



Cloud Volumes ONTAP in GCP のネットワーク要件 Cloud Manager

Ben Cammett, Felix melligan
June 05, 2021

目次

Cloud Volumes ONTAP in GCP のネットワーク要件	1
Cloud Volumes ONTAP の要件	1
コネクタの要件	4
Cloud Volumes ONTAP のファイアウォールルール	6
VPC -1、VPC -2、および VPC -3 のファイアウォールルール	10
コネクタのファイアウォールルール	11

Cloud Volumes ONTAP in GCP のネットワーク要件

Cloud Volumes ONTAP システムが正常に動作するように、Google Cloud Platform 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。

HA ペアを導入する場合は、を実行します ["GCP での HA ペアの仕組みをご確認ください"](#)。

Cloud Volumes ONTAP の要件

GCP では、次の要件を満たす必要があります。

内部ロードバランサ

1 つはクラスタ管理用、もう 1 つはノード 1 への NAS トラフィック用、最後はノード 2 への NAS トラフィック用です。

各ロードバランサの設定は次のとおりです。

- 共有プライベート IP アドレス × 1
- グローバル健全性チェック 1 回

デフォルトでは、ヘルスチェックで使用するポートは 63001、63002、および 63003 です。

- 地域 TCP バックエンドサービス × 1
- 地域 UDP バックエンドサービス × 1
- 1 つの TCP 転送ルール
- 1 つの UDP 転送ルール
- グローバルアクセスは無効です

グローバルアクセスはデフォルトでは無効になっていますが、展開後に有効にすることができます。クロスリージョントラフィックのレイテンシが大幅に高くなるため、この機能は無効にしました。誤ってリージョン間にマウントすることが原因でマイナスの体験が得られないようにしたいと考えていました。このオプションを有効にすることは、ビジネスニーズに固有のものです。

HA ペア用のゾーン

- 複数のゾーン（推奨）

3 つのゾーンに HA 構成を導入することで、ゾーン内で障害が発生した場合の継続的なデータ可用性を確保できます。書き込みパフォーマンスは、単一のゾーンを使用する場合に比べてわずかに低くなりますが、最小のパフォーマンスです。

- シングルゾーン

Cloud Volumes ONTAP HA 構成では、単一のゾーンに導入する場合は分散配置ポリシーを使用します。このポリシーにより、HA 構成がゾーン内の単一点障害から保護されます。障害の切り分けに別々

