



시작하기

NetApp Console setup and administration

NetApp
January 27, 2026

목차

시작하기	1
기본을 배우세요	1
NetApp Console 에 대해 알아보세요	1
NetApp Console 배포 모드에 대해 알아보세요	4
NetApp Console 과 관련된 NSS 자격 증명 관리	11
NetApp Console 에이전트에 대해 알아보세요	14
NetApp Console ID 및 액세스 관리에 대해 알아보세요	18
NetApp Console (SaaS) 시작하기	22
시작하기 워크플로(SaaS)	22
NetApp Console 대한 네트워크 액세스 준비	24
NetApp Console에 가입하거나 로그인하세요	26
NetApp Console 어시스턴트를 사용하여 시작하세요	27
NetApp Console 시작하기(제한 모드)	28
시작하기 워크플로(제한 모드)	28
제한 모드에서 배포 준비	28
제한 모드로 콘솔 에이전트 배포	48
NetApp Intelligent Services 구독(제한 모드)	59
다음에 할 수 있는 일(제한 모드)	65
비공개 모드 시작하기	65
시작하기 워크플로(BlueXP 개인 모드)	65

시작하기

기본을 배우세요

NetApp Console에 대해 알아보세요

콘솔은 통합 데이터 서비스를 통해 하이브리드 멀티 클라우드 전반의 스토리지 관리 및 보호를 통합하여 데이터를 보호하고 최적화합니다.

이 솔루션은 서비스형 소프트웨어(SaaS) 플랫폼으로 제공되거나, 자체 클라우드에 설치하여 사용할 수 있는 셀프 호스팅 옵션으로 제공됩니다. 이 시스템은 스토리지 관리, 데이터 이동성, 데이터 보호, 데이터 분석 및 제어 기능을 제공합니다. 관리 기능은 웹 기반 콘솔과 API를 통해 제공됩니다.

중앙 집중식 스토리지 관리

콘솔을 사용하여 클라우드 및 온프레미스 스토리지를 검색, 배포 및 관리하세요.

지원되는 클라우드 및 온프레미스 스토리지

콘솔에서 다음 유형의 저장소를 관리할 수 있습니다.

클라우드 스토리지 솔루션

- Amazon FSx for NetApp ONTAP
- Azure NetApp Files
- Cloud Volumes ONTAP
- Google Cloud NetApp Volumes

온프레미스 플래시 및 객체 스토리지

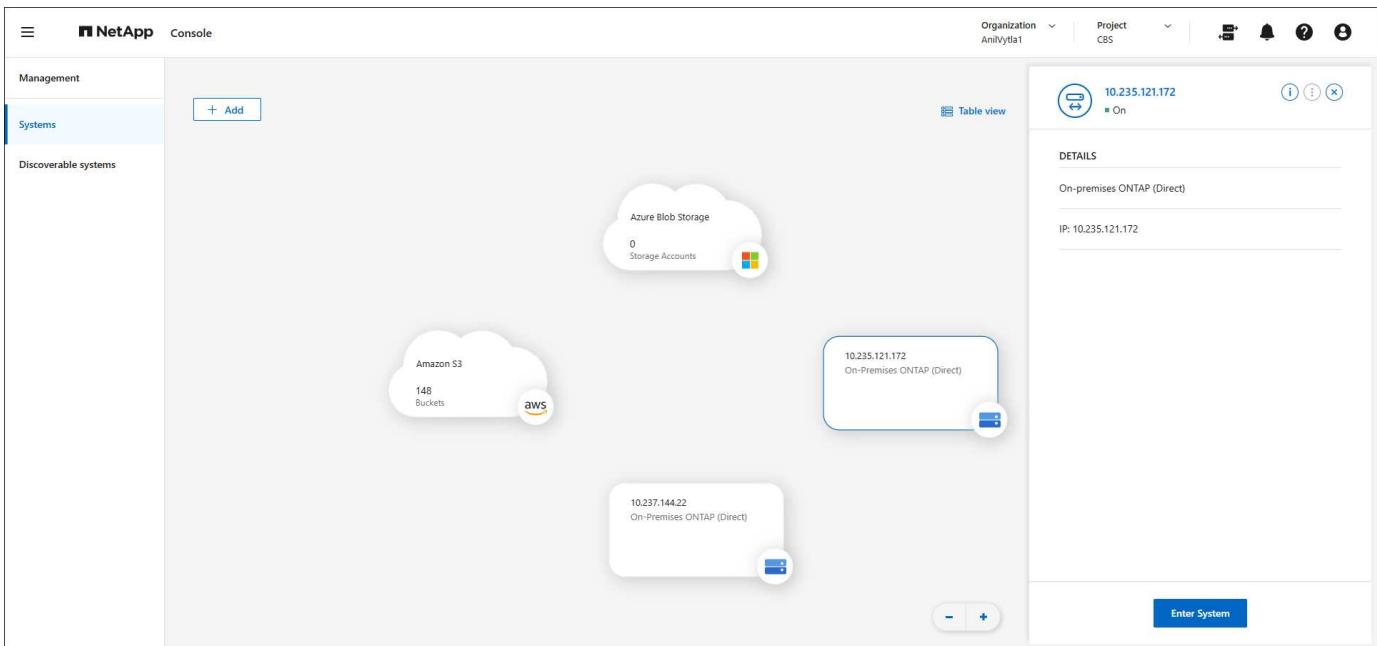
- E-시리즈 시스템
- ONTAP 클러스터
- StorageGRID 시스템

클라우드 객체 스토리지

- Amazon S3 스토리지
- Azure Blob 저장소
- 구글 클라우드 스토리지

스토리지 관리

콘솔 내에서 시스템은 검색되거나 배포된 저장소를 나타냅니다. NetApp 데이터 서비스와 통합하거나 볼륨을 추가하는 등 스토리지를 관리할 시스템을 선택할 수 있습니다.



데이터를 보호, 보안 및 최적화하기 위한 통합 데이터 서비스 및 스토리지 관리

콘솔은 저장 공간 가용성을 보호하고 유지하기 위한 데이터 서비스를 제공합니다.

저장 알림

ONTAP 환경에서 용량, 가용성, 성능, 보호 및 보안과 관련된 문제를 확인하세요.

자동화 허브

스크립트 솔루션을 사용하여 NetApp 제품과 서비스의 배포 및 통합을 자동화합니다.

NetApp Backup and Recovery

클라우드 및 온프레미스 데이터를 백업하고 복원합니다.

NetApp Data Classification

애플리케이션 데이터와 클라우드 환경의 개인정보 보호를 준비하세요.

NetApp Copy and Sync

온프레미스와 클라우드 데이터 저장소 간에 데이터를 동기화합니다.

NetApp 디지털 어드바이저(Active IQ)

예측 분석과 사전 예방적 지원을 활용해 데이터 인프라를 최적화하세요.

Licenses and subscriptions

라이센스와 구독을 관리하고 모니터링하세요.

NetApp Disaster Recovery

Amazon FSx for ONTAP 의 VMware Cloud를 재해 복구 사이트로 사용하여 온프레미스 VMware 워크로드를 보호합니다.

수명주기 계획

현재 또는 예상 용량이 부족한 클러스터를 식별하고 데이터 계층화 또는 추가 용량 권장 사항을 구현합니다.

NetApp Ransomware Resilience

랜섬웨어 공격으로 이어질 수 있는 이상을 감지합니다. 작업 부하를 보호하고 복구합니다.

NetApp Replication

백업 및 재해 복구를 지원하기 위해 저장 시스템 간에 데이터를 복제합니다.

소프트웨어 업데이트

ONTAP 업그레이드의 평가, 계획 및 실행을 자동화합니다.

지속 가능성 대시보드

저장 시스템의 지속 가능성을 분석합니다.

NetApp Cloud Tiering

온프레미스 ONTAP 스토리지를 클라우드로 확장하세요.

NetApp Volume Caching

데이터 액세스 속도를 높이거나 액세스 빈도가 높은 볼륨의 트래픽을 오프로드하려면 쓰기 가능한 캐시 볼륨을 만듭니다.

NetApp 워크로드

Amazon FSx for NetApp ONTAP 사용하여 주요 워크로드를 설계, 설정 및 운영합니다.

"[NetApp Console](#) 과 사용 가능한 데이터 서비스에 대해 자세히 알아보세요."

지원되는 클라우드 제공업체

콘솔을 사용하면 Amazon Web Services, Microsoft Azure, Google Cloud에서 클라우드 스토리지를 관리하고 클라우드 서비스를 사용할 수 있습니다.

비용

NetApp Console에는 비용이 없습니다. 클라우드에 콘솔 에이전트를 배포하거나 클라우드에 배포된 제한 모드를 사용하는 경우 비용이 발생합니다. 일부 NetApp 데이터 서비스에는 비용이 발생합니다.<https://bluexp.netapp.com/pricing>["NetApp 데이터 서비스 가격에 대해 알아보세요"]

NetApp Console 작동 방식

NetApp Console은 SaaS 계층을 통해 제공되는 웹 기반 콘솔로, 리소스 및 액세스 관리 시스템, 스토리지 시스템을 관리하고 NetApp 데이터 서비스를 활성화하는 콘솔 에이전트, 그리고 비즈니스 요구 사항을 충족하는 다양한 배포 모드를 제공합니다.

서비스로서의 소프트웨어

콘솔에 액세스하려면 다음을 수행합니다. "[웹 기반 인터페이스](#)" 및 API. 이 SaaS 환경을 이용하면 최신 기능이 출시되면 자동으로 액세스할 수 있습니다.

ID 및 액세스 관리(IAM)

콘솔은 리소스 및 액세스 관리를 위한 ID 및 액세스 관리(IAM)를 제공합니다. 이 IAM 모델은 리소스와 권한에 대한 세부적인 관리를 제공합니다.

- 최상위 _조직_을 사용하면 다양한 _프로젝트_에 대한 액세스를 관리할 수 있습니다.
- _폴더_를 사용하면 관련 프로젝트를 함께 그룹화할 수 있습니다.
- 리소스 관리를 통해 리소스를 하나 이상의 폴더 또는 프로젝트와 연결할 수 있습니다.
- 액세스 관리를 통해 조직 계층의 다양한 수준에서 멤버에게 역할을 할당할 수 있습니다.
- "[NetApp Console에서 IAM에 대해 자세히 알아보세요](#)"

콘솔 에이전트

일부 추가 기능과 데이터 서비스를 사용하려면 콘솔 에이전트가 필요합니다. 온프레미스와 클라우드 환경 전반에서 리소스와 프로세스를 관리할 수 있습니다. 일부 시스템(예: Cloud Volumes ONTAP)을 관리하고 일부 NetApp 데이터 서비스를 사용하려면 필요합니다.

["콘솔 에이전트에 대해 자세히 알아보세요"](#).

SaaS와 주권 클라우드 배포 비교

NetApp Console SaaS 제품에 가입하거나 자체 클라우드에 배포하여 사용을 시작할 수 있습니다. NetApp Console 독립형 클라우드에 배포하면 NetApp 조직의 보안 및 규정 준수 요구 사항을 충족하기 위해 아웃바운드 연결을 제한합니다. 콘솔을 주권 클라우드에 배포할 경우 모든 기능과 서비스를 사용할 수 있는 것은 아닙니다.

NetApp 외부 연결이 필요 없는 사이트를 위해 BlueXP 계속해서 제공합니다. BlueXP 외부 연결 없이 네트워크에 설치할 수 있습니다. ["인터넷 연결이 없는 사이트를 위한 BlueXP\(비공개 모드\)에 대해 알아보세요."](#)

["배포 모드에 대해 자세히 알아보세요"](#).

SOC 2 유형 2 인증

독립 공인회계사 회사와 서비스 감사원이 콘솔을 조사하여 해당 신탁 서비스 기준에 따라 SOC 2 유형 2 보고서를 달성했다고 확인했습니다.

["NetApp의 SOC 2 보고서 보기"](#)

NetApp Console 배포 모드에 대해 알아보세요

NetApp Console 비즈니스 및 보안 요구 사항을 충족할 수 있는 다양한 _배포 모드_를 제공합니다.

