# 요구 사항

## Amazon FSx for NetApp ONTAP

NetApp
November 28, 2023

This PDF was generated from https://docs.netapp.com/ko-kr/bluexp-fsx-ontap/requirements/task-setting-up-permissions-fsx.html on November 28, 2023. Always check docs.netapp.com for the latest.

# 목차

요구 사항 . . . . . 1
ONTAP용 FSx에 대한 권한을 설정합니다 . . . . . 1
ONTAP용 FSx에 대한 보안 그룹 규칙입니다 . . . . . 4

# 요구 사항

## ONTAP용 FSx에 대한 권한을 설정합니다

FSx for ONTAP 작업 환경을 생성하거나 관리하려면 FSx for ONTAP 작업 환경을 생성하는 데 필요한 권한을 BlueXP에 제공하는 IAM 역할의 ARN을 제공하여 AWS 자격 증명을 BlueXP에 추가해야 합니다.

### IAM 역할을 설정합니다

BlueXP가 역할을 맡을 수 있도록 IAM 역할을 설정합니다.

단계

1. 대상 계정에서 IAM 콘솔로 이동합니다.
2. AWS 계정에 BlueXP 액세스 권한 부여 액세스 관리에서 * 역할 > 역할 만들기 * 를 클릭하고 단계를 따라 역할을 만듭니다.
   - 신뢰할 수 있는 엔터티 유형 * 에서 * AWS 계정 * 을 선택합니다.
   - 다른 AWS 계정 * 을 선택하고 BlueXP * 계정 ID * 를 입력합니다.
     - BlueXP SaaS: 952013314444
     - AWS GovCloud(미국): 033442085313

     보안을 강화하기 위해 을(를) 지정하는 것이 좋습니다 "_외부 ID _". AWS 계정에 액세스하려면 BlueXP가 ARN(Amazon 리소스 이름) 역할과 사용자가 지정한 외부 ID를 제공해야 합니다. 그러면 가 방지됩니다 "혼란스러운 차관 문제".
3. 필요에 따라 다음과 같은 필수 최소 권한 및 선택적 권한이 포함된 정책을 만듭니다.

필수 권한

BlueXP에서 NetApp ONTAP 파일 시스템용 FSx를 생성하려면 다음 최소 권한이 필요합니다.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "VisualEditor0",
            "Effect": "Allow",
            "Action": [
                "fsx:*",
                "ec2:Describe*",
                "ec2:CreateTags",
                "iam:CreateServiceLinkedRole",
                "kms:Describe*",
                "kms:List*",
                "kms:CreateGrant"
            ],
            "Resource": "*"
        }
    ]
}
```

자동 용량

를 사용하려면 다음과 같은 추가 권한이 필요합니다 "자동 용량 관리".

```
"cloudwatch:GetMetricData",
"cloudwatch:GetMetricStatistics"
```

보안 그룹

BlueXP에서 를 사용하려면 다음과 같은 추가 권한이 필요합니다 "보안 그룹을 생성합니다".

