를 선택하세요.

   콘솔은 페이지 상단에 버전을 표시합니다.

네트워크 접속 확인

콘솔 에이전트에 필요한 네트워크 액세스 권한이 있는지 확인하세요."필요한 네트워크 액세스 포인트에 대해 자세히 알아보세요."

콘솔 에이전트에 대한 구성 검사를 실행합니다.

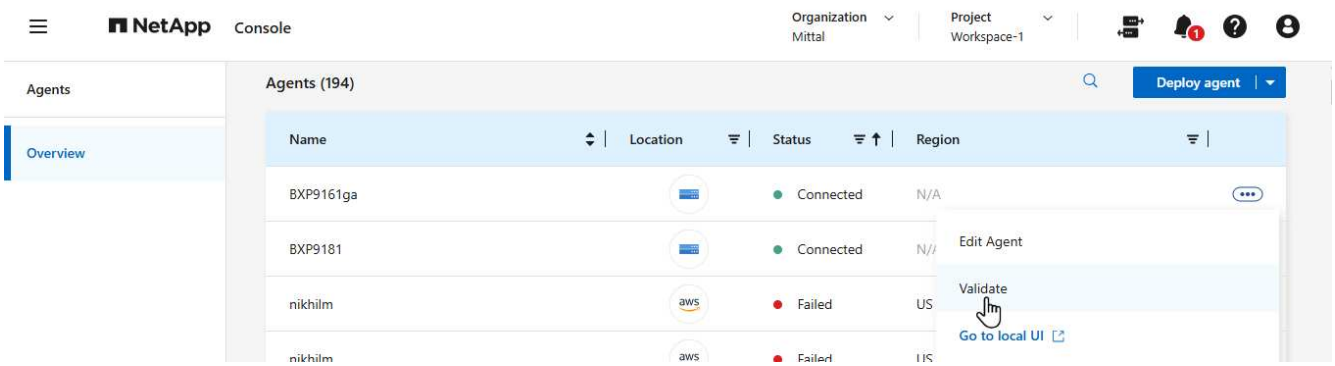
콘솔 또는 에이전트 유지 관리 콘솔에서 콘솔 에이전트에 대한 구성 검사를 실행하여 연결 상태를 확인하십시오.

에이전트 유지 관리 콘솔을 사용하여 구성 검사를 실행할 수도 있습니다."config-checker validate 명령어 사용 방법에 대해 자세히 알아보세요."

연결됨 상태인 에이전트만 인증할 수 있습니다.

콘솔에서 시작하는 단계

1. *관리 > 에이전트*를 선택하세요.
2. 확인하려는 콘솔 에이전트의 작업 메뉴를 선택하고 *유효성 검사*를 선택합니다.



검증에는 최대 15분이 소요될 수 있습니다. 결과는 완료되면 표시됩니다.

콘솔 에이전트 설치 문제

설치에 실패하면 보고서와 로그를 보고 문제를 해결하세요.

다음 디렉토리에 있는 콘솔 에이전트 호스트에서 직접 JSON 형식의 검증 보고서와 구성 로그에 액세스할 수도 있습니다.

```
/tmp/netapp-console-agents/logs

/tmp/netapp-console-agents/results.json
```

- 새로운 에이전트 배포의 경우 NetApp 다음 엔드포인트를 확인합니다."여기에 나열됨" . 업그레이드에 사용된 이전 엔드포인트를 사용하는 경우 이 구성 검사는 오류로 실패합니다."여기에 나열됨" . NetApp 최대한 빨리 현재 엔드포인트에 대한 액세스를 허용하고 이전 엔드포인트에 대한 액세스를 차단하도록 방화벽 규칙을 업데이트할 것을 권장합니다."네트워킹을 업데이트하는 방법을 알아보세요" .
- 방화벽의 엔드포인트를 업데이트하면 기존 에이전트가 계속 작동합니다.

수동 설치에 대한 구성 확인 비활성화

설치 중에 아웃바운드 연결을 확인하는 구성 검사를 비활성화해야 할 때가 있을 수 있습니다. 예를 들어, 정부 클라우드 환경에 에이전트를 수동으로 설치할 때는 구성 검사를 비활성화해야 합니다. 그렇지 않으면 설치가 실패합니다.

단계

com/opt/application/netapp/service-manager-2/config.json 파일에서 *skipConfigCheck* 플래그를 설정하여 구성 확인을 비활성화합니다. 기본적으로 이 플래그는 false로 설정되고 구성 검사는 에이전트에 대한 아웃바운드 액세스를 확인합니다. 검사를 비활성화하려면 이 플래그를 true로 설정합니다. 이 단계를 완료하기 전에 JSON 구문에 익숙해지십시오.

구성 확인을 다시 활성화하려면 다음 단계를 사용하고 *skipConfigCheck* 플래그를 false로 설정합니다.

단계

1. 루트 또는 sudo 권한으로 콘솔 에이전트 호스트에 액세스합니다.
2. 변경 사항을 되돌릴 수 있도록 */opt/application/netapp/service-manager-2/config.json* 파일의 백업 사본을 만드세요.
3. 다음 명령을 실행하여 서비스 관리자 2 서비스를 중지합니다.

```
systemctl stop netapp-service-manager.service
```

1. */opt/application/netapp/service-manager-2/config.json* 파일을 편집하고 *skipConfigCheck* 플래그 값을 true로 변경합니다.

```
  "skipConfigCheck": true
```

2. 파일을 저장하세요.
3. 다음 명령을 실행하여 서비스 관리자 2 서비스를 다시 시작합니다.

```
systemctl restart netapp-service-manager.service
```

NetApp 지원팀과 협력하세요

콘솔 에이전트로 문제를 해결할 수 없는 경우 NetApp 지원팀에 문의해 보세요. NetApp 지원팀에서는 콘솔 에이전트 ID를 요청할 수도 있고, 아직 콘솔 에이전트 로그가 없는 경우 해당 로그를 NetApp 지원팀으로 보내달라고 요청할 수도 있습니다.

콘솔 에이전트 ID 찾기

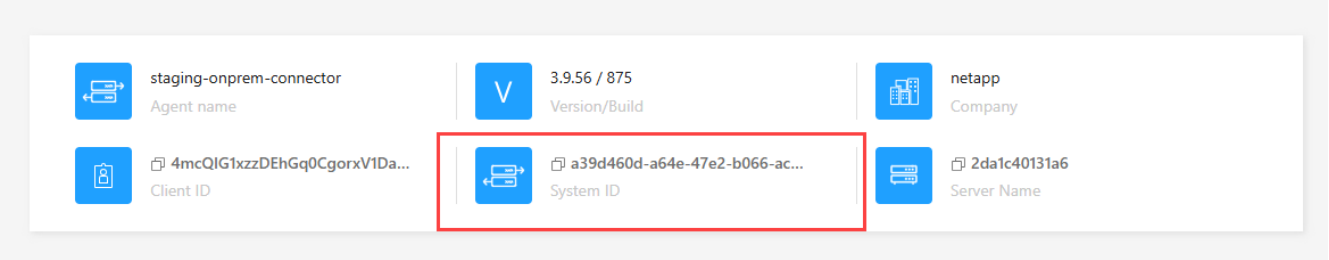
시작하는 데 도움이 되도록 콘솔 에이전트의 시스템 ID가 필요할 수 있습니다. ID는 일반적으로 라이선싱 및 문제 해결 목적으로 사용됩니다.

단계

1. *관리 > 지원 > 에이전트*를 선택하세요.

시스템 ID는 페이지 상단에서 확인할 수 있습니다.

예



2. ID에 마우스를 올려놓고 클릭하면 복사됩니다.

AutoSupport 메시지를 다운로드하거나 보내세요

문제가 발생하는 경우 NetApp 문제 해결을 위해 NetApp 지원팀에 AutoSupport 메시지를 보내달라고 요청할 수 있습니다.

NetApp Console 부하 분산으로 인해 AutoSupport 메시지를 보내는 데 최대 5시간이 걸립니다. 긴급한 연락이 필요한 경우, 파일을 다운로드하여 직접 보내주시기 바랍니다.

단계

1. *관리 > 지원 > 에이전트*를 선택하세요.
2. NetApp 지원팀에 정보를 보내는 방법에 따라 다음 옵션 중 하나를 선택하세요.
   a. AutoSupport 메시지를 로컬 컴퓨터에 다운로드하는 옵션을 선택하세요. 그런 다음 선호하는 방법을 사용하여 NetApp 지원팀에 보낼 수 있습니다.
   b. * AutoSupport 보내기*를 선택하면 NetApp 지원팀에 직접 메시지를 보낼 수 있습니다.

Google Cloud NAT 게이트웨이 사용 시 다운로드 실패 문제 해결

콘솔 에이전트는 Cloud Volumes ONTAP 에 대한 소프트웨어 업데이트를 자동으로 다운로드합니다. Google Cloud NAT 게이트웨이를 사용하는 경우 구성으로 인해 다운로드가 실패할 수 있습니다. 이 문제는 소프트웨어 이미지가 나누어지는 부분의 수를 제한하면 해결할 수 있습니다. 이 단계는 API를 사용하여 완료해야 합니다.

단계

1. 다음 JSON을 본문으로 하여 /occm/config에 PUT 요청을 제출합니다.

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

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

32는 예시 값입니다. 값은 NAT 구성과 동시 세션 수에 따라 달라집니다.

"/occm/config API 호출에 대해 자세히 알아보세요"

NetApp 지식 기반에서 도움 받기

"NetApp 지원팀에서 생성한 문제 해결 정보 보기" .

콘솔 에이전트 제거 및 제거

문제를 해결하거나 호스트에서 영구적으로 제거하려면 콘솔 에이전트를 제거하세요. 사용해야 하는 단계는 사용하는 배포 모드에 따라 달라집니다. 환경에서 콘솔 에이전트를 제거한 후에는 콘솔에서 제거할 수 있습니다.

"NetApp Console 배포 모드에 대해 알아보세요" .

표준 모드 또는 제한 모드를 사용할 때 에이전트를 제거합니다.

표준 모드나 제한 모드(즉, 에이전트 호스트에 아웃바운드 연결이 있는 경우)를 사용하는 경우 아래 단계에 따라 에이전트를 제거해야 합니다.

단계

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

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

   _silent_는 확인을 묻지 않고 스크립트를 실행합니다.

콘솔에서 콘솔 에이전트 제거

에이전트 VM을 삭제하거나 에이전트를 설치 해제한 경우 콘솔의 에이전트 목록에서 해당 에이전트를 제거해야 합니다. 에이전트 VM을 삭제하거나 에이전트 소프트웨어를 제거한 후 에이전트는 콘솔에서 연결 끊김 상태로 표시됩니다.

콘솔 에이전트를 제거하는 방법에 대한 자세한 내용은 다음과 같습니다.

- 이 작업을 수행해도 가상 머신은 삭제되지 않습니다.
- 이 작업은 되돌릴 수 없습니다. 콘솔 에이전트를 제거하면 다시 추가할 수 없습니다.

단계

1. *관리 > 에이전트*를 선택하세요.
2. 개요 페이지에서 연결이 끊긴 에이전트에 대한 작업 메뉴를 선택하고 *에이전트 제거*를 선택합니다.
3. 확인하려면 에이전트 이름을 입력한 후 *제거*를 선택하세요.

클라우드 공급자 자격 증명 관리

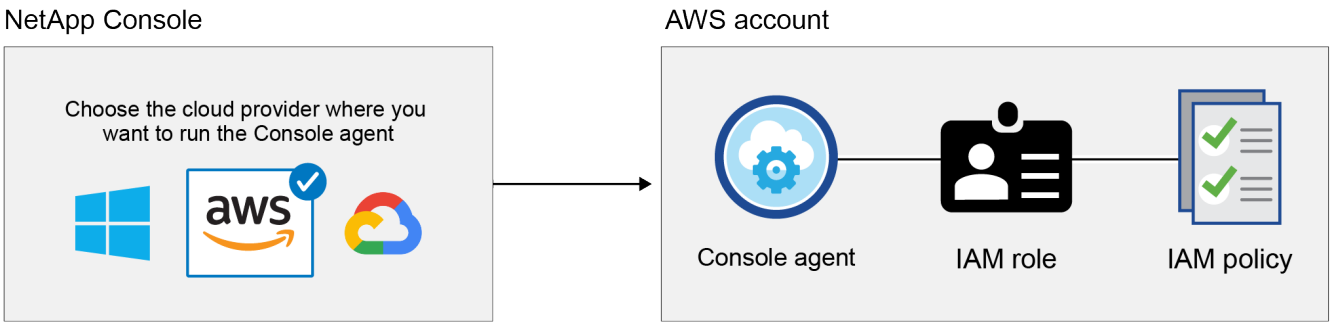
AWS

NetApp Console 에서 직접 AWS 자격 증명과 마켓플레이스 구독을 관리하여 콘솔 에이전트 배포 중에 적절한 IAM 자격 증명을 제공하고 청구를 위해 이를 AWS Marketplace 구독과 연결함으로써 Cloud Volumes ONTAP 및 기타 데이터 서비스의 안전한 배포를 보장합니다.

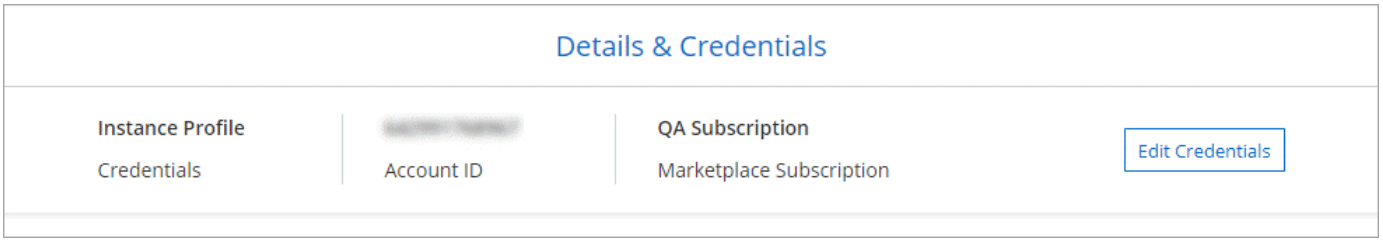
초기 AWS 자격 증명

콘솔에서 콘솔 에이전트를 배포하는 경우 IAM 사용자의 IAM 역할 또는 액세스 키의 ARN을 제공해야 합니다. 인증 방법에는 AWS에 콘솔 에이전트를 배포할 수 있는 권한이 있어야 합니다. 필요한 권한은 다음에 나열되어 있습니다 ."AWS에 대한 에이전트 배포 정책" .

콘솔이 AWS에서 콘솔 에이전트를 시작하면 에이전트에 대한 IAM 역할과 프로필이 생성됩니다. 또한 AWS 계정 내에서 리소스와 프로세스를 관리할 수 있는 권한을 콘솔 에이전트에 제공하는 정책도 첨부합니다. "에이전트가 권한을 사용하는 방식을 검토하세요.".



새로운 Cloud Volumes ONTAP 시스템을 추가하는 경우 콘솔은 기본적으로 다음 AWS 자격 증명을 선택합니다.



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

추가 AWS 자격 증명

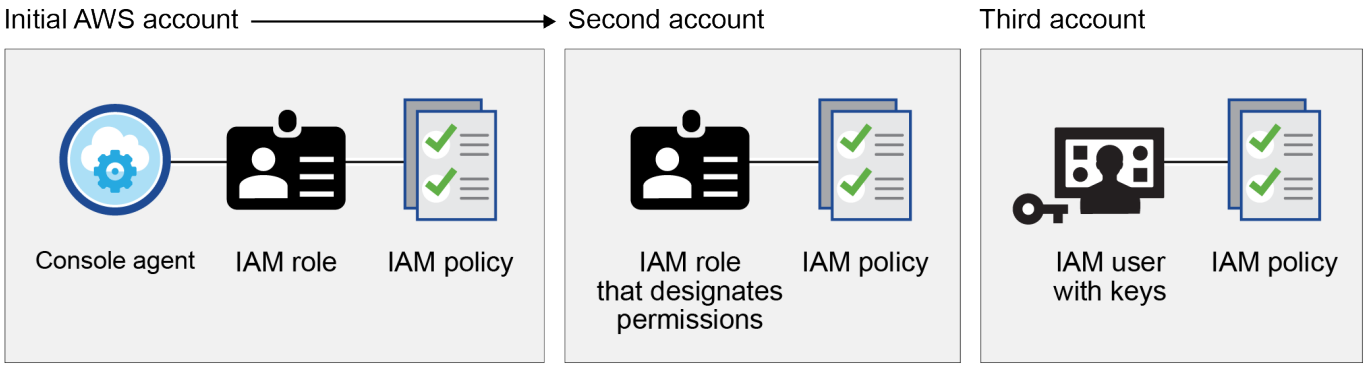
다음과 같은 경우 콘솔에 추가 AWS 자격 증명을 추가할 수 있습니다.

- 기존 콘솔 에이전트를 추가 AWS 계정과 함께 사용하려면
- 특정 AWS 계정에서 새 에이전트를 생성하려면
- ONTAP 파일 시스템용 FSx를 생성하고 관리하려면

자세한 내용은 아래 섹션을 참조하세요.

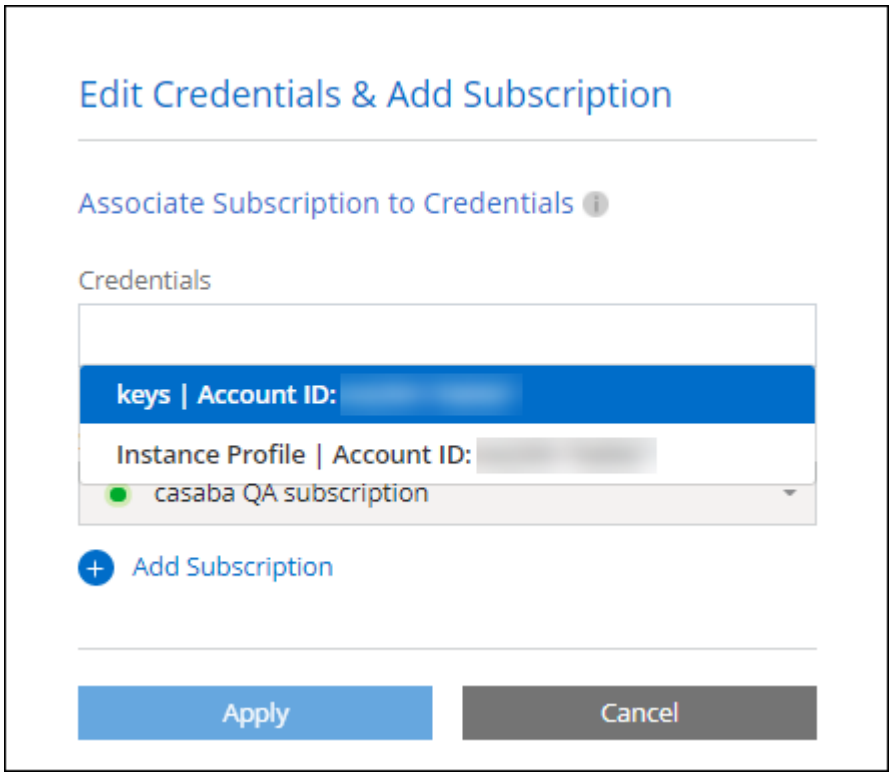
다른 **AWS** 계정으로 콘솔 에이전트를 사용하려면 **AWS** 자격 증명을 추가하세요.

추가 AWS 계정으로 콘솔을 사용하려면 신뢰할 수 있는 계정의 역할에 대한 AWS 키 또는 ARN을 제공하세요. 다음 이미지는 두 개의 추가 계정을 보여줍니다. 하나는 신뢰할 수 있는 계정의 IAM 역할을 통해 권한을 제공하고, 다른 하나는 IAM 사용자의 AWS 키를 통해 권한을 제공합니다.



IAM 역할의 Amazon 리소스 이름(ARN)이나 IAM 사용자의 AWS 키를 지정하여 콘솔에 계정 자격 증명을 추가합니다.

예를 들어, 새로운 Cloud Volumes ONTAP 시스템을 생성할 때 자격 증명 간에 전환할 수 있습니다.



"기존 에이전트에 AWS 자격 증명을 추가하는 방법을 알아보세요."

AWS 자격 증명을 추가하여 콘솔 에이전트를 만듭니다.

AWS 자격 증명을 추가하면 콘솔 에이전트를 생성할 수 있는 권한이 제공됩니다.

"콘솔 에이전트를 생성하기 위해 콘솔에 AWS 자격 증명을 추가하는 방법을 알아보세요."

FSx for ONTAP 에 대한 AWS 자격 증명 추가

FSx for ONTAP 시스템을 생성하고 관리하는 데 필요한 권한을 제공하려면 AWS 자격 증명을 콘솔에 추가합니다.

"Amazon FSx for ONTAP 콘솔에 AWS 자격 증명을 추가하는 방법을 알아보세요."

자격 증명 및 마켓플레이스 구독

시간당 요금(PAYGO)으로 Cloud Volumes ONTAP 및 기타 NetApp 데이터 서비스에 대한 비용을 지불하거나 연간 계약을 통해 비용을 지불하려면 콘솔 에이전트에 추가하는 자격 증명을 AWS Marketplace 구독과 연결해야 합니다. "AWS 구독을 연결하는 방법 알아보기".

AWS 자격 증명 및 마켓플레이스 구독에 대해 다음 사항을 참고하세요.

- AWS 자격 증명 세트에는 단 하나의 AWS Marketplace 구독만 연결할 수 있습니다.
- 기존 마켓플레이스 구독을 새 구독으로 교체할 수 있습니다.

자주 묻는 질문

다음 질문은 자격 증명 및 구독과 관련이 있습니다.

AWS 자격 증명을 안전하게 회전하려면 어떻게 해야 하나요?

위 섹션에서 설명한 대로 콘솔을 사용하면 여러 가지 방법으로 AWS 자격 증명을 제공할 수 있습니다. 콘솔 에이전트와 연결된 IAM 역할, 신뢰할 수 있는 계정에서 IAM 역할을 맡는 방법, AWS 액세스 키를 제공하는 방법 등이 있습니다.

처음 두 가지 옵션을 사용하면 콘솔은 AWS 보안 토큰 서비스를 사용하여 지속적으로 순환되는 임시 자격 증명을 얻습니다. 이 과정은 최적의 방식이며, 자동화되어 있고 안전합니다.

콘솔에 AWS 액세스 키를 제공하는 경우 정기적으로 콘솔에서 키를 업데이트하여 키를 순환해야 합니다. 이는 완전히 수동적인 과정입니다.

Cloud Volumes ONTAP 시스템에 대한 AWS Marketplace 구독을 변경할 수 있나요?

네, 가능합니다. 자격 증명 세트와 연결된 AWS Marketplace 구독을 변경하면 모든 기존 및 새 Cloud Volumes ONTAP 시스템에 새 구독 요금이 청구됩니다.

"AWS 구독을 연결하는 방법 알아보기" .

각기 다른 마켓플레이스 구독을 가진 여러 AWS 자격 증명을 추가할 수 있나요?

동일한 AWS 계정에 속한 모든 AWS 자격 증명은 동일한 AWS Marketplace 구독과 연결됩니다.

서로 다른 AWS 계정에 속하는 AWS 자격 증명이 여러 개 있는 경우 해당 자격 증명을 동일한 AWS Marketplace 구독이나 다른 구독과 연결할 수 있습니다.

기존 Cloud Volumes ONTAP 시스템을 다른 AWS 계정으로 옮길 수 있나요?

아니요, Cloud Volumes ONTAP 시스템과 연결된 AWS 리소스를 다른 AWS 계정으로 이동하는 것은 불가능합니다.

마켓플레이스 배포와 온프레미스 배포에서 자격 증명은 어떻게 작동합니까?

위 섹션에서는 콘솔에서 콘솔 에이전트를 배포하는 데 권장되는 방법을 설명합니다. AWS Marketplace에서 AWS에 에이전트를 배포할 수도 있고, 자신의 Linux 호스트나 VCenter에 콘솔 에이전트 소프트웨어를 수동으로 설치할 수도 있습니다.

마켓플레이스를 사용하는 경우에도 동일한 방식으로 권한이 제공됩니다. IAM 역할을 수동으로 생성하고 설정한 다음, 추가 계정에 대한 권한을 제공하기만 하면 됩니다.

온프레미스 배포의 경우 콘솔에 대한 IAM 역할을 설정할 수 없지만 AWS 액세스 키를 사용하여 권한을 제공할 수 있습니다.

권한을 설정하는 방법을 알아보려면 다음 페이지를 참조하세요.

- 표준 모드
  - "AWS Marketplace 배포에 대한 권한 설정"
  - "온프레미스 배포에 대한 권한 설정"
- 제한 모드
  - "제한 모드에 대한 권한 설정"

NetApp Console 대한 **AWS** 자격 증명 및 마켓플레이스 구독 관리

NetApp Console 에서 AWS 계정의 클라우드 리소스를 배포하고 관리할 수 있도록 AWS 자격 증명을 추가하고 관리합니다. 여러 AWS Marketplace 구독을 관리하는 경우 자격 증명 페이지에서 각 구독에 다른 AWS 자격 증명을 할당할 수 있습니다.

개요

AWS 자격 증명을 기존 콘솔 에이전트에 추가하거나 콘솔에 직접 추가할 수 있습니다.

- 기존 에이전트에 추가 AWS 자격 증명 추가

  AWS 자격 증명을 콘솔 에이전트에 추가하여 클라우드 리소스를 관리합니다. 콘솔 에이전트에 AWS 자격 증명을 추가하는 방법을 알아보세요. .

- 콘솔 에이전트를 생성하기 위해 콘솔에 AWS 자격 증명을 추가합니다.

  콘솔에 새로운 AWS 자격 증명을 추가하면 콘솔 에이전트를 만드는 데 필요한 권한이 제공됩니다. NetApp Console 에 AWS 자격 증명을 추가하는 방법을 알아보세요. .

- FSx for ONTAP 콘솔에 AWS 자격 증명 추가

  FSx for ONTAP 생성하고 관리하려면 콘솔에 새로운 AWS 자격 증명을 추가하세요. "FSx for ONTAP 에 대한 권한을 설정하는 방법을 알아보세요"

자격 증명을 회전하는 방법

NetApp Console 사용하면 에이전트 인스턴스와 연결된 IAM 역할, 신뢰할 수 있는 계정에서 IAM 역할을 맡는 방법, AWS 액세스 키를 제공하는 방법 등 여러 가지 방법으로 AWS 자격 증명을 제공할 수 있습니다. "AWS 자격 증명 및 권한에 대해 자세히 알아보세요" .

처음 두 가지 옵션을 사용하면 콘솔은 AWS 보안 토큰 서비스를 사용하여 지속적으로 순환되는 임시 자격 증명을 얻습니다. 이 프로세스는 자동화되어 있고 안전하므로 가장 좋은 방법입니다.

콘솔에서 AWS 액세스 키를 업데이트하여 수동으로 회전합니다.

콘솔 에이전트에 추가 자격 증명 추가

퍼블릭 클라우드 환경 내에서 리소스와 프로세스를 관리하는 데 필요한 권한을 갖도록 콘솔 에이전트에 추가 AWS 자격 증명을 추가합니다. 다른 계정의 IAM 역할에 대한 ARN을 제공하거나 AWS 액세스 키를 제공할 수 있습니다.

"NetApp Console AWS 자격 증명 및 권한을 사용하는 방법을 알아보세요.".

권한 부여

콘솔 에이전트에 AWS 자격 증명을 추가하기 전에 권한을 부여하세요. 권한을 통해 콘솔 에이전트는 해당 AWS 계정 내의 리소스와 프로세스를 관리할 수 있습니다. 신뢰할 수 있는 계정이나 AWS 키의 역할 ARN을 사용하여 권한을 제공할 수 있습니다.

콘솔에서 콘솔 에이전트를 배포한 경우 콘솔 에이전트를 배포한 계정에 대한 AWS 자격 증명이 자동으로 추가되었습니다. 이를 통해 리소스 관리에 필요한 권한이 있는지 확인할 수 있습니다.

선택사항

- 다른 계정에서 IAM 역할을 맡아 권한 부여
- AWS 키를 제공하여 권한 부여

다른 계정에서 **IAM** 역할을 맡아 권한 부여

IAM 역할을 사용하여 콘솔 에이전트를 배포한 소스 AWS 계정과 다른 AWS 계정 간에 신뢰 관계를 설정할 수 있습니다. 그런 다음 신뢰할 수 있는 계정의 IAM 역할에 대한 ARN을 콘솔에 제공합니다.

온프레미스에 콘솔 에이전트가 설치된 경우 이 인증 방법을 사용할 수 없습니다. AWS 키를 사용해야 합니다.

단계

1. 콘솔 에이전트에 권한을 부여하려는 대상 계정의 IAM 콘솔로 이동합니다.
2. 액세스 관리에서 *역할 > 역할 만들기*를 선택하고 단계에 따라 역할을 만듭니다.

   다음 사항을 꼭 확인하세요.

   - *신뢰할 수 있는 엔터티 유형*에서 *AWS 계정*을 선택합니다.
   - *다른 AWS 계정*을 선택하고 콘솔 에이전트 인스턴스가 있는 계정의 ID를 입력합니다.
   - 내용을 복사하여 붙여넣어 필요한 정책을 만듭니다."콘솔 에이전트에 대한 IAM 정책" .
3. 나중에 콘솔에 붙여넣을 수 있도록 IAM 역할의 역할 ARN을 복사합니다.

결과

해당 계정에는 필요한 권한이 있습니다. 이제 콘솔 에이전트에 자격 증명을 추가할 수 있습니다. .

AWS 키를 제공하여 권한 부여

IAM 사용자에 대한 AWS 키를 콘솔에 제공하려면 해당 사용자에게 필요한 권한을 부여해야 합니다. 콘솔 IAM 정책은 콘솔에서 사용할 수 있는 AWS 작업과 리소스를 정의합니다.

온프레미스에 콘솔 에이전트가 설치된 경우 이 인증 방법을 사용해야 합니다. IAM 역할을 사용할 수 없습니다.

단계

1. IAM 콘솔에서 내용을 복사하여 붙여넣어 정책을 만듭니다."콘솔 에이전트에 대한 IAM 정책" .

   "AWS 설명서: IAM 정책 생성"

2. 정책을 IAM 역할이나 IAM 사용자에게 연결합니다.
   - "AWS 설명서: IAM 역할 생성"
   - "AWS 설명서: IAM 정책 추가 및 제거"

기존 에이전트에 자격 증명 추가

AWS 계정에 필요한 권한을 제공한 후 해당 계정의 자격 증명을 기존 에이전트에 추가할 수 있습니다. 이를 통해 동일한 에이전트를 사용하여 해당 계정에서 Cloud Volumes ONTAP 시스템을 시작할 수 있습니다.

클라우드 제공업체의 새로운 자격 증명이 사용 가능해지는 데 몇 분이 걸릴 수 있습니다.

단계

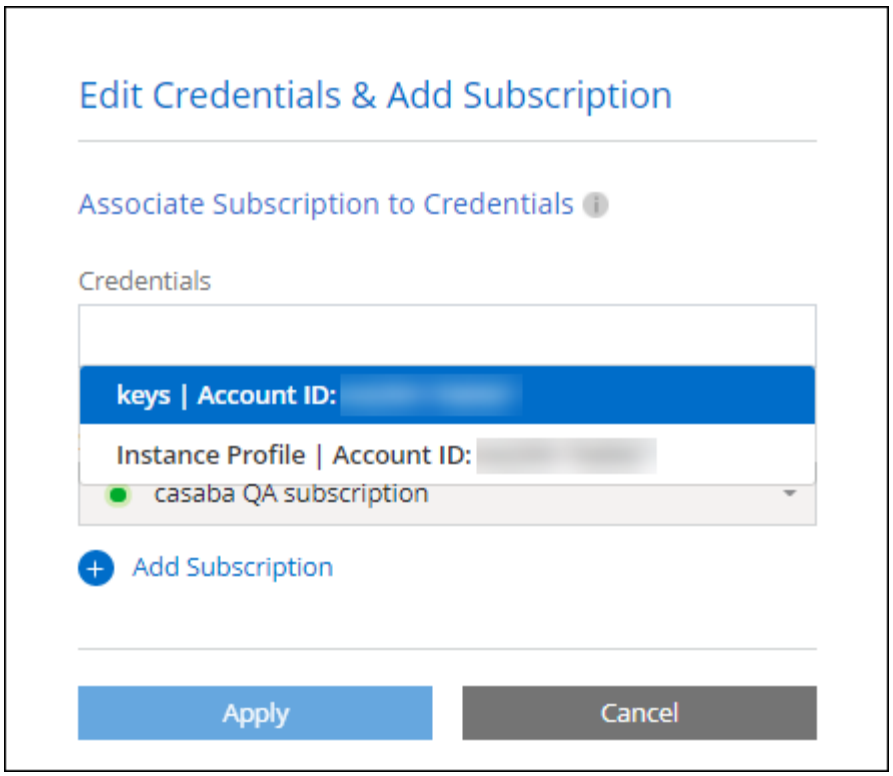
1. 자격 증명을 추가할 콘솔 에이전트를 선택하려면 상단 탐색 모음을 사용하세요.
2. 왼쪽 탐색 모음에서 *관리 > 자격 증명*을 선택합니다.
3. 조직 자격 증명 페이지에서 *자격 증명 추가*를 선택하고 마법사의 단계를 따릅니다.
   a. 자격 증명 위치: *Amazon Web Services > 에이전트*를 선택합니다.
   b. 자격 증명 정의: 신뢰할 수 있는 IAM 역할의 ARN(Amazon 리소스 이름)을 제공하거나 AWS 액세스 키와 비밀 키를 입력합니다.
   c. 마켓플레이스 구독: 지금 구독하거나 기존 구독을 선택하여 마켓플레이스 구독을 이러한 자격 증명과 연결합니다.

      시간당 요금(PAYGO) 또는 연간 계약으로 서비스 비용을 지불하려면 AWS 자격 증명을 AWS Marketplace 구독과 연결해야 합니다.

   d. 검토: 새로운 자격 증명에 대한 세부 정보를 확인하고 *추가*를 선택합니다.

결과

이제 콘솔에 구독을 추가할 때 세부 정보 및 자격 증명 페이지에서 다른 자격 증명 세트로 전환할 수 있습니다.



콘솔 에이전트를 생성하기 위해 콘솔에 자격 증명을 추가합니다.

콘솔 에이전트를 만드는 데 필요한 권한을 부여하는 IAM 역할의 ARN을 제공하여 AWS 자격 증명을 추가합니다. 새로운 에이전트를 생성할 때 이러한 자격 증명을 선택할 수 있습니다.

IAM 역할 설정

NetApp Console SaaS(Software as a Service) 계층이 역할을 수행할 수 있도록 IAM 역할을 설정합니다.

단계

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

   다음 사항을 꼭 확인하세요.

   - *신뢰할 수 있는 엔터티 유형*에서 *AWS 계정*을 선택합니다.
   - *다른 AWS 계정*을 선택하고 NetApp Console SaaS의 ID를 입력하세요: 952013314444
   - 특히 Amazon FSx for NetApp ONTAP 의 경우 "AWS": "arn:aws:iam::952013314444:root"를 포함하도록 신뢰 관계 정책을 편집합니다.

     예를 들어, 정책은 다음과 같아야 합니다.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::952013314444:root",
        "Service": "ec2.amazonaws.com"
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

+
참조하다 "AWS Identity and Access Management(IAM) 문서" IAM에서 계정 간 리소스 액세스에 대한 자세한 내용을 확인하세요.

- 콘솔 에이전트를 만드는 데 필요한 권한을 포함하는 정책을 만듭니다.
  - "FSx for ONTAP 에 필요한 권한 보기"
  - "에이전트 배포 정책 보기"

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

결과

이제 IAM 역할에 필요한 권한이 부여되었습니다. 이제 콘솔에 추가할 수 있습니다..

자격 증명을 추가하세요

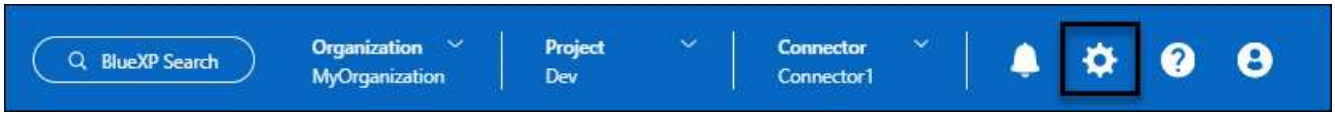
IAM 역할에 필요한 권한을 제공한 후 콘솔에 역할 ARN을 추가합니다.

시작하기 전에

IAM 역할을 방금 생성한 경우 사용할 수 있을 때까지 몇 분이 걸릴 수 있습니다. 콘솔에 자격 증명을 추가하기 전에 몇 분 정도 기다리세요.

단계

1. *관리 > 자격 증명*을 선택합니다.



2. 조직 자격 증명 페이지에서 *자격 증명 추가*를 선택하고 마법사의 단계를 따릅니다.
   a. 자격 증명 위치: *Amazon Web Services > 콘솔*을 선택합니다.
   b. 자격 증명 정의: IAM 역할의 ARN(Amazon 리소스 이름)을 제공합니다.
   c. 검토: 새로운 자격 증명에 대한 세부 정보를 확인하고 *추가*를 선택합니다.

Amazon FSx for ONTAP 콘솔에 자격 증명 추가

자세한 내용은 다음을 참조하세요. "Amazon FSx for ONTAP 에 대한 콘솔 설명서"

AWS 구독 구성

AWS 자격 증명을 추가한 후에는 해당 자격 증명을 사용하여 AWS Marketplace 구독을 구성할 수 있습니다. 구독을 통해 NetApp 데이터 서비스와 Cloud Volumes ONTAP 에 대한 비용을 시간당 요금(PAYGO) 또는 연간 계약으로 지불할 수 있습니다.

자격 증명을 추가한 후 AWS Marketplace 구독을 구성할 수 있는 시나리오는 두 가지가 있습니다.

- 처음 자격 증명을 추가할 때 구독을 구성하지 않았습니다.
- AWS 자격 증명에 구성된 AWS Marketplace 구독을 변경하려고 합니다.

  현재 마켓플레이스 구독을 새 구독으로 교체하면 기존 Cloud Volumes ONTAP 시스템과 모든 새 시스템의 마켓플레이스 구독이 변경됩니다.

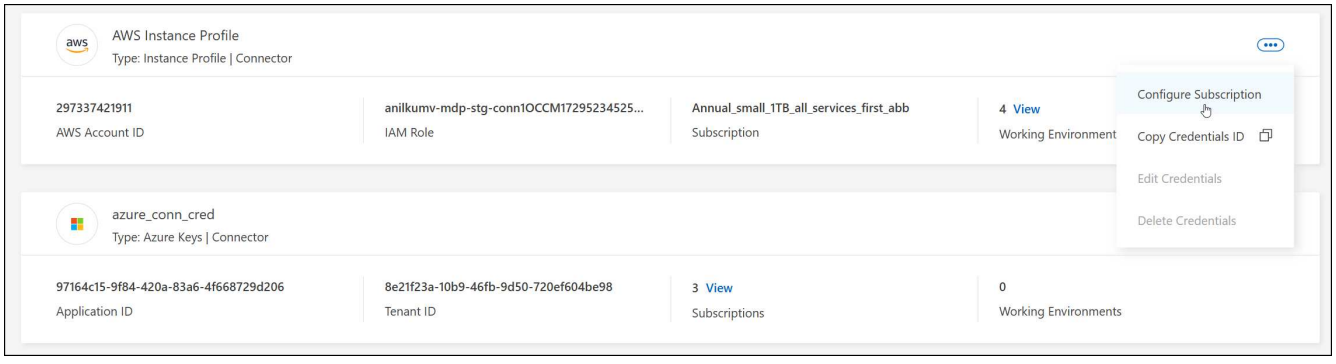
시작하기 전에

구독을 구성하려면 먼저 콘솔 에이전트를 만들어야 합니다. "콘솔 에이전트를 만드는 방법을 알아보세요" .

단계

1. *관리 > 자격 증명*을 선택합니다.
2. *조직 자격 증명*을 선택하세요.
3. 콘솔 에이전트와 연결된 자격 증명 세트에 대한 작업 메뉴를 선택한 다음 *구독 구성*을 선택합니다.

   콘솔 에이전트와 연결된 자격 증명을 선택해야 합니다. NetApp Console 과 연결된 자격 증명에는 마켓플레이스 구독을 연결할 수 없습니다.



4. 자격 증명을 기존 구독과 연결하려면 아래쪽 목록에서 구독을 선택하고 *구성*을 선택합니다.
5. 자격 증명을 새 구독과 연결하려면 *구독 추가 > 계속*을 선택하고 AWS Marketplace의 단계를 따르세요.

   a. *구매 옵션 보기*를 선택하세요.

   b. *구독*을 선택하세요.

   c. *계정 설정*을 선택하세요.

      NetApp Console 로 리디렉션됩니다.

d. 구독 할당 페이지에서:

- 이 구독을 연결할 콘솔 조직이나 계정을 선택하세요.
- 기존 구독 교체 필드에서 하나의 조직 또는 계정에 대한 기존 구독을 이 새로운 구독으로 자동으로 교체할지 여부를 선택합니다.

  콘솔은 조직 또는 계정의 모든 자격 증명에 대한 기존 구독을 이 새로운 구독으로 대체합니다. 자격 증명 세트가 구독과 연결되지 않은 경우 이 새 구독은 해당 자격 증명과 연결되지 않습니다.

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

- *저장*을 선택하세요.

기존 구독을 조직과 연결

AWS Marketplace에서 구독하는 경우 프로세스의 마지막 단계는 구독을 조직과 연결하는 것입니다. 이 단계를 완료하지 않으면 귀하의 조직에서 구독을 사용할 수 없습니다.

