



データ保護とディザスタ リカバリ ONTAP 9

NetApp
March 04, 2026

目次

データ保護とディザスタ リカバリ	1
クラスタとSVMのピアリング	1
ONTAPクラスタとSVMピアリングについて学ぶ	1
クラスタとSVMのピアリングの準備	1
クラスタ間LIFを設定	5
ピア関係の設定	19
ピア関係でONTAPクラスタピアリング暗号化を有効にする	29
ピア関係からONTAPクラスタ ピアリング暗号化を削除する	30
ローカルSnapshotの管理	31
ローカルONTAPスナップショットの管理について学ぶ	31
ONTAP長期保存スナップショットについて学ぶ	31
カスタムSnapshotポリシーの設定	32
スナップショットを手動で管理する	36
Snapshotリザーブの管理	39
Snapshotからファイルをリストアする	43
SnapMirrorボリューム レプリケーション	50
SnapMirrorボリュームレプリケーションについて学ぶ	50
SnapMirrorボリュームレプリケーションを設定	77
SnapMirrorボリューム レプリケーションの管理	100
SnapMirror SVMレプリケーションの管理	133
ONTAP SnapMirror SVMレプリケーションについて学ぶ	133
SVMの設定のレプリケート	140
SnapMirror SVM DRデスティネーションからデータを提供する	156
SnapMirrorソースSVMを再アクティブ化する	161
ONTAP SnapMirrorボリュームDR関係をSVM DR関係に変換する	174
ONTAP SnapMirror SVMレプリケーション関係を削除する	176
SnapMirrorルート ボリューム レプリケーションの管理	178
ONTAP SnapMirrorルート ボリュームのレプリケーションについて学ぶ	178
ONTAP負荷共有ミラー関係の作成と初期化	178
ONTAP負荷共有ミラー関係を更新する	180
ONTAP負荷共有ミラーを昇格する	181
クラウドへのバックアップ	182
ONTAP SnapMirrorクラウドライセンスをインストールする	182
ONTAP SnapMirrorを使用してクラウドにデータをバックアップ	183
NetApp Backup and Recoveryを使用してデータをバックアップする	186
SnapLockテクノロジーを使用したアーカイブとコンプライアンス	190
ONTAP SnapLockについて学ぶ	190
SnapLockの設定	195
WORMファイルの管理	212

ONTAP SnapLockボリュームを移動する	228
ランサムウェア攻撃から保護するために ONTAP スナップショットをロックする	229
整合性グループ	238
ONTAPコンシステンシーグループについて学ぶ	238
ONTAP整合性グループの制限について学ぶ	244
単一のONTAPコンシステンシーグループを構成する	245
階層型ONTAPコンシステンシーグループを構成する	251
ONTAPコンシステンシーグループを保護する	255
ONTAPコンシステンシーグループのメンバーボリュームを変更する	263
ONTAPコンシステンシーグループのジオメトリを変更する	269
ONTAPコンシステンシーグループのアプリケーションとコンポーネントのタグを変更する	275
ONTAPコンシステンシーグループのクローンを作成する	276
ONTAPコンシステンシーグループを削除する	279
SnapMirrorアクティブ同期	280
はじめに	280
Plan	293
設定	303
SnapMirrorアクティブ同期の管理とデータの保護	346
トラブルシューティング	364
MetroClusterおよびSnapMirrorアクティブ同期用のONTAP Mediator	374
ONTAP Mediatorについて学ぶ	374
ONTAP Mediatorの新機能	375
インストールまたはアップグレード	382
ONTAP Mediatorの管理	426
ONTAP MediatorのホストOSを保守する	457
ONTAP System ManagerによるMetroCluster IPサイト管理について学習します	461
テープ バックアップを使用したデータ保護	462
ONTAP FlexVolボリュームのテープ バックアップについて学ぶ	462
ONTAPテープ バックアップとリストアのワークフロー	462
ONTAP SMTapeおよびダンプ バックアップ エンジンの使用例	463
テープ ドライブの管理	464
テープ ドライブについて	470
ストレージ システム間でデータを転送する	480
FlexVolのNDMP	484
ONTAP FlexGroupボリュームでのNDMPサポートについて学ぶ	508
ONTAP SnapLockボリュームを使用したNDMPについて学ぶ	508
FlexVolのノードを対象としたNDMPモードの管理	508
FlexVolのSVMを対象としたNDMPモードの管理	510
FlexVol用のダンプ エンジンについて	517
FlexVol用のSMTapeエンジンについて	529
FlexVolのテープ バックアップおよびリストア処理の監視	534

FlexVolのテープ バックアップおよびリストアに関するエラー メッセージ	538
NDMP設定	559
ONTAP NDMP構成について学ぶ	559
ONTAP NDMP 構成ワークフローについて学ぶ	560
ONTAP NDMP構成を準備する	561
ONTAP NDMPテープ デバイス接続を確認する	564
ONTAP NDMPバックアップ操作のテープ予約を有効にする	565
SVMを対象としたNDMPの設定	566
ノードを対象としたNDMPの設定	576
ONTAP NDMP 構成用のバックアップ アプリケーションを構成する	581
NetApp ElementソフトウェアとONTAPのレプリケーション - 概要	582

データ保護とディザスタ リカバリ

クラスタとSVMのピアリング

ONTAPクラスタとSVMピアリングについて学ぶ

ソースクラスタとデスティネーションクラスタ間、およびソースStorage Virtual Machine (SVM) とデスティネーションStorage Virtual Machine (SVM) 間にピア関係を作成できます。SnapMirrorを使用してSnapshotをレプリケートする前に、これらのエンティティ間にピア関係を作成する必要があります。

ONTAP 9.3では、クラスタとSVM間にピア関係を設定する方法が簡易化されています。クラスタとSVMのピアリング手順は、ONTAP 9のバージョンごとに異なります。ONTAPのバージョンに応じて、該当する手順に従ってください。

この手順は、System Managerや自動スクリプト ツールではなく、コマンドライン インターフェイス (CLI) を使用して実行します。

クラスタとSVMのピアリングの準備

ONTAPピアリングの基本

SnapMirrorを使用してスナップショットをレプリケートする前に、ソース クラスタとデスティネーション クラスタ間、およびソース SVM とデスティネーション SVM 間に_ピア関係_を作成する必要があります。ピア関係は、クラスタと SVM が安全にデータを交換できるようにするネットワーク接続を定義します。

ピア関係にあるクラスタとSVMは、_クラスタ間論理インターフェイス (LIF) _を使用してクラスタ間ネットワークを介して通信します。クラスタ間LIFは、「intercluster-core」ネットワーク・インターフェイス・サービスをサポートするLIFであり、通常は「default-intercluster」ネットワーク・インターフェイス・サービス・ポリシーを使用して作成されます。ピア関係にあるクラスタ内のすべてのノードにクラスタ間LIFを作成する必要があります。

クラスタ間LIFは、LIFが割り当てられているシステムSVMに属するルートを使用します。システムSVMは、クラスタレベルの通信用にIPspace内に自動的に作成されます。

ファンアウトとカスケードの両方のトポロジがサポートされます。カスケード トポロジの場合、クラスタ間ネットワークを作成する必要があるのは、プライマリ クラスタとセカンダリ クラスタの間、およびセカンダリ クラスタとターシャリ クラスタの間のみです。プライマリ クラスタとターシャリ クラスタの間にクラスタ間ネットワークを作成する必要はありません。

管理者は、default-interclusterサービス ポリシーからintercluster-coreサービスを削除することが可能です（ただし推奨されません）。この場合、「default-intercluster」を使用してLIFを作成しても、そのLIFはクラスタ間LIFにはなりません。default-interclusterサービス ポリシーにintercluster-coreサービスが含まれていることを確認するには、次のコマンドを使用します。

```
network interface service-policy show -policy default-intercluster
```



```
`network interface service-policy show`
```

の詳細については、[link:https://docs.netapp.com/us-en/ontap-cli/network-interface-service-policy-show.html](https://docs.netapp.com/us-en/ontap-cli/network-interface-service-policy-show.html)["ONTAP コマンド リファレンス"]を参照してください。

ONTAPピアリングの前提条件

クラスタ ピアリングを設定する前に、接続、ポート、IPアドレス、サブネット、ファイアウォール、およびクラスタの命名要件が下記の条件を満たしているか確認してください。



ONTAP 9.6以降では、クラスタ ピアリングで、データ レプリケーションに対するTLS 1.2 AES-256 GCM暗号化がデフォルトでサポートされます。デフォルトのセキュリティ暗号（「PSK-AES256-GCM-SHA384」）は、暗号化が無効になっていてもクラスタ ピアリングを機能させるために必要です。

ONTAP 9.11.1以降では、DHE-PSKセキュリティ暗号をデフォルトで使用できます。

ONTAP 9.15.1以降では、クラスタ ピアリングで、データ レプリケーションに対するTLS 1.3暗号化がデフォルトでサポートされます。

接続要件

ローカル クラスタのすべてのクラスタ間LIFが、リモート クラスタのすべてのクラスタ間LIFと通信可能であることが必要です。

必須ではありませんが、一般に、クラスタ間LIFには同じサブネットのIPアドレスを使用した方が構成がシンプルになります。使用するIPアドレスは、データLIFと同じサブネットのIPアドレスでも別のサブネットのIPアドレスでもかまいません。各クラスタで使用するサブネットは、次の要件を満たしている必要があります。

- サブネットがクラスタ間通信で使用するポートを含むブロードキャスト ドメインに属している。
- 1つのノードにつき1つのインタークラスタLIFが割り当てられるよう、サブネットに十分な数のIPアドレスを準備する。

たとえば、4ノード クラスタの場合、クラスタ間通信で使用するサブネットには使用可能なIPアドレスが4つ必要です。

クラスタ間ネットワークでは、ノードごとにインタークラスタLIFとIPアドレスが必要です。

クラスタ間LIFのアドレスにはIPv4またはIPv6のいずれかを使用できます。



ONTAPでは、必要に応じてIPv4プロトコルとIPv6プロトコルがクラスタ間LIFに共存することを許可し、IPv4からIPv6にピアリング ネットワークを移行できます。以前のリリースでは、クラスタ全体のすべてのクラスタ間関係がIPv4またはIPv6のどちらかだったため、プロトコルの変更はシステム停止を伴うイベントでした。

ポートの要件

クラスタ間通信には専用のポートを使用することも、データ ネットワークで使用しているポートを共有することもできます。ポートは、次の要件を満たしている必要があります。

- 特定のリモート クラスタとの通信に使用するすべてのポートのIPspaceが同じである。

複数のクラスタとのピア関係の作成には複数のIPspaceを使用できます。ペアワイズのフルメッシュ接続はIPspace内でのみ必要になります。

- クラスタ間通信で使用されるブロードキャスト ドメインに、1ノードあたり最低2つのポートがあり、クラスタ間通信で別のポートへのフェイルオーバーが可能になっている。

ブロードキャスト ドメインに追加できるポートは、物理ネットワーク ポート、VLAN、インターフェイスグループ (ifgrps) です。

- すべてのポートが接続されている。
- すべてのポートが健全な状態である。
- ポートのMTU設定が一貫している。

ファイアウォールの要件



ONTAP 9.10.1以降、ファイアウォールポリシーは廃止され、LIFサービスポリシーに完全に置き換えられました。詳細については、"[LIFのファイアウォール ポリシーの設定](#)"を参照してください。

ファイアウォールとクラスタ間ファイアウォール ポリシーでは、以下のプロトコルを許可する必要があります。

- 双方向ICMPトラフィック
- 双方向で開始され、すべてのクラスタ間LIFのIPアドレスを宛先とし、ポート11104および11105経由のTCPトラフィック
- クラスタ間LIF間の双方向HTTPS

HTTPSはCLIを使用したクラスタ ピアリングのセットアップ時には必要ありませんが、System Managerを使用してデータ保護を設定する場合にはあとで必要になります。

デフォルトの `intercluster` ファイアウォール ポリシーでは、HTTPSプロトコルとすべてのIPアドレス (0.0.0.0/0) からのアクセスが許可されます。必要に応じてポリシーを変更または置き換えることができます。

クラスタの要件

クラスタは、次の要件を満たす必要があります。

- 1つのクラスタに対してピア関係を設定できるクラスタは最大255個である。

共有または専用の**ONTAP**ポートを使用する

クラスタ間通信専用のポートを使用することも、データネットワークで使用するポートを共有することもできます。ポートを共有するかどうかを決定する際には、ネットワーク帯域幅、レプリケーション間隔、およびポートの可用性を考慮する必要があります。



一方のピア クラスタでポートを共有し、もう一方のクラスタでは専用ポートを使用することができます。

ネットワーク帯域幅

高速ネットワーク（10GbEなど）を採用している場合、データ アクセスに使用されるものと同じ10GbEポートでレプリケーションを実行しても、ローカルLANの帯域幅が不足することはあまりありません。

それでも、利用可能なWAN帯域幅とLAN帯域幅を比較する必要があります。利用可能なWAN帯域幅が10 GbEを大幅に下回る場合は、専用ポートの使用が必要になる可能性があります。



このルールの唯一の例外は、クラスタ内のすべてのノードまたは多くのノードがデータをレプリケートする場合です。この場合、帯域幅の使用率は通常、ノード間で分散されます。

専用ポートを使用していない場合は、通常、レプリケーション ネットワークの最大転送単位（MTU）サイズは、データ ネットワークのMTUサイズと同じになります。

レプリケーション間隔

レプリケーションがオフピーク時に行われる場合、10GbE LAN接続がなくてもレプリケーションにデータ ポートを使用できるはずです。

通常の営業時間中にレプリケーションを行う場合は、レプリケーションされるデータの量と、データプロトコルとの競合を引き起こすほどの帯域幅が必要かどうかを考慮する必要があります。データプロトコル（SMB、NFS、iSCSI）によるネットワーク使用率が50%を超える場合は、ノードフェイルオーバーが発生してもパフォーマンスが低下しないように、クラスタ間通信に専用ポートを使用する必要があります。

ポートを使用可能か

レプリケーション トラフィックがデータ トラフィックに干渉していると判断した場合は、クラスタ間LIFを同じノード上の他のクラスタ間対応共有ポートに移行できます。

VLANポートをレプリケーション専用にすることもできます。ポートの帯域幅は、すべてのVLANとベース ポートで共有されます。

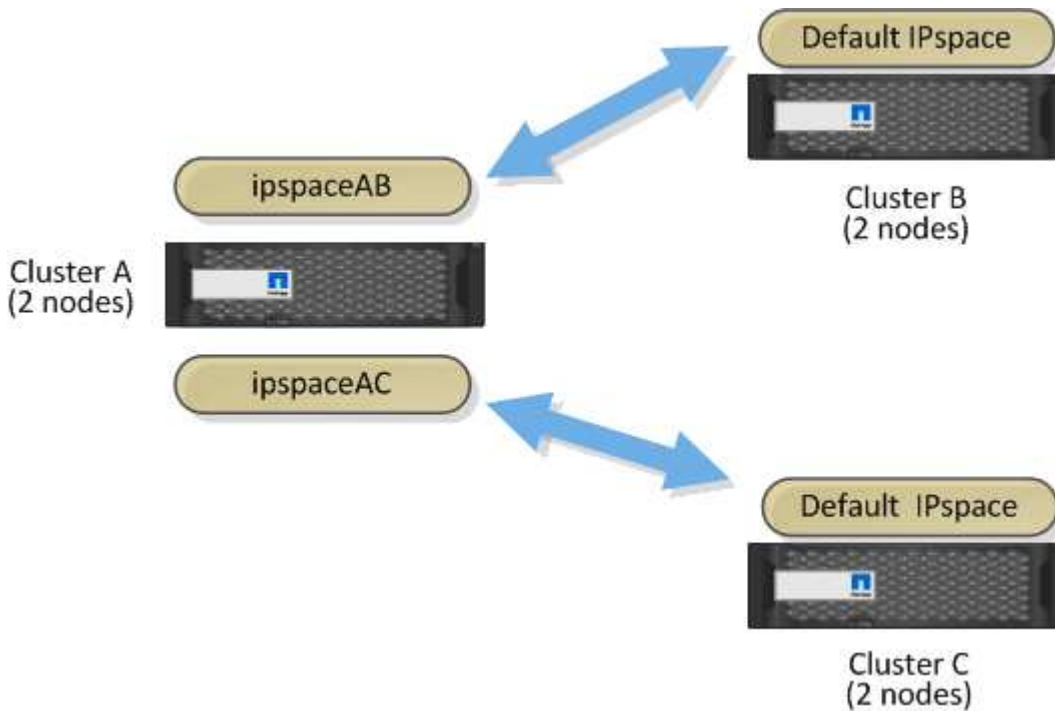
カスタムONTAP IPspaceを使用してレプリケーション トラフィックを分離する

カスタムIPspaceを使用することで、クラスタとピア間の通信を分離できます。この構成は「指定クラスタ間接続」と呼ばれ、サービスプロバイダーはマルチテナント環境におけるレプリケーショントラフィックを分離できます。

たとえば、クラスタAとクラスタBの間のレプリケーション トラフィックをクラスタAとクラスタCの間のレプ

リケーション トラフィックから切り離すためには、クラスタAにIPspaceを2つ作成します。

次の図に示すように、一方のIPspaceにはクラスタBとの通信に使用するクラスタ間LIFを、もう一方のIPspaceにはクラスタCとの通信に使用するクラスタ間LIFを含めます。



関連情報

- ["ONTAP IPspace構成について学ぶ"](#)

クラスタ間LIFを設定

共有データポート上でONTAPインタークラスタLIFを構成する

データ ネットワークと共有するポートにクラスタ間LIFを設定できます。これにより、クラスタ間ネットワークに必要なポート数を減らすことができます。

手順

1. クラスタ内のポートの一覧を表示します。

```
network port show
```

`network port show`の詳細については、[link:https://docs.netapp.com/us-en/ontap-cli/network-port-show.html](https://docs.netapp.com/us-en/ontap-cli/network-port-show.html)["ONTAPコマンド リファレンス"]を参照してください。

次の例は、`cluster01`のネットワーク ポートを示しています：

```
cluster01::> network port show
```

						Speed
(Mbps)						
Node	Port	IPspace	Broadcast Domain	Link	MTU	Admin/Oper
-----	-----	-----	-----	-----	-----	-----
cluster01-01						
	e0a	Cluster	Cluster	up	1500	auto/1000
	e0b	Cluster	Cluster	up	1500	auto/1000
	e0c	Default	Default	up	1500	auto/1000
	e0d	Default	Default	up	1500	auto/1000
cluster01-02						
	e0a	Cluster	Cluster	up	1500	auto/1000
	e0b	Cluster	Cluster	up	1500	auto/1000
	e0c	Default	Default	up	1500	auto/1000
	e0d	Default	Default	up	1500	auto/1000

2. 管理SVM（デフォルトのIPspace）またはシステムSVM（カスタムのIPspace）にクラスタ間LIFを作成します。

オプション	概要
ONTAP 9.6以降：	<code>network interface create -vserver system_SVM -lif LIF_name -service -policy default-intercluster -home -node node -home-port port -address port_IP -netmask netmask</code>
ONTAP 9.5以前の場合：	<code>network interface create -vserver system_SVM -lif LIF_name -role intercluster -home-node node -home -port port -address port_IP -netmask netmask</code>

```
`network interface create`
```

の詳細については、link:<https://docs.netapp.com/us-en/ontap-cli/network-interface-create.html>["ONTAPコマンド リファレンス"]を参照してください。

次の例では、クラスタ間 LIF `cluster01\_icl01`と `cluster01\_icl02`を作成します：

```
cluster01::> network interface create -vserver cluster01 -lif
cluster01_icl01 -service-
policy default-intercluster -home-node cluster01-01 -home-port e0c
-address 192.168.1.201
-netmask 255.255.255.0

cluster01::> network interface create -vserver cluster01 -lif
cluster01_icl02 -service-
policy default-intercluster -home-node cluster01-02 -home-port e0c
-address 192.168.1.202
-netmask 255.255.255.0
```

3. クラスタ間LIFが作成されたことを確認します。

オプション	概要
ONTAP 9.6以降：	<code>network interface show -service-policy default-intercluster</code>
ONTAP 9.5以前の場合：	<code>network interface show -role intercluster</code>

`network interface show`の詳細については、[link:https://docs.netapp.com/us-en/ontap-cli/network-interface-show.html](https://docs.netapp.com/us-en/ontap-cli/network-interface-show.html)["ONTAPコマンド リファレンス"]を参照してください。

```
cluster01::> network interface show -service-policy default-intercluster
```

	Logical	Status	Network	Current
Current Is				
Vserver	Interface	Admin/Oper	Address/Mask	Node
Home				Port
cluster01	cluster01_icl01	up/up	192.168.1.201/24	cluster01-01 e0c
true	cluster01_icl02	up/up	192.168.1.202/24	cluster01-02 e0c
true				

4. クラスタ間LIFが冗長構成になっていることを確認します。

オプション	概要
ONTAP 9.6以降：	<code>network interface show -service-policy default-intercluster -failover</code>
ONTAP 9.5以前の場合：	<code>network interface show -role intercluster -failover</code>

`network interface show`の詳細については、link:<https://docs.netapp.com/us-en/ontap-cli/network-interface-show.html>["ONTAP コマンド リファレンス"]を参照してください。

次の例は、`e0c`ポート上のクラスタ間LIF `cluster01\_icl01`および `cluster01\_icl02`が `e0d`ポートにフェイルオーバーすることを示しています。

```
cluster01::> network interface show -service-policy default-intercluster
-failover
```

	Logical Vserver Interface	Home Node:Port	Failover Policy	Failover Group
cluster01				
	cluster01_icl01	cluster01-01:e0c	local-only	
	192.168.1.201/24			
			Failover Targets: cluster01-01:e0c, cluster01-01:e0d	
	cluster01_icl02	cluster01-02:e0c	local-only	
	192.168.1.201/24			
			Failover Targets: cluster01-02:e0c, cluster01-02:e0d	

専用ポートで**ONTAP**クラスタ間**LIF**を設定する

専用ポートにクラスタ間LIFを設定できます。通常は、この設定により、レプリケーショントラフィックに使用可能な帯域幅が拡張します。

手順

1. クラスタ内のポートの一覧を表示します。

```
network port show
```

`network port show`の詳細については、link:<https://docs.netapp.com/us-en/ontap-cli/network-port-show.html>["ONTAPコマンド リファレンス"]を参照してください。

次の例は、`cluster01`のネットワーク ポートを示しています：

```
cluster01::> network port show
```

						Speed
(Mbps)						
Node	Port	IPspace	Broadcast Domain	Link	MTU	Admin/Oper
-----	-----	-----	-----	-----	-----	-----
cluster01-01						
	e0a	Cluster	Cluster	up	1500	auto/1000
	e0b	Cluster	Cluster	up	1500	auto/1000
	e0c	Default	Default	up	1500	auto/1000
	e0d	Default	Default	up	1500	auto/1000
	e0e	Default	Default	up	1500	auto/1000
	e0f	Default	Default	up	1500	auto/1000
cluster01-02						
	e0a	Cluster	Cluster	up	1500	auto/1000
	e0b	Cluster	Cluster	up	1500	auto/1000
	e0c	Default	Default	up	1500	auto/1000
	e0d	Default	Default	up	1500	auto/1000
	e0e	Default	Default	up	1500	auto/1000
	e0f	Default	Default	up	1500	auto/1000

2. クラスタ間通信専用として使用可能なポートを決定します。

```
network interface show -fields home-port,curr-port
```

`network interface show`の詳細については、link:<https://docs.netapp.com/us-en/ontap-cli/network-interface-show.html>["ONTAPコマンド リファレンス"]を参照してください。

次の例は、ポート `e0e` と `e0f` にLIFが割り当てられていないことを示しています。

```
cluster01::> network interface show -fields home-port,curr-port
vserver lif                home-port curr-port
-----
Cluster cluster01-01_clus1 e0a      e0a
Cluster cluster01-01_clus2 e0b      e0b
Cluster cluster01-02_clus1 e0a      e0a
Cluster cluster01-02_clus2 e0b      e0b
cluster01
      cluster_mgmt          e0c      e0c
cluster01
      cluster01-01_mgmt1    e0c      e0c
cluster01
      cluster01-02_mgmt1    e0c      e0c
```

3. 専用ポートのフェイルオーバー グループを作成します。

```
network interface failover-groups create -vserver system_SVM -failover-group
failover_group -targets physical _or_logical_ports
```

次の例では、システムSVM `cluster01` 上のフェイルオーバー グループ `intercluster01` にポート `e0e` と `e0f` を割り当てます：

```
cluster01::> network interface failover-groups create -vserver cluster01
-failover-group
intercluster01 -targets
cluster01-01:e0e,cluster01-01:e0f,cluster01-02:e0e,cluster01-02:e0f
```

4. フェイルオーバー グループが作成されたことを確認します。

```
network interface failover-groups show
```

```
`network interface failover-groups show`
の詳細については、link:https://docs.netapp.com/us-en/ontap-cli/network-
interface-failover-groups-show.html["ONTAPコマンド リファレンス
"^]をご覧ください。
```

```
cluster01::> network interface failover-groups show
```

Vserver	Group	Failover Targets
Cluster	Cluster	cluster01-01:e0a, cluster01-01:e0b, cluster01-02:e0a, cluster01-02:e0b
cluster01	Default	cluster01-01:e0c, cluster01-01:e0d, cluster01-02:e0c, cluster01-02:e0d, cluster01-01:e0e, cluster01-01:e0f cluster01-02:e0e, cluster01-02:e0f
	intercluster01	cluster01-01:e0e, cluster01-01:e0f cluster01-02:e0e, cluster01-02:e0f

5. システムSVMにクラスタ間LIFを作成して、フェイルオーバー グループに割り当てます。

オプション	概要
ONTAP 9.6以降：	<pre>network interface create -vserver system_SVM -lif LIF_name -service -policy default-intercluster -home -node node -home- port port -address port_IP -netmask netmask -failover -group failover_group</pre>
ONTAP 9.5以前の場合：	<pre>network interface create -vserver system_SVM -lif LIF_name -role intercluster -home-node node -home -port port -address port_IP -netmask netmask -failover-group failover_group</pre>

`network interface create`

の詳細については、link:<https://docs.netapp.com/us-en/ontap-cli/network-interface-create.html>["ONTAPコマンド リファレンス"]を参照してください。

次の例では、フェイルオーバー グループ `intercluster01` にクラスタ間 LIF `cluster01\_icl01` と `cluster01\_icl02` を作成します：

```
cluster01::> network interface create -vserver cluster01 -lif
cluster01_icl01 -service-
policy default-intercluster -home-node cluster01-01 -home-port e0e
-address 192.168.1.201
-netmask 255.255.255.0 -failover-group intercluster01

cluster01::> network interface create -vserver cluster01 -lif
cluster01_icl02 -service-
policy default-intercluster -home-node cluster01-02 -home-port e0e
-address 192.168.1.202
-netmask 255.255.255.0 -failover-group intercluster01
```

6. クラスタ間LIFが作成されたことを確認します。

オプション	概要
ONTAP 9.6以降：	<code>network interface show -service-policy default-intercluster</code>
ONTAP 9.5以前の場合：	<code>network interface show -role intercluster</code>

`network interface show`の詳細については、[link:https://docs.netapp.com/us-en/ontap-cli/network-interface-show.html](https://docs.netapp.com/us-en/ontap-cli/network-interface-show.html)["ONTAPコマンド リファレンス"]を参照してください。

```
cluster01::> network interface show -service-policy default-intercluster
      Logical      Status      Network      Current
Current Is
Vserver      Interface  Admin/Oper  Address/Mask      Node      Port
Home
-----
cluster01
      cluster01_icl01
              up/up      192.168.1.201/24  cluster01-01  e0e
true
      cluster01_icl02
              up/up      192.168.1.202/24  cluster01-02  e0f
true
```

7. クラスタ間LIFが冗長構成になっていることを確認します。

オプション	概要
ONTAP 9.6以降：	<code>network interface show -service-policy default-intercluster -failover</code>
ONTAP 9.5以前の場合：	<code>network interface show -role intercluster -failover</code>

`network interface show`の詳細については、[link:https://docs.netapp.com/us-en/ontap-cli/network-interface-show.html](https://docs.netapp.com/us-en/ontap-cli/network-interface-show.html)["ONTAP コマンド リファレンス"]を参照してください。

次の例は、SVM e0e 上のクラスタ間 LIF `cluster01\_icl01` と `cluster01\_icl02` が `e0f` ポートにフェイルオーバーすることを示しています。

```
cluster01::> network interface show -service-policy default-intercluster
-failover
```

	Logical	Home	Failover	Failover
Vserver	Interface	Node:Port	Policy	Group
cluster01				
	cluster01_icl01	cluster01-01:e0e	local-only	
intercluster01				
		Failover Targets:	cluster01-01:e0e,	
			cluster01-01:e0f	
	cluster01_icl02	cluster01-02:e0e	local-only	
intercluster01				
		Failover Targets:	cluster01-02:e0e,	
			cluster01-02:e0f	

カスタム IPspace で ONTAP クラスタ間 LIF を設定する

カスタム IPspace にクラスタ間 LIF を設定できます。これにより、マルチテナント環境でレプリケーショントラフィックを分離できます。

カスタム IPspace を作成すると、システムによってシステムストレージ仮想マシン (SVM) が作成され、その IPspace 内のシステムオブジェクトのコンテナとして機能します。この新しい SVM は、新しい IPspace 内の任意のクラスタ間 LIF のコンテナとして使用できます。新しい SVM の名前は、カスタム IPspace と同じになります。

手順

1. クラスタ内のポートの一覧を表示します。

```
network port show
```

`network port show`の詳細については、link:<https://docs.netapp.com/us-en/ontap-cli/network-port-show.html>["ONTAPコマンド リファレンス"]を参照してください。

次の例は、`cluster01`のネットワーク ポートを示しています：

```
cluster01::> network port show
```

						Speed
(Mbps)						
Node	Port	IPspace	Broadcast Domain	Link	MTU	Admin/Oper
-----	-----	-----	-----	-----	-----	-----
cluster01-01						
	e0a	Cluster	Cluster	up	1500	auto/1000
	e0b	Cluster	Cluster	up	1500	auto/1000
	e0c	Default	Default	up	1500	auto/1000
	e0d	Default	Default	up	1500	auto/1000
	e0e	Default	Default	up	1500	auto/1000
	e0f	Default	Default	up	1500	auto/1000
cluster01-02						
	e0a	Cluster	Cluster	up	1500	auto/1000
	e0b	Cluster	Cluster	up	1500	auto/1000
	e0c	Default	Default	up	1500	auto/1000
	e0d	Default	Default	up	1500	auto/1000
	e0e	Default	Default	up	1500	auto/1000
	e0f	Default	Default	up	1500	auto/1000

2. クラスタ上にカスタム IPspace を作成します：

```
network ipspace create -ipspace ipspace
```

次の例では、カスタム IPspace `ipspace-IC1`を作成します：

```
cluster01::> network ipspace create -ipspace ipspace-IC1
```

`network ipspace create`の詳細については、link:<https://docs.netapp.com/us-en/ontap-cli/network-ip-space-create.html>["ONTAPコマンド リファレンス"]を参照してください。

3. クラスタ間通信専用として使用可能なポートを決定します。

```
network interface show -fields home-port,curr-port
```

`network interface show`の詳細については、link:<https://docs.netapp.com/us-en/ontap-cli/network-interface-show.html>["ONTAPコマンド リファレンス"]を参照してください。

次の例は、ポート `e0e` と `e0f` にLIFが割り当てられていないことを示しています。

```
cluster01::> network interface show -fields home-port,curr-port
vserver lif                home-port curr-port
-----
Cluster cluster01_clus1    e0a      e0a
Cluster cluster01_clus2    e0b      e0b
Cluster cluster02_clus1    e0a      e0a
Cluster cluster02_clus2    e0b      e0b
cluster01
      cluster_mgmt          e0c      e0c
cluster01
      cluster01-01_mgmt1    e0c      e0c
cluster01
      cluster01-02_mgmt1    e0c      e0c
```

4. デフォルトのブロードキャスト ドメインから使用可能なポートを削除します：

```
network port broadcast-domain remove-ports -broadcast-domain Default -ports
ports
```

1つのポートが同時に複数のブロードキャストドメインに属することはできません。["ONTAPコマンド リファレンス"](#)の `network port broadcast-domain remove-ports` の詳細をご覧ください。

次の例では、ポート `e0e` と `e0f` をデフォルトのブロードキャスト ドメインから削除します：

```
cluster01::> network port broadcast-domain remove-ports -broadcast
-domain Default -ports
cluster01-01:e0e,cluster01-01:e0f,cluster01-02:e0e,cluster01-02:e0f
```

5. ポートがデフォルトのブロードキャスト ドメインから削除されていることを確認します：

```
network port show
```

`network port show`の詳細については、link:<https://docs.netapp.com/us-en/ontap-cli/network-port-show.html>["ONTAPコマンド リファレンス"]を参照してください。

次の例は、ポート `e0e` と `e0f` がデフォルトのブロードキャスト ドメインから削除されたことを示してい

ます。

```
cluster01::> network port show
```

Node	Port	IPspace	Broadcast Domain	Link	MTU	Speed (Mbps) Admin/Oper
-----	-----	-----	-----	-----	-----	-----
cluster01-01						
	e0a	Cluster	Cluster	up	9000	auto/1000
	e0b	Cluster	Cluster	up	9000	auto/1000
	e0c	Default	Default	up	1500	auto/1000
	e0d	Default	Default	up	1500	auto/1000
	e0e	Default	-	up	1500	auto/1000
	e0f	Default	-	up	1500	auto/1000
	e0g	Default	Default	up	1500	auto/1000
cluster01-02						
	e0a	Cluster	Cluster	up	9000	auto/1000
	e0b	Cluster	Cluster	up	9000	auto/1000
	e0c	Default	Default	up	1500	auto/1000
	e0d	Default	Default	up	1500	auto/1000
	e0e	Default	-	up	1500	auto/1000
	e0f	Default	-	up	1500	auto/1000
	e0g	Default	Default	up	1500	auto/1000

6. カスタム IPspace にブロードキャスト ドメインを作成します：

```
network port broadcast-domain create -ipspace ipspace -broadcast-domain  
broadcast_domain -mtu MTU -ports ports
```

次の例では、IPspace `ipspace-IC1` にブロードキャスト ドメイン `ipspace-IC1-bd` を作成します：

```
cluster01::> network port broadcast-domain create -ipspace ipspace-IC1  
-broadcast-domain  
ipspace-IC1-bd -mtu 1500 -ports cluster01-01:e0e,cluster01-01:e0f,  
cluster01-02:e0e,cluster01-02:e0f
```

7. ブロードキャスト ドメインが作成されたことを確認します：

```
network port broadcast-domain show
```

```
`network port broadcast-domain show`  
の詳細については、link:https://docs.netapp.com/us-en/ontap-cli/network-  
port-broadcast-domain-show.html ["ONTAP コマンド リファレンス  
"^] を参照してください。
```

```
cluster01::> network port broadcast-domain show
```

IPspace	Broadcast			Update
Name	Domain Name	MTU	Port List	Status Details
-----	-----	-----	-----	-----
Cluster	Cluster	9000		
			cluster01-01:e0a	complete
			cluster01-01:e0b	complete
			cluster01-02:e0a	complete
			cluster01-02:e0b	complete
Default	Default	1500		
			cluster01-01:e0c	complete
			cluster01-01:e0d	complete
			cluster01-01:e0f	complete
			cluster01-01:e0g	complete
			cluster01-02:e0c	complete
			cluster01-02:e0d	complete
			cluster01-02:e0f	complete
			cluster01-02:e0g	complete
ipspace-IC1				
	ipspace-IC1-bd			
		1500		
			cluster01-01:e0e	complete
			cluster01-01:e0f	complete
			cluster01-02:e0e	complete
			cluster01-02:e0f	complete

8. システムSVMでクラスタ間LIFを作成し、ブロードキャスト ドメインに割り当てます：

オプション	概要
ONTAP 9.6以降：	<pre>network interface create -vserver system_SVM -lif LIF_name -service -policy default-intercluster -home -node node -home-port port -address port_IP -netmask netmask</pre>
ONTAP 9.5以前の場合：	<pre>network interface create -vserver system_SVM -lif LIF_name -role intercluster -home-node node -home -port port -address port_IP -netmask netmask</pre>

LIFは、ホーム ポートが割り当てられているブロードキャスト ドメインに作成されます。ブロードキャスト ドメインには、ブロードキャスト ドメインと同じ名前のデフォルトのフェイルオーバー グループがあります。["ONTAPコマンド リファレンス"](#)の`network interface create`の詳細を確認してください。

次の例では、ブロードキャスト ドメイン `ipspace-IC1-bd` にクラスタ間 LIF `cluster01\_icl01` と `cluster01\_icl02` を作成します：

```
cluster01::> network interface create -vserver ipspace-IC1 -lif
cluster01_icl01 -service-
policy default-intercluster -home-node cluster01-01 -home-port e0e
-address 192.168.1.201
-netmask 255.255.255.0

cluster01::> network interface create -vserver ipspace-IC1 -lif
cluster01_icl02 -service-
policy default-intercluster -home-node cluster01-02 -home-port e0e
-address 192.168.1.202
-netmask 255.255.255.0
```

9. クラスタ間LIFが作成されたことを確認します。

オプション	概要
ONTAP 9.6以降：	network interface show -service-policy default-intercluster
ONTAP 9.5以前の場合：	network interface show -role intercluster

`network interface show`の詳細については、link:<https://docs.netapp.com/us-en/ontap-cli/network-interface-show.html>["ONTAPコマンド リファレンス"]を参照してください。

```
cluster01::> network interface show -service-policy default-intercluster
Current Is
Vserver      Logical      Status      Network      Current
Home         Interface   Admin/Oper  Address/Mask  Node         Port
-----
ipspace-IC1
              cluster01_icl01
                  up/up      192.168.1.201/24  cluster01-01  e0e
true
              cluster01_icl02
                  up/up      192.168.1.202/24  cluster01-02  e0f
true
```

10. クラスタ間LIFが冗長構成になっていることを確認します。

オプション	概要
ONTAP 9.6以降：	<code>network interface show -service-policy default-intercluster -failover</code>
ONTAP 9.5以前の場合：	<code>network interface show -role intercluster -failover</code>

`network interface show`の詳細については、link:<https://docs.netapp.com/us-en/ontap-cli/network-interface-show.html>["ONTAPコマンド リファレンス"]を参照してください。

次の例は、SVM `e0e`上のクラスタ間LIF `cluster01\_icl01`と `cluster01\_icl02`が`e0f`ポートにフェイルオーバーすることを示しています：

```
cluster01::> network interface show -service-policy default-intercluster
-failover
```

Vserver	Logical Interface	Home Node:Port	Failover Policy	Failover Group

ipspace-IC1				
	cluster01_icl01	cluster01-01:e0e	local-only	
intercluster01				
			Failover Targets:	cluster01-01:e0e, cluster01-01:e0f
	cluster01_icl02	cluster01-02:e0e	local-only	
intercluster01				
			Failover Targets:	cluster01-02:e0e, cluster01-02:e0f

ピア関係の設定

ONTAPクラスタ ピア関係を作成する

データ バックアップやディザスタ リカバリ用にリモート クラスタにデータをレプリケートして保護するには、まずローカル クラスタとリモート クラスタの間にクラスタ ピア関係を作成する必要があります。

タスク概要

この手順は、FAS、AFF、およびASAシステムに適用されます。ASA r2システム（ASAA1K、ASAA90、ASAA70、ASAA50、ASAA30、ASAA20、またはASA C30）をご利用の場合は、["これらの手順"](#)に従ってSnapshotレプリケーションをセットアップしてください。ASA r2システムは、SANのみのお客様向けに簡

素化されたONTAPエクスペリエンスを提供します。

デフォルトの保護ポリシーがいくつか用意されています。カスタムの保護ポリシーを使用する場合はあらかじめ作成しておく必要があります。

開始する前に

ONTAP CLIを使用している場合は、以下のいずれかの方法でピアリングするクラスタ内の各ノードにクラスタ間LIFを作成しておく必要があります。

- ["共有データ ポートでのクラスタ間LIFの設定"](#)
- ["専用データ ポートでのクラスタ間LIFの設定"](#)
- ["カスタムIPspaceでのクラスタ間LIFの設定"](#)

手順

このタスクは、ONTAP System ManagerまたはONTAP CLIを使用して実行します。

System Manager

1. ローカル クラスタで、**クラスタ > 設定** をクリックします。
2. **[クラスタ間設定]** セクションで、**[ネットワーク インターフェイスの追加]** をクリックし、IP アドレスとサブネット マスクを入力して、クラスタのクラスタ間ネットワーク インターフェイスを追加します。

同じ手順をリモート クラスタでも実行します。

3. リモート クラスタで、***クラスタ > 設定*** をクリックします。
4. クラスタ ピア セクションで  をクリックし、**パスフレーズの生成** を選択します。
5. リモートONTAPクラスタのバージョンを選択します。
6. 生成されたパスフレーズをコピーします。
7. ローカル クラスタの***クラスタ ピア***で、 をクリックして***ピア クラスタ***を選択します。
8. ピア クラスター ウィンドウでパスフレーズを貼り付けて、**クラスター ピアリングの開始** をクリックします。

CLI

1. デスティネーション クラスタで、ソース クラスタとのピア関係を作成します。

```
cluster peer create -generate-passphrase -offer-expiration  
<MM/DD/YYYY HH:MM:SS|1...7days|1...168hours> -peer-addr  
<peer_LIF_IPs> -initial-allowed-vserver-peers <svm_name|*> -ip  
<ipspace>
```

`-generate-passphrase`と`-peer-addr`の両方を指定した場合、`-peer-addr`でクラスタ間LIFが指定されているクラスタのみが生成されたパスワードを使用できます。

カスタムIPspaceを使用していない場合は、`-ipspace`オプションを無視できます。["ONTAPコマンドリファレンス"](#)の`cluster peer create`の詳細をご覧ください。

ONTAP 9.6以降でピアリング関係を作成し、クラスタ間ピアリング通信を暗号化したくない場合は、`-encryption-protocol-proposed none`オプションを使用して暗号化を無効にする必要があります。

次の例では、指定されていないリモート クラスタとのクラスタ ピア関係を作成し、ローカル クラスタ上の SVM `vs1`と`vs2`とのピア関係を事前承認します：

```
cluster02::> cluster peer create -generate-passphrase -offer
-expiration 2days -initial-allowed-vserver-peers vs1,vs2

Passphrase: UCa+6lRVICXeL/gq1WrK7ShR
Expiration Time: 6/7/2017 08:16:10 EST
Initial Allowed Vserver Peers: vs1,vs2
Intercluster LIF IP: 192.140.112.101
Peer Cluster Name: Clus_7ShR (temporary generated)

Warning: make a note of the passphrase - it cannot be displayed
again.
```

次の例は、クラスタ間LIFのIPアドレス192.140.112.103および192.140.112.104でリモート クラスタとのクラスタ ピア関係を作成し、ローカル クラスタのすべてのSVMとのピア関係を事前承認します。

```
cluster02::> cluster peer create -generate-passphrase -peer-addr
192.140.112.103,192.140.112.104 -offer-expiration 2days -initial
-allowed-vserver-peers *

Passphrase: UCa+6lRVICXeL/gq1WrK7ShR
Expiration Time: 6/7/2017 08:16:10 EST
Initial Allowed Vserver Peers: vs1,vs2
Intercluster LIF IP: 192.140.112.101,192.140.112.102
Peer Cluster Name: Clus_7ShR (temporary generated)

Warning: make a note of the passphrase - it cannot be displayed
again.
```

次の例では、指定されていないリモート クラスタとのクラスタ ピア関係を作成し、ローカル クラスタ上の SVM`vs1`と `vs2`とのピア関係を事前承認します：

```
cluster02::> cluster peer create -generate-passphrase -offer
-expiration 2days -initial-allowed-vserver-peers vs1,vs2

Passphrase: UCa+6lRVICXeL/gq1WrK7ShR
Expiration Time: 6/7/2017 08:16:10 EST
Initial Allowed Vserver Peers: vs1,vs2
Intercluster LIF IP: 192.140.112.101
Peer Cluster Name: Clus_7ShR (temporary generated)

Warning: make a note of the passphrase - it cannot be displayed
again.
```

2. ソース クラスタで、ソース クラスタをデスティネーション クラスタに対して認証します。

```
cluster peer create -peer-addr <peer_LIF_IPs> -ipspace <ipspace>
```

`cluster peer create`の詳細については、[link:https://docs.netapp.com/us-en/ontap-cli/cluster-peer-create.html](https://docs.netapp.com/us-en/ontap-cli/cluster-peer-create.html)["ONTAPコマンド リファレンス"]を参照してください。

次の例は、クラスタ間LIFのIPアドレス192.140.112.101および192.140.112.102でローカル クラスタをリモート クラスタに対して認証します。

```
cluster01::> cluster peer create -peer-addr  
192.140.112.101,192.140.112.102
```

Notice: Use a generated passphrase or choose a passphrase of 8 or more characters.

To ensure the authenticity of the peering relationship, use a phrase or sequence of characters that would be hard to guess.

Enter the passphrase:

Confirm the passphrase:

Clusters cluster02 and cluster01 are peered.

プロンプトが表示されたら、ピア関係のパスフレーズを入力します。

3. クラスタ ピア関係が作成されたことを確認します。

```
cluster peer show -instance
```

```
cluster01::> cluster peer show -instance
```

```
Peer Cluster Name: cluster02
Remote Intercluster Addresses: 192.140.112.101,
192.140.112.102
Availability of the Remote Cluster: Available
Remote Cluster Name: cluster2
Active IP Addresses: 192.140.112.101,
192.140.112.102
Cluster Serial Number: 1-80-123456
Address Family of Relationship: ipv4
Authentication Status Administrative: no-authentication
Authentication Status Operational: absent
Last Update Time: 02/05 21:05:41
IPspace for the Relationship: Default
```

4. ピア関係にあるノードの接続状態とステータスを確認します。

```
cluster peer health show
```

```

cluster01::> cluster peer health show
Node          cluster-Name          Node-Name
              Ping-Status          RDB-Health Cluster-Health
Avail...
-----
cluster01-01
              cluster02          cluster02-01
              Data: interface_reachable
              ICMP: interface_reachable true          true
true
              cluster02-02
              Data: interface_reachable
              ICMP: interface_reachable true          true
true
cluster01-02
              cluster02          cluster02-01
              Data: interface_reachable
              ICMP: interface_reachable true          true
true
              cluster02-02
              Data: interface_reachable
              ICMP: interface_reachable true          true
true

```

ONTAPでこの処理を行うその他の方法

タスクを実行するツール	参照するコンテンツ
System Manager Classic (ONTAP 9.7以前で使用可能)	"ボリューム災害復旧準備の概要"

ONTAPクラスタ間SVMピア関係を作成する

`vserver peer create` コマンドを使用して、ローカル クラスタとリモート クラスタ上の SVM 間にピア関係を作成できます。

開始する前に

- ソース クラスタとデスティネーション クラスタのピア関係が確立されている必要があります。
- リモート クラスタのSVMについて、ピア関係を「事前承認」しておく必要があります。

詳細については、["クラスタ ピア関係の作成"](#)を参照してください。

タスク概要

クラスタ ピア関係の作成時に `initial-allowed-vserver` オプションでSVMをリストすることで、複数のSVMのピア関係を「事前承認」できます。詳細については、"[クラスタ ピア関係の作成](#)"を参照してください。

手順

1. データ保護のデスティネーション クラスタで、ピアリング対象として事前承認されたSVMを表示します。

```
vserver peer permission show
```

```
cluster02::> vserver peer permission show
Peer Cluster      Vserver            Applications
-----
cluster02         vs1,vs2            snapmirror
```

2. データ保護のソース クラスタで、データ保護のデスティネーション クラスタ上の事前承認されたSVMとのピア関係を作成します。

```
vserver peer create -vserver local_SVM -peer-vserver remote_SVM
```

`vserver peer create`の詳細については、[link:https://docs.netapp.com/us-en/ontap-cli/vserver-peer-create.html](https://docs.netapp.com/us-en/ontap-cli/vserver-peer-create.html)["ONTAPコマンド リファレンス"]をご覧ください。

次の例では、ローカル SVM `pvs1`と事前承認されたリモート SVM `vs1`の間にピア関係を作成します：

```
cluster01::> vserver peer create -vserver pvs1 -peer-vserver vs1
```

3. SVMピア関係を確認します。

```
vserver peer show
```

```
cluster01::> vserver peer show
Peer      Peer      Peering
Remote
Vserver   Vserver   State      Peer Cluster  Applications
Vserver
-----
pvs1      vs1       peered     cluster02     snapmirror
vs1
```

ONTAP クラスタ間SVMピア関係を追加する

クラスタ ピア関係を設定した後にSVMを作成する場合は、SVMのピア関係を手動で追加する必要があります。`vserver peer create` コマンドを使用して、SVM間のピア関係を作成できます。ピア関係を作成したら、リモートクラスタで `vserver peer accept` を実行してピア関係を承認できます。

開始する前に

ソース クラスタとデスティネーション クラスタのピア関係が確立されている必要があります。

タスク概要

ローカルデータのバックアップのために、同じクラスタ内のSVM間でピア関係を作成できます。["ONTAP コマンド リファレンス"](#)の `vserver peer create` の詳細をご覧ください。

管理者は、提案されたSVMピア関係を拒否するために `vserver peer reject` コマンドを使用することがあります。SVM間の関係が `rejected` 状態にある場合は、新しい関係を作成する前に、現在の関係を削除する必要があります。["ONTAP コマンド リファレンス"](#)の `vserver peer reject` の詳細を参照してください。

手順

1. データ保護のソース クラスタで、データ保護のデスティネーション クラスタ上のSVMとのピア関係を作成します。

```
vserver peer create -vserver local_SVM -peer-vserver remote_SVM -applications snapmirror|file-copy|lun-copy -peer-cluster remote_cluster
```

次の例では、ローカルSVM`pvs1`とリモートSVM`vs1`の間にピア関係を作成します。

```
cluster01::> vserver peer create -vserver pvs1 -peer-vserver vs1  
-applications snapmirror -peer-cluster cluster02
```

ローカル SVM とリモート SVM の名前が同じ場合は、ローカル名 を使用して SVM ピア関係を作成する必要があります。

```
cluster01::> vserver peer create -vserver vs1 -peer-vserver  
vs1 -applications snapmirror -peer-cluster cluster01  
-local-name cluster1vs1LocallyUniqueName
```

2. データ保護のソース クラスタで、ピア関係が開始されていることを確認します。

```
vserver peer show-all
```

`vserver peer show-all` の詳細については、[link:https://docs.netapp.com/us-en/ontap-cli/vserver-peer-show-all.html](https://docs.netapp.com/us-en/ontap-cli/vserver-peer-show-all.html) ["ONTAP コマンド リファレンス"] を参照してください。

次の例は、SVM_{pvs1}と SVM_{vs1}間のピア関係が開始されたことを示しています：

```
cluster01::> vserver peer show-all
```

Vserver	Peer Vserver	Peer State	Peer Cluster	Peering Applications
pvs1	vs1	initiated	Cluster02	snapmirror

3. データ保護のデスティネーション クラスターで、保留中のSVMピア関係を表示します。

```
vserver peer show
```

`vserver peer show`の詳細については、link:<https://docs.netapp.com/us-en/ontap-cli/vserver-peer-show.html>["ONTAPコマンド リファレンス"]を参照してください。

次の例では、`cluster02`の保留中のピア関係を一覧表示します：

```
cluster02::> vserver peer show
```

Vserver	Peer Vserver	Peer State
vs1	pvs1	pending

4. データ保護のデスティネーション クラスターで、保留中のピア関係を承認します。

```
vserver peer accept -vserver local_SVM -peer-vserver remote_SVM
```

`vserver peer accept`の詳細については、link:<https://docs.netapp.com/us-en/ontap-cli/vserver-peer-accept.html>["ONTAPコマンド リファレンス"]を参照してください。

次の例では、ローカル SVM `vs1`とリモート SVM `pvs1`間のピア関係を承認します：

```
cluster02::> vserver peer accept -vserver vs1 -peer-vserver pvs1
```

5. SVMピア関係を確認します。

```
vserver peer show
```



```
cluster01::> vservers peer show
```

Remote Vserver	Peer Vserver	Peer State	Peer Cluster	Peering Applications
pvs1	vs1	peered	cluster02	snapmirror

ピア関係でONTAPクラスタピアリング暗号化を有効にする

ONTAP 9.6以降では、新しく作成されるすべてのクラスタ ピア関係で、クラスタ ピアリングの暗号化がデフォルトで有効になります。クラスタ ピアリングの暗号化では、事前共有キー（PSK）とTransport Security Layer（TLS）を使用して、クラスタ間ピアリング通信が保護されます。これにより、ピア クラスタ間のセキュリティが強化されます。

タスク概要

ピア クラスタをONTAP 9.6以降にアップグレードする場合に、ONTAP 9.5以前でピア関係が作成されていた場合は、アップグレード後にクラスタ ピアリングの暗号化を手動で有効にする必要があります。クラスタ ピアリングの暗号化を有効にするには、ピア関係の両方のクラスタがONTAP 9.6以降を実行している必要があります。

手順

1. デスティネーション クラスタで、ソース クラスタとの通信の暗号化を有効にします。

```
cluster peer modify source_cluster -auth-status-admin use-authentication
-encryption-protocol-proposed tls-psk
```

2. プロンプトが表示されたら、パスフレーズを入力します。
3. データ保護のソース クラスタで、データ保護のデスティネーション クラスタとの通信の暗号化を有効にします。

```
cluster peer modify data_protection_destination_cluster -auth-status-admin
use-authentication -encryption-protocol-proposed tls-psk
```

4. プロンプトが表示されたら、デスティネーション クラスタで入力したパスフレーズを入力します。

`cluster peer modify`の詳細については、[link:https://docs.netapp.com/us-en/ontap-cli/cluster-peer-modify.html](https://docs.netapp.com/us-en/ontap-cli/cluster-peer-modify.html)["ONTAPコマンド リファレンス"]を参照してください。

ピア関係から**ONTAP**クラスタ ピアリング暗号化を削除する

ONTAP 9.6以降で作成されるすべてのピア関係では、デフォルトでクラスタ ピアリングの暗号化が有効になります。クラスタ間ピアリング通信に暗号化を使用しない場合は、暗号化を無効にできます。

手順

1. デスティネーション クラスタで、クラスタ ピアリングの暗号化を中止するようにソース クラスタとの通信を変更します。

- 認証を維持したまま暗号化を解除するには、次のコマンドを入力します。

```
cluster peer modify <source_cluster> -auth-status-admin use-  
authentication -encryption-protocol-proposed none
```

- 暗号化と認証を解除するには、以下の手順に従います。

- i. 認証されていないアクセスを許可するようにクラスタ ピアリング ポリシーを変更します。

```
cluster peer policy modify -is-unauthenticated-access-permitted  
true
```

- ii. 暗号化および認証アクセスを変更します。

```
cluster peer modify <source_cluster> -auth-status no-  
authentication
```

2. プロンプトが表示されたら、パスフレーズを入力します。
3. パスフレーズを再度入力して確認します。
4. ソース クラスタで、デスティネーション クラスタとの通信の暗号化を無効にします。

- 認証を維持したまま暗号化を解除するには、次のコマンドを入力します。

```
cluster peer modify <destination_cluster> -auth-status-admin use-  
authentication -encryption-protocol-proposed none
```

- 暗号化と認証を解除するには、以下の手順に従います。

- i. 認証されていないアクセスを許可するようにクラスタ ピアリング ポリシーを変更します。

```
cluster peer policy modify -is-unauthenticated-access-permitted  
true
```

- ii. 暗号化および認証アクセスを変更します。

```
cluster peer modify <destination_cluster> -auth-status no-  
authentication
```

5. プロンプトが表示されたら、デスティネーション クラスタで使用したパスフレーズを入力し、再度入力します。

ローカルSnapshotの管理

ローカルONTAPスナップショットの管理について学ぶ

スナップショットとは、ボリュームの読み取り専用のポイントインタイムイメージです。このイメージは、最後のスナップショット以降のファイルの変更のみを記録するため、ストレージ容量の消費は最小限で、パフォーマンス オーバーヘッドもごくわずかです。

スナップショットを使用すると、ボリュームの内容全体を復元したり、個々のファイルまたは LUN を回復したりできます。スナップショットはボリューム上の `.snapshot` ディレクトリに保存されます。

ONTAP 9.4以降では、FlexVolボリュームに最大1023個のスナップショットを保存できます。ONTAP 9.3以前では、ボリュームに最大255個のスナップショットを保存できます。



ONTAP 9.8以降では、FlexGroupボリュームに1023個のスナップショットを保存できます。詳細については、"[スナップショットを使用してFlexGroupボリュームを保護する](#)"を参照してください。

ONTAP長期保存スナップショットについて学ぶ

SnapMirrorポリシータイプが「vault」または「mirror-vault」である関係では、SnapMirror関係のセカンダリ ボリュームに直接スナップショットを作成できます。これらのスナップショットは、バックアップとしてデスティネーションに保持されます。これらのスナップショットは長期保存を目的として作成されることが多く、長期保存スナップショットと呼ばれます。

長期保存スナップショットを作成するには、SnapMirrorポリシー ルールでスナップショット作成スケジュール、スナップショット名のプレフィックス、SnapMirrorラベル、および保存回数を指定します。このスナップショットは、ソースの保存ルールに関係なく、SnapMirrorデスティネーション ボリュームに保持されます。

長期保存SnapshotはFlexVol SnapMirror構成に対してのみ使用できます。FlexGroup SnapMirror構成に対して長期保存Snapshotを作成することはできません。

SnapMirrorカスケード関係では、長期保存Snapshotはカスケードの最後のボリュームにのみ作成できます。

関連情報

- "[カスケード展開の仕組みについて学ぶ](#)"

- ["ONTAP SnapMirrorスケジュールを定義して、デスティネーションにローカル コピーを作成します"](#)

カスタムSnapshotポリシーの設定

カスタムONTAPスナップショット ポリシーの構成について学習します

スナップショットポリシーは、システムがスナップショットを作成する方法を定義します。このポリシーでは、スナップショットを作成するタイミング、保持するコピーの数、およびスナップショットの名前を指定します。例えば、毎日午前0:10にスナップショットを1つ作成し、最新の2つのコピーを保持し、それらのコピーに「`daily.`_timestamp``」という名前を付けるといったことが考えられます。

ボリュームのデフォルト ポリシーでは、次のスケジュールでスナップショットが自動的に作成され、新しいコピーのためのスペースを確保するために最も古いスナップショットが削除されます：

- 毎時5分過ぎに作成される時間単位Snapshotコピーは最大6つです。
- 月曜日から土曜日まで、深夜0時10分に最大2つの日次Snapshotが作成されます。
- 毎週日曜日の午前0時15分に最大2回の週次スナップショットが作成されます。

ボリュームの作成時にSnapshotポリシーを指定しない限り、ボリュームはそれを含むStorage Virtual Machine (SVM) に関連付けられたSnapshotポリシーを継承します。

カスタムONTAPスナップショットポリシーを設定するタイミング

デフォルトのスナップショットポリシーがボリュームに適していない場合は、スナップショットの頻度、保持期間、名前を変更するカスタムポリシーを構成できます。スケジュールは主にアクティブ ファイル システムの変更率によって決まります。

データベースのような頻繁に使用されるファイルシステムは1時間ごとにバックアップし、あまり使用されないファイルは1日に1回バックアップするといった具合です。データベースの場合でも、通常はフル バックアップを1日に1~2回実行し、トランザクションログは1時間ごとにバックアップします。

その他の要因としては、組織におけるファイルの重要性、サービス レベル アグリーメント (SLA)、Recovery Point Objective (RPO)、Recovery Time Objective (RTO) などが挙げられます。一般的に、スナップショットは必要な数だけ保持する必要があります。

ONTAPスナップショット ジョブ スケジュールを作成する

スナップショットポリシーには、少なくとも1つのスナップショットジョブスケジュールが必要です。System Managerまたは`job schedule cron create`コマンドを使用してジョブスケジュールを作成できます。["ONTAPコマンド リファレンス"](#)の`job schedule cron create`の詳細をご覧ください。

タスク概要

この手順は、FAS、AFF、およびASAシステムに適用されます。ASA r2システム (ASAA1K、ASAA90、ASAA70、ASAA50、ASAA30、ASAA20、またはASA C30) をお持ちの場合は、["これらの手順"](#)に従ってSnapshotジョブ スケジュールを作成してください。ASA r2システムは、SANのみのお客様向けに簡素化されたONTAPエクスペリエンスを提供します。

デフォルトでは、ONTAPはジョブ スケジュール名にタイムスタンプを追加してスナップショットの名前を作成します。

日付と曜日の両方の値を指定した場合、それぞれの値は独立して考慮されます。例えば、曜日の指定が`Friday`で日付の指定が`13`のcronスケジュールは、毎月13日の金曜日だけでなく、毎週金曜日と毎月13日に実行されます。

例 1. 手順

System Manager

1. 保護 > 概要 に移動し、ローカル ポリシー設定 を展開します。
2. スケジュール ペインで、➡をクリックします。
3. スケジュール ウィンドウで、+ Add をクリックします。
4. *スケジュールの追加*ウィンドウで、スケジュール名を入力し、コンテキストとスケジュール タイプを選択します。
5. *保存*をクリックします。

CLI

1. ジョブ スケジュールを作成します。

```
job schedule cron create -name <job_name> -month <month> -dayofweek  
<day_of_week> -day <day_of_month> -hour <hour> -minute <minute>
```

`-month`、`-dayofweek`、および `-hour` の場合、
`all` を指定して、それぞれ毎月、曜日ごと、および時間ごとにジョブを実行できます。

ONTAP 9.10.1以降では、ジョブ スケジュールにSVMを含めることができます。

```
job schedule cron create -name <job_name> -vserver <Vserver_name>  
-month <month> -dayofweek <day_of_week> -day <day_of_month> -hour  
<hour> -minute <minute>
```

次の例では、土曜日の午前3:00に実行される `myweekly` という名前のジョブ スケジュールを作成します。

```
cluster1::> job schedule cron create -name myweekly -dayofweek  
"Saturday" -hour 3 -minute 0
```

次の例では、`myweeklymulti` という名前のスケジュールを作成します。このスケジュールでは、複数の日、時間、分を指定します：

```
job schedule cron create -name myweeklymulti -dayofweek  
"Monday,Wednesday,Sunday" -hour 3,9,12 -minute 0,20,50
```

ONTAPスナップショットポリシーを作成する

スナップショットポリシーは、スナップショットを作成するタイミング、保持するコピーの数、およびスナップショットの名前を指定します。例えば、毎日午前0：10にスナップショットを1つ作成し、最新の2つのコピーを保持し、それぞれに「`daily.`timestamp.``」という名前を付けるといったことが可能です。スナップショットポリシーには、最大5つのジョブスケジュールを含めることができます。

タスク概要

この手順は、FAS、AFF、およびASAシステムに適用されます。ASA r2システム（ASAA1K、ASAA90、ASAA70、ASAA50、ASAA30、ASAA20、またはASA C30）をお持ちの場合は、["これらの手順"](#)に従ってSnapshotポリシーを作成してください。ASA r2システムは、SANのみのお客様向けに簡素化されたONTAPエクスペリエンスを提供します。

デフォルトでは、ONTAPはジョブ スケジュール名にタイムスタンプを追加してスナップショットの名前を作成します：

<code>daily.2017-05-14_0013/</code>	<code>hourly.2017-05-15_1106/</code>
<code>daily.2017-05-15_0012/</code>	<code>hourly.2017-05-15_1206/</code>
<code>hourly.2017-05-15_1006/</code>	<code>hourly.2017-05-15_1306/</code>

必要に応じて、プレフィックスをジョブ スケジュール名に置き換えることができます。

この ``snapmirror-label`` オプションはSnapMirrorレプリケーション用です。詳細については、["ポリシーのルール の定義"](#)を参照してください。

手順

スナップショット ポリシーは、System ManagerまたはONTAP CLIを使用して作成できます。この手順では、ローカル クラスタにのみスナップショット ポリシーが作成されます。

System Manager

1. 保護 > 概要 に移動し、ローカル ポリシー設定 を展開します。
2. スナップショット ポリシー ペインで、→をクリックします。
3. スナップショット ポリシー タブで、+ Add をクリックします。
4. *スナップショット ポリシーの追加*ウィンドウで、ポリシー名を入力し、スコープを選択します。
5. + Add をクリックします。
6. スケジュールを選択するには、現在表示されているスケジュール名をクリックし、▼をクリックして、別のスケジュールを選択します。
7. 保持するスナップショットの最大数を入力し、必要に応じてSnapMirrorラベルとSnapLock保持期間を入力します。
8. *保存*をクリックします。

CLI

1. スナップショット ポリシーを作成します：

```
volume snapshot policy create -vserver <SVM> -policy <policy_name>
-enabled true|false -schedule1 <schedule1_name> -count1
<copies_to_retain> -prefix1 <snapshot_prefix> -snapmirror-label1
<snapshot_label> ... -schedule5 <schedule5_name> -count5
<copies_to_retain> -prefix5 <snapshot_prefix> -snapmirror-label5
<snapshot_label>
```

次の例では、`snap_policy_daily` という名前のスナップショット ポリシーを作成します。このポリシーは `daily` スケジュールで実行されます。このポリシーには、それぞれ `daily.timestamp` という名前とSnapMirrorラベル `daily` を持つ最大5つのスナップショットが含まれます：

```
cluster1::> volume snapshot policy create -vserver vs0 -policy
snap_policy_daily -schedule1 daily -count1 5 -snapmirror-label1
daily
```

スナップショットを手動で管理する

手動でのSnapshotの作成と削除

スケジュールされたスナップショットが作成されるのを待てない場合は、手動でスナップショットを作成でき、不要になったスナップショットは削除できます。

タスク概要

この手順は FAS、AFF、および ASA システムに適用されます。ASA r2 システム（ASAA1K、ASAA90、ASAA70、ASAA50、ASAA30、ASAA20、または ASA C30）をご利用の場合は、[これらの手順](#)に従ってオンデマンド Snapshot を作成してください。ASA r2 システムは、SAN のみのお客様向けに簡素化された

ONTAP エクスペリエンスを提供します。

手動で**Snapshot**を作成する

System Manager または ONTAP CLI を使用して、スナップショットを手動で作成できます。

System Manager

手順

1. **Storage > Volumes** に移動し、**Snapshots** タブを選択します。
2. **+ Add** をクリックします。
3. *スナップショットの追加*ウィンドウで、デフォルトのスナップショット名をそのまま使用するか、必要に応じて編集します。
4. オプション：SnapMirrorラベルを追加します。
5. *[追加]*をクリックします。

CLI

1. スナップショットを作成します：

```
volume snapshot create -vserver <SVM> -volume <volume> -snapshot  
<snapshot_name>
```

スナップショットを手動で削除する

System Manager または ONTAP CLI を使用して、スナップショットを手動で削除できます。

System Manager

手順

1. ストレージ > ボリューム に移動し、 **Snapshot コピー** タブを選択します。
2. 削除したいスナップショットを見つけて、 をクリックし、*削除*を選択します。
3. *スナップショットの削除*ウィンドウで、*スナップショットの削除*を選択します。
4. *削除*をクリックします。

CLI

1. `volume snapshot show` コマンドを使用して、削除するSnapshotを確認します。

```
volume snapshot show -vserver <SVM> -volume <volume>
```

この例では、コマンドはSVM vs3のボリュームvol3上のSnapshotを表示します。

```
cluster::> volume snapshot show -vserver vs3 -volume vol3
```

Vserver	Volume	Snapshot	Size	---Blocks---	
				Total%	Used%
vs3	vol3				
		snap1.2013-05-01_0015	100KB	0%	38%
		snap1.2013-05-08_0015	76KB	0%	32%
		snap2.2013-05-09_0010	76KB	0%	32%
		snap2.2013-05-10_0010	76KB	0%	32%
		snap3.2013-05-10_1005	72KB	0%	31%
		snap3.2013-05-10_1105	72KB	0%	31%
		snap3.2013-05-10_1205	72KB	0%	31%
		snap3.2013-05-10_1305	72KB	0%	31%
		snap3.2013-05-10_1405	72KB	0%	31%
		snap3.2013-05-10_1505	72KB	0%	31%

10 entries were displayed.

2. スナップショットを削除します：

状況	コマンド
単一のSnapshotを削除する	<pre>volume snapshot delete -vserver _svm_name_ -volume _vol_name_ -snapshot _snapshot_name_</pre>

状況	コマンド
複数のスナップショットを削除する	<pre>volume snapshot delete -vserver _svm_name_ -volume _vol_name_ -snapshot _snapshot_name1_[,_snapshot_nam e2_,...]</pre>
すべてのSnapshotを削除する	<pre>volume snapshot delete -vserver _svm_name_ -volume _vol_name_ -snapshot *</pre>

Snapshotを削除する前に再利用可能なスペースを計算する

ONTAP 9.10.1 以降では、System Manager を使用して、削除するスナップショットを選択し、削除する前に再利用可能なスペースを計算できます。

手順

1. *[ストレージ]>[ボリューム]*をクリックします。
2. Snapshotを削除するボリュームを選択します。
3. *Snapshot*をクリックします。
4. 1つ以上のSnapshotを選択します。
5. *Calculate Reclaimable Space*をクリックします。

Snapshotリザーブの管理

ONTAPスナップショット リザーブの管理について学ぶ

スナップショット予約 は、スナップショット用にディスク容量の一定割合（デフォルトでは5%）を確保します。スナップショット予約が使い果たされると、スナップショットはアクティブ ファイル システムの領域を使用するため、必要に応じてスナップショット予約を増やすことができます。また、予約がいっぱいになったときにスナップショットを自動的に削除することもできます。

Snapshotリザーブを増やすタイミング

スナップショットの予約容量を増やすかどうかを決める際には、スナップショットは前回のスナップショット作成以降のファイルの変更のみを記録することを覚えておくことが重要です。アクティブ ファイル システム内のブロックが変更または削除された場合にのみ、ディスク容量が消費されます。

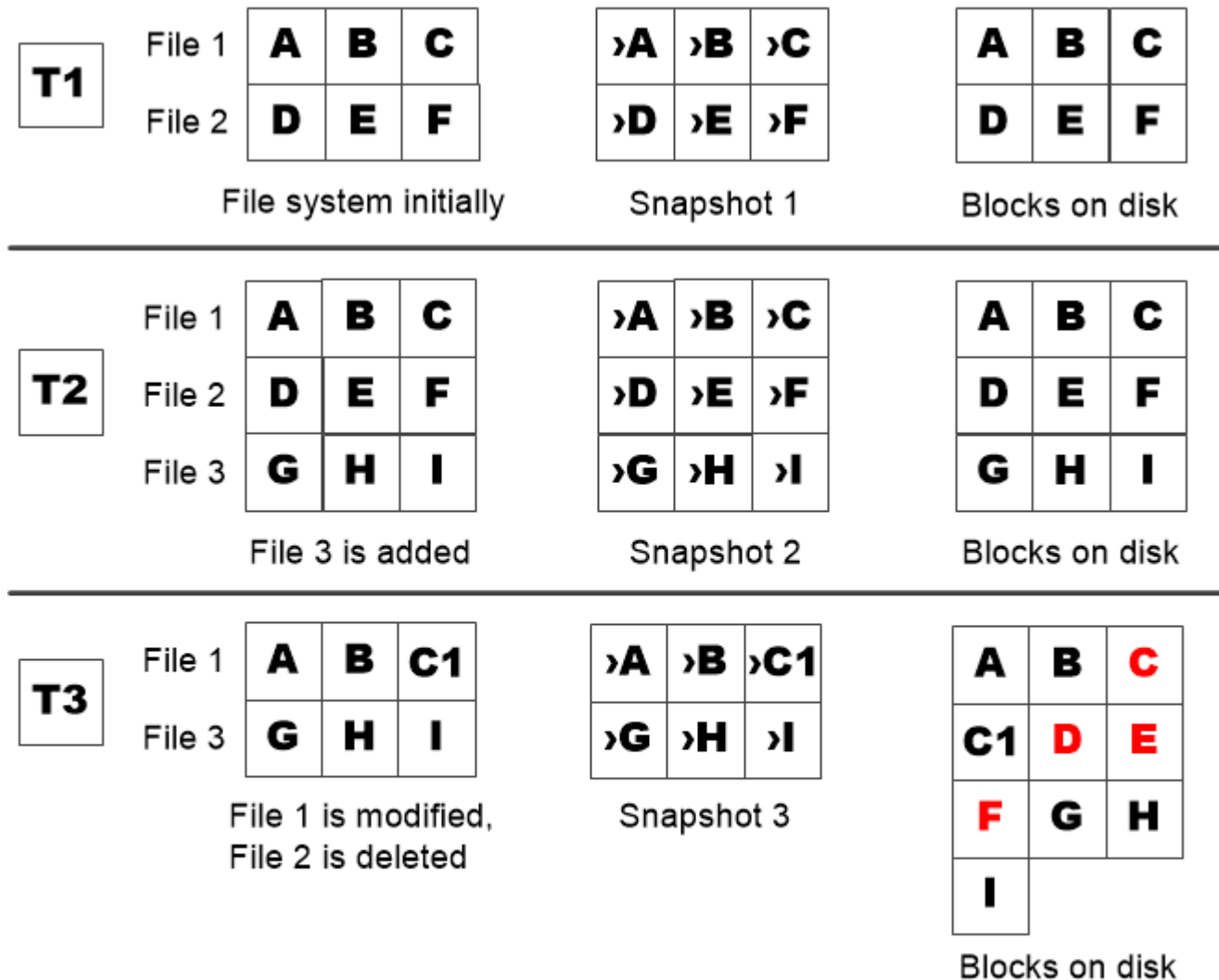
つまり、ファイル システムの変更率は、スナップショットが使用するディスク容量を決定する上で重要な要

素となります。アクティブ ファイル システムに変更がなければ、スナップショットをいくつ作成してもディスク容量は消費されません。

データベース トランザクション ログを含むFlexVol volumeは、例えば、変更頻度が高いため、スナップショットの予約領域を最大20%に設定する場合があります。データベースへの更新頻度が高いほど、より多くのスナップショットを作成する必要があるだけでなく、スナップショットが消費する追加のディスク容量に対応するために、より大きなスナップショット予約領域を設定することも必要になります。



スナップショットは、ブロックのコピーではなく、ブロックへのポインタで構成されます。ポインタはブロックに対する「権利」と考えることができます：ONTAPはスナップショットが削除されるまでブロックを「保持」します。



A Snapshot copy consumes disk space only when blocks in the active file system are modified or deleted.

保護対象のファイルを削除することで想定よりもファイル スペースが少なくなる仕組み

スナップショットは、ブロックを使用していたファイルを削除した後でも、そのブロックを参照します。そのため、スナップショットの予約領域を使い果たすと、ファイルシステム全体を削除したときに、ファイルシステムが占有していた領域よりも利用可能な領域が少なくなるという、直感に反する結果が生じる可能性があります。

ます。

次の例を考えてみましょう。ファイルを削除する前の `df` コマンド出力は次のようになります：

```
Filesystem      kbytes  used   avail  capacity
/vol/vol10/     3000000 3000000 0        100%
/vol/vol10/.snapshot 1000000 500000  500000   50%
```

ファイル システム全体を削除し、ボリュームのスナップショットを作成した後、`df` コマンドは次の出力を生成します：

```
Filesystem      kbytes  used   avail  capacity
/vol/vol10/     3000000 2500000 500000   83%
/vol/vol10/.snapshot 1000000 3500000 0        350%
```

出力に示されているように、削除前に使用されていた 0.5 GB に加えて、以前アクティブ ファイル システムで使用されていた 3 GB 全体が現在スナップショットによって使用されています。

スナップショットによって使用されるディスク領域がスナップショット予約領域を超えるため、2.5 GB のオーバーフローがアクティブ ファイル用に予約された領域に「あふれ」、ファイル用に 3 GB の空き領域が期待される場所に 0.5 GB の空き領域が残ります。

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

ONTAP スナップショットディスク消費量を監視する

`df` コマンドを使用して、スナップショットのディスク消費量を監視できます。このコマンドは、アクティブ ファイル システムとスナップショット リザーブの空き容量を表示します。

手順

1. スナップショットのディスク消費量を表示します： `df`

次の例は、スナップショットのディスク消費量を示しています：

```
cluster1::> df
Filesystem      kbytes  used   avail  capacity
/vol/vol10/     3000000 3000000 0        100%
/vol/vol10/.snapshot 1000000 500000  500000   50%
```

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

ボリューム上の利用可能なONTAP Snapshotリザーブを確認する

`volume show`コマンドで `snapshot-reserve-available`パラメータを使用して、ボリューム上で利用可能なSnapshotリザーブの量を確認できます。link:<https://docs.netapp.com/us-en/ontap-cli/volume-show.html>["ONTAPコマンド リファレンス"]の `volume show`の詳細をご覧ください。

手順

1. ボリュームで使用可能なSnapshotリザーブを確認します：

```
vol show -vserver SVM -volume volume -fields snapshot-reserve-available
```

次の例では、`vol1`の使用可能なSnapshotリザーブを表示します：

```
cluster1::> vol show -vserver vs0 -volume vol1 -fields snapshot-reserve-
available

vserver volume snapshot-reserve-available
-----
vs0      vol1      4.84GB
```

ONTAPスナップショット リザーブを変更する

スナップショットがアクティブ ファイル システム用に予約されたスペースを使用しないようにするために、より大きなSnapshot リザーブを設定することを推奨します。スナップショット用のスペースがそれほど必要でなくなった場合は、Snapshot リザーブを減らすことができます。

手順

1. Snapshotリザーブを変更します：

```
volume modify -vserver SVM -volume volume -percent-snapshot-space snap_reserve
```

`volume modify`の詳細については、link:<https://docs.netapp.com/us-en/ontap-cli/volume-modify.html>["ONTAPコマンド リファレンス"]をご覧ください。

次の例では、`vol1`のスナップショット リザーブを10パーセントに設定します：

```
cluster1::> volume modify -vserver vs0 -volume vol1 -percent-snapshot
-space 10
```

ONTAPスナップショットの自動削除

`volume snapshot autodelete modify` コマンドを使用すると、Snapshotリザーブを超えた場合にスナップショットの自動削除をトリガーできます。デフォルトでは、最も古いスナップショットが最初に削除されます。link:<https://docs.netapp.com/us-en/ontap-cli/volume-snapshot-autodelete-modify.html> ["ONTAPコマンドリファレンス"] の `volume snapshot autodelete modify` の詳細をご覧ください。

タスク概要

削除するSnapshotがなくなると、LUNとファイルのクローンも削除されます。

手順

1. スナップショットの自動削除：

```
volume snapshot autodelete modify -vserver SVM -volume volume -enabled true|false -trigger volume|snap_reserve
```

次の例では、Snapshotリザーブが使い果たされた場合に `vol1` のSnapshotを自動的に削除します：

```
cluster1::> volume snapshot autodelete modify -vserver vs0 -volume vol1 -enabled true -trigger snap_reserve
```

Snapshotからファイルをリストアする

NFSまたは**SMB**クライアント上の**ONTAP**スナップショットからファイルを復元する

NFSまたはSMBクライアント上のユーザーは、ストレージ システム管理者の介入なしに、スナップショットから直接ファイルをリストアできます。

ファイル システム内のすべてのディレクトリには、`.snapshot` という名前のサブディレクトリが含まれており、NFSおよびSMBユーザーがアクセスできます。`.snapshot` サブディレクトリには、ボリュームのSnapshotに対応するサブディレクトリが含まれています。

```
$ ls .snapshot
daily.2017-05-14_0013/      hourly.2017-05-15_1106/
daily.2017-05-15_0012/      hourly.2017-05-15_1206/
hourly.2017-05-15_1006/     hourly.2017-05-15_1306/
```

各サブディレクトリには、スナップショットが参照するファイルが含まれています。ユーザーが誤ってファイルを削除または上書きした場合、スナップショット サブディレクトリから読み書き可能なディレクトリにファイルをコピーすることで、親の読み書き可能なディレクトリにファイルを復元できます：

```
$ ls my.txt
ls: my.txt: No such file or directory
$ ls .snapshot
daily.2017-05-14_0013/          hourly.2017-05-15_1106/
daily.2017-05-15_0012/          hourly.2017-05-15_1206/
hourly.2017-05-15_1006/        hourly.2017-05-15_1306/
$ ls .snapshot/hourly.2017-05-15_1306/my.txt
my.txt
$ cp .snapshot/hourly.2017-05-15_1306/my.txt .
$ ls my.txt
my.txt
```

ONTAPスナップショット ディレクトリへの**NFS**および**SMB**クライアント アクセスを有効または無効にする

ONTAP CLI `snapdir-access` オプションを使用して、`volume modify` コマンドでスナップショット ディレクトリへのアクセスを有効または無効にすることができます。また、ONTAP 9.10.1以降では、System Managerを使用して、クライアント システムによるボリューム上のスナップショット ディレクトリへのアクセスを有効または無効にすることができます。アクセスを有効にすると、スナップショット ディレクトリがクライアントに表示されるようになり、Windowsクライアントはスナップショット ディレクトリにドライブをマッピングして、その内容を表示およびアクセスできるようになります。その後、NFSクライアントとSMBクライアントは、スナップショットからファイルまたはLUNをリストアできます。

ボリューム設定を編集するか、ボリュームの共有設定を編集することで、ボリュームのスナップショット ディレクトリへのアクセスを有効または無効にすることができます。

ボリュームを編集して**Snapshot**ディレクトリへのクライアント アクセスを有効または無効にする

手順

ONTAP System ManagerまたはONTAP CLIを使用して、クライアントのスナップショット ディレクトリへのアクセスを有効または無効にすることができます。ボリューム上のスナップショット ディレクトリは、デフォルトでクライアントからアクセス可能です。

System Manager

1. *[ストレージ]>[ボリューム]*をクリックします。
2. 表示または非表示にするスナップショット ディレクトリを含むボリュームを選択します。
3.  をクリックして*編集*を選択します。
4. **Snapshot (Local) Settings** セクションで、**Show the Snapshot directory to clients** を選択または選択解除します。
5. *保存*をクリックします。

CLI

1. スナップショット ディレクトリのアクセス ステータスを確認します：

```
volume show -vserver <SVM_name> -volume <vol_name> -fields snapdir-  
access
```

例：

```
clus1::> volume show -vserver vs0 -volume vol1 -fields snapdir-  
access  
vserver volume snapdir-access  
-----  
vs0      vol1    false
```

`volume show`の詳細については、[link:https://docs.netapp.com/us-en/ontap-cli/volume-show.html](https://docs.netapp.com/us-en/ontap-cli/volume-show.html)["ONTAPコマンド リファレンス"]をご覧ください。

2. Snapshot ディレクトリ アクセスを有効または無効にします：

```
volume modify -vserver <SVM_name> -volume <vol_name> -snapdir-access  
<true|false>
```

次の例では、vol1 のスナップショット ディレクトリ アクセスを有効にします：

```
clus1::> volume modify -vserver vs0 -volume vol1 -snapdir-access  
true  
Volume modify successful on volume vol1 of Vserver vs0.
```

``volume modify``の詳細については、link:<https://docs.netapp.com/us-en/ontap-cli/volume-modify.html>["ONTAPコマンド リファレンス"]をご覧ください。

共有を編集して**Snapshot**ディレクトリへのクライアントアクセスを有効または無効にする

ボリューム上のスナップショット ディレクトリは、デフォルトでクライアントからアクセスできます。

手順

1. ***Storage > Shares***をクリックします。
2. 表示または非表示にするスナップショット ディレクトリを含むボリュームを選択します。
3.  をクリックして***編集***を選択します。
4. ***共有プロパティ***セクションで、***クライアントに Snapshot ディレクトリへのアクセスを許可する***を選択または選択解除します。
5. ***保存***をクリックします。

ONTAPスナップショットから単一のファイルを復元する

``volume snapshot restore-file``コマンドを使用して、Snapshot から単一のファイルまたはLUNを復元できます。既存のファイルを置き換えたくない場合は、親の読み取り / 書き込みボリューム内の別の場所にファイルを復元できます。

タスク概要

既存のLUNを復元する場合は、LUNクローンが作成され、スナップショット形式でバックアップされます。復元操作中は、LUNの読み取りと書き込みが可能です。

デフォルトでは、ストリームを含むファイルがリストアされます。

手順

1. ボリューム内のスナップショットを一覧表示します：

```
volume snapshot show -vserver SVM -volume volume
```

``volume snapshot show``の詳細については、link:<https://docs.netapp.com/us-en/ontap-cli/volume-snapshot-show.html>["ONTAPコマンド リファレンス"]を参照してください。

次の例は、``vol1``のスナップショットを示しています：

```
clus1::> volume snapshot show -vserver vs1 -volume vol1
```

Vserver	Volume	Snapshot	State	Size	Total%	Used%
vs1	vol1	hourly.2013-01-25_0005	valid	224KB	0%	0%
		daily.2013-01-25_0010	valid	92KB	0%	0%
		hourly.2013-01-25_0105	valid	228KB	0%	0%
		hourly.2013-01-25_0205	valid	236KB	0%	0%
		hourly.2013-01-25_0305	valid	244KB	0%	0%
		hourly.2013-01-25_0405	valid	244KB	0%	0%
		hourly.2013-01-25_0505	valid	244KB	0%	0%

7 entries were displayed.

2. スナップショットからファイルを復元します：

```
volume snapshot restore-file -vserver SVM -volume volume -snapshot snapshot  
-path file_path -restore-path destination_path
```

```
`volume snapshot restore-file`
```

の詳細については、[link:https://docs.netapp.com/us-en/ontap-cli/volume-snapshot-restore-file.html](https://docs.netapp.com/us-en/ontap-cli/volume-snapshot-restore-file.html)["ONTAPコマンド リファレンス"]を参照してください。

次の例では、ファイル `myfile.txt` を復元します：

```
cluster1::> volume snapshot restore-file -vserver vs0 -volume vol1  
-snapshot daily.2013-01-25_0010 -path /myfile.txt
```

ONTAPスナップショットからファイルの一部を復元する

この `volume snapshot partial-restore-file` コマンドを使用すると、データの開始バイトオフセットとバイト数がわかっている場合、スナップショットからLUN、NFSまたはSMBコンテナファイルに一定範囲のデータをリストアできます。このコマンドは、同じLUNに複数のデータベースを保存しているホスト上のデータベースの1つをリストアする場合に使用できます。

ONTAP 9.12.1以降では、[SnapMirrorアクティブ同期](#)を使用するボリュームに対して部分的な復元が可能です。

手順

1. ボリューム内のスナップショットを一覧表示します：

```
volume snapshot show -vserver SVM -volume volume
```

`volume snapshot show`の詳細については、link:<https://docs.netapp.com/us-en/ontap-cli/volume-snapshot-show.html>["ONTAPコマンド リファレンス"]を参照してください。

次の例は、`vol1`のスナップショットを示しています：

```
clus1::> volume snapshot show -vserver vs1 -volume vol1
```

Vserver	Volume	Snapshot	State	Size	Total%	Used%
vs1	vol1	hourly.2013-01-25_0005	valid	224KB	0%	0%
		daily.2013-01-25_0010	valid	92KB	0%	0%
		hourly.2013-01-25_0105	valid	228KB	0%	0%
		hourly.2013-01-25_0205	valid	236KB	0%	0%
		hourly.2013-01-25_0305	valid	244KB	0%	0%
		hourly.2013-01-25_0405	valid	244KB	0%	0%
		hourly.2013-01-25_0505	valid	244KB	0%	0%

7 entries were displayed.

2. スナップショットからファイルの一部を復元します：

```
volume snapshot partial-restore-file -vserver SVM -volume volume -snapshot snapshot -path file_path -start-byte starting_byte -byte-count byte_count
```

開始バイト オフセットとバイト数は4,096の倍数である必要があります。

次の例では、ファイル `myfile.txt` の最初の 4,096 バイトを復元します：

```
cluster1::> volume snapshot partial-restore-file -vserver vs0 -volume vol1 -snapshot daily.2013-01-25_0010 -path /myfile.txt -start-byte 0 -byte-count 4096
```

ONTAPスナップショットからボリュームの内容を復元する

スナップショットから復元することで、ボリュームを以前の時点に復元できます。System Managerまたは `volume snapshot restore` コマンドを使用して、スナップショットからボリュームの内容を復元できます。["ONTAPコマンド リファレンス"](#)の `volume snapshot restore` の詳細をご覧ください。

タスク概要

ボリュームにSnapMirror関係が設定されている場合は、Snapshotからリストアしたあと、すぐにボリュームのすべてのミラー コピーを手動でレプリケートします。レプリケートしないと、ミラー コピーを使用できなくなり、削除および再作成が必要になることがあります。

System Manager またはONTAP CLIを使用して、以前のSnapshotから復元できます。

System Manager

1. *[ストレージ]*をクリックし、ボリュームを選択します。
2. *Snapshotコピー*で、復元するSnapshotの横にある  をクリックし、*復元*を選択します。

CLI

1. ボリューム内のスナップショットを一覧表示します：

```
volume snapshot show -vserver <SVM> -volume <volume>
```

次の例は、`vol1`のスナップショットを示しています：

```
clus1::> volume snapshot show -vserver vs1 -volume vol1
```

Vserver	Volume	Snapshot	State	Size	Total%	Used%
-----	-----	-----	-----	-----	-----	-----
vs1	vol1	hourly.2013-01-25_0005	valid	224KB	0%	0%
		daily.2013-01-25_0010	valid	92KB	0%	0%
		hourly.2013-01-25_0105	valid	228KB	0%	0%
		hourly.2013-01-25_0205	valid	236KB	0%	0%
		hourly.2013-01-25_0305	valid	244KB	0%	0%
		hourly.2013-01-25_0405	valid	244KB	0%	0%
		hourly.2013-01-25_0505	valid	244KB	0%	0%

7 entries were displayed.

2. スナップショットからボリュームの内容を復元します：

```
volume snapshot restore -vserver <SVM> -volume <volume> -snapshot  
<snapshot>
```

次の例では、`vol1`の内容を復元します：

```
cluster1::> volume snapshot restore -vserver vs0 -volume vol1  
-snapshot daily.2013-01-25_0010
```

SnapMirrorボリューム レプリケーション

SnapMirrorボリュームレプリケーションについて学ぶ

ONTAP SnapMirror非同期ディザスタリカバリについて学ぶ

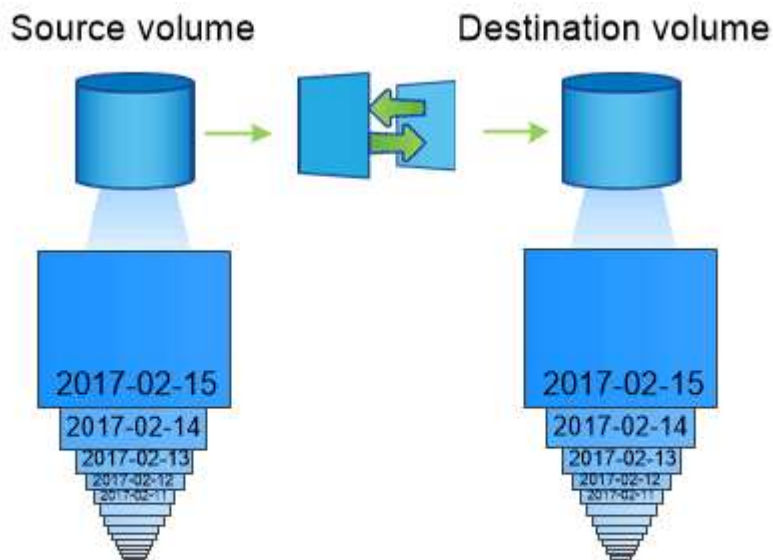
SnapMirror は、地理的に離れたサイトにあるプライマリ ストレージからセカンダリ システムへのフェイルオーバーを目的とした災害復旧テクノロジーです。その名の通り、*SnapMirror*はセカンダリ ストレージに作業データのレプリカ（ミラー）を作成します。プライマリ サイトで災害が発生した場合でも、このミラーから引き続きデータを提供できます。

プライマリ サイトがまだデータを提供できる状態であれば、必要なデータをプライマリ サイトに転送するだけで、ミラー サイトからのクライアントへのデータ提供は一切不要になります。フェイルオーバーのユースケースからもわかるように、セカンダリ システムのコントローラーは、ミラー ストレージから効率的にデータを提供するために、プライマリ システムのコントローラーと同等、またはほぼ同等である必要があります。

データ保護関係

データはボリュームレベルでミラーリングされます。プライマリストレージのソースボリュームとセカンダリストレージのデスティネーションボリュームの関係は、データ保護関係と呼ばれます。ボリュームが存在するクラスタと、ボリュームからデータを提供するSVMは、**"ピア関係にある"**必要があります。ピア関係により、クラスタとSVMは安全にデータを交換できます。

この図はSnapMirrorデータ保護関係を示しています：



A SnapMirror data protection relationship typically mirrors the Snapshot copies available on the source volume.

データ保護関係の範囲

データ保護関係は、ボリューム間またはボリュームを所有するSVM間で直接作成できます。_SVMデータ保護

関係_では、NFSエクスポート、SMB共有、RBACなど、SVM設定のすべてまたは一部がレプリケートされ、SVMが所有するボリューム内のデータもレプリケートされます。

次に示す特殊なデータ保護アプリケーションにSnapMirrorを使用することもできます。

- SVMルート ボリュームの_負荷共有ミラー_ コピーにより、ノードの停止やフェイルオーバーが発生した場合でもデータへのアクセスが維持されます。
- _SnapLock ボリューム_間のデータ保護関係により、WORM ファイルをセカンダリ ストレージにレプリケートできます。

"SnapLockテクノロジーを使用したアーカイブとコンプライアンス"

- ONTAP 9.13.1以降では、SnapMirror非同期レプリケーションを使用して[整合性グループ](#)を保護できます。ONTAP 9.14.1以降では、SnapMirror非同期レプリケーションを使用して、整合性グループ関係によりボリューム単位のスナップショットをデスティネーション クラスタにレプリケートできます。詳細については、[SnapMirror非同期保護を構成する](#)を参照してください。

SnapMirrorデータ保護関係を初期化する方法

SnapMirrorを初めて起動すると、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_が実行されます。関係の_SnapMirrorポリシー_によって、ベースラインの内容と更新内容が定義されます。

デフォルトのSnapMirrorポリシーによるベースライン転送には MirrorAllSnapshots、次の手順が含まれます：

- ソースボリュームのスナップショットを作成します。
- スナップショットとそれが参照するすべてのデータ ブロックを宛先ボリュームに転送します。
- 「active」ミラーが破損した場合に備えて、ソース ボリュームに残っている、それほど新しくないスナップショットを宛先ボリュームに転送します。

SnapMirrorデータ保護関係を更新する方法

更新は非同期で、設定したスケジュールに従って行われます。保持期間はソースのSnapshotポリシーを反映します。

``MirrorAllSnapshots``ポリシーに基づく更新のたびに、SnapMirrorはソースボリュームのスナップショットを作成し、そのスナップショットと前回の更新以降に作成されたスナップショットを転送します。 ``MirrorAllSnapshots``ポリシーの ``snapmirror policy show`` コマンドからの次の出力では、次の点に注意してください：

- `Create Snapshot``が「``true``」の場合、``MirrorAllSnapshots``がSnapMirror関係を更新するときにスナップショットを作成することを示します。
- ``MirrorAllSnapshots``には、ルール“sm_created”と“all_source_snapshots”があり、SnapMirrorによって作成されたスナップショットと、最後の更新以降に作成されたスナップショットの両方が、SnapMirrorが関係を更新するときに転送されることを示します。

```
cluster_dst:> snapmirror policy show -policy MirrorAllSnapshots -instance

Vserver: vs0
SnapMirror Policy Name: MirrorAllSnapshots
SnapMirror Policy Type: async-mirror
Policy Owner: cluster-admin
Tries Limit: 8
Transfer Priority: normal
Ignore accesstime Enabled: false
Transfer Restartability: always
Network Compression Enabled: false
Create Snapshot: true
Comment: SnapMirror asynchronous policy for mirroring
all snapshots
and the latest active file system.
Total Number of Rules: 2
Total Keep: 2
Rules: SnapMirror Label      Keep  Preserve Warn
Schedule Prefix
-----
sm_created                  1  false      0 -
all_source_snapshots       1  false      0 -
```

MirrorLatestポリシー

事前設定された `MirrorLatest` ポリシーは `MirrorAllSnapshots` とまったく同じように動作しますが、初期化および更新時に SnapMirror によって作成されたスナップショットのみが転送される点が異なります。

```
Rules: SnapMirror Label      Keep  Preserve Warn
Schedule Prefix
-----
sm_created                  1  false      0 -
```

関連情報

- ["snapmirror policy show"](#)

ONTAP SnapMirror同期ディザスタリカバリについて学ぶ

ONTAP 9.5以降では、16GB以上のメモリを搭載したすべてのFASプラットフォーム

とAFFプラットフォーム、およびすべてのONTAP SelectプラットフォームでSnapMirror同期（SM-S）テクノロジーがサポートされます。SnapMirror同期テクノロジーはノード単位でライセンスされる機能で、ボリューム レベルの同期データ レプリケーションを提供します。

この機能を使用すると、データ損失ゼロが求められる金融や医療などの業種で、同期レプリケーションに関する規制や国の規定に対応できます。

許可される**SnapMirror**同期の処理

SnapMirror同期レプリケーションのHAペアあたりの最大処理数は、コントローラのモデルによって異なります。

次の表は、1つのHAペアで許可されるSnapMirror同期処理の最大数をプラットフォーム タイプとONTAPのリリース別に示しています。

プラットフォーム	ONTAP 9.14.1からONTAP 9.11.1	ONTAP 9.10.1	ONTAP 9.9.1	ONTAP 9.9.1より前のリリース
AFF	400	200	160	80
ASA	400	200	160	80
FAS	80	80	80	40
ONTAP Select	40	40	40	20

サポートされる機能

次の表に、SnapMirror同期でサポートされる機能と、サポートが提供されるONTAPリリースを示します。

機能	最初にサポートされたリリース	追加情報
SnapMirror同期関係のプライマリ ボリュームに対するウイルス対策	ONTAP 9.6	
アプリケーションで作成されたSnapshotのレプリケーション	ONTAP 9.7	`snapshot create`操作時にCLIまたはONTAP APIを使用してスナップショットに適切なラベルが付けられている場合、SnapMirror同期レプリケーションは、アプリケーションを静止させた後、ユーザーが作成したスナップショットと外部スクリプトで作成されたスナップショットの両方を同期的にレプリケートします。スナップショット ポリシーを使用して作成されたスケジュールされたスナップショットはレプリケートされません。アプリケーション作成スナップショットのレプリケーションの詳細については、" NetAppナレッジベース：アプリケーションが作成したスナップショットをSnapMirror同期的に複製する方法 "を参照してください。

クローンの自動削除	ONTAP 9.6	
階層化ポリシーが「None」、「Snapshot」、「Auto」のいずれかに設定されたFabricPoolアグリゲートがSnapMirror同期のソースとデスティネーションでサポートされます。	ONTAP 9.5	FabricPoolアグリゲート内のデスティネーション ボリュームに「All」階層化ポリシーを設定することはできません。
FC	ONTAP 9.5	すべてのネットワークでレイテンシが10ミリ秒以内に抑えられます。
FC-NVMe	ONTAP 9.7	
ファイルのクローン	ONTAP 9.7	
SnapMirror同期関係のプライマリ ボリュームに対するFPolicy	ONTAP 9.6	
SnapMirror同期関係のプライマリ ボリュームに対するハード クォータおよびソフト クォータ	ONTAP 9.6	クォータ ルールはデスティネーションにレプリケートされないため、クォータ データベースはデスティネーションにレプリケートされません。
クラスタ内同期関係	ONTAP 9.14.1	ソース ボリュームとデスティネーション ボリュームを異なるHAペアに配置することで、高可用性が実現されます。クラスタ全体がダウンした場合、クラスタが回復するまでボリュームにアクセスできなくなります。クラスタ内SnapMirror同期関係は、同時 HAペアごとの関係 の全体的な制限に影響します。
iSCSI	ONTAP 9.5	
LUNクローンとNVMeネームスペースクローン	ONTAP 9.7	
アプリケーションが作成したSnapshotでバックアップされたLUNクローン	ONTAP 9.7	
混在プロトコル アクセス（NFS v3とSMB）	ONTAP 9.6	
NDMP / NDMPのリストア	ONTAP 9.13.1	ソース クラスタとデスティネーション クラスタの両方で、SnapMirror SynchronousでNDMPを使用するにはONTAP 9.13.1以降を実行している必要があります。詳細については、 ndmpコピーを使用してデータを転送する を参照してください。
AFF / ASAプラットフォームでのみ実行できる無停止のSnapMirror同期処理（NDO）。	ONTAP 9.12.1	ノンストップ オペレーションがサポートされることで、ダウンタイムを予定することなく多くの代表的なメンテナンス作業を実行できます。サポートされる処理にはテイクオーバーとギブバック、およびボリューム移動があり、2つのクラスタ間で1つのノードが稼働しているかぎりこれらの処理を実行できます。
NFS v4.2	ONTAP 9.10.1	
NFS v4.0	ONTAP 9.6	
NFS v4.1	ONTAP 9.6	
NVMe/TCP	9.10.1	

メタデータ処理頻度の上限の削除	ONTAP 9.6	
TLS 1.2暗号化を使用した機密データ転送時のセキュリティ	ONTAP 9.6	
単一ファイルのリストアとファイルの部分リストア	ONTAP 9.13.1	
SMB 2.0以降	ONTAP 9.6	
SnapMirror同期ミラー-ミラー カスケード	ONTAP 9.6	SnapMirror同期関係のデスティネーション ボリュームからの関係はSnapMirror非同期関係である必要があります。
SVMディザスタ リカバリ	ONTAP 9.6	* SnapMirror同期ソースは、SVMディザスタ リカバリソースになることもできます。たとえば、SnapMirror同期を一方のレッグとし、SVMディザスタ リカバリをもう一方のレッグとするファンアウト構成などです。* SnapMirror同期はデータ保護ソースのカスケードをサポートしていないため、SnapMirror同期ソースをSVMディザスタ リカバリ デスティネーションにすることはできません。デスティネーション クラスタでSVMディザスタ リカバリのフリップ再同期を実行する前に、同期関係を解放する必要があります。* SVMディザスタ リカバリはDPボリュームのレプリケーションをサポートしていないため、SnapMirror同期デスティネーションをSVMディザスタ リカバリ ソースにすることはできません。同期ソースのフリップ再同期を実行すると、SVMディザスタ リカバリによってデスティネーション クラスタのDPボリュームが除外されます。
ソース ボリュームへのテープベースのリストア	ONTAP 9.13.1	
NASのソース ボリュームとデスティネーション ボリュームの間のタイムスタンプ パリティ	ONTAP 9.6	ONTAP 9.5からONTAP 9.6にアップグレードした場合、タイムスタンプはソース ボリューム内の新規または変更されたファイルについてのみレプリケートされます。ソース ボリューム内の既存のファイルのタイムスタンプは同期されません。

サポートされない機能

SnapMirror同期関係では、次の機能はサポートされません。

- 自律型ランサムウェア対策
- 整合性グループ
- DP_Optimized (DPO) システム
- FlexGroupボリューム
- FlexCacheボリューム
- グローバル スロットル
- ファンアウト構成で確立できるSnapMirror同期関係は1つだけで、ソース ボリュームからの残りの関係はすべてSnapMirror非同期関係にする必要がある。

- LUNの移動
- MetroCluster構成
- 同じボリュームまたはSVMでは、SANとNVMeアクセスLUNおよびNVMe名前空間の混在はサポートされません。
- SnapCenter
- SnapLockボリューム
- 改ざん防止スナップショット
- デスティネーション ボリュームでのダンプおよびSMTapeを使用したテープ バックアップまたはリストア
- ソース ボリュームのしきい値の下限（最小QoS）
- ボリュームのSnapRestore
- VVol

動作モード

SnapMirror同期には、使用するSnapMirrorポリシーに基づいて2つの動作モードがあります。

- **同期モード** 同期モードでは、アプリケーションのI/O操作はプライマリ ストレージ システムとセカンダリ ストレージ システムに並列に送信されます。何らかの理由でセカンダリ ストレージへの書き込みが完了しなかった場合、アプリケーションはプライマリ ストレージへの書き込みを続行できます。エラー状態が修正されると、SnapMirror同期テクノロジはセカンダリ ストレージと自動的に再同期し、プライマリ ストレージからセカンダリ ストレージへのレプリケーションを同期モードで再開します。同期モードでは、セカンダリ レプリケーションに障害が発生するまではRPO=0でRTOは非常に低くなりますが、セカンダリ レプリケーションに障害が発生するとRPOとRTOは不確定になります。ただし、セカンダリ レプリケーションの障害原因を修復し、再同期を完了するまでの時間はRPOとRTOに等しくなります。
- **StrictSyncモード** SnapMirror同期は、オプションでStrictSyncモードで動作できます。何らかの理由でセカンダリ ストレージへの書き込みが完了しなかった場合、アプリケーションI/Oは失敗し、プライマリ ストレージとセカンダリ ストレージの同一性が確保されます。プライマリへのアプリケーションI/Oは、SnapMirror関係が`InSync`ステータスに戻った後にのみ再開されます。プライマリ ストレージに障害が発生した場合、フェイルオーバー後にセカンダリ ストレージでアプリケーションI/Oを再開でき、データ損失はありません。StrictSyncモードでは、RPOは常にゼロであり、RTOは非常に低くなります。

関係のステータス

SnapMirror同期関係のステータスは、通常動作中は常に`InSync`ステータスです。何らかの理由でSnapMirror転送が失敗した場合、デスティネーションはソースと同期していないため、`OutofSync`ステータスになる可能性があります。

SnapMirror同期関係の場合、システムは一定の間隔で関係のステータス（`InSync`または`OutofSync`）を自動的にチェックします。関係のステータスが`OutofSync`の場合、ONTAPは自動再同期プロセスを自動的にトリガーし、関係を`InSync`ステータスに戻します。自動再同期は、ソースまたはデスティネーションでの計画外のストレージフェイルオーバーやネットワーク障害など、何らかの操作が原因で転送が失敗した場合のみトリガーされます。`snapmirror quiesce`や`snapmirror break`などのユーザによる操作では、自動再同期はトリガーされません。

StrictSyncモードのSnapMirror同期関係で関係ステータスが`OutofSync`になると、プライマリボリュームへのすべてのI/O操作が停止されます。SyncモードのSnapMirror同期関係で`OutofSync`状態になっても、プライマリには影響がなく、プライマリボリュームでI/O操作が許可されます。

関連情報

- ["NetAppテクニカル レポート4733：SnapMirror同期構成とベストプラクティス"](#)
- ["snapmirror break"](#)
- ["snapmirror quiesce"](#)

デフォルトのONTAPデータ保護ポリシー

ONTAPには、データ保護関係に使用できるデフォルトの保護ポリシーがいくつか用意されています。使用するポリシーは保護関係タイプによって異なります。

デフォルトのポリシーがデータ保護関係のニーズを満たさない場合は、["カスタム ポリシーを作成する"](#)ができます。

デフォルトの保護ポリシーと説明の一覧

デフォルトの保護ポリシーとそれに関連付けられているポリシー タイプを以下に示します。

Name	概要	ポリシータイプ
非同期	最新のアクティブ ファイルシステムと日単位および週単位のSnapshotを時間単位の転送スケジュールでミラーリングするための、ユニファイドSnapMirror非同期およびバックアップ ポリシー	非同期
AutomatedFailOver	レプリケーションに失敗してもクライアントI/Oが中断されない、RTOゼロ保証のSnapMirror同期用ポリシー	同期
AutomatedFailOverDuplex	RTOゼロ保証と双方向同期レプリケーションを備えたSnapMirror同期用ポリシー	同期
CloudBackupDefault	日単位ルールを使用したバックアップ ポリシー	非同期
継続的	S3バケットのミラーリング用ポリシー	継続的
DailyBackup	日単位ルールと日単位転送スケジュールを使用したバックアップ ポリシー	非同期
DPDefault	すべてのSnapshotと最新のアクティブ ファイルシステムをミラーリングするためのSnapMirror非同期ポリシー	非同期
MirrorAllSnapshots	すべてのSnapshotと最新のアクティブ ファイルシステムをミラーリングするためのSnapMirror非同期ポリシー	非同期
MirrorAllSnapshotsDiscardNetwork	ネットワーク設定を除くすべてのSnapshotと最新のアクティブ ファイルシステムをミラーリングするためのSnapMirror非同期ポリシー	非同期
MirrorAndVault	最新のアクティブ ファイルシステムと日単位および週単位のSnapshotをミラーリングするための、ユニファイドSnapMirror非同期およびバックアップ ポリシー	非同期

Name	概要	ポリシータイプ
MirrorAndVaultDiscardNetwork	ネットワーク設定を除く最新のアクティブ ファイルシステムと日単位および週単位のSnapshotをミラーリングするための、ユニファイドSnapMirror非同期およびバックアップ ポリシー	非同期
MirrorLatest	最新のアクティブ ファイルシステムをミラーリングするためのSnapMirror非同期ポリシー	非同期
SnapCenterSync	アプリケーションで作成されたSnapshot設定を使用したSnapCenter向けSnapMirror同期用ポリシー	同期
StrictSync	レプリケーションに失敗するとクライアント アクセスが中断されるSnapMirror同期用ポリシー	同期
同期	レプリケーションに失敗してもクライアント アクセスが中断されないSnapMirror同期用ポリシー	同期
Unified7year	保持期間が7年のユニファイドSnapMirrorポリシー	非同期
XDPDefault	日単位および週単位ルールを使用したバックアップポリシー	非同期

ONTAP StrictSyncおよび **Sync** ポリシーでサポートされるワークロードについて学習します

StrictSyncポリシーとSyncポリシーでは、FC、iSCSI、FC-NVMeの各プロトコルを使用したLUNベースのすべてのアプリケーションに加え、データベース、VMWareクォータ、SMBなどのエンタープライズ アプリケーションについてはNFSv3およびNFSv4プロトコルもサポートされます。ONTAP 9.6以降では、EDA（Electronic Design Automation）、ホーム ディレクトリ、ソフトウェア ビルド ワークロードなどのエンタープライズ ファイルサービスにSnapMirror同期を使用できます。

ONTAP 9.5では、SyncポリシーでNFSv3またはNFSv4ワークロードを選択する際、いくつかの重要な側面について考慮する必要があります。読み取り処理や書き込み処理のワークロードのデータ量については、SyncポリシーではIOワークロードが高くても対応できるため考慮する必要はありません。ONTAP 9.5では、ファイルの作成、ディレクトリの作成、ファイル権限の変更、ディレクトリ権限の変更などの処理が多いワークロード（「メタデータ比率の高いワークロード」と呼ばれます）は適さない場合があります。メタデータ比率の高いワークロードの典型的な例としては、複数のテスト ファイルを作成して自動化の実行後にファイルを削除するDevOpsワークロードがあります。また、コンパイル時に複数の一時ファイルを生成する並列ビルド ワークロードなども含まれます。メタデータの書き込みアクティビティの比率が高いと、ミラー間の同期が一時的に解除され、クライアントからの読み取りや書き込みのIOが停止することがあります。

ONTAP 9.6以降ではこれらの制限はなくなり、ホーム ディレクトリやソフトウェア ビルド ワークロードなどのマルチユーザ環境を含むエンタープライズ ファイルサービスのワークロードにSnapMirror同期を使用できるようになりました。

関連情報

["SnapMirror 同期の構成とベストプラクティス"](#)

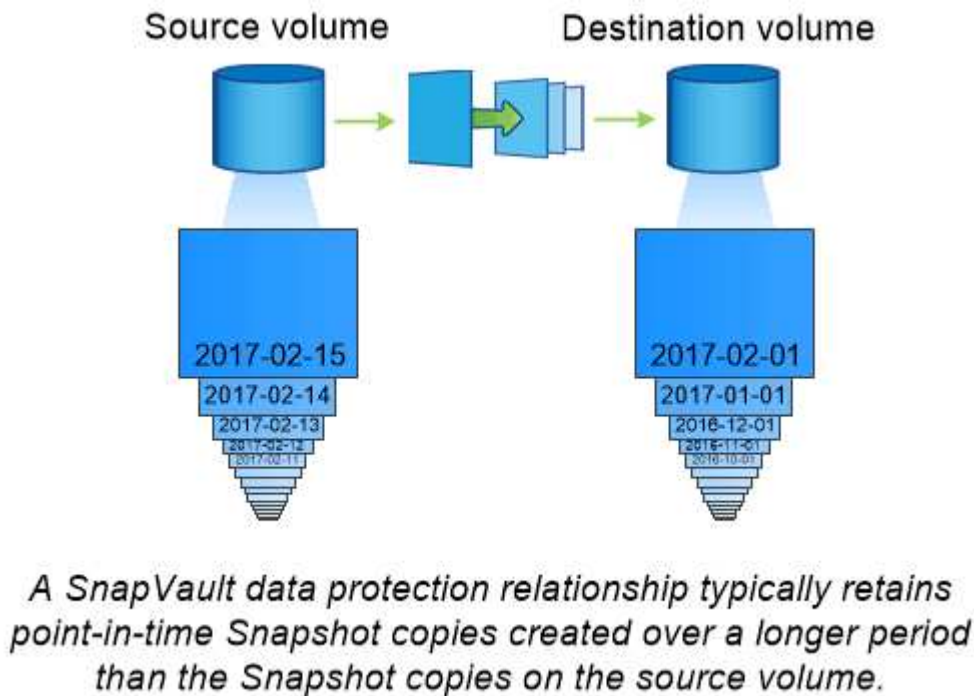
ONTAP SnapMirrorテクノロジーを使用したボールドアーカイブについて学ぶ

SnapMirrorバックアップ ポリシーは、ONTAP 9.3以降でSnapVaultテクノロジーに代わ

るものです。SnapMirrorバックアップ ポリシーは、標準へのコンプライアンスやその他のガバナンス関連の目的で、ディスクツーディスクのSnapshotレプリケーションに使用します。SnapMirror関係では、デスティネーションに通常はソース ボリュームに現在存在するSnapshotのみが含まれますが、これとは対照的に、バックアップ デスティネーションには通常、はるかに長い期間にわたって作成されたポイントインタイムSnapshotが保持されます。

例えば、政府の会計規制を遵守するために、20年間にわたって毎月のデータのスナップショットを保持したい場合があります。Vaultストレージからデータを提供する必要がないため、移行先システムでは低速で安価なディスクを使用できます。

次の図は、SnapMirrorのバックアップ データ保護関係を示しています。



バックアップ データ保護関係を初期化する方法

関係のSnapMirrorポリシーは、ベースラインおよび更新の内容を定義します。

デフォルトのボールド ポリシーに基づくベースライン転送 `XDPEndpointDefault` では、ソース ボリュームのスナップショットが作成され、そのコピーとそれが参照するデータ ブロックがデスティネーション ボリュームに転送されます。SnapMirrorリレーションシップとは異なり、ボールド バックアップでは、ベースラインに古いスナップショットは含まれません。

バックアップ データ保護関係を更新する方法

更新は非同期で、設定したスケジュールに従って行われます。関係のポリシーで定義するルールによって、更新に含める新しいSnapshotと保持するコピー数が決まります。ポリシーで定義されたラベル（例：「monthly」）は、ソースのSnapshotポリシーで定義された1つ以上のラベルと一致している必要があります。一致しない場合、レプリケーションは失敗します。

`XDPDefault`ポリシーに基づく更新のたびに、SnapMirrorは前回の更新以降に作成されたスナップショット（ポリシー ルールで定義されたラベルと一致するラベルを持つもの）を転送します。
`XDPDefault`ポリシーの `snapmirror policy show` コマンドによる以下の出力では、次の点に注意してください：

- Create Snapshot`は「`false`」で、`XDPDefault`がSnapMirror関係を更新するときにスナップショットを作成しないことを示します。
- XDPDefault`には、ルール「`daily`」と「`weekly`」があり、SnapMirrorが関係を更新するときに、ソース上の一致するラベルを持つすべてのSnapshotが転送されることを示しています。

```
cluster_dst::> snapmirror policy show -policy XDPDefault -instance

                Vserver: vs0
SnapMirror Policy Name: XDPDefault
SnapMirror Policy Type: vault
                Policy Owner: cluster-admin
                Tries Limit: 8
                Transfer Priority: normal
Ignore accesstime Enabled: false
                Transfer Restartability: always
Network Compression Enabled: false
                Create Snapshot: false
                Comment: Default policy for XDP relationships with
daily and weekly
                        rules.
                Total Number of Rules: 2
                Total Keep: 59
                Rules: SnapMirror Label      Keep  Preserve Warn
Schedule Prefix
-----
-----
                        daily                7   false    0  -
-
                        weekly              52   false    0  -
-
```

関連情報

- ["snapmirror policy show"](#)

ONTAP SnapMirror統合レプリケーションについて学ぶ

SnapMirror_統合レプリケーション_を使用すると、同じデスティネーション ボリュームでディザスタ リカバリとアーカイブを設定できます。統合レプリケーションが適切な場合、必要なセカンダリ ストレージの量を削減し、ベースライン転送の数を制限し、ネッ

トワーク トラフィックを減らすというメリットがあります。

統合データ保護関係の初期化方法

SnapMirrorと同様に、一元化されたデータ保護機能の初回起動時に、ベースライン転送が実行されます。関係のSnapMirrorポリシーは、ベースラインおよび更新の内容を定義します。

デフォルトの統合データ保護ポリシー `MirrorAndVault` でのベースライン転送では、ソース ボリュームのスナップショットが作成され、そのコピーとそれが参照するデータ ブロックがデスティネーション ボリュームに転送されます。ボルト アーカイブと同様に、統合データ保護では古いスナップショットはベースラインに含まれません。

統合データ保護関係の更新方法

`MirrorAndVault` ポリシーに基づく更新のたびに、SnapMirrorはソース ボリュームのSnapshotを作成し、そのSnapshotと前回の更新以降に作成されたすべてのSnapshotを転送します（ただし、Snapshotポリシー ルールで定義されたラベルと一致するラベルが付いている場合）。

`MirrorAndVault` ポリシーの `snapmirror policy show` コマンドからの次の出力では、以下の点に注意してください：

- Create Snapshot`は「`true`」で、`MirrorAndVault`がSnapMirror関係を更新するときにスナップショットを作成することを示します。
- MirrorAndVault`には、ルール「`sm_created`」、「daily」、および「weekly」があり、SnapMirrorが関係を更新するときに、SnapMirrorによって作成されたスナップショットと、ソース上の一致するラベルを持つスナップショットの両方が転送されることを示します。

```
cluster_dst:> snapmirror policy show -policy MirrorAndVault -instance

Vserver: vs0
SnapMirror Policy Name: MirrorAndVault
SnapMirror Policy Type: mirror-vault
Policy Owner: cluster-admin
Tries Limit: 8
Transfer Priority: normal
Ignore accesstime Enabled: false
Transfer Restartability: always
Network Compression Enabled: false
Create Snapshot: true
Comment: A unified SnapMirror synchronous and
SnapVault policy for
mirroring the latest file system and daily
and weekly snapshots.
Total Number of Rules: 3
Total Keep: 59
Rules: SnapMirror Label      Keep  Preserve Warn
Schedule Prefix
-----
sm_created                  1  false      0 -
daily                       7  false      0 -
weekly                      52  false      0 -
```

統一7年ポリシー

事前設定された `Unified7year` ポリシーは `MirrorAndVault` とまったく同じように動作しますが、4番目のルールによって毎月のスナップショットが転送され、7年間保持される点が異なります。

Schedule Prefix	Rules: SnapMirror Label	Keep	Preserve	Warn
-----	-----	----	-----	----
-	sm_created	1	false	0 -
-	daily	7	false	0 -
-	weekly	52	false	0 -
-	monthly	84	false	0 -
-				

データ破損からの保護

統合レプリケーションは、ベースライン転送の内容を、初期化時にSnapMirrorによって作成されたスナップショットに限定します。更新のたびに、SnapMirrorはソースの別のスナップショットを作成し、そのスナップショットと、スナップショット ポリシー ルールで定義されたラベルと一致するラベルを持つ新しいスナップショットを転送します。

更新されたスナップショットが破損する可能性を防ぐには、最後に転送されたスナップショットのコピーをデスティネーションに作成します。この「ローカル コピー」は、ソースの保持ルールに関係なく保持されるため、SnapMirrorによって最初に転送されたスナップショットがソースで利用できなくなっても、デスティネーションにはそのコピーが存在します。

ユニファイド データ レプリケーション使用の判断

完全なミラーを維持するメリットと、ユニファイド レプリケーションが提供するメリット（セカンダリ ストレージ容量の削減、ベースライン転送の回数削減、ネットワーク トラフィックの削減）を比較検討する必要があります。

統合レプリケーションの適切性を判断する上で重要な要素は、アクティブ ファイル システムの変更率です。たとえば、データベース トランザクション ログの1時間ごとのスナップショットを保持するボリュームには、従来のミラーの方が適している場合があります。

関連情報

- ["snapmirror policy show"](#)

ONTAPデータ保護のデスティネーション ボリュームが自動的に拡張されるとき

ソース ボリュームのサイズが増大していた場合、デスティネーション ボリュームを含むアグリゲートに空きスペースがあれば、データ保護ミラー転送の実行時にデスティネーション ボリュームのサイズが自動的に拡張されます。

この処理は、デスティネーションの自動拡張の設定には関係なく行われます。ボリュームの拡張量を制限したり拡張処理を無効にしたりすることはできません。

デフォルトでは、データ保護ボリュームは `grow\_shrink` 自動サイズ設定モードに設定されており、使用領域の量に応じてボリュームのサイズが拡大または縮小されます。データ保護ボリュームのmax-autosizeは最

大FlexVolサイズと同じで、プラットフォームによって異なります。例：

- FAS8200：DPボリュームのデフォルトのmax-autosize = 100TB

詳細については、"[NetApp Hardware Universe](#)"を参照してください。

ONTAPデータ保護のファンアウトとカスケード展開について学ぶ

ファンアウト型展開を使用すると、データ保護を複数のセカンダリ システムに拡張できます。カスケード型展開を使用すると、データ保護を三次システムに拡張できます。

ファンアウトとカスケード展開はどちらも、SnapMirror DR、SnapVault、または統合レプリケーションの任意の組み合わせをサポートします。ONTAP 9.5以降、SnapMirror同期関係は、1つ以上のSnapMirror非同期関係を含むファンアウト展開をサポートします。ファンアウト構成では、1つの関係のみをSnapMirror同期関係にすることができ、ソース ボリュームからのその他すべての関係はSnapMirror非同期関係にする必要があります。SnapMirror同期関係はカスケード展開もサポートします（ONTAP 9.6以降）。ただし、SnapMirror同期関係のデスティネーション ボリュームからの関係は、SnapMirror非同期関係にする必要があります。[SnapMirrorアクティブ同期](#)（ONTAP 9.13.1以降でサポート）も、ファンアウト構成をサポートします。



ファンイン展開を使用すると、複数のプライマリ システムと単一のセカンダリ システムの間にデータ保護関係を作成できます。各関係では、セカンダリ システム上の異なるボリュームを使用する必要があります。

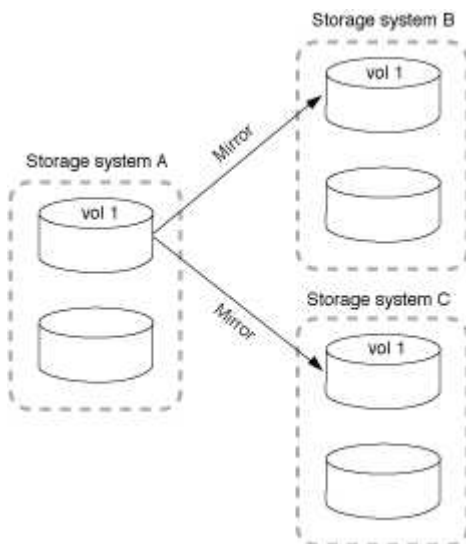


ファンアウト構成またはカスケード構成の一部であるボリュームは、再同期に時間がかかる場合があることにご注意ください。SnapMirror関係のステータスが「準備中」と表示される時間が長くなることは珍しくありません。

ファンアウト構成の仕組み

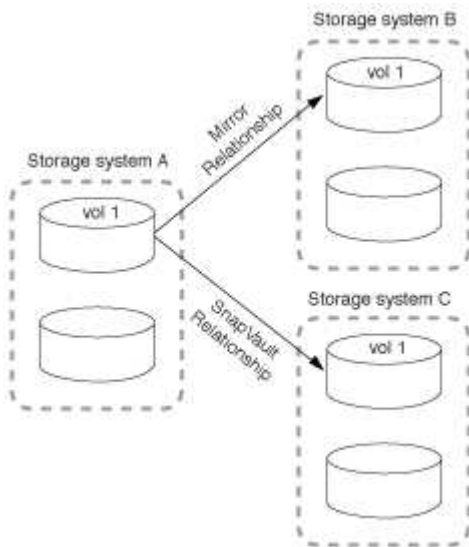
SnapMirrorは_複数ミラー_および_ミラー ボールト_ファンアウト展開をサポートします。

複数ミラー ファンアウト構成では、ソース ボリュームから複数のセカンダリ ボリュームへのミラー関係が確立されます。

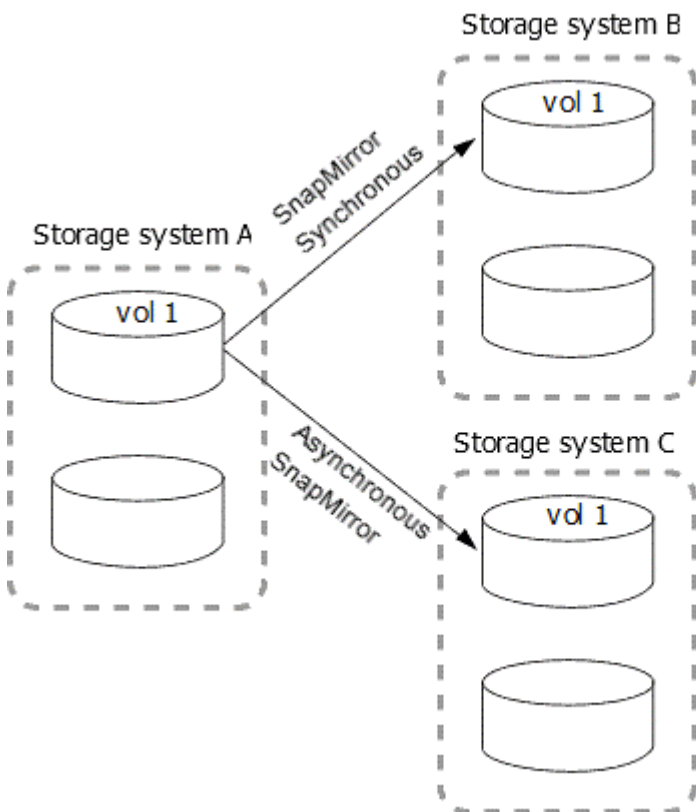


ミラー ボールト ファンアウト導入は、セカンダリ ボリュームへのミラー関係と別のセカンダリ ボリューム

へのSnapVault関係を持つソース ボリュームで構成されます。



ONTAP 9.5以降では、ファンアウト構成でSnapMirror同期関係を確立できます。ただし、ファンアウト構成で確立できるSnapMirror同期関係は1つだけで、ソース ボリュームからの残りの関係はすべてSnapMirror非同期関係にする必要があります。



カスケード構成の仕組み

SnapMirrorは、*mirror-mirror*、*mirror-vault*、*vault-mirror*、および *_vault-vault_* カスケード展開をサポートします。

ミラー-ミラー カスケード構成の関係のチェーンでは、ソース ボリュームがセカンダリ ボリュームにミラーリングされ、そのセカンダリ ボリュームが3番目のボリュームにミラーリングされます。セカンダリ ボリュ

ームが使用できなくなった場合は、プライマリ ボリュームと3番目のボリュームの関係の同期できます。ベースライン転送を新たに実行する必要はありません。

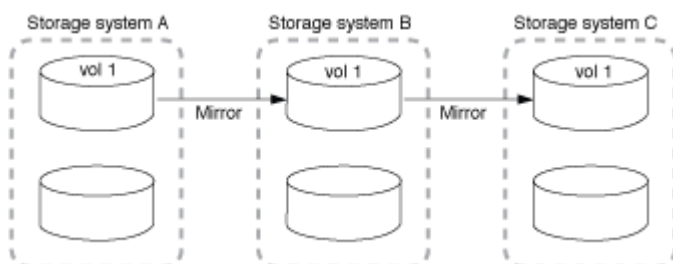
カスケード ボリュームの関係において、長期保存Snapshotは、ONTAP 9のすべてのバージョンで、カスケードの最終SnapMirrorデスティネーション ボリュームでのみサポートされます。カスケードの中間ボリュームで長期保存Snapshotを有効にすると、バックアップとSnapshotが失われます。カスケードの中間ボリュームで長期保存Snapshotが有効になっているサポート対象外の構成の場合は、テクニカル サポートに連絡し、["NetAppナレッジベース：長期保存（LTR）スナップショットが有効になっているボリュームのカスケードはサポートされていません"](#)を参照してサポートを受けてください。

次のONTAPバージョンでは、最終的なSnapMirrorデスティネーション ボリュームを除くカスケード内のどのボリュームでも長期保存Snapshotを有効にすることはできません。

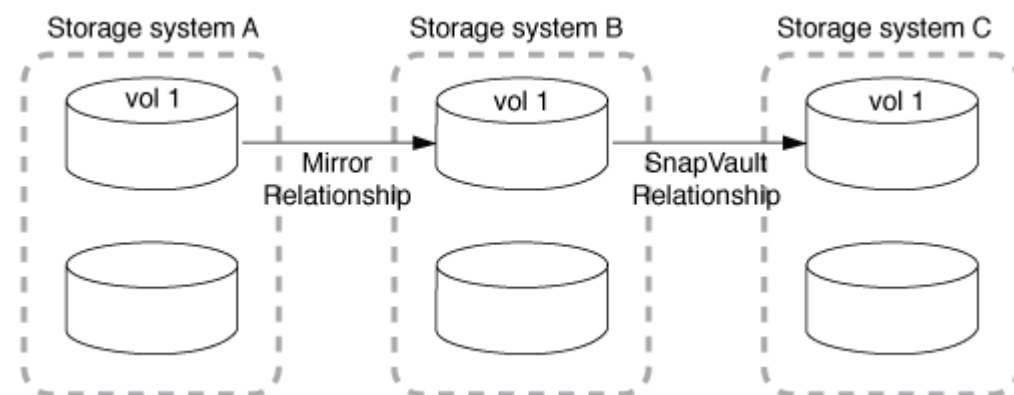
- 9.15.1以降
- 9.14.1P2およびP4～P14
- 9.13.1P9～P17
- 9.12.1 P12～P19
- 9.11.1P15～P20
- 9.10.1P18～P20
- 9.9.1P20

["長期保存Snapshot"](#)についての詳細をご覧ください。

ONTAP 9.6以降では、ミラー-ミラー カスケード構成でSnapMirror同期関係がサポートされています。SnapMirror同期関係に含めることができるのは、プライマリ ボリュームとセカンダリ ボリュームだけです。セカンダリ ボリュームとターシャリ ボリュームの関係は非同期でなければなりません。



ミラー ボールト カスケード展開は、ソース ボリュームがセカンダリ ボリュームにミラーリングされ、セカンダリ ボリュームが三次ボリュームにボールトされる関係のチェーンで構成されます。



Vault-mirror および vault-vault カスケード展開もサポートされています。

- ボールト ミラー カスケード展開は、ソース ボリュームがセカンダリ ボリュームにボールトされ、セカンダリ ボリュームが三次ボリュームにミラーリングされる関係のチェーンで構成されます。
- ボールト-ボールト カスケード展開は、ソース ボリュームがセカンダリ ボリュームにボールトされ、セカンダリ ボリュームが三次ボリュームにボールトされる関係のチェーンで構成されます。

関連情報

- [SnapMirrorアクティブ同期を使用したファンアウト構成での保護の再開](#)

ONTAP SnapMirrorライセンスについて学ぶ

ONTAP 9.3以降、ONTAPインスタンス間のレプリケーションに関するライセンスが簡素化されました。ONTAP 9リリースでは、SnapMirrorライセンスでバックアップ関係とミラー関係の両方がサポートされます。SnapMirrorライセンスを使用すれば、バックアップとディザスタ リカバリの両方のユースケースでONTAPレプリケーションがサポートされます。

ONTAP 9.3リリースより前は、ONTAPインスタンス間で_vault_関係を設定するには別途SnapVaultライセンスが必要でした。DPインスタンスでは、保持期間の長いバックアップのユースケースをサポートするために、より多くのSnapshotを保持できます。また、ONTAPインスタンス間で_mirror_関係を設定するにはSnapMirrorライセンスが必要でした。各ONTAPインスタンスは同じ数のSnapshot（つまり、_mirror_イメージ）を保持し、クラスタフェイルオーバーを可能にするディザスタリカバリのユースケースをサポートします。SnapMirrorライセンスとSnapVaultライセンスは両方とも、ONTAP 8.xおよび9.xリリースで引き続き使用およびサポートされます。

SnapVaultライセンスはONTAP 8.xと9.xの両方のリリースで引き続き機能し、サポートされますが、SnapVaultライセンスの代わりにSnapMirrorライセンスを使用して、ミラー設定とバックアップ設定の両方に対応できます。

ONTAP 9.3以降、非同期レプリケーションでは単一のユニファイド レプリケーション エンジンを使用して拡張データ保護モード（XDP）ポリシーが設定されます。この場合、ミラー ポリシー、バックアップ ポリシー、またはミラー バックアップ ポリシーにSnapMirrorライセンスを設定できます。SnapMirrorライセンスは、ソースとデスティネーションの両方のクラスタに必要です。SnapVaultライセンスは、SnapMirrorライセンスがすでにインストールされていれば必要ありません。SnapMirror非同期の恒久ライセンスは、新しいAFFおよびFASシステムにインストールされるONTAP Oneソフトウェア スイートに含まれています。

