



# Azure の Cloud Volumes ONTAP のネットワーク要件 Cloud Manager

Ben Cammett  
April 02, 2021

This PDF was generated from [https://docs.netapp.com/ja-jp/occm/reference\\_networking\\_azure.html](https://docs.netapp.com/ja-jp/occm/reference_networking_azure.html) on June 14, 2021. Always check docs.netapp.com for the latest.

# 目次

|   |   |
|---|---|
| Azure の Cloud Volumes ONTAP のネットワーク要件 ..... | 1 |
| Cloud Volumes ONTAP の要件 .....               | 1 |
| コネクタの要件 .....                               | 2 |
| Cloud Volumes ONTAP のセキュリティグループのルール .....   | 4 |
| コネクタのセキュリティグループルール .....                    | 9 |

# Azure の Cloud Volumes ONTAP のネットワーク要件

Cloud Volumes ONTAP システムが適切に動作するように Azure ネットワークをセットアップします。これには、コネクタと Cloud Volumes ONTAP のネットワークも含まれます。

## Cloud Volumes ONTAP の要件

Azure では、次のネットワーク要件を満たしている必要があります。

### Cloud Volumes ONTAP 用のアウトバウンドインターネットアクセス

Cloud Volumes ONTAP が AutoSupport メッセージを送信できるように、ルーティングポリシーとファイアウォールポリシーで次のエンドポイントへの HTTP / HTTPS トラフィックを許可する必要があります。

- \ <https://support.netapp.com/aods/asupmessage>
- \ <https://support.netapp.com/asupprod/post/1.0/postAsup>

"AutoSupport の設定方法について説明します"。

### セキュリティグループ

Cloud Manager ではセキュリティグループを作成する必要がないため、セキュリティグループを作成する必要はありません。独自のルールを使用する必要がある場合は、以下のセキュリティグループルールを参照してください。

### IP アドレスの数

- シングルノード：5 つの IP アドレス
- HA ペア：IP アドレス × 16

Cloud Manager では、HA ペア上に SVM 管理 LIF が作成されますが、Azure のシングルノードシステム上には作成されません。



LIF は、物理ポートに関連付けられた IP アドレスです。SnapCenter などの管理ツールには、SVM 管理 LIF が必要です。

クラウドボリューム ONTAP から Azure BLOB ストレージへの接続により、データ階層化を実現します

```
"Microsoft.Network/virtualNetworks/subnets/write",  
"Microsoft.Network/routeTables/join/action",
```

これらの権限は最新のに含まれています "Cloud Manager ポリシー"。

データ階層化の設定の詳細については、を参照してください "コールドデータを低コストのオブジェクトストレージに階層化する"。

他のネットワーク内の **ONTAP** システムへの接続

手順については、を参照してください "[Microsoft Azure のドキュメント：「 Create a Site-to-Site connection in the Azure portal](#)”。

## コネクタの要件

コネクタがパブリッククラウド環境内のリソースやプロセスを管理できるように、ネットワークを設定します。最も重要なステップは、さまざまなエンドポイントへのアウトバウンドインターネットアクセスを確保することです。



ネットワークでインターネットへのすべての通信にプロキシサーバを使用している場合は、[ 設定 ] ページでプロキシサーバを指定できます。を参照してください "[プロキシサーバを使用するようにコネクタを設定します](#)”。

## ターゲットネットワークへの接続

コネクタには、Cloud Volumes ONTAP を導入する VPC および VNet へのネットワーク接続が必要です。

たとえば、企業ネットワークにコネクタを設置する場合は、Cloud Volumes ONTAP を起動する VPC または VNet への VPN 接続を設定する必要があります。

## アウトバウンドインターネットアクセス

Connector では、パブリッククラウド環境内のリソースとプロセスを管理するためにアウトバウンドインターネットアクセスが必要です。コネクタは、Azure でリソースを管理する際に次のエンドポイントに接続します。