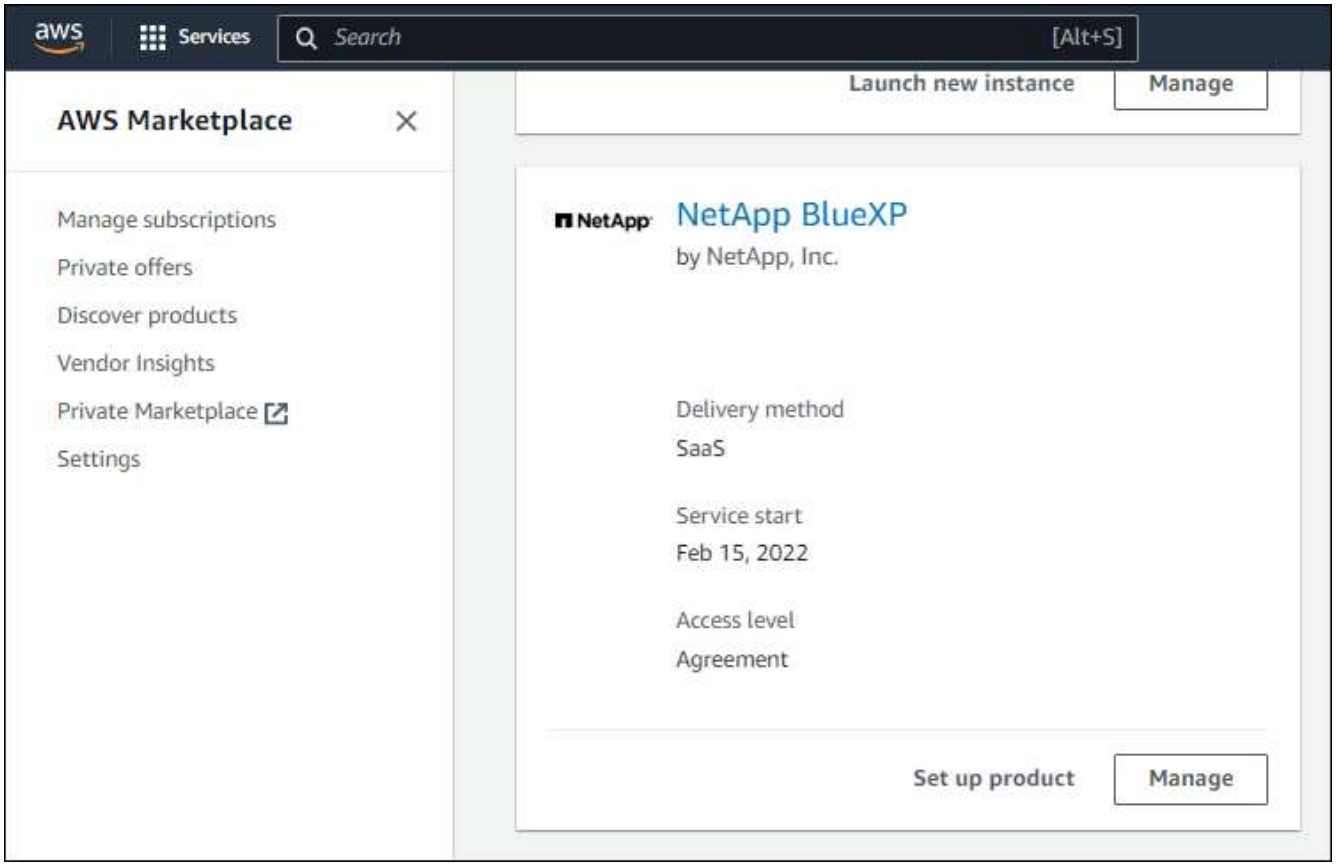
- "콘솔 배포 모드에 대해 알아보세요"
- "콘솔 ID 및 액세스 관리에 대해 알아보세요"

AWS Marketplace에서 NetApp Intelligent Services 구독했지만 구독을 계정과 연결하는 단계를 놓친 경우 아래 단계를 따르세요.

단계

1. 구독을 콘솔 조직과 연결하지 않았는지 확인하세요.
   a. 탐색 메뉴에서 *관리 > Licenses and subscriptions*을 선택합니다.
   b. *구독*을 선택하세요.
   c. 귀하의 구독이 나타나지 않는지 확인하세요.

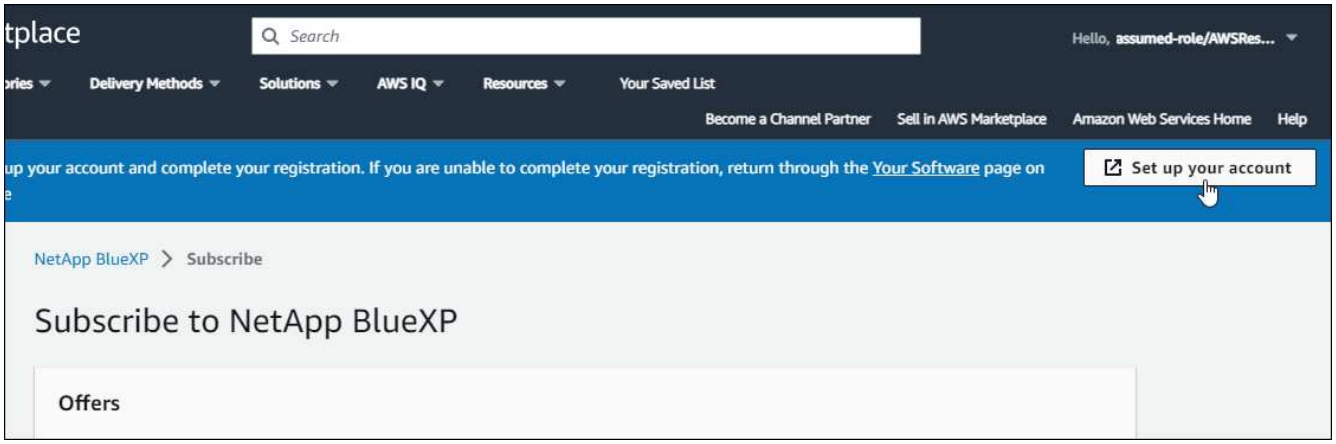
      현재 보고 있는 조직이나 계정과 연결된 구독만 볼 수 있습니다. 구독이 보이지 않으면 다음 단계를 진행하세요.
2. AWS 콘솔에 로그인하고 *AWS Marketplace 구독*으로 이동합니다.
3. 구독을 찾으세요.



4. *제품 설정*을 선택하세요.

   구독 제안 페이지는 새 브라우저 탭이나 창에 로드되어야 합니다.

5. *계정 설정*을 선택하세요.



   netapp.com의 구독 할당 페이지가 새 브라우저 탭이나 창에 로드되어야 합니다.

   먼저 콘솔에 로그인하라는 메시지가 표시될 수 있습니다.

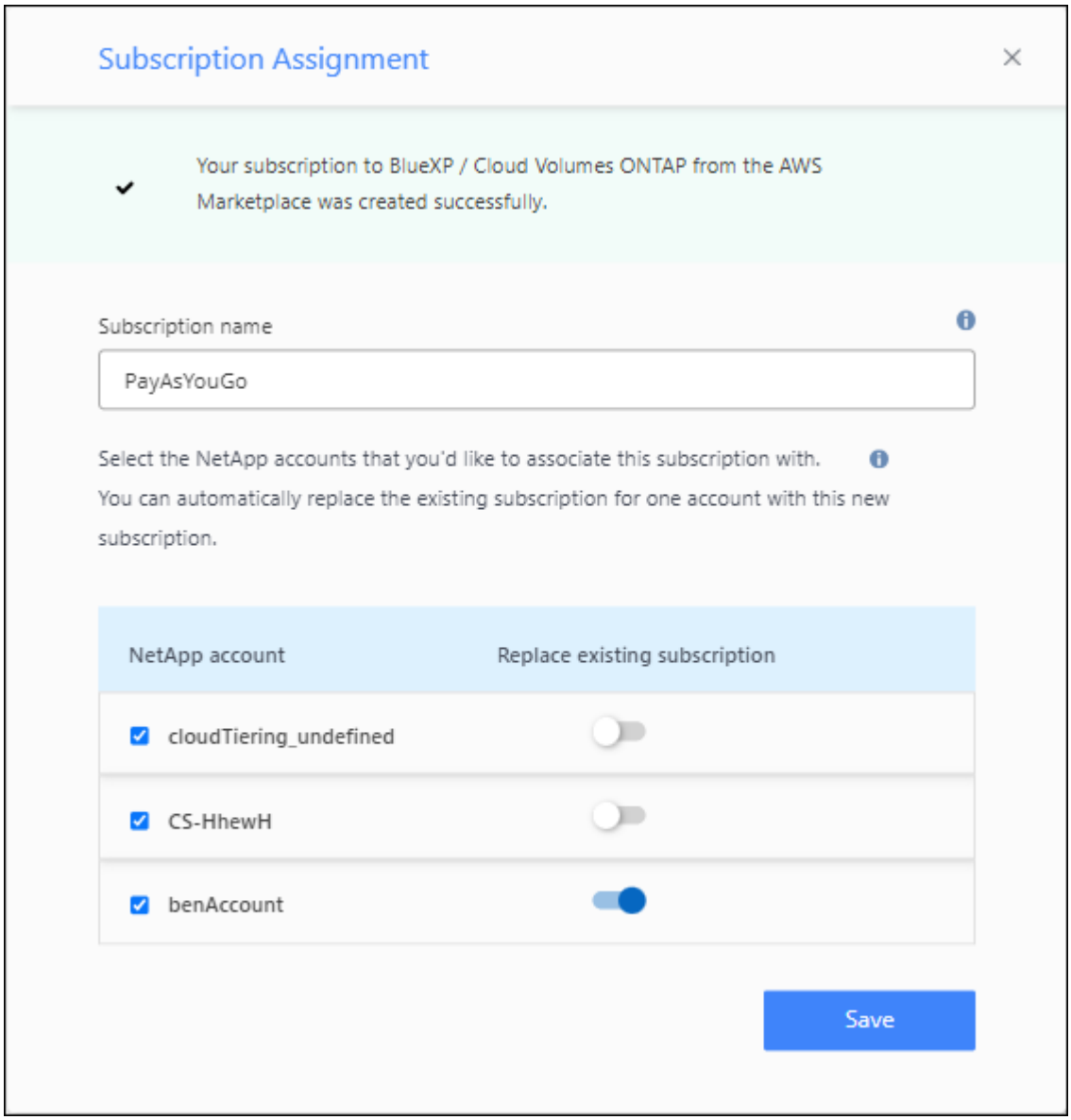
6. 구독 할당 페이지에서:

   ◦ 이 구독을 연결할 콘솔 조직이나 계정을 선택하세요.

◦ 기존 구독 교체 필드에서 하나의 조직 또는 계정에 대한 기존 구독을 이 새로운 구독으로 자동으로 교체할지 여부를 선택합니다.

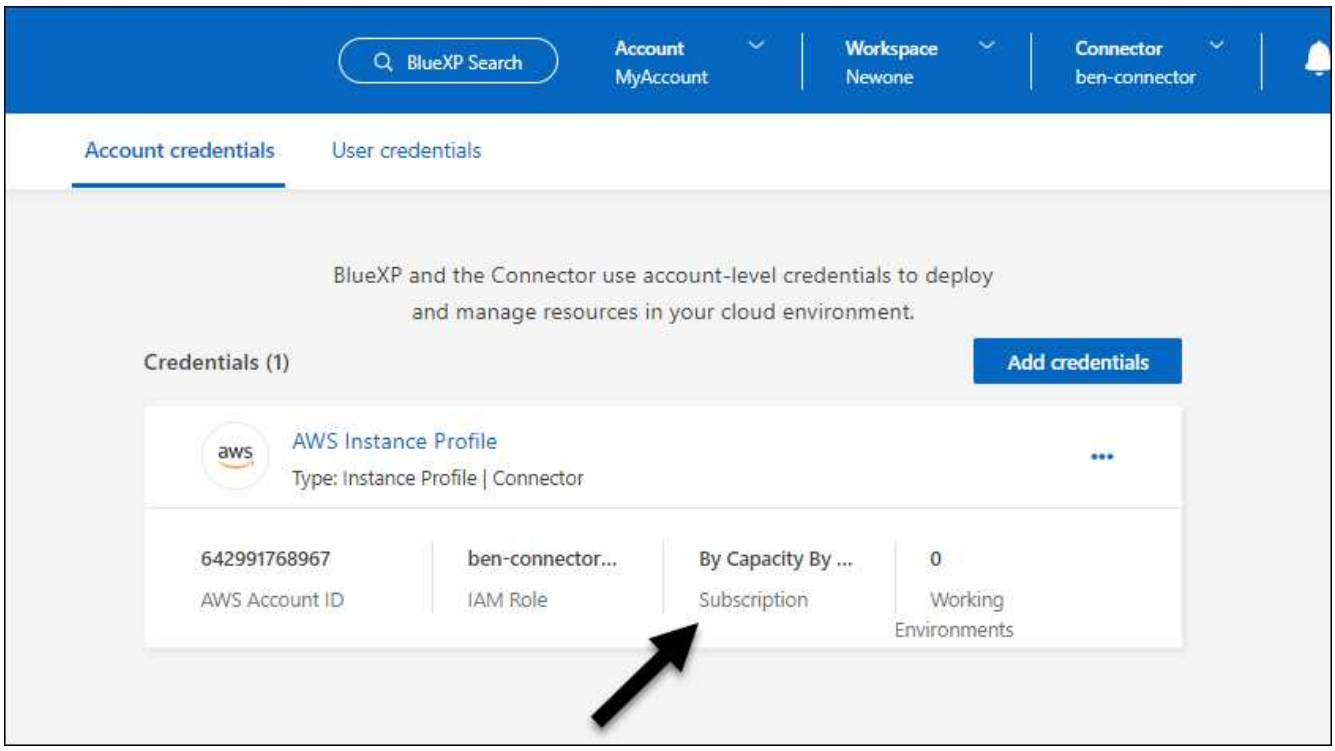
콘솔은 조직 또는 계정의 모든 자격 증명에 대한 기존 구독을 이 새로운 구독으로 대체합니다. 자격 증명 세트가 구독과 연결되지 않은 경우 이 새 구독은 해당 자격 증명과 연결되지 않습니다.

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



7. 구독이 귀하의 조직과 연결되어 있는지 확인하세요.
   a. 탐색 메뉴에서 *관리 > 라이선스 및 구독*을 선택합니다.
   b. *구독*을 선택하세요.
   c. 구독이 표시되는지 확인하세요.
8. 구독이 AWS 자격 증명과 연결되어 있는지 확인하세요.
   a. *관리 > 자격 증명*을 선택합니다.
   b. 조직 자격 증명 페이지에서 구독이 AWS 자격 증명과 연결되어 있는지 확인합니다.

예를 들어 보겠습니다.



자격 증명 편집

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

콘솔 에이전트 인스턴스 또는 Amazon FSx for ONTAP 인스턴스와 연결된 인스턴스 프로필의 자격 증명은 편집할 수 없습니다. FSx for ONTAP 인스턴스의 자격 증명 이름만 바꿀 수 있습니다.

단계

1. *관리 > 자격 증명*을 선택합니다.
2. 조직 자격 증명 페이지에서 자격 증명 세트에 대한 작업 메뉴를 선택한 다음 *자격 증명 편집*을 선택합니다.
3. 필요한 변경 사항을 입력한 후 *적용*을 선택하세요.

자격 증명 삭제

더 이상 자격 증명이 필요하지 않으면 삭제할 수 있습니다. 시스템과 연결되지 않은 자격 증명만 삭제할 수 있습니다.

콘솔 에이전트와 연결된 인스턴스 프로필의 자격 증명은 삭제할 수 없습니다.

단계

1. *관리 > 자격 증명*을 선택합니다.
2. 조직 자격 증명 또는 계정 자격 증명 페이지에서 자격 증명 세트에 대한 작업 메뉴를 선택한 다음 *자격 증명 삭제*를 선택합니다.
3. 삭제를 선택하여 확인하세요.

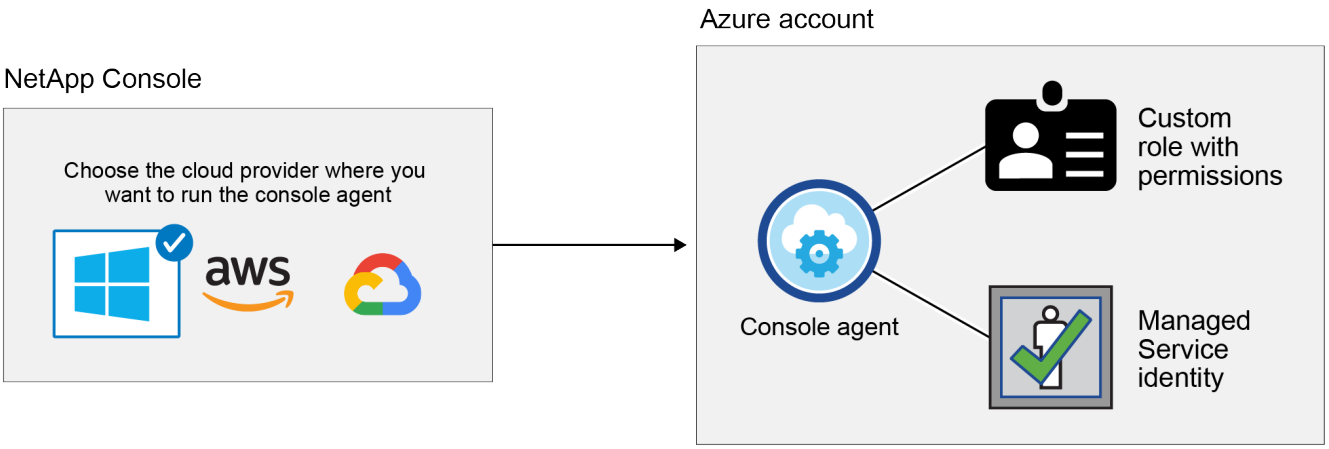
NetApp Console 에서 **Azure** 자격 증명 및 권한에 대해 알아보세요.

NetApp Console Azure 자격 증명을 사용하여 사용자를 대신하여 작업을 수행하는 방법과 해당 자격 증명이 마켓플레이스 구독과 연결되는 방식을 알아보세요. 이러한 세부 정보를 이해하면 하나 이상의 Azure 구독에 대한 자격 증명을 관리할 때 도움이 될 수 있습니다. 예를 들어, 콘솔에 추가 Azure 자격 증명을 추가하는 시기를 알아보고 싶을 수 있습니다.

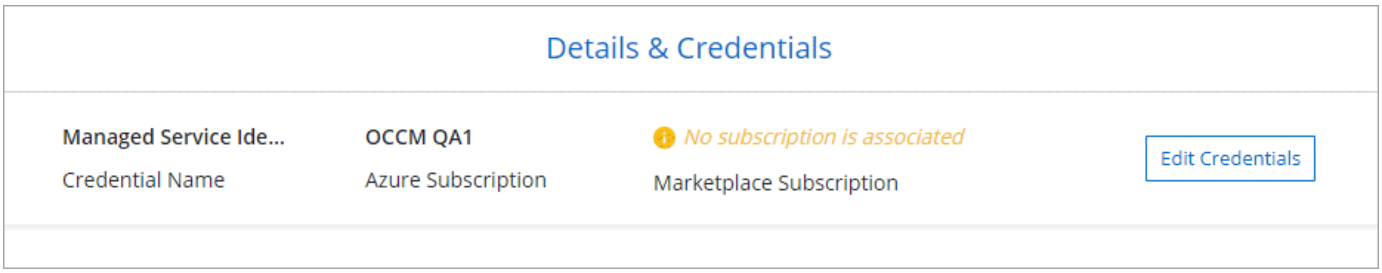
초기 **Azure** 자격 증명

콘솔에서 콘솔 에이전트를 배포하는 경우 콘솔 에이전트 가상 머신을 배포할 수 있는 권한이 있는 Azure 계정이나 서비스 주체를 사용해야 합니다. 필요한 권한은 다음에 나열되어 있습니다."Azure에 대한 에이전트 배포 정책" .

콘솔이 Azure에 콘솔 에이전트 가상 머신을 배포하면 다음을 활성화할 수 있습니다. "시스템 할당 관리 ID" 가상 머신에서 사용자 지정 역할을 만들고 이를 가상 머신에 할당합니다. 이 역할은 Azure 구독 내에서 리소스와 프로세스를 관리하는 데 필요한 권한을 콘솔에 제공합니다. "콘솔이 권한을 사용하는 방식을 검토하세요." .



Cloud Volumes ONTAP 에 대한 새 시스템을 만드는 경우 콘솔은 기본적으로 다음 Azure 자격 증명을 선택합니다.



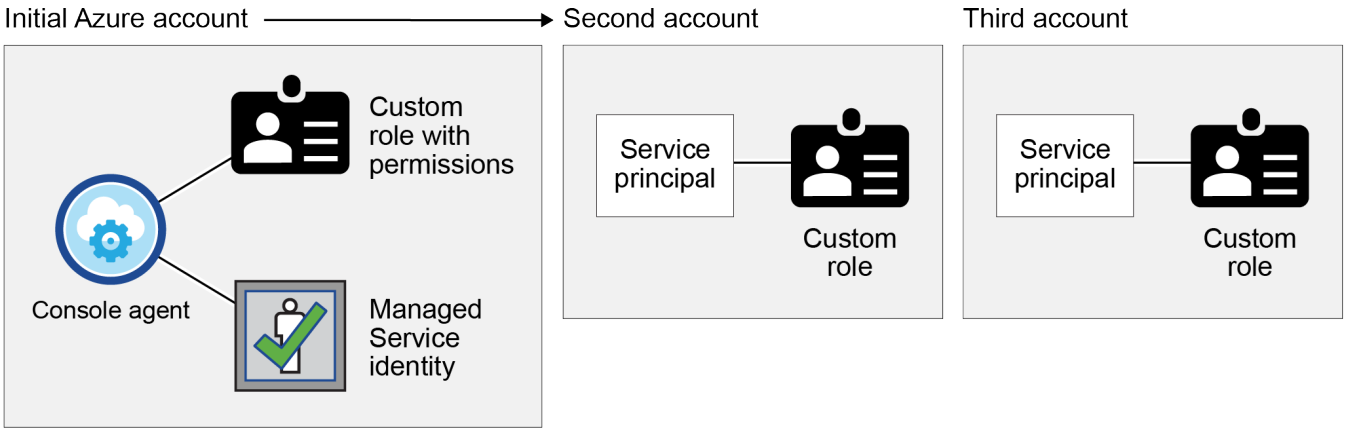
초기 Azure 자격 증명을 사용하여 모든 Cloud Volumes ONTAP 시스템을 배포하거나 추가 자격 증명을 추가할 수 있습니다.

관리 **ID**에 대한 추가 **Azure** 구독

콘솔 에이전트 VM에 할당된 시스템 할당 관리 ID는 콘솔 에이전트를 시작한 구독과 연결됩니다. 다른 Azure 구독을 선택하려면 다음을 수행해야 합니다."관리되는 ID를 해당 구독과 연결합니다." .

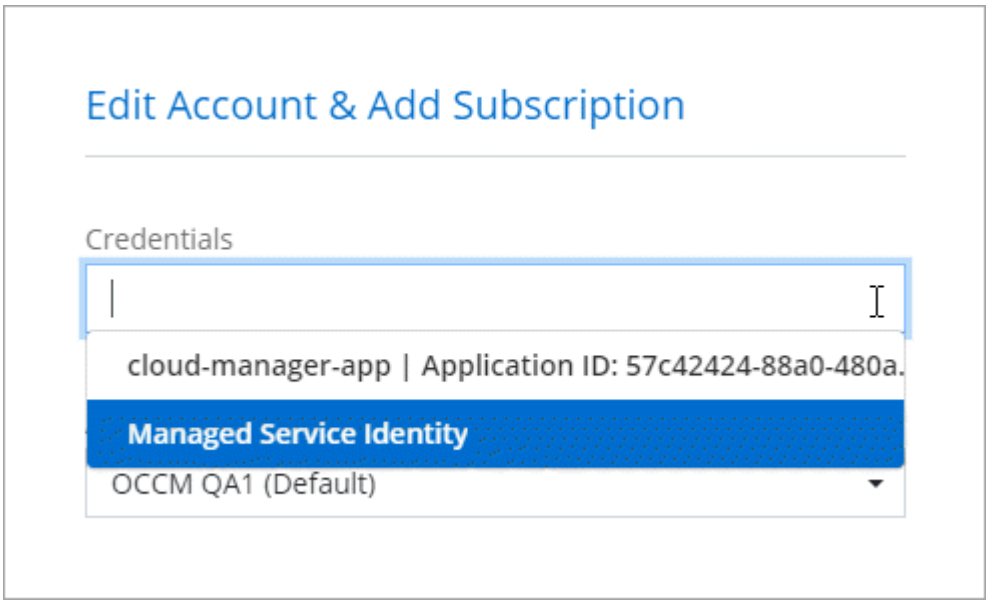
추가 **Azure** 자격 증명

콘솔에서 다른 Azure 자격 증명을 사용하려면 다음을 통해 필요한 권한을 부여해야 합니다."Microsoft Entra ID에서 서비스 주체 만들기 및 설정" 각 Azure 계정에 대해. 다음 이미지는 서비스 주체와 권한을 제공하는 사용자 지정 역할이 설정된 두 개의 추가 계정을 보여줍니다.



그러면 당신은"콘솔에 계정 자격 증명을 추가합니다." AD 서비스 주체에 대한 세부 정보를 제공합니다.

예를 들어, 새로운 Cloud Volumes ONTAP 시스템을 생성할 때 자격 증명 간에 전환할 수 있습니다.



자격 증명 및 마켓플레이스 구독

콘솔 에이전트에 추가하는 자격 증명은 Azure Marketplace 구독과 연결되어야 합니다. 이렇게 하면 시간당 요금(PAYGO)으로 Cloud Volumes ONTAP 에 대한 비용을 지불하거나 NetApp 데이터 서비스 또는 연간 계약을 통해 비용을 지불할 수 있습니다.

"Azure 구독을 연결하는 방법 알아보기" .

Azure 자격 증명 및 Marketplace 구독에 대해 다음 사항을 참고하세요.

- Azure 자격 증명 세트에는 하나의 Azure Marketplace 구독만 연결할 수 있습니다.

- 기존 마켓플레이스 구독을 새 구독으로 교체할 수 있습니다.

자주 묻는 질문

다음 질문은 자격 증명 및 구독과 관련이 있습니다.

Cloud Volumes ONTAP 시스템의 **Azure Marketplace** 구독을 변경할 수 있나요**?**

네, 가능합니다. Azure 자격 증명 세트와 연결된 Azure Marketplace 구독을 변경하면 모든 기존 및 새 Cloud Volumes ONTAP 시스템에 새 구독 요금이 청구됩니다.

"Azure 구독을 연결하는 방법 알아보기" .

각각 다른 **Marketplace** 구독을 사용하여 여러 **Azure** 자격 증명을 추가할 수 있나요**?**

동일한 Azure 구독에 속하는 모든 Azure 자격 증명은 동일한 Azure Marketplace 구독과 연결됩니다.

서로 다른 Azure 구독에 속하는 여러 Azure 자격 증명이 있는 경우 해당 자격 증명을 동일한 Azure Marketplace 구독이나 다른 Marketplace 구독과 연결할 수 있습니다.

기존 **Cloud Volumes ONTAP** 시스템을 다른 **Azure** 구독으로 옮길 수 있나요**?**

아니요, Cloud Volumes ONTAP 시스템과 연결된 Azure 리소스를 다른 Azure 구독으로 이동하는 것은 불가능합니다.

마켓플레이스 배포와 온프레미스 배포에서 자격 증명은 어떻게 작동합니까**?**

위 섹션에서는 콘솔에서 콘솔 에이전트를 배포하는 데 권장되는 방법을 설명합니다. Azure Marketplace에서 Azure에 콘솔 에이전트를 배포할 수도 있고, 자체 Linux 호스트에 콘솔 에이전트 소프트웨어를 설치할 수도 있습니다.

Marketplace를 사용하는 경우 콘솔 에이전트 VM과 시스템에서 할당한 관리 ID에 사용자 지정 역할을 할당하여 권한을 제공하거나 Microsoft Entra 서비스 주체를 사용할 수 있습니다.

온프레미스 배포의 경우 콘솔 에이전트에 대한 관리 ID를 설정할 수 없지만 서비스 주체를 사용하여 권한을 제공할 수 있습니다.

권한을 설정하는 방법을 알아보려면 다음 페이지를 참조하세요.

- 표준 모드
  - "Azure Marketplace 배포에 대한 권한 설정"
  - "온프레미스 배포에 대한 권한 설정"
- 제한 모드
  - "제한 모드에 대한 권한 설정"

NetApp Console 에 대한 **Azure** 자격 증명 및 마켓플레이스 구독 관리

NetApp Console Azure 구독에서 클라우드 리소스를 배포하고 관리하는 데 필요한 권한을 갖도록 Azure 자격 증명을 추가하고 관리합니다. 여러 Azure Marketplace 구독을 관리하는 경우 자격 증명 페이지에서 각 구독에 다른 Azure 자격 증명을 할당할 수 있습니다.

개요

콘솔에서 추가 Azure 구독과 자격 증명을 추가하는 방법에는 두 가지가 있습니다.

1. 추가 Azure 구독을 Azure 관리 ID와 연결합니다.
2. 다양한 Azure 자격 증명을 사용하여 Cloud Volumes ONTAP 배포하려면 서비스 주체를 사용하여 Azure 권한을 부여하고 해당 자격 증명을 콘솔에 추가합니다.

추가 **Azure** 구독을 관리 **ID**와 연결

콘솔을 사용하면 Cloud Volumes ONTAP 을 배포할 Azure 자격 증명과 Azure 구독을 선택할 수 있습니다. 관리 ID 프로필에 대해 다른 Azure 구독을 선택하려면 다음을 수행해야 합니다. "관리되는 ID" 해당 구독을 통해.

이 작업에 관하여

관리되는 ID는"초기 Azure 계정" 콘솔에서 콘솔 에이전트를 배포하는 경우. 콘솔 에이전트를 배포하면 콘솔은 콘솔 에이전트 가상 머신에 콘솔 운영자 역할을 할당합니다.

단계

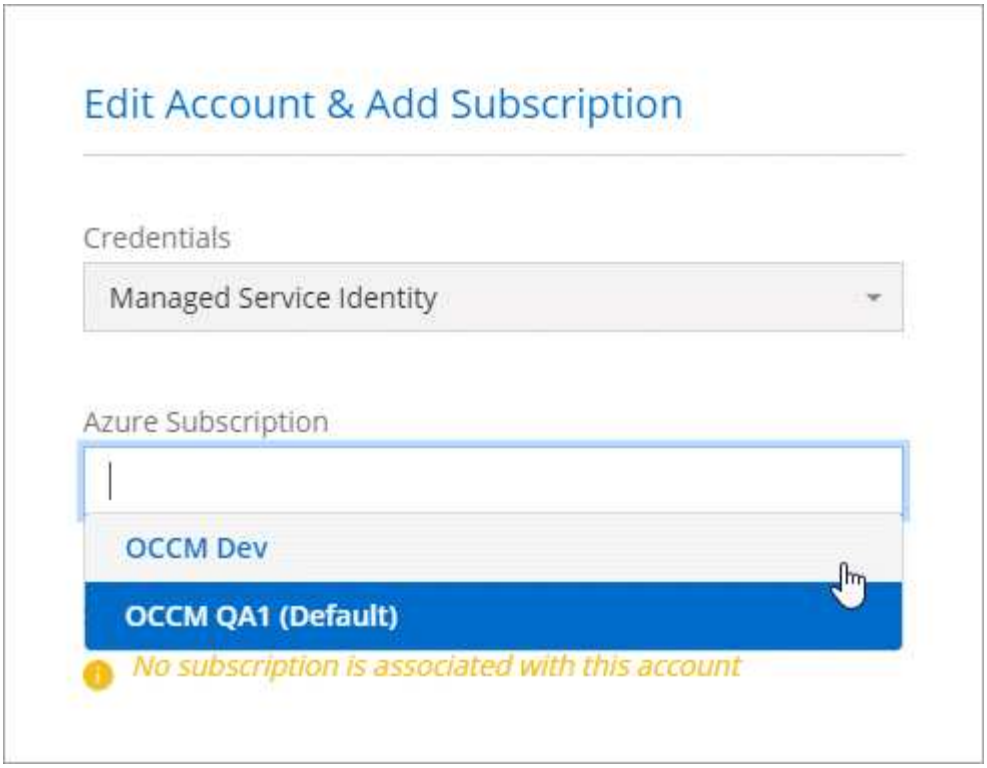
1. Azure Portal에 로그인합니다.
2. 구독 서비스를 열고 Cloud Volumes ONTAP 배포할 구독을 선택합니다.
3. *액세스 제어(IAM)*를 선택합니다.
   a. 추가 > *역할 할당 추가*를 선택한 다음 권한을 추가합니다.
      - 콘솔 운영자 역할을 선택하세요.

        콘솔 운영자는 콘솔 에이전트 정책에 제공되는 기본 이름입니다. 역할에 다른 이름을 선택한 경우 해당 이름을 대신 선택하세요.

      - *가상 머신*에 대한 액세스 권한을 할당합니다.
      - 콘솔 에이전트 가상 머신이 생성된 구독을 선택하세요.
      - 콘솔 에이전트 가상 머신을 선택하세요.
      - *저장*을 선택하세요.
4. 추가 구독에 대해 이 단계를 반복하세요.

결과

새로운 시스템을 만들 때 이제 관리 ID 프로필에 대한 여러 Azure 구독 중에서 선택할 수 있습니다.



NetApp Console 에 추가 **Azure** 자격 증명 추가

콘솔에서 콘솔 에이전트를 배포하면 콘솔은 필요한 권한이 있는 가상 머신에서 시스템이 할당한 관리 ID를 활성화합니다. Cloud Volumes ONTAP 에 대한 새 시스템을 만들 때 콘솔은 기본적으로 이러한 Azure 자격 증명을 선택합니다.

기존 시스템에 콘솔 에이전트 소프트웨어를 수동으로 설치한 경우 초기 자격 증명 세트가 추가되지 않습니다. "Azure 자격 증명 및 권한에 대해 알아보세요" .

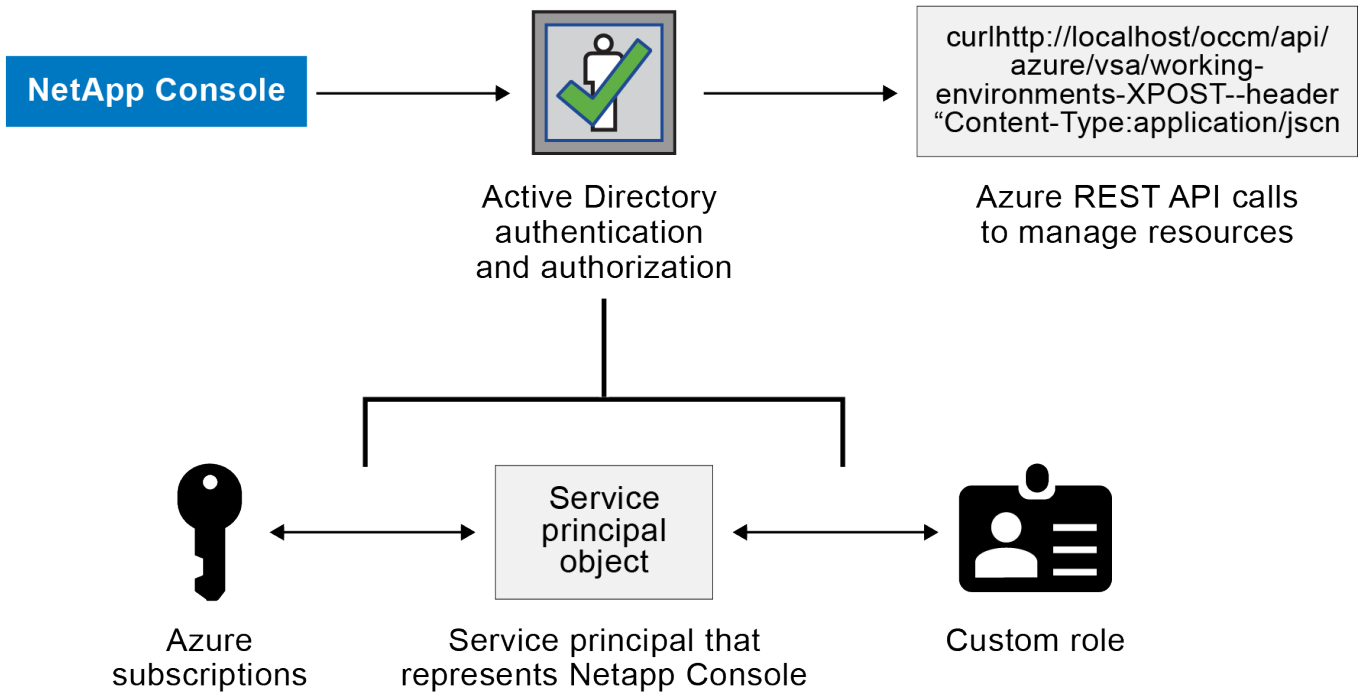
다른 Azure 자격 증명을 사용하여 Cloud Volumes ONTAP 배포하려면 각 Azure 계정에 대해 Microsoft Entra ID에서 서비스 주체를 만들고 설정하여 필요한 권한을 부여해야 합니다. 그런 다음 콘솔에 새 자격 증명을 추가할 수 있습니다.

서비스 주체를 사용하여 **Azure** 권한 부여

Azure에서 작업을 수행하려면 콘솔에 권한이 필요합니다. Microsoft Entra ID에서 서비스 주체를 만들고 설정하고 콘솔에 필요한 Azure 자격 증명을 얻어 Azure 계정에 필요한 권한을 부여할 수 있습니다.

이 작업에 관하여

다음 이미지는 콘솔이 Azure에서 작업을 수행하기 위한 권한을 얻는 방법을 보여줍니다. 하나 이상의 Azure 구독에 연결된 서비스 주체 개체는 Microsoft Entra ID의 콘솔을 나타내며 필요한 권한을 허용하는 사용자 지정 역할에 할당됩니다.



단계

1. Microsoft Entra 애플리케이션 만들기 .
2. 역할에 애플리케이션 할당 .
3. Windows Azure 서비스 관리 API 권한 추가 .
4. 애플리케이션 ID와 디렉토리 ID를 가져옵니다. .
5. 클라이언트 비밀을 생성하세요 .

Microsoft Entra 애플리케이션 만들기

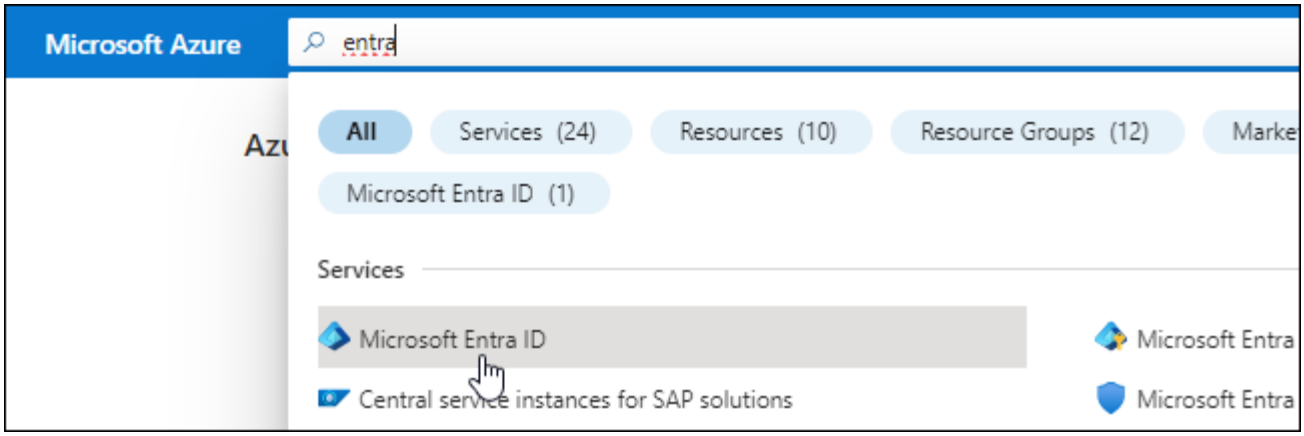
콘솔에서 역할 기반 액세스 제어에 사용할 수 있는 Microsoft Entra 애플리케이션과 서비스 주체를 만듭니다.

단계

1. Azure에서 Active Directory 애플리케이션을 만들고 해당 애플리케이션에 역할을 할당할 수 있는 권한이 있는지 확인하세요.

   자세한 내용은 다음을 참조하세요. "Microsoft Azure 설명서: 필요한 권한"

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



3. 메뉴에서 *앱 등록*을 선택하세요.
4. *신규 등록*을 선택하세요.
5. 신청서에 대한 세부 사항을 지정하세요:
   - 이름: 애플리케이션의 이름을 입력하세요.
   - 계정 유형: 계정 유형을 선택하세요(모든 계정 유형이 NetApp Console 에서 작동합니다).
   - 리디렉션 **URI**: 이 필드는 비워두어도 됩니다.
6. *등록*을 선택하세요.

   AD 애플리케이션과 서비스 주체를 생성했습니다.

역할에 애플리케이션 할당

서비스 주체를 하나 이상의 Azure 구독에 바인딩하고 사용자 지정 "콘솔 운영자" 역할을 할당하여 콘솔이 Azure에서 사용 권한을 갖도록 해야 합니다.

단계

1. 사용자 정의 역할 만들기:

   Azure Portal, Azure PowerShell, Azure CLI 또는 REST API를 사용하여 Azure 사용자 지정 역할을 만들 수 있습니다. 다음 단계에서는 Azure CLI를 사용하여 역할을 만드는 방법을 보여줍니다. 다른 방법을 사용하려면 다음을 참조하세요. "Azure 설명서"

   a. 내용을 복사하세요"콘솔 에이전트에 대한 사용자 정의 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.