データ保護設定の制限は、ONTAPバージョン、ハードウェア プラットフォーム、インストールされているライセンスなど、いくつかの要因に基づいて決定されます。詳細については、"[Hardware Universe](#)"を参照してください。

SnapMirror同期ライセンス

ONTAP 9.5以降では、SnapMirror同期関係がサポートされます。SnapMirror同期関係を作成するには、次のライセンスが必要です。

- ソース クラスタとデスティネーション クラスタの両方にSnapMirror同期ライセンスが必要です。

SnapMirror同期ライセンスは"[ONTAP One ライセンス スイート](#)"の一部です。

2019年6月以前にPremiumまたはFlash Bundleでシステムを購入した場合、必要なSnapMirror同期ライセ

ンスを取得するために、NetApp Support SiteからNetAppマスターキーをダウンロードできます：["マスター ライセンス キー"](#)。

- ・ ソース クラスタとデスティネーション クラスタの両方にSnapMirrorライセンスが必要です。

SnapMirrorクラウド ライセンス

ONTAP 9.8以降、SnapMirrorクラウドライセンスでは、ONTAPインスタンスからオブジェクトストレージエンドポイントへのスナップショットの非同期レプリケーションが提供されます。レプリケーションターゲットは、オンプレミスオブジェクトストアだけでなく、S3およびS3互換のパブリッククラウドオブジェクトストレージサービスを使用して設定できます。SnapMirrorクラウド関係は、ONTAPシステムから事前認定されたオブジェクトストレージターゲットまでサポートされます。

SnapMirrorクラウドはスタンドアロン ライセンスとしては提供されていません。必要なライセンスは、ONTAPクラスタごとに1つだけです。SnapMirrorクラウド ライセンスに加えて、SnapMirror非同期ライセンスも必要です。

SnapMirrorクラウド関係を作成するには、次のライセンスが必要です。

- ・ オブジェクト ストア エンドポイントへの直接レプリケーションには、SnapMirrorライセンスとSnapMirrorクラウド ライセンスの両方が必要です。
- ・ マルチポリシーのレプリケーション ワークフロー（ディスク→ディスク→クラウドなど）を設定する場合、すべてのONTAPインスタンスにSnapMirrorライセンスが必要です。一方、SnapMirrorクラウド ライセンスは、オブジェクト ストレージ エンドポイントに直接レプリケートするソース クラスタにのみ必要です。

ONTAP 9.9.1以降では、["SnapMirrorクラウドレプリケーションにはSystem Managerを使用する"](#)できます。

SnapMirrorクラウドの認定済みアプリケーションの一覧は、NetAppのWebサイトで公開されています。

Data Protection Optimized ライセンス

Data Protection Optimized (DPO) ライセンスの販売は終了し、現在のプラットフォームではDPOはサポートされません。ただし、サポート対象のプラットフォームにDPOライセンスがインストールされている場合、NetAppはそのプラットフォームの販売終了までサポート提供を継続します。

DPOはONTAP Oneライセンス バンドルには含まれていないため、DPOライセンスがシステムにインストールされている場合はONTAP Oneライセンス バンドルにアップグレードできません。

サポートされているプラットフォームの詳細については、["Hardware Universe"](#)を参照してください。

ONTAP DPOシステムの機能強化

ONTAP 9.6以降では、DP_Optimized (DPO) ライセンスをインストールすると、サポートされるFlexVolボリュームの最大数が増加します。ONTAP 9.4以降では、DPOライセンスを持つシステムでSnapMirrorバックオフ、ボリューム間のバックグラウンド重複排除、スナップショット ブロックのドナーとしての使用、およびコンパクションがサポートされます。

ONTAP 9.6以降、セカンダリシステムまたはデータ保護システムでサポートされるFlexVolボリュームの最大数が増加し、ノードあたり最大2,500個のFlexVolボリューム、またはフェイルオーバー モードで最大5,000個まで拡張できるようになりました。FlexVolボリュームの増加は、["DP_Optimized \(DPO\) ライセンス"](#)によっ

て有効になります。ソース ノードとデスティネーション ノードの両方で"**SnapMirrorライセンス**"が必要です。

ONTAP 9.4以降では、DPOシステムの次の機能が強化されています。

- SnapMirrorバックオフ：DPOシステムでは、レプリケーション トラフィックにはクライアント ワークロードと同じ優先順位が与えられます。

DPOシステムでは、SnapMirrorバックオフはデフォルトで無効になります。

- ボリューム バックグラウンド重複排除とボリューム間バックグラウンド重複排除：ボリューム バックグラウンド重複排除とボリューム間バックグラウンド重複排除は、DPO システムで有効になっています。

```
`storage aggregate efficiency cross-volume-dedupe start -aggregate  
_aggregate_name_ -scan-old-data  
true`
```

コマンドを実行して、既存のデータの重複排除を行うことができます。パフォーマンスへの影響を軽減するため、このコマンドはオフピーク時に実行することをお勧めします。

```
`storage aggregate efficiency cross-volume-dedupe start`
```

の詳細については、[link:https://docs.netapp.com/us-en/ontap-cli/storage-aggregate-efficiency-cross-volume-dedupe-start.html](https://docs.netapp.com/us-en/ontap-cli/storage-aggregate-efficiency-cross-volume-dedupe-start.html) ["ONTAP コマンド リファレンス"] をご覧ください。

- スナップショット ブロックをドナーとして使用することで節約を増加：アクティブ ファイル システムでは使用できないがスナップショットにトラップされているデータ ブロックは、ボリューム重複排除のドナーとして使用されます。

新しいデータはスナップショットに保持されていたデータと重複排除され、スナップショットブロックも効果的に共有されます。ドナースペースの増加により、特にボリュームに多数のスナップショットがある場合、さらなる節約効果が得られます。

- 圧縮：DPO ボリュームでは、データ圧縮がデフォルトで有効になっています。

ONTAP SnapMirrorコマンドにおけるパス名パターンマッチングについて学ぶ

パターン マッチングを使用して、snapmirror コマンド内のソース パスと宛先パスを指定できます。

```
`snapmirror`
```

コマンドは、次の形式の完全修飾パス名を使用します： ``vserver:volume``。SVM名を入力しない場合、パス名を省略できます。省略した場合、``snapmirror`` コマンドはユーザーのローカルSVMコンテキストを想定します。

SVM の名前が「vserver1」、ボリュームの名前が「vol1」であると仮定すると、完全修飾パス名は「vserver1:vol1」です。

パス内のアスタリスク (*) をワイルドカードとして使用し、一致する完全修飾パス名を選択できます。次の表に、ワイルドカードを使用してボリュームの範囲を選択する例を示します。

*	すべてのパスに一致します。
vs*	<code>`vs`</code> で始まる SVM 名を持つすべての SVM およびボリュームと一致します。
:*src	ボリューム名に <code>src</code> テキストが含まれるすべての SVM と一致します。
:vol	<code>`vol`</code> で始まるボリューム名を持つすべての SVM と一致します。

```
vs1::> snapmirror show -destination-path *:dest*
```

```
Progress
Source          Destination  Mirror          Relationship  Total
Last
Path            Type  Path            State          Status          Progress
Healthy Updated
-----
vs1:sm_src2
DP    vs2:sm_dest1
Snapmirrored  Idle
true    -
```

``snapmirror show``の詳細については、link:<https://docs.netapp.com/us-en/ontap-cli/snapmirror-show.html>["ONTAPコマンド リファレンス"]を参照してください。

ONTAP SnapMirrorリレーションシップ操作の拡張クエリについて学習します

拡張クエリを使用すると、複数のSnapMirrorリレーションシップに対してSnapMirror操作を一度に実行できます。例えば、初期化されていない複数のSnapMirrorリレーションシップを1つのコマンドで初期化したい場合などです。

タスク概要

拡張クエリは次のSnapMirror操作に適用できます：

- 初期化されていない関係の初期化
- 休止していた関係を再開する

- 壊れた関係を再同期する
- アイドル関係の更新
- 関係データ転送を中止する

手順

1. 複数の関係に対してSnapMirror操作を実行します：

```
snapmirror command {-state state } *
```

次のコマンドは、`Uninitialized`状態にあるSnapMirror関係を初期化します：

```
vs1::> snapmirror initialize {-state Uninitialized} *
```

`snapmirror initialize`の詳細については、[link:https://docs.netapp.com/us-en/ontap-cli/snapmirror-initialize.html](https://docs.netapp.com/us-en/ontap-cli/snapmirror-initialize.html)["ONTAPコマンド リファレンス"]を参照してください。

SnapMirror関係に対応したONTAPバージョン

SnapMirrorデータ保護関係を作成する前に、ソース ボリュームとデスティネーション ボリュームで互換性のあるONTAPバージョンが実行されている必要があります。ONTAPをアップグレードする前に、現在のONTAPバージョンにSnapMirror関係のターゲットONTAPバージョンとの互換性があることを確認する必要があります。

ユニファイド レプリケーション関係

オンプレミスまたはCloud Volumes ONTAPリリースを使用した、タイプ「XDP」のSnapMirror関係の場合：

ONTAP 9.9.0以降：

- ONTAP 9.x.0リリースはクラウド専用リリースであり、Cloud Volumes ONTAPシステムをサポートします。リリースバージョンの後のアスタリスク (*) は、クラウド専用リリースであることを示します。



ONTAP 9.16.0は"ASA r2システム"をサポートしているため、クラウドのみのルールの例外となります。リリースバージョンの後のプラス記号 (+) は、ASA r2とクラウドの両方でサポートされているリリースを示します。ASA r2システムは、他のASA r2システムとのSnapMirror関係のみをサポートします。

- ONTAP 9.x.1は一般リリースで、オンプレミス システムとCloud Volumes ONTAPシステムの両方をサポートします。



ONTAP 9.16.1以降を実行しているクラスタ内のボリュームで"高度な容量バランス調整"が有効になっている場合、ONTAP 9.16.1より前のONTAPバージョンを実行しているクラスタへのSnapMirror転送はサポートされません。



双方向の互換性があります。

ONTAP バージョン9.4以降の相互運用性

ONTAP バージョン	以前の ONTAP バージョンと相互運用できます...																					
	9.1 8.1	9.1 7.1	9.1 6.1	9.1 6.0 以上	9.1 5.1	9.1 5.0 *	9.1 4.1	9.1 4.0 *	9.1 3.1	9.1 3.0 *	9.1 2.1	9.1 2.0 *	9.1 1.1	9.1 1.0 *	9.1 0.1	9.1 0.0 *	9.9 .1	9.9 .0*	9.8	9.7	9.6	9.5
9.1 8.1	はい	はい	はい	はい	はい	いいえ	はい	いいえ	はい	はい	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ	
9.1 7.1	はい	はい	はい	はい	はい	はい	はい	はい	はい	はい	はい	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ	
9.1 6.1	はい	はい	はい	はい	はい	はい	はい	はい	はい	はい	はい	はい	はい	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ	
9.1 6.0 以上	はい	はい	はい	はい	はい	いいえ	はい	いいえ	はい	いいえ	はい	いいえ	はい	いいえ	はい	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ	
9.1 5.1	はい	はい	はい	はい	はい	はい	はい	はい	はい	はい	はい	はい	はい	はい	はい	はい	はい	いいえ	いいえ	いいえ	いいえ	
9.1 5.0 *	いいえ	はい	はい	いいえ	はい	はい	はい	いいえ	はい	いいえ	はい	いいえ	はい	いいえ	はい	いいえ	はい	いいえ	いいえ	いいえ	いいえ	
9.1 4.1	はい	はい	はい	はい	はい	はい	はい	はい	はい	はい	はい	はい	はい	はい	はい	はい	はい	はい	いいえ	いいえ	いいえ	
9.1 4.0 *	いいえ	はい	はい	いいえ	はい	いいえ	はい	はい	はい	いいえ	はい	いいえ	はい	いいえ	はい	いいえ	はい	いいえ	いいえ	いいえ	いいえ	
9.1 3.1	はい	はい	はい	はい	はい	はい	はい	はい	はい	はい	はい	はい	はい	はい	はい	はい	はい	はい	はい	いいえ	いいえ	
9.1 3.0 *	いいえ	はい	はい	いいえ	はい	いいえ	はい	いいえ	はい	はい	はい	いいえ	はい	いいえ	はい	いいえ	はい	いいえ	はい	いいえ	いいえ	

9.1 2.1	はい え	はい	はい	はい	はい	はい	はい	はい	はい	はい	はい	はい	はい	はい	はい	はい	はい	はい	はい	はい	はい	はい
9.1 2.0 *	はい え	はい え	はい	はい え	はい	はい え	はい	はい え	はい	はい	はい	はい	はい え	はい	はい え	はい	はい え	はい	はい	はい	はい え	はい え
9.1 1.1	はい え	はい え	はい	はい	はい	はい	はい	はい	はい	はい	はい	はい	はい	はい	はい	はい	はい	はい	はい	はい	はい	はい え
9.1 1.0 *	はい え	はい え	はい え	はい え	はい	はい え	はい	はい え	はい	はい	はい え	はい	はい	はい	はい え	はい	はい え	はい	はい	はい	はい	はい え
9.1 0.1	はい え	はい え	はい え	はい	はい	はい	はい	はい	はい	はい	はい	はい	はい	はい	はい	はい	はい	はい	はい	はい	はい	はい
9.1 0.0 *	はい え	はい え	はい え	はい え	はい	はい え	はい	はい え	はい	はい	はい え	はい	はい	はい	はい	はい	はい え	はい	はい	はい	はい	はい
9.9 .1	はい え	はい え	はい え	はい え	はい	はい	はい	はい	はい	はい	はい	はい	はい	はい	はい	はい	はい	はい	はい	はい	はい	はい
9.9 .0*	はい え	はい え	はい え	はい え	はい え	はい	はい え	はい	はい え	はい	はい え	はい	はい	はい	はい	はい	はい	はい	はい	はい	はい	はい
9.8	はい え	はい え	はい え	はい え	はい え	はい え	はい え	はい	はい	はい	はい	はい	はい	はい	はい	はい	はい	はい	はい	はい	はい	はい
9.7	はい え	はい え	はい え	はい え	はい え	はい え	はい え	はい え	はい え	はい	はい	はい	はい	はい	はい	はい	はい	はい	はい	はい	はい	はい
9.6	はい え	はい え	はい え	はい え	はい え	はい え	はい え	はい え	はい え	はい え	はい え	はい	はい	はい	はい	はい	はい	はい	はい	はい	はい	はい
9.5	はい え	はい え	はい え	はい え	はい え	はい え	はい え	はい え	はい え	はい え	はい え	はい え	はい え	はい	はい	はい	はい	はい	はい	はい	はい	はい

SnapMirror同期関係



SnapMirror同期は、ONTAP Cloudインスタンスではサポートされません。

ONTAPバージョン	以前の ONTAP バージョンと相互運用できます...													
	9.18.1	9.17.1	9.16.1	9.15.1	9.14.1	9.13.1	9.12.1	9.11.1	9.10.1	9.9.1	9.8	9.7	9.6	9.5

9.18.1	はい	はい	はい	はい	はい	はい	はい	はい	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ
9.17.1	はい	はい	はい	はい	はい	はい	はい	はい	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ
9.16.1	はい	はい	はい	はい	はい	はい	はい	はい	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ
9.15.1	はい	はい	はい	はい	はい	はい	はい	はい	はい	いいえ	いいえ	いいえ	いいえ	いいえ
9.14.1	はい	はい	はい	はい	はい	はい	はい	はい	はい	はい	はい	いいえ	いいえ	いいえ
9.13.1	はい	はい	はい	はい	はい	はい	はい	はい	はい	はい	はい	はい	いいえ	いいえ
9.12.1	はい	はい	はい	はい	はい	はい	はい	はい	はい	はい	はい	はい	いいえ	いいえ
9.11.1	いいえ	いいえ	はい	はい	はい	はい	はい	はい	はい	はい	いいえ	いいえ	いいえ	いいえ
9.10.1	いいえ	いいえ	いいえ	はい	はい	はい	はい	はい	はい	はい	はい	いいえ	いいえ	いいえ
9.9.1	いいえ	いいえ	いいえ	いいえ	はい	はい	はい	はい	はい	はい	はい	はい	いいえ	いいえ
9.8	いいえ	いいえ	いいえ	いいえ	はい	はい	はい	いいえ	はい	はい	はい	はい	はい	いいえ
9.7	いいえ	いいえ	いいえ	いいえ	いいえ	はい	はい	いいえ	いいえ	はい	はい	はい	はい	はい
9.6	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ	はい	はい	はい	はい
9.5	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ	はい	はい	はい

SnapMirror SVMディザスタ リカバリ関係



- このマトリックスは、ONTAP 9.10.1以降のSVMデータ モビリティ移行機能に適用されません。
- SVM DR を使用して、"**SVM移行 (SVMデータモビリティ)**"に示されている制限を満たしていない SVM を移行できます。
- どちらの場合も、ソース クラスタとデスティネーション クラスタを最大 2 つのメジャー 新しい ONTAP バージョンで分離できます。ただし、デスティネーションはソース ONTAP バージョンと同じバージョンかそれより新しいバージョンである必要があります。

SVMディザスタ リカバリ データとSVM保護の場合：

SVM ディザスタ リカバリは、同じバージョンのONTAPを実行しているクラスタ間でのみサポートされます。**SVM** レプリケーションではバージョン非依存はサポートされません。

SVMディザスタ リカバリとSVM移行の場合：

- ソース上の以前のONTAPバージョンから、デスティネーション上の同じかそれ以降のONTAPバージョンへの、単一方向のレプリケーションがサポートされます。

- ターゲット クラスタ上の ONTAP バージョンは、次の表に示すように、オンプレミスのメジャー バージョンより 2 つ以下新しいバージョン、またはクラウドのメジャー バージョンより 2 つ以下新しいバージョン（ONTAP 9.9.0 以降）である必要があります。

。長期的なデータ保護に対してはレプリケーションはサポートされません。

リリース バージョンの後のアスタリスク (*) は、クラウドのみのリリースを示します。

サポート状況を確認するには、表の左側の列でソース バージョンを特定し、最上部の行でデスティネーション バージョンを特定します（同等バージョンの場合は「DR / 移行」、新しいバージョンの場合は「移行」のみ）。



ONTAP 9.10.1以降を使用している場合は、SVM DRの代わりに"**SVMのデータ移動**"機能を使用して、SVMをあるクラスタから別のクラスタに移行できます。

ソ ー ス	デスティネーション																					
	9.5	9.6	9.7	9.8	9.9 .0*	9.9 .1	9.1 0.0 *	9.1 0.1	9.1 1.0 *	9.1 1.1	9.1 2.0 *	9.1 2.1	9.1 3.0 *	9.1 3.1	9.1 4.0 *	9.1 4.1	9.1 5.0 *	9.1 5.1	9.1 6.0	9.1 6.1	9.1 7.1	9.1 8.1
9.5	DR /移行	移行	移行																			
9.6		DR /移行	移行	移行																		
9.7			DR /移行	移行	移行																	
9.8				DR /移行	移行	移行		移行														
9.9 .0*					DR /移行	移行	移行	移行	移行	移行												
9.9 .1						DR /移行	移行	移行	移行	移行												
9.1 0.0 *							DR /移行	移行	移行	移行	移行	移行										
9.1 0.1								DR /移行	移行	移行	移行	移行										
9.1 1.0 *									DR /移行	移行	移行	移行	移行	移行								

9.1 1.1									DR 移行	移行	移行	移行	移行							
9.1 2.0 *									DR 移行	移行	移行	移行	移行	移行						
9.1 2.1										DR 移行	移行	移行	移行	移行						
9.1 3.0 *											DR 移行	移行	移行	移行	移行	移行				
9.1 3.1												DR 移行	移行	移行	移行	移行				
9.1 4.0 *													DR 移行	移行	移行	移行	移行	移行		
9.1 4.1														DR 移行	移行	移行	移行	移行		
9.1 5.0 *															DR 移行	移行	移行	移行	移行	
9.1 5.1																DR 移行	移行	移行	移行	
9.1 6.0																	DR 移行	移行	移行	移行
9.1 6.1																		DR 移行	移行	移行
9.1 7.1																			DR 移行	移行
9.1 8.1																				DR 移行

SnapMirrorディザスタ リカバリ関係

SnapMirrorタイプが「DP」でポリシー タイプが「async-mirror」の関係の場合：



DPタイプのミラーはONTAP 9.11.1以降では初期化できず、ONTAP 9.12.1では完全に廃止されました。詳細については、"[データ保護SnapMirror関係の廃止](#)"を参照してください。



次の表で、左側の列がソース ボリュームのONTAPバージョン、上段がデスティネーション ボリュームで使用可能なONTAPバージョンです。

ソース	デスティネーション								
	9.11.1	9.10.1	9.9.1	9.8	9.7	9.6	9.5	9.4	9.3
9.11.1	はい	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ
9.10.1	はい	はい	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ
9.9.1	はい	はい	はい	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ
9.8	いいえ	はい	はい	はい	いいえ	いいえ	いいえ	いいえ	いいえ
9.7	いいえ	いいえ	はい	はい	はい	いいえ	いいえ	いいえ	いいえ
9.6	いいえ	いいえ	いいえ	はい	はい	はい	いいえ	いいえ	いいえ
9.5	いいえ	いいえ	いいえ	いいえ	はい	はい	はい	いいえ	いいえ
9.4	いいえ	いいえ	いいえ	いいえ	いいえ	はい	はい	はい	いいえ
9.3	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ	はい	はい	はい



双方向の互換性はありません。

ONTAP SnapMirrorの制限事項について学ぶ

データ保護関係を作成する前に、SnapMirrorの基本的な制限事項を把握しておく必要があります。

- 1個のデスティネーション ボリュームにはソース ボリュームを1個だけ設定できます。



1個のソース ボリュームには複数のデスティネーション ボリュームを設定できます。デスティネーション ボリュームを任意のタイプのSnapMirrorレプリケーション関係のソース ボリュームにすることができます。

- アレイ モデルに応じて、1つのソース ボリュームから最大8つまたは16つのデスティネーション ボリュームをファンアウトできます。["Hardware Universe"](#)を参照して、特定の構成の詳細を確認してください。
- SnapMirror DR関係のデスティネーションにファイルをリストアすることはできません。
- ソースまたはデスティネーションのSnapVaultボリュームを32ビット ボリュームにすることはできません。
- SnapVault関係のソース ボリュームをFlexCloneボリュームにはしないでください。



関係は機能しますが、FlexCloneボリュームによる効率化の効果が得られなくなります。

SnapMirrorボリュームレプリケーションを設定

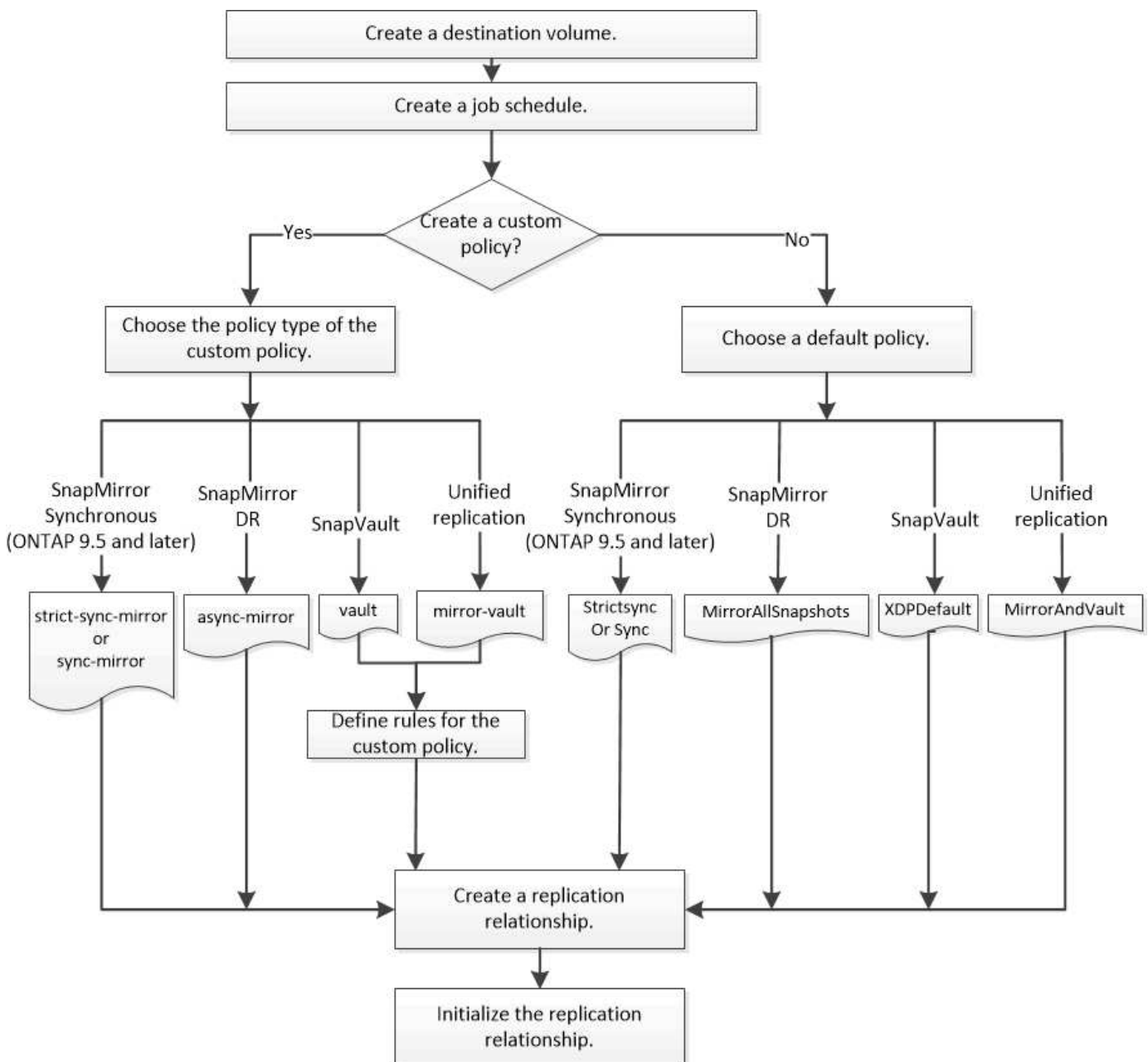
ONTAP SnapMirrorレプリケーション ワークフロー

SnapMirrorは、SnapMirror DR、アーカイブ（旧称SnapVault）、統合レプリケーションの3種類のデータ保護関係を提供します。各タイプの関係は、同じ基本ワークフローに従って設定できます。

ONTAP 9.9.1の一般提供開始以降、"[SnapMirrorアクティブ同期](#)"ゼロ復旧時間目標（Zero RTO）または透過的アプリケーション フェイルオーバー（TAF）が提供され、SAN環境でのビジネス クリティカルなアプリケーションの自動フェイルオーバーが可能になります。

SnapMirrorデータ保護関係の各タイプのワークフロー（デスティネーション ボリュームの作成、ジョブ スケジュールの作成、ポリシーの指定、関係の作成と初期化）は同じです。

ONTAP 9.3以降では、`snapmirror protect` コマンドを使用してデータ保護関係を1つの手順で設定できます。`snapmirror protect`を使用する場合でも、ワークフローの各手順を理解する必要があります。



関連情報

- ["SnapMirror保護"](#)

ONTAP SnapMirrorレプリケーション関係を1ステップで設定する

ONTAP 9.3以降では、`snapmirror protect` コマンドを使用してデータ保護関係をワンステップで設定できます。レプリケートするボリュームのリスト、デスティネーション クラスタ上のSVM、ジョブ スケジュール、SnapMirrorポリシーを指定するだけで、`snapmirror protect` が残りの処理を実行します。

開始する前に

- ソース / デスティネーション クラスタとSVMのピア関係が確立されている必要があります。

["クラスタとSVMのピアリング"](#)

- デスティネーション ボリューム上の言語は、ソース ボリューム上の言語と同じである必要があります。

タスク概要

この `snapmirror protect` コマンドは、指定されたSVMに関連付けられたアグリゲートを選択します。SVMに関連付けられたアグリゲートがない場合、クラスタ内のすべてのアグリゲートから選択されます。アグリゲートの選択は、アグリゲートの空きスペース量とボリューム数に基づいて行われます。

`snapmirror protect` コマンドは次の手順を実行します：

- レプリケートするボリュームのリスト内の各ボリュームについて、適切なタイプとリザーブされたスペースを持つデスティネーション ボリュームを作成します。
- 指定したポリシーに適したレプリケーション関係を設定します。
- 関係を初期化します。

デスティネーション ボリュームの名前は `source\_volume\_name\_dst` という形式です。既存の名前と競合する場合、コマンドはボリューム名に番号を追加します。コマンド オプションでプレフィックスまたはサフィックス（あるいはその両方）を指定できます。サフィックスはシステムが提供する `dst` サフィックスに置き換えられます。

ONTAP 9.4以降では、デスティネーション ボリュームに最大1019個のSnapshotを保存できます。ONTAP 9.3以前では、デスティネーション ボリュームに最大251個のSnapshotを保存できます。



初期化には時間がかかる場合があります。`snapmirror protect` ジョブは初期化の完了を待たずに終了します。そのため、初期化が完了したかどうかを確認するには、`job show` コマンドではなく、`snapmirror show` コマンドを使用する必要があります。

ONTAP 9.5以降では、`snapmirror protect` コマンドを使用してSnapMirror同期関係を作成できます。

`snapmirror protect`の詳細については、[link:https://docs.netapp.com/us-en/ontap-cli/snapmirror-protect.html](https://docs.netapp.com/us-en/ontap-cli/snapmirror-protect.html)["ONTAPコマンド リファレンス"]を参照してください。

手順

1. レプリケーション関係をワンステップで作成して初期化します。

このコマンドを実行する前に、山カッコ内の変数を必要な値に置き換える必要があります。

```
snapmirror protect -path-list <SVM:volume> -destination-vserver  
<destination_SVM> -policy <policy> -schedule <schedule> -auto-initialize  
<true|false> -destination-volume-prefix <prefix> -destination-volume  
-suffix <suffix>
```



このコマンドは、デスティネーションSVMまたはデスティネーション クラスタから実行する必要があります。`-auto-initialize`オプションのデフォルトは「`true`」です。

次の例では、デフォルトの `MirrorAllSnapshots` ポリシーを使用してSnapMirror DR関係を作成し、初期化します：

```
cluster_dst::> snapmirror protect -path-list svm1:volA, svm1:volB  
-destination-vserver svm_backup -policy MirrorAllSnapshots -schedule  
replication_daily
```



必要に応じてカスタムポリシーを使用することもできます。詳細については、"[カスタム レプリケーション ポリシーの作成](#)"をご覧ください。

次の例では、デフォルトの `XDPDefault` ポリシーを使用してSnapVault関係を作成し、初期化します：

```
cluster_dst::> snapmirror protect -path-list svm1:volA, svm1:volB  
-destination-vserver svm_backup -policy XDPDefault -schedule  
replication_daily
```

次の例では、デフォルトの `MirrorAndVault` ポリシーを使用して、統合レプリケーション関係を作成して初期化します：

```
cluster_dst::> snapmirror protect -path-list svm1:volA, svm1:volB  
-destination-vserver svm_backup -policy MirrorAndVault
```

次の例では、デフォルトの `Sync` ポリシーを使用してSnapMirror同期関係を作成し、初期化します：

```
cluster_dst::> snapmirror protect -path-list svm1:volA, svm1:volB
-destination-vserver svm_sync -policy Sync
```



SnapVaultおよび統合レプリケーション ポリシーでは、デスティネーションで最後に転送されたSnapshotのコピーを作成するスケジュールを定義すると便利です。詳細については、"[デスティネーションでローカル コピーを作成するスケジュールの定義](#)"を参照してください。

終了後の操作

`snapmirror show` コマンドを使用して、SnapMirror関係が作成されたことを確認します。

`snapmirror show`の詳細については、[link:https://docs.netapp.com/us-en/ontap-cli/snapmirror-show.html](https://docs.netapp.com/us-en/ontap-cli/snapmirror-show.html)["ONTAPコマンド リファレンス"]を参照してください。

関連情報

- "[job show](#)"

ワンステップでのレプリケーション関係の設定

ONTAP SnapMirrorデスティネーション ボリュームを作成する

デスティネーションで `volume create` コマンドを使用して、デスティネーション ボリュームを作成できます。デスティネーション ボリュームのサイズは、ソース ボリュームと同じかそれ以上である必要があります。"[ONTAPコマンド リファレンス](#)"での `volume create` の詳細を確認してください。

手順

1. デスティネーション ボリュームを作成します：

```
volume create -vserver SVM -volume volume -aggregate aggregate -type DP -size
size
```

次の例では、`volA\_dst`という名前の2GBのデスティネーション ボリュームを作成します：

```
cluster_dst::> volume create -vserver SVM_backup -volume volA_dst
-aggregate node01_aggr -type DP -size 2GB
```

ONTAP SnapMirrorレプリケーションジョブスケジュールを作成する

ジョブ スケジュールは、SnapMirrorがスケジュールの割り当て先であるデータ保護関係を自動的に更新するタイミングを決定します。System Managerまたは `job schedule cron create` コマンドを使用して、レプリケーション ジョブ スケジュールを作成できま

す。["ONTAPコマンド リファレンス"](#)の `job schedule cron create` の詳細を確認してください。

タスク概要

ジョブ スケジュールはデータ保護関係の作成時に割り当てます。ジョブ スケジュールを割り当てない場合は、関係を手動で更新する必要があります。

手順

レプリケーション ジョブ スケジュールは、System ManagerまたはONTAP CLIを使用して作成できます。

System Manager

1. 保護 > 概要 に移動し、ローカル ポリシー設定 を展開します。
2. スケジュール ペインで、→をクリックします。
3. スケジュール ウィンドウで、+ Add をクリックします。
4. *スケジュールの追加*ウィンドウで、スケジュール名を入力し、コンテキストとスケジュール タイプ を選択します。
5. *保存*をクリックします。

CLI

1. ジョブ スケジュールを作成します。

```
job schedule cron create -name <job_name> -month <month> -dayofweek  
<day_of_week> -day <day_of_month> -hour <hour> -minute <minute>
```

`-month`、`-dayofweek`、および `-hour` の場合、
`all` を指定して、それぞれ毎月、曜日ごと、および時間ごとにジョブを実行できます。

ONTAP 9.10.1以降では、ジョブ スケジュールにSVMを含めることができます。

```
job schedule cron create -name <job_name> -vserver <Vserver_name>  
-month <month> -dayofweek <day_of_week> -day <day_of_month> -hour  
<hour> -minute <minute>
```



ボリュームSnapMirror関係のFlexVolボリュームに設定可能な最短スケジュール（RPO）は5分です。ボリュームSnapMirror関係のFlexGroupボリュームに設定可能な最短スケジュール（RPO）は30分です。

次の例では、土曜日の午前3：00に実行される `my\_weekly` という名前のジョブ スケジュールを作成します：

```
cluster_dst::> job schedule cron create -name my_weekly -dayofweek  
"Saturday" -hour 3 -minute 0
```

SnapMirrorレプリケーションポリシーをカスタマイズする

カスタムONTAP SnapMirrorレプリケーションポリシーを作成する

関係のデフォルト ポリシーが適切でない場合は、カスタム レプリケーション ポリシーを作成できます。たとえば、ネットワーク転送でデータを圧縮したり、SnapMirror

がSnapshotを転送する試行回数を変更したりできます。

レプリケーション関係を作成する際には、デフォルトポリシーまたはカスタムポリシーを使用できます。カスタムアーカイブ（旧称SnapVault）または統合レプリケーションポリシーの場合は、初期化時および更新時に転送するスナップショットを決定する1つ以上の_ルール_を定義する必要があります。また、デスティネーションにローカルスナップショットを作成するスケジュールを定義することもできます。

レプリケーション ポリシーの_ポリシー タイプ_によって、サポートされる関係のタイプが決まります。次の表に、使用可能なポリシー タイプを示します。

ポリシー タイプ	関係タイプ
async-mirror	SnapMirror DR
バックアップ	SnapVault
mirror-vault	ユニファイド レプリケーション
strict-sync-mirror	StrictSyncモードのSnapMirror同期（ONTAP 9.5以降でサポート）
sync-mirror	SyncモードのSnapMirror同期（ONTAP 9.5以降でサポート）



カスタム レプリケーション ポリシーを作成する場合は、デフォルト ポリシーをモデルとすることを推奨します。

手順

カスタム データ保護ポリシーは、System ManagerまたはONTAP CLIを使用して作成できます。ONTAP 9.11.1以降では、System Managerを使用して、カスタムのミラー ポリシーとバックアップ ポリシーの作成、従来のポリシーの表示と選択を行うことができます。この機能は、ONTAP 9.8P12およびそれ以降のONTAP 9.8のパッチでも使用できます。

カスタムの保護ポリシーはソース クラスタとデスティネーション クラスタの両方で作成してください。

System Manager

1. **[保護] > [概要] > [ローカル ポリシー設定]**をクリックします。
2. ***保護ポリシー***で、**→**をクリックします。
3. 保護ポリシー ペインで、**+ Add**をクリックします。
4. 新しいポリシー名を入力し、ポリシーのスコープを選択します。
5. ポリシーのタイプを選択します。vault-onlyまたはmirror-onlyポリシーを追加するには、***Asynchronous***を選択し、***Use a legacy policy type***をクリックします。
6. 必須フィールドに入力します。
7. ***保存***をクリックします。
8. もう一方のクラスタに対して同じ手順を繰り返します。

CLI

1. カスタム レプリケーション ポリシーを作成します。

```
snapmirror policy create -vserver <SVM> -policy _policy_ -type  
<async-mirror|vault|mirror-vault|strict-sync-mirror|sync-mirror>  
-comment <comment> -tries <transfer_tries> -transfer-priority  
<low|normal> -is-network-compression-enabled <true|false>
```

ONTAP 9.5以降では、`-common-snapshot-schedule`パラメータを使用して、SnapMirror同期関係の共通Snapshotスケジュールを作成するためのスケジュールを指定できます。デフォルトでは、SnapMirror同期関係の共通Snapshotスケジュールは1時間です。SnapMirror同期関係のSnapshotスケジュールには、30分から2時間までの値を指定できます。

次の例は、データ転送のためにネットワーク圧縮を有効にする、SnapMirror DR用のカスタム レプリケーション ポリシーを作成します。

```
cluster_dst::> snapmirror policy create -vserver svm1 -policy  
DR_compressed -type async-mirror -comment "DR with network  
compression enabled" -is-network-compression-enabled true
```

次の例は、SnapVault用のカスタム レプリケーション ポリシーを作成します。

```
cluster_dst::> snapmirror policy create -vserver svm1 -policy  
my_snapvault -type vault
```

次の例は、ユニファイド レプリケーション用のカスタム レプリケーション ポリシーを作成します。

```
cluster_dst::> snapmirror policy create -vserver svm1 -policy  
my_unified -type mirror-vault
```

次の例は、StrictSyncモードのSnapMirror同期関係用のカスタム レプリケーション ポリシーを作成します。

```
cluster_dst::> snapmirror policy create -vserver svml -policy  
my_strictsync -type strict-sync-mirror -common-snapshot-schedule  
my_sync_schedule
```

```
`snapmirror policy create`  
の詳細については、link:https://docs.netapp.com/us-en/ontap-  
cli/snapmirror-policy-create.html["ONTAPコマンド リファレンス  
"^]を参照してください。
```

終了後の操作

「vault」および「mirror-vault」ポリシー タイプの場合、初期化および更新中に転送される Snapshot を決定するルールを定義する必要があります。

```
`snapmirror policy show`コマンドを使用して、  
SnapMirrorポリシーが作成されたことを確認します。
```

```
`snapmirror policy show`の詳細については、link:https://docs.netapp.com/us-  
en/ontap-cli/snapmirror-policy-show.html["ONTAPコマンド リファレンス  
"^]を参照してください。
```

ONTAP SnapMirrorポリシーのルールを定義する

`vault`または `mirror-vault`ポリシー タイプのカスタム
ポリシーでは、初期化および更新時に転送されるスナップショットを決定するルールを少なくとも1
つ定義する必要があります。 `vault`または `mirror-vault`ポリシー タイプのデフォルト
ポリシーにもルールを定義できます。

タスク概要

`vault`または `mirror-vault`ポリシー
タイプを持つすべてのポリシーには、レプリケートするSnapshotを指定するルールが必要です。た
とえば、ルール `bi-monthly`は、SnapMirrorラベル `bi-monthly`
が割り当てられたSnapshotのみをレプリケートすることを示します。SnapMirrorラベルは、ソー
スでSnapshotポリシーを設定するときに指定します。

各ポリシー タイプは、システム定義の1つ以上のルールに関連付けられています。これらのルールは、ポリシ

ータイプの指定時にポリシーに自動的に割り当てられます。次の表は、システム定義のルールを示しています。

システム定義のルール	ポリシータイプで使用	結果
sm_created	async-mirror、mirror-vault、Sync、StrictSync	SnapMirrorによって作成されたスナップショットは、初期化および更新時に転送されます。
all_source_snapshots	async-mirror	ソース上の新しいスナップショットは、初期化および更新時に転送されます。
daily	vault、mirror-vault	SnapMirrorラベルの付いたソース上の新しいスナップショット`daily`は、初期化および更新時に転送されます。
weekly	vault、mirror-vault	SnapMirrorラベルの付いたソース上の新しいスナップショット`weekly`は、初期化および更新時に転送されます。
monthly	mirror-vault	SnapMirrorラベルの付いたソース上の新しいスナップショット`monthly`は、初期化および更新時に転送されます。
app_consistent	Sync、StrictSync	SnapMirrorラベル`app_consistent`が付いたソース上のスナップショットは、同期的にデスティネーションに複製されます。ONTAP 9.7以降でサポートされます。

「async-mirror」ポリシータイプを除き、必要に応じて、デフォルトポリシーまたはカスタムポリシーに追加のルールを指定できます。例：

- デフォルト MirrorAndVault`ポリシーの場合、`bi-monthly`というルールを作成して、ソース上のスナップショットを`bi-monthly SnapMirrorラベルと一致させることができます。
- mirror-vault`ポリシータイプのカスタムポリシーの場合、`bi-weekly SnapMirrorラベルを持つソース上のスナップショットと一致させる`bi-weekly`というルールを作成できます。

手順

1. ポリシーのルールを定義します。

```
snapmirror policy add-rule -vserver SVM -policy policy_for_rule -snapmirror  
-label snapmirror-label -keep retention_count
```

次の例では、SnapMirrorラベル`bi-monthly`付きのルールをデフォルト`MirrorAndVault`ポリシーに追加します：

```
cluster_dst:> snapmirror policy add-rule -vserver svml -policy MirrorAndVault -snapmirror-label bi-monthly -keep 6
```

次の例では、SnapMirrorラベル `bi-weekly` を持つルールをカスタム `my\_snapvault` ポリシーに追加します：

```
cluster_dst:> snapmirror policy add-rule -vserver svml -policy my_snapvault -snapmirror-label bi-weekly -keep 26
```

次の例では、SnapMirrorラベル `app\_consistent` を持つルールをカスタム `Sync` ポリシーに追加します：

```
cluster_dst:> snapmirror policy add-rule -vserver svml -policy Sync -snapmirror-label app_consistent -keep 1
```

```
`snapmirror policy add-rule`
```

の詳細については、[link:https://docs.netapp.com/us-en/ontap-cli/snapmirror-policy-add-rule.html](https://docs.netapp.com/us-en/ontap-cli/snapmirror-policy-add-rule.html)["ONTAP コマンド リファレンス"]をご覧ください。

次に、このSnapMirrorラベルに一致するソース クラスタからスナップショットを複製できます：

```
cluster_src:> snapshot create -vserver vs1 -volume vol1 -snapshot snapshot1 -snapmirror-label app_consistent
```

ONTAP SnapMirror スケジュールを定義して、デスティネーションにローカル コピーを作成します

SnapVault および統合レプリケーション関係では、デスティネーションで最後に転送されたスナップショットのコピーを作成することで、更新されたスナップショットが破損する可能性を回避できます。この「ローカル コピー」は、ソースの保持ルールに関係なく保持されるため、SnapMirrorによって最初に転送されたスナップショットがソースで使用できなくなった場合でも、そのコピーはデスティネーションで使用できます。

タスク概要

`snapmirror policy add-rule` コマンドの `--schedule` オプションで、ローカル コピーを作成するスケジュールを指定します。

手順

1. デスティネーションでローカル コピーを作成するスケジュールを定義します。

```
snapmirror policy add-rule -vserver SVM -policy policy_for_rule -snapmirror-label snapmirror-label -schedule schedule
```

ジョブ スケジュールを作成する方法の例については、"[レプリケーション ジョブ スケジュールの作成](#)"を参照してください。

次の例では、ローカル コピーを作成するスケジュールをデフォルトの `MirrorAndVault` ポリシーに追加します：

```
cluster_dst:> snapmirror policy add-rule -vserver svml -policy
MirrorAndVault -snapmirror-label my_monthly -schedule my_monthly
```

次の例では、ローカル コピーを作成するためのスケジュールをカスタム `my\_unified` ポリシーに追加します：

```
cluster_dst:> snapmirror policy add-rule -vserver svml -policy
my_unified -snapmirror-label my_monthly -schedule my_monthly
```

```
`snapmirror policy add-rule`
```

の詳細については、[link:https://docs.netapp.com/us-en/ontap-cli/snapmirror-policy-add-rule.html](https://docs.netapp.com/us-en/ontap-cli/snapmirror-policy-add-rule.html)["ONTAP コマンド リファレンス"]をご覧ください。

ONTAP SnapMirrorレプリケーション関係を作成する

プライマリ ストレージのソース ボリュームとセカンダリ ストレージのデスティネーション ボリュームの関係は、データ保護関係と呼ばれます。`snapmirror create` コマンドを使用して、SnapMirror DR、SnapVault、または統合レプリケーション データ保護関係を作成できます。



この手順はFAS、AFF、およびASAシステムに適用されます。ASA r2システム（ASAA1K、ASAA90、ASAA70、ASAA50、ASAA30、ASAA20、またはASA C30）をお持ちの場合は、"[これらの手順](#)"に従ってレプリケーション関係を作成してください。ASA r2システムは、SANのみのお客様向けに簡素化されたONTAPエクスペリエンスを提供します。

ONTAP 9.11.1以降では、ボリュームとStorage VMを保護する際、System Managerを使用して、事前作成済みおよびカスタムのミラー ポリシーとバックアップ ポリシーの選択、従来のポリシーの表示と選択、保護ポリシーに定義された転送スケジュールの上書きを行うことができます。この機能は、ONTAP 9.8P12およびそれ以降のONTAP 9.8のパッチでも使用できます。



ONTAP 9.8P12またはそれ以降のONTAP 9.8パッチ リリースを使用していて、System ManagerからSnapMirrorを設定した場合、ONTAP 9.9.1またはONTAP 9.10.1リリースへのアップグレードにはONTAP 9.9.1P13以降およびONTAP 9.10.1P10以降のパッチ リリースを使用する必要があります。

開始する前に

- ソース / デスティネーション クラスタとSVMのピア関係が確立されている必要があります。

["クラスタとSVMのピアリング"](#)

- デスティネーション ボリューム上の言語は、ソース ボリューム上の言語と同じである必要があります。

タスク概要

ONTAP 9.3までは、DPモードで起動するSnapMirrorとXDPモードで起動するSnapMirrorは異なるレプリケーション エンジンを使用しており、バージョン依存性に対するアプローチも異なっていました。

- SnapMirrorがDPモードで呼び出された場合は、_バージョン依存_のレプリケーション エンジンが使用され、プライマリ ストレージとセカンダリ ストレージでONTAPバージョンが同じである必要がありました。

```
cluster_dst::> snapmirror create -type DP -source-path ... -destination-path ...
```

- XDPモードで呼び出されたSnapMirrorは、プライマリ ストレージとセカンダリ ストレージで異なるONTAPバージョンをサポートする_バージョンに依存しない_レプリケーション エンジンを使用しました：

```
cluster_dst::> snapmirror create -type XDP -source-path ... -destination-path ...
```

パフォーマンスの改善に伴い、レプリケーション スループットではバージョンに依存するモードの方がわずかに優れてはいるものの、バージョンに依存しないSnapMirrorの方がはるかに大きなメリットが得られるようになりました。そのため、ONTAP 9.3以降ではXDPモードが新しいデフォルト値となり、コマンドラインまたは新規 / 既存のスクリプトにおけるDPモードの起動は自動的にXDPモードに変換されます。

既存の関係には影響しません。DPタイプの既存の関係は引き続きDPタイプになります。次の表は、想定される動作を示しています。

指定するモード	タイプ	デフォルト ポリシー（ポリシーを指定しない場合）
DP	XDP	MirrorAllSnapshots（SnapMirror DR）
なし	XDP	MirrorAllSnapshots（SnapMirror DR）
XDP	XDP	XDPDefault（SnapVault）

以下の手順の例も参照してください。

以下は例外です。

- SVMデータ保護関係のデフォルトは引き続きDPモードです。

デフォルトの `MirrorAllSnapshots` ポリシーで XDP モードを取得するには、XDP を明示的に指定します。

- 負荷共有データ保護関係のデフォルトは引き続きDPモードです。
- SnapLockデータ保護関係のデフォルトは引き続きDPモードです。

- 次のクラスタ全体のオプションを設定した場合、DPを明示的に指定した場合のデフォルトは引き続きDPモードです。

```
options replication.create_data_protection_rels.enable on
```

DPを明示的に指定しない場合、このオプションは無視されます。

ONTAP 9.14.1以降では、`-backoff-level``オプションが ``snapmirror create`、`snapmirror modify`、および ``snapmirror restore`` コマンドに追加され、関係ごとにバックオフレベルを指定できるようになりました。このオプションはFlexVol SnapMirror関係でのみサポートされます。オプションのコマンドは、クライアントオペレーションによるSnapMirrorバックオフレベルを指定します。バックオフ値は、`high`、`medium`、`none`のいずれかに設定できます。デフォルト値は`high`です。

ONTAP 9.5以降では、SnapMirror同期関係がサポートされます。

ONTAP 9.4以降では、デスティネーション ボリュームに最大1019個のSnapshotを保存できます。ONTAP 9.3以前では、デスティネーション ボリュームに最大251個のSnapshotを保存できます。

手順

System ManagerまたはONTAP CLIを使用して、レプリケーション関係を作成できます。

System Manager

1. 保護するボリュームまたはLUNを選択します。[ストレージ] > [ボリューム]*または[ストレージ] > [LUN]*をクリックし、ボリュームまたはLUNの名前をクリックします。
2.  **Protect** をクリックします。
3. デスティネーションのクラスタとStorage VMを選択します。
4. デフォルトでは非同期ポリシーが選択されます。同期ポリシーを選択するには、*[その他のオプション]*をクリックします。
5. *[保護]*をクリックします。
6. 選択したボリュームまたはLUNの*[SnapMirror（ローカルまたはリモート）]*タブをクリックし、保護が正しくセットアップされたことを確認します。

CLI

1. デスティネーション クラスタから、レプリケーション関係を作成します。

このコマンドを実行する前に、山カッコ内の変数を必要な値に置き換える必要があります。

```
snapmirror create -source-path <SVM:volume> -destination-path  
<SVM:volume> -type <DP|XDP> -schedule <schedule> -policy <policy>
```



`schedule`パラメータは、SnapMirror同期関係を作成する場合は適用されません。

次の例では、デフォルト `MirrorLatest` ポリシーを使用してSnapMirror DR関係を作成します：

```
cluster_dst:> snapmirror create -source-path svm1:volA -destination  
-path svm_backup:volA_dst -type XDP -schedule my_daily -policy  
MirrorLatest
```

次の例では、デフォルト `XDPDefault` ポリシーを使用してSnapVault関係を作成します：

```
cluster_dst:> snapmirror create -source-path svm1:volA -destination  
-path svm_backup:volA_dst -type XDP -schedule my_daily -policy  
XDPDefault
```

次の例では、デフォルトの `MirrorAndVault` ポリシーを使用して統合レプリケーション関係を作成します：

```
cluster_dst:> snapmirror create -source-path svm1:volA -destination  
-path svm_backup:volA_dst -type XDP -schedule my_daily -policy  
MirrorAndVault
```


次の例では、カスタム `my\_unified` ポリシーを使用して統合レプリケーション関係を作成します：

```
cluster_dst:> snapmirror create -source-path svm1:volA -destination  
-path svm_backup:volA_dst -type XDP -schedule my_daily -policy  
my_unified
```

次の例では、デフォルトの `Sync` ポリシーを使用してSnapMirror同期関係を作成します：

```
cluster_dst:> snapmirror create -source-path svm1:volA -destination  
-path svm_backup:volA_dst -type XDP -policy Sync
```

次の例では、デフォルトの `StrictSync` ポリシーを使用してSnapMirror同期関係を作成します：

```
cluster_dst:> snapmirror create -source-path svm1:volA -destination  
-path svm_backup:volA_dst -type XDP -policy StrictSync
```

以下の例では、SnapMirror DR関係を作成します。DPタイプは自動的にXDPに変換され、ポリシーは指定されていないため、ポリシーは `MirrorAllSnapshots` ポリシーにデフォルト設定されます：

```
cluster_dst:> snapmirror create -source-path svm1:volA -destination  
-path svm_backup:volA_dst -type DP -schedule my_daily
```

次の例では、SnapMirror DR関係を作成します。タイプまたはポリシーを指定しない場合、ポリシーは `MirrorAllSnapshots` ポリシーにデフォルト設定されます：

```
cluster_dst:> snapmirror create -source-path svm1:volA -destination  
-path svm_backup:volA_dst -schedule my_daily
```

次の例では、SnapMirror DR関係を作成します。ポリシーを指定しない場合、ポリシーは `XDPDefault` ポリシーにデフォルト設定されます：

```
cluster_dst:> snapmirror create -source-path svm1:volA -destination  
-path svm_backup:volA_dst -type XDP -schedule my_daily
```

次の例では、定義済みポリシー `SnapCenterSync` を使用してSnapMirror同期関係を作成します：

```
cluster_dst:> snapmirror create -source-path svm1:volA -destination  
-path svm_backup:volA_dst -type XDP -policy SnapCenterSync
```



定義済みポリシー `SnapCenterSync` のタイプは `Sync` です。このポリシーは、`snapmirror-label` が「app_consistent」で作成されたスナップショットをすべて複製します。

終了後の操作

`snapmirror show` コマンドを使用して、SnapMirror関係が作成されたことを確認します。

`snapmirror show` の詳細については、[link:https://docs.netapp.com/us-en/ontap-cli/snapmirror-show.html](https://docs.netapp.com/us-en/ontap-cli/snapmirror-show.html) ["ONTAP コマンド リファレンス"] を参照してください。

関連情報

- ["SnapMirror フェイルオーバー テスト ボリュームの作成と削除"](#)。

ONTAP でこの処理を行うその他の方法

タスクを実行するツール	参照するコンテンツ
System Manager Classic (ONTAP 9.7 以前で使用可能)	"SnapVault を使用したボリューム バックアップの概要"

関連情報

- ["snapmirror create"](#)

ONTAP SnapMirror レプリケーション関係を初期化する

どのタイプの関係性においても、初期化時に ベースライン転送 が実行されます：つまり、ソース ボリュームのスナップショットを作成し、そのコピーとそれが参照するすべてのデータ ブロックをデスティネーション ボリュームに転送します。それ以外の場合、転送内容はポリシーによって異なります。

開始する前に

ソース / デスティネーション クラスタと SVM のピア関係が確立されている必要があります。

["クラスタとSVMのピアリング"](#)

タスク概要

初期化には時間がかかる場合があります。ベースライン転送はオフピークの時間帯に実行することを推奨します。

ONTAP 9.5 以降では、SnapMirror 同期関係がサポートされます。

ノードの再起動、テイクオーバー/ギブバック、パニックなど、何らかの理由でファイル システムが再起動された場合、初期化は自動的に再開されず、手動で再起動する必要があることに注意してください。

手順

1. レプリケーション関係を初期化します。

```
snapmirror initialize -source-path <SVM:volume>|<cluster://SVM/volume>, ...  
-destination-path <SVM:volume>|<cluster://SVM/volume>, ...
```



このコマンドはデスティネーションSVMまたはデスティネーション クラスタから実行する必要があります。

次の例では、`svm1`のソース ボリューム `volA`と `svm\_backup`のデスティネーション ボリューム `volA\_dst`間の関係を初期化します：

```
cluster_dst::> snapmirror initialize -source-path svm1:volA -destination  
-path svm_backup:volA_dst
```

`snapmirror initialize`の詳細については、[link:https://docs.netapp.com/us-en/ontap-cli/snapmirror-initialize.html](https://docs.netapp.com/us-en/ontap-cli/snapmirror-initialize.html)["ONTAPコマンド リファレンス"]を参照してください。

ONTAPミラー - Vaultデプロイメントで共通のSnapshotを確保する

`snapmirror snapshot-owner create`コマンドを使用すると、ミラー - ヴォールト構成において、ラベル付きSnapshotをセカンダリ上に保存できます。これにより、ヴォールト関係の更新時に共通のSnapshotが確保されます。

タスク概要

ミラー ヴォールト ファンアウトまたはカスケード展開の組み合わせを使用する場合は、ソース ボリュームとデスティネーション ボリュームに共通の Snapshot が存在しない場合は更新が失敗することに注意してください。

ミラー ボールト ファンアウトまたはカスケード展開のミラー関係では、SnapMirrorは更新を実行する前に常にソース ボリュームのスナップショットを作成するため、これが問題になることはありません。

ただし、SnapMirrorはボールト関係を更新する際にソースボリュームのスナップショットを作成しないため、ボールト関係に問題が発生する可能性があります。`snapmirror snapshot-owner create`を使用して、ボールト関係のソースとデスティネーションの両方に少なくとも1つの共通スナップショットが存在することを確認する必要があります。["データ保護のファンアウトとカスケード展開の詳細"](#)。

手順

1. ソース ボリュームで、保存するラベル付き Snapshot に所有者を割り当てます：

```
snapmirror snapshot-owner create -vserver <SVM> -volume <volume> -snapshot  
<snapshot> -owner <owner>
```

次の例では、`ApplicationA`を `snap1`スナップショットの所有者として割り当てます：

```
clust1::> snapmirror snapshot-owner create -vserver vs1 -volume vol1
-snapshot snap1 -owner ApplicationA
```

```
`snapmirror snapshot-owner create`
```

の詳細については、link:<https://docs.netapp.com/us-en/ontap-cli/snapmirror-snapshot-owner-create.html>["ONTAPコマンド リファレンス"]を参照してください。

2. "手動によるレプリケーション関係の更新"の説明に従って、ミラー関係を更新します。

または、スケジュールされたミラー関係の更新が実行されるまで待つこともできます。

3. ラベル付けされたスナップショットを Vault のデスティネーションに転送します：

```
snapmirror update -source-path <SVM:volume>|<cluster://SVM/volume>, ...
-destination-path <SVM:volume>|<cluster://SVM/volume>, ... -source-snapshot
snapshot
```

次の例では `snap1` スナップショットを転送します

```
clust1::> snapmirror update -vserver vs1 -volume vol1
-source-snapshot snap1
```

ボールド関係が更新されても、ラベル付けされた Snapshot は保持されます。

```
`snapmirror update`の詳細については、link:https://docs.netapp.com/us-en/ontap-cli/snapmirror-update.html["ONTAPコマンド リファレンス"]をご覧ください。
```

4. ソース ボリュームで、ラベルの付いたスナップショットから所有者を削除します：

```
snapmirror snapshot-owner delete -vserver SVM -volume volume -snapshot
snapshot -owner owner
```

次の例では、`snap1` スナップショットの所有者として `ApplicationA` を削除します：

```
clust1::> snapmirror snapshot-owner delete -vserver vs1 -volume vol1
-snapshot snap1 -owner ApplicationA
```

```
`snapmirror snapshot-owner delete`
```

の詳細については、link:<https://docs.netapp.com/us-en/ontap-cli/snapmirror-snapshot-owner-delete.html>["ONTAPコマンド リファレンス"]を参照してください。

例：ONTAP SnapMirror vault-vault カスケードを構成する

レプリケーション関係を段階的に設定する方法を、具体的な例で示します。例で設定したvault-vaultカスケード展開を使用すると、`my-weekly`というラベルの付いたスナップショットを251個以上保持できます。

開始する前に

ソース / デスティネーション クラスタとSVMのピア関係が確立されている必要があります。

タスク概要

この例では、次のことを前提としています：

- ソース クラスタでSnapMirrorラベル my-daily、 my-weekly、 および `my-monthly`を使用してSnapshotを設定しました。
- セカンダリおよび三次デスティネーション クラスタで `volA`という名前のデスティネーション ボリュームを設定しました。
- セカンダリおよび三次デスティネーション クラスタで `my\_snapvault`という名前のレプリケーション ジョブ スケジュールを設定しました。

この例では、2つのカスタム ポリシーに基づいてレプリケーション関係を作成する方法を示します。

- この `snapvault\_secondary`ポリシーは、セカンダリ デスティネーション クラスタ上に7つの日次、52の週次、および180の月次Snapshotを保持します。
- `snapvault\_tertiary policy`は、第3のデスティネーション クラスタに250個の週次Snapshotを保持します。

手順

1. セカンダリ デスティネーション クラスタで、 `snapvault\_secondary`ポリシーを作成します：

```
cluster_secondary::> snapmirror policy create -policy snapvault_secondary  
-type vault -comment "Policy on secondary for vault to vault cascade" -vserver  
svm_secondary
```

2. セカンダリ デスティネーション クラスタで、ポリシーの `my-daily`ルールを定義します：

```
cluster_secondary::> snapmirror policy add-rule -policy snapvault_secondary  
-snapmirror-label my-daily -keep 7 -vserver svm_secondary
```

3. セカンダリ デスティネーション クラスタで、ポリシーの `my-weekly`ルールを定義します：

```
cluster_secondary::> snapmirror policy add-rule -policy snapvault_secondary  
-snapmirror-label my-weekly -keep 52 -vserver svm_secondary
```

4. セカンダリ デスティネーション クラスタで、ポリシーの `my-monthly`ルールを定義します：

```
cluster_secondary::> snapmirror policy add-rule -policy snapvault_secondary  
-snapmirror-label my-monthly -keep 180 -vserver svm_secondary
```

5. セカンダリ デスティネーション クラスタで、ポリシーを確認します：

```
cluster_secondary::> snapmirror policy show snapvault_secondary -instance
```

```

Vserver: svm_secondary
SnapMirror Policy Name: snapvault_secondary
SnapMirror Policy Type: vault
Policy Owner: cluster-admin
Tries Limit: 8
Transfer Priority: normal
Ignore accesstime Enabled: false
Transfer Restartability: always
Network Compression Enabled: false
Create Snapshot: false
Comment: Policy on secondary for vault to vault
cascade
Total Number of Rules: 3
Total Keep: 239
Rules: SnapMirror Label      Keep  Preserve Warn
Schedule Prefix
-----
-----
my-daily              7  false      0  -
-
my-weekly            52  false      0  -
-
my-monthly          180  false      0  -
-

```

6. セカンダリ デスティネーション クラスタで、ソース クラスタとの関係を作成します：

```
cluster_secondary::> snapmirror create -source-path svm_primary:volA
-destination-path svm_secondary:volA -type XDP -schedule my_snapvault -policy
snapvault_secondary
```

7. セカンダリ デスティネーション クラスタで、ソース クラスタとの関係を初期化します：

```
cluster_secondary::> snapmirror initialize -source-path svm_primary:volA
-destination-path svm_secondary:volA
```

8. 3 番目のデスティネーション クラスタで、`snapvault\_tertiary`ポリシーを作成します：

```
cluster_tertiary::> snapmirror policy create -policy snapvault_tertiary -type
vault -comment "Policy on tertiary for vault to vault cascade" -vserver
svm_tertiary
```

9. 3 番目のデスティネーション クラスタで、ポリシーの `my-weekly`ルールを定義します：

```
cluster_tertiary::> snapmirror policy add-rule -policy snapvault_tertiary
-snapmirror-label my-weekly -keep 250 -vserver svm_tertiary
```

10. 3番目のデスティネーション クラスタで、ポリシーを検証します。

```
cluster_tertiary::> snapmirror policy show snapvault_tertiary -instance
```

```

                Vserver: svm_tertiary
SnapMirror Policy Name: snapvault_tertiary
SnapMirror Policy Type: vault
                Policy Owner: cluster-admin
                Tries Limit: 8
                Transfer Priority: normal
Ignore accesstime Enabled: false
                Transfer Restartability: always
Network Compression Enabled: false
                Create Snapshot: false
                Comment: Policy on tertiary for vault to vault
cascade
                Total Number of Rules: 1
                        Total Keep: 250
                                Rules: SnapMirror Label          Keep  Preserve Warn
Schedule Prefix
-----
-----
                                my-weekly          250   false      0 -
-
```

11. 3番目のデスティネーション クラスタで、セカンダリ クラスタとの関係を作成します。

```
cluster_tertiary::> snapmirror create -source-path svm_secondary:volA
                        -destination-path svm_tertiary:volA -type XDP -schedule my_snapvault -policy
                        snapvault_tertiary
```

12. 三次デスティネーション クラスタで、二次クラスタとの関係を初期化します：

```
cluster_tertiary::> snapmirror initialize -source-path svm_secondary:volA
                        -destination-path svm_tertiary:volA
```

関連情報

- ["snapmirror create"](#)
- ["snapmirror initialize"](#)
- ["snapmirror policy add-rule"](#)
- ["snapmirror policy create"](#)
- ["snapmirror policy show"](#)

SnapMirrorボリューム レプリケーションの管理

既存のONTAP SnapMirror DPタイプ関係をXDPに変換する

ONTAP 9.12.1以降にアップグレードする場合は、アップグレード前にDPタイプの関係をXDPに変換する必要があります。ONTAP 9.12.1以降では、DPタイプの関係はサポートされません。既存のDPタイプの関係を簡単にXDPに変換して、バージョンに依存しないSnapMirrorを活用できます。

ONTAP 9.12.1以降のリリースにアップグレードする前に、既存のDPタイプの関係をXDPに変換する必要があります。

タスク概要

- SnapMirrorでは、既存のDPタイプの関係をXDPに自動的に変換しません。関係を変換するには、既存の関係を解除して削除し、新しいXDP関係を作成して関係を再同期する必要があります。
- 変換を計画する場合は、XDP SnapMirror関係のバックグラウンドでの準備とデータの保存処理に時間がかかることに注意してください。長時間にわたってSnapMirror関係のステータスが「preparing」と表示されることも珍しくありません。



SnapMirror関係のタイプをDPからXDPに変換すると、オートサイズやスペース ギャランティなどのスペース関連の設定はデスティネーションにレプリケートされなくなります。

手順

1. デスティネーション クラスタから、SnapMirror関係がDPタイプ、ミラー状態がSnapMirrored、関係のステータスがIdle、関係が健全であることを確認します。

```
snapmirror show -destination-path <SVM:volume>
```

次の例は、`snapmirror show` コマンドからの出力を示しています：


```
cluster_dst::>snapmirror show -destination-path svm_backup:volA_dst
```

```
Source Path: svml:volA
Destination Path: svm_backup:volA_dst
Relationship Type: DP
SnapMirror Schedule: -
Tries Limit: -
Throttle (KB/sec): unlimited
Mirror State: Snapmirrored
Relationship Status: Idle
Transfer Snapshot: -
Snapshot Progress: -
Total Progress: -
Snapshot Checkpoint: -
Newest Snapshot: snapmirror.10af643c-32d1-11e3-954b-
123478563412_2147484682.2014-06-27_100026
Newest Snapshot Timestamp: 06/27 10:00:55
Exported Snapshot: snapmirror.10af643c-32d1-11e3-954b-
123478563412_2147484682.2014-06-27_100026
Exported Snapshot Timestamp: 06/27 10:00:55
Healthy: true
```



`snapmirror show` コマンド出力のコピーを保持しておく、既存の関係設定を追跡するのに役立ちます。link:<https://docs.netapp.com/us-en/ontap-cli/snapmirror-show.html>["ONTAP コマンド リファレンス"]の`snapmirror show`の詳細をご覧ください。

2. ソース ボリュームとデスティネーション ボリュームの両方に共通のスナップショットがあることを確認します。

```
volume snapshot show -vserver <SVM> -volume <volume>
```

次の例は、ソース ボリュームとデスティネーション ボリュームの `volume snapshot show` 出力を示しています：

```

cluster_src:> volume snapshot show -vserver svml -volume volA
---Blocks---
Vserver Volume Snapshot State Size Total% Used%
-----
-----
svml volA
weekly.2014-06-09_0736 valid 76KB 0% 28%
weekly.2014-06-16_1305 valid 80KB 0% 29%
daily.2014-06-26_0842 valid 76KB 0% 28%
hourly.2014-06-26_1205 valid 72KB 0% 27%
hourly.2014-06-26_1305 valid 72KB 0% 27%
hourly.2014-06-26_1405 valid 76KB 0% 28%
hourly.2014-06-26_1505 valid 72KB 0% 27%
hourly.2014-06-26_1605 valid 72KB 0% 27%
daily.2014-06-27_0921 valid 60KB 0% 24%
hourly.2014-06-27_0921 valid 76KB 0% 28%
snapmirror.10af643c-32d1-11e3-954b-123478563412_2147484682.2014-06-
27_100026
valid 44KB 0% 19%
11 entries were displayed.

cluster_dest:> volume snapshot show -vserver svm_backup -volume volA_dst
---Blocks---
Vserver Volume Snapshot State Size Total% Used%
-----
-----
svm_backup volA_dst
weekly.2014-06-09_0736 valid 76KB 0% 30%
weekly.2014-06-16_1305 valid 80KB 0% 31%
daily.2014-06-26_0842 valid 76KB 0% 30%
hourly.2014-06-26_1205 valid 72KB 0% 29%
hourly.2014-06-26_1305 valid 72KB 0% 29%
hourly.2014-06-26_1405 valid 76KB 0% 30%
hourly.2014-06-26_1505 valid 72KB 0% 29%
hourly.2014-06-26_1605 valid 72KB 0% 29%
daily.2014-06-27_0921 valid 60KB 0% 25%
hourly.2014-06-27_0921 valid 76KB 0% 30%
snapmirror.10af643c-32d1-11e3-954b-123478563412_2147484682.2014-06-
27_100026

```

3. 変換中にスケジュールされた更新が実行されないようにするために、既存のDPタイプの関係を休止します。

```
snapmirror quiesce -source-path <SVM:volume> -destination-path  
<SVM:volume>
```



このコマンドはデスティネーションSVMまたはデスティネーション クラスタから実行する必要があります。

次の例では、`svm1`のソース ボリューム `volA`と `svm\_backup`のデスティネーション ボリューム `volA\_dst`間の関係を休止します：

```
cluster_dst::> snapmirror quiesce -destination-path svm_backup:volA_dst
```

`snapmirror quiesce`の詳細については、[link:https://docs.netapp.com/us-en/ontap-cli/snapmirror-quiesce.html](https://docs.netapp.com/us-en/ontap-cli/snapmirror-quiesce.html)["ONTAPコマンド リファレンス"]を参照してください。

4. 既存のDPタイプの関係を解除します。

```
snapmirror break -destination-path <SVM:volume>
```



このコマンドはデスティネーションSVMまたはデスティネーション クラスタから実行する必要があります。

次の例では、`svm1`のソース ボリューム `volA`と `svm\_backup`のデスティネーション ボリューム `volA\_dst`の関係を解除します：

```
cluster_dst::> snapmirror break -destination-path svm_backup:volA_dst
```

`snapmirror break`の詳細については、[link:https://docs.netapp.com/us-en/ontap-cli/snapmirror-break.html](https://docs.netapp.com/us-en/ontap-cli/snapmirror-break.html)["ONTAPコマンド リファレンス"]を参照してください。

5. デスティネーション ボリュームでSnapshotの自動削除が有効になっている場合は、無効にします：

```
volume snapshot autodelete modify -vserver _SVM_ -volume _volume_  
-enabled false
```

次の例では、デスティネーション ボリューム上のSnapshotの自動削除を無効にします volA_dst：

```
cluster_dst::> volume snapshot autodelete modify -vserver svm_backup  
-volume volA_dst -enabled false
```

6. 既存のDPタイプの関係を削除します。

```
snapmirror delete -destination-path <SVM:volume>
```

`snapmirror-delete`の詳細については、[link:https://docs.netapp.com/us-en/ontap-cli/snapmirror-delete.html](https://docs.netapp.com/us-en/ontap-cli/snapmirror-delete.html)["ONTAPコマンド リファレンス"]を参照してください。



このコマンドはデスティネーションSVMまたはデスティネーション クラスタから実行する必要があります。

次の例では、`svm1`のソース ボリューム `volA`と `svm\_backup`のデスティネーション ボリューム `volA\_dst`間の関係を削除します：

```
cluster_dst::> snapmirror delete -destination-path svm_backup:volA_dst
```

7. ソースで元のSVMディザスタ リカバリ関係をリリースします。

```
snapmirror release -destination-path <SVM:volume> -relationship-info  
-only true
```

次の例では、SVMディザスタ リカバリ関係をリリースしています。

```
cluster_src::> snapmirror release -destination-path svm_backup:volA_dst  
-relationship-info-only true
```

`snapmirror release`の詳細については、[link:https://docs.netapp.com/us-en/ontap-cli/snapmirror-release.html](https://docs.netapp.com/us-en/ontap-cli/snapmirror-release.html)["ONTAPコマンド リファレンス"]を参照してください。

8. `snapmirror show`コマンドから保持した出力を使用して、新しいXDPタイプの関係を作成できます：

```
snapmirror create -source-path <SVM:volume> -destination-path  
<SVM:volume> -type XDP -schedule <schedule> -policy <policy>
```

新しい関係では、同じソースボリュームとデスティネーションボリュームを使用する必要があります。この手順で説明するコマンドの詳細については、"[ONTAPコマンド リファレンス](#)"を参照してください。



このコマンドはデスティネーションSVMまたはデスティネーション クラスタから実行する必要があります。

次の例では、SnapMirrorディザスタ リカバリ関係を、`svm1`のソース ボリューム `volA`と `svm\_backup`のデスティネーション ボリューム `volA\_dst`の間に、デフォルトの `MirrorAllSnapshots`ポリシーを使用して作成します：

```
cluster_dst::> snapmirror create -source-path svm1:volA -destination
-path svm_backup:volA_dst
-type XDP -schedule my_daily -policy MirrorAllSnapshots
```

9. ソース ボリュームとデスティネーション ボリュームを再同期します。

```
snapmirror resync -source-path <SVM:volume> -destination-path
<SVM:volume>
```

再同期時間を短縮するには、`-quick-resync`オプションを使用できますが、ストレージ効率の節約が失われる可能性があることに注意してください。



このコマンドはデスティネーションSVMまたはデスティネーション クラスタから実行する必要があります。再同期の際にベースライン転送は不要ですが、再同期には時間がかかる場合があります。再同期はオフピークの時間帯に実行することを推奨します。

次の例では、`svm1`のソース ボリューム `volA`と `svm\_backup`のデスティネーション ボリューム `volA\_dst`間の関係を再同期します：

```
cluster_dst::> snapmirror resync -source-path svm1:volA -destination
-path svm_backup:volA_dst
```

`snapmirror resync`の詳細については、[link:https://docs.netapp.com/us-en/ontap-cli/snapmirror-resync.html#parameters.html](https://docs.netapp.com/us-en/ontap-cli/snapmirror-resync.html#parameters.html)["ONTAPコマンド リファレンス"]を参照してください。

10. スナップショットの自動削除を無効にした場合は、再度有効にします：

```
volume snapshot autodelete modify -vserver <SVM> -volume <volume>
-enabled true
```

終了後の操作

1. `snapmirror show` コマンドを使用して、SnapMirror関係が作成されたことを確認します。

`snapmirror show`の詳細については、link:<https://docs.netapp.com/us-en/ontap-cli/snapmirror-show.html>["ONTAPコマンド リファレンス"]を参照してください。

2. SnapMirror XDP デスティネーション ボリュームが SnapMirror ポリシーの定義に従ってスナップショットの更新を開始したら、ソース クラスタからの `snapmirror list-destinations` コマンドの出力を使用して、新しい SnapMirror XDP 関係を表示します。

DP型関係に関する追加情報

ONTAP 9.3 以降では、XDP モードがデフォルトとなり、コマンド ラインまたは新規または既存のスクリプトでの DP モードの呼び出しはすべて自動的に XDP モードに変換されます。

既存の関係は影響を受けません。関係がすでにDPタイプの場合、引き続きDPタイプのままとまります。ONTAP 9.5以降では、データ保護モードが指定されていない場合、または関係タイプとしてXDPモードが指定されている場合、MirrorAndVaultがデフォルトポリシーとなります。以下の表は、想定される動作を示しています。

指定するモード	タイプ	デフォルト ポリシー（ポリシーを指定しない場合）
DP	XDP	MirrorAllSnapshots（SnapMirror DR）
なし	XDP	MirrorAndVault（ユニファイド レプリケーション）
XDP	XDP	MirrorAndVault（ユニファイド レプリケーション）

表に示すように、さまざまな状況でXDPに割り当てられるデフォルトポリシーにより、変換後も以前のタイプとの機能的な同等性が維持されます。もちろん、必要に応じて、統合レプリケーション用のポリシーなど、異なるポリシーを使用することもできます：

指定するモード	そしてポリシーは...	結果は...
DP	MirrorAllSnapshots	SnapMirror DR
XDPDefault	SnapVault	MirrorAndVault
ユニファイド レプリケーション	XDP	MirrorAllSnapshots
SnapMirror DR	XDPDefault	SnapVault

以下は例外です。

- ONTAP 9.3以前のSVMデータ保護関係のデフォルトは引き続きDPモードです。

ONTAP 9.4以降では、SVMデータ保護関係のデフォルトがXDPモードに変更されました。

- ルート ボリュームの負荷共有データ保護関係のデフォルト値は引き続きDPモードです。
- ONTAP 9.4以前のSnapLockデータ保護関係のデフォルトは引き続きDPモードです。

ONTAP 9.5以降では、SnapLockデータ保護関係のデフォルトがXDPモードに変更されました。

- 次のクラスタ全体のオプションを設定した場合、DPを明示的に指定した場合のデフォルトは引き続きDPモードです。

```
options replication.create_data_protection_rels.enable on
```

DPを明示的に指定しない場合、このオプションは無視されます。

関連情報

- ["snapmirror create"](#)
- ["snapmirror delete"](#)
- ["snapmirror quiesce"](#)
- ["snapmirror release"](#)
- ["snapmirror resync"](#)

ONTAP SnapMirror関係のタイプを変換する

ONTAP 9.5以降では、SnapMirror同期がサポートされます。SnapMirror非同期関係とSnapMirror同期関係は、ベースライン転送を実行しなくても相互に変換することができます。

タスク概要

SnapMirrorポリシーを変更して、SnapMirror非同期関係をSnapMirror同期関係に変換したり、その逆を行ったりすることはできません。

手順

- **SnapMirror非同期関係をSnapMirror同期関係に変換する**

- a. デスティネーション クラスタから、SnapMirror非同期関係を削除します。

```
snapmirror delete -destination-path <SVM:volume>
```

```
cluster2::>snapmirror delete -destination-path vs1_dr:vol1
```

- b. ソース クラスターから、共通スナップショットを削除せずにSnapMirror関係を解除します：

```
snapmirror release -relationship-info-only true -destination-path
```

```
<destination_SVM>:<destination_volume>
```

```
cluster1::>snapmirror release -relationship-info-only true  
-destination-path vs1_dr:vol1
```

- c. デスティネーション クラスタから、SnapMirror同期関係を作成します。

```
snapmirror create -source-path src_SVM:src_volume -destination-path  
<destination_SVM>:<destination_volume> -policy sync-mirror
```

```
cluster2::>snapmirror create -source-path vs1:vol1 -destination-path  
vs1_dr:vol1 -policy sync
```

- d. SnapMirror同期関係を再同期します。

```
snapmirror resync -destination-path <destination_SVM:destination_volume>
```

```
cluster2::>snapmirror resync -destination-path vs1_dr:vol1
```

• **SnapMirror同期関係をSnapMirror非同期関係に変換する**

- a. デスティネーション クラスタから、既存のSnapMirror同期関係を休止します。

```
snapmirror quiesce -destination-path <destination_SVM>:<destination_volume>
```

```
cluster2::> snapmirror quiesce -destination-path vs1_dr:vol1
```

- b. デスティネーション クラスタから、SnapMirror非同期関係を削除します。

```
snapmirror delete -destination-path <SVM:volume>
```

```
cluster2::>snapmirror delete -destination-path vs1_dr:vol1
```

- c. ソース クラスターから、共通スナップショットを削除せずにSnapMirror関係を解除します：

```
snapmirror release -relationship-info-only true -destination-path  
<destination_SVM:destination_volume>
```

```
cluster1::>snapmirror release -relationship-info-only true  
-destination-path vs1_dr:vol1
```

- d. デスティネーション クラスタから、SnapMirror非同期関係を作成します。


```
snapmirror create -source-path src_SVM:src_volume -destination-path  
<destination_SVM:destination_volume> -policy MirrorAllSnapshots
```

```
cluster2::>snapmirror create -source-path vs1:vol1 -destination-path  
vs1_dr:vol1 -policy sync
```

e. SnapMirror同期関係を再同期します。

```
snapmirror resync -destination-path <destination_SVM:destination_volume>
```

```
cluster2::>snapmirror resync -destination-path vs1_dr:vol1
```

関連情報

- ["snapmirror create"](#)
- ["snapmirror delete"](#)
- ["snapmirror quiesce"](#)
- ["snapmirror release"](#)
- ["snapmirror resync"](#)

ONTAP SnapMirror同期関係のモードを変換する

ONTAP 9.5以降では、SnapMirror同期関係がサポートされます。SnapMirror同期関係のモードはStrictSyncとSyncの間で相互に変換できます。

タスク概要

SnapMirror同期関係のポリシーを変更してモードを変換することはできません。

手順

1. デスティネーション クラスタから、既存のSnapMirror同期関係を休止します。

```
snapmirror quiesce -destination-path <destination_SVM>:<destination_volume>
```

```
cluster2::> snapmirror quiesce -destination-path vs1_dr:vol1
```

2. デスティネーション クラスタから、既存のSnapMirror同期関係を削除します。

```
snapmirror delete -destination-path <destination_SVM>:<destination_volume>
```

```
cluster2::> snapmirror delete -destination-path vs1_dr:vol1
```

3. ソース クラスタから、共通スナップショットを削除せずにSnapMirror関係を解除します：

```
snapmirror release -relationship-info-only true -destination-path  
<destination_SVM>:<destination_volume>
```

```
cluster1::> snapmirror release -relationship-info-only true -destination  
-path vs1_dr:vol1
```

4. デスティネーション クラスタから、変換後のモードを指定してSnapMirror同期関係を作成します。

```
snapmirror create -source-path vs1:vol1 -destination-path  
<destination_SVM>:<destination_volume> -policy Sync|StrictSync
```

```
cluster2::> snapmirror create -source-path vs1:vol1 -destination-path  
vs1_dr:vol1 -policy Sync
```

5. デスティネーション クラスタから、SnapMirror関係を再同期します。

```
snapmirror resync -destination-path <destination_SVM>:<destination_volume>
```

```
cluster2::> snapmirror resync -destination-path vs1_dr:vol1
```

関連情報

- ["snapmirror create"](#)
- ["snapmirror delete"](#)
- ["snapmirror quiesce"](#)
- ["snapmirror release"](#)
- ["snapmirror resync"](#)

ONTAP SnapMirrorフェイルオーバーテストボリュームの作成と削除

ONTAP 9.14.1以降では、System Managerを使用してボリューム クローンを作成することで、アクティブなSnapMirror関係を維持したまま、SnapMirrorのフェイルオーバーとディザスタ リカバリをテストできます。テストが完了したら、関連するデータをクリーンアップしてテスト ボリュームを削除できます。

SnapMirrorフェイルオーバー テスト ボリュームの作成

タスク概要

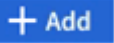
- 同期関係とSnapMirror非同期関係に対してフェイルオーバー テストを実行できます。
- ディザスタ リカバリ テストを実行するためにボリューム クローンが作成されます。
- クローン ボリュームは、SnapMirrorデスティネーションと同じStorage VMに作成されます。
- FlexVolとFlexGroupのSnapMirror関係を使用できます。

- 選択した関係のテスト クローンがすでにある場合、その関係用に別のクローンを作成することはできません。
- SnapLockバックアップ関係はサポートされません。

開始する前に

- クラスタ管理者である必要があります。
- ソース クラスタとデスティネーション クラスタにSnapMirrorライセンスがインストールされている必要があります。

手順

1. デスティネーション クラスタで、***Protection > Relationships***を選択します。
2. リレーションシップ ソースの横にある  を選択し、**テスト フェールオーバー** を選択します。
3. **Test Failover** ウィンドウで、**Test Failover** を選択します。
4. **Storage > Volumes** を選択し、テスト フェールオーバー ボリュームがリストされていることを確認します。
5. ***Storage > Shares***を選択します。
6.  **+ Add** を選択し、***共有***を選択します。
7. **Add share** ウィンドウで、**Share Name** フィールドに共有の名前を入力します。
8. フォルダー フィールドで、**参照** を選択し、テスト クローン ボリュームを選択して、**保存** します。
9. ***共有を追加***ウィンドウの下部で、***保存***を選択します。
10. ***ストレージ > 共有***ペインで、作成した共有を見つけて  を選択し、共有情報を表示します。
11. **SMB/CIFS** アクセス の下で、共有のアクセス パスをコピーまたはメモします（例：
\\123.456.7.890\failover_test）。
12. SMB アクセス パスを使用してクライアント上の共有を開き、テスト ボリュームに読み取りおよび書き込み機能があることを確認します。

フェイルオーバー データのクリーンアップとテスト ボリュームの削除

フェイルオーバー テストが完了したら、テスト ボリュームに関連付けられているすべてのデータをクリーンアップして、テスト ボリュームを削除できます。

手順

1. デスティネーション クラスタで、***Protection > Relationships***を選択します。
2. リレーションシップ ソースの横にある  を選択し、***テスト フェールオーバーのクリーンアップ***を選択します。
3. ***Clean Up Test Failover***ウィンドウで、***Clean Up***を選択します。
4. **Storage > Volumes** を選択し、テスト ボリュームが削除されたことを確認します。

SnapMirror DRデスティネーション ボリュームからのデータの提供

ONTAP SnapMirror デスティネーション ボリュームを書き込み可能にする

デスティネーション ボリュームからクライアントにデータを提供する前に、そのボリュームを書き込み可能にする必要があります。ソースが使用できなくなったときにミラー デスティネーションからデータを提供するには、デスティネーションへのスケジュールされた転送を停止し、SnapMirror関係を解除してデスティネーションを書き込み可能にします。

タスク概要

この手順はデスティネーションSVMまたはデスティネーション クラスタから実行する必要があります。

手順

System ManagerまたはONTAP CLIを使用して、デスティネーション ボリュームを書き込み可能にできます。

System Manager

1. 保護関係を選択します：[保護] > [関係] をクリックし、目的のボリューム名をクリックします。
2.  をクリックします。
3. スケジュールされた転送を停止します。*[一時停止]*をクリックします。
4. デスティネーションを書き込み可能にします。*[解除]*をクリックします。
5. メインの*[関係]*ページに移動し、関係の状態が「切断」と表示されることを確認します。

次の手順

デスティネーション ボリュームを書き込み可能にした後に"[レプリケーション関係を逆再同期する](#)"を実行する必要があります。

無効にしたソース ボリュームが使用可能な状態に戻ったら、関係を逆再同期して現在のデータを元のソース ボリュームにコピーする必要があります。

CLI

1. デスティネーションに対するスケジュールされた転送を停止します。

```
snapmirror quiesce -source-path <SVM:volume|cluster://SVM/volume>  
-destination-path <SVM:volume|cluster://SVM/volume>
```

次の例では、`svm1`のソース ボリューム `volA`と `svm\_backup`のデスティネーション ボリューム `volA\_dst`間のスケジュールされた転送を停止します：

```
cluster_dst:> snapmirror quiesce -source-path svm1:volA  
-destination-path svm_backup:volA_dst
```

`snapmirror quiesce`の詳細については、[link:https://docs.netapp.com/us-en/ontap-cli/snapmirror-quiesce.html](https://docs.netapp.com/us-en/ontap-cli/snapmirror-quiesce.html)["ONTAPコマンド リファレンス"]を参照してください。

2. デスティネーションに対する実行中の転送を停止します。

```
snapmirror abort -source-path <SVM:volume|cluster://SVM/volume>  
-destination-path <SVM:volume|cluster://SVM/volume>
```



SnapMirror同期関係（ONTAP 9.5以降でサポート）ではこの手順は必要ありません。

次の例では、`svm1`のソース ボリューム `volA`と `svm\_backup`のデスティネーション ボリューム `volA\_dst`間の進行中の転送を停止します：

```
cluster_dst::> snapmirror abort -source-path svm1:volA -destination  
-path svm_backup:volA_dst
```

`snapmirror abort`の詳細については、[link:https://docs.netapp.com/us-en/ontap-cli/snapmirror-abort.html](https://docs.netapp.com/us-en/ontap-cli/snapmirror-abort.html)["ONTAPコマンド リファレンス"]をご覧ください。

3. SnapMirror DR関係を解除します。

```
snapmirror break -source-path <SVM:volume|cluster://SVM/volume>  
-destination-path <SVM:volume|cluster://SVM/volume>
```

次の例では、`svm1`のソース ボリューム `volA`と `svm\_backup`のデスティネーション ボリューム `volA\_dst`の関係を解除します：

```
cluster_dst::> snapmirror break -source-path svm1:volA -destination  
-path svm_backup:volA_dst
```

`snapmirror break`の詳細については、[link:https://docs.netapp.com/us-en/ontap-cli/snapmirror-break.html](https://docs.netapp.com/us-en/ontap-cli/snapmirror-break.html)["ONTAPコマンド リファレンス"]を参照してください。

次の手順

デスティネーション ボリュームを書き込み可能にした後に["レプリケーション関係を再同期する"](#)を実行する必要があります。

ONTAPでこの処理を行うその他の方法

タスクを実行するツール	参照するコンテンツ
System Manager Classic（ONTAP 9.7以前で使用可能）	"ボリューム災害復旧の概要"

データアクセス用に**ONTAP SnapMirror**デスティネーションボリュームを設定する

デスティネーションボリュームを書き込み可能にしたあとは、データアクセス用にボリュームを設定する必要があります。ソースボリュームが再アクティブ化されるまで、NASクライアント、NVMeサブシステム、およびSANホストはデスティネーションボリュームからデータにアクセスできます。

NAS環境：

1. ソース ボリュームがソースSVMでマウントされていたのと同じジャンクション パスを使用して、NASボリュームをネームスペースにマウントします。
2. デスティネーション ボリュームのSMB共有に適切なACLを適用します。
3. デスティネーション ボリュームにNFSエクスポート ポリシーを割り当てます。
4. デスティネーション ボリュームにクォータ ルールを適用します。
5. デスティネーション ボリュームにクライアントをリダイレクトします。
6. NFSおよびSMB共有をクライアントに再マウントします。

SAN 環境：

1. ボリューム内のLUNを適切なイニシエータ グループにマッピングします。
2. iSCSIの場合、SANホスト イニシエータからSAN LIFへのiSCSIセッションを作成します。
3. SANクライアントで、ストレージの再スキャンを実行して接続されたLUNを検出します。

NVMe 環境の詳細については、"[SAN管理](#)"を参照してください。

元のONTAP SnapMirrorソースボリュームを再アクティブ化する

デスティネーションからデータを提供する必要がなくなった場合は、ソース ボリュームとデスティネーション ボリュームの間で元のデータ保護関係を再確立できます。

タスク概要

- 次の手順は、元のソース ボリュームにあるベースラインが損なわれていないことを前提としています。ベースラインが損なわれている場合は、この手順を実行する前に、データの提供元のボリュームと元のソース ボリュームの間の関係を作成して初期化する必要があります。
- XDP SnapMirror関係のバックグラウンドでの準備とデータの保存処理に時間がかかります。長時間にわたってSnapMirror関係のステータスが「preparing」と表示されることも珍しくありません。

手順

1. 元のデータ保護関係を反転します。

```
snapmirror resync -source-path SVM:volume -destination-path SVM:volume
```

`snapmirror resync`の詳細については、[link:https://docs.netapp.com/us-en/ontap-cli/snapmirror-resync.html](https://docs.netapp.com/us-en/ontap-cli/snapmirror-resync.html)["ONTAPコマンド リファレンス"]を参照してください。



このコマンドは、元のソースSVMまたは元のソースクラスタから実行する必要があります。再同期にはベースライン転送は必要ありませんが、時間がかかる場合があります。再同期はオフピーク時に実行することをお勧めします。ソースとデスティネーションに共通のSnapshotが存在しない場合、コマンドは失敗します。`snapmirror initialize`を使用して関係を再初期化します。`snapmirror initialize`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。

次の例では、`svm1`上の元のソース ボリューム `volA`と、`svm\_backup`上のデータ提供元ボリューム

`volA\_dst`の関係を反転します：

```
cluster_src::> snapmirror resync -source-path svm_backup:volA_dst  
-destination-path svm1:volA
```

2. 元のソースへのデータ アクセスを再確立する準備ができたなら、元のデスティネーション ボリュームへのアクセスを停止します。その方法の1つが、元のデスティネーションSVMを停止することです。

```
vserver stop -vserver SVM
```



このコマンドは元のデスティネーションSVMまたは元のデスティネーション クラスタから実行する必要があります。このコマンドは、元のデスティネーションSVM全体へのユーザアクセスを停止します。他の方法を使用して元のデスティネーション ボリュームへのアクセスを停止することもできます。

次の例は、元のデスティネーションSVMを停止します。

```
cluster_dst::> vserver stop svm_backup
```

`vserver stop`の詳細については、[link:https://docs.netapp.com/us-en/ontap-cli/vserver-stop.html](https://docs.netapp.com/us-en/ontap-cli/vserver-stop.html)["ONTAPコマンド リファレンス"]を参照してください。

3. 反転した関係を更新します。

```
snapmirror update -source-path SVM:volume -destination-path SVM:volume
```



このコマンドは元のソースSVMまたは元のソース クラスタから実行する必要があります。

次の例では、`svm\_backup`上のデータの提供元ボリューム`volA\_dst`と、`svm1`上の元のソース ボリューム`volA`との関係を更新します：

```
cluster_src::> snapmirror update -source-path svm_backup:volA_dst  
-destination-path svm1:volA
```

`snapmirror update`の詳細については、[link:https://docs.netapp.com/us-en/ontap-cli/snapmirror-update.html](https://docs.netapp.com/us-en/ontap-cli/snapmirror-update.html)["ONTAPコマンド リファレンス"]をご覧ください。

4. 元のソースSVMまたは元のソース クラスタから、反転した関係のスケジュールされた転送を停止します。

```
snapmirror quiesce -source-path SVM:volume -destination-path SVM:volume
```




このコマンドは元のソースSVMまたは元のソース クラスタから実行する必要があります。

次の例では、`svm\_backup`上の元のデスティネーション ボリューム `volA\_dst`と `svm1`上の元のソース ボリューム `volA`間のスケジュールされた転送を停止します：

```
cluster_src::> snapmirror quiesce -source-path svm_backup:volA_dst  
-destination-path svm1:volA
```

`snapmirror quiesce`の詳細については、link:<https://docs.netapp.com/us-en/ontap-cli/snapmirror-quiesce.html>["ONTAPコマンド リファレンス"]を参照してください。

5. 最終更新が完了し、関係のステータスが「Quiesced」と表示されたら、元のソース SVM または元のソース クラスタから次のコマンドを実行して、反転された関係を解除します：

```
snapmirror break -source-path SVM:volume -destination-path SVM:volume
```



このコマンドは元のソースSVMまたはソース クラスタから実行する必要があります。

次の例では、`svm\_backup`上の元のデスティネーション ボリューム `volA\_dst`と、`svm1`上の元のソース ボリューム `volA`の関係を解除します：

```
cluster_scr::> snapmirror break -source-path svm_backup:volA_dst  
-destination-path svm1:volA
```

`snapmirror break`の詳細については、link:<https://docs.netapp.com/us-en/ontap-cli/snapmirror-break.html>["ONTAPコマンド リファレンス"]を参照してください。

6. 元のソースSVMまたは元のソース クラスタから、反転したデータ保護関係を削除します。

```
snapmirror delete -source-path SVM:volume -destination-path SVM:volume
```



このコマンドは元のソースSVMまたは元のソース クラスタから実行する必要があります。

次の例では、`svm1`上の元のソース ボリューム `volA`と、`svm\_backup`上のデータ提供元ボリューム `volA\_dst`との間の逆の関係を削除します：

```
cluster_src::> snapmirror delete -source-path svm_backup:volA_dst  
-destination-path svm1:volA
```

`snapmirror delete`の詳細については、link:<https://docs.netapp.com/us-en/ontap-cli/snapmirror-delete.html>["ONTAPコマンド リファレンス"]をご覧ください。

7. 元のデスティネーションSVMまたは元のデスティネーション クラスタから反転した関係をリリースします。

```
snapmirror release -source-path SVM:volume -destination-path SVM:volume
```



このコマンドは元のデスティネーションSVMまたは元のデスティネーション クラスタから実行する必要があります。

次の例では、`svm\_backup`上の元のデスティネーション ボリューム `volA\_dst`と、`svm1`上の元のソース ボリューム `volA`間の逆の関係を解除します：

```
cluster_dst::> snapmirror release -source-path svm_backup:volA_dst  
-destination-path svm1:volA
```

`snapmirror release`の詳細については、link:<https://docs.netapp.com/us-en/ontap-cli/snapmirror-release.html>["ONTAPコマンド リファレンス"]を参照してください。

8. 元のデスティネーションから元のデータ保護関係を再確立します。

```
snapmirror resync -source-path SVM:volume -destination-path SVM:volume
```

次の例では、`svm1`上の元のソース ボリューム `volA`と、`svm\_backup`上の元のデスティネーション ボリューム `volA\_dst`との関係を再確立します：

```
cluster_dst::> snapmirror resync -source-path svm1:volA -destination  
-path svm_backup:volA_dst
```

`snapmirror resync`の詳細については、link:<https://docs.netapp.com/us-en/ontap-cli/snapmirror-resync.html>["ONTAPコマンド リファレンス"]を参照してください。

9. 必要に応じて、元のデスティネーションSVMを起動します。

```
vserver start -vserver SVM
```

次の例は、元のデスティネーションSVMを起動します。

```
cluster_dst::> vserver start svm_backup
```

`vserver start`の詳細については、link:<https://docs.netapp.com/us-en/ontap-cli/vserver-start.html>["ONTAPコマンド リファレンス"]を参照してください。

終了後の操作

`snapmirror show`コマンドを使用して、SnapMirror関係が作成されたことを確認します。

`snapmirror show`の詳細については、link:<https://docs.netapp.com/us-en/ontap-cli/snapmirror-show.html>["ONTAPコマンド リファレンス"]を参照してください。

SnapMirrorデスティネーション ボリュームからのファイルのリストア

ONTAP SnapMirrorデスティネーションからファイル、LUN、またはNVMeネームスペースをリストアする

単一のファイル、LUN、スナップショットからのファイルまたはLUNのセット、あるいはSnapMirrorデスティネーション ボリュームからのNVMeネームスペースをリストアできます。ONTAP 9.7以降では、SnapMirror同期デスティネーションからのNVMeネームスペースもリストアできます。ファイルは元のソース ボリュームまたは別のボリュームにリストアできます。

開始する前に

SnapMirror同期デスティネーション（ONTAP 9.5以降でサポート）からファイルまたはLUNを復元するには、まず関係を削除して解放する必要があります。

タスク概要

ファイルまたはLUNのリストア先のボリューム（デスティネーション ボリューム）は読み書き可能なボリュームにする必要があります。

- SnapMirrorは、ソース ボリュームとデスティネーション ボリュームに共通のSnapshotがある場合（元のソース ボリュームにリストアする場合が一般的）、`_増分リストア_`を実行します。
- それ以外の場合は、SnapMirrorが`_ベースライン リストア_`を実行し、指定されたSnapshotとそれが参照するすべてのデータ ブロックがデスティネーション ボリュームに転送されます。

手順

1. デスティネーション ボリューム内のSnapshotを一覧表示します：

```
volume snapshot show -vserver <SVM> -volume volume
```

`volume snapshot show`の詳細については、link:<https://docs.netapp.com/us-en/ontap-cli/volume-snapshot-show.html>["ONTAPコマンド リファレンス"]を参照してください。

次の例は、`vserverB:secondary1`デスティネーションのSnapshotを示しています：

```
cluster_dst:> volume snapshot show -vserver vsverB -volume secondary1
```

Vserver Used%	Volume	Snapshot	State	Size	Total%
-----	-----	-----	-----	-----	-----

vserverB	secondary1	hourly.2013-01-25_0005	valid	224KB	0%
0%		daily.2013-01-25_0010	valid	92KB	0%
0%		hourly.2013-01-25_0105	valid	228KB	0%
0%		hourly.2013-01-25_0205	valid	236KB	0%
0%		hourly.2013-01-25_0305	valid	244KB	0%
0%		hourly.2013-01-25_0405	valid	244KB	0%
0%		hourly.2013-01-25_0505	valid	244KB	0%
0%					

7 entries were displayed.

2. SnapMirrorデスティネーション ボリュームのSnapshotから単一のファイルまたはLUN、あるいはファイルまたはLUNのセットをリストアします：

```
snapmirror restore -source-path <SVM:volume>|<cluster://SVM/volume>, ...  
-destination-path <SVM:volume>|<cluster://SVM/volume>, ... -source-snapshot  
snapshot -file-list <source_file_path,@destination_file_path>
```



このコマンドはデスティネーションSVMまたはデスティネーション クラスタから実行する必要があります。

次のコマンドは、元のデスティネーション ボリューム `secondary1` のスナップショット `daily.2013-01-25\_0010` から、ファイル `file1` と `file2` を、元のソース ボリューム `primary1` のアクティブ ファイル システム内の同じ場所に復元します：

```
cluster_dst:> snapmirror restore -source-path vserverB:secondary1
-destination-path vserverA:primary1 -source-snapshot daily.2013-01-
25_0010 -file-list /dir1/file1,/dir2/file2
```

```
[Job 3479] Job is queued: snapmirror restore for the relationship with
destination vserverA:primary1
```

次のコマンドは、元のデスティネーション ボリューム `secondary1` のスナップショット `daily.2013-01-25\_0010` から、ファイル `file1` と `file2` を、元のソース ボリューム `primary1` のアクティブ ファイル システム内の別の場所に復元します。

デスティネーション ファイル パスは@記号で始まり、その後に元のソース ボリュームのルートからのファイル パスが続きます。この例では、`file1` が `/dir1/file1.new` に復元され、`file2` が `/dir2.new/file2` に復元されます (`primary1`) :

```
cluster_dst:> snapmirror restore -source-path vserverB:secondary1
-destination-path vserverA:primary1 -source-snapshot daily.2013-01-
25_0010 -file-list
/dir/file1,@/dir1/file1.new,/dir2/file2,@/dir2.new/file2
```

```
[Job 3479] Job is queued: snapmirror restore for the relationship with
destination vserverA:primary1
```

次のコマンドは、元のデスティネーション ボリューム `secondary1` のスナップショット `daily.2013-01-25\_0010` からファイル `file1` と `file3` を元のソース ボリューム `primary1` のアクティブ ファイル システム内の別の場所に復元し、`file2` を `snap1` から `primary1` のアクティブ ファイル システム内の同じ場所に復元します。

この例では、ファイル `file1` は `/dir1/file1.new` に復元され、`file3` は `/dir3.new/file3` に復元されます :

```
cluster_dst:> snapmirror restore -source-path vserverB:secondary1
-destination-path vserverA:primary1 -source-snapshot daily.2013-01-
25_0010 -file-list
/dir/file1,@/dir1/file1.new,/dir2/file2,/dir3/file3,@/dir3.new/file3
```

```
[Job 3479] Job is queued: snapmirror restore for the relationship with
destination vserverA:primary1
```

関連情報

- ["snapmirror restore"](#)

ONTAP SnapMirror デスティネーション から ボリューム の内容を復元する

SnapMirror デスティネーション ボリューム の Snapshot から ボリューム 全体の内容をリス

ストアできます。ボリュームの内容を元のソース ボリュームまたは別のボリュームにリストアできます。

タスク概要

この手順は、FAS、AFF、およびASAシステムに適用されます。ASA r2システム（ASAA1K、ASAA90、ASAA70、ASAA50、ASAA30、ASAA20、またはASA C30）をご利用の場合は、["これらの手順"](#)に従ってデータを復元してください。ASA r2システムは、SANのみをご利用のお客様向けに、簡素化されたONTAPエクスペリエンスを提供します。

リストア処理のデスティネーション ボリュームは次のいずれかにする必要があります。

- 読み取り / 書き込みボリュームの場合、SnapMirrorはソース ボリュームとデスティネーション ボリュームに共通のSnapshotがあれば（元のソース ボリュームにリストアする場合が一般的）、`_増分リストア_`を実行します。



共通Snapshotがない場合、コマンドは失敗します。ボリュームの内容を空の読み取り / 書き込みボリュームにリストアすることはできません。

- 空のデータ保護ボリューム。この場合、SnapMirrorは`_ベースライン復元_`を実行し、指定されたスナップショットとそれが参照するすべてのデータ ブロックがソース ボリュームに転送されます。

ボリュームの内容のリストアはシステム停止を伴う処理です。リストア処理を実行しているときに、SnapVaultプライマリ ボリューム上でSMBトラフィックを実行してはなりません。

リストア処理のデスティネーション ボリュームで圧縮が有効になっていて、ソース ボリュームで圧縮が有効になっていない場合は、デスティネーション ボリュームで圧縮を無効にします。リストア処理が完了したら、圧縮を再度有効にする必要があります。

復元を実行する前に、デスティネーション ボリュームに定義されているクォータ ルールはすべて無効になります。`volume quota modify`コマンドを使用して、復元処理の完了後にクォータ ルールを再度有効にすることができます。

ボリューム内のデータが失われたり破損したりした場合は、以前のSnapshotから復元することでデータをロールバックできます。

この手順では、ソースボリューム上の現在のデータを以前のスナップショットバージョンのデータに置き換えます。このタスクはデスティネーション クラスターで実行する必要があります。

手順

ボリュームの内容は、System ManagerまたはONTAP CLIを使用してリストアできます。

System Manager

1. *[保護] > [関係]*をクリックし、ソース ボリュームの名前をクリックします。
2.  をクリックし、*復元*を選択します。
3. *Source*では、デフォルトでソース ボリュームが選択されています。ソース以外のボリュームを選択する場合は、*Other Volume*をクリックしてください。
4. *Destination*で、復元するスナップショットを選択します。
5. ソースとデスティネーションのクラスタが異なる場合は、リモート クラスタで*[保護] > [関係]*をクリックしてリストアの進捗を監視します。

CLI

1. デスティネーション ボリューム内のSnapshotを一覧表示します：

```
volume snapshot show -vserver <SVM> -volume <volume>
```

次の例は、`vserverB:secondary1`デスティネーションのSnapshotを示しています：

```
cluster_dst::> volume snapshot show -vserver vserversB -volume
secondary1
```

Vserver	Volume	Snapshot	State	Size	
Total%	Used%				
-----	-----	-----	-----	-----	-----
vserverB	secondary1	hourly.2013-01-25_0005	valid	224KB	0%
0%		daily.2013-01-25_0010	valid	92KB	0%
0%		hourly.2013-01-25_0105	valid	228KB	0%
0%		hourly.2013-01-25_0205	valid	236KB	0%
0%		hourly.2013-01-25_0305	valid	244KB	0%
0%		hourly.2013-01-25_0405	valid	244KB	0%
0%		hourly.2013-01-25_0505	valid	244KB	0%

7 entries were displayed.

2. SnapMirrorデスティネーション ボリュームのSnapshotからボリュームの内容をリストアします：

```
snapmirror restore -source-path <SVM:volume>|<cluster://SVM/volume>
```

```
-destination-path <SVM:volume>|<cluster://SVM/volume> -source-snapshot  
<snapshot>
```



このコマンドは元のソースSVMまたは元のソース クラスタから実行する必要があります。

次のコマンドは、元のデスティネーション ボリューム `secondary1` のSnapshot `daily.2013-01-25\_0010` から元のソース ボリューム `primary1` の内容を復元します：

```
cluster_src:> snapmirror restore -source-path vserverB:secondary1  
-destination-path vserverA:primary1 -source-snapshot daily.2013-01-  
25_0010
```

```
Warning: All data newer than snapshot daily.2013-01-25_0010 on  
volume vserverA:primary1 will be deleted.
```

```
Do you want to continue? {y|n}: y
```

```
[Job 34] Job is queued: snapmirror restore from source  
vserverB:secondary1 for the snapshot daily.2013-01-25_0010.
```

3. リストアしたボリュームを再マウントし、ボリュームを使用するすべてのアプリケーションを再起動します。

ONTAPでこの処理を行うその他の方法

タスクを実行するツール	参照するコンテンツ
System Manager Classic（ONTAP 9.7以前で使用可能）	"SnapVaultを使用したボリューム復元の概要"

関連情報

- ["snapmirror restore"](#)
- ["volume snapshot show"](#)

ONTAP SnapMirrorレプリケーション関係を手動で更新する

ソース ボリュームの移動が原因で更新に失敗した場合、レプリケーション関係を手動で更新する必要があります。

タスク概要

レプリケーション関係を手動で更新するまで、SnapMirrorは移動されたソース ボリュームからの転送をすべて中止します。

ONTAP 9.5以降では、SnapMirror同期関係がサポートされています。これらの関係では、ソース ボリュームとデスティネーション ボリュームは常に同期されていますが、セカンダリ クラスタからのビューはプライマリと1時間ごとに同期されます。デスティネーションのポイントインタイム データを表示するには、

`snapmirror update` コマンドを実行して手動で更新する必要があります。

手順

1. レプリケーション関係を手動で更新します。

```
snapmirror update -source-path <SVM:volume>|<cluster://SVM/volume>, ...  
-destination-path <SVM:volume>|<cluster://SVM/volume>, ...
```



このコマンドは、デスティネーションSVMまたはデスティネーション クラスタから実行する必要があります。ソースとデスティネーションに共通のスナップショットが存在しない場合、コマンドは失敗します。`snapmirror initialize`を使用して関係を再初期化してください。"[ONTAPコマンド リファレンス](#)"の`snapmirror initialize`の詳細を確認してください。

次の例では、`svm1`のソース ボリューム `volA`と `svm\_backup`のデスティネーション ボリューム `volA\_dst`間の関係を更新します：

```
cluster_src::> snapmirror update -source-path svm1:volA -destination  
-path svm_backup:volA_dst
```

`snapmirror update`の詳細については、[link:https://docs.netapp.com/us-en/ontap-cli/snapmirror-update.html](https://docs.netapp.com/us-en/ontap-cli/snapmirror-update.html)["ONTAPコマンド リファレンス"]をご覧ください。

ONTAP SnapMirrorレプリケーション関係を再同期する

デスティネーション ボリュームを書き込み可能にした後、ソース ボリュームとデスティネーション ボリュームに共通のSnapshotコピーが存在しないために更新が失敗した後、または関係のレプリケーション ポリシーを変更する場合は、レプリケーション関係を再同期する必要があります。

ONTAP 9.8以降では、System Managerを使用して逆再同期処理を実行し、既存の保護関係を削除し、ソース ボリュームとデスティネーション ボリュームの機能を切り替えることができます。ソースを修理または交換する間デスティネーション ボリュームでデータを提供し、その後ソースを更新し、システムの元の構成を再確立できます。



System Managerでは、クラスタ内関係の逆再同期はサポートされません。クラスタ内関係の逆再同期処理は、ONTAP CLIを使用して実行できます。

タスク概要

- 再同期の際にベースライン転送は不要ですが、再同期には時間がかかる場合があります。再同期はオフピークの時間帯に実行することを推奨します。
- ファンアウト構成またはカスケード構成の一部であるボリュームの再同期には時間がかかります。長時間にわたってSnapMirror関係のステータスが「preparing」と表示されることも珍しくありません。
- ONTAP 9.13.1以降、ONTAPは再同期時間を短縮するために、デフォルトでクイック再同期を使用するようになりました。クイック再同期をデフォルトで使用するには、以下の条件を満たす必要があります：

- FlexVolボリュームにボリューム上のクローンがありません
- MirrorAllSnapshotsポリシーを使用する場合



`-quick-resync`を使用すると、転送されたデータブロックのストレージ効率が削除されるため、再同期デスティネーション ボリュームで追加のスペースが消費される可能性があります。この追加のスペース消費は、再同期デスティネーションでのインラインまたはレプリケーション後のストレージ効率適用の一部として回復されます。

`-quick-resync`パラメータはオプションです。`snapmirror resync`コマンドで
`-quick-resync
true|false`パラメータを使用して、クイック再同期を有効または無効にすることができます。

`-quick-resync`の詳細については、link:<https://docs.netapp.com/us-en/ontap-cli/snapmirror-resync.html>["ONTAPコマンド リファレンス
"^]を参照してください。

手順

System ManagerまたはONTAP CLIを使用して、このタスクを実行できます。ONTAP CLIを使用する場合は、デスティネーション ボリュームを書き込み可能にするか、レプリケーション関係を更新するかに関係なく同じ手順です。

System Managerの逆再同期

"関係を解除する"してデスティネーションを書き込み可能にした後、関係を逆方向に再同期します：

1. デスティネーション クラスターで、*保護 > 関係*をクリックします。
2. 元に戻したい切断された関係の上にマウスを移動し、をクリックして、*逆再同期*を選択します。
3. *逆再同期関係*ウィンドウで、*逆再同期*をクリックします。
4. *関係*の下で、関係の*転送ステータス*を表示して逆再同期の進行状況を監視します。

次の手順

元のソースが再び使用可能になったら、反転した関係を解除してもう一度逆再同期処理を実行することで、元の関係を再確立できます。逆再同期プロセスにより、データを提供しているサイトから元のソースに変更がすべてコピーされ、元のソースが再び読み取り / 書き込み可能になります。

System Managerの再同期

1. *保護 > 関係*をクリックします。
2. 再同期する関係にマウスを移動し、をクリックして、*解除*を選択します。
3. 関係の状態が「切断」と表示されたら、をクリックして*再同期*を選択します。
4. *[関係]*で、関係の状態をチェックして再同期の進捗を監視します。再同期が完了すると、状態が「ミラーリング」に変わります。

CLI

1. ソース ボリュームとデスティネーション ボリュームを再同期します。

```
snapmirror resync -source-path <SVM:volume|cluster://SVM/volume>  
-destination-path <SVM:volume|cluster://SVM/volume> -type DP|XDP  
-policy <policy>
```



このコマンドはデスティネーションSVMまたはデスティネーション クラスターから実行する必要があります。

次の例では、`svm1`のソース ボリューム `volA`と `svm\_backup`のデスティネーション ボリューム `volA\_dst`間の関係を再同期します：

```
cluster_dst::> snapmirror resync -source-path svm1:volA -destination  
-path svm_backup:volA_dst
```

`snapmirror resync`の詳細については、[link:https://docs.netapp.com/us-en/ontap-cli/snapmirror-resync.html](https://docs.netapp.com/us-en/ontap-cli/snapmirror-resync.html)["ONTAPコマンド リファレンス"]を参照してください。

関連情報

- "ONTAP SnapMirrorデスティネーションSVM上のデータを再同期する"

ONTAP SnapMirrorボリュームのレプリケーション関係を削除する

``snapmirror delete`` コマンドと ``snapmirror release`` コマンドを使用して、ボリュームのレプリケーション関係を削除できます。その後、不要なデスティネーション ボリュームを手動で削除できます。

タスク概要

``snapmirror release`` コマンドは、ソースから SnapMirror で作成されたスナップショットをすべて削除します。 ``-relationship-info-only`` オプションを使用して、スナップショットを保持できます。

手順

1. レプリケーション関係を休止します。

```
snapmirror quiesce -destination-path <SVM:volume>|<cluster://SVM/volume>
```

```
cluster_dst::> snapmirror quiesce -destination-path svm_backup:volA_dst
```

``snapmirror quiesce`` の詳細については、link:<https://docs.netapp.com/us-en/ontap-cli/snapmirror-quiesce.html> ["ONTAP コマンド リファレンス"] を参照してください。

2. (オプション) デスティネーション ボリュームを読み取り / 書き込みボリュームにする必要がある場合は、レプリケーション関係を解除します。デスティネーション ボリュームを削除する場合や、ボリュームを読み取り / 書き込みにする必要がない場合は、この手順を省略できます。

```
snapmirror break -source-path <SVM:volume>|<cluster://SVM/volume>, ...  
-destination-path <SVM:volume>|<cluster://SVM/volume>, ...
```

```
cluster_dst::> snapmirror break -source-path svm1:volA -destination-path  
svm_backup:volA_dst
```

``snapmirror break`` の詳細については、link:<https://docs.netapp.com/us-en/ontap-cli/snapmirror-break.html> ["ONTAP コマンド リファレンス"] を参照してください。

3. レプリケーション関係を削除します。

```
snapmirror delete -source-path <SVM:volume>|<cluster://SVM/volume>, ...  
-destination-path <SVM:volume>|<cluster://SVM/volume>, ...
```



このコマンドはデスティネーション クラスタまたはデスティネーションSVMから実行する必要があります。

次の例では、`svm1`のソース ボリューム `volA`と `svm\_backup`のデスティネーション ボリューム `volA\_dst`間の関係を削除します：

```
cluster_dst::> snapmirror delete -source-path svm1:volA -destination  
-path svm_backup:volA_dst
```

`snapmirror delete`の詳細については、[link:https://docs.netapp.com/us-en/ontap-cli/snapmirror-delete.html](https://docs.netapp.com/us-en/ontap-cli/snapmirror-delete.html)["ONTAPコマンド リファレンス"]をご覧ください。

4. ソースSVMからレプリケーション関係情報をリリースします。

```
snapmirror release -source-path <SVM:volume>|<cluster://SVM/volume>, ...  
-destination-path <SVM:volume>|<cluster://SVM/volume>, ...
```



このコマンドはソース クラスタまたはソースSVMから実行する必要があります。

次の例では、指定されたレプリケーション関係の情報をソース SVM `svm1`から解放します：

```
cluster_src::> snapmirror release -source-path svm1:volA -destination  
-path svm_backup:volA_dst
```

`snapmirror release`の詳細については、[link:https://docs.netapp.com/us-en/ontap-cli/snapmirror-release.html](https://docs.netapp.com/us-en/ontap-cli/snapmirror-release.html)["ONTAPコマンド リファレンス"]を参照してください。

ONTAP SnapMirrorボリュームのストレージ効率を管理する

SnapMirrorは、ソース ボリュームとデスティネーション ボリュームでストレージ効率を維持します。ただし、デスティネーション ボリュームでポストプロセス データ圧縮が有効になっている場合を除きます。その場合、デスティネーション ボリュームではすべてのストレージ効率が失われます。この問題を修正するには、デスティネーション ボリュームでポストプロセス圧縮を無効にして、関係を手動で更新し、Storage Efficiencyを再度有効にする必要があります。

```
`volume efficiency
show` コマンドを使用して、ボリュームで効率化が有効になっているかどうかを確認できます。link:https://docs.netapp.com/us-en/ontap-cli/volume-efficiency-show.html["ONTAPコマンド リファレンス"]の `volume efficiency
show` の詳細をご覧ください。
```

SnapMirror監査ログを表示して転送の説明を確認することで、SnapMirrorがストレージ効率を維持しているかどうかを確認できます。転送の説明に `transfer\_desc=Logical Transfer with Storage Efficiency` と表示されている場合、SnapMirrorはストレージ効率を維持しています。転送の説明に `transfer\_desc=Logical Transfer` と表示されている場合、SnapMirrorはストレージ効率を維持していません。例：

```
Fri May 22 02:13:02 CDT 2020 ScheduledUpdate[May 22 02:12:00]:cc0fbc29-
b665-11e5-a626-00a09860c273 Operation-Uid=39fbcf48-550a-4282-a906-
df35632c73a1 Group=none Operation-Cookie=0 action=End source=<sourcepath>
destination=<destpath> status=Success bytes_transferred=117080571
network_compression_ratio=1.0:1 transfer_desc=Logical Transfer - Optimized
Directory Mode
```

開始する前に

- ソース / デスティネーション クラスタとSVMのピア関係が確立されている必要があります。

"クラスタとSVMのピアリング"

- デスティネーション ボリュームでポストプロセス圧縮を無効にする必要があります。
- ストレージを使用した論理転送：ONTAP 9.3以降では、Storage Efficiencyを再度有効にするために手動で更新する必要がなくなりました。SnapMirrorがポストプロセス圧縮が無効になっていることを検出すると、次のスケジュールされた更新時にStorage Efficiencyが自動的に再度有効になります。ソースとデスティネーションの両方でONTAP 9.3が稼働している必要があります。
- ONTAP 9.3以降では、デスティネーション ボリュームが書き込み可能になったあとで、AFFシステムがStorage Efficiencyの設定をFASシステムとは異なる方法で管理します。
 - `snapmirror break`` コマンドを使用してデスティネーション ボリュームを書き込み可能にすると、ボリューム上のキャッシュ ポリシーは自動的に `auto`（デフォルト）に設定されます。



この動作はFlexVolにのみ該当し、FlexGroupボリュームには該当しません。

```
`snapmirror break`の詳細については、link:https://docs.netapp.com/us-
en/ontap-cli/snapmirror-break.html["ONTAPコマンド リファレンス
"]を参照してください。
```

- 再同期時に、キャッシュポリシーは自動的に `none` に設定され、元の設定に関係なく、重複排除とインライン圧縮は自動的に無効化されます。必要に応じて手動で設定を変更する必要があります。



Storage Efficiencyが有効な状態での手動更新には時間がかかる場合があります。この処理はオフピークの時間帯に実行することを推奨します。

手順

1. レプリケーション関係を更新して、Storage Efficiencyを再度有効にします。

```
snapmirror update -source-path <SVM:volume>|<cluster://SVM/volume>, ...  
-destination-path <SVM:volume>|<cluster://SVM/volume>, ... -enable  
-storage-efficiency true
```



このコマンドは、デスティネーションSVMまたはデスティネーション クラスタから実行する必要があります。ソースとデスティネーションに共通のスナップショットが存在しない場合、コマンドは失敗します。`snapmirror initialize`を使用して関係を再初期化してください。"[ONTAPコマンド リファレンス](#)"の`snapmirror initialize`の詳細を確認してください。

次の例では、`svm1`のソース ボリューム `volA`と `svm\_backup`のデスティネーション ボリューム `volA\_dst`の関係を更新し、ストレージ効率を再度有効にします：

```
cluster_dst::> snapmirror update -source-path svm1:volA -destination  
-path svm_backup:volA_dst -enable-storage-efficiency true
```

`snapmirror update`の詳細については、[link:https://docs.netapp.com/us-en/ontap-cli/snapmirror-update.html](https://docs.netapp.com/us-en/ontap-cli/snapmirror-update.html)["ONTAPコマンド リファレンス"]をご覧ください。

ONTAP SnapMirrorグローバルスロットリングを使用する

ノード単位のSnapMirror転送とSnapVault転送にグローバル ネットワーク スロットルを使用できます。

タスク概要

SnapMirrorグローバル スロットルは、送受信されるSnapMirror転送およびSnapVault転送で使用する帯域幅を制限します。この制限は、クラスタ内のすべてのノードで適用されます。

たとえば、送信スロットルを100MBpsに設定した場合は、クラスタ内の各ノードで送信帯域幅が100MBpsに設定されます。グローバル スロットルを無効にすると、すべてのノードで無効になります。

データ転送速度は多くの場合ビット/秒 (bps) で表されますが、スロットル値はキロバイト/秒 (KBps) で入力する必要があります。



ONTAP 9.9.1以前のリリースでは、スロットルは`volume move`転送や負荷共有ミラー転送には影響しません。ONTAP 9.10.0以降では、ボリューム移動処理のスロットルを設定するオプションを指定できます。詳細については、"[ONTAP 9.10以降でボリューム移動を制限する方法](#)"を参照してください。

グローバルスロットリングはSnapMirrorおよびSnapVault転送におけるリレーションシップごとのスロットリング機能と連携して機能します。リレーションシップごとのスロットリングは、リレーションシップごとの転送の合計帯域幅がグローバルスロットリングの値を超えるまで適用され、超過後はグローバルスロットリングが適用されます。スロットル値`0`は、グローバルスロットリングが無効になっていることを意味します。



SnapMirrorグローバル スロットルは、同期されているSnapMirror同期関係には影響しません。ただし、初期化処理の実行時や非同期イベントのあとなど、SnapMirror同期関係で非同期転送フェーズが実行される場合には影響します。そのため、SnapMirror同期関係でグローバル スロットルを有効にすることは推奨されません。

手順

1. グローバル スロットルを有効にします。

```
options -option-name replication.throttle.enable on|off
```

次の例は、`cluster\_dst`でSnapMirrorグローバル スロットルを有効にする方法を示しています：

```
cluster_dst::> options -option-name replication.throttle.enable on
```

2. デスティネーション クラスタで受信転送に使用される最大総帯域幅を指定します。

```
options -option-name replication.throttle.incoming.max_kbs <KBps>
```

推奨される最小スロットル帯域幅は4キロバイト/秒 (KBps)、最大値は2テラバイト/秒 (TBps) です。このオプションのデフォルト値は`unlimited`で、使用される総帯域幅に制限がないことを意味します。

次の例は、着信転送で使用される最大合計帯域幅を100メガビット/秒 (Mbps) に設定する方法を示しています：

```
cluster_dst::> options -option-name  
replication.throttle.incoming.max_kbs 12500
```



100メガビット/秒 (Mbps) = 12500キロバイト/秒 (KBps)

3. ソース クラスタで送信転送に使用される最大総帯域幅を指定します。

```
options -option-name replication.throttle.outgoing.max_kbs <KBps>
```

推奨される最小スロットル帯域幅は4 KBps、最大値は2 TBpsです。このオプションのデフォルト値は`unlimited`で、使用される総帯域幅に制限がないことを意味します。パラメータ値はキロバイト/秒 (KBps) 単位です。

次の例は、送信転送で使用される最大総帯域幅を100Mbpsに設定します。

```
cluster_src::> options -option-name  
replication.throttle.outgoing.max_kbs 12500
```


SnapMirror SVMレプリケーションの管理

ONTAP SnapMirror SVMレプリケーションについて学ぶ

SnapMirrorを使用すると、SVM間のデータ保護関係を作成できます。このタイプのデータ保護関係では、SVMのすべてまたは一部の設定がNFSエクスポートおよびSMB共有からRBACにレプリケートされます。また、SVMが所有するボリューム内のデータもレプリケートされます。

サポートされている関係タイプ

レプリケート可能なのはデータ提供用SVMのみです。サポートされているデータ保護関係タイプは次のとおりです。

- *SnapMirror DR* では、通常、デスティネーションには現在ソースにあるスナップショットのみが含まれます。

ONTAP 9.9.1以降では、mirror-vaultポリシーを使用している場合、この動作が変更されます。ONTAP 9.9.1以降では、ソースとデスティネーションで異なるSnapshotポリシーを作成でき、デスティネーションのSnapshotがソースのSnapshotによって上書きされることはありません：

- 通常のスケジュールされた操作、更新、再同期中にソースからデスティネーションに上書きされることはありません。
 - ブレーク操作では削除されません。
 - これらは、フリップ再同期操作では削除されません。ONTAP 9.9.1以降でミラー・ヴォールト・ポリシーを使用してSVM災害関係を設定する場合、ポリシーは次のように動作します：
 - ソースのユーザー定義のSnapshotポリシーは、デスティネーションにコピーされません。
 - システム定義のスナップショット ポリシーはデスティネーションにコピーされません。
 - ユーザーおよびシステム定義のスナップショット ポリシーとのボリュームの関連付けは、デスティネーションにコピーされません。+ SVM。
- *SnapMirror* 統合レプリケーション では、デスティネーションは DR と長期保存の両方に対して構成されます。

SnapMirror統合レプリケーションの詳細については、"[SnapMirrorユニファイド レプリケーションの基本](#)"を参照してください。

レプリケーション ポリシーの_ポリシー タイプ_によって、サポートされる関係の種類が決まります。次の表に、使用可能なポリシー タイプを示します。

ポリシー タイプ	関係タイプ
async-mirror	SnapMirror DR
mirror-vault	ユニファイド レプリケーション

ONTAP 9.4におけるSVMレプリケーションのデフォルトの変更（DP→XDP）

ONTAP 9.4以降では、SVMデータ保護関係のデフォルトがXDPモードに変更されました。ONTAP 9.3以前のSVMデータ保護関係のデフォルトは引き続きDPモードです。

既存のリレーションシップはXDPのデフォルト設定の影響を受けません。リレーションシップが既にDPタイプである場合は、引き続きDPタイプのままとなります。次の表に、想定される動作を示します。

指定するモード	タイプ	デフォルト ポリシー（ポリシーを指定しない場合）
DP	XDP	MirrorAllSnapshots（SnapMirror DR）
なし	XDP	MirrorAllSnapshots（SnapMirror DR）
XDP	XDP	MirrorAndVault（ユニファイド レプリケーション）

DP リレーションシップを XDP リレーションシップに変換する方法やその他の詳細については、こちらをご覧ください：["既存のONTAP DPタイプ関係をXDPに変換する"](#)



バージョンに依存しないレプリケーションは、SVMレプリケーションではサポートされません。SVMディザスタ リカバリ構成では、フェイルオーバー処理とフェイルバック処理をサポートするためには、ソースSVMクラスタと同じバージョンのONTAPを実行しているクラスタにデスティネーションSVMを配置する必要があります。

"SnapMirror関係に対応したONTAPバージョン"

SVMの設定のレプリケート方法

SVMレプリケーション関係の内容は、以下に示すフィールドの設定の組み合わせによって決定されます。

- `snapmirror create` コマンドの `-identity-preserve true` オプションは、SVM構成全体を複製します。

`-identity-preserve false` オプションは、SVMのボリュームと認証および承認の設定、および[link:snapmirror-svm-replication-concept.html#configurations-replicated-in-svm-disaster-recovery-relationships](#)["SVMディザスタ リカバリ関係でレプリケートされる設定"]にリストされているプロトコルとネーム サービスの設定のみを複製します。

- `snapmirror policy create` コマンドの `-discard-configs network` オプションは、ソースSVMとデスティネーションSVMが異なるサブネットにある場合に使用するために、LIFと関連するネットワーク設定をSVMレプリケーションから除外します。
- `volume modify` コマンドの `-vserver-dr-protection unprotected` オプションは、指定されたボリュームをSVMレプリケーションから除外します。

上記の点を除き、SVMレプリケーションはボリューム レプリケーションとほぼ同じです。ボリューム レプリケーションに使用するのとほぼ同じワークフローをSVMレプリケーションにも使用できます。

サポートの詳細

次の表は、SnapMirror SVMレプリケーションのサポートの詳細を示しています。

リソースまたは機能	サポートの詳細
構成タイプ	• 1つのソースから1つのデスティネーション • ONTAP 9.4以降はファンアウト（ただしファンアウトのデスティネーションは2つのみ） デフォルトでは、-identity-preserve trueの関係はソースSVMごとに1つだけ許可されます。
関係タイプ	• SnapMirrorディザスタ リカバリ • SnapMirrorユニファイド レプリケーション
レプリケーションの範囲	クラスタ間のみ。同じクラスタ内のSVMをレプリケートすることはできません。
自律型ランサムウェア対策	• ONTAP 9.12.1以降でサポートされます。詳細については、"自律型ランサムウェア対策"を参照してください。
整合性グループの非同期サポート	ONTAP 9.14.1以降では、コンシステンシグループが存在する場合、最大32個のSVMディザスタリカバリ関係がサポートされます。詳細については、" 整合性グループの保護 "および" 整合性グループの制限 "を参照してください。
FabricPool	ONTAP 9.6以降、SnapMirror SVMレプリケーションはFabricPoolでサポートされます。SVM DR関係では、ソースボリュームとデスティネーションボリュームでFabricPoolアグリゲートを使用する必要はありませんが、同じ階層化ポリシーを使用する必要があります。 ONTAP 9.12.1以降、SnapMirror SVMレプリケーションはFabricPoolとFlexGroupボリュームと連携して動作することがサポートされています。9.12.1より前は、これらの機能のうち2つは連携して動作していましたが、3つすべては連携して動作していませんでした。

MetroCluster	ONTAP 9.11.1以降では、MetroCluster構成内のSVMディザスタ リカバリ関係のソースとデスティネーション両方を、追加のSVMディザスタ リカバリ構成のソースにすることができます。 ONTAP 9.5以降のMetroCluster構成では、SnapMirror SVMレプリケーションがサポートされます。 • ONTAP 9.10.Xより前のリリースでは、MetroCluster構成をSVMディザスタ リカバリ関係のデスティネーションにすることはできません。 • ONTAP 9.10.1 以降のリリースでは、MetroCluster構成は移行目的のみで SVM ディザスタ リカバリ関係の宛先になることができ、"TR-4966：SVMをMetroClusterソリューションに移行する"に記載されている必要な要件をすべて満たす必要があります。 • SVMディザスタ リカバリ関係のソースとして使用できるのは、MetroCluster構成のアクティブなSVMだけです。 スイッチオーバー前の同期元のSVMとスイッチオーバー後の同期先のSVMのどちらもソースに使用できます。 • MetroCluster構成が安定した状態のときはMetroClusterの同期先のSVMはオンラインでないため、同期先ボリュームをSVMディザスタ リカバリ関係のソースにすることはできません。 • SVMディザスタ リカバリ関係のソースが同期元のSVMの場合、ソースのSVMディザスタ リカバリ関係情報がMetroClusterパートナーにレプリケートされます。 • スイッチオーバーおよびスイッチバックの実行中に、SVMディザスタ リカバリのデスティネーションへのレプリケーションが失敗することがあります。 ただし、スイッチオーバーまたはスイッチバック処理の完了後、SVMディザスタ リカバリの次のスケジュールされている更新は成功します。
整合性グループ	ONTAP 9.14.1以降でサポートされます。詳細については、整合性グループの保護を参照してください。
ONTAP S3	SVMディザスタ リカバリではサポートされません。