```
"ec2:AuthorizeSecurityGroupEgress",
"ec2:AuthorizeSecurityGroupIngress",
"ec2:RevokeSecurityGroupEgress",
"ec2:RevokeSecurityGroupIngress",
"ec2:CreateSecurityGroup",
"ec2:DeleteSecurityGroup",
"cloudformation:CreateStack",
"cloudformation:ValidateTemplate",
"cloudformation:DescribeStacks",
"cloudformation:DescribeStackEvents"
```

4. 다음 단계에서 BlueXP에 붙여 넣을 수 있도록 IAM 역할의 ARN 역할을 복사합니다.

결과

이제 IAM 역할에 필요한 권한이 있습니다.

## 자격 증명을 추가합니다

필요한 권한을 IAM 역할에 제공한 후 ARN 역할을 BlueXP에 추가합니다.

시작하기 전에

IAM 역할을 방금 생성한 경우 새 자격 증명을 사용할 수 있도록 몇 분 동안 기다립니다.

단계

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

2. 자격 증명 추가 * 를 클릭하고 마법사의 단계를 따릅니다.
   a. * 자격 증명 위치 *: * Amazon Web Services > BlueXP * 를 선택합니다.
   b. * 자격 증명 정의 *: 자격 증명 이름 * 과 역할 ARN * 및 * 외부 ID * (지정된 경우)를 제공합니다 IAM 역할을 설정합니다.

   - AWS GovCloud(US) 계정을 사용하는 경우, * AWS GovCloud(US) 계정을 사용하고 있는지 확인하십시오 *.

   - AWS GovCloud를 사용하여 인증하면 SaaS 플랫폼이 비활성화됩니다. 이는 계정에 대한 영구적인 변경이며 실행 취소할 수 없습니다.

   c. * 검토 *: 새 자격 증명에 대한 세부 정보를 확인하고 * 추가 * 를 클릭합니다.

결과

이제 ONTAP 작업 환경에 대한 FSx를 생성할 때 자격 증명을 사용할 수 있습니다.

## 관련 링크

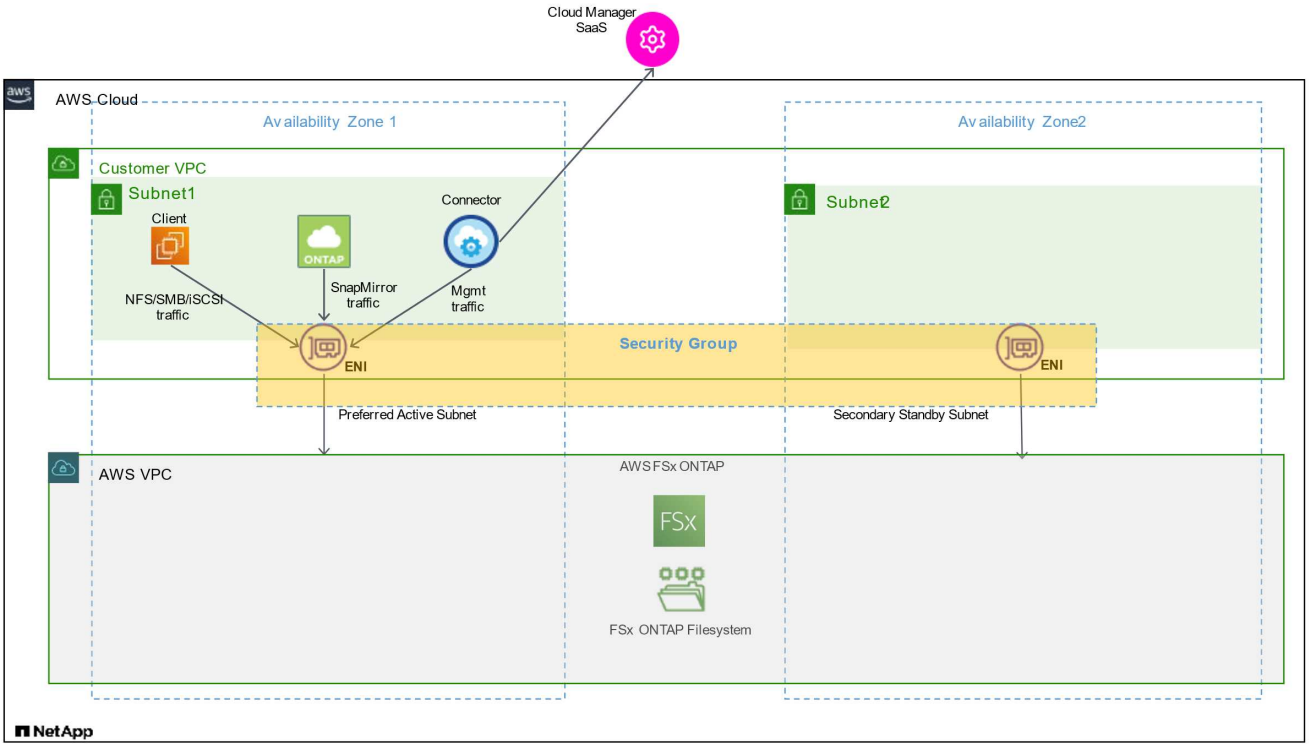
- "AWS 자격 증명 및 권한"
- "BlueXP에 대한 AWS 자격 증명 관리"

# ONTAP용 FSx에 대한 보안 그룹 규칙입니다

BlueXP는 ONTAP용 BlueXP 및 FSx의 성공적인 운영에 필요한 인바운드 및 아웃바운드 규칙을 포함하는 AWS 보안 그룹을 생성합니다. 테스트 목적으로 또는 자체 포트를 사용해야 하는 경우 포트를 참조할 수 있습니다.

## ONTAP의 FSx 규칙

ONTAP용 FSx 보안 그룹에는 인바운드 및 아웃바운드 규칙이 모두 필요합니다. 이 다이어그램은 ONTAP 네트워킹 구성 및 보안 그룹 요구 사항에 대한 FSx를 보여 줍니다.