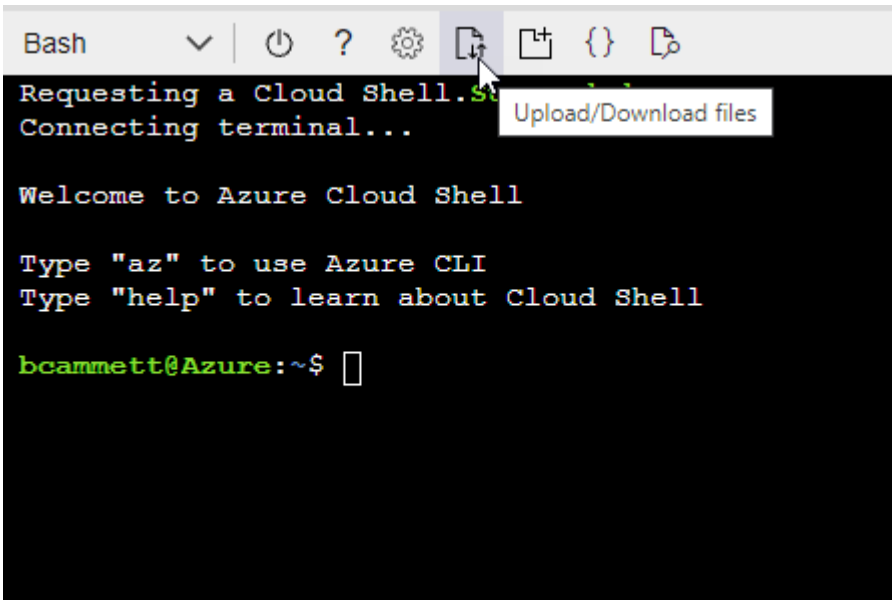
      예

```
"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 만듭니다.

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

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



- Azure CLI를 사용하여 사용자 지정 역할을 만듭니다.

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

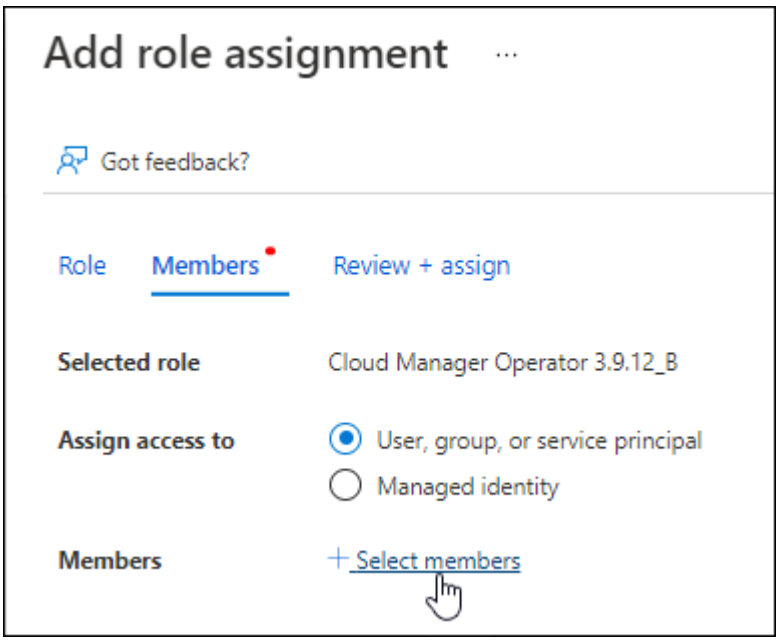
이제 콘솔 에이전트 가상 머신에 할당할 수 있는 콘솔 운영자라는 사용자 지정 역할이 생겼습니다.

2. 역할에 애플리케이션을 할당합니다.

a. Azure Portal에서 구독 서비스를 엽니다.
b. 구독을 선택하세요.
c. *액세스 제어(IAM) > 추가 > 역할 할당 추가*를 선택합니다.
d. 역할 탭에서 콘솔 운영자 역할을 선택하고 *다음*을 선택합니다.
e. 멤버 탭에서 다음 단계를 완료하세요.

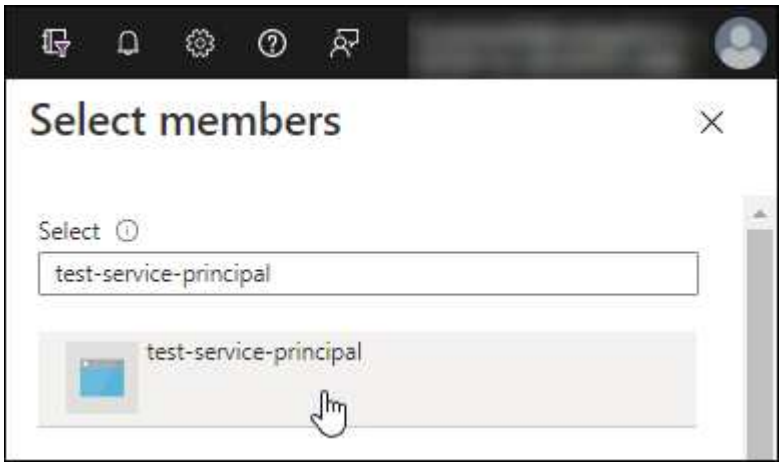
- *사용자, 그룹 또는 서비스 주체*를 선택된 상태로 유지합니다.

- *멤버 선택*을 선택하세요.



- 애플리케이션 이름을 검색하세요.

  예를 들면 다음과 같습니다.



- 애플리케이션을 선택하고 *선택*을 선택하세요.
- *다음*을 선택하세요.

f. *검토 + 할당*을 선택하세요.

이제 서비스 주체는 콘솔 에이전트를 배포하는 데 필요한 Azure 권한을 갖게 되었습니다.

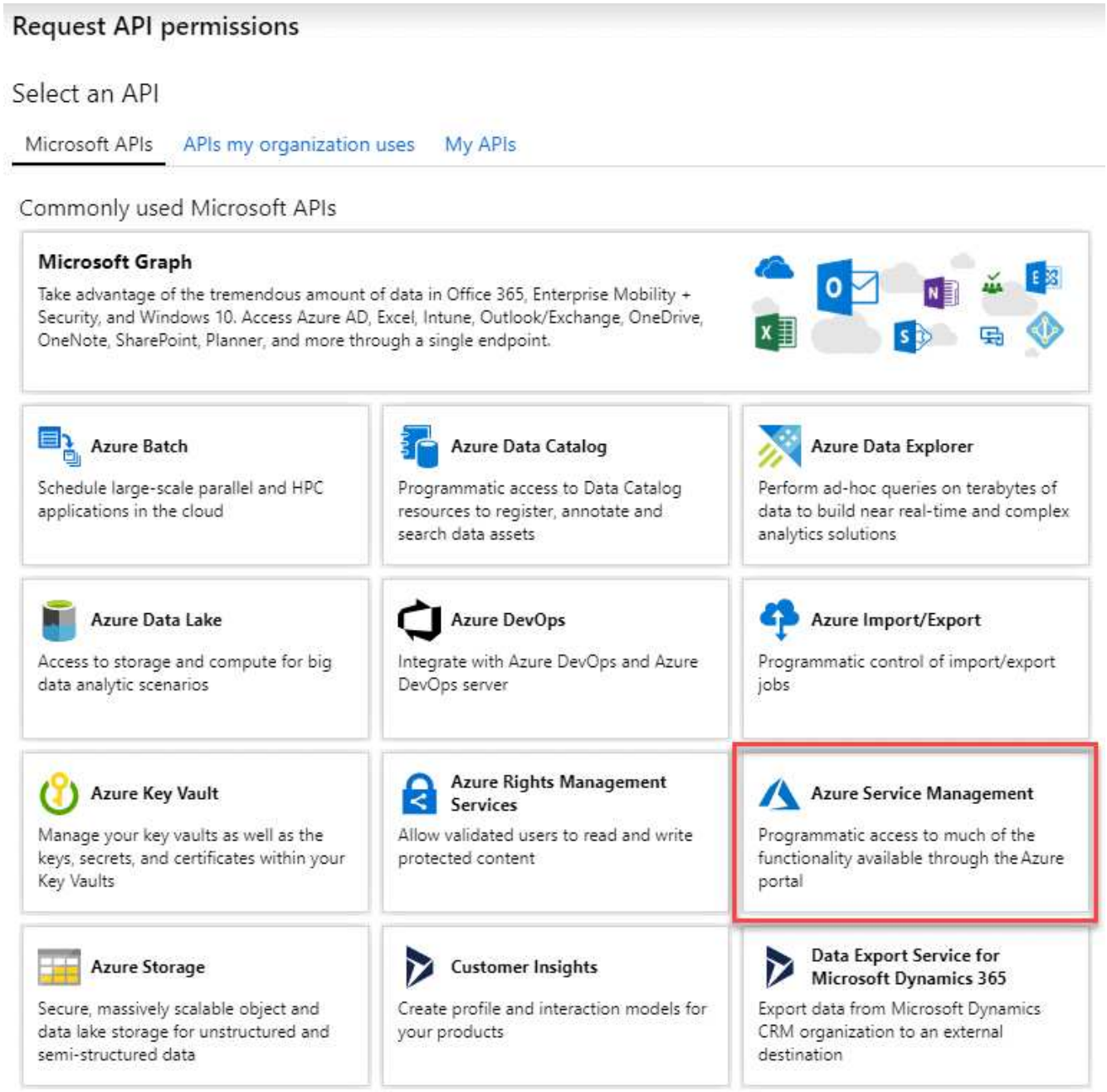
여러 Azure 구독에서 Cloud Volumes ONTAP 배포하려면 각 구독에 서비스 주체를 바인딩해야 합니다. NetApp Console 에서 Cloud Volumes ONTAP 배포할 때 사용할 구독을 선택할 수 있습니다.

Windows Azure 서비스 관리 API 권한 추가

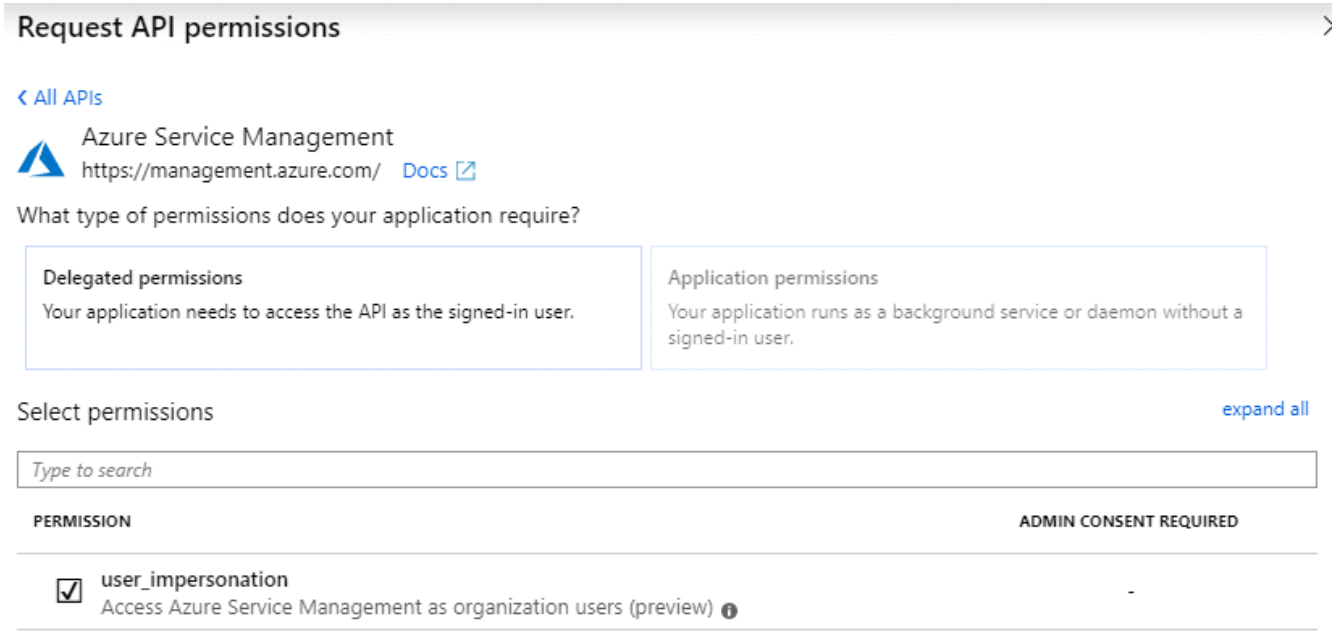
서비스 주체에 "Windows Azure 서비스 관리 API" 권한을 할당해야 합니다.

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.



4. *조직 사용자로 Azure Service Management에 액세스*를 선택한 다음 *권한 추가*를 선택합니다.

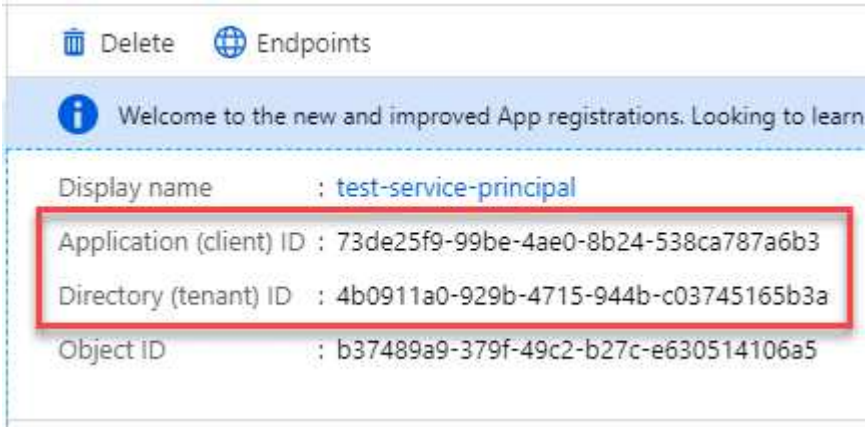


애플리케이션 **ID**와 디렉토리 **ID**를 가져옵니다**.**

콘솔에 Azure 계정을 추가하는 경우 애플리케이션(클라이언트) ID와 애플리케이션의 디렉터리(테넌트) ID를 제공해야 합니다. 콘솔은 ID를 사용하여 프로그래밍 방식으로 로그인합니다.

단계

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



콘솔에 Azure 계정을 추가하는 경우 애플리케이션(클라이언트) ID와 애플리케이션의 디렉터리(테넌트) ID를 제공해야 합니다. 콘솔은 ID를 사용하여 프로그래밍 방식으로 로그인합니다.

클라이언트 비밀을 생성하세요

클라이언트 비밀번호를 생성하고 해당 값을 콘솔에 제공하여 Microsoft Entra ID로 인증합니다.

단계

1. **Microsoft Entra ID** 서비스를 엽니다.

2. *앱 등록*을 선택하고 애플리케이션을 선택하세요.
3. *인증서 및 비밀번호 > 새 클라이언트 비밀번호*를 선택합니다.
4. 비밀에 대한 설명과 기간을 제공하세요.
5. *추가*를 선택하세요.
6. 클라이언트 비밀번호 값을 복사합니다.

결과

이제 서비스 주체가 설정되었고 애플리케이션(클라이언트) ID, 디렉토리(테넌트) ID 및 클라이언트 비밀번호 값을 복사했어야 합니다. Azure 계정을 추가할 때 콘솔에 이 정보를 입력해야 합니다.

콘솔에 자격 증명 추가

Azure 계정에 필요한 권한을 제공한 후 해당 계정의 자격 증명을 콘솔에 추가할 수 있습니다. 이 단계를 완료하면 다양한 Azure 자격 증명을 사용하여 Cloud Volumes ONTAP 시작할 수 있습니다.

시작하기 전에

클라우드 제공업체에서 이러한 자격 증명을 방금 만든 경우, 사용 가능해질 때까지 몇 분이 걸릴 수 있습니다. 콘솔에 자격 증명을 추가하기 전에 몇 분 정도 기다리세요.

시작하기 전에

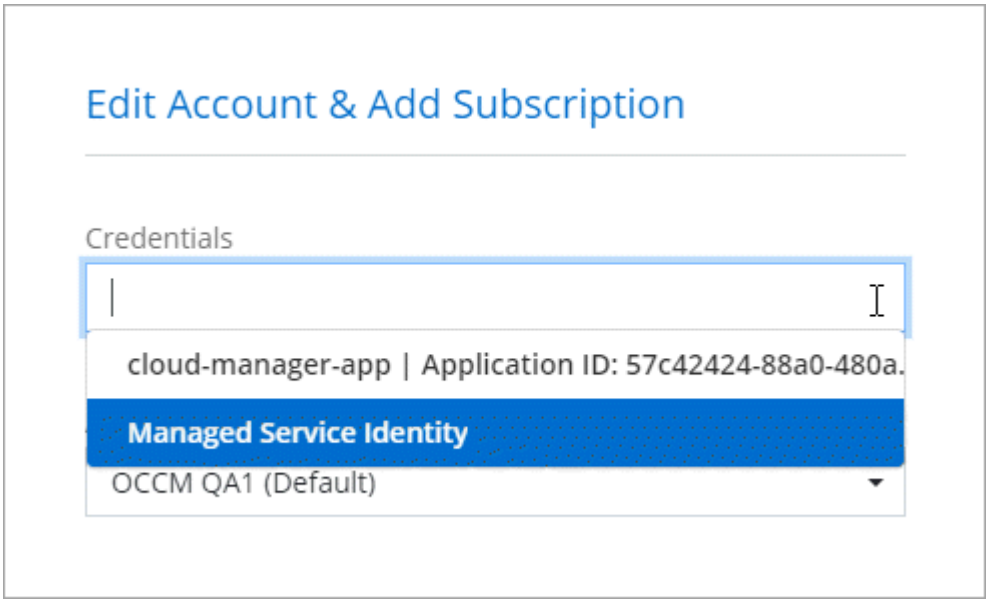
콘솔 설정을 변경하려면 먼저 콘솔 에이전트를 만들어야 합니다. "콘솔 에이전트를 만드는 방법을 알아보세요" .

단계

1. *관리 > 자격 증명*을 선택합니다.
2. *자격 증명 추가*를 선택하고 마법사의 단계를 따르세요.
   a. 자격 증명 위치: *Microsoft Azure > 에이전트*를 선택합니다.
   b. 자격 증명 정의: 필요한 권한을 부여하는 Microsoft Entra 서비스 주체에 대한 정보를 입력합니다.
      - 애플리케이션(클라이언트) ID
      - 디렉토리(테넌트) ID
      - 클라이언트 비밀번호
   c. 마켓플레이스 구독: 지금 구독하거나 기존 구독을 선택하여 마켓플레이스 구독을 이러한 자격 증명과 연결합니다.
   d. 검토: 새로운 자격 증명에 대한 세부 정보를 확인하고 *추가*를 선택합니다.

결과

세부 정보 및 자격 증명 페이지에서 다른 자격 증명 세트로 전환할 수 있습니다. "콘솔에 시스템을 추가할 때"



기존 자격 증명 관리

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

Azure Marketplace 구독을 자격 증명에 연결

콘솔에 Azure 자격 증명을 추가한 후에는 Azure Marketplace 구독을 해당 자격 증명에 연결할 수 있습니다. 구독을 사용하면 사용량에 따라 요금을 지불하는 Cloud Volumes ONTAP 시스템을 만들고 NetApp 데이터 서비스에 액세스할 수 있습니다.

콘솔에 자격 증명을 추가한 후 Azure Marketplace 구독을 연결할 수 있는 시나리오는 두 가지가 있습니다.

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

  현재 마켓플레이스 구독을 교체하면 기존 및 새로운 Cloud Volumes ONTAP 시스템에 대한 구독이 업데이트됩니다.

단계

1. *관리 > 자격 증명*을 선택합니다.
2. *조직 자격 증명*을 선택하세요.
3. 콘솔 에이전트와 연결된 자격 증명 세트에 대한 작업 메뉴를 선택한 다음 *구독 구성*을 선택합니다.

   콘솔 에이전트와 연결된 자격 증명을 선택해야 합니다. NetApp Console 과 연결된 자격 증명에는 마켓플레이스 구독을 연결할 수 없습니다.

4. 자격 증명을 기존 구독과 연결하려면 아래쪽 목록에서 구독을 선택하고 *구성*을 선택합니다.
5. 자격 증명을 새 구독과 연결하려면 *구독 추가 > 계속*을 선택하고 Azure Marketplace의 단계를 따르세요.

   a. 메시지가 표시되면 Azure 계정에 로그인하세요.

b. *구독*을 선택하세요.

c. 양식을 작성하고 *구독*을 선택하세요.

d. 구독 절차가 완료되면 *지금 계정 구성*을 선택하세요.

   NetApp Console 로 리디렉션됩니다.

e. 구독 할당 페이지에서:

   - 이 구독을 연결할 콘솔 조직이나 계정을 선택하세요.
   - 기존 구독 교체 필드에서 하나의 조직 또는 계정에 대한 기존 구독을 이 새로운 구독으로 자동으로 교체할지 여부를 선택합니다.

     콘솔은 조직 또는 계정의 모든 자격 증명에 대한 기존 구독을 이 새로운 구독으로 대체합니다. 자격 증명 세트가 구독과 연결되지 않은 경우 이 새 구독은 해당 자격 증명과 연결되지 않습니다.

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

◦ *저장*을 선택하세요.

자격 증명 편집

콘솔에서 Azure 자격 증명을 편집합니다. 예를 들어, 서비스 주체 애플리케이션에 대한 새 비밀이 생성된 경우 클라이언트 비밀을 업데이트할 수 있습니다.

단계

1. *관리 > 자격 증명*을 선택합니다.
2. *조직 자격 증명*을 선택하세요.
3. 자격 증명 세트에 대한 작업 메뉴를 선택한 다음 *자격 증명 편집*을 선택합니다.
4. 필요한 변경 사항을 입력한 후 *적용*을 선택하세요.

자격 증명 삭제

더 이상 자격 증명이 필요하지 않으면 삭제할 수 있습니다. 시스템과 연결되지 않은 자격 증명만 삭제할 수 있습니다.

단계

1. *관리 > 자격 증명*을 선택합니다.
2. *조직 자격 증명*을 선택하세요.
3. 조직 자격 증명 페이지에서 자격 증명 세트에 대한 작업 메뉴를 선택한 다음 *자격 증명 삭제*를 선택합니다.
4. 삭제를 선택하여 확인하세요.

구글 클라우드

Google Cloud 프로젝트 및 권한에 대해 알아보세요

NetApp Console Google Cloud 자격 증명을 사용하여 사용자를 대신하여 작업을 수행하는 방법과 해당 자격 증명이 마켓플레이스 구독과 연결되는 방식을 알아보세요. 이러한 세부 정보를 이해하면 하나 이상의 Google Cloud 프로젝트에 대한 자격 증명을 관리하는 데 도움이 될 수

있습니다. 예를 들어, 콘솔 에이전트 VM과 연결된 서비스 계정에 대해 알아보고 싶을 수 있습니다.

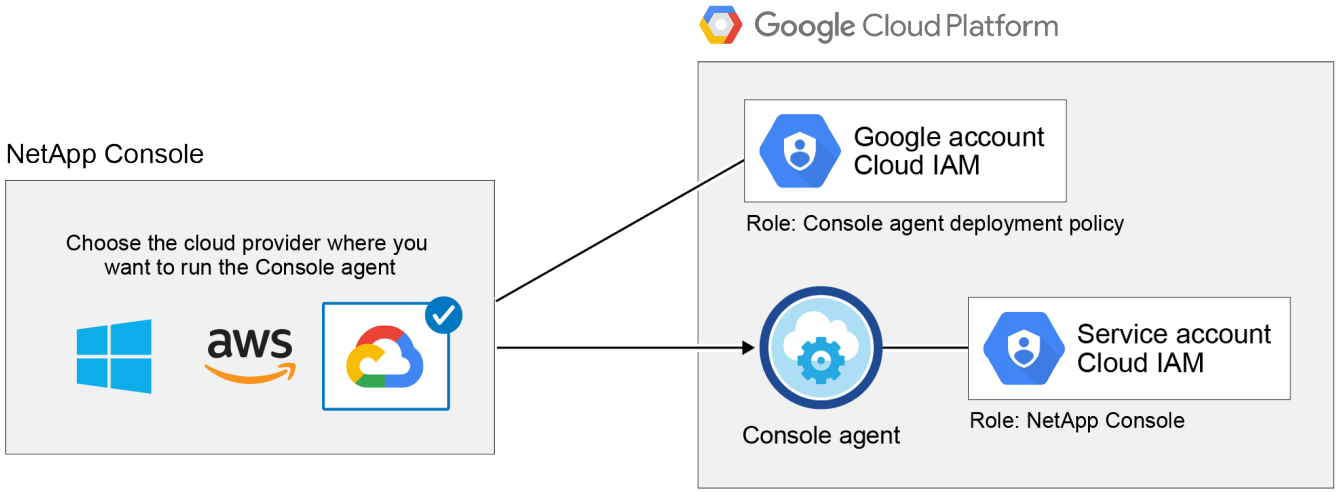
NetApp Console 에 대한 프로젝트 및 권한

Google Cloud 프로젝트의 리소스를 관리하기 위해 콘솔을 사용하려면 먼저 콘솔 에이전트를 배포해야 합니다. 에이전트는 귀하의 사내 또는 다른 클라우드 공급자에서 실행될 수 없습니다.

콘솔에서 직접 콘솔 에이전트를 배포하려면 두 가지 권한 세트가 있어야 합니다.

1. 콘솔에서 콘솔 에이전트를 시작할 수 있는 권한이 있는 Google 계정을 사용하여 콘솔 에이전트를 배포해야 합니다.
2. 콘솔 에이전트를 배포할 때 다음을 선택하라는 메시지가 표시됩니다. "서비스 계정" 에이전트의 경우 콘솔은 서비스 계정으로부터 Cloud Volumes ONTAP 시스템을 생성하고 관리하고, NetApp 백업 및 복구를 사용하여 백업을 관리하는 등의 권한을 얻습니다. 서비스 계정에 사용자 정의 역할을 연결하여 권한을 제공합니다.

다음 이미지는 위의 1번과 2번에 설명된 권한 요구 사항을 보여줍니다.



권한을 설정하는 방법을 알아보려면 다음 페이지를 참조하세요.

- "표준 모드에 대한 Google Cloud 권한 설정"
- "제한 모드에 대한 권한 설정"

자격 증명 및 마켓플레이스 구독

Google Cloud에 콘솔 에이전트를 배포하면 콘솔은 콘솔 에이전트가 있는 프로젝트의 Google Cloud 서비스 계정에 대한 기본 자격 증명 세트를 만듭니다. 이러한 자격 증명은 Cloud Volumes ONTAP 및 NetApp 데이터 서비스 비용을 지불할 수 있도록 Google Cloud Marketplace 구독과 연결되어야 합니다.

"Google Cloud Marketplace 구독을 연결하는 방법 알아보기" .

Google Cloud 자격 증명 및 마켓플레이스 구독에 대해 다음 사항을 참고하세요.

- Google Cloud 자격 증명은 콘솔 에이전트와 한 세트만 연결할 수 있습니다.
- 자격 증명에는 단 하나의 Google Cloud Marketplace 구독만 연결할 수 있습니다.

- 기존 마켓플레이스 구독을 새 구독으로 교체할 수 있습니다.

Cloud Volumes ONTAP 프로젝트

Cloud Volumes ONTAP 콘솔 에이전트와 동일한 프로젝트에 있을 수도 있고, 다른 프로젝트에 있을 수도 있습니다. 다른 프로젝트에 Cloud Volumes ONTAP 배포하려면 먼저 해당 프로젝트에 콘솔 에이전트 서비스 계정과 역할을 추가해야 합니다.

- "서비스 계정을 설정하는 방법을 알아보세요"
- "Google Cloud에 Cloud Volumes ONTAP 배포하고 프로젝트를 선택하는 방법을 알아보세요."

NetApp Console용 Google Cloud 자격 증명 및 구독 관리

마켓플레이스 구독을 연결하고 구독 프로세스 문제를 해결하여 Console 에이전트 VM 인스턴스와 연결된 Google Cloud 자격 증명을 관리할 수 있습니다. 이 두 가지 작업을 통해 마켓플레이스 구독을 사용하여 데이터 서비스 비용을 지불할 수 있습니다.

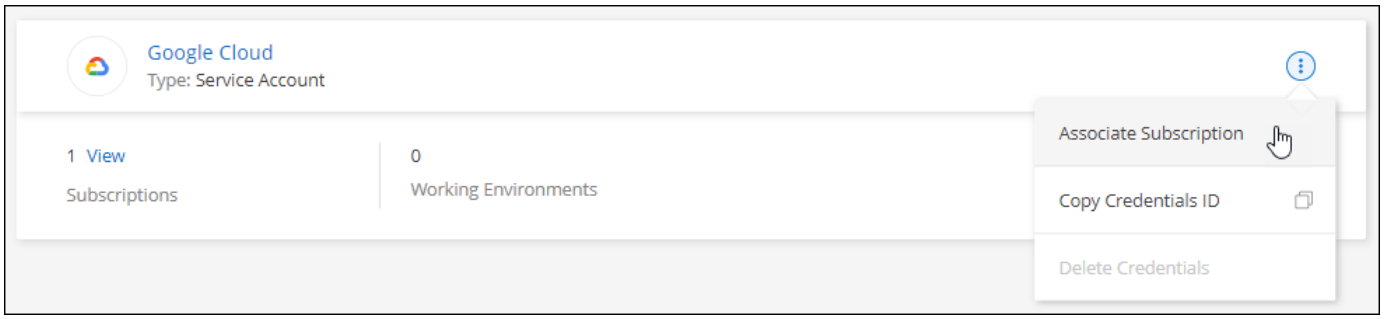
Google Cloud 자격 증명과 마켓플레이스 구독을 연결합니다

Google Cloud에 Console 에이전트를 배포하면 Console에서 Console 에이전트 VM 인스턴스와 연결된 기본 자격 증명 세트를 생성합니다. 언제든지 이러한 자격 증명과 연결된 Google Cloud Marketplace 구독을 변경할 수 있습니다. 이 구독을 통해 종량제 Cloud Volumes ONTAP 시스템을 생성하고 다른 데이터 서비스를 사용할 수 있습니다.

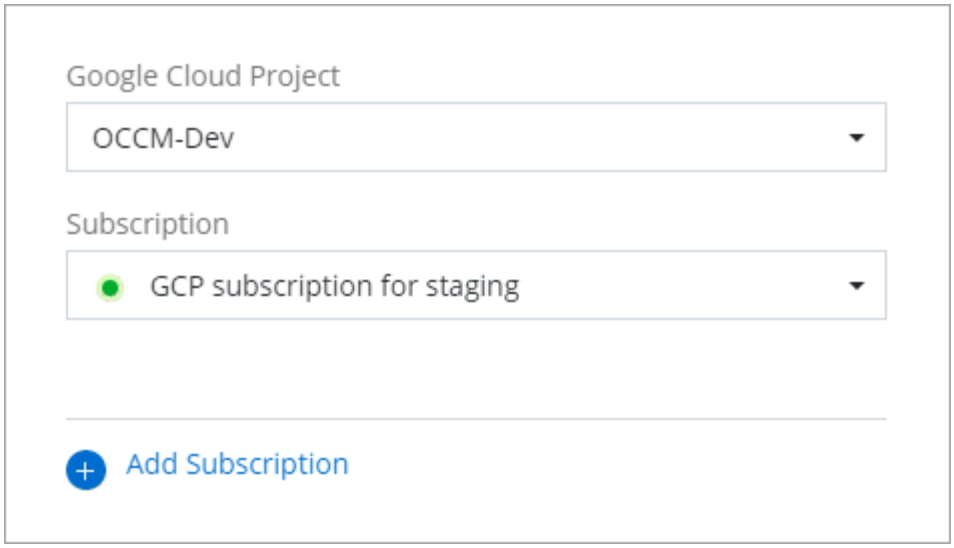
현재 마켓플레이스 구독을 새 구독으로 교체하면 기존 Cloud Volumes ONTAP 시스템과 모든 새 시스템의 마켓플레이스 구독이 변경됩니다.

단계

1. *관리 > 자격 증명*을 선택합니다.
2. *조직 자격 증명*을 선택하세요.
3. 콘솔 에이전트와 연결된 자격 증명 세트에 대한 작업 메뉴를 선택한 다음 *구독 구성*을 선택합니다.



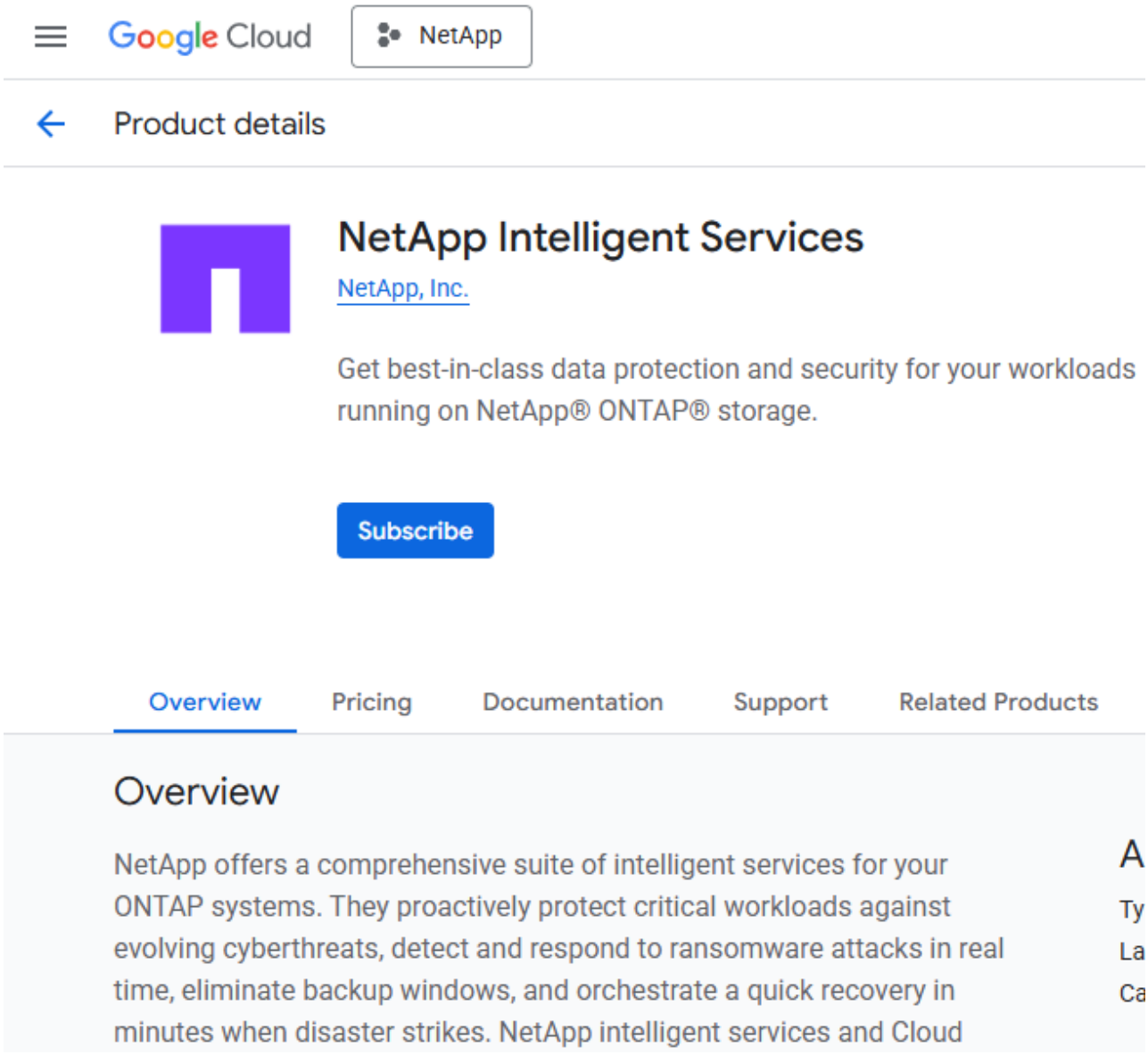
1. 선택한 자격 증명으로 기존 구독을 구성하려면 드롭다운 목록에서 Google Cloud 프로젝트와 구독을 선택한 다음 *구성*을 선택합니다.



2. 아직 구독이 없다면 *구독 추가 > 계속*을 선택하고 Google Cloud Marketplace의 단계를 따르세요.

   다음 단계를 완료하기 전에 Google Cloud 계정에서 청구 관리자 권한과 NetApp Console 로그인 권한이 모두 있는지 확인하세요.

   a. 당신이 리디렉션된 후 "Google Cloud Marketplace의 NetApp Intelligent Services 페이지" 상단 탐색 메뉴에서 올바른 프로젝트가 선택되었는지 확인하세요.



b. *구독*을 선택하세요.

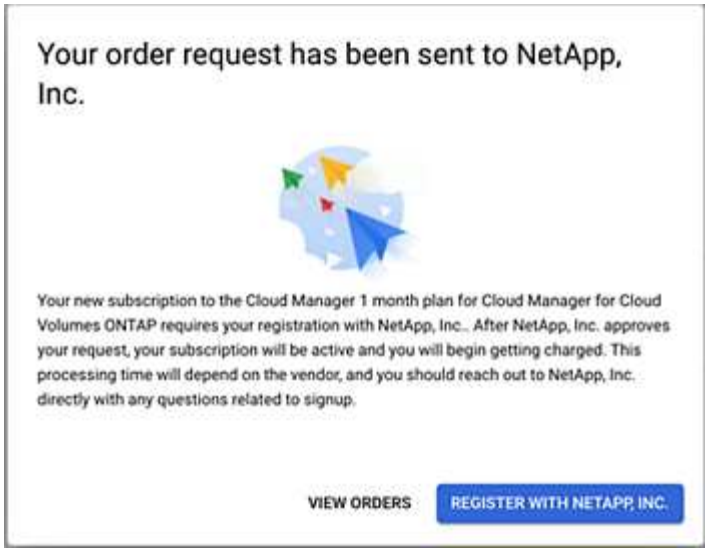
c. 적절한 청구 계정을 선택하고 약관에 동의하세요.

d. *구독*을 선택하세요.

   이 단계에서는 귀하의 전송 요청이 NetApp 으로 전송됩니다.

e. 팝업 대화 상자에서 * NetApp, Inc.에 등록*을 선택합니다.

   Google Cloud 구독을 Console 조직 또는 계정과 연결하려면 이 단계를 완료해야 합니다. 구독 연결 프로세스는 이 페이지에서 리디렉션된 후 콘솔에 로그인할 때까지 완료되지 않습니다.



f. 구독 할당 페이지의 단계를 완료하세요.

> 귀하의 조직에서 이미 귀하의 청구 계정에서 마켓플레이스 구독을 보유한 사람이 있는 경우 귀하는 다음으로 리디렉션됩니다. "NetApp Console 내 Cloud Volumes ONTAP 페이지" 대신에. 예상치 못한 상황이라면 NetApp 영업팀에 문의하세요. Google은 Google 결제 계정당 하나의 구독만 허용합니다.

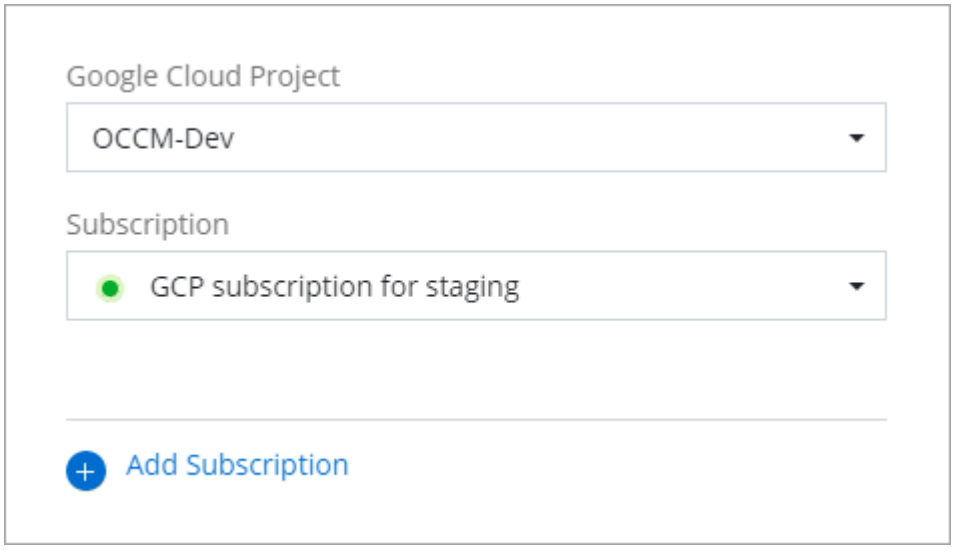
- 이 구독을 연결할 콘솔 조직을 선택하세요.
- 기존 구독 교체 필드에서 한 조직의 기존 구독을 이 새로운 구독으로 자동으로 교체할지 여부를 선택합니다.

  콘솔은 조직의 모든 자격 증명에 대한 기존 구독을 이 새로운 구독으로 대체합니다. 자격 증명 세트가 구독과 연결되지 않은 경우 이 새 구독은 해당 자격 증명과 연결되지 않습니다.

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

◦ *저장*을 선택하세요.

3. 이 프로세스가 완료되면 콘솔의 자격 증명 페이지로 돌아가서 새 구독을 선택하세요.

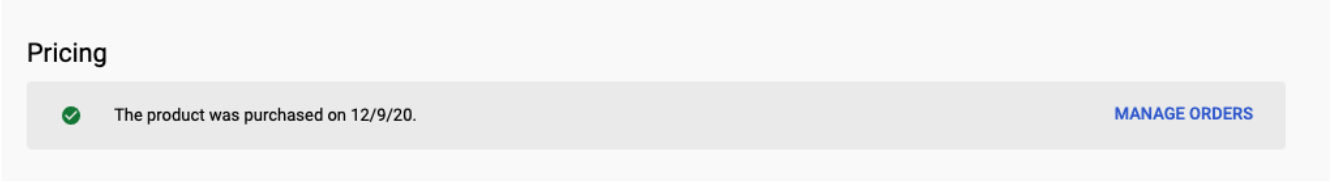


마켓플레이스 구독 프로세스 문제 해결

Google Cloud Marketplace를 통해 NetApp 데이터 서비스를 구독하는 과정에서 권한 설정이 잘못되었거나 Console로의 리디렉션을 실수로 따르지 않아 구독이 중단되는 경우가 있습니다. 이러한 문제가 발생하면 다음 단계를 따라 구독 프로세스를 완료하세요.

단계

1. "Google 클라우드 마켓플레이스의 NetApp 페이지"로 이동하여 주문 상태를 확인하세요. 페이지에 *Manage on Provider*라고 표시되어 있으면 아래로 스크롤하여 *Manage Orders*를 선택하세요.



   - 주문에 녹색 체크 표시가 나타나는데 이것이 예상치 못한 경우, 동일한 결제 계정을 사용하는 조직의 다른 사용자가 이미 구독 중일 수 있습니다. 이러한 상황이 예상치 못한 경우 또는 해당 구독에 대한 자세한 정보가 필요한 경우 NetApp 영업팀에 문의하십시오.

   - 주문에 시계 아이콘과 **Pending** 상태가 표시되면 마켓플레이스 페이지로 돌아가서 *Manage on Provider*를 선택하여 위에 설명된 대로 프로세스를 완료하십시오.

ID 및 액세스 관리

NetApp Console ID 및 액세스 관리에 대해 알아보세요

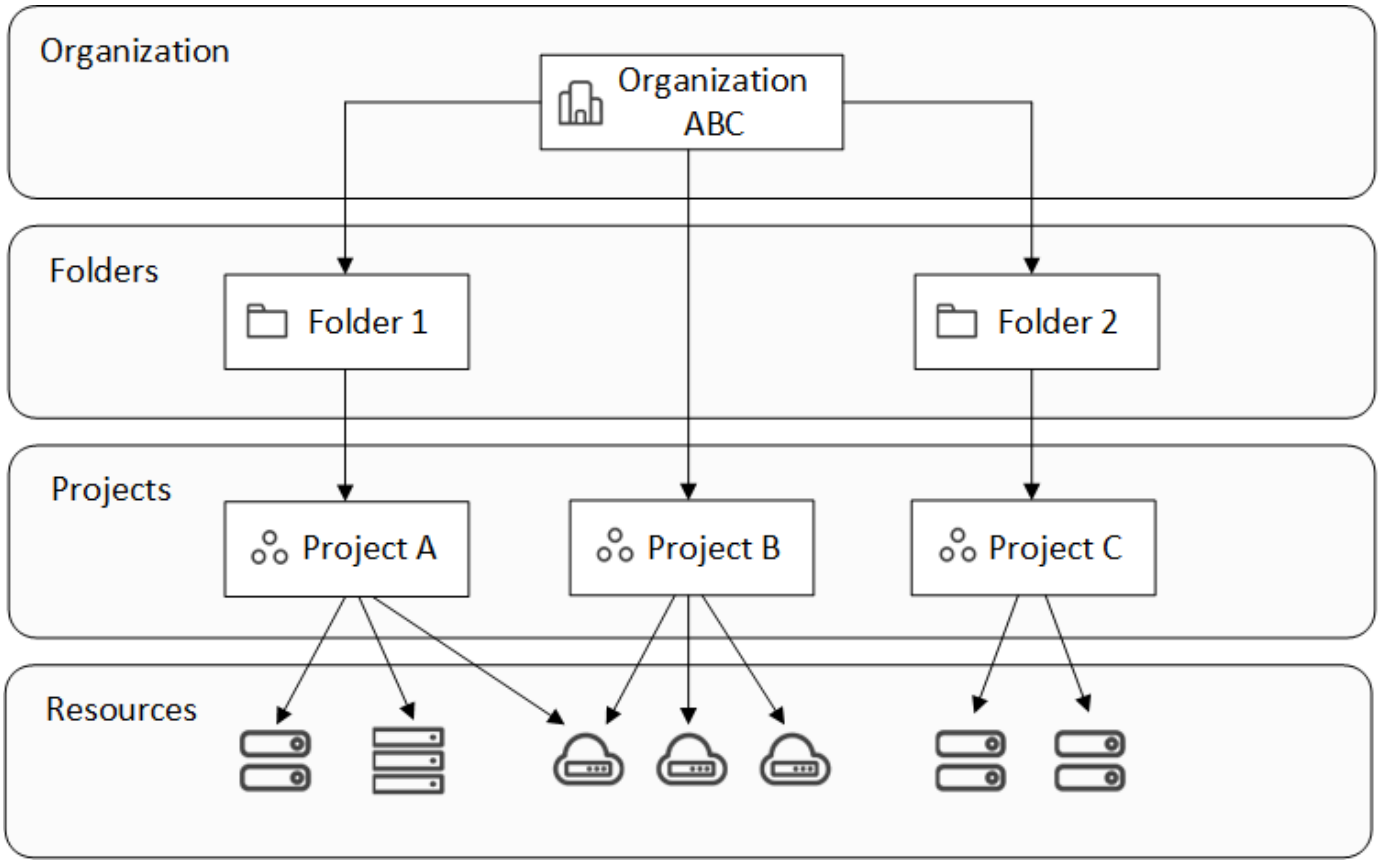
NetApp 콘솔의 ID 및 액세스 관리(IAM)를 사용하여 NetApp 리소스를 구성하고 위치, 부서 또는 프로젝트와 같은 비즈니스 구조에 따라 액세스를 제어하십시오.

리소스는 계층적으로 구성됩니다. 최상위에는 조직이 있고, 그 아래에 폴더(다른 폴더나 프로젝트를 포함할 수 있음)가 있으며, 그 아래에는 스토리지 시스템, 워크로드 및 에이전트를 포함하는 프로젝트가 있습니다.

조직, 폴더 또는 프로젝트 수준에서 액세스 역할을 할당하여 사용자가 리소스에 대한 올바른 액세스 권한을 갖도록 합니다.

NetApp Console 에서 IAM을 관리하려면 슈퍼 관리자, 조직 관리자 또는 폴더 또는 프로젝트 관리자 역할이 있어야 합니다.

다음 이미지는 기본적인 수준의 계층 구조를 보여줍니다.



]

신원 및 접근 관리 구성 요소

NetApp Console 에서는 조직 구성 요소, 리소스 구성 요소 및 사용자 액세스 구성 요소라는 세 가지 주요 구성 요소를 사용하여 스토리지 리소스를 구성합니다.

조직 내 프로젝트 및 폴더

IAM 구조 내에서 조직, 프로젝트 및 폴더라는 세 가지 구성 요소를 사용합니다. 이러한 레벨 중 하나에서 사용자에게 역할을 할당하여 액세스 권한을 부여할 수 있습니다.

조직

_조직_은 콘솔 IAM 시스템의 최상위 수준이며 일반적으로 회사를 나타냅니다. 조직은 폴더, 프로젝트, 구성원, 역할 및 리소스로 구성됩니다. 에이전트는 조직 내의 특정 프로젝트와 연관되어 있습니다.

프로젝트

프로젝트는 스토리지 리소스에 대한 접근 권한을 제공하는 데 사용됩니다. 리소스에 접근하려면 먼저 해당 리소스가 프로젝트에 할당되어야 합니다. 하나의 프로젝트에 여러 리소스를 할당할 수 있으며, 여러 개의 프로젝트를 생성할 수도 있습니다. 그런 다음 사용자에게 프로젝트 권한을 할당하여 프로젝트 내 리소스에 대한 접근 권한을 부여합니다.

예를 들어, 필요에 따라 온프레미스 ONTAP 시스템을 단일 프로젝트 또는 조직 내 모든 프로젝트와 연결할 수 있습니다.

"조직에 프로젝트를 추가하는 방법을 알아보세요."

폴더

관련 프로젝트를 위치, 사이트 또는 사업부별로 정리하려면 폴더로 그룹화하세요. 리소스를 폴더에 직접 연결할 수는 없지만, 폴더 수준에서 사용자에게 역할을 할당하면 해당 폴더에 있는 모든 프로젝트에 대한 액세스 권한을 부여할 수 있습니다.

"조직에 폴더를 추가하는 방법을 알아보세요."

리소스

_리소스_는 NetApp Console이 인식하고 프로젝트에 할당할 수 있는 엔티티입니다. _리소스_에는 스토리지 시스템, Keystone 구독, 일부 NetApp Backup and Recovery 워크로드 및 NetApp Console 에이전트가 포함됩니다.

+ 리소스에 접근하려면 먼저 해당 리소스를 프로젝트와 연결해야 합니다.

+

예를 들어, Cloud Volumes ONTAP 시스템을 특정 프로젝트 또는 조직 내 모든 프로젝트와 연결할 수 있습니다. 리소스를 연결하는 방법은 조직의 요구 사항에 따라 다릅니다.

+

"프로젝트에 리소스를 연결하는 방법을 알아보세요."

스토리지 시스템 및 **Keystone** 구독

스토리지 시스템은 NetApp Console에서 관리하는 주요 리소스입니다. NetApp Console은 온프레미스 및 클라우드 스토리지 시스템 모두의 관리를 지원합니다. 프로젝트에 할당된 사용자가 스토리지 시스템에 액세스할 수 있도록 프로젝트에 스토리지 시스템을 추가해야 합니다.

스토리지 시스템

스토리지 시스템은 추가되는 프로젝트에 자동으로 연결되지만, 리소스 페이지에서 다른 프로젝트 또는 폴더와 연결할 수도 있습니다. FSx for NetApp ONTAP 스토리지 시스템은 프로젝트 또는 폴더와 연결할 수 없지만, 시스템 페이지 또는 워크로드에서 확인할 수 있습니다.

Keystone 구독

Keystone 구독은 NetApp Console 에서 사용자가 구독에 액세스할 수 있도록 프로젝트와 연결할 수 있는 리소스이기도 합니다.

백업 및 복구 워크로드**(Oracle** 및 **Microsoft SQL Server)**

일부 Backup and Recovery 워크로드도 리소스로 간주됩니다. 사용자에게 Backup and

콘솔 에이전트

조직 관리자는 스토리지 시스템을 관리하고 NetApp 데이터 서비스를 활성화하기 위해 콘솔 에이전트를 생성합니다. 에이전트는 처음에 생성된 프로젝트에 연결되지만, 관리자는 에이전트 페이지에서 다른 프로젝트나 폴더에 에이전트를 추가할 수 있습니다.

에이전트를 프로젝트와 연결하면 해당 프로젝트의 리소스를 관리할 수 있으며, 에이전트를 폴더와 연결하면 폴더 또는 프로젝트 관리자가 어떤 프로젝트에서 해당 에이전트를 사용할지 결정할 수 있습니다. 에이전트는 관리 기능을 제공하기 위해 특정 프로젝트와 연결되어야 합니다.

"프로젝트에 에이전트를 연결하는 방법을 알아보세요."

구성원 및 역할

회원들

조직의 구성원은 사용자 계정 또는 서비스 계정입니다. 서비스 계정은 일반적으로 애플리케이션에서 사람의 개입 없이 지정된 작업을 완료하는 데 사용됩니다.

NetApp Console 에 가입한 구성원을 조직에 추가해야 합니다. 추가한 후에는 역할을 할당하여 리소스에 대한 액세스 권한을 부여할 수 있습니다. 콘솔 내에서 수동으로 서비스 계정을 추가하거나 NetApp Console IAM API를 통해 생성 및 관리를 자동화할 수 있습니다.

"조직에 구성원을 추가하는 방법을 알아보세요."

액세스 역할

콘솔은 조직의 구성원에게 할당할 수 있는 액세스 역할을 제공합니다.

구성원에게 역할을 연결할 때, 해당 역할을 조직 전체, 특정 폴더 또는 특정 프로젝트에 대해 부여할 수 있습니다. 선택한 역할은 해당 계층 구조의 선택한 부분에 있는 리소스에 대한 권한을 구성원에게 부여합니다.

NetApp Console "최소 권한" 원칙을 준수하는 세분화된 역할을 제공합니다. 즉, 액세스 역할은 사용자가 필요한 기능에만 접근할 수 있도록 설계되었습니다.

이는 사용자의 업무 범위가 확장됨에 따라 여러 역할을 부여받을 수 있음을 의미합니다.

"액세스 역할에 대해 알아보세요" .

IAM 전략 사례

소규모 조직 전략

사용자 수가 50명 미만이고 스토리지 관리가 중앙 집중식으로 이루어지는 조직의 경우, 슈퍼 관리자 및 슈퍼 뷰어 역할을 사용하는 간소화된 접근 방식을 고려해 보세요.

예시**: ABC** 회사 **(5**인 팀**)**

- 구조**:** 3개의 프로젝트(운영, 개발, 백업)를 보유한 단일 조직
- 역할**:**
  - 2명의 고위 멤버: 완전한 관리자 권한을 가진 슈퍼 관리자 역할
  - 팀 구성원 3명: 수정 권한 없이 모니터링만 가능한 슈퍼 뷰어 역할
- 에이전트 전략**:** 모든 프로젝트에 연결된 단일 에이전트를 사용하여 공유 리소스에 액세스합니다.
- 장점**:** 관리 간소화, 역할 복잡성 감소, 광범위한 접근 권한이 필요한 팀에 적합

다지역 기업 전략

지역별 운영 및 전문 팀을 보유한 대규모 조직의 경우, 지리적 또는 사업부 경계를 나타내는 폴더를 사용하는 계층적 접근 방식을 구현하십시오.

예시**: XYZ** 주식회사**(**다국적 기업**)**

- 구조**:** 조직 > 지역별 폴더(북미, 유럽, 아시아 태평양) > 지역별 프로젝트 폴더

- 플랫폼 역할**:**
  - 1. 조직 관리: 글로벌 총괄 및 정책 관리
  - 3 폴더 또는 프로젝트 관리자: 지역별 관리 (지역당 1명)
  - 1. 연합 관리: 기업 ID 공급자 통합
- 지역별 스토리지 역할**:**
  - 9 스토리지 관리자: 지정된 지역의 스토리지 시스템을 검색하고 관리합니다.
  - 2. 스토리지 뷰어: 여러 지역의 스토리지 리소스를 모니터링합니다.
  - 1. 시스템 상태 전문가: 시스템 수정 없이 스토리지 상태를 관리합니다.
- 데이터 서비스 역할**:**
  - 백업 및 복구 관리자: 백업 책임 범위에 따라 프로젝트별로 책정됩니다.
  - 랜섬웨어 복원력 관리자: 프로젝트 전반에 걸친 보안 팀 모니터링
- 에이전트 전략**:** 해당 지역 프로젝트에 적합한 지역 에이전트를 배정합니다.
- 장점**:** 역할 분리, 지역 자율성 및 현지 규정 준수를 통한 보안 강화

학과별 전문화 전략

특정 데이터 서비스 접근 권한이 필요한 전문 팀을 보유한 조직의 경우, 기능적 책임에 기반한 맞춤형 역할 할당을 활용하십시오.

예시**: TechCorp (**중견 기술 기업**)**

- 구조**:** 조직 > 부서 폴더(IT, 보안, 개발) > 프로젝트별 리소스
- 전문적인 역할**:**
  - 보안팀: 랜섬웨어 복원력 관리자 및 분류 보기 담당자 역할
  - 백업 팀: 포괄적인 백업 작업을 위한 백업 및 복구 최고 관리자
  - 개발팀: 테스트 환경 관리를 위한 저장소 관리자
  - 규정 준수 팀: 모니터링 및 지원 사례 관리를 담당할 운영 지원 분석가
- 에이전트 전략**:** 리소스 소유권을 기반으로 부서 프로젝트에 에이전트를 연결합니다.
- 장점**:** 맞춤형 접근 제어, 운영 효율성 향상, 전문 업무에 대한 명확한 책임 소재 규명

NetApp Console 에서 **IAM** 관련 다음 단계

- "NetApp Console 에서 IAM 시작하기"
- "IAM 활동 모니터링 또는 감사"
- "NetApp Console IAM에 대한 API에 대해 알아보세요"

NetApp Console 에서 ID 및 액세스 시작하기

NetApp Console 에 가입하면 새 조직을 만들라는 메시지가 표시됩니다. 조직에는 한 명의 구성원(조직 관리자)과 한 개의 기본 프로젝트가 포함됩니다. 비즈니스 요구 사항에 맞게 ID 및

액세스 관리(IAM)를 설정하려면 조직의 계층 구조를 사용자 지정하고, 추가 구성원을 추가하고, 리소스를 추가하거나 검색하고, 계층 구조 전반에 걸쳐 해당 리소스를 연결해야 합니다.

조직의 ID 및 액세스를 관리하려면 조직 관리자 또는 슈퍼 관리자 권한이 필요합니다. 폴더 또는 프로젝트 관리자 권한이 있으면 접근 권한이 있는 폴더와 프로젝트만 관리할 수 있습니다.

새로운 조직을 설정하려면 다음 단계를 따르세요. 순서는 조직의 요구 사항에 따라 달라질 수 있습니다.

1 기본 프로젝트를 편집하거나 조직의 계층 구조에 추가하세요.

기본 프로젝트를 사용하거나 비즈니스 계층 구조에 맞는 추가 프로젝트와 폴더를 만드세요.

"폴더와 프로젝트를 사용하여 리소스를 구성하는 방법을 알아보세요." .

2 귀하의 조직과 회원을 연결하세요

사용자가 NetApp Console 에 가입한 후에는 콘솔 조직에 해당 사용자를 명시적으로 추가해야 합니다. 조직에 서비스 계정을 추가하는 옵션도 있습니다.

"멤버와 멤버의 권한을 관리하는 방법을 알아보세요" .

3 리소스 추가 또는 검색

콘솔에 리소스(시스템)를 추가하거나 검색합니다. 조직 구성원은 프로젝트 내에서 시스템을 관리합니다.

리소스를 만들거나 검색하는 방법을 알아보세요.

