



アクセスポリシーステートメントの作成または 変更 ONTAP 9

NetApp
December 20, 2024

目次

アクセスポリシーステートメントの作成または変更	1
ONTAP S3バケットとオブジェクトストアサーバのポリシーの詳細	1
デフォルトのONTAP S3バケットポリシーにアクセスルールを追加する	1
ONTAP S3オブジェクトストアサーバポリシーの作成または変更	4
ONTAP S3アクセス用の外部ディレクトリサービスの設定	6
LDAPユーザまたはドメインユーザが独自のONTAP S3アクセスキーを生成できるようにする	8

アクセスポリシーステートメントの作成または変更

ONTAP S3バケットとオブジェクトストアサーバのポリシーの詳細

S3リソースへのユーザとグループのアクセスは、バケットとオブジェクトストアサーバのポリシーで制御されます。ユーザやグループの数が少ない場合はバケットレベルでアクセスを制御すれば十分ですが、ユーザやグループの数が多場合はオブジェクトストアサーバレベルでアクセスを制御する方が簡単です。

デフォルトのONTAP S3バケットポリシーにアクセスルールを追加する

デフォルトのバケットポリシーにアクセスルールを追加できます。アクセス制御の範囲は包含バケットであるため、バケットが1つの場合に最も適しています。

開始する前に

S3サーバとバケットを含むS3対応Storage VMがすでに存在している必要があります。

権限を付与するには、事前にユーザまたはグループを作成しておく必要があります。

タスクの内容

新しいユーザとグループの新しいステートメントを追加したり、既存のステートメントの属性を変更したりできます。詳細については、のマニュアルページを参照して `vserver object-store-server bucket policy` ください。

ユーザ権限とグループ権限は、バケットの作成時に付与することも、あとで必要に応じて付与することもできます。バケット容量やQoSポリシーグループの割り当てを変更することもできます。

ONTAP 9.9.1以降では、ONTAP S3サーバでAWSクライアントオブジェクトのタグ付け機能をサポートする場合は、バケットポリシーまたはグループポリシーを使用して、および `PutObjectTagging` の `DeleteObjectTagging` 操作を `GetObjectTagging` 許可する必要があります。

実行する手順は、使用するインターフェイス（System ManagerまたはCLI）によって異なります。

System Manager

手順

1. バケットを編集します。 * Storage > Bucket* をクリックし、目的のバケットをクリックして * Edit * をクリックします。権限を追加または変更するときは、次のパラメータを指定できます。

- * Principal * : アクセス権を付与するユーザまたはグループ。
- 影響 : ユーザまたはグループへのアクセスを許可または拒否します。
- * Actions * : 特定のユーザまたはグループに対してバケットで許可されているアクション。
- * Resources * : アクセスが許可または拒否されているバケット内のオブジェクトのパスと名前。

デフォルトの * bucketname* および * bketname / *_* は、バケット内のすべてのオブジェクトへのアクセスを許可します。また、単一のオブジェクトへのアクセスを許可することもできます。たとえば、 * _bketname*_readme.txt * と指定します。

- * Conditions * (オプション) : アクセス試行時に評価される式。たとえば、アクセスを許可または拒否するIPアドレスのリストを指定できます。



ONTAP 9.14.1以降では、* Resources *フィールドでバケットポリシーの変数を指定できます。これらの変数はプレースホルダであり、ポリシーの評価時にコンテキスト値に置き換えられます。たとえば、がポリシーの変数として指定されている場合 `${aws:username}`、この変数は要求コンテキストのユーザ名に置き換えられ、そのユーザに対して設定されたポリシーアクションを実行できます。

CLI

手順

1. バケットポリシーにステートメントを追加します。

```
vserver object-store-server bucket policy add-statement -vserver svm_name  
-bucket bucket_name -effect {allow|deny} -action object_store_actions  
-principal user_and_group_names -resource object_store_resources [-sid  
text] [-index integer]
```

次のパラメータでアクセス権限を定義します。

-effect	アクセスを許可するか拒否するかを指定します。
-action	すべてのアクションを指定するか、または次の1つ以上のリストを指定できます *。 および ListMultipartUploadParts, GetObject, PutObject, DeleteObject, ListBucket, GetBucketAcl, GetObjectAcl, ListBucketMultipartUploads,