- 표준 모드는 SaaS(Software as a Service) 계층을 활용하여 모든 기능을 제공합니다. 사용자는 웹 기반 호스팅 인터페이스를 통해 콘솔에 액세스합니다.
- 제한 모드는 연결 제한이 있는 조직에서 자체 퍼블릭 클라우드에 NetApp Console 설치하려는 경우에 사용할 수 있습니다. 사용자는 클라우드 환경의 콘솔 에이전트에 호스팅된 웹 기반 인터페이스를 통해 콘솔에 액세스합니다.

NetApp Console 제한 모드에서 트래픽, 통신 및 데이터를 제한하며, 환경(온프레미스 및 클라우드)이 필수 규정을 준수하는지 확인해야 합니다.

개요

각 배포 모드는 아웃바운드 연결, 위치, 설치, 인증, 데이터 서비스 및 요금 청구 방법이 다릅니다.

표준 모드

웹 기반 콘솔에서 SaaS 서비스를 사용합니다. 사용하려는 데이터 서비스와 기능에 따라 Console 조직 관리자는 하이브리드 클라우드 환경 내의 데이터를 관리하기 위해 하나 이상의 Console 에이전트를 만듭니다.

이 모드는 공개 인터넷을 통해 암호화된 데이터 전송을 사용합니다.

제한 모드

클라우드(정부, 주권 또는 상업 지역)에 콘솔 에이전트를 설치하면 NetApp Console SaaS 계층에 대한 아웃바운드 연결이 제한됩니다.

이 모드는 일반적으로 주 및 지방 정부와 규제 대상 회사에서 사용됩니다.

[SaaS 계층에 대한 아웃바운드 연결에 대해 자세히 알아보세요 .](#)

BlueXP 개인 모드(레거시 BlueXP 인터페이스만 해당)

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

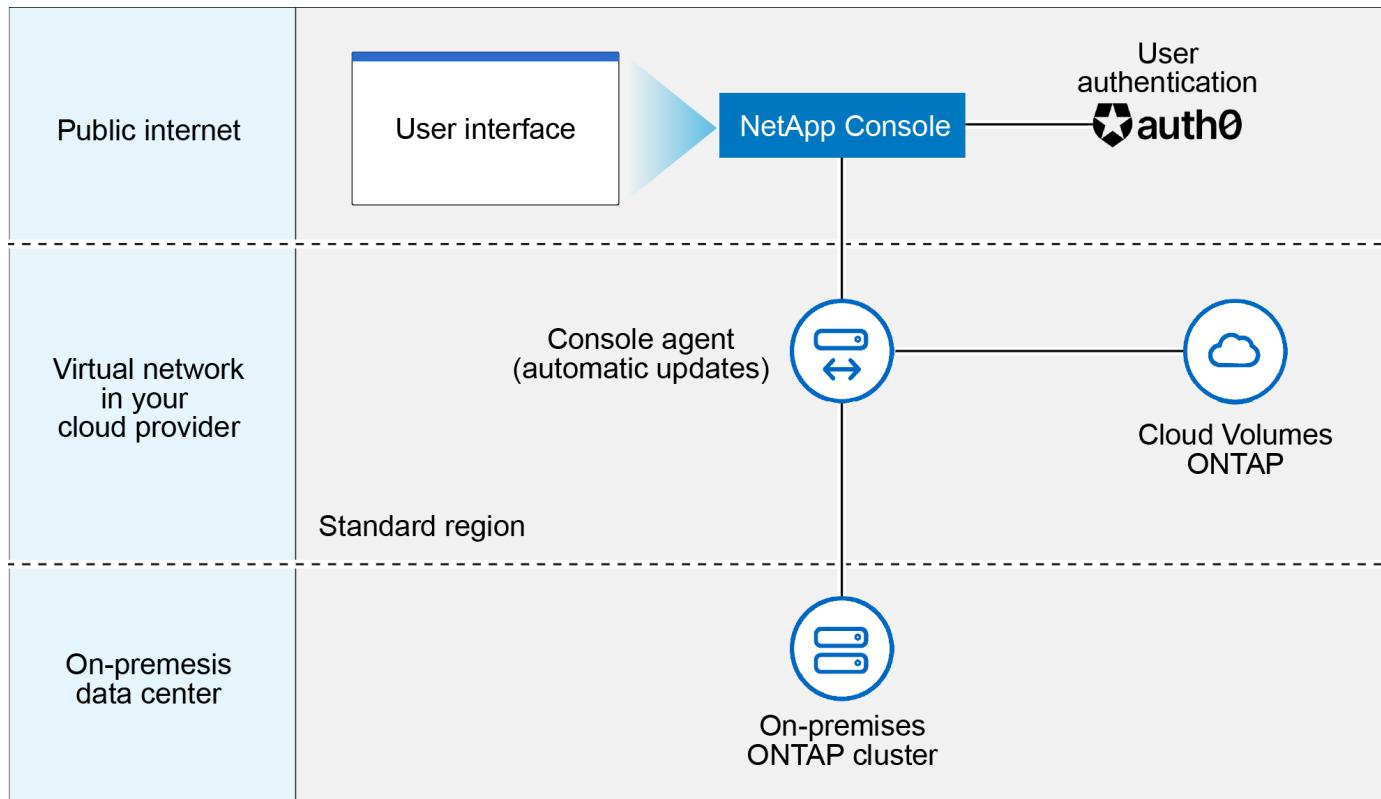
다음 표는 NetApp 콘솔을 비교한 것입니다.

	표준 모드	제한 모드
NetApp Console SaaS 계층에 연결이 필요합니까?	예	아웃바운드 전용
클라우드 공급자에 연결해야 합니까?	예	네, 지역 내에서요
콘솔 에이전트 설치	콘솔, 클라우드 마켓플레이스 또는 수동 설치에서	클라우드 마켓플레이스 또는 수동 설치
콘솔 에이전트 업그레이드	자동 업그레이드	자동 업그레이드
UI 접근	콘솔 SaaS 계층에서	에이전트 VM에서 로컬로
API 엔드포인트	콘솔 SaaS 계층	콘솔 에이전트
입증	auth0, NSS 로그인 또는 ID 연합을 사용하여 SaaS를 통해	auth0 또는 ID 연합을 사용하는 SaaS를 통해
다중 요소 인증	로컬 사용자 사용 가능	사용할 수 없음
저장 및 데이터 서비스	모두 지원됩니다	많은 사람들이 지원받습니다
데이터 서비스 라이선스 옵션	마켓플레이스 구독 및 BYOL	마켓플레이스 구독 및 BYOL

다음 섹션을 읽어 이러한 모드에 대해 자세히 알아보세요. 여기에는 어떤 NetApp Console 기능과 서비스가 지원되는지도 포함됩니다.

표준 모드

다음 이미지는 표준 모드 배포의 예입니다.



콘솔은 표준 모드에서 다음과 같이 작동합니다.

아웃바운드 커뮤니케이션

콘솔 에이전트에서 콘솔 SaaS 계층, 클라우드 공급자의 공개적으로 사용 가능한 리소스 및 일상 운영에 필수적인 기타 구성 요소로의 연결이 필요합니다.

- ["AWS에서 에이전트가 접속하는 엔드포인트"](#)
- ["Azure에서 에이전트가 연락하는 엔드포인트"](#)
- ["Google Cloud에서 에이전트가 연락하는 엔드포인트"](#)

에이전트 지원 위치

표준 모드에서는 에이전트가 클라우드나 고객사 내에서 지원됩니다.

콘솔 에이전트 설치

다음 방법 중 하나를 사용하여 에이전트를 설치할 수 있습니다.

- 콘솔에서
- AWS 또는 Azure Marketplace에서
- Google Cloud SDK에서
- 데이터 센터 또는 클라우드의 Linux 호스트에서 설치 프로그램을 수동으로 사용
- 제공된 OVA를 VCenter 환경에서 사용하세요.

콘솔 에이전트 업그레이드

NetApp 매달 자동으로 에이전트를 업그레이드합니다.

사용자 인터페이스 접근

사용자 인터페이스는 SaaS 계층을 통해 제공되는 웹 기반 콘솔에서 접근할 수 있습니다.

API 엔드포인트

API 호출은 다음 엔드포인트에 대해 수행됩니다: \ <https://api.bluexp.netapp.com>

입증

auth0 또는 NetApp 지원 사이트(NSS) 로그인을 통한 인증. ID 연합을 사용할 수 있습니다.

지원되는 데이터 서비스

모든 NetApp 데이터 서비스가 지원됩니다. ["NetApp 데이터 서비스에 대해 자세히 알아보세요"](#).

지원되는 라이센스 옵션

마켓플레이스 구독과 BYOL은 표준 모드에서 지원됩니다. 그러나 지원되는 라이선스 옵션은 사용 중인 NetApp 데이터 서비스에 따라 달라집니다. 각 서비스에 대한 설명서를 검토하여 사용 가능한 라이선스 옵션에 대해 자세히 알아보세요.

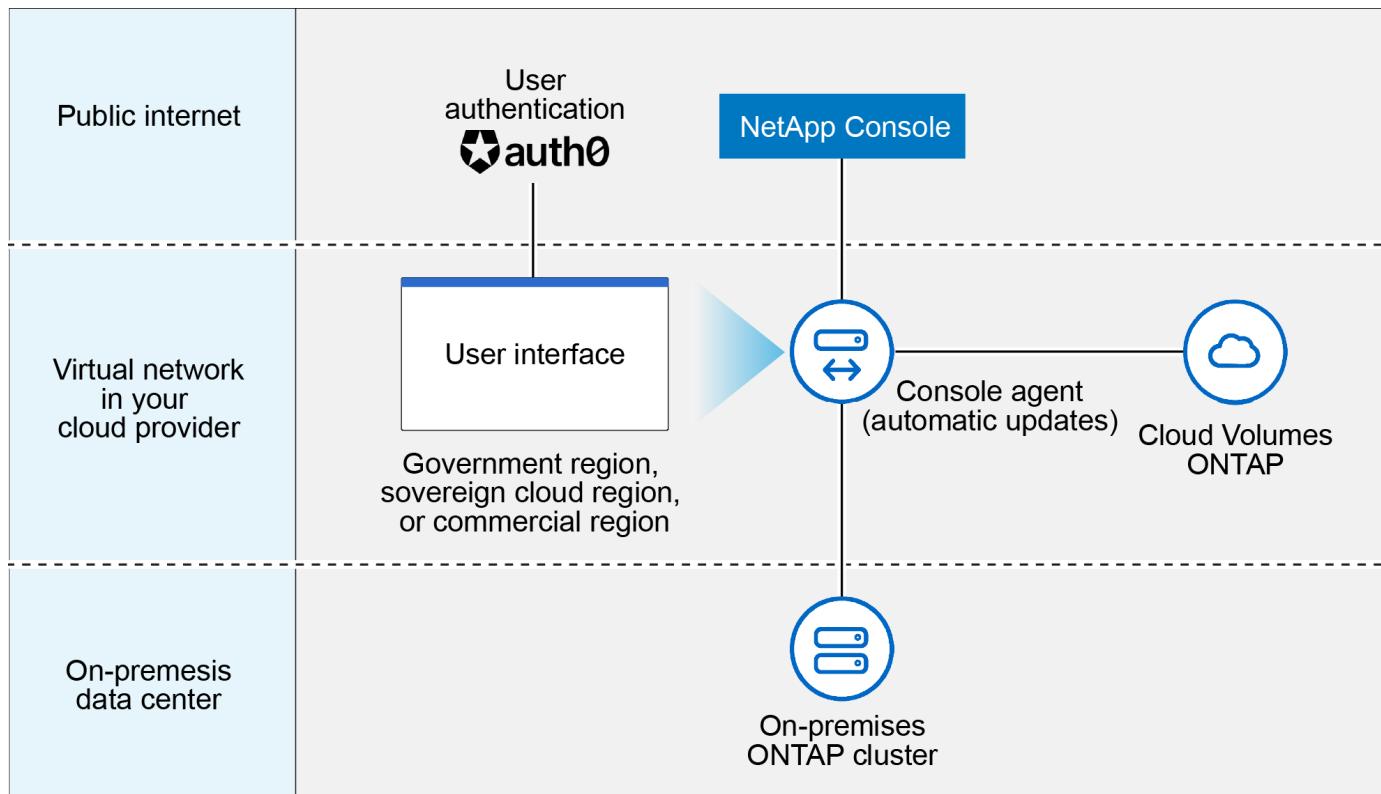
표준 모드를 시작하는 방법

로 가다 ["NetApp Console"](#) 그리고 가입하세요.

