



NASデータへのS3クライアントアクセスの提供

ONTAP 9

NetApp
December 20, 2024

目次

NASデータへのS3クライアントアクセスの提供	1
ONTAPでのS3マルチプロトコルのサポート	1
S3クライアントアクセスに関するNASデータの要件	3
NASデータへのS3プロトコルアクセスを有効にする	4
S3 NASバケットの作成	7
S3クライアントユーザを有効にする	8

NASデータへのS3クライアントアクセスの提供

ONTAPでのS3マルチプロトコルのサポート

ONTAP 9 12.1以降では、S3プロトコルを実行するクライアントが、NFSプロトコルとSMBプロトコルを使用するクライアントに提供されるデータと同じデータに再フォーマットすることなくアクセスできるようになりました。この機能により、NASデータを引き続きNASクライアントに提供しながら、S3アプリケーション（データマイニングや人工知能など）を実行するS3クライアントにオブジェクトデータを提供できます。

S3マルチプロトコル機能は次の2つのユースケースに対応します。

1. S3クライアントを使用した既存のNASデータへのアクセス

従来のNASクライアント（NFSまたはSMB）を使用して作成された既存のデータがNASボリューム（FlexVolまたはFlexGroupボリューム）に格納されている場合は、S3クライアントで分析ツールを使用してデータにアクセスできるようになります。

2. NASプロトコルとS3プロトコルの両方を使用してI/Oを実行できる、最新のクライアント向けのバックエンドストレージ

NASプロトコルとS3プロトコルの両方を使用して同じデータの読み取りと書き込みが可能なSparkやKafkaなどのアプリケーションに、統合アクセスを提供できるようになりました。

S3マルチプロトコルのサポートの仕組み

ONTAPのマルチプロトコルサポートでは、同じデータセットをファイル階層として、またはバケット内のオブジェクトとして表示できます。そのために、ONTAPは「S3 NASバケット」を作成します。このバケットを使用すると、S3クライアントはS3オブジェクト要求を使用してNASストレージ内のファイルを作成、読み取り、削除、列挙できます。このマッピングは、NASセキュリティ設定に準拠しており、ファイルとディレクトリのアクセス権限を監視し、必要に応じてセキュリティ監査証跡に書き込みます。

このマッピングは、指定されたNASディレクトリ階層をS3バケットとして提供することで実現されます。ディレクトリ階層内の各ファイルはS3オブジェクトとして表されます。S3オブジェクトの名前は、マッピングされたディレクトリから下への相対パスで、ディレクトリ境界はスラッシュ (/) で表されます。

ONTAPで定義されたS3ユーザは、NASディレクトリにマッピングされるバケット用に定義されたバケットポリシーに従って、このストレージにアクセスできます。これを実現するには、S3ユーザとSMB / NFSユーザの間にマッピングを定義する必要があります。SMB / NFSユーザのクレデンシャルはNAS権限のチェックに使用され、これらのアクセスから発生する監査レコードに含まれます。

SMBクライアントまたはNFSクライアントによって作成されたファイルは即座にディレクトリに配置されるため、クライアントからはデータが書き込まれる前に参照できます。S3クライアントは異なるセマンティクスを想定しており、すべてのデータが書き込まれるまで新しいオブジェクトはネームスペースに表示されません。S3からNASストレージへのこのマッピングでは、S3のセマンティクスを使用してファイルが作成され、S3の作成コマンドが完了するまでファイルが外部に表示されません。

S3 NASバケットのデータ保護

S3 NASの「バケット」は、S3クライアントのNASデータの単なるマッピングであり、標準のS3バケットではありません。そのため、NetApp SnapMirror S3機能を使用してS3 NASバケットを保護する必要はありません。代わりに、SnapMirrorの非同期ボリュームレプリケーションを使用して、S3 NASバケットを含むボリュームを保護できます。SnapMirror同期およびSVMディザスタリカバリはサポートされません。

ONTAP 9.14.1以降では、MetroCluster IPおよびFC構成のミラーされたアグリゲートとミラーされていないアグリゲートでS3 NASバケットがサポートされます。

