



시작하십시오

Amazon FSx for ONTAP

NetApp
May 03, 2022

목차

시작하십시오	1
ONTAP용 Amazon FSx에 대해 자세히 알아보십시오	1
ONTAP용 Amazon FSx를 시작하십시오	2
ONTAP용 FSx에 대한 권한을 설정합니다	2
ONTAP용 FSx에 대한 보안 그룹 규칙입니다	4

시작하십시오

ONTAP용 Amazon FSx에 대해 자세히 알아보십시오

"ONTAP용 Amazon FSx"는 고객이 NetApp의 ONTAP 스토리지 운영 체제가 제공하는 파일 시스템을 실행하고 실행할 수 있도록 하는 완전 관리형 서비스입니다. ONTAP용 FSx는 NetApp 고객이 사내에서 사용하는 것과 동일한 기능, 성능 및 관리 기능을 기본 AWS 서비스의 단순성, 민첩성, 보안 및 확장성으로 제공합니다.

피처

- 스토리지 디바이스, 소프트웨어 또는 백업을 구성하거나 관리할 필요가 없습니다.
- CIFS, NFSv3, NFSv4.x 및 SMB v2.0-v3.1.1 프로토콜 지원
- 자주 액세스하지 않는(IA) 스토리지 계층을 사용하여 저렴한 비용으로 사실상 제한 없는 데이터 스토리지 용량을 확보할 수 있습니다.
- Oracle RAC를 포함하여 지연 시간에 민감한 애플리케이션에서 실행되도록 인증받았습니다.
- 번들 및 용량제 가격 선택 가능

추가 기능은 Cloud Manager에서 제공됩니다

- AWS 및 Cloud Manager의 커넥터를 사용하여 볼륨을 생성 및 관리하고, 데이터를 복제하고, ONTAP용 FSx를 데이터 센스 및 Cloud Sync와 같은 NetApp 클라우드 서비스와 통합할 수 있습니다.
- 클라우드 데이터 센스는 인공 지능(AI) 기반 기술을 사용하여 데이터 컨텍스트를 이해하고 FSx for ONTAP 계정에 상주하는 중요한 데이터를 식별하는 데 도움을 줄 수 있습니다. ["자세한 정보"](#).
- NetApp Cloud Sync를 사용하면 클라우드 또는 사내 타겟으로 데이터 마이그레이션을 자동화할 수 있습니다. ["자세한 정보"](#)

비용

ONTAP용 FSx 계정은 Cloud Manager가 아니라 AWS에서 유지 관리됩니다. ["ONTAP용 Amazon FSx 시작 가이드"](#)

AWS에서 커넥터를 사용하는 것과 Cloud Sync 및 데이터 센스와 같은 선택적 데이터 서비스를 사용하는 것과 관련된 추가 비용이 있습니다.

지원 지역

["지원되는 아마존 지역을 봅니다."](#)

도움말 보기

ONTAP용 Amazon FSx는 AWS 최초의 솔루션입니다. 이 서비스를 사용하는 AWS FSx 파일 시스템, 인프라 또는 AWS 솔루션과 관련된 질문이나 기술 지원 문제가 있는 경우 AWS 콘솔의 Support Center를 사용하여 AWS에 지원 케이스를 접수하십시오. "FSx for ONTAP" 서비스와 적절한 범주를 선택합니다. AWS 지원 케이스를 생성하는 데 필요한 나머지 정보를 제공합니다.

Cloud Manager 또는 Cloud Manager 마이크로 서비스와 관련된 일반적인 질문은 인라인 Cloud Manager 채팅으로

시작할 수 있습니다.

Cloud Manager 또는 내의 마이크로 서비스와 관련된 기술 지원 문제의 경우 Cloud Manager 계정 레벨 일련 번호를 사용하여 NetApp 지원 티켓을 열 수 있습니다. 지원을 활성화하려면 Cloud Manager 일련 번호를 등록해야 합니다.

제한 사항

- Cloud Manager는 온프레미스 또는 Cloud Volumes ONTAP에서 ONTAP용 FSx로 데이터를 복제할 수 있습니다.
- 이때 ONTAP CLI, ONTAP API 또는 Cloud Manager API를 사용하여 iSCSI 볼륨을 생성할 수 있습니다.

ONTAP용 Amazon FSx를 시작하십시오

몇 가지 단계를 통해 ONTAP용 Amazon FSx를 시작해 보십시오.