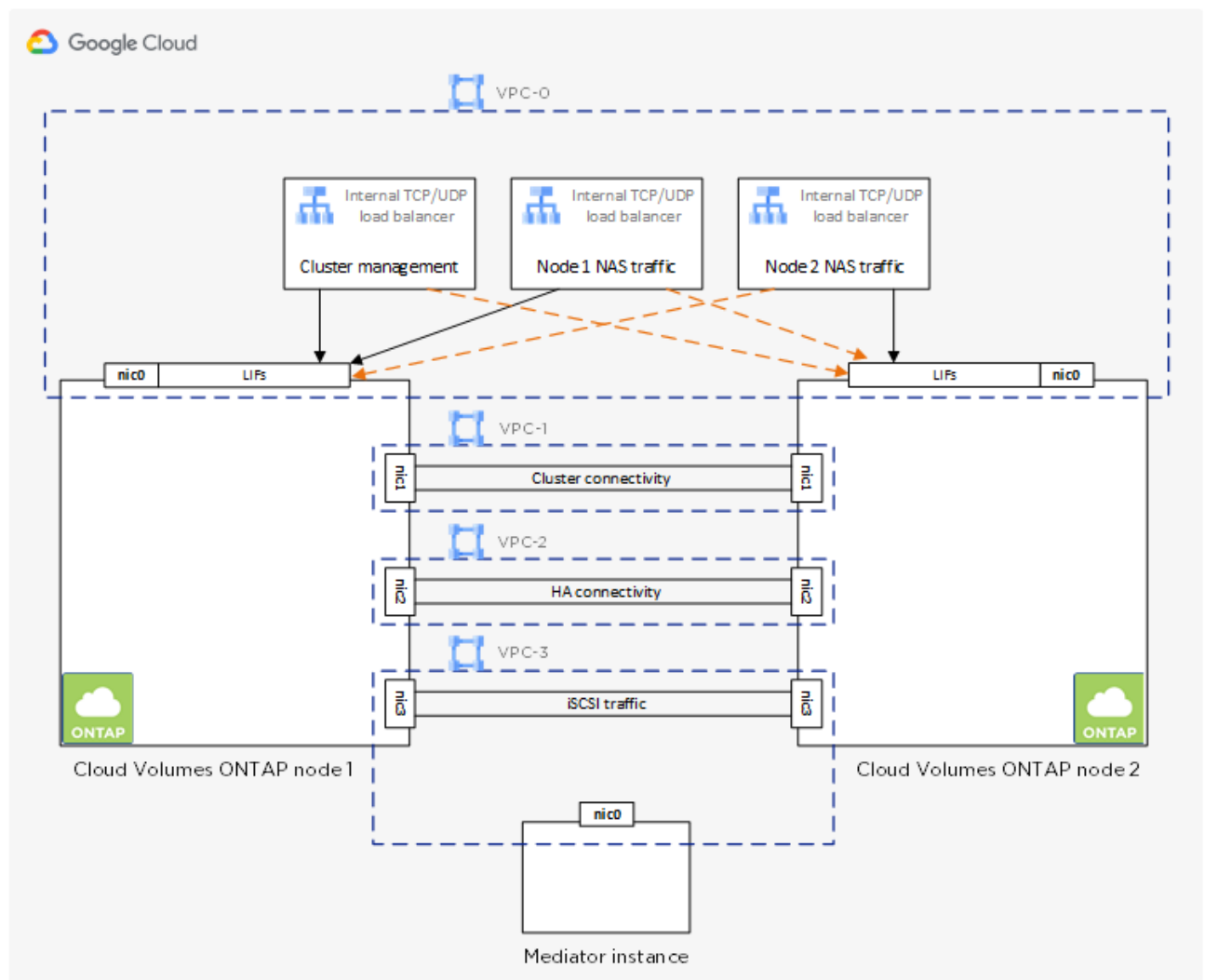
のゾーンを使用する必要はありません。

この導入モデルでは、ゾーン間にデータ出力料金が発生しないため、コストが削減されます。

HA ペア用の仮想プライベートクラウド × 4

HA ペアの作成時に、Cloud Manager から 4 つの VPC を選択するよう求められます。

- vPC-0 : データおよびノードへのインバウンド接続
- vPC-1、VPC -2、および VPC -3 : ノードと HA メディエーター間の内部通信



HA ペアのサブネット

コネクタを VPC 0 に配置する場合は、サブネットに Private Google Access を有効にして API にアクセスし、データの階層化を有効にする必要があります。

これらの VPC 内のサブネットには、個別の CIDR 範囲が必要です。CIDR 範囲を重複させることはできません。

シングルノードシステムに対応した 1 つの仮想プライベートクラウド

シングルノードシステムには 1 つの VPC が必要です。

共有 VPC

共有 VPC を使用すると、複数のプロジェクトの仮想ネットワークを設定し、一元管理できます。ホストプロジェクト _ で共有 VPC ネットワークをセットアップし、Connector および Cloud Volumes ONTAP 仮想マシンインスタンスをサービスプロジェクト _ で導入できます。"[Google Cloud のドキュメント：「Shared VPC Overview」](#)"。

共有 VPC を使用する場合の唯一の要件は、です を指定します "[Compute Network User ロール](#)" をコネクタサービスアカウントに追加します。Cloud Manager は、ホストプロジェクトのファイアウォール、VPC、およびサブネットを照会するためにこれらの権限を必要とします。

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"。



HA ペアを使用している場合、HA メディエーターではアウトバウンドのインターネットアクセスは必要ありません。

プライベート IP アドレス

- * シングルノード * : 3 または 4 つのプライベート IP アドレス

Cloud Volumes ONTAP を API を使用して導入する場合、Storage VM (SVM) 管理 LIF の作成をスキップし、次のフラグを指定できます。

'kipsvmManagementLIF : true

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、Storage VM (SVM) 管理 LIF が必要です。

- * HA ペア * : 15 または 16 個のプライベート IP アドレス
 - VPC -0 の 7 つまたは 8 つのプライベート IP アドレス

Cloud Volumes ONTAP を API を使用して導入する場合、Storage VM (SVM) 管理 LIF の作成をスキップし、次のフラグを指定できます。

'kipsvmManagementLIF : true

- VPC 1 用のプライベート IP アドレスが 2 つあります
- VPC 2 のプライベート IP アドレス × 2
- VPC 3 つのプライベート IP アドレス

ファイアウォールルール

HA 構成には、次の 2 組のファイアウォールルールが必要です。

- VPC -0 の HA コンポーネントのルールセット。これらのルールにより、Cloud Volumes ONTAP への

データアクセスが可能になります。 [詳細はこちら](#)。。

- VPC -1 、 VPC -2 、 および VPC -3 の HA コンポーネントに関するもう 1 つのルールセット。これらのルールは、 HA コンポーネント間のインバウンド通信とアウトバウンド通信に対してオープンです。 [詳細はこちら](#)。。