SnapMirror Synchronous	SVMディザスタ リカバリではサポートされません。
バージョンへの非依存性	サポートされていません。
ボリューム暗号化	• ソースで暗号化されたボリュームがデスティネーションで暗号化されます。 • オンボード キー マネージャまたはKMIPサーバをデスティネーションで設定する必要があります。 • 新しい暗号化キーはデスティネーションで生成されます。 • ボリューム暗号化をサポートするノードがデスティネーションに含まれていない場合、レプリケーションは成功しますが、デスティネーション ボリュームは暗号化されません。

SVMディザスタ リカバリ関係でレプリケートされる設定

次の表は、`snapmirror create -identity-preserve`オプションと `snapmirror policy create -discard-configs network`オプションの相互作用を示しています：

レプリケートされる設定		-identity-preserve true		-identity-preserve false
		* `'-discard-configs network`が設定されていないポリシー*	* `'-discard-configs network`が設定されたポリシー*	
ネットワーク	NAS LIF	はい	いいえ	いいえ
LIFのKerberos設定	はい	いいえ	いいえ	SAN LIF
いいえ	いいえ	いいえ	ファイアウォールポリシー	はい
はい	いいえ	サービス ポリシー	はい	はい
いいえ	ルート	はい	いいえ	いいえ
ブロードキャストドメイン	いいえ	いいえ	いいえ	サブネット
いいえ	いいえ	いいえ	IPspace	いいえ
いいえ	いいえ	SMB	SMB サーバ	はい

はい	いいえ	ローカル グループ およびローカル ユーザ	はい	はい
はい	権限	はい	はい	はい
シャドウ コピー	はい	はい	はい	BranchCache
はい	はい	はい	サーバ オプション	はい
はい	はい	サーバ セキュリ ティ	はい	はい
いいえ	ホーム ディレクト リ、共有	はい	はい	はい
シンボリックリンク	はい	はい	はい	Fpolicyポリシ ー、Fsecurityポリシ ー、およびFsecurity NTFS
はい	はい	はい	ネーム マッピング およびグループ マ ッピング	はい
はい	はい	監査情報	はい	はい
はい	NFS	エクスポート ポリ シー	はい	はい
いいえ	エクスポート ポリ シー ルール	はい	はい	いいえ
NFS サーバ	はい	はい	いいえ	RBAC
セキュリティ証明書	はい	はい	いいえ	ログイン ユーザ、 公開鍵、ロール、お よびロール設定
はい	はい	はい	SSL	はい
はい	いいえ	ネーム サービス	DNSおよびDNSホス ト	はい

はい	いいえ	UNIXユーザおよびUNIXグループ	はい	はい
はい	Kerberos RealmおよびKerberosキーブロック	はい	はい	いいえ
LDAPおよびLDAPクライアント	はい	はい	いいえ	Netgroup
はい	はい	いいえ	NIS	はい
はい	いいえ	WebおよびWebアクセス	はい	はい
いいえ	Volume	オブジェクト	はい	はい
はい	スナップショットとスナップショットポリシー	はい	はい	はい
自動削除ポリシー	いいえ	いいえ	いいえ	効率化ポリシー
はい	はい	はい	クォータ ポリシー およびクォータ ポリシー ルール	はい
はい	はい	リカバリ キュー	はい	はい
はい	ルート ボリューム	ネームスペース	はい	はい
はい	ユーザ データ	いいえ	いいえ	いいえ
qtree	いいえ	いいえ	いいえ	クォータ
いいえ	いいえ	いいえ	ファイルレベルのQoS	いいえ
いいえ	いいえ	属性：ルート ボリュームの状態、スペース ガランティ、サイズ、オートサイズ、およびファイル総数	いいえ	いいえ

いいえ	ストレージQoS	QoSポリシー グループ	はい	はい
はい	Fibre Channel (FC)	いいえ	いいえ	いいえ
iSCSI	いいえ	いいえ	いいえ	LUN
オブジェクト	はい	はい	はい	igroup
いいえ	いいえ	いいえ	ポートセット	いいえ
いいえ	いいえ	シリアル番号	いいえ	いいえ
いいえ	SNMP	v3ユーザ	はい	はい

SVMディザスタ リカバリのストレージ制限

以下の表は、ストレージオブジェクトごとにサポートされるボリュームとSVMディザスタリカバリ関係の推奨最大数を示しています。制限はプラットフォームによって異なる場合がありますことに注意してください。特定の構成の制限については、"[Hardware Universe](#)"を参照してください。

ストレージ オブジェクト	制限
SVM	300個のフレキシブル ボリューム
HAペア	1,000 Flexible Volume
クラスタ	128個のSVMディザスタ リカバリ関係

関連情報

- "[snapmirror create](#)"
- "[snapmirror policy create](#)"

SVMの設定のレプリケート

ONTAP SnapMirror SVM レプリケーション ワークフロー

SnapMirror SVMレプリケーションでは、デスティネーションSVMを作成し、レプリケーション ジョブ スケジュールを作成し、SnapMirror関係を作成して初期化します。

ニーズに最適なレプリケーション ワークフローを決める必要があります。

- "[SVMの設定全体のレプリケート](#)"
- "[SVMレプリケーション対象からのLIFと関連ネットワークの設定の除外](#)"

- ["SVM構成からのネットワーク、ネーム サービス、およびその他の設定の除外"](#)

ONTAP SnapMirrorデスティネーション SVMにボリュームを配置するための基準

ソースSVMからデスティネーションSVMにボリュームをレプリケートするときは、アグリゲートの選択基準を理解しておくことが重要です。

アグリゲートは次の基準に基づいて選択されます。

- ボリュームは常に非ルート アグリゲートに配置されます。
- 非ルートアグリゲートは、使用可能な空き領域と、アグリゲート上ですでにホストされているボリュームの数に基づいて選択されます。

空きスペースが多く、ボリューム数が少ないアグリゲートが優先されます。優先度が最も高いアグリゲートが選択されます。

- FabricPoolアグリゲートのソース ボリュームは、デスティネーションのFabricPoolアグリゲートに同じ階層化ポリシーで配置されます。
- ソース SVM 上のボリュームが Flash Pool アグリゲート上にある場合、そのようなアグリゲートが存在し、十分な空き領域があれば、ボリュームは宛先 SVM 上の Flash Pool アグリゲート上に配置されます。
- 複製されるボリュームの `-space-guarantee` オプションが `volume` に設定されている場合、ボリュームサイズよりも大きい空き領域を持つアグリゲートのみが考慮されます。
- レプリケーション中に、ソースボリュームのサイズに基づいて、デスティネーションSVMのボリュームサイズが自動的に増加します。

デスティネーションSVMでサイズを事前に予約したい場合は、ボリュームのサイズを変更する必要があります。ソースSVMに基づいてデスティネーションSVMのボリュームサイズが自動的に縮小されることはありません。

ボリュームをあるアグリゲートから別のアグリゲートに移動する場合は、宛先 SVM で `volume move` コマンドを使用できます。

ONTAP SVM構成全体を複製する

SVMディザスタ リカバリ (SVM DR) 関係を作成して、SVMの設定を別のSVMにレプリケートできます。プライマリ サイトで災害が発生したときに、デスティネーションSVMを迅速にアクティブ化できます。

開始する前に

ソース クラスタとデスティネーション クラスタおよび SVM はピアリングされている必要があります。詳細については、["クラスタ ピア関係の作成"](#)および["SVMクラスタ間ピア関係を作成する"](#)を参照してください。

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

タスク概要

このワークフローでは、デフォルト ポリシーまたはカスタム レプリケーション ポリシーをすでに使用していることを前提としています。

ONTAP 9.9.1以降では、mirror-vaultポリシーを使用する場合、ソースSVMとデスティネーションSVMで異なるSnapshotポリシーを作成でき、デスティネーションのSnapshotがソースのSnapshotによって上書きされることはありません。詳細については、"[SnapMirror SVMレプリケーションの概要](#)"を参照してください。

この手順は、デスティネーションから実行してください。新しい保護ポリシーを作成する必要がある場合（例えば、ソースストレージVMにSMBが設定されている場合など）は、ポリシーを作成し、*Identity preserve* オプションを使用してください。詳細については、"[カスタムのデータ保護ポリシーの作成](#)"を参照してください。

手順

このタスクは、System ManagerまたはONTAP CLIから実行できます。

System Manager

1. デスティネーション クラスタで、*保護 > 関係*をクリックします。
2. *関係*で、*保護*をクリックし、*Storage VM (DR)*を選択します。
3. 保護ポリシーを選択します。カスタムの保護ポリシーを作成した場合は、そのポリシーを選択してから、レプリケートするソース クラスタとStorage VMを選択します。新しいStorage VM名を入力して新しいデスティネーションStorage VMを作成することもできます。
4. 必要に応じて、デスティネーションの設定を変更し、ID保持を上書きするかどうか、ネットワーク インターフェイスおよびプロトコルを含めるか除外するかを指定します。
5. *保存*をクリックします。

CLI

1. デスティネーションSVMを作成します。

```
vserver create -vserver <SVM_name> -subtype dp-destination
```

SVM名はソース クラスタとデスティネーション クラスタの間で一意である必要があります。

次の例では、`svm\_backup`という名前のデスティネーション SVM を作成します：

```
cluster_dst:> vserver create -vserver svm_backup -subtype dp-destination
```

`vserver create`の詳細については、link:<https://docs.netapp.com/us-en/ontap-cli/vserver-create.html>["ONTAPコマンド リファレンス"]を参照してください。

2. デスティネーション クラスタから、`vserver peer create`コマンドを使用して SVM ピア関係を作成します。

詳細については、"[SVMクラスタ間ピア関係を作成する](#)"を参照してください。

`vserver peer create`の詳細については、link:<https://docs.netapp.com/us-en/ontap-cli/vserver-peer-create.html>["ONTAPコマンド リファレンス"]をご覧ください。

3. レプリケーション ジョブ スケジュールを作成します。

```
job schedule cron create -name <job_name> -month <month> -dayofweek <day_of_week> -day <day_of_month> -hour <hour> -minute <minute>
```

`-month`、`-dayofweek`、および`-hour`の場合、
`all`を指定して、それぞれ毎月、曜日ごと、および時間ごとにジョブを実行できます。



SVM SnapMirror関係のFlexVolに設定可能な最短スケジュール（RPO）は15分です。SVM SnapMirror関係のFlexGroupボリュームに設定可能な最短スケジュール（RPO）は30分です。

次の例では、土曜日の午前3：00に実行される`my\_weekly`という名前のジョブ スケジュールを作成します：

```
cluster_dst:> job schedule cron create -name my_weekly -dayofweek  
saturday -hour 3 -minute 0
```

```
`job schedule cron create`
```

の詳細については、[link:https://docs.netapp.com/us-en/ontap-cli/job-schedule-cron-create.html](https://docs.netapp.com/us-en/ontap-cli/job-schedule-cron-create.html)["ONTAPコマンド リファレンス
"^]を参照してください。

4. デスティネーションSVMまたはデスティネーション クラスタから、レプリケーション関係を作成します。

```
snapmirror create -source-path <SVM_name>: -destination-path  
<SVM_name>: -type <DP|XDP> -schedule <schedule> -policy <policy>  
-identity-preserve true
```



`-source-path`および`-destination-path`オプションでは、SVM 名の後にコロン（:）
を入力する必要があります。

次の例では、デフォルト`MirrorAllSnapshots`ポリシーを使用してSnapMirror DR関係を作成します：

```
cluster_dst:> snapmirror create -source-path svm1: -destination  
-path svm_backup: -type XDP -schedule my_daily -policy  
MirrorAllSnapshots -identity-preserve true
```

次の例では、デフォルトの`MirrorAndVault`ポリシーを使用して統合レプリケーション関係を作成します：

```
cluster_dst:> snapmirror create -source-path svm1: -destination-path  
svm_backup: -type XDP -schedule my_daily -policy MirrorAndVault  
-identity-preserve true
```

ポリシー タイプ `async-mirror` でカスタム ポリシーを作成したと仮定すると、次の例ではSnapMirror DR関係が作成されます：

```
cluster_dst::> snapmirror create -source-path svm1: -destination  
-path svm_backup: -type XDP -schedule my_daily -policy my_mirrored  
-identity-preserve true
```

ポリシー タイプ `mirror-vault` でカスタム ポリシーを作成したと仮定すると、次の例では統合レプリケーション関係が作成されます：

```
cluster_dst::> snapmirror create -source-path svm1: -destination  
-path svm_backup: -type XDP -schedule my_daily -policy my_unified  
-identity-preserve true
```

`snapmirror create`の詳細については、link:<https://docs.netapp.com/us-en/ontap-cli/snapmirror-create.html>["ONTAPコマンド リファレンス"]を参照してください。

5. デスティネーションSVMを停止します。

```
vserver stop -vserver <SVM_name>
```

次の例は、svm_backupという名前のデスティネーションSVMを停止します。

```
cluster_dst::> vserver stop -vserver svm_backup
```

`vserver stop`の詳細については、link:<https://docs.netapp.com/us-en/ontap-cli/vserver-stop.html>["ONTAPコマンド リファレンス"]を参照してください。

6. デスティネーションSVMまたはデスティネーション クラスタから、SVMレプリケーション関係を初期化します。

```
snapmirror initialize -source-path <SVM_name>: -destination-path  
<SVM_name>:
```



`-source-path`および`-destination-path`オプションでは、SVM 名の後にコロン（:）を入力する必要があります。

次の例では、ソース SVM `svm1` とデスティネーション SVM `svm\_backup` の関係を初期化します：

```
cluster_dst:> snapmirror initialize -source-path svm1: -destination  
-path svm_backup:
```

```
`snapmirror initialize`  
の詳細については、link:https://docs.netapp.com/us-en/ontap-  
cli/snapmirror-initialize.html["ONTAP コマンド リファレンス  
"^]を参照してください。
```

ONTAP SnapMirror SVM レプリケーションから LIF と関連ネットワーク設定を除外する

ソース SVM とデスティネーション SVM が異なるサブネットにある場合は、`snapmirror policy create` コマンドの `--discard-configs network` オプションを使用して、LIF および関連するネットワーク設定を SVM レプリケーションから除外できます。

開始する前に

ソース / デスティネーション クラスタと SVM のピア関係が確立されている必要があります。

詳細については、"[クラスタ ピア関係の作成](#)"および"[SVM クラスタ間ピア関係を作成する](#)"を参照してください。

タスク概要

`snapmirror create` コマンドの `--identity-preserve` オプションは、SVM レプリケーション関係を作成するときに `true` に設定する必要があります。

手順

1. デスティネーション SVM を作成します。

```
vserver create -vserver SVM -subtype dp-destination
```

SVM 名はソース クラスタとデスティネーション クラスタの間で一意である必要があります。

次の例では、`svm\_backup` という名前のデスティネーション SVM を作成します：

```
cluster_dst:> vserver create -vserver svm_backup -subtype dp-destination
```

2. デスティネーション クラスタから、`vserver peer create` コマンドを使用して SVM ピア関係を作成します。

詳細については、"[SVM クラスタ間ピア関係を作成する](#)"を参照してください。

`vserver peer create`の詳細については、link:<https://docs.netapp.com/us-en/ontap-cli/vserver-peer-create.html>["ONTAPコマンド リファレンス"]をご覧ください。

3. ジョブ スケジュールを作成します。

```
job schedule cron create -name job_name -month month -dayofweek day_of_week  
-day day_of_month -hour hour -minute minute
```

`-month`、`-dayofweek`、および`-hour`の場合、
`all`を指定して、それぞれ毎月、曜日ごと、および時間ごとにジョブを実行できます。



SVM SnapMirror関係のFlexVolに設定可能な最短スケジュール（RPO）は15分です。SVM SnapMirror関係のFlexGroupボリュームに設定可能な最短スケジュール（RPO）は30分です。

次の例では、土曜日の午前3：00に実行される`my\_weekly`という名前のジョブ スケジュールを作成します：

```
cluster_dst::> job schedule cron create -name my_weekly -dayofweek  
"Saturday" -hour 3 -minute 0
```

4. カスタム レプリケーション ポリシーを作成します。

```
snapmirror policy create -vserver SVM -policy policy -type async-  
mirror|vault|mirror-vault -comment comment -tries transfer_tries -transfer  
-priority low|normal -is-network-compression-enabled true|false -discard  
-configs network
```

次の例は、LIFを除外するSnapMirror DR用のカスタム レプリケーション ポリシーを作成します。

```
cluster_dst::> snapmirror policy create -vserver svm1 -policy  
DR_exclude_LIFs -type async-mirror -discard-configs network
```

次の例は、LIFを除外するユニファイド レプリケーション用のカスタム レプリケーション ポリシーを作成します。

```
cluster_dst::> snapmirror policy create -vserver svm1 -policy  
unified_exclude_LIFs -type mirror-vault -discard-configs network
```



今後のフェイルオーバーやフェイルバックのシナリオに備えて、ソース クラスタに同じカスタムSnapMirrorポリシーを作成することを検討してください。

```
`snapmirror policy create`
```

の詳細については、link:<https://docs.netapp.com/us-en/ontap-cli/snapmirror-policy-create.html>["ONTAPコマンド リファレンス"^]を参照してください。

5. デスティネーションSVMまたはデスティネーション クラスタから次のコマンドを実行して、レプリケーション関係を作成します。

```
snapmirror create -source-path SVM: -destination-path SVM: -type DP|XDP  
-schedule schedule -policy policy -identity-preserve true|false -discard  
-configs true|false
```



`-source-path`および `-destination-path`オプションでは、SVM名の後にコロンの(:)を入力する必要があります。以下の例をご覧ください。

次の例は、LIFを除外するSnapMirror DR関係を作成します。

```
cluster_dst:> snapmirror create -source-path svm1: -destination-path  
svm_backup: -type XDP -schedule my_weekly -policy DR_exclude_LIFs  
-identity-preserve true
```

次の例は、LIFを除外するSnapMirrorユニファイド レプリケーション関係を作成します。

```
cluster_dst:> snapmirror create -source-path svm1: -destination-path  
svm_backup: -type XDP -schedule my_weekly -policy unified_exclude_LIFs  
-identity-preserve true -discard-configs true
```

`snapmirror create`の詳細については、link:<https://docs.netapp.com/us-en/ontap-cli/snapmirror-create.html>["ONTAPコマンド リファレンス"^]を参照してください。

6. デスティネーションSVMを停止します。

```
vserver stop
```

SVM name

次の例は、svm_backupという名前のデスティネーションSVMを停止します。

```
cluster_dst:> vserver stop -vserver svm_backup
```


7. デスティネーションSVMまたはデスティネーション クラスタから、レプリケーション関係を初期化します。

```
snapmirror initialize -source-path SVM: -destination-path SVM:
```

次の例では、ソース `svm1` とデスティネーション `svm\_backup` の関係を初期化します：

```
cluster_dst::> snapmirror initialize -source-path svm1: -destination  
-path svm_backup:
```

`snapmirror initialize`の詳細については、[link:https://docs.netapp.com/us-en/ontap-cli/snapmirror-initialize.html](https://docs.netapp.com/us-en/ontap-cli/snapmirror-initialize.html)["ONTAP コマンド リファレンス"]を参照してください。

終了後の操作

災害発生時のデータ アクセス用に、デスティネーションSVMでネットワークとプロトコルを設定する必要があります。

関連情報

- "[snapmirror create](#)"
- "[snapmirror initialize](#)"
- "[snapmirror policy create](#)"

ONTAPを使用した**SVM** レプリケーションからネットワーク、ネーム サービス、およびその他の設定を除外

デスティネーション SVM との競合や設定の違いを回避するために、ネットワーク、ネーム サービス、およびその他の設定を SVM レプリケーション関係から除外する必要があります。

`snapmirror create` コマンドの `--identity-preserve false`

オプションを使用すると、SVMのボリュームとセキュリティ設定のみをレプリケートできます。一部のプロトコルとネーム サービスの設定も保持されます。

タスク概要

保存されるプロトコルおよび名前サービス設定の一覧については、"[SVM DR関係でレプリケートされる設定](#)"を参照してください。

開始する前に

ソース / デスティネーション クラスタとSVMのピア関係が確立されている必要があります。

詳細については、"[クラスタ ピア関係の作成](#)"および"[SVMクラスタ間ピア関係を作成する](#)"を参照してください。

手順

1. デスティネーションSVMを作成します。

```
vserver create -vserver SVM -subtype dp-destination
```

SVM名はソース クラスタとデスティネーション クラスタの間で一意である必要があります。

次の例では、`svm\_backup`という名前のデスティネーション SVM を作成します：

```
cluster_dst:> vserver create -vserver svm_backup -subtype dp-destination
```

2. デスティネーション クラスタから、`vserver peer create`コマンドを使用して SVM ピア関係を作成します。

詳細については、"[SVMクラスタ間ピア関係を作成する](#)"を参照してください。

`vserver peer create`の詳細については、[link:https://docs.netapp.com/us-en/ontap-cli/vserver-peer-create.html](https://docs.netapp.com/us-en/ontap-cli/vserver-peer-create.html) ["ONTAPコマンド リファレンス"]をご覧ください。

3. レプリケーション ジョブ スケジュールを作成します。

```
job schedule cron create -name job_name -month month -dayofweek day_of_week  
-day day_of_month -hour hour -minute minute
```

`-month`、`-dayofweek`、および `-hour`の場合、
`all`を指定して、それぞれ毎月、曜日ごと、および時間ごとにジョブを実行できます。



SVM SnapMirror関係のFlexVolに設定可能な最短スケジュール（RPO）は15分です。SVM SnapMirror関係のFlexGroupボリュームに設定可能な最短スケジュール（RPO）は30分です。

次の例では、土曜日の午前3：00に実行される `my\_weekly` という名前のジョブ スケジュールを作成します：

```
cluster_dst:> job schedule cron create -name my_weekly -dayofweek  
"Saturday" -hour 3 -minute 0
```

4. ネットワーク、ネーム サービス、およびその他の設定を除外するレプリケーション関係を作成します。

```
snapmirror create -source-path SVM: -destination-path SVM: -type DP|XDP  
-schedule schedule -policy policy -identity-preserve false
```



`-source-path`および`-destination-path`オプションのSVM名の後にコロン（:）を入力する必要があります。以下の例を参照してください。このコマンドは、デスティネーション SVMまたはデスティネーション クラスタから実行する必要があります。

次の例では、デフォルト`MirrorAllSnapshots`ポリシーを使用してSnapMirror DR関係を作成します。この関係では、ネットワーク、ネーム サービス、およびその他の設定がSVMレプリケーションから除外されます。

```
cluster_dst:> snapmirror create -source-path svm1: -destination-path  
svm_backup: -type XDP -schedule my_daily -policy MirrorAllSnapshots  
-identity-preserve false
```

次の例では、デフォルト`MirrorAndVault`ポリシーを使用して統合レプリケーション関係を作成します。この関係では、ネットワーク、ネーム サービス、その他の構成設定は除外されます：

```
cluster_dst:> snapmirror create svm1: -destination-path svm_backup:  
-type XDP -schedule my_daily -policy MirrorAndVault -identity-preserve  
false
```

ポリシータイプ`async-mirror`のカスタムポリシーを作成したと仮定すると、次の例ではSnapMirror DR関係を作成します。この関係では、ネットワーク、ネームサービス、およびその他の設定がSVMレプリケーションから除外されます：

```
cluster_dst:> snapmirror create -source-path svm1: -destination-path  
svm_backup: -type XDP -schedule my_daily -policy my_mirrored -identity  
-preserve false
```

ポリシータイプ`mirror-vault`のカスタムポリシーを作成したと仮定すると、次の例では統合レプリケーション関係を作成します。この関係では、ネットワーク、ネームサービス、およびその他の設定がSVMレプリケーションから除外されます：

```
cluster_dst:> snapmirror create -source-path svm1: -destination-path  
svm_backup: -type XDP -schedule my_daily -policy my_unified -identity  
-preserve false
```

`snapmirror create`の詳細については、link:<https://docs.netapp.com/us-en/ontap-cli/snapmirror-create.html>["ONTAPコマンド リファレンス"]を参照してください。

5. デスティネーションSVMを停止します。

```
vserver stop
```

SVM name

次の例は、dvs1という名前のデスティネーションSVMを停止します。

```
destination_cluster::> vserver stop -vserver dvs1
```

6. SMBを使用している場合は、SMBサーバも設定する必要があります。

"[SMBのみ：SMBサーバーの作成](#)"を参照してください。

7. デスティネーションSVMまたはデスティネーション クラスタから、SVMレプリケーション関係を初期化します。

```
snapmirror initialize -source-path SVM_name: -destination-path SVM_name:
```

`snapmirror initialize`の詳細については、[link:https://docs.netapp.com/us-en/ontap-cli/snapmirror-initialize.html](https://docs.netapp.com/us-en/ontap-cli/snapmirror-initialize.html)["ONTAPコマンド リファレンス"]を参照してください。

終了後の操作

災害発生時のデータ アクセス用に、デスティネーションSVMでネットワークとプロトコルを設定する必要があります。

ONTAP SnapMirror SVM DR関係に使用するローカル階層を指定する

ディザスタ リカバリ SVM が作成された後、`aggr-list`オプションと`vserver modify`コマンドを使用して、SVM DR デスティネーション ボリュームをホストするために使用されるローカル層を制限できます。

手順

1. デスティネーションSVMを作成します。

```
vserver create -vserver SVM -subtype dp-destination
```

2. ディザスタ リカバリSVMのaggr-listを変更して、ディザスタ リカバリSVMのボリュームをホストするために使用されるローカル層を制限します：

```
cluster_dest::> vserver modify -vserver SVM -aggr-list <comma-separated-list>
```

DR関係のONTAP SnapMirrorデスティネーションSVM用のSMBサーバを作成する

ソースSVMにSMB設定があり、`identity-preserve`を`false`に設定する場合は、デステ

イネーションSVM用にSMBサーバを作成する必要があります。SMBサーバは、SnapMirror関係の初期化中の共有など、一部のSMB設定が必要です。

手順

1. `vserver start` コマンドを使用してデスティネーション SVM を起動します。

```
destination_cluster::> vserver start -vserver dvs1
[Job 30] Job succeeded: DONE
```

`vserver start`の詳細については、link:<https://docs.netapp.com/us-en/ontap-cli/vserver-start.html>["ONTAPコマンド リファレンス"]を参照してください。

2. `vserver show` コマンドを使用して、デスティネーションSVMが`running`状態でサブタイプが`dp-destination`になっていることを確認します。

```
destination_cluster::> vserver show
```

Vserver	Type	Subtype	Admin State	Operational State	Root Volume
Aggregate					

dvs1	data	dp-destination	running	running	-

`vserver show`の詳細については、link:<https://docs.netapp.com/us-en/ontap-cli/vserver-show.html>["ONTAPコマンド リファレンス"]を参照してください。

3. `network interface create` コマンドを使用してLIFを作成します。

```
destination_cluster::>network interface create -vserver dvs1 -lif NAS1
-role data -data-protocol cifs -home-node destination_cluster-01 -home
-port a0a-101 -address 192.0.2.128 -netmask 255.255.255.128
```

`network interface create`
の詳細については、link:<https://docs.netapp.com/us-en/ontap-cli/network-interface-create.html>["ONTAPコマンド リファレンス"]を参照してください。

4. `network route create` コマンドを使用してルートを作成します。

```
destination_cluster::>network route create -vserver dvs1 -destination
0.0.0.0/0
-gateway 192.0.2.1
```

"ネットワーク管理"

`network route create`の詳細については、link:<https://docs.netapp.com/us-en/ontap-cli/network-route-create.html>["ONTAPコマンド リファレンス"]を参照してください。

5. `vserver services dns create`コマンドを使用してDNSを設定します。

```
destination_cluster::>vserver services dns create -domains
mydomain.example.com -vserver
dvs1 -name-servers 192.0.2.128 -state enabled
```

`vserver services dns create`
の詳細については、link:<https://docs.netapp.com/us-en/ontap-cli/search.html?q=vserver+services+dns+create>["ONTAPコマンド リファレンス"]を参照してください。

6. `vserver cifs domain preferred-dc add`コマンドを使用して優先ドメイン コントローラを追加します。

```
destination_cluster::>vserver cifs domain preferred-dc add -vserver dvs1
-preferred-dc
192.0.2.128 -domain mydomain.example.com
```

`vserver cifs domain preferred-dc add`
の詳細については、link:<https://docs.netapp.com/us-en/ontap-cli/vserver-cifs-domain-preferred-dc-add.html>["ONTAPコマンド リファレンス"]を参照してください。

7. `vserver cifs create`コマンドを使用してSMBサーバーを作成します。

```
destination_cluster::>vserver cifs create -vserver dvs1 -domain
mydomain.example.com
-cifs-server CIFS1
```

`vserver cifs create`の詳細については、link:<https://docs.netapp.com/us-en/ontap-cli/vserver-cifs-create.html>["ONTAPコマンド リファレンス"]を参照してください。

8. `vserver stop`コマンドを使用してデスティネーション SVM を停止します。

```
destination_cluster::> vserver stop -vserver dvs1  
[Job 46] Job succeeded: DONE
```

`vserver stop`の詳細については、link:<https://docs.netapp.com/us-en/ontap-cli/vserver-stop.html>["ONTAPコマンド リファレンス"]を参照してください。

ONTAP SnapMirror SVM DR関係からボリュームを除外する

デフォルトでは、ソース SVM のすべての RW データ ボリュームがレプリケートされます。ソース SVM 上のすべてのボリュームを保護したくない場合は、`volume modify` コマンドの `-vserver-dr-protection unprotected` オプションを使用して、SVM レプリケーションからボリュームを除外できます。

手順

1. SVMレプリケーション対象からボリュームを除外します。

```
volume modify -vserver SVM -volume volume -vserver-dr-protection unprotected
```

`volume modify`の詳細については、link:<https://docs.netapp.com/us-en/ontap-cli/volume-modify.html>["ONTAPコマンド リファレンス"]をご覧ください。

次の例では、ボリューム `volA\_src` を SVM レプリケーションから除外します：

```
cluster_src::> volume modify -vserver SVM1 -volume volA_src -vserver-dr-protection unprotected
```

除外したボリュームをあとでSVMレプリケーション対象に含めるには、次のコマンドを実行します。

```
volume modify -vserver SVM -volume volume -vserver-dr-protection protected
```

次の例では、ボリューム `volA\_src` を SVM レプリケーションに含めます：

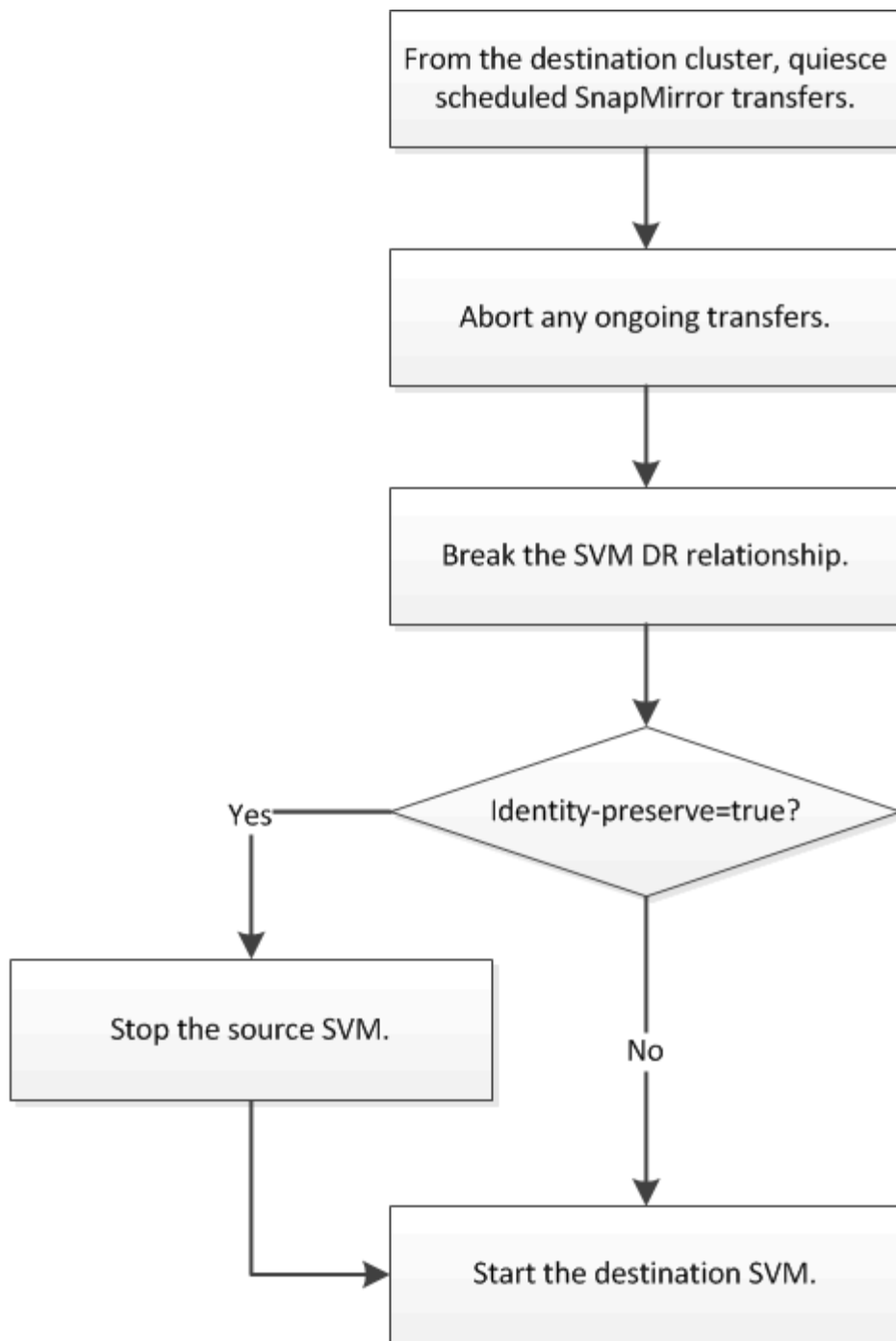
```
cluster_src::> volume modify -vserver SVM1 -volume volA_src -vserver-dr  
-protection protected
```

2. "SVMの設定全体のレプリケート"の説明に従って、SVM レプリケーション関係を作成して初期化します。

SnapMirror SVM DRデスティネーションからデータを提供する

ONTAP SnapMirror SVM災害復旧ワークフロー

災害からリカバリしてデスティネーションSVMからデータを提供するには、デスティネーションSVMをアクティブ化する必要があります。デスティネーションSVMのアクティブ化では、スケジュールされたSnapMirror転送の停止、実行中のSnapMirror転送の中止、レプリケーション関係の解除、ソースSVMの停止、デスティネーションSVMの起動が実行されます。



ONTAP SnapMirror SVMのデスティネーション ボリュームを書き込み可能に設定する

クライアントにデータを提供する前に、SVMデスティネーション ボリュームを書き込み可能にする必要があります。

手順はボリュームレプリケーションの手順とほぼ同じですが、1つだけ例外があります。SVMレプリケーション関係の作成時に `identity-preserve true` を設定した場合は、デスティネーションSVMをアクティブ化する前にソースSVMを停止する必要があります。

タスク概要

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



ディザスタ リカバリのシナリオでは、ソースSVMとそのデータにアクセスできなくなること、および最後の再同期以降の更新が無効または破損している可能性があることから、ソースSVMからディザスタ リカバリ デスティネーションSVMにSnapMirror更新を実行することはできません。

ONTAP 9.8以降では、System Managerを使用して、災害発生後にデスティネーションStorage VMをアクティブ化できます。デスティネーションStorage VMをアクティブ化すると、SVMデスティネーション ボリュームが書き込み可能になり、クライアントにデータを提供できるようになります。

手順

このタスクは、System ManagerまたはONTAP CLIから実行できます。

System Manager

1. ソース クラスタにアクセスできる場合は、SVMが停止していることを確認します。*Storage > Storage VMs*に移動し、SVMの*State*列を確認します。
2. ソース SVM の状態が「実行中」の場合は、停止します。⋮を選択して、*停止*を選択します。
3. デスティネーション クラスタで、必要な保護関係を見つけます：*[保護] > [関係]*に移動します。
4. 目的のソース ストレージ VM 名にマウスを移動し、⋮をクリックして、*宛先ストレージ VM のアクティブ化*を選択します。
5. デスティネーション ストレージ **VM** をアクティブ化 ウィンドウで、デスティネーション ストレージ **VM** をアクティブ化して関係を解除 を選択します。
6. *Activate*をクリックします。

CLI

1. デスティネーション SVM またはデスティネーション クラスタから、SVM を休止して、デスティネーションへのスケジュールされた転送を停止します：

```
snapmirror quiesce -source-path <SVM>: -destination-path <SVM>:
```



`-source-path`および`-destination-path`オプションでは、SVM名の後にコロン（:）を入力する必要があります。以下の例をご覧ください。

次の例では、ソース SVM `svm1`とデスティネーション SVM `svm\_backup`間のスケジュールされた転送を停止します：

```
cluster_dst::> snapmirror quiesce -source-path svm1: -destination  
-path svm_backup:
```

`snapmirror quiesce`の詳細については、[link:https://docs.netapp.com/us-en/ontap-cli/snapmirror-quiesce.html](https://docs.netapp.com/us-en/ontap-cli/snapmirror-quiesce.html)["ONTAPコマンド リファレンス"]を参照してください。

2. デスティネーションSVMまたはデスティネーション クラスタから、デスティネーションへの実行中の転送を停止します。

```
snapmirror abort -source-path <SVM>: -destination-path <SVM>:
```



`-source-path`および`-destination-path`オプションでは、SVM名の後にコロン（:）を入力する必要があります。以下の例をご覧ください。

次の例では、ソース SVM `svm1`とデスティネーション SVM `svm\_backup`間の進行中の転送を停止します：

```
cluster_dst::> snapmirror abort -source-path svm1: -destination-path  
svm_backup:
```

`snapmirror abort`の詳細については、link:<https://docs.netapp.com/us-en/ontap-cli/snapmirror-abort.html>["ONTAPコマンド リファレンス"]をご覧ください。

3. デスティネーションSVMまたはデスティネーション クラスタから、レプリケーション関係を解除します。

```
snapmirror break -source-path <SVM>: -destination-path <SVM>:
```



`-source-path`および`-destination-path`オプションでは、SVM名の後にコロン（:）を入力する必要があります。以下の例をご覧ください。

次の例では、ソース SVM `svm1`とデスティネーション SVM `svm\_backup`間の関係を解除します：

```
cluster_dst::> snapmirror break -source-path svm1: -destination-path  
svm_backup:
```

`snapmirror break`の詳細については、link:<https://docs.netapp.com/us-en/ontap-cli/snapmirror-break.html>["ONTAPコマンド リファレンス"]を参照してください。

4. SVM レプリケーション関係の作成時に`-identity-preserve true`を設定した場合は、ソース SVM を停止します。

```
vserver stop -vserver <SVM>
```

次の例では、ソース SVM を停止します svm1：

```
cluster_src::> vserver stop svm1
```

5. デスティネーションSVMを起動します。

```
vserver start -vserver <SVM>
```

次の例では、デスティネーション SVM を起動します svm_backup：

```
cluster_dst::> vserver start svm_backup
```

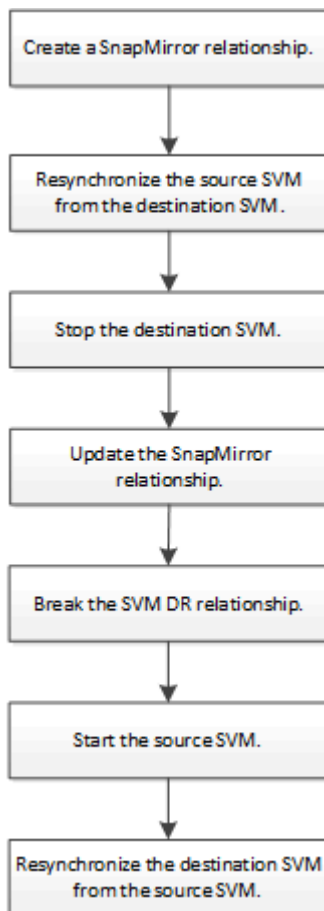
終了後の操作

"[データ アクセスのためのデスティネーション ボリュームの設定](#)"の説明に従って、データ アクセス用に SVM デスティネーション ボリュームを設定します。

SnapMirrorソースSVMを再アクティブ化する

ONTAP SnapMirror ソース SVM の再アクティブ化ワークフロー

災害発生後もソースSVMが残っている場合は、そのソースSVMを再アクティブ化し、SVMディザスタ リカバリ関係を再作成して保護できます。



元のONTAP SnapMirrorソースSVMを再アクティブ化する

デスティネーションからデータを提供する必要がなくなった場合は、ソースSVMとデスティネーションSVMの間で元のデータ保護関係を再確立できます。この手順は、1つの例外を除き、ボリューム レプリケーションの手順とほぼ同じです。ソースSVMを再アクティブ化する前に、デスティネーションSVMを停止する必要があります。

開始する前に

- デスティネーション ボリュームからデータを提供している間にそのサイズを拡張した場合は、ソース ボリュームを再アクティブ化する前に、元のソース ボリュームを十分拡張できるようにmax-autosizeを手動で増やす必要があります。

"デスティネーション ボリュームが自動的に拡張される状況"



クラスタ管理者は、データの損失を避けるために、元のソース SVM を再アクティブ化する前に、クライアントからの書き込みを一時停止する必要があります。

タスク概要

ONTAP 9.11.1以降では、SVM DR関係の逆再同期を実行する際に `snapmirror resync` コマンドのCLI `quick-resync true` オプションを使用することで、ディザスタリカバリのリハーサル中の再同期時間を短縮できます。クイック再同期によりデータ ウェアハウスの再構築とリストア処理をバイパスできるため、本番環境への復帰にかかる時間を短縮できます。["ONTAPコマンド リファレンス"](#)の `snapmirror resync` の詳細をご覧ください。



クイック再同期では、デスティネーション ボリュームのストレージ効率は維持されません。クイック再同期を有効にすると、デスティネーション ボリュームで使用されるボリューム スペースが増加する可能性があります。

この手順は、元のソース ボリュームにあるベースラインが損なわれていないことを前提としています。ベースラインが損なわれている場合は、この手順を実行する前に、データの提供元のボリュームと元のソース ボリュームの関係を作成して初期化する必要があります。

ONTAP 9.8以降では、System Managerを使用して、災害発生後にソースStorage VMを再アクティブ化できます。

手順

このタスクは、System Manager または ONTAP CLI を使用して実行できます。

System Manager ONTAP 9.17.1 以降

1. デスティネーション クラスタで、必要な保護関係を選択します：*保護 > レプリケーション*をクリックします。
2. ソース名の上にカーソルを合わせて  をクリックし、*逆再同期*をクリックします。
3. *逆再同期関係*ウィンドウで、*逆再同期*をクリックします。

関係は **Replication** テーブルから消え、元のソース クラスタによって管理されるようになります。

4. 元のソース クラスタで、**Protection > Replication** をクリックし、状態に **Mirrored** と表示されていることを確認し、逆再同期が完了したことを確認します。
5. 元のデスティネーション クラスタで、クラスタ > ストレージ **VM** に移動します。
6. ストレージ VM を見つけて、ストレージ VM 名の上にカーソルを置き、 をクリックして、*停止*をクリックします。
7. *ストレージ VM の停止*ウィンドウで、*停止*をクリックします。
8. ソース クラスタで、**[保護] > [レプリケーション]** に移動し、再アクティブ化するストレージ VM を見つけて、ストレージ VM 名の上にカーソルを移動し、 をクリックして、**[デスティネーション ストレージ VM のアクティブ化]** をクリックします。
9. *デスティネーション Storage VM のアクティブ化*ウィンドウで、*デスティネーション Storage VM をアクティブ化して関係を解除*を選択し、*アクティブ化*をクリックします。
10. レプリケーション ページに戻ったら、もう一度カーソルをストレージ VM 名の上に置いて  をクリックし、逆再同期 をクリックします。

System Manager ONTAP 9.16.1 以前

1. デスティネーション クラスタで、必要な保護関係を選択します：*[保護] > [関係]*をクリックします。
2. ソース名の上にカーソルを合わせて  をクリックし、*逆再同期*をクリックします。
3. *逆再同期関係*ウィンドウで、*逆再同期*をクリックします。

リレーションシップは元のソース クラスタによって管理されるようになったため、**Relationships** テーブルから消えます。

4. 元のソース クラスタで、**Protection > Relationships** をクリックし、状態が **Mirrored** と表示されていることを確認し、逆再同期が完了したことを確認します。
5. 元のデスティネーション クラスタで、ストレージ > ストレージ **VM** に移動します。
6. ストレージ VM を見つけて、ストレージ VM 名の上にカーソルを置き、 をクリックして、*停止*をクリックします。
7. *ストレージ VM の停止*ウィンドウで、*停止*をクリックします。
8. ソース クラスタで、ストレージ VM (反転された関係のソース SVM) を見つけ、SVM 名の上にカーソルを合わせて  をクリックし、宛先ストレージ **VM** のアクティブ化 をクリックします。
9. *デスティネーション Storage VM のアクティブ化*ウィンドウで、*デスティネーション Storage VM をアクティブ化して関係を解除*を選択し、*アクティブ化*をクリックします。
10. 関係 ページに戻ったら、もう一度カーソルをストレージ VM 名の上に置いて  をクリックし、逆再同期 をクリックします。

CLI

1. 元のソースSVMまたはソース クラスタから、元のSVM DR関係と同じ設定、ポリシー、およびidentity-preserve設定を使用して、反転したSVM DR関係を作成します。

```
snapmirror create -source-path <SVM>: -destination-path <SVM>:
```



`-source-path`および`-destination-path`オプションでは、SVM名の後にコロン（:）を入力する必要があります。以下の例をご覧ください。

次の例では、データの提供元となる SVM `svm\_backup`と元のソース SVM `svm1`の間に関係を作成します：

```
cluster_src::> snapmirror create -source-path svm_backup:
                        -destination-path svm1:
```

`snapmirror create`の詳細については、[link:https://docs.netapp.com/us-en/ontap-cli/snapmirror-create.html](https://docs.netapp.com/us-en/ontap-cli/snapmirror-create.html)["ONTAPコマンド リファレンス"]を参照してください。

2. 元のソースSVMまたはソース クラスタから次のコマンドを実行して、データ保護関係を反転します。

```
snapmirror resync -source-path <SVM>: -destination-path <SVM>:
```



`-source-path`および`-destination-path`オプションでは、SVM名の後にコロン（:）を入力する必要があります。以下の例をご覧ください。

再同期の際にベースライン転送は不要ですが、再同期には時間がかかる場合があります。再同期はオフピークの時間帯に実行することを推奨します。



ソースとデスティネーションに共通の Snapshot が存在しない場合、コマンドは失敗します。`snapmirror initialize`を使用して関係を再初期化します。

次の例では、元のソース SVM `svm1`とデータの提供元となる SVM `svm\_backup`の関係を反転します：

```
cluster_src::> snapmirror resync -source-path svm_backup:
                        -destination-path svm1:
```

-quick-resyncオプションの使用例：


```
cluster_src::> snapmirror resync -source-path svm_backup:
-destination-path svm1: -quick-resync true
```

3. 元のソースSVMへのデータ アクセスを再確立する準備ができたなら、元のデスティネーションSVMを停止してSVMに接続されているクライアントをすべて切断します。

```
vserver stop -vserver <SVM>
```

次の例は、現在データを提供している元のデスティネーションSVMを停止します。

```
cluster_dst::> vserver stop svm_backup
```

4. `vserver show` コマンドを使用して、元のデスティネーション SVM が停止状態になっていることを確認します。

```
cluster_dst::> vserver show
```

Vserver	Type	Subtype	Admin State	Operational State	Root Volume
Aggregate					
-----	-----	-----	-----	-----	-----

svm_backup	data	default	stopped	stopped	rv
aggr1					

5. 元のソースSVMまたはソース クラスタから次のコマンドを実行して反転した関係を最後にもう一度更新し、元のデスティネーションSVMから元のソースSVMにすべての変更を転送します。

```
snapmirror update -source-path <SVM>: -destination-path <SVM>:
```



`-source-path` および `-destination-path` オプションでは、SVM名の後にコロン（:）を入力する必要があります。以下の例をご覧ください。

次の例では、データの提供元である元のデスティネーション SVM、`svm\_backup` と元のソース SVM `svm1` の関係を更新します：

```
cluster_src::> snapmirror update -source-path svm_backup:
-destination-path svm1:
```

`snapmirror update`の詳細については、link:<https://docs.netapp.com/us-en/ontap-cli/snapmirror-update.html>["ONTAPコマンド リファレンス"]をご覧ください。

6. 元のソースSVMまたはソース クラスタから次のコマンドを実行して、反転した関係のスケジュールされた転送を停止します。

```
snapmirror quiesce -source-path <SVM>: -destination-path <SVM>:
```



`-source-path`および`-destination-path`オプションでは、SVM名の後にコロン（:）を入力する必要があります。以下の例をご覧ください。

次の例では、データの提供元である SVM `svm\_backup`と元の SVM `svm1`の間のスケジュールされた転送を停止します：

```
cluster_src::> snapmirror quiesce -source-path svm_backup:
-destination-path svm1:
```

7. 最後の更新が完了して関係のステータスが「Quiesced」になったら、元のソースSVMまたは元のソース クラスタから次のコマンドを実行して反転した関係を解除します。

```
snapmirror break -source-path <SVM>: -destination-path <SVM>:
```



`-source-path`および`-destination-path`オプションでは、SVM名の後にコロン（:）を入力する必要があります。以下の例をご覧ください。

次の例では、データの提供元である元のデスティネーション SVM `svm\_backup`と元のソース SVM `svm1`の関係を解除します：

```
cluster_src::> snapmirror break -source-path svm_backup:
-destination-path svm1:
```

`snapmirror break`の詳細については、link:<https://docs.netapp.com/us-en/ontap-cli/snapmirror-break.html>["ONTAPコマンド リファレンス"]を参照してください。

8. 元のソースSVMを停止していた場合は、元のソース クラスタから元のソースSVMを起動します。

```
vserver start -vserver <SVM>
```

次の例は、元のソースSVMを起動します。

```
cluster_src::> vserver start svm1
```

9. 元のデスティネーションSVMまたはデスティネーション クラスタから、元のデータ保護関係を再確立します。

```
snapmirror resync -source-path <SVM>: -destination-path <SVM>:
```



`-source-path`および`-destination-path`オプションでは、SVM名の後にコロン（:）を入力する必要があります。以下の例をご覧ください。

次の例では、元のソース SVM `svm1`と元のデスティネーション SVM `svm\_backup`の関係を再確立します：

```
cluster_dst::> snapmirror resync -source-path svm1: -destination  
-path svm_backup:
```

10. 元のソースSVMまたはソース クラスタから次のコマンドを実行して、反転したデータ保護関係を削除します。

```
snapmirror delete -source-path <SVM>: -destination-path <SVM>:
```



`-source-path`および`-destination-path`オプションでは、SVM名の後にコロン（:）を入力する必要があります。以下の例をご覧ください。

次の例では、元のデスティネーション SVM `svm\_backup`と元のソース SVM `svm1`間の逆の関係を削除します：

```
cluster_src::> snapmirror delete -source-path svm_backup:  
-destination-path svm1:
```

11. 元のデスティネーションSVMまたはデスティネーション クラスタから、反転したデータ保護関係をリリースします。

```
snapmirror release -source-path <SVM>: -destination-path <SVM>:
```



`-source-path`および`-destination-path`オプションでは、SVM名の後にコロン（:）を入力する必要があります。以下の例をご覧ください。

次の例では、元のデスティネーション SVM である svm_backup と元のソース SVM 間の逆の関係を

解除します。 svm1

```
cluster_dst::> snapmirror release -source-path svm_backup:  
-destination-path svm1:
```

次の手順

- `snapmirror show` コマンドを使用して、SnapMirror関係が作成されたことを確認します。

`snapmirror show`の詳細については、link:<https://docs.netapp.com/us-en/ontap-cli/snapmirror-show.html> ["ONTAPコマンド リファレンス"]を参照してください。

- クライアントから元のソース SVM への書き込み操作を再開します。

関連情報

- ["snapmirror create"](#)
- ["snapmirror delete"](#)
- ["snapmirror initialize"](#)
- ["snapmirror quiesce"](#)
- ["snapmirror release"](#)
- ["snapmirror resync"](#)

元の ONTAP SnapMirror ソース SVM を FlexGroup ボリューム用に再アクティブ化する

デスティネーションからデータを提供する必要がなくなった場合は、ソースSVMとデスティネーションSVMの間に元のデータ保護関係を再確立できます。FlexGroupボリュームを使用している場合に元のソースSVMを再アクティブ化するには、いくつか追加手順を実行する必要があります。まず、元のSVM DR関係を削除し、元の関係をリリースしてから関係を反転する必要があります。また、スケジュールされた転送を停止する前に、反転した関係をリリースし、元の関係を再作成する必要もあります。

手順

1. 元のデスティネーションSVMまたはデスティネーション クラスタから、元のSVM DR関係を削除します。

```
snapmirror delete -source-path SVM: -destination-path SVM:
```



`-source-path`および`-destination-path`オプションでは、SVM名の後にコロン（:）を入力する必要があります。以下の例をご覧ください。

次の例では、元のソース SVM svm1 と元のデスティネーション SVM 間の元の関係を削除します。
svm_backup:

```
cluster_dst:> snapmirror delete -source-path svm1: -destination-path  
svm_backup:
```

2. 元のソース SVM または元のソース クラスタから、Snapshot をそのまま維持したまま元の関係を解除します。

```
snapmirror release -source-path SVM: -destination-path SVM: -relationship-info  
-only true
```



`-source-path`および `-destination-path`オプションでは、SVM名の後にコロン（:）を入力する必要があります。以下の例をご覧ください。

次の例では、元のソース SVM である svm1 と元のデスティネーション SVM `svm\_backup`間の元の関係を解除します。

```
cluster_src:> snapmirror release -source-path svm1: -destination-path  
svm_backup: -relationship-info-only true
```

3. 元のソースSVMまたはソース クラスタから、元のSVM DR関係と同じ設定、ポリシー、およびidentity-preserve設定を使用して、反転したSVM DR関係を作成します。

```
snapmirror create -source-path SVM: -destination-path SVM:
```



`-source-path`および `-destination-path`オプションでは、SVM名の後にコロン（:）を入力する必要があります。以下の例をご覧ください。

次の例では、データの提供元となる SVM `svm\_backup`と元のソース SVM `svm1`の間に関係を作成します：

```
cluster_src:> snapmirror create -source-path svm_backup: -destination  
-path svm1:
```

4. 元のソースSVMまたはソース クラスタから次のコマンドを実行して、データ保護関係を反転します。

```
snapmirror resync -source-path SVM: -destination-path SVM:
```



`-source-path`および `-destination-path`オプションでは、SVM名の後にコロン（:）を入力する必要があります。以下の例をご覧ください。

再同期の際にベースライン転送は不要ですが、再同期には時間がかかる場合があります。再同期はオフピ

ークの時間帯に実行することを推奨します。



ソースとデスティネーションに共通の Snapshot が存在しない場合、コマンドは失敗します。`snapmirror initialize`を使用して関係を再初期化します。

次の例では、元のソース SVM `svm1`とデータの提供元となる SVM `svm\_backup`の関係を反転します：

```
cluster_src::> snapmirror resync -source-path svm_backup: -destination  
-path svm1:
```

5. 元のソースSVMへのデータ アクセスを再確立する準備ができれば、元のデスティネーションSVMを停止してSVMに接続されているクライアントをすべて切断します。

```
vserver stop -vserver SVM
```

次の例は、現在データを提供している元のデスティネーションSVMを停止します。

```
cluster_dst::> vserver stop svm_backup
```

6. `vserver show`コマンドを使用して、元のデスティネーション SVM が停止状態になっていることを確認します。

```
cluster_dst::> vserver show
```

Vserver	Type	Subtype	Admin State	Operational State	Root Volume
Aggregate					
-----	-----	-----	-----	-----	-----
svm_backup aggr1	data	default	stopped	stopped	rv

7. 元のソースSVMまたはソース クラスタから次のコマンドを実行して反転した関係を最後にもう一度更新し、元のデスティネーションSVMから元のソースSVMにすべての変更を転送します。

```
snapmirror update -source-path SVM: -destination-path SVM:
```



`-source-path`および `-destination-path`オプションでは、SVM名の後にコロン（:）を入力する必要があります。以下の例をご覧ください。

次の例では、データの提供元である元のデスティネーション SVM、`svm\_backup`と元のソース SVM `svm1`の関係を更新します：

```
cluster_src::> snapmirror update -source-path svm_backup: -destination  
-path svm1:
```

`snapmirror update`の詳細については、[link:https://docs.netapp.com/us-en/ontap-cli/snapmirror-update.html](https://docs.netapp.com/us-en/ontap-cli/snapmirror-update.html)["ONTAPコマンド リファレンス"]をご覧ください。

8. 元のソースSVMまたはソース クラスタから次のコマンドを実行して、反転した関係のスケジュールされた転送を停止します。

```
snapmirror quiesce -source-path SVM: -destination-path SVM:
```



`-source-path`および `-destination-path`オプションでは、SVM名の後にコロン（:）を入力する必要があります。以下の例をご覧ください。

次の例では、データの提供元である SVM `svm\_backup`と元の SVM `svm1`の間のスケジュールされた転送を停止します：

```
cluster_src::> snapmirror quiesce -source-path svm_backup: -destination  
-path svm1:
```

`snapmirror quiesce`の詳細については、[link:https://docs.netapp.com/us-en/ontap-cli/snapmirror-quiesce.html](https://docs.netapp.com/us-en/ontap-cli/snapmirror-quiesce.html)["ONTAPコマンド リファレンス"]を参照してください。

9. 最後の更新が完了して関係のステータスが「Quiesced」になったら、元のソースSVMまたは元のソース クラスタから次のコマンドを実行して反転した関係を解除します。

```
snapmirror break -source-path SVM: -destination-path SVM:
```



`-source-path`および `-destination-path`オプションでは、SVM名の後にコロン（:）を入力する必要があります。以下の例をご覧ください。

次の例では、データの提供元である元のデスティネーション SVM `svm\_backup`と元のソース SVM `svm1`の関係を解除します：

```
cluster_src::> snapmirror break -source-path svm_backup: -destination  
-path svm1:
```

`snapmirror break`の詳細については、[link:https://docs.netapp.com/us-en/ontap-cli/snapmirror-break.html](https://docs.netapp.com/us-en/ontap-cli/snapmirror-break.html)["ONTAPコマンド リファレンス"]を参照してください。

10. 元のソースSVMを停止していた場合は、元のソース クラスタから元のソースSVMを起動します。

```
vserver start -vserver SVM
```

次の例は、元のソースSVMを起動します。

```
cluster_src::> vserver start svm1
```

11. 元のソースSVMまたはソース クラスタから、反転したSVM DR関係を削除します。

```
snapmirror delete -source-path SVM: -destination-path SVM:
```



`-source-path`および `-destination-path`オプションでは、SVM名の後にコロン（:）を入力する必要があります。以下の例をご覧ください。

次の例では、元のデスティネーション SVM である svm_backup と元のソース SVM `svm1`間の逆の関係を削除します：

```
cluster_src::> snapmirror delete -source-path svm_backup: -destination-path svm1:
```

12. 元のデスティネーション SVM または元のデスティネーション クラスタから、スナップショットをそのまま維持したまま、逆の関係を解除します：

```
snapmirror release -source-path SVM: -destination-path SVM: -relationship-info-only true
```



`-source-path`および `-destination-path`オプションでは、SVM名の後にコロン（:）を入力する必要があります。以下の例をご覧ください。

次の例は、元のデスティネーションSVM svm_backupと元のソースSVM svm1の間の反転した関係をリリースします。

```
cluster_dst::> snapmirror release -source-path svm_backup: -destination-path svm1: -relationship-info-only true
```


13. 元のデスティネーションSVMまたはデスティネーション クラスタから、元の関係を再作成します。元のSVM DR関係と同じ設定、ポリシー、およびidentity-preserve設定を使用します。

```
snapmirror create -source-path SVM: -destination-path SVM:
```



`-source-path`および `-destination-path`オプションでは、SVM名の後にコロン（:）を入力する必要があります。以下の例をご覧ください。

次の例では、元のソース SVM `svm1`と元のデスティネーション SVM `svm\_backup`の間に関係を作成します。

```
cluster_dst::> snapmirror create -source-path svm1: -destination-path  
svm_backup:
```

14. 元のデスティネーションSVMまたはデスティネーション クラスタから、元のデータ保護関係を再確立します。

```
snapmirror resync -source-path SVM: -destination-path SVM:
```



`-source-path`および `-destination-path`オプションでは、SVM名の後にコロン（:）を入力する必要があります。以下の例をご覧ください。

次の例では、元のソース SVM `svm1`と元のデスティネーション SVM `svm\_backup`の関係を再確立します：

```
cluster_dst::> snapmirror resync -source-path svm1: -destination-path  
svm_backup:
```

関連情報

- ["snapmirror create"](#)
- ["snapmirror delete"](#)
- ["snapmirror initialize"](#)
- ["snapmirror quiesce"](#)
- ["snapmirror release"](#)
- ["snapmirror resync"](#)

ONTAP SnapMirrorデスティネーションSVM上のデータを再同期する

ONTAP 9.11.1では、ディザスタ リカバリのリハーサル時にデータ ウェアハウスの完全な再構築を省略するオプションが追加され、迅速に本番環境に戻れるようになりました。

ONTAP 9.8以降では、System Managerを使用して、保護関係が解除されているソースStorage VMからデスティネーションStorage VMにデータおよび設定の詳細を再同期して、関係を再確立できます。

再同期処理は元の関係のデスティネーションからのみ実行できます。再同期を実行すると、ソースStorage VMのデータよりも新しいデスティネーションStorage VMのデータは削除されます。

手順

System ManagerまたはONTAP CLIを使用して、このタスクを実行できます。

System Manager

1. デスティネーションから、目的の保護関係を選択します。**Protection > Relationships** をクリックします。
2. オプションで、災害復旧リハーサル中に完全なデータ ウェアハウスの再構築を回避するには、*クイック再同期を実行*を選択します。
3.  をクリックし、*再同期*をクリックします。
4. *関係*の下で、関係の*転送ステータス*を表示して再同期の進行状況を監視します。

CLI

1. デスティネーション クラスタから、関係を再同期します。

```
snapmirror resync -source-path <svm>: -destination-path <svm>:  
-quick-resync true|false
```

関連情報

- ["snapmirror resync"](#)

ONTAP SnapMirrorボリュームDR関係をSVM DR関係に変換する

ソース上の各ボリューム（ルート ボリュームを除く）がレプリケート対象であり、ソース上の各ボリューム（ルート ボリュームを含む）の名前がデスティネーション上のボリュームと同じである場合は、ボリューム間のレプリケーション関係を、そのボリュームを所有するStorage Virtual Machine（SVM）間のレプリケーション関係に変換できます。

タスク概要

SnapMirror関係がアイドル状態のときに `volume rename` コマンドを使用して、必要に応じてデスティネーション ボリュームの名前を変更します。["ONTAPコマンド リファレンス"](#)の `volume rename` の詳細を確認してください。

手順

1. デスティネーションSVMまたはデスティネーション クラスタから次のコマンドを実行して、ソースとデスティネーションのボリュームを再同期します。

```
snapmirror resync -source-path <SVM:volume> -destination-path <SVM:volume>
```

```
-type DP|XDP -policy <policy>
```

`snapmirror resync`の詳細については、link:<https://docs.netapp.com/us-en/ontap-cli/snapmirror-resync.html>["ONTAPコマンド リファレンス"]を参照してください。



再同期の際にベースライン転送は不要ですが、再同期には時間がかかる場合があります。再同期はオフピークの時間帯に実行することを推奨します。

次の例では、`svm1`のソース ボリューム `volA`と `svm\_backup`のデスティネーション ボリューム `volA`間の関係を再同期します：

```
cluster_dst::> snapmirror resync -source-path svm1:volA -destination  
-path svm_backup:volA
```

2. "SVMの設定のレプリケート"の説明に従って、ソース SVM とデスティネーション SVM の間に SVM レプリケーション関係を作成します。

レプリケーション関係を作成するときは、`snapmirror create`コマンドの`-identity-preserve true`オプションを使用する必要があります。

`snapmirror create`の詳細については、link:<https://docs.netapp.com/us-en/ontap-cli/snapmirror-create.html>["ONTAPコマンド リファレンス"]を参照してください。

3. デスティネーションSVMを停止します。

```
vserver stop -vserver SVM
```

`vserver stop`の詳細については、link:<https://docs.netapp.com/us-en/ontap-cli/vserver-stop.html>["ONTAPコマンド リファレンス"]を参照してください。

次の例では、デスティネーション SVM を停止します svm_backup：

```
cluster_dst::> vserver stop svm_backup
```

4. デスティネーションSVMまたはデスティネーション クラスタから次のコマンドを実行して、ソースとデスティネーションのSVMを再同期します。

```
snapmirror resync -source-path <SVM>: -destination-path <SVM>: -type DP|XDP  
-policy <policy>
```



`-source-path`および`-destination-path`オプションでは、SVM名の後にコロン（:）を入力する必要があります。以下の例をご覧ください。

再同期の際にベースライン転送は不要ですが、再同期には時間がかかる場合があります。再同期はオフピークの時間帯に実行することを推奨します。

次の例では、ソース SVM `svm1`とデスティネーション SVM `svm\_backup`間の関係を再同期します：

```
cluster_dst:> snapmirror resync -source-path svm1: -destination-path  
svm_backup:
```

関連情報

- ["snapmirror create"](#)
- ["snapmirror resync"](#)

ONTAP SnapMirror SVMレプリケーション関係を削除する

`snapmirror delete`コマンドと`snapmirror release`コマンドを使用して、SVMレプリケーション関係を削除できます。その後、不要なデスティネーションボリュームを手動で削除できます。この手順で説明されているコマンドの詳細については、[link:https://docs.netapp.com/us-en/ontap-cli/](https://docs.netapp.com/us-en/ontap-cli/)["ONTAPコマンド リファレンス"]を参照してください。

タスク概要

`snapmirror release`コマンドは、ソースからSnapMirrorで作成されたスナップショットをすべて削除します。`-relationship-info-only`オプションを使用して、スナップショットを保持できます。

手順

1. デスティネーションSVMまたはデスティネーション クラスタから次のコマンドを実行して、レプリケーション関係を解除します。

```
snapmirror break -source-path SVM: -destination-path SVM:
```



`-source-path`および`-destination-path`オプションでは、SVM名の後にコロン（:）を入力する必要があります。以下の例をご覧ください。

次の例では、ソース SVM `svm1`とデスティネーション SVM `svm\_backup`間の関係を解除します：

```
cluster_dst::> snapmirror break -source-path svm1: -destination-path  
svm_backup:
```

`snapmirror break`の詳細については、[link:https://docs.netapp.com/us-en/ontap-cli/snapmirror-break.html](https://docs.netapp.com/us-en/ontap-cli/snapmirror-break.html)["ONTAPコマンド リファレンス"]を参照してください。

2. デスティネーション SVM またはデスティネーション クラスタから次のコマンドを実行して、レプリケーション関係を削除します：

```
snapmirror delete -source-path SVM: -destination-path SVM:
```



`-source-path`および `-destination-path`オプションでは、SVM名の後にコロン（:）を入力する必要があります。以下の例をご覧ください。

次の例では、ソース SVM `svm1`とデスティネーション SVM `svm\_backup`間の関係を削除します：

```
cluster_dst::> snapmirror delete -source-path svm1: -destination-path  
svm_backup:
```

`snapmirror delete`の詳細については、[link:https://docs.netapp.com/us-en/ontap-cli/snapmirror-delete.html](https://docs.netapp.com/us-en/ontap-cli/snapmirror-delete.html)["ONTAPコマンド リファレンス"]をご覧ください。

3. ソース クラスタまたはソース SVM から次のコマンドを実行して、ソース SVM からレプリケーション関係情報を解放します：

```
snapmirror release -source-path SVM: -destination-path SVM:
```



`-source-path`および `-destination-path`オプションでは、SVM名の後にコロン（:）を入力する必要があります。以下の例をご覧ください。

次の例では、指定されたレプリケーション関係の情報をソース SVM `svm1`から解放します：

```
cluster_src::> snapmirror release -source-path svm1: -destination-path  
svm_backup:
```

`snapmirror release`の詳細については、[link:https://docs.netapp.com/us-en/ontap-cli/snapmirror-release.html](https://docs.netapp.com/us-en/ontap-cli/snapmirror-release.html)["ONTAPコマンド リファレンス"]を参照してください。

SnapMirrorルート ボリューム レプリケーションの管理

ONTAP SnapMirrorルート ボリュームのレプリケーションについて学ぶ

NAS環境内のすべてのSVMには、固有の名前空間があります。オペレーティング システムと関連情報を含むSVMの_ルート ボリューム_は、名前空間階層へのエントリ ポイントです。ノードの停止やフェイルオーバーが発生した場合でもクライアントがデータにアクセスできるようにするには、SVMルート ボリュームの負荷共有ミラー コピーを作成する必要があります。

SVMルート ボリュームの負荷共有ミラーの主な目的は、負荷共有ではなく、ディザスタ リカバリにあります。

- ルート ボリュームが一時的に使用できない場合、負荷共有ミラーはルート ボリューム データへの読み取り専用アクセスを自動的に提供します。
- ルート ボリュームが永続的に使用できない場合は、負荷共有ボリュームの 1 つを昇格させて、ルート ボリューム データへの書き込みアクセスを提供できます。

ONTAP負荷共有ミラー関係の作成と初期化

クラスタ内のNASデータを提供するSVMルートボリュームごとに、負荷共有ミラー (LSM) を作成する必要があります。2つ以上のHAペアで構成されるクラスタでは、HAペアの両方のノードに障害が発生した場合でも、クライアントがネームスペースにアクセスできるようにするために、SVMルートボリュームの負荷共有ミラーを検討する必要があります。負荷共有ミラーは、単一のHAペアで構成されるクラスタには適していません。

開始する前に

ONTAP 9.16.1以降では、負荷共有ミラー関係を作成するときに、デスティネーションSVMでストレージ制限を有効にすることはできません。

タスク概要

同じノードにLSMを作成した場合、ノードで障害が発生すると単一点障害となり、クライアントにデータを提供する2つ目のコピーは存在しません。一方、ルート ボリュームを含まないノードや別のHAペアにLSMを作成すると、障害が発生してもデータに引き続きアクセスできます。

たとえば、4ノード クラスタの3つのノードにルート ボリュームがある場合、次のようになります。

- HA 1のノード1のルート ボリュームについて、HA 2のノード1またはHA 2のノード2にLSMを作成します。
- HA 1のノード2のルート ボリュームについて、HA 2のノード1またはHA 2のノード2にLSMを作成しま

す。

- HA 2のノード1のルート ボリュームについて、HA 1のノード1またはHA 1のノード2にLSMを作成します。

手順

1. LSMのデスティネーション ボリュームを作成します。

```
volume create -vserver <SVM> -volume <volume> -aggregate <aggregate>
-type DP -size <size>
```

デスティネーション ボリュームのサイズは、ルート ボリュームと同じかそれ以上である必要があります。

ルート ボリュームと宛先ボリュームの名前には、`\_root`や`\_m1`などのサフィックスを付けるのがベスト プラクティスです。

`volume create`の詳細については、[link:https://docs.netapp.com/us-en/ontap-cli/volume-create.html](https://docs.netapp.com/us-en/ontap-cli/volume-create.html)["ONTAPコマンド リファレンス"]を参照してください。

次の例では、`cluster\_src`のルート ボリューム `svm1\_root`の負荷共有ミラー ボリュームを作成します：

```
cluster_src:> volume create -vserver svm1 -volume svm1_m1 -aggregate
aggr_1 -size 1gb -state online -type DP
```

2. "レプリケーション ジョブ スケジュールを作成する"。
3. SVMルート ボリュームとLSMのデスティネーション ボリュームの間に負荷共有ミラー関係を作成します。

```
snapmirror create -source-path <SVM:volume> -destination-path
<SVM:volume> -type LS -schedule <schedule>
```

次の例では、ルート ボリューム `svm1\_root`と負荷共有ミラー ボリューム `svm1\_m1`の間に負荷共有ミラー関係を作成します：

```
cluster_src::> snapmirror create -source-path svm1:svm1_root
-destination-path svm1:svm1_m1 -type LS -schedule hourly
```

負荷共有ミラーのタイプ属性が`DP`から`LS`に変更されます。

`snapmirror create`の詳細については、link:<https://docs.netapp.com/us-en/ontap-cli/snapmirror-create.html>["ONTAPコマンド リファレンス"]を参照してください。

4. 負荷共有ミラーを初期化します。

```
snapmirror initialize-ls-set -source-path <SVM:volume>
```

次の例では、ルート ボリュームの負荷共有ミラーを初期化します `svm1_root` :

```
cluster_src::> snapmirror initialize-ls-set -source-path svm1:svm1_root
```

`snapmirror initialize`の詳細については、link:<https://docs.netapp.com/us-en/ontap-cli/snapmirror-initialize.html>["ONTAPコマンド リファレンス"]を参照してください。

ONTAP負荷共有ミラー関係を更新する

SVMルートボリュームの負荷共有ミラー (LSM) 関係は、SVM内のボリュームがマウントまたはアンマウントされた後、および `junction-path` オプションを含む `volume create` 操作中に自動的に更新されます。次のスケジュールされた更新の前にLSM関係を更新したい場合は、手動で更新できます。

負荷共有ミラー関係は次の場合に自動で更新されます。

- スケジュールされた更新時
- SVMルート ボリューム内のボリュームに対してマウントまたはアンマウント処理が実行されたとき
- `volume create` オプションを含む `junction-path` コマンドが発行される

`volume create`の詳細については、link:<https://docs.netapp.com/us-en/ontap-cli/volume-create.html>["ONTAPコマンド リファレンス"]を参照してください。

手順

1. 負荷共有ミラー関係を手動で更新します。

このコマンドを実行する前に、山カッコ内の変数を必要な値に置き換える必要があります。

```
snapmirror update-ls-set -source-path <SVM:volume>
```


次の例では、ルート ボリューム `svm1\_root` の負荷共有ミラー関係を更新します：

```
cluster_src::> snapmirror update-ls-set -source-path svm1:svm1_root
```

`snapmirror update`の詳細については、[link:https://docs.netapp.com/us-en/ontap-cli/snapmirror-update.html](https://docs.netapp.com/us-en/ontap-cli/snapmirror-update.html)["ONTAPコマンド リファレンス"]をご覧ください。

ONTAP負荷共有ミラーを昇格する

ルート ボリュームが完全に使用できなくなった場合は、負荷共有ミラー（LSM）ボリュームを昇格して、ルート ボリュームのデータへの書き込みアクセスを提供できます。

開始する前に

このタスクを実行するには、advanced権限レベルのコマンドを使用する必要があります。

手順

1. advanced権限レベルに切り替えます。

```
set -privilege advanced
```

2. LSMボリュームを昇格します。

このコマンドを実行する前に、山カッコ内の変数を必要な値に置き換える必要があります。

```
snapmirror promote -destination-path <SVM:volume>
```

次の例では、ボリューム `svm1\_m2` を新しいSVMルート ボリュームとして昇格します：

```
cluster_src::*> snapmirror promote -destination-path svm1:svm1_m2

Warning: Promote will delete the offline read-write volume
cluster_src://svm1/svm1_root and replace it with
cluster_src://svm1/svm1_m2. Because the volume is offline,
it is not possible to determine whether this promote will
affect other relationships associated with this source.
Do you want to continue? {y|n}: y
```

と入力します y。ONTAPは、LSMボリュームを読み取り / 書き込みボリュームにし、元のルート ボリュームにアクセスできる場合はそれを削除します。



最後の更新が最近行われていない場合は、昇格されたルート ボリュームに元のルート ボリュームのデータがすべて含まれているとは限りません。

`snapmirror promote`の詳細については、[link:https://docs.netapp.com/us-en/ontap-cli/snapmirror-promote.html](https://docs.netapp.com/us-en/ontap-cli/snapmirror-promote.html)["ONTAPコマンド リファレンス"]を参照してください。

3. admin権限レベルに戻ります。

```
set -privilege admin
```

4. ルート ボリュームに使用した命名規則に従って、昇格されたボリュームの名前を変更します。

このコマンドを実行する前に、山カッコ内の変数を必要な値に置き換える必要があります。

```
volume rename -vserver <SVM> -volume <volume> -newname <new_name>
```

次の例では、昇格されたボリューム `svm1\_m2` の名前を `svm1\_root` に変更します：

```
cluster_src::> volume rename -vserver svm11 -volume svm1_m2 -newname  
svm1_root
```

5. "負荷共有ミラー関係の作成および初期化"の手順3から手順4の説明に従って、名前を変更したルート ボリュームを保護します。

クラウドへのバックアップ

ONTAP SnapMirrorクラウドライセンスをインストールする

SnapMirrorクラウド関係は、事前に認定された他社製バックアップ アプリケーションを使用してオーケストレーションできます。ONTAP 9.9.1以降では、SnapMirrorクラウドレプリケーションのオーケストレーションにSystem Managerを使用することもできます。System Managerを使用して、オンプレミスのONTAPからオブジェクト ストレージへのバックアップをオーケストレーションする場合は、SnapMirrorとSnapMirrorクラウドの両方の容量ライセンスが必要です。また、SnapMirrorクラウドAPIライセンスをリクエストしてインストールする必要もあります。

タスク概要

SnapMirror クラウドライセンスと SnapMirror S3 ライセンスはノードライセンスではなくクラスタライセンスであるため、ONTAP One ライセンスバンドルには含まれていません。これらのライセンスは、別途ONTAP One Compatibility バンドルに含まれています。SnapMirror クラウドを有効にするには、このバンドルをリクエストする必要があります。

また、System Managerでオブジェクト ストレージへのSnapMirrorクラウド バックアップをオーケストレーションするには、SnapMirrorクラウドAPIキーが必要です。このAPIライセンスはシングルインスタンスのクラスタ単位ライセンスであり、クラスタ内のすべてのノードにインストールする必要はありません。

手順

ONTAP One CompatibilityバンドルとSnapMirrorクラウドAPIライセンスをリクエストしてダウンロードし、System Managerを使用してインストールする必要があります。

1. ライセンスを付与するクラスタのクラスタUUIDを見つけて記録します。

クラスタ用のONTAP One Compatibilityバンドルを注文するためのリクエストを送信する際に、クラスタUUIDが必要です。

2. NetApp営業チームに連絡して、ONTAP One Compatibilityバンドルをリクエストします。
3. NetAppサポート サイトに記載されている手順に従って、SnapMirrorクラウドAPIライセンスをリクエストします。

"SnapMirrorクラウドAPIライセンスキーをリクエストする"

4. ライセンス ファイルを受け取ってダウンロードしたら、System Managerを使用して、ONTAP Cloud Compatibility NLFとSnapMirrorクラウドAPI NLFをクラスタにアップロードします。
 - a. *[クラスタ] > [設定]*をクリックします。
 - b. *設定*ウィンドウで、*ライセンス*をクリックします。
 - c. ライセンス ウィンドウで、**+ Add** をクリックします。
 - d. [ライセンスの追加] ダイアログ ボックスで、[参照] をクリックしてダウンロードした NLF を選択し、[追加] をクリックしてファイルをクラスタにアップロードします。

関連情報

["SnapMirrorを使用したクラウドへのデータのバックアップ"](#)

["NetApp Software License Search"](#)

ONTAP SnapMirrorを使用してクラウドにデータをバックアップ

ONTAP 9.9.1以降では、System Managerを使用して、クラウドにデータをバックアップし、クラウド ストレージから別のボリュームにデータをリストアできます。StorageGRIDまたはONTAP S3をクラウド オブジェクト ストアとして使用できます。

ONTAP 9.18.1以降：

- SnapMirror cloudは、既存の["ONTAP REST API"](#)を使用して、MetroCluster構成上のFlexGroupボリュームのバックアップおよびリストア操作をサポートします。この機能により、スイッチオーバーおよびスイッチバック後にパートナーサイトから管理されるMetroCluster構成上のFlexGroupボリュームに対してSnapMirror cloudリレーションシップを作成できます。

ONTAP 9.16.1以降：

- SnapMirrorクラウドバックアップはファンアウト関係をサポートしています。つまり、SnapMirrorバック

アップを2つの異なるオブジェクトストアに同時に作成できます。ONTAP 9.16.1では、SnapMirrorクラウドは2つのファンアウト関係をサポートします。ファンアウトは、2つのオブジェクトストア、または2つの異なるオブジェクトストア内の1つまたは2つのバケットに作成できます。2つ以上のファンアウト関係を作成しようとすると失敗します。

- SnapMirrorクラウドは、既存の["ONTAP REST API"](#)を使用したより効率的な同期プロセスを使用して、クラウドに移行されたボリュームのバックアップをサポートします。この機能は、再ベースライン操作を実行することなく、クラウドに移行されたボリュームから同じ宛先オブジェクトストアエンドポイントへのSnapMirrorクラウドバックアップをサポートします。FlexVolとFlexGroupの両方のボリュームがサポートされています。

SnapMirror クラウド機能を使用する前に、NetApp Support Site から SnapMirror クラウド API ライセンス キーをリクエストする必要があります：["SnapMirrorクラウドAPIライセンスキーをリクエストする"](#)。指示に従い、ビジネス機会の簡単な説明を提供し、指定されたメールアドレスにメールを送信して API キーをリクエストしてください。24時間以内に、API キーの取得方法に関する追加の指示が記載されたメールの返信を受け取るはずです。

クラウド オブジェクト ストアの追加

SnapMirrorクラウド バックアップを設定する前に、StorageGRIDまたはONTAP S3クラウド オブジェクト ストアを追加する必要があります。

手順

1. **Protection > Overview > Cloud Object Stores** をクリックします。
2. **+ Add** をクリックします。

デフォルト ポリシーを使用したバックアップ

デフォルトのクラウド保護ポリシーDailyBackupを使用すると、既存のボリュームにSnapMirrorクラウド バックアップを簡単に設定できます。

手順

1. **保護 > 概要** をクリックし、ボリュームをクラウドにバックアップ を選択します。
2. 初めてクラウドにバックアップする場合は、表示されるライセンス フィールドにSnapMirrorクラウドAPI ライセンス キーを入力します。
3. ***認証して続行*** をクリックします。
4. **ソース ボリューム** を選択します。
5. **クラウド オブジェクト ストア** を選択します。
6. ***保存*** をクリックします。

カスタムのクラウド バックアップ ポリシーの作成

SnapMirrorクラウド バックアップにデフォルトのDailyBackupクラウド ポリシーを使用しない場合は、独自のポリシーを作成できます。

手順

1. **保護 > 概要 > ローカル ポリシー設定** をクリックし、**保護ポリシー** を選択します。
2. ***Add*** をクリックし、新しいポリシーの詳細を入力します。

3. ポリシー タイプ セクションで、クラウドにバックアップ を選択して、クラウド ポリシーを作成していることを示します。
4. *保存*をクリックします。

*ボリューム*ページからバックアップを作成します

複数のボリュームのクラウド バックアップを一度に選択して作成する場合、またはカスタム保護ポリシーを使用する場合は、System Managerの*Volumes*ページを使用できます。

手順

1. *[ストレージ]>[ボリューム]*をクリックします。
2. クラウドにバックアップするボリュームを選択し、*保護*をクリックします。
3. *ボリュームの保護*ウィンドウで、*その他のオプション*をクリックします。
4. ポリシーを選択します。

デフォルトのDailyBackupポリシー、または作成したカスタム クラウド ポリシーを選択できます。

5. クラウド オブジェクト ストアを選択します。
6. *保存*をクリックします。

クラウドからのリストア

System Managerを使用して、バックアップしたデータをクラウド ストレージからソース クラスタ上の別のボリュームにリストアできます。



ONTAP 9.16.1以降を使用していて、SnapMirrorクラウド単一ファイルリストアをFlexGroupボリュームに対して実行する場合は、FlexGroupボリューム内の新しいディレクトリにのみファイルをリストアし、デスティネーションFlexGroupボリュームで粒度データを`advanced`に設定する必要があります。`-granular-data advanced` オプションの設定の詳細については、"[ファイルデータの再分配によるONTAP FlexGroupボリュームのバランシング](#)"を参照してください。

手順

1. SnapMirror-to-Cloud関係のソースクラスタから、*ストレージ> ボリューム*をクリックします。
2. リストアするボリュームを選択します。
3. *クラウドにバックアップ*タブを選択します。
4. 復元するソースボリュームの横にある  をクリックしてメニューを表示し、*復元*を選択します。
5. ソース でストレージ VM を選択し、データをリストアするボリュームの名前を入力します。
6. *Destination*で、リストアするSnapshotを選択します。
7. *保存*をクリックします。

SnapMirrorクラウド関係の削除

System Managerを使用してクラウド関係を削除できます。

手順

1. **Storage > Volumes** をクリックし、削除するボリュームを選択します。
2. ソースボリュームの横にある  をクリックし、*削除*を選択します。
3. クラウド オブジェクト ストア エンドポイントを削除する場合は、**Delete the cloud object store endpoint (optional)** を選択します。
4. *削除*をクリックします。

クラウド オブジェクト ストアの削除

クラウド バックアップ関係に含まれていないクラウド オブジェクト ストアは、System Managerを使用して削除できます。クラウド オブジェクト ストアがクラウド バックアップ関係の一部である場合は削除できません。

手順

1. **Protection > Overview > Cloud Object Stores** をクリックします。
2. 削除するオブジェクト ストアを選択し、 をクリックして*削除*を選択します。

NetApp Backup and Recoveryを使用してデータをバックアップする

ONTAP 9.9.1 以降では、System Manager を使用して、NetApp Backup and Recovery サービスでクラウドにデータをバックアップできます。

バックアップとリカバリはFlexVol読み取り/書き込みボリュームとデータ保護（DP）ボリュームをサポートします。ONTAP 9.12.1以降では、バックアップとリカバリはFlexGroupボリュームとSnapLockボリュームをサポートします。

["NetApp Backup and Recovery"](#)についての詳細をご覧ください。

開始する前に

NetApp Consoleでアカウントを作成するには、次の手順を実行してください。サービスアカウントの場合、ロールを「Account Admin」として作成する必要があります。（他のサービスアカウントロールには、System Managerから接続を確立するために必要な権限がありません。）

1. ["NetApp Consoleでアカウントを作成する"](#)。
2. ["NetApp ConsoleでConsoleエージェントを作成する"](#)次のいずれかのクラウド プロバイダを使用：
 - Microsoft Azure
 - Amazon Web Services (AWS)
 - Google Cloud Platform (GCP)
 - StorageGRID (ONTAP 9.10.1)



ONTAP 9.10.1以降では、StorageGRIDをクラウドバックアッププロバイダーとして選べますが、NetApp Consoleがオンプレミスで導入されている場合に限りです。Consoleエージェントはオンプレミスにインストールされ、NetApp ConsoleのSoftware-as-a-Service (SaaS) アプリケーションから利用できる必要があります。

3. ["NetApp ConsoleでNetApp Backup and Recoveryを購読する"](#)（適切なライセンスが必要です）。

4. "NetApp Consoleを使用してアクセスキーとシークレットキーを生成する"。

NetApp Consoleでクラスタを登録する

NetApp ConsoleまたはSystem Managerを使用して、クラスタをConsoleに登録できます。

手順

1. System Managerで、*Protection Overview*に移動します。
2. **NetApp Backup and Recovery** で、次の詳細を入力してください：
 - Client ID
 - クライアント シークレット キー
3. *登録して続行*を選択します。

NetApp Backup and Recoveryを有効にする

クラスタがNetApp Consoleに登録された後、NetApp Backup and Recoveryを有効にし、最初のバックアップをクラウドに開始する必要があります。

手順

1. System Managerで、*保護 > 概要*を選択し、*Cloud Backup Service*セクションまでスクロールします。
2. *クライアントID*と*クライアントシークレット*を入力します。



ONTAP 9.10.1 以降では、*クラウドの使用コストの詳細を確認する*を選択すると、クラウドの使用コストについて知ることができます。

3. *Cloud Backup Serviceに接続して有効化*を選択します。
4. *NetApp Backup and Recoveryを有効にする*ページで、選択したプロバイダに応じて次の詳細を入力します。

このクラウド プロバイダの場合...	次のデータを入力してください...
Azure	• AzureサブスクリプションID • リージョン • リソース グループ名（既存または新規）
AWS	• AWSアカウントID • アクセス キー • シークレット キー • リージョン

Google Cloud Project (GCP)	• Google Cloudプロジェクト名 • Google Cloudアクセス キー • Google Cloudシークレット キー • リージョン
StorageGRID (ONTAP 9.10.1以降、NetApp Consoleのオンプレミス展開のみ)	• サーバ • SGアクセス キー • SGシークレット キー

5. *保護ポリシー*を選択してください:

- 既存のポリシー：既存のポリシーを選択します。
- 新しいポリシー：名前を指定し、転送スケジュールを設定します。



ONTAP 9.10.1以降では、AzureまたはAWSによるアーカイブを有効にするかどうかを指定できます。



AzureまたはAWSによるボリュームのアーカイブを有効にした場合、アーカイブを無効にすることはできません。

AzureまたはAWSのアーカイブを有効にする場合は、次の情報を指定します。

- ボリュームをアーカイブするまでの日数。
- アーカイブに保持するバックアップの数。最新のバックアップまでアーカイブするには「0」（ゼロ）を指定します。
- AWSの場合は、アーカイブ ストレージ クラスを選択します。

6. バックアップするボリュームを選択します。

7. *保存*を選択します。

NetApp Backup and Recoveryに使用する保護ポリシーを編集します

NetApp Backup and Recoveryで使用する保護ポリシーを変更できます。

手順

1. System Managerで、*保護 > 概要*を選択し、*Cloud Backup Service*セクションまでスクロールします。
2. を選択し、*編集*を選択します。
3. *保護ポリシー*を選択してください:
 - 既存のポリシー：既存のポリシーを選択します。
 - 新しいポリシー：名前を指定し、転送スケジュールを設定します。



ONTAP 9.10.1以降では、AzureまたはAWSによるアーカイブを有効にするかどうかを指定できます。



AzureまたはAWSによるボリュームのアーカイブを有効にした場合、アーカイブを無効にすることはできません。

AzureまたはAWSのアーカイブを有効にする場合は、次の情報を指定します。

- ボリュームをアーカイブするまでの日数。
- アーカイブに保持するバックアップの数。最新のバックアップまでアーカイブするには「0」（ゼロ）を指定します。
- AWSの場合は、アーカイブ ストレージ クラスを選択します。

4. *保存*を選択します。

新しいボリュームまたはLUNのクラウドでの保護

新しいボリュームまたはLUNを作成する際にSnapMirror保護関係を確立すると、ボリュームまたはLUNをクラウドにバックアップできます。

開始する前に

- SnapMirrorライセンスが必要です。
- クラスタ間LIFが設定されている必要があります。
- NTPが設定されている必要があります。
- クラスタはONTAP 9.9.1以降を実行している必要があります。

タスク概要

次のクラスタ構成については、新しいボリュームやLUNをクラウドで保護することはできません。

- MetroCluster環境のクラスタ
- SVM-DR
- FlexGroup ボリュームは、NetApp Backup and Recovery を使用してバックアップすることはできません。

手順

1. ボリュームまたは LUN をプロビジョニングするときは、System Manager の 保護 ページで、**SnapMirror** を有効にする（ローカルまたはリモート） というチェックボックスをオンにします。
2. Backup and Recoveryポリシー タイプを選択します。
3. バックアップとリカバリが有効になっていない場合は、*NetApp Backup and Recoveryを使用してバックアップを有効にする*を選択します。

既存のボリュームまたはLUNのクラウドでの保護

既存のボリュームとLUNに対してSnapMirror保護関係を確立できます。

手順

1. 既存のボリュームまたは LUN を選択し、* 保護 * を選択します。
2. *ボリュームの保護*ページで、保護ポリシーに*NetApp Backup and Recoveryを使用したバックアップ*を指定します。

3. ***Protect***を選択します。
4. ***保護***ページで、***SnapMirror**を有効にする（ローカルまたはリモート）*****というラベルの付いたチェックボックスをオンにします。
5. ***Connect and enable NetApp Backup and Recovery***を選択します。

バックアップ ファイルからのデータのリストア

データの復元、リレーションシップの更新、リレーションシップの削除などのバックアップ管理操作は、NetApp Consoleを使用している場合にのみ実行できます。詳細については、["バックアップファイルからデータを復元する"](#)を参照してください。

SnapLockテクノロジーを使用したアーカイブとコンプライアンス

ONTAP SnapLockについて学ぶ

SnapLockは、規制やガバナンスに準拠するためにWORMストレージを使用して変更不可能な状態でファイルを保管する組織向けの、ハイパフォーマンスなコンプライアンスソリューションです。

データの削除、変更、名前変更を防止でき、SEC 17a-4 (f) 、HIPAA、FINRA、CFTC、GDPRなどの規制に準拠することができます。専用のボリュームを作成して、指定した保持期間または永久にファイルを消去および書き換え不可能な状態で保存およびコミットできます。SnapLockでは、CIFSやNFSなどの標準オープン ファイル プロトコルにより、ファイル レベルでこのようなデータ保持を実行できます。サポートされるオープン ファイル プロトコルは、NFS（バージョン2、3、4）とCIFS（SMB 1.0、2.0、3.0）です。

SnapLockを使用すると、ファイルとスナップショットをWORMストレージにコミットし、WORM保護されたデータの保持期間を設定できます。SnapLock WORMストレージはNetAppスナップショット技術を使用し、SnapMirrorレプリケーションとSnapVaultバックアップを基盤技術として活用することで、データのバックアップ・リカバリ保護を実現します。WORMストレージの詳細については、こちらをご覧ください：["NetApp SnapLockを使用した準拠のWORMストレージ - TR-4526"](#)

アプリケーションを使用してNFSまたはCIFS経由でファイルをWORM状態にコミットするか、SnapLock自動コミット機能を使用してファイルを自動的にWORM状態にコミットすることができます。ログ情報のように増分的に書き込まれるデータを保持するには、[_WORM追記可能ファイル](#)を使用できます。詳細については、["ボリューム アペンド モードを使用した追記可能WORMファイルの作成"](#)を参照してください。

SnapLockでサポートされるデータ保護方法は、ほとんどのコンプライアンス要件に対応します。

- セカンダリストレージ上のスナップショットをWORM保護するために、SnapLock for SnapVault を使用できます。["スナップショットをWORMにコミットする"](#)を参照してください。
- SnapMirrorを使用して、災害復旧のためにWORMファイルを別の地理的な場所に複製できます。["WORM ファイルのミラーリング"](#)を参照してください。

SnapLockは、ONTAPのライセンスベースの機能です。1つのライセンスで、SnapLockを、SEC Rule 17a-4(f)などの外部規制を満たす厳格なコンプライアンスモードと、デジタル資産の保護に関する社内規制を満たすより緩やかなエンタープライズモードで使用できます。SnapLockライセンスは、["ONTAP One"](#)ソフトウェアスイートの一部です。

SnapLockは、すべてのAFFおよびFASシステム、さらにONTAP Selectでサポートされています。SnapLockはソフトウェアのみのソリューションではなく、ハードウェアとソフトウェアが統合されたソリューションです。この違いは、SEC 17a-4 (f) のような統合されたハードウェアとソフトウェアのソリューションを要求する厳格なWORM規制にとって重要です。詳細については、["SECによる電子記憶媒体の使用に関するブローカー・ディーラー向けガイダンス"](#)を参照してください。

SnapLockの機能

SnapLockの設定が完了したら、次のタスクを実行できます。

- ["ファイルのWORM状態へのコミット"](#)
- ["セカンダリ ストレージのWORMにSnapshotをコミットする"](#)
- ["ディザスタ リカバリ用のWORMファイルのミラーリング"](#)
- ["リーガル ホールドを使用した訴訟期間中のWORMファイルの保持"](#)
- ["privileged delete機能を使用したWORMファイルの削除"](#)
- ["ファイルの保持期間の設定"](#)
- ["SnapLockボリュームの移動"](#)
- ["ランサムウェア攻撃から保護するためにSnapshotをロックする"](#)
- ["監査ログでの snapLock の使用を確認する"](#)
- ["SnapLock APIの使用"](#)

SnapLockのComplianceモードとEnterpriseモード

SnapLockのComplianceモードとEnterpriseモードの最も大きな違いは、WORMファイルの保護レベルです。

SnapLockモード	保護レベル	保持中のWORMファイルの削除
Complianceモード	ディスク レベル	削除できません
Enterpriseモード	ファイル レベル	コンプライアンス管理者が監査済みの「特権削除」手順を使用して削除できる

保持期間が経過したあとに不要となったファイルは手動で削除する必要があります。一度WORM状態にコミットされたファイルは、ComplianceモードかEnterpriseモードかに関係なく、保持期間が経過したあとも変更することはできません。

WORMファイルは保持期間中も保持期間後も移動できません。WORMファイルはコピーできますが、コピーしたファイルはWORM状態にはなりません。

次の表に、SnapLockのComplianceモードとEnterpriseモードでサポートされる機能の違いを示します。

機能	SnapLock Compliance	SnapLock Enterprise
privileged deleteを使用したファイルの有効化と削除	いいえ	はい

ディスクの再初期化	いいえ	はい
保持期間中のSnapLockアグリゲートとボリュームの破棄	いいえ	○ (SnapLock監査ログ ボリュームを除く)
アグリゲートまたはボリュームの名前変更	いいえ	はい
NetApp以外のディスクの使用	いいえ	いいえ
監査ログでのSnapLockボリュームの使用	はい	○ (ONTAP 9.5以降)

SnapLockでサポートされる機能とされない機能

次の表は、SnapLock ComplianceモードとSnapLock Enterpriseモードでサポートされる機能を示しています。

機能	SnapLock Compliance に対応	SnapLock Enterprise に対応
整合性グループ	いいえ	いいえ
暗号化されたボリューム	はい、 暗号化とSnapLock について詳しくご覧ください。	はい、 暗号化とSnapLock について詳しくご覧ください。
SnapLockアグリゲート上のFabricPool	いいえ	はい、ONTAP 9.8以降で可能です。 SnapLock Enterpriseアグリゲート上のFabricPool の詳細をご覧ください。
Flash Poolアグリゲート	○	○
FlexClone	SnapLockボリュームはクローニングできますが、SnapLockボリュームのファイルはクローニングできません。	SnapLockボリュームはクローニングできますが、SnapLockボリュームのファイルはクローニングできません。
FlexGroupボリューム	はい、ONTAP 9.11.1 以降で可能です。 [flexgroup] の詳細をご覧ください。	はい、ONTAP 9.11.1 以降で可能です。 [flexgroup] の詳細をご覧ください。
LUN	いいえ。SnapLockを使用した LUNのサポート の詳細については、こちらをご覧ください。	いいえ。SnapLockを使用した LUNのサポート の詳細については、こちらをご覧ください。

MetroCluster構成	はい、ONTAP 9.3以降で可能です。 MetroClusterのサポートの詳細 をご覧ください。	はい、ONTAP 9.3以降で可能です。 MetroClusterのサポートの詳細 をご覧ください。
マルチ管理者認証（MAV）	はい、ONTAP 9.13.1 以降で可能です。 MAVのサポートの詳細 をご覧ください。	はい、ONTAP 9.13.1 以降で可能です。 MAVのサポートの詳細 をご覧ください。
SAN	いいえ	いいえ
Single File SnapRestore	いいえ	はい
SnapMirrorアクティブ同期	いいえ	いいえ
SnapRestore	いいえ	はい
SMTape	いいえ	いいえ
SnapMirror Synchronous	いいえ	いいえ
SSD	○	○
Storage Efficiency機能	はい、ONTAP 9.9.1以降で可能です。 ストレージ効率のサポートの詳細 をご覧ください。	はい、ONTAP 9.9.1以降で可能です。 ストレージ効率のサポートの詳細 をご覧ください。

SnapLock Enterprise アグリゲート上のFabricPool

ONTAP 9.8以降では、FabricPoolがSnapLock Enterpriseアグリゲートでサポートされます。ただし、アカウント チームがProduct Variance Requestを申請して、パブリック クラウドまたはプライベート クラウドに階層化されたFabricPoolのデータは、クラウド管理者が削除できるためSnapLockでは保護されないことを承諾する必要があります。



FabricPoolでパブリック クラウドまたはプライベート クラウドに階層化されたデータはクラウド管理者が削除できるため、SnapLockでは保護されなくなりました。

FlexGroup ボリューム

ONTAP 9.11.1以降、SnapLockではFlexGroupボリュームがサポートされますが、次の機能はサポートされません。

- リーガル ホールド
- イベントベースの保持
- SnapLock for SnapVault（ONTAP 9.12.1以降でサポート）

また、次の点についても理解しておく必要があります。

- FlexGroupボリュームのボリューム コンプライアンス クロック（VCC）は、ルート コンスティチュエントのVCCによって決まります。すべての非ルート コンスティチュエントのVCCは、ルートのVCCと密接に同期されます。
- SnapLockの設定プロパティは、FlexGroup全体に対してのみ設定されます。個々のコンスティチュエントに、デフォルトの保持期限や自動コミット期間などの設定プロパティを指定することはできません。

LUNのサポート

LUNは、非SnapLockボリューム上で作成されたスナップショットがSnapLock vaultリレーションシップの一部として保護のためにSnapLockボリュームに転送されるシナリオにおいてのみ、SnapLockボリュームでサポートされます。LUNは読み取り / 書き込みSnapLockボリュームではサポートされません。ただし、改ざん防止スナップショットは、LUNを含むSnapMirrorソースボリュームとデスティネーションボリュームの両方でサポートされます。

MetroClusterのサポート

MetroCluster構成でのSnapLockのサポートは、SnapLock ComplianceモードとSnapLock Enterpriseモードで異なります。

SnapLock Compliance

- ONTAP 9.3以降では、ミラーされていないMetroClusterアグリゲートでSnapLock Complianceがサポートされます。
- ONTAP 9.3以降、ミラーされたアグリゲートでは、SnapLock監査ログ ボリュームのホストとして使用する場合に限りSnapLock Complianceがサポートされます。
- MetroClusterを使用して、プライマリ サイトとセカンダリ サイトにSVM固有のSnapLock構成をレプリケートできます。

SnapLock Enterprise

- SnapLock Enterprise アグリゲートがサポートされています。
- ONTAP 9.3以降では、privileged deleteを使用するSnapLock Enterpriseアグリゲートがサポートされます。
- MetroClusterを使用して、両方のサイトにSVM固有のSnapLock構成をレプリケートできます。

MetroCluster構成とコンプライアンス クロック

MetroCluster構成では、Volume Compliance Clock（VCC;ボリューム コンプライアンス クロック）とSystem Compliance Clock（SCC;システム コンプライアンス クロック）の2つのコンプライアンス クロック メカニズムが使用されます。VCCとSCCはすべてのSnapLock構成で使用できます。ノードに新しいボリュームを作成すると、ボリュームのVCCはそのノードの現在のSCCの値に初期化されます。ボリューム作成後のボリュームとファイルの保持期限の追跡には、常にVCCが使用されます。

ボリュームを別のサイトにレプリケートすると、ボリュームのVCCも一緒にレプリケートされます。ボリュームのスイッチオーバー（サイトAからサイトB）が発生した場合、VCCの更新はサイトBで継続されますが、サイトAのSCCはサイトAがオフラインになると停止します。

サイトAがオンラインに戻ってボリュームのスイッチバックが実行されると、サイトAのSCCのクロックが再開されますが、ボリュームのVCCは引き続き更新されます。VCCは継続的に更新されるため、スイッチオーバーやスイッチバックの処理に関係なくファイルの保持期限はSCCに依存せず、期限が延びることはありません。

マルチ管理者認証 (MAV) のサポート

ONTAP 9.13.1以降、クラスタ管理者はクラスタ上でマルチ管理者検証を明示的に有効にすることで、一部のSnapLock操作を実行する前にクォーラム承認を必須にすることができます。MAVを有効にすると、SnapLockボリュームプロパティ (default-retention-time、minimum-retention-time、maximum-retention-time、volume-append-mode、autocommit-period、privileged-delete) でクォーラム承認が必要になります。"MAV"の詳細をご覧ください。

ストレージ効率

ONTAP 9.9.1 以降、SnapLock は、SnapLock ボリュームおよびアグリゲートに対して、データ圧縮、ボリューム間重複排除、アダプティブ圧縮などのストレージ効率化機能をサポートしています。ストレージ効率化の詳細については、"[ONTAP Storage Efficiencyの概要](#)" を参照してください。

暗号化

ONTAPは、ストレージ メディアの転用、返却、置き忘れ、盗難に際して保存データが読み取られないようにソフトウェア ベースとハードウェア ベースの暗号化テクノロジーを提供します。

*免責事項：*NetAppは、認証キーを紛失した場合、または認証失敗回数が規定の制限を超え、ドライブが永久にロックされた場合、自己暗号化ドライブまたはボリューム上のSnapLock保護されたWORMファイルの復旧を保証することはできません。認証失敗に対する対策はお客様の責任となります。



暗号化されたボリュームはSnapLockアグリゲートでサポートされます。

7-Modeからの移行

7-Mode Transition Toolのコピーベースの移行 (CBT) 機能を使用して、SnapLockボリュームを7-ModeからONTAPに移行できます。デスティネーション ボリュームのSnapLockモード (ComplianceまたはEnterprise) とソース ボリュームのSnapLockモードが一致している必要があります。コピーフリーの移行 (CFT) はSnapLockボリュームの移行には使用できません。

SnapLockの設定

ONTAP SnapLockの設定について学ぶ

SnapLockを使用する前に、SnapLockボリュームを含むアグリゲートをホストする各ノードに対して"[SnapLockライセンスをインストールする](#)"を初期化する、"[コンプライアンス クロック](#)"を初期化する、ONTAP 9.10.1より前のONTAPリリースを実行しているクラスタのSnapLockアグリゲートを作成する、"[SnapLockボリュームを作成してマウントする](#)"などのさまざまなタスクを完了してSnapLockを設定する必要があります。

ONTAP Compliance Clockを初期化する

SnapLockは、WORMファイルの保存期間を変更する可能性のある改ざんを防止するため、_volume Compliance Clock_を使用します。まず、SnapLockアグリゲートをホストする各ノードで_system ComplianceClock_を初期化する必要があります。

ONTAP 9.14.1以降では、SnapLockボリュームがない場合、またはSnapshotロックが有効になっているボリュームがない場合に、システムCompliance Clockを初期化または再初期化できます。再初期化機能により、シス

システム管理者は、システムCompliance Clockが誤って初期化された場合にリセットしたり、システムのクロックドリフトを修正したりできます。ONTAP 9.13.1以前のリリースでは、ノード上でCompliance Clockを一度初期化すると、再度初期化することはできません。

開始する前に

コンプライアンス クロックを再初期化するには：

- クラスタ内のすべてのノードが正常な状態になっている必要があります。
- すべてのボリュームがオンラインになっている必要があります。
- リカバリ キューにボリュームが存在してはいけません。
- SnapLockボリュームが存在してはいけません。
- Snapshot ロックが有効になっているボリュームは存在できません。

コンプライアンス クロックを初期化するための一般的な要件：

- このタスクを実行するには、クラスタ管理者である必要があります。
- "SnapLock ライセンスはノードにインストールする必要があります"。

タスク概要

システムCompliance Clockの時刻は_ボリュームCompliance Clock_に継承されます。ボリュームCompliance Clockは、ボリューム上のWORMファイルの保存期間を制御します。ボリュームCompliance Clockは、新しいSnapLockボリュームを作成すると自動的に初期化されます。



システム コンプライアンス クロックの初期設定は、現在のハードウェア システム クロックに基づきます。そのため、各ノードでシステム コンプライアンス クロックを初期化する前に、システム時間とタイムゾーンが正しいことを確認する必要があります。ノードでシステム コンプライアンス クロックを初期化したあとに、ロックが有効になっているSnapLockボリュームが存在する場合、再度初期化することはできません。

手順

ONTAP CLIを使用してコンプライアンス クロックを初期化できます。また、ONTAP 9.12.1以降では、System Managerを使用してコンプライアンス クロックを初期化できます。

System Manager

1. **Cluster > Overview** に移動します。
2. *ノード*セクションで、*SnapLock Complianceクロックの初期化*をクリックします。
3. コンプライアンス クロック 列を表示し、コンプライアンス クロックが初期化されていることを確認するには、クラスター > 概要 > ノード セクションで、表示 / 非表示 をクリックし、**SnapLock** コンプライアンス クロック を選択します。

CLI

1. システム コンプライアンス クロックを初期化します。

```
snaplock compliance-clock initialize -node node_name
```

次のコマンドは、`node1`のシステムのコンプライアンス クロックを初期化します：

```
cluster1::> snaplock compliance-clock initialize -node node1
```

```
`snaplock compliance-clock initialize`
```

の詳細については、[link:https://docs.netapp.com/us-en/ontap-cli/snaplock-compliance-clock-initialize.html](https://docs.netapp.com/us-en/ontap-cli/snaplock-compliance-clock-initialize.html)["ONTAPコマンドリファレンス"]を参照してください。

2. 確認のプロンプトで、システム クロックが正しいこととコンプライアンス クロックの初期化を実行することを確認します。

```
Warning: You are about to initialize the secure ComplianceClock of
the node "node1" to the current value of the node's system clock.
This procedure can be performed only once on a given node, so you
should ensure that the system time is set correctly before
proceeding.
```

```
The current node's system clock is: Mon Apr 25 06:04:10 GMT 2016
```

```
Do you want to continue? (y|n): y
```

3. SnapLockアグリゲートをホストする各ノードについて、同じ手順を繰り返します。

NTPが設定されたシステムのコンプライアンス クロック再同期の有効化

NTP サーバーが構成されている場合、SnapLock コンプライアンス クロックの同期機能を有効にできます。

開始する前に

- この機能は、advanced権限レベルでのみ使用できます。

- このタスクを実行するには、クラスタ管理者である必要があります。
- "SnapLock ライセンスはノードにインストールする必要があります"。
- この機能は、Cloud Volumes ONTAP、ONTAP Select、およびVSIMのプラットフォームでのみ使用できます。

タスク概要

SnapLockのセキュア クロック デーモンがしきい値を超えるスキューを検出すると、システム時間を使用してシステムとボリュームの両方のコンプライアンス クロックがリセットされます。スキューのしきい値は24時間に設定されています。つまり、システム コンプライアンス クロックはスキューが1日を超えた場合にのみシステム クロックに同期されます。

スキューの検出とシステム時間へのコンプライアンス クロックの変更は、SnapLockのセキュア クロック デーモンによって行われます。コンプライアンス クロックはシステム時間がNTPの時間と同期されている場合しかシステム時間と同期されないため、システム時間を変更してコンプライアンス クロックをシステム時間に強制的に同期しようとしても失敗します。

手順

1. NTP サーバーが構成されている場合は、SnapLock Compliance Clock 同期機能を有効にします：

```
snaplock compliance-clock ntp
```

次のコマンドは、システムの Compliance Clock 同期機能を有効にします。

```
cluster1::*> snaplock compliance-clock ntp modify -is-sync-enabled true
```

```
`snaplock compliance-clock ntp modify`  
の詳細については、link:https://docs.netapp.com/us-en/ontap-cli/snaplock-compliance-clock-ntp-modify.html["ONTAPコマンド リファレンス  
"^]を参照してください。
```

2. 確認のプロンプトで、設定されているNTPサーバが信頼できることと通信チャネルがセキュアであることを確認して機能を有効にします。
3. 機能が有効になっていることを確認します。

```
snaplock compliance-clock ntp show
```

次のコマンドは、システムの Compliance Clock 同期機能が有効になっているかどうかを確認します：

```
cluster1::*> snaplock compliance-clock ntp show  
  
Enable clock sync to NTP system time: true
```

```
`snaplock compliance-clock ntp show`
```

の詳細については、[link:https://docs.netapp.com/us-en/ontap-cli/snaplock-compliance-clock-ntp-show.html](https://docs.netapp.com/us-en/ontap-cli/snaplock-compliance-clock-ntp-show.html)["ONTAP コマンド リファレンス"]を参照してください。

ONTAP SnapLock アグリゲートを作成する

ボリューム `snaplock-type` オプションを使用して、Compliance または Enterprise の SnapLock ボリューム タイプを指定します。ONTAP 9.10.1 より前のリリースでは、別個の SnapLock アグリゲートを作成する必要があります。ONTAP 9.10.1 以降では、SnapLock ボリューム と非 SnapLock ボリューム が同じアグリゲート上に存在できるようになりました。そのため、ONTAP 9.10.1 を使用している場合は、別個の SnapLock アグリゲートを作成する必要はありません。

開始する前に

- このタスクを実行するには、クラスタ管理者である必要があります。
- ノード上の SnapLock **"ライセンスをインストールする必要があります"**。このライセンスは **"ONTAP One"** に含まれています。
- **"ノード上のコンプライアンスクロックを初期化する必要があります"**。
- ディスクを「root」、「data1」、および「data2」としてパーティション分割している場合は、スペアディスクが使用可能であることを確認する必要があります。

アップグレード時の考慮事項

ONTAP 9.10.1 にアップグレードすると、既存の SnapLock および非 SnapLock アグリゲートが SnapLock ボリューム と非 SnapLock ボリューム の両方をサポートするようにアップグレードされますが、既存の SnapLock ボリューム の属性は自動的に更新されません。たとえば、data-compaction、cross-volume-dedupe、cross-volume-background-dedupe の各フィールドは変更されません。既存のアグリゲートに作成された新しい SnapLock ボリューム には非 SnapLock ボリューム と同じデフォルト値が使用され、新しいボリューム とアグリゲート にはプラットフォームに応じて異なるデフォルト値が適用されます。

リバートに関する考慮事項

ONTAP 9.10.1 よりも前のバージョンにリバートする必要がある場合は、すべての SnapLock Compliance ボリューム、SnapLock Enterprise ボリューム、および SnapLock ボリューム をそれぞれの SnapLock アグリゲートに移動する必要があります。

タスク概要

- SyncMirror オプションを指定して Compliance アグリゲートを作成することはできません。
- ミラーされた Compliance アグリゲートを MetroCluster 構成に作成できるのは、アグリゲートを SnapLock 監査ログ ボリューム のホストとして使用する場合だけです。



MetroCluster 構成では、SnapLock Enterprise は、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サポートされます。SnapLock Compliance は、ミラーされていないアグリゲートでのみサポートされます。

手順

1. SnapLockアグリゲートを作成します。

```
storage aggregate create -aggregate <aggregate_name> -node <node_name>
-diskcount <number_of_disks> -snaplock-type <compliance|enterprise>
```

次のコマンドは、`node1`上の3つのディスクを使用して`aggr1`という名前のSnapLock `Compliance`アグリゲートを作成します：

```
cluster1::> storage aggregate create -aggregate aggr1 -node node1
-diskcount 3 -snaplock-type compliance
```

```
`storage aggregate create`
```

の詳細については、[link:https://docs.netapp.com/us-en/ontap-cli/storage-aggregate-create.html](https://docs.netapp.com/us-en/ontap-cli/storage-aggregate-create.html)["ONTAPコマンド リファレンス"]をご覧ください。

ONTAP SnapLockボリュームを作成してマウントする

ファイルやスナップショットをWORM状態にコミットするには、SnapLockボリュームを作成する必要があります。ONTAP 9.10.1以降では、アグリゲートの種類に関係なく、作成されるすべてのボリュームはデフォルトで非SnapLockボリュームとして作成されます。明示的にSnapLockボリュームを作成するには、`-snaplock-type`オプションを使用し、SnapLockタイプとしてComplianceまたはEnterpriseのいずれかを指定する必要があります。デフォルトでは、SnapLockタイプは`non-snaplock`に設定されています。

開始する前に

- SnapLockアグリゲートがオンラインになっている必要があります。
- "SnapLockライセンスがインストールされていることを確認する"する必要があります。SnapLockライセンスがノードにインストールされていない場合は、"インストール"する必要があります。このライセンスは"ONTAP One"に含まれています。ONTAP Oneより前のバージョンでは、SnapLockライセンスはSecurity and Complianceバンドルに含まれていました。Security and Complianceバンドルは現在提供されていませんが、引き続き有効です。現在必須ではありませんが、既存のお客様は"ONTAP Oneにアップグレード"を選択できます。
- "ノード上のコンプライアンスクロックを初期化する必要があります"。

タスク概要

SnapLockの適切な権限があれば、Enterpriseボリュームはいつでも破棄または名前変更できます。Complianceボリュームの削除は保持期間が終了するまでは実行できません。Complianceボリュームの名前は一切変更できません。

SnapLockボリュームはクローニングできますが、SnapLockボリュームのファイルはクローニングできません。クローン ボリュームのSnapLockタイプは親ボリュームと同じになります。



LUNはSnapLockボリュームではサポートされません。LUNは、非SnapLockボリューム上で作成されたスナップショットがSnapLockヴォールト関係の一部として保護のためにSnapLockボリュームに転送される場合にのみ、SnapLockボリュームでサポートされます。LUNは読み取り/書き込みSnapLockボリュームではサポートされません。ただし、改ざん防止スナップショットは、LUNを含むSnapMirrorソースボリュームとデスティネーションボリュームの両方でサポートされます。

このタスクは、ONTAP System ManagerまたはONTAP CLIを使用して実行します。

System Manager

ONTAP 9.12.1以降では、System Managerを使用してSnapLockボリュームを作成できます。

手順

1. ストレージ > ボリューム に移動し、追加 をクリックします。
2. *ボリュームの追加*ウィンドウで、*その他のオプション*をクリックします。
3. 新しいボリュームの情報（ボリュームの名前とサイズなど）を入力します。
4. *SnapLockを有効にする*を選択し、SnapLockタイプ（ComplianceまたはEnterprise）を選択します。
5. *ファイルの自動コミット*セクションで*変更済み*を選択し、ファイルが変更されずに保持される期間を入力すると、その期間経過後に自動的にコミットされます。最小値は5分、最大値は10年です。
6. *Data Retention*セクションで、最小および最大保持期間を選択します。
7. デフォルトの保持期間を選択します。
8. *保存*をクリックします。
9. ボリューム ページで新しいボリュームを選択し、SnapLock 設定を確認します。

CLI

1. SnapLockボリュームを作成します。

```
volume create -vserver <SVM_name> -volume <volume_name> -aggregate  
<aggregate_name> -snaplock-type <compliance|enterprise>
```

`volume create`の詳細については、link:<https://docs.netapp.com/us-en/ontap-cli/volume-create.html>["ONTAPコマンド リファレンス"]を参照してください。次のオプションはSnapLockボリュームでは使用できません：
`-nvfail`、`-atime-update`、`-is-autobalance-eligible`、`-space-mgmt-try-first`、および `vmalign`。

次のコマンドは、`vs1`上の`aggr1`に`vol1`という名前のSnapLock `Compliance`ボリュームを作成します：

```
cluster1::> volume create -vserver vs1 -volume vol1 -aggregate aggr1  
-snaplock-type compliance
```

SnapLockボリュームのマウント

NASクライアントからアクセスできるように、SnapLockボリュームをSVM名前空間のジャンクションパスにマウントすることができます。

開始する前に

SnapLockがオンラインである必要があります。

タスク概要

- SnapLockボリュームはSVMのルートにしかマウントできません。
- 通常のボリュームをSnapLockボリュームにマウントすることはできません。

手順

1. SnapLockボリュームをマウントします。

```
volume mount -vserver SVM_name -volume volume_name -junction-path path
```

`volume mount`の詳細については、[link:https://docs.netapp.com/us-en/ontap-cli/volume-mount.html](https://docs.netapp.com/us-en/ontap-cli/volume-mount.html)["ONTAPコマンド リファレンス"]をご覧ください。

次のコマンドは、SnapLockボリューム`vol1`を`vs1`名前空間内のジャンクションパス`/sales`にマウントします：

```
cluster1::> volume mount -vserver vs1 -volume vol1 -junction-path /sales
```

ONTAP SnapLock保持期間を設定する

保持期限の設定については、ファイルに対して明示的に設定する方法と、ボリュームのデフォルトの保持期間から自動的に設定する方法があります。保持期限を明示的に設定しない場合は、デフォルトの保持期間に基づいて保持期限が計算されます。イベント後にファイルの保持期限を設定することもできます。

保持期間と保持期限について

WORMファイルの_保持期間_は、ファイルがWORM状態にコミットされた後、保持する必要がある期間を指定します。WORMファイルの_保持時間_は、そのファイルを保持する必要があるまでの時間です。例えば、2020年11月10日午前6：00にWORM状態にコミットされたファイルの保持期間が20年の場合、保持時間は2040年11月10日午前6：00になります。



ONTAP 9.10.1以降では、最長で保持期限を3058年10月26日、保持期間を100年に設定できます。保持期限を延長すると、古いポリシーは自動的に変換されます。ONTAP 9.9.1以前のリリースでは、デフォルトの保持期間を無期限に設定した場合を除き、サポートされる最も遅い保持期限は2071年1月19日（GMT）です。

レプリケーションに関する重要な考慮事項

保持期限を2071年1月19日（GMT）よりもあとに設定してSnapLockソース ボリュームとのSnapMirror関係を

確立する場合は、デスティネーション クラスタでONTAP 9.10.1以降が実行されている必要があります。そうでない場合、SnapMirror転送が失敗します。

リバートに関する重要な考慮事項

ONTAPでは、保持期間が「2071年1月19日午前8時44分7秒」以降のファイルがある場合、クラスタをONTAP 9.10.1から以前のONTAPバージョンにリバートすることはできません。

保持期間について

SnapLock ComplianceまたはSnapLock Enterpriseボリュームには、次の4種類の保持期間があります。

- 最小保存期間(min) 、デフォルトは0
- 最大保存期間(max) 、デフォルトは30年
- デフォルトの保持期間。ONTAP 9.10.1以降では、コンプライアンスモードとエンタープライズモードの両方でデフォルトが`min`になります。ONTAP 9.10.1より前のONTAPリリースでは、デフォルトの保持期間はモードによって異なります：
 - コンプライアンス モードの場合、デフォルトは`max`になります。
 - エンタープライズ モードの場合、デフォルトは`min`になります。
- 未指定の保持期間。



ONTAP 9.10.1より前のリリースでは、コンプライアンスモードのファイルをWORM状態にコミットする前に明示的に保持期間を設定せず、デフォルトも変更していない場合、ファイルは30年間保持されます。この変更は元に戻すことが_できません_。同様に、ONTAP 9.10.1以降では、エンタープライズモードのファイルをWORM状態にコミットする前に明示的に保持期間を設定せず、デフォルトも変更していない場合、ファイルは0年間保持され、実質的に全く保持されないことになります。

ONTAP 9.8以降では、ボリューム内のファイルの保持期間を`unspecified`に設定することで、絶対保持期間を設定するまでファイルを保持できるようになりました。絶対保持期間が設定されているファイルを、無指定の保持期間に設定し、新しい絶対保持期間が以前に設定した絶対保持期間よりも後であれば、絶対保持期間に戻すことができます。

ONTAP 9.12.1以降、保持期間が`unspecified`に設定されているWORMファイルは、SnapLockボリュームに設定されている最小保持期間に設定されることが保証されます。ファイルの保持期間を`unspecified`から絶対保持時間に変更する場合、指定する新しい保持時間は、ファイルに既に設定されている最小保持時間よりも長くする必要があります。

デフォルトの保持期間の設定

```
`volume snaplock modify` コマンドを使用して、  
SnapLockボリューム上のファイルのデフォルトの保持期間を設定できます。
```

開始する前に

SnapLockがオンラインである必要があります。

タスク概要

次の表に、デフォルトの保持期間に指定できる値を示します。



デフォルトの保持期間は、最小保持期間以上、最大保持期間以下にする必要があります。

Value	単位	注記
0 - 65535	seconds	
0 - 24	hours	
0 - 365	days	
0 - 12	months	
0 - 100	years	ONTAP 9.10.1以降。以前のリリースのONTAPの場合、値は0 - 70です。
max	-	最大保持期間を使用します。
min	-	最小保持期間を使用します。
infinite	-	ファイルを無期限に保持します。
unspecified	-	明確な保持期間が設定されるまでファイルを保持します。

最大保存期間と最小保存期間の値と範囲は、`max`と`min`を除き同一です。ただし、これらは適用されません。このタスクの詳細については、"[保持期限の設定 - 概要](#)"を参照してください。

```
`volume snaplock show`
```

コマンドを使用して、ボリュームの保持期間設定を表示できます。link:<https://docs.netapp.com/us-en/ontap-cli/volume-snaplock-show.html>["ONTAPコマンド リファレンス"]の`volume snaplock show`の詳細をご覧ください。



ファイルがWORM状態にコミットされたあとは、保持期間を延長することはできますが短縮することはできません。

手順

1. SnapLockボリューム上のファイルにデフォルトの保持期間を設定します。

```
volume snaplock modify -vserver SVM_name -volume volume_name -default
-retention-period default_retention_period -minimum-retention-period
min_retention_period -maximum-retention-period max_retention_period
```

`volume snaplock modify`の詳細については、link:<https://docs.netapp.com/us-en/ontap-cli/volume-snaplock-modify.html>["ONTAPコマンド リファレンス"]を参照してください。



以下の例は、最大保持期間と最小保持期間が過去に変更されていないことを想定しています。

次のコマンドは、ComplianceボリュームまたはEnterpriseボリュームのデフォルトの保持期間を20日に設定します。

```
cluster1::> volume snaplock modify -vserver vs1 -volume vol1 -default  
-retention-period 20days
```

次のコマンドは、Complianceボリュームのデフォルトの保持期間を70年に設定します。

```
cluster1::> volume snaplock modify -vserver vs1 -volume vol1 -maximum  
-retention-period 70years
```

次のコマンドは、Enterpriseボリュームのデフォルトの保持期間を10年に設定します。

```
cluster1::> volume snaplock modify -vserver vs1 -volume vol1 -default  
-retention-period max -maximum-retention-period 10years
```

次のコマンドは、Enterpriseボリュームのデフォルトの保持期間を10日に設定します。

```
cluster1::> volume snaplock modify -vserver vs1 -volume vol1 -minimum  
-retention-period 10days  
cluster1::> volume snaplock modify -vserver vs1 -volume vol1 -default  
-retention-period min
```

次のコマンドは、Complianceボリュームのデフォルトの保持期間を無期限に設定します。

```
cluster1::> volume snaplock modify -vserver vs1 -volume vol1 -default  
-retention-period infinite -maximum-retention-period infinite
```

ファイルに対する保持期限の明示的な設定

ファイルに対して保持期限を明示的に設定するには、最終アクセス時刻を変更します。最終アクセス時刻は、NFSまたはCIFSで適切なコマンドやプログラムを使用して変更できます。

タスク概要

ファイルがWORMモードにコミットされた後、保持期間を延長することはできますが、短縮することはできません。保持期間はファイルの `atime` フィールドに保存されます。



ファイルの保持期間を明示的に `infinite` に設定することはできません。この値は、デフォルトの保持期間を使用して保持期間を計算する場合にのみ使用できます。

手順

1. 適切なコマンドまたはプログラムを使用して、保持期限を設定するファイルの最終アクセス時刻を変更します。

UNIXシェルで、次のコマンドを使用して、`document.txt` という名前のファイルの保持時間を2020年11月21日午前6:00に設定します：

```
touch -a -t 202011210600 document.txt
```



Windowsでは、任意の適切なコマンドまたはプログラムを使用して最終アクセス時刻を変更できます。

イベント発生後のファイル保持期間の設定

ONTAP 9.3 以降では、SnapLock _Event Based Retention (EBR) _機能を使用して、イベント発生後にファイルを保持する期間を定義できます。

開始する前に

- このタスクを実行するには、SnapLock管理者である必要があります。

["SnapLock管理者アカウントの作成"](#)

- セキュアな接続（SSH、コンソール、またはZAPI）でログインする必要があります。

タスク概要

_イベント保持ポリシー_は、イベント発生後のファイルの保持期間を定義します。このポリシーは、単一のファイルまたはディレクトリ内のすべてのファイルに適用できます。

- WORMファイル以外のファイルの場合、ポリシーで定義された保持期間にわたってWORM状態にコミットされます。
- WORMファイルまたは追記可能WORMファイルの場合、保持期間がポリシーで定義された保持期間まで延長されます。

ComplianceモードまたはEnterpriseモードのボリュームを使用できます。



EBRポリシーは、リーガル ホールド中のファイルには適用できません。

高度な使用方法については、["NetApp SnapLockを使用した準拠WORMストレージ"](#)を参照してください。

EBRを使用して既存の**WORM**ファイルの保持期間を延長する

EBRは、既存のWORMファイルの保持期間を延長する場合に便利です。たとえば、会社の規定で、従業員が源泉徴収の選択を変更した場合に、変更後3年間は従業員のW-4レコードを変更不可能な状態で保管するように定められているとします。さらに、従業員の退職後はW-4レコードを5年間保管するように定めた規定もあります。

このような状況では、5年間の保持期間を設定したEBRポリシーを作成できます。従業員が退職した後（「event」）、EBRポリシーを従業員のW-4レコードに適用し、保持期間を延長します。これは通常、手で保持期間を延長するよりも簡単で、特に大量のファイルが関係する場合は効果的です。

手順

1. EBRポリシーを作成します。

```
snaplock event-retention policy create -vserver SVM_name -name policy_name  
-retention-period retention_period
```

次のコマンドは、`vs1`上に保持期間が10年のEBRポリシー`employee\_exit`を作成します：

```
cluster1::>snaplock event-retention policy create -vserver vs1 -name  
employee_exit -retention-period 10years
```

2. EBRポリシーを適用します。

```
snaplock event-retention apply -vserver SVM_name -name policy_name -volume  
volume_name -path path_name
```

次のコマンドは、`vs1`上の`d1`ディレクトリ内のすべてのファイルにEBRポリシー`employee\_exit`を適用します：

```
cluster1::>snaplock event-retention apply -vserver vs1 -name  
employee_exit -volume vol1 -path /d1
```

関連情報

- ["SnapLockイベント保持ポリシーの作成"](#)
- ["SnapLockイベント保持適用"](#)

ONTAP SnapLockで保護された監査ログを作成する

ONTAP 9.9.1以前を使用している場合は、まずSnapLockアグリゲートを作成したうえで、privileged deleteまたはSnapLockボリュームの移動を実行する前に、SnapLockで保護された監査ログを作成しておく必要があります。この監査ログには、SnapLock管理者アカウントの作成と削除、ログ ボリュームに対する変更、privileged deleteが有効になっているかどうか、privileged delete処理、およびSnapLockボリューム移動処理に関する情報が記録されます。

ONTAP 9.10.1以降では、SnapLockアグリゲートを作成しなくなりました。-snaplock-typeオプションを使用

して、SnapLockタイプとしてComplianceまたはEnterpriseを指定することで"明示的にSnapLockボリュームを作成する"する必要があります。

開始する前に

ONTAP 9.9.1以前を使用している場合、SnapLockアグリゲートを作成するにはクラスタ管理者になる必要があります。

タスク概要

監査ログは、ログ ファイルの保持期間が経過するまで削除できません。保持期間が経過したあとも、監査ログを変更することはできません。これは、SnapLockのComplianceモードとEnterpriseモードの両方に該当します。



ONTAP 9.4以前では、監査ログにSnapLock Enterpriseボリュームは使用できません。SnapLock Complianceボリュームを使用する必要があります。ONTAP 9.5以降では、監査ログにSnapLock EnterpriseボリュームまたはSnapLock Complianceボリュームのいずれかを使用できます。いずれの場合も、監査ログボリュームはジャンクションパス `/snaplock_audit_log` にマウントする必要があります。他のボリュームはこのジャンクションパスを使用できません。

SnapLock監査ログは、監査ログボリュームのルート下の `/snaplock_log` ディレクトリにあり、`/privdel_log` (特権削除操作) および `system_log` (その他すべて) という名前のサブディレクトリに格納されています。監査ログファイル名には、最初に記録された操作のタイムスタンプが含まれるため、操作が実行されたおおよその時刻でレコードを簡単に検索できます。

- `snapshot log file show` コマンドを使用して、監査ログ ボリューム上のログ ファイルを表示できます。
- `snapshot log file archive` コマンドを使用すると、現在のログ ファイルをアーカイブし、新しいログ ファイルを作成できます。これは、監査ログ情報を別のファイルに記録する必要がある場合に便利です。

```
`snapshot log file show`および `snapshot log file archive`  
の詳細については、link:https://docs.netapp.com/us-en/ontap-cli/search.html?q=snapshot+log+file["ONTAPコマンド リファレンス  
"]を参照してください。
```



データ保護ボリュームは、SnapLock監査ログ ボリュームとしては使用できません。

手順

1. SnapLockアグリゲートを作成します。

[SnapLockアグリゲートの作成](#)

2. 監査ログを設定するSVMにSnapLockボリュームを作成します。

[SnapLockボリュームの作成](#)

3. SVMに監査ログを設定します。

```
snapshot log create -vserver SVM_name -volume snapshot_volume_name -max-log  
-size size -retention-period default_retention_period
```



監査ログファイルのデフォルトの最小保持期間は6か月です。影響を受けるファイルの保持期間が監査ログの保持期間よりも長い場合、監査ログの保持期間はファイルの保持期間を継承します。したがって、特権削除を使用して削除されたファイルの保持期間が10か月で、監査ログの保持期間が8か月の場合、監査ログの保持期間は10か月に延長されます。保持期間とデフォルトの保持期間の詳細については、"[保持期限の設定](#)"を参照してください。

次のコマンドは、SnapLockボリューム `logVol` を使用して `SVM1` の監査ログを設定します。監査ログの最大サイズは20 GBで、8か月間保持されます。

```
SVM1::> snaplock log create -vserver SVM1 -volume logVol -max-log-size 20GB -retention-period 8months
```

`snaplock log create`の詳細については、[link:https://docs.netapp.com/us-en/ontap-cli/snaplock-log-create.html](https://docs.netapp.com/us-en/ontap-cli/snaplock-log-create.html) ["ONTAPコマンド リファレンス"]を参照してください。

