



# ONTAP 9 ドキュメント

## ONTAP 9

NetApp  
April 24, 2024

# 目次

ONTAP 9ドキュメント	1
リリースノート	2
ONTAP 9リリースのハイライト	2
ONTAP 9リリースのサポート	7
ONTAP 9.14.1の新機能	8
ONTAP 9.13.1の新機能	13
ONTAP 9.12.1の新機能	18
ONTAP 9.11.1の新機能	23
ONTAP 9.10.1の新機能	28
ONTAP 9.9.1の新機能	32
System ManagerとBlueXPの統合	38
BlueXPからクラスタを直接検出します	38
BlueXPの詳細をご覧ください	39
概要と概念	40
ONTAP の概念	40
ONTAPソフトウェアとファームウェアのセットアップ、アップグレード、リバート	90
ONTAPのセットアップ	90
ONTAPのアップグレード	107
ファームウェアおよびシステムの更新	244
ONTAP をリバートする	250
クラスタ管理	284
System Manager を使用したクラスタ管理	284
ライセンス管理	300
CLI を使用したクラスタ管理	310
ディスクと階層（アグリゲート）の管理	427
FabricPool 階層の管理	525
SVM のデータ移動	582
HAペアの管理	593
System Manager を使用した REST API の管理	618
ボリューム管理	622
ボリュームと LUN の管理には System Manager を使用します	622
CLI を使用した論理ストレージ管理	646
FlexGroup を使用して大規模ファイルシステム用の NAS ストレージをプロビジョニング	788
FlexGroup ボリュームの管理には CLI を使用します	790
FlexCache ボリューム管理	880
Network Management の略	900
はじめに	900
ネットワークコンポーネント	904
NASパスのフェイルオーバーワークフロー（ONTAP 9.8以降）	909

NASパスのフェイルオーバーワークフロー（ONTAP 9.7以前）	918
ネットワークポート	933
IPspace	958
ブロードキャストドメイン	965
フェイルオーバーグループとポリシー	988
サブネット（クラスタ管理者のみ）	992
SVMs を作成します	1000
論理インターフェイス（LIF）	1008
ネットワーク負荷の分散	1039
ホストメイカイケツ	1048
ネットワークを保護します	1051
QoSマーキング（クラスタ管理者のみ）	1066
SNMPの管理（クラスタ管理者のみ）	1068
SVM のルーティングを管理します	1079
ネットワーク情報を表示します	1084
NAS ストレージ管理	1118
System Manager を使用して NAS プロトコルを管理します	1118
CLI で NFS を設定	1139
CLIを使用したNFSの管理	1210
NFSトランッキングを管理します。	1331
RDMA 経由の NFS を管理します	1341
CLI を使用して SMB を設定します	1347
CLIを使用したSMBの管理	1391
NASデータへのS3クライアントアクセスを提供	1751
Microsoft Hyper-V および SQL Server 向けの SMB の設定	1761
SANストレージ管理	1822
SANの概念	1822
SAN 管理	1846
SANのデータ保護	1921
SAN 構成リファレンス	1942
S3 オブジェクトストレージの管理	1987
ONTAP 9でのS3サポートの詳細	1987
計画	1990
設定	1995
S3 SnapMirror でバケットを保護します	2045
S3 イベントを監査します	2080
認証とアクセス制御	2090
ニンシヨウトアクセスセイキヨノカイヨウ	2090
管理者認証とRBACの管理	2090
OAuth 2.0を使用した認証と許可	2172
SAML 認証を設定する	2194

Web サービスを管理します	2201
証明書を使用してリモートサーバの ID を確認します	2211
クラスタとKMIPサーバの相互認証	2215
セキュリティとデータ暗号化	2219
System Manager によるセキュリティ管理の概要	2219
ランサムウェアからデータを保護	2219
ウイルスから保護	2244
SVM で NAS イベントを監査します	2286
SVM で FPolicy を使用してファイルを監視および管理します	2334
セキュリティトレースを使用したアクセスの確認	2396
System Manager を使用して暗号化を管理します	2409
CLI を使用して暗号化を管理します	2410
データ保護とディザスタリカバリ	2505
System Manager によるデータ保護	2505
CLI を使用したクラスタと SVM のピアリング	2520
ローカル Snapshot コピーを管理します	2547
SnapMirror ボリュームのレプリケーション	2560
SnapMirror ボリュームレプリケーションを管理します	2580
SnapMirror SVM レプリケーションを管理します	2623
SnapMirror ルートボリュームのレプリケーションを管理します	2656
SnapMirror の技術的な詳細	2660
SnapLock テクノロジーを使用したアーカイブとコンプライアンス	2668
整合グループ	2712
SnapMirror によるビジネス継続性	2750
MetroCluster および SnapMirror のビジネス継続性用のメディアエーターサービス	2785
System Manager を使用して MetroCluster サイトを管理する	2841
テープバックアップによるデータ保護	2852
NDMP構成	2949
NetApp Element ソフトウェアと ONTAP 間のレプリケーション	2966
イベント、パフォーマンス、健全性の監視	2988
System Managerを使用してクラスタパフォーマンスを監視する	2988
CLIを使用してクラスタパフォーマンスを監視および管理します	2998
Unified Manager を使用してクラスタパフォーマンスを監視する	3037
Cloud Insights を使用してクラスタパフォーマンスを監視する	3037
監査ロギング	3038
AutoSupport	3044
健全性の監視	3074
File System Analytics の略	3087
EMSノセツテイ	3102
ONTAP コマンドリファレンス	3119
サポートされているバージョンのONTAP のコマンドリファレンス	3119



限定サポートバージョンのONTAP のコマンドリファレンス (PDFのみ)	3119
CLI比較ツール	3119
法的通知	3120
著作権	3120
商標	3120
特許	3120
プライバシーポリシー	3120
オープンソース	3120

# ONTAP 9ドキュメント

# リリースノート

## ONTAP 9リリースのハイライト

ONTAP 9データ管理ソフトウェアの各リリースには、ONTAPの機能、管理性、パフォーマンス、セキュリティを強化する新機能と強化された機能が搭載されています。

これらのハイライトに加えて、最近のONTAPリリースで導入されたすべての新機能と強化された機能をバージョンごとに包括的にカバーしています。

ONTAP 9のすべてのバージョンにおけるハードウェアプラットフォームとスイッチのサポート、既知の問題、制限事項、またはONTAP 9.9.1より前のリリースで導入された機能の詳細については、を参照してください。 ["ONTAP 9リリースノート"](#)。リリースノートにアクセスするには、NetAppアカウントでサインインするか、アカウントを作成する必要があります。

ONTAPの最新リリースにアップグレードするには、を参照してください。 [ONTAPの最新バージョンへのアップグレード](#) および [ONTAPはいつアップグレードすればよいですか](#)。

### ONTAP 9.14.1の特長

ONTAP 9.14.1は、FabricPool、ランサムウェア対策、OAuthなどの分野で新機能と強化された機能を提供します。新機能と拡張機能の一覧については、を参照してください。 [ONTAP 9.14.1の新機能](#)。

- [WAFL予約の削減](#)

ONTAP 9.14.1では、30TB以上のアグリゲートのWAFLリザーブが削減されることで、FASシステムとCloud Volumes ONTAPシステムで使用可能スペースが即座に5%増加しました。

- [FabricPoolの機能拡張](#)

FabricPoolは、 [読み取りパフォーマンス](#) また、クラウドへの直接書き込みが可能なため、コールドデータを低コストのストレージ階層に移動することで、スペース不足のリスクを軽減し、ストレージコストを削減できます。

- ["OAuth 2.0のサポート"](#)

ONTAPは、System Managerを使用して設定できるOAuth 2.0フレームワークをサポートしています。OAuth 2.0を使用すると、ユーザIDとパスワードをプレーンテキストスクリプトやランブックに作成したり公開したりすることなく、自動化フレームワーク用のONTAPへの安全なアクセスを提供できます。

- ["Autonomous Ransomware Protection \(ARP\) の機能拡張"](#)

ARPを使用すると、イベントのセキュリティをより細かく制御できるようになり、アラートを生成する条件を調整して、誤検出の可能性を減らすことができます。

- [System ManagerでのSnapMirrorディザスタリカバリのリハーサル](#)

System Managerのシンプルなワークフローを使用して、リモートサイトでディザスタリカバ리를簡単にテストしたり、テスト後にクリーンアップしたりできます。この機能により、テストをより簡単かつ頻繁に実施し、目標復旧時間の信頼性を高めることができます。

- [S3オブジェクトロックのサポート](#)

ONTAP S3では、object-lock APIコマンドがサポートされており、S3でONTAPに書き込まれたデータを削除から保護できます。

S3 APIの標準コマンドとを使用して、重要なデータを適切な期間にわたって保護します。

- [クラスタ および ボリューム タグ付け](#)

メタデータタグをボリュームとクラスタに追加します。メタデータタグは、オンプレミスからクラウドにデータを移動したり、データを反転したりするときに追従します。

## ONTAP 9.13.1の特長

ONTAP 9.13.1は、ランサムウェア対策、整合グループ、サービス品質（QoS）、テナント容量管理などの分野で新機能と強化された機能を提供します。新機能と拡張機能の一覧については、[を参照してください](#)。

### ONTAP 9.13.1の新機能。

- Autonomous Ransomware Protection（ARP）の機能強化：

- [シトウユウコウカ](#)

ONTAP 9.13.1では、十分な学習データが得られると、ARPは自動的にトレーニングモードから本番モードに移行します。これにより、管理者が30日間有効にする必要がなくなります。

- [マルチ管理者検証のサポート](#)

ARP disableコマンドはマルチ管理者検証でサポートされているため、1人の管理者がARPを無効にしてデータを潜在的なランサムウェア攻撃にさらすことはできません。

- [FlexGroupのサポート](#)

ONTAP 9.13.1以降では、ARPでFlexGroupがサポートされます。ARPでは、クラスタ内の複数のボリュームとノードにまたがるFlexGroupを監視および保護できるため、大規模なデータセットでもARPを使用して保護できます。

- [System Managerでの整合性グループのパフォーマンスと容量の監視](#)

パフォーマンスと容量を監視することで、整合性グループごとの詳細な監視が可能になり、データオブジェクトレベルではなくアプリケーションレベルで潜在的な問題をすばやく特定して報告することができます。

- [テナントの容量管理](#)

マルチテナントのお客様やサービスプロバイダは、SVMごとに容量の上限を設定できるため、テナントがセルフサービスプロビジョニングを実行しても、1つのテナントがクラスタの容量を過剰に消費するリスクはありません。

- [サービス品質（QoS）の天井と床](#)

ONTAP 9.13.1では、ボリューム、LUN、ファイルなどのオブジェクトをグループにグループ化してQoSの上限（最大IOPS）または下限（最小IOPS）を割り当てることで、アプリケーションに求められるパフォーマンスを向上させることができます。

## ONTAP 9.12.1の特長

ONTAP 9.12.1は、セキュリティ強化、保持、パフォーマンスなどの分野で新機能と強化された機能を提供します。新機能と拡張機能の一覧については、を参照してください。 [ONTAP 9.12.1の新機能](#)。

- [Snapshotの改ざんを防止](#)

SnapLockテクノロジーを使用すると、ソースまたはデスティネーションでSnapshotコピーが削除されないように保護できます。

プライマリストレージとセカンダリストレージのSnapshotをランサムウェア攻撃者や不正な管理者による削除から保護することで、より多くのリカバリポイントを保持できます。

- [自律型ランサムウェア対策（ARP）の強化](#)

プライマリストレージのスクリーニングモデルに基づいて、インテリジェントな自律型ランサムウェア対策をセカンダリストレージで即座に実現します。

フェイルオーバー後、セカンダリストレージに対するランサムウェア攻撃の可能性を瞬時に特定影響を受け始めたデータのSnapshotが即座に取得され、管理者に通知されるため、攻撃を阻止してリカバリを強化できます。

- [FPolicy の](#)

ONTAP FPolicyをワンクリックでアクティブ化して既知の悪意のあるファイルを自動的にブロックシンプルなアクティブ化により、一般的な既知のファイル拡張子を使用する一般的なランサムウェア攻撃から保護できます。

- [セキュリティ強化：改ざん防止保持ロギング](#)

ONTAPでの改ざん防止保持ロギング侵害された管理者アカウントを確実に保護することで、悪意のある操作を隠すことはできません。システムの知識がなければ、管理者およびユーザの履歴を変更または削除することはできません。

発生元に関係なく、すべての管理操作をログに記録して監査することで、データに影響を与えるすべての操作が確実にキャプチャされます。システム監査ログが改ざんされて管理者に変更が通知されると、アラートが生成されます。

- [セキュリティの強化：多要素認証の拡張](#)

CLI（SSH）の多要素認証（MFA）は、Yubikey物理ハードウェアトークンデバイスをサポートしています。これにより、攻撃者は、盗まれたクレデンシャルや侵害されたクライアントシステムを使用してONTAPシステムにアクセスできなくなります。Cisco Duoは、System Managerを使用したMFAでサポートされています。

- [ファイルとオブジェクトの二重性（マルチプロトコルアクセス）](#)

ファイルとオブジェクトの二重性により、S3プロトコルによる標準の読み取り/書き込みアクセスが、すでにNASプロトコルでアクセスされているデータソースと同じデータソースに可能になります。同じデータソースからファイルまたはオブジェクトとしてストレージに同時にアクセスできるため、オブジェクトデータを使用する分析など、さまざまなプロトコル（S3またはNAS）で使用するデータのコピーを重複して作成する必要がありません。

- [FlexGroup のリバランシング](#)

FlexGroupコンスティチュエントの負荷がアンバランスになった場合は、FlexGroupを無停止でリバランシングし、

CLI、REST API、およびSystem Managerを使用できます。最適なパフォーマンスを実現するには、FlexGroup内のコンスティチュエントメンバーに使用容量を均等に分散させる必要があります。

- ストレージ容量の拡張

WAFLのスペースリザベーションが大幅に削減され、アグリゲートあたりの使用可能容量が最大400TiB増えました。

## ONTAP 9.11.1の特長

ONTAP 9.11.1は、セキュリティ、保持、パフォーマンスなどの分野で新機能と強化された機能を提供します。新機能と拡張機能の一覧については、[を参照してください。](#) [ONTAP 9.11.1の新機能。](#)

- [管理者による検証が複数必要です](#)

Multi-admin verification (MAV ; マルチ管理者認証) は、業界初のネイティブな検証アプローチであり、Snapshotやボリュームの削除など、機密性の高い管理タスクに対して複数の承認を必要とします。MAVの実装で必要とされる承認は、悪意のある攻撃やデータへの偶発的な変更を防止します。

- [自律型ランサムウェア対策の強化](#)

Autonomous Ransomware Protection (ARP) は、機械学習を使用してランサムウェアの脅威をきめ細かく検出し、脅威を迅速に特定し、侵害発生時のリカバリを高速化します。

- [FlexGroupボリュームのSnapLock準拠](#)

WORMファイルロックでデータを保護し、変更や削除を防止することで、電子設計の自動化やメディア/エンターテインメントなどのワークロード向けに数ペタバイト規模のデータセットを保護します。

- [非同期ディレクトリの削除](#)

ONTAP 9.11.1では、ONTAPシステムのバックグラウンドでファイルが削除されるため、大規模なディレクトリを簡単に削除しながら、ホストI/Oへのパフォーマンスやレイテンシの影響を排除できます。

- [S3の機能拡張](#)

ONTAPの追加のAPIエンドポイントとバケットレベルのオブジェクトバージョン管理により、S3のオブジェクトデータ管理機能を簡易化、拡張し、オブジェクトの複数のバージョンを同じバケットに格納できるようになります。

- System Manager の機能拡張

System Managerは、ストレージリソースを最適化し、監査管理を強化する高度な機能をサポートしています。この更新には、ストレージアグリゲートの管理と構成の強化、システム分析の可視化の強化、FASシステムのハードウェア可視化などが含まれます。

## ONTAP 9.10.1の特長

ONTAP 9.10.1は、セキュリティ強化、パフォーマンス分析、NVMeプロトコルのサポート、オブジェクトストレージのバックアップオプションに関する新機能と強化された機能を提供します。新機能と拡張機能の一覧については、を参照してください。 [ONTAP 9.10.1の新機能](#)。

- [自律的なランサムウェア防御](#)

Autonomous Ransomware Protectionは、ボリュームのSnapshotコピーを自動的に作成し、異常なアクティビティが検出されたときに管理者にアラートを送信します。これにより、ランサムウェア攻撃を迅速に検出し、より迅速にリカバリすることができます。

- [System Manager の機能拡張](#)

System Managerは、NetApp Active IQデジタルアドバイザ、BlueXP、および証明書管理と新たに統合された機能に加え、ディスク、シェルフ、サービスプロセッサのファームウェアの更新を自動的にダウンロードします。これらの機能強化により、管理が簡素化され、ビジネス継続性が維持

- [ファイルシステム分析の機能拡張](#)

ファイルシステム分析では、ファイル共有内の上位のファイル、ディレクトリ、ユーザを特定するための追加のテレメトリが提供されます。これにより、ワークロードのパフォーマンスの問題を特定し、リソースプランニングとQoSの実装を改善できます。

- [AFFシステムでのNVMe over TCP \(NVMe/TCP\) のサポート](#)

既存のイーサネットネットワークでNVMe/TCPを使用すると、AFFシステムでエンタープライズSANと最新のワークロードのパフォーマンスを向上し、TCOを削減できます。

- [NetApp FASシステムでNVMe over Fibre Channel \(NVMe/FC\) をサポート](#)

ハイブリッドアレイでNVMe/FCプロトコルを使用して、NVMeへの均一な移行を実現します。

- [オブジェクトストレージ向けのハイブリッドクラウドネイティブバックアップ](#)

任意のオブジェクトストレージターゲットを使用して、ONTAP S3データを保護できます。SnapMirrorレプリケーションを使用して、StorageGRIDではオンプレミスストレージ、Amazon S3ではクラウド、NetApp AFFシステムやFASシステムでは別のONTAP S3バケットにバックアップできます。

- [FlexCacheによるグローバルファイルロック](#)

FlexCacheを使用したグローバルファイルロックにより、元のソースファイルの更新時にキャッシュの場所でファイルの整合性を確保できます。この機能拡張により、強化されたロックが必要なワークロードに対して、オリジンとキャッシュの関係で排他的なファイル読み取りロックが有効になります。

## ONTAP 9.9.1の特長

ONTAP 9.9.1は、ストレージ効率化、多要素認証、ディザスタリカバリなどの分野で新機能と強化された機能を提供します。新機能と拡張機能の一覧については、を参照してください。 [ONTAP 9.9.1の新機能](#)。

- [CLIによるリモートアクセス管理のセキュリティの強化](#)

SHA512およびSSH A512パスワードハッシュのサポートにより、システムアクセスを取得しようとする悪意のある攻撃者から管理者アカウントのクレデンシャルを保護します。

- ["MetroCluster IPの機能拡張:8ノードクラスタのサポート"](#)

この新しい制限は、以前の制限の2倍になり、MetroCluster構成をサポートし、継続的なデータ可用性を実現します。

- [SnapMirrorビジネス継続性の機能拡張](#)

NASワークロード向けの大規模データコンテナ向けに、バックアップとディザスタリカバリのためのより多くのレプリケーションオプションを提供します。

- [SANのパフォーマンスの向上](#)

VMwareデータストアなどの単一LUNアプリケーションに対して最大4倍のSANパフォーマンスを提供するため、SAN環境で高いパフォーマンスを実現できます。

- [ハイブリッドクラウド向けの新しいオブジェクトストレージオプション](#)

StorageGRIDをNetApp Cloud Backup Serviceのデスティネーションとして使用し、オンプレミスのONTAPデータのバックアップを簡易化、自動化できます。

次のステップ

- [ONTAPの最新バージョンへのアップグレード](#)
- [ONTAPはいつアップグレードすればよいですか。](#)

## ONTAP 9リリースのサポート

ONTAP 9.8リリース以降、NetAppではONTAPリリースを暦年に2回提供します。計画は変更される可能性があります。新しいONTAPリリースは暦年の第2四半期と第4四半期に提供する予定です。この情報は、最新のONTAPリリースを利用するためのアップグレード期間を計画する際に使用します。

バージョン	リリース日
9.14.1	2024年1月
9.13.1.	2023年6月
9.12.1:	2023年2月
9.11.1	2022年7月
9.10.1	2022年1月
9.9.1	2021年6月



## サポートレベル

特定のバージョンのONTAPで利用できるサポートのレベルは、ソフトウェアのリリース時期によって異なります。

サポートレベル	フルサポート			限定サポート		セルフサービスサポート		
年	1.	2.	3.	4.	5.	6.	7.	8
オンラインマニュアルへのアクセス	はい。	はい。	はい。	はい。	はい。	はい。	はい。	はい。
テクニカルサポート	はい。	はい。	はい。	はい。	はい。			
根本原因の分析	はい。	はい。	はい。	はい。	はい。			
ソフトウェアのダウンロード	はい。	はい。	はい。	はい。	はい。			
サービスアップデート（パッチリリース[P-releases]）	はい。	はい。	はい。					
脆弱性に関するアラート	はい。	はい。	はい。					

ONTAPの最新リリースにアップグレードするには、を参照してください。 [ONTAPの最新バージョンへのアップグレード](#) および [ONTAPはいつアップグレードすればよいですか](#)。

## ONTAP 9.14.1の新機能

ONTAP 9.14.1の新機能について説明します。

以前のONTAP 9リリース、ハードウェアプラットフォームとスイッチのサポート、既知の問題、および制限事項の詳細については、を参照してください。 ["ONTAP 9リリースノート"](#)。ONTAP 9リリースノート\_にアクセスするには、NetAppアカウントでサインインするか、NetAppアカウントを作成する必要があります。

最新バージョンのONTAPにアップグレードするには、を参照してください。 [ONTAPをアップグレードする準備](#)。

## データ保護

更新	説明
<a href="#">SVMルートボリュームでNVEをサポート</a>	SVMルートボリュームは、NetAppボリューム暗号化による一意のキーを使用して暗号化できます。

更新	説明
長期保持のSnapshotコピーに対してSnapshotコピーロックを設定できる および コンプライアンスクロックを再初期化するには	SnapLockライセンスがあるクラスタでは、SnapLock以外のSnapMirrorデスティネーションボリュームで作成されたSnapshotコピーに対して、長期保持によるSnapshotコピーの改ざん防止ロックを設定できます。また、SnapLockボリュームが存在しない場合は、コンプライアンスクロックを初期化できます。
SnapMirrorビジネス継続性 (SM-BC) : SCIS3の永続的予約とWindowsフェイルオーバークラスタリングをサポート	SCSI3の永続的予約とSM-BCのWindow Failover Clusteringは、デバイスにアクセスする複数のノードをサポートし、同時に他のノードへのアクセスをブロックします。これにより、さまざまなアプリケーション環境のクラスタリングの一貫性と安定性が確保されます。
整合グループを使用してボリューム単位のSnapshotをコピー	整合性グループを使用して非同期SnapMirror Snapshotやボリューム単位のSnapshotをデスティネーション整合性グループにレプリケートすることで、ディザスタリカバリをさらに強化できます。
SVMディザスタリカバリ関係での非同期データ保護の整合性グループのサポート	SVMディザスタリカバリ用に設定されたSVMでは、SVMに整合グループが含まれている場合、整合グループの情報をセカンダリサイトにレプリケートできます。
"20個のファンアウトターゲットに対するSnapMirror非同期のサポート"	ONTAP 9.14.1を使用している場合、A700以降のシステムでサポートされるSnapMirror非同期ファンアウトターゲットの数が16から20に増加しました。
整合グループのCLIサポート	ONTAP CLIを使用して整合グループを管理します。

## ファイルアクセスプロトコル

更新	説明
NFSv4.1セッションランキング	セッションランキングでは、エクスポートされたデータストアへの複数のパスを使用できます。これにより、ワークロードのスケールアップに合わせて管理を簡易化し、パフォーマンスを向上できます。これは、VMware ワークロードが発生する環境に特に適しています。

## MetroCluster

更新	説明
ミラーアグリゲートとミラーされていないアグリゲートでのS3オブジェクトストレージのサポート	MetroCluster IPおよびFC構成のミラーされたアグリゲートまたはミラーされていないアグリゲート内のSVMでS3オブジェクトストレージサーバを有効にします。
MetroClusterクラスタ内のミラーされたアグリゲートとミラーされていないアグリゲートでのS3バケットのプロビジョニングのサポート	MetroCluster構成では、ミラーされたアグリゲートまたはミラーされていないアグリゲートにバケットを作成できます。

MetroCluster構成のプラットフォームおよびスイッチ構成の拡張機能については、を参照してください。"ONTAP 9リリースノート"。

## S3オブジェクトストレージ

更新	説明
S3 FlexGroupボリュームでは自動サイズ変更が有効になり、バケット作成時の過剰な容量割り当てが解消されました。	新規または既存のFlexGroupボリュームでバケットを作成または削除すると、必要な最小サイズにボリュームのサイズが変更されます。必要な最小サイズは、FlexGroupボリューム内のすべてのS3バケットの合計サイズです。
ミラーアグリゲートとミラーされていないアグリゲートでのS3オブジェクトストレージのサポート	MetroCluster IPおよびFC構成では、ミラーされたアグリゲートまたはミラーされていないアグリゲート内のSVMでS3オブジェクトストレージサーバを有効にすることができます。
ユーザのロールとロック保持期間に基づくオブジェクトのロック	S3バケット内のオブジェクトは、上書きまたは削除されないようにロックできます。オブジェクトをロックする機能は、特定のユーザまたは時間に基づいています。
外部ディレクトリサービスをサポートするためのLDAPユーザグループのアクセスの設定、およびアクセスキーとシークレットキーの有効期間の追加	ONTAP管理者は、Lightweight Directory Access Protocol (LDAP) またはActive Directoryユーザグループに対してONTAP S3オブジェクトストレージへのアクセスを設定できます。また、LDAP高速バインドモードで認証を有効にすることもできます。ローカルグループ、ドメイングループ、またはLDAPグループのユーザは、S3クライアント用に独自のアクセスキーとシークレットキーを生成できます。 S3ユーザのアクセスキーとシークレットキーの有効期間を定義できます。ONTAPでは、次のような変数がサポートされます。 \$aws:username バケットポリシーとグループポリシーの場合。

## SAN

更新	説明
NVMe/TCPによるホストの自動検出	NVMe/TCPプロトコルを使用するコントローラのホスト検出は、デフォルトで自動化されています。
NVMe/FCホスト側のレポートとトラブルシューティング	ONTAPでは、デフォルトでNVMe/FCホストが一意的識別子で仮想マシンを識別し、NVMe/FCホストが仮想マシンのリソース利用率を監視する機能がサポートされています。これにより、ホスト側のレポート作成とトラブルシューティングが強化されます。
NVMeホストノユウセンワリアテ	特定のホストに対するリソース割り当ての優先順位を設定するようにNVMeサブシステムを設定できます。高い優先度が割り当てられたホストには、より多くのI/Oキューが割り当てられ、より大きなキュー深度が割り当てられます。

## セキュリティ

更新	説明
SSHユーザのCisco Duo多要素認証のサポート	SSHユーザは、サインイン時の2番目の認証要素としてCisco Duoを使用して認証できます。

更新	説明
"OAuth 2.0サポートの強化"	ONTAP 9.14.1は、コアトークンベースの認証を拡張し、ONTAP 9.14.0で最初に提供されたOAuth 2.0のサポートを提供します。許可は、Active DirectoryまたはLDAPとグループとロールのマッピングを使用して設定できます。送信者に制約されたアクセストークンもサポートされており、Mutual TLS (MTLS) に基づいてセキュリティが確保されています。Auth0とKeycloakに加えて、Microsoft Windows Active Directory Federation Service (ADFS) がアイデンティティプロバイダ (IdP) としてサポートされています。
"OAuth 2.0認可フレームワーク"	Open Authorization (OAuth 2.0) フレームワークが追加され、ONTAP REST APIクライアントにトークンベースの認証を提供します。これにより、REST APIスクリプトやAnsibleを基盤とする自動化ワークフローを使用して、ONTAPクラスタの管理と管理をよりセキュアに行うことができます。発行者、オーディエンス、ローカル検証、リモートイントロスペクションなど、標準のOAuth 2.0機能がサポートされています。リモートユーザの要求、プロキシサポート。クライアント認証は、自己完結型のOAuth 2.0スコープを使用するか、ローカルのONTAPユーザをマッピングして設定できます。サポートされるアイデンティティプロバイダ (IdP) には、複数の同時サーバを使用するAuth0とKeycloakが含まれます。
自律型ランサムウェア対策のアラートを調整可能	新しいファイル拡張子が検出されたとき、またはARP Snapshotが作成されたときに通知を受信し、ランサムウェアイベントの可能性に関する事前の警告を受け取るように、Autonomous Ransomware Protectionを設定します。
FPolicyは永続的ストアをサポートしてレイテンシを低減	FPolicyを使用すると、SVM内の非同期（必須ではない）ポリシーのファイルアクセスイベントをキャプチャする永続的ストアを設定できます。永続的ストアを使用すると、クライアントI/O処理とFPolicy通知処理を分離して、クライアントのレイテンシを低減できます。同期および非同期の必須構成はサポートされていません。
FPolicyによるSMBでのFlexCacheボリュームのサポート	FPolicyは、NFSまたはSMBを使用するFlexCacheボリュームでサポートされます。以前は、SMBを使用するFlexCacheではFPolicyはサポートされていませんでした。

## ストレージ効率

更新	説明
ファイルシステム分析でのスキャン追跡	進捗状況と調整に関するリアルタイムの分析情報で、ファイルシステム分析の初期化スキャンを追跡します。
FASプラットフォームで使用可能なアグリゲートスペースの増加	FASプラットフォームでは、30TBを超えるアグリゲートのWAFLリザーブが10%から5%に削減され、アグリゲートで使用可能なスペースが増加します。

更新	説明
TSSEボリュームの使用済み物理スペースに関するレポートの変更点	<p>Temperature-Sensitive Storage Efficiency (TSSE) が有効になっているボリュームでは、ボリュームで使用されているスペース量を報告するONTAP CLIの指標に、TSSEによって実現されるスペース削減量が含まれます。この指標は、volume show-physical-usedコマンドとvolume show-space-physical usedコマンドに反映されます。</p> <p>FabricPoolの場合、-physical-used は、大容量階層と高パフォーマンス階層を組み合わせたものです。</p> <p>特定のコマンドについては、リンク：<a href="https://docs.netapp.com/us-en/ontap-cli-9141/volume-show.html">https://docs.netapp.com/us-en/ontap-cli-9141/volume-show.html</a>を参照してください。[volume show^]およびリンク：<a href="https://docs.netapp.com/us-en/ontap-cli-9141/volume-show-space.html">https://docs.netapp.com/us-en/ontap-cli-9141/volume-show-space.html</a>[volume show space^]をクリックします。</p>

## ストレージリソース管理の機能拡張

更新	説明
プロアクティブなFlexGroupリバランシング	FlexGroupボリュームでは、ディレクトリ内で拡張中のファイルをリモートコンスチチュエントに自動的に移動することで、ローカルコンスチチュエント上のI/Oボトルネックを軽減できます。
FlexGroupボリュームでのSnapshotコピーのタグ付け	では、Snapshotコピーを識別したり、FlexGroupボリューム内のSnapshotコピーが誤って削除されたりしないように、タグやラベル（コメント）を追加、変更、および削除できます。
FabricPoolでクラウドに直接書き込む	FabricPoolでは、FabricPoolのボリュームにデータを書き込む機能が追加されているため、階層化スキャンを待たずに直接クラウドに移動できます。
FabricPoolによる積極的な先読み	FabricPoolでは、FabricPoolボリューム上のムービーストリームなどのファイルを積極的に先読みして、フレームが破棄されないようにします。

## SVM管理の機能拡張

更新	説明
SVMのデータ移動のサポート：ユーザクォータおよびグループクォータおよびqtreeを含むSVMの移行	SVMのデータ移動により、ユーザクォータ、グループクォータ、およびqtreeを含むSVMの移行がサポートされるようになりました。
SVMあたり最大400個のボリューム、最大12個のHAペア、およびSVMのデータ移動を使用するNFS 4.1でのpNFSをサポート	SVMのデータ移動が可能なSVMあたりのサポートされるボリュームの最大数が400に増え、サポートされるHAペアの数が12に増えました。

## System Manager の略

更新	説明
SnapMirrorテストフェイルオーバーのサポート	System Managerを使用すると、既存のSnapMirror関係を中断することなく、SnapMirrorのテストフェイルオーバーのリハーサルを実行できます。

更新	説明
ブロードキャストドメインでのポート管理	System Managerを使用して、ブロードキャストドメインに割り当てられているポートを編集または削除できます。
Mediator-Assisted Automatic Unplanned Switchover (MAUSO; メディエーターアシスト自動計画外スイッチオーバー) の有効化	System Managerを使用して、IP MetroClusterのスイッチオーバーおよびスイッチバックの実行時にMediator-Assisted Automatic Unplanned Switchover (MAUSO; メディエーターアシスト自動計画外スイッチオーバー) を有効または無効にすることができます。
クラスタ および ボリューム タグ付け	System Managerでは、タグを使用して、目的、所有者、環境などさまざまな方法でクラスタやボリュームを分類できます。これは、同じタイプのオブジェクトが多数ある場合に便利です。ユーザは、割り当てられているタグに基づいて特定のオブジェクトをすばやく識別できます。
整合グループ監視のサポートの強化	System Managerには、整合グループの使用状況に関する履歴データが表示されます。
NVMeインバンド認証	System Managerを使用して、NVMeホストとコントローラの間で、DH-HMAC-CHAP認証プロトコルを使用したNVMe/TCPおよびNVMe/FCプロトコルを介したセキュアな一方および双方方向の認証を設定できます。
S3バケットライフサイクル管理のサポートをSystem Managerに拡張	System Managerを使用して、バケット内の特定のオブジェクトを削除したり、削除したバケットオブジェクトを期限切れにしたりするルールを定義できます。

## ONTAP 9.13.1の新機能

ONTAP 9.13.1で利用できる新しい機能について説明します。

以前のONTAP 9リリース、ハードウェアプラットフォームとスイッチのサポート、既知の問題、および制限事項の詳細については、を参照してください。["ONTAP 9リリースノート"](#)。ONTAP 9リリースノート\_にアクセスするには、NetAppアカウントでサインインするか、NetAppアカウントを作成する必要があります。

ONTAPをアップグレードするには、[ONTAPをアップグレードする準備](#)。

### データ保護

更新	説明
"管理者による検証が複数必要です"	クラスタ管理者は、クラスタでマルチ管理者検証を明示的に有効にして、一部のSnapLock処理を実行する前にクォーラムの承認が必要になるようにすることができます。
"ボリュームの移動やジオメトリなど、整合性グループの管理のサポートが強化されました。"	整合グループ間でボリュームを移動したり、階層整合グループのジオメトリを変更したり、整合グループの容量に関する分析情報を取得したりできます。System Managerでは、新しいNASボリュームまたはNVMeネームスペースを使用して整合グループを作成できます。
"SnapMirror Synchronousを使用したNDMPリストア"	NDMPリストアはSnapMirror同期でサポートされています。



更新	説明
SnapMirrorビジネス継続性 (SM-BC) の機能拡張	<ul style="list-style-type: none"> <li>• "アクティブなSM-BC関係が確立された整合性グループに、システムを停止することなくボリュームを追加します。"</li> <li>• "SM-BCでNDMPリストアを利用する"。</li> </ul>
xref:./release-notes/"単一の整合グループでの非同期SnapMirrorのサポート"	整合グループでは非同期SnapMirror構成がサポートされ、単一の整合グループのSnapMirrorバックアップのバックアップが可能になります。

## ファイルアクセスプロトコル

更新	説明
"NFSv4.xストレージプールのサポート"	一部のクライアントがNFSv4.xストレージプールリソースを過剰に消費するため、NFSv4.xストレージプールリソースを使用できないために他のNFSv4.xクライアントがブロックされます。環境でNFSv4.xストレージプールのリソースを大量に消費するクライアントの拒否とブロックを有効にすることができます。

## MetroCluster

更新	説明
"MetroCluster IPおよびイーサネット接続ストレージ用の共有スイッチを使用したMetroCluster FCからMetroCluster IPへの移行"	共有スイッチを使用して、MetroCluster FCからMetroCluster IP構成 (ONTAP 9.8以降) に無停止で移行できます。
"8ノードMetroCluster FC構成からMetroCluster IP構成への無停止での移行"	既存の8ノードMetroCluster FC構成から新しいMetroCluster IP構成に、ワークロードとデータを無停止で移行できます。
"スイッチオーバーとスイッチバックを使用した4ノードMetroCluster IP構成のアップグレード"	スイッチオーバーとスイッチバックを使用して、4ノードMetroCluster IP構成のコントローラをアップグレードします。 system controller replace コマンド
"環境のシャットダウン時にメディアエーターアシスト自動計画外スイッチオーバー (MAUSO) がトリガーされる"	環境のシャットダウンにより一方のサイトが正常にシャットダウンすると、MAUSOがトリガーされます。
"8ノードMetroCluster IP構成のサポート"	8ノードMetroCluster IP構成のコントローラとストレージをアップグレードするには、構成を拡張して一時的な12ノード構成にし、古いDRグループを削除します。
"MetroCluster IP構成から共有ストレージMetroClusterスイッチ構成への変換"	MetroCluster IP構成を共有ストレージMetroClusterスイッチ構成に変換できます。

MetroCluster構成のプラットフォームおよびスイッチ構成の拡張機能については、を参照してください。 "ONTAP 9リリースノート"。

## ネットワーキング

更新	説明
<a href="#">RDMAクラスタインターコネクトに対するハードウェアサポートの拡張</a>	ONTAPは、X91153AクラスタNICを使用したクラスタインターコネクトRDMAでAFF A900、ASA A900、およびFAS9500のシステムをサポートしているため、レイテンシの低減、フェイルオーバー時間の短縮、ノード間の通信の高速化が可能です。
データLIF数の上限が引き上げられます	ONTAPでは、HAペアとクラスタの両方について、データLIFの拡張制限が引き上げられるため、柔軟性が向上します。
A800およびFAS8700プラットフォームでのクラスタセットアップ時のIPv6のサポート	A800およびFAS8700プラットフォームでは、ONTAP CLIを使用して、IPv6のみのネットワーク環境で新しいクラスタを作成および設定できます。

## S3オブジェクトストレージ

更新	説明
<a href="#">S3バケットのライフサイクル管理</a>	S3オブジェクトの有効期限アクションは、バケット内のオブジェクトの有効期限を定義します。この機能を使用すると、オブジェクトバージョンを管理できるため、保持要件を満たし、S3オブジェクトストレージ全体を効率的に管理できます。

## SAN

更新	説明
<a href="#">AIXホストでのNVMe/FCのサポート</a>	ONTAPでは、AIXホストでNVMe/FCプロトコルがサポートされます。を参照してください <a href="#">"NetApp相互運用性ツール"</a> を参照してください。

## セキュリティ

フィーチャー（Feature）	説明
<a href="#">自律的なランサムウェア防御</a>	<ul style="list-style-type: none"><li>自律型ランサムウェア対策による複数管理者による検証機能</li><li>学習モードからアクティブモードへの自動移行</li><li><a href="#">FlexGroupのサポート</a>これには、FlexGroupボリュームの拡張、FlexVolからFlexGroupへの変換、FlexGroupのリバランシングなどのFlexGroupボリュームおよび処理の分析とレポートが含まれます。</li></ul>
<a href="#">Active Directoryを使用したSSH公開鍵認証</a>	Active Directory（AD）ユーザのプライマリ認証方式としてSSH公開鍵を使用することも、ADユーザのあとにSSH公開鍵をセカンダリ認証方式として使用することもできます。
SSH公開鍵を使用したX.509証明書	ONTAPを使用すると、X.509証明書をアカウントのSSH公開鍵に関連付けることができます。これにより、SSHログイン時の証明書の有効期限と失効チェックのセキュリティが強化されます。



フィーチャー（Feature）	説明
FPolicyファイルアクセスエラー通知	FPolicyは、アクセス拒否イベントの通知をサポートしています。NTFS権限によるエラー、UNIXモードビットによるエラー、NFSv4 ACLによるエラーなど、権限がないためにファイル操作が失敗した場合に通知が生成されます。
TOTPを使用した多要素認証（時間ベースのワンタイムパスワード）	時間ベースのワンタイムパスワード（TOTP）を使用して多要素認証を行うローカルユーザアカウントをセットアップします。TOTPは常に2番目の認証方式として使用されます。主な認証方法として、SSH公開鍵またはユーザパスワードを使用できます。

## ストレージ効率

更新	説明
System Managerでのプライマリデータ削減比率に関するレポートの変更	System Managerに表示されるプライマリデータ削減率の計算に、Snapshotコピーのスペース削減率は含まれなくなります。使用済み論理スペースと使用済み物理スペースの比率のみが表示されます。ONTAPの以前のリリースでは、Snapshotコピーのスペース削減効果が大幅に向上していましたが、プライマリのデータ削減比率が向上していませんでした。そのため、ONTAP 9.13.1にアップグレードすると、報告されるプライマリ比率が大幅に低くなります。Snapshotコピーを使用したデータ削減率は、引き続き <b>Capacity</b> の詳細ビューで確認できます。
温度に基づくストレージ効率	温度に基づくストレージ効率化では、連続する物理ブロックのシーケンシャルパッキングが追加され、ストレージ効率が向上します。システムをONTAP 9.13.1にアップグレードすると、温度の影響を受けやすいStorage Efficiencyが有効になっているボリュームでシーケンシャルパッキングが自動的に有効になります。
ロンリスヘエスノテキヨウ	論理スペースの適用はSnapMirrorデスティネーションでサポートされます。
Storage VM容量制限のサポート	Storage VM（SVM）に容量制限を設定し、SVMがしきい値に近づいたときにアラートを有効にすることができます。

## ストレージリソース管理の機能拡張

更新	説明
inodeの最大数の増加	ボリュームのサイズが680GBを超えても、ONTAPは引き続き自動的にinodeを追加します（ボリュームスペース32KBあたりinode 1個の割合）。ONTAPは、最大数の2、147、483,632に達するまでinodeを追加し続けます。
FlexClone作成時のSnapLockタイプの指定のサポート	読み取り/書き込みボリュームのFlexCloneを作成するときに、3つのSnapLockタイプ（Compliance、Enterprise、またはSnapLock以外）のいずれかを指定できます。
ファイルシステム分析をデフォルトで有効にする	新しいボリュームでファイルシステム分析をデフォルトで有効にするように設定します。

更新	説明
<a href="#">FlexGroupとのSVMディザスタリカバリファンアウト関係</a>	FlexGroupを備えたSVM DRのファンアウトの制限は削除されました。FlexGroupを使用したSVM DRでは、8サイトへのSnapMirrorファンアウト関係がサポートされます。
<a href="#">単一FlexGroupのリバランシング処理</a>	1つのFlexGroupリバランシング処理を、指定した日時に開始するようにスケジュールを設定できます。
<a href="#">FabricPoolの読み取りパフォーマンス</a>	FabricPoolは、クラウドに格納されたデータと階層化のスループットに対して、シングルストリームとマルチストリームのワークロードでシーケンシャル読み取りのパフォーマンスを向上させます。この改善により、バックエンドのオブジェクトストアにGETとPUTの割合が高くなる可能性があります。オンプレミスのオブジェクトストアがある場合は、オブジェクトストアサービスのパフォーマンスヘッドルームを考慮し、FabricPool PUTの調整が必要かどうかを判断する必要があります。
<a href="#">アダプティブQoSポリシーテンプレート</a>	アダプティブQoSポリシーテンプレートを使用すると、スループットの下限をSVMレベルで設定できます。

## SVM管理の機能拡張

更新	説明
<a href="#">SVM のデータ移動</a>	最大200個のボリュームを含むSVMの移行のサポートが強化されます。
<a href="#">SVMディレクトリの再作成のサポート</a>	新しいCLIコマンド <code>debug vserver refresh-vserver-dir -node node_name</code> 欠落しているディレクトリとファイルを再作成します。詳細およびコマンド構文については、 <a href="#">"ONTAPコマンドリファレンス"</a> を参照してください。

## System Manager の略

ONTAP 9.12.1以降では、System ManagerがBlueXPに統合されています。の詳細を確認してください [System ManagerとBlueXPの統合](#)。

更新	説明
<a href="#">レポート作成時のプライマリデータ削減比率の変更</a>	System Managerに表示されるプライマリデータ削減率の計算に、Snapshotコピーのスペース削減率は含まれなくなります。使用済み論理スペースと使用済み物理スペースの比率のみが表示されます。ONTAPの以前のリリースでは、Snapshotコピーのスペース削減効果が大幅に向上していましたが、プライマリのデータ削減比率が向上していませんでした。そのため、ONTAP 9.13.1にアップグレードすると、報告されるプライマリ比率が大幅に低くなります。Snapshotコピーを使用したデータ削減率は、引き続き容量の詳細ビューで確認できます。
<a href="#">タンパープルーフスナップショットコピーロック</a>	System Managerを使用してSnapLock以外のボリュームにSnapshotコピーをロックし、ランサムウェア攻撃から保護することができます。
<a href="#">外部キー管理ツールのサポート</a>	System Managerを使用して外部キー管理ツールを管理し、認証キーと暗号化キーを格納および管理できます。

更新	説明
<a href="#">ハードウェアの問題のトラブルシューティング</a>	System Managerユーザは、[ハードウェア]ページに、ASAプラットフォームやAFF Cシリーズプラットフォームなどの追加のハードウェアプラットフォームを視覚的に確認できます。 AFF Cシリーズプラットフォームは、ONTAP 9.12.1、ONTAP 9.11.1、およびONTAP 9.10.1の最新パッチリリースでもサポートされています。 視覚化により、プラットフォームの問題や懸念事項が特定され、ハードウェアの問題を迅速にトラブルシューティングすることができます。

## ONTAP 9.12.1の新機能

ONTAP 9.12.1で利用できる新しい機能について説明します。

以前のONTAP 9リリース、ハードウェアプラットフォームとスイッチのサポート、既知の問題、および制限事項の詳細については、を参照してください。["ONTAP 9リリースノート"](#)。ONTAP 9リリースノート\_にアクセスするには、NetAppアカウントでサインインするか、NetAppアカウントを作成する必要があります。

ONTAPをアップグレードするには、[ONTAPをアップグレードする準備](#)。

### データ保護

更新	説明
<a href="#">SnapMirror Synchronousによる大容量FlexVolのサポート</a>	SnapMirror Synchronous構成でサポートされるFlexVolの最大サイズが100TBから300TBに拡張されました。ソースクラスとデスティネーションクラスとの両方で、ONTAP 9.12.1 P2以降が実行されている必要があります。
<a href="#">SnapMirror SynchronousでのファイルサイズとLUNサイズの拡張のサポート</a>	SnapMirror Synchronous構成でサポートされるファイルとLUNの最大サイズが16TBから128TBに拡張されました。ソースとデスティネーションの両方のクラスでONTAP 9.12.1 P2以降が実行されている必要があります。
<a href="#">整合グループのサポートの強化</a>	<ul style="list-style-type: none"> <li>整合グループへのボリュームの追加と削除、整合グループのクローニング（Snapshotコピーからのボリュームを含む）を実行できます。</li> <li>コンシステンシグループはアプリケーションタギングをサポートし、データ保護と管理のプロセスを合理化します。</li> <li>ONTAP REST APIでは、NFS / SMBボリュームまたはNVMe名前空間を使用した整合性グループの設定がサポートされます。</li> </ul>
<a href="#">SnapMirror Synchronous NDO</a>	SnapMirror Synchronousは、HAのテイクオーバーとギブバック、ボリューム移動、その他のメンテナンス関連処理のノンストップオペレーション（NDO）をサポートします。この機能は、AFF / ASAプラットフォームでのみ使用できます。
<a href="#">ONTAP Mediator 1.5でSnapMirrorビジネス継続性をサポート</a>	ONTAP Mediator 1.5では、SnapMirrorビジネス継続性（SM-BC）関係を監視できます。

更新	説明
SnapMirror Business (SM-BC) の継続性の強化	SM-BCでは、SnapshotからのLUNの部分リストアがサポートされています。また、SM-BCでは、SM-BC関係のないボリュームでもQoSが拡張されます。
SnapMirror非同期のData Warehouseリビルドインジケータ	SnapMirror非同期は、ディザスタリカバリのリハーサル後にData Warehouseのリビルドにかかる時間を示すインジケータとして、完了した割合を表示します。
最小保持期間を「未指定」に設定するSnapLockオプション絶対保持期間	SnapLockには、絶対保持期限が「unspecified」に設定されている場合に最小保持期間を設定するオプションがあります。
改ざん防止Snapshotコピー	SnapLock以外のボリューム上のSnapshotコピーをロックして、ランサムウェア攻撃から保護することができます。Snapshotコピーをロックすると、誤って削除したり故意に削除したりしないようになります。

## ファイルアクセスプロトコル

更新	説明
Kerberos通信の弱い暗号化タイプを無効にする	新しいSMBセキュリティオプションを使用すると、Active Directory (AD) KDCとのKerberosベースの通信にAdvanced Encryption Standard (AES) 暗号化タイプを優先してRC4とDESを無効にできます。
NASデータへのS3クライアントアクセス	S3クライアントは、再フォーマットすることなくNFSクライアントやSMBクライアントと同じNASデータにアクセスできるため、オブジェクトデータを必要とするS3アプリケーションを簡単に提供できます。
NFS拡張属性	NFSv4.2に対応したNFSサーバでは、属性対応クライアントからNFS拡張属性 (xattrs) を格納および取得できます。
NFSv4.2のスパースファイルとスペースリザーベーションのサポート	NFSv4.2クライアントでは、スパースファイル用にスペースをリザーブできます。スペースの割り当てを解除したり、ファイルから予約を解除したりすることもできます。

## MetroCluster

更新	説明
ONTAP Mediator 1.5 はMetroCluster IP構成でサポートされます。	ONTAPメディエーター1.5は、MetroCluster IP構成の監視に使用できます。
フロントエンドホストプロトコル (NFSやiSCSIなど) のIPSecサポートは、MetroCluster IPおよびMetroClusterファブリック接続構成で使用できます。	フロントエンドホストプロトコル (NFSやiSCSIなど) のIPSecサポートは、MetroCluster IPおよびMetroClusterファブリック接続構成で使用できます。
"MetroCluster IP構成でのMetroCluster自動強制スイッチオーバー機能"	MetroClusterの自動強制スイッチオーバー機能は、MetroCluster IP構成で有効にすることができます。この機能は、Mediator-Assisted Unplanned Switchover (MAUSO；メディエーターアシスト計画外スイッチオーバー) 機能の拡張です。

更新	説明
"MetroCluster IP構成のミラーされていないアグリゲート上のSVM上のS3"	MetroClusterの自動強制スイッチオーバー機能は、MetroCluster IP構成で有効にすることができます。この機能は、Mediator-Assisted Unplanned Switchover (MAUSO；メディエーターアシスト計画外スイッチオーバー) 機能の拡張です。

MetroCluster構成のプラットフォームおよびスイッチ構成の拡張機能については、を参照してください。"ONTAP 9リリースノート"。

## ネットワーキング

更新	説明
LIFサアヒス	を使用できます management-log-forwarding 監査ログをリモートsyslogサーバに転送するために使用するLIFを制御するサービス

## S3オブジェクトストレージ

更新	説明
S3操作のサポートを強化	次のAmazon S3 APIアクションがサポートされています。 <ul style="list-style-type: none"> <li>• CopyObject</li> <li>• UploadPartCopy</li> <li>• BucketPolicy (GET、PUT、DELETE)</li> </ul>

## SAN

更新	説明
AFFおよびFASプラットフォームの最大LUNサイズの拡張	ONTAP 9.12.1P2以降では、AFFおよびFASプラットフォームでサポートされるLUNの最大サイズが16TBから128TBに拡張されました。
"NVMeの上限の引き上げ"	NVMeプロトコルでサポートされる機能は次のとおりです。 <ul style="list-style-type: none"> <li>• 1つのStorage VMと1つのクラスタに8Kのサブシステムを配置</li> <li>• 12ノードクラスタNVMe/FCはポートあたり256台のコントローラをサポートし、NVMe/TCPはノードあたり2、000台のコントローラをサポートします。</li> </ul>
NVMe/TCPのサポートによるセキュアな認証	NVMeホストとコントローラの間で、DHHMAC-CHAP認証プロトコルを使用したNVMe/TCP経由のセキュアな一方向認証および双方向認証がサポートされます。
MetroCluster IPでのNVMeのサポート	NVMe/FCプロトコルは、4ノードのMetroCluster IP構成でサポートされます。

## セキュリティ

2022年10月、NetAppは、HTTPSとTLSv1.2またはセキュアSMTPで送信されないAutoSupportメッセージの送信を拒否するための変更を実装しました。詳細については、を参照してください "[SU484：NetAppは不十分な転送セキュリティで送信されたAutoSupportメッセージを拒否します。](#)"。

フィーチャー（Feature）	説明
<a href="#">自律型ランサムウェア対策の相互運用性の強化</a>	Autonomous Ransomware Protectionは、次の構成で使用できます。 <ul style="list-style-type: none"><li>• ボリュームはSnapMirrorで保護されます</li><li>• SVMはSnapMirrorで保護されます</li><li>• 移行が有効になっているSVM（SVMのデータ移動）</li></ul>
<a href="#">FIDO2およびPIVを使用したSSHでの多要素認証（MFA）のサポート（いずれもYubikeyで使用）</a>	SSH MFAでは、ユーザ名とパスワードを使用したハードウェア支援型の公開鍵/秘密鍵交換を使用できます。Yubikeyは、MFAセキュリティを強化するためにSSHクライアントに接続される物理トークンデバイスです。
<a href="#">改ざん防止ロギング</a>	ONTAPのすべての内部ログはデフォルトで改ざんされていないため、侵害された管理者アカウントが悪意のある操作を隠すことができません。
<a href="#">イベントのTLS転送</a>	TLSプロトコルを使用してEMSイベントをリモートsyslogサーバに送信するため、ネットワークを介した保護が強化され、中央の外部監査ログが記録されます。

## ストレージ効率

更新	説明
<a href="#">温度に基づくストレージ効率</a>	新しいAFF C250、AFF C400、AFF C800のプラットフォームおよびボリュームでは、温度に基づくStorage Efficiencyがデフォルトで有効になります。TSSEは既存のボリュームではデフォルトでは有効になっていませんが、ONTAP CLIを使用して手動で有効にすることができます。
<a href="#">使用可能なアグリゲートスペースの増加</a>	All Flash FAS（AFF）およびFAS500fプラットフォームでは、30TBを超えるアグリゲート用のWAFLリザーブが10%から5%に削減され、アグリゲート内の使用可能なスペースが増加します。
<a href="#">ファイルシステム分析：サイズ別上位のディレクトリ</a>	ボリューム内でスペースを最も消費しているディレクトリがファイルシステム分析によって特定されるようになりました。

## ストレージリソース管理の機能拡張



更新	説明
FlexGroup のリバランシング	<p>無停止のFlexGroupボリュームの自動リバランシングを有効にして、FlexGroupコンスティチュエント間でファイルを再配分することができます。</p> <div>  <p>FlexVolからFlexGroupへの変換後は、FlexGroupの自動リバランシングを使用しないことを推奨します。代わりに、ONTAP 9.10.1以降で使用可能なシステム停止を伴う逆アクティブファイル移動機能を使用するには、を入力します volume rebalance file-move コマンドを実行します詳細およびコマンド構文については、を参照してください。 <a href="#">"ONTAPコマンドリファレンス"</a>。</p> </div>
SnapLock for SnapVaultによるFlexGroupボリュームのサポート	SnapLock for SnapVaultによるFlexGroupボリュームのサポート

## SVM管理の機能拡張

更新	説明
SVMデータ移動の機能拡張	<p>クラスタ管理者は、FAS、AFFプラットフォームを使用して、ハイブリッドアグリゲート上でソースクラスタからデスティネーションクラスタにSVMを無停止で再配置できます。</p> <p>停止を伴うSMBプロトコルと自律型ランサムウェア対策の両方がサポートされるようになりました。</p>

## System Manager の略

ONTAP 9.12.1以降では、System ManagerがBlueXPに統合されています。BlueXPを使用すると、管理者は使い慣れたSystem Managerダッシュボードを使用しながら、単一のコントロールプレーンからハイブリッドマルチクラウドインフラを管理できます。System Managerにサインインする際、管理者はBlueXPのSystem Managerインターフェイスにアクセスするか、System Managerに直接アクセスするかを選択できます。の詳細を確認してください [System ManagerとBlueXPの統合](#)。

更新	説明
System ManagerによるSnapLockのサポート	System Managerでは、コンプライアンスクロックの初期化、SnapLockボリュームの作成、WORMファイルのミラーリングなどのSnapLock処理がサポートされます。
ケーブル配線のハードウェア可視化	System Managerユーザは、クラスタ内のハードウェアデバイス間のケーブル接続に関する接続情報を表示して、接続の問題をトラブルシューティングできます。
System Managerへのログイン時にCisco Duoを使用した多要素認証のサポート	Cisco DuoをSAMLアイデンティティプロバイダ (IdP) として設定すると、ユーザがSystem ManagerにログインするときにCisco Duoを使用して認証できるようになります。

更新	説明
System Managerのネットワークの機能拡張	System Managerでは、ネットワークインターフェ이스の作成時に、サブネットやホームポートをより細かく選択できます。System Managerでは、RDMA接続経路のNFSの設定もサポートされます。
システムディスプレイテーマ	System Managerユーザは、System Managerインターフェ이스の表示に明るいテーマと暗いテーマを選択できます。また、オペレーティングシステムやブラウザで使用されているテーマをデフォルトに設定することもできます。この機能を使用すると、表示を読みやすくする設定を指定できます。
ローカル階層の容量の詳細に対する改善点	System Managerユーザは、特定のローカル階層の容量の詳細を表示して、スペースがオーバーコミットされているかどうかを確認できます。ローカル階層のスペースが不足しないようにするために容量を追加する必要がある可能性があります。
検索機能の向上	System Managerの検索機能が強化され、NetApp Support SiteからSystem Managerのインターフェースを介して直接、関連する状況に応じたサポート情報やSystem Manager製品ドキュメントを検索してアクセスできるようになりました。これにより、ユーザは、サポートサイトのさまざまな場所を検索しなくても、適切に対処するために必要な情報を取得できます。
ボリュームプロビジョニングの強化	ストレージ管理者は、System Managerを使用してボリュームを作成するときに、デフォルトのポリシーではなくSnapshotコピーポリシーを選択できます。
ボリュームのサイズを拡張する	System Managerを使用してボリュームのサイズを変更する場合、ストレージ管理者はデータスペースとSnapshotコピーリザーブへの影響を確認できます。
ストレージプール および Flash Pool の機能です 管理	ストレージ管理者は、System Managerを使用して、SSDストレージプールへのSSDの追加、SSDストレージプールの割り当て単位を使用したFlash Poolローカル階層（アグリゲート）の作成、物理SSDを使用したFlash Poolローカル階層の作成を行うことができます。
System ManagerでのNFS over RDMAのサポート	System Managerでは、RDMA経由のNFSのネットワークインターフェース設定がサポートされ、RoCE対応のポートが識別されます。

## ONTAP 9.11.1の新機能

ONTAP 9.11.1で提供される新しい機能について説明します。

以前のONTAP 9リリース、ハードウェアプラットフォームとスイッチのサポート、既知の問題、および制限事項の詳細については、を参照してください。 ["ONTAP 9リリースノート"](#)。ONTAP 9リリースノート\_にアクセスするには、NetAppアカウントでサインインするか、NetAppアカウントを作成する必要があります。

最新バージョンのONTAPにアップグレードするには、を参照してください。 [ONTAPをアップグレードする準備](#)。

### データ保護



更新	説明
クラスタカیفキイサアハ	クラスタ化された外部キー管理サーバは、クラスタ化されたKMIPサーバ解決策を提供するNetAppパートナー向けにサポートされるようになりました。これにより、プライマリとセカンダリのKMIPサーバを追加して、暗号化キーデータの重複を防止できます。サポートされているパートナーについては、" <a href="#">Interoperability Matrix Tool</a> で確認してください"。
System ManagerのSnapMirror非同期ポリシー	<p>System Managerを使用して、ボリュームやStorage VMを保護する際に、事前に作成されたカスタムのミラーとバックアップポリシーを追加したり、従来のポリシーを表示したり、保護ポリシーで定義されている転送スケジュールを上書きしたりできます。また、System Managerを使用して、ボリュームとStorage VMの保護関係を編集することもできます。</p> <div>  <p>ONTAP 9.8P12以降のONTAP 9.8パッチリリースを実行して、System Managerを使用してSnapMirrorを設定済みで、ONTAP 9.9.1またはONTAP 9.10.1リリースにアップグレードする場合は、ONTAP 9.9.1P13以降およびONTAP 9.10.1P10以降のパッチリリースをアップグレードに使用してください。</p> </div>
SnapMirror Cloudによる単一ディレクトリのリストア	admin権限レベルでクラスタ管理者が、クラウドエンドポイントから単一ディレクトリのリストア処理を実行できます。リストア元のバックアップエンドポイントを識別するには、ソースエンドポイントのUUIDを指定する必要があります。複数のバックアップで同じデータを使用できるように、cloud_endpoint_name リストア先として、バックアップに関連付けられたUUIDをrestoreコマンドに指定する必要があります。を使用できます snapmirror show コマンドを使用して source_endpoint_uuid。
SnapMirrorビジネス継続性 (SM-BC) のサポートの強化	<ul style="list-style-type: none"> <li>SM-BCはAIXをホストとしてサポート</li> <li>SM-BCでは単一ファイルSnapRestoreがサポートされているため、SM-BC構成の個々のLUNまたは通常のファイルをリストアできます。</li> </ul>
SVMデータレプリケーションのクイック再同期	SVMデータレプリケーションのクイック再同期を使用すると、ストレージ管理者は、Data Warehouseの完全なリビルドをバイパスし、ディザスタリカバリのリハーサルからより迅速にリカバリできます。
MetroClusterによるSVMデータレプリケーションのサポート	SVM-DRソースはMetroCluster構成の両端でサポートされます。
2フェーズ整合グループSnapshotコピーの作成	REST APIでは、整合グループで2フェーズのSnapshot手順がサポートされるため、Snapshotをコミットする前に事前確認を実行できます。

## ファイルアクセスプロトコル

更新	説明
TLSv1.3のサポート	ONTAPでは、HTTPSおよびREST API管理プロトコルでTLS 1.3がサポートされます。TLS 1.3は、SP / BMCまたはクラスタピアリング暗号化ではサポートされません。

更新	説明
<a href="#">LDAPファストバインドのサポート</a>	LDAPサーバでサポートされている場合は、LDAP高速バインドを使用して、ONTAP管理者ユーザをすばやく簡単に認証できます。

## MetroCluster

更新	説明
<a href="#">ONTAP Mediator 1.4のサポート</a>	MetroCluster IP構成では、ONTAPメディエーターソフトウェアバージョン1.4がサポートされます。
<a href="#">整合グループのサポート</a>	MetroCluster構成では整合グループがサポートされます。
<a href="#">"MetroCluster FC構成からAFF A250 / FAS500f MetroCluster IP構成への移行"</a>	MetroCluster FC構成からAFF A250またはFAS500f MetroCluster IP構成に移行できます。

MetroCluster構成のプラットフォームおよびスイッチ構成の拡張機能については、を参照してください。"[ONTAP 9リリースノート](#)"。

## ネットワーキング

更新	説明
<a href="#">Link Layer Discovery Protocol (LLDP)</a>	クラスタネットワークでは、LLDPがサポートされており、ONTAPではCisco Discovery Protocol (CDP) がサポートされていないクラスタスイッチとの連携が可能です。
<a href="#">LIFサアヒス</a>	新しいクライアント側のLIFサービスは、アウトバウンドのAD、DNS、LDAP、およびNIS要求に使用するLIFをより細かく制御します。

## S3オブジェクトストレージ

更新	説明
<a href="#">S3オブジェクト操作のサポートの追加</a>	ONTAP APIでは、次の操作がサポートされています。CreateBucket、DeleteBucket、DeleteObjects。さらに、ONTAP S3では、オブジェクトのバージョン管理と、PutBucketVersioning、GetBucketVersioning、ListBucketVersions。

## SAN

更新	説明
<a href="#">iSCSI LIFフェイルオーバー</a>	新しいiSCSI LIFフェイルオーバー機能では、SFOパートナーフェイルオーバー時およびローカルフェイルオーバー時にiSCSI LIFを自動および手動で移行できます。iSCSI LIFフェイルオーバーは、All SAN Array (ASA) プラットフォームで使用できます。

更新	説明
LUNからNVMeネームスペースへ、およびNVMeネームスペースからLUNへのシステム停止なしで移行	ONTAP CLIを使用したインプレース変換 <a href="#">既存のLUNをNVMeネームスペースに</a> または <a href="#">キソンノNVMeネームスペースからLUNに</a> 。

## セキュリティ

更新	説明
<a href="#">Autonomous Ransomware Protection (ARP) の機能拡張</a>	ARP検出アルゴリズムが強化され、追加のマルウェアの脅威を検出できるようになりました。また、新しいライセンスキーを使用してAutonomous Ransomware Protectionをアクティブ化します。ONTAPシステムをONTAP 9.10.1からアップグレードした場合も、以前のライセンスキーは同じ機能を提供します。
<a href="#">管理者による検証が複数必要です</a>	複数管理者による検証を有効にすると、ボリュームやSnapshotコピーの削除などの一部の処理は、指定した管理者の承認がないと実行できません。これにより、侵害を受けた管理者、悪意のある管理者、または経験の浅い管理者が、望ましくない変更やデータの削除を行うことを防止でき

## ストレージ効率

更新	説明
<a href="#">物理的な設置面積削減量の表示</a>	ボリュームで温度に基づくStorage Efficiencyを有効にしている場合は、volume show-footprintコマンドを使用して物理的なフットプリントの削減量を表示できます。
<a href="#">SnapLockでのFlexGroupボリュームのサポート</a>	SnapLockでは、FlexGroupボリュームに格納されたデータがサポートされます。FlexGroupボリュームは、SnapLock ComplianceモードとSnapLock Enterpriseモードでサポートされます。
<a href="#">SVM のデータ移動</a>	サポートされるAFFアレイの数が3つに増え、ソースとデスティネーションの両方でONTAP 9.11.1以降を実行している場合にSnapMirror関係がサポートされるようになりました。外部キー管理 (KMIP) も導入され、クラウドとオンプレミスの両方の環境で使用できます。

## ストレージリソース管理の機能拡張


更新	説明
<a href="#">ファイルシステム分析におけるSVMレベルのアクティビティ追跡</a>	アクティビティ追跡はSVMレベルで集計され、読み取り/書き込みIOPSとスループットを追跡することで、データに関する実用的な分析情報を瞬時に提供します。
<a href="#">ファイルアクセス時間の更新を有効にします</a>	有効にすると、現在のアクセス時間がユーザが指定した期間を超えた場合にのみ、FlexCache元のボリュームでアクセス時間が更新されます。


更新	説明
非同期ディレクトリの削除	非同期削除は、ストレージ管理者がボリュームに対する権限をNFSクライアントとSMBクライアントに許可した場合に使用できます。async deleteが有効になっている場合、Linuxクライアントではmvコマンドを使用でき、Windowsクライアントではrenameコマンドを使用してディレクトリを削除し、非表示のディレクトリに移動できます。 .ontaptrashbin ディレクトリ。
SnapLockでのFlexGroupボリュームのサポート	SnapLockでは、FlexGroupボリュームに格納されたデータがサポートされます。FlexGroupボリュームは、SnapLock ComplianceモードとSnapLock Enterpriseモードでサポートされます。SnapLockでは、FlexGroupボリュームでのSnapLock for SnapVault、イベントベースの保持、およびリーガルホールドの処理はサポートされていません。

## SVM管理の機能拡張

更新	説明
SVM のデータ移動	サポートされるAFFアレいの数が3つに増え、ソースとデスティネーションの両方でONTAP 9.11.1以降を実行している場合にSnapMirror関係がサポートされるようになりました。外部キー管理（KMIP）も導入され、クラウドとオンプレミスの両方の環境で使用できます。

## System Manager の略

更新	説明
SnapMirror非同期ポリシーを管理します。	<p>ボリュームやStorage VMを保護する場合は、System Managerを使用して、事前に作成されたカスタムのミラーとバックアップポリシーを追加したり、従来のポリシーを表示したり、保護ポリシーで定義されている転送スケジュールを上書きしたりできます。また、System Managerを使用して、ボリュームとStorage VMの保護関係を編集することもできます。</p> <div>  <p>ONTAP 9.8P12以降のONTAP 9.8パッチリリースを使用していて、System Managerを使用してSnapMirrorを設定していて、ONTAP 9.9.1またはONTAP 9.10.1リリースにアップグレードする場合は、ONTAP 9.9.1P13以降およびONTAP 9.10.1P10以降のパッチリリースをアップグレードに使用してください。</p> </div>
ハードウェアの可視化	System Managerのハードウェア可視化機能は、現在のすべてのAFFおよびFASプラットフォームをサポートしています。
システム分析のインサイト	System Managerの[Insights]ページには、容量やセキュリティに関する追加の情報や、クラスターやStorage VMの構成に関する新しい情報が表示されるため、システムの最適化に役立ちます。

更新	説明
操作性の向上	<ul style="list-style-type: none"> <li>新しく作成したボリュームはデフォルトでは共有できません。代わりに、NFSを介したエクスポートやSMB / CIFSを介した共有、権限レベルの指定など、デフォルトのアクセス権限を指定できます。</li> <li><b>SANの簡易化</b> - igroupを追加または編集するときに、System Managerユーザは、グループ内のイニシエータの接続ステータスを表示して、LUNデータにアクセスできるように、接続されているイニシエータをグループに含めることができます。</li> </ul>
アドバンストローカル階層（アグリゲート）処理	<p>System Manager管理者は、System Managerからの推奨事項を承認しない場合、ローカル階層の設定を指定できます。また、既存のローカル階層のRAID構成を編集することもできます。</p> <div>  <p>ONTAP 9.8P12以降のONTAP 9.8パッチリリースを使用して、System Managerを使用してSnapMirrorを設定していて、ONTAP 9.9.1またはONTAP 9.10.1リリースにアップグレードする場合は、ONTAP 9.9.1P13以降およびONTAP 9.10.1P10以降のパッチリリースをアップグレードに使用してください。</p> </div>
監査ログの管理	System Managerを使用して、ONTAP監査ログを表示および管理できます。

## ONTAP 9.10.1の新機能

ONTAP 9.10.1の新機能について説明します。

以前のONTAP 9リリース、ハードウェアプラットフォームとスイッチのサポート、既知の問題、および制限事項の詳細については、を参照してください。["ONTAP 9リリースノート"](#)。ONTAP 9リリースノート\_にアクセスするには、NetAppアカウントでサインインするか、NetAppアカウントを作成する必要があります。

ONTAPをアップグレードするには、[ONTAPをアップグレードする準備](#)。

### データ保護

更新	説明
<a href="#">SnapLockの保持期間を最大100年に設定</a>	ONTAP 9.10.1より前のリリースでは、サポートされる最大保持期間は2071年1月19日です。ONTAP 9.10.1以降のSnapLock Enterprise and Complianceでは、3058年10月26日までの保持期間と100年までの保持期間がサポートされます。保持期限を延長すると、古いポリシーが自動的に変換されます。
<a href="#">同じアグリゲートにSnapLockボリュームとSnapLock以外のボリュームを作成する機能</a>	ONTAP 9.10.1以降では、SnapLockボリュームとSnapLock以外のボリュームを同じアグリゲートに配置できるため、SnapLockボリューム用に別途SnapLockアグリゲートを作成する必要はありません。
<a href="#">整合グループ</a>	ボリュームとLUNを整合グループに編成してデータ保護ポリシーを管理し、複数のストレージボリュームにまたがるワークロードの書き込み順序に忠実であることを確認します。

更新	説明
パブリッククラウドでバックアップをアーカイブ	SnapMirror Cloudは、ONTAPバックアップをAWSやMS Azureの低コストのパブリッククラウドオブジェクトストレージクラスに階層化して長期保持を実現します。
セキュアなネットログオンチャネル通信のためのAESサポート	Netlogon認証サービスを使用してWindowsドメインコントローラに接続する場合は、Advanced Encryption Standard（AES）を使用してセキュアなチャネル通信を行うことができます。
SMBドメイントンネル認証でのKerberos	Kerberos認証は、NTLMに加えて、ONTAP管理用のドメイントンネル認証にも使用できます。これにより、Active Directoryのクレデンシャルを使用してONTAP CLIおよびSystem Manager GUIにログインする際の安全性が向上します。

## ファイルアクセスプロトコル

更新	説明
NFS over RDMA（NVIDIAのみ）	NFS over RDMA は RDMA アダプタを使用し、ストレージシステムメモリとホストシステムメモリの間でデータを直接コピーできるため、CPU の中断やオーバーヘッドは発生しません。NFS over RDMAを使用すると、サポート対象のNVIDIA GPUを搭載したホストで、GPUアクセラレーションワークロードにNVIDIA GPUDirect Storageを使用できます。

## MetroCluster

更新	説明
"MetroCluster IP構成でのレイヤ3 MetroCluster IPアドレスの設定"	レイヤ3構成のノードのMetroCluster IPアドレス、ネットマスク、およびゲートウェイを編集できます。
"MetroCluster FC構成でのノードのコントローラアップグレードの簡易化"	スイッチオーバーとスイッチバックを使用するアップグレードプロセスのアップグレード手順が簡易化されました。

MetroCluster構成のプラットフォームおよびスイッチ構成の拡張機能については、を参照してください。"ONTAP 9リリースノート"。

## ネットワーキング

更新	説明
RDMAクラスタインターコネク	A400またはASA A400ストレージシステムとX1151AクラスタNICを使用すると、マルチノードクラスタでハイパフォーマンスワークロードを高速化し、クラスタ内トラフィックにRDMAを活用できます。
システムSVMのLIFでステータスadminをdownに設定するには、確認が必要です	これにより、クラスタの適切な運用に欠かせないLIFが誤って停止するのを防ぐことができます。CLIでこの動作を呼び出すスクリプトがある場合は、確認手順に合わせてスクリプトを更新する必要があります。
ネットワーク配線の問題を自動的に検出して修復する	ポートに到達可能性問題が検出された場合、ONTAP System Manager は修復処理を実行して問題を解決することを推奨します。



更新	説明
<a href="#">Internet Protocol Security (IPsec;インターネットプロトコルセキュリティ) 証明書</a>	IPSecポリシーでは、認証用の証明書に加えて、事前共有キー (PSK) がサポートされます。
<a href="#">LIF のサービスポリシー</a>	ファイアウォールポリシーは廃止され、LIFのサービスポリシーに置き換えられました。アウトバウンドNTP要求に使用するLIFをより細かく制御できるように、新しいNTP LIFサービスポリシーも追加されました。

## S3オブジェクトストレージ

更新	説明
<a href="#">S3オブジェクトデータの保護、バックアップ、ディザスタリカバリ</a>	S3 SnapMirrorは、ONTAP S3オブジェクトストレージ用のデータ保護サービスを提供します。これには、ONTAP S3構成へのバケットのミラーリング、NetAppおよびネットアップ以外のデスティネーションへのバケットバックアップなどが含まれます。
<a href="#">S3監査</a>	ONTAP S3環境では、データイベントと管理イベントを監査できます。S3監査機能は既存の NAS 監査機能とほぼ同じであり、S3 および NAS の監査機能はクラスタ内で共存できます。

## SAN

更新	説明
<a href="#">NVMe ネームスペース</a>	ONTAP CLIを使用して、ネームスペースのサイズを拡張または縮小できます。System Managerを使用して、ネームスペースのサイズを拡張できます。
<a href="#">TCPでのNVMeプロトコルのサポート</a>	NVMe (Non-Volatile Memory Express) プロトコルは、TCPネットワーク経由のSAN環境で使用できます。

## セキュリティ

更新	説明
<a href="#">自律的なランサムウェア防御</a>	自律型ランサムウェア対策は、NAS環境でのワークロード分析を使用して、ランサムウェア攻撃を示す可能性のある異常なアクティビティについてアラートを生成します。Autonomous Ransomware Protectionは、スケジュールされたSnapshotコピーからの既存の保護に加えて、攻撃が検出されたときにSnapshotバックアップを自動的に作成します。
<a href="#">暗号化キー管理</a>	Azure Key VaultとGoogle Cloud Platform Key Management Serviceを使用して、ONTAPキーを格納、保護、利用し、キーの管理とアクセスを合理化します。

## ストレージ効率

更新	説明
温度に基づくストレージ効率	新規または既存のAFFボリュームでは、「デフォルト」モードまたは「効率的」モードのいずれかを使用して、温度に基づく Storage Efficiencyを有効にすることができます。
クラスタ間でSVMを無停止で移動する機能	負荷分散、パフォーマンスの向上、機器のアップグレード、データセンターの移行のために、ソースからデスティネーションへの物理AFFクラスタ間でSVMを再配置できます。

## ストレージリソース管理の機能拡張

更新	説明
ファイルシステム分析 (FSA) によるホットオブジェクトのアクティビティ追跡	システムパフォーマンスの評価を改善するために、FSAはホットオブジェクト（ファイル、ディレクトリ、ユーザ、およびトラフィックとスループットが最も多いクライアント）を特定できます。
グローバルファイル読み取りロック	移行中のすべてのキャッシュとオリジンで、単一ポイントから読み取りロックを有効にします。
NFSv4でのFlexCacheのサポート	FlexCacheでは、NFSv4プロトコルがサポートされます。
既存のFlexGroupボリュームからクローンを作成する	既存のFlexGroupボリュームを使用してFlexCloneボリュームを作成できます。
SVMディザスタリカバリソースでFlexVolボリュームをFlexGroupに変換する	FlexVolボリュームは、SVMディザスタリカバリソース内のFlexGroupボリュームに変換できます。

## SVM管理の機能拡張

更新	説明
クラスタ間でのSVMの無停止での移動	負荷分散、パフォーマンスの向上、機器のアップグレード、データセンターの移行のために、ソースからデスティネーションへの物理AFFクラスタ間でSVMを再配置できます。

## System Manager の略

更新	説明
System Managerのログでパフォーマンステレメトリログを有効にする	管理者は、System Managerでパフォーマンスに問題が発生した場合にテレメトリログを有効にしてから、サポートに連絡して問題の分析を依頼できます。
NetAppライセンスファイル	すべてのライセンスキーは、個別の28文字のライセンスキーではなくNetAppライセンスファイルとして提供されるため、1つのファイルを使用して複数の機能のライセンスを取得できます。
ファームウェアを自動的に更新します	System Manager管理者は、ファームウェアを自動的に更新するようにONTAPを設定できます。



更新	説明
リスク軽減のための推奨事項をレビューし、Active IQによって報告されるリスクを承認する	System Managerユーザは、Active IQによって報告されるリスクを確認し、リスクの軽減に関する推奨事項を確認できます。9.10.1以降では、リスクを承認することもできます。
管理者によるEMSイベント通知の受信を設定する	System Manager管理者は、Event Management System（EMS；イベント管理システム）イベント通知の配信方法を設定して、対応が必要なシステムの問題を通知することができます。
証明書を管理します	System Manager管理者は、信頼された認証局、クライアント/サーバ証明書、およびローカル（オンボード）認証局を管理できます。
System Managerを使用して、過去の容量使用状況を表示し、将来の容量ニーズを予測	Active IQとSystem Managerが統合されているため、管理者はクラスタの容量使用状況の履歴データを表示できます。
System Managerを使用して、Cloud Backup Serviceを使用してStorageGRIDにデータをバックアップする	Cloud Managerをオンプレミスに導入している場合は、Cloud Backup Service管理者がStorageGRIDにバックアップできます。AWSまたはAzureでCloud Backup Serviceを使用してオブジェクトをアーカイブすることもできます。
操作性の向上	<p>ONTAP 9.10.1以降では、次のことが可能になります。</p> <ul style="list-style-type: none"> <li>• 親ボリュームではなくLUNにQoSポリシーを割り当てる（VMware、Linux、Windows）</li> <li>• LUN QoS ポリシーグループを編集します</li> <li>• LUN を移動します</li> <li>• LUN をオフラインにします</li> <li>• ONTAPイメージのローリングアップグレードを実行する</li> <li>• ポートセットを作成してigroupにバインドする</li> <li>• ネットワーク配線の問題を自動的に検出して修復する</li> <li>• Snapshot コピーディレクトリへのクライアントアクセスを有効または無効にします</li> <li>• Snapshot コピーを削除する前に再利用可能なスペースを計算します</li> <li>• SMBキョウユウノケイソクテキカヨウセイノフィールドヘンコウヘノアクセス</li> <li>• より正確な表示単位を使用した容量測定値の表示</li> <li>• WindowsとLinuxのホスト固有のユーザとグループの管理</li> <li>• AutoSupport設定を管理します。</li> <li>• 個別の操作でボリュームのサイズを変更する</li> </ul>

## ONTAP 9.9.1の新機能

ONTAP 9.9.1の新機能について説明します。

以前のONTAP 9リリース、ハードウェアプラットフォームとスイッチのサポート、既知の問題、および制限事項の詳細については、を参照してください。 ["ONTAP 9リリースノート"](#)。ONTAP 9リリースノート\_にアクセスするには、NetAppアカウントでサインインするか、NetAppアカウントを作成する必要があります。

最新バージョンのONTAPにアップグレードするには、を参照してください。 [ONTAPをアップグレードする準備](#)。

## データ保護

更新	説明
<a href="#">"SnapLockおよびアグリゲートでのStorage Efficiencyのサポート"</a>	SnapLockボリュームおよびアグリゲートのStorage Efficiency機能が拡張され、データコンパクション、ボリューム間重複排除、アダプティブ圧縮、TSSE（Temperature Sensitive Storage Efficiency）など、WORMデータのスペースを大幅に削減できるようになりました。
<a href="#">"SVM DRソースとデスティネーションでの異なるSnapshotポリシーの設定のサポート"</a>	SVM DR設定では、mirror-vaultポリシーを使用してソースとデスティネーションに異なるSnapshotポリシーを設定できます。デスティネーションのポリシーがソースのポリシーで上書きされることはありません。
<a href="#">"System ManagerでのSnapMirror Cloudのサポート"</a>	System ManagerでSnapMirror Cloudがサポートされるようになりました。
<a href="#">監査を有効にしたSVM</a>	クラスターでサポートされる監査を有効にしたSVMの最大数が50から400に拡張されました。
<a href="#">SnapMirror Synchronous</a>	HAペアあたりのサポートされるSnapMirror Synchronousエンドポイントの最大数が80から160に拡張されました。
<a href="#">FlexGroup SnapMirror トポロジ</a>	FlexGroupボリュームは、A→B、A→Cなど、2つ以上のファンアウト関係をサポートします。FlexVolボリュームと同様に、FlexGroupのファンアウトは最大8つのファンアウトレグをサポートし、A→B→Cのように最大2レベルのカスケードをサポートします。

## ファイルアクセスプロトコル

更新	説明
<a href="#">"LDAPリファール追跡の機能拡張"</a>	LDAPリファール追跡は、LDAPの署名と封印、暗号化されたTLS接続、およびLDAPSポート636経由の通信でサポートされます。
<a href="#">"任意のポートでLDAPSをサポート"</a>	LDAPSは任意のポートに設定できます。デフォルトはポート636です。
<a href="#">"デフォルトで有効になるNFSv4.xのバージョン"</a>	NFSv4.0、NFSv4.1、およびNFSv4.2はデフォルトで有効になります。
<a href="#">"NFSv4.2のサポート"</a>	NFSv4.2が有効になっている場合は、NFSラベルのMandatory Access Control（MAC；必須アクセス制御）がサポートされます。この機能を使用すると、ONTAP NFSサーバはMACに対応し、ストレージと読み出しを実行できます。 sec_label クライアントによって送信される属性。

## MetroCluster

更新	説明
"レイヤ3での共有リンクのIPサポート"	MetroCluster IP設定は、IPルーテッド（レイヤ3）バックエンド接続で実装できます。
"8ノードクラスタのサポート"	永続的な8ノードクラスタは、IPおよびファブリック接続構成でサポートされます。さらに、AFF ASAプラットフォームでは、8ノードのMCC IP構成がサポートされます。

MetroCluster構成のプラットフォームおよびスイッチ構成の拡張機能については、を参照してください。"ONTAP 9リリースノート"。

## ネットワーキング

更新	説明
"クラスタの耐障害性"	<ul style="list-style-type: none"> <li>2ノードスイッチレスクラスタのポートの監視と回避（従来はスイッチ構成でのみ使用可能）</li> <li>クラスタネットワーク経由でデータを提供できないノードの自動フェイルオーバー</li> <li>パケット損失が発生しているクラスタパスを表示する新しいツール</li> </ul>
"仮想IP（VIP）LIFの拡張機能"	<ul style="list-style-type: none"> <li>Border Gateway Protocol（BGP;ボーダーゲートウェイプロトコル）のAutonomous System Number（ASN;自律システム番号）は、4バイトの非負整数をサポートします。</li> <li>Multi-Exit Discriminator（MED）を使用すると、パスの優先順位付けをサポートした高度なルート選択が可能になります。MEDは、BGPアップデートメッセージのオプション属性です。</li> <li>VIP BGP では、BGP ピアグループ化を使用して設定を簡素化するデフォルトルート自動化が提供されます。</li> </ul>

## S3オブジェクトストレージ

更新	説明
"S3メタデータとタグのサポート"	ONTAP S3サーバは、ユーザ定義のオブジェクトメタデータとオブジェクトのタグ付けをサポートし、S3クライアントとアプリケーションに高度な自動化機能を提供します。

## SAN

更新	説明
Foreign LUN Import（FLI）	NetApp Support SiteのSAN LUN Migrateアプリケーションを使用すると、FLIのInteroperability Matrixに記載されていない外部アレイを認定できます。
NVMe-oFリモートパスアクセス	フェイルオーバーで直接パスアクセスが失われた場合でも、リモートI/Oを使用してシステムをリモートパスにフェイルオーバーし、データアクセスを継続できます。

更新	説明
ASAでの12ノードクラスタのサポート	AFF ASA構成では12ノードクラスタがサポートされます。ASAクラスタでは、さまざまなASAシステムタイプを混在させることができます。
ASAのNVMe-oFプロトコル	NVMe-oFプロトコルはAFF ASAシステムでもサポートされます。
	<ul style="list-style-type: none"> <li>• 既存のigroupで構成されるigroupを作成できます。。</li> <li>• igroupまたはホストイニシエータのエイリアスとして機能するigroupまたはホストイニシエータに概要を追加できます。</li> <li>• igroupを2つ以上のLUNに同時にマッピングできます。</li> </ul>
単一LUNのパフォーマンスの向上	AFFの単一LUNのパフォーマンスが大幅に向上し、仮想環境への導入を簡易化するのに最適です。たとえば、A800ではランダムリードIOPSが最大400%向上します。

## セキュリティ

更新	説明
System Managerへのログイン時にCisco Duoを使用した多要素認証のサポート	ONTAP 9.9.1P3以降では、Cisco DuoをSAMLアイデンティティプロバイダ（IdP）として設定して、ユーザがSystem ManagerにログインするときにCisco Duoを使用して認証できるようにすることができます。

## ストレージ効率

更新	説明
"ボリュームのファイル数を最大に設定"	volumeパラメータを使用してファイルの最大数を自動化`-files-set-maximum`ファイルの上限を監視する必要がありません。

## ストレージリソース管理の機能拡張

更新	説明
System Managerのファイルシステム分析（FSA）管理の機能拡張	FSAには、検索とフィルタリング、およびFSAの推奨事項に対するアクションを実行するためのSystem Manager機能が追加されています。
負の検索キャッシュのサポート	FlexCacheボリュームの「file not found」エラーをキャッシュして、元のボリュームへの呼び出しに起因するネットワークトラフィックを削減します。
FlexCacheディザスタリカバリ	キャッシュ間でクライアントを無停止で移行できます。
FlexGroupのSnapMirrorカスケードとファンアウトのサポート	FlexGroupボリュームのSnapMirrorカスケード関係とSnapMirrorファンアウト関係をサポートします。
FlexGroupでのSVMディザスタリカバリのサポート	FlexGroupボリュームに対するSVMディザスタリカバリのサポートでは、SnapMirrorを使用してSVMの設定とデータをレプリケートおよび同期することで、冗長性が確保されます。

更新	説明
FlexGroupボリュームの論理スペースのレポートと適用のサポート	FlexGroupユーザが消費する論理スペースを表示して制限することができます。
qtreeテノSMBアクセスノサポート	SMBアクセスは、SMBが有効なFlexVolおよびFlexGroupボリューム内のqtreeでサポートされます。

## System Manager の略

更新	説明
Active IQで報告されるリスクがSystem Managerに表示される	System Managerを使用してNetApp Active IQにリンクすると、リスクを軽減し、ストレージ環境のパフォーマンスと効率を向上させる機会を報告します。
ローカル階層を手動で割り当てる	System Managerでは、ボリュームおよびLUNを作成および追加するときに、ローカル階層を手動で割り当てることができます。
ディレクトリの高速削除	System Managerでは、低レイテンシの高速ディレクトリ削除機能を使用してディレクトリを削除できます。
Ansibleプレイブックを生成	System Managerユーザは、一部のワークフロー向けにUIからAnsible Playbookを生成し、自動化ツールで使用してボリュームやLUNを繰り返し追加または編集できます。
ハードウェアの視覚化	ONTAP 9.8で初めて導入されたハードウェア可視化機能では、すべてのAFFプラットフォームがサポートされるようになりました。
Active IQ 統合	System Managerユーザは、クラスタに関連するサポートケースを表示してダウンロードできます。また、NetApp Support Siteで新しいサポートケースを送信するために必要なクラスタの詳細をコピーすることもできます。System Managerユーザは、Active IQからアラートを受信して、新しいファームウェアの更新が利用可能になったときに通知することができます。その後、System Managerを使用してファームウェアイメージをダウンロードし、アップロードできます。
Cloud Managerの統合	System Managerユーザは、Cloud Backup Serviceを使用してパブリッククラウドエンドポイントにデータをバックアップする保護を設定できます。
データ保護プロビジョニングワークフローの機能拡張	System Managerユーザは、データ保護の設定時にSnapMirrorデスティネーションとigroupの名前を手動で指定できます。
ネットワークポート管理の強化	[ネットワークインターフェイス]ページでは、ホームポートのインターフェイスを表示および管理する機能が強化されています。
システム管理の機能拡張	<ul style="list-style-type: none"> <li>• <a href="#">ネストされたigroupのサポート</a></li> <li>• <a href="#">1回のタスクで複数のLUNをigroupにマッピングし、処理中にWWPNエイリアスを使用してフィルタリングできます。</a></li> <li>• <a href="#">NVMe-oF LIFの作成時に、両方のコントローラで同一のポートを選択する必要がなくなりました。</a></li> <li>• <a href="#">各ポートのトグルボタンを使用してFCポートを無効にします。</a></li> </ul>

更新	説明
System ManagerでのSnapshotコピーに関する情報の表示の強化	<ul style="list-style-type: none"> <li>• System Managerユーザは、SnapshotコピーのサイズとSnapMirrorラベルを表示できます。</li> <li>• Snapshotコピーが無効な場合、Snapshotコピーリザーブはゼロに設定されます。</li> </ul>
ストレージ階層の容量と場所の情報に関するSystem Managerの表示機能を強化	<ul style="list-style-type: none"> <li>• 新しい[* <b>Tiers</b>列には、各ボリュームが配置されているローカル階層（アグリゲート）が表示されます。]</li> <li>• System Managerには、ローカル階層（アグリゲート）レベルに加え、クラスタレベルの使用済み物理容量と使用済み論理容量が表示されます。</li> <li>• 新しい容量表示フィールドを使用すると、容量を監視したり、容量に近づいているボリュームや使用率が低いボリュームを追跡したりできます。</li> </ul>
EMS緊急アラートおよびその他のエラーと警告をSystem Managerに表示する	24時間以内に受信したEMSアラートの数、およびその他のエラーや警告は、System Managerの[Health]カードに表示されます。



# System ManagerとBlueXPの統合

ONTAP 9.12.1以降、System ManagerはBlueXPと完全に統合されています。BlueXPを使用すると、使い慣れたSystem Managerダッシュボードを維持しながら、単一のコントロールプレーンからハイブリッドマルチクラウドインフラを管理できます。

BlueXPを使用すると、クラウドストレージ（Cloud Volumes ONTAP など）の作成と管理、ネットアップのデータサービス（Cloud Backupなど）の使用、多数のオンプレミスストレージデバイスやエッジストレージデバイスの制御が可能になります。

BlueXPでSystem Managerを使用するには次の手順に従います

## 手順

1. Webブラウザを開き、クラスタ管理ネットワークインターフェイスのIPアドレスを入力します。

クラスタがBlueXPに接続されている場合は、ログインプロンプトが表示されます。

2. [BlueXPに進む]をクリックして、BlueXPへのリンクをクリックします。



システム設定で外部ネットワークがブロックされている場合は、BlueXPにアクセスできません。BlueXPを使用してSystem Managerにアクセスするには、アドレス「cloudmanager.cloud.netapp.com」にシステムからアクセスできることを確認する必要があります。それ以外の場合は、ONTAPシステムにインストールされているバージョンのSystem Managerをプロンプトで使用できます。

3. BlueXPログインページで、「NetApp Support Site 資格情報でログイン」を選択し、資格情報を入力します。

既にBlueXPを使用していて、電子メールとパスワードを使用してログインしている場合は、代わりにそのログインオプションを使用する必要があります。

["BlueXPへのログインの詳細をご覧ください"](#)。

4. プロンプトが表示されたら、新しいBlueXPアカウントの名前を入力します。

ほとんどの場合、BlueXPはクラスタのデータに基づいて自動的にアカウントを作成します。

5. クラスタのクラスタ管理者のクレデンシャルを入力します。

## 結果

System Managerが表示され、クラスタをBlueXPから管理できるようになります。

## BlueXPからクラスタを直接検出します

BlueXPには、クラスタを検出して管理するための2つの方法があります。

- System Managerで管理を直接検出

これは、前のセクションで説明した、リダイレクトに続く検出オプションと同じです。



- コネクタを介した検出

Connectorは環境にインストールされるソフトウェアで、System Managerを使用して管理機能にアクセスしたり、データレプリケーション、バックアップとリカバリ、データ分類、データ階層化などの機能を備えたBlueXPクラウド サービス にアクセスしたりすることができます。

にアクセスします ["BlueXPのマニュアル"](#) 検出と管理のオプションの詳細については、を参照してください。

## BlueXPの詳細をご覧ください

- ["BlueXPの概要"](#)
- ["BlueXPを使用して、NetApp AFF およびFAS システムを管理できます"](#)

# 概要と概念

## ONTAP の概念

### 概念の概要

クラスタストレージ、高可用性、仮想化、データ保護など、ONTAPデータ管理ソフトウェアには次の概念があります。Storage Efficiency、セキュリティ、FabricPoolストレージ解決策を設定する前に、ONTAP のすべての機能とメリットを理解しておく必要があります。

追加情報の場合は、以下を参照してください。

- ["クラスタと SVM の管理"](#)
- ["ハイアベイラビリティ \(HA\) ペア"](#)
- ["ネットワークと LIF の管理"](#)
- ["ディスクおよびアグリゲートの管理"](#)
- ["FlexVol 、 FlexClone テクノロジー、 Storage Efficiency 機能"](#)
- ["SAN ホストプロビジョニング"](#)
- NAS ファイルアクセス
  - ["NFS の管理"](#)
  - ["SMBの管理"](#)
- ["ディザスタリカバリとアーカイブ"](#)

### ONTAPプラットフォーム

ONTAP データ管理ソフトウェアは、ブロックアクセスプロトコルまたはファイルアクセスプロトコルを使用してデータを読み書きするアプリケーションに、ユニファイドストレージを提供します。高速フラッシュから低コストの回転式メディア、クラウドベースのオブジェクトストレージまで、さまざまなストレージ構成がサポートされます。

ONTAPの実装は、ネットアップが開発したFAS、AFF AシリーズとCシリーズ、オールSANフラッシュアレイASAプラットフォーム、コモディティハードウェア (ONTAP Select) 、プライベートクラウド、パブリッククラウド、ハイブリッドクラウド (Cloud Volumes ONTAP) で実行されます。専門的な導入により、業界最高のコンバージドインフラ (FlexPod Datacenter) が提供されます。

これらの実装を組み合わせることで、\_ ネットアップデータファブリックの基本的なフレームワークが形作られます。\_ は、共通のソフトウェア定義型アプローチでデータを管理し、プラットフォーム間で高速かつ効率的なレプリケーションを実現します。

## クラスタストレージ

ONTAP の現在のバージョンは、もともとはネットアップのスケールアウトクラスタストレージアーキテクチャ用に開発されたものです。これは、ONTAP のデータセンター実装で一般的に採用されているアーキテクチャです。この実装でほとんどの ONTAP の機能が使用されるため、最初は ONTAP テクノロジーの概念を理解しておくことを推奨します。

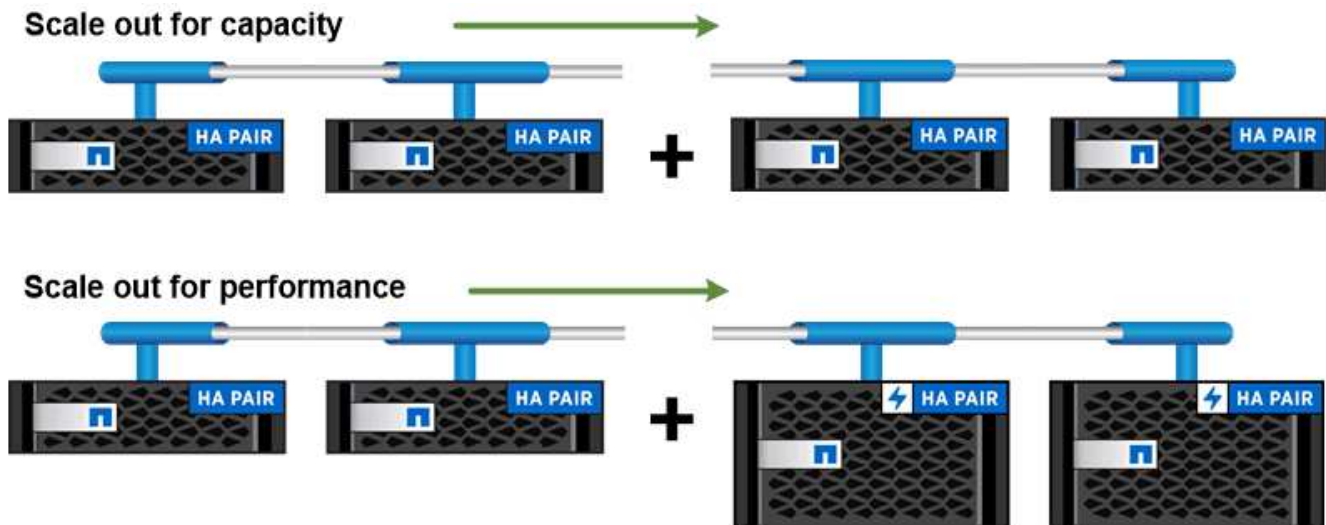
一般にデータセンターアーキテクチャでは、ONTAP データ管理ソフトウェアを実行する専用の FAS コントローラまたは AFF コントローラを導入します。各コントローラとそのストレージ、ネットワーク接続、およびコントローラで実行されている ONTAP のインスタンスを合わせて、*node*. と呼びます

ノードはハイアベイラビリティ（HA）ペアを構成します。このペアを複数配置したものがクラスタです（SAN の場合は最大 12 ノード、NAS の場合は最大 24 ノード）。ノードは、専用のプライベートなクラスタインターコネクトを介して相互に通信します。

ノードストレージは、コントローラのモデルに応じて、フラッシュディスク、大容量ドライブ、またはその両方で構成されます。データへのアクセスはコントローラのネットワークポートから提供されます。物理ストレージとネットワーク接続のリソースは仮想化され、クラスタ管理者のみが見ることができ、NAS クライアントや SAN ホストからは見えません。

HA ペアの各ノードで同じストレージレイモデルを使用する必要があります。それ以外の場合は、サポートされている任意のコントローラの組み合わせを使用できます。スケールアウトすることで、容量を増やすには同じストレージレイモデルを使用するノードを追加し、パフォーマンスを高めるにはハイエンドのストレージレイを使用するノードを追加します。

もちろん、従来の方法によるスケールアップもすべて可能で、必要に応じてディスクやコントローラをアップグレードできます。ONTAP の仮想ストレージインフラでは、データを無停止で簡単に移動できるため、スケールアップやスケールアウトをダウンタイムなしで実行できます。



*You can scale out for capacity by adding nodes with like controller models, or for performance by adding nodes with higher-end storage arrays, all while clients and hosts continue to access data.*

## ハイアベイラビリティペア

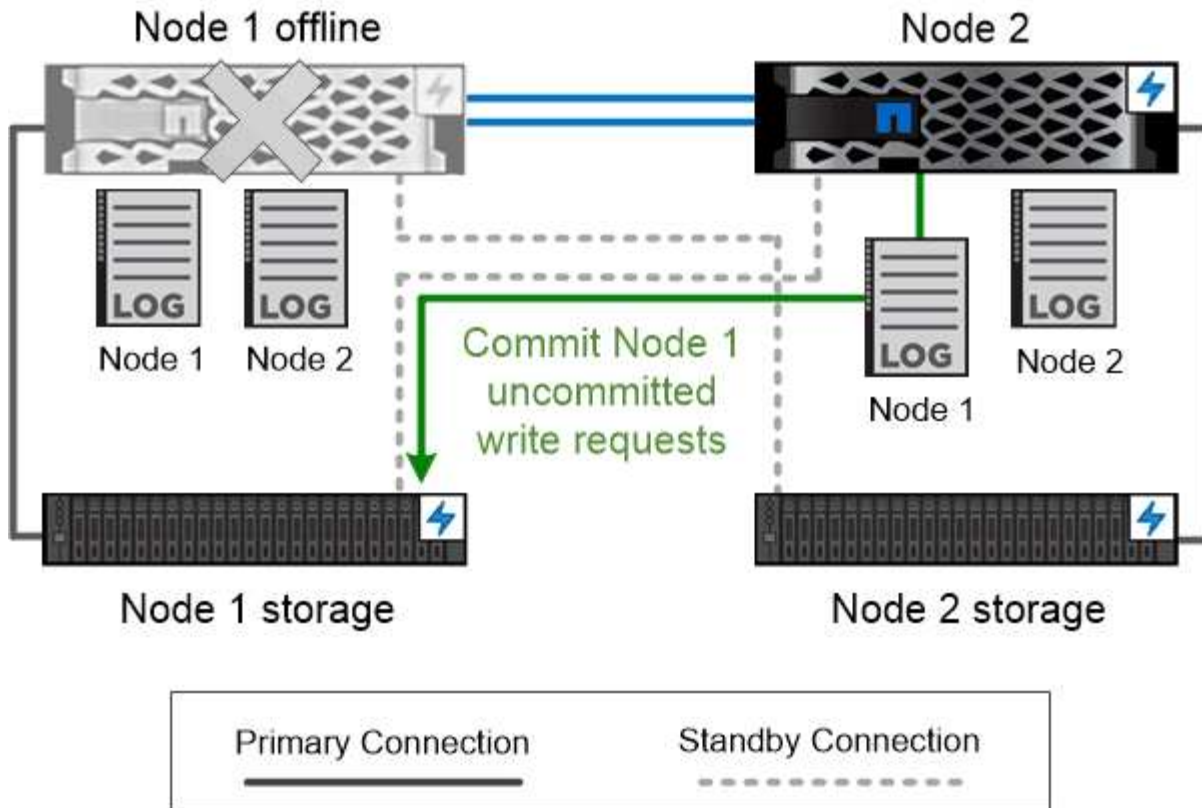
クラスタノードは、フォールトトレランスとノンストップオペレーションを実現するために、\_high-availability (HA) ペア\_で構成されます。ノードに障害が発生した場合や定期的なメンテナンスのためにノードを停止する必要がある場合、パートナーはそのストレージをテイクオーバーしてデータの提供を継続できます。ノードがオンラインに戻ったときに、partner\_ギブバック\_storageを提供します。

HA ペアは、必ず同じモデルのコントローラで構成されます。通常、コントローラは冗長電源装置を備えた同じシャーシに配置されます。

HAペアはフォールトトレラントなノードであり、さまざまな方法で相互に通信できます。各ノードでは、パートナーの動作を継続的に確認したり、パートナーの不揮発性メモリのログデータをミラーリングしたりできます。あるノードへの書き込み要求が発生した場合、両方のノードの NVRAM に要求が記録されたのち、クライアントまたはホストに応答が返されます。フェイルオーバーの際は、障害が発生したノードのコミットされていない書き込み要求が稼働しているパートナーによってディスクにコミットされてデータの整合性が維持されます。

テイクオーバーが発生した場合、各ノードはもう一方のコントローラのストレージメディアに接続して他方のノードのストレージにアクセスできます。ネットワークパスのフェイルオーバーメカニズムにより、クライアントとホストは稼働しているノードと引き続き通信できます。

可用性を確保するには、フェイルオーバー時の追加のワークロードに対応できるように、各ノードのパフォーマンス容量利用率を 50% に抑える必要があります。同じ理由で、1つのノードに割り当てる NAS 仮想ネットワークインターフェイスは最大数の 50% までにすることを推奨します。



*On failover, the surviving partner commits the failed node's uncommitted write requests to disk, ensuring data consistency.*

\* \_ 仮想 ONTAP 実装でのテイクオーバーとギブバック \_ \*

ONTAP Select for AWS や Cloud Volumes ONTAP のような仮想化された「不要な」 ONTAP 環境では、ノード間でストレージが共有されません。ノードが停止した場合、そのノードのデータの同期ミラーリングされたコピーからパートナーがデータの提供を続行します。ノードのストレージはテイクオーバーせず、データ提供機能だけをテイクオーバーします。

## AutoSupport と Active IQ デジタルアドバイザー

ONTAP は、Web ポータルとモバイルアプリを通じて、人工知能を利用したシステムの監視とレポートを提供します。ONTAP の AutoSupport コンポーネントは、Active IQ デジタルアドバイザーによって分析された計測データを送信します。

Active IQ では、クラウドベースのポータルとモバイルアプリを通じて、実用的な予測分析とプロアクティブなサポートを提供することで、グローバルハイブリッドクラウド全体でデータインフラを最適化できます。SupportEdge との契約が締結されているネットアップのすべてのお客様は、Active IQ が提供するデータ主体の分析情報と推奨事項を利用できます（機能は製品やサポートレベルによって異なります）。

Active IQ でできることは次のとおりです。

- アップグレードを計画する。Active IQ では、ONTAP の新しいバージョンにアップグレードすることで解

決可能な問題が環境内で特定されます。また、アップグレードを計画する際に役立つ Upgrade Advisor コンポーネントも用意されています。

- システムの健全性を表示します。Active IQ ダッシュボードで、健全性に関する問題が報告されるため、これらの問題の解決に役立ちます。システム容量を監視して、ストレージスペースが不足しないようにします。
- パフォーマンスを管理Active IQ には、System Manager に表示されるよりも長時間にわたるシステムパフォーマンスが表示されます。パフォーマンスに影響を与えている構成やシステムの問題を特定します。
- 効率性の最大化Storage Efficiency 指標を表示し、より多くのデータをより少ないスペースに格納する方法を特定します。
- インベントリと構成を表示します。Active IQ は、インベントリおよびソフトウェアとハードウェアの構成に関するすべての情報を表示します。サービス契約がいつ期限切れになるかを確認して、契約期間を終了しないようにします。

#### 関連情報

["ネットアップのマニュアル：Active IQ Digital Advisor"](#)

["Active IQ を起動します"](#)

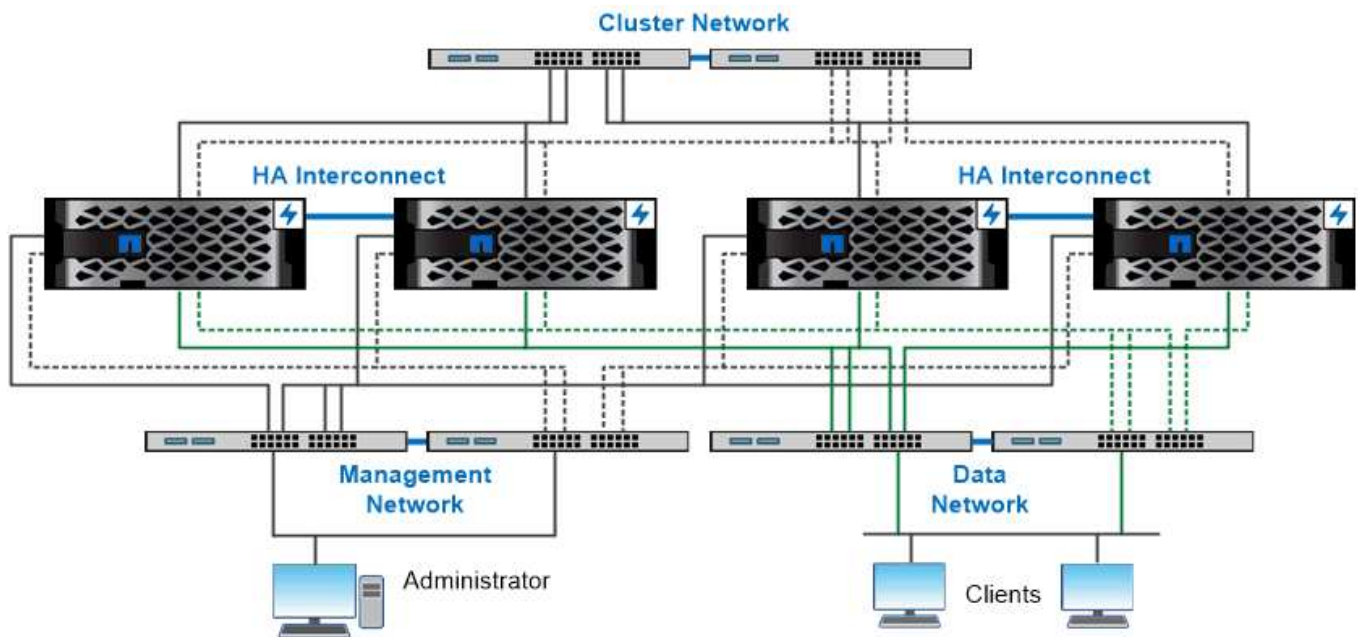
["SupportEdge サービス"](#)

## ネットワークアーキテクチャ

### ネットワークアーキテクチャの概要

ONTAP データセンターの一般的なネットワークアーキテクチャは、クラスターインターコネクト、クラスタ管理用の管理ネットワーク、およびデータネットワークで構成されます。イーサネット接続用の物理ポートには NIC（ネットワークインターフェイスカード）を使用し、FC 接続用の物理ポートには HBA（ホストバスアダプタ）を使用します。





*The network architecture for an ONTAP datacenter implementation typically consists of a cluster interconnect, a management network for cluster administration, and a data network.*

## 論理ポート

各ノードに搭載されている物理ポートに加え、\_logical ports\_を使用してネットワークトラフィックを管理できます。論理ポートには、インターフェイスグループと VLAN があります。

## インターフェイスグループ

\_インターフェイスグループ\_ 複数の物理ポートを1つの論理「トランクポート」に結合します。複数のPCIスロット内のNICのポートで構成されるインターフェイスグループを作成することで、1つのスロットに障害が発生した場合でもビジネスクリティカルなトラフィックの停止を回避することができます。

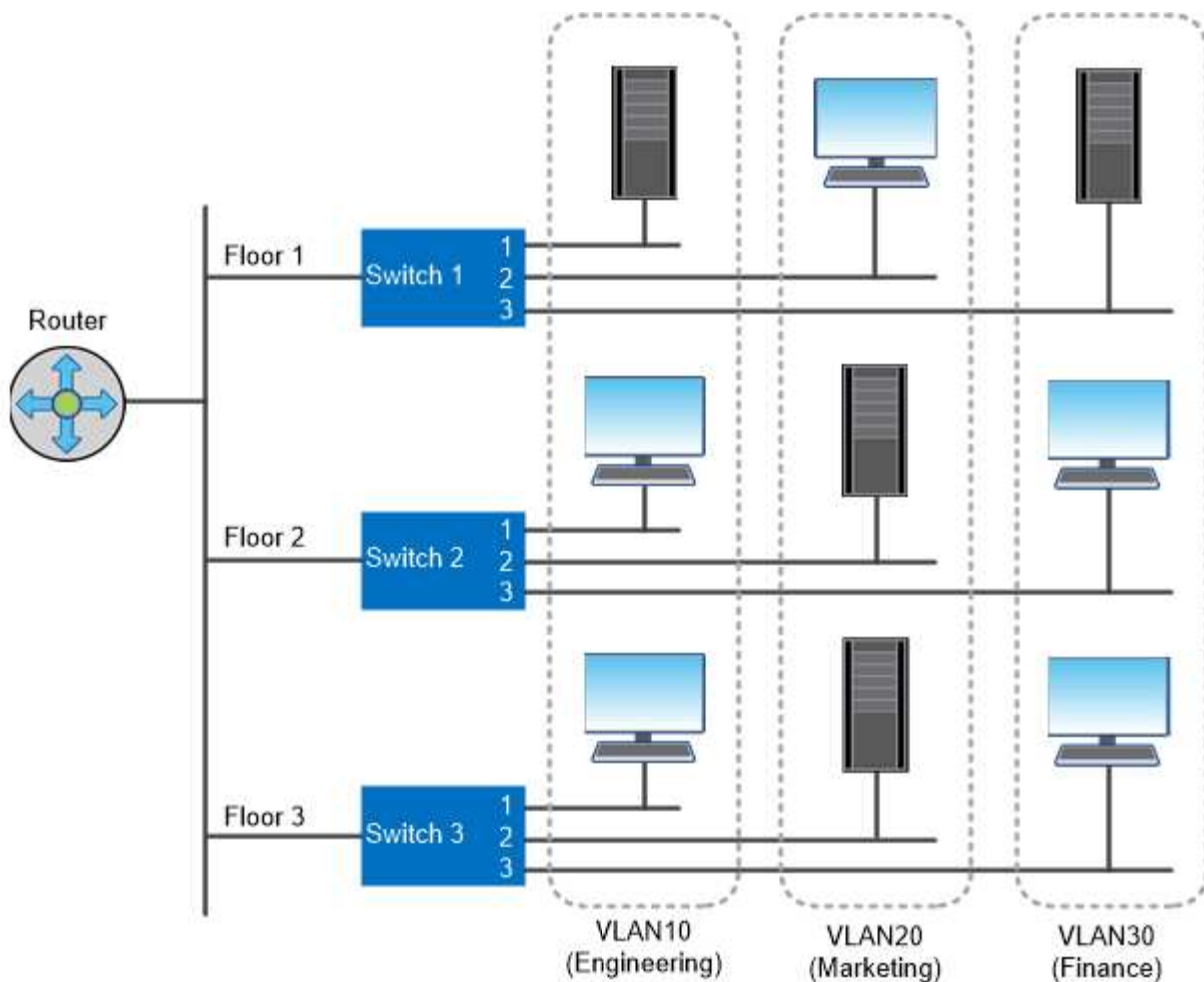
インターフェイスグループには、シングルモード、マルチモード、またはダイナミックマルチモードがあります。モードごとにフォールトトレランスのレベルが異なります。どちらかのタイプのマルチモードインターフェイスグループを使用すると、ネットワークトラフィックを負荷分散できます。

## VLAN

VLAN ネットワークポート（インターフェイスグループ）からのトラフィックを、物理的な境界ではなくスイッチポートに基づいて定義された論理セグメントに分離します。VLAN に属する \_end-stations\_ は、機能またはアプリケーションによって関連付けられます。

たとえば、エンジニアリングやマーケティングなどの部門単位、またはリリース 1 やリリース 2 などのプロジェクト単位で、エンドステーションをまとめることができます。VLAN ではエンドステーションが物理的に近接していることは重要ではないため、地理的に離れた場所に配置することもできます。





*You can use VLANs to segregate traffic by department.*

業界標準のネットワークテクノロジーのサポート

ONTAP は、業界標準の主要なネットワークテクノロジーをすべてサポートしています。たとえば、IPspace、DNS ロードバランシング、SNMP トラップなどです。

ブロードキャストドメイン、フェイルオーバーグループ、およびサブネットについては、[で説明しています](#)  
[NAS パスのフェイルオーバー](#)。

#### IPspace

IPspace を使用すると、クラスタ内の仮想データサーバごとに個別の IP アドレススペースを作成できます。これにより、管理上分離されたネットワークドメインのクライアントが、IP アドレスの同じサブネット範囲内の重複した IP アドレスを使用してクラスタのデータにアクセスできるようになります。

たとえば、サービスプロバイダは、クラスタへのアクセス用に同じ IP アドレスを使用してテナントごとに異なる IPspace を設定できます。

#### DNS ロードバランシング

DNS ロードバランシング \_ を使用すると、使用可能なポートにユーザネットワークトラフィックを分散でき

ます。DNS サーバは、インターフェイスにマウントされているクライアントの数に基づいて、トラフィック用のネットワークインターフェイスを動的に選択します。

## SNMP トラップ

SNMP トラップ \_ を使用すると、しきい値または障害を定期的にチェックできます。SNMP トラップは、SNMP エージェントから SNMP マネージャに非同期で送信されるシステム監視情報をキャプチャします。

## FIPS 準拠

ONTAP は、すべての SSL 接続に対する連邦情報処理標準（FIPS）140-2 に準拠しています。SSL FIPS モードを有効または無効にしたり、SSL プロトコルをグローバルに設定したり、RC4 などの弱い暗号を無効にしたりできます。

## RDMA の概要

ONTAP の Remote Direct Memory Access（RDMA）ソリューションは、レイテンシの影響を受けやすい広帯域のワークロードをサポートします。RDMA を使用すると、ストレージシステムメモリとホストシステムメモリの間でデータを直接コピーでき、CPU の中断やオーバーヘッドは発生しません。

## RDMA 経由の NFS

ONTAP 9.10.1 以降では、を設定できます ["RDMA 経由の NFS"](#) NVIDIA GPU を搭載したホストで GPU アクセラレーション対応のワークロードに NVIDIA GPUDirect Storage を使用できるようにするため。

## RDMA クラスターインターコネクト

RDMA クラスターインターコネクトにより、レイテンシが低減され、フェイルオーバー時間が短縮され、クラスター内のノード間の通信が高速化されます。

ONTAP 9.10.1 以降では、X1151A クラスター NIC を使用する場合、特定のハードウェアシステムでクラスターインターコネクト RDMA がサポートされます。ONTAP 9.13.1 以降では、X91153A NIC でクラスターインターコネクト RDMA もサポートされます。各 ONTAP リリースでサポートされるシステムについては、表を参照してください。

システム	サポートされる <b>ONTAP</b> のバージョン
<ul style="list-style-type: none"><li>• A400</li><li>• ASA A400</li></ul>	ONTAP 9.10.1 以降
<ul style="list-style-type: none"><li>• AFF A900 の略</li><li>• ASA A900</li><li>• FAS9500</li></ul>	ONTAP 9.13.1 以降

ストレージシステムが適切にセットアップされていれば、RDMA インターコネクトを使用するための追加の設定は必要ありません。

## クライアントプロトコル

ONTAP は、業界標準の主要なクライアントプロトコルである NFS、SMB、FC、FCoE、iSCSI をすべてサポートしています。NVMe/FC および S3。

### NFS

NFS は、UNIX および Linux システム向けの従来のファイルアクセスプロトコルです。クライアントは、次のプロトコルを使用して ONTAP ボリューム内のファイルにアクセスできます。

- NFSv3
- NFSv4
- NFSv4.2
- NFSv4.1
- pNFS

ファイルアクセスは、UNIX 形式の権限、NTFS 形式の権限、またはその両方の組み合わせを使用して制御できます。

クライアントは、NFS プロトコルと SMB プロトコルの両方を使用して同じファイルにアクセスできます。

### SMB

SMB は、Windows システム向けの従来のファイルアクセスプロトコルです。クライアントは、SMB 2.0、SMB 2.1、SMB 3.0、および SMB 3.1.1 の各プロトコルを使用して ONTAP ボリューム内のファイルにアクセスできます。NFS と同様に、複数の形式の権限の組み合わせがサポートされています。

SMB 1.0 も使用可能ですが、ONTAP 9.3 以降のリリースではデフォルトで無効になっています。

### FC

Fibre Channel は、ネットワークに接続された最初のブロックプロトコルです。ブロックプロトコルは、ファイルではなく、仮想ディスク全体をクライアントに提供します。従来の FC プロトコルは専用の FC ネットワークと FC スイッチを使用し、クライアントコンピュータに FC ネットワークインターフェイスが必要です。

仮想ディスクは LUN として表され、1 つ以上の LUN が ONTAP ボリュームに格納されます。FC、FCoE、および iSCSI の各プロトコルを使用して同じ LUN にアクセスできますが、複数のクライアントから同じ LUN にアクセスできるのは、クライアントが書き込みの競合を防ぐように設定されたクラスタに属している場合だけです。

### FCoE

FCoE は、FC プロトコルと基本的に同じですが、従来の FC 転送の代わりにデータセンタークラスのイーサネットネットワークを使用します。クライアントには FCoE 固有のネットワークインターフェイスが必要です。

### iSCSI

iSCSI は、標準のイーサネットネットワークで実行できるブロックプロトコルです。ほとんどのクライアントオペレーティングシステムには、標準のイーサネットポートで動作するソフトウェアイニシエータが搭載されています。iSCSI は、特定のアプリケーションにブロックプロトコルが必要で、使用可能な専用の FC ネット

ワークがない場合に適しています。

## NVMe/FC

NVMe / FC は、フラッシュベースのストレージと連携するように設計された最も新しいブロックプロトコルです。スケーラブルなセッションを通じてレイテンシの大幅な低減と並列処理機能の強化を実現できるため、インメモリデータベースや分析など、低レイテンシと高スループットが求められるアプリケーションに適しています。

FC や iSCSI とは異なり、NVMe は LUN を使用しません。代わりに、ONTAP ボリュームに格納されているネームスペースを使用します。NVMe ネームスペースには、NVMe プロトコルでのみアクセスできます。

## S3

ONTAP 9.8以降では、ONTAP クラスタでONTAP Simple Storage Service (S3) サーバを有効にして、S3バケットを使用してオブジェクトストレージ内でデータを提供できます。

ONTAP では、S3オブジェクトストレージを提供するオンプレミスのユースケースを2つサポートしています。

- FabricPool 階層をローカルクラスタ（ローカルバケットへの階層）またはリモートクラスタ（クラウド階層）のバケットに配置します。
- S3 クライアントアプリケーションからローカルクラスタまたはリモートクラスタのバケットへのアクセス。



ONTAP S3 は、ハードウェアや管理の追加なしで既存のクラスタの S3 機能を利用する場合に適しています。300TB を超える環境の場合、ネットアップの解決策ソフトウェアは、オブジェクトストレージ向けの主力製品である StorageGRID として引き続き提供されます。詳細はこちら ["StorageGRID"](#)。

## ディスクとアグリゲート

=  
:allow-uri-read:

### ローカル階層（アグリゲート）とRAIDグループ

最新の RAID テクノロジーは、障害が発生したディスクのデータをスペアディスクに再構築することでディスク障害から保護します。システムは ' パリティ・ディスク上のインデックス情報と ' 残りの正常なディスク上のデータを比較して ' 消失したデータを再構築しますダウンタイムや多大なパフォーマンス・コストは発生しません

ローカル階層（アグリゲート）は、1つ以上の RAIDグループで構成されます。ローカル階層の RAIDタイプは、RAIDグループ内のパリティディスクの数、およびRAID構成で保護される同時ディスク障害の数を決定します。

デフォルトの RAID タイプである RAID-DP （ RAID ダブルパリティ）の場合、RAID グループごとに 2 本のパリティディスクが必要であり、同時に 2 本のディスクで障害が発生してもデータ損失から保護されます。RAID-DP の推奨される RAID グループサイズは、HDD の場合は 12~20 本、SSD の場合は 20~28 本です。

サイジング推奨事項の範囲内でより多くの本数の RAID グループを作成すると、パリティディスクのオーバーヘッドコストを分散させることができます。これは特に、容量ドライブよりもはるかに信頼性が高い SSD の場合に当てはまります。HDDを使用するローカル階層の場合は、ディスクストレージを最大化の必要性和、大規模なRAIDグループほど再構築に要する時間が長くなるといった相反する要件とのバランスを取る必要があります。

ミラーされた、ミラーされていないローカル階層（アグリゲート）

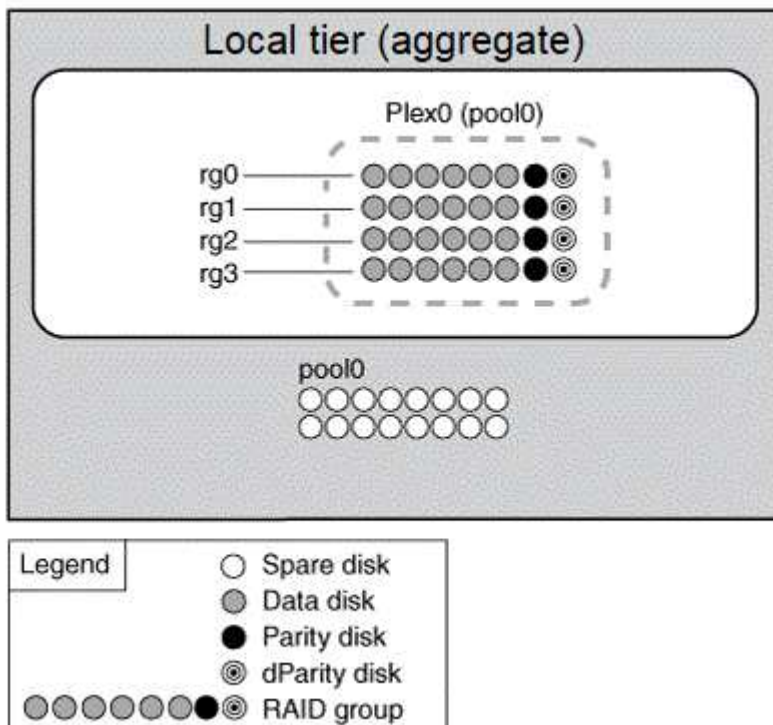
ONTAP には、SyncMirror というオプション機能があります。この機能を使用すると、コピー内のローカル階層（アグリゲート）データまたはプレックスを同期的にミラーリングし、別々のRAIDグループに格納することができます。プレックスを使用すると、RAID タイプで保護されるディスク数よりも多くのディスクで障害が発生した場合や、RAID グループのディスクへの接続が切断された場合に、データ損失を防ぐことができます。

System ManagerまたはCLIを使用してローカル階層を作成する場合は、ローカル階層をミラーリングするかミラーしないかを指定できます。

ミラーされていないローカル階層（アグリゲート）の機能

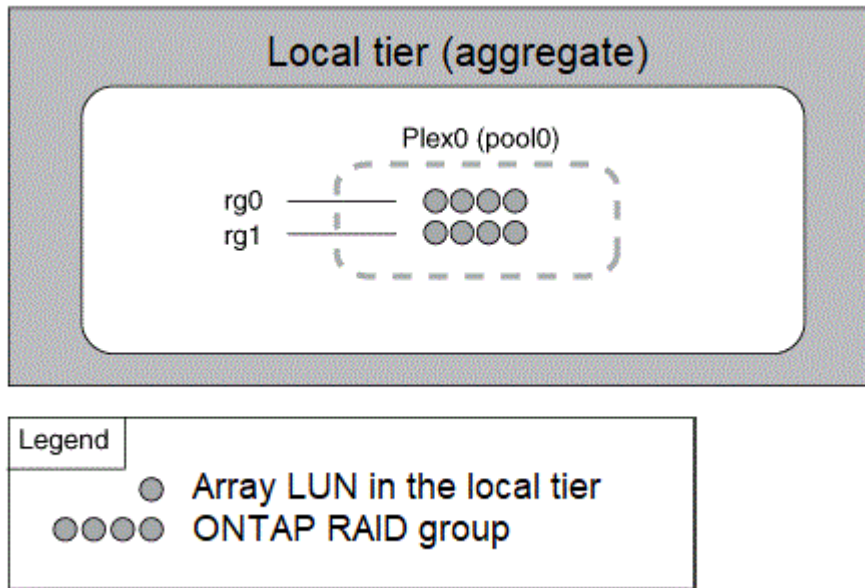
ローカル階層をミラーリングするように指定しない場合、ミラーされていないローカル階層（アグリゲート）として作成されます。ミラーされていないローカル階層には、プレックス\_（データのコピー）が1つだけ含まれ、このローカル階層に属するすべてのRAIDグループが含まれます。

次の図に、1つのプレックスを含む、ディスクで構成されたミラーされていないローカル階層を示します。ローカル階層には、rg0、rg1、rg2、rg3の4つのRAIDグループがあります。各RAIDグループには6本のデータディスクがあり、パリティディスクとdparity（ダブルパリティ）ディスクが1本ずつ含まれます。ローカル階層で使用されるすべてのディスクは同じプールであるpool0から提供されます



次の図に、1つのプレックスを含む、アレイLUNを含むミラーされていないローカル階層を示します。rg0 と

rg1 の 2 つの RAID グループがあります。ローカル階層で使用するすべてのアレイLUNは'同じプールであるpool0から提供されます



ミラーされたローカル階層（アグリゲート）の機能

ミラーされたアグリゲートには、2\_bプレックス\_（データコピー）があります。これらのアグリゲートでは、SyncMirror 機能を使用してデータを複製し、冗長性を確保します。

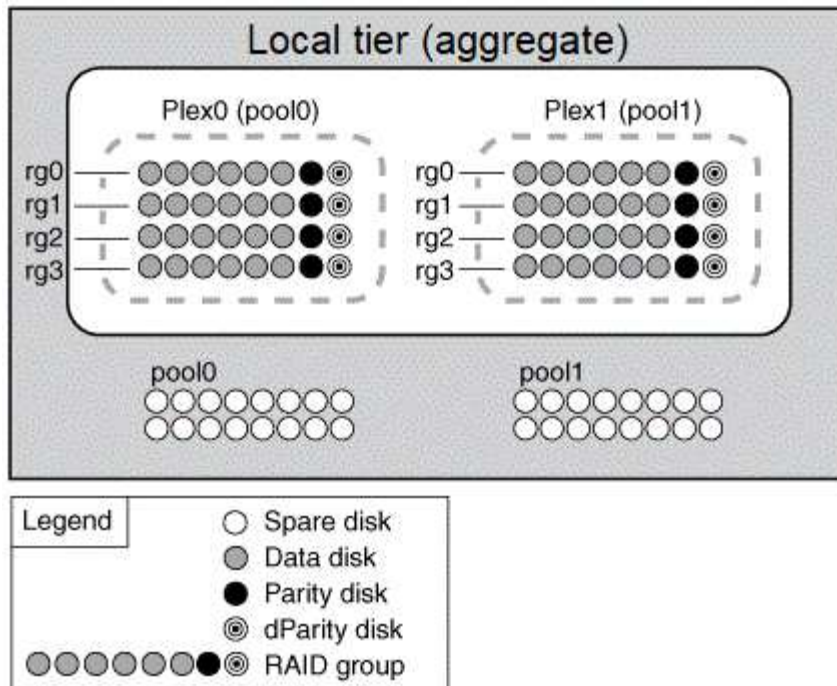
ローカル階層を作成するときに、ミラーされたローカル階層として指定することができます。また、ミラーされていない既存のローカル階層に2つ目のプレックスを追加して、ミラーされた階層にすることもできます。SyncMirror 機能を使用すると、ONTAP は元のプレックス（plex0）のデータを新しいプレックス（plex1）にコピーします。プレックスは物理的に分離されており（各プレックスには独自の RAID グループと独自のプールがあり）、同時に更新されます。

この構成では、アグリゲートのRAIDレベルで保護されるディスク数よりも多くのディスクで障害が発生した場合や接続が切断された場合に、影響を受けていないプレックスで障害の原因を修正する間もデータの提供が継続されるため、データ損失が防止されます。問題のあるプレックスが修正されたら、2つのプレックスが再同期化され、ミラー関係が再確立されます。

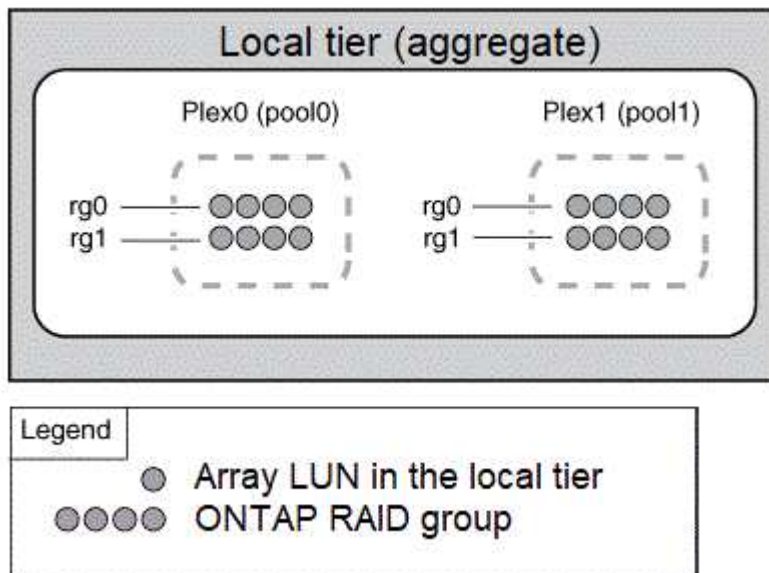
システム上のディスクとアレイLUNは'pool0とpool1という2つのプールに分かれていますplex0 は pool0 からストレージを取得し、plex1 は pool1 からストレージを取得します。

次の図は、SyncMirror 機能を有効にして実装したディスクで構成されるローカル階層を示しています。ローカル階層「plex1」用に2つ目のプレックスが作成されました。plex1 のデータは plex0 のデータの複製であり、RAID グループも同じです。32本のスペアディスクは、各プールに16本のディスクを使用してpool0またはpool1に割り当てられます。





次の図は、SyncMirror 機能を有効にして実装したアレイLUNで構成されるローカル階層を示しています。ローカル階層「plex1」用に2つ目のプレックスが作成されました。plex1 は plex0 の複製であり、RAID グループも同じです。



ストレージのパフォーマンスと可用性を最適化するために、ミラーアグリゲートでは少なくとも20%の空きスペースを確保することを推奨します。ミラーされていないアグリゲートでは10%が推奨されますが、追加の10%のスペースはファイルシステムで増分変更に対応するために使用できます。増分変更を行うと、ONTAPのcopy-on-write Snapshotベースのアーキテクチャにより、ミラーされたアグリゲートのスペース使用率が向上します。これらのベストプラクティスに従わないと、パフォーマンスに悪影響を及ぼす可能性があります。



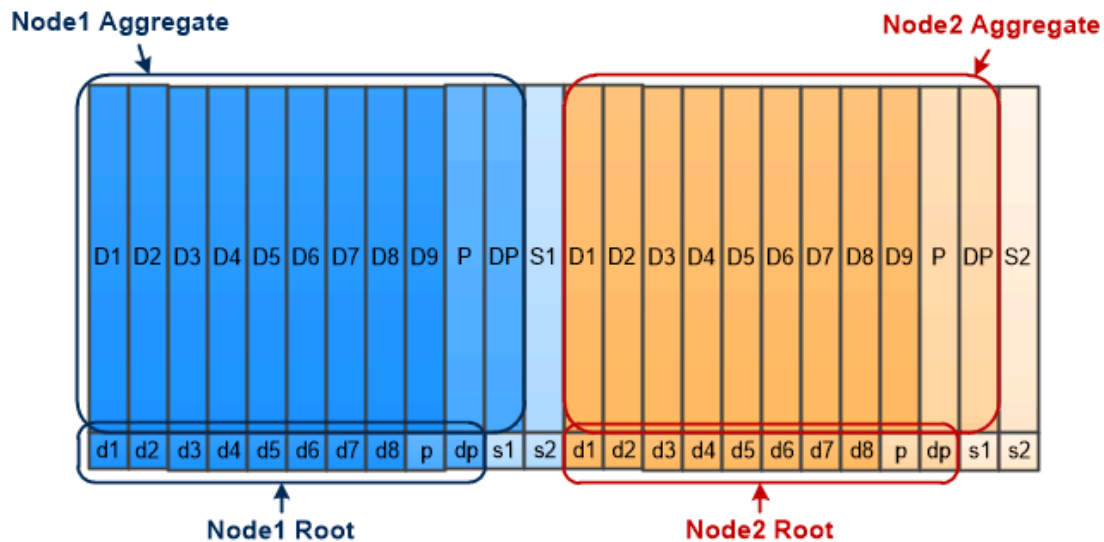
## ルート / データパーティショニング

すべてのノードには、ストレージシステムの構成ファイル用のルートアグリゲートが必要です。ルートアグリゲートの RAID タイプは、データアグリゲートの RAID タイプと同じです

System Manager では、ルート / データパーティショニングやルート / データ / データパーティショニングはサポートされません。

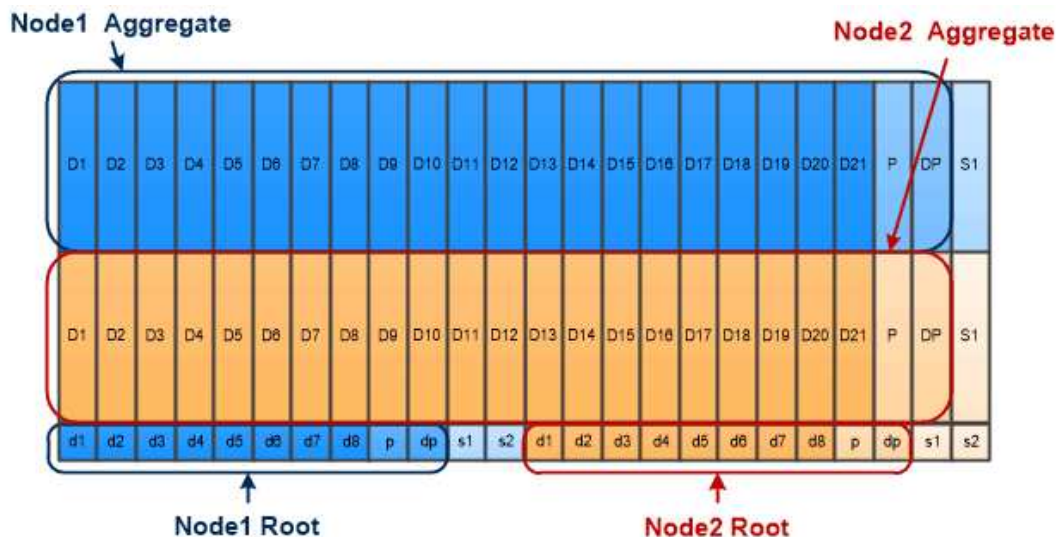
RAID-DP タイプのルートアグリゲートは、通常、1つのデータディスクと2つのパリティディスクで構成されます。これは、アグリゲート内の各 RAID グループ用に2つのディスクがパリティディスクとしてすでにリザーブされている場合、ストレージシステムファイルの料金を支払う「パリティ税」として相当します。

Root-data partitioning ルートアグリゲートを複数のディスクパーティションに分散し、各ディスク上にルートパーティションとして小さなパーティションを1つ、データ用に大きなパーティションを1つリザーブすることで、パリティの負担を軽減します。



*Root-data partitioning creates one small partition on each disk as the root partition and one large partition on each disk for data.*

図からわかるように、ルートアグリゲートの格納に使用するディスクの数が多いほど、ルートパーティションは小さくなります。これは、ルート / データパーティショニングの一種である root-data-data partitioning の場合でもあります。このパーティショニングでは、ルートパーティションとして小さなパーティションを1つ作成し、データ用に同じサイズの大きなパーティションを2つ作成します。



*Root-data-data partitioning creates one small partition as the root partition and two larger, equally sized partitions for data.*

どちらのタイプのルート / データパーティショニングも、ONTAP のアドバンスドドライブパーティショニング (ADP) 機能の一部です。どちらも出荷時点で構成され、エントリレベルの FAS2xxx、FAS9000、FAS8200、FAS80xx、および AFF システムについてはルート / データパーティショニング、AFF システムについてはのみルート / データ / データパーティショニングが使用されます。

の詳細を確認してください ["アドバンスドドライブパーティショニング"](#)。

ルートアグリゲート用にパーティショニングされたドライブ

ルートアグリゲートで使用するためにパーティショニングされるドライブは、システム構成によって異なります。

ルートアグリゲートに使用するドライブ数を把握しておく、ルートパーティション用にリザーブするドライブの容量とデータアグリゲートで使用可能な容量を決定する際に役立ちます。

ルートデータのパーティショニング機能は、エントリレベルのプラットフォーム、オールフラッシュ FAS プラットフォーム、および SSD のみが接続された FAS プラットフォームでサポートされます。

エントリレベルのプラットフォームでは、内蔵ドライブのみがパーティショニングされます。

SSD だけが接続されている All Flash FAS プラットフォームおよび FAS プラットフォームでは、システムの初期化時にコントローラに接続されるすべてのドライブがパーティショニングされます。ノードあたりの最大数は 24 です。システムの構成後に追加されたドライブはパーティショニングされません。

## ボリューム、**qtree**、ファイル、および **LUN**

ONTAP は、\_FlexVol ボリュームと呼ばれる論理コンテナからクライアントとホストにデータを提供します。\_ これらのボリュームは包含アグリゲートと緩やかに結合されているため、従来のボリュームよりも柔軟にデータを管理できます。

1 つのアグリゲートに複数の FlexVol を割り当てて、異なるアプリケーションやサービス専用にすることができます。FlexVol を拡張および縮小したり、FlexVol ボリュームを移動したり、FlexVol ボリュームの効率的なコピーを作成したりできます。qtree \_ を使用して FlexVol ボリュームをより管理しやすい単位にパーティ

ショニングしたり、クォータ\_を使用してボリュームのリソース使用量を制限したりできます。

NAS 環境ではボリュームにファイルシステムが格納され、SAN 環境では LUN が格納されます。LUN（論理ユニット番号）は、SAN プロトコルによって対処される a\_logical unit\_ というデバイスの識別子です。

LUN は、SAN 構成におけるストレージの基本単位です。Windows ホストは、ストレージシステム上の LUN を仮想ディスクとして認識します。LUN は、必要に応じて無停止で別のボリュームに移動できます。

データボリュームのほかに、いくつかの特別なボリュームについて理解しておく必要があります。

- a\_node root volume\_( 通常は「vol0」) には、ノードの構成情報とログが格納されます。
- SVM ルートボリュームは、SVM によって提供されるネームスペースへのエントリポイントとして機能し、ネームスペースディレクトリ情報が格納されます。
- System volume\_ には、サービス監査ログなどの特別なメタデータが格納されます。

これらのボリュームはデータの格納には使用できません。



*Volumes contain files in a NAS environment and LUNs in a SAN environment.*

\* \_ FlexGroup volumes \_ \*

企業によっては、FlexVol ボリュームの 100TB の容量をもはるかに超えるペタバイト規模のストレージが単一のネームスペースで必要になることがあります。

FlexGroup volume\_ は、200 個のコンスティチュエントメンバーボリュームを含む最大 4、000 億個のファイルをサポートします。このメンバーボリュームはコラボレーションにより、負荷を動的に分散し、すべてのメンバーに均等にスペースを割り当てます。

FlexGroup ボリュームではメンテナンスや管理の手間も必要ありません。単に FlexGroup ボリュームを作成して NAS クライアントと共有するだけです。ONTAP が残りの処理を実行します。

## ストレージ仮想化

### ストレージ仮想化の概要

クライアントやホストにデータを提供するには、`_Storage Virtual Machine (SVM)` を使用します。SVM は、ハイパーバイザーで実行される仮想マシンと同様に、物理リソースを抽象化した論理エンティティです。SVM 経由でアクセスされるデータはストレージ内の場所にバインドされません。SVM へのネットワークアクセスは物理ポートにバインドされません。



SVMは、以前は「Vserver」と呼ばれていました。ONTAP のコマンドラインインターフェイスでは、引き続き「vserver」という用語が使用されます。

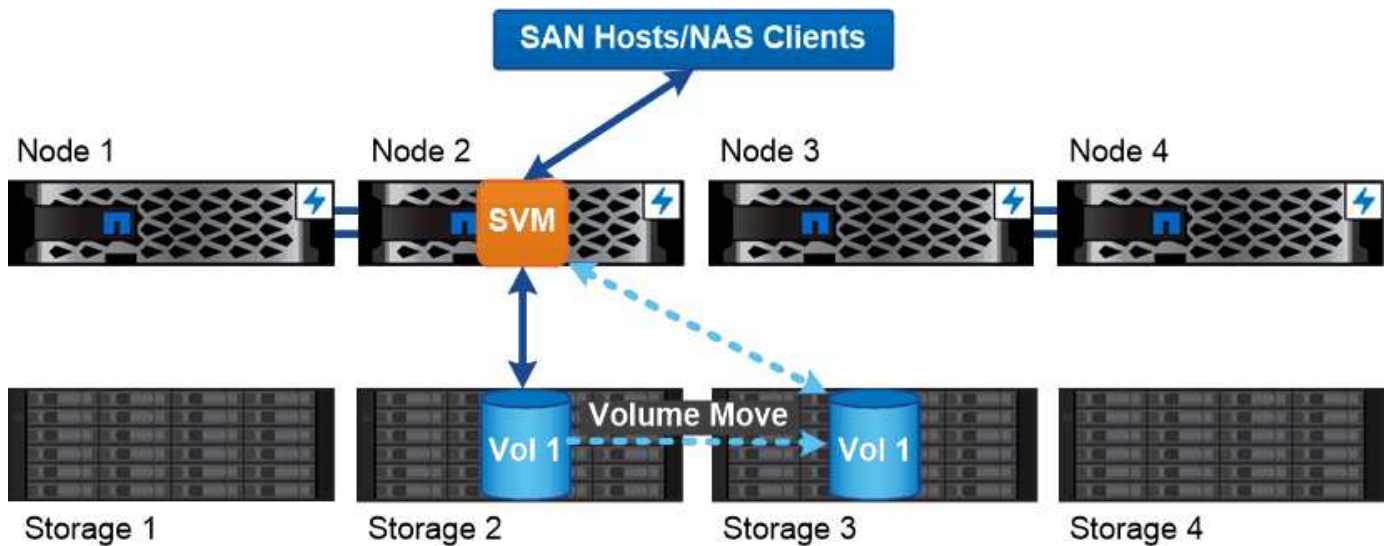
SVM は、1 つ以上のボリュームから 1 つ以上の `network_logical interfaces` (LIF ; ネットワーク論理インターフェイス) を通じてクライアントおよびホストにデータを提供します。ボリュームは、クラスタ内の任意のデータアグリゲートに割り当てることができます。LIF は任意の物理ポートまたは論理ポートでホストできます。ハードウェアのアップグレード、ノードの追加、パフォーマンスの分散、アグリゲート間での容量の最適化などを行う際、ボリュームと LIF のどちらもデータサービスを中断することなく移動できます。

同じ SVM に NAS トラフィック用の LIF と SAN トラフィック用の LIF を設定することができます。クライアントとホストから SVM にアクセスするために必要なのは、LIF のアドレス (NFS、SMB、iSCSI の場合は IP アドレス、FC の場合は WWPN) だけです。LIF のアドレスは移動しても変わりません。ポートは複数の LIF をホストできます。SVM には、それぞれ独自のセキュリティ、管理、およびネームスペースがあります。

ONTAP では、データ SVM に加え、管理用の特別な SVM を使用します。

- クラスタのセットアップ時に `admin SVM` が作成されます。
- ノードが新規または既存のクラスタに追加されると、`_node svm_is` が作成されます。
- IPspace 内のクラスタレベルの通信用に、`_system svm_is` を自動的に作成します。

これらの SVM はデータの提供には使用できません。また、クラスタ内およびクラスタ間のトラフィック用の LIF や、クラスタおよびノードの管理用の LIF もあります。



*Data accessed through an SVM is not bound to a physical storage location. You can move a volume without disrupting data service.*

#### ONTAPがミドルウェアに似ている理由

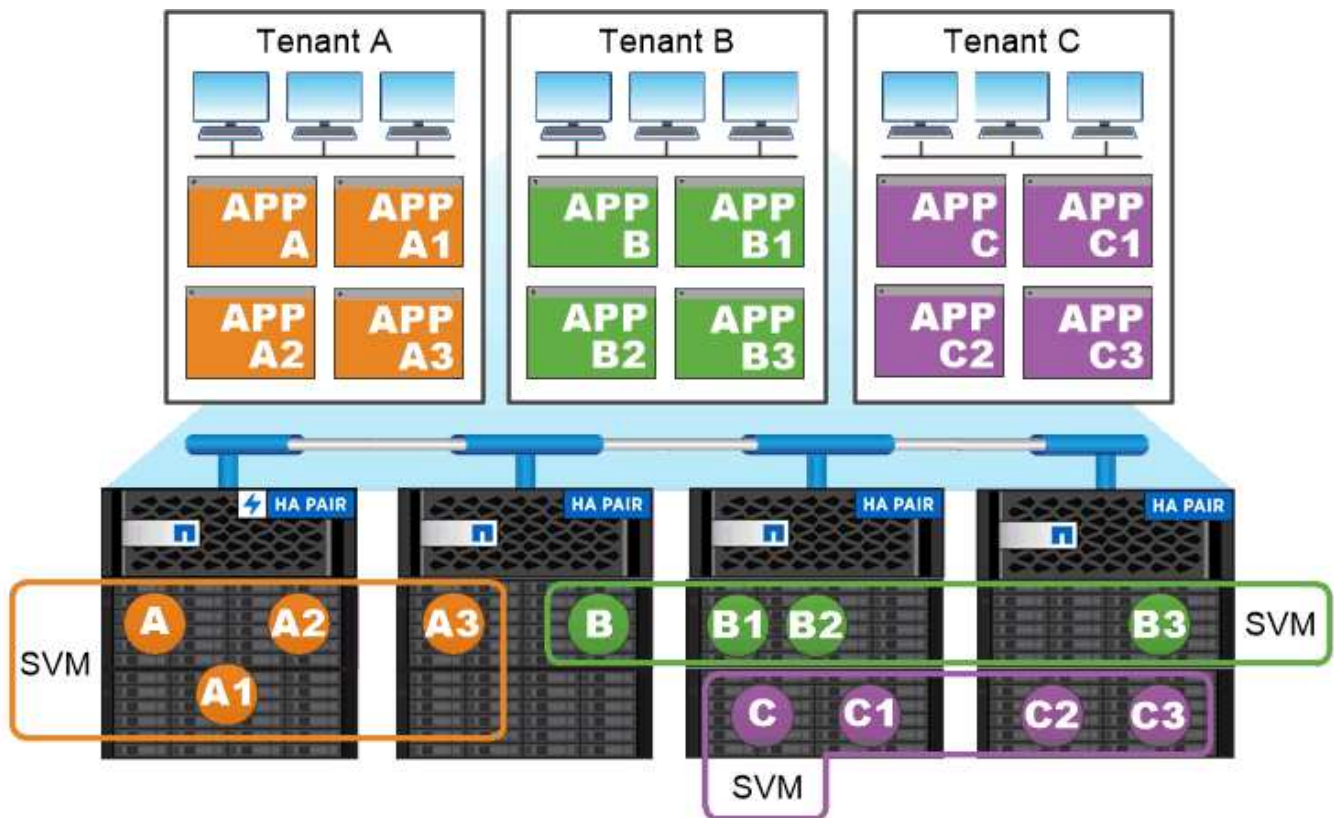
ONTAP がストレージ管理タスクに使用する論理オブジェクトは、適切に設計されたミドルウェアパッケージが従来担っていた役割を果たし、管理者を細かな実装作業から解放し、ノードやポートなどの物理仕様の変更が設定に影響しないようにします。管理者がストレージインフラ全体ではなく一部を再設定するだけで、ポリシーや LIF を簡単に移動できるようにすることが、基本的な目的です。

#### SVM のユースケース

サービスプロバイダはセキュアなマルチテナンシー環境で SVM を使用し、各テナントのデータを分離し、テナントごとに専用の認証と管理を実装して、チャージバックを簡易化します。複数の LIF を同じ SVM に割り当てて異なる顧客のニーズに対応したり、QoS を使用してテナントのワークロードが他のテナントのワークロード「Bully」にならないようにしたりすることができます。

企業の管理者も同じような目的に SVM を使用します。たとえば、データを部門別に分離したり、ホストがアクセスするストレージボリュームとユーザの共有ボリュームを別々の SVM に分けたりできます。iSCSI/FC LUN および NFS データストアと SMB 共有とで SVM を分ける管理者もいます。





*Service providers use SVMs in multitenant environments to isolate tenant data and simplify chargeback.*

#### クラスタと SVM の管理

クラスタ管理者は、クラスタの管理 SVM にアクセスします。管理SVMとクラスタ管理者（予約された名前） `admin` は、クラスタのセットアップ時に自動的に作成されます。

デフォルトを持つクラスタ管理者 `admin` ロールは、クラスタ全体とそのリソースを管理できます。クラスタ管理者は、必要に応じて別のロールを割り当てた別のクラスタ管理者を作成することができます。

SVM administrator は、データ SVM にアクセスします。クラスタ管理者は、必要に応じてデータ SVM と SVM 管理者を作成します。

SVM管理者には、が割り当てられます `vsadmin` デフォルトではロール。クラスタ管理者は、必要に応じて SVM 管理者に別のロールを割り当てることができます。

#### \* \_ ロールベースアクセス制御 (RBAC) \_ \*

管理者がアクセスできるコマンドは、管理者に割り当てられている `_role_assigned` コマンドで決まります。ロールは管理者のアカウントを作成するときに割り当てます。必要に応じて、別のロールを割り当てたりカスタムロールを定義したりできます。

## ネームスペースとジャンクションポイント

`nas_namespace_` は、`_junction points_to` によって結合されたボリュームを論理的にグループ化して、単一のファイルシステム階層を作成します。十分な権限を持つクライアントは、ストレージ内のファイルの場所を指定せずにネームスペース内のファイルにアクセスできます。ジャンクションされたボリュームはクラスタ内の任意の場所に配置できます。

NAS クライアントは、目的のファイルを含むすべてのボリュームをマウントするのではなく、`nfs_export_` をマウントするか、`SMB_share` にアクセスします。`_` エクスポートまたは共有は、ネームスペース全体またはネームスペース内の中間的な場所を表します。クライアントは、アクセスポイントより下にマウントされたボリュームにのみアクセスします。

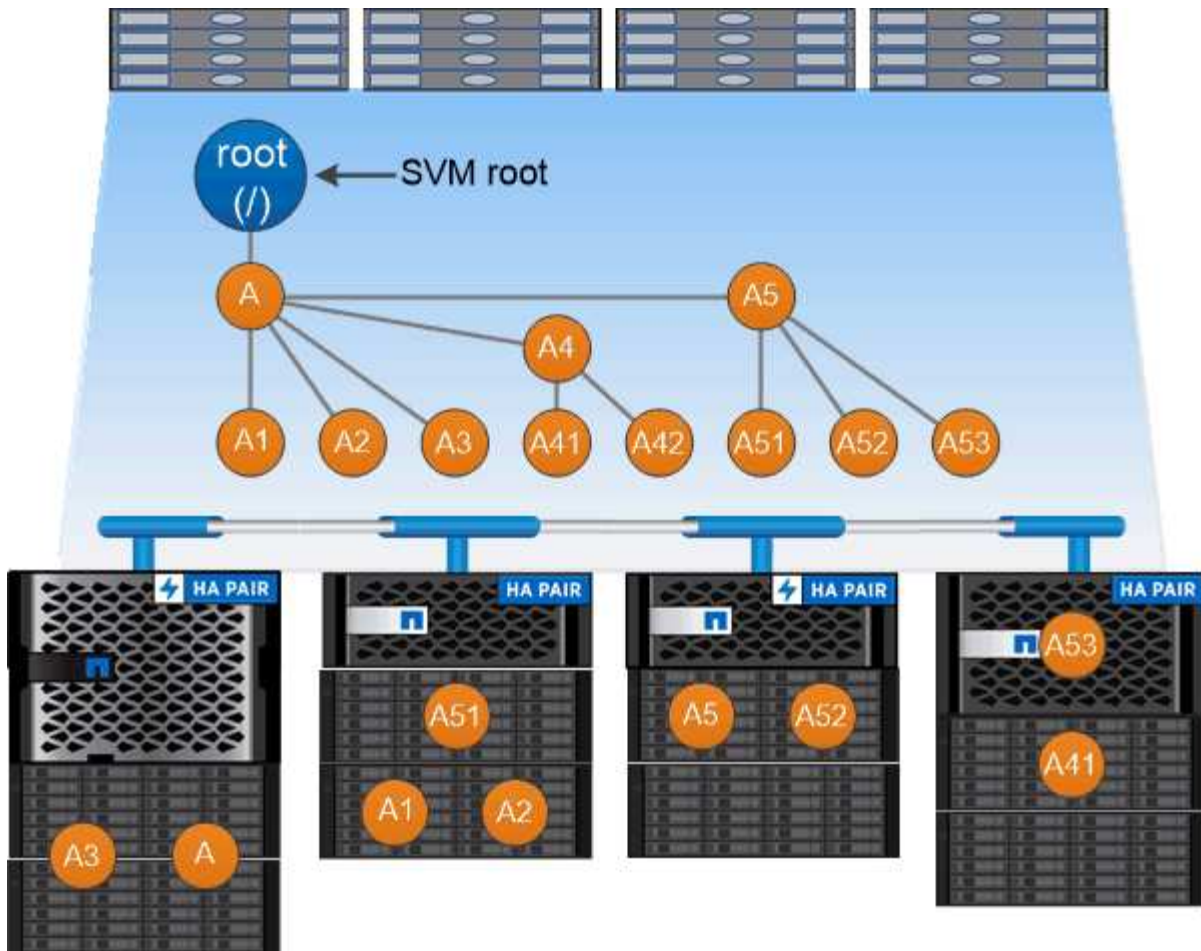
ネームスペースには必要に応じてボリュームを追加できます。ジャンクションポイントは、親ボリュームジャンクションのすぐ下に作成することも、ボリューム内のディレクトリに作成することもできます。「vol3」という名前のボリュームのボリュームジャンクションへのパスは、になることがあります `/vol1/vol2/vol3`` または ``/vol1/dir2/vol3`` あるいは ``/dir1/dir2/vol3`。このパスのことを `_junction` パスと呼びます。 `_`

SVM には、それぞれ一意のネームスペースがあります。SVM ルートボリュームは、ネームスペース階層へのエントリポイントです。



ノードに障害やフェイルオーバーが発生したときにデータを引き続き利用できるようにするには、SVM ルートボリュームに `_load-sharing mirror_copy` を作成する必要があります。





*A namespace is a logical grouping of volumes joined together at junction points to create a single file system hierarchy.*

例

次の例は、ジャンクションパスがである「home4」という名前のボリュームをSVM vs1上に作成します  
/eng/home :

```
cluster1::> volume create -vserver vs1 -volume home4 -aggregate aggr1
-size 1g -junction-path /eng/home
[Job 1642] Job succeeded: Successful
```

## パスのフェイルオーバー

### パスのフェイルオーバーの概要

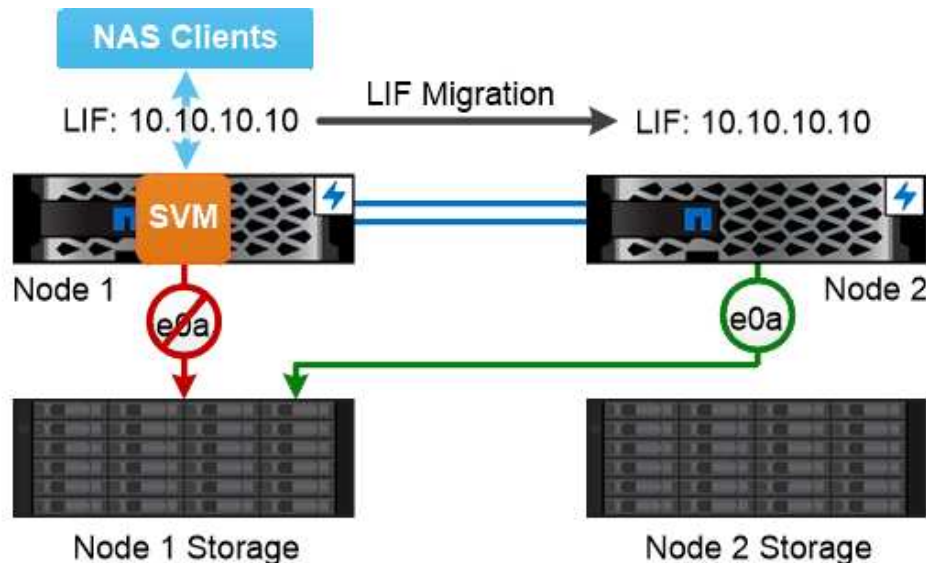
ONTAP でのパスのフェイルオーバーは、NAS トポロジと SAN トポロジで大きく異なります。NAS LIF は、リンク障害が発生すると別のネットワークポートに自動的に移行します。SAN LIF は、障害の発生後に手動で移動しないかぎり移行しません。代わりに、ホストのマルチパステクノロジーによって、同じ SVM 上の、別のネットワークポートにアクセスしている別の LIF にトラフィックが転送されます。

## NAS パスのフェイルオーバー

NAS LIF は、現在のポートでリンク障害が発生すると、稼働しているネットワークポートに自動的に移行します。この移行先のポートは、LIF の *failover group* のメンバーである必要があります。\_failover group policy\_n を使用すると、データ LIF のフェイルオーバーターゲットが、データとその HA パートナーを所有するノード上のポートに移動します。

管理を容易にするため、ONTAP ではネットワークアーキテクチャ内の各 \_ブロードキャストドメイン\_ 用のフェイルオーバーグループが作成されます。ブロードキャストドメインは、同じレイヤ 2 ネットワークに属するポートをグループ化したものです。VLAN を使用している場合、たとえば部門（エンジニアリング、マーケティング、財務など）ごとにトラフィックを分離するには、各 VLAN で別々のブロードキャストドメインを定義します。ブロードキャストドメインに関連付けられたフェイルオーバーグループは、ブロードキャストドメインのポートを追加または削除するたびに自動的に更新されます。

ほとんどの場合、フェイルオーバーグループを最新の状態に保つために、ブロードキャストドメインを使用してフェイルオーバーグループを定義することを推奨します。ただし、ブロードキャストドメインに関連付けられていないフェイルオーバーグループを定義することもできます。たとえば、ブロードキャストドメインに定義されたポートの一部にのみ LIF をフェイルオーバーするように設定できます。



*A NAS LIF automatically migrates to a surviving network port after a link failure on its current port.*

### • \_サブネット\_ \*

a\_subnet\_ は、ブロードキャストドメイン内の IP アドレスのブロックを予約します。これらのアドレスは同じレイヤ 3 ネットワークに属し、LIF の作成時にブロードキャストドメイン内のポートに割り当てられます。LIF アドレスを定義する場合、IP アドレスとネットワークマスクを指定するよりもサブネット名を指定した方が一般に簡単で間違いも少なくなります。

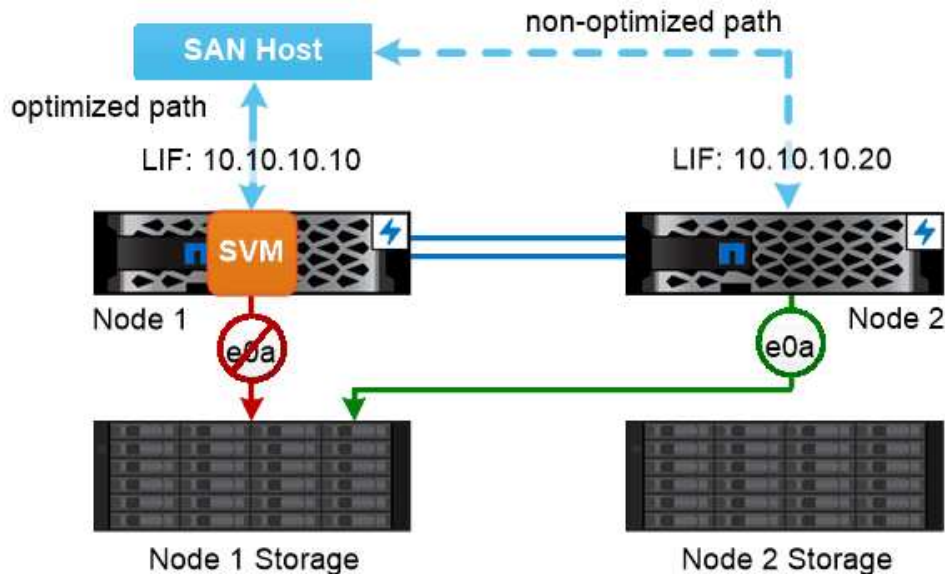
## SANパスのフェイルオーバー

リンク障害が発生すると、SAN ホストは ALUA（非対称論理ユニットアクセス）と MPIO（マルチパス I/O）を使用してトラフィックを稼働している LIF に再ルーティングします。SVM が提供する LUN への使用可能なルートは、事前に定義されたパスで決まります。

SAN 環境では、ホストは lun\_targets への要求の `_イニシエータ_` とみなされます。\_MPIO を使用すると、イニシエータからターゲットへの複数のパスを使用できます。ALUA は、「`_optimized paths_`」と呼ばれる最も直接パスを特定します。\_

通常は、LUN の所有者ノード上の LIF への最適パスと、HA パートナー上の LIF への最適化されていないパスを、それぞれ複数構成します。所有者ノードの 1 つのポートで障害が発生すると、稼働しているポートにトラフィックがルーティングされます。すべてのポートで障害が発生した場合は、最適化されていないパスを介してトラフィックがルーティングされます。

ONTAP の選択的 LUN マップ（SLM）は、ホストから LUN へのパスの数をデフォルトで制限します。新しく作成した LUN には、LUN を所有するノードまたは HA パートナーへのパス経由でのみアクセスできます。また、イニシエータに対して `port set` で LIF を設定して、LUN へのアクセスを制限することもできます。



*A SAN host uses multipathing technology to reroute traffic to a surviving LIF after a link failure.*

### \* \_ SAN 環境でのボリュームの移動 \_ \*

デフォルトでは、ONTAP の選択的 LUN マップ（SLM）\_ は、SAN ホストから LUN へのパスの数を制限します。新しく作成した LUN には、LUN を所有するノードまたは HA パートナーである LUN の `_reporting nodes_` へのパス経由でのみアクセスできます。

そのため、ボリュームを別の HA ペアのノードに移動した場合、移動先の HA ペアのレポートノードを LUN マッピングに追加する必要があります。その後、MPIO に新しいパスを指定します。ボリュームの移動が完了したら、ソース HA ペアのレポートノードをマッピングから削除できます。

## 負荷分散

ノードでの作業量が使用可能なリソースを超えると、ワークロードのパフォーマンスにレイテンシが発生し始めます。ノードの負荷が許容量を超えた場合は、利用可能なリソースを増やす（ディスクや CPU をアップグレードする）か、負荷を減らす（ボリュームや LUN を必要に応じて別のノードに移動する）ことで対処できます。

また、ONTAP ストレージのサービス品質（QoS）`_` を使用して、重要なワークロードのパフォーマンスが競合するワークロードの影響を受けて低下しないようにすることもできます。

- 競合するワークロードに対して QoS スループットの上限を設定すると、そのワークロードによるシステムリソースへの影響を制限できます（最大 QoS）。
- 重要なワークロードに対して QoS スループットの下限を設定すると、競合するワークロードによる要求に関係なく、必要な最小スループットを確保できます（最小 QoS）。
- 同じワークロードに対して QoS の上限と下限を設定することができます。

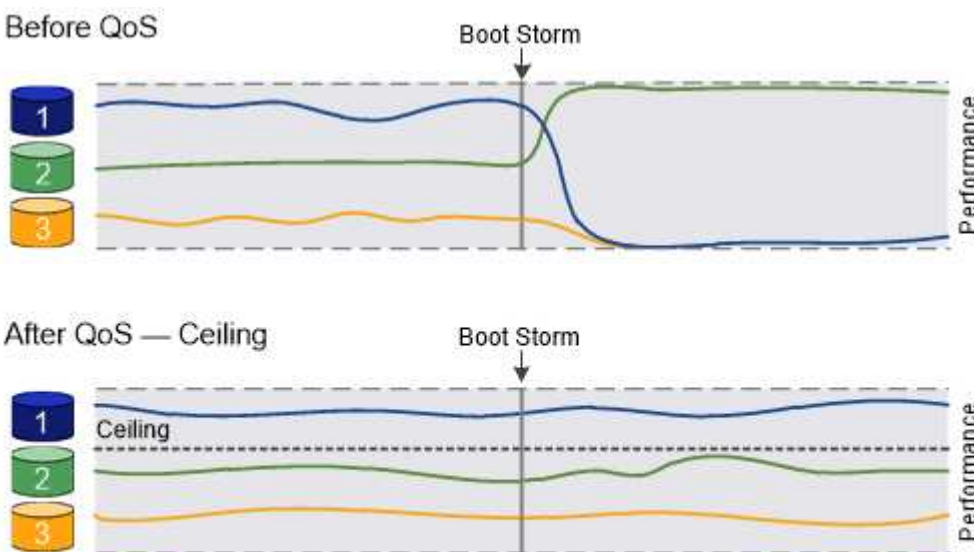
### スループットの上限

スループットの上限は、ワークロードのスループットを最大 IOPS または MB/ 秒に制限します次の図では、ワークロード 2 のスループットの上限により、ワークロード 1 および 3 の「負荷」が発生しないようにしています。

`a_policy group_` は、1 つ以上のワークロードに対するスループットの上限を定義します。ワークロードとは、`a_storage` オブジェクト：`_a` ボリューム、ファイル、LUN、または SVM 内のすべてのボリューム、ファイル、LUN の I/O 処理のことです。上限はポリシーグループの作成時に指定できるほか、ワークロードをしばらく監視したあとで指定することもできます。



ワークロードのスループットは、特にスループットが急激に変化した場合、指定された上限を 10% までは超過することができます。バースト時には、上限を 50% まで超過することができます。



*The throughput ceiling for workload 2 ensures that it does not “bully” workloads 1 and 3.*



## スループットの下限

スループットの下限はワークロードのスループットが最小 IOPS を下回らないことを保証します。次の図では、ワークロード 1 とワークロード 3 のスループットの下限により、ワークロード 2 からの要求に関係なく、最小スループットが確保されています。

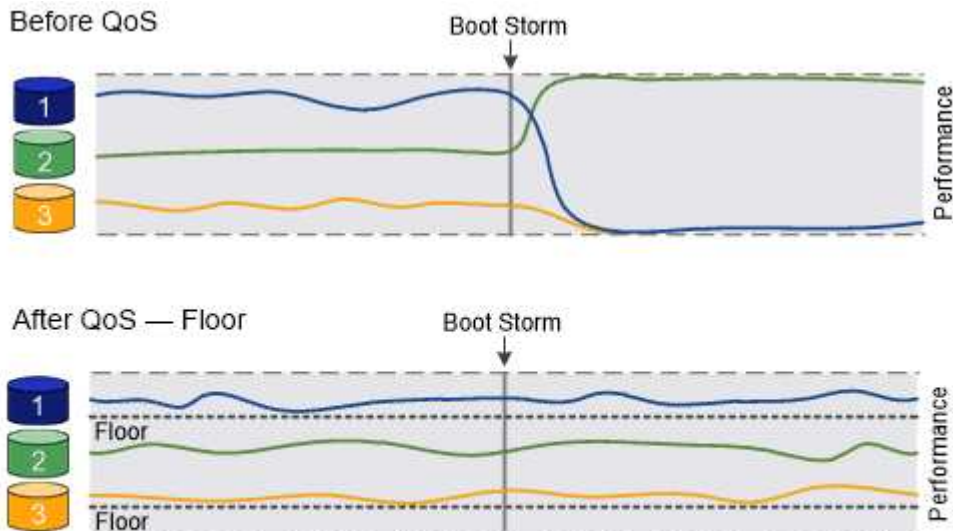


これらの例からわかるように、スループットの上限はスループットを直接調整するのに対し、スループットの下限は下限が設定されたワークロードを優先することでスループットを間接的に調整します。

ワークロードとは、ボリューム、LUN、または ONTAP 9.3 以降のファイルの I/O 処理のことです。スループットの下限を定義するポリシーグループは、SVM には適用できません。下限はポリシーグループの作成時に指定できるほか、ワークロードをしばらく監視したあとで指定することもできます。



ノードやアグリゲートに十分なパフォーマンス容量（ヘッドルーム）がない場合やなどの重要な処理の実行中は、ワークロードのスループットが指定された下限を下回ることがあります volume move trigger-cutover。利用可能な容量が十分にあるときや重要な処理を実行していないときでも、ワークロードのスループットは指定された下限を 5% まで下回ることができます。



*The throughput floors for workload 1 and workload 3 ensure that they meet minimum throughput targets, regardless of demand by workload 2.*

## アダプティブ QoS

通常、ストレージオブジェクトに割り当てたポリシーグループの値は固定値です。ストレージオブジェクトのサイズが変わったときは、値を手動で変更する必要があります。たとえば、ボリュームの使用スペースが増えた場合、通常は指定されているスループットの上限も増やす必要があります。

アダプティブ QoS \_ ワークロードのサイズの変更に合わせてポリシーグループの値が自動的に調整され、TB または GB あたりの IOPS が一定に維持されます。これは、何百何千という数のワークロードを管理する大規模な環境では大きなメリットです。

アダプティブ QoS は、主にスループットの上限の調整に使用しますが、下限の管理（ワークロードサイズが増えた場合）に使用することもできます。ワークロードのサイズは、ストレージオブジェクトに割り当てられ

たスペースまたはストレージオブジェクトで使用されているスペースのいずれかで表されます。



ONTAP 9.5 以降では、使用済みスペースをスループットの下限に使用できます。ONTAP 9.4 以前では使用できません。

[+]

ONTAP 9.13.1以降では、アダプティブQoSを使用してSVMレベルでスループットの下限と上限を設定できます。

- 割り当て済みスペースのポリシーでは、ストレージオブジェクトの公称サイズを基準に IOPS と TB / GB の比率が維持されます。比率が 100 IOPS/GB の場合、150GB のボリュームのスループットの上限はボリュームのサイズが変更されないかぎり 15、000 IOPS です。ボリュームのサイズが 300GB に変更されると、アダプティブ QoS によってスループットの上限が 30、000 IOPS に調整されます。
- a\_used space-policy（デフォルト）は、ストレージ効率化前に格納されている実際のデータの量に基づいて、IOPS/TB|GB の比率を維持します。比率が 100 IOPS/GB の場合、100GB のデータが格納された 150GB のボリュームのスループットの上限は 10、000 IOPS です。使用済みスペースの量が変わると、アダプティブ QoS によって比率が一定になるようにスループットの上限が調整されます。

## レプリケーション

### Snapshot コピー

従来、ONTAP のレプリケーションテクノロジーは、ディザスタリカバリ（DR）とデータアーカイブのニーズに対応してきました。その後、クラウドサービスが登場し、ネットアップデータファブリック内のエンドポイント間のデータ転送に ONTAP レプリケーションが採用されるようになりました。これらすべての用途において、ONTAP の Snapshot テクノロジーが基盤となります。

Snapshot コピー<sub>1</sub> は、ボリュームの読み取り専用のポイントインタイムイメージです。Snapshot コピーが作成されると、アクティブファイルシステムと Snapshot コピーは同じディスクブロックを参照するため、追加のディスクスペースは使用されません。イメージには Snapshot コピーが最後に作成されてからのファイルへの変更のみが記録されるため、時間の経過とともに消費されるストレージスペースは最小限で済み、パフォーマンスのオーバーヘッドもわずかです。

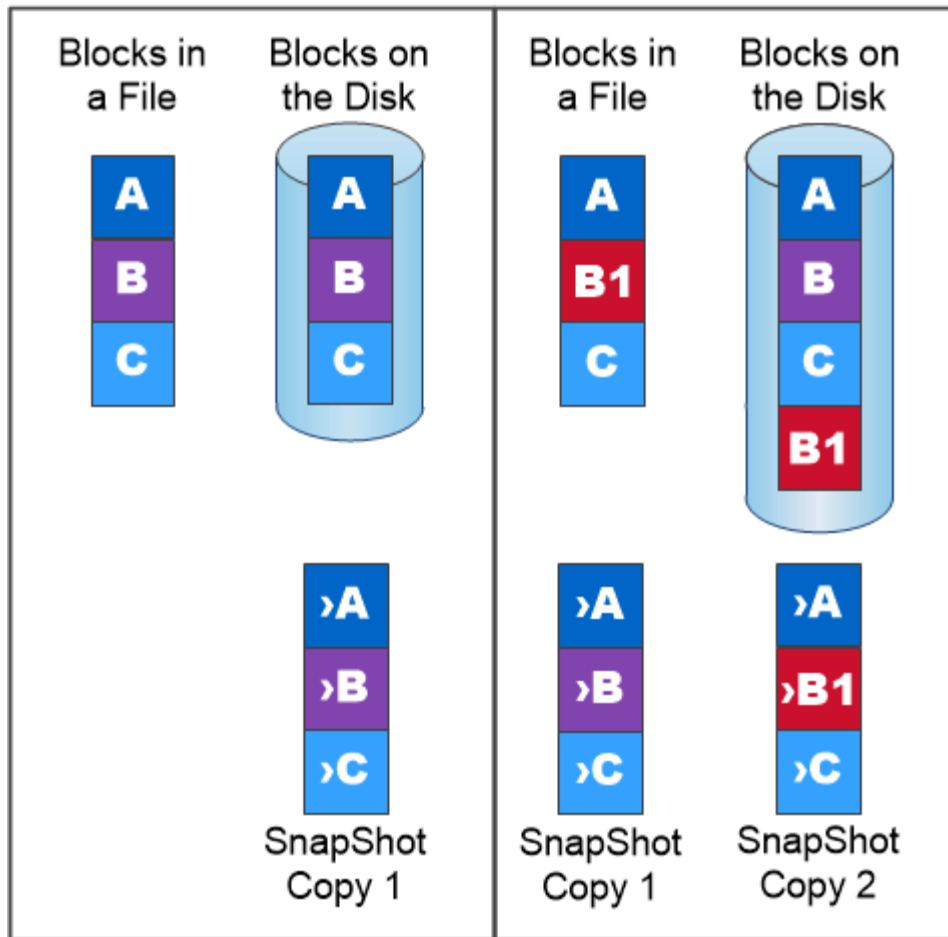
Snapshot コピーの効率性は、ONTAP の中核的なストレージ仮想化テクノロジーである ITS Write Anywhere File Layout（WAFL）によって実現します。<sub>2</sub> WAFL は、データベースと同様に、メタデータを使用してディスク上の実際のデータブロックを参照します。ただし、データベースとは異なり、WAFL は既存のブロックを上書きしません。更新されたデータは新しいブロックに書き込まれ、メタデータが変更されます。

Snapshot コピーの効率性は、コピーデータブロックではなく、ONTAP が Snapshot コピーの作成時にメタデータを参照するためです。これにより、他のシステムがコピーするブロックを特定する際に発生する「シーク時間」と、コピー自体を作成するコストの両方が削減されます。

Snapshot コピーを使用して、個々のファイルまたは LUN をリカバリしたり、ボリュームの内容全体をリストアしたりできます。ONTAP は、Snapshot コピーのポインタ情報をディスク上のデータと比較することで、ダウンタイムや多大なパフォーマンスコストなしで損失オブジェクトや破損オブジェクトを再構築します。

Snapshot ポリシー<sub>3</sub> は、ボリュームの Snapshot コピーの作成方法を定義します。このポリシーは、Snapshot コピーを作成するタイミング、保持するコピーの数、Snapshot コピーの命名方法、および Snapshot コピーにレプリケーション用のラベルを付ける方法を指定します。たとえば、毎日午前 12 時 10 分に Snapshot コピーを 1 つ作成し、最新のコピーを 2 つ保持して、「毎日」（タイムスタンプ付き）という名

前を付け、レプリケーション用に「毎日」というラベルを付けることができます。



*A Snapshot copy records only changes to the active file system since the last Snapshot copy.*

#### SnapMirror によるディザスタリカバリとデータ転送

SnapMirror は、地理的に離れたサイトのプライマリストレージからセカンダリストレージへのフェイルオーバー用に設計されたディザスタリカバリテクノロジーです。名前が示すように、SnapMirror はセカンダリストレージに作業データのレプリカ（\_mirror）を作成します。このデータから、プライマリサイトで災害が発生した場合にもデータの提供を継続できます。

データのミラーリングはボリュームレベルで行われます。プライマリストレージのソースボリュームとセカンダリストレージのデスティネーションボリュームの関係は、\_data 保護関係と呼ばれます。\_ ボリュームが存在するクラスタと、ボリュームからデータを提供する SVM は \_peered になります。\_a ピア関係を設定することで、クラスタと SVM の交換が可能になります データをセキュアに保護



また、SVM 間にデータ保護関係を作成することもできます。このタイプの関係では、SVM のすべてまたは一部の設定が NFS エクスポートおよび SMB 共有から RBAC にレプリケートされます。また、SVM が所有するボリューム内のデータもレプリケートされます。



ONTAP 9.10.1 以降では、S3 SnapMirror を使用して S3 バケット間にデータ保護関係を作成できます。デスティネーションバケットは、ローカルまたはリモートの ONTAP システム、あるいは StorageGRID や AWS などの ONTAP 以外のシステムで使用できます。

SnapMirror を初めて起動すると、ソース・ボリュームからデスティネーション・ボリュームへの \_ ベースライン転送 \_ が実行されます。ベースライン転送の一般的な手順は次のとおりです。

- ソースボリュームの Snapshot コピーを作成します。
- Snapshot コピーおよびコピーが参照するすべてのデータブロックをデスティネーションボリュームに転送します。
- 「アクティブ」ミラーが破損した場合に備えて、ソースボリューム上の最新ではない残りの Snapshot コピーをデスティネーションボリュームに転送します。

ベースライン転送が完了すると、SnapMirror は新しい Snapshot コピーだけをミラーに転送します。更新は、設定したスケジュールに従って非同期に行われます。保持処理によって、ソース上の Snapshot ポリシーがミラーリングされます。プライマリサイトで災害が発生した場合は最小限のシステム停止でデスティネーションボリュームをアクティブ化し、サービスが復旧したらソースボリュームを再アクティブ化できます。

ベースライン作成後は Snapshot コピーだけが転送されるため、無停止で高速なレプリケーションが可能です。フェイルオーバーの事例で示すように、ミラーリングされたストレージからデータを効率的に提供するには、セカンダリシステム上のコントローラがプライマリシステム上のコントローラと同じであるか、ほぼ同じである必要があります。



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

- \_ SnapMirror を使用したデータ転送 \_ \*

SnapMirror を使用して、ネットアップデータファブリック内のエンドポイント間でデータをレプリケートすることもできます。SnapMirror ポリシーを作成するときに、レプリケーションを 1 回だけ行うか繰り返すかを選択できます。

**SnapMirror Cloud** は、データ保護ワークフローをクラウドに移行する ONTAP ユーザ向けに設計されたバックアップおよびリカバリのテクノロジーです。従来のバックアップからテープへのアーキテクチャから脱却するには、オブジェクトストレージを長期的なデータ保持とアーカイブの代替リポジトリとして使用できます。**SnapMirror Cloud** は、持続的な増分バックアップ戦略の一環として、ONTAP とオブジェクト間のストレージレプリケーションを提供します。

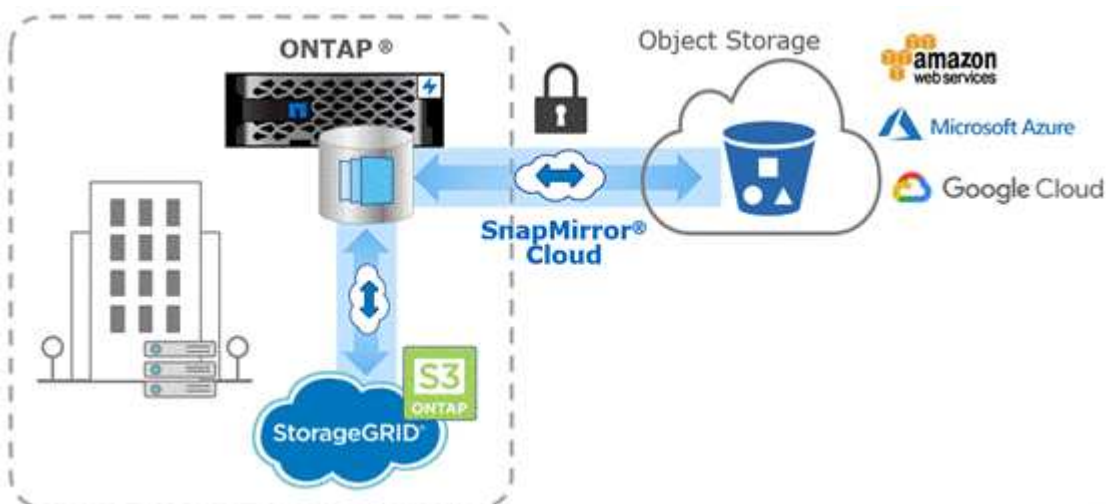
SnapMirror クラウドは、ONTAP 9.8 で SnapMirror レプリケーションテクノロジーファミリーの拡張機能として導入されました。SnapMirror は ONTAP から ONTAP へのバックアップによく使用されますが、SnapMirror Cloud は同じレプリケーションエンジンを使用して、ONTAP の Snapshot コピーを S3 準拠のオブジェクトストレージバックアップに転送します。

バックアップのユースケースをターゲットとした SnapMirror Cloud は、長期保持とアーカイブの両方のワークフローをサポートします。SnapMirror と同様に、最初の SnapMirror Cloud Backup はボリュームのベースライン転送を実行します。以降のバックアップでは、SnapMirror Cloud によってソースボリュームの Snapshot コピーが生成され、変更されたデータブロックのみを含む Snapshot コピーがオブジェクトストレージターゲットに転送されます。

SnapMirror Cloud 関係は、ONTAP システムと、オンプレミスとパブリッククラウドのオブジェクトストレージターゲット（Amazon S3、Google Cloud Storage、Microsoft Azure Blob Storage など）の間で設定できます。その他のオンプレミスオブジェクトストレージターゲットには、StorageGRID や ONTAP S3 などがあります。

SnapMirror クラウドレプリケーションは、ONTAP のライセンス機能であり、データ保護ワークフローをオーケストレーションするための承認されたアプリケーションが必要です。SnapMirror Cloud バックアップの管理には、次のオーケストレーションオプションを使用できます。

- SnapMirror クラウドレプリケーションのサポートを提供するサードパーティのバックアップパートナーが複数存在する。参加ベンダーは、で入手できます ["ネットアップのブログ"](#)。
- ネットアップネイティブの ONTAP 環境向け解決策向け BlueXP バックアップ/リカバリ
- データ保護ワークフロー用のカスタムソフトウェアを開発するための API、または自動化ツールを活用するための API



## SnapVault アーカイブ

SnapMirror ライセンスは、バックアップの SnapVault 関係とディザスタリカバリの SnapMirror 関係の両方をサポートするために使用されます。ONTAP 9.3以降では SnapVault ライセンスが廃止され、SnapMirror ライセンスを使用してバックアップ関係、ミラー関係、およびミラーとバックアップ関係を設定できます。SnapMirror レプリケーションは、Snapshot コピーを ONTAP から ONTAP にレプリケートするために使用されます。これにより、バックアップとディザスタリカバリの両方のユースケースがサポートされます。

\_ SnapVault \_ は、基準への準拠およびその他のガバナンス関連の目的で、ディスクツーディスクの Snapshot コピーレプリケーション用に設計されたアーカイブテクノロジーです。SnapMirror 関係では、通常、ソースボリューム内の Snapshot コピーだけがデスティネーションに含まれますが、SnapVault デスティネーションはより長期間にわたって作成されたポイントインタイムの Snapshot コピーを保持します。

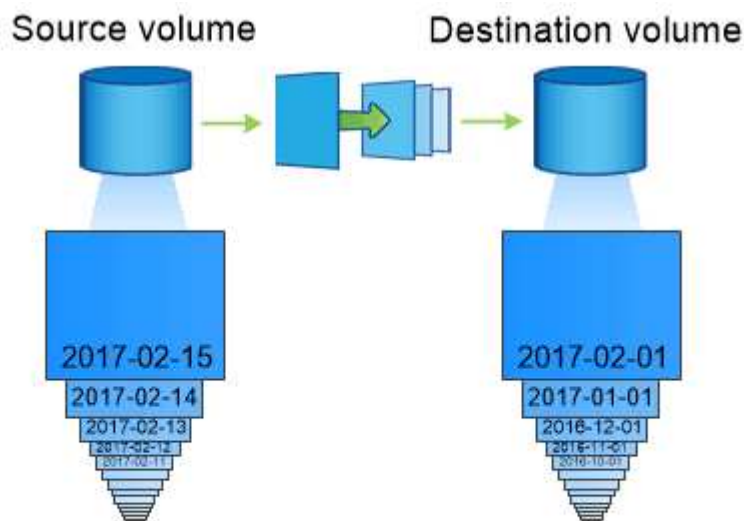
たとえば、ビジネスに関する政府会計規則に準拠するために、20 年にわたってデータの月次 Snapshot コピーを保持しなければならない場合があります。SnapVault ストレージからデータを提供する必要はないため、デスティネーションシステムでは低速かつ低コストのディスクを使用できます。

SnapMirror と同様に、SnapVault を初めて起動すると、ベースライン転送が実行されます。ソースボリュームの Snapshot コピーが作成され、そのコピーおよびコピーが参照するデータブロックがデスティネーションボリュームに転送されます。SnapMirror とは異なり、SnapVault ではベースラインに古い Snapshot コピーは含まれません。

更新は、設定したスケジュールに従って非同期に行われます。関係のポリシーで定義するルールによって、更新に含める新しい Snapshot コピーおよび保持するコピーの数が特定されます。ポリシーで定義されているラベル ("s only") は、ソース上の Snapshot ポリシーで定義されている 1 つ以上のラベルと一致する必要があります。そうしないと、レプリケーションが失敗します。



SnapMirror と SnapVault は同じコマンドインフラを共有します。ポリシーの作成時に使用する方法を指定します。どちらの方法にもピアクラスタとピア SVM が必要です。



*A SnapVault data protection relationship typically retains point-in-time Snapshot copies created over a longer period than the Snapshot copies on the source volume.*

ONTAP 9.7以前でのみディスクツーディスクで実行されていたSnapMirrorとSnapVaultのデータ保護関係に加えて、より低コストで長期的なデータ保持を実現できるバックアップソリューションがいくつか登場しました。

多数のサードパーティ製データ保護アプリケーションが、ONTAP で管理されるデータの従来のバックアップを提供しています。Veeam、Veritas、Commvault などが ONTAP システム向けの統合バックアップ機能を提供しています。

ONTAP 9.8 以降では、SnapMirror クラウドにより、ONTAP インスタンスからオブジェクトストレージエンドポイントへの Snapshot コピーの非同期レプリケーションが可能になりました。SnapMirror クラウドレプリケーションを使用するには、データ保護ワークフローのオーケストレーションおよび管理用に、ライセンスベースのアプリケーションが必要です。ONTAP システムでは、SnapMirror クラウド関係を使用して、オンプレミスおよびパブリッククラウドのオブジェクトストレージターゲットを選択できます。対象となるストレージには、AWS S3、Google Cloud Storage Platform、Microsoft Azure Blob Storage などがあり、これにより、ベンダーバックアップソフトウェアによる効率が向上します。サポートされている認定アプリケーションおよびオブジェクトストレージのベンダーの一覧については、ネットアップの担当者にお問い合わせください。

クラウドネイティブのデータ保護に関心がある場合は、BlueXPを使用して、オンプレミスのボリュームとパブリッククラウドのCloud Volumes ONTAP インスタンスの間にSnapMirrorまたはSnapVault 関係を設定できます。

BlueXPでは、ソフトウェアサービス（SaaS）モデルを使用してCloud Volumes ONTAP インスタンスのバックアップも提供しています。ユーザは、NetApp Cloud Central のクラウドバックアップを使用して、Cloud Volumes ONTAP インスタンスを S3 および S3 準拠のパブリッククラウドオブジェクトストレージにバックアップできます。

["Cloud Volumes ONTAP およびBlueXPのドキュメントリソース"](#)

["NetApp Cloud Central"](#)

## **MetroCluster** の継続的可用性

MetroCluster 構成は、物理的に分離された 2 つのミラークラスタを実装することでデータを保護します。各クラスタが、もう一方のクラスタのデータおよび SVM 設定を同期的にレプリケートします。一方のサイトで災害が発生したときは、ミラーリングされた SVM をアクティブ化し、ミラーリングされたデータをセカンダリサイトから提供できます。

- `_ファブリック接続 MetroCluster` 設定は、メトロポリタン規模のクラスタをサポートします。
- `_Stretch MetroCluster _configurations` は、キャンパス全体のクラスタをサポートします。

いずれの場合も、クラスタ間でピア関係を設定する必要があります

MetroCluster では、`_SyncMirror _` という ONTAP 機能を使用して、もう一方のクラスタのストレージでコピーまたは `_フレックス _` の形式で各クラスタのアグリゲートデータを同期的にミラーリングします。スイッチオーバーでは、サバイバークラスタ上のリモートプレックスがオンラインになり、セカンダリ SVM がデータの提供を開始します。





*When a MetroCluster switchover occurs, the remote plex on the surviving cluster comes online and the secondary SVM begins serving data.*

### **MetroCluster**以外の実装での**SyncMirror**の使用

必要に応じて、MetroCluster以外の実装でSyncMirrorを使用すると、RAIDタイプで保護されるディスク数よりも多くのディスクで障害が発生した場合や、RAIDグループのディスクへの接続が失われた場合にデータ損失を防ぐことができます。この機能は HA ペアに対してのみ使用できます。

アグリゲートデータは、別々のディスクシェルフに格納されたプレックス間でミラーリングされます。一方のシェルフが使用できなくなった場合、影響を受けていないプレックスが障害原因の修正中も引き続きデータを提供します。

SyncMirror を使用してミラーリングされたアグリゲートは、ミラーリングされていないアグリゲートの 2 倍のストレージを必要とすることに注意してください。各プレックスに、ミラーリングするプレックスと同じ数のディスクが必要です。たとえば、1、440GB のアグリゲートをミラーリングするには、プレックス 1 つにつき 1、440GB、合計で 2、880GB のディスクスペースが必要です。

SyncMirrorでは、ストレージのパフォーマンスと可用性を最適化するために、ミラーアグリゲート用に少なくとも20%の空きスペースを確保することを推奨します。ミラーされていないアグリゲートでは10%が推奨されますが、追加の10%のスペースはファイルシステムで増分変更に対応するために使用できます。増分変更を行うと、ONTAPのcopy-on-write Snapshotベースのアーキテクチャにより、ミラーされたアグリゲートのスペース使用率が向上します。これらのベストプラクティスに従わないと、SyncMirrorの再同期のパフォーマンスが低下し、非共有クラウド環境のNDUやMetroCluster環境のスイッチバックなどの運用ワークフローに間接的に影響します。



SyncMirror は、FlexArray 仮想化の実装にも使用できます。

## ストレージ効率

### **ONTAPのStorage Efficiencyの概要**

ストレージ効率とは、ストレージリソースを最適化し、無駄なスペースを最小限に抑え、書き込み済みデータの物理的なフットプリントを削減することで、ストレージシステムが使用可能なスペースを効果的に利用する方法のことです。Storage Efficiencyが高いほど、最大限のデータを最小限のスペースに最小限のコストで格納できます。たとえば、重複するデータブロックとゼロでいっぱいデータブロックを検出して排除するStorage Efficiencyテクノロジーを利用すると、必要な物理ストレージの総容量が削減され、全体的なコストが削減されます。

ONTAPは、さまざまなStorage Efficiencyテクノロジーを提供しています。このテクノロジーを使用すると、データが消費する物理ハードウェアやクラウドストレージの量を削減できます。また、データの読み取り速度、データセットのコピー速度、VMのプロビジョニング速度など、システムのパフォーマンスも大幅に向上します。

**ONTAPのStorage Efficiency**テクノロジーは次のとおりです。

- \* シンプロビジョニング \*

**シンプロビジョニング** ボリュームまたはLUNのストレージを事前にリザーブするのではなく、必要に応じて割り当てることができます。現在使用されていないスペースをリザーブすることなく、潜在的な使用量に基づいてボリュームまたはLUNを過剰に割り当てることができるため、必要な物理ストレージの量が削減されます。

- \* 重複排除 \*

**重複排除** ボリュームに必要な物理ストレージの量を3つの方法で削減します。

- ゼロブロック重複排除

ゼロブロック重複排除は、すべてゼロでいっぱいになったデータブロックを検出して排除し、メタデータのみを更新します。ゼロブロックで一般的に使用されているスペースの100%が削減されます。ゼロブロック重複排除は、すべての重複排除ボリュームでデフォルトで有効になります。

- インライン重複排除

インライン重複排除は、重複するデータブロックを検出し、データがディスクに書き込まれる前に一意の共有ブロックへの参照に置き換えます。インライン重複排除により、VMのプロビジョニングが20~30%高速化されます。インライン重複排除は、ONTAPのバージョンとプラットフォームに応じて、ボリュームレベルまたはアグリゲートレベルで実行できます。AFFシステムおよびASAシステムではデフォルトで有効になっています。FASシステムでは、インライン重複排除を手動で有効にする必要があります。

- バックグラウンド重複排除

バックグラウンド重複排除も、重複するデータブロックを検出して一意の共有ブロックへの参照に置き換えますが、データがディスクに書き込まれたあとに実行することで、ストレージ効率がさらに向上します。ストレージシステムで特定の条件が満たされたときに実行されるように、バックグラウンド重複排除を設定できます。たとえば、ボリュームの利用率が10%に達したときにバックグラウンド重複排除を実行できます。バックグラウンド重複排除は手動でトリガーすることも、特定のスケジュールで実行されるように設定することもできます。AFFシステムおよびASAシステムではデフォルトで有効になっています。FASシステムでは、バックグラウンド重複排除を手動で有効にする必要があります。

重複排除は、ボリューム内およびアグリゲート内のボリューム間でサポートされます。通常、重複排除されたデータの読み取りがパフォーマンスに影響することはありません。

- \* 圧縮 \*

**圧縮** データブロックを圧縮グループに結合し、各ブロックを単一のブロックとして格納することで、ボリュームに必要な物理ストレージの量を削減します。読み取り要求または上書き要求を受信すると、ファイル全体ではなく、少数のブロックグループのみが読み取られます。このプロセスにより、読み取りと上書きのパフォーマンスが最適化され、圧縮されるファイルのサイズの拡張性が向上します。

圧縮は、インラインまたはポストプロセスで実行できます。インライン圧縮では、ディスクに書き込む前にメモリ内のデータを圧縮することで、スペースを即座に削減できます。ポストプロセス圧縮では、まずブロックが圧縮されていない状態でディスクに書き込まれ、次にスケジュールされた時刻にデータが圧縮されます。圧縮は手動で有効にする必要があります。

- 圧縮

コンパクションを使用すると、サイズが4KB未満のデータチャンクを作成して単一のブロックに結合することで、ボリュームに必要な物理ストレージの量が削減されます。コンパクションはデータがメモリに残っている間に実行されるため、ディスク上で不要なスペースが消費されることはありません。AFFシステムおよびASAシステムではデフォルトで有効になっています。FASシステムでは、手動でコンパクションを有効にする必要があります。



- \* FlexCloneボリューム、ファイル、LUN \*

**FlexCloneテクノロジー** Snapshotメタデータを活用して、ボリューム、ファイル、LUNの書き込み可能なポイントインタイムコピーを作成します。コピーはデータブロックを親と共有し、変更がコピーまたはその親に書き込まれるまでメタデータに必要な分以外ストレージを消費しません。変更が書き込まれると、差分のみが保存されます。

従来のデータセットのコピーの作成には数分から数時間かかることがありますが、FlexCloneテクノロジーを使用すると、大規模なデータセットでもほぼ瞬時にコピーできます。

- 温度に敏感なストレージ効率

ONTAPの特長 **"温度に敏感なストレージ効率"** ボリュームのデータへのアクセス頻度を評価し、その頻度とデータに適用される圧縮レベルをマッピングすることで、メリットが得られます。アクセス頻度の低いコールドデータの場合は大容量のデータブロックが圧縮され、頻繁にアクセスされて上書きされるホットデータの場合は小さなデータブロックが圧縮されるため、プロセスが効率化されます。

温度識別型Storage Efficiency (TSSE) はONTAP 9.8で導入された機能で、新しく作成したシンプロビジョニングAFFボリュームでは自動的に有効になります。

これらのテクノロジーのメリットを日常業務で最小限の労力で実現できます。たとえば、5,000人のユーザにホームディレクトリ用のストレージを提供する必要があり、任意のユーザが必要とする最大スペースが1GBであるとしします。潜在的なストレージニーズに合わせて、5TBのアグリゲートを事前にリザーブすることもできます。ただし、ホームディレクトリの容量要件は組織によって大きく異なることもわかっています。組織用に合計スペースを5TBリザーブする代わりに、2TBのアグリゲートを作成できます。シンプロビジョニングを使用すると、名目上は各ユーザに1GBのストレージを割り当てることができますが、ストレージは必要に応じてのみ割り当てることができます。時間の経過とともにアグリゲートをアクティブに監視し、実際の物理サイズを必要に応じて増やすことができます。

別の例として、仮想デスクトップ間で大量の重複データが発生している仮想デスクトップインフラ (VDI) を使用しているとしします。重複排除は、VDI全体で重複する情報ブロックを自動的に排除し、元のブロックへのポインタに置き換えることで、ストレージの使用量を削減します。他のONTAPのStorage Efficiencyテクノロジー (圧縮など) も、手動操作なしでバックグラウンドで実行できます。

ONTAPディスクパーティショニングテクノロジーは、ストレージ効率も向上します。RAID DPテクノロジーは、パフォーマンスを犠牲にしたり、ディスクミラーリングのオーバーヘッドを増大させたりすることなく、二重ディスク障害からデータを保護します。ONTAP 9を使用した高度なSSDパーティショニングにより、使用可能容量が約20%増加します。

NetAppは、オンプレミスのONTAPと同じStorage Efficiency機能をクラウドで提供します。オンプレミスのONTAPからクラウドにデータを移行する場合は、既存のストレージ効率が維持されます。たとえば、ビジネスクリティカルなデータを含むSQLデータベースを、オンプレミスシステムからクラウドに移行するとしします。BlueXPのデータレプリケーションを使用してデータを移行できます。また、移行プロセスの一環として、クラウド内のSnapshotコピーに対して最新のオンプレミスポリシーを有効にすることもできます。

## シンプロビジョニング

ONTAP は、Snapshot コピーに加え、Storage Efficiency テクノロジーも幅広く提供しています。主なテクノロジーには、シンプロビジョニング、重複排除、圧縮、FlexClone ボリューム、ファイル、LUN の割り当てが可能です。Snapshot コピーと同様に、いずれも ONTAP の Write Anywhere File Layout (WAFL) を基盤としています。

シンプロビジョニングされたボリュームまたは LUN は、ストレージが事前に予約されていないボリュームです。代わりに、ストレージは必要に応じて動的に割り当てられます。ボリュームまたは LUN 内のデータが削除されると、空きスペースはストレージシステムに戻されます

たとえば、5、000 人のユーザにホームディレクトリ用のストレージを提供する必要があるとします。ホームディレクトリの消費スペースは、最大で 1GB と推定されます。

この状況では、5TB の物理ストレージを購入することが考えられます。ホームディレクトリを格納するボリュームごとに、最もスペースを消費するユーザのニーズを満たす十分なスペースを確保します。

しかし実際には、ホームディレクトリに必要なとされる容量はコミュニティによって大きく異なることもわかっています。ストレージを大量に消費するユーザごとに、ほとんど、またはまったく消費しないユーザが 10 人あります。

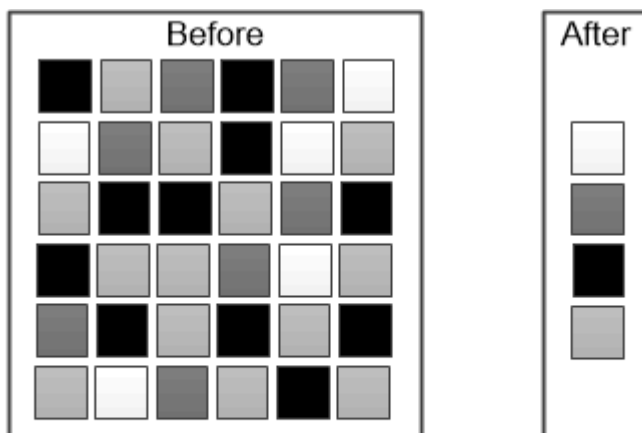
シンプロビジョニングを使用すると、使用しない可能性があるストレージを購入することなく、ストレージを大量に消費するユーザのニーズを満たすことができます。ストレージスペースは実際に消費されるまで割り当てられないため 2TB のアグリゲートを「オーバーコミット」するには、アグリゲートに含まれる 5、000 ボリュームのそれぞれに名目上は 1GB のサイズを割り当てる必要があります。

ライトユーザとヘビーユーザの 10 : 1 という比率に間違いがなければ、アグリゲートの空きスペースを能動的に監視しているかぎり、スペース不足によってボリュームへの書き込みが失敗することはありません。

## 重複排除

重複排除 \_ 重複するブロックを破棄して単一の共有ブロックへの参照に置き換えることで、ボリューム（または AFF アグリゲート内のすべてのボリューム）に必要な物理ストレージの量を削減します。通常、重複排除されたデータの読み取りがパフォーマンスに影響することはありません。ノードに負荷が集中している場合を除き、書き込みによる影響もほとんどありません。

通常の使用でデータが書き込まれると、WAFL はバッチプロセスを使用して \_ ブロックシグネチャのカタログを作成します。\_ 重複排除の開始後、ONTAP はカタログ内のシグネチャを比較して重複ブロックを特定します。一致するブロックがあった場合、カタログの作成後にそのブロックが変更されていないかどうかを検証するために 1 バイトずつ比較されます。すべてのバイトが一致した場合のみ、重複ブロックが破棄され、そのディスクスペースが解放されます。



*Deduplication reduces the amount of physical storage required for a volume by discarding duplicate data blocks.*

## 圧縮

**\_Compression :** 圧縮グループ内のデータブロックを結合し、それぞれを 1 つのブロックとして格納することで、ボリュームに必要な物理ストレージの量を減らします。ONTAP では、ファイルや LUN 全体ではなく、要求されたデータを含む圧縮グループのみが解凍されるため、従来の圧縮手法よりも短時間で圧縮されたデータを読み取ることができます。

インライン圧縮とポストプロセス圧縮の 2 つがあり、個別に実行することも組み合わせて実行することもできます。

- **\_Inline compression\_compression** は、データをメモリで圧縮してからディスクに書き込まれます。ボリュームへの書き込み I/O は大幅に削減されますが、書き込みパフォーマンスが低下する可能性があります。負荷の高い処理は次のポストプロセス圧縮処理まで保留されます。
- **\_ポスト プロセス圧縮**：ディスクに書き込まれたデータを、重複排除と同じスケジュールで圧縮します。

\* **\_インラインデータコンパクション\_** \* ゼロで埋められた小さなファイルまたは I/O は、4KB の物理ストレージが必要かどうかに関係なく、4KB ブロックに格納されます。**\_インラインデータコンパクション\_** では、通常であれば複数の 4KB ブロックを消費するデータチャンクをディスク上の 1 つの 4KB ブロックに結合します。コンパクションはデータがメモリにある間に行われるため、高速のコントローラに適しています。

## FlexClone ボリューム、ファイル、LUN

**\_FlexClone\_technology** は、Snapshot メタデータを参照して、ボリュームの書き込み可能なポイントインタイムコピーを作成しています。コピーと親でデータブロックが共有されるため、変更がコピーに書き込まれるまでメタデータに必要な分しかストレージは消費されません。FlexClone ファイルと FlexClone LUN も使用するテクノロジーは同じですが、元の Snapshot コピーは必要ありません。

従来の手法でコピーを作成すると数分から数時間かかりますが、FlexClone ソフトウェアを使用すれば大規模なデータセットのコピーもほぼ瞬時に作成できます。そのため、同一のデータセットのコピーが複数必要な状況（仮想デスクトップ環境など）や一時的にデータセットのコピーが必要な状況（本番環境のデータセットでアプリケーションをテストする場合など）に適しています。

既存の FlexClone ボリュームをクローニングしたり、LUN クローンを含むボリュームをクローニングしたり、ミラーやバックアップのデータをクローニングしたりできます。FlexClone ボリュームは親からスプリットできます。スプリットされた場合、コピーには独自のストレージが割り当てられます。



*FlexClone copies share data blocks with their parents, consuming no storage except what is required for metadata.*

#### System Manager で測定される容量

システム容量は、物理スペースと論理スペースのどちらかで測定できます。ONTAP 9.7 以降では、System Managerで物理容量と論理容量の両方を測定できます。

2つの測定値の違いについては、次の説明を参照してください。

- 物理容量：物理スペースとは、ボリュームまたはローカル階層で使用されているストレージの物理ブロックのことです。通常、使用済み物理容量の値は、ストレージ効率化機能（重複排除や圧縮など）によるデータの削減が原因で、使用済み論理容量の値よりも小さくなります。
- 論理容量：論理スペースは、ボリュームまたはローカル階層で使用可能なスペース（論理ブロック）です。論理スペースとは、重複排除や圧縮の結果を考慮せずに、理論上のスペースをどのように使用できるかを指します。使用済み論理スペースは、使用済みの物理スペースの量に加えて、設定済みの Storage Efficiency 機能（重複排除や圧縮など）による削減量から導き出されます。Snapshot コピー、クローン、その他のコンポーネントが含まれ、データ圧縮やその他の物理スペースの削減が反映されていないため、この測定値は、多くの場合、物理使用容量よりも大きく表示されます。したがって、合計論理容量は、プロビジョニング済みスペースよりも多くなる可能性があります。



System Manager では、ルートストレージ階層（アグリゲート）の容量は表示されません。

#### 使用済み容量の測定値

使用済み容量の測定値の表示方法は、次の表に示すように、使用している System Manager のバージョンによって異なります。

System Manager のバージョン	容量に使用される用語	参照される容量のタイプ
9.9.1 以降	使用済みの論理容量	使用済みの論理スペース Storage Efficiencyの設定が有効になっている場合)

9.7 および 9.8	使用済み	使用済みの論理スペース (Storage Efficiencyの設定が有効になっている場合)
9.5および9.6 (クラシックビュー)	使用済み	使用済みの物理スペース

#### 容量測定条件

容量の説明では次の用語を使用します。

- 割り当て容量：Storage VM内のボリュームに割り当てられているスペースの量。
- 使用可能：Storage VMまたはローカル階層でデータの格納やボリュームのプロビジョニングに使用できる物理スペースの量。
- ボリューム間の容量：Storage VM上のすべてのボリュームの使用済みストレージと使用可能なストレージの合計。
- クライアントデータ：クライアントデータによって使用されている容量（物理または論理）。
  - ONTAP 9.13.1以降では、クライアントデータで使用されている容量を\*論理使用済み\*と呼び、Snapshotコピーで使用されている容量は別々に表示されます。
  - ONTAP 9.12.1以前では、クライアントデータに使用されている容量がSnapshotコピーで使用されている容量に追加された容量を\*論理使用済み\*と呼びます。
- \* Committed \*：ローカル階層のコミット済み容量。
- データ削減：
  - ONTAP 9.13.1以降では、データ削減比率が次のように表示されます。
    - [容量]\*パネルに表示されるデータ削減値は、SnapshotコピーなどのStorage Efficiency機能を使用した場合に達成される大幅な削減量を考慮していない、使用済み論理スペースと物理スペースの割合です。
    - 詳細パネルを表示すると、概要パネルに表示された比率と、物理使用済みスペースと比較したすべての使用済み論理スペースの総比率の両方が表示されます。 Snapshotコピーを使用する\*と呼ばれるこの値には、Snapshotコピーやその他のStorage Efficiency機能を使用することによるメリットが含まれています。
  - ONTAP 9.12.1以前では、データ削減比率は次のように表示されます。
    - [容量]\*パネルに表示されるデータ削減量には、使用済み物理スペースに対するすべての使用済み論理スペースの総削減率が表示され、Snapshotコピーやその他のStorage Efficiency機能の使用によるメリットも含まれます。
    - 詳細パネルを表示すると、概要パネルに表示された\*[全体]\*の比率と、クライアントデータのみで使用されている物理スペースと比較した、クライアントデータのみで使用されている論理スペースの比率の両方が表示されます。これを「Snapshotコピーとクローンなし」\*と呼びます。
- 使用済み論理容量：
  - ONTAP 9.13.1以降では、クライアントデータで使用されている容量を\*論理使用済み\*と呼び、Snapshotコピーで使用されている容量は別々に表示されます。
  - ONTAP 9.12.1以前では、クライアントデータで使用されている容量がSnapshotコピーで使用されている容量に追加された容量を\*論理使用済み\*と呼びます。

- \* Logical Used%\* : Snapshotリザーブを除く、プロビジョニングサイズに対する現在の使用済み論理容量の割合。この値は、ボリューム内での効率化による削減も含まれるため、100%より大きい値にすることができます。
- 最大容量 : Storage VM上のボリュームに割り当てられる最大スペース。
- 使用済み物理容量 : ボリュームまたはローカル階層の物理ブロックで使用されている容量。
- \* Physical Used %\* : ボリュームの物理ブロックで使用されている容量の、プロビジョニングされたサイズに対する割合。
- プロビジョニングされた容量 : Cloud Volumes ONTAPシステムから割り当てられ、ユーザやアプリケーションのデータを格納できる状態にあるファイルシステム (ボリューム)。
- \* Reserved \* : ローカル階層ですでにプロビジョニングされているボリューム用にリザーブされているスペースの量。
- 使用済み : データが格納されているスペースの量。
- \* usedおよびreserved \* : 使用済みの物理スペースとリザーブスペースの合計です。

### Storage VMの容量

Storage VMの最大容量は、ボリュームに割り当てられている合計スペースに未割り当ての残りスペースを足したものです。

- ボリュームの割り当てスペースは、FlexVol、FlexGroup、およびFlexCacheの使用済み容量と使用可能容量の合計です。
- ボリュームの容量は、制限されている場合、オフラインの場合、または削除後にリカバリキューに格納されている場合でも、合計に含まれます。
- ボリュームに自動拡張が設定されている場合は、ボリュームの最大オートサイズの値が合計で使用されます。自動拡張を使用しない場合は、ボリュームの実際の容量が合計で使用されます。

次のグラフは、ボリューム間の容量の測定値と最大容量の関係を示しています。



ONTAP 9.13.1以降では、クラスタ管理者が使用できます ["Storage VMの最大容量制限を有効にする"](#)。ただし、データ保護、SnapMirror関係、またはMetroCluster 構成のボリュームを含むStorage VMに対してストレージ制限を設定することはできません。また、Storage VMの最大容量を超えるようにクォータを設定することはできません。

最大容量制限の設定後は、現在割り当てられている容量よりも小さいサイズに変更することはできません。

Storage VMが最大容量に達すると、一部の処理を実行できなくなります。System Managerには、の次の手順に関する推奨事項が表示されます ["インサイト"](#)。

#### 容量の単位

System Manager は、1024 ( $2^{10}$ ) バイトのバイナリ単位に基づいてストレージ容量を計算します。

- ONTAP 9.10.1以降では、System Managerにストレージ容量の単位がKiB、MiB、GiB、TiB、およびPiBとして表示されます。
- ONTAP 9.10.0以前では、これらの単位はSystem ManagerにKB、MB、GB、TB、およびPBとして表示されます。



System Manager のスループットに使用される単位は、すべてのリリースの ONTAP について、KB/ 秒、MB/ 秒、GB/ 秒、および PB / 秒です。



ONTAP 9.10.0 以前の System Manager で表示される容量の単位	ONTAP 9.10.1以降のSystem Manager に表示される容量単位	計算	バイト単位の値
KB	KiB	一、〇二四	1024 バイト
MB	MiB	1024 * 1024	1、048、576 バイト
GB	GiB	1024 * 1024 * 1024	1、073、741、824バイト
容量	TiB	1024 * 1024 * 1024 * 1024	1、099、511、627、776 バイト
PB	PiB	1024 * 1024 * 1024 * 1024 * 1024	1、125、899、906、842、624 バイト

## 関連情報

["System Manager で容量を監視"](#)

["ボリュームの論理スペースのレポートと適用"](#)

## 温度に敏感なストレージ効率の概要

ONTAP は、ボリュームのデータへのアクセス頻度を評価し、その頻度とデータに適用される圧縮レベルをマッピングすることで、温度に影響されるStorage Efficiencyのメリットを提供します。アクセス頻度の低いコールドデータの場合は大容量のデータブロックが圧縮され、頻繁にアクセスされて上書きされるホットデータの場合は小さなデータブロックが圧縮されるため、プロセスが効率化されます。

温度識別型Storage Efficiency (TSSE) はONTAP 9.8で導入された機能で、新しく作成したシンプロビジョニングAFFボリュームでは自動的に有効になります。既存のAFFボリュームとシンプロビジョニングされたAFF DP以外のボリュームでは、温度に基づくStorage Efficiencyを有効にすることができます。

「デフォルト」モードと「効率的」モードが導入されました

ONTAP 9.10.1以降では、AFF システムに対してのみ、ボリュームレベルの2つのStorage Efficiencyモード (*default\_*と*\_efficient*) が導入されました。この2つのモードでは、新しいAFFボリュームの作成時のデフォルトモードであるファイル圧縮 (デフォルト) と、温度に基づくStorage Efficiency (効率的) のどちらかを選択できます。ONTAP 9.10.1では、["温度に基づくストレージ効率化は明示的に設定する必要があります"](#) 自動アダプティブ圧縮を有効にします。ただし、AFF プラットフォームでは、データコンパクション、自動重複排除スケジュール、インライン重複排除、ボリューム間インライン重複排除、ボリューム間バックグラウンド重複排除などの他のStorage Efficiency機能が、デフォルトモードと効率モードのどちらでもデフォルトで有効になります。

どちらのStorage Efficiencyモード (デフォルトと効率化) も、FabricPool対応アグリゲートでサポートされ、すべての階層化ポリシータイプでサポートされます。

**C**シリーズプラットフォームで温度に基づく **Storage Efficiency** を有効にします

AFF Cシリーズプラットフォーム、および次のリリースがインストールされたデスティネーションでボリューム移動またはSnapMirrorを使用して、非TSSEプラットフォームからTSSE対応Cシリーズプラットフォームにボリュームを移行する場合、温度に基づくStorage Efficiencyがデフォルトで有効になります。

- ONTAP 9.12.1P4以降
- ONTAP 9.13.1以降

詳細については、を参照してください ["ボリューム移動処理とSnapMirror処理でのStorage Efficiencyの動作"](#)。

既存のボリュームでは、温度に基づくStorage Efficiencyは自動的に有効になりませんが、有効にすることはできます ["Storage Efficiencyモードを変更します"](#) 手動で効率モードに変更します。



Storage Efficiencyモードを効率化モードに変更したあとに元に戻すことはできません。

連続する物理ブロックをシーケンシャルにパッキングすることで、ストレージ効率が向上します

ONTAP 9.13.1以降では、温度に左右されるストレージ効率化機能によって、連続する物理ブロックのシーケンシャルパッキングが追加され、ストレージ効率がさらに向上します。システムをONTAP 9.13.1にアップグレードすると、温度の影響を受けやすいStorage Efficiencyが有効になっているボリュームでは、自動的にシーケンシャルパッキングが有効になります。シーケンシャルパッキングを有効にした後は、を実行する必要があります ["既存のデータを手動で再バックします"](#)。

#### アップグレード時の考慮事項

ONTAP 9.10.1以降にアップグレードする場合、既存のボリュームには、ボリュームで現在有効になっている圧縮のタイプに基づいてStorage Efficiencyモードが割り当てられます。アップグレードの実行時、圧縮が有効なボリュームにはデフォルトモードが割り当てられ、温度に影響されるストレージ効率化が有効になっているボリュームには効率的モードが割り当てられます。圧縮が有効になっていない場合、Storage Efficiency モードは空白のままです。

## セキュリティ

### クライアントの認証と許可

ONTAP では、標準的な方法を使用して、クライアントや管理者によるストレージへのアクセスを保護し、ウィルスから保護します。保存データの暗号化や WORM ストレージでは、高度なテクノロジーも使用できます。

ONTAP では、信頼できるソースで ID を検証してクライアントマシンおよびユーザを認証します。ONTAP は、ユーザのクレデンシャルとファイルまたはディレクトリに対して設定されている権限を比較して、ユーザにファイルまたはディレクトリへのアクセスを許可します。

### 認証

ローカルまたはリモートのユーザアカウントを作成できます。

- ローカルアカウントでは、アカウント情報がストレージシステムに格納されます。
- リモートアカウントでは、アカウント情報が Active Directory ドメインコントローラ、LDAP サーバ、または NIS サーバに格納されます。

ONTAP は、ローカルまたは外部のネームサービスを使用して、ホスト名、ユーザ、グループ、ネットグループ

プ、およびネームマッピング情報を検索します。ONTAP では、次のネームサービスをサポートしています。

- ローカルユーザ
- DNS
- 外部 NIS ドメイン
- 外部LDAPドメイン

a\_name service switch table\_ には、ネットワーク情報を検索するソースと、その検索順序を指定します（UNIX システムの /etc/nsswitch.conf ファイルに相当する機能を提供します）。NAS クライアントが SVM に接続すると、ONTAP は指定されたネームサービスをチェックして、必要な情報を取得します。

*\*kerberos support\**Kerberos は ' クライアント / サーバ実装でユーザ・パスワードを暗号化することによって「三次認証」を提供するネットワーク認証プロトコルですONTAP では、整合性チェック機能を備えた Kerberos 5 認証（krb5i）とプライバシーチェック機能を備えた Kerberos 5 認証（krb5p）をサポートしています。

#### 承認

ONTAP では、3 つのレベルのセキュリティを評価して、SVM 上にあるファイルおよびディレクトリに対して要求された処理を実行する権限がエンティティにあるかどうかを判断します。アクセスは、セキュリティレベルの評価後に有効な権限によって判断されます。

- エクスポート（NFS）および共有（SMB）セキュリティ

指定された NFS エクスポートまたは SMB 共有へのエクスポートおよび共有セキュリティ環境クライアントアクセス管理者権限を持つユーザは、SMB クライアントと NFS クライアントからエクスポートおよび共有レベルのセキュリティを管理できます。

- ストレージレベルのアクセス保護のファイルおよびディレクトリセキュリティ

ストレージレベルのアクセス保護セキュリティ環境 SVM ボリュームへの SMB および NFS クライアントアクセスNTFS のアクセス権のみがサポートされています。ONTAP で、ストレージレベルのアクセス保護が適用されているボリューム上のデータにアクセスする UNIX ユーザのセキュリティチェックを行うには、UNIX ユーザがボリュームを所有する SVM 上の Windows ユーザにマッピングされている必要があります。

- NTFS、UNIX、および NFSv4 のネイティブのファイルレベルのセキュリティ

ストレージオブジェクトを表すファイルやディレクトリには、ネイティブのファイルレベルのセキュリティが存在します。ファイルレベルのセキュリティはクライアントから設定できます。ファイル権限は、データへのアクセスに SMB と NFS のどちらを使用するかに関係なく有効です。

#### SAMLによる認証

ONTAPでは、リモートユーザの認証でSecurity Assertion Markup Language（SAML）がサポートされます。いくつかの一般的なIDプロバイダ（IdP）がサポートされています。サポートされているIdPとSAML認証を有効にする手順の詳細については、[を参照してください。"SAML 認証を設定する"](#)。

ONTAP 9.14以降では、Open Authorization (OAuth 2.0) フレームワークがサポートされています。クライアントがREST APIを使用してONTAPにアクセスする場合、OAuth 2.0のみを使用して認証とアクセス制御を行うことができます。ただし、この機能は、CLI、System Manager、REST APIなどの任意のONTAP管理インターフェイスを使用して設定および有効化できます。

標準のOAuth 2.0機能は、いくつかの一般的な認可サーバーとともにサポートされています。相互TLSに基づいて送信者に制限されたアクセストークンを使用することで、ONTAPのセキュリティをさらに強化できます。また、自己完結型スコープや、ONTAP RESTロールやローカルユーザ定義との統合など、さまざまな認証オプションを利用できます。を参照してください ["ONTAP OAuth 2.0実装の概要"](#) を参照してください。

### 管理者認証と RBAC

管理者は、ローカルまたはリモートのログインアカウントを使用してクラスタおよびSVMへの認証を行います。管理者がアクセスできるコマンドは、ロールベースアクセス制御 (RBAC) に基づいて決まります。

#### 認証

クラスタおよびSVMの管理者アカウントは、ローカルまたはリモートのいずれかとして作成できます。

- ローカルアカウントでは、アカウント情報、公開鍵、セキュリティ証明書がストレージシステムに格納されます。
- リモートアカウントでは、アカウント情報がActive Directory ドメインコントローラ、LDAP サーバ、またはNIS サーバに格納されます。

ONTAP では、DNS を除き、管理者アカウントの認証にクライアントの認証と同じネームサービスを使用します。

#### RBAC

管理者がアクセスできるコマンドは、管理者に割り当てられている `_role_assigned` コマンドで決まります。ロールは管理者のアカウントを作成するときに割り当てます。必要に応じて、別のロールを割り当てたりカスタムロールを定義したりできます。

#### ウィルススキャン

ストレージシステムに統合されたウィルス対策機能を使用して、ウィルスやその他の悪意のあるプログラムからデータを保護することができます。ONTAP ウィルススキャン (`_vscan`) は、クラス最高のサードパーティ製ウィルス対策ソフトウェアとONTAP機能を組み合わせたもので、どのファイルをスキャンするか、いつスキャンするかを柔軟に制御できます。

スキャン処理は、サードパーティベンダーのウィルス対策ソフトウェアをホストする外部サーバで実行されます。ネットアップが提供し、外部サーバにインストールされるONTAP Antivirus Connectorは、ストレージシステムとウィルス対策ソフトウェア間の通信を処理します。

- クライアントがSMB経由でファイルを開く、読み取る、名前を変更する、閉じるたびにウィルスチェックを行うには、`_on_access_scanning_to` を使用します。ファイル処理は、外部サーバからファイルのスキャンステータスがレポートされるまで中断されます。ファイルがすでにスキャンされている場合、

ONTAP はファイル操作を許可します。それ以外の場合は、サーバからのスキャンを要求します。

オンアクセススキャンは NFS ではサポートされていません。

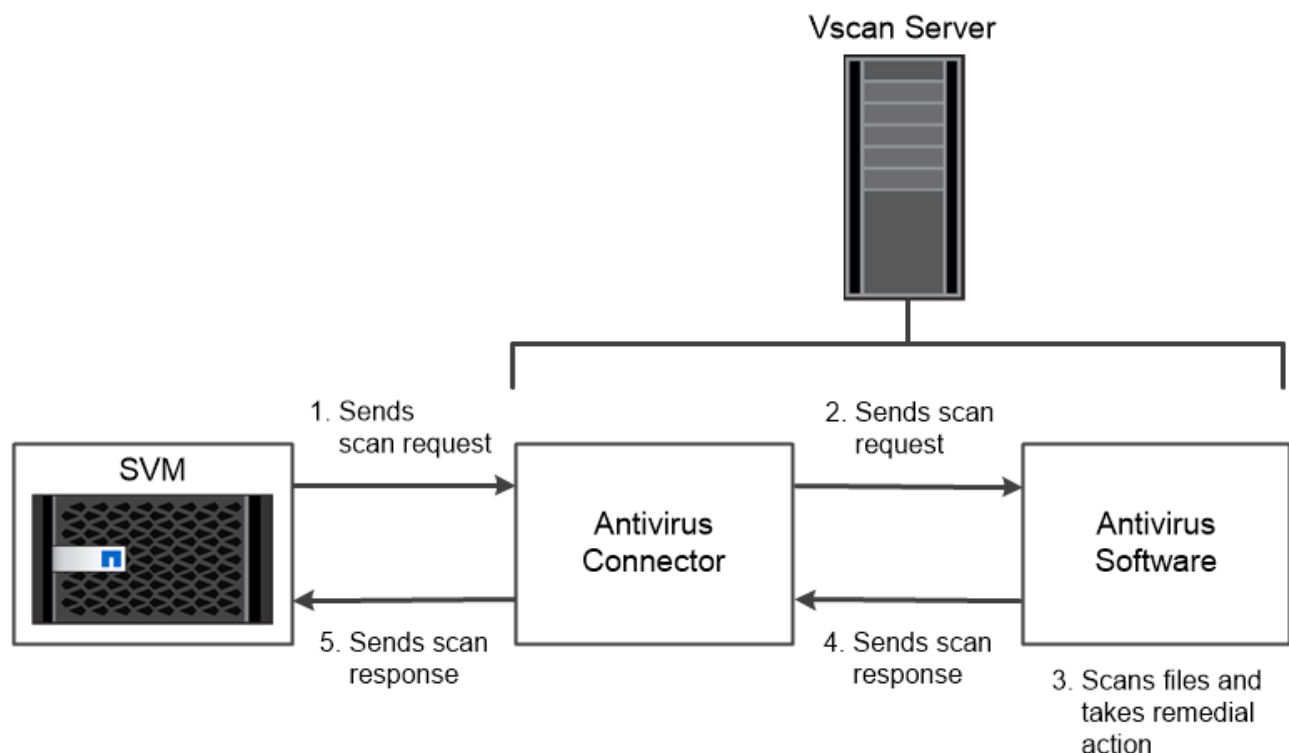
- オンデマンドスキャン \_ を使用すると、ファイルのウイルスチェックをただちにまたはスケジュールに基づいて実行できます。たとえば、ピーク時を避けてスキャンを実行する場合などに便利です。外部サーバはチェックしたファイルのスキャンステータスを更新するため、SMB 経由で次回それらのファイルがアクセスされたときには（ファイルが変更されていなければ）ファイルアクセスレイテンシが低減されます。

オンデマンドスキャンは、NFS 経由でのみエクスポートされたボリュームも含め、SVM ネームスペース内のすべてのパスに対して使用できます。

通常、SVM に対して両方のスキャンモードを有効にします。どちらのモードでも、感染したファイルにはウイルス対策ソフトウェアで設定した処理が実行されます。

\* \_ 災害復旧および MetroCluster 設定でのウイルススキャン \_ \*

ディザスタリカバリ構成と MetroCluster 構成では、ローカルクラスタとパートナークラスタのそれぞれに対して Vscan サーバを個別に設定する必要があります。



*The storage system offloads virus scanning operations to external servers hosting antivirus software from third-party vendors.*

暗号化

ONTAP は、ストレージメディアの転用、返却、置き忘れ、盗難に際して保存データが読み取られないようにソフトウェアベースとハードウェアベースの暗号化テクノ

ログを提供します。

ONTAP は、すべての SSL 接続に対する連邦情報処理標準（FIPS）140-2 に準拠しています。次の暗号化ソリューションを使用できます。

- ハードウェアソリューション：

- NetApp Storage Encryption（NSE）

NSE は、Self-Encrypting Drive（SED；自己暗号化ドライブ）を使用するハードウェア解決策です。

- NVMe SED

ONTAP は、FIPS 140-2 認定を取得していない NVMe SED の完全なディスク暗号化を提供します。

- ソフトウェアソリューション：

- NetApp Aggregate Encryption（NAE）

NAE は、あらゆるドライブタイプのあらゆるデータボリュームを暗号化できるソフトウェア解決策です。NAE は、アグリゲートごとに固有のキーを使用して有効にします。

- NetApp Volume Encryption（NVE）

NVE は、あらゆるドライブタイプのあらゆるデータボリュームを暗号化できるソフトウェア解決策です。ボリュームごとに一意のキーを使用して有効にします。

ソフトウェア（NAE または NVE）とハードウェア（NSE または NVMe SED）の両方の暗号化ソリューションを使用して、保存データを二重に暗号化できます。NAE または NVE 暗号化はストレージ効率に影響しません。

#### NetApp Storage Encryption の略

NetApp Storage Encryption（NSE）は、データを書き込み時に暗号化する SED をサポートします。ディスクに格納された暗号化キーがないとデータを読み取ることはできません。暗号化キーには認証されたノードからしかアクセスできません。

I/O 要求を受け取ったノードは、外部キー管理サーバまたはオンボードキーマネージャから取得した認証キーを使用して SED への認証を行います。

- 外部キー管理サーバはストレージ環境に配置されたサードパーティのシステムで、Key Management Interoperability Protocol（KMIP）を使用してノードに認証キーを提供します。
- オンボードキーマネージャは組み込みのツールで、データと同じストレージシステムからノードに認証キーを提供します。

NSE では、HDD と SSD の自己暗号化ディスクをサポートしています。NetApp Volume Encryption を NSE とともに使用すると、NSE ドライブのデータを二重に暗号化できます。



Flash Cacheモジュールを搭載したシステムでNSEを使用する場合は、NVEまたはNAEも有効にする必要があります。NSEは、Flash Cacheモジュール上のデータを暗号化しません。



## NVMe 自己暗号化ドライブ

NVMe SED には FIPS 140-2 認定はありませんが、これらのディスクでは AES 256 ビットの透過的なディスク暗号化を使用して保存データが保護されます。

認証キーの生成などのデータ暗号化処理は内部的に実行されます。認証キーは、ストレージシステムが初めてディスクにアクセスしたときに生成されます。その後、データ処理が要求されるたびにストレージシステム認証が要求されるため、保存データがディスクで保護されます。

## NetApp Aggregate Encryption の略

NetApp Aggregate Encryption (NAE) は、アグリゲート内のすべてのデータを暗号化するためのソフトウェアベースのテクノロジーです。NAE のメリットは、ボリュームがアグリゲートレベルの重複排除に含まれているのに対し、NVE ボリュームは除外されることです。

NAE が有効になっている場合は、アグリゲートキーを使用してアグリゲート内のボリュームを暗号化できます。

ONTAP 9.7以降では、新規に作成したアグリゲートとボリュームがデフォルトで暗号化されます。["NVEライセンス"](#) およびオンボードまたは外部のキー管理

## NetApp Volume Encryption の略

NetApp Volume Encryption (NVE) は、一度に 1 ボリュームずつ保管データを暗号化するためのソフトウェアベースのテクノロジーです。暗号化キーにはストレージシステムからしかアクセスできないため、基盤のデバイスがシステムから分離されている場合、ボリュームのデータが読み取られることはありません。

Snapshot コピーとメタデータの両方が暗号化されます。データへのアクセスには、ボリュームごとに 1 つずつ、一意の XTS-AES-256 キーを使用します。このキーは、組み込みのオンボードキーマネージャによってデータと同じシステムに安全に保管されます。

NVE は、アグリゲートのタイプ (HDD、SSD、ハイブリッド、アレイ LUN) や RAID タイプを問わず、サポートされるすべての ONTAP 環境 (ONTAP Select を含む) で使用できます。NVE を NetApp Storage Encryption (NSE) と併用して、NSE ドライブのデータを二重に暗号化することもできます。

\*\_KMIP サーバを使用するタイミング\_\* オンボードキーマネージャを使用する方が安価で通常は便利ですが、次のいずれかに該当する場合は KMIP サーバをセットアップする必要があります。

- 連邦情報処理標準 (FIPS) 140-2 または OASIS KMIP 標準に準拠した暗号化キー管理解決策が必要な場合。
- マルチクラスタ解決策が必要な場合。KMIP サーバでは、複数のクラスタの暗号化キーの一元管理がサポートされます。

KMIP サーバでは、複数のクラスタの暗号化キーの一元管理がサポートされます。

- 認証キーをデータとは別のシステムや場所に格納してセキュリティを強化する必要がある場合。

KMIP サーバでは、データとは別に認証キーが格納されます。

## 関連情報

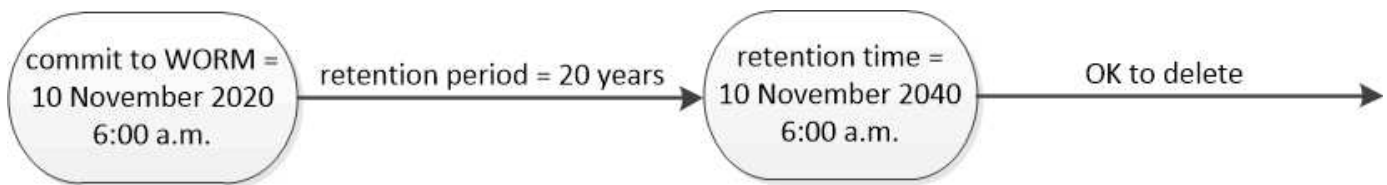
["FAQ - NetApp Volume EncryptionおよびNetApp Aggregate Encryption"](#)

## WORM ストレージ

**解決策** は、規制やガバナンスに準拠するために変更不可能な状態で重要なファイルを保管するために、**Write Once、Read Many (WORM)** ストレージを使用する組織向けの、ハイパフォーマンスなコンプライアンス SnapLock です。

1 つのライセンスで、SEC Rule 17a-4 などの社外規定に準拠するための strict **Compliance** モードと、社内規定に準拠してデジタル資産を保護するためのより緩やかな **Enterprise** モードで SnapLock を使用できます。SnapLock では、改ざん防止機能を備えた **ComplianceClock** を使用して、WORM ファイルの保持期間が経過したかどうかを判断します。

SnapVault から WORM 方式でセカンダリストレージの Snapshot コピーを保護するには、**SnapLock for** を使用します。SnapMirror を使用すると、ディザスタリカバリなどの目的で、地理的に離れた別の場所に WORM ファイルをレプリケートできます。



*SnapLock uses a tamper-proof ComplianceClock to determine when the retention period for a WORM file has elapsed.*

## アプリケーション対応のデータ管理

アプリケーション対応のデータ管理では、ONTAP 経由で導入するアプリケーションを、ストレージの観点ではなくアプリケーションの観点で設定できます。アプリケーションは、System Manager と REST API を使用して、最小限の入力で簡単に設定してデータを提供できる状態にすることができます。

アプリケーション対応のデータ管理機能を使用すると、個々のアプリケーションレベルでストレージをセットアップ、管理、監視できます。関連する ONTAP のベストプラクティスを組み込むことで、必要なパフォーマンスサービスレベルと使用可能なシステムリソースを基にストレージオブジェクトを分散配置し、アプリケーションを最適にプロビジョニングします。

アプリケーション対応のデータ管理機能には、一連のアプリケーションテンプレートが含まれています。各テンプレートは、アプリケーションの設定をまとめた一連のパラメータで構成されています。これらのパラメータは、多くの場合デフォルト値であらかじめ設定されていますが、データベースのサイズ、サービスレベル、LIF などのプロトコルアクセス要素、ローカルの保護条件、リモートの保護条件など、ONTAP システムでストレージをプロビジョニングする際にアプリケーション管理者が指定できる特性を定義します。ONTAP は、LUN やボリュームなどのストレージエンティティを、指定されたパラメータに基づいてアプリケーションに適したサイズとサービスレベルで設定します。

アプリケーションに対しては次のタスクを実行できます。

- アプリケーションテンプレートを使用してアプリケーションを作成します
- アプリケーションに関連付けられているストレージを管理します
- アプリケーションを変更または削除します

- アプリケーションを表示します
- アプリケーションの Snapshot コピーを管理する
- 作成 [整合グループ](#) 同じボリュームまたは異なるボリュームの複数の LUN を選択してデータ保護機能を提供します

## FabricPool

ネットアップのお客様の多くは、ほとんどアクセスされない膨大な量の保存データを保有しています。これは、`_COM_DATA` と呼ばれます。また、お客様は頻繁にアクセスされるデータも保有しており、これを `_hot_data` と呼んでいます。最高のパフォーマンスを得るために、ホットデータを最速のストレージに保存するのが理想的です。コールドデータは、必要に応じてすぐに使用可能であれば、低速のストレージに移動できます。しかし、データのどの部分がホットでコールドなのかをどのようにして把握していますか？

FabricPool は、アクセスパターンに基づいて高パフォーマンスのローカル階層（アグリゲート）とクラウド階層の間でデータを自動的に移動する ONTAP の機能です。階層化によって、コールドデータをクラウド内の低コストのオブジェクトストレージから容易に利用できるようにしながら、ホットデータ用の高価なローカルストレージを解放できます。FabricPool では、データアクセスを常時監視し、階層間でデータを移動することで、パフォーマンスを最大限に高め、コストを削減します。

FabricPool を使用してコールドデータをクラウドに階層化するのは、クラウドの効率化とハイブリッドクラウド構成を作成する最も簡単な方法の 1 つです。FabricPool はストレージブロックレベルで機能するため、ファイルデータと LUN データの両方に対応します。

しかし、FabricPool は、オンプレミスのデータをクラウドに階層化するだけではありません。多くのお客様が、Cloud Volumes ONTAP in FabricPool を使用して、コールドデータを高コストのクラウドストレージからクラウドプロバイダ内の低コストのオブジェクトストレージに階層化しています。ONTAP 9.8 以降では、を使用して FabricPool 対応ボリュームの分析を取得できます ["File System Analytics の略"](#) または ["温度に敏感なストレージ効率"](#)。

データを使用するアプリケーションは、データが階層化されていることを認識しないため、アプリケーションの変更は必要ありません。階層化は完全に自動化されているため、継続的な管理は不要です。

主要なクラウドプロバイダのいずれかからオブジェクトストレージにコールドデータを格納できます。また、コールドデータをプライベートクラウドに保存して、最高のパフォーマンスと完全なデータ管理を実現することも StorageGRID できます。

### 関連情報

["FabricPool システムマネージャドキュメント"](#)

["BlueXPの階層化"](#)

["NetApp TechComm TV で FabricPool 関連ビデオを視聴する"](#)

# ONTAPソフトウェアとファームウェアのセットアップ、アップグレード、リバート

## ONTAPのセットアップ

### ONTAPクラスタセットアップの開始

System ManagerまたはONTAPコマンドラインインターフェイス（CLI）を使用して、新しいONTAPクラスタをセットアップできます。作業を開始する前に、クラスタ管理インターフェイスのポートやIPアドレスなど、クラスタセットアップを完了するために必要な情報を収集しておく必要があります。

NetAppでは、"[System Managerを使用して新しいクラスタをセットアップする](#)"。System Managerでは、ノード管理IPアドレスの割り当て、クラスタの初期化、ローカル階層の作成、プロトコルの設定、初期ストレージのプロビジョニングなど、クラスタのセットアップと設定のワークフローをシンプルかつ簡単に実行できます。

必要なのは "[ONTAP CLIを使用したクラスタのセットアップ](#)" MetroCluster構成でONTAP 9.7以前を実行している場合。

ONTAP 9.13.1以降では、AFF A800およびFAS8700プラットフォームで、IPv6のみのネットワーク環境でONTAP CLIを使用して新しいクラスタを作成および設定することもできます。ONTAP 9.13.0以前、またはONTAP 9.13.1以降の他のプラットフォームでIPv6を使用する必要がある場合は、System Managerを使用してIPv4を使用して新しいクラスタを作成し、"[IPv6に変換します](#)"。

### クラスタセットアップに必要なもの

クラスタのセットアップでは、各ノードをセットアップするために必要な情報を収集し、最初のノードにクラスタを作成し、残りのノードをクラスタに追加します。

まず、クラスタセットアップワークシートに関連するすべての情報を収集します。

クラスタセットアップワークシートを使用して、クラスタセットアッププロセスで必要となる値を記録できます。デフォルト値が指定されている場合は、その値を使用することも、独自の値を入力することもできます。

### システムのデフォルト設定

システムのデフォルトは、プライベートクラスタネットワークのデフォルト値です。これらのデフォルト値を使用することを推奨します。ただし、これらの値が要件に合わない場合は、次の表を使用して独自の値を記録できます。



ネットワークスイッチを使用するように設定されたクラスタの場合、各クラスタスイッチで9000 MTU サイズを使用する必要があります。

情報の種類	値を入力します
プライベートクラスタネットワークのポート	
クラスタネットワークのネットマスク	

情報の種類	値を入力します
<p>クラスタインターフェイスのIPアドレス（各ノードの各クラスタネットワークポート用）</p> <p>各ノードのIPアドレスが同じサブネット上にある必要があります。</p>	

#### クラスタ情報


情報の種類	値を入力します
<p>クラスタ名</p> <p>名前の1文字目はアルファベットにする必要があります、最大文字数は44文字です。名前には次の特殊文字を含めることができます。</p> <p>・ - _</p>	

#### 機能ライセンスキー

初回購入のソフトウェアまたはアドオンソフトウェアのライセンスキーは、NetApp Support Siteの「\* My Support \* > \* Software Licenses」にあります。

情報の種類	値を入力します
機能ライセンスキー	

#### 管理 Storage Virtual Machine（SVM）

情報の種類	値を入力します
<p>クラスタ管理者のパスワード</p> <p>クラスタ管理者がコンソールにアクセスするとき、またはセキュアなプロトコルを介してアクセスするときにクラスタから入力を求められる、管理者アカウントのパスワードです。</p> <div style="display: flex; align-items: center;">  <p>セキュリティ上の理由から、このワークシートにパスワードを記録することは推奨されません。</p> </div> <p>パスワードのデフォルトのルールは次のとおりです。</p> <ul style="list-style-type: none"> <li>パスワードは8文字以上にする必要があります。</li> <li>アルファベットと数字をそれぞれ1文字以上含む。</li> </ul>	

情報の種類	値を入力します
<p>クラスタ管理インターフェイスポート</p> <p>データネットワークに接続されている物理ポートです。クラスタ管理者はこのポートを使用してクラスタを管理できます。</p>	
<p>クラスタ管理インターフェイスの IP アドレス</p> <p>クラスタ管理インターフェイスの一意の IPv4 アドレスまたは IPv6 アドレスです。クラスタ管理者は、このアドレスを使用して管理 SVM にアクセスし、クラスタを管理します。通常、このアドレスはデータネットワーク上になければなりません。</p> <p>この IP アドレスは、組織内で IP アドレスの割り当てを担当している管理者から取得できます。</p> <p>例： 192.0.2.66</p>	
<p>クラスタ管理インターフェイスのネットマスク（IPv4）</p> <p>クラスタ管理ネットワークの有効な IPv4 アドレスの範囲を定義するサブネットマスクです。</p> <p>例： 255.255.255.0</p>	
<p>クラスタ管理インターフェイスのネットマスクの長さ（IPv6）</p> <p>クラスタ管理インターフェイスで IPv6 アドレスを使用する場合のプレフィックス長です。クラスタ管理ネットワークの有効な IPv6 アドレスの範囲を定義するプレフィックス長を指定します。</p> <p>例： 64</p>	
<p>クラスタ管理インターフェイスのデフォルトゲートウェイ</p> <p>クラスタ管理ネットワーク上のルータの IP アドレスです。</p>	



情報の種類	値を入力します
<p>DNS ドメイン名</p> <p>ネットワークの DNS ドメインの名前です。</p> <p>ドメイン名には英数字を使用する必要があります。 複数の DNS ドメイン名を入力するには、カンマまたはスペースでそれぞれの名前を区切ります。</p>	
<p>ネームサーバの IP アドレス</p> <p>DNS ネームサーバの IP アドレスです。各アドレスをカンマまたはスペースで区切ります。</p>	

ノード情報（クラスタ内の各ノード）

情報の種類	値を入力します
<p>コントローラの物理的な場所（オプション）</p> <p>コントローラの物理的な場所の概要。このノードをクラスタ内のどこに配置するかを示す概要を使用します（例：Lab 5、Row 7、Rack B`）。</p>	
<p>ノード管理インターフェイスポート</p> <p>ノード管理ネットワークに接続されている物理ポートで、クラスタ管理者はこのポートを使用してノードを管理できます。</p>	
<p>ノード管理インターフェイスの IP アドレス</p> <p>管理ネットワーク上のノード管理インターフェイスに対する一意の IPv4 アドレスまたは IPv6 アドレスです。ノード管理インターフェイスポートをデータポートとして定義している場合、この IP アドレスはデータネットワーク上で一意の IP アドレスである必要があります。</p> <p>この IP アドレスは、組織内で IP アドレスの割り当てを担当している管理者から取得できます。</p> <p>例：192.0.2.66</p>	

情報の種類	値を入力します
<p>ノード管理インターフェイスのネットマスク（IPv4）</p> <p>ノード管理ネットワークの有効な IP アドレスの範囲を定義するサブネットマスクです。</p> <p>ノード管理インターフェイスポートをデータポートとして定義している場合、ネットマスクはそのデータネットワークのサブネットマスクである必要があります。</p> <p>例：255.255.255.0</p>	
<p>ノード管理インターフェイスのネットマスクの長さ（IPv6）</p> <p>ノード管理インターフェイスで IPv6 アドレスを使用する場合のプレフィックス長です。ノード管理ネットワークの有効な IPv6 アドレスの範囲を定義するプレフィックス長を指定します。</p> <p>例：64</p>	
<p>ノード管理インターフェイスのデフォルトゲートウェイ</p> <p>ノード管理ネットワークのルータの IP アドレスです。</p>	

#### NTP サーバの情報

情報の種類	値を入力します
<p>NTP サーバアドレス</p> <p>サイトの Network Time Protocol（NTP；ネットワークタイムプロトコル）サーバの IP アドレスです。これらのサーバは、クラスタ全体で時間を同期するために使用されます。</p>	

## System Managerを使用して新しいクラスタにONTAPを設定します

System Manager のシンプルで簡単なワークフローで、新しいクラスタをセットアップしてストレージを設定できます。

特定の MetroCluster 環境やクラスタで IPv6 ネットワークアドレスを必要とする場合など、新しいクラスタの設定に ONTAP CLI の使用が必要になることがあります。をクリックします ["こちらをご覧ください"](#) これらの要件の詳細、および ONTAP CLI を使用したクラスタのセットアップ手順については、を参照してください。

作業を開始する前に

- 使用しているプラットフォームモデルの設置とセットアップの手順に従って、新しいストレージシステムを設置し、ケーブル接続して電源をオンにしておく必要があります。  
を参照してください ["AFFおよびFASのドキュメント"](#)。
- クラスタ内通信用に、クラスタの各ノードにクラスタネットワークインターフェイスが設定されている必要があります。
- System Manager の次のサポート要件を確認しておく必要があります。
  - CLI を使用して手動でノード管理を設定すると、System Manager では IPv4 のみがサポートされ、IPv6 はサポートされません。ただし、ハードウェアのセットアップが完了したあとに、DHCP を使用して IP アドレスが自動的に割り当てられ、Windows 検出が行われたあとに System Manager を起動した場合は、System Manager で IPv6 管理アドレスを設定できます。

ONTAP 9.6 以前では、System Manager で IPv6 ネットワークを必要とする導入はサポートされません。

- MetroCluster セットアップがサポートされるのは、各サイトにノードが 2 つある MetroCluster IP 構成です。

ONTAP 9.7 以前では、System Manager で MetroCluster 構成の新しいクラスタセットアップがサポートされません。



ノード管理 IP アドレスを割り当て

#### Windows システム

Windows コンピュータは、コントローラと同じサブネットに接続する必要があります。これにより、システムにノード管理 IP アドレスが自動的に割り当てられます。

#### ステップ

1. Windows システムで、\* Network \* ドライブを開いてノードを検出します。
2. ノードをダブルクリックしてクラスタセットアップウィザードを起動します。

#### その他のシステム

クラスタ内のいずれかのノードにノード管理 IP アドレスを設定する必要があります。このノード管理 IP アドレスを使用して、クラスタセットアップウィザードを起動できます。

を参照してください ["第 1 ノードへのクラスタの作成"](#) ノード管理 IP アドレスの割り当てについては、を参照してください。

#### クラスタを初期化

クラスタを初期化するには、クラスタの管理パスワードを設定し、クラスタ管理ネットワークとノード管理ネットワークをセットアップします。DNS サーバなどのサービスを設定してホスト名を解決したり、NTP サー

バを設定して時間を同期したりすることもできます。

#### 手順

1. Web ブラウザで、設定したノード管理 IP アドレスを入力します。 "<a href="https://node-management-IP"" class="bare">https://node-management-IP"</a>

System Manager は、クラスタ内の残りのノードを自動的に検出します。

2. すべてのノードに対してクラスタ管理ネットワークとノード管理 IP アドレスを設定して、ストレージシステムを初期化します。

#### ローカル階層を作成します

ノードの使用可能なディスクまたは SSD からローカル階層を作成してください。System Manager では、ハードウェアに基づいて最適なティア構成が自動的に計算されます。

#### 手順

1. [Dashboard] をクリックし、[\* Prepare Storage] をクリックします。

ローカル階層に対するストレージの推奨事項を承認します。

#### プロトコルを設定する

クラスタで有効になっているライセンスに応じて、クラスタに必要なプロトコルを有効にすることができます。次に、ストレージへのアクセスに使用するネットワークインターフェイスを作成します。

#### 手順

1. [\* ダッシュボード \*] をクリックし、[\* プロトコルの設定 \*] をクリックします。
  - SAN アクセス用に iSCSI または FC を有効にします。
  - NAS アクセス用に NFS または SMB を有効化
  - FC-NVMe アクセスに対して NVMe を有効にします。

#### ストレージのプロビジョニング

プロトコルを設定したら、ストレージをプロビジョニングできます。表示されるオプションは、インストールされているライセンスによって異なります。

#### 手順

1. [Dashboard] をクリックし、[\* Provision Storage] をクリックします。
  - 終了: "SAN アクセスをプロビジョニング" をクリックし、\* LUN の追加 \* をクリックします。
  - 終了: "NASアクセスのプロビジョニング" をクリックし、\* ボリュームの追加 \* をクリックします。
  - 終了: "NVMe ストレージをプロビジョニングする" をクリックし、[名前空間の追加] をクリックします。

新しいクラスタのビデオで **ONTAP** を設定

# Configure ONTAP on a New Cluster

NetApp ONTAP 9 System Manager



 **NetApp**

© 2020 NetApp, Inc. All rights reserved.