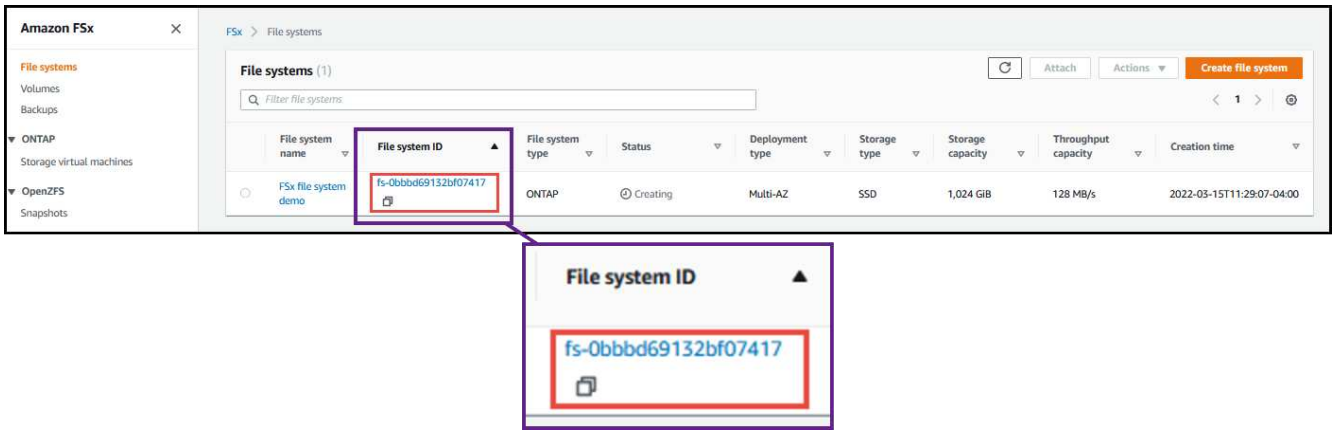



시작하기 전에

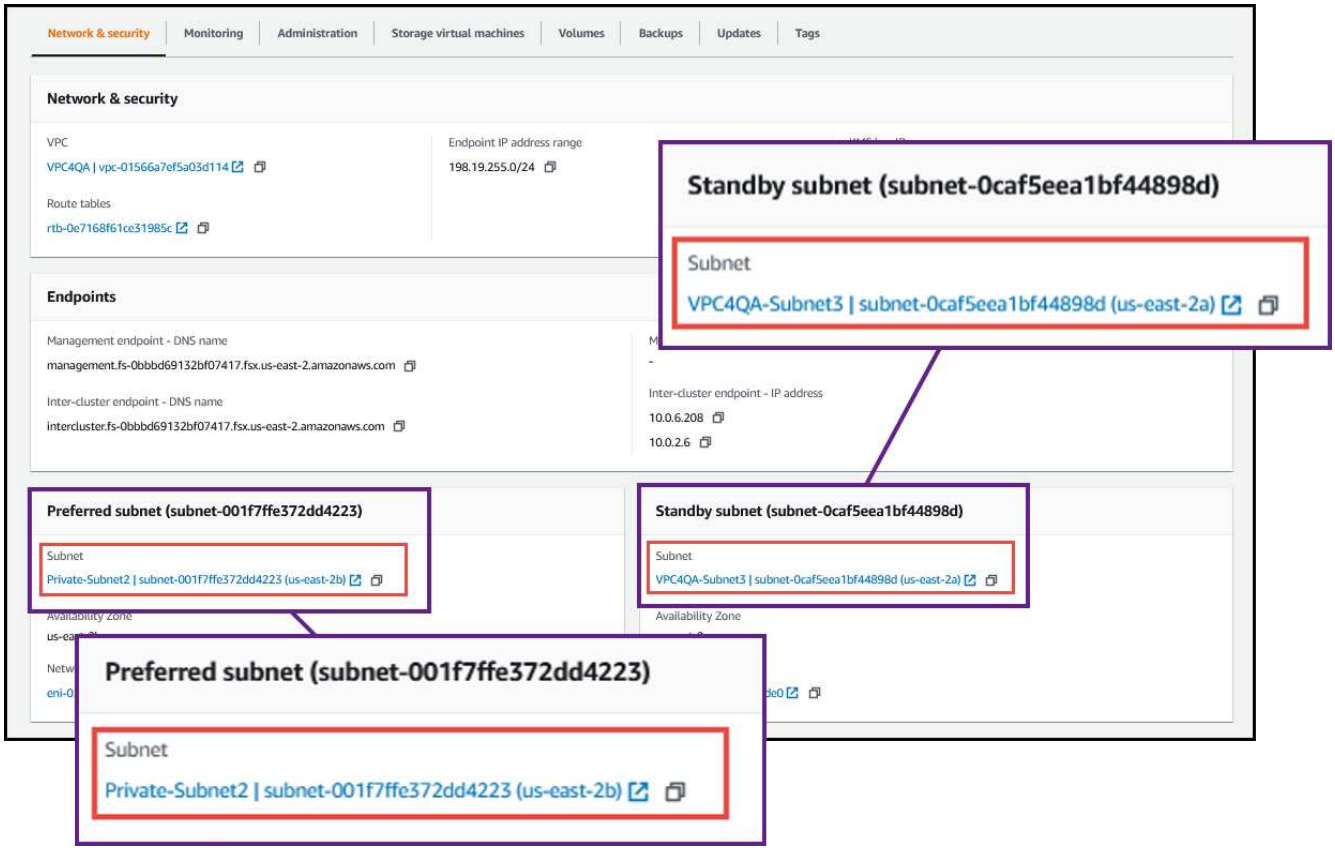
AWS 관리 콘솔을 사용하여 ENIs와 연결된 보안 그룹을 찾아야 합니다.

단계

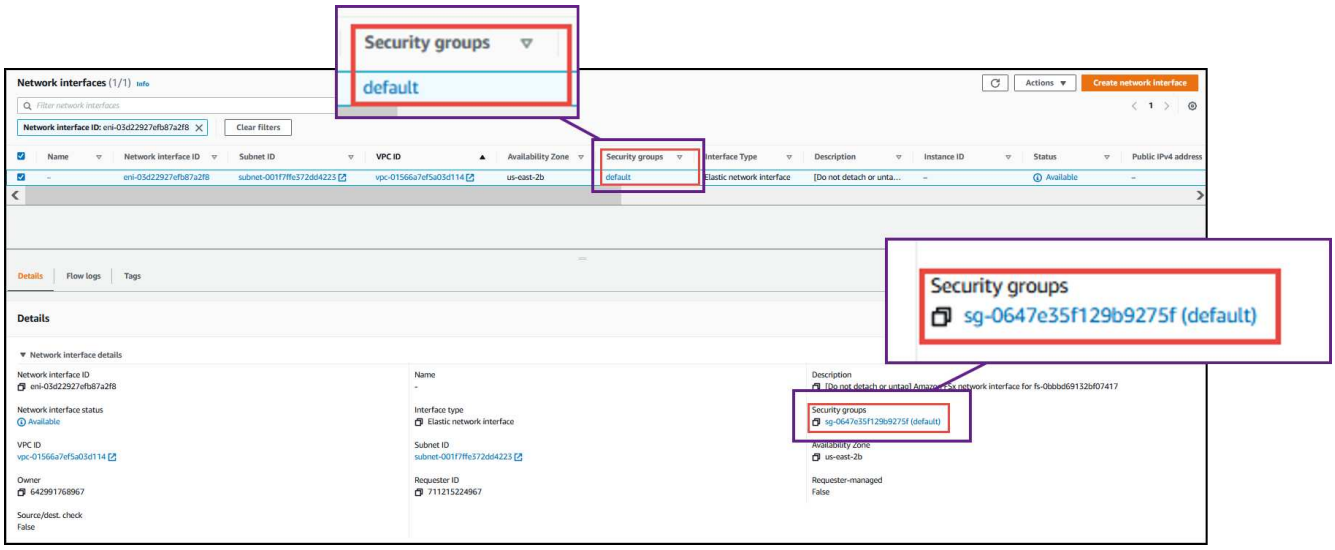
1. AWS 관리 콘솔에서 ONTAP용 FSx 파일 시스템을 열고 파일 시스템 ID 링크를 클릭합니다.




2. 네트워크 및 보안* 탭에서 기본 설정 또는 대기 서브넷의 네트워크 인터페이스 ID를 클릭합니다.




3. 네트워크 인터페이스 표에서 보안 그룹을 클릭하거나 네트워크 인터페이스의 * 세부 정보 * 섹션을 클릭합니다.




인바운드 규칙

| 프로토콜 | 포트 | 목적 |
|---|---|---|
| 모든 ICMP | 모두 | 인스턴스에 Ping을 수행 중입니다 |
| HTTPS | 443 | Connector에서 fsxadmin 관리 LIF로 액세스하여 FSx로 API 호출을 전송합니다 |
| SSH를 클릭합니다 | 22 | 클러스터 관리 LIF 또는 노드 관리 LIF의 IP 주소에 SSH를 액세스할 수 있습니다 |
| TCP | 111 | NFS에 대한 원격 프로시저 호출 |
| TCP | 139 | CIFS에 대한 NetBIOS 서비스 세션입니다 |
| TCP | 161-162 | 단순한 네트워크 관리 프로토콜 |
| TCP | 445 | Microsoft SMB/CIFS over TCP 및 NetBIOS 프레임 |
| TCP | 635 | NFS 마운트 |
| TCP | 749 | Kerberos |
| TCP | 2049 | NFS 서버 데몬 |
| TCP | 3260 | iSCSI 데이터 LIF를 통한 iSCSI 액세스 |
| TCP | 4045 | NFS 잠금 데몬 |
| TCP | 4046 | NFS에 대한 네트워크 상태 모니터 |
| TCP | 10000입니다 | NDMP를 사용한 백업 |
| TCP | 11104 | SnapMirror에 대한 인터클러스터 통신 세션의 관리 |
| TCP | 11105 | 인터클러스터 LIF를 사용하여 SnapMirror 데이터 전송 |
| UDP입니다 | 111 | NFS에 대한 원격 프로시저 호출 |

| 프로토콜 | 포트 | 목적 |
| --- | --- | --- |
| UDP입니다 | 161-162 | 단순한 네트워크 관리 프로토콜 |
| UDP입니다 | 635 | NFS 마운트 |
| UDP입니다 | 2049 | NFS 서버 데몬 |
| UDP입니다 | 4045 | NFS 잠금 데몬 |
| UDP입니다 | 4046 | NFS에 대한 네트워크 상태 모니터 |