- "Amazon FSx for NetApp ONTAP"
- "Azure NetApp Files"
- "Cloud Volumes ONTAP"
- "E-시리즈 시스템"
- "온프레미스 ONTAP 클러스터"
- "StorageGRID"

4 추가 프로젝트와 리소스 연결

콘솔에서 시스템을 추가하거나 검색하면 해당 리소스가 현재 선택된 프로젝트와 자동으로 연결됩니다. 해당 리소스를 조직의 다른 프로젝트에서 사용할 수 있도록 하려면 해당 프로젝트와 연결하세요. 콘솔 에이전트를 사용하여 리소스를 관리하는 경우 콘솔 에이전트를 해당 프로젝트와 연결합니다.

- "조직의 리소스 계층을 관리하는 방법을 알아보세요" .
- "콘솔 에이전트를 폴더 또는 프로젝트와 연결하는 방법을 알아보세요." .

관련 정보

- "NetApp Console 에서 ID 및 액세스 관리에 대해 알아보세요"

- "ID 및 액세스를 위한 API에 대해 알아보세요"

콘솔 구성을 설정하세요

NetApp Console 조직에 폴더와 프로젝트를 추가하세요.

비즈니스 구조에 맞게 폴더와 프로젝트를 추가하세요. 폴더와 프로젝트를 생성한 후에는 해당 폴더에 리소스를 연결하고 프로젝트에 대한 구성원의 액세스 권한을 관리할 수 있습니다.

콘솔은 새 조직을 생성할 때 자동으로 하나의 프로젝트를 생성합니다. 대부분의 조직은 하나 이상의 프로젝트를 필요로 하며, 자료를 정리하기 위한 폴더도 필요합니다. "NetApp Console 의 리소스 계층 구조에 대해 알아보세요.".

폴더와 프로젝트를 사용하여 리소스를 정리하세요

NetApp Console 에서 조직은 리소스를 구성하는 데 도움이 되는 폴더와 프로젝트로 구성됩니다. 폴더를 사용하면 관련 프로젝트를 그룹화할 수 있고, 프로젝트를 사용하면 리소스와 구성원 접근 권한을 관리할 수 있습니다.

폴더

폴더는 관련된 프로젝트를 정리하는 데 도움이 됩니다. 조직 구조의 다양한 계층을 나타내기 위해 중첩 폴더를 만들 수 있습니다. 예를 들어, 각 사업부별로 최상위 폴더를 만들고 그 안에 해당 사업부 내의 여러 팀별로 하위 폴더를 만들 수 있습니다. 그다음에는 폴더 안에 프로젝트를 생성합니다.

폴더를 사용하면 역할 상속을 통해 구성원 접근 권한을 더욱 효율적으로 관리할 수 있습니다. 폴더 수준에서 멤버에게 역할을 할당하면 해당 멤버는 모든 하위 프로젝트 및 폴더에 대한 권한을 상속받습니다.

폴더는 조직 관리를 위한 도구이며, 조직 관리자, 폴더 관리자, 프로젝트 관리자 또는 슈퍼 관리자 역할과 같은 IAM 권한이 없는 구성원에게는 표시되지 않습니다. 회원은 폴더가 아닌 프로젝트에 접근할 수 있습니다.

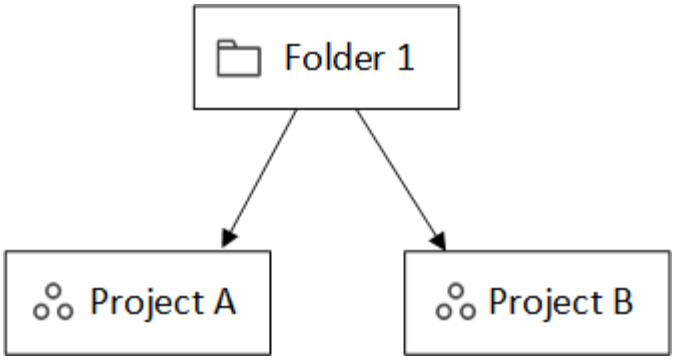
조직 관리자는 폴더를 생성하여 관리 책임을 위임할 수 있습니다. 폴더를 생성한 후, 조직 관리자는 특정 폴더에 대해 구성원에게 폴더 관리자 또는 프로젝트 관리자 역할을 할당할 수 있습니다. 이러한 구성원들은 전체 조직에 대한 접근 권한 없이도 해당 폴더 내의 모든 프로젝트를 관리할 수 있습니다.

폴더는 다른 폴더나 프로젝트를 하위 폴더로 포함할 수 있지만, 리소스를 직접적으로 연결할 수는 없습니다. 리소스는 프로젝트와 연관되어야 합니다.

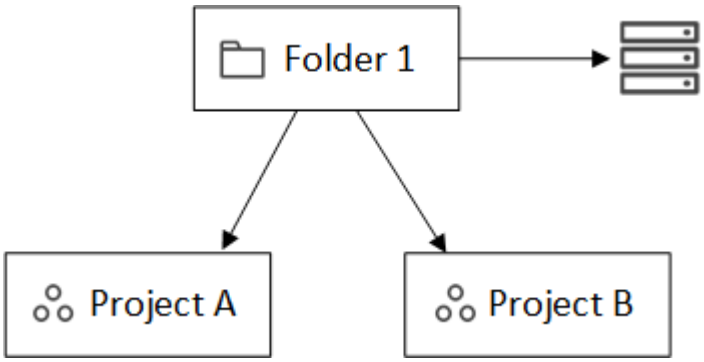
리소스를 폴더와 연결할 때

_조직 관리자_는 리소스를 폴더와 연결할 수 있으므로 _폴더 또는 프로젝트 관리자_는 이를 폴더 내의 적절한 프로젝트에 연결할 수 있습니다.

예를 들어, 두 개의 프로젝트가 포함된 폴더가 있다고 가정해 보겠습니다.

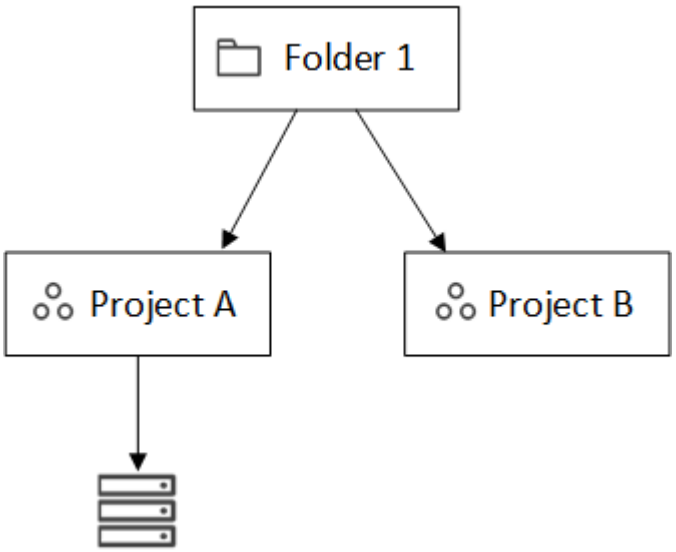


_조직 관리자_는 리소스를 폴더와 연결할 수 있습니다.



리소스를 폴더와 연결해도 모든 프로젝트에서 액세스할 수 있는 것은 아닙니다. 폴더 또는 프로젝트 관리자만 볼 수 있습니다. _폴더 또는 프로젝트 관리자_는 어떤 프로젝트가 액세스할 수 있는지 결정하고 리소스를 적절한 프로젝트와 연결합니다.

이 예에서 관리자는 리소스를 프로젝트 A와 연결합니다.



프로젝트 A에 대한 권한이 있는 멤버는 이제 리소스에 액세스할 수 있습니다.

프로젝트

구성원이 리소스를 관리할 수 있도록 리소스와 프로젝트를 연결하세요. 리소스는 관리 및 사용자 접근을 위해 프로젝트와 연결되어야 합니다.

조직은 하나 또는 여러 개의 프로젝트를 가질 수 있습니다. 프로젝트는 조직 바로 아래에 있거나 폴더 안에 있을 수 있습니다. 프로젝트 내 리소스를 검색하는 데 에이전트를 사용하는 경우 해당 에이전트를 프로젝트와 연결해야 합니다.

사용자는 시스템 페이지에서 할당된 프로젝트 간을 탐색하여 각 프로젝트와 관련된 리소스를 관리할 수 있습니다.

폴더 또는 프로젝트 추가

프로젝트를 추가하여 리소스를 관리하고, 폴더를 추가하여 관련 프로젝트를 그룹화하세요. 새 조직을 생성하면 콘솔에 프로젝트 하나가 포함됩니다.

조직의 리소스 구조에서 최대 7단계의 폴더와 프로젝트를 생성할 수 있습니다. 필요에 따라 하위 폴더를 만들어 리소스를 정리하세요.

단계

1. *관리 > ID 및 액세스*를 선택합니다.
2. *조직*을 선택하세요.
3. 조직 페이지에서 *폴더 또는 프로젝트 추가*를 선택합니다.
4. 폴더 또는 *프로젝트*를 선택하세요.
5. 폴더 또는 프로젝트 세부 정보를 입력하세요:
   - 이름 및 위치: 폴더 또는 프로젝트의 이름을 입력하고 위치를 선택하세요. 폴더나 프로젝트는 조직 아래에 또는 다른 폴더 안에 배치할 수 있습니다.
   - 리소스: 이 폴더 또는 프로젝트와 연결할 리소스를 선택하세요. 콘솔에 스토리지 시스템을 아직 추가하지 않았다면 나중에 이 단계를 진행할 수 있습니다.

     구성원은 해당 리소스가 프로젝트에 할당되기 전까지는 폴더 내의 리소스에 접근할 수 없습니다. 필요한 프로젝트를 만들 때까지 리소스를 임시로 보관하려면 폴더를 사용하세요. 이 기능을 통해 조직 관리자는 리소스 할당을 폴더 또는 프로젝트 관리자에게 위임할 수 있으며, 폴더 또는 프로젝트 관리자는 해당 폴더 내의 프로젝트에 리소스를 할당할 수 있습니다.

   - 접근 권한: *멤버 추가*를 선택하여 접근 권한과 역할을 할당하세요. 프로젝트 또는 폴더에서 언제든지 구성원을 추가하거나 삭제할 수 있습니다.

     "액세스 역할에 대해 알아보세요" .
6. *추가*를 선택하세요.

폴더 또는 프로젝트 이름 바꾸기

필요에 따라 폴더 또는 프로젝트 이름을 변경하세요. 이름 변경은 관련 리소스나 회원 접근 권한에 영향을 미치지 않습니다.

단계

1. 조직 페이지에서 표의 프로젝트나 폴더로 이동하여 다음을 선택합니다. ••• 그런 다음 폴더 편집 또는 *프로젝트 편집*을 선택합니다.
2. 편집 페이지에서 새 이름을 입력하고 *적용*을 선택합니다.

폴더 또는 프로젝트 삭제

팀 재편성이나 프로젝트 완료 후 더 이상 필요하지 않은 폴더와 프로젝트를 삭제하세요.

폴더나 프로젝트를 삭제하기 전에 해당 폴더에 리소스가 포함되어 있지 않은지 확인하십시오. 리소스를 제거하는 방법을 알아보세요.

단계

1. 조직 페이지에서 표의 프로젝트나 폴더로 이동하여 다음을 선택합니다. ••• 그런 다음 *삭제*를 선택하세요.
2. 폴더나 프로젝트를 삭제할지 확인하세요.

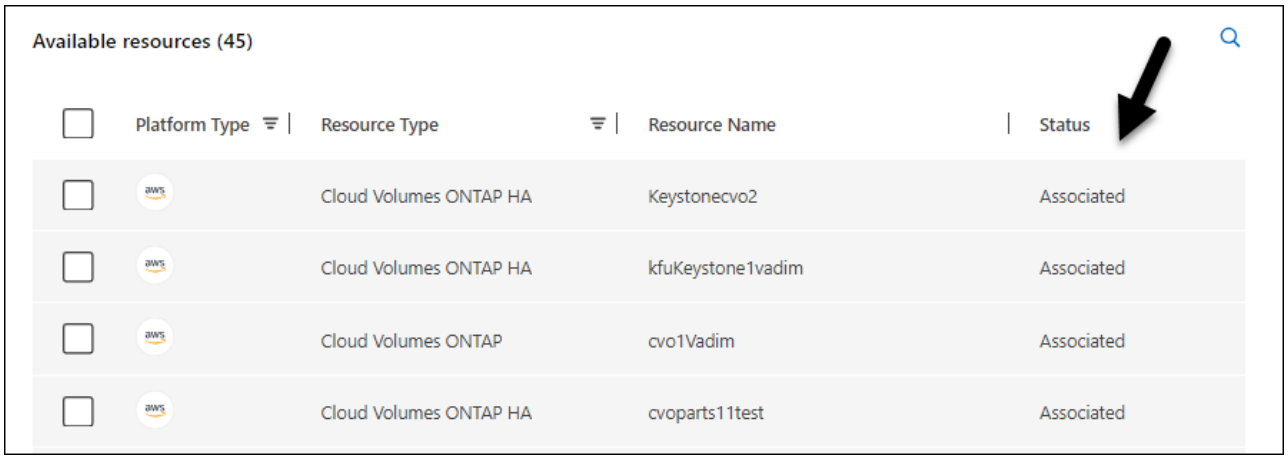
폴더 또는 프로젝트와 관련된 리소스 보기

폴더나 프로젝트와 연관된 리소스와 멤버를 확인하세요.

단계

1. 조직 페이지에서 표의 프로젝트나 폴더로 이동하여 다음을 선택합니다. ••• 그런 다음 폴더 편집 또는 *프로젝트 편집*을 선택합니다.

2. 편집 페이지에서 리소스 또는 액세스 섹션을 확장하여 선택한 폴더나 프로젝트에 대한 세부 정보를 볼 수 있습니다.
   - 연관된 리소스를 보려면 리소스*를 선택하세요. 표에서 *상태 열은 폴더나 프로젝트와 연관된 리소스를 식별합니다.



폴더 또는 프로젝트와 관련된 리소스를 변경합니다.

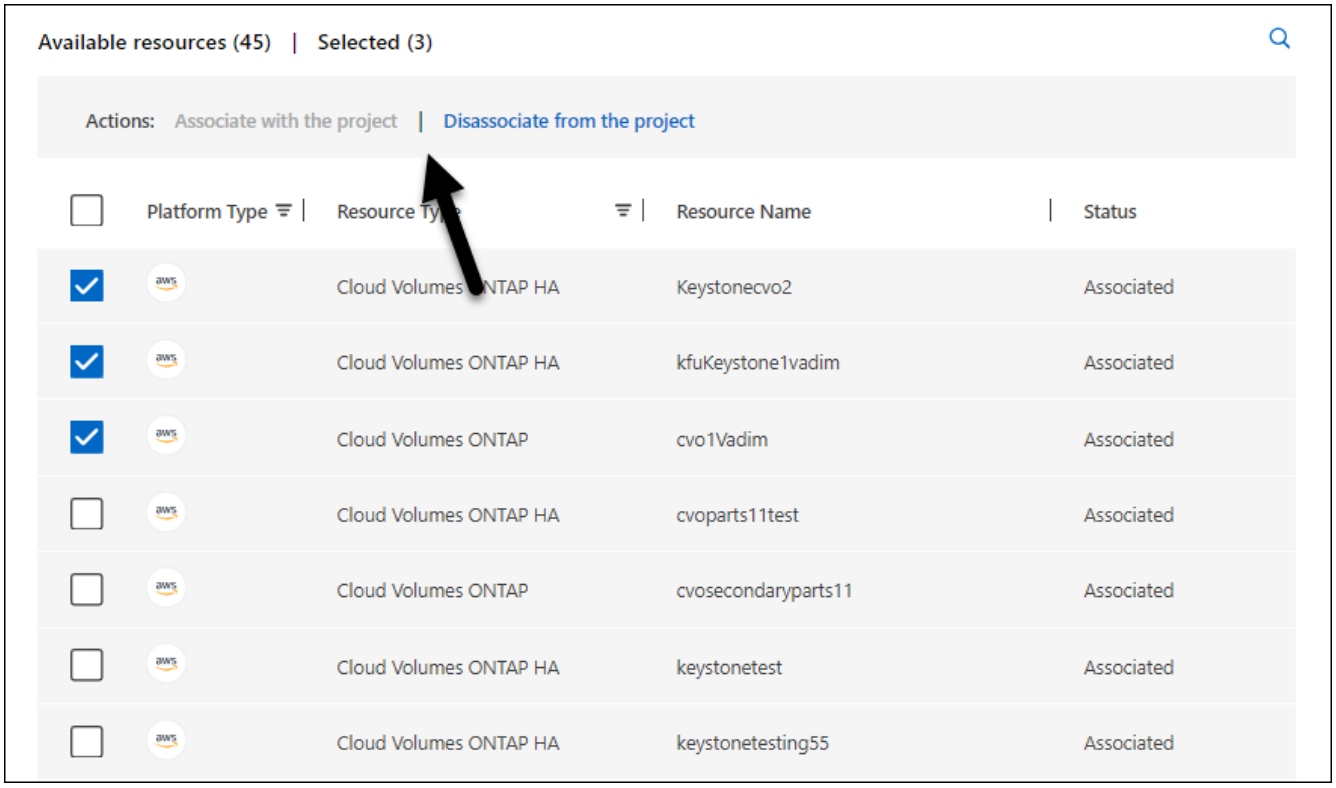
조직의 요구 사항이 변경됨에 따라 폴더 또는 프로젝트와 연결된 리소스를 변경할 수 있습니다.

단계

1. 조직 페이지에서 표의 프로젝트나 폴더로 이동하여 다음을 선택합니다. ••• 그런 다음 폴더 편집 또는 *프로젝트 편집*을 선택합니다.
2. 편집 페이지에서 *리소스*를 선택합니다.

   표에서 상태 열은 폴더나 프로젝트와 연관된 리소스를 식별합니다.

3. 연결하거나 연결 해제할 리소스를 선택하세요.
4. 선택한 리소스를 기반으로 프로젝트에 연결 또는 *프로젝트에서 연결 해제*를 선택하십시오.



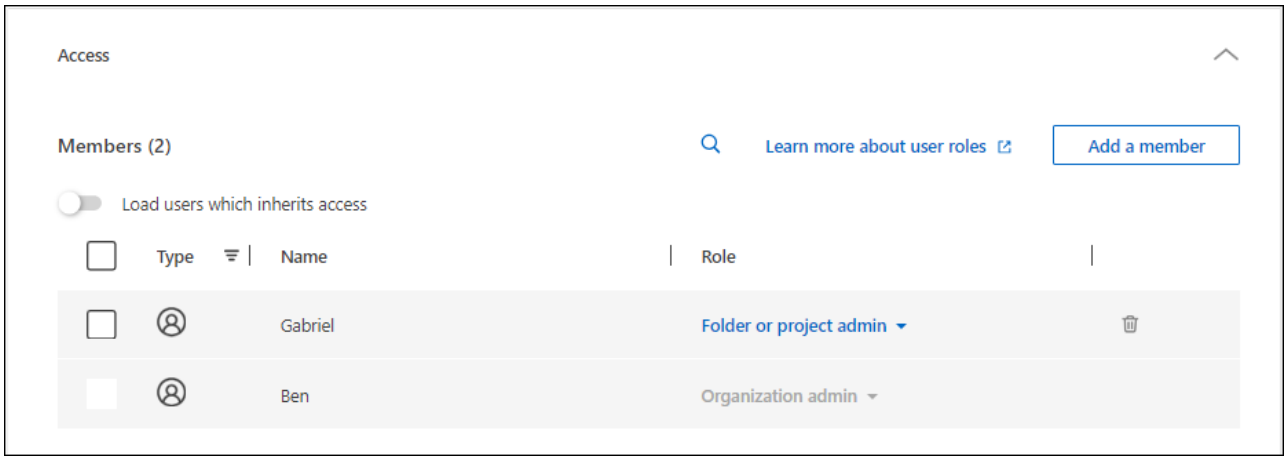
5. *적용*을 선택하세요.

폴더 또는 프로젝트와 연관된 멤버 보기

조직 페이지에서 폴더 또는 프로젝트와 관련된 구성원을 볼 수 있습니다.

단계

1. 조직 페이지에서 표의 프로젝트나 폴더로 이동하여 다음을 선택합니다. ••• 그런 다음 폴더 편집 또는 *프로젝트 편집*을 선택합니다.
2. 편집 페이지에서 *액세스*를 선택하면 선택한 폴더나 프로젝트에 액세스할 수 있는 멤버 목록을 볼 수 있습니다.
   - 폴더나 프로젝트에 접근할 수 있는 멤버를 보려면 *접근*을 선택하세요.



폴더 또는 프로젝트에 대한 멤버 액세스 수정

리소스 접근을 제어하려면 멤버 접근 권한을 수정하세요. 폴더 수준에서 할당된 역할은 모든 하위 프로젝트 및 폴더에 상속된다는 점을 기억하십시오.

폴더 또는 조직 수준에서 상속된 구성원 액세스 권한은 하위 수준에서 변경할 수 없습니다. 상위 계층에서 구성원의 권한을 변경하여 접근 권한을 변경하세요. 또는 다음과 같은 방법도 있습니다. "회원 페이지에서 권한 관리".

단계

1. 조직 페이지에서 표의 프로젝트나 폴더로 이동하여 다음을 선택합니다. ••• 그런 다음 폴더 편집 또는 *프로젝트 편집*을 선택합니다.
2. 편집 페이지에서 *액세스*를 선택하면 선택한 폴더나 프로젝트에 액세스할 수 있는 멤버 목록을 볼 수 있습니다.
3. 멤버 접근 권한 수정:
   - 멤버 추가: 폴더나 프로젝트에 추가하려는 멤버를 선택하고 역할을 할당합니다.
   - 멤버 역할 변경: 조직 관리자 이외의 역할을 가진 멤버의 경우 기존 역할을 선택한 다음 새 역할을 선택합니다.
   - 멤버 접근 권한 제거: 보고 있는 폴더나 프로젝트에 역할이 정의된 멤버의 경우, 해당 접근 권한을 제거할 수 있습니다.
4. *적용*을 선택하세요.

관련 정보

- "NetApp Console 에서 ID 및 액세스에 대해 알아보세요"
- "신원 및 액세스 시작하기"
- "ID 및 액세스 API에 대해 알아보세요"

NetApp Console 에서 폴더 및 프로젝트에 리소스를 추가합니다**.**

NetApp Console 조직의 프로젝트 및 폴더에 사용자를 추가하여 리소스에 대한 사용자 액세스를 제어하십시오. 프로젝트 수준에서 사용자에게 액세스 권한을 부여하세요.

리소스는 콘솔이 인식하는 엔티티로, 스토리지 리소스, 콘솔 에이전트 또는 백업 및 복구 워크로드 등이 있습니다.

콘솔의 리소스 페이지에서 리소스를 보고 관리할 수 있습니다.

콘솔 리소스 유형

NetApp Console 조직의 프로젝트에는 여러 유형의 리소스를 연결할 수 있습니다.

저장 리소스

스토리지 리소스는 조직에서 가장 일반적인 리소스 유형이며 온프레미스 스토리지 시스템과 클라우드 스토리지 시스템을 모두 포함합니다. 콘솔에 스토리지 시스템을 추가할 때 폴더 또는 프로젝트에 추가할 수 있습니다. 그때까지 콘솔은 해당 항목을 발견되지 않은 것으로 표시하고 리소스 페이지에 표시하지 않습니다.

콘솔 에이전트

콘솔 에이전트를 사용하여 스토리지 시스템을 검색한 경우, 해당 에이전트를 동일한 폴더 또는 프로젝트에 추가하십시오. 이를 통해 사용자는 데이터 서비스 또는 콘솔 기본 스토리지 관리와 같은 에이전트 지원 기능을 수행할 수 있습니다. 콘솔의 에이전트 페이지에서 폴더 또는 프로젝트에 에이전트를 추가할 수 있습니다. "콘솔 에이전트를 폴더 또는 프로젝트와 연결하는 방법을 알아보세요.".

Keystone 구독

조직에 Keystone 구독이 있는 경우 리소스 페이지에서 확인할 수 있습니다. Keystone 구독을 폴더 또는 프로젝트와 연결하여 해당 폴더 또는 프로젝트에 대한 권한이 있는 구성원에게 액세스 권한을 부여할 수 있습니다.

귀하의 조직의 리소스를 확인하세요

귀하의 조직과 관련된 발견된 리소스와 발견되지 않은 리소스를 모두 볼 수 있습니다. 시스템은 스토리지 리소스를 찾고 사용자가 콘솔에 추가할 때까지 해당 리소스를 검색되지 않은 상태로 표시합니다.

콘솔에서는 사용자가 해당 리소스를 역할과 연결할 수 없기 때문에 리소스 페이지에서 Amazon FSx for NetApp ONTAP 리소스를 제외합니다. 이러한 리소스는 시스템 페이지 또는 워크로드에서 확인할 수 있습니다.

단계

1. *관리 > ID 및 액세스*를 선택합니다.
2. *리소스*를 선택하세요.
3. *고급 검색 및 필터링*을 선택하세요.
4. 제공되는 옵션을 활용하여 필요한 자료를 찾아보세요.
   - 리소스 이름으로 검색: 텍스트 문자열을 입력하고 *추가*를 선택합니다.
   - 플랫폼: Amazon Web Services 등 하나 이상의 플랫폼을 선택하세요.
   - 리소스: Cloud Volumes ONTAP 과 같은 하나 이상의 리소스를 선택합니다.
   - 조직, 폴더 또는 프로젝트: 전체 조직, 특정 폴더 또는 특정 프로젝트를 선택합니다.
5. *검색*을 선택하세요.

리소스를 폴더 및 프로젝트와 연결

리소스를 폴더 또는 프로젝트에 연결하면 해당 폴더 또는 프로젝트에 대한 권한이 있는 구성원만 해당 리소스를 사용할 수 있습니다.

단계

1. 리소스 페이지에서 표의 리소스로 이동하여 다음을 선택합니다. ••• 그런 다음 *폴더 또는 프로젝트에 연결*을 선택합니다.

2. 폴더나 프로젝트를 선택한 다음 *수락*을 선택하세요.
3. 추가 폴더나 프로젝트를 연결하려면 *폴더 또는 프로젝트 추가*를 선택한 다음 폴더나 프로젝트를 선택합니다.

   관리자 권한이 있는 폴더와 프로젝트에서만 선택할 수 있습니다.

4. *리소스 연결*을 선택하세요.
   - 리소스와 프로젝트를 연결한 경우 해당 프로젝트에 대한 권한이 있는 멤버는 이제 콘솔에서 리소스에 액세스할 수 있습니다.
   - 리소스를 폴더와 연결한 경우, 폴더 또는 프로젝트 관리자는 이제 리소스에 액세스하여 폴더 내의 프로젝트와 연결할 수 있습니다. "리소스를 폴더와 연결하는 방법에 대해 알아보세요".

당신이 완료한 후

콘솔 에이전트를 사용하여 리소스를 발견한 경우 콘솔 에이전트를 프로젝트와 연결하여 액세스 권한을 부여합니다. 그렇지 않으면 조직 관리자 역할이 없는 구성원은 콘솔 에이전트와 관련 리소스에 액세스할 수 없습니다.

"콘솔 에이전트를 폴더 또는 프로젝트와 연결하는 방법을 알아보세요.".

리소스와 연관된 폴더 및 프로젝트 보기

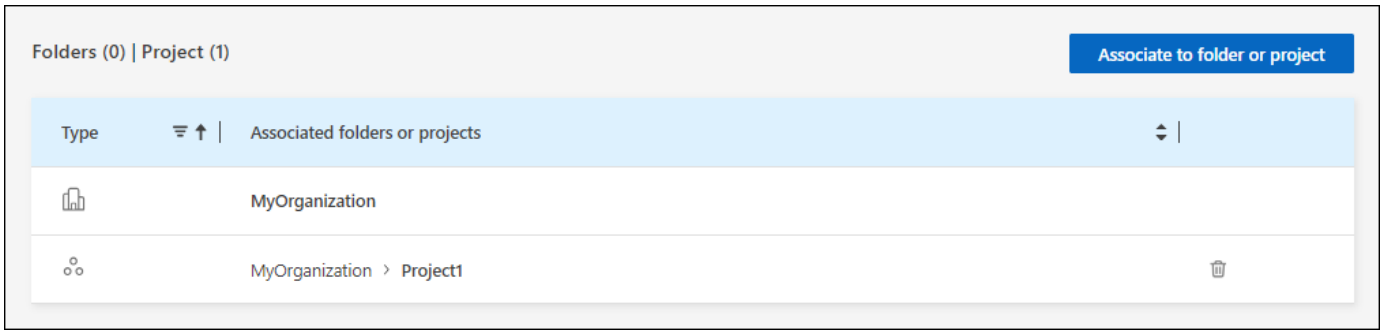
특정 리소스와 관련된 폴더와 프로젝트를 볼 수 있습니다.

리소스에 액세스할 수 있는 조직 구성원을 찾아야 하는 경우 다음을 수행할 수 있습니다."리소스와 연관된 폴더 및 프로젝트에 액세스할 수 있는 멤버를 봅니다." .

단계

1. 리소스 페이지에서 표의 리소스로 이동하여 다음을 선택합니다. ••• 그런 다음 *세부정보 보기*를 선택하세요.

다음 예에서는 하나의 프로젝트와 연관된 리소스를 보여줍니다.



어떤 조직 구성원이 해당 리소스에 접근할 수 있는지 확인하려면,"관련 폴더 및 프로젝트에 대한 액세스 권한이 있는 구성원을 봅니다." .

폴더 또는 프로젝트에서 리소스 제거

폴더 또는 프로젝트에서 리소스를 제거하려면 해당 리소스와의 연결을 제거하십시오. 이렇게 하면 구성원이 해당 폴더 또는 프로젝트의 리소스를 관리할 수 없게 됩니다.

검색된 리소스를 조직 전체에서 제거하려면 시스템 페이지로 이동하여 해당 시스템을 제거하십시오.

단계

1. 리소스 페이지에서 표의 리소스로 이동하여 다음을 선택합니다. ••• 그런 다음 *세부정보 보기*를 선택하세요.
2. 폴더 또는 프로젝트에서 리소스를 제거하려면 다음을 선택하세요. 폴더 또는 프로젝트 옆에 있습니다.
3. 연결을 제거하려면 *삭제*를 선택하세요.

관련 정보

- "NetApp Console 에서 ID 및 액세스에 대해 알아보세요"
- "NetApp Console 에서 ID 및 액세스 시작하기"
- "ID 및 액세스를 위한 API에 대해 알아보세요"

콘솔 에이전트를 다른 폴더 및 프로젝트와 연결합니다.

콘솔 에이전트를 특정 프로젝트와 연결하여 리소스 관리 및 데이터 서비스 액세스를 활성화하십시오. 콘솔 에이전트를 통해 검색된 리소스는 팀 액세스를 위해 해당 리소스와 에이전트가 동일한 프로젝트에 연결되어 있어야 합니다.

최고 관리자 및 조직 관리자는 에이전트를 생성하고 모든 에이전트를 모든 프로젝트 또는 폴더와 연결할 수 있습니다. 폴더 또는 프로젝트 관리자는 자신이 권한을 가진 폴더 및 프로젝트에만 기존 에이전트를 연결할 수 있습니다. "_폴더 또는 프로젝트 관리자_가 완료할 수 있는 작업에 대해 자세히 알아보세요.".

단계

1. 관리 **> ID** 및 액세스 > *에이전트*를 선택합니다.
2. 표에서 연결하려는 콘솔 에이전트를 찾으세요.

   표 위의 검색을 사용하여 특정 콘솔 에이전트를 찾거나 리소스 계층 구조로 표를 필터링하세요.

3. 콘솔 에이전트에 연결된 폴더와 프로젝트를 보려면 다음을 선택하세요. ••• 그런 다음 *세부 정보 보기*를 선택하세요.

   이 페이지에는 콘솔 에이전트와 관련된 폴더와 프로젝트에 대한 세부 정보가 표시됩니다.

4. *폴더 또는 프로젝트에 연결*을 선택합니다.
5. 폴더나 프로젝트를 선택한 다음 *수락*을 선택하세요.
6. 콘솔 에이전트를 추가 폴더나 프로젝트와 연결하려면 *폴더 또는 프로젝트 추가*를 선택한 다음 폴더나 프로젝트를 선택합니다.
7. *협력사 에이전트*를 선택하세요.

당신이 완료한 후

리소스 페이지에서 콘솔 에이전트의 리소스를 동일한 폴더 및 프로젝트와 연결합니다.

"리소스를 폴더 및 프로젝트와 연결하는 방법을 알아보세요." .

관련 정보

- "NetApp Console 에이전트에 대해 알아보세요"
- "NetApp Console ID 및 액세스 관리에 대해 알아보세요"

- "신원 및 액세스 시작하기"
- "ID 및 액세스 관리를 위한 API에 대해 알아보세요"

콘솔 조직에 사용자를 추가하세요

NetApp Console 조직에 사용자 추가

콘솔 내에서 액세스 역할에 따라 사용자에게 프로젝트 또는 폴더에 대한 액세스 권한을 부여할 수 있습니다. 액세스 역할은 구성원(사용자 또는 서비스 계정)이 리소스 계층 구조의 지정된 수준에서 특정 작업을 수행할 수 있도록 하는 권한 집합을 포함합니다.

필수 접근 권한 역할

최고 관리자, 조직 관리자 또는 폴더/프로젝트 관리자(해당 폴더 및 프로젝트를 관리하는 경우에 한함). "액세스 역할에 대해 알아보세요".

NetApp Console 에서 액세스 권한이 부여되는 방식을 이해하십시오.

NetApp Console 역할 기반 액세스 제어(RBAC)를 사용하여 권한을 관리합니다. 사용자에게 개별적으로 또는 연합 그룹을 통해 역할을 할당합니다. 각 역할은 특정 리소스에 대해 허용되는 작업을 정의합니다.

NetApp Console 에서 액세스 권한을 부여할 때 다음 사항에 유의하십시오.

- 모든 사용자는 리소스에 액세스하기 전에 먼저 NetApp Console 에 가입해야 합니다.
- 콘솔에서 각 사용자가 리소스에 액세스하려면 해당 사용자에게 명시적으로 역할을 할당해야 합니다. 이는 역할이 할당된 연합 그룹의 구성원인 경우에도 마찬가지입니다.
- 콘솔에서 직접 서비스 계정을 추가하고 역할을 할당할 수 있습니다.

조직에 구성원 추가

NetApp Console 사용자 계정, 서비스 계정 및 페더레이션 그룹의 세 가지 유형의 멤버를 지원합니다.

연합 그룹에 속해 있더라도 사용자를 추가하고 역할을 할당하려면 먼저 NetApp Console 에 가입해야 합니다. 콘솔에서 직접 서비스 계정을 생성하세요.

모든 구성원은 리소스에 접근하기 위해 최소한 하나의 역할이 명시적으로 할당되어 있어야 합니다.

멤버를 추가할 때는 리소스 수준(조직, 폴더 또는 프로젝트)을 선택하고 필요한 권한이 있는 역할을 할당하세요.

사용자 추가

사용자는 NetApp Console 에 가입하지만, 조직 관리자, 폴더 관리자 또는 프로젝트 관리자가 해당 사용자를 조직, 폴더 또는 프로젝트에 추가해야 리소스에 액세스할 수 있습니다.

시작하기 전에:

사용자는 이미 NetApp Console 에 가입되어 있어야 합니다. 아직 가입하지 않았다면, 가입 페이지로 안내해 주세요. "NetApp Console 에 가입하세요."

연합 그룹에 속한 사용자를 추가하는 경우, 해당 사용자가 이미 NetApp Console 에 가입되어 있고 콘솔에서 명시적으로 역할을 할당받았는지 확인하십시오. NetApp 조직 뷰어와 같은 최소 액세스 역할을 할당하는 것을 권장합니다.

단계

1. *관리 > ID 및 액세스*를 선택합니다.
2. *회원*을 선택하세요.
3. *멤버 추가*를 선택하세요.
4. *회원 유형*에서 *사용자*를 선택된 상태로 둡니다.
5. *사용자 이메일*에는 사용자가 만든 로그인과 연결된 이메일 주소를 입력합니다.
6. 조직, 폴더 또는 프로젝트 선택 섹션을 사용하여 멤버에게 권한이 부여되어야 하는 리소스 계층 수준을 선택합니다.

   다음 사항에 유의하세요.

   - 권한이 있는 폴더와 프로젝트만 선택할 수 있습니다.
   - 조직이나 폴더를 선택하면 해당 구성원에게 모든 콘텐츠에 대한 접근 권한이 부여됩니다.
   - 조직 관리자 역할은 조직 수준에서만 할당할 수 있습니다.
7. 카테고리를 선택한 다음 해당 조직, 폴더 또는 프로젝트에 연결된 리소스에 대한 권한을 멤버에게 제공하는 *역할*을 선택합니다.

   "액세스 역할에 대해 알아보세요" .
8. 더 많은 폴더, 프로젝트 또는 역할에 대한 액세스 권한을 부여하려면 *역할 추가*를 선택하고 폴더, 프로젝트 또는 역할 범주를 선택한 다음 역할을 선택하세요.
9. *추가*를 선택하세요.

   콘솔은 사용자에게 이메일로 지침을 보냅니다.

서비스 계정 추가

서비스 계정을 사용하면 작업을 자동화하고 콘솔 API에 안전하게 연결할 수 있습니다. 간단한 설정을 위해서는 클라이언트 ID와 암호를 선택하고, 자동화 환경이나 클라우드 네이티브 환경에서 보안을 강화하려면 JWT(JSON Web Token)를 선택하십시오. 보안 요구 사항에 맞는 방법을 선택하십시오.

시작하기 전에:

JWT 인증을 위해서는 공개 키 또는 인증서를 준비하십시오.

단계

1. *관리 > ID 및 액세스*를 선택합니다.
2. *회원*을 선택하세요.
3. *멤버 추가*를 선택하세요.
4. *회원 유형*에서 *서비스 계정*을 선택하세요.
5. 서비스 계정의 이름을 입력하세요.

6. JWT 인증을 사용하려면 *개인 키 JWT 인증 사용*을 선택하고 공개 RSA 키 또는 인증서를 업로드하세요. 클라이언트 ID와 시크릿을 사용하는 경우 이 단계를 건너뛰세요.

   귀하의 X.509 인증서. PEM, CRT 또는 CER 형식이어야 합니다.

   a. 인증서 만료 알림을 설정하세요. 7일 또는 30일 중에서 선택하세요. 만료 알림은 슈퍼 관리자 또는 조직 관리자 역할을 가진 사용자에게 이메일로 전송되고 콘솔에 표시됩니다.

7. 조직, 폴더 또는 프로젝트 선택 섹션을 사용하여 멤버에게 권한이 부여되어야 하는 리소스 계층 수준을 선택합니다.

   다음 사항에 유의하세요.

   - 권한이 있는 폴더와 프로젝트에서만 선택할 수 있습니다.
   - 조직이나 폴더를 선택하면 구성원에게 해당 조직의 모든 내용에 대한 권한이 부여됩니다.
   - 조직 관리자 역할은 조직 수준에서만 할당할 수 있습니다.

8. 범주를 선택한 다음, 선택한 조직, 폴더 또는 프로젝트의 리소스에 대한 권한을 구성원에게 부여할 역할(Role)을 선택하십시오.

   "액세스 역할에 대해 알아보세요" .

9. 더 많은 폴더, 프로젝트 또는 역할에 대한 액세스 권한을 부여하려면 *역할 추가*를 선택하고 폴더, 프로젝트 또는 역할 범주를 선택한 다음 역할을 선택하세요.
10. JWT 인증을 사용하지 않기로 선택한 경우 클라이언트 ID와 클라이언트 비밀번호를 다운로드하거나 복사하세요.

    콘솔에는 클라이언트 비밀 키가 한 번만 표시됩니다. 안전하게 복사해 두세요. 나중에 분실하더라도 다시 만들 수 있습니다.

11. JWT 인증을 선택한 경우 클라이언트 ID와 JWT 대상 그룹을 다운로드하거나 복사하십시오. 콘솔에는 이 정보가 한 번만 표시되며, 이후에는 다시 불러올 수 없습니다.
12. *닫기*를 선택하세요.

조직에 연합 그룹을 추가하세요

ID 공급자(IdP)에서 페더레이션 그룹을 조직에 추가하고 하나 이상의 역할을 할당할 수 있습니다. 연합 그룹의 구성원은 콘솔에서 그룹에 할당한 역할을 상속받습니다.

연합 그룹에 역할을 할당하기 전에 다음 사항을 확인하십시오.

- IdP와 콘솔 간의 페더레이션을 설정하십시오. "연합 설정 방법을 알아보세요."
- 해당 그룹은 이미 IdP에 존재해야 하며 콘솔에 대한 앱 액세스 권한이 할당되어 있어야 합니다.
- 해당 그룹에 속한 사용자는 NetApp Console 에 이미 가입되어 있어야 하며 콘솔에서 명시적으로 역할을 할당받아야 합니다. NetApp 조직 뷰어와 같은 최소 액세스 역할을 할당하는 것을 권장합니다.

단계

1. *관리 > ID 및 액세스*를 선택합니다.
2. *회원*을 선택하세요.
3. *멤버 추가*를 선택하세요.
4. *회원 유형*에서 *연합 그룹*을 선택하십시오.

5. 해당 그룹이 소속된 연맹을 선택하세요.
6. *그룹 이름*에는 IdP에 등록된 그룹의 정확한 이름을 입력하세요.
7. 조직, 폴더 또는 프로젝트 선택 섹션을 사용하여 멤버에게 권한이 부여되어야 하는 리소스 계층 수준을 선택합니다.

   다음 사항에 유의하세요.

   - 권한이 있는 폴더와 프로젝트에서만 선택할 수 있습니다.
   - 조직이나 폴더를 선택하면 구성원에게 해당 조직의 모든 내용에 대한 권한이 부여됩니다.
   - 조직 관리자 역할은 조직 수준에서만 할당할 수 있습니다.
8. 범주를 선택한 다음, 선택한 조직, 폴더 또는 프로젝트의 리소스에 대한 권한을 구성원에게 부여할 역할(Role)을 선택하십시오.

   "액세스 역할에 대해 알아보세요" .
9. 더 많은 폴더, 프로젝트 또는 역할에 대한 액세스 권한을 부여하려면 *역할 추가*를 선택하고 폴더, 프로젝트 또는 역할 범주를 선택한 다음 역할을 선택하세요.

관련 정보

- "NetApp Console 에서 ID 및 액세스 관리에 대해 알아보세요"
- "신원 및 액세스 시작하기"
- "NetApp Console 액세스 역할"
- "ID 및 액세스를 위한 API에 대해 알아보세요"

사용자 접근 권한 및 보안 관리

NetApp Console 역할 기반 액세스 제어**(RBAC)**에 대해 알아보세요**.**

역할 기반 액세스 제어(RBAC)를 사용하여 NetApp Console 에 대한 사용자 액세스를 관리하고, 조직, 폴더 또는 프로젝트 수준에서 미리 정의된 역할을 할당할 수 있습니다. 각 역할은 사용자가 할당된 범위 내에서 수행할 수 있는 작업을 정의하는 특정 권한을 부여합니다.

NetApp 최소 권한 원칙에 따라 콘솔 역할을 설계하므로 각 역할에는 해당 작업에 필요한 권한만 포함됩니다. 이러한 접근 방식은 각 구성원에게 필요한 권한만 허용함으로써 보안을 강화합니다.

리소스를 폴더와 프로젝트로 정리한 후에는 조직 구성원에게 특정 폴더 또는 프로젝트에 대한 역할을 할당하여 각자가 자신의 책임만 수행할 수 있도록 하세요.

예를 들어, 특정 프로젝트 수준에 대해 구성원에게 랜섬웨어 복원력 관리자 역할을 할당하여 해당 프로젝트 내의 리소스에 대한 랜섬웨어 복원력 작업을 수행할 수 있도록 허용하되, 조직 전체에 대한 광범위한 액세스 권한은 부여하지 않을 수 있습니다. 이 사용자는 조직 내 여러 프로젝트에 대해 동일한 역할을 부여받을 수 있습니다.

사용자의 책임에 따라 동일한 범위 또는 서로 다른 범위에 대해 여러 역할을 할당할 수 있습니다. 예를 들어, 소규모 조직에서는 동일한 사용자가 조직 차원에서 랜섬웨어 복원력과 백업 및 복구 작업을 모두 관리할 수 있는 반면, 대규모 조직에서는 프로젝트 차원에서 각 역할에 서로 다른 사용자를 할당할 수 있습니다.