の Cloud Volumes ONTAP から Google Cloud Storage への接続 データ階層化

Cloud Manager でデータの階層化を設定するための追加の手順については、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 "[Google Cloud のドキュメント：「 Cloud VPN Overview](#)"。

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 へのネットワーク接続が必要です。HA ペアを導入する場合は、 4 つの VPC すべてに接続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、 GCP 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
https://www.googleapis.com	GCP で Cloud Volumes ONTAP を導入および管理するために、 Connector から Google API に接続できるようにします。
https://api.services.cloud.netapp.com:443	NetApp Cloud Central への API 要求。
https://cloud.support.netapp.com.s3.us-west-1.amazonaws.com	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。
¥ https://cognito-idp.us-east-1.amazonaws.com ¥ https://cognito-identity.us-east-1.amazonaws.com ¥ https://sts.amazonaws.com ¥ https://cloud-support-netapp-com-accelerated.s3.amazonaws.com	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。

エンドポイント	目的
\ https://cloudmanagerinfraprod.azurecr.io	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。
\ https://kinesis.us-east-1.amazonaws.com	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。
\ https://cloudmanager.cloud.netapp.com	Cloud Central アカウントを含む Cloud Manager サービスとの通信。
https://netapp-cloud-account.auth0.com	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 https://mysupport.netapp.com	ネットアップ AutoSupport との通信：コネクタは support.netapp.com:443 と通信し、 https://mysupport.netapp.com にリダイレクトされます。
¥ https://support.netapp.com/svcgw ¥ https://support.netapp.com/ServiceGW/entitlement ¥ https://eval.lic.netapp.com.s3.us-west-1.amazonaws.com ¥ https://cloud-support-netapp-com.s3.us-west-1.amazonaws.com	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
¥ https://client.infra.support.netapp.com.s3.us-west-1.amazonaws.com ¥ https://cloud-support-netapp-com-accelerated.s3.us-west-1.amazonaws.com ¥ https://trigger.asup.netapp.com.s3.us-west-1.amazonaws.com	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。
\ https://ipa-signer.cloudmanager.netapp.com	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）。
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"> • https://repo1.maven.org/maven2 です • https://oss.sonatype.org/content/repository を参照してください • \ https://repo.typesafe.com 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。	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"> • 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 • 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 <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>
¥ https://auth0.com ¥ https://cdn.auth0.com ¥ https://netapp-cloud-account.auth0.com ¥ https://services.cloud.netapp.com	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。
\ https://widget.intercom.io	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 のファイアウォールルール

Cloud Manager 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を含む GCP ファイアウォールルールを作成します。テスト目的または独自のファイアウォールルールを使用する場合は、ポートを参照してください。

Cloud Volumes ONTAP のファイアウォールルールには、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。

HA 構成を導入する場合は、VPC 0 の Cloud Volumes ONTAP のファイアウォールルールを以下に示します。

インバウンドルール

定義済みファイアウォールのインバウンドルールのソースは 0.0.0.0/0 です。

独自のファイアウォールを作成するには、Cloud Volumes ONTAP と通信する必要のあるすべてのネットワークを追加するとともに、内部の Google ロードバランサが正常に機能するように両方のアドレス範囲を追加する必要があります。これらのアドレスは 130.211.0.0/22 および 35.191.0.0/16 です。詳細については、["Google Cloud ドキュメント：ロードバランサファイアウォールルール"](#)を参照してください。

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

プロトコル	ポート	目的
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
TCP	63001-63050	プローブポートをロードバランシングして、どのノードが正常であるかを判断します（ HA ペアの場合のみ必要）
UDP	111	NFS のリモートプロシージャコール
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)

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 に使用できます
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

VPC -1、 VPC -2、 および VPC -3 のファイアウォールルール

GCP では、 4 つの VPC 間で HA 構成が導入されます。 VPC -0 の HA 構成に必要なファイアウォールルールはです [Cloud Volumes ONTAP については上記のリストを参照してください。](#)

一方、 Cloud Manager で VPC -1、 VPC -2、 および VPC -3 のインスタンスに対して作成される事前定義されたファイアウォールポリシーによって、すべてのプロトコルとポートでの入力通信が有効になります。これらのルールによって、 HA ノードと HA メディエーター間の通信が可能になります。

コネクタのファイアウォールルール

コネクタのファイアウォールルールには、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への HTTP アクセスを提供します ユーザインターフェイス
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

アウトバウンドルール

コネクタの定義済みファイアウォールルールによって、すべてのアウトバウンドトラフィックが開かれます。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

コネクタの定義済みファイアウォールルールには、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	GCP 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
DNS	UDP	53	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.