テクニカル レポート

S3 in ONTAP best practices

ONTAP 9.9.1

ネットアップ、John Lantz

2021年8月| TR-4814

概要

このテクニカルレポートでは、Amazon Simple Storage Service（S3）と NetApp ® ONTAP ® ソフトウェアを使用する場合のベストプラクティスについて説明します。また、ネイティブ S3 アプリケーションを使用するオブジェクトストアとして ONTAP を使用する場合や、NetApp FabricPool の階層化のデスティネーションとして を使用する場合の機能と構成についても説明します。

目次

概要 **4**

主なユースケース **4**

ネイティブ S3 アプリケーション 4

FabricPool エンドポイント 4

要件 **5**

プラットフォーム 5

Data LIFs 5

クラスタLIFs 5

S3 ライセンス 5

アーキテクチャ **6**

サービスポリシー 6

オブジェクトストアサーバ 7

バケット 7

ユーザー 8

ネイティブ S3 アプリケーションとリモートクラスタ階層化の構成 **8**

ONTAP System Manager 8

ONTAP CLI 12

ローカルクラスタ階層化の設定 **15**

ONTAP System Manager 16

ONTAP CLI 17

セキュリティ **19**

ローカル階層 19

配線 19

サポートされている S3 処理 **20**

バケット 20

オブジェクト 20

グループポリシー 20

ユーザ管理 20

ONTAP 9.9.1 21

相互運用性 **21**

詳細情報の入手方法

バージョン履歴.....22

お問い合わせはまで 22

表一覧

表 1）ネットアップの相互運用性 21

図一覧

図 1）ONTAP の S3 オブジェクトストレージの中核となる要素 6
図 2）FlexGroup ボリューム.....7
図 3）ローカルクラスタの階層化 15

概要

NetApp ONTAP 9.8 ソフトウェアは、Amazon Simple Storage Service（S3）をサポートします。ONTAP は、AWS S3 API アクションのサブセットをサポートし、AFF、FAS、ONTAP Select などの ONTAP ベースのシステムでデータをオブジェクトとして表現できるようにします。

NetApp StorageGRID® ソフトウェアは、ネットアップのオブジェクトストレージ向けフラッグシップ製品である解決策です。今後も継続して提供します。ONTAP は、エッジ上での取り込み / 前処理ポイントを提供することで StorageGRID を補完します。ネットアップが提供するオブジェクトデータ向けデータファブリックを拡張し、ネットアップ製品ポートフォリオの価値を高めます。

主なユースケース

ONTAP の S3 の主な目的は、ONTAP ベースのシステム上のオブジェクトをサポートすることです。ONTAP ユニファイドストレージアーキテクチャで、ファイル（NFS および SMB）、ブロック（FC および iSCSI）、オブジェクト（S3）がサポートされるようになりました。

ネイティブ **S3** アプリケーション

S3 を使用したオブジェクトのサポートに ONTAP が必要になるお客様が増えています。大容量のアーカイブワークロードには適していますが、ネイティブ S3 アプリケーションの需要は急速に拡大しており、次のようなものがあります。

- 分析
- 人工知能
- エッジからコアへの取り込み
- 機械学習

ONTAP System Manager など、使い慣れた管理ツールを使用して、ONTAP での開発や運用に必要な高性能オブジェクトストレージを迅速にプロビジョニングできるようになりました。そのため、ONTAP の Storage Efficiency 機能とセキュリティを活用できます。

FabricPoolエンドポイント

ONTAP 9.8 以降では、FabricPool で ONTAP のバケットへの階層化がサポートされるため、ONTAP から ONTAP への階層化が可能になります。これは、既存の FAS インフラをオブジェクトストアのエンドポイントとして転用する場合に最適なオプションです。

FabricPool では、次の 2 つの方法で ONTAP への階層化がサポートさ

- **ローカルクラスタ階層化：**アクセス頻度の低いデータは、クラスタ LIF を使用してローカルクラスタにあるバケットに階層化されます。
- **リモートクラスタ階層化：**アクセス頻度の低いデータは、FabricPool クライアントの IC LIF と ONTAP オブジェクトストアのデータ LIF を使用して、リモートクラスタにあるバケットに階層化され、従来の FabricPool クラウド階層と同じように配置されます。

300TB を超える非アクティブデータを階層化する場合、最初のネットアップオブジェクトストア解決策である StorageGRID を使用することを推奨します。ONTAP または StorageGRID をクラウド階層として使用する場合は、FabricPool ライセンスは必要ありません。

要件

プラットフォーム

- **NetApp AFFストレージ システム**S3 は、ONTAP 9.8+ を使用するすべての AFF プラットフォームでサポートされます。
- **FASストレージ システム**S3 は、ONTAP 9.8+ を使用するすべての FAS プラットフォームでサポートされます。
- **NetApp ONTAP Select**S3 は、ONTAP Select 9.8+ を使用するすべてのプラットフォームでサポートされます。
- **Cloud Volumes ONTAP**ONTAP 9.9..1 以降では、Cloud Volumes ONTAP for Azure で S3 がサポートされます。S3 は他の Cloud Volumes ONTAP プロバイダではサポートされていません。

データ LIF

オブジェクトストアサーバをホストしている Storage Virtual Machine（SVM）が S3 を使用してクライアントアプリケーションと通信するには、データ LIF が必要です。リモートクラスタ階層化用に設定されている場合、FabricPool はクライアントで、オブジェクトストアはサーバです。

クラスタ LIF

ローカルクラスタ階層化が設定されている場合、ローカル階層（ONTAP CLI ではストレージアグリゲートとも呼ばれます）はローカルバケットに接続されます。FabricPool は、クラスタ内のトラフィックにクラスタ LIF を使用します。

注： クラスタ LIF のリソースが最大限まで使用されないと、パフォーマンスが低下する可能性があります。この問題を回避するために、ローカルバケットに階層化する場合は 2 ノード以上のクラスタを使用することを推奨します。ベストプラクティスは、ローカル階層の HA ペアとローカルバケットの HA ペアを推奨します。シングルノードクラスタでは、ローカルバケットへの階層化は推奨されません。

S3 ライセンス

FC、iSCSI、NFS、NVMe-oF、SMB などの他のプロトコルと同様、S3 を ONTAP で使用するには、ライセンスのインストールが必要です。S3 ライセンスは無償ライセンスですが、ONTAP 9.8 にアップグレードするシステムにインストールする必要があります。