4. 監査ログ用に設定したSVMで、SnapLockボリュームをジャンクションパスにマウントします
/snaplock_audit_log。

SnapLockボリュームのマウント

ONTAP SnapLock設定を確認する

`volume file fingerprint start`コマンドと `volume file fingerprint dump`コマンドを使用すると、ファイルの種類（通常、WORM、またはWORM追加可能）、ボリュームの有効期限など、ファイルとボリュームに関する重要な情報を表示できます。

手順

1. ファイルフィンガープリントを生成します。

```
volume file fingerprint start -vserver <SVM_name> -file <file_path>
```

```
svm1::> volume file fingerprint start -vserver svm1 -file /vol/s1e/vol/f1  
File fingerprint operation is queued. Run "volume file fingerprint show -session-id 16842791" to view the fingerprint session status.
```

このコマンドは、`volume file fingerprint dump`コマンドへの入力として使用できるセッションIDを生成します。



`volume file fingerprint show` コマンドをセッション IDとともに使用して、フィンガープリント操作の進行状況を監視できます。フィンガープリントを表示する前に、操作が完了していることを確認してください。

2. ファイルのフィンガープリントを表示します。

```
volume file fingerprint dump -session-id <session_ID>
```

```
svml1:> volume file fingerprint dump -session-id 33619976
Vserver:svml
Session-ID:33619976
Volume:slc_vol
Path:/vol/slc_vol/f1
Data
Fingerprint:MOFJVevxNSJm3C/4Bn5oEEYH51CrudOzZYK4r5Cfylg=Metadata
Fingerprint:8iMjqJXiNcqqXT5XuRhLiEwIrJEihDmwS0hrexnjgmc=Fingerprint
Algorithm:SHA256
  Fingerprint Scope:data-and-metadata
  Fingerprint Start Time:1460612586
  Formatted Fingerprint Start Time:Thu Apr 14 05:43:06 GMT 2016
  Fingerprint Version:3
  **SnapLock License:available**
  Vserver UUID:acf7ae64-00d6-11e6-a027-0050569c55ae
  Volume MSID:2152884007
  Volume DSID:1028
  Hostname:my_host
  Filer ID:5f18eda2-00b0-11e6-914e-6fb45e537b8d
  Volume Containing Aggregate:slc_aggr1
  Aggregate ID:c84634aa-c757-4b98-8f07-eeef32565f67
  **SnapLock System ComplianceClock:1460610635
  Formatted SnapLock System ComplianceClock:Thu Apr 14 05:10:35
  GMT 2016
  Volume SnapLock Type:compliance
  Volume ComplianceClock:1460610635
  Formatted Volume ComplianceClock:Thu Apr 14 05:10:35 GMT 2016
  Volume Expiry Date:1465880998**
  Is Volume Expiry Date Wraparound:false
  Formatted Volume Expiry Date:Tue Jun 14 05:09:58 GMT 2016
  Filesystem ID:1028
  File ID:96
  File Type:worm
  File Size:1048576
  Creation Time:1460612515
```

```
Formatted Creation Time:Thu Apr 14 05:41:55 GMT 2016
Modification Time:1460612515
Formatted Modification Time:Thu Apr 14 05:41:55 GMT 2016
Changed Time:1460610598
Is Changed Time Wraparound:false
Formatted Changed Time:Thu Apr 14 05:09:58 GMT 2016
Retention Time:1465880998
Is Retention Time Wraparound:false
Formatted Retention Time:Tue Jun 14 05:09:58 GMT 2016
Access Time:-
Formatted Access Time:-
Owner ID:0
Group ID:0
Owner SID:-
Fingerprint End Time:1460612586
Formatted Fingerprint End Time:Thu Apr 14 05:43:06 GMT 2016
```

WORMファイルの管理

ONTAP SnapLockでWORMファイルを管理

WORMファイルは次の方法で管理できます。

- ["ファイルのWORM状態へのコミット"](#)
- ["スナップショットをボールド デスティネーションの WORM にコミットする"](#)
- ["ディザスタ リカバリ用のWORMファイルのミラーリング"](#)
- ["訴訟期間中のWORMファイルの保持"](#)
- ["WORMファイルの削除"](#)

ONTAP SnapLockを使用してファイルをWORMにコミット

ファイルのWORM（Write Once, Read Many）状態へのコミットは、手動で、または自動的に行うことができます。追記可能WORMファイルを作成することもできます。

ファイルのWORM状態への手動コミット

ファイルを手動でWORM状態にコミットするには、ファイルを読み取り専用にします。ファイルの読み書き属性は、NFSまたはCIFSで適切なコマンドやプログラムを使用して読み取り専用に変更できます。ファイルが早期にコミットされないようアプリケーションがファイルへの書き込みを完了したことを確認したい場合や、ボリューム数が多いために自動コミット スキャナでスケーリングの問題が発生する場合は、手動でファイルをコミットすることができます。

開始する前に

- コミットするファイルがSnapLockボリュームに格納されている必要があります。
- ファイルが書き込み可能になっている必要があります。

タスク概要

コマンドまたはプログラムが実行されると、ボリュームComplianceClock時間がファイルの`ctime`フィールドに書き込まれます。ComplianceClock時間によって、ファイルの保存期間に達したかどうか判断されません。

手順

1. 適切なコマンドまたはプログラムを使用して、ファイルの読み書き属性を読み取り専用に変更します。

UNIXシェルでは、次のコマンドを使用して、`document.txt`という名前のファイルを読み取り専用にします：

```
chmod -w document.txt
```

Windowsシェルで次のコマンドを使用して、`document.txt`という名前のファイルを読み取り専用にします：

```
attrib +r document.txt
```

ファイルのWORM状態への自動コミット

SnapLock自動コミット機能を使用すると、ファイルを自動的にWORM状態にコミットできます。自動コミット機能は、ファイルが自動コミット期間内に変更されなかった場合、SnapLockボリューム上のファイルをWORM状態にコミットします。自動コミット機能はデフォルトで無効になっています。

開始する前に

- 自動コミットするファイルがSnapLockボリュームに格納されている必要があります。
- SnapLockがオンラインである必要があります。
- SnapLockボリュームが読み書き可能ボリュームである必要があります。



SnapLockの自動コミット機能は、ボリューム内のすべてのファイルをスキャンし、自動コミットの要件を満たすファイルをコミットします。ファイルが自動コミットできる状態になってから、SnapLockの自動コミット スキャナによって実際にコミットされるまでに、時間が空くことがあります。ただし、ファイルは自動コミットの対象になった時点からファイルシステムによる削除や変更から保護されます。

タスク概要

自動コミット期間は、ファイルが自動コミットされるまでに変更されない期間を指定します。自動コミット期間が経過する前にファイルを変更すると、そのファイルの自動コミット期間が再開されます。

自動コミット期間に指定できる値は次のとおりです。

Value	単位	注記
なし	-	デフォルト

Value	単位	注記
5 - 5256000	minutes	-
1 - 87600	hours	-
1 - 3650	days	-
1 - 120	months	-
1 - 10	years	-



最小値は5分、最大値は10年です。

手順

1. SnapLockボリュームのファイルをWORM状態に自動コミットします。

```
volume snaplock modify -vserver SVM_name -volume volume_name -autocommit
-period autocommit_period
```

`volume snaplock modify`の詳細については、link:<https://docs.netapp.com/us-en/ontap-cli/volume-snaplock-modify.html>["ONTAPコマンド リファレンス"]を参照してください。

次のコマンドは、ファイルが5時間変更されない限り、SVM vs1のボリューム `vol1` 上のファイルを自動コミットします：

```
cluster1::>volume snaplock modify -vserver vs1 -volume vol1 -autocommit
-period 5hours
```

追記可能WORMファイルの作成

追記可能なWORMファイルは、ログエントリのように増分的に書き込まれるデータを保持します。適切なコマンドやプログラムを使用してWORM追記可能ファイルを作成するか、SnapLock_ボリューム追記モード_機能を使用してデフォルトでWORM追記可能ファイルを作成することもできます。

コマンドまたはプログラムを使用した追記可能WORMファイルの作成

追記可能WORMファイルは、NFSまたはCIFSで適切なコマンドやプログラムを使用して作成できます。追記可能WORMファイルには、ログ エントリのように段階的に書き込まれるデータが格納されます。データは256KBのチャンク単位でファイルに追加されます。チャンクが書き込まれるたびに、前のチャンクがWORM方式で保護されます。このファイルは保持期間が経過するまで削除できません。

開始する前に

追記可能WORMファイルはSnapLockボリュームに格納する必要があります。

タスク概要

アクティブな256 KBチャンクにデータを順番に書き込む必要はありません。ファイルの $n \times 256\text{KB} + 1$ バイト目にデータが書き込まれると、前の256 KBセグメントはWORM保護されます。

現在アクティブな256KBのチャンクを超える順不同の書き込みが発生すると、アクティブな256KBのチャンクが最新のオフセットにリセットされ、古いオフセットへの書き込みが失敗して「Read Only File System (ROFS)」エラーが表示されます。書き込みオフセットは、クライアント アプリケーションによって異なります。クライアントが追記可能WORMファイルの書き込みセマンティクスに準拠していないと、書き込み内容が誤って終了する可能性があります。そのため、クライアントを順不同の書き込みのオフセット制限に準拠させるか、ファイルシステムを同期モードでマウントして同期書き込みが行われるようにすることを推奨します。

手順

1. 適切なコマンドまたはプログラムを使用して、必要な保持期限を指定した空のファイルを作成します。

UNIXシェルで、次のコマンドを使用して、`document.txt`という名前の長さがゼロのファイルの保持時間を2020年11月21日午前6:00に設定します：

```
touch -a -t 202011210600 document.txt
```

2. 適切なコマンドまたはプログラムを使用して、ファイルの読み書き属性を読み取り専用に変更します。

UNIXシェルでは、次のコマンドを使用して、`document.txt`という名前のファイルを読み取り専用にします：

```
chmod 444 document.txt
```

3. 適切なコマンドまたはプログラムを使用して、ファイルの読み書き属性を書き込み可能に戻します。



ファイル内にデータがないため、この手順はコンプライアンス リスクとはみなされません。

UNIXシェルでは、次のコマンドを使用して、`document.txt`という名前のファイルを書き込み可能にします：

```
chmod 777 document.txt
```

4. 適切なコマンドまたはプログラムを使用して、ファイルへのデータの書き込みを開始します。

UNIX シェルでは、次のコマンドを使用して `document.txt` にデータを書き込みます：

```
echo test data >> document.txt
```



ファイルにデータを追加する必要がなくなったら、ファイル権限を読み取り専用に戻してください。

ONTAP 9.3以降では、SnapLock_ボリューム追加モード_ (VAM) 機能を使用して、デフォルトでWORM形式の追記可能ファイルを作成できます。WORM形式の追記可能ファイルは、ログエントリのように増分的に書き込まれるデータを保持します。データは256KBのチャンク単位でファイルに追加されます。各チャンクが書き込まれるたびに、前のチャンクはWORM保護されます。保持期間が経過するまで、ファイルを削除することはできません。

開始する前に

- 追記可能WORMファイルはSnapLockボリュームに格納する必要があります。
- SnapLockボリュームはアンマウントされ、Snapshotとユーザが作成したファイルが含まれていない状態である必要があります。

タスク概要

アクティブな256 KBチャンクにデータを順番に書き込む必要はありません。ファイルの $n \times 256 \text{KB} + 1$ バイト目にデータが書き込まれると、前の256 KBセグメントはWORM保護されます。

ボリュームに自動コミット期間を指定している場合、追記可能WORMファイルに変更がなかった期間が自動コミット期間を超えると、そのファイルはWORM状態にコミットされます。



VAMはSnapLock監査ログ ボリュームではサポートされません。

手順

1. VAMを有効にします。

```
volume snaplock modify -vserver SVM_name -volume volume_name -is-volume-append  
-mode-enabled true|false
```

`volume snaplock modify`の詳細については、link:<https://docs.netapp.com/us-en/ontap-cli/volume-snaplock-modify.html>["ONTAPコマンド リファレンス"]を参照してください。

次のコマンドは、SVM`vs1`のボリューム`vol1`上でVAMを有効にします：

```
cluster1::>volume snaplock modify -vserver vs1 -volume vol1 -is-volume  
-append-mode-enabled true
```

2. 適切なコマンドまたはプログラムを使用して、書き込み権限を指定してファイルを作成します。

ファイルはデフォルトで追記可能WORMファイルになります。

ONTAPヴォールト デスティネーションでSnapshotをWORMにコミットする

セカンダリストレージ上のスナップショットをWORM保護するために、SnapLock for SnapVaultを使用できます。すべての基本的なSnapLockタスクは、ヴォールトのデスティネーションで実行します。デスティネーションボリュームは自動的に読み取り専用でマ

ウントされるため、スナップショットを明示的にWORMにコミットする必要はありません。

開始する前に

- System Managerを使用して関係を設定する場合は、ソースとデスティネーションの両方のクラスターでONTAP 9.15.1以降が実行されている必要があります。
- デスティネーション クラスター：
 - ["SnapLockライセンスをインストールする"](#)。
 - ["コンプライアンス クロックの初期化"](#)。
 - ONTAP 9.10.1より前のONTAPリリースでCLIを使用している場合は、["SnapLockアグリゲートを作成する"](#)。
- 保護ポリシーのタイプは「vault」であることが必要です。
- ソース アグリゲートとデスティネーション アグリゲートはどちらも64ビットである必要があります。
- ソース ボリュームにSnapLockボリュームを使用することはできません。
- ONTAP CLIを使用している場合は、ソース ボリュームとデスティネーション ボリュームを["ピア クラスター"](#)および["SVM"](#)に作成する必要があります。

タスク概要

ソース ボリュームで使用するストレージは、NetAppのストレージでもNetApp以外のストレージでもかまいません。



WORM状態にコミットされたSnapshotの名前を変更することはできません。

SnapLockボリュームはクローニングできますが、SnapLockボリュームのファイルはクローニングできません。



LUNはSnapLockボリュームではサポートされません。LUNは、非SnapLockボリューム上で作成されたスナップショットがSnapLockヴォールト関係の一部として保護のためにSnapLockボリュームに転送される場合にのみ、SnapLockボリュームでサポートされます。LUNは読み取り/書き込みSnapLockボリュームではサポートされません。ただし、改ざん防止スナップショットは、LUNを含むSnapMirrorソースボリュームとデスティネーション ボリュームの両方でサポートされます。

ONTAP 9.10.1以降では、SnapLockボリュームと非SnapLockボリュームを同じアグリゲートに配置できるため、ONTAP 9.10.1を使用している場合はSnapLockアグリゲートを別々に作成する必要はありません。ボリュームの「-snaplock-type」オプションを使用して、SnapLockボリューム タイプ（ComplianceまたはEnterprise）を指定します。ONTAP 9.10.1より前のリリースでは、SnapLockモード（ComplianceまたはEnterprise）はアグリゲートから継承されます。バージョンに依存しないデスティネーション ボリュームはサポートされません。デスティネーション ボリュームの言語設定とソース ボリュームの言語設定が一致している必要があります。

ボルトのデスティネーションであるSnapLockボリュームには、デフォルトの保持期間が割り当てられています。この期間の値は、SnapLock Enterpriseボリュームの場合は最小0年、SnapLock Complianceボリュームの場合は最大30年に最初に設定されます。各NetAppスナップショットは、最初にこのデフォルトの保持期間でコミットされます。必要に応じて、保持期間は後から延長することができます。詳細については、["保持時間の設定の概要"](#)を参照してください。

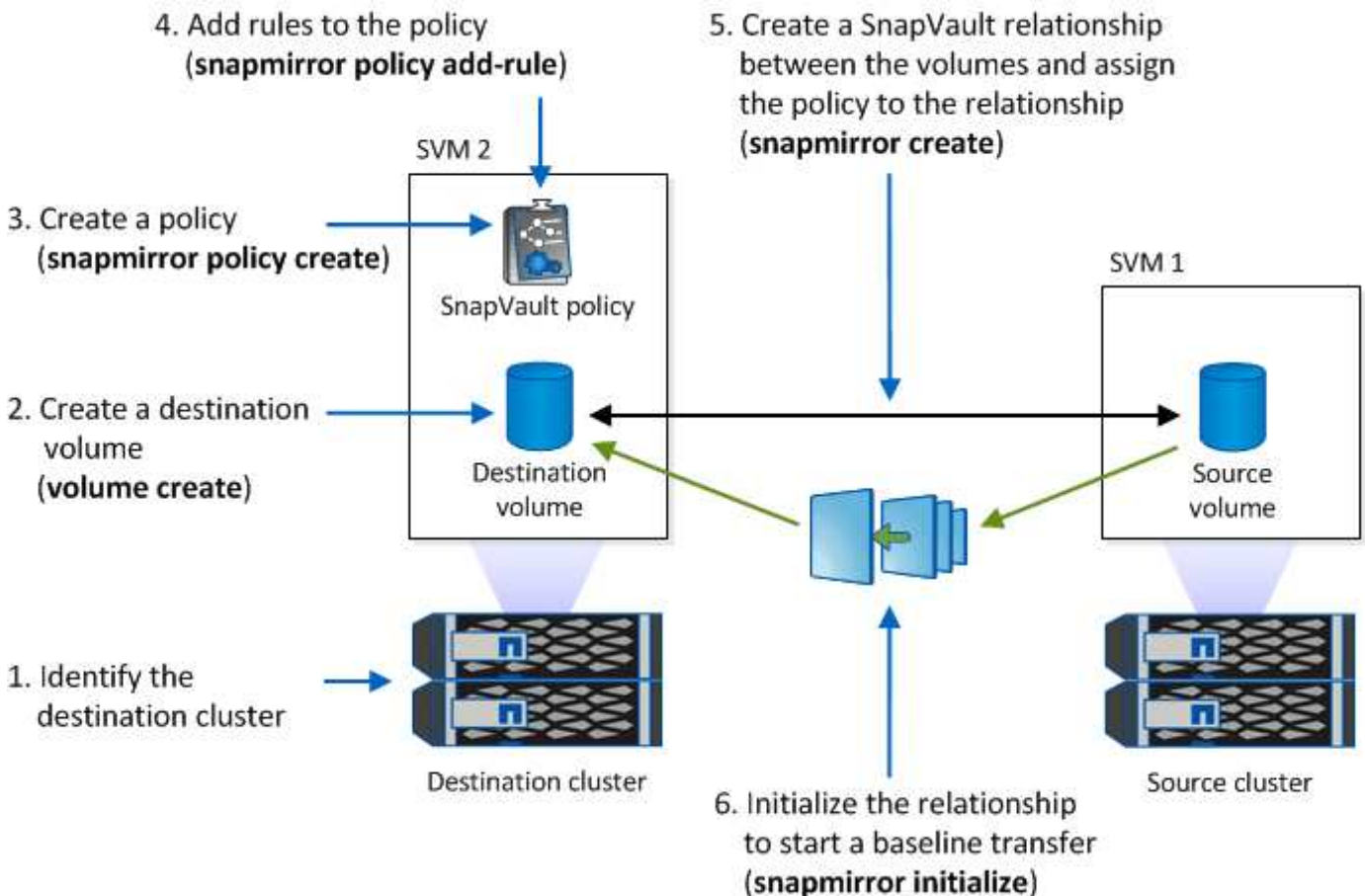
ONTAP 9.14.1以降では、SnapMirror関係のSnapMirrorポリシーで特定のSnapMirrorラベルの保持期間を指定できるようになりました。これにより、ソースボリュームからデスティネーションボリュームにレプリケートされたスナップショットは、ルールで指定された保持期間の間保持されます。保持期間が指定されていない場合は、デスティネーションボリュームのデフォルトの保持期間が使用されます。

ONTAP 9.13.1から、SnapLockボルト関係のデスティネーションSnapLockボリューム上でロックされたスナップショットを、FlexCloneを作成し、`snaplock-type` オプションを `non-snaplock` に設定し、ボリュームクローン作成操作を実行する際にスナップショットを「parent-snapshot」として指定することで、即座にリストアできます。["SnapLockタイプのFlexCloneボリュームを作成する"](#)について詳しくはこちら。

MetroCluster構成の場合は、次の点に注意してください。

- SnapVault関係は、同期元のSVM間でのみ作成できます。同期元のSVMと同期先のSVMの間では作成できません。
- 同期元のSVMのボリュームからデータ提供用のSVMへのSnapVault関係を作成できます。
- データ提供用のSVMのボリュームから同期元のSVMのDPボリュームへのSnapVault関係を作成できます。

次の図は、SnapLockバックアップ関係を初期化する手順を示しています。



手順

ONTAP CLIを使用して、SnapLockバックアップ関係を作成できます。また、ONTAP 9.15.1以降では、System Managerを使用して、SnapLockバックアップ関係を作成できます。

System Manager

1. ボリュームがまだ存在しない場合は、ソース クラスタで*[ストレージ]> に移動し、[追加]*を選択します。
2. *ボリュームの追加*ウィンドウで、*その他のオプション*を選択します。
3. ボリュームの名前、サイズ、エクスポート ポリシー、および共有名を入力します。
4. 変更を保存します。
5. デスティネーション クラスタで、*保護 > 関係*に移動します。
6. *ソース*列の上で、*保護*を選択し、メニューから*ボリューム*を選択します。
7. ボリュームの保護 ウィンドウで、保護ポリシーとして **Vault** を選択します。
8. *ソース*セクションで、保護するクラスタ、Storage VM、ボリュームを選択します。
9. *宛先*セクションの*構成の詳細*で、*宛先スナップショットをロック*を選択し、ロック方法として*SnapLock for SnapVault*を選択します。選択したポリシータイプがタイプ `vault` ではない場合、SnapLockライセンスがインストールされていない場合、またはCompliance Clockが初期化されていない場合、*ロック方法*は表示されません。
10. まだ有効になっていない場合は、*SnapLock Complianceクロックの初期化*を選択します。
11. 変更を保存します。

CLI

1. デスティネーション クラスタで、SnapLockデスティネーション ボリュームのタイプを `DP` ソース ボリュームと同じかそれより大きいサイズで作成します：

```
volume create -vserver <SVM_name> -volume <volume_name> -aggregate  
<aggregate_name> -snaplock-type <compliance|enterprise> -type DP  
-size <size>
```

次のコマンドは、アグリゲート `node01\_aggr` 上の `SVM2` に `dstvolB` という名前の2GBのSnapLock Complianceボリュームを作成します：

```
cluster2::> volume create -vserver SVM2 -volume dstvolB -aggregate  
node01_aggr -snaplock-type compliance -type DP -size 2GB
```

2. デスティネーション クラスタで、["デフォルトの保存期間を設定する"](#)。
3. ["新しいレプリケーション関係を作成する"](#)非SnapLockソースと作成した新しいSnapLockデスティネーションの間。

この例では、SnapMirrorのデスティネーションSnapLockボリューム `dstvolB` との新しい関係を、`XDPDefault` のポリシーを使用して作成します。このポリシーでは、dailyおよびweeklyのラベルが付けられたSnapshotを時間単位のスケジュールでバックアップします。

```
cluster2::> snapmirror create -source-path SVM1:srcvolA -destination  
-path SVM2:dstvolB -vserver SVM2 -policy XDPDefault -schedule hourly
```



"[カスタム レプリケーション ポリシーの作成](#)"または、使用可能なデフォルトが適切でない場合は"[カスタムスケジュール](#)"になります。

4. デスティネーションSVMで、作成したSnapVault関係を初期化します。

```
snapmirror initialize -destination-path <destination_path>
```

次のコマンドは、`SVM1`のソース ボリューム `srcvolA`と `SVM2`のデスティネーション ボリューム `dstvolB`間の関係を初期化します：

```
cluster2::> snapmirror initialize -destination-path SVM2:dstvolB
```

5. 関係が初期化されアイドル状態になったら、デスティネーションで `snapshot show` コマンドを使用して、複製されたSnapshotに適用されたSnapLock有効期限を確認します。

この例では、SnapMirrorラベルとSnapLock有効期限を持つボリューム `dstvolB`上のSnapshotを表示します：

```
cluster2::> snapshot show -vserver SVM2 -volume dstvolB -fields  
snapmirror-label, snaplock-expiry-time
```

関連情報

- "[クラスタとSVMのピアリング](#)"
- "[SnapVaultを使用したボリュームのバックアップ](#)"
- "[snapmirror initialize](#)"

災害復旧のために**ONTAP SnapMirror**で**WORM**ファイルをミラーリングする

SnapMirrorを使用すると、ディザスタ リカバリなどの目的で、地理的に離れた別の場所にWORMファイルをレプリケートできます。ソース ボリュームとデスティネーション ボリュームの両方でSnapLockが設定されていて、両方のボリュームのSnapLockモード（ComplianceまたはEnterprise）が同じである必要があります。ボリュームとファイルの主要なSnapLockプロパティがすべてレプリケートされます。

前提条件

ソースボリュームとデスティネーションボリュームは、ピアSVMを含むピアクラスタ内に作成する必要があります。詳細については、"[クラスタとSVMのピアリング](#)"を参照してください。

タスク概要

- ONTAP 9.5以降では、DP（データ保護）タイプの関係ではなく、XDP（拡張データ保護）タイプのSnapMirror関係を使用してWORMファイルをレプリケートできます。XDPモードはONTAPバージョンに依存せず、同じブロックに格納されているファイルを区別できるため、レプリケートされたComplianceモードのボリュームの再同期が大幅に容易になります。既存のDPタイプの関係をXDPタイプの関係に変換する方法については、"[データ保護](#)"を参照してください。
- DPタイプのSnapMirror関係の再同期処理は、SnapLockがデータ損失につながると判断した場合、コンプライアンスモードボリュームで失敗します。再同期処理が失敗した場合は、`volume clone create`コマンドを使用してデスティネーションボリュームのクローンを作成できます。その後、ソースボリュームをクローンと再同期できます。
- SnapLock ボリュームの SnapMirror 関係は、async-mirror タイプの MirrorAllSnapshots ポリシーのみをサポートします。SnapLock ボリュームの保持期間は、そのボリューム内にあるすべての WORM ファイルの中で最大の保持期間によって決まります。デスティネーションはソースの DR コピーであるため、デスティネーションの SnapLock ボリュームの保持期間はソースと同じになります。
- SnapLock Complianceボリューム間のXDPタイプのSnapMirror関係では、関係解除後にデスティネーションのデータがソースから変化している場合も再同期がサポートされます。

再同期時に共通のSnapshotに基づいてソースとデスティネーションの間でデータの相違が検出されると、この相違をキャプチャするためにデスティネーションで新しいSnapshotが作成されます。新しいSnapshotと共通のSnapshotの両方が次の期間ロックされます。

- デスティネーションのボリューム有効期限
- ボリューム有効期限が過ぎているか設定されていない場合、Snapshotは30日間ロックされます。
- デスティネーションに法的保留がある場合、実際のボリューム有効期限はマスクされ、「indefinite」と表示されます。ただし、実際のボリューム有効期限の間、Snapshotはロックされます。

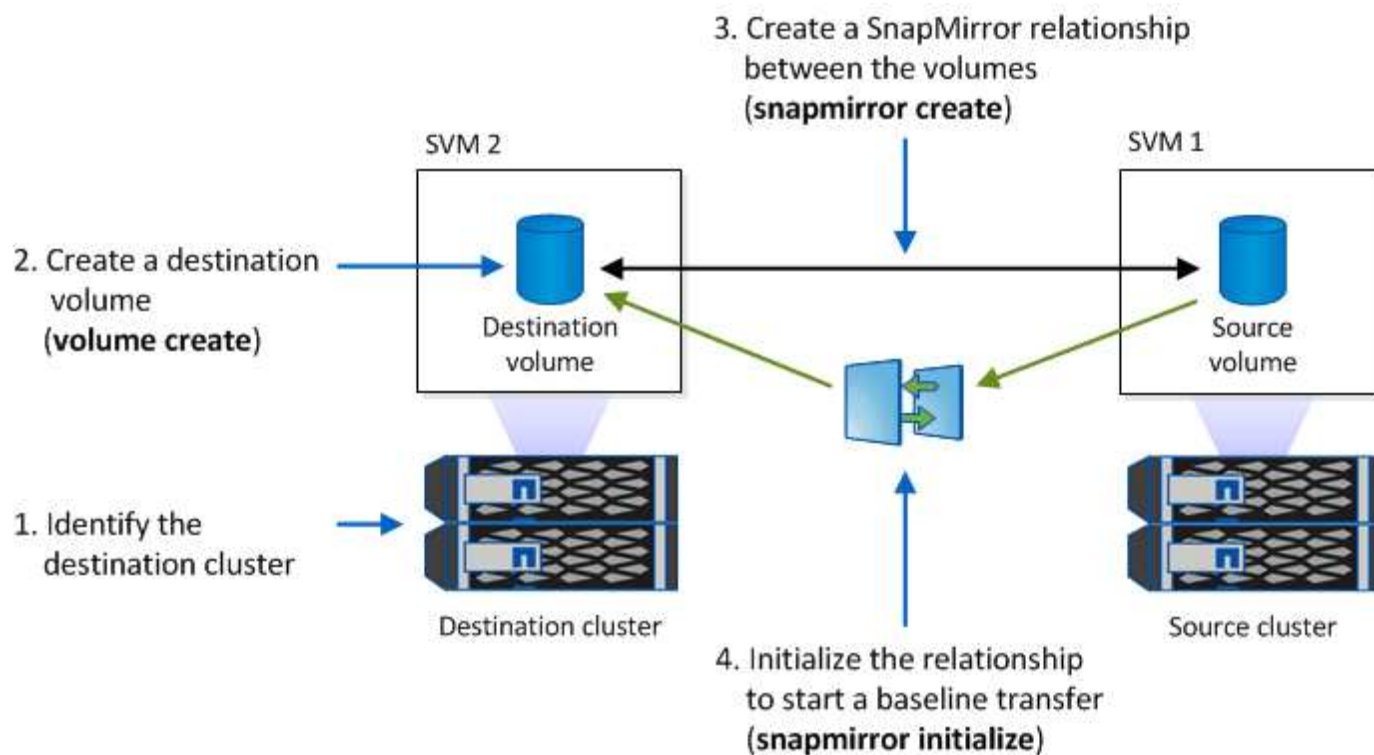
デスティネーション ボリュームの有効期限がソースよりもあとの場合、デスティネーションの有効期限が維持され、再同期後にソース ボリュームの有効期限で上書きされることはありません。

デスティネーションにソースと異なるリーガル ホールドが設定されている場合は、再同期を実行できません。再同期を試行する前に、ソースとデスティネーションに同じリーガル ホールドを設定するか、またはデスティネーションのリーガル ホールドをすべて解除する必要があります。

相違データをキャプチャするために作成された、デスティネーション ボリューム上のロックされたSnapshotは、`snapmirror update -s snapshot`コマンドを実行することでCLIを使用してソースにコピーできます。コピーされたSnapshotは、ソースでも引き続きロックされたままになります。

- SVMデータ保護関係はサポートされません。
- 負荷共有データ保護関係はサポートされません。

次の図は、SnapMirror関係を初期化する手順を示しています。



System Manager

ONTAP 9.12.1以降では、System Managerを使用して、WORMファイルのSnapMirrorレプリケーションを設定できます。

手順

1. *Storage > Volumes*に移動します。
2. *表示 / 非表示*をクリックし、*SnapLockタイプ*を選択すると、*ボリューム*ウィンドウに列が表示されます。
3. SnapLockボリュームを探します。
4.  をクリックして*保護*を選択します。
5. デスティネーション クラスタとデスティネーションStorage VMを選択します。
6. *その他のオプション*をクリックします。
7. **Show legacy policies** を選択し、**DPDefault (legacy)** を選択します。
8. *Destination Configuration details*セクションで、*Override transfer schedule*を選択し、*hourly*を選択します。
9. *保存*をクリックします。
10. ソース ボリューム名の左側にある矢印をクリックしてボリュームの詳細を展開し、ページの右側でリモートSnapMirror保護の詳細を確認します。
11. リモート クラスタで、* Protection Relationships * に移動します。
12. 関係を探し、デスティネーション ボリューム名をクリックして関係の詳細を確認します。
13. デスティネーション ボリュームのSnapLockタイプおよびその他のSnapLock情報を確認します。

CLI

1. デスティネーション クラスタを特定します。
2. デスティネーション クラスタで、["SnapLockライセンスをインストールする"](#)、["Compliance Clockを初期化する"](#)、および ONTAP 9.10.1 より前のリリースを使用している場合は、["SnapLockアグリゲートを作成する"](#)。
3. デスティネーション クラスタで、SnapLockデスティネーション ボリュームのタイプを `DP` ソース ボリュームと同じサイズまたはそれより大きいサイズで作成します：

```
volume create -vserver SVM_name -volume volume_name -aggregate  
aggregate_name -snaplock-type compliance|enterprise -type DP -size size
```



ONTAP 9.10.1以降では、SnapLockボリュームと非SnapLockボリュームを同じアグリゲートに配置できるため、ONTAP 9.10.1を使用している場合はSnapLockアグリゲートを別々に作成する必要はありません。ボリュームの-snaplock-typeオプションを使用して、SnapLockボリューム タイプ（ComplianceまたはEnterprise）を指定します。ONTAP 9.10.1より前のリリースでは、SnapLockモード（ComplianceまたはEnterprise）はアグリゲートから継承されます。デスティネーション ボリュームの言語設定とソース ボリュームの言語設定が一致している必要があります。

次のコマンドは、アグリゲート `node01\_aggr` に `dstvolB` という名前の2 GBのSnapLock `Compliance` ボリュームを `SVM2` に作成します：

```
cluster2::> volume create -vserver SVM2 -volume dstvolB -aggregate  
node01_aggr -snaplock-type compliance -type DP -size 2GB
```

4. デスティネーションSVMで、SnapMirrorポリシーを作成します。

```
snapmirror policy create -vserver SVM_name -policy policy_name
```

次のコマンドは、SVM 全体のポリシー `SVM1-mirror`を作成します：

```
SVM2::> snapmirror policy create -vserver SVM2 -policy SVM1-mirror
```

5. デスティネーションSVMで、SnapMirrorスケジュールを作成します。

```
job schedule cron create -name schedule_name -dayofweek day_of_week -hour  
hour -minute minute
```

次のコマンドは、`weekendcron`という名前のSnapMirrorスケジュールを作成します：

```
SVM2::> job schedule cron create -name weekendcron -dayofweek  
"Saturday, Sunday" -hour 3 -minute 0
```

6. デスティネーションSVMで、SnapMirror関係を作成します。

```
snapmirror create -source-path source_path -destination-path  
destination_path -type XDP|DP -policy policy_name -schedule schedule_name
```

次のコマンドは、`SVM1`のソース ボリューム `srcvolA`と `SVM2`のデスティネーション ボリューム `dstvolB`の間にSnapMirror関係を作成し、ポリシー `SVM1-mirror`とスケジュール `weekendcron`を割り当てます：

```
SVM2::> snapmirror create -source-path SVM1:srcvolA -destination  
-path SVM2:dstvolB -type XDP -policy SVM1-mirror -schedule  
weekendcron
```



XDPタイプはONTAP 9.5以降で使用できます。ONTAP 9.4以前ではDPタイプを使用する必要があります。

7. デスティネーションSVMで、SnapMirror関係を初期化します。

```
snapmirror initialize -destination-path destination_path
```

初期化プロセスでは、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実行されます。SnapMirrorは、ソース ボリュームのSnapshotコピーを作成し、そのコピーとそれが参照するすべてのデータ ブロックをデスティネーション ボリュームに転送します。また、ソース ボリューム上の他のSnapshotコピーもデスティネーション ボリュームに転送されます。

次のコマンドは、`SVM1`のソース ボリューム `srcvolA`と `SVM2`のデスティネーション ボリューム `dstvolB`間の関係を初期化します：

```
SVM2::> snapmirror initialize -destination-path SVM2:dstvolB
```

関連情報

- ["クラスタとSVMのピアリング"](#)
- ["ボリュームのディザスタ リカバリの準備"](#)
- ["データ保護"](#)
- ["snapmirror create"](#)
- ["snapmirror initialize"](#)
- ["snapmirror policy create"](#)

ONTAP SnapLock Legal Holdを使用して訴訟中に**WORM**ファイルを保持

ONTAP 9.3 以降では、*Legal Hold* 機能を使用して、訴訟期間中コンプライアンス モードの WORM ファイルを保持できます。

開始する前に

- このタスクを実行するには、SnapLock管理者である必要があります。

["SnapLock管理者アカウントの作成"](#)

- セキュアな接続（SSH、コンソール、またはZAPI）でログインする必要があります。

タスク概要

リーガル ホールド中のファイルは、保持期間の制限がないWORMファイルのように機能します。リーガル ホールドの期限は管理者が指定する必要があります。

リーガル ホールドとして保存できるファイル数は、ボリュームの使用可能なスペースによって決まります。

手順

1. リーガル ホールドを開始します。

```
snaplock legal-hold begin -litigation-name <litigation_name> -volume  
<volume_name> -path <path_name>
```

次のコマンドは、`vol1`内のすべてのファイルに対して法的保留を開始します：

```
cluster1::>snaplock legal-hold begin -litigation-name litigation1  
-volume vol1 -path /
```

2. リーガル ホールドを終了します。

```
snaplock legal-hold end -litigation-name <litigation_name> -volume  
<volume_name> -path <path_name>
```

次のコマンドは、`vol1`内のすべてのファイルに対する法的保留を終了します：

```
cluster1::> snaplock legal-hold end -litigation-name litigation1 -volume  
vol1 -path /
```

関連情報

- ["SnapLock legal-hold begin"](#)
- ["snaplock リーガルホールド終了"](#)

ONTAP SnapLockでWORMファイルを削除する

privileged delete機能を使用すると、保持期間中にEnterpriseモードのWORMファイルを削除できます。この機能を使用するには、SnapLock管理者アカウントを作成し、そのアカウントを使用して機能を有効にする必要があります。

SnapLock管理者アカウントの作成

SnapLock管理者権限がないと、特権削除を実行できません。これらの権限は、vsadmin-snaplockロールで定義されています。このロールがまだ割り当てられていない場合は、クラスタ管理者に依頼して、SnapLock管理者ロールを持つSVM管理者アカウントを作成してください。

開始する前に

- このタスクを実行するには、クラスタ管理者である必要があります。
- セキュアな接続（SSH、コンソール、またはZAPI）でログインする必要があります。

手順

1. SnapLock管理者ロールが割り当てられたSVM管理者アカウントを作成します。

```
security login create -vserver SVM_name -user-or-group-name user_or_group_name  
-application application -authmethod authentication_method -role role -comment  
comment
```

次のコマンドは、事前定義された`vsadmin-snaplock`ロールを持つ SVM 管理者アカウント`SnapLockAdmin`が、パスワードを使用して`SVM1`にアクセスできるようにします：

```
cluster1::> security login create -vserver SVM1 -user-or-group-name  
SnapLockAdmin -application ssh -authmethod password -role vsadmin-  
snaplock
```

`security login create`の詳細については、[link:https://docs.netapp.com/us-en/ontap-cli/security-login-create.html](https://docs.netapp.com/us-en/ontap-cli/security-login-create.html)["ONTAPコマンド リファレンス"]をご覧ください。

privileged delete機能の有効化

privileged delete機能は、削除するWORMファイルが格納されているEnterpriseボリュームに対して明示的に有効にする必要があります。

タスク概要

`-privileged-delete`オプションの値によって、特権削除が有効かどうかが決まります。指定できる値は`enabled`、`disabled`、`permanently-disabled`です。



`permanently-disabled`は終了状態です。状態を`permanently-disabled`に設定した後は、ボリューム上で特権削除を有効にすることはできません。

手順

1. SnapLock Enterpriseボリュームに対してprivileged deleteを有効にします。

```
volume snaplock modify -vserver SVM_name -volume volume_name -privileged  
-delete disabled|enabled|permanently-disabled
```

次のコマンドは、`SVM1`の Enterprise ボリューム `dataVol`の特権削除機能を有効にします：

```
SVM1::> volume snaplock modify -vserver SVM1 -volume dataVol -privileged  
-delete enabled
```

EnterpriseモードのWORMファイルの削除

privileged delete機能を使用して、保持期間中にEnterpriseモードのWORMファイルを削除できます。

開始する前に

- このタスクを実行するには、SnapLock管理者である必要があります。
- Enterpriseボリュームで、SnapLock監査ログを作成し、privileged delete機能を有効にしておく必要があります。

タスク概要

期限切れのWORMファイルを削除するために、特権削除操作を使用することはできません。`volume file retention show`コマンドを使用して、削除するWORMファイルの保持期間を確認できます。["ONTAPコマンド リファレンス"](#)の`volume file retention show`の詳細をご覧ください。

手順

1. EnterpriseボリュームのWORMファイルを削除します。

```
volume file privileged-delete -vserver SVM_name -file file_path
```

次のコマンドは、SVMsvm1上のファイル`/vol/dataVol/f1`を削除します：

```
SVM1::> volume file privileged-delete -file /vol/dataVol/f1
```

ONTAP SnapLockボリュームを移動する

ONTAP 9.8以降では、SnapLockボリュームを同じタイプのデスティネーション アグリゲートに移動できます（EnterpriseからEnterpriseへの移動またはComplianceからComplianceへの移動）。SnapLockボリュームを移動するには、SnapLockのセキュリティ ロールが割り当てられている必要があります。

SnapLockセキュリティ管理者アカウントの作成

SnapLockボリュームの移動を実行するには、SnapLockセキュリティ管理者権限が必要です。この権限は、ONTAP 9.8で導入された`\_snaplock\_`ロールによって付与されます。このロールがまだ割り当てられていない場合は、クラスタ管理者に依頼して、このSnapLockセキュリティロールを持つSnapLockセキュリティユーザを作成してください。

開始する前に

- このタスクを実行するには、クラスタ管理者である必要があります。
- セキュアな接続（SSH、コンソール、またはZAPI）でログインする必要があります。

タスク概要

snaplockロールは、vsadmin-snaplockロールと違って、データSVMではなく管理SVMに関連付けられます。

手順

1. SnapLock管理者ロールが割り当てられたSVM管理者アカウントを作成します。

```
security login create -vserver SVM_name -user-or-group-name user_or_group_name  
-application application -authmethod authentication_method -role role -comment  
comment
```

次のコマンドを実行すると、事前定義された`\_snaplock\_`ロールを持つ SVM 管理者アカウント`SnapLockAdmin`が、パスワードを使用して管理 SVM `cluster1`にアクセスできるようになります：

```
cluster1::> security login create -vserver cluster1 -user-or-group-name  
SnapLockAdmin -application ssh -authmethod password -role snaplock
```


`security login create`の詳細については、[link:https://docs.netapp.com/us-en/ontap-cli/security-login-create.html](https://docs.netapp.com/us-en/ontap-cli/security-login-create.html)["ONTAPコマンド リファレンス"]をご覧ください。

SnapLockボリュームの移動

`volume move`コマンドを使用して、SnapLockボリュームをデスティネーションアグリゲートに移動できます。

開始する前に

- SnapLockボリュームの移動を実行する前に、SnapLockで保護された監査ログを作成しておく必要があります。

"監査ログの作成"。

- 9.10.1より前のバージョンのONTAPを使用している場合は、デスティネーションアグリゲートのSnapLockタイプが、移動するSnapLockボリュームと同じである必要があります（ComplianceからComplianceへの移動またはEnterpriseからEnterpriseへの移動）。ONTAP 9.10.1以降ではこの制限がなくなり、SnapLock ComplianceボリュームとSnapLock Enterpriseボリュームの両方、および非SnapLockボリュームをアグリゲートに含めることができます。
- SnapLockのセキュリティロールが割り当てられている必要があります。

手順

1. セキュアな接続を使用して、ONTAPクラスタ管理LIFにログインします。

```
ssh snaplock_user@cluster_mgmt_ip
```

2. SnapLockボリュームを移動します。

```
volume move start -vserver SVM_name -volume SnapLock_volume_name -destination  
-aggregate destination_aggregate_name
```

3. ボリューム移動処理の現在のステータスを確認します。

```
volume move show -volume SnapLock_volume_name -vserver SVM_name -fields  
volume,phase,vserver
```

ランサムウェア攻撃から保護するために ONTAP スナップショットをロックする

ONTAP 9.12.1以降では、SnapLock以外のボリュームでスナップショットをロックして、ランサムウェア攻撃からの保護を提供できます。スナップショットをロックすることで、誤ってまたは悪意を持って削除されることを防止できます。

SnapLockコンプライアンスクロック機能を使用すると、スナップショットを指定した期間ロックし、有効期限に達するまで削除できないようにすることができます。スナップショットをロックすることで改ざん防止機能が強化され、ランサムウェアの脅威から保護されます。ランサムウェア攻撃によってボリュームが侵害され

た場合、ロックされたスナップショットを使用してデータをリカバリできます。

ONTAP 9.14.1以降、スナップショットロックはSnapLockヴォールトデスティネーションおよび非SnapLock SnapMirrorデスティネーションボリューム上の長期保存スナップショットをサポートします。スナップショットロックは、[既存のポリシー ラベル](#)に関連付けられたSnapMirrorポリシールールを使用して保存期間を設定することで有効になります。このルールは、ボリュームに設定されているデフォルトの保存期間をオーバーライドします。SnapMirrorラベルに保存期間が関連付けられていない場合は、ボリュームのデフォルトの保存期間が使用されます。

改ざん防止Snapshotの要件と考慮事項

- ONTAP CLIを使用する場合は、クラスタ内のすべてのノードでONTAP 9.12.1以降が実行されている必要があります。System Managerを使用する場合は、すべてのノードでONTAP 9.13.1以降が実行されている必要があります。
- ["SnapLockライセンスはクラスタにインストールする必要があります"](#)。このライセンスは["ONTAP One"](#)に含まれています。
- ["クラスタのコンプライアンスロックを初期化する必要がある"](#)。
- ボリューム上でスナップショット ロックが有効になっている場合、クラスタをONTAP 9.12.1より新しいバージョンのONTAPにアップグレードできます。ただし、ロックされているすべてのスナップショットが有効期限に達して削除され、スナップショット ロックが無効になるまで、以前のバージョンのONTAPに戻すことはできません。
- スナップショットがロックされている場合、ボリュームの有効期限はスナップショットの有効期限に設定されます。複数のスナップショットがロックされている場合、ボリュームの有効期限はすべてのスナップショットの中で最も長い有効期限に設定されます。
- ロックされたスナップショットの保持期間はスナップショット保持数よりも優先されます。つまり、ロックされたスナップショットのスナップショット保持期間が経過していない場合は、保持数の制限は適用されません。
- SnapMirror関係では、ミラー・ヴォールト・ポリシールールに保持期間を設定でき、デスティネーションボリュームでSnapshotロックが有効になっている場合、デスティネーションにレプリケートされたSnapshotに保持期間が適用されます。保持期間は保持数よりも優先されます。たとえば、有効期限が切れていないSnapshotは、保持数を超えても保持されます。
- SnapLock以外のボリュームでスナップショットの名前を変更できます。SnapMirror関係のプライマリボリュームでのスナップショットの名前変更操作は、ポリシーがMirrorAllSnapshotsの場合のみセカンダリボリュームに反映されます。その他のポリシータイプでは、名前が変更されたスナップショットは更新時に伝播されません。
- ONTAP CLIを使用している場合、ロックされたスナップショットが最新のものである場合にのみ、``volume snapshot restore`` コマンドを使用してロックされたスナップショットを復元できます。復元対象のスナップショットよりも後の、有効期限が切れていないスナップショットが存在する場合、スナップショットの復元操作は失敗します。

改ざん防止Snapshotでサポートされる機能

- ["Cloud Volumes ONTAP"](#)
- FlexGroupボリューム

スナップショットロックはFlexGroupボリュームでサポートされています。スナップショットロックはルート構成要素のスナップショットでのみ発生します。ルート構成要素の有効期限が過ぎている場合のみ、FlexGroupボリュームの削除が許可されます。

- FlexVolからFlexGroupへの変換

ロックされたSnapshotを含むFlexVol volumeをFlexGroup volumeに変換できます。変換後もSnapshotはロックされたままです。

- SnapMirror非同期

コンプライアンス クロックは、ソースとデスティネーションの両方で初期化する必要があります。

- SVMデータの移動（ソース クラスタからデスティネーション クラスタにSVMを移行または再配置する場合に使用）

ONTAP 9.14.1以降でサポート。

- ``-schedule``パラメータを使用したSnapMirrorポリシールール
- SVM DR

コンプライアンス クロックは、ソースとデスティネーションの両方で初期化する必要があります。

- ボリューム クローンとファイル クローン

ロックされたスナップショットからボリューム クローンとファイル クローンを作成できます。

- FlexCacheボリューム

ONTAP 9.16.1以降でサポート。

サポートされない機能

現時点では、改ざん防止Snapshotで次の機能はサポートされていません：

- 整合性グループ
- "FabricPool"

改ざん防止スナップショットは、削除できない不変の保護を提供します。FabricPool ではデータを削除する機能が必要なため、FabricPool とスナップショットロックを同じボリュームで有効にすることはできません。

- SMTape
- SnapMirrorアクティブ同期
- SnapMirror Synchronous

ボリューム作成時に**Snapshot**のロックを有効にする

ONTAP 9.12.1以降では、CLIで ``volume create`` コマンドおよび ``volume modify`` コマンドの ``-snapshot-locking-enabled`` オプションを使用することで、新しいボリュームを作成するとき、または既存のボリュームを変更するときに、Snapshotロックを有効にできます。ONTAP 9.13.1以降では、System Managerを使用してSnapshotロックを有効にできます。

System Manager

1. ストレージ > ボリューム に移動し、追加 を選択します。
2. *ボリュームの追加*ウィンドウで、*その他のオプション*を選択します。
3. ボリュームの名前、サイズ、エクスポート ポリシー、および共有名を入力します。
4. *Enable Snapshot locking*を選択します。SnapLockライセンスがインストールされていない場合、この選択は表示されません。
5. まだ有効になっていない場合は、*SnapLock Complianceクロックの初期化*を選択します。
6. 変更を保存します。
7. ボリューム ウィンドウで、更新したボリュームを選択し、概要 を選択します。
8. *SnapLock Snapshot Locking*が*Enabled*として表示されていることを確認します。

CLI

1. 新しいボリュームを作成し、スナップショットのロックを有効にするには、次のコマンドを入力します：

```
volume create -vserver <vserver_name> -volume <volume_name> -snapshot  
-locking-enabled true
```

次のコマンドは、vol1という名前の新しいボリュームでスナップショット ロックを有効にします：

```
> volume create -volume vol1 -aggregate aggr1 -size 100m -snapshot  
-locking-enabled true  
Warning: snapshot locking is being enabled on volume "vol1" in  
Vserver "vs1". It cannot be disabled until all locked snapshots are  
past their expiry time. A volume with unexpired locked snapshots  
cannot be deleted.  
Do you want to continue: {yes|no}: y  
[Job 32] Job succeeded: Successful
```

既存のボリュームでSnapshotロックを有効にする

ONTAP 9.12.1以降では、ONTAP CLIを使用して既存のボリュームのSnapshotロックを有効にできます。ONTAP 9.13.1以降では、System Managerを使用して既存のボリュームのSnapshotロックを有効にできます。

System Manager

1. *Storage > Volumes*に移動します。
2. を選択し、*編集>ボリューム*を選択します。
3. *ボリュームの編集*ウィンドウで、スナップショット（ローカル）設定セクションを見つけて、*スナップショットのロックを有効にする*を選択します。

SnapLockライセンスがインストールされていない場合、このオプションは表示されません。

4. まだ有効になっていない場合は、*SnapLock Complianceクロックの初期化*を選択します。
5. 変更を保存します。
6. ボリューム ウィンドウで、更新したボリュームを選択し、概要 を選択します。
7. *SnapLock Snapshotロック*が*有効*として表示されていることを確認します。

CLI

1. 既存のボリュームを変更してスナップショット ロックを有効にするには、次のコマンドを入力します：

```
volume modify -vserver <vserver_name> -volume <volume_name> -snapshot  
-locking-enabled true
```

ロックされた**Snapshot**ポリシーを作成し、保持を適用する

ONTAP 9.12.1以降では、スナップショットの保持期間を適用するスナップショット ポリシーを作成し、そのポリシーをボリュームに適用して、指定した期間スナップショットをロックできます。また、保持期間を手動で設定してスナップショットをロックすることもできます。ONTAP 9.13.1以降では、System Managerを使用してスナップショット ロック ポリシーを作成し、ボリュームに適用できます。

Snapshotロックポリシーを作成する

System Manager

1. ストレージ > **Storage VM** に移動し、Storage VM を選択します。
2. *設定*を選択します。
3. **Snapshot Policies** を見つけて → を選択します。
4. **Add Snapshot Policy** ウィンドウで、ポリシー名を入力します。
5. **+ Add** を選択します。
6. スケジュール名、保持するスナップショットの最大数、SnapLock 保持期間などのスナップショットスケジュールの詳細を指定します。
7. *SnapLock保持期間*列に、スナップショットを保持する時間、日数、月数、または年数を入力します。たとえば、保持期間が5日のスナップショットポリシーでは、スナップショットが作成されてから5日間ロックされ、その間は削除できません。次の保持期間範囲がサポートされています：
 - 年数：0 - 100
 - 月：0 - 1200
 - 日数：0 - 36500
 - 時間：0 - 24
8. 変更を保存します。

CLI

1. スナップショット ポリシーを作成するには、次のコマンドを入力します：

```
volume snapshot policy create -policy <policy_name> -enabled true  
-schedule1 <schedule1_name> -count1 <maximum snapshots> -retention-period1  
<retention_period>
```

次のコマンドは、スナップショット ロック ポリシーを作成します：

```
cluster1> volume snapshot policy create -policy lock_policy -enabled  
true -schedule1 hourly -count1 24 -retention-period1 "1 days"
```

スナップショットは、アクティブな保持期間中は置き換えられません。つまり、まだ期限が切れていないロックされたスナップショットがある場合、保持カウントは考慮されません。

ボリュームへのロック ポリシーの適用

System Manager

1. *Storage > Volumes*に移動します。
2. を選択し、*編集>ボリューム*を選択します。
3. *ボリュームの編集*ウィンドウで、*スナップショットのスケジュール*を選択します。
4. リストからロック スナップショット ポリシーを選択します。
5. スナップショット ロックがまだ有効になっていない場合は、* Enable snapshot locking * を選択します。
6. 変更を保存します。

CLI

1. 既存のボリュームにスナップショット ロック ポリシーを適用するには、次のコマンドを入力します
:

```
volume modify -volume <volume_name> -vserver <vserver_name> -snapshot  
-policy <policy_name>
```

手動スナップショット作成時に保持期間を適用する

スナップショットを手動で作成する際に、スナップショットの保持期間を適用できます。ボリュームでスナップショットのロックが有効になっている必要があります。有効になっていない場合、保持期間の設定は無視されます。

System Manager

1. **Storage > Volumes** に移動し、ボリュームを選択します。
2. ボリュームの詳細ページで、**Snapshots** タブを選択します。
3. **+ Add** を選択します。
4. スナップショット名とSnapLock有効期限を入力します。カレンダーを選択して、保持期限の日時を選択できます。
5. 変更を保存します。
6. ボリューム > スナップショット ページで、表示/非表示 を選択し、**SnapLock** 有効期限 を選択して **SnapLock** 有効期限 列を表示し、保持時間が設定されていることを確認します。

CLI

1. スナップショットを手動で作成し、ロック保持期間を適用するには、次のコマンドを入力します：

```
volume snapshot create -volume <volume_name> -snapshot <snapshot name>  
-snaplock-expiry-time <expiration_date_time>
```

次のコマンドは、新しいスナップショットを作成し、保持期間を設定します：

```
cluster1> volume snapshot create -vserver vs1 -volume vol1 -snapshot  
snap1 -snaplock-expiry-time "11/10/2022 09:00:00"
```

既存の**Snapshot**に保持期間を適用する

System Manager

1. **Storage > Volumes** に移動し、ボリュームを選択します。
2. ボリュームの詳細ページで、**Snapshots** タブを選択します。
3. スナップショットを選択し、を選択し、*SnapLock有効期限の変更*を選択します。カレンダーを選択して、保持期限の日時を指定できます。
4. 変更を保存します。
5. ボリューム > スナップショット ページで、表示/非表示 を選択し、**SnapLock** 有効期限 を選択して **SnapLock** 有効期限 列を表示し、保持時間が設定されていることを確認します。

CLI

1. 既存のスナップショットに保持期間を手動で適用するには、次のコマンドを入力します：

```
volume snapshot modify-snaplock-expiry-time -volume <volume_name> -snapshot  
<snapshot name> -snaplock-expiry-time <expiration_date_time>
```

次の例では、既存のスナップショットに保持期間を適用します：

```
cluster1> volume snapshot modify-snaplock-expiry-time -volume vol1  
-snapshot snap2 -snaplock-expiry-time "11/10/2022 09:00:00"
```

既存のポリシーの変更による長期保持の適用

SnapMirror関係では、ミラー・ヴォールト・ポリシールールに保持期間を設定でき、デスティネーションボリュームでSnapshotロックが有効になっている場合、デスティネーションにレプリケートされたSnapshotに保持期間が適用されます。保持期間は保持数よりも優先されます。たとえば、有効期限が切れていないSnapshotは、保持数を超えても保持されます。

ONTAP 9.14.1以降では、スナップショットの長期保持を設定するルールを追加することで、既存のSnapMirrorポリシーを変更できます。このルールは、SnapLockヴォールト デスティネーションおよび非SnapLock SnapMirrorデスティネーション ボリュームにおけるデフォルトのボリューム保持期間をオーバーライドするために使用されます。

1. 既存のSnapMirrorポリシーにルールを追加します。

```
snapmirror policy add-rule -vserver <SVM name> -policy <policy name>  
-snapmirror-label <label name> -keep <number of snapshots> -retention-period  
[<integer> days|months|years]
```

次の例では、「lockvault」という既存のポリシーに6カ月の保持期間を適用するルールを作成します。

```
snapmirror policy add-rule -vserver vs1 -policy lockvault -snapmirror  
-label test1 -keep 10 -retention-period "6 months"
```

```
`snapmirror policy add-rule`
```

の詳細については、[link:https://docs.netapp.com/us-en/ontap-cli/snapmirror-policy-add-rule.html](https://docs.netapp.com/us-en/ontap-cli/snapmirror-policy-add-rule.html)["ONTAP コマンド リファレンス"]をご覧ください。

整合性グループ

ONTAP コンシステンシーグループについて学ぶ

整合性グループは、1つの単位として管理されるボリュームの集まりです。ONTAPでは、複数のボリュームにまたがるアプリケーション ワークロードに対し、容易な管理と保護を提供します。

整合性グループを使用すると、シンプルなストレージ管理を実現することができます。20個のLUNにまたがる重要なデータベースが1つあるとします。これらのLUNは、個別に管理することも、独立した整合性グループにまとめて1つのデータセットとして扱うともできます。

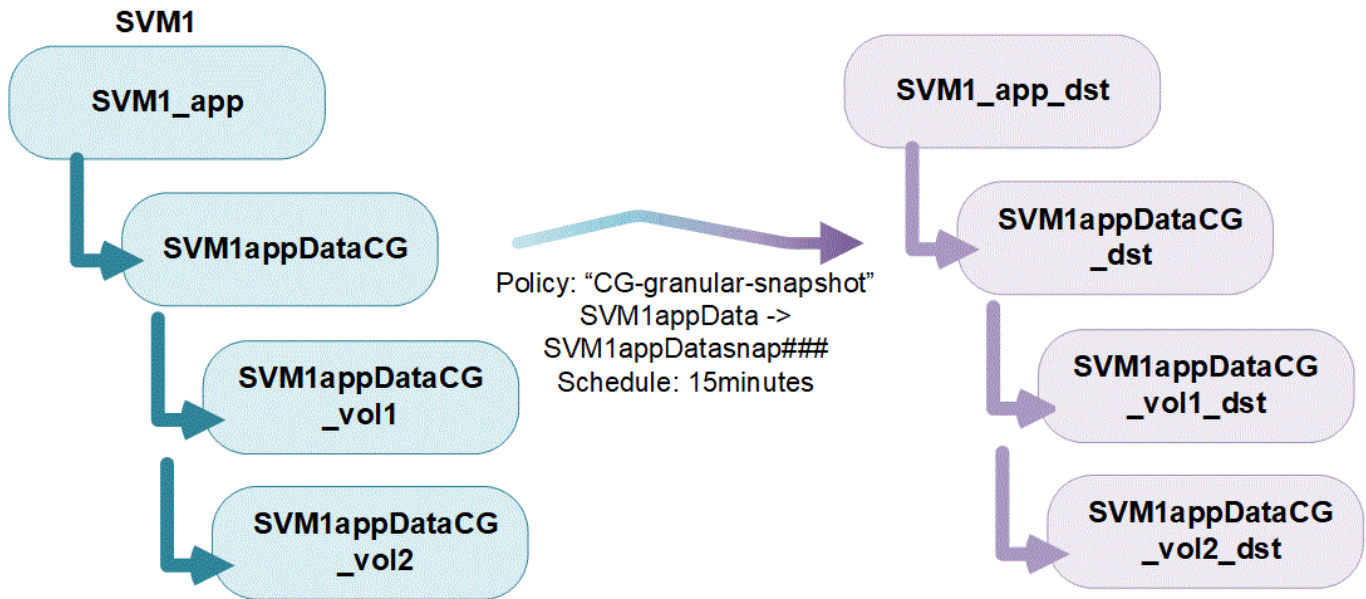
整合性グループはアプリケーション ワークロード管理を容易にし、ローカルおよびリモートの保護ポリシーを容易に設定できるほか、ある時点におけるボリュームの集合体の「crash consistent state（障害など予期しないシャットダウン時と同様）」の状態またはアプリケーション整合性のスナップショットを同時に取得できます。整合性グループのスナップショットにより、アプリケーション ワークロード全体を復元できます。

整合性グループについて

整合性グループは、プロトコル（NAS、SAN、NVMe）を問わずあらゆるFlexVolボリュームをサポートし、ONTAP REST APIまたはSystem Managerの*ストレージ > 整合性グループ*メニュー項目から管理できます。ONTAP 9.14.1以降では、整合性グループはONTAP CLIで管理できます。

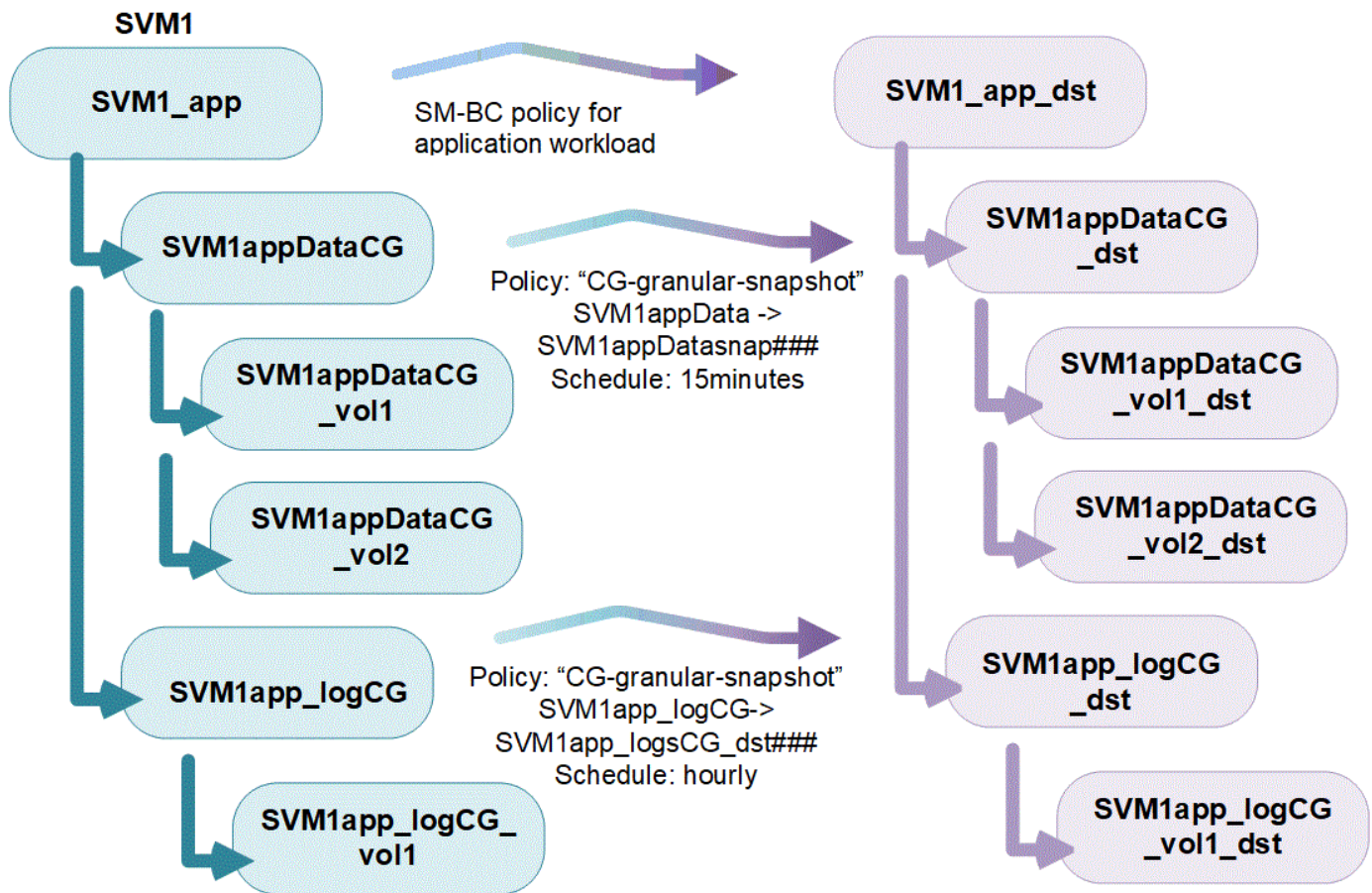
整合性グループは、個別のエンティティ（ボリュームの集まり）として使用することも、他の整合性グループで構成される階層型グループとして設定することもできます。個々のボリュームには、そのボリューム独自のSnapshotポリシーを設定できます。また、整合性グループ全体のSnapshotポリシーを設定することもできます。整合性グループは1つのSnapMirrorアクティブ同期関係とSnapMirrorポリシーをすべてのボリュームで共有し、これらを使用して整合性グループ全体をリカバリします。

次の図は、個々の整合性グループの使用法を示しています。`SVM1`にホストされているアプリケーションのデータは`vol1`と`vol2`の2つのボリュームにまたがっています。整合性グループのスナップショットポリシーは、15分ごとにデータのスナップショットを取得します。



より大規模なアプリケーション ワークロードでは、複数の整合性グループが必要になることがあります。その場合、階層型整合性グループを作成し、整合性グループを親整合性グループの子コンポーネントにすることができます。親整合性グループには、最大5つの子整合性グループを含めることができます。個々の整合性グループと同様に、リモートのSnapMirrorアクティブ同期保護ポリシーを整合性グループ全体（親と子）に適用してアプリケーション ワークロードをリカバリできます。

次の例では、アプリケーションが `SVM1` でホストされています。管理者は親整合性グループ `SVM1\_app` を作成しました。このグループには、データ用の `SVM1appDataCG` とログ用の `SVM1app\_logCG` の2つの子整合性グループが含まれています。各子整合性グループには独自のスナップショットポリシーがあります。`SVM1appDataCG` のボリュームのスナップショットは15分ごとに作成されます。`SVM1app\_logCG` のスナップショットは1時間ごとに作成されます。親整合性グループ `SVM1\_app` にはSnapMirrorアクティブ同期ポリシーがあり、災害発生時にもサービスが継続されるようにデータを複製します。



ONTAP 9.12.1以降、整合性グループは**クローニング**をサポートし、System ManagerとONTAP REST APIの両方で**ボリュームの追加または削除**によって整合性グループのメンバーを変更できます。ONTAP 9.12.1以降、ONTAP REST APIは次の機能もサポートします：

- 新規のNFS / SMBボリュームまたはNVMeネームスペースで整合性グループを作成する。
- 新規または既存のNFS / SMBボリュームまたはNVMeネームスペースを既存の整合性グループに追加する。

ONTAP REST APIの詳細については、"[ONTAP REST APIリファレンスドキュメント](#)"を参照してください。

整合性グループの監視

ONTAP 9.13.1以降の整合性グループは、リアルタイムおよび過去の容量とパフォーマンスを監視し、アプリケーションや個々の整合性グループのパフォーマンスに関する分析情報を提供します。

監視データは5分ごとに更新され、最長1年間にわたって保持されます。追跡可能な指標は次のとおりです。

- パフォーマンス：IOPS、レイテンシ、スループット
- 容量：サイズ、論理使用済み、使用可能

監視データは、System Managerのコンシステンシ・グループ・メニューの概要タブ、またはREST APIで要求することで表示できます。ONTAP 9.14.1以降では、`consistency-group metrics show` コマンドを使用してCLIでコンシステンシ・グループのメトリックを表示できます。`consistency-group metrics show`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。



ONTAP 9.13.1では、REST APIを使用した場合にのみ履歴メトリックを取得できます。ONTAP 9.14.1以降では、System Managerでも履歴メトリックを取得できます。

整合性グループの保護

整合性グループは、アプリケーション整合性のある保護を提供し、複数のボリュームまたはLIFにわたるデータの整合性を保証します。整合性グループのスナップショットを作成すると、整合性グループに「フェンス」が確立されます。フェンスは、スナップショット処理が完了するまでI/Oのキューを開始し、整合性グループ内のすべてのエンティティ間でデータのポイントインタイム整合性を保証します。ただし、スケジュールされたスナップショットポリシーやSystem Managerを使用したスナップショットの作成など、スナップショット作成処理中に、フェンスによって一時的なレイテンシの急増が発生する可能性があります。REST APIとCLIの詳細については、"[ONTAP REST APIドキュメント](#)"および"[ONTAPコマンド リファレンス](#)"をご覧ください。

整合性グループは、次の方法で保護できます。

- Snapshotポリシー
- [SnapMirrorアクティブ同期](#)
- [\[mcc\]](#) (ONTAP 9.11.1以降)
- [SnapMirror非同期](#) (ONTAP 9.13.1以降)
- "[SVMディザスタ リカバリ](#)" (ONTAP 9.14.1以降)

整合性グループを作成しても、保護が自動的に有効になるわけではありません。ローカル保護ポリシーとリモート保護ポリシーは、整合性グループの作成時または作成後に設定できます。

整合性グループの保護を構成するには、"[整合性グループの保護](#)"を参照してください。

リモート保護を使用するには、[SnapMirrorアクティブ同期](#)の要件を満たしている必要があります。



NASアクセス用にマウントされたボリュームではSnapMirrorアクティブ同期関係を確立できません。

整合性グループでのマルチ管理者認証のサポート

ONTAP 9.16.1以降では、整合性グループでマルチ管理者認証（MAV）を使用して、整合性グループの作成、変更、削除などの特定の処理を、指定した管理者からの承認がないと実行できないようにすることができます。これにより、侵害を受けた管理者、悪意のある管理者、または経験の浅い管理者が、既存の設定に望ましくない変更を行えないようにすることができます。

["詳細情報"](#)

MetroCluster構成の整合性グループ

ONTAP 9.11.1以降では、MetroCluster構成内のクラスタにある新しいボリュームで整合性グループをプロビジョニングできます。これらのボリュームはミラーされたアグリゲートにプロビジョニングされます。

プロビジョニングが完了したら、整合性グループに関連付けられているボリュームを、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の間で移動できます。つまり、ミラーされたアグリゲート、ミラーされていないアグリゲート、またはその両方に、整合性グループに関連付けられているボリュームを配置できます。整合性グループに関連付けられているボリュームを含む、ミラーされたアグリゲートを、ミラーされてい

ないアグリゲートに変更することができます。同様に、整合性グループに関連付けられているボリュームを含む、ミラーされていないアグリゲートを変更して、ミラーリングを有効にすることもできます。

ミラーリングされたアグリゲートに配置されたコンシステンシ・グループに関連付けられたボリュームとスナップショットは、リモートサイト（サイトB）に複製されます。サイトBのボリュームの内容は、コンシステンシ・グループの書き込み順序を保証するため、災害発生時にはサイトBからリカバリできます。ONTAP 9.11.1以降を実行しているクラスターでは、REST APIとSystem Managerを使用してコンシステンシ・グループのスナップショットにアクセスできます。ONTAP 9.14.1以降では、ONTAP CLIを使用してスナップショットにアクセスすることもできます。

整合性グループに関連付けられているボリュームの一部またはすべてがミラーされていないアグリゲートに配置されていて、そのアグリゲートに現在アクセスできない場合、整合性グループに対するGETまたはDELETE処理はローカル ボリュームまたはホスティング アグリゲートがオフラインであるかのように動作します。

レプリケーション用の整合性グループ設定

サイトBでONTAP 9.10.1以前が実行されている場合は、整合性グループに関連付けられているボリュームのうち、ミラーされたアグリゲートにあるボリュームだけがサイトBにレプリケートされます。整合性グループの設定がレプリケートされるのは、両方のサイトでONTAP 9.11.1以降が実行されている場合のみです。サイトBをONTAP 9.11.1にアップグレードすると、サイトAの整合性グループのうち、関連付けられているボリュームがすべてミラーされたアグリゲートに配置されている整合性グループのデータが、サイトBにレプリケートされます。



ストレージのパフォーマンスと可用性を最適化するために、ミラーリングされたアグリゲートには少なくとも20%の空きスペースを確保することをお勧めします。ミラーリングされていないアグリゲートの場合は10%が推奨されていますが、追加の10%のスペースはファイルシステムによって増分変更の吸収に使用される可能性があります。ONTAPのリダイレクトオンライトスナップショットベースのアーキテクチャにより、増分変更はミラーリングされたアグリゲートのスペース使用率を増加させます。これらのベストプラクティスを遵守しないと、パフォーマンスに悪影響を与える可能性があります。

アップグレード時の考慮事項

ONTAP 9.10.1以降にアップグレードすると、ONTAP 9.8および9.9.1でSnapMirror Active Sync（旧称SnapMirror Business Continuity）を使用して作成されたコンシステンシグループは自動的にアップグレードされ、System ManagerまたはONTAP REST APIの*Storage > Consistency Groups*で管理できるようになります。ONTAP 9.8または9.9.1からのアップグレードの詳細については、"[SnapMirror Active Sync のアップグレードと復元に関する考慮事項](#)"を参照してください。

REST APIで作成された整合性グループSnapshotは、System Managerの整合性グループインターフェイスおよび整合性グループREST APIエンドポイントを通じて管理できます。ONTAP 9.14.1以降では、整合性グループSnapshotはONTAP CLIでも管理できます。



ONTAPIコマンド `cg-start` および `cg-commit` で作成されたスナップショットは、コンシステンシグループスナップショットとして認識されないため、System ManagerのコンシステンシグループインターフェイスまたはONTAP REST APIのコンシステンシグループエンドポイントでは管理できません。ONTAP 9.14.1以降では、SnapMirror非同期ポリシーを使用している場合、これらのスナップショットをデスティネーションボリュームにミラーリングできます。詳細については、[SnapMirror非同期の設定](#)を参照してください。

リリース別のサポートされる機能

	ONTAP 9.16.1	ONTAP 9.15.1	ONTAP 9.14.1	ONTAP 9.13.1	ONTAP 9.12.1	ONTAP 9.11.1	ONTAP 9.10.1
階層型整合性グループ	✓	✓	✓	✓	✓	✓	✓
スナップショットによるローカル保護	✓	✓	✓	✓	✓	✓	✓
SnapMirrorアクティブ同期	✓	✓	✓	✓	✓	✓	✓
MetroClusterのサポート	✓	✓	✓	✓	✓	✓	
2フェーズ コミット (REST APIのみ)	✓	✓	✓	✓	✓	✓	
アプリケーション タグとコンポーネント タグ	✓	✓	✓	✓	✓		
整合性グループのクローニング	✓	✓	✓	✓	✓		
ボリュームの追加と削除	✓	✓	✓	✓	✓		
新しいNASボリュームを使用した整合性グループの作成	✓	✓	✓	✓	REST APIのみ		
新しいNVMeネームスペースを使用した整合性グループの作成	✓	✓	✓	✓	REST APIのみ		
子整合性グループ間でのボリュームの移動	✓	✓	✓	✓			
整合性グループのジオメトリの変更	✓	✓	✓	✓			
監視	✓	✓	✓	✓			
マルチ管理者認証	✓						
SnapMirror非同期 (独立した整合性グループのみ)	✓	✓	✓	✓			
SVMディザスタ リカバリ (独立した整合性グループのみ)	✓	✓	✓				
CLIのサポート	✓	✓	✓				

整合性グループに関する詳細情報

Consistency Groups for Application Management & Protection

With NetApp ONTAP 9.10.1 + System Manager



 NetApp

© 2022 NetApp, Inc. All rights reserved.

関連情報

- ["ONTAP自動化ドキュメント"](#)
- [SnapMirrorアクティブ同期](#)
- [SnapMirror非同期のディザスタ リカバリの基本](#)
- ["MetroClusterのドキュメント"](#)
- ["マルチ管理者認証"](#)
- ["ONTAPコマンド リファレンス"](#)

ONTAP整合性グループの制限について学ぶ

整合性グループを計画および管理する場合は、クラスタレベルおよび親または子の整合性グループレベルにおけるオブジェクト数の制限を考慮してください。

適用される制限

以下の表は、整合性グループの制限を示しています。SnapMirrorアクティブシンクを使用する整合性グループには、別の制限が適用されます。詳細については、["SnapMirror アクティブ同期の制限"](#)をご覧ください。

制限	Scope	最小	最大
整合性グループの数	クラスタ	0	クラスター内の最大ボリューム数と同じ*
親整合性グループの数	クラスタ	0	クラスターの最大ボリューム数と同じ

個々の整合性グループと親整合性グループの数	クラスタ	0	クラスタの最大ボリューム数と同じ
整合性グループのボリューム数	独立した整合性グループ	1ボリューム	80ボリューム
SnapMirror非同期を使用する整合性グループ内のボリューム数	独立した整合性グループ	1ボリューム	• ONTAP 9.15.1以降：80ボリューム • ONTAP 9.13.1および9.14.1の場合：16ボリューム
親整合性グループの子のボリューム数	親整合性グループ	1ボリューム	80ボリューム
子整合性グループのボリューム数	子整合性グループ	1ボリューム	80ボリューム
親整合性グループの子整合性グループの数	親整合性グループ	1つの整合性グループ	5つの整合性グループ
整合性グループが存在するSVMディザスタリカバリ関係の数（ONTAP 9.14.1以降で使用可能）	クラスタ	0	32

*SnapMirror非同期が有効になっている整合性グループをクラスター上で最大50個ホストできます。

適用されない制限

整合性グループでサポートされる最小スナップショットスケジュールは30分です。これは["FlexGroupボリュームのテスト"](#)に基づいています。整合性グループと同じSnapshotインフラストラクチャを共有しています。

単一のONTAPコンシステンシグループを構成する

整合性グループは、ONTAPのバージョンに応じて、既存のボリュームまたは新しいLUN / ボリュームを使用して作成できます。ボリュームまたはLUNを関連付けることのできる整合性グループは一度に1つだけです。

タスク概要

- ONTAP 9.10.1～9.11.1では、整合性グループの作成後にメンバー ボリュームを変更することはできません。

ONTAP 9.12.1以降では、コンシステンシーグループのメンバーボリュームを変更できるようになりました。このプロセスの詳細については、[整合性グループの変更](#)を参照してください。

- ONTAP 9.17.1 以降では、NVMe プロトコルを選択して、SnapMirror アクティブ同期構成で VMware ワークロードの NVMe サブシステムにホストをマッピングできます。

新しいLUNまたはボリュームを使用した整合性グループの作成

ONTAP 9.10.1～9.12.1では、新しいLUNを使用して整合性グループを作成できます。ONTAP 9.13.1以降のSystem Managerでは、整合性グループの作成に新しいNVMeネームスペースまたは新しいNASボリューム

も使用できます。（これは、ONTAP 9.12.1以降のONTAP REST APIでもサポートされています）。

System Manager (ONTAP 9.16.1以前)

手順

1. *Storage > Consistency groups*を選択します。
2. *+追加*を選択し、ストレージ オブジェクトのプロトコルを選択します。

ONTAP 9.10.1～9.12.1では、新しいストレージオブジェクトのオプションは新しい**LUN**を使用するのみです。ONTAP 9.13.1以降、System Managerは新しいNVMeネームスペースと新しいNASボリュームを使用したコンシステンシグループの作成をサポートします。

3. 整合性グループに名前を付けます。ボリュームまたはLUNの数とボリュームまたはLUNあたりの容量を指定します。
 - a. アプリケーションタイプ：ONTAP 9.12.1以降を使用している場合は、アプリケーションタイプを選択してください。値が選択されていない場合、整合性グループにはデフォルトでその他のタイプが割り当てられます。整合性のタグ付けの詳細については、[アプリケーション タグとコンポーネント タグ](#)を参照してください。リモート保護ポリシーを使用して整合性グループを作成する場合は、*その他*を使用する必要があります。
 - b. 新しい**LUN**の場合：ホストのオペレーティングシステムとLUNフォーマットを選択します。ホストイニシエータ情報を入力します。
 - c. 新しい **NAS** ボリュームの場合：SVM の NAS 構成に基づいて適切なエクスポート オプション (NFS または SMB/CIFS) を選択します。
 - d. 新しい **NVMe** 名前空間の場合：ホスト オペレーティング システムと NVMe サブシステムを選択します。
4. 保護ポリシーを構成したり、子整合性グループやアクセス権限を追加したりするには、*その他のオプション*を選択します。
5. *保存*を選択します。
6. メインの整合性グループメニューに戻り、整合性グループが作成されたことを確認します。保護ポリシーを設定した場合は、該当するリモートまたはローカルのポリシーに表示される緑色の盾アイコンで、保護ポリシーが適用されたことを確認できます。

System Manager (ONTAP 9.17.1以降)

手順

1. *保護 > 整合性グループ*を選択します。
2. *+追加*を選択し、ストレージ オブジェクトのプロトコルを選択します。
3. 整合性グループに名前を付けます。ボリュームまたはLUNの数と、ボリュームまたはLUNあたりの容量を指定します。アプリケーションタイプ：アプリケーションタイプを選択します。値が選択されていない場合、整合性グループにはデフォルトでその他のタイプが割り当てられます。整合性のタグ付けの詳細については、[アプリケーション タグとコンポーネント タグ](#)を参照してください。リモート保護ポリシーを使用して整合性グループを作成する場合は、*その他*を使用する必要があります。
 - a. 新しい**LUN**の場合：ホストのオペレーティングシステムとLUNフォーマットを選択します。ホストイニシエータ情報を入力します。
 - b. 新しい **NAS** ボリュームの場合：SVM の NAS 構成に基づいて適切なエクスポート オプション (NFS または SMB/CIFS) を選択します。
 - c. 新しい **NVMe** 名前空間の場合：ホスト オペレーティング システムと NVMe サブシステムを選択します。

4. 保護ポリシーを構成したり、子整合性グループやアクセス権限を追加したりするには、*その他のオプション*を選択します。
5. *保存*を選択します。
6. メインの整合性グループメニューに戻り、整合性グループが作成されたことを確認します。保護ポリシーを設定した場合は、該当するリモートまたはローカルのポリシーに表示される緑色の盾アイコンで、保護ポリシーが適用されたことを確認できます。

CLI

ONTAP 9.14.1以降では、ONTAP CLIを使用して、新しいボリュームを使用した新しい整合性グループを作成できます。指定するパラメータは、SAN、NVMe、NFSのうち、どのボリュームを使用するかによって異なります。

開始する前に

- このタスクを実行するには、admin権限レベルが必要です。
- ONTAP 9.15.1以降では、admin権限レベルのすべてのユーザがこのタスクを実行できます。ONTAP 9.14.1では、このタスクを実行するには、クラスタ管理者またはSVMの管理者である必要があります。

NFSボリュームを使用した整合性グループの作成

1. 整合性グループを作成します。

```
consistency-group create -vserver <SVM_name> -consistency-group  
<consistency-group-name> -volume-prefix <prefix_for_new_volume_names>  
-volume-count <number> -size <size> -export-policy <policy_name>
```

SANボリュームを使用した整合性グループの作成

1. 整合性グループを作成します。

```
consistency-group create -vserver <SVM_name> -consistency-group  
<consistency-group-name> -lun <lun_name> -size <size> -lun-count <number>  
-lun-os-type <LUN_operating_system_format> -igroup <igroup_name>
```

NVMeネームスペースを使用した整合性グループの作成

1. 整合性グループを作成します。

```
consistency-group create -vserver <SVM_name> -consistency-group  
<consistency_group_name> -namespace <namespace_name> -volume-count <number>  
-namespace-count <number> -size <size> -subsystem <subsystem_name>
```

["ONTAPコマンド リファレンス"](#)の`consistency-group create`の詳細をご覧ください。

完了後

1. `consistency-group show`コマンドを使用して、整合性グループが作成されたことを確認します。

```
`consistency-group show`
```

の詳細については、[link:https://docs.netapp.com/us-en/ontap-cli/search.html?q=consistency-group+show](https://docs.netapp.com/us-en/ontap-cli/search.html?q=consistency-group+show)["ONTAP コマンド リファレンス"]を参照してください。

既存のボリュームを使用した整合性グループの作成

既存のボリュームを使用して整合性グループを作成できます。

System Manager (ONTAP 9.16.1以前)

手順

1. *Storage > Consistency groups*を選択します。
2. *+追加*を選択し、次に*既存のボリュームを使用*を選択します。
3. 整合性グループに名前を付け、Storage VMを選択します。
 - a. アプリケーションタイプ：ONTAP 9.12.1以降をご使用の場合は、アプリケーションタイプを選択してください。値が選択されていない場合、コンシステンシーグループにはデフォルトでその他のタイプが割り当てられます。コンシステンシーのタグ付けの詳細については、[アプリケーション タグとコンポーネント タグ](#)を参照してください。コンシステンシーグループにSnapMirrorアクティブ同期関係がある場合は、*その他*を使用する必要があります。



ONTAP 9.15.1より前のバージョンのONTAPでは、SnapMirrorアクティブ同期をSnapMirrorビジネス継続性と呼びます。

4. グループに追加する既存のボリュームを選択します。選択できるのは、整合性グループに含まれていないボリュームのみです。



既存のボリュームで作成する整合性グループでは、FlexVolがサポートされません。SnapMirror同期関係またはSnapMirror非同期関係が設定されたボリュームは整合性グループには対応していませんが、整合性グループに追加することはできます。整合性グループでは、S3バケットまたはSVM DR関係が確立されたStorage VMはサポートされません。

5. *保存*を選択します。
6. メインの整合性グループのメニューに戻り、整合性グループが作成されたことを確認します。保護ポリシーを選択した場合は、メニューから作成した整合性グループを選択して、ポリシーが適切に設定されていることを確認します。保護ポリシーを設定した場合は、該当するリモートまたはローカルのポリシーに表示される緑色の盾アイコンで、保護ポリシーが適用されたことを確認できます。

CLI

ONTAP 9.14.1以降では、ONTAP CLIを使用して、既存のボリュームを使用した整合性グループを作成できます。

開始する前に

- このタスクを実行するには、admin権限レベルが必要です。
- ONTAP 9.15.1以降では、admin権限レベルのすべてのユーザがこのタスクを実行できます。ONTAP 9.14.1では、このタスクを実行するには、クラスタ管理者またはSVMの管理者である必要があります。

手順

1. `consistency-group create` コマンドを発行します。 `-volumes` パラメータには、ボリューム名をカンマで区切って指定できます。

```
consistency-group create -vserver <SVM_name> -consistency-group  
<consistency-group-name> -volume <volumes>
```

["ONTAPコマンド リファレンス"](#)の `consistency-group create` の詳細をご覧ください。

2. `consistency-group show` コマンドを使用して整合性グループを表示します。

```
`consistency-group show`  
の詳細については、link:https://docs.netapp.com/us-en/ontap-cli/search.html?q=consistency-group+show["ONTAP コマンド リファレンス  
"^] を参照してください。
```

次の手順

- [整合性グループの保護](#)
- [整合性グループの変更](#)
- [整合性グループのクローニング](#)

階層型ONTAPコンシステンシグループを構成する

階層型整合性グループを使えば、子整合性グループの統括を担う親整合性グループを作成し、複数のボリュームにわたる大規模なワークロードを管理できます。

階層型整合性グループには親があり、親には最大5つの個別の整合性グループを含めることができます。階層型整合性グループは、整合性グループ全体または個々のボリュームごとに異なるローカルスナップショットポリシーをサポートできます。リモート保護ポリシーを使用する場合、そのポリシーは階層型整合性グループ全体（親と子）に適用されます。

ONTAP 9.13.1以降では、[整合性グループのジオメトリを変更する](#)および[子整合性グループ間でボリュームを移動する](#)が可能になります。

整合性グループのオブジェクト制限については、[整合性グループのオブジェクト制限](#)を参照してください。

新しいLUNまたはボリュームを使用した階層型整合性グループの作成

階層型整合性グループを作成する際、そのグループに新しいLUNを設定できます。ONTAP 9.13.1以降では、新しいNVMeネームスペースとNASボリュームを使用することもできます。

System Manager

手順

1. *Storage > Consistency groups*を選択します。
2. *+追加*を選択し、ストレージ オブジェクトのプロトコルを選択します。

ONTAP 9.10.1～9.12.1では、新しいストレージオブジェクトのオプションは新しい**LUN**を使用するのみです。ONTAP 9.13.1以降、System Managerは新しいNVMeネームスペースと新しいNASボリュームを使用したコンシステンシグループの作成をサポートします。

3. 整合性グループに名前を付けます。ボリュームまたはLUNの数とボリュームまたはLUNあたりの容量を指定します。
 - a. アプリケーションタイプ：ONTAP 9.12.1以降をご使用の場合は、アプリケーションタイプを選択してください。値が選択されていない場合、整合性グループにはデフォルトでその他のタイプが割り当てられます。[アプリケーション タグとコンポーネント タグ](#)で整合性のタグ付けの詳細をご確認ください。リモート保護ポリシーを使用する場合は、*その他*を選択する必要があります。
4. ホスト オペレーティング システムとLUN形式を選択します。ホスト イニシエータの情報を入力します。
 - a. 新しい**LUN**の場合：ホストのオペレーティングシステムとLUNフォーマットを選択します。ホストイニシエータ情報を入力します。
 - b. 新しい **NAS** ボリュームの場合：SVM の NAS 構成に基づいて適切なエクスポート オプション (NFS または SMB/CIFS) を選択します。
 - c. 新しい **NVMe** 名前空間の場合：ホスト オペレーティング システムと NVMe サブシステムを選択します。
5. 子整合性グループを追加するには、[その他のオプション] を選択し、[+ 子整合性グループの追加] を選択します。
6. パフォーマンス レベル、LUNまたはボリュームの数、LUNまたはボリュームあたりの容量を選択します。使用しているプロトコルに基づいて、適切なエクスポート設定またはオペレーティング システム情報を指定します。
7. 必要に応じて、ローカルSnapshotポリシーを選択し、アクセス権限を設定します。
8. 最大5つの子整合性グループについて、同じ手順を繰り返します。
9. *保存*を選択します。
10. メインの整合性グループのメニューに戻り、整合性グループが作成されたことを確認します。保護ポリシーを設定した場合は、該当するリモートまたはローカルのポリシーにチェックマーク付きの緑色の盾アイコンが表示されることを確認します。

CLI

開始する前に

- このタスクを実行するには、admin権限レベルが必要です。
- ONTAP 9.15.1以降では、admin権限レベルのすべてのユーザがこのタスクを実行できます。ONTAP 9.14.1では、このタスクを実行するには、クラスタ管理者またはSVMの管理者である必要があります。

CLIで新しいボリュームを含む階層型整合性グループを作成する場合は、子整合性グループをそれぞれ個別に作成する必要があります。

手順

1. `consistency-group create` コマンドを使用して新しい整合性グループを作成します。

```
consistency-group create -vserver <SVM_name> -consistency-group  
<consistency_group_name> -parent-consistency-group  
<parent_consistency_group_name> -volume-prefix <volume_prefix> -volume  
-count <number_of_volumes> -size <size>
```

2. CLI のプロンプトが表示されたら、新しい親コンシステンシー グループを作成することを確認します。`y`と入力します。
3. 必要に応じて、手順1を繰り返して子整合性グループをさらに作成します。

"[ONTAP コマンド リファレンス](#)"の `consistency-group create` の詳細をご覧ください。

既存のボリュームを使用した階層型整合性グループの作成

既存のボリュームを階層型整合性グループにまとめることができます。

System Manager

手順

1. *Storage > Consistency groups*を選択します。
2. *+追加*を選択し、次に*既存のボリュームを使用*を選択します。
3. Storage VMを選択します。
4. グループに追加する既存のボリュームを選択します。選択できるのは、整合性グループに含まれていないボリュームのみです。
5. 子整合性グループを追加するには、*+子整合性グループの追加*を選択します。必要な整合性グループを作成します。名前は自動的に付けられます。
 - a. コンポーネントタイプ：ONTAP 9.12.1以降を使用している場合は、「data」、「logs」、または「other」のコンポーネントタイプを選択します。値が選択されていない場合、整合性グループにはデフォルトで**Other**のタイプが割り当てられます。整合性のタグ付けの詳細については、[アプリケーション タグとコンポーネント タグ](#)を参照してください。リモート保護ポリシーを使用する場合は、*Other*を使用する必要があります。
6. 各整合性グループに既存のボリュームを割り当てます。
7. 必要に応じて、ローカル スナップショット ポリシーを選択します。
8. 最大5つの子整合性グループについて、同じ手順を繰り返します。
9. *保存*を選択します。
10. メインの整合性グループのメニューに戻り、整合性グループが作成されたことを確認します。保護ポリシーを選択した場合は、ポリシーが適切に設定されていることを確認します。作成した整合性グループをメニューから選択すると、該当するポリシータイプに、チェックマークが付いた緑色の盾アイコンが表示されます。

CLI

ONTAP 9.14.1以降では、CLIを使用して階層型整合性グループを作成できます。

開始する前に

- このタスクを実行するには、admin権限レベルが必要です。
- ONTAP 9.15.1以降では、admin権限レベルのすべてのユーザがこのタスクを実行できます。ONTAP 9.14.1では、このタスクを実行するには、クラスタ管理者またはSVMの管理者である必要があります。

手順

1. 新しい親整合性グループをプロビジョニングし、新しい子整合性グループにボリュームを割り当てます。

```
consistency-group create -vserver <svm_name> -consistency-group  
<child_consistency_group_name> -parent-consistency-group  
<parent_consistency_group_name> -volumes <volume_names>
```

2. `y`を入力して、新しい親と子の整合性グループを作成することを確認します。

["ONTAPコマンド リファレンス"](#)の `consistency-group create` の詳細をご覧ください。

次の手順

- [整合性グループのジオメトリの変更](#)
- [整合性グループの変更](#)
- [整合性グループの保護](#)

ONTAP コンシステンシグループを保護する

整合性グループを使用すると、複数のボリュームにまたがるSAN、NAS、NVMeのアプリケーションのローカルとリモートの保護を簡単に管理できます。

整合性グループを作成しても、保護が自動的に有効になるわけではありません。保護ポリシーは、整合性グループの作成時または作成後に設定できます。整合性グループは次の方法で保護できます。

- ローカル Snapshot
- SnapMirrorアクティブ同期（9.15.1より前のONTAPバージョンではSnapMirrorビジネス継続性と呼ばれます）
- [MetroCluster（9.11.1以降）](#)
- SnapMirror非同期（9.13.1以降）
- 非同期SVMディザスタ リカバリ（9.14.1以降）

ネストされた整合性グループを使用している場合は、親整合性グループと子整合性グループに別々の保護ポリシーを設定できます。

ONTAP 9.11.1以降、整合グループは[2フェーズ整合性グループSnapshotの作成](#)を提供します。2フェーズのSnapshotオペレーションでは事前チェックが実行され、Snapshotが正常にキャプチャされたことが確認されます。

リカバリは、コンシステンシ・グループ全体、階層構成内の単一のコンシステンシ・グループ、またはコンシステンシ・グループ内の個々のボリュームに対して実行できます。リカバリは、リカバリ元のコンシステンシ・グループを選択し、スナップショットの種類を選択し、復元のベースとなるスナップショットを特定することで実行できます。このプロセスの詳細については、["以前のスナップショットからボリュームをリストアする"](#)を参照してください。

ローカルスナップショットポリシーを設定する

ローカルのSnapshot保護ポリシーを設定すると、整合性グループ内のすべてのボリュームに適用するポリシーを作成できます。

タスク概要

整合性グループでサポートされる最小スナップショットスケジュールは30分です。これは["FlexGroupボリュームのテスト"](#)に基づいています。整合性グループと同じSnapshotインフラストラクチャを共有しています。

System Manager

手順

1. *Storage > Consistency groups*を選択します。
2. 整合性グループ メニューから作成した整合性グループを選択します。
3. 整合性グループの概要ページの右上で、*編集*を選択します。
4. **Schedule Snapshots (local)** の横にあるボックスをオンにします。
5. スナップショットポリシーを選択します。新しいカスタムポリシーを設定するには、"[カスタムデータ保護ポリシーを作成する](#)"を参照してください。
6. *保存*を選択します。
7. 整合性グループの概要メニューに戻ります。左側の列の*スナップショット（ローカル）*の下に  の横に、ステータスが「保護」と表示されます。

CLI

ONTAP 9.14.1以降では、CLIを使用して整合性グループの保護ポリシーを変更できます。

開始する前に

- このタスクを実行するには、admin権限レベルが必要です。
- ONTAP 9.15.1以降では、admin権限レベルのすべてのユーザがこのタスクを実行できます。ONTAP 9.14.1では、このタスクを実行するには、クラスタ管理者またはSVMの管理者である必要があります。

手順

1. 次のコマンドを実行して、保護ポリシーを設定または変更します。

子整合性グループの保護ポリシーを変更する場合は、`-parent-consistency-group parent_consistency_group_name` パラメータを使用して親整合性グループを識別する必要があります。

```
consistency-group modify -vserver svm_name -consistency-group  
consistency_group_name -snapshot-policy policy_name
```

オンデマンドスナップショットを作成する

通常のスケジュールされたポリシー以外で整合性グループのスナップショットを作成する必要がある場合は、オンデマンドで作成できます。

System Manager

手順

1. ストレージ > 整合性グループ に移動します。
2. オンデマンド スナップショットを作成する整合性グループを選択します。
3. **Snapshot** コピー タブに切り替えて、**+ 追加** を選択します。
4. *名前*と*SnapMirrorラベル*を入力します。*一貫性*のドロップダウンメニューで、*アプリケーション一貫性*または*クラッシュ一貫性*を選択します。
5. *保存*を選択します。

CLI

ONTAP 9.14.1 以降では、CLI を使用してコンシステンシー グループのオンデマンド スナップショットを作成できます。

開始する前に

- このタスクを実行するには、admin権限レベルが必要です。
- ONTAP 9.15.1以降では、admin権限レベルのすべてのユーザがこのタスクを実行できます。ONTAP 9.14.1では、このタスクを実行するには、クラスタ管理者またはSVMの管理者である必要があります。

手順

1. Snapshotを作成します：

デフォルトでは、スナップショットの種類は「crash consistent state（障害など予期しないシャットダウン時と同様）」の状態です。オプションの `-type` パラメータを使用してスナップショットの種類を変更できます。

```
consistency-group snapshot create -vserver svm_name -consistency-group  
consistency_group_name -snapshot snapshot_name
```

2フェーズでの整合性グループのSnapshot作成

ONTAP 9.11.1以降、整合性グループでは、整合性グループ（CG）Snapshotコピーの作成時に2フェーズコミットがサポートされます。これにより、Snapshotコピーをコミットする前に事前チェックが実行されます。この機能は、ONTAP REST APIでのみ使用できます。

2フェーズCGスナップショット作成は、スナップショット作成にのみ使用でき、整合性グループのプロビジョニングや整合性グループの復元には使用できません。

2フェーズCGスナップショットでは、スナップショット作成プロセスが2つのフェーズに分割されます。

1. 最初のフェーズでは、APIは事前チェックを実行し、Snapshotの作成をトリガーします。最初のフェーズには、Snapshotが正常にコミットされるまでの時間を指定するタイムアウト パラメータが含まれています。
2. フェーズ1の要求が正常に完了した場合、最初のフェーズから指定された間隔内に2番目のフェーズを呼び出して、Snapshotを適切なエンドポイントにコミットできます。

開始する前に

- 2フェーズCGスナップショット作成を使用するには、クラスタ内のすべてのノードでONTAP 9.11.1以降が実行されている必要があります。
- 整合性グループインスタンスでは、1フェーズまたは2フェーズを問わず、一度に1つのアクティブな整合性グループスナップショット操作の呼び出しのみがサポートされます。別のスナップショット操作の実行中にスナップショット操作を呼び出そうとすると、失敗します。
- スナップショット作成を呼び出す際に、5～120秒のタイムアウト値を任意で設定できます。タイムアウト値を指定しない場合、操作はデフォルトの7秒でタイムアウトします。APIでは、`action\_timeout`パラメータを使用してタイムアウト値を設定します。CLIでは、`-timeout`フラグを使用します。

手順

2フェーズスナップショットはREST API、またはONTAP 9.14.1以降ではONTAP CLIを使用して実行できます。この操作はSystem Managerではサポートされていません。



APIを使用してスナップショットの作成を呼び出した場合は、APIを使用してスナップショットをコミットする必要があります。CLIを使用してスナップショットの作成を呼び出した場合は、CLIを使用してスナップショットをコミットする必要があります。これらのメソッドを混在させることはサポートされていません。

CLI

ONTAP 9.14.1 以降では、CLI を使用して 2 フェーズ スナップショットを作成できます。

開始する前に

- このタスクを実行するには、admin権限レベルが必要です。
- ONTAP 9.15.1以降では、admin権限レベルのすべてのユーザがこのタスクを実行できます。ONTAP 9.14.1では、このタスクを実行するには、クラスタ管理者またはSVMの管理者である必要があります。

手順

1. Snapshotを開始します：

```
consistency-group snapshot start -vserver svm_name -consistency-group  
consistency_group_name -snapshot snapshot_name [-timeout time_in_seconds  
-write-fence {true|false}]
```

2. Snapshotが取得されたことを確認します：

```
consistency-group snapshot show
```

3. Snapshotをコミットします：

```
consistency-group snapshot commit svm_name -consistency-group  
consistency_group_name -snapshot snapshot_name
```

API

1. スナップショットの作成を呼び出します。`action=start`パラメータを使用して、整合性グループのエンドポイントにPOSTリクエストを送信します。

```
curl -k -X POST 'https://<IP_address>/application/consistency-  
groups/<cg-uuid>/snapshots?action=start&action_timeout=7' -H  
"accept: application/hal+json" -H "content-type: application/json"  
-d '  
{  
  "name": "<snapshot_name>",  
  "consistency_type": "crash",  
  "comment": "<comment>",  
  "snapmirror_label": "<SnapMirror_label>"  
}'
```

2. POSTリクエストが成功した場合、出力にはスナップショットのUUIDが含まれます。そのUUIDを使用してPATCHリクエストを送信し、スナップショットをコミットします。

```
curl -k -X PATCH 'https://<IP_address>/application/consistency-groups/<cg_uuid>/snapshots/<snapshot_id>?action=commit' -H "accept: application/hal+json" -H "content-type: application/json"
```

For more information about the ONTAP REST API, see [link:https://docs.netapp.com/us-en/ontap-automation/reference/api_reference.html](https://docs.netapp.com/us-en/ontap-automation/reference/api_reference.html) [API reference^] or the [link:https://devnet.netapp.com/restapi.php](https://devnet.netapp.com/restapi.php) [ONTAP REST API page^] at the NetApp Developer Network for a complete list of API endpoints.

整合性グループに対するリモート保護の設定

整合性グループは、SnapMirrorアクティブ同期のほか、ONTAP 9.13.1以降ではSnapMirror非同期によってリモート保護を提供します。

SnapMirrorアクティブ同期による保護の設定

SnapMirror Active Syncを使用すると、整合性グループ上に作成された整合性グループのSnapshotが宛先にコピーされることを確認できます。SnapMirror Active Syncの詳細、またはCLIを使用してSnapMirror Active Syncを設定する方法については、[ビジネス継続性のための保護の設定](#)を参照してください。

開始する前に

- NASアクセス用にマウントされたボリュームではSnapMirrorアクティブ同期関係を確立できません。
- ソース クラスタとデスティネーション クラスタのポリシー ラベルが一致している必要があります。
- SnapMirror Active Syncは、SnapMirrorラベル付きのルールが定義済み `AutomatedFailOver` ポリシーに追加され、そのラベルを使用してSnapshotが作成されない限り、デフォルトでSnapshotを複製しません。

このプロセスの詳細については、["SnapMirrorアクティブ同期による保護"](#)を参照してください。

- [カスケード展開](#) はSnapMirrorアクティブ同期ではサポートされません。
- ONTAP 9.13.1以降では、アクティブなSnapMirror Active Sync関係を使用して、無停止で[整合性グループにボリュームを追加する](#)ことができます。コンシステンシーグループにその他の変更を加える場合は、SnapMirror Active Sync関係を解除し、コンシステンシーグループを変更した上で、関係を再確立して再同期する必要があります。



CLIを使用してSnapMirrorアクティブ同期を設定するには、[SnapMirrorアクティブ同期による保護](#)を参照してください。

System Managerでの手順

1. ["SnapMirrorアクティブ同期を使用するための前提条件"](#)を満たしていることを確認してください。
2. *Storage > Consistency groups*を選択します。
3. 整合性グループ メニューから作成した整合性グループを選択します。
4. 概要ページの右上で、[詳細] を選択し、[保護] を選択します。

5. System Managerはソース側の情報を自動入力します。適切なクラスタとストレージVMをデスティネーションとして選択します。保護ポリシーを選択します。***関係を初期化する***がチェックされていることを確認してください。
6. ***保存***を選択します。
7. 整合性グループを初期化して同期する必要があります。***整合性グループ***メニューに戻り、同期が正常に完了したことを確認してください。***SnapMirror（リモート）*ステータスに`Protected`**がの横に表示されます。

SnapMirror非同期の設定

ONTAP 9.13.1以降では、単一のコンシステンシグループに対してSnapMirror非同期保護を設定できます。ONTAP 9.14.1以降では、SnapMirror非同期を使用して、コンシステンシグループの関係を**使用して**ボリューム単位のスナップショットをデスティネーション クラスタに複製できます。

タスク概要

ボリューム単位のスナップショットをレプリケートするには、ONTAP 9.14.1以降を実行している必要があります。MirrorAndVaultポリシーとVaultポリシーの場合、ボリューム単位のスナップショットポリシーのSnapMirrorラベルがコンシステンシグループのSnapMirrorポリシールールと一致する必要があります。ボリューム単位のスナップショットは、コンシステンシグループのSnapMirrorポリシーの保持値に従います。この値は、コンシステンシグループのスナップショットとは独立して計算されます。例えば、デスティネーションに2つのスナップショットを保持するポリシーがある場合、ボリューム単位のスナップショットを2つとコンシステンシグループのスナップショットを2つ保持できます。

ボリューム単位のスナップショットを持つSnapMirror関係を再同期する際に、`-preserve`フラグを使用してボリューム単位のスナップショットを保持できます。整合性グループのスナップショットよりも新しいボリューム単位のスナップショットが保持されます。整合性グループのスナップショットがない場合、再同期処理でボリューム単位のスナップショットを転送することはできません。

開始する前に

- SnapMirror非同期保護は単一の整合性グループでのみ利用可能です。階層型整合性グループではサポートされていません。階層型整合性グループを単一の整合性グループに変換するには、[整合性グループのアーキテクチャを変更する](#)を参照してください。
- ソース クラスタとデスティネーション クラスタのポリシー ラベルが一致している必要があります。
- アクティブなSnapMirror非同期関係で[整合性グループにボリュームを追加する](#)を無停止で実行できます。整合性グループにその他の変更を加える場合は、SnapMirror関係を解除し、整合性グループを変更した上で、関係を再確立して再同期する必要があります。
- SnapMirror非同期保護が有効になっている整合性グループには、異なる制限があります。詳細については、[整合性グループの制限](#)をご覧ください。
- 複数の個別ボリュームに対してSnapMirror非同期保護関係を設定している場合、既存のスナップショットを保持したまま、それらのボリュームを整合性グループに変換できます。ボリュームを正常に変換するには：
 - ボリュームの共通Snapshotコピーが必要です。
 - 既存のSnapMirror関係を解除し、[ボリュームを単一の整合性グループに追加する](#)次のワークフローを使用して関係を再同期する必要があります。

手順

1. デスティネーション クラスタから、***ストレージ > 整合性グループ***を選択します。

2. 整合性グループ メニューから作成した整合性グループを選択します。
3. 概要ページの右上で、[詳細] を選択し、[保護] を選択します。
4. System Managerはソース側の情報を自動入力します。適切なクラスタとストレージVMをデスティネーションとして選択します。保護ポリシーを選択します。*関係を初期化する*がチェックされていることを確認してください。

非同期ポリシーを選択する場合は、転送スケジュールを上書きするオプションがあります。



SnapMirror非同期を使用した整合性グループに設定可能な最短スケジュール（目標復旧時点、RPO）は30分です。

5. *保存*を選択します。
6. 整合性グループを初期化して同期する必要があります。*整合性グループ*メニューに戻り、同期が正常に完了したことを確認してください。*SnapMirror（リモート）*ステータスに`Protected`がの横に表示されます。

SVMディザスタ リカバリの設定

ONTAP 9.14.1以降、[SVMディザスタ リカバリ](#)はコンシステンシ グループをサポートし、ソース クラスタからデスティネーション クラスタへコンシステンシ グループ情報をミラーリングできます。

すでにコンシステンシー グループが含まれている SVM で SVM ディザスタ リカバリを有効にする場合は、[System Manager](#)または[ONTAP CLI](#)の SVM 構成ワークフローに従います。

アクティブで正常なSVMディザスタリカバリ関係にあるSVMにコンシステンシグループを追加する場合は、デスティネーション クラスタからSVMディザスタリカバリ関係を更新する必要があります。詳細については、[レプリケーション関係の手動更新](#)を参照してください。コンシステンシグループを拡張するたびに、関係を更新する必要があります。

制限事項

- SVMディザスタ リカバリでは、階層型整合性グループはサポートされません。
- SVMディザスタ リカバリでは、SnapMirror非同期で保護された整合性グループはサポートされません。SVMディザスタ リカバリを設定する前に、SnapMirror関係を解除する必要があります。
- どちらのクラスタでも、ONTAP 9.14.1以降が実行されている必要があります。
- 整合性グループが含まれるSVMディザスタ リカバリ構成では、ファンアウト関係はサポートされません。
- その他の制限については、[整合性グループの制限](#)を参照してください。

関係の可視化

System Managerは、*保護 > 関係*メニューでLUNマップを視覚化します。ソース関係を選択すると、System Managerはソース関係の視覚化を表示します。ボリュームを選択すると、これらの関係をさらに詳しく調べて、含まれるLUNとイニシエータ グループの関係のリストを確認できます。この情報は、個々のボリュームビューからExcelワークブックとしてダウンロードできます。ダウンロード処理はバックグラウンドで実行されます。

関連情報

- ["整合性グループのクローニング"](#)

- ["Snapshotを設定"](#)
- ["カスタムのデータ保護ポリシーの作成"](#)
- ["Snapshotからのリカバリ"](#)
- ["以前のスナップショットからボリュームをリストアする"](#)
- ["SnapMirrorアクティブ同期の概要"](#)
- ["ONTAP自動化ドキュメント"](#)
- [SnapMirror非同期のディザスタ リカバリの基本](#)

ONTAP コンシステンシーグループのメンバーボリュームを変更する

ONTAP 9.12.1以降では、ボリュームを削除するか、ボリュームを追加（整合性グループを拡張）して整合性グループを変更できます。ONTAP 9.13.1以降では、同じ親に所属する子整合性グループ間でボリュームを移動できます。

整合性グループへのボリュームの追加

ONTAP 9.12.1以降では、整合性グループに無停止でボリュームを追加できます。

タスク概要

- 別の整合性グループに関連付けられているボリュームを追加することはできません。
- 整合性グループでは、NAS、SAN、NVMeの各プロトコルがサポートされます。
- 調整が全体の[整合性グループの制限](#)内であれば、一度に最大16個のボリュームを整合性グループに追加できます。
- ONTAP 9.13.1以降では、アクティブなSnapMirrorアクティブ同期ポリシーまたはSnapMirror非同期保護ポリシーを使用して、整合性グループに無停止でボリュームを追加できます。
- SnapMirror Active Syncで保護されているコンシステンシーグループにボリュームを追加すると、新しいボリュームのミラーリングと保護が構成されるまで、SnapMirror Active Sync関係のステータスは「拡張中」に変わります。このプロセスが完了する前にプライマリクラスタで災害が発生した場合、フェイルオーバー操作の一環として、コンシステンシーグループは元の構成に戻ります。
- ONTAP 9.12.1以前では、SnapMirror Active Sync関係にあるコンシステンシーグループにボリュームを追加することはできません。まずSnapMirror Active Sync関係を削除し、コンシステンシーグループを変更してから、SnapMirror Active Syncによる保護を復元する必要があります。
- ONTAP 9.12.1以降、ONTAP REST APIは、整合性グループへの_新規_または既存のボリュームの追加をサポートします。ONTAP REST APIの詳細については、["ONTAP REST APIリファレンスドキュメント"](#)を参照してください。

ONTAP 9.13.1以降では、この機能がSystem Managerでサポートされます。

- 整合性グループを拡張する場合、変更前に取得された整合性グループのスナップショットは部分的なものとみなされます。そのスナップショットに基づく復元処理には、スナップショットのポイントインタイムの整合性グループが反映されます。
- ONTAP 9.10.1～9.11.1を使用している場合は、整合性グループを変更できません。ONTAP 9.10.1または9.11.1で整合性グループの設定を変更するには、整合性グループを削除し、希望するボリュームで新しく整合性グループを作成する必要があります。

- ONTAP 9.14.1以降では、SnapMirror非同期モードの使用時に、ボリューム単位のスナップショットをデスティネーション クラスタにレプリケートできます。SnapMirror非同期モードを使用してコンシステンシグループを拡張する場合、SnapMirrorポリシーがMirrorAllまたはMirrorAndVaultの場合にのみ、コンシステンシグループを拡張した後にボリューム単位のスナップショットがレプリケートされます。ベースラインコンシステンシグループスナップショットよりも新しいボリューム単位のスナップショットのみがレプリケートされます。
- SVMディザスタリカバリ関係（ONTAP 9.14.1以降でサポート）のコンシステンシグループにボリュームを追加する場合は、コンシステンシグループを拡張した後、デスティネーション クラスタからSVMディザスタリカバリ関係を更新する必要があります。詳細については、[レプリケーション関係の手動更新](#)を参照してください。
- ONTAP 9.17.1 で NVMe を使用している場合は、整合性グループを変更できません。

例 2. 手順

System Manager

ONTAP 9.12.1以降では、System Managerでこの処理を実行できます。

1. *Storage > Consistency groups*を選択します。
2. 変更する整合性グループを選択します。
3. 単一の整合性グループを変更する場合は、*ボリューム*メニューの上部にある*詳細*を選択し、*展開*を選択してボリュームを追加します。

子コンシステンシーグループを変更する場合は、変更する親コンシステンシーグループを特定します。*>*ボタンを選択して子コンシステンシーグループを表示し、変更する子コンシステンシーグループの名前の横にあるを選択します。表示されたメニューから*展開*を選択します。

4. 整合性グループに追加するボリュームを最大16個選択します。
5. *保存*を選択します。操作が完了したら、整合性グループの*ボリューム*メニューで新しく追加されたボリュームを表示します。

CLI

ONTAP 9.14.1以降では、ONTAP CLIを使用して整合性グループにボリュームを追加できます。

開始する前に

- このタスクを実行するには、admin権限レベルが必要です。
- ONTAP 9.15.1以降では、admin権限レベルのすべてのユーザがこのタスクを実行できます。ONTAP 9.14.1では、このタスクを実行するには、クラスタ管理者またはSVMの管理者である必要があります。

既存のボリュームの追加

1. 次のコマンドを実行します。`-volumes`パラメータには、カンマ区切りのボリュームリストを指定できます。



整合性グループが階層関係にある場合にのみ、`-parent-consistency-group`パラメータを含めます。

```
consistency-group volume add -vserver svm_name -consistency-group  
consistency_group_name -parent-consistency-group parent_consistency_group  
-volume volumes
```

新しいボリュームの追加

新しいボリュームを追加する手順は、使用するプロトコルによって異なります。



整合性グループが階層関係にある場合にのみ、`-parent-consistency-group`パラメータを含めます。

- エクスポートせずに新しいボリュームを追加するには、次のコマンドを実行します。

```
consistency-group volume create -vserver SVM_name -consistency-group  
child_consistency_group -parent-consistency-group existingParentCg -volume
```

```
volume_name -size size
```

- 新しいNFSボリュームを追加するには、次のコマンドを実行します。

```
consistency-group volume create -vserver SVM_name -consistency-group  
consistency-group-name -volume volume-prefix -volume-count number -size  
size -export-policy policy_name
```

- 新しいSANボリュームを追加するには、次のコマンドを実行します。

```
consistency-group volume create -vserver SVM_name -consistency-group  
consistency-group-name -lun lun_name -size size -lun-count number -igroup  
igroup_name
```

- 新しいNVMeネームスペースを追加するには、次のコマンドを実行します。

```
consistency-group volume create -vserver SVM_name -consistency-group  
consistency_group_name -namespace namespace_name -volume-count number  
-namespace-count number -size size -subsystem subsystem_name
```

整合性グループからのボリュームの削除

整合性グループから削除しても、ボリューム自体は削除されません。クラスタ内でアクティブなままです。

タスク概要

- SnapMirrorアクティブ同期またはSVMディザスタ リカバリ関係にある整合性グループからボリュームを削除することはできません。最初にSnapMirrorアクティブ同期関係を削除し、整合性グループを変更してから、関係を再確立する必要があります。
- 削除後にボリュームが1つもない整合性グループは削除されます。
- ボリュームが整合性グループから削除されると、整合性グループの既存のスナップショットは残りますが、無効とみなされます。既存のスナップショットを使用して整合性グループの内容を復元することはできません。ボリューム単位のスナップショットは有効なままです。
- クラスタからボリュームを削除すると、そのボリュームは整合性グループから自動的に削除されます。
- ONTAP 9.10.1または9.11.1で整合性グループの設定を変更するには、整合性グループを削除してから、必要なメンバー ボリュームで新しく整合性グループを作成する必要があります。
- クラスタからボリュームを削除すると、整合性グループからも自動的に削除されます。

System Manager

ONTAP 9.12.1以降では、System Managerでこの処理を実行できます。

手順

1. *Storage > Consistency groups*を選択します。
2. 変更する独立した整合性グループまたは子整合性グループを選択します。
3. ボリューム メニューで、整合性グループから削除する個々のボリュームの横にあるチェックボックスを選択します。
4. 整合性グループからボリュームを削除 を選択します。
5. ボリュームを削除すると、コンシステンシー グループのすべてのスナップショットが無効になることを理解した上で、削除 を選択します。

CLI

ONTAP 9.14.1以降では、CLIを使用して整合性グループからボリュームを削除できます。

開始する前に

- このタスクを実行するには、admin権限レベルが必要です。
- ONTAP 9.15.1以降では、admin権限レベルのすべてのユーザがこのタスクを実行できます。ONTAP 9.14.1では、このタスクを実行するには、クラスタ管理者またはSVMの管理者である必要があります。

手順

1. ボリュームを削除します。この `-volumes` パラメータには、カンマ区切りのボリュームのリストを指定できます。

整合性グループが階層関係にある場合にのみ、`-parent-consistency-group` パラメータを含めます。

```
consistency-group volume remove -vserver SVM_name -consistency-group  
consistency_group_name -parent-consistency-group  
parent_consistency_group_name -volume volumes
```

整合性グループ間でのボリュームの移動

ONTAP 9.13.1以降では、同じ親に所属する子整合性グループ間でボリュームを移動できます。

タスク概要

- ボリュームは、同じ親整合性グループに含まれる整合性グループ間でのみ移動できます。
- 既存のコンシステンシグループスナップショットは無効になり、コンシステンシグループスナップショットとしてアクセスできなくなります。個々のボリュームスナップショットは有効なままです。
- 親整合性グループのスナップショットは有効なままです。
- 子整合性グループからすべてのボリュームを移動すると、その整合性グループは削除されます。
- 整合性グループへの変更は[整合性グループの制限](#)に従う必要があります。

System Manager

ONTAP 9.12.1以降では、System Managerでこの処理を実行できます。

手順

1. *Storage > Consistency groups*を選択します。
2. 移動するボリュームを含む親コンシステンシグループを選択します。子コンシステンシグループを見つけて、ボリュームメニューを展開します。移動するボリュームを選択します。
3. 移動を選択します。
4. ボリュームを新しい整合性グループと既存のグループのどちらに移動するかを選択します。
 - a. 既存の整合性グループに移動するには、既存の子整合性グループを選択し、ドロップダウンメニューから整合性グループの名前を選択します。
 - b. 新しいコンシステンシグループに移動するには、新しい子コンシステンシグループを選択します。新しい子コンシステンシグループの名前を入力し、コンポーネントタイプを選択します。
5. 移動を選択します。

CLI

ONTAP 9.14.1以降では、ONTAP CLIを使用して整合性グループ間でボリュームを移動できます。

開始する前に

- このタスクを実行するには、admin権限レベルが必要です。
- ONTAP 9.15.1以降では、admin権限レベルのすべてのユーザがこのタスクを実行できます。ONTAP 9.14.1では、このタスクを実行するには、クラスタ管理者またはSVMの管理者である必要があります。

新しい子整合性グループへのボリュームの移動

1. 次のコマンドは、指定したボリュームを含む新しい子整合性グループを作成します。

新しい整合性グループを作成するときに、新しいスナップショット、QoS、および階層化ポリシーを指定できます。

```
consistency-group volume reassign -vserver SVM_name -consistency-group
source_child_consistency_group -parent-consistency-group
parent_consistency_group -volume volumes -new-consistency-group
consistency_group_name [-snapshot-policy policy -qos-policy policy -tiering
-policy policy]
```

既存の子整合性グループへのボリュームの移動

1. ボリュームを再割り当てします。この `'-volumes'` パラメータには、ボリューム名をカンマで区切って指定できます。

```
consistency-group volume reassign -vserver SVM_name -consistency-group
source_child_consistency_group -parent-consistency-group
parent_consistency_group -volume volumes -to-consistency-group
target_consistency_group
```


関連情報

- [整合性グループの制限](#)
- [整合性グループのクローニング](#)

ONTAP コンシステンシグループのジオメトリを変更する

ONTAP 9.13.1以降では、整合性グループのジオメトリを変更できます。整合性グループのジオメトリを変更すると、進行中のI/O処理を停止することなく、子または親整合性グループの構成を変更できます。

整合性グループのジオメトリを変更すると、整合性グループの既存のスナップショットに影響があります。詳細については、実行するジオメトリの変更内容を参照してください。



リモート保護ポリシーが設定されている整合性グループのジオメトリは変更できません。最初に保護関係を解除し、ジオメトリを変更してから、リモート保護をリストアする必要があります。

新しい子整合性グループの追加

ONTAP 9.13.1以降では、既存の親整合性グループに新しい子整合性グループを追加できます。

タスク概要

- 親コンシステンシグループには最大5つの子コンシステンシグループを含めることができます。その他の制限については[整合性グループの制限](#)を参照してください。
- 単一の整合性グループに子整合性グループを追加することはできません。まず整合性グループを[\[promote\]](#)してから、子整合性グループを追加する必要があります。
- 拡張操作前に取得された整合性グループの既存のスナップショットは部分的なものとみなされます。そのスナップショットに基づく復元操作は、スナップショットのポイントインタイムにおける整合性グループを反映します。

System Manager

ONTAP 9.13.1以降では、System Managerでこの処理を実行できます。

新しい子整合性グループの追加

1. *Storage > Consistency groups*を選択します。
2. 子整合性グループを追加する親整合性グループを選択します。
3. 親整合性グループの名前の横にある [詳細] を選択し、[新しい子整合性グループの追加] を選択します。
4. 整合性グループの名前を入力します。
5. 新しいボリュームと既存のボリュームのどちらを追加するかを選択します。
 - a. 既存のボリュームを追加する場合は、既存のボリュームを選択し、ドロップダウン メニューからボリュームを選択します。
 - b. 新しいボリュームを追加する場合は、新しいボリュームを選択し、ボリュームの数とサイズを指定します。
6. 追加を選択します。

CLI

ONTAP 9.14.1以降では、ONTAP CLIを使用して子整合性グループを追加できます。

開始する前に

- このタスクを実行するには、admin権限レベルが必要です。
- ONTAP 9.15.1以降では、admin権限レベルのすべてのユーザがこのタスクを実行できます。ONTAP 9.14.1では、このタスクを実行するには、クラスタ管理者またはSVMの管理者である必要があります。

新しいボリュームを使用した子整合性グループの追加

1. 新しい整合性グループを作成します。整合性グループ名、ボリュームのプレフィックス、ボリューム数、ボリューム サイズ、ストレージ サービス、およびエクスポート ポリシー名の値を指定します。

```
consistency-group create -vserver SVM_name -consistency-group
consistency_group -parent-consistency-group parent_consistency_group
-volume-prefix prefix -volume-count number -size size -storage-service
service -export-policy policy_name
```

既存のボリュームを使用した子整合性グループの追加

1. 新しいコンシステンシグループを作成します。`volumes`パラメータには、ボリューム名のコンマ区切りリストを指定できます。

```
consistency-group create -vserver SVM_name -consistency-group
new_consistency_group -parent-consistency-group parent_consistency_group
-volumes volume
```

子整合性グループの接続解除

ONTAP 9.13.1以降では、子整合性グループを親から削除して、個別の整合性グループに変換することができます。

タスク概要

- 子整合性グループをデタッチすると、親整合性グループのスナップショットは無効になり、アクセスできなくなります。ボリュームの細分スナップショットは有効なままです。
- 個々の整合性グループの既存のスナップショットは有効なままです。
- 接続を解除する子整合性グループと同じ名前の独立した整合性グループがすでにある場合、この処理は失敗します。そのような場合は、接続を解除するときに整合性グループの名前を変更する必要があります。

例 4. 手順

System Manager

ONTAP 9.13.1以降では、System Managerでこの処理を実行できます。

子整合性グループの接続解除

1. *Storage > Consistency groups*を選択します。
2. 接続を解除する子を含む親整合性グループを選択します。
3. デタッチする子整合性グループの横にある [詳細] を選択し、[親からデタッチ] を選択します。
4. 必要に応じて、整合性グループの名前を変更し、アプリケーション タイプを選択します。
5. デタッチを選択します。

CLI

ONTAP 9.14.1以降では、ONTAP CLIを使用して子整合性グループの接続を解除できます。

開始する前に

- このタスクを実行するには、admin権限レベルが必要です。
- ONTAP 9.15.1以降では、admin権限レベルのすべてのユーザがこのタスクを実行できます。ONTAP 9.14.1では、このタスクを実行するには、クラスタ管理者またはSVMの管理者である必要があります。

子整合性グループの接続解除

1. 整合性グループをデタッチします。オプションで、`-new-name` パラメータを使用してデタッチされた整合性グループの名前を変更します。

```
consistency-group detach -vserver SVM_name -consistency-group  
child_consistency_group -parent-consistency-group parent_consistency_group  
[-new-name new_name]
```

親整合性グループへの既存の独立した整合性グループの移動

ONTAP 9.13.1以降では、既存の独立した整合性グループを子整合性グループに変換できます。変換した子整合性グループは、変換時に既存の親整合性グループまたは新しく作成した親整合性グループに移動できます。

タスク概要

- 親コンシステンシグループには、4つ以下の子コンシステンシグループを含める必要があります。親コンシステンシグループには、最大5つの子コンシステンシグループを含めることができます。その他の制限については、[整合性グループの制限](#)を参照してください。
- この操作の前に取得された_親_整合性グループの既存のスナップショットは部分的なものとみなされます。これらのスナップショットのいずれかに基づく復元操作は、スナップショットのポイントインタイムにおける整合性グループを反映します。
- 独立した整合性グループの既存のSnapshotは有効なままです。

System Manager

ONTAP 9.13.1以降では、System Managerでこの処理を実行できます。

親整合性グループへの既存の独立した整合性グループの移動

1. *Storage > Consistency groups*を選択します。
2. 変換する整合性グループを選択します。
3. 詳細を選択し、別の整合性グループに移動を選択します。
4. 必要に応じて、整合性グループの新しい名前を入力し、コンポーネント タイプを選択します。デフォルトでは、コンポーネント タイプは「Other」です。
5. 既存の親整合性グループに移行するか、新しい親整合性グループを作成するかを選択します。
 - a. 既存の親整合性グループに移行するには、既存の整合性グループを選択し、ドロップダウン メニューから整合性グループを選択します。
 - b. 新しい親整合性グループを作成するには、新しい整合性グループを選択し、新しい整合性グループの名前を入力します。
6. 移動を選択します。

CLI

ONTAP 9.14.1以降では、ONTAP CLIを使用して、親整合性グループに独立した整合性グループを移動できます。

開始する前に

- このタスクを実行するには、admin権限レベルが必要です。
- ONTAP 9.15.1以降では、admin権限レベルのすべてのユーザがこのタスクを実行できます。ONTAP 9.14.1では、このタスクを実行するには、クラスタ管理者またはSVMの管理者である必要があります。

新しい親整合性グループへの整合性グループの移動

1. 新しい親整合性グループを作成します。`-consistency-groups`パラメータにより、既存の整合性グループが新しい親グループに移行されます。

```
consistency-group attach -vserver svm_name -consistency-group  
parent_consistency_group -consistency-groups child_consistency_group
```

既存の整合性グループへの整合性グループの移動

1. 整合性グループを移動します。

```
consistency-group add -vserver SVM_name -consistency-group  
consistency_group -parent-consistency-group parent_consistency_group
```

子整合性グループの昇格

ONTAP 9.13.1以降では、独立した整合性グループを親整合性グループに昇格できます。独立した整合性グループを親に昇格する際には、元の独立した整合性グループ内のボリュームをすべて継承する新しい子整合性グループを作成します。

ループも作成します。

タスク概要

- 子整合性グループを親整合性グループに変換する場合は、まず子整合性グループを[\[detach\]](#)してから、この手順に従う必要があります。
- 整合性グループの既存のスナップショットは、整合性グループを昇格した後も有効なままになります。

System Manager

ONTAP 9.13.1以降では、System Managerでこの処理を実行できます。

子整合性グループの昇格

1. *Storage > Consistency groups*を選択します。
2. 昇格する整合性グループを選択します。
3. 詳細を選択し、親整合性グループに昇格を選択します。
4. 子整合性グループの名前を入力し、コンポーネント タイプを選択します。
5. 昇格を選択します。

CLI

ONTAP 9.14.1以降では、ONTAP CLIを使用して、親整合性グループに独立した整合性グループを移動できます。

開始する前に

- このタスクを実行するには、admin権限レベルが必要です。
- ONTAP 9.15.1以降では、admin権限レベルのすべてのユーザがこのタスクを実行できます。ONTAP 9.14.1では、このタスクを実行するには、クラスタ管理者またはSVMの管理者である必要があります。

子整合性グループの昇格

1. 整合性グループを昇格します。このコマンドは、1つの親整合性グループと1つの子整合性グループを作成します。

```
consistency-group promote -vserver SVM_name -consistency-group  
existing_consistency_group -new-name new_child_consistency_group
```

親整合性グループから独立した整合性グループへの降格

ONTAP 9.13.1以降では、親整合性グループを独立した整合性グループに降格できます。親を降格すると、整合性グループの階層がなくなり、関連付けられている子整合性グループはすべて削除されます。削除された整合性グループ内のボリュームは、新しい独立した整合性グループにすべて継承されます。

タスク概要

- 親_整合性グループの既存のスナップショットは、単一整合性グループに降格した後も有効です。その親に関連付けられた_子_整合性グループの既存のスナップショットは、降格時に無効になります。子整合性グループ内の個々のボリュームスナップショットは、ボリューム単位のスナップショットとして引き続きアクセスできます。

例 6. 手順

System Manager

ONTAP 9.13.1以降では、System Managerでこの処理を実行できます。

整合性グループの降格

1. *Storage > Consistency groups*を選択します。
2. 降格する親整合性グループを選択します。
3. 詳細 を選択し、単一の整合性グループに降格 を選択します。
4. 関連するすべての子コンシステンシグループが削除され、それらのボリュームが新しい単一のコンシステンシグループの下に移動されることを通知する警告が表示されます。影響を理解したことを確認するには、**Demote**を選択します。

CLI

ONTAP 9.14.1以降では、ONTAP CLIを使用して整合性グループを降格できます。

開始する前に

- このタスクを実行するには、admin権限レベルが必要です。
- ONTAP 9.15.1以降では、admin権限レベルのすべてのユーザがこのタスクを実行できます。ONTAP 9.14.1では、このタスクを実行するには、クラスタ管理者またはSVMの管理者である必要があります。

整合性グループの降格

1. 整合性グループを降格します。オプションの `-new-name` パラメータを使用して、整合性グループの名前を変更します。

```
consistency-group demote -vserver SVM_name -consistency-group  
parent_consistency_group [-new-name new_consistency_group_name]
```

ONTAPコンシステンシグループのアプリケーションとコンポーネントのタグを変更する

ONTAP 9.12.1以降、整合性グループではコンポーネントとアプリケーションのタグ付けがサポートされます。アプリケーション タグとコンポーネント タグを使用すると、整合性グループ内のさまざまなワークロードをフィルタリングして識別し、管理できます。

タスク概要

整合性グループには、以下の2種類のタグがあります。

- アプリケーション タグ：個々の整合性グループと親整合性グループに適用されます。アプリケーション タグは、MongoDB、Oracle、SQL Serverなどのワークロードにラベルを付けることができます。整合性グループのデフォルトのアプリケーション タグはOtherです。
- コンポーネントタグ：階層型整合性グループの子には、アプリケーションタグではなくコンポーネントタグが設定されます。コンポーネントタグの選択肢は「data」、「logs」、または「other」です。デフォルト値はOtherです。