몇 단계만 거치면 ONTAP용 FSx를 시작할 수 있습니다.

볼륨을 추가하기 전에 ONTAP 작업 환경을 위한 Amazon FSx를 생성해야 합니다. 이 작업을 수행해야 합니다 ["Cloud Manager SaaS가 역할을 맡을 수 있도록 IAM 역할을 설정합니다"](#).

가 있어야 합니다 ["AWS용 커넥터"](#) ONTAP 작업 환경을 위한 FSx를 열려면 볼륨을 생성하거나 다른 작업을 수행합니다. Connector가 필요한 경우 Cloud Manager에서 아직 추가되지 않은 경우 이를 묻습니다.

Cloud Manager를 사용하여 ONTAP 볼륨용 FSx를 생성할 수 있습니다.

Cloud Manager를 사용하여 볼륨을 관리하고 복제, Cloud Sync, 데이터 센스와 같은 추가 서비스를 구성합니다.

관련 링크

- ["Cloud Manager에서 커넥터 생성"](#)
- ["AWS Marketplace에서 커넥터 실행"](#)
- ["Linux 호스트에 Connector 소프트웨어 설치"](#)

ONTAP용 FSx에 대한 권한을 설정합니다

ONTAP 작업 환경을 위한 Amazon FSx를 생성 또는 관리하려면 Cloud Manager에 ONTAP 작업 환경을 위한 FSx를 생성하는 데 필요한 권한을 제공하는 IAM 역할의 ARN을 제공하여 AWS 자격 증명을 Cloud Manager에 추가해야 합니다.

IAM 역할을 설정합니다

Cloud Manager SaaS가 역할을 맡을 수 있도록 IAM 역할을 설정합니다.

단계

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

다음을 수행하십시오.

- 신뢰할 수 있는 엔터티 유형 * 에서 * AWS 계정 * 을 선택합니다.
- 다른 AWS 계정 * 을 선택하고 Cloud Manager SaaS:952013314444의 ID를 입력합니다
- 다음 권한이 포함된 정책을 만듭니다.

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

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

이제 IAM 역할에 필요한 권한이 있습니다.

자격 증명을 추가합니다

필요한 권한을 IAM 역할에 제공한 후 ARN 역할을 Cloud Manager에 추가합니다.

방금 IAM 역할을 생성한 경우 사용할 수 있을 때까지 몇 분 정도 걸릴 수 있습니다. 몇 분 후에 Cloud Manager에 자격 증명을 추가합니다.

단계

1. Cloud Manager 콘솔의 오른쪽 위에서 설정 아이콘을 클릭하고 * 자격 증명 * 을 선택합니다.



2. 자격 증명 추가 * 를 클릭하고 마법사의 단계를 따릅니다.
 - a. * 자격 증명 위치 *: * Amazon Web Services > Cloud Manager * 를 선택합니다.
 - b. * 자격 증명 정의 *: IAM 역할의 ARN(Amazon Resource Name)을 제공합니다.