詳細はこちらをご覧ください "[SnapMirror非同期](#)"。

S3 NASバケットの監査

S3 NASバケットは従来のS3バケットではないため、バケットに対するアクセスを監査するようにS3監査を設定することはできません。詳細については、[こちら](#)をご覧ください "[S3の監査](#)"。

ただし、S3 NASバケットにマッピングされたNASファイルとディレクトリのアクセスイベントは、従来のONTAP監査手順を使用して監査できます。そのため、S3処理でNASの監査イベントがトリガーされることがありますが、次の例外があります。

- S3クライアントアクセスがS3ポリシー設定（グループポリシーまたはバケットポリシー）で拒否された場合、イベントのNAS監査は開始されません。これは、SVMの監査チェックの前にS3権限がチェックされるためです。
- S3 GET要求のターゲットファイルのサイズが0の場合、GET要求には0のコンテンツが返され、読み取りアクセスはログに記録されません。
- S3 GET要求のターゲットファイルがユーザにトラバース権限がないフォルダにある場合は、アクセスの試行が失敗し、イベントはログに記録されません。

詳細はこちらをご覧ください "[SVMでNASイベントを監査する](#)"。

オブジェクトのマルチパートアップロード

ONTAP 9.16.1以降では、FlexGroupボリュームで有効になっている場合にオブジェクトマルチパートアップロードがサポートされ"[高度な容量分散](#)"ます。

NASファイルストレージでのオブジェクトマルチパートアップロードを使用すると、S3プロトコルクライアントで大きなオブジェクトを小さなパートとしてアップロードできます。オブジェクトマルチパートアップロードには次の利点があります。

- オブジェクトを並行してアップロードできます。
- アップロードに失敗した場合や一時停止した場合は、まだアップロードされていないパーツのみをアップロードする必要があります。オブジェクト全体のアップロードを再開する必要はありません。
- オブジェクトのサイズが事前にわかっていない場合（大きなオブジェクトがまだ書き込まれている場合など）、クライアントはオブジェクトの一部のアップロードをただちに開始し、オブジェクト全体が作成されたあとにアップロードを完了できます。

マルチパートアップロードでは、次のS3処理がサポートされます。

- AbortMultipartUpload

- CompleteMultipartUpload
- CreateMultipartUpload
- ListMultipartUpload

S3とNASの相互運用性

ONTAP S3 NASバケットは、ここに記載されているものを除き、標準のNASおよびS3機能をサポートしません。

NAS機能は現在、**S3 NAS**バケットではサポートされていません。

FabricPoolの大容量階層

S3 NASバケットをFabricPoolの大容量階層として設定することはできません。

S3機能は現在、**S3 NAS**バケットではサポートされていません。

AWSユーザメタデータ

- S3ユーザメタデータの一部として受信したキーと値のペアは、現在のリリースではオブジェクトデータとともにディスクに格納されません。
- プレフィックスが「x-amz-meta」の要求ヘッダーは無視されます。

AWSタグ

- PUT Object要求とMultipart Initiate要求では、プレフィックスが「x-amz-tagging」のヘッダーは無視されます。
- 既存のファイルのタグを更新する要求（PUT、GET、DELETE要求などに?tagging query-stringが指定されている）は、エラーで拒否されます。

バージョン管理

バケットのマッピング設定でバージョン管理を指定することはできません。

- null以外のバージョン指定（versionId=xyz query-string）を含む要求は、エラー応答を受信します。
- バケットのバージョン管理状態を変更する要求が拒否され、エラーが発生します。

S3クライアントアクセスに関するNASデータの要件

S3アクセス用にNASファイルとディレクトリをマッピングする場合は、互換性の問題がいくつかあることを理解しておくことが重要です。S3 NASバケットを使用してサービスを提供する前に、NASファイル階層の調整が必要になる場合があります。

S3 NASバケットは、S3バケット構文を使用してそのディレクトリをマッピングすることでNASディレクトリへのS3アクセスを提供し、ディレクトリツリー内のファイルはオブジェクトとして表示されます。オブジェクト名は、S3バケット設定で指定されたディレクトリに対するファイルのパス名をスラッシュで区切って指定します。