新しい ONTAP 9.8 システムには S3 ライセンスが事前にインストールされています。

S3 ライセンス は、ネットアップサポートサイトのマスターライセンスキーのページからダウンロードできます。

インストール

S3 ライセンスをインストールするには、ONTAP CLI で次のコマンドを実行します。

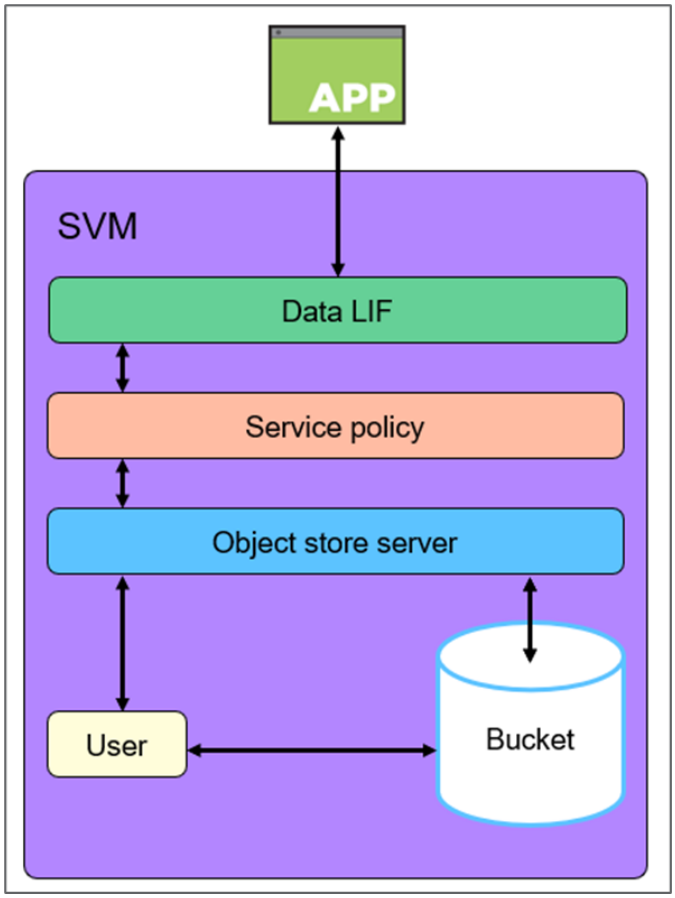
```
system license add <license_key>
```

アーキテクチャ

オブジェクト ストレージは、ファイル ストレージやブロック ストレージなどの他のストレージ アーキテクチャとは対照的に、データをオブジェクトとして管理するストレージ アーキテクチャです。オブジェクトは1つのコンテナ（バケットなど）内に保持され、他のディレクトリ内のディレクトリにあるファイルとしてネストされることはありません。

オブジェクトストレージのパフォーマンスはファイルストレージやブロックストレージよりも低下する可能性がありますが、拡張性は大幅に向上しており、ペタバイト単位のデータを含むバケットも珍しくありません。

図 1）ONTAP の S3 オブジェクトストレージの中核となる要素



サービス ポリシー

データサービスポリシーは SVM に割り当てられ、クライアントアプリケーションプロトコルをサポートするためにデータ LIF で必要な一連のネットワークサービスを提供します。たとえば、データ NFS は NFS トラフィックのサポートに使用され、データ iSCSI は iSCSI トラフィックのサポートに使用されます。

ONTAP 9.8 では、data-s3-server サービスを使用することで、S3 を使用するクライアントアプリケーショントラフィックを LIF がサポートできるようになりました。

注　：data-s3-server サービスに加えて、LIF を使用するアプリケーションが想定どおりに動作するように、data-core サービスをすべてのサービスポリシーに含める必要があります。

オブジェクト ストア サーバ

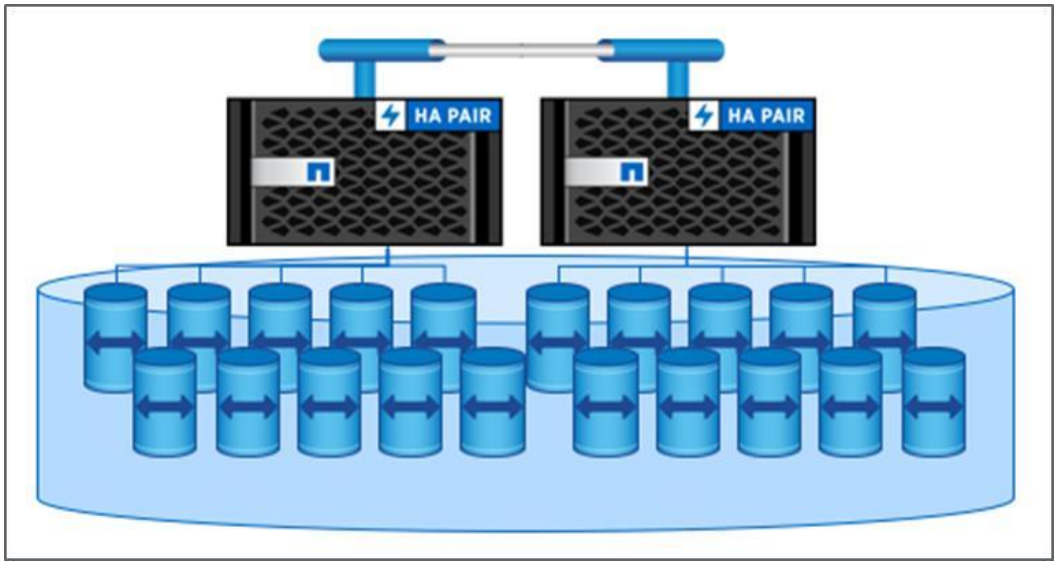
SVM のオブジェクトストアサーバは、ファイルストレージやブロックストレージなどの他のストレージアーキテクチャとは対照的に、データをオブジェクトとして管理します。バケットとユーザの権限レベルの管理は、オブジェクトストアサーバのレベルでも行われます。

ONTAP S3 は、SVM ごとに 1 つのオブジェクトストアサーバをサポートします。

バケット

ONTAP では、バケットの基盤となるアーキテクチャは FlexGroup ボリュームです。複数のコンスティチュエントメンバーボリュームで構成される単一のネームスペースで、図 2 に示すように単一のボリュームとして管理されます。FlexGroup内の個々のファイルは、個々のメンバー ボリュームに割り当てられ、複数のボリュームやノードにまたがってストライプされることはありません。96GB よりも小さいバケットを個別にプロビジョニングすることはできません。