["표준 모드를 시작하는 방법을 알아보세요"](#).

제한 모드

다음 이미지는 제한 모드 배포의 예입니다.



제한 모드에서 콘솔은 다음과 같이 작동합니다.

아웃바운드 커뮤니케이션

에이전트는 데이터 서비스, 소프트웨어 업그레이드, 인증 및 메타데이터 전송을 위해 콘솔 SaaS 계층에 대한 아웃바운드 연결이 필요합니다.

콘솔 SaaS 계층은 에이전트와의 통신을 시작하지 않습니다. 에이전트는 콘솔 SaaS 계층과의 모든 통신을 시작하여 필요에 따라 데이터를 가져오거나 푸시합니다.

해당 지역 내에서 클라우드 공급자 리소스에 대한 연결도 필요합니다.

에이전트 지원 위치

제한 모드에서는 에이전트가 정부 지역, 주권 지역 또는 상업 지역의 클라우드에서 지원됩니다.

콘솔 에이전트 설치

AWS 또는 Azure Marketplace에서 설치하거나, Linux 호스트에 수동으로 설치하거나, VCenter 환경에서 다운로드 가능한 OVA를 사용할 수 있습니다.

콘솔 에이전트 업그레이드

NetApp 매월 업데이트를 통해 에이전트 소프트웨어를 자동으로 업그레이드합니다.

사용자 인터페이스 접근

사용자 인터페이스는 클라우드 지역에 배포된 에이전트 가상 머신에서 접근할 수 있습니다.

API 엔드포인트

API 호출은 에이전트 가상 머신에 이루어집니다.

입증

인증은 auth0을 통해 제공됩니다. ID 연합도 사용 가능합니다.

지원되는 스토리지 관리 및 데이터 서비스

제한 모드가 적용된 다음 저장소 및 데이터 서비스:

지원되는 서비스	노트
Azure NetApp Files	전면적인 지원
백업 및 복구	제한 모드가 적용된 정부 지역 및 상업 지역에서 지원됩니다. 제한 모드가 적용된 주권 지역에서는 지원되지 않습니다. 제한 모드에서 NetApp Backup and Recovery ONTAP 볼륨 데이터의 백업 및 복원만 지원합니다. " ONTAP 데이터에 대해 지원되는 백업 대상 목록 보기 " 애플리케이션 데이터와 가상 머신 데이터의 백업 및 복원은 지원되지 않습니다.
NetApp Data Classification	제한 모드가 적용된 정부 지역에서 지원됩니다. 상업 지역이나 제한 모드가 적용된 주권 지역에서는 지원되지 않습니다.
Cloud Volumes ONTAP	전면적인 지원
Licenses and subscriptions	제한 모드에서 지원되는 라이선스 옵션 아래에 나열된 라이선스 및 구독 정보에 액세스할 수 있습니다.

지원되는 서비스	노트
온프레미스 ONTAP 클러스터	콘솔 에이전트를 사용한 검색과 콘솔 에이전트를 사용하지 않은 검색(직접 검색)이 모두 지원됩니다. 콘솔 에이전트가 없는 온프레미스 클러스터를 발견하면 고급 보기(시스템 관리자)가 지원되지 않습니다.
복제	제한 모드가 적용된 정부 지역에서 지원됩니다. 상업 지역이나 제한 모드가 적용된 주권 지역에서는 지원되지 않습니다.

지원되는 라이센스 옵션

제한 모드에서는 다음 라이선싱 옵션이 지원됩니다.

- 마켓플레이스 구독(시간 및 연간 계약)

다음 사항에 유의하세요.

- Cloud Volumes ONTAP 의 경우 용량 기반 라이선싱만 지원됩니다.
- Azure에서는 정부 지역과의 연간 계약이 지원되지 않습니다.

- 바이올

Cloud Volumes ONTAP 의 경우 BYOL에서는 용량 기반 라이선싱과 노드 기반 라이선싱이 모두 지원됩니다.

제한 모드를 시작하는 방법

NetApp Console 조직을 생성할 때 제한 모드를 활성화해야 합니다.

아직 조직이 없으면 수동으로 설치하거나 클라우드 공급업체의 마켓플레이스에서 만든 콘솔 에이전트에서 처음으로 콘솔에 로그인할 때 조직을 만들고 제한 모드를 활성화하라는 메시지가 표시됩니다.



조직을 만든 후에는 제한 모드 설정을 변경할 수 없습니다.

["제한 모드를 시작하는 방법을 알아보세요"](#).

서비스 및 기능 비교

다음 표는 제한 모드에서 지원되는 서비스와 기능을 빠르게 식별하는 데 도움이 됩니다.

일부 서비스는 제한적으로 지원될 수 있습니다. 이러한 서비스가 제한 모드에서 어떻게 지원되는지에 대한 자세한 내용은 위 섹션을 참조하세요.

제품 영역	NetApp 데이터 서비스 또는 기능	제한 모드
저장소 이 표의 부분에는 콘솔에서 스토리지 시스템을 관리하는 데 대한 지원이 나열되어 있습니다. NetApp Backup and Recovery 에 지원되는 백업 대상을 나타내지 않습니다.	ONTAP 용 Amazon FSx	아니요
	아마존 S3	아니요
	Azure Blob	아니요
	Azure NetApp Files	예
	Cloud Volumes ONTAP	예
	Google Cloud NetApp Volumes	아니요
	구글 클라우드 스토리지	아니요
	온프레미스 ONTAP 클러스터	예
	E-시리즈	아니요
	StorageGRID	아니요
데이터 서비스	NetApp 백업 및 복구	예 https://docs.netapp.com/us-en/data-services-backup-recovery/prev-ontap-protect-journey.html#support-for-sites-with-limited-internet-connectivity ["ONTAP 볼륨 데이터에 대해 지원되는 백업 대상 목록 보기"]
	NetApp Data Classification	예
	NetApp Copy and Sync	아니요
	NetApp Disaster Recovery	아니요
	NetApp Ransomware Resilience	아니요
	NetApp Replication	예
	NetApp Cloud Tiering	아니요
	NetApp 볼륨 캐싱	아니요
	NetApp 워크로드 팩토리	아니요

제품 영역	NetApp 데이터 서비스 또는 기능	제한 모드
특징	알림	아니요
	Digital Advisor	아니요
	라이선스 및 구독 관리	예
	ID 및 액세스 관리	예
	신임장	예
	연합	예
	수명주기 계획	아니요
	다중 요소 인증	예
	NSS 계정	예
	알림	예
	찾다	예
	소프트웨어 업데이트	아니요
	지속 가능성	아니요
	심사	예

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.

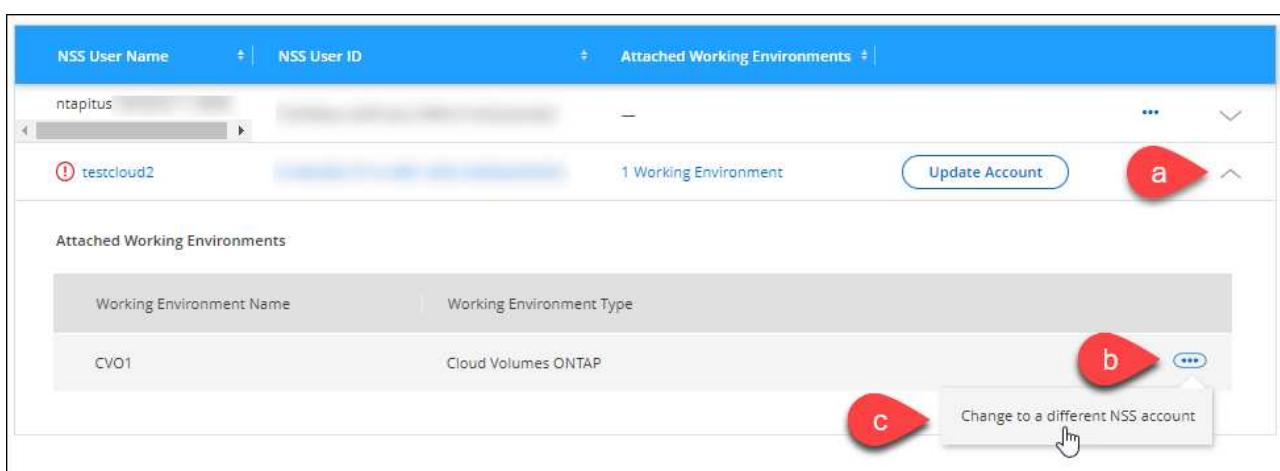
다른 NSS 계정에 시스템 연결

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 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 Console에서 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
소프트웨어 업데이트	예	예

	중개인을 통해 이용 가능합니다.	중개인 없이 구매 가능
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 Console에서 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 온프레미스ONTAP 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.

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.

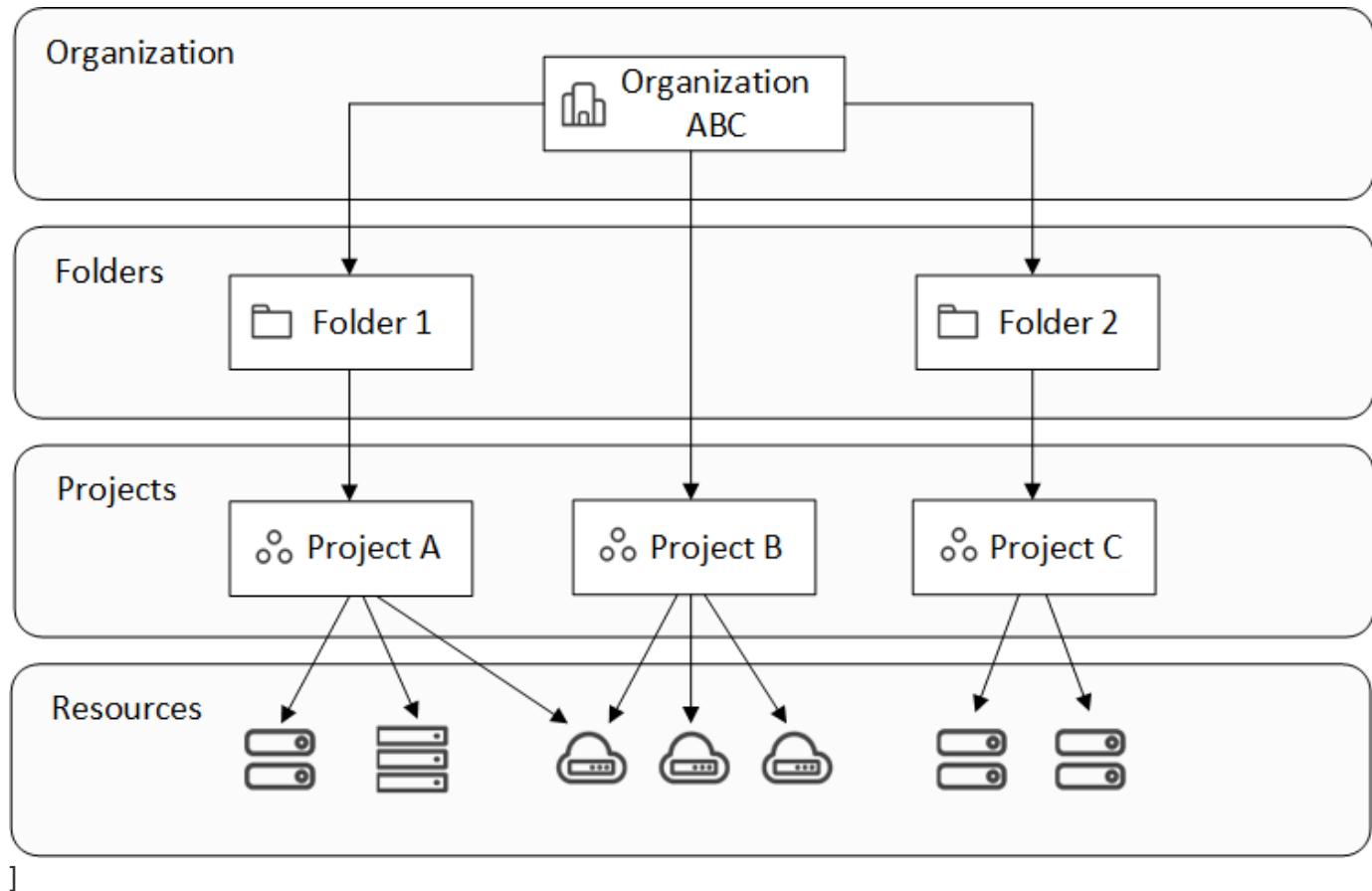
리소스는 계층적으로 구성됩니다. 최상위에는 조직이 있고, 그 아래에 폴더(다른 폴더나 프로젝트를 포함할 수 있음)가 있으며, 그 아래에는 스토리지 시스템, 워크로드 및 에이전트를 포함하는 프로젝트가 있습니다.