| エンドポイント   | 目的  |
|---|---|
| <a href="https://management.azure.com">https://management.azure.com</a><br><a href="https://login.microsoftonline.com">https://login.microsoftonline.com</a>  | Cloud Manager では、ほとんどの Azure リージョンに Cloud Volumes ONTAP を導入して管理できます。                      |
| <a href="https://management.microsoftazure.de">https://management.microsoftazure.de</a><br><a href="https://login.microsoftonline.de">https://login.microsoftonline.de</a>  | Cloud Manager は、Azure Germany リージョンに Cloud Volumes ONTAP を導入して管理できます。                     |
| <a href="https://management.usgovcloudapi.net/">https://management.usgovcloudapi.net/</a><br><a href="https://login.microsoftonline.com">https://login.microsoftonline.com</a>  | Cloud Manager は、Azure US GOV リージョンに Cloud Volumes ONTAP を導入して管理できます。                      |
| \ <a href="https://api.services.cloud.netapp.com:443">https://api.services.cloud.netapp.com:443</a>   | NetApp Cloud Central への API 要求。   |
| \ <a href="https://cloud.support.netapp.com.s3.us-west-1.amazonaws.com">https://cloud.support.netapp.com.s3.us-west-1.amazonaws.com</a>   | ソフトウェアイメージ、マニフェスト、およびテンプレートにアクセスできます。   |
| ¥ <a href="https://cognito-idp.us-east-1.amazonaws.com">https://cognito-idp.us-east-1.amazonaws.com</a> ¥ <a href="https://cognito-identity.us-east-1.amazonaws.com">https://cognito-identity.us-east-1.amazonaws.com</a> ¥ <a href="https://sts.amazonaws.com">https://sts.amazonaws.com</a> ¥ <a href="https://cloud-support-netapp-com-accelerated.s3.amazonaws.com">https://cloud-support-netapp-com-accelerated.s3.amazonaws.com</a> | コネクタがマニフェスト、テンプレート、および Cloud Volumes ONTAP アップグレードイメージにアクセスしてダウンロードできるようにします。             |
| \ <a href="https://cloudmanagerinfraprod.azurecr.io">https://cloudmanagerinfraprod.azurecr.io</a>   | Docker を実行しているインフラのコンテナコンポーネントのソフトウェアイメージにアクセスでき、Cloud Manager とのサービス統合のためのソリューションを提供します。 |

| エンドポイント  | 目的   |
|--|--|
| \ <a href="https://kinesis.us-east-1.amazonaws.com">https://kinesis.us-east-1.amazonaws.com</a>  | ネットアップが監査レコードからデータをストリーミングできるようにします。   |
| \ <a href="https://cloudmanager.cloud.netapp.com">https://cloudmanager.cloud.netapp.com</a>  | Cloud Central アカウントを含む Cloud Manager サービスとの通信。   |
| <a href="https://netapp-cloud-account.auth0.com">https://netapp-cloud-account.auth0.com</a>  | NetApp Cloud Central との通信により、ユーザ認証を一元的に行うことができます。  |
| support.netapp.com:443<br><a href="https://mysupport.netapp.com">https://mysupport.netapp.com</a>  | ネットアップ AutoSupport との通信：コネクタは support.netapp.com:443 と通信し、<br><a href="https://mysupport.netapp.com">https://mysupport.netapp.com</a> にリダイレクトされます。 |
| ¥ <a href="https://support.netapp.com/svcgw">https://support.netapp.com/svcgw</a> ¥<br><a href="https://support.netapp.com/ServiceGW/entitlement">https://support.netapp.com/ServiceGW/entitlement</a> ¥ <a href="https://eval.lic.netapp.com.s3.us-west-1.amazonaws.com">https://eval.lic.netapp.com.s3.us-west-1.amazonaws.com</a> ¥ <a href="https://cloud-support-netapp-com.s3.us-west-1.amazonaws.com">https://cloud-support-netapp-com.s3.us-west-1.amazonaws.com</a> | システムライセンスとサポート登録を行うためのネットアップとの通信   |
| ¥ <a href="https://client.infra.support.netapp.com.s3.us-west-1.amazonaws.com">https://client.infra.support.netapp.com.s3.us-west-1.amazonaws.com</a> ¥ <a href="https://cloud-support-netapp-com-accelerated.s3.us-west-1.amazonaws.com">https://cloud-support-netapp-com-accelerated.s3.us-west-1.amazonaws.com</a> ¥<br><a href="https://trigger.asup.netapp.com.s3.us-west-1.amazonaws.com">https://trigger.asup.netapp.com.s3.us-west-1.amazonaws.com</a>               | ネットアップがサポートの問題のトラブルシューティングに必要な情報を収集できるようにします。  |
| \ <a href="https://ipa-signer.cloudmanager.netapp.com">https://ipa-signer.cloudmanager.netapp.com</a>  | Cloud Manager でライセンスを生成できます（Cloud Volumes ONTAP 用の FlexCache ライセンスなど）。   |
| * .blob.core.windows.net   | プロキシを使用する場合は HA ペアに必要です。   |
| 次のようなさまざまなサードパーティの場所があります。 <ul style="list-style-type: none"> <li>• <a href="https://repo1.maven.org/maven2">https://repo1.maven.org/maven2</a> です</li> <li>• <a href="https://oss.sonatype.org/content/repository">https://oss.sonatype.org/content/repository</a> を参照してください</li> <li>• \ <a href="https://repo.typesafe.com">https://repo.typesafe.com</a></li> </ul> <p>サードパーティの所在地は変更される可能性があります。</p>  | アップグレード時に、Cloud Manager はサードパーティの依存関係に対応する最新のパッケージをダウンロードします。  |