図 2）FlexGroup ボリューム



バケットで FlexGroup ボリュームを使用する場合は、ボリュームの自動拡張ではなく、エラスティックサイジングを使用します。FlexGroup の最大ボリューム数は、基盤となるハードウェアの物理的な最大値によってのみ制限され、10 ノードクラスタで 20PB および 4、000 億ファイルに対してテスト済みです。

ONTAP S3 では最大 12、000 個のバケットがサポートされますが、1 つの FlexGroup ボリュームに作成できるバケットは 1、000 個までです。

Amazon S3 の最大オブジェクトサイズは 5TB です。ONTAP S3 は、最大 16TB のオブジェクトをサポートしています。5TB を超えるオブジェクトは、Amazon が定義した最大オブジェクトサイズを超えることができないクライアントとの相互運用性の問題が発生する可能性があります。

注　：ONTAP 9.7 のバケット（FlexGroup ボリュームごとに 1 つのバケット）と ONTAP 9.8（FlexGroup ボリュームごとに複数のバケット）で構成されているアーキテクチャ上の変更は反映されません。新しいアーキテクチャを活用するには、既存のバケットから ONTAP 9.8 バケットにデータを移行する必要があります。

デフォルトのバケット設定

手動で設定しないバケットは、アグリゲート、FlexGroup、およびバケットのプロビジョニングにデフォルト設定が使用されます。

アグリゲート

バケットをサポートする FlexGroup ボリュームは、次の優先度を使用してアグリゲート上にプロビジョニングします。

- Flash Poolアグリゲート
- HDDアグリゲート
- qlc SSD アグリゲート
- TLC SSD アグリゲート

FlexGroupボリューム

デフォルトの FlexGroup サイズは大きく、ほとんどの環境で大幅に拡張することができます。

- ONTAP では 1.6PB
- ONTAP Select で 100TB

デフォルトサイズをプロビジョニングするための十分な容量がクラスタにない場合、既存の環境でプロビジョニングできるようになるまで、サイズは半分に縮小されます。たとえば 300TB の環境では、FlexGroup ボリュームは 200TB で自動的にプロビジョニングされます。（1.6TB、800TB、400TB の FlexGroup ボリュームは環境に適していません）。

バケット

デフォルトのノードは「」です。

- 800GB ONTAP
- ONTAP Select では 200MB

バケットの拡張用の容量を確保するには、FlexGroup ボリュームのすべてのバケットの総容量が FlexGroup ボリュームの容量の 33% 未満である必要があります。この要件を満たすことができない場合、新しく作成する FlexGroup ボリューム上に、作成中のバケットが自動的にプロビジョニングされます。

ユーザ

許可されたクライアントへの接続を制限するには、すべての ONTAP オブジェクトストアでユーザ許可が必要です。特定のバケットまたは S3 処理へのアクセスを許可、拒否、またはユーザレベルで条件付きにすることができます。

ONTAP S3 では、オブジェクトストアあたり 4、000 ユーザをサポートしています。

ネイティブの S3 アプリケーションとリモートのクラスタ階層化の設定

ネイティブの S3 アプリケーションや FabricPool クライアントなどの外部クライアントは、データ LIF を使用して ONTAP オブジェクトストアに接続します。ONTAP でオブジェクトストアを作成する最も簡単な方法は、ONTAP システムマネージャを使用する方法です。CLI を使用する際に複数の手順が必要になるプロセスは、ネットアップが推奨するベストプラクティスに従って数回のクリックで完了するようになりました。よりカスタムな設定を行うには、CLI を使用した設定が必要です。

ONTAP System Manager

ONTAP でオブジェクトストアを作成する最も簡単な方法は、ONTAP システムマネージャを使用して、CLI で必要な複数の手順を数回のクリックで完了させることです。ONTAP System Manager を使用して作成されたオブジェクトストアはカスタマイズが可能ですが、デフォルトでネットアップが推奨するベストプラクティスに従って作成されます。カスタム構成には CLI を使用した構成が必要です。

ONTAP System Manager を使用してオブジェクトストア、バケット、および権限のユーザを作成するには、次の手順を実行します。

オブジェクトストアを設定します

SMSAPリポジトリを設定するには、次の手順を実行します。

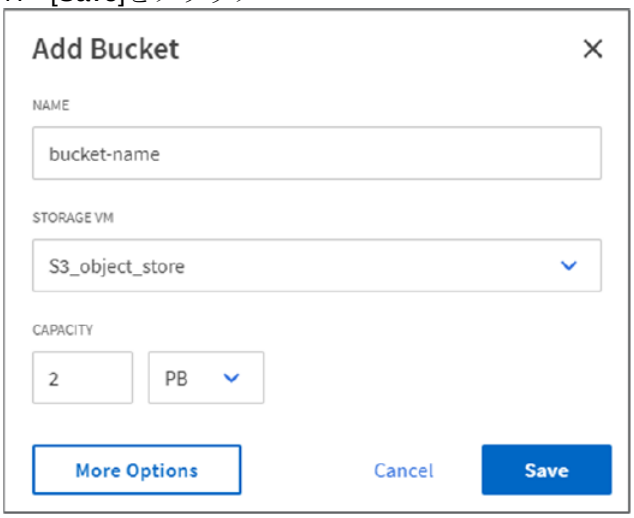
1. ONTAP System Managerを起動します。
2. [Storage]をクリックします。
3. [ストレージ VMs]をクリックします。
4. [追加]をクリックします。新しい SVM は必要ありません。S3 機能は、SVM の「設定」メニューを使用して既存の SVM に追加できます。
5. SVMの名前を必ず指定してください。
6. アクセスプロトコルとして S3 を有効にするを選択します。デフォルトでは、TLS を有効にする（ポート 443）オプションとシステム生成証明書を使用する（Use System-Generated Certificate）オプションが選択されています。ただし、サードパーティの認証局からの署名証明書を使用することを推奨します。
7. S3 サーバに名前を付けます。

   注： サーバ名は、クライアントアプリケーションで Fully Qualified Domain Name（FQDN ；完全修飾ドメイン名）として使用されます。
8. ノードのネットワークインターフェイスを入力してください。

バケットを設定する

LUNを構成するには、次の手順を実行します。

1. ONTAP System Managerを起動します。
2. [Storage]をクリックします。
3. バケットをクリックします。
4. [追加]をクリックします。
5. バケットに名前を付けます。
6. バケットを割り当てる SVM / オブジェクトストアを選択します。以前に作成した SVM とオブジェクトストアが同じである必要があります。
7. [Save]をクリック