콘솔 조직 구성원의 유형

NetApp Console 조직에는 세 가지 유형의 구성원이 있습니다. * 사용자 계정: 리소스를 관리하기 위해 NetApp Console 에 로그인하는 개별 사용자입니다. 사용자를 조직에 추가하려면 먼저 NetApp Console 에 가입해야 합니다. * 서비스 계정: 애플리케이션 또는 서비스가 API를 통해 NetApp Console 과 상호 작용하는 데 사용하는 비인간 계정입니다. 콘솔 조직에 서비스 계정을 직접 추가할 수 있습니다. * 연합 그룹: ID 공급자(IdP)에서 동기화된 그룹으로, 여러 사용자의 액세스 권한을 일괄적으로 관리할 수 있습니다. 연합 그룹 내의 각 사용자는 그룹에 부여된 리소스에 액세스하기 전에 NetApp Console 에 가입하고 액세스 역할을 통해 조직에 추가되어야 합니다.

"조직에 구성원을 추가하는 방법을 알아보세요."

NetApp Console 의 사전 정의된 역할

NetApp Console 조직 구성원에게 할당할 수 있는 사전 정의된 역할이 포함되어 있습니다. 각 역할에는 구성원이 할당된 범위(조직, 폴더 또는 프로젝트) 내에서 수행할 수 있는 작업을 지정하는 권한이 포함되어 있습니다.

NetApp Console 역할은 최소 권한 원칙을 사용하여 구성원이 작업에 필요한 권한만 갖도록 보장하며, 제공하는 액세스 유형에 따라 역할을 분류합니다.

- 플랫폼 역할: 콘솔 관리 권한 제공
- 데이터 서비스 역할: 랜섬웨어 복원력 및 백업/복구와 같은 특정 데이터 서비스를 관리하기 위한 권한을 제공합니다.
- 애플리케이션 역할: 스토리지 관리 및 콘솔 이벤트와 알림 감사에 대한 권한을 제공합니다.

구성원의 책임에 따라 여러 역할을 할당할 수 있습니다. 예를 들어 특정 프로젝트에 대해 멤버에게 랜섬웨어 복원력 관리자 역할과 백업 및 복구 관리자 역할을 모두 할당할 수 있습니다.

"NetApp Console 에서 사용 가능한 사전 정의된 역할에 대해 알아보세요.".

NetApp Console 에서 멤버 액세스를 관리하세요

콘솔 조직에서 구성원 액세스를 관리하세요. 권한을 설정하려면 역할을 할당하세요. 회원이 탈퇴하면 명단에서 삭제합니다.

필수 접근 권한 역할

최고 관리자, 조직 관리자 또는 폴더/프로젝트 관리자(해당 폴더 및 프로젝트를 관리하는 경우에 한함). 링크:reference-iam-predefined-roles.html[접근 권한 역할에 대해 알아보세요].

프로젝트 또는 폴더 단위로 액세스 역할을 할당할 수 있습니다. 예를 들어, 특정 두 프로젝트에 대해 사용자에게 역할을 할당하거나, 폴더 수준에서 역할을 할당하여 해당 폴더 내의 모든 프로젝트에 대해 사용자에게 랜섬웨어 복원력 관리자 역할을 부여할 수 있습니다.

사용자에게 접근 권한을 부여하기 전에 폴더와 프로젝트를 추가하세요. "폴더와 프로젝트를 추가하는 방법을 알아보세요."

NetApp Console 에서 액세스 권한이 부여되는 방식을 이해하십시오.

NetApp Console 역할 기반 접근 제어(RBAC) 모델을 사용하여 사용자 권한을 관리합니다. 구성원에게 개별적으로 또는 연합 그룹을 통해 미리 정의된 역할을 할당할 수 있습니다. 서비스 계정 및 연합 그룹에 역할을 추가하고 할당할 수 있습니다. 각 역할은 구성원이 관련 리소스에서 수행할 수 있는 작업을 정의합니다.

NetApp Console 에서 액세스 권한을 부여할 때 다음 사항에 유의하십시오.

- 모든 사용자는 리소스에 대한 액세스 권한을 부여받기 전에 먼저 NetApp Console 에 가입해야 합니다.
- 콘솔에서 각 사용자가 리소스에 액세스하려면 해당 사용자에게 명시적으로 역할을 할당해야 합니다. 이는 역할이 할당된 연합 그룹의 구성원인 경우에도 마찬가지입니다.
- 콘솔에서 직접 서비스 계정을 추가하고 역할을 할당할 수 있습니다.

역할 상속 사용

NetApp Console 에서 조직, 폴더 또는 프로젝트 수준에서 역할을 할당하면 선택한 범위 내의 모든 리소스가 해당 역할을 자동으로 상속받습니다. 예를 들어, 폴더 수준 역할은 해당 폴더에 포함된 모든 프로젝트에 적용되는 반면, 프로젝트 수준 역할은 해당 프로젝트 내의 모든 리소스에 적용됩니다.

조직 구성원 보기

조직의 리소스 계층 구조에서 다양한 수준에서 멤버에게 할당된 역할을 보면 멤버에게 어떤 리소스와 권한이 제공되는지 파악할 수 있습니다."역할을 사용하여 콘솔 리소스에 대한 액세스를 제어하는 방법을 알아보세요."

단계

1. *관리 > ID 및 액세스*를 선택합니다.
2. *회원*을 선택하세요.

   구성원 표에는 조직의 구성원이 나열됩니다.

3. 회원 페이지에서 테이블의 회원으로 이동하여 다음을 선택합니다. ••• 그런 다음 *세부정보 보기*를 선택하세요.

멤버에게 할당된 역할 보기

현재 그들에게 어떤 역할이 부여되었는지 확인할 수 있습니다.

폴더 또는 프로젝트 관리자 역할이 있는 경우 해당 페이지에는 조직의 모든 구성원이 표시됩니다. 하지만 권한이 있는 폴더와 프로젝트에 대해서만 멤버 권한을 보고 관리할 수 있습니다. "_폴더 또는 프로젝트 관리자_가 완료할 수 있는 작업에 대해 자세히 알아보세요." .

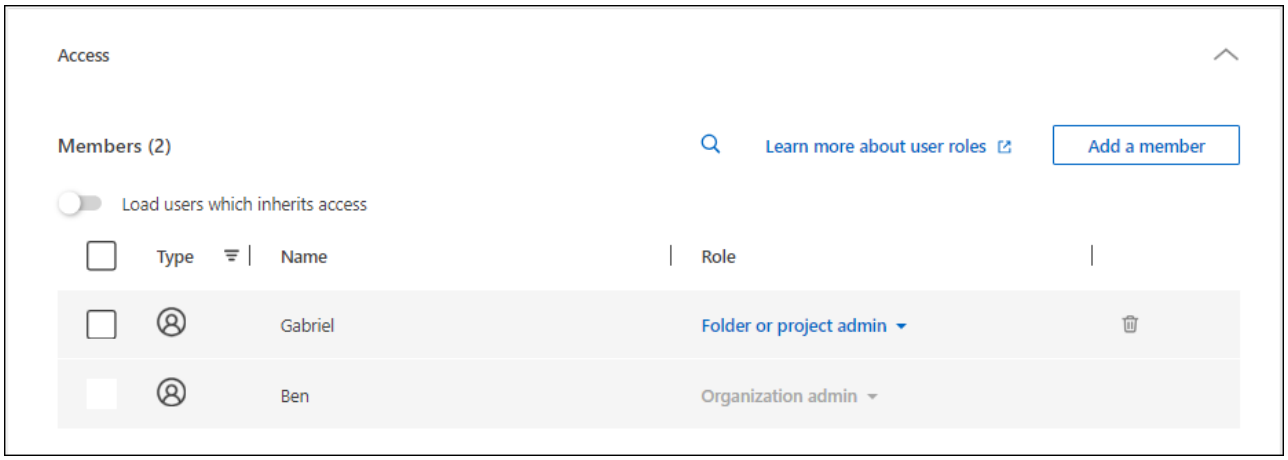
1. 회원 페이지에서 표에 있는 회원을 찾아 선택하세요. ••• 그런 다음 *세부 정보 보기*를 선택하세요.
2. 표에서 멤버에게 할당된 역할을 보고 싶은 조직, 폴더 또는 프로젝트에 해당하는 행을 확장하고 역할 열에서 *보기*를 선택합니다.

폴더 또는 프로젝트와 연관된 멤버 보기

특정 폴더 또는 프로젝트에 대한 접근 권한이 있는 구성원을 확인할 수 있습니다.

단계

1. *관리 > ID 및 액세스*를 선택합니다.
2. *조직*을 선택하세요.
3. 조직 페이지에서 표의 프로젝트나 폴더로 이동하여 다음을 선택합니다. ••• 그런 다음 폴더 편집 또는 *프로젝트 편집*을 선택합니다.
   - 폴더나 프로젝트에 접근할 수 있는 멤버를 보려면 *접근*을 선택하세요.



멤버 접근 권한을 할당하거나 수정합니다.

사용자가 NetApp Console 에 가입하면 해당 사용자를 조직에 추가하고 리소스에 대한 액세스 권한을 부여하는 역할을 할당할 수 있습니다. "조직에 구성원을 추가하는 방법을 알아보세요."

필요에 따라 역할을 추가하거나 삭제하여 구성원의 접근 권한을 조정할 수 있습니다.

멤버에게 액세스 역할 추가

일반적으로 조직에 구성원을 추가할 때 역할을 할당하지만, 역할을 제거하거나 추가하여 언제든지 역할을 업데이트할 수 있습니다.

사용자에게 조직, 폴더 또는 프로젝트에 대한 액세스 역할을 할당할 수 있습니다.

구성원은 동일한 프로젝트 내에서 또는 서로 다른 프로젝트에서 여러 역할을 맡을 수 있습니다. 예를 들어, 소규모 조직에서는 사용 가능한 모든 접근 권한을 동일한 사용자에게 할당할 수 있는 반면, 대규모 조직에서는 사용자가 보다 전문화된 작업을 수행하도록 할 수 있습니다. 또는 조직 차원에서 한 사용자에게 랜섬웨어 복원력 관리자 역할을 부여할 수도 있습니다. 이 예시에서 사용자는 조직 내 모든 프로젝트에 대해 랜섬웨어 복원력 작업을 수행할 수 있습니다.

액세스 역할 전략은 NetApp 리소스를 구성한 방식과 일치해야 합니다.

단계

1. *관리 > ID 및 액세스*를 선택합니다.
2. *회원*을 선택하세요.
3. 사용자, 서비스 계정, 또는 연합 그룹 탭 중 하나를 선택하세요.
4. 작업 메뉴를 선택하세요 ••• 역할을 할당하려는 구성원 옆에 있는 *역할 추가*를 선택합니다.
5. 역할을 추가하려면 대화 상자의 단계를 완료하세요.
   - 조직, 폴더 또는 프로젝트 선택: 멤버에게 권한이 부여되어야 하는 리소스 계층 수준을 선택합니다.

     조직이나 폴더를 선택하면 해당 구성원은 해당 조직이나 폴더 내에 있는 모든 항목에 대한 권한을 갖게 됩니다.
   - 카테고리 선택: 역할 카테고리를 선택하세요. "액세스 역할에 대해 알아보세요" .
   - 역할 선택: 선택한 조직, 폴더 또는 프로젝트와 관련된 리소스에 대한 권한을 멤버에게 제공하는 역할을 선택합니다.
   - 역할 추가: 조직 내 추가 폴더나 프로젝트에 대한 액세스 권한을 제공하려면 *역할 추가*를 선택하고 다른

폴더나 프로젝트 또는 역할 범주를 지정한 다음 역할 범주와 해당 역할을 선택합니다.

6. *새로운 역할 추가*를 선택하세요.

멤버의 할당된 역할 변경

멤버의 역할을 변경하여 접근 권한을 업데이트하세요.

사용자에게는 최소한 하나의 역할이 할당되어야 합니다. 사용자에게서 모든 역할을 제거할 수는 없습니다. 모든 역할을 제거해야 하는 경우 조직에서 해당 사용자를 삭제해야 합니다.

단계

1. *관리 > ID 및 액세스*를 선택합니다.
2. *회원*을 선택하세요.
3. 사용자, 서비스 계정, 또는 연합 그룹 탭 중 하나를 선택하세요.
4. 회원 페이지에서 테이블의 회원으로 이동하여 다음을 선택합니다. ••• 그런 다음 *세부정보 보기*를 선택하세요.
5. 표에서 멤버에게 할당된 역할을 변경하려는 조직, 폴더 또는 프로젝트에 해당하는 행을 확장하고 역할 열에서 *보기*를 선택하여 이 멤버에게 할당된 역할을 확인합니다.
6. 멤버의 기존 역할을 변경하거나 역할을 제거할 수 있습니다.
   a. 멤버의 역할을 변경하려면 변경하려는 역할 옆에 있는 *변경*을 선택하세요. 동일한 역할 범주 내에서만 역할을 변경할 수 있습니다. 예를 들어, 한 데이터 서비스 역할에서 다른 역할로 변경할 수 있습니다. 변경 사항을 확인하세요.
   b. 멤버의 역할을 해제하려면 다음을 선택하세요. 역할 옆에 있는 버튼을 클릭하면 해당 멤버에게서 해당 역할을 제거할 수 있습니다. 삭제를 확인하라는 메시지가 표시됩니다.

조직에서 구성원 제거

구성원이 조직을 떠나면 명단에서 제외하세요.

멤버를 제거하면 시스템에서 해당 멤버의 콘솔 권한은 취소되지만 콘솔 및 NetApp 지원 사이트 계정은 유지됩니다.

연합 회원

- 페더레이션된 사용자는 IdP에서 제거되면 NetApp Console 에 대한 액세스 권한을 자동으로 잃게 됩니다. 하지만 멤버 목록을 최신 상태로 유지하려면 콘솔 조직에서 해당 사용자를 제거해야 합니다.
- IdP에서 페더레이션 그룹에서 사용자를 제거하면 해당 그룹과 연결된 콘솔 액세스 권한을 잃게 됩니다. 하지만 콘솔에서 명시적으로 할당된 역할과 관련된 접근 권한은 여전히 유지됩니다.

단계

1. *관리 > ID 및 액세스*를 선택합니다.
2. *회원*을 선택하세요.
3. 사용자, 서비스 계정, 또는 연합 그룹 탭 중 하나를 선택하세요.
4. 회원 페이지에서 테이블의 회원으로 이동하여 다음을 선택합니다. ••• 그런 다음 *사용자 삭제*를 선택하세요.
5. 조직에서 해당 구성원을 제거할 것인지 확인하세요.

멤버 보안 설정을 관리하여 NetApp Console 조직에 대한 사용자 액세스를 보호하십시오. 사용자 암호를 재설정하고, 다단계 인증(MFA)을 관리하고, 서비스 계정 자격 증명을 다시 생성할 수 있습니다.

필수 접근 권한 역할

최고 관리자, 조직 관리자 또는 폴더/프로젝트 관리자(해당 폴더 및 프로젝트를 관리하는 경우에 한함). 링크:reference-iam-predefined-roles.html[접근 권한 역할에 대해 알아보세요].

사용자 비밀번호 재설정 (로컬 사용자만 해당)

조직 관리자는 로컬 사용자의 비밀번호를 재설정할 수 없습니다. 하지만 사용자에게 직접 비밀번호를 재설정하도록 안내할 수는 있습니다.

콘솔 로그인 페이지에서 *비밀번호를 잊으셨습니까?*를 선택하여 비밀번호를 재설정하도록 사용자에게 안내합니다.

이 옵션은 연합 조직의 사용자에게는 제공되지 않습니다.

사용자의 다중 인증 요소(MFA) 관리

사용자가 MFA 장치에 대한 액세스 권한을 잃은 경우 MFA 구성을 제거하거나 비활성화할 수 있습니다.

다중 요소 인증은 로컬 사용자에게만 제공됩니다. 페더레이션 사용자는 MFA를 활성화할 수 없습니다.

사용자는 MFA를 제거한 후 로그인할 때 다시 설정해야 합니다. 사용자가 일시적으로 MFA 장치에 접근할 수 없게 된 경우, 저장된 복구 코드를 사용하여 로그인할 수 있습니다.

복구 코드가 없는 경우 MFA를 일시적으로 비활성화하여 로그인을 허용합니다. 사용자의 MFA를 비활성화하면 8시간 동안만 비활성화되고 그 후 자동으로 다시 활성화됩니다. 사용자는 해당 기간 동안 MFA 없이 한 번만 로그인할 수 있습니다. 8시간이 지나면 사용자는 MFA를 사용하여 로그인해야 합니다.

사용자의 다중 요소 인증을 관리하려면 영향을 받는 사용자와 동일한 도메인에 이메일 주소가 있어야 합니다.

단계

1. *관리 > ID 및 액세스*를 선택합니다.
2. *회원*을 선택하세요.

   구성원 표에는 조직의 구성원이 나열됩니다.

3. 회원 페이지에서 테이블의 회원으로 이동하여 다음을 선택합니다. ••• 그런 다음 *다중 인증 관리*를 선택하세요.
4. 사용자의 MFA 구성을 제거할지 또는 비활성화할지 선택합니다.

서비스 계정의 자격 증명을 다시 만듭니다.

서비스 자격 증명을 분실했거나 업데이트해야 하는 경우 새 자격 증명을 만들 수 있습니다.

새 자격 증명을 생성하면 이전 자격 증명이 삭제됩니다. 기존 계정 정보는 사용할 수 없습니다.

단계

1. *관리 > ID 및 액세스*를 선택합니다.
2. *회원*을 선택하세요.
3. 멤버 테이블에서 서비스 계정으로 이동하여 다음을 선택합니다. ••• 그런 다음 *비밀 다시 만들기*를 선택하세요.
4. *다시 만들기*를 선택하세요.
5. 클라이언트 ID와 클라이언트 비밀번호를 다운로드하거나 복사하세요.

   콘솔에는 클라이언트 비밀 키가 한 번만 표시됩니다. 파일을 복사하거나 다운로드하여 안전한 곳에 보관하십시오.

NetApp Console 액세스 역할

NetApp Console 액세스 역할에 대해 알아보세요

NetApp Console 의 IAM(ID 및 액세스 관리)은 리소스 계층의 다양한 수준에서 조직 구성원에게 할당할 수 있는 미리 정의된 역할을 제공합니다. 이러한 역할을 할당하기 전에 각 역할에 포함된 권한을 이해해야 합니다. 역할은 플랫폼, 애플리케이션, 데이터 서비스라는 범주로 나뉩니다.

플랫폼 역할

플랫폼 역할은 역할 할당 및 사용자 관리를 포함한 NetApp Console 관리 권한을 부여합니다. 콘솔에는 여러 가지 플랫폼 역할이 있습니다.

플랫폼 역할	책임
"조직 관리자"	사용자에게 조직 내의 모든 프로젝트와 폴더에 대한 제한 없는 액세스를 허용하고, 모든 프로젝트나 폴더에 멤버를 추가하고, 명시적인 역할이 지정되지 않은 모든 작업을 수행하고 모든 데이터 서비스를 사용할 수 있도록 허용합니다. 이 역할을 가진 사용자는 폴더와 프로젝트를 만들고, 역할을 할당하고, 사용자를 추가하고, 적절한 자격 증명이 있는 경우 시스템을 관리하여 조직을 관리합니다. 이는 콘솔 에이전트를 생성할 수 있는 유일한 액세스 역할입니다.
"폴더 또는 프로젝트 관리자"	사용자에게 할당된 프로젝트와 폴더에 대한 제한 없는 액세스를 허용합니다. 자신이 관리하는 폴더나 프로젝트에 멤버를 추가할 수 있고, 할당된 폴더나 프로젝트 내의 리소스에 대한 모든 작업을 수행하고 모든 데이터 서비스나 애플리케이션을 사용할 수 있습니다. 폴더 또는 프로젝트 관리자는 콘솔 에이전트를 생성할 수 없습니다.
"연방 관리자"	사용자가 콘솔을 사용하여 페더레이션을 만들고 관리할 수 있으며, 이를 통해 SSO(Single Sign-On)가 가능합니다.
"연방 뷰어"	사용자가 콘솔을 사용하여 기존 페더레이션을 볼 수 있도록 합니다. 연합을 생성하거나 관리할 수 없습니다.
"파트너십 관리자"	사용자가 파트너십을 만들고 관리할 수 있습니다.
"파트너십 뷰어"	사용자가 기존 파트너십을 볼 수 있도록 합니다. 파트너십을 생성하거나 관리할 수 없습니다.
"슈퍼 관리자"	사용자에게 관리자 역할의 하위 집합을 제공합니다. 이 역할은 여러 사용자에게 콘솔 책임을 분산할 필요가 없는 소규모 조직을 위해 설계되었습니다.

플랫폼 역할	책임
"슈퍼 뷰어"	사용자에게 하위 집합의 뷰어 역할을 제공합니다. 이 역할은 여러 사용자에게 콘솔 책임을 분산할 필요가 없는 소규모 조직을 위해 설계되었습니다.

애플리케이션 역할

다음은 애플리케이션 카테고리의 역할 목록입니다. 각 역할은 지정된 범위 내에서 특정 권한을 부여합니다. 필요한 애플리케이션이나 플랫폼 역할이 없는 사용자는 해당 애플리케이션에 액세스할 수 없습니다.

신청 역할	책임
"Google Cloud NetApp Volumes 관리자"	Google Cloud NetApp Volumes 역할이 있는 사용자는 Google Cloud NetApp Volumes 검색하고 관리할 수 있습니다.
"Google Cloud NetApp Volumes 뷰어"	Google Cloud NetApp Volumes 사용자 역할이 있는 사용자는 Google Cloud NetApp Volumes 볼 수 있습니다.
"Keystone 관리자"	Keystone 관리자 역할이 있는 사용자는 서비스 요청을 생성할 수 있습니다. 사용자가 액세스하는 Keystone 테넌트 내에서 사용량, 리소스 및 관리자 세부 정보를 모니터링하고 볼 수 있습니다.
"Keystone 뷰어"	Keystone 뷰어 역할이 있는 사용자는 서비스 요청을 생성할 수 없습니다. 사용자가 액세스하는 Keystone 테넌트 내에서 소비량, 자산 및 관리 정보를 모니터링하고 볼 수 있습니다.
ONTAP Mediator 설정 역할	ONTAP Mediator 설정 역할이 있는 서비스 계정은 서비스 요청을 생성할 수 있습니다. 이 역할은 서비스 계정에서 인스턴스를 구성하는 데 필요합니다 ."ONTAP 클라우드 중재자" .
"운영 지원 분석가"	알림 및 모니터링 도구에 대한 액세스를 제공하고 지원 사례를 입력 및 관리하는 기능을 제공합니다.
"스토리지 관리자"	스토리지 상태 및 거버넌스 기능을 관리하고, 스토리지 리소스를 검색하고, 기존 시스템을 수정 및 삭제합니다.
"스토리지 뷰어"	저장소 상태 및 거버넌스 기능을 확인하고, 이전에 검색된 저장소 리소스를 확인합니다. 기존 스토리지 시스템을 검색, 수정 또는 삭제할 수 없습니다.
"시스템 건강 전문가"	저장소 및 상태, 거버넌스 기능을 관리합니다. 저장소 관리자의 모든 권한은 기존 시스템을 수정하거나 삭제할 수 없습니다.

데이터 서비스 역할

다음은 데이터 서비스 범주의 역할 목록입니다. 각 역할은 지정된 범위 내에서 특정 권한을 부여합니다. 필요한 데이터 서비스 역할이나 플랫폼 역할이 없는 사용자는 데이터 서비스에 액세스할 수 없습니다.

데이터 서비스 역할	책임
"백업 및 복구 슈퍼 관리자"	NetApp Backup and Recovery 에서 모든 작업을 수행합니다.
"백업 및 복구 관리자"	로컬 스냅샷에 백업을 수행하고, 보조 저장소에 복제하고, 개체 저장소에 백업합니다.
"백업 및 복구 복원 관리자"	백업 및 복구에서 작업 부하를 복원합니다.
"백업 및 복구 클론 관리자"	백업 및 복구에서 애플리케이션과 데이터를 복제합니다.
"백업 및 복구 뷰어"	백업 및 복구 정보를 확인합니다.

데이터 서비스 역할	책임
"재해 복구 관리자"	NetApp Disaster Recovery 서비스에서 모든 작업을 수행합니다.
"재해 복구 장애 조치 관리자"	장애 조치 및 마이그레이션을 수행합니다.
"재해 복구 애플리케이션 관리자"	복제 계획을 만들고, 복제 계획을 변경하고, 테스트 장애 조치를 시작합니다.
"재해 복구 뷰어"	정보만 보기.
분류 뷰어	사용자가 NetApp Data Classification 검사 결과를 볼 수 있습니다. 이 역할이 있는 사용자는 규정 준수 정보를 보고 액세스 권한이 있는 리소스에 대한 보고서를 생성할 수 있습니다. 이러한 사용자는 볼륨, 버킷 또는 데이터베이스 스키마의 스캐닝을 활성화하거나 비활성화할 수 없습니다. 분류에는 관리자 역할이 없습니다.
"랜섬웨어 복원력 관리자"	NetApp Ransomware Resilience 의 보호, 알림, 복구, 설정 및 보고서 탭에서 작업을 관리합니다.
"랜섬웨어 복원력 뷰어"	Ransomware Resilience에서 작업 부하 데이터를 보고, 알림 데이터를 보고, 복구 데이터를 다운로드하고, 보고서를 다운로드하세요.
"랜섬웨어 복원력 사용자 행동 관리자"	Ransomware Resilience에서 의심스러운 사용자 동작 탐지, 알림 및 모니터링을 구성, 관리하고 확인하세요.
"랜섬웨어 복원력 사용자 동작 뷰어"	랜섬웨어 복원력에서 의심스러운 사용자 행동 알림과 통찰력을 확인하세요.
SnapCenter 관리자	NetApp Backup and Recovery 사용하여 온프레미스 ONTAP 클러스터의 스냅샷을 애플리케이션에 백업하는 기능을 제공합니다. 이 역할이 있는 멤버는 다음 작업을 완료할 수 있습니다. * 백업 및 복구 > 애플리케이션에서 모든 작업을 완료합니다. * 권한이 있는 프로젝트 및 폴더의 모든 시스템을 관리합니다. * 모든 NetApp Console 서비스를 사용합니다. SnapCenter 에는 뷰어 역할이 없습니다.

관련 링크

- "NetApp Console ID 및 액세스 관리에 대해 알아보세요"
- "NetApp Console IAM 시작하기"
- "NetApp Console 멤버 및 해당 권한 관리"
- "NetApp Console IAM에 대한 API에 대해 알아보세요"

NetApp Console 플랫폼 액세스 역할

사용자에게 플랫폼 역할을 할당하여 NetApp Console 관리, 역할 할당, 사용자 추가, 콘솔 에이전트 생성, 페더레이션 관리 권한을 부여합니다.

대규모 다국적 기업의 조직 역할에 대한 예

XYZ Corporation은 북미, 유럽, 아시아 태평양 등 지역별로 데이터 저장소 액세스를 구성하여 중앙 집중식 감독을 통해 지역적 제어를 제공합니다.

XYZ Corporation 콘솔의 *조직 관리자*는 각 지역에 대한 초기 조직과 별도 폴더를 만듭니다. 각 지역의 *폴더 또는 프로젝트 관리자*는 해당 지역의 폴더 내에서 프로젝트(관련 리소스 포함)를 구성합니다.

폴더 또는 프로젝트 관리자 역할을 맡은 지역 관리자는 리소스와 사용자를 추가하여 폴더를 적극적으로 관리합니다. 이러한 지역 관리자는 자신이 관리하는 폴더와 프로젝트를 추가, 제거 또는 이름을 바꿀 수도 있습니다. *조직 관리자*는 모든 새 리소스에 대한 권한을 상속받아 조직 전체의 저장소 사용량을 파악할 수 있습니다.

동일한 조직 내에서 한 명의 사용자에게 회사 IdP와의 조직 연합을 관리하는 연합 관리자 역할이 할당됩니다. 이 사용자는 연합 조직을 추가하거나 제거할 수 있지만, 조직 내의 사용자나 리소스를 관리할 수는 없습니다. 조직 관리자 *는 사용자에게 *연합 뷰어 역할을 할당하여 연합 상태를 확인하고 연합 조직을 볼 수 있도록 합니다.

다음 표는 각 콘솔 플랫폼 역할이 수행할 수 있는 작업을 나타냅니다.

조직 관리 역할

일	조직 관리자	폴더 또는 프로젝트 관리자
에이전트 생성	예	아니요
콘솔에서 시스템 생성, 수정 또는 삭제(시스템 추가 또는 검색)	예	예
폴더 및 프로젝트 생성, 삭제 포함	예	아니요
기존 폴더 및 프로젝트 이름 바꾸기	예	예
역할 할당 및 사용자 추가	예	예
리소스를 폴더 및 프로젝트와 연결	예	예
폴더 및 프로젝트와 에이전트 연결	예	아니요
폴더 및 프로젝트에서 에이전트 제거	예	아니요
에이전트 관리(인증서, 설정 등 편집)	예	아니요
관리 > 자격 증명에서 자격 증명을 관리합니다.	예	예
연합을 생성, 관리 및 보기	예	아니요
콘솔을 통해 지원을 등록하고 사례를 제출하세요.	예	예
명시적 액세스 역할과 연결되지 않은 데이터 서비스를 사용하세요.	예	예
감사 페이지 및 알림 보기	예	예

연방 역할

일	연방 관리자	연방 뷰어
연방을 만드세요	예	아니요
도메인 확인	예	아니요
페더레이션에 도메인 추가	예	아니요
페더레이션 비활성화 및 삭제	예	아니요
테스트 연합	예	아니요
연합 및 세부 정보 보기	예	예

파트너십 역할

일	파트너십 관리자	파트너십 뷰어
파트너십을 만들 수 있습니다	예	아니요

일	파트너십 관리자	파트너십 뷰어
파트너 멤버에게 역할 할당	예	아니요
파트너십에 멤버를 추가할 수 있습니다	예	아니요
조직 파트너십 세부 정보를 볼 수 있습니다.	예	예

슈퍼 관리자 및 뷰어 역할

슈퍼 관리자 역할은 콘솔 기능, 저장소 및 데이터 서비스를 관리할 수 있는 전체 액세스 권한을 제공합니다. 이 역할은 행정과 거버넌스를 감독하는 사람에게 적합합니다. 이와 대조적으로, 슈퍼 뷰어 역할은 읽기 전용 액세스를 제공하므로 변경하지 않고도 가시성이 필요한 감사자나 이해 관계자에게 이상적입니다.

조직에서는 보안 위험을 최소화하고 최소 권한 원칙을 준수하기 위해 슈퍼 관리자 권한을 아껴서 사용해야 합니다. 대부분의 조직에서는 위험을 줄이고 감사 가능성을 높이기 위해 필요한 권한만 부여한 세분화된 역할을 할당해야 합니다.

슈퍼 역할에 대한 예

ABC Corporation은 데이터 서비스와 스토리지 관리를 위해 NetApp Console 활용하는 5명으로 구성된 소규모 팀을 보유하고 있습니다. 여러 역할을 분산하는 대신, 사용자 관리 및 리소스 구성을 포함한 모든 관리 작업을 처리하는 두 명의 상임 팀원에게 슈퍼 관리자 역할을 할당합니다. 나머지 3명의 팀원에게는 슈퍼 뷰어 역할이 할당되어 설정을 수정하지 않고도 저장소 상태와 데이터 서비스 상태를 모니터링할 수 있습니다.

역할	상속된 역할
슈퍼 관리자	• 조직 관리자 • 폴더 또는 프로젝트 관리자 • 연방 관리자 • 파트너십 관리자 • 랜섬웨어 복원력 관리자 • 재해 복구 관리 • 백업 슈퍼 관리자 • 스토리지 관리자 • Keystone 관리자 • Google Cloud NetApp Volumes 관리자

역할	상속된 역할
슈퍼 뷰어	• 조직 뷰어 • 연방 뷰어 • 파트너십 뷰어 • 랜섬웨어 복원력 뷰어 • 재해 복구 뷰어 • 백업 뷰어 • 스토리지 뷰어 • Keystone 뷰어 • Google Cloud NetApp Volumes 뷰어

애플리케이션 역할

NetApp Console 의 Google Cloud NetApp Volumes 역할

NetApp Console 에서 Google Cloud NetApp Volumes 에 대한 액세스 권한을 제공하기 위해 사용자에게 다음 역할을 할당할 수 있습니다.

Google Cloud NetApp Volumes 다음 역할을 사용합니다.

- * Google Cloud NetApp Volumes 관리자*: 콘솔에서 Google Cloud NetApp Volumes 검색하고 관리합니다.
- * Google Cloud NetApp Volumes 뷰어*: 콘솔에서 Google Cloud NetApp Volumes 확인합니다.

NetApp Console 의 Keystone 액세스 역할

Keystone 역할은 Keystone 대시보드에 대한 액세스를 제공하고 사용자가 Keystone 구독을 보고 관리할 수 있도록 합니다. Keystone 역할에는 Keystone 관리자와 Keystone 뷰어라는 두 가지가 있습니다. 두 역할의 주요 차이점은 Keystone 에서 수행할 수 있는 작업입니다. Keystone 관리자 역할은 서비스 요청을 만들거나 구독을 수정할 수 있는 유일한 역할입니다.

NetApp Console 의 Keystone 역할에 대한 예

XYZ Corporation에는 Keystone 구독 정보를 확인하는 여러 부서의 스토리지 엔지니어가 4명 있습니다. 이러한 모든 사용자는 Keystone 구독을 모니터링해야 하지만, 서비스 요청을 할 수 있는 사람은 팀 리더뿐입니다. 팀원 3명에게는 * Keystone 뷰어* 역할이 부여되고, 팀 리더에게는 * Keystone 관리자* 역할이 부여되어 회사의 서비스 요청에 대한 통제 지점이 마련됩니다.

다음 표는 각 Keystone 역할이 수행할 수 있는 작업을 나타냅니다.

특징과 동작	Keystone 관리자	Keystone 뷰어
다음 탭을 확인하세요: 구독, 자산, 모니터 및 관리	예	예
* Keystone 구독 페이지*:		

특징과 동작	**Keystone** 관리자	**Keystone** 뷰어
구독 보기	예	예
구독 수정 또는 갱신	예	아니요
* Keystone 자산 페이지*:		
자산 보기	예	예
자산 관리	예	아니요
* Keystone 알림 페이지*:		
알림 보기	예	예
알림 관리	예	아니요
나 자신에 대한 알림 만들기	예	예
* Licenses and subscriptions*:		
라이센스 및 구독을 볼 수 있습니다	예	예
* Keystone 보고서 페이지*:		
보고서 다운로드	예	예
