



データブローカーのインストール方法

Cloud Manager

NetApp
May 27, 2021

目次

データブローカーのインストール方法	1
AWS にデータブローカーをインストールする	1
Azure へのデータブローカーのインストール	3
Google Cloud Platform にデータブローカーをインストールする	6
Linux ホストへのデータブローカーのインストール	9

データブローカーのインストール方法

AWS にデータブローカーをインストールする

新しいデータブローカーを作成するときは、AWS のデータブローカーオプションを選択して、VPC 内の新しい EC2 インスタンスにデータブローカーソフトウェアを導入します。Cloud Sync ではインストールプロセスがガイドされますが、インストールの準備に役立つように、このページの要件と手順が繰り返されています。

また、クラウド内または社内の既存の Linux ホストにデータブローカーをインストールすることもできます。["詳細はこちら。"](#)

サポートされている AWS リージョン

中国と GovCloud（米国）以外のすべての地域がサポートされています。

ネットワーク要件

- データブローカーは、アウトバウンドインターネット接続を必要としているため、クラウド同期サービスにポート 443 経由のタスクをポーリングできます。

Cloud Sync は、AWS にデータブローカーを導入すると、必要なアウトバウンド通信を有効にするセキュリティグループを作成します。インストールプロセス中にプロキシサーバーを使用するようにデータブローカーを設定できます。

アウトバウンド接続を制限する必要がある場合は、を参照してください ["データブローカーが連絡するエンドポイントのリスト"](#)。

- ネットワークタイムプロトコル（NTP）サービスを使用するように、ソース、ターゲット、およびデータブローカーを設定することを推奨します。3 つのコンポーネント間の時間差は 5 分を超えないようにしてください。

AWS にデータブローカーを展開するために必要な権限

の導入に使用する AWS ユーザーアカウントデータブローカーの権限は、に含まれている必要があります ["ネットアップが提供するポリシーです"](#)。

AWS データブローカーで独自の IAM ロールを使用するための要件

Cloud Sync は、データブローカーを導入するときに、データブローカーインスタンスの IAM ロールを作成します。必要に応じて、独自の IAM ロールを使用してデータブローカーを展開できます。組織に厳密なセキュリティポリシーがある場合は、このオプションを使用できます。

IAM ロールは、次の要件を満たす必要があります。

- EC2 サービスは、IAM の役割を信頼できるエンティティとして引き受けることを許可されている必要があります。
- ["この JSON ファイルで定義されている権限"](#) データブローカーが正しく機能するように、IAM ロールに関連付ける必要があります。

