



# AWS のセキュリティグループルール Cloud Manager

Ben Cammett, Tom Onacki  
June 06, 2021

# 目次

|                                    |   |
|------------------------------------|---|
| AWS のセキュリティグループルール .....           | 1 |
| Cloud Volumes ONTAP のルール .....     | 1 |
| HA Mediator 外部セキュリティグループのルール ..... | 4 |
| HA Mediator 内部セキュリティグループのルール ..... | 5 |
| コネクタのルール .....                     | 6 |

# AWS のセキュリティグループルール

Cloud Manager で作成される AWS セキュリティグループには、コネクタと Cloud Volumes ONTAP が正常に動作するために必要なインバウンドとアウトバウンドのルールが含まれています。テスト目的でポートを参照したり、独自のセキュリティグループを使用したりする場合に使用します。

## Cloud Volumes ONTAP のルール

Cloud Volumes ONTAP のセキュリティグループには、インバウンドルールとアウトバウンドルールの両方が必要です。

### インバウンドルール

定義済みセキュリティグループのインバウンドルールの送信元は 0.0.0.0/0 です。

| プロトコル     | ポート     | 目的  |
|-----------|---------|---|
| すべての ICMP | すべて     | インスタンスの ping を実行します   |
| HTTP      | 80      | クラスタ管理 LIF の IP アドレスを使用した System Manager Web コンソールへの HTTP アクセス  |
| HTTPS     | 443     | クラスタ管理 LIF の IP アドレスを使用した System Manager Web コンソールへの HTTPS アクセス |
| SSH       | 22      | クラスタ管理 LIF またはノード管理 LIF の IP アドレスへの SSH アクセス                    |
| TCP       | 111     | NFS のリモートプロシージャコール  |
| TCP       | 139     | CIFS の NetBIOS サービスセッション  |
| TCP       | 161-162 | 簡易ネットワーク管理プロトコル   |
| TCP       | 445     | NetBIOS フレーム同期を使用した Microsoft SMB over TCP                      |
| TCP       | 635     | NFS マウント  |
| TCP       | 749     | Kerberos  |
| TCP       | 2049    | NFS サーバデーモン   |
| TCP       | 3260    | iSCSI データ LIF を介した iSCSI アクセス                                   |
| TCP       | 4045    | NFS ロックデーモン   |
| TCP       | 4046    | NFS のネットワークステータスマニタ   |
| TCP       | 10000   | NDMP を使用したバックアップ  |
| TCP       | 11104   | SnapMirror のクラスタ間通信セッションの管理                                     |
| TCP       | 11105   | クラスタ間 LIF を使用した SnapMirror データ転送                                |
| UDP       | 111     | NFS のリモートプロシージャコール  |

| プロトコル | ポート     | 目的                  |
|-------|---------|---------------------|
| UDP   | 161-162 | 簡易ネットワーク管理プロトコル     |
| UDP   | 635     | NFS マウント            |
| UDP   | 2049    | NFS サーバデーモン         |
| UDP   | 4045    | NFS ロックデーモン         |
| UDP   | 4046    | NFS のネットワークステータスマニタ |
| UDP   | 4049    | NFS rquotad プロトコル   |

## アウトバウンドルール

Cloud Volumes 用の事前定義済みセキュリティグループ ONTAP は、すべての発信トラフィックをオープンします。これが可能な場合は、基本的なアウトバウンドルールに従います。より厳格なルールが必要な場合は、高度なアウトバウンドルールを使用します。

### 基本的なアウトバウンドルール

Cloud Volumes ONTAP 用の定義済みセキュリティグループには、次のアウトバウンドルールが含まれています。

| プロトコル     | ポート | 目的           |
|-----------|-----|--------------|
| すべての ICMP | すべて | すべての発信トラフィック |
| すべての TCP  | すべて | すべての発信トラフィック |
| すべての UDP  | すべて | すべての発信トラフィック |