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

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

관련 링크

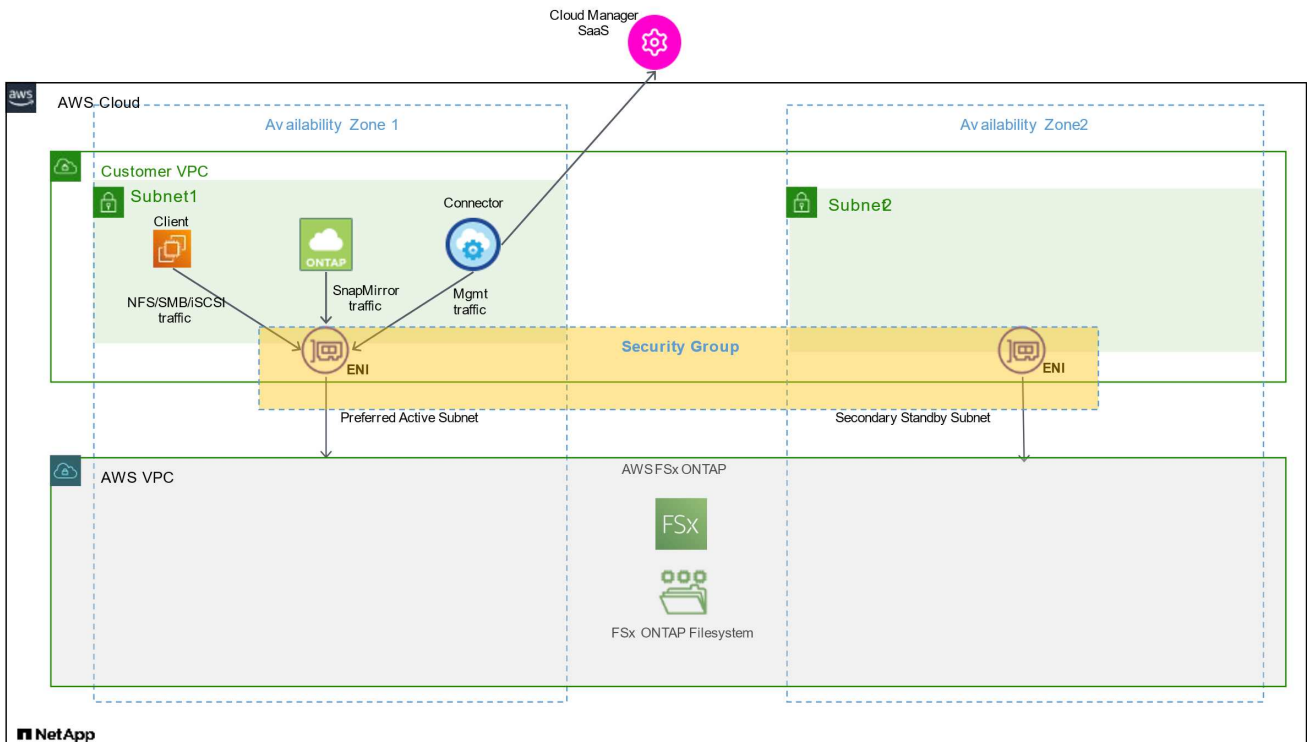
- ["AWS 자격 증명 및 권한"](#)
- ["Cloud Manager의 AWS 자격 증명 관리"](#)

ONTAP용 FSx에 대한 보안 그룹 규칙입니다

Cloud Manager는 Cloud Manager 및 FSx for ONTAP가 성공적으로 운영하는 데 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

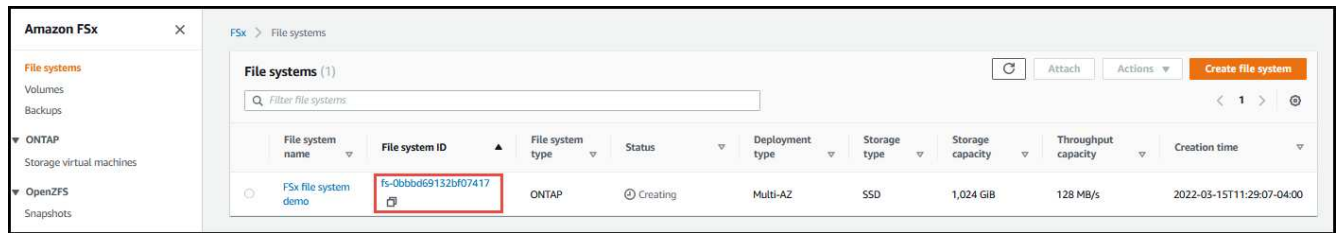
ONTAP용 FSx 보안 그룹에는 인바운드 및 아웃바운드 규칙이 모두 필요합니다. 이 다이어그램은 ONTAP 네트워킹 구성 및 보안 그룹 요구 사항에 대한 FSx를 보여 줍니다.