その他のオプション

階層化に使用

このオプションを選択すると、ONTAP システムマネージャは最も安価なメディアにバケットを作成し、HDD > QLC > TLC > NVMe の優先順位を設定します。

パフォーマンス サービス レベル

バケットに適したサービス品質（QoS）を選択します。次のオプションがあります。

- **Extreme**50、000 IOPS、1562MBps
- **パフォーマンス：**30、000 IOPS、937MBps
- **価値**15,000 IOPS、468MBps
- **カスタム**既存の QoS ポリシーを使用するか、新しいポリシーを作成します。

注　：バケットが階層化に使用されている場合、パフォーマンスサービスレベルは選択できません。FabricPool では FlashPool ワークロードがサポートされません。

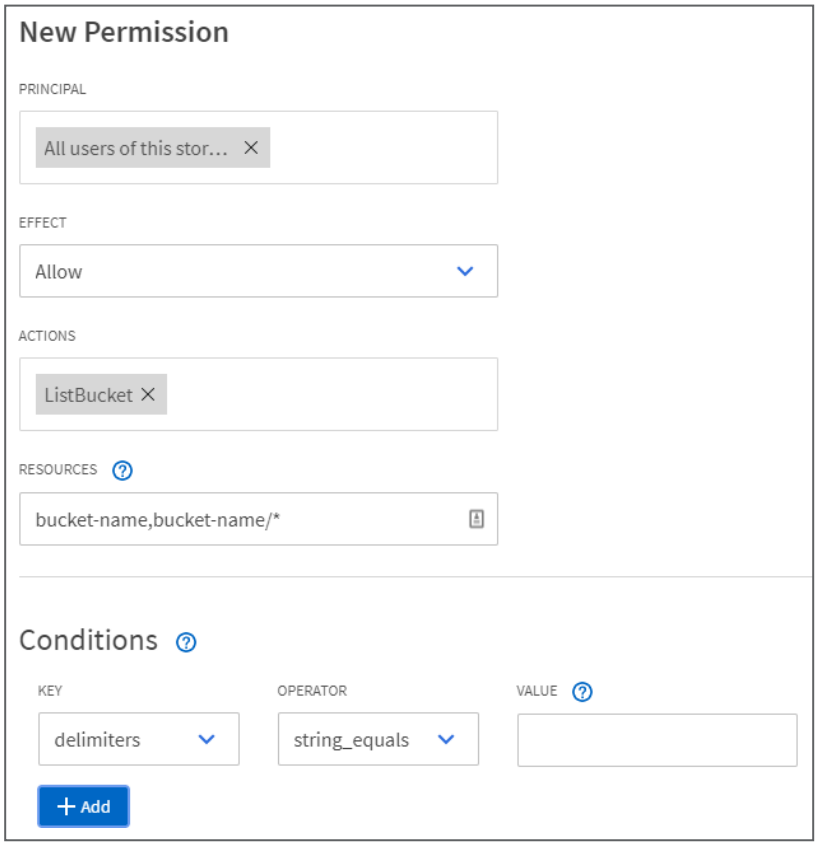
権限

アクセス権限を既存のバケットからコピーするか、新しいバケットを作成します。

注：　ユーザとグループにアクセスするには、事前にユーザとグループを設定しておく必要があります。ユーザとグループの追加

ロールを新規作成するには、次の手順を実行します。

1. [バケットの追加] ページで、[権限] までスクロールダウンし、[追加] をクリックします。
2. プリンシパルユーザーを設定します。オプションを使用して、SVM のすべてのユーザ（デフォルト）、すべてのパブリックユーザと匿名ユーザ、および SVM に関連付けられた個々のユーザを指定できます。
3. エフェクトを設定します。オプションには、Allow（デフォルト）と Deny があります。
4. アクションを設定します。GetObject、PutObject、DeleteObject、ListBucket（デフォルト）、GetBucketAcl、GetObjectAcl、ListBucketMultipartUploads、および ListMultipartUploadParts 。
5. リソースを設定する。デフォルトでは、bucket-name と bucket-name / * が使用されます。
6. 条件を設定します。
7. 条件を追加します。最大 10 個の条件文を追加できます。各条件文は、キー、演算子、および 1 つ以上の値で構成されます。



ユーザとグループの追加

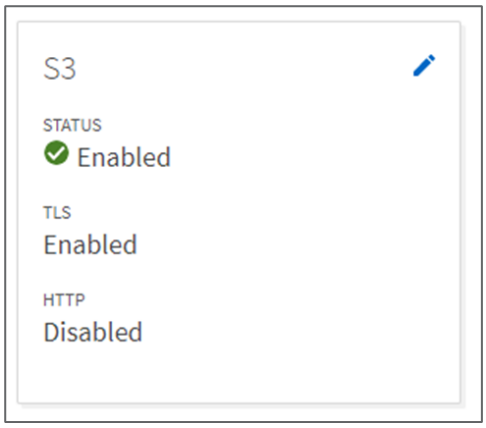
許可されたクライアントへの接続を制限するには、すべての ONTAP オブジェクトストアでユーザ許可が必要です。特定のバケットまたは S3 処理へのアクセスを、権限を使用してユーザレベルおよびグループレベルで許可、拒否、または条件付きにすることができます。

ONTAP S3 では、オブジェクトストアまたは SVM あたり 4、000 ユーザがサポートされます。

注　：バケットの作成時に、デフォルトで root ユーザ（UID 0）が作成されます。root ユーザには、すべてのバケットとオブジェクトに対するフルアクセスが許可されます。クライアントアプリケーションからのアクセスに root ユーザを使用しないでください。クライアントアクセス用に追加のユーザを作成する必要があります。

ユーザとグループを管理するには、次の手順を実行します。

1. ONTAP System Managerを起動します。
2. [Storage]をクリックします。
3. [ストレージ VMs]をクリックします。
4. ユーザとグループを追加する SVM を選択します。
5. S3 プロトコルボックスの Edit アイコンをクリックします。



6. [ユーザー] タブまたは [グループ] タブを選択します。
7. [追加]をクリックします。
8. ユーザまたはグループを選択します。
9. あとで使用できるように、アクセスキーとシークレットキーをコピーまたはダウンロードします。