-principal	<p>S3ユーザまたはグループのリスト。</p> <ul style="list-style-type: none"> • 最大10個のユーザまたはグループを指定できます。 • S3グループを指定する場合は、次の形式で指定する必要があります。 group/group_name. • *には、パブリックアクセス（アクセスキーとシークレットキーを使用しないアクセス）を指定できます。 • プリンシパルを指定しない場合、Storage VM内のすべてのS3ユーザにアクセスが許可されます。
-resource	<p>バケットとバケットに含まれるオブジェクト。ワイルドカード文字とを`?`使用`*`して、リソースを指定するための正規表現を作成できます。リソースについては、ポリシーで変数を指定できます。これらのポリシー変数はプレースホルダであり、ポリシーの評価時にコンテキストに応じた値に置き換えられます。</p>

オプションを使用して、テキスト文字列をコメントとして指定することもできます -sid。

例

次の例では、Storage VM svm1.example.comとbucket1に対するオブジェクトストアサーババケットポリシーのステートメントを作成し、オブジェクトストアサーバユーザuser1にreadmeフォルダへのアクセスを許可するように指定しています。

```
cluster1::> vservers object-store-server bucket policy statement create
-vserver svm1.example.com -bucket bucket1 -effect allow -action
GetObject,PutObject,DeleteObject,ListBucket -principal user1 -resource
bucket1/readme/* -sid "fullAccessToReadmeForUser1"
```

次の例では、Storage VM svm1.example.comとbucket1に対するオブジェクトストアサーババケットポリシーのステートメントを作成し、オブジェクトストアサーバグループgroup1にすべてのオブジェクトへのアクセスを許可するように指定しています。

```
cluster1::> vservers object-store-server bucket policy statement create
-vserver svm1.example.com -bucket bucket1 -effect allow -action
GetObject,PutObject,DeleteObject,ListBucket -principal group/group1
-resource bucket1/* -sid "fullAccessForGroup1"
```

ONTAP 9.14.1以降では、バケットポリシーの変数を指定できます。次の例は、Storage VMとのbucket1`サーババケットポリシーステートメントを作成し、`svm1、ポリシーリソースの変数としてを指定します \${aws:username}。ポリシーが評価されると、ポリシー変数は要求コンテキストのユーザ名に置き換えられ、そのユーザに対して設定されたとおりにポリシーアクションを実行できます。たとえば、次のポリシーステートメントが評価されると \${aws:username}、はS3処理を実行するユーザに置き換えられます。ユーザ `user1`が操作を実行すると、そのユーザにはAS `bucket1/user1/*`へのアクセスが許可され `bucket1`ます。

```
cluster1::> object-store-server bucket policy statement create -vserver
svml -bucket bucket1 -effect allow -action * -principal - -resource
bucket1,bucket1/${aws:username}/*##
```

ONTAP S3オブジェクトストアサーバポリシーの作成または変更

オブジェクトストア内の1つ以上のバケットに適用できるポリシーを作成できます。オブジェクトストアサーバポリシーはユーザのグループに関連付けることができるため、複数のバケットにわたるリソースアクセスの管理が簡易化されます。

開始する前に

S3サーバとバケットを含むS3対応のSVMがすでに存在している必要があります。

タスクの内容

オブジェクトストレージサーバグループにデフォルトまたはカスタムのポリシーを指定することで、SVMレベルでアクセスポリシーを有効にできます。ポリシーは、グループ定義で指定するまで有効になりません。



オブジェクトストレージサーバポリシーを使用する場合は、ポリシー自体ではなく、グループ定義でプリンシパル（ユーザとグループ）を指定します。

ONTAP S3リソースへのアクセスに関するデフォルトの読み取り専用ポリシーは3つあります。

- フルアクセス
- NoS3アクセス
- ReadOnlyAccess

また、新しいカスタムポリシーを作成し、新しいユーザとグループの新しいステートメントを追加したり、既存のステートメントの属性を変更したりすることもできます。リンク[https://docsの](https://docs.netapp.com/us-en/ONTAP-CLI/index.html[vserver object-store-server policy^])詳細については、ONTAP コマンドリファレンスを参照してください。NetApp .com /us-en/ ONTAP -CLI/ index.html[vserver object-store-server policy^]コマンドを参照してください。