データブローカーを導入する際に IAM ロールを指定するには、次の手順に従います。

データブローカーのインストール


同期関係を作成するときに、AWS にデータブローカーをインストールできます。

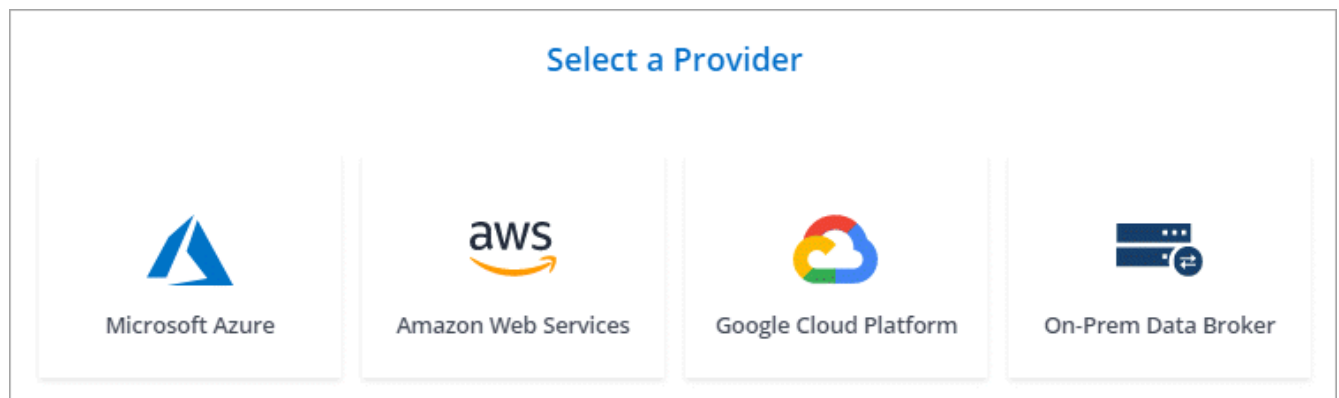
手順

1. [新しい同期の作成 *] をクリックします。
2. [同期関係の定義 *] ページで、ソースとターゲットを選択し、[続行 *] をクリックします。

「 * データブローカー * 」ページが表示されるまで、手順を完了します。

3. [* データブローカー *] ページで、[* データブローカーの作成 *] をクリックし、[* Amazon Web Services *] を選択します。

データブローカーがすでにある場合は、をクリックする必要があります  最初にアイコンをクリックします



4. データブローカーの名前を入力し、[* 続行] をクリックします。
5. AWS でデータブローカーを作成するために、Cloud Sync アクセスキーを入力します。

キーは保存されず、他の目的に使用されることもありません。

アクセスキーを指定しない場合は、ページの下部にあるリンクをクリックして CloudFormation テンプレートを使用します。このオプションを使用する場合は、AWS に直接ログインするため、クレデンシャルを指定する必要はありません。

CloudFormation テンプレートを使用してデータブローカーインスタンスを起動する方法を紹介したビデオを次に示します。

▶ https://docs.netapp.com/us-en/occm/media/video_cloud_sync.mp4 (video)

6. AWS アクセスキーを入力した場合は、インスタンスの場所を選択し、キーペアを選択し、パブリック IP アドレスを有効にするかどうかを選択します。既存の IAM ロールを選択した場合は、Cloud Sync によってロールが作成されるようにこのフィールドを空白のままにします。

独自の IAM ロールを選択した場合は、[必要な権限を指定する必要があります](#)。

Basic Settings

Location

Region

US West | Oregon

VPC

vpc-3c46c059 - 10.60.21.0/25

Subnet

10.60.21.0/25

Connectivity

Key Pair

newKey

Enable Public IP?

☒ Enable ☐ Disable


IAM Role (optional)

7. VPC でのインターネットアクセスにプロキシが必要な場合は、プロキシの設定を指定します。
8. データブローカーが利用可能になったら、Cloud Sync で [* 続行] をクリックします。

次の図は、AWS に正常に導入されたインスタンスを示しています。

Select a NetApp Data Broker

1 NetApp Data Brokers

 name

Active

US West (Oregon) Region	10.60.21.0/25 vpc-3c46c059 VPC	10.60.21.5 Private IP	5f5002eecf378e000a560988 Broker ID
us-west-2c Availability Zone	10.60.21.0/25 subnet-e7f526be Subnet	i-0fc5c97e2f5f22c20 Instance ID	

9. ウィザードのページに入力して、新しい同期関係を作成します。

AWS にデータブローカーを導入し、新しい同期関係を作成しました。このデータブローカーは、追加の同期関係とともに使用できます。

Azure へのデータブローカーのインストール

新しいデータブローカーを作成する場合、Azure のデータブローカーオプションを選択して、VNet 内の新しい仮想マシンにデータブローカーソフトウェアを導入します。Cloud Sync ではインストールプロセスがガイドされますが、インストールの準備に役立つように、このページの要件と手順が繰り返されています。

また、クラウド内または社内の既存の Linux ホストにデータブローカーをインストールすることもできます。["詳細はこちら。"](#)

サポートされている **Azure** リージョン

中国、米国政府、米国国防総省を除くすべての地域がサポートされます。

ネットワーク要件

- データブローカーは、アウトバウンドインターネット接続を必要としているため、クラウド同期サービスにポート 443 経由のタスクをポーリングできます。

Cloud Sync は、データブローカーを Azure に導入するときに、必要なアウトバウンド通信を有効にするセキュリティグループを作成します。

アウトバウンド接続を制限する必要がある場合は、を参照してください ["データブローカーが連絡するエンドポイントのリスト"](#)。

- ネットワークタイムプロトコル (NTP) サービスを使用するように、ソース、ターゲット、およびデータブローカーを設定することを推奨します。3 つのコンポーネント間の時間差は 5 分を超えないようにしてください。