조직, 폴더 또는 프로젝트 수준에서 구성원에게 역할 기반 접근 제어(RBAC) 권한을 할당하여 사용자가 리소스에 대한 적절한 접근 권한을 갖도록 합니다.



NetApp Console에서 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 Console에서는 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

조직은 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

리소스에는 스토리지 시스템, Keystone 구독 및 콘솔 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 Console 온프레미스 및 클라우드 스토리지 시스템 모두의 관리를 지원합니다. 프로젝트에 스토리지 시스템을 추가해야만 다른 사용자가 접근할 수 있습니다.

저장 시스템은 추가되는 프로젝트에 자동으로 연결되지만, 리소스 페이지에서 다른 프로젝트나 폴더와도 연결할 수 있습니다.

Keystone 구독은 NetApp Console에서 사용자가 구독에 액세스할 수 있도록 프로젝트와 연결할 수 있는 리소스이기도 합니다.

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 Console에 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 (5인 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 Console에서 IAM 관련 다음 단계

- "[NetApp Console에서 IAM 시작하기](#)"
- "[IAM 활동 모니터링 또는 감사](#)"
- "[NetApp Console IAM에 대한 API에 대해 알아보세요](#)"

NetApp Console (SaaS) 시작하기

시작하기 워크플로(SaaS)

NetApp Console (SaaS)을 시작하려면 콘솔용 네트워크를 준비하고, 가입하여 계정을 생성한 다음, 콘솔 도우미를 사용하여 초기 기능을 설정하십시오.

NetApp에서 서비스형 소프트웨어(SaaS) 제품으로 호스팅되는 웹 기반 콘솔에 접속할 수 있습니다. 콘솔을 사용하여 하이브리드 클라우드 스토리지 환경을 관리하고 NetApp 데이터 서비스를 이용할 수 있습니다.

1

"NetApp 콘솔을 사용하기 위한 네트워킹 준비"

NetApp 콘솔에 접속하는 컴퓨터가 필요한 엔드포인트에 네트워크로 접속할 수 있는지 확인하십시오.

"[NetApp 콘솔용 네트워킹을 준비하는 방법을 알아보세요.](#)"

2

"가입하고 조직을 만드세요"

가세요 "[NetApp 콘솔](#)" 그리고 가입하세요. 조직을 생성하라는 메시지가 표시되었는데 이미 회사에 조직이 있다고 생각되면 대화 상자를 닫고 조직 관리자에게 알리십시오. 회사에 조직 관리자가 없는 경우, 본인이 해당 역할을 맡을 수 있습니다. "[조직 관리자에게 연락하는 방법을 알아보세요.](#)"

이제 로그인이 완료되었으며 NetApp 도우미를 사용하여 콘솔 구성을 시작할 수 있습니다. 먼저 NetApp 지원 계정과 콘솔 에이전트를 연결하여 모든 기능을 활성화하십시오.

NetApp 어시스턴트를 사용하지 않거나 콘솔 에이전트를 설치하지 않기로 선택한 경우 Digital Advisor, Amazon FSx for ONTAP, Azure NetApp Files 등과 같은 서비스를 사용하여 스토리지를 관리할 수 있습니다. "[콘솔 에이전트 없이 무엇을 할 수 있는지 알아보세요.](#)"

3

NetApp 지원 사이트(NSS) 계정을 연결하세요.

NetApp 지원 사이트(NSS) 계정을 콘솔과 연결하면 라이선스 및 구독을 더욱 쉽게 관리할 수 있을 뿐 아니라 콘솔에서 직접 지원 리소스에 액세스할 수 있습니다.

4

콘솔 에이전트를 생성합니다

고급 스토리지 관리 기능과 일부 NetApp 데이터 서비스를 사용하려면 콘솔 에이전트를 설치해야 합니다. 콘솔 에이전트를 사용하면 콘솔에서 하이브리드 클라우드 환경 내의 리소스와 프로세스를 관리할 수 있습니다.

클라우드 또는 온프레미스 네트워크에서 콘솔 에이전트를 만들 수 있습니다.

- ["콘솔 에이전트가 필요한 경우와 작동 방식에 대해 자세히 알아보세요."](#)
- ["AWS에서 콘솔 에이전트를 만드는 방법을 알아보세요"](#)
- ["Azure에서 콘솔 에이전트를 만드는 방법을 알아보세요."](#)
- ["Google Cloud에서 콘솔 에이전트를 만드는 방법을 알아보세요."](#)
- ["온프레미스에서 콘솔 에이전트를 만드는 방법을 알아보세요."](#)

5

콘솔에 스토리지 시스템 추가

NetApp Console에서 스토리지 시스템을 추가하거나 검색하여 하이브리드 클라우드 스토리지 환경을 관리할 수 있습니다. NetApp 어시스턴트를 사용하여 첫 번째 스토리지 시스템을 추가하세요.



AWS, Microsoft Azure 또는 Google Cloud에 콘솔 에이전트를 설치하면 콘솔은 에이전트가 설치된 위치에 있는 Amazon S3 버킷, Azure Blob 스토리지 또는 Google Cloud Storage 버킷에 대한 정보를 자동으로 검색합니다. 이러한 시스템은 시스템 페이지에 자동으로 추가됩니다.

- "ONTAP 시스템을 찾는 방법을 알아보세요."
- "StorageGRID 시스템을 찾는 방법을 알아보세요."
- "E-시리즈 시스템을 알아보는 방법을 알아보세요."

6

"NetApp Intelligent Services 구독(선택 사항)"

클라우드 공급업체를 통해 NetApp Intelligent Services 에 가입하여 시간당(PAYGO) 또는 연간 요금으로 청구하세요. 구독에는 NetApp Backup and Recovery, Cloud Volumes ONTAP, NetApp Cloud Tiering, NetApp Ransomware Resilience, NetApp Disaster Recovery 및 NetApp Data Classification 포함됩니다.

NetApp Console 대한 네트워크 액세스 준비

NetApp Console, NetApp Console 에이전트 및 NetApp 데이터 서비스에는 아웃바운드 인터넷 액세스와 필요한 엔드포인트에 연결할 수 있는 기능이 필요합니다.

다음에 대한 네트워크 액세스를 설정해야 합니다.

- SaaS(Software as a Service)로 NetApp Console 액세스하는 컴퓨터
- 온프레미스 또는 클라우드에 설치하는 콘솔 에이전트입니다. 콘솔 에이전트.



NetApp 4.0.0을 통해 콘솔 및 콘솔 에이전트에 필요한 네트워크 엔드포인트를 줄여 보안을 강화하고 배포를 간소화했습니다. 중요한 점은 버전 4.0.0 이전의 모든 배포가 계속해서 완벽하게 지원된다는 것입니다. 기존 에이전트에서는 이전 엔드포인트를 계속 사용할 수 있지만 NetApp 에이전트 업그레이드가 성공적으로 완료되었음을 확인한 후 현재 엔드포인트에 대한 방화벽 규칙을 업데이트할 것을 강력히 권장합니다. ["엔드포인트 목록을 업데이트하는 방법을 알아보세요."](#)

NetApp Console 및 콘솔 에이전트가 연락한 엔드포인트

배포하는 각 에이전트와 NetApp Console 액세스하는 각 컴퓨터는 아래 나열된 엔드포인트에 연결되어 있어야 합니다.

클라우드 공급자에 배포된 콘솔 에이전트는 해당 클라우드 공급자와 관련된 엔드포인트에 액세스해야 합니다.

엔드포인트	목적
\ 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 Console에 새로운 NSS 자격 증명을 추가합니다.
\ https://support.netapp.com	라이선스 정보를 얻고 NetApp 지원팀에 AutoSupport 메시지를 보내고 Cloud Volumes ONTAP에 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	<p>콘솔 에이전트 업그레이드를 위한 이미지를 얻으려면.</p> <ul style="list-style-type: none"> 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. <p>이전 엔드포인트는 계속 지원되지만 NetApp 가능한 한 빨리 현재 엔드포인트에 맞게 방화벽 규칙을 업데이트할 것을 권장합니다. "엔드포인트 목록을 업데이트하는 방법을 알아보세요".</p> <ul style="list-style-type: none"> 방화벽의 현재 엔드포인트로 업데이트하면 기존 에이전트도 계속 작동합니다.

클라우드 공급자 엔드포인트가 콘솔 에이전트에 연결되었습니다.

콘솔 에이전트가 클라우드 공급자에 배포된 경우 추가 엔드포인트에 액세스할 수 있어야 합니다.

콘솔 에이전트를 설치하기 전에 클라우드 공급자 네트워크 엔드포인트 액세스를 설정하세요.

- "[콘솔 에이전트에 대한 AWS 네트워크 액세스 설정](#)"
- "[콘솔 에이전트에 대한 Azure 네트워크 액세스 설정](#)"
- "[콘솔 에이전트에 대한 Google Cloud 네트워크 액세스 설정](#)"

콘솔 에이전트가 접속한 데이터 서비스 엔드포인트

일부 NetApp 데이터 서비스와 Cloud Volumes ONTAP 사용하려면 에이전트에 추가 아웃바운드 인터넷 액세스 권한이 필요합니다.

Cloud Volumes ONTAP 의 엔드포인트

- "[AWS의 Cloud Volumes ONTAP 엔드포인트](#)"
- "[Azure의 Cloud Volumes ONTAP 엔드포인트](#)"
- "[Google Cloud의 Cloud Volumes ONTAP 엔드포인트](#)"

워크로드용 엔드포인트

콘솔 에이전트는 NetApp 워크로드에 대해 다음 엔드포인트에 액세스할 수 있어야 합니다.

엔드포인트	목적
https://api.workloads.netapp.com	웹 기반 콘솔은 이 엔드포인트에 연결하여 Workload Factory API와 상호 작용함으로써 ONTAP 기반 워크로드용 FSx를 관리하고 운영합니다.

NetApp Console 에 가입하거나 로그인하세요

콘솔을 사용하려면 NetApp 지원 사이트 자격 증명으로 가입하거나 로그인하거나 NetApp Console 로그인을 생성하십시오. 회사에서 처음으로 가입하는 경우, 관리자 권한으로 새 조직을 생성하게 됩니다. 회사에 이미 조직이 있는 경우 기존 NetApp 지원 사이트 자격 증명 또는 회사 단일 로그인(SSO)을 사용하여 가입하거나 로그인하십시오.

NetApp Console 에 최초 조직 관리자로 등록하세요.

회사에 NetApp Console 조직이 없는 경우 가입하여 조직을 생성하세요. 첫 번째 사용자는 조직 관리자가 되어 사용자 계정 및 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. NetApp에서 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 사용자이거나 조직 관리자인 경우, 안내에 따라 스토리지 리소스를 추가하고 콘솔 에이전트를 생성하는 등의 작업을 수행할 수 있습니다. "[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.

회사에 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. NetApp에서 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.

NetApp Console 어시스턴트를 사용하여 시작하세요

조직 관리자 역할을 가진 NetApp Console (SaaS)을 처음 사용하는 경우 콘솔 도우미를 사용하여 초기 설정 프로세스를 안내받을 수 있습니다. 이 도우미는 NetApp 지원 사이트(NSS) 계정 추가, 콘솔 에이전트 추가, 클러스터 추가, 라이선스 또는 구독 추가를 지원하여 데이터 관리를 더 쉽게 시작할 수 있도록 도와줍니다.

