



## ベストプラクティスと推奨事項 Astra Trident

NetApp  
April 16, 2024

# 目次

ベストプラクティスと推奨事項 .....	1
導入 .....	1
ストレージ構成 .....	1
Astra Trident を統合 .....	8
データ保護 .....	19
セキュリティ .....	24

# ベストプラクティスと推奨事項

## 導入

Astra Trident の導入時には、ここに示す推奨事項を使用してください。

### 専用のネームスペースに導入します

"[ネームスペース](#)" 異なるアプリケーション間で管理を分離できるため、リソース共有の障壁となります。たとえば、あるネームスペースの PVC を別のネームスペースから使用することはできません。Astra Trident は、Kubernetes クラスタ内のすべてのネームスペースに PV リソースを提供するため、権限が昇格されたサービスアカウントを利用します。

また、Trident ポッドにアクセスすると、ユーザがストレージシステムのクレデンシャルやその他の機密情報にアクセスできるようになります。アプリケーションユーザと管理アプリケーションが Trident オブジェクト定義またはポッド自体にアクセスできないようにすることが重要です。

### クォータと範囲制限を使用してストレージ消費を制御します

Kubernetes には、2 つの機能があります。これらの機能を組み合わせることで、アプリケーションによるリソース消費を制限する強力なメカニズムが提供されます。。"[ストレージクォータメカニズム](#)" 管理者は、グローバルおよびストレージクラス固有の、容量とオブジェクト数の使用制限をネームスペース単位で実装できます。さらに、を使用します "[範囲制限](#)" 要求がプロビジョニングツールに転送される前に、PVC 要求が最小値と最大値の両方の範囲内にあることを確認します。

これらの値はネームスペース単位で定義されます。つまり、各ネームスペースに、リソースの要件に応じた値を定義する必要があります。の詳細については、こちらを参照してください "[クォータの活用方法](#)"。

## ストレージ構成

ネットアップポートフォリオの各ストレージプラットフォームには、コンテナ化されたアプリケーションやそうでないアプリケーションに役立つ独自の機能があります。

### プラットフォームの概要

Trident は ONTAP や Element と連携1つのプラットフォームが他のプラットフォームよりもすべてのアプリケーションとシナリオに適しているわけではありませんが、プラットフォームを選択する際には、アプリケーションのニーズとデバイスを管理するチームを考慮する必要があります。

使用するプロトコルに対応したホストオペレーティングシステムのベースラインベストプラクティスに従う必要があります。必要に応じて、アプリケーションのベストプラクティスを適用する際に、バックエンド、ストレージクラス、PVC の設定を利用して、特定のアプリケーションのストレージを最適化することもできます。

### ONTAP と Cloud Volumes ONTAP のベストプラクティス

Trident 向けに ONTAP と Cloud Volumes ONTAP を設定するためのベストプラクティスをご確認ください。

次に示す推奨事項は、Trident によって動的にプロビジョニングされたボリュームを消費するコンテナ化されたワークロード用に ONTAP を設定する際のガイドラインです。それぞれの要件を考慮し、環境内で適切かどうかを評価する必要があります。

## Trident 専用の SVM を使用

Storage Virtual Machine (SVM) を使用すると、ONTAP システムのテナントを分離し、管理者が分離できます。SVM をアプリケーション専用にしておくと、権限の委譲が可能になり、リソース消費を制限するためのベストプラクティスを適用できます。

SVM の管理には、いくつかのオプションを使用できます。

- バックエンド構成でクラスタ管理インターフェイスを適切なクレデンシャルとともに指定し、SVM 名を指定します。
- ONTAP System Manager または CLI を使用して、SVM 専用の管理インターフェイスを作成します。
- NFS データインターフェイスで管理ロールを共有します。

いずれの場合も、インターフェイスは DNS にあり、Trident の設定時には DNS 名を使用する必要があります。これにより、ネットワーク ID を保持しなくても SVM-DR などの一部の DR シナリオが簡単になります。

専用の管理 LIF または共有の管理 LIF を SVM に使用する方法は推奨されませんが、ネットワークセキュリティポリシーを選択した方法と一致させる必要があります。最大の柔軟性を確保するには、どのような場合でも DNS 経由で管理 LIF にアクセスできるようにします **"SVM-DR"** Trident と組み合わせて使用できます。

## 最大ボリューム数を制限します

ONTAP ストレージシステムの最大ボリューム数は、ソフトウェアのバージョンとハードウェアプラットフォームによって異なります。を参照してください **"NetApp Hardware Universe の略"** 具体的な制限については、使用しているプラットフォームと ONTAP のバージョンに対応しています。ボリューム数を使い果たした場合、Trident のプロビジョニング処理だけでなく、すべてのストレージ要求に対してプロビジョニング処理が失敗します。

Trident `ontap-nas` および `ontap-san` ドライバによって、作成された各 Kubernetes Persistent Volume (PV ; 永続ボリューム) 用の FlexVol がプロビジョニングされます。。`ontap-nas-economy` ドライバは、200 PVS ごとに約 1 つの FlexVol を作成します (50~300 で構成可能)。。`ontap-san-economy` ドライバは、PVS 100 個につき FlexVol を約 1 つ作成します (50~200 の間で設定可能)。Trident がストレージシステム上の使用可能なボリュームをすべて消費しないようにするには、SVM に制限を設定する必要があります。コマンドラインから実行できます。

```
vserver modify -vserver <svm_name> -max-volumes <num_of_volumes>
```

の値 `max-volumes` 環境に固有のいくつかの条件によって異なります。

- ONTAP クラスタ内の既存のボリュームの数
- 他のアプリケーション用に Trident 外部でプロビジョニングするボリュームの数
- Kubernetes アプリケーションで消費されると予想される永続ボリュームの数

。 `max-volumes` 値は、ONTAP クラスタ内のすべてのノードでプロビジョニングされているボリュームの合計であり、個々の ONTAP ノードではプロビジョニングされていません。その結果、ONTAP クラスタノード

の Trident でプロビジョニングされたボリュームの数が、別のノードよりもはるかに多い、または少ない場合があります。

たとえば、2 ノードの ONTAP クラスタでは、最大 2、000 個の FlexVol をホストできます。最大ボリューム数を 1250 に設定していると、非常に妥当な結果が得られます。ただし、のみの場合 **"アグリゲート"** あるノードから SVM に割り当てられている場合や、あるノードから割り当てられたアグリゲートをプロビジョニングできない場合（容量など）は、他のノードが Trident でプロビジョニングされたすべてのボリュームのターゲットになります。つまり、そのノードがボリューム数の上限に達するまでの可能性があります `max-volumes` の値に達したため、そのノードを使用する Trident と他のボリューム処理の両方に影響が生じます。\* クラスタ内の各ノードのアグリゲートを、Trident が使用する SVM に同じ番号で確実に割り当てることで、この状況を回避できます。\*

## Trident で作成できるボリュームの最大サイズを制限

Trident で作成できるボリュームの最大サイズを設定するには、を使用します `limitVolumeSize` のパラメータ `backend.json` 定義（Definition）：

ストレージレイでボリュームサイズを制御するだけでなく、Kubernetes の機能も利用する必要があります。

## 双方向 CHAP を使用するように Trident を設定します

バックエンド定義で CHAP イニシエータとターゲットのユーザ名とパスワードを指定し、Trident を使用して SVM で CHAP を有効にすることができます。を使用する `useCHAP` バックエンド構成のパラメータである Trident は、CHAP を使用して ONTAP バックエンドの iSCSI 接続を認証します。双方向 CHAP のサポートは Trident 20.04 以降で利用できます。

## SVM QoS ポリシーを作成して使用します

SVM に適用された ONTAP QoS ポリシーを使用すると、Trident でプロビジョニングされたボリュームが使用できる IOPS の数が制限されます。これはに役立ちます **"Bully を防止します"** Trident SVM 外のワークロードに影響を及ぼす、制御不能なコンテナ。

SVM の QoS ポリシーはいくつかの手順で作成します。正確な情報については、ご使用の ONTAP バージョンのマニュアルを参照してください。次の例は、SVM で使用可能な合計 IOPS を 5000 に制限する QoS ポリシーを作成します。

```
# create the policy group for the SVM
qos policy-group create -policy-group <policy_name> -vserver <svm_name>
-max-throughput 5000iops

# assign the policy group to the SVM, note this will not work
# if volumes or files in the SVM have existing QoS policies
vserver modify -vserver <svm_name> -qos-policy-group <policy_name>
```

また、使用しているバージョンの ONTAP でサポートされている場合は、最小 QoS を使用してコンテナ化されたワークロードへのスループットを保証することもできます。アダプティブ QoS は SVM レベルのポリシーには対応していません。

コンテナ化されたワークロード専用の IOPS は、さまざまな要素によって異なります。その中には、次のよう

なものがあります。

- ストレージレイを使用するその他のワークロード。Kubernetes 環境とは関係なく、ストレージリソースを利用するほかのワークロードがある場合は、それらのワークロードが誤って影響を受けないように注意する必要があります。
- 想定されるワークロードはコンテナで実行されます。IOPS 要件が高いワークロードをコンテナで実行する場合は、QoS ポリシーの値が低いとエクスペリエンスが低下します。

SVM レベルで割り当てた QoS ポリシーを使用すると、SVM にプロビジョニングされたすべてのボリュームで同じ IOPS プールが共有されることに注意してください。コンテナ化されたアプリケーションの 1 つまたは少数のみに高い IOPS が必要な場合、コンテナ化された他のワークロードに対する Bully になる可能性があります。その場合は、外部の自動化を使用したボリュームごとの QoS ポリシーの割り当てを検討してください。



