



포트

NetApp Console setup and administration

NetApp

October 15, 2025

목차

| | |
|---------------------------------|---|
| 포트 | 1 |
| AWS의 콘솔 에이전트 보안 그룹 규칙 | 1 |
| 인바운드 규칙 | 1 |
| 아웃바운드 규칙 | 1 |
| Azure의 콘솔 에이전트 보안 그룹 규칙 | 2 |
| 인바운드 규칙 | 2 |
| 아웃바운드 규칙 | 3 |
| Google Cloud의 에이전트 방화벽 규칙 | 3 |
| 인바운드 규칙 | 3 |
| 아웃바운드 규칙 | 4 |
| 온프레미스 콘솔 에이전트용 포트 | 4 |

포트

AWS의 콘솔 에이전트 보안 그룹 규칙

에이전트의 AWS 보안 그룹에는 인바운드 규칙과 아웃바운드 규칙이 모두 필요합니다. NetApp 콘솔에서 콘솔 에이전트를 생성하면 NetApp Console 자동으로 이 보안 그룹을 생성합니다. 다른 모든 설치 옵션의 경우 이 보안 그룹을 설정해야 합니다.

인바운드 규칙

| 규약 | 포트 | 목적 |
|-------|------|---------------------------------------------------------------------------------------------------------------------------------------------|
| SSH | 22 | 에이전트 호스트에 SSH 액세스를 제공합니다. |
| HTTP | 80 | <ul style="list-style-type: none">클라이언트 웹 브라우저에서 로컬 사용자 인터페이스로 HTTP 액세스를 제공합니다.Cloud Volumes ONTAP 업그레이드 프로세스 중에 사용됨 |
| HTTPS | 443 | 로컬 사용자 인터페이스에 대한 HTTPS 액세스와 NetApp Data Classification 인스턴스의 연결을 제공합니다. |
| TCP | 3128 | Cloud Volumes ONTAP 에 인터넷 접속을 제공합니다. 배포 후에는 수동으로 이 포트를 열어야 합니다. |

아웃바운드 규칙

에이전트에 대해 미리 정의된 보안 그룹은 모든 아웃바운드 트래픽을 개방합니다. 이것이 허용된다면, 기본적인 아웃바운드 규칙을 따르세요. 더욱 엄격한 규칙이 필요한 경우 고급 아웃바운드 규칙을 사용하세요.

기본 아웃바운드 규칙

에이전트에 대한 미리 정의된 보안 그룹에는 다음과 같은 아웃바운드 규칙이 포함됩니다.

| 규약 | 포트 | 목적 |
|--------|----|--------------|
| 모든 TCP | 모두 | 모든 아웃바운드 트래픽 |
| 모든 UDP | 모두 | 모든 아웃바운드 트래픽 |

고급 아웃바운드 규칙

아웃바운드 트래픽에 대한 엄격한 규칙이 필요한 경우 다음 정보를 사용하여 에이전트의 아웃바운드 통신에 필요한 포트만 열 수 있습니다.



소스 IP 주소는 에이전트 호스트입니다.

| 서비스 | 규약 | 포트 | 목적지 | 목적 |
|----------------------|-------|------|-------------------------------|--------------------------------------------------------------------------------------------------|
| API 호출 및 AutoSupport | HTTPS | 443 | 아웃바운드 인터넷 및 ONTAP 클러스터 관리 LIF | AWS, ONTAP, NetApp Data Classification 대한 API 호출 및 NetApp에 대한 AutoSupport에 대한 AutoSupport 메시지 전송 |
| API 호출 | TCP | 3000 | ONTAP HA 중재자 | ONTAP HA 중재자와의 커뮤니케이션 |
| | TCP | 8080 | 데이터 분류 | 배포 중 데이터 분류 인스턴스에 대한 프로브 |
| DNS | UDP | 53 | DNS | 콘솔에서 DNS를 확인하는 데 사용됩니다. |

Azure의 콘솔 에이전트 보안 그룹 규칙

에이전트의 Azure 보안 그룹에는 인바운드 규칙과 아웃바운드 규칙이 모두 필요합니다. NetApp Console 에서 콘솔 에이전트를 만들면 이 보안 그룹이 자동으로 생성됩니다. 다른 설치 옵션의 경우 이 보안 그룹을 수동으로 설정해야 합니다.

인바운드 규칙

| 규약 | 포트 | 목적 |
|-------|------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| SSH | 22 | 에이전트 호스트에 SSH 액세스를 제공합니다. |
| HTTP | 80 | <ul style="list-style-type: none"> 클라이언트 웹 브라우저에서 로컬 사용자 인터페이스로 HTTP 액세스를 제공합니다. Cloud Volumes ONTAP 업그레이드 프로세스 중에 사용됨 |
| HTTPS | 443 | 클라이언트 웹 브라우저에서 로컬 사용자 인터페이스로의 HTTPS 액세스와 NetApp Data Classification 인스턴스로부터의 연결을 제공합니다. |
| TCP | 3128 | NetApp 지원팀에 AutoSupport 메시지를 보내기 위해 Cloud Volumes ONTAP에 인터넷 액세스를 제공합니다. 배포 후에는 수동으로 이 포트를 열어야 합니다. "에이전트가 AutoSupport 메시지의 프록시로 사용되는 방식을 알아보세요." |

아웃바운드 규칙

에이전트에 대해 미리 정의된 보안 그룹은 모든 아웃바운드 트래픽을 개방합니다. 이것이 허용된다면, 기본적인 아웃바운드 규칙을 따르세요. 더욱 엄격한 규칙이 필요한 경우 고급 아웃바운드 규칙을 사용하세요.