ONTAP 9 .9.1以降では、ONTAP S3サーバでAWSクライアントオブジェクトのタグ付け機能をサポートする場合は、バケットポリシーまたはグループポリシーを使用して、および `PutObjectTagging` の `DeleteObjectTagging` 操作を `GetObjectTagging` 許可する必要があります。

実行する手順は、使用するインターフェイス（System ManagerまたはCLI）によって異なります。

System Manager

- System Managerを使用して、オブジェクトストアサーバポリシー*を作成または変更します

手順

1. Storage VMを編集します。[ストレージ]>[Storage VM]*をクリックし、Storage VMをクリックして[設定]*をクリックし、[S3]の下をクリックし  ます。
2. ユーザーの追加：[* ポリシー]をクリックし、[* 追加]をクリックします。
 - a. ポリシー名を入力し、グループのリストから選択します。
 - b. 既存のデフォルトポリシーを選択するか、新しいポリシーを追加します。

グループポリシーを追加または変更するときは、次のパラメータを指定できます。

- Group：アクセスが許可されているグループ。
- 効果：1つ以上のグループへのアクセスを許可または拒否します。
- actions：特定のグループに対して1つ以上のバケットで許可されるアクション。
- Resources：1つ以上のバケット内でアクセスが許可または拒否されたオブジェクトのパスと名前。例：
 - * は、Storage VM 内のすべてのバケットへのアクセスを許可します。
 - * bucketname * および * bucketname / ** は、特定のバケット内のすべてのオブジェクトへのアクセスを許可します。
 - * bucketname/readme.txt * を指定すると、特定のバケット内のオブジェクトへのアクセスが許可されます。
- c. 必要に応じて、既存のポリシーにステートメントを追加します。

CLI

- CLIを使用して、オブジェクトストアサーバポリシー*を作成または変更します

手順

1. オブジェクトストレージサーバポリシーを作成します。

```
vserver object-store-server policy create -vserver svm_name -policy policy_name [-comment text]
```

2. ポリシーのステートメントを作成します。

```
vserver object-store-server policy statement create -vserver svm_name -policy policy_name -effect {allow|deny} -action object_store_actions -resource object_store_resources [-sid text]
```

次のパラメータでアクセス権限を定義します。

-effect	アクセスを許可するか拒否するかを指定します。
---------	------------------------

-action	すべてのアクションを指定するか、または次の1つ以上のリストを指定できます*。および ListMultipartUploadParts, GetObject, PutObject, DeleteObject, ListBucket, GetBucketAcl, GetObjectAcl, ListAllMyBuckets, ListBucketMultipartUploads,
-resource	バケットとバケットに含まれるオブジェクト。 ワイルドカード文字とを`?`使用`*`して、リソースを指定するための正規表現を作成できます。

オプションを使用して、テキスト文字列をコメントとして指定することもできます -sid。

デフォルトでは、新しいステートメントはステートメントのリストの最後に追加され、順番に処理されます。後でステートメントを追加または変更する場合は、ステートメントの設定を変更し`-index`で処理順序を変更できます。

この手順で説明されているコマンドの詳細については、を["ONTAPコマンド リファレンス"](#)参照してください。

ONTAP S3アクセス用の外部ディレクトリサービスの設定

ONTAP 9.14.1以降では、外部ディレクトリのサービスがONTAP S3オブジェクトストレージに統合されました。この統合により、外部ディレクトリサービスによるユーザとアクセスの管理が簡素化されます。

外部ディレクトリサービスに属するユーザグループに、ONTAPオブジェクトストレージ環境へのアクセスを提供できます。Lightweight Directory Access Protocol (LDAP) は、Active Directoryなどのディレクトリサービスと通信するためのインターフェイスで、IDおよびアクセス管理 (IAM) のデータベースとサービスを提供します。アクセスを提供するには、ONTAP S3環境でLDAPグループを設定する必要があります。アクセスの設定が完了すると、グループメンバーにONTAP S3バケットに対する権限が付与されます。LDAPの詳細については、を参照してください["LDAPノシヨウホウホウノカイヨウ"](#)。