   注： シークレットキーは今後表示されません。
10. グループを設定する場合は、ユーザとポリシーを割り当てます。
11. ユーザを設定する場合は、権限メニューを使用します。

ONTAP CLI

ONTAP でオブジェクトストアを作成する最も簡単な方法は ONTAP システムマネージャを使用する方法ですが、ONTAP システムマネージャを使用して作成したオブジェクトストアを使用すると、より簡単にカスタマイズすることができます。

たとえば、ONTAP System Manager は、ストレージ用のバケットで使用されるローカル階層（アグリゲート）を自動的に選択します。ベストプラクティスを推奨してこの方法で実施しますが、複雑な環境の場合は、経験豊富なストレージ管理者と同じローカル階層を選択しないこともあります。

カスタム構成には、ONTAP CLI を使用した構成が必要です。

ONTAP CLI を使用してオブジェクトストア、バケット、および権限のユーザを作成するには、次の手順を実行します。

1. サービスポリシーを作成します。
2. S3 を使用するデータ LIF を作成します。
3. CA 証明書をインストールします。
4. オブジェクト ストア サーバを作成
5. バケットを作成します。
6. ユーザを作成

サービスポリシーを作成します

SVM LIF で S3 データトラフィックを有効にするには、サービスポリシーが必要です。

ONTAP CLI を使用してサービスポリシーを作成するには、次のコマンドを実行します。

```
network interface service-policy create
-vserver <name>
-policy <name>
-services data-s3-server, data-core
```

注　　：data-s3-server サービスに加えて、LIF を使用するアプリケーションが想定どおりに動作するように、data-core サービスをすべてのサービスポリシーに含める必要があります。

S3 を使用するデータ LIF を作成します

オブジェクトストアサーバをホストしている SVM が S3 を使用してクライアントアプリケーションと通信するには、データ LIF が必要です。ベストプラクティスとして、すべてのノードに S3 データ LIF を作成することを推奨します。

リモートクラスタ階層化用に設定されている場合、FabricPool はクライアントで、オブジェクトストアはサーバです。FabricPool ではオブジェクトストアで FQDN を使用する必要があるため、すべての S3 データ LIF をオブジェクトストアサーバが使用する FQDN に関連付ける必要があります。

注：　ONTAP の外部に DNS エントリを作成する必要があります。S3 のデータ LIF のすべての IP アドレスを使用するホストエントリは 1 つにすることを推奨します。

`dns-zone` ONTAP DNS ロードバランシングの設定です。詳細について は、TR-4523 『ONTAP における DNS ロードバランシング』を参照してください。

ONTAP CLI を使用してサービスポリシーを使用する LIF を作成するには、次のコマンドを実行します。

```
network interface create
-vserver <name>
-lif <name>
-service-policy <name>
-home-node <node>
-home-port <port>
-address <number>
-netmask <number>
-status-admin up
```

CA 証明書をインストールします

CA 証明書を使用すると、クライアントアプリケーションと ONTAP オブジェクトストアサーバの間に信頼関係が作成されます。CA 証明書は、リモートクライアントからアクセスできるオブジェクトストアとして使用する前に、ONTAP にインストールする必要があります。

自己署名証明書を使用できますが、サードパーティの認証局からの署名証明書を使用することを推奨します。

ONTAP CLI を使用して CA 証明書をインストールするには、次のコマンドを実行します。

```
security certificate install -type server -vserver <name> -type server-ca
```

オブジェクト ストア サーバを作成

ONTAP オブジェクトストアサーバは、ファイルストレージやブロックストレージなどの他のストレージアーキテクチャとは対照的に、データをオブジェクトとして管理します。

ONTAP CLI を使用してオブジェクトストアサーバを作成するには、次のコマンドを実行します。

```
vserver object-store-server create
-vserver <name>
-object-store-server <FQDN>
-certificate-name <name>
-secure-listener-port <443>
-is-http-enabled <false>
```

注　　：FabricPool は、DNS を介して S3 データ LIF で使用されるすべての IP アドレスにこの名前を解決する必要があります。

バケットを作成します

ONTAP CLI を使用してバケットを作成するには、次のコマンドを実行します。

```
vserver object-store-server bucket create
-vserver <name>
-bucket <name>
-aggr-list <aggregate name>,<aggregate name>
-aggr-list-multiplier <number of constiuent volumes per aggregate> (default 4)
-size <size>
```

ユーザを作成

許可されたクライアントへの接続を制限するには、すべての ONTAP オブジェクトストアでユーザ許可が必要です。

注　：有効なアクセス権とシークレットキーペアを持つすべての S3 ユーザは、SVM 内のすべてのバケットとオブジェクトにアクセスできます。

ONTAP CLI を使用してユーザを作成するには、次のコマンドを実行します。

```
vserver object-store-server user create
-vserver <name>
-user <name>
```

ONTAP CLI を使用してユーザのアクセスキーとシークレットキーを表示するには、次のコマンドを実行します。

注　：Advanced権限レベルが必要です。

```
object-store-server user show
```

rootユーザ

バケットの作成時に、デフォルトで root ユーザ（UID 0）が作成されます。root ユーザには、すべてのバケットとオブジェクトに対するフルアクセスが許可されます。クライアントアプリケーションからのアクセスに root ユーザを使用しないでください。クライアントアクセス用に追加のユーザを作成する必要があります。

ONTAP 管理者は `object-store-server users regenerate-keys`、コマンドを実行してこのユーザのアクセスキーとシークレットキーを設定する必要があります。

ローカルクラスタ階層化の設定

ONTAP 9.8 以降では、FabricPool で ONTAP のバケットへの階層化がサポートされるため、ONTAP 間で階層化できます。これは、既存の FAS インフラをオブジェクトストアのエンドポイントとして転用する場合に最適なオプションです。