このマッピングでは、S3 NASバケットを使用してファイルとディレクトリが提供される場合、いくつかの要件が課せられます。

- S3名は1024バイトに制限されているため、パス名が長いファイルにS3を使用してアクセスすることはできません。
- ファイル名とディレクトリ名は255文字に制限されているため、オブジェクト名の連続するスラッシュ以外の文字は255文字以下にする必要があります。
- s3では、バックスラッシュ（「\」）で区切られたSMBパス名は、代わりにスラッシュ（「/」）文字を含むオブジェクト名として表示されます。
- マッピングされたNASディレクトリツリーに、合法的なS3オブジェクト名の一部のペアを共存させることはできません。たとえば、有効なS3オブジェクト名「part1/part2」と「part1/part2/part3」は、NASディレクトリツリーに同時に存在できないファイルにマッピングされます。これは、「part1/part2」が名のファイルで、もう一方のディレクトリにあるためです。
 - 「part1/part2」が既存のファイルである場合、「part1/part2/part3」のS3作成は失敗します。
 - 「part1/part2/part3」が既存のファイルである場合、S3による「part1/part2」の作成または削除は失敗します。
 - 既存のオブジェクト（バージョン管理されていないバケット内の）が既存のオブジェクトの名前に一致するS3オブジェクトの作成で置き換えられます。このオブジェクトはNASで保持されますが、完全に一致する必要があります。上記の例では、名前が衝突しても一致しないため、既存のオブジェクトが削除されることはありません。

オブジェクトストアは多数の任意の名前をサポートするように設計されていますが、NASディレクトリ構造では、1つのディレクトリに多数の名前が配置されているとパフォーマンスの問題が発生する可能性があります。特に、スラッシュ（/）文字が含まれていない名前は、すべてNASマッピングのルートディレクトリに配置されます。「NASに対応していない」名前を多用するアプリケーションは、NASマッピングではなく実際のオブジェクトストアバケットでホストする方が適しています。

NASデータへのS3プロトコルアクセスを有効にする

S3プロトコルアクセスを有効にするには、NAS対応のSVMがS3対応サーバと同じ要件（オブジェクトストアサーバの追加など）を満たしていることを確認し、ネットワークと認証の要件を確認します。

ONTAPを新規にインストールする場合は、クライアントにNASデータを提供するようにSVMを設定したあとに、そのSVMへのS3プロトコルアクセスを有効にすることを推奨します。NASプロトコルの設定については、以下を参照してください。

- ["NFSの設定"](#)
- ["SMBの設定"](#)

開始する前に

S3プロトコルを有効にする前に、次の項目を設定する必要があります。

- S3プロトコルおよび目的のNASプロトコル（NFS、SMB、またはその両方）のライセンスが設定されています。
- 必要なNASプロトコル用にSVMが設定されている。
- NFSサーバまたはSMBサーバが存在します。
- DNSおよびその他の必要なサービスが設定されている。

- NASデータがクライアントシステムにエクスポートまたは共有されています。

タスクの内容

S3クライアントからS3対応SVMへのHTTPSトラフィックを有効にするには、認証局（CA）証明書が必要です。次の3つのソースからのCA証明書を使用できます。

- SVM上の新しいONTAP自己署名証明書。
- SVM上の既存のONTAP自己署名証明書。
- サードパーティの証明書。

NASデータの提供に使用するデータLIFをS3 / NASバケットにも使用できます。特定のIPアドレスが必要な場合は、を参照してください"[データLIFを作成する](#)"。LIFでS3データトラフィックを有効にするには、S3サービスデータポリシーが必要です。SVMの既存のサービスポリシーにS3を含めるように変更できます。

S3オブジェクトサーバを作成するときは、クライアントがS3アクセスに使用するFully Qualified Domain Name（FQDN；完全修飾ドメイン名）としてS3サーバ名を入力する準備をしておく必要があります。S3サーバのFQDNの1文字目をバケット名にすることはできません。