また、Active Directoryユーザグループを高速バインドモードに設定して、ユーザクレデンシャルを検証し、サードパーティおよびオープンソースのS3アプリケーションをLDAP接続を介して認証できるようにすることもできます。

開始する前に

LDAPグループを設定し、グループアクセスの高速バインドモードを有効にする前に、次のことを確認してください。

1. S3サーバを含むS3対応Storage VMが作成されている。を参照して ["S3用のSVMの作成"](#)
2. そのStorage VMにバケットが作成されている。を参照して ["バケットを作成する"](#)
3. Storage VMにDNSが設定されています。を参照して ["DNSサービスの設定"](#)
4. LDAPサーバの自己署名ルート認証局 (CA) 証明書がStorage VMにインストールされている。を参照して

"自己署名ルートCA証明書をSVMにインストールする"

5. SVMでTLSを有効にしてLDAPクライアントが設定されている。およびを参照してください"[LDAPクライアント設定を作成する](#)"[情報を取得するためのLDAPクライアント設定とSVMの関連付け](#)"。

外部ディレクトリサービス用のS3アクセスの設定

1. グループのSVMの_name service database_ofとしてldapを指定し、ldapのパスワードを指定します。

```
ns-switch modify -vserver <vserver-name> -database group -sources
files,ldap
ns-switch modify -vserver <vserver-name> -database passwd -sources
files,ldap
```

リンク<https://docs.netapp.com/us-en/ONTAP-CLI/vserver-services-name-service-ns-switch-modify.html>[vserver services name-service ns-switch modify^]コマンドを参照してください。

2. オブジェクトストアバケットポリシーのステートメントを作成し、アクセスを許可するLDAPグループを設定し`principal`ます。

```
object-store-server bucket policy statement create -bucket <bucket-name>
-effect allow -principal nasgroup/<ldap-group-name> -resource <bucket-
name>, <bucket-name>/*
```

例：次の例は、用のバケットポリシーステートメントを作成します buck1。このポリシーは、LDAPグループにリソース（バケットとそのオブジェクト）への`buck1`アクセスを許可し`group1`ます。

```
vserver object-store-server bucket policy add-statement -bucket buck1
-effect allow -action
GetObject,PutObject,DeleteObject,ListBucket,GetBucketAcl,GetObjectAcl,Li
stBucketMultipartUploads,ListMultipartUploadParts,
ListBucketVersions,GetObjectTagging,PutObjectTagging,DeleteObjectTagging
,GetBucketVersioning,PutBucketVersioning -principal nasgroup/group1
-resource buck1, buck1/*
```

3. LDAPグループのユーザがS3クライアントからS3処理を実行できることを確認します group1。

認証にLDAP高速バインドモードを使用する

1. グループのSVMの_name service database_ofとしてldapを指定し、ldapのパスワードを指定します。

```
ns-switch modify -vserver <vserver-name> -database group -sources
files,ldap
ns-switch modify -vserver <vserver-name> -database passwd -sources
files,ldap
```

リンク[https://docs](https://docs.netapp.com/us-en/ONTAP-CLI/vserver-services-name-service-ns-switch-modify.html)の詳細については、ONTAPコマンドリファレンスを参照してください。NetApp.com/us-en/ONTAP-CLI/vserver-services-name-service-ns-switch-modify.html[vserver services name-service ns-switch modify^]コマンドを参照してください。

2. S3バケットにアクセスするLDAPユーザの権限がバケットポリシーで定義されていることを確認します。詳細については、[を参照してください](#) "バケットポリシーを変更する"。
3. LDAPグループのユーザが次の処理を実行できることを確認します。
 - a. S3クライアントでアクセスキーを次の形式で設定します。

```
"NTAPFASTBIND" + base64-encode(user-name:password) `例` "NTAPFASTBIND"
:+base64-encode(ldapuser:password) 。
NTAPFASTBINDbGRhcHVzZXI6cGFzc3dvcmQ=
```



