ポート

Setup and administration

NetApp
April 26, 2024

This PDF was generated from https://docs.netapp.com/ja-jp/bluexp-setup-admin/reference-ports-aws.html on April 26, 2024. Always check docs.netapp.com for the latest.

目次

ポート 1
AWSでのコネクタセキュリティグループのルール 1
Azureでのコネクタセキュリティグループのルール 2
Google Cloudのコネクタファイアウォールルール 4
オンプレミスコネクタ用のポート 5

ポート

AWSでのコネクタセキュリティグループのルール

コネクタのAWS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。BlueXPでコネクタを作成すると、BlueXPでこのセキュリティグループが自動的に作成されます。他のすべてのインストールオプションには、このセキュリティグループを設定する必要があります。

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	8時80分	• 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 • Cloud Volumes ONTAPのアップグレードプロセスで使用
HTTPS	443年	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HTTPSアクセス、およびBlueXP分類インスタンスからの接続を提供します
TCP	3128だ	Cloud Volumes ONTAP からネットアップサポートにAutoSupport メッセージを送信するためのインターネットアクセスを提供します。導入後にこのポートを手動で開く必要があります。 "コネクタがAutoSupport メッセージのプロキシとしてどのように使用されるかについて説明します"
TCP	9060、9061	政府機関の地域でBlueXPの分類とBlueXPのバックアップとリカバリを有効にして使用できるようになります。

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
API コールと AutoSupport	HTTPS	443年	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、ONTAP、BlueXPへのAPI呼び出し、NetAppへのAutoSupportメッセージの送信
API コール	TCP	3000	ONTAP HA メディエーター	ONTAP HA メディエーターとの通信
	TCP	8080 です	BlueXPの分類	導入時にBlueXP分類インスタンスを確認します
DNS	UDP	53.	DNS	BlueXPによるDNS解決に使用されます

Azureでのコネクタセキュリティグループのルール

コネクタのAzure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。BlueXPでコネクタを作成すると、BlueXPでこのセキュリティグループが自動的に作成されます。他のすべてのインストールオプションには、このセキュリティグループを設定する必要があります。

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	8時80分	• 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 • Cloud Volumes ONTAPのアップグレードプロセスで使用
HTTPS	443年	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HTTPSアクセス、およびBlueXP分類インスタンスからの接続を提供します

プロトコル	ポート	目的
TCP	3128だ	Cloud Volumes ONTAP からネットアップサポートにAutoSupport メッセージを送信するためのインターネットアクセスを提供します。導入後にこのポートを手動で開く必要があります。 "コネクタがAutoSupport メッセージのプロキシとしてどのように使用されるかについて説明します"
TCP	9060、9061	政府機関の地域でBlueXPの分類とBlueXPのバックアップとリカバリを有効にして使用できるようになります。

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
API コールと AutoSupport	HTTPS	443年	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	Azure、ONTAP、BlueXPへのAPI呼び出し、NetAppへのAutoSupportメッセージの送信
API コール	TCP	8080 です	BlueXPの分類	導入時にBlueXP分類インスタンスを確認します
DNS	UDP	53.	DNS	BlueXPによるDNS解決に使用されます

Google Cloudのコネクタファイアウォールルール

ConnectorのGoogle Cloud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。BlueXPでコネクタを作成すると、BlueXPでこのセキュリティグループが自動的に作成されます。他のすべてのインストールオプションには、このセキュリティグループを設定する必要があります。

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	8時80分	• 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 • Cloud Volumes ONTAPのアップグレードプロセスで使用
HTTPS	443年	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HTTPSアクセスを提供します
TCP	3128だ	Cloud Volumes ONTAP からネットアップサポートにAutoSupport メッセージを送信するためのインターネットアクセスを提供します。導入後にこのポートを手動で開く必要があります。 "コネクタがAutoSupport メッセージのプロキシとしてどのように使用されるかについて説明します"