## CLI を使用してクラスタをセットアップする

### 1 つ目のノードでクラスタを作成

クラスタセットアップウィザードを使用して、第 1 ノードにクラスタを作成できます。このウィザードは、ノード同士を接続するクラスタネットワークの構成、クラスタの管理 Storage Virtual Machine (SVM) の作成、機能ライセンスキーの追加、第 1 ノードのノード管理インターフェイスの作成などに役立ちます。

#### 作業を開始する前に

- 使用しているプラットフォームモデルの設置とセットアップの手順に従って、新しいストレージシステムを設置し、ケーブル接続して電源をオンにしておく必要があります。  
を参照してください ["AFFおよびFASのドキュメント"](#)。
- クラスタ内通信用に、クラスタの各ノードにクラスタネットワークインターフェイスが設定されている必要があります。
- クラスタでIPv6を設定する場合は、Base Management Controller (BMC ; ベース管理コントローラ) でIPv6を設定して、SSHを使用してシステムにアクセスできるようにする必要があります。

#### 手順

1. クラスタに追加するすべてのノードの電源をオンにします。これは、クラスタセットアップの検出を有効にするために必要です。
2. 第 1 ノードのコンソールに接続します。

ノードがブートし、クラスタセットアップウィザードがコンソール上で起動されます。

```
Welcome to the cluster setup wizard....
```

3. AutoSupport 文を承認します。

```
Type yes to confirm and continue {yes}: yes
```



AutoSupport はデフォルトでは有効になっています。

4. 画面の指示に従ってノードに IP アドレスを割り当てます。

ONTAP 9.13.1以降では、A800およびFAS8700プラットフォームの管理LIFにIPv6アドレスを割り当てることができます。9.13.1より前のONTAPリリースまたは他のプラットフォームの9.13.1以降では、管理LIFにIPv4アドレスを割り当て、クラスタのセットアップ完了後にIPv6に変換する必要があります。

5. Enter \* を押して続行します。

```
Do you want to create a new cluster or join an existing cluster?
{create, join}:
```

6. 新しいクラスタを作成します。create

7. システムのデフォルトを受け入れるか、独自の値を入力します。

8. セットアップが完了したら、ONTAP CLIコマンドを入力してクラスタにログインし、クラスタがアクティブで、第1ノードが正常であることを確認します。cluster show

次の例は、第1ノードが含まれるクラスタ（cluster1-01）が正常に機能しており、クラスタへの参加条件を満たしていることを示しています。

```
cluster1::> cluster show
Node                      Health  Eligibility
-----
cluster1-01              true    true
```

を使用すると、クラスタセットアップウィザードにアクセスして、管理SVMまたはノードSVMに対して入力した値を変更できます cluster setup コマンドを実行します

完了後

必要に応じて、["IPv4からIPv6に変換します"](#)。

残りのノードをクラスタに追加

新しいクラスタの作成が完了したら、クラスタセットアップウィザードを使用して、残りの各ノードを一度に1つずつクラスタに追加します。このウィザードを使用して、各



ノードのノード管理インターフェイスを設定できます。

クラスタ内の 2 つのノードを追加すると、ハイアベイラビリティ（HA）ペアが作成されます。4 つのノードを追加する場合は、2 つの HA ペアを作成します。HA の詳細については、[を参照してください "HA の詳細をご確認ください"](#)。

クラスタに一度に追加できるノードは 1 つだけです。クラスタへのノードの追加を開始したら、そのノードの追加処理を完了する必要があります。また、そのノードがクラスタに参加するまでは、次のノードの追加を開始することはできません。

- ベストプラクティス：24 本以下の NL-SAS ドライブで FAS2720 を使用している場合は、ストレージ構成のデフォルトがアクティブ / パッシブに設定されていることを確認し、パフォーマンスを最適化してください。  
詳細については、[を参照してください "ルート / データパーティショニングを使用しているノードでアクティブ / パッシブ構成を設定"](#)

1. クラスタに追加するノードにログインします。

コンソール上でクラスタセットアップウィザードが起動します。

```
Welcome to the cluster setup wizard....
```

2. AutoSupport 文を承認します。



AutoSupport はデフォルトでは有効になっています。

```
Type yes to confirm and continue {yes}: yes
```

3. 画面の指示に従ってノードに IP アドレスを割り当てます。

ONTAP 9.13.1以降では、A800およびFAS8700プラットフォームの管理LIFにIPv6アドレスを割り当てることができます。9.13.1より前のONTAPリリースまたは他のプラットフォームの9.13.1以降では、管理LIFにIPv4アドレスを割り当て、クラスタのセットアップ完了後にIPv6に変換する必要があります。

4. Enter \* を押して続行します。

```
Do you want to create a new cluster or join an existing cluster?
{create, join}:
```

5. クラスタにノードを追加します。join
6. 画面の指示に従ってノードをセットアップし、クラスタに追加します。
7. セットアップが完了したら、ノードが正常に機能しており、クラスタへの参加条件を満たしていることを確認します。cluster show

次の例は、2 つ目のノード（cluster1-02）をクラスタに追加したあとのクラスタを示しています。

```
cluster1::> cluster show
Node                      Health  Eligibility
-----
cluster1-01              true    true
cluster1-02              true    true
```

+

cluster setup コマンドを使用すると、クラスタセットアップウィザードにアクセスして、管理 SVM またはノード SVM に対して入力した値を変更できます。

1. 残りのノードそれぞれについて、同じ手順を繰り返します。

完了後

必要に応じて、["IPv4からIPv6に変換します"](#)。

管理LIFをIPv4からIPv6に変換します

ONTAP 9.13.1以降では、クラスタの初期セットアップ時に、A800およびFAS8700プラットフォームの管理LIFにIPv6アドレスを割り当てることができます。9.13.1より前のONTAPリリースまたは他のプラットフォームの9.13.1以降では、最初にIPv4アドレスを管理LIFに割り当ててから、クラスタのセットアップの完了後にIPv6アドレスに変換する必要があります。

手順

1. クラスタに対してIPv6を有効にします。

```
network options ipv6 modify -enable true
```

2. 権限をadvancedに設定します。

```
set priv advanced
```

3. さまざまなインターフェイスで学習されたRAプレフィックスのリストを表示します。

```
network ndp prefix show
```

4. IPv6管理LIFを作成します。

の形式を使用します prefix::id IPv6アドレスを手動で作成するには、addressパラメータを使用します。

```
network interface create -vserver <svm_name> -lif <LIF> -home-node  
<home_node> -home-port <home_port> -address <IPv6prefix::id> -netmask  
-length <netmask_length> -failover-policy <policy> -service-policy  
<service_policy> -auto-revert true
```

5. LIF が作成されたことを確認します。

```
network interface show
```

6. 設定した IP アドレスに到達できることを確認します。

```
network ping6
```

7. IPv4 LIFを「意図的に停止」とマークします。

```
network interface modify -vserver <svm_name> -lif <lif_name> -status  
-admin down
```

8. IPv4管理LIFを削除します。

```
network interface delete -vserver <svm_name> -lif <lif_name>
```

9. IPv4管理LIFが削除されたことを確認します。

```
network interface show
```

## Active IQ Config Advisor でクラスタを確認します

すべてのノードを新しいクラスタに追加したら、Active IQ Config Advisor を実行して構成を検証し、一般的な構成エラーがないかを確認する必要があります。

Config Advisor は、ラップトップ、仮想マシン、またはサーバにインストールし、Windows、Linux、および Mac の各プラットフォームで機能する Web ベースのアプリケーションです。

Config Advisor は、インストール環境を検証し、クラスタやストレージスイッチなど、構成全体の健全性をチェックするための一連のコマンドを実行します。

1. Active IQ Config Advisor をダウンロードしてインストールします。

["Active IQ Config Advisor"](#)

2. Active IQ を起動し、プロンプトが表示されたらパスフレーズを設定します。
3. 設定を確認して、[ 保存 ] をクリックします。
4. [\* 目的 ] ページで、[ ONTAP Post-Deployment Validation\* ] をクリックします。
5. ガイドモードまたはエキスパートモードのいずれかを選択します。

ガイドモードを選択すると、接続されているスイッチが自動的に検出されます。

6. クラスタのクレデンシャルを入力します。
7. (オプション) \* フォーム検証 \* をクリックします。
8. データの収集を開始するには、\* 保存して評価 \* をクリックします。
9. データ収集が完了したら、\* Job Monitor > Actions \* で、\* Data View \* アイコンをクリックして収集したデータを表示し、\* Results \* アイコンをクリックして結果を表示します。
10. Config Advisor で特定された問題を解決します。

クラスタ全体でシステム時間を同期します

時間を同期することで、クラスタ内のすべてのノードの時刻が同じになり、CIFS や Kerberos のエラーを防ぐことができます。

ネットワークタイムプロトコル (NTP) サーバをサイトにセットアップする必要があります。ONTAP 9.5 以降では、対称認証を使用するように NTP サーバをセットアップできます。  
詳細については、を参照してください "[クラスタ時間の管理 \(クラスタ管理者のみ\)](#)"。

クラスタを 1 つ以上の NTP サーバに関連付けて、クラスタ全体の時間を同期します。

1. 各ノードのシステム時間とタイムゾーンが正しく設定されていることを確認します。

クラスタ内のすべてのノードが同じタイムゾーンに設定されている必要があります。

- a. cluster date show コマンドを使用して、各ノードの現在の日付、時刻、およびタイムゾーンを表示します。

```
cluster1::> cluster date show
Node           Date           Time zone
-----
cluster1-01    01/06/2015 09:35:15 America/New_York
cluster1-02    01/06/2015 09:35:15 America/New_York
cluster1-03    01/06/2015 09:35:15 America/New_York
cluster1-04    01/06/2015 09:35:15 America/New_York
4 entries were displayed.
```

- b. すべてのノードの日付またはタイムゾーンを変更するには、cluster date modify コマンドを使用します。

次の例では、クラスタのタイムゾーンを GMT に変更します。

```
cluster1::> cluster date modify -timezone GMT
```

2. `cluster time-service ntp server create` コマンドを使用して、クラスタを NTP サーバに関連付けます。

- 対称認証を使用せずにNTPサーバを設定するには、次のコマンドを入力します。 `cluster time-service ntp server create -server server_name`
- 対称認証を使用するNTPサーバを設定するには、次のコマンドを入力します。 `cluster time-service ntp server create -server server_ip_address -key-id key_id`



対称認証は ONTAP 9.5 以降で使用できます。ONTAP 9.4 以前では使用できません。

この例では、クラスタに DNS が構成されていると想定しています。DNS を設定していない場合は、NTP サーバの IP アドレスを指定する必要があります。

```
cluster1::> cluster time-service ntp server create -server  
ntp1.example.com
```

3. クラスタがNTPサーバに関連付けられていることを確認します。 `cluster time-service ntp server show`

```
cluster1::> cluster time-service ntp server show  
Server                Version  
-----  
ntp1.example.com      auto
```

## 関連情報

### "システム管理"

**NTP** サーバの対称認証を管理するコマンドです

ONTAP 9.5 以降では、ネットワークタイムプロトコル（NTP）バージョン 3 がサポートされます。NTPv3 には SHA-1 鍵を使用した対称認証機能が含まれ、ネットワークセキュリティが強化されます。

作業	使用するコマンド
対称認証を使用せずに NTP サーバを設定する	<code>cluster time-service ntp server create -server server_name</code>
対称認証を使用して NTP サーバを設定する	<code>cluster time-service ntp server create -server server_ip_address -key-id key_id</code>

作業	使用するコマンド
<p>既存の NTP サーバで対称認証を有効にします</p> <p>必要なキー ID を追加することで、既存の NTP サーバを変更して認証を有効にすることができます</p>	<pre>cluster time-service ntp server modify -server server_name -key-id key_id</pre>
共有 NTP キーを設定する	<pre>cluster time-service ntp key create -id shared_key_id -type shared_key_type -value shared_key_value</pre> <p>• 注：共有キーは ID で参照されます。ID、そのタイプ、および値が、ノードと NTP サーバで同じである必要があります</p>
不明なキー ID で NTP サーバを設定する	<pre>cluster time-service ntp server create -server server_name -key-id key_id</pre>
NTP サーバで設定されていないキー ID でサーバを設定する。	<pre>cluster time-service ntp server create -server server_name -key-id key_id</pre> <p>• 注：* キー ID、タイプ、および値は、NTP サーバに設定されているキー ID、タイプ、および値と同じである必要があります。</p>
対称認証を無効にします	<pre>cluster time-service ntp server modify -server server_name -authentication disabled</pre>

## 追加のシステム設定作業

クラスタのセットアップが完了したら、System Manager または ONTAP コマンドラインインターフェイス（CLI）でクラスタの設定を行います。

システムの設定作業	リソース
<p>ネットワークの設定：</p> <ul style="list-style-type: none"> <li>ブロードキャストドメインを作成する</li> <li>サブネットを作成する</li> <li>IP スペースを作成する</li> </ul>	" <a href="#">ネットワークをセットアップする</a> "
サービスプロセッサをセットアップします	" <a href="#">システム管理</a> "
アグリゲートを配置	" <a href="#">ディスクおよびアグリゲートの管理</a> "



システムの設定作業	リソース
データ Storage Virtual Machine (SVM) の作成と設定	"NFS構成"  "SMBの設定"  "SAN 管理"
イベント通知を設定する	"EMSノセツテイ"

## オールフラッシュ**SAN**アレイソフトウェアの設定

### オールフラッシュ**SAN**アレイソフトウェア構成の概要

NetAppオールフラッシュSANアレイ（ASA）はONTAP 9.7以降で使用できます。ASAは、実績のあるAFF ネットアッププラットフォームを基盤としたオールフラッシュのSAN専用ソリューションです。

ASAプラットフォームでは、マルチパスに対称アクティブ/アクティブ構成を使用します。すべてのパスはアクティブ / 最適化されているため、ストレージフェイルオーバー時に、ホストはALUA によるフェイルオーバーパスの移行を待機しなくても I/O を再開できますこれにより、フェイルオーバーにかかる時間が短縮されます。

### ASA をセットアップする

オールフラッシュSANアレイ（ASA）のセットアップ手順は手順、ASA以外のシステムと同じです。

System Manager では、クラスタの初期化、ローカル階層の作成、プロトコルの設定、および ASA 用のストレージのプロビジョニングに必要な手順を実行することができます。

### ONTAPクラスタセットアップの開始。

#### ASA ホストの設定とユーティリティ

オールフラッシュSANアレイ（ASA）をセットアップするためのホスト設定は、他のすべてのSANホストと同じです。

はダウンロードできます ["NetApp Host Utilities ソフトウェア"](#) サポートサイトから特定のホストにアクセスできるようにします。

#### ASA システムの識別方法

ASA システムは、System Manager または ONTAP のコマンドラインインターフェイス（CLI）を使用して識別できます。

- \* System Managerダッシュボード\*で：\*[クラスタ]>[概要]\*をクリックし、システムノードを選択します。

パーソナリティ\*は\*オールフラッシュSANアレイ\*と表示されます。

- \* CLIから\*： `san config show` コマンドを実行します

ASAシステムについては、「オールフラッシュSANアレイ」の値がtrueになっています。

#### 関連情報

- ["テクニカルレポート4968：『NetApp All-SAN Array Data Availability and Integrity』"](#)
- ["NetAppテクニカルレポート4080：『Best Practices for Modern SAN』"](#)

#### オールフラッシュ**SAN**アレイ構成の制限とサポート

オールフラッシュSANアレイ（ASA）構成の制限とサポートは、ONTAPのバージョンによって異なります。

サポートされる構成の制限に関する最新の詳細については、を参照してください ["NetApp Hardware Universeの略"](#)。

#### クラスタあたりの**SAN**プロトコルとノード数

ASAでは、SANプロトコルとクラスタあたりのノードが次のようにサポートされます。

ONTAP で開始しています...	プロトコルのサポート	クラスタあたりの最大ノード数
9.12.1:	<ul style="list-style-type: none"><li>• NVMe（4ノードのMetroCluster IP構成とMetroCluster以外のIP構成でサポート）</li><li>• FC</li><li>• iSCSI</li></ul>	12
9.9.1	<ul style="list-style-type: none"><li>• NVMe（MetroCluster以外のIP構成でサポート）</li><li>• FC</li><li>• iSCSI</li></ul>	<ul style="list-style-type: none"><li>• 12ノード（MetroCluster以外のIP構成の場合）</li><li>• 8ノード（MetroCluster IP構成の場合）</li></ul>
9.7	<ul style="list-style-type: none"><li>• FC</li><li>• iSCSI</li></ul>	4.

#### 永続ポートのサポート

ONTAP 9.8以降では、FCプロトコルを使用するように設定されたオールフラッシュSANアレイ（ASA）で永続ポートがデフォルトで有効になります。永続ポートはFCにのみ使用でき、World Wide Port Name（WWPN；ワールドワイドポート名）で識別されるゾーンメンバーシップが必要です。

永続的ポートは、HAパートナーの対応する物理ポートにシャドウLIFを作成することで、テイクオーバーの影響を軽減します。ノードのテイクオーバー時、パートナーノードのシャドウLIFには、WWPNなどの元のLIFのIDが引き継がれます。テイクオーバーされたノードへのパスのステータスが「障害」に変更される前は、シャドウLIFがホストMPIOスタックへのアクティブ/最適パスとして表示され、I/Oがシフトされます。これにより、ストレージフェイルオーバー処理の実行中も、ホストには常にターゲットへの同じ数のパスが認識されるため、I/Oの中断が軽減されます。

永続ポートの場合、HA ペア内では、次の FCP ポート特性を同一にする必要があります。

- FCP ポート数
- FCP ポート名
- FCP ポートの速度
- FCP LIF の WWPN ベースのゾーニング

HA ペア内でこれらの特性のいずれかが同じでない場合は、次の EMS メッセージが生成されます。

```
EMS : scsiblade.lif.persistent.ports.fcp.init.error
```

永続ポートの詳細については、を参照してください ["NetAppテクニカルレポート4080：『Best Practices for Modern SAN』"](#)。

## ONTAPのアップグレード

### ONTAPのアップグレードの概要

ONTAPソフトウェアをアップグレードすると、ONTAPの新機能や強化された機能を活用して、コストの削減、重要なワークロードの高速化、セキュリティの強化、組織で利用できるデータ保護の範囲の拡大を実現できます。

ONTAPのメジャーアップグレードでは、ONTAPの番号が小さいリリースから大きいリリースに移行します。たとえば、クラスタをONTAP 9.8からONTAP 9.12.1にアップグレードします。マイナー（またはパッチ）アップグレードでは、同じ番号のリリース内で、下位のONTAPバージョンから上位のONTAPバージョンに移行します。たとえば、クラスタをONTAP 9.12.1P1から9.12.1P4にアップグレードする場合などです。

開始するには、["アップグレードを準備"](#)。Active IQデジタルアドバイザーの有効なSupportEdge契約がある場合は、["Upgrade Advisorを使用したアップグレード計画"](#)。Upgrade Advisorは、クラスタを評価し、構成に固有のアップグレードプランを作成することで、不確実性とリスクを最小限に抑えるためのインテリジェンスを提供します。

アップグレードの準備が完了したら、次を使用してアップグレードを実行することを推奨します。["System Managerからの自動無停止アップグレード \(ANDU\)"](#)。ANDUは、ONTAPの高可用性（HA）フェイルオーバーテクノロジーを活用して、アップグレード中もクラスタが中断することなくデータを提供し続けます。



ONTAP 9.12.1以降、System ManagerはBlueXPと完全に統合されています。システムにBlueXPが設定されている場合は、BlueXP作業環境を使用してアップグレードできます。

ONTAPソフトウェアのアップグレードについてサポートが必要な場合は、NetAppプロフェッショナルサービスをご利用ください。["マネージドアップグレードサービス"](#)。このサービスの利用をご希望の場合は、NetAppの営業担当者にお問い合わせいただくか、["ネットアップの営業問い合わせフォームを送信する"](#)。マネージドアップグレードサービスおよびその他のタイプのアップグレードサポートは、["SupportEdge Expertサービス"](#) 追加コストはかかりません。

**ONTAP**はいつアップグレードすればよいですか。

ONTAPソフトウェアは定期的にアップグレードする必要があります。ONTAPをアップ

グレードすると、新しい機能や拡張された機能を利用して、既知の問題に対する最新の修正を実装できます。

## ONTAPのメジャーアップグレード

ONTAPのメジャーアップグレードまたは機能リリースには通常、次のものが含まれます。

- ONTAPの新機能
- 主なインフラの変更（NetApp WAFLの運用やRAIDの運用の基本的な変更など）
- ネットアップが開発した新しいハードウェアシステムのサポート
- 新しいネットワークインターフェイスカードやホストバスアダプタなどの交換ハードウェアコンポーネントのサポート

新しいONTAPリリースには、3年間のフルサポートが適用されます。NetAppでは、一般提供（GA）後1年間最新リリースを実行し、フルサポート期間内の残りの時間を使用して新しいONTAPリリースへの移行を計画することを推奨しています。

## ONTAPパッチアップグレード

パッチアップグレードでは、重大なバグをタイムリーに修正できます。ONTAPの次のメジャーフィーチャーリリースまで待つことはできません。重要でないパッチのアップグレードは、3~6カ月ごとに適用する必要があります。重要なパッチのアップグレードは、できるだけ早く適用する必要があります。

の詳細を確認してください ["推奨される最小パッチレベル"](#) ONTAPリリースの場合。

## ONTAPのリリース日

ONTAP 9.8リリース以降、NetAppではONTAPリリースを暦年に2回提供します。計画は変更される可能性があります。新しいONTAPリリースは暦年の第2四半期と第4四半期に提供する予定です。この情報は、最新のONTAPリリースを利用するためのアップグレード期間を計画する際に使用します。

バージョン	リリース日
9.14.1	2024年1月
9.13.1.	2023年6月
9.12.1:	2023年2月
9.11.1	2022年7月
9.10.1	2022年1月
9.9.1	2021年6月

## ONTAPのサポートレベル

特定のバージョンのONTAPで利用できるサポートのレベルは、ソフトウェアのリリース時期によって異なり

ます。

サポートレベル	フルサポート			限定サポート		セルフサービスサポート		
年	1.	2.	3.	4.	5.	6.	7.	8.
オンラインマニュアルへのアクセス	はい。	はい。	はい。	はい。	はい。	はい。	はい。	はい。
テクニカルサポート	はい。	はい。	はい。	はい。	はい。			
根本原因の分析	はい。	はい。	はい。	はい。	はい。			
ソフトウェアのダウンロード	はい。	はい。	はい。	はい。	はい。			
サービスアップデート（パッチリリース[P-releases]）	はい。	はい。	はい。					
脆弱性に関するアラート	はい。	はい。	はい。					

#### 関連情報

- 詳細はこちら ["現在サポートされているONTAPリリースの新機能"](#)。
- の詳細を確認してください ["推奨される最小ONTAPリリース"](#)。
- の詳細を確認してください ["ONTAPソフトウェアバージョンのサポート"](#)。
- の詳細については、を参照してください ["ONTAPリリースモデル"](#)。

### 計画的アップグレードの前に**ONTAP**の自動アップグレード前チェックを実行

ONTAPの自動アップグレードの事前チェックを実行するために、ONTAPソフトウェアをアップグレードする必要はありません。アップグレード前チェックをONTAPの自動アップグレードプロセスとは別に実行すると、どのチェックがクラスタに対して実行されたかを確認し、実際のアップグレードを開始する前に修正する必要があるエラーや警告のリストを表示できます。たとえば、2週間後に予定されているメンテナンス時間中にONTAPソフトウェアをアップグレードするとします。スケジュールされた日付を待っている間に、自動アップグレードの事前チェックを実行し、メンテナンス時間に先立って必要な修正措置を講じることができます。これにより、アップグレードの開始後に予期しない設定エラーが発生するリスクを軽減できます。

ONTAPソフトウェアのアップグレードを開始する準備ができている場合は、この手順を実行する必要はありません。次の手順に従う必要があります。["自動アップグレードプロセス"](#)には、自動アップグレードの事前チェックの実行も含まれます。



MetroCluster構成の場合は、最初にクラスタAでこれらの手順を実行してから、クラスタBで同じ手順を実行する必要があります。

作業を開始する前に

お勧めします ["ターゲットのONTAPソフトウェアイメージのダウンロード"](#)。

の自動アップグレードの事前チェックを実行するには ["直接マルチホップアップグレード"](#) の場合、ダウンロードする必要があるのは、ターゲットのONTAPバージョンに対応したソフトウェアパッケージだけです。実際のアップグレードを開始するまで、中間バージョンのONTAPをロードする必要はありません。たとえば、9.8から9.13.1へのアップグレードの自動アップグレード前チェックを実行する場合は、ONTAP 9.13.1のソフトウェアパッケージをダウンロードする必要があります。ONTAP 9.12.1用のソフトウェアパッケージをダウンロードする必要はありません。



## 例 1. 手順

### System Manager の略

#### 1. ONTAPターゲットイメージを検証します。



MetroCluster構成をアップグレードする場合は、クラスタAを検証してから、クラスタBで検証プロセスを繰り返す必要があります。

#### a. 実行している ONTAP のバージョンに応じて、次のいずれかの手順を実行します。

実行内容	手順
ONTAP 9.8以降	[* Cluster] > [Overview] をクリックします。
ONTAP 9.5 、 9.6 、 および 9.7	[* Configuration * (設定 *) ] > [* Cluster * (クラスタ *) ] > [* Update * (アップデート *)
ONTAP 9.4 以前	[* Configuration * (構成 *) ] > [* Cluster Update (クラスタの更新) ] を

#### b. [Overview] ペインの右隅で、をクリックします .

#### c. ONTAP アップデート \* をクリックします。

#### d. [クラスタの更新]\*タブで、新しいイメージを追加するか使用可能なイメージを選択します。

状況	作業
ローカルフォルダからの新しいソフトウェアイメージの追加  お前はもう " <a href="#">イメージをダウンロードしました</a> " ローカルクライアントに送信します。	i. で、[ローカルから追加]*をクリックします。  ii. ソフトウェアイメージを保存した場所を参照し、イメージを選択して、*開く*をクリックします。
HTTPサーバまたはFTPサーバから新しいソフトウェアイメージを追加する	i. [サーバーから追加] をクリックします。  ii. [新しいソフトウェアイメージの追加]ダイアログボックスで、NetApp Support SiteからONTAPソフトウェアイメージをダウンロードしたHTTPサーバまたはFTPサーバのURLを入力します。  匿名 FTP の URL は、で指定する必要があります <a href="#">ftp://anonymous@ftpserver</a> の形式で入力し  iii. [追加 (Add) ] をクリックします。
使用可能なイメージを選択します	表示された画像のいずれかを選択します。

- e. [検証]\*をクリックして、アップグレード前の検証チェックを実行します。

検証中にエラーや警告が検出された場合は、対処方法のリストとともに表示されます。アップグレードを続行する前に、すべてのエラーを解決する必要があります。警告も解決することを推奨します。

## CLI の使用

1. ターゲットのONTAPソフトウェアイメージをクラスタパッケージリポジトリにロードします。

```
cluster image package get -url location
```

```
cluster1::> cluster image package get -url
http://www.example.com/software/9.13.1/image.tgz

Package download completed.
Package processing completed.
```

2. ソフトウェアパッケージがクラスタパッケージリポジトリにあることを確認します。

```
cluster image package show-repository
```

```
cluster1::> cluster image package show-repository
Package Version  Package Build Time
-----
9.13.1           MM/DD/YYYY 10:32:15
```

3. アップグレード前の自動チェックを実行します。

```
cluster image validate -version package_version_number -show
-validation-details true
```



を実行する場合 **"直接マルチホップアップグレード"**を使用して、ターゲットのONTAPパッケージを検証します。中間アップグレードイメージを個別に検証する必要はありません。たとえば、9.8から9.13.1にアップグレードする場合は、9.13.1パッケージを検証に使用する必要があります。9.12.1パッケージを個別に検証する必要はありません。

```
cluster1::> cluster image validate -version 9.14.1 -show-validation  
-details true
```

It can take several minutes to complete validation...  
Validation checks started successfully. Run the "cluster image  
show-update-progress" command to check validation status.

#### 4. 検証ステータスを確認します。

```
cluster image show-update-progress
```



ステータス\*が「in-progress」の場合は、完了するまで待ってからもう一度コマンドを実行します。

```
cluster1::*> cluster image show-update-progress
```

Update Phase	Status	Duration
Pre-update checks	completed	00:10:00

Details:

Pre-update Check	Status	Error-Action
AMPQ Router and Broker Config Cleanup	OK	N/A
Aggregate online status and parity check	OK	N/A
Aggregate plex resync status check	OK	N/A
Application Provisioning Cleanup	OK	N/A
Autoboot Bootargs Status	OK	N/A
Backend	OK	N/A
...		
Volume Conversion In Progress Check	OK	N/A
Volume move progress status check	OK	N/A
Volume online status check	OK	N/A
iSCSI target portal groups status check	OK	N/A
Overall Status	Warning	Warning

75 entries were displayed.

アップグレードの完全な自動事前チェックのリストが、アップグレードプロセスの開始前に対処する必要があるエラーや警告とともに表示されます。



```
cluster1::*> cluster image validate -version 9.14.1 -show-validation
-details true
```

It can take several minutes to complete validation...

WARNING: There are additional manual upgrade validation checks that must be performed after these automated validation checks have completed successfully.

Refer to the Upgrade Advisor Plan or the "What should I verify before I upgrade with or without Upgrade Advisor" section in the "Upgrade ONTAP" documentation for the remaining manual validation checks that need to be performed before update.

Upgrade ONTAP documentation available at: <https://docs.netapp.com/us-en/ontap/upgrade/index.html>

The list of checks are available at: [https://docs.netapp.com/us-en/ontap/upgrade/task\\_what\\_to\\_check\\_before\\_upgrade.html](https://docs.netapp.com/us-en/ontap/upgrade/task_what_to_check_before_upgrade.html)

Failing to do so can result in an update failure or an I/O disruption. Please use Interoperability Matrix Tool (IMT <http://mysupport.netapp.com/matrix>) to verify host system supportability configuration information.

Validation checks started successfully. Run the "cluster image show-update-progress" command to check validation status.

```
fas2820-2n-wic-1::*> cluster image show-update-progress
```

Update Phase	Status	Estimated Duration	Elapsed Duration
Pre-update checks	in-progress	00:10:00	00:00:42

Details:

Pre-update Check	Status	Error-Action
-----	-----	-----
-----	-----	-----

```
fas2820-2n-wic-1::*> cluster image show-update-progress
```

Update Phase	Status	Estimated Duration	Elapsed Duration
Pre-update checks	completed	00:10:00	00:01:03



## Details:

Pre-update Check	Status	Error-Action
-----	-----	-----
AMPQ Router and Broker Config Cleanup	OK	N/A
Aggregate online status and parity check	OK	N/A
Aggregate plex resync status check	OK	N/A
Application Provisioning Cleanup	OK	N/A
Autoboot Bootargs Status	OK	N/A
Backend Configuration Status	OK	N/A
Boot Menu Status	Warning	Warning: bootarg.init.bootmenu is  enabled on nodes: fas2820-wic- 1a,  fas2820-wic-1b. The boot process of  the nodes will be delayed. Action: Set the  bootarg.init.bootmenu  bootarg to false before  proceeding  with the upgrade.
Broadcast Domain availability and uniqueness for HA pair status	OK	N/A
CIFS compatibility status check	OK	N/A
CLAM quorum online status check	OK	N/A
CPU Utilization Status	OK	N/A
Capacity licenses install status check	OK	N/A
Check For SP/BMC Connectivity To Nodes	OK	N/A

Check LDAP fastbind users using unsecure connection.	OK	N/A
Check for unsecure kex algorithm configurations.	OK	N/A
Check for unsecure mac configurations.	OK	N/A
Cloud keymanager connectivity check	OK	N/A
Cluster health and eligibility status	OK	N/A
Cluster quorum status check	OK	N/A
Cluster/management switch check	OK	N/A
Compatible New Image Check	OK	N/A
Current system version check if it is susceptible to possible outage during NDU	OK	N/A
Data ONTAP Version and Previous Upgrade Status	OK	N/A
Data aggregates HA policy check	OK	N/A
Disk status check for failed, broken or non-compatibility	OK	N/A
Duplicate Initiator Check	OK	N/A
Encryption key migration status check	OK	N/A
External key-manager with legacy KMIP client check	OK	N/A
External keymanager key server status check	OK	N/A
Fabricpool Object Store Availability	OK	N/A
High Availability	OK	N/A

configuration		
status check		
Infinite Volume	OK	N/A
availability check		
LIF failover	OK	N/A
capability status		
check		
LIF health check	OK	N/A
LIF load balancing	OK	N/A
status check		
LIFs is on home	OK	N/A
node status		
Logically over	OK	N/A
allocated DP		
volumes check		
MetroCluster	OK	N/A
configuration		
status check for		
compatibility		
Minimum number of	OK	N/A
aggregate disks		
check		
NAE Aggregate and	OK	N/A
NVE Volume		
Encryption Check		
NDMP sessions check	OK	N/A
NFS mounts status	Warning	Warning: This cluster is serving
NFS		
check		clients. If NFS soft mounts are
used,		there is a possibility of
frequent		NFS timeouts and race conditions
that		can lead to data corruption
during		the upgrade.
		Action: Use NFS hard mounts, if
		possible. To list Vservers
running		NFS, run the following command:
		vserver nfs show
Name Service	OK	N/A
Configuration DNS		
Check		
Name Service	OK	N/A

## Configuration LDAP

### Check

Node to SP/BMC connectivity check	OK	N/A
OKM/KMIP enabled systems - Missing keys check	OK	N/A
ONTAP API to REST transition warning data last 30 days approaching automation REST	Warning	Warning: NetApp ONTAP API has been used on this cluster for ONTAP storage management within the last 30 days. NetApp ONTAP API is approaching end of availability. Action: Transition your tools from ONTAP API to ONTAP API. For more details, refer to CPC-00410 - End of availability: ONTAPI
<a href="https://mysupport.netapp.com/info/communications/ECMLP2880232.html">https://mysupport.netapp.com/info/communications/ECMLP2880232.html</a>		
ONTAP Image Capability Status	OK	N/A
OpenSSL 3.0.x upgrade validation check	OK	N/A
Openssh 7.2 upgrade validation check	OK	N/A
Platform Health Monitor check	OK	N/A
Pre-Update Configuration Verification	OK	N/A
RDB Replica Health Check	OK	N/A
Replicated database schema consistency check	OK	N/A
Running Jobs Status	OK	N/A
SAN LIF association status check	OK	N/A

SAN compatibility for manual configurability check	OK	N/A
SAN kernel agent status check	OK	N/A
Secure Purge operation Check	OK	N/A
Shelves and Sensors check	OK	N/A
SnapLock Version Check	OK	N/A
SnapMirror Synchronous relationship status check	OK	N/A
SnapMirror compatibility status check	OK	N/A
Supported platform check	OK	N/A
Target ONTAP release support for FiberBridge 6500N check	OK	N/A
Upgrade Version Compatibility Status	OK	N/A
Verify all bgp peer-groups are in the up state	OK	N/A
Verify if a cluster management LIF exists	OK	N/A
Verify that e0M is home to no LIFs with high speed services.	OK	N/A
Volume Conversion In Progress Check	OK	N/A
Volume move progress status check	OK	N/A
Volume online status check	OK	N/A
iSCSI target portal groups status check	OK	N/A

Overall Status      Warning      Warning  
75 entries were displayed.

## ONTAPのアップグレードを準備する

### ONTAPソフトウェアのアップグレードを準備する

ONTAPソフトウェアのアップグレードを適切に準備することで、アップグレードプロセスを開始する前に、アップグレードの潜在的なリスクや障害を特定して軽減することができます。アップグレードの準備中に、アップグレード前に考慮する必要がある特別な考慮事項を特定することもできます。たとえば、クラスタでSSL FIPSモードが有効になっていて、管理者アカウントで認証にSSH公開鍵を使用している場合は、ホストキーのアルゴリズムがターゲットのONTAPリリースでサポートされていることを確認する必要があります。

アップグレードの準備として、次の作業を実行する必要があります。

1. ["アップグレード計画を作成"](#)。

の有効なSupportEdge契約がある場合 ["Active IQ Digital Advisor"](#)で、Upgrade Advisorを使用してアップグレードを計画します。Active IQデジタルアドバイザーにアクセスできない場合は、独自のアップグレードプランを作成してください。

2. ["ターゲットのONTAPリリースを選択"](#)。

3. を確認します ["ONTAP リリースノート"](#) ターゲットリリース用。

「アップグレードに関する注意事項」セクションでは、新しいリリースにアップグレードする前に把握しておく必要がある潜在的な問題について説明します。「新機能」および「既知の問題と制限」セクションでは、新しいリリースへのアップグレード後の新しいシステム動作について説明します。

4. ["ハードウェア構成に対するONTAPのサポートの確認"](#)。

ハードウェアプラットフォーム、クラスタ管理スイッチ、およびMetroCluster IPスイッチがターゲットリリースをサポートしている必要があります。クラスタがSAN用に構成されている場合は、SAN構成が完全にサポートされている必要があります。

5. ["Active IQ Config Advisorを使用して、一般的な構成エラーがないことを確認します。"](#)

6. サポートされているONTAPの確認 ["アップグレードパス"](#) 直接アップグレードが可能かどうか、またはアップグレードを段階的に完了する必要があるかどうかを判断するため。

7. ["LIFフェイルオーバーの設定を確認する"](#)。

アップグレードを実行する前に、クラスタのフェイルオーバーポリシーとフェイルオーバーグループが正しく設定されていることを確認する必要があります。

8. ["SVMルーティング設定の確認"](#)。

9. ["特別な考慮事項の確認"](#) をクリックします。



クラスタに特定の構成がある場合は、ONTAPソフトウェアのアップグレードを開始する前に特定の操作を実行する必要があります。

#### 10. "SPまたはBMCをリブートする"。

### ONTAPアップグレード計画を作成

アップグレードプランを作成することを推奨します。アクティブながある場合 "SupportEdge サービス" の契約 "Active IQ Digital Advisor"を使用すると、Upgrade Advisorを使用してアップグレードプランを生成できます。それ以外の場合は、独自の計画を作成する必要があります。

Upgrade Advisor を使用してアップグレードを計画します

Active IQ Digital Advisor の Upgrade Advisor サービスは、アップグレードの計画を支援し、不確実性とリスクを最小限に抑えるインテリジェンスを提供します。

Active IQ では、ONTAP を新しいバージョンにアップグレードすることで解決可能な問題が環境内で特定されています。Upgrade Advisor サービスを使用すると、アップグレードを正常に実行するための計画に役立ち、アップグレード後の ONTAP バージョンで発生する可能性がある問題のレポートも表示されます。

#### 手順

1. "Active IQ を起動します"
2. Active IQの場合 "クラスタに関連するリスクを表示して手動で対処"。

ONTAPアップグレードを実行する前に、\* SW Config Change 、 HW Config Change 、 HW Replacement \*の各カテゴリに含まれるリスクを解決する必要があります。

3. 推奨されるアップグレードパスとを確認します "アップグレードプランを生成"。

ONTAPのアップグレードにはどのくらいの時間がかかりますか。

ONTAPアップグレードの準備手順の完了に30分以上、各HAペアのアップグレードに60分、アップグレード後の手順の完了に30分以上かかるように計画してください。



NetApp Encryption を外部キー管理サーバと Key Management Interoperability Protocol ( KMIP ) とともに使用している場合は、各 HA ペアのアップグレードに 1 時間以上かかることを確認してください。

これらのアップグレード期間のガイドラインは、一般的な構成とワークロードに基づいています。これらのガイドラインを使用して、ご使用の環境の無停止アップグレードの実行に必要な時間を見積もることができます。アップグレードプロセスの実際の期間は、環境やノード数によって異なります。

アップグレードの対象となるONTAPリリースを選択

Upgrade Advisorを使用してクラスタのアップグレード計画を生成する場合、アップグレードに推奨されるターゲットONTAPリリースが含まれます。Upgrade Advisorが提供する推奨事項は、現在の構成と現在のONTAPバージョンに基づいています。

アップグレードの計画にUpgrade Advisorを使用しない場合は、NetAppの推奨事項に基づいてアップグレード

対象のONTAPリリースを選択するか、またはパフォーマンスのニーズを満たす最小リリースを選択する必要があります。

- 利用可能な最新リリースへのアップグレード（推奨）

NetAppでは、ONTAPソフトウェアを最新の番号付きONTAPリリースの最新パッチバージョンにアップグレードすることを推奨しています。 クラスタ内のストレージシステムで最新の番号のリリースがサポートされていないために最新の番号のリリースがサポートされていない場合は、サポートされる最新の番号のリリースにアップグレードする必要があります。

- 推奨される最小リリース

アップグレードをクラスタに推奨される最小リリースに制限する場合は、を参照してください。 ["推奨される最小ONTAPリリース"](#) ONTAPのバージョンを確認するには、にアップグレードする必要があります。

## ハードウェア構成に対するONTAPのサポートの確認

ONTAPをアップグレードする前に、ハードウェア構成がターゲットのONTAPリリースに対応していることを確認する必要があります。

### すべての構成

使用 ["NetApp Hardware Universe の略"](#) をクリックして、ハードウェアプラットフォームおよびクラスタスイッチと管理スイッチがターゲットのONTAPリリースでサポートされていることを確認します。 クラスタスイッチと管理スイッチには、クラスタネットワークスイッチ（NX-OS）、管理ネットワークスイッチ（IOS）、およびリファレンス構成ファイル（RCF）があります。 クラスタスイッチと管理スイッチがサポート対象であるにもかかわらず、ターゲットのONTAPリリースに必要な最小限のソフトウェアバージョンを実行していない場合は、スイッチをサポート対象のソフトウェアバージョンにアップグレードします。

- ["ネットアップのダウンロード：Broadcomクラスタスイッチ"](#)
- ["ネットアップのダウンロード：Ciscoイーサネットスイッチ"](#)
- ["ネットアップのダウンロード：ネットアップクラスタスイッチ"](#)



スイッチのアップグレードが必要な場合はNetApp、最初にONTAPソフトウェアのアップグレードを完了してから、スイッチのソフトウェアアップグレードを実行することを推奨します。

### MetroCluster 構成

ONTAPをアップグレードする前に、MetroCluster構成を使用している場合は、["NetApp Interoperability Matrix Tool で確認できます"](#) をクリックして、MetroCluster IPスイッチがターゲットのONTAPリリースでサポートされていることを確認します。

### SAN 構成

クラスタがSAN用に構成されている場合は、ONTAPをアップグレードする前に、["NetApp Interoperability Matrix Tool で確認できます"](#) をクリックして、SAN構成が完全にサポートされていることを確認します。

ターゲットの ONTAP ソフトウェアバージョン、ホスト OS およびパッチ、必須の Host Utilities ソフトウェア、マルチパスソフトウェア、アダプタドライバおよびファームウェアなど、すべての SAN コンポーネントがサポートされている必要があります。

## Active IQ Config Advisorによる構成エラーの特定

ONTAPをアップグレードする前に、Active IQ Config Advisorツールを使用して一般的な構成エラーがないかどうかを確認できます。

Active IQ Config Advisorは、NetAppシステム向けの構成検証ツールです。セキュアなサイトにもセキュアでないサイトにも導入して、データ収集とシステム分析を行うことができます。



Active IQ Config Advisor のサポートには制限があり、オンラインでしか使用できません。

### 手順

1. にログインします ["NetApp Support Site"](#)をクリックし、\* tools > Tools \*をクリックします。
2. Active IQ Config Advisor \*]で、をクリックします ["アプリをダウンロードします"](#)。
3. Active IQ Config Advisorをダウンロード、インストール、実行します。
4. Active IQ Config Advisorを実行したら、ツールの出力を確認し、ツールで検出された問題に対処するための推奨事項に従ってください。

### サポートされるONTAPのアップグレードパス

アップグレード可能なONTAPのバージョンは、ハードウェアプラットフォーム、およびクラスタのノードで現在実行されているONTAPのバージョンによって異なります。

ハードウェアプラットフォームがターゲットアップグレードリリースでサポートされていることを確認するには、を参照してください。 ["NetApp Hardware Universe の略"](#)。 を使用します ["NetApp Interoperability Matrix Tool で確認できます"](#) 終了: ["構成のサポートの確認"](#)。

現在の **ONTAP** バージョンを確認するには、次の手順を実行

- System Manager で、\* Cluster > Overview \* をクリックします。
- コマンドラインインターフェイス (CLI) から、を使用します `cluster image show` コマンドを実行します[+]  
を使用することもできます `system node image show` コマンドをadvanced権限レベルで実行して詳細を表示します。

### アップグレードパスの種類

自動無停止アップグレード (ANDU) は可能なかぎり推奨されます。現在のリリースとターゲットリリースに応じて、アップグレードパスは\* direct、direct multi-hop、または multi-stage \*になります。

- ダイレクト+  
1つのソフトウェアイメージを使用して、隣接する次のONTAPリリースファミリーにいつでも直接アップグレードできます。ほとんどのリリースでは、ソフトウェアイメージをインストールして、実行中のリリースよりも2つ高いリリースに直接アップグレードすることもできます。

たとえば、9.8から9.9.1へ、または9.8から9.10.1への直接更新パスを使用できます。

注: ONTAP 9.11.1以降では、ソフトウェアイメージは、実行中のリリースより3つ以上新しいリリースに直接アップグレードできます。たとえば、9.8から9.12.1への直接アップグレードパスを使用できます。

all\_direct\_upgradeパスのサポート ["バージョンガコンザイノクラスタ"](#)。

- **ダイレクトマルチホップ+**  
一部の自動無停止アップグレード（ANDU）から隣接しないリリースへのアップグレードでは、中間リリースのソフトウェアイメージとターゲットリリースのソフトウェアイメージをインストールする必要があります。自動アップグレードプロセスでは、バックグラウンドの中間イメージを使用してターゲットリリースへの更新を完了します。

たとえば、クラスタで 9.3 を実行している場合に 9.7 にアップグレードするには、9.5 と 9.7 の両方の ONTAP インストールパッケージをロードし、ANDU を 9.7 に開始します。ONTAP は、最初にクラスタを 9.5 に、次に 9.7 に自動的にアップグレードします。テイクオーバー / ギブバック処理や関連するリポートが複数回行われることを想定してください。

- **マルチステージ+**  
隣接していないターゲットリリースで直接または直接のマルチホップパスを使用できない場合は、最初にサポートされている中間リリースにアップグレードしてから、ターゲットリリースにアップグレードする必要があります。

たとえば、現在 9.6 を実行している場合に 9.11.1 にアップグレードするには、まず 9.6 から 9.8 に、次に 9.8 から 9.11.1 に、マルチステージアップグレードを完了する必要があります。以前のリリースからのアップグレードでは、いくつかの中間アップグレードの段階が 3 つ以上必要になる場合があります。

\*注：\*マルチステージ・アップグレードを開始する前に、ターゲット・リリースがハードウェア・プラットフォームでサポートされていることを確認してください。

メジャーアップグレードを開始する前に、まずクラスタで実行されている ONTAP の最新のパッチリリースにアップグレードすることを推奨します。これにより、アップグレード前に現在のバージョンの ONTAP の問題がすべて解決されます。

たとえば、ONTAP 9.3P9 を実行しているシステムを 9.11.1 にアップグレードする場合は、まず最新の 9.3 パッチリリースにアップグレードしてから、9.3 から 9.11.1 へのアップグレードパスを実行する必要があります。

詳細はこちら ["NetApp Support Site で推奨される ONTAP の最小リリース数"](#)。

サポートされているアップグレードパス

ONTAP ソフトウェアの自動アップグレードと手動アップグレードでは、次のアップグレードパスがサポートされます。これらのアップグレードパスは、オンプレミスの ONTAP と ONTAP Select に適用されます。異なるものがあります ["サポートされる Cloud Volumes ONTAP のアップグレードパス"](#)。



バージョンが混在した **ONTAP** クラスタの場合：all\_direct\_and\_direct のマルチホップアップグレードパスには、バージョンが混在したクラスタと互換性のある ONTAP バージョンが含まれます。\_multi-stage\_upgrades に含まれる ONTAP バージョンは、バージョンが混在したクラスタには対応していません。たとえば、9.8 から 9.12.1 へのアップグレードは \_direct\_upgrade です。9.8 と 9.12.1 を実行しているノードで構成されるクラスタは、バージョンの混在クラスタとしてサポートされます。9.8 から 9.13.1 へのアップグレードは、\_multi-stage\_upgrade です。9.8 と 9.13.1 を実行しているノードを含むクラスタは、サポートされているバージョンの混在クラスタではありません。

## ONTAP 9.10.1以降

ONTAP 9.10.1以降からの自動アップグレードと手動アップグレードは、同じアップグレードパスに従います。

現在の <b>ONTAP</b> リリース	ターゲットとなる <b>ONTAP</b> リリースは ...	自動アップグレードパスまたは手動アップグレードパス
9.13.1.	9.14.1	直接
9.12.1:	9.14.1	直接
	9.13.1.	直接
9.11.1	9.14.1	直接
	9.13.1.	直接
	9.12.1:	直接
9.10.1	9.14.1	直接
	9.13.1.	直接
	9.12.1:	直接
	9.11.1	直接

### ONTAP 9.9.1以降

ONTAP 9.9.1からの自動アップグレードと手動アップグレードは、同じアップグレードパスに従います。

現在の <b>ONTAP</b> リリース	ターゲットとなる <b>ONTAP</b> リリースは ...	自動アップグレードパスまたは手動アップグレードパス
9.9.1	9.14.1	マルチステージ -9.9.1 → 9.13.1 -9.13.1 → 9.14.1
	9.13.1.	直接
	9.12.1:	直接
	9.11.1	直接
	9.10.1	直接

### ONTAP 9.8以降

ONTAP 9.8からの自動アップグレードと手動アップグレードは、同じアップグレードパスに従います。



次のいずれかのプラットフォームでMetroCluster IP構成を9.8から9.10.1以降にアップグレードする場合は、9.10.1以降にアップグレードする前に9.9.1にアップグレードする必要があります。

- FAS2750
- FAS500f
- AFF A220の略
- AFF A250

これらのプラットフォームのMetroCluster IP構成のクラスタは、9.8から9.10.1以降に直接アップグレードできません。上記の直接アップグレードパスは、他のすべてのプラットフォームで使用できます。

現在の <b>ONTAP</b> リリース	ターゲットとなる <b>ONTAP</b> リリースは ...	自動アップグレードまたは手動アップグレードパスは次のとおりです。
9.8	9.14.1	マルチステージ -9.8 → 9.12.1 -9.12.1 → 9.14.1
9.13.1.	マルチステージ -9.8 → 9.12.1 -9.12.1 → 9.13.1	9.12.1:
直接	9.11.1	直接
9.10.1	直接	9.9.1

## ONTAP 9.7以降

ONTAP 9.7からのアップグレードパスは、自動アップグレードと手動アップグレードのどちらを実行するかによって異なる場合があります。



## 自動パス

現在の <b>ONTAP</b> リリース	ターゲットとなる <b>ONTAP</b> リリースは ...	自動アップグレードパスは...
9.7	9.14.1	マルチステージ -9.7 → 9.8 -9.8 → 9.12.1 -9.12.1 → 9.14.1
	9.13.1.	マルチステージ -9.7 → 9.9.1 -9.9.1 → 9.13.1
	9.12.1:	マルチステージ -9.7 → 9.8 -9.8 → 9.12.1
	9.11.1	ダイレクトマルチホップ (9.8および9.11.1のイメージが必要)
	9.10.1	ダイレクトマルチホップ (9.8および9.10.1P1以降のPリリースのイメージが必要)
	9.9.1	直接
	9.8	直接

## シユトウハス

現在の <b>ONTAP</b> リリース	ターゲットとなる <b>ONTAP</b> リリースは ...	手動アップグレードパス
9.7	9.14.1	マルチステージ -9.7 → 9.8 -9.8 → 9.12.1 -9.12.1 → 9.14.1
	9.13.1.	マルチステージ -9.7 → 9.9.1 -9.9.1 → 9.13.1
	9.12.1:	マルチステージ -9.7 → 9.8 -9.8 → 9.12.1
	9.11.1	マルチステージ -9.7 → 9.8 -9.8 → 9.11.1
	9.10.1	マルチステージ -9.7 → 9.8 -9.8 → 9.10.1
	9.9.1	直接
	9.8	直接

## **ONTAP 9.6以降**

ONTAP 9.6からのアップグレードパスは、自動アップグレードと手動アップグレードのどちらを実行するかによって異なる場合があります。

## 自動パス

現在の <b>ONTAP</b> リリース	ターゲットとなる <b>ONTAP</b> リリースは ...	自動アップグレードパスは...
9.6	9.14.1	マルチステージ -9.6 → 9.8 -9.8 → 9.12.1 -9.12.1 → 9.14.1
	9.13.1.	マルチステージ -9.6 → 9.8 -9.8 → 9.12.1 -9.12.1 → 9.13.1
	9.12.1:	マルチステージ - 9.6 → 9.8 -9.8 → 9.12.1
	9.11.1	マルチステージ - 9.6 → 9.8 -9.8 → 9.11.1
	9.10.1	ダイレクトマルチホップ (9.8および9.10.1P1以降のPリリースのイメージが必要)
	9.9.1	マルチステージ - 9.6 → 9.8 -9.8 → 9.9.1
	9.8	直接
	9.7	直接

## シユトウハス

現在の <b>ONTAP</b> リリース	ターゲットとなる <b>ONTAP</b> リリースは ...	手動アップグレードパス
9.6	9.14.1	マルチステージ - 9.6 → 9.8 -9.8 → 9.12.1 -9.12.1 → 9.14.1
	9.13.1.	マルチステージ - 9.6 → 9.8 -9.8 → 9.12.1 -9.12.1 → 9.13.1
	9.12.1:	マルチステージ - 9.6 → 9.8 -9.8 → 9.12.1
	9.11.1	マルチステージ - 9.6 → 9.8 -9.8 → 9.11.1
	9.10.1	マルチステージ - 9.6 → 9.8 -9.8 → 9.10.1
	9.9.1	マルチステージ - 9.6 → 9.8 -9.8 → 9.9.1
	9.8	直接
	9.7	直接

## ONTAP 9.5以降

ONTAP 9.5からのアップグレードパスは、自動アップグレードと手動アップグレードのどちらを実行するかによって異なる場合があります。

## 自動パス

現在の <b>ONTAP</b> リリース	ターゲットとなる <b>ONTAP</b> リリースは ...	自動アップグレードパスは...
9.5	9.14.1	マルチステージ -9.5 → 9.9.1 (ダイレクトマルチホップ、9.7および9.9.1のイメージが必要) - 9.9.1 → 9.13.1 -9.13.1 → 9.14.1
	9.13.1.	マルチステージ -9.5 → 9.9.1 (ダイレクトマルチホップ、9.7および9.9.1のイメージが必要) - 9.9.1 → 9.13.1
	9.12.1:	マルチステージ -9.5 → 9.9.1 (ダイレクトマルチホップ、9.7および9.9.1のイメージが必要) -9.9.1 → 9.12.1
	9.11.1	マルチステージ -9.5 → 9.9.1 (ダイレクトマルチホップ、9.7および9.9.1のイメージが必要) -9.9.1 → 9.11.1
	9.10.1	マルチステージ -9.5 → 9.9.1 (ダイレクトマルチホップ、9.7および9.9.1のイメージが必要) -9.9.1 → 9.10.1
	9.9.1	ダイレクトマルチホップ (9.7および9.9.1のイメージが必要)
	9.8	マルチステージ -9.5 → 9.7 -9.7 → 9.8
	9.7	直接
	9.6	直接

## シュドゥアップグレードパス

現在の <b>ONTAP</b> リリース	ターゲットとなる <b>ONTAP</b> リリースは ...	手動アップグレードパス
9.5	9.14.1	マルチステージ -9.5 → 9.7 - 9.7 → 9.9.1 -9.9.1 → 9.12.1 -9.12.1 → 9.14.1
	9.13.1.	マルチステージ -9.5 → 9.7 - 9.7 → 9.9.1 -9.9.1 → 9.12.1 -9.12.1 → 9.13.1
	9.12.1:	マルチステージ -9.5 → 9.7 - 9.7 → 9.9.1 -9.9.1 → 9.12.1
	9.11.1	マルチステージ -9.5 → 9.7 - 9.7 → 9.9.1 -9.9.1 → 9.11.1
	9.10.1	マルチステージ -9.5 → 9.7 - 9.7 → 9.9.1 -9.9.1 → 9.10.1
	9.9.1	マルチステージ -9.5 → 9.7 - 9.7 → 9.9.1
	9.8	マルチステージ -9.5 → 9.7 -9.7 → 9.8
	9.7	直接
	9.6	直接

#### **ONTAP 9.4-9.0以降**

ONTAP 9.4、9.3、9.2、9.1、9.0からのアップグレードパスは、自動アップグレードと手動アップグレードのどちらを実行するかによって異なる場合があります。



現在の <b>ONTAP</b> リリース	ターゲットとなる <b>ONTAP</b> リリースは ...	自動アップグレードパスは...
9.4	9.14.1	マルチステージ -9.4 → 9.5 -9.5 → 9.9.1 (ダイレクトマルチホップ、9.7および9.9.1のイメージが必要) - 9.9.1 → 9.13.1 -9.13.1 → 9.14.1
	9.13.1.	マルチステージ -9.4 → 9.5 -9.5 → 9.9.1 (ダイレクトマルチホップ、9.7および9.9.1のイメージが必要) - 9.9.1 → 9.13.1
	9.12.1:	マルチステージ -9.4 → 9.5 -9.5 → 9.9.1 (ダイレクトマルチホップ、9.7および9.9.1のイメージが必要) -9.9.1 → 9.12.1
	9.11.1	マルチステージ -9.4 → 9.5 -9.5 → 9.9.1 (ダイレクトマルチホップ、9.7および9.9.1のイメージが必要) -9.9.1 → 9.11.1
	9.10.1	マルチステージ -9.4 → 9.5 -9.5 → 9.9.1 (ダイレクトマルチホップ、9.7および9.9.1のイメージが必要) -9.9.1 → 9.10.1
	9.9.1	マルチステージ -9.4 → 9.5 -9.5 → 9.9.1 (ダイレクトマルチホップ、9.7および9.9.1のイメージが必要)
	9.8	マルチステージ -9.4 → 9.5 -9.5 → 9.8 (ダイレクトマルチホップ、9.7および9.8のイメージが必要)
	9.7	マルチステージ -9.4 → 9.5 -9.5 → 9.7
	9.6	マルチステージ -9.4 → 9.5 -9.5 → 9.6
	9.5	直接

現在の <b>ONTAP</b> リリース	ターゲットとなる <b>ONTAP</b> リリースは ...	自動アップグレードパスは...
9.3	9.14.1	マルチステージ -9.3 → 9.7 (直接マルチホップ、9.5および9.7のイメージが必要) - 9.7 → 9.9.1 - 9.9.1 → 9.13.1 -9.13.1 → 9.14.1
	9.13.1.	マルチステージ -9.3 → 9.7 (直接マルチホップ、9.5および9.7のイメージが必要) - 9.7 → 9.9.1 - 9.9.1 → 9.13.1
	9.12.1:	マルチステージ -9.3 → 9.7 (直接マルチホップ、9.5および9.7のイメージが必要) - 9.7 → 9.9.1 -9.9.1 → 9.12.1
	9.11.1	マルチステージ -9.3 → 9.7 (直接マルチホップ、9.5および9.7のイメージが必要) - 9.7 → 9.9.1 -9.9.1 → 9.11.1
	9.10.1	マルチステージ -9.3 → 9.7 (直接マルチホップ、9.5および9.7のイメージが必要) -9.7 → 9.10.1 (ダイレクトマルチホップ、9.8および9.10.1のイメージが必要)
	9.9.1	マルチステージ -9.3 → 9.7 (直接マルチホップ、9.5および9.7のイメージが必要) - 9.7 → 9.9.1
	9.8	マルチステージ -9.3 → 9.7 (直接マルチホップ、9.5および9.7のイメージが必要) -9.7 → 9.8
	9.7	ダイレクトマルチホップ (9.5および9.7のイメージが必要)
	9.6	マルチステージ -9.3 → 9.5 -9.5 → 9.6
	9.5	直接
	9.4	使用できません

現在の <b>ONTAP</b> リリース	ターゲットとなる <b>ONTAP</b> リリースは ...	自動アップグレードパスは...
9.2.		

現在の <b>ONTAP</b> リリース	9.7	マルチステージ -9.2 → 9.3 自動アップグレード（直接マルチステージアップ、9.5および9.7のイメージが必要）
	9.6	マルチステージ -9.2 → 9.3 -9.3 → 9.5 -9.5 → 9.6
	9.5	マルチステージ -9.3 → 9.5 -9.5 → 9.6
	9.4	使用できません
	9.3	直接

現在の <b>ONTAP</b> リリース	ターゲットとなる <b>ONTAP</b> リリースは ...	自動アップグレードパスは...
9.1		

現在の <b>ONTAP</b> リリース	9.7	マルチステージ -9.1 → 9.3 <del>自動アップグレードマルチホップ、9.5および9.7のイメージが必要)</del>
	ターゲットとなる <b>ONTAP</b> リリースは ...	
	9.6	マルチステージ -9.1 → 9.3 -9.3 → 9.6 (ダイレクトマルチホップ、9.5および9.6のイメージが必要)
	9.5	マルチステージ -9.1 → 9.3 -9.3 → 9.5
	9.4	使用できません
	9.3	直接
	9.2.	使用できません

現在の <b>ONTAP</b> リリース	ターゲットとなる <b>ONTAP</b> リリースは ...	自動アップグレードパスは...
9.0		



現在の <b>ONTAP</b> リリース	ターゲットとなる <b>ONTAP</b> リリースは ...	-9.0 → 9.1 -9.1 → 9.3 -9.3 → 9.7（直接マルチホップ、9.5および9.7のイメージが必要） - 9.7 → 9.9.1
	9.8	マルチステージ -9.0 → 9.1 -9.1 → 9.3 -9.3 → 9.7（直接マルチホップ、9.5および9.7のイメージが必要） -9.7 → 9.8
	9.7	マルチステージ -9.0 → 9.1 -9.1 → 9.3 -9.3 → 9.7（直接マルチホップ、9.5および9.7のイメージが必要）
	9.6	マルチステージ -9.0 → 9.1 -9.1 → 9.3 -9.3 → 9.5 -9.5 → 9.6
	9.5	マルチステージ -9.0 → 9.1 -9.1 → 9.3 -9.3 → 9.5
	9.4	使用できません
	9.3	マルチステージ -9.0 → 9.1 -9.1 → 9.3
	9.2	使用できません
	9.1	直接

現在の <b>ONTAP</b> リリース	ターゲットとなる <b>ONTAP</b> リリースは ...	<b>ANDU</b> のアップグレードパス
9.4	9.14.1	マルチステージ -9.4 → 9.5 -9.5 → 9.7 - 9.7 → 9.9.1 -9.9.1 → 9.12.1 -9.12.1 → 9.14.1
	9.13.1.	マルチステージ -9.4 → 9.5 -9.5 → 9.7 - 9.7 → 9.9.1 -9.9.1 → 9.12.1 -9.12.1 → 9.13.1
	9.12.1:	マルチステージ -9.4 → 9.5 -9.5 → 9.7 - 9.7 → 9.9.1 -9.9.1 → 9.12.1
	9.11.1	マルチステージ -9.4 → 9.5 -9.5 → 9.7 - 9.7 → 9.9.1 -9.9.1 → 9.11.1
	9.10.1	マルチステージ -9.4 → 9.5 -9.5 → 9.7 - 9.7 → 9.9.1 -9.9.1 → 9.10.1
	9.9.1	マルチステージ -9.4 → 9.5 -9.5 → 9.7 - 9.7 → 9.9.1
	9.8	マルチステージ -9.4 → 9.5 -9.5 → 9.7 -9.7 → 9.8
	9.7	マルチステージ -9.4 → 9.5 -9.5 → 9.7
	9.6	マルチステージ -9.4 → 9.5 -9.5 → 9.6
	9.5	直接

現在の <b>ONTAP</b> リリース	ターゲットとなる <b>ONTAP</b> リリースは ...	<b>ANDU</b> のアップグレードパス
9.3	9.14.1	マルチステージ -9.3→9.5 -9.5→9.7 -9.7→9.9.1 -9.9.1→9.12.1 -9.12.1→9.14.1
	9.13.1.	マルチステージ -9.3→9.5 -9.5→9.7 -9.7→9.9.1 -9.9.1→9.12.1 -9.12.1→9.13.1
	9.12.1:	マルチステージ -9.3→9.5 -9.5→9.7 -9.7→9.9.1 -9.9.1→9.12.1
	9.11.1	マルチステージ -9.3→9.5 -9.5→9.7 -9.7→9.9.1 -9.9.1→9.11.1
	9.10.1	マルチステージ -9.3→9.5 -9.5→9.7 -9.7→9.9.1 -9.9.1→9.10.1
	9.9.1	マルチステージ -9.3→9.5 -9.5→9.7 -9.7→9.9.1
	9.8	マルチステージ -9.3→9.5 -9.5→9.7 -9.7→9.8
	9.7	マルチステージ -9.3→9.5 -9.5→9.7
	9.6	マルチステージ -9.3→9.5 -9.5→9.6
	9.5	直接
	9.4	使用できません

現在の <b>ONTAP</b> リリース	ターゲットとなる <b>ONTAP</b> リリースは ...	<b>ANDU</b> のアップグレードパス
9.2.		

現在の <b>ONTAP</b> リリース	9.7	マルチステージ -9.2 → 9.3 -9.3 → 9.5 -9.5 → 9.7
	ターゲットとなる <b>ONTAP</b> リリースは ...	ANDUOのアップグレードパス -9.5 → 9.7
	9.6	マルチステージ -9.2 → 9.3 -9.3 → 9.5 -9.5 → 9.6
	9.5	マルチステージ -9.2 → 9.3 -9.3 → 9.5
	9.4	使用できません
	9.3	直接

現在の <b>ONTAP</b> リリース	ターゲットとなる <b>ONTAP</b> リリースは ...	<b>ANDU</b> のアップグレードパス
9.1		

現在の <b>ONTAP</b> リリース	9.7	マルチステージ -9.1 → 9.3 -9.5 → 9.7
	ターゲットとなる <b>ONTAP</b> リリースは ...	ANDUO.5 アップグレードパス -9.5 → 9.7
	9.6	マルチステージ -9.1 → 9.3 -9.3 → 9.5 -9.5 → 9.6
	9.5	マルチステージ -9.1 → 9.3 -9.3 → 9.5
	9.4	使用できません
	9.3	直接
	9.2.	使用できません



現在の <b>ONTAP</b> リリース	ターゲットとなる <b>ONTAP</b> リリースは ...	<b>ANDU</b> のアップグレードパス
9.0		

現在の <b>ONTAP</b> リリース		-9.0 → 9.1 -9.1 → 9.3 -9.3 → 9.5
	ターゲットとなる <b>ONTAP</b> リリースは ...	<b>ANDU のアップグレードパス</b> - 9.7 → 9.9.1
	9.8	マルチステージ -9.0 → 9.1 -9.1 → 9.3 -9.3 → 9.5 -9.5 → 9.7 -9.7 → 9.8
	9.7	マルチステージ -9.0 → 9.1 -9.1 → 9.3 -9.3 → 9.5 -9.5 → 9.7
	9.6	マルチステージ -9.0 → 9.1 -9.1 → 9.3 -9.3 → 9.5 -9.5 → 9.6
	9.5	マルチステージ -9.0 → 9.1 -9.1 → 9.3 -9.3 → 9.5
	9.4	使用できません
	9.3	マルチステージ -9.0 → 9.1 -9.1 → 9.3
	9.2.	使用できません
	9.1	直接

## Data ONTAP 8

を使用して、プラットフォームでターゲットの ONTAP リリースを実行できることを確認します "[NetApp Hardware Universe の略](#)"。

注： Data ONTAP 8.3 アップグレードガイドでは、4 ノードクラスタの場合、イプシロンが設定されているノードを最後にアップグレードするように計画してください。誤って記載されています。Data ONTAP 8.2.3 以降では、これはアップグレードの要件ではなくなりました。詳細については、を参照してください "[NetApp Bugs Online のバグ ID880277](#)"。

## Data ONTAP 8.3.x 以降

ONTAP 9.1 に直接アップグレードしてから、以降のリリースにアップグレードできます。

## 8.2.x より前の Data ONTAP リリース（8.2.x を含む）からのアップ

まず Data ONTAP 8.3.x にアップグレードしてから、ONTAP 9.1 にアップグレードしてから、新しいリリースにアップグレードする必要があります。

## LIF フェイルオーバーの設定を確認する

ONTAP をアップグレードする前に、クラスタのフェイルオーバーポリシーとフェイルオーバーグループが正しく設定されていることを確認する必要があります。

アップグレードプロセスでは、LIF がアップグレード方式に基づいて移行されます。アップグレード方式によっては、LIF フェイルオーバーポリシーが使用される場合と使用されない場合があります。

クラスタにノードが 8 つ以上ある場合は、自動アップグレードがバッチ方式で実行されます。バッチアップグレード方式では、クラスタを複数のバッチに分けて、最初のバッチに含まれるノードのセットをアップグレードし、それらの high-availability (HA) パートナーをアップグレードしてから、残りのバッチについても同じ処理を実行します。ONTAP 9.7 以前では、バッチ方式を使用する場合に、アップグレードするノードの HA パートナーに LIF が移行されます。ONTAP 9.8以降では、バッチ方式を使用している場合に、LIFが他のバッチグループに移行されます。

クラスタ内のノードが 8 つ未満の場合は、ローリング方式で自動アップグレードが実行されます。ローリングアップグレード方式では、HAペアの各ノードでフェイルオーバー処理を開始し、フェイルオーバーしたノードを更新してギブバックを開始します。この処理をクラスタ内のHAペアごとに繰り返します。ローリング方式を使用する場合は、LIF フェイルオーバーポリシーの定義に従って、フェイルオーバーターゲットノードに LIF が移行されます。

### 手順

1. 各データ LIF のフェイルオーバーポリシーを表示します。

ONTAP のバージョン	使用するコマンド
9.6以降	<code>network interface show -service-policy *data* -failover</code>
9.5以前	<code>network interface show -role data -failover</code>

次の例は、2 つのデータ LIF を含む 2 ノードクラスタのデフォルトのフェイルオーバー設定を示しています。

```
cluster1::> network interface show -role data -failover
```

Vserver	Logical Interface	Home Node:Port	Failover Policy	Failover Group
vs0	lif0	node0:e0b	nextavail	system-
defined		Failover Targets: node0:e0b, node0:e0c, node0:e0d, node0:e0e, node0:e0f, node1:e0b, node1:e0c, node1:e0d, node1:e0e, node1:e0f		
vs1	lif1	node1:e0b	nextavail	system-
defined		Failover Targets: node1:e0b, node1:e0c, node1:e0d, node1:e0e, node1:e0f, node0:e0b, node0:e0c, node0:e0d, node0:e0e, node0:e0f		

「\* Failover Targets \*」フィールドには、各 LIF のフェイルオーバーターゲットが優先順位の高いものから順番に表示されます。たとえば、「lif0」がホームポート（node0のe0b）からフェイルオーバーすると、node0のポートe0cへのフェイルオーバーが最初に試行されます。lif0がe0cにフェイルオーバーできない場合は、node0のポートe0dなどへのフェイルオーバーが試行されます。

2. SAN LIF以外のいずれかのLIFでフェイルオーバーポリシーが\* disabled \*に設定されている場合は、`network interface modify` フェイルオーバーを有効にするコマンド。
3. それぞれの LIF について、LIF のホームノードのアップグレード時に稼働したままにする別のノードのデータポートが「\* Failover Targets \*」フィールドに含まれていることを確認します。

を使用できます `network interface failover-groups modify` コマンドを使用してフェイルオーバーグループにフェイルオーバーターゲットを追加します。

例

```
network interface failover-groups modify -vserver vs0 -failover-group
fg1 -targets sti8-vsim-ucs572q:e0d,sti8-vsim-ucs572r:e0d
```

関連情報

["ネットワークと LIF の管理"](#)

## SVM ルーティング設定を確認

システム停止を回避するには、ONTAPソフトウェアをアップグレードする前に、より具体的なルートでは到達できないネットワークアドレスにデフォルトのSVMルートが到達できることを確認する必要があります。SVM にはデフォルトルートを 1 つだけ設定することを推奨します。詳細については、を参照してください ["SU134：ONTAPの誤ったルーティング設定によってネットワークアクセスが中断されることがある"](#)。

SVM のルーティングテーブルは、SVM がデスティネーションとの通信に使用するネットワークパスを決めるものです。ネットワークの問題を未然に防ぐためには、ルーティングテーブルの仕組みを理解しておくことが重要です。

ルーティングルールは次のとおりです。

- ONTAP は、使用可能な最も限定的なルートでトラフィックをルーティングします。
- より限定的なルートがない場合、ONTAP は最後の手段としてデフォルトゲートウェイルート（0 ビットのネットマスク）でトラフィックをルーティングします。

デスティネーション、ネットマスク、メトリックが同じルートが複数ある場合、リブート後またはアップグレード後に同じルートが使用される保証はありません。複数のデフォルトルートを設定している場合、これは特に問題になる可能性があります。

## 特別な考慮事項

### ONTAPのアップグレード前の特別な考慮事項

一部のクラスタ構成では、ONTAPソフトウェアのアップグレードを開始する前に特定の処理を実行する必要があります。たとえば、SAN構成の場合は、アップグレードを開始する前に、各ホストに正しい数の直接パスと間接パスが設定されていることを確認する必要があります。

次の表を参照して、必要な追加手順を確認してください。

ONTAPをアップグレードする際の考慮事項	回答が * はい * の場合、次の操作を実行します ...
クラスタに複数のバージョンが混在していますか？	<a href="#">異なるバージョンが混在しているかどうかを確認</a>
MetroCluster 構成を使用していますか？	<a href="#">MetroCluster 構成の具体的なアップグレード要件を確認します</a>
SAN 構成を使用していますか。	<a href="#">SANホスト構成の確認</a>
クラスタでSnapMirror関係が定義されているか。	<a href="#">"SnapMirror関係に対するONTAPのバージョンの互換性を確認する"</a>
DPタイプのSnapMirror関係は定義されていますか。ONTAP 9.12.1以降にアップグレードしますか。	<a href="#">"既存のDPタイプの関係をXDPに変換します"</a>
外部キー管理サーバに NetApp Storage Encryption を使用しているか？	<a href="#">既存のキー管理サーバ接続を削除します</a>

<b>ONTAP</b> をアップグレードする際の考慮事項	回答が* はい* の場合、次の操作を実行します ...
SVM にネットグループをロードしたか？	ネットグループファイルが各ノードに存在することを確認します
SSLv3 を使用している LDAP クライアントがありますか？	TLS を使用するように LDAP クライアントを設定します
セッション指向プロトコルを使用しているか。	セッション指向プロトコルに関する考慮事項を確認します
SSL FIPSモードは、管理者アカウントがSSH公開鍵を使用して認証するクラスタで有効になっていますか？	SSHホストキーアルゴリズムのサポートの確認

#### バージョンが混在した**ONTAP**クラスタ

バージョンが混在したONTAPクラスタは、2つの異なるメジャーONTAPリリースを一定期間実行するノードで構成されます。たとえば、ONTAP 9.8と9.12.1を実行するノードで構成されたクラスタは、バージョンが混在したクラスタです。同様に、ノードでONTAP 9.9.1と9.13.1が実行されているクラスタは、バージョンが混在したクラスタです。NetAppでは、一定期間、特定のシナリオにおいて、バージョンの異なるONTAPクラスタが混在してサポートされます。

ONTAPクラスタに複数のバージョンが混在する一般的なシナリオを次に示します。

- ・大規模なクラスタでのONTAPソフトウェアのアップグレード
- ・クラスタに新しいノードを追加する場合は、ONTAPソフトウェアのアップグレードが必要です

AFF AシリーズおよびCシリーズ、ASA、FAS、Cシリーズシステムなど、NetAppプラットフォームシステムをサポートする環境ONTAPのバージョン情報。この情報は、9.12.0などのONTAPクラウドリリース（9.x.0）には適用されません。

#### バージョンが混在した**ONTAP**クラスタの要件

クラスタに複数のONTAPバージョンが混在する状態にする必要がある場合は、重要な要件と制限事項に注意する必要があります。

- ・1つのクラスタに同時に使用できるメジャーONTAPバージョンは2つまでです。たとえば、ONTAP 9.9.1と9.13.1はサポートされますが、ONTAP 9.9.1、9.12.1、および9.13.1はサポートされません。同じONTAPリリースのPパッチレベルまたはDパッチレベルが異なるノード（ONTAP 9.9.1P1と9.9.1P5など）を含むクラスタは、バージョンが混在したONTAPクラスタとはみなされません。
- ・クラスタに複数のバージョンが混在している間は、アップグレードプロセスやデータ移行プロセスに必要なコマンドを除き、クラスタの処理や構成を変更するコマンドは実行しないでください。たとえば、LIFの移行、ストレージの計画的フェイルオーバー処理、大規模なオブジェクトの作成や削除などのアクティビティは、アップグレードとデータ移行が完了するまで実行しないでください。
- ・クラスタが最適に動作するためには、クラスタに複数のバージョンが混在した状態になるまでの時間をできるだけ短くする必要があります。クラスタに複数のバージョンが混在した状態を維持できる最大期間は、クラスタ内の最も低いONTAPバージョンによって異なります。

バージョンが混在したクラスタで実行されている <b>ONTAP</b> の最下位バージョンが次の場合：	その後、最大でバージョンが混在した状態のままにすることができます
ONTAP 9.8以降	90日
ONTAP 9.7以前	7日

- ONTAP 9.8以降では、元のノードと新しいノードのバージョンの違いを4つ以上にはできません。たとえば、バージョンが混在したONTAPクラスタでは、ONTAP 9.8と9.12.1を実行しているノードや、ONTAP 9.9.1と9.13.1を実行しているノードを使用できます。ただし、ONTAP 9.8と9.13.1を実行するノードを含むバージョンが混在したONTAPクラスタはサポートされません。

サポートされるバージョンの混在クラスタの一覧については、を参照してください。 ["サポートされるアップグレードパス"](#)。all\_direct\_upgradeパスは、バージョンが混在したクラスタでサポートされます。

## 大規模クラスタの**ONTAP**バージョンの更新

バージョンが混在したクラスタ状態になるシナリオの1つは、複数のノードを含むクラスタのONTAPバージョンをアップグレードして、ONTAP 9の新しいバージョンで利用できる機能を利用することです。大規模なクラスタのONTAPバージョンをアップグレードする必要がある場合は、クラスタ内の各ノードをアップグレードする間、一定期間バージョンが混在したクラスタ状態になります。

### ONTAPクラスタへの新しいノードの追加

バージョンが混在したクラスタ状態になるもう1つのシナリオは、クラスタに新しいノードを追加することです。クラスタに新しいノードを追加して容量を拡張したり、コントローラを完全に交換するプロセスで新しいノードを追加したりできます。どちらの場合も、既存のコントローラから新しいシステムの新しいノードにデータを移行できるようにする必要があります。

クラスタに新しいノードを追加する予定で、それらのノードにクラスタで現在実行されているバージョンよりも新しいバージョンのONTAPが必要な場合は、新しいノードを追加する前に、クラスタ内の既存のノードでサポートされるソフトウェアのアップグレードを実行する必要があります。

既存のすべてのノードを、クラスタに追加するノードに必要な最小バージョンのONTAPにアップグレードするのが理想的です。ただし、既存のノードの一部で新しいバージョンのONTAPがサポートされていないためにこの処理ができない場合は、アップグレードプロセスの一環として一定期間、バージョンが混在した状態にする必要があります。新しいコントローラに必要な最小ONTAPバージョンをサポートしていないノードがある場合は、次の手順を実行する必要があります。

1. ["アップグレード"](#) 新しいコントローラで必要な最小ONTAPバージョンをサポートしていないノードが、新しいコントローラでサポートされる最大ONTAPバージョンまで。

たとえば、ONTAP 9.5を実行しているFAS8080で、ONTAP 9.12.1を実行している新しいCシリーズプラットフォームを追加する場合は、FAS8080をONTAP 9.8（ONTAPでサポートされる最大バージョン）にアップグレードする必要があります。

2. ["クラスタへの新しいノードの追加"](#)。
3. ["データの移行"](#) クラスタから削除するノードから新しく追加したノードに移動します。
4. ["サポート対象外のノードをクラスタから削除します"](#)。
5. ["アップグレード"](#) クラスタ内の残りのノードを新しいノードと同じバージョンに変更します。

必要に応じて、クラスタ全体（新しいノードを含む）を ["推奨される最新のパッチリリース"](#) 新しいノードで実行されているONTAPのバージョン。

データ移行の詳細については、以下を参照してください。

- ["アグリゲートを作成してボリュームを新しいノードに移動"](#)
- ["SANボリュームの移動用に新しいiSCSI接続をセットアップします"](#)
- ["暗号化を使用してボリュームを移動する"](#)

#### MetroCluster構成のONTAPのアップグレード要件

MetroCluster構成のONTAPソフトウェアをアップグレードする前に、クラスタが一定の要件を満たしている必要があります。

- 両方のクラスタで同じバージョンの ONTAP を実行する必要があります。

version コマンドを使用すると、ONTAP のバージョンを確認できます。

- ONTAPのメジャーアップグレードを実行する場合は、MetroCluster設定を通常モードにする必要があります。
- パッチONTAPアップグレードを実行する場合は、MetroCluster設定を通常モードまたはスイッチオーバーモードのいずれかにすることができます。
- 2 ノードのクラスタを除き、すべての構成で両方のクラスタを同時に無停止アップグレードできます。

2 ノードのクラスタを無停止アップグレードする場合は、クラスタのノードを 1 つずつアップグレードする必要があります。

- 両方のクラスタ内のアグリゲートの RAID ステータスが resyncing にならないようにしてください。

MetroCluster の修復中に、ミラーされたアグリゲートが再同期されます。MetroCluster 構成がこの状態になっているかどうかを確認するには、`storage aggregate plex show -in-progress true` コマンドを実行します同期しているアグリゲートがある場合は、再同期が完了するまでアップグレードを実行しないでください。

- アップグレードの実行中はネゴシエートスイッチオーバー処理が失敗します。

アップグレード処理またはリバート処理時の問題を回避するために、両方のクラスタで同じバージョンの ONTAP を実行しているとき以外は、アップグレードまたはリバート処理中に計画外のスイッチオーバーを実行しないでください。

#### MetroClusterの通常動作の設定要件

- ソース SVM LIF が稼働し、ホームノードに配置されている必要があります。

デスティネーション SVM のデータ LIF については、稼働し、ホームノードに配置されている必要はありません。

- ローカルサイトにあるすべてのアグリゲートがオンラインになっている必要があります。
- ローカルクラスタの SVM が所有するルートボリュームとデータボリュームがすべてオンラインになって



いる必要があります。

## MetroClusterスイッチオーバーの設定要件

- すべての LIF が稼働し、ホームノードに配置されている必要があります。
- DR サイトにあるルートアグリゲートを除く、すべてのアグリゲートがオンラインになっている必要があります。

DR サイトにあるルートアグリゲートは、スイッチオーバーの特定のフェーズ中はオフラインになります。

- すべてのボリュームがオンラインである必要があります。

## 関連情報

### "MetroCluster 構成のネットワークとストレージのステータスの確認"

## ONTAPアップグレード前のSANホスト構成の確認

SAN環境でONTAPをアップグレードすると、直接パスが変更されます。SANクラスタをアップグレードする前に、各ホストに正しい数の直接パスと間接パスが設定されていること、および各ホストが正しいLIFに接続されていることを確認する必要があります。

## 手順

1. 各ホストで、十分な数の直接パスと間接パスが設定されていること、および各パスがアクティブであることを確認します。

各ホストには、クラスタ内の各ノードへのパスが必要です。

2. 各ホストが各ノードの LIF に接続されていることを確認します。

アップグレード後の比較用に、イニシエータのリストを記録しておく必要があります。

用途	入力するコマンド
iSCSI	<pre>iscsi initiator show -fields igroup,initiator-name,tpgroup</pre>
FC	<pre>fcp initiator show -fields igroup,wwpn,lif</pre>

## SnapMirror

## SnapMirror 関係に対応した ONTAP バージョン

SnapMirrorデータ保護関係を作成するには、ソースボリュームとデスティネーションボ

リユームで互換性のあるONTAPバージョンが実行されている必要があります。ONTAPをアップグレードする前に、現在のONTAPバージョンがSnapMirror関係のターゲットのONTAPバージョンと互換性があることを確認する必要があります。

## ユニファイドレプリケーション関係

「xdmp」タイプの SnapMirror 関係では、オンプレミスまたは Cloud Volumes ONTAP リリースを使用します。

ONTAP 9.9.9..0以降：



- ONTAP 9.x.0リリースはクラウドのみのリリースであり、Cloud Volumes ONTAPシステムをサポートします。リリースバージョンのあとにアスタリスク（\*）が表示されている場合、クラウドのみのリリースです。
- ONTAP 9.x.1リリースは一般リリースであり、オンプレミスシステムとCloud Volumes ONTAPシステムの両方をサポートします。



双方向の互換性があります。

- ONTAP バージョン9.3以降との相互運用性\*

ONTAP バー ジョ ン...	ONTAP の以前のバージョンとの相互運用性...																	
	9.14 .1	9.14 .0 *	9.13 .1	9.13 .0 *	9.12 .1:	9.12 .0 *	9.11 .1	9.11 .0*	9.10 .1	9.10 .0 *	9.9. 1	9.9.. 0 *	9.8	9.7	9.6	9.5	9.4	9.3
9.14 .1	*はい い *	*はい い *	*はい い *	*はい い *	*はい い *	*はい い *	*はい い *	*はい い *	*はい い *	*はい い *	*はい い *	*はい い *	いい え	いい え	いい え	いい え	いい え	いい え
9.14 .0 *	*はい い *	*はい い *	*はい い *	いい え	*はい い *	いい え	*はい い *	いい え	*はい い *	いい え	*はい い *	いい え	*はい い *	いい え	いい え	いい え	いい え	いい え
9.13 .1	*はい い *	*はい い *	*はい い *	*はい い *	*はい い *	*はい い *	*はい い *	*はい い *	*はい い *	*はい い *	*はい い *	*はい い *	*はい い *	いい え	いい え	いい え	いい え	いい え
9.13 .0 *	*はい い *	いい え	*はい い *	*はい い *	*はい い *	いい え	*はい い *	いい え	*はい い *	いい え	*はい い *	いい え	*はい い *	いい え	いい え	いい え	いい え	いい え
9.12 .1:	*はい い *	*はい い *	*はい い *	*はい い *	*はい い *	*はい い *	*はい い *	*はい い *	*はい い *	*はい い *	*はい い *	*はい い *	*はい い *	*はい い *	いい え	いい え	いい え	いい え
9.12 .0 *	*はい い *	いい え	*はい い *	いい え	*はい い *	*はい い *	*はい い *	いい え	*はい い *	いい え	*はい い *	いい え	*はい い *	*はい い *	いい え	いい え	いい え	いい え
9.11 .1	*はい い *	*はい い *	*はい い *	*はい い *	*はい い *	*はい い *	*はい い *	*はい い *	*はい い *	*はい い *	*はい い *	*はい い *	*はい い *	*はい い *	*はい い *	いい え	いい え	いい え
9.11 .0*	*はい い *	いい え	*はい い *	いい え	*はい い *	いい え	*はい い *	*はい い *	*はい い *	いい え	*はい い *	いい え	*はい い *	*はい い *	*はい い *	いい え	いい え	いい え

9.10.1	*はい*	*はい*	*はい*	*はい*	*はい*	*はい*	*はい*	*はい*	*はい*	*はい*	*はい*	*はい*	*はい*	*はい*	*はい*	*はい*	*はい*	いいえ	いいえ
9.10.0*	*はい*	いいえ	*はい*	いいえ	*はい*	いいえ	*はい*	いいえ	*はい*	*はい*	*はい*	いいえ	*はい*	*はい*	*はい*	*はい*	*はい*	いいえ	いいえ
9.9.1	*はい*	*はい*	*はい*	*はい*	*はい*	*はい*	*はい*	*はい*	*はい*	*はい*	*はい*	*はい*	*はい*	*はい*	*はい*	*はい*	*はい*	いいえ	いいえ
9.9.0*	*はい*	いいえ	*はい*	いいえ	*はい*	いいえ	*はい*	いいえ	*はい*	いいえ	*はい*	*はい*	*はい*	*はい*	*はい*	*はい*	*はい*	いいえ	いいえ
9.8	いいえ	*はい*	*はい*	*はい*	*はい*	*はい*	*はい*	*はい*	*はい*	*はい*	*はい*	*はい*	*はい*	*はい*	*はい*	*はい*	*はい*	いいえ	*はい*
9.7	いいえ	いいえ	いいえ	いいえ	*はい*	*はい*	*はい*	*はい*	*はい*	*はい*	*はい*	*はい*	*はい*	*はい*	*はい*	*はい*	*はい*	いいえ	*はい*
9.6	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ	*はい*	*はい*	*はい*	*はい*	*はい*	*はい*	*はい*	*はい*	*はい*	*はい*	*はい*	いいえ	*はい*
9.5	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ	*はい*	*はい*	*はい*	*はい*	*はい*	*はい*	*はい*	*はい*	*はい*	*はい*	*はい*
9.4	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ	*はい*	*はい*	*はい*
9.3	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ	*はい*	*はい*	*はい*	*はい*	*はい*	*はい*	*はい*

## SnapMirror Synchronous 関係



ONTAP クラウドインスタンスではSnapMirror Synchronousはサポートされません。

ONTAP バージョン...	ONTAP の以前のバージョンとの相互運用性...									
	9.14.1	9.13.1.	9.12.1:	9.11.1	9.10.1	9.9.1	9.8	9.7	9.6	9.5
9.14.1	*はい*	*はい*	*はい*	*はい*	*はい*	*はい*	*はい*	いいえ	いいえ	いいえ
9.13.1.	*はい*	*はい*	*はい*	*はい*	*はい*	*はい*	*はい*	*はい*	いいえ	いいえ
9.12.1:	*はい*	*はい*	*はい*	*はい*	*はい*	*はい*	*はい*	*はい*	いいえ	いいえ
9.11.1	*はい*	*はい*	*はい*	*はい*	*はい*	*はい*	いいえ	いいえ	いいえ	いいえ
9.10.1	*はい*	*はい*	*はい*	*はい*	*はい*	*はい*	*はい*	いいえ	いいえ	いいえ
9.9.1	*はい*	*はい*	*はい*	*はい*	*はい*	*はい*	*はい*	*はい*	いいえ	いいえ
9.8	*はい*	*はい*	*はい*	いいえ	*はい*	*はい*	*はい*	*はい*	*はい*	いいえ
9.7	いいえ	*はい*	*はい*	いいえ	いいえ	*はい*	*はい*	*はい*	*はい*	*はい*
9.6	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ	*はい*	*はい*	*はい*	*はい*
9.5	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ	*はい*	*はい*	*はい*

## SnapMirror SVMディザスタリカバリ関係

- SVMディザスタリカバリのデータとSVM保護の場合：

SVMディザスタリカバリは、同じバージョンのONTAPを実行するクラスタ間でのみサポートされます。バージョンに依存しないレプリケーションは**SVM**レプリケーションではサポートされません。

- SVM移行のためのSVMディザスタリカバリの場合：

- ソース上のONTAPの以前のバージョンから、デスティネーション上のONTAPの同じバージョンまたはそれ以降のバージョンへのレプリケーションが単一方向でサポートされます。

- ターゲットクラスタのONTAPのバージョンが、次の表に示すように、オンプレミスのメジャーバージョンが2つ以上ないか、クラウドのメジャーバージョンが2つ以上ないようにする必要があります。

- 長期的なデータ保護のユースケースでは、レプリケーションはサポートされません。

リリースバージョンのあとにアスタリスク (\*) が表示されている場合、クラウドのみのリリースです。

サポートを確認するには、左側の表の列でソースバージョンを確認し、一番上の行でデスティネーションバージョンを確認します（類似バージョンの場合はDR/Migration、新しいバージョンの場合はMigrationのみ）。

ソース	デスティネーション																	
	9.3	9.4	9.5	9.6	9.7	9.8	9.9.. 0 *	9.9. 1	9.10 .0 *	9.10 .1	9.11 .0*	9.11 .1	9.12 .0 *	9.12 .1:	9.13 .0 *	9.13 .1.	9.14 .0 *	9.14 .1
9.3	DR / 移行	データ移行	データ移行	データ移行	データ移行													
9.4		DR / 移行	データ移行	データ移行	データ移行	データ移行												
9.5			DR / 移行	データ移行	データ移行	データ移行	データ移行											
9.6				DR / 移行	データ移行	データ移行	データ移行	データ移行										
9.7					DR / 移行	データ移行	データ移行	データ移行	データ移行									
9.8						DR / 移行	データ移行	データ移行	データ移行	データ移行								
9.9.. 0 *							DR / 移行	データ移行	データ移行	データ移行	データ移行							
9.9. 1								DR / 移行	データ移行	データ移行	データ移行	データ移行						

9.10 .0 *								DR / 移行	デー タ移 行	デー タ移 行	デー タ移 行	デー タ移 行					
9.10 .1								DR / 移行	デー タ移 行	デー タ移 行	デー タ移 行	デー タ移 行					
9.11 .0*									DR / 移行	デー タ移 行	デー タ移 行	デー タ移 行	デー タ移 行				
9.11 .1										DR / 移行	デー タ移 行	デー タ移 行	デー タ移 行	デー タ移 行			
9.12 .0 *											DR / 移行	デー タ移 行	デー タ移 行	デー タ移 行	デー タ移 行		
9.12 .1:												DR / 移行	デー タ移 行	デー タ移 行	デー タ移 行	デー タ移 行	デー タ移 行
9.13 .0 *													DR / 移行	デー タ移 行	デー タ移 行	デー タ移 行	デー タ移 行
9.13 .1.														DR / 移行	デー タ移 行	デー タ移 行	デー タ移 行
9.14 .0 *															DR / 移行	デー タ移 行	デー タ移 行
9.14 .1																	DR / 移行

## SnapMirrorディザスタリカバリ関係

タイプが「`D」でポリシータイプが「async」の SnapMirror 関係の場合：



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



次の表で、左側の列はソースボリュームの ONTAP のバージョン、上部の行はデスティネーションボリュームで利用できる ONTAP のバージョンを示しています。

ソース	デスティネーション											
	9.11.1	9.10.1	9.9.1	9.8	9.7	9.6	9.5	9.4	9.3	9.2.	9.1	9
9.11.1	はい。	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ
9.10.1	はい。	はい。	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ
9.9.1	はい。	はい。	はい。	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ

9.8	いいえ	はい。	はい。	はい。	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ
9.7	いいえ	いいえ	はい。	はい。	はい。	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ
9.6	いいえ	いいえ	いいえ	はい。	はい。	はい。	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ
9.5	いいえ	いいえ	いいえ	いいえ	はい。	はい。	はい。	いいえ	いいえ	いいえ	いいえ	いいえ
9.4	いいえ	いいえ	いいえ	いいえ	いいえ	はい。	はい。	はい。	いいえ	いいえ	いいえ	いいえ
9.3	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ	はい。	はい。	はい。	いいえ	いいえ	いいえ
9.2	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ	はい。	はい。	はい。	いいえ	いいえ
9.1	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ	はい。	はい。	はい。	いいえ
9	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ	はい。	はい。	はい。



双方向の互換性はありません。

既存の **DP** タイプの関係を **XDP** に変換します

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

このタスクについて

- SnapMirror では、既存の DP タイプの関係を XDP に自動的に変換しません。関係を変換するには、既存の関係を解除して削除し、新しい XDP 関係を作成して関係を再同期する必要があります。背景情報については、[を参照してください "XDP は、DP を SnapMirror のデフォルトとして置き換えます"](#)。
- 変換を計画する場合は、XDP SnapMirror 関係のバックグラウンド準備とデータウェアハウジングフェーズに時間がかかる可能性があることに注意してください。長時間にわたってステータスが「preparing」と報告されている SnapMirror 関係が表示されることは珍しくありません。



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

手順

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

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

次の例は、からの出力を示しています snapmirror show コマンドを実行します

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

```
Source Path: svm1:volA
Destination Path: svm_backup:volA_dst
Relationship Type: DP
SnapMirror Schedule: -
Tries Limit: -
Throttle (KB/sec): unlimited
Mirror State: Snapmirrored
Relationship Status: Idle
Transfer Snapshot: -
Snapshot Progress: -
Total Progress: -
Snapshot Checkpoint: -
Newest Snapshot: snapmirror.10af643c-32d1-11e3-954b-
123478563412_2147484682.2014-06-27_100026
Newest Snapshot Timestamp: 06/27 10:00:55
Exported Snapshot: snapmirror.10af643c-32d1-11e3-954b-
123478563412_2147484682.2014-06-27_100026
Exported Snapshot Timestamp: 06/27 10:00:55
Healthy: true
```



のコピーを保持しておくと便利です snapmirror show 関係設定の既存の情報を追跡するためのコマンド出力。

2. ソースボリュームとデスティネーションボリュームから、両方のボリュームで共通のSnapshotコピーを作成します。

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

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

```

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

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

```

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



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

コマンド構文全体については、を参照してください ["のマニュアルページ"](#)。



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

次の例は、ソースボリューム間の関係を休止します volA オン svm1 デスティネーションボリュームを指定します volA\_dst オン svm\_backup :

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

#### 4. 既存の DP タイプの関係を解除します。

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

コマンド構文全体については、を参照してください ["のマニュアルページ"](#)。



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

次の例は、ソースボリューム間の関係を解除します volA オン svm1 デスティネーションボリュームを指定します volA\_dst オン svm\_backup :

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

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

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

次の例は、デスティネーションボリュームでSnapshotコピーの自動削除を無効にします volA\_dst :

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

#### 6. 既存の DP タイプの関係を削除します。

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

コマンド構文全体については、を参照してください ["のマニュアルページ"](#)。



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

次の例は、ソースボリューム間の関係を削除します volA オン svm1 デスティネーションボリュームを指定します volA\_dst オン svm\_backup :

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

7. ソースで元のSVMディザスタリカバリ関係を解放します。

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

次の例は、SVMディザスタリカバリ関係をリリースします。

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

8. で保持した出力を使用できます snapmirror show 次のコマンドを使用して、新しいXDPタイプの関係を作成します。

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

新しい関係では、同じソースボリュームとデスティネーションボリュームを使用する必要があります。コマンド構文全体については、マニュアルページを参照してください。



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

次の例は、ソースボリューム間のSnapMirrorディザスタリカバリ関係を作成します。 volA オン svm1 デスティネーションボリュームを指定します volA\_dst オン svm\_backup デフォルトを使用します MirrorAllSnapshots ポリシー :

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

## 9. ソースボリュームとデスティネーションボリュームを再同期します。

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

再同期時間を短縮するには、を使用します `-quick-resync` オプションですが、Storage Efficiencyによる削減効果は失われる可能性がある点に注意してください。コマンド構文全体については、マニュアルページを参照してください。"[snapmirror resyncコマンドの実行](#)"。



このコマンドはデスティネーション SVM またはデスティネーションクラスタから実行する必要があります。再同期の際にベースライン転送は不要ですが、再同期には時間がかかる場合があります。再同期はオフピークの時間帯に実行することを推奨します。

次の例は、ソースボリューム間の関係を再同期します `volA` オン `svm1` デスティネーションボリュームを指定します `volA_dst` オン `svm_backup` :

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

## 10. Snapshotコピーの自動削除を無効にした場合は、再度有効にします。

```
volume snapshot autodelete modify -vserver <SVM> -volume <volume>  
-enabled true
```

完了後

1. を使用します `snapmirror show` コマンドを実行して、SnapMirror関係が作成されたことを確認します。
2. SnapMirror XDPデスティネーションボリュームがSnapMirrorポリシーの定義に従ってSnapshotコピーの更新を開始したら、の出力を使用します。 `snapmirror list-destinations` ソースクラスタからコマンドを実行し、新しいSnapMirror XDP関係を表示します。

**ONTAPのアップグレード前に既存の外部キー管理サーバの接続を削除する**

ONTAPをアップグレードする前に、NetAppストレージ暗号化（NSE）でONTAP 9.2以前を実行していて、ONTAP 9.3以降にアップグレードする場合は、コマンドラインインターフェイス（CLI）を使用して既存の外部キー管理（KMIP）サーバの接続を削除する必要があります。

手順

1. NSE ドライブがロック解除されて開いていること、デフォルトのメーカーセキュア ID である「0x0」に設定されていることを確認します。

```
storage encryption disk show -disk *
```

2. advanced 権限モードに切り替えます。

```
set -privilege advanced
```

3. デフォルトのメーカーセキュアIDである0x0を使用して、FIPSキーを自己暗号化ディスク（SED）に割り当てます。

```
storage encryption disk modify -fips-key-id 0x0 -disk *
```

4. すべてのディスクへのFIPSキーの割り当てが完了したことを確認します。

```
storage encryption disk show-status
```

5. すべてのディスクの\* mode \*がdataに設定されていることを確認します。

```
storage encryption disk show
```

6. 設定されているKMIPサーバを表示します。

```
security key-manager show
```

7. 設定されているKMIPサーバを削除します。

```
security key-manager delete -address kmip_ip_address
```

8. 外部キー管理ツールの設定を削除します。

```
security key-manager delete-kmip-config
```



この手順で NSE 証明書が削除されることはありません。

#### 次のステップ

アップグレードが完了したら、次の作業を行う必要があります。 [KMIPサーバ接続を再設定する](#)。

**ONTAP**のアップグレード前にネットグループファイルがすべてのノードに存在することを確認する

ONTAPをアップグレードする前に、ネットグループをStorage Virtual Machine（SVM）にロードした場合は、ネットグループファイルが各ノードに存在することを確認する必要があります。ノード上にネットグループファイルが見つからない場合、原因アップグ

レードが失敗する可能性があります。

#### 手順

1. 権限レベルを advanced に設定します。

```
set -privilege advanced
```

2. 各SVMのネットグループのステータスを表示します。

```
vserver services netgroup status
```

3. 各SVMについて、各ノードに表示されているネットグループファイルのハッシュ値が同じであることを確認します。

```
vserver services name-service netgroup status
```

その場合は、次の手順を省略してアップグレードまたはリバートを実行できます。それ以外の場合は、次の手順に進みます。

4. クラスタのいずれかのノードで、ネットグループファイルを手動でロードします。

```
vserver services netgroup load -vserver vserver_name -source uri
```

このコマンドは、すべてのノードにネットグループファイルをダウンロードします。ノード上に既存のネットグループファイルがある場合は、そのファイルが上書きされます。

#### 関連情報

##### "ネットグループの使用"

**TLS** を使用して高度なセキュリティを実現するように **LDAP** クライアントを設定します

ONTAPをアップグレードする前に、TLSを使用するLDAPサーバとのセキュアな通信を実現するために、SSLv3を使用するLDAPクライアントを設定する必要があります。SSLはアップグレード後に使用できなくなります。

デフォルトでは、クライアントアプリケーションとサーバアプリケーション間の LDAP 通信は暗号化されません。SSL の使用を禁止して、強制的に TLS を使用する必要があります。

#### 手順

1. 環境内の LDAP サーバで TLS がサポートされていることを確認します。

サポートされていない場合は、次の手順に進まないでください。TLS をサポートするバージョンに LDAP サーバをアップグレードする必要があります。

2. どのONTAP LDAPクライアント設定でSSL/TLS経由のLDAPが有効になっているかを確認します。

```
vserver services name-service ldap client show
```

ない場合は、残りの手順を省略できます。ただし、セキュリティを強化するには、TLS 経由の LDAP の使用を検討してください。

3. LDAPクライアント設定ごとに、SSLを禁止して強制的にTLSを使用します。

```
vserver services name-service ldap client modify -vserver vserver_name  
-client-config ldap_client_config_name -allow-ssl false
```

4. LDAPクライアントでSSLの使用が許可されていないことを確認します。

```
vserver services name-service ldap client show
```

## 関連情報

### "NFS の管理"

#### セッション指向プロトコルに関する考慮事項

クラスタおよびセッション指向プロトコルは、アップグレード中のI/Oサービスなど、特定の領域のクライアントとアプリケーションに原因が悪影響を及ぼす可能性があります。

セッション指向プロトコルを使用する場合は、次の点を考慮してください。

- SMB

SMBv3で継続的可用性（CA）共有を提供する場合は、自動化された無停止アップグレード方式（System ManagerまたはCLIを使用）。システム停止は不要クライアントによって経験されています。

SMBv1 または SMBv2 を使用して共有を提供する場合、または SMBv3 を使用する CA 以外の共有を提供する場合は、アップグレードのテイクオーバー処理とリブート処理の実行時にクライアントセッションが中断されます。アップグレードの開始前に、ユーザにセッションを終了するように通知してください。

Hyper-V および SQL Server over SMB はノンストップオペレーション（NDO）をサポートします。Hyper-V または SQL Server over SMB 解決策を設定した場合は、ONTAP のアップグレード中にもアプリケーションサーバおよびそれに格納された仮想マシンやデータベースをオンラインのまま維持し、継続的可用性を実現します。

- NFSv4.x に対応している

NFSv4.x クライアントは、NFSv4.x の通常のリカバリ手順を使用してアップグレードを実行する際に発生するネットワークの切断から自動的にリカバリします。このプロセスでは、アプリケーションの I/O が一時的に遅延することがあります。

- NDMP

状態が失われるので、クライアントユーザは操作を再試行する必要があります。

- バックアップとリストア

状態が失われるので、クライアントユーザは操作を再試行する必要があります。



アップグレードの実行中および開始直前は、バックアップまたはリストアを開始しないでください。データが失われる可能性があります。

- アプリケーション（Oracle や Exchange など）

影響はアプリケーションによって異なります。タイムアウトベースのアプリケーションでは、タイムアウトの値を ONTAP のリブート時間よりも長く設定することで、悪影響を最小限に抑えることができます。

ONTAPのアップグレード前にSSHホストキーアルゴリズムのサポートを確認する

ONTAPをアップグレードする前に、SSH公開鍵を使用して管理者アカウントを認証するクラスターでSSL FIPSモードが有効になっている場合は、ターゲットのONTAPリリースでホストキーのアルゴリズムがサポートされていることを確認する必要があります。

次の表に、ONTAP SSH接続でサポートされるホストキータイプアルゴリズムを示します。これらのキータイプは、SSH公開認証の設定には適用されません。

ONTAP リリース	FIPSモードでサポートされるキータイプ	FIPS以外のモードでサポートされるキータイプ
9.11.1以降	ECDSA - sha2 - nistp256	ECDSA-sha2-nistp256+ rsa-sha2-512+ rsa-sha2-256+ SSH-ed25519以降 SSH-DSS+ SSH-RSA
9.10.1以前	ECDSA-sha2-nistp256+ SSH-ed25519	ECDSA-sha2-nistp256+ SSH-ed25519以降 SSH-DSS+ SSH-RSA



ONTAP 9.11.1以降では、ssh-ed25519ホストキーアルゴリズムのサポートが廃止されました。

詳細については、を参照してください ["FIPS を使用してネットワークセキュリティを設定する"](#)。

サポートされているキーアルゴリズムがない既存のSSH公開鍵アカウントは、アップグレード前にサポートされているキータイプで再設定する必要があります。そうしないと、管理者認証が失敗します。

["SSH公開鍵アカウントの有効化の詳細については、こちらを参照してください。"](#)

## ONTAPアップグレード時のファームウェア更新の準備のためのSPまたはBMCのリブート

ONTAP をアップグレードする前にファームウェアを手動で更新する必要はありません。クラスタのファームウェアはONTAP アップグレードパッケージに含まれており、各ノードのブートデバイスにコピーされます。その後、アップグレードプロセスの一環として新しいファームウェアがインストールされます。

クラスタ内の次のコンポーネントのファームウェアのバージョンが ONTAP アップグレードパッケージに付属しているファームウェアよりも古い場合は、自動的に更新されます。

- BIOS /ローダー
- サービスプロセッサ (SP) またはベースボード管理コントローラ (BMC)
- ストレージシェルフ
- ディスク
- Flash Cache

スムーズな更新を準備するには、アップグレードを開始する前にSPまたはBMCをリブートする必要があります。

### ステップ

1. アップグレードの前にSPまたはBMCをリブートします。

```
system service-processor reboot-sp -node node_name
```

一度にリブートするSPまたはBMCは1つだけです。リブートしたSPまたはBMCが完全にリサイクルされるまで待ってから、次のをリブートします。

また可能です ["ファームウェアを手動で更新します"](#) ONTAP をアップグレードする際の間隔：Active IQ を使用している場合は、を実行できます ["ONTAP イメージに現在含まれているファームウェアバージョンのリストを表示します"](#)。

更新されたファームウェアバージョンは次のとおりです。

- ["システムファームウェア \(BIOS、BMC、SP\) "](#)
- ["シェルフファームウェア"](#)
- ["ディスクおよびFlash Cacheファームウェア"](#)

## ONTAPソフトウェアイメージのダウンロード

ONTAPをアップグレードする前に、ターゲットのONTAPソフトウェアイメージをNetApp Support Siteからダウンロードする必要があります。ONTAPのリリースに応じて、ONTAPソフトウェアをネットワーク上のHTTPS、HTTP、FTPサーバ、またはローカルフォルダにダウンロードできます。



実行内容	イメージをダウンロードできる場所
ONTAP 9.6 以降	<ul style="list-style-type: none"> <li>• HTTPSサーバ+ サーバのCA証明書がローカルシステムにインストールされている必要があります。</li> <li>• ローカルフォルダ</li> <li>• HTTP または FTP サーバ</li> </ul>
ONTAP 9.4以降	<ul style="list-style-type: none"> <li>• ローカルフォルダ</li> <li>• HTTP または FTP サーバ</li> </ul>
ONTAP 9.0以降	HTTP または FTP サーバ

#### このタスクについて

- 自動無停止アップグレード（ANDU）を実行する場合は、"[マルチホップの直接アップグレードパス](#)"、必要な作業 "[ダウンロード](#)" アップグレードに必要な中間ONTAPバージョンとターゲットONTAPバージョンの両方に対応するソフトウェアパッケージ。たとえば、ONTAP 9.8からONTAP 9.13.1にアップグレードする場合は、ONTAP 9.12.1とONTAP 9.13.1の両方のソフトウェアパッケージをダウンロードする必要があります。を参照してください "[サポートされるアップグレードパス](#)" アップグレードパスで中間ソフトウェアパッケージのダウンロードが必要かどうかを確認するには、次の手順を実行します。
- NetApp Volume Encryption を搭載したシステムを ONTAP 9.5 以降にアップグレードする場合は、NetApp Volume Encryption を含む制限のない国の ONTAP ソフトウェアイメージをダウンロードする必要があります。

規制対象国用の ONTAP ソフトウェアイメージを使用して NetApp Volume Encryption を搭載したシステムをアップグレードすると、システムがパニック状態になり、ボリュームへのアクセスが失われます。

- ファームウェア用のソフトウェアパッケージを別途ダウンロードする必要はありません。クラスタのファームウェアの更新は、ONTAPソフトウェアのアップグレードパッケージに含まれており、各ノードのブートデバイスにコピーされます。その後、アップグレードプロセスの一環として新しいファームウェアがインストールされます。

#### 手順

1. で、対象となる ONTAP ソフトウェアを見つけます "[ソフトウェアのダウンロード](#)" NetApp Support Siteの領域。

ONTAP Select のアップグレードの場合は、\* ONTAP Select Node Upgrade\*を選択します。

2. ソフトウェアイメージ（97\_q\_image.tgz など）を適切な場所にコピーします。

ONTAP のリリースに応じて、イメージをローカルシステムまたはストレージシステム上のローカルフォルダへ提供する HTTP、HTTPS、または FTP サーバのディレクトリの場所を指定します。

## ONTAPのアップグレード方法

### ONTAPソフトウェアのアップグレード方法

[System Manage]を使用して、ONTAPソフトウェアの自動アップグレードを実行できま

す。または、ONTAPのコマンドラインインターフェイス（CLI）を使用して、自動アップグレードまたは手動アップグレードを実行することもできます。ONTAPをアップグレードする方法は、構成、現在のONTAPのバージョン、およびクラスタ内のノード数によって異なります。NetAppでは、別のアプローチが必要な構成でないかぎり、System Managerを使用して自動アップグレードを実行することを推奨しています。たとえば、ONTAP 9.3以降を実行している4ノードのMetroCluster構成では、System Managerを使用して自動アップグレード（自動無停止アップグレードまたはANDUと呼ばれることもあります）を実行する必要があります。8ノードのMetroCluster構成でONTAP 9.2以前を実行している場合は、CLIを使用して手動アップグレードを実行する必要があります。

アップグレードは、ローリングアップグレードプロセスまたはバッチアップグレードプロセスを使用して実行できます。どちらも無停止で実行できます。

自動アップグレードの場合、ONTAPはターゲットONTAPイメージを各ノードに自動的にインストールし、クラスタの無停止アップグレードが可能なことを確認するためにクラスタコンポーネントを検証してから、ノード数に基づいてバッチアップグレードまたはローリングアップグレードをバックグラウンドで実行します。手動アップグレードの場合、クラスタ内の各ノードをアップグレードする準備ができていることを管理者が手動で確認してから、ローリングアップグレードを実行します。

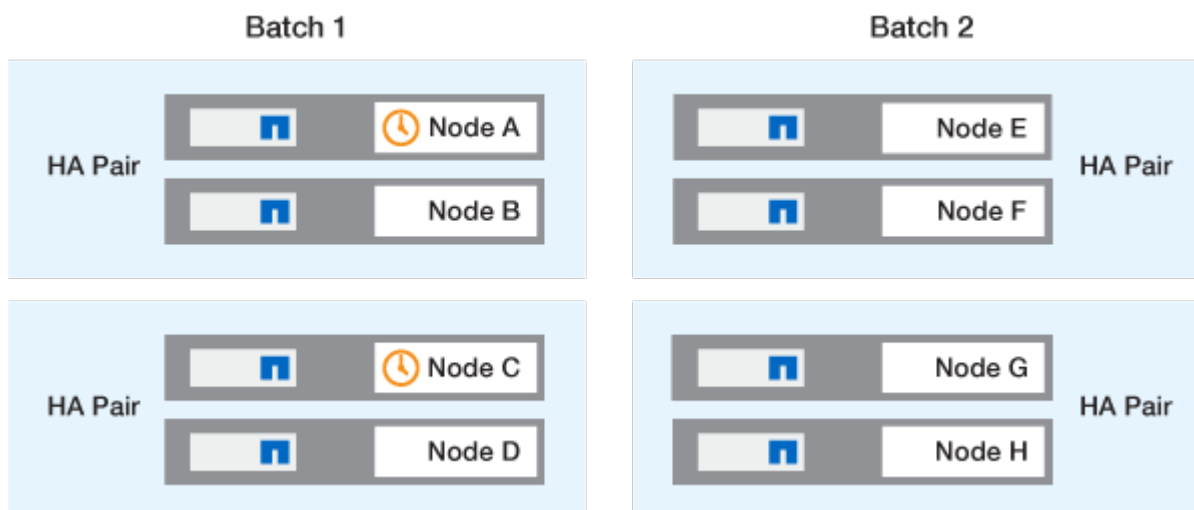
#### ONTAPローリングアップグレード

8ノード未満のクラスタでは、ローリングアップグレードプロセスがデフォルトです。ローリングアップグレードプロセスでは、ノードをオフラインにしてアップグレードし、その間ノードのストレージをパートナーにテイクオーバーします。アップグレードが完了すると、パートナーノードから元の所有者ノードに制御がギブバックされ、パートナーノードで同じ処理が実行されます。HA ペアのそれぞれについて、すべての HA ペアがターゲットリリースに切り替わるまで順番にアップグレードを行います。

#### ONTAPノバッチアップグレード

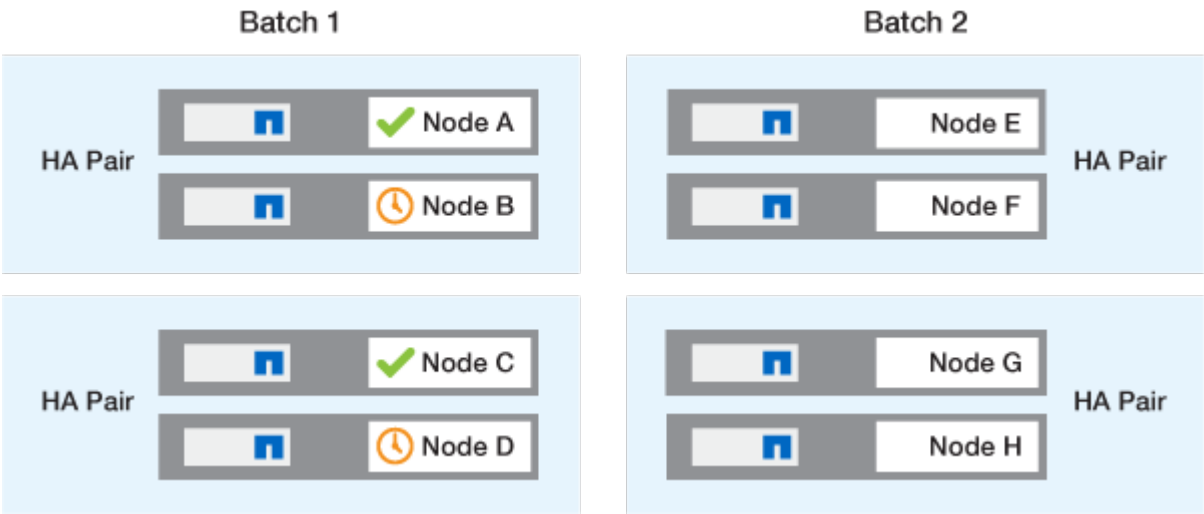
バッチアップグレードプロセスは、8ノード以上のクラスタのデフォルトです。バッチアップグレードプロセスでは、クラスタを2つのバッチに分割します。各バッチに複数のHAペアが含まれます。最初のバッチでは、各HAペアの最初のノードを、バッチに含まれる他のすべてのHAペアの最初のノードと同時にアップグレードします。

次の例では、各バッチにHAペアが2つあります。バッチアップグレードを開始すると、ノードAとノードCが同時にアップグレードされます。



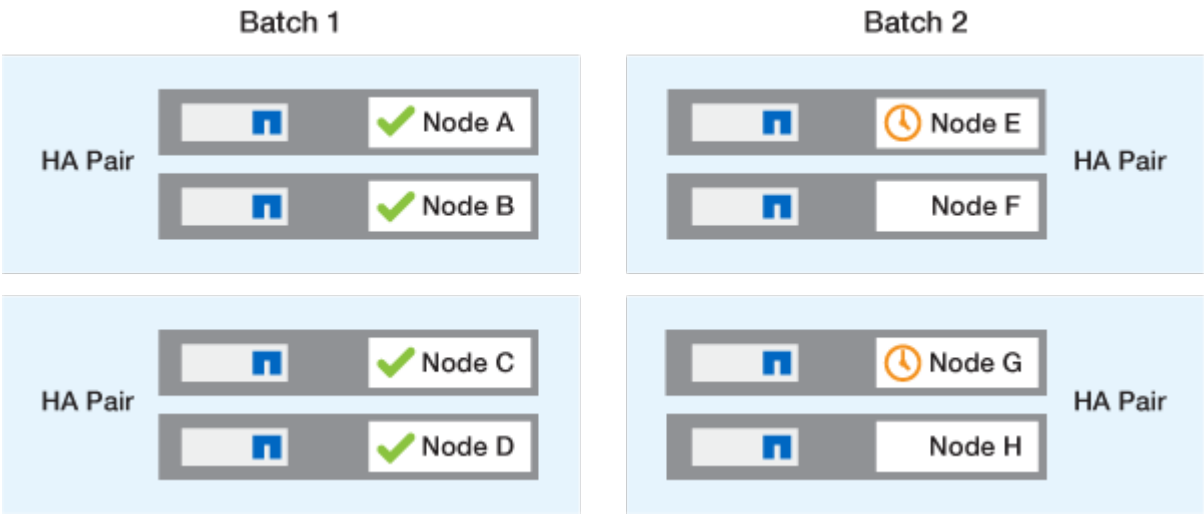
各HAペアの最初のノードのアップグレードが完了したら、バッチ1のパートナーノードが同時にアップグレードされます。

次の例では、ノードAとノードCをアップグレードしたあとに、ノードBとノードDを同時にアップグレードします。



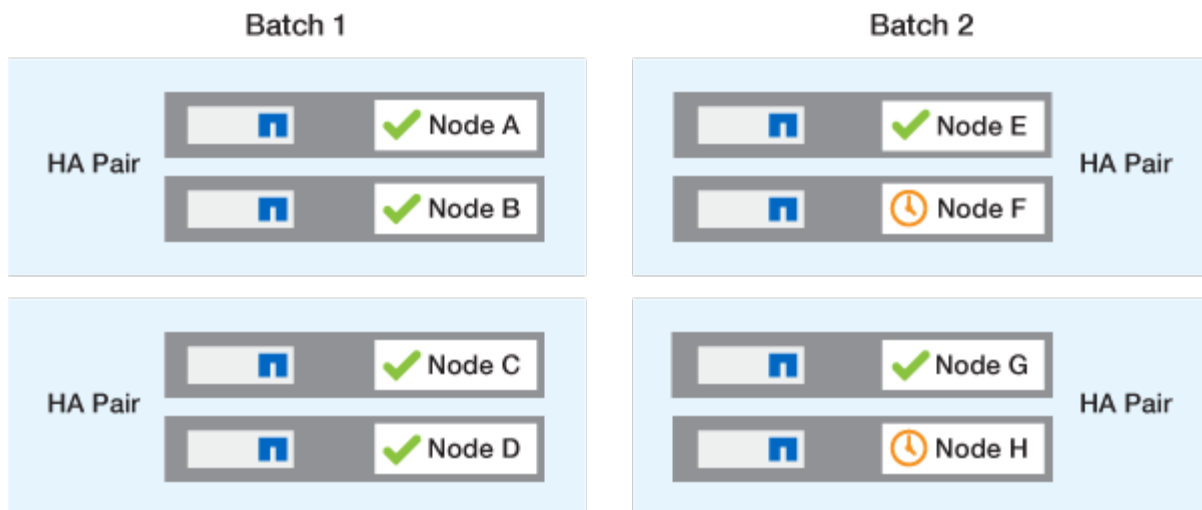
次に、バッチ2に含まれるノードに対して同じ処理を繰り返します。各HAペアの最初のノードは、バッチに含まれる他のすべてのHAペアの最初のノードと同時にアップグレードされます。

次の例では、ノードEとノードGが同時にアップグレードされます。



各HAペアの最初のノードのアップグレードが完了したら、バッチ2のパートナーノードが同時にアップグレードされます。

次の例では、ノードFとノードHを同時にアップグレードしてバッチアップグレードプロセスを完了します。



設定に基づく推奨されるONTAPアップグレード方式

お使いの構成でサポートされているアップグレード方法は、推奨される使用方法の順に記載されています。

設定	ONTAPバージョン	ノードの数	推奨されるアップグレード方式
標準	9.0以降	2以上	<ul style="list-style-type: none"> <li>System Manager を使用した自動無停止アップグレード</li> <li>CLI を使用した自動無停止アップグレード</li> </ul>
標準	9.0以降	シングル	"自動停止機能"
MetroCluster	9.3以降	8	<ul style="list-style-type: none"> <li>CLI を使用した自動無停止アップグレード</li> <li>CLIを使用した4ノードまたは8ノードMetroClusterの手動による無停止化</li> </ul>
MetroCluster	9.3以降	2/4	<ul style="list-style-type: none"> <li>System Manager を使用した自動無停止アップグレード</li> <li>CLI を使用した自動無停止アップグレード</li> </ul>
MetroCluster	9.2 以前	4、8	CLIを使用した4ノードまたは8ノードMetroClusterの手動による無停止化
MetroCluster	9.2 以前	2.	CLIを使用した2ノードMetroClusterの手動無停止アップグレード

設定に関係なく、すべてのパッチアップグレードではSystem Managerを使用したANDUのアップグレードが推奨されます。



**A 手動による停止を伴うアップグレード** 任意の構成で実行できます。ただし、停止を伴うアップグレードを実行するには、アップグレード中にクラスタをオフラインにする必要があります。SAN 環境を使用している場合は、停止を伴うアップグレードを実行する前に、すべてのSAN クライアントをシャットダウンまたは一時停止できるように準備しておく必要があります。停止を伴うアップグレードは、ONTAP CLI を使用して実行します。

## ONTAPの自動無停止アップグレード

自動アップグレードを実行すると、ONTAPによって各ノードにターゲットONTAPイメージが自動的にインストールされ、クラスタが正常にアップグレード可能かどうかを検証されてから、**バッチアップグレードまたはローリングアップグレード** クラスタ内のノード数に基づくバックグラウンドでの処理。

お使いの構成でサポートされている場合は、System Managerを使用して自動アップグレードを実行する必要があります。ご使用の構成でSystem Managerによる自動アップグレードがサポートされない場合は、ONTAPコマンドラインインターフェイス (CLI) を使用して自動アップグレードを実行できます。



の設定の変更 `storage failover modify-auto-giveback` 自動無停止アップグレード (ANDU) の開始前のコマンドオプションは、アップグレードプロセスに影響しません。ANDU プロセスは、更新に必要なテイクオーバー/ギブバックの実行時に、このオプションに設定されている値を無視します。たとえば、を設定します `-autogiveback` ANDUを開始する前に`false`に設定すると、ギブバックの前に自動アップグレードが中断されません。

作業を開始する前に

- お勧めします **"アップグレードを準備"**。
- お勧めします **"ONTAPソフトウェアイメージのダウンロード"** (ターゲットのONTAPリリース用)。

を実行する場合 **"直接マルチホップアップグレード"**をクリックすると、特定のに必要な両方のONTAPイメージをダウンロードする必要があります。 **"アップグレードパス"**。

- HA ペアごとに、1 つ以上のポートが各ノードの同じブロードキャストドメインに必要です。

ノードが8つ以上ある場合は、無停止自動アップグレードでバッチアップグレード方式が使用されます。ONTAP 9.7 以前では、バッチ方式を使用する場合に、アップグレードするノードの HA パートナーに LIF が移行されます。パートナーの同じブロードキャストドメインにポートがない場合、LIFの移行は失敗します。

ONTAP 9.8以降では、バッチ方式を使用している場合に、LIFが他のバッチグループに移行されます。

- MetroCluster FC構成でONTAPをアップグレードする場合は、クラスタで自動計画外スイッチオーバーを有効にする必要があります。
- アップグレードプロセスの進行状況を監視する予定がない場合は、**"手動操作が必要なエラーに関するEMS 通知を要求します"**。
- シングルノードクラスタの場合は、**"自動停止を伴うアップグレード"** プロセス：

シングルノードクラスタのアップグレードはシステムの停止を伴います。

## 例 2. 手順

### System Manager の略

#### 1. ONTAPターゲットイメージを検証します。



MetroCluster構成をアップグレードする場合は、クラスタAを検証してから、クラスタBで検証プロセスを繰り返す必要があります。

#### a. 実行している ONTAP のバージョンに応じて、次のいずれかの手順を実行します。

実行内容	手順
ONTAP 9.8以降	[* Cluster] > [Overview] をクリックします。
ONTAP 9.5 、 9.6 、 および 9.7	[* Configuration * (設定 *) ] > [* Cluster * (クラスタ *) ] > [* Update * (アップデート *)
ONTAP 9.4 以前	[* Configuration * (構成 *) ] > [* Cluster Update (クラスタの更新) ] を

#### b. [Overview] ペインの右隅で、をクリックします .

#### c. ONTAP アップデート \* をクリックします。

#### d. [クラスタの更新]\*タブで、新しいイメージを追加するか使用可能なイメージを選択します。

状況	作業
ローカルフォルダからの新しいソフトウェアイメージの追加  お前はもう "イメージをダウンロードしました" ローカルクライアントに送信します。	i. で、[ローカルから追加]*をクリックします。  ii. ソフトウェアイメージを保存した場所を参照し、イメージを選択して、*開く*をクリックします。
HTTPサーバまたはFTPサーバから新しいソフトウェアイメージを追加する	i. [サーバーから追加] をクリックします。  ii. [新しいソフトウェアイメージの追加]ダイアログボックスで、NetApp Support SiteからONTAPソフトウェアイメージをダウンロードしたHTTPサーバまたはFTPサーバのURLを入力します。  匿名 FTP の URL は、で指定する必要があります <a href="ftp://anonymous@ftpserver">ftp://anonymous@ftpserver</a> の形式で入力し  iii. [追加 (Add) ] をクリックします。
使用可能なイメージを選択します	表示された画像のいずれかを選択します。

- e. [検証]\*をクリックして、アップグレード前の検証チェックを実行します。

検証中にエラーや警告が検出された場合は、対処方法のリストとともに表示されます。アップグレードを続行する前に、すべてのエラーを解決する必要があります。警告も解決することを推奨します。

2. 「\*次へ\*」をクリックします。
3. [更新 (Update)] をクリックします。

再度検証が実行されます。残りのエラーまたは警告は、対処方法のリストとともに表示されます。アップグレードを続行する前に、エラーを修正する必要があります。検証が完了して警告が生成された場合は、警告を修正するか、\*[警告で更新]\*を選択します。



デフォルトでは、ONTAPは **"バッチアップグレードプロセス"** 8ノード以上のクラスタをアップグレードする場合。ONTAP 9.10.1以降では、必要に応じて[一度に1つのHAペアを更新]\*を選択してデフォルトの設定を上書きし、クラスタのHAペアをローリングアップグレードプロセスを使用して一度に1つずつアップグレードすることができます。

ノードが3つ以上のMetroCluster構成の場合は、両方のサイトのHAペアでONTAPのアップグレードプロセスが同時に開始されます。2ノードMetroCluster構成の場合は、アップグレードが開始されないサイトで最初にアップグレードが開始されます。最初のアップグレードが完了すると、残りのサイトでアップグレードが開始されます。

4. エラーが原因でアップグレードが一時停止した場合は、エラーメッセージをクリックして詳細を表示し、エラーを修正し、 **"アップグレードを再開する"**。

完了後

アップグレードが完了すると、ノードがリブートし、System Managerのログインページが表示されます。ノードのリブートに時間がかかる場合は、ブラウザをリフレッシュしてください。

## CLI の使用

1. ONTAPターゲットソフトウェアイメージの検証



MetroCluster構成をアップグレードする場合は、まずクラスタAで次の手順を実行してから、クラスタBで同じ手順を実行する必要があります。

- a. 以前の ONTAP ソフトウェアパッケージを削除します。

```
cluster image package delete -version previous_ONTAP_Version
```

- b. ターゲットのONTAPソフトウェアイメージをクラスタパッケージリポジトリにロードします。

```
cluster image package get -url location
```



```
cluster1::> cluster image package get -url
http://www.example.com/software/9.13.1/image.tgz

Package download completed.
Package processing completed.
```

を実行する場合 **"直接マルチホップアップグレード"**の場合は、アップグレードに必要な中間バージョンのONTAP用のソフトウェアパッケージもロードする必要があります。たとえば、9.8から9.13.1にアップグレードする場合は、ONTAP 9.12.1のソフトウェアパッケージをロードしてから、同じコマンドを使用して9.13.1のソフトウェアパッケージをロードする必要があります。

- c. ソフトウェアパッケージがクラスタパッケージリポジトリにあることを確認します。

```
cluster image package show-repository
```

```
cluster1::> cluster image package show-repository
Package Version  Package Build Time
-----
9.13.1           MM/DD/YYYY 10:32:15
```

- d. アップグレード前の自動チェックを実行します。

```
cluster image validate -version package_version_number
```

を実行する場合 **"直接マルチホップアップグレード"**を使用する必要があるのは、ターゲットのONTAPパッケージのみです。 中間アップグレードイメージを個別に検証する必要はありません。 たとえば、9.8から9.13.1にアップグレードする場合は、9.13.1パッケージを検証に使用します。9.12.1パッケージを個別に検証する必要はありません。

```
cluster1::> cluster image validate -version 9.13.1

WARNING: There are additional manual upgrade validation checks that
must be performed after these automated validation checks have
completed...
```

- a. 検証の進捗を監視します。

```
cluster image show-update-progress
```

- b. 検証で特定された必要なアクションをすべて完了します。



c. MetroCluster構成をアップグレードする場合は、クラスタBで上記の手順を繰り返します。

## 2. ソフトウェアアップグレードの見積もりを生成します。

```
cluster image update -version package_version_number -estimate-only
```



MetroCluster構成をアップグレードする場合は、このコマンドをクラスタAとクラスタBのどちらでも実行できます。両方のクラスタで実行する必要はありません。

ソフトウェアアップグレードの見積もりには、更新対象の各コンポーネントの詳細とアップグレードの推定期間が表示されます。

## 3. ソフトウェアのアップグレードを実行します。

```
cluster image update -version package_version_number
```

- ° を実行する場合 **"直接マルチホップアップグレード"** package\_version\_numberには、ターゲットのONTAPバージョンを使用します。たとえば、ONTAP 9.8から9.13.1にアップグレードする場合は、package\_version\_numberに9.13.1を使用します。
- ° デフォルトでは、ONTAPは **"バッチアップグレードプロセス"** 8ノード以上のクラスタをアップグレードする場合。必要に応じて、-force-rolling デフォルトのプロセスを上書きし、ローリングアップグレードプロセスを使用して一度に1つのノードをクラスタにアップグレードするためのパラメータ。
- ° テイクオーバーとギブバックがそれぞれ完了したら、テイクオーバーとギブバックの際に発生する I/O の中断からクライアントアプリケーションが回復できるように 8 分間待機します。クライアントが安定するために必要な時間が増減する場合は、を使用します -stabilize-minutes 別の待機時間を指定するパラメータ。
- ° 4ノード以上のMetroCluster構成の場合は、両方のサイトのHAペアで同時に自動アップグレードが開始されます。2ノードMetroCluster構成の場合は、アップグレードが開始されないサイトでアップグレードが開始されます。最初のアップグレードが完了すると、残りのサイトでアップグレードが開始されます。

```

cluster1::> cluster image update -version 9.13.1

Starting validation for this update. Please wait..

It can take several minutes to complete validation...

WARNING: There are additional manual upgrade validation checks...

Pre-update Check      Status      Error-Action
-----
...
20 entries were displayed

Would you like to proceed with update ? {y|n}: y
Starting update...

cluster-1::>

```

#### 4. クラスタの更新の進捗を表示します。

```
cluster image show-update-progress
```

4ノードまたは8ノードのMetroCluster 構成をアップグレードする場合は、を参照してください  
cluster image show-update-progress コマンドは、コマンドを実行するノードの進捗状況のみを表示します。個々のノードの進捗を確認するには、各ノードでコマンドを実行する必要があります。

#### 5. 各ノードでアップグレードが正常に完了したことを確認します。

```
cluster image show-update-progress
```

```
cluster1::> cluster image show-update-progress
```

Elapsed		Estimated
Update Phase	Status	Duration
Duration		
-----	-----	-----
-----		
Pre-update checks	completed	00:10:00
00:02:07		
Data ONTAP updates	completed	01:31:00
01:39:00		
Post-update checks	completed	00:10:00
00:02:00		

3 entries were displayed.

Updated nodes: node0, node1.

6. AutoSupport 通知を送信します。

```
autosupport invoke -node * -type all -message "Finishing_NDU"
```

AutoSupport メッセージを送信するようにクラスタが設定されていない場合は、通知のコピーがローカルに保存されます。

7. 2ノードMetroCluster FC構成をアップグレードする場合は、クラスタで自動計画外スイッチオーバーが有効になっていることを確認します。



標準構成、MetroCluster IP構成、またはMetroCluster FC構成のノードが3つ以上の場合は、この手順を実行する必要はありません。

a. 自動計画外スイッチオーバーが有効かどうかを確認します。

```
metrocluster show
```

自動計画外スイッチオーバーが有効な場合、コマンド出力に次のステートメントが表示されます。

```
AUSO Failure Domain      auso-on-cluster-disaster
```

a. 出力にステートメントが表示されない場合は、自動計画外スイッチオーバーを有効にします。

```
metrocluster modify -auto-switchover-failure-domain auso-on-  
cluster-disaster
```

- b. 自動計画外スイッチオーバーが有効になっていることを確認します。

```
metrocluster show
```

自動アップグレードプロセスでエラーが発生した場合に**ONTAP**ソフトウェアのアップグレードを再開する

エラーが原因でONTAPソフトウェアの自動アップグレードが一時停止した場合は、エラーを解決してからアップグレードを続行する必要があります。エラーを解決したら、自動アップグレードプロセスを続行するか、アップグレードプロセスを手動で完了するかを選択できます。自動アップグレードを続行する場合は、アップグレード手順を手動で実行しないでください。

### 例 3. 手順

#### System Manager の略

1. 実行している ONTAP のバージョンに応じて、次のいずれかの手順を実行します。

実行内容	作業
ONTAP 9.8以降	>[概要]*をクリックします。
ONTAP 9.7、9.6、または9.5	[* Configuration *（設定 *）]>[* Cluster *（クラスタ *）]>[* Update *（アップデート *
ONTAP 9.4 以前	<ul style="list-style-type: none"><li>• [* Configuration *（構成 *）]&gt;[* Cluster Update（クラスタの更新）]を</li><li>• ペインの右隅にある青い縦の3つのドットをクリックし、ONTAP Update*を選択します。</li></ul>

2. 自動アップグレードを続行するか、キャンセルして手動で続行します。

状況	作業
自動アップグレードを再開する	[* 再開 *]をクリックします。
自動アップグレードをキャンセルして手動で続行する	[キャンセル（Cancel）]をクリックします。

#### CLI の使用

1. アップグレードエラーを表示します。

```
cluster image show-update-progress
```

2. エラーを解決します。

3. アップグレードを再開します。

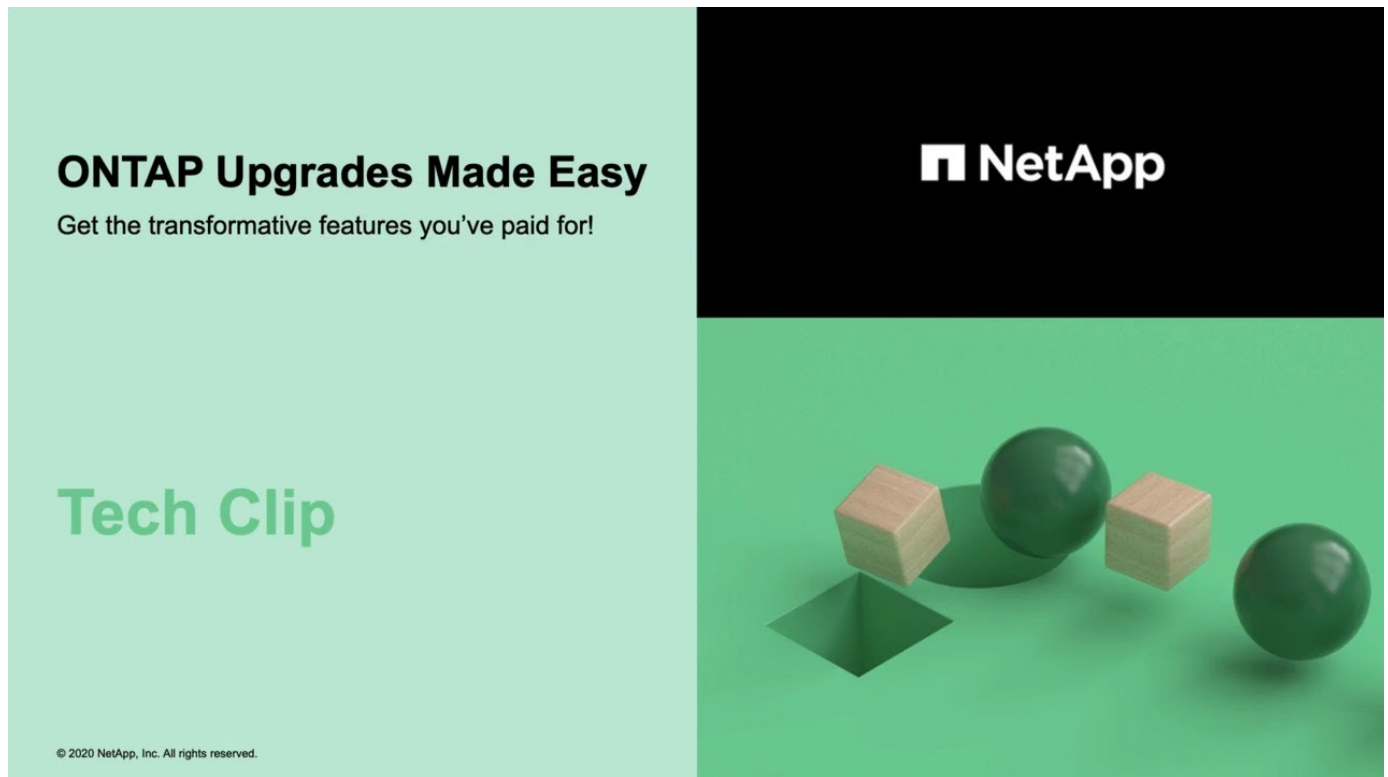
状況	入力するコマンド
自動アップグレードを再開する	<pre>cluster image resume-update</pre>
自動アップグレードをキャンセルして手動で続行する	<pre>cluster image cancel-update</pre>

完了後

"アップグレード後チェックの実行"。

ビデオ : 簡単にアップグレード

ONTAP 9.8 の ONTAP アップグレード機能の簡易化についてご確認ください。



#### 関連情報

- ["Active IQ を起動します"](#)
- ["Active IQ のドキュメント"](#)

#### シュドウアップグレード

手動アップグレードのためのONTAPソフトウェアパッケージのインストール

手動アップグレード用のONTAPソフトウェアパッケージをダウンロードしたら、アップグレードを開始する前にローカルにインストールする必要があります。

#### 手順

1. 権限レベルをadvancedに設定します。続行するかどうかを尋ねられたら、「\*y\*」と入力します。 `set -privilege advanced`  
  
advancedプロンプトが表示されます (\*>) が表示されます。
2. イメージをインストールします。

構成	使用するコマンド
<ul style="list-style-type: none"> <li>• MetroCluster以外</li> <li>• 2ノードMetroCluster</li> </ul>	<pre>system node image update -node * -package _location_ -replace -package true -setdefault true -background true</pre> <p><i>location</i> は、ONTAP のバージョンに応じて、Web サーバまたはローカルフォルダです。を参照してください <code>system node image update</code> のマニュアルページを参照してください。</p> <p>このコマンドを実行すると、ソフトウェアイメージがすべてのノードに同時にインストールされます。一度に1つずつ各ノードにイメージをインストールする場合は、<code>-background</code> パラメータ</p>
<ul style="list-style-type: none"> <li>• 4ノードMetroCluster</li> <li>• 8ノードMetroCluster構成</li> </ul>	<pre>system node image update -node * -package location -replace -package true -background true -setdefault false</pre> <p>このコマンドは両方のクラスタで問題する必要がありません。</p> <p>このコマンドでは、拡張クエリを使用して、各ノードに代替イメージとしてインストールされるターゲットソフトウェアイメージを変更します。</p>

3. 入力するコマンド `y` プロンプトが表示されたら続行します。
4. 各ノードにソフトウェアイメージがインストールされていることを確認します。

```
system node image show-update-progress -node *
```

このコマンドは、ソフトウェアイメージのインストールの現在のステータスを表示します。すべてのノードの Run Status \* が Exited \* になり、\* Exit Status \* が \* Success \* になるまで、このコマンドを繰り返し実行します。

`system node image update` コマンドが失敗して、エラーまたは警告メッセージが表示されることがあります。エラーまたは警告を解決したら、もう一度コマンドを実行できます。

次の例では、2ノードクラスタの両方のノードにソフトウェアイメージが正常にインストールされています。

```
cluster1::*> system node image show-update-progress -node *
There is no update/install in progress
Status of most recent operation:
    Run Status:      Exited
    Exit Status:     Success
    Phase:           Run Script
    Exit Message:    After a clean shutdown, image2 will be set as
the default boot image on node0.
There is no update/install in progress
Status of most recent operation:
    Run Status:      Exited
    Exit Status:     Success
    Phase:           Run Script
    Exit Message:    After a clean shutdown, image2 will be set as
the default boot image on node1.
2 entries were acted on.
```

#### CLIを使用した手動による無停止ONTAPアップグレード（標準構成）

System Managerを使用した自動アップグレードが推奨されるアップグレード方法です。ご使用の構成がSystem Managerでサポートされていない場合は、ONTAPコマンドラインインターフェイス（CLI）を使用して手動で無停止アップグレードを実行できます。手動の無停止方式を使用して2つ以上のノードのクラスタをアップグレードするには、HA ペアの各ノードでフェイルオーバー処理を開始し、「failed」ノードを更新してギブバックを開始してから、クラスタ内の各 HA ペアについてこの処理を繰り返す必要があります。

作業を開始する前に

アップグレードを完了しておく必要があります **"準備"** 要件：

#### HA ペアの最初のノードの更新

ノードのパートナーによるテイクオーバーを開始することで、HA ペアの最初のノードを更新できます。最初のノードをアップグレードしている間、ノードのデータはパートナーから提供されます。

メジャーアップグレードを実行する場合は、外部接続用にデータ LIF を設定し、最初の ONTAP イメージをインストールしたノードをアップグレード対象の最初のノードにする必要があります。

最初のノードをアップグレードしたら、できるだけ早くパートナーノードをアップグレードする必要があります。2つのノードを **"バージョンノコンザイ"** 必要以上に長い状態にします。

手順

1. AutoSupport メッセージを呼び出して、クラスタ内の最初のノードを更新します。



```
autosupport invoke -node * -type all -message "Starting_NDU"
```

この AutoSupport 通知には、更新直前のシステムステータスの記録が含まれます。これにより、更新処理で問題が発生した場合に役立つトラブルシューティング情報が保存されます。

AutoSupport メッセージを送信するようにクラスタが設定されていない場合は、通知のコピーがローカルに保存されます。

2. 権限レベルをadvancedに設定します。続行するかどうかを尋ねられたら、「\*y\*」と入力します。

```
set -privilege advanced
```

advancedプロンプトが表示されます (\*>) が表示されます。

3. 新しいONTAP ソフトウェアイメージをデフォルトのイメージとして設定します。

```
system image modify {-node nodenameA -iscurrent false} -isdefault true
```

system image modify コマンドでは、拡張クエリを使用して、代替イメージとしてインストールされる新しい ONTAP ソフトウェアイメージがノードのデフォルトのイメージに変更されます。

4. 更新の進捗を監視します。

```
system node upgrade-revert show
```

5. 新しいONTAP ソフトウェアイメージがデフォルトのイメージとして設定されたことを確認します。

```
system image show
```

次の例では、image2 が新しい ONTAP バージョンで、node0 のデフォルトのバージョンとして設定されています。

```
cluster1::*> system image show
```

Node	Image	Is Default	Is Current	Version	Install Date
-----					
node0					
	image1	false	true	X.X.X	MM/DD/YYYY TIME
	image2	true	false	Y.Y.Y	MM/DD/YYYY TIME
node1					
	image1	true	true	X.X.X	MM/DD/YYYY TIME
	image2	false	false	Y.Y.Y	MM/DD/YYYY TIME

4 entries were displayed.

6. 自動ギブバックが有効になっている場合は、パートナーノードで無効にします。

```
storage failover modify -node nodenameB -auto-giveback false
```

2 ノードクラスタでは、自動ギブバックを無効にすると、2 つのノードで交互に障害が発生した場合に管理クラスタのサービスがオンラインにならないことを警告するメッセージが表示されます。入力するコマンド y 続行します。

7. ノードのパートナーの自動ギブバックが無効になっていることを確認します。

```
storage failover show -node nodenameB -fields auto-giveback
```

```
cluster1::> storage failover show -node node1 -fields auto-giveback
```

node	auto-giveback
-----	
node1	false

1 entry was displayed.

8. 次のコマンドを2回実行して、更新対象のノードが現在クライアントに対して処理を行っているかどうかを確認します

```
system node run -node nodenameA -command uptime
```

uptimeコマンドは、ノードの前のブート以降にNFS、SMB、FC、およびiSCSIの各クライアントに対してノードが実行した処理の合計数を表示します。プロトコルごとにコマンドを2回実行して、処理数が増加しているかどうかを確認する必要があります。増加している場合は、そのプロトコルのクライアントに対してノードが現在処理を行っています。増加していない場合は、そのプロトコルのクライアントに対してノードは現在処理を行っていません。



ノードの更新後にクライアントトラフィックが再開したことを確認できるように、クライアント処理の増加の原因となっている各プロトコルをメモしておく必要があります。

次の例は、NFS、SMB、FC、およびiSCSIの処理が実行されているノードを示しています。ただし、ノードは現在 NFS クライアントと iSCSI クライアントに対してのみ処理を行っています。

```
cluster1::> system node run -node node0 -command uptime
  2:58pm up  7 days, 19:16 800000260 NFS ops, 1017333 CIFS ops, 0 HTTP
ops, 40395 FCP ops, 32810 iSCSI ops

cluster1::> system node run -node node0 -command uptime
  2:58pm up  7 days, 19:17 800001573 NFS ops, 1017333 CIFS ops, 0 HTTP
ops, 40395 FCP ops, 32815 iSCSI ops
```

#### 9. ノードからすべてのデータLIFを移行します。

```
network interface migrate-all -node nodenameA
```

#### 10. 移行したLIFを確認します。

```
network interface show
```

LIF のステータスの確認に使用できるパラメータの詳細については、network interface show のマニュアルページを参照してください。

次の例は、node0 のデータ LIF が正常に移行されたことを示しています。それぞれの LIF について、この例に含まれるフィールドを使用して、LIF のホームノードとポート、LIF の移行先である現在のノードとポート、および LIF の動作ステータスと管理ステータスを確認できます。

```
cluster1::> network interface show -data-protocol nfs|cifs -role data
-home-node node0 -fields home-node,curr-node,curr-port,home-port,status-
admin,status-oper
vserver lif      home-node home-port curr-node curr-port status-oper
status-admin
-----
-----
vs0      data001 node0      e0a      node1      e0a      up      up
vs0      data002 node0      e0b      node1      e0b      up      up
vs0      data003 node0      e0b      node1      e0b      up      up
vs0      data004 node0      e0a      node1      e0a      up      up
4 entries were displayed.
```

#### 11. テイクオーバーを開始します。

```
storage failover takeover -ofnode nodenameA
```

テイクオーバーされたノードを新しいソフトウェアイメージでブートするには通常のテイクオーバーが必要なため、`-option immediate` パラメータは指定しないでください。ノードから LIF を手動で移行しなかった場合は、LIF がノードの HA パートナーに自動的に移行されるため、サービスが停止することはありません。

最初のノードがブートし、Waiting for giveback 状態になります。



AutoSupportが有効な場合は、ノードがクラスタフォーラムのメンバーでないことを示すAutoSupportメッセージが送信されます。この通知を無視し、更新を続行してかまいません。

12. テイクオーバーが正常に完了したことを確認します。

```
storage failover show
```

バージョン不一致およびメールボックス形式の問題を示すエラーメッセージが表示される場合があります。これは想定されている動作であり、無停止メジャーアップグレードにおける一時的な状態を表しており、悪影響はありません。

次の例は、テイクオーバーが正常に完了したことを示しています。ノード node0 の状態は Waiting for giveback、パートナーの状態は In takeover になっています。

```
cluster1::> storage failover show
```

Node	Partner	Takeover Possible	State Description
node0	node1	-	Waiting for giveback (HA mailboxes)
node1	node0	false	In takeover

2 entries were displayed.

13. 次の状態になるまで少なくとも 8 分待ちます。

- クライアントのマルチパス（導入している場合）が安定している。
- クライアントがテイクオーバー中に発生した I/O 処理の中断から回復している。

回復までの時間はクライアントによって異なり、クライアントアプリケーションの特性によっては 8 分以上かかることもあります。

14. アグリゲートを最初のノードに戻します。

```
storage failover giveback -ofnode nodenameA
```

ギブバックでは、最初にルートアグリゲートがパートナーノードに戻され、そのノードのブートが完了すると、ルート以外のアグリゲートと自動的にリバートするように設定されたすべての LIF が戻されます。新しくブートしたノードで、戻されたアグリゲートから順番にクライアントへのデータ提供が開始されます。

15. すべてのアグリゲートが戻されたことを確認します。

```
storage failover show-giveback
```

Giveback Status フィールドにギブバックするアグリゲートがないことが示されている場合は、すべてのアグリゲートが戻されています。ギブバックが拒否された場合は、コマンドによってギブバックの進捗が表示され、ギブバックを拒否したサブシステムも表示されます。

16. いずれかのアグリゲートが戻されていない場合は、次の手順を実行します。
- 拒否された回避策を確認して、「ve to」状態に対処するか、拒否を無視するかを決定します。
  - 必要に応じて、エラーメッセージに記載されている「宛」の状態に対処し、特定された処理が正常に終了するようにします。
  - storage failover giveback コマンドを再実行します。

「''' ~ '''」条件をオーバーライドする場合は、-override-vetoes パラメータを true に設定します。

17. 次の状態になるまで少なくとも 8 分待ちます。

- クライアントのマルチパス（導入している場合）が安定している。
- クライアントがギブバック中に発生した I/O 処理の中断から回復している。

回復までの時間はクライアントによって異なり、クライアントアプリケーションの特性によっては 8 分以上かかることもあります。

18. ノードの更新が正常に完了したことを確認します。

- a. advanced 権限レベルに切り替えます。

```
set -privilege advanced
```

- b. ノードの更新ステータスが完了になっていることを確認します。

```
system node upgrade-revert show -node nodenameA
```

ステータスが complete になっている必要があります。

ステータスが completeにならない場合は、テクニカルサポートに連絡してください。

a. admin 権限レベルに戻ります。

```
set -privilege admin
```

19. ノードのポートが動作していることを確認します。

```
network port show -node nodenameA
```

このコマンドは、ONTAP 9 の上位バージョンにアップグレードされたノードで実行する必要があります。

次の例は、ノードのすべてのポートが動作していることを示しています。

```
cluster1::> network port show -node node0
```

						Speed
(Mbps)						
Node	Port	IPspace	Broadcast Domain	Link	MTU	Admin/Oper
-----	-----	-----	-----	-----	-----	-----
node0						
	e0M	Default	-	up	1500	auto/100
	e0a	Default	-	up	1500	auto/1000
	e0b	Default	-	up	1500	auto/1000
	e1a	Cluster	Cluster	up	9000	auto/10000
	e1b	Cluster	Cluster	up	9000	auto/10000
5 entries were displayed.						

20. LIFをノードにリバートします。

```
network interface revert *
```

このコマンドを実行すると、移行した LIF が元のノードに戻されます。

```
cluster1::> network interface revert *  
8 entries were acted on.
```

21. ノードのデータLIFが正常にノードにリバートされ、動作していることを確認します。

```
network interface show
```

次の例は、ノードがホストするすべてのデータ LIF が正常にノードにリバートされ、動作ステータスが「

up」になっていることを示しています。

```
cluster1::> network interface show
```

	Logical	Status	Network	Current	
Current Is					
Vserver	Interface	Admin/Oper	Address/Mask	Node	Port
Home					
-----	-----	-----	-----	-----	-----
vs0					
	data001	up/up	192.0.2.120/24	node0	e0a
true					
	data002	up/up	192.0.2.121/24	node0	e0b
true					
	data003	up/up	192.0.2.122/24	node0	e0b
true					
	data004	up/up	192.0.2.123/24	node0	e0a
true					

4 entries were displayed.

22. このノードがクライアントに対して処理を行っているとして以前に判断した場合は、ノードが以前に処理を行っていた各プロトコルに対してサービスを提供していることを確認します。

```
system node run -node nodenameA -command uptime
```

更新中に、処理数はゼロにリセットされます。

次の例は、更新したノードが NFS クライアントと iSCSI クライアントに対する処理を再開していることを示しています。

```
cluster1::> system node run -node node0 -command uptime
3:15pm up 0 days, 0:16 129 NFS ops, 0 CIFS ops, 0 HTTP ops, 0 FCP
ops, 2 iSCSI ops
```

23. 以前に自動ギブバックを無効にした場合は、パートナーノードで再度有効にします。

```
storage failover modify -node nodenameB -auto-giveback true
```

できるだけ早くノードの HA パートナーの更新に進んでください。何らかの理由で更新プロセスを中断する必要がある場合は、HA ペアの両方のノードで同じバージョンの ONTAP を実行する必要があります。

## HA ペアのパートナーノードの更新

HA ペアの最初のノードを更新したあとは、そのノードでテイクオーバーを開始してパートナーを更新します。パートナーをアップグレードしている間、パートナーのデータは最初のノードから提供されます。

1. 権限レベルをadvancedに設定します。続行するかどうかを尋ねられたら、「\*y\*」と入力します。

```
set -privilege advanced
```

advancedプロンプトが表示されます (\*>) が表示されます。

2. 新しいONTAP ソフトウェアイメージをデフォルトのイメージとして設定します。

```
system image modify {-node nodenameB -iscurrent false} -isdefault true
```

system image modify コマンドでは、拡張クエリを使用して、代替イメージとしてインストールされる新しい ONTAP ソフトウェアイメージがノードのデフォルトのイメージになるように変更します。

3. 更新の進捗を監視します。

```
system node upgrade-revert show
```

4. 新しいONTAP ソフトウェアイメージがデフォルトのイメージとして設定されたことを確認します。

```
system image show
```

次の例では、image2 はONTAP の新しいバージョンで、ノードでデフォルトのイメージとして設定されています。

```
cluster1::*> system image show
```

Node	Image	Is Default	Is Current	Version	Install Date
node0					
	image1	false	false	X.X.X	MM/DD/YYYY TIME
	image2	true	true	Y.Y.Y	MM/DD/YYYY TIME
node1					
	image1	false	true	X.X.X	MM/DD/YYYY TIME
	image2	true	false	Y.Y.Y	MM/DD/YYYY TIME

4 entries were displayed.

5. 自動ギブバックが有効になっている場合は、パートナーノードで無効にします。



```
storage failover modify -node nodenameA -auto-giveback false
```

2 ノードクラスタでは、自動ギブバックを無効にすると、2 つのノードで交互に障害が発生した場合に管理クラスタのサービスがオンラインにならないことを警告するメッセージが表示されます。入力するコマンド y 続行します。

6. パートナーノードの自動ギブバックが無効になっていることを確認します。

```
storage failover show -node nodenameA -fields auto-giveback
```

```
cluster1::> storage failover show -node node0 -fields auto-giveback
node      auto-giveback
-----
node0     false
1 entry was displayed.
```

7. 次のコマンドを2回実行して、更新対象のノードが現在クライアントに対して処理を行っているかどうかを確認します。

```
system node run -node nodenameB -command uptime
```

uptimeコマンドは、ノードの前のブート以降にNFS、SMB、FC、およびiSCSIの各クライアントに対してノードが実行した処理の合計数を表示します。プロトコルごとにコマンドを2回実行して、処理数が増加しているかどうかを確認する必要があります。増加している場合は、そのプロトコルのクライアントに対してノードが現在処理を行っています。増加していない場合は、そのプロトコルのクライアントに対してノードは現在処理を行っていません。

- 。注\*：ノードの更新後にクライアントトラフィックが再開したことを確認できるように、クライアント処理の増加に伴う各プロトコルを書き留めてください。

次の例は、NFS、SMB、FC、およびiSCSIの処理が実行されているノードを示しています。ただし、ノードは現在NFSクライアントとiSCSIクライアントに対してのみ処理を行っています。

```
cluster1::> system node run -node node1 -command uptime
2:58pm up 7 days, 19:16 800000260 NFS ops, 1017333 CIFS ops, 0 HTTP
ops, 40395 FCP ops, 32810 iSCSI ops

cluster1::> system node run -node node1 -command uptime
2:58pm up 7 days, 19:17 800001573 NFS ops, 1017333 CIFS ops, 0 HTTP
ops, 40395 FCP ops, 32815 iSCSI ops
```

8. ノードからすべてのデータLIFを移行します。

```
network interface migrate-all -node nodenameB
```

9. 移行したLIFのステータスを確認します。

```
network interface show
```

LIF のステータスの確認に使用できるパラメータの詳細については、network interface show のマニュアルページを参照してください。

次の例は、node1のデータLIFが正常に移行されたことを示しています。それぞれの LIF について、この例に含まれるフィールドを使用して、LIF のホームノードとポート、LIF の移行先である現在のノードとポート、および LIF の動作ステータスと管理ステータスを確認できます。

```
cluster1::> network interface show -data-protocol nfs|cifs -role data
             -home-node node1 -fields home-node,curr-node,curr-port,home-port,status-
             admin,status-oper
vservers lif      home-node home-port curr-node curr-port status-oper
status-admin
-----
vs0      data001 node1      e0a      node0      e0a      up      up
vs0      data002 node1      e0b      node0      e0b      up      up
vs0      data003 node1      e0b      node0      e0b      up      up
vs0      data004 node1      e0a      node0      e0a      up      up
4 entries were displayed.
```

10. テイクオーバーを開始します。

```
storage failover takeover -ofnode nodenameB -option allow-version-
mismatch
```

テイクオーバーされたノードを新しいソフトウェアイメージでブートするには通常のテイクオーバーが必要なため、-option immediate パラメータは指定しないでください。ノードから LIF を手動で移行しなかった場合は、LIF がノードの HA パートナーに自動的に移行されるため、サービスが停止することはありません。

警告が表示されます。 入る必要があります y 続行します。

テイクオーバーされたノードがブートし、Waiting for giveback 状態になります。



AutoSupportが有効な場合は、ノードがクラスタフォーラムのメンバーでないことを示すAutoSupportメッセージが送信されます。この通知を無視し、更新を続行してかまいません。

11. テイクオーバーが正常に完了したことを確認します。

```
storage failover show
```

次の例は、テイクオーバーが正常に完了したことを示しています。ノードnode1の状態はWaiting for giveback、パートナーの状態はIn takeoverになっています。

```
cluster1::> storage failover show
```

Node	Partner	Takeover Possible	State Description
node0	node1	-	In takeover
node1	node0	false	Waiting for giveback (HA mailboxes)

2 entries were displayed.

12. 次の状態になるまで少なくとも 8 分待ちます。

[+]

- クライアントのマルチパス（導入している場合）が安定している。
- クライアントがテイクオーバー中に発生した I/O の中断から回復している。

回復までの時間はクライアントによって異なり、クライアントアプリケーションの特性によっては 8 分以上かかることもあります。

13. アグリゲートをパートナーノードに戻します。

```
storage failover giveback -ofnode nodenameB
```

ギブバック処理では、最初にルートアグリゲートがパートナーノードに戻され、そのノードのブートが完了すると、ルート以外のアグリゲートと自動的にリバートするように設定されたすべての LIF が戻されます。新しくブートしたノードで、戻されたアグリゲートから順番にクライアントへのデータ提供が開始されます。

14. すべてのアグリゲートが戻されたことを確認します。

```
storage failover show-giveback
```

Giveback Status フィールドにギブバックするアグリゲートがないことが示されている場合は、すべてのアグリゲートが戻されています。ギブバックが拒否された場合は、コマンドによってギブバックの進捗が表示され、ギブバック処理を拒否したサブシステムも表示されます。

15. いずれかのアグリゲートが戻されていない場合は、次の手順を実行します。

- a. 拒否された回避策を確認して、「ve to」状態に対処するか、拒否を無視するかを決定します。
- b. 必要に応じて、エラーメッセージに記載されている「宛」の状態に対処し、特定された処理が正常に終了するようにします。
- c. storage failover giveback コマンドを再実行します。

「''' ~ '''」条件をオーバーライドする場合は、-override-vetoes パラメータを true に設定します。

16. 次の状態になるまで少なくとも 8 分待ちます。

- クライアントのマルチパス（導入している場合）が安定している。
- クライアントがギブバック中に発生した I/O 処理の中断から回復している。

回復までの時間はクライアントによって異なり、クライアントアプリケーションの特性によっては 8 分以上かかることもあります。

17. ノードの更新が正常に完了したことを確認します。

- a. advanced 権限レベルに切り替えます。

```
set -privilege advanced
```

- b. ノードの更新ステータスが完了になっていることを確認します。

```
system node upgrade-revert show -node nodenameB
```

ステータスが complete になっている必要があります。

ステータスが complete になっていない場合は、ノードから system node upgrade-revert upgrade コマンドを実行します。このコマンドを実行しても更新が完了しない場合は、テクニカルサポートにお問い合わせください。

- a. admin 権限レベルに戻ります。

```
set -privilege admin
```

18. ノードのポートが動作していることを確認します。

```
network port show -node nodenameB
```

このコマンドは、ONTAP 9.4 にアップグレードされたノードで実行する必要があります。

次の例は、ノードのすべてのデータポートが動作していることを示しています。

```
cluster1::> network port show -node node1
```

						Speed
(Mbps)						
Node	Port	IPspace	Broadcast Domain	Link	MTU	Admin/Oper
-----	-----	-----	-----	-----	-----	-----
node1						
	e0M	Default	-	up	1500	auto/100
	e0a	Default	-	up	1500	auto/1000
	e0b	Default	-	up	1500	auto/1000
	e1a	Cluster	Cluster	up	9000	auto/10000
	e1b	Cluster	Cluster	up	9000	auto/10000
5 entries were displayed.						

19. LIFをノードにリバートします。

```
network interface revert *
```

このコマンドを実行すると、移行した LIF が元のノードに戻されます。

```
cluster1::> network interface revert *  
8 entries were acted on.
```

20. ノードのデータLIFが正常にノードにリバートされ、動作していることを確認します。

```
network interface show
```

次の例は、ノードがホストするすべてのデータ LIF が正常にノードにリバートされ、動作ステータスが「up」になっていることを示しています。

```
cluster1::> network interface show
```

Current Is	Logical	Status	Network	Current	
Vserver	Interface	Admin/Oper	Address/Mask	Node	Port
Home					
-----	-----	-----	-----	-----	-----
vs0					
	data001	up/up	192.0.2.120/24	node1	e0a
true					
	data002	up/up	192.0.2.121/24	node1	e0b
true					
	data003	up/up	192.0.2.122/24	node1	e0b
true					
	data004	up/up	192.0.2.123/24	node1	e0a
true					

4 entries were displayed.

21. このノードがクライアントに対して処理を行っているとは以前に判断した場合は、ノードが以前に処理を行っていた各プロトコルに対してサービスを提供していることを確認します。

```
system node run -node nodenameB -command uptime
```

更新中に、処理数はゼロにリセットされます。

次の例は、更新したノードが NFS クライアントと iSCSI クライアントに対する処理を再開していることを示しています。

```
cluster1::> system node run -node node1 -command uptime
3:15pm up 0 days, 0:16 129 NFS ops, 0 CIFS ops, 0 HTTP ops, 0 FCP
ops, 2 iSCSI ops
```

22. これがクラスタ内で更新される最後のノードであった場合は、AutoSupport 通知をトリガーします。

```
autosupport invoke -node * -type all -message "Finishing_NDU"
```

この AutoSupport 通知には、更新直前のシステムステータスの記録が含まれます。これにより、更新処理で問題が発生した場合に役立つトラブルシューティング情報が保存されます。

AutoSupport メッセージを送信するようにクラスタが設定されていない場合は、通知のコピーがローカルに保存されます。

23. HAペアの両方のノードで新しいONTAP ソフトウェアが実行されていることを確認します。

```
set -privilege advanced
```

```
system node image show
```

次の例では、image2 が ONTAP の更新されたバージョンで、両方のノードのデフォルトのバージョンになっています。

```
cluster1::*> system node image show
```

Node	Image	Is Default	Is Current	Version	Install Date
node0	image1	false	false	X.X.X	MM/DD/YYYY TIME
	image2	true	true	Y.Y.Y	MM/DD/YYYY TIME
node1	image1	false	false	X.X.X	MM/DD/YYYY TIME
	image2	true	true	Y.Y.Y	MM/DD/YYYY TIME

4 entries were displayed.

24. 以前に自動ギブバックを無効にした場合は、パートナーノードで再度有効にします。

```
storage failover modify -node nodenameA -auto-giveback true
```

25. を使用して、クラスタがクォーラムにあること、およびサービスが実行されていることを確認します。  
cluster show および cluster ring show (advanced権限レベル) のコマンドを入力します。

追加の HA ペアをアップグレードする前にこの手順を実行する必要があります。

26. admin 権限レベルに戻ります。

```
set -privilege admin
```

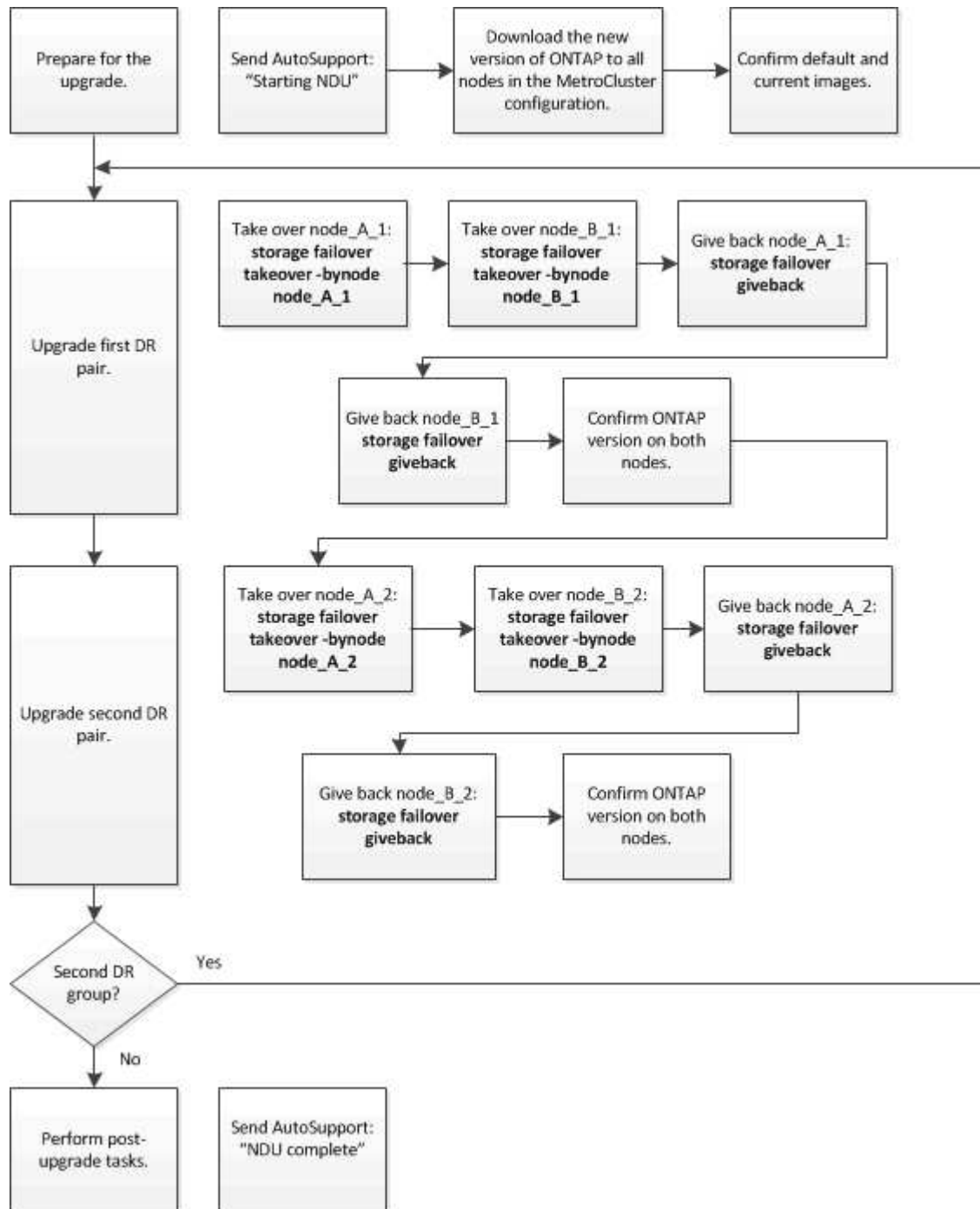
27. 追加の HA ペアがある場合はアップグレードします。

**CLIを使用した4ノードまたは8ノードMetroCluster構成の手動による無停止ONTAPアップグレード**

4ノードまたは8ノードMetroCluster構成の手動アップグレードでは、更新の準備を行い、1つまたは2つのDRグループのそれぞれのDRペアを同時に更新し、アップグレード後の手順を実行します。

- このタスクでは、次の構成を環境に設定します。

- ONTAP 9.2 以前を実行している 4 ノード MetroCluster FC 構成または IP 構成
- ONTAP のバージョンに関係なく、8 ノードの MetroCluster FC 構成
- 2 ノード MetroCluster 構成の場合は、この手順を使用しないでください。
- ここで説明する手順では、ONTAP の古いバージョンと新しいバージョンという表現を使用します。
  - アップグレードの場合、古いバージョンは ONTAP の以前のバージョンで、ONTAP の新しいバージョンよりも下位のバージョン番号が割り当てられます。
  - ダウングレード手順での古いバージョンとは、ONTAP の新しいバージョン、つまり ONTAP の新しいバージョンのバージョン番号よりも上位の番号を持つバージョンを指します。
- このタスクのワークフローは次のとおりです。

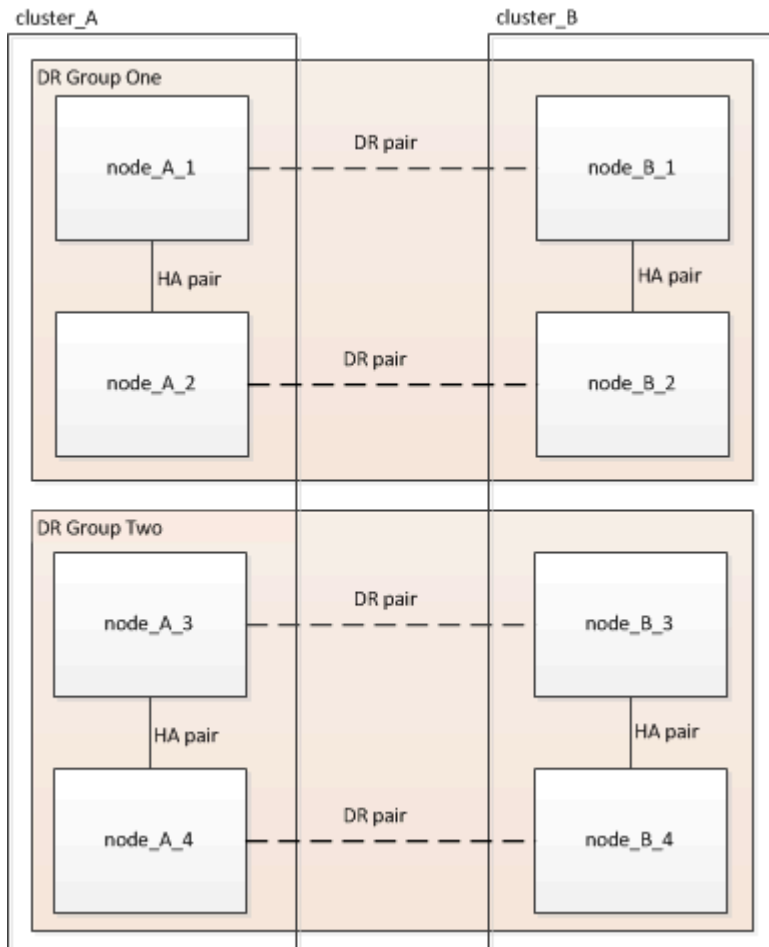




## 8ノードまたは4ノードのMetroCluster構成でONTAPソフトウェアを更新する場合の相違点

MetroClusterソフトウェアのアップグレードプロセスは、MetroCluster構成に8ノードと4ノードのどちらが含まれているかによって異なります。

MetroCluster 構成は、1つまたは2つの DR グループで構成されます。各 DR グループは2つの HA ペアで構成され、各 MetroCluster クラスターに HA ペアが1つずつ配置されます。8 ノードの MetroCluster には、2つの DR グループが含まれています。



DRグループは一度に1つずつアップグレードします。

### 4 ノード MetroCluster 構成の場合：

1. DRグループ1をアップグレードします。
  - a. node\_A\_1とnode\_B\_1をアップグレード
  - b. node\_A\_2とnode\_B\_2をアップグレードします。

8ノードMetroCluster構成の場合は、DRグループのアップグレード手順を2回実行します。

1. DRグループ1をアップグレードします。
  - a. node\_A\_1とnode\_B\_1をアップグレード
  - b. node\_A\_2とnode\_B\_2をアップグレードします。
2. DRグループ2をアップグレードします。

- a. node\_A\_3とnode\_B\_3をアップグレード
- b. node\_A\_4とnode\_B\_4をアップグレード

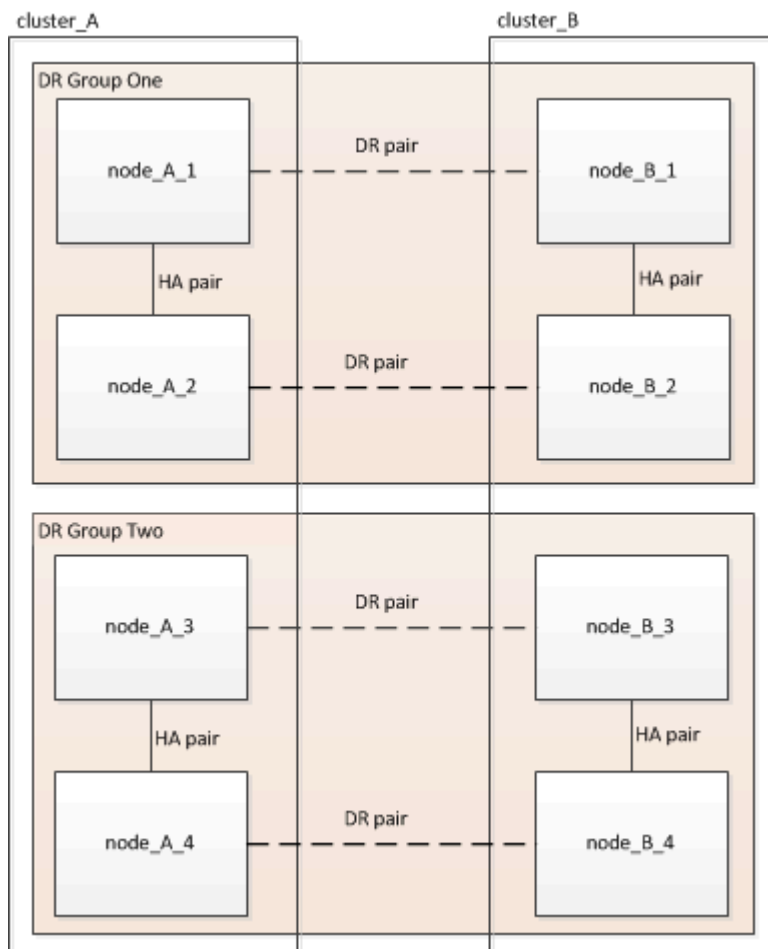
## MetroCluster DRグループをアップグレードする準備

ノードのONTAPソフトウェアをアップグレードする前に、ノード間のDR関係を特定し、アップグレードを開始することを示すAutoSupportメッセージを送信し、各ノードで実行されているONTAPのバージョンを確認する必要があります。

が必要です **"ダウンロードしました"** および **"インストール済み"** ソフトウェアイメージ。

このタスクは DR グループごとに実行する必要があります。MetroCluster 構成が 8 つのノードで構成されている場合は、DR グループが 2 つあります。そのため、DR グループごとにこの手順を繰り返す必要があります。

このタスクの例では、次の図に示すクラスタとノードの名前を使用しています。



1. 構成内のDRペアを特定します。

```
metrocluster node show -fields dr-partner
```

```
cluster_A::> metrocluster node show -fields dr-partner
(metrocluster node show)
dr-group-id cluster      node      dr-partner
-----
1           cluster_A    node_A_1  node_B_1
1           cluster_A    node_A_2  node_B_2
1           cluster_B    node_B_1  node_A_1
1           cluster_B    node_B_2  node_A_2
4 entries were displayed.

cluster_A::>
```

2. 権限レベルをadminからadvancedに設定します。続行するかどうかを尋ねられたら、「\*y\*」と入力します。

```
set -privilege advanced
```

advancedプロンプトが表示されます (\*>) が表示されます。

3. cluster\_AのONTAPバージョンを確認します。

```
system image show
```

```
cluster_A::*> system image show
Node      Image      Is      Is      Version  Install
           Image    Default Current
-----
node_A_1
  image1   true      true    X.X.X    MM/DD/YYYY TIME
  image2   false     false   Y.Y.Y    MM/DD/YYYY TIME
node_A_2
  image1   true      true    X.X.X    MM/DD/YYYY TIME
  image2   false     false   Y.Y.Y    MM/DD/YYYY TIME
4 entries were displayed.

cluster_A::>
```

4. cluster\_Bのバージョンを確認します。

```
system image show
```

```
cluster_B::*> system image show
```

Node	Image	Is Default	Is Current	Version	Install Date
-----					
node_B_1					
	image1	true	true	X.X.X	MM/DD/YYYY TIME
	image2	false	false	Y.Y.Y	MM/DD/YYYY TIME
node_B_2					
	image1	true	true	X.X.X	MM/DD/YYYY TIME
	image2	false	false	Y.Y.Y	MM/DD/YYYY TIME

```
4 entries were displayed.
```

```
cluster_B::>
```

5. AutoSupport 通知を送信します。

```
autosupport invoke -node * -type all -message "Starting_NDU"
```

このAutoSupport通知には、アップグレード前のシステムステータスの記録が含まれます。アップグレードプロセスで問題が発生した場合に役立つトラブルシューティング情報が保存されます。

AutoSupport メッセージを送信するようにクラスタが設定されていない場合は、通知のコピーがローカルに保存されます。

6. 最初のセットに含まれる各ノードについて、ターゲットのONTAP ソフトウェアイメージをデフォルトのイメージとして設定します。

```
system image modify {-node nodename -iscurrent false} -isdefault true
```

このコマンドでは、拡張クエリを使用して、代替イメージとしてインストールされるターゲットのソフトウェアイメージがノードのデフォルトのイメージになるように変更します。

7. ターゲットのONTAPソフトウェアイメージがcluster\_Aでデフォルトのイメージとして設定されたことを確認します。

```
system image show
```

次の例では、image2 が新しい ONTAP バージョンで、最初のセットに含まれる各ノードでデフォルトのイメージとして設定されています。

```
cluster_A::*> system image show
```

Node	Image	Is Default	Is Current	Version	Install Date
-----					
node_A_1	image1	false	true	X.X.X	MM/DD/YYYY TIME
	image2	true	false	Y.Y.Y	MM/DD/YYYY TIME
node_A_2	image1	false	true	X.X.X	MM/DD/YYYY TIME
	image2	true	false	Y.Y.Y	MM/DD/YYYY TIME

2 entries were displayed.

- a. ターゲットのONTAPソフトウェアイメージがcluster\_Bでデフォルトのイメージとして設定されたことを確認します。

```
system image show
```

次の例では、最初のセットに含まれる各ノードで、ターゲットのバージョンがデフォルトのイメージとして設定されています。

```
cluster_B::*> system image show
```

Node	Image	Is Default	Is Current	Version	Install Date
-----					
node_A_1	image1	false	true	X.X.X	MM/DD/YYYY TIME
	image2	true	false	Y.Y.Y	MM/YY/YYYY TIME
node_A_2	image1	false	true	X.X.X	MM/DD/YYYY TIME
	image2	true	false	Y.Y.Y	MM/DD/YYYY TIME

2 entries were displayed.

8. アップグレード対象のノードが各ノードで現在クライアントに対して2回処理を行っているかどうかを確認します。

```
system node run -node target-node -command uptime
```

uptime コマンドは、ノードの前回のブート以降に NFS、CIFS、FC、および iSCSI の各クライアントに対してノードが実行した処理総数を表示します。プロトコルごとにコマンドを 2 回実行して、処理数が増加しているかどうかを確認する必要があります。増加している場合は、そのプロトコルのクライアントに対してノードが現在処理を行っています。増加していない場合は、そのプロトコルのクライアントに対

してノードは現在処理を行っていません。



ノードのアップグレード後にクライアントトラフィックが再開したことを確認できるように、クライアント処理の増加の原因となっている各プロトコルをメモしておく必要があります。

次の例は、NFS、CIFS、FC、および iSCSI の処理が含まれるノードを示しています。ただし、ノードは現在 NFS クライアントと iSCSI クライアントに対してのみ処理を行っています。

```
cluster_x::> system node run -node node0 -command uptime
2:58pm up 7 days, 19:16 800000260 NFS ops, 1017333 CIFS ops, 0 HTTP
ops, 40395 FCP ops, 32810 iSCSI ops

cluster_x::> system node run -node node0 -command uptime
2:58pm up 7 days, 19:17 800001573 NFS ops, 1017333 CIFS ops, 0 HTTP
ops, 40395 FCP ops, 32815 iSCSI ops
```

### MetroCluster DR グループ内の最初の DR ペアの更新

ONTAP の新しいバージョンをノードの現在のバージョンにするには、ノードのテイクオーバーとギブバックを正しい順序で行う必要があります。

すべてのノードで古いバージョンの ONTAP を実行している必要があります。

このタスクでは、node\_A\_1とnode\_B\_1をアップグレードします。

最初のDRグループのONTAPソフトウェアをアップグレードし、8ノードMetroCluster構成の2つ目のDRグループをアップグレードする場合は、この手順でnode\_A\_3とnode\_B\_3を更新します。

1. MetroCluster Tiebreaker ソフトウェアが有効になっている場合は、無効にします。
2. HAペアの各ノードで、自動ギブバックを無効にします。

```
storage failover modify -node target-node -auto-giveback false
```

このコマンドは HA ペアのノードごとに実行する必要があります。

3. 自動ギブバックが無効になったことを確認します。

```
storage failover show -fields auto-giveback
```

次の例は、両方のノードで自動ギブバックが無効になっていることを示しています。

```
cluster_x::> storage failover show -fields auto-giveback
node      auto-giveback
-----
node_x_1  false
node_x_2  false
2 entries were displayed.
```

4. 各コントローラのI/Oが50%を超えていないこと、およびCPU利用率がコントローラあたり50%を超えていないことを確認してください。
5. cluster\_A のターゲットノードのテイクオーバーを開始します。

テイクオーバーされたノードを新しいソフトウェアイメージでブートするには通常のテイクオーバーが必要なため、`-option immediate` パラメータは指定しないでください。

- a. cluster\_A (node\_A\_1) のDRパートナーをテイクオーバーします。

```
storage failover takeover -ofnode node_A_1
```

ノードがブートし、「Waiting for giveback」状態になります。



AutoSupport が有効な場合は、ノードがクラスターフォーラムのメンバーでないことを示す AutoSupport メッセージが送信されます。この通知を無視し、アップグレードを続行してかまいません。

- b. テイクオーバーが正常に完了したことを確認します。

```
storage failover show
```

次の例は、テイクオーバーが正常に完了したことを示しています。node\_A\_1 は「Waiting for giveback」状態、node\_A\_2 は「In takeover」状態です。

```
cluster1::> storage failover show

Node      Partner      Takeover
-----
Possible State Description
-----
node_A_1  node_A_2  -      Waiting for giveback (HA
mailboxes)
node_A_2  node_A_1  false   In takeover
2 entries were displayed.
```

6. cluster\_B (node\_B\_1) のDR パートナーをテイクオーバーします。

テイクオーバーされたノードを新しいソフトウェアイメージでブートするには通常のテイクオーバーが必要なため、`-option immediate` パラメータは指定しないでください。

- a. node\_B\_1をテイクオーバーします。

```
storage failover takeover -ofnode node_B_1
```

ノードがブートし、「Waiting for giveback」状態になります。



AutoSupport が有効な場合は、ノードがクラスターフォーラムのメンバーでないことを示す AutoSupport メッセージが送信されます。この通知を無視し、アップグレードを続行してかまいません。

- b. テイクオーバーが正常に完了したことを確認します。

```
storage failover show
```

次の例は、テイクオーバーが正常に完了したことを示しています。node\_B\_1 が「Waiting for giveback」状態、node\_B\_2 が「In takeover」状態です。

```
cluster1::> storage failover show
```

Node	Partner	Takeover Possible	State Description
node_B_1	node_B_2	-	Waiting for giveback (HA mailboxes)
node_B_2	node_B_1	false	In takeover

2 entries were displayed.

7. 8 分以上待つから、次の条件を満たしていることを確認します。

- クライアントのマルチパス（導入している場合）が安定している。
- クライアントがテイクオーバー中に発生した I/O の中断から回復している。

回復までの時間はクライアントによって異なり、クライアントアプリケーションの特性によっては 8 分以上かかることもあります。

8. アグリゲートをターゲットノードに戻します。

MetroCluster IP 構成を ONTAP 9.5 以降にアップグレードすると、アグリゲートの状態は短時間 degraded になったあとに再同期されて mirrored に戻ります。

- a. アグリゲートを cluster\_A の DR パートナーにギブバックします。



```
storage failover giveback -ofnode node_A_1
```

- b. アグリゲートをcluster\_BのDRパートナーにギブバックします。

```
storage failover giveback -ofnode node_B_1
```

ギブバック処理では、最初にルートアグリゲートがノードに戻され、そのノードのブートが完了するとルート以外のアグリゲートが戻されます。

9. 両方のクラスタで次のコマンドを実行して、すべてのアグリゲートが戻されたことを確認します。

```
storage failover show-giveback
```

Giveback Status フィールドにギブバックするアグリゲートがないことが示されている場合は、すべてのアグリゲートが戻されています。ギブバックが拒否された場合は、コマンドによってギブバックの進捗が表示され、ギブバックを拒否したサブシステムも表示されます。

10. いずれかのアグリゲートが戻されていない場合は、次の手順を実行します。
- 拒否された回避策を確認して、「ve to」状態に対処するか、拒否を無視するかを決定します。
  - 必要に応じて、エラーメッセージに記載されている「宛」の状態に対処し、特定された処理が正常に終了するようにします。
  - storage failover giveback コマンドを再度入力します。

「''' ~ '''」条件をオーバーライドする場合は、-override-vetoes パラメータを true に設定します。

11. 8 分以上待ってから、次の条件を満たしていることを確認します。
- クライアントのマルチパス（導入している場合）が安定している。
  - クライアントがギブバック中に発生した I/O の中断から回復している。

回復までの時間はクライアントによって異なり、クライアントアプリケーションの特性によっては 8 分以上かかることもあります。

12. 権限レベルをadminからadvancedに設定します。続行するかどうかを尋ねられたら、「\* y \*」と入力します。

```
set -privilege advanced
```

advancedプロンプトが表示されます (\*>) が表示されます。

13. cluster\_Aのバージョンを確認します。

```
system image show
```

次の例は、System image2 が node\_A\_1 のデフォルトおよび現在のバージョンであることを示しています。

```
cluster_A::*> system image show
```

Node	Image	Is Default	Is Current	Version	Install Date
-----					
node_A_1					
	image1	false	false	X.X.X	MM/DD/YYYY TIME
	image2	true	true	Y.Y.Y	MM/DD/YYYY TIME
node_A_2					
	image1	false	true	X.X.X	MM/DD/YYYY TIME
	image2	true	false	Y.Y.Y	MM/DD/YYYY TIME

4 entries were displayed.

```
cluster_A::>
```

#### 14. cluster\_Bのバージョンを確認します。

```
system image show
```

次の例は、System image2（ONTAP 9.0.0）が node\_A\_1 のデフォルトおよび現在のバージョンであることを示しています。

```
cluster_A::*> system image show
```

Node	Image	Is Default	Is Current	Version	Install Date
-----					
node_B_1					
	image1	false	false	X.X.X	MM/DD/YYYY TIME
	image2	true	true	Y.Y.Y	MM/DD/YYYY TIME
node_B_2					
	image1	false	true	X.X.X	MM/DD/YYYY TIME
	image2	true	false	Y.Y.Y	MM/DD/YYYY TIME

4 entries were displayed.

```
cluster_A::>
```

### MetroCluster DR グループ内の 2 つ目の DR ペアの更新

ONTAP の新しいバージョンをノードの現在のバージョンにするには、ノードのテイクオーバーとギブバックを正しい順序で行う必要があります。

最初の DR ペア（node\_A\_1 と node\_B\_1）をアップグレードしておく必要があります。

このタスクでは、node\_A\_2とnode\_B\_2をアップグレードします。

最初のDRグループのONTAPソフトウェアをアップグレードし、8ノードMetroCluster構成の2つ目のDRグループを更新する場合は、この手順でnode\_A\_4とnode\_B\_4を更新します。

1. ノードからすべてのデータLIFを移行します。

```
network interface migrate-all -node nodenameA
```

2. cluster\_A のターゲットノードのテイクオーバーを開始します。

テイクオーバーされたノードを新しいソフトウェアイメージでブートするには通常のテイクオーバーが必要なため、-option immediate パラメータは指定しないでください。

- a. cluster\_A の DR パートナーをテイクオーバーします。

```
storage failover takeover -ofnode node_A_2 -option allow-version-mismatch
```



。allow-version-mismatch ONTAP 9.0からONTAP 9.1へのアップグレードやパッチのアップグレードでは、オプションは必要ありません。

ノードがブートし、「Waiting for giveback」状態になります。

AutoSupport が有効な場合は、ノードがクラスタフォーラムのメンバーでないことを示す AutoSupport メッセージが送信されます。この通知を無視し、アップグレードを続行してかまいません。

- b. テイクオーバーが正常に完了したことを確認します。

```
storage failover show
```

次の例は、テイクオーバーが正常に完了したことを示しています。Node\_a\_2 の状態が Waiting for giveback 、 node\_A\_1 の状態が In takeover になっています。

```
cluster1::> storage failover show
```


Node	Partner	Takeover Possible	State Description
node_A_1	node_A_2	false	In takeover
node_A_2	node_A_1	-	Waiting for giveback (HA mailboxes)

2 entries were displayed.

3. cluster\_B のターゲットノードのテイクオーバーを開始します。

テイクオーバーされたノードを新しいソフトウェアイメージでブートするには通常のテイクオーバーが必要のため、-option immediate パラメータは指定しないでください。

a. cluster\_B (node\_B\_2) のDRパートナーをテイクオーバーします。

アップグレード前のバージョン	入力するコマンド
ONTAP 9.2 または ONTAP 9.1	<pre>storage failover takeover -ofnode node_B_2</pre>
ONTAP 9.0 または Data ONTAP 8.3.x	<pre>storage failover takeover -ofnode node_B_2 -option allow- version-mismatch</pre> <div>。 allow-version-mismatch ONTAP 9.0からONTAP 9.1へのア ップグレードやパッチのアップグ レードでは、オプションは必要あ りません。</div>

ノードがブートし、「Waiting for giveback」状態になります。



AutoSupportが有効な場合は、ノードがクラスタフォーラムのメンバーでないことを示すAutoSupportメッセージが送信されます。この通知を無視し、アップグレードを続行してかまいません。

b. テイクオーバーが正常に完了したことを確認します。

```
storage failover show
```

次の例は、テイクオーバーが正常に完了したことを示しています。node\_B\_2 は「Waiting for giveback」状態、node\_B\_1 は「In takeover」状態です。

```
cluster1::> storage failover show
```

Node	Partner	Takeover Possible	State Description
node_B_1	node_B_2	false	In takeover
node_B_2	node_B_1	-	Waiting for giveback (HA mailboxes)

2 entries were displayed.

4. 8 分以上待ってから、次の条件を満たしていることを確認します。

- クライアントのマルチパス（導入している場合）が安定している。
- クライアントがテイクオーバー中に発生した I/O の中断から回復している。

回復までの時間はクライアントによって異なり、クライアントアプリケーションの特性によっては 8 分以上かかることもあります。

5. アグリゲートをターゲットノードに戻します。

MetroCluster IP 構成を ONTAP 9.5 にアップグレードすると、アグリゲートの状態は短時間 degraded になったあとに再同期されて mirrored に戻ります。

a. アグリゲートを cluster\_A の DR パートナーにギブバックします。

```
storage failover giveback -ofnode node_A_2
```

b. アグリゲートを cluster\_B の DR パートナーにギブバックします。

```
storage failover giveback -ofnode node_B_2
```

ギブバック処理では、最初にルートアグリゲートがノードに戻され、そのノードのブートが完了するとルート以外のアグリゲートが戻されます。

6. 両方のクラスタで次のコマンドを実行して、すべてのアグリゲートが戻されたことを確認します。

```
storage failover show-giveback
```

Giveback Status フィールドにギブバックするアグリゲートがないことが示されている場合は、すべてのアグリゲートが戻されています。ギブバックが拒否された場合は、コマンドによってギブバックの進捗が表示され、ギブバックを拒否したサブシステムも表示されます。

7. いずれかのアグリゲートが戻されていない場合は、次の手順を実行します。

- a. 拒否された回避策を確認して、「ve to」状態に対処するか、拒否を無視するかを決定します。

- b. 必要に応じて、エラーメッセージに記載されている「宛」の状態に対処し、特定された処理が正常に終了するようにします。
- c. storage failover giveback コマンドを再度入力します。

「''' ~ '''」条件をオーバーライドする場合は、-override-vetoes パラメータを true に設定します。

8. 8 分以上待ってから、次の条件を満たしていることを確認します。

- クライアントのマルチパス（導入している場合）が安定している。
- クライアントがギブバック中に発生した I/O の中断から回復している。

回復までの時間はクライアントによって異なり、クライアントアプリケーションの特性によっては 8 分以上かかることもあります。

9. 権限レベルを admin から advanced に設定します。続行するかどうかを尋ねられたら、「\*y\*」と入力します。

```
set -privilege advanced
```

advanced プロンプトが表示されます (\*>) が表示されます。

10. cluster\_A のバージョンを確認します。

```
system image show
```

次の例は、System image2（ターゲットの ONTAP イメージ）が node\_A\_2 のデフォルトおよび現在のバージョンであることを示しています。

```
cluster_B::*> system image show
```

Node	Image	Is Default	Is Current	Version	Install Date
node_A_1					
	image1	false	false	X.X.X	MM/DD/YYYY TIME
	image2	true	true	Y.Y.Y	MM/DD/YYYY TIME
node_A_2					
	image1	false	false	X.X.X	MM/DD/YYYY TIME
	image2	true	true	Y.Y.Y	MM/DD/YYYY TIME

4 entries were displayed.

```
cluster_A::>
```

11. cluster\_B のバージョンを確認します。

```
system image show
```

次の例は、System image2（ターゲットのONTAPイメージ）がnode\_B\_2のデフォルトかつ現在のバージョンであることを示しています。

```
cluster_B::*> system image show
```

Node	Image	Is Default	Is Current	Version	Install Date
node_B_1					
	image1	false	false	X.X.X	MM/DD/YYYY TIME
	image2	true	true	Y.Y.Y	MM/DD/YYYY TIME
node_B_2					
	image1	false	false	X.X.X	MM/DD/YYYY TIME
	image2	true	true	Y.Y.Y	MM/DD/YYYY TIME

4 entries were displayed.

```
cluster_A::>
```

12. HAペアの各ノードで、自動ギブバックを有効にします。

```
storage failover modify -node target-node -auto-giveback true
```

このコマンドは HA ペアのノードごとに実行する必要があります。

13. 自動ギブバックが有効になったことを確認します。

```
storage failover show -fields auto-giveback
```

次の例では、両方のノードで自動ギブバックが有効になっています。

```
cluster_x::> storage failover show -fields auto-giveback
```

node	auto-giveback
node_x_1 true	
node_x_2 true	

2 entries were displayed.

**ONTAP 9.2**以前の2ノード**MetroCluster**構成の無停止アップグレード

2ノード**MetroCluster**構成のアップグレード方法は、ONTAPのバージョンによって異なり

ます。ONTAP 9.2以前を実行している場合は、この手順を使用して手動による無停止アップグレードを実行します。具体的には、ネゴシエートスイッチオーバーを開始し、「障害」サイトでクラスタを更新してから、スイッチバックを開始します。この処理をもう一方のサイトのクラスタでも繰り返します。

ONTAP 9.3以降を実行している2ノードMetroCluster構成の場合は、[System Managerを使用した自動アップグレード](#)。

#### 手順

1. 権限レベルをadvancedに設定します。続行するかどうかを尋ねられたら、「\*y\*」と入力します。

```
set -privilege advanced
```

advancedプロンプトが表示されます (\*>) が表示されます。

2. アップグレードするクラスタで、新しいONTAP ソフトウェアイメージをデフォルトとしてインストールします。

```
system node image update -package package_location -setdefault true  
-replace-package true
```

```
cluster_B::*> system node image update -package  
http://www.example.com/NewImage.tgz -setdefault true -replace-package  
true
```

3. ターゲットのソフトウェアイメージがデフォルトのイメージとして設定されたことを確認します。

```
system node image show
```

次の例はそれを示しています NewImage デフォルトのイメージとして設定されています。

```
cluster_B::*> system node image show
```

Node	Image	Is Default	Is Current	Version	Install Date
node_B_1					
	OldImage	false	true	X.X.X	MM/DD/YYYY TIME
	NewImage	true	false	Y.Y.Y	MM/DD/YYYY TIME

2 entries were displayed.



- ターゲットのソフトウェアイメージがデフォルトのイメージとして設定されていない場合は、変更します。

```
system image modify {-node * -iscurrent false} -isdefault true
```

- すべてのクラスタSVMが健全な状態であることを確認します。

```
metrocluster vservers show
```

- 更新されていないクラスタで、ネゴシエートスイッチオーバーを開始します。

```
metrocluster switchover
```

この処理には数分かかることがあります。MetroCluster operation show コマンドを使用して、スイッチオーバーが完了したことを確認できます。

次の例では、ネゴシエート・スイッチオーバーがリモート・クラスタ ("cluster\_a") 上で実行されます。これにより、ローカルクラスタ ("cluster\_B") が停止し、更新できるようになります。

```
cluster_A::> metrocluster switchover

Warning: negotiated switchover is about to start. It will stop all the
data
      Vservers on cluster "cluster_B" and
      automatically re-start them on cluster
      "cluster_A". It will finally gracefully shutdown
      cluster "cluster_B".
Do you want to continue? {y|n}: y
```

- すべてのクラスタSVMが健全な状態であることを確認します。

```
metrocluster vservers show
```

- 「Surviving」クラスタ上のデータアグリゲートを再同期します。

```
metrocluster heal -phase aggregates
```

MetroCluster IP 構成を ONTAP 9.5 以降にアップグレードすると、アグリゲートの状態は短時間 degraded になったあとに再同期されて mirrored に戻ります。

```
cluster_A::> metrocluster heal -phase aggregates
[Job 130] Job succeeded: Heal Aggregates is successful.
```

9. 修復処理が正常に完了したことを確認します。

```
metrocluster operation show
```

```
cluster_A::> metrocluster operation show
Operation: heal-aggregates
State: successful
Start Time: MM/DD/YYYY TIME
End Time: MM/DD/YYYY TIME
Errors: -
```

10. 「Surviving」 クラスタのルートアグリゲートを再同期します。

```
metrocluster heal -phase root-aggregates
```

```
cluster_A::> metrocluster heal -phase root-aggregates
[Job 131] Job succeeded: Heal Root Aggregates is successful.
```

11. 修復処理が正常に完了したことを確認します。

```
metrocluster operation show
```

```
cluster_A::> metrocluster operation show
Operation: heal-root-aggregates
State: successful
Start Time: MM/DD/YYYY TIME
End Time: MM/DD/YYYY TIME
Errors: -
```

12. 停止したクラスタで、LOADERプロンプトからノードをブートします。

```
boot_ontap
```

13. ブートプロセスの終了を待ってから、すべてのクラスタSVMが健全な状態であることを確認します。

```
metrocluster vserver show
```

14. 「Surviving」 クラスタからスイッチバックを実行します。

```
metrocluster switchback
```

15. スイッチバックが正常に完了したことを確認します。

```
metrocluster operation show
```

```
cluster_A::> metrocluster operation show
Operation: switchback
State: successful
Start Time: MM/DD/YYYY TIME
End Time: MM/DD/YYYY TIME
Errors: -
```

16. すべてのクラスタSVMが健全な状態であることを確認します。

```
metrocluster vserver show
```

17. もう一方のクラスタで、ここまでのすべての手順を繰り返します。

18. MetroCluster 構成が正常であることを確認します。

- a. 構成を確認します。

```
metrocluster check run
```

```
cluster_A::> metrocluster check run
```

```
Last Checked On: MM/DD/YYYY TIME
```

Component	Result
nodes	ok
lifs	ok
config-replication	ok
aggregates	ok

```
4 entries were displayed.
```

Command completed. Use the "metrocluster check show -instance" command or sub-commands in "metrocluster check" directory for detailed results.

To check if the nodes are ready to do a switchover or switchback operation, run "metrocluster switchover -simulate" or "metrocluster switchback -simulate", respectively.

- b. より詳細な結果を表示するには、MetroCluster check runコマンドを使用します。

```
metrocluster check aggregate show
```

```
metrocluster check config-replication show
```

```
metrocluster check lif show
```

```
metrocluster check node show
```

- c. 権限レベルを advanced に設定します。

```
set -privilege advanced
```

- d. スイッチオーバー処理をシミュレートします。

```
metrocluster switchover -simulate
```

- e. スイッチオーバーのシミュレーション結果を確認します。

```
metrocluster operation show
```

```
cluster_A::*> metrocluster operation show
  Operation: switchover
    State: successful
  Start time: MM/DD/YYYY TIME
  End time: MM/DD/YYYY TIME
  Errors: -
```

f. admin 権限レベルに戻ります。

```
set -privilege admin
```

g. もう一方のクラスタで上記の手順を繰り返します。

完了後

いずれかを実行 ["アップグレードゴノテジュン"](#)。

関連情報

["MetroCluster によるディザスタリカバリ"](#)

CLIを使用した手動による停止を伴うONTAPアップグレード

新しい ONTAP リリースにアップグレードする際にクラスタをオフラインにしてもかまわない場合は、停止を伴うアップグレードを使用できます。この方式では、各 HA ペアのストレージフェイルオーバーを無効にして、クラスタ内の各ノードをリブートし、完了したらストレージフェイルオーバーを再度有効にします。

- 実行する必要があります ["ダウンロード"](#) および ["をインストールします"](#) ソフトウェアイメージ。
- SAN 環境を使用している場合は、すべての SAN クライアントをシャットダウンするか、アップグレードが完了するまで一時停止する必要があります。

停止を伴うアップグレードの前に SAN クライアントをシャットダウンまたは一時停止しないと、クライアントファイルシステムおよびアプリケーションでエラーが発生し、アップグレードの完了後に手動によるリカバリが必要になる可能性があります。

停止を伴うアップグレードでは、各 HA ペアのストレージフェイルオーバーを無効にして各ノードを更新するため、ダウンタイムが必要です。ストレージフェイルオーバーを無効にすると、各ノードはシングルノードクラスタとして動作します。つまり、ノードに関連するシステムサービスは、システムをリブートするまで中断されます。

手順

1. 権限レベルをadminからadvancedに設定します。続行するかどうかを尋ねられたら、「\* y \*」と入力します。

```
set -privilege advanced
```

advancedプロンプトが表示されます (\*>) が表示されます。

2. 新しいONTAP ソフトウェアイメージをデフォルトのイメージとして設定します。

```
system image modify {-node * -iscurrent false} -isdefault true
```

このコマンドでは、拡張クエリを使用して、代替イメージとしてインストールされるターゲットのONTAP ソフトウェアイメージが各ノードのデフォルトのイメージになるように変更します。

3. 新しいONTAP ソフトウェアイメージがデフォルトのイメージとして設定されたことを確認します。

```
system image show
```

次の例では、イメージ 2 が新しい ONTAP バージョンであり、両方のノードでデフォルトのイメージとして設定されています。

```
cluster1::*> system image show
```

Node	Image	Is Default	Is Current	Version	Install Date
node0					
	image1	false	true	X.X.X	MM/DD/YYYY TIME
	image2	true	false	Y.Y.Y	MM/DD/YYYY TIME
node1					
	image1	false	true	X.X.X	MM/DD/YYYY TIME
	image2	true	false	Y.Y.Y	MM/DD/YYYY TIME

4 entries were displayed.

4. 次のいずれかの手順を実行します。

クラスタの構成	手順
1つのノードです	次の手順に進みます。

クラスタの構成	手順
2 ノード	<p>a. クラスタのハイアベイラビリティを無効にします。</p> <pre>cluster ha modify -configured false</pre> <p>入力するコマンド y プロンプトが表示されたら続行します。</p> <p>b. HAペアのストレージフェイルオーバーを無効にします。</p> <pre>storage failover modify -node * -enabled false</pre>
3 ノード以上	<p>クラスタ内の各HAペアのストレージフェイルオーバーを無効にします。</p> <pre>storage failover modify -node * -enabled false</pre>

5. クラスタ内のノードをリブートします。

```
system node reboot -node nodename -ignore-quorum-warnings
```



一度に複数のノードをリブートしないでください。

ノードが新しい ONTAP イメージでブートします。ONTAP ログインプロンプトが表示され、リブートプロセスが完了したことが示されます。

6. ノードまたはノードセットが新しいONTAP イメージでリブートされたら、権限レベルをadvancedに設定します。

```
set -privilege advanced
```

続行するかどうかを尋ねられたら、「\* y \*」と入力します

7. 新しいソフトウェアが実行されていることを確認します。

```
system node image show
```

次の例では、image1 が新しい ONTAP バージョンで、node0 で現在のバージョンとして設定されています。

```
cluster1::*> system node image show
```

Node	Image	Is Default	Is Current	Version	Install Date
node0	image1	true	true	X.X.X	MM/DD/YYYY TIME
	image2	false	false	Y.Y.Y	MM/DD/YYYY TIME
node1	image1	true	false	X.X.X	MM/DD/YYYY TIME
	image2	false	true	Y.Y.Y	MM/DD/YYYY TIME

4 entries were displayed.

8. アップグレードが正常に完了したことを確認します。

a. 権限レベルを advanced に設定します。

```
set -privilege advanced
```

b. 各ノードのアップグレードステータスが完了になっていることを確認します。

```
system node upgrade-revert show -node nodename
```

ステータスが complete になっている必要があります。

ステータスがcompleteになっていない場合は、["ネットアップサポートにお問い合わせください"](#) すぐに。

a. admin 権限レベルに戻ります。

```
set -privilege admin
```

9. 追加するノードごとに、手順2~8を繰り返します。

10. クラスタが複数のノードで構成されている場合は、クラスタ内の各HAペアのストレージフェイルオーバーを有効にします。

```
storage failover modify -node * -enabled true
```



11. クラスタが2つのノードだけで構成されている場合は、クラスタのハイアベイラビリティを有効にします。

```
cluster ha modify -configured true
```

## ONTAPアップグレード後の作業

### ONTAPアップグレード後の作業

ONTAPをアップグレードしたら、クラスタの準備状況を確認するためにいくつかのタスクを実行する必要があります。

1. ["クラスタを確認します"](#)。

ONTAPをアップグレードしたら、クラスタのバージョン、クラスタの健全性、およびストレージの健全性を確認する必要があります。MetroCluster FC 構成を使用している場合は、クラスタで自動計画外スイッチオーバーが有効になっていることも確認する必要があります。

2. ["すべてのLIFがホームポートにあることを確認する"](#)。

リブートを実行すると、一部の LIF が割り当てられているフェイルオーバーポートに移行されることがあります。クラスタのアップグレードが完了したら、ホームポートにない LIF を有効にしてリポートする必要があります。

3. 確認します ["特別な考慮事項"](#) 使用しているクラスタに固有です。

クラスタに特定の構成が存在する場合は、アップグレード後に追加の手順を実行する必要があります。

4. ["Disk Qualification Package \(DQP\) を更新する"](#)。

ONTAP のアップグレードの一環として DQP が更新されることはありません。

### ONTAPのアップグレード後のクラスタの確認

ONTAPをアップグレードしたら、クラスタのバージョン、クラスタの健全性、およびストレージの健全性を確認します。MetroCluster FC構成の場合は、クラスタで自動計画外スイッチオーバーが有効になっていることも確認します。

#### クラスタのバージョンを確認

すべてのHAペアをアップグレードしたら、versionコマンドを使用して、すべてのノードでターゲットリリースが実行されていることを確認する必要があります。

クラスタのバージョンは、クラスタ内のいずれかのノードで実行されている ONTAP の最下位のバージョンです。クラスタのバージョンがターゲットの ONTAP リリースになっていない場合は、クラスタをアップグレードできます。

1. クラスタのバージョンがターゲットの ONTAP リリースになっていることを確認します。

```
version
```

2. クラスタのバージョンがターゲットのONTAPリリースになっていない場合は、すべてのノードのアップグレードステータスを確認する必要があります。

```
system node upgrade-revert show
```

クラスタの健全性を確認

クラスタをアップグレードしたら、ノードが正常に機能していてクラスタに追加するための条件を満たしていること、およびクラスタがクォーラムにあることを確認する必要があります。

1. クラスタ内のノードがオンラインで、クラスタに追加するための条件を満たしていることを確認します。

```
cluster show
```

```
cluster1::> cluster show
Node                               Health  Eligibility
-----
node0                             true    true
node1                             true    true
```

正常に機能していないノードや条件を満たしていないノードがある場合は、EMS ログでエラーを確認して適切に修正します。

2. 権限レベルを advanced に設定します。

```
set -privilege advanced
```

3. 各 RDB プロセスの構成の詳細を確認します。

- リレーショナルデータベースのエポックとデータベースのエポックが各ノードで一致すること。
- リングごとのクォーラムマスターがすべてのノードで同じであることが必要です。

各リングのクォーラムマスターが異なる場合があることに注意してください。

表示する RDB プロセス	入力するコマンド
管理アプリケーション	cluster ring show -unitname mgmt
ボリュームロケーションデータベース	cluster ring show -unitname vlddb

仮想インターフェイスマネージャ	cluster ring show -unitname vifmgr
SAN 管理デーモン	cluster ring show -unitname bcomd

次の例は、ボリュームロケーションデータベースのプロセスを示しています。

```
cluster1::*> cluster ring show -unitname vlddb
```

Node	UnitName	Epoch	DB Epoch	DB Trnxs	Master	Online
node0	vlddb	154	154	14847	node0	master
node1	vlddb	154	154	14847	node0	secondary
node2	vlddb	154	154	14847	node0	secondary
node3	vlddb	154	154	14847	node0	secondary

4 entries were displayed.

4. SAN 環境を使用している場合は、各ノードが SAN クォーラムにあることを確認します。

```
cluster kernel-service show
```

```
cluster1::*> cluster kernel-service show
```

Master	Cluster	Quorum	Availability
Operational			
Node	Node	Status	Status
cluster1-01	cluster1-01	in-quorum	true
operational	cluster1-02	in-quorum	true
operational			

2 entries were displayed.

## 関連情報

### "システム管理"

自動計画外スイッチオーバーが有効になっていることを確認する（MetroCluster FC構成のみ）

クラスタがMetroCluster FC構成の場合は、ONTAPのアップグレード後に自動計画外スイッチオーバーが有効になっていることを確認する必要があります。

MetroCluster IP 構成を使用している場合は、この手順 を省略してください。

## 手順

1. 自動計画外スイッチオーバーが有効かどうかを確認します。

```
metrocluster show
```

自動計画外スイッチオーバーが有効な場合、コマンド出力に次のステートメントが表示されます。

```
AUSO Failure Domain  auso-on-cluster-disaster
```

2. ステートメントが表示されない場合は、自動計画外スイッチオーバーを有効にします。

```
metrocluster modify -auto-switchover-failure-domain auso-on-cluster-disaster
```

3. 自動計画外スイッチオーバーが有効になっていることを確認します。

```
metrocluster show
```

#### 関連情報

["ディスクおよびアグリゲートの管理"](#)

**ONTAP**のアップグレード後にすべての**LIF**がホームポートにあることを確認する

ONTAPのアップグレードプロセス中に発生するリブートの際に、一部のLIFがホームポートから割り当てられたフェイルオーバーポートに移行されることがあります。アップグレード後、ホームポートにないLIFを有効にしてリバートする必要があります。

#### 手順

1. すべてのLIFのステータスを表示します。

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

いずれかのLIFについて、\* Status Admin が「**down**」または is home \*が「false」の場合は、次の手順に進みます。

2. データLIFを有効にします。

```
network interface modify {-role data} -status-admin up
```

3. LIFをそれぞれのホームポートにリバートします。

```
network interface revert *
```

4. すべてのLIFがそれぞれのホームポートにあることを確認します。

```
network interface show
```

次の例では、SVM vs0 のすべての LIF がそれぞれのホームポートにあります。

```
cluster1::> network interface show -vserver vs0
```

Vserver	Logical Interface	Status Admin/Oper	Network Address/Mask	Current Node	Current Port	Is Home
vs0						
	data001	up/up	192.0.2.120/24	node0	e0e	true
	data002	up/up	192.0.2.121/24	node0	e0f	true
	data003	up/up	192.0.2.122/24	node0	e2a	true
	data004	up/up	192.0.2.123/24	node0	e2b	true
	data005	up/up	192.0.2.124/24	node1	e0e	true
	data006	up/up	192.0.2.125/24	node1	e0f	true
	data007	up/up	192.0.2.126/24	node1	e2a	true
	data008	up/up	192.0.2.127/24	node1	e2b	true

8 entries were displayed.

## 特殊な構成

### ONTAPアップグレード後の特別な考慮事項

クラスタに次のいずれかの機能が設定されている場合は、ONTAPソフトウェアのアップグレード後に追加の手順の実行が必要になることがあります。

自分自身に尋ねる ...	回答が * はい * の場合、次の操作を実行します ...
ONTAP 9.7以前からONTAP 9.8以降にアップグレードしましたか？	<a href="#">ネットワーク構成を確認します</a>  EMSデスティネーションへの到達不能を提供しないネットワークサービスポリシーからEMS LIFサービスを削除します
クラスタはMetroCluster構成に含まれていますか。	<a href="#">ネットワークとストレージのステータスを確認します</a>
SAN 構成を使用していますか。	<a href="#">SAN 構成を確認</a>
ONTAP 9.3以前からアップグレードし、NetAppストレージ暗号化を使用していますか？	<a href="#">KMIP サーバの接続を再設定する</a>
負荷共有ミラーがありますか？	<a href="#">移動した負荷共有ミラーのソースボリュームを再配置します</a>

自分自身に尋ねる ...	回答が * はい * の場合、次の操作を実行します ...
ONTAP 9.9.1より前のバージョンで作成されたサービスプロセッサ（SP）アクセスのユーザアカウントがあるか	<a href="#">サービスプロセッサにアクセスできるアカウントの変更を確認します</a>

#### ONTAP 9.7x以前からのONTAPアップグレード後のネットワーク構成の確認

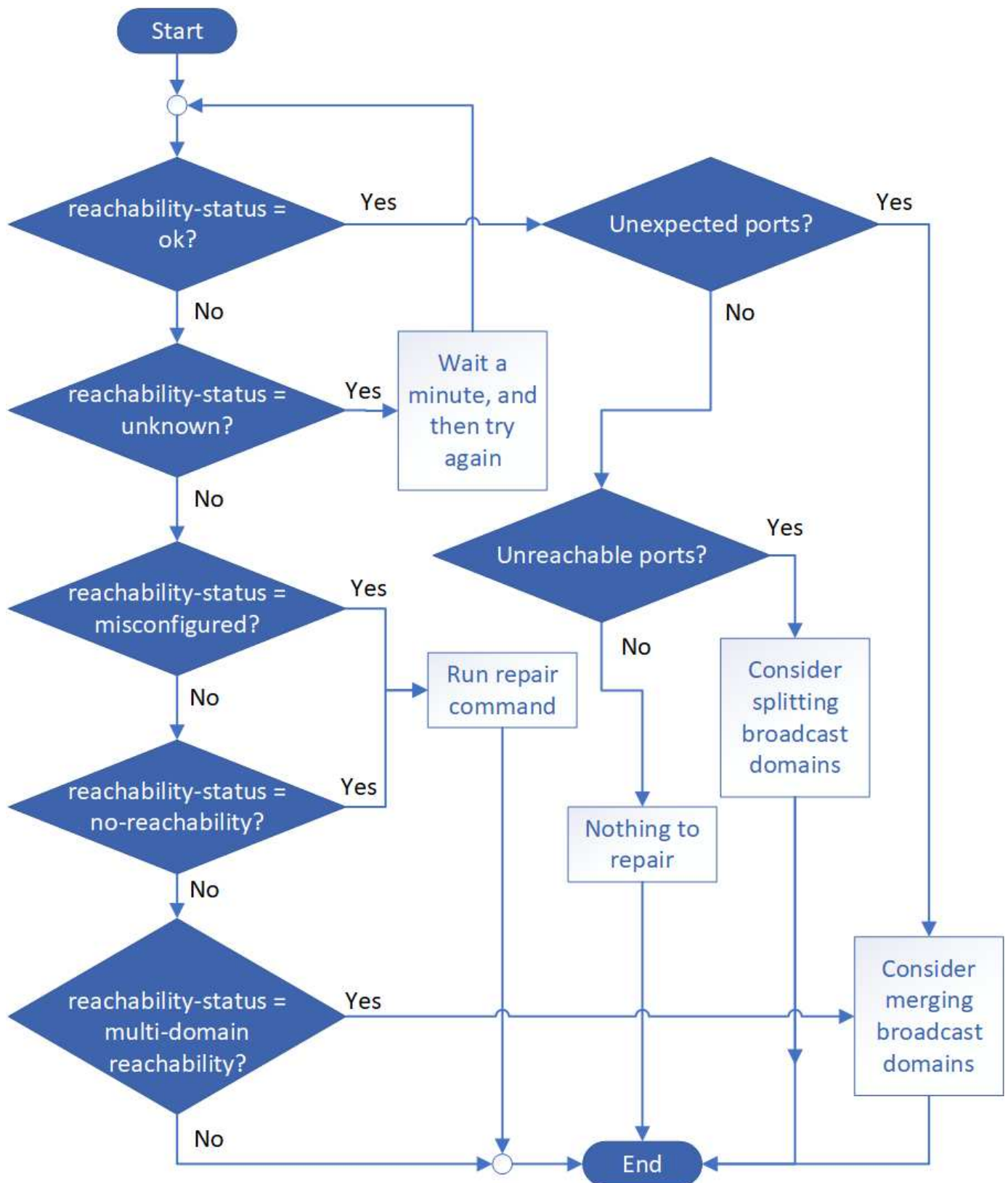
ONTAP 9.7x以前のバージョンからONTAP 9.8以降にアップグレードしたら、ネットワーク構成を確認する必要があります。アップグレード後、ONTAP は自動的にレイヤ 2 の到達可能性を監視します。

#### ステップ

1. 各ポートに想定されるブロードキャストドメインへの到達可能性があることを確認します。

```
network port reachability show -detail
```

コマンド出力に到達可能性の結果が含まれています。次のデシジョンツリーとテーブルを使用して、到達可能性の結果（reachable-status）を理解し、次に何を実行するか（存在する場合）を決定します。



プレゼンスステータス	説明
------------	----

わかりました	<p>ポートに割り当てられているブロードキャストドメインにレイヤ 2 の到達可能性があります。</p> <p>reachable-status が「OK」であるのに、「予想外のポート」がある場合は、1 つ以上のブロードキャストドメインをマージすることを検討してください。詳細については、を参照してください <a href="#">"ブロードキャストドメインをマージします"</a>。</p> <p>reachable-status が「OK」であるが、「到達不能ポート」がある場合は、1 つ以上のブロードキャストドメインをスプリットすることを検討してください。詳細については、を参照してください <a href="#">"ブロードキャストドメインをスプリットします"</a>。</p> <p>reachable-status が「OK」で、予期しないポートや到達不能なポートがない場合は、設定が正しいことを確認してください。</p>
誤設定 - 到達可能性	<p>ポートに割り当てられているブロードキャストドメインにレイヤ 2 に到達できるかどうかは関係ありませんが、ポートは別のブロードキャストドメインにレイヤ 2 に到達できるかどうかは関係ありません。</p> <p>ポートに到達できるかどうかを修復できます。次のコマンドを実行すると、ポートに到達できるブロードキャストドメインにポートが割り当てられます。</p> <pre>network port reachability repair -node -port</pre> <p>詳細については、を参照してください <a href="#">"ポートの到達可能性を修復します"</a>。</p>
到達不能	<p>既存のどのブロードキャストドメインにもレイヤ 2 で接続できません。</p> <p>ポートに到達できるかどうかを修復できます。次のコマンドを実行すると、自動的に作成されたデフォルトの IPspace 内の新しいブロードキャストドメインにポートが割り当てられます。</p> <pre>network port reachability repair -node -port</pre> <p>詳細については、を参照してください <a href="#">"ポートの到達可能性を修復します"</a>。</p>
multi-domain-reachable	<p>ポートには、割り当てられたブロードキャストドメインにレイヤ 2 に到達できることがあります。少なくとも 1 つの他のブロードキャストドメインにレイヤ 2 に到達できることもあります。</p> <p>物理的な接続とスイッチの設定を調べて、正しくないか、またはポートに割り当てられているブロードキャストドメインを 1 つ以上のブロードキャストドメインにマージする必要があるかどうかを確認します。</p> <p>詳細については、を参照してください <a href="#">"ブロードキャストドメインをマージします"</a> または <a href="#">"ポートの到達可能性を修復します"</a>。</p>
不明です	<p>reachable-status が「unknown」の場合は、数分待ってからもう一度コマンドを実行してください。</p>

ポートを修復したら、取り外された LIF や VLAN を確認して解決する必要があります。ポートがインターフ



エイスグループに属していた場合は、そのインターフェイスグループに何が起こったかを理解する必要もあります。詳細については、を参照してください ["ポートの到達可能性を修復します"](#)。

ネットワークサービスポリシーから**EMS LIF**サービスを削除します

ONTAP 9.7以前からONTAP 9.8以降にアップグレードする前にEvent Management System (EMS ; イベント管理システム) メッセージを設定していた場合は、アップグレード後にEMSメッセージが配信されないことがあります。

アップグレードでは、EMS LIFサービスであるmanagement-emsが既存のすべてのサービスポリシーに追加されます。これにより、いずれかのサービスポリシーに関連付けられたいずれかのLIFからEMSメッセージを送信できます。選択したLIFにイベント通知の送信先への到達可能性がない場合、メッセージは配信されません。

これを回避するには、アップグレード後に、デスティネーションに到達できないネットワークサービスポリシーからEMS LIFサービスを削除します。

#### 手順

1. EMSメッセージの送信に使用できるLIFと関連付けられたネットワークサービスポリシーを特定します。

```
network interface show -fields service-policy -services management-ems
```

vserver	lif	service-policy
cluster-1	cluster_mgmt	
		default-management
cluster-1	node1-mgmt	
		default-management
cluster-1	node2-mgmt	
		default-management
cluster-1	inter_cluster	
		default-intercluster

4 entries were displayed.

2. 各LIFでEMSデスティネーションへの接続を確認します。

```
network ping -lif lif_name -vserver svm_name -destination  
destination_address
```

この手順は各ノードで実行します。

例

```
cluster-1::> network ping -lif nodel-mgmt -vserver cluster-1
-destination 10.10.10.10
10.10.10.10 is alive

cluster-1::> network ping -lif inter_cluster -vserver cluster-1
-destination 10.10.10.10
no answer from 10.10.10.10
```

3. advanced 権限レベルに切り替えます。

```
set advanced
```

4. LIFに到達できない場合は、対応するサービスポリシーからmanagement-ems LIFサービスを削除します。

```
network interface service-policy remove-service -vserver svm_name
-policy service_policy_name -service management-ems
```

5. 管理EMS LIFがEMSデスティネーションに到達できるLIFにのみ関連付けられていることを確認します。

```
network interface show -fields service-policy -services management-ems
```

## 関連リンク

["ONTAP 9.6以降のLIFとサービスポリシー"](#)

**ONTAPアップグレード後のMetroCluster構成のネットワークとストレージのステータスの確認**

MetroCluster構成のONTAPクラスタをアップグレードしたら、各クラスタのLIF、アグリゲート、およびボリュームのステータスを確認する必要があります。

1. LIFのステータスを確認します。

```
network interface show
```

通常運用時は、ソース SVM の LIF の管理ステータスが稼働状態で、ホームノードに配置されている必要があります。デスティネーション SVM の LIF については、稼働し、ホームノードに配置されている必要はありません。スイッチオーバー時には、すべての LIF の管理ステータスが稼働状態になっている必要がありますが、ホームノードに配置されている必要はありません。

```

cluster1::> network interface show

```

Current Is	Logical	Status	Network	Current	
Vserver	Interface	Admin/Oper	Address/Mask	Node	Port
Home					
-----	-----	-----	-----	-----	-----
Cluster					
	cluster1-a1_clus1	up/up	192.0.2.1/24	cluster1-01	e2a
true					
	cluster1-a1_clus2	up/up	192.0.2.2/24	cluster1-01	e2b
true					
cluster1-01					
	clus_mgmt	up/up	198.51.100.1/24	cluster1-01	e3a
true					
	cluster1-a1_inet4_intercluster1	up/up	198.51.100.2/24	cluster1-01	e3c
true					
	...				

```

27 entries were displayed.

```

## 2. アグリゲートの状態を確認します。

```
storage aggregate show -state !online
```

このコマンドを実行すると、オンラインでないアグリゲートが表示されます。通常運用時は、ローカルサイトにあるすべてのアグリゲートがオンラインになっている必要があります。ただし、MetroCluster 構成がスイッチオーバー状態の場合は、ディザスタリカバリサイトにあるルートアグリゲートをオフラインにすることができます。

次の例は、通常運用時のクラスタを示しています。

```

cluster1::> storage aggregate show -state !online
There are no entries matching your query.