System Manager

1. NASプロトコルが設定されているStorage VMでS3を有効にします。
 - a. [ストレージ]>[Storage VM]*をクリックし、NAS対応Storage VMを選択して[設定]をクリックし、[S3]の下をクリックし  ます。
 - b. 証明書のタイプを選択します。システムで生成された証明書を選択した場合でも独自の証明書を選択した場合でも、クライアントアクセスに必要なになります。
 - c. ネットワークインターフェイスを入力します。
2. システム生成の証明書を選択した場合は、新しいStorage VMの作成を確認した時点で証明書の情報が表示されます。[ダウンロード]をクリックし、クライアントアクセス用に保存します。
 - 今後シークレットキーは表示されません。
 - 証明書情報が再度必要な場合は、[* ストレージ]、[Storage VMs]の順にクリックし、Storage VMを選択して、[* 設定]をクリックします。

CLI

1. SVMでS3プロトコルが許可されていることを確認します。

```
+ vserver show -fields allowed-protocols
```
2. このSVMの公開鍵証明書を記録します。+新しいONTAP自己署名証明書が必要な場合は、を参照してください"[CA証明書を作成してSVMにインストールする](#)"。
3. サービスデータポリシーを更新する
 - a. SVMのサービスデータポリシーを表示します。

```
+ network interface service-policy show -vserver svm_name
```
 - b. とがない場合は、を data-s3-server services`追加し`data-core`ます。

```
+ `network interface service-policy add-service -vserver svm_name -policy policy_name -service data-core,data-s3-server
```
4. SVMのデータLIFが要件を満たしていることを確認します。

```
+ network interface show -vserver svm_name
```
5. S3サーバを作成します。

```
+ vserver object-store-server create -vserver svm_name -object-store-server s3_server_fqdn -certificate-name ca_cert_name -comment text [additional_options]
```

追加のオプションは、S3サーバの作成時または作成後いつでも指定できます。

- HTTPSはポート443ではデフォルトで有効になっています。ポート番号は、-secure-listener-portオプションを使用して変更できます。+ HTTPSを有効にすると、SSL/TLSとの適切な統合にCA証明書が必要になります。ONTAP 9.15.1以降では、S3オブジェクトストレージでTLS 1.3がサポートされません。
- HTTPはデフォルトでは無効になっています。有効にすると、サーバはポート80でリスンします。is-http-enabledオプションを指定して有効にするか、-listener-portオプションを使用してポート番号を変更できます。+ HTTPを有効にすると、すべての要求と応答がクリアテキストでネットワーク経由で送信されます。

1. S3が設定されていることを確認します。

```
+ vserver object-store-server show
```

例次のコマンドは、すべてのオブジェクトストレージサーバの設定値を検証します。

```
cluster1::> vserver object-store-server show
```

```
Vserver: vs1
```

```
Object Store Server Name: s3.example.com
Administrative State: up
Listener Port For HTTP: 80
Secure Listener Port For HTTPS: 443
HTTP Enabled: false
HTTPS Enabled: true
Certificate for HTTPS Connections: svml_ca
Comment: Server comment
```

S3 NASバケットの作成

S3 NASバケットは、S3バケット名とNASパスのマッピングです。S3 NASバケットを使用すると、既存のボリュームとディレクトリ構造を持つSVMネームスペースの任意の部分へのS3アクセスを提供できます。

開始する前に

- NASデータを含むSVMにS3オブジェクトサーバが設定されている。
- NASデータはに準拠してい["S3クライアントアクセスの要件"](#)ます。

タスクの内容

SVMのルートディレクトリ内の任意のセットのファイルとディレクトリを指定するようにS3 NASバケットを設定できます。

また、次のパラメータを任意に組み合わせてNASデータへのアクセスを許可または禁止するバケットポリシーを設定することもできます。

- ファイルおよびディレクトリ
- ユーザおよびグループの権限
- S3処理

たとえば、大規模なユーザグループに読み取り専用データアクセスを許可するバケットポリシーと、そのデータのサブセットに対して限定されたグループに処理の実行を許可するバケットポリシーが必要になる場合があります。