콘솔 어시스턴트에 액세스하는 데 필요한 역할

콘솔 어시스턴트는 조직 관리자 역할이 있는 사용자만 사용할 수 있습니다.

기본적으로 NetApp Console 조직 관리자 역할을 가진 신규 사용자를 위해 홈 페이지에 콘솔 도우미를 표시합니다. 콘솔 에이전트를 생성하고 시스템을 추가하는 필수 작업을 완료할 때까지 해당 기능은 계속 사용할 수 있습니다.

도우미를 사용하여 다음 작업을 완료하면 NetApp Console 환경을 위한 최소 설정이 완료됩니다.

- NetApp 지원 사이트(NSS) 계정을 추가합니다.
["NSS 계정을 추가하는 방법을 알아보세요".](#)
- 콘솔 에이전트를 배포하여 스토리지 환경에 연결하세요.
["콘솔 에이전트를 온프레미스에 설치하는 방법을 알아보세요."](#)
- 클러스터를 추가하거나 검색하여 스토리지 시스템을 관리하세요.
- 마켓플레이스 구독이나 PAYGO 라이선스를 추가합니다.

"라이선스 및 구독 추가 방법을 알아보세요.".

- 데이터 서비스 정보를 검토하세요.

NetApp Console 시작하기(제한 모드)

시작하기 워크플로(제한 모드)

환경을 준비하고 콘솔 에이전트를 배포하여 제한 모드에서 NetApp Console 을 시작하세요.

제한 모드는 일반적으로 주 및 지방 정부와 규제 대상 기업에서 사용하며, 여기에는 AWS GovCloud 및 Azure Government 지역에 배포하는 것도 포함됩니다. 시작하기 전에 다음 사항을 이해했는지 확인하십시오. "[콘솔 에이전트](#)" 그리고 "[배포 모드](#)".

1

"배치 준비"

- CPU, RAM, 디스크 공간, 컨테이너 오케스트레이션 도구 등의 요구 사항을 충족하는 전용 Linux 호스트를 준비합니다.
- 대상 네트워크에 대한 액세스, 수동 설치를 위한 아웃바운드 인터넷 액세스, 일상적인 액세스를 위한 아웃바운드 인터넷을 제공하는 네트워킹을 설정합니다.
- 콘솔 에이전트 인스턴스를 배포한 후 해당 권한과 연결할 수 있도록 클라우드 공급자에서 권한을 설정합니다.

2

"콘솔 에이전트 배포"

- 클라우드 공급업체의 마켓플레이스에서 콘솔 에이전트를 설치하거나, Linux 호스트에 소프트웨어를 수동으로 설치하세요.
- 웹 브라우저를 열고 Linux 호스트의 IP 주소를 입력하여 NetApp Console 설정합니다.
- 이전에 설정한 권한을 콘솔 에이전트에 제공합니다.

3

"NetApp Intelligent Services 구독(선택 사항)"

선택 사항: 클라우드 공급업체의 마켓플레이스에서 NetApp Intelligent Services 구독하여 시간당 요금(PAYGO) 또는 연간 계약을 통해 데이터 서비스 비용을 지불하세요. NetApp Intelligent Services에는 NetApp Backup and Recovery, Cloud Volumes ONTAP, NetApp Cloud Tiering, NetApp Ransomware Resilience 및 NetApp Disaster Recovery 포함됩니다. NetApp Data Classification 추가 비용 없이 구독에 포함되어 있습니다.

제한 모드에서 배포 준비

제한 모드에서 NetApp Console 배포하기 전에 환경을 준비하세요. 호스트 요구 사항을 검토하고, 네트워킹을 준비하고, 권한을 설정하는 등의 작업이 필요합니다.

1단계: 제한 모드 작동 방식 이해

시작하기 전에 NetApp Console 제한 모드에서 어떻게 작동하는지 이해하세요.

설치된 NetApp Console 에이전트에서 로컬로 사용할 수 있는 브라우저 기반 인터페이스를 사용합니다. SaaS 계층을

통해 제공되는 웹 기반 콘솔에서는 NetApp Console 액세스할 수 없습니다.

또한, 일부 콘솔 기능과 NetApp 데이터 서비스를 이용할 수 없습니다.

["제한 모드의 작동 방식 알아보기"](#).

2단계: 설치 옵션 검토

제한 모드에서는 클라우드에만 콘솔 에이전트를 설치할 수 있습니다. 다음과 같은 설치 옵션을 사용할 수 있습니다.

- AWS Marketplace에서
- Azure Marketplace에서
- AWS, Azure 또는 Google Cloud에서 실행되는 자체 Linux 호스트에 콘솔 에이전트를 수동으로 설치합니다.

3단계: 호스트 요구 사항 검토

콘솔 에이전트를 실행하려면 호스트가 특정 OS, RAM 및 포트 요구 사항을 충족해야 합니다.

AWS 또는 Azure Marketplace에서 콘솔 에이전트를 배포하는 경우 이미지에는 필요한 OS 및 소프트웨어 구성 요소가 포함됩니다. CPU와 RAM 요구 사항을 충족하는 인스턴스 유형을 선택하기만 하면 됩니다.

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.

Azure VM 크기

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

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 <ul style="list-style-type: none">• 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 <ul style="list-style-type: none">• 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		<p>8.6에서 8.10까지</p> <ul style="list-style-type: none"> 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

4단계: Podman 또는 Docker Engine 설치

콘솔 에이전트를 수동으로 설치하려면 Podman이나 Docker Engine을 설치하여 호스트를 준비하세요.

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
```

5단계: 네트워크 액세스 준비

콘솔 에이전트가 퍼블릭 클라우드의 리소스를 관리할 수 있도록 네트워크 액세스를 설정합니다. 콘솔 에이전트에 대한 가상 네트워크와 서브넷을 갖추는 것 외에도 다음 요구 사항이 충족되는지 확인해야 합니다.

대상 네트워크에 대한 연결

콘솔 에이전트가 저장 위치에 네트워크로 연결되어 있는지 확인하세요. 예를 들어, Cloud Volumes ONTAP 배포할 VPC 또는 VNet이나 온프레미스 ONTAP 클러스터가 있는 데이터 센터입니다.

NetApp Console에 대한 사용자 액세스를 위한 네트워킹 준비

제한 모드에서는 사용자가 콘솔 에이전트 VM에서 콘솔에 액세스합니다. 콘솔 에이전트는 몇몇 엔드포인트에 연락하여 데이터 관리 작업을 완료합니다. 이러한 엔드포인트는 콘솔에서 특정 작업을 완료할 때 사용자 컴퓨터에서 접속됩니다.



버전 4.0.0 이전의 콘솔 에이전트에는 추가 엔드포인트가 필요합니다. 4.0.0 이상으로 업그레이드한 경우 허용 목록에서 이전 엔드포인트를 제거할 수 있습니다. ["4.0.0 이전 버전에 필요한 네트워크 액세스에 대해 자세히 알아보세요."](#)

+

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://cdn.auth0.com \ https://services.cloud.netapp.com	웹 브라우저는 NetApp Console 통해 중앙화된 사용자 인증을 위해 이러한 엔드포인트에 연결합니다.

일상 업무를 위한 아웃바운드 인터넷 접속

콘솔 에이전트의 네트워크 위치에는 아웃바운드 인터넷 액세스가 가능해야 합니다. NetApp Console의 SaaS 서비스와 해당 퍼블릭 클라우드 환경 내의 엔드포인트에 도달할 수 있어야 합니다.

엔드포인트	목적
AWS 환경	AWS 서비스(amazonaws.com): <ul style="list-style-type: none">클라우드포메이션탄력적 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: <ul style="list-style-type: none">api.workloads.netapp.com
웹 기반 콘솔은 이 엔드포인트에 연결하여 Workload Factory API와 상호 작용함으로써 ONTAP 기반 워크로드용 FSx를 관리하고 운영합니다.	Azure 환경

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.usgovcloudapi.net \ https://login.microsoftonline.us \ https://blob.core.usgovcloudapi.net \ https://core.usgovcloudapi.net	Azure Government 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.
Google Cloud 환경	https://www.googleapis.com/compute/v1/ https://compute.googleapis.com/compute/v1 https://clouddresourcemanager.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.	<ul style="list-style-type: none"> NetApp Console 엔드포인트*
\ 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 Console에 새로운 NSS 자격 증명을 추가합니다.
\ https://support.netapp.com	라이선스 정보를 얻고 NetApp 지원팀에 AutoSupport 메시지를 보내고 Cloud Volumes ONTAP에 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	<p>콘솔 에이전트 업그레이드를 위한 이미지를 얻으려면.</p> <ul style="list-style-type: none"> 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. <p>이전 엔드포인트는 계속 지원되지만 NetApp 가능한 한 빨리 현재 엔드포인트에 맞게 방화벽 규칙을 업데이트할 것을 권장합니다. "엔드포인트 목록을 업데이트하는 방법을 알아보세요".</p> <ul style="list-style-type: none"> 방화벽의 현재 엔드포인트로 업데이트하면 기존 에이전트도 계속 작동합니다.

Azure의 공용 IP 주소

Azure의 콘솔 에이전트 VM에서 공용 IP 주소를 사용하려면 콘솔에서 이 공용 IP 주소를 사용하도록 IP 주소에 기본 SKU를 사용해야 합니다.

The screenshot shows the 'Create public IP address' wizard in the Azure portal. The first step is 'Name *' with the value 'newIP'. The 'SKU *' section has 'Basic' selected. The 'Assignment' section has 'Static' selected. There is also a note at the bottom: '대신 표준 SKU IP 주소를 사용하면 콘솔은 공용 IP 대신 콘솔 에이전트의 개인 IP 주소를 사용합니다. 콘솔에 액세스하는 데 사용하는 컴퓨터가 해당 개인 IP 주소에 액세스할 수 없는 경우 콘솔의 작업은 실패합니다.'

대신 표준 SKU IP 주소를 사용하면 콘솔은 공용 IP 대신 콘솔 에이전트의 개인 IP 주소를 사용합니다. 콘솔에 액세스하는 데 사용하는 컴퓨터가 해당 개인 IP 주소에 액세스할 수 없는 경우 콘솔의 작업은 실패합니다.

"Azure 설명서: 공용 IP SKU"

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 ONTAP에서 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"](#)

클라우드 공급업체의 마켓플레이스에서 콘솔 에이전트를 만들 계획이라면 콘솔 에이전트를 만든 후 이 네트워킹 요구 사항을 구현하세요.

6단계: 클라우드 권한 준비

콘솔 에이전트는 가상 네트워크에 Cloud Volumes ONTAP 배포하고 NetApp 데이터 서비스를 사용하려면 클라우드 공급자의 권한이 필요합니다. 클라우드 공급자에서 권한을 설정한 다음 해당 권한을 콘솔 에이전트와 연결해야 합니다.

필요한 단계를 보려면 클라우드 공급자에 사용할 인증 옵션을 선택하세요.

AWS IAM 역할

IAM 역할을 사용하여 콘솔 에이전트에 권한을 제공합니다.

AWS Marketplace에서 콘솔 에이전트를 생성하는 경우 EC2 인스턴스를 시작할 때 해당 IAM 역할을 선택하라는 메시지가 표시됩니다.

Linux 호스트에 콘솔 에이전트를 수동으로 설치하는 경우 해당 역할을 EC2 인스턴스에 연결합니다.

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.
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 콘솔 에이전트 EC2 인스턴스에 대한 IAM 역할이 생겼습니다.

AWS 액세스 키

IAM 사용자에 대한 권한과 액세스 키를 설정합니다. 콘솔 에이전트를 설치하고 콘솔을 설정한 후에는 콘솔에 AWS 액세스 키를 제공해야 합니다.

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 Console에 추가할 수 있는 액세스 키가 사용자에게 있는지 확인하세요.

Azure 역할

필요한 권한이 있는 Azure 사용자 지정 역할을 만듭니다. 이 역할은 콘솔 에이전트 VM에 할당합니다.

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 Console과 함께 사용하려는 각 Azure 구독에 대한 ID를 추가해야 합니다.

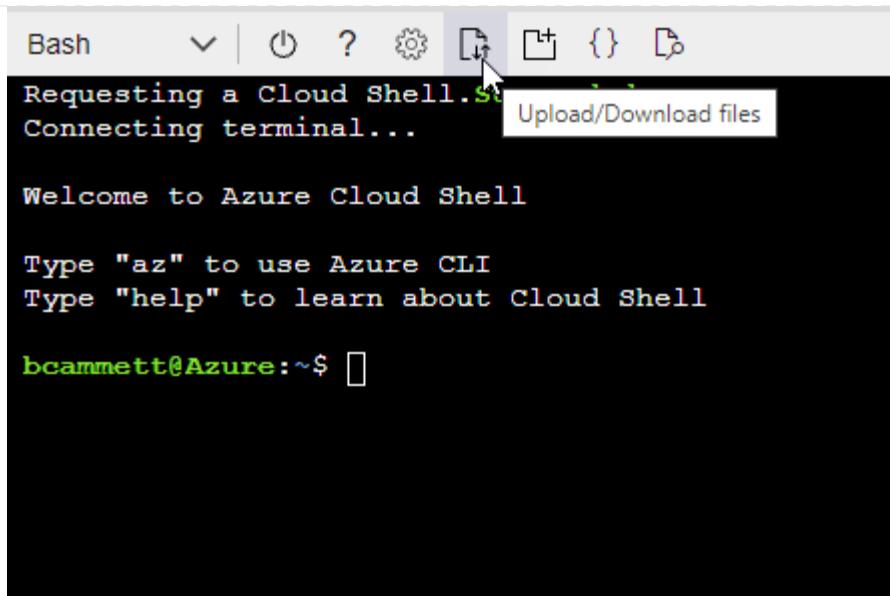
예