```

次の例は、スイッチオーバー時のクラスタを示しています。ディザスタリカバリサイトにあるルートアグリゲートはオフラインです。

```
cluster1::> storage aggregate show -state !online
Aggregate      Size Available Used% State  #Vols  Nodes      RAID
Status
-----
-----
aggr0_b1
                0B          0B    0% offline    0 cluster2-01
raid_dp,
mirror
degraded
aggr0_b2
                0B          0B    0% offline    0 cluster2-02
raid_dp,
mirror
degraded
2 entries were displayed.
```

3. ボリュームの状態を確認します。

```
volume show -state !online
```

このコマンドを実行すると、オンラインでないボリュームが表示されます。

MetroCluster 構成が正常に動作している（スイッチオーバー状態でない）場合は、クラスタのセカンダリ SVM（名前に「-mc」が付いている SVM）が所有するすべてのボリュームが出力に表示されます。

これらのボリュームはスイッチオーバー時にのみオンラインになります。

次の例は、通常運用時のクラスタを示しています。ディザスタリカバリサイトにあるボリュームはオフラインです。

```
cluster1::> volume show -state !online
(volume show)
Vserver   Volume           Aggregate      State      Type      Size
Available Used%
-----
vs2-mc    vol1             aggr1_b1      -          RW        -
-         -
vs2-mc    root_vs2        aggr0_b1      -          RW        -
-         -
vs2-mc    vol2             aggr1_b1      -          RW        -
-         -
vs2-mc    vol3             aggr1_b1      -          RW        -
-         -
vs2-mc    vol4             aggr1_b1      -          RW        -
-         -
5 entries were displayed.
```

#### 4. 整合性のないボリュームがないことを確認します。

```
volume show -is-inconsistent true
```

サポート技術情報の記事を参照してください "[「WAFL inconsistent」を示すボリューム](#)" を参照してください。

アップグレード後に **SAN** 構成を確認

ONTAPのアップグレード後、SAN環境では、アップグレード前にLIFに接続されていた各イニシエータがLIFに正常に再接続されたことを確認する必要があります。

#### 1. 各イニシエータが正しい LIF に接続されていることを確認します。

イニシエータのリストと、アップグレードの準備の際に作成したリストを比較する必要があります。

用途	入力するコマンド
iSCSI	<pre>iscsi initiator show -fields igroup,initiator-name,tpgroup</pre>
FC	<pre>fcp initiator show -fields igroup,wwpn,lif</pre>

ONTAP 9.2以前のバージョンからONTAP 9.3以降にアップグレードした場合は、外部キー管理（KMIP）サーバの接続を再設定する必要があります。

手順

1. キー管理ツールの接続を設定します。

```
security key-manager setup
```

2. KMIPサーバを追加します。

```
security key-manager add -address key_management_server_ip_address
```

3. KMIPサーバが接続されていることを確認します。

```
security key-manager show -status
```

4. キーサーバを照会します。

```
security key-manager query
```

5. 新しい認証キーとパスフレーズを作成します。

```
security key-manager create-key -prompt-for-key true
```

パスフレーズは 32 文字以上にする必要があります。

6. 新しい認証キーを照会します。

```
security key-manager query
```

7. 新しい認証キーを自己暗号化ディスク（SED）に割り当てます。

```
storage encryption disk modify -disk disk_ID -data-key-id key_ID
```



新しい認証キーをクエリで使用していることを確認します。

8. 必要に応じて、FIPSキーをSEDに割り当てます。

```
storage encryption disk modify -disk disk_id -fips-key-id  
fips_authentication_key_id
```

セキュリティの設定によりデータ認証と FIPS 140-2 認証に異なるキーを使用する必要がある場合は、それぞれの認証用のキーを作成する必要があります。そうでない場合は、FIPS 準拠の認証キーをデータアクセスにも使用できます。

**ONTAPのアップグレード後に移動した負荷共有ミラーのソースボリュームの再配置**

ONTAPをアップグレードしたら、負荷共有ミラーのソースボリュームをアップグレード前の場所に戻す必要があります。

手順

1. 負荷共有ミラーのソースボリュームの移動前に作成したレコードを使用して、負荷共有ミラーのソースボリュームの移動先を確認します。
2. 負荷共有ミラーのソースボリュームを元の場所に戻します。

```
volume move start
```

サービスプロセッサにアクセスできるユーザアカウントが変更されました

ONTAP 9.8以前で管理者以外のロールでサービスプロセッサ (SP) にアクセスできるユーザアカウントを作成した場合にONTAP 9.9.1以降にアップグレードすると、`-role` パラメータがに変更されました `admin`。

詳細については、を参照してください ["SP にアクセスできるアカウント"](#)。

**Disk Qualification Packageの更新**

ONTAPソフトウェアをアップグレードしたら、ONTAP Disk Qualification Package (DQP) をダウンロードしてインストールする必要があります。ONTAP のアップグレードの一環として DQP が更新されることはありません。

DQPには、ONTAPが新しく認定されたすべてのドライブと連携するための適切なパラメータが含まれています。使用しているバージョンのDQPに新しく認定されたドライブの情報が含まれていない場合、ONTAPにはドライブを適切に設定するための情報がありません。

DQPは四半期ごとに更新することを推奨します。また、次の理由からDQPを更新する必要があります。

- クラスタ内のノードに新しいタイプまたはサイズのドライブを追加したとき

たとえば、1TB のドライブを使用している環境で 2TB のドライブを追加した場合、DQP の最新版がないかどうかを確認する必要があります。

- ディスクファームウェアを更新するたびに更新されます

- 新しいディスクファームウェアや DQP ファイルが利用可能になったとき

#### 関連情報

- ["ネットアップのダウンロード： Disk Qualification Package"](#)
- ["ネットアップのダウンロード：ディスクドライブファームウェア"](#)

## ファームウェアおよびシステムの更新

### ファームウェアとシステムの更新の概要

ONTAPのバージョンによっては、自動ファームウェアおよびシステム更新を有効にすることができます。

ONTAPバージョン	自動更新に含まれている機能
9.13.1以降	<ul style="list-style-type: none"><li>• ONTAPタイムゾーンデータベース</li><li>• ストレージデバイス、ディスク、およびディスクシェルフのストレージファームウェア</li><li>• サービスプロセッサおよびBMCモジュールのSP / BMCファームウェア</li></ul>
9.10.1以降	<ul style="list-style-type: none"><li>• ストレージデバイス、ディスク、およびディスクシェルフのストレージファームウェア</li><li>• サービスプロセッサおよびBMCモジュールのSP / BMCファームウェア</li></ul>
9.9.1以前	サポート対象外

ONTAP 9.9.1以前を実行している場合、またはを実行していない場合 ["システムの自動更新"](#) 有効にすることができます ["ファームウェアを手動で更新します"](#)。

ONTAP 9.12.1以前を実行している場合、または ["システムの自動更新"](#) 有効にすると、タイムゾーンデータベースを手動で更新できます。次の記事を参照してください。 ["ONTAP 9でタイムゾーン情報を更新する方法"](#) を参照してください。

#### ビデオ:自動ファームウェアアップデート機能

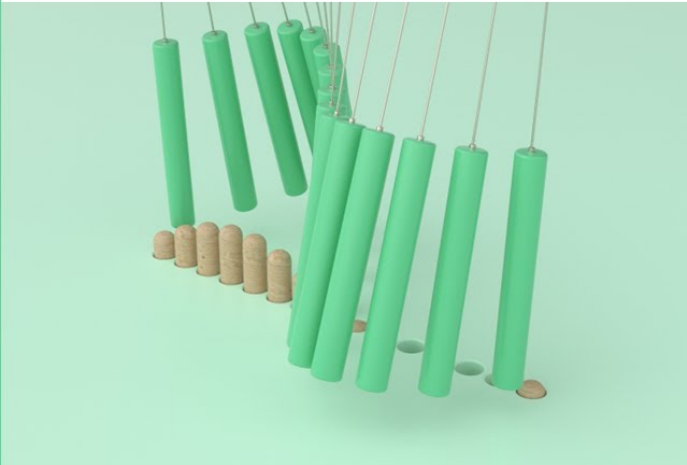
ONTAP 9.10.1以降では、ファームウェアの自動更新機能を利用できます。





Automatic Firmware Update  
feature is available starting  
in ONTAP 9.10.1

By Jim Svesnik,  
Quality Assurance Engineer



インストールの自動更新をスケジュールする方法

同じクラスタ内の対象となるすべてのノードが自動更新対象としてグループ化されます。対象となるノードの自動更新がスケジュールされる期間は、更新の優先度レベルと、環境内で更新が必要なシステムの割合によって異なります。

たとえば、システム全体の10%以下が優先度の低いアップデートの対象となる場合、対象となるすべてのシステムに対して1週間以内にアップデートがスケジュールされます。ただし、システム全体の76%以上が優先度の低いアップデートの対象である場合は、対象となるシステム間で8週間にわたって順次アップデートが行われます。この段階的インストールは、修正が必要な更新が含まれた問題がある場合に、環境全体に対するリスクを軽減するのに役立ちます。

週ごとに自動更新がスケジュールされているシステム全体の割合は、次のとおりです。

重要な更新について

更新が必要なシステムの割合	1週目に発生する更新の割合	2週目に発生する更新の割合
50%以下	100%	
50～100%	30%だ	70%です

優先度の高いアップデート

更新が必要なシステムの割合	週ごとに発生する更新の割合			
	第1週	第2週	第3週	第4週
* 25%以下*	100%			

更新が必要なシステムの割合	週ごとに発生する更新の割合			
* 26～50%*	30%だ	70%です		
* 50～100%*	10%だ	20%だ	30%だ	40%

#### 通常の優先度の更新の場合

更新が必要なシステムの割合	週ごとに発生する更新の割合							
	第1週	第2週	第3週	第4週	第5週	第6週	* 7週目*	第8週
* 10%以下*	100%							
* 11-20%*	30%だ	70%です						
* 21-50%*	10%だ	20%だ	30%だ	40%				
* 51-75%*	5%です	10%だ	15%だ	20%だ	20%だ	30%だ		
* 76-100%*	5%です	5%です	10%だ	10%だ	15%だ	15%だ	20%だ	20%だ

## 自動更新を有効にします

ONTAP 9.10.1以降では、自動更新を有効にして、ONTAPが手動操作なしでファームウェアの更新をダウンロードしてインストールできるようにすることができます。

ONTAP 9.13.1以降、これらの自動更新にはタイムゾーンデータベースの自動更新も含まれています。

作業を開始する前に

最新のサポート契約が必要です。これはで検証できます ["NetApp Support Site"](#) をクリックします。

このタスクについて

自動更新を有効にするには、最初にHTTPSでAutoSupportを有効にする必要があります。 クラスタでAutoSupportが有効になっていない場合、または別の転送プロトコルを使用してクラスタでAutoSupportを有効にしている場合は、この手順でHTTPSで有効にするオプションが表示されます。

手順

1. System Manager で、 \* Events （イベント） \* をクリックします。
2. セクションの[自動更新を有効にする]の横にある[操作]>[有効にする]\*をクリックします。
3. AutoSupportでHTTPSが有効になっていない場合は、を選択して有効にします。
4. 利用条件に同意し、\*[保存]\*を選択します。


関連情報

["HTTP または HTTPS を使用した AutoSupport メッセージ配信のトラブルシューティング"](#)

## 自動更新を変更します

自動更新が有効になっている場合、デフォルトでは、ONTAPは推奨されるすべてのファームウェア更新と、ONTAP 9.13.1以降のONTAPタイムゾーンデータベース更新を自動的に検出、ダウンロード、およびインストールします。推奨される更新プログラムをインストール前に表示する場合や、推奨される更新プログラムを自動的に却下する場合は、デフォルトの動作を設定に変更できます。

### 手順

1. System Manager で、 \* Cluster > Settings \* の順にクリックします。
2. [\* 自動更新 \*] セクションで、をクリックします  をクリックすると、アクションのリストが表示されます。
3. [自動更新設定の編集] をクリックします。
4. イベントタイプごとに実行するデフォルトのアクションを指定します。

イベントタイプごとに、自動的に更新するか、通知を表示するか、または更新を自動的に却下するかを選択できます。






ONTAPタイムゾーンデータベースは、SYSTEM FILESイベントタイプによって制御されません。


## 推奨される自動更新を管理します

自動更新ログには、更新に関する推奨事項のリストと、概要、カテゴリ、インストール予定時刻、ステータス、エラーなどの各項目の詳細が表示されます。ログを表示して、各推奨事項に対して実行するアクションを決定できます。

### 手順

1. 推奨事項のリストを表示します。

をクラスタ設定から表示します	ファームウェアアップデートタブから表示します
<ol style="list-style-type: none"><li>a. [Cluster] &gt; [Settings] の順にクリックします。</li><li>b. [* 自動更新 *] セクションで、をクリックします  をクリックし、 * すべての自動更新を表示 * をクリックします。</li></ol>	<ol style="list-style-type: none"><li>a. [* Cluster] &gt; [Overview] をクリックします。</li><li>b. 「 * 概要 * 」セクションで、「 * 詳細 * 」をクリックします  をクリックし、 * ONTAP アップデート * をクリックします。</li><li>c. [* ファームウェア・アップデート *] タブを選択します。</li><li>d. [* ファームウェア・アップデート *] タブで、[ * 詳細 * ] をクリックします  をクリックし、 * すべての自動更新を表示 * をクリックします。</li></ol>

2. をクリックします  概要の横に表示され、推奨構成に対して実行できる操作のリストが表示されます。

推奨構成の状態に応じて、次のいずれかの操作を実行できます。

更新の状態	可能です
はスケジュールされていません	<ul style="list-style-type: none"> <li>• アップデート * : アップデート処理を開始します。</li> <li>• スケジュール *: 更新プロセスを開始する日付を設定できます。</li> <li>• Dismiss * : 推奨事項をリストから削除します。</li> </ul>
がスケジュールされました	<ul style="list-style-type: none"> <li>• アップデート * : アップデート処理を開始します。</li> <li>• スケジュールの編集 *: 更新プロセスを開始するためのスケジュールされた日付を変更できます。</li> <li>• スケジュールのキャンセル *: スケジュールされた日付をキャンセルします。</li> </ul>
が却下されました	<ul style="list-style-type: none"> <li>• Undismiss * : 推奨事項をリストに返します。</li> </ul>
が適用されているか、ダウンロード中です	<ul style="list-style-type: none"> <li>• キャンセル * : 更新をキャンセルします。</li> </ul>

## ファームウェアを手動で更新します

ONTAP 9.9.1以降では、に登録されている場合 **"Active IQ Unified Manager"**では、サポートされているデバイス（ディスク、ディスクシェルフ、サービスプロセッサ（SP）、ベースボード管理コントローラ（BMC）など）のファームウェアの更新がクラスタで保留されているときに通知するアラートをSystem Managerで受信できます。

ONTAP 9.8を実行している場合やActive IQ Unified Managerに登録していない場合は、NetApp Support Siteに移動してファームウェアの更新をダウンロードできます。

### 作業を開始する前に

ファームウェアのスムーズな更新を準備するには、更新を開始する前にSPまたはBMCをリブートする必要があります。を使用できます `system service-processor reboot-sp -node node_name` リブートするコマンド。

### 手順

使用しているONTAPのバージョンと、Active IQ Unified Managerに登録されている場合は、該当する手順に従います。

## ONTAP 9.9.1以降 (Active IQ使用時)

1. System Managerで、\*[ダッシュボード]\*に移動します。

「\* Health \*」セクションに、クラスタに推奨されるファームウェア・アップデートがあるかどうかを示すメッセージが表示されます。

2. アラートメッセージをクリックします。

[\* ファームウェア・アップデート \*] タブが [\* アップデート \*] ページに表示されます。

3. 実行するファームウェアアップデートのために、\*[Download from NetApp Support Site (からダウンロード)]\*をクリックします。


NetApp Support Siteが表示されます。

4. NetApp Support Siteにログインし、アップデートに必要なファームウェアイメージパッケージをダウンロードします。
5. ネットワーク上の HTTP サーバまたは FTP サーバ、またはローカルフォルダにファイルをコピーします。
6. System Manager で、\* Cluster > Overview \* をクリックします。
7. [\* 概要 \* ( Overview \* ) ] パネルの右隅で、[\* 詳細 \* ( \* More \* ) ] をクリックします。⋮ をクリックし、\* ONTAP アップデート \* を選択します。
8. [\* ファームウェア・アップデート \*] をクリックします。
9. ONTAPのバージョンに応じて、次の手順を実行します。

ONTAP 9.9.1および9.10.0	ONTAP 9.10.1 以降
<ol style="list-style-type: none"><li>a. サーバーから * を選択するか、* ローカルクライアント * を選択します</li><li>b. サーバの URL またはファイルの場所を指定します。</li></ol>	<ol style="list-style-type: none"><li>a. 推奨される更新プログラムのリストで、*[アクション]*を選択します。</li><li>b. アップデートをすぐにインストールする場合は*をクリックし、後でインストールする場合は[スケジュール]*をクリックします。  更新がすでにスケジュールされている場合は、*編集*または*キャンセル*することができます。</li><li>c. [ファームウェアの更新]*ボタンを選択します。</li></ol>

## Active IQなしのONTAP 9.8以降

1. に移動します "NetApp Support Site" ログインします。
2. クラスタファームウェアの更新に使用するファームウェアパッケージを選択します。
3. ネットワーク上の HTTP サーバまたは FTP サーバ、またはローカルフォルダにファイルをコピーします。

4. System Manager で、 \* Cluster > Overview \* をクリックします。
5. [\* 概要 \* ( Overview \* ) ] パネルの右隅で、 [\* 詳細 \* ( \* More \* ) ] をクリックします  をクリックし、 \* ONTAP アップデート \* を選択します。
6. [\* ファームウェア・アップデート \* ] をクリックします。
7. ONTAPのバージョンに応じて、次の手順を実行します。

ONTAP 9.8、9.9.1、9.10.0	ONTAP 9.10.1 以降
<ol style="list-style-type: none"> <li>1. サーバーから * を選択するか、 * ローカルクライアント * を選択します</li> <li>2. サーバの URL またはファイルの場所を指定します。</li> </ol>	<ol style="list-style-type: none"> <li>1. 推奨される更新プログラムのリストで、*[アクション]*を選択します。</li> <li>2. アップデートをすぐにインストールする場合は*をクリックし、後でインストールする場合は[スケジュール]*をクリックします。  更新がすでにスケジュールされている場合は、*編集*または*キャンセル*することができます。</li> <li>3. [ファームウェアの更新]*ボタンを選択します。</li> </ol>

完了後

アップデートは、 \* ファームウェア・アップデートの概要 \* で監視または確認できます。 却下された更新やインストールに失敗した更新を確認するには、\*[クラスタ]>[設定]>[自動更新]>[すべての自動更新を表示]\*をクリックします。

## ONTAP をリバートする

### リバート ONTAP の概要

クラスタを以前の ONTAP リリースに移行するには、リバートを実行する必要があります。

このセクションでは、リバートの前後に行うべき手順について説明します。これには、確認が必要なリソースや、リバート前とリバート後の必要なチェックなどが含まれます。



クラスタを ONTAP 9.1 から ONTAP 9.0 に移行する必要がある場合は、ダウングレード手順に関するドキュメントを使用する必要があります ["こちらをご覧ください"](#)。

### リバートするときにテクニカルサポートが必要ですか？

新規またはテスト用のクラスタについてのサポートがなくてもリバートできます。 本番環境クラスタをリバートする場合は、テクニカルサポートにお問い合わせください。 次のいずれかの問題が発生した場合は、テクニカルサポートにお問い合わせください。

- 本番環境でリバートに失敗した場合や、リバートの前後に問題が発生した場合の例を次に示します。
  - リバートプロセスが失敗して終了できない。

- リバートプロセスは終了したが、本番環境でクラスタを使用できない。
- リバートプロセスが終了してクラスタが本番環境に移行したが、正しく動作しない。
- ONTAP 9.5 以降でボリュームを作成したあと、以前のバージョンにリバートする必要があります。適応圧縮を使用しているボリュームは、リバートの前に圧縮を解除する必要があります

## パスをリバートする

リバート可能な ONTAP のバージョンは、ノードで現在実行している ONTAP のバージョンによって異なります。を使用できます `system image show` コマンドを使用して、各ノードで実行されている ONTAP のバージョンを確認します。

これらのガイドラインで言及しているのは、オンプレミスの ONTAP リリースのみです。クラウドでの ONTAP のリバートについては、を参照してください ["Cloud Volumes ONTAP をリバートまたはダウングレードする"](#)。

現在実行しているバージョン	目的
ONTAP 9.14.1	ONTAP 9.13.1
ONTAP 9.13.1	ONTAP 9.12.1
ONTAP 9.12.1	ONTAP 9.11.1
ONTAP 9.11.1	ONTAP 9.10.1
ONTAP 9.10.1	ONTAP 9.9.1
ONTAP 9.9.1	ONTAP 9.8
ONTAP 9.8	ONTAP 9.7
ONTAP 9.7	ONTAP 9.6
ONTAP 9.6	ONTAP 9.5
ONTAP 9.5	ONTAP 9.4
ONTAP 9.4	ONTAP 9.3
ONTAP 9.3	ONTAP 9.2
ONTAP 9.2	ONTAP 9.1
ONTAP 9.1またはONTAP 9	Data ONTAP 8.3.x





ONTAP 9.1から9.0に変更する必要がある場合は、に従ってください ["ダウングレードプロセス"](#) ここで説明します。

## リバートする前に何を確認すればよいですか？

### リバート前に確認するリソース

ONTAP をリバートする前に、ハードウェアのサポートを確認し、発生した問題や解決が必要な問題を把握するためにリソースを確認しておく必要があります。

1. を確認します ["ONTAP 9リリースノート"](#) ターゲットリリース用。

「重要な注意事項」セクションでは、ダウングレードまたはリバートの前に注意すべき潜在的な問題について説明します。

2. 使用しているハードウェアプラットフォームがターゲットリリースでサポートされていることを確認します。

["NetApp Hardware Universe の略"](#)

3. クラスタと管理スイッチがターゲットリリースでサポートされていることを確認します。

NX-OS（クラスタネットワークスイッチ）、IOS（管理ネットワークスイッチ）、および RCF ソフトウェアのバージョンがリバート先の ONTAP のバージョンに対応していることを確認してください。

["ネットアップのダウンロード：Cisco イーサネットスイッチ"](#)

4. クラスタが SAN 用に構成されている場合は、SAN 構成が完全にサポートされていることを確認します。

ターゲットの ONTAP ソフトウェアバージョン、ホスト OS およびパッチ、必須の Host Utilities ソフトウェア、アダプタドライバおよびファームウェアなど、すべての SAN コンポーネントがサポートされている必要があります。

["NetApp Interoperability Matrix Tool で確認できます"](#)

### リバートに関する考慮事項

ONTAP をリバートするときは、開始前にリバートの問題と制限事項について考慮する必要があります。

- リバートの実行時はシステムが停止

リバートの実行中はクライアントからアクセスできなくなります。本番環境クラスタをリバートする場合は、この停止時間を考慮して計画してください。

- リバートを行う際は、クラスタ内のすべてのノードが対象になり

リバートを行う際は、クラスタ内のすべてのノードが対象になりますが、リバートは HA ペアごとに実行し、それが完了してから次の HA ペアのリバートに進む必要があります。



- リバートは、すべてのノードで新しいターゲットリリースが実行されるようになった時点で完了です。

クラスタに複数のバージョンが混在した状態の間は、リバート要件を満たすために必要なコマンドを除き、クラスタの処理や構成を変更するコマンドは実行しないでください。監視処理は許可されます。



一部のノードのみをリバートした状態で、クラスタを元のリリースにアップグレードしないでください。

- ノードをリバートすると、Flash Cache モジュール内のキャッシュデータはクリアされます。

Flash Cache モジュールにキャッシュデータがないため、初回の読み取り要求に対してはディスクからデータを取り出すことになり、この期間の読み取りパフォーマンスが低下します。読み取り要求に対応するたびに、再びキャッシュにデータが蓄えられます。

- ONTAP 9.x で実行しているテープにバックアップした LUN は、9.x 以降のリリースにのみリストアできます。9.x より前のリリースにはリストアできません。
- 現在使用しているバージョンの ONTAP でインバンド ACP（IBACP）機能がサポートされている場合は、IBACP をサポートしないバージョンの ONTAP にリバートすると、ディスクセルフへの代替パスが無効になります。
- LDAP を使用する Storage Virtual Machine（SVM）がある場合は、リバートの前に LDAP リファールルを無効にする必要があります。
- MetroCluster に準拠しているが MetroCluster 検証は行われていないスイッチを使用する MetroCluster IP システムを ONTAP 9.7 から 9.6 にリバートする場合、ONTAP 9.6 以前を使用するシステムはサポートされないため処理が停止します。

## リバート前に確認しておく項目

リバートを実行する前に、クラスタの健全性、ストレージの健全性、およびシステム時間を確認する必要があります。また、実行中のクラスタジョブを削除し、継続的可用性に対応していない SMB セッションを正常に終了する必要があります。

### クラスタの健全性を確認

クラスタをリバートする前に、ノードが正常に機能していてクラスタに追加するための条件を満たしていること、およびクラスタがクォーラムにあることを確認する必要があります。

- クラスタ内のノードがオンラインで、クラスタに追加するための条件を満たしていることを確認します。

```
cluster show
```

```
cluster1::> cluster show
Node                Health  Eligibility
-----
node0               true    true
node1               true    true
```

正常に機能していないノードや条件を満たしていないノードがある場合は、EMS ログでエラーを確認して適切に修正します。

2. 権限レベルをadvancedに設定+

```
set -privilege advanced
```

入力するコマンド y 続行します。

3. 各 RDB プロセスの構成の詳細を確認します。

- リレーショナルデータベースのエポックとデータベースのエポックが各ノードで一致すること。
- リングごとのクォーラムマスターがすべてのノードで同じであることが必要です。

各リングのクォーラムマスターが異なる場合があることに注意してください。

表示する <b>RDB</b> プロセス	入力するコマンド
管理アプリケーション	<code>cluster ring show -unitname mgmt</code>
ボリュームロケーションデータベース	<code>cluster ring show -unitname vlodb</code>
仮想インターフェイスマネージャ	<code>cluster ring show -unitname vifmgr</code>
SAN 管理デーモン	<code>cluster ring show -unitname bcomd</code>

次の例は、ボリュームロケーションデータベースのプロセスを示しています。

```
cluster1::*> cluster ring show -unitname vlodb
Node      UnitName Epoch      DB Epoch DB Trnxs Master      Online
-----
node0     vlodb      154          154      14847   node0     master
node1     vlodb      154          154      14847   node0     secondary
node2     vlodb      154          154      14847   node0     secondary
node3     vlodb      154          154      14847   node0     secondary
4 entries were displayed.
```

4. admin権限レベルに戻ります。+

```
set -privilege admin
```

5. SAN 環境を使用している場合は、各ノードが SAN クォーラムにあることを確認します。event log show -severity informational -message-name scsiblade.\*

各ノードの最新の scsiblade イベントメッセージに、SCSI ブレードがクォーラムにあることが示されます。

```
cluster1::*> event log show -severity informational -message-name
scsiblade.*
```

Time	Node	Severity	Event
MM/DD/YYYY TIME	node0	INFORMATIONAL	scsiblade.in.quorum: The scsi-blade ...
MM/DD/YYYY TIME	node1	INFORMATIONAL	scsiblade.in.quorum: The scsi-blade ...

## 関連情報

### "システム管理"

#### ストレージの健全性を確認

クラスタをリポートする前に、ディスク、アグリゲート、およびボリュームのステータスを確認する必要があります。

1. ディスクのステータスを確認します。

確認する項目	手順
破損ディスク	a. 破損ディスクを表示します。 <code>storage disk show -state broken</code> b. 破損ディスクを取り外すか交換します。
メンテナンス中または再構築中のディスク	a. 保守、保留、または再構築の状態のディスクを表示します。 <code>`storage disk show -state maintenance</code>
pending	<code>reconstructing`</code> .. メンテナンスまたは再構築の処理が完了するまで待ってから次に進みます。

2. ストレージアグリゲートを含む物理ストレージと論理ストレージの状態を表示して、すべてのアグリゲートがオンラインであることを確認します。 `storage aggregate show -state !online`

このコマンドを実行すると、オンラインでないアグリゲートが表示されます。メジャーアップグレードまたはリポートの実行前と実行後には、すべてのアグリゲートがオンラインになっている必要があります。

```
cluster1::> storage aggregate show -state !online
There are no entries matching your query.
```

3. 次のコマンドを実行して、すべてのボリュームがオンラインであることを確認します。 `_not_online volume show -state !online`

メジャーアップグレードまたはリポートの実行前と実行後には、すべてのボリュームがオンラインになっ

ている必要があります。

```
cluster1::> volume show -state !online
There are no entries matching your query.
```

4. 整合性のないボリュームがないことを確認します。 `volume show -is-inconsistent true`

サポート技術情報の記事を参照してください "[「WAFL inconsistent」を示すボリューム](#)" を参照してください。

## 関連情報

["ディスクおよびアグリゲートの管理"](#)

## システム時間の確認

リポートを行う前に、NTP が設定されていること、および時刻がクラスタ全体で同期されていることを確認する必要があります。

1. クラスタがNTPサーバに関連付けられていることを確認します。 `cluster time-service ntp server show`
2. 各ノードの日付と時刻が同じであることを確認します。 `cluster date show`

```
cluster1::> cluster date show
Node          Date                Timezone
-----
node0         4/6/2013 20:54:38    GMT
node1         4/6/2013 20:54:38    GMT
node2         4/6/2013 20:54:38    GMT
node3         4/6/2013 20:54:38    GMT
4 entries were displayed.
```

## 実行中のジョブがないことを確認します

ONTAP ソフトウェアをリポートする前に、クラスタジョブのステータスを確認する必要があります。アグリゲート、ボリューム、NDMP（ダンプまたはリストア）、または Snapshot に関する実行中のジョブ（作成、削除、移動、変更、複製など）およびマウントジョブが実行中またはキューに登録されている場合は、ジョブが正常に完了するまで待つか、キューのエントリを停止する必要があります。

1. アグリゲート、ボリューム、またはSnapshotに関する実行中のジョブとキューに登録されているジョブのリストを確認します。 `job show`

```
cluster1::> job show
```

Job ID	Name	Owning Vserver	Node	State
8629	Vol Reaper	cluster1	-	Queued
	Description: Vol Reaper Job			
8630	Certificate Expiry Check	cluster1	-	Queued
	Description: Certificate Expiry Check			
.				
.				
.				

2. アグリゲート、ボリューム、またはSnapshotコピーに関する実行中のジョブとキューに登録されているジョブを削除します。 `job delete -id job_id`

```
cluster1::> job delete -id 8629
```

3. アグリゲート、ボリューム、またはSnapshotに関する実行中のジョブとキューに登録されているジョブがないことを確認します。 `job show`

次の例では、実行中のジョブとキューに登録されているジョブがすべて削除されています

```
cluster1::> job show
```

Job ID	Name	Owning Vserver	Node	State
9944	SnapMirrorDaemon_7_2147484678	cluster1	node1	Dormant
	Description: Snapmirror Daemon for 7_2147484678			
18377	SnapMirror Service Job	cluster1	node0	Dormant
	Description: SnapMirror Service Job			

2 entries were displayed

## 終了する必要があるSMBセッション

リバートを行う前に、継続的可用性に対応していないSMBセッションを特定して正常に終了する必要があります。

Hyper-VクライアントまたはMicrosoft SQL ServerクライアントがSMB 3.0プロトコルを使用してアクセスする、継続的可用性を備えたSMB共有は、アップグレードまたはダウングレードの前に終了する必要はありません。

1. 継続的可用性に対応していない、確立済みのSMBセッションを特定します。 `vserver cifs session show -continuously-available No -instance`

このコマンドは、継続的可用性が確保されていないSMBセッションに関する詳細情報を表示します。これらのセッションは、ONTAP のダウングレードを開始する前に終了する必要があります。

```
cluster1::> vserver cifs session show -continuously-available No
-instance
```

```

                Node: node1
                Vserver: vs1
                Session ID: 1
                Connection ID: 4160072788
Incoming Data LIF IP Address: 198.51.100.5
                Workstation IP address: 203.0.113.20
                Authentication Mechanism: NTLMv2
                Windows User: CIFS\user1
                UNIX User: nobody
                Open Shares: 1
                Open Files: 2
                Open Other: 0
                Connected Time: 8m 39s
                Idle Time: 7m 45s
                Protocol Version: SMB2_1
                Continuously Available: No
1 entry was displayed.
```

2. 必要に応じて、特定した各SMBセッションで開いているファイルを確認します。 `vserver cifs session file show -session-id session_ID`

```
cluster1::> vserver cifs session file show -session-id 1

Node:      node1
Vserver:   vs1
Connection: 4160072788
Session:    1
File      File      Open Hosting
Continuously
ID        Type        Mode Volume          Share                Available
-----
-----
1         Regular    rw   vol10              homedirshare         No
Path: \TestDocument.docx
2         Regular    rw   vol10              homedirshare         No
Path: \file1.txt
2 entries were displayed.
```

## NVMeインバンド認証

ONTAP 9.12.1以降からONTAP 9.12.0以前にリバートする場合は、["インバンド認証を無効にする"](#)を参照してください。DH-HMAC-CHAPを使用するインバンド認証が無効になっていない場合、リバートは失敗します。

リバートする前に他に何を確認すればよいですか？

リバート前のチェック

環境によっては、リバート前に特定の要因を考慮する必要があります。次の表を確認して、考慮すべき特別な考慮事項を確認してください。

自分自身に尋ねる ...	回答が * はい * の場合、次の操作を実行します ...
クラスタで SnapMirror を実行しているかどうか	<ul style="list-style-type: none"> <li>• <a href="#">SnapMirror Synchronous</a> 関係が設定されたシステムをリバートする場合の考慮事項を確認して</li> <li>• <a href="#">SnapMirror</a> 関係と <a href="#">SnapVault</a> 関係のリバート要件を確認する</li> </ul>
クラスタで SnapLock を実行しているか？	<a href="#">自動コミット期間の設定</a>
FlexClone ボリュームをスプリットしていますか？	<a href="#">物理ブロック共有を反転する</a>
FlexGroup ボリュームがあるか。	<a href="#">qtree 機能を無効にする</a>
ワークグループモードの CIFS サーバを使用しているか？	<a href="#">ワークグループモードの CIFS サーバを移動または削除する</a>
重複排除ボリュームがあるか？	<a href="#">ボリュームに十分な空きスペースがあることを確認します</a>

自分自身に尋ねる ...	回答が * はい * の場合、次の操作を実行します ...
Snapshot コピーがあるか？	Snapshot コピーを準備します
ONTAP 8.3.x にリバートするか。	SHA-2 ハッシュ関数を使用しているユーザアカウントを特定します
ONTAP 9.11.1以降では、ランサムウェア対策による保護が設定されていますか。	ランサムウェア対策ライセンスを確認する
ONTAP 9.12.1以降用にS3マルチプロトコルアクセスが設定されていますか。	S3 NASバケット設定を削除する
ONTAP 9.14.1以降ではNFSv4.1セッショントランキングが設定されていますか。	NFSv4.1セッションのトランキング設定を削除する

### MetroCluster のリバート前チェック

MetroCluster 構成によっては、リバート前に特定の要因を考慮する必要があります。次の表を確認して、考慮すべき特別な考慮事項を確認してください。

自分自身に尋ねる ...	回答が * はい * の場合、次の操作を実行します ...
2ノードまたは4ノードのMetroCluster 構成を使用しているか。	自動計画外スイッチオーバーを無効にします
ONTAP 9.12.1以降を実行する4ノードまたは8ノードのMetroCluster IP構成またはファブリック接続構成を使用していますか。	IPSecを無効にします

## SnapMirror

### SnapMirror Synchronous 関係が設定されたシステムをリバートする際の考慮事項

ONTAP 9.6 から ONTAP 9.5 にリバートする前に、SnapMirror Synchronous 関係に関する考慮事項を確認しておく必要があります。

SnapMirror Synchronous 関係を使用している場合は、リバート前に次の手順を実行する必要があります。

- ソースボリュームが NFSv4 または SMB を使用してデータを提供している SnapMirror Synchronous 関係を削除する必要があります。

ONTAP 9.5 では、NFSv4 および SMB はサポートされません。

- ミラー - ミラーカスケード構成の SnapMirror Synchronous 関係を削除する必要があります。

ONTAP 9.5 では、ミラー - ミラーカスケード構成の SnapMirror Synchronous 関係はサポートされません。

- リバート時に ONTAP 9.5 の共通の Snapshot コピーを使用できない場合は、リバート後に SnapMirror Synchronous 関係を初期化する必要があります。

ONTAP 9.6 にアップグレードしてから 2 時間後に、ONTAP 9.5 の共通の Snapshot コピーは ONTAP 9.6 の共通の Snapshot コピーに自動的に置き換えられます。そのため、ONTAP 9.5 の共通の Snapshot コピーを使用できない場合、リバート後に SnapMirror Synchronous 関係を再同期することはできません。



system node revert-to コマンドは、リバートプロセスを完了するために削除または再設定する必要のある SnapMirror 関係と SnapVault 関係について通知します。ただし、リバートを開始する前に以下の要件について理解しておく必要があります。

- すべての SnapVault 関係とデータ保護ミラー関係を休止してから解除する必要があります。

共通の Snapshot コピーがある場合は、リバートの完了後にこれらの関係を再同期および再開できます。

- 次のタイプの SnapMirror ポリシーを SnapVault 関係に含めることはできません。

- 非同期ミラー

このポリシータイプを使用する関係をすべて削除する必要があります。

- MirrorAndVault の場合

このような関係が存在する場合は、SnapMirror ポリシーを mirror-vault に変更する必要があります。

- すべての負荷共有ミラー関係とデスティネーションボリュームを削除する必要があります。
- FlexClone デスティネーションボリュームとの SnapMirror 関係を削除する必要があります。
- 各 SnapMirror ポリシーでネットワーク圧縮を無効にする必要があります。
- async-mirror タイプの SnapMirror ポリシーから all\_source\_snapshot ルールを削除する必要があります。



ルートボリュームでの Single File Snapshot Restore (SFSR) 処理と Partial File Snapshot Restore (PFSR) 処理は廃止されました。

- リバートを開始する前に、実行中の単一ファイルおよび Snapshot のリストア処理を完了する必要があります。

リストア処理が完了するまで待つか、リストア処理を中止できます。

- 未完了の単一ファイルおよび Snapshot のリストア処理がある場合は、snapmirror restore コマンドを使用して削除する必要があります。

リバート前に **SnapLock** ボリュームの自動コミット期間を設定します

ONTAP 9 からリバートする場合は、SnapLock ボリュームの自動コミット期間の値を日数ではなく時間数で設定する必要があります。リバートを実行する前に、SnapLock ボリュームの自動コミット値を確認し、必要に応じて日数を時間数に変更してください。

1. クラスタ内にサポートされない自動コミット期間が設定されている SnapLock があることを確認します。volume snaplock show -autocommit-period \*days
2. サポートされない自動コミット期間を時間数に変更します。volume snaplock modify -vserver vserver\_name -volume volume\_name -autocommit-period value hours

スプリット **FlexClone** ボリュームで物理ブロックを逆共有します

FlexClone ボリュームを親ボリュームからスプリットした場合は、ONTAP 9.4 以降からそれより前のバージョンの ONTAP にリバートする前に、クローンと親ボリュームの間の物理ブロックの共有を取り消す必要があります。

このタスクは、AFF システムでいずれかの FlexClone ボリュームがスプリットされている場合にのみ実行します。

1. advanced 権限レベルにログインします。 `set -privilege advanced`
2. 物理ブロックを共有しているスプリット FlexClone ボリュームを特定します。 `volume clone sharing-by-split show`

```
cluster1::> volume clone sharing-by-split show
Node           Vserver    Volume      Aggregate
-----
node1          vs1        vol_clone1   aggr1
node2          vs2        vol_clone2   aggr2
2 entries were displayed.
```

3. クラスタ内のすべてのスプリット FlexClone ボリュームで、物理ブロック共有を取り消します。 `volume clone sharing-by-split undo start-all`
4. 物理ブロックを共有しているスプリット FlexClone ボリュームがないことを確認します。 `volume clone sharing-by-split show`

```
cluster1::> volume clone sharing-by-split show
This table is currently empty.
```

リバート前に **FlexGroup** ボリュームの **qtree** 機能を無効にする

ONTAP 9.3 より前のバージョンでは、FlexGroup ボリュームの qtree がサポートされません。ONTAP 9.3 を以前のバージョンの ONTAP にリバートする前に、FlexGroup ボリュームの qtree 機能を無効にする必要があります。

qtree を作成するか、デフォルトの qtree の security-style および oplock-mode 属性を変更すると、qtree 機能が有効になります。

1. qtree 機能が有効になっている各 FlexGroup ボリューム内の、デフォルト以外のすべての qtree を特定して削除します。
  - a. advanced 権限レベルにログインします。 `set -privilege advanced`
  - b. qtree 機能が有効になっている FlexGroup ボリュームがないか確認してください。

ONTAP 9.6以降： `volume show -is-qtree-caching-enabled true`

ONTAP 9.5以前の場合： `volume show -is-flexgroup-qtrees-enabled true`

```
cluster1::*> volume show -is-flexgroup-qtrees-enabled true
Vserver    Volume      Aggregate    State      Type      Size
Available  Used%
-----
vs0         fg          -            online     RW        320MB
220.4MB    31%
```

- c. qtrees機能が有効になっているFlexGroup ボリュームごとに、デフォルト以外のqtreesをすべて削除します。 `volume qtrees delete -vserver svm_name -volume volume_name -qtrees qtrees_name`

デフォルトの qtrees の属性を変更したために qtrees 機能が有効になっている場合や、 qtrees が 1 つもない場合は、この手順を省略できます。

```
cluster1::*> volume qtrees delete -vserver vs0 -volume fg -qtrees qtrees4
WARNING: Are you sure you want to delete qtrees qtrees4 in volume fg
vserver vs0? {y|n}: y
[Job 38] Job is queued: Delete qtrees qtrees4 in volume fg vserver vs0.
```

2. 各FlexGroup ボリュームでqtrees機能を無効にします。 `volume flexgroup qtrees-disable -vserver svm_name -volume volume_name`

```
cluster1::*> volume flexgroup qtrees-disable -vserver vs0 -volume fg
```

3. qtrees 機能が有効になっている Snapshot コピーを特定し、削除します。

- a. qtrees機能が有効になっているSnapshotコピーがないか確認します。 `volume snapshot show -vserver vserver_name -volume volume_name -fields is-flexgroup-qtrees-enabled`

```
cluster1::*> volume snapshot show -vserver vs0 -volume fg -fields is-
flexgroup-qtrees-enabled
vserver volume snapshot is-flexgroup-qtrees-enabled
-----
vs0         fg          fg_snap1 true
vs0         fg          daily.2017-09-27_0010 true
vs0         fg          daily.2017-09-28_0010 true
vs0         fg          snapmirror.0241f354-a865-11e7-a1c0-
00a098a71764_2147867740.2017-10-04_124524 true
```

- b. qtrees機能が有効になっているSnapshotコピーをすべて削除します。 `volume snapshot delete`

```
-vserver svm_name -volume volume_name -snapshot snapshot_name -force true
-ignore-owners true
```

削除する必要がある Snapshot コピーは、通常の Snapshot コピーと、SnapMirror 関係用に作成された Snapshot コピーです。ONTAP 9.2 以前を実行しているデスティネーションクラスタを使用して FlexGroup ボリュームの SnapMirror 関係を作成した場合は、ソース FlexGroup ボリュームの qtrees 機能が有効なときに作成された Snapshot コピーをすべて削除する必要があります。

```
cluster1::> volume snapshot delete -vserver vs0 -volume fg -snapshot
daily.2017-09-27_0010 -force true -ignore-owners true
```

## 関連情報

### "FlexGroup ボリューム管理"

## ワークグループモードのSMBサーバの特定と移動

リバートを実行する前に、ワークグループモードのSMBサーバを削除するか、ドメインに移動する必要があります。ワークグループモードは、ONTAP 9 より前のバージョンの ONTAP ではサポートされていません。

1. ワークグループの認証形式を使用するSMBサーバを特定します。 `vserver cifs show`
2. 特定したサーバを移動または削除します。

実行する処理	使用するコマンド
ワークグループから Active Directory ドメインに SMB サーバを移動するには、次の手順を実行します。	<code>vserver cifs modify -vserver vserver_name -domain domain_name</code>
SMB サーバを削除	<code>vserver cifs delete -vserver vserver_name</code>

3. SMBサーバを削除した場合は、ドメインのユーザ名を入力し、ユーザパスワードを入力します。

## 関連情報

### "SMBの管理"

重複排除ボリュームにリバート前に十分な空きスペースがあることを確認します

ONTAP 9 のいずれかのバージョンからリバートする前に、リバート処理に使用する十分な空きスペースがボリュームにあることを確認する必要があります。

ゼロのブロックのインライン検出によって実現した削減に対応できる十分なスペースがボリュームに必要です。サポート技術情報の記事を参照してください ["ONTAP 9での重複排除、圧縮、およびコンパクションによるスペース削減効果の確認方法"](#)。

リバートするボリュームで重複排除とデータ圧縮の両方を有効にしている場合は、重複排除をリバートする前

にデータ圧縮をリバートする必要があります。

1. `volume efficiency show` コマンドに `-fields` オプションを指定して、ボリュームで実行されている効率化処理の進捗状況を表示します。

次のコマンドは、効率化処理の進捗状況を表示します。 `volume efficiency show -fields vserver, volume, progress`

2. `volume efficiency stop` コマンドに `-all` オプションを指定して、アクティブな重複排除処理とキューに登録されている重複排除処理をすべて中止します。

次のコマンドは、ボリュームVolAのアクティブな重複排除処理とキューに登録されている重複排除処理をすべて停止します。 `volume efficiency stop -vserver vs1 -volume VolA -all`

3. `set -privilege advanced` コマンドを使用して、`advanced` 権限レベルでログインします。
4. `volume efficiency revert-to` コマンドに `-version` オプションを指定して、ボリュームの効率化メタデータをONTAPの特定のバージョンにリバートします。

次のコマンドは、ボリュームVolAの効率化メタデータをONTAP 9.xにリバートします。 `volume efficiency revert-to -vserver vs1 -volume VolA -version 9.x`



`volume efficiency revert-to` コマンドは、このコマンドを実行するノードにあるボリュームをリバートします。ノード間でのボリュームのリバートは行いません。

5. `volume efficiency show` コマンドに `-op-status` オプションを指定して、ダウングレードの進捗状況を監視します。

次のコマンドは、ダウングレードのステータスを監視および表示します。 `volume efficiency show -vserver vs1 -op-status Downgrading`

6. リバートに失敗した場合は、`volume efficiency show` コマンドに `-instance` オプションを指定して、リバートに失敗した理由を確認します。

次のコマンドは、すべてのフィールドに関する詳細情報を表示します。 `volume efficiency show -vserver vs1 -volume vol1 - instance`

7. リバート処理の完了後、`admin`権限レベルに戻ります。 `set -privilege admin`

## "論理ストレージ管理"

リバート前に **Snapshot** コピーを準備する

以前の ONTAP リリースにリバートする前に、すべての Snapshot コピーポリシーを無効にして、現在のリリースへのアップグレード後に作成された Snapshot コピーを削除する必要があります。

SnapMirror 環境でリバートを実行する場合は、次のミラー関係を事前に削除しておく必要があります。

- すべての負荷共有ミラー関係
- ONTAP 8.3.x で作成したすべてのデータ保護ミラー関係

- ONTAP 8.3.x でクラスタが再作成された場合は、すべてのデータ保護ミラー関係

- a. すべてのデータSVMのSnapshotコピーポリシーを無効にします。 `volume snapshot policy modify -vserver * -enabled false`
- b. 各ノードのアグリゲートに対して Snapshot コピーポリシーを無効にします。
  - i. `run -nodeodnameaggr status` コマンドを使用して、ノードのアグリゲートを特定します。
  - ii. 各アグリゲートのSnapshotコピーポリシーを無効にします。 `run -node nodename aggr options aggr_name nosnap on`
  - iii. 残りのノードそれぞれに対して同じ手順を繰り返します。
- c. 各ノードのルートボリュームに対して Snapshot コピーポリシーを無効にします。
  - i. `run -nodeodevenostatus` コマンドを使用して、ノードのルートボリュームを特定します。

ルートボリュームは、`vol status` コマンドの出力で Options 列に root として表記されます。

```
vs1::> run -node node1 vol status
```

Volume	State	Status	Options
vol0	online	raid_dp, flex 64-bit	root, nvfail=on

- i. ルートボリュームのSnapshotコピーポリシーを無効にします。 `run -node nodename vol options root_volume_name nosnap on`
  - ii. 残りのノードそれぞれに対して同じ手順を繰り返します。
- d. 現在のリリースへのアップグレード後に作成された Snapshot コピーをすべて削除します。
    - i. 権限レベルを advanced に設定します。 `set -privilege advanced`
    - ii. Snapshotを無効にします。 `snapshot policy modify -vserver * -enabled false`
    - iii. ノードの新しいバージョンのSnapshotコピーを削除します。 `volume snapshot prepare-for-revert -node nodename`

このコマンドは、各データボリューム、ルートアグリゲート、およびルートボリュームの新しいバージョンの Snapshot コピーを削除します。

いずれかの Snapshot コピーを削除できない場合、コマンドは失敗し、Snapshot コピーの削除前に実施する必要があるアクションがあれば通知されます。必要なアクションを完了し、`volume snapshot prepare-for-revert` コマンドを再実行してから、次の手順に進んでください。

```
cluster1::*> volume snapshot prepare-for-revert -node node1
```

Warning: This command will delete all Snapshot copies that have the format used by the current version of ONTAP. It will fail if any Snapshot copy polices are enabled, or  
if any Snapshot copies have an owner. Continue? {y|n}: y

- i. Snapshotコピーが削除されたことを確認します。 `volume snapshot show -node nodename`

新しいバージョンのSnapshotコピーが残っている場合は、強制的に削除します。 `volume snapshot delete {-fs-version 9.0 -node nodename -is-constituent true} -ignore-owners -force`

- ii. 残りのノードそれぞれについて、手順 c を繰り返します。
- iii. admin 権限レベルに戻ります。 `set -privilege admin`



これらの手順を MetroCluster 構成内の両方のクラスタで実行する必要があります。

## SHA-2 ハッシュ関数を使用しているユーザアカウントを特定します

ONTAP 9.1 または ONTAP 9.0 から ONTAP 8.3.x にリバートする場合、SHA-2 アカウントユーザは元のパスワードで認証できなくなります。リバートを行う前に、SHA-2 ハッシュ関数を使用しているユーザアカウントを特定して、リバート後に、リバート後のリリースでサポートされている暗号化タイプ（MD5）を使用するようにパスワードをリセットする必要があります。

1. 権限の設定をadvancedに変更します。 `set -privilege advanced`
2. SHA-2に機能があるユーザアカウントを特定します。 `security login show -vserver * -username * -application * -authentication-method password -hash-function !md5`
3. コマンドの出力はリバート後も使用できるように保持しておきます。



リバートの実行中は、advanced権限レベルのコマンドを実行するように求められます `security login password-prepare-to-downgrade MD5`ハッシュ関数を使用するために自分のパスワードをリセットします。パスワードが MD5 で暗号化されていない場合は、新しいパスワードを入力するように求められ、MD5 で暗号化されます。これにより、リバート後にクレデンシャルが認証されるようになります。

**ONTAP 9.11.1以降からリバートする前に、Autonomous Ransomware Protectionのライセンスを確認してください**

自動ランサムウェア防御（ARP）を設定している場合に、ONTAP 9.11.1以降からONTAP 9.10.1以前にリバートすると、警告メッセージが表示され、ARP機能が制限されることがあります。

ONTAP 9.11.1では、アンチランサムウェアライセンスがMulti-Tenant Key Management（MTKM）ライセンス

に置き換えられました。お使いのシステムにAntiランサムウェアライセンスがあり、MT\_EK\_MGMTライセンスがない場合、リバート時にARPを有効にできないという警告が表示されます。

既存の保護が設定されたボリュームはリバート後も正常に機能し続け、ONTAP CLIを使用してARPステータスを表示できます。System Managerでは、MTKMライセンスがないとARPステータスを表示できません。

したがって、ONTAP 9.10.1に戻したあともARPを続行する場合は、リバート前にMTKMライセンスがインストールされていることを確認してください。 ["ARPライセンスについて説明します。"](#)

**ONTAP 9.12.1以降からリバートする前に、S3 NASバケット設定を削除してください**

NASデータ用のS3クライアントアクセスを設定している場合は、ONTAP 9.12.1以降からONTAP 9.11.1以前にリバートする前に、ONTAPコマンドラインインターフェイス（CLI）を使用してNASバケット設定を削除し、ネームマッピングを削除する必要があります。（S3ユーザからWindowsユーザまたはUNIXユーザへ）。

このタスクについて

リバートプロセスの実行中、以下のタスクがバックグラウンドで実行されます。

- 部分的に完了したシングルトンオブジェクトの作成をすべて削除します(つまり'非表示のディレクトリ内のすべてのエントリを削除します)
- 非表示のディレクトリをすべて削除します。S3 NASバケットにマッピングされたエクスポートのルートからアクセスできるボリュームごとに1つずつ存在する場合があります。
- アップロードテーブルを削除します。
- 設定されているすべてのS3サーバについて、default-unix-userおよびdefault-windows-userの値を削除します。

手順

1. S3 NASバケット設定を削除します。

```
vserver object-store-server bucket delete -vserver _svm_name_ -bucket  
_s3_nas_bucket_name_
```

2. UNIXのネームマッピングを削除します。

```
vserver name-mapping delete -vserver _svm_name_ -direction s3-unix
```

3. Windowsのネームマッピングを削除します。

```
vserver name-mapping delete -vserver _svm_name_ -direction s3-win
```

4. SVMからS3プロトコルを削除します。



```
vserver remove-protocols -vserver <svm_name> -protocols s3
```

### ONTAP 9.14.1以降からリバートする前にNFSv4.1セッショントランキング設定を削除する

クライアント接続のトランキングを有効にしている、ONTAP 9.14.1より前のリリースにリバートする場合は、リバート前にすべてのNFSv4.1サーバでトランキングを無効にする必要があります。

を入力すると、`revert-to` コマンドを実行すると、続行する前にトランキングを無効にするように求める警告メッセージが表示されます。

以前のONTAPリリースにリバートすると、トランク接続を使用するクライアントは単一の接続にフォールバックされます。データのスループットには影響しますが、システム停止は発生しません。リバートの動作は、SVMのNFSv4.1トランキングオプションをenabledからdisabledに変更した場合と同じです。

#### 手順

1. NFSv4.1サーバでトランキングを無効にします。+  
`vserver nfs modify -vserver svm_name -v4.1-trunking disabled`
2. NFSが必要に応じて設定されていることを確認します。+  
`vserver nfs show -vserver svm_name`

### 2 ノードと 4 ノードの MetroCluster 構成をリバートする前に自動計画外スイッチオーバーを無効にする

2 ノードまたは 4 ノード MetroCluster 構成をリバートする前に、Automatic Unplanned Switchover (AUSO ; 自動計画外スイッチオーバー) を無効にします。

1. MetroCluster の両方のクラスターで、自動計画外スイッチオーバーを無効にします。`metrocluster modify -auto-switchover-failure-domain auso-disabled`

#### 関連情報

["MetroCluster の管理とディザスタリカバリ"](#)

### MetroCluster 設定をリバートする前にIPSecを無効にしてください

MetroCluster 設定をリバートする前に、IPSecを無効にする必要があります。

IPSecが有効になっているONTAP 9.12.1を実行するMetroCluster 構成では、ONTAP をリバートできません。リバート前にチェックが実行され、MetroCluster 設定にIPSec設定が含まれていないことが確認されます。リバートを続行する前に、IPSecの設定をすべて削除してIPSecを無効にする必要があります。ユーザポリシーを設定していない場合でも、IPSecが有効になっていると、ONTAP のリバートがブロックされます。

### ONTAP ソフトウェアイメージをダウンロードしてインストールします

最初にNetApp Support Siteから ONTAP ソフトウェアをダウンロードして、インストールしておく必要があります。

## ソフトウェアイメージをダウンロードします

ONTAP 9.4 以降からダウングレードまたはリバートするには、ONTAP ソフトウェアイメージを NetApp Support Site からローカルフォルダにコピーします。ONTAP 9.3 以前にダウングレードまたはリバートする場合は、ONTAP ソフトウェアイメージをネットワーク上の HTTP サーバまたは FTP サーバにコピーする必要があります。

次の重要な情報に注意してください。

- ソフトウェアイメージはプラットフォームモデルに固有です。

ご使用のクラスタに対応するイメージを取得してください。ソフトウェアイメージ、ファームウェアのバージョン情報、プラットフォームモデルの最新のファームウェアは、NetApp Support Site で入手できます。

- ソフトウェアイメージには、ONTAP の特定のバージョンのリリース時点でのシステムファームウェアの最新バージョンが含まれています。
- ONTAP 9.5 以降から NetApp Volume Encryption を搭載したシステムをダウングレードする場合は、NetApp Volume Encryption を含む制限のない国の ONTAP ソフトウェアイメージをダウンロードする必要があります。

規制対象国用の ONTAP ソフトウェアイメージを使用して NetApp Volume Encryption を搭載したシステムをダウングレードまたはリバートすると、システムがパニック状態になり、ボリュームへのアクセスが失われます。

- a. で、対象となる ONTAP ソフトウェアを見つけます ["ソフトウェアのダウンロード"](#) NetApp Support Site の領域。
- b. ソフトウェアイメージをコピーします。
  - ONTAP 9.3 以前の場合は、NetApp Support Site から、イメージを提供する HTTP サーバまたは FTP サーバ上のディレクトリにソフトウェアイメージ（93\_q\_image.tgz など）をコピーします。
  - ONTAP 9.4 以降の場合は、NetApp Support Site から、イメージを提供する HTTP サーバまたは FTP サーバ上のディレクトリかローカルフォルダにソフトウェアイメージ（97\_q\_image.tgz など）をコピーします。

## ソフトウェアイメージをインストールします

ターゲットのソフトウェアイメージをクラスタのノードにインストールする必要があります。

- ONTAP 9.5 以降から NetApp Volume Encryption を搭載したシステムをダウングレードまたはリバートする場合は、NetApp Volume Encryption を含む制限のない国の ONTAP ソフトウェアイメージをダウンロードしておく必要があります。

規制対象国用の ONTAP ソフトウェアイメージを使用して NetApp Volume Encryption を搭載したシステムをダウングレードまたはリバートすると、システムがパニック状態になり、ボリュームへのアクセスが失われます。

- a. 権限レベルを advanced に設定します。続行するかどうかを尋ねられたら、「\*y\*」と入力します。

```
set -privilege advanced
```

advanced プロンプトが表示されます (\*>) が表示されます。

- b. ソフトウェアイメージをノードにインストールします。

このコマンドを実行すると、ソフトウェアイメージがすべてのノードに同時にダウンロードされてインストールされます。一度に1つずつ各ノードにイメージをダウンロードしてインストールする場合は、`-background` パラメータを指定せずに実行します。

- MetroCluster以外の構成または2ノードMetroCluster 構成をダウングレードまたはリバートする場合は、次の手順を実行します。`system node image update -node * -package location -replace-package true -setdefault true -background true`

このコマンドでは、拡張クエリを使用して、代替イメージとしてインストールされるターゲットのソフトウェアイメージがノードのデフォルトのイメージになるように変更します。

- 4ノードまたは8ノードMetroCluster 構成をダウングレードまたはリバートする場合は、両方のクラスタで次のコマンドを問題 する必要があります。`system node image update -node * -package location -replace-package true true -background true -setdefault false`

このコマンドでは、拡張クエリを使用して、各ノードに代替イメージとしてインストールされるターゲットソフトウェアイメージを変更します。

- c. 入力するコマンド `y` プロンプトが表示されたら続行します。

- d. ソフトウェアイメージが各ノードにダウンロードおよびインストールされたことを確認します。

```
system node image show-update-progress -node *
```

このコマンドは、ソフトウェアイメージのダウンロードとインストールの現在のステータスを表示します。すべてのノードの Run Status が Exited になり、Exit Status が Success になるまで、このコマンドを繰り返し実行します。

`system node image update` コマンドが失敗して、エラーまたは警告メッセージが表示されることがあります。エラーまたは警告を解決したら、もう一度コマンドを実行できます。

次の例では、2 ノードクラスタの両方のノードでソフトウェアイメージのダウンロードとインストールが正常に完了しています。

```
cluster1::*> system node image show-update-progress -node *
There is no update/install in progress
Status of most recent operation:
    Run Status:      Exited
    Exit Status:     Success
    Phase:           Run Script
    Exit Message:    After a clean shutdown, image2 will be set as
the default boot image on node0.
There is no update/install in progress
Status of most recent operation:
    Run Status:      Exited
    Exit Status:     Success
    Phase:           Run Script
    Exit Message:    After a clean shutdown, image2 will be set as
the default boot image on node1.
2 entries were acted on.
```

## ONTAP クラスタをリバートする

クラスタをオフラインにして以前の ONTAP リリースにリバートするには、ストレージフェイルオーバーとデータ LIF を無効にし、リバートの前提条件を満たしていることを確認してから、ノードのクラスタ設定とファイルシステム設定をリバートします。この処理をクラスタの他の各ノードに対して繰り返す必要があります。

リバートを完了しておく必要があります ["検証"](#) および ["事前チェック"](#)。

クラスタをリバートするには、クラスタをオフラインにした状態でリバートを行う必要があります。

1. 権限レベルを advanced に設定します。 `set -privilege advanced`

続行するかどうかを尋ねられたら、「\* y \*」と入力します。

2. ターゲットの ONTAP ソフトウェアがインストールされていることを確認します。 `system image show`

次の例では、両方のノードに代替イメージとしてバージョン 9.1 がインストールされています。

```
cluster1::*> system image show
```

Node	Image	Is Default	Is Current	Version	Install Date
-----					
node0					
	image1	true	true	9.2	MM/DD/YYYY TIME
	image2	false	false	9.1	MM/DD/YYYY TIME
node1					
	image1	true	true	9.2	MM/DD/YYYY TIME
	image2	false	false	9.1	MM/DD/YYYY TIME

4 entries were displayed.

3. クラスタ内のすべてのデータLIFを無効にします。 `network interface modify {-role data} -status-admin down`
4. クラスタ間FlexCache 関係があるかどうかを確認します。 `flexcache origin show-caches -relationship-type inter-cluster`
5. クラスタ間フラッシュが存在する場合は、キャッシュクラスタのデータLIFを無効にします。 `network interface modify -vserver vservice_name -lif lif_name -status-admin down`
6. クラスタが2つのノードだけで構成されている場合は、クラスタHAを無効にします。 `cluster ha modify -configured false`
7. どちらかのノードからHAペアのノードのストレージフェイルオーバーを無効にします。 `storage failover modify -node nodename -enabled false`

ストレージフェイルオーバーを無効にするのは、HA ペアに対して 1 度だけです。ノードのストレージフェイルオーバーを無効にすると、そのノードのパートナーでもストレージフェイルオーバーが無効になります。

8. リバートするノードにログインします。

ノードをリバートするには、そのノードのノード管理 LIF を通じてクラスタにログインする必要があります。

9. ノードのターゲットONTAP ソフトウェアイメージをデフォルトのイメージとして設定します。 `system image modify -node nodename -image target_image -isdefault true`
10. ターゲットのONTAP ソフトウェアイメージが、リバートするノードのデフォルトのイメージとして設定されたことを確認します。 `system image show`

次の例では、node0 でデフォルトのイメージとしてバージョン 9.1 が設定されています。

```
cluster1::*> system image show
```

Node	Image	Is Default	Is Current	Version	Install Date
-----					
node0					
	image1	false	true	9.2	MM/DD/YYYY TIME
	image2	true	false	9.1	MM/DD/YYYY TIME
node1					
	image1	true	true	9.2	MM/DD/YYYY TIME
	image2	false	false	9.1	MM/DD/YYYY TIME

4 entries were displayed.

11. クラスタが2つのノードだけで構成されている場合は、ノードにイプシロンが設定されていないことを確認します。

- ノードにイプシロンが現在設定されているかどうかを確認します。 `cluster show -node nodename`

次の例では、ノードにイプシロンが設定されています。

```
cluster1::*> cluster show -node node1
```

```
Node: node1
UUID: 026efc12-ac1a-11e0-80ed-0f7eba8fc313
Epsilon: true
Eligibility: true
Health: true
```

- ノードにイプシロンが設定されている場合は、イプシロンをパートナーに転送できるように、イプシロンをfalseに設定します。 `cluster modify -node nodenameA -epsilon false`
- パートナーノードでイプシロンをtrueに設定して、イプシロンをパートナーに転送します。 `cluster modify -node nodenameB -epsilon true`

12. ノードをリバートする準備が完了していることを確認します。 `system node revert-to -node nodename -check-only true -version 9.x`

check-only パラメータを指定すると、リバートを行う前に対処する必要がある前提条件が特定されます。これには、たとえば次のような処理が含まれます。

- ストレージフェイルオーバーを無効にします
- Snapshot ポリシーを無効にします
- 新しいバージョンの ONTAP へのアップグレード後に作成された Snapshot コピーを削除する

13. すべての前提条件を満たしていることを確認します。 `system node revert-to -node nodename -check-only true -version 9.x`

14. ノードのクラスタ構成をリバートします。 `system node revert-to -node nodename -version 9.x`

version オプションは、ターゲットのリリースを表します。たとえば、確認したインストール済みのソフトウェアが ONTAP 9.1 であれば、-version オプションの値は 9.1 になります。

クラスタ設定がリバートされ、クラスタシェルからログアウトされます。

15. もう一度クラスタシェルにログインし、ノードシェルに切り替えます。 `run -node nodename`

クラスタシェルに再度ログインしたあと、ノードシェルコマンドを使用できるようになるまでに数分かかることがあります。そのため、コマンドが失敗した場合は数分待ってからもう一度実行してください。

16. ノードのファイルシステム設定をリバートします。 `revert_to 9.x`

このコマンドを実行すると、ノードのファイルシステム設定をリバートする準備が完了していることが検証され、そのあとにリバートが実行されます。前提条件が示された場合は、それに対処してから `revert_to` コマンドを再実行する必要があります。



システムコンソールを使用してリバートプロセスを監視すると、ノードシェルよりも詳細な情報が表示されます。

AUTOBOOT が true に設定されている場合は、コマンドが完了すると、ノードで ONTAP がリブートされます。

AUTOBOOT が false に設定されている場合は、コマンドで LOADER プロンプトが表示されます。入力するコマンド `yes` を使用してリバートし、を使用します `boot_ontap` ノードを手動でリブートします。

17. ノードがリブートしたら、新しいソフトウェアが実行されていることを確認します。 `system node image show`

次の例では、image1 が新しい ONTAP バージョンで、node0 で現在のバージョンとして設定されています。

```
cluster1::*> system node image show
```

Node	Image	Is Default	Is Current	Version	Install Date
node0	image1	true	true	X.X.X	MM/DD/YYYY TIME
	image2	false	false	Y.Y.Y	MM/DD/YYYY TIME
node1	image1	true	false	X.X.X	MM/DD/YYYY TIME
	image2	false	true	Y.Y.Y	MM/DD/YYYY TIME

4 entries were displayed.

18. [[step-16 ]]各ノードのリバートステータスが完了していることを確認します。 `system node upgrade-revert show -node nodename`

ステータスが「complete」、「not needed」、または「There are no table entries returned」のいずれかになっている必要があります。

19. 繰り返します [\[step-6\]](#) から [\[step-16\]](#) HA ペアのもう一方のノード。
20. クラスタが2つのノードだけで構成されている場合は、クラスタHAを再度有効にします。 `cluster ha modify -configured true`
21. ストレージフェイルオーバーを無効にした場合は、両方のノードで再度有効にします。 `storage failover modify -node nodename -enabled true`
22. 繰り返します [\[step-5\]](#) から [\[step-19\]](#) MetroCluster 構成で、HA ペアのそれぞれおよび両方のクラスタを追加します。

## クラスタをリバートしたあとに何をすればよいですか？

ダウングレードまたはリバート後にクラスタとストレージの健全性を確認

クラスタをダウングレードまたはリバートしたら、ノードが正常に機能していてクラスタに追加するための条件を満たしていること、およびクラスタがクォーラムにあることを確認する必要があります。また、ディスク、アグリゲート、およびボリュームのステータスも確認する必要があります。

クラスタの健全性を確認

1. クラスタ内のノードがオンラインで、クラスタに追加するための条件を満たしていることを確認します。  
`cluster show`

```
cluster1::> cluster show
Node                      Health  Eligibility
-----
node0                     true    true
node1                     true    true
```

正常に機能していないノードや条件を満たしていないノードがある場合は、EMS ログでエラーを確認して適切に修正します。

2. 権限レベルをadvancedに設定+  
`set -privilege advanced`

入力するコマンド `y` 続行します。

3. 各 RDB プロセスの構成の詳細を確認します。
  - リレーショナルデータベースのエポックとデータベースのエポックが各ノードで一致すること。
  - リングごとのクォーラムマスターがすべてのノードで同じであることが必要です。

各リングのクォーラムマスターが異なる場合があることに注意してください。



表示する <b>RDB</b> プロセス	入力するコマンド
管理アプリケーション	<code>cluster ring show -unitname mgmt</code>
ボリュームロケーションデータベース	<code>cluster ring show -unitname vlodb</code>
仮想インターフェイスマネージャ	<code>cluster ring show -unitname vifmgr</code>
SAN 管理デーモン	<code>cluster ring show -unitname bcomd</code>

次の例は、ボリュームロケーションデータベースのプロセスを示しています。

```
cluster1::*> cluster ring show -unitname vlodb
```

Node	UnitName	Epoch	DB Epoch	DB Trnxs	Master	Online
node0	vlodb	154	154	14847	node0	master
node1	vlodb	154	154	14847	node0	secondary
node2	vlodb	154	154	14847	node0	secondary
node3	vlodb	154	154	14847	node0	secondary

4 entries were displayed.

4. admin 権限レベルに戻ります。 `set -privilege admin`
5. SAN 環境を使用している場合は、各ノードが SAN クォーラムにあることを確認します。 `event log show -severity informational -message-name scsiblade.*`

各ノードの最新の scsiblade イベントメッセージに、SCSI ブレードがクォーラムにあることが示されます。

```
cluster1::*> event log show -severity informational -message-name
scsiblade.*
```

Time	Node	Severity	Event
MM/DD/YYYY TIME	node0	INFORMATIONAL	scsiblade.in.quorum: The scsi-blade ...
MM/DD/YYYY TIME	node1	INFORMATIONAL	scsiblade.in.quorum: The scsi-blade ...

## 関連情報

### "システム管理"

#### ストレージの健全性を確認

クラスタをリバートまたはダウングレードしたら、ディスク、アグリゲート、およびボリュームのステータスを確認する必要があります。

## 1. ディスクのステータスを確認します。

確認する項目	手順
破損ディスク	a. 破損ディスクを表示します。 <code>storage disk show -state broken</code> b. 破損ディスクを取り外すか交換します。
メンテナンス中または再構築中のディスク	a. 保守、保留、または再構築の状態のディスクを表示します。 <code>storage disk show -state maintenance</code>
pending	reconstructing` .. メンテナンスまたは再構築の処理が完了するまで待ってから次に進みます。

## 2. ストレージアグリゲートを含む物理ストレージと論理ストレージの状態を表示して、すべてのアグリゲートがオンラインであることを確認します。 `storage aggregate show -state !online`

このコマンドを実行すると、オンラインでないアグリゲートが表示されます。メジャーアップグレードまたはリバートの実行前と実行後には、すべてのアグリゲートがオンラインになっている必要があります。

```
cluster1::> storage aggregate show -state !online
There are no entries matching your query.
```

## 3. 次のコマンドを実行して、すべてのボリュームがオンラインであることを確認します。 `_not_online volume show -state !online`

メジャーアップグレードまたはリバートの実行前と実行後には、すべてのボリュームがオンラインになっている必要があります。

```
cluster1::> volume show -state !online
There are no entries matching your query.
```

## 4. 整合性のないボリュームがないことを確認します。 `volume show -is-inconsistent true`

サポート技術情報の記事を参照してください "[「WAFL inconsistent」を示すボリューム](#)" を参照してください。

### 関連情報

["ディスクおよびアグリゲートの管理"](#)

### MetroCluster 構成の自動スイッチオーバーを有効にします

ここでは、MetroCluster 構成のリバート後に実行する必要がある追加の作業について説明します。

1. 自動計画外スイッチオーバーを有効にします。 `metrocluster modify -auto-switchover -failure-domain auto-on-cluster-disaster`
2. MetroCluster 構成を検証します。 `metrocluster check run`

リバート後に **LIF** を有効にしてホームポートにリバートする

リブートを実行すると、一部の LIF が割り当てられているフェイルオーバーポートに移行されることがあります。クラスタをリバートしたら、ホームポートにない LIF を有効にしてリバートする必要があります。

ホームポートが動作している場合は、`network interface revert` コマンドによって、現在ホームポートにない LIF がホームポートにリバートされます。LIF のホームポートは LIF の作成時に指定します。指定されているホームポートは、`network interface show` コマンドを使用して確認できます。

1. すべてのLIFのステータスを表示します。 `network interface show`

Storage Virtual Machine （SVM） のすべての LIF のステータスを表示する例を次に示します。

```
cluster1::> network interface show -vserver vs0
```

	Logical	Status	Network	Current	
Current Is					
Vserver	Interface	Admin/Oper	Address/Mask	Node	Port
Home					
-----	-----	-----	-----	-----	
-----	-----				
vs0					
	data001	down/down	192.0.2.120/24	node0	e0e
true					
	data002	down/down	192.0.2.121/24	node0	e0f
true					
	data003	down/down	192.0.2.122/24	node0	e2a
true					
	data004	down/down	192.0.2.123/24	node0	e2b
true					
	data005	down/down	192.0.2.124/24	node0	e0e
false					
	data006	down/down	192.0.2.125/24	node0	e0f
false					
	data007	down/down	192.0.2.126/24	node0	e2a
false					
	data008	down/down	192.0.2.127/24	node0	e2b
false					

8 entries were displayed.

Status Admin ステータスが down になっている LIF や Is home ステータスが false になっている LIF がある場合は次の手順に進みます。

2. データLIFを有効にします。network interface modify {-role data} -status-admin up

```
cluster1::> network interface modify {-role data} -status-admin up
8 entries were modified.
```

3. LIFをそれぞれのホームポートにリバートします。network interface revert \*

このコマンドを実行すると、すべての LIF がそれぞれのホームポートにリバートされます。

```
cluster1::> network interface revert *
8 entries were acted on.
```

4. すべてのLIFがそれぞれのホームポートにあることを確認します。network interface show

次の例では、SVM vs0 のすべての LIF がそれぞれのホームポートにあります。

```
cluster1::> network interface show -vserver vs0
```

	Logical	Status	Network	Current	
Current Is					
Vserver	Interface	Admin/Oper	Address/Mask	Node	Port
Home					
-----	-----	-----	-----	-----	-----
vs0					
	data001	up/up	192.0.2.120/24	node0	e0e
true					
	data002	up/up	192.0.2.121/24	node0	e0f
true					
	data003	up/up	192.0.2.122/24	node0	e2a
true					
	data004	up/up	192.0.2.123/24	node0	e2b
true					
	data005	up/up	192.0.2.124/24	node1	e0e
true					
	data006	up/up	192.0.2.125/24	node1	e0f
true					
	data007	up/up	192.0.2.126/24	node1	e2a
true					
	data008	up/up	192.0.2.127/24	node1	e2b
true					

```
8 entries were displayed.
```

リバート後に **Snapshot** コピーポリシーを有効にする

以前のバージョンの ONTAP にリバートした場合は、Snapshot コピーの作成を再開するために、Snapshot コピーポリシーを有効にする必要があります。

以前のバージョンの ONTAP にリバートする前に無効にした Snapshot スケジュールを再度有効にします。

1. すべてのデータ SVM の Snapshot コピーポリシーを有効にします。

```
volume snapshot policy modify -vserver * -enabled true
```

```
snapshot policy modify pg-rpo-hourly -enable true
```

2. 各ノードについて、`run nodeodevenevol options root_vol_namenosnapoff` コマンドを使用して、ルートボリュームの Snapshot コピーポリシーを有効にします。

```
cluster1::> run -node node1 vol options vol0 nosnap off
```

クライアントアクセスの確認 (**SMB**と**NFS**)

設定されているプロトコルについて、SMBクライアントとNFSクライアントからのアクセスをテストして、クラスタにアクセスできることを確認します。

**IPv6** ファイアウォールエントリを確認します

ONTAP 9 のいずれかのバージョンからのリバートを実行すると、ファイアウォールポリシーの一部のサービスのデフォルトの IPv6 ファイアウォールエントリが失われる可能性があります。必要なファイアウォールエントリがシステムにリストアされていることを確認する必要があります。

1. すべてのファイアウォールポリシーをデフォルトのポリシーと比較して、正しいことを確認します。

```
system services firewall policy show
```

次の例は、デフォルトのポリシーを示しています。

```
cluster1::*> system services firewall policy show
```

Policy	Service	Action	IP-List
-----			
cluster			
	dns	allow	0.0.0.0/0
	http	allow	0.0.0.0/0
	https	allow	0.0.0.0/0
	ndmp	allow	0.0.0.0/0
	ntp	allow	0.0.0.0/0
	rsh	allow	0.0.0.0/0
	snmp	allow	0.0.0.0/0
	ssh	allow	0.0.0.0/0
	telnet	allow	0.0.0.0/0
data			
	dns	allow	0.0.0.0/0, ::/0
	http	deny	0.0.0.0/0, ::/0
	https	deny	0.0.0.0/0, ::/0
	ndmp	allow	0.0.0.0/0, ::/0
	ntp	deny	0.0.0.0/0, ::/0
	rsh	deny	0.0.0.0/0, ::/0
.			
.			
.			

2. 新しいファイアウォールポリシーを作成して、不足しているデフォルトのIPv6ファイアウォールエントリを手動で追加します。 `system services firewall policy create`

```
cluster1::*> system services firewall policy create -policy newIPv6  
-service ssh -action allow -ip-list ::/0
```

3. 新しいポリシーをLIFに適用してネットワークサービスへのアクセスを許可します。 `network interface modify`

```
cluster1::*> network interface modify -vserver VS1 -lif LIF1  
-firewall-policy newIPv6
```

パスワードのハッシュ関数をサポートされる暗号化タイプにリバートします

ONTAP 9.1 または ONTAP 9.0 から ONTAP 8.3.x にリバートした場合、SHA-2 アカウントユーザは元のパスワードで認証できなくなります。MDS の暗号化タイプを使用するには、パスワードをリセットする必要があります。

1. SHA-2 ユーザアカウントごとに一時パスワードを設定します [リバート前に特定します](#) : `security`

```
login password -username user_name -vserver vserver_name
```

2. 影響を受けるユーザに一時パスワードを送信します。ユーザに、コンソールまたは SSH セッションからログインして、表示される指示に従ってパスワードを変更するよう指示します。

#### SP ファームウェアを手動で更新するかどうかを判断するための考慮事項

SP 自動更新機能が有効な場合（デフォルト）は、ONTAP 8.3.x にダウングレードまたはリバートするときに、SP ファームウェアを手動で更新する必要はありません。SP ファームウェアは、リバートまたはダウングレード後の ONTAP のバージョンでサポートされている最新の互換バージョンに自動的に更新されます。

SP 自動更新機能が無効になっている（非推奨）場合は、ONTAP のリバートまたはダウングレードのプロセスが完了したら、リバートまたはダウングレードしたバージョンの ONTAP でサポートされる SP ファームウェアのバージョンに手動で更新する必要があります。

["NetApp BIOS / ONTAP サポートマトリックス"](#)

["ネットアップのダウンロード：システムファームウェアおよび診断"](#)

サービスプロセッサにアクセスできるユーザアカウントが変更されました

ONTAP 9.8以前でユーザアカウントを作成した場合は、ONTAP 9.9.1以降にアップグレード（の場合） `-role` パラメータ

が変更されました `admin`）をクリックし、ONTAP 9.8以前にリバートしました `-role` パラメータが元の値に戻ります。ただし、変更した値を使用できることを確認する必要があります。

リバート中にSPユーザのロールが削除されると、「rbac.spuser.role.notfound」というEMSメッセージが記録されます。

詳細については、を参照してください ["SP にアクセスできるアカウント"](#)。

# クラスタ管理

## System Manager を使用したクラスタ管理

### System Manager の管理の概要

System Managerは、HTML5ベースのグラフィカルな管理インターフェイスで、ストレージシステムとストレージオブジェクト（ディスク、ボリューム、ストレージ階層など）の管理やストレージシステムに関連する一般的な管理タスクの実行にWebブラウザを使用できます。

このセクションで説明する手順は、ONTAP 9.7 以降のリリースの System Manager を使用してクラスタを管理する場合に役立ちます。



- System ManagerはWebサービスとしてONTAPソフトウェアに搭載されており、デフォルトで有効になっていて、ブラウザからアクセスできます。
- ONTAP 9.6 以降では、System Manager の名前が変更されています。ONTAP 9.5 以前では、OnCommand システムマネージャと呼ばれていました。ONTAP 9.6 以降では、System Manager と呼ばれます。
- 従来の System Manager （ONTAP 9.7 以前でのみ使用可能）を使用している場合は、を参照してください "[System Manager Classic （ONTAP 9.0 から 9.7）](#)"

System Manager のダッシュボードを使用すると、重要なアラートと通知、ストレージ階層とボリュームの効率性と容量、クラスタで使用可能なノード、HA ペアのノードのステータス、最もアクティブなアプリケーションとオブジェクト、およびクラスタまたはノードのパフォーマンス指標。

System Manager では、次のような多くの一般的な作業を実行できます。

- クラスタを作成し、ネットワークを設定し、クラスタのサポートの詳細を設定する。
- ディスク、ローカル階層、ボリューム、qtree などのストレージオブジェクトを構成し、管理する クォータが含まれます。
- SMB および NFS などのプロトコルを設定し、ファイル共有をプロビジョニングする
- FC 、 FCoE 、 NVMe 、 iSCSI などのプロトコルをブロックアクセス用に設定する。
- サブネット、ブロードキャストドメイン、データ / 管理インターフェイス、インターフェイスグループなどのネットワークコンポーネントを作成および設定する。
- ミラー関係とバックアップ関係をセットアップおよび管理する。
- クラスタ管理、ストレージノード管理、および Storage Virtual Machine （ Storage VM ） 管理の処理を実行する。
- Storage VM の作成と設定、Storage VM に関連付けられたストレージオブジェクトの管理、および Storage VM サービスの管理を行う。
- クラスタでハイアベイラビリティ（HA）構成を監視および管理する。
- ノードに対してその状態に関係なくリモートでログイン、管理、監視、および管理を行うようにサービスプロセッサを設定します。



## System Manager の用語

System Manager では、ONTAP の一部の主要機能について、CLI とは異なる用語が使用されます。

- \* ローカルティア \* –データを保存する物理ソリッドステート・ドライブまたはハードディスク・ドライブのセット。これらはアグリゲートとして認識されていることがあります。実際、ONTAP CLI を使用している場合は、ローカル階層を表す用語として「\_aggregate\_used」が表示されます。
- \* クラウド階層 \* – ONTAP で使用されるクラウド内のストレージで、何らかの理由でデータをオンプレミスに保存する必要がある場合。FabricPool のクラウド部分について考えている場合は、すでにその点を把握しています。また、StorageGRID システムを使用している場合は、クラウドがオフプレミスになっているとは限りません。（オンプレミスでのクラウドレベルのエクスぺリエンスは、*private\_cloud* と呼ばれています）。
- \* Storage VM \* – ONTAP 内で実行される仮想マシンで、クライアントにストレージサービスとデータサービスを提供します。これは、\_SVM\_ または \_SVM\_ であることがわかります。
- ネットワークインターフェイス-物理ネットワークポートに割り当てられたアドレスとプロパティ。これは、\_論理インターフェイス（LIF）\_ であることがわかります。
- \* Pause \* - 処理を停止するアクション。ONTAP 9.8 より前のバージョンの System Manager では、\_quiesce と呼ぶこともあります。

## System Manager を使用してクラスタにアクセスする

コマンドラインインターフェイス（CLI）ではなくグラフィカルインターフェイスを使用してクラスタにアクセスして管理するには、System Manager を使用します。

System Manager は ONTAP に搭載されている Web サービスでデフォルトで有効になっており、ブラウザを使用してアクセスできます。

ONTAP 9.12.1以降、System ManagerはBlueXPと完全に統合されています。



BlueXPを使用すると、使い慣れたSystem Managerダッシュボードを維持しながら、単一のコントロールプレーンからハイブリッドマルチクラウドインフラを管理できます。

を参照してください ["System ManagerとBlueXPの統合"](#)。

### このタスクについて

System Managerには、クラスタ管理ネットワークインターフェイス（LIF）またはノード管理ネットワークインターフェイス（LIF）を使用してアクセスできます。System Managerに無停止でアクセスするには、クラスタ管理ネットワークインターフェイス（LIF）を使用する必要があります。

### 作業を開始する前に

- 「admin」ロールと「http」アプリケーションタイプおよび「console」アプリケーションタイプで構成されたクラスタユーザアカウントが必要です。
- ブラウザでクッキーとサイトのデータを有効にしておく必要があります。

### 手順

1. Webブラウザで、クラスタ管理ネットワークインターフェイスのIPアドレスを指定してアクセスします。

◦ IPv4を使用する場合： **`https://cluster-mgmt-LIF`**

- IPv6を使用する場合：[https://\[cluster-mgmt-LIF\]](https://[cluster-mgmt-LIF])



System Manager のブラウザアクセスでサポートされるのは HTTPS のみです。

自己署名のデジタル証明書がクラスタで使用されている場合、信頼されていない証明書であることを示す警告がブラウザ画面に表示されることがあります。危険を承諾してアクセスを続行するか、認証局（CA）の署名のあるデジタル証明書をクラスタにインストールしてサーバを認証します。

2. \* オプション： \* CLI を使用してアクセスバナーを設定している場合は、 \* 警告 \* ダイアログボックスに表示されるメッセージを読み、必要なオプションを選択して続行します。

Security Assertion Markup Language（SAML）認証が有効になっているシステムでは、このオプションはサポートされていません。

- 続行しない場合は、 \* Cancel \* をクリックしてブラウザを閉じます。
- 続行する場合は、 \* OK \* をクリックして System Manager のログインページに移動します。

3. クラスタ管理者のクレデンシャルを使用して System Manager にログインします。



ONTAP 9.11.1以降では、System Managerにログインするときにロケールを指定できます。ロケールでは、言語、通貨、時刻と日付の形式、同様の設定など、特定のローカライズ設定が指定されます。ONTAP 9.10.1以前のバージョンでは、System Managerのロケールがブラウザで検出されました。System Managerのロケールを変更するには、ブラウザのロケールを変更する必要があります。

4. オプション: ONTAP 9.12.1以降では、System Managerの外観を指定できます。
  - a. System Managerの右上にあるをクリックします ユーザーオプションを管理するには、次の手順
  - b. 「システムテーマ」トグルスイッチを希望の位置に合わせます。

位置を切り替えます	外観の設定
(写真左)	ライトテーマ（ダークテキストの背景）
OS（中央）	デフォルトでは、オペレーティングシステムのアプリケーションに設定されたテーマの設定（通常はSystem Managerへのアクセスに使用されるブラウザのテーマの設定）です。
(写真右)	ダークテーマ（明るいテキストの背景が暗い）

## 関連情報

["Web サービスへのアクセスの管理"](#)

["Web ブラウザを使用してノードのログファイル、コアダンプファイル、および MIB ファイルにアクセスする"](#)


## ライセンスキーを追加して新しい機能を有効にします

ONTAP 9.10.1より前のリリースでは、ONTAPの機能はライセンスキーで有効になり、ONTAP 9.10.1以降の機能はNetAppライセンスファイルで有効になります。System Managerを使用して、ライセンスキーとNetAppライセンスファイルを追加できます。

ONTAP 9.10.1以降では、System Managerを使用してネットアップライセンスファイルをインストールし、複数のライセンス機能を一度に有効にすることができます。NetApp License Fileを使用すると、個別の機能ライセンスキーを追加する必要がなくなるため、ライセンスのインストールが簡単になります。NetApp Support Siteからネットアップライセンスファイルをダウンロードします。

一部の機能のライセンスキーがすでに存在しており、ONTAP 9.10.1にアップグレードする場合も、引き続きそれらのライセンスキーを使用できます。


### 手順

1. [\* Cluster]>[Settings] (設定) \*を選択します。
2. [ライセンス]\*で、 .
3. [\* 参照 \*]を選択します。ダウンロードしたNetAppライセンスファイルを選択します。
4. 追加するライセンスキーがある場合は、「\* 28 文字のライセンスキーを使用する \*」を選択して、キーを入力します。

## クラスタ構成をダウンロードします

ONTAP 9.11.1以降では、System Managerを使用してクラスタの構成をダウンロードできます。

### 手順

1. [\* Cluster] > [Overview] をクリックします。
2. をクリックします  をクリックしてドロップダウンメニューを表示します。
3. [Download configuration]\*を選択します。
4. HAペアを選択し、\*[ダウンロード]\*をクリックします。

設定はExcelスプレッドシートとしてダウンロードされます。

- 最初のシートにはクラスタの詳細が含まれています。
- 他のシートにはノードの詳細が含まれています。

## クラスタへのタグの割り当て

ONTAP 9.14.1以降では、System Managerを使用してクラスタにタグを割り当て、プロジェクトやコストセンターなどのカテゴリに属するオブジェクトを識別することができます。

### このタスクについて

クラスタにタグを割り当てることができます。まず、タグを定義して追加する必要があります。その後、タ

グを編集または削除することもできます。

タグは、クラスタの作成時に追加することも、あとから追加することもできます。

タグを定義するには、キーを指定し、`"key:value"`の形式で値を関連付けます。たとえば、「dept:engineering」や「location:san-jose」などです。

タグを作成するときは、次の点を考慮する必要があります。

- キーの長さは1文字以上で、nullにすることはできません。値にはnullを指定できます。
- キーは、値をカンマで区切って複数の値とペアにすることができます（例：`"location:san-jose, Toronto"`）。
- タグは複数のリソースに使用できます。
- キーの先頭は小文字にする必要があります。

## 手順


タグを管理するには、次の手順を実行します。

1. System Managerで、\*[クラスタ]\*をクリックして概要ページを表示します。

タグは\* Tags \*セクションに表示されます。

2. [タグの管理]\*をクリックして、既存のタグを変更するか、新しいタグを追加します。

タグを追加、編集、または削除できます。

実行する処理	実行する手順
タグの追加	<ol style="list-style-type: none"><li>a. [タグの追加]*をクリックします。</li><li>b. キーとその値を指定します（複数の値はカンマで区切ります）。</li><li>c. [保存（Save）]をクリックします。</li></ol>
タグの編集	<ol style="list-style-type: none"><li>a. 「* Key」および「Values（オプション）*」フィールドの内容を変更します。</li><li>b. [保存（Save）]をクリックします。</li></ol>
タグを削除します	<ol style="list-style-type: none"><li>a. をクリックします  をクリックします。</li></ol>

## サポートケースの表示と送信

ONTAP 9.9.1以降では、クラスタに関連付けられているActive IQ でサポートケースを確認できます。NetApp Support Siteで新しいサポートケースを送信するために必要なクラスタの詳細をコピーすることもできます。

ONTAP 9.10.1以降ではテレメトリログを有効にすることができるため、サポート担当者による問題のトラブルシューティングに役立ちます。



ファームウェアの更新に関するアラートを受信するには、Active IQ Unified Manager に登録する必要があります。を参照してください "[Active IQ Unified Manager のドキュメント](#)"。

#### 手順

1. System Manager で、 \* Support \* を選択します。

このクラスタに関連付けられている、開いているサポートケースのリストが表示されます。

2. 次のリンクをクリックして手順を実行します。

- \* ケース番号 \* : ケースの詳細を参照してください。
- \* NetApp Support Siteにアクセス \* : NetApp Support Siteの「My AutoSupport」ページに移動して、ナレッジベースの記事を参照したり、新しいサポートケースを送信したりできます。
- \* My Cases \* : NetApp Support Siteの \* My Cases \* ページに移動します。
- \* クラスタの詳細を表示 \* : 新しいケースを送信するときに必要な情報を表示してコピーします。

#### テレメトリログを有効にします

ONTAP 9.10.1以降では、System Managerを使用してテレメトリロギングを有効にできます。テレメトリログが許可されている場合、System Managerによってログに記録されるメッセージには、メッセージをトリガーした正確なプロセスを示す特定のテレメトリ識別子が与えられます。そのプロセスに関連して発行されるメッセージはすべて同じ識別子を持ち、運用ワークフローの名前と番号（例：「add-volume - 1941290」）で構成されます。

パフォーマンスの問題が発生した場合はテレメトリログを有効にすると、サポート担当者はメッセージが発行されたプロセスをより簡単に識別できます。メッセージにテレメトリIDが追加されると、ログファイルはわずかに拡大されます。

#### 手順

1. System Managerで、 \* Cluster > Settings \*の順に選択します。
2. [\* UI設定\* (UI Settings) ]セクションで、[テレメータのログを許可する (Allow Telemetry logging \*) ]チェックボックスをオンにし

## System ManagerでStorage VMの最大容量制限を管理します

ONTAP 9.13.1以降では、System Managerを使用してStorage VMの最大容量制限を有効にし、使用済みストレージが最大容量の一定の割合に達したときにアラートをトリガーするしきい値を設定できます。

#### Storage VMの最大容量制限を有効にする

ONTAP 9.13.1以降では、Storage VM内のすべてのボリュームに割り当てることができる最大容量を指定できます。最大容量は、Storage VMを追加するとき、または既存のStorage VMを編集するときに有効にすることができます。

#### 手順

1. >[Storage VMs]\*を選択します。
2. 次のいずれかを実行します。

- Storage VMを追加するには、をクリックします **+ Add**。
- Storage VMを編集するには、をクリックします **:** をクリックし、\*[編集]\*をクリックします。

3. Storage VMの設定を入力または変更し、[最大容量制限を有効にする]チェックボックスを選択します。
4. 最大容量サイズを指定します。
5. アラートをトリガーするしきい値として使用する最大容量の割合を指定します。
6. [保存（Save）] をクリックします。

## Storage VMの最大容量制限を編集します

ONTAP 9.13.1以降では、既存のStorage VMの最大容量制限を編集できます（を参照） [最大容量制限が有効になりました](#) もういいよ

### 手順

1. >[Storage VMs]\*を選択します。
2. をクリックします **:** をクリックし、\*[編集]\*をクリックします。  
  
[最大容量制限を有効にする]チェックボックスはすでにオンになっています。
3. 次のいずれかの手順を実行します。

アクション	手順
最大容量制限を無効にする	<ol style="list-style-type: none"> <li>1. チェックボックスをオフにします。</li> <li>2. [保存（Save）] をクリックします。</li> </ol>
最大容量制限を変更します	<ol style="list-style-type: none"> <li>1. 新しい最大容量サイズを指定します。（Storage VMにすでに割り当てられているスペースよりも小さいサイズを指定することはできません）。</li> <li>2. アラートをトリガーするしきい値として使用する最大容量の新しいパーセンテージを指定します。</li> <li>3. [保存（Save）] をクリックします。</li> </ol>

### 関連情報

- ["Storage VMの最大容量制限を表示します"](#)
- ["System Manager で測定される容量"](#)
- ["ONTAP CLIを使用してSVMの容量制限を管理します"](#)

## System Manager で容量を監視

System Managerを使用して、使用済みのストレージ容量と、クラスタ、ローカル階層、またはStorage VMで使用可能な残りの容量を監視できます。

ONTAP の各バージョンでは、より堅牢な容量監視情報が提供されます。



- ONTAP 9.10.1以降のSystem Managerでは、クラスタの容量に関する履歴データと、使用済みまたは使用可能な容量に関する予測を表示できます。ローカル階層とローカルボリュームの容量も監視できます。
- ONTAP 9.12.1以降では、ローカル階層のコミット済み容量がSystem Managerに表示されます。
- ONTAP 9.13.1以降では、Storage VMの最大容量制限を有効にし、使用済みストレージが最大容量の一定の割合に達したときにアラートをトリガーするしきい値を設定できます。



使用済み容量の測定値は、ONTAP のバージョンによって表示されます。詳細は、[こちら](#)を参照してください "[System Manager で測定される容量](#)"。

クラスタの容量を表示します

クラスタの容量測定値は、System Managerのダッシュボードで確認できます。

作業を開始する前に

クラウド内の容量に関連するデータを表示するには、Active IQ デジタルアドバイザーのアカウントが必要です。このアカウントが接続されている必要があります。

手順

1. System Manager で、\* ダッシュボード \* をクリックします。
2. 容量 \* セクションでは、次の情報を確認できます。

- クラスタの合計使用容量
- クラスタの使用可能な合計容量
- 使用済み容量と使用可能容量の割合。
- データ削減率。
- クラウドで使用されている容量。
- 使用容量の履歴。
- 使用容量の予測



System Manager では、ルートストレージ階層（アグリゲート）の容量は表示されません。

3. グラフをクリックすると、クラスタの容量に関する詳細が表示されます。

容量の測定値は、次の2つの棒グラフで表示されます。

- 上部のグラフには、物理容量（使用済みの物理スペース、リザーブスペース、使用可能なスペース）が表示されます。
- 下部のグラフには、論理容量（クライアントデータ、Snapshotコピー、クローンのサイズ）、および使用済み論理スペースの合計が表示されます。

棒グラフの下には、データ削減の測定値が表示されます。

- クライアントデータのためのデータ削減率（Snapshotコピーとクローンは含まれません）。
- 全体的なデータ削減率。

詳細については、を参照してください "[System Manager で測定される容量](#)".

## ローカル階層の容量を表示します

ローカル階層の容量に関する詳細を確認できます。 ONTAP 9.12.1以降では、\*[容量]\*ビューにローカル階層のコミット済み容量も表示されるため、コミット済み容量に対応して空きスペースが不足しないようにローカル階層に容量を追加する必要があるかどうかを判断できます。

### 手順

1. [ストレージ]、[階層]の順にクリックします。
2. ローカル階層の名前を選択します。
3. [概要] ページの [容量] セクションでは、次の3つの測定値が棒グラフに表示されます。
  - 使用済み容量とリザーブ容量
  - 使用可能容量
  - コミット済み容量 (ONTAP 9.12.1以降)
4. グラフをクリックすると、ローカル階層の容量に関する詳細が表示されます。

容量の測定値は、次の2つの棒グラフで表示されます。

- 上部のバーグラフには、使用済み物理容量、リザーブ済み容量、および使用可能なスペースの物理容量が表示されます。
- 下部の棒グラフには、論理容量 (クライアントデータ、Snapshotコピー、クローンのサイズ)、および使用済み論理スペースの合計が表示されます。

棒グラフの下には、データ削減のための計測比率が表示されます。

- クライアントデータのためのデータ削減率 (Snapshotコピーとクローンは含まれません)。
- 全体的なデータ削減率。

詳細については、を参照してください "[System Manager で測定される容量](#)".

### オプションのアクション

- コミット済み容量がローカル階層の容量よりも大きい場合は、空きスペースが不足する前にローカル階層に容量を追加することを検討してください。 を参照してください "[ローカル階層への容量の追加 \(アグリゲートへのディスクの追加\)](#)".
- 特定のボリュームがローカル階層で使用しているストレージを確認するには、\*[ボリューム]\*タブを選択します。

## Storage VM内のボリュームの容量を表示します

Storage VMのボリュームで使用されているストレージの容量と、まだ使用可能な容量を確認できます。 使用済みストレージと使用可能なストレージの合計測定値を「ボリューム間の容量」と呼びます。

### 手順

1. >[Storage VMs]\*を選択します。
2. Storage VMの名前をクリックします。



3. [Capacity]\*セクションまでスクロールします。このセクションには、次の測定値を含む棒グラフが表示されます。

- 使用済み物理容量：このStorage VMのすべてのボリュームの使用済み物理ストレージの合計。
- 使用可能：このStorage VMのすべてのボリュームで使用可能な容量の合計。
- 使用済み論理容量：このStorage VMのすべてのボリュームの使用済み論理ストレージの合計。

測定値の詳細については、を参照してください ["System Manager で測定される容量"](#)。

### Storage VMの最大容量制限を表示します

ONTAP 9.13.1以降では、Storage VMの最大容量制限を表示できます。

作業を開始する前に

実行する必要があります ["Storage VMの最大容量制限を有効にする"](#) 表示する前に。

手順

1. >[Storage VMs]\*を選択します。

最大容量測定値は次の2つの方法で表示できます。

- Storage VMの行で、\*[最大容量]\*列を確認します。この列には、使用済み容量、使用可能容量、および最大容量を示す棒グラフが表示されます。
- Storage VMの名前をクリックします。[概要]\*タブをスクロールして、左側の列に最大容量、割り当て容量、および容量のアラートしきい値を確認します。

関連情報

- ["Storage VMの最大容量制限を編集します"](#)
- ["System Manager で測定される容量"](#)

### ハードウェア構成を表示して問題を特定します

ONTAP 9.8以降では、System Managerを使用してネットワークのハードウェア構成を表示し、ハードウェアシステムの健全性とケーブル構成を確認できます。

手順

ハードウェア構成を表示するには、次の手順を実行します。

1. System Manager で、 \* Cluster > Hardware \* を選択します。
2. コンポーネントの上にマウスポインタを合わせると、ステータスやその他の詳細が表示されます。

さまざまなタイプの情報を表示できます。

- [\[コントローラに関する情報\]](#)
- [\[ディスクシェルフに関する情報\]](#)
- [\[ストレージスイッチに関する情報\]](#)

3. ONTAP 9.12.1以降では、System Managerでケーブル接続情報を表示できます。ケーブルを表示するには、\*ケーブルを表示\*チェックボックスをクリックし、ケーブルの上にカーソルを置くと接続情報が表示されます。

- [\[ケーブル接続に関する情報\]](#)

コントローラに関する情報

次の情報が表示されます。

## ノード

- ノード \* :
- 正面図と背面図を表示できます。
- ディスクシェルフを内蔵したモデルの場合は、前面ビューでもディスクレイアウトを確認できます。
- 次のプラットフォームを表示できます。

プラットフォーム	ONTAPバージョンのSystem Managerでサポート						
	9.14.1	9.13.1.	9.12.1:	9.11.1	9.10.1	9.9.1	9.8 (プレビューモードのみ)
AFF A150	はい。	はい。					
AFF A220 の略	はい。	はい。	はい。	はい。	はい。	はい。	はい。
AFF A250	はい。	はい。	はい。	はい。	はい。	はい。	
AFF A300	はい。	はい。	はい。	はい。	はい。	はい。	はい。
AFF A320	はい。	はい。	はい。	はい。	はい。	はい。	
AFF A400	はい。	はい。	はい。	はい。	はい。	はい。	はい。
AFF A700 の略	はい。	はい。	はい。	はい。	はい。	はい。	はい。
AFF A700s	はい。	はい。	はい。	はい。	はい。	はい。	
AFF A800	はい。	はい。	はい。	はい。	はい。	はい。	
AFF C190 の略	はい。	はい。	はい。	はい。	はい。	はい。	はい。
AFF C250	はい。	はい。	はい*	はい*	はい*		
AFF C400	はい。	はい。	はい*	はい*	はい*		
AFF C800	はい。	はい。	はい*	はい*	はい*		
ASAA150	はい。	はい。					
ASAA250	はい。	はい。					

ASA A400	はい。	はい。					
ASA A800	はい。	はい。					
ASA A900	はい。	はい。					
ASA C250	はい。	はい。					
ASA C400	はい。	はい。					
ASA C800	はい。	はい。					
FAS500f	はい。	はい。	はい。	はい。	はい。	はい。	
FAS2720	はい。	はい。	はい。	はい。			
FAS2750	はい。	はい。	はい。	はい。			
FAS8300	はい。	はい。	はい。	はい。			
FAS8700	はい。	はい。	はい。	はい。			
FAS9000	はい。	はい。	はい。	はい。			
FAS9500	はい。	はい。	はい。	はい。			

#### ポート

- ポート \* :
- ダウンしている場合は、ポートが赤で強調表示されます。
- ポートにカーソルを合わせると、ポートのステータスやその他の詳細が表示されます。
- コンソールポートは表示できません。

#### 注:

- ONTAP 9.10.1以前では、SASポートが無効になると赤で強調表示されます。
- ONTAP 9.11.1以降では、SASポートがエラー状態にある場合、または使用中のケーブル接続済みポートがオフラインになった場合にのみ、SASポートが赤で強調表示されます。ポートがオフラインで接続されていない場合は白で表示されます。

#### FRU

- FRU \* :

FRU に関する情報は、FRU の状態が最適でない場合にのみ表示されます。

- ・ ノードまたはシャーシ内の PSU に障害が発生しました。
- ・ ノードで高温が検出されました。
- ・ ノードまたはシャーシのファンに障害が発生しています。

#### アダプタカード

- ・ アダプターカード \* :
- ・ 外部カードが挿入されている場合は、部品番号フィールドが定義されているカードがスロットに表示されます。
- ・ ポートがカードに表示されます。
- ・ サポートされているカードの場合は、そのカードの画像を表示できます。カードがサポートされているパーツ番号のリストに含まれていない場合は、一般的な図が表示されます。

### ディスクシェルフに関する情報

次の情報が表示されます。

#### ディスクシェルフ

- ・ ディスクシェルフ \* :
- ・ 正面図と背面図を表示できます。
- ・ 次のディスクシェルフモデルが表示されます。

システムで実行しているバージョン	これで、System Manager を使用した表示
ONTAP 9.9.1以降	「サービス終了」または「販売終了」に指定されているすべてのシェルフ
ONTAP 9.8	DS4243、DS4486、DS212C、DS2246、DS224C、および NS224 に追加できます

#### シェルフポート

- ・ シェルフポート \* :
- ・ ポートのステータスを表示できます。
- ・ ポートが接続されている場合は、リモートポートの情報を表示できます。

#### シェルフFRU

- ・ シェルフ FRU \* :
- ・ PSU障害情報が表示されます。

### ストレージスイッチに関する情報

次の情報が表示されます。

## ストレージスイッチ

### ストレージ・スイッチ：

- ディスプレイには、シェルフをノードに接続するためにストレージスイッチとして機能するスイッチが表示されます。
- ONTAP 9.9.1以降では、ストレージスイッチとクラスタの両方として機能するスイッチに関する情報が表示されます。この情報はHAペアのノード間で共有することもできます。
- 次の情報が表示されます。
  - スイッチ名
  - IP アドレス
  - シリアル番号
  - SNMPバージョン
  - システムのバージョン
- 次のストレージスイッチモデルを表示できます。

システムで実行しているバージョン	これで、 System Manager を使用した表示
ONTAP 9.11.1以降	Cisco Nexus 3232C Cisco Nexus 9336C-FX2 Mellanox SN2100の略
ONTAP 9.9.1および9.10.1	Cisco Nexus 3232C Cisco Nexus 9336C-FX2
ONTAP 9.8	Cisco Nexus 3232C

### ストレージ・スイッチ・ポート

### ストレージ・スイッチ・ポート

- 次の情報が表示されます。
  - ID名
  - IDインデックス
  - 状態
  - リモート接続
  - その他の詳細情報

## ケーブル接続に関する情報

ONTAP 9.12.1以降では、次のケーブル接続情報を表示できます。

- ストレージブリッジを使用しない場合は、コントローラ、スイッチ、シェルフ間の配線
- \* Connectivity \*。ケーブルの両端にあるポートのIDとMACアドレスを示します

## System Managerを使用したノードの管理

System Managerを使用して、クラスタにノードを追加して名前を変更できます。また、ノードをリブート、テイクオーバー、ギブバックすることもできます。

クラスタにノードを追加

新しいノードを追加してクラスタのサイズと容量を拡張できます。

始める前に

新しいノードをクラスタにケーブル接続しておく必要があります。

このタスクについて

ONTAP 9.7またはONTAP 9.8以降では、System Managerを使用するための個別のプロセスがあります。

### ONTAP 9.8以降の手順

- System Managerを使用したクラスタへのノードの追加（ONTAP 9.8以降）\*

手順

1. [\*Cluster] > [Overview] を選択します。

新しいコントローラは、クラスタネットワークに接続されているがクラスタにはないノードとして表示されます。

2. 「\* 追加」を選択します。
  - ノードがクラスタに追加されます。
  - ストレージは暗黙的に割り当てられます。

### ONTAP 9.7手順

- System Managerを使用したクラスタへのノードの追加（ONTAP 9.7）\*

手順

1. \*（クラシックバージョンに戻る）\*を選択します。
2. [構成]>[クラスタの拡張]\*を選択します。


System Manager では、新しいノードが自動的に検出されます。

3. [新しいエクスペリエンスに切り替える]\*を選択します。
4. [クラスタ]>[概要]\*を選択して、新しいノードを表示します。

サービスプロセッサのシャットダウン、再起動、または編集

ノードをリブートまたはシャットダウンすると、ノードのHAパートナーによって自動的にテイクオーバーが実行されます。

手順

1. [\*Cluster] > [Overview] を選択します。
2. [ノード]\*で、。
3. ノードを選択し、[シャットダウン]、[リブート]、または\*[サービスプロセッサの編集]\*を選択します。


ノードがリブートされてギブバックを待機している場合は、\* giveback \*オプションも使用できます。

を選択した場合は、[手動]を選択してIPアドレス、サブネットマスク、およびゲートウェイを入力するか、DHCP \*を選択して動的ホスト設定を指定できます。

## ノードの名前変更

ONTAP 9.14.1以降では、クラスタの概要ページでノードの名前を変更できます。

### 手順

1. [クラスタ]\*を選択します。クラスタの概要ページが表示されます。
2. [ノード]\*セクションまで下にスクロールします。
3. 名前を変更するノードの横にある  をクリックし、\*[名前の変更]\*を選択します。
4. ノード名を変更し、\*[名前の変更]\*を選択します。

# ライセンス管理

## ONTAP ライセンスの概要

ライセンスには、ソフトウェアの使用権が 1 つ以上記録されています。ONTAP 9.10.1以降では、すべてのライセンスがNetAppライセンスファイル（NLF）として提供されます。これは、複数の機能を有効にする単一のファイルです。2023年5月以降、すべてのAFFシステム（AシリーズとCシリーズの両方）とFASシステムは、ONTAP ONEソフトウェアスイートまたはONTAP Baseソフトウェアスイートのいずれかとともに販売され、2023年6月以降は、すべてのASAシステムがONTAP ONE for SANとともに販売されます。各ソフトウェアスイートは単一のNLFとして提供され、ONTAP 9.10.1で最初に導入された個別のNLFバンドルを置き換えます。

### ONTAP Oneに含まれるライセンス

ONTAP Oneには、使用可能なライセンス機能がすべて含まれています以前のCore Bundle、Data Protection Bundle、Security and Compliance Bundle、Hybrid Cloud Bundle、Encryption Bundleの内容が次の表にまとめられています。暗号化は制限された国では使用できません。

以前のバンドル名	含まれるONTAPキー
----------	-------------



Core Bundle	FlexClone
	SnapRestore
	NFS、SMB、S3
	FC、iSCSI
	NVMe-oF
Security and Compliance Bundle	自律的なランサムウェア防御
	MTKM
	SnapLock
Data Protection Bundle	SnapMirror（非同期、同期、ビジネス継続性）
	SnapCenter
	NetAppターゲット用のS3 SnapMirror
Hybrid Cloud Bundle	SnapMirror クラウド
	ネットアップ以外のターゲット用のS3 SnapMirror
暗号化バンドル	NetApp Volume Encryption の略
	Trusted Platformモジュール

## ONTAP Oneに含まれていないライセンス

ONTAP Oneには、以下を含むネットアップのクラウド提供サービスは含まれていません。

- BlueXPの階層化
- Cloud Insights の機能です
- BlueXPバックアップ
- データガバナンス

## 既存システム用のONTAP One

現在NetAppのサポートを受けているが、ONTAP Oneにアップグレードされていない既存のシステムがある場合、これらのシステムの既存のライセンスは引き続き有効であり、期待どおりに機能します。たとえば、既存のシステムにSnapMirrorライセンスがすでにインストールされている場合、ONTAP ONEにアップグレードして新しいSnapMirrorライセンスを取得する必要はありません。ただし、既存のシステムにSnapMirrorライセンスがインストールされていない場合は、追加料金でONTAP ONEにアップグレードするしかありません。

2023年6月以降、28文字のライセンスキーを使用するONTAPシステムでも、["ONTAP OneまたはONTAP Base互換性バンドルへのアップグレード"](#)。

## ONTAP Baseに含まれるライセンス

ONTAP Baseは、ONTAPシステム用のONTAP Oneに代わるオプションのソフトウェアスイートです。専用のテスト環境や開発環境に対応した非本番システムなど、SnapMirrorやSnapCenterなどのデータ保護テクノロジーや、Autonomous Ransomwareなどのセキュリティ機能が不要な特定のユースケースを対象としています。ONTAP Baseにライセンスを追加することはできません。SnapMirrorなどの追加ライセンスが必要な場合は、ONTAP ONEにアップグレードする必要があります。

以前のバンドル名	含まれるONTAPキー
Core Bundle	FlexClone
	SnapRestore
	NFS、SMB、S3
	FC、iSCSI
	NVMe-oF
暗号化バンドル	NetApp Volume Encryption の略
	Trusted Platformモジュール

## ONTAP One for SANに含まれるライセンス

ONTAP One for SANは、ASAAシリーズおよびCシリーズのシステムで使用できます。SANで使用できる唯一のソフトウェアスイートです。ONTAP One for SANには、次のライセンスが含まれています。

含まれるONTAPキー
FlexClone
SnapRestore
FC、iSCSI
NVMe-oF
MTKM
SnapLock
SnapMirror（非同期、同期、ビジネス継続性）
SnapCenter
SnapMirror クラウド
NetApp Volume Encryption の略
Trusted Platformモジュール

## その他のライセンス提供方法

ONTAP 9.9.1では、ライセンスキーは28文字の文字列として提供され、ONTAP 機能ごとに1つのキーがあります。ONTAP 9.9.1を使用している場合は、ONTAP CLIを使用してライセンスキーをインストールします。



ONTAP 9.10.1では、System ManagerまたはCLIを使用した28文字のライセンスキーのインストールがサポートされています。ただし、機能用にNLFライセンスがインストールされている場合、同じ機能用のNetAppライセンスファイルに28文字のライセンスキーをインストールすることはできません。System Managerを使用したNLFまたはライセンスキーのインストールについては、[を参照してください。"ONTAPライセンスのインストール"](#)。

## 関連情報

["システムにすでにNLFがある場合にONTAP Oneライセンスを取得する方法"](#)

"サポートサイトを使用してONTAPソフトウェアの使用権と関連ライセンスキーを確認する方法"

"NetApp：ONTAP使用権リスクステータス"

## NetApp Support SiteからのNetAppライセンスファイル（NLF）のダウンロード

ONTAP 9.10.1以降を実行しているシステムでは、NetApp Support SiteからONTAP One またはONTAP Core用のNLFをダウンロードすることで、既存のシステムのバンドルライセンスファイルをアップグレードできます。



SnapMirror CloudライセンスとS3 SnapMirrorライセンスは、ONTAP ONEには含まれていません。これらはONTAP One Compatibilityバンドルに含まれています。ONTAP Oneをお持ちの場合は無料で入手できます。 ["個別にリクエスト"](#)。

### 手順

ONTAP ONEライセンスファイルは、既存のNetAppライセンスファイルバンドルを含むシステム、および28文字のライセンスキーをNetAppライセンスファイルに変換したシステム（ONTAP 9.10.1以降を実行するシステム）用にダウンロードできます。また、ONTAPベースからONTAP Oneにシステムをアップグレードすることもできます。

#### 既存のNLFをアップグレード

1. アップグレードまたは変換するライセンスファイルバンドル（ONTAP BaseからONTAP One、Core Bundleおよびデータ保護バンドルからONTAP Oneなど）は、NetApp営業チームにお問い合わせください。

リクエストが処理されると、「SO#[SO番号]に対するNetAppソフトウェアライセンス通知」という件名のEメールがnetappsw@netapp.comから送信されます。メールには、ライセンスのシリアル番号が記載されたPDFの添付ファイルが添付されています。

2. にログインします ["NetApp Support Site"](#)。
3. [システム]>[ソフトウェアライセンス]\*を選択します。
4. メニューから\*シリアル番号\*を選択し、受け取ったシリアル番号を入力して\*新規検索\*をクリックします。
5. 変換するライセンスバンドルを探します。
6. 各ライセンスバンドルの[Get NetApp License File]\*をクリックし、NLFが利用可能になったらダウンロードします。
7. ["をインストールします"](#) ONTAP Oneファイル。

#### ライセンスキーから変換されたNLFのアップグレード

1. にログインします ["NetApp Support Site"](#)。
2. [システム]>[ソフトウェアライセンス]\*を選択します。
3. メニューから\*シリアル番号\*を選択し、システムのシリアル番号を入力して\*新規検索\*をクリックします。
4. 変換するライセンスを探し、\* Eligibility 列で Check \*をクリックします。
5. [Check Eligibility]フォーム\*で、\*[Generate Licenses for 9.10.x and later]\*をクリックします。
6. [Check Eligibility]フォーム\*を閉じます。

ライセンスが生成されるまで少なくとも2時間待つ必要があります。

7. 手順1〜3を繰り返します。
8. ONTAP Oneライセンスを探し、\*[Get NetApp License File]\*をクリックして配信方法を選択します。
9. ["をインストールします"](#) ONTAP Oneファイル。

## ONTAPライセンスのインストール

NetAppライセンスファイル（NLF）とライセンスキーは、NLFのインストールに推奨されるSystem Managerを使用してインストールできます。また、ONTAP CLIを使用してライセンスキーをインストールすることもできます。ONTAP 9.10.1以降では機能はNetAppライセンスファイルで有効になり、ONTAP 9.10.1より前のリリースではONTAP機能はライセンスキーで有効になります。

#### 手順

あなたがすでに持っているなら ["ダウンロードしたNetAppライセンスファイル"](#) またはライセンスキーの場合、System ManagerまたはONTAP CLIを使用して、NLFと28文字のライセンスキーをインストールできます。

#### System Manager - ONTAP 9.8以降

1. [\* Cluster]>[Settings] (設定) \*を選択します。
2. [ライセンス]\*で、 [→](#)。
3. [\* 参照 \*] を選択します。ダウンロードしたNetAppライセンスファイルを選択します。
4. 追加するライセンスキーがある場合は、「\* 28 文字のライセンスキーを使用する \*」を選択して、キーを入力します。

#### System Manager - ONTAP 9.7以前

1. [設定]>[クラスタ]>[ライセンス]\*を選択します。
2. [ライセンス]\*で、 [→](#)。
3. [\* パッケージ \*] ウィンドウで、[\* 追加] をクリックします。
4. [\* ライセンスパッケージの追加 \*] ダイアログボックスで、[\* ファイルの選択 \*] をクリックしてダウンロードしたネットアップライセンスファイルを選択し、[\* 追加] をクリックしてファイルをクラスタにアップロードします。

#### CLI の使用

1. 1つ以上のライセンスキーを追加します。

```
system license add
```

次の例では、ローカルノード「/mroot/etc/lic\_file」からライセンスをインストールします（ファイルがこの場所にある場合）。

```
cluster1::> system license add -use-license-file true
```

次に、AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAおよびBBというキーを持つライセンスのリストをクラスタに追加する例を示します。

```
cluster1::> system license add -license-code  
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAA, BBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBB
```

#### 関連情報

["system license add コマンドのマニュアルページ"](#)。

## ONTAP ライセンスを管理します。



System Manager または ONTAP CLI を使用して、ライセンスシリアル番号の表示、ライセンスのステータスの確認、ライセンスの削除など、システムにインストールされているライセンスを表示および管理できます。

ライセンスの詳細を表示する

### 手順

ライセンスに関する詳細の表示方法は、使用している ONTAP のバージョン、および System Manager と ONTAP CLI のどちらを使用しているかによって異なります。

#### System Manager - ONTAP 9.8以降

1. 特定の機能ライセンスに関する詳細を表示するには、\*[クラスタ]>[設定]\*を選択します。
2. [ライセンス]\*で、 。
3. [機能]\*を選択します。
4. 表示するライセンス機能を探して選択します。  をクリックしてライセンスの詳細を表示します。

#### System Manager - ONTAP 9.7以前

1. [設定]>[クラスタ]>[ライセンス]\*を選択します。
2. [Licenses] ウィンドウで、適切なアクションを実行します。
3. [\* 詳細 \*] タブをクリックします。


#### CLI の使用

1. インストールされているライセンスに関する詳細を表示します。

```
system license show
```

ライセンスを削除する

### System Manager - ONTAP 9.8以降

1. ライセンスを削除するには、\*[クラスタ]>[設定]\*を選択します。
2. [ライセンス]\*で、 .
3. [機能]\*を選択します。
4. 削除するライセンス機能を選択し、\*レガシーキーを削除\*を選択します。

### System Manager - ONTAP 9.7以前

1. [設定]>[クラスタ]>[ライセンス]\*を選択します。
2. [Licenses] ウィンドウで、適切なアクションを実行します。

状況	手順
ノードの特定のライセンスパッケージまたはマスターライセンスを削除する	[ * 詳細 * ] タブをクリックします。
クラスタ内のすべてのノードから特定のライセンスパッケージを削除する	[ * パッケージ * ] タブをクリックします。

3. 削除するソフトウェアライセンスパッケージを選択し、\*削除\*をクリックします。

一度に削除できるライセンスパッケージは1つだけです。

4. 確認のチェックボックスをオンにし、\*削除\*をクリックします。

### CLI の使用

1. ライセンスを削除します。

```
system license delete
```

次の例は、CIFSという名前のライセンスとシリアル番号1-81-0000000000000000123456をクラスタから削除します。

```
cluster1::> system license delete -serial-number 1-81-0000000000000000123456 -package CIFS
```

次の例は、シリアル番号123456789のInstalled license Core Bundleの下すべてのライセンスをクラスタから削除します。

```
cluster1::> system license delete { -serial-number 123456789 -installed-license "Core Bundle" }
```

## ライセンスタイプとライセンス方式

ライセンスタイプとライセンス方式について理解しておく、クラスタのライセンスを管理する際に役に立ちます。

### ライセンスタイプ

パッケージには、クラスタにインストールされる次のライセンスタイプが1つ以上含まれます。。 `system license show` コマンドは、パッケージにインストールされているライセンスタイプを表示します。

- Standardライセンス (license)

標準ライセンスはノードロックライセンスです。特定のシステムシリアル番号（別名「*controller serial number*」）を持つノードに対して発行されます。標準ライセンスは、シリアル番号が一致するノードに対してのみ有効です。

標準のノードロックライセンスをインストールすると、ノードでライセンスされた機能を使用できるようになります。ライセンスされた機能をクラスタで使用するには、少なくとも1つのノードで、その機能のライセンスが有効になっている必要があります。ライセンスされた機能の使用権がないノードでその機能を使用すると、ライセンス違反になる可能性があります。

- サイトライセンス (site)

サイトライセンスは、特定のシステムシリアル番号に関連付けられません。サイトライセンスをインストールすると、クラスタ内のすべてのノードで、ライセンスされた機能を使用できるようになります。。

`system license show` コマンドを実行すると、指定したクラスタシリアル番号のサイトライセンスが表示されます。

サイトライセンスがあるクラスタからノードを削除した場合、そのノードはサイトライセンスを保持できず、ライセンスされた機能を使用できなくなります。サイトライセンスのあるクラスタにノードを追加した場合、そのノードには自動的にサイトライセンスが付与され、ライセンスされた機能を使用できるようになります。

- 評価用ライセンス (demo)

評価用ライセンスは、一定期間（で示される）が経過すると失効する一時的なライセンスです `system license show` コマンド）。このライセンスを使用すると、ライセンスを購入せずに特定のソフトウェア機能を試すことができます。このライセンスはクラスタ全体のライセンスであり、ノードの特定のシリアル番号には関連付けられません。

パッケージの評価用ライセンスがあるクラスタからノードを削除した場合、そのノードは評価用ライセンスを保持できません。

### ライセンス方式

クラスタ全体のライセンスの両方をインストールできます（`site` または `demo` タイプ）とノードロックライ



センス（`license` タイプ）を入力します。したがって、インストールされたパッケージには、クラスタ内に複数のライセンスタイプが存在する場合があります。ただし、パッケージのライセンス方式はクラスタに対して 1 つだけです。。`licensed method` のフィールド `system license status show` コマンドは、パッケージに使用されているエンタイトルメントを表示します。このコマンドによって、ライセンス方式が次のように決定します。

- クラスタにインストールされるライセンスタイプがパッケージに 1 つしか含まれていない場合、そのインストールされるライセンスタイプがライセンス方式となります。
- クラスタにインストールされているライセンスがパッケージにない場合、ライセンス方式は `none`。
- クラスタに複数のライセンスタイプがインストールされているパッケージの場合、ライセンス方式は次のライセンスタイプの優先順位で決定されます。`-site`、`license`` および ``demo`。

例：

- パッケージにサイトライセンス、標準ライセンス、および評価用ライセンスがある場合、クラスタでのパッケージのライセンス方式は `site`。
- パッケージに標準ライセンスと評価用ライセンスがある場合、クラスタでのパッケージのライセンス方式は `license`。
- パッケージに評価用ライセンスしかない場合、クラスタでのパッケージのライセンス方式は `demo`。

## ライセンスを管理するためのコマンド

ONTAP CLIを使用できます。 `system license` クラスタの機能ライセンスを管理するコマンド。を使用します `system feature-usage` 機能の使用状況を監視するコマンド。

次の表に、ライセンスを管理するための一般的なCLIコマンドの一部と、追加情報のコマンドマニュアルページへのリンクを示します。

状況	使用するコマンド
ライセンスが必要なパッケージすべてと、次のようなパッケージの現在のライセンスステータスを表示する <ul style="list-style-type: none"><li>• パッケージ名</li><li>• ライセンス方式</li><li>• 有効期限（該当する場合）</li></ul>	<a href="#">"system license show-statusを使用してください"</a>
期限切れのライセンスまたは未使用のライセンスを表示または削除します	<a href="#">"システムライセンスのクリーンアップ"</a>
クラスタでの機能の使用状況の概要をノード単位で表示します	<a href="#">"system feature-usage show-summary"</a>

状況	使用するコマンド
クラスタでの機能の使用ステータスをノード単位および週単位で表示します	<a href="#">"system feature-usage show-historyを使用します"</a>
各ライセンスパッケージのライセンス使用権リスクステータスを表示します	<a href="#">"system license entitlement-risk showのように表示されます"</a>

#### 関連情報

["ONTAP 9コマンド"](#)

["技術情報アーティクル：ONTAP 9.10.1以降のライセンスの概要"](#)

["System Managerを使用してNetAppライセンスファイルをインストールする"](#)

## CLI を使用したクラスタ管理

### CLI での管理の概要

ONTAP システムは、コマンドラインインターフェイス（CLI）を使用して管理できます。ONTAP の管理インターフェイスを使用して、クラスタにアクセスし、ノードを管理できます。

これらの手順は、次のような状況で使用する必要があります。

- ONTAP 管理者の権限の範囲について理解する必要がある。
- System Manager や自動スクリプトツールではなく、CLI を使用する。

#### 関連情報

CLI の構文と使用方法の詳細については、を参照してください

["ONTAP 9 マニュアルページリファレンス"](#) ドキュメント

### クラスタ管理者と SVM 管理者

#### クラスタ管理者と SVM 管理者

クラスタ管理者は、クラスタ全体と、そのクラスタに含まれる Storage Virtual Machine（SVM、旧 Vserver）を管理します。SVM 管理者は、自身が担当するデータ SVM だけを管理します。

クラスタ管理者は、クラスタ全体とそのリソースを管理できます。また、データ SVM をセットアップし、SVM の管理を SVM 管理者に委譲することもできます。クラスタ管理者固有の権限は、それぞれのアクセス制御ロールによって異なります。デフォルトでは、「admin」というアカウント名またはロール名を持つクラスタ管理者は、クラスタと SVM を管理するためのあらゆる権限を持っています。

SVM 管理者は、ボリューム、プロトコル、LIF、サービスなど、自身が担当する SVM のストレージおよびネットワークリソースだけを管理できます。SVM 管理者固有の権限は、クラスタ管理者によって割り当てられた、それぞれのアクセス制御ロールによって異なります。



ONTAP のコマンドラインインターフェイス (CLI) では、の出力に引き続き `_SVM_` と表示されます `vserver` コマンドまたはパラメータの名前は変更されていません。

## System Manager へのアクセスを管理します

Web ブラウザから System Manager へのアクセスを有効または無効にすることができます。System Manager のログを表示することもできます。

を使用して、Web ブラウザから System Manager へのアクセスを制御できます `vserver services web modify -name sysmgr -vserver cluster_name -enabled[true|false]`。

System Manager のログインはに記録されます `/mroot/etc/log/mlog/sysmgr.log` System Manager がアクセスされたときにクラスタ管理 LIF をホストしていたノードのファイル。ログファイルは、ブラウザを使用して表示できます。System Manager のログは、AutoSupport メッセージにも含まれています。

## クラスタ管理サーバとは

クラスタ管理サーバは `admin_ SVM` と呼ばれる、クラスタを 1 つの管理可能なエンティティとして扱う特別な Storage Virtual Machine (SVM) です。クラスタ管理サーバは最上位の管理ドメインとして機能するとともに、データ SVM に論理的に属さないリソースを所有します。

クラスタ管理サーバは、クラスタ上で常に使用できます。クラスタ管理サーバには、コンソールまたはクラスタ管理 LIF からアクセスできます。

ホームネットワークポートに障害が発生すると、クラスタ管理 LIF がクラスタ内の別のノードに自動的にフェイルオーバーします。使用している管理プロトコルの接続特性に応じて、ユーザがフェイルオーバーを認識できる場合とできない場合があります。コネクションレス型プロトコル (SNMP など) を使用している場合、または接続が限定されている場合 (HTTP など) には、フェイルオーバーを認識する可能性は低くなります。ただし、長期的な接続 (SSH など) を使用している場合は、フェイルオーバー後にクラスタ管理サーバに再接続する必要があります。

クラスタを作成した場合は、IP アドレス、ネットマスク、ゲートウェイ、ポートなど、クラスタ管理 LIF のすべての特性を設定します。

データ SVM やノード SVM とは異なり、クラスタ管理サーバにはルートボリュームまたはホストユーザボリュームがありません (システムボリュームをホストすることは可能)。さらに、クラスタ管理サーバで使用できるのはクラスタ管理タイプの LIF だけです。

を実行する場合は、を実行します `vserver show` コマンドを実行すると、そのコマンドの出力リストにクラスタ管理サーバが表示されます。

## SVMs のタイプ

クラスタは、クラスタとそのリソースの管理、およびクライアントとアプリケーションへのデータアクセスを支援する 4 種類の SVM で構成されます。

クラスタには、次の種類の SVM が含まれます。

- 管理 SVM

クラスタのセットアッププロセスでは、クラスタ用の管理 SVM が自動的に作成されます。管理 SVM はクラスタを表します。

- ノード SVM

ノード SVM は、ノードがクラスタに追加されると作成され、ノード SVM はクラスタの個別のノードを表します。

- システム SVM（アドバンスド）

システム SVM は、クラスタレベルの通信用に IPspace 内に自動的に作成されます。

- データ SVM

データ SVM は SVM を提供するデータを表します。クラスタのセットアップ後、クラスタ管理者はデータ SVM を作成し、作成した SVM にボリュームを追加して、クラスタからのデータアクセスを可能にする必要があります。

クラスタがクライアントにデータを提供するためには、少なくとも 1 つのデータ SVM が必要です。



特に指定がないかぎり、SVM という用語はデータ（データ提供用）SVM を指します。

CLI では、SVM は Vserver と表示されます。

## CLI を使用してクラスタにアクセスする（クラスタ管理者のみ）

シリアルポートを使用してクラスタにアクセスする

クラスタには、ノードのシリアルポートに接続されているコンソールから直接アクセスできます。

手順

1. コンソールで Enter キーを押します。

ログインプロンプトが表示されます。

2. ログインプロンプトで、次のいずれかを実行します。

クラスタにアクセスするアカウント	入力するアカウント名
デフォルトのクラスタアカウント	<b>admin</b>
別の管理ユーザアカウント	<i>username</i>

パスワードプロンプトが表示されます。

3. admin または管理ユーザアカウントのパスワードを入力し、Enter キーを押します。

## SSHを使用したクラスタへのアクセス

管理タスクを実行するために、クラスタへの問題 SSH 要求を行うことができます。SSHはデフォルトで有効になっています。

### 必要なもの

- を使用するように設定されたユーザアカウントが必要です ssh アクセス方法として。
  - `-application` のパラメータ `security login` コマンドは、ユーザアカウントのアクセス方法を指定します。◦ `security login` ["マニュアルページ"](#) 追加情報 を含む。
- Active Directory (AD) のドメインユーザアカウントを使用してクラスタにアクセスする場合は、CIFS対応のStorage VMでクラスタの認証トンネルが設定されている必要があり、さらにADのドメインユーザアカウントが ssh アクセス方法としておよび domain を認証方法として指定します。
- IPv6 接続を使用する場合は、クラスタで IPv6 が設定されて有効になっている必要があります。また、ファイアウォールポリシーに IPv6 アドレスが設定されている必要があります。
  - `network options ipv6 show` IPv6が有効になっているかどうかを表示します。◦ `system services firewall policy show` コマンドは、ファイアウォールポリシーを表示します。

### このタスクについて

- OpenSSH 5.7 以降のクライアントを使用する必要があります。
- サポートされているプロトコルは SSH v2 だけです。SSH v1 はサポートされていません。
- ONTAPでは、1つのノードで同時に最大64のSSHセッションがサポートされています。

クラスタ管理 LIF がノード上に存在する場合、クラスタ管理 LIF はこの制限をノード管理 LIF と共有します。

着信接続の速度が 1 秒あたり 10 を超えると、サービスは一時的に 60 秒間無効になります。

- ONTAP は、SSH に対して AES および 3DES 暗号化アルゴリズム（*cipher* と呼ばれる）のみをサポートしています。

AES では、128 ビット、192 ビット、256 ビットのキー長がサポートされます。3DES のキーの長さは DES 同様に 56 ビットですが、3 回繰り返されます。

- FIPS モードが有効な場合、SSH クライアントを接続するには、Elliptic Curve Digital Signature Algorithm（ECDSA）公開鍵アルゴリズムとネゴシエートする必要があります。
- ONTAP CLI に Windows ホストからアクセスする場合は、PuTTY などのサードパーティのユーティリティを使用できます。
- Windows AD ユーザ名を使用して ONTAP にログインする場合、ONTAP で AD ユーザ名とドメイン名が作成されたときと同じように大文字と小文字を区別する必要があります。

AD のユーザ名とドメイン名では、大文字と小文字は区別されませんが、ただし、ONTAP のユーザ名では大文字と小文字が区別されます。ONTAP で作成されたユーザ名と、AD で作成されたユーザ名の大文字小文字表記が違くと、ログインに失敗します。

## SSH認証オプション

- ONTAP 9.3以降では、を実行できます ["SSH多要素認証を有効にします"](#) ローカル管理者アカウントの場合。

SSH 多要素認証が有効な場合は、公開鍵とパスワードを使用してユーザが認証されます。

- ONTAP 9.4以降では、次のことが可能です ["SSH多要素認証を有効にします"](#) LDAPおよびNISのリモートユーザ。
- ONTAP 9.13.1以降では、必要に応じてSSH認証プロセスに証明書の検証を追加して、ログインのセキュリティを強化できます。これを行うには、["X.509証明書を公開鍵に関連付けます"](#) アカウントが使用します。SSH公開鍵とX.509証明書の両方を使用してSSHを使用してログインすると、ONTAPは、SSH公開鍵で認証する前にX.509証明書の有効性をチェックします。証明書の有効期限が切れているか失効している場合、SSHログインは拒否され、SSH公開鍵は自動的に無効になります。
- ONTAP 9.14.1以降では、オプションでCisco Duo 2要素認証をSSH認証プロセスに追加して、ログインセキュリティを強化できます。Cisco Duo認証を有効にした後の最初のログイン時に、ユーザはSSHセッションのオーセンティケータとして機能するデバイスを登録する必要があります。を参照してください ["SSHログイン用のCisco Duo 2FAの設定"](#) ONTAPのCisco Duo SSH認証の設定の詳細については、を参照してください。

## 手順

1. 管理ホストで、を入力します `ssh` 次のいずれかの形式でコマンドを実行します。

- `ssh username@hostname_or_IP [command]`
- `ssh -l username hostname_or_IP [command]`

ADドメインユーザアカウントを使用している場合は、を指定する必要があります `username` 形式はです `domainname\AD_accountname` (ドメイン名のあとにバックスラッシュが2つ付いている場合) または `"domainname\AD_accountname"` (二重引用符で囲み、ドメイン名のあとにバックスラッシュ1つで囲みます)。

`hostname_or_IP` は、クラスタ管理LIFまたはノード管理LIFのホスト名またはIPアドレスです。クラスタ管理 LIF を使用することを推奨します。IPv4 または IPv6 アドレスを使用できます。

`command` SSHインタラクティブセッションでは必要ありません。

## SSH要求の例

次の例は、「joe」という名前のユーザアカウントで、クラスタ管理 LIF が 10.72.137.28 のクラスタにアクセスする SSH 要求を問題で実行する方法を示しています。

```
$ ssh joe@10.72.137.28
Password:
cluster1::> cluster show
Node           Health  Eligibility
-----
node1           true    true
node2           true    true
2 entries were displayed.
```

```
$ ssh -l joe 10.72.137.28 cluster show
Password:
Node                Health  Eligibility
-----
node1                true   true
node2                true   true
2 entries were displayed.
```

次の例は、「DOMAIN1」という名前のドメインの「John」という名前のユーザアカウントが、クラスタ管理 LIF が 10.72.137.28 であるクラスタにアクセスするための SSH 要求を問題でできることを示しています。

```
$ ssh DOMAIN1\\john@10.72.137.28
Password:
cluster1::> cluster show
Node                Health  Eligibility
-----
node1                true   true
node2                true   true
2 entries were displayed.
```

```
$ ssh -l "DOMAIN1\john" 10.72.137.28 cluster show
Password:
Node                Health  Eligibility
-----
node1                true   true
node2                true   true
2 entries were displayed.
```

次の例は、「joe」という名前のユーザアカウントで SSH MFA 要求を問題で実行し、クラスタ管理 LIF が 10.72.137.32 のクラスタにアクセスする方法を示しています。

```
$ ssh joe@10.72.137.32
Authenticated with partial success.
Password:
cluster1::> cluster show
Node                Health  Eligibility
-----
node1                true   true
node2                true   true
2 entries were displayed.
```



## SSH ログインのセキュリティ

ONTAP 9.5 以降では、過去のログイン、失敗したログイン、および前回のログイン後に適用された権限の変更内容に関する情報を表示できます。

セキュリティ関連の情報は、SSH admin ユーザとしてログインしたときに表示されます。次の条件に関するアラートが表示されます。

- 最後にアカウント名がログインされた時刻。
- 前回のログイン成功後にログインに失敗した回数。
- 前回のログイン後にロールに変更があったかどうか（管理者アカウントのロールが「admin」から「backup」に変更された場合など）。
- 前回のログイン後にロールの追加、変更、または削除機能を変更したかどうか。



疑わしい情報が表示された場合は、ただちにセキュリティ部門に連絡してください。

ログイン時にこの情報を取得するには、次の前提条件を満たしている必要があります。

- SSH ユーザアカウントが ONTAP でプロビジョニングされている必要があります。
- SSH セキュリティログインが作成されている必要があります。
- ログインに成功する必要があります。

## SSH ログインのセキュリティに関する制限事項とその他の考慮事項

SSH ログインのセキュリティ情報には、次の制限事項および考慮事項が適用されます。

- この情報は、SSH ベースのログインについてのみ表示されます。
- LDAP / NIS や AD アカウントなどのグループベースの管理者アカウントの場合、ユーザは、メンバーであるグループが ONTAP で管理者アカウントとしてプロビジョニングされている場合、SSH ログイン情報を表示できます。

ただし、これらのユーザについては、ユーザアカウントのロールへの変更に関するアラートを表示することはできません。また、ONTAP で管理者アカウントとしてプロビジョニングされた AD グループに属するユーザは、前回のログイン後にログインに失敗した回数は表示できません。

- ユーザについての情報は、ONTAP からユーザアカウントが削除されると削除されます。
- SSH 以外のアプリケーションへの接続に関する情報は表示されません。

## SSH ログインのセキュリティ情報の例

次の例は、ログイン後に表示される情報の種類を示しています。

- このメッセージは、ログインに成功するたびに表示されます。



```
Last Login : 7/19/2018 06:11:32
```

- 前回のログインに失敗したログインがあった場合、次のメッセージが表示されます。

```
Last Login : 4/12/2018 08:21:26  
Unsuccessful login attempts since last login - 5
```

- 前回のログイン後に失敗したログインがあり、権限が変更されている場合、次のメッセージが表示されます。

```
Last Login : 8/22/2018 20:08:21  
Unsuccessful login attempts since last login - 3  
Your privileges have changed since last login
```

クラスタへの **Telnet** アクセスまたは **RSH** アクセスを有効にします

セキュリティのベストプラクティスとして、事前定義された管理ファイアウォールポリシーではTelnetとRSHは無効にしています (mgmt)。クラスタが Telnet 要求または RSH 要求を受け入れることができるようにするには、Telnet または RSH を有効にした新しい管理ファイアウォールポリシーを作成し、その新しいポリシーをクラスタ管理 LIF に関連付ける必要があります。

このタスクについて

ONTAP では、事前定義されているファイアウォールポリシーは変更できませんが、事前定義されているファイアウォールポリシーをクローニングして新しいポリシーを作成することもできます mgmt ファイアウォールポリシーを管理し、新しいポリシーでTelnetまたはRSHを有効にします。ただし、Telnet および RSH はセキュアなプロトコルではないため、SSH を使用してクラスタにアクセスすることを検討してください。SSH は、セキュアなリモートシェルと対話型のネットワークセッションを提供します。

クラスタへの Telnet アクセスまたは RSH アクセスを有効にするには、次の手順を実行します。

手順

1. advanced 権限モードに切り替えます。  
**set advanced**
2. セキュリティプロトコル (RSH または Telnet) を有効にします。  
**security protocol modify -application security\_protocol -enabled true**
3. に基づいて新しい管理ファイアウォールポリシーを作成します mgmt 管理ファイアウォールポリシー：  
**system services firewall policy clone -policy mgmt -destination-policy policy-name**
4. 新しい管理ファイアウォールポリシーで Telnet または RSH を有効にします。  
**system services firewall policy create -policy policy-name -service security\_protocol -action allow -ip-list ip\_address/netmask**  
すべてのIPアドレスを許可するには、と指定する必要があります -ip-list 0.0.0.0/0

5. 新しいポリシーをクラスタ管理 LIF に関連付けます。

```
network interface modify -vserver cluster_management_LIF -lif cluster_mgmt
-firewall-policy policy-name
```

Telnet を使用してクラスタにアクセスします

管理タスクを実行するために、クラスタへの問題 Telnet 要求を行うことができます。Telnet はデフォルトでは無効になっています。

必要なもの

Telnet を使用してクラスタにアクセスするには、次の条件を満たしている必要があります。

- アクセス方法として Telnet を使用するように設定されたクラスタローカルユーザアカウントを持っている必要があります。

。 -application のパラメータ security login コマンドは、ユーザアカウントのアクセス方法を指定します。詳細については、を参照してください security login マニュアルページ

- Telnet 要求がファイアウォールを通過できるように、クラスタ管理 LIF またはノード管理 LIF によって使用される管理ファイアウォールポリシーで Telnet が有効になっている必要があります。

デフォルトでは、Telnet は無効になっています。。 system services firewall policy show コマンドにを指定します -service telnet パラメータは、ファイアウォールポリシーでTelnetが有効になっているかどうかを表示します。詳細については、を参照してください system services firewall policy マニュアルページ

- IPv6 接続を使用する場合は、クラスタで IPv6 が設定されて有効になっている必要があります。また、ファイアウォールポリシーに IPv6 アドレスが設定されている必要があります。

。 network options ipv6 show IPv6が有効になっているかどうかを表示します。。 system services firewall policy show コマンドは、ファイアウォールポリシーを表示します。

このタスクについて

- Telnet はセキュアなプロトコルではありません。

クラスタにアクセスするときは、SSH を使用することを検討してください。SSH は、セキュアなリモートシェルと対話型のネットワークセッションを提供します。

- ONTAP では、1 つのノードについて同時に最大 50 の Telnet セッションがサポートされています。

クラスタ管理 LIF がノード上に存在する場合、クラスタ管理 LIF はこの制限をノード管理 LIF と共有します。

着信接続数が 1 秒あたり 10 を超えると、サービスは一時的に 60 秒間無効になります。

- ONTAP CLI に Windows ホストからアクセスする場合は、PuTTY などのサードパーティのユーティリティを使用できます。

手順

1. 管理ホストで次のコマンドを入力します。

**telnet *hostname\_or\_IP***

*hostname\_or\_IP* は、クラスタ管理LIFまたはノード管理LIFのホスト名またはIPアドレスです。クラスタ管理 LIF を使用することを推奨します。IPv4 または IPv6 アドレスを使用できます。

### Telnet要求の例

次の例は、Telnet アクセスを使用するように設定された「joe」というユーザが、クラスタ管理 LIF が 10.72.137.28 であるクラスタにアクセスする Telnet 要求を問題に送信する方法を示しています。

```
admin_host$ telnet 10.72.137.28
Data ONTAP
login: joe
Password:
cluster1::>
```

### RSH を使用してクラスタにアクセスします

クラスタへの問題 RSH 要求を使用して、管理タスクを実行できます。RSH はセキュアなプロトコルではなく、デフォルトでは無効になっています。

#### 必要なもの

RSH を使用してクラスタにアクセスするには、次の条件を満たしている必要があります。

- アクセス方法として RSH を使用するように設定された、クラスタのローカルユーザアカウントを持っている必要があります。

。 -application のパラメータ security login コマンドは、ユーザアカウントのアクセス方法を指定します。詳細については、を参照してください security login マニュアルページ

- RSH 要求がファイアウォールを通過できるように、クラスタ管理 LIF またはノード管理 LIF によって使用される管理ファイアウォールポリシーで RSH がすでに有効になっている必要があります。

デフォルトでは、RSHは無効になっています。。 system services firewall policy show コマンドにを指定します -service rsh パラメータは、ファイアウォールポリシーでRSHが有効になっているかどうかを表示します。詳細については、を参照してください system services firewall policy マニュアルページ

- IPv6 接続を使用する場合は、クラスタで IPv6 が設定されて有効になっている必要があります。また、ファイアウォールポリシーに IPv6 アドレスが設定されている必要があります。

。 network options ipv6 show IPv6が有効になっているかどうかを表示します。。 system services firewall policy show コマンドは、ファイアウォールポリシーを表示します。

#### このタスクについて

- RSH はセキュアなプロトコルではありません。

クラスタにアクセスするときは、SSH を使用することを検討してください。SSH は、セキュアなリモートシェルと対話型のネットワークセッションを提供します。

- ONTAP では、1 つのノードについて同時に最大 50 の RSH セッションがサポートされています。

クラスタ管理 LIF がノード上に存在する場合、クラスタ管理 LIF はこの制限をノード管理 LIF と共有します。

着信接続数が 1 秒あたり 10 を超えると、サービスは一時的に 60 秒間無効になります。

## 手順

1. 管理ホストで次のコマンドを入力します。

```
rsh hostname_or_IP -l username:passwordcommand
```

*hostname\_or\_IP* は、クラスタ管理 LIF または ノード管理 LIF のホスト名または IP アドレスです。クラスタ管理 LIF を使用することを推奨します。IPv4 または IPv6 アドレスを使用できます。

*command* は、RSH 経由で実行するコマンドです。

## RSH 要求の例

次の例は、RSH アクセスを使用するように設定された「joe」というユーザが、を実行する RSH 要求を問題で処理する方法を示しています `cluster show` コマンドを実行します

```
admin_host$ rsh 10.72.137.28 -l joe:password cluster show
```

Node	Health	Eligibility
node1	true	true
node2	true	true

2 entries were displayed.

```
admin_host$
```

## ONTAP コマンドラインインターフェイスを使用してください

### ONTAP コマンドラインインターフェイスを使用する

ONTAP コマンドラインインターフェイス（CLI）は、コマンドベースの管理インターフェイスです。ストレージシステムプロンプトでコマンドを入力すると、コマンドの結果がテキストで表示されます。

CLI コマンドプロンプトは、のように表示されます `cluster_name::>`。

権限レベルを設定した場合（つまり `-privilege` のパラメータ `set` コマンド）をに移動します ``advanced`` プロンプトにアスタリスク（\*）が表示されます。次に例を示します。

```
cluster_name::*>
```

## CLI コマンド用のシェルの種類について（クラスタ管理者のみ）

クラスタには、CLI コマンド用の異なる 3 つのシェルとして、`_clustershell_`、`_nodeshell_`、`_systemshell_` があります。各シェルの用途は異なり、それぞれに異なるコマンドセットがあります。

- クラスタシェルは、クラスタにログインすると自動的に開始されるネイティブシェルです。

クラスタの設定と管理に必要なすべてのコマンドが含まれています。クラスタシェルのCLIヘルプ（によってトリガーされます？（クラスタシェルのプロンプト））には、使用可能なクラスタシェルコマンドが表示されます。。 `man command_name` クラスタシェルのコマンドを実行すると、指定したクラスタシェルコマンドのマニュアルページが表示されます。

- ノードシェルは、ノードレベルでのみ有効なコマンドのための特別なシェルです。

ノードシェルには、からアクセスできます `system node run` コマンドを実行します

ノードシェルのCLIヘルプ（によってトリガーされます？または `help`（ノードシェルのプロンプト））には、使用可能なノードシェルコマンドが表示されます。。 `man command_name` ノードシェルのコマンドを実行すると、指定したノードシェルコマンドのマニュアルページが表示されます。

よく使用されるノードシェルコマンドとオプションの多くは、クラスタシェルにトンネリングまたはエイリアスされ、クラスタシェルから実行することもできます。

- システムシェルは、診断とトラブルシューティングの目的に限って使用する低レベルのシェルです。

システムシェルおよび関連する「タグ」アカウントは、下位レベルの診断用です。アクセスには `diagnostic` 権限が必要で、テクニカルサポートがトラブルシューティングタスクを実行するために予約されています。

クラスタシェルでのノードシェルのコマンドおよびオプションへのアクセス

ノードシェルのコマンドとオプションには、ノードシェルからアクセスできます。

```
system node run -node nodename
```

よく使用されるノードシェルコマンドとオプションの多くは、クラスタシェルにトンネリングまたはエイリアスされ、クラスタシェルから実行することもできます。

クラスタシェルでサポートされるノードシェルオプションには、を使用してアクセスできます `vserver options clustershell` コマンドを実行しますこれらのオプションを表示するには、次のいずれかを実行します。

- を使用してクラスタシェルCLIを照会します `vserver options -vserver nodename_or_clustername -option-name ?`
- にアクセスします `vserver options` を使用したクラスタシェルCLIのマニュアルページ `man vserver options`

クラスタシェルでノードシェルまたはレガシー ONTAP のコマンドまたはオプションを入力した場合、そのコマンドまたはオプションに相当するクラスタシェルコマンドがある場合には該当するクラスタシェルコマンドを使用するように通知されます。

クラスタシェルでノードシェルまたはレガシーのコマンドまたはオプションを入力した場合、そのコマンドまたはオプションについて「not supported」ステータスが ONTAP から通知されます。

使用可能なノードシェルコマンドを表示します

ノードシェルから CLI ヘルプを使用すると、使用可能なノードシェルコマンドのリストを取得できます。

手順

1. ノードシェルにアクセスするには、クラスタシェルのシステムプロンプトで次のコマンドを入力します。

```
system node run -node {nodename|local}
```

local は、クラスタへのアクセスに使用したノードです。



。 system node run コマンドにはエイリアスコマンドがあります。 run。

2. 使用可能なノードシェルコマンドのリストを表示するには、ノードシェルで次のコマンドを入力します。

```
[commandname] help
```

``\_commandname\_`` は、可用性を表示するコマンドの名前です。を含めない場合  
``\_commandname\_`` を選択すると、使用可能なすべてのノードシェルコマンドが表示されます。

入力します exit または、Ctrl+Dを入力してクラスタシェルCLIに戻ります。

利用可能なノードシェルコマンドを表示する例

次の例は、node2という名前のノードのノードシェルにアクセスし、ノードシェルコマンドの情報を表示します environment :

```
cluster1::> system node run -node node2
Type 'exit' or 'Ctrl-D' to return to the CLI

node2> environment help
Usage: environment status |
      [status] [shelf [<adapter>[.<shelf-number>]]] |
      [status] [shelf_log] |
      [status] [shelf_stats] |
      [status] [shelf_power_status] |
      [status] [chassis [all | list-sensors | Temperature | PSU 1 |
PSU 2 | Voltage | SYS FAN | NVRAM6-temperature-3 | NVRAM6-battery-3]]
```

CLI コマンドディレクトリの移動方法

CLI のコマンドは、コマンドディレクトリ別の階層に整理されています。完全なコマンドパスを入力するか、ディレクトリ構造を移動することで、階層内のコマンドを実行で

きます。

CLIを使用するときは、プロンプトにディレクトリの名前を入力し、Enter キーを押すと、コマンドディレクトリにアクセスできます。ディレクトリ名がプロンプトテキストに表示され、適切なコマンドディレクトリとやり取りしていることが示されます。コマンド階層のより下層に移動するには、コマンドサブディレクトリの名前を入力し、Enter キーを押します。サブディレクトリ名がプロンプトテキストに表示され、コンテキストがそのサブディレクトリに移動します。

コマンド全体を入力すると、複数のコマンドディレクトリを移動できます。たとえば、を入力すると、ディスクドライブに関する情報を表示できます `storage disk show` プロンプトでコマンドを入力します。また、次の例に示すように、一度に 1 つのコマンドディレクトリを移動して、コマンドを実行することもできます。

```
cluster1::> storage
cluster1::storage> disk
cluster1::storage disk> show
```

コマンドに最小文字数を入力してコマンドを現在のディレクトリに対して一意にすると、コマンドを省略できます。たとえば、前の例のコマンドを省略するには、と入力します `st d sh`。また、Tab キーを使用して省略したコマンドを展開し、デフォルトのパラメータ値を含むコマンドのパラメータを表示することもできます。

使用できます `top` コマンドを入力してコマンド階層の最上位に移動すると、が表示されます `up` コマンドまたは `..` コマンドを入力すると、コマンド階層の1つ上のレベルに移動します。



CLI でアスタリスク (\*) を付けたコマンドおよびコマンドオプションは、advanced 権限レベル以上でのみ実行できます。

## CLI で値を指定する際のルール

ほとんどのコマンドには、1 つ以上の必須またはオプションのパラメータが含まれています。多くのパラメータでは、値を指定する必要があります。CLI で値を指定するには、いくつかのルールがあります。

- 値には、数値、ブール指定子、事前に定義された値の列挙リストからの選択、またはテキスト文字列を指定できます。

一部のパラメータでは、2 つ以上の値をカンマで区切って指定できます。値をカンマで区切って指定したリストは、引用符 ("" ) で囲む必要はありません。テキスト、スペース、またはクエリ文字 (クエリを意図していない場合、または小なり記号または大なり記号で始まるテキスト) を指定する場合は、必ずエンティティを引用符で囲む必要があります。

- CLI は疑問符 ("" ? "" ) を解釈します。 をコマンドとして使用し、特定のコマンドのヘルプ情報を表示します。
- コマンド名、パラメータ、特定の値などの CLI に入力するテキストの一部では、大文字と小文字が区別されません。

たとえば、のパラメータ値を入力した場合などです `vserver cifs` コマンド、大文字と小文字の区別は無視されます。ただし、ノード、Storage Virtual Machine (SVM)、アグリゲート、ボリューム、論理インターフェイスの名前などのほとんどのパラメータ値は大文字と小文字が区別されます。

- 文字列またはリストをとるパラメータの値をクリアする場合は、空の一連の引用符（""）またはダッシュ（"-"）を指定します。
- ハッシュ記号("#") は、シャープ記号とも呼ばれ、コマンドライン入力のコメントを示します。使用する場合は、コマンドラインの最後のパラメータの後に表示されます。

CLI は行の末尾と "#" の間のテキストを無視します。

次の例では、テキストコメント付きで SVM が作成されます。次に、SVM が変更されてコメントが削除されます。

```
cluster1::> vservers create -vservers vs0 -subtype default -rootvolume
root_vs0
-aggregate aggr1 -rootvolume-security-style unix -language C.UTF-8 -is
-repository false -ipstack ipstackA -comment "My SVM"
cluster1::> vservers modify -vservers vs0 -comment ""
```

次の例では、"#" 記号を使用したコマンドラインコメントは、コマンドの動作を示しています。

```
cluster1::> security login create -vservers vs0 -user-or-group-name new-
admin
-application ssh -authmethod password #This command creates a new user
account
```

## コマンド履歴の表示方法とコマンドの再発行方法

各 CLI セッションには、そのセッションで実行されたすべてのコマンドの履歴が保持されます。現在のセッションのコマンド履歴を表示できます。また、コマンドの再発行も可能です。

コマンド履歴を表示するには、を使用します history コマンドを実行します

コマンドを再発行するには、を使用します redo 次のいずれかの引数を指定したコマンド。

- 前のコマンドの一部と一致する文字列

たとえば、のみの場合などです volume 実行したコマンドはです volume show`を使用できます `redo volume コマンドを再実行します。

- 前のコマンドの数値ID。に表示されます history コマンドを実行します

たとえば、を使用できます redo 4 履歴リストの4番目のコマンドを再発行するコマンド。

- 履歴リストの末尾からの負のオフセット

たとえば、を使用できます redo -2 2つ前に実行したコマンドを再発行するコマンド。



たとえば、コマンド履歴の末尾から 3 番目のコマンドを再実行するには、次のコマンドを入力します。

```
cluster1::> redo -3
```

## CLI コマンドを編集するためのキーボードショートカット

現在のコマンドプロンプトのコマンドは、アクティブなコマンドです。キーボードショートカットを使用して、アクティブなコマンドをすばやく編集できます。UNIX `tsch` シェルや Emacs エディタと同様のショートカットを使用できます。

次の表に、CLI コマンドを編集するためのキーボードショートカットを示します。「Ctrl +」は、Ctrl キーを押したまま、指定した文字を入力することを示します。“Esc-”は、Esc キーを押して離し、そのあとに指定した文字を入力することを示します。

状況	使用するキーボードショートカット
カーソルを 1 文字左に移動します	Ctrl+B キーを押下
戻る矢印	カーソルを 1 文字右に移動します
Ctrl+F	右矢印
カーソルを 1 単語分左に移動します	ESC-B
カーソルを 1 単語分右に移動します	ESC-F
カーソルを行頭に移動します	Ctrl+A
カーソルを行末へ移動します	Ctrl+E
行頭からカーソルまでの入力内容を切り取ってバッファに保存する 切り取りバッファは '一部のプログラムでは <i>clipboard</i> と呼ばれるのと同様に '一時的なメモリのよう	Ctrl+U キーを押下
カーソルから行末までの入力内容を切り取ってバッファに保存する	Ctrl+K キーを押下
カーソルから次の単語の末尾までを切り取ってバッファに保存する	ESC-D
カーソルの前の単語を切り取ってバッファに保存します	Ctrl+W キーを押下

状況	使用するキーボードショートカット
切り取りバッファの内容を取得し、カーソルのコマンドラインに挿入します	Ctrl+Y キーを押下
カーソルの前の文字を削除します	Ctrl+H
バックスペース	カーソル位置の文字を削除します
Ctrl+D を使用します	行をクリアします
Ctrl+C キーを押します	画面をクリアします
Ctrl+L キーを押下	コマンドライン上の現在の内容を、履歴リストの前のエントリに置き換えます。  このキーボードショートカットを押すたびに履歴カーソルが 1 つ前のエントリに移動します。
Ctrl+P キーを押下	ESC-P
上矢印	コマンドライン上の現在の内容を、履歴リストの次のエントリに置き換えます。このキーボードショートカットを押すたびに履歴カーソルが次のエントリに移動します。
Ctrl+N キーを押下	ESC-N
下矢印	部分的に入力されたコマンドを展開するか、現在の編集位置から有効な入力の一覧を表示します
タブをクリックする	Ctrl+I
状況に応じたヘルプを表示します	?
疑問符 ("") の特殊なマッピングをエスケープします?"") character. For instance, to enter a question mark into a command's argument, press Esc and then the "?" 文字。	ESC - ?
TTY 出力を開始します	Ctrl+Q キーを押下
TTY 出力を停止します	Ctrl+S

## 管理権限レベルの使用

ONTAP のコマンドとパラメータは、*admin*、*advanced*、*ddiagnostic* の 3 つの権限レベルで定義されます。権限レベルは、タスクの実行に必要なスキルレベルに対応しています。

- \* admin \*

このレベルではほとんどのコマンドとパラメータを使用できます。これらは、一般的なタスクまたはルーチンタスクに使用されます。

- \* 詳細 \*

このレベルのコマンドとパラメータは高度な知識を必要とし、あまり使用されません。不適切に使用すると、原因の問題につながる可能性があります。

高度なコマンドまたはパラメータを使用する場合は、必ずサポート担当者のアドバイスを受けてください。

- \* 診断 \*

診断コマンドおよびパラメータは、システム停止の原因になる可能性がありますこれらのコマンドは、サポート担当者が問題の診断と修正を行う場合にのみ使用します。

## CLI で権限レベルを設定します

CLIで権限レベルを設定するには、を使用します `set` コマンドを実行します権限レベルの設定の変更は、現在のセッションにのみ適用されます。これらは、セッションをまたいで持続することはありません

### 手順

1. CLIで権限レベルを設定するには、を使用します `set` コマンドにを指定します `-privilege` パラメータ

### 権限レベルの設定の例

次の例は、権限レベルを `advanced` に設定してから、`admin` に設定します。

```
cluster1::> set -privilege advanced
Warning: These advanced commands are potentially dangerous; use them only
when directed to do so by NetApp personnel.
Do you wish to continue? (y or n): y
cluster1::*> set -privilege admin
```

## CLI で表示環境を設定します

を使用して、CLIセッションの表示環境を設定できます `set` コマンドおよび `rows` コマンドを実行します設定した環境設定は、現在のセッションにのみ適用されます。これらは、セッションをまたいで持続することはありません

このタスクについて

次の CLI 表示環境を設定できます。

- コマンドセッションの権限レベル
- システムを停止させる可能性のあるコマンドについては確認を発行するかどうか
- かどうか `show` すべてのフィールドが表示されます
- フィールド区切り文字として使用する文字
- データサイズを報告するときのデフォルトの単位
- インターフェイスが出力を一時的に停止する前に、現在の CLI セッションで画面に表示する行数

行数を指定しない場合、端末の実際の高さに基づいて自動的に調整されます。実際の高さが定義されていない場合、デフォルトの行数は 24 です。

- デフォルトの Storage Virtual Machine (SVM) またはノード
- エラーが発生した場合に続行中のコマンドを停止するかどうか

## 手順

1. CLIの表示環境を設定するには、を使用します `set` コマンドを実行します

現在のCLIセッションで画面に表示する行数を設定するには、を使用することもできます `rows` コマンドを実行します

詳細については、のマニュアルページを参照してください `set` コマンドおよび `rows` コマンドを実行します

## CLIでの表示環境の設定の例

次の例では、カンマをフィールド区切り文字として設定します。はを設定します GB デフォルトのデータサイズ単位として、行数を50に設定します。

```
cluster1::> set -showseparator "," -units GB
cluster1::> rows 50
```

## クエリ演算子の使用方法

管理インターフェイスでは、クエリと UNIX 形式のパターンおよびワイルドカードがサポートされており、コマンドパラメータ引数の複数の値を照合できます。

次の表に、サポートされるクエリ演算子を示します。

演算子	説明
*	すべてのエントリに一致するワイルドカード。  たとえば、コマンドなどです <code>volume show -volume *tmp*</code> 名前にこの文字列が含まれるすべてのボリュームのリストが表示されます <code>tmp</code> 。

演算子	説明
!	NOT 演算子。  一致しない値を示します。例： <b>!vs0</b> 値と一致しないことを示します vs0。
OR演算子。  比較する2つの値を区切ります。 例： `*vs0`	vs2*` vs0またはvs2のいずれかに一致します。複数のORステートメントを指定できます。次に例を示します。`a`
b*	*c*` エントリと一致します a、で始まるエントリ b、およびを含むすべてのエントリ c。
。	範囲演算子。  例： <b>5..10</b> の任意の値に一致します 5 終了： 10、包括的。
<	less-than 演算子。  例： <b>&lt;20</b> より小さい値に一致します 20。
>	greater-than 演算子。  例： <b>&gt;5</b> より大きい任意の値に一致します 5。
>=	less-than-or-equal-to 演算子。  例： <b>≤5</b> 以下の値に一致します 5。
>=	greater-than-or-equal-to 演算子。  例： <b>&gt;=5</b> 以上の値に一致します 5。
{query}	拡張クエリ。  拡張クエリは、コマンド名のあとで、他のパラメータの前の最初の引数として指定する必要があります。  たとえば、コマンドなどです volume modify {-volume *tmp*} -state offline 名前に文字列が含まれるすべてのボリュームをオフラインに設定します tmp。

クエリ文字をリテラルとして解析する場合は、文字を二重引用符で囲む必要があります（例： "<10"、"0..100"、"\*abc\*"`または `"a|b"）をクリックして、正しい結果が返されます。

特殊文字が解釈されないように、rawファイル名は二重引用符で囲む必要があります。クラスタシェルで 사용되는環境特殊文字もこれに該当します。

1つのコマンドラインで複数のクエリ演算子を使用できます。たとえば、コマンドなどです `volume show -size >1GB -percent-used <50 -vserver !vs1` 「vs1」という名前のStorage Virtual Machine (SVM) 内ではなく、サイズが1GBを超え、使用率が50%未満のすべてのボリュームが表示されます。

## 関連情報

["CLI コマンドを編集するためのキーボードショートカット"](#)

## 拡張クエリの使用方法

拡張クエリを使用して、指定した値を持つオブジェクトに対して操作を照合し、実行することができます。

拡張クエリは、中括弧（`{}`）で囲んで指定します。拡張クエリは、コマンド名のあとで、他のパラメータの前の最初の引数として指定する必要があります。たとえば、名前に文字列が含まれるすべてのボリュームをオフラインに設定するには、を指定します ``tmp`` 次の例でコマンドを実行します。

```
cluster1::> volume modify {-volume *tmp*} -state offline
```

拡張クエリは通常、でのみ有効です `modify` および `delete` コマンド彼らには意味がありません `create` または `show` コマンド

クエリと変更操作の組み合わせは便利なツールです。ただし、原因を正しく実装しないと、混乱したり、エラーが発生する可能性があります。たとえば、（advanced権限）を使用する場合 `system node image modify` ノードのデフォルトのソフトウェアイメージを設定するコマンドを実行すると、他のソフトウェアイメージが自動的にデフォルトにならないように設定されます。次の例のコマンドは、実質的には NULL 操作です。

```
cluster1::*> system node image modify {-isdefault true} -isdefault false
```

このコマンドは、現在のデフォルトイメージをデフォルト以外のイメージとして設定してから、新しいデフォルトイメージ（以前のデフォルト以外のイメージ）をデフォルト以外のイメージに設定します。その結果、元のデフォルト設定が保持されます。正しく操作を実行するには、次の例のようにコマンドを使用します。

```
cluster1::*> system node image modify {-iscurrent false} -isdefault true
```

## フィールドを使用した **show** コマンド出力のカスタマイズ方法

を使用する場合 `-instance` パラメータにを指定します `show` コマンドを使用して詳細を表示すると、出力に時間がかかり、必要以上の情報が含まれることがあります。。  
`-fields` のパラメータ `show` コマンドでは、指定した情報のみを表示できます。

たとえば、実行中です `volume show -instance` いくつかの画面に情報が表示される可能性があります。を使用できます `volume show -fields fieldname[,fieldname...]` （常に表示されるデフォルトのフィ

ールドに加えて) 指定したフィールドのみが含まれるように出力をカスタマイズします。 使用できます  
-fields ? の有効なフィールドを表示します show コマンドを実行します

次の例は、の出力の違いを示しています -instance パラメータおよび -fields パラメータ：

```
cluster1::> volume show -instance

                                Vserver Name: cluster1-1
                                Volume Name: vol0
                                Aggregate Name: aggr0
                                Volume Size: 348.3GB
                                Volume Data Set ID: -
                                Volume Master Data Set ID: -
                                Volume State: online
                                Volume Type: RW
                                Volume Style: flex
                                ...
                                Space Guarantee Style: volume
                                Space Guarantee in Effect: true
                                ...
Press <space> to page down, <return> for next line, or 'q' to quit...
...
cluster1::>

cluster1::> volume show -fields space-guarantee,space-guarantee-enabled

vserver  volume  space-guarantee  space-guarantee-enabled
-----  -
cluster1-1 vol0    volume                true
cluster1-2 vol0    volume                true
vs1      root_vol
          volume                true
vs2      new_vol
          volume                true
vs2      root_vol
          volume                true
...
cluster1::>
```

位置指定パラメータについて

ONTAP CLI の位置指定パラメータ機能を活用して、効率的にコマンドを入力することができます。あるコマンドの位置指定パラメータは、そのコマンドのヘルプで特定できます。

## 位置指定パラメータとは何ですか

- 位置指定パラメータは、値を指定する前にパラメータ名を指定する必要のないパラメータです。
- コマンド入力には、位置指定パラメータとそれ以外のパラメータを組み合わせで指定できます。ただし、**command\_name ?** 出力。に示すように、同じコマンド内の他の位置指定パラメータとの相対的な順序に従っている必要があります
- 位置指定パラメータは、必須パラメータの場合とオプションパラメータの場合があります。
- あるパラメータが1つのコマンドでは位置指定パラメータで、別のコマンドでは位置指定パラメータでない場合もあります。



位置指定パラメータ機能をスクリプトで使用する場合は、特に位置指定パラメータがオプションパラメータである場合や、位置指定パラメータの前にオプションパラメータを指定する場合には推奨されません。

## 位置指定パラメータを特定します

位置指定パラメータはで特定できます **command\_name ?** コマンド出力。位置指定パラメータは、次のいずれかの形式で、パラメータ名が角かっこで囲まれています。

- `[-parameter_name] parameter_value` は、必須の位置指定パラメータを示しています。
- `[[[-parameter_name] parameter_value]]` は、オプションの位置指定パラメータを示します。

たとえば、で次のように表示されているとします **command\_name ?** の出力では、パラメータは該当するコマンドの位置指定パラメータです。

- `[-lif] <lif-name>`
- `[[[-lif] <lif-name>]]`

ただし、次の出力では、パラメータは該当するコマンドの位置指定パラメータではありません。

- `-lif <lif-name>`
- `[-lif <lif-name>]`

## 位置指定パラメータの使用例

次の例では、を使用しています **volume create ?** の出力から、このコマンドの3つのパラメータが位置指定パラメータであることがわかります。 `-volume`、`-aggregate`および`-size`。



```

cluster1::> volume create ?
    -vserver <vserver name>                Vserver Name
    [-volume] <volume name>                Volume Name
    [-aggregate] <aggregate name>          Aggregate Name
    [[-size] {<integer>[KB|MB|GB|TB|PB]]]   Volume Size
    [ -state {online|restricted|offline|force-online|force-offline|mixed} ]
                                           Volume State (default: online)
    [ -type {RW|DP|DC} ]                   Volume Type (default: RW)
    [ -policy <text> ]                     Export Policy
    [ -user <user name> ]                 User ID
    ...
    [ -space-guarantee|-s {none|volume} ]   Space Guarantee Style (default:
volume)
    [ -percent-snapshot-space <percent> ]   Space Reserved for Snapshot
Copies
    ...

```

次の例では、を使用しています `volume create` 位置指定パラメータ機能を使用せずにコマンドを指定します。

```

cluster1::> volume create -vserver svml -volume vol1 -aggregate aggr1 -size 1g
-percent-snapshot-space 0

```

次の例では、位置指定パラメータ機能を使用して効率的にコマンドを入力しています。位置指定パラメータとそれ以外のパラメータがの中に散在しています `volume create` コマンド、および位置指定パラメータの値は、パラメータ名なしで指定します。位置指定パラメータは、と同じ順序で指定します **volume create ?** 出力。つまり、の値です `-volume` はの前に指定されます `-aggregate` をクリックします。これは、の前に指定されています `-size`。

```

cluster1::> volume create vol2 aggr1 1g -vserver svml -percent-snapshot-space 0

```

```

cluster1::> volume create -vserver svml vol3 -snapshot-policy default aggr1
-nvfail off 1g -space-guarantee none

```

## ONTAP マニュアルページへのアクセス方法

ONTAP のマニュアル（マニュアル） ページでは、ONTAP CLI コマンドの使用方法が説明されています。これらのページはコマンドラインから入手でき、リリース固有の\_コマンドリファレンス\_でも公開されています。

ONTAP コマンドラインで、を使用します `man command name` コマンドを使用して、指定したコマンドのマニュアルページを表示します。コマンド名を指定しない場合は、マニュアルページのインデックスが表示されます。を使用できます `man man` コマンドを使用して、に関する情報を表示します `man` コマンド自体。マニュアルページを終了するには、と入力します **q**。

を参照してください [使用しているONTAP 9のバージョンに対応するコマンドリファレンス](#) を参照して、ご使用のリリースで使用可能な管理者レベルおよびアドバンスレベルのONTAP コマンドの詳細を確認してください。

## CLIセッションを管理します。

指定した名前とサイズの上限を使用して CLI セッションをファイルに記録し、そのファイルを FTP または HTTP のアップロード先にアップロードできます。また、以前に記録した CLI セッションのファイルを表示または削除することもできます。

### CLI セッションを記録します

CLI セッションのレコードを停止するか終了するか、ファイルが指定したサイズの上限に達したときに、CLI セッションのレコードが終了します。デフォルトのファイルサイズの上限は 1MB です。最大ファイルサイズの上限は 2GB です。

CLI セッションを記録しておく、たとえば、問題のトラブルシューティングを行って詳細情報を保存したり、特定の時点でのスペース使用量の永続的なレコードを作成したりする場合に便利です。

#### 手順

1. 現在のCLIセッションのファイルへの記録を開始します。

```
system script start
```

を使用する方法の詳細については、を参照してください system script start コマンドについては、マニュアルページを参照してください。

指定したファイルへの CLI セッションの記録が開始されます。 ONTAP

2. CLI セッションを続行します。
3. 終了したら、セッションの記録を停止します。

```
system script stop
```

を使用する方法の詳細については、を参照してください system script stop コマンドについては、マニュアルページを参照してください。

ONTAP が CLI セッションの記録を停止します。

### CLI セッションのレコードを管理するコマンド

を使用します system script CLIセッションのレコードを管理するコマンド。

状況	使用するコマンド
指定したファイルへの現在の CLI セッションの記録を開始します	system script start
現在の CLI セッションの記録を停止します	system script stop

状況	使用するコマンド
CLI セッションのレコードに関する情報を表示します	<code>system script show</code>
CLI セッションのレコードを FTP または HTTP のデスティネーションにアップロードします	<code>system script upload</code>
CLI セッションのレコードを削除します	<code>system script delete</code>

#### 関連情報

["ONTAP 9 コマンド"](#)

#### CLI セッションの自動タイムアウト時間を管理するコマンド

タイムアウト値は、CLI セッションが自動的に終了するまでアイドル状態を維持する時間を指定します。CLI タイムアウト値はクラスタ全体が対象です。つまり、クラスタ内のどのノードも同じ CLI タイムアウト値を使用します。

デフォルトでは、CLI セッションの自動タイムアウト時間は 30 分です。

を使用します `system timeout` CLI セッションの自動タイムアウト時間を管理するコマンド。

状況	使用するコマンド
CLI セッションの自動タイムアウト時間を表示します	<code>system timeout show</code>
CLI セッションの自動タイムアウト時間を変更します	<code>system timeout modify</code>

#### 関連情報

["ONTAP 9 コマンド"](#)

#### クラスタ管理（クラスタ管理者のみ）

クラスタ内のノードに関する情報を表示します。

ノード名、ノードが正常に機能しているかどうか、ノードがクラスタへの参加条件を満たしているかどうかを表示できます。advanced 権限レベルでは、ノードにイプシロンが設定されているかどうかを表示できます。

#### 手順

1. クラスタ内のノードに関する情報を表示するには、を使用します `cluster show` コマンドを実行します

ノードにイプシロンが設定されているかどうかを表示するには、advanced 権限レベルでコマンドを実行します。

クラスタ内のノードを表示する例

次の例は、4 ノードクラスタ内のすべてのノードに関する情報を表示します。

```
cluster1::> cluster show
Node           Health Eligibility
-----
node1          true  true
node2          true  true
node3          true  true
node4          true  true
```

次の例は、advanced 権限レベルで「node1」という名前のノードに関する詳細情報を表示します。

```
cluster1::> set -privilege advanced
Warning: These advanced commands are potentially dangerous; use them only
when directed to do so by support personnel.
Do you want to continue? {y|n}: y

cluster1::*> cluster show -node node1

      Node: node1
Node UUID: a67f9f34-9d8f-11da-b484-000423b6f094
  Epsilon: false
Eligibility: true
    Health: true
```

クラスタ属性を表示します

クラスタの一意の識別子（UUID）、名前、シリアル番号、場所、連絡先情報を表示できます。

手順

1. クラスタの属性を表示するには、を使用します cluster identity show コマンドを実行します

クラスタ属性を表示する例

次の例は、クラスタの名前、シリアル番号、場所、連絡先情報を表示します。

```
cluster1::> cluster identity show

      Cluster UUID: 1cd8a442-86d1-11e0-ae1c-123478563412
      Cluster Name: cluster1
Cluster Serial Number: 1-80-123456
  Cluster Location: Sunnyvale
    Cluster Contact: jsmith@example.com
```

## クラスタ属性を変更

クラスタ名、場所、および連絡先情報などのクラスタ属性を必要に応じて変更できます。

### このタスクについて

クラスタの作成時に設定されたクラスタの UUID は変更できません。

### 手順

1. クラスタの属性を変更するには、を使用します `cluster identity modify` コマンドを実行します
  - 。 `-name` パラメータは、クラスタの名前を指定します。。 `cluster identity modify` のマニュアルページに、クラスタ名の指定に関するルールが記載されています。
  - 。 `-location` パラメータは、クラスタの場所を指定します。
  - 。 `-contact` パラメータは、名前やEメールアドレスなどの連絡先情報を指定します。

### クラスタ名の変更例

次のコマンドは、現在のクラスタ名（「cluster1」）を「cluster2」に変更します。

```
cluster1::> cluster identity modify -name cluster2
```

## クラスタレプリケーションリングのステータスを表示します

クラスタレプリケーションリングのステータスを表示して、クラスタ全体の問題の診断に役立てることができます。クラスタに問題がある場合は、トラブルシューティングに役立てるために、サポート担当者からこのタスクを実行するように依頼される場合があります。

### 手順

1. クラスタレプリケーションリングのステータスを表示するには、を使用します `cluster ring show` コマンドをadvanced権限レベルで実行します。

### クラスタリングレプリケーションステータスの表示例

次の例では、node0 という名前のノードの VLDB レプリケーションリングのステータスが表示されています。

```

cluster1::> set -privilege advanced
Warning: These advanced commands are potentially dangerous; use them only
when directed to do so by support personnel.
Do you wish to continue? (y or n): y

cluster1::*> cluster ring show -node node0 -unitname vldb
      Node: node0
    Unit Name: vldb
      Status: master
        Epoch: 5
Master Node: node0
  Local Node: node0
      DB Epoch: 5
DB Transaction: 56
  Number Online: 4
      RDB UUID: e492d2c1-fc50-11e1-bae3-123478563412

```

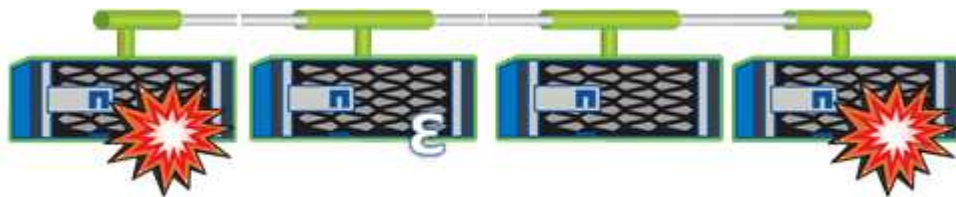
## クォーラムとイプシロンについて

クォーラムとイプシロンは、クラスタの健全性と機能を判断するための重要な基準で、通信および接続に関する潜在的な問題へのクラスタの対応を決定します。

Quorum は、クラスタが完全に機能するための前提条件です。クラスタがクォーラムを構成している場合は、過半数のノードが正常で、相互に通信可能です。クォーラムが失われると、クラスタは通常のクラスタ処理を実行できなくなります。すべてのノードが1つのまとまりとしてデータの単一のビューを共有するため、任意の時点において1つのノードの集まりだけがクォーラムを構成することができます。したがって、通信が確立されていない2つのノードで、異なる方法でデータを変更することが許可されている場合には、データを1つのデータビューに表示できなくなります。

クラスタ内の各ノードはノードマスターを選出する投票プロトコルに属しており、残りの各ノードは secondary です。マスターノードは、クラスタ内に情報を同期する役割を担います。形成されたクォーラムは継続的な投票によって維持されます。マスターノードがオフラインになった場合、クラスタでクォーラムが維持されていれば、オンラインのノードの投票によって新しいマスターが選出されます。

ノード数が偶数のクラスタの場合は同票となる可能性があるため、1つのノードに epsilon という名前の投票荷重が追加で設定されます。大規模なクラスタの同じ数のノード間で接続障害が発生した場合、すべてのノードが正常であることを条件に、イプシロンが設定されたノードのグループがクォーラムを維持します。たとえば、次の図では、4ノードクラスタの2つのノードで障害が発生しています。ただし、残りのノードの1つにイプシロンが設定されているため、正常なノードが過半数に満たなくてもクォーラムが維持されます。



クラスタが作成されると、自動的に最初のノードにイプシロンが割り当てられます。イプシロンを保持してい

るノードで障害が発生したり、ハイアベイラビリティパートナーをテイクオーバーしたり、ハイアベイラビリティパートナーにテイクオーバーされた場合、イプシロンは別の HA ペアの正常なノードに自動的に再割り当てされます。

ノードをオフラインにすると、クラスタがクォーラムを維持できるかどうかに影響することがあります。そのため ONTAP、クラスタのクォーラムが失われたり、あと 1 つのノード障害によってクォーラムが失われるような処理を実行しようとする、警告メッセージが表示されます。クォーラムに関する警告メッセージを無効にするには、を使用します `cluster quorum-service options modify` コマンドを advanced 権限レベルで実行します。

一般に、クラスタのノード間に信頼性の高い接続が確立されている場合、小規模のクラスタよりも大規模のクラスタの方が安定します。ノードの半数にイプシロンを加えた過半数のクォーラムの要件は、2 ノードのクラスタよりも 24 ノードのクラスタの方が簡単に維持できます。

2 ノードクラスタでは、クォーラムの維持に独特な課題が存在します。2 ノードクラスタでは、どちらのノードにもイプシロンが設定されていない `cluster ha_` を使用します。代わりに、両方のノードを継続的にポーリングすることで、一方のノードで障害が発生した場合にデータに対する読み取り / 書き込みのフルアクセスと、論理インターフェイスおよび管理機能へのアクセスが許可されます。

システムボリュームとは

システムボリュームとは、ファイルサービスや監査ログのメタデータなど、特別なメタデータを格納する FlexVol です。クラスタ内のストレージの使用をすべて把握できるように、システムボリュームはクラスタ内で表示することができます。

システムボリュームはクラスタ管理サーバ（管理 SVM）によって所有され、ファイルサービスの監査が有効になっている場合に自動的に作成されます。

を使用してシステムボリュームを表示できます `volume show` コマンドを実行しますが、それ以外のほとんどのボリューム処理は実行できません。たとえば、を使用してシステムボリュームを変更することはできません `volume modify` コマンドを実行します

次に、管理 SVM 上にある 4 個のシステムボリュームの例を示します。これらのボリュームは、クラスタ内でデータ SVM のファイルサービスの監査が有効になっているときに自動的に作成されたものです。

```
cluster1::> volume show -vserver cluster1
```

Vserver	Volume	Aggregate	State	Type	Size	Available
cluster1	MDV_aud_1d0131843d4811e296fc123478563412	aggr0	online	RW	2GB	1.90GB
5%						
cluster1	MDV_aud_8be27f813d7311e296fc123478563412	root_vs0	online	RW	2GB	1.90GB
5%						
cluster1	MDV_aud_9dc4ad503d7311e296fc123478563412	aggr1	online	RW	2GB	1.90GB
5%						
cluster1	MDV_aud_a4b887ac3d7311e296fc123478563412	aggr2	online	RW	2GB	1.90GB
5%						

4 entries were displayed.

## ノードを管理

クラスタにノードを追加します

作成したクラスタは、ノードを追加して拡張できます。一度に追加できるノードは1つだけです。

必要なもの

- 複数ノードクラスタにノードを追加する場合は、クラスタ内の既存のすべてのノードが正常である必要があります（`cluster show`）。
- 2ノードスイッチレスクラスタにノードを追加する場合は、NetAppでサポートされるクラスタスイッチを使用して、2ノードスイッチレスクラスタをスイッチ接続クラスタに変換する必要があります。

スイッチレスクラスタ機能は、2ノードクラスタでのみサポートされます。

- シングルノードクラスタに2つ目のノードを追加する場合は、その2つ目のノードがインストールされていて、クラスタネットワークが構成されている必要があります。
- クラスタでSPの自動設定が有効になっている場合は、追加するノードが指定されたサブネットを使用してSPを自動的に設定できるように、SP用に指定されたサブネットに利用可能なリソースが必要です。
- 新しいノードのノード管理 LIF について、次の情報を収集しておく必要があります。
  - ポート
  - IP アドレス
  - ネットマスク
  - デフォルトゲートウェイ



## このタスクについて

ノードは、HA ペアを形成できるように偶数である必要があります。クラスタへのノードの追加を開始したら、その処理を完了する必要があります。別のノードの追加を開始するには、事前にノードがクラスタに含まれている必要があります。

## 手順

1. クラスタに追加するノードに電源を入れます。

ノードがブートし、ノードのセットアップウィザードがコンソール上で起動されます。

```
Welcome to node setup.
```

```
You can enter the following commands at any time:
```

```
"help" or "?" - if you want to have a question clarified,
```

```
"back" - if you want to change previously answered questions, and
```

```
"exit" or "quit" - if you want to quit the setup wizard.
```

```
Any changes you made before quitting will be saved.
```

```
To accept a default or omit a question, do not enter a value.
```

```
Enter the node management interface port [e0M]:
```

2. ノードのセットアップウィザードを終了します。 `exit`

ノードのセットアップウィザードが終了し、セットアップタスクが完了していないという警告がログインプロンプトに表示されます。

3. を使用して、adminアカウントにログインします `admin` ユーザ名。
4. クラスタセットアップウィザードを開始します。

```
cluster setup
```

```
::> cluster setup
```

Welcome to the cluster setup wizard.

You can enter the following commands at any time:

"help" or "?" - if you want to have a question clarified,  
"back" - if you want to change previously answered questions, and  
"exit" or "quit" - if you want to quit the cluster setup wizard.  
Any changes you made before quitting will be saved.

You can return to cluster setup at any time by typing "cluster setup".  
To accept a default or omit a question, do not enter a value....

Use your web browser to complete cluster setup by accessing  
`https://<node_mgmt_or_e0M_IP_address>`

Otherwise, press Enter to complete cluster setup using the  
command line interface:



セットアップ GUI を使用したクラスタのセットアップの詳細については、を参照してください ["System Manager の略" オンラインヘルプ](#)。

5. CLI を使用してこの作業を完了するには、Enter キーを押します。新しいクラスタを作成するか既存のクラスタに参加するかを確認するメッセージが表示されたら、と入力します **join**。

```
Do you want to create a new cluster or join an existing cluster?  
{create, join}:  
join
```

新しいノードで実行されているONTAPのバージョンが既存のクラスタで実行されているバージョンと異なる場合は、System checks Error: Cluster join operation cannot be performed at this time エラー。これは想定される動作です。続行するには、`add-node -allow-mixed-version -join new_node_name` クラスタ内の既存のノードからadvanced権限レベルでコマンドを実行します。

6. プロンプトに従ってノードをセットアップし、クラスタに追加します。
  - プロンプトでデフォルト値を受け入れるには、Enter キーを押します。
  - プロンプトで独自の値を入力するには、値を入力して Enter キーを押します。
7. 追加するノードごとに前述の手順を繰り返します。

完了後

ノードをクラスタに追加したあと、HA ペアごとにストレージフェイルオーバーを有効にする必要があります。

関連情報

## "バージョンが混在したONTAPクラスタ"

クラスタからノードを削除します

クラスタから不要なノードを一度に 1 つずつ削除できます。ノードを削除したら、フェイルオーバーパートナーも削除する必要があります。ノードを削除すると、そのノードのデータはアクセスできなくなるか、消去されます。

作業を開始する前に

クラスタからノードを削除するには、次の条件を満たしている必要があります。

- クラスタ内のノードのうち半数を上回るノードが正常である必要があります。
- 削除するノード上のすべてのデータを退避しておく必要があります。
  - これには、などが含まれます ["暗号化されたボリュームからのデータのページ"](#)。
- ルート以外のすべてのボリュームが削除されている必要があります ["移動しました"](#) ノードが所有するアグリゲートから作成します。
- ルート以外のアグリゲートはすべて削除されています ["削除済み"](#) をクリックします。
- ノードが Federal Information Processing Standard （ FIPS ；連邦情報処理標準）ディスクまたは Self-Encrypting Disk （ SED ；自己暗号化ディスク）を所有している場合は、["ディスク暗号化が削除されました"](#) ディスクを非保護モードに戻します。
  - 必要に応じて、を実行することもできます ["FIPS ドライブまたは SED を完全消去します"](#)。
- データ LIF が作成されました ["削除済み"](#) または ["再配置済み"](#) をクリックします。
- クラスタ管理 LIF が作成されました ["再配置済み"](#) ノードから、ホームポートが変更されました。
- すべてのクラスタ間 LIF を確認しておきます ["削除されました"](#)。
  - クラスタ間 LIF を削除するときに表示される警告は無視してかまいません。
- ストレージフェイルオーバーは実行されています ["無効"](#) をクリックします。
- すべての LIF フェイルオーバールールが適用されていることを確認し ["変更されました"](#) をクリックしてノードのポートを削除します。
- ノードのすべての VLAN を設定しておきます ["削除済み"](#)。
- 削除するノードにLUNがある場合は、適切な手順を実行してください ["選択的LUNマップ（SLM）のレポートノードリストを変更します"](#) ノードを削除する前に、

SLMのレポートノードリストからノードとそのHAパートナーを削除しないと、LUNを含むボリュームが別のノードに移動された場合でも、ノードに以前格納されていたLUNへのアクセスが失われる可能性があります。

ノードを削除中であることをネットアップテクニカルサポートに通知する AutoSupport メッセージを問題で送信することを推奨します。

\*注：\*などの操作は実行しないでください `cluster remove-node`、`cluster unjoin`および`node rename` ONTAP の自動アップグレードが進行中の場合。

このタスクについて

- バージョンが混在したクラスタを実行している場合は、ONTAP 9.3 以降の advanced 権限のコマンドのいずれかを使用して、バージョンが低い最後のノードを削除できます。
  - ONTAP 9.3: `cluster unjoin -skip-last-low-version-node-check`
  - ONTAP 9.4以降: `cluster remove-node -skip-last-low-version-node-check`
- 4ノードクラスタから2つのノードを分離すると、残りの2つのノードでクラスタHAが自動的に有効になります。



クラスタからノードを削除する前に、ノードに接続されているすべてのディスクのすべてのシステムデータとユーザーデータにユーザがアクセスできないようにする必要があります。ノードが誤ってクラスタから参加解除された場合は、ネットアップサポートにリカバリのオプションを問い合わせてください。

## 手順

1. 権限レベルを advanced に変更します。

```
set -privilege advanced
```

2. クラスタのノードにイプシロンが設定されているかどうかを確認します。

```
cluster show -epsilon true
```

3. クラスタのノードにイプシロンが設定されていて、そのノードを分離する場合は、分離しないノードにイプシロンを移動します。
  - a. 分離するノードからイプシロンを移動します。

```
cluster modify -node <name_of_node_to_be_unjoined> -epsilon false
```

- b. 分離しないノードにイプシロンを移動します。

```
cluster modify -node <node_name> -epsilon true
```

4. 現在のマスターノードを特定します。

```
cluster ring show
```

マスターノードとは、「m GMT」、「vldb」、「vifmgr」、「bcomd」、「crs」などのプロセスを保持するノードです。

5. 削除するノードが現在のマスターノードである場合は、クラスタ内の別のノードがマスターノードとして選出されるようにします。
  - a. 現在のマスターノードをクラスタに参加できないようにします。

```
cluster modify - node <node_name> -eligibility false
```

マスターノードが参加資格を得られなくなると、残りのノードの1つがクラスタクォーラムによって新しいマスターとして選出されます。

- b. 以前のマスターノードを再びクラスタに参加できるようにします。

```
cluster modify - node <node_name> -eligibility true
```

6. 削除するノードとは別のノードのリモートノード管理LIFまたはクラスタ管理LIFにログインします。
7. クラスタからノードを削除します。

ONTAP バージョン	使用するコマンド
ONTAP 9.3	<pre>cluster unjoin</pre>
ONTAP 9.4以降	<pre>cluster remove-node*</pre>

バージョンが混在したクラスタでバージョンが低い最後のノードを削除する場合は、を使用します `-skip-last-low-version-node-check` パラメータを指定します。

次の内容が表示されます。

- また、ノードのフェイルオーバーパートナーをクラスタから削除する必要があります。
- ノードを削除してクラスタに再追加する前に、ブートメニューオプション（4）クリーン構成を使用してすべてのディスクまたはオプションを初期化する（9）アドバンスドドライブパーティショニングの設定を消去してすべてのディスクを初期化する必要があります。

ノードを削除する前に対処が必要な条件がある場合は、エラーメッセージが生成されます。メッセージの内容は、たとえば、削除が必要なノードに共有リソースがある、あるいはノードのクラスタ HA 構成またはストレージフェイルオーバー構成を無効にする必要があるなどの場合があります。

ノードがクォーラムマスターの場合、クラスタのクォーラムがいったん失われて、すぐに戻ります。クォーラムが失われるのは一時的であり、データの操作には影響しません。

8. エラーメッセージにエラー状態が示された場合は、それらの状態に対処し、を再実行します `cluster remove-node` または `cluster unjoin` コマンドを実行します

ノードは、クラスタから正常に削除されると自動的にリブートされます。

9. ノードを転用する場合は、ノードの設定を消去し、すべてのディスクを初期化します。
  - a. ブートプロセス時に、プロンプトが表示されたら Ctrl+C キーを押してブートメニューを表示します。

b. ブートメニューオプション[ (4) Clean configuration and initialize all disks]を選択します。

10. admin 権限レベルに戻ります。

```
set -privilege admin
```

11. クラスタからフェイルオーバーパートナーを削除するには、前述の手順を繰り返します。

**Web** ブラウザを使用して、ノードのログファイル、コアダンプファイル、 **MIB** ファイルにアクセスします

サービスプロセッサインフラ (spi) Webサービスはデフォルトで有効になっており、クラスタ内のノードのログファイル、コアダンプファイル、およびMIBファイルにWebブラウザからアクセスできます。ノードが停止した場合でも、パートナーにテイクオーバーされていれば、ファイルにアクセスできます。

必要なもの

- クラスタ管理 LIF が起動している必要があります。

には、クラスタまたはノードの管理LIFを使用してアクセスできます spi Webサービス。ただし、クラスタ管理 LIF を使用することを推奨します。

。 network interface show コマンドは、クラスタ内のすべてのLIFのステータスを表示します。

- にアクセスするには、ローカルユーザアカウントを使用する必要があります spi Webサービス、ドメインユーザアカウントはサポートされていません。
- ユーザアカウントに「admin」ロール（へのアクセス権を持つ）がない場合 spi デフォルトではWebサービス）、アクセス制御ロールにへのアクセスが許可されている必要があります spi Webサービス。

。 vservice services web access show コマンドは、どのロールにどのWebサービスへのアクセスが許可されているかを表示します。

- 「admin」ユーザアカウント（を含む）を使用していない場合 http アクセス方法（デフォルトでは）を使用してユーザアカウントを設定する必要があります http アクセス方法。

。 security login show コマンドは、ユーザアカウントのアクセス方法、ログイン方法、およびアクセス制御ロールを表示します。

- セキュアな Web アクセスのために HTTPS を使用する場合は、SSL を有効にし、デジタル証明書をインストールする必要があります。

。 system services web show コマンドは、クラスタレベルのWebプロトコルエンジンの設定を表示します。

このタスクについて

。 spi Webサービスはデフォルトで有効になっており、手動で無効にすることができます (vservice services web modify -vservice \* -name spi -enabled false) 。

「admin」ロールにはへのアクセスが許可されます spi デフォルトではWebサービスで、アクセスは手動で無効にすることができます (services web access delete -vservice cluster\_name -name spi

-role admin)。

手順

1. Webブラウザでを指定します spi 次のいずれかの形式のWebサービスURL。

- `http://cluster-mgmt-LIF/spi/`
- `https://cluster-mgmt-LIF/spi/`

cluster-mgmt-LIF は、クラスタ管理LIFのIPアドレスです。

2. ブラウザにプロンプトが表示されたら、ユーザアカウントとパスワードを入力します。

アカウントが認証されると、へのリンクがブラウザに表示されます /mroot/etc/log/、  
/mroot/etc/crash/`および` /mroot/etc/mib/ クラスタ内の各ノードのディレクトリ。

ノードのシステムコンソールにアクセスします

ブートメニューまたはブート環境のプロンプトでハングしているノードには、システム  
コンソール（*serial console*）経由でのみアクセスできます。ノードのシステムコンソールには、ノードの SP またはクラスタへの SSH 接続からアクセスできます。

このタスクについて

SP と ONTAP はどちらもシステムコンソールにアクセスするためのコマンドを提供しています。ただし、SP からはそのノードのシステムコンソールにしかアクセスできません。クラスタからはクラスタ内の任意のノードのシステムコンソールにアクセスできます。

手順

1. ノードのシステムコンソールにアクセスします。

使用する環境	入力するコマンド
ノードの SP CLI	<code>system console</code>
ONTAP CLI	<code>system node run-console</code>

2. プロンプトが表示されたら、システムコンソールにログインします。

3. システムコンソールを終了するには、Ctrl+D を押します

システムコンソールへのアクセスの例

次の例は、を入力した結果を示しています `system console` 「S P node2」プロンプトでコマンドを実行します。システムコンソールに、node2 がブート環境のプロンプトでハングしていることが示されています。。boot\_ontap コンソールでコマンドを入力してノードをONTAP でブートします。続いて Ctrl+D を押してコンソールを終了し、SP に戻ります。

```
SP node2> system console
Type Ctrl-D to exit.
```

```
LOADER>
LOADER> boot_ontap
...
*****
*                                     *
* Press Ctrl-C for Boot Menu. *
*                                     *
*****
...
```

( Ctrl+D を押してシステムコンソールを終了しています)

```
Connection to 123.12.123.12 closed.
SP node2>
```

次の例は、を入力した結果を示しています system node run-console ノード2（ブート環境のプロンプトでハングしているノード2）のシステムコンソールにアクセスするには、ONTAP からコマンドを実行します。。 boot\_ontap コンソールでコマンドを入力してnode2をONTAP でブートします。続いて Ctrl+D を押してコンソールを終了し、ONTAP に戻ります。

```
cluster1::> system node run-console -node node2
Pressing Ctrl-D will end this session and any further sessions you might
open on top of this session.
Type Ctrl-D to exit.

LOADER>
LOADER> boot_ontap
...
*****
*                                     *
* Press Ctrl-C for Boot Menu. *
*                                     *
*****
...
```

( Ctrl+D を押してシステムコンソールを終了しています)

```
Connection to 123.12.123.12 closed.
cluster1::>
```



ノードのルートボリュームとルートアグリゲートを管理します。

ノードのルートボリュームは、工場出荷時またはセットアップソフトウェアによってインストールされた FlexVol ボリュームです。システムファイル、ログファイル、コアファイル用に予約されています。ディレクトリ名はです `/mroot` にアクセスします。これには、テクニカルサポートがシステムシェルからのみアクセスできます。ノードのルートボリュームの最小サイズは、プラットフォームモデルによって異なります。

ノードのルートボリュームとルートアグリゲートに関するルールの概要

ノードのルートボリュームには、そのノードの特別なディレクトリとファイルが格納されています。ルートボリュームはルートアグリゲートに含まれています。ノードのルートボリュームとルートアグリゲートには、いくつかのルールが適用されます。

- ノードのルートボリュームには次のルールが適用されます。
    - テクニカルサポートから指示がないかぎり、ルートボリュームの構成またはコンテンツを変更しないでください。
    - ユーザーデータはルートボリュームに格納しないでください。
- ユーザーデータをルートボリュームに格納すると、HA ペアのノード間でのストレージのギブバックに時間がかかります。
- ルートボリュームを別のアグリゲートに移動できます。を参照してください [\[relocate-root\]](#)。
- ルートアグリゲートは、ノードのルートボリューム専用になります。

ONTAP では、ルートアグリゲートに他のボリュームを作成することはできません。

## "NetApp Hardware Universe の略"

ノードのルートボリュームのスペースを解放する

ノードのルートボリュームがいっぱい、またはほぼいっぱいになると、警告メッセージが表示されます。ルートボリュームがいっぱいになると、ノードは正常に動作できません。コアダンプファイル、パケットトレースファイル、およびルートボリュームの Snapshot コピーを削除することにより、ノードのルートボリュームのスペースを解放できます。

手順

1. ノードのコアダンプファイルとその名前を表示します。

```
system node coredump show
```

2. 不要なコアダンプファイルをノードから削除します。

```
system node coredump delete
```

3. ノードシェルにアクセスします。

```
system node run -node nodename
```

*nodename* は、ルートボリュームのスペースを解放するノードの名前です。

4. ノードシェルからノードシェルの advanced 権限レベルに切り替えます。

```
priv set advanced
```

5. ノードのパケットトレースファイルは、次のようにノードシェルから表示、削除を行います。
  - a. ノードのルートボリュームにあるすべてのファイルを表示します。

```
ls /etc
```

- b. パケットトレースファイルがある場合 (\*.trc) がノードのルートボリュームに含まれている場合は、個々に削除します。

```
rm /etc/log/packet_traces/file_name.trc
```

6. ノードのルートボリュームの Snapshot コピーは、次のようにノードシェルから特定、および削除を行います。
  - a. ルートボリューム名を特定します。

```
vol status
```

ルートボリュームは、の[Options]列に「root」と表示されます vol status コマンド出力。

次の例では、ルートボリュームは vol0 :

```
node1*> vol status
```

Volume	State	Status	Options
vol0	online	raid_dp, flex 64-bit	root, nvfail=on

- a. ルートボリュームの Snapshot コピーを表示します。

```
snap list root_vol_name
```

- b. 不要なルートボリュームの Snapshot コピーを削除します。

```
snap delete root_vol_namesnapshot_name
```

7. ノードシェルを終了してクラスタシェルに戻ります。

```
exit
```

ルートボリュームを新しいアグリゲートに再配置します

ルート交換手順は、現在のルートアグリゲートをシステム停止なしで別のディスクセットに移行します。

このタスクについて

ルートボリュームを再配置するには、ストレージフェイルオーバーを有効にする必要があります。を使用でき

まず `storage failover modify -node nodename -enable true` フェイルオーバーを有効にするコマンド。

次のシナリオで、ルートボリュームの場所を新しいアグリゲートに変更できます。

- ルートアグリゲートが希望するディスク上にない場合
- ノードに接続されているディスクの配置を変更する場合
- EOS ディスクシェルフを交換する場合

#### 手順

1. 権限レベルを `advanced` に設定します。

```
set privilege advanced
```

2. ルートアグリゲートを再配置します。

```
system node migrate-root -node nodename -disklist disklist -raid-type raid-type
```

- `* -node *`

移行するルートアグリゲートを所有しているノードを指定します。

- `*-disklist *`

新しいルートアグリゲートを作成するディスクのリストを指定します。すべてのディスクはスペアであり、同じノードが所有している必要があります。必要なディスクの最小数は RAID タイプによって異なります。

- `* -raid-type *`

ルートアグリゲートの RAID タイプを指定します。デフォルト値は `raid-dp`。

3. ジョブの進捗状況を監視します。

```
job show -id jobid -instance
```

#### 結果

すべての事前確認が完了すると、ルートボリューム交換ジョブが開始されてコマンドが終了します。ノードが再起動するようにします。

ノードの概要を開始または停止します

メンテナンスやトラブルシューティングの目的で、ノードの起動または停止が必要になる場合があります。ノードの起動または停止は、ONTAP CLI、ブート環境プロンプト、または SP CLI から実行できます。

SP CLI コマンドを使用する `system power off` または `system power cycle` ノードの電源をオフにするか再投入すると原因、ノードが誤ってシャットダウンされる (*dirty shutdown*) ことがあります。この方法は、ONTAP を使用した正常なシャットダウンの代わりにはなりません `system node halt` コマンドを実行

します

システムプロンプトでノードをリブートします

ノードは、システムプロンプトから通常モードでリブートできます。ノードは、PC CompactFlash カードなどのブートデバイスからブートするように構成されています。

手順

1. クラスタのノード数が 4 つ以上の場合は、リブートするノードにイプシロンが設定されていないことを確認します。

- a. 権限レベルを advanced に設定します。

```
set -privilege advanced
```

- b. イプシロンが設定されているノードを特定します。

```
cluster show
```

次の例では 'node1' にイプシロンが設定されています

```
cluster1::*> cluster show
Node              Health  Eligibility  Epsilon
-----
node1              true    true         true
node2              true    true         false
node3              true    true         false
node4              true    true         false
4 entries were displayed.
```

- a. リブートするノードにイプシロンが設定されている場合は、そのノードからイプシロンを削除します。

```
cluster modify -node node_name -epsilon false
```

- b. 稼働したままにする別のノードにイプシロンを割り当てます。

```
cluster modify -node node_name -epsilon true
```

- c. admin 権限レベルに戻ります。

```
set -privilege admin
```

2. を使用します system node reboot コマンドを使用してノードをリブートします。

指定しない場合は、を実行します -skip-lif-migration パラメータを指定すると、リブートの前に、別のノードへのデータおよびクラスタ管理LIFの同期的移行が試行されます。LIF の移行が失敗した場合、またはタイムアウトになった場合、リブートプロセスは中止され、LIF の移行の失敗を示すエラーが ONTAP に表示されます。

```
cluster1::> system node reboot -node node1 -reason "software upgrade"
```

ノードのリブートプロセスが開始されます。ONTAP ログインプロンプトが表示され、リブートプロセスが完了したことが示されます。

ブート環境のプロンプトから **ONTAP** をブートします

ノードのブート環境のプロンプトから、ONTAP の現在のリリースまたはバックアップリリースをブートできます。

#### 手順

1. ストレージシステムプロンプトからを使用して、ブート環境のプロンプトにアクセスします `system node halt` コマンドを実行します

ストレージ・システムのコンソールに、ブート環境のプロンプトが表示されます。

2. ブート環境のプロンプトで、次のいずれかのコマンドを入力します。

ブート対象	入力するコマンド
ONTAP の現在のリリース	<code>boot_ontap</code>
ブートデバイスの ONTAP プライマリイメージ	<code>boot_primary</code>
ブートデバイスの ONTAP バックアップイメージ	<code>boot_backup</code>

使用するイメージが不明な場合は、を使用する必要があります `boot_ontap` 最初の例では。

#### ノードをシャットダウン

ノードが応答しなくなった場合や、サポート担当者からトラブルシューティング対応の一環として実行するように指示された場合は、ノードをシャットダウンできます。

#### 手順

1. クラスタのノード数が 4 つ以上の場合は、シャットダウンするノードにイプシロンが設定されていないことを確認します。

- a. 権限レベルを `advanced` に設定します。

```
set -privilege advanced
```

- b. イプシロンが設定されているノードを特定します。

```
cluster show
```

次の例では 'node1 にイプシロンが設定されています

```
cluster1::*> cluster show
Node           Health Eligibility  Epsilon
-----
node1          true   true        true
node2          true   true        false
node3          true   true        false
node4          true   true        false
4 entries were displayed.
```

- a. シャットダウンするノードにイプシロンが設定されている場合は、そのノードからイプシロンを削除します。

```
cluster modify -node node_name -epsilon false
```

- b. 稼働したままにする別のノードにイプシロンを割り当てます。

```
cluster modify -node node_name -epsilon true
```

- c. admin 権限レベルに戻ります。

```
set -privilege admin
```

2. を使用します `system node halt` コマンドを使用してノードをシャットダウンします。

指定しない場合は、を実行します `-skip-lif-migration` パラメータを指定すると、シャットダウンの前に、別のノードへのデータおよびクラスタ管理LIFの同期的移行が試行されます。LIF の移行が失敗した場合、またはタイムアウトになった場合、シャットダウンプロセスは中止され、ONTAP に LIF の移行の失敗を示すエラーが表示されます。

両方を使用して、シャットダウン時にコアダンプを手動でトリガーすることができます `-dump` パラメータ

次の例は、ハードウェアのメンテナンスのために「node1」という名前のノードをシャットダウンします。

```
cluster1::> system node halt -node node1 -reason 'hardware maintenance'
```

ブートメニューを使用してノードを管理します

ブートメニューを使用して、ノードの構成エラーの修正、管理パスワードのリセット、ディスクの初期化、ノード構成のリセット、ブートデバイスへのノード構成情報のリストアを実行できます。



HA ペアが使用している場合 "SAS ドライブまたは NVMe ドライブの暗号化 (SED、NSE、FIPS)"、の手順に従ってください "FIPS ドライブまたは SED を非保護モードに戻します" システムを初期化する前の HA ペア内のすべてのドライブ (ブートオプション 4 または 9)。そうしないと、ドライブを転用した場合にデータが失われる可能性があります。

手順

1. を使用してノードをリブートし、ブートメニューにアクセスします `system node reboot` コマンドを入力します。

ノードのリブートプロセスが開始されます。

2. リブートプロセス時にブートメニューを表示するよう求められたら、`Ctrl+C` キーを押してブートメニューを表示します。

ノードに次のブートメニューオプションが表示されます。

```
(1) Normal Boot.
(2) Boot without /etc/rc.
(3) Change password.
(4) Clean configuration and initialize all disks.
(5) Maintenance mode boot.
(6) Update flash from backup config.
(7) Install new software first.
(8) Reboot node.
(9) Configure Advanced Drive Partitioning.
(10) Set onboard key management recovery secrets.
(11) Configure node for external key management.
Selection (1-11)?
```



Boot Menu Option (2) Boot without /etc/rc は廃止され、システムには影響しません。

3. 対応する番号を入力して、次のいずれかのオプションを選択します。

目的	選択するオプション
通常モードでノードをブートします	1) 通常の起動
ノードのパスワードを変更しますこれは 'admin' アカウント・パスワードでもあります	3) パスワードを変更します

目的	選択するオプション
<p>ノードのディスクを初期化し、そのノードのルートボリュームを作成する</p>	<p>4) すべてのディスクを消去して初期化します</p> <div data-bbox="673 275 730 331">  </div> <p>このメニューオプションを選択すると、ノードのディスク上のすべてのデータが消去され、ノード構成が工場出荷時のデフォルトの設定にリセットされます。</p> <p>このメニュー項目は、ノードがクラスタから削除され（参加していない）、別のクラスタに参加していない場合にのみ選択してください。</p> <p>内蔵または外付けのディスクシェルフがあるノードの場合は、内蔵ディスク上のルートボリュームが初期化されます。内蔵ディスクシェルフがない場合は、外付けディスク上のルートボリュームが初期化されます。</p> <p>内蔵または外付けディスクシェルフを使用して FlexArray 仮想化を実行しているシステムでは、アレイ LUN が初期化されません。内蔵シェルフまたは外付けシェルフのネイティブディスクがすべて初期化されます。</p> <p>アレイ LUN のみで内蔵または外付けディスクシェルフもない FlexArray 仮想化を実行するシステムの場合、ストレージアレイ LUN 上のルートボリュームが初期化されます。を参照してください <a href="#">"FlexArray をインストールしています"</a>。</p> <p>初期化するノードに、ルートデータのパーティショニング用にパーティショニングされたディスクがある場合、ノードを初期化する前にディスクのパーティショニングを停止しておく必要があります。 （*9）アドバンスドドライブパーティショニングの設定 * およびを参照してください <a href="#">"ディスクとアグリゲートの管理"</a>。</p>
<p>アグリゲート処理およびディスクメンテナンス処理を実行し、アグリゲートおよびディスクに関する詳細情報を取得する</p>	<p>5) メンテナンスモードでブートします</p> <p>メンテナンスモードを終了するには、を使用します <code>halt</code> コマンドを実行します</p>
<p>ノードのルートボリュームから PC CompactFlash カードなどのブートデバイスに構成情報をリストアします</p>	<p>6) バックアップ設定からフラッシュを更新します</p> <p>ONTAP は、一部のノード構成情報をブートデバイスに格納します。ノードがリブートすると、ブートデバイス上の情報がノードのルートボリュームに自動的にバックアップされます。ブートデバイスが壊れたり、交換が必要になった場合は、このメニューオプションを使用して構成情報をノードのルートボリュームからブートデバイスにリストアする必要があります。</p>



目的	選択するオプション
ノードに新しいソフトウェアをインストールします	<p>7) 最初に新しいソフトウェアをインストールします</p> <p>ブートデバイス上の ONTAP ソフトウェアにルートボリュームに使用するストレージレイのサポートが含まれない場合は、このメニューオプションを使用して、ストレージレイをサポートするソフトウェアのバージョンを取得してノードにインストールします。</p> <p>このメニューオプションは、ONTAP ソフトウェアの新しいバージョンを、ルートボリュームがインストールされていないノードにインストールするときのみ使用します。DO_not_ONTAP をアップグレードするには 'このメニュー・オプション' を使用します</p>
ノードをリブートします。	8) ノードをリブートします
すべてのディスクのパーティショニングを解除してディスクの所有権情報を削除するか、設定を消去して、ディスク全体またはパーティショニングされたディスクでシステムを初期化します	<p>9) アドバンスドドライブパーティショニングを設定します</p> <p>ONTAP 9.2 以降では、ルート / データパーティショニングまたはルート / データ / データパーティショニング用に設定されたディスク向けの追加の管理機能として、アドバンスドドライブパーティショニングオプションを使用できます。ブートオプション 9 では、次のオプションを使用できます。</p> <div style="border: 1px solid #ccc; padding: 10px; margin-top: 10px;"> <p>(9a) Unpartition all disks and remove their ownership information.</p> <p>(9b) Clean configuration and initialize system with partitioned disks.</p> <p>(9c) Clean configuration and initialize system with whole disks.</p> <p>(9d) Reboot the node.</p> <p>(9e) Return to main boot menu.</p> </div>

ノード属性を表示します

クラスタ内の 1 つ以上のノードについて、名前、所有者、場所、モデル番号、シリアル番号、ノードの実行時間、健全性状態、クラスタへの参加資格を示します。

手順

1. 指定したノードまたはクラスタ内のすべてのノードに関する属性を表示するには、を使用します `system node show` コマンドを実行します

ノードに関する情報を表示する例

次の例では、node1 に関する詳細な情報が表示されています。

```
cluster1::> system node show -node node1
Node: node1
Owner: Eng IT
Location: Lab 5
Model: model_number
Serial Number: 12345678
Asset Tag: -
Uptime: 23 days 04:42
NVRAM System ID: 118051205
System ID: 0118051205
Vendor: NetApp
Health: true
Eligibility: true
Differentiated Services: false
All-Flash Optimized: true
Capacity Optimized: false
QLC Optimized: false
All-Flash Select Optimized: false
SAS2/SAS3 Mixed Stack Support: none
```

ノード属性を変更します

必要に応じて、ノードの属性を変更できます。変更できる属性は、ノードの所有者情報、場所情報、資産タグ、クラスタへの参加資格です。

このタスクについて

ノードのクラスタへの参加資格は、advanced権限レベルでを使用して変更できます `-eligibility` のパラメータ `system node modify` または `cluster modify` コマンドを実行しますノードの参加資格をに設定した場合 `false` に設定すると、ノードはクラスタ内で非アクティブになります。



ノードの参加資格をローカルで変更することはできません。別のノードから変更する必要があります。クラスタ HA 構成でノード委譲を変更することもできません。



ノードの参加資格には設定しないでください `false` (ノード設定のリストアやノードのメンテナンスが長引いている場合などを除く)。ノードにクラスタ参加資格がないと、そのノードへの SAN および NAS のデータアクセスが影響を受ける可能性があります。

手順

1. を使用します `system node modify` ノードの属性を変更するコマンド。

ノード属性を変更する例

次のコマンドでは、「node1」ノードの属性を変更します。ノードの所有者は「ジョー・スミス」に設定され、その資産タグは「js1234」に設定されています。

```
cluster1::> system node modify -node node1 -owner "Joe Smith" -assettag js1234
```

ノードの名前を変更します

ノード名は必要に応じて変更できます。

手順

1. ノードの名前を変更するには、を使用します `system node rename` コマンドを実行します

。 `-newname` パラメータには、ノードの新しい名前を指定します。。 `system node rename` のマニュアルページで、ノード名の指定に関するルールについて説明します。

クラスタ内の複数のノードの名前を変更する場合は、ノードごとにこのコマンドを実行する必要があります。



「all」はシステム予約名なので、ノード名を「all」にすることはできません。

ノード名の変更例

次のコマンドでは、ノード名を "node1" から "node1a" に変更します

```
cluster1::> system node rename -node node1 -newname node1a
```

シングルノードクラスタを管理します。

シングルノードクラスタは、スタンドアロンノード上でクラスタを実行する特殊な実装です。シングルノードクラスタは冗長性を提供しないため、推奨されません。ノードが停止すると、データアクセスが失われます。



フォールトトレランスとノンストップオペレーションを実現するためには、["ハイアベイラビリティ \(HAペア\)"](#)。

シングルノードクラスタを構成またはアップグレードする場合は、次の点に注意してください。

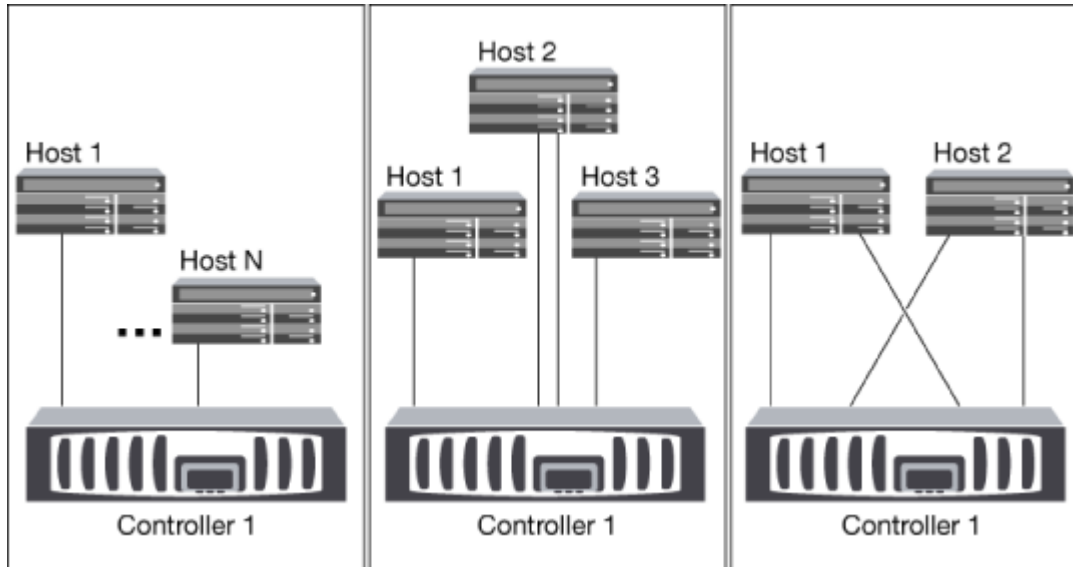
- シングルノードクラスタではルートボリュームの暗号化はサポートされません。
- ノードを削除してシングルノードクラスタにする場合は、データトラフィックを処理するようにクラスタポートを変更する必要があります。そのためには、クラスタポートがデータポートになるように変更し、そのデータポートにデータLIFを作成します。
- シングルノードクラスタの場合は、ソフトウェアのセットアップ時に構成のバックアップ先を指定できます。セットアップ後は、ONTAP コマンドを使用して設定を変更できます。
- ノードに接続するホストが複数ある場合は、各ホストでオペレーティングシステム（WindowsやLinuxなど）を設定できます。ホストからコントローラへのパスが複数ある場合は、ホストでALUAを有効にする必要があります。

## シングルノードを使用する iSCSI SAN ホストの構成方法

iSCSI SANホストは、単一のノードに直接接続するように設定することも、1つ以上のIPスイッチを介して接続するように設定することもできます。ノードからスイッチに複数のiSCSI接続を確立できます。

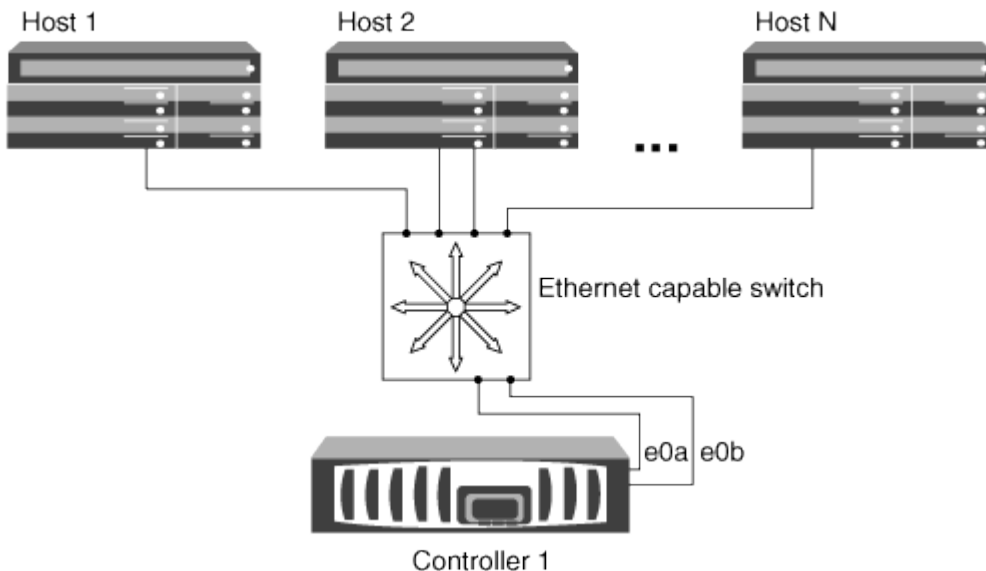
### 直接接続型のシングルノード構成

直接接続型のシングルノード構成では、1つ以上のホストをノードに直接接続します。



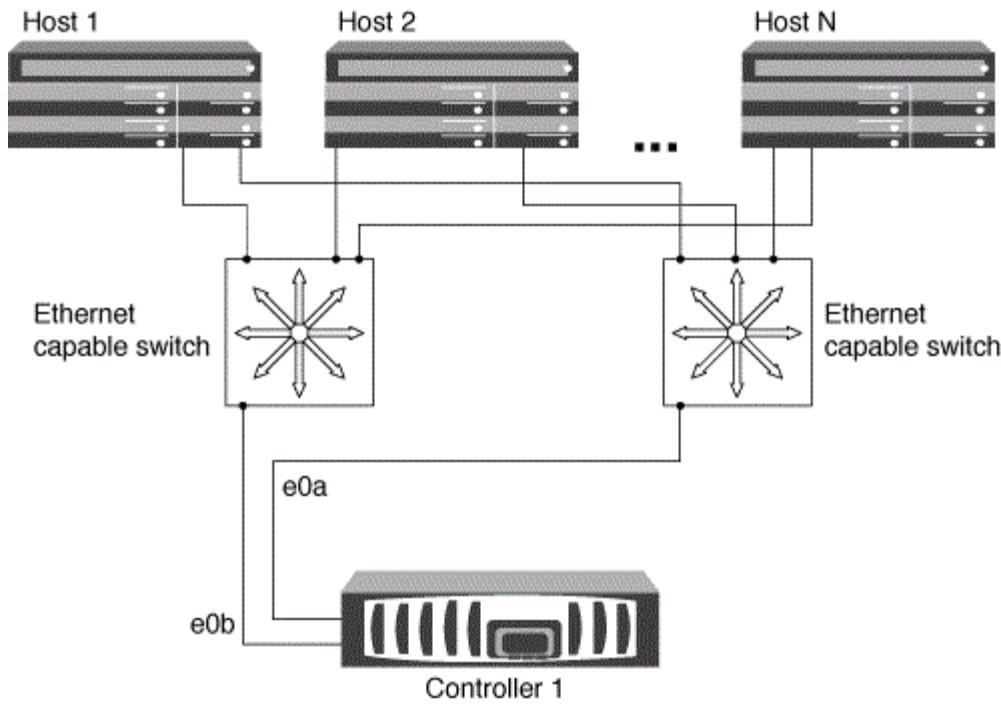
### シングルネットワークのシングルノード構成

シングルネットワークのシングルノード構成では、1つのノードを1台のスイッチで1つまたは複数のホストに接続します。スイッチが1台しかないため、この構成では完全な冗長性は確保されません。



### マルチネットワークのシングルノード構成

マルチネットワークのシングルノード構成では、1つのノードを複数のスイッチで1つまたは複数のホストに接続します。スイッチが複数あるため、この構成では完全な冗長性が確保されます。



#### シングルノードを使用する FC および FC-NVMe SAN ホストの構成方法

シングルノードの FC および FC-NVMe SAN ホストは、1 つ以上のファブリック経由で接続するように構成できます。N-Port ID Virtualization（NPIV；N ポート ID 仮想化）が必要で、ファブリック内のすべての FC スイッチで有効にする必要があります。FC または FC-NVMe SAN ホストを FC スイッチを使用せずにシングルノードに直接接続することはできません。

#### 単一ファブリックのシングルノード構成

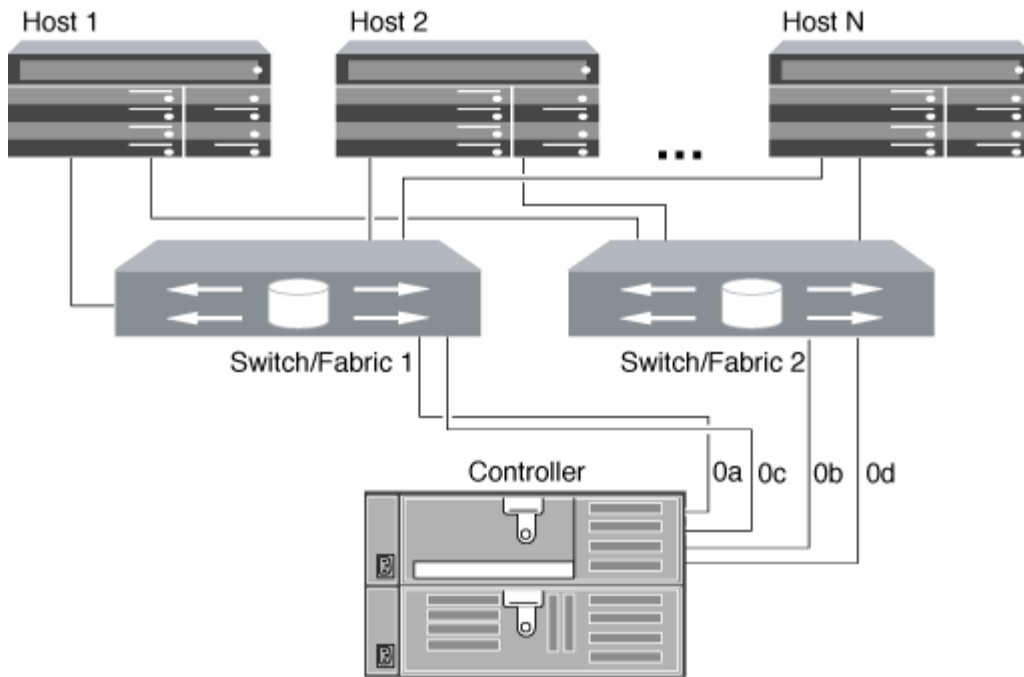
単一ファブリックのシングルノード構成では、1 つのノードを 1 台のスイッチで 1 つまたは複数のホストに接続します。スイッチが 1 台しかないため、この構成では完全な冗長性は確保されません。

単一ファブリックのシングルノード構成では、ホストからノードへのパスが 1 つしかない場合、マルチパスソフトウェアは必要ありません。

#### マルチファブリックのシングルノード構成

マルチファブリックのシングルノード構成では、1 つのノードを複数のスイッチで 1 つまたは複数のホストに接続します。次の図は、マルチファブリックのシングルノード構成を示しています。わかりやすいように、この図ではファブリックが 2 つだけになっていますが、マルチファブリック構成は 2 つ以上の任意の数のファブリックで構成できます。この図では、上のシャーシにストレージコントローラが取り付けられています。下のシャーシは、この例のように空けておくか、IOMX モジュールを使用したりできます。

次の図の FC ターゲットポート（0a、0c、0b、0d）は一例です。実際のポート番号は、使用しているストレージノードのモデル、および拡張アダプタを使用しているかどうかによって異なります。



## 関連情報

"[NetAppテクニカルレポート4684](#)：『Implementing and Configuring Modern SANs with NVMe-oF』"

## シングルノードクラスタでのONTAPのアップグレード

ONTAP 9.2以降では、ONTAP CLIを使用してシングルノードクラスタの自動更新を実行できます。シングルノードクラスタは冗長性に欠けるため、更新時は必ずシステムの停止を伴います。停止を伴うアップグレードは、System Managerでは実行できません。

作業を開始する前に

アップグレードを完了する必要があります "[準備](#)" 手順。

## 手順

1. 以前の ONTAP ソフトウェアパッケージを削除します。

```
cluster image package delete -version previous_package_version
```

2. ターゲットの ONTAP ソフトウェアパッケージをダウンロードします。

```
cluster image package get -url location
```

```
cluster1::> cluster image package get -url  
http://www.example.com/software/9.7/image.tgz
```

```
Package download completed.  
Package processing completed.
```

3. ソフトウェアパッケージがクラスタパッケージリポジトリにあることを確認します。

```
cluster image package show-repository
```

```
cluster1::> cluster image package show-repository
Package Version  Package Build Time
-----
9.7              M/DD/YYYY 10:32:15
```

4. クラスタをアップグレードする準備が完了していることを確認します。

```
cluster image validate -version package_version_number
```

```
cluster1::> cluster image validate -version 9.7
```

```
WARNING: There are additional manual upgrade validation checks that must
be performed after these automated validation checks have completed...
```

5. 検証の進捗を監視します。

```
cluster image show-update-progress
```

6. 検証で特定された必要なアクションをすべて完了します。
7. 必要に応じて、ソフトウェアアップグレードの見積もりを生成します。

```
cluster image update -version package_version_number -estimate-only
```

ソフトウェアアップグレードの見積もりには、更新対象の各コンポーネントの詳細とアップグレードの推定期間が表示されます。

8. ソフトウェアのアップグレードを実行します。

```
cluster image update -version package_version_number
```



問題が検出されると、更新が一時停止し、措置を講じるように求められます。問題の詳細や更新の進捗を確認するには、`cluster image show-update-progress` コマンドを使用します。問題を修正したら、`cluster image resume-update` コマンドを使用して更新を再開できます。

9. クラスタの更新の進捗を表示します。

```
cluster image show-update-progress
```

ノードは更新の一環としてリブートされ、リブート中はアクセスできません。

10. 通知をトリガーします。

```
autosupport invoke -node * -type all -message "Finishing_Upgrade"
```

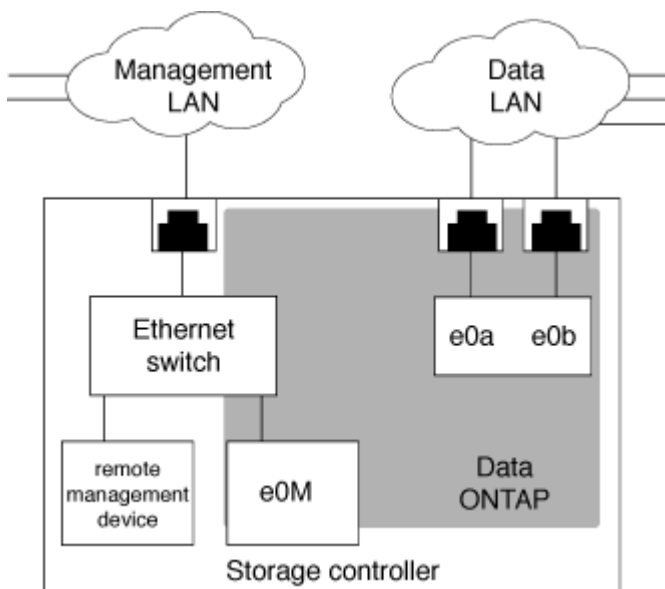
メッセージを送信するようにクラスタが設定されていない場合は、通知のコピーがローカルに保存されます。

## SP / BMC ネットワークを設定する

管理ネットワークトラフィックを分離します

SP / BMC と e0M 管理インターフェイスは、管理トラフィック専用のサブネット上に設定することを推奨します。管理ネットワーク上でデータトラフィックを実行すると、原因のパフォーマンスの低下やルーティングの問題が発生する可能性があります。

ほとんどのストレージコントローラの管理イーサネットポート（シャーシ背面にあるレンチマークの付いたポート）は、内部イーサネットスイッチに接続されます。内部スイッチは、SP / BMC および e0M 管理インターフェイスへの接続を提供します。これらを使用して、Telnet、SSH、SNMP などの TCP/IP プロトコル経由でストレージシステムにアクセスできます。



リモート管理デバイスと e0M の両方を使用する場合は、同じ IP サブネット上に設定する必要があります。これらは低帯域幅のインターフェイスであるため、SP / BMC と e0M は管理トラフィック専用のサブネット上に設定することを推奨します。

管理トラフィックを分離できない場合や、専用の管理ネットワークの規模が非常に大きい場合は、ネットワー



クトラフィックをできるだけ少なく抑える必要があります。イングレスブロードキャストまたはマルチキャストトラフィックが大量になると、SP / BMC のパフォーマンスが低下する可能性があります。



AFF A800 などの一部のストレージコントローラには、外部ポートが2つあります。1つはBMC用、もう1つはe0M用です。これらのコントローラの場合、BMCとe0Mを同じIPサブネット上に設定する必要はありません。

## SP / BMC ネットワーク設定に関する考慮事項

SP に対してクラスタレベルの自動ネットワーク設定を有効にできます（推奨）。SP の自動ネットワーク設定を無効なままにし（デフォルト）、SP ネットワーク設定をノードレベルで手動で管理することもできます。それぞれのケースについて、いくつかの考慮事項があります。



このトピック環境では、SP と BMC の両方について説明します。

SP の自動ネットワーク設定を有効にすると、指定したサブネットのアドレスリソース（IP アドレス、サブネットマスク、ゲートウェイアドレスなど）を使用してネットワークが自動的にセットアップされます。SP の自動ネットワーク設定を使用すると、各ノードの SP に IP アドレスを手動で割り当てる必要がなくなります。SP の自動ネットワーク設定を有効にするには、まず設定に使用するサブネットが先にクラスタに定義されている必要があるため、デフォルトでは、自動ネットワーク設定は無効になっています。

SP の自動ネットワーク設定を有効にした場合、次のシナリオと考慮事項が該当します。

- これまでに一度も SP が設定されていない場合、SP ネットワークは、SP の自動ネットワーク設定に指定したサブネットに基づいて自動的に設定されます。
- 以前に SP が手動で設定されている場合、または別のサブネットに基づく既存の SP ネットワーク設定がある場合、クラスタ内のすべてのノードの SP ネットワークが、SP の自動ネットワーク設定で指定したサブネットに基づいて再設定されます。

再設定によって SP に別のアドレスが割り当てられると、DNS 設定に影響し、SP のホスト名を解決できなくなる可能性があります。そのため、DNS 設定の更新が必要になる場合があります。

- クラスタに参加するノードには、指定したサブネットを使用して SP ネットワークが自動的に設定されます。
- `system service-processor network modify` コマンドを使用して SP IP アドレスを変更することはできません。

SP 自動ネットワーク設定が有効になっている場合、このコマンドで実行できるのは SP ネットワークインターフェ이스の有効化または無効化のみです。

- SP の自動ネットワーク設定が以前に有効になっていた場合、SP ネットワークインターフェ이스を無効にすると、割り当てられたアドレスリソースが解放されてサブネットに戻されます。
- SP ネットワークインターフェ이스を無効にし、その後再度有効にすると、SP は別のアドレスで再設定されることがあります。

SP の自動ネットワーク設定を無効にした場合（デフォルト）、次のシナリオと考慮事項が該当します。

- これまでに一度も SP が設定されていない場合、SP IPv4 ネットワーク設定は、IPv4 DHCP を使用するデフォルトの設定になり、IPv6 は無効になります。

クラスタに参加するノードの SP ネットワーク設定も、デフォルトで IPv4 DHCP に設定されます。

- 。 `system service-processor network modify` コマンドを使用して、ノードの SP IP アドレスを設定できます。

サブネットに割り当てられているアドレスを使用して SP ネットワークを手動で設定しようとする、警告メッセージが表示されます。警告を無視して手動でのアドレス割り当てを続行すると、重複するアドレスが割り当てられる可能性があります。

一度有効にした SP の自動ネットワーク設定を無効にした場合、次のシナリオと考慮事項が該当します。

- SP の自動ネットワーク設定で IPv4 アドレスファミリーが無効になっている場合、SP IPv4 ネットワークは DHCP を使用するデフォルトの設定になります `system service-processor network modify` コマンドを使用すると、個々のノードの SP IPv4 設定を変更できます。
- SP の自動ネットワーク設定で IPv6 アドレスファミリーが無効になっている場合、SP IPv6 ネットワークも無効になります `system service-processor network modify` コマンドを使用すると、個々のノードの SP IPv6 設定を有効にしたり変更したりできます。

### SP / BMC の自動ネットワーク設定を有効にします

SP ネットワークを手動で設定するよりも、自動ネットワーク設定を使用するように SP を設定することを推奨します。SP ネットワークの自動設定はクラスタ全体が対象なので、個々のノードの SP ネットワークを手動で管理する必要がありません。



このタスクでは、SP と BMC の両方を環境に設定します。

- SP 自動ネットワーク設定には、クラスタ内に定義済みで、SP ネットワークインターフェイスとリソースが競合しないサブネットを使用する必要があります。

。 `network subnet show` コマンドは、クラスタのサブネット情報を表示します。

サブネットの関連付けを強制するパラメータ（`-force-update-lif-associations` のパラメータ `network subnet` コマンド）はネットワーク LIF でのみサポートされ、SP ネットワークインターフェイスではサポートされません。

- SP に IPv6 接続を設定する場合、ONTAP に対して IPv6 が設定済みで、有効になっている必要があります。

。 `network options ipv6 show` コマンドは、ONTAP の IPv6 設定の現在の状態を表示します。

### 手順

1. を使用して、SP で使用するサブネットの IPv4 または IPv6 アドレスファミリーと名前を指定します `system service-processor network auto-configuration enable` コマンドを実行します
2. を使用して、SP の自動ネットワーク設定を表示します `system service-processor network auto-configuration show` コマンドを実行します
3. その後クォーラム内のすべてのノードに対して SP IPv4 または IPv6 ネットワークインターフェイスを無効または再度有効にする場合は、を使用します `system service-processor network modify` コマンドにを指定します `-address-family [IPv4|IPv6]` および `-enable [true|false]` パラメータを指定します。

SP 自動ネットワーク設定が有効になっている場合、クォーラム内のノードの SP IP アドレスを変更することはできません。実行できるのは、SP IPv4 または IPv6 ネットワークインターフェイスの有効化または無効化だけです。

ノードがクォーラムのメンバーでない場合は、を実行して、SPのIPアドレスを含むノードのSPネットワーク設定を変更できます `system service-processor network modify` ノードから、およびノードのSP自動ネットワーク設定を上書きすることを確認します。ただし、ノードがクォーラムに参加すると、指定したサブネットに基づいてノードに対して SP の自動再設定が実行されます。

## SP / BMC ネットワークを手動で設定する

SP に自動ネットワーク設定が設定されていない場合、IP アドレスを使用して SP にアクセスできるように、ノードの SP ネットワークを手動で設定する必要があります。

### 必要なもの

SP に IPv6 接続を設定する場合、ONTAP に対して IPv6 が設定済みで、有効になっている必要があります。。 `network options ipv6` コマンドは、ONTAP のIPv6設定を管理します。



このタスクでは、SP と BMC の両方を環境に設定します。

SP は、IPv4、IPv6、またはその両方を使用するように設定できます。SP の IPv4 設定では静的アドレス指定と DHCP アドレス指定をサポートし、SP の IPv6 設定では静的アドレス指定のみをサポートしています。

SPネットワークの自動設定が設定されている場合は、個々のノードおよびのSPネットワークを手動で設定する必要はありません `system service-processor network modify` コマンドで実行できるのは、SP ネットワークインターフェイスの有効化と無効化のみです。