### 高度なアウトバウンドルール

発信トラフィックに厳格なルールが必要な場合は、次の情報を使用して、Cloud Volumes ONTAP による発信通信に必要なポートのみを開くことができます。



source は、Cloud Volumes ONTAP システムのインターフェイス（IP アドレス）です。

| サービス             | プロトコル       | ポート  | ソース                        | 宛先                          | 目的  |
|------------------|-------------|------|----------------------------|-----------------------------|---|
| Active Directory | TCP         | 88   | ノード管理 LIF                  | Active Directory フォレスト      | Kerberos V 認証                                   |
|                  | UDP         | 137  | ノード管理 LIF                  | Active Directory フォレスト      | NetBIOS ネームサービス                                 |
|                  | UDP         | 138  | ノード管理 LIF                  | Active Directory フォレスト      | NetBIOS データグラムサービス                              |
|                  | TCP         | 139  | ノード管理 LIF                  | Active Directory フォレスト      | NetBIOS サービスセッション                               |
|                  | TCP および UDP | 389  | ノード管理 LIF                  | Active Directory フォレスト      | LDAP  |
|                  | TCP         | 445  | ノード管理 LIF                  | Active Directory フォレスト      | NetBIOS フレーム同期を使用した Microsoft SMB over TCP      |
|                  | TCP         | 464  | ノード管理 LIF                  | Active Directory フォレスト      | Kerberos V パスワードの変更と設定 ( SET_CHANGE )           |
|                  | UDP         | 464  | ノード管理 LIF                  | Active Directory フォレスト      | Kerberos キー管理                                   |
|                  | TCP         | 749  | ノード管理 LIF                  | Active Directory フォレスト      | Kerberos V Change & Set Password ( RPCSEC_GSS ) |
|                  | TCP         | 88   | データ LIF ( NFS、CIFS、iSCSI ) | Active Directory フォレスト      | Kerberos V 認証                                   |
|                  | UDP         | 137  | データ LIF ( NFS、CIFS )       | Active Directory フォレスト      | NetBIOS ネームサービス                                 |
|                  | UDP         | 138  | データ LIF ( NFS、CIFS )       | Active Directory フォレスト      | NetBIOS データグラムサービス                              |
|                  | TCP         | 139  | データ LIF ( NFS、CIFS )       | Active Directory フォレスト      | NetBIOS サービスセッション                               |
|                  | TCP および UDP | 389  | データ LIF ( NFS、CIFS )       | Active Directory フォレスト      | LDAP  |
|                  | TCP         | 445  | データ LIF ( NFS、CIFS )       | Active Directory フォレスト      | NetBIOS フレーム同期を使用した Microsoft SMB over TCP      |
|                  | TCP         | 464  | データ LIF ( NFS、CIFS )       | Active Directory フォレスト      | Kerberos V パスワードの変更と設定 ( SET_CHANGE )           |
|                  | UDP         | 464  | データ LIF ( NFS、CIFS )       | Active Directory フォレスト      | Kerberos キー管理                                   |
|                  | TCP         | 749  | データ LIF ( NFS、CIFS )       | Active Directory フォレスト      | Kerberos V Change & Set Password ( RPCSEC_GSS ) |
| S3 へのバックアップ      | TCP         | 5010 | クラスタ間 LIF                  | バックアップエンドポイントまたはリストアエンドポイント | S3 へのバックアップ処理とリストア処理 フィーチャー ( Feature )         |