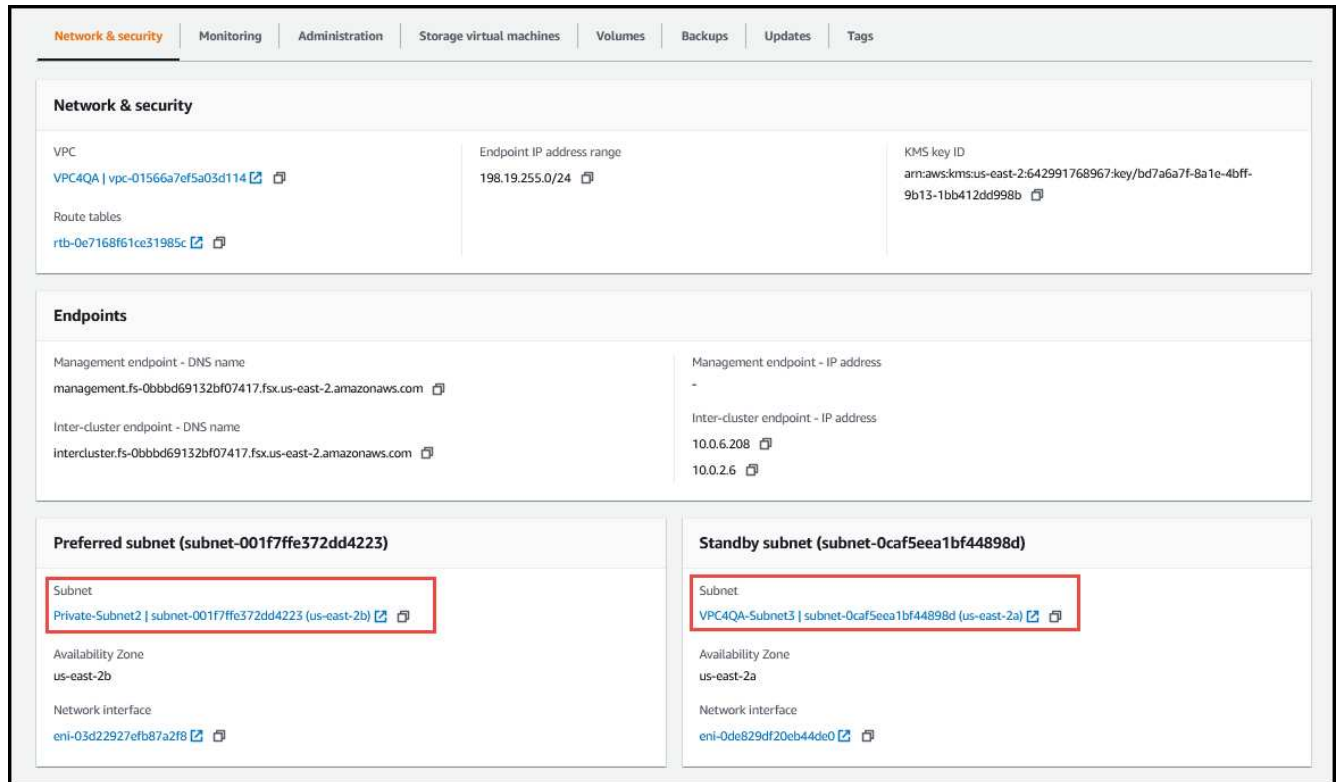
AWS 관리 콘솔을 사용하여 ENIs와 연결된 보안 그룹을 찾아야 합니다.

단계

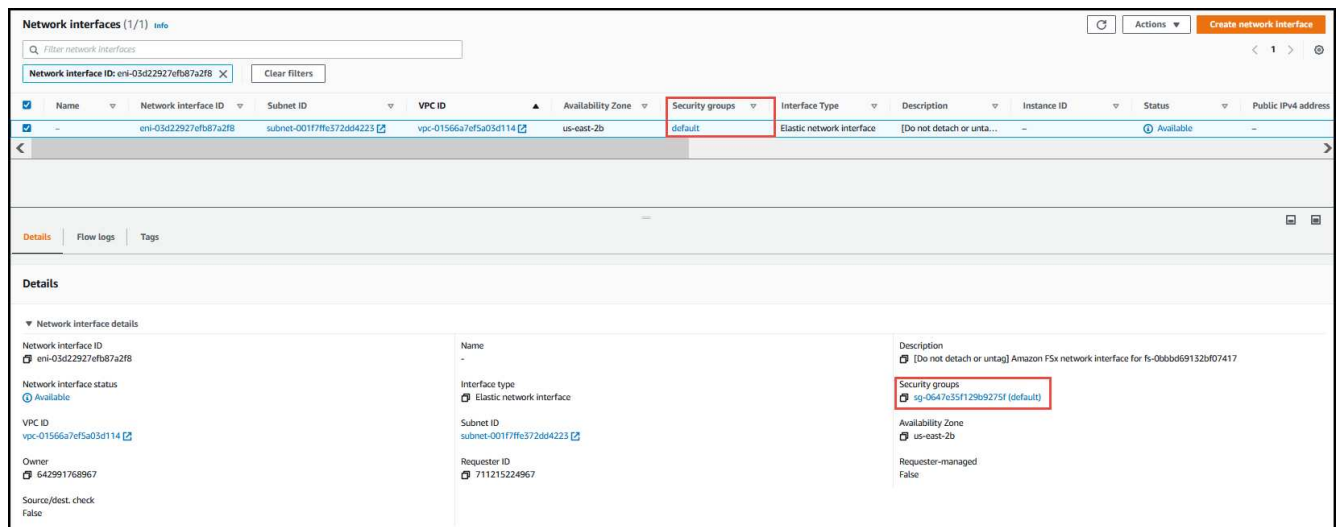
1. AWS 관리 콘솔에서 ONTAP용 FSx 파일 시스템을 열고 파일 시스템 ID 링크를 클릭합니다.