### 手順

1. を使用して、ノードのSPネットワークを設定します `system service-processor network modify` コマンドを実行します

- 。 `-address-family` パラメータは、SPのIPv4とIPv6のどちらの設定を変更するかを指定します。
- 。 `-enable` パラメータは、指定したIPアドレスファミリーのネットワークインターフェイスを有効にします。
- 。 `-dhcp` パラメータは、DHCPサーバのネットワーク設定を使用するか、指定したネットワークアドレスを使用するかを指定します。

DHCPを有効にするには、を設定します `-dhcp` 終了： v4) IPv4を使用している場合のみ。IPv6 設定の場合、DHCP を有効にすることはできません。

- 。 `-ip-address` パラメータには、SPのパブリックIPアドレスを指定します。

サブネットに割り当てられているアドレスを使用して SP ネットワークを手動で設定しようとする、警告メッセージが表示されます。警告を無視して手動でのアドレス割り当てを続行すると、重複するアドレスが割り当てられる可能性があります。

- 。 `-netmask` パラメータは、SPのネットマスクを指定します (IPv4を使用している場合)。
- 。 `-prefix-length` パラメータは、SPのサブネットマスクのネットワークプレフィックス長を指定します (IPv6を使用している場合)。

°。 -gateway パラメータには、SPのゲートウェイIPアドレスを指定します。

2. 手順 1 を繰り返して、クラスタ内の残りのノードの SP ネットワークを設定します。
3. を使用してSPネットワーク設定を表示し、SPのセットアップステータスを確認します `system service-processor network show` コマンドにを指定します `-instance` または `-field setup-status` パラメータ

ノードの SP のセットアップステータスは、次のいずれかになります。

- ° `not-setup` --設定されていません
- ° `succeeded` --設定に成功しました
- ° `in-progress` --設定が進行中です
- ° `failed` --設定に失敗しました

### SPネットワークの設定例

次の例では、ノードの SP を設定して IPv4 を使用し、SP を有効化してから SP ネットワーク設定を表示して設定内容を確認します。

```

cluster1::> system service-processor network modify -node local
-address-family IPv4 -enable true -ip-address 192.168.123.98
-netmask 255.255.255.0 -gateway 192.168.123.1

cluster1::> system service-processor network show -instance -node local

Node: node1
Address Type: IPv4
Interface Enabled: true
Type of Device: SP
Status: online
Link Status: up
DHCP Status: none
IP Address: 192.168.123.98
MAC Address: ab:cd:ef:fe:ed:02
Netmask: 255.255.255.0
Prefix Length of Subnet Mask: -
Router Assigned IP Address: -
Link Local IP Address: -
Gateway IP Address: 192.168.123.1
Time Last Updated: Thu Apr 10 17:02:13 UTC 2014
Subnet Name: -
Enable IPv6 Router Assigned Address: -
SP Network Setup Status: succeeded
SP Network Setup Failure Reason: -

1 entries were displayed.

cluster1::>

```

## SP API サービス設定を変更する

SP API は、ONTAP がネットワークを介して SP と通信できるようにするセキュアなネットワーク API です。SP API サービスで使用するポートを変更したり、サービスが内部通信に使用する証明書を更新したり、サービス全体を無効にしたりできます。設定の変更が必要になることはほとんどありません。

このタスクについて

- SP API サービスはポートを使用します 50000 デフォルトでは

ポートの値は、たとえばネットワーク設定で port を使用している場合に変更できます 50000 は、別のネットワークアプリケーションによる通信に使用されます。また、他のアプリケーションからのトラフィックと SP API サービスによって生成されるトラフィックを区別する場合にも使用されます。

- SP API サービスが使用する SSL 証明書および SSH 証明書は、クラスタ内専用であり、外部に配布されることはありません。

証明書のセキュリティが侵害されることはほとんどありませんが、侵害された場合には証明書を更新できます。

- SP API サービスは、デフォルトで有効になっています。

SP API サービスを無効にする必要があるのは、SP が設定または使用されていないプライベート LAN でサービスを無効にする場合など、例外的な場合だけです。

SP API サービスを無効にすると、API は着信接続を受け付けません。また、ネットワーク・ベースの SP ファームウェア・アップデートやネットワーク・ベースの SP ログ収集などの機能は使用できなくなり、システムはシリアルインターフェイスの使用に切り替わります。

## 手順

1. を使用してadvanced権限レベルに切り替えます `set -privilege advanced` コマンドを実行します
2. SP API サービス設定を変更します。

状況	使用するコマンド
SP API サービスで使用するポートを変更する	<code>system service-processor api-service modify</code> を使用 <code>-port {49152..65535}</code> パラメータ
SP API サービスの内部通信に使用される SSL 証明書および SSH 証明書を更新する	<ul style="list-style-type: none"><li>• ONTAP 9.5以降で使用 <code>system service-processor api-service renew-internal-certificate</code></li><li>• ONTAP 9.4 以前で使用</li><li>• <code>system service-processor api-service renew-certificates</code></li></ul> <p>パラメータを指定しない場合は、ホスト証明書（クライアント証明書とサーバ証明書を含む）のみが更新されます。</p> <p>状況に応じて <code>-renew-all true</code> パラメータを指定すると、ホスト証明書とルートCA証明書の両方が更新されます。</p>
連絡手段	
SP API サービスを無効または再度有効にします	<code>system service-processor api-service modify</code> を使用 <code>-is-enabled {true}</code>

3. を使用して、SP APIサービス設定を表示します `system service-processor api-service show` コマンドを実行します

## SP / BMCを使用したノードのリモート管理

SP / BMC の概要を使用して、ノードをリモートから管理する

ノードをリモートから管理するには、Service Processor（SP；サービスプロセッサ）または Baseboard Management Controller（BMC；ベースボード管理コントローラ）と呼ばれるオンボードコントローラを使用します。このリモート管理コントローラは、現在のすべてのプラットフォームモデルに含まれています。コントローラは、ノードの動作状態に関係なく、継続して機能します。

次のプラットフォームは、SP ではなく BMC をサポートしています。

- FAS 8700
- FAS 8300
- FAS27x0
- AFF A800
- AFF A700s
- AFF A400
- AFF A320
- AFF A220の略
- AFF C190の略

### SP について

サービスプロセッサ（SP）は、ノードに対するアクセス、監視、およびトラブルシューティングをリモートから行うことができるリモート管理デバイスです。

SP の主な機能は次のとおりです。

- SP を使用すると、ノードコントローラの状態に関係なく、ノードにリモートからアクセスして、ノードの診断、シャットダウン、電源の再投入、リブートを実行できます。

SP はスタンバイ電圧で動作するため、少なくとも 1 つのノード電源装置から電力が供給されていれば使用可能です。

SP にログインするには、管理ホストから Secure Shell クライアントアプリケーションを使用します。ログインすると、SP CLI を使用して、リモートからノードの監視とトラブルシューティングを行うことができます。さらに、SP を使用してシリアルコンソールにアクセスし、リモートから ONTAP コマンドを実行できます。

SP にはシリアルコンソールからアクセスでき、また SP からシリアルコンソールにアクセスすることもできます。SP では、SP CLI セッションと別のコンソールセッションを両方同時に開くことができます。

たとえば、温度センサーで異常な高温または低温が検知されると、ONTAP のトリガーによって、SP がマザーボードを正常にシャットダウンします。シリアルコンソールが応答しなくなりますが、コンソールで Ctrl+G を押して SP CLI にアクセスすることができます。その後、を使用できます `system power on` または `system power cycle` SP からコマンドを実行して、ノードの電源をオンまたは再投入します。

- SP によって環境センサーが監視され、イベントがログに記録されるため、タイムリーで効果的なサービスアクションを実施できます。

SP は、ノードの温度、電圧、電流、ファン速度などの環境センサーを監視します。環境センサーが異常な状態になると、SP は異常な測定値をログに記録し、ONTAP に問題を通知します。また SP は、ノードが AutoSupport メッセージを送信できるかどうかに関係なく、AutoSupport メッセージを通じて必要に応じてアラートおよび「自身のシステム」通知を送信します。

さらに、ブートの進行、Field Replaceable Unit（FRU；フィールド交換可能ユニット）の交換、ONTAP が生成するイベント、SP のコマンド履歴といったイベントについてもログに記録します。AutoSupport メッセージを手動で起動し、指定したノードから収集された SP ログファイルを含めることができます。

SP は、停止したノードの代わりにこれらのメッセージを生成し、AutoSupport メッセージに追加の診断情報を添付する以外には、AutoSupport 機能にまったく影響を及ぼしません。AutoSupport の設定値やメッセージ内容は、ONTAP から継承されます。



SP はに依存しません `-transport` のパラメータ設定 `system node autosupport modify` 通知を送信するコマンド。SP は Simple Mail Transport Protocol（SMTP）のみを使用し、メールホストの情報を含めるためにホストの AutoSupport 設定を必要とします。

SNMP が有効になっている場合、SP は SNMP トラップを生成して、すべての「独自のシステム」イベントに対するトラップホストを設定します。

- SP には、System Event Log（SEL；システムイベントログ）に最大 4、000 のイベントを格納できる不揮発性メモリバッファがあるため、問題の診断に役立ちます。

SEL には、各監査ログエントリが監査イベントとして格納されます。SP のオンボードフラッシュメモリに格納されています。SEL のイベントリストは、SP によって、指定された受信者に AutoSupport メッセージを通じて自動的に送信されます。

SEL には次の情報が含まれています。

- SP によって検出されたハードウェアイベント。たとえば、電源装置、電圧、またはその他のコンポーネントに関するセンサーのステータスなどです
- SP が検出したエラー：通信エラー、ファンの障害、メモリまたは CPU のエラーなど
- ノードが SP に送信した重大なソフトウェアイベント。たとえば、パニック、通信障害、ブート障害、SP の発行の結果としてユーザがトリガーした「自己のシステム」など `system reset` または `system power cycle` コマンドを実行します
- SP は、管理者によるコンソールログインまたはコンソール接続の有無にかかわらず、シリアルコンソールを監視します。

コンソールにメッセージが送信されると、SP はメッセージをコンソールログに格納します。ノードのいずれかの電源装置から SP に給電されていれば、コンソールログの機能は維持されます。SP はスタンバイ電源で動作するので、ノードの電源再投入時または電源オフ時にも使用可能です。

- SP が設定されている場合、ハードウェアアシストテイクオーバーが可能です。
- SP API サービスを使用すると、ONTAP と SP がネットワーク経由で通信できます。

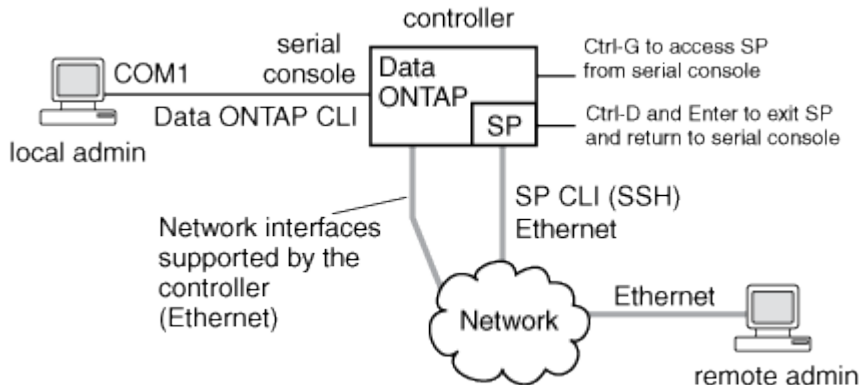
このサービスは、SP ファームウェアの更新にネットワークインターフェイスを使用する、ノードが別の



ノードの SP 機能やシステムコンソールにアクセスできるようにする、別のノードから SP ログをアップロードする、などのネットワークベースの機能をサポートすることで、SP の ONTAP 管理を強化します。

SP API サービスの設定を変更するには、サービスで使用するポートを変更し、サービスで内部の通信に使用する SSL 証明書と SSH 証明書を更新するか、サービス全体を無効にします。

次の図は、ONTAP およびノードの SP へのアクセスを示しています。SP インターフェイスは、イーサネットポート（シャーシ背面にあるレンチマークの付いたポート）経由でアクセスされます。



#### ベースボード管理コントローラの機能

ONTAP 9.1 以降では、特定のハードウェアプラットフォームで、Baseboard Management Controller（BMC；ベースボード管理コントローラ）と呼ばれる新しいオンボードコントローラをサポートするようにソフトウェアがカスタマイズされています。BMC には、デバイスのリモート管理に使用できるコマンドラインインターフェイス（CLI）コマンドが用意されています。

BMC は、サービスプロセッサ（SP）と同じように機能し、同じコマンドを多数使用します。BMC では次の操作を実行できます。

- BMC のネットワーク設定を構成します。
- ノードにリモートからアクセスし、ノードの診断、シャットダウン、電源の再投入、リブートなどのノード管理タスクを実行する。

SP と BMC には、次のようないくつかの違いがあります。

- BMC は、環境全体の電源装置要素、冷却要素、温度センサー、電圧センサー、および電流センサーの監視を制御します。センサー情報は IPMI を介して ONTAP にレポートされます。
- ハイアベイラビリティ（HA）とストレージの一部のコマンドが異なります。
- BMC は AutoSupport メッセージを送信しません。

ONTAP 9.2 GA 以降を実行している場合は、次の要件に従って自動ファームウェア更新も利用できます。

- BMC ファームウェアリビジョン 1.15 以降がインストールされている必要があります。



BMC ファームウェア 1.12 から 1.15 以降にアップグレードするときは手動で更新する必要があります。

- ファームウェアの更新が完了すると BMC が自動的にリブートします。



BMC のリブートがノードの操作に影響することはありません。

## SP / BMC ファームウェアの更新の管理方法

ONTAP には、\_baseline image\_ という SP ファームウェアイメージが含まれています。新しいバージョンの SP ファームウェアがリリースされたときは、そのファームウェアをダウンロードして SP ファームウェアを更新できます。ONTAP のバージョンをアップグレードする必要はありません。



このトピック環境では、SP と BMC の両方について説明します。

ONTAP では、次の方法で SP ファームウェアの更新を管理できます。

- SP 自動更新機能がデフォルトで有効になっており、次のシナリオで SP ファームウェアを自動的に更新できます。
  - 新しいバージョンの ONTAP にアップグレードする場合

ONTAP にバンドルされている SP ファームウェアのバージョンがノードで実行されている SP ファームウェアのバージョンよりも新しい場合、ONTAP のアップグレードプロセスには、SP ファームウェアの更新が自動的に含まれます。



ONTAP は、失敗した SP 自動更新を検出し、修正アクションをトリガーして、SP 自動更新を最大 3 回試行します。3回の再試行がすべて失敗した場合は、ナレッジベースのリンク「[https://kb.netapp.com/Advice\\_and\\_Troubleshooting/Data\\_Storage\\_Software/ONTAP\\_OS/Health\\_Monitor\\_SPAutoUpgradeFailedMajorAlert\\_SP\\_upgrade\\_fails\\_-\\_AutoSupport\\_Message\[HealthモニタSPAutoUpgradeFailedMajorAlert SPアップグレード失敗-AutoSupportメッセージ\]](https://kb.netapp.com/Advice_and_Troubleshooting/Data_Storage_Software/ONTAP_OS/Health_Monitor_SPAutoUpgradeFailedMajorAlert_SP_upgrade_fails_-_AutoSupport_Message[HealthモニタSPAutoUpgradeFailedMajorAlert SPアップグレード失敗-AutoSupportメッセージ])」を参照してください。

- NetApp Support Siteからダウンロードした SP ファームウェアのバージョンが、現在実行している SP ファームウェアのバージョンよりも新しい場合
- ONTAP を以前のバージョンにダウングレードまたはリバートする場合

SP ファームウェアは、リバートまたはダウングレード後の ONTAP のバージョンでサポートされている最新の互換バージョンに自動的に更新されます。SP ファームウェアを手動で更新する必要はありません。

を使用して、SP自動更新機能を無効にすることができます `system service-processor image modify` コマンドを実行しますただし、この機能は有効にしておくことを推奨します。この機能を無効にすると、ONTAP イメージと SP ファームウェアイメージが、未認定の最適ではない組み合わせとなります。

- ONTAP を使用すると、SP更新を手動でトリガーし、を使用して更新の実行方法を指定できます `system`

service-processor image update コマンドを実行します

次のオプションを指定できます。

- 使用するSPファームウェアパッケージ (-package)

パッケージファイル名を指定することで、ダウンロードする SP ファームウェアを更新できます。前進だ system image package show コマンドは、ノードで使用可能なすべてのパッケージファイル (SPファームウェアパッケージのファイルを含む) を表示します。

- SP更新にベースラインSPファームウェアパッケージを使用するかどうか (-baseline)

SP ファームウェアを、現在実行しているバージョンの ONTAP に付属しているベースラインのバージョンに更新できます。



より高度な更新オプションやパラメータを使用すると、BMC の構成設定が一時的にクリアされる場合があります。リブート後、ONTAP で BMC の設定がリストアされるまでに最大 10 分かかることがあります。

- ONTAP では、を使用して、ONTAP からトリガーされた最新のSPファームウェア更新のステータスを表示できます system service-processor image update-progress show コマンドを実行します

SP への既存の接続は、SP ファームウェアを更新するときに切断されます。これは、SP ファームウェア更新が自動的にまたは手動で開始される場合に該当します。

#### 関連情報

["ネットアップのダウンロード：システムファームウェアおよび診断"](#)

**SP / BMC** がネットワークインターフェイスを使用してファームウェアを更新する場合

バージョン 1.5、2.5、3.1、またはそれ以降の SP を搭載した ONTAP から実行される SP ファームウェアの更新では、SP ネットワークインターフェイス経由の IP ベースのファイル転送メカニズムの使用がサポートされます。



このトピック環境では、SP と BMC の両方について説明します。

ネットワークインターフェイス経由の SP ファームウェアの更新は、シリアルインターフェイス経由の更新よりも高速です。そのため、SP ファームウェアを更新中のメンテナンス時間が短縮され、ONTAP の処理が停止されることもありません。この機能をサポートするバージョンの SP は、ONTAP に含まれています。また、これらの SP を NetApp Support Site から入手して、互換性のあるバージョンの ONTAP を実行しているコントローラにインストールすることもできます。

SP バージョン 1.5、2.5、3.1 以降を実行している場合、ファームウェアのアップグレードは次のように動作します。

- ONTAP によって自動でトリガーされる SP ファームウェア更新では、デフォルトでネットワークインターフェイスが使用されます。ただし、次のいずれかの条件に該当する場合、SP 自動更新はシリアルインターフェイス経由に切り替わります。
  - SP ネットワークインターフェイスが設定されていないか、使用できません。

- IP ベースのファイル転送に失敗する。
- SP API サービスが無効になっている。

SP CLI からトリガーされる SP ファームウェア更新では、実行している SP のバージョンに関係なく、常に SP ネットワークインターフェイスが使用されます。

## 関連情報

["ネットアップのダウンロード：システムファームウェアおよび診断"](#)

## SP にアクセスできるアカウント

SP にアクセスする際には、クレデンシャルを求められます。で作成したクラスタユーザアカウント `service-processor` アプリケーションタイプは、クラスタの任意のノードの SP CLI にアクセスできます。SP ユーザアカウントは、ONTAP から管理され、パスワードによって認証されます。ONTAP 9.9.1以降では、SP ユーザアカウントにが必要です `admin` ロール。

SP にアクセスするためのユーザアカウントは、SP CLI ではなく ONTAP で管理します。で作成されたクラスタユーザアカウントは、SP にアクセスできます `-application` のパラメータ `security login create` コマンドをに設定します `service-processor` および `-authmethod` パラメータをに設定します `password`。SP ではパスワード認証のみサポートされます。

を指定する必要があります `-role` SP ユーザアカウント作成時のパラメータ。

- ONTAP 9.9.1以降のリリースでは、を指定する必要があります `admin` をクリックします `-role` パラメータを使用し、アカウントを変更するにはを使用する必要があります `admin` ロール。セキュリティ上の理由から、他のロールは使用できなくなりました。
  - ONTAP 9.9.1以降のリリースにアップグレードする場合は、を参照してください ["サービスプロセッサにアクセスできるユーザアカウントが変更されました"](#)。
  - ONTAP 9.8以前のリリースに戻す場合は、を参照してください ["サービスプロセッサにアクセスできるユーザアカウントを確認します"](#)。
- ONTAP 9.8以前のリリースでは、すべてのロールがSPにアクセスできますが `admin` が推奨されます。

デフォルトでは、「`admin`」という名前のクラスタユーザアカウントにはが含まれています `service-processor` アプリケーションタイプであり、SP へのアクセス権があります。

ONTAP では、システム用に予約されている名前（「`root`」や「`naroot`」など）を使用したユーザアカウントを作成できないようになっています。システム用に予約されている名前を使用してクラスタまたは SP にアクセスすることはできません。

を使用して、現在のSPユーザアカウントを表示できます `-application service-processor` のパラメータ `security login show` コマンドを実行します

## 管理ホストから SP / BMC にアクセスします

管理ホストからノードの SP にログインして、ノードの管理タスクをリモートから実行できます。

必要なもの

次の条件を満たす必要があります。

- SP へのアクセスに使用する管理ホストでは SSHv2 がサポートされている必要がある。
- SP へのアクセス用にユーザアカウントがすでにセットアップされている必要があります。

SPにアクセスするには、でユーザアカウントを作成しておく必要があります `-application` のパラメータ `security login create` コマンドをに設定します `service-processor` および `-authmethod` パラメータをに設定します `password`。



このタスクでは、SP と BMC の両方を環境に設定します。

SP が IPv4 または IPv6 アドレスを使用するように設定されていて、ホストからの SSH ログイン試行が 10 分以内に連続 5 回失敗した場合には、SP は SSH ログイン要求を拒否し、ホストの IP アドレスとの通信を 15 分間中断します。通信は 15 分後に再開され、SP へのログインを再度試行できるようになります。

ONTAP では、システム用に予約されている名前（「root」や「naroot」など）をクラスタまたは SP にアクセスする目的で作成または使用することはできません。

#### 手順

1. 管理ホストから、SP にログインします。

```
ssh username@SP_IP_address
```

2. プロンプトが表示されたら、のパスワードを入力します `username`。

SP プロンプトが表示され、SP CLI にアクセスしていることが示されます。

#### 管理ホストからの SP アクセスの例

次の例は、ユーザアカウントを使用して SP にログインする方法を示しています `joe`（SP にアクセスするように設定されています）。

```
[admin_host]$ ssh joe@192.168.123.98
joe@192.168.123.98's password:
SP>
```

次の例は、IPv6 グローバルアドレスまたは IPv6 ルータ通知アドレスを使用して、IPv6 に対して SSH が設定されかつ SP が設定されているノードの SP にログインする方法を示しています。

```
[admin_host]$ ssh joe@fd22:8b1e:b255:202::1234
joe@fd22:8b1e:b255:202::1234's password:
SP>
```

```
[admin_host]$ ssh joe@fd22:8b1e:b255:202:2a0:98ff:fe01:7d5b
joe@fd22:8b1e:b255:202:2a0:98ff:fe01:7d5b's password:
SP>
```

システムコンソールから **SP / BMC** にアクセスする

システムコンソール（ *serial console* ） から SP にアクセスして、タスクの監視やトラブルシューティングを実行できます。

このタスクについて

このタスクでは、SP と BMC の両方を環境に設定します。

手順

1. システムコンソールから SP CLI にアクセスするには、プロンプトで Ctrl+G を押します。
2. プロンプトが表示されたら、SP CLI にログインします。

SP プロンプトが表示され、SP CLI にアクセスしていることが示されます。

3. SP CLI を終了してシステムコンソールに戻るには、Ctrl+D を押し、Enter キーを押します。

システムコンソールから **SP CLI** へのアクセスの例

次の例に、Ctrl+G を押してシステムコンソールから SP CLI にアクセスした結果を示します。。 help system power SPプロンプトにコマンドを入力し、続いてCtrl+D、Enterキーを押してシステムコンソールに戻ります。

```
cluster1::>
```

（ SP CLI にアクセスするには Ctrl+G を押します。）

```
Switching console to Service Processor
Service Processor Login:
Password:
SP>
SP> help system power
system power cycle - power the system off, then on
system power off - power the system off
system power on - power the system on
system power status - print system power status
SP>
```

（システムコンソールに戻るには、Ctrl+D と Enter キーを押します。）

```
cluster1::>
```

## SP CLI セッション、SP コンソールセッション、システムコンソールセッションの関係

SP CLI セッションを開いてノードをリモートから管理したり、別の SP コンソールセッションを開いてノードのコンソールにアクセスしたりすることができます。SP コンソールセッションは、同時システムコンソールセッションに表示される出力をミラーリングします。SP とシステムコンソールには独立したシェル環境があり、独立したログイン認証が行われます。

SP CLI セッション、SP コンソールセッション、システムコンソールセッションの関係を理解しておくと、ノードをリモートから管理する際に役に立ちます。これらのセッションの関係を次に示します。

- SP CLI セッションには一度に 1 人の管理者しかログインできません。ただし SP では、SP CLI セッションと別の SP コンソールセッションを同時に開くことができます。

SP CLI は SP プロンプトで示されます (SP>)。SP CLI セッションでは、SP を使用できます `system console` SP コンソールセッションを開始するコマンド。同時に、SSH を介して別の SP CLI セッションを開始することもできます。Ctrl+D キーを押して SP コンソールセッションを終了すると、自動的に SP CLI セッションに戻ります。SP CLI セッションがすでに存在する場合は、既存の SP CLI セッションを終了するかどうかを尋ねるメッセージが表示されます。「y」と入力すると、既存の SP CLI セッションが終了し、SP コンソールから SP CLI に戻ることができます。このアクションは、SP イベントログに記録されます。

SSH 経由で接続された ONTAP CLI セッションでは、ONTAP を実行してノードのシステムコンソールに切り替えることができます `system node run-console` 別のノードからコマンドを実行します。

- セキュリティ上の理由から、SP CLI セッションとシステムコンソールセッションには独立したログイン認証機能があります。

SP CLI から (SP を使用して) SP コンソールセッションを開始するとき `system console` コマンド) を入力すると、システムコンソールのクレデンシャルを入力するように求められます。システムコンソールセッションから (Ctrl+G キーで) SP CLI にアクセスすると、SP CLI のクレデンシャルを入力するように求められます。

- SP コンソールセッションとシステムコンソールセッションには独立したシェル環境があります。

SP コンソールセッションは、同時システムコンソールセッションに表示される出力をミラーリングします。ただし、同時システムコンソールセッションでは、SP コンソールセッションをミラーリングしません。

SP コンソールセッションは、同時 SSH セッションの出力をミラーリングしません。

## SP にアクセスできる IP アドレスを管理します

デフォルトでは、SP はすべての IP アドレスの管理ホストからの SSH 接続要求を受け付けます。指定した IP アドレスを持つ管理ホストのみからの SSH 接続要求を受け付けるように SP を設定できます。変更内容は、クラスタ内のすべてのノードの SP への SSH アクセスに適用されます。

## 手順

1. 指定したIPアドレスのみにSPアクセスを付与するには、を使用します `system service-processor ssh add-allowed-addresses` コマンドにを指定します `-allowed-addresses` パラメータ

- の値 `-allowed-addresses` パラメータはの形式で指定する必要があります `address/netmask`、および複数 `address/netmask` ペアはカンマで区切る必要があります。例： `10.98.150.10/24`, `fd20:8b1e:b255:c09b::/64`。

を設定します `-allowed-addresses` パラメータの値 `0.0.0.0/0`, `::/0` すべてのIPアドレスがSPにアクセスできるようにします（デフォルト）。

- 指定したIPアドレスのみにSPアクセスを制限してデフォルトを変更すると、ONTAP は、指定したIPアドレスでデフォルト設定「すべて許可」を置き換えることを確認するプロンプトを表示します (`0.0.0.0/0`, `::/0`) 。

- `system service-processor ssh show` コマンドは、SPにアクセスできるIPアドレスを表示します。

2. 指定したIPアドレスをSPへのアクセスからブロックする場合は、を使用します `system service-processor ssh remove-allowed-addresses` コマンドにを指定します `-allowed-addresses` パラメータ

すべての IP アドレスから SP へのアクセスをブロックすると、管理ホストから SP にアクセスできなくなります。

### SPにアクセスできるIPアドレスの管理の例

次の例は、SP への SSH アクセスのためのデフォルト設定を示しています。ここでは、指定した IP アドレスのみに SP アクセスを制限することで、デフォルトの設定を変更し、指定した IP アドレスをアクセスリストから削除し、すべての IP アドレスに対する SP アクセスをリストアします。



```

cluster1::> system service-processor ssh show
  Allowed Addresses: 0.0.0.0/0, ::/0

cluster1::> system service-processor ssh add-allowed-addresses -allowed
-addresses 192.168.1.202/24, 192.168.10.201/24

Warning: The default "allow all" setting (0.0.0.0/0, ::/0) will be
replaced
      with your changes. Do you want to continue? {y|n}: y

cluster1::> system service-processor ssh show
  Allowed Addresses: 192.168.1.202/24, 192.168.10.201/24

cluster1::> system service-processor ssh remove-allowed-addresses -allowed
-addresses 192.168.1.202/24, 192.168.10.201/24

Warning: If all IP addresses are removed from the allowed address list,
all IP
      addresses will be denied access. To restore the "allow all"
default,
      use the "system service-processor ssh add-allowed-addresses
      -allowed-addresses 0.0.0.0/0, ::/0" command. Do you want to
continue?
      {y|n}: y

cluster1::> system service-processor ssh show
  Allowed Addresses: -

cluster1::> system service-processor ssh add-allowed-addresses -allowed
-addresses 0.0.0.0/0, ::/0

cluster1::> system service-processor ssh show
  Allowed Addresses: 0.0.0.0/0, ::/0

```

## SP / BMC CLI でオンラインヘルプを使用する

オンラインヘルプで SP / BMC CLI のコマンドとオプションを確認できます。

このタスクについて

このタスクでは、SP と BMC の両方を環境に設定します。

手順

1. SP / BMC コマンドのヘルプ情報を表示するには、次のコマンドを入力します。

SP ヘルプにアクセス	BMCヘルプにアクセスする
を入力します <code>help</code> SPプロンプトで、	を入力します <code>system</code> BMCプロンプトで、

次に、SP CLI オンラインヘルプの例を示します。

```
SP> help
date - print date and time
exit - exit from the SP command line interface
events - print system events and event information
help - print command help
priv - show and set user mode
sp - commands to control the SP
system - commands to control the system
version - print SP version
```

次に、BMC CLIオンラインヘルプの例を示します。

```
BMC> system
system acp - acp related commands
system battery - battery related commands
system console - connect to the system console
system core - dump the system core and reset
system cpld - cpld commands
system log - print system console logs
system power - commands controlling system power
system reset - reset the system using the selected firmware
system sensors - print environmental sensors status
system service-event - print service-event status
system fru - fru related commands
system watchdog - system watchdog commands

BMC>
```

2. SP / BMCコマンドのオプションのヘルプ情報を表示するには、と入力します `help` SP / BMCコマンドの実行前または実行後。

次の例は、SPのSP CLIオンラインヘルプを示しています `events` コマンドを実行します

```
SP> help events
events all - print all system events
events info - print system event log information
events newest - print newest system events
events oldest - print oldest system events
events search - search for and print system events
```

次に、BMC CLIオンラインヘルプの例を示します `system power` コマンドを実行します

```
BMC> system power help
system power cycle - power the system off, then on
system power off - power the system off
system power on - power the system on
system power status - print system power status

BMC>
```

ノードをリモートから管理するためのコマンド

ノードをリモートで管理するには、ノードの SP にアクセスし、SP CLI コマンドを実行してノード管理タスクを実行します。よく実行されるいくつかのリモートノード管理タスクについては、クラスタ内の別のノードから ONTAP コマンドを使用することもできます。一部の SP コマンドはプラットフォーム固有であるため、プラットフォームによっては使用できない場合があります。

状況	使用する <b>SP</b> コマンド	使用する <b>BMC</b> コマンド	または <b>ONTAP</b> コマンド
使用できる SP コマンド、または指定した SP コマンドのサブコマンドを表示する	<code>help [command]</code>		
SP CLI の現在の権限レベルを表示します	<code>priv show</code>		
SP CLI について指定されたモードにアクセスするには、権限レベルを設定してください	<code>priv set {admin</code>	<code>advanced</code>	<code>diag}</code>
		システムの日付と時刻を表示します	<code>date</code>

状況	使用する <b>SP</b> コマンド	使用する <b>BMC</b> コマンド	または <b>ONTAP</b> コマンド
	date	SP によって記録されるイベントを表示する	events {all
info	newest number	oldest number	search keyword}
		SP のステータスとネットワーク設定情報を表示する	sp status [-v
-d]  。 -v オプションを指定すると、SP統計が詳細な形式で表示されます。。 -d オプションを指定すると、SPデバッグログが表示に追加されます。	bmc status [-v	-d]  。 -v オプションを指定すると、SP統計が詳細な形式で表示されます。。 -d オプションを指定すると、SPデバッグログが表示に追加されます。	system service-processor show
SP が稼働している時間、および過去 1 分、5 分、15 分間に実行キューに入れているジョブの平均数を表示します	sp uptime	bmc uptime	
システムコンソールログを表示する	system log		
SP ログアーカイブ、またはアーカイブ内のファイルを表示する	sp log history show [-archive {latest	{all	archive-name} ][ -dump {all
file-name} ]	bmc log history show [-archive {latest	{all	archive-name} ][ -dump {all
file-name} ]		ノードのコントローラの電源ステータスを表示する	system power status
	system node power show	バッテリー情報を表示します	system battery show
		ACP 情報またはエクスパンダセンサーのステータスを表示します	system acp [show

状況	使用する <b>SP</b> コマンド	使用する <b>BMC</b> コマンド	または <b>ONTAP</b> コマンド
sensors show]			すべてのシステム FRU とその ID をリストします
system fru list			指定した FRU の製品情報を表示します
system fru show fru_id			FRU のデータ履歴ログを表示します
system fru log show ( advanced 権限レベル )			状態や現在の値など、環境センサーのステータスを表示します
system sensors または system sensors show		system node environment sensors show	指定したセンサーのステータスと詳細を表示する
system sensors get sensor_name  を取得できます sensor_name を使用します system sensors または system sensors show コマンドを実行します			SP ファームウェアのバージョン情報を表示する
version		system service- processor image show	SP コマンド履歴を表示する
sp log audit ( advanced 権限レベル)	bmc log audit		SP デバッグ情報を表示します
sp log debug ( advanced 権限レベル)	bmc log debug ( advanced 権限レベル)		SP メッセージファイルを表示します
sp log messages ( advanced 権限レベル)	bmc log messages ( advanced 権限レベル)		watchdog リセットイベントでシステムの詳細情報を収集する設定を表示するか、watchdog リセットイベント中に収集されたシステムの詳細情報を表示するか、収集されたシステム詳細情報をクリアする

状況	使用する <b>SP</b> コマンド	使用する <b>BMC</b> コマンド	または <b>ONTAP</b> コマンド
system forensics [show	log dump	log clear]	
	システムコンソールにロ グインします	system console	
system node run- console	システムコンソールセッ ションを終了するには、 Ctrl+D キーを押す必要が あります。	ノードをオンまたはオフ にするか、電源の再投入 を行う（電源をオフにし て再度オンにする）	system power on
	system node power on （advanced 権限レベ ル）	system power off	
	system power cycle		

状況	使用する <b>SP</b> コマンド	使用する <b>BMC</b> コマンド	または <b>ONTAP</b> コマンド
<p>スタンバイ電源は、SP が中断されることなく稼働し続けるために、オンのままになります。電源再投入の場合は、電源は一時的に停止したあと、再度オンになります。</p> <div>  <p>これらのコマンドを使用してノードの電源をオフにするか再投入すると原因、ノードが誤ってシャットダウンされる (dirty shutdown) ことがあります。この方法は、ONTAP を使用した正常なシャットダウンの代わりにはなりません</p> <p>system node halt コマンドを実行します</p> </div>	<p>コアダンプを作成してノードをリセットする</p>	<p>system core [-f]</p> <p>。 -f オプションを指定すると、コアダンプが強制的に作成され、ノードがリセットされます。</p>	





状況	使用する <b>SP</b> コマンド	使用する <b>BMC</b> コマンド	または <b>ONTAP</b> コマンド
	現在のバッテリーファームウェアのイメージと指定したファームウェアイメージを比較します	system battery verify [image_URL]  ( advanced 権限レベル )  状況 image_URL が指定されていません。比較にはデフォルトのバッテリーファームウェアイメージが使用されます。	
	指定した場所でイメージからバッテリーファームウェアを更新します	system battery flash image_URL  ( advanced 権限レベル )  何らかの理由でバッテリーファームウェアの自動アップグレードプロセスに失敗した場合は、このコマンドを使用します。	
	指定した場所でイメージを使用して SP ファームウェアを更新します	sp update image_URL image_URL 最大文字数は200文字です。	bmc update image_URL image_URL 最大文字数は200文字です。
system service-processor image update	SP をリブートします	sp reboot	
system service-processor reboot-sp	NVRAM フラッシュコンテンツを消去します	system nvram flash clear ( advanced 権限レベル )  このコマンドは、コントローラの電源がオフのときは開始できません (system power off ) 。	
	SP CLI を終了します	exit	

しきい値ベースの **SP** センサーの読み取り値と **system sensors** コマンドのステータス値について説明します

しきい値ベースのセンサーは、さまざまなシステムコンポーネントを定期的に読み取ります。SP は、しきい値ベースのセンサーの読み取り値を、コンポーネントの許容可能な

動作条件を定義する事前設定されたしきい値と比較します。

SP は、センサーの読み取り値に基づいてセンサーの状態を表示し、コンポーネントの状態の監視に役立ちます。

しきい値ベースのセンサーには、システム温度、電圧、電流、ファン速度のセンサーなどがあります。しきい値ベースのセンサーのリストは、プラットフォームによって異なります。

しきい値ベースのセンサーには次のしきい値があり、これらはSPの出力に表示されます `system sensors` コマンドを実行します

- 異常 - 下限 (LCR)
- 異常 - 下限 (LNC)
- 異常 - 上限 (UNC)
- 重大 - 上限 (UCR)

センサー読み取り値が LNC と LCR の間、または UNC と UCR の間の場合は、コンポーネントが問題の兆候を示しており、その結果、システムに障害が発生する可能性があることを示します。そのため、コンポーネントの保守をすぐに計画する必要があります。

センサーの読み取り値が LCR 以下、または UCR 以上の場合は、コンポーネントが誤動作しており、システム障害が発生しつつあることを意味します。したがって、コンポーネントに対して緊急な対応が必要です。

次の図に、しきい値と対応する重大度の範囲を示します。



しきい値ベースのセンサーの読み取り値は、で確認できます `Current` の列 `system sensors` コマンド出力。。 `system sensors get sensor_name` コマンドは、指定したセンサーの詳細を表示します。読み取り値が異常および重大のしきい値を超えると、センサーは重大度が上昇していることを報告します。読み取り値がしきい値制限を超えると、でセンサのステータスが表示されます `system sensors` コマンド出力がから変更されます `ok` 終了: `nc` (noncritical) または `cr` (重大) しきい値を超えた場合は、SELイベントログにイベントメッセージが記録されます。

しきい値ベースのセンサーには、4つのしきい値レベルが全部揃っていないものもあります。これらのセンサーの場合、欠落したしきい値が表示されます `na` の限界として `system sensors` 特定のセンサーに該当するしきい値や重大度が設定されていないことを示すコマンド出力。SPはそのしきい値についてセンサーを監視しません。

**system sensors** コマンド出力の例を示します

次の例は、によって表示される情報の一部を示しています `system sensors SP CLI`で次のコマンドを実行します。

```
SP node1> system sensors
```

Sensor Name	Current	Unit	Status	LCR	LNC
UNC	UCR				
-----+-----+-----+-----+-----+-----+					
-----+-----+-----+-----+-----+-----+					
CPU0_Temp_Margin	-55.000	degrees C	ok	na	na
-5.000	0.000				
CPU1_Temp_Margin	-56.000	degrees C	ok	na	na
-5.000	0.000				
In_Flow_Temp	32.000	degrees C	ok	0.000	10.000
42.000	52.000				
Out_Flow_Temp	38.000	degrees C	ok	0.000	10.000
59.000	68.000				
CPU1_Error	0x0	discrete	0x0180	na	na
na	na				
CPU1_Therm_Trip	0x0	discrete	0x0180	na	na
na	na				
CPU1_Hot	0x0	discrete	0x0180	na	na
na	na				
IO_Mid1_Temp	30.000	degrees C	ok	0.000	10.000
55.000	64.000				
IO_Mid2_Temp	30.000	degrees C	ok	0.000	10.000
55.000	64.000				
CPU_VTT	1.106	Volts	ok	1.028	1.048
1.154	1.174				
CPU0_VCC	1.154	Volts	ok	0.834	0.844
1.348	1.368				
3.3V	3.323	Volts	ok	3.053	3.116
3.466	3.546				
5V	5.002	Volts	ok	4.368	4.465
5.490	5.636				
STBY_1.8V	1.794	Volts	ok	1.678	1.707
1.892	1.911				
...					

しきい値ベースのセンサーの**system sensors sensor\_name**コマンド出力の例

次の例は、と入力した結果を示しています **system sensors get sensor\_name** しきい値ベースのセンサー-5VのSP CLIで、次の手順を実行します。

```

SP node1> system sensors get 5V

Locating sensor record...
Sensor ID           : 5V (0x13)
Entity ID           : 7.97
Sensor Type (Analog) : Voltage
Sensor Reading       : 5.002 (+/- 0) Volts
Status               : ok
Lower Non-Recoverable : na
Lower Critical        : 4.246
Lower Non-Critical    : 4.490
Upper Non-Critical    : 5.490
Upper Critical        : 5.758
Upper Non-Recoverable : na
Assertion Events      :
Assertions Enabled    : lnc- lcr- ucr+
Deassertions Enabled : lnc- lcr- ucr+

```

**system sensors** コマンド出力でのディスクリート **SP** センサーのステータス値について説明します

ディスクリートセンサーにはしきい値がありません。の下に表示されます [Current](#) 列をクリックします system sensors コマンド出力には実際の意味はないため、SPでは無視されます。。Status の列 system sensors コマンド出力には、ディスクリートセンサーのステータス値が16進形式で表示されます。

ディスクリートセンサーの例としては、ファン、電源ユニット（PSU）エラー、システムエラーのセンサーがあります。ディスクリートセンサーの具体的なリストは、プラットフォームによって異なります。

SP CLIを使用できます system sensors get sensor\_name コマンドを使用して、ほとんどのディスクリートセンサーのステータス値を解釈できます。次の例は、と入力した結果を示しています system sensors get sensor\_name ディスクリートセンサーCPU0\_ErrorおよびIO\_Slot1\_Presentの場合：

```

SP node1> system sensors get CPU0_Error

Locating sensor record...
Sensor ID           : CPU0_Error (0x67)
Entity ID           : 7.97
Sensor Type (Discrete): Temperature
States Asserted      : Digital State
                      [State Deasserted]

```

```

SP node1> system sensors get IO_Slot1_Present
Locating sensor record...
Sensor ID           : IO_Slot1_Present (0x74)
Entity ID           : 11.97
Sensor Type (Discrete): Add-in Card
States Asserted      : Availability State
                      [Device Present]

```

ただし、system sensors get sensor\_name コマンドを実行すると、ほとんどのディスクリットセンサーのステータス情報が表示されますが、System\_FW\_Status、System\_Watchdog、PSU1\_Input\_Type、およびPSU2\_Input\_Typeディスクリットセンサーのステータス情報は表示されません。これらのセンサーのステータス情報は、次の情報を使用して解釈できます。

#### System\_FW\_Status の場合

System\_FW\_Statusセンサーの状態は、の形式で表示されます 0xAABB。の情報を組み合わせることができ、AA および BB センサの状態を確認します。

AA 次のいずれかの値を指定できます。

値	センサの状態
01	システムファームウェアのエラーです
02	システムファームウェアがハングした
04	システムファームウェア実行中です

BB 次のいずれかの値を指定できます。

値	センサの状態
00	システムソフトウェアが正常にシャットダウンされました
01	メモリを初期化しています
02	NVMEM を初期化しています（ NVMEM がある場合 ）
04	メモリコントローラのハブ（ MCH ）値をリストアしています（ NVMEM がある場合 ）
05	ユーザがセットアップを開始しました

値	センサの状態
13	オペレーティングシステムまたは LOADER を起動しています
1F	BIOS を起動しています
20	LOADER を実行しています
21.	LOADER がプライマリ BIOS ファームウェアをプログラミングしています。システムの電源を切らないでください
22	LOADER が代替 BIOS ファームウェアをプログラミングしています。システムの電源を切らないでください
2F	ONTAP が実行されています
60ドルだ	SP によってシステムの電源が切断されました
61歳	SP によってシステムの電源がオンになりました
62	SP によってシステムがリセットされました
63	SP watchdog 電源再投入
64歳	SP watchdog コールドリセット

たとえば、System\_FW\_Status センサのステータス 0x042F は、「システムファームウェアが進行中（04）」で、ONTAP が実行中（2F）」という意味です。

### System\_Watchdog

System\_Watchdog センサの状態は次のいずれかです。

- \* 0x0080\*

このセンサの状態は変更されていません

値	センサの状態
0x0081	タイマー割り込み
0x0180	タイマーが切れました

値	センサの状態
0x0280	ハードリセット
0x0480	電源をオフにします
0x0880	電源を再投入します

たとえば、System\_Watchdog センサーのステータス 0x0880 は、watchdog タイムアウトが発生したことを意味し、システムの電源の再投入につながります。

#### PSU1\_Input\_TypeおよびPSU2\_Input\_Type

直流（DC）電源の場合、PSU1\_Input\_Type および PSU2\_Input\_Type センサーは適用されません。交流（AC）電源の場合、センサーのステータスは次のいずれかの値になります。

値	センサの状態
0x01 xx	220V PSU タイプ
0x02 xx	110V PSUタイプ

たとえば、PSU1\_Input\_Type センサーのステータス 0x0280 は、PSU タイプが 110V であるとセンサーが報告していることを意味します。

#### ONTAP から SP を管理するためのコマンド

ONTAP には、SP ネットワーク設定、SP ファームウェアイメージ、SP への SSH アクセス、一般的な SP の管理など、SP を管理するためのコマンドが用意されています。

#### SP ネットワーク設定の管理用コマンド

状況	実行する ONTAP コマンド
SP の自動ネットワーク設定を有効にして、指定されたサブネットの IPv4 または IPv6 アドレスファミリーを使用します	<code>system service-processor network auto-configuration enable</code>
指定されたサブネットの IPv4 または IPv6 アドレスファミリーを使用する、SP の自動ネットワーク設定を無効にする	<code>system service-processor network auto-configuration disable</code>
SPの自動ネットワーク設定を表示する	<code>system service-processor network auto-configuration show</code>


状況	実行する <b>ONTAP</b> コマンド
<p>ノードの SP ネットワークについて、次の項目を手動で設定する</p> <ul style="list-style-type: none"> <li>• IP アドレスファミリー（IPv4 または IPv6）</li> <li>• 指定した IP アドレスファミリーのネットワークインターフェイスを有効にするかどうか</li> <li>• IPv4 を使用している場合に、DHCP サーバのネットワーク設定と、指定したネットワークアドレスのどちらを使用するか</li> <li>• SP のパブリック IP アドレス</li> <li>• SP のネットマスク（IPv4 を使用している場合）</li> <li>• SP のサブネットマスクのネットワークプレフィックス長（IPv6 を使用している場合）</li> <li>• SP のゲートウェイ IP アドレス</li> </ul>	<p><code>system service-processor network modify</code></p>
<p>次のような SP ネットワーク設定を表示する</p> <ul style="list-style-type: none"> <li>• 設定されているアドレスファミリー（IPv4 または IPv6）、およびそれが有効かどうか</li> <li>• リモート管理デバイスのタイプ</li> <li>• 現在の SP のステータスとリンクのステータス</li> <li>• IP アドレス、MAC アドレス、ネットマスク、サブネットマスクのプレフィックス長、ルータによって割り当てられた IP アドレス、リンクローカル IP アドレス、ゲートウェイ IP アドレスなどのネットワーク設定</li> <li>• SP が最後に更新された時刻</li> <li>• SP の自動設定に使用するサブネットの名前</li> <li>• ルータによって割り当てられた IPv6 IP アドレスが有効かどうか</li> <li>• SP ネットワークのセットアップステータス</li> <li>• SP ネットワークのセットアップが失敗した理由</li> </ul>	<p><code>system service-processor network show</code></p> <p>SP ネットワークの詳細をすべて表示するには、が必要です <code>-instance</code> パラメータ</p>
<p>次の SP API サービス設定を変更する</p> <ul style="list-style-type: none"> <li>• SP API サービスで使用するポートの変更</li> <li>• SP API サービスを有効または無効にします</li> </ul>	<p><code>system service-processor api-service modify</code></p> <p>（advanced 権限レベル）</p>



状況	実行する <b>ONTAP</b> コマンド
SP API サービス設定を表示する	<pre>system service-processor api-service show</pre> <p>( advanced 権限レベル)</p>
SP API サービスの内部通信に使用される SSL 証明書および SSH 証明書を更新する	<ul style="list-style-type: none"> <li>• ONTAP 9.5以降： <pre>system service-processor api-service renew-internal-certificates</pre></li> <li>• ONTAP 9.4以前： <pre>system service-processor api-service renew-certificates</pre></li> </ul> <p>( advanced 権限レベル)</p>

#### SP ファームウェアイメージの管理用コマンド

状況	実行する <b>ONTAP</b> コマンド
<p>現在インストールされている SP ファームウェアイメージの次のような詳細を表示する</p> <ul style="list-style-type: none"> <li>• リモート管理デバイスのタイプ</li> <li>• SP がブートされるイメージ（プライマリまたはバックアップ）とそのステータス、およびファームウェアバージョン</li> <li>• ファームウェアの自動更新が有効かどうかと、最新の更新ステータス</li> </ul>	<pre>system service-processor image show</pre> <p>。 -is-current パラメータは、インストールされているファームウェアのバージョンが最新かどうかではなく、SPが現在ブートされているイメージ（プライマリまたはバックアップ）を指定します。</p>
SP の自動ファームウェア更新を有効または無効にします	<pre>system service-processor image modify</pre> <p>デフォルトでは、SP ファームウェアは、ONTAP の更新時、または SP ファームウェアの新しいバージョンを手動でダウンロードしたときに、自動で更新されます。自動更新を無効にすると、ONTAP イメージと SP ファームウェアイメージの組み合わせが最適でなくなる、または無効になる場合があるため、無効にしないことを推奨します。</p>

状況	実行する <b>ONTAP</b> コマンド
ノードに SP ファームウェアイメージを手動でダウンロードする	<pre>system node image get</pre> <div>  <p>を実行する前に <code>system node image</code> コマンドを実行する場合は、権限レベルを <code>advanced</code> に設定する必要があります (<code>set -privilege advanced</code>) をクリックし、続行するかどうかを尋ねられたら「<code>y</code>」と入力します。</p> </div> <p>SP ファームウェアイメージは ONTAP に同梱されています。ONTAP に同梱されている SP ファームウェアとは異なるバージョンを使用する場合を除き、SP ファームウェアを手動でダウンロードする必要はありません。</p>
ONTAP からトリガーされた最新の SP ファームウェア更新に関し、以下を含むステータスを表示する <ul style="list-style-type: none"> <li>最新の SP ファームウェア更新の開始時刻と終了時刻</li> <li>更新が進行中かどうかと、進行状況</li> </ul>	<pre>system service-processor image update-progress show</pre>

#### SP への SSH アクセスを管理するためのコマンド

状況	実行する <b>ONTAP</b> コマンド
指定した IP アドレスにのみ SP へのアクセスを許可します	<pre>system service-processor ssh add-allowed-addresses</pre>
指定した IP アドレスに対して SP へのアクセスを禁止します	<pre>system service-processor ssh remove-allowed-addresses</pre>
SP にアクセスできる IP アドレスを表示する	<pre>system service-processor ssh show</pre>

#### 一般的な SP 管理用コマンド

状況	実行する <b>ONTAP</b> コマンド
次のような SP の一般情報を表示する <ul style="list-style-type: none"> <li>• リモート管理デバイスのタイプ</li> <li>• 現在の SP のステータス</li> <li>• SP ネットワークが設定されているかどうか</li> <li>• パブリック IP アドレスや MAC アドレスなどのネットワーク情報</li> <li>• SP ファームウェアのバージョンと Intelligent Platform Management Interface (IPMI) のバージョン</li> <li>• SP ファームウェアの自動更新が有効になっているかどうか</li> </ul>	<code>system service-processor show</code> SP情報をすべて表示するには、が必要です <code>-instance</code> パラメータ
ノードでSPをリブートします	<code>system service-processor reboot-sp</code>
指定したノードから収集された SP ログファイルを含む AutoSupport メッセージを生成して送信します	<code>system node autosupport invoke-splog</code>
収集元の各ノードにある SP ログファイルのシーケンス番号など、クラスタ内で収集された SP ログファイルの割り当てマップを表示する	<code>system service-processor log show-allocations</code>

#### 関連情報

["ONTAP 9コマンド"](#)

#### BMC 管理用の **ONTAP** コマンド

ここでは、Baseboard Management Controller（BMC；ベースボード管理コントローラ）に対してサポートされる **ONTAP** コマンドを示します。

BMC では、Service Processor（SP；サービスプロセッサ）と同じコマンドをいくつか使用します。BMC では次の SP コマンドがサポートされます。

状況	使用するコマンド
BMC の情報を表示します	<code>system service-processor show</code>
BMC のネットワーク設定を表示または変更します	<code>system service-processor network show/modify</code>
BMC をリセットします	<code>system service-processor reboot-sp</code>

状況	使用するコマンド
現在インストールされている BMC ファームウェアイメージの詳細を表示または変更します	<b>system service-processor image show/modify</b>
BMC ファームウェアを更新します	<b>system service-processor image update</b>
最新の BMC ファームウェア更新のステータスを表示します	<b>system service-processor image update-progress show</b>
BMC の自動ネットワーク設定を有効にして、指定したサブネットの IPv4 または IPv6 アドレスを使用するように設定します	<b>system service-processor network auto-configuration enable</b>
BMC 用に指定したサブネットで、IPv4 アドレスまたは IPv6 アドレスの自動ネットワーク設定を無効にします	<b>system service-processor network auto-configuration disable</b>
BMC の自動ネットワーク設定を表示する	<b>system service-processor network auto-configuration show</b>

BMC ファームウェアでサポートされていないコマンドを実行すると、次のエラーメッセージが返されます。

```
::> Error: Command not supported on this platform.
```

## BMC CLI コマンド

BMC には SSH を使用してログインできます。BMC コマンドラインでは次のコマンドがサポートされます。

コマンドを実行します	機能
システム	すべてのコマンドのリストを表示します。
システムコンソール	システムのコンソールに接続します。使用 Ctrl+D セッションを終了します。
システムコア	システムコアをダンプしてリセットします。
システムの電源を再投入します	システムの電源をオフにしてからオンにします。
システムの電源がオフになりました	システムの電源をオフにします。
システムの電源が入っている	システムの電源をオンにします。

コマンドを実行します	機能
システムの電源ステータス	システムの電源ステータスを出力します。
システムリセット	システムをリセットします。
システムログ	システムコンソールログを出力します
system fru show [id]	すべてまたは選択した Field Replaceable Unit （FRU；フィールド交換可能ユニット）の情報をダンプします。

## クラスタ時間の管理（クラスタ管理者のみ）

クラスタ時間が不正確だと問題が発生する可能性があります。ONTAP ではクラスタのタイムゾーン、日付、時刻を手動で設定できますが、クラスタ時間を同期する場合はネットワークタイムプロトコル（NTP）サーバを設定する必要があります。

ONTAP 9.5 以降では、対称認証を使用して NTP サーバを設定できます。

NTP は常に有効です。ただし、クラスタを外部の時間ソースと同期するには、引き続き設定が必要です。ONTAP では、次の方法でクラスタの NTP 設定を管理できます。

- 最大10台の外部NTPサーバをクラスタに関連付けることができます (`cluster time-service ntp server create`) 。
  - タイムサービスの冗長性と品質を高めるためには、最低 3 台の外部 NTP サーバをクラスタに関連付ける必要があります。
  - NTP サーバは、IPv4 または IPv6 アドレス、あるいは完全修飾ホスト名を使用して指定できます。
  - 使用する NTP バージョン（v3 または v4）を手動で指定できます。

デフォルトでは、ONTAP は指定された外部 NTP サーバでサポートされている NTP バージョンを自動的に選択します。

指定した NTP バージョンが NTP サーバでサポートされていない場合は、時間を同期できません。

- advanced 権限レベルでは、クラスタに関連付けられている外部 NTP サーバを、クラスタ時間を修正、調整するための主要時間ソースとして指定できます。
- クラスタに関連付けられているNTPサーバを表示できます (`cluster time-service ntp server show`) 。
- クラスタのNTP設定を変更できます (`cluster time-service ntp server modify`) 。
- クラスタと外部NTPサーバの関連付けを解除できます (`cluster time-service ntp server delete`) 。
- advanced権限レベルでは、クラスタに関連付けられているすべての外部NTPサーバをクリアすることで設定をリセットできます (`cluster time-service ntp server reset`) 。

クラスタを統合しているノードは、自動的にクラスタの NTP 設定を取り込みます。

ONTAP では、NTP を使用できるだけでなく、クラスタ時間を手動で管理できます。この機能は、間違った時間を修正する場合に便利です（リブート後にノードの時間が著しくずれた場合など）。その場合は、NTP が外部の時間サーバと同期できるようになるまで、クラスタのおおよその時間を指定します。手動で設定した時間は、クラスタ上のすべてのノードに反映されます。

クラスタ時間を手動で管理するには、次の方法があります。

- ・クラスタのタイムゾーン、日付、時刻を設定または変更できます (cluster date modify) 。
- ・クラスタの現在のタイムゾーン、日付、おおよび時刻の設定を表示できます (cluster date show) 。



手動でのクラスタの日付や時刻変更は、ジョブスケジュールには反映されません。ジョブは、ジョブが作成された時点または最後に実行された時点のクラスタの時刻に基づいて実行されます。そのため、クラスタの日付や時刻を手動で変更する場合は、を使用する必要があります job show および job history show コマンドを使用して、スケジュールされたすべてのジョブが必要に応じてキューに格納されて完了していることを確認します。

## クラスタ時間の管理用コマンド

を使用します cluster time-service ntp server クラスタのNTPサーバを管理するコマンド。を使用します cluster date クラスタ時間を手動で管理するコマンド。

ONTAP 9.5 以降では、対称認証を使用して NTP サーバを設定できます。

次のコマンドによって、クラスタの NTP サーバを管理できます。

状況	使用するコマンド
クラスタを外部 NTP サーバと対称認証を使用せずに関連付ける	<pre>cluster time-service ntp server create -server server_name</pre>
ONTAP 9.5 以降では、クラスタを外部 NTP サーバと対称認証を使用できるように関連付けます	<pre>cluster time-service ntp server create -server server_ip_address -key-id key_id</pre> <div>。key_id 「cluster time-service ntp key」で設定された既存の共有キーを参照する必要があります。</div>
既存の NTP サーバに対して対称認証を有効にする必要なキー ID を追加することで、既存の NTP サーバを変更して認証を有効にすることができます  ONTAP 9.5 以降で利用できます	<pre>cluster time-service ntp server modify -server server_name -key-id key_id</pre>
対称認証を無効にします	<pre>cluster time-service ntp server modify -server server_name -is-authentication-enabled false</pre>

状況	使用するコマンド
共有 NTP キーを設定する	<pre>cluster time-service ntp key create -id shared_key_id -type shared_key_type -value shared_key_value</pre> <div>  <p>共有キーは ID で参照されます。ID、そのタイプ、および値が、ノードと NTP サーバで同じである必要があります</p> </div>
クラスタに関連付けられている NTP サーバに関する情報を表示する	<pre>cluster time-service ntp server show</pre>
クラスタに関連付けられた外部 NTP サーバの設定を変更する	<pre>cluster time-service ntp server modify</pre>
クラスタと NTP サーバの関連付けを解除します	<pre>cluster time-service ntp server delete</pre>
すべての外部 NTP サーバのクラスタとの関連付けを消去して設定をリセットします	<pre>cluster time-service ntp server reset</pre> <div>  <p>このコマンドには、advanced 権限レベルが必要です。</p> </div>

次のコマンドによって、手動でクラスタ時間を管理できます。

状況	使用するコマンド
タイムゾーン、日付、および時刻を設定または変更します	<pre>cluster date modify</pre>
クラスタのタイムゾーン、日付、および時刻の設定を表示します	<pre>cluster date show</pre>

## 関連情報

["ONTAP 9 コマンド"](#)

## バナーと MOTD を管理します

バナーと MOTD の概要を管理します

ONTAP では、ログインバナーまたは Message Of The Day (MOTD) を設定して、クラスタまたは Storage Virtual Machine (SVM) の CLI ユーザに管理情報を提供できます。

バナーは、ユーザにパスワードなどの認証を要求する前に、コンソールセッション（クラスタアクセスのみ）または SSH セッション（クラスタアクセスまたは SVM アクセス）に表示されます。たとえば、バナーを使

用して、システムへのログインを試行したユーザに次のような警告メッセージを表示することができます。

```
$ ssh admin@cluster1-01
```

```
This system is for authorized users only. Your IP Address has been logged.
```

```
Password:
```

MOTD は、ユーザの認証後、クラスタシェルのプロンプトが表示される前に、コンソールセッション（クラスタアクセスのみ）または SSH セッション（クラスタアクセスまたは SVM アクセス）に表示されます。たとえば、MOTD を使用して、認証されたユーザに次のような情報メッセージを表示することができます。

```
$ ssh admin@cluster1-01
```

```
Password:
```

```
Greetings. This system is running ONTAP 9.0.
```

```
Your user name is 'admin'. Your last login was Wed Apr 08 16:46:53 2015  
from 10.72.137.28.
```

バナーまたはMOTDの内容は、を使用して作成または変更できます security login banner modify または security login motd modify コマンドをそれぞれ次の方法で実行します。

- CLI の対話型モードまたは非対話型モードを使用して、バナーまたは MOTD に使用するテキストを指定できます。

対話型モード。を使用せずにコマンドを使用した場合に起動されます -message または -uri パラメータを指定すると、メッセージ内で改行(行末とも呼ばれます)を使用できます。

を使用する非対話型モード -message メッセージ文字列を指定するパラメータで、改行はサポートされません。

- バナーまたは MOTD に使用する内容を FTP または HTTP からアップロードできます。
- 動的な内容を表示するように MOTD を設定できます。

MOTD には、たとえば次のような情報を動的に表示することができます。

- クラスタ名、ノード名、または SVM 名
- クラスタの日付と時刻
- ログインしているユーザの名前
- ユーザによるクラスタのノードへの前回のログイン
- ログインしたデバイスの名前または IP アドレス
- オペレーティングシステムの名前
- ソフトウェアリリースバージョン



- 有効なクラスタバージョン文字列
  - `security login motd modify` のマニュアルページに、動的に生成される内容を MOTD に表示するためのエスケープシーケンスが記載されています。

バナーでは動的な内容はサポートされていません。

バナーと MOTD はクラスタレベルまたは SVM レベルで管理できます。

- バナーには次の特徴があります。
  - クラスタ用に設定したバナーは、バナーメッセージが定義されていない SVM に対しても表示されます。
  - SVM ごとに SVM レベルのバナーを設定できます。

このバナーが設定された SVM では、クラスタレベルのバナーが設定されていても、SVM レベルのバナーだけが表示されます。

- MOTD には次の特徴があります。
  - クラスタ用に設定した MOTD は、デフォルトですべての SVM に対しても有効になります。
  - また、SVM ごとに SVM レベルの MOTD を設定できます。

この場合、SVM にログインしたユーザには、クラスタレベルと SVM レベルの 2 つの MOTD が表示されます。

- クラスタレベルの MOTD を有効にするか無効にするかは、クラスタ管理者が SVM 単位で設定できます。

クラスタ管理者が SVM でクラスタレベルの MOTD を無効にした場合、その SVM にログインしたユーザにはクラスタレベルの MOTD は表示されません。

## バナーを作成します

バナーを作成して、クラスタまたは SVM へのアクセスを試行したユーザにメッセージを表示することができます。バナーは、ユーザに認証を要求する前に、コンソールセッション（クラスタアクセスのみ）または SSH セッション（クラスタアクセスまたは SVM アクセス）に表示されます。

## 手順

1. を使用します `security login banner modify` クラスタまたは SVM 用のバナーを作成するコマンドは次のとおりです。

状況	作業
1 行のメッセージを指定します	を使用します <code>-message "text"</code> パラメータを使用してテキストを指定します。
メッセージで改行（EOL）を使用する必要があります	コマンドは、を使用せずに使用します <code>-message</code> または <code>-uri</code> バナーを編集するための対話型モードを起動するためのパラメータ。

状況	作業
バナーに使用するコンテンツを特定の場所からアップロードします	を使用します -uri コンテンツのFTPまたはHTTPの場所を指定するパラメータ。

バナーの最大サイズは、改行も含めて 2、048 バイトまでです。

を使用して作成されるバナー -uri パラメータは静的です。以降にソースコンテンツが変更されても、自動では反映されません。

クラスタ用に作成したバナーは、既存のバナーがない SVM に対しても表示されます。以降に SVM 用のバナーを作成すると、その SVM に対しては、クラスタレベルのバナーではなくそのバナーが表示されます。を指定する -message 二重引用符で囲まれたハイフンを持つパラメータ ("-") をクリックすると、クラスタレベルのバナーを使用するように SVM がリセットされます。

2. で作成したバナーが表示されていることを確認します security login banner show コマンドを実行します

を指定する -message 空の文字列を持つパラメータ ("") には、コンテンツのないバナーが表示されます。

を指定する -message パラメータをに指定します "-" バナーが設定されていないすべての SVM（管理またはデータ）が表示されます。

## バナーの作成例

次の例では、非対話型モードを使用して「cluster1」クラスタ用のバナーを作成しています。

```
cluster1::> security login banner modify -message "Authorized users only!"
cluster1::>
```

次の例では、対話型モードを使用して「vm1」SVM 用のバナーを作成しています。

```
cluster1::> security login banner modify -vserver svm1

Enter the message of the day for Vserver "svm1".
Max size: 2048. Enter a blank line to terminate input. Press Ctrl-C to
abort.
0          1          2          3          4          5          6          7
8
1234567890123456789012345678901234567890123456789012345678901234
567890
The svm1 SVM is reserved for authorized users only!

cluster1::>
```

次の例は、作成したバナーを表示します。

```
cluster1::> security login banner show
Vserver: cluster1
Message
-----
---
Authorized users only!

Vserver: svm1
Message
-----
---
The svm1 SVM is reserved for authorized users only!

2 entries were displayed.

cluster1::>
```

関連情報

[バナーの管理](#)

バナーの管理

バナーはクラスタレベルまたは SVM レベルで管理できます。クラスタ用に設定したバナーは、バナーメッセージが定義されていない SVM に対しても表示されます。以降に SVM 用のバナーを作成すると、その SVM に対しては、クラスタ用のバナーではなくそのバナーが表示されます。

選択肢

- ・クラスタレベルのバナーの管理タスクを次に示します。

状況	作業
すべての CLI ログインセッションに対して表示するバナーを作成します	クラスタレベルのバナーを設定します。  `*security login banner modify -vserver <i>cluster_name</i> { [-message "text"]
[-uri ftp_or_http_addr] }`	すべてのログイン（クラスタと SVM の両方）に対するバナーを削除する
バナーを空の文字列に設定します ("") ：  <b>security login banner modify -vserver * -message ""</b>	SVM 管理者が作成したバナーを変更する

状況	作業
SVM のバナーメッセージを変更します。  `*security login banner modify -vserver <i>svm_name</i> { [-message " <i>text</i> "]	<code>[-uri <i>ftp_or_http_addr</i>] }*</code>

- SVM レベルのバナーの管理タスクを次に示します。

を指定します `-vserver svm_name` SVMのコンテキストでは必要ありません。

状況	作業
クラスタ管理者が指定したバナーの代わりに SVM 用の別のバナーを表示する	SVM 用のバナーを作成します。  `*security login banner modify -vserver <i>svm_name</i> { [-message " <i>text</i> "]
<code>[-uri <i>ftp_or_http_addr</i>] }*</code>	クラスタ管理者が指定したバナーも含め、いずれのバナーも SVM に対して表示されないようにする
SVM のバナーを空の文字列に設定します。  <b><code>security login banner modify -vserver <i>svm_name</i> -message ""</code></b>	現在 SVM レベルのバナーを使用している SVM でクラスタレベルのバナーを使用している場合

## MOTDの作成

Message Of The Day ( MOTD ) を作成して、認証された CLI ユーザに情報を提供することができます。MOTD は、ユーザの認証後、クラスタシェルスプロンプトが表示される前に、コンソールセッション（クラスタアクセスのみ）または SSH セッション（クラスタアクセスまたは SVM アクセス）に表示されます。

### 手順

1. を使用します `security login motd modify` クラスタまたはSVMのMOTDを作成するコマンドは次のとおりです。

状況	作業
1 行のメッセージを指定します	を使用します <code>-message "text"</code> パラメータを使用してテキストを指定します。
改行（ EOL ）を使用する	コマンドは、を使用せずに使用します <code>-message</code> または <code>-uri</code> MOTDを編集する対話型モードを起動するためのパラメータ。

状況	作業
MOTD に使用する内容を特定の場所からアップロードします	を使用します <code>-uri</code> コンテンツのFTPまたはHTTPの場所を指定するパラメータ。

MOTD の最大サイズは、改行も含めて 2、048 バイトまでです。

。 `security login motd modify` のマニュアルページに、動的に生成される内容をMOTDに表示するためのエスケープシーケンスが記載されています。

を使用して作成したMOTD `-uri` パラメータは静的です。以降にソースコンテンツが変更されても、自動では反映されません。

クラスタ用に作成した MOTD は、デフォルトでは、各 SVM に対して個別に作成した SVM レベルの MOTD と一緒に、すべての SVM ログインに対しても表示されます。を設定します `-is-cluster -message-enabled` パラメータの値 `false` SVMの場合、そのSVMに対するクラスタレベルのMOTDは表示されません。

2. を使用して、作成したMOTDが表示されていることを確認します `security login motd show` コマンドを実行します

を指定する `-message` 空の文字列を持つパラメータ ("`\"`") には、未設定または内容がないMOTDが表示されます。

を参照してください ["security login motd modify のように変更します"](#) 動的に生成される内容を MOTD に表示するために使用するパラメータのリストについては、コマンドのマニュアルページを参照してください。ONTAP のバージョンに固有のマニュアルページを確認してください。

## MOTDの作成例

次の例では、非対話型モードを使用して「cluster1」クラスタ用の MOTD を作成しています。

```
cluster1::> security login motd modify -message "Greetings!"
```

次の例では、対話型モードを使用して「svm1」SVM用の MOTD を作成しています。この MOTD では、エスケープシーケンスを使用して、動的に生成される内容を表示します。

```
cluster1::> security login motd modify -vserver svm1
```

```
Enter the message of the day for Vserver "svm1".
```

```
Max size: 2048. Enter a blank line to terminate input. Press Ctrl-C to abort.
```

```
0          1          2          3          4          5          6          7
8
```

```
1234567890123456789012345678901234567890123456789012345678901234
567890
```

```
Welcome to the \n SVM.  Your user ID is '\N'. Your last successful login
was \L.
```

次の例では、作成した MOTD を表示しています。

```
cluster1::> security login motd show
Vserver: cluster1
Is the Cluster MOTD Displayed?: true
Message
-----
---
Greetings!

Vserver: svm1
Is the Cluster MOTD Displayed?: true
Message
-----
---
Welcome to the \n SVM.  Your user ID is '\N'. Your last successful login
was \L.

2 entries were displayed.
```

**MOTD を管理します**

Message Of The Day （ MOTD ）はクラスタレベルまたは SVM レベルで管理できます。クラスタ用に設定した MOTD は、デフォルトですべての SVM に対しても有効になります。また、SVM ごとに SVM レベルの MOTD を設定できます。クラスタレベルの MOTD を有効にするか無効にするかは、クラスタ管理者が SVM ごとに設定できます。

MOTDの内容を動的に生成するために使用できるエスケープシーケンスのリストについては、[を参照してください](#) **"コマンドリファレンス"**。

**選択肢**

- ・クラスタレベルの MOTD の管理タスクを次に示します。

状況	作業
既存の MOTD がない場合にすべてのログインに対する MOTD を作成する	クラスタレベルの MOTD を設定します。  `*security login motd modify -vserver <i>cluster_name</i> { [-message " <i>text</i> "]
[-uri <i>ftp_or_http_addr</i> ] }`	SVM レベルの MOTD が設定されていない場合にすべてのログインに対する MOTD を変更する

状況	作業
<p>クラスタレベルの MOTD を変更します。</p> <pre>`*security login motd modify -vserver <i>cluster_name</i> { [-message "<i>text</i>"] }</pre>	<pre>[-uri ftp_or_http_addr] }*</pre>
<p>SVM レベルの MOTD が設定されていない場合にすべてのログインに対する MOTD を削除する</p>	<p>クラスタレベルの MOTD を空の文字列に設定します ("") :</p> <pre><b>security login motd modify -vserver <i>cluster_name</i> -message ""</b></pre>
<p>すべての SVM で、SVM レベルの MOTD を使用する代わりに、クラスタレベルの MOTD を表示するように設定します</p>	<p>クラスタレベルの MOTD を設定してから、SVM レベルのすべての MOTD を空の文字列に設定し、クラスタレベルの MOTD を有効にします。</p> <p>a. <code>*security login motd modify -vserver <i>cluster_name</i> { [-message "<i>text</i>"] }</code></p>
<pre>[-uri ftp_or_http_addr] }* ..<b>security login motd modify { -vserver !"<i>cluster_name</i>" } -message "" -is -cluster-message-enabled true</b></pre>	<p>クラスタレベルの MOTD を使用せずに、選択した SVM に対してのみ MOTD を表示する</p>
<p>クラスタレベルの MOTD を空の文字列に設定し、選択した SVM に対する SVM レベルの MOTD を設定します。</p> <p>a. <code>security login motd modify -vserver <i>cluster_name</i> -message ""</code></p> <p>b. <code>*security login motd modify -vserver <i>svm_name</i> { [-message "<i>text</i>"] }</code></p>	<pre>[-uri ftp_or_http_addr] }* +</pre> <p>この手順は、必要に応じて、各 SVM に対して繰り返し実行できます。</p>
<p>すべての SVM（データと管理の両方）に対して同じ SVM レベルの MOTD を使用します</p>	<p>同じ MOTD を使用するようにクラスタとすべての SVM を設定します。</p> <pre>`*security login motd modify -vserver * { [-message "<i>text</i>"] }</pre>
<pre>[-uri ftp_or_http_addr] }*  [NOTE] ==== CLI の対話型モードでは、クラスタと各 SVM について MOTD を個別に入力するように求められます。それぞれのプロンプトに同じ MOTD を貼り付けることができます。  ====</pre>	<p>クラスタレベルの MOTD をすべての SVM で必要に応じて表示できるようにし、クラスタログインに対しては表示されないようにする</p>

状況	作業
<p>クラスタレベルの MOTD を設定し、クラスタに対する表示を無効にします。</p> <pre>`*security login motd modify -vserver <i>cluster_name</i> { [-message "<i>text</i>"]</pre>	<pre>[-uri <i>ftp_or_http_addr</i>] } -is-cluster-message-enabled false`</pre>
<p>一部の SVM のみクラスタレベルと SVM レベルの両方の MOTD が設定されている場合は、クラスタレベルと SVM レベルのすべての MOTD を削除します</p>	<p>MOTD に空の文字列を使用するようにクラスタとすべての SVM を設定します。</p> <pre><b>security login motd modify -vserver * -message ""</b></pre>
<p>他の SVM で空の文字列が使用されている場合やクラスタレベルで別の MOTD が使用されている場合に、文字列が空でない SVM の MOTD だけを変更します</p>	<p>拡張クエリを使用して選択した MOTD を変更します。</p> <pre>`*security login motd modify { -vserver !"<i>cluster_name</i>" -message !"" } { [-message "<i>text</i>"]</pre>
<pre>[-uri <i>ftp_or_http_addr</i>] }`</pre>	<p>該当するテキストが複数行にまたがる場合でも、メッセージ内の任意の場所に特定のテキスト（「January」、「2015」など）を含むすべての MOTD を表示する</p>
<p>クエリを使用して MOTD を表示します。</p> <pre><b>security login motd show -message *"January"*"2015"*</b></pre>	<p>複数の連続する改行（EOL）を含む MOTD を対話型モードで作成する</p>

- SVM レベルの MOTD の管理タスクを次に示します。

を指定します `-vserver svm_name` SVM のコンテキストでは必要ありません。

状況	作業
<p>すでに SVM レベルの MOTD が設定された SVM で、別の SVM レベルの MOTD を使用します</p>	<p>SVM レベルの MOTD を変更します。</p> <pre>`*security login motd modify -vserver <i>svm_name</i> { [-message "<i>text</i>"]</pre>
<pre>[-uri <i>ftp_or_http_addr</i>] }`</pre>	<p>すでに SVM レベルの MOTD が設定された SVM で、クラスタレベルの MOTD だけを使用します</p>



状況	作業
<p>SVM レベルの MOTD を空の文字列に設定し、その SVM に対してクラスタレベルの MOTD を有効にするようにクラスタ管理者に依頼します。</p> <p>a. <b>security login motd modify -vserver <i>svm_name</i> -message ""</b></p> <p>b. (クラスタ管理者) <b>security login motd modify -vserver <i>svm_name</i> -is -cluster-message-enabled true</b></p>	<p>現在クラスタレベルと SVM レベルの両方の MOTD が表示されている SVM で、いずれの MOTD も表示されないようにする</p>

## ジョブとスケジュールの管理

ジョブはジョブキューに配置され、リソースが使用可能になるとバックグラウンドで実行されます。ジョブで使用するクラスタリソースが多すぎる場合は、そのジョブを停止するか、クラスタに対する要求が少なくなるまで一時停止できます。ジョブを監視および再開することもできます。

### ジョブのカテゴリ

管理できるジョブには、サーバ関連、クラスタ関連、およびプライベートの 3 つのカテゴリがあります。

ジョブは、次のいずれかのカテゴリに分類されます。

#### • \* サーバ関連ジョブ \*

このジョブは、実行する特定のノードに対して、管理フレームワークによってキューに登録されます。

#### • \* クラスタ関連ジョブ \*

このジョブは、実行するクラスタ内の任意のノードに対して、管理フレームワークによってキューに登録されます。

#### • \* プライベートジョブ \*

このジョブはノードに固有で、レプリケートされたデータベース（RDB）またはその他のクラスタメカニズムを使用しません。プライベートジョブの管理用コマンドには、advanced 権限レベル以上が必要です。

### ジョブの管理用コマンド

あるジョブを呼び出すコマンドを入力すると、通常、ジョブがキューに登録されたことが通知され、CLI のコマンドプロンプトに戻ります。ただし、一部のコマンドではジョブの進捗状況が表示され、ジョブが完了するまで CLI のコマンドプロンプトに戻りません。このような場合は、Ctrl+C キーを押してジョブをバックグラウンドに移動できます。

状況	使用するコマンド
すべてのジョブに関する情報を表示します	<code>job show</code>

状況	使用するコマンド
ジョブに関する情報をノード単位で表示します	<code>job show bynode</code>
クラスタ関連ジョブに関する情報を表示します	<code>job show-cluster</code>
完了したジョブに関する情報を表示します	<code>job show-completed</code>
ジョブ履歴に関する情報を表示します	<code>job history show</code>  クラスタ内の各ノードには、最大 25、000 個のジョブレコードが格納されます。そのため、ジョブ履歴全体を表示しようとする時間がかかることがあります。待ち時間が長くないようにするには、ジョブをノード、Storage Virtual Machine（SVM）、またはレコード ID ごとに表示します。
プライベートジョブのリストを表示します	<code>job private show</code> （advanced 権限レベル）
完了したプライベートジョブに関する情報を表示します	<code>job private show-completed</code> （advanced 権限レベル）
ジョブマネージャの初期化状態に関する情報を表示します	<code>job initstate show</code> （advanced 権限レベル）
ジョブの進捗状況を監視します	<code>job watch-progress</code>
プライベートジョブの進捗状況を監視する	<code>job private watch-progress</code> （advanced 権限レベル）
ジョブを一時停止します	<code>job pause</code>
プライベートジョブを一時停止します	<code>job private pause</code> （advanced 権限レベル）
一時停止したジョブを再開します	<code>job resume</code>
一時停止したプライベートジョブを再開します	<code>job private resume</code> （advanced 権限レベル）
ジョブを停止します	<code>job stop</code>
プライベートジョブを停止します	<code>job private stop</code> （advanced 権限レベル）
ジョブを削除します	<code>job delete</code>

状況	使用するコマンド
プライベートジョブを削除します	<code>job private delete</code> (advanced 権限レベル)
クラスタ関連ジョブと、そのジョブが所有する使用できないノードとの関連付けを解除し、別のノードがジョブの所有権を取得できるようにします	<code>job unclaim</code> (advanced 権限レベル)



を使用できます `event log show` 完了したジョブの結果を確認するコマンド。

## 関連情報

### "ONTAP 9コマンド"

## ジョブスケジュールの管理用コマンド

多くのタスク（ボリュームのSnapshotコピーなど）は、指定したスケジュールで実行するように設定できます。特定の時間に実行されるスケジュールは、`_cron_schedules`と呼ばれます（UNIXに似ています） `cron` スケジュール）。一定間隔で実行されるスケジュールは、`_interval_schedules` と呼ばれます。を使用します `job schedule` ジョブスケジュールを管理するコマンド。

手動でのクラスタの日付や時刻の変更は、ジョブスケジュールには反映されません。ジョブは、ジョブが作成された時点または最後に実行された時点のクラスタの時刻に基づいて実行されます。そのため、クラスタの日付や時刻を手動で変更する場合は、を使用する必要があります `job show` および `job history show` コマンドを使用して、スケジュールされたすべてのジョブが必要に応じてキューに格納されて完了していることを確認します。

クラスタが MetroCluster 構成に含まれている場合は、両方のクラスタのジョブスケジュールが同じである必要があります。したがって、ジョブスケジュールを作成、変更、または削除する場合は、リモートクラスタでも同じ処理を実行する必要があります。

状況	使用するコマンド
すべてのスケジュールに関する情報を表示する	<code>job schedule show</code>
ジョブのリストをスケジュール別に表示します	<code>job schedule show-jobs</code>
cron スケジュールに関する情報を表示します	<code>job schedule cron show</code>
インターバルスケジュールに関する情報を表示します	<code>job schedule interval show</code>
cron スケジュールを作成します	<code>job schedule cron create</code>  ONTAP 9.10.1以降では、SVMをジョブスケジュールに含めることができます。

状況	使用するコマンド
インターバルスケジュールを作成します	<pre>job schedule interval create</pre> <p>次のパラメータの少なくとも1つを指定する必要があります。-days、-hours、-minutes、または -seconds。</p>
cron スケジュールを変更します	<pre>job schedule cron modify</pre>
インターバルスケジュールを変更します	<pre>job schedule interval modify</pre>
スケジュールを削除します	<pre>job schedule delete</pre>
cron スケジュールを削除します	<pre>job schedule cron delete</pre>
インターバルスケジュールを削除します	<pre>job schedule interval delete</pre>

## 関連情報

["ONTAP 9コマンド"](#)

## クラスタ構成のバックアップとリストア（クラスタ管理者のみ）

構成バックアップファイルとは

構成バックアップファイルは、クラスタとクラスタ内のノードが適切に動作するために必要な、設定可能なすべてのオプションに関する情報が含まれているアーカイブファイル（.7z）です。

これらのファイルには、各ノードのローカル設定に加えて、クラスタ全体にレプリケートされる設定が格納されます。構成バックアップファイルは、クラスタの構成のバックアップとリストアに使用します。

構成バックアップファイルには、次の 2 種類があります。

- \* ノード構成バックアップファイル \*

クラスタ内の正常なノードにはそれぞれノード構成バックアップファイルが含まれています。このファイルには、クラスタ内でノードの動作の正常性を確保するために必要な、すべての設定情報とメタデータが含まれています。

- \* クラスタ構成バックアップファイル \*

クラスタ内のすべてのノード構成バックアップファイルのアーカイブ、およびレプリケートされたクラスタ構成情報（レプリケートされたデータベース、RDB ファイル）が含まれます。クラスタ構成バックアップファイルを使用すると、クラスタ全体またはクラスタ内の任意のノードの設定をリストアできます。クラスタ構成バックアップスケジュールを使用すると、これらのファイルが自動的に作成され、クラスタ内の複数のノードに格納されます。



構成バックアップファイルには、構成情報のみが含まれています。ユーザデータは含まれていません。ユーザデータのリストアの詳細については、を参照してください "[データ保護](#)"。

ノードおよびクラスタ構成を自動的にバックアップする方法

3 通りのスケジュールで、クラスタおよびノードの構成バックアップファイルが自動的に作成され、クラスタ内のノード間で複製します。

構成バックアップファイルは、次のスケジュールに従って自動的に作成されます。


- 8時間ごと
- 毎日
- 毎週


それぞれのスケジュールで、クラスタ内の正常な各ノードにノード構成バックアップファイルが作成されます。これらのすべてのノード構成バックアップファイルが、レプリケートされたクラスタ構成とともに単一のクラスタ構成バックアップファイルに収集され、クラスタ内の 1 つ以上のノードに保存されます。

構成バックアップスケジュールの管理用コマンド

を使用できます `system configuration backup settings` 構成バックアップスケジュールを管理するコマンド。

これらのコマンドは advanced 権限レベルで使用できます。

状況	使用するコマンド
構成バックアップスケジュールの設定を変更します。  • クラスタ内のデフォルトの場所に加えて構成バックアップファイルがアップロードされるリモート URL（HTTP、HTTPS、FTP、FTPS、または TFTP）を指定する必要があります  • リモート URL へのログインに使用するユーザ名を指定します  • 各構成バックアップスケジュールで保持するバックアップ数を設定します	<code>system configuration backup settings modify</code>  リモートURLでHTTPSを使用する場合は、を使用します <code>-validate-certification</code> デジタル証明書の検証を有効または無効にするオプション。証明書の検証はデフォルトでは無効になっています。  <div> 構成バックアップファイルのアップロード先の Web サーバで、HTTP の場合は PUT 処理、HTTPS の場合は POST 処理が有効になっている必要があります。詳細については、Web サーバのマニュアルを参照してください。</div>
リモート URL へのログインに使用するパスワードを設定します	<code>system configuration backup settings set-password</code>


状況	使用するコマンド
構成バックアップスケジュールの設定を表示します	<pre>system configuration backup settings show</pre> <div>  <p>を設定します -instance パラメータを使用して、各スケジュールで保持するバックアップのユーザ名と数を表示します。</p> </div>

#### 構成バックアップファイルを管理するコマンド

を使用します `system configuration backup` クラスタとノードの構成バックアップファイルを管理するコマンド。

これらのコマンドは `advanced` 権限レベルで使用できます。

状況	使用するコマンド
新しいノードまたはクラスタの構成バックアップファイルを作成します	<pre>system configuration backup create</pre>
クラスタ内のノードから別のノードに構成バックアップファイルをコピーする	<pre>system configuration backup copy</pre>
クラスタ内のノードからリモート URL（FTP、HTTP、HTTPS、TFTP、または FTPS）に構成バックアップファイルをアップロードする	<pre>system configuration backup upload</pre> <p>リモートURLでHTTPSを使用する場合は、を使用します <code>-validate-certification</code> デジタル証明書の検証を有効または無効にするオプション。証明書の検証はデフォルトでは無効になっています。</p> <div>  <p>構成バックアップファイルのアップロード先の Web サーバで、HTTP の場合は PUT 処理、HTTPS の場合は POST 処理が有効になっている必要があります。Web サーバーによっては、追加モジュールのインストールが必要な場合があります。詳細については、Web サーバのマニュアルを参照してください。サポートされる URL 形式は ONTAP リリースによって異なります。使用している ONTAP バージョンのコマンドラインヘルプを参照してください。</p> </div>

状況	使用するコマンド
リモートの URL からクラスタ内のノードに構成バックアップファイルをダウンロードし、指定されている場合はデジタル証明書を検証する	<pre>system configuration backup download</pre> <p>リモートURLでHTTPSを使用する場合は、を使用します <code>-validate-certification</code> デジタル証明書の検証を有効または無効にするオプション。証明書の検証はデフォルトでは無効になっています。</p>
クラスタ内のノードで構成バックアップファイルの名前を変更する	<pre>system configuration backup rename</pre>
クラスタ内の 1 つ以上のノードについて、ノードおよびクラスタの構成バックアップファイルを表示する	<pre>system configuration backup show</pre>
ノード上の構成バックアップファイルを削除する	<pre>system configuration backup delete</pre> <div>  <p>このコマンドを実行すると、指定したノードにある構成バックアップファイルだけが削除されます。クラスタ内の他のノードにも構成バックアップファイルが存在する場合、それらのノードには残ります。</p> </div>

ノードのリカバリに使用する構成バックアップファイルを検索します

ノード構成をリカバリするには、リモート URL またはクラスタ内のノードにある構成バックアップファイルを使用します。

このタスクについて

ノード構成をリストアするには、クラスタまたはノード構成バックアップファイルのいずれかを使用します。

ステップ

1. 構成のリストアに必要なノードに構成バックアップファイルを利用できるようにします。

構成バックアップファイルの場所	作業
リモート URL	<p>を使用します <code>system configuration backup download</code> リカバリするノードにダウンロードするコマンドをadvanced権限レベルで実行します。</p>

構成バックアップファイルの場所	作業
クラスタのノード	<p>a. を使用します <code>system configuration backup show</code> リカバリするノードの構成を含むクラスタで使用可能な構成バックアップファイルのリストを表示するには、advanced権限レベルでコマンドを実行します。</p> <p>b. 特定した構成バックアップファイルがリカバリノードに存在しない場合は、を使用します <code>system configuration backup copy</code> コマンドを使用してリカバリノードにコピーします。</p>

以前にクラスタを作成し直したことがある場合は、クラスタの再作成後に作成した構成バックアップファイルを選択します。クラスタの再作成の前に作成した構成バックアップファイルを使用する必要がある場合は、ノードをリカバリしたあとで、クラスタを再度作成する必要があります。

## 構成バックアップファイルを使用してノード構成をリストアする

ノード構成をリストアするには、特定し、リカバリノードに利用可能にした構成バックアップファイルを使用します。

### このタスクについて

ノードのローカル構成ファイルが失われた障害からリカバリするには、このタスクのみを実行する必要があります。

### 手順

1. advanced 権限レベルに切り替えます。

```
set -privilege advanced
```

2. ノードが正常な場合は、別のノードのadvanced権限レベルでを使用します `cluster modify` コマンドに指定します `-node` および `-eligibility` クラスタへの参加資格を無効にし、クラスタから分離するためのパラメータ。

ノードが正常でない場合は、この手順を省略する必要があります。

この例では、`node2` を変更してクラスタへ参加させないようにし、構成をリストアできるようにします。

```
cluster1::*> cluster modify -node node2 -eligibility false
```

3. を使用します `system configuration recovery node restore` コマンドをadvanced権限レベルで実行し、ノード構成を構成バックアップファイルからリストアします。

名前も含めてノードのIDが失われた場合は、を使用してください `-nodename-in-backup` 構成バックアップファイル内のノード名を指定するパラメータ。

この例では、ノードに保存されている構成バックアップファイルの 1 つを使用してノードの構成をリスト



アします。

```
cluster1::*> system configuration recovery node restore -backup  
cluster1.8hour.2011-02-22.18_15_00.7z
```

```
Warning: This command overwrites local configuration files with  
files contained in the specified backup file. Use this  
command only to recover from a disaster that resulted  
in the loss of the local configuration files.  
The node will reboot after restoring the local configuration.  
Do you want to continue? {y|n}: y
```

構成がリストアされ、ノードがリブートします。

4. ノードをクラスタの対象外にした場合は、を使用します `system configuration recovery cluster sync` コマンドを実行してノードを適格とマークし、クラスタと同期します。
5. SAN環境を使用している場合は、を使用します `system node reboot` コマンドを使用してノードをリブートし、SANウォーラムを再確立します。

完了後

以前にクラスタを作成し直したことがある場合、またクラスタの再作成前に作成された構成バックアップファイルを使用してノード構成をリストアする場合は、再度クラスタを作成し直す必要があります。

クラスタのリカバリに使用する構成を検索します

クラスタ内のノード、またはクラスタ構成バックアップファイルのいずれかの構成を使用してクラスタをリカバリできます。

手順

1. クラスタのリカバリに使用する構成の種類を選択します。

- クラスタ内のノード

クラスタが複数のノードで構成されていて、クラスタが適切な構成であった時点からのクラスタ構成がいずれかのノードにある場合は、そのノードに格納された構成を使用してクラスタをリカバリできます。

ほとんどの場合、クラスタ構成のリストアには、最新のトランザクション ID を持つレプリケーションリングが含まれているノードが最適です。。 `cluster ring show advanced` 権限レベルでコマンドを実行すると、クラスタ内の各ノードで使用可能なレプリケートリングのリストを表示できます。

- クラスタ構成バックアップファイル

適切なクラスタ構成を持つノードが特定できない場合、またはクラスタがシングルノードで構成されている場合は、クラスタ構成バックアップファイルを使用してクラスタをリカバリできます。

クラスタを構成バックアップファイルからリカバリする場合は、バックアップ後に行われた構成変更はすべて失われます。リカバリ後に構成バックアップファイルと現在の設定との矛盾をすべて解決しておく必要があります。技術情報アーティクルを参照してください ["ONTAP 構成バックアップ解決ガイド"](#) を参照

してください。

2. クラスタ構成バックアップファイルを使用する場合は、クラスタのリカバリに使用するノードでそのファイルを利用できるようにします。

構成バックアップファイルの場所	作業
リモート URL	を使用します system configuration backup download リカバリするノードにダウンロードするコマンドをadvanced権限レベルで実行します。
クラスタのノード	<p>a. を使用します system configuration backup show advanced権限レベルでコマンドを実行し、クラスタが適切な構成であったときに作成されたクラスタ構成バックアップファイルを検索します。</p> <p>b. クラスタのリカバリに使用するノード上にクラスタ構成バックアップファイルがない場合は、を使用します system configuration backup copy コマンドを使用してリカバリノードにコピーします。</p>

既存の構成からクラスタ構成をリストアします

クラスタ障害後に既存の構成からクラスタ構成をリストアするには、クラスタ構成を選択してリカバリするノードで利用できるようにし、その構成を使用してクラスタを再作成し、各追加ノードを新しいクラスタに再追加します。

このタスクについて

クラスタ構成の損失となる障害からリカバリするには、このタスクのみを実行する必要があります。



構成バックアップファイルからクラスタを再作成する場合は、テクニカルサポートに連絡して、構成バックアップファイルと現在のクラスタ構成との矛盾をすべて解決する必要があります。

クラスタを構成バックアップファイルからリカバリする場合は、バックアップ後に行われた構成変更はすべて失われます。リカバリ後に構成バックアップファイルと現在の設定との矛盾をすべて解決しておく必要があります。サポート技術情報の記事を参照してください"[トラブルシューティングのガイダンス](#)は、[『ONTAP 構成バックアップ解決ガイド』](#)を参照してください"。

手順

1. 各 HA ペアのストレージフェイルオーバーを無効にします。

```
storage failover modify -node node_name -enabled false
```

ストレージフェイルオーバーを無効にするのは、各 HA ペアに対して 1 度だけです。ノードのストレージフェイルオーバーを無効にすると、そのノードのパートナーでもストレージフェイルオーバーが無効になります。

2. リカバリするノード以外の各ノードを停止します。

```
system node halt -node node_name -reason "text"
```

```
cluster1::*> system node halt -node node0 -reason "recovering cluster"

Warning: Are you sure you want to halt the node? {y|n}: y
```

3. 権限レベルを advanced に設定します。

```
set -privilege advanced
```

4. リカバリノードで、を使用します **system configuration recovery cluster recreate** コマンドを使用してクラスタを再作成します。

この例では、リカバリノードに保存された構成情報を使用してクラスタを再作成します。

```
cluster1::*> configuration recovery cluster recreate -from node

Warning: This command will destroy your existing cluster. It will
        rebuild a new single-node cluster consisting of this node
        and its current configuration. This feature should only be
        used to recover from a disaster. Do not perform any other
        recovery operations while this operation is in progress.
Do you want to continue? {y|n}: y
```

リカバリノードに新しいクラスタが作成されます。

5. 構成バックアップファイルからクラスタを再作成する場合は、クラスタのリカバリがまだ進行中であることを確認します。

```
system configuration recovery cluster show
```

正常なノードからクラスタを再作成する場合、クラスタのリカバリの状態を確認する必要はありません。

```
cluster1::*> system configuration recovery cluster show
Recovery Status: in-progress
Is Recovery Status Persisted: false
```

6. 再作成したクラスタに再追加が必要な各ノードをブートします。

ノードは一度に 1 つずつリブートする必要があります。

7. 再作成したクラスタに再追加が必要な各ノードで、次の作業を行います。

- a. 再作成したクラスタ上の正常なノードから、ターゲットノードを再追加します。

```
system configuration recovery cluster rejoin -node node_name
```

この例では 'ターゲット・ノードを再作成されたクラスタに再結合します

```
cluster1::*> system configuration recovery cluster rejoin -node node2

Warning: This command will rejoin node "node2" into the local
cluster, potentially overwriting critical cluster
configuration files. This command should only be used
to recover from a disaster. Do not perform any other
recovery operations while this operation is in progress.
This command will cause node "node2" to reboot.
Do you want to continue? {y|n}: y
```

ターゲットノードがリブートし、クラスタに追加されます。

- b. ターゲットノードが正常であり、クラスタ内の残りのノードとクォーラムを形成していることを確認します。

```
cluster show -eligibility true
```

別のノードを再追加する前に、ターゲットノードを再作成したクラスタに再追加する必要があります。

```
cluster1::*> cluster show -eligibility true
Node           Health Eligibility Epsilon
-----
node0           true   true      false
node1           true   true      false
2 entries were displayed.
```

8. 構成バックアップファイルからクラスタを再作成した場合は、リカバリステータスを「complete」に設定します。

```
system configuration recovery cluster modify -recovery-status complete
```

9. admin 権限レベルに戻ります。

```
set -privilege admin
```

10. クラスタが2つのノードだけで構成されている場合は、を使用します **cluster ha modify** クラスタHAを再度有効にするコマンド。
11. を使用します **storage failover modify** 各HAペアのストレージフェイルオーバーを再度有効にするコマンド。

完了後

クラスタに SnapMirror ピア関係がある場合は、それらの関係も再作成する必要があります。詳細について

は、を参照してください ["データ保護"](#)。

ノードをクラスタと同期します

クラスタ全体のクォーラムが存在するものの、1つ以上のノードがクラスタと同期していない場合は、ノードを同期し、そのノード上でレプリケートされたデータベース（RDB）をリストアしてクォーラムに加える必要があります。

#### ステップ

1. 正常なノードからを使用します `system configuration recovery cluster sync advanced` 権限レベルでコマンドを実行し、クラスタ構成と同期されていないノードを同期します。

次の例では、残りのクラスタとノード（`_node2_`）を同期します。

```
cluster1::*> system configuration recovery cluster sync -node node2
```

```
Warning: This command will synchronize node "node2" with the cluster
configuration, potentially overwriting critical cluster
configuration files on the node. This feature should only be
used to recover from a disaster. Do not perform any other
recovery operations while this operation is in progress. This
command will cause all the cluster applications on node
"node2" to restart, interrupting administrative CLI and Web
interface on that node.
```

```
Do you want to continue? {y|n}: y
```

```
All cluster applications on node "node2" will be restarted. Verify that
the cluster applications go online.
```

#### 結果

RDB がノードにレプリケートされ、そのノードがクラスタに参加できるようになります。

### コアダンプを管理する（クラスタ管理者のみ）

ノードに何らかの障害が発生すると、コアダンプが発生し、システムによってコアダンプファイルが作成されます。このファイルをテクニカルサポートが使用して問題を解決できる可能性があります。コアダンプの属性は、設定または表示できます。コアダンプファイルは、保存、表示、分割、アップロード、または削除することもできます。

コアダンプは、次の方法で管理できます。

- コアダンプの設定および構成設定の表示
- コアダンプの基本情報、ステータス、および属性を表示する

コアダンプファイルおよびレポートはに保存されます `/mroot/etc/crash/` ノードのディレクトリ。を使用して、ディレクトリの内容を表示できます `system node coredump` コマンドまたはWebブラウザ。

- コアダンプの内容の保存と、指定された場所またはテクニカルサポートへの保存済みファイルのアップロード

ONTAP では、テイクオーバー、アグリゲートの再配置、またはギブバック中にコアダンプファイルの保存を開始することはできません。

- 不要になったコアダンプファイルを削除する

## コアダンプの管理用コマンド

を使用します `system node coredump config` コアダンプの設定を管理するコマンド `system node coredump` コアダンプファイルを管理するコマンド、および `system node coredump reports` アプリケーションコアレポートを管理するコマンド。

状況	使用するコマンド
コアダンプを設定する	<code>system node coredump config modify</code>
コアダンプの構成設定を表示する	<code>system node coredump config show</code>
コアダンプに関する基本情報を表示する	<code>system node coredump show</code>
ノードをリブートするときに、コアダンプを手動でトリガーします	<code>system node reboot</code> 両方のを使用します <code>-dump</code> および <code>-skip-lif-migration-before-reboot</code> パラメータ   リンク： <a href="https://docs.netapp.com/us-en/ontap-cli-9141/system-node-reboot.html#parameters[skip-lif-migration-before-reboot]">https://docs.netapp.com/us-en/ontap-cli-9141/system-node-reboot.html#parameters[skip-lif-migration-before-reboot]</a> パラメータを指定すると、リブート前のLIFの移行がスキップされます。
ノードをシャットダウンするときに、コアダンプを手動でトリガーします	<code>system node halt</code> 両方のを使用します <code>-dump</code> および <code>-skip-lif-migration-before-shutdown</code> パラメータ   リンク： <a href="https://docs.netapp.com/us-en/ontap-cli-9141/system-node-halt.html#parameters[skip-lif-migration-before-shutdown]">https://docs.netapp.com/us-en/ontap-cli-9141/system-node-halt.html#parameters[skip-lif-migration-before-shutdown]</a> パラメータを指定すると、シャットダウン前のLIFの移行がスキップされます。
指定したコアダンプを保存します	<code>system node coredump save</code>
指定したノード上で保存されていないすべてのコアダンプを保存します	<code>system node coredump save-all</code>

状況	使用するコマンド
指定したコアダンプファイルを含む AutoSupport メッセージを生成して送信します	<pre>system node autosupport invoke-core-upload</pre> <div>  <p>。 -uri オプションのパラメータは、AutoSupport メッセージの代替送信先を指定します。</p> </div>
コアダンプに関するステータス情報を表示します	<pre>system node coredump status</pre>
指定したコアダンプを削除する	<pre>system node coredump delete</pre>
ノード上で保存されていないすべてのコアダンプ、または保存されているすべてのコアファイルを削除します	<pre>system node coredump delete-all</pre>
アプリケーションコアダンプレポートを表示します	<pre>system node coredump reports show</pre>
アプリケーションコアダンプレポートを削除する	<pre>system node coredump reports delete</pre>

#### 関連情報

["ONTAP 9コマンド"](#)

## ディスクと階層（アグリゲート）の管理

### ディスクとローカル階層（アグリゲート）の概要

ONTAP 物理ストレージは、System ManagerおよびCLIを使用して管理できます。ローカル階層（アグリゲート）の作成、拡張、管理、Flash Poolローカル階層（アグリゲート）の操作、ディスクの管理、RAIDポリシーの管理を行うことができます。

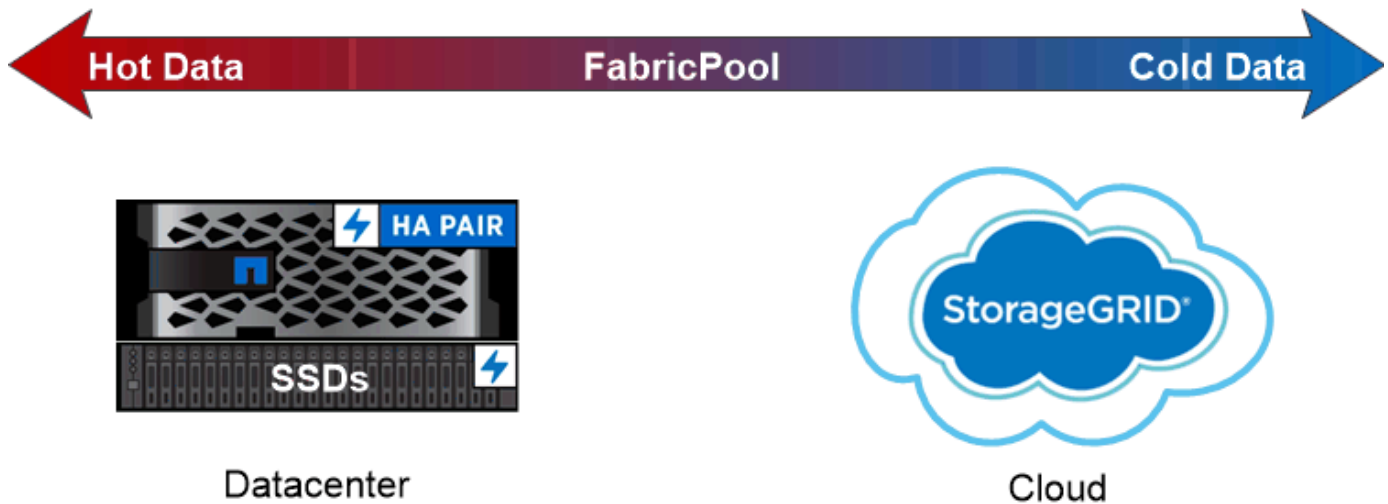
#### ローカル階層（アグリゲート）とは

ローカル階層（別名「\_Aggregates」）は、ノードで管理されるディスクのコンテナです。ローカル階層を使用すると、パフォーマンス要件に応じてワークロードを分離したり、アクセスパターンに応じてデータを階層化したり、規制要件に準拠する目的でデータを分離したりできます。

- レイテンシを最小限に抑えながらパフォーマンスを最大限に高めることが求められるビジネスクリティカルなアプリケーションに対しては、SSDだけで構成されるローカル階層を作成できます。
- アクセスパターンに応じてデータを階層化する場合は、\_hybrid local tier\_を作成し、作業データセットにはフラッシュを導入して高性能なキャッシュを利用しながら、アクセス頻度が低いデータには低コストのHDDやオブジェクトストレージを使用することができます。
  - a\_Flash Poolは、SSDとHDDの両方で構成されます。
  - a\_ssd FabricPool\_は、オブジェクトストアが接続されたオールSSDローカル階層で構成されています。

す。

- 規制要件に準拠する目的でアクティブなデータとは別にアーカイブデータを保持する必要がある場合は、大容量HDDのみ、またはハイパフォーマンスHDDと大容量HDDで構成されるローカル階層を使用できます。



*You can use a FabricPool to tier data with different access patterns, deploying SSDs for frequently accessed “hot” data and object storage for rarely accessed “cold” data.*

ローカル階層（アグリゲート）の使用

次のタスクを実行できます。

- ["ローカル階層（アグリゲート）の管理"](#)
- ["ディスクを管理する"](#)
- ["RAID構成を管理します"](#)
- ["Flash Pool階層を管理します"](#)

次の条件に該当する場合は、これらのタスクを実行します。

- 自動スクリプトツールを使用しない場合。
- すべての選択肢について検討するのではなく、ベストプラクティスに従う。
- MetroCluster 構成を使用しており、の手順に従っている ["MetroCluster"](#) ローカル階層（アグリゲート）とディスクの管理に関する初期設定とガイドラインについては、ドキュメントを参照してください。

関連情報

- ["FabricPool クラウド階層を管理します"](#)

ローカル階層（アグリゲート）の管理



System ManagerまたはONTAP CLIを使用して、ローカル階層（アグリゲート）の追加、使用管理、データ（ディスク）の追加を行うことができます。

次のタスクを実行できます。

- ["ローカル階層（アグリゲート）の追加（作成）"](#)

ローカル階層を追加するには、特定のワークフローに従います。ローカル階層に必要なディスクまたはディスクパーティションの数を決定し、どの方法を使用してローカル階層を作成するかを決定します。ローカル階層は、ONTAP に構成の割り当てを任せることで自動的に追加できます。また、構成を手動で指定することもできます。

- ["ローカル階層（アグリゲート）の使用の管理"](#)

既存のローカル階層については、名前の変更、メディアコストの設定、またはドライブとRAIDグループの情報の決定を行うことができます。ローカル階層のRAID構成を変更し、Storage VM（SVM）にローカル階層を割り当てることができます。

ローカル階層のRAID構成を変更し、Storage VM（SVM）にローカル階層を割り当てることができます。ローカル階層に配置されているボリュームと、それらがローカル階層で使用しているスペースを確認できます。ボリュームが使用できるスペースの量を制御できます。HAペアを使用してローカル階層の所有権を切り替えることができます。ローカル階層を削除することもできます。

- ["ローカル階層（アグリゲート）に容量（ディスク）を追加"](#)

さまざまな方法を使用して、特定のワークフローに従って容量を追加します。ローカル階層にディスクを追加し、ノードまたはシェルフにドライブを追加できます。必要に応じて、ミスアライメントされたスペアパーティションを修正できます。

## ローカル階層（アグリゲート）の追加（作成）

ローカル階層を追加（アグリゲートを作成）

ローカル階層を追加する（アグリゲートを作成する）には、特定のワークフローに従います。

ローカル階層に必要なディスクまたはディスクパーティションの数を決定し、どの方法を使用してローカル階層を作成するかを決定します。ローカル階層は、ONTAP に構成の割り当てを任せることで自動的に追加できます。また、構成を手動で指定することもできます。

- ["ローカル階層（アグリゲート）を追加するワークフロー"](#)
- ["ローカル階層（アグリゲート）に必要なディスクまたはディスクパーティションの数を確認する"](#)
- ["使用するローカル階層（アグリゲート）の作成方法を決定します"](#)
- ["ローカル階層（アグリゲート）を自動的に追加する"](#)
- ["ローカル階層（アグリゲート）を手動で追加してください"](#)

ローカル階層（アグリゲート）を追加するワークフロー

ローカル階層（アグリゲート）を作成すると、システム上のボリュームにストレージが提供されます。

ローカル階層（アグリゲート）を作成するワークフローは、使用するインターフェイスに固有のもので  
す。System ManagerまたはCLIを使用します。

### **System Manager**のワークフロー

- System Managerを使用して、ローカル階層を追加（作成）\*します

System Managerでは、ローカル階層を設定するための推奨されるベストプラクティスに基づいてローカル階層が作成されます。

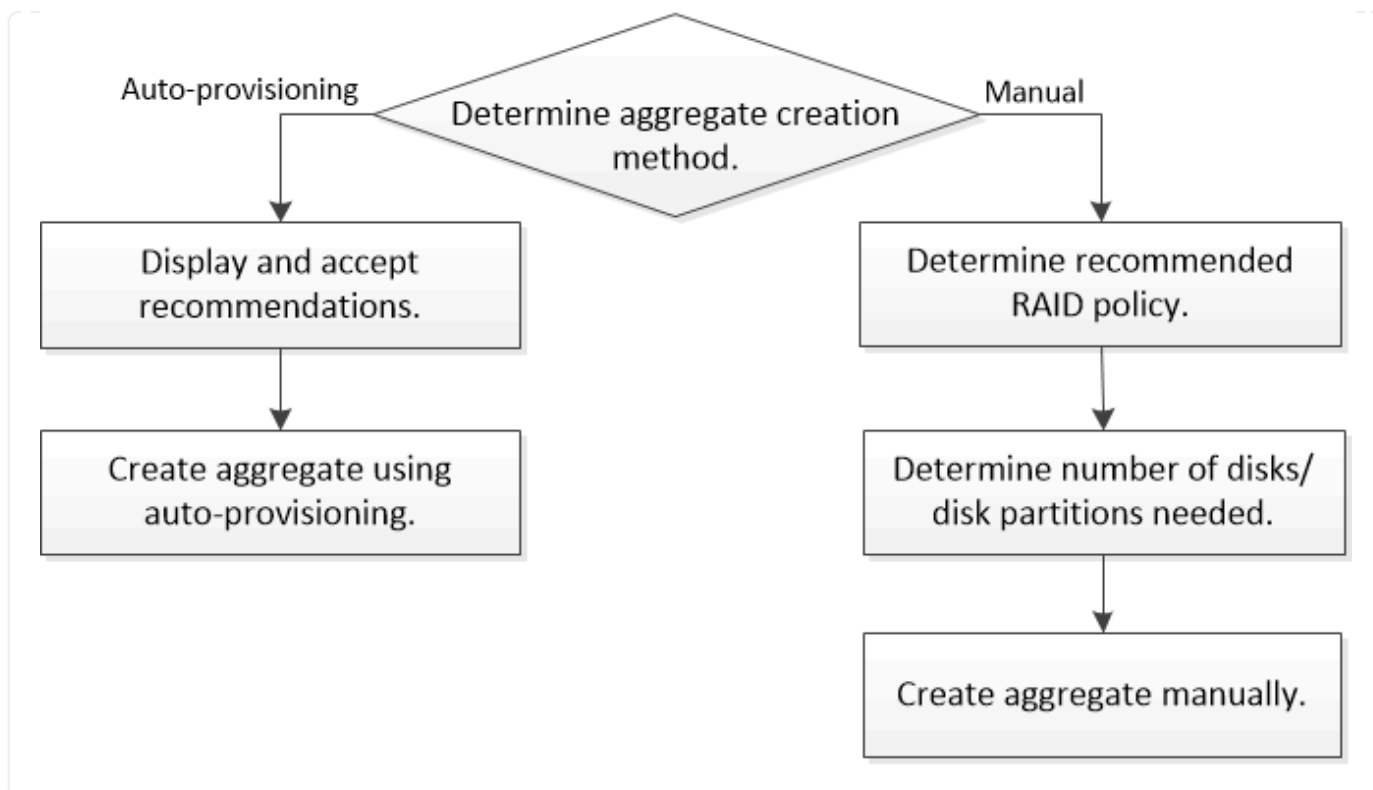
ONTAP 9.11.1以降では、自動プロセスでローカル階層を追加する際に推奨される設定と異なる設定が必要な場合に、ローカル階層を手動で設定できます。



#### CLIワークフロー

- CLIを使用して、アグリゲートを追加（作成）\*します

ONTAP 9.2以降では、アグリゲートの作成時にONTAP の推奨構成を使用できます（自動プロビジョニング）。ベストプラクティスに基づいた推奨構成がご使用の環境に適している場合は、それらの構成を承認してアグリゲートを作成することもできます。アグリゲートを手動で作成することもできます。



ローカル階層（アグリゲート）に必要なディスクまたはディスクパーティションの数を確認する

システムとビジネスの要件を満たす十分な数のディスクまたはディスクパーティションがローカル階層（アグリゲート）に必要です。また、データ損失の可能性を最小限に抑えるために、推奨される数のホットスペアディスクまたはホットスペアディスクパーティションも用意する必要があります。

ルートデータのパーティショニングは、特定の構成においてデフォルトで有効になります。ルート/データパーティショニングが有効になっているシステムでは、ディスクパーティションを使用してローカル階層を作成します。ルート/データパーティショニングが有効になっていないシステムでは、パーティショニングされていないディスクを使用します。

RAID ポリシーに必要な最小数および容量の最小要件を満たす十分な数のディスクまたはディスクパーティションが必要になります。



ONTAP では、ドライブの使用可能スペースがドライブの物理容量よりも少なくなります。特定のドライブの使用可能スペース、および各RAIDポリシーに必要なディスクまたはディスクパーティションの最小数をに記載します ["Hardware Universe"](#)。

特定のディスクの使用可能なスペースを確認します


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

## System Manager の略

- System Managerを使用して、ディスクの使用可能スペースを確認します。\*

ディスクの使用可能なサイズを表示するには、次の手順を実行します。

### 手順

1. 「\*ストレージ」>「階層」に移動します
2. をクリックします  をクリックします。
3. [ディスク情報]タブを選択します。

### CLI の使用

- CLIを使用して、ディスクの使用可能スペースを確認してください。\*

ディスクの使用可能なサイズを表示するには、次の手順を実行します。

### ステップ

1. スペアディスク情報を表示します。

```
storage aggregate show-spare-disks
```

RAID グループを作成して容量の要件を満たすために必要なディスクまたはディスクパーティションの数に加えて、アグリゲートに推奨されるホットスペアディスクまたはホットスペアディスクパーティションの最小数を確保しておく必要があります。

- オールフラッシュアグリゲートには、少なくとも 1 つのホットスペアディスクまたはディスクパーティションが必要です。



AFF C190 には、デフォルトでスペアドライブはありません。この例外は完全にサポートされています。

- フラッシュ以外の同種のアグリゲートには、少なくとも 2 つのホットスペアディスクまたはディスクパーティションが必要です。
- SSD ストレージプールの場合、HA ペアごとに少なくとも 1 つのホットスペアディスクを用意しておく必要があります。
- Flash Pool アグリゲートの場合は、HA ペアごとに少なくとも 2 つのスペアディスクが必要です。Flash Pool アグリゲートでサポートされる RAID ポリシーの詳細については、を参照してください ["Hardware Universe"](#)。
- Maintenance Center を使用できるようにし、同時に複数のディスク障害が発生した場合の問題を回避するには、マルチディスクキャリアに少なくとも 4 つのホットスペアが必要です。

## 関連情報

["NetApp Hardware Universe の略"](#)

["ネットアップテクニカルレポート 3838 : 『 Storage Subsystem Configuration Guide 』"](#)

ローカル階層（アグリゲート）の作成方法を決定する

ONTAP ではローカル階層の自動追加（自動プロビジョニングを使用したアグリゲートの作成）に関するベストプラクティスの推奨事項が提供されますが、お使いの環境で推奨される構成がサポートされているかどうかを確認する必要があります。サポートされていない場合は、使用するRAIDポリシーとディスク構成を決定し、ローカル階層を手動で作成する必要があります。

ローカル階層が自動的に作成されると、ONTAP はクラスタ内の使用可能なスペアディスクを分析し、ベストプラクティスに従ってスペアディスクを使用してローカル階層を追加する方法に関する推奨事項を生成します。推奨構成がONTAP に表示されます。推奨構成を承認するか、ローカル階層を手動で追加できます。

### ONTAP の推奨事項を受け入れる前に

次のいずれかのディスク条件が存在する場合は、ONTAP からの推奨事項を受け入れる前にそれらに対処する必要があります。

- ディスクが不足している
- スペアディスクの数が安定しない
- 未割り当てディスク
- スペアが初期化されていません
- ディスクがメンテナンステスト中である

。storage aggregate auto-provision のマニュアルページに、これらの要件の詳細が記載されています。

### 手動方式を使用する必要がある場合

多くの場合、ローカル階層の推奨レイアウトは環境に最適です。ただし、クラスタがONTAP 9.1以前を実行している場合、または次の構成が環境に含まれている場合は、手動でローカル階層を作成する必要があります。



ONTAP 9.11.1以降では、System Managerを使用してローカル階層を手動で追加できます。

- サードパーティ製アレイ LUN を使用するアグリゲート
- Cloud Volumes ONTAP または ONTAP Select を使用した仮想ディスク
- MetroCluster システム
- SyncMirror
- MSATA ディスク
- FlashPool階層（アグリゲート）
- 複数のタイプまたはサイズのディスクがノードに接続されている場合

ローカル階層（アグリゲート）を作成する方法を選択してください

使用する方法を選択します。

- ["ローカル階層（アグリゲート）を自動的に追加（作成）"](#)

- ["ローカル階層（アグリゲート）を手動で追加（作成）します"](#)

## 関連情報

### ["ONTAP 9 のコマンド"](#)

ローカル階層を自動的に追加する（自動プロビジョニングを使用してアグリゲートを作成する）

ONTAPでローカル階層を自動的に追加する（自動プロビジョニングを使用してアグリゲートを作成する）ことが推奨されるベストプラクティスに従っている場合は環境に適しています。推奨された構成を承認し、ONTAPでローカル階層を追加することもできます。

#### 作業を開始する前に

ディスクをローカル階層（アグリゲート）で使用するには、ディスクがノードに所有されていなければなりません。ディスク所有権の自動割り当てを使用するようにクラスタが設定されていない場合は、["所有権を手動で割り当てる"](#)。



## System Manager の略

### 手順

1. System Manager で、 \* Storage > Tiers \* をクリックします。
2. [\*Tiers]ページで、をクリックします **+ Add Local Tier** 新しいローカル階層を作成するには、次の手順を実行し

Add Local Tier \*ページには、ノード上に作成できるローカル階層と使用可能なストレージが推奨数で表示されます。

3. 推奨構成の詳細を表示するには、\* Recommended details \*をクリックします。

ONTAP 9.8以降のSystem Managerでは、次の情報が表示されます。

- ローカル階層名（ONTAP 9.10.1で始まるローカル階層名を編集できます）
- \* ノード名 \*
- 使用可能なサイズ
- ストレージの種類

ONTAP 9.10.1以降では、追加情報 が表示されます。

- ディスク：ディスクの数、サイズ、タイプが表示されます
- レイアウト：RAIDグループのレイアウトを示します。ディスクがパリティかデータか、どのスロットが未使用かなどが含まれます。
- スペアディスク：ノード名、スペアディスクの数とサイズ、およびストレージのタイプが表示されます。

4. 次のいずれかの手順を実行します。

実行する処理	操作
System Managerからの推奨事項を承認します。	に進みます <a href="#">暗号化用にオンボードキーマネージャを設定する手順</a> 。
ローカル階層を手動で設定し、System Managerの推奨事項を使用して「_not_」を設定します。	に進みます <a href="#">"ローカル階層を手動で追加（アグリゲートの作成）します"</a> ： <ul style="list-style-type: none"><li>• ONTAP 9.10.1以前の場合は、次の手順に従ってCLIを使用します。</li><li>• ONTAP 9.11.1以降では、System Managerの使用手順に従います。</li></ul>

5. （オプション）：オンボードキーマネージャがインストールされている場合は、暗号化を設定できます。Configure Onboard Key Manager for encryption \*チェックボックスをオンにします。
  - a. パスフレーズを入力します。
  - b. パスフレーズを確認のためにもう一度入力します。

c. パスフレーズは、あとでシステムのリカバリが必要になったときのために保存しておきます。

d. あとで使用できるように、キーデータベースをバックアップしておきます。

6. 保存\*をクリックしてローカル階層を作成し、ストレージ解決策 に追加します。

## CLI の使用

を実行します `storage aggregate auto-provision` アグリゲートレイアウトの推奨事項を生成するコマンド。ONTAP の推奨事項を確認および承認したあとでアグリゲートを作成できます。

### 必要なもの

9.2 以降がクラスタで実行されている必要があります。ONTAP

### このタスクについて

で生成されるデフォルトの概要 `storage aggregate auto-provision` コマンドを実行すると、作成が推奨されるアグリゲートのリスト（名前や使用可能なサイズなど）が表示されます。リストを確認し、プロンプトに従って推奨されるアグリゲートを作成するかどうかを判断できます。

を使用して詳細な概要を表示することもできます `-verbose` オプション。次のレポートが表示されます。

- 作成する新しいアグリゲートのノードごとの概要、検出されたスペア、アグリゲートの作成後の残りのスペアディスクとパーティション
- 作成する新しいデータアグリゲートと、使用されるディスクおよびパーティションの数
- 作成する新しいデータアグリゲートにおけるスペアディスクとパーティションの使用方法を示す RAID グループのレイアウト
- アグリゲートの作成後の残りのスペアディスクとパーティションの詳細

自動プロビジョニング方法に精通していて、環境の準備が整っている場合は、を使用できます `-skip -confirmation` 表示と確認を行わずに推奨されるアグリゲートを作成するオプション。。 `storage aggregate auto-provision` コマンドはCLIセッションの影響を受けません `-confirmations` 設定：

。[`storage aggregate auto-provision` のマニュアルページ<sup>4</sup>]には、アグリゲートレイアウトに関する推奨事項の詳細が記載されています。

### 手順

1. を実行します `storage aggregate auto-provision` 必要な表示オプションを指定したコマンド。
  - オプションなし：標準の概要を表示します
  - `-verbose` オプション：詳細な概要を表示します
  - `-skip-confirmation` オプション：表示も確認もせずに推奨されるアグリゲートを作成します
2. 次のいずれかの手順を実行します。

実行する処理	操作
--------	----

ONTAP からの推奨事項を受け入れます。

推奨されるアグリゲートの表示を確認し、プロンプトに従って推奨されるアグリゲートを作成します。

```
myA400-44556677::> storage aggregate auto-
provision
Node                               New Data Aggregate
Usable Size
-----
myA400-364                         myA400_364_SSD_1
3.29TB
myA400-363                         myA400_363_SSD_1
1.46TB
-----
Total:                             2    new data aggregates
4.75TB

Do you want to create recommended
aggregates? {y
```

n}: y

Info: Aggregate auto provision has started. Use the "storage aggregate show-auto-provision-progress" command to track the progress.

myA400-44556677::>

----

ローカル階層を手動で設定し、ONTAP からの推奨事項を使用する\*\_not\_\*。

## 関連情報

### "ONTAP 9コマンド"

ローカル階層を手動で追加（アグリゲートを作成

ONTAP のベストプラクティスの推奨事項を使用してローカル階層を追加（アグリゲートを作成）しない場合は、このプロセスを手動で実行できます。

作業を開始する前に

ディスクをローカル階層（アグリゲート）で使用するには、ディスクがノードに所有されていなければなりません。ディスク所有権の自動割り当てを使用するようにクラスタが設定されていない場合は、["所有権を手動で割り当てる"](#)。

## System Manager の略

ONTAP 9.11.1以降では、System Managerの推奨設定を使用してローカル階層を作成しない場合は、希望する設定を指定できます。

### 手順

1. System Manager で、 \* Storage > Tiers \* をクリックします。
2. [\*Tiers]ページで、をクリックします  新しいローカル階層を作成するには、次の手順を実行し

Add Local Tier \*ページには、ノード上に作成できるローカル階層と使用可能なストレージが推奨数で表示されます。

3. System Managerでローカル階層に対するストレージの推奨が表示されたら、「スペアディスク」セクションの「ローカル階層の手動作成に切り替え」をクリックします。

[Add Local Tier]ページには、ローカル階層の設定に使用するフィールドが表示されます。

4. ローカル階層の追加\*ページの最初のセクションで、次の手順を実行します。
  - a. ローカル階層の名前を入力します。
  - b. (オプション) : ローカル階層をミラーリングする場合は、[このローカル階層をミラーリングする\*]チェックボックスをオンにします。
  - c. ディスクタイプを選択します。
  - d. ディスク数を選択します。
5. [RAID Configuration]セクションで、次の手順を実行します。
  - a. RAIDタイプを選択します。
  - b. RAIDグループサイズを選択します。
  - c. RAID allocationをクリックして、グループ内のディスクの割り当て状況を表示します。
6. (オプション) : オンボードキーマネージャがインストールされている場合は、ページの\* Encryption \*セクションで暗号化を設定できます。Configure Onboard Key Manager for encryption \* チェックボックスをオンにします。
  - a. パスフレーズを入力します。
  - b. パスフレーズを確認のためにもう一度入力します。
  - c. パスフレーズは、あとでシステムのリカバリが必要になったときのために保存しておきます。
  - d. あとで使用できるように、キーデータベースをバックアップしておきます。
7. 保存\*をクリックしてローカル階層を作成し、ストレージ解決策 に追加します。

### CLI の使用

アグリゲートを手動で作成する前に、ディスク構成オプションを確認して作成をシミュレートする必要があります。

次に、を問題 できます `storage aggregate create` コマンドを実行し、結果を確認します。

### 必要なもの

アグリゲートに必要なディスクの数とホットスペアディスクの数を決めておく必要があります。

このタスクについて

ルート/データ/データパーティショニングが有効になっていて、構成に含まれるソリッドステートドライブ (SSD) の数が24本以下の場合は、データパーティションを別々のノードに割り当てることを推奨します。

ルート/データパーティショニングとルート/データ/データパーティショニングが有効になっているシステムでアグリゲートを作成するための手順は、パーティショニングされていないディスクを使用するシステムでアグリゲートを作成するための手順と同じです。システムでルート/データパーティショニングが有効になっている場合は、にディスクパーティションの数を使用する必要があります -diskcount オプションルート/データ/データパーティショニングの場合は、 -diskcount optionは、使用するディスクの数を指定します。



FlexGroup で使用する複数のアグリゲートを作成する場合は、アグリゲートのサイズを可能な限り同じにする必要があります。

。 storage aggregate create のマニュアルページには、アグリゲートの作成オプションと要件の詳細が記載されています。

手順

1. スペアディスクパーティションのリストを表示して、アグリゲートの作成に十分な数のパーティションがあることを確認します。

```
storage aggregate show-spare-disks -original-owner node_name
```

データパーティションはに表示されます Local Data Usable。ルートパーティションをスペアとして使用することはできません。

2. アグリゲートの作成をシミュレートします。

```
storage aggregate create -aggregate aggregate_name -node node_name  
-raidtype raid_dp -diskcount number_of_disks_or_partitions -simulate true
```

3. シミュレートしたコマンドから警告が表示された場合は、コマンドを調整してシミュレーションを繰り返します。
4. アグリゲートを作成します。

```
storage aggregate create -aggregate aggr_name -node node_name -raidtype  
raid_dp -diskcount number_of_disks_or_partitions
```

5. アグリゲートを表示して、作成されたことを確認します。

```
storage aggregate show-status aggregate_name
```

関連情報

["ONTAP 9 のコマンド"](#)

## ローカル階層（アグリゲート）の使用の管理

### ローカル階層（アグリゲート）の使用の管理

ローカル階層（アグリゲート）を作成したあと、それらの使用方法を管理できます。

次のタスクを実行できます。

- "ローカル階層の名前変更（アグリゲート）"
- "ローカル階層（アグリゲート）のメディアコストの設定"
- "ローカル階層（アグリゲート）のドライブおよびRAIDグループの情報を確認する"
- "ローカル階層（アグリゲート）をStorage VM（SVM）に割り当てる"
- "ローカル階層（アグリゲート）に配置するボリュームを決定する"
- "ローカル階層（アグリゲート）でのボリュームのスペース使用量を確認および制御する"
- "ローカル階層（アグリゲート）のスペース使用量を判定する"
- "HAペア内でローカル階層（アグリゲート）の所有権を切り替えます"
- "ローカル階層（アグリゲート）を削除する"

### ローカル階層の名前変更（アグリゲート）


ローカル階層（アグリゲート）の名前は変更できます。実行する方法は、使用するインターフェイスによって異なります。System ManagerまたはCLIを使用します。

## System Manager の略

- System Managerを使用して、ローカル階層（アグリゲート）の名前を変更します。\*

ONTAP 9.10.1以降では、ローカル階層（アグリゲート）の名前を変更できます。

### 手順

1. System Manager で、\* Storage > Tiers \* をクリックします。
2. をクリックします  をクリックします。
3. [ 名前の変更 \* ] を選択します。
4. ローカル階層の新しい名前を指定します。

### CLI の使用

- CLIを使用して、ローカル階層（アグリゲート）の名前を変更します。\*

### ステップ

1. CLIを使用して、ローカル階層（アグリゲート）の名前を変更します。

```
storage aggregate rename -aggregate aggr-name -newname aggr-new-name
```

次の例では、「aggr5」という名前のアグリゲートの名前を「sales-aggr」に変更します。

```
> storage aggregate rename -aggregate aggr5 -newname sales-aggr
```

## ローカル階層（アグリゲート）のメディアコストの設定

ONTAP 9.11.1以降では、System Managerを使用してローカル階層（アグリゲート）のメディアコストを設定できます。

### 手順

1. System Managerで、\* Storage > Tiers をクリックし、目的のローカル階層（アグリゲート）タイトルの Media Cost \*を設定します。
2. 「\* active and inactive Tiers \*」を選択して比較を有効にします。
3. 通貨タイプと金額を入力します。

メディアコストを入力または変更すると、すべてのメディアタイプで変更が行われます。

### 手動高速ゼロドライブ

システムにONTAP 9.4以降を新規にインストールし、システムをONTAP 9.4以降で再初期化した場合、\_fast zeroing\_ is used to zero drives.

高速初期化では、ドライブが数秒で初期化されます。プロビジョニングの前に自動的に実行されるため、スペアドライブを追加した場合に、システムの初期化、アグリゲートの作成、アグリゲートの拡張にかかる時間が大幅に短縮されます。

高速初期化\_はSSDとHDDの両方でサポートされます。



高速初期化\_は、ONTAP 9.3以前からアップグレードされたシステムではサポートされません。ONTAP 9.4以降を新規にインストールするかシステムを再初期化する必要があります。ONTAP 9.3以前では、ドライブはONTAP によって自動的に初期化されますが、プロセスにかかる時間は長くなります。

ドライブを手動で初期化する必要がある場合は、次のいずれかの方法を使用できます。ONTAP 9.4以降では、ドライブの手動初期化も数秒で完了します。

#### CLIコマンド

ドライブを高速に初期化するには、**CLI**コマンドを使用します。

このタスクについて

このコマンドを使用するには管理者権限が必要です。

手順

1. CLIコマンドを入力します。

```
storage disk zerospares
```

ブートメニューのオプション

\*ブートメニューから高速初期化ドライブ\*のオプションを選択します

このタスクについて

- 高速初期化機能拡張は、ONTAP 9.4 よりも前のリリースからアップグレードされたシステムには対応していません。
- いずれかのノードに高速初期化済みドライブを含むローカル階層（アグリゲート）がある場合、そのクラスタをONTAP 9.2以前にリポートすることはできません。

手順

1. ブートメニューから、次のいずれかのオプションを選択します。
  - (4) すべてのディスクをクリーンアップして初期化します
  - (9a) すべてのディスクのパーティショニングを解除し、ディスクの所有権情報を削除します
  - (9b) ストレージシステム全体を含むノードをクリーンアップして初期化します

ディスク所有権を手動で割り当てます

ディスクをローカル階層（アグリゲート）で使用するには、ディスクがノードに所有されていなければなりません。

このタスクについて

- DS460Cシェルフだけのない初期化前のHAペアで所有権を手動で割り当てる場合は、オプション1を使用



します。

- DS460CシェルフしかないHAペアを初期化する場合は、オプション2を使用してルートドライブの所有権を手動で割り当てます。

#### オプション1：ほとんどのHAペア

初期化を実行せず、DS460CシェルフだけがないHAペアの場合は、この手順を使用して手動で所有権を割り当てます。

##### このタスクについて

- 所有権を割り当てるディスクは、所有権を割り当てるノードに物理的にケーブル接続されたシェルフに含まれている必要があります。
- ローカル階層（アグリゲート）のディスクを使用する場合：
  - ディスクをローカル階層（アグリゲート）で使用するには、ディスクがノードに所有されていないければなりません。
  - ローカル階層（アグリゲート）で使用中のディスクの所有権を再割り当てすることはできません。

##### 手順

1. CLIを使用して、所有権が未設定のディスクをすべて表示します。

```
storage disk show -container-type unassigned
```

2. 各ディスクを割り当てます。

```
storage disk assign -disk disk_name -owner owner_name
```

ワイルドカード文字を使用すると、一度に複数のディスクを割り当てることができます。すでに別のノードで所有されているスペアディスクを再割り当てする場合は、「-force」オプションを使用する必要があります。

## オプション2：DS460Cシェルフのみを使用するHAペア

初期化するHAペアで、DS460Cシェルフしかない場合は、この手順を使用してルートドライブの所有権を手動で割り当てます。

このタスクについて

- DS460Cシェルフのみを含むHAペアを初期化する場合は、ハーフドロワーのポリシーに準拠するようにルートドライブを手動で割り当てる必要があります。

HAペアの初期化（ブートアップ）後、ディスク所有権の自動割り当てが自動的に有効になり、ハーフドロワーポリシーを使用して残りのドライブ（ルートドライブ以外）と今後追加されるすべてのドライブ（障害ディスクの交換など）に所有権が割り当てられ、「low spares」というメッセージが表示されます。または容量の追加。

次のトピックで、ハーフドロワーポリシーについて学習します。"[ディスク所有権の自動割り当てについて](#)"。

- DS460Cシェルフに8TBを超えるNL-SASドライブを搭載する場合、RAIDにはHAペアごとに最低10本のドライブ（各ノードに5本）が必要です。

手順

- DS460Cシェルフがフル装備されていない場合は、次の手順を実行します。フル装備されていない場合は、次の手順に進みます。

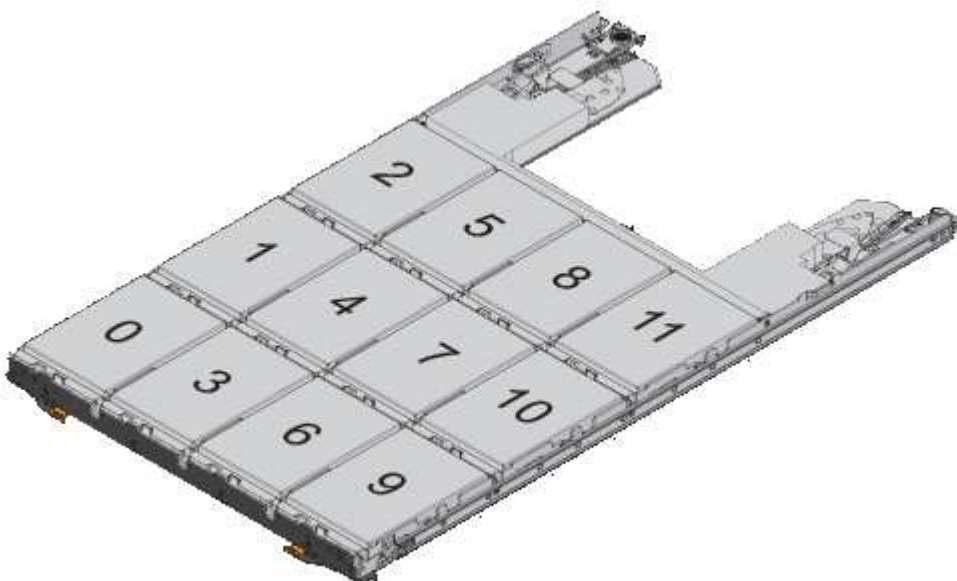
- まず、各ドロワーの前列（ドライブベイ0、3、6、9）にドライブを取り付けます。

各ドロワーの前列にドライブを取り付けると、適切な通気が確保され、過熱を防ぐことができます。

- 残りのドライブについては、各ドロワーに均等に配置します。

引き出しの列を前面から背面に充填します。行を埋めるための十分なドライブがない場合は、ドライブがドロワーの左右に均等に配置されるように2本ずつ取り付けます。

次の図は、DS460Cドロワー内のドライブベイの番号と場所を示しています。



2. ノード管理LIFまたはクラスタ管理LIFを使用してクラスタシェルにログインします。
3. 次の手順を使用して、ハーフトロワーポリシーに準拠するように各ドロワーのルートドライブを手動で割り当てます。

ハーフトロワーポリシーでは、ドロワーのドライブの左半分（ベイ0<sub>5</sub>）をノードAに、右半分（ベイ6<sub>11</sub>）をノードBに割り当てます。

- a. 所有権が未設定のすべてのディスクを表示

```
storage disk show -container-type unassigned`
```

- b. ルートディスクを割り当てます。

```
storage disk assign -disk disk_name -owner owner_name
```

ワイルドカード文字を使用すると、一度に複数のディスクを割り当てることができます。

ローカル階層（アグリゲート）のドライブおよび**RAID**グループの情報を確認する

一部のローカル階層（アグリゲート）管理タスクでは、ローカル階層を構成するドライブのタイプ、サイズ、チェックサム、ステータス、ドライブを他のローカル階層と共有するかどうか、およびRAIDグループのサイズと構成を確認しておく必要があります。

#### ステップ

1. アグリゲートのドライブを RAID グループ別に表示します。

```
storage aggregate show-status aggr_name
```

アグリゲート内の各 RAID グループのドライブが表示されます。

ドライブ（データ、パリティ、ダブルパリティ）のRAIDタイプは確認できます `Position` 列（Column）：状況に応じて `Position` 列が表示されます ``shared`` をクリックすると、そのドライブが共有されます。HDDの場合はパーティショニングされたディスクです。SSDの場合はストレージプールの一部です。

```
cluster1::> storage aggregate show-status nodeA_fp_1
```

Owner Node: cluster1-a

Aggregate: nodeA\_fp\_1 (online, mixed\_raid\_type, hybrid) (block checksums)

Plex: /nodeA\_fp\_1/plex0 (online, normal, active, pool0)

RAID Group /nodeA\_fp\_1/plex0/rg0 (normal, block checksums, raid\_dp)

Position	Disk	Pool	Type	RPM	Usable Size	Physical Size	Status
shared	2.0.1	0	SAS	10000	472.9GB	547.1GB	(normal)
shared	2.0.3	0	SAS	10000	472.9GB	547.1GB	(normal)
shared	2.0.5	0	SAS	10000	472.9GB	547.1GB	(normal)
shared	2.0.7	0	SAS	10000	472.9GB	547.1GB	(normal)
shared	2.0.9	0	SAS	10000	472.9GB	547.1GB	(normal)
shared	2.0.11	0	SAS	10000	472.9GB	547.1GB	(normal)

RAID Group /nodeA\_flashpool\_1/plex0/rg1

(normal, block checksums, raid4) (Storage Pool: SmallSP)

Position	Disk	Pool	Type	RPM	Usable Size	Physical Size	Status
shared	2.0.13	0	SSD	-	186.2GB	745.2GB	(normal)
shared	2.0.12	0	SSD	-	186.2GB	745.2GB	(normal)

8 entries were displayed.

ローカル階層（アグリゲート）を**Storage VM（SVM）**に割り当てる

Storage Virtual Machine（Storage VMまたはSVM、旧Vserver）に1つ以上のローカル階層（アグリゲート）を割り当てた場合、そのStorage VM（SVM）のボリュームはそれらのローカル階層にのみ含めることができます。

必要なもの

Storage VMとそのStorage VMに割り当てるローカル階層を用意しておく必要があります。

このタスクについて

Storage VMにローカル階層を割り当てると、Storage VMどうしの分離に役立ちます。これはマルチテナンシー環境で特に重要になります。

手順

1. SVMにすでに割り当てられているローカル階層（アグリゲート）のリストを確認します。

```
vserver show -fields aggr-list
```

SVM に現在割り当てられているアグリゲートが表示されます。割り当てられているアグリゲートがない場合はと表示されます。

- 要件に応じて、割り当てられているアグリゲートを追加または削除します。

状況	使用するコマンド
追加のアグリゲートを割り当てます	<code>vserver add-aggregates</code>
アグリゲートの割り当てを解除する	<code>vserver remove-aggregates</code>

表示されているアグリゲートが SVM に割り当てられるか、または削除されます。SVM に割り当てられていないアグリゲートを使用するボリュームがすでに SVM に関連付けられている場合、警告メッセージが表示されますが、コマンドは正常に完了します。SVM にすでに割り当てられているアグリゲートとコマンドで指定していないアグリゲートに影響はありません。

## 例

次の例では、アグリゲート `aggr1` および `aggr2` が SVM `svm1` に割り当てられます。

```
vserver add-aggregates -vserver svm1 -aggregates aggr1,aggr2
```

ローカル階層（アグリゲート）に配置するボリュームを決定する

再配置やオフライン化など、ローカル階層での処理を実行する前に、ローカル階層（アグリゲート）に配置されているボリュームを確認しなければならない場合があります。

## 手順

1. アグリゲート上のボリュームを表示するには、と入力します

```
volume show -aggregate aggregate_name
```

指定したアグリゲート上にあるすべてのボリュームが表示されます。

ローカル階層（アグリゲート）でのボリュームのスペース使用量を確認および制御する

ローカル階層（アグリゲート）のスペースを最も使用している FlexVol ボリュームと、具体的にボリュームのどの機能が最も使用しているかを確認することができます。

。 `volume show-footprint` コマンドを使用すると、ボリュームによる占有量（包含アグリゲート内でのスペース使用量）に関する情報が表示されます。

。 `volume show-footprint` コマンドを実行すると、アグリゲート内の各ボリューム（オフラインボリュームを含む）のスペース使用量の詳細が表示されます。このコマンドは、の出力のギャップを埋めます `volume show-space` および `aggregate show-space` コマンド割合の値はいずれもアグリゲートサイズの割合で計算されます。

次の例は、を示しています `volume show-footprint testvol` という名前のボリュームに対するコマンド出力：

```
cluster1::> volume show-footprint testvol
```

```
Vserver : thevs
Volume  : testvol
```

Feature	Used	Used%
-----	-----	-----
Volume Data Footprint	120.6MB	4%
Volume Guarantee	1.88GB	71%
Flexible Volume Metadata	11.38MB	0%
Delayed Frees	1.36MB	0%
Total Footprint	2.01GB	76%

次の表に、の出力のキー行の一部を示します volume show-footprint コマンドを実行し、その機能によるスペース使用量を削減する方法を説明します。

行 / 機能名	説明 / 行の内容	削減方法もあります
Volume Data Footprint	アクティブファイルシステム内のボリュームのデータに使用されている包含アグリゲート内のスペースと、ボリュームの Snapshot コピーに使用されているスペースの合計。この行の値にはリザーブスペースは含まれません。	<ul style="list-style-type: none"> <li>• ボリュームからデータを削除します。</li> <li>• ボリュームから Snapshot コピーを削除します。</li> </ul>
Volume Guarantee	ボリュームによって以降の書き込み用にリザーブされているアグリゲート内のスペース。リザーブされるスペースの量はボリュームのギャランティタイプによって異なります。	ボリュームのギャランティタイプをに変更しています none。
Flexible Volume Metadata	ボリュームのメタデータファイルに使用されているアグリゲート内のスペースの総容量。	直接制御する方法はありません。
Delayed Frees	パフォーマンス目的で ONTAP が使用していた、すぐには解放できないブロック。SnapMirrorデステネーションの場合、この行の値はになります 0 およびは表示されません。	直接制御する方法はありません。
File Operation Metadata	ファイル処理メタデータ用にリザーブされているスペースの総容量。	直接制御する方法はありません。

Total Footprint	ボリュームで使用されているアグリゲート内のスペースの合計。すべての行の合計です。	いずれかの方法でボリュームによるスペース使用量を削減します。
-----------------	--	--------------------------------

## 関連情報

"ネットアップテクニカルレポート 3483 : 『NetApp の SAN または IP SAN 構成のエンタープライズ環境におけるシン プロビジョニング』"

ローカル階層（アグリゲート）のスペース使用量を判定する

1つ以上のローカル階層（アグリゲート）内のすべてのボリュームが使用しているスペースの量を確認して、空きスペースを増やすための操作を実行できます。

WAFL では、アグリゲートレベルのメタデータとパフォーマンス用に合計ディスクスペースの10%がリザーブされます。アグリゲート内のボリュームを維持するために使用されるスペースは、WAFL リザーブから除外され、変更することはできません。



ONTAP 9.12.1以降では、30TBを超えるアグリゲートのWAFLリザーブが、AFFプラットフォームおよびFAS500fプラットフォームで10%から5%に削減されました。ONTAP 9.14.1以降では、すべてのFASプラットフォームで環境アグリゲートが削減され、アグリゲートで使用可能なスペースが5%増加しました。

を使用して、1つ以上のアグリゲート内のすべてのボリュームによるスペース使用量を表示できます aggregate show-space コマンドを実行しますこの情報から包含アグリゲートのスペースを最も使用しているボリュームを確認すると、空きスペースを増やすための対処方法を講じる際に役立ちます。

アグリゲートの使用スペースには、アグリゲートに含まれる FlexVol で使用されるスペースに直接左右されます。また、ボリュームのスペースを増やすための操作もアグリゲートのスペースに影響します。

には次の行が含まれます aggregate show-space コマンド出力：

- ボリュームフットプリント

アグリゲート内のすべてのボリュームによる占有量の合計。これには、包含アグリゲート内のすべてのボリュームのデータおよびメタデータ用に使用またはリザーブされているすべてのスペースが含まれます。

- 集計メタデータ

割り当てビットマップや inode ファイルなど、アグリゲートに必要なファイルシステムの総メタデータ。

- \* Snapshot リザーブ \*

ボリュームサイズに基づいてアグリゲート Snapshot コピー用にリザーブされているスペース。このスペースは使用済みとみなされ、ボリュームやアグリゲートのデータまたはメタデータ用に使用することはできません。

- \* Snapshotリザーブを使用できません\*

当初はアグリゲート Snapshot リザーブ用に割り当てられていたスペース。アグリゲートに関連付けられたボリュームで使用されているため、アグリゲート Snapshot コピーでは使用できません。アグリゲート

Snapshot リザーブが 0 以外のアグリゲートの場合にのみ表示されます。

- 合計使用量

ボリューム、メタデータ、または Snapshot コピー用に使用またはリザーブされているアグリゲート内のスペースの合計

- 合計使用物理容量

現在データに使用されているスペースの量（将来使用するために予約されているのではなく）アグリゲート Snapshot コピーで使用されているスペースが含まれます

次の例は、を示しています aggregate show-space Snapshotリザーブが5%のアグリゲートに対するコマンド出力。Snapshot リザーブが 0 の場合は、その行は表示されません。

```
cluster1::> storage aggregate show-space
```

Aggregate : wqa\_gx106\_aggr1

Feature	Used	Used%
-----	-----	-----
Volume Footprints	101.0MB	0%
Aggregate Metadata	300KB	0%
Snapshot Reserve	5.98GB	5%
Total Used	6.07GB	5%
Total Physical Used	34.82KB	0%

## 関連情報

- ["ナレッジベースの記事：スペース使用量"](#)
- ["ONTAP 9.12.1にアップグレードして、ストレージ容量の5%を解放します"](#)

HAペア内のローカル階層（アグリゲート）の所有権を切り替えます

HAペアのノード間で、ローカル階層（アグリゲート）のサービスを中断することなくローカル階層（アグリゲート）の所有権を変更できます。

HA ペアでは、両方のノードのディスクまたはアレイ LUN が物理的に相互接続され、各ディスクまたはアレイ LUN はどちらか一方のノードで所有されます。

ローカル階層（アグリゲート）内のすべてのディスクまたはアレイLUNの所有権は、テイクオーバーの発生時に一時的に一方のノードからもう一方のノードに切り替わります。ただし、ローカル階層の再配置処理によって所有権が永続的に変更されることもあります（負荷分散の場合など）。ディスクまたはアレイ LUN のデータコピープロセスや物理的な移動を行わずに、所有権が変更されます。

## このタスクについて

- ローカル階層の再配置処理では、ボリューム数の制限がプログラムで検証されるため、手動でチェックする必要はありません。



ボリューム数がサポートされる上限を超えると、ローカル階層の再配置処理が失敗し、関連するエラーメッセージが表示されます。

- ソースノードまたはデスティネーションノードでシステムレベルの処理を実行中のときは、ローカル階層の再配置を開始しないでください。同様に、ローカル階層の再配置の実行中はこれらの処理を開始しないでください。

これらの処理には、次のものが含まれます。

- テイクオーバー
  - ギブバック
  - シャットダウン
  - 別のローカル階層の再配置処理です
  - ディスク所有権が変わります
  - ローカル階層またはボリューム構成の処理
  - ストレージコントローラの交換
  - ONTAP のアップグレード
  - ONTAP が元に戻ります
- MetroCluster 構成を使用する場合は、ディザスタリカバリ処理 (*switchover*、*healing*、または *\_switchback \_*) の実行中にローカル階層の再配置を開始しないでください。
  - MetroCluster 構成を使用する場合に、切り替えられたローカル階層でローカル階層の再配置を開始すると、DRパートナーのボリューム数の制限を超えるため、処理が失敗する可能性があります。
  - 破損しているアグリゲートやメンテナンス中のアグリゲートでは、ローカル階層の再配置を開始しないでください。
  - ローカル階層の再配置を開始する前に、ソースノードとデスティネーションノードにコアダンプを保存する必要があります。

## 手順

1. ノードのアグリゲートを表示して移動するアグリゲートを確認し、そのアグリゲートがオンラインかつ良好な状態であることを確認します。

```
storage aggregate show -node source-node
```

次のコマンドでは、クラスタ内の 4 つのノードにある 6 つのアグリゲートが表示され、すべてのアグリゲートがオンラインです。ノード 1 とノード 3 が HA ペアになっており、ノード 2 とノード 4 も HA ペアになっています。

```
cluster::> storage aggregate show
```

Aggregate	Size	Available	Used%	State	#Vols	Nodes	RAID	Status
aggr_0	239.0GB	11.13GB	95%	online	1	node1	raid_dp,	normal
aggr_1	239.0GB	11.13GB	95%	online	1	node1	raid_dp,	normal
aggr_2	239.0GB	11.13GB	95%	online	1	node2	raid_dp,	normal
aggr_3	239.0GB	11.13GB	95%	online	1	node2	raid_dp,	normal
aggr_4	239.0GB	238.9GB	0%	online	5	node3	raid_dp,	normal
aggr_5	239.0GB	239.0GB	0%	online	4	node4	raid_dp,	normal

6 entries were displayed.

2. 問題でアグリゲートの再配置を開始するコマンドを指定します。

```
storage aggregate relocation start -aggregate-list aggregate-1, aggregate-2...
-node source-node -destination destination-node
```

次のコマンドは、アグリゲート aggr\_1 および aggr\_2 をノード 1 からノード 3 に移動します。ノード 3 はノード 1 の HA パートナーです。アグリゲートは HA ペア内でのみ移動できます。

```
cluster::> storage aggregate relocation start -aggregate-list aggr_1,
aggr_2 -node node1 -destination node3
Run the storage aggregate relocation show command to check relocation
status.
node1::storage aggregate>
```

3. を使用して、アグリゲートの再配置の進捗状況を監視します storage aggregate relocation show コマンドを実行します

```
storage aggregate relocation show -node source-node
```

次のコマンドの出力は、アグリゲートをノード 3 に移動中であることを示しています。

```
cluster::> storage aggregate relocation show -node node1
Source Aggregate      Destination      Relocation Status
-----
node1
      aggr_1          node3            In progress, module: waf1
      aggr_2          node3            Not attempted yet
2 entries were displayed.
node1::storage aggregate>
```

再配置が完了すると、このコマンドの出力には、各アグリゲートの再配置ステータスが「done」と表示されます。

ローカル階層（アグリゲート）を削除する

ローカル階層（アグリゲート）にボリュームがない場合は削除できます。

。storage aggregate delete コマンドは、ストレージアグリゲートを削除します。アグリゲートにボリュームがある場合、コマンドは失敗します。アグリゲートにオブジェクトストアが接続されている場合は、アグリゲートの削除に加えて、オブジェクトストア内のオブジェクトも削除されます。このコマンドの一部としてオブジェクトストア設定に変更はありません。

次に、「aggr1」という名前のアグリゲートを削除する例を示します。

```
> storage aggregate delete -aggregate aggr1
```

アグリゲートの再配置用のコマンド

ONTAP には、HA ペアでアグリゲートの所有権を切り替えるための固有のコマンドが用意されています。

状況	使用するコマンド
アグリゲートの再配置プロセスを開始する	storage aggregate relocation start
アグリゲートの再配置プロセスを監視する	storage aggregate relocation show

関連情報

["ONTAP 9 コマンド"](#)

アグリゲートの管理用コマンド

を使用します storage aggregate コマンドを使用してアグリゲートを管理します。

状況	使用するコマンド
すべての Flash Pool アグリゲートのキャッシュサイズを表示します	<code>storage aggregate show -fields hybrid-cache-size-total -hybrid-cache-size-total &gt;0</code>
アグリゲートのディスクの情報とステータスを表示する	<code>storage aggregate show-status</code>
ノードごとにスペアディスクを表示します	<code>storage aggregate show-spare-disks</code>
クラスタ内のルートアグリゲートを表示する	<code>storage aggregate show -has-mroot true</code>
アグリゲートの基本情報とステータスを表示します	<code>storage aggregate show</code>
アグリゲートで使用されているストレージのタイプを表示します	<code>storage aggregate show -fields storage-type</code>
アグリゲートをオンラインにします	<code>storage aggregate online</code>
アグリゲートを削除します	<code>storage aggregate delete</code>
アグリゲートを制限状態にします	<code>storage aggregate restrict</code>
アグリゲートの名前を変更します	<code>storage aggregate rename</code>
アグリゲートをオフラインにします	<code>storage aggregate offline</code>
アグリゲートの RAID タイプを変更します	<code>storage aggregate modify -raidtype</code>

## 関連情報

### ["ONTAP 9 コマンド"](#)

ローカル階層（アグリゲート）に容量（ディスク）を追加

ローカル階層（アグリゲート）に容量（ディスク）を追加

さまざまな方法を使用して、特定のワークフローに従って容量を追加します。

- ["ローカル階層（アグリゲート）に容量を追加するワークフロー"](#)
- ["ローカル階層（アグリゲート）のスペースの作成方法"](#)

ローカル階層にディスクを追加し、ノードまたはシェルフにドライブを追加できます。

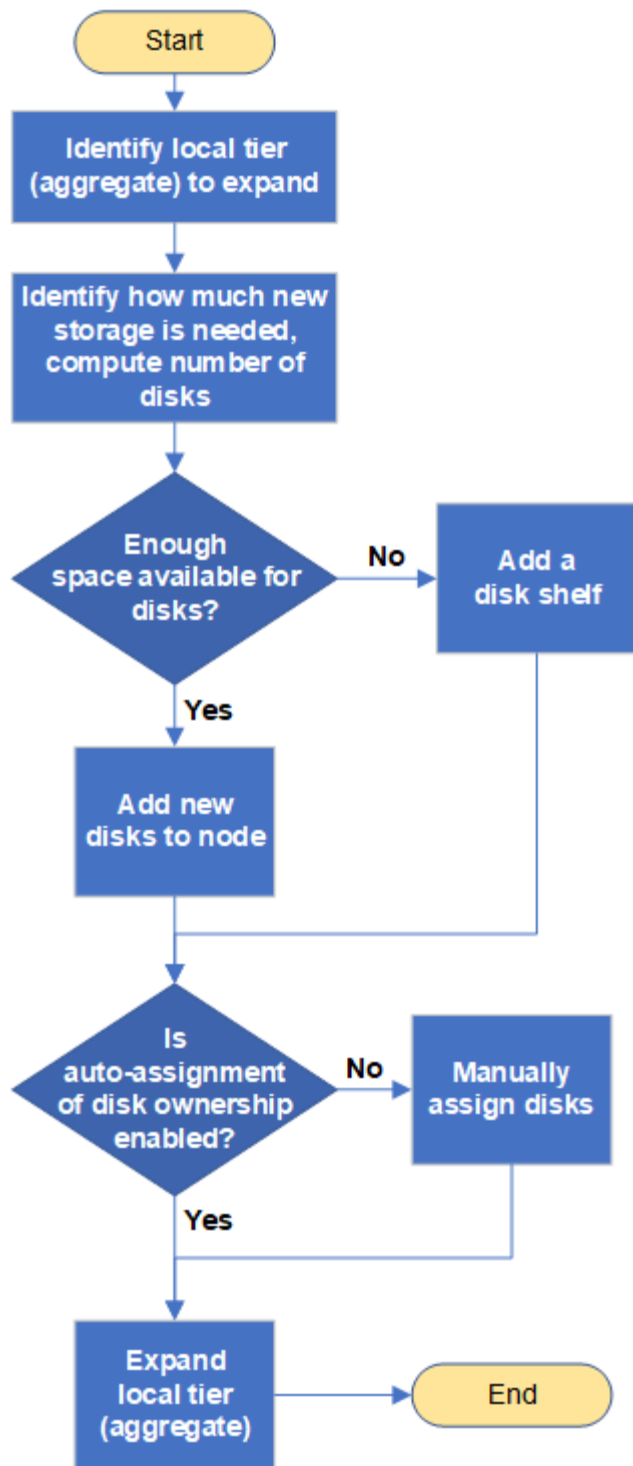
必要に応じて、ミスアライメントされたスペアパーティションを修正できます。

- "ローカル階層（アグリゲート）にディスクを追加"
- "ノードまたはシェルフにドライブを追加"
- "ミスアライメントのあるスペアパーティションを修正します"

ローカル階層への容量の追加（アグリゲートの拡張）のワークフロー

ローカル階層に容量を追加（アグリゲートを拡張）するには、最初に追加するローカル階層を特定し、必要に応じて新しいストレージの容量を決定し、新しいディスクを設置し、ディスク所有権を割り当て、新しいRAIDグループを作成する必要があります。

容量を追加するには、System ManagerまたはCLIを使用します。



#### ローカル階層（アグリゲート）のスペースの作成方法

ローカル階層（アグリゲート）の空きスペースが不足すると、データが失われたり、ボリュームギャランティが無効になるなど、さまざまな問題が発生する可能性があります。ローカル階層のスペースを増やす方法は複数あります。

どの方法にもさまざまな影響があります。対処を実行する前に、ドキュメントの関連するセクションをお読みください。

ローカル階層のスペースを確保するための一般的ないくつかの方法について、影響が小さいものから順に次に

示します。

- ローカル階層にディスクを追加してください。
- 使用可能なスペースがある別のローカル階層に一部のボリュームを移動します。
- ローカル階層内のボリュームギャランティが設定されたボリュームのサイズを縮小する。
- ボリュームのギャランティ・タイプが「none」の場合は、不要なボリュームのSnapshotコピーを削除します。
- 不要なボリュームを削除する。
- 重複排除や圧縮などのスペース削減機能を有効にします。
- 大量のメタデータを使用している機能を（一時的に）無効にする。

ローカル階層への容量の追加（アグリゲートへのディスクの追加）

ローカル階層（アグリゲート）にディスクを追加すると、関連付けられたボリュームに提供できるストレージを増やすことができます。

## System Manager (ONTAP 9.8以降)

- System Managerを使用して容量を追加します (ONTAP 9.8以降) \*

データディスクを追加することでローカル階層に容量を追加できます。



ONTAP 9.12.1以降では、System Managerを使用してローカル階層のコミット済み容量を表示し、ローカル階層に追加の容量が必要かどうかを判断できます。を参照してください ["System Manager で容量を監視"](#)。

### このタスクについて

このタスクは、ONTAP 9.8 以降がインストールされている場合にのみ実行します。以前のバージョンのONTAPをインストールした場合は、「System Manager (ONTAP 9.7以前)」というタブ（またはセクション）を参照してください。

### 手順

1. [ストレージ]、[階層]の順にクリックします。
2. をクリックします をクリックします。
3. [\* 容量の追加 \*] をクリックします。



追加できるスペアディスクがない場合、\* 容量の追加 \* オプションは表示されず、ローカル階層の容量を増やすことはできません。

4. インストールされているONTAP のバージョンに応じて、次の手順を実行します。

インストールされているONTAP のバージョン	実行する手順
ONTAP 9.8、9.9、または9.10.1	<ol style="list-style-type: none"><li>a. ノードに複数のストレージ階層が含まれている場合は、ローカル階層に追加するディスクの数を選択します。 そうしないと、ノードに含まれているストレージ階層が 1 つだけの場合に、追加された容量が自動的に概算されます。</li><li>b. [追加 (Add)] をクリックします。</li></ol>
ONTAP 9.11.1以降	<ol style="list-style-type: none"><li>a. ディスクのタイプと数を選択します。</li><li>b. 新しいRAIDグループにディスクを追加する場合は、チェックボックスをオンにします。 RAID割り当てが表示されます。</li><li>c. [保存 (Save)] をクリックします。</li></ol>

5. (任意) プロセスが完了するまでに時間がかかります。バックグラウンドでプロセスを実行する場合は、[バックグラウンドで実行 (Run in Background)] を選択します。
6. 処理が完了したら、ローカル階層の情報で容量の増加を確認できます。詳細については、「\* Storage」 > 「Tiers \*」を参照してください。

## System Manager (ONTAP 9.7以前)



- System Managerを使用して容量を追加します (ONTAP 9.7以前) \*

データディスクを追加することで、ローカル階層 (アグリゲート) に容量を追加できます。

このタスクについて

このタスクは、ONTAP 9.7 以前がインストールされている場合にのみ実行します。ONTAP 9.8 以降をインストールした場合は、を参照してください [System Managerを使用して容量を追加 \(ONTAP 9.8以降\)](#)。

手順

1. (ONTAP 9.7の場合のみ) をクリックします (クラシックバージョンに戻る)。
2. ハードウェアと診断 > アグリゲート \* をクリックします。
3. データディスクを追加するアグリゲートを選択し、\* Actions > Add Capacity \* をクリックします。



アグリゲート内の他のディスクとサイズが同じディスクを追加する必要があります。

4. (ONTAP 9.7の場合のみ) [新しいエクスペリエンスに切り替え (Switch to the new Experience \*)] をクリックします。
5. Storage > Tiers \* をクリックして、新しいアグリゲートのサイズを確認します。

CLI の使用

容量の追加には**CLI**を使用してください

パーティショニングされたディスクをアグリゲートに追加するための手順は、パーティショニングされていないディスクを追加するための手順と似ています。

必要なもの

ストレージの追加先となるアグリゲートの RAID グループのサイズを確認しておく必要があります。

このタスクについて

アグリゲートを拡張する場合は、パーティションディスクとパーティショニングされていないディスクのどちらをアグリゲートに追加するかを確認しておく必要があります。パーティショニングされていないドライブを既存のアグリゲートに追加する場合は、既存の RAID グループのサイズが新しい RAID グループによって継承されます。これにより、必要なパリティディスクの数に影響を及ぼす可能性があります。パーティショニングされたディスクで構成される RAID グループにパーティショニングされていないディスクが追加されると、新しいディスクがパーティショニングされ、未使用のスペアパーティションが残ります。

パーティションをプロビジョニングする場合は、両方のパーティションを含むスペアドライブがノードに存在しない状態を避けてください。両方のパーティションを含むスペアディスクがノードに存在しない場合にノードのコントローラが停止すると、問題に関する有用な情報 (コアファイル) をテクニカルサポートが利用できなくなる可能性があります。



を使用しないでください `disklist` コマンドを使用してアグリゲートを拡張します。原因パーティションのミスアライメントが発生する可能性があります

手順

1. アグリゲートを所有するシステムで使用可能なスペアストレージを表示します。

```
storage aggregate show-spare-disks -original-owner node_name
```

を使用できます `-is-disk-shared` パーティショニングされたドライブのみ、またはパーティショニングされていないドライブのみを表示するためのパラメータ。

```
cl1-s2::> storage aggregate show-spare-disks -original-owner cl1-s2
-is-disk-shared true
```

Original Owner: cl1-s2

Pool0

Shared HDD Spares

			Local			Local		
						Data		
Root Physical								
Disk			Type	RPM	Checksum	Usable		
Usable	Size	Status						
1.0.1			BSAS	7200	block	753.8GB		
73.89GB	828.0GB	zeroed						
1.0.2			BSAS	7200	block	753.8GB		
0B	828.0GB	zeroed						
1.0.3			BSAS	7200	block	753.8GB		
0B	828.0GB	zeroed						
1.0.4			BSAS	7200	block	753.8GB		
0B	828.0GB	zeroed						
1.0.8			BSAS	7200	block	753.8GB		
0B	828.0GB	zeroed						
1.0.9			BSAS	7200	block	753.8GB		
0B	828.0GB	zeroed						
1.0.10			BSAS	7200	block	0B		
73.89GB	828.0GB	zeroed						
2 entries were displayed.								

## 2. アグリゲートの現在の RAID グループを表示します。

```
storage aggregate show-status aggr_name
```

```
cl1-s2::> storage aggregate show-status -aggregate data_1
```

```
Owner Node: cl1-s2
```

```
Aggregate: data_1 (online, raid_dp) (block checksums)
```

```
Plex: /data_1/plex0 (online, normal, active, pool0)
```

```
RAID Group /data_1/plex0/rg0 (normal, block checksums)
```

	Position	Disk	Pool	Type	RPM	Usable Size	Physical Size	Status
	-----	-----	----	----	-----	-----	-----	
-----								
shared	1.0.10	0	BSAS	7200	753.8GB	828.0GB		
(normal)								
shared	1.0.5	0	BSAS	7200	753.8GB	828.0GB		
(normal)								
shared	1.0.6	0	BSAS	7200	753.8GB	828.0GB		
(normal)								
shared	1.0.11	0	BSAS	7200	753.8GB	828.0GB		
(normal)								
shared	1.0.0	0	BSAS	7200	753.8GB	828.0GB		
(normal)								

5 entries were displayed.

### 3. アグリゲートへのストレージの追加をシミュレートします。

```
storage aggregate add-disks -aggregate aggr_name -diskcount  
number_of_disks_or_partitions -simulate true
```

実際にストレージをプロビジョニングしなくてもストレージの追加結果を確認できます。シミュレートしたコマンドから警告が表示された場合は、コマンドを調整してシミュレーションを繰り返すことができます。

```
cl1-s2::> storage aggregate add-disks -aggregate aggr_test
-diskcount 5 -simulate true
```

Disks would be added to aggregate "aggr\_test" on node "cl1-s2" in the following manner:

First Plex

```
RAID Group rg0, 5 disks (block checksum, raid_dp)

Physical                                     Usable
Position  Disk                               Type      Size
Size
-----
shared    1.11.4                             SSD      415.8GB
415.8GB
shared    1.11.18                            SSD      415.8GB
415.8GB
shared    1.11.19                            SSD      415.8GB
415.8GB
shared    1.11.20                            SSD      415.8GB
415.8GB
shared    1.11.21                            SSD      415.8GB
415.8GB
```

Aggregate capacity available for volume use would be increased by 1.83TB.

#### 4. アグリゲートにストレージを追加します。

```
storage aggregate add-disks -aggregate aggr_name -raidgroup new -diskcount
number_of_disks_or_partitions
```

Flash Poolアグリゲートの作成時に、チェックサムがアグリゲートと異なるディスクを追加する場合や、チェックサムが混在したアグリゲートにディスクを追加する場合は、を使用する必要があります `-checksumstyle` パラメータ

Flash Poolアグリゲートにディスクを追加する場合は、を使用する必要があります `-disktype` ディスクタイプを指定するパラメータ。

を使用できます `-disksize` 追加するディスクのサイズを指定するパラメータ。指定したサイズに近いディスクだけがアグリゲートへの追加対象として選択されます。

```
cl1-s2::> storage aggregate add-disks -aggregate data_1 -raidgroup
new -diskcount 5
```

5. ストレージが正常に追加されたことを確認します。

```
storage aggregate show-status -aggregate aggr_name
```

```
cl1-s2::> storage aggregate show-status -aggregate data_1

Owner Node: cl1-s2
Aggregate: data_1 (online, raid_dp) (block checksums)
Plex: /data_1/plex0 (online, normal, active, pool0)
RAID Group /data_1/plex0/rg0 (normal, block checksums)

Usable
Physical
Position Disk Pool Type RPM Size
Size Status
-----
-----
shared 1.0.10 0 BSAS 7200 753.8GB
828.0GB (normal)
shared 1.0.5 0 BSAS 7200 753.8GB
828.0GB (normal)
shared 1.0.6 0 BSAS 7200 753.8GB
828.0GB (normal)
shared 1.0.11 0 BSAS 7200 753.8GB
828.0GB (normal)
shared 1.0.0 0 BSAS 7200 753.8GB
828.0GB (normal)
shared 1.0.2 0 BSAS 7200 753.8GB
828.0GB (normal)
shared 1.0.3 0 BSAS 7200 753.8GB
828.0GB (normal)
shared 1.0.4 0 BSAS 7200 753.8GB
828.0GB (normal)
shared 1.0.8 0 BSAS 7200 753.8GB
828.0GB (normal)
shared 1.0.9 0 BSAS 7200 753.8GB
828.0GB (normal)
10 entries were displayed.
```

6. ルートパーティションとデータパーティションの両方を含む少なくとも1本のスペアドライブがノードに存在することを確認します。

```
storage aggregate show-spare-disks -original-owner node_name
```

```
cl1-s2::> storage aggregate show-spare-disks -original-owner cl1-s2
-is-disk-shared true
```

Original Owner: cl1-s2

Pool0

Shared HDD Spares

			Local
			Data
Root	Physical		
Disk		Type	RPM Checksum Usable
Usable	Size Status		
-----			
1.0.1		BSAS	7200 block 753.8GB
73.89GB	828.0GB zeroed		
1.0.10		BSAS	7200 block 0B
73.89GB	828.0GB zeroed		
2 entries were displayed.			

ノードまたはシェルフにドライブを追加

ホットスペアの数を増やしたり、ローカル階層（アグリゲート）にスペースを追加したりするには、ノードまたはシェルフにドライブを追加します。

作業を開始する前に

追加するドライブがプラットフォームでサポートされている必要があります。次のコマンドを使用して確認できます。 ["NetApp Hardware Universe の略"](#)。

1 つの手順に追加する必要があるドライブは 6 本以上です。ドライブを 1 本追加するとパフォーマンスが低下する可能性があります。

**NetApp Hardware Universe**の手順

1. **[\* Products]**ドロップダウンメニューで、ハードウェア構成を選択します。
2. プラットフォームを選択します。
3. 実行しているONTAPのバージョンを選択し、**Show Results**を選択します。
4. 図の下で、**[\*別のビューを表示するにはここをクリック]**を選択します。設定に一致するビューを選択します。



## ドライブの取り付け手順

1. を確認します ["NetApp Support Site"](#) 新しいドライブファームウェアやシェルフファームウェア、Disk Qualification Packageファイルについては、を参照してください。

ノードまたはシェルフに最新バージョンがインストールされていない場合は、新しいドライブを取り付ける前に更新します。

最新のファームウェアバージョンがインストールされていない新しいドライブでは、ドライブファームウェアは自動的に（無停止で）更新されます。

2. 自身の適切な接地対策を行います
3. プラットフォームの前面からベゼルをそっと取り外します。
4. 新しいドライブの正しいスロットを特定します。



ドライブを追加するための正しいスロットは、プラットフォームのモデルと ONTAP のバージョンによって異なります。場合によっては、特定のスロットに順番にドライブを追加する必要があります。たとえば、AFF A800 では、特定の間隔でドライブを追加し、クラスタに空のスロットが残っています。一方、AFF A220 では、外からシェルフの中央に向かって実行されている次の空きスロットに新しいドライブを追加します。

使用する構成に適したスロットを特定するには、「**Before You Begin**」の手順を参照してください。["NetApp Hardware Universe の略"](#)。

5. 新しいドライブを挿入します。
  - a. カムハンドルを開いた状態で、両手で新しいドライブを挿入します。
  - b. ドライブが停止するまで押します。
  - c. ドライブがミッドプレーンに完全に収まり、カチッという音がして固定されるまで、カムハンドルを閉じます。カムハンドルは、ドライブの前面に揃うようにゆっくりと閉じてください。
6. ドライブのアクティビティ LED（緑色）が点灯していることを確認します。

ドライブのアクティビティ LED が点灯している場合は、ドライブに電力が供給されています。ドライブのアクティビティ LED が点滅しているときは、ドライブに電力が供給されていて、I/O が実行中です。ドライブファームウェアが自動的に更新されている場合は、LED が点滅します。

7. 別のドライブを追加する場合は、手順 4~6 を繰り返します。

新しいドライブは、ノードに割り当てられるまで認識されません。新しいドライブを手動で割り当てることができます。また、ドライブの自動割り当てルールを適用しているノードの場合は、新しいドライブが ONTAP によって自動的に割り当てられるまで待つこともできます。

8. 新しいドライブがすべて認識されたら、ドライブが追加され、所有権が正しく指定されていることを確認

します。

## インストールの確認手順

1. ディスクのリストを表示します。

```
storage aggregate show-spare-disks
```

新しいドライブが正しいノードで所有されていることを確認してください。

2. 必要に応じて（ONTAP 9.3以前の場合のみ）新しく追加したドライブを初期化します。

```
storage disk zerospares
```

別のONTAP ローカル階層（アグリゲート）で以前使用されていたドライブは、アグリゲートに追加する前に初期化する必要があります。ONTAP 9.3以前では、ノード内の初期化されていないドライブのサイズによっては、初期化が完了するまでに数時間かかることがあります。この時点でドライブを初期化しておく、ローカル階層のサイズをすぐに拡張する必要がある場合に時間を短縮できます。これはONTAP 9.4以降の問題ではありません。ドライブは高速初期化を使用して初期化されますが、これには数秒しかかかりません。

## 結果

新しいドライブの準備が完了しました。ローカル階層（アグリゲート）に追加したり、ホットスペアのリストに配置したり、新しいローカル階層を作成したときに追加したりできます。

ミスアライメントのあるスペアパーティションを修正します

パーティショニングされたディスクをローカル階層（アグリゲート）に追加する場合は、各ノードについて、使用可能なルートパーティションとデータパーティションの両方を含むディスクをスペアとして残しておく必要があります。スペアディスクがない状態でノードが停止すると、ONTAP はスペアデータパーティションにコアをダンプできません。

## 作業を開始する前に

同じノードが所有する同じタイプのディスクには、スペアデータパーティションとスペアルートパーティションの両方が必要です。

## 手順

1. CLIを使用して、ノードのスペアパーティションを表示します。

```
storage aggregate show-spare-disks -original-owner node_name
```

どのディスクにスペアデータパーティション（`spare_data`）とスペアルートパーティション（`spare_root`）があるかに注意してください。スペアパーティションの下にゼロ以外の値が表示されます Local Data Usable または Local Root Usable 列（Column）：

2. スペアデータパーティションを含むディスクを、スペアルートパーティションを含むディスクと交換します。

```
storage disk replace -disk spare_data -replacement spare_root -action start
```



どちらの方向にもデータをコピーできますが、ルートパーティションのコピーは完了までの時間が短くなります。

3. ディスク交換の進捗を監視します。

```
storage aggregate show-status -aggregate aggr_name
```

4. 交換処理が完了したら、もう一度スペアを表示して、スペアディスクが存在することを確認します。

```
storage aggregate show-spare-disks -original-owner node_name
```

「Local Data Usable」との両方に、使用可能なスペースがあるスペアディスクが表示されます Local Root Usable。

例

ノード c1-01 のスペアパーティションを表示して、スペアパーティションがアライメントされていないことを確認します。

```
c1::> storage aggregate show-spare-disks -original-owner c1-01
```

Original Owner: c1-01

Pool0

Shared HDD Spares

Disk	Type	RPM	Checksum	Local Data Usable	Local Root Usable	Physical Size
1.0.1	BSAS	7200	block	753.8GB	0B	828.0GB
1.0.10	BSAS	7200	block	0B	73.89GB	828.0GB

ディスク交換ジョブを開始します。

```
c1::> storage disk replace -disk 1.0.1 -replacement 1.0.10 -action start
```

交換処理が完了するのを待っている間に、処理の進捗を表示します。

```
c1::> storage aggregate show-status -aggregate aggr0_1
```

Owner Node: c1-01  
Aggregate: aggr0\_1 (online, raid\_dp) (block checksums)  
Plex: /aggr0\_1/plex0 (online, normal, active, pool0)  
RAID Group /aggr0\_1/plex0/rg0 (normal, block checksums)

Position	Disk	Pool	Type	RPM	Usable Size	Physical Size	Status
shared	1.0.1	0	BSAS	7200	73.89GB	828.0GB	(replacing, copy in progress)
shared	1.0.10	0	BSAS	7200	73.89GB	828.0GB	(copy 63% completed)
shared	1.0.0	0	BSAS	7200	73.89GB	828.0GB	(normal)
shared	1.0.11	0	BSAS	7200	73.89GB	828.0GB	(normal)
shared	1.0.6	0	BSAS	7200	73.89GB	828.0GB	(normal)
shared	1.0.5	0	BSAS	7200	73.89GB	828.0GB	(normal)

交換処理が完了したら、スペアディスクが存在することを確認します。

```
ie2220::> storage aggregate show-spare-disks -original-owner c1-01
```

Original Owner: c1-01  
Pool0  
Shared HDD Spares

Disk	Type	RPM	Checksum	Local Data Usable	Local Root Usable	Physical Size
1.0.1	BSAS	7200	block	753.8GB	73.89GB	828.0GB

## ディスクを管理する

### ディスクの管理の概要

システム内のディスクを管理するためのさまざまな手順を実行できます。

- ディスク管理の側面
  - ["Disk Qualification Package の更新が必要なタイミング"](#)
  - ["ホットスペアディスクの仕組み"](#)
  - ["スペア不足に対する警告を使用したスペアディスクの管理"](#)
  - ["ルート / データパーティショニングの追加の管理オプション"](#)
- ディスクとパーティションの所有権

- ["ディスクおよびパーティションの所有権"](#)
- ディスクの取り外しに失敗しました
  - ["障害が発生したディスクを取り外します"](#)
- ディスク完全消去
  - ["ディスク完全消去"](#)

## ホットスペアディスクの仕組み

ホットスペアディスクとは、ストレージシステムに割り当てられているディスクで、RAID グループでは使用されていないディスクを指します。データは格納されていませんが、すぐに使用できる状態になっています。

RAID グループ内でディスク障害が発生すると、RAID グループにホットスペアディスクが自動的に割り当てられ、障害ディスクと交換されます。障害ディスクのデータは、RAID パリティディスクからホットスペア交換ディスク上にバックグラウンドで再構築されます。再構築アクティビティが記録されます  
/etc/message ファイルとAutoSupport メッセージが送信されます。

障害ディスクと同じサイズのホットスペアディスクがない場合、次に大きなサイズのディスクが選択され、交換対象のディスクのサイズに合わせて縮小されます。

## マルチディスクキャリアのディスクのスペアに関する要件

ストレージの冗長性を最適化し、ONTAP によるディスクコピーの所要時間を最小限に抑えて、最適なディスクレイアウトを実現するためには、マルチディスクキャリアのディスクに対して適切な数のスペアを用意しておくことが不可欠です。

マルチディスクキャリアのディスクに対しては、常に 2 つ以上のホットスペアを用意しておく必要があります。Maintenance Center を使用できるようにし、同時に複数のディスク障害が発生した場合の問題を回避するには、4 つ以上のホットスペアを用意して安定した運用を確保し、障害が発生したディスクを迅速に交換するようにします。

ONTAP では、同時に 2 つのディスクで障害が発生した場合に利用できるホットスペアが 2 つしかない、障害が発生したディスクとそのキャリアメイトの両方のコンテンツをスペアディスクにスワップできないことがあります。このような状況を「ステールメイト」と呼びます。この場合、EMS メッセージと AutoSupport メッセージで通知されます。交換用キャリアが使用できるようになったら、EMS メッセージに記載されている手順に従う必要があります。

詳細については、ナレッジベースの記事を参照してください ["RAID レイアウトを自動再配置できません-AutoSupport メッセージ"](#)

## スペア不足に対する警告を使用したスペアディスクの管理

デフォルトでは、ストレージシステム内の各ドライブの属性に一致するホットスペアドライブが 1 本もない場合、警告がコンソールとログに出力されます。

システムがベストプラクティスに準拠するようにこれらの警告メッセージのしきい値を変更できます。

## このタスクについて

推奨される最小数のスペア・ディスクを常に持つようにするには 'min\_ssparm\_count' RAID オプションを 2 に設定する必要があります

## ステップ

1. オプションを「2」に設定します。

```
storage raid-options modify -node nodename -name min_spare_count -value 2
```

## ルート / データパーティショニングの追加の管理オプション

ONTAP 9.2 以降では、ブートメニューから新しいルート / データパーティショニングオプションを使用できます。このオプションによって、ルート / データパーティショニング用に設定されたディスクに管理機能が追加されます。

ブートメニューオプション 9 では、次の管理機能を使用できます。

- すべてのディスクのパーティションを解除し、ディスクの所有権情報を削除します。

このオプションは、ルート / データパーティショニング用に設定されているシステムを別の設定を使用して再初期化する必要がある場合に便利です。

- パーティショニングされたディスクを含むノードをクリーンアップして初期化します。

このオプションは、次の場合に役立ちます。

- ルート / データパーティショニング用に設定されていないシステムをルート / データパーティショニング用に設定する
- ルート / データパーティショニング用に正しく設定されていないシステムを修正する必要があります
- SSD だけが接続されている AFF プラットフォームまたは FAS プラットフォームが以前のバージョンのルート / データパーティショニング用に設定されている状況で、ルート / データパーティショニングを新しいバージョンにアップグレードしてストレージ効率を向上する
- 構成を消去し、ディスク全体を含むノードを初期化します。

このオプションは、次の処理が必要な場合に役立ちます。

- 既存のパーティションのパーティショニングを解除します
- ローカルディスクの所有権を削除する
- RAID-DP を使用して、ディスク全体を含むシステムを再初期化します

## Disk Qualification Package の更新が必要なタイミング

Disk Qualification Package (DQP) は、新しく認定されたドライブに対する完全なサポートを追加するためのパッケージです。ドライブファームウェアを更新したり、新しいタイプやサイズのドライブをクラスタに追加したりする前に、DQP を更新する必要があります。また、四半期ごとや半年ごとなど、DQP も定期的に更新することを推奨します。

DQP は、次の場合にダウンロードしてインストールする必要があります。

- 新しいタイプやサイズのドライブをノードに追加したとき

たとえば、1TB のドライブを使用している環境で 2TB のドライブを追加した場合、DQP の最新版がないかどうかを確認する必要があります。

- ディスクファームウェアを更新するたびに更新されます
- 新しいディスクファームウェアや DQP ファイルが利用可能になったとき
- 新しいバージョンの ONTAP にアップグレードするとき

ONTAP のアップグレードの一環として DQP が更新されることはありません。

## 関連情報

["ネットアップのダウンロード：Disk Qualification Package"](#)

["ネットアップのダウンロード：ディスクドライブファームウェア"](#)

## ディスクおよびパーティションの所有権

ディスクおよびパーティションの所有権

ディスクとパーティションの所有権を管理できます。

次のタスクを実行できます。

- ["ディスクおよびパーティションの所有権を表示します"](#)

ディスク所有権を表示して、ストレージを制御しているノードを特定できます。共有ディスクを使用するシステムのパーティション所有権も表示できます。

- ["ディスク所有権の自動割り当ての設定を変更します"](#)

デフォルト以外のポリシーを選択してディスク所有権を自動的に割り当てるか、ディスク所有権の自動割り当てを無効にすることができます。

- ["パーティショニングされていないディスクの所有権を手動で割り当てる"](#)

ディスク所有権の自動割り当てを使用するようにクラスタが設定されていない場合は、所有権を手動で割り当てる必要があります。

- ["パーティショニングされたディスクの所有権を手動で割り当てます"](#)

コンテナディスクまたはパーティションの所有権は、パーティショニングされていないディスクの場合と同様に、手動で設定することも自動割り当てを使用して設定することもできます。

- ["障害が発生したディスクを取り外します"](#)

完全に障害が発生したディスクは、ONTAP で使用可能なディスクとみなされなくなり、シェルフからただちに取り外すことができます。

- ["ディスクから所有権を削除します"](#)

ONTAP は、ディスク所有権情報をディスクに書き込みます。スペアディスクまたはそのシェルフをノードから取り外す前に、所有権情報を削除して、別のノードに適切に統合できるようにする必要があります。

す。

#### ディスク所有権の自動割り当てについて

未割り当てディスクの自動割り当ては、デフォルトで有効になっています。ディスク所有権の自動割り当ては、HAペアの初期化後10分、および通常のシステム動作中は5分おきに実行されます。

HAペアに新しいディスクを追加する場合（障害が発生したディスクを交換する場合、「low spares」というメッセージが表示された場合、または容量を追加する場合など）、デフォルトの自動割り当てポリシーによってディスクの所有権がスペアとしてノードに割り当てられます。

デフォルトの自動割り当てポリシーは、プラットフォーム固有の特性（HAペアに搭載されているシェルフのみの場合）に基づいており、次のいずれかの方法（ポリシー）を使用してディスク所有権が割り当てられます。

割り当て方法	ノードの割り当てに影響します	割り当て方法にデフォルト設定されているプラットフォーム構成
ベイ	偶数番号のベイがノードAに、奇数番号のベイがノードBに割り当てられています	1台の共有シェルフを使用するHAペア構成のエントリレベルのシステム。
シェルフ	シェルフ内のすべてのディスクがノードAに割り当てられます	複数のシェルフを搭載した1つのスタックを使用するHAペア構成におけるエントリレベルのシステム、およびノードごとに1つのスタック、2つ以上のシェルフを使用するMetroCluster構成。
シェルフを分割します  このポリシーは、 <code>-autoassign-policy</code> のパラメータ <code>storage disk option</code> 該当するプラットフォームおよびシェルフ構成用のコマンド。	シェルフの左側のディスクはノードAに、右側のノードBに割り当てられますHAペアの部分的なシェルフは、シェルフの端から中央に向かってディスクが挿入された状態で出荷されます。	ほとんどのAFFプラットフォームと一部のMetroCluster構成。
スタック	スタック内のすべてのディスクがノードAに割り当てられています	エントリレベルのスタンドアロンシステムとその他のすべての構成。

<p>ハーフドロワー</p> <p>このポリシーは、<code>-autoassign-policy</code> のパラメータ <code>storage disk option</code> 該当するプラットフォームおよびシェルフ構成用のコマンド。</p>	<p>DS460Cドロワーの左半分（ドライブベイ0<sub>5</sub>）のすべてのドライブがノードAに割り当てられ、ドロワーの右半分（ドライブベイ6<sub>11</sub>）のすべてのドライブがノードBに割り当てられます。</p> <p>DS460CシェルフのみのHAペアを初期化する場合、ディスク所有権の自動割り当てはサポートされません。ハーフドロワーのポリシーに従って、ルートパーティションが設定されたルート/コンテナドライブを含むドライブに所有権を手動で割り当てる必要があります。</p>	<p>DS460Cシェルフのみを使用したHAペア（HAペアの初期化（ブートアップ）後）</p> <p>HAペアのブート後、ディスク所有権の自動割り当てが自動的に有効になり、ハーフドロワーポリシーを使用して、残りのドライブ（ルートパーティションを含むルートドライブ/コンテナドライブを除く）と今後追加されるすべてのドライブに所有権が割り当てられます。</p> <p>HAペアに他のシェルフモデルに加えてDS460Cシェルフがある場合は、ハーフドロワーポリシーは使用されません。使用されるデフォルトポリシーは、プラットフォーム固有の特性によって決まります。</p>
--	--	--

#### 自動割り当ての設定と変更：

- 現在の自動割り当て設定（オン/オフ）を表示するには、`storage disk option show` コマンドを実行します
- 自動割り当てを無効にするには、`storage disk option modify` コマンドを実行します
- デフォルトの自動割り当てポリシーが環境に適していない場合は、`-autoassign-policy` のパラメータを指定します `storage disk option modify` コマンドを実行します

方法をご確認ください ["ディスク所有権の自動割り当ての設定を変更します"](#)。



ハーフドロワーおよびスプリットシェルフのデフォルトの自動割り当てポリシーは、ベイ、シェルフ、スタックのポリシーなどのユーザが設定できないため、一意です。

アドバンスドドライブパーティショニング（ADP）システムで、収容数が半分のシェルフで自動割り当てを機能させるには、シェルフのタイプに基づいて正しいシェルフベイにドライブを取り付ける必要があります。

- DS460Cシェルフ以外のシェルフの場合は、左端と右端に均等にドライブを取り付けます。たとえば、DS224Cシェルフのベイ0<sub>5</sub>に6本のドライブを、ベイ18<sub>23</sub>に6本のドライブを搭載したとします。
- DS460Cシェルフの場合は、各ドロワーの前列（ドライブベイ0、3、6、9）にドライブを取り付けます。残りのドライブについては、ドロワーの前から後ろまで列を埋めて、各ドロワーに均等に配置します。行を埋めるための十分なドライブがない場合は、ドライブがドロワーの左右に均等に配置されるように2本ずつ取り付けます。

各ドロワーの前列にドライブを取り付けると、適切な通気が確保され、過熱を防ぐことができます。



収容数が半分のシェルフの正しいシェルフベイにドライブが取り付けられていない場合は、コンテナドライブに障害が発生して交換したときに、ONTAPで所有権が自動割り当てされません。この場合、新しいコンテナドライブの割り当てを手動で行う必要があります。コンテナドライブに所有権を割り当てると、必要なドライブのパーティショニングとパーティショニングの割り当てがONTAPによって自動的に処理されます。

自動割り当てが機能しない場合は、を使用してディスク所有権を手動で割り当てる必要があります。  
storage disk assign コマンドを実行します

- 自動割り当てを無効にすると、新しいディスクがノードに手動で割り当てられるまでスペアとして使用できなくなります。
- ディスクの自動割り当てを行う場合に、所有権が異なる複数のスタックまたはシェルフが必要な場合は、それぞれのスタックまたはシェルフで所有権の自動割り当てが機能するように、各スタックまたはシェルフでいずれかのディスクを手動で割り当てておく必要があります。
- 自動割り当てが有効になっている場合に、アクティブポリシーで指定されていないノードに1本のドライブを手動で割り当てると、自動割り当てが停止し、EMSメッセージが表示されます。

方法をご確認ください ["パーティショニングされていないディスクのディスク所有権を手動で割り当てる"](#)。

方法をご確認ください ["パーティショニングされたディスクのディスク所有権を手動で割り当てる"](#)。

ディスクおよびパーティションの所有権を表示します

ディスク所有権を表示して、ストレージを制御しているノードを特定できます。共有ディスクを使用するシステムのパーティション所有権も表示できます。

#### 手順

1. 物理ディスクの所有権を表示します。

```
storage disk show -ownership
```

```
cluster::> storage disk show -ownership
Disk      Aggregate Home      Owner    DR Home  Home ID      Owner ID    DR
Home ID   Reserver  Pool
-----
-----
1.0.0     aggr0_2   node2     node2    -        2014941509  2014941509  -
2014941509 Pool0
1.0.1     aggr0_2   node2     node2    -        2014941509  2014941509  -
2014941509 Pool0
1.0.2     aggr0_1   node1     node1    -        2014941219  2014941219  -
2014941219 Pool0
1.0.3     -         node1     node1    -        2014941219  2014941219  -
2014941219 Pool0
```

2. システムで共有ディスクを使用している場合は、パーティション所有権を表示できます。



```
storage disk show -partition-ownership
```

```
cluster::> storage disk show -partition-ownership
```

Container	Container	Root	Data
Disk	Aggregate	Root Owner	Data Owner
Owner ID		Owner ID	Owner ID
1.0.0	-	node1	node1
1886742616		1886742616	1886742616
1.0.1	-	node1	node1
1886742616		1886742616	1886742616
1.0.2	-	node2	node2
1886742657		1886742657	1886742657
1.0.3	-	node2	node2
1886742657		1886742657	1886742657

ディスク所有権の自動割り当ての設定を変更します

を使用できます `storage disk option modify` コマンドを使用して、デフォルト以外のポリシーを選択してディスク所有権を自動的に割り当てたり、ディスク所有権の自動割り当てを無効にしたりできます。

詳細はこちら ["ディスク所有権の自動割り当て"](#)。

このタスクについて

DS460Cシェルフのみを使用するHAペアの場合、デフォルトの自動割り当てポリシーはハーフトロワーです。デフォルト以外のポリシー（ベイ、シェルフ、スタック）に変更することはできません。

手順

1. ディスクの自動割り当てを変更します。

a. デフォルト以外のポリシーを選択する場合は、次のように入力します。

```
storage disk option modify -autoassign-policy autoassign_policy -node  
node_name
```

- 使用 `stack` として `autoassign_policy` 所有権の自動割り当てをスタックまたはループレベルで実行するように設定します。
- 使用 `shelf` として `autoassign_policy` 所有権の自動割り当てをシェルフレベルで実行するように設定します。
- 使用 `bay` として `autoassign_policy` 所有権の自動割り当てをベイレベルで実行するように設定します。

b. ディスク所有権の自動割り当てを無効にする場合は、次のように入力します。

```
storage disk option modify -autoassign off -node node_name
```

## 2. ディスクの自動割り当ての設定を確認します。

```
storage disk option show
```

```
cluster1::> storage disk option show
```

Node	BKg. FW. Upd.	Auto Copy	Auto Assign	Auto Assign Policy
-----	-----	-----	-----	-----
cluster1-1	on	on	on	default
cluster1-2	on	on	on	default

パーティショニングされていないディスクのディスク所有権を手動で割り当てる

ディスク所有権の自動割り当てを使用するようにHAペアが設定されていない場合は、所有権を手動で割り当てる必要があります。DS460CシェルフしかないHAペアを初期化する場合、ルートドライブの所有権を手動で割り当てる必要があります。

このタスクについて

- DS460Cシェルフだけのない初期化前のHAペアで所有権を手動で割り当てる場合は、オプション1を使用します。
- DS460CシェルフしかないHAペアを初期化する場合は、オプション2を使用してルートドライブの所有権を手動で割り当てます。

## オプション1：ほとんどのHAペア

初期化を実行せず、DS460CシェルフだけがないHAペアの場合は、この手順を使用して手動で所有権を割り当てます。

このタスクについて

- 所有権を割り当てるディスクは、所有権を割り当てるノードに物理的にケーブル接続されたシェルフに含まれている必要があります。
- ローカル階層（アグリゲート）のディスクを使用する場合：
  - ディスクをローカル階層（アグリゲート）で使用するには、ディスクがノードに所有されていない必要があります。
  - ローカル階層（アグリゲート）で使用中のディスクの所有権を再割り当てすることはできません。

手順

1. CLIを使用して、所有権が未設定のディスクをすべて表示します。

```
storage disk show -container-type unassigned
```

2. 各ディスクを割り当てます。

```
storage disk assign -disk disk_name -owner owner_name
```

ワイルドカード文字を使用すると、一度に複数のディスクを割り当てることができます。すでに別のノードで所有されているスペアディスクを再割り当てする場合は、「-force」オプションを使用する必要があります。

## オプション2：DS460Cシェルフのみを使用するHAペア

初期化するHAペアで、DS460Cシェルフしかない場合は、この手順を使用してルートドライブの所有権を手動で割り当てます。

このタスクについて

- DS460Cシェルフのみを含むHAペアを初期化する場合は、ハーフドロワーのポリシーに準拠するようにルートドライブを手動で割り当てする必要があります。

HAペアの初期化（ブートアップ）後、ディスク所有権の自動割り当てが自動的に有効になり、ハーフドロワーポリシーを使用して残りのドライブ（ルートドライブ以外）と今後追加されるすべてのドライブ（障害ディスクの交換など）に所有権が割り当てられ、「low spares」というメッセージが表示されます。または容量の追加。

次のトピックで、ハーフドロワーポリシーについて学習します。"[ディスク所有権の自動割り当てについて](#)"。

- DS460Cシェルフに8TBを超えるNL-SASドライブを搭載する場合、RAIDにはHAペアごとに最低10本のドライブ（各ノードに5本）が必要です。

手順

1. DS460Cシェルフがフル装備されていない場合は、次の手順を実行します。フル装備されていない場合は、次の手順に進みます。

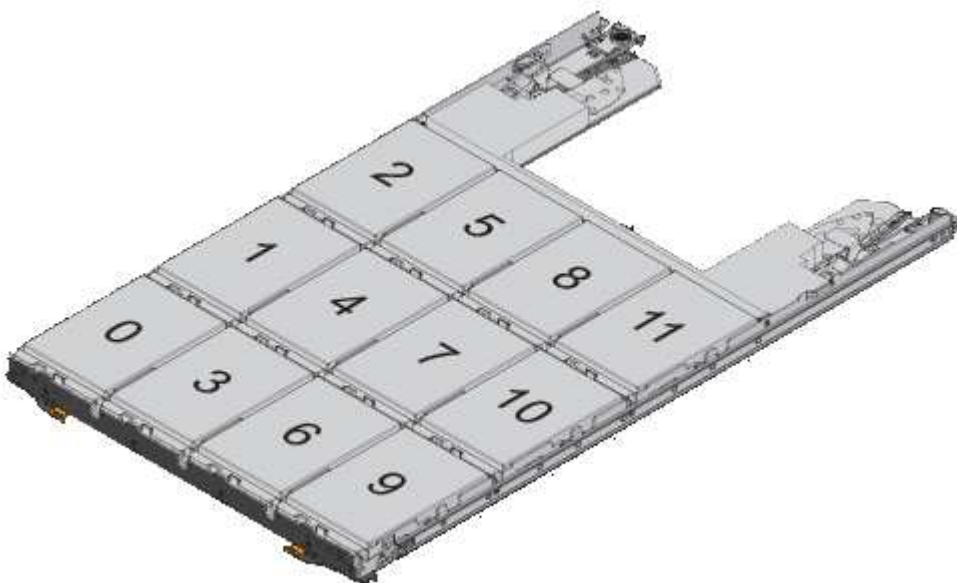
- a. まず、各ドロワーの前列（ドライブベイ0、3、6、9）にドライブを取り付けます。

各ドロワーの前列にドライブを取り付けると、適切な通気が確保され、過熱を防ぐことができます。

- b. 残りのドライブについては、各ドロワーに均等に配置します。

引き出しの列を前面から背面に充填します。行を埋めるための十分なドライブがない場合は、ドライブがドロワーの左右に均等に配置されるように2本ずつ取り付けます。

次の図は、DS460Cドロワー内のドライブベイの番号と場所を示しています。



2. ノード管理LIFまたはクラスタ管理LIFを使用してクラスタシェルにログインします。
3. 次の手順を使用して、ハーフトロワーポリシーに準拠するように各ドロワーのルートドライブを手動で割り当てます。

ハーフトロワーポリシーでは、ドロワーのドライブの左半分（ベイ0<sub>5</sub>）をノードAに、右半分（ベイ6<sub>11</sub>）をノードBに割り当てます。

- a. 所有権が未設定のすべてのディスクを表示

```
storage disk show -container-type unassigned`
```

- b. ルートディスクを割り当てます。

```
storage disk assign -disk disk_name -owner owner_name
```

ワイルドカード文字を使用すると、一度に複数のディスクを割り当てることができます。

パーティショニングされたディスクの所有権を手動で割り当てます

コンテナディスクまたはパーティションの所有権は、アドバンスドドライブパーティショニング（ADP）システムで手動で割り当てることができます。DS460Cシェルフのみを含むHAペアを初期化する場合は、ルートパーティションを含むコンテナドライブの所有権を手動で割り当てする必要があります。

このタスクについて

- サポートされるADPの方式は、ストレージシステムのタイプによって異なります。root-data（RD）とroot-data-data（RD2）のどちらかです。

FASストレージシステムはRDを使用し、AFFストレージシステムはRD2を使用します。

- DS460CシェルフだけがないHAペアの所有権を手動で割り当てる場合は、オプション1を使用してルート/データ（RD）パーティショニングを使用してディスクを手動で割り当てるか、オプション2を使用してルート/データ（RD2）パーティショニングを使用してディスクを手動で割り当てることができます。
- DS460CシェルフしかないHAペアを初期化する場合は、オプション3を使用して、ルートパーティションを含むコンテナドライブに所有権を手動で割り当てます。

オプション1：ルート/データ（RD）パーティショニングを使用してディスクを手動で割り当てる

ルート/データパーティショニングでは、HAペアがまとめて所有する所有権の3つのエンティティ（コンテナディスクと2つのパーティション）があります。

このタスクについて

- コンテナディスクと2つのパーティションがHAペアの一方のノードに所有されていれば、それらがすべて同じHAペアの同じノードに所有されている必要はありません。ただし、ローカル階層（アグリゲート）のパーティションを使用する場合は、ローカル階層を所有するノードが所有している必要があります。
- 収容数が半分のシェルフのコンテナディスクで障害が発生して交換した場合、この場合、ONTAPでは所有権が常に自動割り当てされるとは限らないため、ディスク所有権の手動割り当てが必要になることがあります。
- コンテナディスクの割り当てが完了すると、必要なパーティショニングとパーティションの割り当てがONTAPソフトウェアで自動的に処理されます。

手順

1. CLIを使用して、パーティショニングされたディスクの現在の所有権を表示します。

```
storage disk show -disk disk_name -partition-ownership
```

2. CLIの権限レベルをadvancedに設定します。

```
set -privilege advanced
```

3. 所有権を割り当てる所有権のエンティティに応じて、適切なコマンドを入力します。

所有権エンティティのいずれかがすでに所有されている場合は'-force'オプションを含める必要があります

所有権を割り当てる所有権のエンティティ	使用するコマンド
コンテナディスク	<code>storage disk assign -disk disk_name -owner owner_name</code>
データパーティション	<code>storage disk assign -disk disk_name -owner owner_name -data true</code>
ルートパーティション	<code>storage disk assign -disk disk_name -owner owner_name -root true</code>

## オプション2：ルート/データ/データ（RD2）パーティショニングを使用してディスクを手動で割り当てる

ルート/データ/データパーティショニングでは、HAペアがまとめて所有する所有権の4つのエンティティ（コンテナディスクと3つのパーティション）があります。ルート/データ/データパーティショニングは、ルートパーティションとして小さなパーティションを1つ作成し、データ用に同じサイズの大きなパーティションを2つ作成します。

### このタスクについて

- パラメータは、とともに使用する必要があります `disk assign` コマンドを使用して、ルート/データ/データパーティショニングされたディスクに適切なパーティションを割り当てることができます。これらのパラメータは、ストレージプールに含まれるディスクでは使用できません。デフォルト値は「false」です。
  - 。 `-data1 true` パラメータを指定すると、パーティショニングされたroot-data1-data2ディスクの「data1」パーティションが割り当てられます。
  - 。 `-data2 true` パラメータを指定すると、パーティショニングされたroot-data1-data2ディスクの「data2」パーティションが割り当てられます。
- 収容数が半分のシェルフのコンテナディスクで障害が発生して交換した場合、この場合、ONTAPでは所有権が常に自動割り当てされるとは限らないため、ディスク所有権の手動割り当てが必要になることがあります。
- コンテナディスクの割り当てが完了すると、必要なパーティショニングとパーティションの割り当てがONTAPソフトウェアで自動的に処理されます。

### 手順

- CLIを使用して、パーティショニングされたディスクの現在の所有権を表示します。

```
storage disk show -disk disk_name -partition-ownership
```

- CLI の権限レベルを `advanced` に設定します。

```
set -privilege advanced
```

- 所有権を割り当てる所有権のエンティティに応じて、適切なコマンドを入力します。

所有権エンティティのいずれかがすでに所有されている場合は'-forceオプションを含める必要があります

所有権を割り当てる所有権のエンティティ	使用するコマンド
コンテナディスク	<code>storage disk assign -disk disk_name -owner owner_name</code>
Data1 パーティション	<code>storage disk assign -disk disk_name -owner owner_name -data1 true</code>
data2 パーティション	<code>storage disk assign -disk disk_name -owner owner_name -data2 true</code>

ルートパーティション

```
storage disk assign -disk disk_name -owner owner_name  
-root true
```



### オプション3：ルートパーティションを含むDS460Cコンテナドライブを手動で割り当てる

DS460Cシェルフのみを含むHAペアを初期化する場合は、ハーフドロワーのポリシーに従って、ルートパーティションを含むコンテナドライブに所有権を手動で割り当てる必要があります。

このタスクについて

- DS460Cシェルフのみを含むHAペアを初期化する場合、ADPブートメニュー（ONTAP 9.2以降で使用可能）オプション9aおよび9bではドライブ所有権の自動割り当てがサポートされません。ハーフドロワーのポリシーに従って、ルートパーティションを含むコンテナドライブを手動で割り当てる必要があります。

HAペアの初期化（ブート）後、ディスク所有権の自動割り当てが自動的に有効になり、ハーフドロワーポリシーを使用して残りのドライブ（ルートパーティションを含むコンテナドライブを除く）と今後追加されるすべてのドライブ（障害が発生したドライブの交換など）に所有権が割り当てられます。「low spares（スペア不足）」というメッセージに応答するか、容量を追加しています。

- 次のトピックで、ハーフドロワーポリシーについて学習します。["ディスク所有権の自動割り当てについて"](#)。

手順

- DS460Cシェルフがフル装備されていない場合は、次の手順を実行します。フル装備されていない場合は、次の手順に進みます。

- まず、各ドロワーの前列（ドライブベイ0、3、6、9）にドライブを取り付けます。

各ドロワーの前列にドライブを取り付けると、適切な通気が確保され、過熱を防ぐことができます。

- 残りのドライブについては、各ドロワーに均等に配置します。

引き出しの列を前面から背面に充填します。行を埋めるための十分なドライブがない場合は、ドライブがドロワーの左右に均等に配置されるように2本ずつ取り付けます。

次の図は、DS460Cドロワー内のドライブベイの番号と場所を示しています。



2. ノード管理LIFまたはクラスタ管理LIFを使用してクラスタシェルにログインします。
3. 各ドロワーについて、次の手順を実行してハーフドロワーポリシーに準拠し、ルートパーティションを含むコンテナドライブを手動で割り当てます。

ハーフドロワーポリシーでは、ドロワーのドライブの左半分（ベイ0<sub>5</sub>）をノードAに、右半分（ベイ6<sub>11</sub>）をノードBに割り当てます。

- a. 所有権が未設定のすべてのディスクを表示

```
storage disk show -container-type unassigned
```

- b. ルートパーティションを含むコンテナドライブを割り当てます。

```
storage disk assign -disk disk_name -owner owner_name
```

ワイルドカード文字を使用すると、一度に複数のドライブを割り当てることができます。

ルート/データパーティショニングを使用して、ノードにアクティブ/パッシブ構成を設定します

工場出荷時にルートデータのパーティショニングを使用するようにHAペアが構成されている場合は、アクティブ/アクティブ構成で使用するために、データパーティションの所有権がペアの両方のノードに分割されます。アクティブ/パッシブ構成でHAペアを使用する場合は、データローカル階層（アグリゲート）を作成する前にパーティションの所有権を更新する必要があります。

必要なもの

- アクティブノードおよびパッシブノードとして指定するノードを決めておく必要があります。
- HA ペアでストレージフェイルオーバーを設定する必要があります。

このタスクについて

このタスクは、ノード A とノード B の 2 つのノードで実行します

この手順は、パーティショニングされたディスクからデータローカル階層（アグリゲート）が作成されていないノード用に設計されています。

詳細はこちら ["高度なディスクパーティショニング"](#)。

手順

すべてのコマンドがクラスタシェルに入力されます。

1. データパーティションの現在の所有権を表示します。

```
storage aggregate show-spare-disks
```

この出力から、一方のノードが半数のデータパーティションを所有し、もう一方のノードが残り半数のデータパーティションを所有していることがわかります。すべてのデータパーティションがスペアである必要があります。

```
cluster1::> storage aggregate show-spare-disks
```

Original Owner: cluster1-01

Pool0

Partitioned Spares

Local

Local

Data

Root Physical

Disk	Type	RPM	Checksum	Usable
Usable Size				
-----	-----	-----	-----	-----
-----	-----	-----	-----	-----
1.0.0	BSAS	7200	block	753.8GB
0B 828.0GB				
1.0.1	BSAS	7200	block	753.8GB
73.89GB 828.0GB				
1.0.5	BSAS	7200	block	753.8GB
0B 828.0GB				
1.0.6	BSAS	7200	block	753.8GB
0B 828.0GB				
1.0.10	BSAS	7200	block	753.8GB
0B 828.0GB				
1.0.11	BSAS	7200	block	753.8GB
0B 828.0GB				

Original Owner: cluster1-02

Pool0

Partitioned Spares

Local

Local

Data

Root Physical

Disk	Type	RPM	Checksum	Usable
Usable Size				
-----	-----	-----	-----	-----
-----	-----	-----	-----	-----
1.0.2	BSAS	7200	block	753.8GB
0B 828.0GB				
1.0.3	BSAS	7200	block	753.8GB
0B 828.0GB				
1.0.4	BSAS	7200	block	753.8GB
0B 828.0GB				
1.0.7	BSAS	7200	block	753.8GB
0B 828.0GB				
1.0.8	BSAS	7200	block	753.8GB
73.89GB 828.0GB				
1.0.9	BSAS	7200	block	753.8GB

```
0B 828.0GB
12 entries were displayed.
```

2. advanced 権限レベルに切り替えます。

```
set advanced
```

3. パッシブノードとして指定するノードが所有する各データパーティションをアクティブノードに割り当てます。

```
storage disk assign -force -data true -owner active_node_name -disk disk_name
```

パーティションをディスク名の一部に含める必要はありません。

再割り当てが必要なデータパーティションごとに、次の例のようなコマンドを入力します。

```
storage disk assign -force -data true -owner cluster1-01 -disk 1.0.3
```

4. すべてのパーティションがアクティブノードに割り当てられていることを確認します。

```
cluster1::*> storage aggregate show-spare-disks
```

Original Owner: cluster1-01

Pool0

Partitioned Spares

Local		Local		Data	
Root	Physical			Usable	
Disk		Type	RPM	Checksum	Usable
Usable	Size				
1.0.0		BSAS	7200	block	753.8GB
0B 828.0GB					
1.0.1		BSAS	7200	block	753.8GB
73.89GB 828.0GB					
1.0.2		BSAS	7200	block	753.8GB
0B 828.0GB					
1.0.3		BSAS	7200	block	753.8GB
0B 828.0GB					
1.0.4		BSAS	7200	block	753.8GB
0B 828.0GB					
1.0.5		BSAS	7200	block	753.8GB
0B 828.0GB					
1.0.6		BSAS	7200	block	753.8GB
0B 828.0GB					

```

1.0.7          BSAS      7200 block      753.8GB
0B  828.0GB
1.0.8          BSAS      7200 block      753.8GB
0B  828.0GB
1.0.9          BSAS      7200 block      753.8GB
0B  828.0GB
1.0.10         BSAS      7200 block      753.8GB
0B  828.0GB
1.0.11         BSAS      7200 block      753.8GB
0B  828.0GB

Original Owner: cluster1-02
Pool0
Partitioned Spares

Local
Local
Data
Root Physical
Disk          Type      RPM Checksum      Usable
Usable      Size
-----
1.0.8          BSAS      7200 block      0B
73.89GB  828.0GB
13 entries were displayed.

```

cluster1-02 が引き続きスペアルートパーティションを所有していることに注意してください。

##### 5. admin 権限に戻ります。

```
set admin
```

##### 6. データアグリゲートを作成し、少なくとも 1 つのデータパーティションをスペアとして残します。

```
storage aggregate create new_aggr_name -diskcount number_of_partitions -node
active_node_name
```

データアグリゲートが作成され、アクティブノードが所有します。

ルート/データ/データパーティショニングを使用して、ノードにアクティブ/パッシブ構成を設定します

工場出荷時にルート/データ/データパーティショニングを使用するようにHAペアが構成されている場合は、アクティブ/アクティブ構成で使用するために、データパーティションの所有権がペアの両方のノードに分割されます。アクティブ/パッシブ構成でHAペアを使用する場合は、データローカル階層（アグリゲート）を作成する前にパーティションの所有権を更新する必要があります。

## 必要なもの

- アクティブノードおよびパッシブノードとして指定するノードを決めておく必要があります。
- HA ペアでストレージフェイルオーバーを設定する必要があります。

## このタスクについて

このタスクは、ノード A とノード B の 2 つのノードで実行します

この手順は、パーティショニングされたディスクからデータローカル階層（アグリゲート）が作成されていないノード用に設計されています。

詳細はこちら ["高度なディスクパーティショニング"](#)。

## 手順

コマンドはすべてクラスタシェルで入力します。

1. データパーティションの現在の所有権を表示します。

```
storage aggregate show-spare-disks -original-owner passive_node_name -fields  
local-usable-data1-size, local-usable-data2-size
```

この出力から、一方のノードが半数のデータパーティションを所有し、もう一方のノードが残り半数のデータパーティションを所有していることがわかります。すべてのデータパーティションがスペアである必要があります。

2. advanced 権限レベルに切り替えます。

```
set advanced
```

3. パッシブノードとして指定するノードが所有する data1 パーティションごとに、アクティブノードに割り当てます。

```
storage disk assign -force -data1 -owner active_node_name -disk disk_name
```

パーティションをディスク名の一部に含める必要はありません

4. パッシブノードになるノードが所有する data2 パーティションごとに、アクティブノードに割り当てます。

```
storage disk assign -force -data2 -owner active_node_name -disk disk_name
```

パーティションをディスク名の一部に含める必要はありません

5. すべてのパーティションがアクティブノードに割り当てられていることを確認します。

```
storage aggregate show-spare-disks
```

```
cluster1::*> storage aggregate show-spare-disks
```

```
Original Owner: cluster1-01
```

```
Pool0
```

# Partitioned Spares

				Local
Local				
				Data
Root Physical				
Disk		Type	RPM Checksum	Usable
Usable	Size			
-----				
-----				
1.0.0		BSAS	7200 block	753.8GB
0B 828.0GB				
1.0.1		BSAS	7200 block	753.8GB
73.89GB 828.0GB				
1.0.2		BSAS	7200 block	753.8GB
0B 828.0GB				
1.0.3		BSAS	7200 block	753.8GB
0B 828.0GB				
1.0.4		BSAS	7200 block	753.8GB
0B 828.0GB				
1.0.5		BSAS	7200 block	753.8GB
0B 828.0GB				
1.0.6		BSAS	7200 block	753.8GB
0B 828.0GB				
1.0.7		BSAS	7200 block	753.8GB
0B 828.0GB				
1.0.8		BSAS	7200 block	753.8GB
0B 828.0GB				
1.0.9		BSAS	7200 block	753.8GB
0B 828.0GB				
1.0.10		BSAS	7200 block	753.8GB
0B 828.0GB				
1.0.11		BSAS	7200 block	753.8GB
0B 828.0GB				

Original Owner: cluster1-02

Pool0

# Partitioned Spares

				Local
Local				
				Data
Root Physical				
Disk		Type	RPM Checksum	Usable
Usable	Size			
-----				
-----				
1.0.8		BSAS	7200 block	0B

```
73.89GB 828.0GB
13 entries were displayed.
```

cluster1-02 が引き続きスペアルートパーティションを所有していることに注意してください。

6. admin 権限に戻ります。

```
set admin
```

7. データアグリゲートを作成し、少なくとも 1 つのデータパーティションをスペアとして残します。

```
storage aggregate create new_aggr_name -diskcount number_of_partitions -node
active_node_name
```

データアグリゲートが作成され、アクティブノードが所有します。

8. また、ONTAP の推奨されるアグリゲートレイアウトも使用できます。アグリゲートのレイアウトには、RAID グループのレイアウトとスペア数のベストプラクティスが含まれています。

```
storage aggregate auto-provision
```

ディスクから所有権を削除します

ONTAP は、ディスク所有権情報をディスクに書き込みます。スペアディスクまたはそのシェルフをノードから取り外す前に、所有権情報を削除して、別のノードに適切に統合できるようにする必要があります。



ディスクがルート/データパーティショニング用にパーティショニングされており、ONTAP 9.10.1以降を実行している場合は、NetAppテクニカルサポートに連絡して所有権を削除してください。詳細については、を参照してください ["技術情報アーティクル「Failed to remove the owner of disk」"](#)。

必要なもの

所有権を削除するディスクが次の要件を満たしている必要があります。

- スペアディスクである。

ローカル階層（アグリゲート）で使用されているディスクから所有権を削除することはできません。

- Maintenance Center に割り当てられていない。
- 完全消去の実行中ではない。
- 障害ディスクではない。

障害が発生したディスクから所有権を削除する必要はありません。

このタスクについて

ディスクの自動割り当てが有効になっている場合は、ノードからディスクを取り外す前に、ONTAP によって所有権が自動的に再割り当てされます。そのため、ディスクが取り外されるまで所有権の自動割り当てを無効



にしてから再度有効にします。

#### 手順

1. ディスク所有権の自動割り当てを有効にしている場合は、CLIを使用して無効にします。

```
storage disk option modify -node node_name -autoassign off
```

2. 必要に応じて、ノードの HA パートナーで前述の手順を繰り返します。
3. ディスクからソフトウェア所有権情報を削除します。

```
storage disk removeowner disk_name
```

複数のディスクから所有権情報を削除するには、カンマで区切ったリストを使用します。

#### 例

```
storage disk removeowner sys1:0a.23,sys1:0a.24,sys1:0a.25
```

4. ディスクがルート/データパーティショニング用にパーティショニングされていて、ONTAP 9.9.1以前を実行している場合は、パーティションから所有権を削除します。

```
storage disk removeowner -disk disk_name -root true
```

```
storage disk removeowner -disk disk_name -data true
```

これで、両方のパーティションはどのノードからも所有されなくなります。

5. ディスク所有権の自動割り当てを無効にしていた場合は、ディスクが取り外されたあと、または再割り当てされたあとに再度有効にします。

```
storage disk option modify -node node_name -autoassign on
```

6. 必要に応じて、ノードの HA パートナーで前述の手順を繰り返します。

#### 障害が発生したディスクを取り外します

完全な障害状態にあるディスクは、ONTAP で使用可能なディスクとみなされなくなり、ディスクシェルフからただちに取り外すことができます。ただし、障害が部分的に発生したディスクは、高速 RAID リカバリプロセスが完了するまで接続したままにしておく必要があります。

#### このタスクについて

障害が発生したり、エラーメッセージが頻繁に生成されたりするために取り外したディスクは、そのストレージシステムまたは他のストレージシステムで再利用しないでください。

#### 手順

1. CLIを使用して障害ディスクのディスクIDを確認します。

```
storage disk show -broken
```

障害ディスクのリストにディスクが表示されない場合、高速RAIDリカバリの実行中に部分的な障害が発生している可能性があります。この場合は、障害ディスクのリストに表示されるまで（つまり高速 RAID リカバリプロセスが完了するまで）待ってから、ディスクを取り外してください。

2. 取り外すディスクの物理的な場所を確認します。

```
storage disk set-led -action on -disk disk_name 2
```

ディスク前面の障害 LED が点灯します。

3. ディスクシェルフモデルのハードウェアガイドの指示に従い、ディスクシェルフからディスクを取り外します。

ディスク完全消去

ディスク完全消去の概要

ディスク完全消去は、元のデータのリカバリが不可能になるように、指定したバイトパターンまたはランダムデータでディスクや SSD を上書きして、データを物理的に消去するプロセスです。完全消去プロセスを使用すると、ディスク上のデータをリカバリできなくなります。

この機能は、ONTAP 9 のすべてのリリースのノードシェルから、メンテナンスモードの ONTAP 9.6 以降で利用できます。

ディスク完全消去プロセスでは、1 回の処理で最大 7 サイクルまで、3 連続のデフォルトまたはユーザ指定バイトによる上書きパターンが実行されます。サイクルごとにランダムな上書きパターンが繰り返されます。

ディスク容量、パターン、およびサイクル数によっては、このプロセスに数時間かかることがあります。完全消去はバックグラウンドで実行されます。完全消去プロセスは、開始、停止、およびステータスの表示が可能です。完全消去プロセスには、「フォーマットフェーズ」と「パターン上書きフェーズ」の2つのフェーズがあります。

フォーマットフェーズ

次の表に示すように、フォーマットフェーズで実行される処理は、完全消去するディスクのクラスによって異なります。

ディスククラス	フォーマットフェーズ処理
大容量 HDD	スキップしました
高性能 HDD	SCSI フォーマット処理
SSD	SCSI 完全消去処理

パターン上書きフェーズ

指定した上書きパターンが指定したサイクル数だけ反復されます。

完全消去プロセスが完了すると、指定したディスクは完全に消去された状態になります。これらのディスクは、自動的にスベア状態に戻りません。新たに完全消去したディスクを別のアグリゲートに追加できるようにするには、完全消去したディスクをスベアプールに戻す必要があります。

ディスク完全消去を実行できない状況

ディスク完全消去はすべてのディスクタイプでサポートされているわけではありません。また、ディスク完全消去を実行できない状況もあります。

- 一部のパーツ番号の SSD ではサポートされていません。

ディスク完全消去がサポートされる SSD のパーツ番号については、を参照してください "[Hardware Universe](#)"。

- HA ペアのシステムのテイクオーバーモードではサポートされません。
- 読み取り / 書き込みの問題が原因で障害が発生したディスクでは実行できません。
- ATA ドライブでは、フォーマットフェーズは実行されません。
- ランダムパターンを使用している場合、一度に 100 本を超えるディスクに対して実行することはできません。
- アレイ LUN ではサポートされません。
- 同一の ESH シェルフ内の SES ディスクを両方同時に完全消去する場合、シェルフへのアクセスに関するエラーがコンソールに表示され、完全消去の実行中はシェルフに関する警告は報告されません。

ただし、そのシェルフへのデータアクセスは中断されません。

ディスクの完全消去が中断された場合の動作

ユーザによる操作や予期 ONTAP しない停電などによってディスク完全消去が中断された場合、完全消去を実行していたディスクは既知の状態に戻されますが、完全消去プロセスを完了するには手動の処理も必要になります。

ディスク完全消去の処理には時間がかかります。停電、システムパニック、手動操作などによって完全消去プロセスが中断された場合は、完全消去プロセスを最初からやり直す必要があります。この場合、ディスクは完全消去済みとはみなされません。

ディスク完全消去がフォーマットフェーズ中に中断された場合、ONTAP は、中断によって破損したすべてのディスクをリカバリします。ONTAP は、システムのリブート後 1 時間ごとに、完全消去のフォーマットフェーズが完了していないターゲットディスクの有無をチェックします。該当するディスクが見つかったら、ONTAP によってリカバリされます。リカバリ方法はディスクの種類によって異なります。ディスクのリカバリが完了したら、そのディスクで完全消去プロセスを再実行できます。HDD の場合は使用できます `-s` フォーマットフェーズを再度繰り返さないように指定するオプション。

完全消去するデータを含むローカル階層（アグリゲート）の作成とバックアップについてのヒント

完全消去が必要なデータを格納するためにローカル階層（アグリゲート）を作成またはバックアップする場合は、次に示す簡単なガイドラインに従うことで、データ完全消去にかかる時間を短縮できます。

- 機密データが含まれるローカル階層が、必要以上に大きくないことを確認してください。

必要以上に大きいと、完全消去の実行に、より多くの時間、ディスクスペース、帯域幅が必要になります。

- 機密データが格納されているローカル階層をバックアップする場合は、非機密データを大量に含むローカル階層へのバックアップは避けてください。

これにより、機密データを完全消去する前に、非機密データの移行に必要なリソースを削減できます。

#### ディスクを完全消去する

ディスクを完全消去すると、運用を終了したシステムや動作していないシステムのディスクやディスクのセットからデータを削除し、データをリカバリできないようにすることができます。

CLIを使用してディスクを完全消去するには、次の2つの方法があります。

ディスクの完全消去には、保守モードのコマンド（**ONTAP 9.6**以降のリリース）を使用します。

ONTAP 9.6 以降では、メンテナンスモードでディスク完全消去を実行できます。

作業を開始する前に

- 自己暗号化ディスク（SED）を使用することはできません。

を使用する必要があります `storage encryption disk sanitize SED`を完全消去するコマンド。

["保存データの暗号化"](#)

手順

1. メンテナンスモードでブートします。
  - a. コマンドを入力して、現在のシェルを終了します `halt`。  
  
LOADER プロンプトが表示されます。
  - b. コマンドを入力してメンテナンスモードに切り替えます `boot_ontap maint`。  
  
情報が表示されると、保守モードのプロンプトが表示されます。
2. 完全消去するディスクがパーティショニングされている場合は、各ディスクのパーティショニングを解除します。



ディスクのパーティショニングを解除するコマンドはdiagレベルでのみ使用でき、ネットアップサポートの指示があった場合にのみ実行してください。作業を進める前に、ネットアップサポートに問い合わせることを推奨します。  
Knowledge Base記事も参照できます ["ONTAP でスペアドライブのパーティショニングを解除する方法"](#)

```
disk unpartition disk_name
```

3. 指定したディスクを完全消去します。

```
disk sanitize start [-p pattern1|-r [-p pattern2|-r [-p pattern3|-r]]] [-c cycle_count] disk_list
```



完全消去中はノードの電源をオフにしたり、ストレージの接続を切断したり、ターゲットディスクを取り外したりしないでください。完全消去のフォーマットフェーズで処理が中断された場合、ディスクを完全消去してスペアプールに戻せる状態にするには、フォーマットフェーズを再起動して完了させる必要があります。完全消去プロセスを中止する必要がある場合は、`disk sanitize abort` コマンドを実行します指定したディスクで完全消去のフォーマットフェーズが進行中の場合、そのフェーズが完了するまで処理は中止されません。

```
`-p` `_pattern1_` `-p` `_pattern2_` `-p` `_pattern3_`
```

1~3サイクルのユーザ定義の上書きパターンを16進数で指定します。このパターンは、完全消去するディスクに順に適用されます。デフォルトのパターンは 3 回で、最初のパスに 0x55 、 2 番目のパスに 0xaa 、 3 番目のパスに 0x3C が使用されます。

-r パターン化された上書きを、一部またはすべてのパスのランダムな上書きに置き換えます。

-c *cycle\_count* 指定した上書きパターンを適用する回数を指定します。デフォルト値は 1 サイクルです。最大値は 7 サイクルです。

*disk\_list* 完全消去するスペアディスクのIDを、スペースで区切って指定します。

4. 必要に応じて、ディスク完全消去プロセスのステータスを確認します。

```
disk sanitize status [disk_list]
```

5. 完全消去プロセスが完了したら、各ディスクのスペアステータスにディスクを戻します。

```
disk sanitize release disk_name
```

6. メンテナンスモードを終了します。

ONTAP 9のすべてのバージョンで、ノードシェルコマンドを使用してディスク完全消去を有効にした場合、一部の下のレベルのONTAP コマンドが無効になります。ノードで有効にしたディスク完全消去を無効にすることはできません。

#### 開始する前に

- ディスクはスペアディスクである必要があります。ノードに所有されており、ローカル階層（アグリゲート）で使用されていないディスクを指定する必要があります。

ディスクがパーティショニングされている場合、パーティションをローカル階層（アグリゲート）で使用することはできません。

- 自己暗号化ディスク（SED）を使用することはできません。

を使用する必要があります `storage encryption disk sanitize SED`を完全消去するコマンド。

#### "保存データの暗号化"

- ストレージプールの一部であるディスクを使用することはできません。

#### 手順

- 完全消去するディスクがパーティショニングされている場合は、各ディスクのパーティショニングを解除します。



ディスクのパーティショニングを解除するコマンドはdiagレベルでのみ使用でき、ネットアップサポートの指示があった場合にのみ実行してください。続行する前に、**NetApp**サポートに問い合わせることを強くお勧めします。ナレッジベースの記事も参照してください。"[ONTAP でスペアドライブのパーティショニングを解除する方法](#)"。

```
disk unpartition disk_name
```

- 完全消去するディスクを所有するノードのノードシェルに切り替えます。

```
system node run -node node_name
```

- ディスク完全消去を有効にします。

```
options licensed_feature.disk_sanitization.enable on
```

このコマンドは取り消すことができないため、確認を求められます。

- ノードシェルの advanced 権限レベルに切り替えます。

```
priv set advanced
```

- 指定したディスクを完全消去します。

```
disk sanitize start [-p pattern1|-r [-p pattern2|-r [-p pattern3|-r]]] [-c cycle_count] disk_list
```



ノードの電源をオフにしたり、ストレージ接続を中断したり、ターゲットを取り外したりしないでください。  
完全消去中のディスク。完全消去がフォーマットフェーズで中断された場合、フォーマットは  
ディスクを完全消去して使用できる状態にするには、フェーズを再起動して完了させる必要があります。  
スペアプールに戻ります。完全消去プロセスを中止する必要がある場合は、ディスク完全消去を使用して中止できます。  
中止コマンド指定したディスクで完全消去のフォーマットフェーズが進行中の場合、フェーズが完了するまで中止は実行されません。

`-p pattern1 -p pattern2 -p pattern3` 1〜3個のユーザー定義16進数バイトのサイクルを指定します。

完全消去するディスクに連続して適用できる上書きパターン。デフォルトパターンは3つのパスで、最初のパスには0x55、2番目のパスには0xaa、2番目のパスには0x3Cを使用します。  
3回目のパス。

`-r` パターン化された上書きを、一部またはすべてのパスのランダムな上書きに置き換えます。

`-c cycle_count` 指定した上書きパターンを適用する回数を指定します。

デフォルト値は 1 サイクルです。最大値は 7 サイクルです。

`disk_list` 完全消去するスペアディスクのIDを、スペースで区切って指定します。

6. ディスク完全消去プロセスのステータスを確認するには、次のコマンドを入力します。

```
disk sanitize status [disk_list]
```

7. 完全消去プロセスが完了したら、ディスクをスペア状態に戻します。

```
disk sanitize release disk_name
```

8. ノードシェルの `admin` 権限レベルに戻ります。

```
priv set admin
```

9. ONTAP CLI に戻ります。

```
exit
```

10. すべてのディスクがスペア状態に戻ったかどうかを確認します。

```
storage aggregate show-spare-disks
```

状況	作業
完全消去したすべてのディスクがスペアとして表示されます	これで終了です。ディスクは完全消去され、スペア状態になります。



完全消去した一部のディスクが  
スペアとして表示されない

次の手順を実行します。

- a. advanced 権限モードに切り替えます。

```
set -privilege advanced
```

- b. 完全消去した未割り当てのディスクを各ディスクの適切なノードに割り当てます。

```
storage disk assign -disk disk_name -owner  
node_name
```

- c. 各ディスクのディスクをスペア状態に戻します。

```
storage disk unfail -disk disk_name -s -q
```

- d. adminモードに戻ります。

```
set -privilege admin
```

## 結果

指定したディスクが完全消去され、ホットスペアとしてマーキングされます。完全消去したディスクのシリアル番号がに書き込まれます `/etc/log/sanitized_disks`。

指定されたディスクの完全消去ログ（各ディスクで何が完了したかを示す）がに書き込まれます。  
`/mroot/etc/log/sanitization.log`。

ディスクの管理用コマンドです

を使用できます `storage disk` および `storage aggregate` ディスクを管理するためのコマンド。

状況	使用するコマンド
パーティショニングされたディスクを含むスペアディスクのリストを所有者別に表示します	<code>storage aggregate show-spare-disks</code>
アグリゲートごとのディスクの RAID タイプ、現在の使用状況、および RAID グループを表示します	<code>storage aggregate show-status</code>
スペアを含む RAID タイプ、現在の使用状況、アグリゲート、および RAID グループを表示する 物理ディスクの場合	<code>storage disk show -raid</code>
障害が発生したディスクの一覧を表示します	<code>storage disk show -broken</code>

ディスクのクラスタ構成前の（nodescope）ドライブ名を表示する	<code>storage disk show -primary-paths</code> （アドバンスト）
特定のディスクまたはシェルフの LED を点灯します	<code>storage disk set-led</code>
特定のディスクに対するチェックサム方式を表示する	<code>storage disk show -fields checksum-compatibility</code>
すべてのスペアディスクに対するチェックサム方式を表示する	<code>storage disk show -fields checksum-compatibility -container-type spare</code>
ディスクの接続および配置の情報を表示します	<code>storage disk show -fields disk,primary-port,secondary-name,secondary-port,shelf,bay</code>
特定のディスクのクラスタ構成前のディスク名を表示する	<code>storage disk show -disk diskname -fields diskpathnames</code>
Maintenance Center に割り当てられたディスクの一覧を表示する	<code>storage disk show -maintenance</code>
SSD の寿命を表示します	<code>storage disk show -ssd-wear</code>
共有ディスクのパーティショニングを解除します	<code>storage disk unpartition</code> （diagnosticレベルで使用可能）
初期化されていないすべてのディスクを初期化する	<code>storage disk zerospares</code>
指定した 1 つ以上のディスク上で進行中の完全消去プロセスを停止します	<code>system node run -node nodename -command disk sanitize</code>
ストレージ暗号化に関するディスク情報を表示します	<code>storage encryption disk show</code>
リンクされたすべてのキー管理サーバから認証キーを取得します	<code>security key-manager restore</code>

## 関連情報

### "ONTAP 9 コマンド"

## スペース情報を表示するコマンド

を使用します `storage aggregate` および `volume` アグリゲート、ボリューム、およびそれらのSnapshotコピーで使用されているスペースの状況を表示するコマンドです。

表示する情報	使用するコマンド
使用済みスペースの割合および利用可能スペースの割合に関する詳細も含む、アグリゲート、Snapshot リザーブのサイズ、およびその他のスペース使用量情報	<pre>storage aggregate show storage aggregate show-space -fields snap-size-total,used-including- snapshot-reserve</pre>
アグリゲートでのディスクと RAID グループの使用状況および RAID のステータス	<pre>storage aggregate show-status</pre>
特定の Snapshot コピーを削除した場合に再利用可能になるディスクスペースの量	<pre>volume snapshot compute-reclaimable</pre>
ボリュームによって使用されているスペースの量	<pre>volume show -fields size,used,available,percent-used volume show-space</pre>
包含アグリゲートでボリュームによって使用されているスペースの量	<pre>volume show-footprint</pre>

#### 関連情報

["ONTAP 9 コマンド"](#)

ストレージシェルフに関する情報を表示するコマンド

を使用します `storage shelf show` コマンドを使用して、ディスクシェルフの構成情報やエラー情報を表示します。

表示する項目	使用するコマンド
シェルフの構成とハードウェアのステータスに関する一般的な情報	<pre>storage shelf show</pre>
スタック ID を含む、特定のシェルフの詳細情報	<pre>storage shelf show -shelf</pre>
シェルフごとの対応可能な未解決のエラーです	<pre>storage shelf show -errors</pre>
ベイ情報	<pre>storage shelf show -bay</pre>
接続情報	<pre>storage shelf show -connectivity</pre>
温度センサーや冷却ファンなどの冷却情報	<pre>storage shelf show -cooling</pre>
I/O モジュールに関する情報	<pre>storage shelf show -module</pre>

表示する項目	使用するコマンド
ポート情報	<code>storage shelf show -port</code>
PSU（電源装置ユニット）、電流センサー、電圧センサーなどの電源情報	<code>storage shelf show -power</code>

関連情報

["ONTAP 9コマンド"](#)

## RAID構成を管理します

### RAID構成の管理の概要

システム内のRAID構成を管理するためのさまざまな手順を実行できます。

- \* RAID構成管理の側面\* :
  - ["ローカル階層（アグリゲート）のデフォルトのRAIDポリシー"](#)
  - ["ディスクの RAID 保護レベル"](#)
- ローカル階層（アグリゲート）のドライブおよび**RAID**グループ情報
  - ["ローカル階層（アグリゲート）のドライブおよびRAIDグループの情報を確認する"](#)
- \* RAID構成の変換\*
  - ["RAID-DP から RAID-TEC に変換します"](#)
  - ["RAID-TEC からRAID-DPに変換します"](#)
- \* RAIDグループのサイジング\*
  - ["RAID グループのサイジングに関する考慮事項"](#)
  - ["RAIDグループのサイズをカスタマイズする"](#)

ローカル階層（アグリゲート）のデフォルトの**RAID**ポリシー

すべての新しいローカル階層（アグリゲート）のデフォルトのRAIDポリシーはRAID-DPまたはRAID-TECです。RAID ポリシーによって、ディスク障害が発生した場合に使用するパリティ保護が決まります。

RAID-DP は、単一ディスク障害または二重ディスク障害が発生した場合にダブルパリティ保護を提供します。RAID-DPは、次のタイプのローカル階層（アグリゲート）のデフォルトのRAIDポリシーです。

- オールフラッシュローカル階層
- Flash Poolローカル階層
- 高パフォーマンスハードディスクドライブ（HDD）ローカル階層

RAID-TEC は、AFF を含むすべてのディスクタイプおよびプラットフォームでサポートされます。大容量のディスクを含むローカル階層は、同時にディスク障害が発生する可能性が高くなります。RAID-TEC では、ト

リプルパリティ保護を提供することでこのリスクを軽減し、最大 3 本のディスクで同時に障害が発生してもデータを保護できます。RAID-TEC は、6TB以上のディスクを含む大容量HDDローカル階層のデフォルトのRAIDポリシーです。

各RAIDポリシータ입に必要なディスクの最小数：

- RAID-DP：5本以上のディスク
- RAID-TEC：最低7本のディスク

#### ディスクの **RAID** 保護レベル

ONTAP では、ローカル階層（アグリゲート）に対して3つのレベルのRAID保護をサポートしています。RAID保護のレベルによって、ディスク障害が発生した場合にデータリカバリに使用できるパリティディスクの数が決まります。

RAID 保護を使用すると、RAID グループ内にデータディスク障害が発生した場合に、ONTAP は障害ディスクをスペアディスクと交換し、パリティデータを使用して障害ディスクのデータを再構築します。

##### • \* RAID 4 \*

RAID 4 保護を使用すると、ONTAP は 1 本のスペアディスクを使用して RAID グループ内の 1 本の障害ディスクを交換し、データを再構築します。

##### • \* RAID-DP \*

RAID-DP 保護を使用すると、ONTAP は最大 2 本のスペアディスクを使用して、RAID グループ内で同時に障害が発生した最大 2 本のディスクを交換し、データを再構築します。

##### • \* RAID-TEC \*

RAID-TEC 保護を使用すると、ONTAP は最大 3 本のスペアディスクを使用して、RAID グループ内で同時に障害が発生した最大 3 本のディスクを交換し、データを再構築します。

#### ローカル階層（アグリゲート）のドライブおよび**RAID**グループの情報

一部のローカル階層（アグリゲート）管理タスクでは、ローカル階層を構成するドライブのタイプ、サイズ、チェックサム、ステータス、ドライブを他のローカル階層と共有するかどうか、およびRAIDグループのサイズと構成を確認しておく必要があります。

#### ステップ

1. アグリゲートのドライブを RAID グループ別に表示します。

```
storage aggregate show-status aggr_name
```

アグリゲート内の各 RAID グループのドライブが表示されます。

ドライブ（データ、パリティ、ダブルパリティ）のRAIDタイプは確認できます `Position` 列（Column）：状況に応じて `Position` 列が表示されます。`shared` をクリックすると、そのドライブが共有されます。HDDの場合はパーティショニングされたディスクです。SSDの場合はストレージプールの一部です。

```
cluster1::> storage aggregate show-status nodeA_fp_1
```

Owner Node: cluster1-a

Aggregate: nodeA\_fp\_1 (online, mixed\_raid\_type, hybrid) (block checksums)

Plex: /nodeA\_fp\_1/plex0 (online, normal, active, pool0)

RAID Group /nodeA\_fp\_1/plex0/rg0 (normal, block checksums, raid\_dp)

Position	Disk	Pool	Type	RPM	Usable Size	Physical Size	Status
shared	2.0.1	0	SAS	10000	472.9GB	547.1GB	(normal)
shared	2.0.3	0	SAS	10000	472.9GB	547.1GB	(normal)
shared	2.0.5	0	SAS	10000	472.9GB	547.1GB	(normal)
shared	2.0.7	0	SAS	10000	472.9GB	547.1GB	(normal)
shared	2.0.9	0	SAS	10000	472.9GB	547.1GB	(normal)
shared	2.0.11	0	SAS	10000	472.9GB	547.1GB	(normal)

RAID Group /nodeA\_flashpool\_1/plex0/rg1

(normal, block checksums, raid4) (Storage Pool: SmallSP)

Position	Disk	Pool	Type	RPM	Usable Size	Physical Size	Status
shared	2.0.13	0	SSD	-	186.2GB	745.2GB	(normal)
shared	2.0.12	0	SSD	-	186.2GB	745.2GB	(normal)

8 entries were displayed.