タグは整合性グループの作成時または作成後に適用できます。



整合性グループにSnapMirrorアクティブな同期関係がある場合は、アプリケーションまたはコンポーネント タグとして*Other*を使用する必要があります。

手順

ONTAP 9.12.1以降では、System Managerを使用してアプリケーション タグとコンポーネント タグを変更できます。ONTAP 9.14.1以降では、ONTAP CLIを使用してアプリケーション タグとコンポーネント タグを変更できます。

System Manager

1. *Storage > Consistency groups*を選択します。
2. タグを変更するコンシステンシーグループを選択します。コンシステンシーグループ名の横にある⋮を選択し、*編集*をクリックします。
3. ドロップダウン メニューで、適切なアプリケーション タグまたはコンポーネント タグを選択します。
4. *保存*を選択します。

CLI

ONTAP 9.14.1以降では、ONTAP CLIを使用して、既存の整合性グループのアプリケーション タグまたはコンポーネント タグを変更できます。

開始する前に

- このタスクを実行するには、admin権限レベルが必要です。
- ONTAP 9.15.1以降では、admin権限レベルのすべてのユーザがこのタスクを実行できます。ONTAP 9.14.1では、このタスクを実行するには、クラスタ管理者またはSVMの管理者である必要があります。

アプリケーション タグの変更

1. アプリケーションタグは、限られた数のプリセット文字列を受け入れます。受け入れられる文字列のリストを確認するには、次のコマンドを実行します：
`consistency-group modify -vserver svm_name -consistency-group consistency_group -application-type ?`

2. 出力から適切な文字列を選択し、整合性グループを変更します：
`consistency-group modify -vserver svm_name -consistency-group consistency_group -application-type application_type`

コンポーネント タグの変更

1. コンポーネントの種類を変更します。コンポーネントの種類は、データ、ログ、その他のいずれかになります。SnapMirror Active Syncを使用している場合は、「その他」を選択する必要があります。
`consistency-group modify -vserver svm -consistency-group child_consistency_group -parent-consistency-group parent_consistency_group -application-component-type [data|logs|other]`

ONTAPコンシステンシーグループのクローンを作成する

ONTAP 9.12.1以降では、整合性グループをクローニングして、整合性グループとその内

容のコピーを作成できます。整合性グループをクローニングすると、整合性グループの設定、メタデータ（アプリケーション タイプなど）、およびすべてのボリュームとその内容（ファイル、ディレクトリ、LUN、NVMeネームスペースなど）のコピーが作成されます。

タスク概要

整合性グループのクローンを作成する場合、現在の構成でクローンを作成できますが、ボリュームの内容はそのままにするか、既存の整合性グループのSnapshotに基づいてクローンを作成できます。

クローニングする場合、整合性グループ全体をクローニングする必要があります。階層関係内の子整合性グループを個別にクローニングすることはできません。クローニングできるのは、完全な整合性グループ設定のみです。

整合性グループのクローニング時に、次のコンポーネントはクローニングされません。

- igroup
- LUNマップ
- NVMeサブシステム
- NVMeネームスペースのサブシステム マップ

開始する前に

- コンシステンシ グループをクローンする場合、共有名が指定されていないと、ONTAP はクローン ボリュームに対して SMB 共有を作成しません。* ジャンクション パスが指定されていない場合、クローン コンシステンシ グループはマウントされません。
- 整合性グループの現在の構成ボリュームを反映していないスナップショットに基づいて整合性グループのクローンを作成しようとすると、操作は失敗します。
- 整合性グループのクローニング後、適切なマッピング処理を実行する必要があります。

詳細については、[複数のLUNへのigroupのマッピング](#)または[サブシステムへのNVMeネームスペースのマッピング](#)を参照してください。

- 整合性グループのクローニングは、SnapMirrorアクティブ同期関係の整合性グループや、DPボリュームが関連付けられている整合性グループではサポートされません。

System Manager

手順

1. *Storage > Consistency groups*を選択します。
2. *Consistency Group*メニューから、クローンを作成するコンシステンシ グループを選択します。
3. 整合性グループの概要ページの右上で、**Clone** を選択します。
4. クローニング後の新しい整合性グループの名前を入力するか、デフォルトの名前をそのまま使用します。
 - a. "シンプロビジョニング"を有効にするかどうかを選択します。
 - b. コンシステンシ グループをそのソースから切り離し、クローンされたコンシステンシ グループに追加のディスク領域を割り当てる場合は、**Split Clone** を選択します。
5. 整合性グループを現在の状態で複製するには、新しいスナップショットの追加 を選択します。

スナップショットに基づいて整合性グループのクローンを作成するには、*既存のスナップショットを使用する*を選択します。このオプションを選択すると、新しいサブメニューが開きます。クローン処理のベースとして使用するスナップショットを選択します。

6. *Clone*を選択します。
7. **Consistency Group** メニューに戻り、整合性グループが複製されたことを確認します。

CLI

ONTAP 9.14.1以降では、CLIとクラスタ管理者のクレデンシャルを使用して整合性グループをクローニングできます。

開始する前に

- このタスクを実行するには、admin権限レベルが必要です。
- ONTAP 9.15.1以降では、admin権限レベルのすべてのユーザがこのタスクを実行できます。ONTAP 9.14.1では、このタスクを実行するには、クラスタ管理者またはSVMの管理者である必要があります。

整合性グループのクローニング

1. `consistency-group clone create` コマンドは、現在のポイントインタイムステータスで整合性グループのクローンを作成します。スナップショットに基づいてクローン操作を実行するには、`-source-snapshot` パラメータを指定します。

```
consistency-group clone create -vserver svm_name -consistency-group clone_name -source-consistency-group consistency_group_name [-source-snapshot snapshot_name]
```

```
`consistency-group clone create`
```

の詳細については、[link:https://docs.netapp.com/us-en/ontap-cli/search.html?q=consistency-group+clone+create](https://docs.netapp.com/us-en/ontap-cli/search.html?q=consistency-group+clone+create)["ONTAP コマンドリファレンス"]を参照してください。

次の手順

- [複数のLUNへのigroupのマッピング](#)
- [サブシステムへのNVMeネームスペースのマッピング](#)

ONTAPコンシステンシーグループを削除する

不要になった整合性グループは削除できます。

タスク概要

- 整合性グループを削除すると、整合性グループのインスタンスが削除され、構成ボリュームまたはLUNには影響しません。整合性グループを削除しても、各ボリュームに存在するスナップショットは削除されませんが、整合性グループのスナップショットとしてアクセスできなくなります。ただし、これらのスナップショットは、通常のボリューム単位のスナップショットとして引き続き管理できます。
- 整合性グループ内のボリュームがすべて削除されると、整合性グループが自動的に削除されます。
- 親整合性グループを削除すると、関連付けられている子整合性グループがすべて削除されます。
- ONTAP 9.10.1～9.12.0のバージョンをご利用の場合、ボリューム自体を削除した場合にのみ、コンシステンシーグループからボリュームを削除できます。この場合、ボリュームはコンシステンシーグループから自動的に削除されます。ONTAP 9.12.1以降では、コンシステンシーグループ自体を削除せずに、コンシステンシーグループからボリュームを削除できます。このプロセスの詳細については、[整合性グループの変更](#)を参照してください。

例 7. 手順

System Manager

1. *Storage > Consistency groups*を選択します。
2. 削除する整合性グループを選択します。
3. 整合性グループの名前の横にあるを選択し、次に*削除*を選択します。

CLI

ONTAP 9.14.1以降では、CLIを使用して整合性グループを削除できます。

開始する前に

- このタスクを実行するには、admin権限レベルが必要です。
- ONTAP 9.15.1以降では、admin権限レベルのすべてのユーザがこのタスクを実行できます。ONTAP 9.14.1では、このタスクを実行するには、クラスタ管理者またはSVMの管理者である必要があります。

整合性グループの削除

1. 整合性グループを削除します。

```
consistency-group delete -vserver svm_name -consistency-group  
consistency_group_name
```

SnapMirrorアクティブ同期

はじめに

ONTAP SnapMirror Active Syncについて学ぶ

SnapMirror Active Sync (SnapMirror Business Continuity (SM-BC) と呼ばれる) は、完全なサイト障害が発生した場合でもビジネスサービスの機能を継続できるようにします。このテクノロジーにより、アプリケーションは手動による介入やカスタムスクリプトなしに、セカンダリコピーにシームレスにフェイルオーバーできます。

NetApp SnapMirror Active Sync (SM-AS) は、自動フェイルオーバー機能を備えた、よりきめ細やかで低コスト、そして使いやすいアプリケーションレベルの保護を実現するように設計されています。SnapMirror Active Syncにより、サイト全体の障害発生時でも、ミッションクリティカルなビジネスサービスの運用を継続できます。SnapMirror Active Syncを使用すると、地理的に分散したサイト間で、アプリケーションの複数のボリュームを（整合性グループに追加することで）同期的にレプリケートできます。プライマリコピーが中断された場合、セカンダリコピーに自動的にフェイルオーバーできるため、Tier 1アプリケーションのビジネス継続性を確保できます。

一部の国では、金融機関の規制により、企業はセカンダリ データ センターから定期的にサービスを受けることが義務付けられています。SnapMirror active sync は、高可用性クラスターにより、ビジネス継続性のためにこれらのデータ センターの切り替えを可能にします。

ONTAP 9.9.1以降で利用可能なSnapMirror Active Syncは、AFFおよびオールフラッシュSANアレイ (ASA) クラスターでサポートされています。プライマリクラスターとセカンダリクラスターは、ASA、ASA r2、またはAFFのいずれか同じタイプである必要があります。SnapMirror Active Syncは、iSCSIまたはFCP LUN、あるいはNVMeネームスペースを持つアプリケーションを保護します。

SnapMirror Active Syncは、対称構成と非対称構成の両方をサポートします。対称アクティブ / アクティブのサポートは、ONTAP 9.15.1で導入されました。対称アクティブ / アクティブ構成では、保護されたLUNの両方のコピーが双方向同期レプリケーションで読み取りおよび書き込みI/O処理を実行できるため、各LUNコピーがローカルI/O要求に対応できます。



2024年7月より、これまでPDF形式で公開されていたテクニカルレポートの内容がONTAP製品ドキュメントに統合されました。ONTAP SnapMirror Active Syncドキュメントには、_TR-4878 : SnapMirror Active Sync_ の内容が含まれるようになりました。

メリット

SnapMirrorアクティブ同期には次のようなメリットがあります。

- ビジネスクリティカルなアプリケーションの継続的可用性
- 重要なアプリケーションをプライマリ サイトとセカンダリ サイトで交互にホストすることが可能
- 整合性グループを使用して従属書き込み順序の整合性を維持し、シンプルなアプリケーション管理を実現する
- アプリケーションごとにフェイルオーバーをテストできる
- アプリケーションの可用性に影響を与えることなくミラー クローンを瞬時に作成できる
- 保護されているワークロードと保護されていないワークロードを同じONTAPクラスターに導入できる

- LUN、NVMe 名前空間、NVMe サブシステム、またはストレージ ユニットの ID は同じまなので、アプリケーションはそれらを共有仮想デバイスとして認識します。
- セカンダリ クラスタを柔軟に再利用して、クローンを瞬時に作成することで、アプリケーションのパフォーマンスや可用性に影響を与えることなく、開発テスト、UAT、レポート作成にアプリケーションを使用できる

SnapMirror Active Syncを使用すると、データLUNまたはNVMe名前スペースを保護でき、災害発生時のビジネス継続性を確保するために、アプリケーションを透過的にフェイルオーバーできます。詳細については、"[ユースケース](#)"をご覧ください。

主要な概念

SnapMirror Active Syncは、整合性グループを使用してデータの複製を確実に行います。SnapMirror Active SyncはONTAP MediatorまたはONTAP 9.17.1以降ではCloud Mediatorを使用して自動フェイルオーバーを実現し、災害発生時でもデータが確実に提供されるようにします。SnapMirror Active Syncの導入を計画する際には、SnapMirror Active Syncとそのアーキテクチャの基本概念を理解することが重要です。

非対称と対称

対称アクティブ / アクティブ構成では、両方のサイトがアクティブ I/O のためにローカル ストレージにアクセスできます。対称アクティブ / アクティブは、VMware vMSC、Windows Failover Cluster with SQL、Oracle RAC などのクラスタ化されたアプリケーションに最適化されています。

非対称アクティブ / アクティブ構成では、セカンダリ サイトのデータは LUN、名前スペース、またはストレージ ユニットのプロキシされます。

詳細については、[SnapMirrorアクティブ同期アーキテクチャ](#)を参照してください。

整合性グループ

AFFおよびASAシステムでは、"[整合性グループ](#)"は、ビジネス継続性のために保護する必要があるアプリケーション ワークロードの整合性を保証するFlexVolボリュームの集合です。ASA r2システムでは、整合性グループはストレージ ユニットの集合です。

整合性グループの目的は、ボリュームまたはストレージユニットのコレクションのスナップショットイメージを同時に取得し、ある時点でのコレクションの「crash consistent state（障害など予期しないシャットダウン時と同様）」の状態のコピーを確保することです。整合性グループにより、データセットのすべてのボリュームが静止し、正確に同じ時点でスナップショットが作成されます。これにより、データセットをサポートするボリュームまたはストレージユニット全体で、データの整合性が保たれた復元ポイントが提供されます。これにより、整合性グループは依存関係にある書き込み順序の整合性を維持します。ビジネス継続性のためにアプリケーションを保護する場合は、このアプリケーションに対応するボリュームまたはストレージユニットのグループを整合性グループに追加して、ソースとデスティネーションの整合性グループ間にデータ保護関係を確立する必要があります。ソースとデスティネーションの整合性グループには、同じ数とタイプのボリュームが含まれている必要があります。

コンスティチュエント

SnapMirrorアクティブ同期関係で保護されている整合性グループの一部である個々のボリューム、LUN、または NVMe 名前空間（ONTAP 9.17.1 以降）。

ONTAP Mediator

"[ONTAP Mediator](#)"は、ピア接続されたONTAPクラスタとノードのヘルス情報を受信し、両者間のオーケストレーションを行い、各ノード/クラスタが正常かつ稼働しているかどうかを判断します。ONTAP Mediatorは、以下のヘルス情報を提供します：

- ピア関係にあるONTAPクラスタ
- ピア関係にあるONTAPクラスタ ノード
- (SnapMirrorアクティブ同期関係にあるフェイルオーバー ユニットを定義する) 整合性グループ。各整合性グループの次の情報が提供されます。
 - レプリケーション状態：初期化なし、同期中、または同期外
 - プライマリ コピーをホストしているクラスタ
 - 処理コンテキスト (計画的フェイルオーバーに使用)

このONTAP Mediatorの健全性情報により、クラスタは障害のタイプを区別し、自動フェイルオーバーを実行するかどうかを判断できます。ONTAP Mediatorは、両方のONTAPクラスタ (プライマリおよびセカンダリ) とともに、SnapMirrorアクティブ同期クォーラムを構成する3つのメンバーの1つです。合意に至るには、クォーラムの2つ以上のメンバーが特定の処理に同意する必要があります。



ONTAP 9.15.1以降、System ManagerはどちらのクラスタからでもSnapMirrorアクティブ同期関係のステータスを表示します。また、System ManagerでどちらのクラスタからでもONTAP Mediatorのステータスを監視することもできます。以前のリリースのONTAPでは、System Managerはソース クラスタからのSnapMirrorアクティブ同期関係のステータスを表示していました。

ONTAP Cloud Mediator

ONTAP Cloud MediatorはONTAP 9.17.1以降で利用できます。ONTAP Cloud MediatorはONTAP Mediatorと同じサービスを提供しますが、NetApp Consoleを使用してクラウドでホストされる点が異なります。

計画的フェイルオーバー

SnapMirrorアクティブ同期関係でのコピーの役割を変更する手動処理。プライマリ サイトがセカンダリ サイトに、セカンダリ サイトがプライマリ サイトになります。

自動計画外フェイルオーバー (AUFO)

ミラー コピーへのフェイルオーバーを実行する自動処理。この処理には、プライマリ コピーが使用できないことを検出するためにONTAP Mediatorが必要です。

プライマリファーストとプライマリバイアス

SnapMirrorアクティブ同期では、ネットワークが分割された場合のI/O処理にプライマリ コピーを優先するプライマリファーストの原則が使用されます。

プライマリバイアスとは、SnapMirrorアクティブ同期で保護されたデータセットの可用性を向上させる特別なクォーラムの実装です。どちらのクラスタからもONTAP Mediatorにアクセスできない場合に、プライマリ コピーが使用可能だと、プライマリバイアスが効果を発揮します。

ONTAP 9.15.1以降では、SnapMirrorアクティブ同期でプライマリファーストとプライマリバイアスがサポートされます。プライマリ コピーはSystem Managerで指定され、REST APIおよびCLIを使用して出力されます。

非同期 (OOS)

アプリケーションI/Oがセカンダリ ストレージ システムにレプリケートされていない場合、**out of sync**として報告されます。out of sync状態とは、セカンダリ ボリュームがプライマリ (ソース) と同期されておらず、SnapMirrorレプリケーションが実行されていないことを意味します。

ミラー状態が `Snapmirrored` の場合、SnapMirror関係が確立され、データ転送が完了していることを示しま

す。つまり、デスティネーション ボリュームはソース ボリュームと最新の状態です。

SnapMirrorアクティブ同期は自動再同期をサポートしており、コピーをInSync状態に戻すことができます。

ONTAP 9.15.1 以降、SnapMirror アクティブ同期は["ファンアウト構成における自動再構成"](#)をサポートします。

均一な構成と非均一な構成

- 均一なホストアクセス とは、両サイトのホストが両サイトのストレージ クラスタへのすべてのパスに接続されていることを意味します。サイト間パスは長距離にわたって拡張されます。
- 非均一ホストアクセス とは、各サイトのホストが同じサイト内のクラスタにのみ接続されることを意味します。サイト間パスとストレッチパスは接続されません。



均一なホスト アクセスは、すべてのSnapMirrorアクティブ同期構成でサポートされます。不均一なホスト アクセスは、対称アクティブ / アクティブ構成でのみサポートされます。

RPOゼロ

RPOはRecovery Point Objective（目標復旧時点）の略で、所定の期間内に許容可能とみなされるデータ損失量を指します。RPOゼロとは、データ損失が一切許容されないことを意味します。

RTOゼロ

RTOはRecovery Time Objective（目標復旧時間）の略で、システム停止、障害、またはその他のデータ損失イベントが発生してから、アプリケーションが無停止で通常の処理に戻るまでに許容可能とみなされる時間です。RTOゼロとは、ダウンタイムが一切許容されないことを意味します。

ONTAPバージョンによるSnapMirrorアクティブ同期構成のサポート

SnapMirrorアクティブ同期のサポートは、ONTAPのバージョンによって異なります：

ONTAPのバージョン	サポートされているクラスタ	サポートされるプロトコル	サポートされている構成

9.17.1以降	• AFF • ASA • Cシリーズ • ASA r2	• iSCSI • FC • VMware ワークロード向け NVMe	• 非対称アクティブ / アクティブ  非対称アクティブ / アクティブは ASA r2 と NVMe をサポートしています。NVMe サポートの詳細については、"NVMe の構成、サポート、制限事項"を参照してください。 • 対称アクティブ / アクティブ
9.16.1以降	• AFF • ASA • Cシリーズ • ASA r2	• iSCSI • FC	• 非対称アクティブ / アクティブ • 対称アクティブ / アクティブ 対称アクティブ / アクティブ構成は、ONTAP 9.16.1 以降で 4 ノードから 4 ノードのクラスタをサポートします。ASA r2 では、2 ノードクラスタのみがサポートされます。

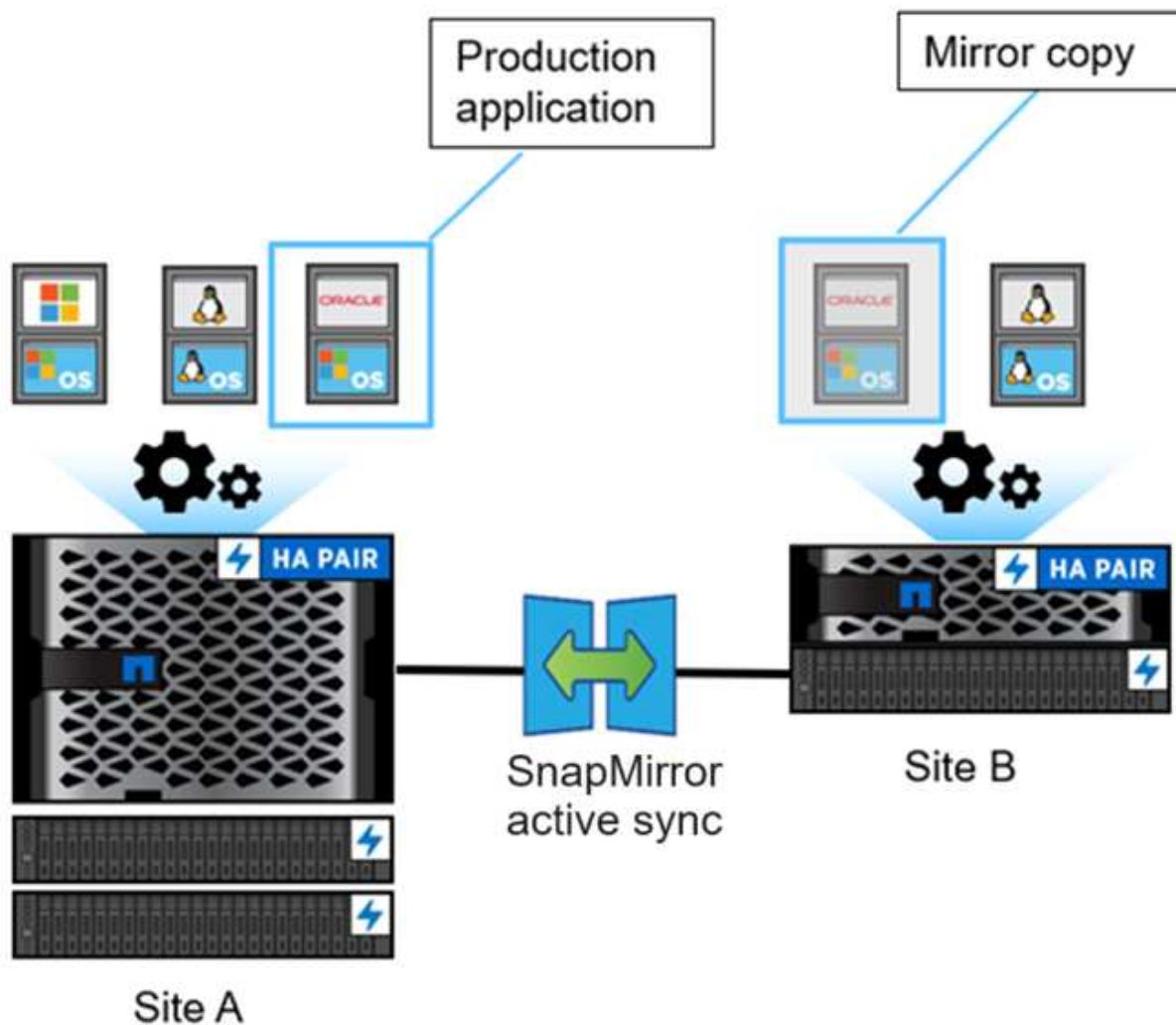
9.15.1以降	• AFF • ASA • Cシリーズ	• iSCSI • FC	• 非対称アクティブ / アクティブ • 対称アクティブ / アクティブ対称アクティブ / アクティブ構成は、ONTAP 9.15.1で2ノードクラスタをサポートします。2ノード対2ノードクラスタおよび4ノード対4ノードクラスタは、ONTAP 9.16.1以降でサポートされます。
9.9.1以降	• AFF • ASA • Cシリーズ	• iSCSI • FC	非対称アクティブ / アクティブ

プライマリ クラスタとセカンダリ クラスタは同じタイプである必要があります ("ASA"、"ASA r2"、またはAFF)。

ONTAP SnapMirror アクティブ同期アーキテクチャ

SnapMirror Active Syncアーキテクチャは、両方のクラスタでアクティブなワークロードを可能にし、プライマリワークロードを両方のクラスタから同時に処理できます。一部の国では、金融機関の規制により、セカンダリ データ センターからも定期的にサービスを提供すること（「Tick-Tock」 デプロイメントと呼ばれる）が求められており、SnapMirror Active Syncによってこれが可能になります。

ビジネス継続性を確保するためのデータ保護関係は、ソース ストレージ システムとデスティネーション ストレージ システムの間に作成されます。これは、ストレージ仮想マシン (SVM) 内の異なるボリュームからアプリケーション固有のLUNまたはNVMeネームスペースをコンシステンシーグループに追加することで実現されます。通常の運用では、エンタープライズアプリケーションはプライマリコンシステンシーグループに書き込みを行い、プライマリコンシステンシーグループはこのI/Oをミラーコンシステンシーグループに同期的に複製します。



データ保護関係にはデータの2つの個別のコピーが存在するにもかかわらず、SnapMirror active syncは同じLUNまたはNVMeネームスペースIDを維持するため、アプリケーションホストはこれを複数のパスを持つ共有仮想デバイスと認識し、一度に1つのLUNまたはNVMeネームスペースコピーのみに書き込みます。障害によってプライマリストレージシステムがオフラインになると、ONTAPはこの障害を検出し、Mediatorを使用して再確認を行います。ONTAPとMediatorのどちらもプライマリサイトにpingを送信できない場合、ONTAPは自動フェイルオーバー処理を実行します。このプロセスにより、以前はフェイルオーバーのために必要だった手動による介入やスクリプト作成が不要になり、特定のアプリケーションのみをフェイルオーバーできます。

その他の考慮事項：

- ビジネス継続性を目的とする保護の対象から外れた、ミラーされていないボリュームがサポートされる
- ビジネス継続性を目的として保護されているボリュームでは、他のSnapMirror非同期関係は1つのみサポートされる
- ビジネス継続性を目的とする保護では、カスケードトポロジはサポートされない

仲介者の役割

SnapMirror active syncは、メディエーターを使用してSnapMirror active syncコピーの受動的な監視を行います。

す。ネットワークが分断された場合、または一方のコピーが使用できなくなった場合、SnapMirror active syncはメディアーターを使用して、どちらのコピーがI/O処理を継続するかを決定し、もう一方のコピーのI/O処理を停止します。オンプレミスONTAP Mediatorに加えて、ONTAP 9.17.1以降では、ONTAP Cloud Mediatorをインストールすることで、クラウド環境で同様の機能を提供できます。ONTAP MediatorとONTAP Cloud Mediatorのどちらか一方を使用できますが、両方を同時に使用することはできません。

Mediatorは、SnapMirrorアクティブ同期構成においてパッシブ クォーラム監視として重要な役割を果たし、クォーラムの維持を確保し、障害発生時のデータ アクセスを容易にします。コントローラのpingプロキシとして機能し、ピア コントローラの稼働状態を確認します。Mediatorはスイッチオーバー処理を積極的にトリガーすることはありませんが、ネットワーク通信に問題が発生した場合に、正常なノードがパートナーのステータスを確認できるようにするという重要な機能を提供します。クォーラム監視としての役割において、ONTAP Mediatorはピア クラスタへの代替パス（実質的にはプロキシとして機能）を提供します。

さらに、クラスタがクォーラム プロセスの一部としてこの情報を取得できるようにします。通信には、ノード管理 LIF とクラスタ管理 LIF を使用します。サイト障害とInterSwitch Link (ISL) 障害を区別するために、複数のパスを介して冗長接続を確立します。イベントが原因でクラスタが Mediator ソフトウェアおよびそのすべてのノードとの接続を失うと、到達不能とみなされます。これによりアラートがトリガーされ、セカンダリ サイトのミラー コンシステンシ グループへの自動フェイルオーバーが有効になり、クライアントの中断のない I/O が保証されます。レプリケーション データ パスはハートビート メカニズムに依存しており、ネットワークの障害またはイベントが一定期間を超えて継続すると、ハートビート障害が発生し、関係が同期されなくなる可能性があります。ただし、別のポートへの LIF フェイルオーバーなどの冗長パスが存在すると、ハートビートが維持され、このような中断を防ぐことができます。

ONTAP Mediator

ONTAP Mediatorは、監視対象の2つのONTAPクラスタとは別の3番目の障害ドメインにインストールされます。このセットアップには、3つの主要コンポーネントがあります：

- SnapMirrorアクティブ同期プライマリ整合性グループをホストするプライマリONTAPクラスタ
- ミラー整合性グループをホストするセカンダリONTAPクラスタ
- ONTAP Mediator

ONTAP Mediator は次の目的で使用されます：

- クォーラムの確立
- 自動フェイルオーバー（AUFO）による継続的可用性
- 計画的フェイルオーバー（PFO）



ONTAP Mediator 1.7 は、ビジネス継続性のために 10 個のクラスタ ペアを管理できます。



ONTAP Mediatorが利用できない場合、計画的フェイルオーバーや自動フェイルオーバーは実行できません。アプリケーション データは中断することなく同期的にレプリケーションを継続し、データ損失は発生しません。

ONTAP Cloud Mediator

ONTAP 9.17.1以降、ONTAP Cloud MediatorはNetApp Consoleでクラウドベースのサービスとして利用可能になり、SnapMirror Active Syncと連携して使用できます。ONTAP Mediatorと同様に、ONTAP Cloud MediatorはSnapMirror Active Sync関係において以下の機能を提供します：

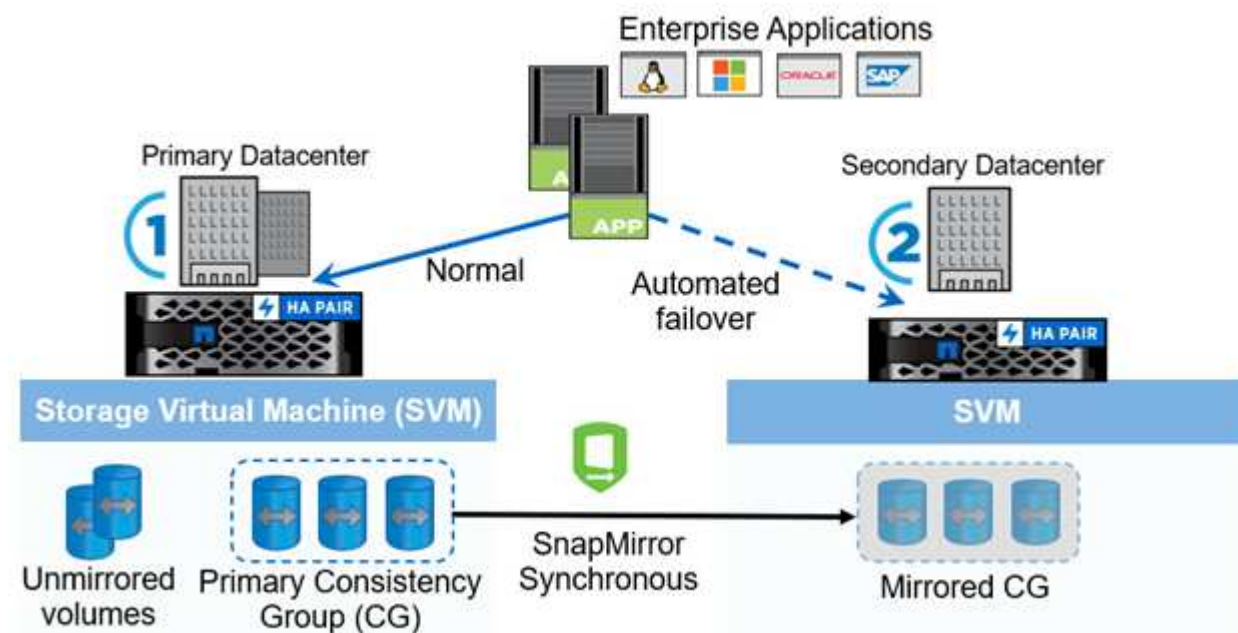
- HAまたはSnapMirrorアクティブ同期メタデータ用の永続的かつ隔離されたストアを提供します。

- コントローラの稼働を確認するpingプロキシとして機能します。
- クォーラムを判定するために、ノードの健全性を同期的に照会します。

ONTAP Cloud Mediatorは、SnapMirror Active Syncの導入を簡素化します。NetApp Consoleクラウド サービスを、管理が不要な第3サイトとして使用します。ONTAP Cloud Mediatorサービスは、オンプレミスのONTAP Mediatorと同じ機能を提供しますが、ONTAP Cloud Mediatorは第3サイトの維持に伴う運用上の複雑さを軽減します。一方、ONTAP Mediatorはパッケージとして提供されており、独立した電源とネットワーク インフラを備えた第3サイトで稼働するLinuxホストにインストールする必要があります。

SnapMirrorアクティブ同期操作ワークフロー

次の図は、SnapMirrorアクティブ同期の設計の概要を表しています。



この図は、プライマリ データセンターのStorage VM (SVM) でホストされているエンタープライズ アプリケーションを示しています。SVMには5つのボリュームがあり、そのうちの3つは整合性グループに属しています。整合性グループ内の3つのボリュームはセカンダリ データセンターにミラーリングされています。通常は、書き込み処理がいずれもプライマリ データセンターに対して実行されます。つまり、そのデータセンターがI/O処理のソースとして機能し、セカンダリ データセンターがデスティネーションとして機能します。

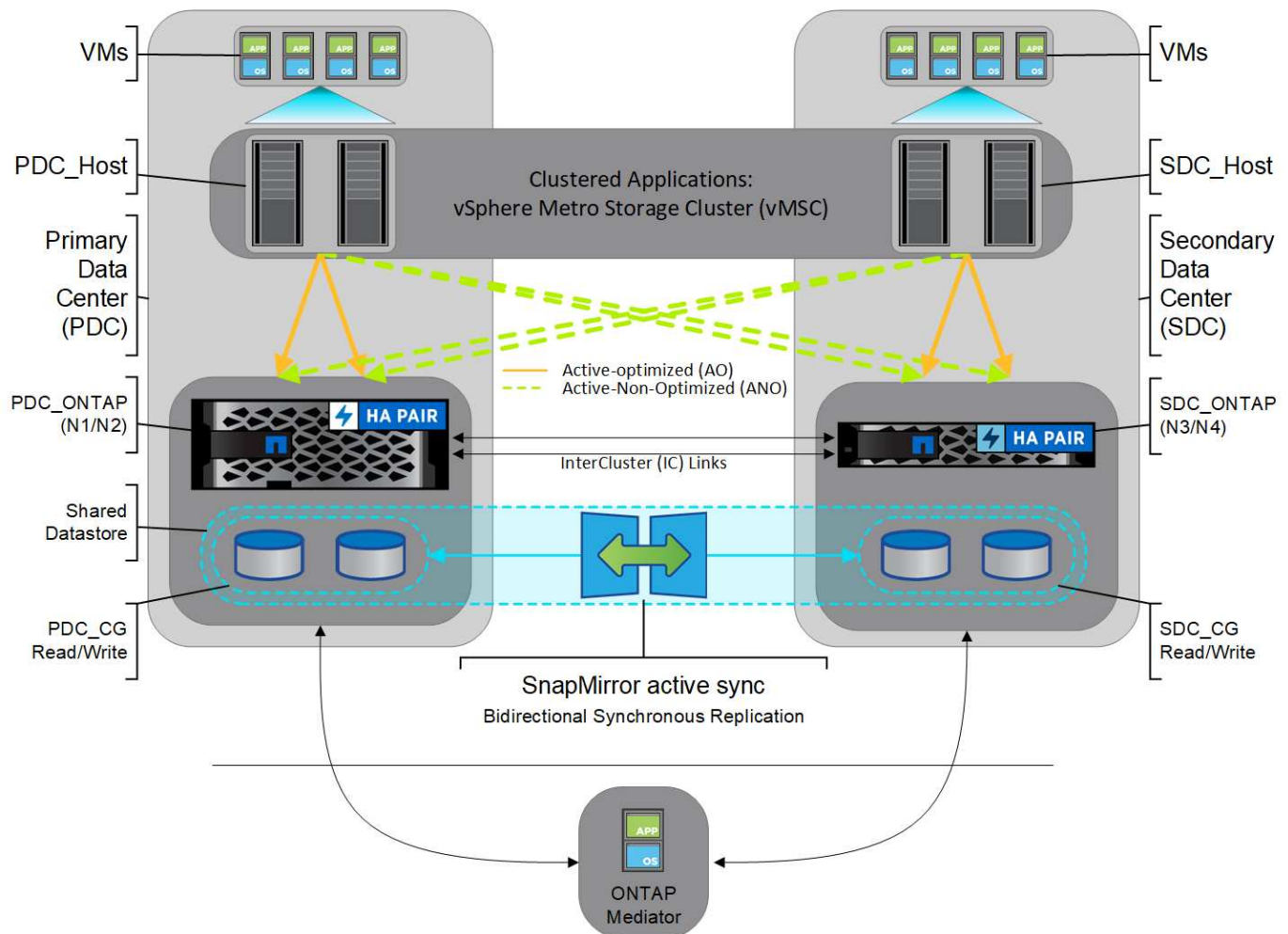
プライマリ データ センターで災害が発生した場合、ONTAPはセカンダリ データ センターをプライマリとして動作させ、すべてのI/O操作を処理します。処理対象となるのは、コンシステンシ グループ内でミラーリングされているボリュームのみです。SVM上の他の2つのボリュームに関連する操作は、災害の影響を受けません。

対称アクティブ / アクティブ

SnapMirrorアクティブ同期は、非対称ソリューションと対称ソリューションを提供します。

非対称構成 では、プライマリ ストレージ コピーはアクティブ最適化パスを公開し、クライアントI/Oをアクティブに処理します。セカンダリ サイトはI/Oにリモート パスを使用します。セカンダリ サイトのストレージ パスはアクティブ非最適化パスとみなされます。書き込みLUNへのアクセスはセカンダリ サイトからプロキシされます。NVMeプロトコルは非対称構成ではサポートされません。

対称アクティブ / アクティブ構成では、アクティブに最適化されたパスは両方のサイトで公開され、ホスト固有であり、構成可能であるため、どちらの側のホストもアクティブ I/O のローカルストレージにアクセスできます。ONTAP 9.16.1 以降、対称アクティブ / アクティブは 2 ノードクラスターと 4 ノードクラスターでサポートされます。SnapMirror Active Sync は、2 ノードクラスターから 2 ノードクラスターの構成と、4 ノードクラスターから 4 ノードクラスターの構成をサポートします。4 ノードクラスターから 2 ノードクラスターの構成、または 2 ノードクラスターから 4 ノードクラスターの構成はサポートされていません。ONTAP 9.17.1 以降、対称アクティブ / アクティブ構成は、2 ノードクラスターで NVMe プロトコルをサポートします。



対称アクティブ / アクティブは、VMware Metro Storage Cluster、Oracle RAC、SQLを使用したWindowsフェイルオーバー クラスタリングなどのクラスターアプリケーションを対象としています。

ONTAP SnapMirror Active Syncのユースケース

グローバルに接続されたビジネス環境の要求により、サイバー攻撃、停電、自然災害などの障害が発生した場合に、ビジネス クリティカルなアプリケーション データをデータ損失ゼロで迅速に復旧することが求められます。こうした要求は、金融業界や一般データ保護規則（GDPR）などの規制遵守が求められる分野で特に高まっています。

SnapMirrorアクティブ同期のユース ケースは次のとおりです。

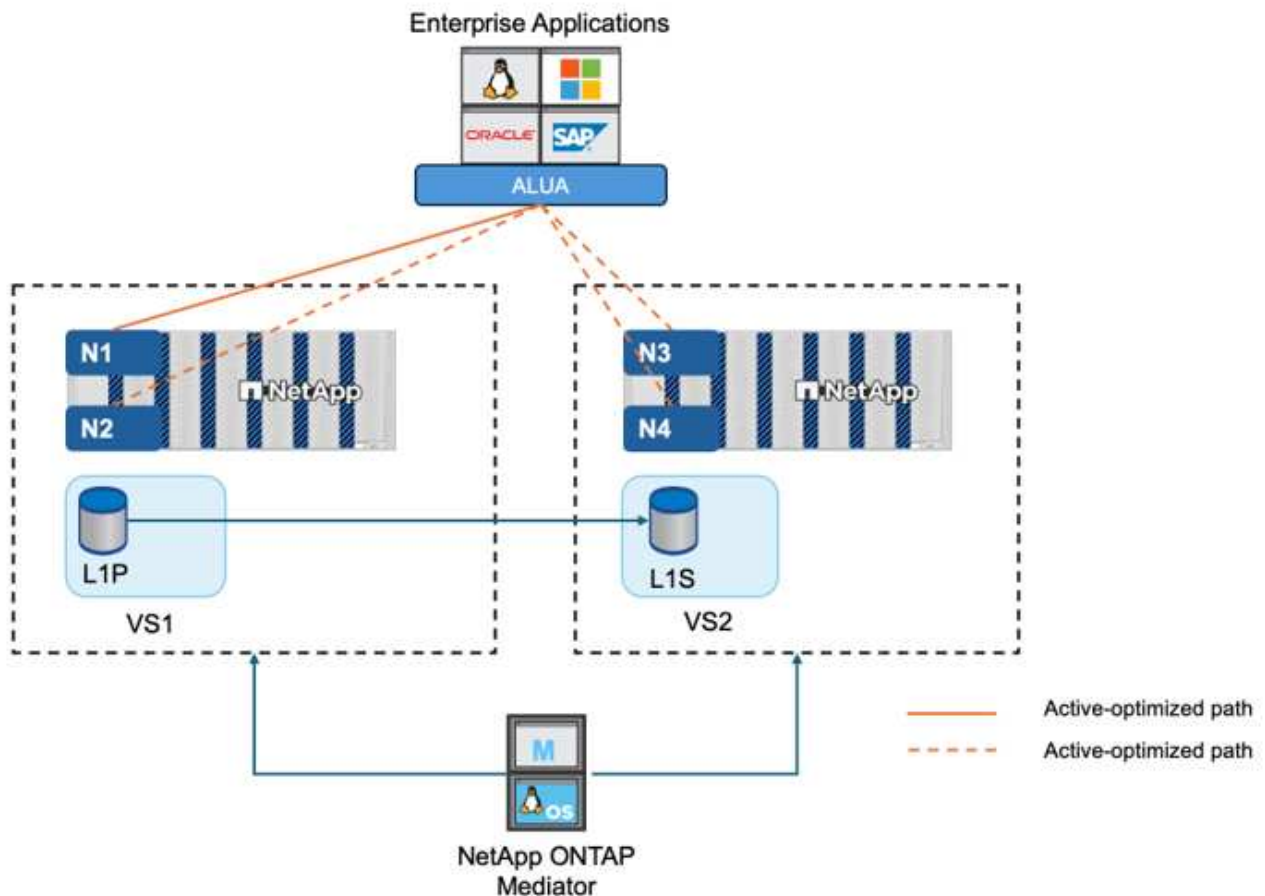
ゼロ復旧時間目標（RTO）を実現するアプリケーション展開

SnapMirror Active Sync デプロイメントでは、プライマリクラスターとセカンダリクラスターが存在します。プラ

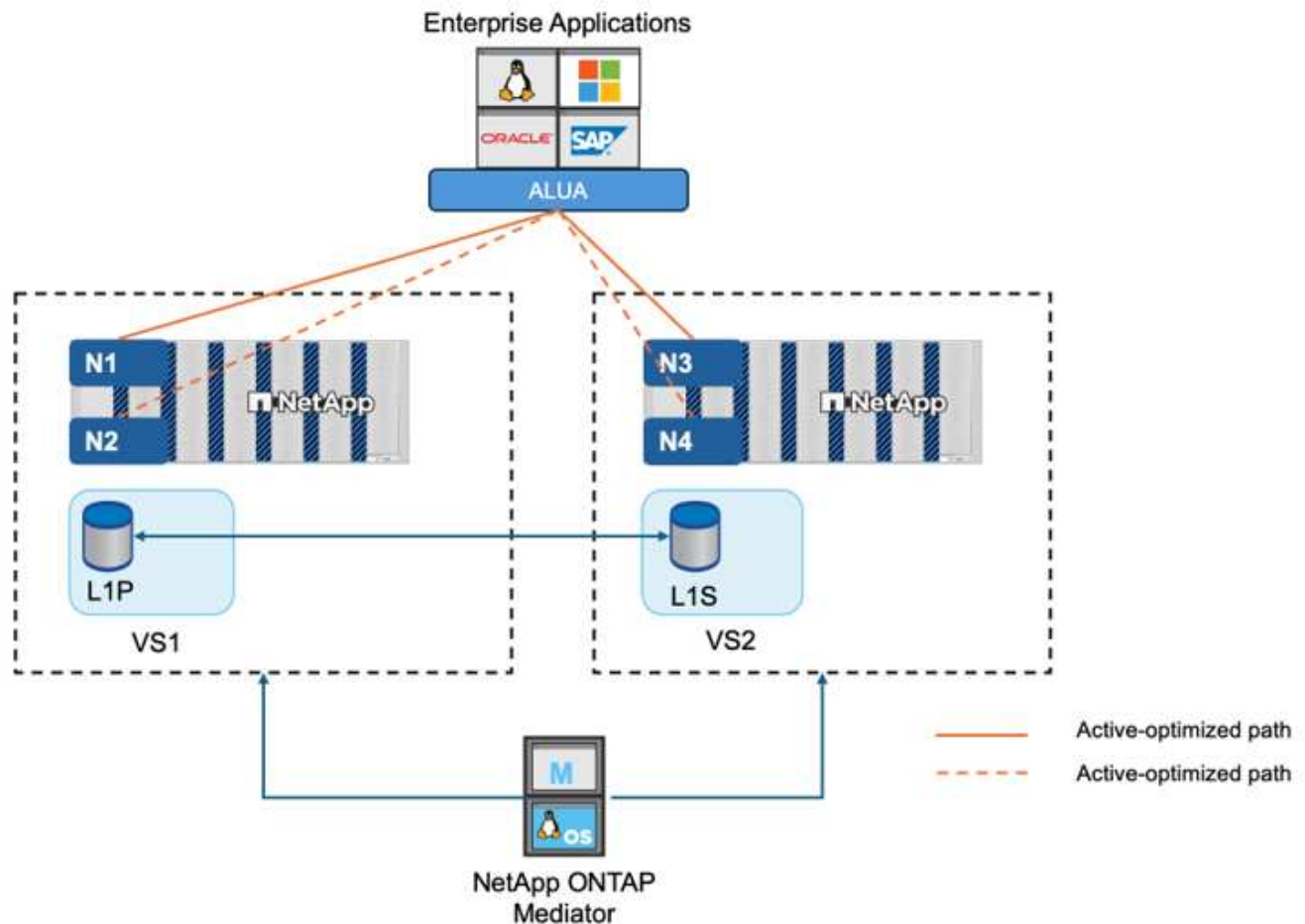
イマリクラスタの LUN `L1P`には、セカンダリにミラー `L1S`があります。両方の LUN は同じシリアル ID を共有し、ホストには読み取り / 書き込み LUN として報告されます。ただし、非対称構成では、読み取りおよび書き込み操作はプライマリ LUN `L1P`に対してのみ実行されます。ミラー `L1S`への書き込みはプロキシによって実行されます。

ゼロ **RTO** または透過的アプリケーション フェイルオーバー (**TAF**) のためのアプリケーション展開

TAFは、ホストMPIOソフトウェアベースのパスフェイルオーバーに基づいており、ストレージへの無停止アクセスを実現します。プライマリLUNコピー (L1P) とミラーコピー (L1S) の両方が同じID (シリアル番号) を持ち、ホストには読み取り/書き込み可能として報告されます。ただし、非対称構成では、読み取りと書き込みはプライマリボリュームによってのみ処理されます。ミラーコピーへのI/Oは、プライマリコピーにプロキシされます。ホストのL1への優先パスは、非対称論理ユニットアクセス (ALUA) のアクセス状態がアクティブ最適化 (A/O) であるVS1:N1です。ONTAPメディアーターは、主にプライマリストレージでストレージ障害が発生した場合にフェイルオーバー (計画的または計画外) を実行するために、導入の一部として必要です。



TAFは、自動フェイルオーバーと自動フェイルオーバーデュプレックスの2つのモードで動作します。自動フェイルオーバーでは、読み取りと書き込みはプライマリボリュームのみで処理されるため、ミラーコピー (ミラーコピー自身は書き込み処理を実行できません) へのI/Oはプライマリコピーにプロキシされます。自動フェイルオーバーデュプレックスでは、プライマリコピーとセカンダリコピーの両方でI/Oを処理できるため、プロキシは不要です。



ONTAP 9.17.1 でホスト アクセスに NVMe を使用している場合は、AutomatedFailoverDuplex ポリシーのみがサポートされます。

SnapMirrorアクティブ同期では、ALUAが使用されます。ALUAは、アプリケーション ホストのマルチパス ソフトウェアがアドバタイズされたパス、優先順位、アクセスの可否情報を使用して、アプリケーション ホストがストレージ アレイと通信できるようにするメカニズムです。ALUAは、LUNなどを所有するコントローラへのアクティブ / 最適化パスを、プライマリ パスで障害が発生した場合にのみ使用するアクティブ / 非最適パスとしてマークします。

SnapMirror アクティブ同期でNVMeプロトコルを使用すると、非対称ネームスペースアクセス（ANA）が使用されます。これにより、アプリケーションホストは、保護されているNVMeネームスペースへの最適化されたパスと最適化されていないパスを検出できます。ONTAP NVMeターゲットは適切なパス状態を公開し、アプリケーションホストが保護されたNVMeネームスペースに最適なパスを使用できるようにします。

クラスタ アプリケーション

VMware Metro Storage Cluster、Oracle RAC、Windows Failover Clustering with SQLなどのクラスタ化されたアプリケーションでは、パフォーマンス オーバーヘッドなしで他のサイトにVMをフェイルオーバーできるように、同時アクセスが必要です。SnapMirror active sync symmetric アクティブ / アクティブは、双方向レプリケーションによってローカルでIOを提供し、クラスタ化されたアプリケーションの要件を満たします。ONTAP 9.16.1以降では、symmetric アクティブ / アクティブは4ノードクラスタ構成でサポートされ、ONTAP 9.15.1の2ノードクラスタの制限から拡張されました。

災害シナリオ

地理的に分散したサイト間で、アプリケーション用の複数のボリュームを同期的にレプリケートします。プラ

イマリが停止した場合に自動的にセカンダリ コピーにフェイルオーバーできるため、ティア1アプリケーションのビジネス継続性を確保できます。プライマリ クラスタをホストしているサイトで災害が発生すると、ホストのマルチパス ソフトウェアはそのクラスタを経由するすべてのパスを停止とマークし、セカンダリ クラスタからのパスを使用します。その結果、ONTAP Mediatorによる無停止でのミラー コピーへのフェイルオーバーが可能になります。

拡張アプリケーション サポート

SnapMirror active syncは、使いやすいアプリケーション レベルの粒度と自動フェイルオーバーにより柔軟性を実現します。SnapMirror active syncは、実績のあるSnapMirror同期レプリケーションをIPネットワーク経由で使用して、LANまたはWAN経由で高速にデータをレプリケートし、仮想環境と物理環境の両方でOracle、Microsoft SQL Serverなどのビジネス クリティカルなアプリケーションの高いデータ可用性と高速なデータレプリケーションを実現します。

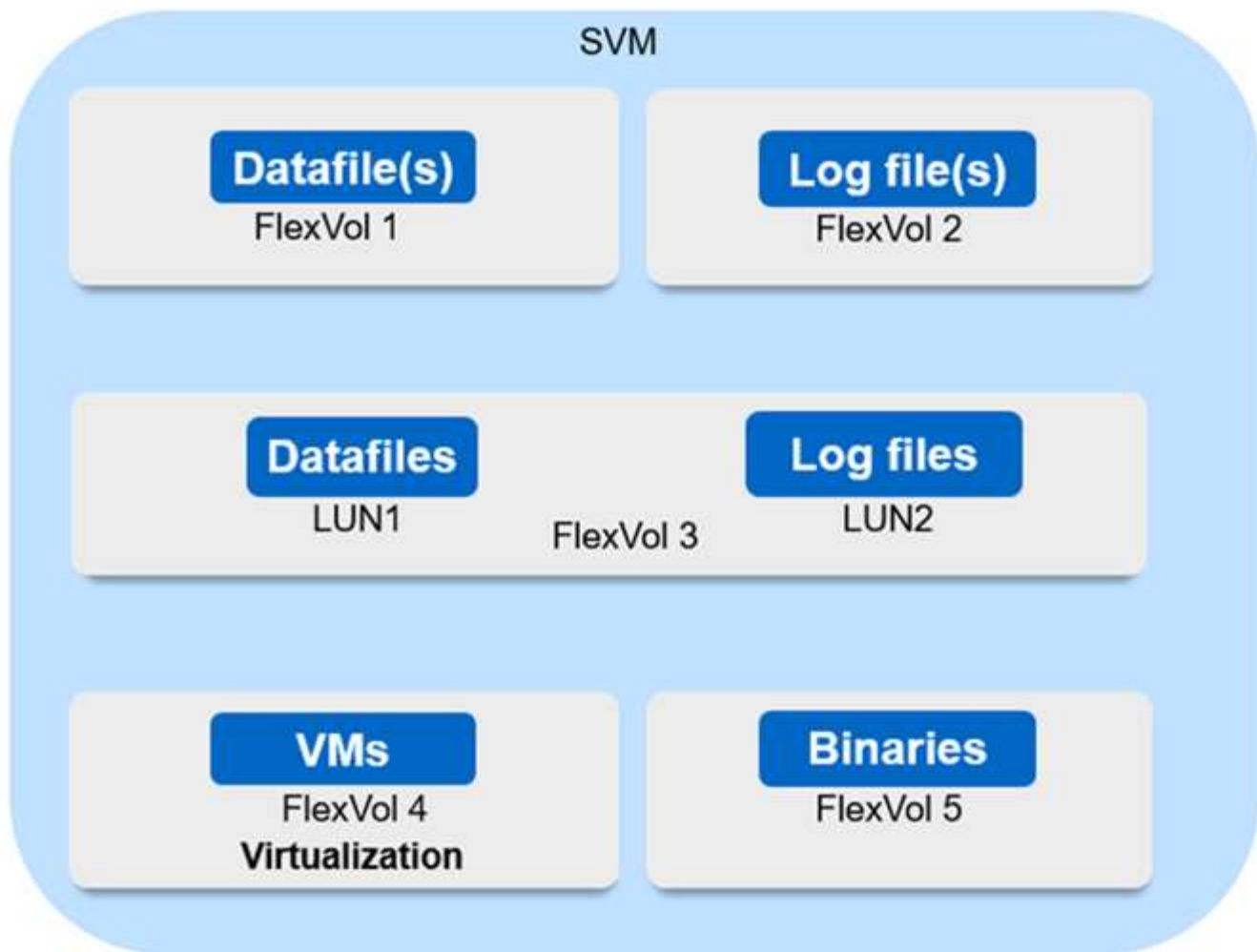
SnapMirror Active Syncは、サイト障害が発生した場合でも、セカンダリコピーへのTAFにより、ミッションクリティカルなビジネスサービスの運用を継続できるようにします。このフェイルオーバーをトリガーするために、手動による介入や追加のスクリプトは必要ありません。

ONTAP SnapMirror Active Syncの導入戦略とベストプラクティス

データ保護戦略において、ビジネス継続性のために保護が必要なワークロードを明確に特定することが重要です。データ保護戦略において最も重要なステップは、エンタープライズ アプリケーションのデータ レイアウトを明確にすることです。これにより、ボリュームをどのように分散し、ビジネス継続性を保護するかを決定できます。フェイルオーバーはアプリケーションごとに整合性グループ レベルで発生するため、必要なデータボリュームを整合性グループに追加してください。

SVM構成

次の図は、SnapMirrorアクティブ同期に推奨されるStorage VM（SVM）構成を示しています。



- データ ボリュームの場合：

- ランダム リードのワークロードはシーケンシャル ライトとは切り離されています。そのため、データ ベースのサイズによりますが、データ ファイルとログ ファイルは通常、別々のボリュームに配置されます。

- 重要な大規模データベースの場合、単一のデータ ファイルがFlexVol 1に、対応するログ ファイルがFlexVol 2にあります。

- 統合を効率化するために、重要でない小規模から中規模のデータベースはグループ化して、すべてのデータ ファイルがFlexVol 1に配置され、対応するログ ファイルがFlexVol 2に配置されるようにします。ただし、このグループ化によって、アプリケーションレベルのきめ細かな対応ができなくなります。

- 別の方法としては、すべてのファイルを同じFlexVol 3に格納し、データ ファイルをLUN1に、ログ ファイルをLUN 2に格納する方法があります。

- 環境が仮想化されている場合は、さまざまなエンタープライズ アプリケーションのすべてのVMを1つのデータストアで共有します。通常、VMとアプリケーション バイナリはSnapMirrorを使用して非同期でレプリケートされます。

Plan

ONTAP SnapMirror Active Syncの前提条件

SnapMirrorアクティブ同期の導入を計画する際には、ハードウェア、ソフトウェア、およびシステムのさまざまな構成要件を満たしていることを確認する必要があります。

ハードウェア

次の表は、サポートされているNetAppクラスタ構成の概要を示しています。

クラスタタイプ	サポートされているモデル	サポートされる機能	サポートされる最大クラスタノード数
AFF	A-Series、C-Series	自動フェイルオーバー デュプレックス（対称アクティブ / アクティブ）、自動フェイルオーバー（非対称アクティブ / アクティブ）	• 2（ONTAP 9.9.1以降） • 4（対称アクティブ / アクティブ構成のONTAP 9.16.1）
ASA	A-Series、C-Series	自動フェイルオーバー デュプレックス（対称アクティブ / アクティブ）、自動フェイルオーバー（非対称アクティブ / アクティブ）	• 2（ONTAP 9.9.1以降） • 4（対称アクティブ / アクティブ構成のONTAP 9.16.1）
ASA r2	All	自動フェイルオーバー デュプレックス（対称アクティブ / アクティブ）	• 2（ONTAP 9.17.1以前） • 4（ONTAP 9.18.1以降）

以下の表は、クラスタ タイプ間のレプリケーション機能の概要を示しています。

クラスタタイプ1	クラスタ タイプ 2	レプリケーションはサポートされていますか？
AFF Aシリーズ	AFF Cシリーズ	はい
ASA r2 A シリーズ	ASA r2 Cシリーズ	はい
AFF	ASA	いいえ
ASA	ASA r2	いいえ
ASA r2	ASA r2	はい

ソフトウェア

- ONTAP 9.9.1以降
- ONTAP Mediator 1.2以降
- 次のいずれかを実行している ONTAP Mediator 用の Linux サーバまたは仮想マシン：

ONTAP Mediatorのバージョン	サポートされるLinuxバージョン
1.11	• Red Hat Enterprise Linux ◦ 互換性：9.5¹ ◦ 推奨：10.1、10.0、9.7、9.6、9.4、8.10 • Rocky Linux 10.1、9.7、および 8.10 • Oracle Linux 10.0 および 9.6
1.10	• Red Hat Enterprise Linux ◦ 互換性：9.5¹ ◦ 推奨：10.0、9.6、9.4、8.10 • Rocky Linux 10.0、9.6、および 8.10
1.9.1	• Red Hat Enterprise Linux ◦ 互換性：9.3、9.1、8.9、8.7、8.6、8.5、8.4¹ ◦ 推奨：9.5、9.4、9.2、9.0、8.10、8.8 • Rocky Linux 9.5、8.10
1.9	• Red Hat Enterprise Linux ◦ 互換性：9.3、9.1、8.9、8.7、8.6、8.5、8.4¹ ◦ 推奨：9.5、9.4、9.2、9.0、8.10、8.8 • Rocky Linux 9.5、8.10
1.8	• Red Hat Enterprise Linux： ◦ 互換性：8.7、8.6、8.5、8.4¹ ◦ 推奨：9.4、9.3、9.2、9.1、9.0、8.10、8.9、8.8 • Rocky Linux 9.4、8.10
1.7	• Red Hat Enterprise Linux： ◦ 互換性：8.7、8.6、8.5、8.4¹ ◦ 推奨：9.3、9.2、9.1、9.0、8.9、8.8 • Rocky Linux 9.3、8.9

1.6	- Red Hat Enterprise Linux : - 互換性 : 8.7、8.6、8.5、8.4 ¹ - 推奨 : 9.2、9.1、9.0、8.8 - Rocky Linux 9.2、8.8
1.5	- Red Hat Enterprise Linux : 8.5、8.4、8.3、8.2、8.1、8.0、7.9、7.8、7.7、および 7.6 - CentOS : 7.9、7.8、7.7、7.6
1.4	- Red Hat Enterprise Linux : 8.5、8.4、8.3、8.2、8.1、8.0、7.9、7.8、7.7、および 7.6 - CentOS : 7.9、7.8、7.7、7.6
1.3	- Red Hat Enterprise Linux : 8.3、8.2、8.1、8.0、7.9、7.8、7.7、および 7.6 - CentOS : 7.9、7.8、7.7、7.6
1.2	- Red Hat Enterprise Linux : 8.1、8.0、7.9、7.8、7.7、および 7.6 - CentOS : 7.9、7.8、7.7、7.6

1. 互換性があるとは、Red Hat がこれらの RHEL バージョンをサポートしなくなったものの、ONTAP Mediator をこれらのバージョンにインストールできることを意味します。

ライセンス

次のSnapMirrorライセンスは ONTAP One ライセンス スイートの一部として使用可能であり、両方のクラスターに適用する必要があります：

- SnapMirror Synchronous
- SnapMirror



ONTAPストレージシステムを2019年6月より前に購入した場合は、"[ONTAPマスター ライセンス キー](#)"を参照して、必要なSnapMirror同期ライセンスを取得してください。

- vSphere Metro Storage Cluster (vMSC) の場合、VMware vSphereライセンスが必要です。

ネットワーク環境

- クラスター間レイテンシのラウンド トリップ タイム (RTT) が10ミリ秒未満である必要があります。
- ONTAP 9.14.1 以降では、"[SCSI-3 永続予約](#)"がSnapMirrorアクティブ同期でサポートされます。

サポートされるプロトコル

SnapMirror Active Sync は SAN プロトコルをサポートします。

- FC および iSCSI プロトコルは、ONTAP 9.9.1 以降でサポートされます。
- NVMe プロトコルは、ONTAP 9.17.1 以降の VMware vSphere ワークロードでサポートされます。

SnapMirror active sync は、NVMe プロトコルでは以下をサポートしません：

- 4ノード対称active/active構成
- 非対称アクティブ / アクティブ構成
- 整合性グループのサイズの変更

NVMeプロトコルをSnapMirrorアクティブ同期で使用している場合、整合性グループを無停止で拡張または縮小することはできません。NVMeプロトコルをSnapMirrorアクティブ同期で使用している場合、整合性グループの拡張および縮小処理には停止が伴います。

- 同じ整合性グループ内の LUN と namespace の共存。

IPspace

デフォルトの IPspace は、クラスタピア関係確立のために SnapMirror アクティブ同期が必要です。カスタム IPspace はサポートされていません。

NTFSセキュリティ形式

NTFSセキュリティ スタイルは、SnapMirrorアクティブ同期ボリュームではサポートされて*いません*。

ONTAP Mediator

- 透過的なアプリケーション フェイルオーバーを実現するには、ONTAP Mediator を外部でプロビジョニングし、ONTAP に接続する必要があります。
- 完全に機能し、計画外の自動フェイルオーバーを有効にするには、外部ONTAP Mediatorをプロビジョニングし、ONTAPクラスタで設定する必要があります。
- ONTAP Mediator は、2 つの ONTAP クラスタとは別の 3 番目の障害ドメインにインストールする必要があります。
- ONTAP Mediator をインストールするときは、自己署名証明書を、主流の信頼できる CA によって署名された有効な証明書に置き換える必要があります。
- ONTAP Mediator の詳細については、["ONTAPメディエーターのインストール準備"](#)を参照してください。

その他の前提条件

- ONTAP 9.15.1より前のリリースでは、読み取り / 書き込みデスティネーション ボリューム（非対称アクティブ / アクティブでDPから読み取り / 書き込みに変換されたボリューム）では、SnapMirrorアクティブ同期関係はサポートされません。読み取り / 書き込みボリュームを使用するには、ボリューム レベルのSnapMirror関係（非同期または同期）を作成してから、その関係を削除することで、DPボリュームに変換する必要があります。詳細については、["既存のSnapMirror関係をSnapMirrorアクティブ同期に変換する"](#)を参照してください。
- SnapMirror アクティブ同期を使用するストレージ VM は、クライアント コンピューターとして Active Directory に参加できません。

- ["Hardware Universe"](#)
- ["ONTAP Mediatorの概要"](#)

ONTAP SnapMirror アクティブ同期の相互運用性

SnapMirrorアクティブ同期は、多数のオペレーティング システム、アプリケーション ホスト、ONTAPのその他の機能と互換性があります。



ここで説明されていない特定のサポート性と相互運用性の詳細については、Interoperability Matrix Tool(["IMT にログインします。"](#))を参照してください。

アプリケーション ホスト

SnapMirror active sync は、Hyper-V、ESXi などのハイパーバイザー、Red Hat Enterprise Linux (RHEL)、Windows Server などのオペレーティング システム、vSphere Metro Storage Cluster (vMSC) などのクラスタリング ソリューション、および ONTAP 9.14.1 以降では Windows Server Failover Cluster をサポートします。

オペレーティング システム

SnapMirrorアクティブ同期は、次のようなさまざまなオペレーティング システムでサポートされています。

- PVRを介したAIX (ONTAP 9.11.1以降)
- HP-UX (ONTAP 9.10.1以降)
- Solaris 11.4 (ONTAP 9.10.1以降)

AIX

ONTAP 9.11.1 以降、AIX は標準エンジニアリング機能ポリシー変動要求 (FPVR) による SnapMirror アクティブ同期でサポートされます。ただし、以下の規定を理解していることが条件となります：

- SnapMirror active syncはゼロRPOのデータ保護を提供できますが、AIXのフェイルオーバープロセスではパスの変更を認識するための追加手順が必要です。ルートボリュームグループに属していないLUNは、`cfgmgr` コマンドが実行されるまでI/Oが一時停止します。これは自動化可能であり、ほとんどのアプリケーションはそれ以上の中断なく動作を再開できます。
- ルートボリュームグループに含まれるLUNは、通常SnapMirror active syncで保護すべきではありません。フェイルオーバー後に `cfgmgr` コマンドを実行することはできないため、SANパスの変更を認識するには再起動が必要です。ルートボリュームグループのゼロRPOデータ保護は実現可能ですが、フェイルオーバーは中断を伴います。

AIXでのSnapMirrorアクティブ同期の詳細については、NetAppアカウント チームにお問い合わせください。

HP-UX

ONTAP 9.10.1 以降では、HP-UX 用の SnapMirror active sync がサポートされます。

HP-UXでの自動計画外フェイルオーバー

分離されたマスタークラスタにおける自動計画外フェイルオーバー (AUFO) イベントは、プライマリクラス

タとセカンダリクラスタ間の接続が失われ、プライマリクラスタとメディアエーター間の接続も失われるという二重イベント障害によって発生する可能性があります。これは、他のAUFOイベントとは異なり、まれなイベントと考えられます。

- このような場合、HP-UXホストでI/Oが再開されるまでに120秒以上かかることがあります。実行中のアプリケーションによっては、I/Oが中断しない場合や、エラーメッセージが表示されない場合があります。
- 問題を修正するには、許容される中断時間が120秒未満のHP-UXホストでアプリケーションを再起動する必要があります。

Solaris

ONTAP 9.10.1以降では、SnapMirrorアクティブ同期でSolaris 11.4がサポートされます。

SnapMirror Active Sync環境で計画外のサイトフェイルオーバースイッチオーバーが発生した場合でも、Solarisクライアントアプリケーションが中断されないよう、Solaris OSのデフォルト設定を変更してください。推奨設定でSolarisを構成するには、["NetAppナレッジベース：Solaris ホストサポートのSnapMirror active syncの推奨設定"](#)を参照してください。

ONTAPの相互運用性

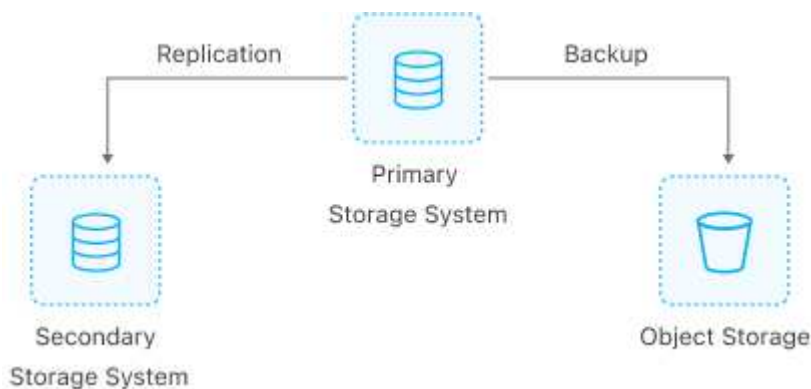
SnapMirrorアクティブ同期は、ONTAPのコンポーネントと統合されて、データ保護機能を拡張します。

FabricPool

SnapMirrorアクティブ同期では、階層化ポリシーが「None」、「Snapshot」、「Auto」のいずれかに設定されたFabricPoolアグリゲート内のボリュームがソースとデスティネーションとしてサポートされます。「All」階層化ポリシーを使用するFabricPoolアグリゲートはサポートされません。

ファンアウト構成

[ファンアウト構成](#)では、ソース ボリュームをSnapMirrorアクティブ同期の宛先エンドポイントと1つのSnapMirror非同期関係にミラーリングできます。



SnapMirror active syncは[ファンアウト構成](#)と`MirrorAllSnapshots`ポリシーをサポートし、ONTAP 9.11.1以降では`MirrorAndVault`ポリシーをサポートします。ファンアウト構成は、`XDPDefault`ポリシーを使用するSnapMirror active syncではサポートされていません。

ONTAP 9.15.1以降、SnapMirror active syncは、フェイルオーバーイベント後のファンアウトレグにおける自動再構成をサポートします。プライマリサイトからセカンダリサイトへのフェイルオーバーが成功すると、セカンダリサイトをソースとして扱うように、第3サイトが自動的に再構成されます。非同期ファンアウトレグは、コンシステンシグループ関係または独立ボリューム関係のいずれかです。再構成はどちらの場合でも

機能します。再構成は、計画的フェイルオーバーまたは計画外フェイルオーバーによってトリガーされます。また、プライマリサイトへのフェイルバック時にも再構成が実行されます。

以前のリリースのONTAPでファンアウト構成を管理する方法については、[ファンアウト構成で保護を再開する](#)を参照してください。

NDMPのリストア

ONTAP 9.13.1以降では、[NDMPによるデータのコピーとリストア](#)をSnapMirror active syncで使用できます。NDMPを使用すると、データをSnapMirror active syncソースに移動して、保護を一時停止することなくリストアを完了できます。これはファンアウト構成で特に便利です。

SnapCenter

SnapMirror active syncは、["SnapCenter 5.0"](#)以降のSnapCenterでサポートされています。SnapCenterでは、アプリケーションと仮想マシンの保護とリカバリに使用できるSnapshotを作成でき、アプリケーションレベルの精度で常時使用可能なストレージソリューションを実現します。

SnapRestore

SnapMirrorアクティブ同期では、Partial File SnapRestoreとSingle File SnapRestoreがサポートされます。

Single File SnapRestore

ONTAP 9.11.1以降、[単一ファイルSnapRestore](#)はSnapMirror Active Syncボリュームでサポートされます。SnapMirror Active Syncソースからデスティネーションにレプリケートされたスナップショットから、単一のファイルをリストアできます。ボリュームには1つ以上のLUNを含めることができるため、この機能により、他のLUNに影響を与えることなく単一のLUNをきめ細かくリストアすることで、システムの停止を最小限に抑えたリストア操作を実現できます。単一ファイルSnapRestoreには、インプレースとアウトオブプレースの2つのオプションがあります。

Partial File SnapRestore

ONTAP 9.12.1以降、["部分的な LUN の復元"](#)はSnapMirror Active Syncボリュームでサポートされます。SnapMirror Active Syncのソース（ボリューム）ボリュームとデスティネーション（スナップショット）ボリューム間でレプリケートされた、アプリケーション作成のスナップショットからデータをリストアできます。複数のデータベースを同一LUNに格納しているホスト上のデータベースをリストアする必要がある場合は、LUNまたはファイルの部分リストアが必要になる場合があります。この機能を使用するには、データの開始バイトオフセットとバイト数を知っておく必要があります。

改ざん防止スナップショット

改ざん防止スナップショットはSnapMirrorアクティブ同期ではサポートされていません。

大規模なLUNと大容量ボリューム

大規模なLUNと大容量ボリューム（100TBを超えるボリューム）がサポートされるかどうかは、使用しているONTAPのバージョンとプラットフォームによって決まります。

ONTAP 9.12.1P2以降

- ONTAP 9.12.1P2以降では、ASAおよびAFF（AシリーズとCシリーズ）で大規模なLUNと100TBを超える大容量ボリュームがサポートされます。プライマリ クラスタとセカンダリ クラスタのタイプ（ASAまたはAFF）が同じである必要があります。AFF AシリーズからAFF Cシリーズ（またはその逆）へのレプリケーションがサポートされます。



ONTAPリリース9.12.1P2以降では、プライマリ クラスタとセカンダリ クラスタの両方がオールフラッシュSANアレイ（ASA）またはオールフラッシュ アレイ（AFF）のいずれかで、両方にONTAP 9.12.1P2以降がインストールされていることを確認する必要があります。セカンダリ クラスタでONTAP 9.12.1P2よりも前のバージョンが実行されている場合やアレイ タイプがプライマリ クラスタと異なる場合、プライマリ ボリュームが100TBを超えると同期関係が維持されなくなることがあります。

ONTAP 9.9.1～9.12.1P1

- ONTAP 9.9.1～9.12.1P1のONTAPリリースでは、大規模なLUNと100TBを超える大容量ボリュームが、オールフラッシュSANアレイでのみサポートされます。AFF AシリーズからAFF Cシリーズ（またはその逆）へのレプリケーションがサポートされます。



ONTAP 9.9.1～9.12.1P2のONTAPリリースでは、プライマリ クラスタとセカンダリ クラスタの両方がオールフラッシュSANアレイで、両方にONTAP 9.9.1以降がインストールされていることを確認する必要があります。セカンダリ クラスタでONTAP 9.9.1よりも前のバージョンが実行されている場合やオールフラッシュSANアレイでない場合、プライマリ ボリュームが100TBを超えると同期関係を維持できなくなります。

詳細情報

- ["AIXホストをSnapMirrorアクティブ同期用に設定する方法"](#)

ONTAP SnapMirror Active Syncのオブジェクト制限

SnapMirrorアクティブ同期を使用する際は、以下のオブジェクト数の制限に注意してください。

クラスタ内の整合性グループ数

SnapMirrorアクティブ同期を使用するクラスタに対する整合性グループ数の制限は、関係に基づいて計算され、使用するONTAPのバージョンによって異なります。制限はプラットフォームには依存しません。

ONTAPのバージョン	関係の最大数
ONTAP 9.11.1以降	50*
ONTAP 9.10.1	20
ONTAP 9.9.1	5

*ONTAP 9.16.1以降、SnapMirror Active Syncは対称アクティブ / アクティブ構成の4ノードクラスタをサポートします。4ノードクラスタでは、100個のコンシステンシグループがサポートされます。

整合性グループあたりのボリューム数

SnapMirrorアクティブ同期を使用する整合性グループあたりの最大ボリューム数は、プラットフォームに依存しません。

ONTAPのバージョン	整合性グループ関係でサポートされる最大ボリューム数
ONTAP 9.15.1以降	80
ONTAP 9.10.1～9.14.1	16
ONTAP 9.9.1	12

ボリューム

SnapMirrorアクティブ同期でのボリューム数の制限は、関係の数ではなくエンドポイントの数に基づいて計算されます。12個のボリュームを含む整合性グループの場合、エンドポイントはプライマリ クラスタとセカンダリ クラスタの両方に12個です。SnapMirrorアクティブ同期関係とSnapMirror同期関係の両方がエンドポイントの総数に影響します。



これらの制限は FAS、AFF、および ASA システムに適用されます。ASA r2 システム（ASA A1K、ASAA90、ASAA70、ASAA50、ASAA30、またはASAA20）をご利用の場合は、"[ASA r2 ドキュメント](#)"を参照してください。

プラットフォームあたりの最大エンドポイント数を次の表に示します。

プラットフォーム	SnapMirror アクティブ同期の HA あたりのエンドポイント数			HA あたりの全体的な同期エンドポイントと SnapMirror アクティブ同期エンドポイント		
	ONTAP 9.11.1 以降	ONTAP 9.10.1	ONTAP 9.9.1	ONTAP 9.11.1 以降	ONTAP 9.10.1	ONTAP 9.9.1
AFF	400*	200	60	400	200	80
ASA	400*	200	60	400	200	80

*ONTAP 9.16.1以降、SnapMirror active syncは対称型アクティブ / アクティブ構成の4ノードクラスタをサポートします。4ノードクラスタの合計エンドポイント数の上限は800です。

SANオブジェクト数

SANオブジェクト数の制限を次の表に示します。ここに挙げた制限は、プラットフォームに関係なく適用されます。

SnapMirror アクティブ同期関係内のオブジェクト	数
ボリュームあたりのLUN数	256（ONTAP 9.9.1 - ONTAP 9.15.0） 512（ONTAP 9.15.1以降）
2 x 2 SnapMirrorアクティブ同期ソリューションあたりの一意の LUN、名前空間、またはストレージ ユニットの数	4,096

SnapMirror アクティブ同期関係内のオブジェクト	数
4 x 4 SnapMirror アクティブ同期ソリューションあたりの一意の LUN、ネームスペース、またはストレージユニットの数 (ONTAP 9.16.1 以降で利用可能)	6,144
SVM あたりの LIF 数 (SnapMirror アクティブ同期関係にあるボリュームが少なくとも 1 つある場合)	256
ノードあたりのクラスタ間LIF数	4
クラスタあたりのクラスタ間LIF数	8

NVMe オブジェクトの制限

ONTAP 9.17.1以降、SnapMirror active syncはNVMeプロトコルをサポートします。NVMeオブジェクトの制限については、次の表をご覧ください。

SnapMirrorアクティブ同期関係におけるオブジェクトの最大数	数
ノードあたりのネームスペースマップの数	4K
クラスタサイズ	2 ノード
HAペアあたりの整合性グループの数	50
単一のNVMe SnapMirror active sync整合性グループ内のボリュームの数	80
HAペアのボリューム数	400
整合性グループあたりのNVMeサブシステム	16
整合性グループごとの名前空間マップ	256

関連情報

- ["Hardware Universe"](#)
- ["整合性グループの制限"](#)

設定

SnapMirror アクティブ同期用に ONTAP クラスタを構成する

SnapMirror アクティブ同期は、フェイルオーバー シナリオが発生した場合にデータを保護するために、ピア クラスタを使用します。SnapMirror アクティブ同期用に ONTAP Mediator または ONTAP Cloud Mediator を設定する前に、まずクラスタが正しく設定されていることを確認する必要があります。

開始する前に

ONTAP Mediator または ONTAP Cloud Mediator を設定する前に、次の点を確認する必要があります：

1. クラスタ間にクラスタ ピアリング関係が存在します。



SnapMirror Active Sync では、クラスタ ピア関係にデフォルトの IPspace が必要です。カスタム IPspace はサポートされていません。

"クラスタ ピア関係の作成"

2. SVM は各クラスタ上に作成されます。

"SVMの作成"

3. 各クラスタの SVM 間にはピア関係が存在します。

"SVMピア関係の作成"

4. LUN 用のボリュームが存在します。

"ボリュームの作成"

5. 両方のクラスタの各ノードに、少なくとも 1 つの SAN LIF（該当する場合は FC または iSCSI）が作成されます。

"クラスタSAN環境でのLIFに関する注意事項"

"NVMe LIFの設定"

6. 必要な LUN が作成され、igroup にマップされます。igroup は、LUN をアプリケーション ホスト上のイニシエーターにマップするために使用されます。

"LUNの作成およびigroupへのマッピング"

7. アプリケーション ホストが再スキャンされ、新しい LUN が検出されます。

SnapMirror アクティブ同期用に **ONTAP Mediator** を設定

SnapMirror active syncは、ピアクラスタを使用してフェイルオーバーシナリオ発生時にデータを保護します。ONTAP Mediatorは、各クラスタの健全性を監視することでビジネス継続性を実現する重要なリソースです。SnapMirror active syncを設定するには、まずONTAP Mediatorをインストールし、プライマリクラスタとセカンダリクラスタが適切に設定されていることを確認する必要があります。

ONTAP Mediator をインストールしてクラスタを設定したら、[自己署名証明書を使用してSnapMirrorアクティブ同期用にONTAP Mediatorを初期化します](#)。次に、[SnapMirrorアクティブ同期の整合性グループを作成、初期化、およびマッピングする](#)を実行する必要があります。

ONTAP Mediator

ONTAP Mediatorは、SnapMirrorアクティブ同期関係にあるONTAPクラスタで使用される高可用性（HA）メタデータのための永続的かつフェンスされたストアを提供します。さらに、ONTAP Mediatorは、クォーラムの決定を支援する同期ノードヘルスクエリ機能を提供し、コントローラの稼働状態検出のためのpingプロキシとして機能します。

各クラスタ ピア関係は、1つのONTAP Mediatorインスタンスにのみ関連付けることができます。HA Mediator

インスタンスはサポートされていません。クラスタが他のクラスタと複数のピア関係にある場合、以下のONTAP Mediatorオプションが利用可能です：

- SnapMirror アクティブ同期が各関係で設定されている場合、各クラスタ ピア関係は独自の ONTAP Mediator インスタンスを持つことができます。
- クラスタは、すべてのピア関係に対して同じ ONTAP Mediator インスタンスを使用できます。

たとえば、クラスタBがクラスタA、クラスタC、クラスタDとピア関係を持っている場合、各関係でSnapMirror Active Syncが設定されていれば、3つのクラスタピア関係すべてに固有の関連付けられたONTAP Mediatorインスタンスを持つことができます。または、クラスタBは3つのピア関係すべてに同じONTAP Mediatorインスタンスを使用することもできます。このシナリオでは、同じONTAP Mediatorインスタンスがクラスタに対して3回リストされます。

ONTAP 9.17.1 以降では、["ONTAP Cloud Mediator"](#) を SnapMirror アクティブ同期構成でクラスタの健全性を監視するように設定できますが、両方のメディアエーターを同時に使用することはできません。



ONTAP 9.17.1 で SnapMirror アクティブ同期と ONTAP Mediator または ONTAP Cloud Mediator を使用している場合は、これらの構成に関する重要な情報について ["ONTAP Release Notes"](#) の*既知の問題と制限事項*を確認する必要があります。

ONTAP Mediatorの前提条件

- ONTAP Mediator には独自の前提条件が含まれています。ONTAP Mediator をインストールする前に、これらの前提条件を満たす必要があります。

詳細については、["ONTAP Mediatorサービスのインストールの準備"](#)を参照してください。

- デフォルトでは、ONTAP MediatorはTCPポート31784を介してサービスを提供します。ONTAPクラスタとONTAP Mediatorの間でポート31784が開いていて使用可能であることを確認する必要があります。

ONTAP Mediatorをインストールし、クラスタ構成を確認する

ONTAP Mediatorをインストールし、クラスタ構成を確認するには、以下の各手順を実行します。各手順で、特定の構成が実行されたことを確認する必要があります。各手順には、従う必要がある具体的な手順へのリンクが含まれています。

手順

1. ソース クラスタとデスティネーションクラスタが正しく設定されていることを確認する前に、ONTAP Mediator をインストールします。

ONTAP Mediatorのインストールまたはアップグレードの準備

2. クラスタ間にクラスタ ピア関係が確立されていることを確認します。



SnapMirror Active Sync では、クラスタ ピア関係にデフォルトの IPspace が必要です。カスタム IPspace はサポートされていません。

["SnapMirror アクティブ同期用に ONTAP クラスタを構成する"](#)

自己署名証明書を使用して**SnapMirror**アクティブ同期用に**ONTAP Mediator**を初期化します

ONTAP Mediatorをインストールし、クラスタ構成を確認したら、クラスタ監視のためにONTAP Mediatorを初期化する必要があります。ONTAP Mediatorの初期化は、System ManagerまたはONTAP CLIを使用して行うことができます。

System Manager

System Managerを使用すると、自動フェイルオーバー用にONTAP Mediatorを設定できます。また、まだ行っていない場合は、自己署名SSL証明書とCAをサードパーティの検証済みSSL証明書とCAに置き換えることもできます。

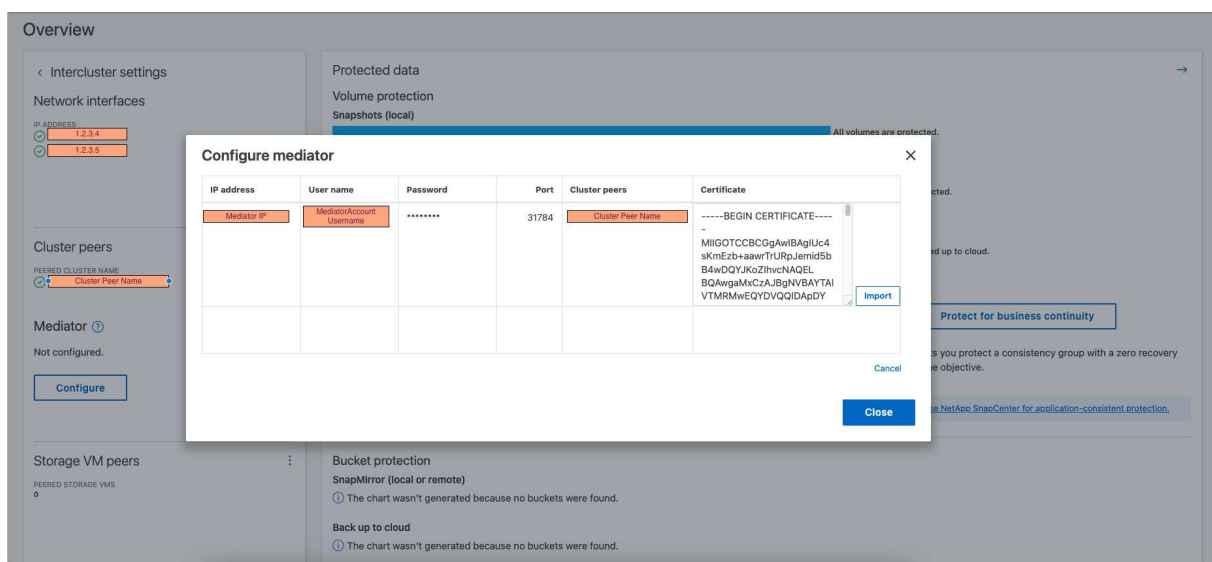


ONTAP 9.14.1から9.8では、SnapMirrorアクティブ同期はSnapMirror Business Continuity (SM-BC) と呼ばれます。

ONTAP Mediator 1.9以降

1. **Protection > Overview > Mediator > Configure** に移動します。
2. [追加] を選択し、次の ONTAP Mediator 情報を入力します：
 - IPv4 アドレス
 - ユーザー名
 - パスワード
 - Certificate
3. [Certificate]への入力、以下の2つの方法で指定できます。
 - オプション (a) : *インポート*を選択して `intermediate.crt` ファイルに移動し、インポートします。
 - オプション (b) : `intermediate.crt` ファイルの内容をコピーし、*証明書*フィールドに貼り付けます。

すべての詳細を正しく入力すると、指定した証明書がすべてのピア クラスタにインストールされます。



証明書の追加が完了すると、ONTAP Mediator が ONTAP クラスタに追加されます。

次の図は、ONTAP Mediatorの設定に成功したことを示しています。

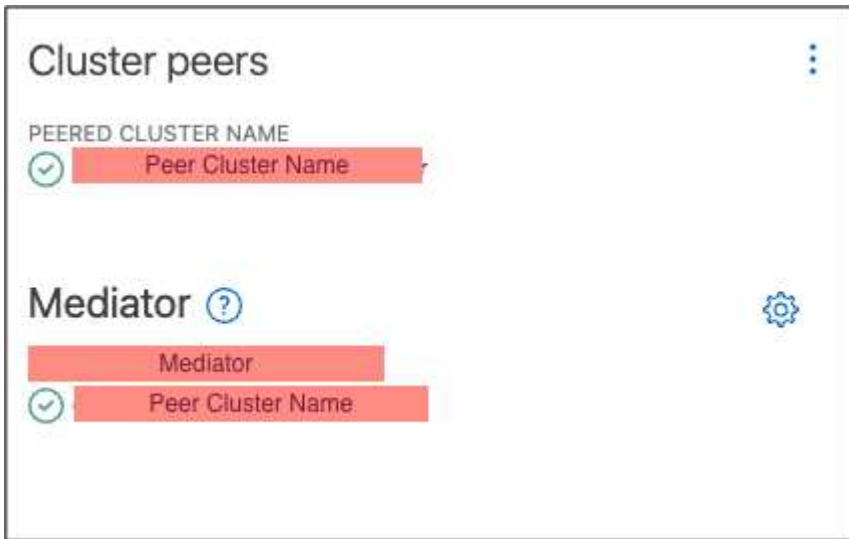
ONTAP Mediator 1.8 以前

1. **Protection > Overview > Mediator > Configure** に移動します。
2. [追加] を選択し、次の ONTAP Mediator 情報を入力します：
 - IPv4 アドレス
 - ユーザー名
 - パスワード
 - Certificate
3. [Certificate]への入力、以下の2つの方法で指定できます。
 - オプション (a)：*インポート*を選択して `ca.crt` ファイルに移動し、インポートします。
 - オプション (b)：`ca.crt` ファイルの内容をコピーし、*証明書*フィールドに貼り付けます。

すべての詳細を正しく入力すると、指定した証明書がすべてのピア クラスタにインストールされます。

証明書の追加が完了すると、ONTAP Mediator が ONTAP クラスタに追加されます。

次の図は、ONTAP Mediatorの設定に成功したことを示しています。



CLI

ONTAP CLIを使用して、プライマリクラスタまたはセカンダリクラスタのどちらからでもONTAP Mediatorを初期化できます。一方のクラスタで `mediator add` コマンドを実行すると、もう一方のクラスタにONTAP Mediatorが自動的に追加されます。

ONTAP Mediatorを使用してSnapMirrorアクティブ同期関係を監視する場合、有効な自己署名証明書または認証局（CA）証明書がないと、ONTAP MediatorをONTAPで初期化できません。ピアクラスタの証明書ストアに有効な証明書を追加します。ONTAP Mediatorを使用してMetroCluster IPシステムを監視する場合、初期設定後はHTTPSは使用されないため、証明書は必要ありません。

ONTAP Mediator 1.9以降

1. ONTAP Mediator Linux VM / ホスト ソフトウェアのインストール場所から ONTAP Mediator CA 証明書を見つけます `cd /opt/netapp/lib/ontap_mediator/ontap_mediator/server_config`。
2. ピア クラスタの証明書ストアに有効な認証局を追加します。

例：

```
[root@ontap-mediator_config]# cat intermediate.crt
-----BEGIN CERTIFICATE-----
<certificate_value>
-----END CERTIFICATE-----
```

3. ONTAP Mediator CA証明書をONTAPクラスタに追加します。プロンプトが表示されたら、ONTAP Mediatorから取得したCA証明書を挿入します。すべてのピアクラスタでこの手順を繰り返します：

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

例：

```
[root@ontap-mediator ~]# cd
/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config

[root@ontap-mediator_config]# cat intermediate.crt
-----BEGIN CERTIFICATE-----
<certificate_value>
-----END CERTIFICATE-----
```

```
C1_test_cluster::*> security certificate install -type server-ca
-vserver C1_test_cluster
```

Please enter Certificate: Press when done

-----BEGIN CERTIFICATE-----

<certificate_value>

-----END CERTIFICATE-----

You should keep a copy of the CA-signed digital certificate for future reference.

The installed certificate's CA and serial number for reference:

CA: ONTAP Mediator CA

serial: D86D8E4E87142XXX

The certificate's generated name for reference: ONTAPMediatorCA

```
C1_test_cluster::*>
```

4. 生成された証明書名を使用して、インストールされている自己署名CA証明書を表示します。

```
security certificate show -common-name <common_name>
```

例：

```
C1_test_cluster::*> security certificate show -common-name
```

```
ONTAPMediatorCA
```

Vserver	Serial Number	Certificate Name

Type

```
C1_test_cluster
```

```
6BFD17DXXXXX7A71BB1F44D0326D2DEEXXXXX
```

```
ONTAPMediatorCA
```

```
server-ca
```

```
Certificate Authority: ONTAP Mediator CA
```

```
Expiration Date: Thu Feb 15 14:35:25 2029
```

5. 一方のクラスタでONTAP Mediatorを初期化します。もう一方のクラスタにはONTAP Mediatorが自動的に追加されます：

```
snapmirror mediator add -mediator-address <ip_address> -peer-cluster
<peer_cluster_name> -username user_name
```

例：

```
C1_test_cluster::*> snapmirror mediator add -mediator-address  
1.2.3.4 -peer-cluster C2_test_cluster -username mediatoradmin  
Notice: Enter the mediator password.
```

```
Enter the password: *****
```

```
Enter the password again: *****
```

6. 必要に応じて、ジョブ ID のステータスをチェックして `job show -id`、SnapMirror Mediator 追加コマンドが成功したかどうかを確認します。

例：

```
C1_test_cluster::*> snapmirror mediator show
```

This table is currently empty.

```
C1_test_cluster::*> snapmirror mediator add -peer-cluster  
C2_test_cluster -type on-prem -mediator-address 1.2.3.4 -username  
mediatoradmin
```

Notice: Enter the mediator password.

Enter the password:

Enter the password again:

Info: [Job: 87] 'mediator add' job queued

```
C1_test_cluster::*> job show -id 87
```

Job	ID	Name	Owning Vserver	Node	State
87		mediator add	C1_test_cluster	C2_test	Running

Description: Creating a mediator entry

```
C1_test_cluster::*> job show -id 87
```

Job	ID	Name	Owning Vserver	Node	State
87		mediator add	C1_test_cluster	C2_test	Success

Description: Creating a mediator entry

```
C1_test_cluster::*> snapmirror mediator show
```

Mediator Type	Address	Peer Cluster	Connection Status	Quorum Status
on-prem	1.2.3.4	C2_test_cluster	connected	true

```
C1_test_cluster::*>
```

7. ONTAP Mediator設定のステータスを確認します。

```
snapmirror mediator show
```

Mediator Address	Peer Cluster	Connection Status	Quorum Status
1.2.3.4	C2_test_cluster	connected	true

`Quorum Status`は、SnapMirrorコンシステンシーグループの関係がONTAP Mediatorと同期されているかどうかを示します。`true`のステータスは、同期が正常に行われたことを示します。

ONTAP Mediator 1.8 以前

1. ONTAP Mediator Linux VM / ホスト ソフトウェアのインストール場所から ONTAP Mediator CA 証明書を見つけます `cd /opt/netapp/lib/ontap_mediator/ontap_mediator/server_config`
2. ピア クラスタの証明書ストアに有効な認証局を追加します。

例：

```
[root@ontap-mediator_config]# cat ca.crt
-----BEGIN CERTIFICATE-----
<certificate_value>
-----END CERTIFICATE-----
```

3. ONTAP MediatorのCA証明書をONTAPクラスタに追加します。プロンプトが表示されたら、ONTAP Mediatorから取得したCA証明書を挿入します。すべてのピア クラスタで同じ手順を繰り返します。

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

例：

```
[root@ontap-mediator ~]# cd
/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config

[root@ontap-mediator_config]# cat ca.crt
-----BEGIN CERTIFICATE-----
<certificate_value>
-----END CERTIFICATE-----
```

```
C1_test_cluster::*> security certificate install -type server-ca
-vserver C1_test_cluster
```

Please enter Certificate: Press when done

-----BEGIN CERTIFICATE-----

<certificate_value>

-----END CERTIFICATE-----

You should keep a copy of the CA-signed digital certificate for future reference.

The installed certificate's CA and serial number for reference:

CA: ONTAP Mediator CA

serial: D86D8E4E87142XXX

The certificate's generated name for reference: ONTAPMediatorCA

```
C1_test_cluster::*>
```

4. 生成された証明書名を使用して、インストールされている自己署名CA証明書を表示します。

```
security certificate show -common-name <common_name>
```

例：

```
C1_test_cluster::*> security certificate show -common-name
```

```
ONTAPMediatorCA
```

Vserver	Serial Number	Certificate Name

Type

```
C1_test_cluster
```

```
6BFD17DXXXXX7A71BB1F44D0326D2DEEXXXXX
```

```
ONTAPMediatorCA
```

```
server-ca
```

```
Certificate Authority: ONTAP Mediator CA
```

```
Expiration Date: Thu Feb 15 14:35:25 2029
```

5. 一方のクラスタでONTAP Mediatorを初期化します。もう一方のクラスタにはONTAP Mediatorが自動的に追加されます：

```
snapmirror mediator add -mediator-address <ip_address> -peer-cluster
<peer_cluster_name> -username user_name
```

例：

```
C1_test_cluster::*> snapmirror mediator add -mediator-address  
1.2.3.4 -peer-cluster C2_test_cluster -username mediatoradmin  
Notice: Enter the mediator password.
```

```
Enter the password: *****
```

```
Enter the password again: *****
```

6. 必要に応じて、ジョブ ID のステータスをチェックして `job show -id`、SnapMirror Mediator 追加コマンドが成功したかどうかを確認します。

例：


```
C1_test_cluster::*> snapmirror mediator show
This table is currently empty.
```

```
C1_test_cluster::*> snapmirror mediator add -peer-cluster
C2_test_cluster -type on-prem -mediator-address 1.2.3.4 -username
mediatoradmin
```

Notice: Enter the mediator password.

Enter the password:

Enter the password again:

Info: [Job: 87] 'mediator add' job queued

```
C1_test_cluster::*> job show -id 87
```

Job	ID	Name	Owning Vserver	Node	State
87		mediator add	C1_test_cluster	C2_test	Running

Description: Creating a mediator entry

```
C1_test_cluster::*> job show -id 87
```

Job	ID	Name	Owning Vserver	Node	State
87		mediator add	C1_test_cluster	C2_test	Success

Description: Creating a mediator entry

```
C1_test_cluster::*> snapmirror mediator show
```

Mediator Type	Address	Peer Cluster	Connection Status	Quorum Status
on-prem	1.2.3.4	C2_test_cluster	connected	true

```
C1_test_cluster::*>
```

7. ONTAP Mediator設定のステータスを確認します。

```
snapmirror mediator show
```

Mediator Address	Peer Cluster	Connection Status	Quorum Status
1.2.3.4	C2_test_cluster	connected	true

`Quorum Status` SnapMirror 整合性グループの関係が ONTAP Mediator と同期されているかどうかを示します。ステータスが `true` の場合は、同期が成功したことを示します。

サードパーティの証明書を使用した **ONTAP Mediator** の再初期化

ONTAP Mediator の再初期化が必要になる場合があります。ONTAP Mediator の IP アドレスの変更、証明書の有効期限切れなど、ONTAP Mediator の再初期化が必要になる状況が発生する場合があります。

以下の手順は、自己署名証明書をサードパーティの証明書に置き換える必要がある場合に、ONTAP Mediator を再初期化する方法を示しています。

タスク概要

SnapMirror アクティブ同期クラスタの自己署名証明書をサードパーティの証明書に置き換え、ONTAP から ONTAP Mediator 設定を削除してから、ONTAP Mediator を追加する必要があります。

System Manager

System Manager では、古い自己署名証明書で設定された ONTAP Mediator バージョンを ONTAP クラスタから削除し、新しいサードパーティ証明書で ONTAP クラスタを再設定する必要があります。

手順

1. メニュー オプション アイコンを選択し、[削除] を選択して ONTAP Mediator を削除します。



この手順では、ONTAP クラスタから自己署名された server-ca は削除されません。NetApp では、次の手順を実行してサードパーティの証明書を追加する前に、証明書 タブに移動して手動で削除することをお勧めします：

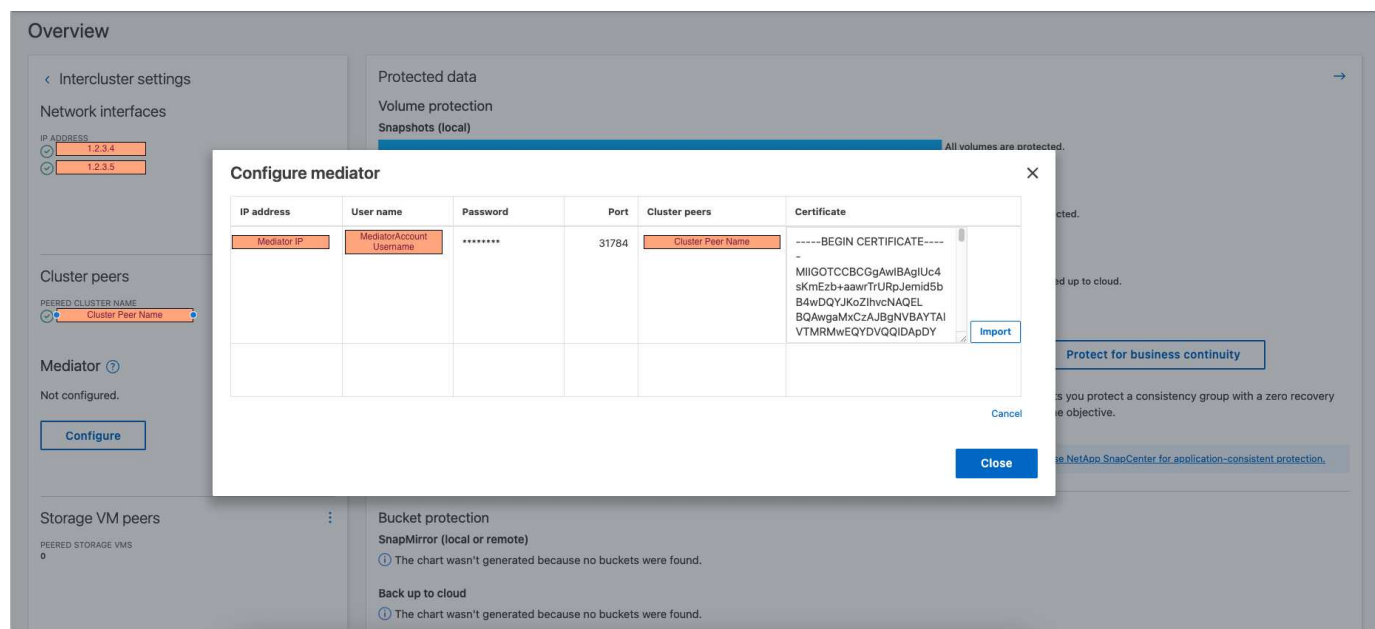
Configure mediator

IP address	User name	Password	Port	Cluster peers	Certificate
Mediator IP			31784	Peer Cluster Name	
Remove					
+ Add					

Close

2. 正しい証明書を使用して ONTAP Mediator を再度追加します。

ONTAP Mediator に新しいサードパーティの自己署名証明書が設定されました。



CLI

ONTAP CLI を使用して自己署名証明書をサードパーティの証明書に置き換えることにより、プライマリ クラスタまたはセカンダリ クラスタから ONTAP Mediator を再初期化できます。

ONTAP Mediator 1.9以降

1. すべてのクラスタで自己署名証明書を使用した際にインストールした自己署名 `intermediate.crt` を削除します。以下の例では、2つのクラスタがあります：

例：

```
C1_test_cluster::*> security certificate delete -vserver
C1_test_cluster -common-name ONTAPMediatorCA
2 entries were deleted.

C2_test_cluster::*> security certificate delete -vserver
C2_test_cluster -common-name ONTAPMediatorCA *
2 entries were deleted.
```

2. `force true` を使用して、以前に設定したONTAP MediatorをSnapMirror Active Syncクラスタから削除します：

例：

```
C1_test_cluster::*> snapmirror mediator show
Mediator Address Peer Cluster      Connection Status Quorum Status
-----
1.2.3.4          C2_test_cluster  connected          true

C1_test_cluster::*> snapmirror mediator remove -mediator-address
1.2.3.4 -peer-cluster C2_test_cluster -force true

Warning: You are trying to remove the ONTAP Mediator configuration
with force. If this configuration exists on the peer cluster, it
could lead to failure of a SnapMirror failover operation. Check if
this configuration
           exists on the peer cluster C2_test_cluster and remove it as
well.
Do you want to continue? {y|n}: y

Info: [Job 136] 'mediator remove' job queued

C1_test_cluster::*> snapmirror mediator show
This table is currently empty.
```

3. 下位CA（`intermediate.crt` と呼ばれる）から証明書を取得する方法については、["信頼できるサードパーティの証明書への自己署名証明書の置き換え"](#)に記載されている手順を参照してください。自己署名証明書を信頼できるサードパーティの証明書に置き換えます



`intermediate.crt`には、PKI機関に送信する必要のあるリクエストから派生した特定のプロパティがあり、ファイル
`/opt/netapp/lib/ontap\_mediator/ontap\_mediator/server\_config/openssl\_ca.cnf`で定義されています。

4. ONTAP Mediator Linux VM / ホスト ソフトウェアのインストール場所から、新しいサードパーティの ONTAP Mediator CA 証明書 `intermediate.crt` を追加します：

例：

```
[root@ontap-mediator ~]# cd
/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config
[root@ontap-mediator_config]# cat intermediate.crt
-----BEGIN CERTIFICATE-----
<certificate_value>
-----END CERTIFICATE-----
```

5. `intermediate.crt` ファイルをピアクラスタに追加します。すべてのピアクラスタに対してこの手順を繰り返します：

例：

```
C1_test_cluster::*> security certificate install -type server-ca
-vserver C1_test_cluster

Please enter Certificate: Press when done
-----BEGIN CERTIFICATE-----
<certificate_value>
-----END CERTIFICATE-----

You should keep a copy of the CA-signed digital certificate for
future reference.

The installed certificate's CA and serial number for reference:
CA: ONTAP Mediator CA
serial: D86D8E4E87142XXX

The certificate's generated name for reference: ONTAPMediatorCA

C1_test_cluster::*>
```

6. 以前に設定したONTAP MediatorをSnapMirrorアクティブ同期クラスタから削除します。

例：

```
C1_test_cluster::*> snapmirror mediator show
Mediator Address Peer Cluster      Connection Status Quorum Status
-----
1.2.3.4          C2_test_cluster  connected          true

C1_test_cluster::*> snapmirror mediator remove -mediator-address
1.2.3.4 -peer-cluster C2_test_cluster

Info: [Job 86] 'mediator remove' job queued
C1_test_cluster::*> snapmirror mediator show
This table is currently empty.
```

7. ONTAP Mediator を再度追加します：

例：

```
C1_test_cluster::*> snapmirror mediator add -mediator-address
1.2.3.4 -peer-cluster C2_test_cluster -username mediatoradmin

Notice: Enter the mediator password.

Enter the password:
Enter the password again:

Info: [Job: 87] 'mediator add' job queued

C1_test_cluster::*> snapmirror mediator show
Mediator Address Peer Cluster      Connection Status Quorum Status
-----
1.2.3.4          C2_test_cluster  connected          true
```

`Quorum Status` SnapMirror 整合性グループの関係がメディエータと同期されているかどうかを示します。`true`のステータスは同期が成功したことを示します。

ONTAP Mediator 1.8 以前

1. すべてのクラスターで自己署名証明書を使用した際にインストールした自己署名 `ca.crt` を削除します。以下の例では、2つのクラスターがあります：

例：

```
C1_test_cluster::*> security certificate delete -vserver
C1_test_cluster -common-name ONTAPMediatorCA
2 entries were deleted.
```

```
C2_test_cluster::*> security certificate delete -vserver
C2_test_cluster -common-name ONTAPMediatorCA *
2 entries were deleted.
```

2. `-force true`を使用して、以前に設定したONTAP MediatorをSnapMirror Active Syncクラスタから削除します：

例：

```
C1_test_cluster::*> snapmirror mediator show
Mediator Address Peer Cluster      Connection Status Quorum Status
-----
1.2.3.4          C2_test_cluster  connected          true
```

```
C1_test_cluster::*> snapmirror mediator remove -mediator-address
1.2.3.4 -peer-cluster C2_test_cluster -force true
```

Warning: You are trying to remove the ONTAP Mediator configuration with force. If this configuration exists on the peer cluster, it could lead to failure of a SnapMirror failover operation. Check if this configuration

exists on the peer cluster C2_test_cluster and remove it as well.

Do you want to continue? {y|n}: y

Info: [Job 136] 'mediator remove' job queued

```
C1_test_cluster::*> snapmirror mediator show
This table is currently empty.
```

3. 下位CA（``ca.crt``と呼ばれる）から証明書を取得する方法については、["信頼できるサードパーティの証明書への自己署名証明書の置き換え"](#)に記載されている手順を参照してください。自己署名証明書を信頼できるサードパーティの証明書に置き換えます



``ca.crt``には、PKI機関に送信する必要のあるリクエストから派生した特定のプロパティがあり、ファイル ``/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/openssl_ca.cnf`` で定義されています。

4. ONTAP Mediator Linux VM / ホスト ソフトウェアのインストール場所から、新しいサードパーティのONTAP Mediator CA 証明書 ``ca.crt``を追加します：

例：

```
[root@ontap-mediator ~]# cd
/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config
[root@ontap-mediator_config]# cat ca.crt
-----BEGIN CERTIFICATE-----
<certificate_value>
-----END CERTIFICATE-----
```

5. `intermediate.crt` ファイルをピアクラスタに追加します。すべてのピアクラスタに対してこの手順を繰り返します：

例：

```
C1_test_cluster::*> security certificate install -type server-ca
-vserver C1_test_cluster

Please enter Certificate: Press when done
-----BEGIN CERTIFICATE-----
<certificate_value>
-----END CERTIFICATE-----

You should keep a copy of the CA-signed digital certificate for
future reference.

The installed certificate's CA and serial number for reference:
CA: ONTAP Mediator CA
serial: D86D8E4E87142XXX

The certificate's generated name for reference: ONTAPMediatorCA

C1_test_cluster::*>
```

6. 以前に設定したONTAP MediatorをSnapMirrorアクティブ同期クラスタから削除します。

例：


```
C1_test_cluster::*> snapmirror mediator show
Mediator Address Peer Cluster      Connection Status Quorum Status
-----
1.2.3.4          C2_test_cluster  connected          true

C1_test_cluster::*> snapmirror mediator remove -mediator-address
1.2.3.4 -peer-cluster C2_test_cluster

Info: [Job 86] 'mediator remove' job queued
C1_test_cluster::*> snapmirror mediator show
This table is currently empty.
```

7. ONTAP Mediator を再度追加します：

例：

```
C1_test_cluster::*> snapmirror mediator add -mediator-address
1.2.3.4 -peer-cluster C2_test_cluster -username mediatoradmin

Notice: Enter the mediator password.

Enter the password:
Enter the password again:

Info: [Job: 87] 'mediator add' job queued

C1_test_cluster::*> snapmirror mediator show
Mediator Address Peer Cluster      Connection Status Quorum Status
-----
1.2.3.4          C2_test_cluster  connected          true
```

`Quorum Status` SnapMirror 整合性グループの関係がメディエータと同期されているかどうかを示します。`true`のステータスは同期が成功したことを示します。

関連情報

- ["job show"](#)
- ["security certificate delete"](#)
- ["security certificate install"](#)
- ["セキュリティ証明書の表示"](#)
- ["SnapMirror Mediator add"](#)
- ["SnapMirror Mediator の削除"](#)
- ["SnapMirror Mediator show"](#)

ONTAP Cloud Mediatorの設定準備

"ONTAP Cloud Mediatorを設定する"する前に、前提条件が満たされていることを確認する必要があります。

ファイアウォールの要件

ドメイン コントローラのファイアウォール設定では、両方のクラスタからの HTTPS トラフィックを `api.bluexp.netapp.com` 許可する必要があります。

プロキシ サーバの要件

SnapMirror アクティブ同期にプロキシ サーバを使用する場合は、プロキシ サーバが作成されており、次のプロキシ サーバ情報があることを確認してください：

- HTTPS プロキシ IP
- ポート
- ユーザー名
- パスワード

レイテンシ

NetApp Console クラウド サーバと SnapMirror アクティブ同期クラスタ ピア間で推奨される ping レイテンシは 200 ミリ秒未満です。

ルート CA 証明書

クラスタの証明書を確認する

ONTAPには既知のルートCA証明書がプリインストールされているため、ほとんどの場合NetApp Consoleサーバのルート CA 証明書をインストールする必要はありません。ONTAP Cloud Mediatorの設定を開始する前に、クラスタをチェックして証明書が存在することを確認できます：

例：

```
C1_cluster% openssl s_client -showcerts -connect
api.bluexp.netapp.com:443 | egrep "s:|i:"
depth=2 C = US, O = DigiCert Inc, OU = www.digicert.com, CN = DigiCert
Global Root G2
verify return:1
depth=1 C = US, O = Microsoft Corporation, CN = Microsoft Azure RSA TLS
Issuing CA 04
verify return:1
depth=0 C = US, ST = WA, L = Redmond, O = Microsoft Corporation, CN =
*.azureedge.net
verify return:1
  0 s:/C=US/ST=WA/L=Redmond/O=Microsoft Corporation/CN=*.azureedge.net
    i:/C=US/O=Microsoft Corporation/CN=Microsoft Azure RSA TLS Issuing CA
04
```

```
1 s:/C=US/O=Microsoft Corporation/CN=Microsoft Azure RSA TLS Issuing CA
04
i:/C=US/O=DigiCert Inc/OU=www.digicert.com/CN=DigiCert Global Root G2
2 s:/C=US/O=DigiCert Inc/OU=www.digicert.com/CN=DigiCert Global Root G2
i:/C=US/O=DigiCert Inc/OU=www.digicert.com/CN=DigiCert Global Root G2
<=====
```

```
C1_cluster::> security certificate show -common-name DigiCert*
```

Vserver	Serial Number	Certificate Name	Type
-----	-----	-----	-----

```
C1_cluster 0CE7E0EXXXXX46FE8FE560FC1BFXXXXX DigiCertAssuredIDRootCA
server-ca
```

```
    Certificate Authority: DigiCert Assured ID Root CA
```

```
        Expiration Date: Mon Nov 10 05:30:00 2031
```

```
C1_cluster 0B931C3XXXXX67EA6723BFC3AF9XXXXX DigiCertAssuredIDRootG2
server-ca
```

```
    Certificate Authority: DigiCert Assured ID Root G2
```

```
        Expiration Date: Fri Jan 15 17:30:00 2038
```

```
C1_cluster 0BA15AFXXXXXA0B54944AFCD24AXXXXXX DigiCertAssuredIDRootG3
server-ca
```

```
    Certificate Authority: DigiCert Assured ID Root G3
```

```
        Expiration Date: Fri Jan 15 17:30:00 2038
```

```
C1_cluster 083BE05XXXXX46B1A1756AC9599XXXXX DigiCertGlobalRootCA server-ca
```

```
    Certificate Authority: DigiCert Global Root CA
```

```
        Expiration Date: Mon Nov 10 05:30:00 2031
```

```
C1_cluster 033AF1EXXXXXA9A0BB2864B11D0XXXXX DigiCertGlobalRootG2 server-ca
```

```
    Certificate Authority: DigiCert Global Root G2
```

```
        Expiration Date: Fri Jan 15 17:30:00 2038
```

```
C1_cluster 055556BXXXXXA43535C3A40FD5AXXXXXX DigiCertGlobalRootG3 server-ca
```

```
    Certificate Authority: DigiCert Global Root G3
```

```
        Expiration Date: Fri Jan 15 17:30:00 2038
```

```
C1_cluster 02AC5C2XXXXX409B8F0B79F2AE4XXXXX DigiCertHighAssuranceEVRootCA
server-ca
```

```
    Certificate Authority: DigiCert High Assurance EV Root CA
```

```
        Expiration Date: Mon Nov 10 05:30:00 2031
```

```
C1_cluster 059B1B5XXXXX2132E23907BDA77XXXXX DigiCertTrustedRootG4 server-
ca
```

```
    Certificate Authority: DigiCert Trusted Root G4
```

プロキシ サーバにインストールされている証明書を確認する

NetApp Console でプロキシを使用して ONTAP Cloud Mediator サービスに接続している場合は、プロキシ サーバのルート CA 証明書が ONTAP にインストールされていることを確認します：

例：

```
C1_cluster% openssl s_client -showcerts -proxy <ip:port> -connect
api.blueexp.netapp.com:443 |egrep "s:|i:"
```

CA 証明書をダウンロードします：

必要に応じて、認証局の Web サイトからルート CA 証明書をダウンロードし、クラスタにインストールできます。

例：

```
C1_cluster::> security certificate install -type server-ca -vserver
C1_cluster

C2_cluster::> security certificate install -type server-ca -vserver
C2_cluster
```

SnapMirror アクティブ同期用に ONTAP Cloud Mediator を設定する

ONTAP 9.17.1以降では、ONTAP Cloud Mediatorを使用して各クラスタの健全性を監視することで、ビジネス継続性を実現できます。ONTAP Cloud Mediatorはクラウドベースのサービスです。ONTAP Cloud MediatorをSnapMirror Active Syncと併用する場合は、まずNetApp Consoleサービスとクライアント情報が設定されていることを確認し、クラスタピアリングが適切に行われていることを確認する必要があります。

ONTAP Mediatorと同様に、ONTAP Cloud Mediatorは、SnapMirrorアクティブ同期関係にあるONTAPクラスタで使用される高可用性（HA）メタデータ用の永続的かつフェンスされたストアを提供します。ONTAP Cloud Mediatorは、クォーラム判定を支援する同期ノードヘルスクエリ機能を提供し、コントローラの稼働状態検出のためのpingプロキシとして機能します。



ONTAP 9.17.1 で SnapMirror アクティブ同期と ONTAP Mediator または ONTAP Cloud Mediator を使用している場合は、これらの構成に関する重要な情報について "[ONTAP Release Notes](#)" の*既知の問題と制限事項*を確認する必要があります。

開始する前に

ONTAP Cloud Mediator を設定する前に、次の情報を確認する必要があります：

- クラスタが設定されました。

"SnapMirror アクティブ同期用に ONTAP クラスタを構成する"

- NetApp Console から NetApp Console 組織 ID をコピーし、ONTAP Cloud Mediator の設定時に使用する Console メンバー サービス アカウントを作成しました。サービス アカウントを作成する際は、組織を ONTAP Cloud Mediator を設定したサブスクリプションに設定する必要があります。カテゴリは **Application**、ロール タイプは **ONTAP Mediator Setup Role** に設定する必要があります。ロールを作成する際に、クライアント ID とクライアント シークレットを保存する必要があります。

"NetApp Console メンバーとサービス アカウントを追加する"

手順

System Manager または ONTAP CLI を使用して ONTAP Cloud Mediator を追加できます。

System Manager

1. 保護 > 概要 > メディエーター に移動し、追加 を選択します。
2. メディエーターの追加 ウィンドウで、メディエーターの種類として クラウド を選択し、次の情報を入力します：
 - NetApp Console組織ID
 - NetApp Console クライアント ID
 - NetApp Console クライアント シークレット
3. クラスター ピアを選択します。
4. HTTP プロキシを使用しており、まだ設定されていない場合は、ローカル ホストとリモート ホストの HTTP プロキシ情報を入力します。

クラスター ピアごとに異なるプロキシ サーバを使用することをお勧めします。

5. オプション：ONTAP にルート CA 証明書をインストールする必要がある場合（特にプロキシ サーバを使用している場合）、指定されたテキスト ボックスに証明書を貼り付けます。
6. *追加*を選択します。
7. [保護] > [概要] に移動し、SnapMirror アクティブ同期クラスターと ONTAP Cloud Mediator 間の関係のステータスを確認します。

CLI

1. ONTAP Cloud Mediator を構成します：

```
snapmirror mediator add -peer-cluster <peerClusterName> -type cloud -bluexp  
-org-id <NetApp Console Organization ID> -service-account-client-id  
<Service Account Client ID> -use-http-proxy-local <true|false> -use-http  
-proxy-remote <true|false>
```
2. ONTAP Cloud Mediator のステータスを確認します：

```
snapmirror mediator show
```

例：

```
C1_cluster::> snapmirror mediator show
Mediator Address Peer Cluster      Connection Status Quorum Status
Type
-----
0.0.0.0          C2_cluster      connected      true
cloud
```

ONTAP SnapMirror Active Syncで保護

SnapMirrorアクティブ同期は、非対称保護のほか、ONTAP 9.15.1以降では対称アクティブ / アクティブ保護も提供します。

非対称保護の設定

SnapMirrorアクティブ同期を使用した非対称保護を設定するには、ONTAPソース クラスタでLUNを選択し、整合性グループに追加します。

開始する前に

- SnapMirror Synchronousライセンスが必要です。
- クラスタ管理者またはStorage VM管理者である必要があります。
- 整合性グループ内のコンスティチュエント ボリュームは、すべて1つのStorage VM (SVM) に含まれている必要があります。
 - LUNが属するボリュームは同じである必要はありません。
- ソースとデスティネーションのクラスタを同じにすることはできません。
- ASAクラスタと非ASAクラスタの間にSnapMirrorアクティブ同期整合性グループ関係を確立することはできません。
- SnapMirrorアクティブ同期でクラスタ ピア関係を確立するには、デフォルトのIPspaceが必要です。カスタムのIPspaceはサポートされていません。
- 整合性グループの名前は一意である必要があります。
- セカンダリ（デスティネーション）クラスタ上のボリュームのタイプはDPでなければなりません。
- プライマリSVMとセカンダリSVMのピア関係が確立されている必要があります。

手順

ONTAP CLIまたはSystem Managerを使用して整合性グループを設定できます。

ONTAP 9.10.1以降、ONTAPはSystem Managerにコンシステンシグループのエンドポイントとメニューを提供し、追加の管理ユーティリティを提供しています。ONTAP 9.10.1以降を使用している場合は、"[整合性グループを設定する](#)"を参照してから"[保護を設定する](#)"を参照してSnapMirrorアクティブ同期関係を作成してください。



ONTAP 9.14.1から9.8では、SnapMirrorアクティブ同期はSnapMirror Business Continuity (SM-BC) と呼ばれます。

System Manager

1. プライマリ クラスタで、[保護] > [概要] > [ビジネス継続性の保護] > [LUNの保護] に移動します。
2. 保護するLUNを選択し、保護グループに追加します。
3. デスティネーションのクラスタとSVMを選択します。
4. デフォルトでは*関係を初期化*が選択されています。保護を開始するには*保存*をクリックします。
5. LUN の IOPS アクティビティを確認するには、* ダッシュボード > パフォーマンス * に移動します。
6. デスティネーション クラスタで、System Manager を使用して、ビジネス継続性関係の保護が同期されていることを確認します：保護 > 関係。

CLI

1. デスティネーション クラスタから整合性グループ関係を作成します。

```
destination::> snapmirror create -source-path source-path -destination-path destination-path -cg-item-mappings volume-paths -policy policy-name
```

`snapmirror create`コマンドの `cg-item-mappings` パラメータを使用して、最大12個の構成ボリュームをマップできます。

次の例では、`cg\_src` on the source with `vol1` と `vol2` の2つの整合性グループ、およびミラー化されたデスティネーション整合性グループ `cg\_dst` を作成します。

```
destination::> snapmirror create -source-path vs1_src:/cg/cg_src -destination-path vs1_dst:/cg/cg_dst -cg-item-mappings vol_src1:@vol_dst1,vol_src2:@vol_dst2 -policy AutomatedFailOverDuplex
```

2. デスティネーション クラスタから、整合性グループを初期化します。

```
destination::> snapmirror initialize -destination-path destination-consistency-group
```

3. 初期化操作が正常に完了したことを確認してください。ステータスは `InSync` になります。

```
snapmirror show
```

4. 各クラスタで igroup を作成し、LUN をアプリケーション ホスト上のイニシエーターにマップできるようにします。

```
lun igroup create -igroup name -protocol fcp|iscsi -ostype os -initiator initiator_name
```

`lun igroup create`の詳細については、link:<https://docs.netapp.com/us-en/ontap-cli/lun-igroup-create.html>["ONTAPコマンド リファレンス"]を参照してください。

5. 各クラスタで、LUNをigroupにマッピングします。

```
lun map -path path_name -igroup igroup_name
```


6. `lun map` コマンドを実行して、LUNマッピングが正常に完了したことを確認します。その後、アプリケーションホスト上で新しいLUNを検出できます。

対称アクティブ / アクティブ保護の設定

対称保護は、System ManagerまたはONTAP CLIを使用して確立できます。どちらのインターフェースでも、[均一な構成と非均一な構成](#)の手順は異なります。

開始する前に

- どちらのクラスタでも、ONTAP 9.15.1以降が実行されている必要があります。
- 対称アクティブ / アクティブ構成には `AutomatedFailoverDuplex` 保護ポリシーが必要です。または、`type` が `automated-failover-duplex` である場合は、[カスタムSnapMirrorポリシーを作成する](#)を指定することもできます。
- ONTAP 9.15.1では、対称アクティブ / アクティブは2ノードクラスタでのみサポートされます。
- ONTAP 9.16.1 GA以降、SnapMirrorアクティブ同期は4ノードクラスタで対称アクティブ / アクティブ構成をサポートします。
 - 4ノードクラスタでSnapMirror Active Syncを使用するには、ONTAP 9.16.1 GA以降を実行している必要があります。
 - 4ノード構成を導入する前に、[クラスタ ピア関係を作成](#)する必要があります。
 - 4ノードクラスタの[制限](#)を確認します。
 - 2ノードクラスタに戻す場合は、戻す前にクラスタからSnapMirrorアクティブな同期関係を削除する必要があります。
 - 4ノード構成を使用して、ストレージとコントローラーをアップグレードできます。このプロセスは中断を伴わず、ボリュームを新しいノードに移動しながらクラスタを拡張します。詳細については、["クラスタを更新する"](#)をご覧ください。
- ONTAP 9.17.1以降では、両方のクラスタがONTAP 9.17.1以降を実行している場合にのみ、NVMe名前空間で対称アクティブ / アクティブ保護を設定できます。

SCSI SnapMirrorアクティブ同期構成を使用した対称アクティブ / アクティブ保護の設定

手順

System Manager または ONTAP CLI を使用して、SCSI プロトコル ホスト マッピングを使用した対称アクティブ / アクティブ保護を設定できます。

System Manager

均一な構成の手順

1. プライマリサイトで、**"新しい LUN を使用して整合性グループを作成します。"**
 - a. 整合性グループを作成する際は、igroupを作成するホスト イニシエータを指定します。
 - b. **SnapMirror**を有効にするチェックボックスをオンにして、`AutomatedFailoverDuplex`ポリシーを選択します。
 - c. 表示されるダイアログボックスで、igroup をレプリケートするには、「イニシエータグループをレプリケートする」チェックボックスをオンにします。「近接設定の編集」で、ホストの近接 SVM を設定します。
 - d. 保存を選択します。

不均一な構成の手順

1. プライマリサイトで、**"新しい LUN を使用して整合性グループを作成します。"**
 - a. 整合性グループを作成する際は、igroupを作成するホスト イニシエータを指定します。
 - b. **SnapMirror**を有効にするチェックボックスをオンにして、`AutomatedFailoverDuplex`ポリシーを選択します。
 - c. 保存を選択して、LUN、整合性グループ、igroup、SnapMirror関係、およびigroupマッピングを作成します。
2. セカンダリ サイトで、igroupを作成し、LUNをマッピングします。
 - a. ホスト > **SAN** イニシエータ グループ に移動します。
 - b. 新しい igroup を作成するには、+ 追加を選択します。
 - c. 名前 を入力し、ホスト オペレーティング システム を選択して、イニシエーター グループ メンバー を選択します。
 - d. 関係を初期化するには、保存を選択します。
3. 新しいigroupをデスティネーションLUNにマッピングします。
 - a. **Storage > LUN** に移動します。
 - b. igroupにマッピングするLUNをすべて選択します。
 - c. 詳細を選択し、イニシエーター グループにマップを選択します。

CLI

均一な構成の手順

1. アプリケーション内のすべてのボリュームをグループ化する新しいSnapMirror関係を作成します。双方向同期レプリケーションを確立するために `AutomatedFailOverDuplex` ポリシーを指定してください。

```
snapmirror create -source-path <source_path> -destination-path  
<destination_path> -cg-item-mappings <source_volume:@destination_volume>  
-policy AutomatedFailOverDuplex
```

例：次の例では、ソースに vol1 と vol2 を含む cg_src と、デスティネーションにミラー化された整合性グループ cg_dst という 2 つの整合性グループを作成します。

```
destination::> snapmirror create -source-path vs1_src:/cg/cg_src
-destination-path vs1_dst:/cg/cg_dst -cg-item-mappings
vol_src1:@vol_dst1,vol_src2:@vol_dst2 -policy
AutomatedFailOverDuplex
```

2. SnapMirror 関係を初期化します：

```
snapmirror initialize -destination-path <destination-consistency-group>
```

3. 'Mirrored State'が'SnapMirrored'として表示され、'Relationship Status'が'Insync'として表示されるまで待機して、操作が成功したことを確認します。

```
snapmirror show -destination-path <destination_path>
```

4. ホストで、必要に応じて、各クラスタにアクセスできるようホスト接続を設定します。

5. igroupの設定を確立します。ローカルクラスタ上のイニシエータの優先パスを設定します。逆アフィニティのために、設定をピアクラスタにレプリケートするオプションを指定します。

```
SiteA::> igroup create -vserver <svm_name> -ostype <os_type> -igroup
<igroup_name> -replication-peer <peer_svm_name> -initiator <host>
```



ONTAP 9.16.1以降では、このコマンドで`-proximal-vserver local`パラメータを使用します。

```
SiteA::> igroup add -vserver <svm_name> -igroup <igroup_name> -ostype
<os_type> -initiator <host>
```



ONTAP 9.16.1以降では、このコマンドで`-proximal-vserver peer`パラメータを使用します。

6. ホストからパスを検出し、優先クラスタからストレージLUNへのアクティブ / 最適化パスがホストに設定されていることを確認します。

7. アプリケーションを導入し、VMワークロードをクラスタ間に分散して、必要な負荷分散を実現します。

不均一な構成の手順

1. アプリケーション内のすべてのボリュームをグループ化する新しいSnapMirror関係を作成します。双方向同期レプリケーションを確立するために`AutomatedFailOverDuplex`ポリシーを指定してください。

```
snapmirror create -source-path <source_path> -destination-path
<destination_path> -cg-item-mappings <source_volume:@destination_volume>
-policy AutomatedFailOverDuplex
```

例：次の例では、ソースに vol1 と vol2 を含む cg_src と、デスティネーションにミラー化された整合性グループ cg_dst という 2 つの整合性グループを作成します。

```
destination::> snapmirror create -source-path vs1_src:/cg/cg_src
-destination-path vs1_dst:/cg/cg_dst -cg-item-mappings
vol_src1:@vol_dst1,vol_src2:@vol_dst2 -policy
AutomatedFailOverDuplex
```

2. SnapMirror 関係を初期化します：

```
snapmirror initialize -destination-path <destination-consistency-group>
```

3. 'Mirrored State'が 'SnapMirrored'として表示され、 'Relationship Status'が 'Insync'として表示されるまで待機して、操作が成功したことを確認します。

```
snapmirror show -destination-path <destination_path>
```

4. ホストで、必要に応じて、各クラスタにアクセスできるようホスト接続を設定します。

5. ソースとデスティネーションの両方のクラスタでigroup設定を確立します。

```
# primary site
SiteA::> igroup create -vserver <svm_name> -igroup <igroup_name> -initiator
<host_1_name_>
```

```
# secondary site
SiteB::> igroup create -vserver <svm_name> -igroup <igroup_name> -initiator
<host_2_name>
```

6. ホストからパスを検出し、優先クラスタからストレージLUNへのアクティブ / 最適化パスがホストに設定されていることを確認します。

7. アプリケーションを導入し、VMワークロードをクラスタ間に分散して、必要な負荷分散を実現します。

NVMeSnapMirrorアクティブ同期構成を使用して対称アクティブ / アクティブ保護を構成する

開始する前に

対称アクティブ / アクティブ保護を構成するための要件に加えて、NVMeプロトコルを使用するときは、サポートされている構成とサポートされていない構成に注意する必要があります。

- 整合性グループには 1 つ以上のサブシステムを含めることができます。
- 整合性グループ内のボリュームには、複数のサブシステムからのネームスペースマップを設定できます。
- サブシステムは、複数の整合性グループに属する名前空間マップを持つことはできません。
- サブシステムには、整合性グループに属する名前空間マップと整合性グループに属さない名前空間マップを混在させることはできません。
- サブシステムには、同じ整合性グループに含まれるネームスペースマップが必要です。

手順

ONTAP 9.17.1以降では、System ManagerまたはONTAP CLIを使用してコンシステンシ グループを作成し、NVMeプロトコル ホスト マッピングを使用して対称アクティブ / アクティブ保護を設定できます。

System Manager

1. プライマリ サイトで、"新しいボリュームまたは NVMe 名前空間を使用して整合性グループを作成します。"
2. ***+Add***を選択し、***Using new NVMe namespaces***を選択します。
3. 整合性グループ名を入力します。
4. **詳細** を選択します。
5. ***保護***セクションで、***SnapMirrorを有効にする***を選択し、**`AutomatedFailoverDuplex`**ポリシーを選択します。
6. ホスト マッピング セクションで、既存の **NVMe** サブシステム または 新しい **NVMe** サブシステム のいずれかを選択します。
7. ***近接***を選択して、近接SVMを変更します。デフォルトでは、ソースSVMが選択されています。
8. 必要に応じて、別の NVMe サブシステムを追加します。

CLI

1. アプリケーションで使用されるすべてのNVMe名前空間を含むすべてのボリュームをグループ化する新しいSnapMirror関係を作成します。`AutomatedFailOverDuplex`ポリシーを指定して、双方向同期レプリケーションを確立してください。

```
snapmirror create -source-path <source_path> -destination-path  
<destination_path> -cg-item-mappings <source_volume:@destination_volume>  
-policy AutomatedFailOverDuplex
```