| UDP입니다 | 4049 | NFS rquotad 프로토콜 |

아웃바운드 규칙

ONTAP용 FSx에 대해 미리 정의된 보안 그룹은 모든 아웃바운드 트래픽을 엽니다. 허용 가능한 경우 기본 아웃바운드 규칙을 따릅니다. 더 엄격한 규칙이 필요한 경우 고급 아웃바운드 규칙을 사용합니다.

기본 아웃바운드 규칙

ONTAP용 FSx에 대해 미리 정의된 보안 그룹에는 다음과 같은 아웃바운드 규칙이 포함됩니다.

| 프로토콜 | 포트 | 목적 |
| --- | --- | --- |
| 모든 ICMP | 모두 | 모든 아웃바운드 트래픽 |
| 모든 TCP | 모두 | 모든 아웃바운드 트래픽 |
| 모든 UDP | 모두 | 모든 아웃바운드 트래픽 |

고급 아웃바운드 규칙

ONTAP용 FSx에서 중재자를 위해 또는 노드 간에 특정 포트를 열 필요가 없습니다.

소스는 ONTAP 시스템용 FSx의 인터페이스(IP 주소)입니다.

| 서비스 | 프로토콜 | 포트 | 출처 | 목적지 | 목적 |
|---|---|---|---|---|---|
| Active Directory를 클릭합니다 | TCP | 88 | 노드 관리 LIF | Active Directory 포리스트입니다 | Kerberos V 인증 |
| | UDP입니다 | 137 | 노드 관리 LIF | Active Directory 포리스트입니다 | NetBIOS 이름 서비스입니다 |
| | UDP입니다 | 138 | 노드 관리 LIF | Active Directory 포리스트입니다 | NetBIOS 데이터그램 서비스 |
| | TCP | 139 | 노드 관리 LIF | Active Directory 포리스트입니다 | NetBIOS 서비스 세션입니다 |
| | TCP 및 UDP | 389 | 노드 관리 LIF | Active Directory 포리스트입니다 | LDAP를 지원합니다 |
| | TCP | 445 | 노드 관리 LIF | Active Directory 포리스트입니다 | Microsoft SMB/CIFS over TCP 및 NetBIOS 프레임 |
| | TCP | 464 | 노드 관리 LIF | Active Directory 포리스트입니다 | Kerberos V 변경 및 암호 설정(set_change) |
| | UDP입니다 | 464 | 노드 관리 LIF | Active Directory 포리스트입니다 | Kerberos 키 관리 |
| | TCP | 749 | 노드 관리 LIF | Active Directory 포리스트입니다 | Kerberos V 변경 및 암호 설정(RPCSEC_GSS) |
| | TCP | 88 | 데이터 LIF(NFS, CIFS, iSCSI) | Active Directory 포리스트입니다 | Kerberos V 인증 |