보고서 관리	예	예
자신을 위한 보고서 만들기	예	예
서비스 요청:		
서비스 요청 생성	예	아니요
조직 내 모든 사용자가 생성한 서비스 요청 보기	예	예

NetApp Console 에 대한 운영 지원 분석가 액세스 역할

운영 지원 분석가 역할을 사용자에게 할당하면 해당 사용자에게 알림 및 모니터링 기능에 대한 접근 권한을 부여할 수 있습니다. 이 역할을 가진 사용자는 지원 사례를 열 수도 있습니다.

운영 지원 분석가

일	수행할 수 있습니다
설정 > 자격 증명에서 자신의 사용자 자격 증명을 관리하세요.	예

일	수행할 수 있습니다
발견된 리소스 보기	예
콘솔을 통해 지원을 등록하고 사례를 제출하세요.	예
감사 페이지 및 알림 보기	예
알림 보기, 다운로드 및 구성	예

NetApp Console 의 스토리지 액세스 역할

NetApp Console 에서 스토리지 관리 기능에 액세스할 수 있도록 사용자에게 다음 역할을 할당할 수 있습니다. 사용자에게 저장소를 관리하는 관리자 역할이나 모니터링을 위한 뷰어 역할을 할당할 수 있습니다.

이러한 역할은 NetApp Console 파트너십 API에서 사용할 수 없습니다.

관리자는 다음과 같은 스토리지 리소스 및 기능에 대해 사용자에게 스토리지 역할을 할당할 수 있습니다.

저장 리소스:

- 온프레미스 ONTAP 클러스터
- StorageGRID
- E-시리즈

콘솔 서비스 및 기능:

- 디지털 어드바이저
- 소프트웨어 업데이트
- 수명주기 계획
- 지속 가능성

NetApp Console 의 스토리지 역할에 대한 예

다국적 기업인 XYZ Corporation은 스토리지 엔지니어와 스토리지 관리자로 구성된 대규모 팀을 보유하고 있습니다. 이를 통해 팀은 사용자 관리, 에이전트 생성, 라이선스 관리와 같은 핵심 콘솔 작업에 대한 액세스를 제한하는 동시에 해당 지역의 스토리지 자산을 관리할 수 있습니다.

12명으로 구성된 팀 내에서 두 명의 사용자에게 저장소 뷰어 역할이 부여됩니다. 이 역할을 통해 이들은 할당된 콘솔 프로젝트와 연관된 저장 리소스를 모니터링할 수 있습니다. 나머지 9명에게는 소프트웨어 업데이트를 관리하고, 콘솔을 통해 ONTAP 시스템 관리자에 액세스하고, 스토리지 리소스를 검색(시스템 추가)하는 기능이 포함된 스토리지 관리자 역할이 부여됩니다. 팀 내 한 사람에게 시스템 상태 전문가 역할이 부여되어 해당 지역의 스토리지 리소스 상태를 관리할 수 있지만, 시스템을 수정하거나 삭제할 수는 없습니다. 이 사람은 자신에게 할당된 프로젝트의 스토리지 리소스에 대한 소프트웨어 업데이트도 수행할 수 있습니다.

조직에는 사용자 관리, 에이전트 생성, 라이선스 관리를 포함하여 콘솔의 모든 측면을 관리할 수 있는 조직 관리자 역할이 있는 두 명의 추가 사용자가 있으며, 할당된 폴더와 프로젝트에 대한 콘솔 관리 작업을 수행할 수 있는 폴더 또는 프로젝트 관리자 역할이 있는 여러 사용자가 있습니다.

다음 표는 각 저장소 역할이 수행하는 작업을 보여줍니다.

특징과 동작	스토리지 관리자	시스템 건강 전문가	스토리지 뷰어
저장 관리:			
새로운 리소스 발견(시스템 생성)	예	예	아니요
발견된 시스템 보기	예	예	아니요
콘솔에서 시스템 삭제	예	아니요	아니요
시스템 수정	예	아니요	아니요
에이전트 생성	아니요	아니요	아니요
디지털 어드바이저			
모든 페이지 및 기능 보기	예	예	예
* Licenses and subscriptions*			
모든 페이지 및 기능 보기	아니요	아니요	아니요
소프트웨어 업데이트			
랜딩 페이지와 추천 보기	예	예	예
잠재적인 버전 권장 사항과 주요 이점을 검토하세요	예	예	예
클러스터에 대한 업데이트 세부 정보 보기	예	예	예
업데이트 전 점검을 실행하고 업그레이드 계획을 다운로드하세요	예	예	예
소프트웨어 업데이트 설치	예	예	아니요
수명주기 계획			
용량 계획 상태 검토	예	예	예
다음 작업(모범 사례, 계층)을 선택하세요	예	아니요	아니요
콜드 데이터를 클라우드 스토리지로 계층화하고 스토리지를 확보하세요	예	예	아니요
알림 설정	예	예	예
지속가능성			
대시보드 및 권장 사항 보기	예	예	예

특징과 동작	스토리지 관리자	시스템 건강 전문가	스토리지 뷰어
보고서 데이터 다운로드	예	예	예
탄소 감축 비율 편집	예	예	아니요
권장 사항 수정	예	예	아니요
권장 사항을 연기하다	예	예	아니요
시스템 관리자 접근			
자격 증명을 입력할 수 있습니다	예	예	아니요
신임장			
사용자 자격 증명	예	예	아니요

데이터 서비스 역할

NetApp Console 의 NetApp Backup and Recovery 역할

콘솔 내에서 NetApp Backup and Recovery 에 대한 액세스 권한을 제공하기 위해 사용자에게 다음 역할을 할당할 수 있습니다. 백업 및 복구 역할을 사용하면 조직 내에서 수행해야 하는 작업에 맞는 역할을 사용자에게 할당할 수 있는 유연성이 제공됩니다. 역할을 할당하는 방법은 귀하의 사업과 스토리지 관리 관행에 따라 달라집니다.

이 서비스는 NetApp Backup and Recovery 에 특정한 다음 역할을 사용합니다.

- 백업 및 복구 슈퍼 관리자: NetApp Backup and Recovery 에서 모든 작업을 수행합니다.
- 백업 및 복구 백업 관리자: NetApp Backup and Recovery 에서 로컬 스냅샷으로 백업을 수행하고, 보조 스토리지로 복제하고, 개체 스토리지로 백업 작업을 수행합니다.
- 백업 및 복구 복원 관리자: NetApp Backup and Recovery 사용하여 워크로드를 복원합니다.
- 백업 및 복구 복제 관리자: NetApp Backup and Recovery 사용하여 애플리케이션과 데이터를 복제합니다.
- 백업 및 복구 뷰어: NetApp Backup and Recovery 에서 정보를 볼 수 있지만, 어떤 작업도 수행할 수 없습니다.

모든 NetApp Console 액세스 역할에 대한 자세한 내용은 다음을 참조하세요. "콘솔 설정 및 관리 문서" .

일반적인 작업에 사용되는 역할

다음 표는 각 NetApp Backup and Recovery 역할이 모든 워크로드에 대해 수행할 수 있는 작업을 나타냅니다.

특징과 동작	백업 및 복구 슈퍼 관리자	백업 및 복구 백업 관리자	백업 및 복구 복원 관리자	백업 및 복구 클론 관리자	백업 및 복구 뷰어
호스트 추가, 편집 또는 삭제	예	아니요	아니요	아니요	아니요

특징과 동작	백업 및 복구 슈퍼 관리자	백업 및 복구 백업 관리자	백업 및 복구 복원 관리자	백업 및 복구 클론 관리자	백업 및 복구 뷰어
플러그인 설치	예	아니요	아니요	아니요	아니요
자격 증명 추가(호스트, 인스턴스, vCenter)	예	아니요	아니요	아니요	아니요
대시보드 및 모든 탭 보기	예	예	예	예	예
무료 체험 시작	예	아니요	아니요	아니요	아니요
워크로드 검색 시작	아니요	예	예	예	아니요
라이센스 정보 보기	예	예	예	예	예
라이센스 활성화	예	아니요	아니요	아니요	아니요
호스트 보기	예	예	예	예	예
일정:					
일정 활성화	예	예	예	예	아니요
일정을 중단하다	예	예	예	예	아니요
정책 및 보호:					
보호 계획 보기	예	예	예	예	예
보호 계획 생성, 수정 또는 삭제	예	예	아니요	아니요	아니요
작업 부하 복원	예	아니요	예	아니요	아니요
클론 생성, 분할 또는 삭제	예	아니요	아니요	예	아니요
정책 생성, 수정 또는 삭제	예	예	아니요	아니요	아니요
보고서:					
보고서 보기	예	예	예	예	예
보고서 만들기	예	예	예	예	아니요
보고서 삭제	예	아니요	아니요	아니요	아니요
* SnapCenter 에서 가져오기 및 호스트 관리*:					

특징과 동작	백업 및 복구 슈퍼 관리자	백업 및 복구 백업 관리자	백업 및 복구 복원 관리자	백업 및 복구 클론 관리자	백업 및 복구 뷰어
가져온 SnapCenter 데이터 보기	예	예	예	예	예
SnapCenter 에서 데이터 가져오기	예	예	아니요	아니요	아니요
호스트 관리 (마이그레이션)	예	예	아니요	아니요	아니요
설정 구성:					
로그 디렉토리 구성	예	예	예	아니요	아니요
인스턴스 자격 증명 연결 또는 제거	예	예	예	아니요	아니요
버킷:					
버킷 보기	예	예	예	예	예
버킷 생성, 편집 또는 삭제	예	예	아니요	아니요	아니요

작업별 작업에 사용되는 역할

다음 표는 각 NetApp Backup and Recovery 역할이 특정 작업 부하에 대해 수행할 수 있는 작업을 나타냅니다.

쿠버네티스 워크로드

이 표는 각 NetApp Backup and Recovery 역할이 Kubernetes 워크로드에 대한 특정 작업에 대해 수행할 수 있는 작업을 나타냅니다.

특징과 동작	백업 및 복구 슈퍼 관리자	백업 및 복구 백업 관리자	백업 및 복구 복원 관리자	백업 및 복구 뷰어
클러스터, 네임스페이스, 스토리지 클래스 및 API 리소스 보기	예	예	예	예
새로운 Kubernetes 클러스터 추가	예	예	아니요	아니요
클러스터 구성 업데이트	예	아니요	아니요	아니요
관리에서 클러스터 제거	예	아니요	아니요	아니요
신청서 보기	예	예	예	예
새로운 애플리케이션을 만들고 정의합니다.	예	예	아니요	아니요

특징과 동작	백업 및 복구 슈퍼 관리자	백업 및 복구 백업 관리자	백업 및 복구 복원 관리자	백업 및 복구 뷰어
애플리케이션 구성 업데이트	예	예	아니요	아니요
관리에서 애플리케이션 제거	예	예	아니요	아니요
보호된 리소스 및 백업 상태 보기	예	예	예	예
백업을 생성하고 정책을 사용하여 애플리케이션을 보호합니다.	예	예	아니요	아니요
앱 보호 해제 및 백업 삭제	예	예	아니요	아니요
복구 지점 및 리소스 뷰어 결과 보기	예	예	예	예
복구 지점에서 애플리케이션 복원	예	아니요	예	아니요
Kubernetes 백업 정책 보기	예	예	예	예
Kubernetes 백업 정책 생성	예	예	예	아니요
백업 정책 업데이트	예	예	예	아니요
백업 정책 삭제	예	예	예	아니요
실행 후크 및 후크 소스 보기	예	예	예	예
실행 후크 및 후크 소스 생성	예	예	예	아니요
실행 후크 및 후크 소스 업데이트	예	예	예	아니요
실행 후크 및 후크 소스 삭제	예	예	예	아니요
실행 후크 템플릿 보기	예	예	예	예
실행 후크 템플릿 만들기	예	예	예	아니요
실행 후크 템플릿 업데이트	예	예	예	아니요
실행 후크 템플릿 삭제	예	예	예	아니요
작업 요약 및 분석 대시보드 보기	예	예	예	예

특징과 동작	백업 및 복구 슈퍼 관리자	백업 및 복구 백업 관리자	백업 및 복구 복원 관리자	백업 및 복구 뷰어
StorageGRID 버킷 및 스토리지 대상 보기	예	예	예	예

NetApp Console 의 NetApp Disaster Recovery 역할

콘솔 내에서 NetApp Disaster Recovery 에 대한 액세스 권한을 제공하기 위해 사용자에게 다음 역할을 할당할 수 있습니다. 재해 복구 역할을 통해 조직 내에서 수행해야 하는 작업에 맞는 역할을 사용자에게 할당할 수 있는 유연성이 제공됩니다. 역할을 할당하는 방법은 귀하의 사업과 스토리지 관리 관행에 따라 달라집니다.

재해 복구에는 다음과 같은 역할이 사용됩니다.

- 재해 복구 관리자: 모든 작업을 수행합니다.
- 재해 복구 장애 조치 관리자: 장애 조치 및 마이그레이션을 수행합니다.
- 재해 복구 애플리케이션 관리자: 복제 계획을 만듭니다. 복제 계획을 수정합니다. 테스트 장애 조치를 시작합니다.
- 재해 복구 뷰어: 정보만 봅니다.

다음 표는 각 역할이 수행할 수 있는 작업을 나타냅니다.

특징과 동작	재해 복구 관리	재해 복구 장애 조치 관리자	재해 복구 애플리케이션 관리자	재해 복구 뷰어
대시보드 및 모든 탭 보기	예	예	예	예
무료 체험 시작	예	아니요	아니요	아니요
워크로드 검색 시작	예	아니요	아니요	아니요
라이센스 정보 보기	예	예	예	예
라이센스 활성화	예	아니요	예	아니요
사이트 탭에서:				
사이트 보기	예	예	예	예
사이트 추가, 수정 또는 삭제	예	아니요	아니요	아니요
복제 계획 탭에서:				
복제 계획 보기	예	예	예	예
복제 계획 세부 정보 보기	예	예	예	예

특징과 동작	재해 복구 관리	재해 복구 장애 조치 관리자	재해 복구 애플리케이션 관리자	재해 복구 뷰어
복제 계획을 생성하거나 수정합니다.	예	예	예	아니요
보고서 만들기	예	아니요	아니요	아니요
스냅샷 보기	예	예	예	예
장애 조치 테스트 수행	예	예	예	아니요
장애 조치 수행	예	예	아니요	아니요
장애 복구 수행	예	예	아니요	아니요
마이그레이션 수행	예	예	아니요	아니요
리소스 그룹 탭에서:				
리소스 그룹 보기	예	예	예	예
리소스 그룹 생성, 수정 또는 삭제	예	아니요	예	아니요
작업 모니터링 탭에서:				
채용공고 보기	예	아니요	예	예
작업 취소	예	예	예	아니요

NetApp Console 의 랜섬웨어 복원력 액세스 역할

랜섬웨어 복원력 역할은 사용자에게 NetApp Ransomware Resilience 에 대한 액세스 권한을 제공합니다. 랜섬웨어 복원력은 다음과 같은 역할을 지원합니다.

기준 역할

- 랜섬웨어 복원력 관리자 - 랜섬웨어 복원력 설정 구성, 암호화 경고 조사 및 대응
- 랜섬웨어 복원력 뷰어 - 암호화 사고, 보고서 및 검색 설정 보기

사용자 행동 활동 역할"의심스러운 사용자 활동 감지" 알림은 파일 활동 이벤트와 같은 데이터에 대한 가시성을 제공합니다. 이러한 알림에는 파일 이름과 사용자가 수행한 파일 작업(예: 읽기, 쓰기, 삭제, 이름 바꾸기)이 포함됩니다. 이 데이터의 가시성을 제한하기 위해 이러한 역할을 가진 사용자만 이러한 알림을 관리하거나 볼 수 있습니다.

- 랜섬웨어 복원력 사용자 행동 관리 - 의심스러운 사용자 활동 감지를 활성화하고, 의심스러운 사용자 활동 알림을 조사하고 대응합니다.
- 랜섬웨어 복원력 사용자 동작 뷰어 - 의심스러운 사용자 활동 알림 보기

사용자 동작 역할은 독립된 역할이 아니며, 랜섬웨어 복원력 관리자 또는 뷰어 역할에 추가되도록 설계되었습니다. 자세한 내용은 다음을 참조하세요. 사용자 행동 역할.

각 역할에 대한 자세한 설명은 다음 표를 참조하세요.

기준 역할

다음 표에서는 랜섬웨어 복원력 관리자 및 뷰어 역할에서 사용할 수 있는 작업을 설명합니다.

특징과 동작	랜섬웨어 복원력 관리자	랜섬웨어 복원력 뷰어
대시보드 및 모든 탭 보기	예	예
대시보드에서 권장 사항 상태를 업데이트합니다.	예	아니요
무료 체험 시작	예	아니요
워크로드 검색 시작	예	아니요
워크로드 재발견 시작	예	아니요
보호 탭에서:		
암호화 정책에 대한 보호 계획을 추가, 수정 또는 삭제합니다.	예	아니요
작업 부하 보호	예	아니요
데이터 분류를 통해 민감한 데이터에 대한 노출을 식별하세요	예	아니요
보호 계획 및 세부 정보 목록	예	예
보호 그룹 목록	예	예
보호 그룹 세부 정보 보기	예	예
보호 그룹 생성, 편집 또는 삭제	예	아니요
데이터 다운로드	예	예
알림 탭에서:		
암호화 알림 및 알림 세부 정보 보기	예	예
암호화 사고 상태 편집	예	아니요
복구를 위한 암호화 경고 표시	예	아니요

특징과 동작	랜섬웨어 복원력 관리자	랜섬웨어 복원력 뷰어
암호화 사고 세부 정보 보기	예	예
암호화 사고를 기각하거나 해결합니다.	예	아니요
암호화 이벤트에서 영향을 받은 파일의 전체 목록을 가져옵니다.	예	아니요
암호화 이벤트 알림 데이터 다운로드	예	예
사용자 차단(Workload Security 에이전트 구성 포함)	예	아니요
복구 탭에서:		
암호화 이벤트에서 영향을 받은 파일 다운로드	예	아니요
암호화 이벤트에서 작업 부하 복원	예	아니요
암호화 이벤트에서 복구 데이터 다운로드	예	예
암호화 이벤트에서 보고서 다운로드	예	예
설정 탭에서:		
백업 대상 추가 또는 수정	예	아니요
백업 대상 나열	예	예
연결된 SIEM 대상 보기	예	예
SIEM 대상 추가 또는 수정	예	아니요
준비 훈련 구성	예	아니요
준비 훈련 시작, 재설정 또는 편집	예	아니요
준비 훈련 상태 검토	예	예
검색 구성 업데이트	예	아니요
검색 구성 보기	예	예
보고서 탭에서:		
보고서 다운로드	예	예

사용자 행동 역할

의심스러운 사용자 동작 설정을 구성하고 알림에 대응하려면 사용자에게 랜섬웨어 복원력 사용자 동작 관리자 역할이 있어야 합니다. 의심스러운 사용자 동작 알림만 보려면 사용자에게 랜섬웨어 복원력 사용자 동작 뷰어 역할이 있어야 합니다.

기존 Ransomware Resilience 관리자 또는 뷰어 권한이 있는 사용자에게는 사용자 동작 역할을 부여해야 합니다. "의심스러운 사용자 활동 설정 및 알림" . 예를 들어 랜섬웨어 복원력 관리자 역할이 있는 사용자는 사용자 활동 에이전트를 구성하고 사용자를 차단하거나 차단을 해제하기 위해 랜섬웨어 복원력 사용자 동작 관리자 역할을 받아야 합니다. 랜섬웨어 복원력 사용자 동작 관리자 역할은 랜섬웨어 복원력 뷰어에게 부여되어서는 안 됩니다.

의심스러운 사용자 활동 감지를 활성화하려면 콘솔 조직 관리자 역할이 있어야 합니다.

다음 표에서는 랜섬웨어 복원력 사용자 동작 관리자 및 뷰어 역할에서 사용할 수 있는 작업을 설명합니다.

특징과 동작	랜섬웨어 복원력 사용자 행동 관리자	랜섬웨어 복원력 사용자 동작 뷰어
설정 탭에서:		
사용자 활동 에이전트를 생성, 수정 또는 삭제합니다.	예	아니요
사용자 디렉토리 커넥터 생성 또는 삭제	예	아니요
데이터 수집기 일시 중지 또는 재개	예	아니요
데이터 침해 대비 훈련을 실행하세요	예	아니요
보호 탭에서:		
의심스러운 사용자 동작 정책에 대한 보호 계획을 추가, 수정 또는 삭제합니다.	예	아니요
알림 탭에서:		
사용자 활동 알림 및 알림 세부 정보 보기	예	예
사용자 활동 사고 상태 편집	예	아니요
복구를 위해 사용자 활동 알림을 표시합니다.	예	아니요
사용자 활동 사고 세부 정보 보기	예	예
사용자 활동 사고를 기각하거나 해결합니다.	예	아니요
의심스러운 사용자에 의해 영향을 받은 파일의 전체 목록을 가져옵니다.	예	예
사용자 활동 이벤트 알림 데이터 다운로드	예	예

특징과 동작	랜섬웨어 복원력 사용자 행동 관리자	랜섬웨어 복원력 사용자 동작 뷰어
사용자 차단 또는 차단 해제	예	아니요
복구 탭에서:		
사용자 활동 이벤트에 영향을 받은 파일 다운로드	예	아니요
사용자 활동 이벤트에서 작업 부하 복원	예	아니요
사용자 활동 이벤트에서 복구 데이터 다운로드	예	예
사용자 활동 이벤트에서 보고서 다운로드	예	예

신원 및 액세스 API

조직 및 프로젝트 ID

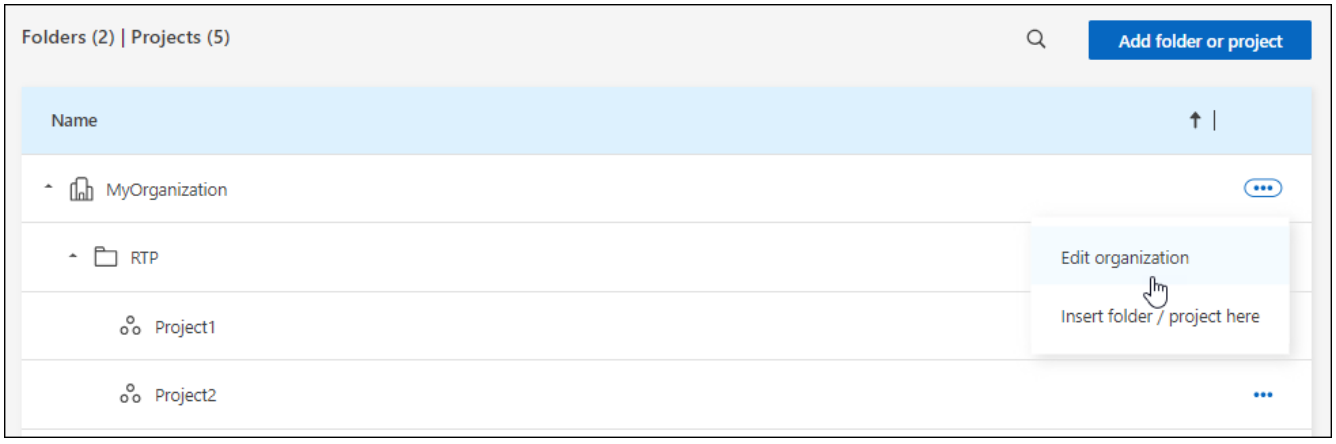
NetApp Console 조직에는 이름과 ID가 있습니다. 조직을 식별하는 데 도움이 되는 이름을 선택할 수 있습니다. 특정 통합을 위해 조직 ID를 검색해야 할 수도 있습니다.

조직 이름 변경

조직의 이름을 바꿀 수 있습니다. 조직 이상의 것을 지원하는 경우 도움이 됩니다.

단계

1. *관리 > ID 및 액세스*를 선택합니다.
2. *조직*을 선택하세요.
3. 조직 페이지에서 표의 첫 번째 행으로 이동하여 다음을 선택합니다. ••• 그런 다음 *조직 편집*을 선택하세요.



4. 새로운 조직 이름을 입력하고 *적용*을 선택하세요.

조직 ID를 얻으세요

조직 ID는 콘솔과의 특정 통합에 사용됩니다.

조직 페이지에서 조직 ID를 보고 필요에 따라 클립보드에 복사할 수 있습니다.

단계

1. 관리 > ID 및 액세스 > *조직*을 선택합니다.
2. 조직 페이지에서 요약 표시줄에 있는 조직 ID를 찾아 클립보드에 복사합니다. 나중에 사용하기 위해 저장할 수도 있고, 필요한 곳에 직접 복사해서 사용할 수도 있습니다.

프로젝트에 대한 ID를 얻으세요

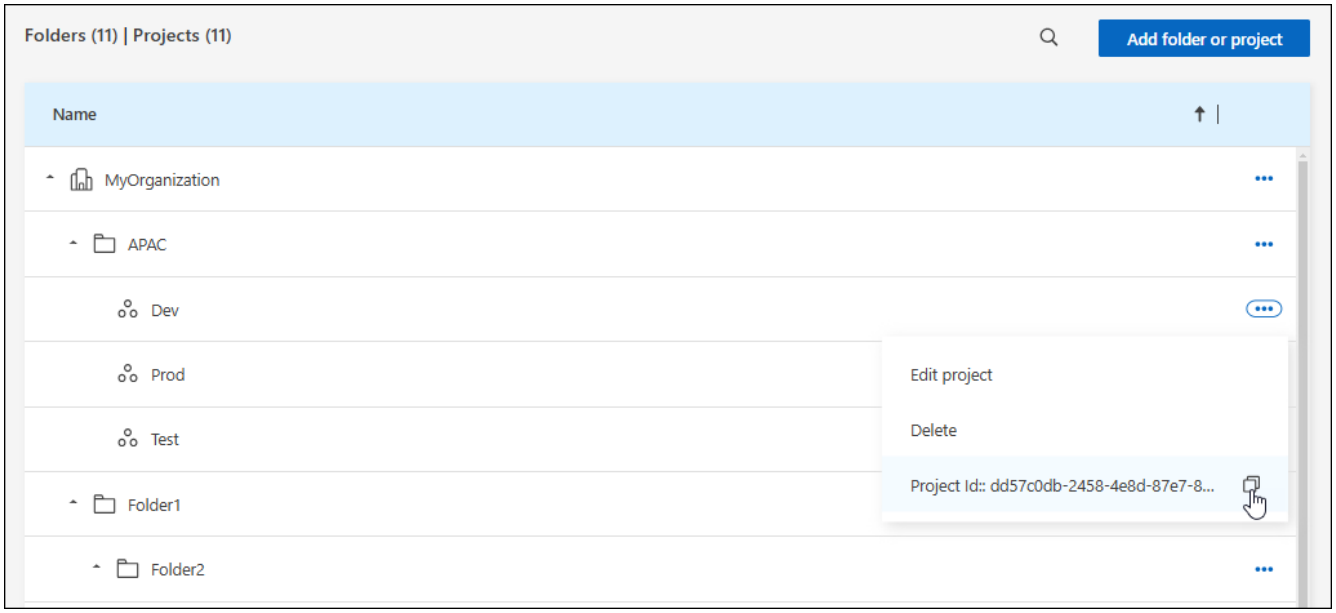
API를 사용하는 경우 프로젝트의 ID를 얻어야 합니다. 예를 들어, Cloud Volumes ONTAP 시스템을 생성할 때.

단계

1. 조직 페이지에서 표의 프로젝트로 이동하여 다음을 선택합니다. •••

   프로젝트 ID가 표시됩니다.

2. ID를 복사하려면 복사 버튼을 선택하세요.



관련 정보

- "ID 및 액세스 관리에 대해 알아보세요"
- "신원 및 액세스 시작하기"
- "ID 및 액세스를 위한 API에 대해 알아보세요"

보안 및 규정 준수

ID 페더레이션

NetApp Console 사용하여 **ID** 페더레이션을 사용하여 단일 로그인을 활성화합니다**.**

Single Sign-On(페더레이션)은 사용자가 회사 자격 증명을 사용하여 NetApp Console 에 로그인할 수 있도록 하여 로그인 프로세스를 간소화하고 보안을 강화합니다. ID 공급자(IdP) 또는 NetApp 지원 사이트를 통해 SSO(단일 로그인)를 활성화할 수 있습니다.

필수 역할

조직 관리자, 연합 관리자, 연합 뷰어."액세스 역할에 대해 자세히 알아보세요."

NetApp Support Site를 통한 Single Sign-On

NetApp 지원 사이트와 페더레이션하면 사용자는 동일한 자격 증명을 사용하여 콘솔, Active IQ Digital Advisor 및 기타 관련 앱에 로그인할 수 있습니다.

NetApp 지원 사이트와 페더레이션하는 경우 기업 ID 관리 공급자와 페더레이션할 수 없습니다. 귀하의 조직에 가장 적합한 것을 선택하세요.

단계

1. 다운로드하고 완료하세요 "NetApp 페더레이션 요청 양식" .
2. 양식에 명시된 이메일 주소로 양식을 제출해 주세요.

   NetApp 지원팀은 귀하의 요청을 검토하고 처리합니다.

ID 공급자를 사용한 Single Sign-On

콘솔에 대한 SSO(Single Sign-On)를 활성화하려면 ID 공급자와 페더레이션 연결을 설정할 수 있습니다. 이 프로세스에는 NetApp 서비스 공급자로 신뢰하도록 ID 공급자를 구성한 다음 콘솔에서 연결을 만드는 작업이 포함됩니다.

이전에 NetApp Cloud Central(콘솔의 외부 애플리케이션)을 사용하여 페더레이션을 구성한 경우, 콘솔 내에서 이를 관리하려면 페더레이션 페이지를 사용하여 페더레이션을 가져와야 합니다."연방을 가져오는 방법을 알아보세요."

지원되는 **ID** 공급자

NetApp 페더레이션을 위해 다음과 같은 프로토콜과 ID 공급자를 지원합니다.

프로토콜

- SAML(Security Assertion Markup Language) ID 공급자
- Active Directory 페더레이션 서비스(AD FS)

ID 공급자

- 마이크로소프트 엔트라 ID
- 핑페더레이트

NetApp Console 플로우와의 페더레이션

NetApp 서비스 공급자가 시작하는(SP 가 시작하는) SSO만 지원합니다. 먼저 NetApp 서비스 공급자로 신뢰하도록 ID 공급자를 구성해야 합니다. 그런 다음 콘솔에서 ID 공급자의 구성을 사용하는 연결을 만들 수 있습니다.

귀하의 이메일 도메인이나 귀하가 소유한 다른 도메인과 연합할 수 있습니다. 이메일 도메인과 다른 도메인과 페더레이션하려면 먼저 해당 도메인을 소유하고 있는지 확인하세요.


도메인을 확인하세요(이메일 도메인을 사용하지 않는 경우)

이메일 도메인과 다른 도메인과 페더레이션하려면 해당 도메인의 소유자인지 확인하세요. 추가 단계 없이 이메일 도메인을 연합할 수 있습니다.


NetApp 서비스 공급자로 신뢰하도록 **IdP**를 구성하세요.

새로운 애플리케이션을 만들고 ACS URL, 엔터티 ID 또는 기타 자격 증명 정보와 같은 세부 정보를 제공하여 NetApp 신뢰하도록 ID 공급자를 구성합니다. 서비스 제공자 정보는 ID 제공자마다 다르므로 자세한 내용은 해당 ID 제공자의 설명서를 참조하세요. 이 단계를 완료하려면 IdP 관리자와 협력해야 합니다.


콘솔에서 페더레이션 연결을 만듭니다.

연결을 생성하려면 ID 공급자의 SAML 메타데이터 URL이나 파일을 제공하세요. 이 정보는 콘솔과 ID 공급자 간의 신뢰 관계를 설정하는 데 사용됩니다. 귀하가 제공하는 정보는 귀하가 사용하는 IdP에 따라 달라집니다. 예를 들어 Microsoft Entra ID를 사용하는 경우 클라이언트 ID, 비밀번호, 도메인을 제공해야 합니다.


콘솔에서 페더레이션을 테스트하세요

페더레이션 연결을 활성화하기 전에 테스트하세요. 콘솔의 페더레이션 페이지에서 테스트 옵션을 사용하여 테스트 사용자가 성공적으로 인증할 수 있는지 확인하세요. 테스트가 성공하면 연결을 활성화할 수 있습니다.


콘솔에서 연결을 활성화하세요

연결을 활성화하면 사용자는 회사 자격 증명을 사용하여 콘솔에 로그인할 수 있습니다.

시작하려면 해당 프로토콜이나 IdP에 대한 주제를 검토하세요.

- "AD FS를 사용하여 페더레이션 연결 설정"
- "Microsoft Entra ID를 사용하여 페더레이션 연결 설정"
- "PingFederate를 사용하여 페더레이션 연결 설정"
- "SAML ID 공급자와 페더레이션 연결 설정"

도메인 확인

페더레이션 연결에 대한 이메일 도메인을 확인하세요.

이메일 도메인과 다른 도메인과 페더레이션하려면 먼저 해당 도메인을 소유하고 있는지 확인해야 합니다. 페더레이션에는 검증된 도메인만 사용할 수 있습니다.

필수 역할

연합을 만들고 관리하려면 연합 관리자 역할이 필요합니다. 연방 뷰어는 연방 페이지를 볼 수 있습니다."액세스 역할에 대해 자세히 알아보세요."

도메인을 확인하려면 도메인의 DNS 설정에 TXT 레코드를 추가해야 합니다. 이 레코드는 사용자가 도메인을 소유하고 있음을 증명하는 데 사용되며 NetApp Console 페더레이션을 위해 도메인을 신뢰할 수 있도록 합니다. 이 단계를 완료하려면 IT 또는 네트워크 관리자와 협력해야 할 수도 있습니다.

단계

1. *관리 > ID 및 액세스*를 선택합니다.
2. 연합*을 선택하면 *연합 페이지를 볼 수 있습니다.
3. *새 페더레이션 구성*을 선택합니다.
4. *도메인 소유권 확인*을 선택하세요.
5. 검증하려는 도메인을 입력하고 *계속*을 선택하세요.
6. 제공된 TXT 레코드를 복사하세요.
7. 도메인의 DNS 설정으로 이동하여 도메인의 TXT 레코드로 제공된 TXT 값을 구성합니다. 필요한 경우 IT 관리자나 네트워크 관리자와 협력하세요.
8. TXT 레코드를 추가한 후 콘솔로 돌아가서 *확인*을 선택하세요.

페더레이션 구성

NetApp Console Active Directory Federation Services(AD FS)와 페더레이션

NetApp Console NetApp Console 과 Active Directory Federation Services(AD FS)를 페더레이션합니다. 이를 통해 사용자는 회사 자격 증명을 사용하여 콘솔에 로그인할 수 있습니다.

필수 역할

연합을 만들고 관리하려면 연합 관리자 역할이 필요합니다. 연방 뷰어는 연방 페이지를 볼 수 있습니다."액세스 역할에 대해 자세히 알아보세요."

회사 IdP 또는 NetApp 지원 사이트와 연합할 수 있습니다. NetApp 둘 중 하나만 선택하는 것을 권장하지만, 둘 다 선택하는 것은 권장하지 않습니다.

NetApp 서비스 공급자가 시작하는(SP 가 시작하는) SSO만 지원합니다. 먼저, NetApp Console 서비스 공급자로 신뢰하도록 ID 공급자를 구성합니다. 그런 다음 ID 공급자의 구성을 사용하여 콘솔에서 연결을 만듭니다.

NetApp Console 에 대한 SSO(Single Sign-On)를 활성화하려면 AD FS 서버와 페더레이션을 설정할 수 있습니다. 이 프로세스에는 콘솔을 서비스 공급자로 신뢰하도록 AD FS를 구성한 다음 NetApp Console 에서 연결을 만드는 작업이 포함됩니다.

단계

1. *관리 > ID 및 액세스*를 선택합니다.
2. 연합*을 선택하면 *연합 페이지를 볼 수 있습니다.
3. *새 페더레이션 구성*을 선택합니다.
4. 도메인 세부 정보를 입력하세요:

a. 검증된 도메인을 사용할지, 이메일 도메인을 사용할지 선택하세요. 이메일 도메인은 로그인한 계정과 연결된 도메인입니다.

b. 구성 중인 페더레이션의 이름을 입력하세요.

c. 검증된 도메인을 선택한 경우 목록에서 도메인을 선택하세요.

5. *다음*을 선택하세요.
6. 연결 방법으로 *프로토콜*을 선택한 다음 *Active Directory Federation Services(AD FS)*를 선택합니다.
7. *다음*을 선택하세요.
8. AD FS 서버에서 신뢰 당사자 트러스트를 만듭니다. PowerShell을 사용하거나 AD FS 서버에서 수동으로 구성할 수 있습니다. 신뢰 당사자 트러스트를 만드는 방법에 대한 자세한 내용은 AD FS 설명서를 참조하세요.

a. 다음 스크립트를 사용하여 PowerShell을 사용하여 신뢰를 만듭니다.