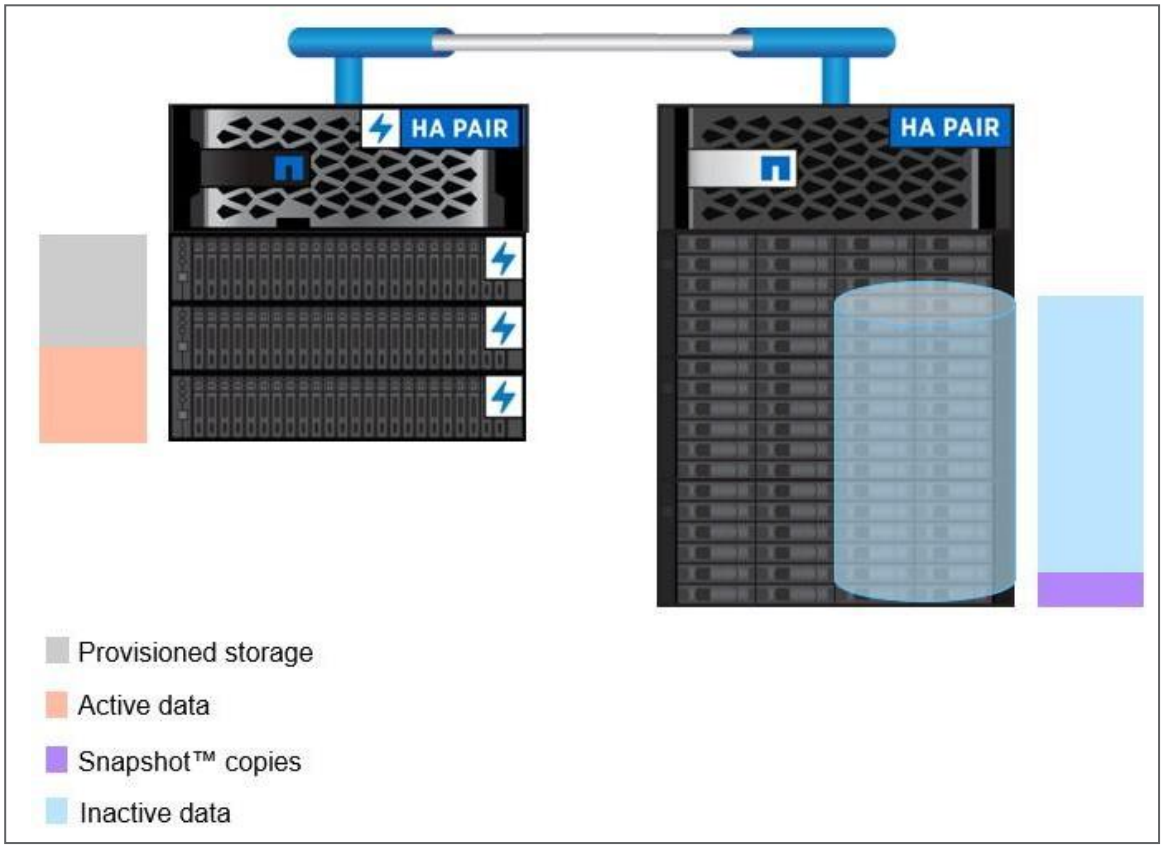
ローカルクラスタの階層化が設定されている場合、アクセス頻度の低いデータはローカルアグリゲート（通常は SSD）からローカルバケット（通常は HDD）に階層化され、クラスタ LIF を使用します。

使用頻度の低いデータを 300TB 以上階層化する場合は、ネットアップのオブジェクトストア解決策である StorageGRID を使用することを推奨します。ONTAP または StorageGRID をクラウド階層として使用する場合は、FabricPool ライセンスは必要ありません。

FabricPool の詳細について は、TR-4598 ：『 FabricPool Best Practices 』を参照してください。

注： クラスタ LIF のリソースが最大限まで使用されないと、パフォーマンスが低下する可能性があります。この問題を回避するために、ローカルバケットに階層化する場合は 2 ノード以上のクラスタを使用することを推奨します。ベストプラクティスは、ローカル階層の HA ペアとローカルバケットの HA ペアを推奨します。シングルノードクラスタでは、ローカルバケットへの階層化は推奨されません。

図 3）ローカルクラスタの階層化



ONTAP System Manager

ONTAP でローカル階層化用のオブジェクトストアを作成する最も簡単な方法は、ONTAP システムマネージャを使用することです。CLI を使用する複数の手順を数回のクリックで削減できます。ONTAP システムマネージャを使用して作成したオブジェクトストアはカスタマイズが可能ですが、デフォルトでネットアップが推奨するベストプラクティスを使用してください。
カスタム構成には、CLI を使用した設定が必要です。

オブジェクトストアを設定します

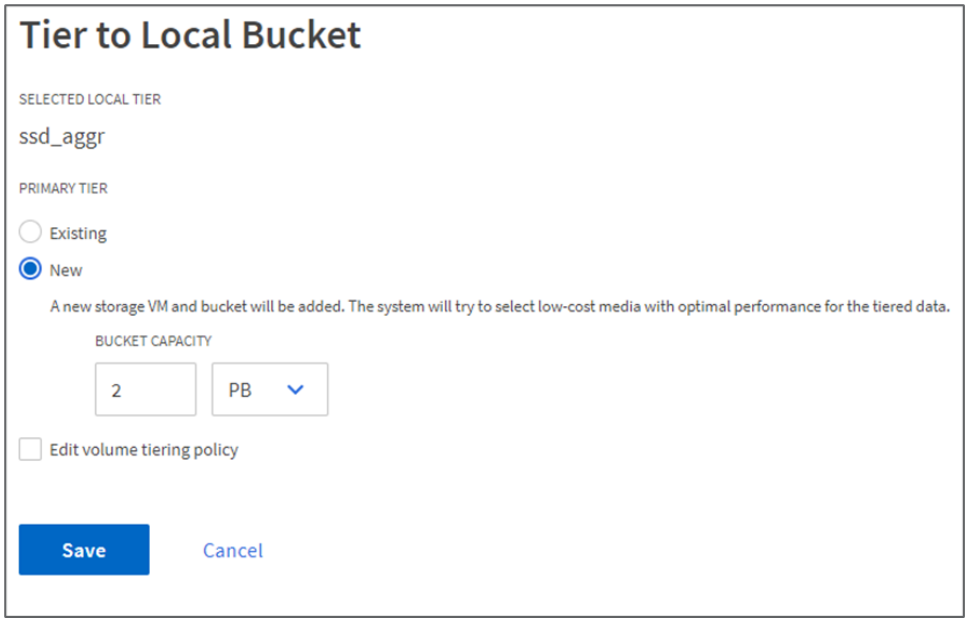
ローカルクラスタの階層化に使用するオブジェクトストアを作成するには、次の手順を実行します。

1. ONTAP System Managerを起動します。
2. [Storage]をクリックします。
3. 階層をクリックします
4. ローカル階層を選択してください。
5. More >>
6. ローカル バケットに階層化
7. システムの最初のローカルバケットの場合は、New を選択します。