S3クライアントからシークレットキーの入力を求められることがあります。シークレットキーがない場合は、16文字以上のパスワードを入力できます。

- b. ユーザに権限が割り当てられているS3クライアントから基本的なS3処理を実行します。

UIDとGIDを使用しないユーザに対するActive Directoryのリソース認証

bucket-policyステートメントで指定されたnasgroupまたはnasgroupの一部であるユーザにUIDとGIDが設定されていない場合、これらの属性が見つからないと検索が失敗します。

検索の失敗を避けるため、NetAppでは、信頼できるドメインをUPN形式を使用することを推奨していません。nasgroup / [group@trusted_domain.com](#)

LDAP高速バインドを使用しない場合に信頼できるドメインユーザのユーザアクセスキーを生成するには

UPN形式で指定されたユーザを持つエンドポイントを使用します s3/services/<svm_uuid>/users。例：

```
$curl -siku FQDN\\user:<user_name> -X POST
https://<LIF_IP_Address>/api/protocols/s3/services/<SVM_UUID>/users -d
{"comment":"<S3_user_name>",
"name":<user[@fqdn] (https://github.com/fqdn)>,"<key_time_to_live>":"PT6H3M"}'
```

LDAPユーザまたはドメインユーザが独自のONTAP S3アクセスキーを生成できるようにする

ONTAP 9.14.1以降では、ONTAP管理者としてカスタムロールを作成し、ローカルグル

ープ、ドメイングループ、またはLightweight Directory Access Protocol (LDAP) グループに付与して、それらのグループに属するユーザがS3クライアントアクセス用の独自のアクセスキーとシークレットキーを生成できるようにすることができます。

カスタムロールを作成してアクセスキーを生成するAPIを呼び出すユーザに割り当てるには、Storage VMでいくつかの設定手順を実行する必要があります。

開始する前に

次の点を確認します。

1. S3サーバを含むS3対応Storage VMが作成されている。を参照して "[S3用のSVMの作成](#)"
2. そのStorage VMにバケットが作成されている。を参照して "[バケットを作成する](#)"
3. Storage VMにDNSが設定されています。を参照して "[DNSサービスの設定](#)"
4. LDAPサーバの自己署名ルート認証局 (CA) 証明書がStorage VMにインストールされている。を参照して "[自己署名ルートCA証明書をSVMにインストールする](#)"
5. Storage VMでTLSが有効になっているLDAPクライアントが設定されています。を参照して "[LDAPクライアント設定を作成する](#)"
6. クライアント設定をSVMに関連付けます。を参照して "[LDAPクライアント設定をSVMに関連付ける](#)"リンク <https://docs>の詳細については、『ONTAPコマンドリファレンス』を参照してください。NetApp.com /us-en/ ONTAP -CLI/ vserver-services-name-service-ldap-create.html[vserver services name-service ldap create^]コマンドを参照してください。
7. データStorage VMを使用している場合は、管理ネットワークインターフェイス (LIF) とVM上に、LIFのサービスポリシーを作成します。^]および[[network interface service-policy create](#)]コマンドの詳細については[[network interface create](#)、ONTAPコマンドリファレンスを参照してください。

アクセスキー生成のためのユーザの設定

1. グループのStorage VMの_name service database_としてldapを指定し、ldapのパスワードを指定します。

```
ns-switch modify -vserver <vserver-name> -database group -sources
files,ldap
ns-switch modify -vserver <vserver-name> -database passwd -sources
files,ldap
```

リンク<https://docs>の詳細については、ONTAPコマンドリファレンスを参照してください。NetApp.com /us-en/ ONTAP -CLI/ vserver-services-name-service-ns-switch-modify.html[vserver services name-service ns-switch modify^]コマンドを参照してください。