SaaS ユーザインターフェイスからほとんどのタスクを実行する必要がありますが、ローカルユーザインターフェイスは引き続きコネクタで使用できます。Web ブラウザを実行するマシンは、次のエンドポイントに接続する必要があります。

|   |  |
|---|--|
| エンドポイント   | 目的   |
| コネクタホスト   | <p>Cloud Manager コンソールをロードするには、Web ブラウザでホストの IP アドレスを入力する必要があります。</p> <p>クラウドプロバイダへの接続に応じて、ホストに割り当てられたプライベート IP またはパブリック IP を使用できます。</p> <ul style="list-style-type: none"> <li>• プライベート IP は、VPN とがある場合に機能します 仮想ネットワークへの直接アクセス</li> <li>• パブリック IP は、あらゆるネットワークシナリオで機能します</li> </ul> <p>いずれの場合も、セキュリティグループのルールで許可された IP またはサブネットからのアクセスのみを許可することで、ネットワークアクセスを保護する必要があります。</p> |
| ¥ <a href="https://auth0.com">https://auth0.com</a> ¥ <a href="https://cdn.auth0.com">https://cdn.auth0.com</a> ¥ <a href="https://netapp-cloud-account.auth0.com">https://netapp-cloud-account.auth0.com</a> ¥ <a href="https://services.cloud.netapp.com">https://services.cloud.netapp.com</a> | Web ブラウザはこれらのエンドポイントに接続し、NetApp Cloud Central を介してユーザ認証を一元化します。  |
| \ <a href="https://widget.intercom.io">https://widget.intercom.io</a>   | 製品内でのチャットにより、ネットアップのクラウドエキスパートと会話できます。   |

## Cloud Volumes ONTAP のセキュリティグループのルール

Cloud Manager で作成される Azure セキュリティグループには、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。

### シングルノードシステムのインバウンドルール

次のルールでは、説明で特定の着信トラフィックがブロックされている場合を除き、トラフィックは許可されます。

| 優先順位と名前               | ポートおよびプロトコル | ソースとデスティネーションの 2 つです | 説明   |
|-----------------------|-------------|----------------------|--|
| 1000 inbound_ssh      | 22 TCP      | Any から Any           | 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                  |
| 1001 INBOUND _http    | 80 TCP      | Any から Any           | 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 |
| 1002 INBOUND _111_TCP | 111 TCP     | Any から Any           | NFS のリモートプロシージャコール   |

| 優先順位と名前                        | ポートおよびプロトコル     | ソースとデスティネーションの 2 つです | 説明  |
|--------------------------------|-----------------|----------------------|---|
| 1003 INBONED_111_UDP           | 111 UDP         | Any から Any           | NFS のリモートプロシージャコール  |
| 1004 INBOUND _139              | 139 TCP         | Any から Any           | CIFS の NetBIOS サービスセッション  |
| 1005 inbound_161-162_TCP       | 161-162 TCP     | Any から Any           | 簡易ネットワーク管理プロトコル   |
| 1006 INBOUND _161-162_UDP      | UDP 161-162     | Any から Any           | 簡易ネットワーク管理プロトコル   |
| 1007 INBOUND _443              | 443 tcp         | Any から Any           | 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 |
| 1008 INBOUND _445              | 445 TCP         | Any から Any           | NetBIOS フレーム同期を使用した Microsoft SMB over TCP                      |
| 1009 INBOUND _635_TCP          | 635 TCP         | Any から Any           | NFS マウント  |
| 1010 INBOUND _635_UDP          | 635 UDP         | Any から Any           | NFS マウント  |
| 1011 INBOUND _749              | 749 TCP         | Any から Any           | Kerberos  |
| 1012 INBOUND _2049_TCP         | 2049 TCP        | Any から Any           | NFS サーバデーモン   |
| 1013 INBOUND _2049_UDP         | 2049 UDP        | Any から Any           | NFS サーバデーモン   |
| 1014 インバウンド _3260              | 3260 TCP        | Any から Any           | iSCSI データ LIF を介した iSCSI アクセス                                   |
| 1015 INBOUND _4045-4046_tcp の略 | 4045-4046 TCP   | Any から Any           | NFS ロックデーモンとネットワークステータスマニタ                                      |
| 1016 INBOUND _4045-4046_UDP    | 4045-4046 UDP   | Any から Any           | NFS ロックデーモンとネットワークステータスマニタ                                      |
| 1017 INBOUND _10000            | 10000 TCP       | Any から Any           | NDMP を使用したバックアップ  |
| 1018 INBOUND _11104-11105      | 11104-11105 TCP | Any から Any           | SnapMirror によるデータ転送   |
| 3000 inbound_deny_all_tcp      | 任意のポート TCP      | Any から Any           | 他のすべての TCP インバウンドトラフィックをブロックします                                 |