   新しい SVM、オブジェクトストアサーバ、およびバケットが作成されます。ONTAP システムマネージャが最も安価なメディアにバケットを作成し、HDD > QLC > TLC > NVMe の優先順位を設定します。

   ローカルバケットがすでに作成されている場合は、「既存」を選択します。

   注　：クラスタ内のすべての FabricPool ローカル階層に同じローカルバケットを接続することで、ボリューム移動の最適化が実現します。ボリューム移動のデスティネーションローカル階層がソースローカル階層と同じバケットを使用している場合、バケットに格納されているソースボリューム上のデータはローカル階層に戻されません。ボリュームの移動を最適化することで、ネットワーク効率が大幅に向上します。



8. バケットの容量を設定
9. ボリューム階層化ポリシーを変更（オプション）
10. [Save]をクリックします。

ONTAP CLI

ONTAP でローカル階層化用のオブジェクトストアを作成する最も簡単な方法は ONTAP システムマネージャを使用する方法ですが、ONTAP システムマネージャを使用して作成したオブジェクトストアを使用すると、より簡単にカスタマイズすることができます。

たとえば、ONTAP System Manager は、バケットがストレージに使用するローカル階層（アグリゲート）を自動的に選択します。ONTAP System Manager では推奨されるベストプラクティスに従っているため、複雑な環境の場合は、経験豊富なストレージ管理者が選択したローカル階層と同じではないこともあります。

カスタム構成には、ONTAP CLI を使用した構成が必要です。

ONTAP CLI を使用してローカル階層化用のオブジェクトストアとバケットを作成するには、次の手順を実行します。

1. クラスタ SVM にオブジェクトストアサーバを作成
2. データ SVM にバケットを作成します。
3. ユーザを作成
4. オブジェクトストアとバケットを使用してクラウド階層を追加する
5. クラウド階層をローカル階層に接続します

クラスタ SVM にオブジェクトストアサーバを作成

ONTAP CLI を使用してクラスタ SVM にオブジェクトストアサーバを作成するには、次のコマンドを実行します。

```
vserver object-store-server create
-vserver Cluster
-object-store-server <name> (This is the FGDN used by FabricPool)
-certificate-name <name>
```

ベストプラクティスとしては認証局（CA）証明書のインストールと使用が推奨されていますが、CA 証明書のインストールは必須ではありません。証明書を使用しない場合は、http を有効にし、https を無効にする必要があります。

```
vserver object-store-server create
-vserver Cluster
-object-store-server <name> (This is the FGDN used by FabricPool)
-is-http-enabled true
-is-https-enabled false
```

オブジェクトストアの権限の設定

権限はオブジェクトストアレベルで設定でき、オブジェクトストア内のすべてのバケットに適用されます（または指定したバケットに適用されます）。ONTAP CLI を使用してオブジェクトストアポリシーステートメントを設定するには、次のコマンドを実行します。

```
vserver vserver object-store-server policy statement create
-vserver <data svm>
-policy <name>
-effect <allow/deny>
-action <*, GetObject, PutObject, DeleteObject, ListBucket, GetBucketAcl,GetObjectAcl,
ListBucketMultipartUploads, ListMultipartUploadParts>
-principal <S3 user or group> （ポリシーごとに最大 10 個）
-resource <bucket name>
```

データ SVM にバケットを作成します

ONTAP CLI を使用してバケットを作成するには、次のコマンドを実行します。

```
vserver object-store-server bucket create
-vserver <name>
-bucket <name>
-aggr-list <aggregate name>,<aggregate name>
-aggr-list-multiplier <number of constiuent volumes per aggregate> (default 4)
-size <size> (95GB minimum)
```

注： Advanced 権限 `-aggr-list`は使用する必要があります。

バケットの権限を設定

ONTAP CLI を使用してバケット権限ステートメントを設定するには、次のコマンドを実行します。

```
vserver vserver object-store-server bucket policy add-statement
-vserver <data svm>
-bucket <name>
-effect <allow/deny>
-action <*, GetObject, PutObject, DeleteObject, ListBucket, GetBucketAcl,GetObjectAcl,
ListBucketMultipartUploads, ListMultipartUploadParts>
-principal <S3 user or group> （ポリシーごとに最大 10 個）
-resource <bucket name>
```

ユーザを作成

許可されたクライアントへの接続を制限するには、すべての ONTAP オブジェクトストアでユーザ許可が必要です。

注 ：有効なアクセス権とシークレットキーペアを持つすべての S3 ユーザは、SVM 内のすべてのバケットとオブジェクトにアクセスできます。

ONTAP CLI を使用してユーザを作成するには、次のコマンドを実行します。

```
vserver object-store-server user create
-vserver <name>
-user <name>
```

ONTAP CLI を使用してユーザのアクセスキーとシークレットキーを表示するには、次のコマンドを実行します。

Advanced権限レベルが必要です。

```
object-store-server user show
```

ユーザ グループ

ユーザは、オブジェクトストアレベルまたはバケットレベルでポリシーステートメントに関連付けることができるグループに追加できます。ONTAP CLI を使用してグループポリシーを作成し、にユーザを追加するには、次のコマンドを実行します。

```
vserver vserver object-store-server group create
-vserver <data svm>
-name <group name>
-users <user1, user2, etc.
-policy <policy name>
```

オブジェクトストアとバケットを使用してクラウド階層を追加する

ONTAP CLIを使用してクラウド階層を追加するには、次のコマンドを入力します。

```
storage aggregate object-store config create
-object-store-name <name the cloud tier>
-provider-type ONTAP_S3
-server <name of the Cluster svm object store server>
-container-name <bucket-name>
-access-key <string>
-secret-password <string>
-ipspace Cluster
-ssl-enabled <true/false>
-is-certificate-validation-enabled true
-use-http-proxy false
-url-stle <path-style/virtual-hosted-stle>
```

クラウド階層をローカル階層に接続します

ONTAP CLI を使用してローカルバケット階層（ストレージアグリゲート）に接続するには、次のコマンドを実行します。

```
storage aggregate object-store attach
-aggregate <name>
-object-store-name <cloud tier name>
```

注： ローカルバケットをローカル階層に接続することは、永続的なアクションです。接続後にローカルバケットとローカル階層の接続を解除することはできません。FabricPool ミラーを使用すると、別のローカルバケットまたはクラウド階層を接続できます。

セキュリティ

ローカル階層

NetApp Storage Encryption（NSE）、NetApp Volume Encryption（NVE）、および NetApp Aggregate Encryption（NAE）は、ONTAP のバケットに書き込まれるオブジェクトにも同様に適しています。ONTAP では、S3 に NSE、NVE、NAE のいずれも必要ありません。