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
API コールと AutoSupport	HTTPS	443年	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	Google Cloud 、ONTAP、BlueXP へのAPI呼び出し、NetAppへのAutoSupportメッセージの送信
API コール	TCP	8080 です	BlueXPの分類	導入時にBlueXP分類インスタンスを確認します
DNS	UDP	53.	DNS	BlueXPによるDNS解決に使用されます

オンプレミスコネクタ用のポート

コネクタは、オンプレミスのLinuxホストに手動でインストールした場合、_inbound_portsを使用します。計画のためにこれらのポートを参照しなければならない場合があります。

これらのインバウンドルールは、すべてのBlueXP導入モデルに適用されます。

プロトコル	ポート	目的
HTTP	8時80分	• 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 • Cloud Volumes ONTAPのアップグレードプロセスで使用
HTTPS	443年	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HTTPSアクセスを提供します

著作権に関する情報

Copyright © 2024 NetApp, Inc. All Rights Reserved. Printed in the U.S.このドキュメントは著作権によって保護されています。著作権所有者の書面による事前承諾がある場合を除き、画像媒体、電子媒体、および写真複写、記録媒体、テープ媒体、電子検索システムへの組み込みを含む機械媒体など、いかなる形式および方法による複製も禁止します。

ネットアップの著作物から派生したソフトウェアは、次に示す使用許諾条項および免責条項の対象となります。

このソフトウェアは、ネットアップによって「現状のまま」提供されています。ネットアップは明示的な保証、または商品性および特定目的に対する適合性の暗示的保証を含み、かつこれに限定されないいかなる暗示的な保証も行いません。ネットアップは、代替品または代替サービスの調達、使用不能、データ損失、利益損失、業務中断を含み、かつこれに限定されない、このソフトウェアの使用により生じたすべての直接的損害、間接的損害、偶発的損害、特別損害、懲罰的損害、必然的損害の発生に対して、損失の発生の可能性が通知されていたとしても、その発生理由、根拠とする責任論、契約の有無、厳格責任、不法行為（過失またはそうでない場合を含む）にかかわらず、一切の責任を負いません。

ネットアップは、ここに記載されているすべての製品に対する変更を随時、予告なく行う権利を保有します。ネットアップによる明示的な書面による合意がある場合を除き、ここに記載されている製品の使用により生じる責任および義務に対して、ネットアップは責任を負いません。この製品の使用または購入は、ネットアップの特許権、商標権、または他の知的所有権に基づくライセンスの供与とはみなされません。

このマニュアルに記載されている製品は、1つ以上の米国特許、その他の国の特許、および出願中の特許によって保護されている場合があります。

権利の制限について：政府による使用、複製、開示は、DFARS 252.227-7013（2014年2月）およびFAR 5252.227-19（2007年12月）のRights in Technical Data -Noncommercial Items（技術データ - 非商用品目に関する諸権利）条項の(b)(3)項、に規定された制限が適用されます。

本書に含まれるデータは商用製品および / または商用サービス（FAR 2.101の定義に基づく）に関係し、データの所有権はNetApp, Inc.にあります。本契約に基づき提供されるすべてのネットアップの技術データおよびコンピュータ ソフトウェアは、商用目的であり、私費のみで開発されたものです。米国政府は本データに対し、非独占的かつ移転およびサブライセンス不可で、全世界を対象とする取り消し不能の制限付き使用権を有し、本データの提供の根拠となった米国政府契約に関連し、当該契約の裏付けとする場合にのみ本データを使用できます。前述の場合を除き、NetApp, Inc.の書面による許可を事前に得ることなく、本データを使用、開示、転載、改変するほか、上演または展示することはできません。国防総省にかかる米国政府のデータ使用権については、DFARS 252.227-7015(b)項（2014年2月）で定められた権利のみが認められます。

商標に関する情報

NetApp、NetAppのロゴ、http://www.netapp.com/TMに記載されているマークは、NetApp, Inc.の商標です。その他の会社名と製品名は、それを所有する各社の商標である場合があります。