```
"AssignableScopes": [  
    "/subscriptions/d333af45-0d07-4154-943d-c25fbzzzzzz",  
    "/subscriptions/54b91999-b3e6-4599-908e-416e0zzzzzz",  
    "/subscriptions/398e471c-3b42-4ae7-9b59-ce5bbzzzzzz"  
]
```

4. JSON 파일을 사용하여 Azure에서 사용자 지정 역할을 만듭니다.

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

- a. 시작 ["Azure 클라우드 셀"](#) Bash 환경을 선택하세요.
- b. JSON 파일을 업로드합니다.



- c. Azure CLI를 사용하여 사용자 지정 역할을 만듭니다.

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

Azure 서비스 주체

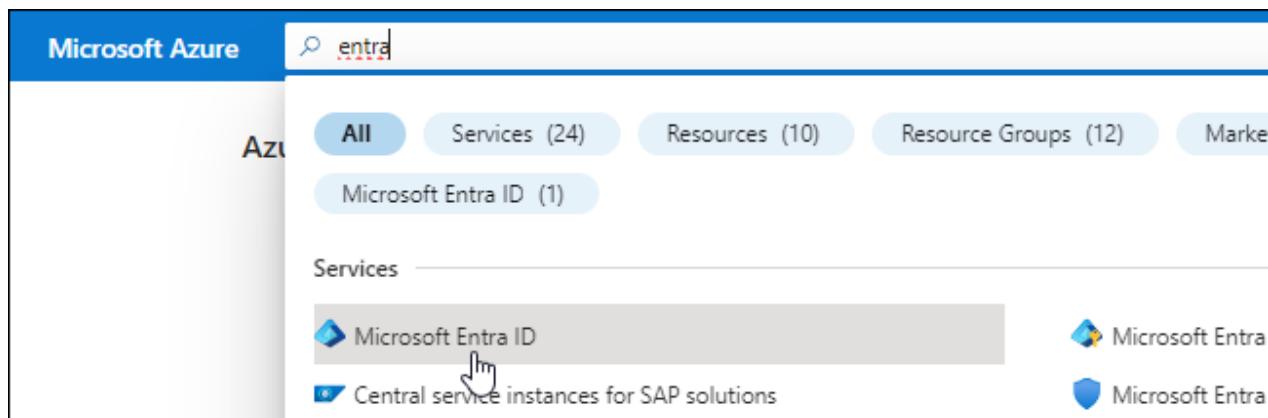
Microsoft Entra ID에서 서비스 주체를 만들고 설정하고 콘솔에 필요한 Azure 자격 증명을 얻습니다. 콘솔에이전트를 설치한 후 콘솔에 이러한 자격 증명을 제공해야 합니다.

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 Console에서 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.

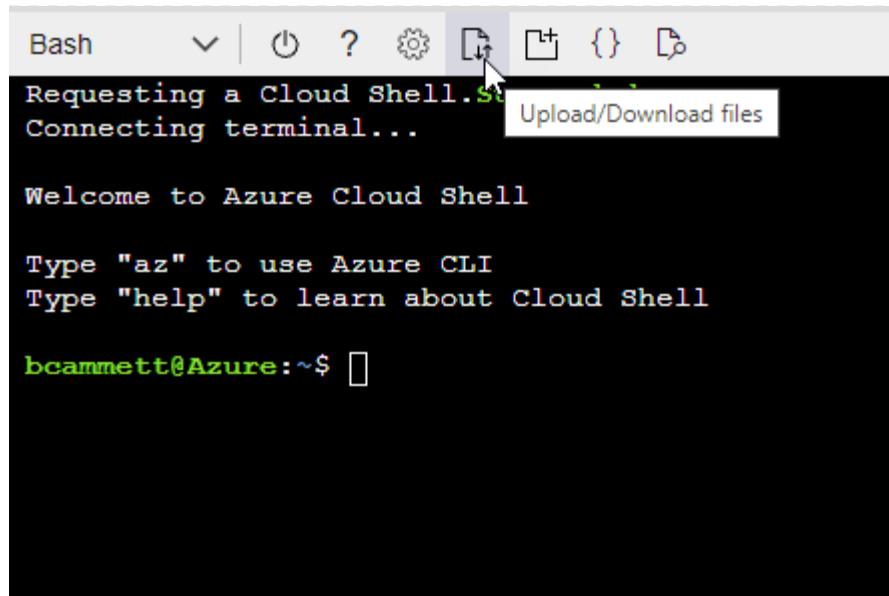
예

```
"AssignableScopes": [  
    "/subscriptions/d333af45-0d07-4154-943d-c25fbzzzzzz",  
    "/subscriptions/54b91999-b3e6-4599-908e-416e0zzzzzz",  
    "/subscriptions/398e471c-3b42-4ae7-9b59-ce5bbzzzzzz"  
]
```

- 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.

Add role assignment

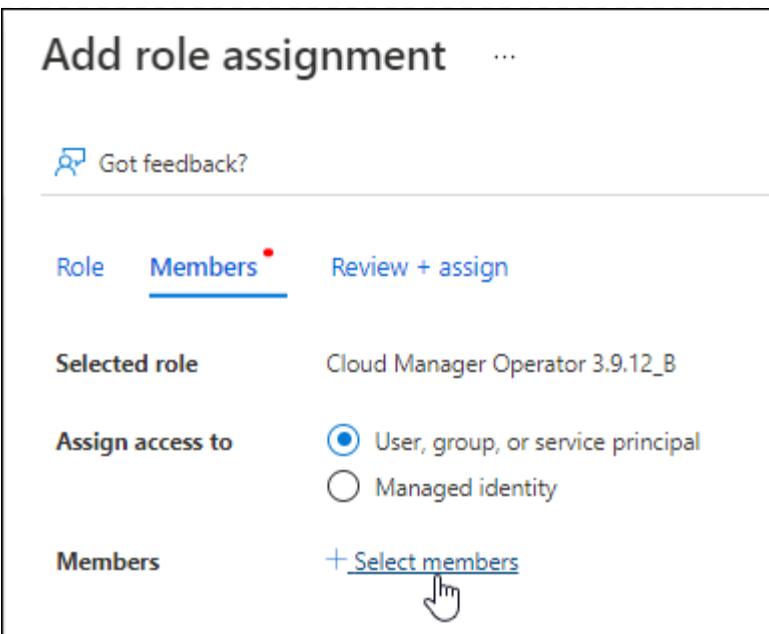
Got feedback?

Role **Members** Review + assign

Selected role Cloud Manager Operator 3.9.12_B

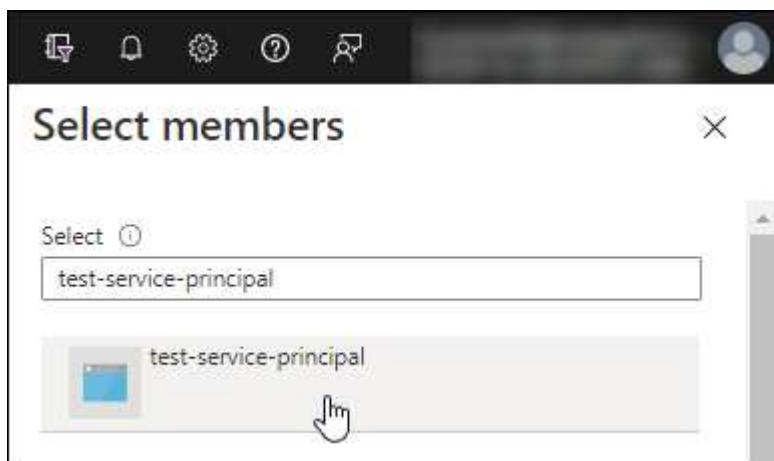
Assign access to User, group, or service principal Managed identity

Members [Select members](#)



- 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 Console에서 Cloud Volumes ONTAP 배포할 때 사용할 구독을 선택할 수 있습니다.

Windows Azure 서비스 관리 API 권한 추가

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

Request API permissions

Select an API

[Microsoft APIs](#) [APIs my organization uses](#) [My APIs](#)

Commonly used Microsoft APIs

Microsoft Graph

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



Azure Batch

Schedule large-scale parallel and HPC applications in the cloud

Azure Data Lake

Access to storage and compute for big data analytic scenarios

Azure Key Vault

Manage your key vaults as well as the keys, secrets, and certificates within your Key Vaults

Azure Storage

Secure, massively scalable object and data lake storage for unstructured and semi-structured data

Azure Data Catalog

Programmatic access to Data Catalog resources to register, annotate and search data assets

Azure DevOps

Integrate with Azure DevOps and Azure DevOps server

Azure Rights Management Services

Allow validated users to read and write protected content

Customer Insights

Create profile and interaction models for your products

Azure Data Explorer

Perform ad-hoc queries on terabytes of data to build near real-time and complex analytics solutions

Azure Import/Export

Programmatic control of import/export jobs

Azure Service Management

Programmatic access to much of the functionality available through the Azure portal

Data Export Service for Microsoft Dynamics 365

Export data from Microsoft Dynamics CRM organization to an external destination

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

Request API permissions

[All APIs](#)

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

What type of permissions does your application require?

Delegated permissions

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

Application permissions

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

Select permissions

[expand all](#)

Type to search		PERMISSION	ADMIN CONSENT REQUIRED
<input checked="" type="checkbox"/> user_impersonation	Access Azure Service Management as organization users (preview)	Details	-

애플리케이션의 애플리케이션 ID와 디렉토리 ID를 가져옵니다.

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

[Delete](#) [Endpoints](#)

Welcome to the new and improved App registrations. Looking to learn

Display name	: test-service-principal
Application (client) ID	: 73de25f9-99be-4ae0-8b24-538ca787a6b3
Directory (tenant) ID	: 4b0911a0-929b-4715-944b-c03745165b3a
Object ID	: b37489a9-379f-49c2-b27c-e630514106a5

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.

Client secrets

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

New client secret		
DESCRIPTION	EXPIRES	VALUE
test secret	8/16/2020	*sZ1jSe2By:D*-ZRvV4NLfdAcY7:+0vA

Copy to clipboard

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.

Google Cloud 서비스 계정

역할을 만들고 콘솔 에이전트 VM 인스턴스에 사용할 서비스 계정에 적용합니다.

단계

1. Google Cloud에서 사용자 지정 역할을 만듭니다.

- a. 정의된 권한을 포함하는 YAML 파일을 만듭니다. ["Google Cloud용 콘솔 에이전트 정책"](#).
- b. Google Cloud에서 Cloud Shell을 활성화합니다.
- c. 콘솔 에이전트에 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 agent --project=myproject --file=agent.yaml
```

+

["Google Cloud 문서: 사용자 지정 역할 만들기 및 관리"](#)

2. Google Cloud에서 서비스 계정을 만듭니다.

- 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"](#)

7단계: Google Cloud API 활성화

Google Cloud에 Cloud Volumes ONTAP 배포하려면 여러 API가 필요합니다.