S3 NASの「バケット」はマッピングであり、S3バケットではないため、次の標準S3バケットのプロパティはS3 NASバケットには適用されません。

- * aggr-list\aggr-list-multiplier \storage-service-level \volume\size\exclude-aggr-list\qos-policy-group *+ S3 NASバケットの設定時にボリュームまたはqtreeが作成されません。
- * role\is-protected\is-protected-on-\ is-protected-on-cloud *+ S3 ONTAPバケットは、SnapMirror S3を使用して保護またはミラーリングされませんが、代わりにボリューム単位で使用できる通常のSnapMirror保護が使用されます。

- バージョン管理状態+ NASボリュームには、通常、異なるバージョンを保存するためのスナップショット・テクノロジーが備わっています。ただし、S3 NASバケットでは現在バージョン管理を使用できません。
- * logical-used/object-count *+と同等の統計情報は、volumeコマンドを使用してNASボリュームに対して利用できます。

System Manager

NAS対応Storage VMに新しいS3 NASバケットを追加します。

1. [* ストレージ]、[バケット]の順にクリックし、[* 追加]をクリックします。
2. S3 NASバケットの名前を入力してStorage VMを選択し、サイズを入力せずに* More Options *をクリックします。
3. 有効なパス名を入力するか、[参照]をクリックして有効なパス名のリストから選択します。+有効なパス名を入力すると、S3 NAS設定に関係のないオプションは表示されません。
4. S3ユーザをNASユーザとグループにすでにマッピングしている場合は、権限を設定し、* Save *をクリックします。+この手順で権限を設定する前に、S3ユーザをNASユーザにマッピングしておく必要があります。

それ以外の場合は、* Save *をクリックしてS3 NASバケットの設定を完了します。

CLI

NASファイルシステムを含むSVMにS3 NASバケットを作成します。+ `vserver object-store-server bucket create -vserver svm_name -bucket bucket_name -type nas -nas-path junction_path [-comment text]`

例：+ `cluster1::> vserver object-store-server bucket create -bucket testbucket -type nas -path /voll`

S3クライアントユーザを有効にする

S3クライアントユーザがNASデータにアクセスできるようにするには、S3ユーザ名を対応するNASユーザにマッピングし、バケットのサービスポリシーを使用してNASデータにアクセスする権限をユーザに付与する必要があります。

開始する前に

クライアントアクセスのユーザ名 (Linux / UNIX、Windows、S3クライアントユーザ) がすでに存在している必要があります。

S3の一部の機能はであることに注意して"[S3 NASバケットではサポートされない](#)"ください。

タスクの内容

S3ユーザ名を対応するLinux/UNIXまたはWindowsユーザにマッピングすると、NASファイルがS3クライアントからアクセスされたときにNASファイルの認証チェックが有効になります。S3からNASへのマッピングは、単一の名前またはPOSIXの正規表現で指定できるS3ユーザ名_Pattern_、およびLinux/UNIXまたはWindowsのユーザ名_Replacement_を指定して指定します。

ネームマッピングが存在しない場合は、デフォルトのネームマッピングが使用され、S3ユーザ名自体がUNIXユーザ名およびWindowsユーザ名として使用されます。UNIXおよびWindowsのデフォルトのユーザ名マッピングは、コマンドを使用して変更できます `vserver object-store-server modify`。

ローカルのネームマッピング設定のみがサポートされます。LDAPはサポートされません。

S3ユーザをNASユーザにマッピングしたら、ユーザに権限を付与できます。ユーザがアクセスできるリソース（ディレクトリとファイル）と、そのユーザに対して実行を許可または許可しないアクションを指定できます。