ネットワークを介して転送

TLS/SSL 暗号化は、システムで生成された証明書を使用してデフォルトで有効になります。ただし、サードパーティの認証局からの署名証明書を使用することを推奨します。

TLS 暗号化を使用しないクライアント / オブジェクトストア通信（HTTP、ポート 80）もサポートされていますが、推奨されるベストプラクティスではありません。

署名バージョン 4

ONTAP の S3 では、署名バージョン 4（v4 署名）を使用する必要があります。

注 ： v2 シグニチャを使用すると、接続に失敗します。一般に使用される S3 ブラウザも含め、多くのクライアントアプリケーションではデフォルトで v2 の署名が使用されるため、この点に注意する必要があります。接続エラーを回避するために、v4 署名を使用するようにクライアントアプリケーションを設定します。

サポートされる S3 処理数

バケット

アスタリスクが付いているアクションは、S3 REST API ではなく ONTAP でサポートされています。

- DeleteBucket*
- DeleteBucketPolicy *
- GetBucketAcl
- ヘッドバケット
- ListBuckets
- PutBucket*

オブジェクト

- PutObject
- PutObjectTagging（9.9..1）
- GetObject
- GetObjectAcl
- GetObjectTagging（9.9..1）
- DeleteObject
- DeleteObjectTagging（9.9..1）
- HeadObject（ヘッドオブジェクト）
- ListObjects
- ListObjectsV2
- ListParts
- UploadPart のアップロード
- AbortMultipartUpload
- CompleteMultipartUpload
- CreateMultipartUpload を実行します
- ListMultipartUpload の略

グループ ポリシー

これらの処理は S3 に固有ではなく、一般に Identity and Management（IAM）に関連付けられます。ONTAP ではこれらのコマンドをサポートしていますが、IAM REST API は使用していません。

- [ポリシーの作成]
- AttachGroup ポリシー

ユーザ管理

これらの処理は S3 専用ではなく、一般に IAM に関連付けられています。

- createUser
- deleteUser を指定します
- CreateGroup をクリックします
- DeleteGroup

ONTAP 9、9.1

ONTAP 9.9.1 では、ONTAP S3 にオブジェクトメタデータとタグ付けのサポートが追加されました。

- PutObject、CreateMultipartUpload に、を使用したキーと値のペアが追加されました `x-amz-meta-<key>`
  例：`x-amz-meta-project: ontap_s3`
- GetObject、および HeadObject からユーザ定義のメタデータが返されるようになりました
- タグはバケットと一緒に使用することもできます。メタデータとは異なり、タグは次の機能を使用してオブジェクトから独立して読み取ることができます。
- PutObjectTagging の 2 つのグループが
- GetObjectTagging の 2 つの機能を
- DeleteObjectTagging の場合

相互運用性

表 1 に示す通常の相互運用性の例外は、ONTAP オブジェクトストアに固有です。

表 1）ネットアップの相互運用性

重点項目	サポート	サポート対象外
データ保護	• Cloud Sync	• イレイジャー コーディング • 情報ライフサイクル管理 • NetApp MetroCluster™ • NDMP • NetApp SnapLock®テクノロジ • NetApp SnapMirror®テクノロジ： • NetApp SyncMirror®テクノロジ • オブジェクトのバージョン管理 • SMTape • SVM-DR • ユーザが作成した Snapshot • WORM
暗号化	• NetApp Aggregate Encryption（NAE） • NetApp Volume Encryption（NVE） • NetApp Storage Encryption（NSE） • TLS/SSL	• SLAG
ストレージの効率化	• 重複排除 • 圧縮 • コンパクション	アグリゲートレベルの効率化
ストレージ仮想化	-	NetApp FlexArray®テクノロジ
QoS	QoSの最大数（上限） QoSの最小値（下限）	-
その他の機能	-	• 監査 • NetApp FPolicyソフトウェア • qtree • クォータ

詳細情報の入手方法

このドキュメントに記載されている情報の詳細については、以下のドキュメントやWebサイトを確認してください。

- S3構成パワー ガイド
  https://docs.netapp.com/ontap-9/topic/com.netapp.doc.pow-s3-cg/S3%20configuration.pdf
- オブジェクトストレージのプロビジョニング
  https://docs.netapp.com/ontap/us-en/pdfs/sidebar/Provision_object_storage.pdf
- TR-4598：『FabricPool Best Practices』
  https://www.netapp.com/jp/media/tr-4598.pdf
- ONTAP 9ドキュメント センター
  https://docs.netapp.com/ontap-9/index.jsp
- ONTAPとONTAP System Managerのドキュメント リソース
  https://www.netapp.com/us/documentation/ontap-and-oncommand-system-manager.aspx
- ネットアップの製品ドキュメント
  https://www.netapp.com/us/documentation/index.aspx

バージョン履歴

バージョン	日付	ドキュメントの改訂履歴
1.3	2021年8月	9.9..1 用に更新。 オブジェクトタギングのサポートデフォルトのプロビジョニング容量とアクセス権に関する詳細を追加。
1.2	2021年3月	ローカルクラスタ階層化のための ONTAP CLI が更新されました。
1.1	2021年1月	サポートされる S3 処理を更新しました。
1.0	2021年1月	初版リリース

お問い合わせ

本テクニカル レポートの品質向上について、ご意見をお寄せください。

連絡先は、docfeedback@netapp.com（英語）です。

ご連絡の際は、件名に本ドキュメントのタイトル名「TR-4814 S3のベストプラクティス」を含めてください。

本ドキュメントに記載されている、特定バージョンの製品と機能がお客様の環境でサポートされるかどうかは、ネットアップ サポート サイトにあるInteroperability Matrix Tool（IMT）で確認してください。NetApp IMTには、ネットアップがサポートする構成を構築するために使用できる製品コンポーネントやバージョンが定義されています。翻訳対象外サポートの可否は、お客様の実際のインストール環境が公表されている仕様に従っているかどうかによって異なります。

機械翻訳に関する免責事項

原文は英語で作成されました。英語と日本語訳の間に不一致がある場合には、英語の内容が優先されます。公式な情報については、本資料の英語版を参照してください。翻訳によって生じた矛盾や不一致は、法令の順守や施行に対していかなる拘束力も法的な効力も持ちません。

著作権に関する情報

商標に関する情報

TR-4814-0821-JP

NetApp