단계

1. "프로젝트에서 다음 Google Cloud API를 활성화하세요."

- 클라우드 인프라 관리자 API
- 클라우드 배포 관리자 V2 API
- 클라우드 로깅 API
- 클라우드 리소스 관리자 API
- 컴퓨터 엔진 API
- ID 및 액세스 관리(IAM) API
- 클라우드 키 관리 서비스(KMS) API

(고객 관리 암호화 키(CMEK)와 함께 NetApp Backup and Recovery 사용하려는 경우에만 필요함)

제한 모드로 콘솔 에이전트 배포

NetApp Console 제한된 아웃바운드 연결로 사용할 수 있도록 콘솔 에이전트를 제한 모드로 배포합니다. 시작하려면 콘솔 에이전트를 설치하고, 콘솔 에이전트에서 실행되는 사용자 인터페이스에 액세스하여 콘솔을 설정한 다음, 이전에 설정한 클라우드 권한을 제공하세요.

1단계: 콘솔 에이전트 설치

클라우드 공급업체의 마켓플레이스에서 콘솔 에이전트를 설치하거나 Linux 호스트에 수동으로 설치합니다.

콘솔 에이전트를 설치하기 전에 환경을 미리 준비해야 합니다. AWS 마켓플레이스, Azure 마켓플레이스에서 설치하거나 AWS, Azure 또는 Google Cloud에서 실행 중인 자체 Linux 호스트에 수동으로 설치할 수 있습니다.

AWS 커머셜 마켓플레이스

시작하기 전에

다음 사항을 숙지하십시오:

- 네트워킹 요구 사항을 충족하는 VPC 및 서브넷.

["네트워킹 요구 사항에 대해 알아보세요"](#)

- 콘솔 에이전트에 필요한 권한이 포함된 정책이 첨부된 IAM 역할입니다.

["AWS 권한을 설정하는 방법을 알아보세요"](#)

- IAM 사용자가 AWS Marketplace를 구독하고 구독을 취소할 수 있는 권한입니다.
- 에이전트의 CPU 및 RAM 요구 사항에 대한 이해.

["에이전트 요구 사항 검토".](#)

- EC2 인스턴스에 대한 키 쌍입니다.

단계

- 로 가다 ["AWS Marketplace에 NetApp Console 에이전트 목록이 추가되었습니다."](#)
- 마켓플레이스 페이지에서 *구독 계속하기*를 선택하세요.
- 소프트웨어를 구독하려면 *약관 동의*를 선택하세요.

구독 절차는 몇 분 정도 걸릴 수 있습니다.

- 구독 프로세스가 완료되면 *구성 계속*을 선택하세요.
- 이 소프트웨어 구성 페이지에서 올바른 지역을 선택했는지 확인한 다음 *계속 실행*을 선택합니다.
- 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.

- 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.

결과

AWS는 지정된 설정으로 소프트웨어를 시작합니다. 콘솔 에이전트는 약 5분 안에 배포됩니다.

다음은 무엇인가요?

NetApp Console 설정합니다.

AWS Gov 마켓플레이스

시작하기 전에

다음 사항을 숙지하십시오:

- 네트워킹 요구 사항을 충족하는 VPC 및 서브넷.

["네트워킹 요구 사항에 대해 알아보세요"](#)

- 콘솔 에이전트에 필요한 권한이 포함된 정책이 첨부된 IAM 역할입니다.

["AWS 권한을 설정하는 방법을 알아보세요"](#)

- IAM 사용자가 AWS Marketplace를 구독하고 구독을 취소할 수 있는 권한입니다.
- EC2 인스턴스에 대한 키 쌍입니다.

단계

- AWS Marketplace에서 NetApp Console 에이전트 제품으로 이동합니다.
 - EC2 서비스를 열고 *인스턴스 시작*을 선택합니다.
 - *AWS Marketplace*를 선택하세요.
 - NetApp Console 검색하고 제품을 선택하세요.

- d. *계속*을 선택하세요.
2. 안내에 따라 인스턴스를 설정하고 시작하십시오.
- 인스턴스 유형 선택: 지역별 가용성에 따라 지원되는 인스턴스 유형 중 하나를 선택합니다(t3.2xlarge 권장).
 - "[인스턴스 요구 사항 검토](#)".
 - 인스턴스 세부 정보 구성: VPC와 서브넷을 선택하고, 1단계에서 생성한 IAM 역할을 선택하고, 종료 보호를 활성화(권장)하고, 요구 사항을 충족하는 다른 구성 옵션을 선택합니다.

Number of instances	<input type="text" value="1"/>	Launch into Auto Scaling Group
Purchasing option	<input type="checkbox"/> Request Spot instances	
Network	vpc-a76d91c2 VPC4QA (default)	Create new VPC
Subnet	subnet-39536c13 QASubnet1 us-east-1b	Create new subnet 155 IP Addresses available
Auto-assign Public IP	Enable	
Placement group	<input type="checkbox"/> Add instance to placement group	
Capacity Reservation	Open	Create new Capacity Reservation
IAM role	Cloud_Manager	Create new IAM role
CPU options	<input type="checkbox"/> Specify CPU options	
Shutdown behavior	Stop	
Enable termination protection	<input checked="" type="checkbox"/> Protect against accidental termination	
Monitoring	<input type="checkbox"/> Enable CloudWatch detailed monitoring Additional charges apply.	

- 저장 공간 추가: 기본 저장 공간 옵션을 유지합니다.
- 태그 추가: 원하는 경우 인스턴스에 대한 태그를 입력합니다.
- 보안 그룹 구성: 콘솔 에이전트 인스턴스에 필요한 연결 방법(SSH, HTTP, HTTPS)을 지정합니다.
- 검토: 선택 사항을 검토하고 *실행*을 선택합니다.

결과

AWS는 지정된 설정으로 소프트웨어를 시작합니다. 콘솔 에이전트는 약 5분 안에 배포됩니다.

다음은 무엇인가요?

콘솔을 설정합니다.

Azure Gov 마켓플레이스

시작하기 전에

다음 사항이 있어야 합니다.

- 네트워킹 요구 사항을 충족하는 VNet 및 서브넷.

["네트워킹 요구 사항에 대해 알아보세요"](#)

- 콘솔 에이전트에 필요한 권한이 포함된 Azure 사용자 지정 역할입니다.

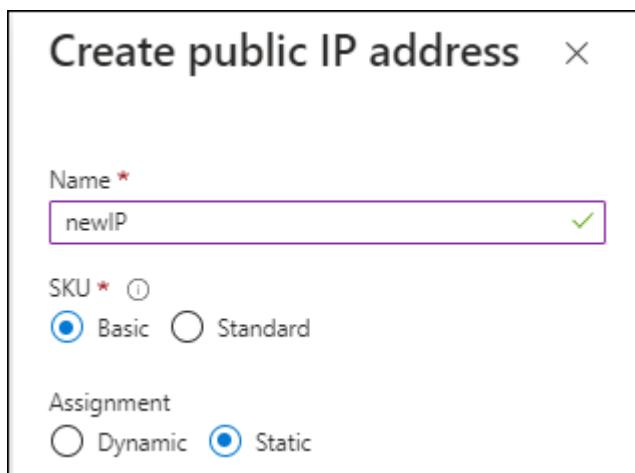
["Azure 권한을 설정하는 방법 알아보기"](#)

단계

- Azure Marketplace의 NetApp Console 에이전트 VM 페이지로 이동합니다.
 - ["상업 지역을 위한 Azure Marketplace 페이지"](#)
 - ["Azure Government 지역에 대한 Azure Marketplace 페이지"](#)
- *지금 받기*를 선택한 다음 *계속*을 선택하세요.
- 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.
- 공용 IP:** 콘솔 에이전트 VM에서 공용 IP 주소를 사용하려면 기본 SKU를 선택하십시오.



대신 표준 SKU IP 주소를 사용하면 콘솔은 공용 IP 대신 콘솔 에이전트의 개인 IP 주소를 사용합니다.

콘솔에 접속하는 데 사용하는 기기가 사설 IP 주소에 연결할 수 없는 경우 콘솔이 작동하지 않습니다.

"Azure 설명서: 공용 IP SKU"

- 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.

관리되는 ID를 사용하면 콘솔 에이전트 VM이 자격 증명 없이 Microsoft Entra ID에 자신을 식별할 수 있습니다. ["Azure 리소스에 대한 관리 ID에 대해 자세히 알아보세요."](#).

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

결과

Azure는 지정된 설정으로 가상 머신을 배포합니다. 가상 머신과 콘솔 에이전트 소프트웨어는 약 5분 안에 실행될 것입니다.

다음은 무엇인가요?

NetApp Console 설정합니다.

수동 설치 (Google Cloud에서 사용해야 함)

AWS, Azure 또는 Google Cloud에서 실행 중인 자체 Linux 호스트에 콘솔 에이전트를 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"](#).

- 설치 중에 아웃바운드 연결을 확인하는 구성 검사를 비활성화해야 합니다. 이 검사를 비활성화하지 않으면 수동 설치가 실패합니다. ["수동 설치에 대한 구성 검사를 비활성화하는 방법을 알아보세요."](#)
- 콘솔 에이전트를 설치하기 전에 운영 체제에 따라 Podman 또는 Docker Engine이 필요합니다.

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.

결과

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

다음은 무엇인가요?

NetApp Console 설정합니다.

2단계: NetApp Console 설정

처음으로 콘솔에 액세스하면 콘솔 에이전트의 조직을 선택하라는 메시지가 표시되고 제한 모드를 활성화해야 합니다.

시작하기 전에

콘솔 에이전트를 설정하는 사람은 콘솔 조직에 속하지 않은 로그인을 사용하여 콘솔에 로그인해야 합니다.

로그인 정보가 다른 기관과 연결되어 있는 경우, 새 로그인 정보를 사용하여 가입해야 합니다. 그렇지 않으면 설정화면에서 제한 모드를 활성화하는 옵션이 표시되지 않습니다.

단계

1. 콘솔 에이전트 인스턴스에 연결된 호스트에서 웹 브라우저를 열고 설치한 콘솔 에이전트의 다음 URL을 입력합니다.
2. NetApp Console에 가입하거나 로그인하세요.
3. 로그인한 후 콘솔을 설정하세요.
 - a. 콘솔 에이전트의 이름을 입력하세요.
 - b. 새로운 콘솔 조직의 이름을 입력하세요.
 - c. *보안된 환경에서 실행하고 있습니까?*를 선택하세요.
 - d. *이 계정에서 제한 모드 사용*을 선택하세요.

계정이 생성된 후에는 이 설정을 변경할 수 없습니다. 제한 모드는 나중에 활성화할 수 없고, 나중에 비활성화할 수도 없습니다.

정부 지역에 콘솔 에이전트를 배포한 경우 확인란이 이미 활성화되어 있으므로 변경할 수 없습니다. 제한 모드는 정부 지역에서 지원되는 유일한 모드이기 때문입니다.

- a. *시작하기*를 선택하세요.

결과

이제 콘솔 에이전트가 설치되고 콘솔 조직에 설정되었습니다. 모든 사용자는 콘솔 에이전트 인스턴스의 IP 주소를 사용하여 콘솔에 액세스해야 합니다.

다음은 무엇인가요?

이전에 설정한 권한을 콘솔에 제공하세요.

3단계: 콘솔 에이전트에 권한 제공

Azure Marketplace에서 또는 수동으로 콘솔 에이전트를 설치한 경우 이전에 설정한 권한을 부여해야 합니다.