例：

```
DST::> snapmirror create -source-path vs_src:/cg/cg_src_1  
-destination-path vs_dst:/cg/cg_dst_1 -cg-item-mappings  
vs_src_vol1:@vs_dst_vol1,vs_src_vol2:@vs_dst_vol2 -policy  
AutomatedFailOverDuplex
```

2. SnapMirror 関係を初期化します：

```
snapmirror initialize -destination-path <destination-consistency-group>
```

例：

```
DST::> snapmirror initialize -destination-path vs1:/cg/cg_dst_1
```

3. `Mirrored State`が`SnapMirrored`として表示され、`Relationship Status`が`Insync`として表示されるまで待機して、操作が成功したことを確認します。

```
snapmirror show -destination-path <destination_path>
```

プライマリ ボリューム内のNVMe名前空間に関連付けられたNVMeサブシステムは、セカンダリ クラスタに自動的にレプリケートされます。

4. ホストで、必要に応じて、各クラスタにアクセスできるようホスト接続を設定します。
5. 各ホストに近接するSVMを指定します。これにより、優先クラスタからのパスを使用してNVMeネームスペースへのホストアクセスが可能になります。これは、プライマリ クラスタ内のSVM_または_DRクラスタ内のSVMのいずれかになります。

次のコマンドは、SVM VS_A がホスト H1 に近いことを示し、VS_A を近位 SVM として設定します：

```
SiteA::> vserver nvme subsystem host add -subsystem ssl -host-nqn <H1_NQN>
-proximal-vservers <VS_A>
```

次のコマンドは、SVM VS_B がホスト H2 に近いことを示し、VS_B を近位 SVM として設定します：

```
SiteB::> vserver nvme subsystem host add -subsystem ssl -host-nqn <H2_NQN>
-proximal-vservers <VS_B>
```

6. ホストからパスを検出し、優先クラスターからストレージへのアクティブ / 最適化されたパスがホストにあることを確認します。
7. アプリケーションを導入し、VMワークロードをクラスタ間に分散して、必要な負荷分散を実現します。

関連情報

- ["snapmirror create"](#)
- ["snapmirror initialize"](#)
- ["snapmirror show"](#)

既存の **ONTAP SnapMirror** 関係を **SnapMirror** アクティブ同期関係に変換する

SnapMirror保護を設定している場合は、関係をSnapMirrorアクティブ同期に変換できません。ONTAP 9.15.1以降では、対称アクティブ / アクティブ保護を使用するように関係を変換できます。

既存の **iSCSI** または **FC SnapMirror** 関係を非対称 **SnapMirror** アクティブ同期関係に変換する

ソース クラスタとデスティネーション クラスタ間に既存の iSCSI または FC SnapMirror 同期関係がある場合は、それを非対称 SnapMirror アクティブ同期関係に変換できます。これにより、ミラー ボリュームを整合性グループに関連付けることができ、マルチ ボリューム ワークロード全体で RPO ゼロを確保できます。さらに、SnapMirror アクティブ同期関係を確立する前の時点に戻す必要がある場合は、既存の SnapMirror Snapshot を保持できます。

タスク概要

- プライマリ クラスタとセカンダリ クラスタのクラスタ管理者およびSVM管理者である必要があります。
- SnapMirrorポリシーを変更してRPOゼロの同期をRTOゼロの同期に変換することはできません。
- `snapmirror create` コマンドを発行する前に、LUN のマッピングが解除されていることを確認する必要があります。

セカンダリ ボリューム上の既存の LUN がマップされ、`AutomatedFailover` ポリシーが設定されている場

合、`snapmirror create`コマンドによってエラーが発生します。

開始する前に

- プライマリ クラスタとセカンダリ クラスタの間には、ゼロ RPO SnapMirror 同期関係が存在する必要があります。
- RTOゼロのSnapMirror関係を作成する前に、デスティネーション ボリュームのすべてのLUNのマッピングを解除する必要があります。
- SnapMirrorアクティブ同期ではSANプロトコルのみサポートされます（NFS / CIFSはサポートされません）。NASアクセス用に整合性グループのコンスチチュエントがマウントされていないことを確認します。
- ["ONTAP Mediator"](#) SnapMirror アクティブ同期用に設定する必要があります。

手順

1. セカンダリ クラスタから、既存の関係に対してSnapMirror更新を実行します。

```
SiteB::>snapmirror update -destination-path vs1_dst:vol1
```

2. SnapMirrorの更新が正常に完了したことを確認します。

```
SiteB::>snapmirror show
```

3. RPOゼロの各同期関係を一時停止します。

```
SiteB::>snapmirror quiesce -destination-path vs1_dst:vol1
```

```
SiteB::>snapmirror quiesce -destination-path vs1_dst:vol2
```

4. RPOゼロの各同期関係を削除します。

```
SiteB::>snapmirror delete -destination-path vs1_dst:vol1
```

```
SiteB::>snapmirror delete -destination-path vs1_dst:vol2
```

5. ソース SnapMirror 関係を解放しますが、共通のスナップショットは保持します：

```
SiteA::>snapmirror release -relationship-info-only true -destination-path  
vs1_dst:vol1
```

```
SiteA::>snapmirror release -relationship-info-only true -destination-path  
vs1_dst:vol2
```

6. RTOゼロのSnapMirror同期関係を作成します。

```
SiteB::> snapmirror create -source-path vs1_src:/cg/cg_src -destination-path  
vs1_dst:/cg/cg_dst -cg-item-mappings vol1:@vol1,vol2:@vol2 -policy  
AutomatedFailover
```

7. 整合性グループを再同期します。

```
SiteB::> snapmirror resync -destination-path vs1_dst:/cg/cg_dst
```

8. ホストのLUN I/Oパスを再スキャンして、LUNへのすべてのパスをリストアします。

既存の **iSCSI** または **FC SnapMirror** 関係を対称アクティブ / アクティブに変換する

ONTAP 9.15.1 以降では、既存の iSCSI または FC SnapMirror 関係を SnapMirror アクティブ同期対称アクティブ / アクティブ関係に変換できます。

開始する前に

- ONTAP 9.15.1以降が実行されている必要があります。
- プライマリ クラスタとセカンダリ クラスタの間にRPOゼロのSnapMirror同期関係が存在している必要があります。
- RTOゼロのSnapMirror関係を作成する前に、デスティネーション ボリュームのすべてのLUNのマッピングを解除する必要があります。
- SnapMirrorアクティブ同期ではSANプロトコルのみサポートされます（NFS / CIFSはサポートされません）。NASアクセス用に整合性グループのコンスティチュエントがマウントされていないことを確認します。
- "**ONTAP Mediator**" SnapMirror アクティブ同期用に設定する必要があります。

手順

1. セカンダリ クラスタから、既存の関係に対してSnapMirror更新を実行します。

```
SiteB::>snapmirror update -destination-path vs1_dst:vol1
```

2. SnapMirrorの更新が正常に完了したことを確認します。

```
SiteB::>snapmirror show
```

3. RPOゼロの各同期関係を一時停止します。

```
SiteB::>snapmirror quiesce -destination-path vs1_dst:vol1
```

```
SiteB::>snapmirror quiesce -destination-path vs1_dst:vol2
```

4. RPOゼロの各同期関係を削除します。

```
SiteB::>snapmirror delete -destination-path vs1_dst:vol1
```

```
SiteB::>snapmirror delete -destination-path vs1_dst:vol2
```

5. ソース SnapMirror 関係を解放しますが、共通のスナップショットは保持します：

```
SiteA::>snapmirror release -relationship-info-only true -destination-path  
vs1_dst:vol1
```

```
SiteA::>snapmirror release -relationship-info-only true -destination-path  
vs1_dst:vol2
```

6. AutomatedFailoverDuplexポリシーを使用して、RTOゼロのSnapMirror同期関係を作成します。

```
SiteB::> snapmirror create -source-path vs1_src:/cg/cg_src -destination-path
```



```
vs1_dst:/cg/cg_dst -cg-item-mappings vol1:@vol1,vol2:@vol2 -policy
AutomatedFailoverDuplex
```

7. 既存のホストがプライマリ クラスタに対してローカルである場合は、ホストをセカンダリ クラスタに追加し、各クラスタにそれぞれアクセスできるよう接続を確立します。
8. セカンダリ サイトで、リモート ホストに関連付けられているigroupのLUNマップを削除します。



レプリケートされていないLUNのマッピングがigroupに含まれていないことを確認します。

```
SiteB::> lun mapping delete -vserver <svm_name> -igroup <igroup> -path <>
```

9. プライマリ サイトで、既存のホストのイニシエータ設定を変更して、ローカル クラスタのイニシエータの近接パスを設定します。

```
SiteA::> igroup initiator add-proximal-vserver -vserver <svm_name> -initiator
<host> -proximal-vserver <server>
```

10. 新しいホスト用の新しいigroupとイニシエータを追加し、ホストの近接性を設定してローカル サイトに対するホスト アフィニティを確立します。igroupレプリケーションを有効にして、設定をレプリケートし、リモート クラスタのホストのローカル性を反転させます。

```
SiteA::> igroup modify -vserver vsA -igroup ig1 -replication-peer vsB
SiteA::> igroup initiator add-proximal-vserver -vserver vsA -initiator host2
-proximal-vserver vsB
```

11. ホスト上のパスを検出し、優先クラスタからストレージLUNへのアクティブ / 最適化パスがホストに設定されていることを確認します。
12. アプリケーションを導入し、VMワークロードをクラスタ間に分散します。
13. 整合性グループを再同期します。

```
SiteB::> snapmirror resync -destination-path vs1_dst:/cg/cg_dst
```

14. ホストのLUN I/Oパスを再スキャンして、LUNへのすべてのパスをリストアします。

関連情報

- ["snapmirror create"](#)
- ["snapmirror delete"](#)
- ["snapmirror quiesce"](#)
- ["snapmirror release"](#)
- ["snapmirror resync"](#)
- ["snapmirror show"](#)

ONTAP SnapMirrorアクティブ同期関係タイプを変換する

ONTAP 9.15.1以降では、SnapMirrorアクティブ同期保護のタイプを非対称から対称アクティブ / アクティブに変換できます。その逆も可能です

対称アクティブ / アクティブ関係への変換

iSCSI または FC SnapMirror アクティブ同期関係を非対称保護から対称アクティブ / アクティブに変換できます。

開始する前に

- どちらのクラスタでも、ONTAP 9.15.1以降が実行されている必要があります。
- 対称アクティブ / アクティブ構成には `AutomatedFailoverDuplex` 保護ポリシーが必要です。または、`type` が `automated-failover-duplex` である場合は、[カスタムSnapMirrorポリシーを作成する](#)を指定することもできます。

System Manager

均一な構成の手順

1. デスティネーションigroupを削除します。
 - a. デスティネーション クラスタで、[ホスト] > [SAN イニシエーター グループ] に移動します。
 - b. SnapMirror関係のあるigroupを選択し、削除します。
 - c. ダイアログ ボックスで、[関連付けられている LUN のマップを解除] ボックスを選択し、[削除] を選択します。
2. SnapMirrorアクティブ同期関係を編集します。
 - a. 保護 > 関係に移動します。
 - b. 変更する関係の横にあるケバブ メニューを選択し、編集を選択します。
 - c. 保護ポリシーをAutomatedFailoverDuplexに変更します。
 - d. `AutoMatedFailoverDuplex`を選択すると、ホストの近接設定を変更するためのダイアログボックスが表示されます。イニシエーターの場合は、**Initiator proximal to**で適切なオプションを選択し、**Save**をクリックします。
 - e. 保存を選択します。
3. 保護メニューで、関係が `InSync` と表示されたら操作が成功したことを確認します。

不均一な構成の手順

1. デスティネーションigroupを削除します。
 - a. セカンダリ サイトで、ホスト > **SAN** イニシエーター グループに移動します。
 - b. SnapMirror関係のあるigroupを選択し、削除します。
 - c. ダイアログ ボックスで、[関連付けられている LUN のマップを解除] ボックスを選択し、[削除] を選択します。
2. 新しいigroupを作成します。
 - a. デスティネーション サイトの **SAN** イニシエーター グループ メニューで、追加 を選択します。
 - b. 名前 を入力し、ホスト オペレーティング システム を選択して、イニシエーター グループ メンバー を選択します。
 - c. 保存を選択します。
3. 新しいigroupをデスティネーションLUNにマッピングします。
 - a. **Storage** > **LUN** に移動します。
 - b. igroupにマッピングするLUNをすべて選択します。
 - c. 詳細を選択し、イニシエーター グループにマップを選択します。
4. SnapMirrorアクティブ同期関係を編集します。
 - a. 保護 > 関係に移動します。
 - b. 変更する関係の横にあるケバブ メニューを選択し、編集を選択します。
 - c. 保護ポリシーをAutomatedFailoverDuplexに変更します。
 - d. AutoMatedFailoverDuplexを選択すると、ホストの近接設定を変更するオプションが起動しま

す。イニシエーターの場合は、**Initiator proximal to**で適切なオプションを選択し、**Save**をクリックします。

e. 保存を選択します。

5. 保護メニューで、関係が `InSync` と表示されたら操作が成功したことを確認します。

CLI

均一な構成の手順

1. SnapMirrorポリシーを `AutomatedFailover` から `AutomatedFailoverDuplex` に変更します：

```
snapmirror modify -destination-path <destination_path> -policy  
AutomatedFailoverDuplex
```

2. ポリシーを変更すると再同期が実行されます。再同期が完了するまで待ち、関係が `Insync` であることを確認します：

```
snapmirror show -destination-path <destination_path>
```

3. 既存のホストがプライマリ クラスタに対してローカルである場合は、ホストをセカンダリ クラスタに追加し、各クラスタにそれぞれアクセスできるよう接続を確立します。

4. セカンダリ サイトで、リモート ホストに関連付けられているigroupのLUNマップを削除します。



レプリケートされていないLUNのマッピングがigroupに含まれていないことを確認します。

```
SiteB::> lun mapping delete -vserver <svm_name> -igroup <igroup> -path <>
```

5. プライマリサイトで、権限レベルを `advanced` に設定します：

```
SiteA::> set -privilege advanced
```

6. 既存のホストのイニシエーター構成を変更して、ローカル クラスタ上のイニシエーターの近位パスを設定します。

```
SiteA::*> igroup initiator add-proximal-vserver -vserver <svm_name>  
-initiator <host> -proximal-vserver <server>
```



この手順を完了したら、権限レベルを admin に戻すことができます。

7. 新しいホスト用の新しいigroupとイニシエータを追加し、ホストの近接性を設定してローカル サイトに対するホスト アフィニティを確立します。igroupレプリケーションを有効にして、設定をレプリケートし、リモート クラスタのホストのローカル性を反転させます。

```
SiteA::> igroup modify -vserver vsA -igroup ig1 -replication-peer vsB  
SiteA::> igroup initiator add-proximal-vserver -vserver vsA -initiator  
host2 -proximal-vserver vsB
```

8. ホスト上のパスを検出し、優先クラスタからストレージLUNへのアクティブ / 最適化パスがホストに設定されていることを確認します。

9. アプリケーションを導入し、VMワークロードをクラスタ間に分散します。

不均一な構成の手順

1. SnapMirrorポリシーを `AutomatedFailover` から `AutomatedFailoverDuplex` に変更します：

```
snapmirror modify -destination-path <destination_path> -policy  
AutomatedFailoverDuplex
```

2. ポリシーを変更すると再同期が実行されます。再同期が完了するまで待ち、関係が `Insync` であることを確認します：

```
snapmirror show -destination-path <destination_path>
```

3. 既存のホストがプライマリ クラスタに対してローカルである場合は、ホストをセカンダリ クラスタに追加し、各クラスタにそれぞれアクセスできるよう接続を確立します。
4. セカンダリ サイトで、新しいホスト用の新しいigroupとイニシエータを追加し、ホストの近接性を設定してローカル サイトに対するホスト アフィニティを確立します。LUNをigroupにマッピングします。

```
SiteB::> igroup create -vserver <svm_name> -igroup <igroup>  
SiteB::> igroup add -vserver <svm_name> -igroup <igroup> -initiator  
<host_name>  
SiteB::> lun mapping create -igroup <igroup> -path <path_name>
```

5. ホスト上のパスを検出し、優先クラスタからストレージLUNへのアクティブ / 最適化パスがホストに設定されていることを確認します。
6. アプリケーションを導入し、VMワークロードをクラスタ間に分散します。

対称アクティブ / アクティブから非対称iSCSIまたはFC関係に変換する

iSCSI または FC を使用して対称アクティブ / アクティブ保護を構成した場合は、ONTAP CLI を使用して関係を非対称保護に変換できます。

手順

1. すべてのVMワークロードを、ソース クラスタのローカル ホストに移動します。
2. VM インスタンスを管理していないホストの igroup 構成を削除し、igroup 構成を変更して igroup レプリケーションを終了します。

```
igroup modify -vserver <svm_name> -igroup <igroup> -replication-peer -
```

3. セカンダリ サイトで、LUNのマッピングを解除します。

```
SiteB::> lun mapping delete -vserver <svm_name> -igroup <igroup> -path <>
```

4. セカンダリ サイトで、対称アクティブ / アクティブ関係を削除します。

```
SiteB::> snapmirror delete -destination-path <destination_path>
```

5. プライマリ サイトで、対称アクティブ / アクティブ関係を解除します。

```
SiteA::> snapmirror release -destination-path <destination_path> -relationship  
-info-only true
```

6. セカンダリ サイトから、`AutomatedFailover`ポリシーを使用して同じボリューム セットへの関係を作成し、関係を再同期します。

```
SiteB::> snapmirror create -source-path <source_path> -destination-path  
<destination_path> -cg-item-mappings <source:@destination> -policy  
AutomatedFailover  
SiteB::> snapmirror resync -destination-path vs1:/cg/cg1_dst -policy  
<policy_type>
```



関係を再作成する前に、セカンダリ サイトの整合性グループに**"削除される"**が必要です。デスティネーション ボリューム**"DP型に変換する必要がある"**。ボリュームをDPに変換するには、`-AutomatedFailover``以外のポリシー（``MirrorAndVault``、`MirrorAllSnapshots``、または `Sync``）を使用して ``snapmirror resync`` コマンドを実行します。

7. 関係ミラー状態が `Snapmirrored` であり、関係ステータスが `Insync` であることを確認します。

```
snapmirror show -destination-path destination_path
```

8. ホストからパスを再検出します。

関連情報

- ["snapmirror delete"](#)
- ["snapmirror modify"](#)
- ["snapmirror release"](#)
- ["snapmirror resync"](#)
- ["snapmirror show"](#)

SnapMirrorアクティブ同期の管理とデータの保護

ONTAPコンシステンシグループ間で共通のスナップショットを作成する

定期的にスケジュールされたスナップショット操作に加えて、プライマリ SnapMirror 整合性グループ内のボリュームとセカンダリ SnapMirror 整合性グループ内のボリューム間の共通 **"Snapshot"** を手動で作成できます。

タスク概要

スケジュールされたスナップショットの作成間隔は12時間です。

開始する前に

- SnapMirrorグループ関係が同期されている必要があります。

手順

1. 共通スナップショットを作成します：

```
destination::>snapmirror update -destination-path vs1_dst:/cg/cg_dst
```

2. 更新の進行状況を監視します。

```
destination::>snapmirror show -fields newest-snapshot
```

関連情報

- ["snapmirror show"](#)

SnapMirrorアクティブ同期関係にある ONTAP クラスタの計画的なフェイルオーバーを実行する

SnapMirrorアクティブ同期関係にあるONTAPクラスタの計画的フェイルオーバーでは、セカンダリ クラスタがプライマリ クラスタをテイクオーバーするように、プライマリ クラスタとセカンダリ クラスタのロールを切り替えます。フェイルオーバー中は、通常はセカンダリ クラスタがローカルで入出力要求を処理し、クライアントの処理は中断されません。

計画的フェイルオーバーを実行する場面としては、ディザスタ リカバリ設定の健全性をテストする場合や、プライマリ クラスタでメンテナンスを実施する場合があります。

タスク概要

計画的フェイルオーバーは、セカンダリ クラスタの管理者が開始します。この処理を実行するには、セカンダリ クラスタがプライマリをテイクオーバーするように、プライマリとセカンダリのロールを切り替える必要があります。新しいプライマリ クラスタがローカルで入出力要求の処理を開始できるようになり、クライアントの処理は中断されません。

開始する前に

- SnapMirrorアクティブ同期関係が同期されている必要があります。
- ノンストップ オペレーションの実行中は、計画的フェイルオーバーを開始できません。ノンストップ オペレーションには、ボリュームの移動、アグリゲートの再配置、ストレージ フェイルオーバーなどがあります。
- ONTAP Mediatorが設定されて接続され、クォーラムを構成している必要があります。

手順

計画的フェイルオーバーは、ONTAP CLIまたはSystem Managerを使用して実行できます。

System Manager



ONTAP 9.14.1から9.8では、SnapMirrorアクティブ同期はSnapMirror Business Continuity (SM-BC) と呼ばれます。

1. System Manager で、保護 > 概要 > 関係 を選択します。
2. フェイルオーバーするSnapMirrorアクティブ同期関係を特定します。その名前の横にある `...` を選択し、次にフェイルオーバーを選択します。
3. フェイルオーバーのステータスを監視するには、ONTAP CLI の `snapmirror failover show` を使用します。

CLI

1. デスティネーション クラスタから、フェイルオーバー処理を開始します。

```
destination::>snapmirror failover start -destination-path  
vs1_dst:/cg/cg_dst
```

2. フェイルオーバーの進捗状況を監視します。

```
destination::>snapmirror failover show
```

3. フェイルオーバー処理が完了したら、デスティネーションからSnapMirror同期保護関係のステータスを監視できます。

```
destination::>snapmirror show
```

関連情報

- ["snapmirror failover show"](#)
- ["SnapMirrorフェイルオーバーの開始"](#)
- ["snapmirror show"](#)

計画外の自動ONTAPクラスタ フェイルオーバー操作からの回復

自動計画外フェイルオーバー (AUFO) は、プライマリクラスタがダウンまたは孤立した場合に発生します。ONTAPメディエーターはフェイルオーバーの発生を検知し、セカンダリクラスタへの自動計画外フェイルオーバーを実行します。セカンダリクラスタはプライマリクラスタに変換され、クライアントへのサービス提供を開始します。この処理は、ONTAPメディエーターの支援を受けてのみ実行されます。



自動計画外フェイルオーバーが実行されたあと、ホストのLUN I/Oパスを再スキャンしてI/Oパスの損失がないことを確認することが重要です。

計画外フェイルオーバー後の保護関係の再確立

保護関係は、System ManagerまたはONTAP CLIを使用して再確立できます。

System Manager



手順

ONTAP 9.14.1から9.8では、SnapMirrorアクティブ同期はSnapMirror Business Continuity (SM-BC) と呼ばれます。

1. *保護 > 関係*に移動し、関係の状態が「InSync」と表示されるまで待ちます。
2. 元のソース クラスタで操作を再開するには、をクリックして [フェールオーバー] を選択します。

CLI

```
`snapmirror failover  
show` コマンドを使用して、自動計画外フェイルオーバーのステータスを監視できます。
```

例：

```
ClusterB::> snapmirror failover show -instance  
Start Time: 9/23/2020 22:03:29  
    Source Path: vs1:/cg/scg3  
Destination Path: vs3:/cg/dcg3  
Failover Status: completed  
    Error Reason:  
        End Time: 9/23/2020 22:03:30  
Primary Data Cluster: cluster-2  
Last Progress Update: -  
    Failover Type: unplanned  
Error Reason codes: -
```

イベント メッセージと修正アクションの詳細については、"[EMS リファレンス](#)"を参照してください。

フェイルオーバー後のファンアウト構成での保護の再開

ONTAP 9.15.1以降、SnapMirror active syncは、フェイルオーバーイベント後のファンアウトレグの自動再構成をサポートします。非同期ファンアウトレグは、整合グループ関係または独立したボリューム関係のいずれかになります。詳細については、"[ファンアウト構成](#)"を参照してください。

ONTAP 9.14.1以前を使用して、SnapMirrorアクティブ同期関係にあるセカンダリ クラスタでフェイルオーバーが発生すると、SnapMirror非同期デスティネーションが健全な状態ではなくなります。SnapMirror非同期エンドポイントとの関係を削除してから再作成し、保護を手動でリストアする必要があります。

手順

1. フェイルオーバーが正常に完了したことを確認します（
`snapmirror failover show`
2. SnapMirror非同期エンドポイントで、ファンアウトエンドポイントを削除します：
`snapmirror delete -destination-path destination_path`

- 3番目のサイトで、新しいSnapMirrorアクティブ同期プライマリ ボリュームと非同期ファンアウト デスティネーション ボリュームの間にSnapMirror非同期関係を作成します：

```
snapmirror create -source-path source_path -destination-path destination_path  
-policy MirrorAllSnapshots -schedule schedule
```

4. 関係を再同期します：

```
snapmirror resync -destination-path destination_path
```

5. 関係のステータスと健全性を確認します（

```
snapmirror show
```

関連情報

- ["snapmirror create"](#)
- ["snapmirror delete"](#)
- ["snapmirror failover show"](#)
- ["snapmirror resync"](#)
- ["snapmirror show"](#)

ONTAP SnapMirrorアクティブ同期操作を監視する

SnapMirrorアクティブ同期の以下の処理を監視すると、SnapMirrorアクティブ同期設定の健全性を確保できます。

- ONTAP Mediator
- 計画的フェイルオーバー処理
- 自動計画外フェイルオーバー処理
- SnapMirrorアクティブ同期の可用性



ONTAP 9.15.1以降、System Managerは、どちらのクラスタからでもSnapMirrorアクティブ同期関係のステータスを表示します。また、System ManagerでどちらのクラスタからでもONTAPメディエーターのステータスを監視することもできます。

ONTAP Mediator

通常の動作中、ONTAP Mediatorの状態は接続済みになっているはずです。それ以外の状態の場合は、エラーが発生している可能性があります。["Event Management System \(EMS\) メッセージ"](#)を確認して、エラーの内容と適切な修正措置を判断できます。

計画的フェイルオーバー処理

計画されたフェイルオーバー操作のステータスと進行状況は、`snapmirror failover show` コマンドを使用して監視できます。例：

```
ClusterB::> snapmirror failover start -destination-path vs1:/cg/dcg1
```

フェイルオーバー操作が完了すると、新しいデスティネーション クラスタからSnapMirror保護ステータスを監視できます。例：

```
ClusterA::> snapmirror show
```

イベント メッセージと修正アクションの詳細については、"[EMS リファレンス](#)"を参照してください。

自動計画外フェイルオーバー処理

計画外の自動フェイルオーバー中に、`snapmirror failover show` コマンドを使用して操作のステータスを監視できます。

```
ClusterB::> snapmirror failover show -instance
Start Time: 9/23/2020 22:03:29
      Source Path: vs1:/cg/scg3
Destination Path: vs3:/cg/dcg3
Failover Status: completed
      Error Reason:
      End Time: 9/23/2020 22:03:30
Primary Data Cluster: cluster-2
Last Progress Update: -
      Failover Type: unplanned
Error Reason codes: -
```

イベント メッセージと修正アクションの詳細については、"[EMS リファレンス](#)"を参照してください。

SnapMirrorアクティブ同期の可用性

SnapMirrorアクティブ同期関係の可用性は、プライマリ クラスタまたはセカンダリ クラスタ、あるいはその両方で一連のコマンドを使用して確認できます。

使用するコマンドには、プライマリ クラスタとセカンダリ クラスタの両方で接続とクォーラム ステータスを確認するための `snapmirror mediator show` コマンド、`snapmirror show` コマンド、および `volume show` コマンドが含まれます。例：

```

SMBC_A::*> snapmirror mediator show
Mediator Address Peer Cluster      Connection Status Quorum Status
-----
10.236.172.86    SMBC_B      connected      true

SMBC_B::*> snapmirror mediator show
Mediator Address Peer Cluster      Connection Status Quorum Status
-----
10.236.172.86    SMBC_A      connected      true

SMBC_B::*> snapmirror show -expand

Progress
Source          Destination Mirror Relationship Total
Last
Path            Type Path            State Status Progress Healthy
Updated
-----
-----
vs0:/cg/cg1 XDP vs1:/cg/cg1_dp Snapmirrored Insync - true -
vs0:vol1 XDP vs1:vol1_dp Snapmirrored Insync - true -
2 entries were displayed.

SMBC_A::*> volume show -fields is-smbc-master,smbc-consensus,is-smbc-
failover-capable -volume vol1
vserver volume is-smbc-master is-smbc-failover-capable smbc-consensus
-----
vs0 vol1 true false Consensus

SMBC_B::*> volume show -fields is-smbc-master,smbc-consensus,is-smbc-
failover-capable -volume vol1_dp
vserver volume is-smbc-master is-smbc-failover-capable smbc-consensus
-----
vs1 vol1_dp false true No-consensus

```

関連情報

- ["snapmirror failover show"](#)
- ["SnapMirrorフェイルオーバーの開始"](#)
- ["SnapMirror Mediator show"](#)

ONTAPコンシステンシグループにボリュームを追加または削除する

アプリケーション ワークロードの要件が変更された場合は、ビジネス継続性を確保するために、整合性グループに対するボリュームの追加や削除が必要になることがあります

す。アクティブなSnapMirrorアクティブ同期関係でボリュームを追加および削除するプロセスは、使用しているONTAPのバージョンによって異なります。

このプロセスは、SnapMirror関係を削除し、整合性グループを変更してから保護を再開する必要があることがほとんどであり、その場合にはシステム停止を伴います。ONTAP 9.13.1以降では、アクティブなSnapMirror関係にある整合性グループにボリュームを追加する処理については、無停止で行えます。

タスク概要

- ONTAP 9.9.1では、ONTAP CLIを使用して、整合性グループにボリュームを追加または削除できます。
- ONTAP 9.10.1以降では、System ManagerまたはONTAP REST APIを使用して"[整合性グループ](#)"を管理することを推奨します。

ボリュームを追加または削除して整合性グループのメンバーを変更する場合は、最初に元の関係を削除してから、新しいメンバーで整合性グループを作成し直す必要があります。

- ONTAP 9.13.1以降では、アクティブなSnapMirror関係を持つ整合性グループに、ソースまたはデスティネーションからボリュームを無停止で追加できます。このアクションはNVMeプロトコルではサポートされていません。

ボリュームの削除はシステム停止を伴う処理です。ボリュームを削除する前に、SnapMirror関係を削除する必要があります。

ONTAP 9.9.1～9.13.0

開始する前に

- `InSync`状態にある間は、整合性グループの変更を開始することはできません。
- デスティネーション ボリュームのタイプはDPでなければなりません。
- 整合性グループを拡張するために追加する新しいボリュームには、ソース ボリュームとデスティネーション ボリューム間の共通スナップショットのペアが必要です。

手順

エンドポイント `vs1_src:/cg/cg_src`と`vs1_dst:/cg/cg_dst`間の整合性グループ関係における2つのボリューム マッピング (`vol_src1 ↔ vol_dst1`および `vol_src2 ↔ vol_dst2`)の例を示します。`

1. ソース クラスタとデスティネーション クラスタで、次のコマンドを使用して、ソース クラスタとデスティネーション クラスタの間に共通のスナップショットがあることを確認します `snapshot show -vserver svm_name -volume volume_name -snapshot snapmirror`

```
source::>snapshot show -vserver vs1_src -volume vol_src3 -snapshot snapmirror*
```

```
destination::>snapshot show -vserver vs1_dst -volume vol_dst3 -snapshot snapmirror*
```

2. 共通のスナップショットが存在しない場合は、FlexVol SnapMirror関係を作成して初期化します：

```
destination::>snapmirror initialize -source-path vs1_src:vol_src3  
-destination-path vs1_dst:vol_dst3
```

3. 整合性グループ関係を削除します。

```
destination::>snapmirror delete -destination-path vs1_dst:/cg/cg_dst
```

4. ソースSnapMirror関係を解放し、共通のスナップショットを保持します：

```
source::>snapmirror release -relationship-info-only true -destination-path  
vs1_dst:vol_dst3
```

5. LUNのマッピングを解除し、既存の整合性グループ関係を削除します。

```
destination::>lun mapping delete -vserver vs1_dst -path <lun_path> -igroup  
<igroup_name>
```



デスティネーションLUNのマッピングが解除され、プライマリ コピーのLUNでホストI/Oの処理が継続されます。

```
destination::>snapmirror delete -destination-path vs1_dst:/cg/cg_dst
```

```
source::>snapmirror release -destination-path vs1_dst:/cg/cg_dst  
-relationship-info-only true
```

6. **ONTAP 9.10.1～9.13.0**を使用している場合、ソース上の整合性グループを削除し、正しい構成で再作成してください。["整合性グループの削除"](#)の手順に従い、次に["独立した整合性グループの設定"](#)を実行してください。ONTAP 9.10.1以降では、削除および作成操作はSystem ManagerまたはONTAP REST APIで実行する必要があります。CLI手順はありません。

ONTAP 9.9.1を使用している場合は、次の手順に進んでください。

7. デスティネーションに新しいメンバーで新しい整合性グループを作成します。

```
destination::>snapmirror create -source-path vs1_src:/cg/cg_src  
-destination-path vs1_dst:/cg/cg_dst -cg-item-mappings vol_src1:@vol_dst1,  
vol_src2:@vol_dst2, vol_src3:@vol_dst3
```

8. RTOゼロの整合性グループ関係を再同期し、同期されていることを確認します。

```
destination::>snapmirror resync -destination-path vs1_dst:/cg/cg_dst
```

9. 手順5でマッピングを解除したLUNを再マッピングします。

```
destination::> lun map -vserver vs1_dst -path lun_path -igroup igroup_name
```

10. ホストのLUN I/Oパスを再スキャンして、LUNへのすべてのパスをリストアします。

ONTAP 9.13.1以降

ONTAP 9.13.1 以降では、アクティブなSnapMirrorアクティブ同期関係を持つ整合性グループに、中断なくボリュームを追加できます。SnapMirrorアクティブ同期は、ソースとデスティネーションの両方からのボリュームの追加をサポートします。



ONTAP 9.14.1から9.8では、SnapMirrorアクティブ同期はSnapMirror Business Continuity (SM-BC) と呼ばれます。

ソース整合性グループからボリュームを追加する方法の詳細については、[整合性グループの変更](#)を参照してください。

デスティネーション クラスタからのボリュームの追加

1. デスティネーション クラスタで、保護 > リレーションシップ を選択します。
2. ボリュームを追加するSnapMirror構成を見つけます。⋮を選択し、展開をクリックします。
3. 整合性グループにボリュームを追加するボリューム関係を選択します。
4. **Expand**を選択します。

関連情報

- ["snapmirror delete"](#)
- ["snapmirror initialize"](#)
- ["snapmirror release"](#)
- ["snapmirror resync"](#)

ONTAP SnapMirror Active Syncによるアップグレードと復元

SnapMirror Active SyncはONTAP 9.9.1以降でサポートされています。ONTAPクラスタまたはコントローラのアップグレードとリバートは、アップグレードまたはリバートするONTAPのバージョンに応じて、SnapMirror Active Sync関係に影響を及ぼします。

クラスタを更新する

ONTAP 9.16.1以降、SnapMirror active syncは対称型アクティブ / アクティブ構成の4ノードクラスタをサポートします。4ノードクラスタを使用して、コントローラとストレージをアップグレードできます。

開始する前に

- "4ノードクラスタの要件"を確認します。
- 技術更新プロセス中に非対称構成を作成できますが、更新が完了したら対称構成に戻す必要があります。
- これらの手順は、50個以下の整合性グループと400個以下のボリュームエンドポイントを持つ既存の4ノード構成に適用されます。

手順

1. "すべてのSnapMirrorアクティブ同期ボリュームを_単一_の高可用性（HA）ペアに移動する"。
2. "未使用のノードをクラスタから削除する"。
3. "新しいノードをクラスタに追加する"。
4. "すべてのボリュームを移動する"新しいノードに移動します。
5. "未使用のノードをクラスタから削除する"次にそれらを置き換えます"新しいノードで"。

SnapMirrorアクティブ同期を使用したONTAPのアップグレード

SnapMirrorアクティブ同期を使用するには、ソース クラスタとデスティネーション クラスタのすべてのノードでONTAP 9.9.1以降が実行されている必要があります。

アクティブなSnapMirrorアクティブ同期関係を持つONTAPをアップグレードする場合は、[自動無停止アップグレード（ANDU）](#)を使用する必要があります。ANDUを使用すると、アップグレードプロセス中にSnapMirrorアクティブ同期関係が同期され、正常な状態が維持されます。

ONTAPのアップグレードに向けてSnapMirrorアクティブ同期構成を準備するための設定手順はありません。ただし、アップグレードの前後に次の点を確認することを推奨します。

- SnapMirrorアクティブ同期関係が同期されている
- SnapMirrorに関連するエラーがイベント ログに記録されていない
- 両方のクラスタからMediatorがオンラインで、正常な状態である
- LUNを保護するために、すべてのホストがすべてのパスを正しく認識できる



クラスタをONTAP 9.9.1または9.9.1からONTAP 9.10.1以降にアップグレードすると、ONTAPは、System Managerを使用して設定できるSnapMirrorアクティブ同期関係のソース クラスタとデスティネーション クラスタの両方に新しい[整合性グループ](#)を作成します。



`snapmirror quiesce` コマンドと `snapmirror resume` コマンドは SnapMirror Active Sync ではサポートされません。

ONTAP 9.10.1 から ONTAP 9.9.1 へのリバート

9.10.1 から 9.9.1 に関係を戻すには、SnapMirror アクティブ同期関係を削除してから、9.10.1 のコンシステンシ・グループ・インスタンスを削除する必要があります。アクティブな SnapMirror アクティブ同期関係を持つコンシステンシ・グループは削除できません。9.9.1 以前のバージョンで別のスマートコンテナまたはエンタープライズアプリケーションに関連付けられていた FlexVol ボリュームを 9.10.1 にアップグレードした場合、それらのボリュームは、戻した時点で関連付けが解除されます。コンシステンシ・グループを削除しても、構成ボリュームやボリュームの細分スナップショットは削除されません。["整合性グループの削除"](#) ONTAP 9.10.1 以降でのこのタスクの詳細については、「」を参照してください。

ONTAP 9.9.1 からのリバート



SnapMirror アクティブ同期は、ONTAP 9.9.1 より前のリリースが混在する ONTAP クラスタではサポートされません。

ONTAP 9.9.1 から以前のリリースの ONTAP にリバートする場合は、次の点に注意してください。

- ・ クラスタが SnapMirror アクティブ同期デスティネーションをホストしている場合、関係を解除して削除するまで ONTAP 9.8 以前にリバートすることはできません。
- ・ クラスタが SnapMirror アクティブ同期ソースをホストしている場合、関係を解放するまで ONTAP 9.8 以前にリバートすることはできません。
- ・ ユーザが作成したカスタムの SnapMirror アクティブ同期ポリシーは、ONTAP 9.8 以前にリバートする前にすべて削除する必要があります。

これらの要件を満たすには、["SnapMirror アクティブ同期設定の削除"](#)を参照してください。

手順

1. SnapMirror アクティブ同期関係にあるいずれかのクラスタで次のコマンドを入力して、リバートの準備状況を確認します。

```
cluster::> system node revert-to -version 9.7 -check-only
```

次の出力例では、リバートする準備ができていないクラスタとクリーンアップ手順が示されています。

```
cluster::> system node revert-to -version 9.7 -check-only
Error: command failed: The revert check phase failed. The following
issues must be resolved before revert can be completed. Bring the data
LIFs down on running vservers. Command to list the running vservers:
vserver show -admin-state running Command to list the data LIFs that are
up: network interface show -role data -status-admin up Command to bring
all data LIFs down: network interface modify {-role data} -status-admin
down
Disable snapshot policies.
    Command to list snapshot policies: "snapshot policy show".
    Command to disable snapshot policies: "snapshot policy modify
```

```
-vserver
  * -enabled false"
```

Break off the initialized online data-protection (DP) volumes and delete

Uninitialized online data-protection (DP) volumes present on the local node.

Command to list all online data-protection volumes on the local node:

```
volume show -type DP -state online -node <local-node-name>
```

Before breaking off the initialized online data-protection volumes, quiesce and abort transfers on associated SnapMirror relationships and

wait for the Relationship Status to be Quiesced.

Command to quiesce a SnapMirror relationship: `snapmirror quiesce`

Command to abort transfers on a SnapMirror relationship: `snapmirror abort`

Command to see if the Relationship Status of a SnapMirror relationship

is Quiesced: `snapmirror show`

Command to break off a data-protection volume: `snapmirror break`

Command to break off a data-protection volume which is the destination

of a SnapMirror relationship with a policy of type "vault":
`snapmirror`

```
break -delete-snapshots
```

Uninitialized data-protection volumes are reported by the "snapmirror

break" command when applied on a DP volume.

Command to delete volume: `volume delete`

Delete current version snapshots in advanced privilege level.

Command to list snapshots: `"snapshot show -fs-version 9.9.1"`

Command to delete snapshots: `"snapshot prepare-for-revert -node <nodename>"`

Delete all user-created policies of the type active-strict-sync-mirror

and active-sync-mirror.

The command to see all active-strict-sync-mirror and active-sync-mirror

type policies is:

```
snapmirror policy show -type
```

active-strict-sync-mirror,active-sync-mirror

The command to delete a policy is :

```
snapmirror policy delete -vserver <SVM-name> -policy <policy-name>
```

2. 元に戻すチェックの要件を満たしたら、["ONTAPのリバート"](#)を参照してください。

関連情報

- ["ネットワーク インターフェイス"](#)
- ["snapmirror break"](#)
- ["snapmirror policy delete"](#)
- ["snapmirror policy show"](#)
- ["snapmirror quiesce"](#)
- ["snapmirror show"](#)

ONTAP SnapMirror Active Sync構成を削除する

RTOゼロのSnapMirror同期保護が不要になった場合は、SnapMirrorアクティブ同期関係を削除できます。

非対称構成の削除

- SnapMirrorアクティブ同期関係を削除する前に、デスティネーション クラスタのすべてのLUNのマッピングを解除する必要があります。
- LUNのマッピングが解除されてホストが再スキャンされると、SCSIターゲットはLUNのインベントリが変更されたことをホストに通知します。RTOゼロの関係が削除されたあと、RTOゼロのセカンダリ ボリュームにある既存のLUNに新しいIDが反映されます。ホストは、セカンダリ ボリュームのLUNをソース ボリュームのLUNと関係ない新しいLUNとして検出します。
- 関係が削除された後も、セカンダリボリュームはDPボリュームのままです。`snapmirror break`コマンドを発行して、それらを読み取り / 書き込みに変換できます。
- 関係が反転されていない場合、フェイルオーバー状態のときに関係を削除することはできません。

手順

1. セカンダリ クラスタから、ソース エンドポイントとデスティネーション エンドポイントの間のSnapMirrorアクティブ同期整合性グループ関係を削除します。

```
destination::>snapmirror delete -destination-path vs1_dst:/cg/cg_dst
```

2. プライマリ クラスタから、整合性グループの関係と、その関係に対して作成された Snapshot を解放します：

```
source::>snapmirror release -destination-path vs1_dst:/cg/cg_dst
```

3. ホストの再スキャンを実行してLUNのインベントリを更新します。
4. ONTAP 9.10.1以降では、SnapMirror関係を削除してもコンシステンシーグループは削除されません。コンシステンシーグループを削除する場合は、System ManagerまたはONTAP REST APIを使用する必要があります。詳細については、[整合性グループの削除](#)を参照してください。

iSCSIまたは**FC**対称アクティブ / アクティブ構成を削除

対称構成は、System ManagerまたはONTAP CLIを使用して削除できます。どちらのインターフェースでも、**均一な構成**と**非均一な構成**の手順は異なります。

System Manager

均一な構成の手順

1. プライマリ サイトで、リモート ホストをigroupから削除し、レプリケーションを終了します。
 - a. ホスト > **SAN** イニシエーター グループ に移動します。
 - b. 変更する igroup を選択し、編集 をクリックします。
 - c. リモートイニシエーターを削除し、igroupレプリケーションを終了します。保存を選択します。
2. セカンダリ サイトで、LUNのマッピングを解除してレプリケートされた関係を削除します。
 - a. ホスト > **SAN** イニシエーター グループ に移動します。
 - b. SnapMirror関係のあるigroupを選択し、削除します。
 - c. ダイアログ ボックスで、[関連付けられている **LUN** のマップを解除] ボックスを選択し、[削除] を選択します。
 - d. 保護 > 関係に移動します。
 - e. SnapMirror アクティブ同期関係を選択し、**Release** をクリックして関係を削除します。

不均一な構成の手順

1. プライマリ サイトで、リモート ホストをigroupから削除し、レプリケーションを終了します。
 - a. ホスト > **SAN** イニシエーター グループ に移動します。
 - b. 変更する igroup を選択し、編集 をクリックします。
 - c. リモートイニシエーターを削除し、igroupレプリケーションを終了します。保存を選択します。
2. セカンダリ サイトで、SnapMirrorアクティブ同期関係を削除します。
 - a. 保護 > 関係に移動します。
 - b. SnapMirror アクティブ同期関係を選択し、**Release** をクリックして関係を削除します。

CLI

均一な構成の手順

1. すべてのVMワークロードを、SnapMirrorアクティブ同期のソース クラスタのローカル ホストに移動します。
2. ソース クラスタで、igroupからイニシエーターを削除し、igroupのレプリケーションを終了するようにigroup設定を変更します。

```
SiteA::> igroup remove -vserver <svm_name> -igroup <igroup_name> -os-type <os_type> -initiator <host2>
SiteA::> igroup modify -vserver <svm_name> -igroup <igroup_name> -os-type <os_type> -replication-peer "-"
```

3. セカンダリ サイトで、LUNマッピングを削除し、igroup設定を削除します。

```
SiteB::> lun mapping delete -vserver <svm_name> -igroup <igroup_name> -path <>
SiteB::> igroup delete -vserver <svm_name> -igroup <igroup_name>
```

4. セカンダリ サイトで、SnapMirrorアクティブ同期関係を削除します。

```
SiteB::> snapmirror delete -destination-path destination_path
```

5. プライマリ サイトで、プライマリ サイトからSnapMirrorアクティブ同期関係を解放します。

```
SiteA::> snapmirror release -destination-path <destination_path>
```

6. パスを再検出して、ホストへのローカル パスのみが使用可能であることを確認します。

不均一な構成の手順

1. すべてのVMワークロードを、SnapMirrorアクティブ同期のソース クラスタのローカル ホストに移動します。
2. ソース クラスタで、igroupからイニシエータを削除します。

```
SiteA::> igroup remove -vserver <svm_name> -igroup <igroup_name> -initiator <host2>
```

3. セカンダリ サイトで、LUNマッピングを削除し、igroup設定を削除します。

```
SiteB::> lun mapping delete -vserver <svm_name> -igroup <igroup_name> -path <>
SiteB::> igroup delete -vserver <svm_name> -igroup <igroup_name>
```

4. セカンダリ サイトで、SnapMirrorアクティブ同期関係を削除します。

```
SiteB::> snapmirror delete -destination-path <destination_path>
```

5. プライマリ サイトで、プライマリ サイトからSnapMirrorアクティブ同期関係を解放します。

```
SiteA::> snapmirror release -destination-path <destination_path>
```

6. パスを再検出して、ホストへのローカル パスのみが使用可能であることを確認します。

NVMe対称アクティブ/アクティブ構成を削除する

System Manager

手順

1. ソース クラスタで、保護 > レプリケーション に移動します。
2. 削除する関係を見つけて、 を選択し、*削除*を選択します。

CLI

1. デスティネーション クラスタから、SnapMirror アクティブ同期関係を削除します。

```
snapmirror delete -destination-path <destination_path> -unmap-namespace true
```

例：

```
DST::> snapmirror delete -destination-path vs1:/cg/cg_dst_1 -force true
```

サブシステムとその名前空間はセカンダリ クラスタから削除されます。

2. ソース クラスタから、プライマリ サイトのSnapMirror アクティブ同期関係を解放します。

```
snapmirror release -destination-path <destination_path>
```

例：

```
SRC::> snapmirror release -destination-path vs1:/cg/cg_dst_1
```

3. パスを再検出して、ホストへのローカル パスのみが使用可能であることを確認します。

関連情報

- ["snapmirror break"](#)
- ["snapmirror delete"](#)
- ["snapmirror release"](#)

ONTAP MediatorまたはONTAP Cloud Mediatorを削除します

ONTAPクラスタから既存のONTAP MediatorまたはONTAP Cloud Mediatorの設定を削除するには、`snapmirror mediator remove`コマンドを使用します。たとえば、一度に使用できるMediatorは1つのタイプだけなので、1つのインスタンスを削除してから、別のインスタンスをインストールする必要があります。

手順

次のいずれかの手順を実行すると、ONTAP Mediator または ONTAP Cloud Mediator を削除できます。

ONTAP Mediator

1. ONTAP Mediatorを削除します。

```
snapmirror mediator remove -mediator-address <address> -peer-cluster  
<peerClusterName>
```

例：

```
snapmirror mediator remove -mediator-address 12.345.678.90 -peer  
-cluster cluster_xyz
```

ONTAP Cloud Mediator

1. ONTAP Cloud Mediatorを削除します：

```
snapmirror mediator remove -peer-cluster <peerClusterName> -type cloud
```

例：

```
snapmirror mediator remove -peer-cluster cluster_xyz -type cloud
```

関連情報

- ["SnapMirror Mediator の削除"](#)

トラブルシューティング

ONTAP SnapMirror 削除操作がテイクオーバー状態で失敗する

SnapMirrorアクティブ同期整合性グループの関係がテイクオーバー状態にあるときに `snapmirror delete` コマンドが失敗する場合は、次の情報を使用します。

問題：

ONTAP 9.9.1 がクラスタにインストールされている場合、SnapMirror アクティブ同期整合性グループ関係がテイクオーバー状態にあるときに `snapmirror delete` コマンドを実行すると失敗します。

```
C2_cluster::> snapmirror delete vs1:/cg/dd  
  
Error: command failed: RPC: Couldn't make connection
```

解決策

SnapMirrorアクティブ同期関係にあるノードがテイクオーバー状態にある場合は、「-force」オプションをtrueに設定してSnapMirrorの削除および解放操作を実行します。


```
C2_cluster::> snapmirror delete vs1:/cg/dd -force true

Warning: The relationship between source "vs0:/cg/ss" and destination
        "vs1:/cg/dd" will be deleted, however the items of the
destination
        Consistency Group might not be made writable, deletable, or
modifiable
        after the operation. Manual recovery might be required.
Do you want to continue? {y|n}: y
Operation succeeded: snapmirror delete for the relationship with
destination "vs1:/cg/dd".
```

関連情報

- ["snapmirror delete"](#)

ONTAP SnapMirror関係の作成と整合性グループの初期化に失敗しました

SnapMirror関係の作成と整合性グループの初期化に失敗した場合は、次の情報を使用します。

問題：

SnapMirror関係の作成と整合性グループの初期化が失敗します。

解決策：

クラスタあたりのコンシステンシ・グループの制限を超えていないことを確認してください。SnapMirror active syncにおけるコンシステンシ・グループの制限はプラットフォームに依存せず、ONTAPのバージョンによって異なります。ご使用のONTAPバージョン固有のガイダンスについては、["オブジェクト数の制限"](#)をご覧ください。

エラー：

コンシステンシ グループの初期化が停止している場合は、ONTAP REST API、System Manager、またはコマンド `sn show -expand` を使用して、コンシステンシ グループの初期化のステータスを確認します。



ONTAP 9.14.1から9.8では、SnapMirrorアクティブ同期はSnapMirror Business Continuity (SM-BC) と呼ばれます。

解決策：

整合性グループの初期化に失敗する場合は、SnapMirrorアクティブ同期関係を削除し、整合性グループを削除してから、関係を再作成して初期化します。ワークフローは、使用しているONTAPのバージョンによって異なります。

ONTAP 9.9.1を使用している場合	ONTAP 9.10.1以降を使用している場合

1. "SnapMirrorアクティブ同期設定を削除します。"
2. "整合性グループ関係を作成してから、整合性グループ関係を初期化します。"

1. 保護 > 関係 で、整合性グループの SnapMirror アクティブ同期関係を見つけます。 を選択し、削除 をクリックして SnapMirror アクティブ同期関係を削除します。
2. "整合性グループを削除します。"
3. "整合性グループを設定します。"

計画された**ONTAP**クラスタ フェイルオーバーが失敗しました

計画フェイルオーバー処理が失敗した場合は、次の情報を使用してください。

問題：

`snapmirror failover start`コマンドを実行すると、`snapmirror failover show` コマンドの出力に、無停止処理が進行中であることを示すメッセージが表示されます。

```
Cluster1::> snapmirror failover show
Source Destination Error
Path Path Type Status start-time end-time Reason
-----
vs1:/cg/cg vs0:/cg/cg planned failed 10/1/2020 10/1/2020 SnapMirror
Failover cannot start because a volume move is running. Retry the command
once volume move has finished.
08:35:04
```

原因：

ボリュームの移動、アグリゲートの再配置、ストレージのフェイルオーバーなどの無停止操作の実行中は、計画的フェイルオーバーを開始できません。

解決策：

無停止操作が完了してから、フェイルオーバー処理をもう一度実行してください。

関連情報

- "snapmirror failover show"
- "SnapMirrorフェイルオーバーの開始"

ONTAP Mediator または **ONTAP Cloud Mediator** にアクセスできないか、**Mediator** のクォーラム ステータスが **false** です

ONTAP Mediator または ONTAP Cloud Mediator にアクセスできない場合、または Mediator クォーラム ステータスが false の場合は、次の情報を使用します。

問題：

```
`snapmirror failover start`コマンドを実行すると、`snapmirror failover show`コマンドの出力に、ONTAP Mediator または ONTAP Cloud Mediator のいずれかが設定されていないことを示すメッセージが表示されます。
```

["SnapMirrorアクティブ同期用のONTAP Mediatorとクラスタの設定"](#)または["SnapMirror アクティブ同期用にONTAP Cloud Mediator を設定する"](#)を参照してください。

```
Cluster1::> snapmirror failover show
Source Destination Error
Path Path Type Status start-time end-time Reason
-----
vs0:/cg/cg vs1:/cg/cg planned failed 10/1/2020 10/1/2020 SnapMirror
failover cannot start because the source-side precheck failed. reason:
Mediator not configured.
05:50:42 05:50:43
```

原因：

Mediatorが設定されていないか、ネットワーク接続に問題があります。

解決策：

ONTAP Mediatorが設定されていない場合は、SnapMirrorアクティブ同期関係を確立する前にONTAP Mediatorを設定する必要があります。ネットワーク接続の問題を修正します。snapmirror mediator showコマンドを使用して、Mediatorが接続され、ソース サイトとデスティネーション サイトの両方でクォーラム ステータスがtrueであることを確認します。詳細については、["ONTAPメディアーターを設定する"](#)を参照してください。

```
cluster::> snapmirror mediator show
Mediator Address Peer Cluster Connection Status Quorum Status
-----
10.234.10.143 cluster2 connected true
```

関連情報

- ["snapmirror failover show"](#)
- ["SnapMirrorフェイルオーバーの開始"](#)
- ["SnapMirror Mediator show"](#)

ONTAP Cloud Mediator はアクセス可能ですが、応答が遅いです

ONTAP Cloud Mediator が、ping レイテンシが推奨レイテンシよりも高いというエラーで失敗する場合は、次の情報を使用します。

問題：

System Manager：Cloud Mediator サービスはアクセス可能ですが、応答が遅いです。

CLI: mediator add コマンドは次のエラーで失敗します:

```
`Error: command failed: The ping latency of the BlueXP cloud server is <x> ms  
which is higher than twice the recommended latency of 200 ms.
```

原因:

クラスターがNetApp Console クラウドの近くに配置されていないか、ネットワーク パスのボトルネックがある可能性があります。

解決策:

- 地理的な場所とNetApp Console クラウド（米国東部）への近さを確認します。
- ネットワーク パスを最適化したり、ボトルネックに対処したりします。
- ネットワーク ツールを使用してラウンド トリップ時間（RTT）を測定し、レイテンシを推奨制限内に短縮します。
- パフォーマンスを向上させるには、HTTP プロキシ サーバを使用します。

["SnapMirror アクティブ同期のために ONTAP Cloud Mediator とクラスタを設定する"](#)を参照してください。

サイトBで自動計画外フェイルオーバーがトリガーされない

サイト A の障害によってサイト B の計画外のフェイルオーバーがトリガーされない場合は、次の情報を使用します。

問題:

サイトAで障害が発生しても、サイトBで計画外フェイルオーバーがトリガーされません。

考えられる原因1:

ONTAP MediatorまたはONTAP Cloud Mediatorが設定されていません。これが原因かどうかを確認するには、サイトBクラスタで `snapmirror mediator show` コマンドを実行してください。

```
Cluster2::> snapmirror mediator show  
This table is currently empty.
```

この例は、Mediator がサイト B で構成されていないことを示しています。

解決策:

両方のクラスタにMediatorを設定し、ステータスが「connected」で、クォーラムがTrueに設定されていることを確認します。

考えられる原因2:

SnapMirror整合性グループが同期されていません。これが原因かどうかを確認するには、イベント ログを表示し、サイトAで障害が発生したときに整合性グループが同期されていたかどうかを確認します。

```
cluster::> event log show -event *out.of.sync*
```

Time	Node	Severity	Event

10/1/2020 23:26:12	sti42-vs1m-ucs511w	ERROR	sms.status.out.of.sync:
Source volume "vs0:zrto_cg_556844_511u_RW1" and destination volume			
"vs1:zrto_cg_556881_511w_DP1" with relationship UUID "55ab7942-03e5-11eb-			
ba5a-005056a7dc14" is in "out-of-sync" status due to the following reason:			
"Transfer failed."			

解決策：

次の手順に従って、サイトBで強制的にフェイルオーバーを実行します。

1. この整合性グループに属するすべてのLUNのサイトBへのマッピングを解除します。
2. `force` オプションを使用してSnapMirror整合性グループの関係を削除します。
3. 整合性グループの構成ボリュームに対して `snapmirror break` コマンドを入力し、ボリュームを DP から R/W に変換して、サイト B からの I/O を有効にします。
4. サイトAのノードをブートして、サイトBからサイトAへのRTOゼロの関係を作成します。
5. サイト A で `relationship-info-only` を使用して整合性グループを解放し、共通スナップショットを保持して整合性グループに属する LUN のマッピングを解除します。
6. SyncポリシーまたはAsyncポリシーを使用してボリューム レベルの関係を設定し、サイトAのボリュームをR/WからDPに変換します。
7. `snapmirror resync` を発行して関係を同期します。
8. サイトAでSyncポリシーが設定されたSnapMirror関係を削除します。
9. サイト B で `relationship-info-only true` を使用して、同期ポリシーを持つSnapMirror関係を解除します。
10. サイトBからサイトAへの整合性グループ関係を作成します。
11. サイトAから整合性グループの再同期を実行し、整合性グループが同期されていることを確認します。
12. ホストのLUN I/Oパスを再スキャンして、LUNへのすべてのパスをリストアします。

関連情報

- ["snapmirror break"](#)
- ["SnapMirror Mediator show"](#)
- ["snapmirror resync"](#)

サイト B と **ONTAP Mediator** 間のリンクがダウンし、サイト A がダウン

ONTAP MediatorまたはONTAP Cloud Mediatorの接続を確認するには、`snapmirror mediator show` コマンドを使用します。接続ステータスが到達不能で、サイトBからサイトAにアクセスできない場合は、以下のような出力が表示されます。ソリューションの手順に従って接続を復元してください。

例：

ONTAP Cloud Mediator 出力の `snapmirror mediator show` コマンドを使用します。

```
cluster::> snapmirror mediator show
Mediator Address Peer Cluster      Connection Status Quorum Status Type
-----
0.0.0.0          C1_cluster      unreachable      true      cloud
```

ONTAP Mediator 出力の `snapmirror mediator show` コマンドを使用します：

```
cluster::> snapmirror mediator show
Mediator Address Peer Cluster      Connection Status Quorum Status
-----
10.237.86.17     C1_cluster      unreachable      true
SnapMirror consistency group relationship status is out of sync.

C2_cluster::> snapmirror show -expand
Source              Destination Mirror Relationship Total
Last
Path                Type Path          State Status          Progress Healthy
Updated
-----
-----
vs0:/cg/src_cg_1 XDP vs1:/cg/dst_cg_1 Snapmirrored OutOfSync - false -
vs0:zrto_cg_655724_188a_RW1 XDP vs1:zrto_cg_655755_188c_DP1 Snapmirrored
OutOfSync - false -
vs0:zrto_cg_655733_188a_RW2 XDP vs1:zrto_cg_655762_188c_DP2 Snapmirrored
OutOfSync - false -
vs0:zrto_cg_655739_188b_RW1 XDP vs1:zrto_cg_655768_188d_DP1 Snapmirrored
OutOfSync - false -
vs0:zrto_cg_655748_188b_RW2 XDP vs1:zrto_cg_655776_188d_DP2 Snapmirrored
OutOfSync - false -
5 entries were displayed.

Site B cluster is unable to reach Site A.
C2_cluster::> cluster peer show
Peer Cluster Name      Cluster Serial Number Availability
Authentication
-----
-----
C1_cluster             1-80-000011             Unavailable      ok
```

解決策

フェイルオーバーを強制的に実行してサイトBからのI/Oを可能にし、サイトBからサイトAへのRTOゼロの関

係を確立します。サイトBで強制的にフェイルオーバーを実行するには、以下の手順に従います。

1. サイト B からコンシステンシ グループに属するすべての LUN のマッピングを解除します。これは失敗するため、最初に igroup を変更してレプリケーション ピア SVM を削除してから、LUN マップを削除する必要があります。

例：

```
C1_cluster::> lun mapping show
Vserver      Path                                     Igroup    LUN ID
Protocol
-----
vs0          /vol/cg1_lun/lun_1                     igroup1    0
mixed
vs0          /vol/cg1_lun/lun_2                     igroup1    1
mixed
2 entries were displayed.

C1_cluster::> lun mapping delete -path /vol/cg1_lun/lun_5 -igroup igroup1
Error: command failed: The peer cluster is unreachable and a SnapMirror
Mediator is not configured. The configuration is locked for
replicated
objects in this Vserver peer relationship on both clusters. The
only
supported configuration change is to manually disable replication
on
both sides of the relationship, after which configuration changes
are
supported.
C1_cluster::> igroup modify -igroup igroup1 -replication-peer -

C1_cluster::> lun mapping delete -path /vol/cg1_lun/lun_1 -igroup igroup1

C1_cluster::> lun mapping show
Vserver      Path                                     Igroup    LUN ID
Protocol
-----
vs0          /vol/cg1_lun/lun_2                     igroup1    1
mixed
1 entries were displayed.
```

1. forceオプションを使用して、SnapMirror整合性グループ関係を削除します。
2. 整合性グループを構成するボリュームに対してSnapMirror break コマンド(snapmirror break -destination_path svm:_volume_)を入力し、ボリュームを DP から RW に変換して、サイト B か

らの I/O を有効にします。

整合性グループ内の関係ごとに、SnapMirror breakコマンドを実行する必要があります。たとえば、整合性グループ内にボリュームが3つある場合は、ボリュームごとにコマンドを実行します。

3. サイトAのノードをブートして、サイトBからサイトAへのRTOゼロの関係を作成します。
4. 共通のスナップショットを保持し、整合性グループに属する LUN のマッピングを解除するには、サイト A で relationship-info-only を指定して整合性グループを解放します。
5. SyncポリシーまたはAsyncポリシーを使用してボリューム レベルの関係を設定し、サイトAのボリュームをRWからDPに変換します。
6. `snapmirror resync` コマンドを問題して、関係を同期します。
7. サイトAでSyncポリシーが設定されたSnapMirror関係を削除します。
8. サイトBでSyncポリシーが設定されたSnapMirror関係をrelationship-info-only trueを使用して解放します。
9. サイトBからサイトAへの整合性グループ関係を作成します。
10. ソース クラスタから、整合性グループを再同期します。整合性グループの状態が同期中になっていることを確認します。
11. ホストのLUN I/Oパスを再スキャンして、LUNへのすべてのパスをリストアします。

関連情報

- ["snapmirror break"](#)
- ["SnapMirror Mediator show"](#)
- ["snapmirror resync"](#)
- ["snapmirror show"](#)

サイト **A** と **ONTAP Mediator** 間のリンクがダウンし、サイト **B** がダウンしています

SnapMirrorアクティブ同期の使用時に、ONTAP Mediatorまたはピアリングされているクラスタ間の接続が失われる場合があります。SnapMirrorアクティブ同期関係のさまざまな部分の接続、可用性、合意ステータスを確認して問題を診断したうえで、接続を強制的に再開します。

チェックする項目	CLIコマンド	インジケータ
Mediator（サイトAから）	<code>snapmirror mediator show</code>	接続ステータスは次のように表示されます unreachable
サイトBの接続	<code>cluster peer show</code>	可用性は次のように表示されます unavailable
SnapMirrorアクティブ同期ボリュームの合意ステータス	<code>volume show volume_name -fields smbc-consensus</code>	sm-bc consensus`フィールドが表示されます `Awaiting-consensus

この問題の診断と解決に関する追加情報については、["NetAppナレッジベース：SnapMirrorアクティブ同期の使用時にサイトAとメディアーター間のリンクがダウンし、サイトBがダウンする"](#)を参照してください。

関連情報

- "cluster peer show"
- "SnapMirror Mediator show"

デスティネーション ボリュームにフェンスが設定されている場合、**ONTAP SnapMirror** の削除操作は失敗します

いずれかのデスティネーション ボリュームにリダイレクト フェンスが設定されている場合にSnapMirror削除操作が失敗する場合は、次の情報を使用します。

問題：

デスティネーション ボリュームのいずれかでリダイレクトのフェンシングが設定されていると、SnapMirror 削除処理が失敗します。

解決策

次の処理を実行して、リダイレクトを再試行し、デスティネーション ボリュームからフェンシングを削除します。

- SnapMirrorの再同期
- SnapMirrorの更新

ONTAPプライマリがダウンするとボリューム移動操作が停止する

SnapMirrorアクティブ同期関係でプライマリ サイトがダウンしているときに、ボリューム移動処理がカットオーバー延期状態で無期限にスタックする場合は、次の情報を使用します。

問題：

SnapMirrorアクティブ同期関係でプライマリ サイトが停止すると、ボリューム移動処理がカットオーバー保留状態になり、それ以上進まなくなります。プライマリ サイトが停止すると、セカンダリ サイトで自動計画外フェイルオーバー（AUFO）が実行されます。ボリューム移動処理の進行中にAUFOがトリガーされると、ボリューム移動は中断します。

解決策：

中断したボリューム移動処理を中止して、ボリューム移動処理を再開します。

ONTAP SnapMirrorリリースは、**Snapshot**を削除できない場合に失敗します

スナップショットを削除できず、SnapMirror 解放操作が失敗する場合は、次の情報を使用します。

問題：

スナップショットを削除できない場合、SnapMirror 解放操作は失敗します。

解決策：

スナップショットには一時タグが含まれています。 `-ignore-owners` オプションを指定した ``snapshot delete`` コマンドを使用して、一時スナップショットを削除します。

```
`snapshot delete -volume <volume_name> -snapshot <snapshot_name> -ignore-owners true -force true
```

``snapmirror release`` コマンドを再試行してください。

関連情報

- ["snapmirror release"](#)

ボリューム移動参照スナップショットは**ONTAP SnapMirror**関係の最新のものとして表示されます

ボリューム移動操作後にボリューム移動参照スナップショットがSnapMirror関係の最新のものとして表示される場合は、次の情報を使用します。

問題：

整合性グループ ボリュームでボリューム移動操作を実行した後、ボリューム移動参照スナップショットがSnapMirror関係の最新のものとして誤って表示される場合があります。

次のコマンドで最新のスナップショットを表示できます：

```
snapmirror show -fields newest-snapshot status -expand
```

解決策：

ボリューム移動操作が完了したら、``snapmirror resync``を手動で実行するか、次の自動再同期操作を待機します。

関連情報

- ["snapmirror resync"](#)
- ["snapmirror show"](#)

MetroClusterおよびSnapMirrorアクティブ同期用のONTAP Mediator

ONTAP Mediatorについて学ぶ

このドキュメントは、オンプレミス版のONTAP Mediatorについて説明しています。ONTAP 9.17.1以降で利用可能なONTAP Cloud Mediatorの詳細については、["SnapMirror アクティブ同期のドキュメント"](#)を参照してください。

ONTAP Mediator は ONTAP 機能に対していくつかの機能を提供します：

- HAメタデータ用にフェンシングされた永続的なストアを提供します。
- コントローラの稼働を確認するpingプロキシとして機能します。
- クォーラムを判定するために、ノードの健全性を同期的に照会します。

ONTAP Mediator は、次の 2 つの追加の systemctl サービスを提供します。

- **ontap_mediator.service**

ONTAP 関係を管理するための REST API サーバーを管理します。

- **mediator-scst.service**

iSCSIモジュール（SCST）の起動とシャットダウンを制御します。

システム管理者向けのツール

システム管理者向けのツールは以下のとおりです。

- **/usr/local/bin/mediator_change_password**

現在のAPIユーザ名とパスワードが提供された場合に、新しいAPIパスワードを設定します。

- **/usr/local/bin/mediator_change_user**

現在のAPIユーザ名とパスワードが提供された場合に、新しいAPIユーザ名を設定します。

- **/usr/local/bin/mediator_generate_support_bundle**

NetAppカスタマーサポートとのやり取りに必要なすべての有用なサポート情報を含むローカルtgzファイルを生成します。これには、アプリケーション構成、ログ、および一部のシステム情報が含まれます。バンドルはローカルディスク上に生成され、必要に応じて手動で転送できます。保存場所
：/opt/netapp/data/support_bundles/

- **/usr/local/bin/uninstall_ontap_mediator**

ONTAP MediatorパッケージとSCSTカーネル モジュールを削除します。すべての設定、ログ、およびメールボックス データが削除されます。

- **/usr/local/bin/mediator_unlock_user**

認証の最大試行回数を超えたAPIユーザ アカウントに対し、ロックアウトを解除します。この機能は、総当たり攻撃によるパスワードの漏えいを防ぐために使用されます。ユーザには、正しいユーザ名とパスワードの入力を求めるプロンプトが表示されます。

- **/usr/local/bin/mediator_add_user**

（サポートのみ） インストール時にAPIユーザを追加します。

注意事項

ONTAP Mediatorは、iSCSIを提供するためにSCSTに依存しています（ <http://scst.sourceforge.net/index.html> を参照）。このパッケージは、インストール時にカーネル専用にコンパイルされるカーネルモジュールです。カーネルを更新すると、SCSTの再インストールが必要になる場合があります。または、ONTAP Mediatorをアンインストールしてから再インストールし、ONTAP関係を再設定してください。



サーバOSカーネルの更新には、ONTAPのメンテナンス時間を設ける必要があります。

ONTAP Mediatorの新機能

ONTAP Mediatorはリリースごとに新しい機能強化が提供されます。新機能は以下のとお

りです。

機能強化

SCST のバージョン情報については、[SCSTのサポート対応表](#)を参照してください。

ONTAP Mediatorのバージョン	機能強化
1.11	• RHELのサポート： ◦ 互換性：9.5。 ◦ 推奨：10.1、10.0、9.7、9.6、9.4、8.10。 • Rocky Linux 10.1、9.7、8.10 のサポート。 • Oracle Linux 10.0 および 9.6 のサポート。 • MetroCluster IP 構成に IPv6 のサポートを追加します。 • fapolicyd のサポートを追加します。
1.10	• RHELのサポート： ◦ 互換性：9.5。 ◦ 推奨：10.0、9.6、9.4、8.10。 • Rocky Linux 10.0、9.6、8.10 のサポート。 • 基本 Python バージョンを Python 3.9 から Python 3.12 にアップグレードします。
1.9.1	• RHELのサポート： ◦ 互換性：9.3、9.1、8.9、8.7、8.6、8.5、8.4。 ◦ 推奨：9.5、9.4、9.2、9.0、8.10、8.8。 • Rocky Linux 9.5および8.10のサポート。 • コード署名検証用の新しい証明書を追加します。 • <code>-skip-code-signature-check</code> フラグを使用してコード署名チェックをスキップするためのサポートが追加されました。 • インストーラーは、期限切れのコード署名証明書を検出すると警告を表示します。

1.9	• RHELのサポート： ◦ 互換性：9.3、9.1、8.9、8.7、8.6、8.5、8.4。 ◦ 推奨：9.5、9.4、9.2、9.0、8.10、8.8。 • Rocky Linux 9.5および8.10のサポート。 • RHELおよびRocky LinuxでのFIPSのサポート。 • パフォーマンスの強化によって拡張性が向上。 • ファイル名の改善によってPKI署名証明書のセットアップを簡易化。
1.8	• RHELのサポート： ◦ 互換性：8.7、8.6、8.5、8.4。 ◦ 推奨：9.4、9.3、9.2、9.1、9.0、8.10、8.9、8.8。 • Rocky Linux 9.4および8.10のサポート。
1.7	• RHELのサポート： ◦ 互換性：8.7、8.6、8.5、8.4。 ◦ 推奨：9.3、9.2、9.1、9.0、8.9、8.8。 • Rocky Linux 9.3および8.9のサポート。 • 自己署名証明書およびサードパーティ署名証明書でのSAN（サブジェクトの別名）データのサポート。
1.6	• Python 3.9の更新。 • RHELのサポート： ◦ 互換性：8.7、8.6、8.5、8.4。 ◦ 推奨：9.2、9.1、9.0、8.8。 • Rocky Linux 9.2および8.8のサポート。 • RHEL 7.x / CentOSの全リリースのサポートを終了。
1.5	• RHEL 8.5、8.4、8.3、8.2、8.1、8.0、7.9、7.8、7.7、7.6のサポート。 • CentOS 7.9、7.8、7.7、7.6のサポート。 • RHEL 7.x / CentOS 7.xの廃止に関する警告を追加。 • 大規模なSnapMirrorアクティブ同期システム向けに速度を最適化。 • インストーラーに暗号コード署名が追加されました。
1.4	• RHEL 8.5、8.4、8.3、8.2、8.1、8.0、7.9、7.8、7.7、7.6のサポート。 • CentOS 7.9、7.8、7.7、7.6のサポート。 • UEFIベースのファームウェアのセキュア ブート（SB）をサポート。

1.3	• RHEL 8.3、8.2、8.1、8.0、7.9、7.8、7.7、7.6のサポート。 • CentOS 7.9、7.8、7.7、7.6のサポート。
1.2	• RHEL 8.1、8.0、7.9、7.8、7.7、7.6のサポート。 • CentOS 7.9、7.8、7.7、7.6のサポート。 • HTTPSメールボックスのサポート。 • ONTAP 9.8+ MCC-IP AUSO およびSnapMirror Active Sync ZRTO で使用します。
1.1	• RHEL 8.0および7.6のサポート。 • CentOS 7.6のサポート。 • Perlの依存関係を削除。
1.0	• iSCSIメールボックスのサポート。 • ONTAP 9.7+ MCC-IP AUSO で使用します。 • RHEL / CentOS 7.6のサポート。

OSのサポート対応表

ONTAP Mediator 用OS	1.11	1.10	1.9.1	1.9	1.8	1.7	1.6	1.5	1.4	1.3	1.2	1.1	1.0
RHEL 10.1	はい	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ
RHEL 10.0	はい	はい	はい	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ
RHEL 9.7	はい	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ
RHEL 9.6	はい	はい	はい	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ
RHEL 9.5	互換性がある	互換性がある	はい	はい	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ
RHEL 9.4	はい	はい	はい	はい	はい	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ

RHEL 9.3	いいえ	いいえ	互換性がある	互換性がある	はい	はい	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ
RHEL 9.2	いいえ	いいえ	はい	はい	はい	はい	はい	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ
RHEL 9.1	いいえ	いいえ	互換性がある	互換性がある	はい	はい	はい	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ
RHEL 9.0	いいえ	いいえ	はい	はい	はい	はい	はい	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ
RHEL 8.10	はい	はい	はい	はい	はい	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ
RHEL 8.9	いいえ	いいえ	互換性がある	互換性がある	はい	はい	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ
RHEL 8.8	いいえ	いいえ	はい	はい	はい	はい	はい	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ
RHEL 8.7	いいえ	いいえ	互換性がある	互換性がある	はい	はい	はい	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ
RHEL 8.6	いいえ	いいえ	互換性がある	互換性がある	はい	はい	はい	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ
RHEL 8.5	いいえ	いいえ	互換性がある	互換性がある	はい	はい	はい	はい	はい	いいえ	いいえ	いいえ	いいえ
RHEL 8.4	いいえ	いいえ	互換性がある	互換性がある	はい	はい	はい	はい	はい	いいえ	いいえ	いいえ	いいえ
RHEL 8.3	廃止	廃止	廃止	廃止	廃止	廃止	廃止	はい	はい	はい	いいえ	いいえ	いいえ
RHEL 8.2	廃止	廃止	廃止	廃止	廃止	廃止	廃止	はい	はい	はい	いいえ	いいえ	いいえ

RHEL 8.1	廃止	廃止	廃止	廃止	廃止	廃止	廃止	はい	はい	はい	はい	いいえ	いいえ
RHEL 8.0	廃止	廃止	廃止	廃止	廃止	廃止	廃止	はい	はい	はい	はい	はい	いいえ
RHEL および CentOS 7.9	廃止	廃止	廃止	廃止	廃止	廃止	廃止	はい	はい	はい	互換性がある	いいえ	いいえ
RHEL および CentOS 7.8	廃止	廃止	廃止	廃止	廃止	廃止	廃止	はい	はい	はい	はい	いいえ	いいえ
RHEL および CentOS 7.7	廃止	廃止	廃止	廃止	廃止	廃止	廃止	はい	はい	はい	はい	いいえ	いいえ
RHEL および CentOS 7.6	廃止	廃止	廃止	廃止	廃止	廃止	廃止	はい	はい	はい	はい	はい	はい (RHELのみ)
CentOS 8 と stream	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ	該当なし	該当なし	該当なし
Rocky Linux 10.0	はい	はい	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ
Rocky Linux 9	はい	はい	はい	はい	はい	はい	はい	該当なし	該当なし	該当なし	該当なし	該当なし	該当なし
Rocky Linux 8	はい	はい	はい	はい	はい	はい	はい	該当なし	該当なし	該当なし	該当なし	該当なし	該当なし

Oracle Linux 10.0	はい	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ
Oracle Linux 9	はい	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ

- 「○」は、ONTAP Mediatorのインストールに推奨されるOSであり、完全な互換性があり、サポートされることを意味します。
- 「×」は、OSとONTAP Mediatorに互換性がないことを意味します。
- 「互換性あり」とは、Red Hat がこれらの RHEL バージョンをサポートしなくなったものの、ONTAP Mediator をこれらのバージョンにインストールできることを意味します。
- ONTAP Mediator 1.6では、Rocky Linux 9および8のサポートが追加されています。
- ONTAP Mediator 1.5は、RHEL 7.xブランチ オペレーティング システムでサポートされる最後のリリースです。
- CentOS 8は再ブランチのためすべてのリリースで削除されました。CentOS Streamは、本番環境のターゲットOSとしては適切でないとみなされていました。サポートは予定されていません。

SCSTのサポート対応表

次の表に、ONTAP Mediatorの各バージョンでサポートされるSCSTのバージョンを示します。

ONTAP Mediatorのバージョン	サポートされるSCSTのバージョン
ONTAP Mediator 1.11	scst-3.9.tar.gz
ONTAP Mediator 1.10	scst-3.9.tar.gz
ONTAP Mediator 1.9.1	scst-3.8.0.tar.bz2
ONTAP Mediator 1.9	scst-3.8.0.tar.bz2
ONTAP Mediator 1.8	scst-3.8.0.tar.bz2
ONTAP Mediator 1.7	scst-3.7.0.tar.bz2
ONTAP Mediator 1.6	scst-3.7.0.tar.bz2
ONTAP Mediator 1.5	scst-3.6.0.tar.bz2
ONTAP Mediator 1.4	scst-3.6.0.tar.bz2
ONTAP Mediator 1.3	scst-3.5.0.tar.bz2
ONTAP Mediator 1.2	scst-3.4.0.tar.bz2
ONTAP Mediator 1.1	scst-3.4.0.tar.bz2
ONTAP Mediator 1.0	scst-3.3.0.tar.bz2

インストールまたはアップグレード

ONTAP Mediatorのインストールワークフローの概要

ONTAP Mediator のインストールには、インストールの準備、リポジトリへのアクセスの提供、インストールパッケージのダウンロード、コード署名の検証、ONTAP Mediator パッケージのインストール、およびインストール後の設定タスクの実行が含まれます。

1

"ONTAP Mediatorのインストールまたはアップグレードの準備"

ONTAP Mediator をインストールまたはアップグレードするには、すべての前提条件が満たされていることを確認する必要があります。

2

"ホストOSとMediatorのアップグレード"

既存のONTAP Mediatorをアップグレードする場合は、まず以前のバージョンをアンインストールしてから、新しいバージョンをインストールする必要があります。ONTAP Mediatorを初めてインストールする場合は、この手順をスキップできます。

3

"リポジトリアクセスを提供する"

ONTAP Mediator がインストール プロセス中に必要なパッケージにアクセスできるように、リポジトリへのアクセスを有効にする必要があります。

4

"ONTAPメディエーターのインストールパッケージをダウンロードします"

ONTAP Mediator ダウンロード ページから ONTAP Mediator インストール パッケージをダウンロードします。

5

"ONTAPメディエーターインストールパッケージのコード署名を確認します"

NetApp は、ONTAP Mediator インストールパッケージをインストールする前に、ONTAP Mediator のコード署名を検証することを推奨しています。

6

"ONTAPメディエーターをインストールする"

ONTAP Mediator をインストールするには、インストールパッケージを取得し、ホスト上でインストーラを実行する必要があります。

7

"ONTAPメディエーターのインストールを確認する"

ONTAP Mediator をインストールした後、正常に実行されていることを確認します。

8

"インストール後の構成タスクを実行する"

ONTAP Mediator をインストールして実行した後、ONTAP Mediator 機能を使用するには追加の設定タスクを実行する必要があります。

ONTAPメディエーターをインストールまたはアップグレードする

ONTAP Mediator をインストールまたはアップグレードするには、すべての前提条件を満たし、インストールパッケージをダウンロードして、ホスト上でインストーラを実行する必要があります。

- ONTAP 9.8以降では、任意のバージョンのONTAP Mediatorを使用してSnapMirrorアクティブ同期関係を監視できます。
- 任意のバージョンのONTAP Mediatorを使用してMetroCluster IP構成を監視できます。

インストールとアップグレードに関する考慮事項

ONTAP Mediator をアップグレードまたはインストールする前に、これらの点を確認してください。



ONTAP Mediator 1.8以前はRed Hat Enterprise Linux (RHEL) FIPSモードと互換性がないため、正常にインストールできません。FIPSモードが有効になっているかどうかは`fips-mode-setup --check`コマンドを使用して確認できます。FIPSモードを無効にするには`fips-modesetup --disable`コマンドを使用してください。FIPSモードを無効にした後、再起動すると、ONTAP Mediator 1.8以前を正常にインストールできます。

- ONTAP Mediatorを最新バージョンにアップグレードする必要があります。古いバージョンもすべてのONTAPリリースで動作しますが、新しいバージョンにはサードパーティ製コンポーネントのセキュリティパッチが含まれています。
- ONTAP Mediatorの新しいバージョンにアップグレードすると、より上位のバージョンが利用可能でない限り、インストーラは推奨されるSCSTバージョンに自動的にアップグレードします。より上位のSCSTバージョンを手動でインストールする手順については、"[ONTAP Mediatorの管理](#)"を参照してください。サポートされているバージョンについては、"[SCSTのサポート対応表](#)"を参照してください。



- インストールが失敗した場合は、ONTAP Mediatorの新しいバージョンにアップグレードする必要がある場合があります。
- 2025年6月15日以降、コード署名証明書の有効期限が切れているため、ONTAP Mediator 1.9および1.8のインストールまたはアップグレードは行えません。インストールまたはアップグレードに失敗した場合は、代わりにONTAP Mediator 1.9.1パッチバージョンをご使用ください。

- `yum-utils`パッケージをインストールすると、`needs-restarting`コマンドを使用できます。
- ONTAP Mediator 1.11 以降では、MetroCluster IP 構成で IPv6 がサポートされます。

ホストの要件

RHEL または Rocky Linux をインストールし、関連するリポジトリを構成するときは、次の要件に従ってください。



インストールまたは構成プロセスを変更する場合は、追加の手順を実行する必要がある場合があります。

Linuxディストリビューションの要件

- Red Hatのベストプラクティスに従って、RHELまたはRocky Linuxをインストールしてください。CentOS 8.xはサポート終了となったため、CentOS 8.xの互換バージョンは推奨されません。
- ONTAP Mediator をインストールするときは、インストール プログラムが必要なすべてのソフトウェア依存関係を取得してインストールできるように、システムが必要なリポジトリにアクセスできることを確認してください。
- yum インストーラーが RHEL リポジトリ内の依存ソフトウェアを見つけられるようにするには、インストール中またはインストール後に有効な Red Hat サブスクリプションを使用してシステムを登録します。



詳細については、Red Hat Subscription Manager のドキュメントを参照してください。

ネットワーク要件

次のポートが ONTAP Mediator で使用可能であり、未使用であることを確認します。

ポート/サービス	ソース	送受信方向	デスティネーション	目的
22 / TCP	管理ホスト	インバウンド	ONTAP Mediator	(オプション) SSH / ONTAP Mediator管理
31784 / TCP	cluster-mgmt および node-mgmt LIF	インバウンド	ONTAP Mediator のWebサーバ	(必須) REST API (HTTPS)
3260 / TCP	ノード管理LIF	インバウンド	ONTAP Mediator のiSCSIターゲット	(MetroCluster IP構成に必須) メールボックスのiSCSIデータ接続

SMBC のお客様の場合、ONTAP ではポート 3260 を有効にしたり接続したりする必要はありません。

- サードパーティのファイアウォールを使用している場合は、["ONTAP Mediatorのファイアウォール要件"](#)を参照してください。
- インターネットにアクセスできない Linux ホストの場合は、必要なパッケージがローカルリポジトリで使用可能であることを確認してください。

Linux 環境で Link Aggregation Control Protocol (LACP) を使用している場合は、カーネルを構成して `sysctl net.ipv4.conf.all.arp\_ignore` を `2` に設定します。

OSの要件

OS は次の要件を満たしている必要があります：

- 64ビットの物理インストールまたは仮想マシン
- 8GBのRAM
- 1GBのディスク スペース（アプリケーションのインストール、サーバ ログ、およびデータベースに使用）
- ユーザー：Root アクセス

次の表は ONTAP Mediator の各バージョンでサポートされている OS を示しています。

ONTAP Mediatorのバージョン	サポートされるLinuxバージョン
1.11	• Red Hat Enterprise Linux ◦ 互換性：9.5¹ ◦ 推奨：10.1、10.0、9.7、9.6、9.4、8.10 • Rocky Linux 10.1、9.7、および 8.10 • Oracle Linux 10.0 および 9.6
1.10	• Red Hat Enterprise Linux ◦ 互換性：9.5¹ ◦ 推奨：10.0、9.6、9.4、8.10 • Rocky Linux 10.0、9.6、および 8.10
1.9.1	• Red Hat Enterprise Linux ◦ 互換性：9.3、9.1、8.9、8.7、8.6、8.5、8.4¹ ◦ 推奨：9.5、9.4、9.2、9.0、8.10、8.8 • Rocky Linux 9.5、8.10
1.9	• Red Hat Enterprise Linux ◦ 互換性：9.3、9.1、8.9、8.7、8.6、8.5、8.4¹ ◦ 推奨：9.5、9.4、9.2、9.0、8.10、8.8 • Rocky Linux 9.5、8.10
1.8	• Red Hat Enterprise Linux : ◦ 互換性：8.7、8.6、8.5、8.4¹ ◦ 推奨：9.4、9.3、9.2、9.1、9.0、8.10、8.9、8.8 • Rocky Linux 9.4、8.10
1.7	• Red Hat Enterprise Linux : ◦ 互換性：8.7、8.6、8.5、8.4¹ ◦ 推奨：9.3、9.2、9.1、9.0、8.9、8.8 • Rocky Linux 9.3、8.9

1.6	• Red Hat Enterprise Linux : ◦ 互換性 : 8.7、8.6、8.5、8.4 ¹ ◦ 推奨 : 9.2、9.1、9.0、8.8 • Rocky Linux 9.2、8.8
1.5	• Red Hat Enterprise Linux : 8.5、8.4、8.3、8.2、8.1、8.0、7.9、7.8、7.7、および 7.6 • CentOS : 7.9、7.8、7.7、7.6
1.4	• Red Hat Enterprise Linux : 8.5、8.4、8.3、8.2、8.1、8.0、7.9、7.8、7.7、および 7.6 • CentOS : 7.9、7.8、7.7、7.6
1.3	• Red Hat Enterprise Linux : 8.3、8.2、8.1、8.0、7.9、7.8、7.7、および 7.6 • CentOS : 7.9、7.8、7.7、7.6
1.2	• Red Hat Enterprise Linux : 8.1、8.0、7.9、7.8、7.7、および 7.6 • CentOS : 7.9、7.8、7.7、7.6

1. 互換性があるとは、Red Hat がこれらの RHEL バージョンをサポートしなくなったものの、ONTAP Mediator をこれらのバージョンにインストールできることを意味します。

OS必須パッケージ

ONTAP Mediator には次のパッケージが必要です。



パッケージは事前にインストールされているか、ONTAP Mediator インストーラによって自動的にインストールされます。

RHEL / CentOSのすべてのバージョン	RHEL 10.x / Rocky Linux 10 用の追加パッケージ	RHEL 9.x / Rocky Linux 9 用の追加パッケージ	RHEL 8.x / Rocky Linux 8 用の追加パッケージ

• openssl • openssl-devel • kernel-devel-\$ (uname -r) • gcc • make • libselinux-utils • パッチ • bzip2 • perl-Data-Dumper • perl-ExtUtils- MakeMaker • efibootmgr • mokutil	• python3.12 • python3.12-devel	• elfutils-libelf-devel • policycoreutils-python- utils • python3 • python3-devel	• elfutils-libelf-devel • policycoreutils-python- utils • redhat-lsb-core • python39 • python39-devel

Mediator インストールパッケージは、次の内容を含む自己解凍型の圧縮 tar ファイルです：

- サポートされているリリースのリポジトリから取得できないすべての依存関係を含むRPMファイル。
- インストール スクリプト。

有効な SSL 証明書を推奨します。

OSのアップグレードに関する考慮事項とカーネルの互換性

- カーネルを除くすべてのライブラリパッケージを更新できますが、ONTAP Mediatorに変更を適用するには再起動が必要になる場合があります。再起動が必要な場合は、ダウンタイムをスケジュールしてください。
- OSカーネルを最新の状態に維持してください。カーネルコアを、["ONTAP Mediatorのバージョンマトリックス"](#)に記載されているサポート対象バージョンにアップグレードしてください。システムを再起動する必要があるため、停止期間に備えてメンテナンス時間を設けてください。
 - 再起動する前に SCST カーネルモジュールをアンインストールし、その後再インストールします。
 - カーネル OS のアップグレードを開始する前に、再インストールするサポート対象バージョンの SCST を準備します。



- カーネルのバージョンがオペレーティング システムのバージョンと一致している必要があります。
- テスト済みの SCST モジュールが動作しない可能性があるため、ONTAP Mediator リリースでサポートされている OS バージョンを超えてカーネルをアップグレードしないでください。

UEFIセキュアブートが有効になっている場合は**ONTAP Mediator**をインストールします

ONTAP Mediator は、UEFI セキュア ブートが有効になっているかどうかに関係なくシステムにインストールできます。

タスク概要

ONTAP Mediatorが不要な場合、またはONTAP Mediatorのインストールに関する問題をトラブルシューティングする場合は、ONTAP Mediatorをインストールする前にUEFIセキュアブートを無効にすることができます。マシンの設定からUEFIセキュアブートオプションを無効にしてください。



UEFI セキュアブートを無効にする詳細な手順については、ホスト OS のドキュメントを参照してください。

UEFI セキュアブートを有効にした ONTAP Mediator をインストールするには、サービスを開始する前にセキュリティキーを登録する必要があります。このキーは SCST インストールのコンパイルステップで生成され、秘密鍵と公開鍵のペアとしてマシンに保存されます。`mokutil`ユーティリティを使用して、公開鍵をマシンオーナーキー（MOK）として UEFI ファームウェアに追加することで、システムが署名済みモジュールを信頼してロードできるようになります。`mokutil`パスフレーズは安全な場所に保存してください。システムを再起動して MOK をアクティブ化する際に必要になります。

手順

1. システムでUEFIセキュアブートが有効になっているかどうかを確認します：

```
mokutil --sb-state
```

結果は、このシステムでUEFIセキュアブートが有効になっているかどうかを示します。

状況	移動先...
UEFIセキュアブートが有効になっています	
UEFIセキュアブートが無効になっています	"ホストオペレーティングシステムをアップグレードしてから、ONTAP Mediatorをアップグレードします。"



- パスフレーズを作成するように求められます。パスフレーズは安全な場所に保管しておく必要があります。このパスフレーズは、UEFI Boot Managerでキーを有効にする際に必要になります。
- ONTAP Mediator 1.2.0以前のバージョンでは、このモードはサポートされていません。

2. `mokutil`ユーティリティがインストールされていない場合は、次のコマンドを実行します：

```
yum install mokutil
```

ホストOSとONTAP Mediatorをアップグレードする

ONTAP MediatorのホストOSを新しいバージョンにアップグレードするには、最初にONTAP Mediatorをアンインストールする必要があります。

タスク概要

leapp-upgrade ツールを使用して ONTAP Mediator のホスト OS をアップグレードする前に、ONTAP Mediator をアンインストールしてください。このツールは、登録済みリポジトリ内の新しい RPM バージョンをチェックします。

ONTAP Mediatorインストーラは.rpmファイルをインストールしますが、leapp-upgradeツールはこのファイルを検索対象に含めません。インストーラは登録済みリポジトリからファイルをダウンロードするのではなく、解凍するため、ツールはアップグレードを見つけることができません。パッケージをアンインストールするには、leapp-upgradeツールを使用する必要があります。

手順

1. ログ ファイルをバックアップします：

```
[rootmediator-host ~]# tar -czf ontap_mediator_file_backup.tgz -C
/opt/netapp/lib/ontap_mediator ./log
./ontap_mediator/server_config/ontap_mediator.user_config.yaml
[rootmediator-host ~]# tar -tf ontap_mediator_file_backup.tgz
./log/
./log/ontap_mediator.log
./log/scstadmin.log
./log/ontap_mediator_stdout.log
./log/ontap_mediator_requests.log
./log/install_20230419134611.log
./log/scst.log
./log/ontap_mediator_syslog.log
./ontap_mediator/server_config/ontap_mediator.user_config.yaml
[rootmediator-host ~]#
```

2. leapp-upgrade ツールを使用してアップグレードを実行します：

```
[rootmediator-host ~]# leapp preupgrade --target 8.4
..<snip upgrade checks>..
..<fix issues found>..
[rootmediator-host ~]# leapp upgrade --target 8.4
..<snip upgrade>..
[rootmediator-host ~]# cat /etc/os-release | head -2
NAME="Red Hat Enterprise Linux"
VERSION="8.4 (Ootpa)"
[rootmediator-host ~]#
```

3. ONTAP Mediatorを再インストールします：



ログ ファイルが失われないように、ONTAP Mediatorの再インストール後すぐに残りの手順を実行してください。

```
[rootmediator-host ~]# ontap-mediator-1.11.0/ontap-mediator-1.11.0

ONTAP Mediator: Self Extracting Installer

..<snip installation>..
[rootmediator-host ~]#
```

4. ontap_mediatorを停止します：

```
[rootmediator-host ~]# systemctl stop ontap_mediator
[rootmediator-host ~]#
```

5. ログ ファイルを置き換えます：

```
[rootmediator-host ~]# tar -xf ontap_mediator_log_backup.tgz -C
/opt/netapp/lib/ontap_mediator
[rootmediator-host ~]#
```

6. ontap_mediatorを起動します：

```
[rootmediator-host ~]# systemctl start ontap_mediator
[rootmediator-host ~]#
```

7. すべてのONTAPクラスタをアップグレードしたONTAP Mediatorに再接続します：

IP経由のMetroCluster

```
siteA::> metrocluster configuration-settings mediator show
Mediator IP      Port      Node      Configuration
Connection
Status      Status
-----
-----
172.31.40.122
31784      siteA-node2      true      false
           siteA-node1      true      false
           siteB-node2      true      false
           siteB-node2      true      false

siteA::> metrocluster configuration-settings mediator remove
Removing the mediator and disabling Automatic Unplanned Switchover. It
may take a few minutes to complete.
Please enter the username for the mediator: mediatoradmin
Please enter the password for the mediator:
Confirm the mediator password:
Automatic Unplanned Switchover is disabled for all nodes...
Removing mediator mailboxes...
Successfully removed the mediator.

siteA::> metrocluster configuration-settings mediator add -mediator
-address 172.31.40.122
Adding the mediator and enabling Automatic Unplanned Switchover. It may
take a few minutes to complete.
Please enter the username for the mediator: mediatoradmin
Please enter the password for the mediator:
Confirm the mediator password:
Successfully added the mediator.

siteA::> metrocluster configuration-settings mediator show
Mediator IP      Port      Node      Configuration
Connection
Status      Status
-----
-----
172.31.40.122
31784      siteA-node2      true      true
           siteA-node1      true      true
           siteB-node2      true      true
           siteB-node2      true      true

siteA::>
```

SnapMirrorアクティブ同期

SnapMirror Active Sync の場合、/opt/netapp の外部に保存されている TLS 証明書を再インストールする必要はありません。/opt/netapp に保存されている証明書をバックアップして復元してください。

```
peer1::> snapmirror mediator show
Mediator Address Peer Cluster      Connection Status Quorum Status
-----
172.31.49.237    peer2                unreachable        true

peer1::> snapmirror mediator remove -mediator-address 172.31.49.237
-peer-cluster peer2

Info: [Job 39] 'mediator remove' job queued

peer1::> job show -id 39
Job ID Name                               Owing
Vserver      Node                               State
-----
39    mediator remove    peer1    peer1-node1    Success
Description: Removing entry in mediator

peer1::> security certificate show -common-name ONTAPMediatorCA
Vserver      Serial Number  Certificate Name                                Type
-----
peer1
4A790360081F41145E14C5D7CE721DC6C210007F
ONTAPMediatorCA                                server-
ca
Certificate Authority: ONTAP Mediator CA
Expiration Date: Mon Apr 17 10:27:54 2073

peer1::> security certificate delete -common-name ONTAPMediatorCA *
1 entry was deleted.

peer1::> security certificate install -type server-ca -vserver peer1

Please enter Certificate: Press <Enter> when done
..<snip ONTAP Mediator CA public key>..

You should keep a copy of the CA-signed digital certificate for future
reference.

The installed certificate's CA and serial number for reference:
CA: ONTAP Mediator CA
serial: 44786524464C5113D5EC966779D3002135EA4254
```

The certificate's generated name for reference: ONTAPMediatorCA

```
peer2::> security certificate delete -common-name ONTAPMediatorCA *  
1 entry was deleted.
```

```
peer2::> security certificate install -type server-ca -vserver peer2
```

Please enter Certificate: Press <Enter> when done
..
..<snip ONTAP Mediator CA public key>..

You should keep a copy of the CA-signed digital certificate for future reference.

The installed certificate's CA and serial number for reference:

CA: ONTAP Mediator CA

serial: 44786524464C5113D5EC966779D3002135EA4254

The certificate's generated name for reference: ONTAPMediatorCA

```
peer1::> snapmirror mediator add -mediator-address 172.31.49.237 -peer  
-cluster peer2 -username mediatoradmin
```

Notice: Enter the mediator password.

Enter the password:

Enter the password again:

Info: [Job: 43] 'mediator add' job queued

```
peer1::> job show -id 43
```

Job ID	Name	Owning Vserver	Node	State
43	mediator add	peer1	peer1-node2	Success
Description: Creating a mediator entry				

```
peer1::> snapmirror mediator show
```

Mediator Address	Peer	Cluster	Connection Status	Quorum Status
172.31.49.237	peer2		connected	true

```
peer1::>
```

関連情報

- ["security certificate delete"](#)
- ["security certificate install"](#)
- ["セキュリティ証明書の表示"](#)
- ["SnapMirror Mediator add"](#)
- ["SnapMirror Mediator の削除"](#)
- ["storage iscsi-initiator show"](#)

ONTAP Mediatorのインストールにリポジトリアクセスを提供する

ONTAP Mediator がインストール プロセス中に必要なパッケージにアクセスできるように、リポジトリへのアクセスを有効にする必要があります。

手順

1. 次の表を参照して、アクセスする必要があるリポジトリを特定します。

オペレーティング システム	アクセスが必要なリポジトリ
RHEL 10.x	• rhel-10-for-x86_64-baseos-rpms • rhel-10-for-x86_64-appstream-rpms
RHEL 9.x	• rhel-9-for-x86_64-baseos-rpms • rhel-9-for-x86_64-appstream-rpms
RHEL 8.x	• rhel-8-for-x86_64-baseos-rpms • rhel-8-for-x86_64-appstream-rpms
RHEL 7.x	• rhel-7-server-optional-rpms
CentOS 7.x	• C7.6.1810 - Baseリポジトリ
Rocky Linux 10	• appstream • baseos
Rocky Linux 9	• appstream • baseos
Rocky Linux 8	• appstream • baseos

2. インストール中にONTAP Mediatorが必要なパッケージにアクセスできるように、次のいずれかの手順を実行して上記のリポジトリへのアクセスを有効にします。



ONTAP Mediator が「extras」リポジトリと「optional」リポジトリにある Python モジュールに依存している場合は、`rhel-X-for-x86\_64-extras-rpms` および `rhel-X-for-x86\_64-optional-rpms` ファイルにアクセスする必要がある場合があります。

RHEL 10.x オペレーティング システムの手順

オペレーティング システムが **RHEL 10.x** の場合、リポジトリへのアクセスを有効にするには、次の手順を使用します：

手順

1. 必要なリポジトリにサブスクライブします。

```
subscription-manager repos --enable rhel-10-for-x86_64-baseos-rpms
```

```
subscription-manager repos --enable rhel-10-for-x86_64-appstream-rpms
```

次の例は、このコマンドの実行例を示しています。

```
[root@localhost ~]# subscription-manager repos --enable rhel-10-for-x86_64-baseos-rpms
Repository 'rhel-10-for-x86_64-baseos-rpms' is enabled for this system.
[root@localhost ~]# subscription-manager repos --enable rhel-10-for-x86_64-appstream-rpms
Repository 'rhel-10-for-x86_64-appstream-rpms' is enabled for this system.
```

2. `yum repolist` コマンドを実行します。

新しくサブスクライブしたリポジトリがリストに表示されます。

オペレーティング システムが **RHEL 9.x** の場合、リポジトリへのアクセスを有効にするには、次の手順を使用します：

手順

1. 必要なリポジトリにサブスクライブします。

```
subscription-manager repos --enable rhel-9-for-x86_64-baseos-rpms
```

```
subscription-manager repos --enable rhel-9-for-x86_64-appstream-rpms
```

次の例は、このコマンドの実行例を示しています。

```
[root@localhost ~]# subscription-manager repos --enable rhel-9-for-
x86_64-baseos-rpms
Repository 'rhel-9-for-x86_64-baseos-rpms' is enabled for this
system.
[root@localhost ~]# subscription-manager repos --enable rhel-9-for-
x86_64-appstream-rpms
Repository 'rhel-9-for-x86_64-appstream-rpms' is enabled for this
system.
```

2. `yum repolist` コマンドを実行します。

新しくサブスクライブしたリポジトリがリストに表示されます。

オペレーティング システムが **RHEL 8.x** の場合、リポジトリへのアクセスを有効にするには、次の手順を使用します：

手順

1. 必要なリポジトリにサブスクライブします。

```
subscription-manager repos --enable rhel-8-for-x86_64-baseos-rpms
```

```
subscription-manager repos --enable rhel-8-for-x86_64-appstream-rpms
```

次の例は、このコマンドの実行例を示しています。

```
[root@localhost ~]# subscription-manager repos --enable rhel-8-for-x86_64-baseos-rpms
Repository 'rhel-8-for-x86_64-baseos-rpms' is enabled for this system.
[root@localhost ~]# subscription-manager repos --enable rhel-8-for-x86_64-appstream-rpms
Repository 'rhel-8-for-x86_64-appstream-rpms' is enabled for this system.
```

2. `yum repolist` コマンドを実行します。

新しくサブスクライブしたリポジトリがリストに表示されます。

オペレーティング システムが **RHEL 7.x** の場合、リポジトリへのアクセスを有効にするには、次の手順を使用します：

手順

1. 必要なリポジトリにサブスクライブします。

```
subscription-manager repos --enable rhel-7-server-optional-rpms
```

次の例は、このコマンドの実行例を示しています。

```
[root@localhost ~]# subscription-manager repos --enable rhel-7-
server-optional-rpms
Repository 'rhel-7-server-optional-rpms' is enabled for this system.
```

2. `yum repolist` コマンドを実行します。

次の例は、このコマンドの実行例を示しています。「rhel-7-server-optional-rpms」リポジトリがリストに表示されます。

```
[root@localhost ~]# yum repolist
Loaded plugins: product-id, search-disabled-repos, subscription-
manager
rhel-7-server-optional-rpms | 3.2 kB  00:00:00
rhel-7-server-rpms | 3.5 kB  00:00:00
(1/3): rhel-7-server-optional-rpms/7Server/x86_64/group
| 26 kB  00:00:00
(2/3): rhel-7-server-optional-rpms/7Server/x86_64/updateinfo
| 2.5 MB  00:00:00
(3/3): rhel-7-server-optional-rpms/7Server/x86_64/primary_db
| 8.3 MB  00:00:01
repo id                                repo name
status
rhel-7-server-optional-rpms/7Server/x86_64  Red Hat Enterprise
Linux 7 Server - Optional (RPMs)  19,447
rhel-7-server-rpms/7Server/x86_64          Red Hat Enterprise
Linux 7 Server (RPMs)              26,758
repolist: 46,205
[root@localhost ~]#
```

オペレーティング システムが **CentOS 7.x** の場合、リポジトリへのアクセスを有効にするには、次の手順に従います：



次の例は、CentOS 7.6用のリポジトリを示しており、その他のCentOSバージョンでは使用できない可能性があります。お使いのバージョンのCentOS用のBaseリポジトリを使用してください。

手順

1. C7.6.1810 - Baseリポジトリを追加します。C7.6.1810 - Base保管用リポジトリには、ONTAP Mediatorに必要な「kernel-devel」パッケージが含まれています。
2. /etc/yum.repos.d/CentOS-Vault.repoに次の行を追加します。

```
[C7.6.1810-base]
name=CentOS-7.6.1810 - Base
baseurl=http://vault.centos.org/7.6.1810/os/$basearch/
gpgcheck=1
gpgkey=file:///etc/pki/rpm-gpg/RPM-GPG-KEY-CentOS-7
enabled=1
```

3. `yum repolist` コマンドを実行します。

次の例は、このコマンドの実行例を示しています。CentOS-7.6.1810 - Baseリポジトリがリストに表示されます。

```
Loaded plugins: fastestmirror
Loading mirror speeds from cached hostfile
* base: distro.ibiblio.org
* extras: distro.ibiblio.org
* updates: ewr.edge.kernel.org
C7.6.1810-base | 3.6 kB 00:00:00
(1/2): C7.6.1810-base/x86_64/group_gz | 166 kB 00:00:00
(2/2): C7.6.1810-base/x86_64/primary_db | 6.0 MB 00:00:04
repo id repo name status
C7.6.1810-base/x86_64 CentOS-7.6.1810 - Base 10,019
base/7/x86_64 CentOS-7 - Base 10,097
extras/7/x86_64 CentOS-7 - Extras 307
updates/7/x86_64 CentOS-7 - Updates 1,010
repolist: 21,433
[root@localhost ~]#
```

オペレーティングシステムが **Rocky Linux 10**、**Rocky Linux 9**、または **Rocky Linux 8** の場合、リポジトリへのアクセスを有効にするには、次の手順に従います：

手順

1. 必要なリポジトリにサブスクライブします。

```
dnf config-manager --set-enabled baseos
```

```
dnf config-manager --set-enabled appstream
```

2. `clean`操作を実行します：

```
dnf clean all
```

3. リポジトリのリストを確認します。

```
dnf repolist
```

```
[root@localhost ~]# dnf config-manager --set-enabled baseos
[root@localhost ~]# dnf config-manager --set-enabled appstream
[root@localhost ~]# dnf clean all
[root@localhost ~]# dnf repolist
repo id                      repo name
appstream                    Rocky Linux 10 - AppStream
baseos                       Rocky Linux 10 - BaseOS
[root@localhost ~]#
```

```
[root@localhost ~]# dnf config-manager --set-enabled baseos
[root@localhost ~]# dnf config-manager --set-enabled appstream
[root@localhost ~]# dnf clean all
[root@localhost ~]# dnf repolist
repo id                      repo name
appstream                    Rocky Linux 9 - AppStream
baseos                       Rocky Linux 9 - BaseOS
[root@localhost ~]#
```

```
[root@localhost ~]# dnf config-manager --set-enabled baseos
[root@localhost ~]# dnf config-manager --set-enabled appstream
[root@localhost ~]# dnf clean all
[root@localhost ~]# dnf repolist
repo id                                repo name
appstream                              Rocky Linux 8 - AppStream
baseos                                 Rocky Linux 8 - BaseOS
[root@localhost ~]#
```

ONTAPメディアエーターのインストールパッケージをダウンロードします

ONTAP Mediator インストール パッケージをダウンロードしてインストールします。

手順

1. ONTAP Mediator ダウンロード ページから ONTAP Mediator インストール パッケージをダウンロードします。

["ONTAP Mediatorのダウンロードページ"](#)

2. Mediator インストールパッケージが現在の作業ディレクトリに配置されていることを確認してください：

```
[root@sdot-r730-0003a-d6 ~]# ls ontap-mediator-1.11.0.tgz
```

```
ontap-mediator-1.11.0.tgz
```



ONTAP Mediator バージョン 1.4 以前では、インストーラの名前は `ontap-mediator` です。

システムがインターネットにアクセスできない場合は、インストーラーが必要なパッケージにアクセスできることを確認してください。

3. 必要に応じて、Mediator インストール パッケージをインストール ディレクトリに移動します。
4. インストール パッケージを解凍します。

```
tar xvfz ontap-mediator-1.11.0.tgz
```

```
ontap-mediator-1.11.0/  
ontap-mediator-1.11.0/csc-prod-ONTAP-Mediator.pem  
ontap-mediator-1.11.0/csc-prod-chain-ONTAP-Mediator.pem  
ontap-mediator-1.11.0/tsa-prod-ONTAP-Mediator.pem  
ontap-mediator-1.11.0/tsa-prod-chain-ONTAP-Mediator.pem  
ontap-mediator-1.11.0/ONTAP-Mediator-production.pub  
ontap-mediator-1.11.0/ontap-mediator-1.11.0  
ontap-mediator-1.11.0/ontap-mediator-1.11.0.sig.tsr  
ontap-mediator-1.11.0/ontap-mediator-1.11.0.tsr  
ontap-mediator-1.11.0/ontap-mediator-1.11.0.sig
```

ONTAP Mediatorのコード署名の検証

NetAppでは、インストール前にONTAP Mediatorのコード署名を検証することを推奨しています。この手順はオプションです。

開始する前に

ONTAP Mediator コード署名を検証する前に、システムがこれらの要件を満たしていることを確認してください。



- 2025年6月15日以降、コード署名検証証明書の有効期限が切れているため、ONTAP Mediator 1.9および1.8のインストールまたはアップグレードはできません。代わりに、ONTAP Mediator 1.11または1.10をインストールまたはアップグレードしてください。
- システムが以下の要件を満たしていない場合、検証プロセスは必要なく、直接["ONTAP Mediatorのインストール パッケージのインストール"](#)に進むことができます。

- OpenSSLバージョン1.0.2～3.0：基本的な検証の場合
- OpenSSLバージョン1.1.0以降：時刻認証局（TSA）の処理の場合
- パブリック インターネットへのアクセス：OCSP検証の場合

ダウンロード パッケージには次のファイルが含まれています：

ファイル	概要
ONTAP-Mediator-production.pub	署名の検証に使用された公開鍵
csc-prod-chain-ONTAP-Mediator.pem	公開証明書CAの信頼チェーン
csc-prod-ONTAP-Mediator.pem	キーの生成に使用された証明書
ontap-mediator-1.11.0	バージョン1.11の製品インストール実行ファイル
ontap-mediator-1.11.0.sig	SHA-256でハッシュ化され、csc-prodキーを使用してRSA署名された、インストーラの署名

ontap-mediator-1.11.0.sig.tsr	OCSCPがインストーラの署名に使用する失効要求
ontap-mediator-1.11.0.tsr	タイムスタンプ署名要求ファイル
tsa-prod-ONTAP-Mediator.pem	TSRの公開証明書
tsa-prod-chain-ONTAP-Mediator.pem	TSRの公開証明書のCAチェーン

手順

1. `csc-prod-ONTAP-Mediator.pem`でオンライン証明書ステータス プロトコル（OCSP）を使用して失効チェックを実行します。

- a. 証明書のOCSP URLを見つけます。開発者証明書ではURIが提供されない場合があります：

```
openssl x509 -noout -ocsp_uri -in csc-prod-chain-ONTAP-Mediator.pem
```

- b. 証明書のOCSP要求を生成します。

```
openssl ocsp -issuer csc-prod-chain-ONTAP-Mediator.pem -CAfile csc-prod-chain-ONTAP-Mediator.pem -cert csc-prod-ONTAP-Mediator.pem -reqout req.der
```

- c. OCSP Managerに接続してOCSP要求を送信します。

```
openssl ocsp -issuer csc-prod-chain-ONTAP-Mediator.pem -CAfile csc-prod-chain-ONTAP-Mediator.pem -cert csc-prod-ONTAP-Mediator.pem -url ${ocsp_uri} -resp_text -respout resp.der -verify_other csc-prod-chain-ONTAP-Mediator.pem
```

2. ローカル ホストに照らしてCSCの信頼チェーンと有効期限を検証します。

```
openssl verify
```



PATH からの openssl バージョンには、有効な `cert.pem`（自己署名ではない）が必要です。

```
openssl verify -untrusted csc-prod-chain-ONTAP-Mediator.pem -CApath  
${OPENSSLDIR} csc-prod-ONTAP-Mediator.pem # Failure action: The Code-  
Signature-Check certificate has expired or is invalid. Download a newer  
version of the ONTAP Mediator.  
openssl verify -untrusted tsa-prod-chain-ONTAP-Mediator.pem -CApath  
${OPENSSLDIR} tsa-prod-ONTAP-Mediator.pem # Failure action: The Time-  
Stamp certificate has expired or is invalid. Download a newer version of  
the ONTAP Mediator.
```

3. 関連する証明書を使用して、`ontap-mediator-1.11.0.sig.tsr`および`ontap-mediator-1.11.0.tsr`ファイルを検証します：

OpenSSL 3.x

```
openssl ts -verify -data ontap-mediator-1.11.0.sig -in ontap-mediator-  
1.11.0.sig.tsr -CAfile tsa-prod-chain-ONTAP-Mediator.pem -untrusted tsa-  
prod-ONTAP-Mediator.pem
```

OpenSSL 1.x

```
openssl ts -verify -data ontap-mediator-1.11.0 -in ontap-mediator-  
1.11.0.tsr -CAfile tsa-prod-chain-ONTAP-Mediator.pem -partial_chain
```



`tsr`ファイルには、インストーラに関連付けられたタイムスタンプレスポンスとコード署名が含まれています。処理では、タイムスタンプにTSAの有効な署名があり、入力ファイルが変更されていないことを確認します。検証はマシン上でローカルに実行されます。TSAサーバーにアクセスする必要はありません。

4. キーに照らして署名を検証します。

```
openssl -dgst -verify
```

```
openssl dgst -sha256 -verify ONTAP-Mediator-production.pub -signature  
ontap-mediator-1.11.0.sig ontap-mediator-1.11.0
```

ONTAP Mediatorのインストール パッケージのインストール

ONTAP Mediator をインストールするには、インストールパッケージを取得し、ホスト上でインストーラを実行する必要があります。

手順

1. インストーラを実行し、必要に応じてプロンプトに応答します。

```
./ontap-mediator-1.11.0/ontap-mediator-1.11.0 -y
```



```
[root@scs000099753 ~]# ./ontap-mediator-1.11.0/ontap-mediator-1.11.0 -y
```



インストール中に署名のチェックをスキップするには、次のコマンドを使用します：

```
./ontap-mediator-1.11.0/ontap-mediator-1.11.0 -y --skip-code  
-signature-check
```

インストーラーは必要なアカウントを作成し、必要なパッケージをインストールします。Mediatorが既にインストールされている場合は、アップグレードを促すメッセージが表示されます。

ONTAP Mediatorのインストール例 (コンソール出力)

```
[root@mediator_host ~]# tar -zxvf ontap-mediator-1.11.0.tgz
ontap-mediator-1.11.0/
ontap-mediator-1.11.0/csc-prod-chain-ONTAP-Mediator.pem
ontap-mediator-1.11.0/csc-prod-ONTAP-Mediator.pem
ontap-mediator-1.11.0/tsa-prod-ONTAP-Mediator.pem
ontap-mediator-1.11.0/tsa-prod-chain-ONTAP-Mediator.pem
ontap-mediator-1.11.0/ONTAP-Mediator-production.pub
ontap-mediator-1.11.0/ontap-mediator-1.11.0
ontap-mediator-1.11.0/ontap-mediator-1.11.0.sig.tsr
ontap-mediator-1.11.0/ontap-mediator-1.11.0.tsr
ontap-mediator-1.11.0/ontap-mediator-1.11.0.sig
[root@mediator_host ~]# ./ontap-mediator-1.11.0/ontap-mediator-1.11.0
```

ONTAP Mediator: Self Extracting Installer

```
+ Extracting the ONTAP Mediator installation/upgrade archive
+ Performing the ONTAP Mediator run-time code signature check
  Using openssl from the path: /usr/bin/openssl configured for
CApath:/etc/pki/tls
Error querying OCSP responder
80BBA032607F0000:error:1E800080:HTTP
routines:OSSL_HTTP_REQ_CTX_nbio:failed reading
data:crypto/http/http_client.c:549:
80BBA032607F0000:error:1E800067:HTTP
routines:OSSL_HTTP_REQ_CTX_exchange:error
receiving:crypto/http/http_client.c:901:server=http://ocsp.entrust.net:
80
```

WARNING: The OCSP check failed while attempting to test the Code-Signature-Check certificate

Continue without code signature checking (only recommended if integrity has been established manually)? yes/no: yes

SKIPPING: Code signature check, manual override due to lack of OCSP response

+ Unpacking the ONTAP Mediator installer

ONTAP Mediator requires two user accounts. One for the service (netapp), and one for use by ONTAP to the mediator API (mediatoradmin). Would you like to use the default account names: netapp + mediatoradmin? (Y(es)/n(o)): yes

Enter ONTAP Mediator user account (mediatoradmin) password:

Re-Enter ONTAP Mediator user account (mediatoradmin) password:

+ Checking if SELinux is in enforcing mode

The installer will change the SELinux context type of
/opt/netapp/lib/ontap_mediator/pyenv/bin/uwsgi from type 'lib_t' to
'bin_t'.

+ Checking for default Linux firewall

+ Installing required packages.

Updating Subscription Management repositories.

Unable to read consumer identity

This system is not registered with an entitlement server. You can use
"rhc" or "subscription-manager" to register.

Last metadata expiration check: 5 days, 14:34:13 ago on Thu 10 Jul 2025
01:28:32 AM EDT.

Package openssl-1:3.2.2-16.el10.x86_64 is already installed.

Package libselinux-utils-3.8-1.el10.x86_64 is already installed.

Package perl-Data-Dumper-2.189-512.el10.x86_64 is already installed.

Package bzip2-1.0.8-25.el10.x86_64 is already installed.

Package efibootmgr-18-8.el10.x86_64 is already installed.

Package mokutil-2:0.6.0-11.el10.x86_64 is already installed.

Package polycoreutils-python-utils-3.8-1.el10.noarch is already
installed.

Package python3-3.12.9-1.el10.x86_64 is already installed.

Dependencies resolved.

=====
=====
=====
=====

Package	Version
Architecture	Size
Repository	
=====	
=====	
=====	
=====	

Installing:

elfutils-libelf-devel	
x86_64	0.192-5.el10

```

AppStream                                50 k
gcc
x86_64                                14.2.1-7.el10
AppStream                                37 M
kernel-devel
x86_64                                6.12.0-55.9.1.el10_0
AppStream                                22 M
make
x86_64                                1:4.4.1-9.el10
BaseOS                                  591 k
openssl-devel
x86_64                                1:3.2.2-16.el10
AppStream                                3.9 M
patch
x86_64                                2.7.6-26.el10
AppStream                                134 k
perl-ExtUtils-MakeMaker
noarch                                2:7.70-513.el10
AppStream                                297 k
python3-devel
x86_64                                3.12.9-1.el10
AppStream                                334 k
python3-pip
noarch                                23.3.2-7.el10
AppStream                                3.2 M
Installing dependencies:
annobin-docs
noarch                                12.92-1.el10
AppStream                                94 k
annobin-plugin-gcc
x86_64                                12.92-1.el10
AppStream                                985 k
bison
x86_64                                3.8.2-9.el10
AppStream                                1.0 M
cmake-filesystem
x86_64                                3.30.5-2.el10
AppStream                                29 k
cpp
x86_64                                14.2.1-7.el10
AppStream                                12 M
dwz
x86_64                                0.15-7.el10
AppStream                                139 k
efi-srpm-macros

```

noarch	6-6.el10
AppStream	25 k
flex	
x86_64	2.6.4-19.el10
AppStream	303 k
fonts-srpm-macros	
noarch	1:2.0.5-18.el10
AppStream	29 k
forge-srpm-macros	
noarch	0.4.0-6.el10
AppStream	23 k
gcc-plugin-annobin	
x86_64	14.2.1-7.el10
AppStream	62 k
glibc-devel	
x86_64	2.39-37.el10
AppStream	641 k
go-srpm-macros	
noarch	3.6.0-4.el10
AppStream	29 k
kernel-headers	
x86_64	6.12.0-55.9.1.el10_0
AppStream	2.3 M
kernel-srpm-macros	
noarch	1.0-25.el10
AppStream	11 k
libxcrypt-devel	
x86_64	4.4.36-10.el10
AppStream	33 k
libzstd-devel	
x86_64	1.5.5-9.el10
AppStream	
53 k	
lua-srpm-macros	
noarch	1-15.el10
AppStream	10 k
m4	
x86_64	1.4.19-11.el10
AppStream	309 k
ocaml-srpm-macros	
noarch	10-4.el10
AppStream	10 k
openblas-srpm-macros	
noarch	2-19.el10
AppStream	9.0 k
package-notes-srpm-macros	

noarch	0.5-13.e110
AppStream	11 k
perl-AutoSplit	
noarch	5.74-512.e110
AppStream	23 k
perl-Benchmark	
noarch	1.25-512.e110
AppStream	28 k
perl-CPAN-Meta-Requirements	
noarch	2.143-11.e110
AppStream	39 k
perl-CPAN-Meta-YAML	
noarch	0.018-512.e110
AppStream	29 k
perl-Devel-PPPort	
x86_64	3.72-512.e110
AppStream	223 k
perl-ExtUtils-Command	
noarch	2:7.70-513.e110
AppStream	16 k
perl-ExtUtils-Constant	
noarch	0.25-512.e110
AppStream	47 k
perl-ExtUtils-Install	
noarch	2.22-511.e110
AppStream	47 k
perl-ExtUtils-Manifest	
noarch	1:1.75-511.e110
AppStream	37 k
perl-ExtUtils-ParseXS	
noarch	1:3.51-512.e110
AppStream	190 k
perl-File-Compare	
noarch	1.100.800-512.e110
AppStream	15 k
perl-File-Copy	
noarch	2.41-512.e110
AppStream	22 k
perl-I18N-Langinfo	
x86_64	0.24-512.e110
AppStream	28 k
perl-JSON-PP	
noarch	1:4.16-512.e110
AppStream	69 k
perl-Test-Harness	
noarch	1:3.48-512.e110

```

AppStream                                288 k
  perl-lib
x86_64                                0.65-512.el10
AppStream                                16 k
  perl-srpm-macros
noarch                                1-57.el10
AppStream                                9.7 k
  perl-version
x86_64                                8:0.99.32-4.el10
AppStream                                68 k
  pyproject-srpm-macros
noarch                                1.16.2-1.el10
AppStream                                16 k
  python-srpm-macros
noarch                                3.12-9.1.el10
AppStream                                26 k
  python3-pyparsing
noarch                                3.1.1-7.el10
BaseOS                                  273 k
  qt6-srpm-macros
noarch                                6.8.1-3.el10
AppStream
  11 k
  redhat-rpm-config
noarch                                288-1.el10
AppStream                                83 k
  rust-toolset-srpm-macros
noarch                                1.84.1-1.el10
AppStream                                13 k
  systemtap-sdt-devel
x86_64                                5.2-2.el10
AppStream                                78 k
  systemtap-sdt-dtrace
x86_64                                5.2-2.el10
AppStream                                72 k
  zlib-ng-compat-devel
x86_64                                2.2.3-1.el10
AppStream                                41 k
Installing weak dependencies:
  perl-CPAN-Meta
noarch                                2.150010-511.el10
AppStream                                202 k
  perl-Encode-Locale
noarch                                1.05-31.el10
AppStream                                21 k
  perl-Time-HiRes

```

```

x86_64                                4:1.9777-511.el10
AppStream                             62 k
perl-devel
x86_64                                4:5.40.1-512.el10
AppStream                             772 k
perl-doc
noarch                                5.40.1-512.el10
AppStream                             4.9 M

```

Transaction Summary

```

=====
=====
=====
=====

```

Install 63 Packages

Total size: 94 M

Installed size: 282 M

Downloading Packages:

BaseOS Packages Red Hat Enterprise Linux 10

439 kB/s | 3.7 kB 00:00

Importing GPG key 0xFD431D51:

Userid : "Red Hat, Inc. (release key 2) <security@redhat.com>"

Fingerprint: 567E 347A D004 4ADE 55BA 8A5F 199E 2F91 FD43 1D51

From : /etc/pki/rpm-gpg/RPM-GPG-KEY-redhat-release

Key imported successfully

Importing GPG key 0x5A6340B3:

Userid : "Red Hat, Inc. (auxiliary key 3) <security@redhat.com>"

Fingerprint: 7E46 2425 8C40 6535 D56D 6F13 5054 E4A4 5A63 40B3

From : /etc/pki/rpm-gpg/RPM-GPG-KEY-redhat-release

Key imported successfully

Running transaction check

Transaction check succeeded.

Running transaction test

Transaction test succeeded.

Running transaction

Preparing :

1/1

Installing : perl-version-8:0.99.32-4.el10.x86_64

1/63

Installing : perl-File-Copy-2.41-512.el10.noarch

2/63

Installing : perl-CPAN-Meta-Requirements-2.143-11.el10.noarch

3/63

Installing : perl-Time-HiRes-4:1.9777-511.el10.x86_64

4/63


```
Installing      : perl-JSON-PP-1:4.16-512.el10.noarch
5/63
Installing      : perl-File-Compare-1.100.800-512.el10.noarch
6/63
Installing      : perl-ExtUtils-ParseXS-1:3.51-512.el10.noarch
7/63
Installing      : m4-1.4.19-11.el10.x86_64
8/63
Installing      : make-1:4.4.1-9.el10.x86_64
9/63
Installing      : bison-3.8.2-9.el10.x86_64
10/63
Installing      : flex-2.6.4-19.el10.x86_64
11/63
Installing      : perl-ExtUtils-Command-2:7.70-513.el10.noarch
12/63
Installing      : perl-ExtUtils-Manifest-1:1.75-511.el10.noarch
13/63
Installing      : systemtap-sdt-devel-5.2-2.el10.x86_64
14/63
Installing      : rust-toolset-srpm-macros-1.84.1-1.el10.noarch
15/63
Installing      : qt6-srpm-macros-6.8.1-3.el10.noarch
16/63
Installing      : python3-pip-23.3.2-7.el10.noarch
17/63
Installing      : pyproject-srpm-macros-1.16.2-1.el10.noarch
18/63
Installing      : perl-srpm-macros-1-57.el10.noarch
19/63
Installing      : perl-lib-0.65-512.el10.x86_64
20/63
Installing      : perl-doc-5.40.1-512.el10.noarch
21/63
Installing      : perl-I18N-Langinfo-0.24-512.el10.x86_64
22/63
Installing      : perl-Encode-Locale-1.05-31.el10.noarch
23/63
Installing      : perl-ExtUtils-Constant-0.25-512.el10.noarch
24/63
Installing      : perl-Devel-PPPort-3.72-512.el10.x86_64
25/63
Installing      : perl-CPAN-Meta-YAML-0.018-512.el10.noarch
26/63
Installing      : perl-CPAN-Meta-2.150010-511.el10.noarch
27/63
```

```
Installing      : perl-Benchmark-1.25-512.el10.noarch
28/63
Installing      : perl-Test-Harness-1:3.48-512.el10.noarch
29/63
Installing      : perl-AutoSplit-5.74-512.el10.noarch
30/63
Installing      : package-notes-srpm-macros-0.5-13.el10.noarch
31/63
Installing      : openssl-devel-1:3.2.2-16.el10.x86_64
32/63
Installing      : openblas-srpm-macros-2-19.el10.noarch
33/63
Installing      : ocaml-srpm-macros-10-4.el10.noarch
34/63
Installing      : lua-srpm-macros-1-15.el10.noarch
35/63
Installing      : libzstd-devel-1.5.5-9.el10.x86_64
36/63
Installing      : kernel-srpm-macros-1.0-25.el10.noarch
37/63
Installing      : kernel-headers-6.12.0-55.9.1.el10_0.x86_64
38/63
Installing      : libxcrypt-devel-4.4.36-10.el10.x86_64
39/63
Installing      : glibc-devel-2.39-37.el10.x86_64
40/63
Installing      : efi-srpm-macros-6-6.el10.noarch
41/63
Installing      : dwz-0.15-7.el10.x86_64
42/63
Installing      : cpp-14.2.1-7.el10.x86_64
43/63
Installing      : gcc-14.2.1-7.el10.x86_64
44/63
Installing      : gcc-plugin-annobin-14.2.1-7.el10.x86_64
45/63
Installing      : cmake-filesystem-3.30.5-2.el10.x86_64
46/63
Installing      : zlib-ng-compat-devel-2.2.3-1.el10.x86_64
47/63
Installing      : elfutils-libelf-devel-0.192-5.el10.x86_64
48/63
Installing      : annobin-docs-12.92-1.el10.noarch
49/63
Installing      : annobin-plugin-gcc-12.92-1.el10.x86_64
50/63
```

```

Installing      : fonts-srpm-macros-1:2.0.5-18.el10.noarch
51/63
Installing      : forge-srpm-macros-0.4.0-6.el10.noarch
52/63
Installing      : go-srpm-macros-3.6.0-4.el10.noarch
53/63
Installing      : python-srpm-macros-3.12-9.1.el10.noarch
54/63
Installing      : redhat-rpm-config-288-1.el10.noarch
55/63
Running scriptlet: redhat-rpm-config-288-1.el10.noarch
55/63
Installing      : python3-pyparsing-3.1.1-7.el10.noarch
56/63
Installing      : systemtap-sdt-dtrace-5.2-2.el10.x86_64
57/63
Installing      : perl-devel-4:5.40.1-512.el10.x86_64
58/63
Installing      : perl-ExtUtils-Install-2.22-511.el10.noarch
59/63
Installing      : perl-ExtUtils-MakeMaker-2:7.70-513.el10.noarch
60/63
Installing      : kernel-devel-6.12.0-55.9.1.el10_0.x86_64
61/63
Running scriptlet: kernel-devel-6.12.0-55.9.1.el10_0.x86_64
61/63
Installing      : python3-devel-3.12.9-1.el10.x86_64
62/63
Installing      : patch-2.7.6-26.el10.x86_64
63/63
Running scriptlet: patch-2.7.6-26.el10.x86_64
63/63
Installed products updated.

Installed:
  annobin-docs-12.92-1.el10.noarch          annobin-plugin-gcc-
12.92-1.el10.x86_64          bison-3.8.2-9.el10.x86_64
cmake-filesystem-3.30.5-2.el10.x86_64      cpp-14.2.1-
7.el10.x86_64
dwz-0.15-7.el10.x86_64          efi-srpm-macros-6-
6.el10.noarch          elfutils-libelf-devel-0.192-
5.el10.x86_64  flex-2.6.4-19.el10.x86_64          fonts-
srpm-macros-1:2.0.5-18.el10.noarch
forge-srpm-macros-0.4.0-6.el10.noarch      gcc-14.2.1-
7.el10.x86_64          gcc-plugin-annobin-14.2.1-
7.el10.x86_64      glibc-devel-2.39-37.el10.x86_64          go-

```

```

srpm-macros-3.6.0-4.el10.noarch
  kernel-devel-6.12.0-55.9.1.el10_0.x86_64      kernel-headers-6.12.0-
55.9.1.el10_0.x86_64      kernel-srpm-macros-1.0-25.el10.noarch
libxcrypt-devel-4.4.36-10.el10.x86_64      libzstd-devel-1.5.5-
9.el10.x86_64
  lua-srpm-macros-1-15.el10.noarch      m4-1.4.19-
11.el10.x86_64      make-1:4.4.1-9.el10.x86_64
ocaml-srpm-macros-10-4.el10.noarch      openblas-srpm-macros-2-
19.el10.noarch
  openssl-devel-1:3.2.2-16.el10.x86_64      package-notes-srpm-
macros-0.5-13.el10.noarch      patch-2.7.6-26.el10.x86_64
perl-AutoSplit-5.74-512.el10.noarch      perl-Benchmark-1.25-
512.el10.noarch
  perl-CPAN-Meta-2.150010-511.el10.noarch      perl-CPAN-Meta-
Requirements-2.143-11.el10.noarch      perl-CPAN-Meta-YAML-0.018-
512.el10.noarch      perl-Devel-PPPort-3.72-512.el10.x86_64      perl-
Encode-Locale-1.05-31.el10.noarch
  perl-ExtUtils-Command-2:7.70-513.el10.noarch      perl-ExtUtils-Constant-
0.25-512.el10.noarch      perl-ExtUtils-Install-2.22-511.el10.noarch
perl-ExtUtils-MakeMaker-2:7.70-513.el10.noarch      perl-ExtUtils-Manifest-
1:1.75-511.el10.noarch
  perl-ExtUtils-ParseXS-1:3.51-512.el10.noarch      perl-File-Compare-
1.100.800-512.el10.noarch      perl-File-Copy-2.41-512.el10.noarch
perl-I18N-Langinfo-0.24-512.el10.x86_64      perl-JSON-PP-1:4.16-
512.el10.noarch
  perl-Test-Harness-1:3.48-512.el10.noarch      perl-Time-HiRes-
4:1.9777-511.el10.x86_64      perl-devel-4:5.40.1-512.el10.x86_64
perl-doc-5.40.1-512.el10.noarch      perl-lib-0.65-
512.el10.x86_64
  perl-srpm-macros-1-57.el10.noarch      perl-version-8:0.99.32-
4.el10.x86_64      pyproject-srpm-macros-1.16.2-1.el10.noarch
python-srpm-macros-3.12-9.1.el10.noarch      python3-devel-3.12.9-
1.el10.x86_64
  python3-pip-23.3.2-7.el10.noarch      python3-pyparsing-
3.1.1-7.el10.noarch      qt6-srpm-macros-6.8.1-3.el10.noarch
redhat-rpm-config-288-1.el10.noarch      rust-toolset-srpm-
macros-1.84.1-1.el10.noarch
  systemtap-sdt-devel-5.2-2.el10.x86_64      systemtap-sdt-dtrace-
5.2-2.el10.x86_64      zlib-ng-compat-devel-2.2.3-1.el10.x86_64

```

Complete!