기본 아웃바운드 규칙

에이전트에 대한 미리 정의된 보안 그룹에는 다음과 같은 아웃바운드 규칙이 포함됩니다.

| 규약 | 포트 | 목적 |
|--------|----|--------------|
| 모든 TCP | 모두 | 모든 아웃바운드 트래픽 |
| 모든 UDP | 모두 | 모든 아웃바운드 트래픽 |

고급 아웃바운드 규칙

아웃바운드 트래픽에 대한 엄격한 규칙이 필요한 경우 다음 정보를 사용하여 에이전트의 아웃바운드 통신에 필요한 포트만 열 수 있습니다.



소스 IP 주소는 에이전트 호스트입니다.

| 서비스 | 규약 | 포트 | 목적지 | 목적 |
|----------------------|-------|------|-------------------------------|------------------------------------------------------------------------------------|
| API 호출 및 AutoSupport | HTTPS | 443 | 아웃바운드 인터넷 및 ONTAP 클러스터 관리 LIF | Azure, ONTAP, NetApp Data Classification 대한 API 호출 및 NetApp에 대한 AutoSupport 메시지 전송 |
| API 호출 | TCP | 8080 | 데이터 분류 | 배포 중 데이터 분류 인스턴스에 대한 프로브 |
| DNS | UDP | 53 | DNS | 콘솔에서 DNS를 확인하는 데 사용됩니다. |

Google Cloud의 에이전트 방화벽 규칙

에이전트에 대한 Google Cloud 방화벽 규칙에는 인바운드 규칙과 아웃바운드 규칙이 모두 필요합니다. NetApp Console 에서 콘솔 에이전트를 만들면 이 보안 그룹이 자동으로 생성됩니다. 다른 설치 옵션의 경우 이 보안 그룹을 수동으로 설정해야 합니다.

인바운드 규칙

| 규약 | 포트 | 목적 |
|-----|----|---------------------------|
| SSH | 22 | 에이전트 호스트에 SSH 액세스를 제공합니다. |

| 규약 | 포트 | 목적 |
|-------|------|------------------------------------------------------------------------------------------------------------------------------------------------|
| HTTP | 80 | <ul style="list-style-type: none"> 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. |
| TCP | 3128 | Cloud Volumes ONTAP 에 인터넷 접속을 제공합니다. 배포 후에는 수동으로 이 포트를 열어야 합니다. |

아웃바운드 규칙

에이전트의 사전 정의된 방화벽 규칙은 모든 아웃바운드 트래픽을 개방합니다. 허용되는 경우 기본 아웃바운드 규칙을 따르고, 더 엄격한 요구 사항이 있는 경우 고급 아웃바운드 규칙을 사용하세요.

기본 아웃바운드 규칙

에이전트에 대한 미리 정의된 방화벽 규칙에는 다음과 같은 아웃바운드 규칙이 포함됩니다.

| 규약 | 포트 | 목적 |
|--------|----|--------------|
| 모든 TCP | 모두 | 모든 아웃바운드 트래픽 |
| 모든 UDP | 모두 | 모든 아웃바운드 트래픽 |

고급 아웃바운드 규칙

아웃바운드 트래픽에 대한 엄격한 규칙이 필요한 경우 다음 정보를 사용하여 에이전트의 아웃바운드 통신에 필요한 포트만 열 수 있습니다.



소스 IP 주소는 에이전트 호스트입니다.

| 서비스 | 규약 | 포트 | 목적지 | 목적 |
|----------------------|-------|------|-------------------------------|--------------------------------------------------------------------------------------------|
| API 호출 및 AutoSupport | HTTPS | 443 | 아웃바운드 인터넷 및 ONTAP 클러스터 관리 LIF | Google Cloud, ONTAP, NetApp Data Classification 대한 API 호출 및 NetApp 에 대한 AutoSupport 메시지 전송 |
| API 호출 | TCP | 8080 | 데이터 분류 | 배포 중 데이터 분류 인스턴스에 대한 프로브 |
| DNS | UDP | 53 | DNS | 데이터 분류에 의한 DNS 확인에 사용됨 |

온프레미스 콘솔 에이전트용 포트

콘솔 에이전트는 온프레미스 Linux 호스트에 수동으로 설치되는 경우 인바운드 포트를

사용합니다. 계획 목적으로 다음 항목을 참조하세요.

이러한 인바운드 규칙은 모든 NetApp Console 배포 모드에 적용됩니다.

| 규약 | 포트 | 목적 |
|-------|-----|---------------------------------------------------------------------------------------------------------------------------------------------|
| HTTP | 80 | <ul style="list-style-type: none">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. |

저작권 정보

Copyright © 2025 NetApp, Inc. All Rights Reserved. 미국에서 인쇄된 본 문서의 어떠한 부분도 저작권 소유자의 사전 서면 승인 없이는 어떠한 형식이나 수단(복사, 녹음, 녹화 또는 전자 검색 시스템에 저장하는 것을 비롯한 그래픽, 전자적 또는 기계적 방법)으로도 복제될 수 없습니다.

NetApp이 저작권을 가진 자료에 있는 소프트웨어에는 아래의 라이선스와 고지사항이 적용됩니다.

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

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

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

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

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

상표 정보

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