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
HTTP	80	클러스터 관리 LIF의 IP 주소를 사용하여 System Manager 웹 콘솔에 대한 HTTP 액세스
HTTPS	443	클러스터 관리 LIF의 IP 주소를 사용하여 System Manager 웹 콘솔에 대한 HTTPS 액세스
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
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 quotad 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
DHCP	UDP입니 다	67	노드 관리 LIF	DHCP를 선택합니다	DHCP 서버
DNS	UDP입니 다	53	노드 관리 LIF 및 데이터 LIF(NFS, CIFS)	DNS	DNS
NDMP	TCP	1860 0-18 699	노드 관리 LIF	대상 서버	NDMP 복제
SMTP	TCP	25	노드 관리 LIF	메일 서버	AutoSupport에 사용할 수 있는 SMTP 경고
SNMP를 선택합니 다	TCP	161	노드 관리 LIF	서버 모니터링	SNMP 트랩으로 모니터링
	UDP입니 다	161	노드 관리 LIF	서버 모니터링	SNMP 트랩으로 모니터링
	TCP	162	노드 관리 LIF	서버 모니터링	SNMP 트랩으로 모니터링
	UDP입니 다	162	노드 관리 LIF	서버 모니터링	SNMP 트랩으로 모니터링
SnapMirr or를 참조하십 시오	TCP	1110 4	인터클러스터 LIF	ONTAP 인터클러스터 LIF	SnapMirror에 대한 인터클러스터 통신 세션의 관리
	TCP	1110 5	인터클러스터 LIF	ONTAP 인터클러스터 LIF	SnapMirror 데이터 전송
Syslog를 클릭합니 다	UDP입니 다	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 클릭합니 다	22	커넥터 호스트에 대한 SSH 액세스를 제공합니다
HTTP	80	클라이언트 웹 브라우저에서 로컬 사용자 인터페이스로 HTTP 액세스를 제공하고 Cloud Data Sense에서 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 클라우드 데이터 감지 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	Cloud Manager에서 DNS Resolve에 사용됩니다
클라우드 데이터 감지	HTTP	80	클라우드 데이터 감지 인스턴스	Cloud Volumes ONTAP에 대한 클라우드 데이터 감지

Copyright Information

Copyright © 2022 NetApp, Inc. All rights reserved. Printed in the U.S. No part of this document covered by copyright may be reproduced in any form or by any means-graphic, electronic, or mechanical, including photocopying, recording, taping, or storage in an electronic retrieval system-without prior written permission of the copyright owner.

Software derived from copyrighted NetApp material is subject to the following license and disclaimer:

THIS SOFTWARE IS PROVIDED BY NETAPP "AS IS" AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, WHICH ARE HEREBY DISCLAIMED. IN NO EVENT SHALL NETAPP BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

NetApp reserves the right to change any products described herein at any time, and without notice. NetApp assumes no responsibility or liability arising from the use of products described herein, except as expressly agreed to in writing by NetApp. The use or purchase of this product does not convey a license under any patent rights, trademark rights, or any other intellectual property rights of NetApp.

The product described in this manual may be protected by one or more U.S. patents, foreign patents, or pending applications.

RESTRICTED RIGHTS LEGEND: Use, duplication, or disclosure by the government is subject to restrictions as set forth in subparagraph (c)(1)(ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.277-7103 (October 1988) and FAR 52-227-19 (June 1987).

Trademark Information

NETAPP, the NETAPP logo, and the marks listed at <http://www.netapp.com/TM> are trademarks of NetApp, Inc. Other company and product names may be trademarks of their respective owners.