OS package installations finished

+ Installing ONTAP Mediator. (Log: /root/ontap_mediator.vdizgQ/ontap-mediator-1.11.0/ontap-mediator-1.11.0/install_20250715160240.log)

This step takes several minutes. View progress in the log file.

Sudoer config verified

```

    ONTAP Mediator rsyslog and logging rotation enabled
+ Install successful. (Moving log to
/opt/netapp/lib/ontap_mediator/log/install_20250715160240.log)
+ WARNING: This system supports UEFI
    Secure Boot (SB) is currently disabled on this system.
    If SB is enabled in the future, SCST will not work unless
the following action is taken:
    Using the keys in
/opt/netapp/lib/ontap_mediator/ontap_mediator/SCST_mod_keys follow
    instructions in
/opt/netapp/lib/ontap_mediator/ontap_mediator/SCST_mod_keys/README.modu
le-signing
    to sign the SCST kernel module. Note that a reboot is
needed.
    SCST does not start automatically when Secure Boot is enabled and
not configured properly.

+ Note: ONTAP Mediator generated a self-signed server certificate for
temporary use on
    this host. If the DNS name or IP address for the host is changed,
the certificate
    will no longer be valid. The default certificates should be
replaced with secure
    trusted certificates signed by a known certificate authority prior
to use for production.
    For more information, see /opt/netapp/lib/ontap_mediator/README

+ Note: ONTAP Mediator uses a kernel module compiled specifically for
the current
    OS. Using 'yum update' to upgrade the kernel might cause
service interruption.
    For more information, see /opt/netapp/lib/ontap_mediator/README
root@mediator_host:~# systemctl status ontap_mediator
● ontap_mediator.service - ONTAP Mediator
    Loaded: loaded (/etc/systemd/system/ontap_mediator.service;
enabled; preset: disabled)
    Active: active (running) since Tue 2025-07-15 16:07:29 EDT; 4min
9s ago
    Invocation: 395e9479487e4e308be2ae030c800c7f
    Process: 28745
ExecStartPre=/opt/netapp/lib/ontap_mediator/tools/otm_logs_fs.sh
(code=exited, status=0/SUCCESS)
    Main PID: 28759 (python)
    Tasks: 1 (limit: 22990)
    Memory: 66.8M (peak: 68.8M)
    CPU: 2.865s

```

```

CGroup: /system.slice/ontap_mediator.service
└─28759 /opt/netapp/lib/ontap_mediator/pyenv/bin/python
/opt/netapp/lib/ontap_mediator/ontap_mediator/server

Jul 15 16:07:29 mediator_host systemd[1]: Starting
ontap_mediator.service - ONTAP Mediator...
Jul 15 16:07:29 mediator_host systemd[1]: Started
ontap_mediator.service - ONTAP Mediator.
root@mediator_host:~# systemctl status mediator-scst
● mediator-scst.service
   Loaded: loaded (/etc/systemd/system/mediator-scst.service;
   enabled; preset: disabled)
   Active: active (running) since Tue 2025-07-15 16:07:29 EDT; 4min
  15s ago
     Invocation: f1d3be6calf9492b943e61872676f384
    Process: 28653 ExecStart=/etc/init.d/scst start (code=exited,
status=0/SUCCESS)
    Process: 28738 ExecStartPost=/usr/sbin/modprobe scst_vdisk
(code=exited, status=0/SUCCESS)
   Main PID: 28696 (iscsi-scstd)
      Tasks: 1 (limit: 22990)
     Memory: 5.2M (peak: 35.2M)
        CPU: 547ms
    CGroup: /system.slice/mediator-scst.service
           └─28696 /usr/local/sbin/iscsi-scstd

Jul 15 16:07:28 mediator_host systemd[1]: Starting mediator-
scst.service...
Jul 15 16:07:29 mediator_host iscsi-scstd[28694]: max_data_seg_len
1048576, max_queued_cmds 2048
Jul 15 16:07:29 mediator_host scst[28653]: Loading and configuring SCST
Jul 15 16:07:29 mediator_host systemd[1]: Started mediator-
scst.service.
root@mediator_host:~#

```

UEFIセキュアブートのセキュリティキーを登録する

ONTAP Mediator 1.4以降、UEFIシステムでSecure Bootメカニズムが有効になっています。Secure Bootを有効にすると、インストール後にセキュリティキーを登録するための追加手順が必要になります。

手順

1. README ファイルの指示に従って、SCST カーネルモジュールに署名します：

```

/opt/netapp/lib/ontap_mediator/ontap_mediator/SCST_mod_keys/README.module-
signing

```

2. 必要なキーを特定します。

```
/opt/netapp/lib/ontap_mediator/ontap_mediator/SCST_mod_keys
```



インストール後、システム出力に README ファイルとキーの場所が表示されます。

3. 公開鍵をMOKリストに追加します。

```
mokutil --import  
/opt/netapp/lib/ontap_mediator/ontap_mediator/SCST_mod_keys/scst_module_key.de  
r
```



秘密鍵はデフォルトの場所に置いておくことも、安全な場所に移動することもできます。公開鍵はBoot Managerが使用できるように、既存の場所に保管する必要があります。詳細については、README.module-signing ファイルをご覧ください：

```
[root@hostname ~]# ls  
/opt/netapp/lib/ontap_mediator/ontap_mediator/SCST_mod_keys/  
README.module-signing scst_module_key.der scst_module_key.priv
```

4. ホストを再起動し、デバイスのUEFI Boot Managerを使用して新しいMOKを承認します。["UEFIセキュアブートが有効になっている場合はONTAP Mediatorをインストールします"](#)の `mokutil` ユーティリティで提供されたパスフレーズが必要になります。

SCSTカーネルモジュールの署名

ONTAP Mediator をインストールした後、`systemctl status `mediator-scst`` が failed (inactive) と表示される場合は、次の手順に従って SCST カーネル モジュールに署名します。

手順

1. ビルド プロセス中に、次のコマンドを使用して

`/opt/netapp/lib/ontap_mediator/ontap_mediator/SCST_mod_keys/` ディレクトリに公開キーと秘密キーのペアが生成されます：

```
[root@mediator-host ~]# ls  
/opt/netapp/lib/ontap_mediator/ontap_mediator/SCST_mod_keys/  
README.module-signing scst_module_key.der scst_module_key.priv  
[root@mediator-host ~]#
```

2. 次のコマンドを実行して、公開キーを UEFI キー リポジトリにインポートするプロセスを開始します：

```
[root@mediator-host ~]# mokutil --import  
/opt/netapp/lib/ontap_mediator/ontap_mediator/SCST_mod_keys/scst_module_key.de  
r  
input password:  
input password again:  
  
[root@mediator-host ~]#
```

3. mokutil ソフトウェアは、インポート プロセス中にこのキーに使用する一時パスワードを要求します。

4. インポートプロセスが `mokutil --list-new` で開始されたかどうかを確認してから、システムを再起動します。ブートローダーがEFI MOKマネージャーを起動します。
5. 画面上のメニューを使用して、SCSTカーネルモジュールキーをオンにします。起動後、`systemctl status mediator-scst` を実行します。サービスが起動すると、SCSTカーネルモジュールが署名されます。

ONTAP Mediatorのインストールステータスを確認する

ONTAP Mediator をインストールした後、正常に実行されていることを確認します。

手順

1. ONTAP Mediator のステータスを表示します：

- a. `systemctl status ontap_mediator`

```
[root@scspr1915530002 ~]# systemctl status ontap_mediator

ontap_mediator.service - ONTAP Mediator
Loaded: loaded (/etc/systemd/system/ontap_mediator.service; enabled;
vendor preset: disabled)
Active: active (running) since Mon 2022-04-18 10:41:49 EDT; 1 weeks 0
days ago
Process: 286710 ExecStop=/bin/kill -s INT $MAINPID (code=exited,
status=0/SUCCESS)
Main PID: 286712 (uwsgi)
Status: "uWSGI is ready"
Tasks: 3 (limit: 49473)
Memory: 139.2M
CGroup: /system.slice/ontap_mediator.service
├─286712 /opt/netapp/lib/ontap_mediator/pyenv/bin/uwsgi --ini
/opt/netapp/lib/ontap_mediator/uwsgi/ontap_mediator.ini
├─286716 /opt/netapp/lib/ontap_mediator/pyenv/bin/uwsgi --ini
/opt/netapp/lib/ontap_mediator/uwsgi/ontap_mediator.ini
└─286717 /opt/netapp/lib/ontap_mediator/pyenv/bin/uwsgi --ini
/opt/netapp/lib/ontap_mediator/uwsgi/ontap_mediator.ini

[root@scspr1915530002 ~]#
```

- b. `systemctl status mediator-scst`


```
[root@scspr1915530002 ~]# systemctl status mediator-scst
Loaded: loaded (/etc/systemd/system/mediator-scst.service;
enabled; vendor preset: disabled)
Active: active (running) since Mon 2022-04-18 10:41:47 EDT; 1
weeks 0 days ago
Process: 286595 ExecStart=/etc/init.d/scst start (code=exited,
status=0/SUCCESS)
Main PID: 286662 (iscsi-scstd)
Tasks: 1 (limit: 49473)
Memory: 1.2M
CGroup: /system.slice/mediator-scst.service
└─286662 /usr/local/sbin/iscsi-scstd

[root@scspr1915530002 ~]#
```

2. ONTAP Mediator で使用されるポートを確認します。

netstat

```
[root@scspr1905507001 ~]# netstat -anlt | grep -E '3260|31784'

tcp        0      0 0.0.0.0:31784      0.0.0.0:*        LISTEN
tcp        0      0 0.0.0.0:3260      0.0.0.0:*        LISTEN
tcp6       0      0 :::3260           :::*             LISTEN
```

インストール後のONTAP Mediator の設定

ONTAP Mediator をインストールして実行した後、ONTAP Mediator の機能を使用するには、ONTAP ストレージ システムで追加の設定タスクを実行する必要があります。

- ONTAP Mediator をMetroCluster IP 構成で使用するには、"[MetroCluster IP設定からONTAP Mediatorを設定する](#)"を参照してください。
- SnapMirrorアクティブ同期を使用するには、"[ONTAP Mediatorをインストールし、ONTAPクラスタ構成を確認します](#)"を参照してください。

ONTAP Mediatorのセキュリティ ポリシーの設定

ONTAP Mediatorは、設定可能な複数のセキュリティ設定をサポートしています。すべての設定のデフォルト値は、`low\_space\_threshold\_mib: 10`読み取り専用ファイルで提供されています：

```
/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_mediator.user_config.yaml
```

`ontap\_mediator.user\_config.yaml`に配置されたすべての値は、デフォルト値を上書きし、すべての ONTAP Mediator アップグレードにわたって維持されます。

変更後 `ontap_mediator.user_config.yaml`、ONTAP Mediator を再起動します。

```
systemctl restart ontap_mediator
```

ONTAP Mediatorの属性の変更

このセクションで説明する ONTAP Mediator 属性は、必要に応じて変更できます。



`ontap\_mediator.config.yaml`内のその他のデフォルト値は、変更された値がONTAP Mediatorのアップグレード中に維持されないため、変更しないでください。

必要な変数を `ontap\_mediator.user\_config.yaml` ファイルにコピーしてデフォルト設定を上書きすることで、ONTAP Mediator 属性を変更します。

サードパーティのSSL証明書をインストールする

デフォルトの自己署名証明書をサードパーティの SSL 証明書に置き換える必要がある場合は、次のファイル内の特定の属性を変更します：

- `/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_mediator.config.yaml`
- `/opt/netapp/lib/ontap_mediator/uwsgi/ontap_mediator.ini`

これらのファイル内の変数は、ONTAP Mediator で使用される証明書ファイルを制御するために使用されます。

ONTAP Mediator 1.9以降

次の表にリストされているデフォルトの変数が

`/opt/netapp/lib/ontap\_mediator/ontap\_mediator/server\_config/ontap\_mediator.config.yaml` ファイルに含まれています。

変数	パス
cert_path	/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_mediator_server.crt
key_path	/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_mediator_server.key
ca_cert_path	/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/intermediate.crt
ca_key_path	/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/intermediate.key
ca_serial_path	/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/intermediate.srl
cert_valid_days	1095
x509_passin_pwd	pass:ontap

- `cert\_valid\_days` は、クライアント証明書の有効期限を設定するために使用されます。最大値は3年（1095日）です。
- x509_passin_pwd は署名されたクライアント証明書のパスフレーズです。

次の表にリストされているデフォルトの変数が `/opt/netapp/lib/ontap\_mediator/uwsgi/ontap\_mediator.ini` ファイルに含まれています。

変数	パス
mediator_cert	/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_mediator_server.crt
mediator_key	/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_mediator_server.key
ca_cert_path	/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/intermediate.crt

ONTAP Mediator 1.8 以前

次の表にリストされているデフォルトの変数が

`/opt/netapp/lib/ontap\_mediator/ontap\_mediator/server\_config/ontap\_mediator.config.yaml` ファイルに含まれています。

変数	パス
cert_path	/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_mediator_server.crt
key_path	/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_mediator_server.key
ca_cert_path	/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ca.crt
ca_key_path	/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ca.key
ca_serial_path	/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ca.srl
cert_valid_days	1095
x509_passin_pwd	pass:ontap

- `cert\_valid\_days`は、クライアント証明書の有効期限を設定するために使用されます。最大値は3年（1095日）です。
- x509_passin_pwd は署名されたクライアント証明書のパスフレーズです。

次の表にリストされているデフォルトの変数が `/opt/netapp/lib/ontap\_mediator/uwsgi/ontap\_mediator.ini` ファイルに含まれています。

変数	パス
mediator_cert	/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_mediator_server.crt
mediator_key	/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_mediator_server.key
ca_cert_path	/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ca.crt

これらの属性を変更した場合は、変更を適用するためにONTAP Mediatorを再起動してください。デフォルトの証明書をサードパーティの証明書に置き換える方法の詳細については、["自己署名証明書を信頼できるサードパーティの証明書に置き換える"](#)を参照してください。

パスワード攻撃保護

次の設定は、ブルートフォースパスワード推測攻撃に対する保護を提供します。

この機能を有効にするには、`window\_seconds`と`retry\_limit`の値を設定します。

例：

- 類推に使用できる時間を5分に設定し、5分後に失敗回数をゼロにリセットします。

```
authentication_lock_window_seconds: 300
```

- 時間内に5回失敗した場合にアカウントをロックします。

```
authentication_retry_limit: 5
```

- 各試行の拒否を遅延させることで、攻撃をスローダウンさせ、総当たりによるパスワード類推攻撃の影響を軽減します。

```
authentication_failure_delay_seconds: 5
```

```
authentication_failure_delay_seconds: 0    # seconds (float) to delay
failed auth attempts prior to response, 0 = no delay
authentication_lock_window_seconds: null    # seconds (int) since the
oldest failure before resetting the retry counter, null = no window
authentication_retry_limit: null            # number of retries to allow
before locking API access, null = unlimited
```

パスワードの複雑さのルール

次のフィールドは ONTAP Mediator API ユーザーアカウントのパスワードの複雑さのルールを制御します。

```
password_min_length: 8

password_max_length: 64

password_uppercase_chars: 0    # min. uppercase characters
password_lowercase_chars: 1    # min. lowercase character
password_special_chars: 1      # min. non-letter, non-digit
password_nonletter_chars: 2    # min. non-letter characters (digits,
specials, anything)
```

空き容量の制御

`/opt/netapp/lib/ontap\_mediator` ディスクに必要な空き容量を制御する設定があります。

スペースが設定されたしきい値を下回ると、警告イベントが発行されます。

```
low_space_threshold_mib: 10
```

予備ログスペースの制御

RESERVE_LOG_SPACE は特定の設定によって制御されます。デフォルトでは、ONTAP Mediator のインストール時にログ用に別のディスクスペースが作成されます。インストーラは ONTAP Mediator のログ記録専用として、合計 700MB のディスクスペースを持つ新しい固定サイズのファイルを作成します。

この機能を無効にしてデフォルトのディスク スペースを使用するには、以下の手順に従います。

1. 次のファイルで、RESERVE_LOG_SPACE の値を 1 から 0 に変更します：

```
/opt/netapp/lib/ontap_mediator/tools/mediator_env
```

2. Mediatorを再起動します。

- a. `cat /opt/netapp/lib/ontap_mediator/tools/mediator_env | grep "RESERVE_LOG_SPACE"`

```
RESERVE_LOG_SPACE=0
```

- b. `systemctl restart ontap_mediator`

機能を再度有効にするには、値を 0 から 1 に変更し、Mediator を再起動します。



ディスク スペースを切り替えても、既存のログはパージされません。以前のログはすべてバックアップされ、切り替えとMediatorの再起動を行ったあとに現在のディスク スペースに移動されます。

ONTAP Mediatorの管理

ONTAPメディアーターの管理（ユーザークレデンシャルの変更、サービスの停止と再有効化、ヘルスチェック、ホストメンテナンスのためのSCSTのインストールまたはアンインストールなど）を行います。また、自己署名証明書の再生成、信頼できるサードパーティ証明書への置き換え、証明書関連の問題のトラブルシューティングなど、証明書の管理も可能です。

ユーザー名を変更する

以下の手順でユーザー名を変更できます。

タスク概要

この作業は、ONTAP Mediator をインストールした Linux ホストで実行してください。

このコマンドを実行できない場合は、次の例のように完全パスを使用してコマンドを実行する必要があります。

/usr/local/bin/mediator_username

手順

次のいずれかを実行してユーザ名を変更します。

- オプション **(a)** : `mediator\_change\_user` コマンドを実行し、次の例に示すようにプロンプトに応答します :

```
[root@mediator-host ~]# mediator_change_user
Modify the Mediator API username by entering the following values:
    Mediator API User Name: mediatoradmin
    Password:
New Mediator API User Name: mediator
The account username has been modified successfully.
[root@mediator-host ~]#
```

- オプション **(b)**: 次のコマンドを実行します :

```
MEDIATOR_USERNAME=mediator MEDIATOR_PASSWORD=mediator2
MEDIATOR_NEW_USERNAME=mediatoradmin mediator_change_user
```

```
[root@mediator-host ~]# MEDIATOR_USERNAME=mediator
MEDIATOR_PASSWORD='mediator2' MEDIATOR_NEW_USERNAME=mediatoradmin
mediator_change_user
The account username has been modified successfully.
[root@mediator-host ~]#
```

パスワードの変更

以下の手順でパスワードを変更できます。

タスク概要

この作業は、ONTAP Mediator をインストールした Linux ホストで実行してください。

このコマンドを実行できない場合は、次の例のように完全パスを使用してコマンドを実行する必要があります。

/usr/local/bin/mediator_change_password

手順

次のいずれかを実行してパスワードを変更します。

- オプション **(a)** : `mediator\_change\_password` コマンドを実行し、次の例に示すようにプロンプトに応答します :

```
[root@mediator-host ~]# mediator_change_password
Change the Mediator API password by entering the following values:
  Mediator API User Name: mediatoradmin
    Old Password:
    New Password:
    Confirm Password:
The password has been updated successfully.
[root@mediator-host ~]#
```

- オプション (b): 次のコマンドを実行します：

```
MEDIATOR_USERNAME=mediatoradmin MEDIATOR_PASSWORD=mediator1
MEDIATOR_NEW_PASSWORD=mediator2 mediator_change_password
```

この例では、パスワードを「mediator1」から「mediator2」に変更しています。

```
[root@mediator-host ~]# MEDIATOR_USERNAME=mediatoradmin
MEDIATOR_PASSWORD=mediator1 MEDIATOR_NEW_PASSWORD=mediator2
mediator_change_password
The password has been updated successfully.
[root@mediator-host ~]#
```

ONTAP Mediatorを停止する

ONTAP Mediator を停止するには、次の手順を実行します：

手順

1. ONTAP Mediatorを停止します：

```
systemctl stop ontap_mediator
```

2. SCSTを停止します。

```
systemctl stop mediator-scst
```

3. ONTAP メディエーターと SCST を無効にします：

```
systemctl disable ontap_mediator mediator-scst
```

ONTAP メディエーターを再度有効にする

ONTAP Mediator を再度有効にするには、次の手順を実行します：

手順

1. ONTAP MediatorとSCSTを有効にします：


```
systemctl enable ontap_mediator mediator-scst
```

2. SCST を開始：

```
systemctl start mediator-scst
```

3. ONTAP Mediatorを起動します：

```
systemctl start ontap_mediator
```

ONTAPメディアーターが正常であることを確認する

ONTAP Mediator をインストールした後、正常に実行されていることを確認します。

手順

1. ONTAP Mediator のステータスを表示します：

a. systemctl status ontap_mediator

```
[root@scspr1915530002 ~]# systemctl status ontap_mediator

ontap_mediator.service - ONTAP Mediator
Loaded: loaded (/etc/systemd/system/ontap_mediator.service; enabled;
vendor preset: disabled)
Active: active (running) since Mon 2022-04-18 10:41:49 EDT; 1 weeks 0
days ago
Process: 286710 ExecStop=/bin/kill -s INT $MAINPID (code=exited,
status=0/SUCCESS)
Main PID: 286712 (uwsgi)
Status: "uWSGI is ready"
Tasks: 3 (limit: 49473)
Memory: 139.2M
CGroup: /system.slice/ontap_mediator.service
├─286712 /opt/netapp/lib/ontap_mediator/pyenv/bin/uwsgi --ini
/opt/netapp/lib/ontap_mediator/uwsgi/ontap_mediator.ini
├─286716 /opt/netapp/lib/ontap_mediator/pyenv/bin/uwsgi --ini
/opt/netapp/lib/ontap_mediator/uwsgi/ontap_mediator.ini
└─286717 /opt/netapp/lib/ontap_mediator/pyenv/bin/uwsgi --ini
/opt/netapp/lib/ontap_mediator/uwsgi/ontap_mediator.ini

[root@scspr1915530002 ~]#
```

b. systemctl status mediator-scst

```
[root@scspr1915530002 ~]# systemctl status mediator-scst
Loaded: loaded (/etc/systemd/system/mediator-scst.service;
enabled; vendor preset: disabled)
Active: active (running) since Mon 2022-04-18 10:41:47 EDT; 1
weeks 0 days ago
Process: 286595 ExecStart=/etc/init.d/scst start (code=exited,
status=0/SUCCESS)
Main PID: 286662 (iscsi-scstd)
Tasks: 1 (limit: 49473)
Memory: 1.2M
CGroup: /system.slice/mediator-scst.service
└─286662 /usr/local/sbin/iscsi-scstd

[root@scspr1915530002 ~]#
```

2. ONTAP Mediator で使用されるポートを確認します。

netstat

```
[root@scspr1905507001 ~]# netstat -anlt | grep -E '3260|31784'

tcp        0      0 0.0.0.0:31784        0.0.0.0:*            LISTEN
tcp        0      0 0.0.0.0:3260         0.0.0.0:*            LISTEN
tcp6       0      0 :::3260              :::*                  LISTEN
```

ONTAP Mediatorのアンインストール

必要に応じて、ONTAP Mediatorを削除できます。

開始する前に

ONTAP から ONTAP Mediator を削除する前に、切断する必要があります。

タスク概要

この作業は、ONTAP Mediator をインストールした Linux ホストで実行してください。

このコマンドを実行できない場合は、次の例のように完全パスを使用してコマンドを実行する必要があります。

```
/usr/local/bin/uninstall_ontap_mediator
```

手順

1. ONTAP Mediator をアンインストールします：

```
uninstall_ontap_mediator
```

```
[root@mediator-host ~]# uninstall_ontap_mediator

ONTAP Mediator: Self Extracting Uninstaller

+ Removing ONTAP Mediator. (Log:
/tmp/ontap_mediator.GmRGdA/uninstall_ontap_mediator/remove.log)
+ Remove successful.
[root@mediator-host ~]#
```

一時的な自己署名証明書の再生成

ONTAP Mediator 1.7 以降では、次の手順で一時的な自己署名証明書を再生成できます。



この手順は、ONTAP Mediator 1.7以降を実行しているシステムでのみサポートされます。

タスク概要

- この作業は、ONTAP Mediator をインストールした Linux ホストで実行してください。
- このタスクは、ONTAP Mediator のインストール後にホストのホスト名または IP アドレスが変更されたために、生成された自己署名証明書が古くなった場合にのみ実行できます。
- 一時的な自己署名証明書を信頼できるサードパーティの証明書に置き換えた後は、このタスクを使用して証明書を再生成し_ない_でください。自己署名証明書がない場合、この手順は失敗します。

手順

現在のホストの一時的な自己署名証明書を新たに再生成するには、以下の手順を実行します。

1. ONTAP Mediatorを再起動します：

```
./make_self_signed_certs.sh overwrite
```

```
[root@xyz000123456 ~]# cd
/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config
[root@xyz000123456 server_config]# ./make_self_signed_certs.sh overwrite

Adding Subject Alternative Names to the self-signed server certificate
#
# OpenSSL example configuration file.
Generating self-signed certificates
Generating RSA private key, 4096 bit long modulus (2 primes)
.....
.....
.....++++
.....++++
e is 65537 (0x010001)
Generating a RSA private key
.....++++
.....
.....+++
+
writing new private key to 'ontap_mediator_server.key'
-----
Signature ok
subject=C = US, ST = California, L = San Jose, O = "NetApp, Inc.", OU =
ONTAP Core Software, CN = ONTAP Mediator, emailAddress =
support@netapp.com
Getting CA Private Key
```

信頼できるサードパーティの証明書への自己署名証明書の置き換え

サポートされている場合は、自己署名証明書を信頼できるサードパーティの証明書に置き換えることができます。

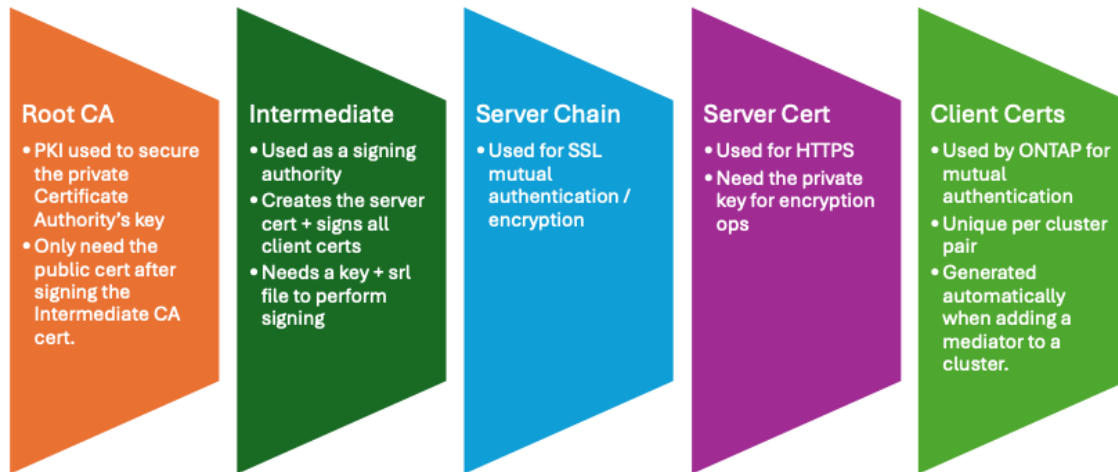


- サードパーティ証明書はONTAP 9.16.1以降およびそれ以前の一部のONTAPパッチリリースでのみサポートされます。["NetApp Bugs Online バグID CONTAP-243278"](#)を参照してください。
- サードパーティの証明書は、ONTAP Mediator 1.7以降を実行しているシステムでのみサポートされます。

タスク概要

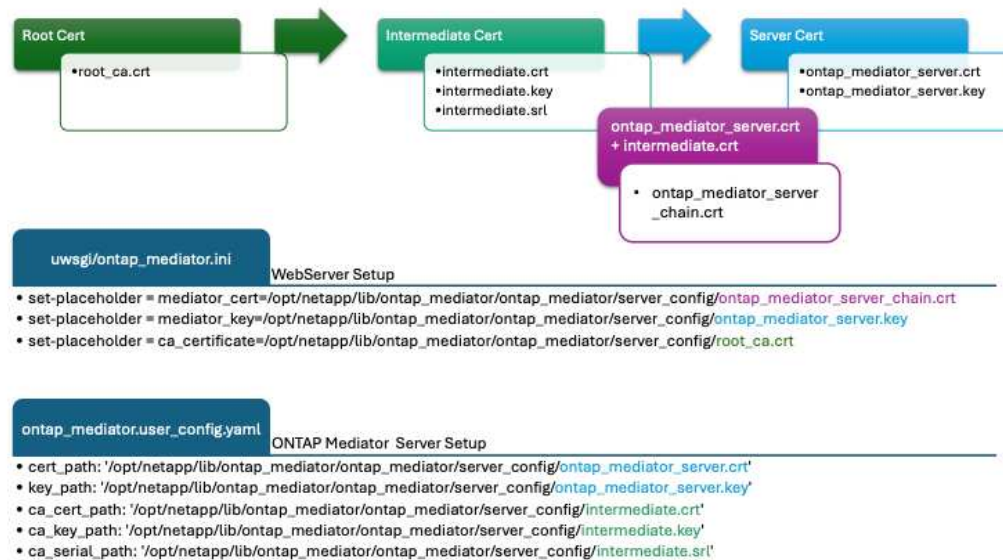
- この作業は、ONTAP Mediator をインストールした Linux ホストで実行してください。
- 生成された自己署名証明書を、信頼できる従属証明機関（CA）から取得した証明書に置き換える必要がある場合に、このタスクを実行できます。これを行うには、信頼できる公開鍵基盤（PKI）機関にアクセスする必要があります。
- 次の図は、各ONTAP Mediator証明書の目的を示しています。

ONTAP Mediator Certificate Purposes



- 次の図は、Web サーバのセットアップと ONTAP Mediator のセットアップの構成を示しています。

ONTAP Mediator Certificates



ステップ1：CA証明書を発行するサードパーティから証明書を取得する

以下の手順に従って、PKI 機関から証明書を取得できます。

次の例は、自己署名証明書アクターを `/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/` にあるサードパーティ証明書アクターに置き換える方法を示しています。



この例では、ONTAP Mediatorに必要な証明書の必要な基準を示しています。PKI認証局から証明書を取得する方法は、この手順とは異なる場合があります。ビジネスニーズに応じて手順を調整してください。

ONTAP Mediator 1.9以降

1. PKI機関が証明書を生成するために使用する秘密キー `intermediate.key` と構成ファイル `openssl\_ca.cnf` を作成します。

- a. 秘密鍵を生成します `intermediate.key` :

例

```
openssl genrsa -aes256 -out intermediate.key 4096
```

- a. 構成ファイル `openssl_ca.cnf` (`/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/openssl_ca.cnf` にあります) は、生成される証明書に必要なプロパティを定義します。

2. 秘密鍵と構成ファイルを使用して証明書署名要求を作成します `intermediate.csr` :

例 :

```
openssl req -key <private_key_name>.key -new -out  
<certificate_csr_name>.csr -config <config_file_name>.cnf
```

```
[root@scs000216655 server_config]# openssl req -key intermediate.key  
-new -config openssl_ca.cnf -out intermediate.csr  
Enter pass phrase for intermediate.key:  
[root@scs000216655 server_config]# cat intermediate.csr  
-----BEGIN CERTIFICATE REQUEST-----  
<certificate_value>  
-----END CERTIFICATE REQUEST-----
```

3. 証明書署名要求 `intermediate.csr` をPKI機関に送信して署名をもらいます。

PKI機関はリクエストを検証し、`.csr` に署名して証明書 `intermediate.crt` を生成します。さらに、PKI機関から `intermediate.crt` 証明書に署名した `root\_ca.crt` 証明書を取得する必要があります。



SnapMirrorビジネス継続性 (SM-BC) クラスタの場合は、`intermediate.crt` および `root\_ca.crt` 証明書をONTAPクラスタに追加する必要があります。["SnapMirror アクティブ同期のために ONTAP Mediator とクラスタを設定する"](#)を参照してください。

ONTAP Mediator 1.8 以前

1. PKI 機関が証明書を生成するために使用する秘密キー `ca.key` と構成ファイル `openssl\_ca.cnf` を作成します。

- a. 秘密鍵を生成します `ca.key` :

例

```
openssl genrsa -aes256 -out ca.key 4096
```

- a. 構成ファイル `openssl_ca.cnf` (`/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/openssl_ca.cnf`にあります) は、生成される証明書に必要なプロパティを定義します。

2. 秘密鍵と構成ファイルを使用して証明書署名要求を作成します `ca.csr` :

例 :

```
openssl req -key <private_key_name>.key -new -out  
<certificate_csr_name>.csr -config <config_file_name>.cnf
```

```
[root@scs000216655 server_config]# openssl req -key ca.key -new  
-config openssl_ca.cnf -out ca.csr  
Enter pass phrase for ca.key:  
[root@scs000216655 server_config]# cat ca.csr  
-----BEGIN CERTIFICATE REQUEST-----  
<certificate_value>  
-----END CERTIFICATE REQUEST-----
```

3. 証明書署名要求 `ca.csr` をPKI機関に送信して署名をもらいます。

PKI機関はリクエストを検証し、`ca.csr`に署名して証明書を生成します `ca.crt`。さらに、PKI機関から `root_ca.crt` that signed the `ca.crt` 証明書を取得する必要があります。



SnapMirrorビジネス継続性 (SM-BC) クラスタの場合は、`ca.crt` および `root_ca.crt` 証明書をONTAPクラスタに追加する必要があります。"[SnapMirror アクティブ同期のために ONTAP Mediator とクラスタを設定する](#)"を参照してください。

ステップ2: サードパーティのCA証明書で署名してサーバー証明書を生成する

ONTAP Mediator 1.9以降

サーバー証明書は、秘密鍵 `intermediate.key` とサードパーティの証明書 `intermediate.crt` によって署名されている必要があります。さらに、構成ファイル
`/opt/netapp/lib/ontap\_mediator/ontap\_mediator/server\_config/openssl\_server.cnf` には、OpenSSLによって発行されるサーバー証明書に必要なプロパティを指定する特定の属性が含まれています。

次のコマンドでサーバー証明書を生成できます。

手順

1. サーバー証明書署名要求（CSR）を生成するには、
`/opt/netapp/lib/ontap\_mediator/ontap\_mediator/server\_config` フォルダーから次のコマンドを実行します：

```
openssl req -config openssl_server.cnf -extensions v3_req -nodes -newkey  
rsa:4096 -sha512 -keyout ontap_mediator_server.key -out  
ontap_mediator_server.csr
```

2. CSR からサーバー証明書を生成するには、
`/opt/netapp/lib/ontap\_mediator/ontap\_mediator/server\_config` フォルダーから次のコマンドを実行します：



これらのファイルはPKI認証局から取得されました。異なる証明書名を使用している場合は、`intermediate.crt` と `intermediate.key` を該当するファイル名に置き換えてください。

```
openssl x509 -extfile openssl_server.cnf -extensions v3_req -CA  
intermediate.crt -CAkey intermediate.key -CAcreateserial -sha512 -days 1095  
-req -in ontap_mediator_server.csr -out ontap_mediator_server.crt
```

。`-CAcreateserial` オプションは `intermediate.srl` ファイルを生成するために使用されます。

ONTAP Mediator 1.8 以前

サーバー証明書は、秘密鍵 `ca.key` とサードパーティの証明書 `ca.crt` によって署名されている必要があります。さらに、構成ファイル
`/opt/netapp/lib/ontap\_mediator/ontap\_mediator/server\_config/openssl\_server.cnf` には、OpenSSLによって発行されるサーバー証明書に必要なプロパティを指定する特定の属性が含まれています。

次のコマンドでサーバー証明書を生成できます。

手順

1. サーバー証明書署名要求（CSR）を生成するには、
`/opt/netapp/lib/ontap\_mediator/ontap\_mediator/server\_config` フォルダーから次のコマンドを実行します：

```
openssl req -config openssl_server.cnf -extensions v3_req -nodes -newkey  
rsa:4096 -sha512 -keyout ontap_mediator_server.key -out  
ontap_mediator_server.csr
```

2. CSR からサーバー証明書を生成するには、
`/opt/netapp/lib/ontap\_mediator/ontap\_mediator/server\_config` フォルダーから次の

コマンドを実行します：



これらのファイルはPKI認証局から取得されました。異なる証明書名を使用している場合は、`ca.crt`と`ca.key`を該当するファイル名に置き換えてください。

```
openssl x509 -extfile openssl_server.cnf -extensions v3_req -CA ca.crt  
-CAkey ca.key -CAcreateserial -sha512 -days 1095 -req -in  
ontap_mediator_server.csr -out ontap_mediator_server.crt
```

° `-CAcreateserial` オプションは `ca.srl` ファイルを生成するために使用されます。

ステップ3：ONTAP Mediator構成で新しいサードパーティCA証明書とサーバ証明書を置き換える

ONTAP Mediator 1.10以降

証明書の設定は、

`/opt/netapp/lib/ontap\_mediator/ontap\_mediator/server\_config/ontap\_mediator.config.yaml`にある設定ファイルでONTAP Mediatorに提供されます。このファイルには、以下の属性が含まれます：

```
cert_path:
  '/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_mediator_server.crt'
key_path:
  '/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_mediator_server.key'
ca_cert_path:
  '/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/intermediate.crt'
ca_key_path:
  '/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/intermediate.key'
ca_serial_path:
  '/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/intermediate.srl'
```

- `cert\_path`および`key\_path`はサーバー証明書変数です。
- `ca\_cert\_path`、`ca\_key\_path`、および`ca\_serial\_path`はCA証明書変数です。

手順

1. すべての`intermediate.\*`ファイルをサードパーティの証明書に置き換えます。
2. `intermediate.crt`および`ontap\_mediator\_server.crt`証明書から証明書チェーンを作成します：

```
cat ontap_mediator_server.crt intermediate.crt >
ontap_mediator_server_chain.crt
```

3. `/opt/netapp/lib/ontap\_mediator/unicorn/config.json`ファイルを更新します。

`ssl\_keyfile`、`ssl\_certfile`、`ssl\_ca\_certs`の値を更新します：

```
ssl_keyfile:
  /opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_mediator_server.key

ssl_certfile:
  /opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_mediator_server_chain.crt

ssl_ca_certs:
```

```
/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/root_ca.crt
```

- `ssl\_keyfile` 値は `ontap\_mediator\_server.crt` ファイル内のキーパスで、`ontap\_mediator\_server.key` です。
- `ssl\_certfile` 値は `ontap\_mediator\_server\_chain.crt` ファイルのパスです。
- `ssl\_ca\_certs` 値は `root\_ca.crt` ファイルのパスです。

4. 新しく生成された証明書の次の属性が正しく設定されていることを確認します：

- Linux グループのオーナー：netapp:netapp
- Linux の権限：600

5. ONTAP Mediatorを再起動します：

```
systemctl restart ontap_mediator
```

ONTAP Mediator 1.9.1 および 1.9

証明書の設定は、

`/opt/netapp/lib/ontap\_mediator/ontap\_mediator/server\_config/ontap\_mediator.config.yaml`にある設定ファイルでONTAP Mediatorに提供されます。このファイルには、以下の属性が含まれます：

```
cert_path:
'/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_medi
ator_server.crt'
key_path:
'/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_medi
ator_server.key'
ca_cert_path:
'/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/intermedia
te.crt'
ca_key_path:
'/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/intermedia
te.key'
ca_serial_path:
'/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/intermedia
te.srl'
```

- `cert\_path` および `key\_path` はサーバー証明書変数です。
- `ca\_cert\_path`、`ca\_key\_path`、および `ca\_serial\_path` は CA 証明書変数です。

手順

1. すべての `intermediate.\*` ファイルをサードパーティの証明書に置き換えます。
2. `intermediate.crt` および `ontap\_mediator\_server.crt` 証明書から証明書チェーンを作成します：

```
cat ontap_mediator_server.crt intermediate.crt >
ontap_mediator_server_chain.crt
```

3. `/opt/netapp/lib/ontap_mediator/uwsgi/ontap_mediator.ini` ファイルを更新します。

``mediator_cert``、``mediator_key``、および
``ca_certificate`` の値を更新します：

```
set-placeholder = mediator_cert =  
/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_mediator_  
server_chain.crt
```

```
set-placeholder = mediator_key =  
/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_mediator_  
server.key
```

```
set-placeholder = ca_certificate =  
/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/root_ca.crt
```

- ``mediator_cert`` 値は ``ontap_mediator_server_chain.crt`` ファイルのパスです。
- `mediator_key value`` は ``ontap_mediator_server.crt`` ファイル内のキーパスです
``ontap_mediator_server.key``。
- ``ca_certificate`` 値は ``root_ca.crt`` ファイルのパスです。

4. 新しく生成された証明書の次の属性が正しく設定されていることを確認します：

- Linux グループのオーナー: `netapp:netapp`
- Linux の権限: `600`

5. ONTAP Mediatorを再起動します：

```
systemctl restart ontap_mediator
```

ONTAP Mediator 1.8 以前

証明書の設定は、

`/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_mediator.config.yaml` にある設定ファイルでONTAP Mediatorに提供されます。このファイルには、以下の属性が含まれます：

```
cert_path:
'/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_medi
ator_server.crt'
key_path:
'/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_medi
ator_server.key'
ca_cert_path:
'/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ca.crt'
ca_key_path:
'/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ca.key'
ca_serial_path:
'/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ca.srl'
```

- `cert\_path`および`key\_path`はサーバー証明書変数です。
- `ca\_cert\_path`、`ca\_key\_path`、および`ca\_serial\_path`はCA証明書変数です。

手順

1. すべての`ca.\*`ファイルをサードパーティの証明書に置き換えます。
2. `ca.crt`および`ontap\_mediator\_server.crt`証明書から証明書チェーンを作成します：

```
cat ontap_mediator_server.crt ca.crt > ontap_mediator_server_chain.crt
```

3. `/opt/netapp/lib/ontap\_mediator/uwsgi/ontap\_mediator.ini`ファイルを更新します。

`mediator\_cert`、`mediator\_key`、および
`ca\_certificate`の値を更新します：

```
set-placeholder = mediator_cert =
/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_mediator_
server_chain.crt
```

```
set-placeholder = mediator_key =
/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_mediator_
server.key
```

```
set-placeholder = ca_certificate =
/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/root_ca.crt
```

- `mediator\_cert`値は`ontap\_mediator\_server\_chain.crt`ファイルのパスです。
 - `mediator\_key value`は`ontap\_mediator\_server.crt`ファイル内のキーパスです
`ontap\_mediator\_server.key`。
 - `ca\_certificate`値は`root\_ca.crt`ファイルのパスです。
4. 新しく生成された証明書の次の属性が正しく設定されていることを確認します：
 - Linux グループのオーナー: netapp:netapp

◦ Linux の権限： 600

5. ONTAP Mediatorを再起動します：

```
systemctl restart ontap_mediator
```

ステップ4：オプションで、サードパーティの証明書に別のパスまたは名前を使用します

ONTAP Mediator 1.10以降

``intermediate.*``以外の別の名前でサードパーティの証明書を使用したり、別の場所に保存したりすることもできます。

手順

1. ``/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_mediator.user_config.yaml`` ファイルを設定して、``ontap_mediator.config.yaml`` ファイル内のデフォルトの変数値を上書きします。

``intermediate.crt``をPKI機関から取得し、その秘密鍵 ``intermediate.key``を ``/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config``の場所に保存する場合、
``ontap_mediator.user_config.yaml``ファイルは次の例のようになります：



``intermediate.crt``を使用して ``ontap_mediator_server.crt`` 証明書に署名した場合、
``intermediate.srl`` ファイルが生成されます。詳細については、[ステップ2：サードパーティのCA証明書で署名してサーバー証明書を生成する](#)を参照してください。


```
[root@scs000216655 server_config]# cat
ontap_mediator.user_config.yaml

# This config file can be used to override the default settings in
ontap_mediator.config.yaml
# To override a setting, copy the property key from
ontap_mediator.config.yaml to this file and
# set the property to the desired value. e.g.,
#
# The default value for 'default_mailboxes_per_target' is 4 in
ontap_mediator.config.yaml
#
# To override this value with 6 mailboxes per target, add the
following key/value pair
# below this comment:
#
# 'default_mailboxes_per_target': 6
#
cert_path:
'/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_m
ediator_server.crt'
key_path:
'/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_m
ediator_server.key'
ca_cert_path:
'/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/interme
diate.crt'
ca_key_path:
'/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/interme
diate.key'
ca_serial_path:
'/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/interme
diate.srl'
```

- a. `root\_ca.crt` 証明書が `ontap\_mediator\_server.crt` 証明書に署名する `intermediate.crt` 証明書を提
供する証明書構造を使用している場合は、`intermediate.crt` 証明書と
`ontap\_mediator\_server.crt` 証明書から証明書チェーンを作成します。



手順の早い段階で、PKI 機関から `intermediate.crt` 証明書と
`ontap\_mediator\_server.crt` 証明書を取得しておく必要があります。

```
cat ontap_mediator_server.crt intermediate.crt >
ontap_mediator_server_chain.crt
```

- b. `/opt/netapp/lib/ontap\_mediator/unicorn/config.json` ファイルを更新します。

``ssl_keyfile``、``ssl_certfile``、``ssl_ca_certs``の値を更新します：

```
ssl_keyfile:  
/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_mediator_server.key
```

```
ssl_certfile:  
/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_mediator_server_chain.crt
```

```
ssl_ca_certs:  
/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/root_ca.crt
```

- ``ssl_keyfile``値は ``ontap_mediator_server.crt`` ファイル内のキープスで、``ontap_mediator_server.key`` です。
- ``ssl_certfile``値は ``ontap_mediator_server_chain.crt`` ファイルのパスです。
- ``ssl_ca_certs``値は ``root_ca.crt`` ファイルのパスです。



SnapMirrorビジネス継続性 (SM-BC) クラスタの場合は、``intermediate.crt`` および ``root_ca.crt`` 証明書をONTAPクラスタに追加する必要があります。["SnapMirror アクティブ同期のために ONTAP Mediator とクラスタを設定する"](#)を参照してください。

c. 新しく生成された証明書の次の属性が正しく設定されていることを確認します：

- Linux グループのオーナー: `netapp:netapp`
- Linux の権限: `600`

2. 設定ファイルで証明書が更新されたら、ONTAP Mediator を再起動します。

```
systemctl restart ontap_mediator
```

ONTAP Mediator 1.9.1 および 1.9

``intermediate.*`` 以外の別の名前でサードパーティの証明書を使用したり、別の場所に保存したりすることもできます。

手順

1. ``/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_mediator.user_config.yaml`` ファイルを設定して、``ontap_mediator.config.yaml`` ファイル内のデフォルトの変数値を上書きします。

``intermediate.crt`` をPKI機関から取得し、その秘密鍵 ``intermediate.key`` を ``/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config`` の場所に保存する場合、``ontap_mediator.user_config.yaml`` ファイルは次の例のようになります：



`intermediate.crt`を使用して`ontap\_mediator\_server.crt`証明書に署名した場合、`intermediate.srl`ファイルが生成されます。詳細については、[ステップ2：サードパーティのCA証明書で署名してサーバー証明書を生成する](#)を参照してください。

```
[root@scs000216655 server_config]# cat
ontap_mediator.user_config.yaml

# This config file can be used to override the default settings in
ontap_mediator.config.yaml
# To override a setting, copy the property key from
ontap_mediator.config.yaml to this file and
# set the property to the desired value. e.g.,
#
# The default value for 'default_mailboxes_per_target' is 4 in
ontap_mediator.config.yaml
#
# To override this value with 6 mailboxes per target, add the
following key/value pair
# below this comment:
#
# 'default_mailboxes_per_target': 6
#
cert_path:
'/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_m
ediator_server.crt'
key_path:
'/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_m
ediator_server.key'
ca_cert_path:
'/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/interme
diate.crt'
ca_key_path:
'/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/interme
diate.key'
ca_serial_path:
'/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/interme
diate.srl'
```

- a. `root\_ca.crt` 証明書が`ontap\_mediator\_server.crt` 証明書に署名する`intermediate.crt` 証明書を提供する証明書構造を使用している場合は、`intermediate.crt` 証明書と`ontap\_mediator\_server.crt` 証明書から証明書チェーンを作成します。



手順の早い段階で、PKI 機関から`intermediate.crt` 証明書と`ontap\_mediator\_server.crt` 証明書を取得しておく必要があります。

```
cat ontap_mediator_server.crt intermediate.crt >
ontap_mediator_server_chain.crt
```

- b. `/opt/netapp/lib/ontap_mediator/uwsgi/ontap_mediator.ini` ファイルを更新します。

``mediator_cert``、``mediator_key``、および
``ca_certificate`` の値を更新します：

```
set-placeholder = mediator_cert =
/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_mediato
r_server_chain.crt
```

```
set-placeholder = mediator_key =
/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_mediato
r_server.key
```

```
set-placeholder = ca_certificate =
/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/root_ca.crt
```

- ``mediator_cert`` 値は ``ontap_mediator_server_chain.crt`` ファイルのパスです。
- ``mediator_key`` 値は ``ontap_mediator_server.crt`` ファイル内のキーパスで、``ontap_mediator_server.key`` です。
- ``ca_certificate`` 値は ``root_ca.crt`` ファイルのパスです。



SnapMirrorビジネス継続性 (SM-BC) クラスタの場合は、``intermediate.crt`` および ``root_ca.crt`` 証明書をONTAPクラスタに追加する必要があります。"[SnapMirror アクティブ同期のために ONTAP Mediator とクラスタを設定する](#)"を参照してください。

- c. 新しく生成された証明書の次の属性が正しく設定されていることを確認します：

- Linux グループのオーナー: `netapp:netapp`
- Linux の権限: `600`

2. 設定ファイルで証明書が更新されたら、ONTAP Mediator を再起動します。

```
systemctl restart ontap_mediator
```

ONTAP Mediator 1.8 以前

``ca.*`` 以外の別の名前でサードパーティの証明書を使用したり、別の場所に保存したりすることもできます。

手順

1. `/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_mediator.user_config.yaml`` ファイルを設定して、``ontap_mediator.config.yaml`` ファイル内のデフォルトの変数値を上書きします。

`ca.crt`をPKI機関から取得し、その秘密鍵 `ca.key`を
`/opt/netapp/lib/ontap\_mediator/ontap\_mediator/server\_config`の場所に
保存する場合、
`ontap\_mediator.user\_config.yaml`ファイルは次の例のようになります：



`ca.crt`を使用して `ontap\_mediator\_server.crt` 証明書に署名した場合、`ca.srl` ファイルが生成されます。詳細については、[ステップ2：サードパーティのCA証明書で署名してサーバー証明書を生成する](#)を参照してください。

```
[root@scs000216655 server_config]# cat
ontap_mediator.user_config.yaml

# This config file can be used to override the default settings in
ontap_mediator.config.yaml
# To override a setting, copy the property key from
ontap_mediator.config.yaml to this file and
# set the property to the desired value. e.g.,
#
# The default value for 'default_mailboxes_per_target' is 4 in
ontap_mediator.config.yaml
#
# To override this value with 6 mailboxes per target, add the
following key/value pair
# below this comment:
#
# 'default_mailboxes_per_target': 6
#
cert_path:
'/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_m
ediator_server.crt'
key_path:
'/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_m
ediator_server.key'
ca_cert_path:
'/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ca.crt'
ca_key_path:
'/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ca.key'
ca_serial_path:
'/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ca.srl'
```

- a. `root\_ca.crt` 証明書が `ontap\_mediator\_server.crt` 証明書に署名する `ca.crt` 証明書を提供する証明書構造を使用している場合は、`ca.crt` 証明書と `ontap\_mediator\_server.crt` 証明書から証明書チェーンを作成します：



手順の早い段階で、PKI 機関から `ca.crt` 証明書と `ontap\_mediator\_server.crt` 証明書を取得しておく必要があります。

```
cat ontap_mediator_server.crt ca.crt > ontap_mediator_server_chain.crt
```

b. `/opt/netapp/lib/ontap\_mediator/uwsgi/ontap\_mediator.ini` ファイルを更新します。

`mediator\_cert`、`mediator\_key`、および
`ca\_certificate` の値を更新します：

```
set-placeholder = mediator_cert =  
/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_mediator_server_chain.crt
```

```
set-placeholder = mediator_key =  
/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_mediator_server.key
```

```
set-placeholder = ca_certificate =  
/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/root_ca.crt
```

- `mediator\_cert` 値は `ontap\_mediator\_server\_chain.crt` ファイルのパスです。
- `mediator\_key` 値は `ontap\_mediator\_server.crt` ファイル内のキーパスで、`ontap\_mediator\_server.key` です。
- `ca\_certificate` 値は `root\_ca.crt` ファイルのパスです。



SnapMirrorビジネス継続性（SM-BC）クラスタの場合は、`ca.crt` および `root\_ca.crt` 証明書をONTAPクラスタに追加する必要があります。["SnapMirror アクティブ同期のために ONTAP Mediator とクラスタを設定する"](#)を参照してください。

c. 新しく生成された証明書の次の属性が正しく設定されていることを確認します：

- Linux グループのオーナー: netapp:netapp
- Linux の権限: 600

2. 設定ファイルで証明書が更新されたら、ONTAP Mediator を再起動します。

```
systemctl restart ontap_mediator
```

証明書関連の問題のトラブルシューティング

証明書の特定のプロパティを確認できます。

証明書の有効期限を確認する

証明書の有効範囲を識別するには、次のコマンドを使用します。

ONTAP Mediator 1.9以降

```
[root@mediator_host server_config]# openssl x509 -in intermediate.crt
-text -noout
Certificate:
    Data:
    ...
        Validity
            Not Before: Feb 22 19:57:25 2024 GMT
            Not After  : Feb 15 19:57:25 2029 GMT
```

ONTAP Mediator 1.8 以前

```
[root@mediator_host server_config]# openssl x509 -in ca.crt -text
-noout
Certificate:
    Data:
    ...
        Validity
            Not Before: Feb 22 19:57:25 2024 GMT
            Not After  : Feb 15 19:57:25 2029 GMT
```

CA 証明書における X509v3 拡張の検証

次のコマンドを使用して、CA 証明書の X509v3 拡張機能を検証します。

ONTAP Mediator 1.9以降

`openssl\_ca.cnf`内の `\*v3\_ca\*`で定義されたプロパティは、
`intermediate.crt`では `X509v3 extensions`として表示されます。

```
[root@mediator_host server_config]# pwd
/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config

[root@mediator_host server_config]# cat openssl_ca.cnf
...
[ v3_ca ]
subjectKeyIdentifier = hash
authorityKeyIdentifier = keyid:always,issuer
basicConstraints = critical, CA:true
keyUsage = critical, cRLSign, digitalSignature, keyCertSign

[root@mediator_host server_config]# openssl x509 -in intermediate.crt
-text -noout
Certificate:
    Data:
    ...
        X509v3 extensions:
            X509v3 Subject Key Identifier:

9F:06:FA:47:00:67:BA:B2:D4:82:70:38:B8:48:55:B5:24:DB:FC:27
            X509v3 Authority Key Identifier:

keyid:9F:06:FA:47:00:67:BA:B2:D4:82:70:38:B8:48:55:B5:24:DB:FC:27

            X509v3 Basic Constraints: critical
                CA:TRUE
            X509v3 Key Usage: critical
                Digital Signature, Certificate Sign, CRL Sign
```

ONTAP Mediator 1.8 以前

`openssl\_ca.cnf`内の `\*v3\_ca\*`で定義されたプロパティは、 `ca.crt`では
`X509v3 extensions`として表示されます。


```

[root@mediator_host server_config]# pwd
/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config

[root@mediator_host server_config]# cat openssl_ca.cnf
...
[ v3_ca ]
subjectKeyIdentifier = hash
authorityKeyIdentifier = keyid:always,issuer
basicConstraints = critical, CA:true
keyUsage = critical, cRLSign, digitalSignature, keyCertSign

[root@mediator_host server_config]# openssl x509 -in ca.crt -text
-noout
Certificate:
    Data:
    ...
        X509v3 extensions:
            X509v3 Subject Key Identifier:

9F:06:FA:47:00:67:BA:B2:D4:82:70:38:B8:48:55:B5:24:DB:FC:27
            X509v3 Authority Key Identifier:

keyid:9F:06:FA:47:00:67:BA:B2:D4:82:70:38:B8:48:55:B5:24:DB:FC:27

            X509v3 Basic Constraints: critical
                CA:TRUE
            X509v3 Key Usage: critical
                Digital Signature, Certificate Sign, CRL Sign

```

サーバー証明書とサブジェクトの代替名における **X509v3** 拡張機能を検証する

`openssl\_server.cnf`構成ファイルで定義された `v3\_req` プロパティは、証明書内で `X509v3 extensions` として表示されます。

次の例では、ONTAP Mediator がインストールされている Linux VM で `hostname -A` および `hostname -l` コマンドを実行することで、`alt\_names` セクション内の変数を取得できます。

変数の正しい値については、ネットワーク管理者に確認してください。

ONTAP Mediator 1.9以降

```
[root@mediator_host server_config]# pwd
/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config

[root@mediator_host server_config]# cat openssl_server.cnf
...
[ v3_req ]
basicConstraints          = CA:false
extendedKeyUsage          = serverAuth
keyUsage                  = keyEncipherment, dataEncipherment
subjectAltName            = @alt_names

[ alt_names ]
DNS.1 = abc.company.com
DNS.2 = abc-v6.company.com
IP.1 = 1.2.3.4
IP.2 = abcd:abcd:abcd:abcd:abcd:abcd

[root@mediator_host server_config]# openssl x509 -in intermediate.crt
-text -noout
Certificate:
    Data:
    ...

    X509v3 extensions:
        X509v3 Basic Constraints:
            CA:FALSE
        X509v3 Extended Key Usage:
            TLS Web Server Authentication
        X509v3 Key Usage:
            Key Encipherment, Data Encipherment
        X509v3 Subject Alternative Name:
            DNS:abc.company.com, DNS:abc-v6.company.com, IP
Address:1.2.3.4, IP Address:abcd:abcd:abcd:abcd:abcd:abcd
```

ONTAP Mediator 1.8 以前

```

[root@mediator_host server_config]# pwd
/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config

[root@mediator_host server_config]# cat openssl_server.cnf
...
[ v3_req ]
basicConstraints          = CA:false
extendedKeyUsage          = serverAuth
keyUsage                  = keyEncipherment, dataEncipherment
subjectAltName            = @alt_names

[ alt_names ]
DNS.1 = abc.company.com
DNS.2 = abc-v6.company.com
IP.1  = 1.2.3.4
IP.2  = abcd:abcd:abcd:abcd:abcd:abcd

[root@mediator_host server_config]# openssl x509 -in ca.crt -text
-noout
Certificate:
    Data:
    ...

        X509v3 extensions:
            X509v3 Basic Constraints:
                CA:FALSE
            X509v3 Extended Key Usage:
                TLS Web Server Authentication
            X509v3 Key Usage:
                Key Encipherment, Data Encipherment
            X509v3 Subject Alternative Name:
                DNS:abc.company.com, DNS:abc-v6.company.com, IP
                Address:1.2.3.4, IP Address:abcd:abcd:abcd:abcd:abcd:abcd

```

秘密鍵が証明書と一致していることを確認する

特定の秘密鍵が証明書と一致するかどうかを確認できます。

キーと証明書に対してそれぞれ次の OpenSSL コマンドを使用します。

ONTAP Mediator 1.9以降

```
[root@mediator_host server_config]# openssl rsa -noout -modulus -in
intermediate.key | openssl md5
Enter pass phrase for intermediate.key:
(stdin)= 14c6b98b0c7c59012b1de89eee4a9dbc
[root@mediator_host server_config]# openssl x509 -noout -modulus -in
intermediate.crt | openssl md5
(stdin)= 14c6b98b0c7c59012b1de89eee4a9dbc
```

ONTAP Mediator 1.8 以前

```
[root@mediator_host server_config]# openssl rsa -noout -modulus -in
ca.key | openssl md5
Enter pass phrase for ca.key:
(stdin)= 14c6b98b0c7c59012b1de89eee4a9dbc
[root@mediator_host server_config]# openssl x509 -noout -modulus -in
ca.crt | openssl md5
(stdin)= 14c6b98b0c7c59012b1de89eee4a9dbc
```

両方の `-modulus` 属性が一致する場合、秘密鍵と証明書のペアに互換性があり、相互に動作できることを示します。

サーバー証明書が特定のCA証明書から作成されたことを確認する

次のコマンドを使用して、サーバー証明書が特定のCA証明書から作成されていることを確認できます。

ONTAP Mediator 1.9以降

```
[root@mediator_host server_config]# openssl verify -CAfile root_ca.crt
--untrusted intermediate.crt ontap_mediator_server.crt
ontap_mediator_server.crt: OK
[root@mediator_host server_config]#
```

ONTAP Mediator 1.8 以前

```
[root@mediator_host server_config]# openssl verify -CAfile ca.crt
ontap_mediator_server.crt
ontap_mediator_server.crt: OK
```

オンライン証明書ステータス プロトコル (OCSP) 検証を使用している場合は、コマンド"[openssl-verify](#)"を使用します。

ONTAP MediatorのホストOSを保守する

最適なパフォーマンスを実現するために、ONTAP Mediator のホスト OS が定期的にメンテナンスされていることを確認してください。

ホストのリブート

クラスタが正常な状態になった場合にのみホストを再起動してください。ONTAP Mediatorがオフラインの間は、クラスタは障害に対応できません。再起動する前に、メンテナンスの時間を設定してください。

ONTAP Mediator は再起動時に自動的に再開し、ONTAP クラスタとの以前に設定された関係を再入力します。

ホスト パッケージの更新

カーネルを除くすべてのライブラリまたはyumパッケージを更新します。変更を有効にするために必要な場合は、ホストを再起動します。ホストを再起動する前に、サービスウィンドウをスケジュールします。

``yum-utils`` パッケージをインストールする場合は、``needs-restarting`` コマンドを使用して、パッケージの変更に再起動が必要かどうかを検出します。

変更はすぐには有効にならないため、ONTAP Mediator の依存関係を更新した後は再起動してください。

ホストOSカーネルをアップグレードする

SCSTは、使用しているカーネルに合わせてコンパイルする必要があります。OSをアップデートするには、メンテナンスのための時間をスケジュールする必要があります。

手順

ホスト OS カーネルをアップグレードするには、次の手順に従います。



カーネルをアップグレードする前に、OSとONTAP Mediatorのバージョンに互換性があることを確認してください。サポートされているバージョンについては、"[OSのサポート対応表](#)"を参照してください。

1. ONTAPメディアーターを停止します。
2. SCST パッケージをアンインストールします。[\[ホストのメンテナンスを実行する\]](#)を参照してください。
(SCST ではアップグレード メカニズムは提供されません。)
3. OSをアップグレードし、リブートします。
4. SCSTパッケージを再インストールします。
5. ONTAP Mediator を再度有効にします。

ホストのメンテナンスを実行する

VMカーネルをアップグレードすると、SCSTモジュールとの互換性の問題が発生する可能性があります。SCSTを手動でアンインストールし、再インストールしてください。

ステップ1：SCSTをアンインストールする

SCST をアンインストールするには、ONTAP Mediator バージョンの tar バンドルを使用します。

手順

1. 適切な SCST バンドル（次の表を参照）をダウンロードして解凍します。

このバージョンでは...	この tar バンドルを使用してください...
ONTAP Mediator 1.11	scst-3.9.tar.gz
ONTAP Mediator 1.10	scst-3.9.tar.gz
ONTAP Mediator 1.9.1	scst-3.8.0.tar.bz2
ONTAP Mediator 1.9	scst-3.8.0.tar.bz2
ONTAP Mediator 1.8	scst-3.8.0.tar.bz2
ONTAP Mediator 1.7	scst-3.7.0.tar.bz2
ONTAP Mediator 1.6	scst-3.7.0.tar.bz2
ONTAP Mediator 1.5	scst-3.6.0.tar.bz2
ONTAP Mediator 1.4	scst-3.6.0.tar.bz2
ONTAP Mediator 1.3	scst-3.5.0.tar.bz2
ONTAP Mediator 1.1	scst-3.4.0.tar.bz2
ONTAP Mediator 1.0	scst-3.3.0.tar.bz2

- a. ["SCST SourceForge ダウンロード"](#)からオープンソース パッケージにアクセスします。
 - b. *Download released versions*を選択します。
 - c. バンドルを VM に抽出します。
2. `scst`ディレクトリ内で次のアンインストール コマンドを実行します：
 - a. `systemctl stop mediator-scst`
 - b. `make scstadm_uninstall`
 - c. `make iscsi_uninstall`
 - d. `make usr_uninstall`
 - e. `make scst_uninstall`
 - f. `depmod`

ステップ2：SCSTをインストールする

SCSTを手動でインストールするには、インストールされているバージョンのONTAP Mediatorで使用されるSCST tar バンドルが必要です（[SCSTテーブル](#)[ARPテーブル](#)を参照）。



ONTAP Mediatorをインストールする前にこの手順を実行してください。使用しているSCSTのバージョンがONTAP Mediatorインストーラにバンドルされているバージョンよりも新しい場合、インストーラはこの手順をスキップします。

1. `scst`ディレクトリで次のインストールコマンドを実行します：

- a. `make 2release`
- b. `make scst_install`
- c. `make usr_install`
- d. `make iscsi_install`
- e. `make scstadm_install`
- f. `depmod`



初めてインストールを実行し、ONTAP Mediatorを事前にインストールする場合は、次の手順に進む前に次のコマンドを実行します：

```
mkdir -p  
/opt/netapp/lib/ontap_mediator/ontap_mediator/SCST_mod_keys
```

- g. `cp scst/src/certs/scst_module_key.der
/opt/netapp/lib/ontap_mediator/ontap_mediator/SCST_mod_keys/`
- h. `patch /etc/init.d/scst < /opt/netapp/lib/ontap_mediator/systemd/scst.patch`



初回インストール時にONTAP Mediatorの前にSCSTを事前にインストールする場合は、この手順をスキップしてください。インストーラによって関連するSCSTパッチが適用されます。

2. オプションとして、セキュア ブートが有効になっている場合は、再起動する前に次の手順を実行します：

- a. `scst_vdisk`、`scst`、および `iscsi_scst` モジュールの各ファイル名を決定します：

```
[root@localhost ~]# modinfo -n scst_vdisk  
[root@localhost ~]# modinfo -n scst  
[root@localhost ~]# modinfo -n iscsi_scst
```

- b. カーネルリリースを確認します：

```
[root@localhost ~]# uname -r
```

c. 各モジュール ファイルをカーネルで署名します：

```
[root@localhost ~]# /usr/src/kernels/<KERNEL-RELEASE>/scripts/sign-  
file \sha256 \  
/opt/netapp/lib/ontap_mediator/ontap_mediator/SCST_mod_keys/scst_modu  
le_key.priv \  
/opt/netapp/lib/ontap_mediator/ontap_mediator/SCST_mod_keys/scst_modu  
le_key.der \  
_module-filename_
```

d. ファームウェアとともに UEFI キーをインストールします。

UEFIキーのインストール手順については、以下を参照してください。

```
/opt/netapp/lib/ontap_mediator/ontap_mediator/SCST_mod_keys/README.module-  
signing
```

生成されたUEFIキーは次の場所に保存されます。

```
/opt/netapp/lib/ontap_mediator/ontap_mediator/SCST_mod_keys/scst_module_key.de  
r
```

3. システムを再起動します：

```
reboot
```

ホストのホスト名またはIPの変更

タスク概要

- この作業は、ONTAP Mediator をインストールした Linux ホストで実行してください。
- ONTAP Mediator をインストールした後にホスト名または IP アドレスが変更されたために自己署名証明書が有効でなくなった場合にのみ、これを実行してください。
- 一時的な自己署名証明書を信頼できるサードパーティの証明書に置き換えた後は、このタスクを使用して証明書を再生成しないでください。自己署名証明書をお持ちでない場合は、この手順は使用できません。

手順

現在のホストの一時的な自己署名証明書を作成します：

1. ONTAP Mediatorを再起動します：

```
./make_self_signed_certs.sh overwrite
```



```

[root@xyz000123456 ~]# cd
/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config
[root@xyz000123456 server_config]# ./make_self_signed_certs.sh overwrite

Adding Subject Alternative Names to the self-signed server certificate
#
# OpenSSL example configuration file.
Generating self-signed certificates
Generating RSA private key, 4096 bit long modulus (2 primes)
.....
.....
.....++++
.....++++
e is 65537 (0x010001)
Generating a RSA private key
.....++++
.....
.....+++
+
writing new private key to 'ontap_mediator_server.key'
-----
Signature ok
subject=C = US, ST = California, L = San Jose, O = "NetApp, Inc.", OU =
ONTAP Core Software, CN = ONTAP Mediator, emailAddress =
support@netapp.com
Getting CA Private Key

[root@xyz000123456 server_config]# systemctl restart ontap_mediator

```

ONTAP System ManagerによるMetroCluster IPサイト管理について学習します

MetroCluster構成では、別々の場所にある2つのONTAPクラスタ間でデータと設定を同期的にミラーリングします。ONTAP 9.8以降では、MetroCluster IP構成を管理するためのシンプルなインターフェイスとしてSystem Managerを使用できます。



System Managerを使用してMetroCluster処理を実行できるのは、MetroCluster IP構成内のみです。MetroCluster FC構成でも、System Managerを使用してMetroCluster構成内の各ノードを管理することはできませんが、MetroCluster固有の処理は実行できません。

通常は、2つの地理的に離れたサイトでMetroCluster構成の各クラスタをセットアップおよび設定します。その後、クラスタ間でデータが同期および共有されるようにピアリングをセットアップします。ピアネットワークにある2つのクラスタは、それぞれがもう一方のクラスタのソース クラスタまたはバックアップ クラスタになることで、双方向のディザスタ リカバリ（DR）を実現します。8ノードまたは4ノードMetroCluster IP

構成では、それぞれのサイトに、1つまたは2つのハイアベイラビリティ（HA）ペアを構成するストレージコントローラが含まれます。

"[ONTAP Mediatorをインストールする](#)"を第3の場所に配置して、ノードとそのDRパートナーの状態を監視できます。ONTAP Mediatorは、災害発生時にMediator-Assisted Unplanned Switchover（MAUSO）を実行できます。

計画的なメンテナンスのために一方のクラスタを停止する場合には、ネゴシエート スイッチオーバーも実行できます。メンテナンスを実施したクラスタを起動してスイッチバック処理を実行するまで、両方のクラスタのすべてのデータI/O処理がパートナー クラスタで処理されます。

System Manager を使用した MetroCluster IP 構成のセットアップと管理の手順については、"[MetroClusterのドキュメント](#)"を参照してください。

テープ バックアップを使用したデータ保護

ONTAP FlexVolボリュームのテープ バックアップについて学ぶ

ONTAPでは、Network Data Management Protocol（NDMP;ネットワーク データ管理プロトコル）を使用したテープ バックアップおよびリストアがサポートされます。NDMPを使用すると、ストレージ システム内のデータを直接テープにバックアップできるため、ネットワーク帯域幅を効率的に使用できます。ONTAPでは、テープ バックアップ用のダンプ エンジンとSMTapeエンジンの両方がサポートされます。

NDMP準拠のバックアップ アプリケーションを使用して、ダンプまたはSMTapeバックアップ / リストアを実行できます。NDMPバージョン4のみがサポートされます。

ダンプによるテープ バックアップ

ダンプは、ファイル システムのデータをテープにバックアップするSnapshotベースのバックアップです。ONTAPダンプ エンジンは、ファイル、ディレクトリ、および該当するアクセス制御リスト（ACL）情報をテープにバックアップします。ボリューム全体、qtree全体、またはボリューム全体やqtree全体ではないサブツリーをバックアップできます。ダンプは、ベースライン、差分、増分のテープ バックアップをサポートしています。

SMTapeによるテープ バックアップ

SMTapeは、データのブロックをテープにバックアップするONTAPのSnapshotベースのディザスタリカバリソリューションです。SMTapeを使用して、ボリュームのテープ バックアップを実行できます。ただし、qtreeレベルまたはサブツリーレベルでのバックアップは実行できません。SMTapeは、ベースライン、差分、増分バックアップをサポートしています。

ONTAP 9.13.1 以降では、SMTape を使用したテープ バックアップが[SnapMirrorアクティブ同期](#)でサポートされています。

ONTAPテープ バックアップとリストアのワークフロー

NDMP対応のバックアップ アプリケーションを使用して、テープ バックアップおよびリストア処理を実行できます。

タスク概要

テープ バックアップおよびリストア ワークフローでは、テープ バックアップおよびリストア処理の実行に関連するタスクの概要を示します。バックアップおよびリストア処理の実行の詳細については、バックアップ アプリケーションのマニュアルを参照してください。

手順

1. NDMPでサポートされているテープ トポロジを選択してテープ ライブラリの構成を設定します。
2. ストレージ システムでNDMPサービスを有効にします。

NDMPサービスはノード レベルまたはStorage Virtual Machine (SVM) レベルで有効にすることができます。これは、テープ バックアップおよびリストア処理を実行するために選択するNDMPモードによって異なります。

3. NDMPオプションを使用して、ストレージ システムでNDMPを管理します。

NDMPオプションはノード レベルまたはSVMレベルで使用できます。これは、テープ バックアップおよびリストア処理を実行するために選択するNDMPモードによって異なります。

NDMPオプションは、ノードレベルでは ``system services ndmp modify`` コマンドを使用して、SVMレベルでは ``vserver services ndmp modify`` コマンドを使用して変更できます。["ONTAPコマンド リファレンス"](#) の ``system services ndmp modify`` および ``vserver services ndmp modify`` の詳細を確認してください。

4. NDMP対応のバックアップ アプリケーションを使用して、テープ バックアップまたはリストア処理を実行します。

ONTAPでは、テープ バックアップおよびリストア用のダンプ エンジンとSMTapeエンジンの両方がサポートされます。

バックアップ アプリケーション (*Data Management Applications* または *DMA* と呼ばれます) を使用してバックアップまたはリストア処理を実行する方法の詳細については、バックアップ アプリケーションのドキュメントを参照してください。

関連情報

[一般的なNDMPテープ バックアップ トポロジ](#)

[FlexVol用のダンプ エンジンの概要](#)

ONTAP SMTapeおよびダンプ バックアップ エンジンの使用例

ONTAPは、SMTapeとdumpの2つのバックアップ エンジンをサポートしています。テープ バックアップおよびリストア処理を実行するバックアップ エンジンを選択する際には、SMTapeとdumpのバックアップ エンジンのユースケースを理解しておく必要があります。

ダンプは次の場合に使用できます：

- ファイルとディレクトリのDirect Access Recovery (DAR)
- 特定のパス内のサブディレクトリまたはファイルのサブセットのバックアップ
- バックアップ中に特定のファイルとディレクトリを除外する

- 長期間のバックアップの保存

SMTapeは、次の場合に使用できます：

- ディザスタ リカバリ ソリューション
- リストア処理中にバックアップ データの重複排除による削減効果と重複排除設定を維持
- 大容量ボリュームのバックアップ

テープ ドライブの管理

ONTAPテープ ドライブの管理について学ぶ

テープ バックアップまたはリストア処理を実行する前に、テープ ライブラリの接続とテープ ドライブの情報を確認できます。未認定テープ ドライブを使用するには、そのドライブを認定テープ ドライブにエミュレートする必要があります。また、既存のエイリアスを確認するだけでなく、テープ エイリアスを割り当てたり、削除したりすることもできます。

テープにデータをバックアップすると、データはテープ ファイルに格納されます。各テープ ファイルはファイル マークで区切られ、名前はありません。テープ ファイルはテープ上の位置で指定します。テープ ファイルへの書き込みには、テープ デバイスを使用します。テープ ファイルを読み取るには、書き込み時と同じ圧縮形式のデバイスを指定する必要があります。

テープ ドライブ、メディア チェンジャー、およびテープ ドライブ操作を管理するための **ONTAP** コマンド

クラスタ内のテープ ドライブとメディア チェンジャーに関する情報の表示、テープ ドライブのオンライン化とオフライン化、テープ ドライブ カートリッジ位置の変更、テープ ドライブ エイリアス名の設定とクリア、テープ ドライブのリセットを行うコマンドがあります。また、テープ ドライブ統計情報の表示とリセットも可能です。

状況	使用するコマンド
テープ ドライブをオンラインにする	<code>storage tape online</code>
テープ ドライブまたはメディア チェンジャーのエイリアス名をクリアする	<code>storage tape alias clear</code>
テープ ドライブのテープ トレース処理を有効または無効にします	<code>storage tape trace</code>
テープ ドライブのカートリッジ位置を変更する	<code>storage tape position</code>
テープ ドライブをリセットする	 このコマンドは、advanced権限レベルでのみ使用できます。 <code>storage tape reset</code>

状況	使用するコマンド
テープ ドライブまたはメディア チェンジャのエイリアス名を設定する	<code>storage tape alias set</code>
テープ ドライブをオフラインにする	<code>storage tape offline</code>
すべてのテープ ドライブとメディア チェンジャーに関する情報を表示する	<code>storage tape show</code>
クラスタに接続されているテープ ドライブに関する情報を表示します	• <code>storage tape show-tape-drive</code> • <code>system node hardware tape drive show</code>
クラスタに接続されているメディア チェンジャーに関する情報を表示します	<code>storage tape show-media-changer</code>
クラスタに接続されたテープ ドライブに関するエラー情報を表示します	<code>storage tape show-errors</code>
クラスタ内の各ノードに接続されているすべての ONTAP 認定およびサポートされているテープ ドライブを表示します	<code>storage tape show-supported-status</code>
クラスタ内の各ノードに接続されているすべてのテープ ドライブとメディア チェンジャーのエイリアスを表示します。	<code>storage tape alias show</code>
テープ ドライブの統計情報の読み取り値をゼロにリセットする	<code>storage stats tape zero tape_name</code> このコマンドはノードシェルで使用する必要があります。
ONTAPでサポートされるテープドライブを表示	<code>storage show tape supported [-v]</code> このコマンドはノードシェルで使用する必要があります。`-v`オプションを使用すると、各テープドライブの詳細を表示できます。
テープ デバイス統計情報を表示して、テープのパフォーマンスを理解し、使用パターンを確認する	<code>storage stats tape tape_name</code> このコマンドはノードシェルで使用する必要があります。

関連情報

- ["ストレージ テープ"](#)
- ["storage tape show"](#)

- "storage tape show-supported-status"
- "storage tape show-tape-drive"
- "ストレージ テープ エイリアス クリア"
- "ストレージ テープ エイリアス セット"
- "storage tape エイリアスの表示"
- "ストレージ テープ トレース"

ONTAPテープ バックアップに非認定テープ ドライブを使用する

未認定テープ ドライブで認定テープ ドライブをエミュレートできる場合は、ストレージ システムでその未認定テープ ドライブを使用できます。エミュレート後、未認定テープ ドライブは認定テープ ドライブとして扱われます。未認定テープ ドライブを使用するには、そのドライブで認定テープ ドライブのエミュレートが可能かどうかを最初に確認する必要があります。

タスク概要

未認定テープ ドライブはストレージ システムに接続されているドライブですが、ONTAPではサポートまたは認識されません。

手順

1. `storage tape show-supported-status` コマンドを使用して、ストレージ システムに接続されている非認定テープ ドライブを表示します。

次のコマンドは、ストレージ システムに接続されているテープ ドライブと、各テープ ドライブのサポートおよび認定ステータスを表示します。認定されていないテープ ドライブも表示されます。

`tape\_drive\_vendor\_name` は、ストレージ システムに接続されているものの、ONTAPではサポートされていない認定されていないテープ ドライブです。

```
cluster1::> storage tape show-supported-status -node Node1
```

Node: Node1	Is	
Tape Drive	Supported	Support Status
-----	-----	-----
"tape_drive_vendor_name"	false	Nonqualified tape drive
Hewlett-Packard C1533A	true	Qualified
Hewlett-Packard C1553A	true	Qualified
Hewlett-Packard Ultrium 1	true	Qualified
Sony SDX-300C	true	Qualified
Sony SDX-500C	true	Qualified
StorageTek T9840C	true	Dynamically Qualified
StorageTek T9840D	true	Dynamically Qualified
Tandberg LTO-2 HH	true	Dynamically Qualified

2. 認定テープ ドライブをエミュレートします。

"NetAppのダウンロード：テープ デバイスの構成ファイル"

関連情報

- [認定テープ ドライブとは](#)
- ["storage tape show-supported-status"](#)

ONTAPテープ バックアップ用にテープ ドライブまたはメディア チェンジャーにテープ エイリアスを割り当てる

テープ ドライブやメディア チェンジャーにテープ エイリアスを割り当てると、デバイスを簡単に識別できます。エイリアスを割り当てることで、バックアップ デバイスの論理名と、テープ ドライブやメディア チェンジャーに永続的に割り当てられた名前を関連付けることができます。

手順

1. ``storage tape alias set`` コマンドを使用して、テープ ドライブまたはメディア チェンジャーにエイリアスを割り当てます。

``storage tape alias set``の詳細については、[link:https://docs.netapp.com/us-en/ontap-cli/storage-tape-alias-set.html](https://docs.netapp.com/us-en/ontap-cli/storage-tape-alias-set.html)["ONTAPコマンド リファレンス"]を参照してください。

``system node hardware tape drive show`` コマンドを使用してテープ ドライブのシリアル番号 (SN) 情報を表示したり、``system node hardware tape library show`` コマンドを使用してテープ ライブラリのシリアル番号 (SN) 情報を表示したりできます。

次のコマンドは、ノードcluster1-01に接続されたシリアル番号SN[123456]L4のテープ ドライブにエイリアス名を設定します：

```
cluster-01::> storage tape alias set  -node cluster-01 -name st3  
-mapping SN[123456]L4
```

次のコマンドは、ノードcluster1-01に接続されているシリアル番号SN[65432]のメディア チェンジャーにエイリアス名を設定します：

```
cluster-01::> storage tape alias set  -node cluster-01 -name mc1  
-mapping SN[65432]
```

関連情報

- [テープのエイリアス設定 - 概要](#)

- [テープ エイリアスの削除](#)
- ["ストレージ テープ エイリアス セット"](#)

ONTAPテープ バックアップ用のテープ ドライブまたはメディア チェンジャーへのテープ エイリアスを削除します

テープ ドライブまたはメディア チェンジャーで永続的なエイリアスが不要になった場合は、`storage tape alias clear` コマンドを使用してエイリアスを削除できます。

手順

1. `storage tape alias clear` コマンドを使用して、テープ ドライブまたはメディア チェンジャーからエイリアスを削除します。

```
`storage tape alias clear`  
の詳細については、link:https://docs.netapp.com/us-en/ontap-cli/storage-tape-alias-clear.html["ONTAP コマンド リファレンス"^]を参照してください。
```

次のコマンドは、エイリアス クリア操作の範囲を `tape` に指定して、すべてのテープ ドライブのエイリアスを削除します：

```
cluster-01::>storage tape alias clear -node cluster-01 -clear-scope tape
```

終了後の操作

NDMPを使用してテープ バックアップまたはリストア処理を実行する場合は、テープ ドライブまたはメディア チェンジャーからエイリアスを削除したあとで、そのテープ ドライブまたはメディア チェンジャーに新しいエイリアス名を割り当てて、テープ デバイスに引き続きアクセスできるようにする必要があります。

関連情報

- [テープのエイリアス設定 - 概要](#)
- [テープ エイリアスの割り当て](#)
- ["ストレージ テープ エイリアス クリア"](#)

ONTAPテープ予約を有効または無効にする

```
`tape.reservations` オプションを使用して、ONTAPによるテープ  
デバイスの予約の管理方法を制御できます。デフォルトでは、テープの予約はオフになっています  
。
```

タスク概要

テープ予約オプションを有効にすると、テープ ドライブ、メディア チェンジャー、ブリッジ、またはテープ ライブラリの障害時に、問題が発生する可能性があります。tape コマンドを実行した際に、他のストレージ システムがデバイスを使用していないにもかかわらず、デバイスが予約されているというメッセージが表示される場合には、このオプションを無効にしてください。

手順

1. SCSI予約 / リリース メカニズムまたはSCSI永続的予約機能を使用するか、テープ予約機能を無効にするには、クラスタシェルで次のコマンドを入力します。

```
options -option-name tape.reservations -option-value {scsi | persistent | off}
```

scsi SCSI 予約/解放メカニズムを選択します。

persistent SCSI 永続予約を選択します。

off テープ予約を無効にします。

関連情報

テープ予約機能とは

テープ ライブラリ接続を確認するための **ONTAP** コマンド

ストレージ システムとそのストレージ システムに接続されているテープ ライブラリ構成との間の接続パスに関する情報を表示できます。この情報は、テープ ライブラリ構成への接続パスを確認する場合や、接続パスに関連する問題のトラブルシューティングを行う場合に使用します。

テープ ライブラリに関する次の詳細情報を表示して、新しいテープ ライブラリを追加 / 作成したあとや、テープ ライブラリへのシングルパス アクセスまたはマルチパス アクセスで障害が発生したパスをリストアしたあとに、テープ ライブラリの接続を確認できます。この情報は、パス関連のエラーのトラブルシューティングを行う場合や、テープ ライブラリへのアクセスが失敗した場合にも使用できます。

- テープ ライブラリの接続先のノード
- デバイスID
- NDMPパス
- テープ ライブラリ名
- ターゲット ポートとイニシエータ ポートのID
- 各ターゲット ポートまたはFCイニシエータ ポートのテープ ライブラリへのシングルパス アクセスまたはマルチパス アクセス
- 「Path Errors」や「Path Qual」などのパス関連のデータ整合性の詳細
- LUNグループとLUN数

状況	使用するコマンド
クラスタ内のテープ ライブラリに関する情報を表示する	system node hardware tape library show
テープ ライブラリのパス情報を表示する	storage tape library path show

状況	使用するコマンド
各イニシエータ ポートのテープ ライブラリのパス情報を表示する	storage tape library path show-by-initiator
ストレージのテープ ライブラリとクラスタ間の接続情報を表示する	storage tape library config show

関連情報

- ["ストレージ テープ ライブラリ構成表示"](#)
- ["system node hardware テープ ライブラリ show"](#)
- ["ストレージ テープ ライブラリ パスの表示"](#)
- ["ストレージ テープ ライブラリ パス show-by-initiator"](#)

テープ ドライブについて

認定されたONTAPテープ ドライブについて

ストレージ システムで正常に動作することがテストによって確認された認定テープ ドライブを使用する必要があります。テープのエイリアス設定に従って、さらにテープ予約機能も有効にすると、一度に1つのストレージ システムだけがテープ ドライブにアクセスできるよう制御できます。

認定テープ ドライブとは、ストレージ システムで正常に動作することがテストで確認されたテープ ドライブです。テープ構成ファイルを使用することで、既存のONTAPリリースでテープ ドライブを認定することができます。

ONTAPテープ構成ファイルの形式

テープ構成ファイルの記述形式は、テープ ドライブのベンダーID、製品ID、圧縮形式の詳細などのフィールドで構成されています。また、このファイルには、テープ ドライブの自動ロード機能を有効にしたり、テープ ドライブのコマンド タイムアウト値を変更したりするためのフィールド（省略可能）も含まれています。

次の表に、テープ構成ファイルの記述形式を示します。

項目	サイズ	概要
vendor_id (文字列)	8バイト以下	`SCSI Inquiry` コマンドによって報告されるベンダー ID。

項目	サイズ	概要
product_id (文字列)	16バイト以下	`SCSI Inquiry` コマンドによって報告される製品ID。
id_match_size (番号)		テープドライブの識別に使用される製品IDのバイト数を指定します。このバイト数は、Inquiryコマンドで表示される製品IDの最初の文字から数えます。
vendor_pretty (文字列)	16バイト以下	このパラメータが存在する場合は、コマンドによって表示される文字列で指定され、`storage tape show -device-names` それ以外の場合は INQ_VENDOR_ID が表示されます。
product_pretty (文字列)	16バイト以下	このパラメータが存在する場合は、コマンドによって表示される文字列で指定され、storage tape show -device-names、存在しない場合は INQ_PRODUCT_ID が表示されます。



`vendor\_pretty` フィールドおよび `product\_pretty` フィールドはオプションですが、いずれかのフィールドに値がある場合は、他のフィールドにも値がなければなりません。

次の表は、l、m、h、`a`などのさまざまな圧縮タイプの説明、密度コード、および圧縮アルゴリズムを示しています：

項目	サイズ	概要
`l`	m	h
a}_description=(string)`	24バイト以下	特定の密度設定の特性を説明する、ノードシェル コマンド `sysconfig -t` で印刷される文字列。
`l`	m	h

項目	サイズ	概要
a}_density=(hex codes)`		l、m、h、またはaの密度コードに対応し、SCSIモードのページブロック記述子内に設定される密度コード。
`{l	m	h
a}_algorithm=(hex codes)`		密度コードと目的の密度特性に対応し、SCSI圧縮モード ページ内に設定される圧縮アルゴリズム。

次の表に、テープ構成ファイル内の省略可能なフィールドを示します。

フィールド	概要
autoload=(Boolean yes/no)	このフィールドは yes`に設定されます（テープ ドライブに自動ローディング機能がある場合）。つまり、テープ カートリッジを挿入すると、`SCSI load (start/stopユニット) コマンドを実行しなくてもテープ ドライブが準備完了状態になります。このフィールドのデフォルトは`no`です。
cmd_timeout_0x	個々のタイムアウト値。このフィールドは、テープ ドライブのデフォルトのタイムアウト値と異なるタイムアウト値を指定する場合にのみ使用してください。サンプル ファイルには、テープ ドライブのデフォルトのSCSIコマンド タイムアウト値の一覧が記載されています。タイムアウト値は、分 (m)、秒 (s)、またはミリ秒 (ms) で指定できます。  このフィールドは変更しないでください。

テープ構成ファイルはNetApp サポート サイトからダウンロードして確認できます。

テープ構成ファイルの記述形式の例

HP LTO5 ULTRIUMテープ ドライブのテープ構成ファイルの記述形式は次のとおりです。

```

vendor_id= 「HP」

product_id= 「Ultrium 5-SCSI」

id_match_size=9

vendor_pretty= 「Hewlett-Packard」

product_pretty= 「LTO-5」

```

```
l_description=「LTO-3 (ro) /4 4/800GB」  
l_density=0x00  
l_algorithm=0x00  
m_description=「LTO-3 (ro) /4 8/1600GB cmp」  
m_density=0x00  
m_algorithm=0x01  
h_description=「LTO-5 1600GB」  
h_density=0x58  
h_algorithm=0x00  
a_description=「LTO-5 3200GB cmp」  
a_density=0x58  
a_algorithm=0x01  
autoload=「はい」
```

関連情報

- ["NetAppツール：テープ デバイス構成ファイル"](#)
- ["storage tape show"](#)

ONTAPストレージ システムがテープ ドライブを動的に認定する方法

ストレージ システムは、テープ ドライブのベンダーIDと製品IDをテープ認定テーブル内の情報と照合することによって、テープ ドライブを動的に認定します。

テープ ドライブを接続したストレージ システムでは、テープ検出で取得したベンダーIDと製品IDを内部テープ認定テーブル内の情報と照合します。一致する情報が見つかったと、そのテープ ドライブが認定ドライブとしてマークされ、ストレージ システムからそのテープ ドライブにアクセスできるようになります。一致する情報が見つからなかった場合、そのテープ ドライブは未認定のままになり、ストレージ システムからアクセスすることはできません。

テープ デバイス - 概要

ONTAPテープ デバイスについて学ぶ

テープ デバイスはテープ ドライブを表し、テープ ドライブの巻き戻しタイプと圧縮容量を組み合わせたものです。

テープ デバイスは、巻き戻しタイプと圧縮機能の組み合わせごとに作成されます。そのため、テープ ドライブまたはテープ ライブラリには複数のテープ デバイスを関連付けることができます。テープの移動、書き込

み、または読み取りを行うには、テープ デバイスを指定する必要があります。

ストレージ システムにテープ ドライブまたはテープ ライブラリを取り付けると、ONTAPによってそのテープ ドライブまたはテープ ライブラリに関連付けられたテープ デバイスが作成されます。

ONTAPはテープ ドライブとテープ ライブラリを検出し、論理番号とテープ デバイスを割り当てます。ONTAPは、ファイバ チャネル、SAS、およびパラレルSCSIテープ ドライブとライブラリがインターフェース ポートに接続されているときに検出します。ONTAPは、これらのドライブのインターフェースが有効になっているときに検出します。

ONTAPテープ デバイス名の形式

各テープ デバイスには、対応する名前が定義された形式で割り当てられています。名前には、デバイスの種類、巻き戻しタイプ、エイリアス、および圧縮タイプに関する情報が含まれています。

テープ デバイス名の形式は次のとおりです：

```
rewind_type st alias_number compression_type
```

`rewind\_type`は巻き戻しタイプです。

以下は、巻き戻しタイプの値です。

- **r**

ONTAPは、テープ ファイルの書き込みが完了するとテープを巻き戻します。

- **nr**

ONTAPは、テープ ファイルの書き込み完了後、テープを巻き戻しません。同じテープに複数のテープ ファイルを書き込む場合は、この巻き戻しタイプを使用する必要があります。

- **ur**

アンロード / リロード巻き戻しタイプです。この巻き戻しタイプを使用すると、テープ ファイルの終わりに達するとテープ ライブラリによってテープが取り出され（アンロード）、次のテープがある場合はそのテープがロードされます。

この巻き戻しタイプは、次の場合にのみ使用してください。

- このデバイスに関連付けられたテープ ドライブは、テープ ライブラリ内にあるか、ライブラリ モードのメディア チェンジャー内にあります。
- このデバイスに関連付けられたテープ ドライブは、ストレージ システムに接続されています。
- 実行している操作に十分なテープが、このテープ ドライブに定義されているライブラリ テープ シーケンスで使用可能です。



巻き戻しなしのデバイスを使用してテープに書き込みを行った場合、そのテープを読み取る前にテープを巻き戻す必要があります。

`st`はテープ ドライブの標準的な名称です。

`alias\_number`は、ONTAPがテープドライブに割り当てるエイリアスです。ONTAPが新しいテープドライブを検出すると、ONTAPはそのテープドライブにエイリアスを割り当てます。

`compression\_type`は、テープ上のデータの密度と圧縮の種類を表すドライブ固有のコードです。

次のリストは、`compression\_type`のさまざまな値について説明します。

- **a**

最高圧縮

- **h**

高圧縮

- **m**

中程度の圧縮

- **l**

低圧縮

例

`nrst0a`最高の圧縮を使用して、テープドライブ 0 上の巻き戻しなしデバイスを指定します。

テープ デバイス リストの例

以下は、HP Ultrium 2-SCSIに関連付けられたテープ デバイス リストの例です。

	Tape drive (fc202_6:2.126L1)	HP	Ultrium 2-SCSI
rst0l	- rewind device,	format is:	HP (200GB)
nrst0l	- no rewind device,	format is:	HP (200GB)
urst0l	- unload/reload device,	format is:	HP (200GB)
rst0m	- rewind device,	format is:	HP (200GB)
nrst0m	- no rewind device,	format is:	HP (200GB)
urst0m	- unload/reload device,	format is:	HP (200GB)
rst0h	- rewind device,	format is:	HP (200GB)
nrst0h	- no rewind device,	format is:	HP (200GB)
urst0h	- unload/reload device,	format is:	HP (200GB)
rst0a	- rewind device,	format is:	HP (400GB w/comp)
nrst0a	- no rewind device,	format is:	HP (400GB w/comp)
urst0a	- unload/reload device,	format is:	HP (400GB w/comp)

次のリストは、前述の例の略語について説明しています：

- GB - ギガバイト。テープの容量を示します。
- w/comp - 圧縮あり。圧縮時のテープ容量を示します。

ONTAPでは、Fibre Channel、SCSI、SASの接続を任意に組み合わせた環境において、各ストレージ システムにつき（ノードあたり）最大64個のテープ ドライブの同時接続、16台のメディア チェンジャ、および16台のブリッジまたはルータ デバイスをサポートします。

物理テープ ライブラリまたは仮想テープ ライブラリ内のデバイスやスタンドアロン デバイスをテープ ドライブまたはメディア チェンジャとして使用できます。



ストレージ システムは64個のテープ ドライブの接続を検出できますが、同時に実行できるバックアップおよびリストア セッションの最大数はバックアップ エンジンのスケーラビリティ制限によって異なります。

関連情報

[ダンプ バックアップおよびリストア セッションのスケーラビリティ制限](#)

テープのエイリアス設定

テープのエイリアス設定 - 概要

エイリアス設定を行うと、デバイスの識別が容易になります。エイリアス設定では、テープまたはメディア チェンジャの物理パス名（PPN）またはシリアル番号（SN）を、永続的かつ変更可能なエイリアス名にバインドします。

テープのエイリアス設定では、次の規則に従って、テープ ドライブ（またはテープ ライブラリやメディア チェンジャ）に常に単一のエイリアス名が関連付けられます。

シナリオ	エイリアスの再割り当て
システムのリブート時	テープ ドライブには以前のエイリアスが自動的に再割り当てされます。
テープ デバイスが別のポートに移動したとき	新しいアドレスにエイリアスを調整できます。
複数のシステムで同じテープ デバイスを使用するとき	すべてのシステムに同じエイリアスを設定できます。



Data ONTAP 8.1.xからData ONTAP 8.2.xにアップグレードすると、Data ONTAP 8.2.xのテープ エイリアス機能によって既存のテープ エイリアス名が変更されます。その場合、バックアップ アプリケーションでテープ エイリアス名の更新が必要になることがあります。

テープ エイリアスを割り当てることによって、バックアップ デバイスの論理名（st0、mc1など）と、ポート、テープ ドライブ、またはメディア チェンジャに永続的に割り当てられた名前を関連付けることができます。



st0とst00は異なる論理名です。



論理名とシリアル番号は、デバイスへのアクセスにのみ使用されます。アクセスしたあとは、デバイスのエラーメッセージはすべて物理パス名で返されます。

エイリアス設定に使用できる名前は、物理パス名とシリアル番号の2種類です。

物理パス名について

物理パス名（PPN）は、ストレージシステムに接続されているSCSI-2/3アダプタまたはスイッチ（特定の場所）に基づいて、ONTAPがテープドライブおよびテープライブラリに割り当てる数値アドレスシーケンスです。PPNは電気名とも呼ばれます。

直接接続デバイスの PPN は次の形式を使用します： `host_adapter device_id lun`



LUN 値は、LUN 値がゼロでないテープデバイスおよびメディアチェンジャーデバイスに対してのみ表示されます。つまり、LUN 値がゼロの場合、PPN の `lun` 部分は表示されません。

たとえば、PPN 8.6 はホストアダプタ番号が 8、デバイス ID が 6、論理ユニット番号（LUN）が 0 であることを示します。

SASテープデバイスも直接接続デバイスです。例えば、PPN 5c.4は、ストレージシステムにおいてSAS HBAがスロット5に接続され、SASテープがSAS HBAのポートCに接続され、デバイスIDが4であることを示します。

Fibre Channel スイッチ接続デバイスの PPN は次の形式を使用します： `switch:port_id.device_id lun`

たとえば、PPN MY_SWITCH : 5.3L2 は、MY_SWITCH というスイッチのポート 5 に接続されたテープドライブがデバイス ID 3 に設定され、LUN 2 を持っていることを示します。

LUN（論理ユニット番号）はドライブによって決まります。ファイバーチャネル、SCSIテープドライブとテープライブラリ、およびディスクにはPPNがあります。

テープドライブとライブラリのPPNは、スイッチ名の変更、テープドライブまたはライブラリの移動、またはテープドライブまたはライブラリの再構成が行われない限り変更されません。PPNは再起動後も変更されません。例えば、MY_SWITCH:5.3L2という名前のテープドライブを取り外し、同じデバイスIDとLUNを持つ新しいテープドライブをスイッチMY_SWITCHのポート5に接続した場合、新しいテープドライブはMY_SWITCH:5.3L2を使用してアクセスできます。

シリアル番号について

シリアル番号（SN）はテープドライブまたはメディアチェンジャーの一意の識別子です。ONTAPはWWNではなくSNに基づいてエイリアスを生成します。

SNはテープドライブまたはメディアチェンジャーの一意の識別子であるため、テープドライブまたはメディアチェンジャーへの接続パスが複数あっても、エイリアスは変わりません。これにより、ストレージシステムは、テープライブラリ構成内の同じテープドライブまたはメディアチェンジャーを追跡できます。

テープドライブまたはメディアチェンジャーのSNは、テープドライブまたはメディアチェンジャーが接続されているファイバチャネルスイッチの名前を変更しても変更されません。ただし、テープライブラリで既存のテープドライブを新しいテープドライブに交換すると、テープドライブのSNが変更されるため、ONTAPによって新しいエイリアスが生成されます。また、既存のテープドライブをテープライブラリ内の新しいスロットに移動したり、テープドライブのLUNを再マッピングしたりした場合も、ONTAPはそのテープドライブ

の新しいエイリアスを生成します。



新しく生成されたエイリアスを使用してバックアップ アプリケーションを更新する必要があります。

テープ デバイスのSNは次の形式を使用します： SN[xxxxxxxxxx]L[X]

`x`は英数字で、Lxはテープ デバイスのLUNです。LUNが0の場合、文字列のLx部分は表示されません。

各 SN は最大 32 文字で構成され、SN の形式では大文字と小文字は区別されません。

ONTAPマルチパス テープ アクセスを設定する際の考慮事項

ストレージ システムからテープ ライブラリ内のテープ ドライブにアクセスするための 2 つのパスを設定できます。1 つのパスに障害が発生した場合、ストレージ システムは障害が発生したパスをすぐに修復することなく、他のパスを使用してテープ ドライブにアクセスできます。これにより、テープ操作を再開できるようになります。

ストレージ システムからマルチパス テープ アクセスを構成するときは、次の点を考慮する必要があります：

- LUN マッピングをサポートするテープ ライブラリでは、LUN グループへのマルチパス アクセスのために、LUN マッピングは各パスで対称である必要があります。

テープ ドライブとメディア チェンジャーは、テープ ライブラリ内のLUNグループ（同じイニシエータ パス セットを共有するLUNのセット）に割り当てられます。LUNグループのすべてのテープ ドライブは、すべての複数のパスでバックアップおよびリストア処理に使用できる必要があります。

- ストレージ システムからテープ ライブラリ内のテープ ドライブにアクセスするために、最大 2 つのパスを設定できます。
- マルチパス テープ アクセスはロード バランシングをサポートします。ロード バランシングはデフォルトでは無効になっています。

次の例では、ストレージ システムは2つのイニシエータ パス（0bと0d）を介してLUNグループ0にアクセスしています。どちらのパスでも、LUNグループのLUN番号は0、LUN数は5です。ストレージ システムは、1つのイニシエータ パス（3d）を介してのみLUNグループ1にアクセスしています。

```
STSW-3070-2_cluster::> storage tape library config show
```

Node	LUN Group	LUN Count	Library Name	Library
Target Port	Initiator			

STSW-3070-2_cluster-01	0	5	IBM 3573-TL_1	
510a09800000412d	0b			
0d				
	1	2	IBM 3573-TL_2	
50050763124b4d6f	3d			
3 entries were displayed				

関連情報

- ["ストレージ テープ ライブラリ構成表示"](#)

ONTAPストレージ システムにテープ ドライブとテープ ライブラリを追加する方法を学びます

テープ ドライブとライブラリをストレージ システムに動的に追加できます（ストレージ システムをオフラインにする必要はありません）。

新しいメディアチェンジャーを追加すると、ストレージシステムはその存在を検出し、構成に追加します。そのメディアチェンジャーがエイリアス情報で既に参照されている場合、新しい論理名は作成されません。ライブラリが参照されていない場合、ストレージシステムはそのメディアチェンジャーの新しいエイリアスを作成します。

テープ ライブラリ構成では、ONTAPがそのターゲット ポート上のすべてのメディア チェンジャーとテープ ドライブを検出できるように、ターゲット ポートのLUN 0にテープ ドライブまたはメディア チェンジャーを構成する必要があります。

ONTAPテープ予約について学ぶ

テープ ドライブ、メディア チェンジャー、ブリッジ、テープ ライブラリなどは共有可能であるため、複数のストレージ システムからアクセスできます。テープ予約機能を利用すると、すべてのテープ ドライブ、メディア チェンジャー、ブリッジ、およびテープ ライブラリで、SCSI予約 / リリース メカニズムまたはSCSI永続的予約機能のいずれかを有効にして、一度に1つのストレージ システムだけがデバイスにアクセスするよう制御できます。



スイッチが含まれているかどうかにかかわらず、ライブラリ内のデバイスを共有するすべてのシステムでは同じ予約方法を使用する必要があります。

SCSI予約 / リリース メカニズムによるデバイス予約は、通常の状態では適切に機能します。ただし、インターフェイス エラーからのリカバリ処理中に予約内容が消失することがあります。予約内容が消失すると、予

約した所有者以外のイニシエータがデバイスにアクセスできるようになります。

SCSI永続的予約機能による予約は、ループリセットやターゲットリセットなどのエラーリカバリメカニズムには影響されません。ただし、すべてのデバイスに、適切なSCSI永続的予約機能が実装されているとは限りません。

ストレージシステム間でデータを転送する

ndmcopyを使用してONTAPデータを転送する

``ndmcopy`nodeshell` コマンドは、NDMP v4をサポートするストレージシステム間でデータを転送します。完全転送と増分転送の両方を実行できます。ボリューム、`qtree`、ディレクトリ、または個々のファイルの完全または一部を転送できます。

タスク概要

ONTAP 8.x以前のリリースでは、増分転送できるのは最大2回（フルバックアップ1回と増分バックアップ最大2回）に制限されます。

ONTAP 9.0以降のリリースでは、増分転送できるのは最大9回（フルバックアップ1回と増分バックアップ最大9回）に制限されます。

``ndmcopy`` は、ソースストレージシステムおよびデスティネーションストレージシステムのノードシェルコマンドラインで実行することも、データ転送のソースでもデスティネーションでもないストレージシステムで実行することもできます。また、``ndmcopy`` は、データ転送のソースとデスティネーションの両方である単一のストレージシステムで実行することもできます。

``ndmcopy`` コマンドでは、ソースストレージシステムおよびデスティネーションストレージシステムのIPv4またはIPv6アドレスを使用できます。パスの形式は ``/vserver_name/volume_name \[path\]`` です。

手順

1. ソースストレージシステムとデスティネーションストレージシステムで、NDMPサービスを有効にします。

ソースまたはデスティネーションでデータ転送を実行している場合...	次のコマンドを使用します...

SVMを対象としたNDMPモード	<pre>vserver services ndmp on</pre>  管理SVMのNDMP認証の場合、ユーザアカウントは <code>admin</code>、ユーザロールは <code>admin</code> または <code>`backup`</code> です。データSVMの場合、ユーザアカウントは <code>`vsadmin`</code>、ユーザロールは <code>`vsadmin`</code> または <code>`vsadmin-backup`</code> ロールです。
ノードを対象としたNDMPモード	<pre>system services ndmp on</pre>

2. ノードシェルの ``ndmpcopy`` コマンドを使用して、ストレージシステム内またはストレージシステム間でデータを転送します。

```
::> system node run -node <node_name> < ndmpcopy [options]
source_IP:source_path destination_IP:destination_path [-mcs {inet|inet6}] [-mcd {inet|inet6}] [-md {inet|inet6}]
```



`ndmpcopy`では、DNS名はサポートされません。ソースまたはデスティネーションのIPアドレスを指定する必要があります。ソースまたはデスティネーションのIPアドレスでは、ループバックアドレス（127.0.0.1）はサポートされません。

- ``ndmpcopy`` コマンドは、制御接続のアドレス モードを次のように決定します。
 - 制御接続のアドレス モードは、提供されたIPアドレスに対応します。
 - ``-mcs`` および ``-mcd`` オプションを使用して、これらのルールを上書きできます。
- ソースまたはデスティネーションがONTAPシステムの場合は、NDMPモード（ノードスコープまたはSVMスコープ）に応じて、ターゲット ボリュームへのアクセスを許可するIPアドレスを使用します。
- ``source_path`` および ``destination_path`` は、ボリューム、qtree、ディレクトリ、またはファイルの粒度レベルまでの絶対パス名です。
- ``-mcs`` ソース ストレージ システムへの制御接続に優先するアドレッシング モードを指定します。
``inet`` はIPv4アドレス モードを示し、``inet6`` はIPv6アドレス モードを示します。
- ``-mcd`` デスティネーション ストレージ システムへの制御接続に優先するアドレッシング モードを指定します。
``inet`` はIPv4アドレス モードを示し、``inet6`` はIPv6アドレス モードを示します。
- ``-md`` ソース ストレージ システムとデスティネーション ストレージ システム間のデータ転送に優先するアドレス指定モードを指定します。
``inet`` はIPv4アドレス モードを示し、``inet6`` はIPv6アドレス モードを示します。

`-md` オプションを

`ndmcopy` コマンドで使わない場合、データ接続のアドレス指定モードは次のように決定されます：

- 制御接続に指定されたアドレスのいずれかがIPv6アドレスの場合、データ接続のアドレス モードはIPv6になります。
- 制御接続に指定されたアドレスが両方ともIPv4アドレスの場合、`ndmcopy` コマンドは最初にデータ接続に対してIPv6アドレス モードを試行します。

IPv6アドレス モードで失敗した場合は、IPv4アドレス モードを使用します。



IPv6アドレスを指定する場合は、角かっこで囲む必要があります。

このサンプル コマンドは、ソース パス(source_path) からデスティネーション パス(destination_path) にデータを移行します。

```
> ndmcopy -sa admin:<ndmp_password> -da admin:<ndmp_password>
  -st md5 -dt md5 192.0.2.129:/<src_svm>/<src_vol>
192.0.2.131:/<dst_svm>/<dst_vol>
```

+

このコマンド例では、制御接続とデータ接続でIPv6アドレス モードを使用するように明示的に設定します。

```
> ndmcopy -sa admin:<ndmp_password> -da admin:<ndmp_password> -st md5
-dt md5 -mcs inet6 -mcd inet6 -md
  inet6 [2001:0db8:1:1:209:6bff:feae:6d67]:/<src_svm>/<src_vol>
[2001:0ec9:1:1:200:7cgg:gfdg:7e78]:/<dst_svm>/<dst_vol>
```

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

ndmcopy コマンドのオプション

`ndmcopy` nodeshell コマンドで使えるオプションを理解して、`link:transfer-data-ndmcopy-task.html`["データを転送する"]を正常に実行する必要があります。

次の表は、使用可能なオプションを示しています。

オプション	概要
-sa username:[password]	ソース ストレージ システムに接続するための、ソース側の認証のユーザ名とパスワードを設定します。これは必須のオプションです。 管理者権限を持たないユーザは、そのユーザに対応する、システムによって生成されたNDMP固有のパスワードを指定する必要があります。システムによって生成されたパスワードは、adminユーザとadmin以外のユーザの両方に必須です。
-da username:[password]	デスティネーション ストレージ システムに接続するための、デスティネーション側の認証のユーザ名とパスワードを設定します。これは必須のオプションです。
-st {md5	text}
このオプションは、ソース ストレージ システムに接続する際に使用するソース認証タイプを設定します。これは必須オプションであるため、ユーザーは`text`または`md5`オプションのいずれかを指定する必要があります。	-dt {md5
text}	デスティネーション ストレージ システムに接続するときに使用する、デスティネーション側の認証タイプを設定します。
-l	このオプションは、転送に使用するダンプ レベルを指定されたレベルの値に設定します。有効な値は 0、`1`から`9`です。ここで、`0`は完全転送を示し、`1`から`9`は増分転送を指定します。デフォルトは`0`です。
-d	このオプションは、ndmpcopyデバッグ ログ メッセージの生成を有効にします。ndmpcopyデバッグ ログ ファイルは`/mroot/etc/log`ルート ボリュームに保存されます。ndmpcopyデバッグ ログ ファイル名は`ndmpcopy.yyyymmdd`形式になります。
-f	このオプションは強制モードを有効にします。このモードでは、7-Modeボリュームのルートにある`etc`ディレクトリ内のシステム ファイルを上書きできます。
-h	ヘルプ メッセージが出力されます。

オプション	概要
-p	このオプションを選択すると、ソースとデスティネーションの認証用のパスワードの入力を求められます。このパスワードは`-sa`および`-da`オプションで指定されたパスワードよりも優先されます。  このオプションは、対話型コンソールでコマンドを実行する場合にのみ使用できます。
-exclude	このオプションは、データ転送用に指定されたパスから、指定されたファイルまたはディレクトリを除外します。値は`.pst`または`.txt`などのディレクトリ名またはファイル名のコンマ区切りのリストです。サポートされる除外パターンの最大数は32、サポートされる文字の最大数は255です。

FlexVolのNDMP

ONTAP FlexVolボリュームのNDMPについて学ぶ

NDMPは、ストレージ システムやテープ ライブラリなど、プライマリ ストレージ デバイスとセカンダリ ストレージ デバイスとの間で、バックアップやリカバリなどのデータ転送を制御するための標準化されたプロトコルです。

ストレージ システムでNDMPサポートを有効にすると、そのストレージ システムは、バックアップまたはリカバリ処理に参加しているNDMP対応のネットワーク接続型バックアップ アプリケーション（_Data Management Applications_ または _DMA_ と呼ばれます）、データ サーバ、およびテープ サーバと通信できるようになります。すべてのネットワーク通信はTCP/IPまたはTCP/IPv6ネットワーク経由で行われます。NDMPは、テープ ドライブとメディア チェンジャーの低レベルの制御も提供します。

ノードを対象としたNDMPモードとStorage Virtual Machine (SVM) を対象としたNDMPモードのどちらでもテープによるバックアップとリストア処理を実行できます。

NDMPを使用する際の注意事項、環境変数のリスト、およびサポートされているNDMPテープ バックアップ トポロジを把握しておく必要があります。拡張DAR機能を有効または無効にすることもできます。ONTAPでストレージ システムへのNDMPアクセス認証にサポートされている認証方式は、プレーンテキストとチャレンジの2つです。

関連情報

[ONTAPでサポートされる環境変数](#)

NDMPの動作モードについて

ONTAP NDMPの動作モードについて学ぶ

テープ バックアップ処理とリストア処理は、ノード レベルとStorage Virtual Machine (SVM) レベルのどちらで実行するかを選択できます。これらの処理をSVMレベルで正

常に実行するには、SVMでNDMPサービスを有効にする必要があります。

Data ONTAP 8.2からData ONTAP 8.3にアップグレードする場合は、8.2で使用していたNDMPの動作モードがアップグレード後も維持されます。

Data ONTAP 8.2以降で新しいクラスタをインストールする場合は、デフォルトでSVMを対象としたNDMPモードになります。ノードを対象としたNDMPモードでテープバックアップおよびリストア処理を実行するには、ノードを対象としたNDMPモードを明示的に有効にする必要があります。

ノードスコープのONTAP NDMPモードについて学ぶ

ノードを対象としたNDMPモードでは、テープバックアップおよびリストア処理をノードレベルで実行できます。Data ONTAP 8.2で使用されるNDMPの動作モードは、8.2から8.3へのアップグレード後も維持されます。

ノードを対象としたNDMPモードでは、ボリュームを所有するノードでテープバックアップおよびリストア処理を実行できます。これらの処理を実行するには、ボリュームまたはテープデバイスを所有するノードでホストされているLIFでNDMP制御接続を確立する必要があります。



このモードは非推奨となっており、今後のメジャーリリースで削除される予定です。

SVMスコープのONTAP NDMPモードについて学ぶ

NDMPサービスがStorage Virtual Machine (SVM) で有効になっている場合、テープバックアップおよびリストア処理をSVMレベルで正常に実行できます。バックアップアプリケーションでCAB拡張がサポートされている場合は、クラスタのSVMの異なるノード間でホストされているすべてのボリュームをバックアップおよびリストアできます。

NDMP制御接続は、さまざまなタイプのLIFで確立できます。SVMを対象としたNDMPモードでは、このようなLIFはデータSVMまたは管理SVMに属しています。LIFで接続を確立できるのは、そのLIFを所有するSVMでNDMPサービスが有効になっている場合だけです。

データLIFはデータSVMに属しています。クラスタ間LIF、ノード管理LIF、およびクラスタ管理LIFは管理SVMに属しています。

SVMを対象としたNDMPモードでは、バックアップおよびリストア処理に使用できるボリュームとテープデバイスは、NDMP制御接続が確立されるLIFタイプおよびCAB拡張のステータスによって異なります。バックアップアプリケーションでCAB拡張がサポートされており、ボリュームとテープデバイスが同じアフィニティを共有している場合は、3ウェイバックアップまたはリストア処理の代わりにローカルバックアップまたはリストア処理をバックアップアプリケーションで実行できます。

関連情報

[ノードを対象としたNDMPモードの管理用コマンド](#)

ONTAP NDMPサービスを使用する際の考慮事項

ストレージシステム上でNDMPサービスを開始する際の考慮事項について説明します。

- 接続されたテープドライブを使用して各ノードでサポートされるバックアップとリストアの同時実行数は、合計で最大16個までです。
- NDMPサービスでは、NDMPバックアップアプリケーションからの要求に応じてファイル履歴データを生

成できます。

バックアップ アプリケーションはファイル履歴を使用して、選択したデータのサブセットだけをバックアップ イメージから適切にリカバリします。ただし、ファイル履歴の生成と処理は、ストレージ システムとバックアップ アプリケーションの双方にとって、時間がかかり、CPUが占有される場合があります。



SMTapeでは、ファイル履歴はサポートされていません。

ディザスタ リカバリ用にデータ保護が設定されている場合（バックアップ イメージ全体がリカバリされます）は、ファイル履歴の生成を無効にしてバックアップ時間を短縮できます。NDMPのファイル履歴の生成を無効にできるかどうかについては、バックアップ アプリケーションのマニュアルを参照してください。

- すべてのLIFタイプで、NDMPのファイアウォール ポリシーがデフォルトで有効になっています。
- ノードを対象としたNDMPモードでFlexVolをバックアップするには、バックアップ アプリケーションを使用して、ボリュームを所有するノードでバックアップを開始する必要があります。

ただし、ノード ルート ボリュームをバックアップすることはできません。

- ファイアウォール ポリシーで許可されている場合は、任意のLIFからNDMPバックアップを実行できます。

データLIFを使用する場合は、フェイルオーバーに設定されたものでないLIFを選択する必要があります。NDMP処理中にデータLIFがフェイルオーバーすると、NDMP処理は失敗するため、再実行する必要があります。

- ノードを対象としたNDMPモードおよびStorage Virtual Machine (SVM) を対象としたNDMPモードでCAB拡張がサポートされていない場合、NDMPデータ接続では、NDMP制御接続と同じLIFを使用します。
- LIFを移行する際は、進行中のバックアップおよびリストア処理が中断されます。

LIFの移行が完了したあとにバックアップおよびリストア処理を開始する必要があります。

- NDMPバックアップ パスの形式は ``/vserver_name/volume_name/path_name`` です。

``path_name`` はオプションであり、ディレクトリ、ファイル、またはスナップショットのパスを指定します。

- ダンプ エンジンを使用してSnapMirrorデスティネーションをテープにバックアップする場合は、ボリューム内のデータだけがバックアップされます。

ただし、SMTapeを使用してSnapMirrorデスティネーションをテープにバックアップする場合は、メタデータもバックアップされます。SnapMirror関係および関連するメタデータはテープにバックアップされません。そのため、リストア時には、そのボリュームのデータだけがリストアされますが、関連するSnapMirror関係はリストアされません。

関連情報

[Cluster Aware Backup拡張機能の機能](#)

"システム管理"

環境変数

ONTAP NDMPでサポートされている環境変数について学習します

環境変数は、NDMP 対応バックアップ アプリケーションとストレージ システム間のバックアップまたはリストア操作に関する情報を伝達するために使用されます。

たとえば、ユーザーがバックアップ アプリケーションで `\vserver1/vol1/dir1` をバックアップするように指定した場合、バックアップ アプリケーションはFILESYSYSTEM環境変数を `\vserver1/vol1/dir1` に設定します。同様に、ユーザーがバックアップをレベル1のバックアップにするように指定した場合、バックアップ アプリケーションはLEVEL環境変数を1に設定します。



通常、環境変数の設定と確認についてバックアップ管理者の対応は不要で、バックアップ アプリケーションによって自動的に設定されます。

バックアップ管理者が環境変数を指定することはまれですが、機能やパフォーマンスの問題を特定または回避するために、バックアップ アプリケーションによって設定された環境変数の値の変更が必要になる場合があります。たとえば、パフォーマンスや機能の問題が、バックアップ アプリケーションによるファイル履歴情報の処理に起因しているかどうかを調べる場合、管理者はファイル履歴の生成を一時的に無効にすることがあります。

多くのバックアップ アプリケーションでは、環境変数を無効化または変更したり、新たに環境変数を指定したりできます。詳細については、ご使用のバックアップ アプリケーションのマニュアルを参照してください。

ONTAPでサポートされる環境変数

ONTAPは環境変数をサポートしており、環境変数にはデフォルト値が関連付けられています。ただし、これらのデフォルト値は手動で変更できます。

バックアップ アプリケーションによって設定された値を手動で変更すると、アプリケーションが予期しない動作をする可能性があります。これは、バックアップまたは復元操作がバックアップ アプリケーションの想定通りに動作しない可能性があるためです。ただし、場合によっては、適切な変更を行うことで、問題の特定や回避に役立つことがあります。

以下の表は、dumpとSMTapeで共通の動作をする環境変数と、dumpとSMTapeでのみサポートされる環境変数の一覧です。また、これらの表には、ONTAPでサポートされている環境変数を使用した場合の動作についても説明されています：



ほとんどの場合、`Y`という値を持つ変数は`T`も受け入れ、`N`も`F`を受け入れます。

ダンプとSMTapeでサポートされる環境変数

環境変数	有効な値	デフォルト	概要
DEBUG	Y または N	N	デバッグ情報を出力することを指定します。

環境変数	有効な値	デフォルト	概要
ファイルシステム	string	none	バックアップするデータのルートのパス名を指定します。
NDMP_VERSION	return_only	none	NDMP_VERSION変数は変更しないでください。バックアップ操作によって作成されるNDMP_VERSION変数は、NDMPのバージョンを返します。 ONTAPは、内部使用のため、およびバックアップアプリケーションに情報として渡すために、バックアップ中にNDMP_VERSION変数を設定します。NDMPセッションのNDMPバージョンは、この変数では設定されません。
PATHNAME_SEPARATOR	return_value	none	パス名の区切り文字を指定します。 この文字は、バックアップ対象のファイルシステムによって異なります。ONTAPの場合、この変数には文字「/」が割り当てられます。NDMPサーバはテープバックアップ処理を開始する前にこの変数を設定します。
タイプ	dump または smtape	dump	tape backupおよび復元操作を実行するためにサポートされるバックアップの種類を指定します。
詳細	Y または N	N	テープバックアップまたはリストア操作の実行中にログメッセージを増やします。

ダンプでサポートされる環境変数

環境変数	有効な値	デフォルト	概要
ACL開始	return_only	none	バックアップ操作によって作成される ACL_START 変数は、ダイレクト アクセス リストアまたは再開可能なNDMP バックアップ操作で使用されるオフセット値です。 オフセット値は、ダンプファイル内のACLデータ (Pass V) の開始位置を示すバイトオフセットで、バックアップの終了時に返されます。ダイレクトアクセスリストア操作でバックアップデータを正しくリストアするには、リストア操作の開始時にACL_START値を渡す必要があります。NDMPの再開可能なバックアップ操作では、ACL_START値を使用して、バックアップストリームの再開不可能な部分の開始位置をバックアップ アプリケーションに通知します。

環境変数	有効な値	デフォルト	概要
BASE_DATE	0、-1、または `DUMP_DATE`値	-1	増分バックアップの開始日を指定します。 `-` 1`に設定すると、BASE_DATE増分指定子は無効になります。レベル0のバックアップで</p> <p>`0`に設定すると、増分バックアップが有効になります。最初のバックアップ後、前回の増分バックアップのDUMP_DATE変数の値がBASE_DATE変数に割り当てられます。 これらの変数は、LEVEL/UPDATE ベースの増分バックアップの代替手段です。
DIRECT	Y または N	N	復元時にテーブル全体をスキャンするのではなく、ファイル データが存在するテーブル上の場所に直接早送りすることを指定します。 ダイレクトアクセスリカバリが機能するには、バックアップ アプリケーションが位置情報を提供する必要があります。この変数が `Y` に設定されている場合、バックアップ アプリケーションがファイル名またはディレクトリ名と位置情報を指定します。

環境変数	有効な値	デフォルト	概要
DMP_NAME	string	none	複数のサブツリーのバックアップの名前を指定します。 この変数は複数のサブツリーのバックアップに必須です。
DUMP_DATE	return_value	none	この変数は直接変更しないでください。BASE_DATE変数が`-1`以外の値に設定されている場合は、バックアップによって作成されます。 DUMP_DATE変数は、32ビットのレベル値をダンプソフトウェアによって計算された32ビットの時刻値の前に付加することで生成されます。レベルは、BASE_DATE変数に渡された最後のレベル値から増分されます。その結果得られた値は、以降の増分バックアップのBASE_DATE値として使用されます。

環境変数	有効な値	デフォルト	概要
拡張DARが有効	Y または N	N	拡張DAR機能を有効にするかどうかを指定します。拡張DAR機能は、ディレクトリDARとNT Streamsを使用したファイルのDARをサポートします。これによりパフォーマンスが向上します。 復元中の拡張 DAR は、次の条件が満たされている場合にのみ可能です： • ONTAPは拡張DARをサポートします。 • バックアップ中にファイル履歴が有効になっています (HIST=Y) 。 • `ndmpd.offset_map.enable` オプションは `on` に設定されています。 • 復元中に ENHANCED_DAR_ENABLED 変数が `Y` に設定されます。

環境変数	有効な値	デフォルト	概要
EXCLUDE	pattern_string	none	データのバックアップ時に除外するファイルまたはディレクトリを指定します。 除外リストは、ファイル名またはディレクトリ名をカンマで区切ったリストです。ファイル名またはディレクトリ名がリスト内のいずれかの名前と一致する場合、そのファイルはバックアップから除外されます。 除外リストに名前を指定する際には、次のルールが適用されます： • ファイルまたはディレクトリの正確な名前を使用する必要があります。 • ワイルドカード文字であるアスタリスク(*) は、文字列の最初または最後の文字である必要があります。 各文字列には最大 2 つのアスタリスクを含めることができます。 • ファイル名またはディレクトリ名のカンマの前には、バックスラッシュを付ける必要があります。 • 除外リストには最大 32 個の名前を含めることができます。

環境変数	有効な値	デフォルト	概要
EXTRACT	Y、 N、 または E	N	バックアップされたデータ セットのサブツリーを復元することを指定します。 バックアップ アプリケーションは、抽出するサブツリーの名前を指定します。指定されたファイルが、バックアップされた内容を持つディレクトリと一致する場合、そのディレクトリは再帰的に抽出されます。 DAR を使用せずにリストア中にファイル、ディレクトリ、または qtree の名前を変更するには、EXTRACT 環境変数を `E` に設定する必要があります。
EXTRACT_ACL	Y または N	Y	復元操作時にバックアップされたファイルからのACLが復元されることを指定します。 デフォルトでは、DAR (DIRECT=Y) を除き、データを復元するときにACL が復元されます。

環境変数	有効な値	デフォルト	概要
FORCE	Y または N	N	復元操作で、デスティネーション ボリューム上のボリューム スペースと inode の可用性を確認する必要があるかどうかを決定します。 この変数を `Y` に設定すると、復元操作で、宛先パス上のボリューム スペースと inode の可用性のチェックがスキップされます。 復元先ボリュームに十分なボリューム スペースまたはinodeがない場合、復元処理では、復元先ボリューム スペースとinodeの可用性に基づいて可能な限り多くのデータが復元されます。ボリューム スペースまたはinodeが利用できなくなると、復元処理は停止します。

環境変数	有効な値	デフォルト	概要
HIST	Y または N	N	ファイル履歴情報がバックアップ アプリケーションに送信されることを指定します。 ほとんどの市販バックアップ アプリケーションは、HIST変数を `Y` に設定します。バックアップ操作の速度を上げたい場合や、ファイル履歴収集に関する問題をトラブルシューティングしたい場合は、この変数を `N` に設定できます。  バックアップ アプリケーションがファイル履歴をサポートしていない場合は、HIST変数を `Y` に設定しないでください。

環境変数	有効な値	デフォルト	概要
IGNORE_CTIME	Y または N	N	前回の増分バックアップ以降にファイルの ctime 値のみが変更された場合は、ファイルが増分バックアップされないことを指定します。 ウイルス スキャン ソフトウェアなどの一部のアプリケーションは、ファイル自体やその属性が変更されていないにもかかわらず、inode 内のファイルの ctime 値を変更します。その結果、増分バックアップでは変更されていないファイルがバックアップされる可能性があります。 `IGNORE_CTIME` 変数は、ctime 値の変更によって増分バックアップに許容できないほどの時間と容量がかかる場合にのみ指定してください。
			

環境変数	有効な値	デフォルト	概要
IGNORE_QTREES	Y または N	N	復元操作で、バックアップされた qtree から qtree 情報を復元しないことを指定します。
レベル	0-31	0	バックアップ レベルを指定します。 レベル0はデータセット全体をコピーします。0より大きい値で指定される増分バックアップ レベルでは、前回の増分バックアップ以降のすべてのファイル（新規または変更されたファイル）がコピーされます。例えば、レベル1はレベル0のバックアップ以降の新規または変更されたファイルをバックアップし、レベル2はレベル1のバックアップ以降の新規または変更されたファイルをバックアップします。
LIST	Y または N	N	実際にデータを復元せずに、バックアップされたファイル名とinode番号を一覧表示します。
qtree の一覧表示	Y または N	N	実際にデータを復元せずに、バックアップされた qtree を一覧表示します。

ります：
す：

1. `IGNORE\_INCREMENTAL\_NDMP\_COPY` をボリュームレベルの incremental ndmpcopy で true に設定すると、ソース上の

環境変数	有効な値	デフォルト	概要
マルチサブツリー名	string	none	バックアップが複数のサブツリーのバックアップであることを指定します。 文字列には複数のサブツリーが指定されます。文字列は改行で区切れ、NULLで終了するサブツリー名のリストです。サブツリーは、共通のルート ディレクトリを基準とした相対パス名で指定されます。ルート ディレクトリは、リストの最後の要素として指定する必要があります。 この変数を使用する場合は、DMP_NAME 変数も使用する必要があります。
NDMP_UNICODE_FH	Y または N	N	ファイル履歴情報にファイルの NFS 名に加えて Unicode 名が含まれるように指定します。 このオプションはほとんどのバックアップ アプリケーションでは使用されません。バックアップ アプリケーションがこれらの追加ファイル名を受け取るように設計されていない限り、このオプションを設定しないでください。HIST変数も設定する必要があります。
ACLがありません	Y または N	N	データのバックアップ時に ACL をコピーしないように指定します。

CTIME`を false に設定する必要があります。

環境変数	有効な値	デフォルト	概要
非クォータ qtree	Y または N	N	データをバックアップするときに、qtree 内のファイルとディレクトリを無視する必要があることを指定します。 `Y` に設定すると、 FILESYSTEM 変数で指定されたデータセット内の qtree 内の項目はバックアップされません。この変数は、FILESYSTEM 変数でボリューム全体を指定している場合にのみ有効です。 NON_QUOTA_TREE 変数はレベル 0 のバックアップでのみ機能し、MULTI_SUBTREE_NAMES 変数が指定されている場合は機能しません。  バックアップから除外するように指定されたファイルまたはディレクトリは、NON_QUOTA_TREE を `Y` に同時に設定した場合、除外されません。
NOWRITE	Y または N	N	復元操作でディスクにデータを書き込まないように指定します。 この変数はデバッグに使用されます。

環境変数	有効な値	デフォルト	概要
再帰的	Y または N	Y	DAR 復元中にディレクトリ エントリを拡張することを指定します。 DIRECTおよびENHANCED_DAR_ENABLED環境変数も有効（`Y`に設定）にする必要があります。RECURSIVE変数が無効（`N`に設定）の場合、元のソースパスにあるすべてのディレクトリの権限とACLのみがテープから復元され、ディレクトリの内容は復元されません。RECURSIVE変数が`N`に設定されている場合、またはRECOVER_FULL_PATHS変数が`Y`に設定されている場合、リカバリパスは元のパスで終わる必要があります。  RECURSIVE変数が無効で、複数のリカバリパスが存在する場合、すべてのリカバリパスが最長のリカバリパス内に含まれている必要があります。そうでない場合は、エラーメッセージが表示されます。 たとえば、次のリカバリパスは、すべてのリカバリパスが`foo/dir1/deepdir/myfile`内にあるため、有効です： • /foo • /foo/dir