ONTAP バージョン 9.8 より前の場合は、QoS ポリシーグループを SVM \* only \* に割り当ててください。

### Trident の QoS ポリシーグループを作成

Quality of Service (QoS ; サービス品質) は、競合するワークロードによって重要なワークロードのパフォーマンスが低下しないようにします。ONTAP の QoS ポリシーグループには、ボリュームに対する QoS オプションが用意されており、ユーザは 1 つ以上のワークロードに対するスループットの上限を定義できます。QoS の詳細については、を参照してください ["QoS によるスループットの保証"](#)。

QoS ポリシーグループはバックエンドまたはストレージプールに指定でき、そのプールまたはバックエンドに作成された各ボリュームに適用されます。

ONTAP には、従来型とアダプティブ型の 2 種類の QoS ポリシーグループがあります。従来のポリシーグループは、最大スループット（以降のバージョンでは最小スループット）がフラットに表示されます。アダプティブ QoS では、ワークロードのサイズの変更に合わせてスループットが自動的に調整され、TB または GB あたりの IOPS が一定に維持されます。これにより、何百何千という数のワークロードを管理する大規模な環境では大きなメリットが得られます。

QoS ポリシーグループを作成するときは、次の点に注意してください。

- を設定する必要があります qosPolicy キーを押します defaults バックエンド構成のブロック。次のバックエンド設定例を参照してください。

```
{
  "version": 1,
  "storageDriverName": "ontap-nas",
  "managementLIF": "0.0.0.0",
  "dataLIF": "0.0.0.0",
  "svm": "svm0",
  "username": "user",
  "password": "pass",
  "defaults": {
    "qosPolicy": "standard-pg"
  },
  "storage": [
    {
      "labels": {"performance": "extreme"},
      "defaults": {
        "adaptiveQosPolicy": "extremely-adaptive-pg"
      }
    },
    {
      "labels": {"performance": "premium"},
      "defaults": {
        "qosPolicy": "premium-pg"
      }
    }
  ]
}
```

- ボリュームごとにポリシーグループを適用して、各ボリュームがポリシーグループの指定に従ってスループット全体を取得するようにします。共有ポリシーグループはサポートされません。

QoS ポリシーグループの詳細については、を参照してください ["ONTAP 9.8 QoS コマンド"](#)。

## ストレージリソースへのアクセスを **Kubernetes** クラスタメンバーに制限する

Trident によって作成される NFS ボリュームと iSCSI LUN へのアクセスを制限することは、Kubernetes 環境のセキュリティ体制に欠かせない要素です。これにより、Kubernetes クラスタに属していないホストがボリュームにアクセスしたり、データが予期せず変更されたりすることを防止できます。

ネームスペースは Kubernetes のリソースの論理的な境界であることを理解することが重要です。ただし、同じネームスペース内のリソースは共有可能であることが前提です。重要なのは、ネームスペース間に機能がなことです。つまり、PVS はグローバルオブジェクトですが、PVC にバインドされている場合は、同じネームスペース内のポッドからのみアクセス可能です。\* 適切な場合は、名前空間を使用して分離することが重要です。\*

Kubernetes 環境でデータセキュリティを使用する場合、ほとんどの組織で最も懸念されるのは、コンテナ内のプロセスがホストにマウントされたストレージにアクセスできることです。コンテナ用ではないためです。 ["ネームスペース"](#) この種の妥協を防ぐように設計されています。ただし、特権コンテナという例外が 1 つあります。



権限付きコンテナは、通常よりもホストレベルの権限で実行されるコンテナです。デフォルトでは拒否されないため、を使用してこの機能を無効にしてください ["ポッドセキュリティポリシー"](#)。

Kubernetes と外部ホストの両方からアクセスが必要なボリュームでは、Trident ではなく管理者が導入した PV で、ストレージを従来の方法で管理する必要があります。これにより、Kubernetes と外部ホストの両方が切断され、ボリュームを使用していない場合にのみ、ストレージボリュームが破棄されます。また、カスタムエクスポートポリシーを適用して、Kubernetes クラスターノードおよび Kubernetes クラスターの外部にあるターゲットサーバからのアクセスを可能にすることもできます。

専用のインフラノード（OpenShift など）や、ユーザアプリケーションにスケジュールできない他のノードを導入する場合は、別々のエクスポートポリシーを使用してストレージリソースへのアクセスをさらに制限する必要があります。これには、これらのインフラノードに導入されているサービス（OpenShift Metrics サービスや Logging サービスなど）のエクスポートポリシーの作成と、非インフラノードに導入されている標準アプリケーションの作成が含まれます。

専用のエクスポートポリシーを使用します

Kubernetes クラスター内のノードへのアクセスのみを許可するエクスポートポリシーが各バックエンドに存在することを確認する必要があります。Trident では、20.04 リリース以降、エクスポートポリシーを自動的に作成、管理できます。これにより、Trident はプロビジョニング対象のボリュームへのアクセスを Kubernetes クラスター内のノードに制限し、ノードの追加や削除を簡易化します。

また、エクスポートポリシーを手動で作成し、各ノードのアクセス要求を処理する 1 つ以上のエクスポートルールを設定することもできます。

- を使用します `vserver export-policy create` ONTAP の CLI コマンドを使用してエクスポートポリシーを作成します。
- を使用して、エクスポートポリシーにルールを追加します `vserver export-policy rule create` ONTAP CLI コマンド。

これらのコマンドを実行すると、データにアクセスできる Kubernetes ノードを制限できます。

無効にします `showmount` アプリケーション **SVM** 用

。 `showmount` 機能を使用すると、NFS クライアントが SVM を照会して、使用可能な NFS エクスポートのリストを表示できます。Kubernetes クラスターに導入されたポッドは、問題 に対応しています `showmount -e` コマンドをデータ LIF に対して実行し、アクセス権のないマウントも含めて使用可能なマウントのリストを取得します。これだけではセキュリティ上の妥協ではありませんが、権限のないユーザが NFS エクスポートに接続するのを阻止する可能性のある不要な情報が提供されます。

を無効にする必要があります `showmount` SVM レベルの ONTAP CLI コマンドを使用して、次の作業を行います。

```
vserver nfs modify -vserver <svm_name> -showmount disabled
```

## SolidFire のベストプラクティス

Trident に SolidFire ストレージを設定するためのベストプラクティスをご確認ください。



## SolidFire アカウントを作成します

各 SolidFire アカウントは固有のボリューム所有者で、Challenge Handshake Authentication Protocol（CHAP；チャレンジハンドシェイク認証プロトコル）クレデンシャルのセットを受け取ります。アカウントに割り当てられたボリュームには、アカウント名とその CHAP クレデンシャルを使用してアクセスするか、ボリュームアクセスグループを通じてアクセスできます。アカウントには最大 2、000 個のボリュームを関連付けることができますが、1 つのボリュームが属することのできるアカウントは 1 つだけです。

## QoS ポリシーを作成する

標準的なサービス品質設定を作成して保存し、複数のボリュームに適用する場合は、SolidFire のサービス品質（QoS）ポリシーを使用します。

QoS パラメータはボリューム単位で設定できます。QoS を定義する 3 つの設定可能なパラメータである Min IOPS、Max IOPS、Burst IOPS を設定することで、各ボリュームのパフォーマンスが保証されます。

4KB のブロックサイズの最小 IOPS、最大 IOPS、バースト IOPS の値を次に示します。

IOPS パラメータ	定義（Definition）	最小価値	デフォルト値	最大値（4KB）
最小 IOPS	ボリュームに対して保証されたレベルのパフォーマンス。	50 です	50 です	15、000
最大 IOPS	パフォーマンスはこの制限を超えません。	50 です	15、000	20 万
バースト IOPS	短時間のバースト時に許容される最大 IOPS。	50 です	15、000	20 万



Max IOPS と Burst IOPS は最大 200、000 に設定できますが、実際のボリュームの最大パフォーマンスは、クラスタの使用量とノードごとのパフォーマンスによって制限されます。

ブロックサイズと帯域幅は、IOPS に直接影響します。ブロックサイズが大きくなると、システムはそのブロックサイズを処理するために必要なレベルまで帯域幅を増やします。帯域幅が増えると、システムが処理可能な IOPS は減少します。を参照してください ["SolidFire のサービス品質"](#) QoS およびパフォーマンスの詳細については、を参照してください。

## SolidFire 認証

Element では、認証方法として CHAP とボリュームアクセスグループ（VAG）の 2 つがサポートされています。CHAP は CHAP プロトコルを使用して、バックエンドへのホストの認証を行います。ボリュームアクセスグループは、プロビジョニングするボリュームへのアクセスを制御します。CHAP はシンプルで拡張性に制限がないため、認証に使用することを推奨します。



Trident と強化された CSI プロビジョニングツールは、CHAP 認証の使用をサポートします。VAG は、従来の CSI 以外の動作モードでのみ使用する必要があります。

CHAP 認証（イニシエータが対象のボリュームユーザであることの確認）は、アカウントベースのアクセス制御でのみサポートされます。認証に CHAP を使用している場合は、単方向 CHAP と双方向 CHAP の 2 つのオプションがあります。単方向 CHAP は、SolidFire アカウント名とイニシエータシークレットを使用してボリュームアクセスを認証します。双方向の CHAP オプションを使用すると、ボリュームがアカウント名とイニシエータシークレットを使用してホストを認証し、ホストがアカウント名とターゲットシークレットを使用してボリュームを認証するため、ボリュームを最も安全に認証できます。