| | UDP입니다 | 137 | 데이터 LIF(NFS, CIFS) | Active Directory 포리스트입니다 | NetBIOS 이름 서비스입니다 |
| | UDP입니다 | 138 | 데이터 LIF(NFS, CIFS) | Active Directory 포리스트입니다 | NetBIOS 데이터그램 서비스 |
| | TCP | 139 | 데이터 LIF(NFS, CIFS) | Active Directory 포리스트입니다 | NetBIOS 서비스 세션입니다 |
| | TCP 및 UDP | 389 | 데이터 LIF(NFS, CIFS) | Active Directory 포리스트입니다 | LDAP를 지원합니다 |
| | TCP | 445 | 데이터 LIF(NFS, CIFS) | Active Directory 포리스트입니다 | Microsoft SMB/CIFS over TCP 및 NetBIOS 프레임 |
| | TCP | 464 | 데이터 LIF(NFS, CIFS) | Active Directory 포리스트입니다 | Kerberos V 변경 및 암호 설정(set_change) |
| | UDP입니다 | 464 | 데이터 LIF(NFS, CIFS) | Active Directory 포리스트입니다 | Kerberos 키 관리 |
| | TCP | 749 | 데이터 LIF(NFS, CIFS) | Active Directory 포리스트입니다 | Kerberos V 변경 및 암호 설정(RPCSEC_GSS) |
| S3로 백업 | TCP | 5010 | 인터클러스터 LIF | 엔드포인트 백업 또는 복원 | S3로 백업 기능의 백업 및 복원 작업 |
| DHCP를 선택합니다 | UDP입니다 | 68 | 노드 관리 LIF | DHCP를 선택합니다 | 처음으로 설정하는 DHCP 클라이언트 |

| 서비스 | 프로토콜 | 포트 | 출처 | 목적지 | 목적 |
|---|---|---|---|---|---|
| DHCPS | UDP입니다 | 67 | 노드 관리 LIF | DHCP를 선택합니다 | DHCP 서버 |
| DNS | UDP입니다 | 53 | 노드 관리 LIF 및 데이터 LIF(NFS, CIFS) | DNS | DNS |
| NDMP | TCP | 18600–18699 | 노드 관리 LIF | 대상 서버 | NDMP 복제 |
| SMTP | TCP | 25 | 노드 관리 LIF | 메일 서버 | AutoSupport에 사용할 수 있는 SMTP 경고 |
| SNMP를 선택합니다 | TCP | 161 | 노드 관리 LIF | 서버 모니터링 | SNMP 트랩으로 모니터링 |
| | UDP입니다 | 161 | 노드 관리 LIF | 서버 모니터링 | SNMP 트랩으로 모니터링 |
| | TCP | 162 | 노드 관리 LIF | 서버 모니터링 | SNMP 트랩으로 모니터링 |