## RAID-DP から RAID-TEC に変換します

トリプルパリティの保護を強化する場合は、RAID-DP を RAID-TEC に変換できます。ローカル階層（アグリゲート）で使用されるディスクのサイズが4TiBを超える場合は、RAID-TEC を推奨します。

必要なもの

変換するローカル階層（アグリゲート）には少なくとも7本のディスクが必要です。

このタスクについて

ハードディスクドライブ（HDD）ローカル階層はRAID-DPからRAID-TEC に変換できます。これには、Flash Poolローカル階層内のHDD階層が含まれます。

手順

1. アグリゲートがオンラインであり、少なくとも 6 本のディスクがあることを確認します。

```
storage aggregate show-status -aggregate aggregate_name
```

2. アグリゲートをRAID-DPからRAID-TECに変換します。

```
storage aggregate modify -aggregate aggregate_name -raidtype raid_tec
```

3. アグリゲートのRAIDポリシーがRAID-TECであることを確認します。

```
storage aggregate show aggregate_name
```

## RAID-TEC からRAID-DPに変換します

ローカル階層（アグリゲート）のサイズを縮小し、トリプルパリティが不要になった場合は、RAIDポリシーをRAID-TEC からRAID-DPに変換して、RAIDパリティに必要なディスクの数を減らすことができます。

### 必要なもの

RAID-TEC の最大 RAID グループサイズは、RAID-DP の最大 RAID グループサイズよりも大きくなります。最大の RAID-TEC グループサイズが RAID-DP の制限内にない場合、RAID-DP に変換することはできません。

### 手順

1. アグリゲートがオンラインであり、少なくとも 6 本のディスクがあることを確認します。

```
storage aggregate show-status -aggregate aggregate_name
```

2. アグリゲートを RAID-TEC から RAID-DP に変換します。

```
storage aggregate modify -aggregate aggregate_name -raidtype raid_dp
```

3. アグリゲートの RAID ポリシーが RAID-DP であることを確認します。

```
storage aggregate show aggregate_name
```

## RAID グループのサイジングに関する考慮事項

最適な RAID グループサイズを設定するには、さまざまな要素について優先度を考慮する必要があります。設定する（ローカル階層）アグリゲートにとって最も重要な要素を、RAIDのリカバリ速度、ドライブ障害によるデータ損失のリスクに対する保証、I/O パフォーマンスの最適化、データストレージスペースの最大化の中から決定する必要があります。

より大容量の RAID グループを作成すると、パリティに使用されるストレージ容量（パリティの負荷）と同じ容量のデータ・ストレージに使用できる容量が最大化されます。一方、大規模な RAID グループで 1 つのディスクに障害が発生した場合、再構築の時間は増加し、パフォーマンスへの影響が長時間に及びます。さらに、RAID グループ内のディスク数が増えると、その RAID グループ内で複数のディスクに障害が発生する可能性が高くなります。

### HDD またはアレイ LUN RAID グループ

HDD またはアレイ LUN を構成する RAID グループのサイジングを行う際は、次のガイドラインに従う必要が

あります。

- ローカル階層（アグリゲート）のすべてのRAIDグループを同数のディスクで構成する必要があります。

1つのローカル階層で異なるRAIDグループのディスク数を最大50%削減することも、最大でパフォーマンスのボトルネックになることもあるため、この構成は避けることを推奨します。

- RAID グループのディスク数の推奨範囲は 12~20 です。

信頼性の高いパフォーマンスディスクを使用する場合は、RAID グループのディスク数を必要に応じて最大 28 まで増やすことができます。

- 上記の 2 つのガイドラインを満たすディスク数の中から、より大きいディスク数を選択してください。

#### **Flash Poolローカル階層内のSSD RAIDグループ（アグリゲート）**

SSD RAIDグループサイズは、Flash Poolローカル階層（アグリゲート）内のHDD RAIDグループのRAIDグループサイズと同じである必要はありません。通常は、パリティに必要なSSDの数を最小限に抑えるために、Flash Poolローカル階層にはSSD RAIDグループを1つだけ作成します。

#### **SSDローカル階層内のSSD RAIDグループ（アグリゲート）**

SSD を構成する RAID グループのサイジングを行う際は、次のガイドラインに従う必要があります。

- ローカル階層（アグリゲート）内のすべてのRAIDグループを同数のドライブで構成する必要があります。

RAIDグループは完全に同じサイズにする必要はありませんが、可能な場合は、同じローカル階層内の他のRAIDグループの半分未満のRAIDグループが存在しないようにしてください。

- RAID-DP の場合、RAID グループサイズの推奨範囲は 20~28 です。

#### **RAID グループのサイズをカスタマイズする**

RAIDグループのサイズをカスタマイズして、ローカル階層（アグリゲート）に含めるストレージの容量に応じたサイズのRAIDグループを設定できます。

このタスクについて

標準のローカル階層（アグリゲート）の場合は、各ローカル階層のRAIDグループのサイズを別々に変更します。Flash Poolローカル階層の場合は、SSD RAIDグループとHDD RAIDグループのサイズを別々に変更できます。

RAID グループのサイズ変更に関する注意事項を次に示します。

- デフォルトでは、最後に作成された RAID グループのディスクまたはアレイ LUN の数が新しい RAID グループのサイズよりも少ない場合、新しいサイズになるまで、最後に作成された RAID グループにディスクまたはアレイ LUN が追加されます。
- そのローカル階層内の他のすべての既存RAIDグループのサイズは、明示的にディスクを追加しないかぎり変更されません。
- RAIDグループの原因 サイズを、ローカル階層の現在の最大RAIDグループサイズよりも大きくすることはできません。



- すでに作成されている RAID グループのサイズを縮小することはできません。
- 新しいサイズ的环境 ローカル階層内のすべてのRAIDグループ（Flash Poolローカル階層の場合は、該当するタイプのRAIDグループ- SSDまたはHDD）。

## 手順

1. 該当するコマンドを使用します。

状況	入力するコマンド
Flash Pool アグリゲートの SSD RAID グループの最大サイズを変更します	<code>storage aggregate modify -aggregate aggr_name -cache-raid-group-size size</code>
その他の RAID グループの最大サイズを変更します	<code>storage aggregate modify -aggregate aggr_name -maxraidsize size</code>

## 例

アグリゲート n1\_A4 の最大 RAID グループサイズを 20 本のディスクまたはアレイ LUN に変更するコマンドの例を次に示します。

```
storage aggregate modify -aggregate n1_a4 -maxraidsize 20
```

Flash Pool アグリゲート n1\_cache\_a2 の SSD キャッシュ RAID グループの最大サイズを 24 に変更するコマンドの例を次に示します。

```
storage aggregate modify -aggregate n1_cache_a2 -cache-raid-group-size 24
```

## Flash Poolローカル階層（アグリゲート）の管理

### Flash Pool階層（アグリゲート）の管理

システムでFlash Pool階層（アグリゲート）を管理するためのさまざまな手順を実行できます。

- キャッシングポリシー
  - ["Flash Poolのローカル階層（アグリゲート）キャッシングポリシー"](#)
  - ["Flash Poolのキャッシングポリシーを管理します"](#)
- \* SSDパーティショニング\*
  - ["ストレージプールを使用するFlash Poolローカル階層（アグリゲート）用のFlash Pool SSDパーティショニング"](#)
- 候補とキャッシュサイズ
  - ["Flash Pool の候補と最適なキャッシュサイズを確認します"](#)
- \* Flash Poolの作成\*
  - ["物理SSDを使用してFlash Poolローカル階層（アグリゲート）を作成します"](#)
  - ["SSDストレージプールを使用してFlash Poolローカル階層（アグリゲート）を作成します"](#)

## Flash Poolのローカル階層（アグリゲート）キャッシングポリシー

Flash Poolローカル階層（アグリゲート）のボリュームに対するキャッシングポリシーで、作業データセットにはFlashを導入して高性能なキャッシュを利用しながら、アクセス頻度が低いデータには低コストのHDDを使用するように定義できます。複数のFlash Poolローカル階層にキャッシュを提供する場合は、Flash Pool SSDパーティショニングを使用して、Flash Pool内のローカル階層間でSSDを共有します。

キャッシングポリシーは、Flash Poolローカル階層内のボリュームに適用されます。キャッシングポリシーを変更する前に、その機能を理解しておく必要があります。

ほとんどの場合、デフォルトのキャッシングポリシーである「auto」が使用するのに最適なキャッシングポリシーです。キャッシングポリシーを変更する必要があるのは、別のポリシーを使用したほうがワークロードのパフォーマンスが向上する場合のみです。適切でないキャッシングポリシーを設定すると、ボリュームのパフォーマンスが大幅に低下しかねません。また、時間とともにパフォーマンスの低下が進むおそれがあります。

キャッシングポリシーは、読み取りキャッシングポリシーと書き込みキャッシングポリシーを組み合わせたものです。ポリシー名は、読み取りキャッシングポリシーと書き込みキャッシングポリシーの名前をハイフンでつないだものです。ポリシー名にハイフンが含まれていない場合、書き込みキャッシングポリシーは「none」になります（「auto」ポリシーを除く）。

読み取りキャッシングポリシーは、HDDに格納されたデータに加えて、データのコピーをキャッシュに格納することで、以降の読み取りパフォーマンスを最適化します。書き込み処理用にキャッシュにデータを挿入する読み取りキャッシングポリシーの場合、キャッシュは\_write-through キャッシュとして機能します。

書き込みキャッシングポリシーを使用してキャッシュに挿入されたデータはキャッシュにのみ存在し、HDDにコピーが格納されることはありません。Flash Pool キャッシュはRAIDで保護されています。書き込みキャッシュを有効にすると、書き込み処理されたデータをキャッシュから即座に読み取ることができます。HDDへのデータの書き込みは、時間が経過してそのデータがキャッシュから削除されるまで先送りされます。

Flash Poolのローカル階層から単一層のローカル階層にボリュームを移動すると、ボリュームのキャッシングポリシーが失われます。あとでFlash Poolのローカル階層にボリュームを戻すと、デフォルトのキャッシングポリシー「auto」が割り当てられます。2つのFlash Poolローカル階層間でボリュームを移動した場合は、キャッシングポリシーが維持されます。

キャッシングポリシーを変更します

を使用して、Flash Poolローカル階層にあるボリュームのキャッシングポリシーを変更するには、CLIを使用します `-caching-policy` パラメータと `volume create` コマンドを実行します

Flash Poolのローカル階層にボリュームを作成すると、デフォルトで「auto」キャッシングポリシーがボリュームに割り当てられます。

## Flash Poolのキャッシングポリシーを管理します

Flash Poolのキャッシングポリシーの管理の概要を示します

CLIを使用すると、システムでFlash Poolのキャッシングポリシーを管理するためのさまざまな手順を実行できます。

- 準備

- "Flash Poolローカル階層（アグリゲート）のキャッシングポリシーを変更するかどうかの確認"
- キャッシングポリシーの変更
  - "Flash Poolローカル階層（アグリゲート）のキャッシングポリシーの変更"
  - "Flash Poolローカル階層（アグリゲート）のキャッシュ保持ポリシーを設定する"

**Flash Poolローカル階層（アグリゲート）のキャッシングポリシーを変更するかどうかの確認**

Flash Poolローカル階層（アグリゲート）にあるボリュームにキャッシュ保持ポリシーを割り当てて、ボリュームデータをFlash Poolキャッシュに保存する期間を決定することができます。ただし、キャッシュ保持ポリシーを変更しても、ボリュームのデータがキャッシュに保存される時間に影響を及ぼさない場合があります。

このタスクについて

データが次のいずれかの条件に当てはまる場合は、キャッシュ保持ポリシーを変更しても影響がない可能性があります。

- ワークロードがシーケンシャルである。
- ソリッドステートドライブ（SSD）にキャッシュされたランダムなブロックがワークロードによって再度読み取られない。
- ボリュームのキャッシュサイズが小さすぎます。

手順

データが満たす必要のある条件について、次の手順で確認します。このタスクは、advanced権限モードでCLIを使用して実行する必要があります。

1. CLIを使用してワークロードのボリュームを表示します。

```
statistics start -object workload_volume
```

2. ボリュームのワークロードのパターンを確認します。

```
statistics show -object workload_volume -instance volume-workload -counter sequential_reads
```

3. ボリュームのヒット率を確認します。

```
statistics show -object waf1_hya_vvol -instance volume -counter read_ops_replaced_ppercent|wc_write_blks_overwritten_percent
```

4. を決定します Cacheable Read および Project Cache Alloc ボリューム：

```
system node run -node node_name waf1 awa start aggr_name
```

5. AWA の概要を表示します。

```
system node run -node node_name waf1 awa print aggr_name
```

6. ボリュームのヒット率をと比較します Cacheable Read。

ボリュームのヒット率がよりも大きい場合 `Cacheable Read` これにより、SSDにキャッシュされたランダムブロックがワークロードで再読み取りされなくなります。

#### 7. ボリュームの現在のキャッシュサイズをと比較します Project Cache Alloc。

ボリュームの現在のキャッシュサイズがよりも大きい場合 `Project Cache Alloc` をクリックすると、ボリュームキャッシュのサイズが小さすぎます。

#### Flash Poolローカル階層（アグリゲート）のキャッシングポリシーの変更

ボリュームのキャッシングポリシーを変更する必要があるのは、別のポリシーを使用したほうがパフォーマンスが向上すると予想される場合のみです。Flash Poolローカル階層（アグリゲート）のボリュームのキャッシングポリシーを変更することができます。

必要なもの

キャッシングポリシーを変更するかどうかを確認する必要があります。

このタスクについて

ほとんどの場合、デフォルトのキャッシングポリシー「auto」は、使用できるキャッシングポリシーとして最適です。キャッシングポリシーを変更する必要があるのは、別のポリシーを使用したほうがワークロードのパフォーマンスが向上する場合のみです。適切でないキャッシングポリシーを設定すると、ボリュームのパフォーマンスが大幅に低下しかねません。また、時間とともにパフォーマンスの低下が進むおそれがあります。キャッシングポリシーを変更する場合は注意が必要です。キャッシングポリシーが変更されたボリュームでパフォーマンスに問題が発生した場合は、キャッシングポリシーを「auto」に戻してください。

ステップ

1. CLIを使用してボリュームのキャッシングポリシーを変更します。

```
volume modify -volume volume_name -caching-policy policy_name
```

例

次の例では、「vol2」という名前のボリュームのキャッシングポリシーを「none」というポリシーに変更します。

```
volume modify -volume vol2 -caching-policy none
```

#### Flash Poolローカル階層（アグリゲート）のキャッシュ保持ポリシーを設定する

Flash Poolローカル階層（アグリゲート）に含まれるボリュームにキャッシュ保持ポリシーを割り当てることができます。キャッシュ保持ポリシーが「high」に設定されたボリューム内のデータは長期間キャッシュに残り、キャッシュ保持ポリシーが「low」に設定されたボリューム内のデータはすぐに削除されます。これにより、優先度の高い情報に長期にわたって高速アクセスできるようにすることで、重要なワークロードのパフォーマンスが向上します。

必要なもの

キャッシュ保持ポリシーがデータをキャッシュに保存する期間に影響しないような状況がシステムで発生していないかどうかを把握する必要があります。

## 手順

advanced権限モードでCLIを使用して、次の手順を実行します。

1. 権限の設定を advanced に変更します。

```
set -privilege advanced
```

2. ボリュームのキャッシュ保持ポリシーを確認します。

デフォルトでは'キャッシュ保持ポリシーは"normal"です

3. キャッシュ保持ポリシーを設定します。

ONTAPバージョン	コマンドを実行します
ONTAP 9.0、9.1	<pre>priority hybrid-cache set volume_name read-cache=read_cache_value write- cache=write_cache_value cache- retention- priority=cache_retention_policy</pre> <p>設定 cache_retention_policy 終了: high データをキャッシュに長期間保持する場合に使用します。設定 cache_retention_policy 終了: low データをキャッシュからすぐに削除することができます。</p>
ONTAP 9.2以降	<pre>volume modify -volume volume_name -vserver vservers_name -caching-policy policy_name.</pre>

4. ボリュームのキャッシュ保持ポリシーが選択したオプションに変更されたことを確認します。
5. 権限の設定を admin に戻します。

```
set -privilege admin
```

ストレージプールを使用する**Flash Pool**ローカル階層（アグリゲート）用の**Flash Pool SSD**パーティショニング

複数のFlash Poolローカル階層（アグリゲート）にキャッシュを提供する場合は、Flash Poolソリッドステートドライブ（SSD）パーティショニングを使用します。Flash Pool SSDパーティショニングを使用すると、Flash Poolを使用するすべてのローカル階層でSSDを共有できます。これにより、パリティのコストを複数のローカル階層に分散させ、SSDキャッシュ割り当ての柔軟性を高めるとともに、SSDのパフォーマンスを最大限に高めることができます。

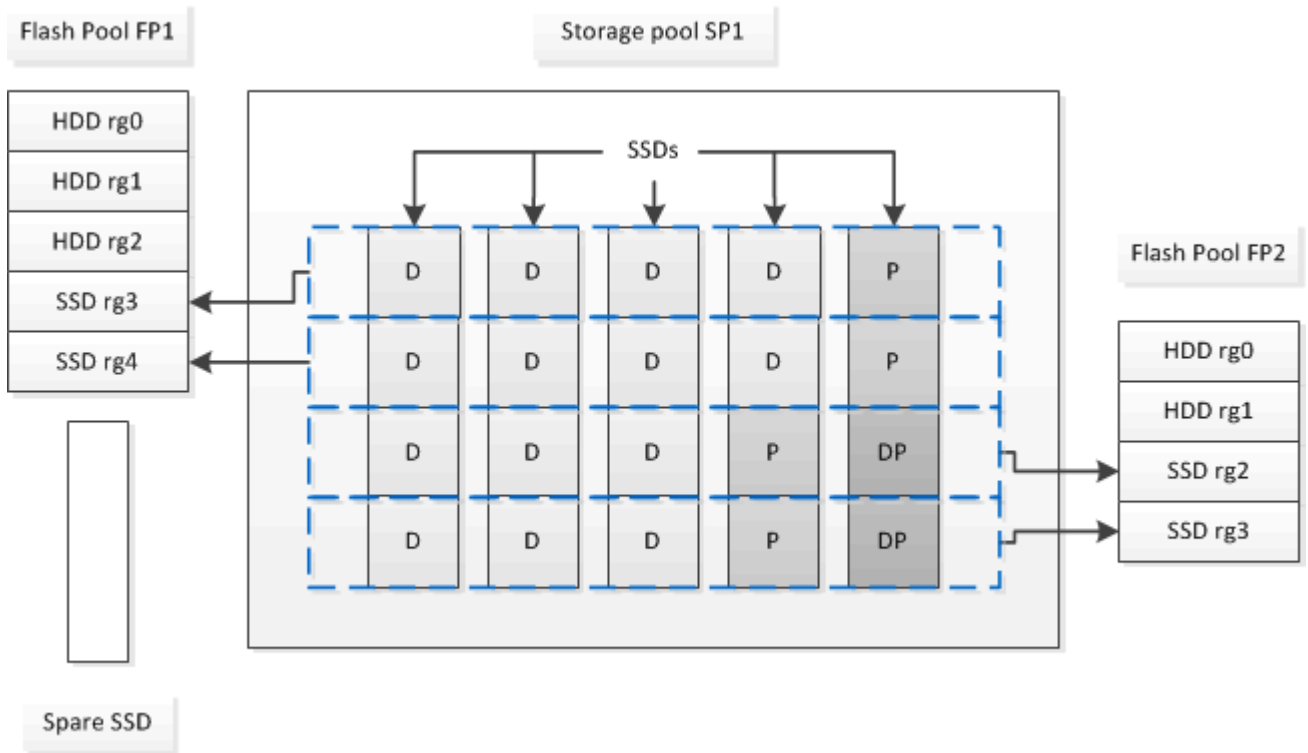
Flash Poolローカル階層で使用するSSDはストレージプールに配置する必要があります。ストレージプール内でルートデータのパーティショニング用にパーティショニングされたSSDは使用できません。ストレージプールに配置したSSDは、スタンドアロンのディスクとして管理できなくなります。また、Flash Poolに関連付

けられているローカル階層を削除してストレージプールを削除しないかぎり、SSDをストレージプールから削除することもできません。

SSD ストレージプールは、同じ大きさの 4 つの割り当て単位に分割されます。ストレージプールに追加された SSD は 4 つのパーティションに分割され、1 つのパーティションが 4 つの割り当て単位のそれぞれに割り当てられます。ストレージプール内の SSD は、同じ HA ペアによって所有されている必要があります。デフォルトでは、HA ペアの各ノードに 2 つの割り当て単位が割り当てられます。割り当て単位は、対象のローカル階層を所有するノードによって所有されている必要があります。いずれかのノード上のローカル階層に追加のFlashキャッシュが必要な場合は、一方のノードの割り当て単位数を減らしてパートナーノードの割り当て単位数を増やすようにデフォルトの割り当て単位数を変更できます。

スペアSSDを使用してSSDストレージプールに追加します。HAペアの両方のノードが所有するFlash Poolローカル階層にストレージプールが割り当て単位を提供する場合は、どちらのノードでもスペアSSDを所有できます。ただし、HAペアの一方のノードが所有するFlash Poolローカル階層にのみストレージプールが割り当て単位を提供する場合は、その同じノードがSSDスペアを所有する必要があります。

次の図は、Flash Pool SSD パーティショニングの例を示しています。SSDストレージプールは、2つのFlash Poolローカル階層にキャッシュを提供します。



ストレージプール SP1 は、5 本の SSD と 1 本のホットスペア SSD で構成されます。ストレージプールの割り当て単位 2 つが Flash Pool FP1 に割り当てられ、2 つが Flash Pool FP2 に割り当てられます。FP1 のキャッシュの RAID タイプは RAID 4 です。そのため、FP1 に提供された割り当て単位には、そのパリティに指定されたパーティションが 1 つだけ含まれます。FP2 のキャッシュの RAID タイプは RAID-DP です。そのため、FP2 に提供された割り当て単位には、パリティパーティションとダブルパリティパーティションが含まれます。

この例では、2つの割り当て単位が各Flash Poolローカル階層に割り当てられます。ただし、1つのFlash Poolローカル階層で大容量のキャッシュが必要な場合、そのFlash Poolローカル階層に3つの割り当て単位を割り当て、他の階層には1つだけ割り当てることができます。

## Flash Pool の候補と最適なキャッシュサイズを確認します

既存のローカル階層（アグリゲート）をFlash Poolローカル階層に変換する前に、ローカル階層がI/Oバウンドであるかどうか、およびワークロードと予算に応じた最適なFlash Poolのキャッシュサイズを確認できます。また、既存のFlash Poolローカル階層のキャッシュサイズが正しく設定されているかどうかを確認できます。

### 必要なもの

分析するローカル階層の負荷がピークになるおおよその時間帯を把握しておく必要があります。

### 手順

1. advanced モードに切り替えます。

```
set advanced
```

2. 既存のローカル階層（アグリゲート）がFlash Poolアグリゲートへの変換に適しているかどうかを確認する必要がある場合は、負荷のピーク時におけるアグリゲート内のディスクのビジー率と、それがレイテンシにどのような影響を及ぼすかを確認します。

```
statistics show-periodic -object disk:raid_group -instance raid_group_name
-counter disk_busy|user_read_latency -interval 1 -iterations 60
```

Flash Pool キャッシュを追加してレイテンシを短縮する処理がこのアグリゲートに適しているかどうかを判断することができます。

次のコマンドは、アグリゲート「aggr1」の最初の RAID グループの統計情報を表示します。

```
statistics show-periodic -object disk:raid_group -instance /aggr1/plex0/rg0
-counter disk_busy|user_read_latency -interval 1 -iterations 60
```

3. Automated Workload Analyzer（AWA）を起動します。

```
storage automated-working-set-analyzer start -node node_name -aggregate
aggr_name
```

指定されたアグリゲートに関連付けられているボリュームのワークロードデータの収集が開始されます。

4. advanced モードを終了します。

```
set admin
```

ピーク負荷が間隔をあけて複数回発生するまで AWA の実行を許可します。AWA は、指定されたアグリゲートに関連付けられているボリュームのワークロードの統計情報を収集し、期間内で最長 1 週間にわたってデータを分析します。複数の週にわたって AWA を実行すると、直近の週に収集されたデータのみレポートされます。キャッシュサイズの推定値は、データ収集期間内に確認された最も高い負荷に基づいています。データ収集期間全体の負荷が高くなってもかまいません。

5. advanced モードに切り替えます。

```
set advanced
```

6. ワークロードの分析を表示します。

```
storage automated-working-set-analyzer show -node node_name -instance
```

7. AWAを停止します。

```
storage automated-working-set-analyzer stop node_name
```

すべてのワークロードデータがフラッシュされ、分析に使用できなくなります。

8. advanced モードを終了します。

```
set admin
```

物理**SSD**を使用して**Flash Pool**ローカル階層（アグリゲート）を作成します

Flash Poolローカル階層（アグリゲート）を作成するには、HDD RAIDグループで構成された既存のローカル階層で該当する機能を有効にし、そのローカル階層に1つ以上のSSD RAIDグループを追加します。そのローカル階層には、SSD RAIDグループ（SSDキャッシュ）とHDD RAIDグループの2セットのRAIDグループが作成されます。

このタスクについて

ローカル階層にSSDキャッシュを追加してFlash Poolローカル階層を作成したあとで、SSDキャッシュを削除してローカル階層を元の構成に戻すことはできません。

SSD キャッシュの RAID レベルは、デフォルトでは、HDD RAID グループの RAID レベルと同じになります。最初のSSD RAIDグループを追加するときに「raidtype」オプションを指定することで、このデフォルト設定を変更できます。

作業を開始する前に

- Flash Poolローカル階層に変換する、HDDで構成された有効なローカル階層を特定しておく必要があります。
- ローカル階層に関連付けられたボリュームが書き込みキャッシュに対応しているかどうかを確認し、対応していない場合は必要な手順を実行して問題を解決しておく必要があります。
- 追加するSSDを決めておく必要があります。これらのSSDはFlash Poolローカル階層を作成するノードが所有している必要があります。
- 追加するSSDとローカル階層内の既存のHDDの両方について、チェックサム方式を確認しておく必要があります。
- 追加する SSD の数を決め、SSD RAID グループに最適な RAID グループサイズを確認しておく必要があります。

SSD キャッシュ内で使用する RAID グループが少ないほど、必要なパリティディスク数が少なくなります。RAID グループを拡張すると RAID-DP が必要になります。

- SSD キャッシュで使用する RAID レベルを決めておく必要があります。
- システムの最大キャッシュサイズを決めて、ローカル階層にSSDキャッシュを追加してもそれを超える原因は作成されないことを確認しておく必要があります。
- Flash Poolローカル階層の構成要件を確認しておく必要があります。





## 手順

FlashPoolアグリゲートは、System ManagerまたはONTAP CLIを使用して作成できます。

### System Manager の略

ONTAP 9.12.1以降では、System Managerを使用して、物理SSDを使用するFlash Poolローカル階層を作成できます。

#### 手順

1. [ストレージ]>[階層]\*を選択し、既存のローカルHDDストレージ階層を選択します。
2. 選択するオプション  次に、\* Flash Poolキャッシュの追加\*をクリックします。
3. [\*キャッシュとして専用**SSD**を使用する]を選択します。
4. ディスクタイプとディスク数を選択します。
5. RAIDタイプを選択してください。
6. [保存（Save）]を選択します。
7. ストレージ階層を特定し、.
8. [詳細]\*を選択します。Flash Poolが「enabled」\*と表示されていることを確認します。

### CLI の使用

#### 手順

1. ローカル階層（アグリゲート）をFlash Poolアグリゲートとして使用できるように指定します。

```
storage aggregate modify -aggregate aggr_name -hybrid-enabled true
```

この手順が正常に完了しない場合は、ターゲットアグリゲートが書き込みキャッシュに対応しているかどうかを確認してください。

2. を使用して、アグリゲートにSSDを追加します `storage aggregate add` コマンドを実行します
  - SSDは、IDまたはを使用して指定できます `diskcount` および `disktype` パラメータ
  - HDDとSSDでチェックサム方式が異なる場合やチェックサムが混在したアグリゲートの場合は、を使用する必要があります `checksumstyle` アグリゲートに追加するディスクのチェックサム方式を指定するパラメータ。
  - を使用して、SSDキャッシュに別のRAIDタイプを指定できます `raidtype` パラメータ
  - キャッシュRAIDグループサイズを使用するRAIDタイプのデフォルトと異なるサイズにする場合は、を使用してこの時点で変更する必要があります `-cache-raid-group-size` パラメータ

**SSDストレージプールを使用してFlash Poolローカル階層（アグリゲート）を作成します**

**SSDストレージプールを使用するFlash Poolローカル階層（アグリゲート）の作成の概要**

SSDストレージプールを使用してFlash Poolローカル階層（アグリゲート）を作成するためのさまざまな手順を実行できます。

- 準備
  - "Flash Poolのローカル階層（アグリゲート）でSSDストレージプールを使用しているかどうかを確認します"
- \* SSDストレージプールの作成\*
  - "SSD ストレージプールを作成する"
  - "SSD ストレージプールに SSD を追加します"
- \* SSDストレージプールを使用したFlash Poolの作成\*
  - "SSDストレージプールの割り当て単位を使用してFlash Poolローカル階層（アグリゲート）を作成します"
  - "SSD ストレージプールへの SSD の追加がキャッシュサイズに及ぼす影響を決定する"

Flash Poolのローカル階層（アグリゲート）でSSDストレージプールを使用しているかどうかを確認します

Flash Pool（ローカル階層）アグリゲートを設定するには、SSDストレージプールから既存のHDDローカル階層に1つ以上の割り当て単位を追加します。

SSDストレージプールを使用してキャッシュを提供する場合と、単独のSSDを使用する場合とでは、Flash Poolのローカル階層を管理方法が異なります。

#### ステップ

1. RAID グループ別のアグリゲートのドライブを表示します。

```
storage aggregate show-status aggr_name
```

アグリゲートで1つ以上のSSDストレージプールを使用している場合は、の値 `Position` SSD RAIDグループの列にはと表示されます `Shared` および、RAIDグループ名の横にストレージプールの名前が表示されます。

SSDストレージプールを作成して、ローカル階層（アグリゲート）にキャッシュを追加します

ソリッドステートドライブ（SSD）を追加することで、既存のローカル階層（アグリゲート）をFlash Poolローカル階層（アグリゲート）に変換してキャッシュをプロビジョニングできます。

2~4つのFlash Poolローカル階層（アグリゲート）にSSDキャッシュを提供するためのソリッドステートドライブ（SSD）ストレージプールを作成できます。Flash Pool アグリゲートを使用すると、作業データセットにはフラッシュを導入して高性能なキャッシュを利用しながら、アクセス頻度が低いデータには低コストのHDDを使用することができます。

#### このタスクについて

- ストレージプールにディスクを作成または追加するときは、ディスクリストを指定する必要があります。

ストレージプールではサポートされません `diskcount` パラメータ

- ストレージプールで使用する SSD は同じサイズでなければなりません。

## System Manager の略

### System Managerを使用してSSDキャッシュを追加する（ONTAP 9.12.1以降）

ONTAP 9.12.1以降では、System Managerを使用してSSDキャッシュを追加できます。



ストレージプールのオプションは、AFF システムでは使用できません。

#### 手順

1. [\*Cluster]、[Disks]の順にクリックし、[\*Show/Hide \*]をクリックします。
2. タイプ\*を選択し、スペアSSDがクラスタに存在することを確認します。
3. [ストレージ]、[階層]の順にクリックし、[\*ストレージプールの追加]をクリックします。
4. ディスクタイプを選択します。
5. ディスクサイズを入力してください。
6. ストレージプールに追加するディスクの数を選択します。
7. 推定キャッシュサイズを確認します。

### System Manager を使用して SSD キャッシュを追加する（ONTAP 9.7 のみ）



ONTAP 9.12.1よりも前ONTAP のONTAP バージョンを使用している場合は、CLI手順 を使用します。

#### 手順

1. [( クラシックバージョンに戻る )] をクリックします。
2. ストレージ > アグリゲートとディスク > アグリゲート \* をクリックします。
3. ローカル階層（アグリゲート）を選択し、\* Actions > Add Cache \* をクリックします。
4. キャッシュソースとして、「ストレージプール」または「専用 SSD 」を選択します。
5. （新しいエクスペリエンスに切り替える） \* をクリックします。
6. Storage > Tiers \* をクリックして、新しいアグリゲートのサイズを確認します。

## CLI の使用

- SSDストレージプールの作成にはCLIを使用\*

#### 手順

1. 使用可能なスペア SSD の名前を指定します。

```
storage aggregate show-spare-disks -disk-type SSD
```

ストレージプールで使用される SSD は、HA ペアのどちらのノードでも所有できます。

2. ストレージプールを作成します。

```
storage pool create -storage-pool sp_name -disk-list disk1,disk2,...
```

3. \* オプション：\* 新しく作成したストレージ・プールを検証します。

```
storage pool show -storage-pool sp_name
```

## 結果

ストレージプールが提供するストレージがまだどの Flash Pool キャッシュにも割り当てられていなくても、ストレージプールに配置された SSD は、クラスタではスペアとして表示されなくなります。SSD を単独のドライブとして RAID グループに追加することはできません。ストレージをプロビジョニングできるのは、SSD が属しているストレージプールの割り当て単位を使用する場合に限られます。

**SSDストレージプールの割り当て単位を使用してFlash Poolローカル階層（アグリゲート）を作成します**

Flash Poolのローカル階層（アグリゲート）を設定するには、SSDストレージプールから既存のHDDローカル階層に1つ以上の割り当て単位を追加します。

ONTAP 9.12.1以降では、再設計したSystem Managerを使用して、ストレージプール割り当て単位を使用するFlash Poolローカル階層を作成できます。

## 必要なもの

- Flash Poolローカル階層に変換する、HDDで構成された有効なローカル階層を特定しておく必要があります。
- ローカル階層に関連付けられたボリュームが書き込みキャッシュに対応しているかどうかを確認し、対応していない場合は必要な手順を実行して問題を解決しておく必要があります。
- このFlash Poolローカル階層にSSDキャッシュを提供するためのSSDストレージプールを作成しておく必要があります。

使用するストレージプールのすべての割り当て単位が、Flash Poolのローカル階層を所有するノードに所有されている必要があります。

- ローカル階層に追加するキャッシュの容量を決めておく必要があります。

ローカル階層にキャッシュを追加するには、割り当て単位を使用します。ストレージプールに余裕がある場合は、ストレージプールに SSD を追加することで割り当て単位のサイズをあとから拡張できます。

- SSD キャッシュで使用する RAID タイプを決めておく必要があります。

SSDストレージプールからローカル階層にキャッシュを追加したあとで、キャッシュRAIDグループのRAIDタイプを変更することはできません。

- システムの最大キャッシュサイズを決めて、ローカル階層にSSDキャッシュを追加してもそれを超える原因は作成されないことを確認しておく必要があります。

合計キャッシュサイズに追加されるキャッシュの量は、を使用して確認できます storage pool show コマンドを実行します

- Flash Poolローカル階層の構成要件を確認しておく必要があります。

## このタスクについて



キャッシュのRAIDタイプをHDD RAIDグループと異なるタイプにする場合は、SSDの容量を追加するときにキャッシュのRAIDタイプを指定する必要があります。ローカル階層にSSDの容量を追加したあとで、キャッシュのRAIDタイプを変更することはできません。

ローカル階層にSSDキャッシュを追加してFlash Poolローカル階層を作成したあとで、SSDキャッシュを削除してローカル階層を元の構成に戻すことはできません。

## System Manager の略

ONTAP 9.12.1以降では、System Managerを使用してSSDストレージプールにSSDを追加できます。

### 手順

1. [ストレージ>階層]をクリックし、既存のローカルHDDストレージ階層を選択します。
2. をクリックします  をクリックし、\* Add Flash Pool Cache \*を選択します。
3. [ストレージプールを使用する] を選択します。
4. ストレージプールを選択します。
5. キャッシュサイズとRAID構成を選択してください。
6. [保存 (Save) ] をクリックします。
7. ストレージ階層を再度探して、をクリックします .
8. 「\* More Details」を選択し、Flash Poolの表示が「\* Enabled」になっていることを確認します。

## CLI の使用

### 手順

1. アグリゲートを Flash Pool アグリゲートとして使用できるように指定します。

```
storage aggregate modify -aggregate aggr_name -hybrid-enabled true
```

この手順が正常に完了しない場合は、ターゲットアグリゲートが書き込みキャッシュに対応しているかどうかを確認してください。

2. 使用可能な SSD ストレージプールの割り当て単位を表示します。

```
storage pool show-available-capacity
```

3. アグリゲートに SSD の容量を追加します。

```
storage aggregate add aggr_name -storage-pool sp_name -allocation-units  
number_of_units
```

キャッシュのRAIDタイプをHDD RAIDグループと異なるタイプにする場合は、このコマンドを入力するときに、を使用してRAIDタイプを変更する必要があります `raidtype` パラメータ

新しい RAID グループを指定する必要はありません。ONTAP では、HDD RAID グループとは別の RAID グループに SSD キャッシュが自動的に配置されます。

キャッシュの RAID グループサイズを設定することはできません。このサイズは、ストレージプール内の SSD の数によって決まります。

キャッシュがアグリゲートに追加され、アグリゲートが Flash Pool アグリゲートになります。アグリゲートに追加された各割り当て単位は独自の RAID グループになります。

4. SSD キャッシュが存在すること、およびそのサイズを確認します。

```
storage aggregate show aggregate_name
```

キャッシュのサイズは、に表示されます Total Hybrid Cache Size。

## 関連情報

"[ネットアップテクニカルレポート 4070](#) : 『Flash Pool Design and Implementation Guide』"

**SSD** ストレージプールへの **SSD** の追加がキャッシュサイズに及ぼす影響を決定する

ストレージプールにSSDを追加するとプラットフォームモデルのキャッシュ制限を超えてしまう場合、ONTAP では新しく追加した容量をどのFlash Poolローカル階層（アグリゲート）にも割り当てません。その結果、新しく追加した容量の一部またはすべてを使用できなくなる可能性があります。

## このタスクについて

割り当て単位がFlash Poolのローカル階層（アグリゲート）にすでに割り当てられているSSDストレージプールにSSDを追加すると、追加した各ローカル階層のキャッシュサイズとシステム全体のキャッシュサイズが増加します。ストレージプールのどの割り当て単位も割り当てられていない場合は、そのストレージプールにSSDを追加しても、1つ以上の割り当て単位がキャッシュに割り当てられるまでSSDのキャッシュサイズには影響しません。

## 手順

1. ストレージプールに追加するSSDの使用可能なサイズを確認します。

```
storage disk show disk_name -fields usable-size
```

2. ストレージプールの未割り当ての割り当て単位の数を確認します。

```
storage pool show-available-capacity sp_name
```

ストレージプール内の未割り当てのすべての割り当て単位が表示されます。

3. 次の式を使用して、追加するキャッシュの容量を計算します。

$(4 - \text{未割り当ての割り当て単位の数}) \times 25\% \times \text{使用可能なサイズ} \times \text{SSDの数}$

**SSD** ストレージプールに **SSD** を追加します

SSD ストレージプールにソリッドステートドライブ（SSD）を追加する場合は、ストレージプールの物理サイズと使用可能なサイズ、および割り当て単位のサイズを拡張します。割り当て単位のサイズが大きいほど、ローカル階層（アグリゲート）にすでに割り当てられている割り当て単位にも影響します。

## 必要なもの

この処理で HA ペアのキャッシュ制限を超えないように原因を設定しておく必要があります。ONTAP では、SSD ストレージプールへの SSD の追加時にキャッシュ制限を超えてもかまいませんが、その場合、新しく追加したストレージ容量が使用できなくなる可能性があります。

## このタスクについて

既存の SSD ストレージプールに SSD を追加する場合は、ストレージプール内の既存の SSD を所有するノー


ドと同じ HA ペアのどちらかのノードが所有する SSD を追加する必要があります。HA ペアのどちらのノードが所有する SSD でもかまいません。

ストレージプールに追加する SSD は、そのストレージプールで現在使用されているディスクと同じサイズである必要があります。

#### System Manager の略

ONTAP 9.12.1以降では、System Managerを使用してSSDストレージプールにSSDを追加できます。

##### 手順

1. [ストレージ>階層]をクリックし、[ストレージプール]セクションを探します。
2. ストレージプールを探し、をクリックします  をクリックし、\*ディスクの追加\*を選択します。
3. ディスクタイプを選択し、ディスク数を選択します。
4. 推定キャッシュサイズを確認します。

#### CLI の使用

##### 手順

1. \* オプション：ストレージプールの現在の割り当て単位のサイズと使用可能なストレージを表示します。

```
storage pool show -instance sp_name
```

2. 使用可能な SSD を探します。

```
storage disk show -container-type spare -type SSD
```

3. ストレージプールに SSD を追加します。

```
storage pool add -storage-pool sp_name -disk-list disk1,disk2...
```

どの Flash Pool アグリゲートのサイズがこの処理によってどのくらい拡張されるかが表示され、処理を実行するかどうかの確認を求められます。

#### SSD ストレージプールの管理用コマンド

ONTAP はを提供します storage pool SSDストレージプールの管理用コマンド。

状況	使用するコマンド
ストレージプールがアグリゲートに提供しているストレージの容量を表示する	<code>storage pool show-aggregate</code>
両方の RAID タイプの全体的なキャッシュ容量（割り当て単位のデータサイズ）に追加するキャッシュの容量を表示する	<code>storage pool show -instance</code>



ストレージプール内のディスクを表示します	<code>storage pool show-disks</code>
ストレージプールの未割り当ての割り当て単位を表示します	<code>storage pool show-available-capacity</code>
ストレージプールの 1 つ以上の割り当て単位の所有権をある HA パートナーからもう一方の HA パートナーに変更します	<code>storage pool reassign</code>

関連情報

["ONTAP 9 コマンド"](#)

## FabricPool 階層の管理

### FabricPool 階層の管理の概要

FabricPool を使用すると、アクセス頻度に応じてデータを自動的に階層化できます。

FabricPool は、オールフラッシュ（オール SSD）アグリゲートを高パフォーマンス階層として、オブジェクトストアをクラウド階層として使用するハイブリッドストレージ解決策です。FabricPool を使用すると、パフォーマンス、効率、保護を犠牲にすることなくストレージコストを削減できます。

クラウド階層は、NetApp StorageGRID または ONTAP S3（ONTAP 9.8 以降）に配置することも、次のいずれかのサービスプロバイダに配置することもできます。

- Alibaba クラウド
- Amazon S3
- Amazon Commercial クラウドサービスの略
- Google Cloud
- IBM クラウド
- Microsoft Azure Blob Storage



ONTAP 9.7以降では、S3\_compatibleオブジェクトストアプロバイダを選択することで、汎用のS3 APIをサポートする追加のオブジェクトストアプロバイダを使用できます。

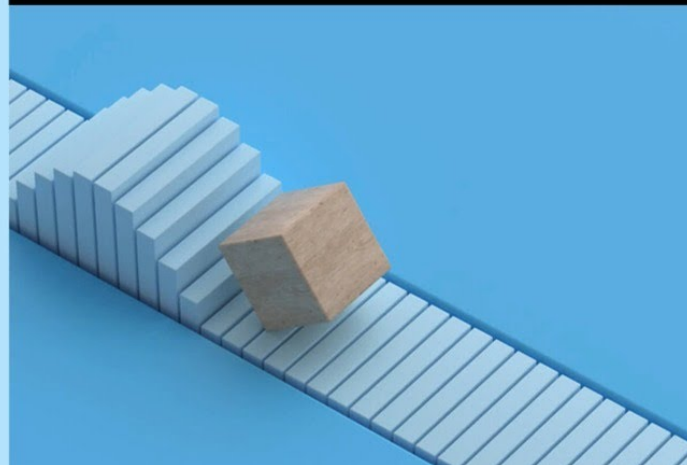
データを階層化してコストを削減ユースケースビデオ

# ONTAP FabricPool

Tier Data and Lower Costs

## Use Case

© 2020 NetApp, Inc. All rights reserved.



### 関連情報

も参照してください ["NetApp Cloud Tiering"](#) ドキュメント

### FabricPool を使用したストレージ階層のメリット

FabricPool を使用するようにアグリゲートを設定すると、ストレージ階層を使用することができます。ストレージシステムのパフォーマンスとコストのバランスを取り、スペース使用量を監視および最適化し、ストレージ階層間でポリシーベースのデータ移動を効率的に実行できます。

- データへのアクセス頻度に基づいて階層にデータを格納することで、ストレージパフォーマンスを最適化し、ストレージコストを削減できます。

- 頻繁にアクセスされる（「ホット」）データは `_performance` 階層に保存されます。

高パフォーマンス階層では、ストレージシステムのオールフラッシュ（オール SSD）アグリゲートなどの高性能なプライマリストレージを使用します。

- 頻繁にアクセスされない（コールド）データは、`cloud tier`（別名 `capacity tier`）に保存されます。

クラウド階層では、高いパフォーマンスを必要としない低コストのオブジェクトストアが使用されます。

- データを格納する階層を柔軟に指定できます。

サポートされるいずれかの階層化ポリシーオプションをボリュームレベルで指定することができます。これらのオプションを使用すると、データがホットまたはコールドになったときに階層間でデータを効率的に移動できます。

## "FabricPool 階層化ポリシーのタイプ"

- サポートされるいずれかのオブジェクトストアを選択して FabricPool のクラウド階層として使用できます。
- FabricPool 対応アグリゲートのスペース使用量を監視できます。
- Inactive Data Reporting でボリューム内のアクセス頻度の低いデータの量を確認できます。
- ストレージシステムのオンプレミスに必要な容量を削減できます。

クラウドベースのオブジェクトストアをクラウド階層として使用すると、物理スペースが削減されます。

## FabricPool を使用する際の考慮事項と要件

ここでは、FabricPool の使用に関するいくつかの考慮事項と要件を示します。

### 一般的な考慮事項と要件

- FabricPool を使用するには、ONTAP 9.2 以降が実行されている必要があります。
- 次の FabricPool 機能を使用するには、ONTAP 9.4 以降のリリースが必要です。
  - auto "階層化ポリシー"
  - 階層化の最小クーリング期間の指定
  - Inactive Data Reporting (IDR)
  - FabricPool のクラウド階層としての Microsoft Azure Blob Storage の使用
  - ONTAP Select で FabricPool を使用する
- 次の FabricPool 機能を使用するには、ONTAP 9.5 以降のリリースが実行されている必要があります。
  - 階層化の使用率しきい値を指定してい
  - FabricPool のクラウド階層として IBM Cloud Object Storage を使用している
  - クラウド階層の NetApp Volume Encryption (NVE) (デフォルトで有効)
- FabricPoolの次の機能を使用するには、ONTAP 9.6以降のリリースが必要です。
  - all 階層化ポリシー
  - HDD アグリゲートでアクセス頻度の低いデータのレポートを手動で有効にした
  - ONTAP 9.6 にアップグレードし、アグリゲートを作成すると、SSD アグリゲートに対して Inactive Data Reporting が自動的に有効になります。ただし、CPU が 4 個未満、RAM が 6GB 未満、または WAFL バッファキャッシュサイズが 3GB 未満のローエンドシステムでは例外です。

ONTAP でシステムの負荷が監視され、負荷が高い状態が 4 分間続くと、IDR は無効になり自動的に有効になりません。IDR を手動で再度有効にすることはできますが、手動で有効にした IDR は自動的に無効になりません。

  - FabricPool のクラウド階層としての Alibaba Cloud Object Storage の使用
  - FabricPool のクラウド階層として Google Cloud Platform を使用する
  - クラウド階層のデータコピーを使用せずにボリュームを移動する

- FabricPoolの次の機能を使用するには、ONTAP 9.7以降のリリースが必要です。
  - 非透過型 HTTP および HTTPS プロキシ：ホワイトリストに登録されたアクセスポイントにのみアクセスを提供し、監査およびレポート機能を提供します。
  - FabricPool ミラーリング：コールドデータを 2 つのオブジェクトストアに同時に階層化します
  - MetroCluster ミラーは FabricPool 構成にあります
  - FabricPool に接続されたアグリゲートでは、NDMP ダンプおよびリストアがデフォルトで有効になっています。



バックアップアプリケーションでNDMP以外のプロトコル（NFSやSMBなど）を使用すると、高パフォーマンス階層にバックアップされているすべてのデータがホットになり、そのデータのクラウド階層への階層化に影響する可能性があります。NDMP 以外の読み取りでは、クラウド階層からパフォーマンス階層への原因データの移行が可能です。

#### "FabricPool での NDMP バックアップおよびリストアのサポート"

- 次の FabricPool 機能を使用するには、ONTAP 9.8 以降が実行されている必要があります。
  - クラウドへの移行制御を有効にして、デフォルトの階層化ポリシーを無効にすることができます
  - データを高パフォーマンス階層に昇格します
  - FabricPool with SnapLock Enterprise.FabricPool with SnapLock Enterpriseには、Feature Product Variance Request (FPVR) が必要です。FPVRを作成するには、営業チームにお問い合わせください。
  - 最小冷却期間は 183 日です
  - ユーザが作成したカスタムタグを使用したオブジェクトタグ付け
  - HDD プラットフォームおよびアグリゲート上の FabricPool

HDD FabricPool は、SAS、FSAS、BSAS、および MSATA の各ディスクに対して、6 つ以上の CPU コアを搭載したシステムでのみサポートされます。これには、次のモデルが含まれます。

- FAS9000
- FAS8700
- FAS8300
- FAS8200
- FAS8080
- FAS8060
- FAS8040
- FAS2750
- FAS2720
- FAS2650
- FAS2620

チェックしてください "[Hardware Universe](#)" サポートされている最新のモデルについては、を参照

- FabricPool は、次の点を除いて、ONTAP 9.2 を実行可能なすべてのプラットフォームでサポートされます。
  - FAS8020
  - FAS2554
  - FAS2552
  - FAS2520
- FabricPool でサポートされるアグリゲートタイプは次のとおりです。
  - AFF システムでは、FabricPool にオールフラッシュ（オール SSD）アグリゲートのみを使用できます。
  - FAS システムでは、FabricPool にオールフラッシュ（オール SSD）アグリゲートまたは HDD アグリゲートのいずれかを使用できます。  
[+]  
SSDとHDDの両方を含むFlash Poolアグリゲートは使用できません。
  - Cloud Volumes ONTAP および ONTAP Select では、FabricPool に SSD アグリゲートまたは HDD アグリゲートのいずれかを使用できます。

ただし、SSD アグリゲートを使用することを推奨します。

- FabricPool では、次のオブジェクトストアをクラウド階層として使用できます。
  - NetApp StorageGRID 10.3 以降
  - NetApp ONTAP S3 （ONTAP 9.8 以降）
  - Alibaba Cloud Object Storage の略
  - Amazon Web Services Simple Storage Service （AWS S3）
  - Google クラウドストレージ
  - IBM クラウドオブジェクトストレージ
  - クラウドの Microsoft Azure Blob Storage
- 使用するオブジェクトストア “bucket”（コンテナ）はすでに設定されている必要がありますまた ' 少なくとも 10 GB のストレージスペースが必要であり ' 名前を変更することはできません
- FabricPool を使用する HA ペアがオブジェクトストアと通信するには、クラスタ間 LIF が必要です。
- 接続後にローカル階層からクラウド階層の接続を解除することはできませんが、"[FabricPoolミラー](#)" をクリックして、別のクラウド階層にローカル階層を接続します。
- スループットの下限（最小QoS）を使用する場合は、ボリュームの階層化ポリシーをに設定する必要があります none アグリゲートをFabricPool に接続する前に、

それ以外の階層化ポリシーに設定されていると、アグリゲートを FabricPool に接続できません。FabricPoolが有効な場合、QoSポリシーではスループットの下限は適用されません。

- 特定のシナリオで FabricPool を使用する場合は、ベストプラクティスのガイドラインに従う必要があります。

"[ネットアップテクニカルレポート 4598](#) : 『FabricPool Best Practices in ONTAP 9』"

## Cloud Volumes ONTAP を使用する際のその他の考慮事項

FabricPool では、使用するオブジェクトストアプロバイダに関係なく、Cloud Volumes ONTAP ライセンスは必要ありません。

## SAN プロトコルがアクセスするデータの階層化に関するその他の考慮事項

SAN プロトコルがアクセスするデータを階層化する場合は、接続に関する考慮事項があるため、StorageGRID などのプライベートクラウドを使用することを推奨します。

### • 重要 \* :

Windowsホストを使用するSAN環境でFabricPoolを使用している場合、データをクラウドに階層化する際にオブジェクトストレージを長時間使用できなくなると、Windowsホスト上のNetApp LUN上のファイルにアクセスできなくなるか、表示されなくなることがあります。サポート技術情報の記事を参照してください  
["FabricPool S3オブジェクトストアを使用できないときに、Windows SANホストでファイルシステムの破損が報告されました"](#)。

## FabricPool でサポートされていない機能

- WORM とオブジェクトのバージョン管理が有効なオブジェクトストア
- オブジェクトストアバケットに適用される情報ライフサイクル管理（ILM）ポリシー

FabricPoolは、クラウド階層のデータを障害から保護するために、データレプリケーションとイレイジャーコーディングに関してのみStorageGRIDの情報ライフサイクル管理ポリシーをサポートしています。ただし、FabricPoolは、ユーザメタデータやタグに基づくフィルタリングなどの高度なILMルールをサポートしていません。通常、ILM には移動と削除に関するさまざまなポリシーが含まれています。これらのポリシーは、FabricPool のクラウド階層内のデータに影響を与える可能性があります。オブジェクトストアで設定されている ILM ポリシーと FabricPool を同時に使用すると、データが失われる可能性があります。

- ONTAP CLI コマンドまたは 7-Mode Transition Tool を使用した 7-Mode のデータ移行
- FlexArray 仮想化
- SyncMirror 構成を除く RAID MetroCluster
- ONTAP 9.7 以前のリリースを使用している場合、SnapLock ボリュームが必要です
- FabricPool 対応アグリゲート用の SMTape を使用したテープバックアップ
- 自動負荷分散機能
- 以外のスペースギャランティを使用しているボリューム none

ルートSVMボリュームとCIFS監査ステージングボリュームを除き、FabricPool では、以外のスペースギャランティを使用するボリュームを含むアグリゲートにクラウド階層を接続することはサポートされていません none。たとえば、スペースギャランティがに設定されたボリュームなどです `volume (-space -guarantee volume)` はサポートされていません。

- クラスタ ["DP\\_Optimizedライセンス"](#)
- Flash Pool アグリゲート



## FabricPool 階層化ポリシーについて

FabricPool 階層化ポリシーを使用すると、データがホットまたはコールドになったときに階層間でデータを効率的に移動できます。階層化ポリシーの概要を理解することで、ストレージ管理のニーズに応じた適切なポリシーを選択できます。

### FabricPool 階層化ポリシーのタイプ

FabricPool 階層化ポリシーは、FabricPool 内のボリュームのユーザデータブロックをクラウド階層に移動するタイミングとそのタイミングを、ホット（アクティブ）のボリューム「temperature」またはコールド（非アクティブ）に基づいて決定します。ボリューム「温度」は、頻繁にアクセスされると増加し、アクセスされない場合は減少します。一部の階層化ポリシーには、階層化の最小クーリング期間が関連付けられています。最小クーリング期間は、データが「コールド」とみなされてクラウド階層に移動されるために、FabricPool のボリューム内のユーザデータが非アクティブのままになる時間を設定します。

ブロックがコールドとして識別されると、階層化の対象としてマークされます。毎日のバックグラウンド階層化スキャンでコールドブロックが検索されます。同じボリュームから十分な4KBブロックが収集されると、それらは4MBオブジェクトに連結され、ボリューム階層化ポリシーに基づいてクラウド階層に移動されます。



シヨウシタホリユウムナイノテエタ all 階層化ポリシーはすぐにコールドとしてマークされ、できるだけ早くクラウド階層への階層化を開始します。毎日の階層化スキャンの実行を待つ必要はありません。

を使用できます `volume object-store tiering show` コマンドを使用してFabricPoolボリュームの階層化ステータスを表示します。詳細については、[を参照してください "コマンドリファレンス"](#)。

FabricPool 階層化ポリシーはボリュームレベルで指定し、次の 4 つのオプションがあります。

- `snapshot-only` 階層化ポリシー（デフォルト）は、アクティブなファイルシステムに関連付けられていないボリュームSnapshotコピーのユーザデータブロックをクラウド階層に移動します。

階層化の最小クーリング期間は 2 日です。階層化の最小クーリング期間のデフォルト設定は、で変更できます `-tiering-minimum-cooling-days` パラメータを指定します `volume create` および `volume modify` コマンド有効な値は、ONTAP 9.8 以降で 2 ~ 183 日です。9.8 より前のバージョンの ONTAP を使用している場合、有効な値は 2~63 日です。

- `auto` 階層化ポリシーはONTAP 9.4以降のリリースでのみサポートされ、Snapshotコピーとアクティブなファイルシステムの両方のコールドユーザデータブロックをクラウド階層に移動します。

アクティブなファイルシステムと Snapshot コピーのどちらについても、階層化の最小クーリング期間のデフォルトは 31 日、ボリューム全体の環境を設定します。

階層化の最小クーリング期間のデフォルト設定は、で変更できます `-tiering-minimum-cooling-days` パラメータを指定します `volume create` および `volume modify` コマンド有効な値は 2 ~ 183 日です。

- `all` 階層化ポリシー（ONTAP 9.6以降でのみサポート）は、アクティブなファイルシステムとSnapshotコピーの両方のすべてのユーザデータブロックをクラウド階層に移動します。の代わりになります `backup` 階層化ポリシー：

- `all` クライアントトラフィックが正常な読み取り/書き込みボリュームでは、ボリューム階層化ポリシーを使用しないでください。

階層化スキュンの実行と同時にデータがクラウド階層に移動するため、階層化の最小クーリング期間は適用されません。この設定は変更できません。

- `none` 階層化ポリシーはボリュームのデータを高パフォーマンス階層に保持し、コールドデータをクラウド階層に移動しません。

階層化ポリシーをに設定しています `none` 新しい階層化を防止以前にクラウド階層に移動されたボリュームデータは、ホットになるまでクラウド階層に残り、自動的にローカル階層に戻ります。

データがクラウド階層に移動されることはないため、階層化の最小クーリング期間は適用されません。この設定は変更できません。

階層化ポリシーがに設定されているボリューム内のコールドブロック `none` が読み取られ、ホットになり、ローカル階層に書き込まれます。

。 `volume show` コマンド出力には、ボリュームの階層化ポリシーが表示されます。FabricPool で使用されたことがないボリュームにはが表示されます `none` 出力に階層化ポリシーが表示されます。

### FabricPool でボリュームの階層化ポリシーを変更した場合の動作

ボリュームの階層化ポリシーを変更するには、を実行します `volume modify` 操作。階層化ポリシーを変更することが、データがコールドと認識されてクラウド階層に移動されるまでの時間にどのように影響するかを理解しておく必要があります。

- 階層化ポリシーをから変更しています `snapshot-only` または `none` 終了： `auto` アクティブなファイルシステム内のすでにコールドなユーザデータブロックをONTAP からクラウド階層に送信します。これは、それらのユーザデータブロックが以前はクラウド階層に送信されなかった場合でも同様です。
- 階層化ポリシーをに変更しています `all` 別のポリシーを使用すると、ONTAPは、アクティブファイルシステムとSnapshotコピー内のすべてのユーザブロックをできるだけ早くクラウドに移動します。ONTAP 9.8より前のバージョンでは、次の階層化スキュンが実行されるまでブロックが待機する必要がありました。

移動されたブロックを高パフォーマンス階層に戻すことはできません。

- 階層化ポリシーをから変更しています `auto` 終了： `snapshot-only` または `none` は、すでにクラウド階層に移動されて高パフォーマンス階層に戻すために移動されたアクティブなファイルシステムブロックを原因 にしません。

データを高パフォーマンス階層に戻すには、ボリュームの読み取りが必要です。

- ボリュームの階層化ポリシーを変更すると、階層化の最小クーリング期間は常にそのポリシーのデフォルト値にリセットされます。

### ボリュームを移動した場合の階層化ポリシーへの影響

- ボリュームを FabricPool 対応アグリゲートに移動したり FabricPool 対応アグリゲートから移動しても、別の階層化ポリシーを明示的に指定しないかぎり、ボリュームの階層化ポリシーは元のままです。

ただし、階層化ポリシーが適用されるのは、ボリュームが FabricPool 対応アグリゲート内にある場合のみです。

- の既存の値 `-tiering-minimum-cooling-days` ボリュームのパラメータは、デスティネーションに別



の階層化ポリシーを指定しないかぎり、ボリュームと一緒に移動します。

別の階層化ポリシーを指定した場合は、そのポリシーのデフォルトの階層化の最小クーリング期間が使用されます。デスティネーションが FabricPool かどうかは関係ありません。

- アグリゲート間でボリュームを移動し、同時に階層化ポリシーも変更できます。
- あなたは特別な注意を払う必要がありますとき a volume move 操作には、が含まれます auto 階層化ポリシー：

次の表に、ソースとデスティネーションの両方がFabricPool対応アグリゲートである場合の処理結果を示します volume move に関連するポリシーの変更を含む処理 auto：

ボリュームの階層化ポリシー	移動時に設定する階層化ポリシー	ボリューム移動後の結果
all	auto	すべてのデータが高パフォーマンス階層に移動されます。
snapshot-only、 none または `auto	auto	データブロックは、以前ソースと同じデスティネーションの階層に移動されます。
auto または all	snapshot-only	すべてのデータが高パフォーマンス階層に移動されます。
auto	all	すべてのユーザーデータがクラウド階層に移動されます。
snapshot-only,auto または all	none	すべてのデータが高パフォーマンス階層に保持されます。

#### ボリュームをクローニングした場合の階層化ポリシーへの影響

- ONTAP 9.8 以降では、クローンボリュームは常に階層化ポリシーとクラウド読み出しポリシーの両方を親ボリュームから継承します。

ONTAP 9.8より前のリリースでは、親にがある場合を除き、クローンは親から階層化ポリシーを継承します all 階層化ポリシー：

- 親ボリュームにがある場合 never クラウド読み出しポリシーを使用している場合、クローンボリュームにはどちらかのが必要です never クラウド読み出しポリシーまたは all 階層化ポリシー、および対応するクラウド読み出しポリシー default。
- 親ボリュームのクラウド読み出しポリシーをに変更することはできません never すべてのクローンボリュームにクラウド読み出しポリシーが設定されていない場合 never。

ボリュームをクローニングするときは、次のベストプラクティスに注意してください。

- 。 -tiering-policy オプションおよび tiering-minimum-cooling-days クローンのオプションで制御されるのは、クローンに固有のブロックの階層化のみです。そのため、親 FlexVol では、同じ量のデータを移動するか、クローンよりも少ないデータを移動する階層化設定を使用することを推奨します

- 親 FlexVol でのクラウド読み出しポリシーでは、同じ量のデータを移動するか、いずれかのクローンの読み出しポリシーよりも多くのデータを移動する必要があります

## 階層化ポリシーがクラウド移行とどのように連携するか

FabricPool クラウドデータの読み出しは、読み取りパターンに基づいてクラウド階層からパフォーマンス階層へのデータの読み出しを決定する階層化ポリシーで制御されます。読み取りパターンは、シーケンシャルまたはランダムいずれかです。

次の表に、各ポリシーについて、階層化ポリシーとクラウドデータの読み出しルールを示します。

階層化ポリシー	取得動作
なし	シーケンシャルリードとランダムリード
Snapshot のみ	シーケンシャルリードとランダムリード
自動	ランダムリード
すべて	データの取得は行われません

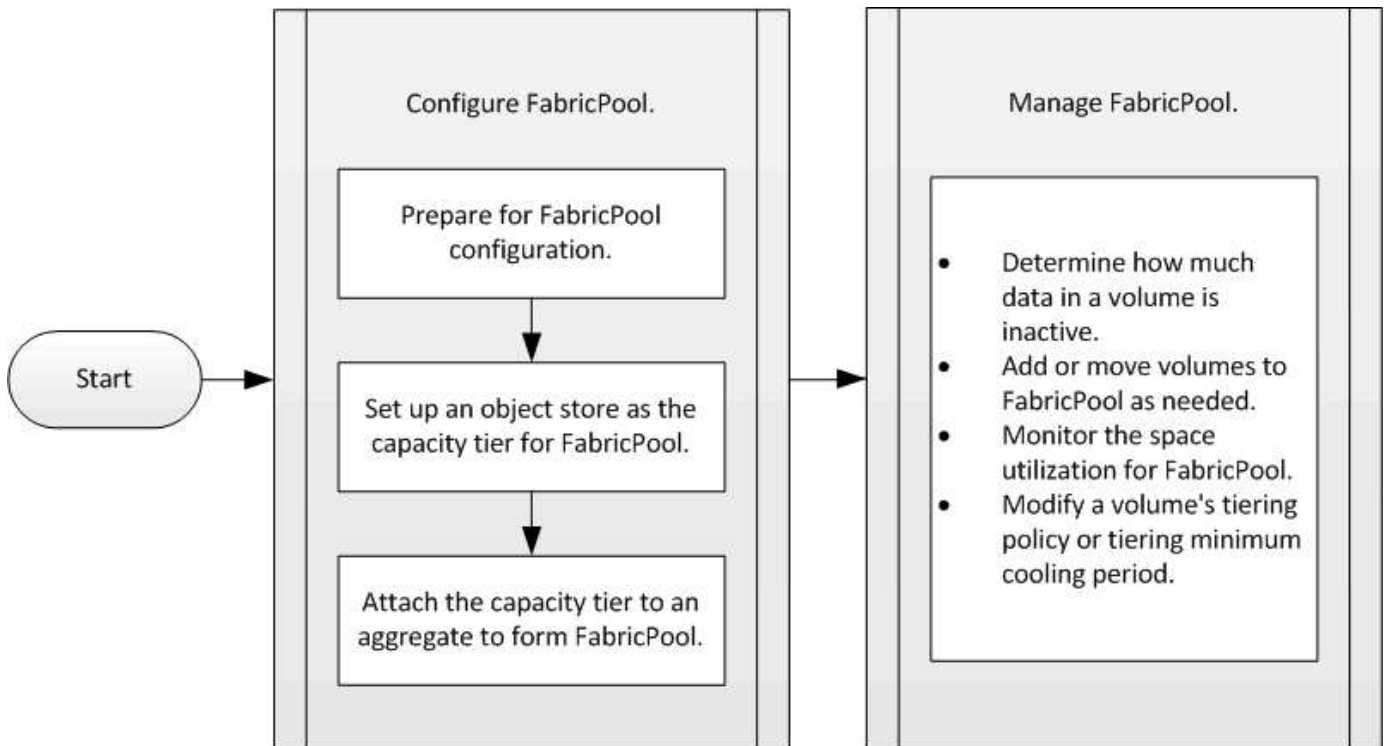
ONTAP 9.8以降では、クラウド移行の管理が可能になりました `cloud-retrieval-policy` オプションは、階層化ポリシーで制御されるデフォルトのクラウド移行または読み出し動作を上書きします。

次の表に、サポートされているクラウドの読み出しポリシーとその読み出し動作を示します。

クラウド取得ポリシー	取得動作
デフォルト	どのデータを移行するかは階層化ポリシーによって決定されるため、「デフォルト」のクラウドデータの読み出しに変更はありません," `cloud-retrieval-policy。ホストされているアグリゲートタイプに関係なく、このポリシーはすべてのボリュームのデフォルト値です。
オンリード	クライアントからの読み取りは、すべてクラウド階層からパフォーマンス階層に送られます。
なし	クラウド階層からパフォーマンス階層にクライアントベースのデータが移動されることはありません
ステートアップ	<ul style="list-style-type: none"> <li>• 階層化ポリシー「none」の場合、すべてのクラウドデータはクラウド階層からパフォーマンス階層にプルされます</li> <li>• 階層化ポリシー「スナップショットのみ」の場合、「AFS データ」はプルされます。</li> </ul>

## FabricPool 管理ワークフロー

FabricPool のワークフロー図を使用して、設定タスクと管理タスクを計画できます。



## FabricPool を設定します

### FabricPool 構成を準備

#### FabricPool 構成の概要を準備

FabricPool を設定すると、アクセス頻度に基づいてデータを格納するストレージ階層（ローカルの高パフォーマンス階層またはクラウド階層）を管理する際に役立ちます。

FabricPool 構成に必要な準備は、クラウド階層として使用するオブジェクトストアによって異なります。

クラウドへの接続を追加します

ONTAP 9.9.9.0 以降では、System Manager を使用してクラウドへの接続を追加できます。

まず、NetApp Cloud Insights を使用してコレクタを設定します。設定プロセスでは、Cloud Insights で生成されたペアリングコードをコピーし、System Manager を使用してクラスタにログインします。そこで、そのペアリングコードを使用してクラウド接続を追加します。残りのプロセスは Cloud Insights で実行します。



Cloud Volumes ONTAP から Cloud Insights サービスへの接続を追加するときにプロキシサーバを使用するオプションを選択する場合は、URLを確認してください <https://example.com> プロキシサーバからアクセスできます。には、「HTTPプロキシ設定が無効です」というメッセージが表示されます <https://example.com> にアクセスできません。

## 手順

1. Cloud Insights で、コレクタを設定するプロセス中に、生成されたペアリングコードをコピーします。
2. ONTAP 9.9.0 以降の System Manager を使用して、クラスタにログオンします。
3. [ クラスタ ]>[ 設定 \* ] を選択します。
4. [ クラウド接続 ] セクションで、[ \* 追加 ] を選択して接続を追加します。
5. 接続の名前を入力し、表示されたスペースにペアリングコードを貼り付けます。
6. 「 \* 追加 」を選択します。
7. Cloud Insights に戻り、コレクタの設定を完了します。

追加情報 About Cloud Insights については、を参照してください ["Cloud Insights のドキュメント"](#)。

**FabricPool** ライセンスをインストールする。

過去に使用したFabricPool ライセンスは変更されており、BlueXPでサポートされていない構成にのみ保持されています。2021年8月21日より、Cloud Tieringサービスを使用したBlueXPでサポートされる階層化構成に対してCloud Tiering BYOLライセンスが導入されました。

["新しい Cloud Tiering BYOL ライセンスの詳細については、こちらをご覧ください"](#)。

BlueXPでサポートされる構成ではBlueXPのDigital Walletページを使用してONTAP クラスタの階層化のライセンスを取得する必要がありますそのためには、使用する特定のオブジェクトストレージプロバイダに対して、BlueXPアカウントを設定し、階層化を設定する必要があります。BlueXPでは現在、Amazon S3、Azure Blob Storage、Google Cloud Storage、S3互換オブジェクトストレージ、StorageGRID などのオブジェクトストレージへの階層化をサポートしています。

["クラウド階層化サービスの詳細をご確認ください"](#)。

BlueXPでサポートされていない構成のいずれかがある場合は、System Managerを使用してFabricPool ライセンスをダウンロードして有効にすることができます。

- ダークサイトでの ONTAP のインストール
- IBM Cloud Object Storage または Alibaba Cloud Object Storage にデータを階層化する ONTAP クラスタ

FabricPool ライセンスはクラスタ規模のライセンスです。このライセンスには、クラスタ内の FabricPool に関連付けられているオブジェクトストレージに対して購入する使用量の制限が設定されています。クラスタ全体での使用量がこの容量を超えないようにする必要があります。ライセンスの使用量の制限を増やす必要がある場合は、営業担当者にお問い合わせください。

FabricPool ライセンスには、恒久ライセンスとタームベースライセンス、1 年または 3 年ライセンスがあります。

BlueXPでサポートされていない既存のクラスタ構成では、10TBの空き容量を含むタームベースFabricPool ライセンスを初めてFabricPool から購入できます。無期限のライセンスには空き容量は含まれていません。クラウド階層に NetApp StorageGRID または ONTAP S3 を使用する場合は、ライセンスは必要ありません。使用しているプロバイダに関係なく、Cloud Volumes ONTAP には FabricPool ライセンスは必要ありません。

このタスクは、System Manager を使用してクラスタにライセンスファイルをアップロードすることでのみサポートされます。

#### 手順

1. から FabricPool ライセンスのネットアップライセンスファイル（NLF）をダウンロードします ["NetApp Support Site"](#)。
2. System Manager を使用して次の操作を実行し、FabricPool ライセンスをクラスタにアップロードします。
  - a. [\* Cluster]>[設定\*]パネルの[Licenses]カードで、をクリックします →。
  - b. [License] ページで、をクリックします + Add。
  - c. [\* ライセンスの追加 \*] ダイアログボックスで、[\* 参照] をクリックしてダウンロードした NLF を選択し、[\* 追加] をクリックしてファイルをクラスタにアップロードします。

#### 関連情報

["ONTAP FabricPool（FP）ライセンスの概要"](#)

["ネットアップソフトウェアライセンスの検索"](#)

["NetApp TechComm TV：FabricPool 関連ビデオ"](#)

StorageGRID を使用する場合は、CA 証明書をインストールします

StorageGRID の証明書のチェックを無効にする予定でないかぎり、ONTAP のオブジェクトストアとして StorageGRID が FabricPool で認証できるように、StorageGRID CA 証明書をクラスタにインストールする必要があります。

#### このタスクについて

ONTAP 9.4 以降のリリースでは、StorageGRID の証明書チェックを無効にすることができます。

#### 手順

1. StorageGRID 管理者に問い合わせして StorageGRID システムの CA 証明書を入手します。
2. を使用します `security certificate install` コマンドにを指定します `-type server-ca` StorageGRID CA証明書をクラスタにインストールするためのパラメータ。

入力する完全修飾ドメイン名（FQDN）と StorageGRID CA 証明書のカスタム共通名が一致している必要があります。

#### 期限切れの証明書を更新します

期限切れの証明書を更新する場合は、信頼された CA を使用して新しいサーバ証明書を生成することを推奨します。また、ダウンタイムを最小限に抑えるために、StorageGRID サーバと ONTAP クラスタの証明書が同時に更新されていることを確認する必要があります。

#### 関連情報

["StorageGRID リソース"](#)

ONTAP S3 を使用する場合は、**CA** 証明書をインストールします

ONTAP S3 の証明書のチェックを無効にする予定でないかぎり、ONTAP S3 CA 証明書をクラスタにインストールし、ONTAP が FabricPool S3 を ONTAP のオブジェクトストアとして認証できるようにする必要があります。

#### 手順

1. ONTAP S3 システムの CA 証明書を取得します。
2. 使用します `security certificate install` コマンドにを指定します `-type server-ca` ONTAP S3 CA証明書をクラスタにインストールするためのパラメータ。

入力する完全修飾ドメイン名（FQDN）と ONTAP S3 CA 証明書のカスタム共通名が一致している必要があります。

#### 期限切れの証明書を更新します

期限切れの証明書を更新する場合は、信頼された CA を使用して新しいサーバ証明書を生成することを推奨します。また、ダウンタイムを最小限に抑えるために、ONTAP S3 サーバと ONTAP クラスタの両方で証明書が同時に更新されていることを確認する必要があります。

#### 関連情報

["S3構成"](#)

**FabricPool** のクラウド階層として使用するオブジェクトストアをセットアップします

**FabricPool** の概要用にクラウド階層として使用するオブジェクトストアをセットアップする

FabricPool FabricPoolのセットアップで、クラウド階層として使用するオブジェクトストア（StorageGRID、ONTAP S3、Alibaba Cloud Object Storage、Amazon S3、Google Cloud Storage、IBM Cloud Object Storage、Microsoft Azure Blob Storage）の設定情報を指定します。

クラウド階層として **StorageGRID** をセットアップします

ONTAP 9.2 以降を実行している場合は、StorageGRID を FabricPool のクラウド階層としてセットアップできます。SAN プロトコルがアクセスするデータを階層化する場合は、接続に関する考慮事項があるため、StorageGRID などのプライベートクラウドを使用することを推奨します。

**FabricPool** で**StorageGRID** を使用する場合の考慮事項

- 証明書のチェックを明示的に無効にした場合を除き、StorageGRID の CA 証明書をインストールする必要があります。
- オブジェクトストアバケットで StorageGRID オブジェクトのバージョン管理を有効にすることはできません。
- FabricPool ライセンスは必要ありません。
- NetApp AFF システムからストレージが割り当てられた仮想マシンに StorageGRID ノードが導入されている場合は、ボリュームで FabricPool 階層化ポリシーが有効になっていないことを確認してください。

StorageGRID ノードで使用するボリュームで FabricPool による階層化を無効にすることで、トラブルシューティングとストレージの処理がシンプルになります。



StorageGRID を使用して StorageGRID に関連するデータを FabricPool 自体に階層化しないでください。StorageGRID データを StorageGRID に階層化すると、トラブルシューティングと運用がより複雑になります。

#### このタスクについて

ONTAP 9.8 以降では、StorageGRID に対してロードバランシングが有効になっています。サーバのホスト名が複数の IP アドレスに解決される場合、ONTAP は、返されるすべての IP アドレス（最大 16 個の IP アドレス）とのクライアント接続を確立します。接続が確立されると、IP アドレスはラウンドロビン方式でピックアップされます。

#### の手順

ONTAP System Manager または ONTAP CLI を使用して、FabricPool のクラウド階層として StorageGRID をセットアップできます。

## System Manager の略

1. [\*ストレージ]、[階層]、[クラウド階層の追加]の順にクリックし、オブジェクトストアプロバイダとして[ StorageGRID ]を選択します。
2. 必要な情報を入力します。
3. CloudMirror を作成する場合は、\* FabricPool ミラーとして追加 \* をクリックします。

FabricPool ミラーを使用すると、データストアをシームレスに置き換えることができ、災害発生時にデータを確実に使用できるようになります。

## CLI の使用

1. を使用して、StorageGRID の設定情報を指定します `storage aggregate object-store config create` コマンドにを指定します `-provider-type SGWS` パラメータ
  - 。 `storage aggregate object-store config create` 指定された情報でONTAP がStorageGRID にアクセスできない場合、コマンドは失敗します。
  - 。 を使用します `-access-key` パラメータを指定して、StorageGRID オブジェクトストアへの要求を認証するためのアクセスキーを指定します。
  - 。 を使用します `-secret-password` StorageGRID オブジェクトストアへの要求を認証するためのパスワード（シークレットアクセスキー）を指定するパラメータ。
  - 。 StorageGRID パスワードが変更された場合は、ONTAP に格納されている対応するパスワードをただちに更新する必要があります。

これにより、ONTAP は引き続き StorageGRID 内のデータにアクセスできます。

- 。 を設定します `-is-certificate-validation-enabled` パラメータの値 `false` StorageGRID の証明書チェックを無効にします。

```
cluster1::> storage aggregate object-store config create
-object-store-name mySGWS -provider-type SGWS -server mySGWSserver
-container-name mySGWScontainer -access-key mySGWSkey
-secret-password mySGWSpass
```

2. を使用して、StorageGRID の設定情報を表示して確認します `storage aggregate object-store config show` コマンドを実行します
  - 。 `storage aggregate object-store config modify` コマンドを使用すると、FabricPool のStorageGRID 設定情報を変更できます。

クラウド階層として **ONTAP S3** をセットアップします

ONTAP 9.8 以降を実行している場合は、ONTAP S3 を FabricPool のクラウド階層としてセットアップできます。

必要なもの

リモートクラスタの ONTAP S3 サーバ名とその LIF に関連付けられている IP アドレスが必要です。



ローカルクラスタにクラスタ間LIFがある。

"リモートの FabricPool 階層化用にクラスタ間 LIF を作成しています"

このタスクについて

ONTAP 9.8 以降では、ONTAP S3 サーバのロードバランシングが有効になっています。サーバのホスト名が複数の IP アドレスに解決される場合、ONTAP は、返されるすべての IP アドレス（最大 16 個の IP アドレス）とのクライアント接続を確立します。接続が確立されると、IP アドレスはラウンドロビン方式でピックアップされます。

の手順

ONTAP System ManagerまたはONTAP CLIを使用して、FabricPool のクラウド階層としてONTAP S3をセットアップできます。

## System Manager の略

1. ストレージ>階層>クラウド階層の追加\*をクリックし、オブジェクトストアプロバイダとしてONTAP S3を選択します。
2. 必要な情報を入力します。
3. CloudMirror を作成する場合は、\* FabricPool ミラーとして追加 \* をクリックします。

FabricPool ミラーを使用すると、データストアをシームレスに置き換えることができ、災害発生時にデータを確実に使用できるようになります。

## CLI の使用

1. S3 サーバと LIF のエントリを DNS サーバに追加します。

オプション	説明
• 外部 DNS サーバーを使用する場合 *	S3 サーバの名前と IP アドレスを DNS サーバ管理者に渡します。
• ローカルシステムの DNS hosts テーブル * を使用している場合	次のコマンドを入力します。  <code>dns host create -vserver svm_name -address ip_address -hostname s3_server_name</code>

2. を使用して、ONTAP S3の設定情報を指定します `storage aggregate object-store config create` コマンドにを指定します `-provider-type ONTAP_S3` パラメータ

- 。 `storage aggregate object-store config create` 指定した情報でローカルのONTAP システムがONTAP S3サーバにアクセスできない場合、コマンドは失敗します。
- を使用します `-access-key` ONTAP S3サーバへの要求を認証するためのアクセスキーを指定するパラメータ。
- を使用します `-secret-password` ONTAP S3サーバへの要求を認証するためのパスワード（シークレットアクセスキー）を指定するパラメータ。
- ONTAP S3 サーバのパスワードが変更された場合は、ローカルの ONTAP システムに格納されている対応するパスワードをただちに更新する必要があります。

これにより、ONTAP S3 オブジェクトストア内のデータに中断なくアクセスできます。

- を設定します `-is-certificate-validation-enabled` パラメータの値 `false` ONTAP S3の証明書のチェックを無効にします。

```
cluster1::> storage aggregate object-store config create  
-object-store-name myS3 -provider-type ONTAP_S3 -server myS3server  
-container-name myS3container -access-key myS3key  
-secret-password myS3pass
```

3. を使用して、ONTAP\_S3の設定情報を表示して確認します `storage aggregate object-store config show` コマンドを実行します

- `storage aggregate object-store config modify` コマンドを使用して、を変更できます  
ONTAP\_S3 FabricPool の設定情報。

クラウド階層として **Alibaba Cloud Object Storage** をセットアップします

ONTAP 9.6 以降を実行している場合は、Alibaba Cloud Object Storage を FabricPool のクラウド階層としてセットアップできます。

**FabricPool** でAlibaba Cloud Object Storageを使用する場合の考慮事項

- FabricPool ライセンスが必要な場合があります。

新規に購入した AFF システムには、FabricPool を使用するための 10TB の空き容量が含まれています。AFFシステムで追加の容量が必要な場合、AFF以外のシステムでAlibaba Cloud Object Storageを使用する場合、または既存のクラスタからアップグレードする場合は、"[FabricPool ライセンス](#)"。

- AFF および FAS システムと ONTAP Select では、FabricPool で Alibaba Object Storage Service の次のクラスがサポートされます。
  - Alibaba Object Storage Service Standard の略
  - Alibaba Object Storage Service のアクセス頻度が低い

["Alibaba Cloud : ストレージクラスの概要"](#)

上記以外のストレージクラスについては、ネットアップ営業担当者にお問い合わせください。

手順

1. を使用して、Alibaba Cloud Object Storageの設定情報を指定します `storage aggregate object-store config create` コマンドにを指定します `-provider-type AliCloud` パラメータ
  - `storage aggregate object-store config create` 指定された情報でONTAP がAlibaba Cloud Object Storageにアクセスできない場合、コマンドが失敗します。
  - を使用します `-access-key` Alibaba Cloud Object Storageオブジェクトストアへの要求を認証するためのアクセスキーを指定するパラメータ。
  - Alibaba Cloud Object Storage のパスワードが変更された場合は、ONTAP に格納されている対応するパスワードをただちに更新する必要があります。

これにより、ONTAP は引き続き Alibaba Cloud Object Storage 内のデータにアクセスできます。

```
storage aggregate object-store config create my_ali_oss_store_1
-provider-type AliCloud -server oss-us-east-1.aliyuncs.com
-container-name my-ali-oss-bucket -access-key DXJRXHPXHYXA9X31X3JX
```

2. を使用して、Alibaba Cloud Object Storageの設定情報を表示して確認します `storage aggregate`

object-store config show コマンドを実行します

。 storage aggregate object-store config modify コマンドを使用して、FabricPool のAlibaba クラウドオブジェクトストレージの設定情報を変更できます。

## クラウド階層としてのAmazon S3のセットアップ

ONTAP 9.2以降を実行している場合は、Amazon S3をFabricPoolのクラウド階層としてセットアップできます。ONTAP 9.5以降を実行している場合は、FabricPool用にAmazon コマーシャルクラウドサービス（C2S）をセットアップできます。

### FabricPoolでAmazon S3を使用する場合の考慮事項

- FabricPool ライセンスが必要な場合があります。
  - 新規に購入した AFF システムには、FabricPool を使用するための 10TB の空き容量が含まれています。

AFFシステムで追加の容量が必要な場合、AFF以外のシステムでAmazon S3を使用する場合、または既存のクラスタからアップグレードする場合は、"[FabricPool ライセンス](#)"。

既存のクラスタ用に FabricPool を初めて購入した場合は、10TB の空き容量を含む FabricPool ライセンスが付随します。

- ONTAPがAmazon S3オブジェクトサーバとの接続に使用するLIFは10Gbpsポートに配置することを推奨します。
- AFF および FAS システムと ONTAP Select では、FabricPool で次の Amazon S3 ストレージクラスがサポートされます。
  - Amazon S3 Standard の略
  - Amazon S3 標準 - 低頻度アクセス（標準 -IA）
  - Amazon S3 ONE ゾーン - アクセス頻度が低い（1 ザーン -IA）
  - Amazon S3 インテリジェント階層化
  - Amazon Commercial クラウドサービスの略
  - ONTAP 9.11.1以降では、Amazon S3 Glacier Instant Retrieval（FabricPoolではGlacier Flexible RetrievalやGlacier Deep Archiveはサポートされません）

["Amazon Web Servicesドキュメント：「Amazon S3 Storage Classes」"](#)

上記以外のストレージクラスについては、営業担当者にお問い合わせください。

- Cloud Volumes ONTAP では、FabricPool が Amazon Elastic Block Store（EBS）の汎用 SSD（gp2）ボリュームおよびスループット最適化 HDD（st1）ボリュームからの階層化をサポートします。

### 手順

1. を使用して、Amazon S3の設定情報を指定します。 storage aggregate object-store config create コマンドにを指定します -provider-type AWS\_S3 パラメータ
  - を使用します -auth-type CAP C2Sアクセスのクレデンシャルを取得するためのパラメータ。

を使用する場合 `-auth-type CAP` パラメータを使用する必要があります `-cap-url` C2Sアクセス用の一時的なクレデンシャルを要求する完全なURLを指定するパラメータ。

- 。 `storage aggregate object-store config create` 指定された情報でONTAPがAmazon S3にアクセスできない場合、コマンドが失敗します。
- 。 使用します `-access-key` Amazon S3オブジェクトストアへの要求を認証するためのアクセスキーを指定するパラメータ。
- 。 使用します `-secret-password` Amazon S3オブジェクトストアへの要求を認証するためのパスワード（シークレットアクセスキー）を指定するパラメータ。
- 。 Amazon S3のパスワードが変更された場合は、ONTAPに格納されている対応するパスワードをただちに更新する必要があります。

これにより、ONTAPは引き続きAmazon S3内のデータにアクセスできます。

```
cluster1::> storage aggregate object-store config create
-object-store-name my_aws_store -provider-type AWS_S3
-server s3.amazonaws.com -container-name my-aws-bucket
-access-key DXJRXHPXHYXA9X31X3JX
```

+

```
cluster1::> storage aggregate object-store config create -object-store
-name my_c2s_store -provider-type AWS_S3 -auth-type CAP -cap-url
https://123.45.67.89/api/v1/credentials?agency=XYZ&mission=TESTACCT&role
=S3FULLACCESS -server my-c2s-s3server-fqdn -container my-c2s-s3-bucket
```

2. を使用して、Amazon S3の設定情報を表示して確認します。 `storage aggregate object-store config show` コマンドを実行します

- 。 `storage aggregate object-store config modify` コマンドを使用して、FabricPoolのAmazon S3の設定情報を変更できます。

クラウド階層として **Google Cloud Storage** をセットアップします

ONTAP 9.6 以降を実行している場合は、Google Cloud Storage を FabricPool のクラウド階層としてセットアップできます。

**FabricPool** で **Google Cloud Storage** を使用する場合はその他の考慮事項を示します

- FabricPool ライセンスが必要な場合があります。

新規に購入した AFF システムには、FabricPool を使用するための 10TB の空き容量が含まれています。AFFシステムで追加の容量が必要な場合、AFF以外のシステムでGoogle Cloud Storageを使用する場合、または既存のクラスタからアップグレードする場合は、[xref:./fabricpool/"FabricPool ライセンス"](#)。

- ONTAP がGoogle Cloud Storageオブジェクトサーバとの接続に使用するLIFは10Gbpsポートに配置する

ことを推奨します。

- AFF および FAS システムと ONTAP Select では、FabricPool で次の Google Cloud Object ストレージクラスがサポートされます。
  - Google Cloud Multi-Regional の場合
  - Google Cloud リージョナル
  - Google Cloud Nearline
  - Google Cloud Coldline

#### "Google Cloud : ストレージクラス"

#### 手順

1. を使用して、Google Cloud Storageの設定情報を指定します `storage aggregate object-store config create` コマンドにを指定します `-provider-type GoogleCloud` パラメータ
  - `storage aggregate object-store config create` 指定された情報でONTAP がGoogle Cloud Storageにアクセスできない場合は、コマンドが失敗します。
  - を使用します `-access-key` パラメータを使用して、Google Cloud Storageオブジェクトストアへの要求を認証するためのアクセスキーを指定します。
  - Google Cloud Storage のパスワードが変更された場合は、ONTAP に格納されている対応するパスワードをただちに更新する必要があります。

これにより、ONTAP は引き続き Google Cloud Storage 内のデータにアクセスできます。

```
storage aggregate object-store config create my_gcp_store_1 -provider
-type GoogleCloud -container-name my-gcp-bucket1 -access-key
GOOGAUZZUV2USCFGHGQ511I8
```

2. を使用して、Google Cloud Storageの設定情報を表示して確認します `storage aggregate object-store config show` コマンドを実行します
  - `storage aggregate object-store config modify` コマンドを使用して、FabricPool のGoogle Cloud Storageの設定情報を変更できます。

クラウド階層として **IBM Cloud Object Storage** をセットアップします

ONTAP 9.5 以降を実行している場合は、FabricPool のクラウド階層として IBM Cloud Object Storage をセットアップできます。

**FabricPool** で**IBM Cloud Object Storage**を使用する場合の考慮事項について説明します

- FabricPool ライセンスが必要な場合があります。

新規に購入した AFF システムには、FabricPool を使用するための 10TB の空き容量が含まれています。AFFシステムで追加の容量が必要な場合、AFF以外のシステムでIBM Cloud Object Storageを使用する場合、または既存のクラスタからアップグレードする場合は、"[FabricPool ライセンス](#)"。

既存のクラスタ用に FabricPool を初めて購入した場合は、10TB の空き容量を含む FabricPool ライセンスが付随します。

- ONTAP が IBM Cloud オブジェクトサーバとの接続に使用する LIF は 10Gbps ポートに配置することを推奨します。

## 手順

1. を使用して、IBM Cloud Object Storage の設定情報を指定します `storage aggregate object-store config create` コマンドにを指定します `-provider-type IBM_COS` パラメータ
  - `storage aggregate object-store config create` 指定された情報で ONTAP が IBM Cloud Object Storage にアクセスできない場合は、コマンドが失敗します。
  - を使用します `-access-key` IBM Cloud Object Storage オブジェクトストアへの要求を認証するためのアクセスキーを指定するパラメータ。
  - を使用します `-secret-password` IBM Cloud Object Storage オブジェクトストアへの要求を認証するためのパスワード（シークレットアクセスキー）を指定するパラメータ。
  - IBM Cloud Object Storage のパスワードが変更された場合は、ONTAP に格納されている対応するパスワードをただちに更新する必要があります。

これにより、ONTAP は引き続き IBM Cloud Object Storage 内のデータにアクセスできます。

```
storage aggregate object-store config create
-object-store-name MyIBM -provider-type IBM_COS
-server s3.us-east.objectstorage.softlayer.net
-container-name my-ibm-cos-bucket -access-key DXJRHPXHYXA9X31X3JX
```

2. を使用して、IBM Cloud Object Storage の設定情報を表示して確認します `storage aggregate object-store config show` コマンドを実行します
  - `storage aggregate object-store config modify` コマンドを使用して、FabricPool の IBM Cloud Object Storage の設定情報を変更できます。

クラウド階層としてクラウド用の **Azure Blob Storage** をセットアップします

ONTAP 9.4 以降を実行している場合は、クラウド用 Azure Blob Storage を FabricPool のクラウド階層としてセットアップできます。

## FabricPool で Microsoft Azure Blob Storage を使用する場合の考慮事項

- FabricPool ライセンスが必要な場合があります。

新規に購入した AFF システムには、FabricPool を使用するための 10TB の空き容量が含まれています。AFF システムで追加の容量が必要な場合、AFF 以外のシステムで Azure Blob Storage を使用する場合、または既存のクラスタからアップグレードする場合は、[xref:./fabricpool/"FabricPool ライセンス"](#)。

既存のクラスタ用に FabricPool を初めて購入した場合は、10TB の空き容量を含む FabricPool ライセンスが付随します。

- Cloud Volumes ONTAP で Azure Blob Storage を使用する場合は、FabricPool ライセンスは必要ありません。
- ONTAP が Azure Blob Storage オブジェクトサーバとの接続に使用する LIF は、10Gbps ポートに配置することを推奨します。
- 現在、FabricPool はオンプレミスの Azure サービスである Azure Stack をサポートしていません。
- Microsoft Azure Blob Storage のアカウントレベルでは、FabricPool はホットとクールのストレージ階層のみをサポートします。

FabricPool では、blob レベルの階層化はサポートされません。また、Azure のアーカイブストレージ階層への階層化もサポートされません。

#### このタスクについて

現在、FabricPool はオンプレミスの Azure サービスである Azure Stack をサポートしていません。

#### 手順

1. を使用して、Azure Blob Storage の設定情報を指定します `storage aggregate object-store config create` コマンドにを指定します `-provider-type Azure_Cloud` パラメータ
  - `storage aggregate object-store config create` 指定された情報で ONTAP が Azure Blob Storage にアクセスできない場合、コマンドが失敗します。
  - を使用します `-azure-account` Azure Blob Storage アカウントを指定するパラメータ。
  - を使用します `-azure-private-key` Azure Blob Storage への要求を認証するためのアクセスキーを指定するパラメータ。
  - Azure Blob Storage のパスワードが変更された場合は、ONTAP に格納されている対応するパスワードをただちに更新する必要があります。

これにより、ONTAP は引き続き Azure Blob Storage 内のデータにアクセスできます。

```
cluster1::> storage aggregate object-store config create
-object-store-name MyAzure -provider-type Azure_Cloud
-server blob.core.windows.net -container-name myAzureContainer
-azure-account myAzureAcct -azure-private-key myAzureKey
```

2. を使用して、Azure Blob Storage の設定情報を表示して確認します `storage aggregate object-store config show` コマンドを実行します
  - `storage aggregate object-store config modify` コマンドを使用して、FabricPool の Azure Blob Storage の設定情報を変更できます。

#### MetroCluster 構成で FabricPool のオブジェクトストアを設定する

ONTAP 9.7 以降を実行している場合、MetroCluster 構成にミラーリングされた FabricPool をセットアップして、2 つの異なる障害ゾーンにあるオブジェクトストアにコールドデータを階層化できます。



## このタスクについて

- MetroCluster の FabricPool では、基盤となるミラーアグリゲートと関連するオブジェクトストア設定が同じ MetroCluster 構成に所属している必要があります。
- リモートの MetroCluster サイトで作成されたオブジェクトストアにアグリゲートを接続することはできません。
- アグリゲートが所属する MetroCluster 構成にオブジェクトストアを設定する必要があります。

## 作業を開始する前に

- MetroCluster 構成がセットアップされ、適切に設定されている。
- 2 つのオブジェクトストアが適切な MetroCluster サイトにセットアップされている。
- 各オブジェクトストアにコンテナが設定されている。
- 2 つの MetroCluster 構成に IP スペースが作成または識別され、それらの名前が一致している。

## ステップ

1. を使用して、各 MetroCluster サイトのオブジェクトストア設定情報を指定します `storage object-store config create` コマンドを実行します

この例では、MetroCluster 構成の一方のクラスタにのみ FabricPool が必要です。オブジェクトストアバケットごとに 1 つずつ、計 2 つのオブジェクトストア設定をそのクラスタに作成します。

```
storage aggregate
  object-store config create -object-store-name mccl-ostore-config-s1
  -provider-type SGWS -server
    <SGWS-server-1> -container-name <SGWS-bucket-1> -access-key <key>
  -secret-password <password> -encrypt
    <true|false> -provider <provider-type> -is-ssl-enabled <true|false>
  ipspace
    <IPSpace>
```

```
storage aggregate object-store config create -object-store-name mccl-
ostore-config-s2
  -provider-type SGWS -server <SGWS-server-2> -container-name <SGWS-
bucket-2> -access-key <key> -secret-password <password> -encrypt
  <true|false> -provider <provider-type>
  -is-ssl-enabled <true|false> ipspace <IPSpace>
```

この例では、MetroCluster 構成のもう一方のクラスタに FabricPool をセットアップします。

```
storage aggregate
  object-store config create -object-store-name mcc2-ostore-config-s1
  -provider-type SGWS -server
    <SGWS-server-1> -container-name <SGWS-bucket-3> -access-key <key>
  -secret-password <password> -encrypt
    <true|false> -provider <provider-type> -is-ssl-enabled <true|false>
  ipspace
    <IPSpace>
```

```
storage aggregate
  object-store config create -object-store-name mcc2-ostore-config-s2
  -provider-type SGWS -server
    <SGWS-server-2> -container-name <SGWS-bucket-4> -access-key <key>
  -secret-password <password> -encrypt
    <true|false> -provider <provider-type> -is-ssl-enabled <true|false>
  ipspace
    <IPSpace>
```

ローカル階層に接続する前にオブジェクトストアのスループットパフォーマンスをテストする

オブジェクトストアをローカル階層に接続する前に、オブジェクトストアプロファイラを使用してオブジェクトストアのレイテンシとスループットのパフォーマンスをテストできます。

その前に

- オブジェクトストアプロファイラでクラウド階層を使用するには、ONTAPにクラウド階層を追加する必要があります。
- ONTAP CLIのadvanced権限モードに切り替える必要があります。

手順

1. オブジェクトストアプロファイラを起動します。

```
storage aggregate object-store profiler start -object-store-name <name> -node
<name>
```

2. 結果を表示します。

```
storage aggregate object-store profiler show
```

クラウド階層をローカル階層（アグリゲート）に接続する

クラウド階層として使用するオブジェクトストアのセットアップが完了したら、使用するローカル階層（アグリゲート）をFabricPoolに接続して指定します。ONTAP 9.5以降では、対象となるFlexGroup ボリュームコンスティチュエントを含むローカル階層（ア

グリゲート) を接続することもできます。

このタスクについて

ローカル階層へのクラウド階層の接続は永続的な操作です。接続後にローカル階層からクラウド階層の接続を解除することはできません。ただし、"[FabricPoolミラー](#)" をクリックして、別のクラウド階層にローカル階層を接続します。

作業を開始する前に

ONTAP CLI を使用して FabricPool 用のアグリゲートをセットアップする場合は、既存のアグリゲートを使用する必要があります。




System Managerを使用してFabricPool のローカル階層をセットアップする場合は、ローカル階層を作成し、FabricPool に使用するように設定できます。

手順

ONTAP System ManagerまたはONTAP CLIを使用して、FabricPool オブジェクトストアにローカル階層（アグリゲート）を接続できます。

## System Manager の略

1. 「\*ストレージ」>「階層」に移動し、クラウド階層を選択して、をクリックします .
2. ローカル階層の接続\*を選択します。
3. [プライマリとして追加]で、ボリュームが接続可能であることを確認します。
4. 必要に応じて、\*ボリュームをシンプロビジョニングに変換\*を選択します。
5. [保存 (Save) ] をクリックします。

## CLI の使用

CLIを使用してアグリゲートにオブジェクトストアを接続するには、次の手順を実行します。

1. \* オプション \* : ボリューム内のアクセス頻度の低いデータの量を確認するには、の手順に従います ["Inactive Data Reporting によるボリューム内のアクセス頻度の低いデータ量の確認"](#)。

ボリューム内のアクセス頻度の低いデータの量を確認すると、FabricPool に使用するアグリゲートを決定するのに役立ちます。

2. を使用してオブジェクトストアをアグリゲートに接続します `storage aggregate object-store attach` コマンドを実行します

FabricPool で使用したことがないアグリゲートで、既存のボリュームが含まれている場合は、デフォルトのボリュームが割り当てられます `snapshot-only` 階層化ポリシー：

```
cluster1::> storage aggregate object-store attach -aggregate myaggr
-object-store-name Amazon01B1
```

を使用できます `allow-flexgroup true` FlexGroup ボリュームのコンスティチュエントを含むアグリゲートを接続するオプション。

3. を使用してオブジェクトストアの情報を表示し、接続したオブジェクトストアが使用可能であることを確認します `storage aggregate object-store show` コマンドを実行します

```
cluster1::> storage aggregate object-store show
```

Aggregate	Object Store Name	Availability State
-----	-----	-----
myaggr	Amazon01B1	available

データをローカルバケットに階層化します

ONTAP 9.8 以降では、ONTAP S3 を使用してローカルオブジェクトストレージにデータを階層化できます。


データをローカルバケットに階層化すると、データを別のローカル階層に移動する簡単な方法が提供されます。この手順では、ローカルクラスタの既存のバケットを使用することも、ONTAP で新しい Storage VM と

新しいバケットを自動的に作成することもできます。

ローカル階層（アグリゲート）に接続したクラウド階層は接続を解除できないことに注意してください。

このワークフローには S3 ライセンスが必要です。このライセンスでは、新しい S3 サーバと新しいバケットを作成するか、または既存の S3 ライセンスを使用します。このライセンスは、**"ONTAP One"**。このワークフローには FabricPool ライセンスは必要ありません。

#### ステップ

1. データをローカルバケットに階層化します。「\* Tiers \*」をクリックし、階層を選択して、をクリックします .
2. 必要に応じて、シンプロビジョニングを有効にします。
3. 既存の階層を選択するか、新しい階層を作成してください。
4. 必要に応じて、既存の階層化ポリシーを編集します。

## FabricPool を管理します

### Manage FabricPool の概要

ストレージ階層化のニーズに対応するため、ONTAP では、ボリューム内のアクセス頻度の低いデータ量の表示、FabricPool へのボリュームの追加と移動、FabricPool のスペース使用量の監視、ボリュームの階層化ポリシーや階層化の最小クーリング期間の変更が可能です。

**Inactive Data Reporting** でボリューム内のアクセス頻度の低いデータの量を確認

ボリューム内のアクセス頻度の低いデータの量を確認することで、ストレージ階層を効率よく使用することができます。Inactive Data Reporting の情報を参考に、FabricPool に使用するアグリゲート、FabricPool との間でボリュームを移動するかどうか、ボリュームの階層化ポリシーを変更するかどうかを決定することができます。

#### 必要なもの

Inactive Data Reporting 機能を使用するには、ONTAP 9.4 以降が必要です。

#### このタスクについて

- Inactive Data Reporting は、一部のアグリゲートではサポートされません。

FabricPool を有効にできない場合は、次のような Inactive Data Reporting を有効にできません。

- ルートアグリゲート
- 9.7 より前のバージョンの ONTAP を実行している MetroCluster アグリゲート
- Flash Pool（ハイブリッドアグリゲートまたは SnapLock アグリゲート）
- アダプティブ圧縮が有効になっているボリュームがあるアグリゲートでは、Inactive Data Reporting がデフォルトで有効になります。
- ONTAP 9.6 では、すべての SSD アグリゲートに対して Inactive Data Reporting がデフォルトで有効になります。


- ONTAP 9.4 および ONTAP 9.5 の FabricPool アグリゲートでは、Inactive Data Reporting がデフォルトで有効になります。
- ONTAP 9.6 以降では、HDD アグリゲートを含む ONTAP CLI を使用して、FabricPool 以外のアグリゲートに対して Inactive Data Reporting を有効にできます。

#### 手順

アクセス頻度の低いデータの量は、ONTAP System ManagerまたはONTAP CLIで確認できます。

## System Manager の略

### 1. 次のいずれかのオプションを選択します。

- 既存の HDD アグリゲートがある場合は、「\* Storage 」 > 「 Tiers \* 」の順に選択し、をクリックします  アクセス頻度の低いデータのレポートを有効にするアグリゲートについて選択します。
- クラウド階層が設定されていない場合は、\* ダッシュボード \* に移動し、\* 容量 \* の下の \* 非アクティブデータレポートの有効化 \* リンクをクリックします。

## CLI の使用

CLIを使用して非アクティブデータレポートを有効にするには、次の手順

1. Inactive Data Reportingを表示するアグリゲートがFabricPool で使用されていない場合は、を使用してアグリゲートのInactive Data Reportingを有効にします storage aggregate modify コマンドにを指定します -is-inactive-data-reporting-enabled true パラメータ

```
cluster1::> storage aggregate modify -aggregate aggr1 -is-inactive
-data-reporting-enabled true
```

FabricPool に使用されていないアグリゲートでは、Inactive Data Reporting 機能を明示的に有効にする必要があります。

FabricPool 対応アグリゲートについては、すでに Inactive Data Reporting が有効になっているため有効にする必要はありません。。 -is-inactive-data-reporting-enabled パラメータはFabricPool対応アグリゲートでは機能しません。

◦ -fields is-inactive-data-reporting-enabled のパラメータ storage aggregate show コマンドは、アグリゲートでInactive Data Reportingが有効になっているかどうかを表示します。

2. ボリューム上のアクセス頻度の低いデータの量を表示するには、を使用します volume show コマンドにを指定します -fields performance-tier-inactive-user-data,performance-tier-inactive-user-data-percent パラメータ

```
cluster1::> volume show -fields performance-tier-inactive-user-
data,performance-tier-inactive-user-data-percent

vserver volume performance-tier-inactive-user-data performance-tier-
inactive-user-data-percent
-----
-----
vsim1    vol0    0B                                0%
vs1      vs1rv1  0B                                0%
vs1      vv1     10.34MB                             0%
vs1      vv2     10.38MB                             0%
4 entries were displayed.
```

- °。 performance-tier-inactive-user-data フィールドには、アグリゲートに格納されているアクセス頻度の低いユーザデータの量が表示されます。
- °。 performance-tier-inactive-user-data-percent フィールドには、アクティブファイルシステムとSnapshotコピー全体でアクセス頻度の低いデータの割合が表示されます。
- ° FabricPool に使用されていないアグリゲートの場合、Inactive Data Reportingは階層化ポリシーを使用してコールドとしてレポートするデータの量を決定します。
  - をクリックします none 階層化ポリシーでは31日が使用されます。
  - をクリックします snapshot-only および auto、Inactive Data Reportingのを使用します tiering-minimum-cooling-days。
  - をクリックします ALL ポリシーのInactive Data Reportingでは、データが1日以内に階層化されることが想定されています。

期間が終了するまで ' 出力には ' 値ではなく ' 非アクティブなデータの量が表示されます
- ° FabricPool に含まれるボリュームの場合、アクセス頻度の低いデータとして報告される ONTAP は、ボリュームに設定されている階層化ポリシーによって異なります。
  - をクリックします none 階層化ポリシーのONTAP では、ボリューム全体のうち、少なくとも31日間アクセスされていないデータの量が報告されます。を使用することはできません -tiering-minimum-cooling-days パラメータと none 階層化ポリシー：
  - をクリックします ALL、 snapshot-only`および `auto 階層化ポリシーのInactive Data Reportingはサポートされません。

**FabricPool**のボリュームを管理します。

**FabricPool** 用のボリュームを作成します

FabricPool にボリュームを追加するには、 FabricPool 対応アグリゲートに直接ボリュームを新規作成するか、別のアグリゲートから FabricPool 対応アグリゲートに既存のボリュームを移動します。

FabricPool 用のボリュームを作成するときに、階層化ポリシーを指定できます。階層化ポリシーを指定しない場合、作成されるボリュームではデフォルトが使用されます snapshot-only 階層化ポリシー：を含むボリュームの場合 snapshot-only または auto 階層化ポリシーでは、階層化の最小クーリング期間も指定できます。

必要なもの

- を使用するようにボリュームを設定します auto 階層化ポリシーまたは階層化の最小クーリング期間を指定するには、ONTAP 9.4以降が必要です。
- FlexGroup ボリュームを使用するには、ONTAP 9.5 以降が必要です。
- を使用するようにボリュームを設定します all 階層化ポリシーにはONTAP 9.6以降が必要です。
- を使用するようにボリュームを設定します -cloud-retrieval-policy パラメータにはONTAP 9.8以降が必要です。

手順

1. を使用して、FabricPool 用の新しいボリュームを作成します volume create コマンドを実行します



- 。 -tiering-policy オプションのパラメータを使用すると、ボリュームの階層化ポリシーを指定できます。

次のいずれかの階層化ポリシーを指定できます。

- snapshot-only (デフォルト)
- auto
- all
- backup (廃止予定)
- none

#### "FabricPool 階層化ポリシーのタイプ"

- 。 -cloud-retrieval-policy オプションのパラメータを指定すると、advanced権限レベルのクラスタ管理者は、階層化ポリシーで制御されるデフォルトのクラウド移行または読み出し動作を上書きできます。

次のいずれかのクラウド読み出しポリシーを指定できます。

- default

どのデータを移行するかは階層化ポリシーによって決定されるため、でのクラウドデータの読み出しに変更はありません default cloud-retrieval-policy：つまり、ONTAP 9.8 より前のリリースと同じです。

- 階層化ポリシーがの場合 none または snapshot-only 「default」とは、クライアントによって読み取られたデータがすべてクラウド階層から高パフォーマンス階層に移行されることを意味します。
- 階層化ポリシーがの場合 `auto` に設定すると、クライアントによるランダムリードはすべてプルされますが、シーケンシャルリードはプルされません。
- 階層化ポリシーがの場合 all その後、クライアントによって読み取られたデータはクラウド階層から移行されません。

- on-read

クライアントからのデータ読み取りは、すべてクラウド階層からパフォーマンス階層に引き上げられます。

- never

クライアント中心のデータは、クラウド階層からパフォーマンス階層に移動されません

- promote

- 階層化ポリシーに使用します `none` すべてのクラウドデータがクラウド階層から高パフォーマンス階層に移行されます
- 階層化ポリシーに使用します `snapshot-only` のすべてのアクティブなファイルシステムデータがクラウド階層から高パフォーマンス階層に移行されます。

- 。 -tiering-minimum-cooling-days advanced権限レベルでオプションのパラメータを指定する

と、を使用するボリュームの階層化の最小クーリング期間を指定できます snapshot-only または auto 階層化ポリシー：

ONTAP 9.8 以降では、階層化の最小クーリング日数に 2 ~ 183 の値を指定できます。9.8 より前のバージョンの ONTAP を使用している場合は、階層化の最小クーリング期間に 2~63 の値を指定できません。

#### FabricPool 用のボリュームを作成する例

次の例は、「FabricPool」対応アグリゲートに「myvol1」という名前のボリュームを作成します。階層化ポリシーがに設定されている auto 階層化の最小クーリング期間は45日に設定されています。

```
cluster1::*> volume create -vserver myVS -aggregate myFabricPool  
-volume myvol1 -tiering-policy auto -tiering-minimum-cooling-days 45
```

#### 関連情報

##### "FlexGroup ボリューム管理"

ボリュームを **FabricPool** に移動します

ボリュームを FabricPool に移動する場合は、move コマンドを使用してボリュームの階層化ポリシーを指定または変更できます。ONTAP 9.8 以降では、Inactive Data Reporting を有効にして FabricPool 以外のボリュームを移動する場合、FabricPool はヒートマップを使用して階層化可能なブロックを読み取り、コールドデータを FabricPool デステーションの大容量階層に移動します。

#### 必要なもの

階層化ポリシーを変更することが、データがコールドと認識されてクラウド階層に移動されるまでの時間にどのように影響するかを理解しておく必要があります。

##### "ボリュームを移動した場合の階層化ポリシーへの影響"

#### このタスクについて

FabricPool以外のボリュームでInactive Data Reportingが有効になっている場合は、階層化ポリシーを使用してボリュームを移動したとき auto または snapshot-only FabricPool はFabricPool に対して、ヒートマップファイルから階層化可能な温度ブロックを読み取り、その温度を使用してコールドデータをFabricPool デステーションの大容量階層に直接移動します。

を使用しないでください -tiering-policy オプション（ONTAP 9.8を使用していて、Inactive Data Reportingの情報をを使用してデータを大容量階層に直接移動する場合）。このオプションを使用すると、ONTAP 9.8 より前のリリースの移動動作に従って、FabricPool は温度データを無視します。

#### ステップ

1. 使用します volume move start コマンドを使用してボリュームをFabricPool に移動します。

。 -tiering-policy オプションのパラメータを使用すると、ボリュームの階層化ポリシーを指定できます。

次のいずれかの階層化ポリシーを指定できます。

- snapshot-only (デフォルト)
  - auto
  - all
  - none
- [+]  
["FabricPool 階層化ポリシーのタイプ"](#)

#### ボリュームを**FabricPool**に移動する例

次の例は、「vs1」 SVM 内の「myvol2」という名前のボリュームを「dest\_FabricPool」 FabricPool 対応アグリゲートに移動します。ボリュームはを使用するように明示的に設定されます  
 `none` 階層化ポリシー：

```
cluster1::> volume move start -vserver vs1 -volume myvol2
               -destination-aggregate dest_FabricPool -tiering-policy none
```

#### ボリュームをクラウドに直接書き込むための有効化と無効化

ONTAP 9.14.1以降では、FabricPoolの新規または既存のボリュームに対してクラウドへの直接書き込みを有効または無効にすることで、NFSクライアントが階層化スキャンを待たずにクラウドに直接データを書き込むことができます。SMBクライアントは、クラウドの書き込みが有効なボリュームの高パフォーマンス階層に引き続き書き込みます。cloud-writeモードはデフォルトで無効になっています。

クラウドに直接書き込む機能は、ローカル階層でクラスタでサポートできない大量のデータがクラスタに転送されるなど、移行のような場合に役立ちます。cloud-writeモードを使用しない場合は、移行中に少量のデータが転送されてから階層化され、移行が完了するまで再び転送されて階層化されます。cloud-writeモードを使用すると、データがローカル階層に転送されないため、この種の管理は不要になります。

#### 作業を開始する前に

- クラスタ管理者またはSVM管理者である必要があります。
- advanced権限レベルが必要です。
- 読み取り/書き込みタイプのボリュームである必要があります。
- ボリュームの階層化ポリシーが「すべて」である必要があります。

#### ボリューム作成時のクラウドへの直接書き込みを可能にする

##### 手順

1. 権限レベルを advanced に設定します。

```
set -privilege advanced
```

2. ボリュームを作成し、cloud-writeモードを有効にします。

```
volume create -volume <volume name> -is-cloud-write-enabled <true|false>
-aggregate <local tier name>
```

次の例は、FabricPoolローカル階層（aggr1）に、クラウド書き込みを有効にしてvol1という名前のボリュームを作成します。

```
volume create -volume vol1 -is-cloud-write-enabled true -aggregate aggr1
```

既存のボリュームのクラウドへの直接書き込みを可能にする

手順

1. 権限レベルを advanced に設定します。

```
set -privilege advanced
```

2. ボリュームを変更してcloud-writeモードを有効にします。

```
volume modify -volume <volume name> -is-cloud-write-enabled <true|false>
-aggregate <local tier name>
```

次の例は、FabricPoolローカル階層（aggr1）でクラウド書き込みを有効にしたvol1という名前のボリュームを変更します。

```
volume modify -volume vol1 -is-cloud-write-enabled true -aggregate aggr1
```

ボリュームのクラウドへの直接書き込みを無効にする

手順

1. 権限レベルを advanced に設定します。

```
set -privilege advanced
```

2. cloud-writeモードを無効にします。

```
volume modify -volume <volume name> -is-cloud-write-enabled <true|false>
-aggregate <aggregate name>
```

次の例は、vol1という名前のボリュームを作成し、クラウド書き込みを有効にします。

```
volume modify -volume vol1 -is-cloud-write-enabled false -aggregate
aggr1
```

#### アグレッシブ先読みモードの有効化と無効化

ONTAP 9.14.1以降では、ムービーストリーミングワークロードなどのメディアやエンターテインメントをサポートするFabricPoolのボリュームで、積極的な先読みモードを有効または無効にすることができます。ONTAP 9.14.1では、FabricPoolをサポートするすべてのオンプレミスプラットフォームでアグレッシブ先読みモードを使用できます。この機能はデフォルトで無効になっています。

#### このタスクについて

。 aggressive-readahead-mode コマンドには2つのオプションがあります。

- none:先読みは無効です。
- file\_prefetch:クライアントアプリケーションよりも先にファイル全体がメモリに読み込まれます。

#### 作業を開始する前に

- クラスタ管理者またはSVM管理者である必要があります。
- advanced権限レベルが必要です。

#### ボリューム作成時に積極的な先読みモードを有効にする

##### 手順

1. 権限レベルを advanced に設定します。

```
set -privilege advanced
```

2. ボリュームを作成し、アグレッシブ先読みモードを有効にします。

```
volume create -volume <volume name> -aggressive-readahead-mode
<none|file_prefetch>
```

次の例は、file\_prefetchオプションを指定して、アグレッシブ先読みを有効にしたvol1という名前のボリュームを作成します。

```
volume create -volume vol1 -aggressive-readahead-mode file_prefetch
```

#### アグレッシブ先読みモードを無効にする

##### 手順

1. 権限レベルを advanced に設定します。

```
set -privilege advanced
```

2. アグレッシブ先読みモードを無効にします。

```
volume modify -volume <volume name> -aggressive-readahead-mode none
```

次の例は、vol1という名前のボリュームを変更して、アグレッシブ先読みモードを無効にします。

```
volume modify -volume vol1 -aggressive-readahead-mode none
```

ボリュームのアグレッシブ先読みモードを表示する

手順

1. 権限レベルを advanced に設定します。

```
set -privilege advanced
```

2. アグレッシブ先読みモードを表示します。

```
volume show -fields aggressive-readahead-mode
```

ユーザが作成したカスタムタグを使用したオブジェクトタグ付け

ユーザが作成したカスタムタグを使用したオブジェクトタグ付けの概要

ONTAP 9.8 以降では、FabricPool でユーザが作成したカスタムタグを使用したオブジェクトタグ付けがサポートされているため、オブジェクトを分類して分類し、管理を容易にすることができます。admin 権限レベルのユーザは、新しいオブジェクトタグを作成し、既存のタグを変更、削除、および表示できます。

ボリュームの作成時に新しいタグを割り当てます

作成する新しいボリュームから階層化された新しいオブジェクトに 1 つ以上のタグを割り当てる場合は、新しいオブジェクトタグを作成できます。タグを使用すると、階層化オブジェクトを分類およびソートしてデータを簡単に管理できます。ONTAP 9.8以降では、System Managerを使用してオブジェクトタグを作成できます。

このタスクについて

タグは、StorageGRID に接続された FabricPool でのみ設定できます。これらのタグはボリュームの移動時に

保持されます。

- ボリュームあたり最大 4 つのタグを使用できます
- CLIでは、各オブジェクトタグはキーと値のペアを等号で区切って指定する必要があります ("")
- CLIでは、複数のタグをカンマで区切る必要があります ("")
- 各タグ値の最大文字数は 127 文字です
- 各タグキーの 1 文字目はアルファベットかアンダースコアにする必要があります。

キーに使用できる文字は英数字とアンダースコアのみです。最大文字数は 127 文字です。

## 手順

オブジェクトタグは、ONTAP システムマネージャまたはONTAP CLIを使用して割り当てることができます。

### System Manager の略

1. [ストレージ]>[階層]に移動します。
2. タグを付けるボリュームを含むストレージ階層を特定します。
3. [\* Volumes (ボリューム) ] タブをクリックします
4. タグを付けるボリュームを探し、\*オブジェクトタグ\*列で\*クリックしてタグを入力\*を選択します。
5. キーと値を入力します。
6. [ 適用 ( Apply ) ] をクリックします。

### CLI の使用

1. を使用します volume create コマンドにを指定します -tiering-object-tags 指定したタグを使用して新しいボリュームを作成するオプション。複数のタグをカンマで区切って指定できます。

```
volume create [ -vserver <vserver name> ] -volume <volume_name>
-tiering-object-tags <key1=value1> [
    ,<key2=value2>,<key3=value3>,<key4=value4> ]
```

次の例は、3 つのオブジェクトタグが指定された FP\_volume1 という名前のボリュームを作成します。

```
vol create -volume fp_volume1 -vserver vs0 -tiering-object-tags
project=fabricpool,type=abc,content=data
```

## 既存のタグを変更します

タグの名前を変更したり、オブジェクトストア内の既存のオブジェクトでタグを置き換えたり、あとで追加する予定の新しいオブジェクトに別のタグを追加したりできます。

## このタスクについて

を使用する `volume modify` コマンドにを指定します `-tiering-object-tags` オプションを指定すると、既存のタグが指定した新しい値に置き換えられます。

## 手順

### System Manager の略

1. [ストレージ]>[階層]に移動します。
2. 変更するタグが含まれているボリュームを含むストレージ階層を特定します。
3. [\* Volumes (ボリューム) ] タブをクリックします
4. 変更するタグが付いたボリュームを探し、\*オブジェクトタグ\*列でタグ名をクリックします。
5. タグを変更します。
6. [適用 (Apply) ] をクリックします。

### CLI の使用

1. 使用します `volume modify` コマンドにを指定します `-tiering-object-tags` 既存のタグを変更するオプション。

```
volume modify [ -vserver <vserver name> ] -volume <volume_name>  
-tiering-object-tags <key1=value1> [ ,<key2=value2>,  
<key3=value3>,<key4=value4> ]
```

次の例では、既存のタグタイプ =abc の名前を type=xyz に変更します。

```
vol create -volume fp_volume1 -vserver vs0 -tiering-object-tags  
project=fabricpool,type=xyz,content=data
```

## タグを削除します

ボリュームまたはオブジェクトストア内のオブジェクトに設定する必要がなくなったオブジェクトタグは削除できます。

## 手順

ONTAP システムマネージャまたはONTAP CLIを使用して、オブジェクトタグを削除できます。



## System Manager の略

1. [ストレージ]>[階層]に移動します。
2. 削除するタグが含まれているボリュームを含むストレージ階層を特定します。
3. [\* Volumes (ボリューム) ] タブをクリックします
4. 削除するタグが付いたボリュームを探し、\*オブジェクトタグ\*列でタグ名をクリックします。
5. タグを削除するには、ごみ箱のアイコンをクリックします。
6. [ 適用 ( Apply ) ] をクリックします。

## CLI の使用

1. を使用します volume modify コマンドにを指定します -tiering-object-tags オプションの後に空の値を入力します ("" ) をクリックして既存のタグを削除します。

次の例は、FP\_volume1 の既存のタグを削除します。

```
vol modify -volume fp_volume1 -vserver vs0 -tiering-object-tags ""
```

ボリュームの既存のタグを表示します

ボリューム上の既存のタグを表示して、新しいタグをリストに追加する前に使用できるタグを確認できます。

## ステップ

1. を使用します volume show コマンドにを指定します -tiering-object-tags ボリュームの既存のタグを表示するオプション。

```
volume show [ -vserver <vserver name> ] -volume <volume_name> -fields  
-tiering-object-tags
```

**FabricPool** ボリュームでオブジェクトのタグ付けステータスを確認します

1 つ以上の FabricPool ボリュームでタギングが完了しているかどうかを確認できます。

## ステップ

1. を使用します vol show コマンドにを指定します -fieldsneeds-object-retagging タグ付けが進行中かどうか、完了しているかどうか、またはタグ付けが設定されていないかどうかを確認するオプション。

```
vol show -fields needs-object-retagging [ -instance | -volume <volume  
name>]
```

次のいずれかの値が表示されます。

- `true` --このボリュームに対してオブジェクトタグ付けスキャナがまだ実行されていないか、再実行する必要があります
- `false` --このボリュームに対するオブジェクトタグ付けスキャナのタグ付けが完了しました
- `<->` --オブジェクトタグ付けスキャナはこのボリュームには適用されません。これは、FabricPool がないボリュームで発生します。

## FabricPool のスペース使用量を監視します

FabricPool のパフォーマンス階層とクラウド階層に格納されているデータ量を把握しておく必要があります。この情報は、ボリュームの階層化ポリシーの変更、FabricPool ライセンスで許可された使用量の制限の拡張、またはクラウド階層のストレージスペースの拡張が必要かどうかを確認するのに役立ちます。

### 手順

1. 次のいずれかのコマンドを使用して情報を表示し、FabricPool 対応アグリゲートのスペース使用量を監視します。

表示する項目	使用するコマンド
アグリゲートのクラウド階層の使用済みサイズ	<code>storage aggregate show</code> を使用 <code>-instance</code> パラメータ
オブジェクトストアの参照容量を含む、アグリゲート内のスペース使用量の詳細	<code>storage aggregate show-space</code> を使用 <code>-instance</code> パラメータ
アグリゲートに接続されているオブジェクトストアのスペース使用率。ライセンススペースの使用量も含まれます	<code>storage aggregate object-store show-space</code>
アグリゲート内のボリュームおよびそのデータとメタデータの容量のリスト	<code>volume show-footprint</code>

CLI コマンドに加え、Active IQ Unified Manager（旧 OnCommand Unified Manager）と FabricPool Advisor（ONTAP 9.4 以降のクラスタでサポート）または System Manager を使用してスペース使用量を監視することもできます。

次の例は、FabricPool のスペース使用量と関連情報を表示する方法を示しています。

```
cluster1::> storage aggregate show-space -instance
```

```
Aggregate: MyFabricPool
...
Aggregate Display Name:
MyFabricPool
...
Total Object Store Logical Referenced
Capacity: -
Object Store Logical Referenced Capacity
Percentage: -
...
Object Store
Size: -
Object Store Space Saved by Storage
Efficiency: -
Object Store Space Saved by Storage Efficiency
Percentage: -
Total Logical Used
Size: -
Logical Used
Percentage: -
Logical Unreferenced
Capacity: -
Logical Unreferenced
Percentage: -
```

```
cluster1::> storage aggregate show -instance
```

```
Aggregate: MyFabricPool
...
Composite: true
Capacity Tier Used Size:
...
```

```
cluster1::> volume show-footprint
```

```
Vserver : vs1
```

```
Volume : rootvol
```

Feature	Used	Used%
Volume Footprint	KB	%
Volume Guarantee	MB	%
Flexible Volume Metadata	KB	%
Delayed Frees	KB	%
Total Footprint	MB	%

```
Vserver : vs1
```

```
Volume : vol
```

Feature	Used	Used%
Volume Footprint	KB	%
Footprint in Performance Tier	KB	%
Footprint in Amazon01	KB	%
Flexible Volume Metadata	MB	%
Delayed Frees	KB	%
Total Footprint	MB	%
...		

2. 必要に応じて、次のいずれかの操作を実行します。

状況	作業
ボリュームの階層化ポリシーを変更する	の手順に従います " <a href="#">ボリュームの階層化ポリシーや階層化の最小クーリング期間を変更してストレージ階層化を管理する</a> "。
FabricPool ライセンスの使用量の上限を引き上げます	ネットアップまたはパートナーの営業担当者にお問い合わせください。  " <a href="#">ネットアップサポート</a> "
クラウド階層のストレージスペースを拡張する	クラウド階層として使用するオブジェクトストアのプロバイダにお問い合わせください。

ボリュームの階層化ポリシーまたは階層化の最小クーリング期間を変更して、ストレージの階層化を管理します

ボリュームの階層化ポリシーを変更することで、アクセス頻度が低くなったデータ（COM）をクラウド階層に移動するかどうかを制御できます。を含むボリュームの場合 snapshot-only または auto 階層化ポリシーでは、アクセスされていないユーザーデータがクラウド階層に移動されるまでの階層化の最小クーリング期間も指定できます。

#### 必要なもの

ボリュームをに変更しています auto 階層化ポリシーや階層化の最小クーリング期間を変更するには、ONTAP 9.4以降が必要です。

#### このタスクについて

ボリュームの階層化ポリシーを変更すると、そのボリュームに対する以降の階層化の動作のみ変更されます。変更前までさかのぼってデータがクラウド階層に移動されることはありません。

階層化ポリシーを変更すると、データがコールドと認識されてクラウド階層に移動されるまでの時間に影響することがあります。

#### "FabricPool でボリュームの階層化ポリシーを変更した場合の動作"

##### 手順

1. を使用して、既存のボリュームの階層化ポリシーを変更します volume modify コマンドにを指定します -tiering-policy パラメータ：

次のいずれかの階層化ポリシーを指定できます。

- snapshot-only （デフォルト）
- auto
- all
- none

#### "FabricPool 階層化ポリシーのタイプ"

2. ボリュームでが使用されている場合 snapshot-only または auto 階層化ポリシーを使用して階層化の最小クーリング期間を変更する場合は、を使用します volume modify コマンドにを指定します -tiering-minimum-cooling-days advanced権限レベルのオプションのパラメータ。

階層化の最小クーリング期間の値は、2~183 の範囲で指定できます。9.8 より前のバージョンの ONTAP を使用している場合は、階層化の最小クーリング期間に 2~63 の値を指定できます。

#### ボリュームの階層化ポリシーと階層化の最小クーリング期間の変更の例

次の例は、SVM「vs1」内のボリューム「myvol」の階層化ポリシーをに変更します auto 階層化の最小クーリング期間は45日です。

```
cluster1::> volume modify -vserver vs1 -volume myvol  
-tiering-policy auto -tiering-minimum-cooling-days 45
```

## FabricPool によるボリュームのアーカイブ（ビデオ）

このビデオでは、System Manager を使用して、FabricPool でクラウド階層にボリュームをアーカイブする方法の概要を紹介します。

["ネットアップのビデオ： Archiving volumes with FabricPool （ backup + volume move ） "](#)

### 関連情報

["NetApp TechComm TV ： FabricPool 関連ビデオ"](#)

クラウド移行コントロールを使用して、ボリュームのデフォルトの階層化ポリシーを上書きします

を使用して、クラウド階層から高パフォーマンス階層へのユーザデータの読み出しを制御するボリュームのデフォルトの階層化ポリシーを変更できます -cloud-retrieval-policy ONTAP 9.8で導入されたオプション。

### 必要なもの

- を使用したボリュームの変更 -cloud-retrieval-policy このオプションを使用するには、ONTAP 9.8以降が必要です。
- この処理を実行するには advanced 権限レベルが必要です。
- での階層化ポリシーの動作について理解しておく必要があります -cloud-retrieval-policy。

["階層化ポリシーがクラウド移行とどのように連携するか"](#)

### ステップ

1. を使用して、既存のボリュームの階層化ポリシーの動作を変更します volume modify コマンドにを指定します -cloud-retrieval-policy オプション：

```
volume create -volume <volume_name> -vserver <vserver_name> - tiering-policy <policy_name> -cloud-retrieval-policy
```

```
vol modify -volume fp_volume4 -vserver vs0 -cloud-retrieval-policy promote
```

データを高パフォーマンス階層に昇格

データをパフォーマンス階層の概要に昇格

ONTAP 9.8以降では、advanced権限レベルのクラスタ管理者は、を組み合わせで使用して、クラウド階層からパフォーマンス階層にデータをプロアクティブに昇格できます tiering-policy および cloud-retrieval-policy 設定：

## このタスクについて

この処理は、ボリュームでFabricPool の使用を停止する場合やを使用している場合に実行します snapshot-only 階層化ポリシーを使用していて、リストアされたSnapshotコピーのデータを高パフォーマンス階層に戻したいと考えています。

**FabricPool** ボリュームのすべてのデータを高パフォーマンス階層に昇格します

クラウド内の FabricPool ボリューム上のすべてのデータをプロアクティブに読み出し、高パフォーマンス階層に昇格できます。

### ステップ

1. を使用します volume modify 設定するコマンド tiering-policy 終了： none および cloud-retrieval-policy 終了： promote。

```
volume modify -vserver <vserver-name> -volume <volume-name> -tiering  
-policy none -cloud-retrieval-policy promote
```

ファイルシステムのデータを高パフォーマンス階層に昇格

クラウド階層内のリストア済み Snapshot コピーからアクティブなファイルシステムデータをプロアクティブに読み出し、パフォーマンス階層に昇格できます。

### ステップ

1. を使用します volume modify 設定するコマンド tiering-policy 終了： snapshot-only および cloud-retrieval-policy 終了： promote。

```
volume modify -vserver <vserver-name> -volume <volume-name> -tiering  
-policy snapshot-only cloud-retrieval-policy promote
```

パフォーマンス階層の昇格のステータスを確認します

パフォーマンス階層の昇格のステータスを確認することで、処理が完了したかどうかを判断できます。

### ステップ

1. ボリュームを使用します object-store コマンドにを指定します tiering 高パフォーマンス階層への昇格のステータスを確認するオプションです。

```

volume object-store tiering show [ -instance | -fields <fieldname>, ...
] [ -vserver <vserver name> ] *Vserver
[[-volume] <volume name>] *Volume [ -node <nodename> ] *Node Name [ -vol
-dsid <integer> ] *Volume DSID
[ -aggregate <aggregate name> ] *Aggregate Name

```

```

volume object-store tiering show v1 -instance

Vserver: vs1
Volume: v1
Node Name: node1
Volume DSID: 1023
Aggregate Name: a1
State: ready
Previous Run Status: completed
Aborted Exception Status: -
Time Scanner Last Finished: Mon Jan 13 20:27:30 2020
Scanner Percent Complete: -
Scanner Current VBN: -
Scanner Max VBNs: -
Time Waiting Scan will be scheduled: -
Tiering Policy: snapshot-only
Estimated Space Needed for Promotion: -
Time Scan Started: -
Estimated Time Remaining for scan to complete: -
Cloud Retrieve Policy: promote

```

移行と階層化のスケジュール設定を開始

ONTAP 9.8以降では、デフォルトの階層化スキャンを待たずにいつでも階層化スキャン要求をトリガーできます。

#### ステップ

1. を使用します volume object-store コマンドにを指定します trigger 移行と階層化を申請するオプションがあります。

```

volume object-store tiering trigger [ -vserver <vserver name> ] *VServer
Name [-volume] <volume name> *Volume Name

```

## FabricPool ミラーを管理します



## Manage FabricPool mirrors の概要

災害発生時もデータストア内のデータへのアクセスを継続したり、データストアを交換したりできるように、2 つ目のデータストアを追加して FabricPool ミラーを構成し、2 つのデータストアにデータを同期的に階層化することができます。新規または既存の FabricPool 構成に 2 つ目のデータストアを追加したり、ミラーステータスを監視したり、FabricPool ミラーの詳細を表示したり、ミラーを昇格させたり、ミラーを削除したりできます。ONTAP 9.7以降が実行されている必要があります。

### FabricPool ミラーを作成します

FabricPool ミラーを作成するには、2 つのオブジェクトストアを 1 つの FabricPool に接続します。FabricPool ミラーを作成するには、既存の単一のオブジェクトストア FabricPool 構成に 2 つ目のオブジェクトストアを接続するか、新しい単一のオブジェクトストア FabricPool 構成を作成してから 2 つ目のオブジェクトストアを接続します。MetroCluster 構成上に FabricPool ミラーを作成することもできます。

#### 必要なもの

- を使用して2つのオブジェクトストアを作成しておく必要があります `storage aggregate object-store config` コマンドを実行します
- MetroCluster 構成上に FabricPool ミラーを作成する場合の要件は次のとおりです。
  - MetroCluster のセットアップと設定が完了している必要があります
  - 選択したクラスタにオブジェクトストア設定を作成しておく必要があります。

MetroCluster 構成の両方のクラスタに FabricPool ミラーを作成する場合は、両方のクラスタにオブジェクトストア設定を作成しておく必要があります。

- MetroCluster 構成にオンプレミスのオブジェクトストアを使用しない場合は、次のいずれかのシナリオに該当する必要があります。
  - オブジェクトストアは異なるアベイラビリティゾーンにあります
  - オブジェクトストアは、複数のアベイラビリティゾーンにオブジェクトのコピーを保持するように設定されます

#### "MetroCluster 構成での FabricPool 用オブジェクトストアのセットアップ"

#### このタスクについて

FabricPool ミラーには、プライマリオブジェクトストアとは別のオブジェクトストアを使用する必要があります。

FabricPool ミラーを作成する手順は、MetroCluster 構成と MetroCluster 以外の構成で同じです。

#### 手順

1. 既存の FabricPool 構成を使用しない場合は、を使用してオブジェクトストアをアグリゲートに接続して新しい構成を作成します `storage aggregate object-store attach` コマンドを実行します

この例では、オブジェクトストアをアグリゲートに接続して新しい FabricPool を作成します。

```
cluster1::> storage aggregate object-store attach -aggregate aggr1 -name my-store-1
```

2. を使用して、2つ目のオブジェクトストアをアグリゲートに接続します `storage aggregate object-store mirror` コマンドを実行します

この例では、2つ目のオブジェクトストアをアグリゲートに接続して FabricPool ミラーを作成します。

```
cluster1::> storage aggregate object-store mirror -aggregate aggr1 -name my-store-2
```

### FabricPool ミラー再同期ステータスを監視します

プライマリオブジェクトストアをミラーに置き換える場合、必要に応じてミラーがプライマリデータストアと再同期されるまで待つ必要があります。

このタスクについて

FabricPool ミラーが同期されている場合はエントリは表示されません。

#### ステップ

1. を使用して、ミラー再同期ステータスを監視します `storage aggregate object-store show-resync-status` コマンドを実行します

```
aggregate1::> storage aggregate object-store show-resync-status -aggregate aggr1
```

Aggregate	Primary	Mirror	Complete Percentage
aggr1	my-store-1	my-store-2	40%

### FabricPool ミラーの詳細を表示します

FabricPool ミラーの詳細を表示して、設定に含まれているオブジェクトストアや、オブジェクトストアミラーがプライマリオブジェクトストアと同期されているかどうかを確認できます。

#### ステップ

1. を使用して、FabricPool ミラーに関する情報を表示します `storage aggregate object-store show` コマンドを実行します

次の例は、FabricPool ミラーのプライマリオブジェクトストアとミラーオブジェクトストアの詳細を表示

します。

```
cluster1::> storage aggregate object-store show
```

Aggregate	Object Store Name	Availability	Mirror Type
aggr1	my-store-1	available	primary
	my-store-2	available	mirror

次の例は、再同期処理によってミラーがデグレード状態になっているかどうかを含む、FabricPool ミラーに関する詳細を表示します。

```
cluster1::> storage aggregate object-store show -fields mirror-type,is-mirror-degraded
```

aggregate	object-store-name	mirror-type	is-mirror-degraded
aggr1	my-store-1	primary	-
	my-store-2	mirror	false

## FabricPool ミラーをプロモートします

オブジェクトストアミラーを昇格してプライマリオブジェクトストアとして再割り当てすることができます。オブジェクトストアミラーがプライマリになると、元のプライマリは自動的にミラーになります。

### 必要なもの

- FabricPool ミラーが同期されている必要があります
- オブジェクトストアが動作している必要があります

### このタスクについて

元のオブジェクトストアを別のクラウドプロバイダのオブジェクトストアに置き換えることができます。たとえば、元のミラーが AWS オブジェクトストアである場合に Azure オブジェクトストアに置き換えることができます。

### ステップ

1. を使用して、オブジェクトストアミラーを昇格します `storage aggregate object-store modify -aggregate` コマンドを実行します

```
cluster1::> storage aggregate object-store modify -aggregate aggr1 -name  
my-store-2 -mirror-type primary
```

### FabricPool ミラーを削除します

オブジェクトストアをレプリケートする必要がなくなった場合は、FabricPool ミラーを削除できます。

#### 必要なもの

プライマリオブジェクトストアが動作している必要があります。動作していないとコマンドは失敗します。

#### ステップ

1. を使用して、FabricPool のオブジェクトストアミラーを削除します `storage aggregate object-store unmirror -aggregate` コマンドを実行します

```
cluster1::> storage aggregate object-store unmirror -aggregate aggr1
```

### FabricPool ミラーを使用して既存のオブジェクトストアを置き換えます

FabricPool ミラーテクノロジーを使用して、あるオブジェクトストアを別のオブジェクトストアに置き換えることができます。新しいオブジェクトストアは、元のオブジェクトストアと同じクラウドプロバイダを使用する必要はありません。

#### このタスクについて

元のオブジェクトストアを、別のクラウドプロバイダを使用するオブジェクトストアに置き換えることができます。たとえば、AWS をクラウドプロバイダとして使用しているオブジェクトストアが Azure を使用するオブジェクトストアに置き換えることも、その逆も可能です。ただし、オブジェクトサイズは新しいオブジェクトストアと元のオブジェクトストアで同じである必要があります。

#### 手順

1. を使用して既存のFabricPool に新しいオブジェクトストアを追加し、FabricPool ミラーを作成します `storage aggregate object-store mirror` コマンドを実行します

```
cluster1::> storage aggregate object-store mirror -aggregate aggr1 -name  
my-AZURE-store
```

2. を使用して、ミラー再同期ステータスを監視します `storage aggregate object-store show-resync-status` コマンドを実行します

```
cluster1::> storage aggregate object-store show-resync-status -aggregate  
aggr1
```

Aggregate	Primary	Mirror	Complete Percentage
-----	-----	-----	-----
aggr1	my-AWS-store	my-AZURE-store	40%

3. を使用して、ミラーが同期されていることを確認します `storage aggregate object-store> show -fields mirror-type,is-mirror-degraded` コマンドを実行します

```
cluster1::> storage aggregate object-store show -fields mirror-type,is-
mirror-degraded
```

aggregate	object-store-name	mirror-type	is-mirror-degraded
-----	-----	-----	-----
aggr1	my-AWS-store	primary	-
	my-AZURE-store	mirror	false

4. を使用して、プライマリオブジェクトストアをミラーオブジェクトストアとスワップします `storage aggregate object-store modify` コマンドを実行します

```
cluster1::> storage aggregate object-store modify -aggregate aggr1 -name
my-AZURE-store -mirror-type primary
```

5. を使用して、FabricPool ミラーに関する詳細を表示します `storage aggregate object-store show -fields mirror-type,is-mirror-degraded` コマンドを実行します

この例は、FabricPool ミラーに関する情報を表示したもので、ミラーがデグレード状態（同期されていない状態）になっているのかも含まれます。

```
cluster1::> storage aggregate object-store show -fields mirror-type, is-
mirror-degraded
```

aggregate	object-store-name	mirror-type	is-mirror-degraded
-----	-----	-----	-----
aggr1	my-AZURE-store	primary	-
	my-AWS-store	mirror	false

6. を使用してFabricPool ミラーを取り外します `storage aggregate object-store unmirror` コマンドを実行します

```
cluster1::> storage aggregate object-store unmirror -aggregate aggr1
```

7. を使用して、FabricPool が単一オブジェクトストア設定に戻ったことを確認します `storage aggregate object-store show -fields mirror-type,is-mirror-degraded` コマンドを実行します

```
cluster1::> storage aggregate object-store show -fields mirror-type,is-mirror-degraded
```

aggregate	object-store-name	mirror-type	is-mirror-degraded
aggr1	my-AZURE-store	primary	-

### MetroCluster 構成の FabricPool ミラーを交換します

MetroCluster ミラーのオブジェクトストアの 1 つが破棄された場合、または FabricPool 構成で完全に使用できなくなった場合、オブジェクトストアがまだミラーでない場合はミラーにして、破損したオブジェクトストアを FabricPool ミラーから削除します。次に、新しいオブジェクトストアミラーを FabricPool に追加します。

#### 手順

1. 破損したオブジェクトストアがまだミラーでない場合は、オブジェクトストアをを使用してミラーにします `storage aggregate object-store modify` コマンドを実行します

```
storage aggregate object-store modify -aggregate -aggregate fp_aggr1_A01 -name mccl_ostore1 -mirror-type mirror
```

2. を使用して、FabricPool からオブジェクトストアミラーを削除します `storage aggregate object-store unmirror` コマンドを実行します

```
storage aggregate object-store unmirror -aggregate <aggregate name> -name mccl_ostore1
```

3. を使用して、ミラーデータストアを削除したあとにプライマリデータストアで階層化を強制的に再開できます `storage aggregate object-store modify` を使用 `-force-tiering-on-metrocluster true` オプション

ミラーがないと、MetroCluster 構成のレプリケーション要件が満たされません。

```
storage aggregate object-store modify -aggregate <aggregate name> -name
mcc1_ostore1 -force-tiering-on-metrocluster true
```

4. を使用して、置き換え用のオブジェクトストアを作成します storage aggregate object-store config create コマンドを実行します

```
storage aggregate object-store config create -object-store-name
mcc1_ostore3 -cluster clusterA -provider-type SGWS -server <SGWS-server-
1> -container-name <SGWS-bucket-1> -access-key <key> -secret-password
<password> -encrypt <true|false> -provider <provider-type> -is-ssl
-enabled <true|false> ipspace <IPSpace>
```

5. を使用して、FabricPool ミラーにオブジェクトストアミラーを追加します storage aggregate object-store mirror コマンドを実行します

```
storage aggregate object-store mirror -aggregate aggr1 -name
mcc1_ostore3-mc
```

6. を使用してオブジェクトストアの情報を表示します storage aggregate object-store show コマンドを実行します

```
storage aggregate object-store show -fields mirror-type,is-mirror-
degraded
```

aggregate	object-store-name	mirror-type	is-mirror-degraded
aggr1	mcc1_ostore1-mc	primary	-
	mcc1_ostore3-mc	mirror	true

7. を使用して、ミラー再同期ステータスを監視します storage aggregate object-store show-resync-status コマンドを実行します

```
storage aggregate object-store show-resync-status -aggregate aggr1
```

Aggregate	Primary	Mirror	Complete Percentage
aggr1	mcc1_ostore1-mc	mcc1_ostore3-mc	40%

## FabricPool を使用したアグリゲートの管理用コマンド

を使用します storage aggregate object-store FabricPool のオブジェクトストアを管理するコマンド。を使用します storage aggregate FabricPool のアグリゲートを管理するためのコマンド。を使用します volume FabricPool 用のボリュームを管理するコマンドです。

状況	使用するコマンド
オブジェクトストアの設定を定義して、ONTAP からアクセスできるようにします	<code>storage aggregate object-store config create</code>
オブジェクトストア設定の属性を変更する	<code>storage aggregate object-store config modify</code>
既存のオブジェクトストア設定の名前を変更する	<code>storage aggregate object-store config rename</code>
オブジェクトストアの設定を削除する	<code>storage aggregate object-store config delete</code>
オブジェクトストア設定のリストを表示します	<code>storage aggregate object-store config show</code>
新規または既存の FabricPool にミラーとして 2 つ目のオブジェクトストアを接続します	<code>storage aggregate object-store mirror</code> を使用 <code>-aggregate</code> および <code>-name</code> パラメータを指定します
既存の FabricPool ミラーからオブジェクトストアミラーを削除する	<code>storage aggregate object-store unmirror</code> を使用 <code>-aggregate</code> および <code>-name</code> パラメータを指定します
FabricPool ミラー再同期ステータスを監視します	<code>storage aggregate object-store show-resync-status</code>
FabricPool ミラーの詳細を表示します	<code>storage aggregate object-store show</code>
FabricPool ミラー構成でオブジェクトストアミラーを昇格してプライマリオブジェクトストアを置き換えます	<code>storage aggregate object-store modify</code> を使用 <code>-aggregate</code> パラメータを指定します
オブジェクトストアをアグリゲートに接続せずにオブジェクトストアのレイテンシとパフォーマンスをテストする	<code>storage aggregate object-store profiler start</code> を使用 <code>-object-store-name</code> および <code>-node</code> パラメータを <code>advanced</code> 権限レベルで指定します



オブジェクトストアプロファイラのステータスを監視する	<code>storage aggregate object-store profiler show</code> を使用 <code>-object-store-name</code> および <code>-node</code> パラメータをadvanced権限レベルで指定します
実行中のオブジェクトストアプロファイラを中止します	<code>storage aggregate object-store profiler abort</code> を使用 <code>-object-store-name</code> および <code>-node</code> パラメータをadvanced権限レベルで指定します
FabricPool を使用するために、オブジェクトストアをアグリゲートに接続します	<code>storage aggregate object-store attach</code>
FabricPool を使用するために、FlexGroup ボリュームを含むアグリゲートにオブジェクトストアを接続します	<code>storage aggregate object-store attach</code> を使用 <code>allow-flexgroup true</code>
FabricPool 対応アグリゲートに接続されているオブジェクトストアの詳細を表示します	<code>storage aggregate object-store show</code>
階層化スキャンで使用するアグリゲートのスペース不足しきい値を表示します	<code>storage aggregate object-store show</code> を使用 <code>-fields tiering-fullness-threshold</code> パラメータをadvanced権限レベルで指定します
FabricPool 対応アグリゲートに接続されているオブジェクトストアのスペース使用量を表示します	<code>storage aggregate object-store show-space</code>
FabricPool で使用されていないアグリゲートで Inactive Data Reporting を有効にする	<code>storage aggregate modify</code> を使用 <code>-is -inactive-data-reporting-enabled true</code> パラメータ
アグリゲートでアクセス頻度の低いデータのレポートが有効になっているかどうかを表示する	<code>storage aggregate show</code> を使用 <code>-fields is-inactive-data-reporting-enabled</code> パラメータ
アグリゲート内のコールドユーザデータの量に関する情報を表示します	<code>storage aggregate show-space</code> を使用 <code>-fields performance-tier-inactive-user-data,performance-tier-inactive-user-data-percent</code> パラメータ
次の項目を指定して、FabricPool 用のボリュームを作成します。  <ul style="list-style-type: none"> <li>階層化ポリシー</li> <li>階層化の最小クーリング期間（の <code>snapshot-only</code> または <code>auto</code> 階層化ポリシー）</li> </ul>	<code>volume create</code>  <ul style="list-style-type: none"> <li>を使用します <code>-tiering-policy</code> 階層化ポリシーを指定するパラメータ。</li> <li>を使用します <code>-tiering-minimum-cooling-days</code> 階層化の最小クーリング期間を指定するためのパラメータをadvanced権限レベルで指定します。</li> </ul>

<p>FabricPool のボリュームを変更し、以下を変更する</p> <ul style="list-style-type: none"> <li>・階層化ポリシー</li> <li>・階層化の最小クーリング期間（の snapshot-only または auto 階層化ポリシー）</li> </ul>	<p>volume modify</p> <ul style="list-style-type: none"> <li>・を使用します <code>-tiering-policy</code> 階層化ポリシーを指定するパラメータ。</li> <li>・を使用します <code>-tiering-minimum-cooling-days</code> 階層化の最小クーリング期間を指定するためのパラメータをadvanced権限レベルで指定します。</li> </ul>
<p>次のような、ボリュームに関連する FabricPool 情報を表示する</p> <ul style="list-style-type: none"> <li>・階層化の最小クーリング期間</li> <li>・コールドユーザデータの量</li> </ul>	<p>volume show</p> <ul style="list-style-type: none"> <li>・を使用します <code>-fields tiering-minimum-cooling-days</code> 階層化の最小クーリング期間を表示するためのadvanced権限レベルのパラメータ。</li> <li>・を使用します <code>-fields performance-tier-inactive-user-data,performance-tier-inactive-user-data-percent</code> コールドユーザデータの量を表示するパラメータ。</li> </ul>
<p>ボリュームを FabricPool の内外に移動します</p>	<p>volume move start を使用します <code>-tiering-policy</code> ボリュームの階層化ポリシーを指定するオプションのパラメータ。</p>
<p>FabricPool で参照されていないスペースを再生するしきい値（デフラグしきい値）を変更します</p>	<p>storage aggregate object-store modify を使用 <code>-unreclaimed-space-threshold</code> パラメータをadvanced権限レベルで指定します</p>
<p>階層化スキャンで FabricPool のデータ階層化を開始する前に、アグリゲートの使用率のしきい値を変更します</p> <p>FabricPool は、ローカル階層の容量が 98% に達するまで、コールドデータをクラウド階層に階層化し続けます。</p>	<p>storage aggregate object-store modify を使用 <code>-tiering-fullness-threshold</code> パラメータをadvanced権限レベルで指定します</p>
<p>FabricPool で参照されていないスペースを再生するしきい値を表示します</p>	<p>storage aggregate object-store show または storage aggregate object-store show-space コマンドにを指定します <code>-unreclaimed-space-threshold</code> パラメータをadvanced権限レベルで指定します</p>

## SVM のデータ移動

### SVM のデータ移動の概要

ONTAP 9.10.1以降では、ONTAP CLIを使用して、容量とロードバランシングを管理した

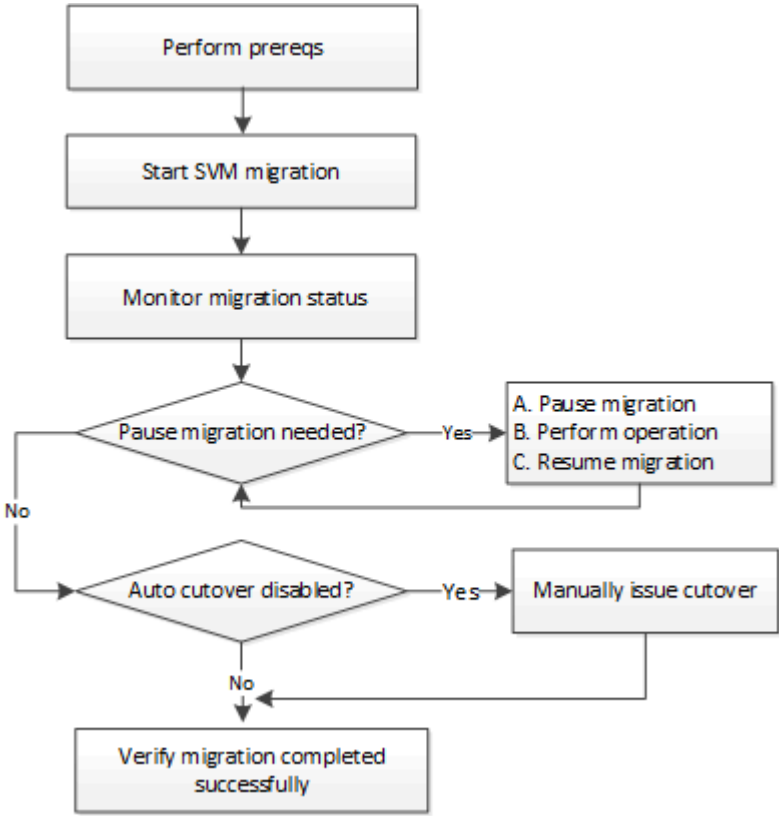
り、機器のアップグレードやデータセンターの統合を有効にしたりするために、システムを停止することなくSVMをソースクラスタからデスティネーションクラスタに再配置できます。

この無停止のSVM再配置機能は、ONTAP 9.10.1および9.11.1のAFFプラットフォームでサポートされます。ONTAP 9.12.1以降では、この機能はFASプラットフォームとAFFプラットフォームの両方、およびハイブリッドアグリゲートでサポートされます。

SVM の名前と UUID は、移行後も変更されず、データ LIF 名、IP アドレス、ボリューム名などのオブジェクト名も変更されません。SVM 内のオブジェクトの UUID は異なります。

SVM 移行ワークフロー

次の図は、SVM 移行の一般的なワークフローを示しています。SVM の移行はデスティネーションクラスタから開始します。移行元または移行先のどちらからでも移行を監視できます。手動カットオーバーまたは自動カットオーバーを実行できます。自動カットオーバーはデフォルトで実行されます。



SVM移行プラットフォームのサポート

コントローラファミリー	サポートされるONTAPのバージョン
AFF Aシリーズ	ONTAP 9.10.1 以降
AFF Cシリーズ	ONTAP 9.12.1パッチ4以降
FAS	ONTAP 9.12.1以降



AFF クラスタからハイブリッドアグリゲートを使用するFAS クラスタに移行する場合、ボリュームの自動配置で同様のアグリゲートの一致が試行されます。たとえば、ソースクラスタにボリュームが60個ある場合、ボリュームの配置では、ボリュームを配置するデスティネーションにAFF アグリゲートが検索されます。AFFアグリゲートに十分なスペースがない場合、ボリュームはフラッシュディスク以外のアグリゲートに配置されます。

## ONTAPのバージョンによる拡張性のサポート

ONTAPバージョン	ソースとデスティネーションのHAペア
ONTAP 9.14.1	12
ONTAP 9.13.1	6.
ONTAP 9.11.1	3.
ONTAP 9.10.1	1.

ソースクラスタとデスティネーションクラスタ間の**TCP**ラウンドトリップタイム（**RTT**）に関するネットワークインフラのパフォーマンス要件

クラスタにインストールされているONTAPのバージョンに応じて、ソースクラスタとデスティネーションクラスタを接続するネットワークの最大応答時間を次に示します。

ONTAPバージョン	最大RTT
ONTAP 9.12.1以降	10ミリ秒
ONTAP 9.11.1以前	2ミリ秒

## SVMあたりのサポートされる最大ボリューム数

ソース	デスティネーション	ONTAP 9.14.1	ONTAP 9.13.1	ONTAP 9.12.1	ONTAP 9.11.1以前
AFF	AFF	400	200	100	100
FAS	FAS	80	80	80	N/A
FAS	AFF	80	80	80	N/A
AFF	FAS	80	80	80	N/A

## 前提条件

SVMの移行を開始する前に、次の前提条件を満たしている必要があります。

- クラスタ管理者である必要があります。
- **"ソースクラスタとデスティネーションクラスタが相互にピア関係にある必要があります"**。
- ソースクラスタとデスティネーションクラスタでSnapMirror同期が確立されている必要があります。 **"インストールされたライセンス"**。このライセンスは、 **"ONTAP One"**。
- ソースクラスタのすべてのノードでONTAP 9.10.1以降が実行されている必要があります。特定のONTAP アレイコントローラのサポートについては、を参照してください **"Hardware Universe"**。

- ソースクラスタ内のすべてのノードで同じバージョンのONTAPが実行されている必要があります。
- デスティネーションクラスタ内のすべてのノードで同じバージョンのONTAPが実行されている必要があります。
- デスティネーションクラスタは、ソースクラスタと同じかそれよりも新しいメジャーなEffective Cluster Version (ECV；有効なクラスタバージョン) が2つ以下である必要があります。
- ソースクラスタとデスティネーションクラスタで、データLIFへのアクセス用に同じIPサブネットがサポートされている必要があります。
- ソースSVMに含まれているボリュームの数がよりも少ない必要があります [このリリースでサポートされるデータボリュームの最大数](#)。
- デスティネーションにボリューム配置用の十分なスペースが必要です
- ソース SVM に暗号化されたボリュームがある場合は、デスティネーションでオンボードキーマネージャを設定する必要があります

## ベストプラクティス

SVM移行を実行するときは、CPUワークロードが実行されるように、ソースクラスタとデスティネーションクラスタの両方にCPUヘッドルームを30%確保しておくことを推奨します。

## SVM処理

SVM の移行と競合する可能性がある処理がないかどうかを確認する必要があります。

- 実行中のフェイルオーバー処理はありません
- wafliron を実行できない
- フィンガープリントを実行中ではありません
- vol move 、 rehost 、 clone 、 create 、 convert 、または analytics が実行されていません

## サポートされる機能とサポートされない機能

次の表に、SVMデータ移動とONTAPリリースでサポートされるONTAP機能を示します。

フィーチャー（Feature）	最初にサポートされたリリース	コメント
自律的なランサムウェア防御	ONTAP 9.12.1	
Cloud Volumes ONTAP	サポート対象外	
外部キー管理ツール	ONTAP 9.11.1	
FabricPool	ONTAP 9.11.1	の詳細を確認してください <a href="#">FabricPoolのサポート</a> 。
ファンアウト関係（移行するソースにSnapMirrorソースボリュームと複数のデスティネーションがある）	ONTAP 9.11.1	

FC SAN	サポート対象外	
Flash Pool の機能です	ONTAP 9.12.1	
FlexCache ボリューム	サポート対象外	
FlexGroup	サポート対象外	
IPSecポリシー	サポート対象外	
IPv6 LIF	サポート対象外	
iSCSI SAN	サポート対象外	
ジョブスケジュールのレプリケーション	ONTAP 9.11.1	ONTAP 9.10.1では、移行時にジョブスケジュールがレプリケートされないため、デスティネーションで手動で作成する必要があります。ONTAP 9.11.1以降では、ソースで使用されているジョブスケジュールが移行時に自動的にレプリケートされます。
負荷共有ミラー	サポート対象外	
MetroCluster SVM	サポート対象外	SVMの移行ではMetroCluster SVMの移行がサポートされませんが、にSnapMirror非同期レプリケーションを使用できる場合があります <a href="#">"MetroCluster構成のSVMを移行する"</a> 。MetroCluster構成でSVMを移行する手順は、無停止方式である_not_aであることに注意してください。
NetApp Aggregate Encryption （ NAE ）	サポート対象外	暗号化されていないソースから暗号化されたデスティネーションへの移行はサポートされていません。
NDMP構成	サポート対象外	
NetApp Volume Encryption （ NVE ）	ONTAP 9.10.1	

NFSおよびSMB監査ログ	ONTAP 9.13.1	 <p>監査ログリダイレクトは、クラウドモードでのみ使用できます。監査を有効にしたオンプレミスのSVM移行の場合は、ソースSVMで監査を無効にしてから移行を実行する必要があります。</p> <p>SVM移行前：</p> <ul style="list-style-type: none"> <li>• "デスティネーションクラスタで監査ログリダイレクトを有効にする必要がある"。</li> <li>• "ソースSVMからの監査ログデスティネーションパスがデスティネーションクラスタに作成されている必要があります"。</li> </ul>
NFS v3、NFS v4.1、NFS v4.2	ONTAP 9.10.1	
NFS v4.0	ONTAP 9.12.1	
pNFSを使用したNFSv4.1	ONTAP 9.14.1	
NVMe over Fabric	サポート対象外	
ソースクラスタでCommon Criteriaモードを有効にしたオンボードキーマネージャ（OKM）	サポート対象外	
qtree	ONTAP 9.14.1	
クォータ	ONTAP 9.14.1	
S3	サポート対象外	
SMBプロトコル	ONTAP 9.12.1	SMBの移行にはシステムの停止が伴い、移行後にクライアントの更新が必要になります。
SnapMirrorCloudカンケイ	ONTAP 9.12.1	ONTAP 9.12.1以降では、SnapMirror Cloud関係が設定されたSVMを移行する場合、デスティネーションクラスタに " <a href="#">SnapMirror Cloud ライセンス</a> " をインストールし、クラウドにミラーリングするボリューム内の容量を移動するための十分な容量が必要です。
SnapMirror非同期デスティネーション	ONTAP 9.12.1	

SnapMirrorヒトウキソオス	ONTAP 9.11.1	<ul style="list-style-type: none"> <li>ほとんどのマイグレーション中、FlexVol SnapMirror関係では転送は通常どおり続行できます。</li> <li>実行中の転送はカットオーバー中にキャンセルされ、カットオーバー中に新しい転送は失敗します。移行が完了するまで再開できません。</li> <li>移行中にキャンセルされた、または実行されなかったスケジュールされた転送は、移行完了後に自動的に開始されません。</li> </ul> <div>  <p>SnapMirrorソースをマイグレートする場合、ONTAPでは、SnapMirror更新が実行されるまで、移行後のボリュームの削除は禁止されません。これは、移動されたSnapMirrorソースボリュームのSnapMirror関連情報を使用できるのは、移動が完了して最初の更新が実行されたあとに限られるためです。</p> </div>
SMTape設定	サポート対象外	
SnapLock	サポート対象外	
SnapMirror によるビジネス継続性	サポート対象外	
SnapMirror SVMピア関係	ONTAP 9.12.1	
SnapMirror SVMディザスタリカバリ	サポート対象外	
SnapMirror Synchronous	サポート対象外	
Snapshot コピー	ONTAP 9.10.1	
タンパープルーフスナップショットコピーロック	ONTAP 9.14.1	改ざん防止機能を備えたSnapshotコピーロックは、SnapLockとは異なります。SnapLockはサポートされません。
仮想IP LIF / BGP	サポート対象外	
Virtual Storage Console 7.0以降	サポート対象外	VSCには含まれています <a href="#">"ONTAP Tools for VMware vSphere 仮想アプライアンス"</a> VSC 7.0以降
ボリュームクローン	サポート対象外	



vStorageの略	サポート対象外	
------------	---------	--

## FabricPoolのサポート

SVMの移行は、FabricPoolのボリュームで次のプラットフォームでサポートされます。

- Azure NetApp Filesプラットフォーム。すべての階層化ポリシーがサポートされます（snapshot-only、auto、all、none）。
- オンプレミスプラットフォーム：サポートされるボリューム階層化ポリシーは「none」のみです。

## 移行中にサポートされる処理

次の表に、移動中のSVMでサポートされるボリューム処理を、移動状態に基づいて示します。

ボリューム操作	SVMの移行状態		
	* 実行中 *	一時停止	* カットオーバー *
作成	許可されません	許可されます	サポート対象外
削除	許可されません	許可されます	サポート対象外
ファイルシステム分析の無効化	許可されます	許可されます	サポート対象外
ファイルシステム分析の有効化	許可されません	許可されます	サポート対象外
変更	許可されます	許可されます	サポート対象外
オフライン/オンライン	許可されません	許可されます	サポート対象外
移動/リホスト	許可されません	許可されます	サポート対象外
qtreeの作成/変更	許可されません	許可されます	サポート対象外
クォータの作成/変更	許可されません	許可されます	サポート対象外
名前を変更する	許可されません	許可されます	サポート対象外
サイズ変更	許可されます	許可されます	サポート対象外
制限	許可されません	許可されます	サポート対象外
Snapshotコピーの属性が変更されました	許可されます	許可されます	サポート対象外
Snapshotコピー自動削除の変更	許可されます	許可されます	サポート対象外
Snapshotコピーの作成	許可されます	許可されます	サポート対象外
Snapshotコピーの削除	許可されます	許可されます	サポート対象外
Snapshotコピーからファイルをリストアします	許可されます	許可されます	サポート対象外

## SVM を移行する

SVM の移行が完了すると、クライアントがデスティネーションクラスタに自動的にカットオーバーされ、不要な SVM がソースクラスタから削除されます。自動カットオーバー

ーとソースの自動クリーンアップはデフォルトで有効になっています。必要に応じて、カットオーバーの発生前にクライアントの自動カットオーバーを無効にして移行を一時停止することもできます。また、ソース SVM の自動クリーンアップを無効にすることもできます。

- 使用できます `-auto-cutover false` クライアントの自動カットオーバーが通常発生したときに移動を一時停止し、あとで手動でカットオーバーを実行するオプションです。

#### SVM 移行後にクライアントを手動でカットオーバーする

- `advanced`権限を使用できます `-auto-source-cleanup false` カットオーバー後にソースSVMの削除を無効にし、カットオーバー後にソースのクリーンアップを手動で開始するオプション。

#### カットオーバー後にソース SVM を手動で削除

自動カットオーバーを有効にして **SVM** を移行します

デフォルトでは、移行の完了時にクライアントがデスティネーションクラスタに自動的にカットオーバーされ、不要な SVM がソースクラスタから削除されます。

手順

1. デスティネーションクラスタから、移行の事前確認を実行します。

```
dest_cluster> vservers migrate start -vservers SVM_name -source-cluster cluster_name -check-only true
```

2. デスティネーションクラスタから、SVM 移行を開始します。

```
dest_cluster> vservers migrate start -vservers SVM_name -source-cluster cluster_name
```

3. 移行ステータスを確認します。

```
dest_cluster> vservers migrate show
```

SVM の移行が完了すると、ステータスに「`migrate-complete`」と表示されます。

クライアントの自動カットオーバーを無効にして **SVM** を移行します

自動クライアントカットオーバーが正常に実行されたときに移行を一時停止してから、あとから手動でカットオーバーを実行するには、`-auto-cutover false` オプションを使用します。を参照してください [SVM 移行後にクライアントを手動でカットオーバーする](#)。

手順

1. デスティネーションクラスタから、移行の事前確認を実行します。

```
dest_cluster> vservers migrate start -vservers SVM_name -source-cluster cluster_name -check-only true
```

2. デスティネーションクラスタから、SVM 移行を開始します。

```
dest_cluster> vservers migrate start -vservers SVM_name -source-cluster
cluster_name -auto-cutover false
```

### 3. 移行ステータスを確認します。

```
dest_cluster> vservers migrate show
```

SVM 移行が非同期データ転送を完了し、カットオーバー処理の準備が完了した時点で、ステータスには「カットオーバー準備完了」と表示されます。

ソースのクリーンアップが無効になっている **SVM** を移行します

カットオーバー後にソース SVM の削除を無効にしてから、カットオーバー後にソースのクリーンアップを手動でトリガーするには、advanced 権限の `-auto-giveback false` オプションを使用します。を参照してください [ソース SVM を手動で削除します](#)。

#### 手順

##### 1. デスティネーションクラスタから、移行の事前確認を実行します。

```
dest_cluster*> vservers migrate start -vservers SVM_name -source-cluster
cluster_name -check-only true
```

##### 2. デスティネーションクラスタから、SVM 移行を開始します。

```
dest_cluster*> vservers migrate start -vservers SVM_name -source-cluster
cluster_name -auto-source-cleanup false
```

##### 3. 移行ステータスを確認します。

```
dest_cluster*> vservers migrate show
```

SVM 移行のカットオーバーが完了し、ソースクラスタの SVM を削除する準備ができている場合は、ステータスに「ready for -source-cleanup」と表示されます。

## ボリュームの移行を監視

を使用してSVMの移行全体を監視することに加えて `vservers migrate show` コマンドを入力すると、SVMに含まれるボリュームの移行ステータスを監視できます。

#### 手順

##### 1. ボリュームの移行ステータスを確認します。

```
dest_clust> vservers migrate show-volume
```

## SVM 移行を一時停止して再開します

移行のカットオーバーを開始する前に、SVM 移行を一時停止することができます。を使用してSVMの移行を一時停止できます `vservers migrate pause` コマンドを実行します

## 移行を一時停止

を使用すると、クライアントのカットオーバーを開始する前にSVMの移行を一時停止できます `vserver migrate pause` コマンドを実行します

移行処理の実行中は、一部の設定変更が制限されます。ただし、ONTAP 9.12.1以降では、移行を一時停止して制限された設定や一部の失敗した状態を修正することで、障害の原因となった可能性のある設定の問題を修正できます。SVMの移行を一時停止するときに解決できる失敗状態には、次のようなものがあります。

- `setup-configuration - failed` (セットアップ-設定-失敗)
- `migrate -失敗しました`

## 手順

1. デスティネーションクラスタから、移行を一時停止します。

```
dest_cluster> vserver migrate pause -vserver <vserver name>
```

## 移行を再開

一時停止したSVMの移行を再開する準備ができたなら、またはSVMの移行が失敗した場合は、を使用できます `vserver migrate resume` コマンドを実行します

## ステップ

1. SVM の移行を再開します。

```
dest_cluster> vserver migrate resume
```

2. SVM の移行が再開されたことを確認し、進捗状況を監視します。

```
dest_cluster> vserver migrate show
```

## SVM の移行をキャンセルします

SVMの移行を完了前にキャンセルする必要がある場合は、を使用できます `vserver migrate abort` コマンドを実行しますSVM の移行は、処理が `PAUSED` または `FAILED` 状態のときにのみキャンセルできます。SVM の移行は、ステータスが「カットオーバー開始」のときやカットオーバーが完了したあとはキャンセルできません。を使用することはできません `abort` オプションは、SVMの移行が進行中の場合に表示されます。

## 手順

1. 移行ステータスを確認します。

```
dest_cluster> vserver migrate show -vserver <vserver name>
```

2. 移行をキャンセルします。

```
dest_cluster> vserver migrate abort -vserver <vserver name>
```

3. キャンセル処理の進捗を確認します。

```
dest_cluster> vsserver migrate show
```

キャンセル処理の実行中は、移行ステータスにmigrate-abortingと表示されます。キャンセル処理が完了すると、移行ステータスには何も表示されません。

## 手動でクライアントをカットオーバーします

デフォルトでは、SVM の移行が「カットオーバー準備完了」状態になったあと、デスティネーションクラスタへのクライアントカットオーバーは自動的に実行されます。クライアントの自動カットオーバーを無効にする場合は、クライアントカットオーバーを手動で実行する必要があります。

### 手順

1. クライアントカットオーバーを手動で実行：

```
dest_cluster> vsserver migrate cutover -vsserver <vsserver name>
```

2. カットオーバー処理のステータスを確認します。

```
dest_cluster> vsserver migrate show
```

## クライアントカットオーバー後にソース **SVM** を手動で削除します

ソースのクリーンアップを無効にして SVM の移行を実行した場合は、クライアントカットオーバーの完了後にソース SVM を手動で削除できます。

### 手順

1. ソースのクリーンアップの準備が完了していることを確認します。

```
dest_cluster> vsserver migrate show
```

2. ソースをクリーンアップします。

```
dest_cluster> vsserver migrate source-cleanup -vsserver <vsserver_name>
```

# HAペアの管理

## HAペアの管理の概要

クラスタノードは、フォールトトレランスとノンストップオペレーションを実現するためにハイアベイラビリティ（HA）ペアとして構成されます。ノードに障害が発生した場合や定期的なメンテナンスのためにノードを停止する必要がある場合、パートナーがストレージをテイクオーバーしてデータの提供を継続できます。ノードがオンラインに戻ったら、パートナーはストレージをギブバックします。

HA ペアコントローラ構成は、対応する FAS / AFF ストレージコントローラ（ローカルノードとパートナーノード）のペアで構成されます。これらの各ノードは、もう一方のディスクシェルフに接続されます。HA ペアの一方のノードでエラーが発生し、データの処理が停止すると、パートナーによって障害ステータスが検出され、そのコントローラからすべてのデータ処理がテイクオーバーされます。

\_Takeover は、ノードがパートナーのストレージの制御を引き継ぐプロセスです。

giveback は、ストレージがパートナーに返されるプロセスです。

デフォルトでは、テイクオーバーは次のいずれかの状況で自動的に実行されます。

- パニック状態になるノードでソフトウェアまたはシステムの障害が発生した場合 HA ペアコントローラは、対応するパートナーノードに自動的にフェイルオーバーします。パートナーがパニック状態から回復してブートされると、ノードで自動的にギブバックが実行されてパートナーが通常の動作状態に戻ります。
- ノードでシステム障害が発生し、ノードをリブートできない。たとえば、電源の喪失によってノードに障害が発生した場合、HA ペアコントローラがパートナーノードに自動的にフェイルオーバーされ、稼働しているストレージコントローラからデータが提供されます。



ノードのストレージへの電源も同時に喪失した場合は、標準テイクオーバーは実行できません。

- ノードのパートナーからハートビートメッセージが届かない場合この状況は、パートナーでハードウェア障害またはソフトウェア障害（インターコネクト障害など）が発生してパニック状態にならなかったが、正常に機能しなくなった場合に発生することがあります。
- を使用せずに一方のノードを停止した場合 `-f` または `-inhibit-takeover true` パラメータ



クラスタ HA が有効な 2 ノードクラスタで、を使用してノードを停止またはリブートする `-inhibit-takeover true` パラメータを指定すると、クラスタ HA を無効にしてからオンラインのままにするノードにイプシロンを割り当てないかぎり、両方のノードでデータの提供が停止します。

- を使用せずに一方のノードをリブートした場合 `-inhibit-takeover true` パラメータ（`-onboot` のパラメータ `storage failover` コマンドはデフォルトで有効になっています）。
- リモート管理デバイス（サービスプロセッサ）でパートナーノードの障害が検出されました。これは、ハードウェアアシストテイクオーバーを無効にした場合は該当しません。

を使用してテイクオーバーを手動で開始することもできます `storage failover takeover` コマンドを実行します

## クラスタの耐障害性と診断の強化

ONTAP 9.9.1以降では、耐障害性と診断機能が次のように追加され、クラスタの運用が改善されています。

- ポートの監視と回避：2 ノードスイッチレスクラスタ構成では、全体的なパケット損失（接続の損失）が発生するポートを回避します。ONTAP 9.8.1以前では、この機能はスイッチ経由の構成でのみ使用できました。
- ノードの自動フェイルオーバー：クラスタネットワーク経由でデータを提供できないノードは、ディスクを所有しないでください。パートナーが健全な場合は、代わりに HA パートナーにテイクオーバーする必要があります。

- 接続の問題を分析するコマンド：次のコマンドを使用して、パケット損失が発生しているクラスタパスを表示します。`network interface check cluster-connectivity show`

## ハードウェアアシストテイクオーバーの仕組み

デフォルトで有効になっているハードウェアアシストテイクオーバー機能では、ノードのリモート管理デバイス（サービスプロセッサ）を使用してテイクオーバー処理を高速化できます。

リモート管理デバイスで障害が検出されると、パートナーのハートビートの停止を ONTAP が認識するのを待たずに、迅速にテイクオーバーが開始されます。この機能を有効にしないと障害が発生した場合、ノードからハートビートが届かなくなったことをパートナーで認識するまでは待機状態となり、ハートビートがなくなったことを確認してからテイクオーバーが開始されます。

ハードウェアアシストテイクオーバー機能では、次のプロセスを使用してこの待機時間が回避されます。

1. リモート管理デバイスは、特定の種類の障害についてローカルシステムを監視します。
2. 障害が検出されると、リモート管理デバイスからパートナーノードにすぐにアラートが送信されます。
3. アラートを受け取ったあと、パートナーでテイクオーバーが開始されます。

### ハードウェアアシストテイクオーバーをトリガーするイベント

リモート管理デバイス（サービスプロセッサ）から受信するアラートの種類によっては、パートナーノードでテイクオーバーが生成される場合があります。

アラート	テイクオーバーが開始されるか	説明
異常再起動	いいえ	ノードの異常リブートが発生しました。
l2_watchdog_reset	はい。	システムの watchdog ハードウェアが L2 リセットを検出しました。 システムの CPU が応答しないことがリモート管理デバイスで検出され、システムがリセットされました。
ハートビートの損失	いいえ	リモート管理デバイスがノードからハートビートメッセージを受信しなくなりました。 このアラートの対象は、HA ペアのノード間のハートビートメッセージではなく、ノードとそのローカルのリモート管理デバイスの間のハートビートメッセージです。
PERIODIC_MESSAGE	いいえ	通常のハードウェアアシストテイクオーバー中に送信される定期的なメッセージです。
power_cycle_via_sp	はい。	リモート管理デバイスの電源をオフにしてからオンにしてください。
power_loss です	はい。	ノードで電源喪失が発生しました。 リモート管理デバイスには、電源喪失時に一時的に電力を供給する電源装置が備わっているため、パートナーノードに電力喪失を通知することができます。
power_off_via_sp	はい。	リモート管理デバイスの電源がオフになりました。

reset_via_sp	はい。	リモート管理デバイスによってシステムがリセットされました。
テスト	いいえ	ハードウェアアシストテイクオーバー処理を確認するためのテストメッセージが送信されます。

## 自動テイクオーバーと自動ギブバックの仕組み

自動テイクオーバー処理と自動ギブバック処理を組み合わせることで、クライアントの停止を短くしたり回避したりできます。

デフォルトでは、HA ペアの一方向のノードでパニック、リブート、または停止が発生すると、パートナーノードに自動的にテイクオーバーされ、影響を受けたノードのリブート時にストレージが戻されます。その後、HA ペアが通常の動作状態に戻ります。

自動テイクオーバーは、いずれかのノードが応答しなくなった場合にも実行されます。

自動ギブバックがデフォルトで実行されます。ギブバックによるクライアントへの影響を制御する場合は、自動ギブバックを無効にしてを使用します `storage failover modify -auto-giveback false -node <node>` コマンドを実行します。自動ギブバックは、トリガーされた状況に関係なく実行されます。パートナーノードでは、で制御される一定の時間待機します `-delay- seconds` のパラメータ `storage failover modify` コマンドを実行します。デフォルトの遅延は 600 秒です。ギブバックを遅らせることで、このプロセスでは短時間の停止が 2 回発生します。テイクオーバー時とギブバック時の 2 回です。

これにより、次の処理に必要な時間を含む 1 回の長時間の停止が回避されます。

- テイクオーバー処理
- テイクオーバーされたノードがブートし、ギブバック可能な状態になります
- ギブバック処理

ルート以外のアグリゲートで自動ギブバックが失敗した場合、自動的にあと 2 回ギブバックが試行されます。



テイクオーバープロセスでは、パートナーノードがギブバック可能な状態になる前に自動ギブバックプロセスが開始されます。自動ギブバックプロセスの期限内にパートナーノードがギブバック可能な状態にならないと、タイマーがリスタートします。その結果、パートナーノードがギブバック可能な状態になってから実際にギブバックが実行されるまでの時間が自動ギブバック時間よりも短くなる可能性があります。

## テイクオーバー時の動作

パートナーをテイクオーバーしたノードは、パートナーのアグリゲートとボリュームのデータを引き続き提供および更新します。

テイクオーバープロセスの実行中は次の手順が実行されます。

1. ユーザが開始したネゴシエートテイクオーバーの場合は、集約されたデータがパートナーノードからテイクオーバーを実行中のノードに移動されます。短時間の停止は、各アグリゲート（ルートアグリゲートを除く）の現在の所有者がテイクオーバーノードに切り替わったときに発生します。ただし、アグリゲートの再配置を伴わないテイクオーバーに比べると短時間で済みます。





パニック時のネゴシエートテイクオーバーは実行できません。テイクオーバーが発生する原因としては、パニックに関連しない障害が考えられます。ノードとそのパートナー間の通信が失われると、障害が発生します（ハートビート損失とも呼ばれます）。障害が原因でテイクオーバーが発生した場合は、パートナーノードがハートビートの損失を検出するために時間がかかるため、停止時間が長くなる可能性があります。

- 進捗状況はを使用して監視できます `storage failover show-takeover` コマンドを実行します
- を使用すると、このテイクオーバーインスタンスの実行中にアグリゲートの再配置を実行しないことができます `-bypass-optimization` パラメータと `storage failover takeover` コマンドを実行します

計画的テイクオーバー処理では、クライアントの停止を最小限にするため、アグリゲートが順に再配置されます。アグリゲートの再配置を省略すると、計画的テイクオーバーの際のクライアントの停止時間が長くなります。

2. ユーザが開始したネゴシエートテイクオーバーの場合は、ターゲットノードが正常にシャットダウンされ、そのあとにルートアグリゲートと手順 1 で再配置されなかったアグリゲートのテイクオーバーが実行されます。
3. LIFのフェイルオーバールールに基づいて、ターゲットノードからテイクオーバーノード、またはクラスタ内の他のノードにデータLIF（論理インターフェイス）が移行されます。を使用すると、LIFの移行を回避できます `-skip-lif-migration` パラメータと `storage failover takeover` コマンドを実行します。ユーザが開始したテイクオーバーの場合、ストレージのテイクオーバーの開始前にデータLIFが移行されます。パニック状態や障害発生時には、データLIFとストレージが一緒に移行されます。
4. テイクオーバーの発生時に既存の SMB セッションが切断されます。



SMB プロトコルの性質上、すべての SMB セッションは中断されます（Continuous Availability プロパティが設定された共有に接続している SMB 3.0 セッションを除く）。SMB 1.0 および SMB 2.x のセッションは、テイクオーバー後に再接続できないため、テイクオーバー時に停止が発生し、一部のデータが失われる可能性があります。

5. 継続的な可用性が有効な共有に対する SMB 3.0 セッションは、テイクオーバー後に元の共有に再接続できます。サイトで SMB 3.0 を使用して Microsoft Hyper-V に接続している場合、関連付けられている共有で継続的な可用性プロパティが有効になっていれば、テイクオーバー時にそれらのセッションは停止されません。

テイクオーバーを実行中のノードがパニック状態になった場合の動作

テイクオーバーを実行中のノードが、テイクオーバーを開始してから 60 秒以内にパニック状態になると、次のような状態になります。

- パニックが発生したノードがリブートします。
- リブートしたノードではセルフリカバリ処理が実行され、テイクオーバーモードではなくなります。
- フェイルオーバーが無効になります。
- パートナーの一部のアグリゲートをまだ所有している場合は、ストレージフェイルオーバーを有効にしたあとに、を使用してそれらのアグリゲートをパートナーに戻します `storage failover giveback` コマンドを実行します

## ギブバック時の動作

問題が解決されるか、パートナーノードがブートされるか、ギブバックが開始されると、ローカルノードからパートナーノードに所有権が戻されます。

通常のギブバック処理は次のように実行されます。ここでは、ノード A にノード B がテイクオーバーされていますノード B の問題が解決され、データの提供を再開できる状態になっている。

1. ノード B の問題が解決され、次のメッセージが表示されます。 `Waiting for giveback`
2. によってギブバックが開始されます `storage failover giveback` コマンドを使用するか、自動ギブバック（設定されている場合）を使用します。これにより、ノード B のアグリゲートおよびボリュームの所有権をノード A からノード B に戻すプロセスが開始されます
3. ノード A から最初にルートアグリゲートの制御が戻されます。
4. ノード B を通常の動作状態に戻すためのブートプロセスが完了します。
5. ノード B のブートプロセスでルート以外のアグリゲートを受け取れる状態になった時点で、すぐに他のアグリゲートの所有権を戻すプロセスが開始されます。ギブバックが完了するまでの間に、それらの所有権がノード A から 1 つずつ戻されます。を使用して、ギブバックの進捗を監視できます `storage failover show-giveback` コマンドを実行します



。 `storage failover show-giveback` コマンドでは、ストレージフェイルオーバーのギブバック処理中に発生するすべての処理に関する情報が表示されるわけではありません（また、そのような意図はありません）。を使用できます `storage failover show` コマンドを使用して、ノードの現在のフェイルオーバーステータス（ノードが完全に機能しているか、テイクオーバーが可能か、ギブバックが完了したかなど）に関するその他の詳細情報を表示します。

各アグリゲートの I/O は、そのアグリゲートのギブバックが完了したあとに再開されます。これにより、アグリゲートの全体的な停止時間が短くなります。

## テイクオーバーおよびギブバックに対する HA ポリシーの影響

ONTAP は、CFO（コントローラフェイルオーバー）と SFO（ストレージフェイルオーバー）の HA ポリシーをアグリゲートに自動的に割り当てます。このポリシーは、アグリゲートとそのボリュームでストレージフェイルオーバー処理がどのように実行されるかを決定します。

CFO と SFO の 2 つのうち、どちらが割り当てられているかによって、ONTAP がストレージフェイルオーバーおよびギブバック処理で使用するアグリゲートの制御順序が決まります。

CFO および SFO という用語は、ストレージフェイルオーバー（テイクオーバーとギブバック）処理を表すこともありますが、実際はアグリゲートに割り当てられる HA ポリシーのことを表しています。たとえば、SFO アグリゲートや CFO アグリゲートという表現は、単にアグリゲートに割り当てられた HA ポリシーを指しています。

HA ポリシーは、テイクオーバー処理とギブバック処理に次のように影響します。

- ONTAP システムで作成されたアグリゲート（ルートボリュームを含むルートアグリゲートを除く）には、SFO の HA ポリシーが割り当てられます。手動で開始されたテイクオーバーでは、テイクオーバー前に SFO（ルート以外）アグリゲートをパートナーに順番に再配置することで、パフォーマンスが最適化されます。ギブバック処理では、テイクオーバーされたシステムがブートして管理アプリケーションがオンラインになり、ノードがアグリゲートを受け取れる状態になってから、アグリゲートが順番にギブバ

ックされます。

- アグリゲートの再配置処理では、アグリゲートのディスク所有権が再割り当てされ、ノードの制御がパートナーに移るため、SFO の HA ポリシーが割り当てられたアグリゲートだけが再配置の対象になります。
- ルートアグリゲートには常に CFO の HA ポリシーが割り当てられ、ギブバック処理の開始時にアグリゲートがギブバックされます。これは、テイクオーバーされたシステムをブートできるようにするために必要です。その他のすべてのアグリゲートは、テイクオーバーされたシステムのブートプロセスが完了して管理アプリケーションがオンラインになり、ノードがアグリゲートを受け取れる状態になってから、順番にギブバックされます。



アグリゲートの HA ポリシーを SFO から CFO に変更する処理はメンテナンスモードの処理です。この設定は、カスタマーサポート担当者から指示がないかぎり変更しないでください。

### バックグラウンド更新がテイクオーバーとギブバックに与える影響

ディスクファームウェアのバックグラウンド更新による HA ペアのテイクオーバー、ギブバック、およびアグリゲートの再配置の処理に対する影響は、処理がどのように開始されたかによって異なります。

ディスクファームウェアのバックグラウンド更新によるテイクオーバー、ギブバック、およびアグリゲートの再配置に対する影響は次のとおりです。

- いずれかのノードのディスクでディスクファームウェアのバックグラウンド更新を実行した場合、手動で開始したテイクオーバー処理は、そのディスクでディスクファームウェアの更新が完了するまで保留されます。ディスクファームウェアのバックグラウンド更新が 120 秒経っても完了しないと、テイクオーバー処理は中止され、ディスクファームウェアの更新の完了後に手動で再開する必要があります。でテイクオーバーが開始された場合 `-bypass-optimization` のパラメータ `storage failover takeover` コマンドをに設定します ``true`` デスティネーションノードでディスクファームウェアのバックグラウンド更新を実行していても、テイクオーバーには影響しません。
- ソース（テイクオーバー）ノードのディスクでディスクファームウェアのバックグラウンド更新を実行中の場合、を使用してテイクオーバーが手動で開始されたとき `-options` のパラメータ `storage failover takeover` コマンドをに設定します ``immediate`` テイクオーバー処理がただちに開始されます。
- ノードのディスクでディスクファームウェアのバックグラウンド更新を実行中の場合に、そのノードがパニック状態になると、パニック状態になったノードのテイクオーバーが開始されます。
- いずれかのノードのディスクでディスクファームウェアのバックグラウンド更新を実行中の場合、データアグリゲートのギブバックは、そのディスクでディスクファームウェアの更新が完了するまで保留されます。
- ディスクファームウェアのバックグラウンド更新が 120 秒経っても完了しないと、ギブバック処理は中止され、ディスクファームウェアの更新の完了後に手動で再開する必要があります。
- いずれかのノードのディスクでディスクファームウェアのバックグラウンド更新を実行中の場合、アグリゲートの再配置処理は、そのディスクでディスクファームウェアの更新が完了するまで保留されます。ディスクファームウェアのバックグラウンド更新が 120 秒経っても完了しないと、アグリゲートの再配置処理は中止され、ディスクファームウェアの更新の完了後に手動で再開する必要があります。アグリゲートの再配置をで開始した場合 `-override-destination-checks` の `storage aggregate relocation` コマンドをに設定します ``true`` デスティネーションノードでディスクファームウェアのバックグラウンド更新を実行していても、アグリゲートの再配置には影響しません。

## 自動テイクオーバーのコマンド

自動テイクオーバーは、サポート対象のすべての NetApp FAS、AFF、ASA プラットフォームでデフォルトで有効になります。パートナーノードのリブート、パニック、または停止時に自動テイクオーバーが実行されるタイミングについては、デフォルトの動作を変更したり制御したりする必要があります。

テイクオーバーを自動で実行するパートナーノードの状況	使用するコマンド
リブートまたは停止します	<code>storage failover modify -node nodename -onreboot true</code>
パニック	<code>storage failover modify -node nodename -onpanic true</code>

テイクオーバー機能が無効になっている場合は、E メール通知を有効にします

テイクオーバー機能が無効になった場合に通知を受け取るようにするには、EMS メッセージ「takeover impossible」の自動 E メール通知を有効にするようにシステムを設定します。

- `ha.takeoverImpVersion`
- `ha.takeoverImpLowMem`
- `ha.takeoverImpDegraded`
- `ha.takeoverImpUnsync`
- `ha.takeoverImpIC`
- `ha.takeoverImpHotShelf`
- `ha.takeoverImpNotDef`

## 自動ギブバックコマンド

デフォルトでは、オフラインのノードがオンラインに戻った時点でテイクオーバーパートナーノードがストレージを自動的にギブバックするため、ハイアベイラビリティペア関係がリストアされます。ほとんどの場合、これが望ましい動作です。自動ギブバックを無効にする必要がある場合：テイクオーバーの原因を調査してからギブバックする場合は、デフォルト以外の設定のやり取りについて確認しておく必要があります。

状況	使用するコマンド
自動ギブバックを有効にして、テイクオーバーされたノードのブート後、Waiting for giveback 状態に達し、Auto giveback 期間が終了するまでの待機時間が経過した時点でギブバックが実行されるようにします。  デフォルト設定は true です。	<code>storage failover modify -node nodename -auto-giveback true</code>

自動ギブバックを無効にするデフォルト設定は <code>true</code> です。  *注：*このパラメータを <code>false</code> に設定しても、パニック時のテイクオーバー後の自動ギブバックは無効になりません。パニック時のテイクオーバー後の自動ギブバックは、を <code>storage failover modify</code> コマンドで設定して無効にする必要があります <code>-auto-giveback-after-panic</code> パラメータを <code>false</code> に設定します。	<code>storage failover modify -node nodename -auto-giveback false</code>
パニック時のテイクオーバーのあとに実行される自動ギブバックを無効にします（この設定はデフォルトで有効になります）。	<code>storage failover modify -node nodename -auto-giveback-after-panic false</code>
自動ギブバックが開始されるまでの待機時間（秒）を設定します（デフォルトは 600 秒）。このオプションで指定した待機時間が経過するまでは、自動ギブバックは実行されません。	<code>storage failover modify -node nodename -delay-seconds seconds</code>

## storage failover modify コマンドの設定による自動ギブバックへの影響

自動ギブバックの処理は、 `storage failover modify` コマンドのパラメータの設定によって異なります。

次の表に、のデフォルト設定を示します `storage failover modify` パニック以外のテイクオーバーイベントに適用されるコマンドパラメータ。

パラメータ	デフォルト設定です
<code>-auto-giveback true</code>	<code>false</code>
<code>true</code>	<code>-delay-seconds integer (seconds)</code>
600	<code>-onreboot true</code>
<code>false</code>	<code>true</code>

次の表に、の組み合わせを示します `-onreboot` および `-auto-giveback` パラメータは、パニック以外のテイクオーバーイベントの自動ギブバックに適用されます。

storage failover modify 使用するパラメータ	テイクオーバーの原因	自動ギブバックの実行
<code>-onreboot true</code>	reboot コマンド	はい。
<code>-auto-giveback true</code>		

halt コマンド、またはサービスプロセッサからの電源再投入	はい。	<code>-onreboot true</code>  <code>-auto-giveback false</code>
reboot コマンド	はい。	halt コマンド、またはサービスプロセッサからの電源再投入
いいえ	<code>-onreboot false</code>  <code>-auto-giveback true</code>	reboot コマンド
N/A この場合、テイクオーバーは実行されません。	halt コマンド、またはサービスプロセッサからの電源再投入	はい。
<code>-onreboot false</code>  <code>-auto-giveback false</code>	reboot コマンド	いいえ

。 `-auto-giveback` パラメータは、パニックおよびその他すべての自動テイクオーバー後のギブバックを制御します。状況に応じて `-onreboot` パラメータはに設定されます `true` リブートが原因でテイクオーバーが発生すると、がどちらであるかに関係なく、常に自動ギブバックが実行されます `-auto-giveback` パラメータはに設定されます `true`。

。 `-onreboot` Parameter環境 がリブートし、ONTAP から実行されたコマンドが停止します。をクリックします `-onreboot` パラメータが`false`に設定されている場合、ノードがリブートしてもテイクオーバーは実行されません。そのため、があるかどうかに関係なく、自動ギブバックは実行されません `-auto-giveback` パラメータが`true`に設定されている。クライアントのアクセスが中断します。

#### パニック時に適用される自動ギブバックパラメータの組み合わせとその影響

次の表に、を示します `storage failover modify` パニック状態に適用されるコマンドパラメータは次のとおりです。

パラメータ	デフォルト設定です
<code>`-onpanic_true`</code>	<code>false_`</code>
<code>true`</code>	<code>`-auto-giveback-after-panic_true`</code>
<code>false_`</code> (権限: advanced)	<code>true`</code>
<code>`-auto-giveback_true`</code>	<code>false_`</code>

次の表に、のパラメータの組み合わせを示します `storage failover modify` コマンドは、パニック時の自動ギブバックに適用されます。

storage failover 使用するパラメータ	パニック発生後の自動ギブバックの実行
----------------------------	--------------------

-onpanic true -auto-giveback true -auto-giveback-after-panic true	はい。
-onpanic true -auto-giveback true -auto-giveback-after-panic false	はい。
-onpanic true -auto-giveback false -auto-giveback-after-panic true	はい。
-onpanic true -auto-giveback false -auto-giveback-after-panic false	いいえ
-onpanic false 状況 -onpanic がに設定されます false`に設定されている値 に関係なく、テイクオーバー/ギブバックは実行されません ` - auto-giveback または -auto-giveback-after-panic	いいえ



テイクオーバーが発生する原因としては、パニックに関連しない障害が考えられます。  
a\_failure\_は、ノードとそのパートナー間の通信が失われたときに実行されます。これは、\_ハ  
ートビートlost\_とも呼ばれます。障害が原因でテイクオーバーが発生した場合は、によってギ  
ブバックが制御されます -onfailure ではなくパラメータを使用します -auto-giveback  
-after-panic parameter。



ノードでパニックが発生すると、パートナーノードにパニックパケットが送信されます。何ら  
かの理由でパートナーノードがパニックパケットを受信しなかった場合、パニック状態と誤っ  
て解釈される可能性があります。パニックパケットを受信しなかった場合、パートナーノード  
は通信が失われたことだけを認識し、パニック状態になったことは通知しません。この場合、  
パートナーノードはパニック状態ではなく障害として通信の喪失を処理し、ギブバックはによ  
って制御されます -onfailure パラメータ（ではなく） -auto-giveback-after-panic  
parameter）。

詳細については、を参照してください storage failover modify パラメータについては、を参照してく  
ださい ["ONTAP のマニュアルページ"](#)。

## 手動テイクオーバーのコマンド

パートナーで保守を実施する場合、およびその他の同様の状況では、テイクオーバーを  
手動で実行できます。テイクオーバーの実行に使用するコマンドは、パートナーの状態  
に応じて異なります。

状況	使用するコマンド
パートナーノードをテイクオーバーします	storage failover takeover
パートナーのアグリゲートをテイクオーバーを実行中 のノードに移動するまでのテイクオーバーの進捗を監視する	storage failover show-takeover



クラスタ内のすべてのノードのストレージフェイルオーバーのステータスを表示します	<code>storage failover show</code>
LIF を移行せずにパートナーノードをテイクオーバーする	<code>storage failover takeover -skip-lif -migration-before-takeover true</code>
ディスクが一致していなくてもパートナーノードをテイクオーバーする	<code>storage failover takeover -skip-lif -migration-before-takeover true</code>
ONTAPバージョンが一致していなくてもパートナーノードをテイクオーバーする  *注：*このオプションは、ONTAPの無停止アップグレードプロセスでのみ使用されます。	<code>storage failover takeover -option allow -version-mismatch</code>
アグリゲートの再配置を実行せずにパートナーノードをテイクオーバーする	<code>storage failover takeover -bypass -optimization true</code>
パートナーによるストレージリソースの正常終了を待たずにパートナーノードをテイクオーバーします	<code>storage failover takeover -option immediate</code>

`immediate` オプションを指定して `storage failover` コマンドを問題 する前に、次のコマンドを使用して別のノードにデータLIFを移行する必要があります。 `network interface migrate-all -node node`



を指定する場合は `storage failover takeover -option immediate` コマンドを実行する前にデータLIFを移行しないと、があっても、ノードからのデータLIFの移行が大幅に遅れます `skip-lif-migration-before-takeover` オプションが指定されていません。

同様に、 `immediate` オプションを指定した場合は、 `bypass - optimization` オプションを `false` に設定しても、ネゴシエートテイクオーバーの最適化が省略されます。

## テイクオーバーを手動で開始する場合のイプシロンの移動

手動で開始したテイクオーバーによって、ストレージシステムの 1 つのノードで予期しないノード障害が発生するとクラスタ全体のクォーラムが失われる可能性がある場合は、イプシロンを移動する必要があります。

### このタスクについて

計画的なメンテナンスを実施するときは、HA ペアの一方のノードをテイクオーバーする必要があります。残りのノードでクライアントデータの計画外の中断を防ぐには、クラスタ全体のクォーラムを維持する必要があります。場合によっては、テイクオーバーを実行すると、クラスタで予期しないノード障害が発生してクラスタ全体のクォーラムが失われる可能性があります。

この状況は、テイクオーバーするノードにイプシロンが設定されている場合や、イプシロンが設定されたノードが正常な状態でない場合に発生します。クラスタの耐障害性を高めるには、テイクオーバーするノード以外の正常なノードにイプシロンを移動します。通常は HA パートナーに移動します。

クォーラムの投票に参加するのは、対象となる正常なノードだけです。クラスタ全体のクォーラムを維持するには、対象となる、オンラインかつ正常なノードの半数を超える投票が必要です。クラスタオンラインのノード数が偶数の場合、イプシロンによって、割り当て先のノードのクォーラムを維持するための投票加重が追加されます。





クラスタ形成の投票はを使用して変更できますが `cluster modify -eligibility false` コマンドを使用する場合は、ノード設定をリストアする場合やノードのメンテナンスが長時間かかる場合を除き、この設定は避けてください。クラスタ参加資格を無効に設定すると、参加資格を再設定してリブートするまで、そのノードは SAN データを提供しなくなります。ノードにクラスタ参加資格がないと、そのノードへの NAS データアクセスも影響を受ける可能性があります。

## 手順

1. クラスタの状態を確認し、テイクオーバーするノード以外の正常なノードにイプシロンが設定されていることを確認します。

- a. advanced モードのプロンプト (`*>`) が表示されたら、次のコマンドを入力して advanced 権限レベルに切り替えます。

```
set -privilege advanced
```

- b. イプシロンが設定されているノードを特定します。

```
cluster show
```

次の例では、Node1 にイプシロンが設定されています。

ノード	健全性	資格	イプシロン
ノード1 ノード 2	正しいです 正しいです	正しいです 正しいです	正しいです いいえ

+

テイクオーバーするノードにイプシロンが設定されていない場合は、手順 4 に進みます。

2. テイクオーバーするノードからイプシロンを削除します。

```
cluster modify -node Node1 -epsilon false
```

3. パートナーノード（この例では Node2）にイプシロンを割り当てます。

```
cluster modify -node Node2 -epsilon true
```

4. テイクオーバー処理を実行します。

```
storage failover takeover -ofnode node_name
```

5. admin 権限レベルに戻ります。

```
set -privilege admin
```

## 手動ギブバックコマンド

パートナーノードのプロセスを終了する標準ギブバック、または強制ギブバックを実行できます。



ギブバックを実行する前に、で説明するように、障害が発生したドライブをテイクオーバーされたシステムから取り外す必要があります **"ディスクとアグリゲートの管理"**。

#### ギブバックが中断された場合

ギブバックプロセス中にテイクオーバーノードで障害が発生したり停電が発生したりした場合、そのプロセスは停止します。障害が修復されるか電源が回復するまで、テイクオーバーノードはテイクオーバーモードに戻ります。

ただし、障害がギブバックのどの段階で発生したかによって、これとは異なる動作になります。障害や停電が部分的なギブバック状態の間（ルートアグリゲートのギブバックの完了後）に発生した場合、ノードはテイクオーバーモードには戻りません。部分的なギブバックモードに戻ります。この場合、プロセスを完了するには、ギブバック処理をもう一度実行します。

#### ギブバックが拒否された場合

ギブバックが拒否された場合、EMS メッセージを調べて原因を特定する必要があります。その理由に応じて、拒否を無視しても問題がないかどうかを判断することができます。

。storage failover show-giveback ギブバックの進捗が表示されます。ギブバックを拒否したサブシステムがある場合はそのサブシステムも表示されます。拒否の中には、無視してもかまわないソフトなものと、強制しても無視できないハードなものがあります。次の表に、無視できないソフトな拒否と、推奨される対処方法を示します。

次のコマンドを使用して、ギブバックの拒否に関する EMS の詳細を確認できます。

```
event log show -node * -event gb*
```

#### ルートアグリゲートのギブバック

次の拒否は、アグリゲートの再配置処理には適用されません。

拒否しているサブシステムモジュールです	回避策
vFiler_low_level	拒否の原因となっているSMBセッションを終了するか、開いているセッションを確立したSMBアプリケーションをシャットダウンします。  この拒否を無視すると、SMBを使用しているアプリケーションが原因によって突然切断され、データが失われる可能性があります。
ディスクチェック	ギブバックを実行する前に、障害が発生したかバイパスされたディスクをすべて取り外します。ディスクの完全消去を実行中の場合は、処理が完了するまで待ちます。  この拒否を無視すると、容量確保の競合やディスクにアクセスできないことが原因でアグリゲートやボリュームがオフラインになり、原因が停止する可能性があります。

## SFO アグリゲートのギブバックを実行します

次の拒否は、アグリゲートの再配置処理には適用されません。

拒否しているサブシステムモジュールです	回避策
ロックマネージャ	<p>ファイルを開いているSMBアプリケーションを正常にシャットダウンするか、それらのボリュームを別のアグリゲートに移動します。</p> <p>この拒否を無視すると、SMBロック状態が失われ、システムが停止してデータが失われます。</p>
ロックマネージャ NDO	<p>ロックがミラーされるまで待ちます。</p> <p>この拒否を無視すると、Microsoft Hyper-V 仮想マシンの処理が停止します。</p>
RAID の場合	<p>EMS メッセージを調べて拒否の原因を特定します。</p> <p>nvfile が原因である場合は、オフラインのボリュームおよびアグリゲートをオンラインにします。</p> <p>ディスクの追加処理またはディスク所有権の再割り当て処理を実行中の場合は、それらの処理が完了するまで待ちます。</p> <p>アグリゲートの名前または UUID の競合が原因である場合は、問題のトラブルシューティングを行ってその問題を解決します。</p> <p>ミラーの再同期、ミラーの検証、またはディスクのオフライン化が原因で拒否された場合は無視してかまいません。これらの処理は、ギブバック後に再開されます。</p>
ディスクインベントリ	<p>トラブルシューティングを行って、問題の原因を特定し、解決します。</p> <p>移行中のアグリゲートに属するディスクは、デスティネーションノードで認識できないことがあります。</p> <p>ディスクにアクセスできないと、アグリゲートまたはボリュームにアクセスできない可能性があります。</p>
ボリューム移動処理	<p>トラブルシューティングを行って、問題の原因を特定し、解決します。</p> <p>この拒否は、重要なカットオーバーフェーズ中にボリューム移動処理が中止されるのを防止します。カットオーバー中にジョブが中止されると、ボリュームにアクセスできなくなる可能性があります。</p>

手動ギブバックを実行するためのコマンドです

メンテナンスの完了後または解決後に元の所有者にストレージを戻すには、HAペアのノードでギブバックを手動で開始します。

テイクオーバーの原因となった問題。

状況	使用するコマンド
パートナーノードにストレージをギブバックします	<code>storage failover giveback -ofnode nodename</code>
パートナーがギブバック待機モードになっていなくてもストレージをギブバックします	<code>storage failover giveback -ofnode nodename -require-partner-waiting false</code>  このオプションは、長時間クライアントが停止しても問題がない場合にのみ使用してください。
ギブバック処理がプロセスで拒否されてもストレージをギブバックする（強制的にギブバックを実行する）	<code>storage failover giveback -ofnode nodename -override-vetoes true</code>  このオプションを使用すると、クライアントの停止が長引いたり、ギブバックの完了後にアグリゲートとボリュームがオンラインに復帰しない可能性があります。
CFO アグリゲート（ルートアグリゲート）だけをギブバックする	<code>storage failover giveback -ofnode nodename  -only-cfo-aggregates true</code>
ギブバックコマンドを実行したあとにギブバックの進捗を監視します問題	<code>storage failover show-giveback</code>

## テイクオーバーとギブバックをテストする

HA ペアについてのすべての設定が完了したら、テイクオーバー処理やギブバック処理の際に両方のノードのストレージに中断なくアクセスできることを確認する必要があります。テイクオーバーの処理中は、通常はパートナーノードから提供されるデータがローカル（テイクオーバー）ノードで継続して提供されるようにする必要があります。ギブバックの際は、パートナーのストレージを制御および提供する役割がパートナーノードに戻らなければなりません。

### 手順

1. HA インターコネクトケーブルのケーブル接続を調べて、確実に接続されていることを確認します。
2. ライセンスが付与されたプロトコルごとに、両方のノードでファイルを作成および取得できることを確認します。
3. 次のコマンドを入力します。

```
storage failover takeover -ofnode partnernode
```

コマンドの詳細については、マニュアルページを参照してください。

4. 次のいずれかのコマンドを入力して、テイクオーバーが実行されたことを確認します。

```
storage failover show-takeover
```

```
storage failover show
```

を使用している場合 storage failover コマンド `-auto-giveback` オプション有効：

ノード	パートナー	テイクオーバーが可能です	State 概要の略
ノード 1	ノード 2	-	ギブバックを待っています
ノード 2	ノード 1	いいえ	テイクオーバーの発生後、 number of seconds で示された秒数以内に自動ギブバックが開始されます

を使用している場合 storage failover コマンド `-auto-giveback` オプション無効：

ノード	パートナー	テイクオーバーが可能です	State 概要の略
ノード 1	ノード 2	-	ギブバックを待っています
ノード 2	ノード 1	いいえ	テイクオーバー中です

5. パートナーノード（ノード 2）に属するディスクのうち、テイクオーバーノード（ノード 1）で検出できるすべてのディスクを表示します。

```
storage disk show -home node2 -ownership
```

次のコマンドは、ノード 2 に属するディスクのうち、ノード 1 で検出できるすべてのディスクを表示します。

```
cluster::> storage disk show -home node2 -ownership
```

ディスク	アグリゲート	ホーム	オーナー	DR ホーム	ホーム ID	所有者 ID	DR ホーム ID	予約者	プール
1.0.2	-	ノード 2	ノード 2	-	4078312453	4078312453	-	4078312452	プール 0
1.0.3	-	ノード 2	ノード 2	-	4078312453	4078312453	-	4078312452	プール 0

6. テイクオーバーノード（ノード 1）がパートナーノード（ノード 2）のアグリゲートを制御していることを確認します。

```
aggr show -fields home-id,home-name,is-home
```

アグリゲート	home-id	Home - 名前 h	is-fhome
aggr0_cluster1_01 の実行	2014942045	ノード 1	正しいです
aggr0_2 です	4078312453	ノード 2	いいえ
aggr1_cluster1_01 があります	2014942045	ノード 1	正しいです
aggr1_2 の構成ファイル	4078312453	ノード 2	いいえ

テイクオーバー時、パートナーノードのアグリゲートの「is-home」の値が false になります。

- 「Waiting for giveback」メッセージが表示されたら、パートナー・ノードのデータ・サービスをギブバックします。

```
storage failover giveback -ofnode partnernode
```

- 次のいずれかのコマンドを入力して、ギブバック処理の進捗を監視します。

```
storage failover show-giveback
```

```
storage failover show
```

- ギブバックが正常に完了したというメッセージが表示されたかどうかに応じて、次の手順に進みます。

テイクオーバーおよびギブバックの結果	作業
が完了しました	パートナーノードで手順 2~8 を繰り返します。
失敗	テイクオーバーまたはギブバックの失敗を修正してから、この手順を繰り返します。

## HA ペアの監視用コマンドです

ONTAP コマンドを使用して HA ペアのステータスを監視できます。テイクオーバーが発生した場合は、テイクオーバーの原因も確認できます。

をオンにする場合は	使用するコマンド
フェイルオーバーの有効 / 無効と発生の有無、または現在フェイルオーバーを実行できない理由	<pre>storage failover show</pre>
ストレージフェイルオーバーのHAモード設定が有効になっているノードを表示する ストレージフェイルオーバー（HAペア）構成に含めるノードについては、この値をhaに設定する必要があります。	<pre>storage failover show -fields mode</pre>

ハードウェアアシストテイクオーバーが有効になっているかどうか	<code>storage failover hwassist show</code>
これまでに発生したハードウェアアシストテイクオーバーイベントの履歴です	<code>storage failover hwassist stats show</code>
パートナーのアグリゲートをテイクオーバーを実行中のノードに移動するまでのテイクオーバー処理の進捗	<code>storage failover show-takeover</code>
アグリゲートをパートナーノードに戻すまでのギブバック処理の進捗	<code>storage failover show-giveback</code>
テイクオーバーまたはギブバックの処理中にアグリゲートがホームであるかどうか	<code>aggregate show -fields home-id,owner-id,home-name,owner-name,is-home</code>
クラスタ HA が有効になっているかどうか（2 ノードクラスタの場合のみ）	<code>cluster ha show</code>
HA ペアのコンポーネントの HA の状態（HA の状態を使用するシステム）	<code>ha-config show</code> これはメンテナンスモードのコマンドです。

### storage failover show-type コマンドで表示されるノードの状態

次に、にノードの状態が表示される例を示します `storage failover show` コマンドが表示されます。

ノードの状態	説明
partner_name に接続されています。自動テイクオーバーは無効になっています。	HA インターコネクトがアクティブでパートナーノードにデータを転送できます。パートナーの自動テイクオーバーは無効になっています。
partner_name で待機しているパートナーのスペアディスクのギブバックが保留中です。	ローカルノードとパートナーノードの間で、HA インターコネクトを介して情報を交換できません。パートナーへの SFO アグリゲートのギブバックは完了しましたが、パートナーのスペアディスクがまだローカルノードで所有されています。  • を実行します <code>storage failover show-giveback</code> 詳細については、コマンドを参照してください。
partner_name を待機していますパートナーロックの同期を待っています。	ローカルノードとパートナーノードの間で、HA インターコネクトを介して情報を交換できません。パートナーロックの同期が実行されるのを待っています。
partner_name を待機していますローカルノードでクラスタのアプリケーションがオンラインになるのを待っています。	ローカルノードとパートナーノードの間で、HA インターコネクトを介して情報を交換できません。クラスタのアプリケーションがオンラインになるのを待っています。

テイクオーバーのスケジュール：テイクオーバーの準備として、ターゲットノードで SFO アグリゲートを再配置しています。	テイクオーバーの処理が開始されました。テイクオーバーの準備として、ターゲットノードで SFO アグリゲートの所有権を切り替えています。
テイクオーバーのスケジュール：テイクオーバーの準備として、ターゲットノードで SFO アグリゲートが再配置されました。	テイクオーバーの処理が開始されました。テイクオーバーの準備として、ターゲットノードで SFO アグリゲートの所有権を切り替えました。
テイクオーバーのスケジュール：ローカルノードでディスクファームウェアのバックグラウンド更新を無効にするのを待っています。ノードでファームウェアの更新を実行中です。	テイクオーバーの処理が開始されました。ローカルノードでのディスクファームウェアのバックグラウンド更新が完了するのを待っています。
テイクオーバーの準備としてテイクオーバーするノードへの SFO アグリゲートの再配置	テイクオーバーの準備として、ローカルノードでテイクオーバーするノードに SFO アグリゲートの所有権を切り替えています。
テイクオーバーするノードに SFO アグリゲートを再配置しました。テイクオーバーするノードを待っています。	ローカルノードからテイクオーバーするノードへの SFO アグリゲートの所有権の切り替えが完了しました。テイクオーバーするノードによるテイクオーバーを待っています。
SFO アグリゲートを partner_name に再配置していますローカルノードでディスクファームウェアのバックグラウンド更新を無効にするのを待っています。ノードでファームウェアの更新を実行中です。	ローカルノードからテイクオーバーするノードへの SFO アグリゲートの所有権の切り替えを実行中です。ローカルノードでのディスクファームウェアのバックグラウンド更新が完了するのを待っています。
SFO アグリゲートを partner_name に再配置していますpartner_name でディスクファームウェアのバックグラウンド更新を無効にするのを待っています。ノードでファームウェアの更新を実行中です。	ローカルノードからテイクオーバーするノードへの SFO アグリゲートの所有権の切り替えを実行中です。パートナーノードでのディスクファームウェアのバックグラウンド更新が完了するのを待っています。
partner_name に接続されています。前回のテイクオーバーの試行が理由で中止されました。パートナーの一部の SFO アグリゲートがローカルノードで所有されています。 を使用してパートナーのテイクオーバーを再実行します -bypass-optimization パラメータをtrueに設定すると、残りのアグリゲートをテイクオーバーします。再配置されたアグリゲートを戻すには、パートナーのギブバックを問題 します。	HA インターコネクトがアクティブでパートナーノードにデータを転送できます。前回のテイクオーバーの試行が reason で示された理由により中止されました。パートナーの一部の SFO アグリゲートがローカルノードで所有されています。  <ul style="list-style-type: none"> <li>残りの SFO アグリゲートをテイクオーバーする場合は、- bypass - optimization パラメータを true に設定して、パートナーノードのテイクオーバーを再発行するか、再配置されたアグリゲートを戻す場合はパートナーのギブバックを実行します。</li> </ul>



<p>partner_name に接続されています。前回のテイクオーバーの試行が中止されました。パートナーの一部の SFO アグリゲートがローカルノードで所有されています。</p> <p>を使用してパートナーのテイクオーバーを再実行します -bypass-optimization パラメータを true に設定すると、残りのアグリゲートをテイクオーバーします。再配置されたアグリゲートを戻すには、パートナーのギブバックを問題 します。</p>	<p>HA インターコネクトがアクティブでパートナーノードにデータを転送できます。前回のテイクオーバーの試行が中止されました。パートナーの一部の SFO アグリゲートがローカルノードで所有されています。</p> <ul style="list-style-type: none"> <li>残りの SFO アグリゲートをテイクオーバーする場合は、- bypass - optimization パラメータを true に設定して、パートナーノードのテイクオーバーを再発行するか、再配置されたアグリゲートを戻す場合はパートナーのギブバックを実行します。</li> </ul>
<p>partner_name を待機しています前回のテイクオーバーの試行が理由で中止されました。パートナーの一部の SFO アグリゲートがローカルノードで所有されています。</p> <p>残りのアグリゲートをテイクオーバーする場合は「-bypass -optimization」パラメータを true に設定して、パートナーのテイクオーバーをもう一度実行します。再配置されたアグリゲートを戻す場合は、パートナーのギブバックを問題に設定します。</p>	<p>ローカルノードとパートナーノードの間で、HA インターコネクトを介して情報を交換できません。前回のテイクオーバーの試行が reason で示された理由により中止されました。パートナーの一部の SFO アグリゲートがローカルノードで所有されています。</p> <ul style="list-style-type: none"> <li>残りの SFO アグリゲートをテイクオーバーする場合は、- bypass - optimization パラメータを true に設定して、パートナーノードのテイクオーバーを再発行するか、再配置されたアグリゲートを戻す場合はパートナーのギブバックを実行します。</li> </ul>
<p>partner_name を待機しています前回のテイクオーバーの試行が中止されました。パートナーの一部の SFO アグリゲートがローカルノードで所有されています。</p> <p>残りのアグリゲートをテイクオーバーする場合は「-bypass -optimization」パラメータを true に設定して、パートナーのテイクオーバーをもう一度実行します。再配置されたアグリゲートを戻す場合は、パートナーのギブバックを問題に設定します。</p>	<p>ローカルノードとパートナーノードの間で、HA インターコネクトを介して情報を交換できません。前回のテイクオーバーの試行が中止されました。パートナーの一部の SFO アグリゲートがローカルノードで所有されています。</p> <ul style="list-style-type: none"> <li>残りの SFO アグリゲートをテイクオーバーする場合は、- bypass - optimization パラメータを true に設定して、パートナーノードのテイクオーバーを再発行するか、再配置されたアグリゲートを戻す場合はパートナーのギブバックを実行します。</li> </ul>
<p>partner_name に接続されています。ローカルノードでディスクファームウェアのバックグラウンド更新（BDFU）に失敗したため、前回のテイクオーバーの試行が中止されました。</p>	<p>HA インターコネクトがアクティブでパートナーノードにデータを転送できます。ローカルノードでのディスクファームウェアのバックグラウンド更新が無効になっていたため、前回のテイクオーバーの試行が中止されました。</p>
<p>partner_name に接続されています。前回のテイクオーバーの試行が理由で中止されました。</p>	<p>HA インターコネクトがアクティブでパートナーノードにデータを転送できます。前回のテイクオーバーの試行が reason で示された理由により中止されました。</p>

partner_name を待機しています前回のテイクオーバーの試行が理由で中止されました。	ローカルノードとパートナーノードの間で、HA インターコネクトを介して情報を交換できません。前回のテイクオーバーの試行が reason で示された理由により中止されました。
partner_name に接続されています。partner_name による前回のテイクオーバーの試行が reason で示された理由により中止されました。	HA インターコネクトがアクティブでパートナーノードにデータを転送できます。パートナーノードによる前回のテイクオーバーの試行が reason で示された理由により中止されました。
partner_name に接続されています。partner_name による前回のテイクオーバーの試行が中止されました。	HA インターコネクトがアクティブでパートナーノードにデータを転送できます。パートナーノードによる前回のテイクオーバーの試行が中止されました。
partner_name を待機していますpartner_name による前回のテイクオーバーの試行が reason で示された理由により中止されました。	ローカルノードとパートナーノードの間で、HA インターコネクトを介して情報を交換できません。パートナーノードによる前回のテイクオーバーの試行が reason で示された理由により中止されました。
前回のギブバックがモジュールで失敗しました：module name。number of seconds で示された秒数以内に自動ギブバックが開始されます。	<p>前回のギブバックの試行が module_name で示されたモジュールで失敗しました。秒数で自動ギブバックが開始されます。</p> <ul style="list-style-type: none"> <li>• を実行します storage failover show-giveback 詳細については、コマンドを参照してください。</li> </ul>
コントローラの無停止アップグレード手順の一環として、ノードがパートナーのアグリゲートを所有します。	コントローラの無停止アップグレードを実行中の手順があるため、パートナーのアグリゲートがノードで所有されています。
partner_name に接続されています。クラスタ内の別のノードに属するアグリゲートがノードで所有されています。	HA インターコネクトがアクティブでパートナーノードにデータを転送できます。クラスタ内の別のノードに属するアグリゲートがノードで所有されています。
partner_name に接続されています。パートナーロックの同期を待っています。	HA インターコネクトがアクティブでパートナーノードにデータを転送できます。パートナーロックの同期が完了するのを待っています。
partner_name に接続されています。ローカルノードでクラスタのアプリケーションがオンラインになるのを待っています。	HA インターコネクトがアクティブでパートナーノードにデータを転送できます。ローカルノードでクラスタのアプリケーションがオンラインになるのを待っています。

非 HA モードでは、NVRAM をすべて使用するにはリブートしてください。	<p>ストレージフェイルオーバーを実行できません。HA モードのオプションが <code>non_ha</code> に設定されています。</p> <ul style="list-style-type: none"> <li>ノードの NVRAM をすべて使用できるようにするには、ノードをリブートする必要があります。</li> </ul>
非 HA モード。ノードをリブートして HA をアクティブ化します。	<p>ストレージフェイルオーバーを実行できません。</p> <ul style="list-style-type: none"> <li>HA 機能を有効にするには、ノードをリブートする必要があります。</li> </ul>
非 HA モード。	<p>ストレージフェイルオーバーを実行できません。HA モードのオプションが <code>non_ha</code> に設定されています。</p> <ul style="list-style-type: none"> <li>を実行する必要があります <code>storage failover modify -mode ha -node nodename</code> HAペアの両方のノードでコマンドを実行し、ノードをリブートしてHA機能を有効にします。</li> </ul>

## ストレージフェイルオーバーを有効または無効にするコマンド

ストレージフェイルオーバー機能を有効または無効にするには、次のコマンドを使用します。

状況	使用するコマンド
テイクオーバーを有効にする	<code>storage failover modify -enabled true -node nodename</code>
テイクオーバーを無効にする	<code>storage failover modify -enabled false -node nodename</code>



ストレージフェイルオーバーを無効にするのは、メンテナンス手順の一部として必要な場合にのみしてください。

## 2 ノードクラスタでテイクオーバーを開始せずにノードを停止またはリブートします

ノードまたはシェルフで特定のハードウェアのメンテナンスを実施し、パートナーノードを稼働させて停止時間を制限する場合は、テイクオーバーを開始せずに、2ノードクラスタ内のノードを停止またはリブートします。また、手動テイクオーバーを実行できない問題がある場合に、パートナーノードのアグリゲートを稼働させてデータを提供したいときも、また、テクニカルサポートから問題のトラブルシューティングを依頼された場合は、その一環としてこの手順を実行しなければならないことがあります。

このタスクについて

- テイクオーバーを抑制する前に（を使用して） `-inhibit-takeover true` パラメータ）を指定した場合は、クラスタHAを無効にします。



- クラスタHAは、2ノードクラスタの一方のノードで障害が発生してもクラスタが無効にならないようにする機能です。ただし、を使用する前にクラスタHAを無効にしない場合 `-inhibit-takeover true` パラメータを指定すると、両方のノードがデータの提供を停止します
- クラスタHAを無効にする前にノードを停止またはリブートしようとする、ONTAP から警告が表示され、クラスタHAを無効にするように指示されます。

- オンラインのままにするパートナーノードにLIF（論理インターフェイス）を移行します。
- 停止またはリブートするノードに保持しておくアグリゲートがある場合は、オンラインのままにするノードに移動します。

#### 手順

1. 両方のノードが正常であることを確認します。

```
cluster show
```

両方のノードで、 `true` に表示されます Health 列（Column）：

```
cluster::> cluster show
Node           Health  Eligibility
-----
node1          true   true
node2          true   true
```

2. 停止またはリブートするノードからすべてのLIFをパートナーノードに移行します。  
`network interface migrate-all -node node_name`
3. ノードで停止またはリブートするノードが停止したときにオンラインのままにするアグリゲートがある場合は、そのアグリゲートをパートナーノードに再配置します。それ以外の場合は、次の手順に進みます。
  - a. 停止またはリブートするノード上のアグリゲートを表示します。  
`storage aggregates show -node node_name`

たとえば、node1は停止またはリブートするノードです。

```
cluster::> storage aggregates show -node node1
Aggregate  Size  Available  Used%  State  #Vols  Nodes  RAID
Status
-----  ----  -
aggr0_node_1_0
          744.9GB   32.68GB   96% online      2 node1  raid_dp,
normal
aggr1      2.91TB    2.62TB   10% online     8 node1  raid_dp,
normal
aggr2      4.36TB    3.74TB   14% online    12 node1  raid_dp,
normal
test2_aggr 2.18TB    2.18TB    0% online     7 node1  raid_dp,
normal
4 entries were displayed.
```

b. アグリゲートをパートナーノードに移動します。

```
storage aggregate relocation start -node node_name -destination node_name
-aggregate-list aggregate_name
```

たとえば、アグリゲートaggr1、aggr2、test2\_aggrは、node1からnode2に移動されます。

```
storage aggregate relocation start -node node1 -destination node2 -aggregate
-list aggr1,aggr2,test2_aggr
```

4. クラスタHAを無効にします。

```
cluster ha modify -configured false
```

HAが無効になっていることを示す出力が表示されます。Notice: HA is disabled



この処理ではストレージフェイルオーバーは無効になりません。

5. 該当するコマンドを使用して、ターゲットノードを停止またはリブートしてテイクオーバーを抑制します。

```
° system node halt -node node_name -inhibit-takeover true
```

```
° system node reboot -node node_name -inhibit-takeover true
```



コマンド出力に、続行するかどうかを確認する警告が表示されます。と入力します y。

6. オンラインのノードが健全な状態（パートナーが停止している状態）であることを確認します。

```
cluster show
```

オンラインノードの場合は、true に表示されます Health 列 (Column) :



コマンドの出力に、クラスタHAが構成されていないことを示す警告が表示されます。この警告は無視してかまいません。

7. ノードの停止またはリブートに必要な操作を実行します。
8. オフラインになったノードをLOADERプロンプトからブートします。

```
boot_ontap
```

9. 両方のノードが正常であることを確認します。

```
cluster show
```

両方のノードで、true に表示されます Health 列 (Column) :



コマンドの出力に、クラスタHAが構成されていないことを示す警告が表示されます。この警告は無視してかまいません。

10. クラスタHAを再度有効にします。
11. この手順 で以前にパートナーノードにアグリゲートを再配置した場合は、アグリゲートをホームノードに戻します。それ以外の場合は、次の手順に進みます。

```
cluster ha modify -configured true  
storage aggregate relocation start -node node_name -destination node_name  
-aggregate-list aggregate_name
```

たとえば、アグリゲートaggr1、aggr2、およびtest2\_aggrをノードnode2からノードnode1に移動します。

```
storage aggregate relocation start -node node2 -destination node1 -aggregate  
-list aggr1,aggr2,test2_aggr
```

12. LIFをそれぞれのホームポートにリバートします。
  - a. ホームにないLIFを表示します。

```
network interface show -is-home false
```
  - b. 停止しているノードから移行されなかったホーム以外のLIFがある場合は、リバート前に移動しても安全であることを確認してください。
  - c. 安全な場合は、すべてのLIFをホームに戻します。

```
network interface revert *
```

## System Manager を使用した REST API の管理

### System Manager を使用した REST API の管理

REST API ログには、System Manager から ONTAP に発行される API 呼び出しが記録されます。このログを使用して、ONTAP のさまざまな管理タスクを実行するために必要な呼び出しの性質と順序を把握できます。

## System Manager での REST API および API ログの使用方法

System Manager から ONTAP への REST API 呼び出しは、いくつかの方法で実行されます。

**System Manager 問題 API** は、で呼び出します

System Manager で ONTAP REST API 呼び出しを実行する際の最も重要な例を次に示します。

### 自動ページ更新

System Manager は API 呼び出しをバックグラウンドで自動的に実行して、ダッシュボードページなどの情報を更新します。

### ユーザーごとにアクションを表示します

特定のストレージリソースまたはリソースの集合を System Manager の UI で表示すると、1 つ以上の API 呼び出しが実行されます。

### アクションをユーザーごとに更新します

ONTAP リソースを System Manager UI で追加、変更、または削除すると、API 呼び出しが実行されます。

### API 呼び出しを再発行する

ログエントリをクリックして、API 呼び出しを手動で再発行することもできます。呼び出しの JSON 出力が表示されます。


### 詳細情報

- ["ONTAP 9 自動化に関するドキュメント"](#)

## REST API ログへのアクセス

System Manager から実行された ONTAP REST API 呼び出しのレコードを含むログにアクセスできます。ログを表示する際には、API 呼び出しの再発行と出力の確認も行うことができます。

### 手順

1. ページの上部で、をクリックします  をクリックして REST API ログを表示します。  
ページの下部に最新のエントリが表示されます。
2. 左側の \* dashboard \* をクリックして、ページを更新するために発行された API 呼び出しに対して新しく作成されるエントリを確認します。
3. storage \* をクリックし、\* qtrees \* をクリックします。  
その結果、問題 System Manager で特定の API 呼び出しを実行して qtree のリストを取得できるようになります。
4. 次の形式の API 呼び出しを説明するログエントリを探します。

GET /api/storage/qtrees

エントリには、などの追加のHTTPクエリパラメータが含まれています max\_records。

5. ログエントリをクリックして GET API 呼び出しを再発行し、raw JSON 出力を表示します。

例

```
{
  "records": [
    {
      "svm": {
        "uuid": "19507946-e801-11e9-b984-00a0986ab770",
        "name": "SMQA",
        "_links": {
          "self": {
            "href": "/api/svm/svms/19507946-e801-11e9-b984-00a0986ab770"
          }
        }
      },
      "volume": {
        "uuid": "1e173258-f98b-11e9-8f05-00a0986abd71",
        "name": "vol_vol_test2_dest_dest",
        "_links": {
          "self": {
            "href": "/api/storage/volumes/1e173258-f98b-11e9-8f05-00a0986abd71"
          }
        }
      },
      "id": 1,
      "name": "test2",
      "security_style": "mixed",
      "unix_permissions": 777,
      "export_policy": {
        "name": "default",
        "id": 12884901889,
        "_links": {
          "self": {
            "href": "/api/protocols/nfs/export-policies/12884901889"
          }
        }
      },
      "path": "/vol_vol_test2_dest_dest/test2",
      "_links": {
        "self": {
```



```
      "href": "/api/storage/qtrees/1e173258-f98b-11e9-8f05-00a0986abd71/1"
    }
  },
],
"num_records": 1,
"_links": {
  "self": {
    "href":
"/api/storage/qtrees?max_records=20&fields=*&name=!%22%22"
  }
}
```

# ボリューム管理

## ボリュームと LUN の管理には **System Manager** を使用します

### System Manager によるボリューム管理の概要

ONTAP 9.7 以降では、FlexVol ボリュームや LUN、qtree、Storage Efficiency、クォータなどの論理ストレージを System Manager で管理できます。

従来の System Manager（ONTAP 9.7 以前でのみ使用可能）を使用している場合は、[を参照してください "論理ストレージを管理する"](#)

### ボリュームを管理します

#### ボリュームの管理の概要

System Manager にボリュームのリストを表示したら、さまざまな操作を実行してボリュームを管理できます。



#### 手順

1. System Manager で、\* Storage > Volumes（ボリューム）\* をクリックします。

ボリュームのリストが表示されます。

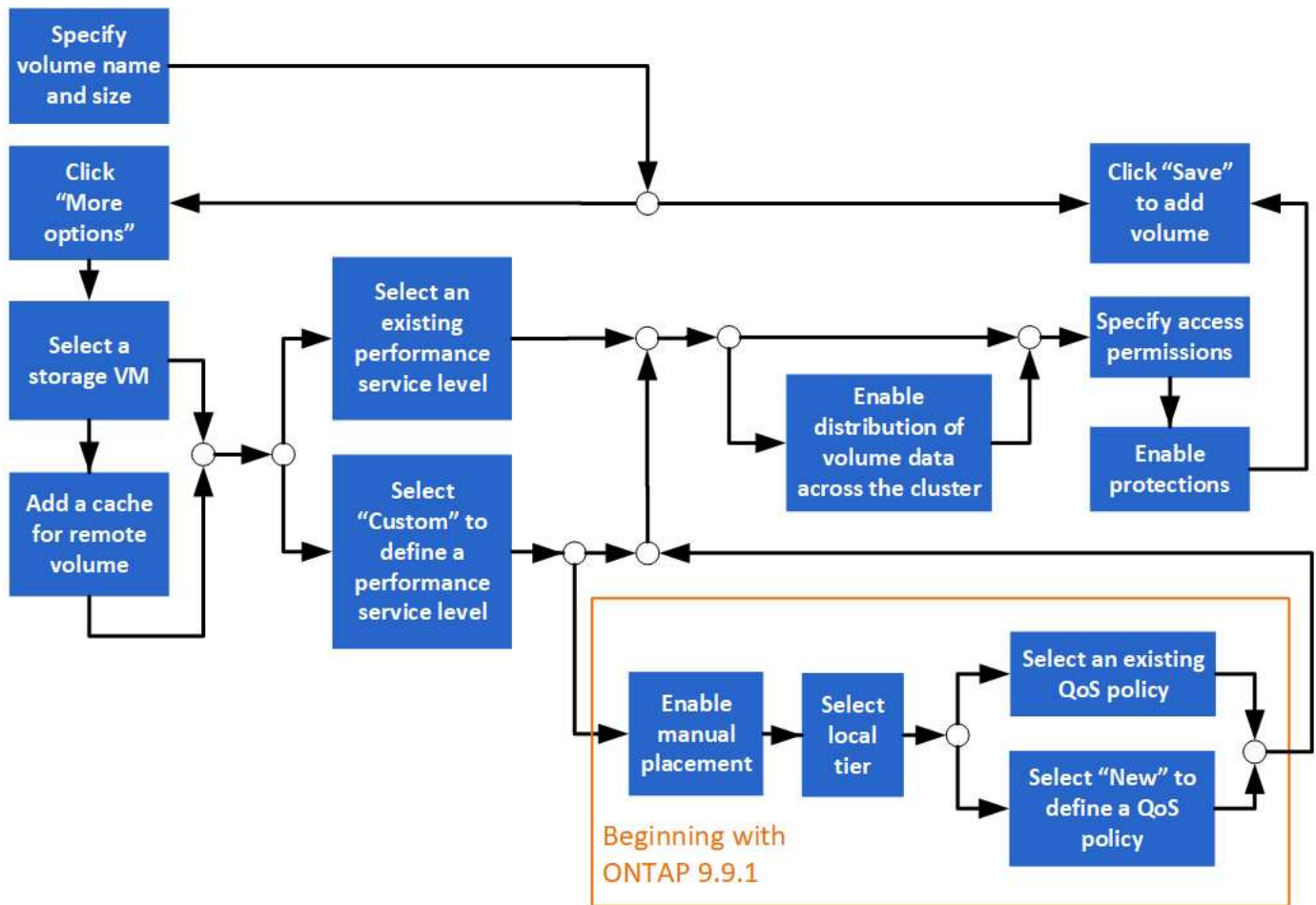
2. 次の操作を実行できます。

このタスクを実行します。	対処方法
ボリュームを追加します	をクリックします  <b>Add</b> 。を参照してください " <a href="#">ボリュームを追加します</a> "。
複数のボリュームを管理	<p>ボリュームの横にあるチェックボックスをオンにします。</p> <ul style="list-style-type: none"><li>• をクリックします  <b>Delete</b> をクリックして、選択したボリュームを削除します</li><li>• をクリックします  <b>Protect</b> をクリックして、選択したボリュームに保護ポリシーを割り当てます。</li><li>• をクリックします  <b>More</b> アイコン"] 選択したすべてのボリュームに対して次のいずれかの操作を実行します。<ul style="list-style-type: none"><li>◦ クォータを有効にします</li><li>◦ オフラインにする</li><li>◦ 移動</li><li>◦ 削除したボリュームを表示します</li></ul></li></ul>

1つのボリュームを管理します	<p>ボリュームの横にあるをクリックします  をクリックし、次のいずれかの操作を選択して実行します。</p> <ul style="list-style-type: none"> <li>• 編集</li> <li>• サイズ変更（ONTAP 9.10.1 以降、オンラインボリュームと DP FlexVol ボリュームのみ）</li> <li>• 削除</li> <li>• クローン</li> <li>• オフライン化（オンライン化）</li> <li>• クォータの有効化（またはクォータの無効化）</li> <li>• エクスポートポリシーを編集します</li> <li>• マウントパスを編集します</li> <li>• 移動</li> <li>• クラウド階層の設定を編集します</li> <li>• 保護</li> </ul>
ボリュームの名前を変更します	<p>概要ページでボリュームの名前を変更できます。</p> <p>をクリックします  をクリックし、ボリューム名を変更します。</p>

ボリュームを追加します

ボリュームを作成して、NFSサービスまたはSMBサービス用に設定された既存のStorage VMに追加できます。



作業を開始する前に

- NFS サービスまたは SMB サービス用に設定された Storage VM がクラスタに存在する必要があります。
- ONTAP 9.13.1以降では、新しいボリュームに対して容量分析とアクティビティ追跡をデフォルトで有効にすることができます。System Managerでは、クラスタレベルまたはStorage VMレベルでデフォルト設定を管理できます。詳細については、を参照してください [File System Analytics](#) を有効にします。

手順

1. [ストレージ]>[ボリューム]に移動します。
2. 選択するオプション **+ Add**。
3. ボリュームの名前とサイズを指定します。
4. 次のいずれかの手順を実行します。

選択するボタン	実行する処理
* 保存 *	ボリュームが作成され、システムのデフォルトを使用して追加されます。追加の手順は必要ありません。
* その他のオプション *	に進みます <a href="#">[step5]</a> ボリュームの仕様を定義します。

5. [\[\[step5、 Step 5\]](#) ボリュームの名前とサイズを指定した場合は、それらが表示されます。それ以外の場合は、名前とサイズを入力します。
6. プルダウンリストから Storage VM を選択します。

NFS プロトコルが設定されている Storage VM のみが表示されます。NFS プロトコルが設定された Storage VM が 1 つしかない場合、「\* Storage VM \*」フィールドは表示されません。

7. リモートボリュームのキャッシュを追加するには、\* リモートボリュームのキャッシュを追加 \* を選択し、次の値を指定します。
  - クラスタを選択
  - Storage VM を選択してください。
  - キャッシュボリュームにするボリュームを選択します。
8. ストレージと最適化 \* セクションで、次の値を指定します。
  - a. ボリュームの容量はすでに表示されていますが、変更することはできます。
  - b. [パフォーマンスサービスレベル \*] フィールドで、サービスレベルを選択します。

選択するサービスレベル	発生する処理
「最高レベル」、「パフォーマンス」、「バリュー」などの既存のサービスレベル。  システムプラットフォームに有効なサービスレベル（AFF、FAS など）のみが表示されます。	ローカル階層が自動的に選択されます。に進みます <a href="#">[step9]</a> 。
カスタム	に進みます <a href="#">[step8c]</a> 新しいサービスレベルを定義します。

- c. [\[\[step8c、手順8c\]\]](#) ONTAP 9.9.1以降では、System Managerを使用して、ボリュームを配置するローカル階層を手動で選択できます（サービスレベルが「カスタム」を選択している場合）。



このオプションは、リモートボリュームのキャッシュとして \* 追加を選択した場合、または \* ボリュームデータをクラスタに分散した場合には使用できません \*（以下を参照）。

選択内容	実行する手順
* 手動配置 *	手動配置が有効になっています。 *Distribute volume data across the cluster * selection（* ボリュームデータのクラスタへの分散）が無効になっています（以下を参照）。に進みます <a href="#">Step 8d</a> をクリックしてプロセスを完了します。
選択なし	手動配置が有効になっていません。ローカル階層が自動的に選択されます。に進みます <a href="#">[step9]</a> 。

- a. プルダウンメニューからローカル階層を選択します。
- b. QoS ポリシーを選択します。

「既存」を選択して既存のポリシーのリストから選択するか、「新規」を選択して新しいポリシーの仕様を入力します。

9. [\[\[step9、Step 9\] \\* Optimization options \\* セクションで、ボリュームデータをクラスタ全体に分散するかどうかを決定します。](#)

選択内容	発生する処理
* ボリュームデータをクラスタ全体に分散 *	追加するボリュームが FlexGroup ボリュームになります。このオプションは、以前に * 手動配置 * を選択した場合は使用できません。
選択なし	追加するボリュームは、デフォルトで FlexVol ボリュームになります。

10. アクセス権限 \* セクションで、ボリュームを構成するプロトコルのアクセス権限を指定します。

ONTAP 9.11.1以降では、新しいボリュームをデフォルトで共有できません。デフォルトのアクセス権限を指定するには、次のチェックボックスをオンにします。

- **NGS**によるエクスポート:ユーザーにデータへのフル・アクセスを許可するデフォルトのエクスポート・ポリシーを使用してボリュームを作成します
- \* SMB/CIFSで共有\*: 名前が自動生成されて編集可能な共有を作成します。アクセス権は「Everyone」に付与されます。また、権限レベルを指定することもできます。

11. 「\* 保護」セクションで、ボリュームの保護を指定します。

- ONTAP 9.12.1以降では、デフォルトを使用する代わりに、\*[Snapshotコピーを有効にする（ローカル）]\*を選択し、Snapshotコピーポリシーを選択できます。
- SnapMirror を有効にする（ローカルまたはリモート）\*を選択する場合は、プルダウンリストからデスティネーションクラスタの保護ポリシーと設定を指定します。

12. [ 保存（ Save ） ] を選択します。

ボリュームが作成され、クラスタと Storage VM に追加されます。



このボリュームの仕様は Ansible Playbook に保存することもできます。詳細については、[を参照してください "Ansible Playbook を使用して、ボリュームや LUN を追加、編集できます"](#)。

ボリュームへのタグの割り当て

ONTAP 9.14.1以降では、System Managerを使用してボリュームにタグを割り当て、プロジェクトやコストセンターなど、あるカテゴリに属するオブジェクトを識別することができます。

このタスクについて

ボリュームにタグを割り当てることができます。まず、タグを定義して追加する必要があります。その後、タグを編集または削除することもできます。

タグは、ボリュームの作成時に追加することも、あとから追加することもできます。

タグを定義するには、キーを指定し、"key:value"の形式で値に関連付けます。たとえば、「dept:engineering」や「location:san-jose」などです。

タグを作成するときは、次の点を考慮する必要があります。

- キーの長さは1文字以上で、nullにすることはできません。 値にはnullを指定できます。
- キーは、値をカンマで区切って複数の値とペアにすることができます（例："location:san-jose, Toronto"）。
- タグは複数のリソースに使用できます。
- キーの先頭は小文字にする必要があります。
- ボリュームに割り当てられているタグは、ボリュームを削除すると削除されます。
- ボリュームがリカバリキューからリカバリされた場合、タグはリカバリされません。
- タグは、ボリュームを移動またはクローニングしても保持されます。
- ディザスタリカバリ関係でStorage VMに割り当てられたタグは、パートナーサイトのボリュームにレプリケートされます。

## 手順


タグを管理するには、次の手順を実行します。

1. System Managerで、\*[ボリューム]\*をクリックし、タグを追加するボリュームを選択します。

タグは\* Tags \*セクションに表示されます。

2. [タグの管理]\*をクリックして、既存のタグを変更するか、新しいタグを追加します。

タグを追加、編集、または削除できます。

実行する処理	実行する手順
タグの追加	<ol style="list-style-type: none"> <li>a. [タグの追加]*をクリックします。</li> <li>b. キーとその値を指定します（複数の値はカンマで区切ります）。</li> <li>c. [保存（Save）]をクリックします。</li> </ol>
タグの編集	<ol style="list-style-type: none"> <li>a. 「* Key」および「Values（オプション）*」フィールドの内容を変更します。</li> <li>b. [保存（Save）]をクリックします。</li> </ol>
タグを削除します	<ol style="list-style-type: none"> <li>a. をクリックします  をクリックします。</li> </ol>

## 削除したボリュームをリカバリします

FlexVol ボリュームを誤って削除した場合は、System Manager を使用してそれらのボリュームをリカバリできます。ONTAP 9.8 以降では、System Manager を使用して FlexGroup ボリュームをリカバリすることもできます。ボリュームをページして永続的に削除することもできます。

ボリューム保持期限は Storage VM レベルで設定できます。デフォルトでは、ボリュームの保持期間は 12 時間に設定されています。

削除したボリュームを選択する

#### 手順

1. [ ストレージ ]、[ ボリューム ] の順にクリックします。
2. [ 詳細 ]、[ 削除されたボリュームを表示する \* ] の順にクリックし
3. ボリュームを選択し、目的の操作をクリックして、ボリュームをリカバリまたは完全に削除します。

ボリューム設定をリセットしています

ボリュームを削除すると、そのボリュームに関連付けられている設定が削除されます。ボリュームをリカバリしても、すべての構成がリセットされるわけではありません。ボリュームを元の状態に戻すには、ボリュームのリカバリ後に次のタスクを手動で実行します。

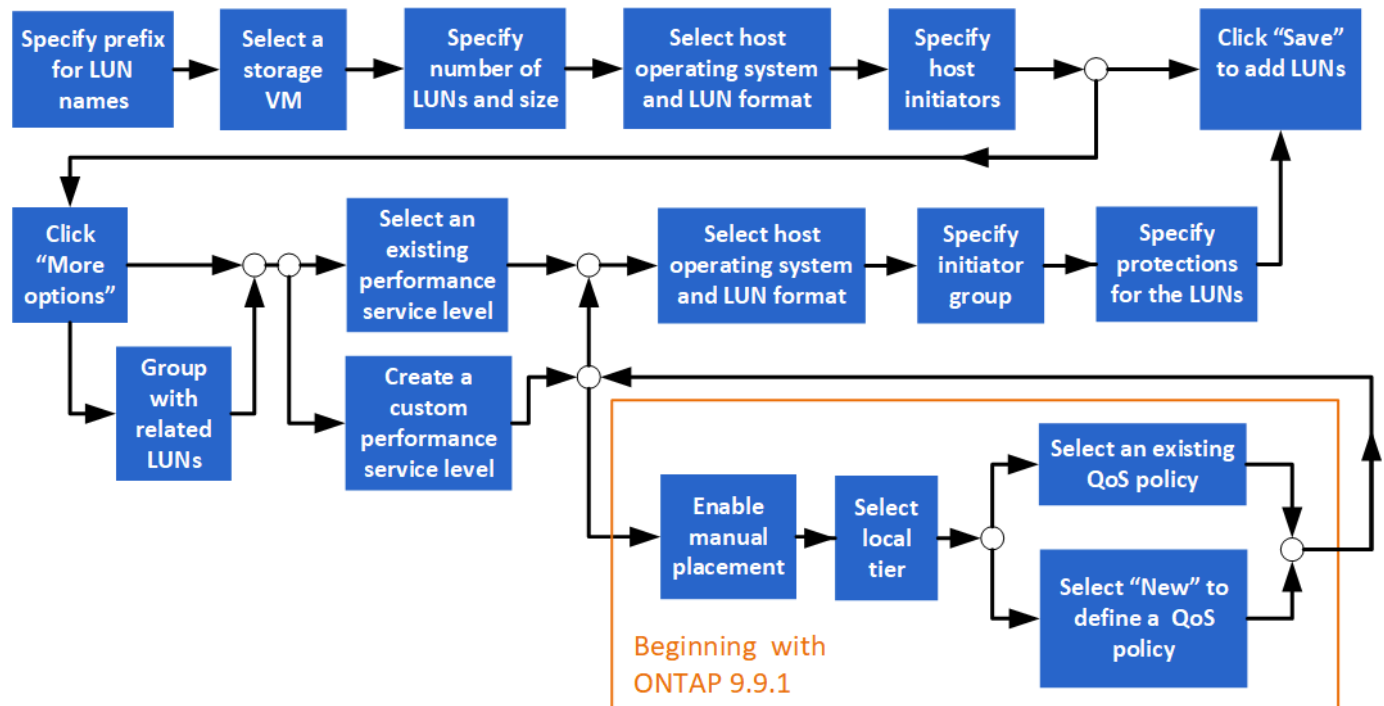
#### 手順

1. ボリュームの名前を変更します。
2. ジャンクションパス（NAS）を設定する。
3. ボリューム内の LUN に対するマッピングの作成（SAN）
4. Snapshot ポリシーとエクスポートポリシーをボリュームに関連付けます。
5. ボリュームの新しいクォータポリシールールを追加します。
6. ボリュームの QoS ポリシーを追加します。

## LUNを管理します

LUN を作成し、SAN プロトコルが設定されている既存の Storage VM に追加できます。LUNをグループ化したり、名前を変更したりすることもできます。

#### LUN を追加します





始める前に

SAN サービス用に設定された Storage VM がクラスタに存在する必要があります。

手順

1. [\* ストレージ] > [LUN] に移動します。
2. をクリックします **+ Add**。
3. 各 LUN 名の先頭に使用するプレフィックスを指定します。（LUN を 1 つだけ作成する場合は、LUN 名を入力します）。
4. プルダウンリストから Storage VM を選択します。

SAN プロトコル用に設定されている Storage VM のみが表示されます。SAN プロトコル用に設定されている Storage VM が 1 つしかない場合、「\* Storage VM \*」フィールドは表示されません。

5. 作成する LUN の数と各 LUN のサイズを指定します。
6. プルダウンリストからホストのオペレーティングシステムと LUN の形式を選択します。
7. ホストイニシエータを入力する場合は、カンマで区切ります。
8. 次のいずれかを実行します。

クリックするボタン	実行する処理
* 保存 *	入力した仕様で LUN が作成されます。その他の仕様では、システムのデフォルト設定が使用されます。追加の手順は必要ありません。
* その他のオプション *	に進みます <a href="#">[step9-define-add-specs]</a> LUN の詳細な仕様を定義します。

9. [\[step9-define-add-specs、Step 9\]](#)：以前にLUNプレフィックスを入力した場合はすでにLUNプレフィックスが表示されますが、変更することができます。それ以外の場合は、プレフィックスを入力します。

10. プルダウンリストから Storage VM を選択します。

SAN プロトコル用に設定されている Storage VM のみが表示されます。SAN プロトコル用に設定されている Storage VM が 1 つしかない場合、「\* Storage VM \*」フィールドは表示されません。

11. LUN をグループ化する方法を決定します。

選択内容	発生する処理
* 関連する LUN* でグループ化します	Storage VM 上の既存のボリューム上の関連する LUN と LUN がグループ化されます。
選択なし	LUN は、「container」と呼ばれるボリュームにグループ化されます。

12. ストレージと最適化 \* セクションで、次の値を指定します。

- a. 以前に入力した LUN の数と容量は、すでに表示されていますが、変更することもできます。それ以外の場合は、値を入力します。
- b. [パフォーマンスサービスレベル \*] フィールドで、サービスレベルを選択します。

選択するサービスレベル	発生する処理
-------------	--------

「最高レベル」、「パフォーマンス」、「バリュー」などの既存のサービスレベル。  システムプラットフォームに有効なサービスレベル（AFF、FAS など）のみが表示されます。	ローカル階層が自動的に選択されます。に進みます <a href="#">[step13]</a> 。
カスタム	に進みます <a href="#">[step12c]</a> 新しいサービスレベルを定義します。

- c. [\[\[step12c、手順12c\]\]](#) ONTAP 9.9.1以降では、System Managerを使用して、作成するLUNを配置するローカル階層を手動で選択できます（「カスタム」サービスレベルを選択した場合）。

選択内容	実行する手順
* 手動配置 *	手動配置が有効になっています。に進みます <a href="#">Step 12D</a> をクリックしてプロセスを完了します。
選択なし	手動選択が有効になっていません。ローカル階層が自動的に選択されます。に進みます <a href="#">[step13]</a> 。

- d. プルダウンメニューからローカル階層を選択します。

- e. QoS ポリシーを選択します。

「既存」を選択して既存のポリシーのリストから選択するか、「新規」を選択して新しいポリシーの仕様を入力します。

13. [\[\[step13、Step 13\]\]](#) 「\* Host Information \*」セクションには、ホストオペレーティングシステムと LUN 形式はすでに表示されていますが、変更することができます。

14. [\[\\* Host Mapping\]](#) で、LUN のイニシエータのタイプを選択します。

- 既存のイニシエータグループ：表示するイニシエータグループを選択します。
- 既存のイニシエータグループを使用する新しいイニシエータグループ：新しいグループの名前を指定し、新しいグループの作成に使用するグループを選択します。
- \* ホストイニシエータ \*：新しいイニシエータグループから名前を指定し、\* + イニシエータの追加 \* をクリックしてイニシエータをグループに追加します。

15. 「\* Protection \*」セクションで、LUN の保護を指定します。

SnapMirror を有効にする（ローカルまたはリモート）\* を選択する場合は、プルダウンリストからデステイネーションクラスタの保護ポリシーと設定を指定します。

16. [\[保存（Save）\]](#) をクリックします。

LUN が作成され、クラスタと Storage VM に追加されます。




また、これらの LUN の仕様を Ansible Playbook に保存することもできます。詳細については、[を参照してください "Ansible Playbook を使用して、ボリュームや LUN を追加、編集できます"](#)。

## LUNの名前を変更する

概要ページでLUNの名前を変更できます。

### 手順

1. System Managerで、\*[LUN]\*をクリックします。
2. をクリックします  をクリックし、LUN名を変更します。
3. [ 保存 ( Save ) ] をクリックします。

## ストレージを拡張する

System Manager を使用してボリュームまたは LUN のサイズを拡張し、ホストが使用できるスペースを増やすことができます。LUN のサイズが包含ボリュームのサイズを超えることはできません。

ONTAP 9.12.1以降では、ボリュームの新しい容量を入力すると、\*ボリュームのサイズ変更\*ウィンドウに、ボリュームのサイズ変更がデータスペースとSnapshotコピーリザーブに与える影響が表示されます。

- [\[ボリュームのサイズを拡張する\]](#)
- [LUN のサイズを拡張する](#)


また、既存のボリュームに LUN を追加することもできます。 ONTAP 9.7 または 9.8 で System Manager を使用する場合は、プロセスが異なります

- [既存のボリュームへの LUN の追加 \( ONTAP 9.7 \)](#)
- [既存のボリュームへのLUNの追加 \(ONTAP 9.8\)](#)

また、ONTAP 9.8 以降では、System Manager を使用して既存のボリュームに LUN を追加できます。


## ボリュームのサイズを拡張する

### 手順

1. [ ストレージ ]、[ ボリューム ] の順にクリックします。
2. サイズを拡張するボリュームの名前にカーソルを合わせます。
3. をクリックします .
4. 「 \* 編集 \* 」を選択します。
5. 容量値を増やします。
6. 既存の\*および新しい\*データスペースとSnapshotリザーブの詳細を確認します。

## LUN のサイズを拡張する

### 手順

1. [\*Storage] > [LUNs] をクリックします。
2. サイズを拡張する LUN の名前にカーソルを合わせます。
3. をクリックします .