```
(new-object Net.WebClient -property @{Encoding = [Text.Encoding]
::UTF8}).DownloadString("https://raw.github.com/auth0/AD FS-
auth0/master/AD FS.ps1") | iex
AddRelyingParty "urn:auth0:netapp-cloud-account" "https://netapp-
cloud-account.auth0.com/login/callback"
```

b. 또는 AD FS 관리 콘솔에서 수동으로 신뢰를 만들 수 있습니다. 신뢰를 생성할 때 다음 NetApp Console 값을 사용하세요.

- Relying Trust Identifier를 생성할 때 **YOUR_TENANT** 값을 사용하세요. `netapp-cloud-account`
- *WS-Federation 지원 활성화*를 선택하는 경우 **YOUR_AUTH0_DOMAIN** 값을 사용하세요. `netapp-cloud-account.auth0.com`

c. 신뢰를 생성한 후 AD FS 서버에서 메타데이터 URL을 복사하거나 페더레이션 메타데이터 파일을 다운로드합니다. 콘솔에서 연결을 완료하려면 이 URL이나 파일이 필요합니다.

NetApp NetApp Console 최신 AD FS 구성을 자동으로 검색하도록 메타데이터 URL을 사용할 것을 권장합니다. 페더레이션 메타데이터 파일을 다운로드한 경우 AD FS 구성이 변경될 때마다 NetApp Console 에서 수동으로 업데이트해야 합니다.

9. 콘솔로 돌아가서 *다음*을 선택하여 연결을 만듭니다.
10. AD FS로 연결을 만듭니다.

a. 이전 단계에서 AD FS 서버에서 복사한 *AD FS URL*을 입력하거나 AD FS 서버에서 다운로드한 페더레이션 메타데이터 파일을 업로드합니다.

11. *연결 만들기*를 선택합니다. 연결을 만드는 데 몇 초가 걸릴 수 있습니다.
12. *다음*을 선택하세요.
13. 연결을 테스트하려면 *연결 테스트*를 선택하세요. IdP 서버의 로그인 페이지로 이동됩니다. IdP 자격 증명으로 로그인하세요. 로그인 후 콘솔로 돌아가서 연결을 활성화하세요.

> 제한 모드에서 콘솔을 사용하는 경우, URL을 시크릿 브라우저 창이나 별도의 브라우저에 복사하여 IdP에 로그인하십시오.

14. 콘솔에서 *다음*을 선택하여 요약 페이지를 검토하십시오.

15. 알림을 설정하세요.

    7일 또는 30일 중에서 선택하세요. 이 시스템은 만료 알림을 이메일로 발송하고 콘솔에 표시하며, 해당 알림은 슈퍼 관리자, 조직 관리자, 페더레이션 관리자 및 페더레이션 뷰어 역할을 가진 모든 사용자에게 제공됩니다.

16. 연동 세부 정보를 검토한 다음 *연동 활성화*를 선택하십시오.
17. *마침*을 선택하여 과정을 완료하세요.

페더레이션을 활성화하면 사용자는 회사 자격 증명을 사용하여 NetApp Console 에 로그인합니다.

Microsoft Entra ID를 사용하여 **NetApp Console** 페더레이션

NetApp Console 에 대한 SSO(Single Sign-On)를 활성화하려면 Microsoft Entra ID IdP 공급자와 페더레이션하세요. 이를 통해 사용자는 회사 자격 증명을 사용하여 로그인할 수 있습니다.

필수 역할

연합을 만들고 관리하려면 연합 관리자 역할이 필요합니다. 연방 뷰어는 연방 페이지를 볼 수 있습니다."액세스 역할에 대해 자세히 알아보세요."

회사 IdP 또는 NetApp 지원 사이트와 연합할 수 있습니다. NetApp 둘 중 하나만 선택하는 것을 권장하지만, 둘 다 선택하는 것은 권장하지 않습니다.

NetApp 서비스 공급자가 시작하는(SP 가 시작하는) SSO만 지원합니다. 먼저 NetApp 서비스 공급자로 신뢰하도록 ID 공급자를 구성해야 합니다. 그런 다음 콘솔에서 ID 공급자의 구성을 사용하는 연결을 만들 수 있습니다.

Microsoft Entra ID를 사용하여 페더레이션 연결을 설정하면 콘솔에 대한 SSO(Single Sign-On)를 사용할 수 있습니다. 이 프로세스에는 콘솔을 서비스 공급자로 신뢰하도록 Microsoft Entra ID를 구성한 다음 콘솔에서 연결을 만드는 작업이 포함됩니다.

단계

1. *관리 > ID 및 액세스*를 선택합니다.
2. 연합*을 선택하면 *연합 페이지를 볼 수 있습니다.
3. *새 페더레이션 구성*을 선택합니다.

도메인 세부 정보

1. 도메인 세부 정보를 입력하세요:
   a. 검증된 도메인을 사용할지, 이메일 도메인을 사용할지 선택하세요. 이메일 도메인은 로그인한 계정과 연결된 도메인입니다.
   b. 구성 중인 페더레이션의 이름을 입력하세요.
   c. 검증된 도메인을 선택한 경우 목록에서 도메인을 선택하세요.
2. *다음*을 선택하세요.

연결 방법

1. 연결 방법으로 *공급자*를 선택한 다음 *Microsoft Entra ID*를 선택하세요.

2. *다음*을 선택하세요.

구성 지침

1. NetApp 서비스 공급자로 신뢰하도록 Microsoft Entra ID를 구성하세요. 이 단계는 Microsoft Entra ID 서버에서 수행해야 합니다.
   a. 콘솔을 신뢰하려면 Microsoft Entra ID 앱을 등록할 때 다음 값을 사용하세요.
      - *리디렉션 URL*의 경우 다음을 사용하세요. `https://services.cloud.netapp.com`
      - *답변 URL*의 경우 다음을 사용하세요. `https://netapp-cloud-account.auth0.com/login/callback`
   b. Microsoft Entra ID 앱에 대한 클라이언트 비밀번호를 만듭니다. 페더레이션을 완료하려면 클라이언트 ID, 클라이언트 비밀번호, Entra ID 도메인 이름을 제공해야 합니다.
2. 콘솔로 돌아가서 *다음*을 선택하여 연결을 만듭니다.

연결 생성

1. Microsoft Entra ID로 연결 만들기
   a. 이전 단계에서 생성한 클라이언트 ID와 클라이언트 비밀번호를 입력하세요.
   b. Microsoft Entra ID 도메인 이름을 입력하세요.
2. *연결 만들기*를 선택하세요. 시스템은 몇 초 안에 연결을 생성합니다.

연결을 테스트하고 활성화합니다.

1. *다음*을 선택하세요.
2. 연결을 테스트하려면 *연결 테스트*를 선택하세요. IdP 서버의 로그인 페이지로 이동됩니다. IdP 자격 증명으로 로그인하세요. 로그인 후 콘솔로 돌아가서 연결을 활성화하세요.

   제한 모드에서 콘솔을 사용하는 경우, URL을 시크릿 브라우저 창이나 별도의 브라우저에 복사하여 IdP에 로그인하십시오.

3. 콘솔에서 *다음*을 선택하여 요약 페이지를 검토하십시오.
4. 알림을 설정하세요.

   7일 또는 30일 중에서 선택하세요. 이 시스템은 만료 알림을 이메일로 발송하고 콘솔에 표시하며, 해당 알림은 슈퍼 관리자, 조직 관리자, 페더레이션 관리자 및 페더레이션 뷰어 역할을 가진 모든 사용자에게 제공됩니다.

5. 연동 세부 정보를 검토한 다음 *연동 활성화*를 선택하십시오.
6. *마침*을 선택하여 과정을 완료하세요.

페더레이션을 활성화하면 사용자는 회사 자격 증명을 사용하여 NetApp Console 에 로그인합니다.

PingFederate를 사용하여 **NetApp Console** 페더레이션

PingFederate IdP 공급자와 페더레이션하여 NetApp Console 에 대한 SSO(Single Sign-On)를 활성화합니다. 이를 통해 사용자는 회사 자격 증명을 사용하여 로그인할 수 있습니다.

필수 역할

연합을 만들고 관리하려면 연합 관리자 역할이 필요합니다. 연방 뷰어는 연방 페이지를 볼 수 있습니다."액세스 역할에 대해 자세히 알아보세요."

회사 IdP 또는 NetApp 지원 사이트와 연합할 수 있습니다. NetApp 둘 중 하나만 선택하는 것을 권장하지만, 둘 다 선택하는 것은 권장하지 않습니다.

NetApp 서비스 공급자가 시작하는(SP 가 시작하는) SSO만 지원합니다. 먼저 NetApp 서비스 공급자로 신뢰하도록 ID 공급자를 구성해야 합니다. 그런 다음 콘솔에서 ID 공급자의 구성을 사용하는 연결을 만들 수 있습니다.

PingFederate를 사용하여 페더레이션 연결을 설정하면 콘솔에 대한 SSO(Single Sign-On)를 활성화할 수 있습니다. 이 프로세스에는 PingFederate 서버가 콘솔을 서비스 공급자로 신뢰하도록 구성한 다음 콘솔에서 연결을 만드는 작업이 포함됩니다.

단계

1. *관리 > ID 및 액세스*를 선택합니다.
2. 연합*을 선택하면 *연합 페이지를 볼 수 있습니다.
3. *새 페더레이션 구성*을 선택합니다.
4. 도메인 세부 정보를 입력하세요:
   a. 검증된 도메인을 사용할지, 이메일 도메인을 사용할지 선택하세요. 이메일 도메인은 로그인한 계정과 연결된 도메인입니다.
   b. 구성 중인 페더레이션의 이름을 입력하세요.
   c. 검증된 도메인을 선택한 경우 목록에서 도메인을 선택하세요.
5. *다음*을 선택하세요.
6. 연결 방법으로 *공급자*를 선택한 다음 *PingFederate*를 선택하세요.
7. *다음*을 선택하세요.
8. NetApp 서비스 공급자로 신뢰하도록 PingFederate 서버를 구성합니다. 이 단계는 PingFederate 서버에서 수행해야 합니다.
   a. PingFederate가 NetApp Console 신뢰하도록 구성할 때 다음 값을 사용하세요.
      - 답변 **URL** 또는 *Assertion Consumer Service(ACS) URL*의 경우 다음을 사용하세요. `https://netapp-cloud-account.auth0.com/login/callback`
      - *로그아웃 URL*의 경우 다음을 사용하세요. `https://netapp-cloud-account.auth0.com/logout`
      - *대상/엔터티 ID*의 경우 다음을 사용하세요. `urn:auth0:netapp-cloud-account:<fed-domain-name-saml>` 여기서 <fed-domain-name-pingfederate>는 페더레이션의 도메인 이름입니다. 예를 들어, 귀하의 도메인이 `example.com` , 대상/엔터티 ID는 다음과 같습니다. `urn:auth0:netappcloud-account:fed-example-com-pingfederate` .
   b. PingFederate 서버 URL을 복사합니다. 콘솔에서 연결을 생성하려면 이 URL이 필요합니다.
   c. PingFederate 서버에서 X.509 인증서를 다운로드합니다. Base64로 인코딩된 PEM 형식(.pem, .crt, .cer)이어야 합니다.
9. 콘솔로 돌아가서 *다음*을 선택하여 연결을 만듭니다.
10. PingFederate로 연결을 만듭니다.

a. 이전 단계에서 복사한 PingFederate 서버 URL을 입력하세요.

b. X.509 서명 인증서를 업로드합니다. 인증서는 PEM, CER 또는 CRT 형식이어야 합니다.

11. *연결 만들기*를 선택하세요. 시스템은 몇 초 안에 연결을 생성합니다.
12. *다음*을 선택하세요.
13. 연결을 테스트하려면 *연결 테스트*를 선택하세요. IdP 서버의 로그인 페이지로 이동됩니다. IdP 자격 증명으로 로그인하세요. 로그인 후 콘솔로 돌아가서 연결을 활성화하세요.

> 제한 모드에서 콘솔을 사용하는 경우, URL을 시크릿 브라우저 창이나 별도의 브라우저에 복사하여 IdP에 로그인하십시오.

14. 콘솔에서 *다음*을 선택하여 요약 페이지를 검토하십시오.
15. 알림을 설정하세요.

    7일 또는 30일 중에서 선택하세요. 이 시스템은 만료 알림을 이메일로 발송하고 콘솔에 표시하며, 해당 알림은 슈퍼 관리자, 조직 관리자, 페더레이션 관리자 및 페더레이션 뷰어 역할을 가진 모든 사용자에게 제공됩니다.

16. 연동 세부 정보를 검토한 다음 *연동 활성화*를 선택하십시오.
17. *마침*을 선택하여 과정을 완료하세요.

페더레이션을 활성화하면 사용자는 회사 자격 증명을 사용하여 NetApp Console 에 로그인합니다.

SAML ID 공급자와 페더레이션

SAML 2.0 IdP 공급자와 연합하여 NEtApp 콘솔에 대한 SSO(Single Sign-On)를 활성화합니다. 이를 통해 사용자는 회사 자격 증명을 사용하여 로그인할 수 있습니다.

필수 역할

연합을 만들고 관리하려면 연합 관리자 역할이 필요합니다. 연방 뷰어는 연방 페이지를 볼 수 있습니다."액세스 역할에 대해 자세히 알아보세요."

> 회사 IdP 또는 NetApp 지원 사이트와 연합할 수 있습니다. 두 나라 모두와 연합할 수는 없습니다.

NetApp 서비스 공급자가 시작하는(SP 가 시작하는) SSO만 지원합니다. 먼저 NetApp 서비스 공급자로 신뢰하도록 ID 공급자를 구성해야 합니다. 그런 다음 콘솔에서 ID 공급자의 구성을 사용하는 연결을 만들 수 있습니다.

SAML 2.0 공급자와 페더레이션 연결을 설정하면 콘솔에 대한 SSO(Single Sign-On)를 사용할 수 있습니다. 이 프로세스에는 서비스 공급자로서 NetApp 신뢰하도록 공급자를 구성한 다음 콘솔에서 연결을 만드는 작업이 포함됩니다.

단계

1. *관리 > ID 및 액세스*를 선택합니다.
2. 연합*을 선택하면 *연합 페이지를 볼 수 있습니다.
3. *새 페더레이션 구성*을 선택합니다.
4. 도메인 세부 정보를 입력하세요:

   a. 검증된 도메인을 사용할지, 이메일 도메인을 사용할지 선택하세요. 이메일 도메인은 로그인한 계정과 연결된

도메인입니다.

b. 구성 중인 페더레이션의 이름을 입력하세요.

c. 검증된 도메인을 선택한 경우 목록에서 도메인을 선택하세요.

5. *다음*을 선택하세요.
6. 연결 방법으로 *프로토콜*을 선택한 다음 *SAML ID 공급자*를 선택하세요.
7. *다음*을 선택하세요.
8. NetApp 서비스 공급자로 신뢰하도록 SAML ID 공급자를 구성합니다. 이 단계는 SAML 공급자 서버에서 수행해야 합니다.

a. IdP에 속성이 있는지 확인하세요. `email` 사용자의 이메일 주소로 설정됩니다. 이는 콘솔이 사용자를 올바르게 식별하는 데 필요합니다.