| 優先順位と名前                                 | ポートおよびプロトコル    | ソースとデスティネーションの 2 つです         | 説明  |
|---|----------------|------------------------------|---|
| 3001 INBOUND _DENY_ALL_UDP              | 任意のポート UDP     | Any から Any                   | 他のすべての UDP 着信トラフィックをブロックします               |
| 65000 AllowVnetInBound                  | 任意のポート任意のプロトコル | VirtualNetwork               | VNet 内からのインバウンドトラフィック                     |
| 65001 AllowAzureLoad BalancerInBound の略 | 任意のポート任意のプロトコル | AzureLoadBalancer を任意のに設定します | Azure Standard Load Balancer からのデータトラフィック |
| 65500 DenyAllInBound                    | 任意のポート任意のプロトコル | Any から Any                   | 他のすべてのインバウンドトラフィックをブロックする                 |

## HA システムのインバウンドルール

次のルールでは、説明で特定の着信トラフィックがブロックされている場合を除き、トラフィックは許可されます。



HA システムのインバウンドデータトラフィックは Azure Standard Load Balancer を経由するため、シングルノードシステムよりもインバウンドルールが少なくなります。そのため、「AllowAzureLoadBalancerInBound」ルールに示されているように、ロードバランサからのトラフィックがオープンである必要があります。

| 優先順位と名前                                 | ポートおよびプロトコル    | ソースとデスティネーションの 2 つです         | 説明  |
|---|----------------|------------------------------|---|
| 100 インバウンド _443                         | 443 : 任意のプロトコル | Any から Any                   | 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 |
| 101 INBOUND _111_TCP                    | 111 すべてのプロトコル  | Any から Any                   | NFS のリモートプロシージャコール  |
| 102 インバウンド _2049_TCP                    | 2049 任意のプロトコル  | Any から Any                   | NFS サーバデーモン   |
| 111 inbound_ssh                         | 22 すべてのプロトコル   | Any から Any                   | 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                   |
| 121 INBOUND _53                         | 53 任意のプロトコル    | Any から Any                   | DNS と CIFS  |
| 65000 AllowVnetInBound                  | 任意のポート任意のプロトコル | VirtualNetwork               | VNet 内からのインバウンドトラフィック   |
| 65001 AllowAzureLoad BalancerInBound の略 | 任意のポート任意のプロトコル | AzureLoadBalancer を任意のに設定します | Azure Standard Load Balancer からのデータトラフィック                       |



| 優先順位と名前              | ポートおよびプロトコル    | ソースとデスティネーションの 2 つです | 説明                        |
|----------------------|----------------|----------------------|---------------------------|
| 65500 DenyAllInBound | 任意のポート任意のプロトコル | Any から Any           | 他のすべてのインバウンドトラフィックをブロックする |