System Manager

1. UNIXクライアントまたはWindowsクライアント（またはその両方）のローカルネームマッピングを作成します。
 - a. Storage > Buckets *をクリックし、S3 / NAS対応のStorage VMを選択します。
 - b. を選択し、[ネームマッピング] ([ホストユーザとグループ]*) をクリックします →。
 - c. S3からWindows または S3からUNIX へのタイル（またはその両方）で、Add をクリックし、目的の Pattern (**S3**) および Replacement * (NAS) ユーザ名を入力します。
2. クライアントアクセスを許可するバケットポリシーを作成します。
 - a. [Storage]>[Buckets]をクリックし、目的の**S3**バケットの横にあるをクリックし  て、[Edit]*をクリックします。
 - b. [*追加 (Add)]をクリックし、必要な値を入力する。
 - * Principal *- S3ユーザ名を指定するか、デフォルト（すべてのユーザ）を使用します。
 - エフェクト-「*許可」または「*拒否」を選択します。
 - アクション-これらのユーザーとリソースのアクションを入力します。オブジェクトストアサーバで現在S3 NASバケットに対してサポートされているリソース処理のセットは、GetObject、PutObject、DeleteObject、ListBucket、GetBucketAclです。GetObjectAcl、GetObjectTagging、PutObjectTagging、DeleteObjectTagging、GetBucketLocation、GetBucketVersioning、PutBucketVersioning、ListBucketVersionsの各メソッドに対応しています。このパラメータではワイルドカードを使用できます。
 - * Resources *-アクションを許可または拒否するフォルダまたはファイルのパスを入力するか、デフォルト（バケットのルートディレクトリ）を使用します。

CLI

1. UNIXクライアントまたはWindowsクライアント（またはその両方）のローカルネームマッピングを作成します。

```
+vserver name-mapping create -vserver svm_name> -direction {s3-win|s3-unix} -position integer -pattern s3_user_name -replacement nas_user_name
```

 - -position-マッピング評価のプライオリティ番号。1または2を入力します。
 - -pattern- S3ユーザ名または正規表現
 - -replacement- WindowsまたはUNIXのユーザ名

例+ vserver name-mapping create -direction s3-win -position 1 -pattern s3_user_1 -replacement win_user_1 vserver name-mapping create -direction s3-unix -position 2 -pattern s3_user_1 -replacement unix_user_1

1. クライアントアクセスを許可するバケットポリシーを作成します。

```
+vserver object-store-server bucket policy add-statement -vserver svm_name -bucket bucket_name -effect {deny|allow} -action list_of_actions -principal list_of_users_or_groups -resource [-sid alphanumeric_text]
```

 - -effect {deny|allow}-ユーザが操作を要求したときにアクセスを許可するか拒否するかを指定します。
 - -action <Action>, ...-許可または拒否されるリソース操作を指定しますオブジェクトストアサーバで現在S3 NASバケットに対してサポートされている一連のリソース処理は、GetObject

、PutObject、DeleteObject、ListBucket、GetBucketAcl、GetObjectAcl、およびGetBucketLocationです。このパラメータではワイルドカードを使用できます。

- ° -principal <Objectstore Principal>, ...このパラメータで指定したオブジェクトストアサーバのユーザまたはグループに対して、アクセスを要求しているユーザを検証します。
 - オブジェクトストアサーバグループを指定するには、グループ名にプレフィックスグループ/を追加します。
 - -principal- (ハイフン文字) は、すべてのユーザにアクセス権を付与します。
- ° -resource <text>, ...権限の許可/拒否を設定するバケット、フォルダ、またはオブジェクトを指定します。このパラメータではワイルドカードを使用できます。
- ° [-sid <SID>]-オブジェクトストアサーバのバケットポリシーのステートメントのテキストコメント (オプション) を指定します。

```
例+ cluster1::> vservers object-store-server bucket policy add-statement
-bucket testbucket -effect allow -action
GetObject,PutObject,DeleteObject,ListBucket,GetBucketAcl,GetObjectAcl,
GetBucketLocation,GetBucketPolicy,PutBucketPolicy,DeleteBucketPolicy
-principal user1 -resource testbucket,testbucket/* sid "FullAccessForUser1"
```

```
cluster1::> vservers object-store-server bucket policy statement create
-vserver vs1 -bucket bucket1 -effect allow -action GetObject -principal -
-resource bucket1/readme/* -sid "ReadAccessToReadmeForAllUsers"
```

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。