認証方式

データブローカーを導入する際には、認証方式として、パスワードまたは SSH 公開鍵ペアを選択する必要があります。

キー・ペアの作成方法については、を参照してください ["Azure のドキュメント：「 Create and use an SSH public-private key pair for Linux VMs in Azure"](#)。

データブローカーのインストール

同期関係を作成するときに、Azure にデータブローカーをインストールできます。

手順

1. [新しい同期の作成 *] をクリックします。
2. [同期関係の定義 *] ページで、ソースとターゲットを選択し、[続行 *] をクリックします。

ページを完了して、「 * データブローカー * 」ページを表示します。

3. [* データブローカー *] ページで、[* データブローカーの作成 *] をクリックし、[Microsoft Azure *] を選択します。


データブローカーがすでにある場合は、をクリックする必要があります




最初にアイコンをクリック

します


Select a Provider




Microsoft Azure



Amazon Web Services



Google Cloud Platform



On-Prem Data Broker

4. データブローカーの名前を入力し、[* 続行] をクリックします。
5. プロンプトが表示されたら、Microsoft アカウントにログインします。プロンプトが表示されない場合は、*「* Azure へのログイン*」をクリックします。

このフォームは、Microsoft が所有およびホストしています。クレデンシャルがネットアップに提供されていません。

6. データブローカーの場所を選択し、仮想マシンに関する基本的な詳細を入力します。

Location

Virtual Machine

Subscription

OCCM Dev ▼

Azure Region

West US 2 ▼

VNet

Vnet1 ▼

Subnet

Subnet1 ▼

VM Name

netappdatabroker ⓘ

User Name

databroker ⓘ

Authentication Method:

☒ Password
☐ Public Key

Enter Password

..... ⓘ

Resource Group:

☒ Generate a new group
☐ Use an existing group

7. VNet でのインターネットアクセスにプロキシが必要な場合は、プロキシ設定を指定します。
8. [* Continue (続行)] をクリックし、展開が完了するまでページを開いたままにします。

この処理には最大 7 分かかることがあります。

9. Cloud Sync で、データブローカーが利用可能になったら、[* 続行] をクリックします。

10. ウィザードのページに入力して、新しい同期関係を作成します。

Azure にデータブローカーを導入し、新しい同期関係を作成しました。このデータブローカーは、追加の同期関係とともに使用できます。

管理者の同意が必要なことを示すメッセージを受信しますか？

Cloud Sync で組織内のリソースに代理でアクセスする権限が必要であるために管理者の承認が必要であることが通知された場合は、次の 2 つのオプションがあります。

1. AD 管理者に次の権限を提供するよう依頼します。

Azure では、[管理センター] > [Azure AD] > [ユーザーとグループ] > [ユーザー設定 *] の順に選択し、* ユーザーが代わりに会社のデータにアクセスするアプリに同意できるようにします。*

2. 次の URL を使用して、* CloudSync-AzureDataBrokerCreator* に代わって、AD 管理者に同意するよう依頼してください（これは管理者同意エンドポイントです）。

\ https://login.microsoftonline.com/{FILL テナント ID }/v2.0/adminconsent?client_id=8ee4ca3a-BAFA-4831-97cc-5a38923cab85&redirect_uri=https://cloudsync.netapp.com&scope=https://management.azure.com/user_impersonationhttps://graph.microsoft.com/User.Read に移動します

URL に示されているように、アプリケーションの URL は <https://cloudsync.netapp.com> で、アプリケーションのクライアント ID は 8ee4ca3a-BAFA-4831-97cc-5a38923cab85 です。

Google Cloud Platform にデータブローカーをインストールする

新しいデータブローカーを作成する場合、GCP Data Broker オプションを選択して、VPC 内の新しい仮想マシンインスタンスにデータブローカーソフトウェアを導入します。Cloud Sync ではインストールプロセスがガイドされますが、インストールの準備に役立つように、このページの要件と手順が繰り返されています。