2. S3ユーザREST APIエンドポイントへのアクセスを含むカスタムロールを作成：
security login rest-role create -vserver <vserver-name> -role <custom-role-name> -api "/api/protocols/s3/services/*/users" -access <access-type>`この例では`s3-role、Storage VM上のユーザに対してロールが生成され svm-1、読み取り、作成、更新のすべてのアクセス権が付与されます。

```
security login rest-role create -vserver svm-1 -role s3role -api
"/api/protocols/s3/services/*/users" -access all
```

リンク[https://docs](https://docs.netapp.com/us-en/ONTAP-CLI/security-login-rest-role-create.html)の詳細については、ONTAPコマンドリファレンスを参照してください。NetApp.com /us-en/ ONTAP -CLI/ security-login-rest-role-create.html[security login rest-role create^]コマンドを参照してください。

3. security loginコマンドを使用してLDAPユーザグループを作成し、S3ユーザREST APIエンドポイントにアクセスするための新しいカスタムロールを追加します。リンク[https://docs](https://docs.netapp.com/us-en/ONTAP-CLI/security-login-create.html)の詳細については、『ONTAPコマンドリファレンス』を参照してください。NetApp.com /us-en/ ONTAP -CLI/ security-login-create.html[security login create^]コマンドを参照してください。

```
security login create -user-or-group-name <ldap-group-name> -application
http -authentication-method nsswitch -role <custom-role-name> -is-ns
-switch-group yes
```

この例では、LDAPグループを ldap-group-1`に作成し `svm-1、APIエンドポイントにアクセスするためのカスタムロールを `s3role`追加し、高速バインドモードでLDAPアクセスを有効にします。

```
security login create -user-or-group-name ldap-group-1 -application http
-authentication-method nsswitch -role s3role -is-ns-switch-group yes
-second-authentication-method none -vserver svm-1 -is-ldap-fastbind yes
```

詳細については、[を参照してください "nsswitch認証にLDAP高速バインドを使用する"](#)。

ドメインまたはLDAPグループにカスタムロールを追加すると、そのグループのユーザはONTAPエンドポイントへの制限付きアクセスが許可されます /api/protocols/s3/services/{svm.uuid}/users。APIを呼び出すことで、ドメインまたはLDAPグループのユーザは、S3クライアントにアクセスするための独自のアクセスキーとシークレットキーを生成できます。キーを生成できるのは自分だけで、他のユーザーには生成できません。

S3ユーザまたはLDAPユーザとして、独自のアクセスキーを生成

ONTAP 9.14.1以降では、S3クライアントにアクセスするための独自のアクセスキーとシークレットキーを生成できます（管理者が独自のキーを生成するロールをユーザに許可している場合）。次のONTAP REST API エンドポイントを使用すると、自分専用のキーを生成できます。

HTTPメソッドとエンドポイント

このREST API呼び出しでは、次のメソッドとエンドポイントを使用します。このエンドポイントの他のメソッドの詳細については、リファレンスを参照して ["APIドキュメント"](#) ください。

HTTPメソッド	パス
投稿	/api/protocols/s3/services/ {svm.uuid} /users

カールの例

```
curl
--request POST \
--location "https://$FQDN_IP /api/protocols/s3/services/{svm.uuid}/users "
\
--include \
--header "Accept: */*" \
--header "Authorization: Basic $BASIC_AUTH"
--data '{"name": "_name_"}'
```

JSON出力の例

```
{
  "records": [
    {
      "access_key":
"Pz3SB54G2B_6dsXQPrA5HrTPcf478qoAW6_Xx6qyqZ948AgZ_7YfCf_9nO87YoZmskxx3cq41
U2JAH2M3_fs321B4rkzS3a_oC5_8u7D8j_45N8OsBCBPWGD_1d_ccfq",
      "_links": {
        "next": {
          "href": "/api/resourcelink"
        },
        "self": {
          "href": "/api/resourcelink"
        }
      },
      "name": "user-1",
      "secret_key":
"A20_tDhC_cux2C2BmtL45bXB_a_Q65c_96FsAcOdo14Az8V31jBKDTc0uCL62Bh559gPB8s9r
rn0868QrF38_1dsV2u1_9H2tSf3qQ5xp9NT259C6z_GiZQ883Qn63X1"
    }
  ],
  "num_records": "1"
}
```

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权を有し、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权については、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。