| サービス       | プロトコル      | ポート           | ソース                             | 宛先                | 目的                                   |
|------------|------------|---------------|---------------------------------|-------------------|--------------------------------------|
| クラスタ       | すべてのトラフィック | すべてのトラフィック    | 1 つのノード上のすべての LIF               | もう一方のノードのすべての LIF | クラスタ間通信（ Cloud Volumes ONTAP HA のみ）  |
|            | TCP        | 3000          | ノード管理 LIF                       | HA メディエータ         | ZAPI コール（ Cloud Volumes ONTAP HA のみ） |
|            | ICMP       | 1.            | ノード管理 LIF                       | HA メディエータ         | キープアライブ（ Cloud Volumes ONTAP HA のみ）  |
| DHCP       | UDP        | 68            | ノード管理 LIF                       | DHCP              | 初回セットアップ用の DHCP クライアント               |
| DHCP       | UDP        | 67            | ノード管理 LIF                       | DHCP              | DHCP サーバ                             |
| DNS        | UDP        | 53            | ノード管理 LIF とデータ LIF（ NFS、 CIFS ） | DNS               | DNS                                  |
| NDMP       | TCP        | 18600 ~ 18699 | ノード管理 LIF                       | 宛先サーバ             | NDMP コピー                             |
| SMTP       | TCP        | 25            | ノード管理 LIF                       | メールサーバ            | SMTP アラート。 AutoSupport に使えます         |
| SNMP       | TCP        | 161           | ノード管理 LIF                       | サーバを監視します         | SNMP トラップによる監視                       |
|            | UDP        | 161           | ノード管理 LIF                       | サーバを監視します         | SNMP トラップによる監視                       |
|            | TCP        | 162           | ノード管理 LIF                       | サーバを監視します         | SNMP トラップによる監視                       |
|            | UDP        | 162           | ノード管理 LIF                       | サーバを監視します         | SNMP トラップによる監視                       |
| SnapMirror | TCP        | 11104         | クラスタ間 LIF                       | ONTAP クラスタ間 LIF   | SnapMirror のクラスタ間通信セッションの管理          |
|            | TCP        | 11105         | クラスタ間 LIF                       | ONTAP クラスタ間 LIF   | SnapMirror によるデータ転送                  |
| syslog     | UDP        | 514           | ノード管理 LIF                       | syslog サーバ        | syslog 転送メッセージ                       |

## HA Mediator 外部セキュリティグループのルール

Cloud Volumes ONTAP HA Mediator 用に事前定義された外部セキュリティグループには、次のインバウンドルールとアウトバウンドルールが含まれています。

### インバウンドルール

インバウンドルールの送信元は 0.0.0.0/0 です。

| プロトコル | ポート  | 目的                       |
|-------|------|--------------------------|
| SSH   | 22   | HA メディエータへの SSH 接続       |
| TCP   | 3000 | コネクタからの RESTful API アクセス |

## アウトバウンドルール

HA メディエータの定義済みセキュリティグループは、すべての発信トラフィックを開きます。これが可能な場合は、基本的なアウトバウンドルールに従います。より厳格なルールが必要な場合は、高度なアウトバウンドルールを使用します。

### 基本的なアウトバウンドルール

HA Mediator 用の定義済みセキュリティグループには、次のアウトバウンドルールが含まれます。

| プロトコル    | ポート | 目的           |
|----------|-----|--------------|
| すべての TCP | すべて | すべての発信トラフィック |
| すべての UDP | すべて | すべての発信トラフィック |

### 高度なアウトバウンドルール

発信トラフィックに厳格なルールが必要な場合は、次の情報を使用して、HA メディエータによる発信通信に必要なポートだけを開くことができます。

| プロトコル | ポート | 宛先            | 目的                        |
|-------|-----|---------------|---------------------------|
| HTTP  | 80  | コネクタの IP アドレス | メディエーターのアップグレードをダウンロードします |
| HTTPS | 443 | AWS API サービス  | ストレージのフェイルオーバーを支援します      |
| UDP   | 53  | AWS API サービス  | ストレージのフェイルオーバーを支援します      |



ポート 443 および 53 を開く代わりに、ターゲットサブネットから AWS EC2 サービスへのインターフェイス VPC エンドポイントを作成できます。

## HA Mediator 内部セキュリティグループのルール

Cloud Volumes ONTAP HA Mediator 用に事前定義された内部セキュリティグループには、次のルールが含まれています。Cloud Manager は常にこのセキュリティグループを作成します。独自のオプションはありません。

### インバウンドルール

事前定義されたセキュリティグループには、次の着信ルールが含まれています。

| プロトコル      | ポート | 目的                    |
|------------|-----|-----------------------|
| すべてのトラフィック | すべて | HA メディエータと HA ノード間の通信 |