また、クラウド内または社内の既存の Linux ホストにデータブローカーをインストールすることもできます。["詳細はこちら。"](#)

サポートされる GCP リージョン

すべてのリージョンがサポートされています。

ネットワーク要件

- データブローカーは、アウトバウンドインターネット接続を必要としているため、クラウド同期サービスにポート 443 経由のタスクをポーリングできます。

Cloud Sync は、GCP にデータブローカーを導入すると、必要なアウトバウンド通信を可能にするセキュリティグループを作成します。

アウトバウンド接続を制限する必要がある場合は、を参照してください ["データブローカーが連絡するエンドポイントのリスト"](#)。

- ネットワークタイムプロトコル（ NTP ）サービスを使用するように、ソース、ターゲット、およびデータブローカーを設定することを推奨します。3 つのコンポーネント間の時間差は 5 分を超えないようにしてください。

GCP にデータブローカーを導入するために必要な権限

データブローカーを導入する GCP ユーザに次の権限があることを確認します。

```
- compute.networks.list
- compute.regions.list
- deploymentmanager.deployments.create
- deploymentmanager.deployments.delete
- deploymentmanager.operations.get
- iam.serviceAccounts.list
```

サービスアカウントに必要な権限

データブローカーを導入する場合、次の権限を持つサービスアカウントを選択する必要があります。

```
- logging.logEntries.create
- resourcemanager.projects.get
- storage.buckets.get
- storage.buckets.list
- storage.objects.*
```

データブローカーのインストール

同期関係を作成するときに、データブローカーを GCP にインストールできます。

手順

1. [新しい同期の作成 *] をクリックします。
2. [同期関係の定義 *] ページで、ソースとターゲットを選択し、[続行 *] をクリックします。

「 * データブローカー * 」ページが表示されるまで、手順を完了します。


3. [* データブローカー *] ページで、[* データブローカーの作成 *] をクリックし、[* Google Cloud Platform*] を選択します。

データブローカーがすでにある場合は、をクリックする必要があります




最初にアイコンをクリック


Select a Provider




Microsoft Azure



Amazon Web Services



Google Cloud Platform



On-Prem Data Broker

- データブローカーの名前を入力し、[* 続行]をクリックします。
- メッセージが表示されたら、Google アカウントでログインします。

このフォームは Google が所有およびホストしています。クレデンシャルがネットアップに提供されていません。

- プロジェクトとサービスアカウントを選択し、データブローカーの場所を選択します。

Basic Settings

Project	Location
Project OCCM-Dev ▼	Region us-west1 ▼
Service Account test ▼	Zone us-west1-a ▼
Select a Service Account that includes these permissions	VPC default ▼
	Subnet default ▼

- VPC でのインターネットアクセスにプロキシが必要な場合は、プロキシの設定を指定します。

インターネットアクセスにプロキシが必要な場合は、データブローカーと同じサービスアカウントを Google Cloud で使用してプロキシを設定する必要があります。

- データブローカーが利用可能になったら、Cloud Sync で [* 続行]をクリックします。

このインスタンスの導入には、約 5 ～ 10 分かかります。Cloud Sync サービスから進捗状況を監視できます。このサービスは、インスタンスが使用可能になると自動的に更新されます。

9. ウィザードのページに入力して、新しい同期関係を作成します。

GCP にデータブローカーを導入し、新しい同期関係を作成しておきます。このデータブローカーは、追加の同期関係とともに使用できます。

他の Google Cloud プロジェクトでバケットを使用する権限を付与する

同期関係 Cloud Sync を作成し、ソースまたはターゲットとして Google Cloud Storage を選択すると、データブローカーのサービスアカウントに使用する権限があるバケットから選択できるようになります。デフォルトでは、これにはデータブローカーサービスアカウントと同じ `_PROJECT` に含まれるバケットが含まれます。ただし、必要な権限を指定した場合は、`_other_projects` からバケットを選択できます。