| | UDP입니다 | 162 | 노드 관리 LIF | 서버 모니터링 | SNMP 트랩으로 모니터링 |
| SnapMirror를 참조하십시오 | TCP | 11104 | 인터클러스터 LIF | ONTAP 인터클러스터 LIF | SnapMirror에 대한 인터클러스터 통신 세션의 관리 |
| | TCP | 11105 | 인터클러스터 LIF | ONTAP 인터클러스터 LIF | SnapMirror 데이터 전송 |
| Syslog를 클릭합니다 | UDP입니다 | 514 | 노드 관리 LIF | Syslog 서버 | Syslog 메시지를 전달합니다 |

## 커넥터 규칙

Connector의 보안 그룹에는 인바운드 및 아웃바운드 규칙이 모두 필요합니다.

### 인바운드 규칙

| 프로토콜 | 포트 | 목적 |
|---|---|---|
| SSH를 클릭합니다 | 22 | 커넥터 호스트에 대한 SSH 액세스를 제공합니다 |
| HTTP | 80 | 클라이언트 웹 브라우저에서 로컬 사용자 인터페이스에 대한 HTTP 액세스 및 BlueXP 분류 인스턴스의 연결을 제공합니다 |
| HTTPS | 443 | 클라이언트 웹 브라우저에서 로컬 사용자 인터페이스로 HTTPS 액세스를 제공합니다 |
| TCP | 3128 | AWS 네트워크에서 NAT 또는 프록시를 사용하지 않는 경우 인터넷 액세스가 가능한 BlueXP 분류 인스턴스를 제공합니다 |

### 아웃바운드 규칙

Connector에 대해 미리 정의된 보안 그룹은 모든 아웃바운드 트래픽을 엽니다. 허용 가능한 경우 기본 아웃바운드

규칙을 따릅니다. 더 엄격한 규칙이 필요한 경우 고급 아웃바운드 규칙을 사용합니다.

#### 기본 아웃바운드 규칙

Connector에 대해 미리 정의된 보안 그룹에는 다음과 같은 아웃바운드 규칙이 포함됩니다.

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

#### 고급 아웃바운드 규칙

아웃바운드 트래픽에 대해 엄격한 규칙이 필요한 경우 다음 정보를 사용하여 Connector의 아웃바운드 통신에 필요한 포트만 열 수 있습니다.

> 소스 IP 주소는 커넥터 호스트입니다.

| 서비스 | 프로토콜 | 포트 | 목적지 | 목적 |
|---|---|---|---|---|
| Active Directory를 클릭합니다 | TCP | 88 | Active Directory 포리스트입니다 | Kerberos V 인증 |
| | TCP | 139 | Active Directory 포리스트입니다 | NetBIOS 서비스 세션입니다 |
| | TCP | 389 | Active Directory 포리스트입니다 | LDAP를 지원합니다 |
