



コネクタのネットワーク要件

Cloud Manager

Ben Cammett, Tom Onacki
June 06, 2021

This PDF was generated from https://docs.netapp.com/ja-jp/occm/reference_networking_cloud_manager.html on June 14, 2021. Always check docs.netapp.com for the latest.

目次

| | |
|-------------------------------------|---|
| コネクタのネットワーク要件 | 1 |
| ターゲットネットワークへの接続 | 1 |
| 172 の範囲の IP アドレスと競合する可能性があります | 1 |
| アウトバウンドインターネットアクセス | 1 |
| ポートおよびセキュリティグループ | 7 |

コネクタのネットワーク要件

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、作成する作業環境の種類と、有効にする予定のサービス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。

172 の範囲の IP アドレスと競合する可能性があります

ネットワークのサブネットが 172 範囲に設定されている場合、Cloud Manager から接続エラーが発生することがあります。 ["この問題の詳細については、こちらをご覧ください"](#)。

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。アウトバウンドのインターネットアクセスは、コネクタを Linux ホストに手動でインストールする場合や、コネクタで実行されているローカル UI にアクセスする場合にも必要です。

次のセクションでは、特定のエンドポイントについて説明します。

AWS でリソースを管理するエンドポイント

コネクタは、AWS 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。



VPC がネットワークアクセス制御リスト (ACL) を使用してトラフィックをフィルタリングする場合は、アウトバウンドとインバウンドの両方のトラフィックに対してこれらのエンドポイントを有効にしてください。

| エンドポイント | 目的 |
|--|---|
| <p>AWS サービス（amazonaws.com）：</p> <ul style="list-style-type: none"> ・クラウド形成 ・柔軟なコンピューティングクラウド（EC2） ・キー管理サービス（KMS） ・セキュリティトークンサービス（STS） ・シンプルなストレージサービス（S3） <p>正確なエンドポイントは、Cloud Volumes ONTAP を導入する地域によって異なります。"詳細については、AWS のマニュアルを参照してください。"</p> | <p>AWS に Cloud Volumes ONTAP を導入して管理できるようにします。</p> |
| <p>\ https://api.services.cloud.netapp.com:443</p> | <p>NetApp Cloud Central への API 要求。</p> |
| <p>\ https://cloud.support.netapp.com.s3.us-west-1.amazonaws.com</p> | <p>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。</p> |
| <p>¥ 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</p> | <p>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。</p> |
| <p>\ https://cloudmanagerinfraprod.azurecr.io</p> | <p>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。</p> |
| <p>\ https://kinesis.us-east-1.amazonaws.com</p> | <p>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。</p> |
| <p>\ https://cloudmanager.cloud.netapp.com</p> | <p>Cloud Central アカウントを含む Cloud Manager サービスとの通信。</p> |
| <p>https://netapp-cloud-account.auth0.com</p> | <p>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。</p> |
| <p>support.netapp.com:443 https://mysupport.netapp.com</p> | <p>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。</p> |
| <p>¥ 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</p> | <p>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</p> |

| エンドポイント | 目的 |
|---|--|
| ¥ 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 <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。 |

Azure でリソースを管理するエンドポイント

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 |
|---|---|
| https://management.azure.com https://login.microsoftonline.com | 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。 |
| https://management.microsoftazure.de https://login.microsoftonline.de | 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。 |
| https://management.usgovcloudapi.net/ https://login.microsoftonline.com | 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。 |
| \ 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。 |
| \ 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。 |

| エンドポイント | 目的 |
|--|--|
| \ 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）。 |
| * .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"> • 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 <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。 |

GCP でリソースを管理するためのエンドポイント

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。 |

| エンドポイント | 目的 |
|---|--|
| \ 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。 |
| \ https://cloudmanagerinfraproduct.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）。 |

| エンドポイント | 目的 |
|--|--|
| <p>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。</p> <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 <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> | <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。</p> |

Linux ホストにコネクタをインストールするエンドポイント

Connector ソフトウェアは、手動でインストールすることもできます。その場合、Connector のインストーラは、インストールプロセス中に次の URL にアクセスする必要があります。

- <http://dev.mysql.com/get/mysql-community-release-el7-5.noarch.rpm>
- <https://dl.fedoraproject.org/pub/epel/epel-release-latest-7.noarch.rpm>
- <https://s3.amazonaws.com/aws-cli/awscli-bundle.zip>

ホストは、インストール中にオペレーティングシステムパッケージの更新を試みる可能性があります。ホストは、これらの OS パッケージの別のミラーリングサイトにアクセスできます。

ローカルを使用するときに **Web** ブラウザからアクセスするエンドポイント UI

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> |

| エンドポイント | 目的 |
|---|---|
| ¥ 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。 |

ポートおよびセキュリティグループ

コネクタへの着信トラフィックは、開始しない限りありません。へのアクセスは、HTTP および HTTPS を使用して提供されます。"ローカル UI"は、まれな状況で使われます。SSH が必要になるのは、トラブルシューティングのためにホストに接続する必要がある場合のみです。

AWS のコネクタのルール

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 |
| クラウドデータの意味 | HTTP | 80 | Cloud Data Sense インスタンス | Cloud Volumes ONTAP に最適なクラウドデータ |

Azure のコネクタのルール

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

| 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 |
| API コールと AutoSupport | 443 | HTTPS | 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 | 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 |

GCP のコネクタのルール

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 |

| プロトコル | ポート | 目的 |
|-------|-----|--|
| 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.