배포 중에 필요한 IAM 역할을 선택했기 때문에 AWS Marketplace에서 콘솔 에이전트를 배포한 경우에는 이러한 단계가 적용되지 않습니다.

["클라우드 권한을 준비하는 방법을 알아보세요"](#).

AWS IAM 역할

이전에 생성한 IAM 역할을 콘솔 에이전트를 설치한 EC2 인스턴스에 연결합니다.

이 단계는 AWS에 콘솔 에이전트를 수동으로 설치한 경우에만 적용됩니다. AWS Marketplace 배포의 경우 이미 필요한 권한이 포함된 IAM 역할과 콘솔 에이전트 인스턴스를 연결했습니다.

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.

AWS 액세스 키

필요한 권한이 있는 IAM 사용자의 AWS 액세스 키를 NetApp Console에 제공합니다.

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.

Azure 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.

Azure 서비스 주체

이전에 설정한 Azure 서비스 주체에 대한 자격 증명을 NetApp Console 제공합니다.

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 NetApp Console Azure에서 사용자를 대신하여 작업을 수행하는 데 필요한 권한을 갖게 되었습니다.

Google Cloud 서비스 계정

서비스 계정을 콘솔 에이전트 VM과 연결합니다.

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

NetApp Intelligent Services 구독(제한 모드)

클라우드 공급업체의 마켓플레이스에서 NetApp Intelligent Services 구독하면 시간당 요금(PAYGO) 또는 연간 계약을 통해 데이터 서비스 비용을 지불할 수 있습니다. NetApp (BYOL)에서 라이선스를 구매한 경우 마켓플레이스 제공 서비스도 구독해야 합니다. 귀하의 라이센스 요금이 항상 먼저 청구되지만, 라이센스 용량을 초과하거나 라이센스 기간이 만료되면 시간당 요금이 청구됩니다.

마켓플레이스 구독을 통해 제한 모드로 다음 데이터 서비스에 대한 요금을 청구할 수 있습니다.

- NetApp Backup and Recovery
- Cloud Volumes ONTAP
- NetApp Cloud Tiering
- NetApp Ransomware Resilience
- NetApp Disaster Recovery

NetApp Data Classification 구독을 통해 활성화되지만 분류 사용에는 비용이 청구되지 않습니다.

시작하기 전에

데이터 서비스를 구독하려면 콘솔 에이전트를 이미 배포했어야 합니다. 콘솔 에이전트에 연결된 클라우드 자격 증명에 마켓플레이스 구독을 연결해야 합니다.

AWS

단계

- *관리 > 자격 증명*을 선택합니다.
- *조직 자격 증명*을 선택하세요.
- 콘솔 에이전트와 연결된 자격 증명 세트에 대한 작업 메뉴를 선택한 다음 *구독 구성*을 선택합니다.

콘솔 에이전트와 연결된 자격 증명을 선택해야 합니다. NetApp Console과 연결된 자격 증명에는 마켓플레이스 구독을 연결할 수 없습니다.

The screenshot shows the AWS IAM Instance Profile configuration page. It lists two profiles:

- aws**: AWS Instance Profile, Type: Instance Profile | Connector. Details: AWS Account ID (297337421911), IAM Role (anilkumv-mdp-stg-conn1OCCM17295234525...), Subscription (4 View). Action buttons: Configure Subscription, Copy Credentials ID, Edit Credentials, Delete Credentials.
- azure_conn_cred**: Azure Keys | Connector. Details: Application ID (97164c15-9f84-420a-83a6-4f668729d206), Tenant ID (8e21f23a-10b9-46fb-9d50-720ef604be98), Subscriptions (3 View). Action buttons: 0 Working Environments.

- 자격 증명을 기존 구독과 연결하려면 아래쪽 목록에서 구독을 선택하고 *구성*을 선택합니다.
- 자격 증명을 새 구독과 연결하려면 *구독 추가 > 계속*을 선택하고 AWS Marketplace의 단계를 따르세요.
 - *구매 옵션 보기*를 선택하세요.
 - *구독*을 선택하세요.
 - *계정 설정*을 선택하세요.

NetApp Console로 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.

하늘빛

단계

- *관리 > 자격 증명*을 선택합니다.
- *조직 자격 증명*을 선택하세요.
- 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 Console로 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.

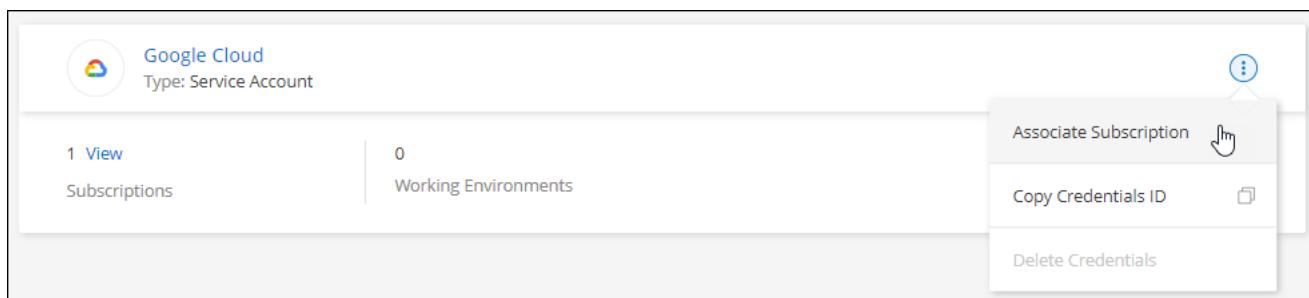
다른 모든 조직이나 계정의 경우 이 단계를 반복하여 구독을 수동으로 연결해야 합니다.

- *저장*을 선택하세요.

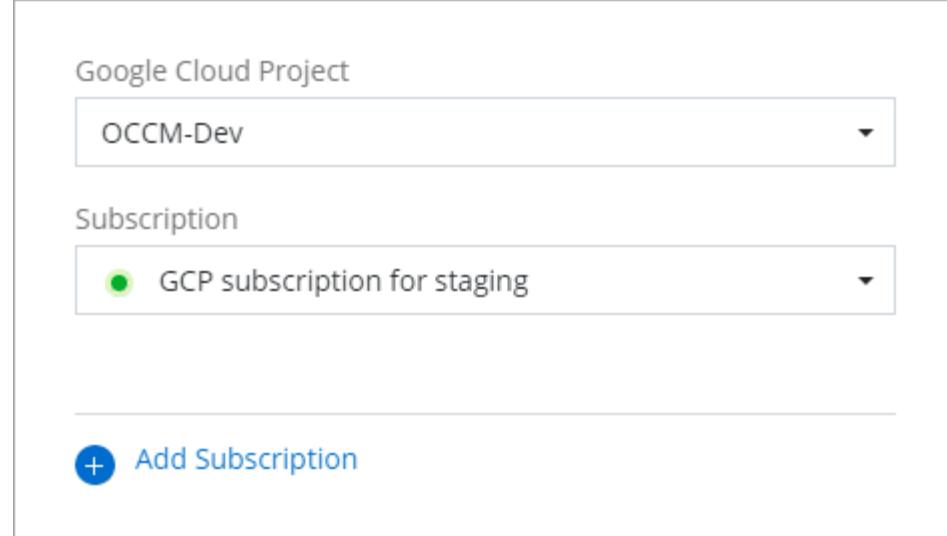
구글 클라우드

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.



NetApp Intelligent Services

[NetApp, Inc.](#)

Get best-in-class data protection and security for your workloads running on NetApp® ONTAP® storage.

[Subscribe](#)

[Overview](#)

[Pricing](#)

[Documentation](#)

[Support](#)

[Related Products](#)

Overview

NetApp offers a comprehensive suite of intelligent services for your ONTAP systems. They proactively protect critical workloads against evolving cyberthreats, detect and respond to ransomware attacks in real time, eliminate backup windows, and orchestrate a quick recovery in minutes when disaster strikes. NetApp intelligent services and Cloud

A
Ty
La
Ca

- 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.

Your order request has been sent to NetApp, Inc.



Your new subscription to the Cloud Manager 1 month plan for Cloud Manager for Cloud Volumes ONTAP requires your registration with NetApp, Inc.. After NetApp, Inc. approves your request, your subscription will be active and you will begin getting charged. This processing time will depend on the vendor, and you should reach out to NetApp, Inc. directly with any questions related to signup.

[VIEW ORDERS](#)

[REGISTER WITH NETAPP, INC.](#)

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.

Google Cloud Project

OCCM-Dev

Subscription

GCP subscription for staging

[Add Subscription](#)

관련 정보

- "[Cloud Volumes ONTAP 대한 BYOL 용량 기반 라이선스 관리](#)"
- "[데이터 서비스에 대한 BYOL 라이선스 관리](#)"
- "[AWS 자격 증명 및 구독 관리](#)"
- "[Azure 자격 증명 및 구독 관리](#)"
- "[Google Cloud 자격 증명 및 구독 관리](#)"

다음에 할 수 있는 일(제한 모드)

제한 모드에서 NetApp Console 실행한 후에는 제한 모드에서 지원되는 서비스를 사용할 수 있습니다.

도움이 필요하면 다음 서비스에 대한 설명서를 참조하세요.

- "[Azure NetApp Files 문서](#)"
- "[백업 및 복구 문서](#)"
- "[분류 문서](#)"
- "[Cloud Volumes ONTAP 문서](#)"
- "[디지털 지갑 문서](#)"
- "[온프레미스 ONTAP 클러스터 문서](#)"
- "[복제 문서](#)"

관련 정보

["NetApp Console 배포 모드"](#)

비공개 모드 시작하기

시작하기 워크플로(BlueXP 개인 모드)

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

["BlueXP 개인 모드에 대한 PDF 문서"](#)

개인 모드에서 지원되는 기능 및 데이터 서비스

다음 표는 어떤 BlueXP 서비스와 기능이 개인 모드에서 지원되는지 빠르게 식별하는 데 도움이 됩니다.

일부 서비스는 제한적으로 지원될 수 있습니다.

제품 영역	BlueXP 서비스 또는 기능	개인 모드
작업 환경 이 표의 일부는 BlueXP 캔버스에서 작업 환경 관리에 대한 지원을 나열합니다. BlueXP backup and recovery 에 지원되는 백업 대상은 표시되지 않습니다.	ONTAP 용 Amazon FSx	아니요
	아마존 S3	아니요
	Azure Blob	아니요
	Azure NetApp Files	아니요
	Cloud Volumes ONTAP	예
	Google Cloud NetApp Volumes	아니요
	구글 클라우드 스토리지	아니요
	온프레미스 ONTAP 클러스터	예
	E-시리즈	아니요
	StorageGRID	아니요
서비스	알림	아니요
	백업 및 복구	예 https://docs.netapp.com/us-en/data-services-backup-recovery/prev-ontap-protect-journey.html#support-for-sites-with-no-internet-connectivity [{"ONTAP 볼륨 데이터에 대해 지원되는 백업 대상 목록 보기"}]
	분류	예
	복사 및 동기화	아니요
	디지털 어드바이저	아니요
	디지털 지갑	예
	재해 복구	아니요
	경제적 효율성	아니요
	랜섬웨어 복원력	아니요
	복제	예
	소프트웨어 업데이트	아니요
	지속 가능성	아니요
	티어링	아니요
	볼륨 캐싱	아니요
	작업량 공장	아니요

제품 영역	BlueXP 서비스 또는 기능	개인 모드
특징	ID 및 액세스 관리	예
	신임장	예
	연합	아니요
	다중 요소 인증	아니요
	NSS 계정	아니요
	알림	아니요
	찾다	아니요
	타임라인	예

저작권 정보

Copyright © 2026 NetApp, Inc. All Rights Reserved. 미국에서 인쇄됨 본 문서의 어떠한 부분도 저작권 소유자의 사전 서면 승인 없이는 어떠한 형식이나 수단(복사, 녹음, 녹화 또는 전자 검색 시스템에 저장하는 것을 비롯한 그레픽, 전자적 또는 기계적 방법)으로도 복제될 수 없습니다.

NetApp이 저작권을 가진 자료에 있는 소프트웨어에는 아래의 라이센스와 고지사항이 적용됩니다.

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

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

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

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

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

상표 정보

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