ただし、CHAP を有効にできず VAG が必要な場合は、アクセスグループを作成し、ホストのイニシエータとボリュームをアクセスグループに追加します。アクセスグループに追加した各 IQN は、CHAP 認証の有無に関係なく、グループ内の各ボリュームにアクセスできます。iSCSI イニシエータが CHAP 認証を使用するように設定されている場合は、アカウントベースのアクセス制御が使用されます。iSCSI イニシエータが CHAP 認証を使用するように設定されていない場合は、ボリュームアクセスグループのアクセス制御が使用されます。

## 詳細情報の入手方法

ベストプラクティスのドキュメントの一部を以下に示します。を検索します ["NetApp ライブラリ"](#) 最新バージョンの場合。

- ONTAP \*
- ["NFS Best Practice and Implementation Guide"](#)
- ["SAN アドミニストレーションガイド"](#)（iSCSI の場合）
- ["RHEL 向けの iSCSI のクイック構成"](#)
- Element ソフトウェア \*
- ["SolidFire for Linux を設定しています"](#)
- NetApp HCI \*
- ["NetApp HCI 導入の前提条件"](#)
- ["NetApp Deployment Engine にアクセスします"](#)
- アプリケーションのベストプラクティス情報 \*
- ["ONTAP での MySQL に関するベストプラクティスです"](#)
- ["SolidFire での MySQL に関するベストプラクティスです"](#)
- ["NetApp SolidFire および Cassandra"](#)
- ["SolidFire での Oracle のベストプラクティス"](#)
- ["SolidFire での PostgreSQL のベストプラクティスです"](#)

すべてのアプリケーションに具体的なガイドラインがあるわけではありません。そのためには、ネットアップのチームと協力し、を使用することが重要です ["NetApp ライブラリ"](#) 最新のドキュメントを検索できます。

## Astra Trident を統合

Astra Trident を統合するには、設計とアーキテクチャに関する次の要素を統合する必要があります。ドライバの選択と導入、ストレージクラス的设计、仮想ストレージプールの設計、永続的ボリューム要求（PVC）は、Astra Trident を使用したストレージプロビジョニング、ボリューム運用、OpenShift サービスの導入に影響を及ぼします。

## ドライバの選択と展開

ストレージシステム用のバックエンドドライバを選択して導入します。

### ONTAP バックエンドドライバ

ONTAP バックエンドドライバは、使用されるプロトコルと、ストレージシステムでのボリュームのプロビジョニング方法によって異なります。そのため、どのドライバを展開するかを決定する際には、慎重に検討する必要があります。

アプリケーションに共有ストレージを必要とするコンポーネント（同じ PVC にアクセスする複数のポッド）がある場合、NAS ベースのドライバがデフォルトで選択されますが、ブロックベースの iSCSI ドライバは非共有ストレージのニーズを満たします。アプリケーションの要件と、ストレージチームとインフラチームの快適さレベルに基づいてプロトコルを選択してください。一般的に、ほとんどのアプリケーションでは両者の違いはほとんどないため、共有ストレージ（複数のポッドで同時にアクセスする必要がある場合）が必要かどうかに基づいて判断することがよくあります。

使用可能なONTAP バックエンドドライバは次のとおりです。

- `ontap-nas`：プロビジョニングされた各PVは、ONTAP のフルFlexVolです。
- `ontap-nas-economy`：PVがプロビジョニングされた各ボリュームはqtreeであり、FlexVolあたりのqtree数は設定可能です（デフォルトは200）。
- `ontap-nas-flexgroup`：すべてのONTAP FlexGroup としてプロビジョニングされたPVごとに、SVM に割り当てられたすべてのアグリゲートが使用されます。
- `ontap-san`：プロビジョニングされた各PVは、固有のFlexVol内のLUNです。
- `ontap-san-economy`：プロビジョニングされた各PVはLUNで、FlexVolあたりのLUN数は設定可能です（デフォルトは100）。

3 つの NAS ドライバの間で選択すると、アプリケーションで使用できる機能にいくつかの影響があります。

次の表では、Astra Trident からすべての機能が提供されるわけではありません。一部の機能は、プロビジョニング後にストレージ管理者が適用する必要があります。上付き文字の脚注は、機能やドライバごとに機能を区別します。

ONTAP NAS ドライバ	Snapshot	クローン	動的なエクスポートポリシー	マルチアタッチ	QoS	サイズ変更	レプリケーション
<code>ontap-nas</code>	はい。	はい。	○脚注：5[]	はい。	Yesfootnote: 1[]	はい。	Yesfootnote: 1[]
<code>ontap-nas-economy</code>	Yesfootnote: 3[]	Yesfootnote: 3[]	○脚注：5[]	はい。	Yesfootnote: 3[]	はい。	Yesfootnote: 3[]
<code>ontap-nas-flexgroup</code>	Yesfootnote: 1[]	いいえ	○脚注：5[]	はい。	Yesfootnote: 1[]	はい。	Yesfootnote: 1[]

Astra Trident は、ONTAP 向けに 2 つの SAN ドライバを提供しています。このドライバの機能は次のとおりです。

ONTAP SANドライバ	Snapshot	クローン	マルチアタッチ	双方向CHAP	QoS	サイズ変更	レプリケーション
ontap-san	はい。	はい。	Yesfootnote: 4[]	はい。	Yesfootnote: 1[]	はい。	Yesfootnote: 1[]
ontap-san-economy	はい。	はい。	Yesfootnote: 4[]	はい。	Yesfootnote: 3[]	はい。	Yesfootnote: 3[]

上記の表の脚注：

Yes [1]：Astra Tridentで管理されない

Yesfootnote: 2[]：Astra Tridentが管理しますが、PV Granularは管理しません

Yesfootnote: 3[]：Astra Tridentで管理されず、PV Granularでは管理されない

Yes [4]:raw-blockボリュームでサポート

Yesfootnote: 5[]：CSI Tridentによるサポート

PV に細分化されていない機能は FlexVol 全体に適用され、PVS（共有 FlexVol 内の qtree または LUN）にはすべて共通のスケジュールが適用されます。

上の表に示すように、の機能の多くはです ontap-nas および ontap-nas-economy は同じです。しかし、だからです ontap-nas-economy ドライバは、PV単位でスケジュールを制御する機能を制限します。これは、ディザスタリカバリやバックアップ計画に特に影響を与える可能性があります。ONTAP ストレージでPVCクローン機能を利用したい開発チームの場合、この方法はを使用する場合にのみ使用できます ontap-nas、ontap-san または ontap-san-economy ドライバ。



。solidfire-san また、ドライバはPVCをクローニングすることもできます。

## Cloud Volumes ONTAP バックエンドドライバ

Cloud Volumes ONTAP は、ファイル共有や NAS および SAN プロトコル（NFS、SMB / CIFS、iSCSI）を提供するブロックレベルストレージなど、さまざまなユースケースでデータ制御とエンタープライズクラスのストレージ機能を提供します。Cloud Volume ONTAP の互換性のあるドライバはです ontap-nas、ontap-nas-economy、ontap-san および ontap-san-economy。Cloud Volume ONTAP for Azure と Cloud Volume ONTAP for GCP に該当します。

## ONTAP バックエンドドライバ用のAmazon FSX

Amazon FSX for ONTAP を使用すると、お客様は使い慣れたネットアップの機能、パフォーマンス、管理機能を活用しながら、AWS にデータを格納する際のシンプルさ、即応性、セキュリティ、拡張性を活用できます。FSX for ONTAP は、ONTAP のファイルシステム機能と管理 API の多くをサポートしています。Cloud Volume ONTAP の互換性のあるドライバはです ontap-nas、ontap-nas-economy、ontap-nas-flexgroup、ontap-san および ontap-san-economy。

## NetApp HCI / SolidFire バックエンドドライバ

。solidfire-san NetApp HCI / SolidFireプラットフォームで使用されるドライバ。管理者は、QoS制限に基づいてTrident用にElementバックエンドを設定できます。Tridentでプロビジョニングされるボリュームに特定のQoS制限を設定するためにバックエンドを設計する場合は、を使用してください type バックエンドファイル内のパラメータ。また、管理者は、を使用してストレージに作成できるボリュームサイズを制限することもできます limitVolumeSize パラメータ現在のところ、ボリュームのサイズ変更やボリュームのレプリケーションなどのElementストレージ機能は、ではサポートされていません solidfire-san ドライバ。これらの処理は、Element ソフトウェアの Web UI から手動で実行する必要があります。

SolidFire ドライバ	Snapshot	クローン	マルチアタッチ	CHAP	QoS	サイズ変更	レプリケーション
solidfire-san	はい。	はい。	○脚注： 2 []	はい。	はい。	はい。	Yesfootnote: 1[]

脚注：

Yes [1]：Astra Tridentで管理されない

Yes [2]:raw-blockボリュームでサポート

## Azure NetApp Files バックエンドドライバ

Astra Tridentがを使用 azure-netapp-files を管理するドライバ "Azure NetApp Files の特長" サービス

このドライバの詳細と設定方法については、を参照してください "Azure NetApp Files 向けの Trident バックエンド構成"。

Azure NetApp Files ドライバ	Snapshot	クローン	マルチアタッチ	QoS	を展開します	レプリケーション
azure-netapp-files	はい。	はい。	はい。	はい。	はい。	Yesfootnote: 1[]