環境変数	有効な値	デフォルト	概要
フルパスのリカバリ	Y または N	N	完全なリカバリ パスで、DAR 後に権限と ACL が復元されることを指定します。 DIRECT と ENHANCED_DAR_ENABLED も有効（`Y` に設定）にする必要があります。RECOVER_FULL_PATHS が `Y` に設定されている場合、リカバリパスは元のパスで終わる必要があります。復元先ボリュームに既にディレクトリが存在する場合、それらの権限と ACL はテープから復元されません。
UPDATE	Y または N	Y	メタデータ情報を更新して、LEVEL ベースの増分バックアップを有効にします。

SM Tape でサポートされている環境変数

環境変数	有効な値	デフォルト	概要
BASE_DATE	DUMP_DATE	-1	増分バックアップの開始日を指定します。 `BASE_DATE` は、参照 Snapshot 識別子の文字列表現です。SMTape は、`BASE_DATE` 文字列を使用して参照 Snapshot を特定します。 `BASE_DATE` は、ベースラインバックアップには必要ありません。増分バックアップの場合、前回のベースラインまたは増分バックアップの`DUMP_DATE` 変数の値が`BASE_DATE` 変数に割り当てられます。 バックアップ アプリケーションは、以前の SMTape ベースラインまたは増分バックアップからの `DUMP_DATE` 値を割り当てます。

環境変数	有効な値	デフォルト	概要
DUMP_DATE	return_value	none	SMTapeバックアップの最後に、DUMP_DATEには、そのバックアップに使用されたSnapshotを識別する文字列識別子が含まれます。このSnapshotは、後続の増分バックアップの参照Snapshotとして使用できます。 DUMP_DATE の結果値は、後続の増分バックアップの BASE_DATE 値として使用されます。
SMTAPE_BACKUP_SET_ID	string	none	ベースライン バックアップに関連付けられた増分バックアップのシーケンスを識別します。 バックアップセットIDは、ベースラインバックアップ中に生成される128ビットの一意的IDです。バックアップ アプリケーションは、増分バックアップ中にこのIDを `SMTAPE_BACKUP_SET_ID` 変数への入力として割り当てます。
SMTAPE_SNAPSHOT_NAME	ボリューム内で利用可能な有効な Snapshot	Invalid	SMTAPE_SNAPSHOT_NAME 変数が Snapshot に設定されている場合、その Snapshot とその古い Snapshot がテープにバックアップされます。 増分バックアップの場合、この変数は増分スナップショットを指定します。BASE_DATE 変数はベースラインスナップショットを提供します。

環境変数	有効な値	デフォルト	概要
SMTAPE_DELETE_SNAPSHOT	Y または N	N	SMTapeによって自動的に作成されたスナップショットの場合、SMTAPE_DELETE_SNAPSHOT変数が`Y`に設定されている場合、バックアップ操作の完了後、SMTapeはこのスナップショットを削除します。ただし、バックアップアプリケーションによって作成されたスナップショットは削除されません。
SMTAPE_BREAK_MIRROR	Y または N	N	SMTAPE_BREAK_MIRROR 変数が`Y`に設定されている場合、`DP`タイプのボリュームは、復元が成功した後、`RW`ボリュームに変更されます。

一般的な**ONTAP NDMP**テープ バックアップ トポロジについて学習します。

NDMPは、バックアップ アプリケーションと、データ（ファイルシステム）を提供するストレージ システムや他のNDMPサーバ、およびテープ サービスとの間の、複数のトポロジおよび構成をサポートします。

ストレージ システム→ローカル テープ

最もシンプルな構成では、バックアップ アプリケーションがストレージ システムのデータをストレージ システムに接続されたテープ サブシステムにバックアップします。NDMP制御接続はネットワークをまたいで設定されます。ストレージ システム内のデータ サービスとテープ サービス間のNDMPデータ接続は、NDMPローカル構成と呼ばれます。

ストレージ システム→別のストレージ システムに接続されたテープ

バックアップ アプリケーションは、あるストレージ システムのデータを、別のストレージ システムに接続されたテープ ライブラリ（1つ以上のテープ ドライブを備えたメディア チェンジャ）にバックアップすることもできます。この場合、データ サービスとテープ サービス間のNDMPデータ接続は、TCPまたはTCP / IPv6 ネットワーク接続によって提供されます。これは、NDMP 3ウェイ ストレージ システム間構成と呼ばれます。

ストレージ システム→ネットワーク接続型テープ ライブラリ

NDMP対応テープ ライブラリを使用すると、また別の3ウェイ構成が可能となります。この場合、テープ ライブラリはTCP / IPネットワークに直接接続され、内蔵のNDMPサーバを通じてバックアップ アプリケーションおよびストレージ システムと通信します。

ストレージ システム→データ サーバ→テープ、またはデータ サーバ→ストレージ システム→テープ

それほど広くは使用されませんが、NDMPではストレージ システムからデータ サーバ、およびデータ サーバからストレージ システムへの3ウェイ構成もサポートされています。ストレージ システムからサーバへの構成では、ストレージ システムのデータを、バックアップ アプリケーション ホストまたは別のデータ サーバ システムに接続されたテープ ライブラリにバックアップできます。サーバからストレージ システムへの構成では、サーバのデータを、ストレージ システムに接続されたテープ ライブラリにバックアップできます。

ONTAPでサポートされるNDMP認証方式

NDMPの接続要求を許可する認証方式を指定できます。ONTAPでは、ストレージ システムへのNDMPアクセスについて、プレーンテキストおよびチャレンジの2種類の認証方式をサポートしています。

ノードを対象としたNDMPモードでは、チャレンジとプレーンテキストの両方がデフォルトで有効になっています。ただし、チャレンジを無効にすることはできません。プレーンテキストは有効または無効にすることができます。プレーンテキスト認証方式では、ログイン パスワードがクリア テキストで送信されます。

Storage Virtual Machine (SVM) を対象としたNDMPモードでは、デフォルトの認証方式はチャレンジです。ノードを対象としたNDMPモードとは異なり、このモードでは、プレーンテキストとチャレンジの両方の認証方式を有効または無効にすることができます。

関連情報

[ノードを対象としたNDMPモードでのユーザ認証](#)

[SVMを対象としたNDMPモードでのユーザ認証](#)

ONTAPでサポートされるNDMPの拡張機能

NDMP v4は、コアとなるNDMP v4プロトコルを変更することなく、NDMP v4プロトコル拡張を作成するためのメカニズムを提供します。ONTAPでサポートされているNDMP v4拡張について知っておく必要があります。

ONTAPでは、次のNDMP v4拡張機能がサポートされています：

- Cluster Aware Backup (CAB)



この拡張機能は、SVMスコープのNDMPモードでのみサポートされます。

- IPv6サポートのための接続アドレス拡張 (CAE)
- 拡張クラス 0x2050

この拡張機能は、再開可能なバックアップ操作とSnapshot Management Extensionsをサポートします。



この `NDMP\_SNAP\_RECOVER` メッセージはスナップショット管理拡張機能の一部であり、リカバリ操作を開始し、リカバリされたデータをローカルスナップショットからローカルファイルシステムの場所に転送するために使用されます。ONTAPでは、このメッセージはボリュームと通常のファイルのみのリカバリを許可します。

この `NDMP\_SNAP\_DIR\_LIST` メッセージにより、ボリュームのスナップショットを参照できます。参照操作の進行中に無停止操作が行われた場合、バックアップ アプリケーションは参照操作を再開する必要があります。

• NDMP再開可能バックアップ拡張機能

NDMP再開可能バックアップ拡張機能（RBE）機能を使用すると、障害発生前のデータ ストリーム内の既知のチェックポイントからバックアップを再開できます。

ONTAP NDMPの拡張DAR機能について学ぶ

拡張Direct Access Recovery（DAR）機能は、ディレクトリのDAR、およびファイルとNTストリームのDARに使用できます。デフォルトでは、拡張DAR機能は有効になっています。

拡張DAR機能を有効にすると、オフセット マップを作成してテープに書き込む必要があるため、バックアップのパフォーマンスに影響を及ぼす可能性があります。拡張DARは、ノードを対象としたNDMPモードとStorage Virtual Machine（SVM）を対象としたNDMPモードの両方で有効または無効にすることができます。

ONTAP NDMPセッションのスケーラビリティ制限

システムメモリ容量が異なるストレージ システムでは、同時に確立できるNDMPセッションの最大数に注意する必要があります。この最大数は、ストレージ システムのシステム メモリによって異なります。

以下の表に記載されている制限は、NDMPサーバーに関するものです。「ダンプ バックアップおよびリストア セッションのスケーラビリティ制限」セクションに記載されている制限は、ダンプおよびリストア セッションに関するものです。

ダンプ バックアップおよびリストア セッションのスケーラビリティ制限

ストレージ システムのシステム メモリ	NDMPセッションの最大数
16GB未満	8
16GB以上24GB未満	20
24GB以上	36

ストレージ システムのシステム メモリは、`sysconfig -a` コマンド（nodeshellから使用可能）を使用して取得できます。`sysconfig -a`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。

ONTAP FlexGroupボリュームでのNDMPサポートについて学ぶ

ONTAP 9.7以降では、FlexGroupボリュームでNDMPがサポートされます。

ONTAP 9.7以降では、ndmpcopyコマンドを使用してFlexVolとFlexGroupボリュームの間でデータを転送できます。

ONTAP 9.7から以前のバージョンにリバートした場合、以前の転送の差分転送情報は保持されないため、リバート後にベースライン コピーを実行する必要があります。

ONTAP 9.8以降では、FlexGroupボリュームで次のNDMP機能がサポートされます。

- 拡張クラス0x2050のNDMP_SNAP_RECOVERメッセージは、FlexGroupボリューム内の個別ファイルのリカバリに使用できます。
- FlexGroupボリュームでは、NDMPのRestartable Backup Extension（RBE）がサポートされます。
- FlexGroupボリュームでは、環境変数EXCLUDEおよびMULTI_SUBTREE_NAMESがサポートされます。

ONTAP SnapLockボリュームを使用したNDMPについて学ぶ

規制対象データのコピーを複数作成すると冗長なリカバリ シナリオが実現し、NDMPダンプおよびリストアを使用することにより、ソース ファイルのWrite Once Read Many（WORM）特性をSnapLockボリュームでも維持できます。

SnapLockボリューム内のファイルのWORM属性はデータのバックアップ、リストア、およびコピー時に保持されますが、WORM属性が適用されるのはSnapLockボリュームへのリストア時のみです。SnapLockからSnapLock以外のボリュームにバックアップをリストアした場合、WORM属性は維持されますが無視され、ONTAPでは適用されません。

FlexVolのノードを対象としたNDMPモードの管理

FlexVolボリュームの **ONTAP** ノードスコープ **NDMP** モードの管理について学習します

NDMPオプションとコマンドを使用して、ノードレベルでNDMPを管理できます。
`options` コマンドを使用してNDMPオプションを変更できます。テープ バックアップおよびリストア操作を実行するには、ストレージシステムにアクセスするためのNDMP固有の認証情報を使用する必要があります。

`options`の詳細については、link:<https://docs.netapp.com/us-en/ontap-cli/search.html?q=options>["ONTAPコマンド リファレンス"]を参照してください。

ONTAP ノード スコープ **NDMP** モードを管理するためのコマンド

`system services ndmp`コマンドを使用して、ノード レベルでNDMPを管理できます。これらのコマンドの一部は廃止予定であり、今後のメジャーリリースで削除されます。

次の NDMP コマンドは、高度な権限レベルでのみ使用できます：

- `system services ndmp service terminate`
- `system services ndmp service start`
- `system services ndmp service stop`
- `system services ndmp log start`
- `system services ndmp log stop`

状況	使用するコマンド
NDMPサービスを有効にする	<code>system services ndmp on*</code>
NDMPサービスを無効にする	<code>system services ndmp off*</code>
NDMP 構成を表示する	<code>system services ndmp show*</code>
NDMP設定を変更する	<code>system services ndmp modify*</code>
デフォルトのNDMPバージョンを表示する	<code>system services ndmp version*</code>
NDMPサービス設定を表示する	<code>system services ndmp service show</code>
NDMPサービス設定を変更する	<code>system services ndmp service modify</code>
すべてのNDMPセッションを表示する	<code>system services ndmp status</code>
すべてのNDMPセッションに関する詳細情報を表示します	<code>system services ndmp probe</code>
指定されたNDMPセッションを終了する	<code>system services ndmp kill</code>
すべてのNDMPセッションを終了する	<code>system services ndmp kill-all</code>
NDMPパスワードを変更する	<code>system services ndmp password*</code>
ノードを対象としたNDMPモードを有効にする	<code>system services ndmp node-scope-mode on*</code>
ノードスコープのNDMPモードを無効にする	<code>system services ndmp node-scope-mode off*</code>
ノードを対象としたNDMPモードのステータスを表示する	<code>system services ndmp node-scope-mode status*</code>

状況	使用するコマンド
すべてのNDMPセッションを強制的に終了する	<code>system services ndmp service terminate</code>
NDMPサービス デーモンを開始する	<code>system services ndmp service start</code>
NDMPサービス デーモンを停止します	<code>system services ndmp service stop</code>
指定したNDMPセッションのロギングを開始する	<code>system services ndmp log start*</code>
指定したNDMPセッションのロギングを停止する	<code>system services ndmp log stop*</code>

- これらのコマンドは非推奨となっており、今後のメジャー リリースで削除される予定です。

`system services ndmp`の詳細については、link:<https://docs.netapp.com/us-en/ontap-cli/search.html?q=system+services+ndmp>["ONTAPコマンド リファレンス"^]を参照してください。

ノードを対象とした**NDMP**モードでのユーザ認証

ノードを対象としたNDMPモードでは、テープ バックアップおよびリストア処理を実行するために、NDMP 固有のクレデンシャルを使用してストレージ システムにアクセスする必要があります。

デフォルトのユーザIDは「root」です。ノードでNDMPを使用する前に、NDMPユーザに関連付けられているデフォルトのNDMPパスワードを変更する必要があります。デフォルトのNDMPユーザIDを変更することもできます。

関連情報

[ノードを対象としたNDMPモードの管理用コマンド](#)

[ノードを対象としたNDMPモードとは](#)

FlexVolのSVMを対象としたNDMPモードの管理

FlexVolボリュームのONTAP SVMスコープNDMPモードの管理について学習します

NDMPオプションとコマンドを使用することで、SVMごとにNDMPを管理できます。NDMPオプションは `vserver services ndmp modify` コマンドを使用して変更できます。SVMを対象としたNDMPモードでは、ユーザ認証がロールベース アクセス制御メカニズムに統合されています。

``vserver modify`` コマンドを使用して、NDMPを許可または禁止するプロトコルリストに追加できます。デフォルトでは、NDMPは許可されるプロトコルリストに含まれています。NDMPを禁止するプロトコルリストに追加すると、NDMPセッションを確立できなくなります。

``-preferred-interface-role`` オプションを使用すると、NDMPデータ接続を確立するLIFのタイプを制御できます。NDMPデータ接続の確立時に、NDMPはこのオプションで指定されたLIFタイプに属するIPアドレスを選択します。IPアドレスがこれらのLIFタイプのいずれにも属していない場合、NDMPデータ接続を確立できません。link:<https://docs.netapp.com/us-en/ontap-cli/vserver-services-ndmp-modify.html>["ONTAPコマンド リファレンス"]の ``vserver services ndmp modify`` の詳細をご覧ください。

ONTAP SVMスコープのNDMPモードを管理するためのコマンド

``vserver services ndmp`` コマンドを使用して、各Storage Virtual Machine (SVM、旧Vserver) でNDMPを管理できます。

状況	使用するコマンド
NDMPサービスを有効にする	<code>vserver services ndmp on</code>  NDMPサービスは、クラスタ内のすべてのノードで常に有効にする必要があります。<code>`system services ndmp on`</code> コマンドを使用して、ノードでNDMPサービスを有効にできます。デフォルトでは、NDMPサービスはノードで常に有効になっています。
NDMPサービスを無効にする	<code>vserver services ndmp off</code>
NDMP 構成を表示する	<code>vserver services ndmp show</code>
NDMP設定を変更する	<code>vserver services ndmp modify</code>
デフォルトのNDMPバージョンを表示する	<code>vserver services ndmp version</code>
すべてのNDMPセッションを表示する	<code>vserver services ndmp status</code>
すべてのNDMPセッションに関する詳細情報を表示します	<code>vserver services ndmp probe</code>

状況	使用するコマンド
指定されたNDMPセッションを終了する	<code>vserver services ndmp kill</code>
すべてのNDMPセッションを終了する	<code>vserver services ndmp kill-all</code>
NDMPパスワードを生成する	<code>vserver services ndmp generate-password</code>
NDMPの拡張機能のステータスを表示する	<code>vserver services ndmp extensions show</code> このコマンドは、advanced権限レベルで使用できません。
NDMPの拡張機能のステータスを変更（有効または無効に）する	<code>vserver services ndmp extensions modify</code> このコマンドは、advanced権限レベルで使用できません。
指定したNDMPセッションのロギングを開始する	<code>vserver services ndmp log start</code> このコマンドは、advanced権限レベルで使用できません。
指定したNDMPセッションのロギングを停止する	<code>vserver services ndmp log stop</code> このコマンドは、advanced権限レベルで使用できません。

`vserver services ndmp`の詳細については、[link:https://docs.netapp.com/us-en/ontap-cli/search.html?q=vserver+services+ndmp](https://docs.netapp.com/us-en/ontap-cli/search.html?q=vserver+services+ndmp)["ONTAPコマンドリファレンス"]をご覧ください。

関連情報

[SVMを対象としたNDMPモードの管理用コマンド](#)

[Cluster Aware Backup拡張機能の機能](#)

[SVMを対象としたNDMPモードとは](#)

["システム管理"](#)

ONTAP NDMP の Cluster Aware Backup 拡張機能について学ぶ

CAB（Cluster Aware Backup）は、NDMP v4プロトコルの機能拡張です。この機能拡張により、NDMPサーバは、ボリリュームを所有するノードでデータ接続を確立できます。また、ボリリュームとテープ デバイスがクラスタ内の同じノードに配置されているかどうか

かをバックアップ アプリケーションが判断できます。

NDMPサーバがボリュームを所有するノードを特定し、そのノードでデータ接続を確立できるようにするには、バックアップ アプリケーションでCAB拡張がサポートされている必要があります。CAB拡張を使用する場合、バックアップ アプリケーションは、データ接続を確立する前に、バックアップまたはリストア対象のボリュームについてNDMPサーバに通知する必要があります。これにより、NDMPサーバはボリュームをホストするノードを特定して、適切にデータ接続を確立できます。

バックアップ アプリケーションでCAB拡張がサポートされている場合は、ボリュームとテープ デバイスに関するアフィニティ情報がNDMPサーバから提供されます。ボリュームとテープ デバイスがクラスタ内の同じノードに配置されている場合、バックアップ アプリケーションではこのアフィニティ情報を使用して、3ウェイ バックアップの代わりにローカル バックアップを実行できます。

さまざまなLIFタイプでのバックアップとリストアのためのONTAPボリュームとテープデバイスの可用性

バックアップ アプリケーションは、クラスタ内のあらゆるタイプのLIF上にNDMP制御接続を確立するように設定できます。Storage Virtual Machine (SVM) を対象としたNDMPモードではLIFタイプとCAB拡張のステータスに応じて、バックアップおよびリストア処理に使用できるボリュームとテープ デバイスが決まります。

次の表は、NDMP制御接続のLIFタイプとCAB拡張のステータスに応じた、使用可能なボリュームとテープ デバイスの一覧です。

使用可能なボリュームとテープ デバイス：バックアップ アプリケーションでCAB拡張がサポートされていない場合

NDMP制御接続LIFタイプ	バックアップまたはリストアに使用できるボリューム	バックアップまたはリストアに使用できるテープ デバイス
ノード管理LIF	ノードによってホストされるすべてのボリューム	ノード管理LIFをホストしているノードに接続されているテープ デバイス
Data LIF	データLIFをホストしているノードでホストされているSVMに属するボリュームのみ	なし
クラスタ管理LIF	クラスタ管理LIFをホストするノードによってホストされるすべてのボリューム	なし
クラスタ間LIF	クラスタ間LIFをホストするノードによってホストされるすべてのボリューム	クラスタ間LIFをホストするノードに接続されたテープ デバイス

使用可能なボリュームとテープ デバイス：バックアップ アプリケーションでCAB拡張がサポートされている場合

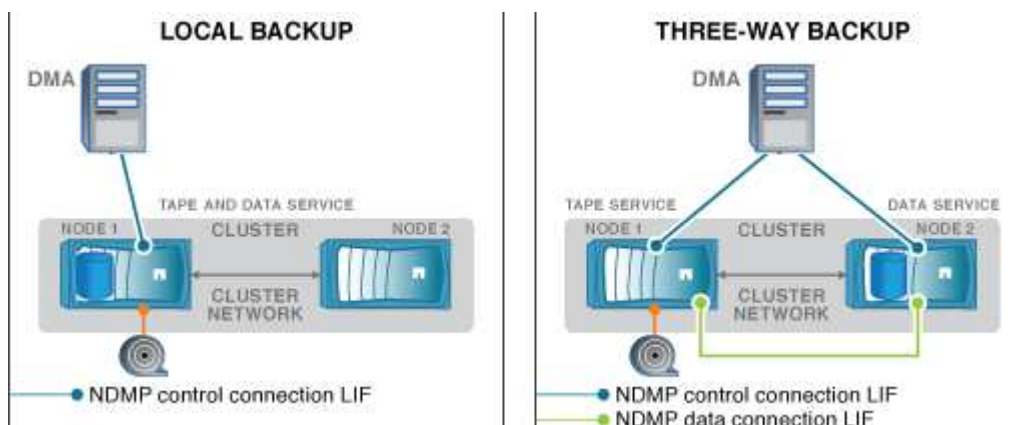
NDMP制御接続LIFタイプ	バックアップまたはリストアに使用できるボリューム	バックアップまたはリストアに使用できるテープ デバイス
ノード管理LIF	ノードによってホストされるすべてのボリューム	ノード管理LIFをホストしているノードに接続されているテープ デバイス
Data LIF	データLIFをホストしているSVMに属するすべてのボリューム	なし
クラスタ管理LIF	クラスタ内のすべてのボリューム	クラスタ内のすべてのテープ デバイス
クラスタ間LIF	クラスタ内のすべてのボリューム	クラスタ内のすべてのテープ デバイス

ONTAP NDMPのアフィニティ情報について学ぶ

CAB対応のバックアップ アプリケーションには、ボリュームとテープ デバイスに関する一意の位置情報がNDMPサーバから提供されます。このアフィニティ情報を使用して、ボリュームとテープ デバイスのアフィニティが同じ場合、バックアップ アプリケーションは3ウェイ バックアップではなくローカル バックアップを実行できます。

NDMP制御接続がノード管理LIF、クラスタ管理LIF、またはクラスタ間LIF上に確立されている場合、バックアップ アプリケーションは、このアフィニティ情報を使用してボリュームとテープ デバイスが同じノードに配置されているかどうかを判断し、ローカル バックアップ、3ウェイ バックアップ、またはリストア処理のいずれかを実行できます。NDMP制御接続がデータLIF上に確立されている場合、バックアップ アプリケーションは常に3ウェイ バックアップを実行します。

ローカルのNDMPバックアップと3ウェイのNDMPバックアップ



DMA（バックアップ アプリケーション）は、ボリュームとテープ デバイスのアフィニティ情報を使用して、クラスタ内のノード1にあるボリュームとテープ デバイスに対してローカルのNDMPバックアップを実行します。ボリュームがノード1からノード2に移動すると、ボリュームとテープ デバイスのアフィニティ情報が変わります。そのため、その後のバックアップについては、DMAは3ウェイのNDMPバックアップ処理を実行します。これにより、ボリュームが別のノードに移動しても、ボリュームのバックアップ ポリシーが維持されます。

NDMPサーバは、**SVM**を対象としたモードでセキュアな**ONTAP**制御接続をサポートします

セキュアソケット（SSL/TLS）を通信メカニズムとして使用することで、データ管理アプリケーション（DMA）とNDMPサーバー間の安全な制御接続を確立できます。このSSL通信はサーバー証明書に基づいています。NDMPサーバーはポート30000（IANAによって「ndmps」サービス用に割り当てられたポート）をリッスンします。

このポートでクライアントからの接続が確立されると、標準のSSLハンドシェイクが実行され、サーバがクライアントに証明書を提示します。クライアントが証明書を受け入れると、SSLハンドシェイクが完了します。このプロセスが完了すると、クライアントとサーバ間のすべての通信が暗号化されます。NDMPプロトコルのワークフローはこれまでとまったく同じです。セキュアNDMP接続では、サーバ側の証明書認証のみが必要です。DMAは、セキュアNDMPサービスまたは標準NDMPサービスに接続して接続を確立することを選択できます。

デフォルトでは、Storage Virtual Machine（SVM）のセキュアNDMPサービスは無効になっています。``vserver services ndmp modify -vserver vserver -is-secure-control-connection-enabled [true|false]`` コマンドを使用して、特定のSVMでセキュアNDMPサービスを有効または無効にすることができます。

NDMP ONTAPデータ接続タイプ

Storage Virtual Machine（SVM）を対象としたNDMPモードでは、サポート対象のNDMPデータ接続タイプは、NDMP制御接続のLIFタイプおよびCAB拡張のステータスによって異なります。このNDMPデータ接続タイプは、ローカルまたは3ウェイNDMPバックアップ / リストア処理を実行できるかどうかを示します。

TCPまたはTCP / IPv6ネットワーク経由で3ウェイNDMPバックアップまたはリストア処理を実行できます。次の表は、NDMP制御接続のLIFタイプおよびCAB拡張のステータスに基づくNDMPデータ接続タイプを示しています。

NDMPデータ接続タイプ（CAB拡張がバックアップ アプリケーションでサポートされている場合）

NDMP制御接続LIFタイプ	NDMPデータ接続タイプ
ノード管理LIF	ローカル、TCP、TCP / IPv6
Data LIF	TCP、TCP / IPv6
クラスタ管理LIF	ローカル、TCP、TCP / IPv6
クラスタ間LIF	ローカル、TCP、TCP / IPv6

NDMPデータ接続タイプ（CAB拡張がバックアップ アプリケーションでサポートされていない場合）

NDMP制御接続LIFタイプ	NDMPデータ接続タイプ
ノード管理LIF	ローカル、TCP、TCP / IPv6
Data LIF	TCP、TCP / IPv6
クラスタ管理LIF	TCP、TCP / IPv6
クラスタ間LIF	ローカル、TCP、TCP / IPv6

関連情報

[Cluster Aware Backup拡張機能の機能](#)

"ネットワーク管理"

SVM スコープの NDMP モードでの ONTAP ユーザ認証

ストレージ仮想マシン（SVM）を対象とするNDMPモードでは、NDMPユーザ認証はロールベース アクセス制御と統合されています。SVMコンテキストでは、NDMPユーザには「vsadmin」または「vsadmin-backup」のいずれかのロールが必要です。クラスタコンテキストでは、NDMPユーザには「admin」または「backup」のいずれかのロールが必要です。

これらの事前定義済みロールに加えて、カスタム ロールに関連付けられたユーザ アカウントもNDMP認証に使用できます。ただし、カスタム ロールのコマンド ディレクトリに「vserver services ndmp」フォルダがあり、そのフォルダのアクセス レベルが「none」でない場合に限られます。このモードでは、ロールベース アクセス制御によって作成された、特定のユーザ アカウントのNDMPパスワードを生成する必要があります。管理者またはバックアップ ロールのクラスタ ユーザは、ノード管理LIF、クラスタ管理LIF、またはクラスタ間LIFにアクセスできます。vsadmin-backupまたはvsadmin ロールのユーザは、そのSVMのデータLIFにのみアクセスできます。したがって、ユーザのロールに応じて、バックアップおよびリストア処理で利用できるボリュームとテープ デバイスが異なります。

このモードでは、NISユーザとLDAPユーザのユーザ認証もサポートされます。そのため、NISユーザとLDAPユーザは、共通のユーザIDとパスワードを使用して複数のSVMにアクセスできます。ただし、NDMP認証ではActive Directoryユーザがサポートされません。

このモードでは、ユーザ アカウントを SSH アプリケーションと「User password」認証方式に関連付ける必要があります。

関連情報

[SVMを対象としたNDMPモードの管理用コマンド](#)

"システム管理"

ONTAP NDMPユーザー用のNDMP固有のパスワードを生成する

Storage Virtual Machine（SVM）を対象としたNDMPモードでは、特定のユーザID用のパスワードを生成する必要があります。NDMPユーザ用の実際のログイン パスワードに

基づいてパスワードが生成されます。実際のログイン パスワードが変更された場合は、NDMP固有のパスワードを生成し直す必要があります。

手順

1. `vserver services ndmp generate-password` コマンドを使用して、NDMP固有のパスワードを生成します。

このパスワードは、パスワード入力を必要とする現在または将来のすべてのNDMP処理で使用できます。



Storage Virtual Machine (SVM、旧Vserver) のコンテキストから、対象のSVMにのみ属しているユーザ用のNDMPパスワードを生成できます。

次の例は、user1というIDを持つユーザ用のNDMP固有のパスワードを生成する方法を示しています。

```
cluster1::vserver services ndmp> generate-password -vserver vs1 -user
user1

Vserver: vs1
User: user1
Password: jWZiNt57huPOoD8d
```

2. 通常のストレージ システム アカウントのパスワードを変更した場合は、この手順を繰り返して、新たなNDMP固有のパスワードを生成してください。

ONTAP MetroCluster構成での災害復旧時にテープ バックアップとリストア処理がどのように影響を受けるか

MetroCluster構成では、ディザスタ リカバリ時にテープ バックアップおよびリストア処理を同時に実行できます。ディザスタ リカバリ時にこれらの処理が受ける影響について理解しておく必要があります。

ディザスタ リカバリ関係にあるSVMのボリュームでテープ バックアップおよびリストア処理が実行される場合は、スイッチオーバーとスイッチバックのあとに増分テープ バックアップおよびリストア処理を引き続き実行できます。

FlexVol用のダンプ エンジンについて

ONTAP FlexVol ボリュームのONTAPダンプエンジンについて学ぶ

DumpはONTAPのスナップショット ベースのバックアップおよびリカバリ ソリューションで、スナップショットからテープ デバイスへのファイルやディレクトリのバックアップ、およびバックアップされたデータのストレージ システムへのリストアに役立ちます。

ダンプ バックアップを使用して、ファイルシステムのデータ（ディレクトリ、ファイル、およびそれらに関連するセキュリティ設定）をテープ デバイスにバックアップできます。バックアップ対象には、ボリューム全体、qtree全体、またはボリューム全体でもqtree全体でもないサブツリーを指定できます。

NDMP準拠のバックアップ アプリケーションを使用して、ダンプ バックアップやダンプ リストアを実行できます。

ダンプ バックアップを実行する際に、バックアップに使用するSnapshotを指定できます。バックアップのSnapshotを指定しない場合、ダンプ エンジンバックアップ用のSnapshotを作成します。バックアップ処理が完了すると、ダンプ エンジンはこのSnapshotを削除します。

ダンプ エンジンを使用して、テープへのレベル0バックアップ、増分バックアップ、または差分バックアップを実行できます。



Data ONTAP 8.3より前のリリースへのリバート後は、ベースライン バックアップ処理を実行してから増分バックアップ処理を実行する必要があります。

関連情報

["アップグレード、リバート、ダウングレード"](#)

ONTAP NDMPでのダンプ バックアップの仕組み

ダンプ バックアップは、定義済みのプロセスに基づいて、ディスクからテープにファイルシステムのデータを書き込みます。バックアップ対象には、ボリューム、qtree、またはボリューム全体でもqtree全体でもないサブツリーを指定できます。

次の表は、ダンプ パスによって示されるオブジェクトをバックアップするために ONTAP が使用するプロセスを示しています：

段階	アクション
1	フル ボリューム バックアップまたはフルqtreeバックアップ以外の場合、ONTAPはディレクトリをたどってバックアップ対象のファイルを特定します。ボリューム全体またはqtree全体をバックアップする場合は、段階2のプロセスから実行されます。
2	フル ボリューム バックアップまたはフルqtreeバックアップの場合、ONTAPはボリュームまたはqtree内のバックアップ対象のディレクトリを特定します。
3	ディレクトリをテープに書き出します。
4	ファイルをテープに書き出します。
5	必要に応じてACL情報をテープに書き出します。

ダンプ バックアップでは、データのSnapshotを使用してバックアップを行います。そのため、バックアップを開始する前にボリュームをオフラインにする必要はありません。

ダンプ バックアップでは、作成する各Snapshotに `snapshot\_for\_backup.n` という名前が付けられます。`n` は0から始まる整数です。ダンプ バックアップでSnapshotが作成されるたびに、整数が1ずつ増分されます。ストレージ システムのリブート後、整数は0にリセットされます。バックアップ処理が完了すると、ダンプ エンジンによってこのSnapshotが削除されます。

ONTAPが複数のダンプバックアップを同時に実行すると、ダンプエンジンは複数のスナップショットを作成

します。例えば、ONTAPが2つのダンプバックアップを同時に実行している場合、データのバックアップ元ボリュームには、以下のスナップショットが作成されます： `snapshot_for_backup.0` および ``snapshot_for_backup.1`。



スナップショットからバックアップする場合、ダンプ エンジンには追加のスナップショットを作成しません。

ダンプ エンジンでバックアップされるデータの種類

ダンプ エンジンを使用すると、災害やコントローラの障害に備えてデータをテープにバックアップできます。ファイル、ディレクトリ、qtree、ボリューム全体などのデータ オブジェクトのバックアップに加えて、ダンプ エンジンでは各ファイルに関する様々な種類の情報をバックアップできます。ダンプ エンジンでバックアップできるデータの種類の種類と考慮すべき制限事項を理解することで、災害復旧へのアプローチを計画するのに役立ちます。

ファイル内のデータのバックアップに加えて、ダンプ エンジンでは、必要に応じて各ファイルに関する次の情報をバックアップできます：

- UNIX GID、所有者UID、およびファイル権限
- UNIXのアクセス時刻、作成時刻、変更時刻
- ファイル タイプ
- ファイル サイズ
- DOS名、DOS属性、作成時刻
- 1,024個のアクセス制御エントリ（ACE）を含むアクセス制御リスト（ACL）
- qtree情報
- ジャンクション パス

ジャンクション パスはシンボリック リンクとしてバックアップされます。

- LUNおよびLUNクローン

LUNオブジェクト全体をバックアップすることはできますが、LUNオブジェクト内の単一のファイルをバックアップすることはできません。同様に、LUNオブジェクト全体を復元することはできますが、LUN内の単一のファイルを復元することはできません。



ダンプ エンジンでは、LUNクローンを独立したLUNとしてバックアップします。

- VM整合ファイル

VM アラインメント ファイルのバックアップは、Data ONTAP 8.1.2 より前のリリースではサポートされていません。



スナップショットでバックアップされたLUNクローンをData ONTAP 7-ModeからONTAPに移行すると、不整合なLUNになります。ダンプ エンジンでは不整合なLUNをバックアップしません。

ボリュームにデータを復元する場合、復元対象のLUNに対するクライアントI/Oは制限されます。LUNの制限

は、ダンプ復元操作が完了した時点で解除されます。同様に、SnapMirror単一ファイルまたはLUNの復元操作中は、復元対象のファイルとLUNの両方に対するクライアントI/Oは制限されます。この制限は、単一ファイルまたはLUNの復元操作が完了した時点で解除されます。ダンプ復元、またはSnapMirror単一ファイルまたはLUNの復元操作が行われているボリュームでダンプバックアップを実行する場合、クライアントI/O制限のあるファイルまたはLUNはバックアップに含まれません。これらのファイルまたはLUNは、クライアントI/O制限が解除された後続のバックアップ操作に含まれます。



Data ONTAP 8.3で実行され、テープにバックアップされたLUNは、8.3以降のリリースにのみリストアでき、それ以前のリリースにはリストアできません。LUNを以前のリリースにリストアする場合、LUNはファイルとしてリストアされます。

SnapVaultセカンダリ ボリュームまたはボリュームSnapMirrorデスティネーションをテープにバックアップすると、ボリューム上のデータのみがバックアップされます。関連するメタデータはバックアップされません。そのため、ボリュームをリストアしようとすると、そのボリューム上のデータのみがリストアされます。ボリュームSnapMirror関係に関する情報はバックアップに含まれていないため、リストアされません。

Windows NT権限のみを持つファイルをダンプし、それをUNIXスタイルのqtreeまたはボリュームに復元すると、ファイルはそのqtreeまたはボリュームのデフォルトのUNIX権限を取得します。

UNIX権限のみを持つファイルをダンプし、それをNTFSスタイルのqtreeまたはボリュームに復元すると、ファイルはそのqtreeまたはボリュームのデフォルトのWindows権限を取得します。

その他のダンプおよび復元では権限が保持されます。

VMアラインメントされたファイルと `vm-align-sector` オプションをバックアップできます。VMアラインメントされたファイルの詳細については、"[論理ストレージ管理](#)"を参照してください。

増分チェーンとONTAP NDMPについて学ぶ

増分チェーンとは、同じパスに対する一連の増分バックアップです。いつでも任意のレベルのバックアップを指定できるため、バックアップとリストアを効率的に実行するには、増分チェーンを理解する必要があります。31レベルの増分バックアップ操作を実行できます。

インクリメント チェーンには 2 つの種類があります：

- 連続増分チェーン。レベル 0 から始まり、後続のバックアップごとに 1 ずつ増加する増分バックアップのシーケンスです。
- 連続しない増分チェーン。増分バックアップではレベルがスキップされるか、レベルの順序が乱れます (0、2、3、1、4、またはより一般的には0、1、1、1または0、1、2、1、2など)。

増分バックアップでは、よりレベルが低い最新のバックアップがベースとして使用されます。たとえば、0、2、3、1、4という一連のバックアップレベルには、「0、2、3」と「0、1、4」の2つの漸増チェーンがあります。次の表に、増分バックアップのベースを示します。

バックアップの順序	増分レベル	漸増チェーン	基本	バックアップされるファイル
1	0	両方	ストレージ システム上のファイル	バックアップ パスのすべてのファイル

バックアップの順序	増分レベル	漸増チェーン	基本	バックアップされるファイル
2	2	0、2、3	レベル0のバックアップ	レベル0バックアップ以降に作成されたバックアップパスのファイル
3	3	0、2、3	レベル2 バックアップ	レベル2バックアップ以降に作成されたバックアップパスのファイル
4	1	0、1、4	レベル0バックアップ（レベル1バックアップよりもレベルが低く最新であるため）	レベル0バックアップ以降に作成されたバックアップパスのファイル（レベル2とレベル3のバックアップファイルを含む）
5	4	0、1、4	レベル1バックアップ（指定されたレベルより低く、レベル0、レベル2、レベル3のバックアップよりも新しいため）	レベル1バックアップ以降に作成されたファイル

ブロッキング ファクタと **ONTAP NDMP** について学ぶ

テープ ブロックは1,024バイトのデータです。テープ バックアップまたはリストア中に、各読み取り / 書き込み操作で転送されるテープ ブロックの数を指定できます。この数値は_ブロッキング ファクタ_と呼ばれます。

ブロッキング係数は4～256の範囲で使用できます。バックアップを実行したシステムとは別のシステムにバックアップをリストアする場合、リストア先のシステムがバックアップに使用したブロッキング係数をサポートしている必要があります。たとえば、ブロッキング係数128を使用する場合、そのバックアップをリストアするシステムもブロッキング係数128をサポートしている必要があります。

NDMP バックアップ中、MOVER_RECORD_SIZE によってブロッキング係数が決まります。ONTAP では、MOVER_RECORD_SIZE の最大値は 256 KB です。

ONTAPダンプバックアップを再開するタイミング

ダンプ バックアップは、テープ書き込みエラー、停電、ユーザーによる偶発的な中断、ストレージシステムの内部不整合など、内部または外部のエラーにより完了しない場合があります。これらの理由のいずれかでバックアップが失敗した場合は、バックアップを再開できます。

ストレージシステムのトラフィックが集中する時間帯を避けたり、テープドライブなどのストレージシステム上の他の限られたリソースの競合を避けたりするために、バックアップを中断して再開することができます。より緊急な復元（またはバックアップ）で同じテープドライブが必要な場合は、長時間のバックアップを中断して後で再開できます。再開可能なバックアップは、再起動後も保持されます。中止したテープへのバックアップを再開できるのは、以下の条件を満たす場合のみです：

- 中止されたバックアップはフェーズIVにあります。
- dumpコマンドによってロックされたすべての関連Snapshotが利用可能です。
- ファイル履歴を有効にする必要があります。

このようなダンプ操作が中止され、再開可能な状態のままになっている場合、関連するスナップショットはロックされます。これらのスナップショットは、バックアップ コンテキストが削除された後に解放されます。バックアップ コンテキストのリストは、`vserver services ndmp restartable backup show` コマンドを使用して表示できます。

```
cluster::> vserver services ndmp restartable-backup show
Vserver      Context Identifier      Is Cleanup Pending?
-----
vserver1 330e6739-0179-11e6-a299-005056bb4bc9 false
vserver1 481025c1-0179-11e6-a299-005056bb4bc9 false
vserver2 5cf10132-0179-11e6-a299-005056bb4bc9 false
3 entries were displayed.

cluster::> vserver services ndmp restartable-backup show -vserver
vserver1 -context-id 330e6739-0179-11e6-a299-005056bb4bc9

Vserver: vserver1
Context Identifier: 330e6739-0179-11e6-a299-005056bb4bc9
Volume Name: /vserver1/vol1
Is Cleanup Pending?: false
Backup Engine Type: dump
Is Snapshot Auto-created?: true
Dump Path: /vol/vol1
Incremental Backup Level ID: 0
Dump Name: /vserver1/vol1
Context Last Updated Time: 1460624875
Has Offset Map?: true
Offset Verify: true
Is Context Restartable?: true
Is Context Busy?: false
Restart Pass: 4
Status of Backup: 2
Snapshot Name: snapshot_for_backup.1
State of the Context: 7

cluster::>"
```

ONTAP NDMPでのダンプリストアの仕組み

ダンプ リストアでは、事前定義されたプロセスを使用して、ファイル システム データをテープ デバイスからディスクに書き込みます。

次の表のプロセスは、ダンプのリストアがどのように機能するかを示しています：

段階	アクション
1	ONTAPは、テープから抽出する必要があるファイルをカタログ化します。
2	ONTAPはディレクトリと空のファイルを作成します。
3	ONTAPはテープからファイルを読み取り、ディスクに書き込み、そのファイルに権限（ACLを含む）を設定します。
4	ONTAPは、指定されたすべてのファイルがテープからコピーされるまで、ステージ2と3を繰り返します。

ダンプ エンジンでリストアされるデータの種類

災害やコントローラーの障害が発生した場合、ダンプ エンジンは、単一のファイルからファイル属性、ディレクトリ全体まで、バックアップしたすべてのデータをリカバリするための複数の方法を提供します。ダンプ エンジンがリストアできるデータのタイプと、どのリカバリ方法をいつ使用するかを覚えておくことで、ダウンタイムを最小限に抑えることができます。

マッピングされたオンラインのLUNにデータをリストアできます。ただし、リストア処理が完了するまで、ホスト アプリケーションはこのLUNにアクセスできません。リストア処理が完了したら、LUNデータのホスト キャッシュをフラッシュして、リストアされたデータとの一貫性を確保する必要があります。

ダンプ エンジンでは、次のデータをリカバリできます。

- ファイルとディレクトリの内容
- UNIXファイル権限
- ACL

UNIXファイル権限のみを持つファイルをNTFS qtreeまたはボリュームにリストアした場合、そのファイルにはWindows NT ACLは設定されません。ストレージ システムは、このファイルにWindows NT ACLが作成されるまで、UNIXファイル権限のみを使用します。



Data ONTAP 8.2を実行しているストレージ システムからバックアップされたACLを、ACE制限が1,024未満のData ONTAP 8.1.x以前を実行しているストレージ システムに復元すると、デフォルトのACLが復元されます。

• qtree情報

qtree情報は、qtreeがボリュームのルートにリストアされる場合にのみ使用されます。qtree情報は、qtreeが `vs1/vol1/subdir/lowerdir` などの下位ディレクトリにリストアされ、qtreeでなくなる場合は使用されません。

- その他すべてのファイルとディレクトリの属性
- Windows NTストリーム
- LUN

◦ LUNをLUNとして残すには、ボリューム レベルまたはqtreeレベルに復元する必要があります。

ディレクトリに復元する場合は、有効なメタデータが含まれていないため、ファイルとして復元されます。

◦ 7-Mode LUN は ONTAP ボリューム上の LUN として復元されます。

- 7-ModeボリュームはONTAPボリュームに復元できます。
- デスティネーション ボリュームにリストアされたVMアライン ファイルは、デスティネーション ボリュームのVMアライン プロパティを継承します。
- 復元操作のデスティネーション ボリュームには、必須ロックまたは警告ロックが設定されたファイルが含まれている可能性があります。

このような宛先ボリュームへの復元操作を実行する際、dumpエンジンはこれらのロックを無視します。

ONTAP NDMPでデータをリストアする前に考慮すべき事項

バックアップしたデータは、元のパスまたは別の保存先に復元できます。バックアップしたデータを別の保存先に復元する場合は、復元操作のために保存先を準備する必要があります。

データを元のパスまたは別のデスティネーションに復元する前に、次の情報を用意し、次の要件を満たしている必要があります：

- 復元のレベル
- データを復元するパス
- バックアップ中に使用されるブロッキング ファクタ
- 増分リストアを実行する場合は、すべてのテープがバックアップ チェーンに含まれている必要があります
- 復元するテープと互換性のある使用可能なテープ ドライブ

データを別のデスティネーションに復元する前に、次の操作を実行する必要があります：

- ボリュームを復元する場合は、新しいボリュームを作成する必要があります。
- qtree またはディレクトリを復元する場合は、復元するファイルと同じ名前を持つ可能性のあるファイルの名前を変更するか、移動する必要があります。



ONTAP 9では、qtree名はUnicode形式をサポートしています。以前のリリースのONTAPでは、この形式はサポートされていません。ONTAP 9でUnicode名を持つqtreeを`ndmcopy`コマンドまたはテープ内のバックアップ イメージからのリストアを使用して以前のリリースのONTAPにコピーした場合、qtreeはUnicode形式のqtreeではなく、通常のディレクトリとしてリストアされます。



復元されたファイルの名前が既存のファイルと同じ場合、既存のファイルは復元されたファイルによって上書きされます。ただし、ディレクトリは上書きされません。

DAR を使用せずにリストア中にファイル、ディレクトリ、または qtree の名前を変更するには、EXTRACT 環境変数を `E` に設定する必要があります。

デスティネーション ストレージ システムに必要なスペース

デスティネーション ストレージ システムには、復元するデータの量よりも約 100 MB 多いスペースが必要です。



リストア処理では、リストア処理の開始時にデスティネーション ボリュームのボリューム スペースとinode可用性を確認します。FORCE環境変数を `Y` に設定すると、リストア処理でデスティネーション パスのボリューム スペースとinode可用性の確認がスキップされます。デスティネーション ボリュームに十分なボリューム スペースまたはinodeがない場合、リストア処理では、デスティネーション ボリューム スペースとinode可用性で許可されるデータ量がリカバリされます。ボリューム スペースまたはinodeがなくなると、リストア処理は停止します。

ONTAPダンプ バックアップおよびリストア セッションのスケーラビリティ制限

システム メモリ容量が異なるストレージ システムで同時に実行できるダンプ バックアップおよびリストア セッションの最大数に注意する必要があります。この最大数は、ストレージ システムのシステム メモリによって異なります。

次の表に、ダンプまたはリストア エンジンの制限を示します。「NDMPセッションのスケーラビリティ制限」に記載されている制限は、NDMPサーバの制限であり、エンジンの制限よりも高くなります。

ストレージ システムのシステム メモリ	dumpバックアップと復元セッションの合計数
16GB未満	4
16GB以上24GB未満	16
24GB以上	32



`ndmpcopy` コマンドを使用してストレージ システム内でデータをコピーする場合、dumpバックアップ用とdumpリストア用の 2 つの NDMP セッションが確立されます。

ストレージ システムのシステム メモリは、`sysconfig -a` コマンド (nodeshellから使用可能) を使用して取得できます。`sysconfig -a` 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。

関連情報

[NDMPセッションのスケーラビリティ制限](#)

ONTAP SVM名とコンテキストIDを指定して、再起動可能なコンテキストを削除します。

コンテキストを再起動する代わりにバックアップを開始する場合は、コンテキストを削除できます。

タスク概要

``vserver services ndmp restartable-backup delete``コマンドを使用して SVM名とコンテキストIDを指定することで、再起動可能なコンテキストを削除できます。

手順

1. 再開可能なコンテキストを削除します。

`vserver services ndmp restartable-backup delete -vserver vservice-name -context -id context_identifier`

```
cluster::> vserver services ndmp restartable-backup show
Vserver      Context Identifier      Is Cleanup Pending?
-----
vserver1     330e6739-0179-11e6-a299-005056bb4bc9 false
vserver1     481025c1-0179-11e6-a299-005056bb4bc9 false
vserver2     5cf10132-0179-11e6-a299-005056bb4bc9 false
3 entries were displayed.

cluster::>
cluster::> vserver services ndmp restartable-backup delete -vserver
vserver1 -context-id 481025c1-0179-11e6-a299-005056bb4bc9

cluster::> vserver services ndmp restartable-backup show
Vserver      Context Identifier      Is Cleanup Pending?
-----
vserver1     330e6739-0179-11e6-a299-005056bb4bc9 false
vserver2     5cf10132-0179-11e6-a299-005056bb4bc9 false
3 entries were displayed.

cluster::>
```

ONTAP SnapVault セカンダリ ボリュームでのダンプの動作

SnapVaultセカンダリ ボリュームでミラーリングされたデータに対してテープ バックアップ処理を実行できます。バックアップできるのは、SnapVaultセカンダリ ボリュームでテープにミラーリングされたデータのみです。SnapVault関係のメタデータはバックアップできません。

データ保護ミラー関係を解除した場合(snapmirror break、またはSnapMirror再同期が発生した場合は、必

ずベースライン バックアップを実行する必要があります。

関連情報

- ["snapmirror break"](#)

ONTAPストレージフェイルオーバーおよびARL操作でのダンプの仕組み

ダンプ バックアップまたはリストア操作を実行する前に、これらの操作がストレージ フェイルオーバー（テイクオーバーとギブバック）またはアグリゲートの再配置（ARL）操作とどのように連携するかを理解しておく必要があります。`-override-vetoes` オプションは、ストレージ フェイルオーバーまたはARL操作中のダンプ エンジンの動作を決定します。

ダンプ バックアップまたはリストア処理の実行中に `override-vetoes` オプションが `false` に設定されている場合、ユーザが開始したストレージ フェイルオーバーまたはARL処理は停止されます。ただし、`override-vetoes` オプションが `true` に設定されている場合、ストレージ フェイルオーバーまたはARL処理は続行され、ダンプ バックアップまたはリストア処理は中止されます。ストレージ フェイルオーバーまたはARL処理がストレージ システムによって自動的に開始された場合、アクティブなダンプ バックアップまたはリストア処理は常に中止されます。ストレージ フェイルオーバーまたはARL処理が完了したあとも、ダンプ バックアップおよびリストア処理を再開することはできません。

CAB拡張がサポートされている場合のダンプ処理

バックアップ アプリケーションでCAB拡張がサポートされている場合は、ストレージ フェイルオーバーまたはARL処理のあとにバックアップ ポリシーを再設定しなくても、増分ダンプ バックアップおよびリストア処理を引き続き実行できます。

CAB拡張がサポートされていない場合のダンプ処理

バックアップ アプリケーションでCAB拡張がサポートされていない場合は、バックアップ ポリシーで設定されたLIFをデスティネーション アグリゲートをホストするノードに移行すれば、増分ダンプ バックアップおよびリストア処理を引き続き実行できます。移行しない場合は、ストレージ フェイルオーバーおよびARL処理のあと、増分バックアップ処理を実行する前にベースライン バックアップを実行する必要があります。



ストレージ フェイルオーバー処理の場合は、バックアップ ポリシーで設定されたLIFをパートナー ノードに移行する必要があります。

関連情報

["高可用性"](#)

ONTAPボリューム移動でのダンプの仕組み

ストレージ システムで最終フェーズ（カットオーバー）が開始されるまでは、テープ バックアップおよびリストア処理とボリューム移動を並行して実行できます。最終フェーズのあとは、移動中のボリュームで新しいテープ バックアップおよびリストア処理を実行することはできません。ただし、現在の処理は完了するまで引き続き実行されます。

次の表は、ボリューム移動処理後のテープ バックアップおよびリストア処理の動作を示しています。

tape backupおよび復元操作を実行している場合は...	操作
Storage Virtual Machine (SVM) を対象としたNDMPモード (CAB拡張がバックアップ アプリケーションでサポートされている場合)	バックアップ ポリシーを再設定しなくても、読み取り / 書き込みボリュームおよび読み取り専用ボリュームで増分テープ バックアップおよびリストア処理を引き続き実行できます。
SVMを対象としたNDMPモード (CAB拡張がバックアップ アプリケーションでサポートされていない場合)	バックアップ ポリシーで設定されたLIFを、デスティネーション アグリゲートをホストするノードに移行する場合は、読み取り / 書き込みボリュームおよび読み取り専用ボリュームで増分テープ バックアップおよびリストア処理を引き続き実行できます。それ以外の場合は、ボリューム移動後にベースライン バックアップを実行してから増分バックアップ処理を実行する必要があります。



ボリュームを移動する場合に、デスティネーション ノード上の別のSVMに属しているボリュームの名前が移動対象のボリュームの名前と同じであると、移動対象のボリュームの増分バックアップ処理を実行できません。

ONTAP FlexVolボリュームがいっぱいになったときのダンプの動作

増分ダンプ バックアップ処理を実行する前に、FlexVolに十分な空きスペースを確保する必要があります。

操作が失敗した場合は、FlexVol volumeのサイズを増やすか、スナップショットを削除して、FlexVol volumeの空き容量を増やす必要があります。その後、増分バックアップ操作を再度実行してください。

ONTAPボリュームのアクセスタイプが変更された場合のダンプの動作

SnapMirrorデスティネーション ボリュームまたはSnapVaultセカンダリ ボリュームの状態が読み取り / 書き込みから読み取り専用に、または読み取り専用から読み取り / 書き込みに変わった場合は、ベースライン テープ バックアップまたはリストア処理を実行する必要があります。

SnapMirrorデスティネーション ボリュームとSnapVaultセカンダリ ボリュームは読み取り専用ボリュームです。これらのボリュームでテープ バックアップおよびリストア処理を実行する場合は、ボリュームの状態が読み取り専用から読み取り / 書き込みに、または読み取り / 書き込みから読み取り専用に変わるたびにベースライン バックアップまたはリストア処理を実行する必要があります。

ONTAP SnapMirror単一ファイルまたはLUNリストアでのダンプの仕組み

SnapMirrorテクノロジーを使用して単一ファイルまたはLUNがリストアされているボリュームでダンプ バックアップまたはリストア処理を実行する場合は、ダンプ処理と単一ファイル / LUNリストア処理との関係を理解しておく必要があります。

SnapMirrorによる単一ファイル / LUNリストア処理中は、リストア対象のファイルまたはLUNでクライアントI/Oが制限されます。単一ファイル / LUNリストア処理が完了すると、ファイルまたはLUNのI/Oの制限は解除されます。単一ファイルまたはLUNのリストア先ボリュームでダンプ バックアップが実行された場合、ク

ライアントI/Oが制限されているファイルまたはLUNはダンプ バックアップに含まれません。その後、I/O制限が解除されたあとのバックアップ処理では、このファイルまたはLUNはテープにバックアップされます。

ダンプ リストアとSnapMirrorによる単一ファイル / LUNリストア処理を同じボリュームで同時に実行することはできません。

ONTAP MetroCluster構成におけるダンプバックアップとリストア操作への影響

MetroCluster構成内でダンプ バックアップおよび復元操作を実行する前に、スイッチオーバーまたはスイッチバック操作が発生したときにダンプ操作がどのように影響を受けるかを理解する必要があります。

ダンプ バックアップまたはリストア処理の後にスイッチオーバーを実行する

クラスター 1 とクラスター 2 という 2 つのクラスターについて考えます。クラスター 1 でのダンプ バックアップまたは復元操作中に、クラスター 1 からクラスター 2 へのスイッチオーバーが開始されると、次の処理が実行されます：

- `override-vetoes` オプションの値が `false` の場合、スイッチオーバーは中止され、バックアップまたは復元操作は続行されます。
- オプションの値が `true` の場合、ダンプ バックアップまたは復元操作は中止され、スイッチオーバーは続行されます。

ダンプ バックアップまたはリストア処理の後にスイッチバックを実行する

クラスター1からクラスター2へのスイッチオーバーが実行され、クラスター2でダンプ バックアップまたはリストア処理が開始されます。ダンプ処理では、クラスター2にあるボリュームがバックアップまたはリストアされます。この時点で、クラスター2からクラスター1へのスイッチバックが開始されると、次の処理が行われます：

- `override-vetoes` オプションの値が `false` の場合、スイッチバックはキャンセルされ、バックアップまたは復元操作が続行されます。
- オプションの値が `true` の場合、バックアップまたは復元操作は中止され、スイッチバックが続行されます。

スイッチオーバーまたはスイッチバック中に開始されたダンプ バックアップまたはリストア処理

クラスター 1 からクラスター 2 へのスイッチオーバー中に、クラスター 1 でダンプ バックアップまたは復元操作が開始されると、バックアップまたは復元操作は失敗し、スイッチオーバーは続行されます。

クラスター2からクラスター1へのスイッチバック中に、クラスター2からダンプ バックアップまたはリストア処理が開始されると、バックアップまたはリストア処理は失敗し、スイッチバックが続行されます。

FlexVol用のSMTapeエンジンについて

FlexVolボリューム用のONTAP SMTapeエンジンについて

SMTapeは、データのブロックをテープにバックアップするONTAPのディザスタリカバリソリューションです。SMTapeを使用して、ボリュームのバックアップをテープに対して実行できます。ただし、qtreeレベルまたはサブツリーレベルでのバックアップは実行できません。SMTapeは、ベースライン バックアップ、差分バックアップ、増分バックアップ

クアッパをサポートしています。SMTapeにはライセンスは必要ありません。

NDMP準拠のバックアップ アプリケーションを使用して、SMTapeバックアップおよびリストア処理を実行できます。SMTapeを選択すると、Storage Virtual Machine (SVM) を対象とするNDMPモードでのみバックアップおよびリストア処理を実行できます。



SMTapeバックアップまたはリストア セッションの実行中は、リバート プロセスはサポートされません。セッションが終了するまで待つか、NDMPセッションを中止する必要があります。

SMTapeを使用すると、255個のSnapshotをバックアップできます。それ以降のベースライン、増分、または差分バックアップでは、古いバックアップ済みSnapshotを削除する必要があります。

ベースライン復元を実行する前に、データの復元先となるボリュームが `DP` タイプであり、制限状態になっている必要があります。復元が成功すると、このボリュームは自動的にオンラインになります。その後は、バックアップを実行した順序で、このボリュームに対して増分復元または差分バックアップを実行できます。

SMTapeバックアップ中の**ONTAP**スナップショットの使用について学習します

SMTapeのベースライン バックアップと増分バックアップでSnapshotがどのように使用されるかを理解する必要があります。また、SMTapeを使用してバックアップを実行する際には、考慮すべき点があります。

ベースライン バックアップ

ベースライン バックアップを実行する際に、テープにバックアップするSnapshotの名前を指定できます。Snapshotを指定しない場合は、ボリュームのアクセス タイプ（読み取り / 書き込みまたは読み取り専用）に応じて、Snapshotが自動的に作成されるか、既存のSnapshotが使用されます。バックアップのSnapshotを指定すると、指定したSnapshotよりも古いすべてのSnapshotもテープにバックアップされます。

バックアップのSnapshotを指定しない場合は、次のようになります：

- 読み取り / 書き込みボリュームの場合、Snapshotが自動的に作成されます。

新しく作成されたSnapshotとすべての古いSnapshotがテープにバックアップされます。

- 読み取り専用ボリュームの場合、最新のSnapshotを含むすべてのSnapshotがテープにバックアップされます。

バックアップの開始後に作成された新しいSnapshotはバックアップされません。

増分バックアップ

SMTapeの増分または差分バックアップ処理の場合、NDMP準拠のバックアップ アプリケーションがSnapshotを作成および管理します。

増分バックアップ操作を実行する際は、必ずスナップショットを指定してください。増分バックアップ操作を正常に実行するには、前回のバックアップ操作（ベースラインまたは増分）でバックアップされたスナップショットが、バックアップ元のボリューム上に存在している必要があります。このバックアップされたスナップショットを確実に使用するには、バックアップ ポリシーの設定時に、このボリュームに割り当てられているスナップショット ポリシーを考慮する必要があります。

SnapMirrorデスティネーションでのSMTapeバックアップに関する考慮事項

- データ保護ミラー関係では、レプリケーション用にデスティネーション ボリュームに一時的なSnapshotが作成されます。

これらのスナップショットをSMTapeバックアップに使用しないでください。

- SnapMirror更新が、同じボリュームでのSMTapeバックアップ操作中にデータ保護ミラー関係の宛先ボリュームで発生した場合、SMTapeによってバックアップされたSnapshotはソース ボリューム上で削除してはなりません。

バックアップ操作中、SMTape は宛先ボリューム上のスナップショットをロックし、対応するスナップショットがソース ボリューム上で削除されると、後続のSnapMirror更新処理は失敗します。

- 増分バックアップ中はこれらのSnapshotを使用しないでください。

ONTAPテープ バックアップおよびリストア処理を最適化するSMTape機能

スナップショットのバックアップ、増分および差分バックアップ、リストアされたボリューム上の重複排除および圧縮機能の保持、テープ シーディングなどの SMTape 機能は、テープ バックアップおよびリストア処理の最適化に役立ちます。

SMTapeには次の機能があります。

- ディザスタ リカバリ ソリューションを提供
- 増分バックアップと差分バックアップが可能
- Snapshotをバックアップする
- 重複排除されたボリュームのバックアップとリストアを可能にし、リストアされたボリュームの重複排除を維持します
- 圧縮されたボリュームをバックアップし、リストアされたボリュームでも圧縮を維持します
- テープ シーディングを有効にする

SMTape は、4 KB から 256 KB までの範囲で、4 KB の倍数のブロッキング係数をサポートします。



データは、最大2つの連続するONTAPメジャー リリースにわたって作成されたボリュームにのみリストアできます。

SMTapeバックアップおよびリストア セッションのONTAPスケーラビリティ制限

NDMPまたはCLIを使用したSMTapeバックアップおよびリストア処理（テープ シーディング）の実行中は、システム メモリ容量が異なるストレージ システムで同時に実行できるSMTapeバックアップおよびリストア セッションの最大数に注意する必要があります。この最大数は、ストレージ システムのシステム メモリによって異なります。



SMTapeバックアップおよびリストア セッションのスケーラビリティ制限は、NDMPセッションの制限やダンプ セッションの制限とは異なります。

ストレージ システムのシステム メモリ	SMTapeバックアップおよびリストアセッションの合計数
16GB未満	6
16GB以上24GB未満	16
24GB以上	32

ストレージ システムのシステム メモリは、`sysconfig -a` コマンド（nodeshellから使用可能）を使用して取得できます。`sysconfig -a`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。

関連情報

- [NDMPセッションのスケラビリティ制限](#)
- [ダンプ バックアップおよびリストア セッションのスケラビリティ制限](#)

ONTAPテープ シーディングについて学ぶ

テープ シーディングはSMTapeの機能で、データ保護ミラー関係が確立されたデスティネーションFlexVolの初期化に使用できます。

テープ シーディングを使用すると、低帯域幅の接続でストレージ システムとデスティネーション システムの間にSnapMirror関係を確立できます。

ソースからデスティネーションへのSnapshotの増分ミラーリングは、低帯域幅接続でも実行可能です。ただし、低帯域幅接続では、ベースSnapshotの初期ミラーリングに長い時間がかかります。このような場合は、ソース ボリュームのSMTapeバックアップをテープに作成し、そのテープを使用して初期ベースSnapshotをデスティネーションに転送することができます。その後、低帯域幅接続を使用して、デスティネーション システムへの増分SnapMirror更新を設定できます。

SMTapeがONTAPストレージ フェイルオーバーおよびARL処理でどのように機能するか

SMTapeバックアップまたはリストア処理を実行する前に、ストレージ フェイルオーバー（テイクオーバーとギブバック）またはアグリゲートの再配置（ARL）処理でこれらの処理がどのように機能するかを理解しておく必要があります。`-override-vetoes` オプションは、ストレージ フェイルオーバーまたはARL処理中のSMTapeエンジンの動作を決定します。

SMTapeバックアップまたはリストア処理の実行中に`-override-vetoes` オプションが`false`に設定されている場合、ユーザが開始したストレージ フェイルオーバーまたはARL処理は停止され、バックアップまたはリストア処理が完了します。バックアップ アプリケーションがCAB拡張をサポートしている場合は、バックアップ ポリシーを再設定することなく、増分SMTapeバックアップおよびリストア処理を続行できます。ただし、`-override-vetoes` オプションが`true`に設定されている場合、ストレージ フェイルオーバーまたはARL処理は続行され、SMTapeバックアップまたはリストア処理は中止されます。

関連情報

["ネットワーク管理"](#)

SMTapeとONTAPボリューム移動の仕組み

ストレージ システムで最終フェーズ（カットオーバー試行）が実行されるまでは、SMTapeバックアップ処理とボリューム移動処理を並行して実行できます。最終フェーズのあとは、移動するボリュームで新しいSMTapeバックアップ処理を実行することはできません。ただし、現在の処理は完了するまで引き続き実行されます。

ボリューム移動処理では、ボリュームのカットオーバー フェーズを開始する前に、同じボリュームでアクティブなSMTapeバックアップ処理を確認します。アクティブなSMTapeバックアップ処理がある場合、ボリューム移動処理はカットオーバー保留状態になり、SMTapeバックアップ処理を完了できます。これらのバックアップ処理が完了したあとで、ボリューム移動処理を手動で再開する必要があります。

バックアップ アプリケーションでCAB拡張がサポートされている場合は、バックアップ ポリシーを再設定しなくても、読み取り / 書き込みボリュームおよび読み取り専用ボリュームで増分テープ バックアップおよびリストア処理を引き続き実行できます。

ベースライン リストア処理とボリューム移動処理を同時に実行することはできません。ただし、増分リストアはボリューム移動処理と並行して実行できます。このリストアの動作は、ボリューム移動処理時のSMTapeバックアップ処理と同様です。

SMTapeがONTAPボリュームの再ホスト処理でどのように機能するか

ボリューム上でボリューム再ホスト操作が進行中の場合、SMTape操作を開始できません。ボリュームがボリューム再ホスト操作の対象となっている場合、そのボリューム上でSMTapeセッションを開始しないでください。

ボリュームの再ホスト操作が進行中の場合、SMTapeのバックアップまたはリストアは失敗します。SMTapeのバックアップまたはリストアが進行中の場合、ボリュームの再ホスト操作は失敗し、適切なエラーメッセージが表示されます。この状況は、NDMPベースとCLIベースの両方のバックアップまたはリストア操作に適用されます。

ADB 実行中に ONTAP NDMP バックアップ ポリシーが受ける影響

自動データ バランサ（ADB）が有効になっている場合、バランサはアグリゲートの使用状況統計を分析し、設定された上限しきい値の使用率を超えたアグリゲートを識別します。

しきい値を超えたアグリゲートを特定した後、バランサはクラスタ内の別のノードにあるアグリゲートに移動可能なボリュームを特定し、そのボリュームの移動を試みます。この状況は、このボリュームに設定されているバックアップ ポリシーに影響を及ぼします。データ管理アプリケーション（DMA）がCABに対応していない場合、ユーザーはバックアップ ポリシーを再設定し、ベースライン バックアップ処理を実行する必要があります。



DMAがCABに対応しており、バックアップ ポリシーが特定のインターフェイスを使用して構成されている場合、ADBは影響を受けません。

ONTAP MetroCluster構成におけるSMTapeバックアップおよびリストア操作への影響

MetroCluster構成でSMTapeバックアップおよびリストア処理を実行する前に、スイッチオーバーまたはスイッチバック処理が発生したときにSMTape処理がどのように影響を受けるかを理解しておく必要があります。

SMTapeバックアップまたはリストア処理後のスイッチオーバー

クラスタ1とクラスタ2という2つのクラスタがあるとします。クラスタ1でのSMTapeバックアップまたは復元操作中に、クラスタ1からクラスタ2へのスイッチオーバーが開始されると、次の処理が実行されます：

- `-override-vetoes` オプションの値が `false` の場合、スイッチオーバー プロセスは中止され、バックアップまたは復元操作は続行されます。
- オプションの値が `true` の場合、SMTapeバックアップまたはリストア処理は中止され、スイッチオーバー プロセスが続行されます。

SMTapeバックアップまたはリストア処理後のスイッチバック

クラスタ 1 からクラスタ 2 へのスイッチオーバーが実行され、クラスタ 2 で SMTape バックアップまたは復元操作が開始されます。SMTape 操作は、クラスタ 2 にあるボリュームをバックアップまたは復元します。この時点で、クラスタ 2 からクラスタ 1 へのスイッチバックが開始されると、次の処理が行われます：

- `-override-vetoes` オプションの値が `false` の場合、スイッチバック プロセスは中止され、バックアップまたは復元操作は続行されます。
- オプションの値が `true` の場合、バックアップまたは復元操作は中止され、スイッチバック プロセスが続行されます。

スイッチオーバーまたはスイッチバック中に開始されたSMTapeバックアップまたはリストア操作

クラスタ 1 からクラスタ 2 へのスイッチオーバー プロセス中に、クラスタ 1 で SMTape バックアップまたはリストア処理が開始されると、バックアップまたはリストア処理は失敗し、スイッチオーバーは続行されます。

クラスタ 2 からクラスタ 1 へのスイッチバック プロセス中に、クラスタ 2 から SMTape バックアップまたはリストア処理が開始されると、バックアップまたはリストア処理は失敗し、スイッチバックが続行されます。

FlexVolのテープ バックアップおよびリストア処理の監視

FlexVolボリュームのONTAPテープバックアップとリストア操作を監視する

イベント ログ ファイルを表示して、テープ バックアップおよびリストア処理を監視できます。ONTAPは、重要なバックアップおよびリストア イベントとその発生時刻を、コントローラの `/etc/log/` ディレクトリにある `backup` という名前のログ ファイルに自動的に記録します。デフォルトでは、イベント ロギングは `on` に設定されています。

次の理由でイベント ログ ファイルを表示する場合があります：

- 夜間のバックアップが成功したかどうかを確認する
- バックアップ操作に関する統計の収集

- 過去のイベント ログ ファイルの情報をを使用した、バックアップおよびリストア処理に関する問題の診断

イベント ログ ファイルは毎週 1 回ローテーションされます。 `/etc/log/backup`` ファイルの名前は ``/etc/log/backup.0`` に変更され、 ``/etc/log/backup.0`` ファイルの名前は ``/etc/log/backup.1`` に変更されます。システムはログ ファイルを最大 6 週間保存するため、最大 7 つのメッセージ ファイル (`/etc/log/backup.[0-5]` と現在の ``/etc/log/backup`` ファイル) を保持できます。

テープ バックアップおよびリストア操作の **ONTAP** イベント ログ ファイルにアクセスします

``/etc/log/`` ディレクトリ内のテープ バックアップおよびリストア操作のイベント ログ ファイルには、ノードシェルで ``rdfile`` コマンドを使用してアクセスできます。これらのイベント ログ ファイルを表示して、テープ バックアップおよびリストア操作を監視できます。

タスク概要

``spi`` Web サービスへのアクセス権を持つアクセス制御ロールや、``http`` アクセス方法で設定されたユーザー アカウントなどの追加構成を使用すると、Web ブラウザを使用してこれらのログ ファイルにアクセスすることもできます。

手順

1. 次のコマンドを実行して、ノードシェルにアクセスします。

```
node run -node node_name
```

`node_name` はノードの名前です。

2. 次のコマンドを実行して、テープ バックアップおよびリストア処理用のイベント ログ ファイルにアクセスします。

```
rdfile /etc/log/backup
```

関連情報

["システム管理"](#)

ダンプ イベント ログ メッセージおよびリストア イベント ログ メッセージの形式とは

ONTAP ダンプおよびリストア イベント ログ メッセージの形式

ダンプ イベントとリストア イベントが発生すると、そのたびにバックアップ ログ ファイルにメッセージが書き込まれます。

ダンプ イベント ログとリストア イベント ログのメッセージの形式は次のとおりです。

```
type timestamp identifier event (event_info)
```

以下に、イベント ログ メッセージの各フィールドについて説明します。

- 各ログメッセージは、次の表に示すいずれかのタイプインジケータで始まります。

タイプ	概要
ログ	ロギング イベント
dmp	ダンプ イベント
rst	リストア イベント

- `timestamp` イベントの日時を表示します。
- ダンプイベントの `identifier` フィールドには、ダンプパスとダンプの一意的IDが含まれます。リストアイベントの `identifier` フィールドでは、リストア先のパス名のみが一意的識別子として使用されます。ログ関連のイベントメッセージには、`identifier` フィールドは含まれません。

ONTAP ログイベントについて学ぶ

logで始まるメッセージのeventフィールドは、ロギングの開始または終了を表します。

eventフィールドは、次のいずれかのイベントになります。

イベント	概要
Start_Logging	ロギングの開始、または無効になっていたロギングの再開を表します。
Stop_Logging	ロギングの停止を表します。

ONTAP ダンプイベントについて学ぶ

ダンプ イベントのeventフィールドには、イベント タイプに続けてカッコ内にイベント固有の情報が示されます。

次の表は、ダンプ処理に対して記録されるイベント、その説明、および関連するイベント情報を示しています。

イベント	概要	イベント情報
開始	NDMPダンプが開始されました	ダンプ レベルおよびダンプのタイプ
終わり	ダンプが完了しました	処理されたデータの量
中止	処理がキャンセルされました	処理されたデータの量
オプション	指定したオプションが表示されます	NDMPオプションを含むすべてのオプションと関連する値

イベント	概要	イベント情報
Tape_open	テープが読み取り / 書き込み用にオープンされました	新しいテープ デバイスの名前
Tape_close	テープの読み取り / 書き込みが終了しました	テープ デバイスの名前
Phase-change	ダンプが新しい処理フェーズに切り替わりました	新しいフェーズの名前
エラー	ダンプで予期せぬイベントが発生しました	エラー メッセージ
Snapshot	スナップショットが作成または配置されます	スナップショットの名前と時刻
Base_dump	内部メタファイル内のベース ダンプ エントリが指定されました	ベース ダンプのレベルと時刻（増分ダンプの場合のみ）

ONTAP リストア イベントについて学ぶ

リストア イベントのeventフィールドでは、イベント形式のあとのカッコ内にイベント固有の情報が示されます。

次の表に、リストア処理に関して記録されるイベント、その説明、および関連するイベント情報を示します。

イベント	概要	イベント情報
開始	NDMP リストア が開始されました	リストア レベルおよびリストア 形式
終わり	リストア が完了しました	処理されたファイルの数およびデータの量
中止	処理がキャンセルされました	処理されたファイルの数およびデータの量
オプション	指定したオプションが表示されます	NDMP オプションを含むすべてのオプションと関連する値
Tape_open	テープが読み取り / 書き込み用にオープンされました	新しいテープ デバイスの名前
Tape_close	テープの読み取り / 書き込みが終了しました	テープ デバイスの名前

イベント	概要	イベント情報
Phase-change	リストアの新しい処理フェーズが開始されました	新しいフェーズの名前
エラー	リストアで予期せぬイベントが発生しました	エラー メッセージ

ONTAP テープ バックアップおよびリストア操作のイベント ログの有効化または無効化

イベント ログをオンまたはオフにすることができます。

手順

1. イベント ログिंगを有効または無効にするには、クラスタシェルで次のコマンドを入力します。

```
options -option_name backup.log.enable -option-value {on | off}
```

on イベント ログをオンにします。

off イベントのログ記録をオフにします。



イベント ログはデフォルトでオンになっています。

FlexVolのテープ バックアップおよびリストアに関するエラー メッセージ

バックアップおよびリストアに関するエラー メッセージ

Resource limitation: no available thread

- メッセージ

```
Resource limitation: no available thread
```

- 原因

現在、アクティブなローカル テープ I/O スレッドの最大数が使用されています。アクティブなローカル テープ ドライブは最大16台まで使用できます。

- 対処方法

いくつかのテープ ジョブが完了するまで待ってから、新しいバックアップ ジョブまたはリストア ジョブを開始します。

Tape reservation preempted

- メッセージ

```
Tape reservation preempted
```

- 原因

テープドライブが別の処理で使用されているか、テープがすでに閉じられています。

- 対処方法

テープドライブが別の処理で使用されていないこと、およびDMAアプリケーションによってジョブが中断されていないことを確認してから、再試行します。

Could not initialize media

- メッセージ

Could not initialize media

- 原因

このエラーは、次のいずれかの原因で発生する可能性があります。

- バックアップに使用したテープドライブが破損または損傷しています。
- テープには完全なバックアップが含まれていないか、破損しています。
- 現在、アクティブなローカル テープ I/O スレッドの最大数が使用されています。

アクティブなローカル テープドライブは最大 16 台まで使用できます。

- 対処方法

- テープドライブが破損または損傷している場合は、有効なテープドライブで操作を再試行してください。
- テープ内に完全なバックアップが含まれていないか破損している場合は、復元操作を実行できません。
- テープリソースが利用できない場合は、一部のバックアップジョブまたはリストアジョブが完了するまで待ってから、操作を再試行してください。

Maximum number of allowed dumps or restores (maximum session limit) in progress

- メッセージ

Maximum number of allowed dumps or restores (maximum session limit) in progress

- 原因

最大数のバックアップジョブまたはリストアジョブがすでに実行中です。

- 対処方法

現在実行中のジョブがいくつか完了してから、処理を再試行します。

Media error on tape write

- メッセージ

Media error on tape write

- 原因

バックアップに使用するテープが破損しています。

- 対処方法

テープを取り替えて、バックアップ ジョブを再試行します。

Tape write failed

- メッセージ

Tape write failed

- 原因

バックアップに使用するテープが破損しています。

- 対処方法

テープを取り替えて、バックアップ ジョブを再試行します。

Tape write failed - new tape encountered media error

- メッセージ

Tape write failed - new tape encountered media error

- 原因

バックアップに使用するテープが破損しています。

- 対処方法

テープを取り替えて、バックアップを再試行します。

Tape write failed - new tape is broken or write protected

- メッセージ

Tape write failed - new tape is broken or write protected

- 原因

バックアップに使用するテープが破損しているか、テープに書き込み保護がかけられています。

- 対処方法

テープを取り替えて、バックアップを再試行します。

Tape write failed - new tape is already at the end of media

- メッセージ

Tape write failed - new tape is already at the end of media

- 原因

テープにはバックアップを完了できるだけのスペースがありません。

- 対処方法

テープを取り替えて、バックアップを再試行します。

Tape write error

- メッセージ

Tape write error - The previous tape had less than the required minimum capacity, size MB, for this tape operation, The operation should be restarted from the beginning

- 原因

テープ容量が不足していてバックアップ データを格納することができません。

- 対処方法

より大きな容量のテープを使用して、バックアップ ジョブを再試行します。

Media error on tape read

- メッセージ

Media error on tape read

- 原因

データのリストア元のテープが破損しており、テープに完全なバックアップ データが含まれていない可能性があります。

- 対処方法

テープに完全なバックアップが含まれていることがわかっている場合は、リストア処理を再試行します。テープに完全なバックアップが含まれていなければ、リストア処理は実行できません。

Tape read error

- メッセージ

`Tape read error`

- 原因

テープドライブが破損しているか、テープに完全なバックアップが含まれていません。

- 対処方法

テープドライブが破損している場合は、別のテープドライブを使用します。テープに完全なバックアップが含まれていない場合は、データをリストアできません。

Already at the end of tape

- メッセージ

`Already at the end of tape`

- 原因

テープにデータが含まれていないか、テープを巻き戻す必要があります。

- 対処方法

テープにデータが含まれていない場合は、バックアップが含まれているテープを使用してリストア ジョブを再試行します。テープにデータが含まれている場合は、テープを巻き戻してリストア ジョブを再試行します。

Tape record size is too small.Try a larger size.

- メッセージ

`Tape record size is too small. Try a larger size.`

- 原因

バックアップ時に使用されたブロック化因数より小さいブロック化因数がリストア処理に指定されました。

- 対処方法

バックアップ時に指定したのと同じブロック化因数を使用します。

Tape record size should be block_size1 and not block_size2

- メッセージ

`Tape record size should be block_size1 and not block_size2`

- 原因

ローカル リストアに指定されたブロック化因数が正しくありません。

- 対処方法

``block_size1``をブロック係数として復元ジョブを再試行します。

Tape record size must be in the range between 4KB and 256KB

- メッセージ

Tape record size must be in the range between 4KB and 256KB

- 原因

バックアップまたはリストア処理に指定されたブロック化因数が、許容範囲内に収まっていません。

- 対処方法

ブロック化因数を、4～256KBの範囲で指定します。

NDMPに関するエラー メッセージ

Network communication error

- メッセージ

Network communication error

- 原因

NDMP 3ウェイ接続でのリモート テープとの通信に失敗しました。

- 対処方法

リモート ムーバーとのネットワーク接続を確認します。

Message from Read Socket: error_string

- メッセージ

Message from Read Socket: error_string

- 原因

NDMP 3ウェイ接続でのリモート テープからのリストア通信でエラーが発生しています。

- 対処方法

リモート ムーバーとのネットワーク接続を確認します。

Message from Write Dirnet: error_string

- メッセージ

Message from Write Dirnet: error_string

- 原因

NDMP 3ウェイ接続でのリモート テープとのバックアップ通信でエラーが発生しています。

- 対処方法

リモート ムーバーとのネットワーク接続を確認します。

Read Socket received EOF

- メッセージ

Read Socket received EOF

- 原因

NDMP 3ウェイ接続でリモート テープとの通信が試行されましたが、ファイルの終わりを示すマークに到達しました。ブロック サイズが大きいバックアップ イメージから3ウェイ リストアを試行している可能性があります。

- 対処方法

正しいブロック サイズを指定して、リストア処理を再試行します。

ndmpd invalid version number: version_number ``

- メッセージ

ndmpd invalid version number: version_number

- 原因

指定したNDMPバージョンがストレージ システムでサポートされていません。

- 対処方法

NDMPバージョン4を指定します。

ndmpd session session_ID not active

- メッセージ

ndmpd session session_ID not active

- 原因

NDMPセッションが存在していない可能性があります。

- 対処方法

``ndmpd status`` コマンドを使用して、アクティブなNDMPセッションを表示します。

Could not obtain vol ref for Volume volume_name

- メッセージ

```
Could not obtain vol ref for Volume vol_name
```

- 原因

ボリュームが他の処理で使用されている可能性があるため、ボリューム参照を取得できませんでした。

- 対処方法

あとで処理を再試行します。

Data connection type ["NDMP4_ADDR_TCP"|"NDMP4_ADDR_TCP_IPv6"] not supported for ["IPv6"|"IPv4"] control connections

- メッセージ

```
Data connection type ["NDMP4_ADDR_TCP"|"NDMP4_ADDR_TCP_IPv6"] not supported  
for ["IPv6"|"IPv4"] control connections
```

- 原因

ノードを対象としたNDMPモードでは、確立されたNDMPデータ接続のネットワーク アドレス タイプ (IPv4またはIPv6) がNDMP制御接続と同じである必要があります。

- 対処方法

バックアップ アプリケーションのベンダーにお問い合わせください。

DATA LISTEN : CABデータ接続準備の前提条件エラー

- メッセージ

```
DATA LISTEN: CAB data connection prepare precondition error
```

- 原因

バックアップ アプリケーションがCAB拡張に関してNDMPサーバとネゴシエートし、NDMP_CAB_DATA_CONN_PREPAREメッセージとNDMP_DATA_LISTENメッセージで指定されているNDMPデータ接続のアドレス タイプが異なる場合、NDMPデータ リスンは失敗します。

- 対処方法

バックアップ アプリケーションのベンダーにお問い合わせください。

DATA CONNECT : CAB データ接続準備の前提条件エラー

- メッセージ

```
DATA CONNECT: CAB data connection prepare precondition error
```

- 原因

バックアップ アプリケーションがCAB拡張に関してNDMPサーバとネゴシエートし、NDMP_CAB_DATA_CONN_PREPAREメッセージとNDMP_DATA_CONNECTメッセージ間で、指定されたNDMPデータ接続のアドレス タイプが一致しない場合は、NDMPデータ接続が失敗します。

- 対処方法

バックアップ アプリケーションのベンダーにお問い合わせください。

Error:show failed: Cannot get password for user '<username>'

- メッセージ

```
Error: show failed: Cannot get password for user '<username>'
```

- 原因

NDMP用のユーザ アカウントの設定が完了していません。

- 対処方法

ユーザ アカウントにSSHのアクセス方式を関連付け、認証方法としてユーザ パスワードを指定します。

ダンプに関するエラー メッセージ

Destination volume is read-only

- メッセージ

```
Destination volume is read-only
```

- 原因

リストア先のパスが読み取り専用です。

- 対処方法

データを別の場所にリストアしてください。

Destination qtree is read-only

- メッセージ

Destination qtree is read-only

- 原因

リストア先のqtreeが読み取り専用です。

- 対処方法

データを別の場所にリストアしてください。

Dumps temporarily disabled on volume, try again

- メッセージ

Dumps temporarily disabled on volume, try again

- 原因

SnapMirrorデスティネーション ボリュームで NDMP ダンプ バックアップが試行されます。このボリュームは `snapmirror break` または `snapmirror resync` 操作の一部です。

- 対処方法

`snapmirror break` または `snapmirror resync` 操作が完了するまで待ってから、ダンプ操作を実行します。



SnapMirrorデスティネーション ボリュームの状態が読み取り / 書き込みから読み取り専用
に、または読み取り専用から読み取り / 書き込みに変わったときは、必ずベースライン バ
ックアップを実行する必要があります。

関連情報

- ["snapmirror break"](#)
- ["snapmirror resync"](#)

NFS labels not recognized

- メッセージ

Error: Aborting: dump encountered NFS security labels in the file system

- 原因

ONTAP 9.9.1以降では、NFSv4.2が有効になっている場合にNFSセキュリティ ラベルがサポートされま
す。ただし、NFSセキュリティ ラベルは現時点でダンプ エンジンでは認識されません。ファイル、ディ
レクトリ、またはその他のダンプ形式のファイルでNFSセキュリティ ラベルが検出されると、ダンプは失

敗します。

- 対処方法

NFSセキュリティ ラベルの付いたファイルやディレクトリがないことを確認します。

No files were created

- メッセージ

```
No files were created
```

- 原因

拡張DAR機能を有効にしないで、ディレクトリDARが試行されました。

- 対処方法

拡張DAR機能を有効にしてから、DARを再試行します。

ファイル<file name>の復元に失敗しました

- メッセージ

```
Restore of the file file name failed
```

- 原因

デスティネーション ボリューム上のLUNと名前が同じファイルのDirect Access Recovery (DAR) が実行された場合、そのDARは失敗します。

- 対処方法

ファイルのDARを再試行します。

src inode <inode number>の切り捨てに失敗しました...

- メッセージ

```
Truncation failed for src inode <inode number>. Error <error number>. Skipping inode.
```

- 原因

ファイルのリストア時に、ファイルのinodeが削除されます。

- 対処方法

ボリューム上のリストア処理が完了するまで待機してから、そのボリュームを使用します。

Unable to lock a snapshot needed by dump

- メッセージ

Unable to lock a snapshot needed by dump

- 原因

バックアップに指定されたSnapshotは利用できません。

- 対処方法

別のスナップショットを使用してバックアップを再試行します。

``snap list`` コマンドを使用して、利用可能なスナップショットのリストを表示します。

``snap list`` の詳細については、link:<https://docs.netapp.com/us-en/ontap-cli/search.html?q=snap+list>["ONTAPコマンド リファレンス"^]を参照してください。

Unable to locate bitmap files

- メッセージ

Unable to locate bitmap files

- 原因

バックアップ処理に必要なビットマップ ファイルが削除されている可能性があります。削除されている場合は、バックアップを再開できません。

- 対処方法

バックアップを再度実行します。

Volume is temporarily in a transitional state

- メッセージ

Volume is temporarily in a transitional state

- 原因

バックアップ対象のボリュームが一時的にマウント解除された状態になっています。

- 対処方法

少し待ってから、再度バックアップを実行します。

SMTapeに関するエラー メッセージ

Chunks out of order

- メッセージ

Chunks out of order

- 原因

バックアップ テープが正しい順序でリストアされていません。

- 対処方法

リストア処理を再試行し、正しい順序でテープを装填します。

Chunk format not supported

- メッセージ

Chunk format not supported

- 原因

SMTapeにバックアップ イメージが含まれていません。

- 対処方法

SMTapeにバックアップ イメージが含まれていない場合は、SMTapeバックアップを含むテープを使用して処理を再試行します。

Failed to allocate memory

- メッセージ

Failed to allocate memory

- 原因

システムのメモリが不足しています。

- 対処方法

システムがあまりビジー状態でないときに、ジョブを再試行します。

Failed to get data buffer

- メッセージ

Failed to get data buffer

- 原因

ストレージ システムのバッファが不足しています。

- 対処方法

ストレージ システムの処理がいくつか完了するのを待ってから、ジョブを再試行します。

Failed to find snapshot

- メッセージ

Failed to find snapshot

- 原因

バックアップに指定されたSnapshotは利用できません。

- 対処方法

指定されたスナップショットが利用可能かどうかを確認してください。利用できない場合は、正しいスナップショットで再試行してください。

Failed to create snapshot

- メッセージ

Failed to create snapshot

- 原因

ボリュームにはすでに最大数の Snapshot が含まれています。

- 対処方法

いくつかのスナップショットを削除してから、バックアップ操作を再試行してください。

Failed to lock snapshot

- メッセージ

Failed to lock snapshot

- 原因

スナップショットは使用中か、削除されています。

- 対処方法

スナップショットが別の操作で使用中の場合は、その操作が完了するまで待ってからバックアップを再試行してください。スナップショットが削除されている場合は、バックアップを実行できません。

Failed to delete snapshot

- メッセージ

Failed to delete snapshot

- 原因

自動スナップショットは他の操作で使用されているため削除できませんでした。

- 対処方法

``snap`` コマンドを使用してスナップショットのステータスを確認します。スナップショットが不要な場合は、手動で削除してください。

Failed to get latest snapshot

- メッセージ

Failed to get latest snapshot

- 原因

ボリュームがSnapMirrorによって初期化されているため、最新のスナップショットが存在しない可能性があります。

- 対処方法

初期化が完了してから再試行します。

Failed to load new tape

- メッセージ

Failed to load new tape

- 原因

テープドライブまたはメディアのエラーです。

- 対処方法

テープを交換して処理を再試行します。

Failed to initialize tape

- メッセージ

Failed to initialize tape

- 原因

このエラー メッセージは、次のいずれかの原因で表示されることがあります。

- SMTapeにバックアップ イメージが含まれていません。
- 指定されたテープ ブロッキング係数が正しくありません。
- テープが破損しているか、損傷しています。
- 復元用に間違ったテープがロードされています。

- 対処方法

- バックアップ イメージが SMTape ではない場合は、SMTape バックアップがあるテープを使用して操作を再試行してください。
- ブロッキング ファクタが正しくない場合は、正しいブロッキング ファクタを指定して操作を再試行してください。
- テープが破損している場合は、リストア処理を実行できません。
- 間違ったテープがロードされている場合は、正しいテープを使用して操作を再試行してください。

Failed to initialize restore stream

- メッセージ

```
Failed to initialize restore stream
```

- 原因

このエラー メッセージは、次のいずれかの原因で表示されることがあります。

- SMTapeにバックアップ イメージが含まれていません。
- 指定されたテープ ブロッキング係数が正しくありません。
- テープが破損しているか、損傷しています。
- 復元用に間違ったテープがロードされています。

- 対処方法

- SMTapeにバックアップ イメージが含まれていない場合は、SMTapeバックアップを含むテープを使用して処理を再試行します。
- ブロッキング ファクタが正しくない場合は、正しいブロッキング ファクタを指定して操作を再試行してください。
- テープが破損している場合は、リストア処理を実行できません。
- 間違ったテープがロードされている場合は、正しいテープを使用して操作を再試行してください。

Failed to read backup image

- メッセージ

```
Failed to read backup image
```

- 原因

テープが破損しています。

- 対処方法

テープが破損している場合は、リストア処理を実行できません。

Image header missing or corrupted

- メッセージ

```
Image header missing or corrupted
```

- 原因

テープに有効なSMTapeバックアップが含まれていません。

- 対処方法

有効なバックアップが含まれているテープを使用して再試行します。

Internal assertion

- メッセージ

```
Internal assertion
```

- 原因

SMTape内部エラーがあります。

- 対処方法

エラーを報告し、etc/log/backup ファイルをテクニカル サポートに送信します。

Invalid backup image magic number

- メッセージ

```
Invalid backup image magic number
```

- 原因

SMTapeにバックアップ イメージが含まれていません。

- 対処方法

SMTapeにバックアップ イメージが含まれていない場合は、SMTapeバックアップを含むテープを使用して処理を再試行します。

Invalid backup image checksum

- メッセージ

Invalid backup image checksum

- 原因

テープが破損しています。

- 対処方法

テープが破損している場合は、リストア処理を実行できません。

Invalid input tape

- メッセージ

Invalid input tape

- 原因

テープ ヘッダー内のバックアップ イメージのシグネチャが有効ではありません。テープ内のデータが破損しているか、テープに有効なバックアップ イメージが含まれていません。

- 対処方法

有効なバックアップ イメージを使用して、リストア ジョブを再試行します。

Invalid volume path

- メッセージ

Invalid volume path

- 原因

バックアップ処理またはリストア処理に指定されたボリュームが見つかりません。

- 対処方法

有効なボリューム パスとボリューム名を指定してジョブを再試行します。

Mismatch in backup set ID

- メッセージ

Mismatch in backup set ID

- 原因

テープ交換時に装填されたテープが、バックアップ セットに含まれるテープではありません。

- 対処方法

正しいテープを装填して、ジョブを再試行します。

Mismatch in backup time stamp

- メッセージ

```
Mismatch in backup time stamp
```

- 原因

テープ交換時に装填されたテープが、バックアップ セットに含まれるテープではありません。

- 対処方法

```
`smtape restore -h` コマンドを使用して、テープのヘッダー情報を確認します。
```

Job aborted due to shutdown

- メッセージ

```
Job aborted due to shutdown
```

- 原因

ストレージ システムをリブート中です。

- 対処方法

ストレージ システムのリブート後にジョブを再試行します。

Snapshot の自動削除によりジョブが中止されました

- メッセージ

```
Job aborted due to snapshot autodelete
```

- 原因

ボリュームに十分なスペースがないため、Snapshotの自動削除がトリガーされました。

- 対処方法

ボリューム内の空きスペースを増やしてから、ジョブを再試行します。

Tape is currently in use by other operations

- メッセージ

Tape is currently in use by other operations

- 原因

テープドライブが別のジョブで使用しています。

- 対処方法

現在アクティブなジョブが完了してから、バックアップを再試行します。

Tapes out of order

- メッセージ

Tapes out of order

- 原因

リストア処理に使用する一連のテープの最初のテープに、イメージ ヘッダーがありません。

- 対処方法

イメージ ヘッダーの付いたテープを装填して、ジョブを再試行します。

Transfer failed (Aborted due to MetroCluster operation)

- メッセージ

Transfer failed (Aborted due to MetroCluster operation)

- 原因

スイッチオーバー処理またはスイッチバック処理が原因で、SMTape処理が中止されます。

- 対処方法

スイッチオーバー処理またはスイッチバック処理が終了したあとにSMTape処理を実行します。

Transfer failed (ARL initiated abort)

- メッセージ

Transfer failed (ARL initiated abort)

- 原因

SMTape処理の実行中にアグリゲートの再配置を開始すると、SMTape処理が中止されます。

- 対処方法

アグリゲートの再配置処理が終了したあとにSMTape処理を実行します。

Transfer failed (CFO initiated abort)

- メッセージ

Transfer failed (CFO initiated abort)

- 原因

CFOアグリゲートのストレージ フェイルオーバー（テイクオーバーとギブバック）処理が原因で、SMTape処理が中止されます。

- 対処方法

CFOアグリゲートのストレージ フェイルオーバーが終了したあとにSMTape処理を実行します。

Transfer failed (SFO initiated abort)

- メッセージ

Transfer failed (SFO initiated abort)

- 原因

ストレージ フェイルオーバー（テイクオーバーとギブバック）処理が原因で、SMTape処理が中止されます。

- 対処方法

ストレージ フェイルオーバー（テイクオーバーとギブバック）処理が終了したあとにSMTape処理を実行します。

Underlying aggregate under migration

- メッセージ

Underlying aggregate under migration

- 原因

移行（ストレージ フェイルオーバーまたはアグリゲートの再配置）を実行中のアグリゲートでSMTape処理が開始されると、そのSMTape処理は失敗します。

- 対処方法

アグリゲートの移行が終了したあとにSMTape処理を実行します。

Volume is currently under migration

- メッセージ

Volume is currently under migration

- 原因

ボリューム移行とSMTapeバックアップは同時に実行できません。

- 対処方法

ボリューム移行が完了してから、バックアップ ジョブを再試行します。

ボリュームはオフライン

- メッセージ

Volume offline

- 原因

バックアップ対象のボリュームがオフラインです。

- 対処方法

ボリュームをオンラインに戻してから、バックアップを再試行します。

Volume not restricted

- メッセージ

Volume not restricted

- 原因

データのリストア先ボリュームが制限されていません。

- 対処方法

ボリュームを制限して、リストア処理を再試行します。

NDMP設定

ONTAP NDMP構成について学ぶ

サードパーティ製バックアップ アプリケーションを使用してデータをテープに直接バックアップするために、Network Data Management Protocol (NDMP) を使用するようにONTAP 9クラスタを設定することができます。

バックアップ アプリケーションがCluster Aware Backup (CAB) をサポートしている場合は、NDMPを_SVMスコープ_または_ノードスコープ_として設定できます：

- クラスタ（管理SVM）レベルでSVMを対象としたNDMPでは、クラスタの各ノードでホストされているすべてのボリュームをバックアップできます。可能な場合は、SVMを対象としたNDMPを設定することを推奨します。

- ノードを対象としたNDMPでは、そのノードでホストされているすべてのボリュームをバックアップできません。

バックアップ アプリケーションでCAB拡張がサポートされていない場合は、ノードを対象としたNDMPを使用する必要があります。

SVMを対象としたNDMPとノードを対象としたNDMPを同時に使用することはできず、同じクラスタに設定することはできません。



ノードを対象としたNDMPは、ONTAP 9で廃止されました。

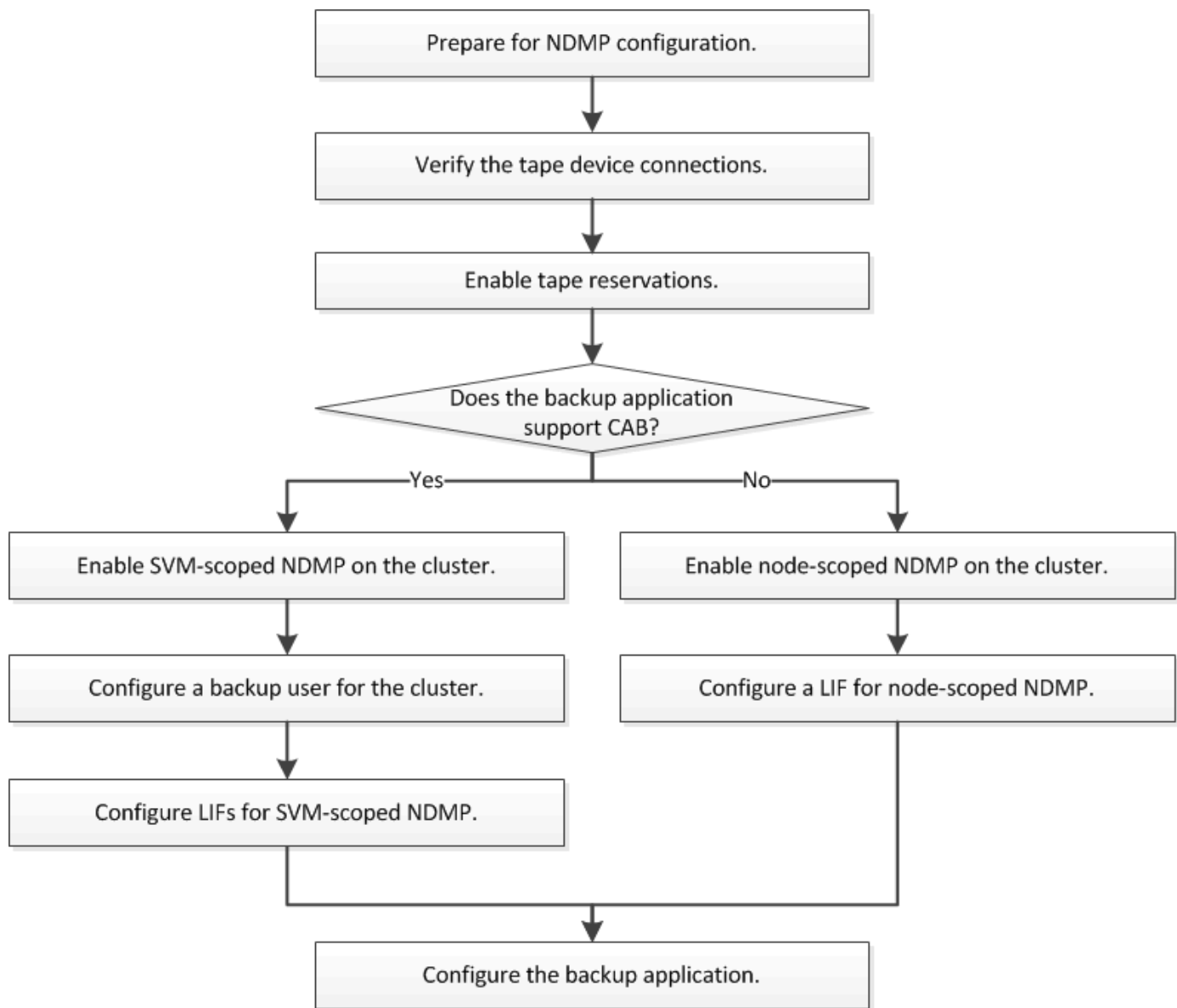
["Cluster Aware Backup \(CAB\) "](#)についての詳細をご覧ください。

NDMPを設定する前に、次の項目を確認してください。

- サードパーティ製バックアップ アプリケーション（データ管理アプリケーションまたはDMAとも呼ばれる）がある。
- マニュアルの利用者はクラスタ管理者である。
- テープ デバイスおよびメディア サーバ（オプション）が導入されている。
- テープ デバイスがクラスタにFibre Channel（FC）スイッチを介して、またはローカルに接続されている。
- 少なくとも1つのテープ デバイスのLogical Unit Number（LUN;論理ユニット番号）が0である。

ONTAP NDMP 構成ワークフローについて学ぶ

NDMPを使用したテープ バックアップのセットアップでは、NDMP構成の準備、テープ デバイスの接続の確認、テープ予約の有効化、SVMまたはノード レベルでのNDMPの設定、クラスタでのNDMPの有効化、バックアップ ユーザの設定、LIFの設定、バックアップ アプリケーションの設定を行います。



ONTAP NDMP構成を準備する

Network Data Management Protocol (NDMP) 経由のテープ バックアップ アクセスを設定する前に、計画した構成がサポートされていること、各ノードでテープドライブが認定ドライブとしてリストされていること、すべてのノードにクラスタ間LIFがあることを確認し、バックアップ アプリケーションがCluster Aware Backup (CAB) 拡張をサポートしているかどうかを確認する必要があります。

手順

1. ONTAPがサポートされているかどうかを、バックアップ アプリケーション プロバイダの互換性マトリックスで参照します (NetAppはONTAPまたはNDMPでの他社製バックアップ アプリケーションの使用を認定していません)。

次のNetAppコンポーネントに互換性があることを確認する必要があります。

- 。クラスタ上で実行されているONTAP 9のバージョン。

- バックアップ アプリケーション ベンダーとバージョン：たとえば、Veritas NetBackup 8.2またはCommVault。
- テープ デバイスの詳細（テープ ドライブの製造元、モデル、インターフェイスなど）：たとえば、IBM Ultrium 8 または HPe StoreEver Ultrium 30750 LTO-8。
- クラスター内のノードのプラットフォーム：たとえば、FAS8700またはA400。



バックアップ アプリケーションの従来のONTAP互換性サポート マトリックスは ["NetApp Interoperability Matrix Tool"](#)で確認できます。

2. 各ノードの組み込みのテープ構成ファイルにテープ ドライブが認定ドライブとしてリストされていることを確認します。

- a. コマンド ライン インターフェイスで、`storage tape show-supported-status` コマンドを使用して組み込みのテープ構成ファイルを表示します。

```
cluster1::> storage tape show-supported-status

Node: cluster1-1

Tape Drives                                Is Supported   Support Status
-----
Certance Ultrium 2                         true          Dynamically Qualified
Certance Ultrium 3                         true          Dynamically Qualified
Digital DLT2000                            true          Qualified
```

- b. テープ ドライブを出力に表示された認定ドライブのリストと比較します。



出力に表示されるテープ デバイスの名前は、デバイス ラベルまたはInteroperability Matrixに表示された名前と多少異なる場合があります。たとえば、Digital DLT2000 はDLT2kと表示されることもあります。このような小さな名前の違いは無視してかまいません。

- c. デバイスがInteroperability Matrixでは認定されているにもかかわらず、出力に認定デバイスとしてリストされない場合は、NetApp サポート サイトの手順に従って、デバイスの更新された構成ファイルをダウンロードしてインストールします。

"NetAppのダウンロード：テープ デバイスの構成ファイル"

ノードの出荷後にテープ デバイスが認定された場合、認定デバイスが組み込みのテープ構成ファイルにリストされていないことがあります。

3. クラスタ内のすべてのノードにクラスタ間LIFがあることを確認します。

- a. `network interface show -role intercluster` コマンドを使用して、ノード上のクラスタ間LIFを表示します。

```
cluster1::> network interface show -role intercluster
```

	Logical	Status	Network	Current
Current Is				
Vserver	Interface	Admin/Oper	Address/Mask	Node
Port	Home			
-----	-----	-----	-----	-----
-----	-----	-----	-----	-----
cluster1	IC1	up/up	192.0.2.65/24	cluster1-1
e0a	true			

`network interface show`

の詳細については、link:<https://docs.netapp.com/us-en/ontap-cli/network-interface-show.html>["ONTAPコマンド リファレンス"]を参照してください。

- b. どのノードにもクラスタ間 LIF が存在しない場合は、network interface create コマンドを使用してクラスタ間 LIF を作成します。

```
cluster1::> network interface create -vserver cluster1 -lif IC2 -role
intercluster
-home-node cluster1-2 -home-port e0b -address 192.0.2.68 -netmask
255.255.255.0
-status-admin up -failover-policy local-only -firewall-policy
intercluster
```

```
cluster1::> network interface show -role intercluster
```

	Logical	Status	Network	Current
Current Is				
Vserver	Interface	Admin/Oper	Address/Mask	Node
Port	Home			
-----	-----	-----	-----	-----
-----	-----	-----	-----	-----
cluster1	IC1	up/up	192.0.2.65/24	cluster1-1
e0a	true			
cluster1	IC2	up/up	192.0.2.68/24	cluster1-2
e0b	true			

`network interface create`

の詳細については、link:<https://docs.netapp.com/us-en/ontap-cli/network-interface-create.html>["ONTAPコマンド リファレンス"]を参照してください。

4. バックアップ アプリケーションに付属のドキュメントを参照して、バックアップ アプリケーションがCluster Aware Backup (CAB) をサポートしているかどうかを確認します。

CABのサポートは、実行できるバックアップの種類に影響する重要な要素です。

関連情報

- ["storage tape show"](#)
- ["storage tape show-supported-status"](#)

ONTAP NDMPテープ デバイス接続を確認する

すべてのドライブとメディア チェンジャーがONTAPでデバイスとして表示されることを確認する必要があります。

手順

1. `storage tape show` コマンドを使用して、すべてのドライブとメディア チェンジャーに関する情報を表示します。

```
cluster1::> storage tape show
```

```
Node: cluster1-01
```

Device ID	Device Type	Description

Status		

-----	-----	-----

sw4:10.11	tape drive	HP LTO-3

normal		

0b.125L1	media changer	HP MSL G3 Series

normal		

0d.4	tape drive	IBM LTO 5 ULT3580

normal		

0d.4L1	media changer	IBM 3573-TL

normal		

...		

2. テープ ドライブが表示されない場合は、問題のトラブルシューティングを行ってください。
3. メディア チェンジャーが表示されない場合は、`storage tape show-media-changer` コマンドを使用してメディア チェンジャーに関する情報を表示し、問題のトラブルシューティングを行います。


```
cluster1::> storage tape show-media-changer
```

```
Media Changer: sw4:10.11L1
```

```
Description: PX70-TL
```

```
WWNN: 2:00a:000e11:10b919
```

```
WWPN: 2:00b:000e11:10b919
```

```
Serial Number: 00FRU7800000_LL1
```

```
Errors: -
```

```
Paths:
```

```
Node Initiator Alias Device State
```

```
Status
```

```
-----
```

```
cluster1-01 2b mc0 in-use
```

```
normal
```

```
...
```

関連情報

- ["storage tape show-media-changer"](#)

ONTAP NDMPバックアップ操作のテープ予約を有効にする

NDMPバックアップ処理用のバックアップ アプリケーションで使用するために、テープドライブが予約されていることを確認する必要があります。

タスク概要

予約設定はバックアップ アプリケーションによって異なり、これらの設定はバックアップ アプリケーションと、同じドライブを使用するノードまたはサーバーに一致する必要があります。正しい予約設定については、バックアップ アプリケーションのベンダーのドキュメントを参照してください。

手順

1. `options -option-name tape.reservations -option-value persistent` コマンドを使用して予約を有効にします。

次のコマンドは、`persistent` 値で予約を有効にします：

```
cluster1::> options -option-name tape.reservations -option-value  
persistent  
2 entries were modified.
```

2. `options tape.reservations` コマンドを使用して、すべてのノードで予約が有効になっていることを確認し、出力を確認します。

```
cluster1::> options tape.reservations

cluster1-1
  tape.reservations          persistent

cluster1-2
  tape.reservations          persistent
2 entries were displayed.
```

SVMを対象としたNDMPの設定

ONTAPクラスタでSVMスコープのNDMPを有効にする

DMAがCluster Aware Backup (CAB) 拡張をサポートしている場合は、SVMを対象としたNDMPを有効にし、クラスタ（管理SVM）でNDMPサービスを有効にして、データ接続と制御接続に使用するLIFを設定することで、クラスタの各ノードでホストされているすべてのボリュームをバックアップできます。

開始する前に

DMAでCAB拡張がサポートされている必要があります。

タスク概要

ノードを対象としたNDMPモードをオフにすると、クラスタでSVMを対象としたNDMPモードが有効になります。

手順

1. SVMを対象としたNDMPモードを有効にします。

```
cluster1::> system services ndmp node-scope-mode off
```

SVMを対象としたNDMPモードが有効になります。

2. 管理SVMでNDMPサービスを有効にします。

```
cluster1::> vserver services ndmp on -vserver cluster1
```

認証タイプはデフォルトで `challenge` に設定されており、プレーンテキスト認証は無効になっています。



セキュアな通信のために、プレーンテキスト認証は無効にしておく必要があります。

3. NDMPサービスが有効になっていることを確認します。

```
cluster1::> vserver services ndmp show
```

Vserver	Enabled	Authentication type
-----	-----	-----
cluster1	true	challenge
vs1	false	challenge

ONTAP NDMP認証のバックアップ ユーザーを有効にする

バックアップ アプリケーションからSVMを対象としたNDMPを認証するには、十分な権限とNDMPパスワードを持つ管理ユーザが必要です。

タスク概要

バックアップの管理ユーザ用にNDMPパスワードを生成する必要があります。バックアップの管理ユーザはクラスタ レベルまたはSVMレベルで有効にすることができます。必要に応じて、新しいユーザを作成することもできます。デフォルトでは、次のロールを持つユーザがNDMPバックアップを認証できます。

- クラスタ全体: admin または backup
- 個別 SVM: vsadmin または vsadmin-backup

NISユーザまたはLDAPユーザを使用している場合は、それぞれのサーバにユーザが存在している必要があります。Active Directoryユーザは使用できません。

手順

1. 現在の管理ユーザと権限を表示します。

```
security login show
```

`security login show`の詳細については、link:<https://docs.netapp.com/us-en/ontap-cli/security-login-show.html>["ONTAPコマンド リファレンス"]を参照してください。

2. 必要に応じて、`security login create`コマンドとクラスタ全体または個々の SVM 権限の適切なロールを使用して、新しい NDMP バックアップ ユーザーを作成します。

`-user-or-group-name`パラメータには、ローカル バックアップ ユーザー名、NIS または LDAP ユーザー名を指定できます。

次のコマンドは、クラスタ全体の `backup` ロールを持つバックアップ ユーザー `backup\_admin1`を作成します：

```
cluster1::> security login create -user-or-group-name backup_admin1  
-application ssh -authmethod password -role backup
```

次のコマンドは、個々の SVM の `vsadmin-backup` ロールを持つバックアップ ユーザー `vsbackup\_admin1` を作成します：

```
cluster1::> security login create -user-or-group-name vsbackup_admin1  
-application ssh -authmethod password -role vsadmin-backup
```

新しいユーザのパスワードを入力し、確認のためにもう一度入力します。

`security login create`の詳細については、[link:https://docs.netapp.com/us-en/ontap-cli/security-login-create.html](https://docs.netapp.com/us-en/ontap-cli/security-login-create.html) ["ONTAP コマンド リファレンス"] をご覧ください。

3. `vserver services ndmp generate password` コマンドを使用して、管理SVMのパスワードを生成します。

生成されたパスワードは、バックアップ アプリケーションによるNDMP接続の認証で必要になります。

```
cluster1::> vserver services ndmp generate-password -vserver cluster1  
-user backup_admin1  
  
Vserver: cluster1  
User: backup_admin1  
Password: qG5CqQHYxw7tE57g
```

SVM スコープの NDMP 用に ONTAP LIF を設定する

データとテープのリソース間のデータ接続、および管理SVMとバックアップ アプリケーションの間の制御接続の確立に使用されるLIFを特定する必要があります。LIFを特定したら、サービス ポリシーとフェイルオーバー ポリシーが設定されていることを確認する必要があります。



ONTAP 9.10.1以降、ファイアウォール ポリシーは廃止され、LIFサービス ポリシーに完全に置き換えられました。詳細については、"[サポートされるトラフィックの管理](#)"を参照してください。

ONTAP 9.10.1 以降

手順

1. `network interface show` コマンドに `-service-policy` パラメータを指定して、ノード上でホストされているクラスタ間 LIF を識別します。

```
network interface show -service-policy default-intercluster
```

```
`network interface show`
```

の詳細については、[link:https://docs.netapp.com/us-en/ontap-cli/network-interface-show.html](https://docs.netapp.com/us-en/ontap-cli/network-interface-show.html) ["ONTAP コマンド リファレンス"] を参照してください。

2. `-service-policy` パラメータを指定した `network interface show` コマンドを使用して、ノード上でホストされている管理 LIF を識別します。

```
network interface show -service-policy default-management
```

3. クラスタ間 LIF に `backup-ndmp-control` サービスが含まれていることを確認します：

```
network interface service-policy show
```

```
`network interface service-policy show`
```

の詳細については、[link:https://docs.netapp.com/us-en/ontap-cli/network-interface-service-policy-show.html](https://docs.netapp.com/us-en/ontap-cli/network-interface-service-policy-show.html) ["ONTAP コマンド リファレンス"] を参照してください。

4. すべての LIF のフェイルオーバー ポリシーが適切に設定されていることを確認します。
 - a. `network interface show -failover` コマンドを使用して、クラスタ管理 LIF のフェイルオーバー ポリシーが `broadcast-domain-wide` に設定され、クラスタ間 LIF と ノード管理 LIF のポリシーが `local-only` に設定されていることを確認します。

次のコマンドは、クラスタ管理 LIF、クラスタ間 LIF、および ノード管理 LIF のフェイルオーバー ポリシーを表示します。

```
cluster1::> network interface show -failover
```

Vserver	Logical Interface	Home Node:Port	Failover Policy	Failover Group
cluster	cluster1_clus1	cluster1-1:e0a	local-only	cluster Failover
Targets:				
cluster1	cluster_mgmt	cluster1-1:e0m	broadcast-domain-wide	Default Failover
Targets:				
	IC1	cluster1-1:e0a	local-only	Default Failover
Targets:				
	IC2	cluster1-1:e0b	local-only	Default Failover
Targets:				
cluster1-1	c1-1_mgmt1	cluster1-1:e0m	local-only	Default Failover
Targets:				
cluster1-2	c1-2_mgmt1	cluster1-2:e0m	local-only	Default Failover
Targets:				

- a. フェイルオーバー ポリシーが適切に設定されていない場合は、`-failover-policy` パラメータを指定した `network interface modify` コマンドを使用してフェイルオーバー ポリシーを変更します。

```
cluster1::> network interface modify -vserver cluster1 -lif IC1
-failover-policy local-only
```

```
`network interface modify`
```

の詳細については、[link:https://docs.netapp.com/us-en/ontap-cli/network-interface-modify.html](https://docs.netapp.com/us-en/ontap-cli/network-interface-modify.html) ["ONTAP コマンド リファレンス"] を参照してください。

5. `vserver services ndmp modify` コマンドに `preferred-interface-role` パラメータを指定して、データ接続に必要な LIF を指定します。

```
cluster1::> vserver services ndmp modify -vserver cluster1
-preferred-interface-role intercluster,cluster-mgmt,node-mgmt
```

6. `vserver services ndmp show` コマンドを使用して、クラスタに優先インターフェイス ロールが設定されていることを確認します。

```
cluster1::> vserver services ndmp show -vserver cluster1

Vserver: cluster1
NDMP Version: 4
.....
.....
Preferred Interface Role: intercluster, cluster-mgmt, node-mgmt
```

ONTAP 9.9以前

手順

1. `network interface show` コマンドに `-role` パラメータを指定して、クラスタ間LIF、クラスタ管理LIF、およびノード管理LIFを特定します。

次のコマンドは、クラスタ間LIFを表示します。

```
cluster1::> network interface show -role intercluster
```

Current Is	Logical	Status	Network	Current
Vserver	Interface	Admin/Oper	Address/Mask	Node
Port	Home			
-----	-----	-----	-----	-----
-----	-----			
cluster1	IC1	up/up	192.0.2.65/24	cluster1-1
e0a	true			
cluster1	IC2	up/up	192.0.2.68/24	cluster1-2
e0b	true			

次のコマンドは、クラスタ管理LIFを表示します。

```
cluster1::> network interface show -role cluster-mgmt
```

	Logical	Status	Network	Current
Current Is				
Vserver	Interface	Admin/Oper	Address/Mask	Node
Port	Home			
-----	-----	-----	-----	-----
-----	-----	-----	-----	-----
cluster1	cluster_mgmt	up/up	192.0.2.60/24	cluster1-2
e0M	true			

次のコマンドは、ノード管理LIFを表示します。

```
cluster1::> network interface show -role node-mgmt
```

	Logical	Status	Network	Current
Current Is				
Vserver	Interface	Admin/Oper	Address/Mask	Node
Port	Home			
-----	-----	-----	-----	-----
-----	-----	-----	-----	-----
cluster1	cluster1-1_mgmt1	up/up	192.0.2.69/24	cluster1-1
e0M	true			
	cluster1-2_mgmt1	up/up	192.0.2.70/24	cluster1-2
e0M	true			

```
`network interface show`
```

の詳細については、link:<https://docs.netapp.com/us-en/ontap-cli/network-interface-show.html>["ONTAPコマンド リファレンス"]を参照してください。

2. クラスタ間LIF、クラスタ管理(`cluster-mgmt` LIF、ノード管理(`node-mgmt` LIFでNDMPのファイアウォール ポリシーが有効になっていることを確認します：
 - a. `system services firewall policy show` コマンドを使用して、ファイアウォール ポリシーが NDMP に対して有効になっていることを確認します。

次のコマンドは、クラスタ管理LIFのファイアウォール ポリシーを表示します。


```
cluster1::> system services firewall policy show -policy cluster
```

Vserver	Policy	Service	Allowed
cluster	cluster	dns	0.0.0.0/0
		http	0.0.0.0/0
		https	0.0.0.0/0
		ndmp	0.0.0.0/0
		ndmps	0.0.0.0/0
		ntp	0.0.0.0/0
		rsh	0.0.0.0/0
		snmp	0.0.0.0/0
		ssh	0.0.0.0/0
		telnet	0.0.0.0/0

10 entries were displayed.

次のコマンドは、クラスタ間LIFのファイアウォール ポリシーを表示します。

```
cluster1::> system services firewall policy show -policy  
intercluster
```

Vserver	Policy	Service	Allowed
cluster1	intercluster	dns	-
		http	-
		https	-
		ndmp	0.0.0.0/0, ::/0
		ndmps	-
		ntp	-
		rsh	-
		ssh	-
		telnet	-

9 entries were displayed.

次のコマンドは、ノード管理LIFのファイアウォール ポリシーを表示します。

```
cluster1::> system services firewall policy show -policy mgmt
```

Vserver	Policy	Service	Allowed
cluster1-1	mgmt	dns	0.0.0.0/0, ::/0
		http	0.0.0.0/0, ::/0
		https	0.0.0.0/0, ::/0
		ndmp	0.0.0.0/0, ::/0
		ndmps	0.0.0.0/0, ::/0
		ntp	0.0.0.0/0, ::/0
		rsh	-
		snmp	0.0.0.0/0, ::/0
		ssh	0.0.0.0/0, ::/0
		telnet	-

10 entries were displayed.

- b. ファイアウォール ポリシーが有効になっていない場合は、`-service`パラメータを指定した `system services firewall policy modify` コマンドを使用してファイアウォール ポリシーを有効にします。

次のコマンドは、クラスタ間LIFのファイアウォール ポリシーを有効にします。

```
cluster1::> system services firewall policy modify -vserver cluster1  
-policy intercluster -service ndmp 0.0.0.0/0
```

3. すべてのLIFのフェイルオーバー ポリシーが適切に設定されていることを確認します。
- a. `network interface show -failover` コマンドを使用して、クラスタ管理LIFのフェイルオーバー ポリシーが `broadcast-domain-wide` に設定され、クラスタ間LIFとノード管理LIFのポリシーが `local-only` に設定されていることを確認します。

次のコマンドは、クラスタ管理LIF、クラスタ間LIF、およびノード管理LIFのフェイルオーバー ポリシーを表示します。

```
cluster1::> network interface show -failover
```

Failover Vserver Group	Logical Interface	Home Node:Port	Failover Policy
cluster1 cluster	cluster1_clus1	cluster1-1:e0a	local-only
			Failover
Targets:			
cluster1 cluster	cluster_mgmt	cluster1-1:e0m	broadcast-domain-wide Default
			Failover
Targets:			
cluster1 Default	IC1	cluster1-1:e0a	local-only
			Failover
Targets:			
cluster1 Default	IC2	cluster1-1:e0b	local-only
			Failover
Targets:			
cluster1-1 Default	cluster1-1_mgmt1	cluster1-1:e0m	local-only
			Failover
Targets:			
cluster1-2 Default	cluster1-2_mgmt1	cluster1-2:e0m	local-only
			Failover
Targets:			

- a. フェイルオーバー ポリシーが適切に設定されていない場合は、`-failover-policy`パラメータを指定した `network interface modify` コマンドを使用してフェイルオーバー ポリシーを変更します。

```
cluster1::> network interface modify -vserver cluster1 -lif IC1
-failover-policy local-only
```

```
`network interface modify`
```

の詳細については、[link:https://docs.netapp.com/us-en/ontap-cli/network-interface-modify.html](https://docs.netapp.com/us-en/ontap-cli/network-interface-modify.html)["ONTAPコマンド リファレンス"]を参照してください。

4. `vserver services ndmp modify` コマンドに `preferred-interface-role` パラメータを指定して、データ接続に必要なLIFを指定します。

```
cluster1::> vserver services ndmp modify -vserver cluster1  
-preferred-interface-role intercluster,cluster-mgmt,node-mgmt
```

5. `vserver services ndmp show` コマンドを使用して、クラスタに優先インターフェイス ロールが設定されていることを確認します。

```
cluster1::> vserver services ndmp show -vserver cluster1  
  
Vserver: cluster1  
NDMP Version: 4  
.....  
.....  
Preferred Interface Role: intercluster, cluster-mgmt,  
node-mgmt
```

ノードを対象としたNDMPの設定

ONTAPクラスタでノードスコープのNDMPを有効にする

単一のノードでホストされているボリュームをバックアップするには、ノードを対象としたNDMPを有効にし、NDMPサービスを有効にして、データ接続と制御接続に使用するLIFを設定します。この処理は、クラスタのすべてのノードに対して実行できます。



ノードを対象としたNDMPは、ONTAP 9で廃止されました。

タスク概要

NDMPをノードスコープモードで使用する場合、認証はノードごとに設定する必要があります。詳細については、["ナレッジベースの記事「ノードスコープモードでNDMP認証を構成する方法」"](#)を参照してください。

手順

1. ノードを対象としたNDMPモードを有効にします。

```
cluster1::> system services ndmp node-scope-mode on
```

NDMPのnode-scope-modeが有効になります。

2. クラスタ内のすべてのノードでNDMPサービスを有効にします。

ワイルドカード「*」を使用すると、すべてのノードで同時にNDMPサービスが有効になります。

バックアップ アプリケーションによるNDMP接続の認証でパスワードを指定する必要があります。

```
cluster1::> system services ndmp on -node *
```

```
Please enter password:
Confirm password:
2 entries were modified.
```

3. NDMPパスワードの安全な通信のための`-clear-text`オプションを無効にします：

ワイルドカード “*” disables the -clear-text オプションをすべてのノードで同時に使用します。

```
cluster1::> system services ndmp modify -node * -clear-text false
```

4. NDMPサービスが有効になっていて、-clear-text オプションが無効になっていることを確認します：

```
cluster1::> system services ndmp show
```

Node	Enabled	Clear text	User Id
cluster1-1	true	false	root
cluster1-2	true	false	root

2 entries were displayed.

ノード スコープ **NDMP** 用に **ONTAP LIF** を構成する

ノードとバックアップ アプリケーションの間のデータ接続と制御接続の確立に使用されるLIFを特定する必要があります。LIFを特定したら、そのLIFに対してファイアウォールポリシーとフェイルオーバー ポリシーが設定されていることを確認する必要があります。



ONTAP 9.10.1以降、ファイアウォール ポリシーは廃止され、LIFサービス ポリシーに完全に置き換えられました。詳細については、"[サポートされるトラフィックの管理](#)"を参照してください。

ONTAP 9.10.1 以降

手順

1. `network interface show` コマンドに `-service-policy` パラメータを指定して、ノード上でホストされているクラスタ間 LIF を識別します。

```
network interface show -service-policy default-intercluster
```

2. クラスタ間 LIF に `backup-ndmp-control` サービスが含まれていることを確認します：

```
network interface service-policy show
```

3. クラスタ間 LIF のフェイルオーバー ポリシーが適切に設定されていることを確認します。

- a. `network interface show -failover` コマンドを使用して、クラスタ間 LIF のフェイルオーバー ポリシーが `local-only` に設定されていることを確認します。

```
cluster1::> network interface show -failover
```

	Logical	Home	Failover	
Failover				
Vserver	Interface	Node:Port	Policy	Group
-----	-----	-----	-----	
cluster1	IC1	cluster1-1:e0a	local-only	
Default				
			Failover	
Targets:				
	IC2	cluster1-2:e0b	local-only	
Default				
			Failover	
Targets:				
cluster1-1	cluster1-1_mgmt1	cluster1-1:e0m	local-only	
Default				
			Failover	
Targets:				

- b. フェイルオーバー ポリシーが適切に設定されていない場合は、`-failover-policy` パラメータを指定した `network interface modify` コマンドを使用してフェイルオーバー ポリシーを変更します。

```
cluster1::> network interface modify -vserver cluster1 -lif IC1  
-failover-policy local-only
```

`network interface show`、`network interface service-policy show`、および `network interface modify`
の詳細については、link:<https://docs.netapp.com/us-en/ontap-cli/search.html?q=network+interface>["ONTAPコマンド リファレンス"]をご覧ください。

ONTAP 9.9以前

手順

1. `network interface show` コマンドに `-role` パラメータを指定して、ノード上でホストされているクラスタ間 LIF を識別します。

```
cluster1::> network interface show -role intercluster
```

	Logical	Status	Network	Current
Current Is				
Vserver	Interface	Admin/Oper	Address/Mask	Node
Port	Home			
-----	-----	-----	-----	-----
cluster1	IC1	up/up	192.0.2.65/24	cluster1-1
e0a	true			
cluster1	IC2	up/up	192.0.2.68/24	cluster1-2
e0b	true			

2. クラスタ間LIFでNDMPに対してファイアウォール ポリシーが有効になっていることを確認します。
 - a. `system services firewall policy show` コマンドを使用して、ファイアウォール ポリシーが NDMP に対して有効になっていることを確認します。

次のコマンドは、クラスタ間LIFのファイアウォール ポリシーを表示します。

```
cluster1::> system services firewall policy show -policy
intercluster
```

Vserver	Policy	Service	Allowed
cluster1	intercluster	dns	-
		http	-
		https	-
		ndmp	0.0.0.0/0, ::/0
		ndmps	-
		ntp	-
		rsh	-
		ssh	-
		telnet	-

9 entries were displayed.

- b. ファイアウォール ポリシーが有効になっていない場合は、`-service`パラメータを指定した `system services firewall policy modify` コマンドを使用してファイアウォール ポリシーを有効にします。

次のコマンドは、クラスタ間LIFのファイアウォール ポリシーを有効にします。

```
cluster1::> system services firewall policy modify -vserver cluster1
-policy intercluster -service ndmp 0.0.0.0/0
```

3. クラスタ間LIFのフェイルオーバー ポリシーが適切に設定されていることを確認します。

- a. `network interface show -failover` コマンドを使用して、クラスタ間 LIF のフェイルオーバー ポリシーが `local-only` に設定されていることを確認します。


```
cluster1::> network interface show -failover
```

Failover	Logical	Home	Failover	
Vserver	Interface	Node:Port	Policy	Group
cluster1	IC1	cluster1-1:e0a	local-only	
Default				Failover
Targets:				
	IC2	cluster1-2:e0b	local-only	
Default				Failover
Targets:				
cluster1-1	cluster1-1_mgmt1	cluster1-1:e0m	local-only	
Default				Failover
Targets:				

- b. フェイルオーバー ポリシーが適切に設定されていない場合は、`-failover-policy`パラメータを指定した `network interface modify` コマンドを使用してフェイルオーバー ポリシーを変更します。

```
cluster1::> network interface modify -vserver cluster1 -lif IC1
-failover-policy local-only
```

`network interface show` および `network interface modify` の詳細については、[link:https://docs.netapp.com/us-en/ontap-cli/search.html?q=network+interface](https://docs.netapp.com/us-en/ontap-cli/search.html?q=network+interface) ["ONTAP コマンド リファレンス"] をご覧ください。

ONTAP NDMP 構成用のバックアップ アプリケーションを構成する

クラスターを NDMP アクセス用に構成した後、クラスター構成から情報を収集し、バックアップ アプリケーションで残りのバックアップ プロセスを構成する必要があります。

手順

1. 以前に ONTAP で設定した次の情報を収集します：
 - 。バックアップ アプリケーションが NDMP 接続を作成するために必要なユーザー名とパスワード

。バックアップアプリケーションがクラスタに接続するために必要なクラスタ間 LIF の IP アドレス

2. ONTAP で、`storage tape alias show` コマンドを使用して、ONTAP が各デバイスに割り当てたエイリアスを表示します。

エイリアスは、バックアップアプリケーションの設定に役立つことがよくあります。

```
cluster1::> storage tape show -alias
```

```
Device ID: 2a.0
Device Type: tape drive
Description: Hewlett-Packard LTO-5
```

Node	Alias	Mapping
-----	-----	-----
stsw-3220-4a-4b-02	st2	SN[HU19497WVR]
...		

3. バックアップアプリケーションで、バックアップアプリケーションのドキュメントを使用して、残りのバックアッププロセスを設定します。

終了後の操作

ボリュームの移動や LIF の移行などのデータ移動イベントが発生した場合は、中断されたバックアップ操作を再初期化する準備をする必要があります。

関連情報

- ["storage tape エイリアスの表示"](#)

NetApp ElementソフトウェアとONTAPのレプリケーション - 概要

SnapMirrorを使用してElementボリュームのスナップショットをONTAP宛先に複製することで、Elementシステムにおけるビジネス継続性を確保できます。Elementサイトで災害が発生した場合は、ONTAPシステムからクライアントにデータを提供した後、サービスが復旧したらElementシステムを再アクティブ化できます。

ONTAP 9.4以降では、ONTAPノードで作成されたLUNのスナップショットをElementシステムに複製できます。Elementサイトの停止中にLUNを作成したか、LUNを使用してONTAPからElementソフトウェアにデータを移行している可能性があります。

["NetApp Element ソフトウェアと ONTAP のレプリケーションの設定"](#)。

著作権に関する情報

Copyright © 2026 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。