| | TCP | 445 | Active Directory 포리스트입니다 | Microsoft SMB/CIFS over TCP 및 NetBIOS 프레임 |
| | TCP | 464 | Active Directory 포리스트입니다 | Kerberos V 변경 및 암호 설정(set_change) |
| | TCP | 749 | Active Directory 포리스트입니다 | Active Directory Kerberos V 변경 및 암호 설정(RPCSEC_GSS) |
| | UDP입니다 | 137 | Active Directory 포리스트입니다 | NetBIOS 이름 서비스입니다 |
| | UDP입니다 | 138 | Active Directory 포리스트입니다 | NetBIOS 데이터그램 서비스 |
| | UDP입니다 | 464 | Active Directory 포리스트입니다 | Kerberos 키 관리 |
| API 호출 및 AutoSupport | HTTPS | 443 | 아웃바운드 인터넷 및 ONTAP 클러스터 관리 LIF | API는 AWS 및 ONTAP를 호출하고 AutoSupport 메시지를 NetApp에 보냅니다 |
| API 호출 | TCP | 8088 | S3로 백업 | API에서 S3로 백업을 호출합니다 |

| 서비스 | 프로토콜 | 포트 | 목적지 | 목적 |
| --- | --- | --- | --- | --- |
| DNS | UDP입니다 | 53 | DNS | BlueXP에서 DNS Resolve에 사용됩니다 |
| BlueXP 분류 | HTTP | 80 | BlueXP 분류 | Cloud Volumes ONTAP에 대한 BlueXP 분류 |

저작권 정보

Copyright © 2023 NetApp, Inc. All Rights Reserved. 미국에서 인쇄된 본 문서의 어떠한 부분도 저작권 소유자의 사전 서면 승인 없이는 어떠한 형식이나 수단(복사, 녹음, 녹화 또는 전자 검색 시스템에 저장하는 것을 비롯한 그래픽, 전자적 또는 기계적 방법)으로도 복제될 수 없습니다.

NetApp이 저작권을 가진 자료에 있는 소프트웨어에는 아래의 라이센스와 고지사항이 적용됩니다.

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

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

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

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

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

상표 정보

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