脚注：

Yes [1]：Astra Tridentで管理されない

## Cloud Volumes Service とGCPバックエンドドライバ

Astra Tridentがを使用 gcp-cvs GCPバックエンドのCloud Volumes Service とリンクするドライバ。TridentでGCPバックエンドを設定するには、を指定する必要があります projectNumber、apiRegion`および`apiKey バックエンドファイル内。プロジェクト番号は GCP Web ポータルで確認できますが、GCPでCloud Volume のAPI アクセスを設定する際に作成したサービスアカウントの秘密鍵ファイルからAPI キーを取得する必要があります。Astra Trident なら、CVS ボリュームを 2 つのうちの 1 つで作成できます "サービスタイプ"：

1. \* CVS \*：基本 CVS サービスのタイプ。パフォーマンスレベルが限定的か中程度かに関係なく、高ゾーンの可用性を実現します。

2. \* CVS - パフォーマンス \* : パフォーマンスを重視する本番環境のワークロードに最適な、パフォーマンスに最適化されたサービスタイプ。3つの独自のサービスレベルから選択できます [standard、premium、および `extreme]。

CVSとCVSパフォーマンスのボリュームの最小サイズは100GiBです。

CVS for GCPドライバ	Snapshot	クローン	マルチアタッチ	QoS	を展開します	レプリケーション
gcp-cvs	はい。	はい。	はい。	はい。	はい。	Yes <sup>footnote: 1</sup>

脚注：

Yes <sup>[1]</sup> : Astra Tridentで管理されない

。 gcp-cvs ドライバは仮想ストレージプールを使用します。仮想ストレージプールはバックエンドを抽象化し、Astra Trident がボリュームの配置を決定できるようにします。管理者が backend.json ファイルに仮想ストレージプールを定義します。ストレージクラスは、ラベルを使用する仮想ストレージプールを識別します。

## ストレージクラスの設計

Kubernetes ストレージクラスオブジェクトを作成するには、個々のストレージクラスを設定して適用する必要があります。このセクションでは、アプリケーション用のストレージクラスの設計方法について説明します。

### 特定のバックエンド使用率

フィルタリングは、特定のストレージクラスオブジェクト内で使用でき、そのストレージクラスで使用するストレージプールまたはプールのセットを決定します。ストレージクラスでは、次の3セットのフィルタを設定できます。 storagePools、 additionalStoragePools、または `excludeStoragePools。

。 storagePools パラメータを指定すると、指定した属性に一致するプールのセットだけにストレージが制限されます。。 additionalStoragePools パラメータは、属性とで選択されたプールのセットに加えて、Astra Tridentがプロビジョニングに使用する一連のプールを拡張するために使用されます storagePools パラメータどちらか一方のパラメータを単独で使用することも、両方を使用して、適切なストレージプールセットが選択されていることを確認することもできます。

。 excludeStoragePools パラメータを使用すると、属性に一致する一連のプールが具体的に除外されます。

### QoSポリシーをエミュレートします

ストレージクラスを設計してQoSポリシーをエミュレートする場合は、でストレージクラスを作成します media 属性の形式 hdd または ssd。に基づきます media ストレージクラスで説明されている属性の中から、Tridentが提供する適切なバックエンドを選択します hdd または ssd media属性に一致するアグリゲートを作成し、ボリュームのプロビジョニングを特定のアグリゲートに転送します。そこで、Premiumストレージクラスを作成します media 属性をとして設定します ssd Premium QoSポリシーに分類できます。メディア属性を「hdd」に設定し、標準のQoSポリシーとして分類できる、別のストレージクラス標準を作成できます。また、ストレージクラスの「IOPS」属性を使用して、QoSポリシーとして定義できる Element アプライアンスにプロビジョニングをリダイレクトすることもできます。



特定の機能に基づいてバックエンドを利用する

ストレージクラスは、シンプロビジョニングとシックプロビジョニング、Snapshot、クローン、暗号化などの機能が有効になっている特定のバックエンドでボリュームを直接プロビジョニングするように設計できます。使用するストレージを指定するには、必要な機能を有効にしてバックエンドに適したストレージクラスを作成します。

## 仮想ストレージプール

Virtual Storage Pool は、すべての Astra Trident バックエンドで利用可能 Trident が提供する任意のドライバを使用して、任意のバックエンドに対して仮想ストレージプールを定義できます。

仮想ストレージプールを使用すると、管理者はストレージクラスで参照可能なバックエンド経由で抽象化レベルを作成して、バックエンドにボリュームを柔軟かつ効率的に配置できます。同じサービスクラスを使用して異なるバックエンドを定義できます。さらに、同じバックエンドに異なる特性を持つ複数のストレージプールを作成することもできます。セレクトラで特定のラベルを設定したストレージクラスがある場合、Astra Trident は、ボリュームを配置するすべてのセレクトララベルに一致するバックエンドを選択します。ストレージクラスセレクトラのラベルが複数のストレージプールに一致する場合、Astra Trident がボリュームのプロビジョニングに使用するストレージクラスを 1 つ選択します。

## 仮想ストレージプールの設計

バックエンドの作成時に、一般に一連のパラメータを指定できます。管理者が、同じストレージクレデンシャルと異なるパラメータセットを使用して別のバックエンドを作成することはできませんでした。この問題は、仮想ストレージプールの導入に伴って、軽減されています。仮想ストレージプールは、バックエンドと Kubernetes ストレージクラスの間に抽象化されたレベルです。管理者は、Kubernetes ストレージクラスを介してパラメータとラベルを定義でき、セレクトラとしてバックエンドに依存しない方法で参照できます。Virtual Storage Pools は、サポート対象のすべてのネットアップバックエンドに Astra Trident を使用して定義できます。リストには、SolidFire / NetApp HCI、ONTAP、GCP 上の Cloud Volumes Service、Azure NetApp Files が含まれます。



仮想ストレージプールを定義する場合は、バックエンド定義内の既存の仮想プールの順序を変更しないことを推奨します。また、既存の仮想プールの属性を編集または変更したり、新しい仮想プールを定義したりしないことを推奨します。

## さまざまなサービスレベル/QoSのエミュレート

サービスクラスをエミュレートするための仮想ストレージプールを設計することができます。Cloud Volume Service for Azure NetApp Files の仮想プール実装を使用して、さまざまなサービスクラスをセットアップする方法を見ていきましょう。さまざまなパフォーマンスレベルを表す複数のラベルで ANF バックエンドを設定します。設定 servicelevel 適切なパフォーマンスレベルを考慮し、各ラベルの下にその他の必要な側面を追加します。では、別の仮想ストレージプールにマッピングする別の Kubernetes ストレージクラスを作成します。を使用する parameters.selector 各ストレージクラスは、ボリュームのホストに使用できる仮想プールを呼び出します。

## 特定の一連の側面を割り当てます

特定の側面を持つ複数の仮想ストレージプールは、単一のストレージバックエンドから設計できます。そのため、バックエンドに複数のラベルを設定し、各ラベルに必要な側面を設定します。を使用して、さまざまな Kubernetes ストレージクラスを作成します parameters.selector 異なる仮想ストレージプールにマッピングされるフィールド。バックエンドでプロビジョニングされるボリュームには、選択した仮想ストレージプールに定義された設定が適用されます。



## ストレージプロビジョニングに影響する PVC 特性

要求されたストレージクラスを超えたパラメータの一部は、PVC の作成時に Astra Trident のプロビジョニング決定プロセスに影響を与える可能性があります。

### アクセスモード

PVC 経由でストレージを要求する場合、必須フィールドの 1 つがアクセスモードです。必要なモードは、ストレージ要求をホストするために選択されたバックエンドに影響を与える可能性があります。

Astra Trident は、次のマトリックスで指定されたアクセス方法で使用されているストレージプロトコルと一致するかどうかを試みます。これは、基盤となるストレージプラットフォームに依存しません。

	ReadWriteOnce コマンドを使用します	ReadOnlyMany	ReadWriteMany
iSCSI	はい。	はい。	○ (Raw ブロック)
NFS	はい。	はい。	はい。

NFS バックエンドが設定されていない Trident 環境に送信された ReadWriteMany PVC が要求された場合、ボリュームはプロビジョニングされません。このため、リクエストは、アプリケーションに適したアクセスモードを使用する必要があります。

## ボリューム操作

### 永続ボリュームの変更

永続ボリュームとは、Kubernetes で変更不可のオブジェクトを 2 つだけ除いてです。再利用ポリシーとサイズは、いったん作成されると変更できます。ただし、これにより、ボリュームの一部の側面が Kubernetes 以外で変更されることが防止されるわけではありません。特定のアプリケーション用にボリュームをカスタマイズしたり、誤って容量が消費されないようにしたり、何らかの理由でボリュームを別のストレージコントローラに移動したりする場合に便利です。



Kubernetes のツリー内プロビジョニングツールは、現時点では NFS または iSCSI PVS のボリュームサイズ変更処理をサポートしていません。Astra Trident では、NFS ボリュームと iSCSI ボリュームの両方の拡張がサポートされています。

作成後に PV の接続の詳細を変更することはできません。

### オンデマンドのボリューム **Snapshot** を作成

Astra Trident は、CSI フレームワークを使用して、オンデマンドでボリュームスナップショットを作成し、スナップショットから PVC を作成できます。Snapshot は、データのポイントインタイムコピーを管理し、Kubernetes のソース PV とは無関係にライフサイクルを管理する便利な方法です。これらの Snapshot を使用して、PVC をクローニングできます。