手順

1. Google Cloud Platform コンソールを開き、Cloud Storage サービスをロードします。
2. 同期関係のソースまたはターゲットとして使用するバケットの名前をクリックします。
3. **[Permissions]** をクリックします
4. **[追加 (Add)]** をクリックします。
5. データブローカーのサービスアカウントの名前を入力します。
6. 提供するロールを選択します [上記と同じ権限](#)。
7. **[保存 (Save)]** をクリックします。

同期関係を設定するときに、そのバケットを同期関係のソースまたはターゲットとして選択できるようになりました。

Linux ホストへのデータブローカーのインストール

新しいデータブローカーを作成する場合は、オンプレミスのデータブローカーオプションを選択して、オンプレミスの Linux ホストまたはクラウド内の既存の Linux ホストにデータブローカーソフトウェアをインストールします。Cloud Sync ではインストールプロセスがガイドされますが、インストールの準備に役立つように、このページの要件と手順が繰り返されています。

Linux ホストの要件

- * オペレーティング・システム * :
 - CentOS 7.0 、 7.7 、 および 8.0
 - Red Hat Enterprise Linux 7.7 および 8.0
 - Ubuntu Server 20.04 LTS の場合は
 - SUSE Linux Enterprise Server 15 SP1

コマンド 'yum update all' は ' データ ・ ブローカをインストールする前に ' ホスト上で実行する必要があります

Red Hat Enterprise Linux システムは、 Red Hat サブスクリプション管理に登録する必要があります。登録されていない場合、システムはインストール中に必要なサードパーティソフトウェアをアップデートす

るためのリポジトリにアクセスできません。

- * RAM * : 16GB
- * CPU * : 4 コア
- * 空きディスク容量 * : 10 GB
- * SELinux * : 無効にすることをお勧めします ["SELinux"](#) ホスト。

SELinux では、データブローカーソフトウェアの更新をブロックし、通常運用に必要なエンドポイントにデータブローカーがアクセスできないようにするポリシーが適用されます。

- * OpenSSL * : Linux ホストに OpenSSL がインストールされている必要があります。

ネットワーク要件

- Linux ホストは、ソースとターゲットに接続されている必要があります。
- ファイルサーバが Linux ホストにエクスポートへのアクセスを許可している必要があります。
- AWS へのアウトバウンドトラフィック（データブローカーは常に Amazon SQS サービスと通信）を処理するために、Linux ホストでポート 443 が開いている必要があります。
- ネットワークタイムプロトコル（ NTP ）サービスを使用するように、ソース、ターゲット、およびデータブローカーを設定することを推奨します。3 つのコンポーネント間の時間差は 5 分を超えないようにしてください。

AWS へのアクセスを有効化

S3 バケットを含む同期関係でデータブローカーを使用する場合は、Linux ホストで AWS にアクセスする準備をしておく必要があります。データブローカーをインストールする際、プログラム経由のアクセス権と特定の権限を持つ AWS ユーザに対して AWS キーを提供する必要があります。

手順

1. を使用して、IAM ポリシーを作成します ["ネットアップが提供するポリシーです"](#)。 ["AWS の手順を表示します。"](#)。
2. プログラムによるアクセス権を持つ IAM ユーザを作成します。 ["AWS の手順を表示します。"](#)。

データブローカーソフトウェアをインストールするときに AWS キーを指定する必要があるため、必ず AWS キーをコピーしてください。

Google Cloud へのアクセスを有効にします

Google Cloud Storage バケットを含む同期関係でデータブローカーを使用する場合は、Linux ホストで GCP アクセスを準備しておく必要があります。データブローカーをインストールする場合、特定の権限を持つサービスアカウントにキーを提供する必要があります。

手順

1. まだ Storage Admin の権限がない GCP サービスアカウントを作成します。
2. JSON 形式で保存されたサービスアカウントキーを作成します。 ["GCP の手順を表示します。"](#)。