4. 「\* 編集 \*」を選択します。
5. 容量値を増やします。

#### 既存のボリュームへの LUN の追加（ONTAP 9.7）

ONTAP 9.7 で System Manager を使用して既存のボリュームに LUN を追加するには、最初に従来のビューに切り替えてください。

##### 手順

1. ONTAP 9.7 で System Manager にログインします。
2. [クラシック表示（Classical View）] をクリックする。
3. Storage > LUNs > Create \* を選択します
4. LUN を作成するための詳細を指定します。
5. LUN を追加する既存のボリュームまたは qtree を指定します。

#### 既存のボリュームへの LUN の追加（ONTAP 9.8）

ONTAP 9.8 以降では、System Manager を使用して、すでに LUN が 1 つ以上ある既存のボリュームに LUN を追加できます。

##### 手順

1. [\*Storage] > [LUNs] をクリックします。
2. [\* 追加 +\*] をクリックします。
3. [Add LUNs] ウィンドウのフィールドに値を入力します。
4. [\* その他のオプション \*] を選択します。
5. 「Group with related LUN\*」チェックボックスを選択します。
6. ドロップダウンフィールドで、別の LUN を追加するボリューム上の LUN を選択します。
7. 残りのフィールドに入力します。\* Host Mapping \* の場合は、次のいずれかのオプションボタンをクリックします。
  - \* 既存のイニシエータグループ \* を使用すると、リストから既存のグループを選択できます。
  - \* 新しいイニシエータグループ \* を指定すると、フィールドに新しいグループを入力できます。

#### 圧縮、コンパクション、重複排除を使用してストレージスペースを節約します


AFF 以外のクラスタのボリュームでは、重複排除、データ圧縮、データコンパクションを一緒に、または個別に実行して、最善のスペース削減効果を得ることができます。

- 重複排除は重複したデータブロックを排除し、
- データ圧縮はデータブロックを圧縮して必要な物理ストレージ量を減らします。
- データコンパクションを実行すると、少ないスペースに多くのデータを格納できるようになり、ストレージ効率が向上します。



これらのタスクは、AFF 以外のクラスタ上のボリュームでサポートされます。ONTAP 9.2 以降では、インラインの Storage Efficiency 機能（インライン重複排除、インライン圧縮など）がすべて AFF でデフォルトで有効になります。

#### 手順

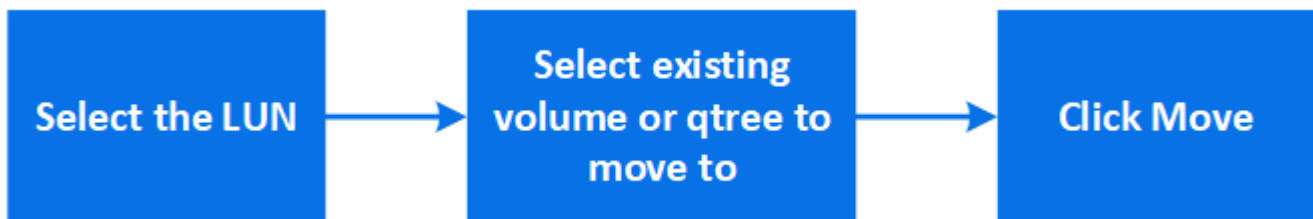
1. [ストレージ]、[ボリューム]の順にクリックします。
2. ストレージを保存するボリュームの名前の横にあるをクリックします .
3. 「\* Edit」をクリックし、「\* Storage Efficiency \*」までスクロールします。
4. \_オプション\_：バックグラウンド重複排除を有効にする場合は、チェックボックスがオンになっていることを確認します。
5. \_オプション\_：バックグラウンド圧縮を有効にする場合は、ストレージ効率化ポリシーを指定し、チェックボックスをオンにします。
6. \_オプション\_：インライン圧縮を有効にする場合は、チェックボックスがオンになっていることを確認します。

## LUN を移動して負荷を分散します

負荷を分散するために Storage VM 内の別のボリュームに LUN を移動したり、パフォーマンスサービスレベルが高いボリュームに LUN を移動してパフォーマンスを向上させることができます。

#### 移動の制限

- 同じボリューム内の qtree に LUN を移動することはできません。
- CLI を使用してファイルから作成された LUN は、System Manager では移動できません。
- オンラインでデータを提供している LUN は移動できません。
- デスティネーションボリュームに割り当てられているスペースに LUN を含めることができない場合は、LUN を移動できません（ボリュームで自動拡張が有効になっている場合も含む）。
- SnapLock ボリュームの LUN は、System Manager では移動できません。



#### 手順

1. [\*Storage] > [LUNs] をクリックします。
2. 移動する LUN を選択し、\* Move \* をクリックします。
3. LUN を移動する既存のボリュームを選択します。ボリュームに qtree が含まれている場合は、qtree を選択します。



移動処理の実行中は、移動元のボリュームと移動先のボリュームの両方に LUN が表示されます。

ボリュームを別の階層に移動して負荷を分散します

ONTAP 9.8 以降では、System Manager を使用してボリュームを別の階層に移動して負荷を分散できます。

ONTAP 9.9.1以降では、アクティブなデータストレージとアクセス頻度の低いデータストレージの分析に基づいてボリュームを移動することもできます。詳細については、を参照してください ["File System Analytics の概要"](#)。

手順

1. [ ストレージ ]、[ ボリューム ] の順にクリックします。
2. 移動する 1 つ以上のボリュームを選択し、\* 移動 \* をクリックします。
3. ボリュームを移動する既存の階層（アグリゲート）を選択します。

**Ansible Playbook** を使用して、ボリュームや **LUN** を追加、編集できます

ONTAP 9.9.1以降では、ボリュームまたはLUNを追加または編集するときに、System ManagerでAnsible Playbookを使用できます。

この機能を使用すると、同じ構成を複数回使用したり、ボリュームや LUN を追加または編集するときに構成をわずかに変更して同じ構成を使用したりできます。

**Ansible** プレイブックを有効または無効にします

System Manager で Ansible プレイブックの使用を有効または無効にすることができます。

手順

1. System Manager のクラスタ設定ページで、UI 設定に移動します。
  - クラスタ > 設定 \*
2. [\*UI 設定 \*] で、スライダスイッチを [ 有効 ] または [ 無効 ] に変更します。

ボリューム構成を **Ansible Playbook** に保存します

ボリュームの構成を作成または変更するときは、構成を Ansible Playbook ファイルとして保存できます。

手順

1. ボリュームを追加または編集します。

ボリューム>追加（または\*ボリューム>編集\*）
2. ボリュームの設定値を指定または編集します。
3. 「\* Save to Ansible Playbook \*」を選択して、構成を Ansible Playbook ファイルに保存してください。

次のファイルを含む zip ファイルがダウンロードされます。

- **variable.yaml**：ボリュームを追加または編集するために入力または変更した値。
- **volumeAdd.yaml**（または **volumeEdit.yaml**）：からの入力を読み取る時に値を作成または変更するために必要なテストケース variable.yaml ファイル。

## LUN の設定を **Ansible Playbook** に保存します

LUN の構成を作成または変更する場合は、構成を Ansible Playbook ファイルとして保存できます。

### 手順

1. LUN を追加または編集します。
  - lun> 追加 \*（または \* lun > 編集 \*）
2. LUN の設定値を指定または編集します。
3. Ansible Playbook に保存 \* を選択して、構成を Ansible Playbook ファイルに保存：


次のファイルを含む zip ファイルがダウンロードされます。

- **variable.yaml**：LUNを追加または編集するために入力または変更した値。
- **lunAdd.yaml**（または **lunEdit.yaml**）：からの入力を読み取る時に値を作成または変更するために必要なテストケース variable.yaml ファイル。

## グローバル検索結果から **Ansible Playbook** ファイルをダウンロードできます

グローバル検索を実行するときは、Ansible Playbook ファイルをダウンロードできます。

### 手順

1. 検索フィールドに、「volume」、「LUN」、または「Playbook」と入力します。
2. 検索結果は、「Volume Management（Ansible Playbook）」または「LUN Management（Ansible Playbook）」で確認できます。
3. をクリックします  Ansible Playbook ファイルをダウンロードできます。

## **Ansible Playbook** ファイルを利用できます

Ansible Playbook ファイルを変更して実行することで、ボリュームや LUN の構成を指定できます。

### このタスクについて

操作を実行するには、次の 2 つのファイル（「add」または「edit」）を使用します。

状況	使用する変数ファイル	使用する実行ファイル
ボリュームを追加します	volumeAdd-variable.yaml	valueAdd.yaml
ボリュームを編集します	volumeEdit-variable.yaml	volumeEdit.yaml
LUN を追加します	lunAdd-variable.yaml	lunAdd.yaml
LUN を編集します	lunEdit-variable.yaml	lunEdit.yaml

## 手順

1. 変数ファイルを変更します。

ファイルには、ボリュームまたは LUN の設定に使用するさまざまな値が含まれています。

- 値を変更しない場合は、コメントを付けたままにします。
- 値を変更する場合は、コメントを削除します。

2. 関連付けられた実行ファイルを実行します。

実行ファイルには、変数ファイルから入力を読み取るときに値を作成または変更するために必要なテストケースが含まれています。

3. ユーザログインクレデンシャルを入力します。

## ストレージ効率化ポリシーを管理します

ONTAP 9.8 以降では、System Manager を使用して、FAS システム上の Storage VM の効率化ポリシーを有効化、無効化、追加、編集、削除できます。



この機能は AFF システムでは使用できません。

## 手順

1. Storage > Storage VM\* を選択します
2. 効率化ポリシーを管理する Storage VM を選択してください。
3. [\* 設定 \*] タブで、を選択します → をクリックします。その Storage VM の効率化ポリシーが表示されます。

次のタスクを実行できます。

- \* 効率化ポリシーを有効または無効にするには、Status 列の切り替えボタンをクリックします。
- \* Add \* をクリックして効率化ポリシーを追加します。
- \* 編集 \* をクリックして効率化ポリシーを編集します : ポリシー名の右にある \* Edit \* を選択します。
- \* をクリックして、効率化ポリシーを削除します : をクリックし、\* Delete \* を選択します。

## 効率化ポリシーのリスト

- \* 自動 \*

重複排除がバックグラウンドで継続的に実行されるように指定します。このポリシーは、新規に作成するすべてのボリューム、およびアップグレードしたボリュームのうち、バックグラウンド重複排除が手動で設定されていないボリュームに対して設定されます。ポリシーをデフォルトまたはその他のポリシーに変更すると'auto'ポリシーは無効になります

ボリュームがAFF以外のシステムからAFF システムに移動した場合、デスティネーションノードで「auto」ポリシーがデフォルトで有効になります。ボリュームがAFF ノードからAFF以外のノードに移動すると、デフォルトでデスティネーションノードの「auto」ポリシーが「inline-only」ポリシーに置き換えられます。



- \* ポリシー \*

効率化ポリシーの名前を指定します。

- \* ステータス \*

効率化ポリシーのステータスを指定します。ステータスは、次のいずれかになります。

- 有効

効率化ポリシーを重複排除処理に割り当てることができるように指定します。

- 無効

効率化ポリシーが無効であることを示します。ポリシーを有効にするには、status ドロップダウンメニューを使用してポリシーを有効にし、あとで重複排除処理に割り当てることができます。

- \* 実行者 \*

ストレージ効率化ポリシーをスケジュールとしきい値（変更ログのしきい値）のどちらに基づいて実行するかを指定します。

- \* QoS ポリシー \*

ストレージ効率化ポリシーの QoS タイプを指定します。QoS タイプは、次のいずれかになります。

- 背景（Background）

QoS ポリシーをバックグラウンドで実行するように指定します。このタイプを使用すると、クライアント処理へのパフォーマンスの影響を軽減できます。

- ベストエフォート

QoS ポリシーをベストエフォートベースで実行するように指定します。これにより、システムリソースの利用率を最大限に高めることができます。

- \* 最大実行時間 \*

効率化ポリシーの最大実行時間を指定します。この値を指定しない場合は、処理が完了するまで効率化ポリシーが実行されます。

## 詳細領域

効率化ポリシーのリストの下領域には、選択した効率化ポリシーに関する追加情報が表示されます。スケジュールベースのポリシーのスケジュール名と詳細、およびしきい値ベースのポリシーのしきい値などが含まれます。

## クォータを使用してリソースを管理する

ONTAP 9.7 以降では、System Manager を使用して使用クォータを設定し、管理できます。

ONTAP CLIを使用して使用クォータを設定および管理する場合は、を参照してください "[Logical Storage Managementの略](#)"。

ONTAP 9.7 以前のリリースで OnCommand System Manager を使用して使用クォータを設定および管理する場合は、ご使用のリリースで次の項目を参照してください。

- "[ONTAP 9.6 および 9.7 ドキュメント](#)"
- "[ONTAP 9.5のドキュメント](#)"
- "[ONTAP 9.4ドキュメント](#)"
- "[ONTAP 9.3ドキュメント](#)"
- "[ONTAP 9.2 ドキュメントアーカイブ](#)"
- "[ONTAP 9.0ドキュメントアーカイブ](#)"

## クォータの概要

クォータを使用すると、ユーザ、グループ、または qtree によって使用されるディスクスペースやファイル数を制限したり、追跡したりできます。クォータは、特定のボリュームまたは qtree に適用されます。

クォータを使用して、ボリューム内のリソース使用量を追跡して制限したり、リソース使用量が特定のレベルに達したときに通知したりできます。

クォータには、ソフトクォータとハードクォータがあります。ソフトクォータ原因 ONTAP では、指定された制限を超過すると通知が送信されますが、ハードクォータでは、指定された制限を超過すると書き込み処理が失敗します。

## リソースの使用を制限するためにクォータを設定します

クォータターゲットで利用できるディスクスペースの容量を制限するには、クォータを追加します。

クォータにはハードリミットとソフトリミットを設定できます。

ハードクォータを設定すると、システムリソースにハードリミットが適用されます。実行することで制限値を超えてしまう処理は、すべて失敗します。ソフトクォータを設定すると、リソース使用量が特定のレベルに達したときに警告メッセージが送信されますが、データアクセス処理には影響しないため、クォータを超過する前に適切な処理を実行できます。

## 手順

1. [ ストレージ ]、[ クォータ ] の順にクリックします。
2. [ 追加 (Add) ] をクリックします。

## テスト用にボリュームと LUN をクローニングする

ボリュームおよび LUN をクローニングして、テスト用に一時的な書き込み可能なコピーを作成できます。クローンには、データの現在のポイントインタイム状態が反映されます。また、クローンを使用すると、本番環境のデータにアクセスすることなくユーザがデータにアクセスできるようになります。




FlexCloneライセンスは "インストール済み" ストレージシステム。

ボリュームをクローニングする

次の手順で、ボリュームのクローンを作成します。

手順


1. [ストレージ]、[ボリューム]の順にクリックします。
2. をクリックします  をクリックします。
3. リストから \* Clone \* を選択します。
4. クローンの名前を指定し、他のオプションを選択します。
5. \* Clone \* をクリックし、ボリュームのリストにボリュームクローンが表示されていることを確認します。

また、ボリュームの詳細を表示したときに表示される「\* Overview \*」からボリュームをクローニングすることもできます。

## LUN のクローニング

次の手順で、LUN のクローンを作成します。

手順

1. [\*Storage] > [LUNs] をクリックします。
2. をクリックします  をクリックします。
3. リストから \* Clone \* を選択します。
4. クローンの名前を指定し、他のオプションを選択します。
5. [\* Clone\*] をクリックし、LUN のリストに LUN クローンが表示されていることを確認します。

また、LUN の詳細を表示したときに表示される「\* Overview \*」から LUN のクローンを作成することもできます。

LUN クローンを作成すると、スペースが必要になったときに System Manager でクローンを自動的に削除できるようになります。

## System Manager で情報を検索、フィルタ、ソートできます

System Managerでは、さまざまな操作、オブジェクト、および情報トピックを検索できます。 テーブルデータで特定のエントリを検索することもできます。

System Manager では、次の 2 種類の検索を実行できます。

### • [\[グローバル検索\]](#)

各ページの上部にあるフィールドに検索指数を入力すると、System Manager ではインターフェイス全体が検索され、一致する項目が検索されます。 その後、結果をソートおよびフィルタできます。

ONTAP 9.12.1以降では、NetApp Support Site から検索結果を提供し、関連するサポート情報へのリンク

を提供します。

## • 表 - グリッド検索

ONTAP 9.8 以降では、テーブルグリッドの上部にあるフィールドに検索指数を入力すると、System Manager によってそのテーブルの列と行だけが検索され、一致するデータが検索されます。

## グローバル検索

System Manager の各ページの上部では、グローバル検索フィールドを使用して、インターフェイスのさまざまなオブジェクトやアクションを検索できます。たとえば、名前、ナビゲータ列 ( 左側 ) で使用可能なページ、「ボリュームの追加」や「ライセンスの追加」などのさまざまなアクション項目、外部ヘルプトピックへのリンクなどで、さまざまなオブジェクトを検索できます。また、結果をフィルタリングしてソートすることもできます。



ログイン後 1 分、オブジェクトの作成、変更、削除後 5 分で、検索、フィルタ、ソートを実行して、より適切な結果を得ることができます。

## 検索結果を取得しています

検索では、大文字と小文字は区別されません。さまざまなテキスト文字列を入力して、必要なページ、アクション、または情報トピックを検索できます。最大 20 件の結果が表示されます。検索結果がさらに見つかった場合は、\* Show More \* をクリックしてすべての結果を表示できます。一般的な検索の例を次に示します。

検索のタイプ	検索文字列の例	検索結果の例
オブジェクト名で検索できます	vol_	Storage VM svm0のvol_lun_dest ( ボリューム) Storage VM svm0上 の/vol/vol...est1/lun (LUN) svm0 : vol_lun_dest1ロール : デスティネーション (関係)
インターフェイス内の場所で検索 できます	ボリューム	ボリュームの追加 (操作) 保護-概要 (ページ) 削除したボリュームのリカバリ (ヘルプ)
アクション別	追加 ( Add )	ボリュームの追加 (操作) Network-Overview (ページ) ボリュームとLUNの拡張 (ヘルプ)
ヘルプコンテンツ	SAN	ストレージ-概要 (ページ) SANの概要 (ヘルプ) データベース用のSANストレージ のプロビジョニング (ヘルプ)

## NetApp Support Site によるグローバル検索結果

ONTAP 9.12.1以降では、Active IQ に登録されているユーザに対して、System Managerには、NetApp Support Site 情報へのリンクを提供する、System Manager製品情報を含むもう1列の結果が表示されます。

検索結果には次の情報が含まれます。

- \* HTML、PDF、EPUB、またはその他の形式でドキュメントにリンクする情報のタイトル\*。
- コンテンツタイプ。製品ドキュメントトピック、KnowledgeBase記事、または別の種類の情報のいずれであるかを識別します。
- \*コンテンツのサマリー概要\*。
- \*最初に公開された日付。
- \*更新日\*最終更新日。

次の操作を実行できます。

アクション	結果
ONTAP System Manager*をクリックし、検索フィールドにテキストを入力します。	検索結果には、System Managerに関するNetApp Support Site 情報が含まれます。
[すべての製品]をクリックし、検索フィールドにテキストを入力します。	検索結果には、System Managerだけでなく、すべてのネットアップ製品のNetApp Support Site 情報も含まれます。
検索結果をクリックします。	NetApp Support Site の情報は、別のブラウザウィンドウまたはタブに表示されます。
「その他の結果を見る」をクリックします。	10件を超える結果がある場合は、10番目の結果の後に[さらに結果を表示 (See more results) ]をクリックして、さらに結果を表示できます。 [さらに結果を表示 (See more results) ]をクリックするたびに、可能な場合は別の10件の結果が表示されます。
リンクをコピーします。	リンクがクリップボードにコピーされます。 リンクは、ファイルまたはブラウザウィンドウに貼り付けることができます。
をクリックします  .	結果が表示されるパネルはピンで固定され、別のパネルで作業しても表示されたままになります。
をクリックします  .	結果パネルはピン固定されず、閉じられます。


#### 検索結果のフィルタリング

次の例に示すように、フィルタを使用して結果を絞り込むことができます。

フィルタ	構文	検索文字列の例
オブジェクトタイプ別	<タイプ> : <オブジェクト名>	ボリューム : vol_2
オブジェクトサイズ別	<type><size-symbol><number><units>	LUN の数が 500MB 以上です

破損ディスク別	「broken disk」または「unhealthy disk」	正常でないディスクです
ネットワークインターフェイス別	IP アドレス	172.22.108.21

#### 検索結果のソート

すべての検索結果を表示すると、それらはアルファベット順にソートされます。をクリックすると、結果をソートできます  **Filter**。そして、結果の並べ替え方法を選択します。

#### 表 - グリッド検索

ONTAP 9.8 以降では、System Manager でテーブルグリッド形式で情報が表示されるたびに、テーブルの上部に検索ボタンが表示されます。

- 検索 \* をクリックすると、検索指数を入力できるテキストフィールドが表示されます。System Manager はテーブル全体を検索し、検索指数に一致するテキストを含む行のみを表示します。

アスタリスク（\*）を「ワイルドカード」文字として使用し、文字の代わりに使用できます。たとえば、を検索します vol\* 次の行を指定できます。

- VOL\_122\_D9
- vol\_lun\_dest1
- vol2866
- ボリュームスペック1
- volum\_dest\_765
- ボリューム
- volume\_new4
- ボリューム 9987

### System Manager で測定される容量

システム容量は、物理スペースと論理スペースのどちらかで測定できます。ONTAP 9.7 以降では、System Managerで物理容量と論理容量の両方を測定できます。

2 つの測定値の違いについては、次の説明を参照してください。

- 物理容量：物理スペースとは、ボリュームまたはローカル階層で使用されているストレージの物理ブロックのことです。通常、使用済み物理容量の値は、ストレージ効率化機能（重複排除や圧縮など）によるデータの削減が原因で使用済み論理容量の値よりも小さくなります。
- 論理容量：論理スペースは、ボリュームまたはローカル階層で使用可能なスペース（論理ブロック）です。論理スペースとは、重複排除や圧縮の結果を考慮せずに、理論上のスペースをどのように使用できるかを指します。使用済み論理スペースは、使用済みの物理スペースの量に加えて、設定済みの Storage Efficiency 機能（重複排除や圧縮など）による削減量から導き出されます。Snapshot コピー、クローン、その他のコンポーネントが含まれ、データ圧縮やその他の物理スペースの削減が反映されていないため、この測定値は、多くの場合、物理使用容量よりも大きく表示されます。したがって、合計論理容量は、プロビジョニング済みスペースよりも多くなる可能性があります。



System Manager では、ルートストレージ階層（アグリゲート）の容量は表示されません。

## 使用済み容量の測定値

使用済み容量の測定値の表示方法は、次の表に示すように、使用している System Manager のバージョンによって異なります。

System Manager のバージョン	容量に使用される用語	参照される容量のタイプ
9.9.1 以降	使用済みの論理容量	使用済みの論理スペース Storage Efficiencyの設定が有効になっている場合)
9.7 および 9.8	使用済み	使用済みの論理スペース (Storage Efficiencyの設定が有効になっている場合)
9.5および9.6 (クラシックビュー)	使用済み	使用済みの物理スペース

## 容量測定条件

容量の説明では次の用語を使用します。

- 割り当て容量：Storage VM内のボリュームに割り当てられているスペースの量。
- 使用可能：Storage VMまたはローカル階層でデータの格納やボリュームのプロビジョニングに使用できる物理スペースの量。
- ボリューム間の容量：Storage VM上のすべてのボリュームの使用済みストレージと使用可能なストレージの合計。
- クライアントデータ：クライアントデータによって使用されている容量（物理または論理）。
  - ONTAP 9.13.1以降では、クライアントデータで使用されている容量を\*論理使用済み\*と呼び、Snapshotコピーで使用されている容量は別々に表示されます。
  - ONTAP 9.12.1以前では、クライアントデータに使用されている容量がSnapshotコピーで使用されている容量に追加された容量を\*論理使用済み\*と呼びます。
- \* Committed \*：ローカル階層のコミット済み容量。
- データ削減：
  - ONTAP 9.13.1以降では、データ削減比率が次のように表示されます。
    - [容量]\*パネルに表示されるデータ削減値は、SnapshotコピーなどのStorage Efficiency機能を使用した場合に達成される大幅な削減量を考慮していない、使用済み論理スペースと物理スペースの割合です。
    - 詳細パネルを表示すると、概要パネルに表示された比率と、物理使用済みスペースと比較したすべての使用済み論理スペースの総比率の両方が表示されます。 Snapshotコピーを使用する\*と呼ばれるこの値には、Snapshotコピーやその他のStorage Efficiency機能を使用することによるメリットが含まれています。

◦ ONTAP 9.12.1以前では、データ削減比率は次のように表示されます。

- [容量]\*パネルに表示されるデータ削減量には、使用済み物理スペースに対するすべての使用済み論理スペースの総削減率が表示され、Snapshotコピーやその他のStorage Efficiency機能の使用によるメリットも含まれます。
- 詳細パネルを表示すると、概要パネルに表示された\*[全体]\*の比率と、クライアントデータのみで使用されている物理スペースと比較した、クライアントデータのみで使用されている論理スペースの比率の両方が表示されます。これを「Snapshotコピーとクローンなし」\*と呼びます。

• 使用済み論理容量：

- ONTAP 9.13.1以降では、クライアントデータで使用されている容量を\*論理使用済み\*と呼び、Snapshotコピーで使用されている容量は別々に表示されます。
- ONTAP 9.12.1以前では、クライアントデータで使用されている容量がSnapshotコピーで使用されている容量に追加された容量を\*論理使用済み\*と呼びます。

- \* Logical Used%\*：Snapshotリザーブを除く、プロビジョニングサイズに対する現在の使用済み論理容量の割合。この値は、ボリューム内での効率化による削減も含まれるため、100%より大きい値にすることができます。
- 最大容量：Storage VM上のボリュームに割り当てられる最大スペース。
- 使用済み物理容量：ボリュームまたはローカル階層の物理ブロックで使用されている容量。
- \* Physical Used %\*：ボリュームの物理ブロックで使用されている容量の、プロビジョニングされたサイズに対する割合。
- プロビジョニングされた容量：Cloud Volumes ONTAPシステムから割り当てられ、ユーザやアプリケーションのデータを格納できる状態にあるファイルシステム（ボリューム）。
- \* Reserved \*：ローカル階層ですでにプロビジョニングされているボリューム用にリザーブされているスペースの量。
- 使用済み：データが格納されているスペースの量。
- \* usedおよびreserved \*：使用済みの物理スペースとリザーブスペースの合計です。

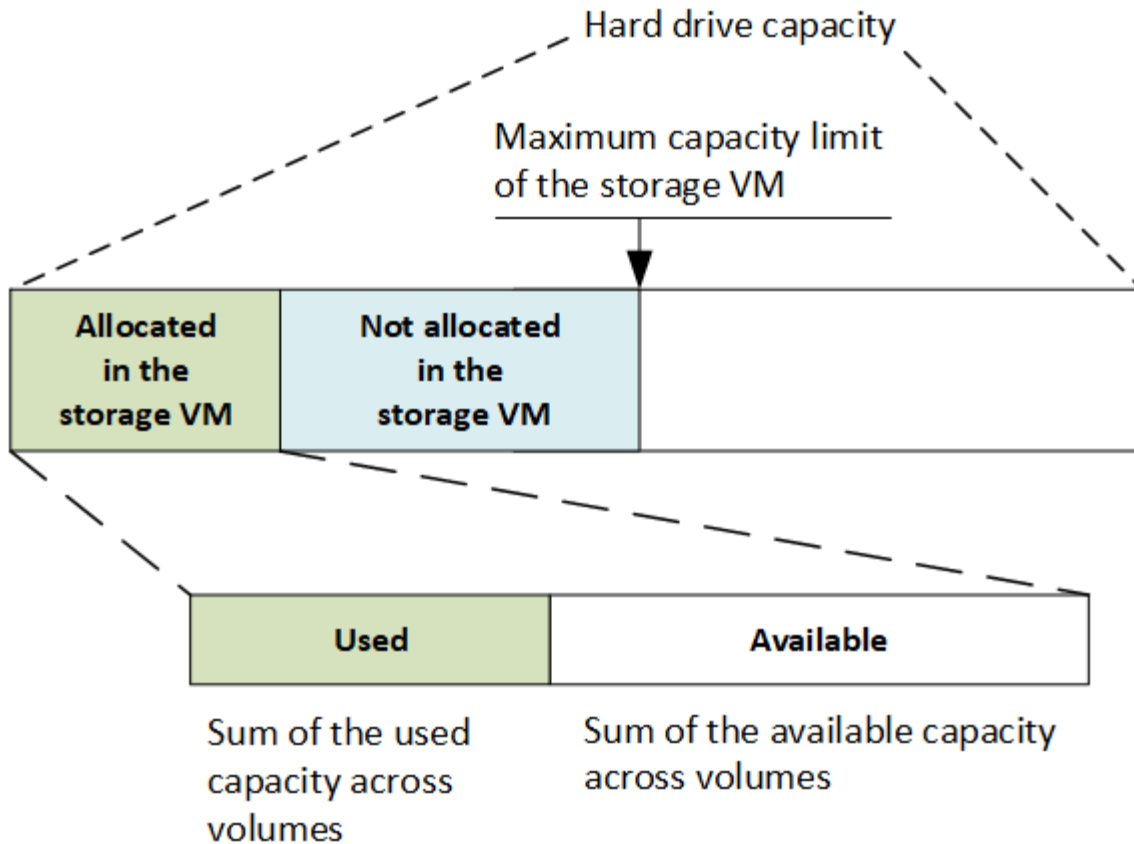
## Storage VMの容量

Storage VMの最大容量は、ボリュームに割り当てられている合計スペースに未割り当ての残りスペースを足したものです。

- ボリュームの割り当てスペースは、FlexVol、FlexGroup、およびFlexCacheの使用済み容量と使用可能容量の合計です。
- ボリュームの容量は、制限されている場合、オフラインの場合、または削除後にリカバリキューに格納されている場合でも、合計に含まれます。
- ボリュームに自動拡張が設定されている場合は、ボリュームの最大オートサイズの値が合計で使用されます。自動拡張を使用しない場合は、ボリュームの実際の容量が合計で使用されます。

次のグラフは、ボリューム間の容量の測定値と最大容量の関係を示しています。





ONTAP 9.13.1以降では、クラスタ管理者が使用できます ["Storage VMの最大容量制限を有効にする"](#)。ただし、データ保護、SnapMirror関係、またはMetroCluster 構成のボリュームを含むStorage VMに対してストレージ制限を設定することはできません。また、Storage VMの最大容量を超えるようにクォータを設定することはできません。

最大容量制限の設定後は、現在割り当てられている容量よりも小さいサイズに変更することはできません。

Storage VMが最大容量に達すると、一部の処理を実行できなくなります。System Managerには、の次の手順に関する推奨事項が表示されます ["インサイト"](#)。

## 容量の単位

System Manager は、1024 ( $2^{10}$ ) バイトのバイナリ単位に基づいてストレージ容量を計算します。

- ONTAP 9.10.1以降では、System Managerにストレージ容量の単位がKiB、MiB、GiB、TiB、およびPiBとして表示されます。
- ONTAP 9.10.0以前では、これらの単位はSystem ManagerにKB、MB、GB、TB、およびPBとして表示されます。



System Manager のスループットに使用される単位は、すべてのリリースの ONTAP について、KB/ 秒、MB/ 秒、GB/ 秒、および PB / 秒です。

ONTAP 9.10.0 以前の System Manager で表示される容量の単位	ONTAP 9.10.1以降のSystem Manager に表示される容量単位	計算	バイト単位の値
KB	KiB	一、〇二四	1024 バイト
MB	MiB	1024 * 1024	1、048、576 バイト
GB	GiB	1024 * 1024 * 1024	1、073、741、824バイト
容量	TiB	1024 * 1024 * 1024 * 1024	1、099、511、627、776 バイト
PB	PiB	1024 * 1024 * 1024 * 1024 * 1024	1、125、899、906、842、624 バイト

関連情報

["System Manager で容量を監視"](#)

["ボリュームの論理スペースのレポートと適用"](#)

## CLI を使用した論理ストレージ管理

### CLI による論理ストレージ管理の概要

ONTAP の CLI を使用して、FlexVol の作成と管理、FlexClone テクノロジーを使用したボリューム、ファイル、LUN の効率的なコピーの作成、qtree とクォータの作成、重複排除や圧縮などの効率化機能の管理を行うことができます。

これらの手順は、次のような状況で使用する必要があります。

- ONTAP FlexVol の機能と Storage Efficiency 機能について理解する必要がある。
- System Manager や自動スクリプトツールではなく、コマンドラインインターフェイス（CLI）を使用する必要がある。

### ボリュームを作成および管理する

ボリュームを作成します

を使用して、ボリュームを作成し、ジャンクションポイントやその他のプロパティを指定できます volume create コマンドを実行します

このタスクについて

クライアントがデータを使用できるようにするには、ボリュームに *junction path* を含める必要があります。ジャンクションパスは、新しいボリュームを作成するときに指定できます。ジャンクションパスを指定せずに

ボリュームを作成する場合は、を使用してSVMネームスペースにボリュームを\_mount\_する必要があります  
volume mount コマンドを実行します

作業を開始する前に

- 新しいボリュームの SVM とそのボリュームにストレージを提供するアグリゲートが、すでに存在している必要があります。
- SVM に関連付けられているアグリゲートのリストがある場合は、アグリゲートがそのリストに含まれている必要があります。
- ONTAP 9.13.1以降では、容量分析とアクティビティ追跡を有効にしてボリュームを作成できます。容量またはアクティビティトラッキングを有効にするには、を問題します volume create コマンドにを指定します -analytics-state または -activity-tracking-state をに設定します on。

容量分析とアクティビティ追跡の詳細については、を参照してください [File System Analytics を有効にします](#)。

手順

## 1. ボリュームを作成します

```
volume create -vserver svm_name -volume volume_name -aggregate aggregate_name  
-size {integer[KB|MB|GB|TB|PB]} -security-style {ntfs|unix|mixed} -user  
user_name_or_number -group group_name_or_number -junction-path junction_path  
[-policy export_policy_name]
```

。 -security style、 -user、 -group、 -junction-path`および ` -policy オプションはNASネームスペース専用です。

の選択 -junction-path 次のようなものがあります。

- ルートの直下。例： /new\_vol

新しいボリュームを作成し、SVMのルートボリュームに直接マウントされるように指定することができます。

- 既存のディレクトリの下（例： /existing\_dir/new\_vol

新しいボリュームを作成し、ディレクトリとして表現されている既存のボリューム（既存の階層内）にマウントされるように指定できます。

新しいディレクトリ（新しいボリュームの下の新しい階層）にボリュームを作成する場合は、次のように指定します。`/new\_dir/new\_vol`その後、SVMルートボリュームにジャンクションされた新しい親ボリュームを作成しておく必要があります。その後、新しい親ボリューム（新しいディレクトリ）のジャンクションパスに新しい子ボリュームを作成します。

## 2. 目的のジャンクションポイントでボリュームが作成されたことを確認します。

```
volume show -vserver svm_name -volume volume_name -junction
```

例

次のコマンドは、SVM上にusers1という名前の新しいボリュームを作成します vs1.example.com およびアグリゲート aggr1。新しいボリュームは、で使用できます /users。ボリュームのサイズは 750GB で、ボリ

ユーモギャランティのタイプは volume（デフォルト）です。

```
cluster1::> volume create -vserver vs1.example.com -volume users1
-aggregate aggr1 -size 750g -junction-path /users
[Job 1642] Job succeeded: Successful
```

```
cluster1::> volume show -vserver vs1.example.com -volume users1 -junction
```

Vserver	Volume	Active	Junction Path	Junction Path Source
vs1.example.com	users1	true	/users	RW_volume

次のコマンドでは、「home4」という名前の新しいボリュームを SVM 「vs1.example.com」 およびアグリゲート「aggr1」に作成します。ディレクトリ /eng/ はvs1 SVMのネームスペースにすでに存在し、新しいボリュームはで使用するようになります /eng/home`をクリックします。これがのホームディレクトリになります ` /eng/ ネームスペース：ボリュームのサイズは750GBで、ボリュームギャランティのタイプはです volume（デフォルト）。

```
cluster1::> volume create -vserver vs1.example.com -volume home4
-aggregate aggr1 -size 750g -junction-path /eng/home
[Job 1642] Job succeeded: Successful
```

```
cluster1::> volume show -vserver vs1.example.com -volume home4 -junction
```

Vserver	Volume	Active	Junction Path	Junction Path Source
vs1.example.com	home4	true	/eng/home	RW_volume

大容量ファイルと大容量ファイルのサポートを実現

ONTAP 9.12.1 P2以降では、新しいボリュームを作成したり既存のボリュームを変更したりして、サポートされる最大ボリュームサイズを300TB、ファイル（LUN）の最大サイズを128TBに変更したりできます。

作業を開始する前に

- ONTAP 9.12.1 P2以降がクラスタにインストールされている。
- SnapMirror関係にあるソースクラスタで大容量ボリュームのサポートを有効にする場合は、ソースボリュームをホストするクラスタとデスティネーションボリュームをホストするクラスタにONTAP 9.12.1 P2以降がインストールされている必要があります。
- クラスタ管理者またはSVM管理者である。

新しいボリュームを作成します

ステップ

1. 大容量ボリュームでファイルのサポートが有効になっているボリュームを作成します。

```
volume create -vserver _svm_name_ -volume _volume_name_ -aggregate  
_aggregate_name_ -is-large-size-enabled true
```

例

次の例は、大容量ボリュームとファイルサイズのサポートを有効にして新しいボリュームを作成します。

```
volume create -vserver vs1 -volume big_vol1 -aggregate aggr1 -is-large  
-size-enabled true
```

既存のボリュームを変更します

ステップ

1. ボリュームを変更して、大容量ボリュームとファイルのサポートを有効にします。

```
volume modify -vserver _svm_name_ -volume _volume_name_ -is-large-size  
-enabled true
```

例

次の例は、大容量のボリュームとファイルサイズをサポートするように既存のボリュームを変更します。

```
volume modify -vserver vs2 -volume data_vol -is-large-size-enabled true
```

関連情報

- ["ボリュームを作成します"](#)
- ["コマンドリファレンス"](#)

## SANボリューム

SAN ボリュームについて

ONTAP には、基本的なボリュームプロビジョニングオプションとして、シックプロビジョニング、シンプロビジョニング、セミシックプロビジョニングの 3 つが用意されています。各オプションでは、ボリュームスペースおよび ONTAP ブロック共有テクノロジーでのスペース要件がさまざまな方法で管理されます。これらのオプションの仕組みを理解することで、環境に最も適したオプションを選択できるようになります。



SAN LUN と NAS 共有を同じ FlexVol に配置することは推奨されません。SAN LUN と FlexVol NAS 共有それぞれに専用の FlexVol ボリュームをプロビジョニングしてください。これにより、管理とレプリケーションの導入が簡易化され、Active IQ Unified Manager (旧 OnCommand Unified Manager) での FlexVol ボリュームのサポート方法が統一されます。

## ボリュームのシンプロビジョニング

シンプロビジョニングボリュームは、作成時に ONTAP によって追加のスペースが確保されることはありません。ボリュームにデータが書き込まれるときに、書き込み処理に対応するために必要なアグリゲート内のストレージをボリュームが要求します。シンプロビジョニングボリュームを使用する場合はアグリゲートをオーバーコミットできますが、アグリゲートの空きスペースが不足すると、必要なスペースをボリュームが確保できなくなる可能性があります。

シンプロビジョニング FlexVol を作成するには、そのボリュームを設定します `-space-guarantee` オプションをに設定します `none`。

## ボリュームのシックプロビジョニング

シックプロビジョニングボリュームを作成すると、ボリューム内のブロックにいつでも書き込むことができるように、ONTAP はアグリゲートから十分なストレージを確保します。シックプロビジョニングを使用するようにボリュームを構成する場合は、圧縮や重複排除などの ONTAP の Storage Efficiency 機能を使用して、事前に必要となる大容量のストレージをオフセットすることができます。

シックプロビジョニング FlexVol ボリュームを作成するには、そのボリュームを設定します `-space-slo` (サービスレベル目標) オプションをに設定します `thick`。

## ボリュームのセミシックプロビジョニング

セミシックプロビジョニングを利用するボリュームを作成すると、ONTAP はボリュームサイズに相当するストレージスペースをアグリゲートから確保します。ブロック共有テクノロジーでブロックが使用されているためにボリュームの空きスペースが不足しそうになると、ONTAP は保護データオブジェクト (Snapshot コピー、FlexClone ファイル、FlexClone LUN) を削除して、該当するオブジェクトが保持しているスペースを解放します。上書きに必要なスペースを確保できる速度で ONTAP が保護データオブジェクトを削除できるかぎり、書き込み処理は続行されます。これは「ベストエフォート」書き込み保証と呼ばれます。



セミシックプロビジョニングを使用しているボリュームでは、重複排除、圧縮、コンパクションなどのストレージ効率化テクノロジーは使用できません。

セミシックプロビジョニング FlexVol ボリュームを作成するには、そのボリュームを設定します `-space-slo` (サービスレベル目標) オプションをに設定します `semi-thick`。

## スペースリザーブファイルおよびスペースリザーブ LUN で使用します

スペースリザーブファイルまたはスペースリザーブ LUN は、ストレージの作成時にそのストレージに割り当てられるものです。ネットアップではこれまで、スペース・リザーベーションが無効になっている LUN (スペース・リザーブなしの LUN) を「シン・プロビジョニング LUN」と呼んできました。



スペースリザーブなしのファイルは、一般に「シンプロビジョニングされたファイル」とは呼ばれません。

次の表に、スペースリザーブファイルおよびスペースリザーブ LUN で使用できる 3 つのボリュームプロビジ

ヨニングオプションの主な違いを示します。

ボリュームのプロビジョニング	LUN/file のスペースリザベーション	上書きします	保護データ <sup>2</sup>	ストレージ効率 <sup>3</sup>
厚み (Thick)	サポートされます	保証された <sup>1</sup>	保証	サポートされます
シン	効果はありません	なし	保証	サポートされます
セミシック	サポートされます	ベストエフォート <sup>1</sup>	ベストエフォート	サポート対象外

• メモ \*

1. 上書きの保証またはベストエフォートの上書き保証が行われるには、LUN またはファイルでスペースリザベーションが有効になっている必要があります。
2. 保護データには、Snapshot コピーおよび自動削除の対象とマークされた FlexClone ファイルと FlexClone LUN (バックアップクローン) が含まれます。
3. Storage Efficiency には、重複排除、圧縮、自動削除の対象とマークされていない FlexClone ファイルと FlexClone LUN (アクティブクローン)、および FlexClone サブファイル (コピーオフロードに使用) が含まれます。

## SCSI シンプロビジョニング LUN のサポート

ONTAP は、T10 SCSI シンプロビジョニング LUN に加え、ネットアップのシンプロビジョニング LUN もサポートしています。T10 SCSI シンプロビジョニングを使用すると、ホストアプリケーションで、LUN のスペース再生やブロック環境の LUN スペース監視機能などの SCSI 機能をサポートできます。使用する SCSI ホストソフトウェアも、T10 SCSI シンプロビジョニングをサポートしている必要があります。

ONTAP を使用します space-allocation LUNでのT10シンプロビジョニングのサポートを有効または無効にするための設定。ONTAP を使用します space-allocation enable LUNでT10 SCSIシンプロビジョニングを有効にするための設定。

。 [-space-allocation {enabled|disabled}] ONTAP でT10シンプロビジョニングのサポートを有効または無効にする方法、およびT10 SCSIシンプロビジョニングを有効にする方法の詳細については、『Command Reference Manual』のコマンドを参照してください。

## "ONTAP 9コマンド"

ボリュームのプロビジョニングオプションを設定

ボリュームにシンプロビジョニング、シックプロビジョニング、またはセミシックプロビジョニングを設定できます。

このタスクについて

を設定します -space-slo オプションをに設定します thick 次のことを確認します。

- ボリューム全体がアグリゲートに事前に割り当てられます。を使用することはできません volume create または volume modify ボリュームを設定するコマンド -space-guarantee オプション

- 上書きに必要なスペースの 100% がリザーブされます。を使用することはできません volume modify ボリュームを設定するコマンド -fractional-reserve オプション

を設定します -space-slo オプションをに設定します semi-thick 次のことを確認します。

- ボリューム全体がアグリゲートに事前に割り当てられます。を使用することはできません volume create または volume modify ボリュームを設定するコマンド -space-guarantee オプション
- スペースは上書き用にリザーブされません。を使用できます volume modify ボリュームを設定するコマンド -fractional-reserve オプション
- Snapshot コピーの自動削除が有効になります。

## ステップ

1. ボリュームのプロビジョニングオプションを設定します。

```
volume create -vserver vs1 -volume vol1 -aggregate
aggregate_name -space-slo none|thick|semi-thick -space-guarantee none|volume
```

。 -space-guarantee オプションのデフォルトはです none（AFF システムの場合）および AFF 以外の DP ボリュームの場合。それ以外の場合は、デフォルトでになります volume。既存の FlexVol ボリュームの場合は、を使用します volume modify プロビジョニングオプションを設定するコマンド。

次のコマンドを使うと、SVM vs1 上の vol1 にシンプロビジョニングが設定されます。

```
cluster1::> volume create -vserver vs1 -volume vol1 -space-guarantee
none
```

次のコマンドを使うと、SVM vs1 上の vol1 にシックプロビジョニングが設定されます。

```
cluster1::> volume create -vserver vs1 -volume vol1 -space-slo thick
```

次のコマンドを使うと、SVM vs1 上の vol1 にセミシックプロビジョニングが設定されます。

```
cluster1::> volume create -vserver vs1 -volume vol1 -space-slo semi-
thick
```

ボリュームまたはアグリゲートのスペース使用量を判定します

ある機能を ONTAP で有効にすると、想定よりも多くのスペースが消費される可能性があります。ONTAP では、消費されるスペースを、ボリューム、アグリゲート内のボリュームのフットプリント、およびアグリゲートの 3 つの観点から判定できます。

ボリューム、アグリゲート、またはその両方でのスペース消費またはスペース不足により、ボリュームのスペースが不足することがあります。スペース使用量の機能別の内訳をさまざまな観点から確認することで、調整や無効化が必要な機能や、その他の処理（アグリゲートやボリュームのサイズ拡張など）が必要かどうかを判



断できます。

スペース使用量は、以下の観点から詳細に確認できます。

- ボリュームのスペース使用量

Snapshot コピーによる使用量も含めて、ボリューム内のスペース使用量の詳細を確認できます。

を使用します `volume show-space` コマンドを使用してボリュームのスペース使用量を確認します。

ONTAP 9.14.1以降、ボリューム [温度に基づくStorage Efficiency \(TSSE\)](#) Enabledに設定されている場合、によって報告されるボリュームで使用されているスペースの量。 `volume show-space -physical used` コマンドには、TSSEによって実現されるスペース削減量が含まれます。

- アグリゲート内のボリュームの占有量

ボリュームのメタデータも含め、包含アグリゲートで各ボリュームが使用しているスペースの量に関する詳細を把握できます。

を使用します `volume show-footprint` コマンドを使用して、ボリュームとアグリゲートのフットプリントを確認します。

- アグリゲートのスペース使用量

アグリゲートに含まれるすべてのボリュームのボリュームフットプリント、アグリゲート Snapshot コピーにリザーブされたスペース、およびその他のアグリゲートメタデータの合計です。

WAFL では、アグリゲートレベルのメタデータとパフォーマンス用に合計ディスクスペースの10%がリザーブされます。アグリゲート内のボリュームを維持するために使用されるスペースは、WAFL リザーブから除外され、変更することはできません。

ONTAP 9.12.1以降では、30TBを超えるアグリゲートのWAFLリザーブが、AFFプラットフォームおよびFAS500fプラットフォームの10%から5%に削減されました。ONTAP 9.14.1以降では、すべてのFASプラットフォームで環境アグリゲートが削減され、アグリゲートで使用可能なスペースが5%増加しました。

を使用します `storage aggregate show-space` コマンドを使用してアグリゲートのスペース使用量を確認します。

テープバックアップおよび重複排除などの特定の機能は、ボリュームからとアグリゲートから直接、メタデータ用のスペースを使用します。これらの機能については、ボリュームとボリュームのフットプリントで異なるスペース使用量が表示されます。

## 関連情報

- ["ナレッジベースの記事：スペース使用量"](#)
- ["ONTAP 9.12.1にアップグレードして、ストレージ容量の5%を解放します"](#)

## Snapshot コピーを自動的に削除する

Snapshot コピーと FlexClone LUN の自動削除ポリシーを定義して有効にすることができます。Snapshot コピーと FlexClone LUN の自動削除はスペース使用の管理に役立ち

ます。

このタスクについて

読み書き可能なボリュームの Snapshot コピーと読み書き可能な親ボリュームの FlexClone LUN について、自動的に削除されるように設定できます。SnapMirror デスティネーションボリュームなど、読み取り専用ボリュームからの Snapshot コピーの自動削除は設定できません。

ステップ

1. を使用して、Snapshot コピーの自動削除ポリシーを定義して有効にします volume snapshot autodelete modify コマンドを実行します

を参照してください volume snapshot autodelete modify のマニュアルページを参照してください。このコマンドで使用できるパラメータについては、ニーズに合わせてポリシーを定義できます。

次のコマンドは、Snapshot コピーの自動削除を有効にし、トリガーをに設定します snap\_reserve vs0.example.com Storage Virtual Machine (SVM) に属する vol3 ボリュームに対して、次の手順を実行します。

```
cluster1::> volume snapshot autodelete modify -vserver vs0.example.com
-volume vol3 -enabled true -trigger snap_reserve
```

次に、Storage Virtual Machine (SVM) vs0.example.com に属するボリューム vol3 に対して、Snapshot コピーと対象としてマークされた FlexClone LUN の自動削除を有効にするコマンドを示します。

```
cluster1::> volume snapshot autodelete modify -vserver vs0.example.com
-volume vol3 -enabled true -trigger volume -commitment try -delete-order
oldest_first -destroy-list lun_clone,file_clone
```



アグリゲートレベルの Snapshot コピーの機能は、ボリュームレベルの Snapshot コピーとは異なり、また、ONTAP によって自動的に管理されます。アグリゲート Snapshot コピーを削除するオプションは常に有効になっており、スペース使用の管理に役立ちます。

trigger パラメータがに設定されている場合 snap\_reserve アグリゲートの場合、Snapshot コピーは、リザーブされているスペースが容量のしきい値を超えるまで維持されます。そのため、trigger パラメータがに設定されていない場合でも同様です snap\_reserve コマンドで Snapshot コピーに使用されているスペースはと表示されます `0` これらの Snapshot コピーは自動的に削除されるためです。また、アグリゲートで Snapshot コピーによって使用されるスペースは空きスペースとみなされ、コマンドの使用可能なスペースのパラメータに含まれます。

ボリュームがフルになったときにスペースを自動的に確保するようにボリュームを設定します

FlexVol では、ONTAP がフルに近くなったときに、さまざまな方法でボリュームの空きスペースを自動的に増やすことができます。ONTAP で使用できる方法、およびアプリケーションとストレージアーキテクチャの要件に応じた順序を選択します。

このタスクについて

ONTAP では、ボリュームがフルになったときに、次のいずれかまたは両方の方法を使用して空きスペースを自動的に増やすことができます。

- ボリュームのサイズを増やす（*autogrow*）。

この方法は、ボリュームの包含アグリゲートに、より大容量のボリュームに対応できる十分なスペースがある場合に便利です。ボリュームの最大サイズは ONTAP で設定できます。拡張は、ボリュームに書き込まれるデータ量と現在使用されているスペースの量、およびしきい値設定に基づいて自動的にトリガーされます。

自動拡張は、Snapshot コピーの作成時にはトリガーされません。自動拡張が有効になっていても、十分なスペースがないと Snapshot コピーの作成は失敗します。

- Snapshot コピー、FlexClone ファイル、または FlexClone LUN を削除する。

たとえば、クローンボリュームや LUN の Snapshot コピーにリンクされていない Snapshot コピーを自動的に削除するように ONTAP を設定したり、古い Snapshot コピーや新しい Snapshot コピーから ONTAP で削除する Snapshot コピーを定義したりできます。また、ボリュームがフルに近くなったときやボリュームの Snapshot リザーブがフルに近づいたときなど、ONTAP で Snapshot コピーの削除が開始されるタイミングを確認することもできます。

両方 ONTAP の方法を有効にする場合、ボリュームがフルに近くなったときに最初にどちらの方法を試行するかを指定できます。最初の方法でボリュームの追加のスペースが十分に確保されない場合は、次に ONTAP がもう一方の方法を試行します。

デフォルトでは、ONTAP は最初にボリュームサイズの拡張を試行します。削除した Snapshot コピーはリストアできないため、通常はデフォルトの設定が推奨されます。ただし、可能な限りボリュームのサイズを拡張しないようにする必要がある場合は、ボリュームサイズを拡張する前に Snapshot コピーを削除するように ONTAP を設定できます。

#### 手順

1. ボリュームがフルに近くなったときに ONTAP でボリュームサイズの拡張を試行するように設定するには、を使用してボリュームの自動拡張機能を有効にします `volume autosize` コマンドにを指定します `grow` モード (Mode) :

ボリュームが拡張される際には、関連付けられているアグリゲートの空きスペースが使用されることに注意してください。スペースが必要なときは常にボリュームを拡張して対処する場合は、関連付けられているアグリゲートの空きスペースを監視し、必要に応じて追加する必要があります。

2. ボリュームがフルに近くなったときに ONTAP で Snapshot コピー、FlexClone ファイル、または FlexClone LUN を削除するように設定するには、該当するタイプのオブジェクトの自動削除を有効にします。
3. ボリュームの自動拡張機能と自動削除機能の両方を有効にした場合は、を使用して ONTAP がボリュームの空きスペースを確保するために最初に実行する方法を選択します `volume modify` コマンドにを指定します `-space-mgmt-try-first` オプション

最初にボリュームのサイズを拡張することを指定するには (デフォルト)、を使用します `volume_grow`。最初に Snapshot コピーを削除するには、を使用します `snap_delete`。

ボリュームのサイズを自動的に拡張および縮小するように設定します

必要なスペースに応じて FlexVol ボリュームを自動的に拡張または縮小するように設定できます。自動拡張機能を使用すると、アグリゲートがスペースを多く提供できても、ボリュームがスペース不足になるのを防止できます。自動縮小機能を使用すると、ボリュームが必要以上に拡張されるのを防止し、アグリゲート内のスペースを他のボリュームで使用できるように解放できます。

必要なもの

FlexVol ボリュームはオンラインである必要があります。

このタスクについて

自動縮小は、変化するスペース需要に対応するために自動拡張と組み合わせて使用することができ、単独で使用することはできません。自動縮小を有効にした場合、自動拡張と自動縮小の処理が無限に繰り返されないように縮小動作が ONTAP で自動的に制御されます。

ボリュームが拡張されると、格納できるファイルの最大数が自動的に増える可能性があります。ボリュームが縮小されても格納できるファイルの最大数は変わらず、ボリュームが縮小前のファイルの最大数に対応するサイズよりも小さくなることはありません。そのため、自動縮小でボリュームを元のサイズに戻すことはできません。

デフォルトでは、ボリュームの最大サイズは、自動拡張を有効にしたときのサイズの 120% まで拡張できます。それよりも大容量にする必要がある場合は、必要に応じてボリュームの最大サイズを設定する必要があります。

ステップ

1. ボリュームのサイズを自動的に拡張および縮小するように設定します。

```
volume autosize -vserver vs1 vol_name -mode grow_shrink
```

次のコマンドは、test2というボリュームで自動サイズ変更を有効にします。ボリュームの 60% が使用された時点で縮小を開始するように設定します。拡張を開始するタイミングおよび最大サイズについてはデフォルト値のままです。

```
cluster1::> volume autosize -vserver vs2 test2 -shrink-threshold-percent 60
vol autosize: Flexible volume "vs2:test2" autosize settings UPDATED.

Volume modify successful on volume: test2
```

自動縮小と **Snapshot** コピーの自動削除の両方を有効にするための要件

特定の設定要件を満たせば、自動縮小機能を Snapshot コピーの自動削除と併用できます。

自動縮小機能と Snapshot コピーの自動削除機能の両方を有効にする場合、設定が次の要件を満たしている必要があります。

- Snapshotコピーの削除を試行する前に、ボリュームサイズの拡張を試行するようにONTAPを設定する必要があります（を参照） `-space-mgmt-try-first` オプションをに設定する必要があります `volume_grow`）。
- Snapshotコピーの自動削除のトリガーは、ボリュームがフルである必要があります（ `trigger` パラメータはに設定する必要があります `volume`）。

#### 自動縮小機能と Snapshot コピーの削除機能の連動

自動縮小機能は FlexVol のサイズを縮小するため、ボリューム Snapshot コピーの自動削除のタイミングにも影響します。

自動縮小機能とボリューム Snapshot コピーの自動削除は次のように連動します。

- 両方の場合 `grow_shrink` オートサイズモードとSnapshotコピーの自動削除が有効になっています。ボリュームサイズが縮小すると、Snapshotコピーの自動削除がトリガーされることがあります。

これは、Snapshot リザーブがボリュームサイズに対する割合（デフォルトは 5%）に基づいているためです。現在、この割合はボリュームサイズの縮小に基づいています。原因 Snapshot コピーは、リザーブからオーバーフローして自動的に削除されます。

- 状況に応じて `grow_shrink` オートサイズモードが有効になっている場合にSnapshotコピーを手動で削除すると、自動ボリューム縮小がトリガーされることがあります。

#### FlexVol のスペース不足アラートと過剰割り当てアラートへの対処

ONTAP では、FlexVol ボリュームがスペース不足になると、該当するボリュームにスペースを追加して対処できるように EMS メッセージが表示されます。アラートの種類とその対処方法を理解しておくと、データの可用性を維持するのに役立ちます。

ボリュームが `_full` とみなされるのは、アクティブファイルシステム（ユーザデータ）で使用可能なボリューム内のスペースの割合がしきい値（設定可能）を下回った場合です。ボリュームが過剰割り当ての状態になると、メタデータを格納したり基本的なデータアクセスをサポートしたりするために ONTAP で使用されるスペースが不足した状態になります。他の目的のために確保されているスペースを使用してボリュームを引き続き利用できる場合もありますが、スペースリザーベーションやデータの可用性を維持できなくなるリスクがあります。

過剰割り当てには論理的なものと物理的なものがあります。\_ 論理的な過剰割り当て \_ は、スペースリザーベーションなど、以降のスペースコミットメントを受け入れるためにリザーブされたスペースが別の目的に使用されたことを意味します。\_ 物理的な過剰割り当て \_ は、ボリュームで使用する物理ブロックが不足した状態を示します。この状態のボリュームには、書き込みができなくなったり、オフラインになったりするリスクがあり、これが原因でコントローラが停止してしまう可能性もあります。

ボリュームは、メタデータ用に使用またはリザーブされているスペースによって 100% を超えることがあります。100% を超えているからといって必ずしも過剰割り当ての状態であるとは限りません。qtree レベルの共有とボリュームレベルの共有が同じ FlexVol または SCVMM プールに存在する場合は、qtree が FlexVol 共有上のディレクトリとして表示されます。そのため、誤って削除しないように注意する必要があります。

次の表に、ボリュームのスペース不足アラートと過剰割り当てアラートについて、問題への対処方法と対処しなかった場合のリスクを示します。

アラートの種類	EMS レベル	設定可能かどうか	定義（ Definition）	対処方法	対処しなかった 場合はリスクが あります
ほぼフルです	デバッグ	Y	ファイルシステムがこのアラートのしきい値（デフォルトは95%）を超えています。パーセンテージはです Used 合計からSnapshotリザーブのサイズを引いた値。	<ul style="list-style-type: none"> <li>• ボリュームサイズを増やしています</li> <li>• ユーザーデータを減らす</li> </ul>	書き込み処理やデータ可用性に対する影響はまだありません。
フル	デバッグ	Y	ファイルシステムがこのアラートに設定されたしきい値（デフォルトは98%）を超えています。パーセンテージはです Used 合計からSnapshotリザーブのサイズを引いた値。	<ul style="list-style-type: none"> <li>• ボリュームサイズを増やしています</li> <li>• ユーザーデータを減らす</li> </ul>	書き込み処理やデータ可用性に対する影響はまだありませんが、ボリュームは書き込み処理ができなくなるリスクのある段階に近づいています。
論理的な過剰割り当て	SVC エラーです	N	ファイルシステムがフルの状態で、さらにメタデータ用のボリュームのスペースが不足しています。	<ul style="list-style-type: none"> <li>• ボリュームサイズを増やしています</li> <li>• Snapshot コピーを削除しています</li> <li>• ユーザーデータを減らす</li> <li>• ファイルまたはLUNのスペースリザーベーションを無効にします</li> </ul>	リザーブされていないファイルに対する書き込み処理が失敗する可能性があります

アラートの種類	EMS レベル	設定可能かどうか	定義（ Definition）	対処方法	対処しなかった 場合はリスクが あります
物理的な過剰割り当て	ノードエラー	N	ボリュームで書き込み可能な物理ブロックが不足しています。	<ul style="list-style-type: none"> <li>• ボリュームサイズを増やしています</li> <li>• Snapshot コピーを削除しています</li> <li>• ユーザデータを減らす</li> </ul>	書き込み処理ができなくなり、データの可用性を維持できなくなるリスクがあり、ボリュームがオフラインになる可能性もあります。

あるボリュームで、フルの割合が上下してしきい値にかかるたびに、EMS メッセージが生成されます。ボリュームのフルレベルがしきい値を下回ると、`volume ok` EMSメッセージが生成されます。

アグリゲートのスペース不足アラートと過剰割り当てアラートに対処します

ONTAP では、アグリゲートがスペース不足になると、該当するアグリゲートにスペースを追加して対処できるように EMS メッセージが表示されます。アラートの種類とその対処方法を理解しておくと、データの可用性を維持するのに役立ちます。

アグリゲートが `_full_` とみなされるのは、アグリゲート内のボリュームで使用可能なスペースの割合が事前に定義されたしきい値を下回った場合です。アグリゲートが過剰割り当ての状態になると、メタデータを格納したり基本的なデータアクセスをサポートしたりするために ONTAP で使用されるスペースが不足した状態になります。他の目的のために確保されているスペースを使用してアグリゲートを引き続き利用できる場合がありますが、アグリゲートに関連付けられているボリュームのボリュームギャランティやデータの可用性を維持できなくなるリスクがあります。

過剰割り当てには論理的なものと物理的なものがあります。`_論理的な過剰割り当て_` は、ボリュームギャランティなどの以降のスペースコミットメントを考慮してリザーブされたスペースが別の目的に使用されていることを示します。`_物理的な過剰割り当て_` は、アグリゲートで使用する物理ブロックが不足した状態を示します。この状態のアグリゲートには、書き込みができなくなったり、オフラインになったりするリスクがあり、これが原因でコントローラが停止してしまう可能性もあります。

次の表に、アグリゲートのスペース不足アラートと過剰割り当てアラートについて、問題への対処方法と対処しなかった場合のリスクを示します。

アラートの種類	EMSレベル	設定可能かどうか	定義（Definition）	対処方法	対処しなかった場合はリスクがあります
ほぼフルです	デバッグ	N	ボリュームに割り当てられたスペース量（ギャランティも含む）がこのアラートのしきい値（95%）を超えています。パーセンテージはです Used 合計からSnapshotリザーブのサイズを引いた値。	<ul style="list-style-type: none"> <li>• アグリゲートにストレージを追加しています</li> <li>• ボリュームを縮小するか削除する</li> <li>• スペースが多い別のアグリゲートにボリュームを移動する</li> <li>• ボリュームギャランティを削除する（に設定する） none)</li> </ul>	書き込み処理やデータ可用性に対する影響はまだありません。
フル	デバッグ	N	ファイルシステムがこのアラートのしきい値（98%）を超えています。パーセンテージはです Used 合計からSnapshotリザーブのサイズを引いた値。	<ul style="list-style-type: none"> <li>• アグリゲートにストレージを追加しています</li> <li>• ボリュームを縮小するか削除する</li> <li>• スペースが多い別のアグリゲートにボリュームを移動する</li> <li>• ボリュームギャランティを削除する（に設定する） none)</li> </ul>	アグリゲート内のボリュームのボリュームギャランティを維持できなくなったり、ボリュームに対する書き込み処理ができなくなったりするリスクがあります。
論理的な過剰割り当て	SVCEエラーです	N	ボリューム用にリザーブされたスペースがフルの状態、さらにメタデータ用のアグリゲートのスペースが不足しています。	<ul style="list-style-type: none"> <li>• アグリゲートにストレージを追加しています</li> <li>• ボリュームを縮小するか削除する</li> <li>• スペースが多い別のアグリゲートにボリュームを移動する</li> <li>• ボリュームギャランティを削除する（に設定する） none)</li> </ul>	アグリゲート内のボリュームのボリュームギャランティを維持できなくなったり、ボリュームに対する書き込み処理ができなくなったりするリスクがあります。



アラートの種類	EMS レベル	設定可能かどうか	定義（Definition）	対処方法	対処しなかった場合はリスクがあります
物理的な過剰割り当て	ノードエラー	N	アグリゲートで書き込み可能な物理ブロックが不足しています。	<ul style="list-style-type: none"> <li>アグリゲートにストレージを追加しています</li> <li>ボリュームを縮小するか削除する</li> <li>スペースが多い別のアグリゲートにボリュームを移動する</li> </ul>	アグリゲート内のボリュームに対する書き込み処理ができなくなり、データの可用性を維持できなくなるリスクがあり、アグリゲートがオフラインになる可能性もあります。最悪の場合、ノードが停止することもあります。

あるアグリゲートで、フルの割合が上下してしきい値にかかるたびに、EMS メッセージが生成されます。アグリゲートのフルレベルがしきい値を下回ると、が表示されます aggregate ok EMSメッセージが生成されます。

#### フラクショナルリザーブの設定に関する考慮事項

フラクショナルリザーブは、`_lun overwrite reserve` と呼ばれ、FlexVol ボリューム内のスペースリザーブ LUN およびファイルのオーバーライトリザーブを無効にすることができます。これはストレージ利用率を最大限に高めるのに役立ちますが、スペース不足による書き込みエラーが悪影響を及ぼす環境では、この設定を利用する場合の要件を確認しておく必要があります。

フラクショナルリザーブ設定はパーセンテージで表され、有効な値はのみです 0 および 100 パーセントフラクショナルリザーブ設定はボリュームの属性です。

フラクショナルリザーブをに設定しています 0 ストレージ利用率が向上します。ただし、ボリュームの空きスペースがなくなると、ボリュームギャランティがに設定されていても、ボリュームに格納されたデータにアクセスするアプリケーションでデータを利用できなくなる可能性があります volume。ただし、ボリュームを適切に設定して使用することで、書き込みが失敗する可能性を最小限に抑えることができます。ONTAP では、フラクショナルリザーブがに設定されたボリュームに対して「ベストエフォート」の書き込み保証が提供されます 0 次の要件の\_all\_が満たされている場合：

- 重複排除を使用していません
- 圧縮を使用していません
- FlexClone サブファイルが使用されていません
- すべての FlexClone ファイルと FlexClone LUN で自動削除が有効になっています

これはデフォルト設定ではありません。FlexClone ファイルや FlexClone LUN の自動削除は、作成時に設定するか作成後に変更して明示的に有効にする必要があります。

- ODX コピーオフロードと FlexClone コピーオフロードは使用されていません
- ボリュームギャランティがに設定されている volume
- ファイルまたはLUNのスペースリザーベーションはです enabled
- ボリュームのSnapshotリザーブがに設定されている 0
- ボリュームSnapshotコピーの自動削除はです enabled を使用しています destroy`を削除します  
`lun\_clone,vol\_clone,cifs\_share,file\_clone,sfsr`をクリックします `volume`

この設定では、必要に応じて FlexClone ファイルと FlexClone LUN も削除されます。



- 上記の要件をすべて満たしていても変更率が高いと、まれに、Snapshotコピーの自動削除が遅れてボリュームのスペースが不足することがあります。
- 上記のすべての要件が満たされ、Snapshotコピーが使用されていない場合、ボリューム書き込みでスペースが不足することはありません。

また、必要に応じてボリュームの自動拡張機能を使用することで、ボリュームの Snapshot コピーの自動削除が発生する可能性を抑えることができます。自動拡張機能を有効にする場合は、関連付けられたアグリゲートの空きスペースを監視する必要があります。アグリゲートの空きスペースがなくなり、ボリュームを拡張できなくなると、ボリュームの空きスペースがなくなったときに削除される Snapshot コピーが増える可能性があります。

上記の設定要件をすべて満たすことができず、ボリュームのスペース不足を防ぐ必要がある場合は、ボリュームのフラクショナルリザーブ設定をに設定する必要があります 100。これにより、事前に確保する必要がある空きスペースは増えますが、上記のテクノロジーを使用する場合でもデータ変更処理が確実に実行されるようになります。

フラクショナルリザーブ設定のデフォルト値と有効値は、ボリュームのギャランティによって異なります。

ボリュームギャランティ	デフォルトのフラクショナルリザーブ	使用できる値
ボリューム	100	0、100
なし	0	0、100

ファイルまたは **inode** の使用量を表示します

FlexVol には、収容可能なファイルの最大数があります。ボリュームに含まれているファイル数を把握しておく、最大ファイルリミットに達しないようにボリュームの（パブリック）inode の数を増やす必要があるかどうかの判断に役立ちます。

このタスクについて

パブリック inode は、空き（ファイルに関連付けられていない）か使用済み（ファイルを参照している）のどちらかです。ボリュームの空き inode の数は、ボリュームの inode の合計数から、使用済み inode の数（ファイル数）を引いたものです。

qtree レベルの共有とボリュームレベルの共有が同じ FlexVol または SCVMM プールに存在する場合は、qtree が FlexVol 共有上のディレクトリとして表示されます。そのため、誤って削除しないように注意する必

必要があります。

## ステップ

1. ボリュームの inode 使用量を表示するには、次のコマンドを入力します。

```
volume show -vserver <SVM_name> -volume <volume_name> -fields files
```

## 例

```
cluster1::*> volume show -vserver vs1 -volume vol1 -fields files
Vserver Name: vs1
Files Used (for user-visible data): 98
```

ストレージ **QoS** を使用して、**FlexVol** ボリュームへの **I/O** パフォーマンスを制御および監視します

FlexVol ボリュームへの入出力（I/O）パフォーマンスは、ストレージ QoS ポリシーグループにボリュームを割り当てることによって制御できます。I/O パフォーマンスを制御することで、ワークロードが特定のパフォーマンス目標を達成できるようにしたり、他のワークロードに悪影響を与えるワークロードを抑制したりできます。

## このタスクについて

ポリシーグループは最大スループット制限（100MB/s など）を適用します。ポリシーグループは最大スループットを指定せずに作成することもでき、ワークロードの制御に先立ってパフォーマンスを監視できます。

SVM、LUN、およびファイルをポリシーグループに割り当てることもできます。

ポリシーグループへのボリュームの割り当てについては、次の要件に注意してください。

- ボリュームは、ポリシーグループが属する SVM に含まれている必要があります。

SVM は、ポリシーグループを作成するときに指定します。

- ボリュームをポリシーグループに割り当てた場合、そのボリュームに含まれる SVM またはそのボリュームの子 LUN や子ファイルをポリシーグループに割り当てることはできなくなります。

ストレージ QoS の使用方法の詳細については、を参照してください ["システムアドミニストレーションリファレンス"](#)。

## 手順

1. を使用します qos policy-group create コマンドを使用してポリシーグループを作成します。
2. を使用します volume create コマンドまたはを実行します volume modify コマンドにを指定します -qos-policy-group ボリュームをポリシーグループに割り当てるためのパラメータ。
3. を使用します qos statistics パフォーマンスデータを表示するためのコマンド。
4. 必要に応じて、を使用します qos policy-group modify コマンドを使用してポリシーグループの最大スループット制限を調整します。

## FlexVol ボリュームを削除します

不要になった FlexVol ボリュームやデータが破損した ボリュームは削除することができます。

必要なもの

削除するボリューム内のデータにアプリケーションがアクセスしていない必要があります。



ボリュームを誤って削除した場合は、記事を参照してください ["ボリュームリカバリキューの使用方法"](#)。

### 手順

1. ボリュームがマウントされている場合は、アンマウントします。

```
volume unmount -vserver vservers_name -volume volume_name
```

2. ボリュームがSnapMirror関係の一部である場合は、を使用して関係を削除します snapmirror delete コマンドを実行します

3. ボリュームがオンラインの場合は、ボリュームをオフラインにします。

```
volume offline -vserver vservers_name volume_name
```

4. ボリュームを削除します。

```
volume delete -vserver vservers_name volume_name
```

### 結果

関連付けられているクォータポリシーや qtree とともに、ボリュームが削除されます。

### 偶発的なボリューム削除の防止

デフォルトのボリューム削除動作では、誤って削除した FlexVol ボリュームを容易にリカバリできるようになっています。

A volume delete タイプがのボリュームに対する要求 RW または DP (を参照) volume show コマンド出力) を指定すると、ボリュームが部分的に削除された状態に移行します。デフォルトでは、このボリュームは 12 時間以上リカバリキューに保持されたあと、完全に削除されます。

詳細については、KnowledgeBaseの記事を参照してください ["ボリュームリカバリキューの使用方法"](#)。

### FlexVol ボリュームを管理するためのコマンド

ONTAP CLI を使用して FlexVol ボリュームを管理するためのコマンドが用意されています。

状況	使用するコマンド
ボリュームをオンラインにします	<code>volume online</code>
ボリュームのサイズを変更する	<code>volume size</code>
ボリュームに関連付けられているアグリゲートを特定します	<code>volume show</code>
Storage Virtual Machine（SVM）のすべてのボリュームに関連付けられているアグリゲートを判別する	<code>volume show -vserver -fields aggregate</code>
ボリュームの形式を決定します	<code>volume show -fields block-type</code>
ジャンクションを使用してボリュームを別のボリュームにマウントします	<code>volume mount</code>
ボリュームを制限状態にします	<code>volume restrict</code>
ボリュームの名前を変更します	<code>volume rename</code>
ボリュームをオフラインにします	<code>volume offline</code>

詳細については、各コマンドのマニュアルページを参照してください。

#### スペース情報を表示するコマンド

を使用します `storage aggregate` および `volume` アグリゲート、ボリューム、およびそれらのSnapshotコピーで使用されているスペースの状況を表示するコマンドです。

表示する情報	使用するコマンド
使用済みスペースの割合および利用可能スペースの割合に関する詳細も含む、アグリゲート、Snapshot リザーブのサイズ、およびその他のスペース使用量情報	<code>storage aggregate show storage aggregate show-space -fields snap-size-total,used-including-snapshot-reserve</code>
アグリゲートでのディスクと RAID グループの使用状況および RAID のステータス	<code>storage aggregate show-status</code>
特定の Snapshot コピーを削除した場合に再利用可能になるディスクスペースの量	<code>volume snapshot compute-reclaimable</code> （アドバンスド）

表示する情報	使用するコマンド
ボリュームによって使用されているスペースの量	<code>volume show -fields size,used,available,percent-used volume show-space</code>
包含アグリゲートでボリュームによって使用されているスペースの量	<code>volume show-footprint</code>

## ボリュームの移動とコピー

### FlexVol ボリュームの移動の概要

容量利用率やパフォーマンスの向上、およびサービスレベル契約を満たすために、ボリュームを移動またはコピーできます。

FlexVol ボリュームの移動の仕組みを理解しておく、ボリュームの移動がサービスレベル契約を満たすかどうかの判断や、ボリューム移動がボリューム移動プロセスのどの段階にあるかを把握するのに役立ちます。

FlexVol ボリュームは、1つのアグリゲートまたはノードから同じ Storage Virtual Machine（SVM）内の別のアグリゲートまたはノードに移動されます。ボリュームを移動しても、移動中にクライアントアクセスが中断されることはありません。

ボリュームの移動は次のように複数のフェーズで行われます。

- 新しいボリュームがデスティネーションアグリゲート上に作成されます。
- 元のボリュームのデータが新しいボリュームにコピーされます。

この間、元のボリュームはそのまま、クライアントからアクセス可能です。

- 移動プロセスの最後に、クライアントアクセスが一時的にブロックされます。

この間にソースボリュームからデスティネーションボリュームへの最終レプリケーションが実行され、ソースボリュームとデスティネーションボリュームの ID がスワップされ、デスティネーションボリュームがソースボリュームに変更されます。

- 移動が完了すると、クライアントトラフィックが新しいソースボリュームにルーティングされ、クライアントアクセスが再開されます。

クライアントアクセスのブロックはクライアントが中断とタイムアウトを認識する前に終了するため、移動によってクライアントアクセスが中断されることはありません。デフォルトでは、クライアントアクセスは 35 秒間ブロックされます。アクセスが拒否されている間にボリューム移動操作が完了しなかった場合、この最終フェーズは中止されてクライアントアクセスが許可されます。デフォルトでは、最終フェーズは 3 回試行されます。3 回目の試行後、1 時間待機してからもう一度最終フェーズのシーケンスが試行されます。ボリューム移動操作の最後のフェーズは、ボリューム移動が完了するまで実行されます。

### ボリュームを移動する際の考慮事項と推奨事項

ボリュームを移動するときは、移動するボリュームやシステム構成（MetroCluster 構成など）によって影響を受ける考慮事項や推奨事項が多数あります。ここでは、ボリュー

## ムの移動に関する考慮事項と推奨事項を示します。

### 一般的な考慮事項と推奨事項

- クラスタのリリースファミリーをアップグレードする場合は、クラスタのすべてのノードをアップグレードするまでボリュームを移動しないでください。

この推奨事項に従うことで、ボリュームを新しいリリースファミリーから古いリリースファミリーに誤って移動するのを防ぐことができます。

- ソースボリュームには整合性が必要です。
- 関連 Storage Virtual Machine (SVM) に 1 つ以上のアグリゲートを割り当てている場合、デスティネーションアグリゲートは、割り当てられたアグリゲートのいずれかである必要があります。
- テイクオーバーされた CFO アグリゲートとの間でボリュームを移動することはできません。
- LUN を含むボリュームで NVFAIL が有効になっていない場合、ボリュームの移動後に NVFAIL が有効になります。
- ボリュームを Flash Pool アグリゲートから別の Flash Pool アグリゲートに移動することができます。
  - ボリュームのキャッシングポリシーも一緒に移動されます。
  - ボリュームのパフォーマンスに影響する可能性があります。
- ボリュームを Flash Pool アグリゲートと Flash Pool アグリゲート以外のアグリゲートの間で移動することができます。
  - ボリュームを Flash Pool アグリゲートから Flash Pool アグリゲート以外のアグリゲートに移動する場合、ボリュームのパフォーマンスに影響する可能性があることを示す警告メッセージが ONTAP に表示され、続行するかどうかの確認を求められます。
  - ボリュームを Flash Pool アグリゲート以外のアグリゲートから Flash Pool アグリゲートに移動すると、ONTAP によって割り当てられます auto キャッシングポリシー。
- ボリュームには、そのボリュームが配置されているアグリゲートの保管データの保護機能が適用されます。NSE ドライブで構成されるアグリゲートからそれ以外のドライブで構成されるアグリゲートにボリュームを移動した場合、NSE による保管データの保護機能は適用されなくなります。

### FlexClone ボリュームに関する考慮事項と推奨事項

- FlexClone ボリュームは、移動中にオフラインにすることはできません。
- FlexClone ボリュームは、を開始せずに、同じ SVM 内の同じノードまたは別のノード上のアグリゲート間で移動できます `vol clone split start` コマンドを実行します

FlexClone ボリューム上でボリューム移動処理を開始することにより、クローンボリュームは移動プロセス中に別のアグリゲートにスプリットされます。クローンボリューム上でのボリュームの移動が完了すると、移動したボリュームはクローンとしてではなく、前の親ボリュームとのクローン関係が設定されていない独立したボリュームとして表示されます。

- FlexClone ボリュームの Snapshot コピーはクローンの移動後も失われません。
- FlexClone の親ボリュームをアグリゲート間で移動することができます。

FlexClone の親ボリュームを移動すると、元のアグリゲートに一時ボリュームが残り、すべての FlexClone ボリュームの親ボリュームとして機能します。この一時ボリュームに対して実行できるのはオ

フラインにする処理と削除する処理だけで、それ以外の処理は実行できません。すべての FlexClone ボリュームのスプリットまたは破棄が完了すると、一時ボリュームは自動的にクリーンアップされます。

- FlexClone の子ボリュームは、移動後は FlexClone ボリュームではなくなります。
- FlexClone の移動処理は、FlexClone のコピー処理やスプリット処理と同時に実行することはできません。
- クローンスプリット処理が実行中の場合、ボリュームの移動が失敗することがあります。

クローンスプリット処理が完了するまで、ボリュームを移動しないでください。

#### MetroCluster の設定に関する考慮事項

- MetroCluster 構成内でボリュームを移動する際、ソースクラスタのデスティネーションアグリゲートに一時ボリュームが作成されると、ミラーされているが同期されていないアグリゲート内のボリュームに対応する一時ボリュームのレコードも稼働しているクラスタに作成されます。
- カットオーバー前に MetroCluster のスイッチオーバーが発生した場合、デスティネーションボリュームは一時ボリューム（タイプが TMP のボリューム）として記録されます。

稼働している（ディザスタリカバリ）クラスタで移動ジョブが再開され、障害を報告し、移動に関連する項目（一時ボリュームなど）をすべてクリーンアップします。クリーンアップを正しく実行できなかった場合は、必要なクリーンアップを実行するようシステム管理者に警告する EMS が生成されます。

- MetroCluster のスイッチオーバーが、カットオーバーフェーズは開始しているが移動ジョブは完了していない（つまり、デスティネーションアグリゲートを参照するようにクラスタを更新できるところまでは完了した）時点で発生した場合、移動ジョブは稼働している（ディザスタリカバリ）上で再開されます。クラスタと実行されて処理が完了します。

移動に関連する項目は、一時ボリューム（元のソース）を含めてすべてクリーンアップされます。クリーンアップを正しく実行できなかった場合は、必要なクリーンアップを実行するようシステム管理者に警告する EMS が生成されます。

- スwitchオーバーされたサイトに属するボリュームに対して実行中のボリューム移動処理がある場合、MetroCluster のスイッチバックは強制的かどうかに関係なく実行できません。

稼働しているサイトのローカルボリュームに対してボリューム移動処理を実行中の場合、スイッチバックはブロックされません。

- 実行中のボリューム移動処理がある場合、MetroCluster の強制的でないスイッチオーバーはブロックされますが、MetroCluster の強制的なスイッチオーバーはブロックされません。

#### SAN 環境でのボリューム移動に関する要件

LUN またはネームスペースを含むボリュームを移動する場合は、一定の要件を満たす必要があります。

- ボリュームに 1 つ以上の LUN が含まれている場合は、クラスタ内の各ノードに接続する LUN（LIF）ごとに少なくとも 2 つのパスが必要です。

これにより、単一点障害が排除され、コンポーネント障害に備えてシステムの運用を継続することができます。



- ・ ボリュームにネームスペースが含まれている場合は、クラスタで ONTAP 9.6 以降が実行されている必要があります。

ONTAP 9.5 を実行する NVMe 構成では、ボリューム移動はサポートされません。

## ボリュームを移動する

ストレージ容量に不均衡があるときは、FlexVol ボリュームを同じ Storage Virtual Machine (SVM) 内で別のアグリゲート、ノード、またはその両方に移動してストレージ容量のバランスを調整することができます。

### このタスクについて

デフォルトでは、カットオーバー処理が 30 秒以内に完了しないと再試行されます。を使用して、デフォルトの動作を調整できます `-cutover-window` および `-cutover-action advanced` 権限レベルのアクセスが必要なパラメータ。詳細については、`volume move start` のマニュアルページ。

### 手順

1. データ保護ミラーを移動する際にミラー関係を初期化していない場合は、を使用してミラー関係を初期化します `snapmirror initialize` コマンドを実行します

ボリュームを移動するには、データ保護のミラー関係を初期化する必要があります。

2. を使用して、ボリュームの移動先となるアグリゲートを特定します `volume move target-aggr show` コマンドを実行します

ボリュームに使用できるスペースが十分にあるアグリゲート、つまり利用可能なサイズが移動するボリュームよりも大きいアグリゲートを選択する必要があります。

次の例では、表示されたどのアグリゲートにも vs2 ボリュームを移動できます。

```
cluster1::> volume move target-aggr show -vserver vs2 -volume user_max
Aggregate Name    Available Size    Storage Type
-----
aggr2             467.9GB          hdd
node12a_aggr3     10.34GB          hdd
node12a_aggr2     10.36GB          hdd
node12a_aggr1     10.36GB          hdd
node12a_aggr4     10.36GB          hdd
5 entries were displayed.
```

3. を使用して、目的のアグリゲートにボリュームを移動できることを確認します `volume move start -perform-validation-only` 検証チェックを実行するコマンド。
4. を使用してボリュームを移動します `volume move start` コマンドを実行します

SVM vs2 上の `user_max` ボリュームを `node12a_aggr3` アグリゲートに移動するコマンドを次に示します。移動はバックグラウンドプロセスとして実行されます。

```
cluster1::> volume move start -vserver vs2 -volume user_max
-destination-aggregate node12a_aggr3
```

5. を使用して、ボリューム移動処理のステータスを確認します `volume move show` コマンドを実行します

次の例は、レプリケーションフェーズを完了し、カットオーバーフェーズにあるボリューム移動の状態を示しています。

```
cluster1::> volume move show
Vserver    Volume      State      Move Phase  Percent-Complete  Time-To-Complete
-----
vs2        user_max    healthy    cutover     -                  -
```

ボリューム移動がに表示されなくなると、これで完了です `volume move show` コマンド出力。

ボリュームを移動するためのコマンド

ONTAP には、ボリューム移動を管理するためのコマンドが用意されています。

状況	使用するコマンド
実行中のボリューム移動処理を中止する。	<code>volume move abort</code>
アグリゲート間のボリューム移動のステータスを表示します。	<code>volume move show</code>
アグリゲート間のボリューム移動を開始する。	<code>volume move start</code>
ボリューム移動のターゲットアグリゲートを管理します。	<code>volume move target-aggr</code>
移動ジョブのカットオーバーをトリガーする。	<code>volume move trigger-cutover</code>
デフォルトの設定が適切でない場合は、クライアントアクセスがブロックされる時間を変更します。	<code>volume move start</code> または <code>volume move modify</code> を使用 <code>-cutover-window</code> パラメータ。 <code>volume move modify command</code> はadvanced権限レベルのコマンドで <code>-cutover-window</code> は、拡張パラメータです。

状況	使用するコマンド
クライアントアクセスがブロックされている時間内にボリューム移動処理が完了しなかった場合のシステムの対応を指定する。	<code>volume move start</code> または <code>volume move modify</code> を使用 <code>-cutover-action</code> パラメータ。 <code>volume move modify command</code> は advanced 権限レベルのコマンドで <code>-cutover-action</code> は、拡張パラメータです。

詳細については、各コマンドのマニュアルページを参照してください。

## ボリュームをコピーする方法

ボリュームをコピーするとスタンドアロンのボリュームコピーが作成され、テストなどの用途に使用できます。ボリュームをコピーする方法は状況によって異なります。

ボリュームをコピーする方法は、コピー先が同じアグリゲートか別のアグリゲートか、および元のボリュームの Snapshot コピーを保持するかどうかによって異なります。次の表に、それぞれのコピーの特性と作成に使用する方法を示します。

ボリュームをコピーする状況	使用する方法
同じアグリゲート内にコピーし、元のボリュームの Snapshot コピーは保持しない。	元のボリュームの FlexClone ボリュームを作成します。
別のアグリゲートにコピーし、元のボリュームの Snapshot コピーは保持しない。	元のボリュームの FlexClone ボリュームを作成し、を使用して別のアグリゲートに移動します <code>volume move</code> コマンドを実行します
別のアグリゲートにコピーし、元のボリュームのすべての Snapshot コピーを保持する。	<code>SnapMirror</code> を使用して元のボリュームをレプリケートしたあと、 <code>SnapMirror</code> 関係を解除して読み書き可能なボリュームにします。

## FlexClone ボリュームを使用して FlexVol の効率的なコピーを作成できます

FlexClone ボリュームを使用して、FlexVol ボリュームの効率的なコピーの作成の概要を示します

FlexClone ボリュームは、親 FlexVol のポイントインタイムの書き込み可能なコピーです。FlexClone ボリュームは共通データについて親 FlexVol と同じデータブロックを共有するため、スペース効率に優れています。FlexClone ボリュームの作成に使用される Snapshot コピーも、親ボリュームと共有されます。

既存の FlexClone ボリュームをクローニングして、別の FlexClone ボリュームを作成できます。LUN と LUN クローンを含む FlexVol のクローンを作成することもできます。

FlexClone ボリュームを親ボリュームからスプリットすることもできます。ONTAP 9.4 以降では、AFF システム上のボリュームのギャランティが none である場合、FlexClone ボリュームのスプリット処理では物理ブロックが共有され、データはコピーされません。したがって、ONTAP 9.4 以降のリリースでは、AFF システムの FlexClone ボリュームのスプリットは他の FAS システムの FlexClone スプリット処理よりも短時間で完了

します。

読み書き可能 FlexClone ボリュームとデータ保護 FlexClone ボリュームの 2 種類の FlexClone ボリュームを作成できます。読み書き可能 FlexClone ボリュームは通常の FlexVol から作成できますが、データ保護 FlexClone ボリュームは SnapVault セカンダリボリュームからしか作成できません。

## FlexClone ボリュームを作成します

データ保護 FlexClone ボリュームは、SnapMirror デスティネーションから作成するか、SnapVault セカンダリボリュームである親の FlexVol から作成できます。ONTAP 9.7以降では、FlexGroup ボリュームから FlexClone ボリュームを作成できます。FlexClone ボリュームの作成後は、FlexClone ボリュームが存在する間は親ボリュームを削除できません。

作業を開始する前に

- クラスタに FlexClone ライセンスがインストールされている必要があります。このライセンスは、["ONTAP One"](#)。
- クローニングするボリュームはオンライン状態である必要があります。



MetroCluster構成では、ボリュームを FlexClone ボリュームとして別の SVM にクローニングすることはできません。

## FlexVol または FlexGroup の FlexClone ボリュームを作成します

### ステップ

1. FlexClone ボリュームを作成します。

```
volume clone create
```



読み書き可能な親ボリュームから読み書き可能な FlexClone ボリュームを作成する場合、ベースの Snapshot コピーを指定する必要はありません。クローンのベース Snapshot コピーを特に指定しない場合、ONTAP によって Snapshot コピーが作成されます。親ボリュームがデータ保護ボリュームである場合は、FlexClone ボリュームを作成するためのベースの Snapshot コピーを指定する必要があります。

### 例

- 次のコマンドを実行すると、親ボリューム vol1 から、読み書き可能 FlexClone ボリューム vol1\_clone が作成されます。

```
volume clone create -vserver vs0 -flexclone vol1_clone -type RW -parent-volume vol1
```

- 次のコマンドを実行すると、ベース Snapshot コピー snap1 を使用して、親ボリューム dp\_vol からデータ保護 FlexClone ボリューム vol\_dp\_clon が作成されます。

```
volume clone create -vserver vs1 -flexclone vol_dp_clone -type DP -parent-volume dp_vol -parent-snapshot snap1
```

任意のSnapLock タイプのFlexCloneを作成

ONTAP 9.13.1以降では、次の3つのSnapLock タイプのいずれかを指定できます。compliance、enterprise、non-snaplock（RWボリュームのFlexCloneを作成する場合）。デフォルトでは、FlexCloneボリュームは親ボリュームと同じSnapLock タイプで作成されます。ただし、を使用してデフォルトの設定を上書きできます snaplock-type FlexCloneボリュームの作成時のオプション。

を使用する non-snaplock パラメータと snaplock-type オプションを使用すると、SnapLock の親ボリュームからSnapLockタイプ以外のFlexCloneボリュームを作成して、必要に応じてデータを迅速にオンラインに戻すことができます。

の詳細を確認してください ["SnapLock"](#)。

作業を開始する前に

SnapLock タイプが親ボリュームと異なる場合は、FlexCloneボリュームに次の制限事項があることに注意してください。

- RWタイプのクローンのみがサポートされます。SnapLock タイプが親ボリュームと異なるDPタイプのクローンはサポートされません。
- SnapLockボリュームではLUNがサポートされないため、snaplock-typeオプションを「non-snaplock」以外の値に設定してLUNを含むボリュームをクローニングすることはできません。
- MetroCluster のミラーされたアグリゲートではSnapLock Complianceボリュームがサポートされないため、MetroCluster のミラーされたアグリゲート上のボリュームをCompliance SnapLock タイプでクローニングすることはできません。
- リーガルホールドを使用するSnapLock Complianceボリュームを別のSnapLock タイプでクローニングすることはできません。リーガルホールドは、SnapLock Complianceボリュームでのみサポートされます。
- SVM DRはSnapLock ボリュームをサポートしません。SVM DR関係の一部であるSVMのボリュームからSnapLock クローンを作成しようとすると失敗します。
- FabricPool のベストプラクティスでは、クローンの階層化ポリシーは親と同じにすることを推奨しています。ただし、FabricPool対応ボリュームのSnapLock Complianceクローンに、親と同じ階層化ポリシーを使用することはできません。階層化ポリシーはに設定する必要があります none。階層化ポリシーが以外の親からSnapLock Complianceクローンを作成しようとしています none 失敗します。

手順

1. SnapLock タイプのFlexCloneボリュームを作成します。volume clone create -vserver svm\_name -flexclone flexclone\_name -type RW [ -snaplock-type {non-snaplock|compliance|enterprise} ]

例

```
> volume clone create -vserver vs0 -flexclone vol1_clone -type RW  
-snaplock-type enterprise -parent-volume vol1
```

**FlexClone** ボリュームを親ボリュームからスプリットします

FlexCloneボリュームを親ボリュームからスプリットして、クローンを通常のFlexVolボリュームにすることができます。

クローンスプリット処理はバックグラウンドで実行されます。スプリット中は、クローンおよび親のデータにアクセスできます。ONTAP 9.4以降では、スペース効率が維持されます。スプリットプロセスではメタデータのみが更新され、IOは最小限に抑えられます。データブロックはコピーされません。

このタスクについて

- FlexCloneボリュームの新しいSnapshotコピーは、スプリット処理中は作成できません。
- データ保護関係に属しているFlexCloneボリュームや負荷共有ミラーに属しているFlexCloneボリュームは、親ボリュームからスプリットすることはできません。
- スプリットの実行中にFlexCloneボリュームをオフラインにすると、スプリット処理が中断されます。FlexCloneボリュームをオンラインに戻すと、スプリット処理が再開されます。
- スプリットの実行後、親FlexVolボリュームとクローンの両方で、それぞれのボリュームギャランティに基づいたスペースの完全な割り当てが必要になります。
- FlexCloneボリュームを親ボリュームからスプリットしたあとは、この2つを再び結合することはできません。
- ONTAP 9.4 以降では、AFF システム上のボリュームのギャランティが none である場合、FlexClone ボリュームのスプリット処理では物理ブロックが共有され、データはコピーされません。そのため、ONTAP 9.4以降では、AFFシステムのFlexCloneボリュームのスプリットは、他のFASシステムのFlexCloneスプリット処理よりも高速です。AFF システムでの FlexClone スプリット処理の向上には、次の利点があります。
  - 親からクローンをスプリットしたあともストレージ効率が維持されます。
  - 既存の Snapshot コピーは削除されません。
  - 処理時間が短縮されます。
  - FlexClone ボリュームをクローン階層の任意のポイントからスプリットできます。

作業を開始する前に

- クラスタ管理者である必要があります。
- FlexCloneボリュームは、スプリット処理の開始時にオンラインになっている必要があります。
- スプリットが成功するには、親ボリュームがオンラインである必要があります。

手順

1. スプリット処理を完了するために必要な空きスペースの量を確認します。

```
volume clone show -estimate -vserver vs1 -flexclone clone1 -parent-volume vol1
```

次の例は、FlexCloneボリューム「clone1」を親ボリューム「vol1」からスプリットするために必要な空きスペースに関する情報を表示します。

```
cluster1::> volume clone show -estimate -vserver vs1 -flexclone clone1 -parent-volume vol1
```

Vserver	FlexClone	Split Estimate
vs1	clone1	40.73MB

2. FlexClone ボリュームとその親が含まれているアグリゲートに十分なスペースがあることを確認します。

a. FlexClone ボリュームとその親が含まれているアグリゲートの空きスペースの量を確認します。

```
storage aggregate show
```

b. 包含アグリゲートで利用可能な空きスペースが不足している場合は、アグリゲートにストレージを追加します。

```
storage aggregate add-disks
```

3. スプリット処理を開始します。

```
volume clone split start -vserver vserver_name -flexclone clone_volume_name
```

次の例は、FlexCloneボリューム「Clone1」を親ボリューム「vol1」からスプリットするプロセスを開始する方法を示しています。

```
cluster1::> volume clone split start -vserver vs1 -flexclone clone1

Warning: Are you sure you want to split clone volume clone1 in Vserver
vs1 ?
{y|n}: y
[Job 1617] Job is queued: Split clone1.
```

4. FlexClone スプリット処理のステータスを監視します。

```
volume clone split show -vserver vserver_name -flexclone clone_volume_name
```

次の例は、AFF システムでの FlexClone スプリット処理のステータスを表示します。

```
cluster1::> volume clone split show -vserver vs1 -flexclone clone1
```

		Inodes				
Blocks						
-----		-----				
Vserver	FlexClone	Processed	Total	Scanned	Updated	% Inode
% Block						
Complete	Complete					
vs1	clone1	0	0	411247	153600	0
37						

5. スプリットボリュームが FlexClone ボリュームでなくなったことを確認します。

```
volume show -volume volume_name -fields clone-volume
```

の値 clone-volume FlexCloneボリューム以外のボリュームの場合、オプションは「false」です。

次の例は、親からスプリットしたボリューム「Clone1」がFlexCloneボリュームでないかどうかを確認する方法を示しています。

```
cluster1::> volume show -volume clone1 -fields clone-volume
vserver volume **clone-volume**
----- **-----**
vs1      clone1 **false**
```

**FlexClone** ボリュームが使用しているスペースを確認します

FlexClone ボリュームの使用スペースを公称サイズおよび親 FlexVol と共有しているスペースに基づいて判断できます。作成された FlexClone ボリュームは、そのすべてのデータを親ボリュームと共有します。したがって、FlexVol の公称サイズは親と同じですが、アグリゲートの空きスペースはわずかししか使用しません。

このタスクについて

新たに作成された FlexClone ボリュームが使用する空きスペースは、その公称サイズの約 0.5% です。このスペースは FlexClone ボリュームのメタデータの保存に使用されます。

親または FlexClone ボリュームのいずれかに書き込まれた新しいデータは、ボリューム間で共有されません。FlexClone ボリュームに書き込まれる新しいデータが増えるにつれて、FlexClone ボリュームがその包含アグリゲートから使用するスペースも増えます。

ステップ

1. を使用して、FlexCloneボリュームが実際に使用している物理スペースを確認します volume show コマンドを実行します

次の例は、FlexClone ボリュームの使用済みの物理スペースの合計を示しています。

```
cluster1::> volume show -vserver vs01 -volume clone_vol1 -fields
size,used,available,
percent-used,physical-used,physical-used-percent
vserver    volume    size  available  used  percent-used  physical-
used       physical-used-percent
-----
vs01      clone_vol1  20MB  18.45MB   564KB    7%           196KB
1%
```

**SnapMirror** のソースボリュームまたはデスティネーションボリュームから **FlexClone** ボリュームを作成する際の考慮事項

既存の Volume SnapMirror 関係にあるソースボリュームまたはデスティネーションボリ



ユーモから FlexClone ボリュームを作成できます。ただし、これを行うと、以降に行う SnapMirror のレプリケーション処理が正常に完了しないことがあります。

FlexClone ボリュームを作成すると、SnapMirror によって使用される Snapshot コピーがロックされる可能性があるため、レプリケーションが機能しないことがあります。この場合、FlexClone ボリュームが削除されるか、親ボリュームからスプリットされるまで、SnapMirror はデスティネーションボリュームへのレプリケーションを停止します。この問題には、次の 2 つの方法で対処できます。

- FlexClone ボリュームが一時的に必要で、SnapMirror レプリケーションが一時的に停止されても構わない場合は、FlexClone ボリュームを作成し、可能となった時点で削除するか親からスプリットします。

FlexClone ボリュームが削除されるか親からスプリットされた時点で、SnapMirror レプリケーションが正常に続行されます。

- SnapMirror レプリケーションの一時的な停止を許容できない場合は、SnapMirror ソースボリュームで Snapshot コピーを作成し、その Snapshot コピーを使用して FlexClone ボリュームを作成します。（FlexClone ボリュームをデスティネーションボリュームから作成している場合、Snapshot コピーが SnapMirror デスティネーションボリュームにレプリケートされるまで待機する必要があります）。

この方法で SnapMirror ソースボリューム内に Snapshot コピーを作成すると、SnapMirror によって使用されている Snapshot コピーをロックすることなくクローンを作成できます。

**FlexClone ファイルと FlexClone LUN** を使用して、ファイルと **LUN** の効率的なコピーを作成できます

**FlexClone ファイルと FlexClone LUN** を使用して、ファイルと **LUN** の効率的なコピーの作成の概要を示します

FlexClone ファイルと FlexClone LUN は、親ファイルや親 LUN の書き込み可能でスペース効率の高いクローンです。これらは、物理的なアグリゲートスペースを効率的に利用するのに役立ちます。FlexClone ファイルと FlexClone LUN は、FlexVol ボリュームでのみサポートされます。

FlexClone ファイルと FlexClone LUN は、そのサイズの 0.4% をメタデータの保存に使用します。クローンは、親ファイルおよび親 LUN のデータブロックを共有し、クライアントが親ファイルまたは LUN に、またはクローンに新しいデータを書き込むまで、わずかなストレージスペースを占有します。

クライアントはファイルおよび LUN のすべての処理を、親エンティティとクローンエンティティの両方で実行できます。

FlexClone ファイルと FlexClone LUN は複数の方法で削除できます。

**FlexClone ファイルまたは FlexClone LUN** を作成します

を使用すると、FlexVol ボリュームまたは FlexClone ボリュームに存在するファイルや LUN のクローンを、スペース効率に優れた方法で短時間で作成できます `volume file clone create` コマンドを実行します

必要なもの

- クラスタに FlexClone ライセンスがインストールされている必要があります。このライセンスは、

"ONTAP One".

- サブ LUN のクローニングまたはサブファイルのクローニングに複数のブロック範囲が使用される場合は、ブロック番号が重ならないようにする必要があります。
- 適応圧縮が有効なボリュームでサブ LUN またはサブファイルを作成する場合は、ブロック範囲がミスアライメントされないようにする必要があります。

つまり、ソースの開始ブロック番号とデスティネーションの開始ブロック番号が、偶数または奇数のいずれかでアライメントされている必要があります。

このタスクについて

SVM 管理者は、クラスタ管理者によって割り当てられた権限に応じて、FlexClone ファイルおよび FlexClone LUN を作成できます。

FlexClone ファイルおよび FlexClone LUN に対して、クローンの作成時と変更時に自動削除設定を指定できます。デフォルトでは、自動削除設定は無効になっています。

既存の FlexClone ファイルまたは FlexClone LUN をクローンの作成時に上書きするには、を使用します volume file clone create コマンドにを指定します -overwrite-destination パラメータ

スプリット負荷の最大値に達すると、FlexClone ファイルおよび FlexClone LUN の作成要求の受け入れが一時的に中止され、が実行されます EBUSY エラーメッセージ。ノードのスプリット負荷が最大値を下回ると、FlexClone ファイルおよび FlexClone LUN の作成要求の受け入れが再開されます。クローンの作成に必要な容量がノードに確保されてから、次の作成要求を行うようにしてください。

手順

1. を使用して、FlexClone ファイルまたは FlexClone LUN を作成します volume file clone create コマンドを実行します

次の例は、ボリューム vol1 内の親ファイル file1\_source から、FlexClone ファイル file1\_clone を作成する方法を示しています。

```
cluster1::> volume file clone create -vserver vs0 -volume vol1 -source  
-path /file1_source -destination-path /file1_clone
```

このコマンドの使用の詳細については、マニュアルページを参照してください。

関連情報

"ONTAP 9 コマンド"

**FlexClone** ファイルおよび **FlexClone LUN** の作成や削除に使用できるノード容量を表示します

ノードのスプリット負荷を表示することで、FlexClone ファイルおよび FlexClone LUN の作成要求や削除要求を新たに受け入れられるだけの容量がノードにあるかどうかを確認することができます。スプリット負荷の最大値に達すると、スプリット負荷が最大値を下回るまで新しい要求が受け付けられなくなります。

このタスクについて

ノードのスプリット負荷が最大値に達すると、が表示されます EBUSY 作成要求と削除要求に応答してエラーメッセージが表示されます。ノードのスプリット負荷が最大値を下回ると、 FlexClone ファイルおよび FlexClone LUN の作成要求や削除要求の受け入れが再開されます。

ノードでは、 Allowable Split Load フィールドに容量が表示され、作成要求に必要な容量が使用可能である場合に新しい要求が受け入れられます。

#### ステップ

1. を使用して、 FlexClone ファイルおよび FlexClone LUN の作成や削除にノードに必要な容量を表示します  
volume file clone split load show コマンドを実行します

次の例では、 cluster1 のすべてのノードのスプリット負荷を表示しています。 Allowable Split Load フィールドの値から、クラスタのすべてのノードに、 FlexClone ファイルおよび FlexClone LUN の作成や削除に使用できる容量があることがわかります。

```
cluster1::> volume file clone split load show
Node           Max           Current           Token           Allowable
              Split Load Split Load Reserved Load Split Load
-----
node1           15.97TB           0B           100MB           15.97TB
node2           15.97TB           0B           100MB           15.97TB
2 entries were displayed.
```

#### FlexClone ファイルおよび FlexClone LUN によるスペース削減量を表示します

FlexClone ファイルおよび FlexClone LUN を含むボリューム内でブロック共有によって削減されたディスクスペースの割合を表示できます。

#### ステップ

1. FlexClone ファイルおよび FlexClone LUN によって達成されたスペース削減を表示するには、次のコマンドを入力します。

```
df -s volname
```

volname は、 FlexVol ボリュームの名前です。



を実行する場合は、を実行します df -s コマンド重複排除が有効な FlexVol ボリュームでは、重複排除と FlexClone ファイルおよび FlexClone LUN の両方で削減されたスペースを表示できます。

#### 例

次に、 FlexClone ボリューム test1 でのスペース削減についての例を示します。

```
systemA> df -s test1
```

Filesystem	used	saved	%saved	Vserver
/vol/test1/	4828	5744	54%	vs1

## FlexClone ファイルおよび FlexClone LUN の削除方法

FlexClone ファイルと FlexClone LUN は複数の方法で削除できます。それぞれの方法について理解しておく、クローンの管理方法を計画する際に役立ちます。

FlexClone ファイルと FlexClone LUN は、次の方法で削除できます。

- FlexVol ボリュームの空きスペースが特定のしきい値を下回った場合に、自動削除を有効にしたクローンを自動的に削除するように FlexVol を設定できます。
- NetApp Manageability SDK を使用してクローンを削除するようにクライアントを設定できます。
- クライアントで NAS プロトコルおよび SAN プロトコルを使用してクローンを削除できます。

デフォルトでは、NetApp Manageability SDK を使用しない低速な削除方式が有効になっています。ただし、を使用して FlexClone ファイルを削除するときに高速削除方式を使用するようにシステムを設定することができます volume file clone deletion コマンド

## 自動削除設定を使用して FlexVol ボリュームの空きスペースを再生する方法

自動削除設定の概要を使用して FlexVol ボリュームの空きスペースを再生する方法

FlexVol の自動削除設定を有効にすると、FlexClone ファイルおよび FlexClone LUN を自動的に削除できます。自動削除を有効にすると、ボリュームがフルに近くなったときに、指定した量の空きスペースをボリューム内に再生できます。

ボリュームの空きスペースが一定のしきい値を下回ったときに FlexClone ファイルおよび FlexClone LUN の削除を自動的に開始し、ボリュームの空きスペースを指定の量だけ再生したらクローンの削除を自動的に中止するように設定できます。クローンの自動削除を開始するしきい値を指定することはできませんが、それぞれのクローンを削除対象に含めるかどうかと、ボリュームの空きスペースの目標量を指定することができます。

ボリュームの空きスペースが一定のしきい値を下回ったとき、および次の要件の両方に達したときに、FlexClone ファイルおよび FlexClone LUN が自動的に削除されます。

- FlexClone ファイルおよび FlexClone LUN が格納されているボリュームに対して自動削除機能が有効になっている。

FlexVol に対して自動削除機能を有効にするには、を使用します volume snapshot autodelete modify コマンドを実行しますを設定する必要があります -trigger パラメータの値 volume または snap\_reserve ボリュームが FlexClone ファイルおよび FlexClone LUN を自動的に削除するように設定します。

- FlexClone ファイルおよび FlexClone LUN に対して自動削除機能が有効になっている。

FlexClone ファイルまたは FlexClone LUN に対して自動削除を有効にするには、を使用します file

clone create コマンドにを指定します `-autodelete` パラメータこのクローン設定はボリュームの他の設定よりも優先されるため、この設定で個別に自動削除を無効にすることで、特定の FlexClone ファイルや FlexClone LUN を保持することができます。

**FlexClone ファイルおよび FlexClone LUN を自動的に削除するように FlexVol を設定する**

ボリュームの空きスペースが特定のしきい値を下回った場合に、自動削除を有効にした FlexClone ファイルおよび FlexClone LUN を自動的に削除するように FlexVol を設定できます。

必要なもの

- FlexVol ボリュームに FlexClone ファイルおよび FlexClone LUN が含まれていて、オンラインになっている必要があります。
- FlexVol ボリュームを読み取り専用ボリュームにすることはできません。

手順

1. を使用して、FlexVol ボリューム内の FlexClone ファイルおよび FlexClone LUN の自動削除を有効にします  
`volume snapshot autodelete modify` コマンドを実行します

- をクリックします `-trigger` パラメータを指定することもできます `volume` または `snap_reserve`。
- をクリックします `-destroy-list` パラメータは常に指定する必要があります  
`lun_clone, file_clone` 削除するクローンのタイプが1つだけであるかどうかは関係ありません。  
次の例は、ボリューム `vol1` で FlexClone ファイルおよび FlexClone LUN の自動削除を有効にし、ボリュームの 25% が空きスペースになるまでスペースが再生されるようにします。

```
cluster1::> volume snapshot autodelete modify -vserver vs1 -volume  
vol1 -enabled true -commitment disrupt -trigger volume -target-free  
-space 25 -destroy-list lun_clone,file_clone
```

```
Volume modify successful on volume:vol1
```



FlexVol ボリュームの自動削除を有効にする際に、の値を設定した場合 `-commitment` パラメータの値 `destroy` を使用して、すべての FlexClone ファイルおよび FlexClone LUN を削除します `-autodelete` パラメータをに設定します `true` ボリュームの空きスペースが指定したしきい値を下回った場合に削除されることがあります。ただし、FlexClone ファイルと FlexClone LUN はを使用します `-autodelete` パラメータをに設定します `false` は削除されません。

2. を使用して、FlexVol ボリュームで FlexClone ファイルおよび FlexClone LUN の自動削除が有効になっていることを確認します `volume snapshot autodelete show` コマンドを実行します

次の例では、ボリューム `vol1` で FlexClone ファイルおよび FlexClone LUN の自動削除が有効になっています。

```
cluster1::> volume snapshot autodelete show -vserver vs1 -volume vol1

Vserver Name: vs1
Volume Name: vol1
Enabled: true
Commitment: disrupt
Defer Delete: user_created
Delete Order: oldest_first
Defer Delete Prefix: (not specified)
Target Free Space: 25%
Trigger: volume
*Destroy List: lun_clone,file_clone*
Is Constituent Volume: false
```

3. 次の手順を実行して、ボリューム内の削除対象とする FlexClone ファイルおよび FlexClone LUN の自動削除を有効にします。

- a. を使用して、特定の FlexClone ファイルまたは FlexClone LUN の自動削除を有効にします volume file clone autodelete コマンドを実行します

を使用して、特定の FlexClone ファイルまたは FlexClone LUN を強制的に自動削除することができます volume file clone autodelete コマンドにを指定します -force パラメータ

次の例は、ボリューム vol1 に含まれる FlexClone LUN lun1\_clone の自動削除が有効になっていることを示します。

```
cluster1::> volume file clone autodelete -vserver vs1 -clone-path
/vol/vol1/lun1_clone -enabled true
```

FlexClone ファイルおよび FlexClone LUN の作成時に自動削除を有効にすることができます。

- b. を使用して、FlexClone ファイルまたは FlexClone LUN で自動削除が有効になっていることを確認します volume file clone show-autodelete コマンドを実行します

次の例は、FlexClone LUN lun1\_clone で自動削除が有効になっていることを示します。

```
cluster1::> volume file clone show-autodelete -vserver vs1 -clone
-path vol/vol1/lun1_clone
Vserver Name: vs1
Clone Path: vol/vol1/lun1_clone
**Autodelete Enabled: true**
```

コマンドの使用の詳細については、該当するマニュアルページを参照してください。

特定の **FlexClone** ファイルまたは **FlexClone LUN** を自動削除の対象から除外します

FlexClone ファイルおよび FlexClone LUN を自動的に削除するように FlexVol を設定すると、指定した条件を満たすすべてのクローンが削除される可能性があります。特定の FlexClone ファイルまたは FlexClone LUN を残したい場合は、それらを FlexClone の自動削除プロセスから除外できます。

必要なもの

FlexClone ライセンスがインストールされている必要があります。このライセンスは、**"ONTAP One"**。

このタスクについて

FlexClone ファイルまたは FlexClone LUN を作成すると、クローンの自動削除設定がデフォルトで無効になります。自動削除を無効にした FlexClone ファイルと FlexClone LUN は、ボリュームのスペースを再生するためにクローンを自動的に削除するように FlexVol を設定しても保持されます。



を設定した場合は commitment ボリュームのレベルをに設定します try または disrupt、特定の FlexClone ファイルまたは FlexClone LUN を個別に保持するには、それらのクローンの自動削除を無効にします。ただし、を設定した場合、commitment ボリュームのレベルをに設定します destroy 削除リストには次のものが含まれます `lun\_clone, file\_clone` では、ボリューム設定はクローン設定よりも優先され、クローンの自動削除設定に関係なく、すべての FlexClone ファイルと FlexClone LUN が削除されます。

手順

1. を使用して、特定の FlexClone ファイルまたは FlexClone LUN を自動的に削除しないように設定します  
volume file clone autodelete コマンドを実行します

次の例は、vol1 に含まれている FlexClone LUN lun1\_clone の自動削除を無効にする方法を示しています。

```
cluster1::> volume file clone autodelete -vserver vs1 -volume vol1  
-clone-path lun1_clone -enable false
```

自動削除を無効にした FlexClone ファイルまたは FlexClone LUN は、ボリュームのスペース再生を目的とした自動削除の対象になりません。

2. を使用して、FlexClone ファイルまたは FlexClone LUN で自動削除が無効になっていることを確認します  
volume file clone show-autodelete コマンドを実行します

次の例では、FlexClone LUN lun1\_clone の自動削除が false になっています。

```
cluster1::> volume file clone show-autodelete -vserver vs1 -clone-path
vol/vol1/lun1_clone
```

	Vserver
Name: vs1	
	Clone Path:
vol/vol1/lun1_clone	
	Autodelete
Enabled: false	

**FlexClone** ファイルの削除を設定するためのコマンド

クライアントがNetApp Manageability SDKを使用せずにFlexCloneファイルを削除する場合は、を使用できます `volume file clone deletion FlexVol` ボリュームからのFlexCloneファイルの高速削除を有効にするコマンド。高速削除では、FlexClone ファイルの拡張子と最小サイズが使用されます。

を使用できます `volume file clone deletion` ボリューム内のFlexCloneファイルでサポートされる拡張子のリストと最小サイズの要件を指定するコマンド。高速削除方式は、要件を満たす FlexClone ファイルに対してのみ使用され、要件を満たさない FlexClone ファイルに対しては、より低速な削除方式が使用されます。

クライアントが NetApp Manageability SDK を使用してボリュームから FlexClone ファイルおよび FlexClone LUN を削除する場合は、常に高速削除方式が使用されるため、拡張子とサイズの要件は適用されません。

目的	使用するコマンド
ボリュームでサポートされる拡張子のリストに拡張子を追加します	<code>volume file clone deletion add-extension</code>
高速削除方式でボリュームから削除する FlexClone ファイルの最小サイズを変更します	<code>volume file clone deletion modify</code>
ボリュームでサポートされる拡張子のリストから拡張子を削除します	<code>volume file clone deletion remove-extension</code>
クライアントが高速削除方式でボリュームから削除可能な、サポートされる拡張子のリストと FlexClone ファイルの最小サイズを表示します	<code>volume file clone deletion show</code>

これらのコマンドの詳細については、該当するマニュアルページを参照してください。

## qtree を使用して **FlexVol** ボリュームをパーティショニングします

「**qtree** を使用した **FlexVol** ボリュームのパーティショニングの概要」を参照してください

`qtree` を使用すると、FlexVol を小さなセグメントにパーティショニングして、それぞれ個別に管理できます。`qtree` を使用して、クォータ、セキュリティ形式、および CIFS



oplock を管理できます。

ONTAP は、各ボリュームに qtree0 という名前のデフォルトの qtree を作成します。qtree にデータを配置しない場合、データは qtree0 に格納されます。

qtree 名の最大文字数は 64 文字です。

ディレクトリは qtree 間で移動できません。qtree 間で移動できるのはファイルだけです。

qtree レベルの共有とボリュームレベルの共有を同じ FlexVol または SCVMM プールに作成すると、qtree が FlexVol 共有上のディレクトリとして表示されます。そのため、誤って削除しないように注意する必要があります。

### qtree のジャンクションパスを取得する

qtree のジャンクションパスまたはネームスペースパスを取得して個々の qtree をマウントできます。CLI コマンドで表示される qtree パス `qtree show -instance` は、の形式です `/vol/<volume_name>/<qtree_name>`。ただし、このパスは qtree のジャンクションパスまたはネームスペースパスではありません。

このタスクについて

qtree のジャンクションパスまたはネームスペースパスを取得するには、ボリュームのジャンクションパスが必要です。

#### ステップ

1. を使用します `vserver volume junction-path` コマンドを使用してボリュームのジャンクションパスを取得します。

次の例は、`vs0` という名前の Storage Virtual Machine (SVM) にある `vol1` という名前のボリュームのジャンクションパスを表示します。

```
cluster1::> volume show -volume vol1 -vserver vs0 -fields junction-path

-----
vs0 vol1 /vol1
```

上記の出力から、ボリュームのジャンクションパスは `/vol1`。qtree は常にボリュームにルートされるため、qtree のジャンクションパスまたはネームスペースパスは `/vol1/qtree1`。

### qtree 名の制限事項

qtree 名の最大文字数は 64 文字です。また、カンマやスペースなどの特殊文字を qtree 名に使用すると、原因で他の機能に関する問題が発生する可能性があるため、使用しないでください。

["ファイル名を作成する際のCLIの動作と制約の詳細"](#)。

ディレクトリを **qtree** に変換します

ディレクトリの **qtree** への変換の概要

FlexVol ボリュームのルートにあるディレクトリを **qtree** に変換する場合は、クライアントアプリケーションを使用して、ディレクトリ内のデータを同じ名前の新しい **qtree** に移行する必要があります。

このタスクについて

ディレクトリを **qtree** に変換するための手順は、使用するクライアントによって異なります。実行する必要がある一般的なタスクの概要を以下に示します。

手順

1. **qtree** に変換するディレクトリの名前を変更します。
2. 元のディレクトリ名を指定した新しい **qtree** を作成します。
3. クライアントアプリケーションを使用して、ディレクトリの内容を新しい **qtree** に移動します。
4. 空になったディレクトリを削除します。



既存の CIFS 共有と関連付けられているディレクトリは削除できません。

**Windows** クライアントを使用して、ディレクトリを **qtree** に変換します

Windows クライアントを使用してディレクトリを **qtree** に変換するには、ディレクトリの名前を変更し、ストレージシステムに **qtree** を作成して、ディレクトリの内容を **qtree** に移動します。

このタスクについて

この手順にはエクスプローラを使用する必要があります。Windows のコマンドラインインターフェイスや DOS プロンプト環境は使用できません。

手順

1. エクスプローラを開きます。
2. 変更するディレクトリのフォルダ表示をクリックします。



ディレクトリは、その格納先ボリュームのルートに配置する必要があります。

3. 「\* ファイル」メニューから「\* 名前の変更 \*」を選択して、このディレクトリに別の名前を付けます。
4. ストレージシステムで、を使用します `volume qtree create` コマンドを使用して、ディレクトリの元の名前を使用して新しい **qtree** を作成します。
5. エクスプローラで、名前を変更したディレクトリフォルダを開き、フォルダ内のファイルを選択します。
6. 新しい **qtree** のフォルダアイコンに、これらのファイルをドラッグします。



移動するフォルダ内のサブフォルダ数が多いほど、移動処理に時間がかかります。

7. 「\* ファイル」メニューから「\* 削除 \*」を選択して、名前が変更された空のディレクトリ・フォルダを削除します。

UNIX クライアントを使用してディレクトリを **qtree** に変換します

UNIX でディレクトリを **qtree** に変換するには、ディレクトリの名前を変更し、ストレージシステムに **qtree** を作成して、ディレクトリの内容を **qtree** に移動します。

手順

1. UNIX クライアントのウィンドウを開きます。
2. を使用します **mv** コマンドを使用してディレクトリの名前を変更します。

```
client: mv /n/user1/vol1/dir1 /n/user1/vol1/olddir
```

3. ストレージシステムからを使用します **volume qtree create** コマンドを使用して、元の名前の**qtree**を作成します。

```
system1: volume qtree create /n/user1/vol1/dir1
```

4. クライアントからを使用します **mv** コマンドを使用して、古いディレクトリの内容を**qtree**に移動します。



移動するディレクトリ内のサブディレクトリ数が多いほど、移動処理に時間がかかります。

```
client: mv /n/user1/vol1/olddir/* /n/user1/vol1/dir1
```

5. を使用します **rmdir** 空になった古いディレクトリを削除するコマンド。

```
client: rmdir /n/user1/vol1/olddir
```

完了後

UNIXクライアントでの実装方法に応じて異なります **mv** コマンド、ファイルの所有権、権限が維持されない場合があります。この場合は、ファイルの所有者と権限を以前の値に更新します。

**qtree** を管理および設定するためのコマンド

特定の ONTAP コマンドを使用して、**qtree** を管理および設定できます。

状況	使用するコマンド
<b>qtree</b> を作成します	<code>volume qtree create</code>

フィルタリングされた qtree のリストを表示します	<code>volume qtree show</code>
qtree を削除する	<code>volume qtree delete</code> <div>  <p>qtree コマンド <code>volume qtree delete qtree</code> が空またはでないで処理は失敗します <code>-force true</code> フラグが追加されました。</p> </div>
qtree の UNIX アクセス権を変更する	<code>volume qtree modify -unix-permissions</code>
qtree の CIFS oplock 設定を変更します	<code>volume qtree oplocks</code>
qtree のセキュリティ設定を変更する	<code>volume qtree security</code>
qtree の名前を変更する	<code>volume qtree rename</code>
qtree の統計を表示する	<code>volume qtree statistics</code>
qtree の統計情報をリセットする	<code>volume qtree statistics -reset</code>



。 `volume rehost` コマンドは、そのボリュームを対象として同時に実行されている他の管理処理を原因して失敗します。

## ボリュームの論理スペースのレポートと適用

ボリュームの論理スペースのレポートと適用の概要が表示されます

ONTAP 9.4 以降では、ボリュームで使用されている論理スペースと残りのストレージスペースの量をユーザに表示できます。ONTAP 9.5以降では、ユーザが消費する論理スペースの量を制限できます。

論理スペースのレポートと適用は、デフォルトでは無効になっています。

論理スペースのレポートと適用は、次のボリュームタイプでサポートされています。

ボリュームタイプ	スペースレポートはサポートされていますか。	スペースの適用はサポートされていますか
FlexVol ボリューム	はい、ONTAP 9.4 以降で導入されました	はい、ONTAP 9.5 以降で使用できます
SnapMirror デスティネーションボリューム	はい、ONTAP 9.8 以降です	はい。ONTAP 9.13.1以降でサポートされています

ボリュームタイプ	スペースレポートはサポートされていますか。	スペースの適用はサポートされていますか
FlexGroup ボリューム	はい、ONTAP 9.9.1 以降でサポートされています	はい、ONTAP 9.9.1 以降でサポートされています
FlexCache ボリューム	元の設定はキャッシュで使用されます	該当なし

## 論理スペースレポートの内容

ボリュームで論理スペースのレポートを有効にすると、ボリュームの合計スペースに加えて使用済みの論理スペースと使用可能な論理スペースの量も表示されます。また、Linux および Windows クライアントシステムのユーザは、使用済みの物理スペースと使用可能な物理スペースではなく、使用済みの論理スペースと使用可能な論理スペースを確認できます。

### 定義：

- 物理スペースとは、ボリュームで使用可能または使用されているストレージの物理ブロックのことです。
- 論理スペースとは、ボリューム内の使用可能なスペースのことです。
- 使用済みの論理スペースに加えて、設定済みの Storage Efficiency 機能（重複排除や圧縮など）による削減効果も表示されます。

ONTAP 9.5 以降では、論理スペースの適用とスペースのレポートを有効にすることができます。

論理スペースのレポートを有効にすると、に次のパラメータが表示されます `volume show` コマンドを実行します

パラメータ	意味
<code>-logical-used</code>	使用済み論理サイズが指定した値に一致するボリュームに関する情報のみを表示します。この値には、Storage Efficiency 機能で削減されたすべてのスペースと物理的に使用されているスペースが含まれます。Snapshot リザーブは含まれませんが、Snapshot オーバーフローは考慮されます。
<code>-logical-used-by-afs</code>	アクティブファイルシステムで使用されている論理サイズが指定した値に一致するボリュームに関する情報のみを表示します。この値はとは異なります <code>-logical-used</code> Snapshot リザーブを超過した Snapshot オーバーフローの量による値。
<code>-logical-available</code>	論理スペースのレポートのみが有効になっている場合は、使用可能な物理スペースのみが表示されます。スペースのレポートと適用の両方が有効な場合、Storage Efficiency 機能によって削減されたスペースを考慮して現在使用可能な空きスペースの量が表示されます。これには Snapshot リザーブは含まれません。

パラメータ	意味
-logical-used -percent	現在の割合が表示されます -logical-used ボリュームのSnapshotリザーブを除いたプロビジョニングサイズの値。  この値は100%を超える場合があります。これは、が原因です -logical-used -by-afs 値には、ボリューム内の効率化による削減効果が含まれます。。 -logical-used-by-afs ボリュームの値には、使用済みスペースとしてSnapshotオーバーフローは含まれません。。 -physical-used ボリュームの値には、使用済みスペースとしてSnapshotオーバーフローが含まれます。
-used	ユーザデータおよびファイルシステムメタデータによって占有されているスペースの量が表示されます。とは異なります。 physical-used 以降の書き込み用にリザーブされているスペースとアグリゲートのストレージ効率化によって削減されたスペースの合計です。 Snapshotオーバーフロー（Snapshotリザーブを超過したSnapshotコピーのスペースの量）も含まれます。 Snapshotリザーブは含まれません。

CLI で論理スペースのレポートを有効にすると、 Logical Used Space （ % ） 値と Logical Space 値も System Manager に表示されます

クライアント・システムでは、次のシステム・ディスプレイに論理スペースが使用済みスペースとして表示されます

- \* Linux システムでの df \* 出力
- Windows システムの Windows エクスプローラを使用したプロパティの領域の詳細。



論理スペースの適用なしで論理スペースのレポートが有効になっている場合は、クライアントシステムに表示される合計容量が、プロビジョニングされたスペースよりも大きくなる可能性があります。

## 論理スペースの適用機能

ONTAP 9.5 以降で論理スペースの適用を有効にすると、ONTAP ではボリューム内の使用済み論理ブロック数がカウントされ、使用可能な残りのスペースが算出されます。ボリュームに使用可能なスペースがない場合、ENOSPC（スペース不足）エラーメッセージが返されます。

論理スペースの適用では、ボリュームがフルになったときやフルに近づいたときにユーザに通知されます。論理スペースの適用では、ボリュームの使用可能スペースについて 3 種類のアラートが返されます。

- Monitor.vol.full.inc.sav：このアラートは、ボリュームの論理スペースの使用率が98%に達するとトリガーされます。
- Monitor.vol.nearFull.inc.sav：このアラートは、ボリュームの論理スペースの95%が使用されたときにトリガーされます。
- Vol.log.overalloc.inc.sav：このアラートは、ボリュームで使用されている論理スペースがボリュームの合計サイズよりも大きい場合にトリガーされます。

このアラートがトリガーされた場合、ボリュームにスペースを追加しても超過した論理ブロックによって

使用されてしまうため、使用可能なスペースにならない可能性があります。



論理スペースの適用を使用するボリュームの Snapshot リザーブを除く、合計（論理スペース）がプロビジョニングスペースと同じである必要があります。

詳細については、を参照してください ["ボリュームがフルになったときにスペースを自動的に確保するように設定する"](#)

論理スペースのレポートと適用を有効にします

ONTAP 9.4 以降では、論理スペースのレポートを有効にすることができます。9.5 以降では、論理スペースの適用を有効にすることも、レポートと適用の両方を同時に有効にすることもできます。

このタスクについて

個々のボリュームレベルで論理スペースのレポートと適用を有効にできるだけでなく、この機能をサポートするすべてのボリュームについて SVM レベルで有効にすることができます。SVM 全体で論理スペース機能を有効にする場合は、個々のボリュームに対して無効にすることもできます。

ONTAP 9.8以降では、SnapMirrorソースボリュームで論理スペースのレポートを有効にすると、転送後にデスティネーションボリュームで自動的に有効になります。

ONTAP 9.13.1以降では、SnapMirrorソースボリュームで適用オプションが有効になっていると、デスティネーションで論理スペースの消費が報告されて適用されるため、より適切なキャパシティプランニングが可能になります。



ONTAP 9.13.1より前のONTAP リリースを実行している場合、適用設定はSnapMirrorデスティネーションボリュームに転送されますが、デスティネーションボリュームでは適用がサポートされないことを理解しておく必要があります。そのため、デスティネーションでは論理スペースの使用量は報告されますが、適用は実行されません。

の詳細を確認してください ["ONTAP リリースでの論理スペースのレポートのサポート"](#)。

選択肢

- ボリュームの論理スペースのレポートを有効にします。

```
volume modify -vserver svm_name -volume volume_name -size volume_size -is-space-reporting-logical true
```

- ボリュームの論理スペースの適用を有効にします。

```
volume modify -vserver svm_name -volume volume_name -size volume_size -is-space-enforcement-logical true
```

- ボリュームの論理スペースのレポートと適用を一緒に有効にします。

```
volume modify -vserver svm_name -volume volume_name -size volume_size -is-space-reporting-logical true -is-space-enforcement-logical true
```

- 新しい SVM の論理スペースのレポートまたは適用を有効にします。



```
vserver create -vserver _svm_name_ -rootvolume root-_volume_name_ -rootvolume
-security-style unix -data-services {desired-data-services} [-is-space-
reporting-logical true] [-is-space-enforcement-logical true]
```

- 既存の SVM の論理スペースのレポートまたは適用を有効にします。

```
vserver modify -vserver _svm_name_ {desired-data-services} [-is-space-
reporting-logical true] [-is-space-enforcement-logical true]
```

## SVMの容量制限を管理します

ONTAP 9.13.1以降では、Storage VM（SVM）に最大容量を設定できます。また、SVMの容量レベルがしきい値に近づいたときにアラートを設定することもできます。

### このタスクについて

SVM上の容量は、FlexVol、FlexGroup、FlexClone、FlexCache の合計として計算されます。削除後にボリュームが制限状態、オフライン状態、またはリカバリキュー内にある場合でも、ボリュームは容量の計算に影響します。ボリュームで自動拡張が設定されている場合は、ボリュームの最大オートサイズの値がSVMのサイズに合わせて計算されます。自動拡張を設定しない場合は、ボリュームの実際のサイズが計算されます。

次の表に、その方法を示します autosize-mode パラメータは容量の計算に影響します。

autosize-mode off	サイズパラメーターは計算に使用されます
autosize-mode grow	。 max-autosize パラメータは計算に使用されます
autosize-mode grow-shrink	。 max-autosize パラメータは計算に使用されます

### 作業を開始する前に

- SVM数の上限を設定するには、クラスタ管理者である必要があります。
- ストレージ制限は、データ保護ボリュームを含むSVM、SnapMirror関係にあるボリューム、またはMetroCluster 構成には設定できません。
- SVMを移行する際、ソースSVMでストレージの制限を有効にすることはできません。移行処理を完了するには、ソースのストレージ制限を無効にしてから移行を完了してください。
- SVMの容量とは異なります [クォータ](#)。クォータは最大サイズを超えることはできません。
- SVMで他の処理を実行中のときは、ストレージ制限を設定することはできません。を使用します `job show vservser svm_name` コマンドを使用して既存のジョブを表示します。ジョブが完了したら、もう一度コマンドを実行してください。

### 容量への影響

容量制限に達すると、次の処理が失敗します。

- LUN、ネームスペース、またはボリュームを作成しています
- LUN、ネームスペース、またはボリュームのクローニング
- LUN、ネームスペース、またはボリュームを変更しています
- LUN、ネームスペース、またはボリュームのサイズの拡張




- LUN、ネームスペース、またはボリュームを拡張する
- LUN、ネームスペース、またはボリュームをリホストします

新しい**SVM**に容量制限を設定します

### System Manager の略

手順

1. >[Storage VMs]\*を選択します。
2. 選択するオプション  をクリックしてSVMを作成します。
3. SVMに名前を付け、\*アクセスプロトコル\*を選択します。
4. で、[最大容量制限を有効にする]\*を選択します。

SVMの最大容量サイズを指定します。

5. [保存（Save）]を選択します。

### CLI の使用

手順

1. SVMを作成ストレージの制限を設定するには、を指定します `storage-limit` 価値。ストレージ制限のしきい値アラートを設定するには、の割合を指定します `-storage-limit-threshold` `-alert`。

```
vserver create -vserver vserver_name -aggregate aggregate_name -rootvolume
root_volume_name -rootvolume-security-style {unix|ntfs|mixed} -storage
-limit value [GiB|TiB] -storage-limit-threshold-alert percentage [-ipSpace
IPspace_name] [-language <language>] [-snapshot-policy
snapshot_policy_name] [-quota-policy quota_policy_name] [-comment comment]
```

しきい値を指定しない場合、デフォルトでは、SVMの容量が90%に達したときにアラートがトリガーされます。しきい値アラートを無効にするには、値を0にします。

2. SVMが作成されたことを確認します。

```
vserver show -vserver vserver_name
```

3. ストレージの上限を無効にする場合は、を使用してSVMを変更します `-storage-limit` パラメータをゼロに設定：

```
vserver modify -vserver vserver_name -storage-limit 0
```


既存の**SVM**の容量制限を設定または変更する

既存のSVMに対して容量制限としきい値アラートを設定したり、容量制限を無効にしたりできます。

容量制限を設定したあとに、現在割り当てられている容量よりも小さい値に変更することはできません。

## System Manager の略

### 手順

1. >[Storage VMs]\*を選択します。
2. 変更するSVMを選択します。SVM名の横にあるを選択します  次に\*[編集]\*をクリックします。
3. 容量制限を有効にするには、\*容量制限を有効にする\*の横にあるボックスを選択します。[Maximum capacity]に値を入力し、[Alert threshold]にパーセント値を入力します。

容量制限を無効にする場合は、[容量制限を有効にする]\*の横にあるチェックボックスをオフにします。

4. [保存 ( Save ) ]を選択します。

## CLI の使用

### 手順

1. SVMをホストするクラスターで、を問題 します `vserver modify` コマンドを実行しますに数値を指定してください `-storage-limit` にパーセント値を入力します `-storage-limit-threshold` `-alert`。

```
vserver modify -vserver vserver_name -storage-limit value [GiB|TiB]
-storage-limit-threshold-alert percentage
```

しきい値を指定しないと、容量の90%となるデフォルトのアラートが生成されます。しきい値アラートを無効にするには、値を0にします。

2. ストレージの上限を無効にする場合は、を使用してSVMを変更します `-storage-limit` ゼロに設定：

```
vserver modify -vserver vserver_name -storage-limit 0
```

### 容量の上限に達しています

最大容量またはアラートしきい値に達した場合は、を参照してください `vserver.storage.threshold` EMSメッセージを表示するか、System Managerの\* Insights \*ページで実行可能な対処方法を確認してください。考えられる解決策は次のとおりです。

- SVMの最大容量制限を編集しています
- ボリュームリカバリキューをパージしてスペースを解放します
- ボリュームにスペースを確保するには、Snapshotを削除します

### 追加情報

- [System Manager で測定される容量](#)
- [System Manager で容量を監視](#)

クォータは、リソース使用量を制限または追跡するために使用します

## クォータプロセスの概要

### クォータプロセス

クォータを使用すると、ユーザ、グループ、または qtree によって使用されるディスクスペースやファイル数を制限したり、追跡したりできます。クォータは、特定の FlexVol または qtree に適用されます。

クォータには、ソフトクォータとハードクォータがあります。ソフトクォータ原因 ONTAP では、指定された制限を超過すると通知が送信されますが、ハードクォータでは、指定された制限を超過すると書き込み処理が失敗します。

ONTAP は、FlexVol ボリュームへの書き込み要求をユーザまたはユーザグループから受信すると、そのボリュームでユーザまたはユーザグループに対してクォータがアクティブ化されているかどうかをチェックし、次の点を判断します。

- ハードリミットに到達するかどうか

「はい」の場合は、ハードリミットに達したときに書き込み処理が失敗し、ハードクォータ通知が送信されます。

- ソフトリミットを超過するかどうか

「はい」の場合は、ソフトリミットを超えても書き込み処理が成功し、ソフトクォータ通知が送信されません。

- 書き込み処理でソフトリミットを超えないかどうか

「はい」の場合は、書き込み処理が成功し、通知は送信されません。

### ハードクォータ、ソフトクォータ、およびしきい値クォータの違い

ハードクォータは処理を阻止し、ソフトクォータは通知をトリガーします。

ハードクォータを設定すると、システムリソースにハードリミットが適用されます。実行することで制限値を超えてしまう処理は、すべて失敗します。以下の設定でハードクォータを作成します。

- ディスク制限パラメータ
- ファイル制限パラメータ

ソフトクォータを設定すると、リソース使用量が特定のレベルに達したときに警告メッセージが送信されますが、データアクセス処理には影響しません。そのため、クォータを超過する前に適切な処理を実行できます。ソフトクォータは以下の設定で構成されます。

- ディスク制限しきい値パラメータ
- ディスクのソフトリミットパラメータ
- ファイルのソフトリミットパラメータ

しきい値クォータとソフトディスククォータを使用すると、管理者はクォータについての通知を複数受け取ることができます。通常、書き込みが失敗し始める前にしきい値によって「最終警告」が通知されるようにする

ため、管理者はディスク制限のしきい値をディスク制限よりもわずかに小さい値に設定します。

クォータ通知について

クォータ通知は Event Management System（EMS；イベント管理システム）に送信されるメッセージであり、SNMPトラップとしても設定されます。

通知は次のイベントに対応して送信されます。

- ・つまり、ハードクォータに達したときに、クォータを超えようとしたときです
- ・ソフトクォータを超えています
- ・ソフトクォータを超過しなくなりました

しきい値は他のソフトクォータとは若干異なります。しきい値を指定した場合に通知がトリガーされるのは、しきい値を超えた場合だけです。しきい値を超えた場合は

ハードクォータ通知は volume quota modify コマンドを使用して設定できます。不必要なメッセージが送信されないように、通知を完全にオフにしたり、頻度を変更したりすることができます。

ソフトクォータ通知は、冗長なメッセージが生成される可能性は低く、通知が唯一の目的であるため、設定できません。

次の表に、クォータが EMS システムに送信するイベントを示します。

発生する状況	EMS に送信されるイベント
ツリークォータのハードリミットに達した	<code>wافل.quota.qtree.exceeded</code>
ボリューム上のユーザクォータのハードリミットに達した	<code>wافل.quota.user.exceeded</code> （UNIXユーザの場合） <code>wافل.quota.user.exceeded.win</code> （Windowsユーザの場合）
qtree 上のユーザクォータのハードリミットに達した	<code>wافل.quota.userQtree.exceeded</code> （UNIXユーザの場合） <code>wافل.quota.userQtree.exceeded.win</code> （Windowsユーザの場合）
ボリューム上のグループクォータのハードリミットに達した	<code>wافل.quota.group.exceeded</code>
qtree 上のグループクォータのハードリミットに達した	<code>wافل.quota.groupQtree.exceeded</code>
しきい値を含むソフトリミットを超えている	<code>quota.softlimit.exceeded</code>
ソフトリミットを超過しなくなりました	<code>quota.softlimit.normal</code>

次の表に、クォータで生成される SNMP トラップを示します。

発生する状況	送信される <b>SNMP</b> トラップ
ハードリミットに達しました	quotaExceeded です
しきい値を含むソフトリミットを超えている	quotaExceeded および softQuotaExceeded です
ソフトリミットを超過しなくなりました	quotaNormal および softQuotaNormal です



通知には、qtree 名ではなく qtree の ID 番号が含まれます。を使用して、qtree 名を ID 番号に関連付けることができます `volume qtree show -id` コマンドを実行します

#### クォータの使用目的

クォータは、FlexVol ボリュームのリソース使用量を制限したり、リソース使用量が特定のレベルに達したときに通知したり、リソース使用量を追跡したりするために使用できます。

クォータを指定する理由は次のとおりです。

- ユーザやグループが使用できる、または qtree に格納できる、ディスクスペースの容量やファイル数を制限する場合
- 制限を適用せずに、ユーザ、グループ、または qtree によって使用されるディスクスペースの容量やファイル数を追跡する場合
- ディスク使用率やファイル使用率が高いときにユーザに警告する場合

ディスク使用量を最も効率的に管理するには、デフォルトクォータ、明示的クォータ、派生クォータ、および追跡クォータを使用します。

#### クォータルール、クォータポリシー、およびクォータとは

クォータは、FlexVol ボリュームに固有のクォータルールで定義されます。これらのクォータルールは Storage Virtual Machine (SVM) のクォータポリシーにまとめられ、SVM 上の各ボリュームでアクティブ化されます。

クォータルールは常にボリュームに固有です。クォータルールは、クォータルールに定義されているボリュームでクォータがアクティブ化されるまで作用しません。

クォータポリシーは、SVM のすべてのボリュームに対するクォータルールの集まりです。クォータポリシーは SVM 間で共有されません。1 つの SVM に最大 5 つのクォータポリシーを保持できるため、クォータポリシーのバックアップコピーを保持できます。1 つの SVM に割り当てられるクォータポリシーは常に 1 つです。

クォータは、ONTAP で適用される実際の制限、または ONTAP で実行される実際の追跡処理です。クォータルールからは常に少なくとも 1 つのクォータが作成され、そのほかに多数の派生クォータが作成されることもあります。適用クォータの一覧は、クォータレポートでのみ表示できます。

アクティブ化とは、割り当てられたクォータポリシーの現在のクォータルールセットから適用クォータを作成するように ONTAP をトリガーするプロセスです。アクティブ化はボリューム単位で実行されます。ボリュームでのクォータの最初のアクティブ化を初期化と呼びます。以降のアクティブ化は、変更の範囲に応じて再初期化またはサイズ変更と呼びます。



ボリューム上のクォータを初期化またはサイズ変更すると、その SVM に現在割り当てられているクォータポリシー内のクォータルールがアクティブ化されます。

#### クォータのターゲットとタイプ

クォータにはユーザ、グループ、またはツリーのいずれかのタイプがあります。クォータターゲットは、クォータ制限が適用されるユーザ、グループ、または qtree を指定します。

次の表に、クォータターゲットの種類、各クォータターゲットに関連付けられているクォータのタイプ、および各クォータターゲットの指定方法を示します。

クォータターゲット	クォータタイプ	ターゲットの指定方法	注：
ユーザ	ユーザクォータ	UNIX ユーザ名 UNIX UID  UID がユーザと一致しているファイルまたはディレクトリ  Windows 2000 より前の形式の Windows ユーザ名  Windows SID  ユーザの SID によって所有されている ACL を持つファイルまたはディレクトリ	ユーザクォータは、特定のボリュームまたは qtree に適用できます。
グループ	グループクォータ	UNIX グループ名 UNIX GID  GID がグループと一致するファイルまたはディレクトリ	グループクォータは、特定のボリュームまたは qtree に適用できます。  <div>            ONTAP では、Windows ID に基づいてグループクォータを適用しません。         </div>
qtree	ツリークォータ	qtree 名	ツリークォータは特定のボリュームに適用され、他のボリューム内の qtree には影響しません。

""	ユーザ quotagroup ク ォータ  ツリークォ ータ	二重引用符（""）	と表示されたクォータターゲット は、a_default QUOTA_示されてい ます。デフォルトクォータの場合、 クォータのタイプは type フィールド の値によって決まります。
----	---	-----------	--

## 特殊なクォータ

### デフォルトクォータの機能

デフォルトクォータを使用して、特定のクォータタイプのすべてのインスタンスにクォータを適用できます。たとえば、デフォルトユーザクォータは、指定した FlexVol または qtree について、システム上のすべてのユーザに適用されます。また、デフォルトクォータを使用すると、クォータを簡単に変更できます。

デフォルトクォータを使用すると、大量のクォータターゲットに自動的に制限を適用でき、ターゲットごとに個別のクォータを作成する必要はありません。たとえば、ほとんどのユーザの使用ディスクスペースを 10GB に制限する場合、ユーザごとにクォータを作成する代わりに、10GB のディスクスペースのデフォルトユーザクォータを指定できます。特定のユーザに異なる制限を適用する場合は、それらのユーザに対して明示的クォータを作成できます。（特定のターゲットまたはターゲットリストを指定した明示的クォータは、デフォルトクォータを上書きします）。

また、デフォルトクォータを使用すると、クォータの変更を有効にする必要がある場合に、再初期化ではなくサイズ変更を使用できます。たとえば、すでにデフォルトユーザクォータが設定されているボリュームに明示的ユーザクォータを追加すると、サイズ変更によって新しいクォータをアクティブ化できます。

デフォルトクォータは、3 種類のクォータターゲット（ユーザ、グループ、および qtree）のすべてに適用できます。

デフォルトクォータには、必ずしも制限を指定する必要はありません。デフォルトクォータは追跡クォータにもなります。

クォータは、コンテキストに応じて、空の文字列（""）またはアスタリスク（\*）であるターゲットによって示されます。

- を使用してクォータを作成した場合 volume quota policy rule create コマンドを実行し、を設定します -target 空の文字列（""）のパラメータを指定すると、デフォルトクォータが作成されます。
- を参照してください volume quota policy rule create コマンドを入力します -qtree パラメータは、クォータルールの適用先のqtreeの名前を指定します。このパラメータは、ツリータイプのルールには適用されません。ボリュームレベルのユーザまたはグループのタイプルールの場合、このパラメータには "" を指定する必要があります。
- をクリックします volume quota policy rule show コマンドを実行すると、デフォルトクォータのターゲットに空の文字列（""）が表示されます。
- をクリックします volume quota report コマンドを実行すると、デフォルトクォータのIDとクォータ指定子にアスタリスク（\*）が表示されます。

## デフォルトユーザクォータの例

次のクォータルールでは、デフォルトユーザクォータを使用して、vol1の各ユーザに50MBの制限を適用しています。

```
cluster1::> volume quota policy rule create -vserver vs0 -volume vol1
-policy-name default -type user -target "" -qtree "" -disk-limit 50m
```

```
cluster1::> volume quota policy rule show -vserver vs0 -volume vol1
```

Vserver: vs0			Policy: default		Volume: vol1		
Type	Target	Qtree	User Mapping	Disk Limit	Soft Disk Limit	Soft Files Limit	
user	""	""	off	50MB	-	-	

システム上原因のユーザが、vol1内に占めるそのユーザのデータが50MBを超えるようなコマンドを入力した場合（エディタからのファイルへの書き込みなど）、そのコマンドは失敗します。

## 明示的クォータの使用方法

明示的クォータは、特定のクォータターゲットに対してクォータを指定する場合、または特定のターゲットに対するデフォルトクォータを上書きする場合に使用できます。

明示的クォータは、特定のユーザ、グループ、または qtree の制限を指定します。同じターゲットに設定されているデフォルトクォータがある場合は、明示的クォータによって置き換えられます。

派生ユーザクォータを持つユーザに明示的ユーザクォータを追加する場合は、デフォルトユーザクォータと同じユーザマッピング設定を使用する必要があります。そうしないと、クォータのサイズを変更したときに、明示的ユーザクォータが新しいクォータとみなされて拒否されます。

明示的クォータが影響するのは、同じレベル（ボリュームまたは qtree）のデフォルトクォータのみです。たとえば、qtree の明示的ユーザクォータが、その qtree を含むボリュームのデフォルトユーザクォータに影響することはありません。ただし、qtree の明示的ユーザクォータは、その qtree のデフォルトユーザクォータを上書きします（制限を置き換えます）。

## 明示的クォータの例

次のクォータルールは、vol1内のすべてのユーザのスペースを50MBに制限するデフォルトユーザクォータを定義します。ただし、jsmithという1人のユーザには、明示的クォータ（太字）により80MBのスペースが許可されています。



```
cluster1::> volume quota policy rule create -vserver vs0 -volume vol1
-policy-name default -type user -target "" -qtree "" -disk-limit 50m

cluster1::> volume quota policy rule create -vserver vs0 -volume vol1
-policy-name default -type user -target "jsmith" -qtree "" -disk-limit 80m

cluster1::> volume quota policy rule show -vserver vs0 -volume vol1
```

Vserver: vs0			Policy: default		Volume: vol1		
Type	Target	Qtree	User Mapping	Disk Limit	Soft Disk Limit	Files Limit	Soft Files Limit
user	""	""	off	50MB	-	-	-
user	jsmith	""	off	80MB	-	-	-

次のクォータルールでは、4つのIDで表されるユーザを、vol1ボリューム内の550MBのディスクスペースと10、000ファイルに制限しています。

```
cluster1::> volume quota policy rule create -vserver vs0 -volume vol1
-policy-name default -type user -target "
jsmith,corp\jsmith,engineering\john smith,S-1-5-32-544" -qtree "" -disk
-limit 550m -file-limit 10000

cluster1::> volume quota policy rule show -vserver vs0 -volume vol1
```

Vserver: vs0			Policy: default		Volume: vol1		
Type	Target	Qtree	User Mapping	Disk Limit	Soft Disk Limit	Files Limit	Soft Files Limit
user	"jsmith,corp\jsmith,engineering\john smith,S-1-5-32-544"	""	off	550MB	-	10000	-

次のクォータルールは、eng1グループのディスクスペースを150MBに制限し、proj1 qtree内のファイル数を無制限に制限します。

```
cluster1::> volume quota policy rule create -vserver vs0 -volume vol2
-policy-name default -type group -target "eng1" -qtree "proj1" -disk-limit
150m
```

```
cluster1::> volume quota policy rule show -vserver vs0 -volume vol2
```

Vserver: vs0			Policy: default			Volume: vol2	
					Soft		Soft
			User	Disk	Disk	Files	Files
Type	Target	Qtree	Mapping	Limit	Limit	Limit	Limit
Threshold							
-----	-----	-----	-----	-----	-----	-----	-----
-----							
group	eng1	proj1	off	150MB	-	-	-
-							

次のクォータルールでは、vol2ボリューム内のproj1 qtreeのディスクスペースが750MB、ファイル数が75、000に制限されています。

```
cluster1::> volume quota policy rule create -vserver vs0 -volume vol2
-policy-name default -type tree -target "proj1" -disk-limit 750m -file
-limit 75000
```

```
cluster1::> volume quota policy rule show -vserver vs0 -volume vol2
```

Vserver: vs0			Policy: default			Volume: vol2	
					Soft		Soft
			User	Disk	Disk	Files	Files
Type	Target	Qtree	Mapping	Limit	Limit	Limit	Limit
Threshold							
-----	-----	-----	-----	-----	-----	-----	-----
-----							
tree	proj1	""	-	750MB	-	75000	-
-							

## 派生クォータの機能

明示的クォータ（特定のターゲットを指定したクォータ）によってではなく、デフォルトクォータによって適用されるクォータを、`_derived quota_`と呼びます。

派生クォータの数と場所は、クォータタイプによって異なります。

- ボリューム上のデフォルトツリークォータによって、そのボリューム上のすべてのqtreeに派生デフォルトツリークォータが作成されます。

- デフォルトユーザクォータまたはデフォルトグループクォータによって、同じレベル（ボリュームまたは qtree）でファイルを所有するユーザまたはグループごとに、派生ユーザクォータまたは派生グループクォータが作成されます。
- ボリューム上のデフォルトユーザクォータまたはデフォルトグループクォータによって、ツリークォータもあるすべての qtree に、派生デフォルトユーザクォータまたは派生グループクォータが作成されます。

制限やユーザマッピングなどの派生クォータの設定は、対応するデフォルトクォータの設定と同じです。たとえば、ボリュームに 20GB のディスク制限が適用されるデフォルトツリークォータの場合、そのボリュームの qtree に 20GB のディスク制限が適用される派生ツリークォータを作成します。デフォルトクォータが追跡クォータ（制限なし）の場合、派生クォータも追跡クォータになります。

派生クォータを確認するには、クォータレポートを生成します。レポートでは、派生ユーザクォータまたは派生グループクォータは、ブランクまたはアスタリスク（\*）のクォータ指定子で示されます。ただし派生ツリークォータにはクォータ指定子が指定されます。派生ツリークォータを特定するには、そのボリューム上で同じ制限が適用されるデフォルトのツリークォータを探す必要があります。

明示的クォータは、派生クォータと次のように連動します。

- 同じターゲットにすでに明示的クォータが存在する場合は、派生クォータは作成されません。
- ターゲットに明示的クォータを作成する際に派生クォータが存在する場合は、クォータの完全な初期化を実行する代わりに、サイズ変更によって明示的クォータをアクティブ化できます。

## 追跡クォータの使用方法

追跡クォータでは、ディスクおよびファイルの使用状況についてレポートが生成され、リソースの使用量は制限されません。追跡クォータを使用すると、クォータをいったんオフにしてからオンにしくなくてもクォータのサイズを変更できるため、クォータ値の変更による中断時間が短縮されます。

追跡クォータを作成するには、ディスク制限パラメータとファイル制限パラメータを省略します。これにより ONTAP は、制限を課することなく、ターゲットのレベル（ボリュームまたは qtree）でそのターゲットのディスクとファイルの使用状況を監視するようになります。追跡クォータは、の出力に示されます show コマンドおよびクォータレポートのすべての制限にダッシュが表示されます。ONTAPでは、System Manager UIを使用して明示的クォータ（特定のターゲットを持つクォータ）を作成すると、追跡クォータが自動的に作成されます。CLIを使用する場合、ストレージ管理者は明示的クォータの上に追跡クォータを作成します。

また、ターゲットのすべてのインスタンスを環境で管理する `_default` 追跡 `quota_policy` を指定することもできます。デフォルト追跡クォータを使用すると、あるクォータタイプのすべてのインスタンス（すべての qtree またはすべてのユーザなど）の使用量を追跡できます。また、クォータの変更を有効にする必要がある場合に、クォータの再初期化ではなくサイズ変更を使用できます。

## 例

ボリュームレベルの追跡ルール 次の例に示すように、追跡ルールの出力には、qtree、ユーザ、およびグループの追跡クォータが表示されます。

Vserver: vs0			Policy: default			Volume: fv1		
Type	Target	Qtree	User	Disk	Soft Disk	Files	Soft Files	Threshold
			Mapping	Limit	Limit	Limit	Limit	
tree	""	""	-	-	-	-	-	-
user	""	""	off	-	-	-	-	-
group	""	""	-	-	-	-	-	-

## クォータの適用方法

クォータの適用方法を理解すると、クォータを設定し、想定される制限を設定できます。

クォータが有効な FlexVol ボリュームでファイルの作成またはファイルへのデータの書き込みを試行されると、処理が続行される前にクォータ制限がチェックされます。その処理がディスク制限またはファイル制限を超える場合、その処理は実行されません。

クォータ制限は次の順序でチェックされます。

1. その qtree のツリークォータ（ファイルの作成または書き込みが qtree0 に対して行われる場合、このチェックは行われません）
2. ボリューム上のファイルを所有しているユーザのユーザクォータ
3. ボリューム上のファイルを所有しているグループのグループクォータ
4. その qtree のファイルを所有しているユーザのユーザクォータ（ファイルの作成または書き込みが qtree0 に対して行われる場合、このチェックは行われません）
5. その qtree のファイルを所有しているグループのグループクォータ（ファイルの作成または書き込みが qtree0 に対して行われる場合、このチェックは行われません）

最も上限の低いクォータが、最初に超過するクォータとはかぎりません。たとえば、ボリューム vol1 のユーザクォータが 100GB の場合、また、ボリューム vol1 に含まれる qtree q2 のユーザクォータは 20GB、そのユーザがすでに 80GB を超えるデータをボリューム vol1 に（ただし qtree q2 以外）書き込んでいる場合、ボリュームの制限を最初に超過する可能性があります。

## クォータポリシーの割り当てに関する考慮事項

クォータポリシーは、SVM のすべての FlexVol に対するクォータルールをグループ化したものです。クォータポリシーを割り当てる際には、一定の考慮事項に注意する必要があります。

- SVM には、常に 1 つのクォータポリシーが割り当てられています。SVM が作成されると、空のクォータポリシーが作成され、SVM に割り当てられます。このデフォルトのクォータポリシーには、SVM の作成時に別の名前を指定しないかぎり、「default」という名前が付けられます。
- SVM には、最大 5 つのクォータポリシーを設定できます。1 つの SVM に 5 つのクォータポリシーが存在する場合、既存のクォータポリシーを削除しないかぎり、その SVM に新しいクォータポリシーを作成できません。

- クォータポリシーのクォータルールを作成または変更する必要がある場合は、次のいずれかの方法を選択できます。
    - SVM に割り当てられているクォータポリシーを直接編集します。その場合、そのクォータポリシーを SVM に割り当てする必要はありません。
    - 割り当てられていないクォータポリシーを編集し、そのポリシーを SVM に割り当てます。その場合、必要に応じて元に戻せるように、クォータポリシーのバックアップを作成しておく必要があります。
- たとえば、割り当てられているクォータポリシーのコピーを作成して、そのコピーを変更して変更したコピーを SVM に割り当て、元のクォータポリシーの名前を変更します。
- クォータポリシーの名前変更は、そのクォータポリシーが SVM に割り当てられている場合でも可能です。

## ユーザおよびグループとクォータ

### クォータとユーザおよびグループとの連携の概要

ユーザまたはグループをクォータのターゲットとして指定すると、そのクォータの制限がそのユーザまたはグループに適用されます。ただし、一部の特殊なグループとユーザについては処理が異なります。ユーザの ID を指定する方法は環境によって異なります。

### クォータに **UNIX** ユーザを指定する方法

クォータに UNIX ユーザを指定するには、ユーザ名、UID、またはユーザによって所有されているファイルまたはディレクトリの 3 つの形式のいずれかを使用します。

クォータに UNIX ユーザを指定するには、次のいずれかの形式を使用します。

- jsmith などのユーザ名



UNIX ユーザ名にバックスラッシュ (\) または @ 記号が含まれている場合、その名前を使用してクォータを指定することはできません。ONTAP では、これらの文字を含む名前は Windows 名として処理されます。

- UID (20 など)。
- ユーザが所有するファイルまたはディレクトリのパス。ファイルの UID がユーザと一致するように設定されます。



ファイル名またはディレクトリ名を指定する場合は、システム上で対象のユーザアカウントを使用するかぎり削除されることのないファイルまたはディレクトリを選択する必要があります。

UID のファイルまたはディレクトリ名原因 ONTAP を指定しても、そのファイルまたはディレクトリにクォータを適用されるわけではありません。

## クォータに **Windows** ユーザを指定する方法

クォータに Windows ユーザを指定するには、Windows 2000 より前の形式の Windows ユーザ名、SID、ユーザの SID によって所有されているファイルまたはディレクトリの 3 つの形式のいずれかを使用します。

クォータに Windows ユーザを指定するには、次のいずれかの形式を使用します。

- Windows 2000 より前の形式の Windows 名。
- S-1-5-32-544 など、Windows によってテキスト形式で表示される Security ID（SID；セキュリティ ID）。
- ユーザの SID によって所有されている ACL を持つファイルまたはディレクトリの名前。

ファイル名またはディレクトリ名を指定する場合は、システム上で対象のユーザアカウントを使用するかぎり削除されることのないファイルまたはディレクトリを選択する必要があります。

ONTAP が ACL から SID を取得するには、その ACL が有効である必要があります。



ファイルまたはディレクトリが UNIX 形式の qtree に存在する場合、またはストレージシステムでユーザ認証に UNIX モードが使用されている場合、ONTAP は、SID ではなく UID \* がファイルまたはディレクトリの UID に一致するユーザにユーザクォータを適用します。

ファイルまたはディレクトリ原因 ONTAP の名前でクォータのユーザを指定しても、そのファイルまたはディレクトリにクォータを適用されるわけではありません。

## デフォルトのユーザクォータおよびグループクォータで派生クォータを作成する方法

デフォルトのユーザクォータまたはグループクォータを作成すると、同じレベルでファイルを所有するユーザまたはグループごとに、対応する派生ユーザクォータまたは派生グループクォータが自動的に作成されます。

派生ユーザクォータと派生グループクォータは、次のように作成されます。

- FlexVol 上のデフォルトユーザクォータによって、ボリューム上のファイルを所有するすべてのユーザに派生ユーザクォータが作成されます。
- qtree 上のデフォルトユーザクォータによって、qtree 内のファイルを所有するすべてのユーザに派生ユーザクォータが作成されます。
- FlexVol 上のデフォルトグループクォータによって、ボリューム上の任意の場所のファイルを所有するすべてのグループに派生グループクォータが作成されます。
- qtree 上のデフォルトグループクォータによって、qtree 内のファイルを所有するすべてのグループに派生グループクォータが作成されます。

デフォルトのユーザクォータまたはグループクォータのレベルでファイルを所有していないユーザまたはグループには、派生クォータは作成されません。たとえば、qtree proj1 にデフォルトユーザクォータが作成され、ユーザ jsmith が異なる qtree 上のファイルを所有している場合、jsmith には派生ユーザクォータが作成されません。

派生クォータの設定は、制限やユーザマッピングなど、デフォルトクォータと同じです。たとえば、デフォルトユーザクォータのディスク制限が 50MB でユーザマッピングが有効の場合、作成される派生クォータもディスク制限が 50MB でユーザマッピングが有効になります。

ただし、3 つの特殊なユーザとグループの場合、派生クォータに制限はありません。次のユーザとグループがデフォルトのユーザクォータまたはグループクォータのレベルでファイルを所有している場合、派生クォータはデフォルトのユーザクォータまたはグループクォータと同じユーザマッピング設定で作成されますが、単なる追跡クォータになります（制限なし）。

- UNIX root ユーザ（UID 0）
- UNIX ルートグループ（GID 0）
- Windows BUILTIN\Administrators グループ

Windows グループのクォータはユーザクォータとして追跡されるため、このグループの派生クォータは、デフォルトグループクォータではなくデフォルトユーザクォータから派生するユーザクォータになります。

#### 派生ユーザクォータの例

root、jsmith、および bob -own の 3 人のファイルが格納されているボリュームにデフォルトユーザクォータを作成すると、ONTAP によって自動的に 3 つの派生ユーザクォータが作成されます。このため、このボリュームのクォータを再初期化すると、次の 4 つの新しいクォータがクォータレポートに表示されます。

```
cluster1::> volume quota report
Vserver: vs1
```

Volume	Tree	Type	ID	Used	Limit	Used	Limit	Quota
Specifier								
vol1		user	*	0B	50MB	0	-	*
vol1		user	root	5B	-	1	-	
vol1		user	jsmith	30B	50MB	10	-	*
vol1		user	bob	40B	50MB	15	-	*

4 entries were displayed.

最初の新しい行は作成したデフォルトユーザクォータで、ID がアスタリスク（\*）であることから判別できます。ほかの新しい行は派生ユーザクォータです。jsmith と bob の派生クォータのディスク制限は、デフォルトクォータと同じく 50MB です。root ユーザの派生クォータは、制限のない追跡クォータです。

#### root ユーザへのクォータの適用方法

UNIX クライアント上の root ユーザ（UID=0）はツリークォータの影響を受けますが、ユーザクォータまたはグループクォータの影響を受けません。これにより、root ユーザは、通常ならクォータによって妨げられるような操作を他のユーザに代わって実行できます。

root がファイルまたはディレクトリの所有権の変更、またはその他の操作（UNIX など）を実行する場合

chown コマンド) 権限の少ないユーザに代わって、ONTAP は新しい所有者に基づいてクォータをチェックしますが、新しい所有者のハードクォータ制限を超えてもエラーを報告したり処理を停止したりすることはありません。これは、消失データのリカバリなど、管理作業のために一時的にクォータを超過する場合に役立ちます。



ただし、所有権の変更後、クォータの超過中にユーザがディスクスペースの割り当てサイズを増やそうとすると、クライアントシステムによりディスクスペースエラーが報告されます。

## 特殊な **Windows** グループとクォータ

Everyone グループおよび BUILTIN\Administrators グループと、その他の Windows グループでは、クォータの適用方法が異なります。

次のリストは、クォータターゲットが特別な Windows GID である場合の処理を示しています。

- クォータターゲットが Everyone グループである場合、ACL で所有者が Everyone になっているファイルには Everyone の SID で処理されます。
- クォータターゲットが BUILTIN\Administrators である場合、そのエントリは追跡だけを目的としたユーザクォータであるとみなされます。

BUILTIN\Administrators には制限を適用できません。

BUILTIN\Administrators のメンバーがファイルを作成した場合、そのファイルは BUILTIN\Administrators によって所有され、そのユーザの個人 SID ではなく、BUILTIN\Administrators の SID にカウントされます。



ONTAP では、Windows GID に基づいたグループクォータはサポートされません。Windows GID をクォータターゲットとして指定した場合、そのクォータはユーザクォータとみなされます。

## 複数の ID を持つユーザにクォータを適用する方法

ユーザは複数の ID で表すことができます。ID のリストをクォータターゲットとして指定して、このようなユーザに対して単一のユーザクォータを設定できます。これらの ID のいずれかによって所有されるファイルには、ユーザクォータの制限が適用されます。

ユーザが UNIX の UID 20 と、Windows ID の corp\john\_smith および engineering\jsmith を持っているとします。このユーザに対して、UID および Windows ID のリストをクォータターゲットとするクォータを指定できます。このユーザがストレージシステムに書き込むと、その書き込み元が UID 20、corp\john\_smith、あるいは engineering\jsmith のいずれの場合でも、指定されたクォータが適用されます。



複数の ID が同じユーザに属している場合でも、別々のクォータルールは別々のターゲットとみなされます。たとえば、UID 20 と corp\john\_smith が同一のユーザを表す場合でも、UID 20 のディスクスペースを 1GB に制限するクォータを指定し、corp\john\_smith のディスクスペースを 2GB に制限する別のクォータを指定できます。ONTAP は UID 20 と corp\john\_smith に対して個別にクォータを適用します。

この場合、同じユーザが使用する他の ID に制限が適用される場合でも、engineering\jsmith には制限が適用されません。



## ONTAP が混在環境でユーザ ID を決定する方法

ユーザが Windows クライアントと UNIX クライアントの両方から ONTAP ストレージにアクセスする場合は、ファイルの所有権を決定するために、Windows セキュリティと UNIX セキュリティの両方のセキュリティ形式が使用されます。ONTAP では、ユーザクォータの適用時に UNIX ID と Windows ID のどちらを使用するかを、複数の条件から決定します。

ファイルを含む qtree または FlexVol ボリュームのセキュリティ形式が NTFS のみまたは UNIX のみである場合、そのセキュリティ形式によって、ユーザクォータの適用時に使用される ID の種類が決定されます。mixed セキュリティ形式の qtree の場合、使用される ID の種類は、ファイルに ACL が設定されているかどうかによって決まります。

次の表に、使用される ID の種類を示します。

セキュリティ形式	アクセスできます	ACL はありません
「UNIX」	UNIX ID	UNIX ID
混在	Windows ID	UNIX ID
NTFS	Windows ID	Windows ID

### 複数のユーザがターゲットであるクォータ

複数のユーザを同じクォータターゲットに指定した場合、そのクォータで定義されているクォータ制限は各ユーザに個別に適用されるのではなく、クォータターゲットにリストされているすべてのユーザ間でクォータ制限が共有されます。

ボリュームや qtree などのオブジェクトを管理するコマンドとは異なり、マルチユーザクォータなどのクォータターゲットの名前は変更できません。つまり、マルチユーザクォータが定義されたあとで、クォータターゲット内のユーザを変更することはできず、ターゲットへのユーザの追加やターゲットからのユーザの削除もできません。マルチユーザクォータに対してユーザを追加または削除する場合は、そのユーザを含むクォータを削除し、ターゲットに定義されているユーザを使用して新しいクォータルールを定義する必要があります。



複数のユーザクォータを 1 つのマルチユーザクォータに結合する場合、クォータのサイズを変更することで変更をアクティブ化できます。ただし、複数のユーザを含むクォータターゲットからユーザを削除する場合、またはすでに複数のユーザを含むターゲットにユーザを追加する場合は、変更を有効にするためにクォータを再初期化する必要があります。

### クォータルールに複数のユーザが含まれる例

次の例では、クォータエントリに 2 人のユーザがリストされています。2 人のユーザーは、合計で最大 80MB のスペースを使用できます。一方が 75MB を使用している場合、もう一方は 5MB しか使用できません。

```
cluster1::> volume quota policy rule create -vserver vs0 -volume vol1
-policy-name default -type user -target "jsmith,chen" -qtree "" -disk
-limit 80m

cluster1::> volume quota policy rule show -vserver vs0 -volume vol1
```

Vserver: vs0			Policy: default		Volume: vol1		
					Soft		Soft
			User	Disk	Disk	Files	Files
Type	Target	Qtree	Mapping	Limit	Limit	Limit	Limit
Threshold							
-----	-----	-----	-----	-----	-----	-----	-----
-----							
user	"jsmith,chen"	""	off	80MB	-	-	-
-							

クォータの **UNIX** 名と **Windows** 名をリンクさせる方法

混在環境では、ユーザは Windows ユーザまたは UNIX ユーザとしてログインできます。クォータは、ユーザの UNIX ID と Windows ID が同じユーザを表すことを認識するように設定できます。

次の両方の条件が満たされると、Windows ユーザ名のクォータは UNIX ユーザ名にマッピングされ、UNIX ユーザ名のクォータは Windows ユーザ名にマッピングされます。

- user-mapping ユーザのクォータルールでパラメータが「on」に設定されている。
- ユーザ名がにマッピングされている vserver name-mapping コマンド

マッピングされた UNIX 名と Windows 名は同じユーザとして扱われ、クォータ使用量の算定に使用されます。

## qtree とクォータ

クォータを作成する際に、qtree をターゲットにすることができます。これらのクォータを、`_tree quotas` と呼びます。特定の qtree に対して、ユーザクォータやグループクォータを作成することもできます。また、FlexVol ボリュームのクォータは、そのボリュームに含まれる qtree に継承される場合があります。

## ツリークォータの機能

### ツリークォータの機能の概要

qtree をターゲットとしてクォータを作成して、ターゲットの qtree の大きさを制限できます。これらのクォータは、`_tree quotas` と呼ばれます。

qtree にクォータを適用すると、ディスクパーティションと同様の結果が得られます。ただし、クォータを変

更することで、qtree の最大サイズをいつでも変更できます。ツリークォータを適用すると、ONTAP は所有者に関係なく qtree のディスクスペースとファイル数を制限します。書き込み処理によってツリークォータを超える場合、root ユーザと BUILTIN\Administrators グループのメンバーを含むすべてのユーザは qtree への書き込みを行うことができません。



クォータのサイズは、利用可能なスペースの量を保証するものではありません。クォータのサイズは、qtree で使用可能な空きスペースの量よりも多く設定できます。を使用できます volume quota report コマンドを実行して、qtree内で実際に使用可能なスペースの量を確認します。

**qtree** でのユーザクォータおよびグループクォータの処理

ツリークォータは、qtree の全体的なサイズを制限します。個々のユーザまたはグループが qtree 全体を使用するのを防ぐには、その qtree のユーザクォータまたはグループクォータを指定します。

**qtree**内のユーザクォータの例

次のクォータルールがあるとしてします。

```
cluster1::> volume quota policy rule show -vserver vs0 -volume vol1
```

Vserver: vs0			Policy: default			Volume: vol1	
Type	Target	Qtree	User Mapping	Disk Limit	Soft Disk Limit	Files Limit	Soft Files Limit
user	""	""	off	50MB	-	-	-
user	jsmith	""	off	80MB	-	-	-

あるユーザkjonesが、vol1に存在する重要なqtree proj1で大量のスペースを消費しています。次のクォータルールを追加することで、このユーザのスペースを制限できます。

```
cluster1::> volume quota policy rule create -vserver vs0 -volume vol1
-policy-name default -type user -target "kjones" -qtree "proj1" -disk
-limit 20m -threshold 15m
```

```
cluster1::> volume quota policy rule show -vserver vs0 -volume vol1
```

Vserver: vs0			Policy: default		Volume: vol1		
Type	Target	Qtree	User Mapping	Disk Limit	Soft Disk Limit	Files Limit	Soft Files Limit
user	""	""	off	50MB	-	-	-
45MB							
user	jsmith	""	off	80MB	-	-	-
75MB							
user	kjones	proj1	off	20MB	-	-	-
15MB							

## FlexVol ボリ्यूムのデフォルトツリークォータで派生ツリークォータを作成する方法

FlexVol ボリ्यूム上にデフォルトのツリークォータを作成すると、そのボリ्यूム内のすべての qtree に、対応する派生ツリークォータが自動的に作成されます。

これらの派生ツリークォータには、デフォルトのツリークォータと同じ制限があります。他のクォータが存在しない場合、これらの制限は次のように作用します。

- ユーザはそのボリ्यूム全体で割り当てられているスペースと同じスペースを qtree で使用できます（ただし、ルートまたは別の qtree のスペースを使用してボリ्यूムの制限値を超えていない場合）。
- 各 qtree がボリ्यूムの全容量まで拡張できます。

ボリ्यूム上のデフォルトのツリークォータは、そのボリ्यूムに追加されるすべての新しい qtree に引き続き適用されます。新しい qtree が作成されるたびに、派生ツリークォータも作成されます。

すべての派生クォータと同様に、派生ツリークォータは次のように動作します。

- ターゲットに明示的クォータがない場合にのみ作成されます。
- クォータレポートには表示されますが、でクォータルールを表示する場合は表示されません volume quota policy rule show コマンドを実行します

## 派生ツリークォータの例

3 つの qtree （proj1、proj2、および proj3）を含むボリ्यूムが存在し、唯一のツリークォータがディスクサイズを 10GB に限定する proj1 qtree 上の明示的クォータであるとしします。このボリ्यूムでデフォルトのツリークォータを作成し、ボリ्यूムのクォータを再初期化すると、クォータレポートには 4 つのツリークォータが表示されます。

Volume Specifier	Tree	Type	ID	----Disk----		----Files-----		Quota
				Used	Limit	Used	Limit	
-----	-----	-----	-----	-----	-----	-----	-----	
-----								
vol1	proj1	tree	1	0B	10GB	1	-	proj1
vol1		tree	*	0B	20GB	0	-	*
vol1	proj2	tree	2	0B	20GB	1	-	proj2
vol1	proj3	tree	3	0B	20GB	1	-	proj3
...								

最初の行には、proj1 qtree 上の当初の明示的クォータが示されます。このクォータは変更されません。

2 行目には、ボリュームの新しいデフォルトのツリークォータが示されます。アスタリスク（\*）クォータ指定子は、デフォルトクォータであることを示します。このクォータは、作成したクォータールールの結果です。

最後の 2 行には、proj2 および proj3 qtree の新しい派生ツリークォータが示されます。これらのクォータは、ボリューム上のデフォルトのツリークォータの結果として、ONTAP によって自動的に作成されました。これらの派生ツリークォータには、ボリューム上のデフォルトのツリークォータと同じ 20GB のディスク制限があります。proj1 qtree にはすでに明示的クォータが存在するため、proj1 qtree には派生ツリークォータが作成されませんでした。ONTAP

#### FlexVol ボリュームのデフォルトユーザクォータがそのボリュームの qtree のクォータに与える影響

FlexVol ボリュームにデフォルトユーザクォータが定義されている場合、明示的ツリークォータまたは派生ツリークォータが存在する、そのボリュームに含まれるすべての qtree にデフォルトユーザクォータが自動的に作成されます。

qtree にデフォルトユーザクォータがすでに存在する場合は、ボリュームにデフォルトユーザクォータが作成されても qtree のデフォルトユーザクォータが影響を受けることはありません。

qtree に自動的に作成されるデフォルトユーザクォータには、ユーザがボリュームに作成するデフォルトユーザクォータと同じ制限があります。

qtree の明示的ユーザクォータは、管理者が作成した qtree のデフォルトユーザクォータを上書きするのと同様に、自動的に作成されるデフォルトユーザクォータを上書きします（制限を置き換えます）。

#### qtree の変更がクォータに与える影響

##### qtree の変更がクォータの概要に与える影響

qtree を削除したり、名前やセキュリティ形式を変更したりすると、現在適用されているクォータに応じて、ONTAP が適用するクォータが変更される場合があります。

##### qtree の削除がツリークォータに与える影響

qtree を削除すると、その qtree に適用されるクォータはすべて、明示的クォータか派生クォータかにかかわらず、ONTAP によって適用されなくなります。

クォータルールが維持されるかどうかは、qtree を削除した場所によって異なります。

- ONTAP を使用して qtree を削除した場合、ツリークォータルールや、その qtree に設定されているユーザおよびグループクォータルールも含め、その qtree のクォータルールは自動的に削除されます。
- CIFS または NFS クライアントを使用して qtree を削除した場合、クォータの再初期化時のエラー発生を避けるため、このクォータのルールをすべて削除する必要があります。削除した qtree と同じ名前の新しい qtree を作成した場合、既存のクォータルールは、クォータを再初期化するまで新しい qtree に適用されません。

#### qtree の名前変更がクォータに与える影響

ONTAP を使用して qtree の名前を変更すると、その qtree のクォータルールは自動的に更新されます。CIFS または NFS クライアントを使用して qtree の名前を変更する場合、その qtree のクォータルールをすべて更新する必要があります。



CIFS または NFS クライアントを使用して qtree の名前を変更し、クォータを再初期化する前にこの名前での qtree のクォータルールを更新しないと、クォータは qtree および qtree の明示的クォータに適用されません — qtree のツリークォータ、ユーザクォータ、グループクォータも含み、これらは派生クォータに変換されることがあります。

#### qtree のセキュリティ形式の変更がユーザクォータに与える影響

アクセス制御リスト（ACL）は、NTFS または mixed セキュリティ形式では qtree に適用できますが、UNIX セキュリティ形式では適用できません。そのため、qtree のセキュリティ形式を変更すると、クォータの計算方法が変わる可能性があります。qtree のセキュリティ形式を変更した場合は、必ずクォータを再初期化してください。

qtree のセキュリティ形式を NTFS 形式または mixed 形式から UNIX 形式に変更した場合、その qtree 内のファイルに適用された ACL はすべて無視され、ファイルの使用量は UNIX ユーザ ID に基づいて加算されるようになります。

qtree のセキュリティ形式を UNIX 形式から mixed 形式、または NTFS 形式に変更した場合は、それまで非表示だった ACL が表示されるようになります。また、無視されていた ACL が再び有効になり、NFS ユーザ情報が無視されます。既存の ACL がない場合、NFS 情報がクォータの計算で引き続き使用されます。



qtree のセキュリティ形式を変更したあとに UNIX ユーザと Windows ユーザ両方のクォータの使用が正しく計算されるように、その qtree を含むボリュームのクォータを再初期化する必要があります。

#### 例

次の例は、qtree のセキュリティ形式の変更によって、特定の qtree 内のファイルの使用量を加算されるユーザがどのように変わるかを示しています。

qtree A では NTFS セキュリティが有効であり、ACL によって Windows ユーザ corp\joe に 5MB のファイルの所有権が与えられているとします。ユーザ corp\joe には、qtree A について 5MB のディスクスペース使用量が加算されています

ここで、qtree A のセキュリティ形式を NTFS 形式から UNIX 形式に変更します。クォータの再初期化を行うと、Windows ユーザ corp\joe に対して、このファイルが加算されなくなります。代わりに、ファイルの UID

に対応する UNIX ユーザに対して、このファイルが加算されます。UID は、corp\joe にマッピングされた UNIX ユーザまたはルートユーザになります。

#### クォータをアクティブ化する方法

#### クォータをアクティブ化する方法の概要

新しいクォータおよびクォータに対する変更は、アクティブ化されるまで有効になりません。クォータのアクティブ化の仕組みを理解しておくと、クォータをより効率的に管理できます。

クォータはボリュームレベルでアクティブ化できます。

クォータは、`_initializing`（有効にする）または `_resizing` でアクティブ化されます。クォータをいったん無効にして再度有効にする操作は、再初期化と呼ばれます。

アクティブ化にかかる時間とアクティブ化がクォータ適用に及ぼす影響は、アクティブ化のタイプによって異なります。

- 初期化プロセスは2つの部分で構成されます `quota on` ボリュームのファイルシステム全体のジョブおよびクォータスキャン。スキャンはの後に開始されます `quota on` ジョブが正常に完了しました。クォータスキャンには時間がかかることがあり、ボリュームに含まれるファイルが多いほど所要時間は長くなります。スキャンが完了するまで、クォータのアクティブ化は完了せず、クォータも適用されません。
- サイズ変更プロセスでは、のみが実行されます `quota resize` 仕事だサイズ変更にはクォータスキャンが含まれないため、クォータの初期化よりも短時間で完了します。サイズ変更プロセス中もクォータは引き続き適用されます。

デフォルトでは、が表示されます `quota on` および `quota resize` ジョブはバックグラウンドで実行されるため、他のコマンドを同時に使用できます。

アクティブ化プロセスのエラーと警告は、イベント管理システムに送信されます。を使用する場合 `-foreground` パラメータと `volume quota on` または `volume quota resize` コマンドを入力した場合、ジョブが完了するまでコマンドは戻りません。これは、スクリプトから再初期化する場合に便利です。エラーや警告をあとで表示するには、を使用します `volume quota show` コマンドにを指定します `-instance` パラメータ

クォータのアクティブ化は、停止およびリブート後も維持されます。クォータのアクティブ化プロセスがストレージシステムデータの可用性に影響することはありません。

#### サイズ変更を使用できる場合

クォータのサイズ変更はクォータ初期化よりも高速であるため、可能な限りサイズ変更を使用してください。ただし、サイズ変更を使用できるのは、クォータに対する特定の種類のみに限られます。

次の種類の変更をクォータルールに加えた場合、クォータのサイズを変更できます。

- 既存のクォータを変更する場合

たとえば、既存のクォータの制限を変更する場合などです。

- デフォルトクォータまたはデフォルト追跡クォータが適用されているクォータターゲットにクォータを追加した場合
- デフォルトクォータまたはデフォルト追跡クォータのエントリが指定されているクォータを削除した場合
- 別々のユーザクォータを 1 つのマルチユーザクォータに統合した場合



クォータの大幅な変更を行った場合は、完全な再初期化を実行して、すべての変更を確実に有効にしてください。



サイズを変更しようとしてサイズ変更処理では反映できないクォータの変更があった場合、ONTAP は警告を発行します。ストレージシステムが特定のユーザ、グループ、または qtree のディスク使用量を追跡しているかどうかは、クォータレポートから判断できます。クォータレポートにクォータが表示される場合、ストレージシステムは、クォータターゲットによって所有されているディスクスペースとファイル数を追跡しています。

サイズ変更によって有効にできるクォータ変更の例

一部のクォータルール変更は、サイズ変更によって有効にできます。次のクォータを考えてみましょう。

```
#Quota Target type          disk  files thold  sdisk  sfile
#-----
*          user@/vol/vol2    50M   15K
*          group@/vol/vol2   750M   85K
*          tree@/vol/vol2    -      -
jdoe       user@/vol/vol2/   100M   75K
kbuck      user@/vol/vol2/   100M   75K
```

次の変更を行ったとします。

- デフォルトユーザターゲットのファイル数を増やします。
- デフォルトユーザクォータよりも多くのディスク制限が必要な新規ユーザ boris への、新しいユーザクォータの追加
- kbuck ユーザの明示的クォータエントリの削除。この新しいユーザに必要なのは、デフォルトクォータ制限だけになります。

これらの変更により、クォータは次のようになります。

```
#Quota Target type          disk  files thold  sdisk  sfile
#-----
*          user@/vol/vol2    50M   25K
*          group@/vol/vol2   750M   85K
*          tree@/vol/vol2    -      -
jdoe       user@/vol/vol2/   100M   75K
boris      user@/vol/vol2/   100M   75K
```

サイズ変更によって、これらの変更がすべてアクティブ化されます。完全なクォータ再初期化は必要ありません。



ん。

完全なクォータ再初期化が必要な場合

クォータのサイズ変更の方が高速ですが、クォータに特定の変更を加えた場合は、完全なクォータ再初期化を実行する必要があります。

次の状況では、クォータの完全な再初期化を実行する必要があります。

- これまでクォータを持っていなかったターゲット（明示的クォータでもデフォルトクォータから派生したクォータでもない）にクォータを作成した場合。
- qtree のセキュリティ形式を UNIX 形式から mixed 形式、または NTFS 形式に変更する場合
- qtree のセキュリティ形式を mixed 形式または NTFS 形式から UNIX 形式に変更した場合
- 複数のユーザを含むクォータターゲットからユーザを削除する場合、またはすでに複数のユーザを含むターゲットにユーザを追加する場合
- クォータに大幅な変更を加える場合

初期化を必要とするクォータの変更例

3つのqtreeを含むボリュームがあり、そのボリューム内のクォータは3つの明示的ツリークォータだけであるとします。このボリュームに次の変更を加えることにしました。

- 新しい qtree を追加し、新しいツリークォータを作成する
- ボリュームのデフォルトユーザクォータを追加する

これらのどちらの変更にも、クォータの完全な初期化が必要です。クォータのサイズ変更では有効に機能しません。

クォータ情報の表示方法

クォータ情報の概要の表示方法

クォータレポートを使用して、クォータルールおよびクォータポリシーの設定、適用および設定されたクォータ、クォータのサイズ変更および再初期化中に発生したエラーなどの詳細を表示できます。

クォータ情報は、次のような場合に表示すると役に立ちます。

- クォータの設定 — たとえば 'クォータを設定して構成を確認するために使用します
- もうすぐディスクスペースまたはファイルの上限に達する、または上限に達したという通知に対応します
- スペースの拡張要求に応答する

クォータレポートを使用して有効なクォータを確認する方法

クォータインタラクションはさまざまな方法で行われるため、ユーザが明示的に作成したクォータ以外のクォータも有効になります。有効なクォータを確認するには、クォータレポートを表示します。

次に、FlexVol ボリューム vol1 と、このボリュームに含まれる qtree q1 に適用されている各種クォータのクォータレポートを表示する例を示します。

qtreeにユーザクォータが指定されていない例

この例では、ボリューム vol1 に含まれる qtree q1 が存在します。管理者が 3 つのクォータを作成しました。

- vol1に対するデフォルトのツリークォータ制限は400MB
- vol1に対して100MBのデフォルトユーザクォータ制限
- ユーザjsmith用にvol1に対して200MBの明示的ユーザクォータ制限

これらのクォータのクォータルールは、次の例のようになります。

```
cluster1::*> volume quota policy rule show -vserver vs1 -volume vol1
```

Vserver: vs1			Policy: default		Volume: vol1		
Type	Target	Qtree	User Mapping	Disk Limit	Soft Disk Limit	Files Limit	Soft Files Limit
tree	""	""	-	400MB	-	-	-
user	""	""	off	100MB	-	-	-
user	jsmith	""	off	200MB	-	-	-

これらのクォータのクォータレポートの例を次に示します。

```
cluster1::> volume quota report
Vserver: vs1
```

Volume	Tree	Type	ID	----Disk----		----Files-----		Quota
				Used	Limit	Used	Limit	
Specifier								
vol1	-	tree	*	0B	400MB	0	-	*
vol1	-	user	*	0B	100MB	0	-	*
vol1	-	user	jsmith	150B	200MB	7	-	jsmith
vol1	q1	tree	1	0B	400MB	6	-	q1
vol1	q1	user	*	0B	100MB	0	-	
vol1	q1	user	jsmith	0B	100MB	5	-	
vol1	-	user	root	0B	0MB	1	-	
vol1	q1	user	root	0B	0MB	8	-	

クォータレポートの最初の 3 行には、管理者が指定した 3 つのクォータが表示されます。これらのクォータのうちの 2 つはデフォルトクォータであるため、ONTAP は自動的に派生クォータを作成します。

4 行目には、vol1 のすべての qtree （この例では q1 のみ）のデフォルトツリークォータから派生するツリークォータが表示されます。

5 行目には、ボリュームのデフォルトユーザクォータと qtree クォータが存在するために qtree に作成される、デフォルトユーザクォータが表示されます。

6 行目には、jsmith のために qtree に作成される派生ユーザクォータが表示されます。このクォータが作成されるのは、qtree （5 行目）にデフォルトユーザクォータが存在し、ユーザ jsmith がその qtree 上のファイルを所有しているためです。qtree q1 のユーザ jsmith に適用される制限は、明示的ユーザクォータ制限（200MB）では決定されません。これは、明示的ユーザクォータ制限がボリューム上にあるため、qtree の制限には影響しないためです。代わりに、qtree の派生ユーザクォータ制限は、qtree のデフォルトユーザクォータ（100MB）で決定されます。

最後の 2 行には、そのボリュームおよび qtree のデフォルトユーザクォータから派生するその他のユーザクォータが表示されます。root ユーザがボリュームと qtree の両方でファイルを所有しているため、ボリュームと qtree の両方の root ユーザに派生ユーザクォータが作成されました。クォータに関して root ユーザは特別な扱いを受けるため、root ユーザの派生クォータは追跡クォータのみです。

#### qtree にユーザクォータが指定された例

この例は、管理者が qtree にクォータを 2 つ追加したことを除き、前の例と似ています。

この場合も、ボリューム vol1 と qtree q1 が 1 つ残っています。管理者が次のクォータを作成しました。

- vol1 に対するデフォルトのツリークォータ制限は 400MB
- vol1 に対して 100MB のデフォルトユーザクォータ制限
- ユーザ jsmith のために vol1 に対して 200MB の明示的ユーザクォータ制限
- qtree q1 に対する 50MB のデフォルトユーザクォータ制限
- ユーザ jsmith のために qtree q1 に対して 75MB の明示的ユーザクォータ制限

これらのクォータのクォータルールは次のようになります。

```
cluster1::> volume quota policy rule show -vserver vs1 -volume vol1
```

Vserver: vs1			Policy: default		Volume: vol1		
Type	Target	Qtree	User Mapping	Disk Limit	Soft Disk Limit	Files Limit	Soft Files Limit
Threshold							
tree	""	""	-	400MB	-	-	-
user	""	""	off	100MB	-	-	-
user	""	q1	off	50MB	-	-	-
user	jsmith	""	off	200MB	-	-	-
user	jsmith	q1	off	75MB	-	-	-

次に、これらのクォータのクォータレポートの例を示します。

```
cluster1::> volume quota report
```

Vserver: vs1				----Disk----		----Files-----		Quota
Volume	Tree	Type	ID	Used	Limit	Used	Limit	
Specifier								
vol1	-	tree	*	0B	400MB	0	-	*
vol1	-	user	*	0B	100MB	0	-	*
vol1	-	user	jsmith	2000B	200MB	7	-	jsmith
vol1	q1	user	*	0B	50MB	0	-	*
vol1	q1	user	jsmith	0B	75MB	5	-	jsmith
vol1	q1	tree	1	0B	400MB	6	-	q1
vol1	-	user	root	0B	0MB	2	-	
vol1	q1	user	root	0B	0MB	1	-	

クォータレポートの最初の 5 行には、管理者が作成した 5 つのクォータが表示されます。これらのクォータのいくつかはデフォルトクォータであるため、ONTAP は自動的に派生クォータを作成します。

6 行目には、vol1 のすべての qtree（この例では q1 のみ）のデフォルトツリークォータから派生するツリークォータが表示されます。

最後の 2 行には、そのボリュームおよび qtree のデフォルトユーザクォータから派生するユーザクォータが表示されます。root ユーザがボリュームと qtree の両方でファイルを所有しているため、ボリュームと qtree の両方の root ユーザに派生ユーザクォータが作成されました。クォータに関して root ユーザは特別な扱いを受けるため、root ユーザの派生クォータは追跡クォータのみです。

次の理由から、ほかのデフォルトクォータや派生クォータは作成されませんでした。

- ユーザ jsmith は、このボリュームと qtree の両方にファイルを所有していますが、両方のレベルですでに明示的クォータが存在するため、このユーザに派生ユーザクォータは作成されませんでした。
- 他のユーザがボリュームまたは qtree のどちらかにファイルを所有していないため、他のユーザに派生ユーザクォータは作成されませんでした。
- qtree にはすでにデフォルトユーザクォータが存在するため、このボリュームのデフォルトユーザクォータによって qtree にデフォルトユーザクォータが作成されることはありませんでした。

適用クォータが設定されたクォータとは異なる理由

適用クォータは、設定されたクォータとは異なります。派生クォータが設定されることなく適用されるのに対し、設定されたクォータは正常に初期化されたあとにのみ適用されるためです。これらの違いを理解すると、クォータレポートに表示される適用クォータを、設定したクォータと比較しやすくなります。

クォータレポートに示される適用クォータは、次の理由から、設定されたクォータルールとは異なる場合があります。

- 派生クォータはクォータルールとして設定されることなく適用されるため、ONTAP ではデフォルトクォータに対応して自動的に派生クォータが作成されます。
- あるボリュームで、クォータルールが設定されたあとにクォータが再初期化されていない可能性があるため。
- ボリュームでクォータが初期化されたときにエラーが発生した可能性がある。

クォータレポートを使用して、特定のファイルへの書き込みを制限しているクォータを確認します

特定のファイルパスを指定して volume quota report コマンドを実行し、どのクォータ制限がファイルへの書き込み処理に影響しているかを特定できます。これは、どのクォータが書き込み処理を妨げているかを把握するのに役立ちます。

ステップ

1. path パラメータを指定して volume quota report コマンドを実行します。

特定のファイルに影響しているクォータを表示する例

次の例は、FlexVol ボリューム vol2 の qtree q1 にあるファイル file1 への書き込みに対して有効なクォータを確認するコマンドと出力を示しています。

```
cluster1:> volume quota report -vserver vs0 -volume vol2 -path
/vol/vol2/q1/file1
Virtual Server: vs0
```

Volume Specifier	Tree	Type	ID	----Disk----		----Files-----		Quota
				Used	Limit	Used	Limit	
vol2	q1	tree	jsmith	1MB	100MB	2	10000	q1
vol2	q1	group	eng	1MB	700MB	2	70000	
vol2		group	eng	1MB	700MB	6	70000	*
vol2		user	corp\jsmith	1MB	50MB	1	-	*
vol2	q1	user	corp\jsmith	1MB	50MB	1	-	

5 entries were displayed.

クォータに関する情報を表示するためのコマンド

コマンドを使用して、適用クォータとリソース使用量が含まれるクォータレポート、クォータの状態とエラーに関する情報、またはクォータポリシーとクォータルールに関する情報を表示できます。



次のコマンドは、FlexVol ボリュームに対してのみ実行できます。

状況	使用するコマンド
適用クォータに関する情報を表示します	<code>volume quota report</code>
クォータターゲットのリソース使用量（ディスクスペースとファイル数）を表示します	<code>volume quota report</code>
ファイルへの書き込みが許可された場合にどのクォータ制限に影響するかを確認します	<code>volume quota report</code> を使用 <code>-path</code> パラメータ
クォータの状態（など）を表示します <code>on</code> 、 <code>off</code> および <code>`initializing</code>	<code>volume quota show</code>
クォータのメッセージロギングに関する情報を表示します	<code>volume quota show</code> を使用 <code>-logmsg</code> パラメータ
クォータの初期化とサイズ変更中に発生するエラーを表示する	<code>volume quota show</code> を使用 <code>-instance</code> パラメータ

状況	使用するコマンド
クォータポリシーに関する情報を表示します	<code>volume quota policy show</code>
クォータルールに関する情報を表示します	<code>volume quota policy rule show</code>
Storage Virtual Machine（SVM、旧 Vserver）に割り当てられているクォータポリシーの名前を表示する	<code>vserver show</code> を使用 <code>-instance</code> パラメータ

詳細については、各コマンドのマニュアルページを参照してください。

## volume quota policy rule show コマンドと volume quota report コマンドを使用する状況

どちらのコマンドでもクォータに関する情報は表示されますが、には表示されず `volume quota policy rule show` の実行中に、設定されたクォータルールをすばやく表示できます `volume quota report` コマンドを実行すると、より多くの時間とリソースが消費され、適用クォータとリソース使用量が表示されます。

。 `volume quota policy rule show` コマンドは、次の場合に役立ちます。

- アクティブ化する前にクォータルールの設定を確認してください

このコマンドは、クォータが初期化されているかサイズ変更されているかに関係なく、設定されているクォータルールをすべて表示します。

- システムリソースに影響を与えずにクォータルールを迅速に表示します

ディスクとファイルの使用量は表示されないため、このコマンドはクォータレポートほどリソースを消費しません。

- SVM に割り当てられていないクォータポリシー内のクォータルールを表示する

。 `volume quota report` コマンドは、次の場合に役立ちます。

- 派生クォータも含め、適用クォータを表示する
- 派生クォータの影響を受けるターゲットも含め、有効になっているすべてのクォータによって使用されているディスクスペースとファイル数を表示する

（デフォルトクォータの場合、生成される派生クォータに照らして使用状況が追跡されるため、使用量は「0」と表示されます。）

- ファイルへの書き込みが許可される状況にどのクォータ制限が影響するかを確認します

を追加します `-path` パラメータをに設定します `volume quota report` コマンドを実行します



クォータレポートの生成には大量のリソースを消費します。クラスタ内の多数の FlexVol ボリュームに対してこの操作を実行すると、完了までに時間がかかることがあります。SVM 内の個々のボリュームのクォータレポートを表示する方が効率的です。

クォータレポートと **UNIX** クライアントで表示されるスペース使用量の相違

クォータレポートと **UNIX** クライアントの概要に表示されるスペース使用量の相違

FlexVol または qtree のクォータレポートに表示される使用済みディスクスペースの値が、UNIX クライアントに表示される同じボリュームまたは qtree の使用済みスペースの値と異なる場合があります。使用量の値が異なる理由は、クォータレポートと UNIX コマンドがそれぞれ異なる方法でボリュームまたは qtree 内のデータブロックを計算するためです。

たとえば、空のデータブロック（データが書き込まれていないブロック）のあるファイルがボリュームに含まれている場合、ボリュームのクォータレポートでは、スペース使用量のレポート作成時に空のデータブロックはカウントされません。ただし、ボリュームがUNIXクライアントにマウントされている場合は、ファイルが出力として表示されます。ls コマンドを実行すると、空のデータブロックもスペース使用量に含まれます。したがって、ls コマンドを実行すると、クォータレポートに表示されるスペース使用量よりも大きなファイルサイズが表示されます。

同様に、クォータレポートに表示されるスペース使用量の値は、などのUNIXコマンドの結果として表示される値と異なる場合があります。df および du。

クォータレポートのディスクスペースとファイル使用量の表示

FlexVol または qtree のクォータレポートに指定される使用済みファイル数とディスクスペース容量は、ボリュームまたは qtree 内のすべての inode に対応する使用済みデータブロックの数によって決まります。

ブロック数には、通常のファイルとストリームファイルで使用される直接ブロックと間接ブロックの両方が含まれます。ディレクトリ、アクセス制御リスト（ACL）、ストリームディレクトリ、およびメタファイルによって使用されるブロックは、クォータレポートの使用済みブロック数には含まれません。UNIX のスパーファイルの場合、空のデータブロックはクォータレポートに含まれません。

クォータサブシステムは、ユーザが制御可能なファイルシステムの要素だけを考慮し、含めるように設計されています。ディレクトリ、ACL、およびSnapshotスペースは、いずれもクォータ計算から除外されるスペースの例です。クォータは、保証ではなく制限の適用に使用され、アクティブなファイルシステム上でのみ動作します。クォータ計算では、特定のファイルシステム構成はカウントされず、ストレージ効率（圧縮や重複排除など）も考慮されません。

ls コマンドによるスペース使用量の表示

を使用する場合 ls コマンドを使用して、UNIXクライアントにマウントされたFlexVol ボリュームの内容を表示する場合、出力に表示されるファイルサイズは、ファイルのデータブロックのタイプに応じて、そのボリュームのクォータレポートに表示されるスペース使用量よりも増減することがあります。

の出力 ls コマンドを実行すると、ファイルのサイズのみが表示され、ファイルで使用される間接ブロックは表示されません。ファイルの空ブロックも、コマンドの出力に含まれます。



したがって、ファイルに空のブロックがない場合は、に表示されるサイズです `ls` クォータレポートには間接ブロックが含まれるため、コマンドのディスク使用量がクォータレポートで指定されたディスク使用量より少なくなることがあります。逆に、ファイルに空のブロックがある場合は、に表示されるサイズです `ls` コマンドは、クォータレポートで指定されたディスク使用量よりも多くなることがあります。

の出力 `ls` コマンドを実行すると、ファイルのサイズのみが表示され、ファイルで使用される間接ブロックは表示されません。ファイルの空ブロックも、コマンドの出力に含まれます。

**ls**コマンドとクォータレポートにおけるスペース使用量の違いの例

次のクォータレポートには、`qtree q1` の制限が 10MB であると表示されています。

Volume	Tree	Type	ID	----Disk----		----Files-----		Quota
				Used	Limit	Used	Limit	
Specifier								
-----	-----	-----	-----	-----	-----	-----	-----	
-----								
vol1	q1	tree	user1	10MB	10MB	1	-	q1
...								

UNIXクライアントからを使用して表示した場合、同じ`qtree`内のファイルのサイズがクォータ制限を超えることがあります `ls` 次の例に示すように、コマンドを実行します。

```
[user1@lin-sys1 q1]$ ls -lh
-rwxr-xr-x  1 user1 nfsuser  **27M** Apr 09  2013 file1
```

**df** コマンドによるファイルサイズの表示

での方法 `df` コマンドでは、スペース使用量は、`qtree`を含むボリュームでクォータが有効になっているか無効になっているか、`qtree`内のクォータ使用量が追跡されているかという2つの条件によって報告されます。

`qtree`を含むボリュームでクォータが有効になっている場合、および`qtree`内のクォータ使用量が追跡されると、によって報告されるスペース使用量が追跡されます `df` コマンドは、クォータレポートで指定された値に等しくなります。この場合、クォータ使用量では、ディレクトリ、ACL、ストリームディレクトリ、およびメタファイルによって使用されるブロックが除外されます。

ボリュームでクォータが無効になっている場合、または `qtree` にクォータルールが設定されていない場合、報告されるスペース使用量には、ボリューム内の他の `qtree` を含むボリューム全体のディレクトリ、ACL、ストリームディレクトリ、およびメタファイルによって使用されるブロックが含まれます。この場合、によって報告されるスペース使用量 `df` コマンドがクォータを追跡するときに報告される想定値を超えています。

を実行すると `df` コマンドを実行すると、クォータ使用量が追跡される`qtree`のマウントポイントから、クォータレポートの値と同じスペース使用量が表示されます。ほとんどの場合、ツリークォータルールにディスクのハードリミットが設定されている場合、によって報告される合計サイズ `df` コマンドはディスク制限に等しく、使用可能なスペースはクォータのディスク制限とクォータ使用量の差に等しくなります。

ただし、で報告される使用可能なスペースが表示される場合もあります df コマンドは、ボリューム全体で使用可能なスペースと同じになる場合があります。この状況は、 qtree にハードディスク制限が設定されていない場合に発生することがあります。ONTAP 9.9.1以降では、ボリューム全体で使用可能なスペースが残りのツリークォータスペースよりも少ない場合にも発生することがあります。これらのいずれかの状況が発生した場合、によって報告される合計サイズ df コマンドは、qtree内で使用されているクォータにFlexVol ボリュームで使用可能なスペースを加えたものです。



合計サイズは、 qtree ディスクの制限サイズでもボリュームの設定サイズでもありません。また、他の qtree 内の書き込みアクティビティや、バックグラウンドのストレージ効率化アクティビティによっても異なります。

で使用されているスペース使用量の例 df コマンドとクォータレポート

次のクォータレポートには、 qtree Alice の場合はディスク制限が 1 GB 、 qtree bob の場合は 2 GB 、 qtree Project1 の場合は制限がないことが示されています。

```
C1_vsim1:> quota report -vserver vs0
Vserver: vs0
```

Volume	Tree	Type	ID	Used	Limit	Used	Limit	Quota
vol2	alice	tree	1	502.0MB	1GB	2	-	alice
vol2	bob	tree	2	1003MB	2GB	2	-	bob
vol2	project1	tree	3	200.8MB	-	2	-	
project1	vol2	tree	*	0B	-	0	-	*

4 entries were displayed.

次の例は、の出力です df qtreeに対するコマンドAliceとBobは、クォータレポートと同じ使用済みスペース、およびディスク制限と同じ合計サイズ（1Mブロック単位）を報告します。これは、 alice と bob の qtree のクォータルールにディスク制限が定義されており、ボリュームの使用可能スペース（ 1211MB ）が qtree alice （ 523MB ）と qtree bob （ 1045MB ）のツリークォータスペースよりも大きいためです。

```
linux-client1 [~]$ df -m /mnt/vol2/alice
Filesystem      1M-blocks  Used Available Use% Mounted on
172.21.76.153:/vol2      1024    502      523   50% /mnt/vol2

linux-client1 [~]$ df -m /mnt/vol2/bob
Filesystem      1M-blocks  Used Available Use% Mounted on
172.21.76.153:/vol2      2048   1004     1045   50% /mnt/vol2
```

次の例は、の出力です df qtree Project1に対するコマンドでは、クォータレポートと同じ使用済みスペースが

報告されますが、合計サイズは、ボリューム全体の使用可能スペース（1211MB）をqtree Project1（201MB）のクォータ使用量に加算して合計1412MBになります。これは、qtree Project1 のクォータルールにディスクの制限がないためです。

```
linux-client1 [~]$ df -m /mnt/vol2/project1
Filesystem          1M-blocks  Used Available Use% Mounted on
172.21.76.153:/vol2    1412    201     1211  15% /mnt/vol2
```

次に、の出力例を示します df ボリューム全体に対してコマンドを実行すると、Project1と同じ使用可能スペースが報告されます。



```
linux-client1 [~]$ df -m /mnt/vol2
Filesystem          1M-blocks  Used Available Use% Mounted on
172.21.76.153:/vol2    2919  1709     1211  59% /mnt/vol2
```

## du コマンドによるスペース使用量の表示

を実行すると du UNIXクライアントにマウントされたqtreeまたはFlexVol ボリュームのディスクスペース使用量を確認するコマンドでは、使用量の値は、qtreeまたはボリュームのクォータレポートに表示される値よりも大きくなる場合があります。

の出力 du コマンドには、コマンドが発行されたディレクトリレベルから始まるディレクトリツリー内のすべてのファイルの合計スペース使用量が含まれます。これは、によって表示される使用量の値です du コマンドにはディレクトリのデータブロックも含まれ、クォータレポートに表示される値よりも大きくなります。

### duコマンドとクォータレポートにおけるスペース使用量の違いの例

次のクォータレポートには、qtree q1 の制限が 10MB であると表示されています。

Volume Specifier	Tree	Type	ID	----Disk----		----Files-----		Quota
				Used	Limit	Used	Limit	
-----	-----	-----	-----	-----	-----	-----	-----	
-----								
vol1	q1	tree	user1	10MB	10MB	1	-	q1
...								

次の例では、の出力としてのディスクスペース使用量を示しています du クォータ制限を超える大きい値が表示されます。

```
[user1@lin-sys1 q1]$ du -sh
**11M**      q1
```

これらの例は、クォータを設定する方法とクォータレポートを確認する方法を理解するのに役立ちます。

次の例は、vol1 というボリューム 1 つで構成された vs1 という SVM を含むストレージシステムを想定しています。クォータのセットアップを開始するにあたり、次のコマンドを実行してこの SVM の新しいクォータポリシーを作成します。

```
cluster1::>volume quota policy create -vserver vs1 -policy-name  
quota_policy_vs1_1
```

このクォータポリシーは新規であるため、SVM に割り当てます。

```
cluster1::>vserver modify -vserver vs1 -quota-policy quota_policy_vs1_1
```

#### 例1：デフォルトユーザクォータ

vol1 では、各ユーザに 50MB のハードリミットを適用します。

```
cluster1::>volume quota policy rule create -vserver vs1 -policy-name  
quota_policy_vs1_1 -volume vol1 -type user -target "" -disk-limit 50MB  
-qtree ""
```

新しいルールをアクティブ化するには、ボリュームでクォータを初期化します。

```
cluster1::>volume quota on -vserver vs1 -volume vol1 -foreground
```

クォータレポートを表示するには、次のコマンドを入力します。

```
cluster1::>volume quota report
```

次のようなクォータレポートが表示されます。

Vserver: vs1

Volume Specifier	Tree	Type	ID	----Disk----		----Files-----		Quota
				Used	Limit	Used	Limit	
-----	-----	-----	-----	-----	-----	-----	-----	
-----								
vol1		user	*	0B	50MB	0	-	*
vol1		user	jsmith	49MB	50MB	37	-	*
vol1		user	root	0B	-	1	-	

1 行目には、ディスクリミットを含めて作成したデフォルトユーザクォータが表示されます。すべてのデフォルトクォータと同様に、このデフォルトユーザクォータにはディスクまたはファイルの使用量に関する情報は表示されません。作成されたクォータに加えて、vol1 上のファイルを現在所有しているユーザごとに、2 つの他のクォータが表示されます。これらの追加クォータは、デフォルトユーザクォータから自動的に派生するユーザクォータです。ユーザ jsmith の派生ユーザクォータのディスク制限は、デフォルトユーザクォータと同じく 50MB です。root ユーザの派生ユーザクォータは、追跡クォータ（制限なし）です。

root ユーザ以外のシステム上のユーザが vol1 で 50MB を超える容量を使用する操作（エディタからのファイル書き込みなど）の実行を試みると、その操作は失敗します。

## 例2：デフォルトユーザクォータを無効にする明示的ユーザクォータ

ユーザ jsmith がボリューム vol1 で使用できるスペースを増やす必要がある場合は、次のコマンドを入力します。

```
cluster1::>volume quota policy rule create -vserver vs1 -policy-name  
quota_policy_vs1_1 -volume vol1 -type user -target jsmith -disk-limit 80MB  
-qtree ""
```

ユーザがクォータールのターゲットとして明示的に示されるため、これは明示的ユーザクォータになります。

これは、このボリュームにおけるユーザ jsmith の派生ユーザクォータのディスク制限を変更するため、既存のクォータ制限に対する変更になります。したがって、変更をアクティブ化するためにボリュームのクォータを再初期化する必要はありません。

クォータのサイズを変更するには：

```
cluster1::>volume quota resize -vserver vs1 -volume vol1 -foreground
```

サイズを変更する間、クォータは有効なままです。サイズ変更プロセスは短時間で完了します。

次のようなクォータレポートが表示されます。

```
cluster1::> volume quota report
Vserver: vs1
```

Volume	Tree	Type	ID	----Disk----		----Files-----		Quota
				Used	Limit	Used	Limit	
Specifier								
-----	-----	-----	-----	-----	-----	-----	-----	
vol1		user	*	0B	50MB	0	-	*
vol1		user	jsmith	50MB	80MB	37	-	jsmith
vol1		user	root	0B	-	1	-	

3 entries were displayed.

2 行目にはディスク制限 80MB とクォータ指定子 jsmith が示されています。

このため、jsmith は最大 80MB のスペースを vol1 で使用できます。これは、他のすべてのユーザが 50MB に制限されている場合でも同様です。

### 例3：しきい値

ここでは、ユーザが 5MB のディスク制限に達するという時点で通知を受け取ることを想定します。すべてのユーザに 45MB のしきい値を作成し、jsmith に 75MB のしきい値を作成するには、既存のクォータルールを変更します。

```
cluster1::>volume quota policy rule modify -vserver vs1 -policy
quota_policy_vs1_1 -volume vol1 -type user -target "" -qtree "" -threshold
45MB
cluster1::>volume quota policy rule modify -vserver vs1 -policy
quota_policy_vs1_1 -volume vol1 -type user -target jsmith -qtree ""
-threshold 75MB
```

既存のルールのサイズが変更されるため、変更をアクティブ化するためにボリュームのクォータのサイズを変更します。サイズ変更プロセスが完了するまで待ちます。

クォータレポートとしきい値を表示するには、を追加します -thresholds パラメータをに設定します  
volume quota report コマンドを実行します

```
cluster1:>>volume quota report -thresholds
Vserver: vs1
```

Volume	Tree	Type	ID	----Disk----		----Files-----		Quota
				Used	Limit (Thold)	Used	Limit	
Specifier								
-----	-----	-----	-----	-----	-----	-----	-----	
-----								
vol1		user	*	0B	50MB (45MB)	0	-	*
vol1		user	jsmith	59MB	80MB (75MB)	55	-	jsmith
vol1		user	root	0B	- ( -)	1	-	

3 entries were displayed.

しきい値は、Disk Limit 列にかっこ内に表示されます。

#### 例4：qtreeのクォータ

2つのプロジェクトのために、いくつかのスペースを分割する必要があるとします。proj1 と proj2 という名前の2つのqtreeを作成して、これらのプロジェクトをvol1内に含めることができます。

現在、ユーザはそのボリューム全体で割り当てられているスペースと同じスペースをqtreeで使用できます（ただし、ルートまたは別のqtreeでのスペースの使用によってボリュームの制限値を超えていない場合）。さらに、1つのqtreeで、ボリュームの全容量を使用することもできます。どちらのqtreeも20GBを超えることがないようにするには、そのボリュームにデフォルトのツリークォータを作成します。

```
cluster1:>>volume quota policy rule create -vserver vs1 -policy-name
quota_policy_vs1_1 -volume vol1 -type tree -target "" -disk-limit 20GB
```

正しいタイプは、qtreeではなく、**TREE**です。

これは新しいクォータであるため、サイズ変更によってアクティブ化することはできません。ボリュームのクォータを再初期化します。

```
cluster1:>>volume quota off -vserver vs1 -volume vol1
cluster1:>>volume quota on -vserver vs1 -volume vol1 -foreground
```



影響を受ける各ボリュームのクォータは、の実行直後にアクティブ化されるため、5分ほど待つから再アクティブ化する必要があります volume quota off コマンドでエラーが発生する可能性があります。また、コマンドを実行して、特定のボリュームを含むノードからボリュームのクォータを再初期化することもできます。

クォータの再初期化プロセスでは強制的にクォータが適用されないため、サイズ変更プロセスよりも時間がかかります。

クォータレポートを表示すると、新しい行がいくつか追加されます。一部の行はツリークォータについてのものです、一部の行は派生ユーザクォータについてのものです。

以下の新しい行は、ツリークォータについてのものです。

Volume Specifier	Tree	Type	ID	----Disk----		----Files-----		Quota
				Used	Limit	Used	Limit	
-----	-----	-----	-----	-----	-----	-----	-----	
-----								
...								
vol1		tree	*	0B	20GB	0	-	*
vol1	proj1	tree	1	0B	20GB	1	-	proj1
vol1	proj2	tree	2	0B	20GB	1	-	proj2
...								

作成したデフォルトのツリークォータが最初の新しい行に表示されます。この行の ID 列にはアスタリスク（\*）が付きます。ボリュームのデフォルトツリークォータに対応して、ONTAP ではボリューム内の qtree ごとに派生ツリークォータを自動的に作成します。これらは、proj1 と proj2 が Tree 列に表示される行に示されます。

以下の新しい行には、派生ユーザクォータについての情報が表示されます。

Volume Specifier	Tree	Type	ID	----Disk----		----Files-----		Quota
				Used	Limit	Used	Limit	
-----	-----	-----	-----	-----	-----	-----	-----	
-----								
...								
vol1	proj1	user	*	0B	50MB	0	-	
vol1	proj1	user	root	0B	-	1	-	
vol1	proj2	user	*	0B	50MB	0	-	
vol1	proj2	user	root	0B	-	1	-	
...								