### **Snapshot** からボリュームを作成します

Astra Trident は、ボリューム Snapshot からの PersistentVolumes の作成もサポートしています。これを実現するには、PersistentVolumeClaimを作成し、を指定します datasource ボリュームの作成元となる必要がある Snapshot。Astra Trident がこの PVC を処理するには、Snapshot にデータが存在するボリュームを作成します。この機能を使用すると、複数のリージョン間でデータを複製したり、テスト環境を作成したり、破損し

た本番ボリューム全体を交換したり、特定のファイルとディレクトリを取得して別の接続ボリュームに転送したりできます。

## クラスタ内でボリュームを移動します

ストレージ管理者は、ONTAP クラスタ内のアグリゲート間およびコントローラ間で、ストレージ利用者への無停止でボリュームを移動できます。この処理は、デスティネーションアグリゲートが Trident が使用している SVM からアクセス可能なアグリゲートであるかぎり、Astra Trident または Kubernetes クラスタには影響しません。この点が重要なのは、アグリゲートが SVM に新たに追加された場合、Astra Trident に再追加してバックエンドを更新する必要があることです。これにより、Astra Trident が SVM のインベントリを再作成し、新しいアグリゲートが認識されるようになります。

ただし、バックエンド間でのボリュームの移動は Astra Trident では自動ではサポートされていません。これには、同じクラスタ内の SVM 間、クラスタ間、または別のストレージプラットフォーム上の SVM 間が含まれます（たとえストレージシステムが Trident から Astra に接続されている場合でも）。

ボリュームが別の場所にコピーされた場合、ボリュームインポート機能を使用して現在のボリュームを Astra Trident にインポートできます。

## ボリュームを展開します

Astra Trident は、NFS と iSCSI PVS のサイズ変更をサポートしています。これにより、ユーザは Kubernetes レイヤを介してボリュームのサイズを直接変更できます。ボリュームを拡張できるのは、ONTAP、SolidFire / NetApp HCI、Cloud Volumes Service バックエンドなど、主要なすべてのネットアップストレージプラットフォームです。あとで拡張できるようにするには、をに設定します `allowVolumeExpansion` 終了: `true` ボリュームに関連付けられているストレージクラス内のストレージクラス。永続ボリュームのサイズを変更する必要がある場合は、を編集します `spec.resources.requests.storage Persistent Volume Claim` のアノテーションを、必要なボリュームサイズに設定します。Tridentによって、ストレージクラス上のボリュームのサイズが自動的に変更されます。

## 既存のボリュームを **Kubernetes** にインポートする

Volume Import では、既存のストレージボリュームを Kubernetes 環境にインポートできます。これは現在、でサポートされています `ontap-nas`、`ontap-nas-flexgroup`、`solidfire-san`、`azure-netapp-files` および `gcp-cvs` ドライバ。この機能は、既存のアプリケーションを Kubernetes に移植する場合や、ディザスタリカバリシナリオで使用する場合に便利です。

ONTAP およびを使用する場合 `solidfire-san` ドライバの場合は、コマンドを使用します `tridentctl import volume <backend-name> <volume-name> -f /path/pvc.yaml` 既存のボリュームを Kubernetes にインポートして Astra Trident で管理 `import volume` コマンドで使った PVC YAML または JSON ファイルは、Astra Trident をプロビジョニングツールとして識別するストレージクラスを指定します。NetApp HCI / SolidFire バックエンドを使用する場合は、ボリューム名が一意であることを確認してください。ボリューム名が重複している場合は、ボリュームインポート機能で区別できるように、ボリュームを一意の名前にクローニングします。

状況に応じて `azure-netapp-files` または `gcp-cvs` ドライバを使用する場合は、コマンドを使用します `tridentctl import volume <backend-name> <volume path> -f /path/pvc.yaml` から Kubernetes にボリュームをインポートして Astra Trident で管理。これにより、ボリューム参照が一意になります。

上記のコマンドを実行すると、Astra Trident がバックエンド上にボリュームを検出し、サイズを確認します。設定された PVC のボリュームサイズが自動的に追加（必要に応じて上書き）されます。次に Astra Trident が新しい PV を作成し、Kubernetes が PVC を PV にバインド

特定のインポートされた PVC を必要とするようにコンテナを導入した場合、ボリュームインポートプロセスによって PVC/PV ペアがバインドされるまで、コンテナは保留状態のままになります。PVC/PV ペアがバインドされると、他に問題がなければコンテナが起動します。

## OpenShift サービスを導入します

OpenShift の付加価値クラスタサービスは、クラスタ管理者とホストされているアプリケーションに重要な機能を提供します。これらのサービスが使用するストレージはノードローカルリソースを使用してプロビジョニングできますが、これにより、サービスの容量、パフォーマンス、リカバリ性、持続可能性が制限されることがよくあります。エンタープライズストレージアレイを活用してこれらのサービスに容量を提供することで、劇的に向上したサービスを実現できます。ただし、すべてのアプリケーションと同様に、OpenShift とストレージ管理者は、緊密に連携してそれぞれに最適なオプションを決定する必要があります。Red Hat のドキュメントは、要件を決定し、サイジングとパフォーマンスのニーズを確実に満たすために大きく活用する必要があります。

### レジストリサービス

レジストリのストレージの導入と管理については、に記載されています ["netapp.io のコマンドです"](#) を参照してください ["ブログ"](#)。

### ロギングサービス

他の OpenShift サービスと同様に、ログ記録サービスは、Ansible と、インベントリファイル（別名）で提供される構成パラメータを使用して導入されますホスト。プレイブックに含まれています。インストール方法には、OpenShiftの初期インストール時にログを導入する方法と、OpenShiftが終了した後にログを導入する方法の2つがあります。  
インストール済み。



Red Hat OpenShift バージョン 3.9 以降、データ破損に関する懸念があるため、記録サービスに NFS を使用しないことを公式のドキュメントで推奨しています。これは、Red Hat 製品のテストに基づいています。ONTAP の NFS サーバにはこのような問題はなく、簡単にロギング環境をバックアップできます。ロギングサービスには最終的にどちらかのプロトコルを選択する必要がありますが、両方のプロトコルがネットアッププラットフォームを使用する場合に適していることと、NFS を使用する理由がないことを確認してください。

ロギングサービスでNFSを使用する場合は、Ansible変数を設定する必要があります

`openshift_enable_unsupported_configurations` 終了: `true` インストーラが失敗しないようにします。

はじめに

ロギングサービスは、必要に応じて、両方のアプリケーションに導入することも、OpenShift クラスタ自体のコア動作に導入することもできます。操作ログを配置する場合は、変数を指定します

`openshift_logging_use_ops` として `'true'` サービスのインスタンスが2つ作成されます。操作のロギングインスタンスを制御する変数には「ops」が含まれ、アプリケーションのインスタンスには含まれません。

導入方法に基づいて Ansible 変数を設定することは、基盤のサービスが正しいストレージを利用できるようにするために重要です。各導入方法のオプションを見てみましょう。



以下の表には、ロギングサービスに関連するストレージ構成に関連する変数のみが含まれています。その他のオプションは、で確認できます ["Red Hat OpenShift のロギングに関するドキュメント"](#) 導入環境に応じて、確認、設定、使用する必要があります。

次の表の変数では、入力した詳細を使用してロギングサービスの PV と PVC を作成する Ansible プレイブックが作成されます。この方法は、OpenShift インストール後にコンポーネントインストールプレイブックを使用するよりもはるかに柔軟性に劣るが、既存のボリュームがある場合はオプションとなります。

変数（ <b>Variable</b> ）	詳細
openshift_logging_storage_kind	をに設定します nfs ログ記録サービス用のNFS PVを作成するため。
openshift_logging_storage_host	NFS ホストのホスト名または IP アドレス。仮想マシンのデータ LIF に設定してください。
openshift_logging_storage_nfs_directory	NFS エクスポートのマウントパス。たとえば、ボリュームがとしてジャンクションされている場合などで <code>/openshift_logging`</code> この変数には、このパスを使用します。
openshift_logging_storage_volume_name	名前。例 <code>`pv_ose_logs`</code> 作成するPVの。
openshift_logging_storage_volume_size	たとえば、NFSエクスポートのサイズ 100Gi。

OpenShift クラスタがすでに実行中で、そのため Trident を導入して設定した場合、インストーラは動的プロビジョニングを使用してボリュームを作成できます。次の変数を設定する必要があります。

変数（ <b>Variable</b> ）	詳細
openshift_logging_es_pvc_dynamic	動的にプロビジョニングされたボリュームを使用する場合は true に設定します。
openshift_logging_es_pvc_storage_class_name	PVC で使用されるストレージクラスの名前。
openshift_logging_es_pvc_size	PVC で要求されたボリュームのサイズ。
openshift_logging_es_pvc_prefix	ロギングサービスで使用する PVC のプレフィックス。
openshift_logging_es_ops_pvc_dynamic	をに設定します true 動的にプロビジョニングされたボリュームをopsロギングインスタンスに使用する。
openshift_logging_es_ops_pvc_storage_class_name	処理ロギングインスタンスのストレージクラスの名前。
openshift_logging_es_ops_pvc_size	処理インスタンスのボリューム要求のサイズ。
openshift_logging_es_ops_pvc_prefix	ops インスタンス PVC のプレフィックス。

ロギングスタックを導入します

初期の OpenShift インストールプロセスの一部としてロギングを導入する場合、標準の導入プロセスに従うだけで済みます。Ansible は、必要なサービスと OpenShift オブジェクトを構成および導入して、Ansible が完了したらすぐにサービスを利用できるようにします。