```
<saml:AttributeStatement
xmlns:x500="urn:oasis:names:tc:SAML:2.0:profiles:attribute:X500"
xmlns:xs="http://www.w3.org/2001/XMLSchema"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
    <saml:Attribute Name="email"
NameFormat="urn:oasis:names:tc:SAML:1.1:nameid-format:X509SubjectName">
        <saml:AttributeValue
xsi:type="xs:string">email@domain.com</saml:AttributeValue>
    </saml:Attribute>
</saml:AttributeStatement>
```

1. 콘솔에 SAML 애플리케이션을 등록할 때 다음 값을 사용하세요.
   - 답변 **URL** 또는 *Assertion Consumer Service(ACS) URL*의 경우 다음을 사용하세요. `https://netapp-cloud-account.auth0.com/login/callback`
   - *로그아웃 URL*의 경우 다음을 사용하세요. `https://netapp-cloud-account.auth0.com/logout`
   - *대상/엔터티 ID*의 경우 다음을 사용하세요. `urn:auth0:netapp-cloud-account:<fed-domain-name-saml>` 여기서 <fed-domain-name-saml>은 페더레이션에 사용하려는 도메인 이름입니다. 예를 들어, 귀하의 도메인이 `example.com` , 대상/엔터티 ID는 다음과 같습니다. `urn:auth0:netapp-cloud-account:fed-example-com-samlp` .
2. 신뢰를 생성한 후 SAML 공급자 서버에서 다음 값을 복사합니다.
   - 로그인 URL
   - 로그아웃 URL(선택 사항)
3. SAML 공급자 서버에서 X.509 인증서를 다운로드합니다. PEM, CER 또는 CRT 형식이어야 합니다.

a. 콘솔로 돌아가서 *다음*을 선택하여 연결을 만듭니다.

b. SAML로 연결을 생성합니다.

4. SAML 서버의 *로그인 URL*을 입력하세요.
5. SAML 공급자 서버에서 다운로드한 X.509 인증서를 업로드합니다.
6. 선택적으로 SAML 서버의 *로그아웃 URL*을 입력하세요.

a. *연결 만들기*를 선택하세요. 시스템은 몇 초 안에 연결을 생성합니다.

b. *다음*을 선택하세요.

c. 연결을 테스트하려면 *연결 테스트*를 선택하세요. IdP 서버의 로그인 페이지로 이동됩니다. IdP 자격 증명으로 로그인하세요. 로그인 후 콘솔로 돌아가서 연결을 활성화하세요.

> 제한 모드에서 콘솔을 사용하는 경우, URL을 시크릿 브라우저 창이나 별도의 브라우저에 복사하여 IdP에 로그인하십시오.

d. 콘솔에서 *다음*을 선택하여 요약 페이지를 검토하십시오.

e. 알림을 설정하세요.

7일 또는 30일 중에서 선택하세요. 이 시스템은 만료 알림을 이메일로 발송하고 콘솔에 표시하며, 해당 알림은 슈퍼 관리자, 조직 관리자, 페더레이션 관리자 및 페더레이션 뷰어 역할을 가진 모든 사용자에게 제공됩니다.

f. 연동 세부 정보를 검토한 다음 *연동 활성화*를 선택하십시오.

g. *마침*을 선택하여 과정을 완료하세요.

페더레이션을 활성화하면 사용자는 회사 자격 증명을 사용하여 NetApp Console 에 로그인합니다.

연합 관리

NetApp Console 에서 페더레이션 관리

NetApp Console 에서 페더레이션을 관리할 수 있습니다. 이 기능을 비활성화하고, 만료된 자격 증명을 업데이트하고, 더 이상 필요하지 않으면 비활성화할 수 있습니다.

필수 역할

연합을 만들고 관리하려면 연합 관리자 역할이 필요합니다. 연방 뷰어는 연방 페이지를 볼 수 있습니다."액세스 역할에 대해 자세히 알아보세요."

기존 페더레이션에 추가적인 인증된 도메인을 추가할 수도 있습니다. 이를 통해 페더레이션 연결에 여러 도메인을 사용할 수 있습니다.

- NetApp Cloud Central을 사용하여 페더레이션을 구성한 경우 페더레이션 페이지를 통해 가져와서 콘솔에서 관리하세요."연방을 가져오는 방법을 알아보세요"
- 감사 페이지에서 페더레이션 활성화, 비활성화 및 업데이트와 같은 페더레이션 관리 이벤트를 확인할 수 있습니다. "NetApp Console 에서 작업 모니터링에 대해 자세히 알아보세요."

연합 활성화

연합을 생성했지만 활성화되지 않은 경우, 연합 페이지를 통해 활성화할 수 있습니다. 페더레이션을 활성화하면 페더레이션에 연결된 사용자가 회사 자격 증명을 사용하여 콘솔에 로그인할 수 있습니다. 연합을 활성화하기 전에 연합을 성공적으로 생성하고 테스트하세요.

단계

1. *관리 > ID 및 액세스*를 선택합니다.
2. 연방 탭을 선택하세요.

3. 작업 메뉴를 선택하세요••• 활성화하려는 페더레이션 옆에 있는 *활성화*를 선택합니다.

기존 페더레이션에 검증된 도메인 추가

콘솔에서 기존 페더레이션에 검증된 도메인을 추가하여 동일한 ID 공급자(IdP)를 사용하는 여러 도메인을 사용할 수 있습니다.

페더레이션에 도메인을 추가하려면 먼저 콘솔에서 도메인을 확인해야 합니다. 아직 도메인을 확인하지 않은 경우 다음 단계에 따라 확인할 수 있습니다."콘솔에서 도메인을 확인하세요" .

단계

1. *관리 > ID 및 액세스*를 선택합니다.
2. 연방 탭을 선택하세요.
3. 작업 메뉴를 선택하세요⋮ 검증된 도메인을 추가하려는 페더레이션 옆에 있는 도메인 업데이트*를 선택합니다. *도메인 업데이트 대화 상자에는 이 페더레이션에 이미 연결된 도메인이 표시됩니다.
4. 사용 가능한 도메인 목록에서 확인된 도메인을 선택하세요.
5. *업데이트*를 선택하세요. 새로운 도메인 사용자는 30초 이내에 페더레이션 콘솔 액세스 권한을 얻을 수 있습니다.

만료되는 페더레이션 연결 업데이트

콘솔에서 페더레이션의 세부 정보를 업데이트할 수 있습니다. 예를 들어, 인증서나 클라이언트 비밀번호와 같은 자격 증명이 만료되면 페더레이션을 업데이트해야 합니다. 필요한 경우 알림 날짜를 업데이트하여 만료되기 전에 연결을 업데이트하도록 상기시켜줍니다.

로그인 문제를 방지하려면 IdP를 업데이트하기 전에 먼저 콘솔을 업데이트하세요. 프로세스 중에는 콘솔에 로그인 상태를 유지하세요.

단계

1. *관리 > ID 및 액세스*를 선택합니다.
2. 연방 탭을 선택하세요.
3. 업데이트하려는 페더레이션 옆에 있는 작업 메뉴(세 개의 세로 점)를 선택하고 *페더레이션 업데이트*를 선택합니다.
4. 필요에 따라 연방의 세부 정보를 업데이트하세요.
5. *업데이트*를 선택하세요.

기존 연합 테스트

기존 연합의 연결을 테스트하여 제대로 작동하는지 확인합니다. 이를 통해 연합의 문제를 파악하고 해결하는 데 도움이 될 수 있습니다.

단계

1. *관리 > ID 및 액세스*를 선택합니다.
2. 연방 탭을 선택하세요.
3. 작업 메뉴를 선택하세요⋮ 검증된 도메인을 추가하려는 페더레이션 옆에 있는 *연결 테스트*를 선택합니다.
4. *테스트*를 선택하세요. 시스템에서 회사 자격 증명을 사용하여 로그인하라는 메시지가 표시됩니다. 연결에 성공하면 NetApp Console 로 리디렉션됩니다. 연결에 실패하면 페더레이션에 문제가 있음을 나타내는 오류

메시지가 표시됩니다.

5. 완료*를 선택하면 *연방 탭으로 돌아갑니다.

페더레이션 비활성화

더 이상 연방이 필요하지 않으면 연방을 비활성화할 수 있습니다. 이렇게 하면 연합에 연결된 사용자가 회사 자격 증명을 사용하여 콘솔에 로그인하는 것을 방지할 수 있습니다. 필요한 경우 나중에 페더레이션을 다시 활성화할 수 있습니다.

IdP를 해제하거나 페더레이션을 중단하는 경우와 같이 페더레이션을 삭제하기 전에 페더레이션을 비활성화합니다. 나중에 필요할 경우 다시 활성화할 수 있습니다.

단계

1. *관리 > ID 및 액세스*를 선택합니다.
2. 연방 탭을 선택하세요.
3. 작업 메뉴를 선택하세요: 검증된 도메인을 추가하려는 페더레이션 옆에 있는 *비활성화*를 선택합니다.

연합 삭제

더 이상 연합이 필요하지 않으면 삭제할 수 있습니다. 이렇게 하면 페더레이션이 제거되고 페더레이션에 연결된 사용자가 회사 자격 증명을 사용하여 콘솔에 로그인하는 것이 방지됩니다. 예를 들어, IdP가 폐기되거나 연합이 더 이상 필요하지 않은 경우입니다.

연합을 삭제한 후에는 복구할 수 없습니다. 새로운 연방을 만들어야 합니다.

삭제하려면 먼저 페더레이션을 비활성화해야 합니다. 연합을 삭제한 후에는 삭제를 취소할 수 없습니다.

단계

1. *관리 > ID 및 액세스*를 선택합니다.
2. 연합*을 선택하면 *연합 페이지를 볼 수 있습니다.
3. 작업 메뉴를 선택하세요: 검증된 도메인을 추가하려는 페더레이션 옆에 있는 *삭제*를 선택합니다.

NetApp Console 로 페더레이션 가져오기

이전에 NetApp Cloud Central(NetApp Console 의 외부 애플리케이션)을 통해 페더레이션을 설정한 경우 페더레이션 페이지에서 기존 페더레이션 연결을 콘솔로 가져와서 새 인터페이스에서 관리할 수 있도록 하라는 메시지가 표시됩니다. 그러면 페더레이션 연결을 다시 만들지 않고도 최신 개선 사항을 활용할 수 있습니다.

기존 페더레이션을 가져온 후에는 페더레이션 페이지에서 페더레이션을 관리할 수 있습니다."연합 관리에 대해 자세히 알아보세요."

필수 역할

조직 관리자 또는 연방 관리자."액세스 역할에 대해 자세히 알아보세요."

단계

1. *관리 > ID 및 액세스*를 선택합니다.

2. 연방 탭을 선택하세요.
3. *연합 가져오기*를 선택하세요.

ONTAP Advanced View(ONTAP System Manager)에 대한 ONTAP 권한 적용

기본적으로 콘솔 에이전트 자격 증명을 통해 사용자는 고급 보기(ONTAP 시스템 관리자)에 액세스할 수 있습니다. 대신 사용자에게 ONTAP 자격 증명을 입력하라는 메시지를 표시할 수 있습니다. 이를 통해 사용자 Cloud Volumes ONTAP 과 온프레미스 ONTAP 클러스터 모두에서 ONTAP 클러스터를 사용할 때 사용자의 ONTAP 권한이 적용됩니다.

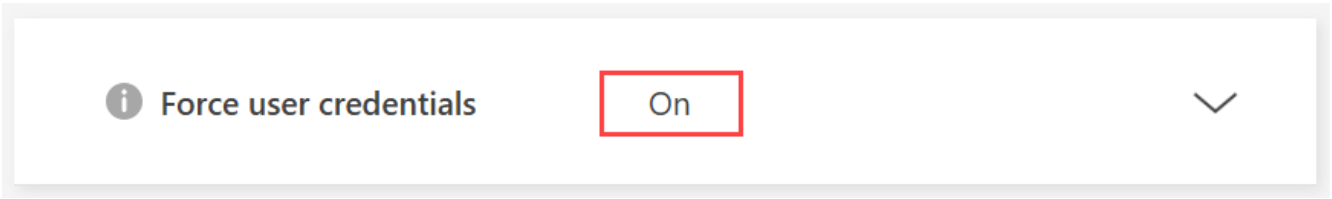
콘솔 에이전트 설정을 편집하려면 조직 관리자 역할이 있어야 합니다.

단계

1. *관리 > 에이전트*를 선택하세요.
2. 개요 페이지에서 콘솔 에이전트의 작업 메뉴를 선택하고 *에이전트 편집*을 선택합니다.

   편집하려면 콘솔 에이전트가 활성화되어 있어야 합니다.

3. 자격 증명 강제 적용 옵션을 확장합니다.
4. 자격 증명 강제 옵션을 활성화하려면 확인란을 선택한 다음 *저장*을 선택합니다.
5. 자격 증명 강제 옵션이 활성화되어 있는지 확인하세요.



NetApp Console 조직에 대해 읽기 전용 모드를 활성화합니다.

보안상의 예방 조치로 NetApp Console 조직에 대해 읽기 전용 모드를 활성화할 수 있습니다. 읽기 전용 모드에서는 사용자가 리소스와 설정을 볼 수는 있지만 변경할 수는 없습니다.

읽기 전용 모드에서는 관리자 권한을 가진 사용자가 변경을 하려면 수동으로 권한을 높여야 하므로 변경 사항이 의도적인 것임을 보장합니다.

필수 접근 권한 역할

최고 관리자 또는 조직 관리자.

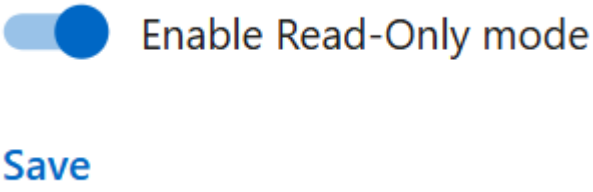
콘솔 조직에 대해 읽기 전용 모드를 활성화합니다.

콘솔 조직에 대한 변경을 제한하려면 읽기 전용 모드를 활성화하세요. 모든 사용자는 여전히 리소스를 볼 수 있습니다. 관리자 권한을 가진 사용자는 수동으로 권한을 높이지 않으면 콘솔에서 어떤 작업도 수행할 수 없습니다.

읽기 전용 모드가 활성화되면 사용자는 조직이 읽기 전용 모드임을 알리는 배너를 보게 됩니다. 사용자는 자신의 역할을 높이기 위해 사용자 설정으로 이동해야 합니다.

단계

1. *관리 > ID 및 액세스*를 선택합니다.
2. 조직 탭에서 읽기 전용 모드로 설정하려는 조직의 *조직 설정 편집*을 선택합니다.
3. 읽기 전용 모드 섹션에서 토글 스위치를 켜짐 위치로 이동하여 읽기 전용 모드를 활성화한 다음 *저장*을 선택합니다.



NetApp Console 에 최초 조직 관리자로 등록하세요**.**

회사에 NetApp Console 조직이 없는 경우 가입하여 조직을 생성하세요. 첫 번째 사용자는 관리자이며 계정과 권한을 관리합니다. 역할은 나중에 업데이트하고 관리자를 추가할 수 있습니다.

단계

1. 웹 브라우저를 열고 이동하세요 "NetApp Console"
2. NetApp 지원 사이트 계정이 있는 경우, 로그인 페이지에서 계정과 연결된 이메일 주소를 직접 입력하십시오.

   콘솔은 초기 로그인 과정에서 NetApp 지원 사이트 자격 증명을 사용하여 사용자를 등록합니다.

3. 콘솔 로그인을 만들어 가입하려면 *가입*을 선택하세요.
   a. 가입 페이지에서 필요한 정보를 입력하고 *다음*을 선택하세요.

      회원가입 양식에는 영문자만 입력할 수 있습니다.

   b. NetApp 에서 보낸 이메일이 받은 편지함에서 확인되었는지 확인하세요. 이메일 주소 확인 지침이 포함되어 있습니다.

      가입을 완료하려면 이메일 주소를 인증하세요.

4. 로그인 후 최종 사용자 라이선스 계약을 검토하고 동의하십시오.
5. 환영 페이지에서 조직을 생성하세요.
6. *시작하기*를 선택하세요.

+ 처음 관리자 권한을 획득한 경우, 안내에 따라 스토리지를 추가하고 콘솔 에이전트를 생성하는 등의 작업을 진행하세요. "콘솔 지원 사용법에 대해 알아보세요."

다음 단계

관리자로서 콘솔 지원 도구에 포함된 단계를 완료한 후에는 ID 및 액세스 전략을 계획하고, 조직에 사용자를 추가하고, 역할을 할당해야 합니다. "NetApp Console 의 ID 및 액세스 관리에 대해 알아보세요."

이미 조직이 있는 경우 **NetApp Console** 에 가입하거나 로그인하세요**.**

귀사에 이미 NetApp Console 조직이 있는 경우, 가입하거나 로그인하여 액세스하십시오. 가입 또는 로그인 방법은 회사에서 ID 페더레이션을 사용하는지 또는 NetApp 지원 사이트 자격 증명을 보유하고 있는지에 따라 다릅니다. 그렇지 않다면 NetApp Console 로그인 계정을 생성하십시오.

단계

1. 웹 브라우저를 열고 이동하세요 "NetApp Console"
2. NetApp 지원 사이트 계정이 있거나 회사에서 단일 로그인(SSO)을 설정한 경우 로그인 페이지에서 연결된 이메일 주소 또는 SSO 자격 증명을 입력하십시오. 안내에 따라 로그인을 완료하세요.

   두 경우 모두, 초기 로그인의 일부로 콘솔에 가입하게 됩니다.

3. 콘솔 로그인을 만들어 가입하려면 *가입*을 선택하세요.
   a. 가입 페이지에서 필요한 정보를 입력하고 *다음*을 선택하세요.

      회원가입 양식에는 영문자만 입력할 수 있습니다.

   b. NetApp 에서 보낸 이메일이 받은 편지함에서 확인되었는지 확인하세요. 이메일 주소 확인 지침이 포함되어 있습니다.

      가입을 완료하려면 이메일 주소를 인증하세요.

4. 로그인 후 최종 사용자 라이선스 계약을 검토하고 동의하십시오.
5. 시스템에서 조직을 생성하라는 메시지가 표시되면 대화 상자를 닫고 콘솔 관리자에게 알려 콘솔 조직에 추가하고 액세스 권한을 부여받으십시오. "조직 관리자에게 연락하는 방법을 알아보세요."

다음 단계

조직에 대한 액세스 권한이 부여되면 스토리지를 관리하고 할당된 데이터 서비스를 사용할 수 있습니다.

조직 간 파트너십 관리

NetApp Console의 조직 파트너십

NetApp Console 에서 조직 간 파트너십을 구축하면 파트너는 조직 경계를 넘어 NetApp 리소스를 안전하게 관리하여 협업을 간소화하고 보안을 강화할 수 있습니다.

필수 역할

파트너십 관리자"액세스 역할에 대해 자세히 알아보세요."

파트너십을 통해 콘솔에서 역할 기반 관계를 사용하여 조직 전체에서 NetApp 리소스를 안전하게 관리할 수 있습니다. 시작 조직은 리소스에 대한 액세스 권한을 부여하고, 수락 조직은 액세스 권한이 부여될 사용자 또는 서비스 계정을 제공합니다. 파트너십은 셀프 서비스 워크플로를 통해 구축되며, 이를 통해 시작한 조직은 어떤 리소스를 공유할지, 어떤 역할을 할당할지, 필요에 따라 파트너 액세스를 온보딩, 관리 또는 취소할 수 있는 권한을 완벽하게 제어할 수 있습니다.

고객은 복잡한 설정 없이도 MSP 또는 리셀러가 NetApp 환경을 관리하도록 권한을 부여할 수 있습니다. 고객은 파트너가 액세스할 수 있는 클러스터와 파트너가 맡고 있는 역할을 제어할 수 있으며, 보안과 규정 준수를 유지하기 위해 언제든지 액세스 권한을 취소할 수 있습니다.

파트너로서 귀하는 고객 환경 전반에 대한 중앙 집중화된 가시성과 제어력을 확보하게 됩니다. 정의된 경계 내에서 리소스를 관리하고, 데이터 서비스를 실행하고, 상태를 모니터링하기 위해 고객의 조직으로 쉽게 전환할 수 있으며, 이를 통해 사용자 정의 툴을 줄이고 각 고객의 정책에 맞춰 조정할 수 있습니다.

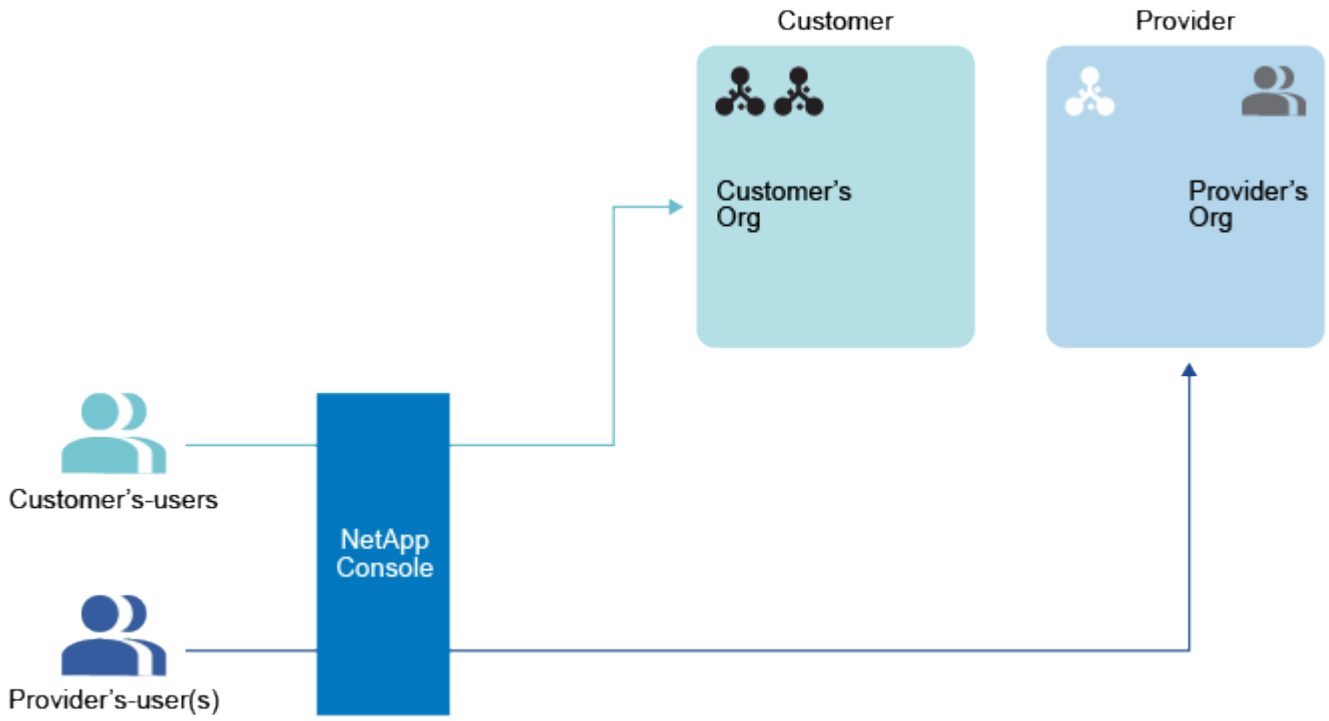
1 한 명 이상의 사용자에게 파트너십 관리자 역할을 할당합니다.

파트너십을 생성하고 관리하려면 시작 조직과 수신 조직 모두에서 한 명 이상의 사용자에게 Partnership admin 역할을 할당하십시오. 파트너십을 보기만 하고 관리할 필요가 없는 사용자에게는 Partnership viewer 역할을 할당할 수 있습니다.

2 귀하의 조직 **ID**를 시작 조직과 공유하세요.

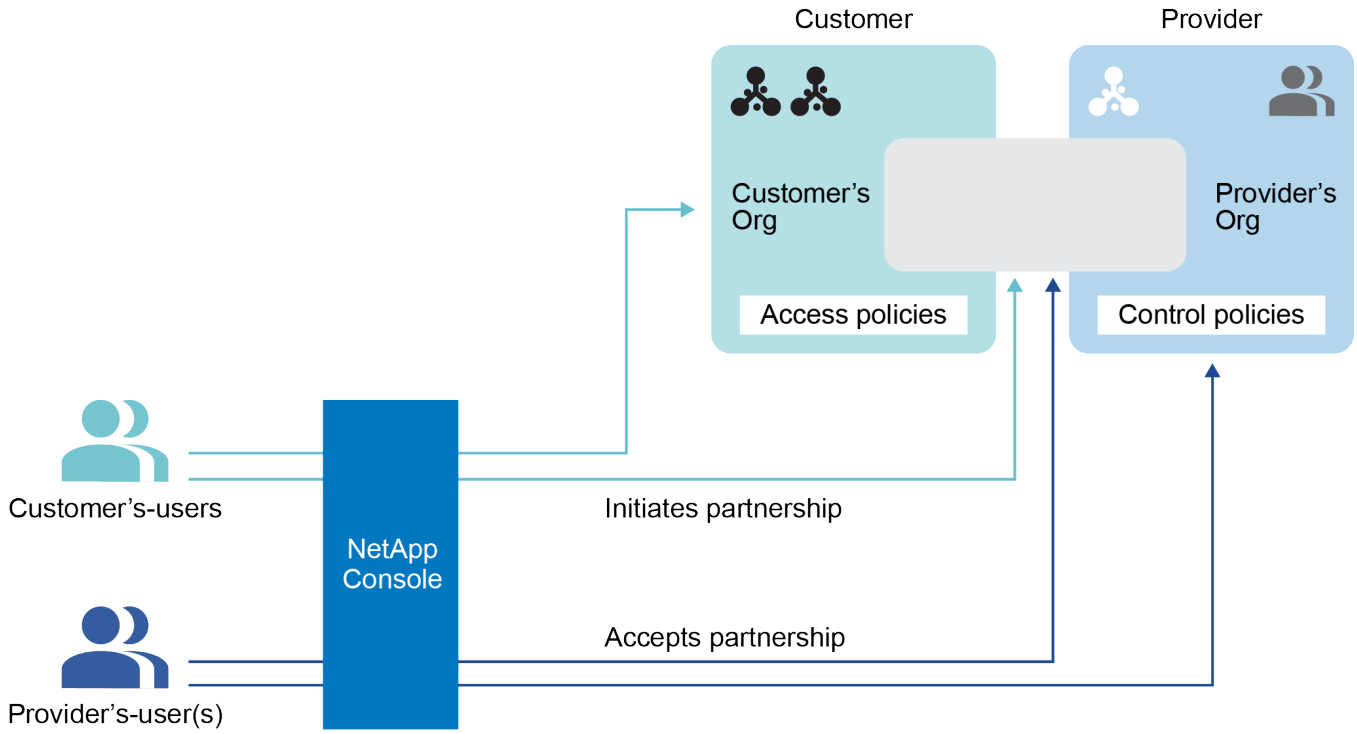
파트너십을 시작하려면 시작자는 대상 조직의 조직 ID를 알아야 합니다. 해당 조직에서만 이 조직 ID에 접근할 수 있습니다. NetApp Console 외부에서 이메일이나 다른 방법을 통해 시작 조직과 직접 공유하세요.

시작 조직이란 자원에 대한 접근 권한을 부여하는 조직입니다.



3 **NetApp Console** 내에서 파트너십 시작

파트너십을 시작하는 조직은 NetApp Console 에서 파트너십 요청을 보내 파트너십을 시작합니다.



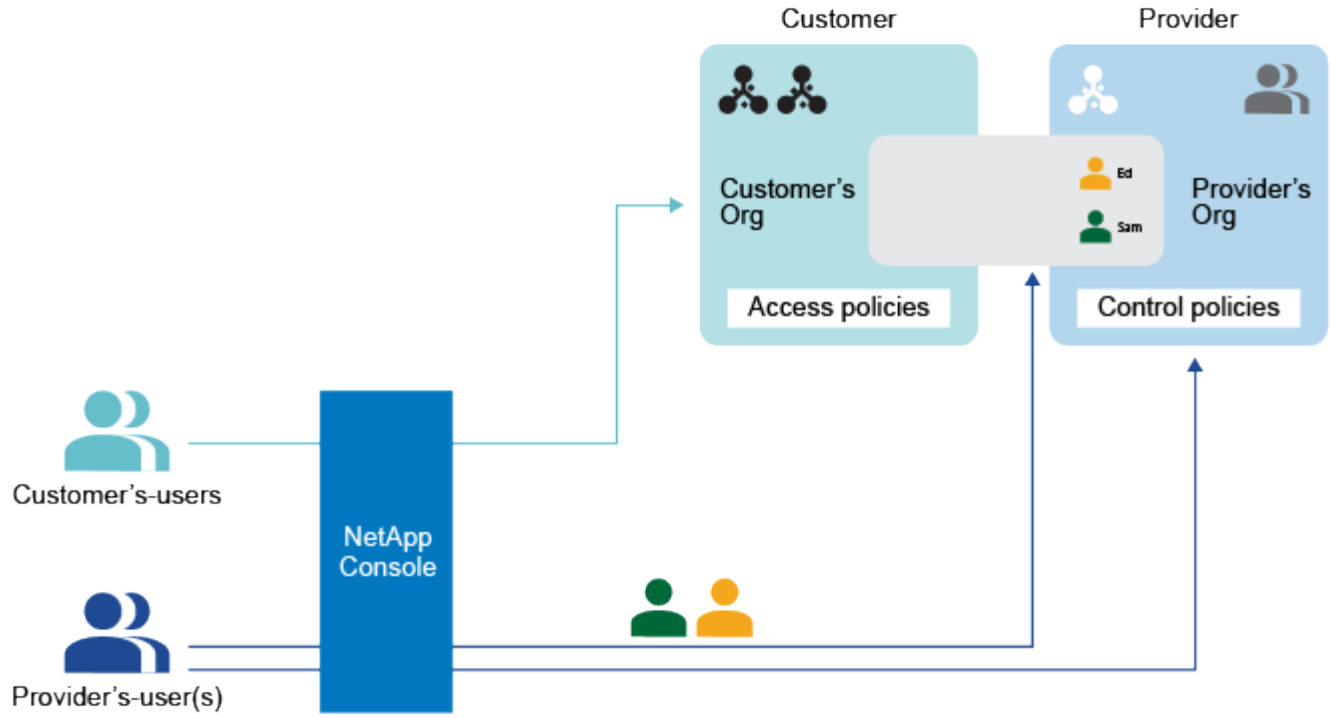
4 파트너십 승인

수신 기관은 요청을 수락해야 합니다.

수신 조직이란 리소스에 대한 접근 권한이 부여되는 조직입니다.

5 파트너십에 사용자 할당

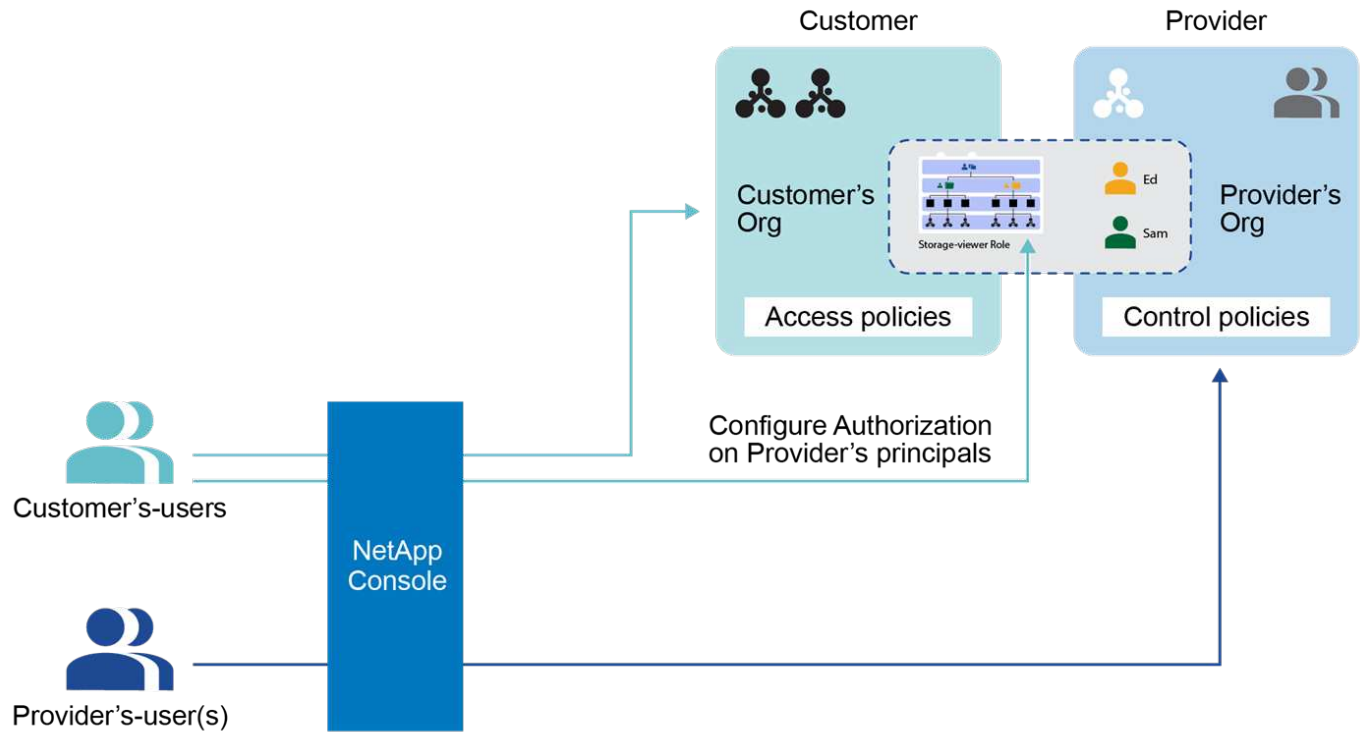
수신 조직은 귀하의 조직에서 특정 사용자나 서비스 계정을 파트너십에 할당합니다. 시작 조직은 이러한 사용자에게 역할을 할당합니다.



6 할당된 사용자에게 리소스에 대한 액세스 권한 부여

귀하가 시작 조직인 경우 파트너십에 할당된 사용자에게 특정 리소스에 대한 액세스 권한을 부여할 수 있습니다. 언제든지 접근을 취소할 수 있습니다.

조직 내의 특정 프로젝트나 폴더에 역할을 할당하여 이를 수행할 수 있습니다.



NetApp Console 에서 파트너십 관리

귀하의 조직과 신뢰할 수 있는 파트너 간에 안전하고 관리되는 연결을 구축하여 협업적인 NetApp 리소스 관리를 실현하기 위한 파트너십을 구축하세요.

파트너십을 통해 콘솔에서 역할 기반 관계를 통해 경계를 넘어 NetApp 리소스를 안전하게 관리할 수 있습니다. 시작 조직은 리소스에 대한 액세스 권한을 부여하는 반면, 수락 조직은 액세스 권한이 부여될 사용자 또는 서비스 계정을 제공합니다. 파트너십은 셀프 서비스 워크플로를 통해 구축되며, 이를 통해 시작한 조직은 어떤 리소스를 공유할지, 어떤 역할을 할당할지, 필요에 따라 파트너 액세스를 온보딩, 관리 또는 취소할 수 있는 권한을 완벽하게 제어할 수 있습니다.

필수 역할

파트너십 관리자 역할은 파트너십을 만들고 관리하는 데 필요합니다. *파트너십 뷰어*는 파트너십 페이지를 볼 수 있습니다."액세스 역할에 대해 자세히 알아보세요."

조직 파트너십을 시작하세요

다른 조직의 조직 ID를 알고 있다면 해당 조직과의 파트너십을 요청할 수 있습니다. 수신 기관이 요청을 승인해야만 파트너십이 진행됩니다.

시작하기 전에 파트너 조직의 조직 ID가 있는지 확인하고 파트너십 관리자 역할이 할당되었는지 확인하세요.

단계

1. *관리 > ID 및 액세스*를 선택합니다.
2. 파트너십 탭을 선택하세요.
3. *파트너십 추가*를 선택하세요.
4. 파트너십 생성 대화 상자에서 요청한 파트너의 파트너 조직 ID를 입력하고 *추가*를 선택합니다.

   파트너십 요청은 승인을 위해 파트너 조직에 전송됩니다. 파트너십 요청 상태는 파트너십 페이지에서 확인할 수 있습니다.

조직 파트너십 승인

파트너십을 진행하려면 조직 파트너십 요청이 수신 조직에서 승인되어야 합니다. 파트너십을 승인하고 관리하려면 파트너십 관리자 역할이 있어야 합니다.

단계

1. *관리 > ID 및 액세스*를 선택합니다.
2. *파트너십*을 선택하세요.
3. 파트너십 수신 탭을 선택하세요.
4. 승인하려는 수신된 파트너십으로 이동하여 선택하십시오. ••• 그런 다음 *승인*을 선택하세요.
5. 파트너십을 요청한 조직의 이름과 조직 ID를 포함한 파트너십 세부 정보를 검토하고 *다음*을 선택합니다.
6. 선택 사항으로, 파트너십에 조직 구성원을 추가하고 *적용*을 선택합니다.

   언제든지 파트너십 페이지를 통해 추가 멤버를 추가할 수 있습니다.

   추가한 모든 멤버는 파트너의 조직에 표시되며, 파트너는 해당 멤버를 리소스에 할당할 수 있습니다.

결과

승인하신 파트너십은 현재 설립됨 상태로 표시됩니다. 두 조직 중 하나에서 파트너십 관리자 또는 파트너십 뷰어 역할을 가진 사용자는 파트너십을 볼 수 있습니다.

파트너십 상태 보기

파트너십 상태를 확인하세요.

필수 역할

파트너십 관리자, 파트너십 뷰어."액세스 역할에 대해 자세히 알아보세요."

단계

1. *관리 > ID 및 액세스*를 선택합니다.
2. *파트너십*을 선택하세요.
3. 시작된 파트너십 또는 수신된 파트너십 탭을 선택하세요.
4. 파트너십과 해당 상태를 표시하는 해당 표를 검토하세요.

조직 파트너십 비활성화

파트너십을 비활성화하려면 해당 조직의 회원이어야 합니다. 파트너십을 비활성화하면 파트너 조직과 공유된 조직의 모든 리소스에 대한 액세스 권한이 즉시 취소됩니다.

필수 역할

파트너십 관리."액세스 역할에 대해 자세히 알아보세요."

단계

1. *관리 > ID 및 액세스*를 선택합니다.
2. *파트너십*을 선택하세요.
3. 시작된 파트너십 탭을 선택하세요.
4. 파트너십과 해당 상태를 표시하는 해당 표를 검토하세요.
5. 비활성화하려는 시작된 파트너십으로 이동하여 선택하십시오. ••• 그런 다음 *비활성화*를 선택하세요.

파트너십 조직의 회원 관리

파트너 조직에 사용자를 추가하여 파트너십에 사용자를 추가할 수 있습니다. 사용자를 추가한 후, 파트너 조직은 해당 조직 내 특정 리소스에 대한 역할을 사용자에게 할당해야 합니다.

필수 역할

파트너십 관리자 역할은 파트너십을 만들고 관리하는 데 필요합니다. *파트너십 뷰어*는 파트너십 페이지를 볼 수 있습니다."액세스 역할에 대해 자세히 알아보세요."

언제든지 파트너십에서 사용자를 제거할 수 있습니다. 파트너십에서 사용자를 제거하면 파트너 조직의 모든 리소스에 대한 액세스 권한이 즉시 취소됩니다.

파트너십에 멤버 추가

파트너십에 멤버를 추가하는 경우 파트너 조직의 *파트너십 관리자*가 멤버에게 해당 리소스에 대한 역할을 할당해야 해당 리소스에 액세스할 수 있습니다.

파트너십에 멤버를 추가하면 해당 멤버는 파트너 조직의 멤버로 표시되며, 파트너는 해당 멤버를 리소스에 할당할 수 있습니다.

단계

1. *관리 > ID 및 액세스*를 선택합니다.
2. *파트너십*을 선택하세요.
3. 파트너십 수신 탭을 선택하세요.
4. 작업 메뉴를 선택하세요 ••• 회원으로 추가하려는 기존 파트너십 옆에 있는 *회원 추가*를 선택하세요.
5. 파트너십에 추가할 멤버를 한 명 이상 선택하고 *추가*를 선택하세요.

파트너십에서 멤버 제거

언제든지 파트너십에서 멤버를 제거할 수 있습니다. 파트너십에서 사용자를 제거하면 파트너 조직의 모든 리소스에 대한 액세스 권한이 즉시 취소됩니다.

멤버의 역할이나 액세스할 수 있는 리소스를 조정하려면 파트너 조직의 파트너십 관리자가 해당 변경 작업을 수행해야 합니다.

단계

1. *관리 > ID 및 액세스*를 선택합니다.
2. *파트너십*을 선택하세요.
3. 파트너십 수신 탭을 선택하세요.
4. 작업 메뉴를 선택하세요 ••• 제거하려는 회원 옆에 있는 *연관 제거*를 선택하세요.
5. 대화 상자에서 *제거*를 선택하여 작업을 확인하세요.

사용자의 역할 정보 보기

사용자에게 할당된 역할과 관련 리소스를 볼 수 있습니다.

사용자와 연결된 역할은 변경할 수 없습니다. 리소스나 제공되는 역할에 대해 궁금한 사항이 있으면 파트너 조직의 관리자에게 문의하세요.

단계

1. *관리 > ID 및 액세스*를 선택합니다.
2. *파트너십*을 선택하세요.
3. 파트너십 수신 탭을 선택하세요.
4. 회원 페이지에서 테이블의 회원으로 이동하여 다음을 선택합니다. ••• 그런 다음 *세부정보 보기*를 선택하세요.
5. 표에서 멤버에게 할당된 역할을 보고 싶은 조직, 폴더 또는 프로젝트에 해당하는 행을 확장하고 역할 열에서 번호를 선택합니다.

파트너십 사용자에게 리소스 액세스 제공

조직 내 폴더와 프로젝트에 대한 특정 역할을 할당하여 파트너십 사용자에게 액세스 권한을 부여할 수 있습니다.

필수 역할

파트너십 관리."액세스 역할에 대해 자세히 알아보세요."

파트너 조직은 조직의 리소스에 대한 역할을 할당하기 전에 먼저 파트너십에 구성원을 추가해야 합니다."파트너십에 멤버를 추가하는 방법을 알아보세요."

파트너십 사용자의 역할 이해

파트너 조직의 구성원에 대한 역할은 자신의 역할과 동일한 방식으로 관리할 수 있습니다. 하지만 모든 역할을 파트너십 사용자가 사용할 수 있는 것은 아닙니다. 특히, 파트너 사용자에게 소프트웨어 업데이트를 허용하는 역할을 부여할 수 없습니다. ONTAP 소프트웨어를 업데이트하려면 일반적으로 네트워크에 직접 액세스해야 합니다.

파트너 사용자에게 다음 역할을 할당할 수 있습니다.

- "조직 관리자"
- "폴더 또는 프로젝트 관리자"
- "연방 관리자"
- "연방 뷰어"
- "백업 및 복구 관리자"
- "백업 뷰어"
- "관리자 복원"
- "관리자 복제"
- "재해 복구 관리"
- "재해 복구 장애 조치 관리자"
- "재해 복구 애플리케이션 관리자"
- "재해 복구 뷰어"
- "운영 지원 분석가"
- "분류 뷰어"

"미리 정의된 역할에 대해 자세히 알아보세요"

파트너 사용자에게 역할 추가

조직의 리소스에 대한 액세스 권한을 제공하려면 구성원에게 역할을 추가해야 합니다. 역할을 할당할 때는 하나의 리소스와 하나의 역할을 지정합니다. 사용자에게 두 개 이상의 역할을 할당할 수 있습니다.

예를 들어, 두 개의 프로젝트가 있고 동일한 사용자에게 두 프로젝트 모두의 백업 및 복구 관리자 역할을 부여하려면 각 프로젝트에 대한 사용자에게 해당 역할을 제공해야 합니다. 마찬가지로 동일한 프로젝트에 대해 사용자에게 두 가지 다른 역할을 제공하려면 각 역할을 별도로 할당해야 합니다.

단계

1. *관리 > ID 및 액세스*를 선택합니다.
2. *파트너십*을 선택하세요.
3. 파트너십 시작 탭을 선택하세요.
4. 작업 메뉴를 선택하세요 ••• 보고 싶은 기존 파트너십 옆에 있는 *세부정보 보기*를 선택하세요.

   회원 목록에는 파트너 조직이 파트너십에 추가한 회원이 표시됩니다.

5. 작업 메뉴를 선택하세요 ••• 역할을 할당하려는 구성원 옆에 있는 *역할 추가*를 선택합니다.
6. 역할을 추가하려면 대화 상자의 단계를 완료하세요.
   - 조직, 폴더 또는 프로젝트 선택: 멤버에게 권한이 부여되어야 하는 리소스 계층 수준을 선택합니다.

     조직이나 폴더를 선택하면 해당 구성원은 해당 조직이나 폴더 내에 있는 모든 항목에 대한 권한을 갖게 됩니다.

   - 카테고리 선택: 역할 카테고리를 선택하세요. "액세스 역할에 대해 알아보세요" .
   - 역할 선택: 선택한 조직, 폴더 또는 프로젝트와 관련된 리소스에 대한 권한을 멤버에게 제공하는 역할을 선택합니다.
   - 역할 추가: 조직 내 추가 폴더나 프로젝트에 대한 액세스 권한을 제공하려면 *역할 추가*를 선택하고 다른 폴더나 프로젝트 또는 역할 범주를 지정한 다음 역할 범주와 해당 역할을 선택합니다.
7. *새로운 역할 추가*를 선택하세요.

파트너 사용자의 역할 변경 또는 제거

파트너 조직의 구성원에게 할당한 역할을 변경하거나 제거할 수 있습니다.

단계

1. *관리 > ID 및 액세스*를 선택합니다.
2. *파트너십*을 선택하세요.
3. 파트너십 시작 탭을 선택하세요.
4. 작업 메뉴를 선택하세요 ••• 보고 싶은 기존 파트너십 옆에 있는 *세부정보 보기*를 선택하세요.

   회원 목록에는 파트너 조직이 파트너십에 추가한 회원이 표시됩니다.

5. 회원 페이지에서 테이블의 회원으로 이동하여 다음을 선택합니다. ••• 그런 다음 *세부정보 보기*를 선택하세요.
6. 표에서 멤버에게 할당된 역할을 변경하려는 조직, 폴더 또는 프로젝트에 해당하는 행을 확장하고 역할 열에서 *보기*를 선택하여 이 멤버에게 할당된 역할을 확인합니다.
7. 멤버의 기존 역할을 변경하거나 역할을 제거할 수 있습니다.
   a. 멤버의 역할을 변경하려면 변경하려는 역할 옆에 있는 *변경*을 선택하세요. 동일한 역할 범주 내에서만 역할을 변경할 수 있습니다. 예를 들어, 한 데이터 서비스 역할에서 다른 역할로 변경할 수 있습니다. 변경 사항을 확인하세요.
   b. 멤버의 역할을 해제하려면 다음을 선택하세요. 🗑 역할 옆에 있는 버튼을 클릭하면 해당 멤버에게서 해당 역할을 제거할 수 있습니다. 삭제를 확인하라는 메시지가 표시됩니다.

파트너 조직에서 일하다

파트너 조직에서 역할을 맡게 되면 해당 조직으로 전환하여 수행 권한이 있는 작업을 수행할 수 있습니다.

조직 메뉴를 사용하면 자신의 조직과 액세스 권한이 있는 파트너 조직 간에 전환할 수 있습니다."조직 및 프로젝트 전환에 대해 자세히 알아보세요."

파트너 조직에서 공유된 리소스를 확인하고, 할당된 역할에 따라 작업을 수행할 수 있습니다. 파트너십 관리자와 협력하여 액세스해야 하는 리소스에 대한 적절한 역할을 맡고 있는지 확인하세요.

NetApp Console 작업 모니터링

콘솔이 수행하는 작업 상태를 모니터링하여 해결해야 할 문제가 있는지 확인할 수 있습니다. 감사 페이지나 알림 센터에서 상태를 확인하거나 이메일로 알림을 받을 수 있습니다.

이 표에서는 감사 페이지와 알림 센터의 기능을 비교하여 강조합니다.

알림 센터	감사 페이지
이벤트 및 작업에 대한 높은 수준의 상태를 표시합니다.	추가 조사를 위해 각 이벤트 또는 작업에 대한 세부 정보를 제공합니다.
현재 로그인 세션의 상태를 표시합니다(로그오프 후에는 알림 센터에 정보가 나타나지 않습니다)	지난 달의 상태를 유지합니다.
사용자 인터페이스에서 시작된 작업만 표시합니다.	UI 또는 API의 모든 작업을 표시합니다.
사용자가 시작한 작업을 표시합니다.	사용자가 시작한 작업이나 시스템에서 시작한 작업을 모두 표시합니다.
중요도에 따라 결과 필터링	서비스, 작업, 사용자, 상태 등으로 필터링
사용자 및 다른 사람들에게 이메일로 알림을 보내는 기능을 제공합니다.	이메일 기능이 없습니다

감사 페이지에서 사용자 활동을 감사하세요

감사 페이지를 사용하여 누가 작업을 수행했는지 또는 작업의 상태를 식별합니다.

감사 페이지에서는 사용자가 조직이나 계정을 관리하기 위해 완료한 작업을 보여줍니다. 여기에는 사용자 연결, 시스템 생성, 에이전트 생성 등의 관리 작업이 포함됩니다.

또한 누가 조직에 구성원을 추가했는지 또는 프로젝트가 성공적으로 삭제되었는지 확인할 수 있습니다.

단계

1. *관리 > 감사*를 선택합니다.
2. 표 위에 있는 필터를 사용하여 표에 표시되는 작업을 변경하세요.

   예를 들어, 서비스 필터를 사용하여 특정 서비스와 관련된 작업을 표시하거나, 사용자 필터를 사용하여 특정 사용자 계정과 관련된 작업을 표시할 수 있습니다.

감사 페이지에서 감사 로그를 다운로드하세요

감사 페이지에서 감사 로그를 CSV 파일로 다운로드할 수 있습니다. 이를 통해 조직 내에서 사용자가 수행하는 작업을 기록할 수 있습니다. CSV 파일에는 감사 페이지에 표시된 열이나 필터에 관계없이 다운로드한 CSV 파일의 모든 열이 포함됩니다.

단계

1. 감사 페이지에서 표의 오른쪽 상단에 있는 다운로드 아이콘을 선택하세요.

알림 센터를 사용하여 활동 모니터링

알림은 콘솔 작업을 추적하여 성공 여부를 확인합니다. 이를 통해 현재 로그인 세션 동안 시작한 많은 콘솔 작업의 상태를 볼 수 있습니다. 모든 콘솔 서비스가 알림 센터에 정보를 보고하는 것은 아닙니다.

알림 벨( )을 선택하면 알림을 표시할 수 있습니다. ) 메뉴 표시줄에서. 종 모양의 작은 거품의 색상은 활성화된 가장 높은 수준의 심각도 알림을 나타냅니다. 따라서 빨간색 거품이 보인다면 꼭 확인해야 할 중요한 알림이 있다는 의미입니다.

또한 콘솔을 구성하여 특정 유형의 알림을 이메일로 보내면 시스템에 로그인하지 않은 상태에서도 중요한 시스템 활동에 대한 정보를 받을 수 있습니다. 이메일은 귀하의 조직에 속한 모든 사용자나 특정 유형의 시스템 활동을 알아야 하는 다른 수신자에게 보낼 수 있습니다. 방법을 확인하세요이메일 알림 설정 .

알림 센터와 경고 비교

알림 센터를 사용하면 시작한 작업의 상태를 보고 특정 유형의 시스템 활동에 대한 알림을 설정할 수 있습니다. 알림을 통해 ONTAP 스토리지 환경에서 용량, 가용성, 성능, 보호 및 보안과 관련된 문제나 잠재적 위험을 확인할 수 있습니다.

"NetApp Console 알림에 대해 자세히 알아보세요"

알림 유형

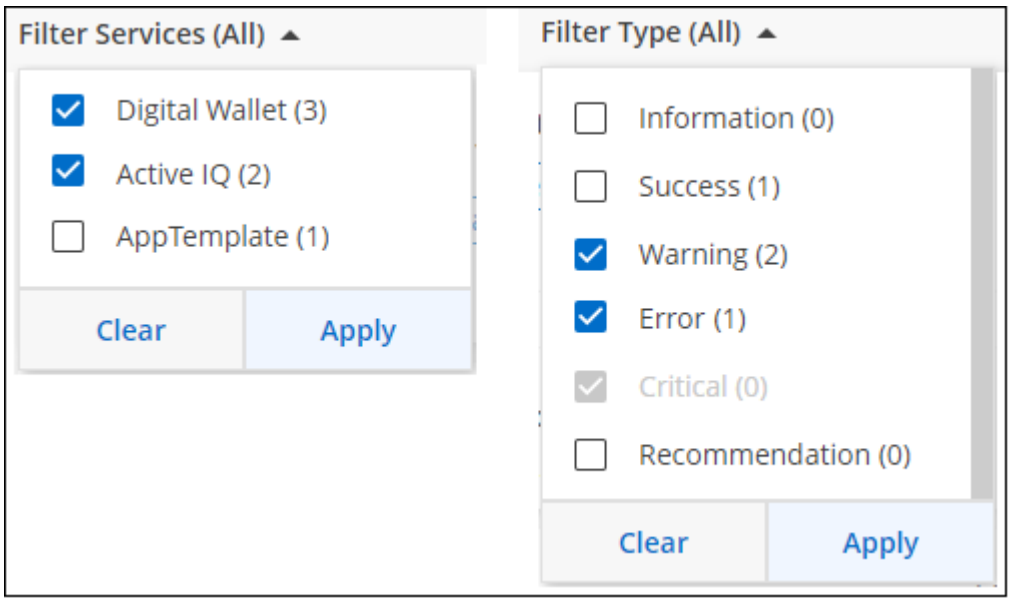
콘솔은 알림을 다음 범주로 분류합니다.

알림 유형	설명
비판적인	즉각적인 시정 조치를 취하지 않으면 서비스 중단으로 이어질 수 있는 문제가 발생했습니다.
오류	어떤 행동이나 과정이 실패로 끝났거나, 시정 조치를 취하지 않으면 실패로 이어질 수 있습니다.
경고	심각한 수준에 이르지 않도록 주의해야 할 문제입니다. 이 정도 심각도의 알림은 서비스 중단을 일으키지 않으며, 즉각적인 시정 조치가 필요하지 않을 수도 있습니다.
추천	시스템이나 특정 서비스를 개선하기 위한 조치를 취하도록 권장하는 시스템입니다. 예를 들어, 비용 절감, 새로운 서비스에 대한 제안, 권장되는 보안 구성 등이 있습니다.
정보	작업이나 프로세스에 대한 추가 정보를 제공하는 메시지입니다.
성공	작업이나 프로세스가 성공적으로 완료되었습니다.

알림 필터링

기본적으로 모든 활성 알림은 알림 센터에서 볼 수 있습니다. 중요한 알림만 표시되도록 알림을 필터링할 수 있습니다.

"서비스" 및 "알림 유형"별로 필터링할 수 있습니다.



예를 들어, 콘솔 작업에 대해 "오류" 및 "경고" 알림만 보고 싶은 경우 해당 항목을 선택하면 해당 유형의 알림만 표시됩니다.

알림 해제

더 이상 알림을 볼 필요가 없다면 페이지에서 알림을 제거할 수 있습니다. 알림을 개별적으로 또는 한꺼번에 해제할 수 있습니다.

모든 알림을 해제하려면 알림 센터에서 다음을 선택하세요. 그리고 *모두 닫기*를 선택하세요.

개별 알림을 해제하려면 알림 위에 커서를 올려놓고 *해제*를 선택하세요.

이메일 알림 설정

로그인하지 않아도 중요한 시스템 활동에 대한 알림을 받을 수 있도록 특정 유형의 알림을 이메일로 보낼 수 있습니다. 조직이나 계정에 속한 모든 사용자 또는 특정 유형의 시스템 활동을 알아야 하는 다른 수신자에게 이메일을 보낼 수 있습니다.

- 콘솔은 에이전트, 라이선스 및 구독, NetApp Copy and Sync, NetApp Backup and Recovery 대한 이메일 알림을 보냅니다.
- 인터넷 접속이 불가능한 사이트에 콘솔 에이전트가 설치된 경우 이메일 알림을 보내는 기능은 지원되지 않습니다.

알림 센터에서 설정한 필터는 이메일로 받는 알림 유형을 결정하지 않습니다. 기본적으로 모든 조직 관리자는 모든 "중요" 및 "권장 사항" 알림에 대한 이메일을 받게 됩니다. 이러한 알림은 모든 서비스에 적용됩니다. 에이전트나 NetApp Backup and Recovery 등 특정 서비스에 대해서만 알림을 받도록 선택할 수는 없습니다.

다른 모든 사용자와 수신자는 알림 이메일을 받지 않도록 구성되어 있습니다. 따라서 추가 사용자에 대한 알림 설정을 구성해야 합니다.

알림 설정을 사용자 지정하려면 조직 관리자 역할이 있어야 합니다.

단계

1. *관리 > 알림 설정*을 선택하세요.
2. 조직 사용자 또는 *추가 수신자*를 선택하세요.

   추가 수신자 페이지를 사용하면 콘솔 조직의 구성원에게 알림을 보내도록 콘솔을 구성할 수 있습니다.

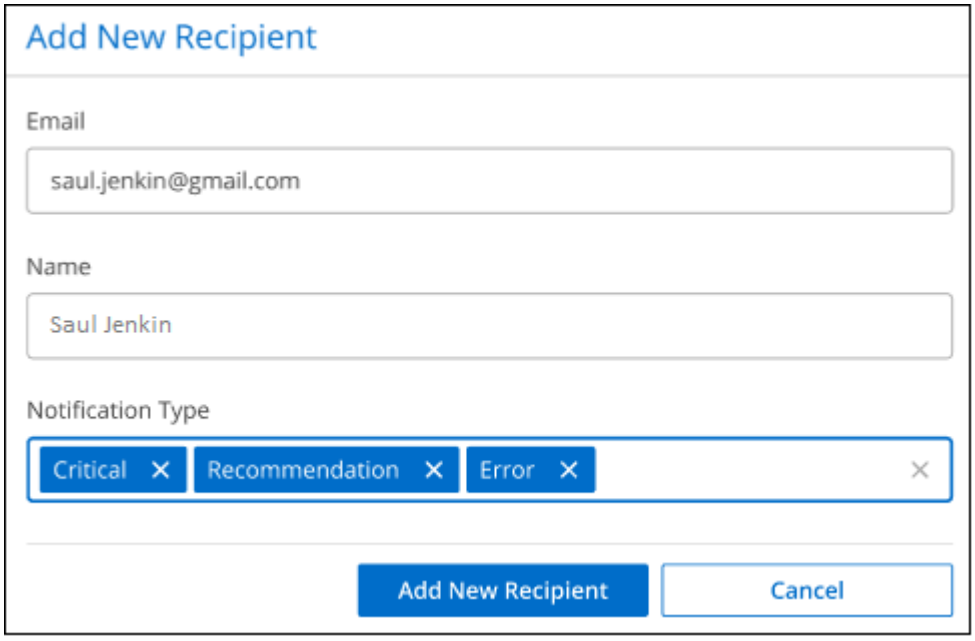
3. 조직 사용자 페이지나 추가 수신자 페이지에서 사용자 한 명 또는 여러 명을 선택하고, 보낼 알림 유형을 선택합니다.
   - 단일 사용자에 대한 변경 사항을 적용하려면 해당 사용자의 알림 열에서 메뉴를 선택하고, 보낼 알림 유형을 선택한 다음 *적용*을 선택합니다.
   - 여러 사용자에 대한 변경 사항을 적용하려면 각 사용자에 대한 상자를 선택하고, *이메일 알림 관리*를 선택하고, 보낼 알림 유형을 선택한 후 *적용*을 선택합니다.

추가 이메일 수신자 추가

조직 사용자 페이지에 나타나는 사용자는 조직이나 계정의 사용자 중에서 자동으로 채워집니다. 콘솔에 액세스할 수 없지만 특정 유형의 경고 및 알림에 대한 알림을 받아야 하는 다른 사람이나 그룹의 이메일 주소를 추가 수신자 페이지에 추가할 수 있습니다.

단계

1. 알림 설정 페이지에서 *새 수신자 추가*를 선택합니다.



2. 이름, 이메일 주소를 입력하고, 수신자가 받을 알림 유형을 선택한 후 *새 수신자 추가*를 선택합니다.