ボリュームのデフォルトユーザクォータは、qtree に対してクォータが有効になっている場合、そのボリュームに含まれるすべての qtree に自動的に継承されます。最初の qtree クォータを追加したときに、qtree のクォータを有効にしました。このため、qtree ごとに派生デフォルトユーザクォータが作成されました。これらは、ID がアスタリスク（\*）である行に示されています。

root ユーザはファイルの所有者であるため、qtree ごとにデフォルトユーザクォータが作成されたときに、各 qtree の root ユーザに対して特別な追跡クォータも作成されました。これらは、ID が root である行に示されています。

例5：qtreeのユーザクォータ

ユーザが proj1 qtree で使用できるスペースが、ボリューム全体で使用できるスペースよりも小さくなるように設定します。proj1 qtree ではユーザが使用できるスペースを 10MB に制限します。したがって、qtree のデ



フォルトユーザクォータを作成します。

```
cluster1::>volume quota policy rule create -vserver vs1 -policy-name
quota_policy_vs1_1 -volume vol1 -type user -target "" -disk-limit 10MB
-qtrees proj1
```

これは、このボリュームのデフォルトユーザクォータから派生した proj1 qtrees のデフォルトユーザクォータを変更するため、既存のクォータに対する変更になります。したがって、クォータのサイズを変更して変更をアクティブ化します。サイズ変更プロセスが完了したら、クォータレポートを表示できます。

qtrees の新しい明示的ユーザクォータが示された、次の新しい行がクォータレポートに表示されます。

Volume Specifier	Tree	Type	ID	----Disk----		----Files-----		Quota
				Used	Limit	Used	Limit	
-----	-----	-----	-----	-----	-----	-----	-----	
-----								
vol1	proj1	user	*	0B	10MB	0	-	*

しかし、デフォルトユーザクォータを上書きする（ユーザ jsmith のスペースを増やす）ために作成したクォータがボリューム上にあったため、jsmith は proj1 qtrees にデータをこれ以上書き込むことができなくなっています。proj1 qtrees にデフォルトユーザクォータを追加したため、そのクォータが適用され、その qtrees で jsmith を含むすべてのユーザのスペースを制限しています。ユーザ jsmith が使用できるスペースを増やすには、ディスク制限を 80MB にする qtrees の明示的ユーザクォータルールを追加して、qtrees のデフォルトユーザクォータルールを無効にします。

```
cluster1::>volume quota policy rule create -vserver vs1 -policy-name
quota_policy_vs1_1 -volume vol1 -type user -target jsmith -disk-limit 80MB
-qtrees proj1
```

これは、デフォルトクォータがすでに存在する明示的クォータであるため、クォータのサイズを変更することで変更をアクティブ化できます。サイズ変更プロセスが完了したら、クォータレポートを表示します。

クォータレポートに次の新しい行が表示されます。

Volume Specifier	Tree	Type	ID	----Disk----		----Files-----		Quota
				Used	Limit	Used	Limit	
-----	-----	-----	-----	-----	-----	-----	-----	
-----								
vol1	proj1	user	jsmith	61MB	80MB	57	-	jsmith

最終的に次のようなクォータレポートが表示されます。

```
cluster1::>volume quota report
Vserver: vs1
```

Volume Specifier	Tree	Type	ID	----Disk----		----Files-----		Quota
				Used	Limit	Used	Limit	
vol1		tree	*	0B	20GB	0	-	*
vol1		user	*	0B	50MB	0	-	*
vol1		user	jsmith	70MB	80MB	65	-	jsmith
vol1	proj1	tree	1	0B	20GB	1	-	proj1
vol1	proj1	user	*	0B	10MB	0	-	*
vol1	proj1	user	root	0B	-	1	-	
vol1	proj2	tree	2	0B	20GB	1	-	proj2
vol1	proj2	user	*	0B	50MB	0	-	
vol1	proj2	user	root	0B	-	1	-	
vol1		user	root	0B	-	3	-	
vol1	proj1	user	jsmith	61MB	80MB	57	-	jsmith

11 entries were displayed.

proj1 内のファイルに書き込むためには、ユーザ jsmith は次のクォータ制限を満たす必要があります。

1. proj1 qtree のツリークォータ
2. proj1 qtree のユーザクォータ
3. ボリュームのユーザクォータ。

## SVM でクォータを設定します

新しい Storage Virtual Machine（SVM、旧 Vserver）でクォータを設定するには、クォータポリシーを作成してクォータポリシールールをポリシーに追加し、そのポリシーを SVM に割り当て、SVM 上の各 FlexVol でクォータを初期化する必要があります。

### 手順

1. 入力するコマンド `vserver show -instance` をクリックして、SVMの作成時に自動的に作成されたデフォルトのクォータポリシーの名前を表示します。

SVM の作成時に名前が指定されなかった場合、名前は「default」です。を使用できます `vserver quota policy rename` デフォルトポリシーに名前を付けるコマンド。



を使用して新しいポリシーを作成することもできます `volume quota policy create` コマンドを実行します

2. を使用します `volume quota policy rule create` SVM上の各ボリュームに次のクォータルールを作成するコマンド：

- すべてのユーザに対するデフォルトのクォータルール

- 特定のユーザに対する明示的クォータルール
  - すべてのグループに対するデフォルトのクォータルール
  - 特定のグループに対する明示的クォータルール
  - すべての qtree に対するデフォルトのクォータルール
  - 特定の qtree に対する明示的クォータルール
3. を使用します `volume quota policy rule show` コマンドを使用して、クォータルールが正しく設定されていることを確認します。
  4. 新しいポリシーを作成する場合は、を使用します `vserver modify` コマンドを使用して新しいポリシーをSVMに割り当てます。
  5. を使用します `volume quota on` SVM上の各ボリュームでクォータを初期化するコマンド。

初期化プロセスは、次の方法で監視できます。

- を使用する場合 `volume quota on` コマンドを使用すると、を追加できます `-foreground` フォアグラウンドのジョブでクォータを実行するためのパラメータ。（デフォルトでは、このジョブはバックグラウンドで実行されます）。

バックグラウンドでジョブが実行されると、を使用して進捗状況を監視できます `job show` コマンドを実行します

- を使用できます `volume quota show` クォータの初期化のステータスを監視するコマンド。
6. を使用します `volume quota show -instance` 初期化に失敗したクォータルールなど、初期化エラーがないかどうかを確認するコマンド。
  7. を使用します `volume quota report` クォータレポートを表示するコマンド。適用クォータが想定どおりであることを確認できます。

クォータ制限を変更（サイズ変更）します

既存のクォータのサイズを変更する場合、影響を受けるすべてのボリューム上のクォータのサイズを変更できます。この処理は、これらのボリューム上のクォータを再初期化するよりも高速です。

このタスクについて

クォータが適用されている Storage Virtual Machine（SVM、旧 Vserver）で、既存のクォータのサイズ制限を変更するか、すでに派生クォータが存在するターゲットに対してクォータを追加または削除します。

手順

1. を使用します `vserver show` コマンドにを指定します `-instance` SVMに現在割り当てられているポリシーの名前を確認するためのパラメータ。
2. 次のいずれかの操作を実行してクォータルールを変更します。
  - を使用します `volume quota policy rule modify` コマンドを使用して、既存のクォータルールのディスク制限またはファイル制限を変更します。
  - を使用します `volume quota policy rule create` コマンドを使用して、現在派生クォータが存在するターゲット（ユーザ、グループ、またはqtree）に対する明示的クォータルールを作成します。

。を使用します `volume quota policy rule delete` コマンドを使用して、デフォルトクォータを持つターゲット（ユーザ、グループ、またはqtree）に対する明示的クォータルールを削除します。

3. 使用します `volume quota policy rule show` コマンドを使用して、クォータルールが正しく設定されていることを確認します。
4. 使用します `volume quota resize` クォータを変更した各ボリュームでコマンドを実行し、各ボリュームで変更をアクティブ化します。

サイズ変更プロセスは、次のいずれかの方法で監視できます。

。を使用する場合 `volume quota resize` コマンドを使用すると、を追加できます `-foreground` フォアグラウンドでサイズ変更ジョブを実行するためのパラメータ。（デフォルトでは、このジョブはバックグラウンドで実行されます）。

バックグラウンドでジョブが実行されると、を使用して進捗状況を監視できます `job show` コマンドを実行します

。を使用できます `volume quota show` コマンドを使用してサイズ変更ステータスを監視します。

5. 使用します `volume quota show -instance` コマンドを使用して、サイズ変更失敗したクォータルールなどのサイズ変更エラーを確認します。

特に '派生クォータがまだ存在しないターゲットの明示的クォータを追加した後でクォータのサイズを変更すると発生する "new definition" エラーをチェックします

6. 使用します `volume quota report` クォータレポートを表示して、適用クォータが要件を満たしていることを確認するコマンド。

大幅な変更を行ったあとにクォータを再初期化する

クォータが適用されていないターゲットに対してクォータを追加または削除するなど、既存のクォータに大幅な変更を加える場合は、影響を受けるすべてのボリュームのクォータを変更して再初期化する必要があります。

このタスクについて

クォータが適用されている Storage Virtual Machine（SVM）に対し、クォータの完全な再初期化が必要となる変更を実行します。

手順

1. 使用します `vserver show` コマンドにを指定します `-instance SVM`に現在割り当てられているポリシーの名前を確認するためのパラメータ。
2. 次のいずれかの操作を実行してクォータルールを変更します。

状況	作業
新しいクォータルールを作成します	使用します <code>volume quota policy rule create</code> コマンドを実行します
既存のクォータルールの設定を変更します	使用します <code>volume quota policy rule modify</code> コマンドを実行します

状況	作業
既存のクォータルールを削除します	を使用します volume quota policy rule delete コマンドを実行します

3. を使用します volume quota policy rule show コマンドを使用して、クォータルールが正しく設定されていることを確認します。
4. クォータを変更した各ボリュームで、クォータをオフにしてからクォータをオンにして、クォータを再初期化します。
  - a. を使用します volume quota off 影響を受ける各ボリュームに対してコマンドを実行し、そのボリュームのクォータを非アクティブ化します。
  - b. を使用します volume quota on 影響を受ける各ボリュームに対してコマンドを実行し、そのボリュームでクォータをアクティブ化します。



影響を受ける各ボリュームのクォータは、の実行直後にアクティブ化されるため、5分ほど待ってから再アクティブ化する必要があります volume quota off コマンドでエラーが発生する可能性があります。

また、コマンドを実行して、特定のボリュームを含むノードからボリュームのクォータを再初期化することもできます。

初期化プロセスは、次のいずれかの方法で監視できます。

- を使用する場合 volume quota on コマンドを使用すると、を追加できます -foreground フォアグラウンドのジョブでクォータを実行するためのパラメータ。（デフォルトでは、このジョブはバックグラウンドで実行されます）。

バックグラウンドでジョブが実行されると、を使用して進捗状況を監視できます job show コマンドを実行します

- を使用できます volume quota show クォータの初期化のステータスを監視するコマンド。

5. を使用します volume quota show -instance 初期化に失敗したクォータルールなど、初期化エラーがないかどうかを確認するコマンド。
6. を使用します volume quota report クォータレポートを表示するコマンド。適用クォータが想定どおりであることを確認できます。

クォータルールとクォータポリシーを管理するためのコマンドです

を使用できます volume quota policy rule クォータルールを設定するコマンドを実行し、を使用します volume quota policy コマンドと一部 vservers クォータポリシーを設定するコマンド。



次のコマンドは、FlexVol ボリュームに対してのみ実行できます。

クォータルールを管理するためのコマンド

状況	使用するコマンド
新しいクォータルールを作成します	<code>volume quota policy rule create</code>
既存のクォータルールを削除します	<code>volume quota policy rule delete</code>
既存のクォータルールを変更します	<code>volume quota policy rule modify</code>
設定されているクォータルールに関する情報を表示します	<code>volume quota policy rule show</code>

クォータポリシーを管理するためのコマンド

状況	使用するコマンド
クォータポリシーとそのクォータポリシーに含まれるクォータルールを複製します	<code>volume quota policy copy</code>
新しい空のクォータポリシーを作成します	<code>volume quota policy create</code>
Storage Virtual Machine （SVM）に現在割り当てられていない既存のクォータポリシーを削除する	<code>volume quota policy delete</code>
クォータポリシーの名前を変更します	<code>volume quota policy rename</code>
クォータポリシーに関する情報を表示します	<code>volume quota policy show</code>
クォータポリシーをSVMに割り当てます	<code>vserver modify -quota-policy <i>policy_name</i></code>
SVMに割り当てられているクォータポリシーの名前を表示する	<code>vserver show</code>

を参照してください ["ONTAP コマンドリファレンス"](#) を参照してください。

クォータをアクティブ化および変更するためのコマンド

を使用できます `volume quota` クォータの状態を変更し、クォータのメッセージロギングを設定するコマンド。

状況	使用するコマンド
クォータをオンにする（ <code>_initialing_them</code> ）	<code>volume quota on</code>
既存のクォータのサイズを変更する	<code>volume quota resize</code>

状況	使用するコマンド
クォータをオフにします	<code>volume quota off</code>
クォータのメッセージロギングの変更、クォータのオンへの切り替え、クォータのオフへの切り替え、または既存のクォータのサイズ変更を行います	<code>volume quota modify</code>

詳細については、各コマンドのマニュアルページを参照してください。

重複排除、データ圧縮、データコンパクションを使用して、ストレージ効率を向上できます

重複排除、データ圧縮、データコンパクションを使用して、ストレージ効率の概要を向上させます

重複排除、データ圧縮、データコンパクションを一緒に、または個別に実行して、FlexVol で最適なスペース削減効果を得ることができます。重複排除は重複したデータブロックを排除し、データ圧縮はデータブロックを圧縮して必要な物理ストレージ量を減らします。データコンパクションを実行すると、少ないスペースに多くのデータを格納できるようになり、ストレージ効率が向上します。



ONTAP 9.2 以降では、インラインの Storage Efficiency 機能（インライン重複排除、インライン圧縮など）がすべて AFF でデフォルトで有効になります。

ボリュームで重複排除を有効にします

FlexVol で重複排除を有効にしてストレージ効率を向上させることができます。ポストプロセス重複排除はすべてのボリュームで、インライン重複排除は AFF または Flash Pool アグリゲート内のボリュームで有効にできます。

他のタイプのボリュームでインライン重複排除を有効にする場合は、技術情報アートを参照してください ["AFF以外の（オールフラッシュFAS）アグリゲートでボリュームのインライン重複排除を有効にする方法"](#)。

必要なもの

FlexVol ボリュームの場合、ボリュームおよびアグリゲート内に重複排除メタデータ用の十分な空きスペースがあることを確認しておく必要があります。重複排除メタデータ用に、アグリゲート内に最小限の空きスペースが必要です。アグリゲート内のすべての重複排除対象 FlexVol ボリュームまたはデータコンスティチュエントの総物理データ量の 3% に相当するスペースです。各 FlexVol またはデータ構成要素では総物理データ量の 4% に相当する空きスペースを確保する必要があるため、合計で 7% が必要になります。



ONTAP 9.2 以降では、AFF システムでインライン重複排除がデフォルトで有効になります。

選択肢

- 使用します `volume efficiency on` ポストプロセス重複排除を有効にするコマンド。

次のコマンドは、ボリューム VolA でポストプロセス重複排除を有効にします。

```
volume efficiency on -vserver vs1 -volume VolA
```

- を使用します volume efficiency on コマンドのあとにを入力します volume efficiency modify コマンドにを指定します -inline-deduplication オプションをに設定します true ポストプロセス重複排除とインライン重複排除の両方を有効にします。

次のコマンドは、ボリューム VolA でポストプロセス重複排除とインライン重複排除の両方を有効にします。

```
volume efficiency on -vserver vs1 -volume VolA
```

```
volume efficiency modify -vserver vs1 -volume VolA -inline-dedupe true
```

- を使用します volume efficiency on コマンドのあとにを入力します volume efficiency modify コマンドにを指定します -inline-deduplication オプションをに設定します true および -policy オプションをに設定します inline-only インライン重複排除のみを有効にする場合。

次のコマンドは、ボリューム VolA でインライン重複排除だけを有効にします。

```
volume efficiency on -vserver vs1 -volume VolA
```

```
volume efficiency modify -vserver vs1 -volume VolA -policy inline-only -inline  
-dedupe true
```

完了後

ボリューム効率化の設定を表示して、設定が変更されたことを確認します。

```
volume efficiency show -instance
```

ボリュームの重複排除を無効にします

ポストプロセス重複排除とインライン重複排除は、ボリュームで個別に無効にすることができます。

必要なもの

ボリューム上で現在アクティブになっているボリューム効率化処理を停止します。 volume efficiency stop

このタスクについて

ボリュームでデータ圧縮を有効にした場合は、を実行します volume efficiency off コマンドは、データ圧縮を無効にします。

選択肢

- を使用します volume efficiency off ポストプロセス重複排除とインライン重複排除の両方を無効にするコマンド。

次のコマンドは、ボリューム VolA でポストプロセス重複排除とインライン重複排除の両方を無効にします。

```
volume efficiency off -vserver vs1 -volume VolA
```



- を使用します `volume efficiency modify` コマンドにを指定します `-policy` オプションをに設定します `inline only` ポストプロセス重複排除を無効にし、インライン重複排除は有効なままにします。

次のコマンドは、ボリューム VolA でポストプロセス重複排除を無効にします。ただし、インライン重複排除は有効なままになります。

```
volume efficiency modify -vserver vs1 -volume VolA -policy inline-only
```

- を使用します `volume efficiency modify` コマンドにを指定します `-inline-deduplication` オプションをに設定します `false` インライン重複排除のみを無効にします。

次のコマンドは、ボリューム VolA でインライン重複排除だけを無効にします。

```
volume efficiency modify -vserver vs1 -volume VolA -inline-deduplication false
```

## AFF システムで、ボリュームレベルの自動バックグラウンド重複排除を管理します

ONTAP 9.3以降では、事前定義されたを使用してボリュームレベルのバックグラウンド重複排除が自動的に実行されるように管理できます `auto` AFF ポリシー：スケジュールを手動で設定する必要はありません。。 `auto` ポリシーは、バックグラウンドで継続的な重複排除を実行します。

。 `auto` 新しく作成したすべてのボリューム、およびアップグレードしたすべてのボリュームに対して、バックグラウンド重複排除の対象として手動で設定されていないボリュームに対してポリシーが設定されます。ポリシーはに変更できます `default` またはその他のポリシーを使用して機能を無効にします。

ボリュームがAFF以外のシステムからAFFシステムに移動した場合は `auto` デスティネーションノードでは、デフォルトでポリシーが有効になっています。ボリュームがAFF ノードからAFF以外のノードに移動した場合は、 `auto` デスティネーションノードのポリシーが置き換えられます `inline-only` デフォルトではポリシーです。

AFF では、を持つすべてのボリュームが監視されます `auto policy`と指定すると、削減量が少ないボリュームや頻繁に上書きされるボリュームの優先順位が解除されます。優先度が下がったボリュームは、自動バックグラウンド重複排除の対象ではなくなります。優先度が下がったボリュームの変更ロギングは無効になり、ボリューム上のメタデータは切り捨てられます。

ユーザは、を使用して、優先度が下がったボリュームを昇格し、自動バックグラウンド重複排除の対象に戻すことができます `volume efficiency promote advanced`権限レベルで使用できるコマンドです。

## AFF システムでアグリゲートレベルのインライン重複排除を管理します

アグリゲートレベルの重複排除は、同じアグリゲートに属するボリューム間で重複するブロックを排除します。ONTAP 9.2 以降の AFF システムでは、アグリゲートレベルの重複排除をインラインで実行できます。この機能は、新規に作成したすべてのボリューム、およびボリュームのインライン重複排除をオンにしてアップグレードしたすべてのボリュームに対してデフォルトで有効になります。

このタスクについて

重複排除処理は、データがディスクに書き込まれる前に重複するブロックを排除します。が含まれているボリ

ユーモのみ space guarantee をに設定します none アグリゲートレベルのインライン重複排除を実行できます。これは、AFF システムのデフォルト設定です。



アグリゲートレベルのインライン重複排除は、ボリューム間インライン重複排除とも呼ばれます。

## ステップ

1. AFF システムでアグリゲートレベルのインライン重複排除を管理します。

状況	使用するコマンド
アグリゲートレベルのインライン重複排除を有効にします	<code>volume efficiency modify -vserver vserver_name -volume vol_name -cross -volume-inline-dedupe true</code>
アグリゲートレベルのインライン重複排除を無効にします	<code>volume efficiency modify -vserver vserver_name -volume vol_name -cross -volume-inline-dedupe false</code>
アグリゲートレベルのインライン重複排除のステータスを表示します	<code>volume efficiency config -volume vol_name</code>

## 例

次のコマンドは、アグリゲートレベルのインライン重複排除のステータスを表示します。

```
wfit-8020-03-04::> volume efficiency config -volume choke0_wfit_8020_03_0
Vserver:                                vs0
Volume:                                choke0_wfit_8020_03_0
Schedule:                               -
Policy:                                choke_VE_policy
Compression:                            true
Inline Compression:                     true
Inline Dedupe:                          true
Data Compaction:                        true
Cross Volume Inline Deduplication:      false
```

## AFF システムでアグリゲートレベルのバックグラウンド重複排除を管理します

アグリゲートレベルの重複排除は、同じアグリゲートに属するボリューム間で重複するブロックを排除します。ONTAP 9.3 以降では、AFF システムでアグリゲートレベルの重複排除をバックグラウンドで実行できます。この機能は、新規に作成したすべてのボリューム、およびボリュームのバックグラウンド重複排除をオンにしてアップグレードしたすべてのボリュームに対してデフォルトで有効になります。

このタスクについて

この処理は、変更ログがある程度いっぱいになった時点で自動的にトリガーされます。スケジュールもポリシーも関連付けられません。

ONTAP 9.4 以降では、AFF ユーザがアグリゲートレベルの重複排除スキャンを実行して、アグリゲート内のボリューム間で既存データの重複を排除することもできます。を使用できます `storage aggregate efficiency cross-volume-dedupe start` コマンドにを指定します `-scan-old-data=true` スキャナを起動するオプション：

```
cluster-1::> storage aggregate efficiency cross-volume-dedupe start
-aggregate aggr1 -scan-old-data true
```

重複排除スキャンには時間がかかる場合があります。この処理はオフピークの時間帯に実行することを推奨します。



アグリゲートレベルのバックグラウンド重複排除は、ボリューム間バックグラウンド重複排除とも呼ばれます。

## ステップ

1. AFF システムでアグリゲートレベルのバックグラウンド重複排除を管理します。

状況	使用するコマンド
アグリゲートレベルのバックグラウンド重複排除を有効にする	<code>volume efficiency modify -vserver &lt;vserver_name&gt; -volume &lt;vol_name&gt; -cross-volume-background-dedupe true</code>
アグリゲートレベルのバックグラウンド重複排除を無効にします	<code>volume efficiency modify -vserver &lt;vserver_name&gt; -volume &lt;vol_name&gt; -cross-volume-background-dedupe false</code>
アグリゲートレベルのバックグラウンド重複排除のステータスを表示します	<code>aggregate efficiency cross-volume-dedupe show</code>

## 温度に敏感なストレージ効率の概要

ONTAP は、ボリュームのデータへのアクセス頻度を評価し、その頻度とデータに適用される圧縮レベルをマッピングすることで、温度に影響される Storage Efficiency のメトリックを提供します。アクセス頻度の低いコールドデータの場合は大容量のデータブロックが圧縮され、頻繁にアクセスされて上書きされるホットデータの場合は小さなデータブロックが圧縮されるため、プロセスが効率化されます。

温度識別型 Storage Efficiency (TSSE) は ONTAP 9.8 で導入された機能で、新しく作成したシンプロビジョニング AFF ボリュームでは自動的に有効になります。既存の AFF ボリュームとシンプロビジョニングされた AFF DP 以外のボリュームでは、温度に基づく Storage Efficiency を有効にすることができます。

「デフォルト」モードと「効率的」モードが導入されました

ONTAP 9.10.1以降では、AFF システムに対してのみ、ボリュームレベルの2つのStorage Efficiencyモード (`default_`と`_efficient`) が導入されました。この2つのモードでは、新しいAFFボリュームの作成時のデフォルトモードであるファイル圧縮（デフォルト）と、温度に基づくStorage Efficiency（効率的）のどちらかを選択できます。ONTAP 9.10.1では、["温度に基づくストレージ効率化は明示的に設定する必要があります"](#) 自動アダプティブ圧縮を有効にします。ただし、AFF プラットフォームでは、データコンパクション、自動重複排除スケジュール、インライン重複排除、ボリューム間インライン重複排除、ボリューム間バックグラウンド重複排除などの他のStorage Efficiency機能が、デフォルトモードと効率モードのどちらでもデフォルトで有効になります。

どちらのStorage Efficiencyモード（デフォルトと効率化）も、FabricPool対応アグリゲートでサポートされ、すべての階層化ポリシータイプでサポートされます。

#### Cシリーズプラットフォームで温度に基づく **Storage Efficiency** を有効にします

AFF Cシリーズプラットフォーム、および次のリリースがインストールされたデスティネーションでボリューム移動またはSnapMirrorを使用して、非TSSEプラットフォームからTSSE対応Cシリーズプラットフォームにボリュームを移行する場合、温度に基づくStorage Efficiencyがデフォルトで有効になります。

- ONTAP 9.12.1P4以降
- ONTAP 9.13.1以降

詳細については、を参照してください ["ボリューム移動処理とSnapMirror処理でのStorage Efficiencyの動作"](#)。

既存のボリュームでは、温度に基づくStorage Efficiencyは自動的に有効になりませんが、有効にすることはできます ["Storage Efficiencyモードを変更します"](#) 手動で効率モードに変更します。



Storage Efficiencyモードを効率化モードに変更したあとに元に戻すことはできません。

連続する物理ブロックをシーケンシャルにパッキングすることで、ストレージ効率が向上します

ONTAP 9.13.1以降では、温度に左右されるストレージ効率化機能によって、連続する物理ブロックのシーケンシャルパッキングが追加され、ストレージ効率がさらに向上します。システムをONTAP 9.13.1にアップグレードすると、温度の影響を受けやすいStorage Efficiencyが有効になっているボリュームでは、自動的にシーケンシャルパッキングが有効になります。シーケンシャルパッキングを有効にした後は、を実行する必要があります ["既存のデータを手動で再バックします"](#)。

#### アップグレード時の考慮事項

ONTAP 9.10.1以降にアップグレードする場合、既存のボリュームには、ボリュームで現在有効になっている圧縮のタイプに基づいてStorage Efficiencyモードが割り当てられます。アップグレードの実行時、圧縮が有効なボリュームにはデフォルトモードが割り当てられ、温度に影響されるストレージ効率化が有効になっているボリュームには効率的モードが割り当てられます。圧縮が有効になっていない場合、Storage Efficiency モードは空白のままです。

#### ボリューム移動処理と**SnapMirror**処理での**Storage Efficiency**の動作

ボリューム移動またはSnapMirror処理を実行したときのボリュームでのStorage Efficiencyの動作、およびSnapMirrorの解除を実行して温度に応じたStorage Efficiencyを手動で有効にした場合の動作は、ソースボリュームでの効率化の種類によって異なります。

次の表に、Storage Efficiencyタイプの異なるボリューム移動またはSnapMirror処理を実行した場合のソースボリュームとデスティネーションボリュームの動作、およびTemperature-Sensitive Storage Efficiency (TSSE)

を手動で有効にした場合の動作を示します。

ソースボリュームの効率化	デスティネーションボリュームのデフォルトの動作			手動でTSSEを有効にしたあとのデフォルトの動作（SnapMirrorの解除後）		
	* Storage Efficiency タイプ*	新規書き込み	コールドデータ圧縮	* Storage Efficiency タイプ*	新規書き込み	コールドデータ圧縮
Storage Efficiency 機能なし（FASと思われる）	ファイル圧縮	新しく書き込まれたデータに対して、ファイルの圧縮がインラインで試行されます	コールドデータ圧縮は行われず、データはそのまま残ります	コールドデータスキャンアルゴリズムをZSTDとして使用するTSSE	8Kのインライン圧縮がTSSE形式で試行されます	ファイル圧縮データ：N/A [] *非圧縮データ*：しきい値日数に達したあとに32Kの圧縮が試行されました [] 新規書き込まれたデータ：しきい値日数に達したあとに32Kの圧縮が試行されました
Storage Efficiency 機能なし（FASと思われる）	ONTAP 9.11.1P10 またはONTAP 9.12.1P3 を使用したCシリーズプラットフォームでのファイル圧縮	TSSE対応のコールドデータ圧縮機能はありません	ファイル圧縮データ：N/A	コールドデータスキャンアルゴリズムをZSTDとして使用するTSSE	8Kのインライン圧縮	ファイル圧縮データ：N/A [] *非圧縮データ*：しきい値日数に達したあとに32Kの圧縮が試行されました [] 新規書き込まれたデータ：しきい値日数に達したあとに32Kの圧縮が試行されました
Storage Efficiency 機能なし（FASと思われる）	ONTAP 9.12.1P4以降またはONTAP 9.13.1以降を使用するCシリーズプラットフォーム上のTSSE	8Kのインライン圧縮がTSSE形式で試行されます	ファイル圧縮データ：N/A [] *非圧縮データ*：しきい値日数に達したあとに32Kの圧縮が試行されました [] 新規書き込まれたデータ：しきい値日数に達したあとに32Kの圧縮が試行されました	コールドデータスキャンアルゴリズムをZSTDとして使用するTSSE	8Kのインライン圧縮がTSSE形式で試行されます	ファイル圧縮データ：N/A [] *非圧縮データ*：しきい値日数に達したあとに32Kの圧縮が試行されました [] 新規書き込まれたデータ：しきい値日数に達したあとに32Kの圧縮が試行されました
ファイル圧縮グループ	ソースと同じ	新しく書き込まれたデータに対して、ファイルの圧縮がインラインで試行されます	コールドデータ圧縮は行われず、データはそのまま残ります	コールドデータスキャンアルゴリズムをZSTDとして使用するTSSE	8Kのインライン圧縮がTSSE形式で試行されます	ファイル圧縮データ：圧縮されていません [] *非圧縮データ*：しきい値の日数に達したあとに32Kの圧縮が試行されます [] 新規に書き込まれたデータ：しきい値日数に達したあとに32Kの圧縮が試行されます

TSSEコールドデータスキャン	ソースボリュームと同じ圧縮アルゴリズムを使用するTSSE (LZOPro → LZOPro およびZSTD → ZSTD)	TSSE形式で8Kのインライン圧縮が試行されました	既存データと新しく書き込まれたデータの両方で、しきい値日数ベースの寒さが満たされた後、LzoProで32Kの圧縮が試行されます。	TSSEはイネーブルです。注：LZOProコールドデータスキャンアルゴリズムはZSTDに変更できます。	8Kのインライン圧縮がTSSE形式で試行されます	既存データと新規書き込まれたデータの両方が寒さをしきい値日数に達したあとに、32Kの圧縮が試行されます。
-----------------	---	---------------------------	--	---	--------------------------	--

ボリューム作成時に **Storage Efficiency** モードを設定します


ONTAP 9.10.1以降では、新しいAFFボリュームの作成時にStorage Efficiencyモードを設定できます。パラメータを使用 `-storage-efficiency-mode`` では、ボリュームで効率的モードとデフォルトのパフォーマンスモードのどちらを使用するかを指定できます。この2つのモードでは、ファイル圧縮（デフォルト）（新しいAFF が作成されたときのデフォルトモード）と、温度に基づくStorage Efficiency（効率的）のどちらかを選択できます。。 ``-storage-efficiency-mode` このパラメータは、AFF以外のボリュームまたはデータ保護ボリュームではサポートされません。

#### 手順

このタスクは、ONTAPシステムマネージャまたはONTAP CLIを使用して実行できます。

## System Manager の略

ONTAP 9.10.1 以降の System Manager では、温度に応じた Storage Efficiency 機能を使用してより高いストレージ効率を実現することができます。パフォーマンスベースの Storage Efficiency は、デフォルトで有効になっています。

1. [ストレージ]、[ボリューム]の順にクリックします。
2. Storage Efficiency を有効または無効にするボリュームを探し、をクリックします .
3. [編集]>[ボリューム]をクリックし、[Storage Efficiency]\*までスクロールします。
4. Enable Higher Storage Efficiency \* を選択します。

## CLI の使用

効率化モードを使用して新しいボリュームを作成します

新しいボリュームの作成時に温度に基づく Storage Efficiency モードを設定するには、を使用します  
-storage-efficiency-mode パラメータを指定します efficient。

1. 効率化モードを有効にして新しいボリュームを作成します。

```
volume create -vserver <vserver name> -volume <volume name> -aggregate  
<aggregate name> -size <volume size> -storage-efficiency-mode efficient
```

```
volume create -vserver vs1 -volume aff_vol1 -aggregate aff_aggr1  
-storage-efficiency-mode efficient -size 10g
```

パフォーマンスモードを使用して新しいボリュームを作成します

パフォーマンスモードは、Storage Efficiencyを使用して新しいAFFを作成するとデフォルトで設定されます。必須ではありませんが、オプションで 사용할 수 있습니다 default を使用した値 -storage-efficiency-mode パラメータは、新しいAFFボリュームを作成するときに使用します。

1. パフォーマンスStorage Efficiencyモード「default」を使用して新しいボリュームを作成します。

```
volume create -vserver <vserver name> -volume <volume name> -aggregate  
<aggregate name> -size <volume size> -storage-efficiency-mode default
```

```
volume create -vserver vs1 -volume aff_vol1 -aggregate aff_aggr1 -storage  
-efficiency-mode default -size 10g
```

ボリュームの非アクティブデータ圧縮しきい値を変更します

ONTAPがコールドデータスキャンを実行する頻度を変更するには、温度の影響を受けやすいStorage Efficiencyを使用してボリュームのコールドしきい値を変更します。

作業を開始する前に

クラスタ管理者またはSVM管理者であり、ONTAP CLIのadvanced権限レベルを使用する必要があります。

このタスクについて

寒さのしきい値は1〜60日です。デフォルトのしきい値は14日です。

手順

1. 権限レベルを設定します。

```
set -privilege advanced
```

2. ボリュームのアクセス頻度の低いデータ圧縮を変更します。

```
volume efficiency inactive-data-compression modify -vserver <vserver_name>  
-volume <volume_name> -threshold-days <integer>
```

詳細については、追加情報のマニュアルページを参照してください ["非アクティブデータ圧縮を変更しています"](#)。

ボリューム効率化モードを確認します

を使用できます `volume-efficiency-show` コマンドをAFF に対して実行し、効率化が設定されているかどうかを確認し、現在の効率化モードを表示します。

ステップ

1. ボリュームの効率化モードを確認します。

```
volume efficiency show -vserver <vserver name> -volume <volume name> -fields  
storage-efficiency-mode
```

ボリューム効率化モードを変更します

ONTAP 9.10.1以降では、AFF システムに対してのみ、ボリュームレベルの2つのStorage Efficiencyモード (`default` と `efficient`) が導入されました。この2つのモードでは、新しいAFFボリュームの作成時のデフォルトモードであるファイル圧縮（デフォルト）と、温度に基づくStorage Efficiency（効率的）のどちらかを選択できます。を使用できます `volume efficiency modify` コマンドを使用して、AFF ボリュームに設定されているStorage Efficiencyモードを変更します。モードはから変更できます `default` 終了: `efficient` また、ボリューム効率化がまだ設定されていない場合は、効率化モードを設定することもできます。

手順

1. ボリューム効率化モードを変更します。

```
volume efficiency modify -vserver <vserver name> -volume <volume name>  
-storage-efficiency-mode <default|efficient>
```



温度の影響を受けやすい**Storage Efficiency**の有無にかかわらず、ボリュームのフットプリント削減量を表示します

ONTAP 9.11.1以降では、を使用できます volume show-footprint コマンドを使用して、ボリュームの物理的なフットプリントによる削減量を表示します "[温度に基づく Storage Efficiency \(TSSE\) で有効](#)"。ONTAP 9.13.1以降では、同じコマンドを使用して、TSSEが有効になっていないボリュームでの物理的なフットプリントによる削減量を表示できます。

#### ステップ

1. ボリュームのフットプリントによる削減量を表示します。

```
volume show-footprint
```

#### TSSEがイネーブルの場合の出力例

```
Vserver : vs0
Volume  : vol_tsse_75_per_compress
```

Feature	Used	Used%
-----	-----	-----
Volume Data Footprint	10.15GB	13%
Volume Guarantee	0B	0%
Flexible Volume Metadata	64.25MB	0%
Delayed Frees	235.0MB	0%
File Operation Metadata	4KB	0%
 Total Footprint	 10.45GB	 13%
 Footprint Data Reduction	 6.85GB	 9%
Auto Adaptive Compression	6.85GB	9%
Effective Total Footprint	3.59GB	5%

## TSSEをイネーブルにしない場合の出力例

```
Vserver : vs0
Volume  : vol_file_cg_75_per_compress
```

Feature	Used	Used%
-----	-----	-----
Volume Data Footprint	5.19GB	7%
Volume Guarantee	0B	0%
Flexible Volume Metadata	32.12MB	0%
Delayed Frees	90.17MB	0%
File Operation Metadata	4KB	0%
 Total Footprint	 5.31GB	 7%
 Footprint Data Reduction	 1.05GB	 1%
Data Compaction	1.05GB	1%
Effective Total Footprint	4.26GB	5%

ボリュームでデータ圧縮を有効にします

を使用すると、FlexVol ボリュームでデータ圧縮を有効にしてスペースを削減できます  
volume efficiency modify コマンドを実行しますデフォルトの圧縮形式が適していない場合は、ボリュームに圧縮形式を割り当てることもできます。

必要なもの

ボリュームの重複排除を有効にしておく必要があります。



- 重複排除は有効にさえなっていれば、実行されている必要はありません。
- AFF プラットフォーム内のボリューム上の既存のデータは、圧縮スキャナを使用して圧縮する必要があります。

### "ボリュームの重複排除を有効にする"

このタスクについて

- HDD アグリゲートと Flash Pool アグリゲートのボリュームでは、インライン圧縮とポストプロセス圧縮の両方を有効にするか、ポストプロセス圧縮のみを有効にすることができます。

両方を有効にする場合は、ポストプロセス圧縮を有効にしてからインライン圧縮を有効にする必要があります。

- AFF プラットフォームでは、インライン圧縮のみがサポートされます。

ボリュームのインライン圧縮を有効にする前にポストプロセス圧縮を有効にしておく必要があります。ただし、AFF プラットフォームではポストプロセス圧縮がサポートされないため、ボリュームではポストプロセス圧縮は実行されず、ポストプロセス圧縮がスキップされたことを通知する EMS メッセージが生成されます。

- ONTAP 9.8 では、温度に敏感なストレージ効率が導入されています。この機能では、データがホットかコールドかに応じてストレージ効率が適用されます。コールドデータの場合、大容量のデータブロックが圧縮されます。ホットデータの場合、より頻繁に上書きされるデータブロックの場合、小さいデータブロックが圧縮されるため、プロセスの効率が向上します。新しく作成されたシンプロビジョニング AFF ボリュームでは、温度に影響されるストレージ効率が自動的に有効になります。
- 圧縮形式は、アグリゲートのプラットフォームに基づいて自動的に割り当てられます。

プラットフォーム / アグリゲート	圧縮形式
AFF	適応圧縮
Flash Pool アグリゲート	適応圧縮
HDD アグリゲート	二次圧縮

## 選択肢

- を使用します `volume efficiency modify` デフォルトの圧縮形式を使用してデータ圧縮を有効にするコマンド。

次のコマンドは、SVM vs1 のボリューム VolA でポストプロセス圧縮を有効にします。

```
volume efficiency modify -vserver vs1 -volume VolA -compression true
```

次のコマンドは、SVM vs1 のボリューム VolA でポストプロセス圧縮とインライン圧縮の両方を有効にします。

```
volume efficiency modify -vserver vs1 -volume VolA -compression true -inline
-compression true
```

- を使用します `volume efficiency modify` コマンドをadvanced権限レベルで実行し、特定の圧縮形式でデータ圧縮を有効にします。
  - a. を使用します `set -privilege advanced` コマンドを実行して権限レベルをadvancedに変更します。
  - b. を使用します `volume efficiency modify` コマンドを使用してボリュームに圧縮形式を割り当てることができます。

次のコマンドは、SVM vs1 のボリューム VolA でポストプロセス圧縮を有効にして、適応圧縮形式を割り当てます。

```
volume efficiency modify -vserver vs1 -volume VolA -compression true
-compression-type adaptive
```

次のコマンドは、SVM vs1 のボリューム VolA でポストプロセス圧縮とインライン圧縮の両方を有効にして、適応圧縮形式を割り当てます。

```
volume efficiency modify -vserver vs1 -volume VolA -compression true
-compression-type adaptive -inline-compression true
```

- a. を使用します `set -privilege admin` コマンドを実行して権限レベルをadminに変更します。

## 二次圧縮と適応圧縮を切り替えます

データの読み取り量に応じて、二次圧縮と適応圧縮を切り替えることができます。ランダムリードの量が多く、高いパフォーマンスが要求されるシステムには、適応圧縮が適しています。データがシーケンシャルに書き込まれ、圧縮で多くの量を削減することが要求される場合は、二次圧縮が適しています。

このタスクについて

デフォルトの圧縮形式は、使用するアグリゲートとプラットフォームに基づいて選択されます。

## 手順

1. ボリュームのデータ圧縮を無効にします。

```
volume efficiency modify
```

次のコマンドは、ボリューム vol1 のデータ圧縮を無効にします。

```
volume efficiency modify -compression false -inline-compression false -volume vol1
```

2. advanced 権限レベルに切り替えます。

```
set -privilege advanced
```

3. 圧縮データを解凍します。

```
volume efficiency undo
```

次のコマンドは、ボリューム vol1 上の圧縮データを解凍します。

```
volume efficiency undo -vserver vs1 -volume vol1 -compression true
```



圧縮データを格納するための十分なスペースがボリュームにあることを確認する必要があります。

4. 処理のステータスがアイドルであることを確認します。

```
volume efficiency show
```

次のコマンドは、ボリューム vol1 の効率化処理のステータスを表示します。

```
volume efficiency show -vserver vs1 -volume vol1
```

5. データ圧縮を有効にして、圧縮形式を設定します。

```
volume efficiency modify
```

次のコマンドは、ボリューム vol1 でデータ圧縮を有効にして、圧縮形式を二次圧縮に設定します。

```
volume efficiency modify -vserver vs1 -volume vol1 -compression true  
-compression-type secondary
```

この手順では、ボリュームで二次圧縮が有効になるだけで、ボリューム上のデータは圧縮されません。



- AFF システムで既存のデータを圧縮するには、バックグラウンド圧縮スキャナを実行する必要があります。
- Flash Pool アグリゲートまたは HDD アグリゲートで既存のデータを圧縮するには、バックグラウンド圧縮を実行する必要があります。

6. admin 権限レベルに切り替えます。

```
set -privilege admin
```

7. オプション：インライン圧縮を有効にします。

```
volume efficiency modify
```

次のコマンドは、ボリューム vol1 のインライン圧縮を有効にします。

```
volume efficiency modify -vserver vs1 -volume vol1 -inline-compression true
```

ボリュームのデータ圧縮を無効にします

を使用して、ボリュームでのデータ圧縮を無効にできます volume efficiency modify コマンドを実行します

このタスクについて

ポストプロセス圧縮を無効にする場合は、まずボリュームのインライン圧縮を無効にする必要があります。

手順

1. ボリューム上で現在アクティブになっているボリューム効率化処理を停止します。

```
volume efficiency stop
```

2. データ圧縮を無効にします。

```
volume efficiency modify
```

ボリューム上の既存の圧縮済みデータは圧縮されたままになります。圧縮されないのは、ボリュームへの新規の書き込みだけです。

例

次のコマンドは、ボリューム VolA でインライン圧縮を無効にします。

```
volume efficiency modify -vserver vs1 -volume VolA -inline-compression false
```

次のコマンドは、ボリューム VolA でポストプロセス圧縮とインライン圧縮の両方を無効にします。

```
volume efficiency modify -vserver vs1 -volume VolA -compression false -inline  
-compression false
```

## AFF システムのインラインデータコンパクションを管理します

AFF システムでインラインデータコンパクションをボリュームレベルで制御するには、  
を使用します volume efficiency modify コマンドを実行しますAFF システム上の  
すべてのボリュームでは、データコンパクションがデフォルトで有効になっています。

### 必要なもの

データコンパクションを使用するには、ボリュームのスペースギャランティをに設定する必要があります  
none。これはAFF システムのデフォルトです。



AFF 以外のデータ保護ボリュームでは、デフォルトのスペースギャランティが none に設定され  
ます。

### 手順

1. ボリュームのスペースギャランティ設定を確認するには、次の手順を実行します。

```
volume show -vserver vs1 -volume volume_name -fields space-guarantee
```

2. データコンパクションを有効にするには、次の

```
volume efficiency modify -vserver vs1 -volume volume_name -data  
-compaction true
```

3. データコンパクションを無効にする場合：

```
volume efficiency modify -vserver vs1 -volume volume_name -data  
-compaction false
```

4. データコンパクションのステータスを表示するには：

```
volume efficiency show -instance
```

### 例

```
cluster1::> volume efficiency modify -vserver vs1 -volume vol1 -data-compaction  
true cluster1::> volume efficiency modify -vserver vs1 -volume vol1 -data  
-compaction false
```

## FAS システムのインラインデータコンパクションを有効にします

Flash Pool（ハイブリッド）アグリゲートまたはHDDアグリゲートを使用するFAS シス  
テムでは、を使用して、ボリュームレベルまたはアグリゲートレベルでインラインデー  
タコンパクションを制御できます volume efficiency cluster shellコマンド。FAS シ  
ステムのデータコンパクションはデフォルトで無効になっています。

### このタスクについて

アグリゲートレベルでデータコンパクションを有効にすると、ボリュームのスペースギャランティをにして作成された新しいボリュームでデータコンパクションが有効になります `none` アグリゲート内。HDD アグリゲートのボリュームでデータコンパクションを有効にすると、追加の CPU リソースが使用されます。

手順

1. `advanced`権限レベルに切り替えます。+  
`set -privilege advanced`
2. 目的のノードのボリュームとアグリゲートのデータコンパクションの状態を確認します。+  
`volume efficiency show -volume volume_name [+]`
3. ボリュームでデータコンパクションを有効にします：+  
`volume efficiency modify -volume volume_name -data-compaction true`



データコンパクションがに設定されている場合 `false` アグリゲートまたはボリュームの場合、コンパクションは失敗します。コンパクションを有効にしても既存のデータに対しては実行されず、システムへの新規の書き込みに対してのみ実行されます。。 `volume efficiency start` コマンドには、既存データの圧縮方法の詳細が記載されています (ONTAP 9.1以降)。 [+]  
["ONTAP 9コマンド"](#)

4. コンパクションの統計を表示します。  
`volume efficiency show -volume volume_name`

インラインの **Storage Efficiency** 機能は、 **AFF** システムではデフォルトで有効になっています

これまで **Storage Efficiency** 機能は、 **AFF** システムに新規で作成されたすべてのボリュームでデフォルトで有効になっていました。ONTAP 9.2 以降、インラインの **Storage Efficiency** 機能は、すべての **AFF** システムの既存および新規で作成されたすべてのボリュームでデフォルトで有効になります。

**Storage Efficiency** 機能には、インライン重複排除、インラインのボリューム間重複排除、インライン圧縮があります。次の表に示すように、 **AFF** システムではこれらの機能がデフォルトで有効になっています。



データコンパクションは **AFF** ですでにデフォルトで有効になっているため、ONTAP 9.2 での変更はありません。

ボリュームの状態	ONTAP 9.2 では、 <b>Storage Efficiency</b> 機能がデフォルトで有効になります		
	インライン重複排除	インラインのボリューム間重複排除	インライン圧縮
9.2 へのクラスタアップグレード	はい。	はい。	はい。
ONTAP 7-Mode から clustered ONTAP への移行	はい。	はい。	はい。

ボリュームの状態	<b>ONTAP 9.2</b> では、 <b>Storage Efficiency</b> 機能がデフォルトで有効になります		
ボリューム移動	はい。	はい。	はい。
シックプロビジョニングされたボリューム	はい。	いいえ	はい。
暗号化されたボリューム	はい。	いいえ	はい。

次の例外は、1 つ以上のインラインの Storage Efficiency 機能に該当します。

- デフォルトのインラインの Storage Efficiency 機能がサポートされるのは、読み書き可能なボリュームだけです。
- 圧縮による削減が設定されたボリュームでは、インライン圧縮は有効になりません。
- ポストプロセスの重複排除が有効になっているボリュームでは、インライン圧縮は有効になりません。
- ボリューム効率化が無効になっているボリュームでは、既存のボリューム効率化ポリシーの設定が上書きされ、インラインのみのポリシーを有効にするように設定されます。

ストレージ効率情報の表示を有効にします

を使用します `storage aggregate show-efficiency` コマンドを使用して、システム内のすべてのアグリゲートのストレージ効率化に関する情報を表示します。

。 `storage aggregate show-efficiency Command`には、コマンドオプションを渡すことで呼び出すことができる3つの異なるビューがあります。

デフォルトビュー

デフォルトビューには、各アグリゲートの総削減率が表示されます。

```
cluster1::> storage aggregate show-efficiency
```

詳細ビュー

で詳細ビューを呼び出します `-details` コマンドオプション。このビューには次の情報が表示されます。

- 各アグリゲートの総削減率
- Snapshot コピーを除いた総削減率
- 次の効率化テクノロジー別の削減率の内訳：ボリュームの重複排除、ボリュームの圧縮、Snapshot コピー、クローン、データコンパクション、アグリゲートインライン重複排除

```
cluster1::> storage aggregate show-efficiency -details
```

詳細ビュー

アドバンスドビューは詳細ビューと似ており、使用済み論理容量と物理容量の両方の詳細が表示されます。

このコマンドは、advanced 権限レベルで実行する必要があります。を使用してadvanced権限に切り替えま



す `set -privilege advanced` コマンドを実行します

コマンドプロンプトがに変わります `cluster::*>`。

```
cluster1::> set -privilege advanced
```

で詳細ビューを呼び出します `-advanced` コマンドオプション。

```
cluster1::*> storage aggregate show-efficiency -advanced
```

単一のアグリゲートの削減比率を個別に表示するには、を呼び出します `-aggregate aggregate_name` コマンドを実行しますこのコマンドは、 `advanced` 権限レベルだけでなく `admin` レベルでも実行できます。

```
cluster1::> storage aggregate show-efficiency -aggregate aggr1
```

効率化処理を実行するボリューム効率化ポリシーを作成します

効率化処理を実行するボリューム効率化ポリシーを作成します

を使用して、ボリュームに対して重複排除、またはデータ圧縮とそれに続く重複排除を特定の期間実行するボリューム効率化ポリシーを作成し、ジョブスケジュールを指定できます `volume efficiency policy create` コマンドを実行します

作業を開始する前に

を使用してcronスケジュールを作成しておく必要があります `job schedule cron create` コマンドを実行しますcron スケジュールの管理の詳細については、を参照してください "[システムアドミニストレーションリファレンス](#)"。

このタスクについて

事前定義されたデフォルトのロールが割り当てられた SVM 管理者は、重複排除ポリシーを管理できません。ただし、クラスタ管理者は、カスタマイズされた任意のロールを使用して、SVM 管理者に割り当てられている権限を変更できます。SVM 管理者の権限の詳細については、を参照してください "[管理者認証と RBAC](#)"。



重複排除またはデータ圧縮処理は、スケジュールした時刻に実行するか、特定の期間を指定したスケジュールを作成するか、しきい値を指定して実行できます。しきい値を指定した場合、新規データがしきい値を超えた時点で重複排除またはデータ圧縮処理がトリガーされます。このしきい値は、ボリュームで使用されているブロックの総数の割合です。たとえば、ボリュームで使用されるブロックの総数が50%の場合にボリュームのしきい値を20%に設定すると、ボリュームに書き込まれた新しいデータが10%（使用済み50%ブロックの20%）に達したときに、データ重複排除またはデータ圧縮が自動的にトリガーされます。必要に応じて、で使われるブロックの総数を確認できます `df` コマンド出力。

手順

1. を使用します `volume efficiency policy create` コマンドを使用してボリューム効率化ポリシーを作成します。

例

次のコマンドを実行すると、効率化処理を毎日実行する `pol1` という名前のボリューム効率化ポリシーが作成されます。

```
volume efficiency policy create -vserver vs1 -policy pol1 -schedule daily
```

次のコマンドを実行すると、しきい値が 20% に達したときに効率化処理を実行する pol2 という名前のボリューム効率化ポリシーが作成されます。

```
volume efficiency policy create -vserver vs1 -policy pol2 -type threshold -start  
-threshold-percent 20%
```

ボリュームにボリューム効率化ポリシーを割り当てます

を使用して、ボリュームに効率化ポリシーを割り当て、重複排除またはデータ圧縮処理を実行できます volume efficiency modify コマンドを実行します

このタスクについて

効率化ポリシーが SnapVault セカンダリボリュームに割り当てられている場合は、ボリューム効率化処理の実行時に考慮される属性はボリューム効率化優先度のみです。ジョブスケジュールを無視され、重複排除処理は SnapVault セカンダリボリュームに増分更新が実行されたときに実行されます。

ステップ

1. を使用します volume efficiency modify コマンドを使用してボリュームにポリシーを割り当てます。

例

次のコマンドを実行すると、new\_policy という名前のボリューム効率化ポリシーが VolA に割り当てられます。

```
volume efficiency modify -vserver vs1 -volume VolA -policy new_policy
```

ボリューム効率化ポリシーを変更します

を使用して、ボリューム効率化ポリシーを変更して別の期間で重複排除やデータ圧縮を実行したり、ジョブスケジュールを変更したりできます volume efficiency policy modify コマンドを実行します

ステップ

1. を使用します volume efficiency policy modify ボリューム効率化ポリシーを変更するコマンド。

例

次のコマンドを実行すると、policy1 という名前のボリューム効率化ポリシーが変更され、1 時間ごとに実行されるようになります

```
volume efficiency policy modify -vserver vs1 -policy policy1 -schedule hourly
```

次のコマンドを実行すると、pol2 という名前のボリューム効率化ポリシーがしきい値 30% に変更されます。

```
volume efficiency policy modify -vserver vs1 -policy pol1 -type threshold -start  
-threshold-percent 30%
```

ボリューム効率化ポリシーを表示します

を使用して、ボリューム効率化ポリシーの名前、スケジュール、期間、および概要を表示できます `volume efficiency policy show` コマンドを実行します

このタスクについて

を実行すると `volume efficiency policy show` コマンドをクラスタスコープから実行すると、クラスタを対象としたポリシーは表示されません。ただし、Storage Virtual Machine (SVM) のコンテキストでは、クラスタ対象のポリシーを表示できます。

ステップ

1. 使用します `volume efficiency policy show` コマンドを使用して、ボリューム効率化ポリシーに関する情報を表示します。

出力される内容は指定するパラメータによって異なります。詳細ビューおよびその他のパラメータの表示の詳細については、このコマンドのマニュアルページを参照してください。

例

次のコマンドを実行すると、SVM vs1用に作成されたポリシーに関する情報が表示されます。 `volume efficiency policy show -vserver vs1`

次のコマンドは、期間が10時間に設定されているポリシーを表示します。 `volume efficiency policy show -duration 10`

ボリュームからボリューム効率化ポリシーの関連付けを解除します

ボリュームからボリューム効率化ポリシーの割り当てを解除して、そのボリュームに対してスケジュールされている以降の重複排除またはデータ圧縮処理を中止できます。割り当てを解除したボリューム効率化ポリシーは、手動で開始する必要があります。

ステップ

1. 使用します `volume efficiency modify` コマンドを使用して、ボリュームからボリューム効率化ポリシーの関連付けを解除します。

例

次のコマンドは、ボリュームVolAからボリューム効率化ポリシーの関連付けを解除します。 `volume efficiency modify -vserver vs1 -volume VolA -policy -`

ボリューム効率化ポリシーを削除します

を使用して、ボリューム効率化ポリシーを削除できます `volume efficiency policy delete` コマンドを実行します

必要なもの

削除するポリシーが関連付けられているボリュームがないことを確認してください。



*inline-only* および *\_default\_predefined* 効率化ポリシーは削除できません。

## ステップ

1. を使用します `volume efficiency policy delete` ボリューム効率化ポリシーを削除するコマンド。

## 例

次のコマンドは、`policy1`という名前のボリューム効率化ポリシーを削除します。 `volume efficiency policy delete -vserver vs1 -policy policy1`

## ボリューム効率化処理を手動で管理します

ボリューム効率化処理の手動による概要を管理します

効率化処理を手動で実行することで、ボリュームに対する効率化処理の実行方法を管理できます。

また、次の条件に基づいて効率化処理の実行方法を制御することもできます。

- チェックポイントを使用するかどうか
- 既存のデータに対して効率化処理を実行するか、新しいデータに対してのみ実行するかを指定します
- 必要に応じて効率化処理を停止します

を使用できます `volume efficiency show` コマンドにを指定します `schedule` の値 `-fields` オプションを選択して、ボリュームに割り当てられているスケジュールを表示します。

## 効率化処理を手動で実行

を使用して、ボリュームに対して効率化処理を手動で実行できます `volume efficiency start` コマンドを実行します

## 必要なもの

手動で実行する効率化処理に応じて、重複排除またはデータ圧縮と重複排除の両方をボリュームで有効にしておく必要があります。

## このタスクについて

温度に基づくStorage Efficiencyをボリュームで有効にすると、最初に重複排除が実行され、続けてデータ圧縮が実行されます。

重複排除は、実行中にシステムリソースを消費するバックグラウンドプロセスです。ボリューム内のデータの変更頻度が高くない場合は、重複排除の実行頻度を低くすることを推奨します。ストレージシステムで複数の重複排除処理が同時に実行されると、システムリソースの消費量が増加します。

ノードあたり、最大 8 つの重複排除またはデータ圧縮処理を同時に実行できます。これより多くの効率化処理がスケジュール設定されている場合、処理はキューに登録されます。

ONTAP 9.13.1以降では、温度に基づくストレージ効率化がボリュームで有効になっている場合、既存データに対して`volume efficiency`を実行することで、シーケンシャルパッキングを利用してストレージ効率をさらに向上させることができます。

## 効率化を手動で実行

### ステップ

1. ボリュームで効率化処理を開始します。 `volume efficiency start`

#### 例

次のコマンドを使用すると、重複排除のみを手動で開始し、続いて論理圧縮とコンテナ圧縮をボリュームVolAで開始できます

```
volume efficiency start -vserver vs1 -volume VolA
```

### 既存のデータを再パックします

温度の影響を受けやすいStorage Efficiencyが有効になっているボリュームで、ONTAP 9.13.1で導入されたシークエンシャルデータパッキングを利用するには、既存データを再パックします。このコマンドを使用するには、advanced権限モードにする必要があります。

### ステップ

1. 権限レベルを設定します。 `set -privilege advanced`
2. 既存データの再パック： `volume efficiency inactive-data-compression start -vserver vs1 -volume vol1 -scan-mode extended_recompression`

#### 例

```
volume efficiency inactive-data-compression start -vserver vs1 -volume vol1 -scan-mode extended_recompression
```

チェックポイントを使用して効率化処理を再開してください

チェックポイントは、効率化処理の実行プロセスを記録するために内部的に使用されます。何らかの理由（システムの停止、システムの中断、リブート、前回の効率化処理の失敗や停止など）で効率化処理が停止した場合にチェックポイントデータが存在すると、最新のチェックポイントファイルから効率化処理を再開できます。

チェックポイントが作成されます。

- 処理の各段階またはサブ段階
- を実行したとき `sis stop` コマンドを実行します
- 有効期間が終了したとき

停止した効率化処理を再開します

システムの停止、システムの停止、リブートのために効率化処理が停止した場合は、を使用して同じポイントから効率化処理を再開できます `volume efficiency start` チェックポイントオプションを指定したコマンド。これにより、効率化処理を最初からや

り直す必要がなくなるため、時間とリソースを節約できます。

このタスクについて

ボリュームで重複排除のみを有効にした場合は、データに対して重複排除が実行されます。ボリュームで重複排除とデータ圧縮の両方を有効にした場合は、データ圧縮が先に実行され、そのあとに重複排除が実行されます。

を使用して、ボリュームのチェックポイントの詳細を表示できます `volume efficiency show` コマンドを実行します

デフォルトでは、効率化処理はチェックポイントから再開されます。ただし、前回の効率化処理（が実行されたフェーズ）に対応するチェックポイントがある場合は `volume efficiency start -scan-old-data` コマンドを実行）が24時間以上経過している場合、効率化処理は前回のチェックポイントから自動的に再開されません。この場合、効率化処理は最初から開始されます。ただし、前回のスキャン以降にボリュームで重要な変更が行われていないことがわかっている場合は、を使用して強制的に前回のチェックポイントから続行できます `-use-checkpoint` オプション

ステップ

1. を使用します `volume efficiency start` コマンドにを指定します `-use-checkpoint` 効率化処理を再開するオプション。

次のコマンドは、ボリューム VolA 上の新しいデータに対して効率化処理を再開します。

```
volume efficiency start -vserver vs1 -volume VolA -use-checkpoint true
```

次のコマンドは、ボリューム VolA 上の既存データに対して効率化処理を再開します。

```
volume efficiency start -vserver vs1 -volume VolA -scan-old-data true -use-checkpoint true
```

既存データに対して効率化処理を手動で実行します

ONTAP 9.8 より前のバージョンの ONTAP で重複排除、データ圧縮、データコンパクションを有効にする前に、温度に影響しない Storage Efficiency ボリューム上のデータに対して効率化処理を手動で実行できます。これらの処理は、を使用して実行できます

`volume efficiency start -scan-old-data` コマンドを実行します

このタスクについて

。 `-compression` オプションはでは機能しません `-scan-old-data` 温度に影響される Storage Efficiency ボリューム。ONTAP 9.8 以降では、すでに存在しているデータに対して非アクティブなデータ圧縮が自動的に実行され、温度の影響を受けやすい Storage Efficiency ボリュームが対象になります。

ボリュームで重複排除のみを有効にすると、データに対して重複排除が実行されます。ボリュームで重複排除、データ圧縮、データコンパクションを有効にすると、データ圧縮が先に実行され、そのあとに重複排除とデータコンパクションが実行されます。

既存データにデータ圧縮を実行する場合、デフォルトでは、重複排除によって共有されているデータブロックと Snapshot コピーによってロックされているデータブロックがスキップされます。共有ブロックに対してデータ圧縮を実行することを選択した場合、最適化が無効になり、フィンガープリント情報が取得されて再度共有するために使用されます。既存データを圧縮する際には、データ圧縮のデフォルトの動作を変更できます。

ノードあたり最大 8 つの重複排除、データ圧縮、データコンパクション処理を同時に実行できます。残りの処理はキューに登録されます。



AFF プラットフォームではポストプロセス圧縮が実行されません。この処理がスキップされたことを通知する EMS メッセージが生成されます。

#### ステップ

1. 使用します `volume efficiency start -scan-old-data` コマンドを使用して、既存データに対して重複排除、データ圧縮、またはデータコンパクションを手動で実行します。

次のコマンドは、これらの処理をボリューム VolA の既存データに対して手動で実行します。

```
volume efficiency start -vserver vs1 -volume VolA -scan-old-data true [-compression | -dedupe | -compaction ] true
```

#### スケジュールを使用してボリューム効率化処理を管理します

書き込まれた新しいデータの量に応じて効率化処理を実行します

効率化処理スケジュールを変更し、前回の効率化処理（手動またはスケジュールによる）後にボリュームに書き込まれた新規ブロック数が指定のしきい値を超えたときに、重複排除またはデータ圧縮を実行することができます。

#### このタスクについて

状況に応じて `schedule` オプションはに設定されています `auto` スケジュールされた効率化処理は、新規データの量が指定した割合を超えると実行されます。デフォルトのしきい値は 20% です。このしきい値は、すでに効率化処理によって処理された総ブロック数に対する割合です。

#### ステップ

1. 使用します `volume efficiency modify` コマンドにを指定します `auto@num` しきい値を変更するオプション。

`num` は、パーセンテージを指定する2桁の数値です。

#### 例

次のコマンドは、ボリューム VolA のしきい値を 30% に変更します。

```
volume efficiency modify -vserver vs1 -volume -VolA -schedule auto@30
```

#### スケジュールを使用して効率化処理を実行

を使用して、ボリュームに対する重複排除やデータ圧縮処理のスケジュールを変更できます `volume efficiency modify` コマンドを実行しますスケジュールおよびボリューム効率化ポリシーの設定オプションを同時に指定することはできません。

#### ステップ

1. 使用します `volume efficiency modify` コマンドを使用して、ボリュームに対する重複排除またはデータ圧縮処理のスケジュールを変更します。

## 例

次のコマンドは、VolA の効率化処理が月曜日から金曜日の午後 11 時に実行されるようにスケジュールを変更します。

```
volume efficiency modify -vserver vs1 -volume VolA -schedule mon-fri@23
```

## ボリューム効率化処理を監視

効率化処理とステータスを表示します

ボリュームで重複排除またはデータ圧縮が有効になっているかどうかを確認できます。また、を使用して、ボリュームに対する効率化処理のステータス、状態、圧縮形式、および進捗状況を表示できます volume efficiency show コマンドを実行します

効率化ステータスを表示します

## ステップ

1. ボリュームに対する効率化処理のステータスを表示します。 volume efficiency show

次のコマンドは、適応圧縮形式が割り当てられたボリューム VolA に対する効率化処理のステータスを表示します。

```
volume efficiency show -instance -vserver vs1 -volume VolA
```

効率化処理が VolA に対して有効になっており、処理がアイドルの場合、次のシステム出力が表示されます。

```
cluster1::> volume efficiency show -vserver vs1 -volume VolA
```

```
Vserver Name: vs1
Volume Name: VolA
Volume Path: /vol/VolA
    State: Enabled
    Status: Idle
    Progress: Idle for 00:03:20
```

ボリュームにシーケンシャルにパックされたデータがあるかどうかを確認します

シーケンシャルパッキングが有効になっているボリュームのリストを表示できます。たとえば、9.13.1より前のONTAP リリースにリポートする必要がある場合などです。このコマンドを使用するには、advanced権限モードにする必要があります。

## ステップ

1. 権限レベルを設定します。 set -privilege advanced
2. シーケンシャルパッキングが有効になっているボリュームを表示します。 'volume efficiency show -extended-auto-adaptive-compression true'



効率化によるスペース削減率を表示します

を使用して、ボリュームで重複排除およびデータ圧縮によって達成されたスペース削減量を表示できます volume show コマンドを実行します

このタスクについて

Snapshot コピーのスペース削減量は、ボリュームに対して達成されたスペース削減量の算出には含まれません。重複排除を使用しても、ボリュームのクォータに影響しません。クォータは論理レベルで報告され、変更されません。

ステップ

1. 使用します volume show コマンドを使用して、重複排除とデータ圧縮を使用してボリュームで達成されたスペース削減量を表示します。

例

次のコマンドを使用すると、ボリュームVolAで重複排除およびデータ圧縮を使用して達成されたスペース削減量を表示できます。 volume show -vserver vs1 -volume VolA

```
cluster1::> volume show -vserver vs1 -volume VolA

Vserver Name: vs1
Volume Name: VolA

...
    Space Saved by Storage Efficiency: 115812B
Percentage Saved by Storage Efficiency: 97%
    Space Saved by Deduplication: 13728B
Percentage Saved by Deduplication: 81%
    Space Shared by Deduplication: 1028B
    Space Saved by Compression: 102084B
Percentage Space Saved by Compression: 97%

...
```

**FlexVol** ボリュームの効率化に関する統計を表示します

を使用して、FlexVol ボリュームに対して実行される効率化処理の詳細を表示できます volume efficiency stat コマンドを実行します

ステップ

1. 使用します volume efficiency stat コマンドを使用して、FlexVol に対する効率化処理の統計を表示します。

例

次のコマンドを使用すると、ボリュームVolAに対する効率化処理の統計を表示できます。

volume efficiency stat -vserver vs1 -volume VolA

```
cluster1::> volume efficiency stat -vserver vs1 -volume VolA
```

```
Vserver Name: vs1
```

```
Volume Name: VolA
```

```
Volume Path: /vol/VolA
```

```
Inline Compression Attempts: 0
```

ボリューム効率化処理を停止します

重複排除またはポストプロセス圧縮処理は、を使用して停止できます `volume efficiency stop` コマンドを実行しますこのコマンドではチェックポイントが自動的に生成されます。

ステップ

1. を使用します `volume efficiency stop` コマンドを使用して、アクティブな重複排除処理またはポストプロセス圧縮処理を停止します。

を指定する場合は `-all` オプション。アクティブな効率化処理とキューに登録されている効率化処理は中止されます。

例

次のコマンドを実行すると、ボリューム VolA で現在アクティブな重複排除処理またはポストプロセス圧縮処理が停止します。

```
volume efficiency stop -vserver vs1 -volume VolA
```

次のコマンドを実行すると、ボリューム VolA でアクティブな、およびキューに登録されている重複排除処理またはポストプロセス圧縮処理が停止します。

```
volume efficiency stop -vserver vs1 -volume VolA -all true
```

ボリュームからのスペース削減の取り消しに関する情報

ボリュームで効率化処理を実行した場合に削減されるスペースを削除することもできますが、その逆も十分なスペースが必要です。

次の記事を参照してください。

- ["ONTAP 9での重複排除、圧縮、およびコンパクションによるスペース削減効果の確認方法"](#)
- ["ONTAP でのStorage Efficiencyによる削減効果を取り消す方法"](#)

**SVM** から別の **SVM** にボリュームをリホストします

**SVM** から別の **SVM** にボリュームをリホストする処理の概要

ボリュームをリホストすると、NAS または SAN ボリュームをある Storage Virtual

Machine（SVM、旧 Vserver）から別の SVM に再割り当てできます。SnapMirror コピーは必要ありません。ボリュームのリホスト手順は、プロトコルのタイプとボリュームのタイプによって異なります。ボリュームのリホストはシステム停止を伴う処理であり、データアクセスとボリューム管理のために実行されます。

作業を開始する前に

ボリュームをある SVM から別の SVM にリホストするには、次の条件を満たしている必要があります。

- ボリュームはオンラインである必要があります。
- プロトコル：SAN または NAS

NAS プロトコルの場合は、ボリュームをアンマウントする必要があります。

- ボリュームが SnapMirror 関係にある場合は、ボリュームをリホストする前に、その関係を削除または解除する必要があります。

ボリュームのリホスト処理後に、SnapMirror 関係を再同期できます。

### **SMB**ボリュームをリホストします

SMBプロトコル経由でデータを提供するボリュームをリホストできます。CIFS ボリュームのリホスト後、引き続き SMB プロトコル経由でデータにアクセスするためには、ポリシーと関連ルールを手動で設定する必要があります。

このタスクについて

- リホストはシステム停止を伴う処理です。
- リホスト処理が失敗した場合は、ソースボリュームでボリュームのポリシーおよび関連するルールを再設定しなければならない場合があります。
- ソース SVM とデスティネーション SVM の Active Directory ドメインが異なる場合は、ボリューム上のオブジェクトへのアクセスが失われる可能性があります。
- ONTAP 9.8以降では、NetApp Volume Encryption（NVE）を使用するボリュームのリホストがサポートされます。オンボードキーマネージャを使用している場合は、リホスト処理中に暗号化されたメタデータが変更されます。ユーザデータは変更されません。

ONTAP 9.8以前を使用している場合は、リホスト処理を実行する前にボリュームの暗号化を解除する必要があります。

- ソース SVM にローカルユーザとローカルグループが含まれている場合、ファイルとディレクトリに対して設定された権限（ACL）はボリュームのリホスト処理後に無効になります。

監査 ACL（SACL）についても同様です。

- 次のボリュームポリシー、ポリシールール、および構成はリホスト処理後にソースボリュームから失われるため、リホスト後のボリュームで手動で再設定する必要があります。
  - ボリュームと qtree のエクスポートポリシー
  - ウィルス対策ポリシー

- ボリューム効率化ポリシー
- Quality of Service （ QoS ; サービス品質）ポリシー
- Snapshot ポリシー
- クォータルール
- ns-switch とネームサービスの設定のエクスポートポリシーとルール
- ユーザ ID とグループ ID

作業を開始する前に

- ボリュームはオンラインである必要があります。
- ボリュームの移動や LUN の移動など、ボリューム管理操作を実行しないでください。
- リホストするボリュームへのデータアクセスを停止する必要があります。
- リホストするボリュームのデータアクセスをサポートするようにターゲット SVM の ns-switch とネームサービスを設定する必要があります。
- ソース SVM とデスティネーション SVM の Active Directory ドメインと DNS ドメインが同じであることが必要です。
- ボリュームのユーザ ID とグループ ID をターゲット SVM で使用可能であるか、またはホストするボリュームで変更する必要があります。



ローカルユーザとローカルグループが設定されていて、それらのユーザまたはグループに対して権限が設定されたボリューム上にファイルとディレクトリがある場合、それらの権限は無効になります。

手順

1. ボリュームのリホスト処理が失敗した場合に CIFS 共有の情報が失われないように、CIFS 共有に関する情報を記録します。
2. 親ボリュームからボリュームをアンマウントします。

```
volume unmount
```

3. advanced 権限レベルに切り替えます。

```
set -privilege advanced
```

4. デスティネーション SVM でボリュームをリホストします。

```
volume rehost -vserver source_svm -volume vol_name -destination-vserver destination_svm
```

5. デスティネーション SVM の適切なジャンクションパスにボリュームをマウントします。

```
volume mount
```

6. リホストしたボリューム用の CIFS 共有を作成します。

```
vserver cifs share create
```

7. ソース SVM とデスティネーション SVM で DNS ドメインが異なる場合は、新しいユーザとグループを作成します。
8. 新しいデスティネーション SVM の LIF とリホストしたボリュームへのジャンクションパスで、CIFS クライアントを更新します。

完了後

ポリシーおよび関連するルールをリホストしたボリュームに手動で再設定する必要があります。

## "SMBの設定"

### "SMB および NFS のマルチプロトコル構成"

#### NFS ボリュームをリホスト

NFS プロトコル経由でデータを提供するボリュームをリホストできます。NFS ボリュームのリホスト後、引き続き NFS プロトコル経由でデータに継続的にアクセスするためには、ボリュームをホストする SVM のエクスポートポリシーに関連付けて、ポリシーと関連ルールを手動で設定する必要があります。

このタスクについて

- リホストはシステム停止を伴う処理です。
- リホスト処理が失敗した場合は、ソースボリュームでボリュームのポリシーおよび関連するルールを再設定しなければならない場合があります。
- ONTAP 9.8以降では、NetApp Volume Encryption (NVE) を使用するボリュームのリホストがサポートされます。オンボードキーマネージャを使用している場合は、リホスト処理中に暗号化されたメタデータが変更されます。ユーザデータは変更されません。

ONTAP 9.8以前を使用している場合は、リホスト処理を実行する前にボリュームの暗号化を解除する必要があります。

- 次のボリュームポリシー、ポリシールール、および構成はリホスト処理後にソースボリュームから失われるため、リホスト後のボリュームで手動で再設定する必要があります。
  - ボリュームと qtree のエクスポートポリシー
  - ウィルス対策ポリシー
  - ボリューム効率化ポリシー
  - Quality of Service (QoS ; サービス品質) ポリシー
  - Snapshot ポリシー
  - クォータルール
  - ns-switch とネームサービスの設定のエクスポートポリシーとルール
  - ユーザ ID とグループ ID

作業を開始する前に

- ボリュームはオンラインである必要があります。
- ボリューム移動や LUN 移動などのボリューム管理操作は実行しないでください。

- リホストするボリュームへのデータアクセスを停止する必要があります。
- リホストするボリュームのデータアクセスをサポートするようにターゲット SVM の ns-switch とネームサービスを設定する必要があります。
- ボリュームのユーザ ID とグループ ID をターゲット SVM で使用可能であるか、またはホストするボリュームで変更する必要があります。

#### 手順

1. ボリュームのリホスト処理が失敗した場合に NFS ポリシーの情報が失われないように、NFS エクスポートポリシーに関する情報を記録します。
2. 親ボリュームからボリュームをアンマウントします。

```
volume unmount
```

3. advanced 権限レベルに切り替えます。

```
set -privilege advanced
```

4. デスティネーション SVM でボリュームをリホストします。

```
volume rehost -vserver source_svm -volume volume_name -destination-vserver destination_svm
```

デスティネーション SVM のデフォルトのエクスポートポリシーがリホストしたボリュームに適用されます。

5. エクスポートポリシーを作成します。

```
vserver export-policy create
```

6. リホストしたボリュームのエクスポートポリシーをユーザ定義のエクスポートポリシーに更新します。

```
volume modify
```

7. デスティネーション SVM の適切なジャンクションパスにボリュームをマウントします。

```
volume mount
```

8. デスティネーション SVM で NFS サービスが実行されていることを確認します。
9. リホストしたボリュームへの NFS アクセスを再開します。
10. NFS クライアントのクレデンシャルと LIF の構成を更新して、デスティネーション SVM の LIF を反映させます。

これは、ボリュームのアクセスパス（LIF とジャンクションパス）が変更されているためです。

#### 完了後

ポリシーおよび関連するルールをリホストしたボリュームに手動で再設定する必要があります。

#### "NFS構成"

## SANボリュームのリホスト

LUN をマッピングしたボリュームをリホストできます。デスティネーション SVM でイニシエータグループ（igroup）を再作成したら、ボリュームのリホストによって同じ SVM でボリュームを自動的に再マッピングできます。

このタスクについて

- リホストはシステム停止を伴う処理です。
- リホスト処理が失敗した場合は、ソースボリュームでボリュームのポリシーおよび関連するルールを再設定しなければならない場合があります。
- ONTAP 9.8以降では、NetApp Volume Encryption（NVE）を使用するボリュームのリホストがサポートされます。オンボードキーマネージャを使用している場合は、リホスト処理中に暗号化されたメタデータが変更されます。ユーザデータは変更されません。

ONTAP 9.8以前を使用している場合は、リホスト処理を実行する前にボリュームの暗号化を解除する必要があります。

- 次のボリュームポリシー、ポリシールール、および構成はリホスト処理後にソースボリュームから失われるため、リホスト後のボリュームで手動で再設定する必要があります。
  - ウィルス対策ポリシー
  - ボリューム効率化ポリシー
  - Quality of Service（QoS；サービス品質）ポリシー
  - Snapshot ポリシー
  - ns-switch とネームサービスの設定のエクスポートポリシーとルール
  - ユーザ ID とグループ ID

作業を開始する前に

- ボリュームはオンラインである必要があります。
- ボリューム移動や LUN 移動などのボリューム管理操作は実行しないでください。
- ボリュームまたは LUN にアクティブな I/O がないことを確認します。
- デスティネーション SVM に同じ名前でイニシエータが異なる igroup がないことを確認しておく必要があります。

igroup の名前が同じ場合は、どちらか（ソースまたはデスティネーション）の SVM で igroup の名前を変更する必要があります。

- を有効にしておく必要があります force-unmap-luns オプション
  - のデフォルト値 force-unmap-luns オプションは false。
  - を設定しても、警告メッセージや確認メッセージは表示されません force-unmap-luns オプションを true に設定します。

手順

1. ターゲットボリュームの LUN マッピング情報を記録します。

```
lun mapping show volume volume vserver source_svm
```

これは、ボリュームのリホストが失敗した場合に LUN マッピングに関する情報が失われないようにするための予防的な手順です。

2. ターゲットボリュームに関連付けられている igroup を削除します。
3. デスティネーション SVM にターゲットボリュームをリホストします。

```
volume rehost -vserver source_svm -volume volume_name -destination-vserver destination_svm
```

4. ターゲットボリューム上の LUN を適切な igroup にマッピングします。
  - ボリュームのリホストではターゲットボリュームに LUN が保持されますが、マッピングされていないままです。
  - LUN のマッピングにはデスティネーション SVM のポートセットを使用します。
  - 状況に応じて `auto-remap-luns` オプションはに設定されています `true` を指定すると、リホスト後に LUN が自動的にマッピングされます。

## SnapMirror 関係にあるボリュームをリホストします

## SnapMirror 関係にあるボリュームをリホストできます。

### このタスクについて

- リホストはシステム停止を伴う処理です。
- リホスト処理が失敗した場合は、ソースボリュームでボリュームのポリシーおよび関連するルールを再設定しなければならない場合があります。
- 次のボリュームポリシー、ポリシールール、および構成はリホスト処理後にソースボリュームから失われるため、リホスト後のボリュームで手動で再設定する必要があります。
  - ボリュームと qtrees のエクスポートポリシー
  - ウィルス対策ポリシー
  - ボリューム効率化ポリシー
  - Quality of Service (QoS ; サービス品質) ポリシー
  - Snapshot ポリシー
  - クォータルール
  - ns-switch とネームサービスの設定のエクスポートポリシーとルール
  - ユーザ ID とグループ ID

### 作業を開始する前に

- ボリュームはオンラインである必要があります。
- ボリューム移動や LUN 移動などのボリューム管理操作は実行しないでください。
- リホストするボリュームへのデータアクセスを停止する必要があります。
- リホストするボリュームのデータアクセスをサポートするようにターゲット SVM の ns-switch とネームサービスを設定する必要があります。



- ボリュームのユーザ ID とグループ ID をターゲット SVM で使用可能であるか、またはホストするボリュームで変更する必要があります。

## 手順

1. SnapMirror 関係のタイプを記録します。

```
snapmirror show
```

これは、ボリュームのリホストが失敗した場合に SnapMirror 関係のタイプに関する情報が失われないようにするための予防的な手順です。

2. デスティネーションクラスタから、SnapMirror 関係を削除します。

```
snapmirror delete
```

SnapMirror 関係は解除しないでください。解除するとデスティネーションボリュームのデータ保護機能が失われ、リホスト処理の完了後に関係を再確立できません。

3. ソースクラスタから、SnapMirror 関係情報を削除します。

```
snapmirror release relationship-info-only true
```

を設定します relationship-info-only パラメータの値 true Snapshotコピーを削除せずにソースの関係情報を削除します。

4. advanced 権限レベルに切り替えます。

```
set -privilege advanced
```

5. デスティネーション SVM でボリュームをリホストします。

```
volume rehost -vserver source_svm -volume vol_name -destination-vserver  
destination_svm
```

6. SVM ピア関係が存在しない場合は、ソース SVM とデスティネーション SVM 間に SVM ピア関係を作成します。

```
vserver peer create
```

7. ソースボリュームとデスティネーションボリューム間に SnapMirror 関係を作成します。

```
snapmirror create
```

を実行する必要があります snapmirror create DPボリュームをホストしているSVMからコマンドを実行します。リホストしたボリュームは、SnapMirror 関係のソースまたはデスティネーションにすることができます。

8. SnapMirror 関係を再同期

ボリュームのリホストをサポートしていない機能

特定の機能では、ボリュームのリホストがサポートされません。

次の機能では、ボリュームのリホストがサポートされません。

- SVM DR
- MetroCluster 構成



MetroCluster構成では、ボリュームをFlexCloneボリュームとして別のSVMにクローニングすることもできません。

- SnapLock ボリューム
- NetApp Volume Encryption (NVE) ボリューム (ONTAP 9.8より前のバージョン)

ONTAP 9.8より前のリリースでは、ボリュームをリホストする前に暗号化を解除する必要があります。ボリュームの暗号化キーは SVM キーによって異なります。ボリュームを別の SVM に移動した場合に、ソースまたはデスティネーションの SVM でマルチテナントキーの設定が有効になっていれば、ボリュームと SVM キーは一致しません。

ONTAP 9.8以降では、NVEを使用してボリュームをリホストできます。

- FlexGroup ボリューム
- ボリュームをクローニングする

## ストレージの制限

ストレージオブジェクトには、ストレージアーキテクチャを計画および管理するときに考慮する必要がある制限があります。

制限は多くの場合、プラットフォームによって異なります。を参照してください ["NetApp Hardware Universe の略"](#) をクリックして、それぞれの構成の制限事項を確認してください。を参照してください [\[hwu\]](#) ONTAP構成に適した情報を特定する手順については、を参照してください。

制限は次のセクションに記載されています。

- [\[vollimits\]](#)
- [\[flexclone\]](#)

Cloud Volumes ONTAP でのストレージの制限については、を参照してください ["Cloud Volumes ONTAP リリースノート"](#)。

## ボリュームの制限

ストレージオブジェクト	制限 ( Limit )	ネイティブストレージ	ストレージアレイ
• アレイ LUN *	ルートボリュームの最小サイズ <sup>^1</sup>	N/A	モデルによって異なります
• ファイル *	最大サイズ	バージョンに依存 <sup>2</sup>	バージョンに依存 <sup>2</sup>

ストレージオブジェクト	制限 ( Limit )	ネイティブストレージ	ストレージアレイ
ボリュームあたりの最大数 <sup>4</sup>	ボリュームサイズに依存、最大20億	ボリュームサイズに依存、最大20億	• FlexClone ボリューム *
クローン階層の深さ <sup>5</sup>	499	499	• FlexVol ボリューム *
ノードあたりの最大値 <sup>1</sup> ^	モデルによって異なります	モデルによって異なります	各SVMのノードあたりの最大数 <sup>6</sup>
モデルによって異なります	モデルによって異なります	最小サイズ	20MB
20MB	最大サイズ <sup>1</sup> ^	モデルによって異なります	モデルによって異なります
• プライマリワークロード用の FlexVol ボリューム *	ノードあたりの最大数 <sup>3</sup>	モデルによって異なります	モデルによって異なります
• FlexVol ルートボリューム *	最小サイズ <sup>1</sup> ^	モデルによって異なります	モデルによって異なります
• LUN*	ノードあたりの最大数 <sup>6</sup>	モデルによって異なります	モデルによって異なります
クラスタあたりの最大数 <sup>6</sup>	モデルによって異なります	モデルによって異なります	ボリュームあたりの最大値 <sup>6</sup>
モデルによって異なります	モデルによって異なります	最大サイズ	バージョンに依存 <sup>2</sup>
バージョンに依存 <sup>2</sup>	• qtree *	FlexVol あたりの最大数	4,995人
4,995人	• Snapshot コピー *	ボリュームあたりの最大数 <sup>7</sup>	255/1023
255/1023	• ボリューム *	NAS のクラスタあたりの最大数	12、000
12、000	SAN プロトコルが設定されたクラスタあたりの最大数	モデルによって異なります	モデルによって異なります

• 注： \*

1. ONTAP 9.3 以前では、ボリュームに格納できる Snapshot コピーは最大 255 個です。ONTAP 9.4 以降では、ボリュームに格納できる Snapshot コピーは最大 1023 個です。

2. ONTAP 9.12.1P2以降では、上限は128TBです。ONTAP 9.11.1以前のバージョンでは、最大16TBです。
3. ONTAP FlexVol 9.7以降では、128GB以上のメモリを搭載したAFFプラットフォームでサポートされるFlexVolの最大数がノードあたり2、500個に引き上げられました。

プラットフォーム固有の情報およびサポートの最新情報については、を参照してください "[Hardware Universe](#)"。

4. 20 億  $= 2 \times 10^9$ 。
5. 1 つの FlexVol から作成できる、ネストされた FlexClone ボリュームの最大階層数。
6. この制限は SAN 環境にのみ適用されます。

#### "SAN構成"

7. SnapMirror カスケード構成を使用してこの制限を引き上げることができます。

### FlexClone ファイルと FlexClone LUN の制限

制限 ( Limit )	ネイティブストレージ	ストレージアレイ
• ファイルまたは LUN あたりの最大数 <sup>**^1</sup>	32、767	32、767
• FlexVol ボリュームあたりの最大合計共有データ数 *	640 TB	640 TB

#### • 注： \*

1. 32 、 767 個を超えるクローンを作成しようとする、親ファイルまたは親 LUN の新しい物理コピーが ONTAP によって自動的に作成されます。

重複排除を使用する FlexVol の場合、上限値はこれよりも低い可能性があります。

### NetApp Hardware Universeのナビゲート

プラットフォーム固有の制限およびモデルに依存する制限については、を参照してください。 "[NetApp Hardware Universe の略](#)"。

#### 手順

1. [**\* Products**]ドロップダウンメニューで、ハードウェア構成を選択します。

| Hardware Universe

Products
Utilities
Toolbox
Information
Support

**Platforms**  
AFF A-Series  
AFF C-Series  
All SAN Array (ASA)  
- ASA A-Series  
- ASA C-Series  
- ASA AFF  
FAS  
HCI and SolidFire (H-Series, eSDS)  
E-Series  
StorageGRID  
ONTAP Select

**Networking**  
Adapters  
Switches  
Cables / Transceivers

**Storage**  
Shelves  
- ONTAP (AFF, ASA, FAS)  
- SANtricity OS  
Drives

**Cabinets and Power Cords**  
Cabinets  
Power Cords  
Rackmount Kits

**Legacy Products**  
Platforms  
- AltaVault  
- SA-Series  
- SF-Series  
Shelves  
- AltaVault

2. プラットフォームを選択します。

☒ **Start with Platforms**
☐ **Start with OS**
Help

☐ **Show EOA Platforms**
☒ **Display Platform Configurations**

Filter Platforms

☐ **AFF C-Series**
☐ **AFF C250**
☐ AFF C250 Single Chassis HA Pair
☐ AFF C250 Single Chassis HA Pair 100V
☐ AFF C250 4-Node MetroCluster IP
☐ AFF C250 8-Node MetroCluster IP
☐ **AFF C400**
☐ AFF C400 Single Chassis HA Pair, Ethernet Bundle
☐ AFF C400 Single Chassis HA Pair, FC Bundle
☐ AFF C400 4-Node MetroCluster IP, Ethernet Bundle
☐ AFF C400 4-Node MetroCluster IP, FC Bundle
☐ AFF C400 8-Node MetroCluster IP, Ethernet Bundle
☐ AFF C400 8-Node MetroCluster IP, FC Bundle
☐ **AFF C800**
☐ AFF C800 Single Chassis HA Pair
☐ AFF C800 4-Node MetroCluster IP

3. 適切なバージョンのONTAPを選択し、**Show Results**を選択します。

Start with Platforms

Start with OS

Help

☐ Show EOA Platforms
 ☒ Display Platform Configurations

Filter Platforms

AFF C-Series

☐ AFF C250
 

☐ AFF C250 Single Chassis HA Pair
 ☐ AFF C250 Single Chassis HA Pair 100V
 ☐ AFF C250 4-Node MetroCluster IP
 ☐ AFF C250 8-Node MetroCluster IP

☐ AFF C400
 

☐ AFF C400 Single Chassis HA Pair, Ethernet Bundle
 ☐ AFF C400 Single Chassis HA Pair, FC Bundle
 ☐ AFF C400 4-Node MetroCluster IP, Ethernet Bundle
 ☐ AFF C400 4-Node MetroCluster IP, FC Bundle
 ☐ AFF C400 8-Node MetroCluster IP, Ethernet Bundle
 ☐ AFF C400 8-Node MetroCluster IP, FC Bundle

☒ AFF C800
 

☒ AFF C800 Single Chassis HA Pair
 ☒ AFF C800 4-Node MetroCluster IP
 ☒ AFF C800 8-Node MetroCluster IP

Clear

Filter by OS Status :

☐ Show All
 ☒ Hide EOVS
 ☐ Hide Obsolete

Show OS :

☒ Support at least one of the platform selected
 ☐ Support all the platform selected
 ☐ Show all

DataONTAP

9.14.1

☐ Release Candidate
 

☐ 9.14.1RC1

9.13.1

☒ General Availability
 

☒ 9.13.1

☐ Patch Release
 

☐ 9.13.1P6
 ☐ 9.13.1P4
 ☐ 9.13.1P3
 ☐ 9.13.1P2
 ☐ 9.13.1P1

9.12.1

☐ Patch Release
 

☐ 9.12.1P10
 ☐ 9.12.1P9
 ☐ 9.12.1P8

Clear

Note: AFF C190 model information is in the AFF A-Series product category

Preference ▾

Show Results

## 関連情報

"使用しているバージョンの Cloud Volumes ONTAP のリリースノートを検索してください"

## 推奨されるボリュームとファイルまたは LUN の設定の組み合わせ

推奨されるボリュームとファイルまたは LUN の設定の組み合わせの概要

使用可能な FlexVol の設定とファイルまたは LUN の設定の組み合わせは、使用するアプリケーションと管理要件によって異なります。これらの組み合わせのメリットとデメリットを理解しておく、環境に適したボリュームと LUN の設定の組み合わせを決定する際に役立ちます。

推奨されるボリュームと LUN の設定の組み合わせは次のとおりです。

- スペースリザーブファイルまたはスペースリザーブ LUN とシックボリュームプロビジョニング

- スペースリザーブなしのファイルまたはスペースリザーブなしの LUN とシンボリックボリュームプロビジョニング
- スペースリザーブファイルまたはスペースリザーブ LUN とセミシックボリュームプロビジョニング

これらのいずれかの設定の組み合わせとともに、LUN で SCSI シンボリックプロビジョニングを使用できます。

スペースリザーブファイルまたはスペースリザーブ **LUN** とシックボリュームプロビジョニング

- 利点 :\*
- スペースリザーブファイルでのすべての書き込み処理が保証されます。スペース不足のために失敗することはありません。
- ボリュームでの Storage Efficiency テクノロジーとデータ保護テクノロジーに関する制限はありません。
- コストと制限 : \*
- シックプロビジョニングボリュームをサポートするための十分なスペースをアグリゲートから事前に確保しておく必要があります。
- LUN 作成時に、LUN の 2 倍のサイズのスペースがボリュームから割り当てられます。

スペースリザーブなしのファイルまたはスペースリザーブなしの **LUN** とシンボリックボリュームプロビジョニング

- 利点 :\*
- ボリュームでの Storage Efficiency テクノロジーとデータ保護テクノロジーに関する制限はありません。
- スペースは使用時に初めて割り当てられます。
- 費用および制限 :\*
- 書き込み処理は保証されず、ボリュームの空きスペースが不足すると失敗する場合があります。
- アグリゲートの空きスペースを効果的に管理して、空きスペースが不足しないようにする必要があります。

スペースリザーブファイルまたはスペースリザーブ **LUN** とセミシックボリュームプロビジョニング

- 利点 :\*

事前に確保されるスペースがシックボリュームプロビジョニングの場合よりも少なく、ベストエフォートの書き込み保証も提供されます。

- 費用および制限 :\*
- このオプションを指定すると、書き込み処理が失敗することがあります。

このリスクは、ボリュームの空きスペースとデータの揮発性の適切なバランスを維持することで軽減できます。

- Snapshot コピー、FlexClone ファイル、FlexClone LUN などのデータ保護オブジェクトは保持できません。
- 重複排除、圧縮、ODX / コピーオフロードなど、自動で削除できない ONTAP のブロック共有ストレージ効率化機能は使用できません。

環境に適したボリュームと **LUN** の構成の組み合わせを決定します

環境に関するいくつかの基本的な質問に答えることで、環境に最も適した FlexVol ボリュームと LUN の設定を決定できます。

このタスクについて

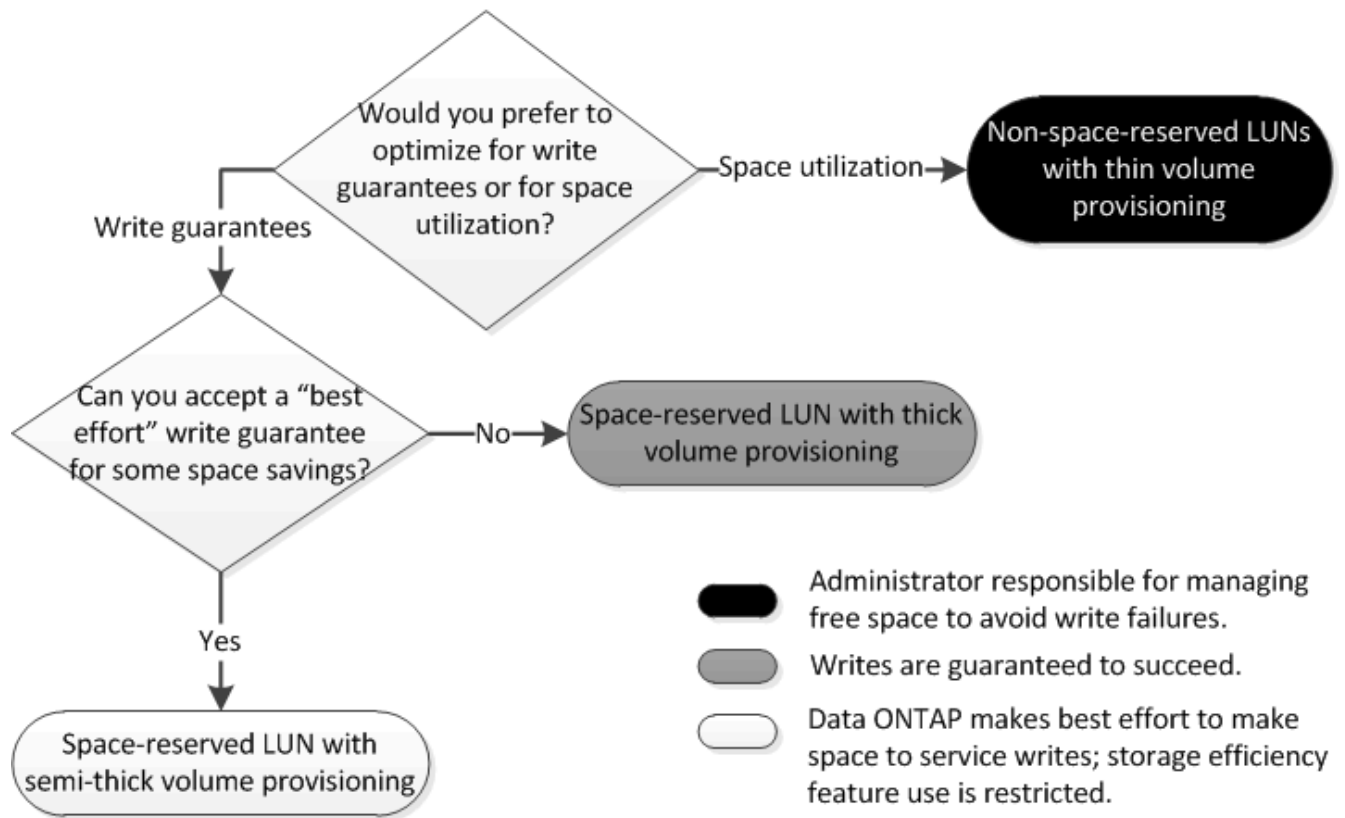
LUN とボリュームの設定は、ストレージ利用率を最大限に高めるため、または書き込みを確実に保証するために最適化することができます。ストレージの利用要件と、空きスペースを監視し迅速に補充するための要件に基づいて、ご使用の環境に適した FlexVol ボリュームと LUN ボリュームを決める必要があります。



LUN ごとに個別のボリュームを設定する必要はありません。

#### ステップ

1. 次のデシジョンツリーを使用して、環境に最も適したボリュームと LUN の設定の組み合わせを決定してください。



スペースリザーブファイルまたはスペースリザーブ **LUN** とシックプロビジョニングボリュームを組み合わせた場合の構成設定

この FlexVol とファイルまたは LUN の設定の組み合わせでは、Storage Efficiency テクノロジーを使用できます。また、事前に十分なスペースが割り当てられるため、空きスペースを能動的に監視する必要はありません。

シックプロビジョニングを使用するボリュームでスペースリザーブファイルまたはスペースリザーブ LUN を設定するには、次の設定が必要です。



音量設定	価値
保証	ボリューム
フラクショナルリザーブ	100
Snapshot リザーブ	任意
Snapshot の自動削除	任意。
自動拡張	オプション。有効にした場合は、アグリゲートの空きスペースを能動的に監視する必要があります。

ファイルまたは <b>LUN</b> の設定	価値
スペースリザーベーション	有効

スペースリザーブなしのファイルまたはスペースリザーブなしの **LUN** とシンプロビジョニングボリュームを組み合わせた場合の構成設定

この FlexVol とファイルまたは LUN の設定の組み合わせでは、事前に割り当てられるストレージの量が最小になりますが、スペース不足によるエラーを回避するために空きスペースを能動的に管理する必要があります。

シンプロビジョニングボリュームでスペースリザーブなしのファイルまたはスペースリザーブなしの LUN を設定するには、次の設定が必要です。

音量設定	価値
保証	なし
フラクショナルリザーブ	0
Snapshot リザーブ	任意
Snapshot の自動削除	任意。
自動拡張	任意。

ファイルまたは <b>LUN</b> の設定	価値
スペースリザーベーション	無効

その他の考慮事項については

ボリュームまたはアグリゲートのスペースが不足すると、ファイルまたは LUN への書き込み処理が失敗する場合があります。

ボリュームとアグリゲートの両方の空きスペースを能動的に監視しない場合は、ボリュームの自動拡張を有効にして、ボリュームの最大サイズをアグリゲートのサイズに設定してください。この設定では、アグリゲートの空きスペースを能動的に監視する必要がありますが、ボリュームの空きスペースを監視する必要はありません。

スペースリザーブファイルまたはスペースリザーブ **LUN** とセミシックボリュームプロビジョニングを組み合わせた場合の構成設定

この FlexVol とファイルまたは LUN の設定の組み合わせでは、フルプロビジョニングとの組み合わせに比べて事前に割り当てるストレージが少なくても済みますが、ボリュームに使用できる効率化テクノロジーが制限されます。この設定の組み合わせでは、上書きがベストエフォートベースで行われます。

セミシックプロビジョニングを使用するボリュームでスペースリザーブ LUN を設定するには、次の設定が必要です。

音量設定	価値
保証	ボリューム
フラクショナルリザーブ	0
Snapshot リザーブ	0
Snapshot の自動削除	オン。この場合、コミットメントレベルを destroy に設定し、削除リストにすべてのオブジェクトを追加し、トリガーを volume に設定し、すべての FlexClone LUN と FlexClone ファイルの自動削除を有効にします。
自動拡張	オプション。有効にした場合は、アグリゲートの空きスペースを能動的に監視する必要があります。

ファイルまたは <b>LUN</b> の設定	価値
スペースリザーベーション	有効

テクノロジーの制限事項

この設定の組み合わせでは、次のボリュームの Storage Efficiency テクノロジーを使用できません。

- 圧縮
- 重複排除

- ODX コピーオフロードと FlexClone コピーオフロード
- 自動削除の対象としてマークされていない FlexClone LUN と FlexClone ファイル（アクティブクローン）
- FlexClone サブファイル
- ODX / コピーオフロード

その他の考慮事項については

この設定の組み合わせを使用する場合は、次の点を考慮する必要があります。

- 対象の LUN をサポートするボリュームのスペースが不足した場合は、保護データ（FlexClone LUN、FlexClone ファイル、および Snapshot コピー）が削除されます。
- ボリュームの空きスペースが不足すると、書き込み処理がタイムアウトして失敗することがあります。

AFF プラットフォームではデフォルトで圧縮が有効になります。AFF プラットフォームのセミシックプロビジョニングを使用するボリュームに対しては、明示的に圧縮を無効にする必要があります。

## ファイルおよびディレクトリの容量を変更する際の注意事項および考慮事項

### FlexVol ボリューム上で許可される最大ファイル数の変更に関する考慮事項

FlexVol には、収容可能なファイルの最大数があります。ボリュームに収容可能なファイルの最大数は変更できますが、その前に、この変更がボリュームにどのような影響を及ぼすかを理解しておく必要があります。

データが膨大な数のファイルまたは大容量のディレクトリを必要とする場合、ONTAP のファイル容量またはディレクトリ容量を拡張できます。ただし、これらの容量を拡張する前に、制限事項と注意事項を理解しておく必要があります。

ボリュームに含めることができるファイル数は、ボリューム内の inode の数によって決まります。a\_inode\_ は ' ファイルに関する情報を含むデータ構造ですボリュームには、プライベート inode とパブリック inode の両方があります。パブリック inode はユーザーに表示されるファイルで使用され、プライベート inode は ONTAP で内部的に使用されるファイルで使用されます。変更できるのは、ボリュームのパブリック inode の最大数のみです。プライベート inode の数は変更できません。

ONTAP は、ボリュームサイズに基づいて、新しく作成するボリュームのパブリック inode の最大数をボリュームサイズ 32KB あたり 1 個の inode に自動的に設定します。管理者によって直接、または ONTAP のオートサイズ機能を通じてボリュームのサイズが拡張された場合、ボリュームサイズが 32KB あたり少なくとも 1 個の inode を確保するために、ONTAP は必要に応じてパブリック inode の最大数も引き上げます。ボリュームのサイズが約 680GB に達するまで。

ONTAP 9.13.1 より前のバージョンでは、ボリュームのサイズを 680GB よりも大きくしても、ONTAP では 22、369、621 個を超える inode は自動的に作成されないため、inode は増えません。ボリュームサイズに対するデフォルト数を超えるファイルが必要な場合は、volume modify コマンドを使用してボリュームの最大 inode 数を増やすことができます。

ONTAP 9.13.1 以降では、inode の最大数は引き続き増加するため、ボリュームが 680GB を超えていても、32KB のボリュームスペースにつき inode が 1 つになります。この増加は、ボリュームが inode の最大値である 2、147、483,632 に達するまで続きます。

パブリック inode の最大数は削減することもできます。パブリックinodeの数を減らすと、inodeに割り当てられるスペースの量は変化しますが、パブリックinodeファイルが消費できるスペースの最大量は減少します。inode用に割り当てられたスペースがボリュームに戻されることはありません。したがって、inodeの最大数を現在割り当てられているinodeの数より少なくしても、割り当てられているinodeで使用されているスペースは返されません。

#### 詳細情報

- [ファイルまたは inode の使用量を表示します](#)

#### FlexVol ボリュームの最大ディレクトリサイズを増やす場合の注意事項

特定のFlexVol ボリュームのデフォルトの最大ディレクトリサイズは、を使用して増やすことができます `-maxdir-size` のオプション `volume modify` コマンドですが、実行するとシステムのパフォーマンスに影響する可能性があります。サポート技術情報の記事を参照してください ["maxdirsizeは何ですか？"](#)。

FlexVol ボリュームのモデルごとに異なる最大ディレクトリサイズの詳細については、を参照してください ["NetApp Hardware Universe の略"](#)。

#### ノードのルートボリュームとルートアグリゲートに関するルール

ノードのルートボリュームには、そのノードの特別なディレクトリとファイルが格納されています。ルートボリュームはルートアグリゲートに含まれています。ノードのルートボリュームとルートアグリゲートには、いくつかのルールが適用されます。

ノードのルートボリュームは、工場出荷時またはセットアップソフトウェアによってインストールされた FlexVol ボリュームです。システムファイル、ログファイル、コアファイル用に予約されています。ディレクトリ名は `/mroot` にアクセスします。これには、テクニカルサポートがシステムシェルからのみアクセスできます。ノードのルートボリュームの最小サイズは、プラットフォームモデルによって異なります。

- ノードのルートボリュームには次のルールが適用されます。
  - テクニカルサポートから指示がないかぎり、ルートボリュームの構成またはコンテンツを変更しないでください。
  - ユーザーデータはルートボリュームに格納しないでください。

ユーザーデータをルートボリュームに格納すると、HA ペアのノード間でのストレージのギブバックに時間がかかります。

- ルートボリュームを別のアグリゲートに移動できます。

#### ["新しいアグリゲートへのルートボリュームの再配置"](#)

- ルートアグリゲートは、ノードのルートボリューム専用になります。

ONTAP では、ルートアグリゲートに他のボリュームを作成することはできません。

["NetApp Hardware Universe の略"](#)

ルートボリュームを新しいアグリゲートに再配置します

ルート交換手順は、現在のルートアグリゲートをシステム停止なしで別のディスクセットに移行します。

このタスクについて

次のシナリオで、ルートボリュームの場所を新しいアグリゲートに変更できます。

- ルートアグリゲートが希望するディスク上にない場合
- ノードに接続されているディスクの配置を変更する場合
- EOS ディスクシェルフを交換する場合

手順

1. ルートアグリゲートを再配置します。

```
system node migrate-root -node node_name -disklist disk_list -raid-type  
raid_type
```

- \* -node \*

移行するルートアグリゲートを所有しているノードを指定します。

- \* -disklist \*

新しいルートアグリゲートを作成するディスクのリストを指定します。すべてのディスクはスペアであり、同じノードが所有している必要があります。必要なディスクの最小数は RAID タイプによって異なります。

- \* -raid-type \*

ルートアグリゲートの RAID タイプを指定します。デフォルト値は `raid-dp`。advanced モードでは、このタイプのみがサポートされます。

2. ジョブの進捗状況を監視します。

```
job show -id jobid -instance
```

結果

すべての事前確認が完了すると、ルートボリューム交換ジョブが開始されてコマンドが終了します。

## FlexClone ファイルと FlexClone LUN でサポートされる機能

**FlexClone** ファイルと **FlexClone LUN** でサポートされる機能

FlexClone ファイルと FlexClone LUN は、重複排除、Snapshot コピー、クォータ、Volume SnapMirror などのさまざまな ONTAP 機能と相互運用できます。

FlexClone ファイルと FlexClone LUN では、次の機能がサポートされます。

- 重複排除
- Snapshot コピー
- アクセス制御リスト
- クォータ
- FlexClone ボリューム
- NDMP
- Volume SnapMirror の略
- 。 volume move コマンドを実行します
- スペースリザベーション
- HA構成

### 重複排除機能と **FlexClone** ファイルおよび **FlexClone LUN** との相互運用性

データブロックの物理ストレージスペースは、重複排除が有効なボリュームで親ファイルの FlexClone ファイルまたは親 LUN の FlexClone LUN を作成することによって効率的に使用できます。

FlexClone ファイルおよび FlexClone LUN で使用されるブロック共有メカニズムは、重複排除でも使用されます。ボリュームで重複排除を有効にし、重複排除が有効になったボリュームをクローニングすると、FlexVol で最大限のスペースを節約できます。



を実行しているとき `sis undo` 重複排除が有効なボリュームに対してコマンドを実行した場合、そのボリュームに存在する親ファイルおよび親 LUN の FlexClone ファイルおよび FlexClone LUN は作成できません。

### Snapshot コピーと **FlexClone** ファイルおよび **FlexClone LUN** との相互運用性

FlexClone ファイルと FlexClone LUN は、FlexVol に含まれる親ファイルと親 LUN の既存の Snapshot コピーから作成できます。

ただし、Snapshot コピーから FlexClone ファイルまたは FlexClone LUN を作成しているとき、親とクローンの間のブロック共有処理が完了するまでは、Snapshot コピーを手動で削除することはできません。Snapshot コピーは、バックグラウンドで実行されているブロック共有処理が完了するまで、ロックされたままです。したがって、ロックされている Snapshot コピーを削除しようとすると、しばらくしてから処理を再試行するように求めるメッセージが表示されます。その場合、特定の Snapshot コピーを手動で削除するには、再試行を繰り返して、ブロック共有が完了した時点で Snapshot コピーが削除されるようにする必要があります。

### **FlexClone** ファイルおよび **FlexClone LUN** でのアクセス制御リストの処理

FlexClone ファイルと FlexClone LUN は、親ファイルおよび親 LUN のアクセス制御リストを継承します。

親ファイルに Windows NT ストリームが含まれている場合、FlexClone ファイルもそのストリーム情報を継承します。ただし、6 個を超えるストリームを含む親ファイルはクローニングできません。

## クォータと FlexClone ファイルおよび FlexClone LUN との相互運用性

クォータ制限は、FlexClone ファイルまたは FlexClone LUN の合計論理サイズに適用されます。ブロック共有によってクォータが超過する場合でも、クローニング処理でブロック共有が停止されることはありません。

FlexClone ファイルまたは FlexClone LUN を作成した場合、クォータではスペース削減量が認識されません。たとえば、10GB の親ファイルの FlexClone ファイルを作成した場合、使用される物理スペースは 10GB ですが、クォータ利用率は 20GB（親は 10GB、FlexClone ファイルは 10GB）と記録されます。

FlexClone ファイルまたは FlexClone LUN を作成するとグループクォータまたはユーザクォータを超過する場合、FlexVol にクローンのメタデータを保管できるだけの十分なスペースがあれば、クローンの操作は成功します。ただし、そのユーザまたはグループのクォータはオーバーサブスクライブになります。

## FlexClone ボリュームと FlexClone ファイルおよび FlexClone LUN との相互運用性

FlexClone ファイルおよび FlexClone LUN とその親ファイルまたは親 LUN の両方を含む FlexVol ボリュームの、FlexClone ボリュームを作成できます。

FlexClone ボリューム内に存在する FlexClone ファイルまたは FlexClone LUN とそれらの親ファイルまたは親 LUN は、親 FlexVol ボリューム内と同じ方法で引き続きブロックを共有します。実際、すべての FlexClone エンティティとそれらの親は、基盤となる同じ物理データブロックを共有するため、物理ディスクスペース使用量が最小限に抑えられます。

FlexClone ボリュームを親ボリュームからスプリットすると、FlexClone ファイルまたは FlexClone LUN とそれらの親ファイルまたは親 LUN は、FlexClone ボリュームのクローン内のブロックを共有しなくなります。以降は独立したファイルまたは LUN となります。つまり、ボリュームのクローンはスプリット前よりも多くのスペースを使用します。

## NDMP による FlexClone ファイルおよび FlexClone LUN の処理

NDMP は、論理レベルで FlexClone ファイルおよび FlexClone LUN に影響を与えます。すべての FlexClone ファイルまたは FlexClone LUN は、独立したファイルまたは LUN としてバックアップされます。

NDMP サービスを使用して FlexClone ファイルまたは FlexClone LUN を含む qtree または FlexVol をバックアップする場合、親エンティティとクローンエンティティの間のブロック共有は維持されず、クローンエンティティは独立したファイルまたは LUN としてテープにバックアップされます。スペースの削減は失われます。したがって、バックアップ先のテープには、拡張された分のデータを格納できるだけの十分なスペースが必要です。リストア時には、すべての FlexClone ファイルおよび FlexClone LUN は独立した物理ファイルおよび LUN としてリストアされます。ボリュームで重複排除を有効にすると、ブロック共有のメリットを復元できます。



FlexVol の既存の Snapshot コピーから FlexClone ファイルと FlexClone LUN が作成されている間は、バックグラウンドのブロック共有プロセスが完了するまではボリュームをテープにバックアップすることはできません。ブロック共有プロセスの進行中にボリューム上の NDMP を使用すると、しばらくしてから処理を再試行するように求めるメッセージが表示されます。その場合、再試行を繰り返して、ブロック共有が完了した時点でテープバックアップ処理が実行されるようにする必要があります。

## Volume SnapMirror と FlexClone ファイルおよび FlexClone LUN との相互運用性

クローニングされたエンティティは一度しか複製されないため、Volume SnapMirror と FlexClone ファイルおよび FlexClone LUN を併用すると、継続的にスペースを節約しやすくなります。

FlexVol ボリュームが Volume SnapMirror ソースで、FlexClone ファイルまたは FlexClone LUN を含んでいる場合、Volume SnapMirror は共有物理ブロックと少量のメタデータのみを Volume SnapMirror デスティネーションに転送します。デスティネーションでは物理ブロックのコピーが 1 つだけ保存され、このブロックが親エンティティとクローニングされたエンティティとの間で共有されます。したがって、デスティネーションボリュームはソースボリュームの正確なコピーであり、デスティネーションボリューム上のすべてのクローンファイルまたはクローン LUN は同じ物理ブロックを共有します。

ボリューム移動が **FlexClone** ファイルと **FlexClone LUN** に及ぼす影響

ボリューム移動処理のカットオーバーフェーズ中は、FlexVol ボリュームの FlexClone ファイルまたは FlexClone LUN を作成することはできません。

## スペースリザベーションと **FlexClone** ファイルおよび **FlexClone LUN** との相互運用性

FlexClone ファイルと FlexClone LUN は、デフォルトでは親ファイルおよび親 LUN のスペースリザベーション属性を継承します。ただし、FlexClone ファイルと FlexClone LUN の作成時に、親ファイルおよび親 LUN でスペースリザベーションを有効にした状態で、FlexVol ボリュームに十分なスペースがない場合はスペースリザベーションを無効にすることができます。

親と同じスペースリザベーションが設定された FlexClone ファイルまたは FlexClone LUN を作成できるだけのスペースが FlexVol にない場合、クローニング処理は失敗します。

## HA 構成と **FlexClone** ファイルおよび **FlexClone LUN** との相互運用性

FlexClone ファイルと FlexClone LUN の操作は、HA 構成でサポートされています。

HA ペアでは、テイクオーバー処理またはギブバック処理が進行している間は、パートナー上に FlexClone ファイルまたは FlexClone LUN を作成できません。パートナー上の保留されたブロック共有処理はすべて、テイクオーバー処理またはギブバック処理が完了したあと再開されます。

## FlexGroup を使用して大規模ファイルシステム用の **NAS** ストレージをプロビジョニング

FlexGroup ボリュームは拡張性に優れた NAS コンテナで、ハイパフォーマンスと自動負荷分散を実現します。FlexGroup ボリュームは、FlexVol の制限をはるかに超える大容量（ペタバイト単位）を提供し、管理オーバーヘッドを発生させることはありません。

このセクションのトピックでは、ONTAP 9.7 以降のリリースで System Manager を使用して FlexGroup ボリュームを管理する方法を説明します。従来の System Manager（ONTAP 9.7 以前でのみ使用可能）を使用している場合は、次のトピックを参照してください。



- "FlexGroup ボリュームを作成します"

ONTAP 9.9.1以降では、2つ以上のFlexGroup のSnapMirrorファンアウト関係（最大8つのファンアウトレグ）がサポートされます。System Manager では、 SnapMirror カスケード FlexGroup ボリューム関係はサポートされません。

ONTAP は、 FlexGroup ボリュームの作成に必要なローカル階層を自動的に選択します。

ONTAP 9.8 以降では、ストレージをプロビジョニングすると QoS がデフォルトで有効になります。QoS を無効にするか、プロビジョニングプロセス中またはあとからカスタムの QoS ポリシーを選択できます。

#### 手順

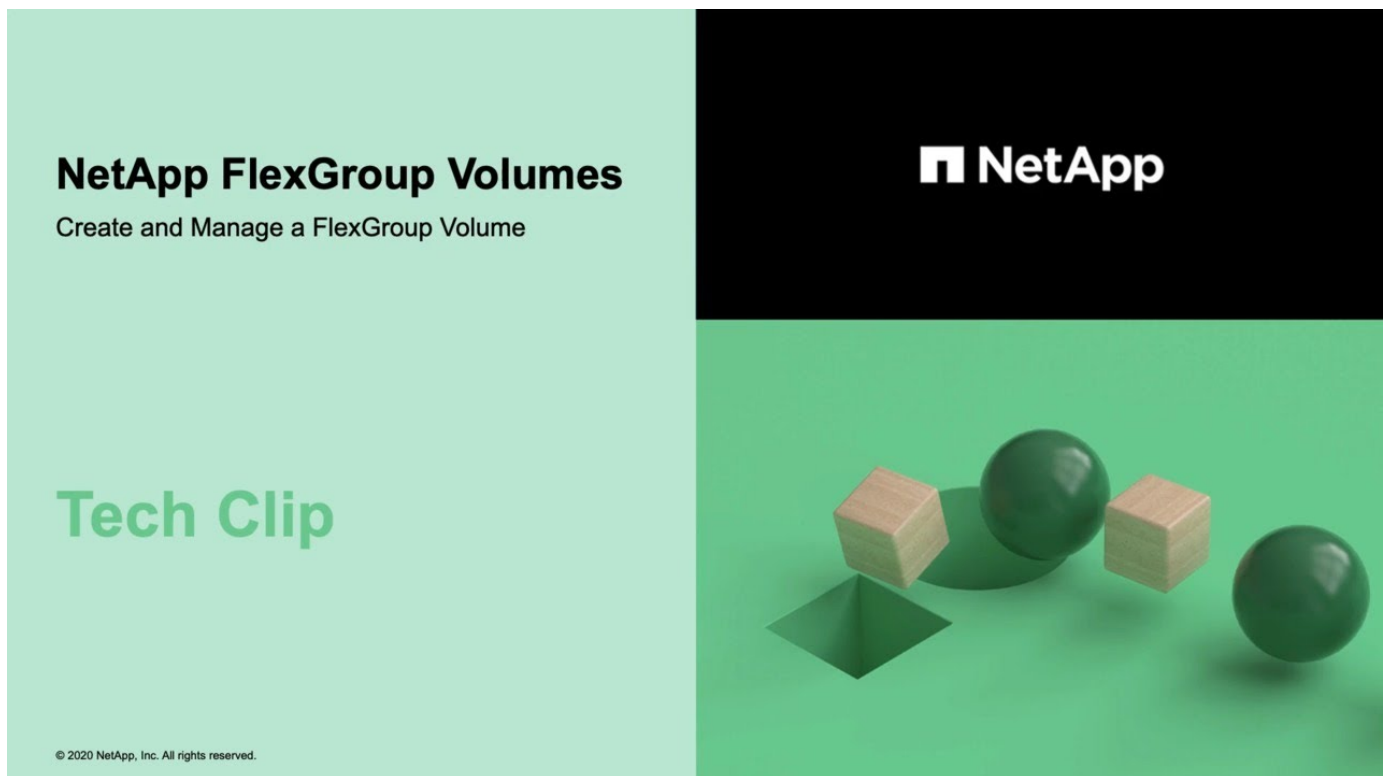
1. [ ストレージ ]、[ ボリューム ] の順にクリックします。
2. [ 追加（Add） ] をクリックします。
3. [ \* その他のオプション \* ] をクリックし、 [ \* ボリュームデータをクラスタに分散する \* ] を選択します。



ONTAP 9.8以降を実行していて、QoSを無効にするかカスタムQoSポリシーを選択する場合は、【その他のオプション】\*をクリックし、【ストレージと最適化】で【パフォーマンスサービスレベル】\*を選択します。

#### ビデオ

**FlexGroup** ボリュームを作成および管理します





## FlexGroup ボリュームの管理には CLI を使用します

### CLI での FlexGroup ボリューム管理の概要

拡張性とパフォーマンスを確保するために、FlexGroup ボリュームをセットアップ、管理、および保護することができます。FlexGroup ボリュームは、ハイパフォーマンスと自動負荷分散を実現するスケールアウトボリュームです。

次の条件に該当する場合は、FlexGroup ボリュームを設定できます。

- ONTAP 9.1以降を実行している。
- NFSv4.x、NFSv3、SMB 2.0、または SMB 2.1 を使用する。
- System Manager や自動スクリプトツールではなく、ONTAP コマンドラインインターフェイス（CLI）を使用する必要がある。

コマンド構文の詳細については、CLI のヘルプと ONTAP のマニュアルページを参照してください。

FlexGroup の重要な機能は System Manager で実行できます。

- すべての選択肢について検討するのではなく、ベストプラクティスに従う。
- SVM 管理者権限ではなくクラスタ管理者権限を持っている。



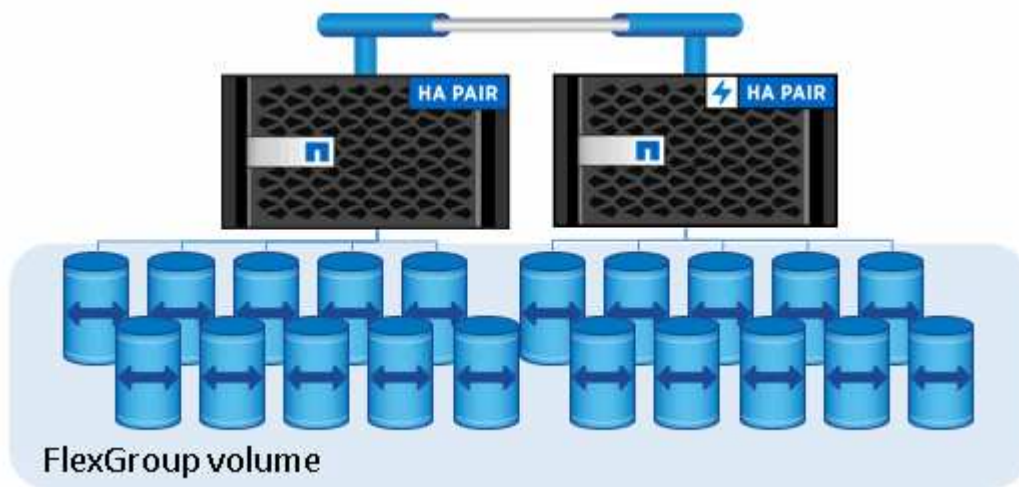
ONTAP 9.5以降では、ONTAP 9.5以降のリリースではサポートされていないInfinite Volume がFlexGroupに置き換えられます。

## 関連情報

FlexVol ボリュームの基本的な概念については、FlexGroup ボリュームを参照してください。FlexVol ボリュームおよび ONTAP テクノロジーの情報については、ONTAP リファレンスライブラリおよびテクニカルレポート (TR) を参照してください。

## FlexGroup ボリュームとは

FlexGroup ボリュームは、ハイパフォーマンスと自動負荷分散を実現する、拡張性を備えたスケールアウト NAS コンテナです。FlexGroup ボリュームには、自動的かつ透過的にトラフィックを共有する複数のコンスティチュエントが含まれます。`_constituents_` は、FlexGroup ボリュームを構成する基盤となる FlexVol ボリュームです。



FlexGroup ボリュームには次の利点があります。

- 高い拡張性

ONTAP 9.1 以降では、FlexGroup ボリュームの最大サイズは 20PB で、10 ノードのクラスタにファイルを 4、000 億個まで格納できます。

- ハイパフォーマンス

FlexGroup ボリュームは、クラスタのリソースを利用してワークロードに対応することで高スループットと低レイテンシを実現します。

- 管理の簡易化

FlexGroup ボリュームは、FlexVol と同様に管理できる単一のネームスペースコンテナです。

## FlexGroup ボリュームでサポートされる構成とされない構成

ONTAP 9 の FlexGroup でサポートされる ONTAP 機能とサポートされない機能を確認しておく必要があります。

### ONTAP 9.14.1以降でサポートされる機能

- Snapshotコピーのタグ付け：を使用したFlexGroupボリュームでのSnapshotコピーのSnapshotコピータグ（SnapMirrorラベルとコメント）の作成、変更、および削除のサポート volume snapshot コマンドを実行します

### ONTAP 9.13.1以降でサポートされる機能

- FlexGroupボリューム向けのAutonomous Ransomware Protection（ARP；自律ランサムウェア対策）。サポートされる次の機能が含まれます。
  - FlexGroupの拡張処理：新しいコンスチチュエントは、Autonomous Ransomware Protectionの属性を継承します。
  - FlexVolからFlexGroupへの変換：自律型ランサムウェア対策が有効なFlexVolを変換できます。
  - FlexGroupのリバランシング：自律型ランサムウェア対策は、システムの停止を伴うリバランシング処理と無停止のリバランシング処理でサポートされます。
- 単一のFlexGroupリバランシング処理をスケジュールします。
- FlexGroup上のSVM DRとのSnapMirrorファンアウト関係。8つのサイトへのファンアウトをサポートします。

### ONTAP 9.12.1以降でサポートされる機能

- FlexGroup のリバランシング
- SnapLock for SnapVault の略
- FabricPool、FlexGroup、SVM DRが連携して動作する。（ONTAP 9.12.1より前のリリースでは、これらの機能のうちいずれか2つが連動していましたが、3つすべてが連動しているわけではありません）。
- ONTAP 9.12.1 P2以降を使用している場合、AFFおよびFASプラットフォームのFlexGroupボリュームコンスチチュエントサイズは最大300TBです。

### ONTAP 9.11.1以降でサポートされる機能

- SnapLock ボリューム

SnapLock では、FlexGroup ボリュームの次の機能はサポートされません。

- リーガルホールド
- イベントベースの保持
- SnapLock for SnapVault の略

SnapLock はFlexGroup レベルで設定します。SnapLock をコンスチチュエントレベルで設定することはできません。

### SnapLock とは

- クライアントの非同期ディレクトリの削除

ディレクトリを迅速に削除するためのクライアント権限を管理します

### ONTAP 9.10.1 以降でサポートされる機能

- SVM-DR ソースで FlexVol ボリュームを FlexGroup ボリュームに変換します

[FlexGroup ボリュームを SVM-DR 関係内で FlexVol ボリュームに変換します](#)

- FlexGroup ボリュームに対する SVM DR FlexClone のサポート

[FlexClone ボリュームの作成に関する詳細情報](#)

### ONTAP 9.9.1 以降でサポートされる機能

- SVM ディザスタリカバリ

SVM-DR 関係に含まれている FlexGroup ボリュームのクローニングはサポートされません。

- 2 つ以上（A から B、A から C）の SnapMirror ファンアウト関係。ファンアウト関係の最大数は 8 です。

[FlexGroup の SnapMirror カスケード関係とファンアウト関係の作成に関する考慮事項](#)

- 最大 2 つのレベル（A ~ B ~ C）の SnapMirror カスケード関係

[FlexGroup の SnapMirror カスケード関係とファンアウト関係の作成に関する考慮事項](#)

### ONTAP 9.8 以降でサポートされている機能

- FlexGroup の SnapMirror バックアップまたは UDP デスティネーションからの単一ファイルのリストア
  - 任意の形状の FlexGroup ボリュームから任意の形状の FlexGroup ボリュームへのリストアが可能です
  - リストア処理ごとに 1 つのファイルのみがサポートされます
- 7-Mode システムから FlexGroup ボリュームに移行したボリュームの変換

詳細については、技術情報アートを参照してください "[移行した FlexVol を FlexGroup に変換する方法](#)"。

- NFSv4.2
- ファイルとディレクトリの非同期削除
- FSA（ファイルシステム分析）
- VMware vSphere データストアとしての FlexGroup
- NDMP を使用したテープバックアップおよびリストアのサポートが追加されました。次の機能が含まれます。
  - NDMP の Restartable Backup Extension（RBE）および Snapshot Management Extension（SSME）
  - 環境変数 EXCLUDE および MULTI\_SUBTREE\_NAMES は FlexGroup バックアップをサポートします
  - FlexGroup バックアップ用の IGNORE\_CTH\_mtime 環境変数が導入されました
  - NDMP\_SNAP\_RECOVER メッセージ（拡張機能 0x2050 の一部）を使用した FlexGroup での個々のフ

ファイルリカバリ

アップグレードまたはリバートの実行中にダンプセッションとリストアセッションが中止されます。

### ONTAP 9.7 以降でサポートされる機能

- FlexClone ボリューム
- NFSv4およびNFSv4.1
- pNFS
- NDMP を使用したテープバックアップおよびリストア

FlexGroup ボリュームでの NDMP のサポートについては、次の点に注意する必要があります。

- 拡張クラス 0x2050 の NDMP\_SNAP\_RECOVER メッセージは、FlexGroup ボリューム全体のリカバリにのみ使用できます。

FlexGroup ボリューム内の個々のファイルはリカバリできません。

- FlexGroup ボリュームでは、NDMP の Restartable Backup Extension (RBE) はサポートされません。
- 環境変数 EXCLUDE および MULTI\_SUBTREE\_NAMES は、FlexGroup ボリュームではサポートされません。
- `ndmpcopy` コマンドは、FlexVol ボリュームとFlexGroup ボリュームの間のデータ転送に対応しています。

Data ONTAP 9.7 から以前のバージョンにリバートした場合、以前の転送の差分転送情報は保持されないため、リバート後にベースラインコピーを実行する必要があります。

- VMware vStorage APIs for Array Integration (VAAI)
- FlexVol ボリュームから FlexGroup ボリュームへの変換
- FlexGroup ボリュームを FlexCache の元のボリュームとして使用する

### ONTAP 9.6以降でサポートされる機能

- 継続的可用性を備えた SMB 共有
- MetroCluster 構成
- FlexGroup ボリュームの名前を変更しています (`volume rename` コマンド)
- FlexGroup ボリュームのサイズを縮小または縮小します (`volume size` コマンド)
- エラスティックサイジング
- NetApp Aggregate Encryption (NAE)
- Cloud Volumes ONTAP

### ONTAP 9.5以降でサポートされる機能

- ODX コピーオフロード
- ストレージレベルのアクセス保護

- SMB 共有の変更通知の機能拡張

変更通知は、が置かれている親ディレクトリに対する変更について送信されます `changenotify` プロパティは、その親ディレクトリ内のすべてのサブディレクトリに対する変更に対して設定されます。

- FabricPool
- クォータの適用
- qtree の統計
- FlexGroup ボリューム内のファイルに対するアダプティブ QoS
- FlexCache（キャッシュのみ。ONTAP 9.7 では FlexGroup が送信元としてサポートされます）

#### ONTAP 9.4以降でサポートされる機能

- FPolicy の
- ファイル監査
- FlexGroup ボリュームのスループットの下限（最小 QoS）とアダプティブ QoS
- FlexGroup ボリューム内のファイルに対するスループットの上限（最大 QoS）と下限（最小 QoS）

を使用します `volume file modify` コマンドを使用して、ファイルに関連付けられている QoS ポリシーグループを管理します。

- SnapMirror の制限を緩和
- SMB 3.x マルチチャネル

#### ONTAP 9.3以降でサポートされる機能

- ウィルス対策の設定
- SMB 共有の変更通知

通知は、が置かれている親ディレクトリに対する変更についてのみ送信されます `changenotify` プロパティが設定されます。親ディレクトリのサブディレクトリに対する変更については送信されません。

- qtree
- スループットの上限（最大 QoS）
- SnapMirror 関係にあるソース FlexGroup ボリュームとデスティネーション FlexGroup ボリュームを拡張します
- SnapVault のバックアップとリストア
- 一元化されたデータ保護関係
- 自動拡張オプションと自動縮小オプション
- 取り込みで考慮される inode 数

#### ONTAP 9.2 以降でサポートされる機能です

- ボリューム暗号化

- アグリゲートインライン重複排除（ボリューム間重複排除）
- NetApp Volume Encryption （ NVE ）

## ONTAP 9.1以降でサポートされる機能

FlexGroup ボリュームは ONTAP 9.1 で導入された機能で、 ONTAP のいくつかの機能がサポートされます。

- SnapMirror テクノロジ
- Snapshot コピー
- Active IQ
- インラインアダプティブ圧縮
- インライン重複排除
- インラインデータコンパクション
- AFF
- クォータレポート
- NetApp Snapshot テクノロジ
- SnapRestore ソフトウェア（ FlexGroup レベル）
- ハイブリッドアグリゲート
- コンスティチュエントまたはメンバーボリュームの移動
- ポストプロセスの重複排除
- NetApp RAID-TEC テクノロジ
- アグリゲートごとの整合ポイント
- 同じ SVM 内の FlexVol ボリュームと FlexGroup を共有する

## ONTAP 9 でサポートされない構成です

サポート対象外のプロトコルです	サポートされていないデータ保護機能です	サポートされないその他の ONTAP 機能
<ul style="list-style-type: none"> <li>• pNFS （ ONTAP 9.0 から 9.6 ）</li> <li>• SMB 1.0</li> <li>• SMB 透過的フェイルオーバー（ ONTAP 9.0 から 9.5 ）</li> <li>• SAN</li> </ul>	<ul style="list-style-type: none"> <li>• SnapLock ボリューム（ ONTAP 9.10.1以前）</li> <li>• SMTape の場合</li> <li>• 同期SnapMirror</li> <li>• FabricPoolを含むFlexGroup を備えたSVM DR</li> </ul>	<ul style="list-style-type: none"> <li>• リモートの Volume Shadow Copy Service （ VSS ； ボリュームシャドウコピーサービス）</li> <li>• SVM のデータ移動</li> </ul>

## 関連情報

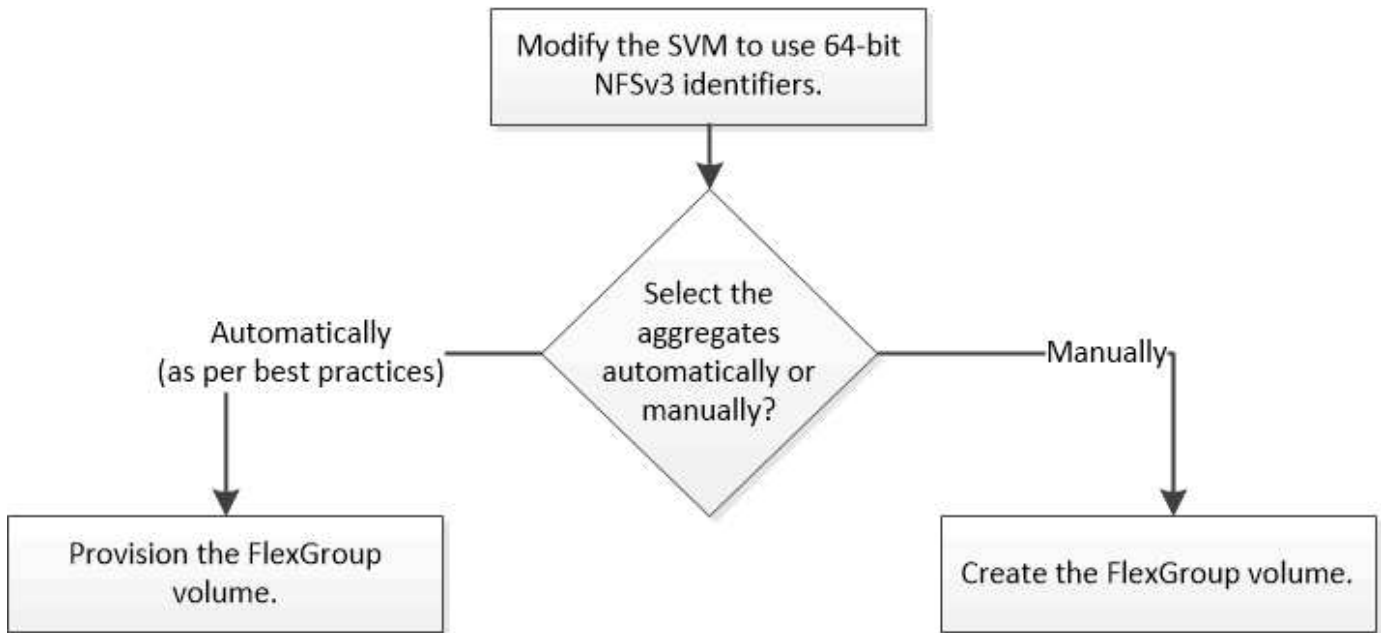
["ONTAP 9 ドキュメンテーション・センター"](#)



## FlexGroup ボリュームのセットアップ

### FlexGroup ボリュームのセットアップワークフロー

最適なパフォーマンスになるようにベストプラクティスに基づいてアグリゲートが ONTAP で自動的に選択されるように FlexGroup ボリュームをプロビジョニングするか、アグリゲートを手動で選択してデータアクセスを設定することで FlexGroup ボリュームを作成することができます。



#### 必要なもの

SVM を作成し、SVM で許可されるプロトコルの一覧に NFS および SMB を追加しておく必要があります。

#### このタスクについて

FlexGroup ボリュームの自動プロビジョニングは、4 ノード以下のクラスタでのみ実行できます。ノード数がそれより多いクラスタでは、FlexGroup ボリュームを手動で作成する必要があります。

#### SVM で 64 ビットの NFSv3 ID を有効にします

FlexGroup ボリュームの大量のファイルをサポートし、ファイル ID の競合を防ぐためには、FlexGroup ボリュームを作成する必要がある SVM で 64 ビットのファイル ID を有効にします。

#### 手順

1. advanced 権限レベルにログインします。 `set -privilege advanced`
2. 64ビットのNFSv3 FSIDとファイルIDを使用するようにSVMを変更します。 `vserver nfs modify -vserver svm_name -v3-64bit-identifiers enabled`

```
cluster1::*> vsriver nfs modify -vsriver vs0 -v3-64bit-identifiers
enabled

Warning: You are attempting to increase the number of bits used for
NFSv3
        FSIIDs and File IDs from 32 to 64 on Vserver "vs0". This could
        result in older client software no longer working with the
volumes
        owned by Vserver "vs0".
Do you want to continue? {y|n}: y

Warning: Based on the changes you are making to the NFS server on
Vserver
        "vs0", it is highly recommended that you remount all NFSv3
clients
        connected to it after the command completes.
Do you want to continue? {y|n}: y
```

完了後

すべてのクライアントを再マウントする必要があります。これは、ファイルシステム ID が変わるため、クライアントが NFS 処理を試みたときに stale file handle メッセージが表示される可能性があるためです。

### FlexGroup ボリュームを自動的にプロビジョニング

FlexGroup ボリュームは自動的にプロビジョニングできます。ONTAP でアグリゲートが自動的に選択され、FlexGroup ボリュームが作成されて設定されます。アグリゲートは、最適なパフォーマンスになるようにベストプラクティスに基づいて選択されます。

必要なもの

クラスタの各ノードにアグリゲートが少なくとも 1 つ必要です。



ONTAP 9.5 で FabricPool 用の FlexGroup ボリュームを作成するには、各ノードに FabricPool であるアグリゲートが少なくとも 1 つ必要です。


このタスクについて

ONTAP は、各ノードから使用可能なスペースが大きい順に 2 つのアグリゲートを選択して FlexGroup ボリュームを作成します。使用可能なアグリゲートが 2 つない場合、ONTAP はノードごとに 1 つのアグリゲートを選択して FlexGroup ボリュームを作成します。

手順

1. FlexGroup ボリュームをプロビジョニングします。

使用するポート	使用するコマンド
---------	----------

<p>ONTAP 9.2以降</p>	<pre>volume create -vserver svm_name -volume fg_vol_name -auto-provision-as flexgroup -size fg_size [-encrypt true] [-qos-policy-group qos_policy_group_name] [-support- tiering true]</pre> <p>ONTAP 9.5以降では、FabricPool 用のFlexGroup ボリュームを作成できます。FabricPool でFlexGroup ボリュームを自動的にプロビジョニングするには、を設定する必要があります <code>-support-tiering</code> パラメータの値 <code>true</code>。ボリュームギャランティは常にに設定する必要があります <code>none</code> FabricPool の場合。FlexGroup ボリュームには、階層化ポリシーと階層化の最小クーリング期間も指定できます。</p> <p>"ディスクおよびアグリゲートの管理"</p> <p>ONTAP 9.3 以降では、FlexGroup ボリュームにスループットの上限（最大 QoS）を指定して、FlexGroup ボリュームが消費できるパフォーマンスリソースを制限できます。ONTAP 9.4 以降では、FlexGroup ボリュームにスループットの下限（最小 QoS）とアダプティブ QoS を指定できます。</p> <p>"パフォーマンス管理"</p> <p>ONTAP 9.2以降では、を設定できます <code>-encrypt</code> パラメータの値 <code>true</code> FlexGroup ボリュームで暗号化を有効にする場合。暗号化されたボリュームを作成するには、ボリューム暗号化ライセンスとキー管理ツールをインストールしておく必要があります。</p> <div>  <p>暗号化は FlexGroup の作成時に有効にする必要があります。既存の FlexGroup ボリュームで暗号化を有効にすることはできません。</p> </div> <p>"保存データの暗号化"</p>
<p>ONTAP 9.1</p>	<pre>volume flexgroup deploy -vserver svm_name -size fg_size</pre>

。 `size` パラメータは、FlexGroup ボリュームのサイズ（KB、MB、GB、TB、またはPB）を指定します。

次の例は、ONTAP 9.2 で 400TB の FlexGroup ボリュームをプロビジョニングする方法を示しています。

```
cluster-1::> volume create -vserver vs0 -volume fg -auto-provision-as
flexgroup -size 400TB
Warning: The FlexGroup "fg" will be created with the following number of
constituents of size 25TB: 16.
The constituents will be created on the following aggregates:
aggr1,aggr2
Do you want to continue? {y|n}: y
[Job 34] Job succeeded: Successful
```

次の例は、スループットの上限が設定された QoS ポリシーグループを作成して FlexGroup に適用する方法を示しています。

```
cluster1::> qos policy-group create -policy group pg-vs1 -vserver vs1
-max-throughput 5000iops
```

```
cluster-1::> volume create -vserver vs0 -volume fg -auto-provision-as
flexgroup -size 400TB -qos-policy-group pg-vs1
Warning: The FlexGroup "fg" will be created with the following number of
constituents of size 25TB: 16.
The constituents will be created on the following aggregates:
aggr1,aggr2
Do you want to continue? {y|n}: y
[Job 34] Job succeeded: Successful
```

次の例は、ONTAP 9.5 の FabricPool のアグリゲートに 400TB の FlexGroup ボリュームをプロビジョニングする方法を示しています。

```
cluster-1::> volume create -vserver vs0 -volume fg -auto-provision-as
flexgroup -size 400TB -support-tiering true -tiering-policy auto
Warning: The FlexGroup "fg" will be created with the following number of
constituents of size 25TB: 16.
The constituents will be created on the following aggregates:
aggr1,aggr2
Do you want to continue? {y|n}: y
[Job 34] Job succeeded: Successful
```

クラスタの各ノードに 8 つのコンスティチュエントで構成される FlexGroup ボリュームが作成されます。コンスティチュエントは、各ノードの最も大きい 2 つのアグリゲートに均等に分散されます。

デフォルトでは、FlexGroup ボリュームはを使用して作成されます volume スペースギャランティの設定（AFF システムの場合を除く）。AFF システムの場合、デフォルトでは、FlexGroup ボリュームはを使用して作成されます none スペースギャランティ：

2. ジャンクションパスを使用してFlexGroup ボリュームをマウントします。 volume mount -vserver vserver\_name -volume vol\_name -junction-path junction\_path

```
cluster1::> volume mount -vserver vs0 -volume fg2 -junction-path /fg2
```

完了後

クライアントから FlexGroup ボリュームをマウントする必要があります。

ONTAP 9.6 以前を実行していて、Storage Virtual Machine (SVM) で NFSv3 と NFSv4 の両方が設定されている場合、クライアントからの FlexGroup ボリュームのマウントが失敗することがあります。このような場合は、クライアントから FlexGroup ボリュームをマウントする際に、NFS バージョンを明示的に指定する必要があります。

```
# mount -t nfs -o vers=3 192.53.19.64:/fg2 /mnt/fg2
# ls /mnt/fg2
file1  file2
```

## FlexGroup ボリュームを作成します

FlexGroup ボリュームを作成するアグリゲートを手動で選択し、各アグリゲートのコンスティチュエントの数を指定して、FlexGroup ボリュームを作成することができます。

このタスクについて

FlexGroup ボリュームを作成するためにアグリゲート内に必要なスペースを把握しておく必要があります。

FlexGroup ボリュームで最適なパフォーマンスを実現するには、FlexGroup ボリュームを作成する際に次のガイドラインを考慮する必要があります。

- FlexGroup ボリュームは、同一のハードウェアシステム上にあるアグリゲートでのみ構成される必要があります。

同一のハードウェアシステムを使用することで、FlexGroup ボリューム全体のパフォーマンスを予測できるようになります。

- FlexGroup ボリュームは、同じディスクタイプおよび RAID グループ構成のアグリゲートで構成される必要があります。

安定したパフォーマンスを実現するには、すべてのアグリゲートがオール SSD、オール HDD、またはオールハイブリッドアグリゲートであることが必要です。また、FlexGroup ボリュームを構成するすべてのアグリゲートでドライブ数と RAID グループ数が同じであることが必要です。

- FlexGroup ボリュームは、クラスタの一部でのみ構成することができます。

FlexGroup ボリュームをクラスタ全体にまたがるように設定する必要はありませんが、そのように設定すると、使用可能なハードウェアリソースをより有効に活用できます。

- FlexGroup ボリュームを作成する場合は、次の特性を持つアグリゲートに FlexGroup ボリュームを導入することを推奨します。

- シンプロビジョニングを使用する場合は特に、複数のアグリゲート間でほぼ同じ量の空きスペースを使用できます。
- FlexGroup ボリュームの作成後に、空きスペースの約 3% がアグリゲートメタデータ用に確保される。
- FAS システムの場合は、ノードごとに 2 つのアグリゲートを用意し、AFF システムの場合は、FlexGroup ボリュームのノードごとに 1 つのアグリゲートを用意することを推奨します。
- FlexGroup ボリュームごとに少なくとも 8 つのコンスティチュエントを作成して、FAS システムの場合は 2 つ以上のアグリゲートに、AFF システムの場合は 1 つ以上のアグリゲートに分散させる必要があります。

#### 作業を開始する前に

- ONTAP 9.13.1以降では、容量分析とアクティビティ追跡を有効にしてボリュームを作成できます。容量またはアクティビティトラッキングを有効にするには、`volume create` コマンドに `-analytics-state` または `-activity-tracking-state` を `on` に設定します。

容量分析とアクティビティ追跡の詳細については、[を参照してください](#) [File System Analytics を有効にします](#)。

#### 手順

1. FlexGroup ボリュームを作成します。
 

```
volume create -vserver svm_name -volume flexgroup_name -aggr-list aggr1,aggr2,... -aggr-list-multiplier constituents_per_aggr -size fg_size [-encrypt true] [-qos-policy-group qos_policy_group_name]
```

- 。 `-aggr-list` パラメータは、FlexGroup ボリュームのコンスティチュエントに使用するアグリゲートのリストを指定します。

指定したエントリごとに、そのアグリゲート上にコンスティチュエントが 1 つ作成されます。同じアグリゲートを複数回指定すると、そのアグリゲート上に複数のコンスティチュエントを作成できます。

FlexGroup 全体で一貫したパフォーマンスが得られるように、すべてのアグリゲートで同じディスクタイプと RAID グループ構成を使用する必要があります。

- 。 `-aggr-list-multiplier` パラメータは、に表示されるアグリゲートを反復する回数を指定します `-aggr-list` FlexGroup ボリューム作成時のパラメータ。

のデフォルト値 `-aggr-list-multiplier` パラメータは4です。

- 。 `size` パラメータは、FlexGroup ボリュームのサイズ（KB、MB、GB、TB、またはPB）を指定します。
- ONTAP 9.5 以降では、オール SSD アグリゲートのみを使用する FabricPool 用の FlexGroup ボリュームを作成できます。

FabricPool 用の FlexGroup ボリュームを作成するには、で指定したすべてのアグリゲートを指定します `-aggr-list` パラメータは FabricPool にする必要があります。ボリュームギャランティは常にに設定する必要があります `none` FabricPool の場合。FlexGroup ボリュームには、階層化ポリシーと階層化の最小クォーリング期間も指定できます。

#### [ディスクおよびアグリゲートの管理](#)

- ONTAP 9.4 以降では、FlexGroup ボリュームにスループットの下限（最小 QoS）とアダプティブ QoS を指定できます。

### "パフォーマンス管理"

- ONTAP 9.3 以降では、FlexGroup ボリュームにスループットの上限（最大 QoS）を指定して、FlexGroup ボリュームが消費できるパフォーマンスリソースを制限できます。
- ONTAP 9.2以降では、を設定できます `-encrypt` パラメータの値 `true` FlexGroup ボリュームで暗号化を有効にする場合。

暗号化されたボリュームを作成するには、ボリューム暗号化ライセンスとキー管理ツールをインストールしておく必要があります。



暗号化は FlexGroup の作成時に有効にする必要があります。既存の FlexGroup ボリュームで暗号化を有効にすることはできません。

### "保存データの暗号化"

```
cluster-1::> volume create -vserver vs0 -volume fg2 -aggr-list
aggr1,aggr2,aggr3,aggr1 -aggr-list-multiplier 2 -size 500TB

Warning: A FlexGroup "fg2" will be created with the following number of
constituents of size 62.50TB: 8.
Do you want to continue? {y|n}: y

[Job 43] Job succeeded: Successful
```

この例の場合、FabricPool 用の FlexGroup ボリュームを作成するには、すべてのアグリゲート（`aggr1`、`aggr2`、`aggr3`）が FabricPool 内のアグリゲートである必要があります。ジャンクションパスを使用して FlexGroup ボリュームをマウントします。 `volume mount -vserver vserver_name -volume vol_name -junction-path junction_path`

```
cluster1::> volume mount -vserver vs0 -volume fg2 -junction-path /fg
```

完了後

クライアントから FlexGroup ボリュームをマウントする必要があります。

ONTAP 9.6 以前を実行していて、Storage Virtual Machine（SVM）で NFSv3 と NFSv4 の両方が設定されている場合、クライアントからの FlexGroup ボリュームのマウントが失敗することがあります。このような場合は、クライアントから FlexGroup ボリュームをマウントするときに、NFS バージョンを明示的に指定する必要があります。

```
# mount -t nfs -o vers=3 192.53.19.64:/fg /mnt/fg2
# ls /mnt/fg2
file1  file2
```

## FlexGroup ボリュームを管理します

### FlexGroup ボリュームのスペース使用量を監視します

FlexGroup とそのコンスティチュエントを表示して、FlexGroup ボリュームで使用されているスペースを監視することができます。

このタスクについて

ONTAP 9.6 以降では、エラスティックサイジングがサポートされます。FlexGroup ボリュームのコンスティチュエントがスペース不足になると、空きスペースがある FlexGroup ボリュームの他のコンスティチュエントを同じ量だけ縮小することで、ONTAP によって自動的に拡張されます。エラスティックサイジングを使用すると、1 つ以上の FlexGroup コンスティチュエントボリュームのスペース不足が原因で発生するスペース不足エラーを回避できます。



ONTAP 9.9.1以降では、FlexGroup ボリュームに対して論理スペースのレポートと適用も使用できます。詳細については、を参照してください "[ボリュームの論理スペースのレポートと適用](#)"。

### ステップ

1. FlexGroup ボリュームとそのコンスティチュエントで使用されているスペースを表示します。 `volume show -vserver vs1 -volume-style-extended flexgroup`

```
cluster-2::> volume show -vserver vs1 -volume-style-extended flexgroup
Vserver   Volume      Aggregate    State      Type      Size
Available Used%
-----
vs1        fg1          -            online     RW        500GB
207.5GB   56%
```



```
ccluster-2::> volume show -vserver vs1 -volume-style-extended flexgroup-
constituent
```

Vserver	Volume	Aggregate	State	Type	Size
Available	Used%				
vs1	fg1__0001	aggr3	online	RW	31.25GB
12.97GB	56%				
vs1	fg1__0002	aggr1	online	RW	31.25GB
12.98GB	56%				
vs1	fg1__0003	aggr1	online	RW	31.25GB
13.00GB	56%				
vs1	fg1__0004	aggr3	online	RW	31.25GB
12.88GB	56%				
vs1	fg1__0005	aggr1	online	RW	31.25GB
13.00GB	56%				
vs1	fg1__0006	aggr3	online	RW	31.25GB
12.97GB	56%				
vs1	fg1__0007	aggr1	online	RW	31.25GB
13.01GB	56%				
vs1	fg1__0008	aggr1	online	RW	31.25GB
13.01GB	56%				
vs1	fg1__0009	aggr3	online	RW	31.25GB
12.88GB	56%				
vs1	fg1__0010	aggr1	online	RW	31.25GB
13.01GB	56%				
vs1	fg1__0011	aggr3	online	RW	31.25GB
12.97GB	56%				
vs1	fg1__0012	aggr1	online	RW	31.25GB
13.01GB	56%				
vs1	fg1__0013	aggr3	online	RW	31.25GB
12.95GB	56%				
vs1	fg1__0014	aggr3	online	RW	31.25GB
12.97GB	56%				
vs1	fg1__0015	aggr3	online	RW	31.25GB
12.88GB	56%				
vs1	fg1__0016	aggr1	online	RW	31.25GB
13.01GB	56%				

16 entries were displayed.

使用可能なスペースと使用済みスペースの割合の情報を使用して、FlexGroup ボリュームのスペース使用量を監視できます。

**FlexGroup ボリュームのサイズを拡張する**

FlexGroup ボリュームのサイズを拡張するには、FlexGroup の既存のコンスティチュエントに容量を追加するか、新しいコンスティチュエントを追加して FlexGroup を拡張します。

**必要なもの**

アグリゲートに十分なスペースが必要です。

**このタスクについて**

スペースをさらに追加するには、FlexGroup ボリューム全体のサイズを増やします。FlexGroup ボリュームのサイズを増やすと、FlexGroup ボリュームの既存のコンスティチュエントのサイズが変更されます。

パフォーマンスの向上が必要な場合は、FlexGroup ボリュームを拡張します。FlexGroup ボリュームを拡張して新しいコンスティチュエントを追加する状況としては、次のような場合があります。

- クラスタに新しいノードが追加された。
- 既存のノードに新しいアグリゲートが作成された。
- FlexGroup ボリュームの既存のコンスティチュエントがハードウェアの最大 FlexVol サイズに達しているため、FlexGroup ボリュームのサイズを変更できません。

ONTAP 9.3 よりも前のリリースでは、SnapMirror 関係が確立されたあとに FlexGroup ボリュームを拡張することはできません。ONTAP 9.3 よりも前のリリースで SnapMirror 関係の解除後にソース FlexGroup を拡張した場合は、デスティネーション FlexGroup ボリュームへのベースライン転送をもう一度実行する必要があります。ONTAP 9.3 以降では、SnapMirror 関係にある FlexGroup ボリュームを拡張できます。

**ステップ**

1. 必要に応じて、FlexGroup の容量またはパフォーマンスを拡張し、FlexGroup ボリュームのサイズを拡張します。

追加する項目	操作
FlexGroup ボリュームの容量	<div>FlexGroup ボリュームのコンスティチュエントのサイズを変更します。</div> <div><pre>volume modify -vserver vs_server_name -volume fg_name -size new_size</pre></div>

FlexGroup ボリュームのパフォーマンス	<p>新しいコンスティチュエントを追加して FlexGroup ボリュームを拡張します。</p> <pre>volume expand -vserver vs1 -volume fg_name -aggr-list aggregate name,... [-aggr-list-multiplier constituents_per_aggr]</pre> <p>のデフォルト値 <code>-aggr-list-multiplier</code> パラメータは1です。</p> <p>ONTAP 9.5 で FabricPool の FlexGroup ボリュームを拡張するには、新たに使用するアグリゲートがすべて FabricPool である必要があります。</p>
-------------------------	---

FlexGroup ボリュームの容量は、可能な限り増やす必要があります。FlexGroup ボリュームを拡張する必要がある場合は、一貫したパフォーマンスが得られるように、既存の FlexGroup ボリュームのコンスティチュエント数の倍数となるように追加します。たとえば、既存の FlexGroup にノードごとに 8 つのコンスティチュエントがある 16 個のコンスティチュエントがある場合は、コンスティチュエントを 8 個または 16 個追加して既存の FlexGroup を拡張します。

例

- 既存のコンスティチュエントの容量拡張の例 \*

次の例は、FlexGroup ボリューム volX に 20TB のスペースを追加します。

```
cluster1::> volume modify -vserver svml -volume volX -size +20TB
```

FlexGroup ボリュームに 16 個のコンスティチュエントがある場合、各コンスティチュエントのスペースが 1.25TB ずつ増えます。

- 新しいコンスティチュエントを追加してパフォーマンスを向上させる例 \*

次の例は、FlexGroup ボリューム volX に 2 つのコンスティチュエントを追加します。

```
cluster1::> volume expand -vserver vs1 -volume volX -aggr-list aggr1,aggr2
```

新しいコンスティチュエントのサイズは、既存のコンスティチュエントと同じです。

### FlexGroup ボリュームのサイズを縮小します

ONTAP 9.6 以降では、FlexGroup ボリュームのサイズを現在のサイズよりも小さい値に変更して、ボリュームから未使用のスペースを解放できます。FlexGroup ボリュームのサイズを縮小すると、ONTAP によってすべての FlexGroup コンスティチュエントのサイズが自動的に変更されます。

## ステップ

1. 現在のFlexGroup ボリュームサイズを確認します。「volume size -vserver \_vserver\_name \_ - volume\_fg\_name \_」
2. FlexGroup ボリュームのサイズを縮小します。 volume size -vserver vserver\_name -volume fg\_name new\_size

新しいサイズを指定するときは、現在のサイズよりも小さい値を指定するか、マイナス記号 (-) を使用してFlexGroup ボリュームの現在のサイズが縮小される負の値を指定できます。



ボリュームで自動縮小が有効になっている場合 (volume autosize コマンド) を入力した場合、最小オートサイズはボリュームの新しいサイズに設定されます。

次の例は、volXという名前のFlexGroup ボリュームの現在のボリュームサイズを表示し、ボリュームのサイズを10TBに変更します。

```
cluster1::> volume size -vserver svml -volume volX
(volume size)
vol size: FlexGroup volume 'svml:volX' has size 15TB.

cluster1::> volume size -vserver svml -volume volX 10TB
(volume size)
vol size: FlexGroup volume 'svml:volX' size set to 10TB.
```

次の例は、volXという名前のFlexGroup ボリュームの現在のボリュームサイズを表示し、ボリュームのサイズを5TBだけ縮小します。

```
cluster1::> volume size -vserver svml -volume volX
(volume size)
vol size: FlexGroup volume 'svml:volX' has size 15TB.

cluster1::> volume size -vserver svml -volume volX -5TB
(volume size)
vol size: FlexGroup volume 'svml:volX' size set to 10TB.
```

**FlexGroup** ボリュームのサイズを自動的に拡張および縮小するように設定します

ONTAP 9.3 以降では、必要なスペースに応じて FlexGroup ボリュームを自動的に拡張または縮小するように設定できます。

必要なもの

FlexGroup はオンラインである必要があります。

このタスクについて

FlexGroup ボリュームのオートサイズには 2 つのモードがあります。

- ボリュームのサイズを自動的に拡張します (grow モード)

自動拡張機能を使用すると、アグリゲートが追加のスペースを提供できる場合に、FlexGroup ボリュームがスペース不足になるのを防ぐことができます。ボリュームの最大サイズを設定できます。拡張は、ボリュームに書き込まれるデータ量と現在使用されているスペースの量、およびしきい値設定に基づいて自動的にトリガーされます。

デフォルトでは、ボリュームの最大サイズは、自動拡張を有効にしたときのサイズの 120% まで拡張できます。それよりも大容量にする必要がある場合は、必要に応じてボリュームの最大サイズを設定する必要があります。

- ボリュームのサイズを自動的に縮小します (grow\_shrink モード)

自動縮小機能を使用すると、ボリュームが必要以上に拡張されるのを防止し、アグリゲート内のスペースを他のボリュームでできるように解放できます。

自動縮小は、変化するスペース需要に対応するために自動拡張と組み合わせて使用することができ、単独で使用することはできません。自動縮小を有効にした場合、自動拡張と自動縮小の処理が無限に繰り返されないように縮小動作が ONTAP で自動的に制御されます。

ボリュームが拡張されると、格納できるファイルの最大数が自動的に増える可能性があります。ボリュームが縮小されても格納できるファイルの最大数は変わらず、ボリュームが縮小前のファイルの最大数に対応するサイズよりも小さくなることはありません。そのため、自動縮小でボリュームを元のサイズに戻すことはできません。

## ステップ

1. ボリュームのサイズを自動的に拡張および縮小するように設定します。 `volume autosize -vserver vs_server_name -volume vol_name -mode [grow | grow_shrink]`

ボリュームを拡張または縮小する最大サイズ、最小サイズ、およびしきい値を指定することもできます。

次に、fg1 という名前のボリュームで自動サイズ変更を有効にするコマンドを示します。ボリュームの 70% が使用された時点で最大 5TB までサイズを拡張するように設定します。

```
cluster1::> volume autosize -volume fg1 -mode grow -maximum-size 5TB
-grow-threshold-percent 70
vol autosize: volume "vs_src:fg1" autosize settings UPDATED.
```

クラスタ上のディレクトリを迅速に削除できます

ONTAP 9.8以降では、低遅延高速ディレクトリ削除機能を使用して、LinuxおよびWindowsクライアント共有から非同期（つまりバックグラウンド）でディレクトリを削除できます。クラスタ管理者およびSVM管理者は、FlexVol とFlexGroup の両方のボリュームに対して非同期削除処理を実行できます。

ONTAP 9.11.1よりも前のバージョンのONTAP を使用している場合は、クラスタ管理者またはadvanced権限モードを使用するSVM管理者である必要があります。

ONTAP 9.11.1以降、ストレージ管理者はボリュームに対する権限を付与して、NFSクライアントとSMBクラ

クライアントに非同期削除処理を実行させることができます。詳細については、を参照してください ["ディレクトリを迅速に削除するためのクライアント権限を管理します"](#)。

ONTAP 9.8以降では、ONTAP CLIを使用して、高速ディレクトリ削除機能を使用できます。ONTAP 9.9.1以降では、この機能をSystem Managerで使用できます。このプロセスの詳細については、を参照してください ["分析に基づいて修正措置を講じる"](#)。

## System Manager の略

1. [\* ストレージ]、[ボリューム]の順にクリックし、[\* エクスプローラ \*]をクリックします。

ファイルまたはフォルダにカーソルを合わせると、削除するオプションが表示されます。一度に削除できるオブジェクトは 1 つだけです。



ディレクトリとファイルを削除しても、新しいストレージ容量の値はすぐには表示されません。

## CLI の使用

- CLIを使用して、高速ディレクトリ削除\*を実行します

1. advanced 権限モードに切り替えます。

```
-privilege advance
```

2. FlexVol またはFlexGroup ボリューム上のディレクトリを削除します。

```
volume file async-delete start -vserver vs1 -volume vol1 -path d1/d2
```

最小スロットル値は 10、最大スロットル値は 100、000、デフォルトは 5000 です。

次に、d1 という名前のディレクトリにある d2 という名前のディレクトリを削除する例を示します。

```
cluster::*>volume file async-delete start -vserver vs1 -volume  
vol1 -path d1/d2
```

3. ディレクトリが削除されたことを確認します。

```
event log show
```

次の例は、ディレクトリが正常に削除されたときのイベントログの出力を示しています。

```
cluster-cli::*> event log show
```

Time	Node	Severity	Event
MM/DD/YYYY 00:11:11	cluster-vsim	INFORMATIONAL	asyncDelete.message.success: Async delete job on path d1/d2 of volume (MSID: 2162149232) was completed.

\*ディレクトリ削除ジョブ\*をキャンセルします

1. advanced 権限モードに切り替えます。

```
set -privilege advanced
```

2. ディレクトリの削除が実行中であることを確認します。

```
volume file async-delete show
```

ディレクトリのSVM、ボリューム、ジョブID、およびパスが表示された場合は、ジョブをキャンセルできます。

3. ディレクトリの削除をキャンセルします。

```
volume file async-delete cancel -vserver SVM_name -volume volume_name  
-jobid job_id
```

ディレクトリを迅速に削除するためのクライアント権限を管理します

ONTAP 9.11.1以降、ストレージ管理者はボリュームに対する権限を付与して、NFSクライアントとSMBクライアントが自身で低レイテンシの高速ディレクトリ削除操作を実行できるようにすることができます。クラスタで非同期削除が有効になっている場合、Linuxクライアントユーザはを使用できます mv コマンドおよびWindowsクライアントユーザはを使用できます rename 指定したボリューム上のディレクトリを、デフォルトで.ontaptrashbinという非表示のディレクトリに移動して迅速に削除するコマンド。

クライアントの非同期ディレクトリ削除を有効にします

手順

1. クラスタCLIからadvanced権限モードに切り替えます。 -privilege advance
2. クライアントの非同期削除を有効にし、必要に応じてtrashbinディレクトリに別の名前を指定します。

```
volume file async-delete client enable volume volname vsriver vsriverName  
trashbinname name
```

デフォルトのごみ箱名を使用する例：

```
cluster1::*> volume file async-delete client enable -volume v1 -vserver  
vs0
```

```
Info: Async directory delete from the client has been enabled on volume  
"v1" in  
Vserver "vs0".
```

代替ごみ箱名の指定例：



```
cluster1::*> volume file async-delete client enable -volume test
-trashbin .ntaptrash -vserver vs1

Success: Async directory delete from the client is enabled on volume
"v1" in
      Vserver "vs0".
```

### 3. クライアントの非同期削除が有効であることを確認します。

```
volume file async-delete client show
```

例

```
cluster1::*> volume file async-delete client show

Vserver Volume      async-delete client TrashBinName
-----
vs1         vol1         Enabled         .ntaptrash
vs2         vol2         Disabled        -

2 entries were displayed.
```

クライアントの非同期ディレクトリの削除を無効にします

手順

#### 1. クラスタCLIで、クライアントの非同期ディレクトリ削除を無効にします。

```
volume file async-delete client disable volume volname vserver vserverName
```

例

```
cluster1::*> volume file async-delete client disable -volume vol1
-vserver vs1

      Success: Asynchronous directory delete client disabled
successfully on volume.
```

#### 2. クライアントの非同期削除が無効になっていることを確認する。

```
volume file async-delete client show
```

例

```
cluster1::*> volume file async-delete client show
```

Vserver	Volume	async-delete client	TrashBinName
vs1	vol1	Disabled	-
vs2	vol2	Disabled	-

```
2 entries were displayed.
```

## FlexGroup を備えた qtree を作成します

ONTAP 9.3 以降では、FlexGroup ボリュームで qtree を作成できます。qtree を使用すると、FlexGroup を小さなセグメントにパーティショニングして、それぞれ個別に管理できます。

### このタスクについて

- ONTAP を 9.2 以前のバージョンにリバートする場合で、FlexGroup ボリュームに qtree を作成したか、デフォルト qtree の属性（セキュリティ形式および SMB oplock）を変更した場合は、デフォルト以外のすべての qtree を削除してから、各 FlexGroup ボリュームで qtree 機能を無効にしてから、ONTAP 9.2 以前のバージョンにリバートする必要があります。

### "リバート前に FlexGroup ボリュームの qtree 機能を無効にする"

- ソース FlexGroup ボリュームに SnapMirror 関係が確立された qtree がある場合、デスティネーションクラスタで ONTAP 9.3 以降（qtree をサポートする ONTAP ソフトウェアのバージョン）が実行されている必要があります。
- ONTAP 9.5 以降では、FlexGroup ボリュームで qtree の統計がサポートされます。

### 手順

1. FlexGroup ボリュームに qtree を作成します。 `volume qtree create -vserver vs1 -volume vol1 -qtree qt1`

必要に応じて、qtree のセキュリティ形式、SMB oplock、UNIX 権限、およびエクスポートポリシーを指定できます。

```
cluster1::*> volume qtree create -vserver vs0 -volume fg1 -qtree qt1  
-security-style mixed
```

### 関連情報

["論理ストレージ管理"](#)

## FlexGroup ボリュームにクォータを使用する

ONTAP 9.4 以前では、FlexGroup ボリュームにクォータルールを適用してもレポートの

対象となるだけで、クォータ制限を適用することはできませんでした。ONTAP 9.5 以降では、FlexGroup ボリュームに適用されるクォータルールに制限を適用できます。

このタスクについて

- ONTAP 9.5 以降では、FlexGroup ボリュームにハードリミット、ソフトリミット、しきい値制限の各クォータを指定できます。

これらの制限を指定して、特定のユーザ、グループ、または qtree が作成できるスペースの量、ファイルの数、またはその両方を制限できます。クォータ制限を指定すると、次の状況で警告メッセージが生成されます。

  - 使用量が設定されたソフトリミットを超えると、ONTAP は警告メッセージを発行しますが、それ以上のトラフィックは許可されます。

その後使用量がソフトリミットを再び下回ると、解決済みのメッセージが表示されます。
  - 使用量が設定されているしきい値制限を超えた場合、ONTAP は 2 つ目の警告メッセージを発行します。

その後使用量がしきい値制限を下回っても、解決済みのメッセージは表示されません。
  - 使用量が設定されたハードリミットに達すると、ONTAP はトラフィックを拒否して、それ以上のリソース消費を防止します。
- ONTAP 9.5 では、SnapMirror 関係のデスティネーション FlexGroup ボリュームでクォータルールを作成またはアクティブ化することができません。
- クォータの初期化ではクォータは適用されず、クォータの初期化後に超過したクォータの通知も生成されません。

クォータの初期化中にクォータに違反がなかったかどうかを確認するには、を使用します `volume quota report` コマンドを実行します

クォータのターゲットとタイプ

クォータにはユーザ、グループ、またはツリーのいずれかのタイプがあります。クォータターゲットは、クォータ制限が適用されるユーザ、グループ、または qtree を指定します。

次の表に、クォータターゲットの種類、各クォータターゲットに関連付けられているクォータのタイプ、および各クォータターゲットの指定方法を示します。

クォータターゲット	クォータタイプ	ターゲットの指定方法	注：
ユーザ	ユーザクォータ	UNIX ユーザ名 UNIX UID  Windows 2000 より前の形式の Windows ユーザ名  Windows SID	ユーザクォータは、特定のボリュームまたは qtree に適用できます。

グループ	グループクォータ	UNIX グループ名 UNIX GID	<p>グループクォータは、特定のボリュームまたは qtree に適用できます。</p> <div>  <p>ONTAP では、Windows ID に基づいてグループクォータを適用しません。</p> </div>
qtree	ツリークォータ	qtree 名	ツリークォータは特定のボリュームに適用され、他のボリューム内の qtree には影響しません。
""	<p>ユーザ quotagroup クォータ</p> <p>ツリークォータ</p>	二重引用符 ("" )	と表示されたクォータターゲットは、a_default QUOTA_示されています。デフォルトクォータの場合、クォータのタイプは type フィールドの値によって決まります。

#### クォータ制限を超えた場合の FlexGroup ボリュームの動作

ONTAP 9.5 以降では、FlexGroup ボリュームでクォータ制限がサポートされます。FlexGroup ボリュームと FlexVol ボリュームでは、クォータ制限の適用方法にいくつかの違いがあります。

クォータ制限を超えたときの FlexGroup ボリュームの動作は次のとおりです。

- FlexGroup ボリュームのスペースとファイルの使用量が、設定されているハードリミットを最大で 5% 上回っても、クォータ制限が適用されず、後続のトラフィックが拒否されない場合があります。

ONTAP では、最大のパフォーマンスを実現するために、スペース消費量が設定されているハードリミットをわずかに超えてもクォータが適用されないことがあります。この追加で消費されるスペースは、設定されているハードリミットの 5%、1GB、または 65536 のファイルのいずれか小さい方を超えません。

- クォータ制限に達したあとにユーザまたは管理者が一部のファイルやディレクトリを削除してクォータ使用量が制限を下回ると、クォータを消費する後続のファイル処理が遅れて再開されます（再開までの時間は 5 秒以内）。
- FlexGroup ボリュームのスペースとファイルの合計使用量が設定されているクォータ制限を超えた場合、イベントログメッセージのロギングがわずかに遅れることがあります。
- FlexGroup ボリュームの一部のコンスティチュエントがいっぱいになったにもかかわらず、クォータ制限に達していない場合は、「スペース不足」エラーが表示されます。
- クォータのハードリミットが設定されているクォータターゲットで、ファイルまたはディレクトリの名前変更や qtree 間のファイル移動などの処理を実行すると、FlexVol で同様の処理を実行する場合に比べて

時間がかかることがあります。

#### FlexGroup ボリュームのクォータ適用の例

以下の各例では、ONTAP 9.5 以降で制限が指定されたクォータを設定する方法を説明します。

##### 例 1：ディスク制限を指定してクォータルールを適用する

1. タイプがのクォータポリシールールを作成する必要があります user ディスクのソフトリミットとハードリミットをどちらも達成可能。

```
cluster1::> volume quota policy rule create -vserver vs0 -policy-name
default -volume FG -type user -target "" -qtree "" -disk-limit 1T -soft
-disk-limit 800G
```

2. クォータポリシールールを表示できます。

```
cluster1::> volume quota policy rule show -vserver vs0 -policy-name
default -volume FG
```

Vserver: vs0			Policy: default		Volume: FG		
Type	Target	Qtree	User Mapping	Disk Limit	Soft Disk Limit	Files Limit	Soft Files Limit
user	""	""	off	1TB	800GB	-	-

3. 新しいクォータルールをアクティブ化するには、ボリュームでクォータを初期化します。

```
cluster1::> volume quota on -vserver vs0 -volume FG -foreground true
[Job 49] Job succeeded: Successful
```

4. クォータレポートを使用して、FlexGroup ボリュームのディスク使用量とファイル使用量の情報を表示できます。

```
cluster1::> volume quota report -vserver vs0 -volume FG
Vserver: vs0
```

Volume	Tree	Type	ID	----Disk----		----Files-----		Quota
				Used	Limit	Used	Limit	
FG		user	root	50GB	-	1	-	
FG		user	*	800GB	1TB	0	-	*

2 entries were displayed.

ディスクのハードリミットに達すると、クォータポリシーールのターゲット（この場合はユーザ）はファイルへのデータの書き込みをブロックされます。

## 例 2：複数のユーザにクォータルールを適用する

1. タイプがのクォータポリシーールを作成する必要があります user。クォータターゲットに複数のユーザ（UNIXユーザ、SMBユーザ、またはその両方の組み合わせ）が指定されていて、現実的な値のディスクのソフトリミットとハードリミットがルールに設定されている場合。

```
cluster1::> quota policy rule create -vserver vs0 -policy-name default
-volume FG -type user -target "rdavis,ABCCORP\RobertDavis" -qtree ""
-disk-limit 1TB -soft-disk-limit 800GB
```

2. クォータポリシーールを表示できます。

```
cluster1::> quota policy rule show -vserver vs0 -policy-name default
-volume FG
```

Vserver: vs0			Policy: default			Volume: FG	
Type	Target	Qtree	User	Disk	Soft	Files	Soft
Threshold			Mapping	Limit	Disk	Limit	Files
					Limit		Limit
user	"rdavis,ABCCORP\RobertDavis"	""	off	1TB	800GB	-	-

3. 新しいクォータルールをアクティブ化するには、ボリュームでクォータを初期化します。

```
cluster1::> volume quota on -vserver vs0 -volume FG -foreground true
[Job 49] Job succeeded: Successful
```

4. クォータの状態がアクティブであることを確認できます。

```
cluster1::> volume quota show -vserver vs0 -volume FG
Vserver Name: vs0
Volume Name: FG
Quota State: on
Scan Status: -
Logging Messages: on
Logging Interval: 1h
Sub Quota Status: none
Last Quota Error Message: -
Collection of Quota Errors: -
```

5. クォータレポートを使用して、FlexGroup ボリュームのディスク使用量とファイル使用量の情報を表示できます。

```
cluster1::> quota report -vserver vs0 -volume FG
Vserver: vs0
```

Volume Specifier	Tree	Type	ID	----Disk----		----Files-----		Quota
				Used	Limit	Used	Limit	
FG		user	rdavis,ABCCORP\RobertDavis	0B	1TB	0	-	

クォータ制限は、クォータターゲットにリストされているすべてのユーザに適用されます。

ディスクのハードリミットに達すると、クォータターゲットにリストされているユーザはそれ以降のファイルへのデータの書き込みをブロックされます。

### 例 3：ユーザマッピングが有効なクォータを適用する

1. タイプがのクォータポリシールールを作成する必要があります `user`` を使用して、クォータターゲットとしてUNIXユーザまたはWindowsユーザを指定します ``user-mapping` をに設定します ``on`` を使用し、現実的な値のディスクのソフトリミットとハードリミットを指定してルールを作成します。

UNIXユーザとWindowsユーザ間のマッピングは、を使用して事前に設定しておく必要があります  
`vserver name-mapping create` コマンドを実行します

```
cluster1::> quota policy rule create -vserver vs0 -policy-name default
-volume FG -type user -target rdavis -qtree "" -disk-limit 1TB -soft
-disk-limit 800GB -user-mapping on
```

2. クォータポリシールールを表示できます。

```
cluster1::> quota policy rule show -vserver vs0 -policy-name default
-volume FG
```

```
Vserver: vs0                Policy: default                Volume: FG
```

Type	Target	Qtree	User Mapping	Disk Limit	Soft Disk Limit	Files Limit	Soft Files Limit
Threshold							
-----	-----	-----	-----	-----	-----	-----	-----
-----							
user	rdavis	""	on	1TB	800GB	-	-
-							

3. 新しいクォータルールをアクティブ化するには、ボリュームでクォータを初期化します。

```
cluster1::> volume quota on -vserver vs0 -volume FG -foreground true
[Job 49] Job succeeded: Successful
```

4. クォータの状態がアクティブであることを確認できます。

```
cluster1::> volume quota show -vserver vs0 -volume FG
Vserver Name: vs0
Volume Name: FG
Quota State: on
Scan Status: -
Logging Messages: on
Logging Interval: 1h
Sub Quota Status: none
Last Quota Error Message: -
Collection of Quota Errors: -
```

5. クォータレポートを使用して、FlexGroup ボリュームのディスク使用量とファイル使用量の情報を表示できます。



```
cluster1::> quota report -vserver vs0 -volume FG
Vserver: vs0
```

Volume	Tree	Type	ID	----Disk----		----Files-----		Quota
				Used	Limit	Used	Limit	
FG		user	rdavis,ABCCORP\RobertDavis	0B	1TB	0	-	

クォータ制限は、クォータターゲットにリストされているユーザと、そのユーザに対応する Windows ユーザまたは UNIX ユーザの両方に適用されます。

ディスクのハードリミットに達すると、クォータターゲットにリストされているユーザと、そのユーザに対応する Windows ユーザまたは UNIX ユーザは、それ以降のファイルへのデータの書き込みをブロックされます。

例 4：クォータが有効になっている場合に **qtree** のサイズを確認する

1. タイプがのクォータポリシールールを作成する必要があります tree ルールに達成可能なディスクのソフトリミットとハードリミットがある場合。

```
cluster1::> quota policy rule create -vserver vs0 -policy-name default
-volume FG -type tree -target tree_4118314302 -qtree "" -disk-limit 48GB
-soft-disk-limit 30GB
```

2. クォータポリシールールを表示できます。

```
cluster1::> quota policy rule show -vserver vs0
```

Vserver: vs0			Policy: default			Volume: FG	
Type	Target	Qtree	User	Disk	Soft	Files	Soft
Threshold			Mapping	Limit	Disk	Limit	Files
					Limit		Limit
tree	tree_4118314302	""	-	48GB	-	20	-

3. 新しいクォータルールをアクティブ化するには、ボリュームでクォータを初期化します。

```
cluster1::> volume quota on -vserver vs0 -volume FG -foreground true
[Job 49] Job succeeded: Successful
```

- a. クォータレポートを使用して、FlexGroup ボリュームのディスク使用量とファイル使用量の情報を表示できます。

```
cluster1::> quota report -vserver vs0
Vserver: vs0
----Disk---- ----Files----- Quota
Volume Tree Type ID Used Limit Used Limit Specifier
-----
FG tree_4118314302 tree 1 30.35GB 48GB 14 20 tree_4118314302
```

クォータ制限は、クォータターゲットにリストされているユーザと、そのユーザに対応する Windows ユーザまたは UNIX ユーザの両方に適用されます。

4. NFSクライアントからを使用します df コマンドを使用して、合計スペース使用量、使用可能スペース、および使用済みスペースを表示します。

```
scsps0472342001# df -m /t/10.53.2.189/FG-3/tree_4118314302
Filesystem 1M-blocks Used Available Use% Mounted on
10.53.2.189/FG-3 49152 31078 18074 63% /t/10.53.2.189/FG-3
```

ハードリミットが指定されている場合、NFS クライアントでは次のようにスペース使用量が計算されます。

- 合計スペース使用量 = ツリーのハードリミット
- 空きスペース = ハードリミットからqtreeのスペース使用量を引いた値  
ハードリミットが指定されていない場合、NFSクライアントでは次のようにスペース使用量が計算されます。
- スペース使用量 = クォータ使用量
- 合計スペース = ボリューム内のクォータ使用量と物理的な空きスペースの合計です

5. SMB 共有からは、エクスプローラを使用して、合計スペース使用量、使用可能なスペース、および使用済みスペースを表示します。

SMB 共有では、スペース使用量の計算に関する次の考慮事項を理解しておく必要があります。

- 使用可能な合計スペースの計算では、ユーザおよびグループのユーザクォータのハードリミットが考慮されます。
- ツリークォータルール、ユーザクォータルール、グループクォータルールの空きスペースの中で最も小さな値が、SMB 共有の空きスペースと見なされます。
- SMB では合計スペース使用量が一定ではなく、ツリー、ユーザ、グループの中で最も小さな空きスペースに対応するハードリミットによって決まります。

## FlexGroup ボリュームにルールと制限を適用します

### 手順

1. ターゲットのクォータルールを作成します。 `volume quota policy rule create -vserver vs0 -policy-name quota_policy_of_the_rule -volume flexgroup_vol -type {tree|user|group} -target target_for_rule -qtree qtree_name [-disk-limit hard_disk_limit_size] [-file-limit hard_limit_number_of_files] [-threshold threshold_disk_limit_size] [-soft-disk-limit soft_disk_limit_size] [-soft-file-limit soft_limit_number_of_files]`

- ONTAP 9.2およびONTAP 9.1では、クォータターゲットタイプとしてのみを指定できます user または group (FlexGroup ボリュームの場合)。

FlexGroup 9.2 および ONTAP 9.1 の ONTAP では、ツリークォータタイプはサポートされません。

- ONTAP 9.3以降では、クォータターゲットのタイプをにすることができます user、group または tree (FlexGroup ボリュームの場合)。
- FlexGroup ボリュームのクォータルールを作成する際に、ターゲットとしてパスを指定することはできません。
- ONTAP 9.5 以降では、FlexGroup ボリュームに対して、ディスクのハードリミット、ファイルのハードリミット、ディスクのソフトリミット、ファイルのソフトリミット、しきい値制限の各クォータを指定できます。

ONTAP 9.4 以前では、FlexGroup ボリュームのクォータルールを作成するときに、ディスクリミット、ファイルリミット、ディスクリミットのしきい値、ディスクのソフトリミット、ファイルのソフトリミットを指定できません。

次の例は、ユーザターゲットタイプにデフォルトのクォータルールを作成します。

```
cluster1::> volume quota policy rule create -vserver vs0 -policy-name
quota_policy_vs0_1 -volume fg1 -type user -target "" -qtree ""
```

次の例は、qtree1 という名前の qtree にツリークォータルールを作成します。

```
cluster1::> volume quota policy rule create -policy-name default -vserver
vs0 -volume fg1 -type tree -target "qtree1"
```

1. 指定したFlexGroup ボリュームのクォータをアクティブ化します。 `volume quota on -vserver svm_name -volume flexgroup_vol -foreground true`

```
cluster1::> volume quota on -vserver vs0 -volume fg1 -foreground true
```

1. クォータの初期化状態を監視します。 `volume quota show -vserver svm_name`

FlexGroup ボリュームにが表示される場合があります mixed 状態。これは、まだすべてのコンスティチュエントボリュームの状態が同じではないことを示します。

```
cluster1::> volume quota show -vserver vs0
```

Vserver	Volume	State	Scan Status
vs0	fg1	initializing	95%
vs0	vol1	off	-

2 entries were displayed.

1. アクティブなクォータがあるFlexGroup のクォータレポートを表示します。 volume quota report -vserver svm\_name -volume flexgroup\_vol

でパスを指定することはできません volume quota report FlexGroup ボリューム用のコマンドです。

次の例は、 FlexGroup ボリューム fg1 のユーザクォータを表示します。

```
cluster1::> volume quota report -vserver vs0 -volume fg1
```

Vserver: vs0

Quota				----Disk----		----Files-----		
Volume Specifier	Tree	Type	ID	Used	Limit	Used	Limit	
fg1		user	*	0B	-	0	-	*
fg1		user	root	1GB	-	1	-	*

2 entries were displayed.

次の例は、 FlexGroup ボリューム fg1 のツリークォータを表示します。

```
cluster1::> volume quota report -vserver vs0 -volume fg1
```

Vserver: vs0

				----Disk----		----Files-----		Quota
Volume Specifier	Tree	Type	ID	Used	Limit	Used	Limit	
fg1	qtree1	tree	1	68KB	-	18	-	
fg1		tree	*	0B	-	0	-	*

2 entries were displayed.

クォータルールとクォータ制限が FlexGroup ボリュームに適用されます。

使用量が設定されているハードリミットを最大 5% 超過するまで、ONTAP はそれ以上のトラフィックを拒否してクォータを適用しません。

## 関連情報

### "ONTAP 9 コマンド"

## FlexGroup ボリュームで Storage Efficiency を有効にします

FlexGroup に重複排除とデータ圧縮を一緒に、または個別に実行して、最善のスペース削減効果を得ることができます。

## 必要なもの

FlexGroup はオンラインである必要があります。

## 手順

1. FlexGroup ボリュームで Storage Efficiency を有効にします。 `volume efficiency on -vserver svm_name -volume volume_name`

Storage Efficiency 処理は、FlexGroup のすべてのコンスティチュエントで有効になります。

ボリュームで Storage Efficiency を有効にしたあとに FlexGroup ボリュームを拡張した場合は、新しいコンスティチュエントでも Storage Efficiency が自動的に有効になります。

2. を使用して、FlexGroup ボリュームに必要な Storage Efficiency 処理を有効にします `volume efficiency modify` コマンドを実行します

FlexGroup ボリュームでは、インライン重複排除、ポストプロセス重複排除、インライン圧縮、およびポストプロセス圧縮を有効にすることができます。FlexGroup ボリュームに対して圧縮形式（二次圧縮またはアダプティブ圧縮）を設定し、スケジュールや効率化ポリシーを指定することもできます。

3. スケジュールや効率化ポリシーを使用せずに Storage Efficiency 処理を実行する場合は、効率化処理を開始します。 `volume efficiency start -vserver svm_name -volume volume_name`

重複排除とデータ圧縮が有効になっている場合は、最初にデータ圧縮が実行され、続けて重複排除が実行されます。FlexGroup ボリュームですでにいずれかの効率化処理がアクティブになっている場合、このコマンドは失敗します。

4. FlexGroup ボリュームで有効になっている効率化処理を確認します。 `volume efficiency show -vserver svm_name -volume volume_name`

```
cluster1::> volume efficiency show -vserver vs1 -volume fg1
Vserver Name: vs1
Volume Name: fg1
Volume Path: /vol/fg1
State: Enabled
Status: Idle
Progress: Idle for 17:07:25
Type: Regular
Schedule: sun-sat@0

...

Compression: true
Inline Compression: true
Incompressible Data Detection: false
Constituent Volume: false
Compression Quick Check File Size: 524288000
Inline Dedupe: true
Data Compaction: false
```

## Snapshot コピーを使用して **FlexGroup** ボリュームを保護する

Snapshot コピーの作成を自動的に管理する Snapshot ポリシーを作成したり、FlexGroup ボリュームの Snapshot コピーを手動で作成したりできます。FlexGroup ボリュームの有効な Snapshot コピーが作成されるのは、FlexGroup が ONTAP ボリュームの各コンスティチュエントの Snapshot コピーを正常に作成できたあとのみです。

このタスクについて

- Snapshot ポリシーに複数の FlexGroup ボリュームが関連付けられている場合は、FlexGroup ボリュームのスケジュールが重ならないようにする必要があります。
- ONTAP 9.8 以降、FlexGroup ボリュームでサポートされる Snapshot コピーの最大数は 1023 です。



ONTAP 9.8以降では volume snapshot show FlexGroup 用のコマンドでは、最も新しい所有ブロックが計算されるのではなく、論理ブロックを使用してSnapshotコピーのサイズが報告されます。この新しいサイズ計算方法では、Snapshot コピーのサイズが以前のバージョンの ONTAP での計算よりも大きく表示される場合があります。

## 手順

1. Snapshot ポリシーを作成するか、手動で Snapshot コピーを作成します。

作成する項目	入力するコマンド
--------	----------

スナップショットポリシー	<p>volume snapshot policy create</p> <div>  <p>FlexGroup ボリュームの Snapshot ポリシーに関連付けるスケジュールは、間隔を 30 分よりも長くする必要があります。</p> </div> <p>FlexGroup ボリュームを作成すると、が表示されます default SnapshotポリシーがFlexGroup ボリュームに適用されます。</p>
Snapshot コピーを手動で作成	<p>volume snapshot create</p> <div>  <p>FlexGroup ボリュームの Snapshot コピーを作成したあとに、Snapshot コピーの属性を変更することはできません。属性を変更する場合は、Snapshot コピーを削除して作成し直す必要があります。</p> </div>

Snapshot コピーの作成中は、FlexGroup ボリュームへのクライアントアクセスが一時的に休止されます。

1. FlexGroup ボリュームの有効なSnapshotコピーが作成されたことを確認します。 volume snapshot show -volume volume\_name -fields state

```
cluster1::> volume snapshot show -volume fg -fields state
vserver volume snapshot                state
-----
fg_vs    fg        hourly.2016-08-23_0505 valid
```

2. FlexGroup ボリュームのコンスチチュエントのSnapshotコピーを表示します。 volume snapshot show -is-constituent true

```
cluster1::> volume snapshot show -is-constituent true
```

---Blocks---				
Vserver	Volume	Snapshot	Size	Total%
Used%				
-----	-----	-----	-----	-----
fg_vs	fg__0001	hourly.2016-08-23_0505	72MB	0%
27%				
	fg__0002	hourly.2016-08-23_0505	72MB	0%
27%				
	fg__0003	hourly.2016-08-23_0505	72MB	0%
27%				
...				
	fg__0016	hourly.2016-08-23_0505	72MB	0%
27%				

## FlexGroup ボリュームのコンスティチュエントを移動します

FlexGroupボリュームのコンスティチュエントをアグリゲート間で移動して、特定のコンスティチュエントのトラフィックが多い場合に負荷を分散することができます。コンスティチュエントを移動することで、アグリゲートのスペースを解放して既存のコンスティチュエントのサイズを変更することもできます

### 必要なもの

SnapMirror 関係にある FlexGroup ボリュームコンスティチュエントを移動する場合は、SnapMirror 関係を初期化しておく必要があります。

### このタスクについて

ボリューム移動処理は、FlexGroup のコンスティチュエントの拡張中は実行できません。

### 手順

1. 移動するFlexGroup ボリュームコンスティチュエントを特定します。

```
volume show -vserver svm_name -is-constituent true
```



```
cluster1::> volume show -vserver vs2 -is-constituent true
```

Vserver	Volume	Aggregate	State	Type	Size
Available	Used%				
vs2	fg1	-	online	RW	400TB
15.12TB	62%				
vs2	fg1__0001	aggr1	online	RW	25TB
8.12MB	59%				
vs2	fg1__0002	aggr2	online	RW	25TB
2.50TB	90%				
...					

## 2. FlexGroup ボリュームコンスティチュエントの移動先となるアグリゲートを特定します。

```
volume move target-aggr show -vserver svm_name -volume vol_constituent_name
```

選択するアグリゲート内の使用可能なスペースは、移動する FlexGroup ボリュームコンスティチュエントのサイズよりも大きくする必要があります。

```
cluster1::> volume move target-aggr show -vserver vs2 -volume fg1_0002
```

Aggregate Name	Available Size	Storage Type
aggr2	467.9TB	hdd
node12a_aggr3	100.34TB	hdd
node12a_aggr2	100.36TB	hdd
node12a_aggr1	100.36TB	hdd
node12a_aggr4	100.36TB	hdd
5 entries were displayed.		

## 3. FlexGroup ボリュームコンスティチュエントを目的のアグリゲートに移動できることを確認します。

```
volume move start -vserver svm_name -volume vol_constituent_name -destination  
-aggregate aggr_name -perform-validation-only true
```

```
cluster1::> volume move start -vserver vs2 -volume fg1_0002 -destination  
-aggregate node12a_aggr3 -perform-validation-only true  
Validation succeeded.
```

## 4. FlexGroup ボリュームコンスティチュエントを移動します。

```
volume move start -vserver svm_name -volume vol_constituent_name -destination  
-aggregate aggr_name [-allow-mixed-aggr-types {true|false}]
```

ボリューム移動処理はバックグラウンドプロセスとして実行されます。

ONTAP 9.5以降では、を設定することで、FlexGroup ボリュームコンスティチュエントをFabric Poolから非Fabric Poolに（またはその逆に）移動できます `-allow-mixed-aggr-types` パラメータの値 `true`。デフォルトでは、が表示されます `-allow-mixed-aggr-types` オプションはに設定されています `false`。



を使用することはできません `volume move` FlexGroup ボリュームで暗号化を有効にするコマンド。

```
cluster1::> volume move start -vserver vs2 -volume fg1_002 -destination
-aggregate node12a_aggr3
```



アクティブなSnapMirror処理が原因でボリューム移動処理が失敗した場合は、を使用してSnapMirror処理を中止する必要があります `snapmirror abort -h` コマンドを実行します 場合によっては、SnapMirror の中止処理も失敗することがあります。このような場合は、ボリューム移動処理を中止してから再試行してください。

## 5. ボリューム移動処理の状態を確認します。

```
volume move show -volume vol_constituent_name
```

次の例は、ボリューム移動処理のレプリケーションフェーズを完了し、カットオーバーフェーズにあるFlexGroup コンスティチュエントボリュームの状態を示しています。

```
cluster1::> volume move show -volume fg1_002
Vserver    Volume      State      Move Phase  Percent-Complete Time-To-
Complete
-----
vs2        fg1_002     healthy   cutover     -              -
```

既存の **FlexGroup** ボリュームには、**FabricPool** 内のアグリゲートを使用します

ONTAP 9.5 以降では、FlexGroup ボリュームで FabricPool がサポートされます。FabricPool 内のアグリゲートを既存の FlexGroup ボリュームに使用する場合は、FlexGroup ボリュームが配置されているアグリゲートを FabricPool 内のアグリゲートに変換するか、FlexGroup ボリュームのコンスティチュエントを FabricPool 内のアグリゲートに移行します。

必要なもの

- FlexGroup ボリュームのスペースギャランティをに設定する必要があります `none`。
- FlexGroup ボリュームが配置されているアグリゲートを FabricPool 内のアグリゲートに変換する場合は、アグリゲートが SSD ディスクのみを使用している必要があります。

このタスクについて

既存の FlexGroup ボリュームが SSD 以外のアグリゲートにある場合は、FlexGroup ボリュームのコンスチチュエントを FabricPool 内のアグリゲートに移行する必要があります。

#### 選択肢

- FlexGroup ボリュームが配置されているアグリゲートを FabricPool のアグリゲートに変換するには、次の手順を実行します。

- a. 既存の FlexGroup ボリュームで階層化ポリシーを設定します。 `volume modify -volume flexgroup_name -tiering-policy [auto|snapshot|none|backup]`

```
cluster-2::> volume modify -volume fg1 -tiering-policy auto
```

- b. FlexGroup ボリュームが配置されているアグリゲートを特定します。 `volume show -volume flexgroup_name -fields aggr-list`

```
cluster-2::> volume show -volume fg1 -fields aggr-list
vserver volume aggr-list
-----
vs1      fg1      aggr1,aggr3
```

- c. アグリゲートリストに表示された各アグリゲートにオブジェクトストアを接続します。 `storage aggregate object-store attach -aggregate aggregate name -name object-store-name -allow-flexgroup true`

すべてのアグリゲートをオブジェクトストアに接続する必要があります。

```
cluster-2::> storage aggregate object-store attach -aggregate aggr1
-object-store-name Amazon01B1
```

- FlexGroup ボリュームのコンスチチュエントを FabricPool 内のアグリゲートに移行するには、次の手順を実行します。

- a. 既存の FlexGroup ボリュームで階層化ポリシーを設定します。 `volume modify -volume flexgroup_name -tiering-policy [auto|snapshot|none|backup]`

```
cluster-2::> volume modify -volume fg1 -tiering-policy auto
```

- b. FlexGroup ボリュームの各コンスチチュエントを、同じクラスタ内の FabricPool 内のアグリゲートに移動します。 `volume move start -volume constituent-volume -destination -aggregate FabricPool_aggregate -allow-mixed-aggr-types true`

FlexGroup ボリュームのすべてのコンスチチュエントを FabricPool 内のアグリゲートに移動し（FlexGroup ボリュームのコンスチチュエントが異なるタイプのアグリゲートに配置されている場合）、それらのコンスチチュエントをクラスタ内のノード間に分散します。

```
cluster-2::> volume move start -volume fg1_001 -destination-aggregate  
FP_aggr1 -allow-mixed-aggr-types true
```

## 関連情報

"ディスクおよびアグリゲートの管理"

## FlexGroup ボリュームのリバランシング

ONTAP 9.12.1以降では、FlexGroup 内のコンスティチュエント間でファイルが無停止で移動することにより、FlexGroup ボリュームをリバランシングできます。

FlexGroup のリバランシングは、新しいファイルの追加やファイルの拡張によって不均衡が時間の経過とともに生じた場合に容量を再配分するのに役立ちます。リバランシング処理を手動で開始すると、ONTAP はファイルを選択し、システムを停止せずに自動的に移動します。



マルチパートinodeの作成により、1つのリバランシングイベントまたは複数のリバランシングイベントの一部として大量のファイルが移動された場合、FlexGroupのリバランシングではシステムパフォーマンスが低下することに注意してください。リバランシングイベントの一環として移動されたすべてのファイルには、そのファイルに2つのマルチパートinodeが関連付けられています。FlexGroup内のファイル総数に対するマルチパートinodeを持つファイル数の割合が大きいくほど、パフォーマンスへの影響が大きくなります。FlexVolからFlexGroupへの変換など、特定のユースケースでは、大量のマルチパートinodeが作成される可能性があります。

リバランシングは、クラスタ内のすべてのノードでONTAP 9.12.1以降のリリースが実行されている場合にのみ使用できます。リバランシング処理を実行するすべてのFlexGroupボリュームで、きめ細かなデータ機能を有効にする必要があります。一度有効にすると、このボリュームを削除するか、設定を有効にする前に作成されたSnapshotコピーからリストアしないかぎり、ONTAP 9.11.1以前のバージョンにリバートすることはできません。

ONTAP 9.14.1以降では、きめ細かなデータが有効なボリューム内のファイルが無停止でプロアクティブに移動するアルゴリズムがONTAPに導入されています。ユーザの操作は不要です。このアルゴリズムは、パフォーマンスのボトルネックを軽減するために、非常に具体的なターゲットシナリオで動作します。このアルゴリズムが機能するシナリオには、クラスタ内の1つのノード上の特定のファイルセットに対する非常に高い書き込み負荷や、非常にホットな親ディレクトリ内の継続的に増加するファイルなどがあります。

## FlexGroup のリバランシングに関する考慮事項

FlexGroup のリバランシングの仕組みと他のONTAP 機能との連携について理解しておく必要があります。

### • FlexVol からFlexGroup への変換

FlexVol からFlexGroup への変換後は、FlexGroup の自動リバランシングを使用しないことを推奨します。代わりに、ONTAP 9.10.1以降で使用可能なシステム停止を伴う逆アクティブファイル移動機能を使用するには、を入力します volume rebalance file-move コマンドを実行しますコマンド構文については、を参照してください volume rebalance file-move start のマニュアルページ。

FlexGroupの自動リバランシング機能を使用したリバランシングでは、FlexVolからFlexGroupへの変換を実行し、FlexVolボリューム上のデータの50~85%が新しいコンスティチュエントに移動されるなど、多数のファイルを移動する際のパフォーマンスが低下する可能性があります。

- ファイルの最小サイズと最大サイズ

LIFの自動リバランシングで選択されるファイルは、保存されたブロックに基づいています。リバランシングのために考慮される最小ファイルサイズはデフォルトで100MB（下記のmin-file-sizeパラメータを使用して20MBまで設定可能）で、最大ファイルサイズは100GBです。

- Snapshotコピー内のファイル

FlexGroup のリバランシングを設定して、Snapshotコピーに現在存在しないファイルのみを移動することができます。リバランシングが開始されると、リバランシング処理中にいつでもSnapshotコピー処理がスケジュールされているかどうかが通知されます。

ファイルの移動中で、デスティネーションでフレーミングが実行されている場合、Snapshotコピーは制限されます。ファイルのリバランシングが実行中の場合、Snapshotコピーのリストア処理は実行できません。

- SnapMirror 処理

FlexGroup のリバランシングは、スケジュールされたSnapMirror処理の間に行う必要があります。SnapMirror処理の開始前にファイルを再配置している場合、そのファイルの移動が24時間のSnapMirror再試行期間内に完了しないと、SnapMirror処理が失敗することがあります。SnapMirror転送の開始後に開始される新しいファイルの再配置は失敗しません。

- ファイルベースの圧縮のストレージ効率化

ファイルベースの圧縮によるストレージ効率化では、ファイルはデスティネーションに移動する前に解凍されるため、圧縮による削減が失われます。リバランシング後に手動で開始したバックグラウンドスキナをFlexGroup で実行した場合、圧縮による削減効果が再び得られます。ただし、いずれかのボリューム上のSnapshotコピーに関連付けられたファイルは、圧縮の対象として無視されます。

- 重複排除

重複排除されたファイルを移動すると、原因でFlexGroup ボリュームの全体的な使用量が増加する可能性がファイルのリバランシング時には、一意のブロックのみがデスティネーションに移動され、ソースの容量が解放されます。共有ブロックはソースに保持され、デスティネーションにコピーされます。このため、ほぼフルのソースコンスチチュエントで使用済み容量を減らすことは目標ですが、新しいデスティネーションに共有ブロックがコピーされるため、FlexGroup ボリューム全体の使用量が増加することもあります。また、Snapshotコピーの一部であるファイルを移動する場合にも使用できます。Snapshotコピースケジュールがリサイクルされるまでスペース削減は完全には認識されず、Snapshotコピー内のファイルのコピーも削除されます。

- FlexClone ボリューム

FlexCloneボリュームの作成時にファイルのリバランシングが実行中の場合、FlexCloneボリュームではリバランシングは実行されません。FlexCloneボリュームでのリバランシングは、FlexCloneボリュームの作成後に実行する必要があります。

- ファイル移動

FlexGroup のリバランシング処理中にファイルが移動されると、ソースとデスティネーションの両方のコンスチチュエントについて、クォータアカウンティングの一部としてファイルサイズが報告されます。移動が完了すると、クォータアカウンティングは通常に戻り、ファイルサイズは新しいデスティネーションでのみ報告されます。

- 自律的なランサムウェア防御

ONTAP 9.13.1以降では、システムの停止を伴うリバランシング処理と無停止のリバランシング処理で自律型ランサムウェア対策がサポートされます。

- オブジェクトストアボリューム

ボリューム容量のリバランシングは、S3バケットなどのオブジェクトストアボリュームではサポートされていません。

#### FlexGroup のリバランシングを有効にする

ONTAP 9.12.1以降では、無停止のFlexGroupボリュームの自動リバランシングを有効にして、FlexGroupコンスチチュエント間でファイルを再配分することができます。

ONTAP 9.13.1以降では、特定の日時にFlexGroupのリバランシング処理を開始するようにスケジュールを設定できます。

作業を開始する前に


を有効にしておく必要があります `granular-data` FlexGroup のリバランシングを有効にする前にFlexGroupボリュームのオプションを選択します。有効にするには、次のいずれかの方法を使用します。

- を使用してFlexGroup ボリュームを作成する場合 `volume create` コマンドを実行します
- を使用して、既存のFlexGroup ボリュームを変更して設定を有効にします `volume modify` コマンドを実行します
- を使用してFlexGroup のリバランシングを開始した場合に自動的に設定されます `volume rebalance` コマンドを実行します

手順

FlexGroup のリバランシングは、ONTAP のSystem ManagerまたはONTAP のCLIを使用して管理できます。

## System Manager の略

1. [ストレージ]>[ボリューム]に移動し、再バランスするFlexGroup ボリュームを探します。
2. 選択するオプション  をクリックしてボリュームの詳細を確認してください。
3. [リバランス]\*を選択します。
4. 「\* Rebalance Volume \*」（ボリュームの再バランス）ウィンドウで、必要に応じてデフォルト設定を変更します。
5. リバランシング処理をスケジュールするには、\*[あとでリバランシング]\*を選択して日時を入力します。

## CLI の使用

1. 自動リバランシングを開始します。 `volume rebalance start -vserver SVM_name -volume volume_name`

必要に応じて、次のオプションを指定できます。

`[-max-runtime]<time interval>`最大実行時間

`[-max-threshold <percent>]`コンスティチュエントあたりの最大不均衡しきい値

`[-min-threshold <percent>]`コンスティチュエントあたりの最小不均衡しきい値

`[-max-file-moves <integer>]`コンスティチュエントあたりの同時ファイル移動の最大数

`[-min-file-size {<integer>[KB|MB|GB|TB|PB]}]`最小ファイルサイズ

`[-start-time <mm/dd/yyyy-00:00:00>]`再バランスの開始日時をスケジュールする

`[-exclude-snapshots {true|false}]` Snapshotコピーで停止しているファイルを除外する


例

```
volume rebalance start -vserver vs0 -volume fg1
```

## FlexGroup のリバランシング設定を変更します

FlexGroup のリバランシング設定を変更して、不均衡しきい値、同時ファイルの移動数の最小ファイルサイズ、最大実行時間、およびSnapshotコピーを追加または除外することができます。FlexGroup リバランシングスケジュールを変更するオプションは、ONTAP 9.13.1以降で使用できます。

### System Manager の略

1. [ストレージ]>[ボリューム]に移動し、再バランスするFlexGroup ボリュームを探します。
2. 選択するオプション  をクリックしてボリュームの詳細を確認してください。
3. [リバランス]\*を選択します。
4. 「\* Rebalance Volume \*」（ボリュームの再バランス）ウィンドウで、必要に応じてデフォルト設定を変更します。

### CLI の使用

1. 自動リバランシングを変更します。 `volume rebalance modify -vserver SVM_name -volume volume_name`

次のオプションを1つ以上指定できます。

`[-max-runtime]<time interval>`最大実行時間

`[-max-threshold <percent>]`コンスティチュエントあたりの最大不均衡しきい値

`[-min-threshold <percent>]` コンスティチュエントあたりの最小不均衡しきい値

`[-max-file-moves <integer>]`コンスティチュエントあたりの同時ファイル移動の最大数

`[-min-file-size {<integer>[KB|MB|GB|TB|PB]}]` 最小ファイルサイズ


`[-start-time <mm/dd/yyyy-00:00:00>]`再バランスの開始日時をスケジュールする

`[-exclude-snapshots {true|false}]` Snapshotコピーで停止しているファイルを除外する

### FlexGroup のリバランシングを停止します

FlexGroupのリバランシングを有効またはスケジュール設定したあとは、いつでも停止できます。

### System Manager の略

1. [ストレージ]>[ボリューム]の順に選択し、FlexGroup ボリュームを探します。
2. 選択するオプション  をクリックしてボリュームの詳細を確認してください。
3. [Stop Rebalance]\*を選択します。

### CLI の使用


1. FlexGroup のリバランシングを停止します。 `volume rebalance stop -vserver SVM_name -volume volume_name`

### FlexGroup のリバランシングステータスを確認します

FlexGroup のリバランシング処理、FlexGroup のリバランシング設定、リバランシング処理の時間、およびリバランシングインスタンスの詳細に関するステータスを表示できます。



## System Manager の略

1. [ストレージ]>[ボリューム]の順に選択し、FlexGroup ボリュームを探します。
2. 選択するオプション  をクリックしてFlexGroup の詳細を確認してください。
3. \* FlexGroup Balance Status \*は、詳細ペインの下部に表示されます。
4. 前回のリバランシング処理に関する情報を表示するには、\*[前回のボリュームのリバランシングステータス]\*を選択します。

## CLI の使用

1. FlexGroup のリバランシング処理のステータスを表示します。 `volume rebalance show`

再バランス状態の例：

```
> volume rebalance show
Vserver: vs0
```

Imbalance				Target	
Volume	State	Total	Used	Used	
Size	%				
-----					
fg1	idle	4GB	115.3MB	-	
8KB	0%				

設定のリバランシングの例：

```
> volume rebalance show -config
Vserver: vs0
```

Min		Max	Threshold		Max
Volume	Exclude	Runtime	Min	Max	File Moves
File Size	Snapshot				
-----					
fg1		6h0m0s	5%	20%	25
4KB	true				

リバランシング時間の詳細の例：

```
> volume rebalance show -time
Vserver: vs0
Volume                               Start Time                               Runtime
Max Runtime                           -----
-----
fgl                                   Wed Jul 20 16:06:11 2022           0h1m16s
6h0m0s
```

インスタンスの再バランスの詳細の例：

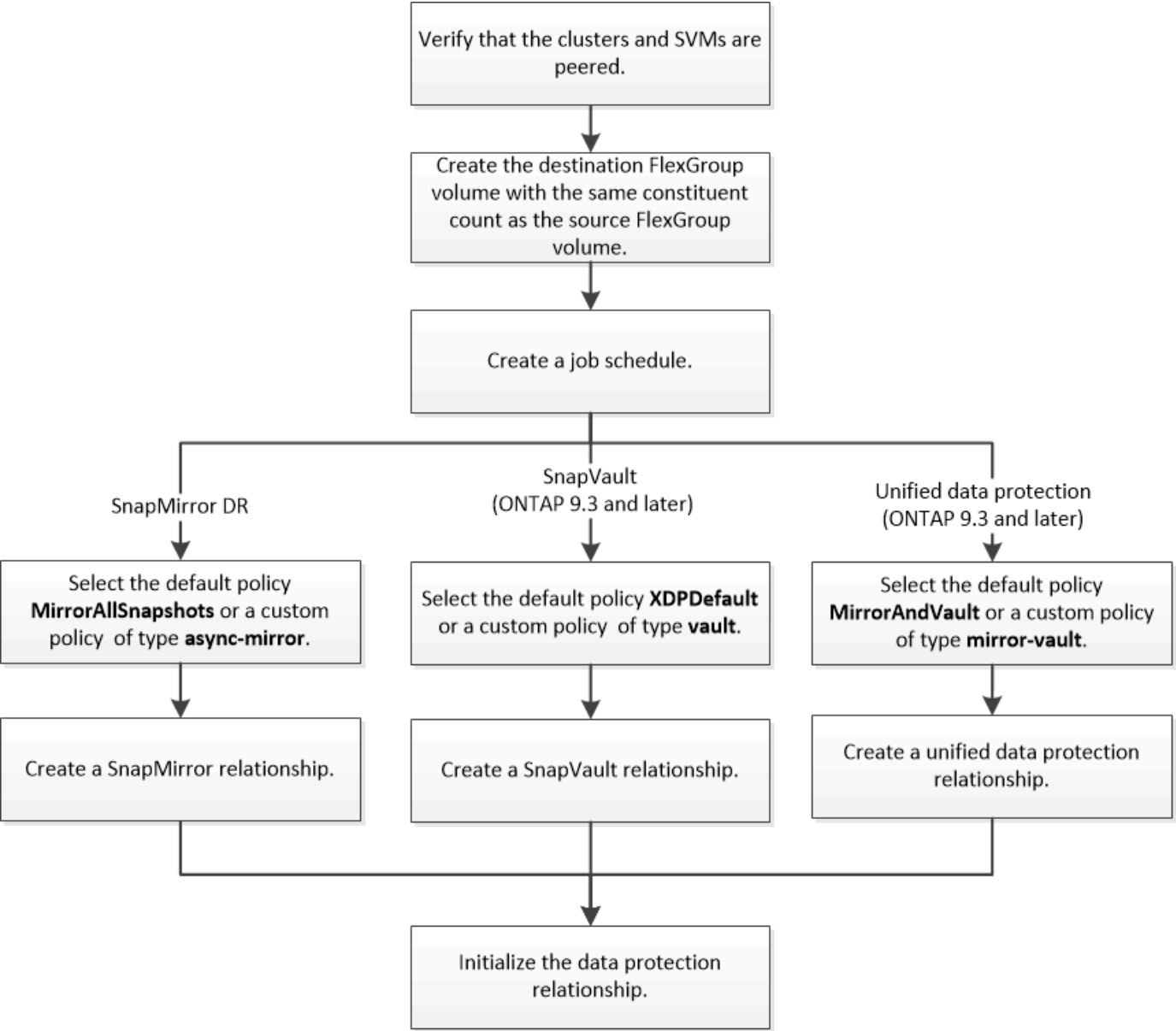
```
> volume rebalance show -instance
Vserver Name: vs0
Volume Name: fgl
Is Constituent: false
Rebalance State: idle
Rebalance Notice Messages: -
Total Size: 4GB
AFS Used Size: 115.3MB
Constituent Target Used Size: -
Imbalance Size: 8KB
Imbalance Percentage: 0%
Moved Data Size: -
Maximum Constituent Imbalance Percentage: 1%
Rebalance Start Time: Wed Jul 20 16:06:11 2022
Rebalance Stop Time: -
Rebalance Runtime: 0h1m32s
Rebalance Maximum Runtime: 6h0m0s
Maximum Imbalance Threshold per Constituent: 20%
Minimum Imbalance Threshold per Constituent: 5%
Maximum Concurrent File Moves per Constituent: 25
Minimum File Size: 4KB
Exclude Files Stuck in Snapshot Copies: true
```

## FlexGroup ボリュームのデータ保護

### FlexGroup ボリュームのデータ保護ワークフロー

FlexGroup ボリュームの SnapMirror ディザスタリカバリ（DR）関係を作成できます。ONTAP 9.3 以降では、SnapVault テクノロジを使用した FlexGroup のバックアップとリストアや、バックアップと DR に同じデスティネーションを使用する一元化されたデータ保護関係の作成も可能です。

データ保護ワークフローは、クラスタと SVM のピア関係の確認、デスティネーションボリュームの作成、ジョブスケジュールの作成、ポリシーの指定、データ保護関係の作成、関係の初期化で構成されます。



このタスクについて

SnapMirror関係のタイプはalwaysです XDP（FlexGroup ボリュームの場合）。SnapMirror 関係によって提供されるデータ保護のタイプは、使用するレプリケーションポリシーで決まります。作成するレプリケーション関係に応じて、必要なタイプのデフォルトポリシーまたはカスタムポリシーを使用できます。次の表に、デフォルトポリシーのタイプとサポートされるカスタムポリシーのタイプをデータ保護関係のタイプ別に示します。

関係タイプ	デフォルトポリシー	カスタムポリシータイプ
SnapMirror DR	MirrorAllSnapshots	非同期ミラー
SnapVault バックアップ	XDPDefault	バックアップ

一元化されたデータ保護	MirrorAndVault の場合	ミラー - バックアップ
-------------	--------------------	--------------

MirrorLatest ポリシーは FlexGroup ボリュームではサポートされません。

## FlexGroup ボリュームの SnapMirror 関係を作成

ディザスタリカバリ用にデータをレプリケートするために、ピア関係にある SVM のソース FlexGroup ボリュームとデスティネーション FlexGroup ボリュームの間で SnapMirror 関係を作成することができます。災害が発生した場合は、FlexGroup ボリュームのミラーコピーを使用してデータをリカバリできます。

### 必要なもの

クラスタと SVM のピア関係を作成しておく必要があります。

### "クラスタと SVM のピアリング"

#### このタスクについて

- FlexGroup ボリュームには、クラスタ間 SnapMirror 関係とクラスタ内 SnapMirror 関係の両方を作成することができます。
- ONTAP 9.3 以降では、SnapMirror 関係にある FlexGroup ボリュームを拡張できます。

ONTAP 9.3 より前 FlexGroup のバージョンの ONTAP を使用している場合は、SnapMirror 関係の確立後に FlexGroup ボリュームを拡張することはできませんが、容量を拡張することはできます。ONTAP 9.3 よりも前のリリースで SnapMirror 関係の解除後にソース FlexGroup ボリュームを拡張した場合は、デスティネーション FlexGroup へのベースライン転送を実行する必要があります。

### 手順

1. タイプがのデスティネーション FlexGroup ボリュームを作成します DP ソース FlexGroup と同じ数のコンスティチュエントを含むデータセンターを作成します。
  - a. ソースクラスタから、ソース FlexGroup ボリュームのコンスティチュエントの数を確認します。

```
volume show -volume volume_name* -is-constituent true
```

```
cluster1::> volume show -volume srcFG* -is-constituent true
```

Vserver	Volume	Aggregate	State	Type	Size
Available	Used%				
vss	srcFG	-	online	RW	400TB
172.86GB	56%				
vss	srcFG__0001	Aggr_cmode	online	RW	25GB
10.86TB	56%				
vss	srcFG__0002	aggr1	online	RW	25TB
10.86TB	56%				
vss	srcFG__0003	Aggr_cmode	online	RW	25TB
10.72TB	57%				
vss	srcFG__0004	aggr1	online	RW	25TB
10.73TB	57%				
vss	srcFG__0005	Aggr_cmode	online	RW	25TB
10.67TB	57%				
vss	srcFG__0006	aggr1	online	RW	25TB
10.64TB	57%				
vss	srcFG__0007	Aggr_cmode	online	RW	25TB
10.63TB	57%				
...					

- b. デスティネーションクラスタから、タイプがのデスティネーションFlexGroup ボリュームを作成します DP ソースFlexGroup と同じ数のコンスティチュエントで構成されています。

```
cluster2::> volume create -vserver vsd -aggr-list aggr1,aggr2 -aggr
-list-multiplier 8 -size 400TB -type DP dstFG
```

Warning: The FlexGroup volume "dstFG" will be created with the following number of constituents of size 25TB: 16.

Do you want to continue? {y|n}: y

[Job 766] Job succeeded: Successful

- c. デスティネーションクラスタから、デスティネーションFlexGroup ボリュームのコンスティチュエントの数を確認します。 volume show -volume volume\_name\* -is-constituent true

```
cluster2::> volume show -volume dstFG* -is-constituent true
```

Vserver	Volume	Aggregate	State	Type	Size
Available	Used%				
-----	-----	-----	-----	-----	-----
vsd	dstFG	-	online	DP	400TB
172.86GB	56%				
vsd	dstFG__0001	Aggr_cmode	online	DP	25GB
10.86TB	56%				
vsd	dstFG__0002	aggr1	online	DP	25TB
10.86TB	56%				
vsd	dstFG__0003	Aggr_cmode	online	DP	25TB
10.72TB	57%				
vsd	dstFG__0004	aggr1	online	DP	25TB
10.73TB	57%				
vsd	dstFG__0005	Aggr_cmode	online	DP	25TB
10.67TB	57%				
vsd	dstFG__0006	aggr1	online	DP	25TB
10.64TB	57%				
vsd	dstFG__0007	Aggr_cmode	online	DP	25TB
10.63TB	57%				
...					

2. ジョブスケジュールを作成します。 `job schedule cron create -name job_name -month month -dayofweek day_of_week -day day_of_month -hour hour -minute minute`

をクリックします `-month`、`-dayofweek` および `-hour` オプションを指定できます all ジョブを毎月、毎日、および1時間ごとに実行します。

次の例は、という名前のジョブスケジュールを作成します `my_weekly` 土曜日の午前3時に実行されます。

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

3. タイプがのカスタムポリシーを作成します `async-mirror SnapMirror`関係に対して次のコマンドを実行します。 `snapmirror policy create -vserver SVM -policy snapmirror_policy -type async-mirror`

カスタムポリシーを作成しない場合は、を指定する必要があります `MirrorAllSnapshots SnapMirror`関係のポリシー。

4. デスティネーションクラスタから、ソースFlexGroup ボリュームとデスティネーションFlexGroup ボリュームの間のSnapMirror関係を作成します。 `snapmirror create -source-path src_svm:src_flexgroup -destination-path dest_svm:dest_flexgroup -type XDP -policy snapmirror_policy -schedule sched_name`

FlexGroup ボリュームのSnapMirror関係のタイプはである必要があります XDP。

FlexGroup ボリュームの SnapMirror 関係にスロットル値を指定した場合、各コンスティチュエントに同じスロットル値が使用されます。スロットル値はコンスティチュエント間で分配されません。



FlexGroup ボリュームでは、Snapshot コピーの SnapMirror ラベルは使用できません。

ONTAP 9.4以前では、でポリシーが指定されていない場合 `snapmirror create` コマンドを入力します MirrorAllSnapshots デフォルトではポリシーが使用されます。ONTAP 9.5では、でポリシーが指定されていない場合 `snapmirror create` コマンドを入力します MirrorAndVault デフォルトではポリシーが使用されます。

```
cluster2::> snapmirror create -source-path vss:srcFG -destination-path  
vsd:dstFG -type XDP -policy MirrorAllSnapshots -schedule hourly  
Operation succeeded: snapmirror create for the relationship with  
destination "vsd:dstFG".
```

##### 5. デスティネーションクラスタから、ベースライン転送を実行してSnapMirror関係を初期化します。

```
snapmirror initialize -destination-path dest_svm:dest_flexgroup
```

ベースライン転送の完了後は、SnapMirror 関係のスケジュールに基づいて定期的にデスティネーション FlexGroup ボリュームが更新されます。

```
cluster2::> snapmirror initialize -destination-path vsd:dstFG  
Operation is queued: snapmirror initialize of destination "vsd:dstFG".
```



ONTAP 9.3 を実行しているソースクラスタと ONTAP 9.2 以前を実行しているデスティネーションクラスタの FlexGroup ボリューム間に SnapMirror 関係を作成した場合、ソース FlexGroup ボリュームに `qtree` を作成すると SnapMirror の更新が失敗します。この状況からリカバリするには、FlexGroup ボリューム内のデフォルト以外のすべての `qtree` を削除し、FlexGroup ボリュームの `qtree` 機能を無効にしてから、`qtree` 機能で有効化されたすべての Snapshot コピーを削除する必要があります。FlexGroup ボリュームで `qtree` 機能を有効にしている場合、ONTAP 9.3 から以前のバージョンの ONTAP にリポートする前に以下の手順も実行する必要があります。"リポート前に FlexGroup ボリュームの `qtree` 機能を無効にする"

完了後

LIF やエクスポートポリシーなどの必要な設定を行って、デスティネーション SVM のデータアクセスを設定します。

### FlexGroup ボリュームの SnapVault 関係を作成

SnapVault 関係を設定し、その関係に SnapVault ポリシーを割り当てて、SnapVault バックアップを作成することができます。

必要なもの

FlexGroup ボリュームの SnapVault 関係の作成に関する考慮事項を確認しておく必要があります。

#### 手順

1. タイプがのデスティネーションFlexGroup ボリュームを作成します DP ソースFlexGroup と同じ数のコンスティチュエントを含むデータセンターを作成します。

- a. ソースクラスタから、ソースFlexGroup ボリュームのコンスティチュエントの数を確認します。

```
volume show -volume volume_name* -is-constituent true
```

```
cluster1::> volume show -volume src* -is-constituent true
```

Vserver	Volume	Aggregate	State	Type	Size
Available	Used%				
-----	-----	-----	-----	-----	-----
vss	src	-	online	RW	400TB
172.86GB	56%				
vss	src__0001	Aggr_cmode	online	RW	25GB
10.86TB	56%				
vss	src__0002	aggr1	online	RW	25TB
10.86TB	56%				
vss	src__0003	Aggr_cmode	online	RW	25TB
10.72TB	57%				
vss	src__0004	aggr1	online	RW	25TB
10.73TB	57%				
vss	src__0005	Aggr_cmode	online	RW	25TB
10.67TB	57%				
vss	src__0006	aggr1	online	RW	25TB
10.64TB	57%				
vss	src__0007	Aggr_cmode	online	RW	25TB
10.63TB	57%				
...					

- b. デスティネーションクラスタから、タイプがのデスティネーションFlexGroup ボリュームを作成します DP ソースFlexGroup と同じ数のコンスティチュエントで構成されています。

```
cluster2::> volume create -vserver vsd -aggr-list aggr1,aggr2 -aggr  
-list-multiplier 8 -size 400TB -type DP dst
```

```
Warning: The FlexGroup volume "dst" will be created with the  
following number of constituents of size 25TB: 16.
```

```
Do you want to continue? {y|n}: y
```

```
[Job 766] Job succeeded: Successful
```

- c. デスティネーションクラスタから、デスティネーションFlexGroup ボリュームのコンスティチュエントの数を確認します。 volume show -volume volume\_name\* -is-constituent true



```
cluster2::> volume show -volume dst* -is-constituent true
```

Vserver	Volume	Aggregate	State	Type	Size
Available	Used%				
-----	-----	-----	-----	-----	-----
vsd	dst	-	online	RW	400TB
172.86GB	56%				
vsd	dst__0001	Aggr_cmode	online	RW	25GB
10.86TB	56%				
vsd	dst__0002	aggr1	online	RW	25TB
10.86TB	56%				
vsd	dst__0003	Aggr_cmode	online	RW	25TB
10.72TB	57%				
vsd	dst__0004	aggr1	online	RW	25TB
10.73TB	57%				
vsd	dst__0005	Aggr_cmode	online	RW	25TB
10.67TB	57%				
vsd	dst__0006	aggr1	online	RW	25TB
10.64TB	57%				
vsd	dst__0007	Aggr_cmode	online	RW	25TB
10.63TB	57%				
...					

2. ジョブスケジュールを作成します。 `job schedule cron create -name job_name -month month -dayofweek day_of_week -day day_of_month -hour hour -minute minute`

の場合 `-month`、`-dayofweek` および `-hour` を指定できます ``all`` 毎月、曜日、および時間ごとにジョブを実行します。

次の例は、という名前のジョブスケジュールを作成します `my_weekly` 土曜日の午前3時に実行されます。

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

3. SnapVault ポリシーを作成し、SnapVault ポリシーのルールを定義します。
- タイプがのカスタムポリシーを作成します `vault SnapVault` 関係の場合: `snapmirror policy create -vserver svm_name -policy policy_name -type vault`
  - 初期化処理と更新処理の際に転送するSnapshotコピーを決定するSnapVault ポリシーのルールを定義します。 `snapmirror policy add-rule -vserver svm_name -policy policy_for_rule - snapmirror-label snapmirror-label -keep retention_count -schedule schedule`
- カスタムポリシーを作成しない場合は、を指定する必要があります `XDPEDefault` SnapVault 関係のポリシー。

4. SnapVault 関係を作成します。 `snapmirror create -source-path src_svm:src_flexgroup -destination-path dest_svm:dest_flexgroup -type XDP -schedule schedule_name -policy XDPDefault`

ONTAP 9.4以前では、でポリシーが指定されていない場合 `snapmirror create` コマンドを入力します MirrorAllSnapshots デフォルトではポリシーが使用されます。ONTAP 9.5では、でポリシーが指定されていない場合 `snapmirror create` コマンドを入力します MirrorAndVault デフォルトではポリシーが使用されます。

```
cluster2::> snapmirror create -source-path vss:srcFG -destination-path  
vsd:dstFG -type XDP -schedule Daily -policy XDPDefault
```

5. デスティネーションクラスタから、ベースライン転送を実行してSnapVault 関係を初期化します。  
`snapmirror initialize -destination-path dest_svm:dest_flexgroup`

```
cluster2::> snapmirror initialize -destination-path vsd:dst  
Operation is queued: snapmirror initialize of destination "vsd:dst".
```

## FlexGroup ボリュームの一元化されたデータ保護関係を作成

ONTAP 9.3 以降では、SnapMirror の一元化されたデータ保護関係を作成して設定することで、同じデスティネーションボリュームにディザスタリカバリとアーカイブを設定することができます。

### 必要なもの

FlexGroup ボリュームの一元化されたデータ保護関係の作成に関する考慮事項を確認しておく必要があります。

"FlexGroup ボリュームの SnapVault バックアップ関係および一元化されたデータ保護関係を作成する際の考慮事項について説明します"

### 手順

1. タイプがのデスティネーションFlexGroup ボリュームを作成します DP ソースFlexGroup と同じ数のコンスティチュエントを含むデータセンターを作成します。
  - a. ソースクラスタから、ソースFlexGroup ボリュームのコンスティチュエントの数を確認します。  
`volume show -volume volume_name* -is-constituent true`

```
cluster1::> volume show -volume srcFG* -is-constituent true
```

Vserver	Volume	Aggregate	State	Type	Size
Available	Used%				
-----	-----	-----	-----	-----	-----
vss	srcFG	-	online	RW	400TB
172.86GB	56%				
vss	srcFG__0001	Aggr_cmode	online	RW	25GB
10.86TB	56%				
vss	srcFG__0002	aggr1	online	RW	25TB
10.86TB	56%				
vss	srcFG__0003	Aggr_cmode	online	RW	25TB
10.72TB	57%				
vss	srcFG__0004	aggr1	online	RW	25TB
10.73TB	57%				
vss	srcFG__0005	Aggr_cmode	online	RW	25TB
10.67TB	57%				
vss	srcFG__0006	aggr1	online	RW	25TB
10.64TB	57%				
vss	srcFG__0007	Aggr_cmode	online	RW	25TB
10.63TB	57%				
...					

- b. デスティネーションクラスタから、タイプがのデスティネーションFlexGroup ボリュームを作成します DP ソースFlexGroup と同じ数のコンスティチュエントで構成されています。

```
cluster2::> volume create -vserver vsd -aggr-list aggr1,aggr2 -aggr
-list-multiplier 8 -size 400TB -type DP dstFG
```

Warning: The FlexGroup volume "dstFG" will be created with the following number of constituents of size 25TB: 16.

Do you want to continue? {y|n}: y

[Job 766] Job succeeded: Successful

- c. デスティネーションクラスタから、デスティネーションFlexGroup ボリュームのコンスティチュエントの数を確認します。 volume show -volume volume\_name\* -is-constituent true

```
cluster2::> volume show -volume dstFG* -is-constituent true
```

Vserver	Volume	Aggregate	State	Type	Size
Available	Used%				
-----	-----	-----	-----	-----	-----
-----	-----				
vsd	dstFG	-	online	RW	400TB
172.86GB	56%				
vsd	dstFG__0001	Aggr_cmode	online	RW	25GB
10.86TB	56%				
vsd	dstFG__0002	aggr1	online	RW	25TB
10.86TB	56%				
vsd	dstFG__0003	Aggr_cmode	online	RW	25TB
10.72TB	57%				
vsd	dstFG__0004	aggr1	online	RW	25TB
10.73TB	57%				
vsd	dstFG__0005	Aggr_cmode	online	RW	25TB
10.67TB	57%				
vsd	dstFG__0006	aggr1	online	RW	25TB
10.64TB	57%				
vsd	dstFG__0007	Aggr_cmode	online	RW	25TB
10.63TB	57%				
...					

2. ジョブスケジュールを作成します。 `job schedule cron create -name job_name -month month -dayofweek day_of_week -day day_of_month -hour hour -minute minute`

をクリックします `-month`、`-dayofweek` および `-hour` オプションを指定できます all ジョブを毎月、毎日、および1時間ごとに実行します。

次の例は、という名前のジョブスケジュールを作成します `my_weekly` 土曜日の午前3時に実行されます。

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

3. タイプがのカスタムポリシーを作成します `mirror-vault` をクリックし、ミラーとバックアップポリシーのルールを定義します。
- タイプがのカスタムポリシーを作成します `mirror-vault` 一元化されたデータ保護関係の場合：  
`snapmirror policy create -vserver svm_name -policy policy_name -type mirror-vault`
  - 初期化と更新の際にどのSnapshotコピーを転送するかを決定する、ミラーとバックアップポリシーのルールを定義します。 `snapmirror policy add-rule -vserver svm_name -policy policy_for_rule - snapmirror-label snapmirror-label -keep retention_count -schedule schedule`

カスタムポリシーを指定しない場合は、MirrorAndVault ポリシーは一元化されたデータ保護関係に使用されます。

4. 一元化されたデータ保護関係を作成します。snapmirror create -source-path src\_svm:src\_flexgroup -destination-path dest\_svm:dest\_flexgroup -type XDP -schedule schedule\_name -policy MirrorAndVault

ONTAP 9.4以前では、でポリシーが指定されていない場合 snapmirror create コマンドを入力します MirrorAllSnapshots デフォルトではポリシーが使用されます。ONTAP 9.5では、でポリシーが指定されていない場合 snapmirror create コマンドを入力します MirrorAndVault デフォルトではポリシーが使用されます。

```
cluster2::> snapmirror create -source-path vss:srcFG -destination-path  
vsd:dstFG -type XDP -schedule Daily -policy MirrorAndVault
```

5. デスティネーションクラスタから、ベースライン転送を実行して一元化されたデータ保護関係を初期化します。snapmirror initialize -destination-path dest\_svm:dest\_flexgroup

```
cluster2::> snapmirror initialize -destination-path vsd:dstFG  
Operation is queued: snapmirror initialize of destination "vsd:dstFG".
```

## FlexGroup ボリュームの SVM ディザスタリカバリ関係を作成します

ONTAP 9.9.1以降では、FlexGroup ボリュームを使用してSVMディザスタリカバリ (SVM DR) 関係を作成できます。SVM DR 関係は、SVM の設定とそのデータを同期およびレプリケートすることで、災害発生時に冗長性を確保し、FlexGroup をリカバリする機能を提供します。SVM DR には SnapMirror ライセンスが必要です。

作業を開始する前に

次の条件に該当する場合は、FlexGroup SVM DR関係を作成できません。

- FlexClone FlexGroup 設定が存在します
- FlexGroupボリュームはカスケード関係の一部です
- FlexGroupボリュームはファンアウト関係の一部であり、クラスタでONTAP 9.12.1より前のバージョンのONTAPが実行されている。(ONTAP 9.13.1以降では、ファンアウト関係がサポートされます)。

このタスクについて

- 両方のクラスタのすべてのノードで、SVM DR がサポートされているノードと同じバージョンの ONTAP を実行している必要があります (ONTAP 9.9.1 以降)。
- プライマリサイトとセカンダリサイト間の SVM DR 関係が正常であり、FlexGroup ボリュームをサポートするための十分なスペースがプライマリとセカンダリの両方の SVM に必要です。
- ONTAP 9.12.1以降では、FabricPool、FlexGroup、およびSVM DRを連動させることができます。ONTAP 9.12.1よりも前のリリースでは、これらの機能のいずれか2つが連携して動作していましたが、3つすべてが連携しているわけではありません。

- ファンアウト関係の一部であるFlexGroup SVM DR関係を作成する場合はFlexGroup、次の要件に注意してください。
  - ソースクラスタとデスティネーションクラスタでONTAP 9.13.1以降が実行されている必要があります。
  - FlexGroup を備えたSVM DRでは、8サイトへのSnapMirrorファンアウト関係がサポートされます。

SVM DR 関係の作成の詳細については、を参照してください ["SnapMirror SVM レプリケーションを管理します"](#)。

#### 手順

1. SVM DR 関係を作成するか、既存の関係を使用します。

#### "SVM の設定全体をレプリケート"

2. 必要な数のコンスティチュエントを含む FlexGroup ボリュームをプライマリサイトに作成します。

#### "FlexGroup ボリュームを作成します"。

FlexGroup とそのすべてのコンスティチュエントが作成されるまで待ってから次に進みます。

3. FlexGroup ボリュームをレプリケートするには、セカンダリサイトでSVMを更新します。 `snapmirror update -destination-path destination_svm_name: -source-path source_svm_name:`

スケジュールされたSnapMirror更新がすでに存在するかどうかを確認するには、と入力します

```
snapmirror show -fields schedule
```

4. セカンダリサイトで、SnapMirror関係が正常であることを確認します。 `snapmirror show`

```
cluster2::> snapmirror show
```

Progress

Source	Destination	Mirror	Relationship	Total
Last				
Path	Type	Path	State	Status
Updated				
-----	-----	-----	-----	-----
-----				
vs1:	XDP	vs1_dst:	Snapmirrored	
			Idle	-
				true
				-

5. セカンダリサイトで、新しいFlexGroup ボリュームとそのコンスティチュエントが存在することを確認します。 `snapmirror show -expand`

```
cluster2::> snapmirror show -expand
```

```
Progress
Source          Destination Mirror Relationship Total
Last
Path            Type  Path            State  Status          Progress Healthy
Updated
-----
-----
vs1:             XDP  vs1_dst:        Snapmirrored
                               Idle          -          true  -
vs1:fg_src       XDP  vs1_dst:fg_src  Snapmirrored
                               Idle          -          true  -
vs1:fg_src__0001 XDP  vs1_dst:fg_src__0001
                               Snapmirrored
                               Idle          -          true  -
vs1:fg_src__0002 XDP  vs1_dst:fg_src__0002
                               Snapmirrored
                               Idle          -          true  -
vs1:fg_src__0003 XDP  vs1_dst:fg_src__0003
                               Snapmirrored
                               Idle          -          true  -
vs1:fg_src__0004 XDP  vs1_dst:fg_src__0004
                               Snapmirrored
                               Idle          -          true  -
6 entries were displayed.
```

既存の **FlexGroup SnapMirror** 関係を **SVM DR** に移行します

FlexGroup SVM DR 関係を作成するには、既存の FlexGroup Volume SnapMirror 関係を移行します。

必要なもの

- FlexGroup Volume SnapMirror 関係は正常な状態です。
- ソース FlexGroup ボリュームとデスティネーション ボリュームの名前が同じです。

手順

1. SnapMirrorデスティネーションから、FlexGroup レベルのSnapMirror関係を再同期します。 `snapmirror resync`

- FlexGroup SVM DRのSnapMirror関係を作成FlexGroup Volume SnapMirror関係に設定されているのと同じSnapMirrorポリシーを使用します。 `snapmirror create -destination-path dest_svm: -source-path src_svm: -identity-preserve true -policy MirrorAllSnapshots`



を使用する必要があります `-identity-preserve true` のオプション `snapmirror create` コマンドを使用してレプリケーション関係を作成します。

- 関係が解除されていることを確認します。 `snapmirror show -destination-path dest_svm: -source-path src_svm:`

```
snapmirror show -destination-path fg_vs_renamed: -source-path fg_vs:
```

Progress

Source	Destination	Mirror	Relationship	Total
Last Path	Type	Path	State	Status
Updated				Progress
fg_vs:	XDP	fg_vs1_renamed:	Broken-off	
			Idle	-
				true

- デスティネーション SVM を停止します。 `vserver stop -vserver vs_name`

```
vserver stop -vserver fg_vs_renamed
[Job 245] Job is queued: Vserver Stop fg_vs_renamed.
[Job 245] Done
```

- SVM SnapMirror関係を再同期します。 `snapmirror resync -destination-path dest_svm: -source-path src_svm:`

```
snapmirror resync -destination-path fg_vs_renamed: -source-path fg_vs:
Warning: This Vserver has volumes which are the destination of FlexVol
or FlexGroup SnapMirror relationships. A resync on the Vserver
SnapMirror relationship will cause disruptions in data access
```

- SVM DRレベルのSnapMirror関係が正常なアイドル状態になっていることを確認します。 `snapmirror show -expand`
- FlexGroup SnapMirror関係が健全な状態であることを確認します。 `snapmirror show`



**FlexGroup** ボリュームを **SVM-DR** 関係内で **FlexVol** ボリュームに変換します

ONTAP 9.10.1 以降では、FlexVol ボリュームを SVM-DR ソース上の FlexGroup ボリュームに変換できます。

必要なもの

- 変換する FlexVol がオンラインになっている必要があります。
- FlexVol ボリュームの処理と設定が変換プロセスに対応している必要があります。

FlexVol ボリュームに互換性の問題があり、ボリューム変換がキャンセルされた場合は、エラーメッセージが生成されます。対処方法を実行し、変換を再試行できます。

詳細については、を参照してください [FlexVol ボリュームを FlexGroup ボリュームに変換する際の考慮事項](#)

手順

1. advanced権限モードでログインします。 `set -privilege advanced`
2. デスティネーションから、SVM-DR 関係を更新します。

```
snapmirror update -destination-path destination_svm_name: -source-path source_svm_name:
```

3. SVM-DR 関係が SnapMirrored 状態であり、かつ切断されていないことを確認します。

```
snapmirror show
```

4. デスティネーション SVM から、FlexVol ボリュームで変換の準備が完了していることを確認します。

```
volume conversion start -vserver svm_name -volume vol_name -check-only true
```

このコマンドで「This is a destination SVM-DR volume」以外のエラーが発生した場合は、該当する対処方法を実行し、コマンドをもう一度実行して変換を続行します。

5. デスティネーションから、SVM-DR 関係の転送を無効にします。

```
snapmirror quiesce -destination-path dest_svm:
```

6. 変換を開始します。

```
volume conversion start -vserver svm_name -volume vol_name
```

7. 変換が正常に完了したことを確認します。

```
volume show vol_name -fields -volume-style-extended,state
```

```
cluster-1::*> volume show my_volume -fields volume-style-extended,state
```

vserver	volume	state	volume-style-extended
vs0	my_volume	online	flexgroup

8. デスティネーションクラスタから、関係の転送を再開します。

```
snapmirror resume -destination-path dest_svm:
```

9. デスティネーションクラスタから更新を実行して、変換をデスティネーションに伝播します。

```
snapmirror update -destination-path dest_svm:
```

10. SVM-DR 関係が SnapMirrored 状態であり、かつ切断されていないことを確認します。

```
snapmirror show
```

11. 変換がデスティネーションで行われたことを確認します。

```
volume show vol_name -fields -volume-style-extended,state
```

```
cluster-2::*> volume show my_volume -fields volume-style-extended,state
```

vserver	volume	state	volume-style-extended
vs0_dst	my_volume	online	flexgroup

## FlexGroup の SnapMirror カスケード関係とファンアウト関係の作成に関する考慮事項

FlexGroup の SnapMirror カスケード関係とファンアウト関係を作成する場合は、サポートに関する考慮事項と制限事項に注意する必要があります。

### カスケード関係の作成に関する考慮事項

- 各関係は、クラスタ間関係またはクラスタ内関係のどちらかになります。
- 両方の関係で、async-mirror、mirror-vault、バックアップなどのすべての非同期ポリシータイプがサポートされます。
- サポートされる非同期ミラーポリシーは「MirrorAllSnapshots」のみで、「MirrorLatest」はサポートされません。
- カスケードされた XDP 関係の同時更新がサポートされます。
- A から B へ、B から C への再同期、または C から A への再同期をサポートします
- また、すべてのノードで ONTAP 9.9.1 以降を実行している場合は、A と B の FlexGroup ボリュームでもファンアウトがサポートされます。

- B または C の FlexGroup ボリュームからのリストア処理がサポートされます。
- デスティネーションがリストア関係のソースである間は、FlexGroup 関係の転送はサポートされません。
- FlexGroup リストアのデスティネーションを他の FlexGroup 関係のデスティネーションにすることはできません。
- FlexGroup ファイルのリストア処理には、通常の FlexGroup リストア処理と同じ制限事項があります。
- B および C の FlexGroup ボリュームが配置されているクラスタ内のすべてのノードで ONTAP 9.9.1 以降が実行されている必要があります。
- すべての拡張機能と自動拡張機能がサポートされています。
- A から B、C へのカスケード構成で、A から B、B から C へのコンスティチュエント SnapMirror 関係の数が異なる場合、ソースから C への SnapMirror 関係の中止はサポートされません。
- ONTAP 9.9.1では、System Managerでカスケード関係はサポートされません。
- A から B への FlexVol 関係の C セットを FlexGroup 関係に変換する場合は、まず B を C ホップに変換する必要があります。
- REST でサポートされるポリシータイプを使用する関係の FlexGroup カスケード構成は、カスケード FlexGroup 構成の REST API でもサポートされます。
- FlexVol 関係と同様に、FlexGroup カスケードはサポートされません `snapmirror protect` コマンドを実行します

#### ファンアウト関係の作成に関する考慮事項

- 2 つ以上の FlexGroup ファンアウト関係がサポートされます。たとえば、A ~ B、A ~ C、最大 8 つのファンアウトレッグがあります。
- それぞれの関係は、クラスタ間でもクラスタ内でもかまいません。
- この 2 つの関係については、同時更新がサポートされています。
- すべての拡張機能と自動拡張機能がサポートされています。
- 関係のファンアウト脚でコンスティチュエント SnapMirror 関係の数が異なる場合は、A から B、および A から C の関係に対してソースから中止処理を実行することはできません。
- ソースとデスティネーションの FlexGroup が配置されているクラスタ内のすべてのノードで ONTAP 9.9.1 以降が実行されている必要があります。
- 現在 FlexGroup SnapMirror でサポートされているすべての非同期ポリシータイプが、ファンアウト関係でサポートされています。
- B から C の FlexGroup へのリストア処理を実行できます。
- FlexGroup ファンアウト構成で REST API でも、ポリシータイプのファンアウト構成をサポートしています。

**FlexGroup** ボリュームの **SnapVault** バックアップ関係および一元化されたデータ保護関係を作成する際の考慮事項について説明します

FlexGroup ボリュームの SnapVault バックアップ関係および一元化されたデータ保護関係の作成に関する考慮事項を確認しておく必要があります。

- を使用して、SnapVault バックアップ関係と一元化されたデータ保護関係を再同期できます `-preserve` 最新の共通の Snapshot コピーよりも新しい Snapshot コピーをデスティネーションボリュームに保持でき

ます。

- 長期保持は FlexGroup ボリュームではサポートされません。

長期保持では Snapshot コピーをデスティネーションボリュームに直接作成でき、ソースボリュームに格納する必要はありません。

- snapshot コマンドを実行します expiry-time オプションは FlexGroup ボリュームではサポートされません。
- Storage Efficiency は、SnapVault バックアップ関係および一元化されたデータ保護関係のデスティネーション FlexGroup には設定できません。
- FlexGroup バックアップ関係および SnapVault ボリュームの一元化されたデータ保護関係の Snapshot コピーは、名前を変更できません。
- 1 つの FlexGroup ボリュームをソースボリュームにできるのは、1 つのバックアップ関係またはリストア関係だけです。

2 つの SnapVault 関係、2 つのリストア関係、または SnapVault バックアップ関係とリストア関係のソースにすることはできません。FlexGroup

- ソース FlexGroup ボリュームで Snapshot コピーを削除したあとに同じ名前で Snapshot コピーを作成した場合、デスティネーションボリュームに同じ名前の Snapshot コピーがあると、デスティネーション FlexGroup ボリュームへの次の更新転送が失敗します。

これは、FlexGroup ボリュームの Snapshot コピーの名前は変更できないためです。

## FlexGroup ボリュームの SnapMirror データ転送を監視する

FlexGroup Volume SnapMirror 関係のステータスを定期的に監視して、デスティネーション FlexGroup ボリュームが指定したスケジュールに従って定期的に更新されていることを確認する必要があります。

このタスクについて

この手順はデスティネーションクラスタで実行する必要があります。

手順

1. すべての FlexGroup ボリューム関係の SnapMirror 関係ステータスを表示します。snapmirror show -relationship-group-type flexgroup

```
cluster2::> snapmirror show -relationship-group-type flexgroup
```

Progress

Source	Destination	Mirror	Relationship	Total
--------	-------------	--------	--------------	-------

Last

Path	Type	Path	State	Status	Progress	Healthy
------	------	------	-------	--------	----------	---------

Updated

vss:s	XDP	vsd:d	Snapmirrored	Idle	-	true	-
vss:s2	XDP	vsd:d2	Uninitialized	Idle	-	true	-

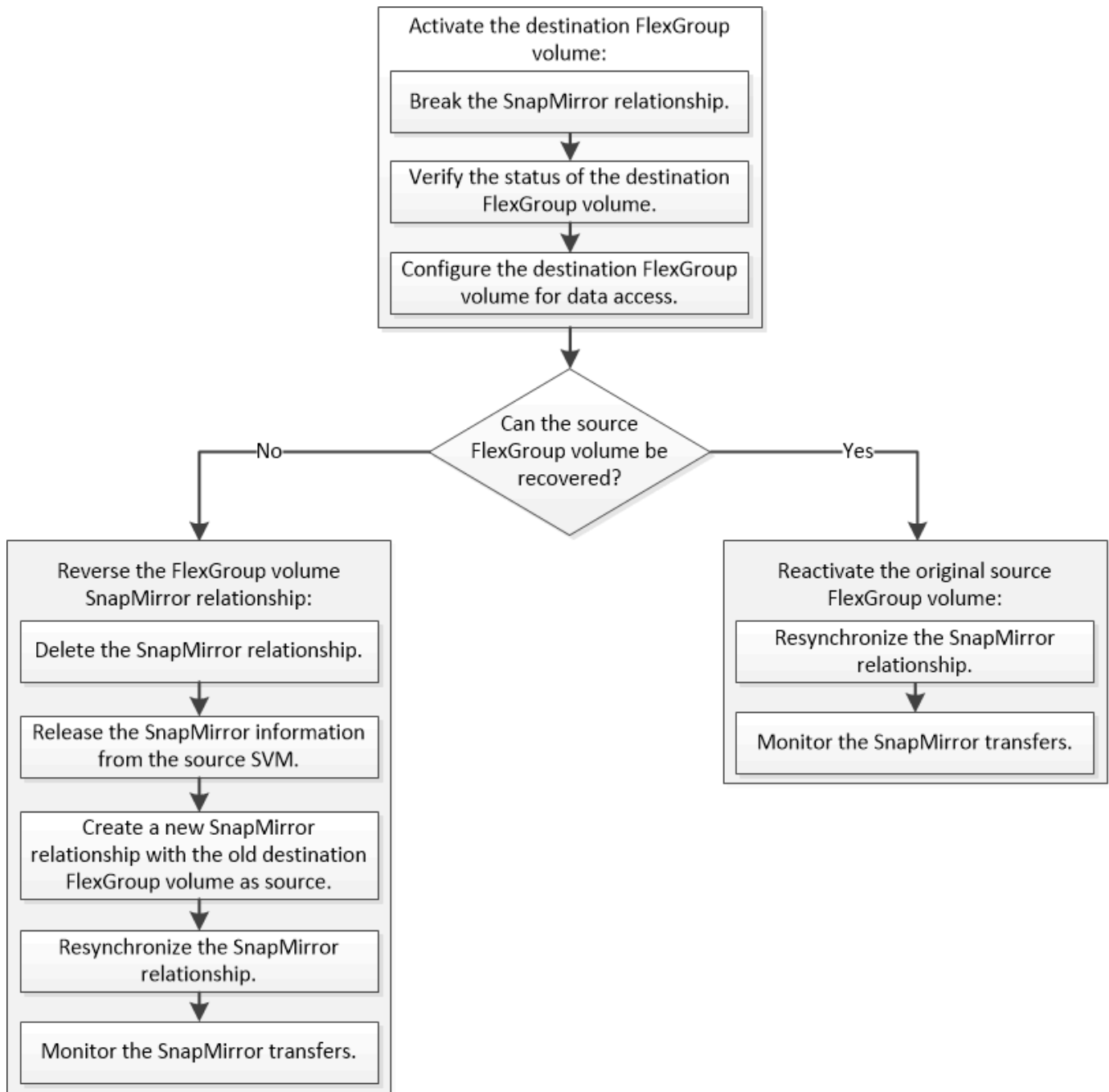
2 entries were displayed.