ただし、最初のインストール後に導入する場合は、コンポーネントプレイブックを Ansible で使用する必要があります。このプロセスは、OpenShift のバージョンが異なるためわずかに変更される場合があるので、必ず読んで従うようにしてください ["Red Hat OpenShift Container Platform 3.11 のドキュメント"](#) 使用しているバージョンに対応した

## 指標サービス

この指標サービスは、OpenShift クラスタのステータス、リソース利用率、可用性に関する重要な情報を管理者に提供します。ポッドの自動拡張機能にも必要であり、多くの組織では、チャージバックやショーバックのアプリケーションに指標サービスのデータを使用しています。

ロギングサービスや OpenShift 全体と同様に、Ansible を使用して指標サービスを導入します。また、ロギングサービスと同様に、メトリックサービスは、クラスタの初期セットアップ時またはコンポーネントのインストール方法を使用して運用可能になった後に導入できます。次の表に、指標サービスに永続的ストレージを設定する際に重要となる変数を示します。



以下の表には、指標サービスに関連するストレージ構成に関連する変数のみが含まれています。このドキュメントには、他にも導入環境に応じて確認、設定、使用できるオプションが多数あります。

変数 ( <b>Variable</b> )	詳細
<code>openshift_metrics_storage_kind</code>	をに設定します <code>nfs</code> ログ記録サービス用の NFS PV を作成するため。
<code>openshift_metrics_storage_host</code>	NFS ホストのホスト名または IP アドレス。これは SVM のデータ LIF に設定されている必要があります。
<code>openshift_metrics_storage_nfs_directory</code>	NFS エクスポートのマウントパス。たとえば、ボリュームがとしてジャンクションされている場合などで <code>/openshift_metrics</code> この変数には、このパスを使用します。
<code>openshift_metrics_storage_volume_name</code>	名前、 例： <code>'pv_ose_metrics'</code> 作成する PV の。
<code>openshift_metrics_storage_volume_size</code>	たとえば、NFS エクスポートのサイズ 100Gi。

OpenShift クラスタがすでに実行中で、そのため Trident を導入して設定した場合、インストーラは動的プロビジョニングを使用してボリュームを作成できます。次の変数を設定する必要があります。

変数 ( <b>Variable</b> )	詳細
<code>openshift_metrics_cassandra_pvc_prefix</code>	メトリック PVC に使用するプレフィックス。
<code>openshift_metrics_cassandra_pvc_size</code>	要求するボリュームのサイズ。
<code>openshift_metrics_cassandra_storage_type</code>	指標に使用するストレージのタイプ。適切なストレージクラスを使用して PVC を作成するには、Ansible に対してこれを <code>dynamic</code> に設定する必要があります。
<code>openshift_metrics_cassandra_pvc_storage_class_name</code>	使用するストレージクラスの名前。

### 指標サービスを導入する

ホスト / インベントリファイルに適切な Ansible 変数を定義して、Ansible でサービスを導入します。OpenShift インストール時に導入する場合は、PV が自動的に作成されて使用されます。コンポーネントプレイブックを使用して導入する場合、OpenShift のインストール後に Ansible によって必要な PVC が作成

されます。また、Trident 用のストレージをプロビジョニングしたあとにサービスを導入します。

上記の変数と導入プロセスは、OpenShift の各バージョンで変更される可能性があります。必ず見直しを行ってください ["RedHat OpenShift 導入ガイド"](#) をバージョンに合わせて設定し、環境に合わせて設定します。

## データ保護

ネットアップのストレージプラットフォームが提供するデータ保護とリカバリのオプションについて説明します。Astra Trident では、こうした機能の一部を活用できるボリュームをプロビジョニングできます。永続性に関する要件があるアプリケーションごとに、データ保護とリカバリの戦略を用意しておく必要があります。

### をバックアップします etcd クラスタデータ

Astra Tridentは、Kubernetesクラスタのメタデータを格納します etcd データベース：を定期的にバックアップしてください etcd クラスタデータは、災害発生時にKubernetesクラスタをリカバリする際に重要です。

#### 手順

1. `etcdctl snapshot save` コマンドを使用すると、のポイントインタイムスナップショットを作成できます etcd クラスタ：

```
sudo docker run --rm -v /backup:/backup \
  --network host \
  -v /etc/kubernetes/pki/etcd:/etc/kubernetes/pki/etcd \
  --env ETCDCTL_API=3 \
  registry.k8s.io/etcd-amd64:3.2.18 \
  etcdctl --endpoints=https://127.0.0.1:2379 \
  --cacert=/etc/kubernetes/pki/etcd/ca.crt \
  --cert=/etc/kubernetes/pki/etcd/healthcheck-client.crt \
  --key=/etc/kubernetes/pki/etcd/healthcheck-client.key \
  snapshot save /backup/etcd-snapshot.db
```

このコマンドは、etcdコンテナをスピンアップしてetcd Snapshotを作成し、に保存します /backup ディレクトリ。

2. 災害が発生した場合は、etcd Snapshot を使用して Kubernetes クラスタをスピンアップできます。使用します `etcdctl snapshot restore` に作成された特定のSnapshotをリストアするコマンド `/var/lib/etcd` フォルダ。リストア後、を確認します `/var/lib/etcd` フォルダに追加されました member フォルダ。次に、の例を示します `etcdctl snapshot restore` コマンドを実行します

```
etcdctl snapshot restore '/backup/etcd-snapshot-latest.db' ; mv
/default.etcd/member/ /var/lib/etcd/
```

3. Kubernetes クラスタを初期化する前に、必要な証明書をすべてコピーしておきます。
4. を使用してクラスタを作成します `--ignore-preflight-errors=DirAvailable-var-lib-etcd` フ



ラグ。

5. クラスタが起動したら、 kube-system ポッドが起動していることを確認します。
6. を使用します `kubectl get crd Trident`で作成されたカスタムリソースが存在するかどうかを確認し、 Tridentオブジェクトを取得してすべてのデータが利用可能であることを確認するコマンド。

## ONTAP スナップショットを使用して日付をリカバリします

Snapshot は、アプリケーションデータのポイントインタイムリカバリオプションを提供することで重要な役割を果たします。ただし、スナップショットは単独ではバックアップされず、ストレージシステムの障害やその他の災害に対する保護は行われません。しかし、ほとんどのシナリオで、データをすばやく簡単にリカバリできる便利な方法です。ONTAP Snapshot テクノロジーを使用してボリュームのバックアップを作成する方法とリストアする方法について説明します。

- Snapshotポリシーがバックエンドで定義されていない場合、デフォルトでが使用されます none ポリシー：そのため、 ONTAP では自動 Snapshot は作成されません。ただし、ストレージ管理者は、 ONTAP 管理インターフェイスから手動で Snapshot を作成したり、 Snapshot ポリシーを変更したりできます。これは Trident の動作には影響しません。
- デフォルトでは、 snapshot ディレクトリは表示されません。これにより、を使用してプロビジョニングしたボリュームの互換性を最大限に高めることができます `ontap-nas` および `ontap-nas-economy` ドライバ。を有効にします `.snapshot` を使用するときのディレクトリ `ontap-nas` および `ontap-nas-economy` アプリケーションがスナップショットからデータを直接リカバリできるようにするドライバ。
- を使用して、以前のSnapshotに記録されている状態にボリュームをリストアします `volume snapshot restore` ONTAP CLIコマンド。Snapshot コピーをリストアすると、既存のボリューム構成は上書きされます。Snapshot コピーの作成後にボリューム内のデータに加えた変更はすべて失われます。

```
cluster1::*> volume snapshot restore -vserver vs0 -volume vol3 -snapshot vol3_snap_archive
```

## ONTAP を使用してデータをレプリケート

データのレプリケートは、ストレージレイの障害によるデータ損失から保護する上で重要な役割を果たします。



ONTAP レプリケーションテクノロジーの詳細については、を参照してください ["ONTAP のドキュメント"](#)。

### SnapMirror Storage Virtual Machine (SVM) レプリケーション

を使用できます **"SnapMirror"** 設定とそのボリュームを含む SVM 全体をレプリケートすること。災害が発生した場合は、 SnapMirror デスティネーション SVM をアクティブ化してデータの提供を開始できます。システムがリストアされたら、プライマリに戻すことができます。

Astra Trident は、レプリケーション関係自体を構成できないため、ストレージ管理者は ONTAP の SnapMirror SVM レプリケーション機能を使用して、ボリュームをディザスタリカバリ (DR) デスティネーションに自動的にレプリケートできます。