このファイルには、少なくとも「 project_id 」、「 private_key 」、および「 client_email 」というプロ

パティを含める必要があります。



キーを作成すると、ファイルが生成され、マシンにダウンロードされます。

3. JSON ファイルを Linux ホストに保存します。

Microsoft Azure へのアクセスを有効にしています

Azure へのアクセスは、関係ごとに定義されます。そのためには、同期関係ウィザードでストレージアカウントと接続文字列を指定します。

データブローカーのインストール

同期関係を作成するときに、Linux ホストにデータブローカーをインストールできます。

手順

1. [新しい同期の作成 *] をクリックします。
2. [同期関係の定義 *] ページで、ソースとターゲットを選択し、[続行 *] をクリックします。

「* データブローカー *」ページが表示されるまで、手順を完了します。
3. [* データブローカー *] ページで、[* データブローカーの作成 *] をクリックし、[* オンプレミスのデータブローカー *] を選択します。

データブローカーがすでにある場合は、をクリックする必要があります



最初にアイコンをクリック



このオプションには「*_オンプレミス_データブローカー*」というラベルが付けられていますが、オンプレミスまたはクラウド上の Linux ホストにも該当します。

4. データブローカーの名前を入力し、[* 続行] をクリックします。

手順ページがすぐにロードされます。これらの手順に従う必要があります。インストーラをダウンロードするための固有のリンクが含まれています。

5. 手順ページで次の手順を実行します。

- a. 「* AWS *」、「* Google Cloud *」、またはその両方へのアクセスを有効にするかどうかを選択し

ます。

- b. インストールオプションとして、 * プロキシなし * 、 * プロキシサーバーを使用 * 、または * 認証付きプロキシサーバーを使用 * を選択します。
- c. データブローカーをダウンロードしてインストールするには、コマンドを使用します。

次の手順では、使用可能な各インストールオプションの詳細を示します。インストールオプションに基づいて正確なコマンドを取得するには、手順ページを参照してください。

- d. インストーラをダウンロードします。

- プロキシなし：

```
curl <uri>-o data_broker_installer.sh
```

- プロキシサーバを使用：

```
curl <uri>-o data_broker_installer.sh -x <proxy_host>: <proxy_port>`
```

- プロキシサーバで認証を使用する：

```
curl <uri>-o data_broker_installer.sh -x <proxy_username>:<proxy_password>@<proxy_host>:<proxy_port>` -x
```

URI

Cloud Sync の指示ページにインストールファイルの URI が表示され、オンプレミスのデータブローカーを導入するプロンプトに従ってロードされます。この URI はリンクが動的に生成され、1 回しか使用できないため、ここでは繰り返し使用されません。 [Cloud Sync から URI を取得するには、次の手順を実行します。](#)

- e. スーパーユーザーに切り替え、インストーラを実行可能にしてソフトウェアをインストールします。



以下に示す各コマンドには、AWS アクセスと GCP アクセスのパラメータが含まれています。インストールオプションに基づいて正確なコマンドを取得するには、手順ページを参照してください。

- プロキシ構成なし：

```
「 sudo -s chmod +x data_broker_installer.sh 」 / data_broker_installer.sh - A <AWS_access_key> -s <AWS_secret_key> -g <absolute_path-to-the _json ファイル>`
```

- プロキシ設定：

```
「 sudo -s chmod +x data_broker_installer.sh 」 / data_broker_installer.sh - A <AWS_access_key> -s <AWS_secret_key> -g <absolute_path-to-the _json ファイル> -h <proxy_host> -p <proxy_port>`
```

- 認証を使用したプロキシ設定：

```
「 sudo -s chmod +x data_broker_installer.sh 」 / data_broker_installer.sh - A <AWS_access_key> -s <AWS_secret_key> -g <absolute_path-to-the _json _file> -h <proxy_host> -p <proxy_port> -u <proxy_username> -w <proxy_password>
```

AWS キー

これらはユーザに適切なキーです 準備しておきます [次の手順を実行します](#)。AWS のキーはデータブローカーに格納され、オンプレミスネットワークやクラウドネットワークで実行されます。ネットアップでは、データブローカー以外でキーを使用していません。

JSON ファイル

この JSON ファイルにサービスアカウントが含まれています 準備しておく必要があるキー [次の手順を実行します](#)。

6. データブローカーが利用可能になったら、Cloud Sync で [* 続行] をクリックします。
7. ウィザードのページに入力して、新しい同期関係を作成します。

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.