## アウトバウンドルール

定義済みのセキュリティグループには、次の発信ルールが含まれます。

| プロトコル      | ポート | 目的                    |
|------------|-----|-----------------------|
| すべてのトラフィック | すべて | HA メディエータと HA ノード間の通信 |

## コネクタのルール

コネクタのセキュリティグループには、インバウンドとアウトバウンドの両方のルールが必要です。

### インバウンドルール

| プロトコル | ポート  | 目的  |
|-------|------|---|
| SSH   | 22   | コネクタホストへの SSH アクセスを提供します  |
| HTTP  | 80   | クライアント Web ブラウザからローカルユーザインターフェイスへの HTTP アクセス、および Cloud Data Sense からの接続を提供します |
| HTTPS | 443  | クライアント Web ブラウザからローカルへの HTTPS アクセスを提供します ユーザインターフェイス                          |
| TCP   | 3128 | AWS ネットワークで NAT やプロキシを使用していない場合に、 Cloud Data Sense インスタンスにインターネットアクセスを提供します   |

## アウトバウンドルール

コネクタの事前定義されたセキュリティグループは、すべての発信トラフィックを開きます。これが可能な場合は、基本的なアウトバウンドルールに従います。より厳格なルールが必要な場合は、高度なアウトバウンドルールを使用します。

### 基本的なアウトバウンドルール

コネクタの事前定義されたセキュリティグループには、次のアウトバウンドルールが含まれています。

| プロトコル    | ポート | 目的           |
|----------|-----|--------------|
| すべての TCP | すべて | すべての発信トラフィック |
| すべての UDP | すべて | すべての発信トラフィック |



## 高度なアウトバウンドルール

発信トラフィックに固定ルールが必要な場合は、次の情報を使用して、コネクタによる発信通信に必要なポートだけを開くことができます。



送信元 IP アドレスは、コネクタホストです。

| サービス                 | プロトコル | ポート  | 宛先                                 | 目的  |
|----------------------|-------|------|------------------------------------|---|
| Active Directory     | TCP   | 88   | Active Directory フォレスト             | Kerberos V 認証   |
|                      | TCP   | 139  | Active Directory フォレスト             | NetBIOS サービスセッション   |
|                      | TCP   | 389  | Active Directory フォレスト             | LDAP  |
|                      | TCP   | 445  | Active Directory フォレスト             | NetBIOS フレーム同期を使用した Microsoft SMB over TCP                |
|                      | TCP   | 464  | Active Directory フォレスト             | Kerberos V パスワードの変更と設定 ( SET_CHANGE )                     |
|                      | TCP   | 749  | Active Directory フォレスト             | Active Directory Kerberos v の変更とパスワードの設定 ( RPCSEC_GSS )   |
|                      | UDP   | 137  | Active Directory フォレスト             | NetBIOS ネームサービス   |
|                      | UDP   | 138  | Active Directory フォレスト             | NetBIOS データグラムサービス  |
|                      | UDP   | 464  | Active Directory フォレスト             | Kerberos キー管理   |
| API コールと AutoSupport | HTTPS | 443  | アウトバウンドインターネットおよび ONTAP クラスタ管理 LIF | AWS および ONTAP への API コール、およびネットアップへの AutoSupport メッセージの送信 |
| API コール              | TCP   | 3000 | ONTAP クラスタ管理 LIF                   | ONTAP への API コール  |
|                      | TCP   | 8088 | S3 へのバックアップ                        | S3 へのバックアップを API で呼び出します                                  |
| DNS                  | UDP   | 53   | DNS                                | Cloud Manager による DNS 解決に使用されます                           |

| サービス       | プロトコル | ポート | 宛先                         | 目的                                     |
|------------|-------|-----|----------------------------|--|
| クラウドデータの意味 | HTTP  | 80  | Cloud Data Sense<br>インスタンス | Cloud Volumes<br>ONTAP に最適なク<br>ラウドデータ |

## Copyright Information

Copyright © 2021 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.