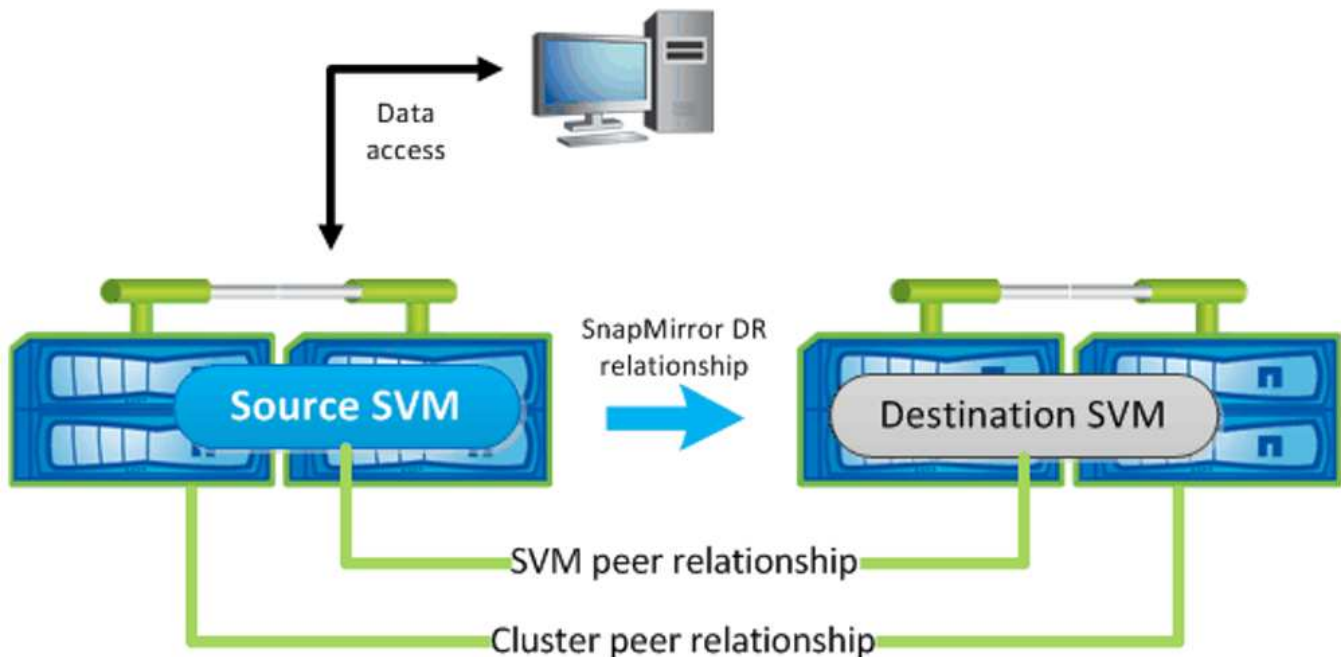
SnapMirror SVM レプリケーション機能を使用する場合や、現在この機能を使用している場合は、次の点を考慮してください。



- SVM-DR が有効になっている SVM ごとに別個のバックエンドを作成する必要があります。
- レプリケートされたバックエンドを必要な場合を除き選択しないようにストレージクラスを設定する必要があります。SVM DR をサポートするバックエンドにレプリケーション関係の保護をプロビジョニングする必要がないボリュームがある場合、この問題を回避することが重要です。
- アプリケーション管理者は、データのレプリケーションに伴う追加のコストと複雑さを理解し、リカバリプランを決定してから、データレプリケーションを利用する必要があります。
- SnapMirror デスティネーション SVM をアクティブ化する前に、スケジュールされたすべての SnapMirror 転送を停止し、実行中のすべての SnapMirror 転送を中止してレプリケーション関係を解除し、ソース SVM を停止してから、SnapMirror デスティネーション SVM を起動します。
- Astra Trident では、SVM の障害は自動では検出されない。そのため、障害が発生した場合は、管理者が実行する必要があります `tridentctl backend update` 新しいバックエンドへのTridentのフェールオーバーをトリガーするコマンド。

SVM のセットアップ手順の概要を次に示します。

- ソースクラスタとデスティネーションクラスタ間にピア関係を設定します。
- を使用してデスティネーションSVMを作成します `-subtype dp-destination` オプション
- レプリケーションジョブスケジュールを作成して、必要な間隔でレプリケーションが実行されるようにします。
- を使用して、デスティネーションSVMからソースSVMへのSnapMirrorレプリケーションを作成します `-identity-preserve true` ソースSVM構成とソースSVMインターフェイスをデスティネーションに確実にコピーするオプション。デスティネーション SVM から、 SnapMirror SVM レプリケーション関係を初期化します。



#### Trident のディザスタリカバリワークフロー

Astra Trident 19.07 以降では、Kubernetes の SSD を使用して独自の状態を保存、管理しています。Kubernetes クラスタを使用します `etcd` をクリックしてメタデータを格納します。ここで

は、Kubernetesを使用することを前提としています etcd データファイルと証明書はネットアップFlexVol に格納されています。この FlexVol は SVM にあり、 SVM の SnapMirror SVM-DR 関係はセカンダリサイトの デスティネーション SVM と一緒にあります。

災害発生時に Astra Trident を使用して、単一のマスター Kubernetes クラスタをリカバリする手順を次に示します。

1. ソース SVM で障害が発生した場合は、 SnapMirror デスティネーション SVM をアクティブ化します。そのためには、スケジュールされた SnapMirror 転送を停止し、実行中の SnapMirror 転送を中止して、レプリケーション関係を解除し、ソース SVM を停止して、デスティネーション SVM を起動します。
2. デスティネーションSVMから、Kubernetesが含まれているボリュームをマウントします etcd マスターノードとしてセットアップされるホストのデータファイルと証明書。
3. Kubernetesクラスタに関連する必要な証明書をのにすべてコピーします /etc/kubernetes/pki そして etcd member のファイル /var/lib/etcd。
4. を使用してKubernetesクラスタを作成します kubeadm init コマンドにを指定します --ignore -preflight-errors=DirAvailable-var-lib-etcd フラグ。Kubernetes ノードに使用するホスト名は、ソースの Kubernetes クラスタと同じであることが必要です。
5. を実行します kubectl get crd コマンドを使用して、すべてのTridentカスタムリソースが稼働しているかどうかを確認し、Tridentオブジェクトを取得して、すべてのデータが利用可能であることを確認します。
6. を実行して、必要なすべてのバックエンドを更新し、新しいデスティネーションSVM名を反映させます `./tridentctl update backend <backend-name> -f <backend-json-file> -n <namespace>` コマンドを実行します



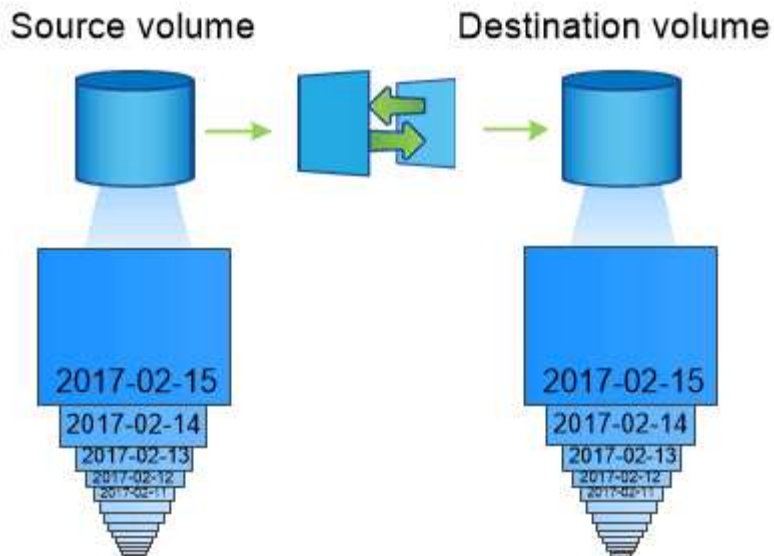
アプリケーション永続ボリュームの場合、デスティネーション SVM がアクティブ化されると、Trident によってプロビジョニングされたすべてのボリュームがデータの提供を開始します。前述の手順に従って Kubernetes クラスタをデスティネーション側でセットアップしたら、すべての導入ポッドとポッドが開始され、コンテナ化されたアプリケーションは問題なく実行されます。

## SnapMirror ボリュームのレプリケーション

ONTAP SnapMirrorボリュームレプリケーションはディザスタリカバリ機能で、ボリュームレベルのプライマリストレージからデスティネーションストレージへのフェイルオーバーを可能にします。SnapMirror は、Snapshot を同期することで、セカンダリストレージ上のプライマリストレージのボリュームレプリカまたはミラーを作成します。

ONTAP の SnapMirror ボリュームレプリケーションのセットアップ手順の概要を次に示します。

- ボリュームが配置されているクラスタとボリュームからデータを提供する SVM 間のピアリングを設定します。
- 関係の動作を制御する SnapMirror ポリシーを作成し、その関係の設定属性を指定します。
- を使用して、デスティネーションボリュームとソースボリューム間の SnapMirror 関係を作成します [snapmirror create コマンド]を押して、適切なSnapMirrorポリシーを割り当てます。
- SnapMirror 関係の作成後、ソースボリュームからデスティネーションボリュームへのベースライン転送が完了するように、関係を初期化します。



#### Trident の SnapMirror ボリュームディザスタリカバリワークフロー

Astra Trident で単一のマスター Kubernetes クラスタをリカバリする手順を次に示します。

1. 災害が発生した場合は、スケジュールされたすべての SnapMirror 転送を停止し、実行中のすべての SnapMirror 転送を中止します。デスティネーションボリュームが読み取り / 書き込み可能になるように、デスティネーションボリュームとソースボリュームの間のレプリケーション関係を解除します。
2. デスティネーションSVMから、Kubernetesが含まれているボリュームをマウントします etcd ホストに保存されるデータファイルと証明書で、マスターノードとして設定されます。
3. Kubernetesクラスタに関連する必要な証明書をのにすべてコピーします /etc/kubernetes/pki そして etcd member のファイル /var/lib/etcd。
4. を実行してKubernetesクラスタを作成します kubeadm init コマンドにを指定します --ignore -preflight-errors=DirAvailable-var-lib-etcd フラグ。ホスト名はソースの Kubernetes クラスタと同じにする必要があります。
5. を実行します kubectl get crd すべてのTridentカスタムリソースが稼働しているかどうかを確認するコマンドです。すべてのデータが利用可能かどうかを確認するためにTridentオブジェクトを取得します。
6. 前のバックエンドをクリーンアップし、Trident に新しいバックエンドを作成します。デスティネーション SVM の新しい管理 LIF とデータ LIF 、新しい SVM 名、パスワードを指定します。