## 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。

| ポート | プロトコル    | 目的           |
|-----|----------|--------------|
| すべて | すべての TCP | すべての発信トラフィック |
| すべて | すべての UDP | 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             | ポート | プロ<br>トコ<br>ル         | ソース                        | 宛先                     | 目的  |
|------------------|-----|-----------------------|----------------------------|------------------------|---|
| Active Directory | 88  | TCP                   | ノード管理 LIF                  | Active Directory フォレスト | Kerberos V 認証                                   |
|                  | 137 | UDP                   | ノード管理 LIF                  | Active Directory フォレスト | NetBIOS ネームサービス                                 |
|                  | 138 | UDP                   | ノード管理 LIF                  | Active Directory フォレスト | NetBIOS データグラムサービス                              |
|                  | 139 | TCP                   | ノード管理 LIF                  | Active Directory フォレスト | NetBIOS サービスセッション                               |
|                  | 389 | TCP<br>およ<br>び<br>UDP | ノード管理 LIF                  | Active Directory フォレスト | LDAP  |
|                  | 445 | TCP                   | 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      |
|                  | 464 | TCP                   | 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 )           |
|                  | 464 | UDP                   | ノード管理 LIF                  | Active Directory フォレスト | Kerberos キー管理                                   |
|                  | 749 | TCP                   | ノード管理 LIF                  | Active Directory フォレスト | Kerberos V Change & Set Password ( RPCSEC_GSS ) |
|                  | 88  | TCP                   | データ LIF ( NFS、CIFS、iSCSI ) | Active Directory フォレスト | Kerberos V 認証                                   |
|                  | 137 | UDP                   | データ LIF ( NFS、CIFS )       | Active Directory フォレスト | NetBIOS ネームサービス                                 |
|                  | 138 | UDP                   | データ LIF ( NFS、CIFS )       | Active Directory フォレスト | NetBIOS データグラムサービス                              |
|                  | 139 | TCP                   | データ LIF ( NFS、CIFS )       | Active Directory フォレスト | NetBIOS サービスセッション                               |
|                  | 389 | TCP<br>およ<br>び<br>UDP | データ LIF ( NFS、CIFS )       | Active Directory フォレスト | LDAP  |
|                  | 445 | TCP                   | 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      |
|                  | 464 | TCP                   | 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 )           |
|                  | 464 | UDP                   | データ LIF ( NFS、CIFS )       | Active Directory フォレスト | Kerberos キー管理                                   |
|                  | 749 | TCP                   | データ LIF ( NFS、CIFS )       | Active Directory フォレスト | Kerberos V Change & Set Password ( RPCSEC_GSS ) |

| サービス       | ポート           | プロトコル | ソース                             | 宛先              | 目的                            |
|------------|---------------|-------|---------------------------------|-----------------|-------------------------------|
| DHCP       | 68            | UDP   | 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       | 67            | UDP   | ノード管理 LIF                       | DHCP            | DHCP サーバ                      |
| DNS        | 53            | UDP   | ノード管理 LIF とデータ LIF ( NFS、CIFS ) | DNS             | DNS                           |
| NDMP       | 18600 ~ 18699 | TCP   | ノード管理 LIF                       | 宛先サーバ           | NDMP コピー                      |
| SMTP       | 25            | TCP   | ノード管理 LIF                       | メールサーバ          | SMTP アラート。AutoSupport に使用できます |
| SNMP       | 161           | TCP   | 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                |
|            | 161           | UDP   | 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                |
|            | 162           | TCP   | 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                |
|            | 162           | UDP   | 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 | 11104         | TCP   | 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   |
|            | 11105         | TCP   | クラスタ間 LIF                       | ONTAP クラスタ間 LIF | SnapMirror によるデータ転送           |
| syslog     | 514           | UDP   | ノード管理 LIF                       | syslog サーバ      | syslog 転送メッセージ                |

## コネクタのセキュリティグループルール

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

| ポート | プロトコル | 目的   |
|-----|-------|--|
| 22  | SSH   | コネクタホストへの SSH アクセスを提供します                             |
| 80  | HTTP  | クライアント Web ブラウザからローカルへの HTTP アクセスを提供します ユーザインターフェイス  |
| 443 | HTTPS | 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 |

### 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。

| ポート | プロトコル    | 目的           |
|-----|----------|--------------|
| すべて | すべての TCP | すべての発信トラフィック |
| すべて | すべての UDP | 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             | ポート | プロトコル | 宛先                     | 目的  |
|------------------|-----|-------|------------------------|---|
| Active Directory | 88  | TCP   | Active Directory フォレスト | Kerberos V 認証   |
|                  | 139 | TCP   | Active Directory フォレスト | NetBIOS サービスセッション                                       |
|                  | 389 | TCP   | Active Directory フォレスト | LDAP  |
|                  | 445 | TCP   | Active Directory フォレスト | NetBIOS フレーム同期を使用した Microsoft SMB over TCP              |
|                  | 464 | TCP   | Active Directory フォレスト | Kerberos V パスワードの変更と設定 ( SET_CHANGE )                   |
|                  | 749 | TCP   | 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 ) |
|                  | 137 | UDP   | Active Directory フォレスト | NetBIOS ネームサービス   |
|                  | 138 | UDP   | Active Directory フォレスト | NetBIOS データグラムサービス                                      |
|                  | 464 | UDP   | Active Directory フォレスト | Kerberos キー管理   |

| サービス                    | ポート  | プロトコル | 宛先                                    | 目的  |
|-------------------------|------|-------|---------------------------------------|---|
| API コールと<br>AutoSupport | 443  | HTTPS | アウトバウンドインターネットおよび<br>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                 | 3000 | TCP   | ONTAP クラスタ管理 LIF                      | ONTAP への API コール  |
| DNS                     | 53   | UDP   | DNS                                   | Cloud Manager による DNS 解決に使用されます                           |

## 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.