#### アプリケーション永続ボリュームのディザスタリカバリワークフロー

次の手順は、災害発生時に SnapMirror デスティネーションボリュームをコンテナ化されたワークロードで使  
用できるようにする方法を示しています。

1. スケジュールされたすべての SnapMirror 転送を中止し、実行中のすべての SnapMirror 転送を中止しま  
す。デスティネーションボリュームが読み取り / 書き込み可能になるように、デスティネーションボリ  
ュームとソースボリュームの間のレプリケーション関係を解除します。ソース SVM のボリュームにバイン  
ドされた PVC を使用していた環境をクリーンアップします。
2. 前述の手順に従ってデスティネーション側で Kubernetes クラスタをセットアップしたら、Kubernetes ク  
ラスタから導入環境、PVC、PV をクリーンアップします。

3. Trident で新しい管理 LIF とデータ LIF、デスティネーション SVM の新しい SVM 名とパスワードを指定して、新しいバックエンドを作成します。
4. Trident のインポート機能を使用して、必要なボリュームを、新しい PVC にバインドされた PV としてインポートします。
5. 新しく作成した PVC を使用してアプリケーション展開を再展開します。

## Element Snapshot を使用してデータをリカバリします

ボリュームの Snapshot スケジュールを設定し、必要な間隔で Snapshot が作成されていることを確認して、Element ボリューム上のデータをバックアップします。Snapshot スケジュールは、Element UI または API を使用して設定します。現在、を使用してボリュームに Snapshot スケジュールを設定することはできません `solidfire-san` ドライバ。

データが破損した場合は、特定の Snapshot を選択し、Element UI または API を使用してボリュームを手動で Snapshot にロールバックできます。その Snapshot の作成後にボリュームに対して行われた変更はすべて元に戻ります。

## セキュリティ

ここに記載された推奨事項を参考に、Astra Tridentのインストールを安全に行ってください。

### Astra Trident を独自のネームスペースで実行

アプリケーション、アプリケーション管理者、ユーザ、および管理アプリケーションが Astra Trident オブジェクト定義またはポッドにアクセスしないようにして、信頼性の高いストレージを確保し、悪意のあるアクティビティをブロックすることが重要です。

他のアプリケーションやユーザを Astra Trident から分離するには、Astra Trident を必ず独自の Kubernetes ネームスペースにインストールしてください (`trident`)。Astra Trident を独自の名前空間に配置することで、Kubernetes 管理担当者のみが Astra Trident ポッドにアクセスでき、名前空間 CRD オブジェクトに格納されたアーティファクト（バックエンドや CHAP シークレット（該当する場合））にアクセスできるようになります。

Astra Trident のネームスペースにアクセスできるのは管理者だけであることを確認してから、にアクセスできるようにしてください `tridentctl` アプリケーション：

### ONTAP SAN バックエンドで CHAP 認証を使用します

Astra Trident は、ONTAP SAN ワークロードに対して（を使用して）CHAP ベースの認証をサポート (`ontap-san` および `ontap-san-economy` ドライバ)。ネットアップでは、ホストとストレージバックエンドの間の認証に、双方向 CHAP と Astra Trident を使用することを推奨しています。

SAN ストレージドライバを使用する ONTAP バックエンドの場合、Astra Trident は双方向 CHAP を設定し、を使用して CHAP ユーザ名とシークレットを管理できます `tridentctl`。  
を参照してください ["こちらをご覧ください"](#) ONTAP バックエンドで Trident が CHAP を構成する方法をご確認ください。



ONTAP バックエンドの CHAP サポートは Trident 20.04 以降で利用可能

## NetApp HCI および SolidFire バックエンドで CHAP 認証を使用します

ホストと NetApp HCI バックエンドと SolidFire バックエンドの間の認証を確保するために、双方向の CHAP を導入することを推奨します。Astra Trident は、テナントごとに 2 つの CHAP パスワードを含むシークレットオブジェクトを使用します。Trident を CSI プロビジョニングツールとしてインストールすると、CHAP シークレットが管理され、に格納されます `tridentvolume` 対応する PV の CR オブジェクト。PV を作成すると、CSI Astra Trident は CHAP シークレットを使用して iSCSI セッションを開始し、CHAP を介して NetApp HCI および SolidFire システムと通信します。



CSI Trident によって作成されたボリュームは、どのボリュームアクセスグループにも関連付けられていません。

CSI 以外のフロントエンドでは、ワーカーノード上のデバイスとしてのボリュームの接続は Kubernetes で処理されます。ボリュームの作成後、Astra Trident が NetApp HCI / SolidFire システムに対して API 呼び出しを実行し、テナントのシークレットがない場合はシークレットを取得します。Trident が Kubernetes にシークレットを渡します。各ノード上の kubelet は Kubernetes API を介してシークレットにアクセスし、ボリュームにアクセスする各ノードとボリュームが配置されている NetApp HCI / SolidFire システム間で CHAP を実行 / 有効化するために使用します。

## NVE および NAE で Astra Trident を使用する

NetApp ONTAP は、保管データの暗号化を提供し、ディスクが盗難、返却、転用された場合に機密データを保護します。詳細については、を参照してください ["NetApp Volume Encryption の設定の概要"](#)。

- NAE がバックエンドで有効になっている場合は、Astra Trident でプロビジョニングされたすべてのボリュームが NAE に対応します。
- NAE がバックエンドで有効になっていない場合、NVE 暗号化フラグをに設定していないかぎり、Astra Trident でプロビジョニングされたすべてのボリュームが NVE 対応になります `false` バックエンド構成

NAE 対応バックエンドの Astra Trident で作成されるボリュームは、NVE または NAE で暗号化されている必要があります。



- NVE 暗号化フラグはに設定できます `true` Trident バックエンド構成で NAE 暗号化を無効にし、ボリューム単位で特定の暗号化キーを使用します。
- NVE 暗号化フラグをに設定する `false` NAE が有効なバックエンドでは、NAE が有効なボリュームが作成されます。NAE 暗号化を無効にするには、NVE 暗号化フラグをに設定します `false`。

- 明示的に NVE 暗号化フラグをに設定することで、Astra Trident で NVE ボリュームを手動で作成できます `true`。

バックエンド構成オプションの詳細については、以下を参照してください。

- ["ONTAP の SAN 構成オプション"](#)
- ["ONTAP NAS の構成オプション"](#)



## Linux Unified Key Setup (LUKS ; 統合キーセットアップ) を使用したボリューム単位 のホスト側暗号化を有効にする

Linux Unified Key Setup (LUKS ; ユニファイドキーセットアップ) を有効にして、Astra Trident上のONTAP SANおよびONTAP SANエコノミーボリュームを暗号化できます。Astra Tridentでは、で推奨されるとおり、LUKSによって暗号化されたボリュームがAES-XTS -原64定型とモードを使用します ["NIST"](#)。

ONTAP SANのバックエンド構成オプションの詳細については、を参照してください ["ONTAP のSAN構成オプション"](#)

作業を開始する前に

- ワーカーノードにはcryptsetup 2.1以上がインストールされている必要があります。詳細については、を参照してください ["Gitlab: cryptsetup"](#)。
- パフォーマンス上の理由から、ワーカーノードでAdvanced Encryption Standard New Instructions (AES-NI) をサポートすることを推奨します。AES-NIサポートを確認するには、次のコマンドを実行します。

```
grep "aes" /proc/cpuinfo
```

何も返されない場合、お使いのプロセッサはAES-NIをサポートしていません。AES-NIの詳細については、以下を参照してください。 ["Intel : Advanced Encryption Standard Instructions \(AES-NI\) "](#)。

手順

1. バックエンド構成でLUKS暗号化属性を定義します。

```
"storage": [  
  {  
    "labels":{"luks": "true"},  
    "zone":"us_east_1a",  
    "defaults": {  
      "luksEncryption": "true"  
    }  
  },  
  {  
    "labels":{"luks": "false"},  
    "zone":"us_east_1a",  
    "defaults": {  
      "luksEncryption": "false"  
    }  
  },  
]
```

2. 使用 `parameters.selector` LUKS暗号化を使用してストレージプールを定義する方法。例：

```
apiVersion: storage.k8s.io/v1
kind: StorageClass
metadata:
  name: luks
provisioner: netapp.io/trident
parameters:
  selector: "luks=true"
  csi.storage.k8s.io/node-stage-secret-name: luks-${pvc.name}
  csi.storage.k8s.io/node-stage-secret-namespace: ${pvc.namespace}
```

### 3. LUKSパスフレーズを含むシークレットを作成します。例：

```
apiVersion: v1
kind: Secret
metadata:
  name: luks-pvc1
stringData:
  luks-passphrase-name: B
  luks-passphrase: secretB
  previous-luks-passphrase-name: A
  previous-luks-passphrase: secretA
```

#### 制限

- LUKS暗号化されたボリュームは、ONTAP 重複排除と圧縮を利用できません。
- 現時点では、LUKSパスフレーズのローテーションはサポートされていません。パスフレーズを変更するには、PVC間でデータを手動でコピーします。



## 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。