## FlexGroup ボリュームに対するデータ保護処理を管理します

### FlexGroup ボリュームのディザスタリカバリ

#### FlexGroup ボリュームのディザスタリカバリワークフロー

ソース FlexGroup ボリュームで災害が発生した場合は、デスティネーション FlexGroup をアクティブ化してクライアントアクセスをリダイレクトします。ソース FlexGroup ボリュームをリカバリできるかどうかに応じて、ソース FlexGroup ボリュームを再アクティブ化するか、SnapMirror 関係を反転させる必要があります。



#### このタスクについて

SnapMirror の解除と再同期など、一部の SnapMirror 処理の実行中は、デスティネーション FlexGroup ボリュームへのクライアントアクセスが一時的にブロックされます。SnapMirror 処理に失敗した場合、一部のコンスチチュエントがその状態のまま残り、FlexGroup ボリュームへのアクセスが拒否されることがあります。このような場合は、SnapMirror 処理を再試行する必要があります。

#### デスティネーション **FlexGroup** ボリュームをアクティブ化

データが破損した場合や誤って削除した場合、あるいはオフライン状態の場合など、データをソース FlexGroup から提供できないときは、ソース FlexGroup ボリュームのデータをリカバリするまでの間、デスティネーション FlexGroup ボリュームをアクティブ化してデータアクセスを提供する必要があります。アクティブ化には、以降の SnapMirror

データ転送の中止と、 SnapMirror 関係の解除が伴います。

このタスクについて

この手順はデスティネーションクラスタで実行する必要があります。

手順

1. FlexGroup Volume SnapMirror関係の以降の転送を無効にします。 `snapmirror quiesce dest_svm:dest_flexgroup`

```
cluster2::> snapmirror quiesce -destination-path vsd:dst
```

2. FlexGroup Volume SnapMirror関係を解除します。 `snapmirror break dest_svm:dest_flexgroup`

```
cluster2::> snapmirror break -destination-path vsd:dst
```

3. SnapMirror関係のステータスを表示します。 `snapmirror show -expand`

```
cluster2::> snapmirror show -expand
```

Progress	Source	Destination	Mirror	Relationship	Total		
Last	Path	Type	Path	State	Status	Progress	Healthy
Updated							
-----	-----	-----	-----	-----	-----	-----	-----
-----	vss:s	XDP	vsd:dst	Broken-off			
				Idle	-	true	-
	vss:s__0001	XDP	vsd:dst__0001	Broken-off			
				Idle	-	true	-
	vss:s__0002	XDP	vsd:dst__0002	Broken-off			
				Idle	-	true	-
	vss:s__0003	XDP	vsd:dst__0003	Broken-off			
				Idle	-	true	-
	vss:s__0004	XDP	vsd:dst__0004	Broken-off			
				Idle	-	true	-
	vss:s__0005	XDP	vsd:dst__0005	Broken-off			
				Idle	-	true	-
	vss:s__0006	XDP	vsd:dst__0006	Broken-off			
				Idle	-	true	-
	vss:s__0007	XDP	vsd:dst__0007	Broken-off			
				Idle	-	true	-
	vss:s__0008	XDP	vsd:dst__0008	Broken-off			
				Idle	-	true	-
...							

各コンスティチュエントのSnapMirror関係のステータスはです Broken-off。

4. デスティネーションFlexGroup ボリュームが読み取り/書き込み可能であることを確認します。 volume show -vserver svm\_name



```
cluster2::> volume show -vserver vsd
```

Vserver	Volume	Aggregate	State	Type	Size
Available	Used%				
vsd	dst	-	online	**RW**	2GB
1.54GB	22%				
vsd	d2	-	online	DP	2GB
1.55GB	22%				
vsd	root_vs0	aggr1	online	RW	100MB
94.02MB	5%				

3 entries were displayed.

5. デスティネーション FlexGroup ボリュームにクライアントをリダイレクトします。

災害発生後に元のソース **FlexGroup** ボリュームを再アクティブ化します

ソース FlexGroup ボリュームが使用可能になったら、元のソース FlexGroup ボリュームと元のデスティネーション ボリュームを再同期できます。デスティネーション FlexGroup ボリュームの新しいデータはすべて失われます。

このタスクについて

再同期が実行される前に、デスティネーションボリュームのアクティブなクォータルールは非アクティブ化され、削除されます。

を使用できます `volume quota policy rule create` および `volume quota modify` 再同期処理の完了後にクォータルールを作成して再アクティブ化するコマンド。

手順

1. デスティネーションクラスタから、FlexGroup Volume SnapMirror関係を再同期します。 `snapmirror resync -destination-path dst_svm:dest_flexgroup`
2. SnapMirror関係のステータスを表示します。 `snapmirror show -expand`

```
cluster2::> snapmirror show -expand
```

Progress

Source		Destination	Mirror	Relationship	Total	
Last						
Path	Type	Path	State	Status	Progress	Healthy
Updated						
-----	----	-----	-----	-----	-----	-----
vss:s	XDP	vsd:dst	Snapmirrored			
			Idle		-	true -
vss:s__0001	XDP	vsd:dst__0001	Snapmirrored			
			Idle		-	true -
vss:s__0002	XDP	vsd:dst__0002	Snapmirrored			
			Idle		-	true -
vss:s__0003	XDP	vsd:dst__0003	Snapmirrored			
			Idle		-	true -
vss:s__0004	XDP	vsd:dst__0004	Snapmirrored			
			Idle		-	true -
vss:s__0005	XDP	vsd:dst__0005	Snapmirrored			
			Idle		-	true -
vss:s__0006	XDP	vsd:dst__0006	Snapmirrored			
			Idle		-	true -
vss:s__0007	XDP	vsd:dst__0007	Snapmirrored			
			Idle		-	true -
vss:s__0008	XDP	vsd:dst__0008	Snapmirrored			
			Idle		-	true -
...						

各コンスティチュエントのSnapMirror関係のステータスはです Snapmirrored。

ディザスタリカバリ時に **FlexGroup** ボリューム間の **SnapMirror** 関係を反転する

災害によって SnapMirror 関係のソース FlexGroup が機能しなくなった場合、ソース FlexGroup ボリュームの修理や交換を行う間、デスティネーション FlexGroup ボリュームを使用してデータを提供できます。ソース FlexGroup ボリュームがオンラインになったら、元のソース FlexGroup ボリュームを読み取り専用のデスティネーションにして、SnapMirror 関係を反転できます。

このタスクについて

再同期が実行される前に、デスティネーションボリュームのアクティブなクォータールールは非アクティブ化され、削除されます。

を使用できます volume quota policy rule create および volume quota modify 再同期処理の完了後にクォータールールを作成して再アクティブ化するコマンド。

## 手順

1. 元のデスティネーションFlexGroup ボリュームで、ソースFlexGroup ボリュームとデスティネーションFlexGroup ボリュームの間のデータ保護ミラー関係を削除します。 `snapmirror delete -destination-path svm_name:volume_name`

```
cluster2::> snapmirror delete -destination-path vsd:dst
```

2. 元のソースFlexGroup ボリュームで、ソースFlexGroup ボリュームから関係の情報を削除します。  
`snapmirror release -destination-path svm_name:volume_name -relationship-info -only`

SnapMirror 関係を削除したあと、再同期処理を実行する前に、ソース FlexGroup ボリュームから関係の情報を削除する必要があります。

```
cluster1::> snapmirror release -destination-path vsd:dst -relationship  
-info-only true
```

3. 新しいデスティネーションFlexGroup で、ミラー関係を作成します。 `snapmirror create -source -path src_svm_name:volume_name -destination-path dst_svm_name:volume_name -type XDP -policy MirrorAllSnapshots`

```
cluster1::> snapmirror create -source-path vsd:dst -destination-path  
vss:src -type XDP -policy MirrorAllSnapshots
```

4. 新しいデスティネーションFlexGroup ボリュームで、ソースFlexGroup を再同期します。 `snapmirror resync -source-path svm_name:volume_name`

```
cluster1::> snapmirror resync -source-path vsd:dst
```

5. SnapMirror転送を監視します。 `snapmirror show -expand`

```
cluster2::> snapmirror show -expand
```

```
Progress
Source          Destination Mirror Relationship Total
Last
Path            Type Path            State Status           Progress Healthy
Updated
-----
-----
vsd:dst          XDP  vss:src          Snapmirrored
                  Idle           -             true  -
vss:dst__0001 XDP  vss:src__0001 Snapmirrored
                  Idle           -             true  -
vss:dst__0002 XDP  vss:src__0002 Snapmirrored
                  Idle           -             true  -
vss:dst__0003 XDP  vss:src__0003 Snapmirrored
                  Idle           -             true  -
vss:dst__0004 XDP  vss:src__0004 Snapmirrored
                  Idle           -             true  -
vss:dst__0005 XDP  vss:src__0005 Snapmirrored
                  Idle           -             true  -
vss:dst__0006 XDP  vss:src__0006 Snapmirrored
                  Idle           -             true  -
vss:dst__0007 XDP  vss:src__0007 Snapmirrored
                  Idle           -             true  -
vss:dst__0008 XDP  vss:src__0008 Snapmirrored
                  Idle           -             true  -
...
```

各コンスティチュエントのSnapMirror関係のステータスはになります Snapmirrored は、再同期が成功したことを示します。

## SnapMirror 関係にある FlexGroup ボリュームを展開します

SnapMirror 関係にある FlexGroup ボリュームを展開します

ONTAP 9.3 以降では、 SnapMirror 関係にあるソースの FlexGroup ボリュームとデスティネーションの FlexGroup ボリュームに新しいコンスティチュエントを追加することで、それらのボリュームを拡張することができます。デスティネーションボリュームは、手動で拡張することも自動で拡張することもできます。

このタスクについて

- 拡張後、 SnapMirror 関係のソース FlexGroup ボリュームとデスティネーション FlexGroup ボリュームでコンスティチュエントの数が一致している必要があります。

ボリューム内のコンスティチュエントの数が一致していないと、SnapMirror 転送は失敗します。

- 拡張プロセスの実行中は SnapMirror 処理は実行しないでください。
- 拡張プロセスが完了する前に災害が発生した場合は、SnapMirror 関係を解除し、その処理が完了するまで待つ必要があります。



拡張プロセスの実行中に SnapMirror 関係を解除するのは、災害が発生した場合のみにしてください。災害が発生した場合の解除処理にはしばらく時間がかかることがあります。解除処理が完了してから再同期処理を実行するようにしてください。解除処理が失敗した場合は、解除処理を再試行する必要があります。解除処理に失敗すると、一部の新しいコンスティチュエントがデスティネーション FlexGroup ボリュームに残ることがあります。処理を進める前に、それらのコンスティチュエントを手動で削除することを推奨します。

**SnapMirror** 関係のソース **FlexGroup** ボリュームを拡張します

ONTAP 9.3 以降では、新しいコンスティチュエントをソースボリュームに追加することで、SnapMirror 関係のソース FlexGroup ボリュームを拡張できます。通常の FlexGroup ボリューム（読み書き可能ボリューム）を拡張する場合と同じ方法でソースボリュームを拡張できます。

手順

1. ソース FlexGroup ボリュームを拡張します。 `volume expand -vserver vs_server_name -volume fg_src -aggr-list aggregate name,... [-aggr-list-multiplier constituents_per_aggr]`

```
cluster1::> volume expand -volume src_fg -aggr-list aggr1 -aggr-list
-multiplier 2 -vserver vs_src
```

```
Warning: The following number of constituents of size 50GB will be added
to FlexGroup "src_fg": 2.
```

```
Expanding the FlexGroup will cause the state of all Snapshot copies to
be set to "partial".
```

```
Partial Snapshot copies cannot be restored.
```

```
Do you want to continue? {y|n}: Y
```

```
[Job 146] Job succeeded: Successful
```

ボリュームの拡張前に作成されたすべての Snapshot コピーの状態が「partial」に変わります。

**SnapMirror** 関係のデスティネーション **FlexGroup** ボリュームを拡張します

デスティネーション FlexGroup ボリュームの拡張と SnapMirror 関係の再確立は、自動または手動で実行できます。デフォルトでは、SnapMirror 関係は自動拡張用に設定されており、ソースボリュームが拡張されるとデスティネーション FlexGroup ボリュームも自動的に拡張されます。

必要なもの

- ソース FlexGroup ボリュームが拡張されている必要があります。
- SnapMirror関係がで確立されている必要があります SnapMirrored 状態。

SnapMirror 関係が解除または削除されていない必要があります。

#### このタスクについて

- デスティネーション FlexGroup ボリュームを作成すると、そのボリュームにはデフォルトで自動拡張が設定されます。

必要に応じて、デスティネーション FlexGroup ボリュームを手動拡張に変更できます。



デスティネーション FlexGroup ボリュームは自動的に拡張することを推奨します。

- ソースの FlexGroup ボリュームとデスティネーションの FlexGroup ボリュームの拡張が完了し、コンス ティチュエントの数が同じになるまでは、すべての SnapMirror 処理が失敗します。
- SnapMirror 関係を解除または削除したあとにデスティネーション FlexGroup ボリュームを拡張した場合、元の関係を再同期することはできません。

デスティネーション FlexGroup ボリュームを再利用する場合は、 SnapMirror 関係の削除後にボリューム を拡張しないでください。

#### 選択肢

- 更新の転送を実行し、デスティネーション FlexGroup ボリュームを自動的に拡張します。
  - a. SnapMirror更新の転送を実行します。 `snapmirror update -destination-path svm:vol_name`
  - b. にSnapMirror関係のステータスが表示されていることを確認します SnapMirrored 都道府県：  
`snapmirror show`

```
cluster2::> snapmirror show

Progress
Source          Destination Mirror Relationship Total
Last
Path            Type Path            State Status Progress
Healthy Updated
-----
vs_src:src_fg
                XDP vs_dst:dst_fg
                               Snapmirrored
                               Idle           -           true
-
```

アグリゲートのサイズと可用性に基づいてアグリゲートが自動的に選択され、ソース FlexGroup のコンス

ティチュエントに一致する新しいコンスティチュエントがデスティネーション FlexGroup ボリュームに追加されます。拡張の完了後、再同期処理が自動的に開始されます。

- デスティネーション FlexGroup ボリュームを手動で拡張します。
  - a. SnapMirror関係が自動拡張モードになっている場合は、SnapMirror関係を手動拡張モードに設定します。 `snapmirror modify -destination-path svm:vol_name -is-auto-expand-enabled false`

```
cluster2::> snapmirror modify -destination-path vs_dst:dst_fg -is
-auto-expand-enabled false
Operation succeeded: snapmirror modify for the relationship with
destination "vs_dst:dst_fg".
```

- b. SnapMirror関係を休止します。 `snapmirror quiesce -destination-path svm:vol_name`

```
cluster2::> snapmirror quiesce -destination-path vs_dst:dst_fg
Operation succeeded: snapmirror quiesce for destination
"vs_dst:dst_fg".
```

- c. デスティネーション FlexGroup ボリュームを拡張します。 `volume expand -vserver vs_server_name -volume fg_name -aggr-list aggregate name,... [-aggr-list-multiplier constituents_per_aggr]`

```
cluster2::> volume expand -volume dst_fg -aggr-list aggr1 -aggr-list
-multiplier 2 -vserver vs_dst

Warning: The following number of constituents of size 50GB will be
added to FlexGroup "dst_fg": 2.
Do you want to continue? {y|n}: y
[Job 68] Job succeeded: Successful
```

- d. SnapMirror関係を再同期します。 `snapmirror resync -destination-path svm:vol_name`

```
cluster2::> snapmirror resync -destination-path vs_dst:dst_fg
Operation is queued: snapmirror resync to destination
"vs_dst:dst_fg".
```

- e. SnapMirror関係のステータスがあることを確認します `SnapMirrored: snapmirror show`

```
cluster2::> snapmirror show
```

Progress	Source	Destination	Mirror	Relationship	Total
Last	Path	Type	Path	State	Status
Healthy	Updated				Progress
-----	-----	-----	-----	-----	-----
-----	-----				
vs_src:src_fg	XDP	vs_dst:dst_fg		Snapmirrored	
				Idle	-
-					true

**FlexGroup** から **SnapMirror** による単一ファイルのリストアを実行する

ONTAP 9.8 以降では、FlexGroup の SnapMirror ヴォールトまたは UDP デスティネーションから単一のファイルをリストアできます。

このタスクについて

- 任意の形状の FlexGroup ボリュームから任意の形状の FlexGroup ボリュームにリストアできます
- リストア処理ごとに 1 つのファイルのみがサポートされます
- 元のソース FlexGroup ボリュームにリストアするか、新しい FlexGroup ボリュームにリストアできます
- リモートフェンシングファイルはサポートされていません。

ソースファイルがフェンシングされている場合、単一ファイルのリストアが失敗します。

- 中止した単一ファイルのリストアを再開またはクリーンアップできます
- 単一ファイルのリストア転送に失敗した場合は、を使用してクリーンアップする必要があります `cleanup-failure` のオプション `snapmirror restore` コマンドを実行します
- FlexGroup ボリュームの拡張は、FlexGroup による単一ファイルのリストアが進行中または中止された状態の場合にサポートされます

手順

1. FlexGroup ボリュームからファイルをリストアします。 `snapmirror restore -destination-path destination_path -source-path source_path -file-list /f1 -throttle throttle -source-snapshot snapshot`

次に、FlexGroup ボリュームの単一ファイルのリストア処理の例を示します。

```
vserverA::> snapmirror restore -destination-path vs0:fg2 -source-path vs0:fgd -file-list /f1 -throttle 5 -source-snapshot snapmirror.81072cel-
```



d57b-11e9-94c0-005056a7e422\_2159190496.2019-09-19\_062631

[Job 135] Job is queued: snapmirror restore from source "vs0:fgd" for the snapshot snapmirror.81072ce1-d57b-11e9-94c0-005056a7e422\_2159190496.2019-09-19\_062631.

vserverA::> snapmirror show

Source	Destination	Mirror	Relationship		
Total	Last				
Path	Type	Path	State	Status	Progress
Healthy	Updated				
-----	----	-----		-----	-----
-----	-----	-----			
vs0:v1d	RST	vs0:v2	-	Transferring	Idle 83.12KB
true	09/19 11:38:42				

vserverA::\*> snapmirror show vs0:fg2

Source Path: vs0:fgd  
Source Cluster: -  
Source Vserver: vs0  
Source Volume: fgd  
Destination Path: vs0:fg2  
Destination Cluster: -  
Destination Vserver: vs0  
Destination Volume: fg2  
Relationship Type: RST  
Relationship Group Type: none  
Managing Vserver: vs0  
SnapMirror Schedule: -  
SnapMirror Policy Type: -  
SnapMirror Policy: -  
Tries Limit: -  
Throttle (KB/sec): unlimited  
Current Transfer Throttle (KB/sec): 2  
Mirror State: -  
Relationship Status: Transferring  
File Restore File Count: 1  
File Restore File List: f1  
Transfer Snapshot: snapmirror.81072ce1-d57b-11e9-94c0-005056a7e422\_2159190496.2019-09-19\_062631  
Snapshot Progress: 2.87MB  
Total Progress: 2.87MB  
Network Compression Ratio: 1:1  
Snapshot Checkpoint: 2.97KB  
Newest Snapshot: -  
Newest Snapshot Timestamp: -

```
Exported Snapshot: -
Exported Snapshot Timestamp: -
Healthy: true
Physical Replica: -
Relationship ID: e6081667-dacb-11e9-94c0-005056a7e422
Source Vserver UUID: 81072ce1-d57b-11e9-94c0-005056a7e422
Destination Vserver UUID: 81072ce1-d57b-11e9-94c0-005056a7e422
Current Operation ID: 138f12e6-dacc-11e9-94c0-005056a7e422
Transfer Type: cg_file_restore
Transfer Error: -
Last Transfer Type: -
Last Transfer Error: -
Last Transfer Error Codes: -
Last Transfer Size: -
Last Transfer Network Compression Ratio: -
Last Transfer Duration: -
Last Transfer From: -
Last Transfer End Timestamp: -
Unhealthy Reason: -
Progress Last Updated: 09/19 07:07:36
Relationship Capability: 8.2 and above
Lag Time: -
Current Transfer Priority: normal
SMTape Operation: -
Constituent Relationship: false
Destination Volume Node Name: vserverA
Identity Preserve Vserver DR: -
Number of Successful Updates: 0
Number of Failed Updates: 0
Number of Successful Resyncs: 0
Number of Failed Resyncs: 0
Number of Successful Breaks: 0
Number of Failed Breaks: 0
Total Transfer Bytes: 0
Total Transfer Time in Seconds: 0
Source Volume MSIDs Preserved: -
OpMask: ffffffffffffffff
Is Auto Expand Enabled: -
Source Endpoint UUID: -
Destination Endpoint UUID: -
Is Catalog Enabled: false
```

**SnapVault** バックアップから **FlexGroup** ボリュームをリストアします

SnapVault セカンダリボリューム内の Snapshot コピーから、FlexGroup ボリュームの

フルリストア処理を実行できます。FlexGroup ボリュームは元のソースボリュームにリストアするか、新しい FlexGroup ボリュームにリストアできます。

作業を開始する前に

FlexGroup の SnapVault バックアップからリストアする場合は、一定の考慮事項について理解しておく必要があります。

- SnapVault バックアップからの部分的な Snapshot コピーでサポートされるのはベースラインリストアのみです。  
デスティネーションボリュームのコンスティチュエントの数は、Snapshot コピーが作成された時点のソースボリュームのコンスティチュエントの数と一致する必要があります。
- リストア処理に失敗した場合、リストア処理が完了するまでは他の処理を実行できなくなります。  
リストア処理を再試行するか、を使用してリストア処理を実行できます `cleanup` パラメータ
- 1 つの FlexGroup ボリュームをソースボリュームにできるのは、1 つのバックアップ関係またはリストア関係だけです。  
2 つの SnapVault 関係、2 つのリストア関係、または SnapVault 関係とリストア関係のソースにすることはできません。FlexGroup
- SnapVault のバックアップ処理とリストア処理を同時に実行することはできません。  
ベースラインリストア処理または増分リストア処理が実行中の場合は、バックアップ処理を休止する必要があります。
- 部分的な Snapshot コピーのリストア処理は、デスティネーション FlexGroup から中止する必要があります。  
ソースボリュームから部分的な Snapshot コピーのリストア処理を中止することはできません。
- リストア処理を中止した場合、前回のリストア処理で使用されていた Snapshot コピーでリストア処理を再開する必要があります。

このタスクについて

デスティネーション FlexGroup ボリュームのアクティブなクォータールールは、リストアの実行前に非アクティブ化されます。

を使用できます `volume quota modify` リストア処理の完了後にクォータールールを再アクティブ化するコマンド。

手順

1. FlexGroup ボリュームをリストアします。 `snapmirror restore -source-path src_svm:src_flexgroup -destination-path dest_svm:dest_flexgroup -snapshot snapshot_name`  
`snapshot_name` は、ソースボリュームからデスティネーションボリュームにリストアする Snapshot コピーです。Snapshot コピーを指定しない場合、デスティネーションボリュームは最新の Snapshot コピーからリストアされます。

```
vserverA::> snapmirror restore -source-path vserverB:dstFG -destination
-path vserverA:newFG -snapshot daily.2016-07-15_0010
Warning: This is a disruptive operation and the volume vserverA:newFG
will be read-only until the operation completes
Do you want to continue? {y|n}: y
```

## FlexGroup ボリュームの SVM 保護を無効にする

SVM DRフラグがに設定されている場合 protected FlexGroup ボリュームでは、フラグをunprotectedに設定してSVM DRを無効にすることができます protection FlexGroup ボリューム上。

### 必要なもの

- ・プライマリとセカンダリ間の SVM DR 関係は正常な状態です。
- ・ SVM DR保護パラメータがに設定されている protected。

### 手順

1. を使用して保護を無効にします volume modify コマンドを使用してを変更します vservers-dr-protection パラメータをに設定しますFlexGroup unprotected。

```
cluster2::> volume modify -vservers vs1 -volume fg_src -vservers-dr
-protection unprotected
[Job 5384] Job is queued: Modify fg_src.
[Job 5384] Steps completed: 4 of 4.
cluster2::>
```

2. セカンダリサイトでSVMを更新します。 snapmirror update -destination-path destination\_svm\_name: -source-path Source\_svm\_name:
3. SnapMirror関係が正常であることを確認します。 snapmirror show
4. FlexGroup SnapMirror関係が削除されたことを確認します。 snapmirror show -expand

## FlexGroup ボリュームで SVM 保護を有効にします

SVM DR保護フラグがに設定されている場合 unprotected FlexGroup ボリュームでは、このフラグをに設定できます protected をクリックしてSVM DR保護を有効にします。

### 必要なもの

- ・プライマリとセカンダリ間の SVM DR 関係は正常な状態です。
- ・ SVM DR保護パラメータがに設定されている unprotected。

### 手順

1. を使用して保護を有効にします volume modify を変更します vservers-dr-protection パラメータをに設定しますFlexGroup protected。

```
cluster2::> volume modify -vserver vs1 -volume fg_src -vserver-dr
-protection protected
[Job 5384] Job is queued: Modify fg_src.
[Job 5384] Steps completed: 4 of 4.
cluster2::>
```

2. セカンダリサイトでSVMを更新します。 snapmirror update -destination-path destination\_svm\_name -source-path source\_svm\_name

```
snapmirror update -destination-path vs1_dst: -source-path vs1:
```

3. SnapMirror関係が正常であることを確認します。 snapmirror show

```
cluster2::> snapmirror show
```

Progress		Destination Mirror		Relationship	Total		
Source							
Last							
Path	Type	Path	State	Status	Progress	Healthy	
Updated							
-----	----	-----	-----	-----	-----	-----	
-----							
vs1:	XDP	vs1_dst:	Snapmirrored				
			Idle		-	true	-

4. FlexGroup SnapMirror関係が正常であることを確認します。 snapmirror show -expand

```
cluster2::> snapmirror show -expand
```

```
Progress
Source          Destination Mirror Relationship Total
Last
Path            Type Path            State Status Progress Healthy
Updated
-----
-----
vs1:            XDP vs1_dst:      Snapmirrored
                                Idle - true -
vs1:fg_src     XDP vs1_dst:fg_src
                                Snapmirrored
                                Idle - true -
vs1:fg_src__0001
                XDP vs1_dst:fg_src__0001
                                Snapmirrored
                                Idle - true -
vs1:fg_src__0002
                XDP vs1_dst:fg_src__0002
                                Snapmirrored
                                Idle - true -
vs1:fg_src__0003
                XDP vs1_dst:fg_src__0003
                                Snapmirrored
                                Idle - true -
vs1:fg_src__0004
                XDP vs1_dst:fg_src__0004
                                Snapmirrored
                                Idle - true -
6 entries were displayed.
```

## FlexVol ボリュームを FlexGroup ボリュームに変換します

FlexVol ボリュームから FlexGroup ボリュームへの変換の概要を参照してください

FlexVol ボリュームをそのスペース制限を超えて拡張する場合は、FlexVol ボリュームを FlexGroup ボリュームに変換できます。ONTAP 9.7 以降では、スタンドアロンの FlexVol ボリュームや SnapMirror 関係にある FlexVol ボリュームを FlexGroup ボリュームに変換できます。

FlexVol ボリュームを FlexGroup ボリュームに変換する際の考慮事項

FlexVol ボリュームを FlexGroup ボリュームに変換する前に、サポートされる機能と処理を確認しておく必要があります。

ONTAP 9.13.1以降では、変換中も自律型ランサムウェア対策を有効にしておくことができます。保護がアクティブな場合は、変換後に元のFlexVolがFlexGroupルートコンスチチュエントになります。保護がアクティブでない場合は、変換時に新しいFlexGroupが作成され、元のFlexVolがルートコンスチチュエントの役割を担います。

変換中は処理がサポートされません

ボリューム変換の実行中は、次の処理は実行できません。

- ボリューム移動
- アグリゲートの自動負荷分散
- アグリゲートの再配置
- ハイアベイラビリティ構成での計画的なテイクオーバーとギブバック
- ハイアベイラビリティ構成での手動および自動のギブバック
- クラスタのアップグレードとリバート
- FlexClone ボリュームのスプリット
- ボリュームをリホスト
- ボリュームの変更とオートサイズ
- ボリュームの名前を変更
- アグリゲートにオブジェクトストアを接続しています
- MetroCluster 構成でのネゴシエートスイッチオーバー
- SnapMirror 処理
- Snapshot コピーからのリストア
- クォータの処理
- ストレージ効率化の処理

これらの処理は、変換の完了後に FlexGroup ボリュームに対して実行できます。

**FlexGroup** ボリュームでサポートされない構成

- オフラインまたは制限状態のボリューム
- SVM ルートボリューム
- SAN
- SMB 1.0
- NVMe ネームスペース
- リモートの Volume Shadow Copy Service (VSS ; ボリュームシャドウコピーサービス)

**FlexVol** ボリュームを **FlexGroup** ボリュームに変換します

ONTAP 9.7 以降では、FlexVol ボリュームから FlexGroup ボリュームへのインプレース変換が可能です。データコピーや追加のディスクスペースは必要ありません。

## 必要なもの

- ONTAP 9.8以降では、移行したボリュームをFlexGroup ボリュームに変換できます。移行したボリュームをFlexGroup に変換する場合は、技術情報アートを参照してください ["移行したFlexVol をFlexGroup に変換する方法"](#) を参照してください。
- 変換する FlexVol がオンラインになっている必要があります。
- FlexVol ボリュームの処理と設定が変換プロセスに対応している必要があります。

FlexVol ボリュームに互換性の問題があり、ボリュームの変換が中止された場合、エラーメッセージが生成されます。対処方法を実行し、変換を再試行できます。

- FlexVol ボリュームが非常に大きく（80<sub>100TB</sub>など）、非常にフル（80<sub>100%</sub>）な場合は、変換せずにデータをコピーする必要があります。



非常に大容量のFlexGroup を変換すると、FlexGroup ボリュームのメンバーコンスティテュエントがいっぱいになり、パフォーマンスの問題が生じる可能性があります。詳細については、TRで「When not to create a FlexGroup volume」を参照してください ["FlexGroup ボリューム-ベストプラクティスおよび実装ガイド"](#)。

## 手順

1. FlexVol ボリュームがオンラインであることを確認します。 `volume show vol_name -volume-style -extended, state`

```
cluster-1::> volume show my_volume -fields volume-style-extended, state
vserver volume      state  volume-style-extended
-----
vs0      my_volume  online flexvol
```

2. FlexVol ボリュームを問題なく変換できるかどうかを確認します。
  - a. advanced権限モードにログインします。 `set -privilege advanced`
  - b. 変換プロセスを確認します。 `volume conversion start -vserver vs1 -volume flexvol -check-only true`

ボリュームを変換する前に、すべてのエラーを修正する必要があります。



FlexGroup ボリュームを FlexVol ボリュームに戻すことはできません。

3. 変換を開始します。 `volume conversion start -vserver svm_name -volume vol_name`



```
cluster-1::*> volume conversion start -vserver vs0 -volume my_volume

Warning: Converting flexible volume "my_volume" in Vserver "vs0" to a
FlexGroup
        will cause the state of all Snapshot copies from the volume to
be set
        to "pre-conversion". Pre-conversion Snapshot copies cannot be
        restored.
Do you want to continue? {y|n}: y
[Job 57] Job succeeded: success
```

4. 変換が正常に完了したことを確認します。 `volume show vol_name -fields -volume-style -extended,state`

```
cluster-1::*> volume show my_volume -fields volume-style-extended,state
vserver volume      state  volume-style-extended
-----
vs0      my_volume online flexgroup
```

#### 結果

FlexVol ボリュームが単一メンバーの FlexGroup ボリュームに変換されます。

#### 完了後

必要に応じて、FlexGroup ボリュームを拡張できます。

#### FlexVol Volume SnapMirror 関係を FlexGroup Volume SnapMirror 関係に変換します

FlexVol Volume SnapMirror 関係を ONTAP で FlexGroup Volume SnapMirror 関係に変換するには、まずデスティネーション FlexVol ボリュームを変換し、そのあとにソース FlexVol ボリュームを変換する必要があります。

#### このタスクについて

- FlexGroup 変換は、非同期 SnapMirror 関係でのみサポートされます。
- 変換時間はいくつかの変数に依存する。変数には次のようなものがあります。
  - コントローラのCPU
  - 他のアプリケーションによるCPU利用率
  - 初期Snapshotコピー内のデータ量
  - ネットワーク帯域幅
  - 他のアプリケーションで使用する帯域幅

#### 作業を開始する前に

- 変換する FlexVol がオンラインになっている必要があります。
- SnapMirror 関係のソース FlexVol を複数の SnapMirror 関係のソースボリュームにすることはできません。

ONTAP 9.9.1以降では、FlexGroup ボリュームでファンアウトSnapMirror関係がサポートされます。詳細については、を参照してください ["FlexGroup の SnapMirror カスケード関係とファンアウト関係の作成に関する考慮事項"](#)。

- FlexVol ボリュームの処理と設定が変換プロセスに対応している必要があります。

FlexVol ボリュームに互換性の問題があり、ボリュームの変換が中止された場合、エラーメッセージが生成されます。対処方法を実行し、変換を再試行できます。

## 手順

1. SnapMirror関係が正常であることを確認します。

```
snapmirror show
```

変換できるのは XDP タイプのミラー関係のみです。

## 例

```
cluster2::> snapmirror show
```

Progress

Source		Destination	Mirror	Relationship	Total		
Last							
Path	Type	Path	State	Status	Progress	Healthy	
Updated							
-----	----	-----	-----	-----	-----	-----	-----
-----							
vs0:src_dp	DP	vs2:dst_dp	Snapmirrored	Idle	-	true	-
vs0:src_xdp	XDP	vs2:dst_xdp	Snapmirrored	Idle	-	true	-

2. ソースボリュームが変換に対応しているかどうかを確認します。

- a. advanced権限モードにログインします。

```
set -privilege advanced
```

- b. 変換プロセスを確認します。

```
volume conversion start -vserver <src_svm_name> -volume <src_vol>
-check-only true
```

例

```
volume conversion start -vserver vs1 -volume src_vol -check-only true
```

+

ボリュームを変換する前に、すべてのエラーを修正する必要があります。

### 3. デスティネーション FlexVol ボリュームを FlexGroup ボリュームに変換します。

#### a. FlexVol SnapMirror関係を休止します。

```
snapmirror quiesce -destination-path <dest_svm:dest_volume>
```

例

```
cluster2::> snapmirror quiesce -destination-path vs2:dst_xdp
```

#### b. 変換を開始します。

```
volume conversion start -vserver <dest_svm> -volume <dest_volume>
```

例

```
cluster-1::> volume conversion start -vserver vs2 -volume dst_xdp
```

Warning: After the volume is converted to a FlexGroup, it will not be possible

to change it back to a flexible volume.

Do you want to continue? {y|n}: y

[Job 510] Job succeeded: SnapMirror destination volume "dst\_xdp" has been successfully converted to a FlexGroup volume.

You must now convert the relationship's source volume, "vs0:src\_xdp", to a FlexGroup.

Then, re-establish the SnapMirror relationship using the "snapmirror resync" command.

### 4. ソース FlexVol ボリュームを FlexGroup ボリュームに変換します。'

```
volume conversion start -vserver <src_svm_name> -volume <src_vol_name>
```

例

```
cluster-1::> volume conversion start -vserver vs0 -volume src_xdp

Warning: Converting flexible volume "src_xdp" in Vserver "vs0" to a
FlexGroup
        will cause the state of all Snapshot copies from the volume to
be set
        to "pre-conversion". Pre-conversion Snapshot copies cannot be
        restored.
Do you want to continue? {y|n}: y
[Job 57] Job succeeded: success
```

## 5. 関係を再同期します。

```
snapmirror resync -destination-path dest_svm_name:dest_volume
```

例

```
cluster2::> snapmirror resync -destination-path vs2:dst_xdp
```

完了後

ソース FlexGroup ボリュームを拡張してコンスティチュエントを追加した場合は、デスティネーションボリュームも拡張する必要があります。

# FlexCache ボリューム管理

## FlexCacheの概要

NetApp FlexCacheテクノロジーは、特にクライアントが同じデータに繰り返しアクセスする必要がある場合に、データアクセスの高速化、WANレイテンシの低減、読み取り処理が大量に発生するワークロードのWAN帯域幅コストの削減を実現します。FlexCacheボリュームを作成する場合は、元のボリュームのアクティブにアクセスされるデータ（ホットデータ）のみを含む既存（元の）ボリュームのリモートキャッシュを作成します。

FlexCacheに含まれるホットデータの読み取り要求を受信した場合、クライアントに到達するまでデータを移動する必要がないため、元のボリュームよりも高速に応答できます。FlexCacheボリュームは、読み取り頻度の低いデータ（コールドデータ）の読み取り要求を受信した場合、元のボリュームから必要なデータを取得し、クライアント要求を処理する前にデータを格納します。以降、そのデータに対する読み取り要求はFlexCacheボリュームから直接提供されます。最初の要求が完了すると、データをネットワーク経由で転送

したり、負荷の高いシステムから提供したりする必要がなくなります。たとえば、単一のアクセスポイントで頻繁に要求されるデータに対して、クラスタ内でボトルネックが発生しているとします。クラスタ内でFlexCacheを使用してホットデータに複数のマウントポイントを提供することで、ボトルネックを軽減し、パフォーマンスを向上させることができます。別の例として、複数のクラスタからアクセスされるボリュームへのネットワークトラフィックを減らす必要があるとします。FlexCacheボリュームを使用して、元のボリュームからネットワーク内のクラスタにホットデータを分散させることができます。これにより、ユーザにより近いアクセスポイントが提供されるため、WANトラフィックが削減されます。

FlexCacheテクノロジーを使用して、クラウド環境やハイブリッドクラウド環境のパフォーマンスを向上させることもできます。FlexCacheボリュームを使用すると、オンプレミスのデータセンターからクラウドにデータをキャッシュすることで、ワークロードをハイブリッドクラウドに移行できます。また、FlexCacheボリュームを使用して、あるクラウドプロバイダから別のクラウドプロバイダへ、または同じクラウドプロバイダの2つのリージョン間でデータをキャッシュすることで、クラウドサイロを解消することもできます。

ONTAP 9.10.1以降では、次のことが可能になります ["グローバルファイルロックを有効にする"](#) すべてのFlexCacheボリューム間。グローバルファイルロックを使用すると、別のユーザがすでに開いているファイルにユーザがアクセスできなくなります。元のボリュームに対する更新は、すべてのFlexCacheボリュームに同時に分散されます。

ONTAP 9.9.1以降では、FlexCacheボリュームで見つからなかったファイルのリストが維持されます。これにより、クライアントが存在しないファイルを検索する際に、複数の呼び出しを送信元に送信する必要がなくなり、ネットワークトラフィックが削減されます。

追加のリスト ["FlexCacheとその元のボリュームでサポートされる機能"](#)ONTAPのバージョン別にサポートされているプロトコルのリストなども参照できます。

ONTAP FlexCacheテクノロジーのアーキテクチャの詳細については、を参照してください。 ["TR-4743 : 『FlexCache in ONTAP』"](#)。

ビデオ

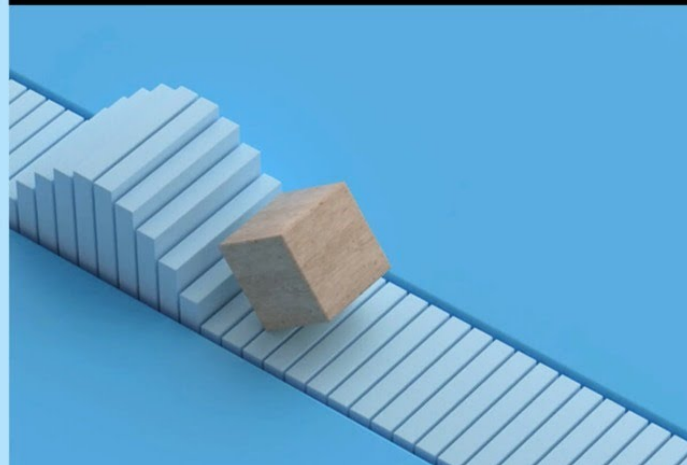
**FlexCache** を使用してグローバルデータの **WAN** レイテンシと読み取り時間を短縮する方法

## ONTAP FlexCache

Data Access Where You Need It

## Use Case

© 2020 NetApp, Inc. All rights reserved.



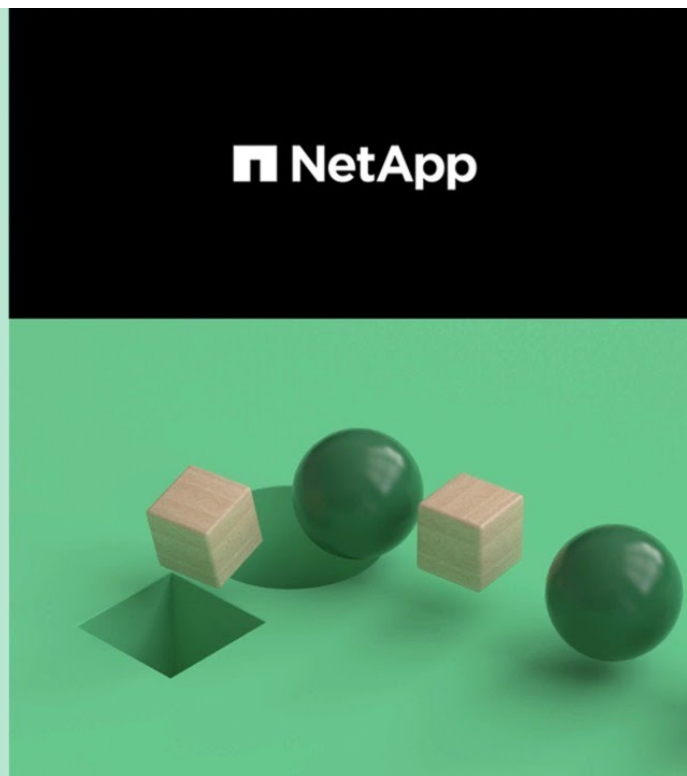
ONTAP FlexCache のパフォーマンス上のメリットをご確認ください。

## ONTAP FlexCache

Data Access Where You Need It

## Tech Clip

© 2020 NetApp, Inc. All rights reserved.



### FlexCache ボリュームでサポートされる機能とサポートされない機能

ONTAP 9.5以降では、FlexCacheボリュームを設定できます。FlexVolボリュームは元のボリュームとして、FlexGroupボリュームはFlexCacheボリュームとしてサポートされま

す。ONTAP 9.7以降では、FlexVolボリュームとFlexGroupボリュームの両方が元のボリュームとしてサポートされます。元のボリュームとFlexCacheボリュームでサポートされる機能とプロトコルは異なります。

#### サポートされているプロトコル

プロトコル	元のボリュームでのサポート	FlexCache ボリュームでのサポート
NFSv3	はい。	はい。
NFSv4	はい。  NFSv4.xプロトコルを使用してキャッシュボリュームにアクセスするには、元のクラスタとキャッシュクラスタの両方でONTAP 9.10.1以降が使用されている必要があります。元のクラスタとFlexCacheクラスタでは異なるONTAPバージョンを使用できますが、どちらもONTAP 9.10.1以降のバージョンである必要があります。たとえば、元のクラスタのONTAPはONTAP 9.10.1、キャッシュの9.11.1などです。	はい。  ONTAP 9.10.1以降でサポートされます。  NFSv4.xプロトコルを使用してキャッシュボリュームにアクセスするには、元のクラスタとキャッシュクラスタの両方でONTAP 9.10.1以降が使用されている必要があります。元のクラスタとFlexCacheクラスタでは異なるONTAPバージョンを使用できますが、どちらもONTAP 9.10.1以降のバージョンである必要があります。たとえば、元のクラスタのONTAPはONTAP 9.10.1、キャッシュの9.11.1などです。
NFSv4.2	はい。	いいえ
SMB	はい。	はい。  ONTAP 9.8 以降でサポートされます。

#### サポートされている機能

フィーチャー（Feature）	元のボリュームでのサポート	FlexCache ボリュームでのサポート
自律型ランサムウェア対策	はい。  ONTAP 9.10.1 以降の FlexVol の元のボリュームでは、FlexGroup の元のボリュームはサポートされません。	いいえ

ウイルス対策	<p>はい。</p> <p>ONTAP 9.7以降でサポートされます。</p>	<p>該当なし</p> <p>オリジンでアンチウイルススキャンを設定する場合、キャッシュでは必要ありません。オリジンのウイルス対策スキャンは、書き込み元に関係なく、書き込みがコミットされる前にウイルスに感染したファイルを検出します。FlexCacheでアンチウイルススキャンを使用する方法の詳細については、<a href="#">を参照してください。"FlexCacheとONTAPのテクニカルレポート"</a>。</p>
監査	<p>はい。</p> <p>ONTAP 9.7以降でサポートされます。</p> <p>標準のONTAP監査を使用して、FlexCache関係におけるNFSファイルアクセスイベントを監査できます。</p> <p>詳細については、<a href="#">を参照してください FlexCache ボリュームの監査に関する考慮事項</a></p>	<p>はい。</p> <p>ONTAP 9.7以降でサポートされます。</p> <p>標準のONTAP監査を使用して、FlexCache関係におけるNFSファイルアクセスイベントを監査できます。</p> <p>詳細については、<a href="#">を参照してください FlexCache ボリュームの監査に関する考慮事項</a></p>
Cloud Volumes ONTAP	<p>はい。</p> <p>ONTAP 9.6以降でサポート</p>	<p>はい。</p> <p>ONTAP 9.6以降でサポート</p>
コンパクション	<p>はい。</p> <p>ONTAP 9.6以降でサポート</p>	<p>はい。</p> <p>ONTAP 9.7 以降でサポートされます</p>
圧縮	<p>はい。</p> <p>ONTAP 9.6以降でサポート</p>	<p>はい。</p> <p>ONTAP 9.6以降でサポート</p>
重複排除	<p>はい。</p>	<p>はい。</p> <p>FlexCache 9.6 以降では、ONTAP ボリュームでインライン重複排除がサポートされます。ONTAP 9.7 以降では、FlexCache ボリュームでボリューム間重複排除がサポートされます。</p>



FabricPool	はい。  ONTAP 9.7 以降でサポートされます	はい。  ONTAP 9.7 以降でサポートされます
FlexCache DR	はい。  ONTAP 9.7 以降でサポートされます	はい。  ONTAP 9.9.1以降でNFSv3プロトコルを使用する場合にのみサポートされます。FlexCache ボリュームは、別々の SVM またはクラスターに配置する必要があります。
FlexGroup ボリューム	はい。  ONTAP 9.7 以降でサポートされます	はい。
FlexVol ボリューム	はい。	いいえ
FPolicy の	はい。  ONTAP 9.7 以降でサポートされます	はい。  ONTAP 9.7以降ではNFSでサポートされます。 ONTAP 9.14.1以降ではSMBでサポートされます。
MetroCluster の設定	はい。  ONTAP 9.7 以降でサポートされます	はい。  ONTAP 9.7 以降でサポートされます
Microsoft オフロードデータ転送 (ODX)	はい。	いいえ
NetApp Aggregate Encryption (NAE)	はい。  ONTAP 9.6以降でサポート	はい。  ONTAP 9.6以降でサポート
NetApp Volume Encryption (NVE)	はい。  ONTAP 9.6以降でサポート	はい。  ONTAP 9.6以降でサポート
ONTAP S3 NASバケット	はい。  ONTAP 9.12.1以降でサポート	いいえ

QoS	はい。	はい。   ファイルレベルの QoS は FlexCache ではサポートされません。
qtree	はい。  ONTAP 9.6以降では、qtreeを作成および変更できます。ソース上に作成されたqtreeには、キャッシュ上でアクセスできます。	いいえ
クォータ	はい。  ONTAP 9.6以降では、FlexCache 元のボリュームでのクォータの適用がユーザとグループでサポートされます。	いいえ  FlexCacheライトアラウンドモード（デフォルトモード）では、キャッシュの書き込みは元のボリュームに転送されます。クォータは元のボリュームで適用されます。   ONTAP 9.6 以降では、FlexCache ボリュームでリモートクォータ（rquota）がサポートされます。
SMB変更通知	はい。	はい。  ONTAP 9.14.1以降では、SMB変更通知がキャッシュでサポートされます。
SnapLock ボリューム	いいえ	いいえ
SnapMirror非同期関係*	はい。	いいえ

	<ul style="list-style-type: none"> <li>• FlexCacheの起源：</li> <li>• 元のFlexVolからFlexCacheボリュームを作成できます。</li> <li>• 元のFlexGroupからFlexCacheボリュームを作成できます。</li> <li>• SnapMirror関係の元のプライマリボリュームからFlexCache ボリュームを作成できます。</li> <li>• ONTAP 9.8 以降では、SnapMirror セカンダリボリュームを FlexCache の元のボリュームにすることができます。</li> </ul>	SnapMirror Synchronous 関係
いいえ	いいえ	SnapRestore
はい。	いいえ	Snapshot コピー
はい。	いいえ	SVM の IP 設定
<p>はい。</p> <p>ONTAP 9.5 以降でサポート。SVM DR 関係のプライマリ SVM に元のボリュームを含めることができます。ただし、SVM DR 関係が解除された場合は、新しい元のボリュームを使用して FlexCache 関係を再作成する必要があります。</p>	<p>いいえ</p> <p>プライマリ SVM には FlexCache を作成できますが、セカンダリ SVM には作成できません。プライマリ SVM 内の FlexCache ボリュームは、SVM DR 関係の一部としてレプリケートされません。</p>	ストレージレベルのアクセス保護 (SLAG)
いいえ	いいえ	シンプロビジョニング
はい。	<p>はい。</p> <p>ONTAP 9.7 以降でサポートされます</p>	ボリュームクローニング
<p>はい。</p> <p>ONTAP 9.6 以降では、元のボリュームおよび元のボリューム内のファイルのクローニングがサポートされます。</p>	いいえ	ボリューム移動

はい。	<ul style="list-style-type: none"> <li>○ (ボリュームコンスティチュエントのみ)</li> </ul> <p>FlexCacheボリュームのボリュームコンスティチュエントの移動は、ONTAP 9.6以降でサポートされます。</p>	ボリュームをリホスト
いいえ	いいえ	vStorage API for Array Integration (VAAI)



FlexVol 9 リリース 9.5 よりも前では、ONTAP 8.2.x 7-Mode を実行しているシステムで作成された FlexCache ボリュームにのみ、送信元 Data ONTAP ボリュームがデータを提供できます。ONTAP 9.5 以降では、ONTAP 9 システムの FlexCache ボリュームに元の FlexVol ボリュームからデータを提供することもできます。7-Mode FlexCacheからONTAP 9 FlexCacheへの移行の詳細については、["NetAppテクニカルレポート4743 : 『FlexCache in ONTAP』"](#)を参照してください。

## FlexCache ボリュームのサイジングに関するガイドライン

ボリュームのプロビジョニングを開始する前に、FlexCache ボリュームの制限を確認しておく必要があります。

FlexVol ボリュームのサイズ制限は元のボリュームに適用されます。FlexCache ボリュームのサイズは、元のボリューム以下にする必要があります。FlexCache ボリュームのサイズは、元のボリュームのサイズの 10% 以上にすることを推奨します。

また、FlexCache ボリュームに関する次の制限も把握しておく必要があります。

制限 (Limit)	ONTAP 9.5-9.6	ONTAP 9.7	ONTAP 9.8以降
元のボリュームから作成できる FlexCache の最大数	10	10	100
ノードあたりの推奨される元のボリュームの最大数	10	100	100
ノードあたりの推奨される FlexCache の最大数	10	100	100
1 つの FlexCache に推奨されるノードあたりの FlexGroup コンスティチュエントの最大数	40	800	800
各ノードの FlexCache ボリュームの最大コンスティチュエント数	32だ	32だ	32だ

### 関連情報

["ネットアップの相互運用性"](#)

## FlexCache ボリュームを作成します

同じクラスタに FlexCache ボリュームを作成すると、ホットオブジェクトにアクセスする際のパフォーマンスが向上します。データセンターが複数の場所にある場合は、リモ

ートクラスタに FlexCache ボリュームを作成することでデータアクセスを高速化できます。

このタスクについて

- ONTAP 9.5以降では、FlexCacheでFlexVolボリュームが元のボリュームとして、FlexGroupボリュームがFlexCacheボリュームとしてサポートされます。
- ONTAP 9.7以降では、FlexVolボリュームとFlexGroupボリュームの両方が元のボリュームとしてサポートされます。
- ONTAP 9.14.0以降では、暗号化されたソースから暗号化されていないFlexCacheボリュームを作成できます。

作業を開始する前に

- ONTAP 9.5以降が実行されている必要があります。
- ONTAP 9.6以前を実行している場合は、"[FlexCacheライセンスを追加する](#)"。

ONTAP 9.7以降ではFlexCacheライセンスは必要ありません。ONTAP 9.7以降では、FlexCache機能がONTAPに組み込まれており、ライセンスやアクティブ化は不要になりました。



HA ペアが使用している場合 "[SAS ドライブまたは NVMe ドライブの暗号化（SED、NSE、FIPS）](#)"、の手順に従ってください "[FIPS ドライブまたは SED を非保護モードに戻します](#)" システムを初期化する前の HA ペア内のすべてのドライブ（ブートオプション 4 または 9）。そうしないと、ドライブを転用した場合にデータが失われる可能性があります。

## 例 4. 手順

### System Manager の略

1. FlexCacheボリュームが元のボリュームとは別のクラスタにある場合は、クラスタピア関係を作成します。
    - a. ローカルクラスタで、\* Protection > Overview \* をクリックします。
    - b. を展開し、[ネットワークインターフェイスの追加]\*をクリックして、クラスタのクラスタ間ネットワークインターフェイスを追加します。

リモートクラスタでこの手順を繰り返します。

    - c. リモートクラスタで、[\* Protection] > [Overview] をクリックします。をクリックします [ クラスタピア ] セクションで、[ パスフレーズの生成 ] をクリックします。
    - d. 生成されたパスフレーズをコピーしてローカルクラスタに貼り付けます。
    - e. ローカルクラスタで、[ クラスタピア ] の下の [\* ピアクラスタ \*] をクリックし、ローカルクラスタとリモートクラスタをピアリングします。
  2. FlexCacheボリュームが元のボリュームと同じクラスタにあるが、別のSVMにある場合は、タイプが「FlexCache」のクラスタ間SVMピア関係を作成します。
- [Storage VMピア]で、 さらに \* Storage VM\* をピアリングして、Storage VM のピアリングを行います。
3. Storage > Volumes (ストレージ) を選択します。
  4. 「\* 追加」を選択します。
  5. を選択し、[リモートボリュームのキャッシュとして追加]\*を選択します。



ONTAP 9.8以降を実行していて、QoSを無効にするかカスタムQoSポリシーを選択する場合は、[その他のオプション]\*をクリックし、[ストレージと最適化]で[パフォーマンスサービスレベル]\*を選択します。

### CLI の使用

1. 別のクラスタに作成する FlexCache ボリュームを作成する場合は、クラスタピア関係を作成します。
  - a. デスティネーションクラスタで、データ保護のソースクラスタとのピア関係を作成します。

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

ONTAP 9.6 以降では、クラスタピア関係の作成時に TLS 暗号化がデフォルトで有効になります。TLS 暗号化は、元のボリュームと FlexCache ボリュームの間のクラスタ間通信でサポートされます。必要に応じて、クラスタピア関係の TLS 暗号化を無効にすることもできます。

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

Passphrase: UCa+6lRVICXeL/gq1WrK7ShR  
Expiration Time: 6/7/2017 08:16:10 EST  
Initial Allowed Vserver Peers: \*  
Intercluster LIF IP: 192.140.112.101  
Peer Cluster Name: Clus\_7ShR (temporary generated)

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

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

```
cluster peer create -peer-addr <peer_LIF_IPs> -ip-space <ip-space>
```

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

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

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

Enter the passphrase:  
Confirm the passphrase:

Clusters cluster02 and cluster01 are peered.

2. FlexCache ボリュームが元のボリュームとは異なるSVMにある場合は、を使用してSVMピア関係を作成します flexcache アプリケーションとして:

- a. SVMが別のクラスタにある場合は、ピアリングするSVMのSVM権限を作成します。

```
vserver peer permission create -peer-cluster <cluster_name>
-vserver <svm-name> -applications flexcache
```

次の例は、すべてのローカル SVM に適用される SVM ピア権限を作成する方法を示しています。

```
cluster1::> vserver peer permission create -peer-cluster cluster2
-vserver "*" -applications flexcache
```

Warning: This Vserver peer permission applies to all local Vservers.  
After that no explicit  
"vserver peer accept" command required for Vserver peer relationship  
creation request  
from peer cluster "cluster2" with any of the local Vservers. Do you  
want to continue? {y|n}: y

a. SVMピア関係を作成します。

```
vserver peer create -vserver <local_SVM> -peer-vserver
<remote_SVM> -peer-cluster <cluster_name> -applications flexcache
```

3. FlexCache ボリュームを作成します。

```
volume flexcache create -vserver <cache_svm> -volume
<cache_vol_name> -auto-provision-as flexgroup -size <vol_size>
-origin-vserver <origin_svm> -origin-volume <origin_vol_name>
```

次の例では、FlexCache ボリュームを作成し、プロビジョニングする既存のアグリゲートを自動的に選択します。

```
cluster1::> volume flexcache create -vserver vs_1 -volume fc1 -auto
-provision-as flexgroup -origin-volume vol_1 -size 160MB -origin
-vserver vs_1
[Job 443] Job succeeded: Successful
```

次の例では、FlexCache ボリュームを作成し、ジャンクションパスを設定します。

```
cluster1::> flexcache create -vserver vs34 -volume fc4 -aggr-list
aggr34,aggr43 -origin-volume origin1 -size 400m -junction-path /fc4
[Job 903] Job succeeded: Successful
```

4. FlexCache ボリュームと元のボリュームの FlexCache 関係を確認します。

a. クラスタ内のFlexCache関係を表示します。

```
volume flexcache show
```



```
cluster1::> volume flexcache show
Vserver Volume      Size      Origin-Vserver Origin-Volume
Origin-Cluster
-----
vs_1      fc1        160MB     vs_1         vol_1
cluster1
```

- b. 元のクラスタのすべてのFlexCache関係を表示します。

[+]

```
volume flexcache origin show-caches
```

```
cluster::> volume flexcache origin show-caches
Origin-Vserver Origin-Volume  Cache-Vserver  Cache-Volume
Cache-Cluster
-----
vs0            ovol1         vs1            cfg1
clusA
vs0            ovol1         vs2            cfg2
clusB
vs_1           vol_1         vs_1           fc1
cluster1
```

## 結果

FlexCache ボリュームが作成されました。クライアントは、FlexCache ボリュームのジャンクションパスを使用してボリュームをマウントできます。

## 関連情報

["クラスタと SVM のピアリング"](#)

## FlexCacheボリュームを管理します。

### FlexCache ボリュームの監査に関する考慮事項

ONTAP 9.7 以降では、FPolicy でのネイティブの ONTAP 監査とファイルポリシー管理を使用して、FlexCache 関係の NFS ファイルアクセスイベントを監査できます。

ONTAP 9.14.1以降では、NFSまたはSMBを使用するFlexCacheボリュームでFPolicyがサポートされます。以前は、SMBを使用するFlexCacheではFPolicyはサポートされていませんでした。

標準の監査と FPolicy は、FlexVol ボリュームと同じ CLI コマンドで設定および管理されます。ただし、FlexCache ボリュームにはいくつかの動作があります。

## • \* ネイティブ監査 \*

- FlexCache ボリュームを監査ログのデスティネーションとして使用することはできません。
- FlexCache に対する読み取りと書き込みを監査する場合は、キャッシュ SVM と元の SVM の両方で監査を設定する必要があります。

これは、ファイルシステム操作が処理される場所で監査されるためです。つまり、読み取りはキャッシュ SVM で監査され、書き込みは元の SVM で監査されます。

- 書き込み処理の元を追跡するために、SVM UUID と MSID が監査ログに追加され、書き込みが開始された FlexCache ボリュームが識別されます。
- システムアクセス制御リスト (SACL) は NFSv4 または SMB プロトコルを使用してファイルに設定できますが、FlexCache ボリュームでは NFSv3 のみがサポートされます。そのため、SACL を設定できるのは元のボリュームのみです。

## • \* FPolicy \*

- FlexCache ボリュームへの書き込みは元のボリュームでコミットされますが、FPolicy 設定はキャッシュボリュームへの書き込みを監視します。これは、元のボリュームに対する書き込みが監査される標準の監査とは異なります。
- キャッシュと送信元の SVM で ONTAP を同じ FPolicy 設定する必要はありませんが、2 つの同様の設定を導入することを推奨します。そのためには、元の SVM のように設定され、新しいポリシーのスコープがキャッシュ SVM に制限されているキャッシュ用の新しい FPolicy ポリシーを作成します。

元のボリュームから **FlexCache** ボリュームのプロパティを同期する

FlexCache ボリュームの一部のボリュームプロパティは、常に元のボリュームと同期されている必要があります。元のボリュームでプロパティが変更されたあとに、FlexCache ボリュームのボリュームプロパティの自動同期が失敗した場合は、プロパティを手動で同期できます。

このタスクについて

FlexCache ボリュームの次のボリュームプロパティは、常に元のボリュームと同期されている必要があります。

- セキュリティ形式 (-security-style)
- ボリューム名 (-volume-name)
- 最大ディレクトリサイズ (-maxdir-size)
- 最小先読み (-min-readahead)

ステップ

1. FlexCache ボリュームから、ボリュームプロパティを同期します。

```
volume flexcache sync-properties -vserver svm_name -volume flexcache_volume
```

```
cluster1::> volume flexcache sync-properties -vserver vs1 -volume fcl
```

## FlexCache 関係の設定を更新する

ボリュームの移動、アグリゲートの再配置、ストレージフェイルオーバーなどのイベントが発生すると、元のボリュームと FlexCache ボリュームの構成情報が自動的に更新されます。自動更新が失敗した場合は EMS メッセージが生成され、FlexCache 関係の設定を手動で更新する必要があります。

元のボリュームと FlexCache ボリュームが切断モードになっている場合は、FlexCache 関係を手動で更新するために追加の処理が必要になることがあります。

### このタスクについて

FlexCache ボリュームの設定を更新する場合は、元のボリュームからコマンドを実行する必要があります。元のボリュームの設定を更新する場合は、FlexCache からコマンドを実行する必要があります。

### ステップ

1. FlexCache 関係の設定を更新します。

```
volume flexcache config-refresh -peer-vserver peer_svm -peer-volume  
peer_volume_to_update -peer-endpoint-type [origin | cache]
```

### ファイルアクセス時間の更新を有効にします

ONTAP 9.11.1以降では、を有効にすることができます `-atime-update` ファイルアクセス時間の更新を許可する FlexCache ボリュームのフィールド。でアクセス時間の更新期間を設定することもできます `-atime-update-period` 属性 (Attribute) :。  
`-atime-update-period` 属性は、アクセス時間の更新を実行する頻度と、更新がいつ元のボリュームに反映されるかを制御します。

### 概要

ONTAP には、というボリュームレベルのフィールドがあります `-atime-update`` READ、READLINK、REaddirを使用して読み取られたファイルおよびディレクトリのアクセス時間の更新を管理します。アクセス頻度の低いファイルとディレクトリのデータライフサイクルの決定には `atime` が使用されます。アクセス頻度の低いファイルは最終的にアーカイブストレージに移行され、あとでテープに移動されることもあります。

`atime` 更新フィールドは、既存および新規に作成された FlexCache ボリュームではデフォルトで無効になります。9.11.1 よりも前の ONTAP リリースで FlexCache ボリュームを使用している場合は、`atime` 更新フィールドを無効にして、元のボリュームで読み取り処理が実行されるときにキャッシュが不要に削除されないようにする必要があります。ただし、大規模な FlexCache キャッシュでは、管理者が特別なツールを使用してデータを管理し、ホットデータがキャッシュに残ってコールドデータがパージされるのを確保します。`atime` 更新を無効にする場合は実行できません。ただし、ONTAP 9.11.1以降では、を有効にすることができます `-atime-update` および `-atime-update-period`, キャッシュされたデータの管理に必要なツールを使用します。

### 作業を開始する前に

すべての FlexCache で ONTAP 9.11.1以降が実行されている必要があります。

このタスクについて

設定 `-atime-update-period 86400`秒に設定すると、ファイルに対して実行された読み取りに類似した操作の数に関係なく、24時間ごとに1回のアクセス時間更新が許可されます。

を設定します `-atime-update-period 0`にすると、読み取りアクセスごとにメッセージが送信元に送信されます。その後、元のFlexCache は各に、パフォーマンスに影響するatimeが古いことを通知します。

手順

1. ファイルアクセス時間の更新を有効にし、更新頻度を設定します。

```
volume modify -volume vol_name -vserver SVM_name -atime-update true -atime-update-period seconds
```

次に、を有効にする例を示します `-atime-update` とセット `-atime-update-period 86400`秒（24時間）まで：

```
c1: volume modify -volume origin1 vs1_c1 -atime-update true -atime-update-period 86400
```

2. 確認します `-atime-update` 有効：

```
volume show -volume vol_name -fields atime-update,atime-update-period
```

```
c1::*> volume show -volume cache1_origin1 -fields atime-update,atime-update-period
vserver volume          atime-update atime-update-period
-----
vs2_c1   cache1_origin1 true          86400
```

グローバルファイルロックを有効にします

ONTAP 9.10.1 以降では、グローバルファイルロックを適用して、関連するキャッシュファイルすべての読み取りを防止できます。

グローバルファイルロックを有効にすると、すべてのFlexCacheボリュームがオンラインになるまで元のボリュームに対する変更が中断されます。グローバルファイルロックを有効にする必要があるのは、キャッシュと送信元の間の接続の信頼性を一時停止することが原因でのみです。また、FlexCache ボリュームがオフラインになった場合には、変更がタイムアウトする可能性があります。

作業を開始する前に

- グローバルファイルロックを使用するには、元のクラスタとすべての関連キャッシュを含むクラスタでONTAP 9.9.1 以降が実行されている必要があります。グローバルファイルロックは、新規または既存のFlexCache ボリュームで有効にできます。このコマンドは1つのボリュームに対して実行でき、関連付けられているすべてのFlexCacheボリュームを環境できます。
- グローバルファイルロックを有効にするには、advanced 権限レベルが必要です。

- ONTAP 9.9.1より前のバージョンにリバートする場合は、最初に送信元キャッシュと関連するキャッシュでグローバルファイルロックを無効にする必要があります。無効にするには、元のボリュームから次のコマンドを実行します。 `volume flexcache prepare-to-downgrade -disable-feature-set 9.10.0`
- グローバルファイルロックを有効にするプロセスは、オリジンに既存のキャッシュがあるかどうかによって異なります。
  - [\[enable-gfl-new\]](#)
  - [\[enable-gfl-existing\]](#)

新しい **FlexCache** ボリュームでグローバルファイルロックを有効にします

#### 手順

1. を使用してFlexCache ボリュームを作成します `-is-global-file-locking true`に設定：

```
volume flexcache create volume volume_name -is-global-file-locking-enabled true
```



のデフォルト値 `-is-global-file-locking` は `"false"` です。次のいずれかの場合 `volume flexcache create` コマンドはボリュームに対して実行されます。コマンドは `-is-global-file-locking enabled` 「true」に設定します。

既存の **FlexCache** ボリュームでグローバルファイルロックを有効にします

#### 手順

1. グローバルファイルロックは元のボリュームから設定する必要があります。
2. 元のボリュームに他の既存の関係（SnapMirror など）を含めることはできません。既存の関係の関連付けを解除する必要があります。すべてのキャッシュとボリュームは、コマンドの実行時に接続する必要があります。接続ステータスを確認するには、次のコマンドを実行します。

```
volume flexcache connection-status show
```

表示されたすべてのボリュームのステータスが `connected` と表示されます。詳細については、[を参照してください](#) "FlexCache 関係のステータスを確認します" または "元のボリュームから FlexCache ボリュームのプロパティを同期する"。

3. キャッシュ上でグローバルファイルロックを有効にします。

```
volume flexcache origin config show/modify -volume volume_name -is-global-file-locking-enabled true
```

### FlexCache ボリュームを事前に取り込む

FlexCache ボリュームを事前に取り込むことで、キャッシュされたデータにアクセスするまでの時間を短縮できます。

#### 必要なもの

- advanced 権限レベルのクラスタ管理者である必要があります

- ・事前取り込みのために渡されたパスが存在している必要があります。存在していないと、事前入力処理

このタスクについて

- ・ファイルのみを事前に読み込み、ディレクトリをクロールします
- ・。 -isRecursion 環境 に、事前入力に渡されたディレクトリのリスト全体にフラグを設定します

手順

#### 1. FlexCache ボリュームを事前に取り込む：

```
volume flexcache prepopulate -cache-vserver vs1 -cache-volume -path
-list path_list -isRecursion true|false
```

- °。 -path-list パラメータは、元のルートディレクトリから事前に取り込む相対ディレクトリパスを指定します。たとえば、元のルートディレクトリの名前が/originで、ディレクトリ/origin/dir1と/origin/dir2が含まれている場合は、次のようにパスのリストを指定できます。 -path-list dir1, dir2 または -path-list /dir1, /dir2。
- ° のデフォルト値 -isRecursion パラメータはTrueです。

この例では、単一のディレクトリパスが事前に設定されています

```
cluster1::*> flexcache prepopulate start -cache-vserver vs2 -cache
-volume fg_cachevol_1 -path-list /dir1
(volume flexcache prepopulate start)
[JobId 207]: FlexCache prepopulate job queued.
```

次の例では、複数のディレクトリからファイルを事前に取り込みます。

```
cluster1::*> flexcache prepopulate start -cache-vserver vs2 -cache
-volume fg_cachevol_1 -path-list /dir1,/dir2,/dir3,/dir4
(volume flexcache prepopulate start)
[JobId 208]: FlexCache prepopulate job queued.
```

次の例では、単一のファイルが事前に読み込まれます。

```
cluster1::*> flexcache prepopulate start -cache-vserver vs2 -cache
-volume fg_cachevol_1 -path-list /dir1/file1.txt
(volume flexcache prepopulate start)
[JobId 209]: FlexCache prepopulate job queued.
```

次の例では、オリジンのすべてのファイルを事前に取り込みます。

```
cluster1::*> flexcache prepopulate start -cache-vserver vs2 -cache
-volume fg_cachevol_1 -path-list / -isRecursion true
(volume flexcache prepopulate start)
[JobId 210]: FlexCache prepopulate job queued.
```

この例には、事前取り込みの無効なパスが含まれています。

```
cluster1::*> flexcache prepopulate start -cache-volume
vol_cache2_vs3_c2_vol_origin1_vs1_c1 -cache-vserver vs3_c2 -path-list
/dir1, dir5, dir6
(volume flexcache prepopulate start)

Error: command failed: Path(s) "dir5, dir6" does not exist in origin
volume
      "vol_origin1_vs1_c1" in Vserver "vs1_c1".
```

2. 読み取られたファイル数を表示します。

```
job show -id job_ID -ins
```

## FlexCache 関係を削除

不要 FlexCache になった FlexCache 関係と FlexCache ボリュームは削除できます。

### 手順

1. FlexCache ボリュームが含まれるクラスタから、FlexCache ボリュームをオフラインにします。

```
volume offline -vserver svm_name -volume volume_name
```

2. FlexCache ボリュームを削除します。

```
volume flexcache delete -vserver svm_name -volume volume_name
```

FlexCache 関係の詳細が元のボリュームと FlexCache ボリュームから削除されます。

# Network Management の略

## はじめに

### ネットワーク管理の概要

System ManagerまたはCLIを使用してストレージネットワークの基本的な管理を実行するには、次の情報を使用します。物理 / 仮想ネットワークポート（VLAN およびインターフェイスグループ）の設定、IPv4 と IPv6 を使用した LIF の作成、クラスタでのルーティングサービスとホスト解決サービスの管理、ロードバランシングを使用したネットワークトラフィックの最適化、SNMP を使用したクラスタの監視が可能です。

特に記載がないかぎり、CLIの手順はONTAP 9のすべてのバージョンに適用されます。

各ONTAP 9リリースで利用できるネットワーク機能の影響については、を参照してください。"[ONTAP リリースノート](#)"。

ONTAP 9.8 以降では、System Manager を使用して、ネットワークのコンポーネントと構成を示す図を表示できます。ONTAP 9.12以降では、ネットワークインターフェイスグリッドでLIFとサブネットの関連付けを表示できます。従来のSystem Manager（ONTAP 9.7以前でのみ使用可能）を使用している場合は、を参照してください。"[ネットワークの管理](#)"。

この新しいネットワーク可視化機能を使用すると、ホスト、ポート、SVM、ボリュームなど全体のネットワーク接続パスをグラフィカルインターフェイスに表示できます。

[ ネットワーク ] > [ 概要 \* ] を選択するか、またはを選択すると、グラフィックが表示されます → ダッシュボードの \* ネットワーク \* セクションから。

次のカテゴリのコンポーネントが図に示されています。

- ホスト
- ストレージポート
- ネットワークインターフェイス
- Storage VMs
- データアクセスコンポーネント


各セクションには、ネットワーク管理タスクと設定タスクを実行するためにマウスを合わせるか、選択することができる詳細が表示されます。

### 例

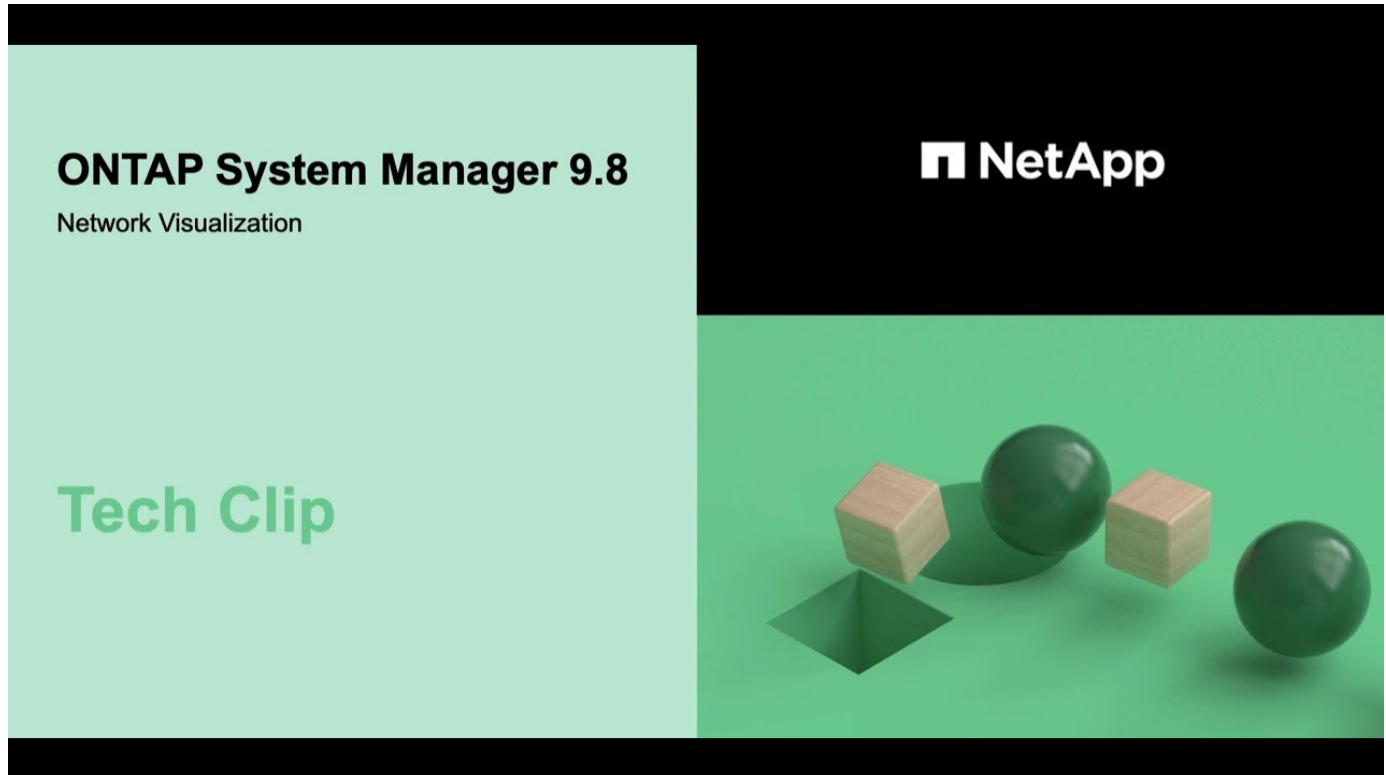
次の例は、グラフィックを操作して各コンポーネントの詳細を表示したり、ネットワークを管理するためのアクションを開始したりするさまざまな方法を示しています。

- ホストをクリックすると、ホストの設定（ポート、ネットワークインターフェイス、Storage VM、関連付けられているデータアクセスコンポーネント）が表示されます。
- Storage VM 内のボリューム数にカーソルを合わせると、ボリュームが選択されて詳細が表示されます。



- 過去 1 週間のパフォーマンスを表示するには、iSCSI インターフェイスを選択してください。
- をクリックします  をクリックして、そのコンポーネントを変更するアクションを開始します。
- 問題のあるコンポーネントの横に「X」と表示されている、ネットワークで問題が発生する可能性のある場所をすばやく特定します。

## System Manager のネットワーク可視化に関するビデオ



## ONTAP 9.7x以前からのONTAPアップグレード後のネットワーク構成の確認

ONTAP 9.7x以前のバージョンからONTAP 9.8以降にアップグレードしたら、ネットワーク構成を確認する必要があります。アップグレード後、ONTAP は自動的にレイヤ 2 の到達可能性を監視します。

### ステップ

1. 各ポートに想定されるブロードキャストドメインへの到達可能性があることを確認します。

```
network port reachability show -detail
```

コマンド出力に到達可能性の結果が含まれています。次のデシジョンツリーとテーブルを使用して、到達可能性の結果（reachable-status）を理解し、次に何を実行するか（存在する場合）を決定します。



プレゼンスステータス	説明
------------	----

わかりました	<p>ポートに割り当てられているブロードキャストドメインにレイヤ 2 の到達可能性があります。</p> <p>reachable-status が「OK」であるのに、「予想外のポート」がある場合は、1 つ以上のブロードキャストドメインをマージすることを検討してください。詳細については、を参照してください <a href="#">"ブロードキャストドメインをマージします"</a>。</p> <p>reachable-status が「OK」であるが、「到達不能ポート」がある場合は、1 つ以上のブロードキャストドメインをスプリットすることを検討してください。詳細については、を参照してください <a href="#">"ブロードキャストドメインをスプリットします"</a>。</p> <p>reachable-status が「OK」で、予期しないポートや到達不能なポートがない場合は、設定が正しいことを確認してください。</p>
誤設定 - 到達可能性	<p>ポートに割り当てられているブロードキャストドメインにレイヤ 2 に到達できるかどうかは関係ありませんが、ポートは別のブロードキャストドメインにレイヤ 2 に到達できるかどうかは関係ありません。</p> <p>ポートに到達できるかどうかを修復できます。次のコマンドを実行すると、ポートに到達できるブロードキャストドメインにポートが割り当てられます。</p> <pre>network port reachability repair -node -port</pre> <p>詳細については、を参照してください <a href="#">"ポートの到達可能性を修復します"</a>。</p>
到達不能	<p>既存のどのブロードキャストドメインにもレイヤ 2 で接続できません。</p> <p>ポートに到達できるかどうかを修復できます。次のコマンドを実行すると、自動的に作成されたデフォルトの IPspace 内の新しいブロードキャストドメインにポートが割り当てられます。</p> <pre>network port reachability repair -node -port</pre> <p>詳細については、を参照してください <a href="#">"ポートの到達可能性を修復します"</a>。</p>
multi-domain-reachable	<p>ポートには、割り当てられたブロードキャストドメインにレイヤ 2 に到達できることがあります。少なくとも 1 つの他のブロードキャストドメインにレイヤ 2 に到達できることもあります。</p> <p>物理的な接続とスイッチの設定を調べて、正しくないか、またはポートに割り当てられているブロードキャストドメインを 1 つ以上のブロードキャストドメインにマージする必要があるかどうかを確認します。</p> <p>詳細については、を参照してください <a href="#">"ブロードキャストドメインをマージします"</a> または <a href="#">"ポートの到達可能性を修復します"</a>。</p>
不明です	<p>reachable-status が「unknown」の場合は、数分待ってからもう一度コマンドを実行してください。</p>

ポートを修復したら、取り外された LIF や VLAN を確認して解決する必要があります。ポートがインターフ

エイスグループに属していた場合は、そのインターフェイスグループに何が起こったかを理解する必要もあります。詳細については、を参照してください "[ポートの到達可能性を修復します](#)"。

## ネットワークコンポーネント

### クラスタのネットワークコンポーネントの概要

クラスタをセットアップする前に、クラスタのネットワークコンポーネントについて理解しておく必要があります。クラスタの物理ネットワークコンポーネントを論理コンポーネントに設定することで、ONTAP の持つ柔軟性とマルチテナンシー機能を活かします。

クラスタのさまざまなネットワークコンポーネントを次に示します。

- 物理ポート

Network Interface Card（NIC；ネットワークインターフェイスカード）と Host Bus Adapter（HBA；ホストバスアダプタ）は、各ノードから物理ネットワーク（管理ネットワークとデータネットワーク）への物理接続（イーサネットおよびファイバチャネル）を提供します。

サイトの要件、スイッチの情報、ポートのケーブル接続の情報、コントローラのオンボードポートのケーブル接続については、の Hardware Universe を参照してください "[hwu.netapp.com](http://hwu.netapp.com)"。

- 論理ポート

論理ポートは仮想ローカルエリアネットワーク（VLAN）とインターフェイスグループで構成されます。インターフェイスグループは複数の物理ポートを 1 つのポートとして扱い、VLAN は 1 つの物理ポートを複数の個別のポートに分割します。

- IPspace

IPspace を使用すると、クラスタ内の SVM ごとに個別の IP アドレススペースを作成できます。これにより、管理上分離されたネットワークドメインのクライアントが、IP アドレスの同じサブネット範囲内の重複した IP アドレスを使用してクラスタのデータにアクセスできるようになります。

- ブロードキャストドメイン

ブロードキャストドメインは IPspace 内に存在し、同じレイヤ 2 ネットワークに属する、クラスタ内の多数のノードからのネットワークポートグループを含んでいます。このグループのポートは、SVM でデータトラフィック用に使用されます。

- サブネット

サブネットはブロードキャストドメイン内に作成され、同じレイヤ 3 サブネットに属する IP アドレスのプールを含んでいます。この IP アドレスプールを使用すると、LIF の作成時の IP アドレスの割り当てが簡単になります。

- 論理インターフェイス

論理インターフェイス（LIF）は、ポートに関連付けられた IP アドレスまたはワールドワイドポート名（WWPN）です。フェイルオーバーグループ、フェイルオーバールール、ファイアウォールルールなどの属性があります。LIF は、現在バインドされているポート（物理または論理）からネットワーク経由で

通信します。

クラスタ内の LIF のタイプには、データ LIF、クラスタを対象とした管理 LIF、ノードを対象とした管理 LIF、クラスタ間 LIF、およびクラスタ LIF があります。LIF の所有権は、LIF を実装する SVM によって異なります。データ LIF はデータ SVM によって、ノードを対象とした管理 LIF、クラスタを対象とした管理 LIF、およびクラスタ間 LIF は管理 SVM によって、クラスタ LIF はクラスタ SVM によって所有されます。

- DNS ゾーン

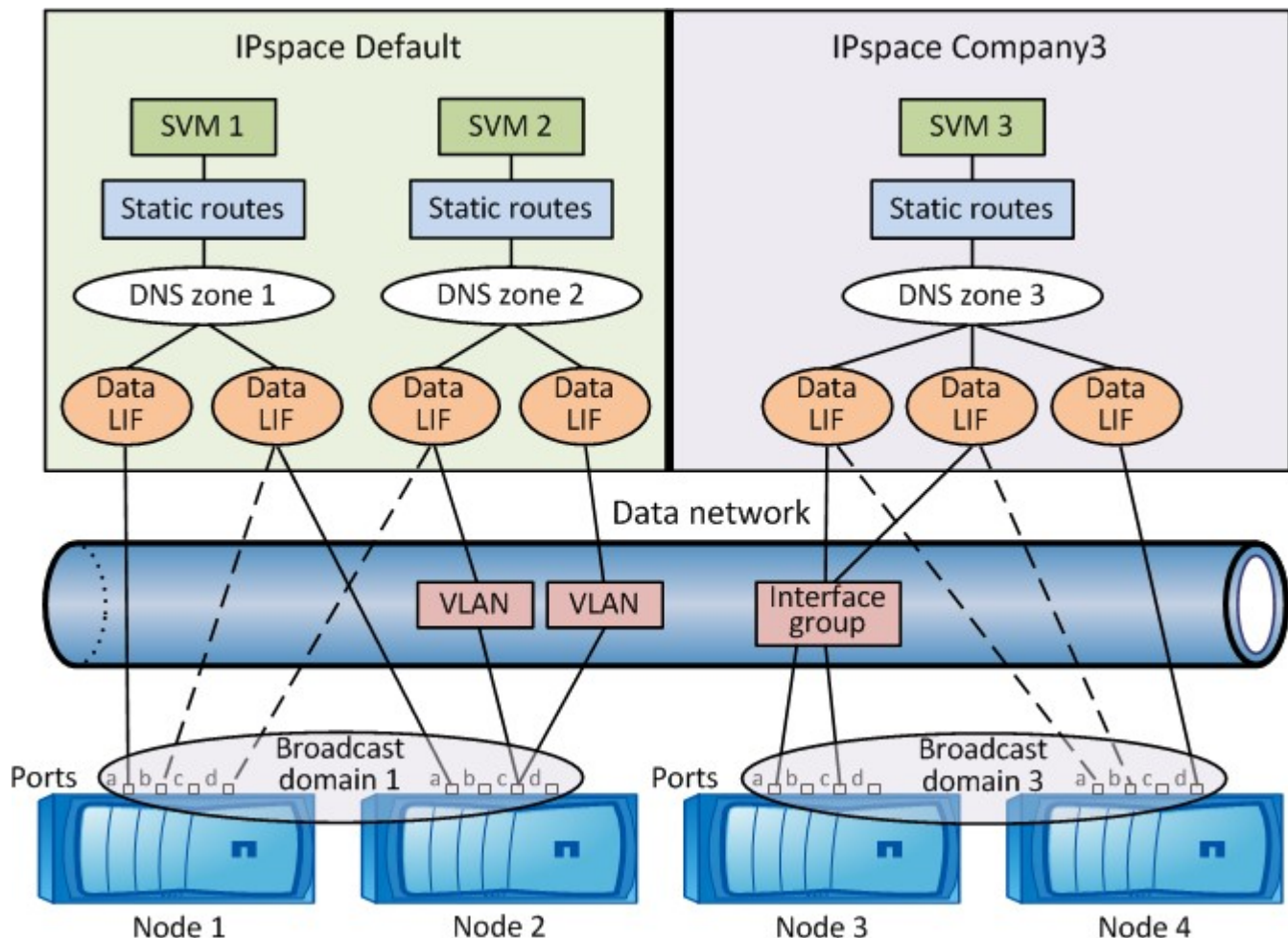
DNS ゾーンは LIF の作成時に指定でき、クラスタの DNS サーバ経由でエクスポートされる LIF の名前を提供します。複数の LIF で同じ名前を共有できるため、DNS ロードバランシング機能を使用し、その名前の IP アドレスを負荷に従って分散させることができます。

SVM には、複数の DNS ゾーンを設定できます。

- ルーティング

各 SVM は、ネットワーク上で完全な機能を持つ独立した存在です。SVM は、LIF および設定済みの外部サーバに到達可能なルートを持っています。

次の図は、4 ノードクラスタにおける各種ネットワークコンポーネントの関係を示しています。



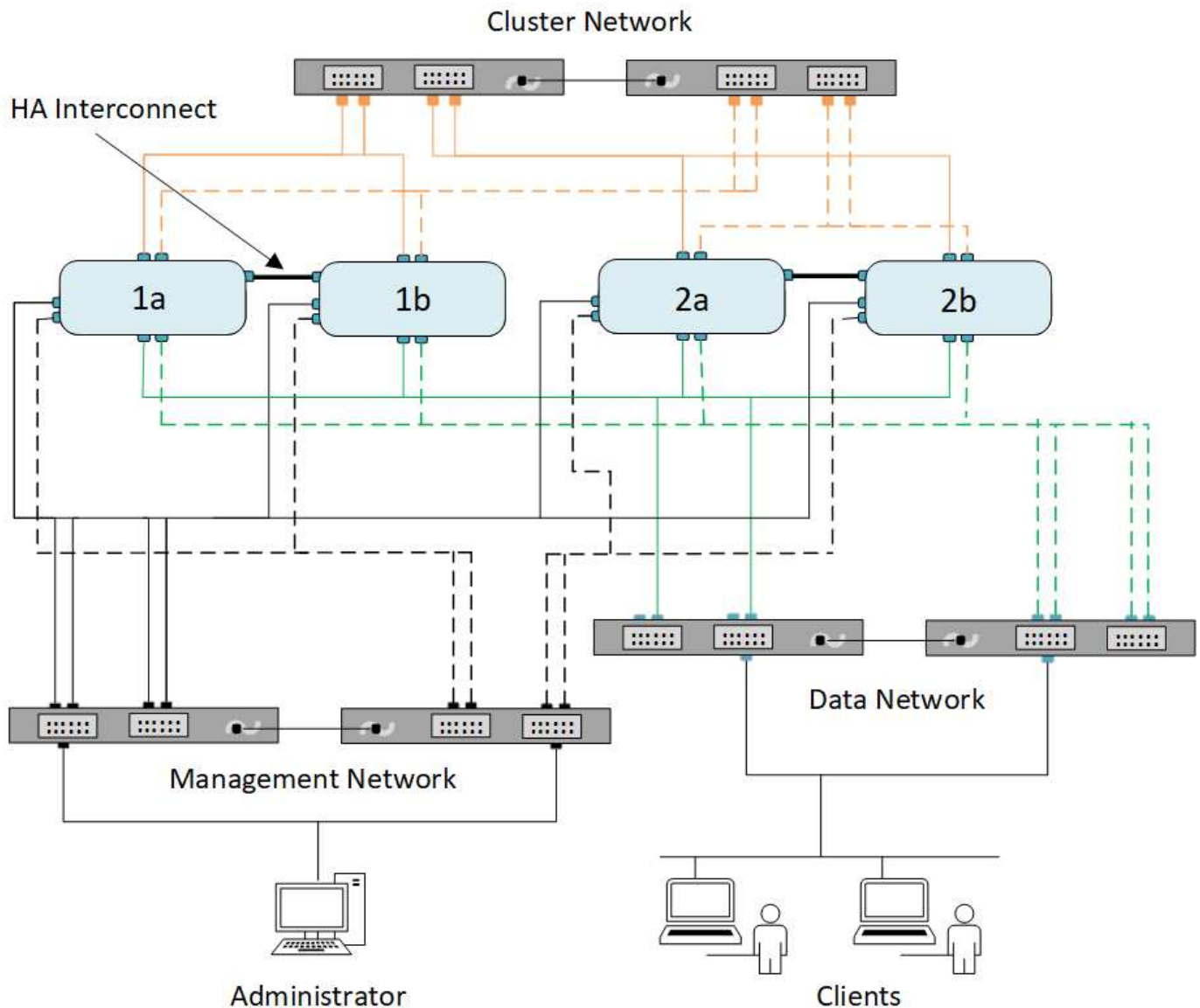


## ネットワークのケーブル配線のガイドライン

ネットワークのケーブル配線のベストプラクティスでは、クラスタ、管理、データの各ネットワークにトラフィックを分離しています。

クラスタをケーブル配線するときは、クラスタのトラフィックが他のすべてのトラフィックとは別のネットワーク上にあるようにします。オプションですが、ネットワーク管理トラフィックをデータとクラスタ内のトラフィックから分離することを推奨します。分離されたネットワークを維持することで、パフォーマンスの向上、管理の容易さ、ノードへのセキュリティアクセスと管理アクセスの向上を実現できます。

次の図は、3つのネットワークを持つ、4ノードHAクラスタのケーブル配線を示しています。



ネットワークのケーブル配線を行うときは、次のガイドラインに従う必要があります。

- 各ノードは、3つの個別のネットワークに接続する必要があります。

1つは管理用、もう1つはデータアクセス用、もう1つはクラスタ内通信用です。管理ネットワークとデ

ータネットワークは論理的に分離できます。

- クライアント（データ）トラフィックのフローを向上させるために、各ノードへのデータネットワーク接続を複数確立することができます。
- クラスタを作成する際、データネットワーク接続はなくてもかまいませんが、クラスタインターコネクト接続は必ず必要です。
- 各ノードへのクラスタ接続は常に2つ以上にする必要があります。

ネットワークのケーブル配線の詳細については、を参照してください ["AFF および FAS システムドキュメントセンター"](#) および ["Hardware Universe"](#)。

## ブロードキャストドメイン、フェイルオーバーグループ、フェイルオーバーポリシー間の関係

ブロードキャストドメイン、フェイルオーバーグループ、およびフェイルオーバーポリシーを組み合わせて、LIF が設定されているノードまたはポートに障害が発生した場合にテイクオーバーするポートを決定します。

ブロードキャストドメインには、同じレイヤ 2 イーサネットネットワークで到達できるすべてのポートがリストされます。いずれかのポートから送信されたイーサネットブロードキャストパケットが、ブロードキャストドメイン内の他のすべてのポートで認識されます。LIF がブロードキャストドメイン内の他のポートにフェイルオーバーされた場合でも、元のポートから到達可能なすべてのローカルホストおよびリモートホストに到達できる可能性があるため、ブロードキャストドメインの一般的な到達可能性特性は LIF にとって重要です。

フェイルオーバーグループは、ブロードキャストドメイン内のポートを定義し、それぞれのポートが LIF のフェイルオーバー対象となります。各ブロードキャストドメインには、ポートをすべて含むフェイルオーバーグループが 1 つあります。このフェイルオーバーグループにはブロードキャストドメインのすべてのポートが含まれており、LIF に対して推奨されるフェイルオーバーグループです。ブロードキャストドメイン内に同じリンク速度のポートのフェイルオーバーグループなど、定義したサブセットを減らしてフェイルオーバーグループを作成できます。

フェイルオーバーポリシーは、ノードまたはポートが停止した場合に、LIF がフェイルオーバーグループのポートをどのように使用するかを定義します。フェイルオーバーポリシーは、フェイルオーバーグループに適用されるフィルタの一種とみなされます。LIF のフェイルオーバーターゲット（LIF がフェイルオーバーできるポートのセット）は、ブロードキャストドメイン内の LIF のフェイルオーバーグループにその LIF のフェイルオーバーポリシーを適用することによって決まります。

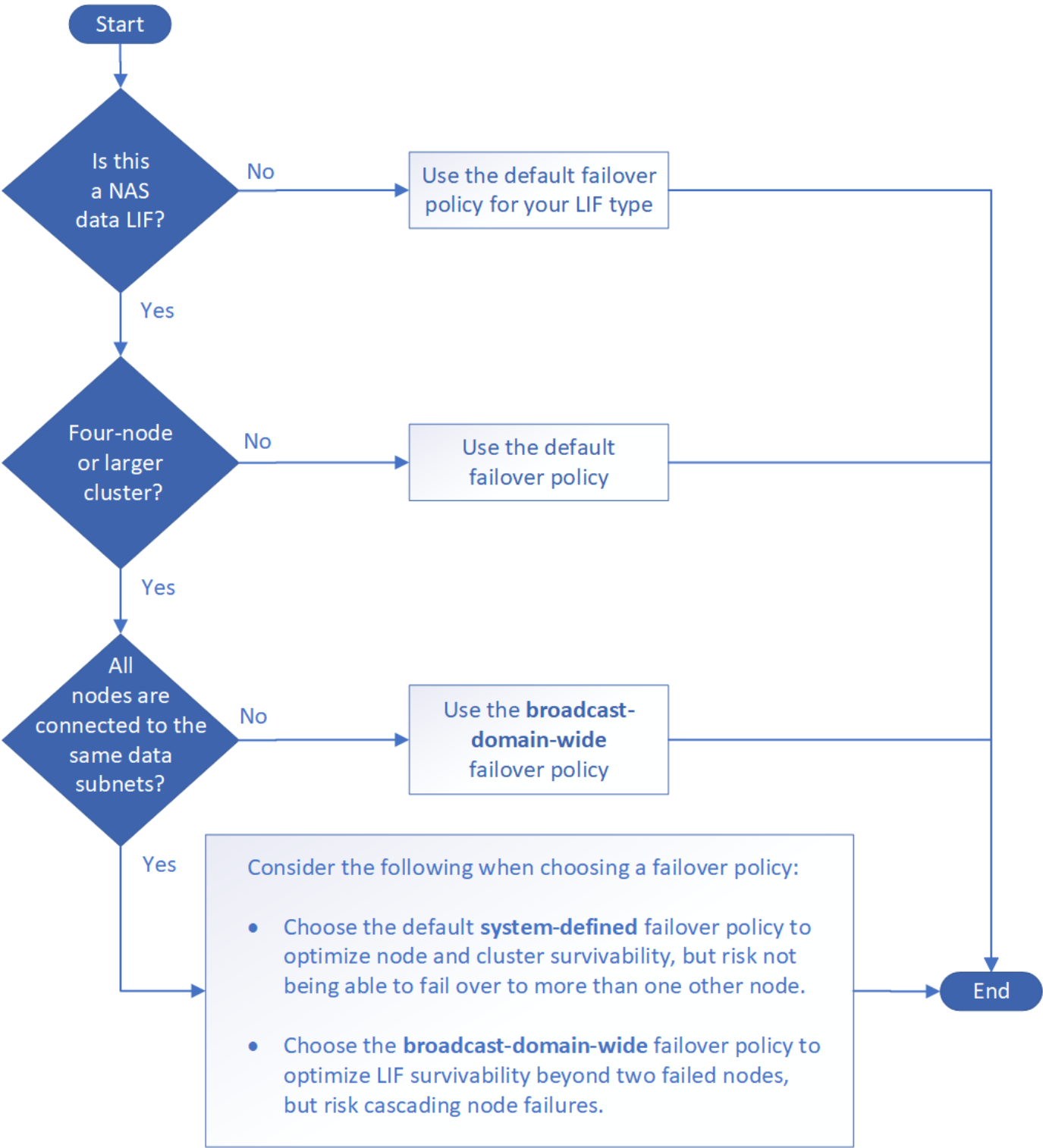
LIF のフェイルオーバーターゲットを表示するには、次の CLI コマンドを使用します。

```
network interface show -failover
```

LIF のタイプにはデフォルトのフェイルオーバーポリシーを使用することを強く推奨します。

使用する **LIF** フェイルオーバーポリシーを決定します

推奨されるデフォルトのフェイルオーバーポリシーを使用するか、LIF のタイプと環境に基づいて変更するかを決定します。



LIF タイプ別のデフォルトのフェイルオーバーポリシー

LIFタイプ	デフォルトのフェイルオーバーポリシーです	説明
BGP LIF	無効	LIF は別のポートにフェイルオーバーしません。



クラスタ LIF	ローカルのみ	LIF は、同じノードのポートにのみフェイルオーバーします。
クラスタ管理 LIF	broadcast-domain-wide	LIF は、クラスタ内のすべてのノード上の同じブロードキャストドメイン内のポートにフェイルオーバーします。
クラスタ間 LIFs	ローカルのみ	LIF は、同じノードのポートにのみフェイルオーバーします。
NAS データ LIF	システム定義	LIF は、HA パートナーではないもう一方のノードにフェイルオーバーします。
ノード管理 LIFs	ローカルのみ	LIF は、同じノードのポートにのみフェイルオーバーします。
SANデータLIF	無効	LIF は別のポートにフェイルオーバーしません。

「sfo-partner-only」フェイルオーバーポリシーはデフォルトではありませんが、LIFをホームノードまたはSFOパートナー上のポートにのみフェイルオーバーする場合に使用できます。

## NASパスのフェイルオーバーワークフロー（ONTAP 9.8以降）

### NASパスのフェイルオーバーについて（ONTAP 9.8以降）

このワークフローでは、ONTAP 9.8 以降で NAS パスのフェイルオーバーを設定するためのネットワーク設定手順を示します。このワークフローは次のことを前提としています。

- NAS パスのフェイルオーバーに関するベストプラクティスを、ネットワーク設定を簡易化するワークフローで使用する。
- System Manager ではなく、CLI を使用する。
- ONTAP 9.8 以降を実行している新しいシステムでネットワークを設定する場合。

9.8 より前のリリースの ONTAP を実行している場合は、ONTAP 9.0 から 9.7 の NAS パスフェイルオーバー手順を使用してください。

- ["ONTAP 9.1-9.7 NAS パスのフェイルオーバーワークフロー"](#)

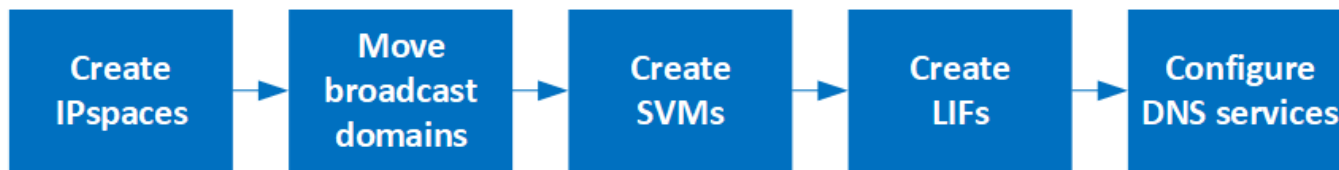
ネットワーク管理の詳細が必要な場合は、ネットワーク管理の参考資料を参照してください。

- [ネットワーク管理の概要](#)

### ワークフロー（ONTAP 9.8以降）

ネットワークの基本概念をすでに理解している場合は、NAS パスのフェイルオーバー設定に関するこの「ハンズオン」ワークフローを確認することで、ネットワークの設定にかかる時間を節約できます。

NAS LIF は、現在のポートでリンク障害が発生すると、稼働しているネットワークポートに自動的に移行します。パスのフェイルオーバーは、ONTAP のデフォルトを利用して管理できます。



リンク障害の発生後に手動で移動しないかぎり、SAN LIF は移行されません。代わりに、ホストのマルチパステクノロジーによって、別の LIF にトラフィックが転送されます。詳細については、[を参照してください "SAN 管理"](#)。

1

#### "ワークシートに記入する"

ワークシートを使用して、NASパスのフェイルオーバーを計画します。

2

#### "IPspaces を作成します"

クラスタ内のSVMごとに個別のIPアドレススペースを作成します。

3

#### "ブロードキャストドメインを IPspace に移動します"

ブロードキャストドメインをIPspaceに移動します。

4

#### "SVMs を作成します"

クライアントにデータを提供するSVMを作成します。

5

#### "LIFs を作成します"

データへのアクセスに使用するポートにLIFを作成します。

6

#### "SVM用のDNSサービスの設定"

NFSサーバまたはSMBサーバを作成する前に、SVM用のDNSサービスを設定してください。

### NASパスのフェイルオーバー設定用ワークシート（ONTAP 9.8以降）

NAS パスのフェイルオーバーを設定する前に、ワークシートのすべてのセクションに記入しておく必要があります。

#### IPspace の設定

IPspace を使用すると、クラスタ内の SVM ごとに個別の IP アドレススペースを作成できます。これにより、管理上分離されたネットワークドメインのクライアントが、IP アドレスの同じサブネット範囲内の重複した IP アドレスを使用してクラスタのデータにアクセスできるようになります。

情報	必須	値を入力します
----	----	---------

IPspace 名 IPspaceの一意的識別子。	はい。	
------------------------------	-----	--

## ブロードキャストドメイン設定

ブロードキャストドメインは、同じレイヤ 2 ネットワークに属するポートをグループ化し、そのブロードキャストドメインポートに MTU を設定します。

ブロードキャストドメインは IPspace に割り当てられます。1 つの IPspace に複数のブロードキャストドメインを含めることができます。



LIF のフェイルオーバー先のポートは、LIF のフェイルオーバーグループのメンバーである必要があります。ONTAP で作成したブロードキャストドメインごとに、同じ名前のフェイルオーバーグループが作成され、ブロードキャストドメインのすべてのポートが追加されます。

情報	必須	値を入力します
IPspace 名 ブロードキャストドメインを割り当てる IPspace を指定します。  既存の IPspace を指定する必要があります。	はい。	
ブロードキャストドメイン名 ブロードキャストドメインの名前を指定します。  この名前は IPspace 内で一意である必要があります。	はい。	
MTU ブロードキャストドメインの最大伝送ユニットの値。一般に、* 1500 または 9000 *のいずれかに設定されます。  MTU 値は、ブロードキャストドメインのすべてのポートと、あとでブロードキャストドメインに追加されるすべてのポートに適用されます。  MTU値は、ネットワークに接続されているすべてのデバイスで同じである必要があります。e0Mポートの処理管理とサービスプロセッサのトラフィックでは、MTUを1500バイト以下に設定する必要があります。	はい。	

<p>ポート</p> <p>ポートは、到達可能性に基づいてブロードキャストドメインに割り当てられます。ポート割り当てが完了したら、を実行して到達可能性を確認します <code>network port reachability show</code> コマンドを実行します</p> <p>追加できるポートは、物理ポート、VLAN、インターフェイスグループです。</p>	はい。	
--	-----	--

## サブネット構成

サブネットには IP アドレスのプールとデフォルトゲートウェイが 1 つ含まれ、IPspace 内に配置された SVM で使用する LIF に割り当てることができます。

- SVM 上で LIF を作成する際には、IP アドレスとサブネットを指定する代わりにサブネット名を指定できます。
- サブネットはデフォルトゲートウェイと一緒に設定できるため、SVM を作成する際に別途デフォルトゲートウェイを作成する必要はありません。
- ブロードキャストドメインには、1 つ以上のサブネットを含めることができます。
- 複数のサブネットを IPspace のブロードキャストドメインと関連付けることによって、別のサブネット上にある SVM LIF を設定できます。
- 各サブネットには、同じ IPspace 内の他のサブネットに割り当てられた IP アドレスと重複しない IP アドレスを含める必要があります。
- サブネットを使用する代わりに、SVM データ LIF に特定の IP アドレスを割り当てて SVM 用のデフォルトゲートウェイを作成することができます。

情報	必須	値を入力します
<p>IPspace 名</p> <p>サブネットを割り当てる IPspace 。</p> <p>既存の IPspace を指定する必要があります。</p>	はい。	
<p>サブネット名</p> <p>サブネットの名前。</p> <p>この名前は IPspace 内で一意である必要があります。</p>	はい。	
<p>ブロードキャストドメイン名</p> <p>サブネットを割り当てるブロードキャストドメインを指定します。</p> <p>このブロードキャストドメインは、指定した IPspace 内に存在する必要があります。</p>	はい。	

サブネット名とマスク IP アドレスが存在するサブネットとマスクです。	はい。	
ゲートウェイ サブネットのデフォルトゲートウェイを指定できます。  ゲートウェイはサブネットを作成するときに割り当てなくても、あとから割り当てることができます。	いいえ	
IP アドレスの範囲 IP アドレスの範囲または特定の IP アドレスを指定できます。  たとえば、次のような範囲を指定できます。  192.168.1.1-192.168.1.100, 192.168.1.112, 192.168.1.145  IP アドレスの範囲を指定しない場合、指定したサブネット内のすべての範囲の IP アドレスが LIF に割り当て可能になります。	いいえ	
LIF との関連付けを強制的に更新します 既存の LIF との関連付けを強制的に更新するかどうかを指定します。  デフォルトでは、サービスプロセッサインターフェイスやネットワークインターフェイスが指定した範囲の IP アドレスを使用している場合、サブネットの作成は失敗します。  このパラメータを使用すると、手動でアドレスを指定したすべてのインターフェイスがサブネットに関連付けられ、コマンドは問題なく実行されます。	いいえ	

## SVM設定

SVM を使用して、クライアントやホストにデータを提供します。

記録した値は、デフォルトデータ SVM を作成するために使用します。MetroCluster ソース SVM を作成する場合は、を参照してください ["Fabric-attached MetroCluster Installation and Configuration Guide"](#) または ["ストレッチ MetroCluster インストールおよび設定ガイド"](#)。

情報	必須	値を入力します
----	----	---------

SVM 名 SVMの完全修飾ドメイン名（FQDN）。	はい。	
この名前はクラスタリーグ全体で一意である必要があります。		
ルートボリューム名 SVM ルートボリュームの名前。	はい。	
アグリゲート名 SVM ルートボリュームを保持するアグリゲートの名前。	はい。	
既存のアグリゲートを指定する必要があります		
セキュリティ形式 SVM ルートボリュームのセキュリティ形式。	はい。	
指定できる値は、 * ntfs *、 * unix *、および * mixed * です。		
IPspace 名 SVM を割り当てる IPspace 。	いいえ	
既存の IPspace を指定する必要があります。		
SVM の言語設定 SVM とそのボリュームで使用されるデフォルトの言語。	いいえ	
ボリュームの言語を指定しなかった場合は、SVM のデフォルトの言語設定は * C.UTF-8 * になります。		
SVM の言語の設定によって、SVM 内のすべての NAS ボリュームのファイル名とデータの表示に使用される文字セットが決定されます。		
言語は SVM の作成後に変更できます。		

## LIFの構成

SVM は、1 つ以上のネットワーク論理インターフェイス（LIF）を通じてクライアントとホストにデータを提供します。

情報	必須	値を入力します
SVM 名 LIF の SVM の名前。	はい。	

<p>LIF 名 LIFの名前。</p> <p>ノードに使用可能なデータポートがある場合は、ノードごとに複数のデータ LIF を割り当てたり、クラスタ内の任意のノードに LIF を割り当てたりできます。</p> <p>冗長性を確保するには、データサブネットごとに少なくとも 2 つのデータ LIF を作成する必要があり、特定のサブネットに割り当てられた LIF には、異なるノード上のホームポートを割り当てる必要があります。</p> <p>* 重要：ノンストップオペレーションソリューション用に Hyper-V または SQL Server over SMB をホストする SMB サーバを設定する場合、クラスタ内の SVM のすべてのノードに少なくとも 1 つのデータ LIF が存在する必要があります。</p>	<p>はい。</p>	
<p>サービスポリシー LIFのサービスポリシー。</p> <p>サービスポリシーは、LIF を使用できるネットワークサービスを定義します。データ SVM とシステム SVM の両方でデータトラフィックと管理トラフィックの管理に使用できる組み込みのサービスとサービスポリシーを用意しています。</p>	<p>はい。</p>	
<p>許可するプロトコル IPベースのLIFでは許可されたプロトコルは必要ありません。代わりにサービスポリシーの行を使用してください。</p> <p>ファイバチャネルポートで SAN LIF に許可するプロトコルを指定します。これらのプロトコルで LIF を使用できます。LIF を使用するプロトコルは、LIF が作成されたあとは変更できません。LIF の設定時にすべてのプロトコルを指定する必要があります。</p>	<p>いいえ</p>	
<p>ホームノード LIF がホームポートにリバートされるときに LIF が戻るノード。</p> <p>各データ LIF のホームノードを記録する必要があります。</p>	<p>はい。</p>	

<p>ホームポートまたはブロードキャストドメイン次のいずれかを選択します。</p> <p>* Port * : LIFがホームポートにリバートされるときに論理インターフェイスが戻るポートを指定します。これは、IPspace のサブネットにある最初の LIF に対してのみ実行されます。LIF がないと必須ではありません。</p> <p>* ブロードキャストドメイン * : ブロードキャストドメインを指定します。LIF がホームポートにリバートされるときに論理インターフェイスが戻る適切なポートがシステムによって選択されます。</p>	はい。	
<p>サブネット名 SVM に割り当てるサブネット。</p> <p>アプリケーションサーバへの継続的な可用性が確保された SMB 接続を確立するために使用されるデータ LIF はすべて、同じサブネット上にある必要があります。</p>	○ (サブネットを使用する場合)	

## DNS設定

NFS または SMB サーバを作成する前に、SVM で DNS を設定する必要があります。

情報	必須	値を入力します
<p>SVM 名 NFS または SMB サーバを作成する SVM の名前を指定します。</p>	はい。	
<p>DNS ドメイン名 ホストと IP の名前解決を行う際に、ホスト名に付加するドメイン名のリスト。</p> <p>ローカルドメインを最初にリストし、そのあとに DNS クエリが最も頻繁に実行されるドメイン名を指定します。</p>	はい。	



<p>DNSサーバのIPアドレス NFSサーバまたはSMBサーバの名前解決を提供するDNSサーバのIPアドレスのリスト。</p> <p>これらのDNSサーバには、Active DirectoryのLDAPサーバとSMBサーバが参加するドメインのドメインコントローラを見つけるために必要なサービスロケーションレコード（SRV）が含まれている必要があります。</p> <p>SRV レコードは、サービスの名前を、そのサービスを提供するサーバの DNS コンピュータ名にマップするために使用されます。ローカルの DNS クエリを介してサービスロケーションレコードを取得できない場合は、SMB サーバ ONTAP の作成に失敗します。</p> <p>ONTAP が Active Directory SRV レコードを確実に見つけることができるようにする最も簡単な方法は、Active Directory を統合した DNS サーバを SVM の DNS サーバとして構成することです。</p> <p>DNS 管理者が手動で、Active Directory ドメインコントローラに関する情報を含んだ DNS ゾーンに SRV のレコードを追加した場合は、Active Directory を統合していない DNS サーバを使用することができます。</p> <p>Active Directory 統合 SRV レコードの詳細については、トピックを参照してください  <a href="#">"Microsoft TechNet での Active Directory の DNS サポートのしくみ"</a>。</p>	はい。	
---	-----	--

## 動的 DNS 設定

動的 DNS を使用して自動的に Active Directory 統合 DNS サーバに DNS エントリを追加する前に、SVM に動的 DNS（DDNS）を設定する必要があります。

SVM 上にあるすべてのデータ LIF について DNS レコードが作成されます。SVM 上に複数のデータ LIF を作成することによって、割り当てられたデータ IP アドレスへのクライアント接続の負荷を分散することができます。DNS は、そのホスト名を使用して、割り当てられた IP アドレスへの接続をラウンドロビン方式で確立することで、接続の負荷を分散します。

情報	必須	値を入力します
SVM 名 NFS または SMB サーバを作成する SVM。	はい。	

DDNS を使用するかどうか DDNS を使用するかどうかを指定します。	はい。	
SVM 上で設定されている DNS サーバが DDNS をサポートしている必要があります。デフォルトでは、DDNS は無効になっています。		
セキュアな DDNS を使用するかどうか Secure DDNS は、Active Directory 統合 DNS でのみサポートされています。	いいえ	
Active Directory 統合 DNS で Secure DDNS 更新のみを許可する場合、このパラメータの値を true に設定する必要があります。		
デフォルトでは、Secure DDNS は無効になっています。		
Secure DDNS は、SVM 用の SMB サーバまたは Active Directory アカウントが作成されたあとにのみ有効にすることができます。		
DNS ドメインの FQDN DNS ドメインの FQDN。	いいえ	
SVM 上の DNS ネームサービスに設定されているドメイン名と同じ名前を使用する必要があります。		

## NASパスのフェイルオーバーワークフロー（ONTAP 9.7以前）

### NASパスのフェイルオーバーのセットアップ（ONTAP 9.7以前）

このワークフローは、ONTAP 9.1-9.7 の NAS パスフェイルオーバーを設定するためのネットワーク設定手順を示しています。このワークフローは次のことを前提としています。

- NAS パスのフェイルオーバーに関するベストプラクティスを使用して、ネットワーク構成を簡易化したい。
- System Manager ではなく、CLI を使用する。
- ONTAP 9.0 から 9.7 を実行している新しいシステムでネットワークを設定する。

9.7 よりも前のリリースの ONTAP を実行している場合は、ONTAP 9.8 以降で NAS パスフェイルオーバー手順を使用する必要があります。

- [ONTAP 9.8 以降の NAS パスフェイルオーバーワークフロー](#)

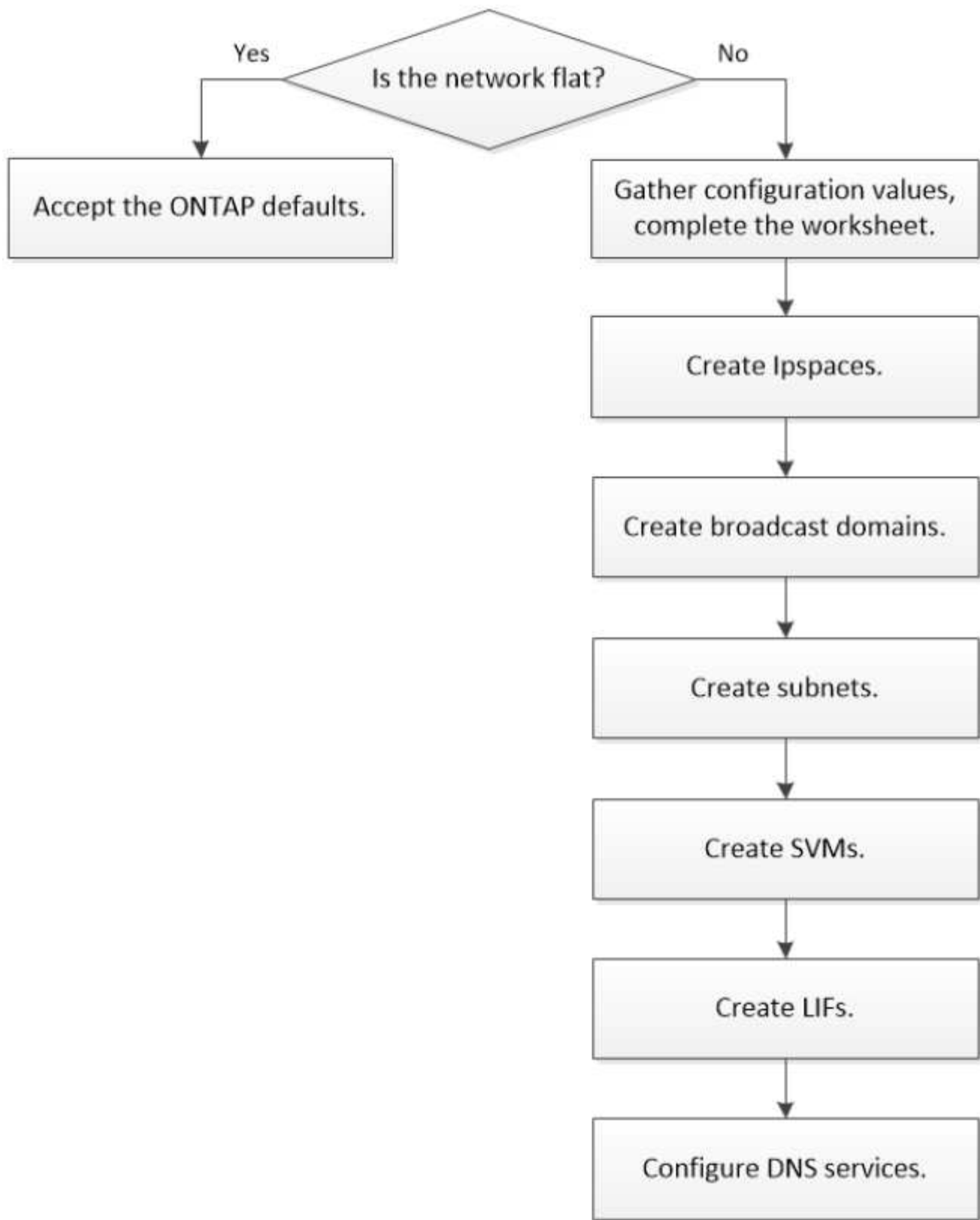
ネットワークコンポーネントと管理の詳細については、ネットワーク管理リファレンスを参照してください。

- [ネットワーク管理の概要](#)

## ワークフロー（ONTAP 9.7以前）

ネットワークの基本概念をすでに理解している場合は、NAS パスのフェイルオーバー設定に関するこの「ハンズオン」ワークフローを確認することで、ネットワークの設定にかかる時間を節約できます。

NAS LIF は、現在のポートでリンク障害が発生すると、稼働しているネットワークポートに自動的に移行します。ネットワークがフラット構成であれば、ONTAP のデフォルトを利用してパスのフェイルオーバーを管理できます。それ以外の場合は、このワークフローの手順に従ってパスのフェイルオーバーを設定する必要があります。



リンク障害の発生後に手動で移動しないかぎり、SAN LIF は移行されません。代わりに、ホストのマルチパステクノロジーによって、別の LIF にトラフィックが転送されます。詳細については、を参照してください ["SAN 管理"](#)。

1

**"ワークシートに記入する"**

ワークシートを使用して、NASパスのフェイルオーバーを計画します。

2

**"IPspaces を作成します"**

クラスタ内のSVMごとに個別のIPアドレススペースを作成します。

3

**"ブロードキャストドメインを作成する"**

ブロードキャストドメインを作成する

4

**"サブネットを作成する"**

サブネットを作成する。

5

**"SVMs を作成します"**

クライアントにデータを提供するSVMを作成します。

6

**"LIFs を作成します"**

データへのアクセスに使用するポートにLIFを作成します。

7

**"SVM用のDNSサービスの設定"**

NFSサーバまたはSMBサーバを作成する前に、SVM用のDNSサービスを設定してください。

## NASパスのフェイルオーバー設定用ワークシート（ONTAP 9.7以前）

NAS パスのフェイルオーバーを設定する前に、ワークシートのすべてのセクションに記入しておく必要があります。

### IPspace の設定

IPspace を使用すると、クラスタ内の SVM ごとに個別の IP アドレススペースを作成できます。これにより、管理上分離されたネットワークドメインのクライアントが、IP アドレスの同じサブネット範囲内の重複した IP アドレスを使用してクラスタのデータにアクセスできるようになります。

情報	必須	値を入力します
----	----	---------

IPspace 名	はい。	
<ul style="list-style-type: none"> <li>• IPspace の名前。</li> <li>• この名前はクラスタ内で一意である必要があります。</li> </ul>		

## ブロードキャストドメイン設定

ブロードキャストドメインは、同じレイヤ 2 ネットワークに属するポートをグループ化し、そのブロードキャストドメインポートに MTU を設定します。

ブロードキャストドメインは IPspace に割り当てられます。1 つの IPspace に複数のブロードキャストドメインを含めることができます。



LIF のフェイルオーバー先のポートは、LIF のフェイルオーバーグループのメンバーである必要があります。ブロードキャストドメインを作成すると、ONTAP によって同じ名前のフェイルオーバーグループが自動的に作成されます。フェイルオーバーグループには、ブロードキャストドメインに割り当てられたすべてのポートが含まれます。

情報	必須	値を入力します
IPspace 名	はい。	
<ul style="list-style-type: none"> <li>• ブロードキャストドメインを割り当てる IPspace を指定します。</li> <li>• 既存の IPspace を指定する必要があります。</li> </ul>		
ブロードキャストドメイン名	はい。	
<ul style="list-style-type: none"> <li>• ブロードキャストドメインの名前を指定します。</li> <li>• この名前は IPspace 内で一意である必要があります。</li> </ul>		

<p>MTU</p> <ul style="list-style-type: none"> <li>• ブロードキャストドメインの MTU を指定します。</li> <li>• 一般的には* 1500 または 9000 *に設定されます。</li> <li>• MTU 値は、ブロードキャストドメインのすべてのポートと、あとでブロードキャストドメインに追加されるすべてのポートに適用されます。</li> </ul> <div>  <p>MTU値は、ネットワークに接続されているすべてのデバイスで同じである必要があります。e0Mポートの処理管理とサービスプロセッサのトラフィックでは、MTUを1500バイト以下に設定する必要があります。</p> </div>	<p>はい。</p>	
<p>ポート</p> <ul style="list-style-type: none"> <li>• ブロードキャストドメインに追加するネットワークポートを指定します。</li> <li>• ブロードキャストドメインには、物理ポート、VLAN、インターフェイスグループ（ifgroup）を割り当てることができます。</li> <li>• ポートが別のブロードキャストドメイン内にある場合は、そのドメインから削除してからブロードキャストドメインに追加する必要があります。</li> <li>• ポートは、ノード名とポートの両方を指定して割り当てます。たとえば node1 : e0d とします。</li> </ul>	<p>はい。</p>	

## サブネット構成

サブネットには IP アドレスのプールとデフォルトゲートウェイが 1 つ含まれ、IPspace 内に配置された SVM で使用する LIF に割り当てることができます。

- SVM 上で LIF を作成する際には、IP アドレスとサブネットを指定する代わりにサブネット名を指定できます。
- サブネットはデフォルトゲートウェイと一緒に設定できるため、SVM を作成する際に別途デフォルトゲートウェイを作成する必要はありません。
- ブroadcastドメインには、1 つ以上のサブネットを含めることができます。  
複数のサブネットを IPspace のブroadcastドメインと関連付けることによって、別のサブネット上にある SVM LIF を設定できます。
- 各サブネットには、同じ IPspace 内の他のサブネットに割り当てられた IP アドレスと重複しない IP アドレスを含める必要があります。
- サブネットを使用する代わりに、SVM データ LIF に特定の IP アドレスを割り当てて SVM 用のデフォルトゲートウェイを作成することができます。

情報	必須	値を入力します
<b>IPspace 名</b> <ul style="list-style-type: none"> <li>• サブネットを割り当てる IPspace。</li> <li>• 既存の IPspace を指定する必要があります。</li> </ul>	はい。	
<b>サブネット名</b> <ul style="list-style-type: none"> <li>• サブネットの名前。</li> <li>• 名前は IPspace 内で一意である必要があります。</li> </ul>	はい。	
<b>ブroadcastドメイン名</b> <ul style="list-style-type: none"> <li>• サブネットを割り当てるブroadcastドメインを指定します。</li> <li>• ブroadcastドメインは、指定された IPspace 内に存在する必要があります。</li> </ul>	はい。	
<b>サブネット名とマスク</b> <ul style="list-style-type: none"> <li>• IP アドレスが存在するサブネットとマスクです。</li> </ul>	はい。	



<p>ゲートウェイ</p> <ul style="list-style-type: none"> <li>サブネットのデフォルトゲートウェイを指定できます。</li> <li>ゲートウェイはサブネットを作成するときに割り当てなくても、いつでも割り当てることができます。</li> </ul>	いいえ	
<p>IP アドレスの範囲</p> <ul style="list-style-type: none"> <li>IP アドレスの範囲または特定の IP アドレスを指定できます。 たとえば、次のような範囲を指定できます。 192.168.1.1– 192.168.1.100, 192.168.1.112, 192.168.1.145</li> <li>IP アドレスの範囲を指定しない場合、指定したサブネット内のすべての範囲の IP アドレスが LIF に割り当て可能になります。</li> </ul>	いいえ	
<p>LIF との関連付けを強制的に更新します</p> <ul style="list-style-type: none"> <li>既存の LIF との関連付けを強制的に更新するかどうかを指定します。</li> <li>デフォルトでは、サービスプロセスサインターフェイスやネットワークインターフェイスが指定した範囲の IP アドレスを使用している場合、サブネットの作成は失敗します。</li> <li>このパラメータを使用すると、手動でアドレスを指定したすべてのインターフェイスがサブネットに関連付けられ、コマンドは問題なく実行されます。</li> </ul>	いいえ	

## SVM設定

SVM を使用して、クライアントやホストにデータを提供します。

記録した値は、デフォルトデータ SVM を作成するために使用します。MetroCluster ソース SVM を作成する

場合は、を参照してください ["ファブリック接続 MetroCluster をインストール"](#) または ["ストレッチ MetroCluster をインストールします"](#)。

情報	必須	値を入力します
<p>SVM 名</p> <ul style="list-style-type: none"> <li>• SVM の名前。</li> <li>• SVM 名がクラスタリーグ全体で一意になるように、完全修飾ドメイン名（FQDN）を使用します。</li> </ul>	はい。	
<p>ルートボリューム名</p> <ul style="list-style-type: none"> <li>• SVM ルートボリュームの名前。</li> </ul>	はい。	
<p>アグリゲート名</p> <ul style="list-style-type: none"> <li>• SVM ルートボリュームを保持するアグリゲートの名前。</li> <li>• 既存のアグリゲートを指定する必要があります</li> </ul>	はい。	
<p>セキュリティ形式</p> <ul style="list-style-type: none"> <li>• SVM ルートボリュームのセキュリティ形式。</li> <li>• 指定できる値は、* ntfs *、* unix *、および * mixed * です。</li> </ul>	はい。	
<p>IPspace 名</p> <ul style="list-style-type: none"> <li>• SVM を割り当てる IPspace。</li> <li>• 既存の IPspace を指定する必要があります。</li> </ul>	いいえ	

SVM の言語設定 <ul style="list-style-type: none"> <li>• SVM とそのボリュームで使用されるデフォルトの言語。</li> <li>• ボリュームの言語を指定しなかった場合は、SVM のデフォルトの言語設定は * C.UTF-8 * になります。</li> <li>• SVM の言語の設定によって、SVM 内のすべての NAS ボリュームのファイル名とデータの表示に使用される文字セットが決定されます。 言語は SVM の作成後に変更できます。</li> </ul>	いいえ	
--	-----	--

## LIFの構成

SVM は、1 つ以上のネットワーク論理インターフェイス（LIF）を通じてクライアントとホストにデータを提供します。

情報	必須	値を入力します
SVM 名 <ul style="list-style-type: none"> <li>• LIF の SVM の名前。</li> </ul>	はい。	

<p>LIF 名</p> <ul style="list-style-type: none"> <li>• LIFの名前。</li> <li>• ノードに使用可能なデータポートがある場合は、ノードごとに複数のデータ LIF を割り当てたり、クラスタ内の任意のノードに LIF を割り当てたりできます。</li> <li>• 冗長性を確保するには、データサブネットごとに少なくとも 2 つのデータ LIF を作成する必要があり、特定のサブネットに割り当てられた LIF には、異なるノード上のホームポートを割り当てる必要があります。</li> <li>• 重要：ノンストップオペレーションソリューション用に Hyper-V または SQL Server over SMB をホストする SMB サーバを設定する場合、クラスタ内の SVM のすべてのノードに少なくとも 1 つのデータ LIF が存在する必要があります。</li> </ul>	<p>はい。</p>	
<p>LIF のロール</p> <ul style="list-style-type: none"> <li>• LIF のロール。</li> <li>• データ LIF にはデータロールが割り当てられます。</li> </ul>	<p>はい。 ONTAP 9.6から廃止</p>	<p>データ</p>
<p>サービスポリシー LIFのサービスポリシー。</p> <p>サービスポリシーは、LIF を使用できるネットワークサービスを定義します。データ SVM とシステム SVM の両方でデータトラフィックと管理トラフィックの管理に使用できる組み込みのサービスとサービスポリシーを用意しています。</p>	<p>はい。 ONTAP 9.6以降</p>	

<p>許可するプロトコル</p> <ul style="list-style-type: none"> <li>• LIF を使用できるプロトコル。</li> <li>• デフォルトでは、SMB、NFS、およびFlexCacheが許可されています。 FlexCache プロトコルを使用すると、Data ONTAP 7-Mode を実行しているシステムの FlexCache ボリュームの元のボリュームとしてボリュームを使用できます。</li> </ul> <div>  <p>LIF を使用するプロトコルは、LIF が作成されたあとは変更できません。LIF の設定時にすべてのプロトコルを指定する必要があります。</p> </div>	<p>いいえ</p>	
<p>ホームノード</p> <ul style="list-style-type: none"> <li>• LIF がホームポートにリバートされるときに LIF が戻るノード。</li> <li>• 各データ LIF のホームノードを記録する必要があります。</li> </ul>	<p>はい。</p>	
<p>ホームポートまたはブロードキャストドメイン</p> <ul style="list-style-type: none"> <li>• LIF がホームポートにリバートされるときに論理インターフェイスが戻るポート。</li> <li>• 各データ LIF のホームポートを記録する必要があります。</li> </ul>	<p>はい。</p>	
<p>サブネット名</p> <ul style="list-style-type: none"> <li>• SVM に割り当てるサブネット。</li> <li>• アプリケーションサーバへの継続的な可用性が確保された SMB 接続を確立するために使用されるデータ LIF はすべて、同じサブネット上にある必要があります。</li> </ul>	<p>○ (サブネットを使用する場合)</p>	

DNS設定

NFS または SMB サーバを作成する前に、SVM で DNS を設定する必要があります。

情報	必須	値を入力します
<div>SVM 名</div> <div><ul style="list-style-type: none"><li>NFS または SMB サーバを作成する SVM の名前を指定します。</li></ul></div>	はい。	
<div>DNS ドメイン名</div> <div><ul style="list-style-type: none"><li>ホストと IP の名前解決を行う際に、ホスト名に付加するドメイン名のリスト。</li><li>ローカルドメインを最初にリストし、そのあとに DNS クエリが最も頻繁に実行されるドメイン名を指定します。</li></ul></div>	はい。	

<p>DNSサーバのIPアドレス</p> <ul style="list-style-type: none"> <li>• NFSサーバまたはSMBサーバの名前解決を提供するDNSサーバのIPアドレスのリスト。</li> <li>• これらのDNSサーバには、Active DirectoryのLDAPサーバとSMBサーバが参加するドメインのドメインコントローラを見つけるために必要なサービスロケーションレコード（SRV）が含まれている必要があります。</li> </ul> <p>SRV レコードは、サービスの名前を、そのサービスを提供するサーバの DNS コンピュータ名にマップするために使用されます。ローカルの DNS クエリを介してサービスロケーションレコードを取得できない場合は、SMB サーバ ONTAP の作成に失敗します。</p> <p>ONTAP が Active Directory SRV レコードを確実に見つけることができるようにする最も簡単な方法は、Active Directory を統合した DNS サーバを SVM の DNS サーバとして構成することです。</p> <p>DNS 管理者が手動で、Active Directory ドメインコントローラに関する情報を含んだ DNS ゾーンに SRV のレコードを追加した場合は、Active Directory を統合していない DNS サーバを使用することができます。</p> <ul style="list-style-type: none"> <li>• Active Directory 統合 SRV レコードの詳細については、トピックを参照してください  <a href="#">"Microsoft TechNet での Active Directory の DNS サポートのしくみ"</a>。</li> </ul>	<p>はい。</p>	
--	------------	--

## 動的 DNS 設定

動的 DNS を使用して自動的に Active Directory 統合 DNS サーバに DNS エントリを追加する前に、SVM に動的 DNS （DDNS）を設定する必要があります。

SVM 上にあるすべてのデータ LIF について DNS レコードが作成されます。SVM 上に複数のデータ LIF を作成することによって、割り当てられたデータ IP アドレスへのクライアント接続の負荷を分散することができます。

ます。DNS は、そのホスト名を使用して、割り当てられた IP アドレスへの接続をラウンドロビン方式で確立することで、接続の負荷を分散します。

情報	必須	値を入力します
SVM 名  • NFS または SMB サーバを作成する SVM。	はい。	
DDNS を使用するかどうか  • DDNS を使用するかどうかを指定します。  • SVM 上で設定されている DNS サーバが DDNS をサポートしている必要があります。デフォルトでは、DDNS は無効になっています。	はい。	
セキュアな DDNS を使用するかどうか  • Secure DDNS は、Active Directory 統合 DNS でのみサポートされています。  • Active Directory 統合 DNS で Secure DDNS 更新のみを許可する場合、このパラメータの値を true に設定する必要があります。  • デフォルトでは、Secure DDNS は無効になっています。  • Secure DDNS は、SVM 用の SMB サーバまたは Active Directory アカウントが作成されたあとにのみ有効にすることができます。	いいえ	
DNS ドメインの FQDN  • DNS ドメインの FQDN。  • SVM 上の DNS ネームサービスに設定されているドメイン名と同じ名前を使用する必要があります。	いいえ	



# ネットワークポート

## ネットワークポート設定の概要

ポートは、物理ポート（NIC）と仮想ポート（インターフェイスグループや VLAN など）に分類されます。

仮想ポートは仮想ローカルエリアネットワーク（VLAN）とインターフェイスグループで構成されます。インターフェイスグループは複数の物理ポートを 1 つのポートとして扱い、VLAN は 1 つの物理ポートを複数の個別の論理ポートに分割します。

- 物理ポート：LIF は物理ポートに直接設定できます。
- インターフェイスグループ：複数の物理ポートを含むポートアグリゲートで、1 つのトランクポートとして機能します。インターフェイスグループには、シングルモード、マルチモード、またはダイナミックマルチモードがあります。
- VLAN：VLAN タグ付き（IEEE 802.1Q 規格）トラフィックを送受信する論理ポートです。VLAN ポートの特性には、ポートの VLAN ID が含まれます。基になる物理ポートまたはインターフェイスグループポートは VLAN トランクポートとみなされるため、接続するスイッチポートは VLAN ID をトランクするように構成する必要があります。

VLAN ポートの基になる物理ポートまたはインターフェイスグループポートは引き続き LIF をホストし、タグなしのトラフィックを送受信できます。

- 仮想 IP（VIP）ポート：VIP LIF のホームポートとして使用される論理ポート。VIP ポートはシステムによって自動的に作成され、サポートされる操作は限られています。VIP ポートは ONTAP 9.5 以降でサポートされています。

ポートの命名規則は *enumberletter*：

- 最初の文字は、ポートの種類を示します。  
「e」はイーサネットを表します。
- 2 文字目は、ポートアダプタのスロット番号を示します。
- 3 文字目は複数ポートアダプタ上のポートの位置を示します。  
「a」は最初のポート、「b」は 2 番目のポート、というように続きます。

例：e0b イーサネットポートは、ノードのマザーボード上にある 2 番目のポートです。

VLAN の名前には、という構文を使用する必要があります `port_name-vlan-id`。

`port_name` 物理ポートまたはインターフェイスグループを示します。

`vlan-id` ネットワーク上の VLAN ID を指定します。例：e1c-80 は有効な VLAN 名です。

## ネットワークポートを設定

物理ポートを組み合わせるインターフェイスグループを作成する

インターフェイスグループは Link Aggregation Group（LAG；リンクアグリゲーショング

ループ) と呼ばれ、同じノード上の複数の物理ポートを1つの論理ポートにまとめることで作成されます。論理ポートを使用すると、耐障害性と可用性が向上し、負荷も共有できます。

#### インターフェイスグループのタイプ

ストレージシステムでは、シングルモード、スタティックマルチモード、およびダイナミックマルチモードという 3 種類のインターフェイスグループがサポートされています。インターフェイスグループごとに、フォールトトレランスのレベルが異なります。マルチモードインターフェイスグループは、ネットワークトラフィックのロードバランシング方法を提供します。

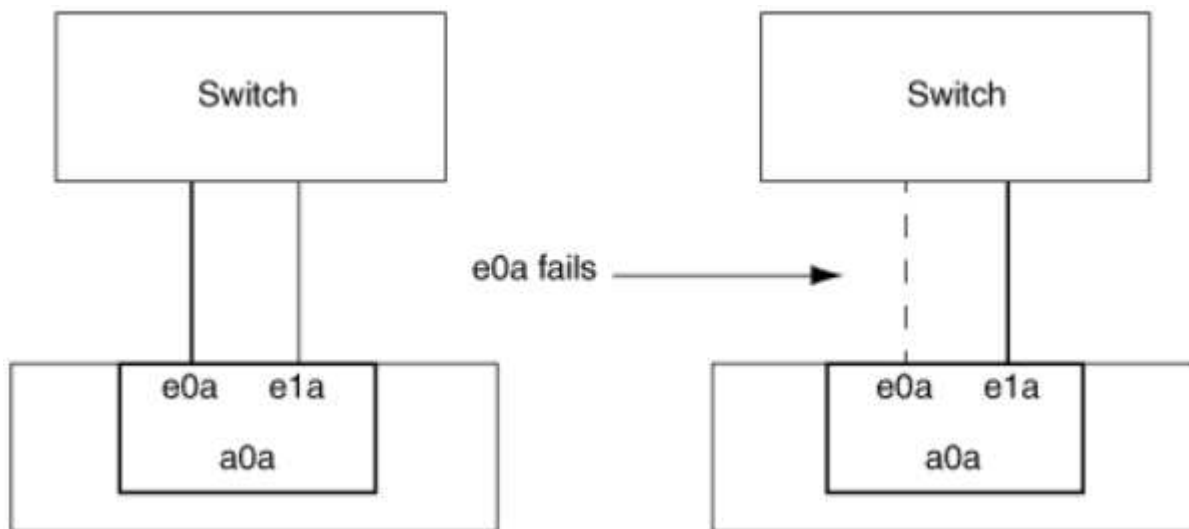
#### シングルモードインターフェイスグループの特性

シングルモードインターフェイスグループでは、インターフェイスグループの 1 つのインターフェイスだけがアクティブになります。他のインターフェイスはスタンバイで、アクティブインターフェイスに障害が発生した場合に動作を引き継ぎます。

シングルモードインターフェイスグループの特性は、次のとおりです。

- フェイルオーバーでは、クラスタがアクティブリンクを監視して、フェイルオーバーを制御します。クラスタがアクティブリンクを監視するため、スイッチを設定する必要はありません。
- シングルモードインターフェイスグループには、複数のスタンバイインターフェイスを設定できます。
- シングルモードインターフェイスグループが複数のスイッチをカバーする場合は、スイッチどうしを Inter-Switch Link (ISL ; スイッチ間リンク) で接続する必要があります。
- シングルモードインターフェイスグループの場合は、スイッチポートが同じブロードキャストドメインに属している必要があります。
- 送信元アドレスが 0.0.0.0 であるリンクモニタリング ARP パケットは、ポートを介して送信され、ポートが同じブロードキャストドメイン内にあることが確認されます。

次の図はシングルモードインターフェイスグループの例です。この例では、e0a と e1a が a0a というシングルモードインターフェイスグループを構成しています。アクティブインターフェイスの e0a に障害が発生すると、スタンバイインターフェイスの e1a が処理を引き継ぎ、スイッチとの接続を維持します。





シングルモード機能を実現するためには、フェイルオーバーグループを使用するアプローチが推奨されます。フェイルオーバーグループを使用すると、2 番目のポートを引き続き他の LIF に使用でき、未使用のままにする必要はありません。また、フェイルオーバーグループは複数のポートにまたがることができ、複数のノードのポートにまたがることができます。

## スタティックマルチモードインターフェイスグループの特性

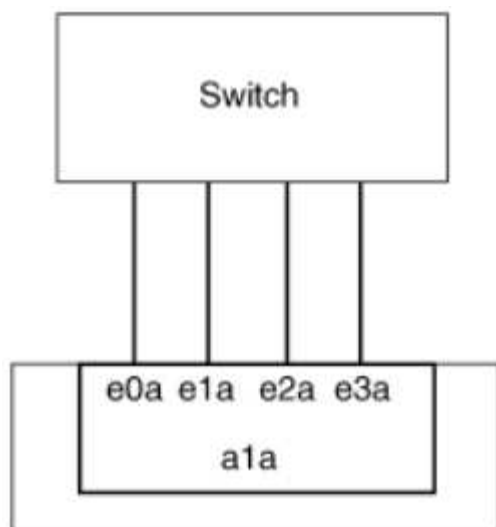
ONTAP に実装されているスタティックマルチモードインターフェイスグループは、IEEE 802.3ad (static) に準拠しています。スタティックマルチモードインターフェイスグループでは、アグリゲーションはサポートするがアグリゲーション設定のための制御パケット交換は行わないスイッチを使用できます。

スタティックマルチモードインターフェイスグループは、Link Aggregation Control Protocol (LACP) とも呼ばれる IEEE 802.3ad (dynamic) に準拠していません。LACP はポートアグリゲーションプロトコル (PAgP) と同等な、Cisco 独自のリンクアグリゲーションプロトコルです。

スタティックマルチモードインターフェイスグループの特性は、次のとおりです。

- インターフェイスグループ内のすべてのインターフェイスがアクティブで、1 つの MAC アドレスを共有します。
  - 複数の接続が、インターフェイスグループ内のインターフェイスに分散されます。
  - 各接続またはセッションは、インターフェイスグループ内の 1 つのインターフェイスを使用します。シーケンシャルロードバランシング方式を使用する場合、すべてのセッションはパケット単位で使用可能なリンク全体に分散され、インターフェイスグループの特定のインターフェイスにバインドされません。
- スタティックマルチモードインターフェイスグループは、最大「n-1」個のインターフェイスの障害から回復できます。n は、インターフェイスグループを構成しているインターフェイスの合計数です。
- あるポートで障害が発生した場合や切断された場合は、そのリンクを経由していたトラフィックが残りのインターフェイスの 1 つに自動的に再分散されます。
- スタティックマルチモードインターフェイスグループではリンクの喪失は検出できますが、クライアントへの接続の切断や、接続性とパフォーマンスに影響を及ぼす可能性があるスイッチの設定ミスは検出できません。
- スタティックマルチモードインターフェイスグループには、複数のスイッチポートでのリンクアグリゲーションをサポートするスイッチが必要です。インターフェイスグループの各リンクの接続先ポートがすべて 1 つの論理ポートを構成するよう、そのスイッチを設定します。一部のスイッチは、ジャンボフレーム用に構成されたポートのリンクアグリゲーションをサポートしていない場合があります。詳細については、スイッチベンダーのマニュアルを参照してください。
- スタティックマルチモードインターフェイスグループのインターフェイス間でのトラフィック分散には、いくつかのロードバランシングオプションを使用できます。

次の図はスタティックマルチモードインターフェイスグループの例を示したものです。インターフェイス e0a、e1a、e2a、および e3a は、a1a というマルチモードインターフェイスグループの一部です。この a1a マルチモードインターフェイスグループの 4 つのインターフェイスはすべてアクティブです。



1つの集約リンク内のトラフィックを複数の物理スイッチに分散できるテクノロジーがいくつか存在します。この機能を有効にするテクノロジーは、ネットワーク製品によって異なります。ONTAPのスタティックマルチモードインターフェイスグループは、IEEE 802.3規格に準拠しています。IEEE 802.3規格に対応または準拠すると言われている複数スイッチリンクアグリゲーションテクノロジーであれば、ONTAPと一緒に使用できます。

IEEE 802.3規格には、集約リンク内の送信デバイスが送信用の物理インターフェイスを決定することが規定されています。そのため、ONTAPが受け持つのは発信トラフィックの分散だけで、着信フレームの受信方法を制御することはできません。集約リンクでの着信トラフィックの転送を管理または制御する場合は、直接接続されたネットワークデバイス上でその転送を変更する必要があります。

#### ダイナミックマルチモードインターフェイスグループ

ダイナミックマルチモードインターフェイスグループは、Link Aggregation Control Protocol（LACP）を実装して、直接接続されたスイッチへのグループメンバーシップの通信を行います。LACPを使用すると、リンクステータスの喪失および直接接続されたスイッチポートと通信できないノードを検出できます。

ONTAPに実装されているダイナミックマルチモードインターフェイスグループは、IEEE 802.3 AD（802.1AX）に準拠しています。ONTAPは、シスコ独自のリンクアグリゲーションプロトコルである Port Aggregation Protocol（PAgP）をサポートしていません。

ダイナミックマルチモードインターフェイスグループには、LACPをサポートするスイッチが必要です。

ONTAPは、アクティブまたはパッシブモードに設定されているスイッチとの相性がよい、設定不可のアクティブモードでLACPを実装します。ONTAPは、IEEE 802.3 AD（802.1AX）の規定に従い、long および short のLACP タイマーを実装し、設定不可の値（3秒と90秒）で使します。

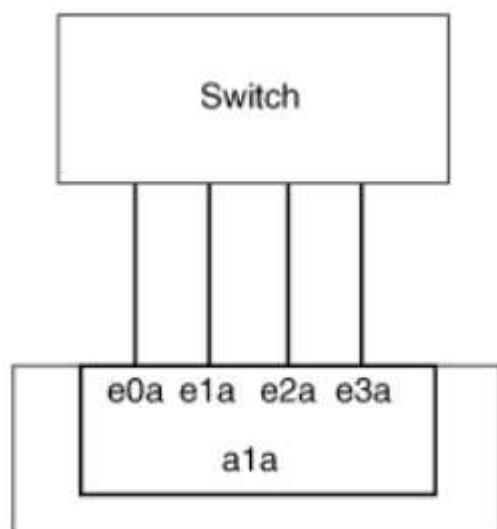
ONTAP ロードバランシングアルゴリズムは、発信トラフィックの転送に使用されるメンバーポートを決定しますが、着信フレームの受信方法は制御しません。スイッチは、スイッチのポートチャネルグループに設定されたロードバランシングアルゴリズムに基づいて、転送に使用されるポートチャネルグループのメンバー（個々の物理ポート）を決定します。したがって、スイッチの設定により、トラフィックを受信するストレージシステムのメンバーポート（個々の物理ポート）が決まります。スイッチ設定の詳細については、スイッチベンダーのマニュアルを参照してください。

あるインターフェイスが、連続するLACPプロトコルパケットの受信に失敗すると、そのインターフェイスに対して、「ifgrp status」コマンドで「lag\_inactive」と出力されます。既存のトラフィックは、残りのアクティブインターフェイスに自動的に再ルーティングされます。

ダイナミックマルチモードインターフェイスグループを使用する場合、次のルールが適用されます。

- ダイナミックマルチモードインターフェイスグループは、ポートベース、IP ベース、MAC ベース、またはラウンドロビンによるロードバランシング方式を使用するように設定する必要があります。
- ダイナミックマルチモードインターフェイスグループでは、すべてのインターフェイスをアクティブにして、1つの MAC アドレスを共有する必要があります。

次の図は、ダイナミックマルチモードインターフェイスグループの例です。インターフェイス e0a、e1a、e2a、および e3a は、a1a というマルチモードインターフェイスグループの一部です。a1a ダイナミックマルチモードインターフェイスグループの 4 つのインターフェイスはすべてアクティブです。



#### マルチモードインターフェイスグループでのロードバランシング

IP アドレスベース、MAC アドレスベース、シーケンシャル、またはポートベースのロードバランシング方式を使用してマルチモードインターフェイスグループのネットワークポート上でネットワークトラフィックを均等に分散させることにより、マルチモードインターフェイスグループのすべてのインターフェイスが送信トラフィックに均等に利用されるようにすることができます。

マルチモードインターフェイスグループのロードバランシング方式を指定できるのは、インターフェイスグループの作成時だけです。

- **ベストプラクティス \***：可能なかぎりポートベースのロードバランシングを推奨します。ポートベースのロードバランシングは、ネットワークに特定の理由または制限がない場合にのみ使用してください。

#### ポートベースのロードバランシング

推奨される方法はポートベースのロードバランシングです。

ポートベースのロードバランシング方式を使用して、マルチモードインターフェイスグループ上のトラフィックをトランスポートレイヤ（TCP または UDP）ポートに基づいて均等に分散させることができます。

ポートベースのロードバランシング方式では、トランスポートレイヤのポート番号に加え、送信元と送信先の IP アドレスに対して高速ハッシュアルゴリズムを使用します。

## IP アドレスおよび MAC アドレスによるロードバランシング

IP アドレスおよび MAC アドレスによるロードバランシングは、マルチモードインターフェイスグループのトラフィックを均等にする方法です。

これらのロードバランシング方式では、送信元アドレスと送信先アドレス（IP アドレスと MAC アドレス）に対して高速ハッシュアルゴリズムを使用します。ハッシュアルゴリズムの結果がリンク状態が UP でないインターフェイスに一致した場合は、次のアクティブなインターフェイスが使用されます。



ルータに直接接続するシステムでインターフェイスグループを作成する場合は、MAC アドレスによるロードバランシング方式を選択しないでください。このような構成では、すべての発信 IP フレームの宛先 MAC アドレスはルータの MAC アドレスです。そのため、使用されるインターフェイスグループのインターフェイスは 1 つだけです。

IP アドレスによるロードバランシングは、IPv4 アドレスと IPv6 アドレスの両方で同様に機能します。

## シーケンシャルロードバランシング

シーケンシャルロードバランシングでは、ラウンドロビンアルゴリズムを使用して複数のリンク間でパケットを均等に分散できます。シーケンシャルオプションを使用すると、1 つの接続のトラフィックを複数のリンクに分散させて、単一の接続のスループットを向上させることができます。

ただし、シーケンシャルロードバランシングによって原因のパケット配信順序が乱れることがあるため、パフォーマンスが大幅に低下する可能性があります。したがって、一般にシーケンシャルロードバランシングは推奨されません。

インターフェイスグループまたは**LAG**を作成します

インターフェイスグループまたはLAG（シングルモード、スタティックマルチモード、またはダイナミックマルチモード（LACP））を作成すると、集約されたネットワークポートの機能を組み合わせて、クライアントに単一のインターフェイスを提供できます。

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

## System Manager の略

- System Managerを使用してLAGを作成します。\*

### 手順

1. [\*Network]>[Ethernet port]>[+ Link Aggregation Group]を選択して、LAGを作成します。
2. ドロップダウンリストからノードを選択します。
3. 次のいずれかを選択します。
  - a. ONTAP to \* automatically select broadcast domain (推奨) \*。
  - b. ブロードキャストドメインを手動で選択します。
4. LAGを形成するポートを選択します。
5. モードを選択します。
  - a. Single：一度に1つのポートのみが使用されます。
  - b. 複数：すべてのポートを同時に使用できます。
  - c. LACP：LACPプロトコルによって、使用できるポートが決まります。
6. ロードバランシングを選択します。
  - a. IPベース
  - b. MACベース
  - c. ポート
  - d. シーケンシャル
7. 変更を保存します。

The screenshot shows the 'Add Link Aggregation Group' dialog box in the ONTAP System Manager interface. The left sidebar contains a navigation menu with categories like DASHBOARD, INSIGHTS, STORAGE, NETWORK, EVENTS & JOBS, PROTECTION, HOSTS, and CLUSTER. The 'NETWORK' section is expanded, showing 'Ethernet Ports'. The main dialog box has the following fields and options:

- NODE:** A dropdown menu showing 'sti47-vs1m-ucs521e'.
- BROADCAST DOMAIN:** A dropdown menu showing 'Automatically select broadcast domain (Recommended)'. A red arrow points to this field with a note: 'Note: Instead of a global switch or checkbox, what if we expose BD dropdown with "Automatic" as a default selection?'.
- PORTS TO INCLUDE:** Two checkboxes, 'e0e' and 'e0f', both of which are unchecked.
- MODE:** Three radio button options: 'Single' (selected), 'Multiple', and 'LACP'. Below 'Single' is the text 'Only one port is used at a time.' Below 'Multiple' is 'All ports can be used simultaneously.' Below 'LACP' is 'The LACP protocol determines the ports that can be used.'
- LOAD DISTRIBUTION:** Two radio button options: 'IP based' (selected) and 'MAC based'. Below 'IP based' is the text 'Network traffic is distributed based on the destination IP address.' Below 'MAC based' is 'Network traffic is distributed based on the next-hop MAC addresses.'

## CLI の使用

- CLIを使用してインターフェイスグループを作成\*

ポートインターフェイスグループに適用される設定上の制限事項の一覧については、を参照してください `network port ifgrp add-port` のマニュアルページ。

マルチモードインターフェイスグループを作成するときは、次のいずれかのロードバランシング方式を指定できます。

- `port` : ネットワークトラフィックは、トランスポートレイヤ（TCP / UDP）ポートに基づいて分散されます。これは推奨されるロードバランシング方式です。
- `mac` : ネットワークトラフィックはMACアドレスに基づいて分散されます。
- `ip` : ネットワークトラフィックはIPアドレスに基づいて分散されます。
- `sequential` : ネットワークトラフィックは受信したとおりに分散されます。



インターフェイスグループの MAC アドレスは、基盤となるポートの順序およびそれらのポートがブートアップ時にどのように初期化されるかによって決まります。そのため、`ifgrp` の MAC アドレスがリブート後や ONTAP のアップグレード後に変わる可能性があることを想定しておいてください。

## ステップ

を使用します `network port ifgrp create` インターフェイスグループを作成するコマンド。

インターフェイスグループの名前には、という構文を使用する必要があります `a<number><letter>`。たとえば、`a0a`、`a0b`、`a1c`、`a2a` は有効なインターフェイスグループ名です。

このコマンドの詳細については、を参照してください ["ONTAP 9 のコマンド"](#)。

次の例は、ポートの分散機能を使用し、モードを `multimode` に設定して、`a0a` という名前のインターフェイスグループを作成する方法を示しています。

```
network port ifgrp create -node cluster-1-01 -ifgrp a0a -distr-func port -mode multimode
```

インターフェイスグループまたは**LAG**にポートを追加します

インターフェイスグループまたはLAGには、すべてのポート速度に対して最大16個の物理ポートを追加できます。

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



## System Manager の略

- System Managerを使用して、LAGにポートを追加します。\*

### 手順

1. [\*Network]>[Ethernet port]>[LAG]を選択して、LAGを編集します。
2. LAGに追加する同じノードの追加ポートを選択します。
3. 変更を保存します。

### CLI の使用

- CLIを使用して、インターフェイス・グループにポートを追加します。\*

### ステップ

インターフェイスグループにネットワークポートを追加します。

```
network port ifgrp add-port
```

このコマンドの詳細については、を参照してください ["ONTAP 9 のコマンド"](#)。

次の例は、a0a というインターフェイスグループにポート e0c を追加する方法を示しています。

```
network port ifgrp add-port -node cluster-1-01 -ifgrp a0a -port e0c
```

ONTAP 9.8 以降では、最初の物理ポートがインターフェイスグループに追加されてから約 1 分後に、インターフェイスグループが適切なブロードキャストドメインに自動的に配置されます。ONTAP でこの処理を行わず、ifgrpをブロードキャストドメインに手動で配置する場合は、を指定します `-skip -broadcast-domain-placement` パラメータをに指定します ifgrp add-port コマンドを実行します

インターフェイスグループまたは**LAG**からポートを削除します

LIF をホストするインターフェイスグループからポートを削除できます。ただし、そのポートがインターフェイスグループの最後のポートでない場合に限りです。最後のポートをインターフェイスグループから削除しないという前提により、インターフェイスグループが LIF をホストできない、またはインターフェイスグループを LIF のホームポートに指定できないという要件はありません。ただし、最後のポートを削除する場合は、先にインターフェイスグループから LIF を移行または移動しておく必要があります。

このタスクについて

インターフェイスグループまたはLAGから最大16個のポート（物理インターフェイス）を削除できます。

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

## System Manager の略

- System Managerを使用して、LAGからポートを削除します。\*

### 手順

1. [\*Network]>[Ethernet port]>[LAG]を選択して、LAGを編集します。
2. LAGから削除するポートを選択します。
3. 変更を保存します。

### CLI の使用

- CLIを使用して、インターフェイスグループからポートを削除します。\*

### ステップ

インターフェイスグループからネットワークポートを削除します。

```
network port ifgrp remove-port
```

次の例は、a0a というインターフェイスグループからポート e0c を削除する方法を示しています。

```
network port ifgrp remove-port -node cluster-1-01 -ifgrp a0a -port e0c
```

インターフェイスグループまたは**LAG**を削除します

基盤となる物理ポートにLIFを直接設定したり、インターフェイスグループやLAGモード、または分散機能を変更したりする場合は、インターフェイスグループまたはLAGを削除できます。

作業を開始する前に

- インターフェイスグループまたはLAGがLIFをホストしていないことを確認する必要があります。
- インターフェイスグループまたはLAGは、LIFのホームポートでもフェイルオーバーターゲットでもない必要があります。

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

## System Manager の略

- LAGを削除するには、System Managerを使用します。\*

### 手順

1. [\*Network]>[Ethernet port]>[LAG]を選択して、LAGを削除します。
2. 削除するLAGを選択します。
3. LAGを削除します。

### CLI の使用

- CLIを使用してインターフェイスグループ\*を削除してください

### ステップ

を使用します `network port ifgrp delete` インターフェイスグループを削除するコマンド。

このコマンドの詳細については、を参照してください ["ONTAP 9 のコマンド"](#)。

次に、a0b という名前のインターフェイスグループを削除する例を示します。

```
network port ifgrp delete -node cluster-1-01 -ifgrp a0b
```

## 物理ポートを介して VLAN を設定します

ONTAPでVLANを使用すると、分離されたブロードキャストドメインを作成してネットワークを論理的にセグメント化できます。ブロードキャストドメインは、物理的な境界に定義された従来のブロードキャストドメインとは異なり、スイッチポート単位で定義されます。

VLAN は、複数の物理ネットワークセグメントにまたがることができます。VLAN に属するエンドステーションは、機能またはアプリケーションに基づいて関連付けられます。

たとえば、エンジニアリングや財務などの部門単位、またはリリース 1 やリリース 2 などのプロジェクト単位で、VLAN のエンドステーションをまとめることができます。VLAN ではエンドステーションが物理的に近接して配置されることは重要ではないので、エンドステーションを地理的に分散させても、スイッチドネットワークにブロードキャストドメインを含めることができます。

ONTAP 9.13.1および9.14.1では、任意の論理インターフェイス（LIF）で使用されておらず、接続されているスイッチでネイティブVLAN接続が確立されていないタグなしポートは、デグレードとマークされます。これは使用されていないポートを特定するためのもので、停止を示すものではありません。ネイティブVLANでは、ONTAP CFMブロードキャストなどのタグなしトラフィックをifgrpベースポートで許可します。タグなしトラフィックをブロックしないように、スイッチにネイティブVLANを設定します。

VLAN の管理では、VLAN を作成、削除、またはその情報を表示できます。



スイッチのネイティブ VLAN と同じ識別子の VLAN をネットワークインターフェイス上に作成しないでください。たとえば、ネットワークインターフェイス e0b がネイティブ VLAN 10 に割り当てられている場合、そのインターフェイス上に VLAN e0b-10 を作成しないでください。

## VLAN を作成します

同じネットワークドメイン内の分離されたブロードキャストドメインを管理するためのVLANを作成するには、System Managerまたはを使用します `network port vlan create` コマンドを実行します

作業を開始する前に

次の要件を満たしていることを確認します。

- ネットワーク上に配置されたスイッチが、IEEE 802.1Q 規格に準拠しているか、またはベンダー固有の VLAN を実装している。
- 複数の VLAN をサポートするには、エンドステーションが 1 つ以上の VLAN に属するように静的に設定されている必要があります。
- VLAN は、クラスタ LIF をホストしているポートに接続されていない。
- VLAN は、「Cluster」IPspace に割り当てられているポートに接続されていない。
- VLAN は、メンバーポートのないインターフェイスグループポートには作成されません。

このタスクについて

VLAN を作成すると、クラスタ内の指定したノードのネットワークポートにその VLAN が接続されます。

VLAN を初めてポートに設定したときに、ポートが停止してネットワーク接続が一時的に切断されることがあります。その後同じポートに VLAN を追加しても、ポートの状態には影響しません。



スイッチのネイティブ VLAN と同じ識別子の VLAN をネットワークインターフェイス上に作成しないでください。たとえば、ネットワークインターフェイス e0b がネイティブ VLAN 10 に割り当てられている場合、そのインターフェイス上に VLAN e0b-10 を作成しないでください。

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

## System Manager の略

- System Managerを使用してVLAN \*を作成します

ONTAP 9.12.0以降では、ブロードキャストドメインを自動的に選択することも、リストから手動で選択することもできます。これまでは、レイヤ2接続に基づいて常にブロードキャストドメインが自動的に選択されていました。ブロードキャストドメインを手動で選択した場合は、ブロードキャストドメインを手動で選択すると接続が失われる可能性があることを示す警告が表示されます。

### 手順

1. Network > Ethernet port > +VLAN \*を選択します。
2. ドロップダウンリストからノードを選択します。
3. 次のいずれかを選択します。
  - a. ONTAP to \* automatically select broadcast domain (推奨) \*。
  - b. リストからブロードキャストドメインを手動で選択します。
4. VLANを形成するポートを選択します。
5. VLAN IDを指定します。
6. 変更を保存します。

### CLI の使用

- CLIを使用してVLAN \*を作成します

特定の状況で、ハードウェア問題 やソフトウェアの設定ミスを修正せずにデグレード状態のポートにVLANポートを作成する場合は、を設定できます `-ignore-health-status` のパラメータ `network port modify` としてコマンドを実行します `true`。

### 手順

1. を使用します `network port vlan create` VLANを作成するコマンド。
2. どちらかを指定する必要があります `vlan-name` または `port` および `vlan-id` VLAN作成時のオプション。  
VLAN 名は、ポート（またはインターフェイスグループ）の名前と、ネットワークスイッチのVLANの識別子をハイフンでつないだ形式です。例： `e0c-24` および `e1c-80` は有効なVLAN名です。

次に、VLANを作成する例を示します `e1c-80` ネットワークポートに接続されています `e1c` をクリックします `cluster-1-01`：

```
network port vlan create -node cluster-1-01 -vlan-name e1c-80
```

ONTAP 9.8 以降では、作成後約 1 分後に、VLAN が適切なブロードキャストドメインに自動的に配置されます。ONTAP でこの処理を行わず、VLANをブロードキャストドメインに手動で配置する場合は、を指定します `-skip-broadcast-domain-placement` パラメータをに指定します `vlan create` コマンドを実行します

このコマンドの詳細については、を参照してください ["ONTAP 9 のコマンド"](#)。

## VLANを編集します

ブロードキャストドメインを変更したり、VLANを無効にしたりできます。

### System Managerを使用してVLANを編集する

ONTAP 9.12.0以降では、ブロードキャストドメインを自動的に選択することも、リストから手動で選択することもできます。以前は、レイヤ2接続に基づいて、常に自動的にブロードキャストドメインが選択されていました。ブロードキャストドメインを手動で選択した場合は、ブロードキャストドメインを手動で選択すると接続が失われる可能性があることを示す警告が表示されます。

#### 手順

1. Network > Ethernet port > VLAN \*を選択します。
2. 編集アイコンを選択します。
3. 次のいずれかを実行します。
  - リストから別のブロードキャストドメインを選択して、ブロードキャストドメインを変更します。
  - [有効\*]チェックボックスをオフにします。
4. 変更を保存します。

## VLAN を削除します

NIC をスロットから取り外す前に、VLAN の削除が必要になることがあります。VLAN を削除すると、そのVLAN を使用しているすべてのフェイルオーバールールとフェイルオーバーグループから自動的に削除されます。

#### 作業を開始する前に

VLAN に関連付けられている LIF がないことを確認します。

#### このタスクについて

ポートから最後の VLAN 原因を削除すると、そのポートからネットワークが一時的に切断される可能性があります。

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

## System Manager の略

- System Managerを使用してVLANを削除します。\*

### 手順

1. Network > Ethernet port > VLAN \*を選択します。
2. 削除するVLANを選択します。
3. [ 削除 ( Delete ) ] をクリックします。

### CLI の使用

- CLIを使用してVLAN \*を削除します

### ステップ

を使用します `network port vlan delete` VLANを削除するコマンド。

次に、VLANを削除する例を示します `e1c-80` ネットワークポートから `e1c` をクリックします `cluster-1-01` :

```
network port vlan delete -node cluster-1-01 -vlan-name e1c-80
```

ネットワークポートの属性を変更します

物理ネットワークポートの自動ネゴシエーション、二重モード、フロー制御、速度、および健全性の設定を変更することができます。

作業を開始する前に

LIF をホストしているポートは変更できません。

このタスクについて

- 100GbE、40GbE、10GbE、または1GbEのネットワークインターフェ이스の管理設定を変更することは推奨されません。

二重モードおよびポート速度の設定値のことを管理設定と呼びます。ネットワークの制限によっては、管理設定が運用設定（ポートで実際に使用されている二重モードおよび速度）と異なる場合があります。

- インターフェイスグループの基盤となる物理ポートの管理設定を変更することは推奨されません。
  - `-up-admin` パラメータ（advanced権限レベルで使用可能）は、ポートの管理設定を変更します。
- を設定することは推奨されません `-up-admin` ノード上のすべてのポート、またはノードで動作している最後のクラスタLIFをホストしているポートの管理設定を`false`にします。
- 管理ポートのMTUサイズを変更することは推奨されません。 `e0M`。
- ブロードキャストドメインのポートの MTU サイズを、そのブロードキャストドメイン用に設定された MTU 値以外に変更することはできません。
- VLAN の MTU サイズがベースポートの MTU サイズの値を超えることはできません。

## 手順

1. ネットワークポートの属性を変更します。

```
network port modify
```

2. を設定できます `-ignore-health-status` フィールドを `true` に設定すると、指定したポートのネットワークポートヘルスステータスを無視できるようになります。

ネットワークポートの健全性ステータスは「デグレード」から「正常」に自動的に変わり、このポートを使用して LIF をホストできるようになりました。クラスターポートのフロー制御はに設定する必要があります `none`。デフォルトでは、フロー制御はに設定されています `full`。

次のコマンドは、フロー制御を `none` に設定してポート `e0b` のフロー制御を無効にします。

```
network port modify -node cluster-1-01 -port e0b -flowcontrol-admin none
```

**10GbE** 接続用に、**40GbE NIC** ポートを複数の **10GbE** ポートに変換します

**X1144A-R6** および **X91440A-R6 40GbE** ネットワークインターフェイスカード（NIC）を変換して、4 個の **10GbE** ポートをサポートできます。

どちらかの NIC をサポートするハードウェアプラットフォームを、10GbE のクラスターインターコネクトと顧客データ接続をサポートするクラスターに接続する場合は、NIC を変換して必要な 10GbE 接続を提供する必要があります。

作業を開始する前に

サポートされているブレイクアウトケーブルを使用する必要があります。

このタスクについて

NIC をサポートするプラットフォームの一覧については、を参照してください "[Hardware Universe](#)"。



X1144A-R6 NIC では、4 つの 10GbE 接続をサポートするために変換できるのはポート A だけです。ポート A が変換されると、ポート e は使用できなくなります。

## 手順

1. メンテナンスモードに切り替えます。
2. NIC を 40GbE のサポートから 10GbE のサポートに変換します。

```
nicadmin convert -m [40G | 10G] [port-name]
```

3. `convert` コマンドを使用した後、ノードを停止します。
4. ケーブルを取り付けるか、交換します。
5. ハードウェアモデルに応じて、SP（サービスプロセッサ）または BMC（ベースボード管理コントローラ）を使用してノードの電源を再投入し、変換を有効にします。



## ノードからのNICの取り外し (ONTAP 9.8以降)

このトピックは 環境 ONTAP 9.8以降です。障害の発生した NIC をスロットから取り外したり、メンテナンスのために NIC を別のスロットに移したりしなければならない場合があります。

### 手順

1. ノードの電源をオフにします。
2. NIC をスロットから物理的に取り外します。
3. ノードの電源をオンにします。
4. ポートが削除されたことを確認します。

```
network port show
```



ONTAP は、すべてのインターフェイスグループからポートを自動的に削除します。ポートがインターフェイスグループの唯一のメンバーであった場合は、インターフェイスグループが削除されます。

5. ポートに VLAN が設定されている場合は、ポートが取り外されます。次のコマンドを使用すると、削除された VLAN を表示できます。

```
cluster controller-replacement network displaced-vlans show
```



。displaced-interface show、displaced-vlans show`および `displaced-vlans restore コマンドは一意であり、で始まる完全修飾コマンド名は必要ありません cluster controller-replacement network。

6. これらの VLAN は削除されますが、次のコマンドを使用してリストアできます。

```
displaced-vlans restore
```

7. ポートに LIF が設定されている場合は、同じブロードキャストドメインの別のポート上のそれらの LIF に新しいホームポートが ONTAP によって自動的に選択されます。同じ Filer 上に適切なホーム・ポートが見つからない場合、これらの LIF は取り外されたと見なされます。削除した LIF を表示するには、次のコマンドを使用します。

```
displaced-interface show
```

8. 同じノードのブロードキャストドメインに新しいポートを追加すると、LIF のホームポートは自動的にリストアされます。または、を使用してホームポートを設定することもできます network interface modify -home-port -home-node or use the displaced- interface restore コマンドを実行します

## ノードからのNICの取り外し（ONTAP 9.7以前）

このトピックは環境 ONTAP 9.7 以前です。障害の発生した NIC をスロットから取り外したり、メンテナンスのために NIC を別のスロットに移したりしなければならない場合があります。

作業を開始する前に

- NIC ポートにホストされているすべての LIF を移行または削除しておく必要があります。
- NIC のポートが LIF のホームポートでないことを確認します。
- NIC からポートを削除するには advanced 権限が必要です。

手順

1. NIC からポートを削除します。

```
network port delete
```

2. ポートが削除されたことを確認します。

```
network port show
```

3. network port show コマンドの出力に、削除したポートが表示される場合は、手順 1 を繰り返します。

## ネットワークポートの監視

ネットワークポートのヘルスを監視する

ネットワークポートの ONTAP 管理では、健全性の自動監視機能と一連のヘルスマニタを使用して、LIF のホストに適さない可能性のあるネットワークポートを特定できます。

このタスクについて

ヘルスマニタで健全でないと判断されたネットワークポートは、EMS メッセージで管理者に警告が送信されるか、またはデグレードとマークされます。LIF に対して別の正常なフェイルオーバーターゲットが用意されている場合、ONTAP はデグレード状態のネットワークポートでの LIF のホストを回避します。ポートは、リンクフラッピング（リンクがアップとダウンを高速で繰り返す状態）やネットワークパーティショニングなどの軽度な障害イベントが原因でデグレード状態になります。

- クラスタ IPspace 内のネットワークポートは、リンクフラッピングが発生した場合や、ブロードキャストドメイン内の他のネットワークポートへのレイヤ 2（L2）到達可能性が失われた場合にデグレードとマークされます。
- クラスタ以外の IPspace 内のネットワークポートは、リンクフラッピングが発生した場合にデグレードとマークされます。

デグレード状態のポートの以下の動作に注意してください。

- デグレード状態のポートを VLAN またはインターフェイスグループに含めることはできません。

インターフェイスグループのメンバーポートがデグレードとマークされていて、インターフェイスグループが正常とマークされている場合は、そのインターフェイスグループで LIF をホストできます。

- LIF は、デグレード状態のポートから正常なポートに自動的に移行されます。
- フェイルオーバー時には、デグレード状態のポートはフェイルオーバーターゲットとみなされません。正常なポートがない場合は、通常のフェイルオーバーポリシーに従って、デグレード状態のポートが LIF をホストします。
- デグレード状態のポートに LIF を作成、移行、リバートすることはできません。

を変更できます `ignore-health-status` ネットワークポートをに設定します `true`。これで、正常なポートで LIF をホストできます。

## 手順

1. advanced 権限モードにログインします。

```
set -privilege advanced
```

2. ネットワークポートのヘルスの監視が有効になっているヘルスマニタを確認します。

```
network options port-health-monitor show
```

ポートのヘルスステータスは、ヘルスマニタの値によって決まります。

ONTAP でデフォルトで有効になっていて使用可能なヘルスマニタは次のとおりです。

- リンクフラッピングヘルスマニタ：リンクフラッピングを監視します

5 分以内に複数回のリンクフラッピングが発生しているポートは、デグレードとマークされます。

- L2 到達可能性ヘルスマニタ：同じブロードキャストドメインに設定されたすべてのポートで相互のポートに対するレイヤ 2 到達可能性が確保されているかどうかを監視します

このヘルスマニタは、すべての IPspace におけるレイヤ 2 到達可能性の問題を報告しますが、デグレードとマークされるのはクラスタ IPspace 内のポートのみです。

- CRC モニタ：ポートの CRC 統計を監視します

このヘルスマニタはポートをデグレードとマークしませんが、CRC エラー率が非常に高い場合に EMS メッセージを生成します。

3. を使用して、IPspaceのヘルスマニタを必要に応じて有効または無効にします `network options port-health-monitor modify` コマンドを実行します

4. ポートの詳細な健全性を表示します。

```
network port show -health
```

コマンド出力には、ポートのヘルスステータスが表示されます。 `ignore health status` 設定、およびポートがデグレードとマークされた理由のリスト。

ポートのヘルスステータスはになります `healthy` または `degraded`。

状況に応じて `ignore health status` 設定はです `true` `ポートのヘルスステータスがから変更されたことを示します` `degraded` 終了: `healthy` 管理者によって作成されます。

状況に応じて `ignore health status` 設定はです `false` の場合、ポートのヘルスステータスはシステムによって自動的に判断されます。

ネットワークポートの到達可能性を監視する (ONTAP 9.8以降)

ONTAP 9.8 以降には、到達可能性の監視機能が組み込まれています。この監視機能を使用して、物理ネットワークポートが ONTAP 構成と一致しない状況を特定します。場合によっては、ONTAP がポートの到達可能性を修復できます。それ以外の場合は、追加の手順が必要になります。

このタスクについて

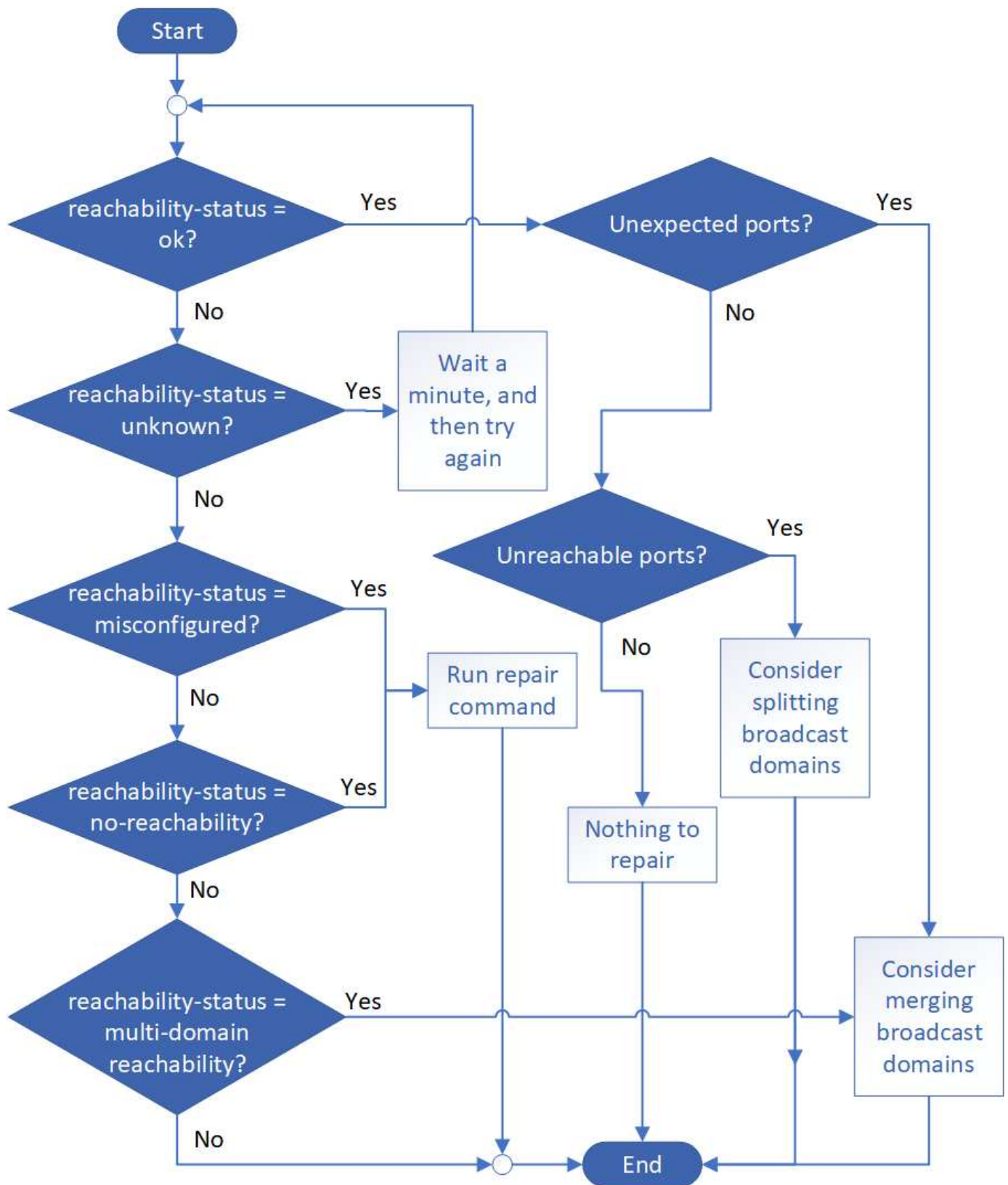
これらのコマンドを使用して、物理的なケーブル接続とネットワークスイッチの設定のどちらにも一致しない ONTAP 設定に起因するネットワークの設定ミスを検証、診断、および修復します。

ステップ

1. ポート到達可能性を表示します。

```
network port reachability show
```

2. 次のデシジョンツリーとテーブルを使用して、次のステップがあるかどうかを判断します。



プレゼンスステータス	説明
------------	----

わかりました	<p>ポートに割り当てられているブロードキャストドメインにレイヤ 2 の到達可能性があります。</p> <p>reachable-status が「OK」であるのに、「予想外のポート」がある場合は、1 つ以上のブロードキャストドメインをマージすることを検討してください。詳細については、次の <code>_unexpected ports_row</code> を参照してください。</p> <p>reachable-status が「OK」であるが、「到達不能ポート」がある場合は、1 つ以上のブロードキャストドメインをスプリットすることを検討してください。詳細については、次の <code>_Unreachable Ports_row</code> を参照してください。</p> <p>reachable-status が「OK」で、予期しないポートや到達不能なポートがない場合は、設定が正しいことを確認してください。</p>
予期しないポートです	<p>ポートには、割り当てられたブロードキャストドメインにレイヤ 2 に到達できることがあります。少なくとも 1 つの他のブロードキャストドメインにレイヤ 2 に到達できることもあります。</p> <p>物理的な接続とスイッチの設定を調べて、正しくないか、またはポートに割り当てられているブロードキャストドメインを 1 つ以上のブロードキャストドメインにマージする必要があるかどうかを確認します。</p> <p>詳細については、を参照してください <a href="#">"ブロードキャストドメインをマージします"</a>。</p>
到達不能ポート	<p>1 つのブロードキャストドメインが 2 つの異なる到達可能性セットにパーティショニングされている場合は、ブロードキャストドメインをスプリットして ONTAP 構成を物理ネットワークトポロジと同期できます。</p> <p>通常、到達不能ポートのリストでは、物理ポートとスイッチの設定が正確であることを確認したあとに別のブロードキャストドメインにスプリットする必要があるポートを定義します。</p> <p>詳細については、を参照してください <a href="#">"ブロードキャストドメインをスプリットします"</a>。</p>
誤設定 - 到達可能性	<p>ポートに割り当てられているブロードキャストドメインにレイヤ 2 に到達できるかどうかは関係ありませんが、ポートは別のブロードキャストドメインにレイヤ 2 に到達できるかどうかは関係ありません。</p> <p>ポートに到達できるかどうかを修復できます。次のコマンドを実行すると、ポートに到達できるブロードキャストドメインにポートが割り当てられます。</p> <pre>network port reachability repair -node -port</pre> <p>詳細については、を参照してください <a href="#">"ポートの到達可能性を修復します"</a>。</p>

到達不能	<p>既存のどのブロードキャストドメインにもレイヤ 2 で接続できません。</p> <p>ポートに到達できるかどうかを修復できます。次のコマンドを実行すると、自動的に作成されたデフォルトの IPspace 内の新しいブロードキャストドメインにポートが割り当てられます。</p> <pre>network port reachability repair -node -port</pre> <p>詳細については、を参照してください <a href="#">"ポートの到達可能性を修復します"</a>。</p>
multi-domain-reachable	<p>ポートには、割り当てられたブロードキャストドメインにレイヤ 2 に到達できることがあります、少なくとも 1 つの他のブロードキャストドメインにレイヤ 2 に到達できることもあります。</p> <p>物理的な接続とスイッチの設定を調べて、正しくないか、またはポートに割り当てられているブロードキャストドメインを 1 つ以上のブロードキャストドメインにマージする必要があるかどうかを確認します。</p> <p>詳細については、を参照してください <a href="#">"ブロードキャストドメインをマージします"</a> または <a href="#">"ポートの到達可能性を修復します"</a>。</p>
不明です	<p>reachable-status が「unknown」の場合は、数分待ってからもう一度コマンドを実行してください。</p>

ポートを修復したら、取り外された LIF や VLAN を確認して解決する必要があります。ポートがインターフェイスグループに属していた場合は、そのインターフェイスグループに何が起こったかを理解する必要もあります。詳細については、を参照してください ["ポートの到達可能性を修復します"](#)。

#### ONTAP ポートの概要

既知の多数のポートは、特定のサービスとの ONTAP 通信用に予約されています。ストレージネットワーク環境におけるポート値が ONTAP ポートの値と同じである場合は、ポートの競合が発生します。

次の表に、ONTAP で使用される TCP ポートと UDP ポートを示します。

サービス	ポート / プロトコル	説明
SSH	22 / TCP	Secure Shell ログイン
Telnet	23 / TCP	リモートログイン
DNS	53 / TCP	ロードバランシングされた DNS
HTTP	80 / TCP	Hyper Text Transfer Protocol の略
rpcbind	111/TCP	リモート手順コール
rpcbind	111/UDP	リモート手順コール
NTP	123 / UDP	Network Time Protocol の略
MSRPC	135 / UDP	MSRPC
NetBios - SSN	139 / TCP	NetBIOS サービスセッション

SNMP	161 / UDP	簡易ネットワーク管理プロトコル
HTTPS	443 tcp	HTTP over TLS
Microsoft - DS	445 / TCP	Microsoft - DS
マウント	635 / TCP	NFS マウント
マウント	635/UDP	NFS マウント
名前付き	953 / UDP	名前デーモン
NFS	2049 UDP	NFS サーバデーモン
NFS	2049 / TCP	NFS サーバデーモン
NRV	2050 / TCP	NetApp リモートボリュウムプロトコル
iSCSI	3260 / TCP	iSCSI ターゲットポート
ロック	4045 / TCP	NFS ロックデーモン
ロック	4045 / UDP	NFS ロックデーモン
nsm の場合	4046 / TCP	Network Status Monitor サービスの略
nsm の場合	4046 / UDP	Network Status Monitor サービスの略
rquotad	4049/UDP	NFS rquotad プロトコル
krb524	444/UDP	Kerberos 524
mDNS	533/UDP	マルチキャスト DNS
HTTPS	5986/UDP	HTTPS ポートリスンバイナリプロトコル
HTTPS	8443 / TCP	7MTT GUI ツールから https : //
NDMP	10000 / TCP	Network Data Management Protocol の略
クラスタピアリング	11104 / TCP	クラスタピアリング、双方向
クラスタピアリング、双方向	11105/TCP	クラスタピアリング
NDMP	18600-18699/TCP	NDMP
NDMP	30000 / TCP	セキュアソケットを介した制御接続の受け入れ
CIFS 監視ポート	40001/tcp のようになります	CIFS 監視ポート
TLS	50000 / TCP	トランスポートレイヤのセキュリティ
iSCSI	65200/TCP	iSCSIポート

#### ONTAP の内部ポート

次の表に、ONTAP によって内部的に使用される TCP ポートと UDP ポートを示します。これらのポートは、クラスタ内 LIF の通信を確立するために使用されます。

ポート / プロトコル	説明
514	syslog



900	ネットアップクラスタ RPC
902	ネットアップクラスタ RPC
904	ネットアップクラスタ RPC
905	ネットアップクラスタ RPC
910	ネットアップクラスタ RPC
911	ネットアップクラスタ RPC
913	ネットアップクラスタ RPC
914	ネットアップクラスタ RPC
915	ネットアップクラスタ RPC
918	ネットアップクラスタ RPC
920	ネットアップクラスタ RPC
921	ネットアップクラスタ RPC
924	ネットアップクラスタ RPC
925	ネットアップクラスタ RPC
927	ネットアップクラスタ RPC
928	ネットアップクラスタ RPC
929	ネットアップクラスタ RPC
931	ネットアップクラスタ RPC
932	ネットアップクラスタ RPC
933	ネットアップクラスタ RPC
934	ネットアップクラスタ RPC
935	ネットアップクラスタ RPC
936	ネットアップクラスタ RPC
937	ネットアップクラスタ RPC
939	ネットアップクラスタ RPC
940	ネットアップクラスタ RPC
951	ネットアップクラスタ RPC
954	ネットアップクラスタ RPC
九五五	ネットアップクラスタ RPC
956	ネットアップクラスタ RPC
958	ネットアップクラスタ RPC
961	ネットアップクラスタ RPC
九六三	ネットアップクラスタ RPC
九六四	ネットアップクラスタ RPC

九六六	ネットアップクラスタ RPC
967	ネットアップクラスタ RPC
982	ネットアップクラスタ RPC
983	ネットアップクラスタ RPC
五一五	ディスクの代替制御ポート
5133	ディスクの代替制御ポート
5144	ディスクの代替制御ポート
65502	ノードスコープ SSH
65503	LIF 共有
7810	ネットアップクラスタ RPC
7811	ネットアップクラスタ RPC
7812	ネットアップクラスタ RPC
7813	ネットアップクラスタ RPC
7814	ネットアップクラスタ RPC
7815	ネットアップクラスタ RPC
7816	ネットアップクラスタ RPC
7817	ネットアップクラスタ RPC
7818	ネットアップクラスタ RPC
7819	ネットアップクラスタ RPC
7820	ネットアップクラスタ RPC
7821	ネットアップクラスタ RPC
7822	ネットアップクラスタ RPC
7823	ネットアップクラスタ RPC
7824	ネットアップクラスタ RPC
8023	ノードスコープ Telnet
8514	ノードスコープ RSH
977	KMIP クライアントポート（内部ローカルホストのみ）

## IPspace

### IPspaceの設定の概要

IPspace を使用すると、単一の ONTAP クラスタを設定し、複数の管理上分離されたネットワークドメインのクライアントが、たとえ同じ IP アドレス範囲を使用している場合でもアクセスできるようにすることができます。これにより、クライアントトラフィックを分離してプライバシーとセキュリティを確保できます。

IPspace は、Storage Virtual Machine（SVM）が実装される、個別の IP アドレススペースを定義します。ある IPspace に対して定義されたポートと IP アドレスは、その IPspace 内でのみ適用されます。IPspace 内の SVM ごとに個別のルーティングテーブルが保持されるため、SVM や IPspace をまたがってトラフィックがルーティングされることはありません。



IPspace のルーティングドメインでは、IPv4 および IPv6 の両方のアドレスがサポートされます。

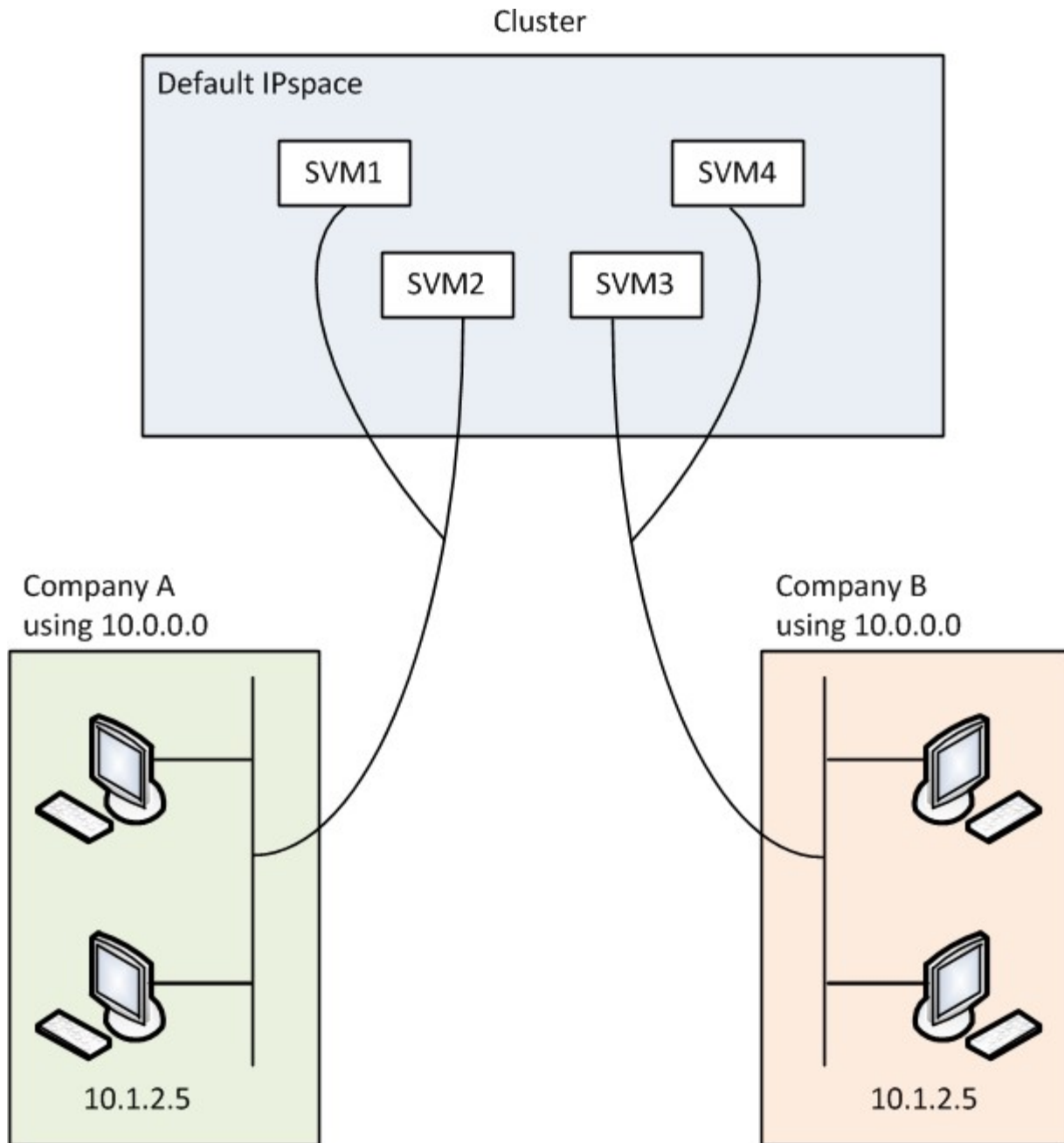
単一の組織のストレージを管理する場合は、IPspace を設定する必要はありません。単一の ONTAP クラスターで複数企業のストレージを管理していて、ユーザ間のネットワーク設定がないことが確実な場合も、IPspace を使用する必要はありません。多くの場合、Storage Virtual Machine（SVM）を専用の IP ルーティングテーブルと一緒に使用することで、IPspace を使用しなくても固有のネットワーク設定を分離できます。

### IPspace の使用例

ここでは、IPspace の一般的な用途として、ストレージサービスプロバイダ（SSP）が、その顧客の A 社と B 社を SSP の ONTAP クラスターに接続させる必要があり、両方の会社が同じプライベート IP アドレスの範囲を使用する場合を取り上げます。

SSP は、顧客ごとにクラスターに SVM を作成し、2 つの SVM から A 社のネットワークへの専用ネットワークパス、別の 2 つの SVM から B 社のネットワークへの専用ネットワークパスを提供します。

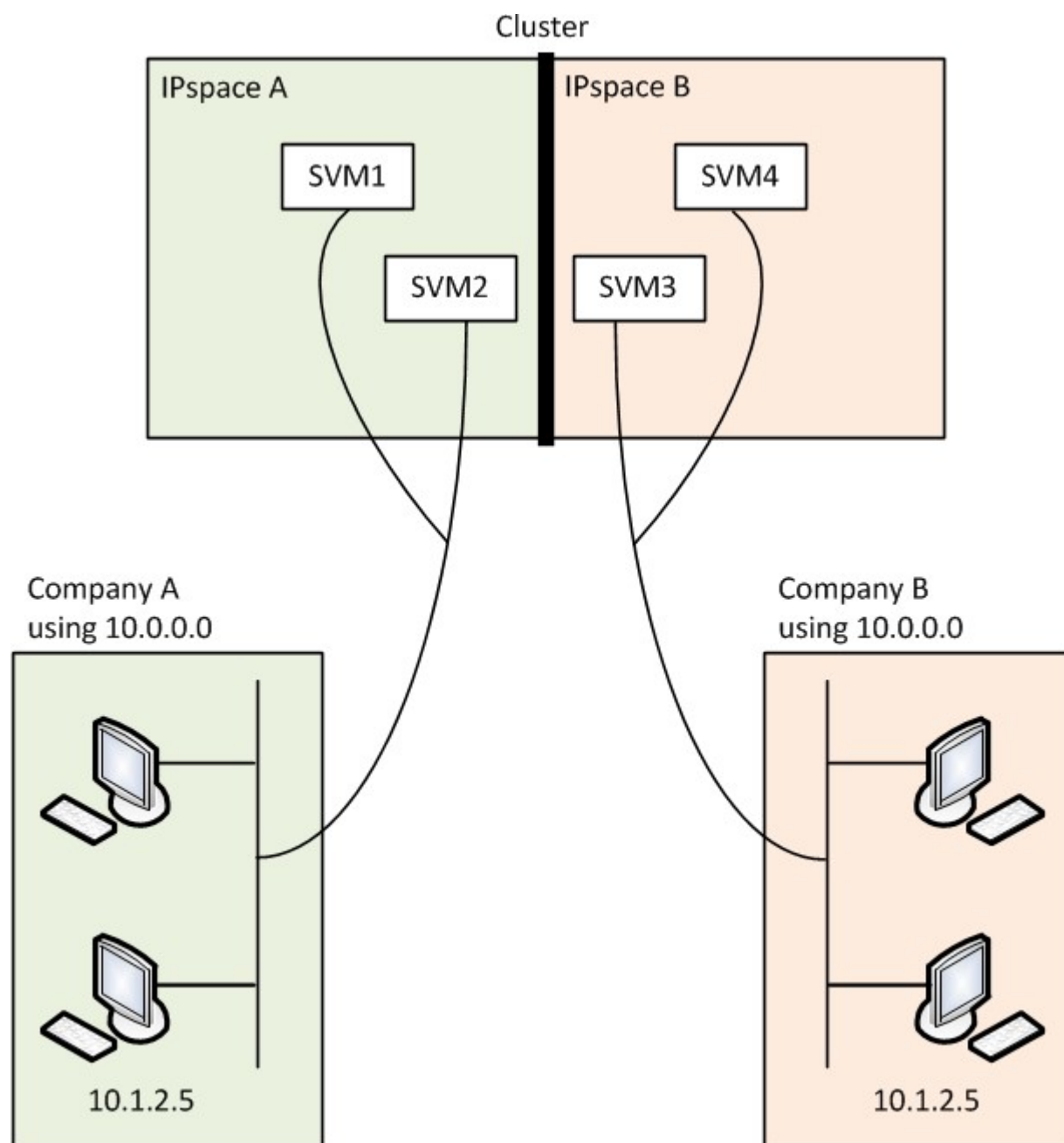
次の図に、このタイプの導入を示します。両社で非プライベート IP アドレスの範囲を使用する場合に機能します。ただし、図では、両方の企業が同じプライベート IP アドレス範囲を使用しているために問題が発生しています。



両社がプライベート IP アドレスのサブネット 10.0.0.0 を使用すると、次のような問題が起こります。

- 両社がそれぞれの SVM に同じ IP アドレスを使用した場合は、SSP にあるクラスタ内の SVM で IP アドレスの競合が発生します。
- 両社がそれぞれの SVM に別々の IP アドレスを使用することにした場合でも、まだ問題は残ります。
- たとえば、A のネットワーク内のクライアントの IP アドレスが B のネットワーク内のクライアントと同じ場合、A のアドレス空間内のクライアント宛てのパケットは B のアドレス空間内のクライアントにルーティングされ、その逆も同様です。
- 両社が相互に排他的なアドレススペースを使用する場合（たとえば、A がアドレス 10.0.0.0 とネットワークマスク 255.128.0.0 を、B がアドレス 10.128.0.0 とネットワークマスク 255.128.0.0 を使用する場合は、次のように入力します。SSP は、トラフィックを A および B のネットワークに適切にルーティングするように、クラスタ上のスタティックルートを設定する必要があります。
- この解決策は拡張性に優れておらず（静的ルートであるため）、セキュアではありません（ブロードキャ

ストトラフィックはクラスタのすべてのインターフェイスに送信されます)。この問題を解決するために、SSP はクラスタに 2 つの IPspace を定義します (会社ごとに 1 つ)。トラフィックが IPspace をまたがってルーティングされることはないので、すべての SVM が 10.0.0.0 というアドレススペースに設定されても、次の図に示すように、それぞれの会社のデータが該当するネットワークにセキュアにルーティングされます。



また、などの各種構成ファイルで参照されるIPアドレス `/etc/hosts` ファイル、`/etc/hosts.equiv` ファイル、および `/etc/rc` ファイルは、そのIPspaceを基準とした相対パスです。そのため、IPspace を正しく使用すれば、SSP が複数の SVM の設定と認証データに同じ IP アドレスを設定しても競合することはありません。

### IPspace の標準プロパティ

クラスタの初回作成時に、特別な IPspace がデフォルトで作成されます。さらに、IPspace ごとに特別な Storage Virtual Machine (SVM) が作成されます。

クラスタの初期化時に 2 つの IPspace が自動的に作成されます。

- 「Default」 IPspace

この IPspace は、ポート、サブネット、およびデータ提供元 SVM のコンテナです。クライアントごとに固有の IPspace を作成する必要がない設定であれば、すべての SVM をこの IPspace に作成できます。この IPspace には、クラスタ管理ポートとノード管理ポートも含まれます。

- 「Cluster」 IPspace に追加されました

この IPspace には、クラスタ内のすべてのノードのクラスタポートが含まれます。クラスタの作成時に自動的に作成されます。この IPspace は、内部のプライベートクラスタネットワークへの接続を提供します。ノードをクラスタに追加すると、追加したノードのクラスタポートが「Cluster」 IPspace に追加されます。

IPspace ごとに「システム」 SVM が 1 つ存在します。IPspace を作成すると、デフォルトのシステム SVM が IPspace と同じ名前で作成されます。

- 「Cluster」 IPspace のシステム SVM は、内部プライベートクラスタネットワークのノード間でクラスタトラフィックを伝送します。

この SVM の管理はクラスタ管理者が担当し、「Cluster」という名前が割り当てられます。

- 「default」 IPspace のシステム SVM は、クラスタ間トラフィックを含め、クラスタとノードの管理トラフィックをクラスタ間で伝送します。

この SVM の管理はクラスタ管理者が担当し、クラスタと同じ名前が使用されます。

- ユーザが作成するカスタム IPspace のシステム SVM は、この SVM の管理トラフィックを伝送します。

この SVM の管理はクラスタ管理者が担当し、IPspace と同じ名前が使用されます。

1 つの IPspace には、クライアントの SVM が 1 つ以上存在できます。各クライアント SVM は固有のデータボリュームと設定を持ち、他の SVM からは独立して管理されます。

## IPspaces を作成します

IPspace は、Storage Virtual Machine（SVM）が属する個別の IP アドレススペースです。SVM でセキュアなストレージ、管理、ルーティングを必要とする場合に、IPspace を作成します。IPspace を使用すると、クラスタ内の SVM ごとに個別の IP アドレススペースを作成できます。これにより、管理上分離されたネットワークメインのクライアントが、IP アドレスの同じサブネット範囲内の重複した IP アドレスを使用してクラスタのデータにアクセスできるようになります。

このタスクについて

IPspace の数はクラスタ全体で 512 個に制限されます。6GB の RAM を搭載したノードを含むクラスタの IPspace は、クラスタ全体で 256 個までに制限されます。お使いのプラットフォームに適用されるその他の制限を確認するには、Hardware Universe を参照してください。

["NetApp Hardware Universe の略"](#)



「all」はシステムに予約されている名前なので、IPspace 名を「all」にすることはできません。

作業を開始する前に

このタスクを実行するには、クラスタ管理者である必要があります。

#### ステップ

1. IPspace を作成します。

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

ipspace\_name は、作成するIPspaceの名前です。次のコマンドは、クラスタに ipspace1 という IPspace を作成します。

```
network ipspace create -ipspace ipspace1
```

2. IPspaceを表示します。

```
network ipspace show
```

IPspace	Vserver List	Broadcast Domains
Cluster	Cluster	Cluster
Default	Cluster1	Default
ipspace1	ipspace1	-

IPspace が、その IPspace のシステム SVM とともに作成されます。システム SVM は管理トラフィックを伝送します。

完了後

MetroCluster 設定を使用しているクラスタ内に IPspace を作成する場合は、IPspace オブジェクトをパートナークラスタに手動でレプリケートする必要があります。IPspace をレプリケートする前に作成されて IPspace に割り当てられた SVM は、パートナークラスタにレプリケートされません。

ブロードキャストドメインは「default」IPspace に自動的に作成され、次のコマンドを使用して IPspace 間で移動できます。

```
network port broadcast-domain move
```

たとえば、次のコマンドを使用して、ブロードキャストドメインを「default」から「ips1」に移動します。

```
network port broadcast-domain move -ipspace Default -broadcast-domain
Default -to-ipspace ips1
```

## IPspace を表示します

クラスタに存在する IPspace のリストを表示して、各 IPspace に割り当てられている Storage Virtual Machine (SVM)、ブロードキャストドメイン、およびポートを確認することができます。

### ステップ

クラスタ内の IPspace と SVM を表示します。

```
network ipspace show [-ipspace ipspace_name]
```

次のコマンドは、クラスタ内の IPspace、SVM、およびブロードキャストドメインをすべて表示します。

```
network ipspace show
IPspace          Vserver List          Broadcast Domains
-----
Cluster
Default          Cluster              Cluster
                  vs1, cluster-1        Default
ipspace1         vs3, vs4, ipspace1    bcast1
```

次のコマンドは、ipspace1 という IPspace に属するノードとポートを表示します。

```
network ipspace show -ipspace ipspace1
IPspace name: ipspace1
Ports: cluster-1-01:e0c, cluster-1-01:e0d, cluster-1-01:e0e, cluster-1-
02:e0c, cluster-1-02:e0d, cluster-1-02:e0e
Broadcast Domains: Default-1
Vservers: vs3, vs4, ipspace1
```

## IPspace を削除します

不要になった IPspace は削除できます。

作業を開始する前に

削除する IPspace に関連付けられているブロードキャストドメイン、ネットワークインターフェイス、または SVM がないようにします。



システムで定義された「default」IPspace と「Cluster」IPspace は削除できません。

ステップ

IPspace を削除：

```
network ipspace delete -ipspace ipspace_name
```

次のコマンドは、クラスタから ipspace1 という IPspace を削除します。

```
network ipspace delete -ipspace ipspace1
```

## ブロードキャストドメイン

### ブロードキャストドメイン（ONTAP 9.8以降）

ブロードキャストドメインの概要（ONTAP 9.8以降）

ブロードキャストドメインの目的は、同じレイヤ 2 ネットワークに属するネットワークポートをグループ化することです。グループ化したポートは、データまたは管理トラフィック用の Storage Virtual Machine（SVM）で使用できます。

ブロードキャストドメインは IPspace 内に配置されます。クラスタを初期化すると、デフォルトのブロードキャストドメインが 2 つ作成されます。

- 「デフォルト」のブロードキャストドメインには、「デフォルト」の IPspace 内にあるポートが含まれています。

これらのポートは、主にデータの提供に使用されます。クラスタ管理ポートとノード管理ポートも、このブロードキャストドメインに含まれています。

- 「クラスタ」のブロードキャストドメインには、「クラスタ」の IPspace 内にあるポートが含まれています。

これらのポートはクラスタ通信に使用され、クラスタ内のすべてのノードのすべてのクラスタポートが含まれます。

必要に応じて、追加のブロードキャストドメインがデフォルト IPspace に作成されます。「default」ブロードキャストドメインには、管理 LIF のホームポートに加え、そのポートにレイヤ 2 に到達できるその他のポートが含まれます。追加のブロードキャストドメインには、「default-1」、「default-2」などの名前が付けられます。

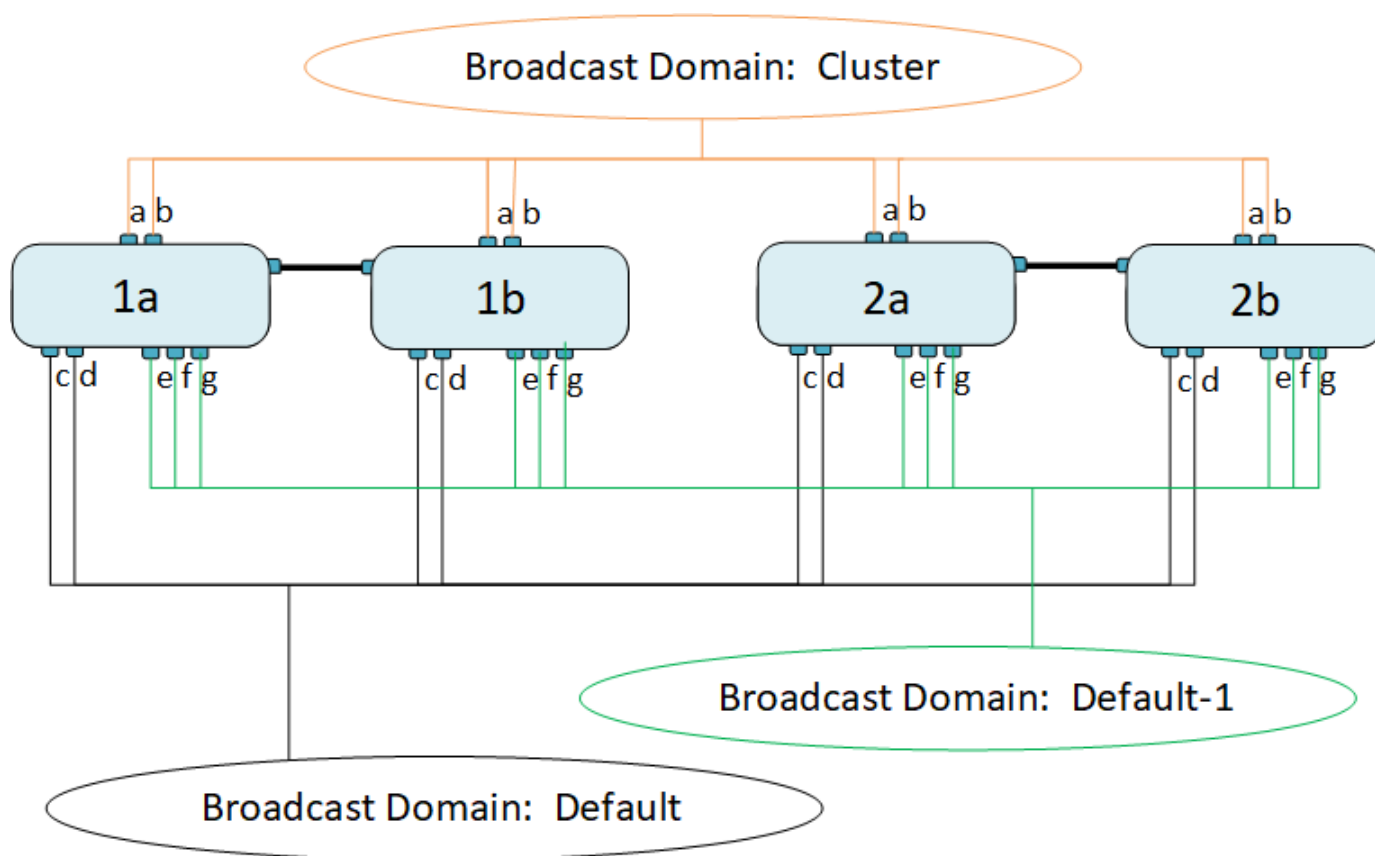
ブロードキャストドメインの使用例

ブロードキャストドメインは、同じ IPspace 内の一連のネットワークポートで、一般にクラスタ内の多数のノードのポートを含む、相互にレイヤ 2 に到達できるかどうかを示します。

次の図は、4 ノードクラスタの 3 つのブロードキャストドメインにポートを割り当てている例を示していま

す。

- 「Cluster」ブロードキャストドメインはクラスタの初期化中に自動的に作成され、クラスタ内の各ノードのポート a と b を含んでいます。
- 「default」ブロードキャストドメインもクラスタの初期化時に自動的に作成され、クラスタ内の各ノードのポート c と d を含んでいます。
- レイヤ 2 ネットワークの到達可能性に基づいて、クラスタの初期化時に追加のブロードキャストドメインが自動的に作成されます。追加されるブロードキャストドメインには、default-1、default-2 などの名前が付けられます。



各ブロードキャストドメインと同じ名前で、同じネットワークポートを持つフェイルオーバーグループが自動的に作成されます。このフェイルオーバーグループはシステムによって自動的に管理されます。つまり、ブロードキャストドメインのポートが追加または削除されると、フェイルオーバーグループのポートも自動的に追加または削除されます。

ブロードキャストドメインを追加します

ブロードキャストドメインは、同じレイヤ2ネットワークに属するクラスタ内のネットワークポートをグループ化したものです。これらのポートは、SVMで使用されます。

ONTAP 9.8 以降では、ブロードキャストドメインはクラスタの作成処理または参加処理中に自動的に作成されます。ONTAP 9.12.0以降では、自動的に作成されるブロードキャストドメインに加え、System Managerでブロードキャストドメインを手動で追加できます。

作業を開始する前に

ブロードキャストドメインに追加するポートは、他のブロードキャストドメインに属していないポートでなけ

ればなりません。使用するポートが別のブロードキャストドメインに属しているが、使用されていない場合は、元のブロードキャストドメインからそのポートを削除します。

このタスクについて

- すべてのブロードキャストドメイン名が IPspace 内で一意である必要があります。
- ブロードキャストドメインに追加できるポートは、物理ネットワークポート、VLAN、またはリンクアグリゲーショングループ/インターフェイスグループ（LAG / ifgrp）です。
- 使用するポートが別のブロードキャストドメインに属しているが、使用されていない場合は、新しいブロードキャストドメインに追加する前に既存のブロードキャストドメインから削除してください。
- ブロードキャストドメインに追加したポートの最大伝送ユニット（MTU）は、ブロードキャストドメインに設定されているMTU値に更新されます。
- 管理トラフィックを処理する e0M ポートを除く、レイヤ 2 ネットワークに接続されているすべてのデバイスの MTU 値が一致している必要があります。
- IPspace 名を指定しない場合、ブロードキャストドメインは「Default」IPspace に作成されます。

システムの設定を簡単にするために、同じポートを含む同じ名前のフェイルオーバーグループが自動的に作成されます。

## System Manager の略

### 手順

1. [ネットワーク]>[概要]>[ブロードキャストドメイン\*]を選択します。
2. をクリックします [+ Add](#)
3. ブロードキャストドメインの名前を指定します。
4. MTUを設定します。
5. IPspace を選択します。
6. ブロードキャストドメインを保存します。

ブロードキャストドメインは追加後に編集または削除できます。

### CLI の使用

ONTAP 9.7以前では、手動でブロードキャストドメインを作成できます。

ONTAP 9.8以降を使用している場合は、レイヤ2の到達可能性に基づいてブロードキャストドメインが自動的に作成されます。詳細については、[を参照してください "ポートの到達可能性を修復します"](#)。

### 手順

1. 現在ブロードキャストドメインに割り当てられていないポートを表示します。

```
network port show
```

ディスプレイが大きい場合は、`network port show -broadcast-domain` 未割り当てのポートのみを表示するコマンド。

2. ブロードキャストドメインを作成します。

```
network port broadcast-domain create -broadcast-domain  
broadcast_domain_name -mtu mtu_value [-ipspace ipspace_name] [-ports  
ports_list]
```

a. `broadcast_domain_name` は、作成するブロードキャストドメインの名前です。

b. `mtu_value` はIPパケットのMTUサイズです。通常は1500と9000です。

この値は、このブロードキャストドメインに追加するすべてのポートに適用されます。

c. `ipspace_name` は、このブロードキャストドメインを追加するIPspaceの名前です。

「default」 IPspace は、このパラメータの値を指定しないかぎり使用されます。

d. `ports_list` は、ブロードキャストドメインに追加するポートのリストです。

ポートはという形式で追加されます `node_name:port_number` `例えば、`node1:e0c。

3. 必要に応じて、ブロードキャストドメインが作成されたことを確認します。

```
network port show -instance -broadcast-domain new_domain
```

#### 例

次のコマンドは、Default IPspace にブロードキャストドメイン bcast1 を作成し、MTU を 1500 に設定してポートを 4 つ追加します。

```
network port broadcast-domain create -broadcast-domain bcast1 -mtu 1500 -ports  
cluster1-01:e0e,cluster1-01:e0f,cluster1-02:e0e,cluster1-02:e0f
```

#### 完了後

この時点で、サブネットを作成してブロードキャストドメインで使用可能になる IP アドレスのプールを定義するか、SVM とインターフェイスを IPspace に割り当てることができます。詳細については、を参照してください ["クラスタと SVM のピアリング"](#)。

既存のブロードキャストドメインの名前を変更する必要がある場合は、を使用します network port broadcast-domain rename コマンドを実行します

#### ブロードキャストドメインのポートの追加と削除（ONTAP 9.8以降）

ブロードキャストドメインは、クラスタの作成または追加の処理中に自動的に作成されます。ブロードキャストドメインからポートを手動で削除する必要はありません。

ネットワークポートの到達可能性が、物理ネットワーク接続またはスイッチの設定を通じて変更され、ネットワークポートが別のブロードキャストドメインに属している場合は、次のトピックを参照してください。


["ポートの到達可能性を修復します"](#)

### System Manager の略

ONTAP 9.14.1以降では、System Managerを使用してブロードキャストドメイン間でイーサネットポートを再割り当てできます。すべてのイーサネットポートをブロードキャストドメインに割り当てることを推奨します。そのため、ブロードキャストドメインからイーサネットポートの割り当てを解除した場合は、別のブロードキャストドメインに再割り当てする必要があります。

#### 手順

イーサネットポートを再割り当てするには、次の手順を実行します。

1. [ネットワーク]>[概要]\*を選択します。
2. [ブロードキャストドメイン]セクションで、 をクリックします。
3. ドロップダウンメニューで、 \* Edit \* を選択します。
4. [ブロードキャストドメインの編集]\*ページで、別のドメインに再割り当てするイーサネットポートの選択を解除します。
5. 選択解除された各ポートについて、\* Reassign Ethernet Port ウィンドウが表示されます。ポートを再割り当てするブロードキャストドメインを選択し、[再割り当て]\*を選択します。
6. 現在のブロードキャストドメインに割り当てするすべてのポートを選択し、変更を保存します。

#### CLI の使用

ネットワークポートの到達可能性が、物理ネットワーク接続またはスイッチの設定を通じて変更され、ネットワークポートが別のブロードキャストドメインに属している場合は、次のトピックを参照してください。

#### "ポートの到達可能性を修復します"

または、ブロードキャストドメインに対してポートを手動で追加または削除することもできます。  
`network port broadcast-domain add-ports` または `network port broadcast-domain remove-ports` コマンドを実行します

#### 作業を開始する前に

- このタスクを実行するには、クラスタ管理者である必要があります。
- ブロードキャストドメインに追加するポートは、他のブロードキャストドメインに属していないポートでなければなりません。
- すでにインターフェイスグループに属しているポートを個別にブロードキャストドメインに追加することはできません。

#### このタスクについて

ネットワークポートの追加と削除には、次のルールが適用されます。

ポートの追加	ポートの削除
追加できるポートは、ネットワークポート、VLAN、インターフェイスグループ（ifgrp）です。	N/A
ポートは、ブロードキャストドメインのシステム定義のフェイルオーバーグループに追加されます。	ポートは、ブロードキャストドメインのすべてのフェイルオーバーグループから削除されます。

ポートの MTU は、ブロードキャストドメインに設定されている MTU 値に更新されます。	ポートの MTU は変更されません。
ポートの IPspace は、ブロードキャストドメインの IPspace 値に更新されます。	ポートは「Default」IPspace に移動し、ブロードキャストドメイン属性はない。



を使用してインターフェイスグループの最後のメンバーポートを削除した場合 `network port ifgrp remove-port` このコマンドを実行すると、ブロードキャストドメインからインターフェイスグループポートが削除されます。これは、ブロードキャストドメインに空のインターフェイスグループポートが許可されていないためです。

#### 手順

1. を使用して、ブロードキャストドメインに現在割り当てられているポートまたは割り当てられていないポートを表示します `network port show` コマンドを実行します
2. ブロードキャストドメインにポートを追加するか、ブロードキャストドメインからポートを削除します。

状況	使用
ブロードキャストドメインにポートを追加します	<code>network port broadcast-domain add-ports</code>
ブロードキャストドメインからポートを削除します	<code>network port broadcast-domain remove-ports</code>

3. ポートがブロードキャストドメインに対して追加または削除されたことを確認します。

```
network port show
```

これらのコマンドの詳細については、を参照してください ["ONTAP 9 のコマンド"](#)。

#### ポートの追加と削除の例

次のコマンドは、Default IPspace のブロードキャストドメイン `bcast1` に、ノード `cluster-1-01` のポート `e0g` と、ノード `cluster-1-02` の `e0g` を追加します。

```
cluster-1::> network port broadcast-domain add-ports -broadcast-domain bcast1
-ports cluster-1-01:e0g,cluster1-02:e0g
```

次のコマンドは、Cluster IPspace のブロードキャストドメイン `Cluster` にクラスタポートを 2 つ追加します。

```
cluster-1::> network port broadcast-domain add-ports -broadcast-domain Cluster
-ports cluster-2-03:e0f,cluster2-04:e0f -ipspace Cluster
```

次のコマンドは、Default IPspace のブロードキャストドメイン `bcast1` から、ノード `cluster1-01` のポート `e0e` を削除します。

```
cluster-1::> network port broadcast-domain remove-ports -broadcast-domain
bcast1 -ports cluster-1-01:e0e
```

ブロードキャストドメインを**IPspace**に移動（ONTAP 9.8以降）

レイヤ 2 の到達可能性に基づいて作成したブロードキャストドメインを、作成した IPspace に移動します。

ブロードキャストドメインを移動する前に、ブロードキャストドメインのポートに到達できるかどうかを確認する必要があります。

ポートの自動スキャンでは、到達可能なポートを特定して同じブロードキャストドメインに配置できますが、このスキャンでは適切な IPspace を特定できません。ブロードキャストドメインがデフォルト以外の IPspace に属している場合は、このセクションの手順に従って手動で移動する必要があります。

作業を開始する前に

ブロードキャストドメインは、クラスタの作成処理および追加処理の一環として自動的に設定されます。ONTAP では、「Default」ブロードキャストドメインを定義します。このドメインは、クラスタに最初に作成したノードの管理インターフェイスのホームポートにレイヤ 2 で接続されるポートのセットです。他のブロードキャストドメインも必要に応じて作成され、「\* default-1 \*」、「\* default-2 \*」などの名前が付けられます。

ノードが既存のクラスタに参加すると、そのノードのネットワークポートは、レイヤ 2 の到達可能性に基づいて自動的に既存のブロードキャストドメインに追加されます。既存のブロードキャストドメインに到達できない場合、ポートは 1 つ以上の新しいブロードキャストドメインに配置されます。

このタスクについて

- ・クラスタ LIF が設定されたポートは、自動的に「Cluster」IPspace に配置されます。
- ・ノード管理 LIF のホームポートに到達できるポートは、「default」ブロードキャストドメインに配置されます。
- ・その他のブロードキャストドメインは、クラスタの作成または追加処理の一環として、ONTAP によって自動的に作成されます。
- ・VLAN やインターフェイスグループを追加すると、作成後約 1 分後に適切なブロードキャストドメインに自動的に配置されます。

手順

1. ブロードキャストドメイン内のポートに到達できるかどうかを確認します。ONTAP はレイヤ 2 の到達可能性を自動的に監視します。次のコマンドを使用して、各ポートがブロードキャストドメインに追加され、「OK」の到達可能性があることを確認します。

```
network port reachability show -detail
```

2. 必要に応じて、ブロードキャストドメインを他の IPspace に移動します。

```
network port broadcast-domain move
```

たとえば、ブロードキャストドメインを「default」から「ips1」に移動する場合、次のようになります。

```
network port broadcast-domain move -ip-space Default -broadcast-domain Default  
-to-ip-space ips1
```



ブロードキャストドメインをIPspaceに移動 (ONTAP 9.8以降)

レイヤ 2 の到達可能性に基づいて作成したブロードキャストドメインを、作成した IPspace に移動します。

ブロードキャストドメインを移動する前に、ブロードキャストドメインのポートに到達できるかどうかを確認する必要があります。

ポートの自動スキャンでは、到達可能なポートを特定して同じブロードキャストドメインに配置できますが、このスキャンでは適切な IPspace を特定できません。ブロードキャストドメインがデフォルト以外の IPspace に属している場合は、このセクションの手順に従って手動で移動する必要があります。

作業を開始する前に

ブロードキャストドメインは、クラスタの作成処理および追加処理の一環として自動的に設定されます。ONTAP では、「Default」ブロードキャストドメインを定義します。このドメインは、クラスタに最初に作成したノードの管理インターフェイスのホームポートにレイヤ 2 で接続されるポートのセットです。他のブロードキャストドメインも必要に応じて作成され、「\* default-1 \*」、「\* default-2 \*」などの名前が付けられます。

ノードが既存のクラスタに参加すると、そのノードのネットワークポートは、レイヤ 2 の到達可能性に基づいて自動的に既存のブロードキャストドメインに追加されます。既存のブロードキャストドメインに到達できない場合、ポートは 1 つ以上の新しいブロードキャストドメインに配置されます。

このタスクについて

- ・クラスタ LIF が設定されたポートは、自動的に「Cluster」IPspace に配置されます。
- ・ノード管理 LIF のホームポートに到達できるポートは、「default」ブロードキャストドメインに配置されます。
- ・その他のブロードキャストドメインは、クラスタの作成または追加処理の一環として、ONTAP によって自動的に作成されます。
- ・VLAN やインターフェイスグループを追加すると、作成後約 1 分後に適切なブロードキャストドメインに自動的に配置されます。

手順

1. ブロードキャストドメイン内のポートに到達できるかどうかを確認します。ONTAP はレイヤ 2 の到達可能性を自動的に監視します。次のコマンドを使用して、各ポートがブロードキャストドメインに追加され、「OK」の到達可能性があることを確認します。

```
network port reachability show -detail
```

2. 必要に応じて、ブロードキャストドメインを他の IPspace に移動します。

```
network port broadcast-domain move
```

たとえば、ブロードキャストドメインを「default」から「ips1」に移動する場合、次のようになります。

```
network port broadcast-domain move -ip-space Default -broadcast-domain Default  
-to-ip-space ips1
```

## ブロードキャストドメインのスプリット (ONTAP 9.8以降)

ネットワークポートの到達可能性が、物理ネットワーク接続またはスイッチの設定によって変更された場合は、次の手順を実行します。また、単一のブロードキャストドメインに設定していたネットワークポートのグループが、2つの到達可能性セットにパーティショニングされます。ブロードキャストドメインをスプリットして、ONTAP 設定を物理ネットワークトポロジと同期できます。

ネットワークポートのブロードキャストドメインが複数の到達可能性セットに分割されているかどうかを確認するには、を使用します `network port reachability show -details` コマンドを実行し、どのポートが相互に接続されていないかに注意してください (「Unreachable ports」)。通常、到達不能なポートのリストには、物理的な設定とスイッチの設定に間違いがないことを確認したうえで、別のブロードキャストドメインに分割する必要があります。

### ステップ

ブロードキャストドメインを2つのブロードキャストドメインにスプリットします。

```
network port broadcast-domain split -ipspace <ipspace_name> -broadcast  
-domain <broadcast_domain_name> -new-broadcast-domain  
<broadcast_domain_name> -ports <node:port,node:port>
```

- `ipspace_name` は、ブロードキャストドメインが配置されているIPspaceの名前です。
- `-broadcast-domain` は、スプリットするブロードキャストドメインの名前です。
- `-new-broadcast-domain` は、作成する新しいブロードキャストドメインの名前です。
- `-ports` は、新しいブロードキャストドメインに追加するノードの名前とポートです。

## ブロードキャストドメインのマージ (ONTAP 9.8以降)

物理ネットワーク接続またはスイッチ設定によってネットワークポートの到達可能性が変更され、複数のブロードキャストドメインで設定されていた2つのネットワークポートグループがすべて到達可能性を共有するようになった場合、2つのブロードキャストドメインをマージすることで、ONTAP 設定と物理ネットワークトポロジを同期できます。

複数のブロードキャストドメインが1つの到達可能性セットに属しているかどうかを確認するには、「`network port reachability show-details`」コマンドを使用して、別のブロードキャストドメインに設定されているポート (「想定外のポート」) を調べます。通常、一連の予期しないポートのリストでは、物理ポートとスイッチの設定が正確であることを確認したあとに、ブロードキャストドメインにマージする必要がある一連のポートが定義されています。

### ステップ

1つのブロードキャストドメインのポートを既存のブロードキャストドメインにマージします。

```
network port broadcast-domain merge -ipspace <ipspace_name> -broadcast
-domain <broadcast_domain_name> -into-broadcast-domain
<broadcast_domain_name>
```

- `ipspace_name` は、ブロードキャストドメインのあるIPspaceの名前です。
- `-broadcast-domain` は、マージするブロードキャストドメインの名前です。
- `-into-broadcast-domain` は、追加のポートを受け取るブロードキャストドメインの名前です。

#### ブロードキャストドメインのポートのMTU値の変更（ONTAP 9.8以降）

あるブロードキャストドメインの MTU 値を変更することにより、そのブロードキャストドメインのすべてのポートの MTU 値を変更できます。これは、ネットワークで行われたトポロジの変更をサポートするために実行できます。

#### 作業を開始する前に

管理トラフィックを処理する e0M ポートを除く、レイヤ 2 ネットワークに接続されているすべてのデバイスの MTU 値が一致している必要があります。

#### このタスクについて

MTU 値を変更すると、影響を受けるポートを経由するトラフィックが一時的に中断されます。プロンプトが表示され、回答の MTU 値を変更するために「y」と入力する必要があります。

#### ステップ

ブロードキャストドメインのすべてのポートの MTU 値を変更します。

```
network port broadcast-domain modify -broadcast-domain
<broadcast_domain_name> -mtu <mtu_value> [-ipspace <ipspace_name>]
```

- `broadcast_domain` は、ブロードキャストドメインの名前です。
- `mtu` はIPパケットのMTUサイズです。通常は1500と9000です。
- `ipspace` は、このブロードキャストドメインが配置されているIPspaceの名前です。「default」IPspace は、このオプションの値を指定しないかぎり使用されます。次のコマンドは、ブロードキャストドメイン「bcast1」のすべてのポートの MTU を 9000 に変更します。

```
network port broadcast-domain modify -broadcast-domain <Default-1> -mtu <
9000 >
Warning: Changing broadcast domain settings will cause a momentary data-
serving interruption.
Do you want to continue? {y|n}: <y>
```

ブロードキャストドメインを表示する (ONTAP 9.8以降)

クラスタの各 IPspace 内にあるブロードキャストドメインのリストを表示できます。この出力には、各ブロードキャストドメインのポートと MTU 値のリストも含まれます。

#### ステップ

クラスタのブロードキャストドメイン、および関連付けられているポートを表示します。

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

次のコマンドは、クラスタのすべてのブロードキャストドメイン、および関連付けられているポートを表示します。

```
network port broadcast-domain show
IPspace Broadcast
Name      Domain Name  MTU   Port List
-----
Cluster Cluster      9000
          cluster-1-01:e0a    complete
          cluster-1-01:e0b    complete
          cluster-1-02:e0a    complete
          cluster-1-02:e0b    complete
Default Default      1500
          cluster-1-01:e0c    complete
          cluster-1-01:e0d    complete
          cluster-1-02:e0c    complete
          cluster-1-02:e0d    complete
          Default-1      1500
          cluster-1-01:e0e    complete
          cluster-1-01:e0f    complete
          cluster-1-01:e0g    complete
          cluster-1-02:e0e    complete
          cluster-1-02:e0f    complete
          cluster-1-02:e0g    complete
```

次のコマンドは、default-1 ブロードキャストドメイン内のポートの更新ステータスがエラーであることを示し、ポートを正しく更新できなかったことを示しています。

```
network port broadcast-domain show -broadcast-domain Default-1 -port  
-update-status error
```

IPspace	Broadcast				Update
Name	Domain Name	MTU	Port List		Status Details
-----	-----	-----	-----	-----	-----
Default	Default-1	1500	cluster-1-02:e0g		error

詳細については、を参照してください ["ONTAP 9 のコマンド"](#)。

ブロードキャストドメインを削除する

不要になったブロードキャストドメインは削除できます。削除することで、そのブロードキャストドメインに関連付けられていたポートは「Default」IPspace に移動します。

作業を開始する前に

削除するブロードキャストドメインに、関連付けられているサブネット、ネットワークインターフェイス、SVM がないようにします。

このタスクについて

- システムで作成された「Cluster」ブロードキャストドメインを削除することはできません。
- ブロードキャストドメインを削除すると、そのドメインに関連するフェイルオーバーグループもすべて削除されます。


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

## System Manager の略

- ONTAP 9.12.0以降では、System Managerを使用してブロードキャストドメイン\*を削除できます

ブロードキャストドメインにポートが含まれている場合やサブネットに関連付けられている場合は、削除オプションは表示されません。

### 手順

1. [ネットワーク]>[概要]>[ブロードキャストドメイン\*]を選択します。
2. 選択するオプション  削除するブロードキャストドメインの横にある削除\*をクリックします。

### CLI の使用

\*ブロードキャストドメイン\*を削除するには、CLIを使用してください

### ステップ

ブロードキャストドメインを削除します。

```
network port broadcast-domain delete -broadcast-domain broadcast_domain_name  
[-ipspace ipspace_name]
```

次のコマンドは、ipspace1 という IPspace のブロードキャストドメイン default-1 を削除します。

```
network port broadcast-domain delete -broadcast-domain Default-1 -ipspace  
ipspace1
```

## ブロードキャストドメイン（ONTAP 9.7以前）

### ブロードキャストドメインの概要（ONTAP 9.7以前）

ブロードキャストドメインの目的は、同じレイヤ 2 ネットワークに属するネットワークポートをグループ化することです。グループ化したポートは、データまたは管理トラフィック用の Storage Virtual Machine（SVM）で使用できます。

ブロードキャストドメインは IPspace 内に配置されます。クラスタを初期化すると、デフォルトのブロードキャストドメインが 2 つ作成されます。

- デフォルトのブロードキャストドメインには、デフォルトの IPspace 内にあるポートが含まれています。これらのポートは、主にデータの提供に使用されます。クラスタ管理ポートとノード管理ポートも、このブロードキャストドメインに含まれています。
- クラスタのブロードキャストドメインには、クラスタの IPspace 内にあるポートが含まれています。これらのポートはクラスタ通信に使用され、クラスタ内のすべてのノードのすべてのクラスタポートが含まれます。

クライアントトラフィックを分離するために独自の IPspace を作成した場合は、作成する個々の IPspace 内にブロードキャストドメインを作成する必要があります。



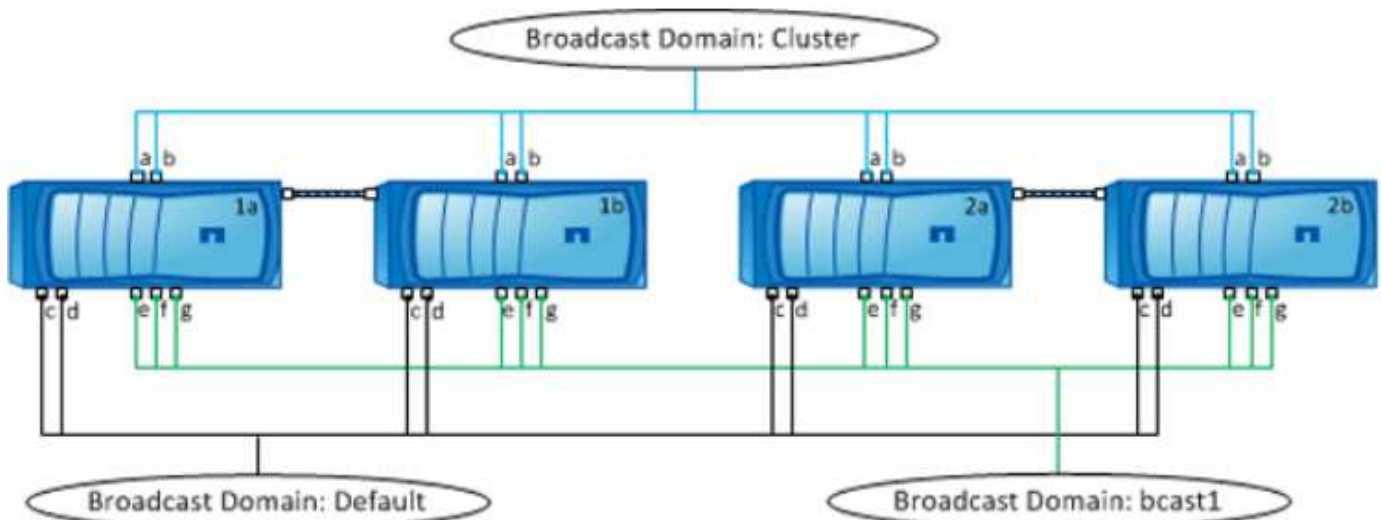
ブロードキャストドメインを作成して、同じレイヤ 2 ネットワークに属するクラスタのネットワークポートをグループ化します。これらのポートは、SVM で使用されます。

## ブロードキャストドメインの使用例

ブロードキャストドメインは、同じ IPspace 内の一連のネットワークポートで、一般にクラスタ内の多数のノードのポートを含む、相互にレイヤ 2 に到達できるかどうかを示します。

次の図は、4 ノードクラスタの 3 つのブロードキャストドメインにポートを割り当てている例を示しています。

- Cluster ブロードキャストドメインはクラスタの初期化中に自動的に作成され、クラスタ内の各ノードのポート a と b を含んでいます。
- Default ブロードキャストドメインもクラスタの初期化中に自動的に作成され、クラスタ内の各ノードのポート c と d を含んでいます。
- bcast1 というブロードキャストドメインは手動で作成されたドメインです。クラスタ内の各ノードのポート e、f、g を含んでいます。  
このブロードキャストドメインは、新しい SVM を介してデータにアクセスする新しいクライアント専用  
に、システム管理者が作成したものです。



各ブロードキャストドメインと同じ名前で、同じネットワークポートを持つフェイルオーバーグループが自動的に作成されます。このフェイルオーバーグループはシステムによって自動的に管理されます。つまり、ブロードキャストドメインのポートが追加または削除されると、フェイルオーバーグループのポートも自動的に追加または削除されます。

## ブロードキャストドメインに使用できるポートの確認 (ONTAP 9.7以前)

新しい IPspace に追加するブロードキャストドメインを設定する前に、ブロードキャストドメインに使用できるポートを確認する必要があります。



このタスクは、ONTAP 9.8 ではなく、ONTAP 9.1-9.7 に関連しています。

作業を開始する前に

このタスクを実行するには、クラスタ管理者である必要があります。

このタスクについて

- 使用できるポートは、物理ポート、VLAN、インターフェイスグループ (ifgroup) です。

- 新しいブロードキャストドメインに追加するポートを既存のブロードキャストドメインに割り当ててすることはできません。
- ブロードキャストドメインに追加するポートがすでに別のブロードキャストドメイン（たとえば、デフォルト IPspace 内のデフォルトブロードキャストドメイン）に割り当てられている場合は、そのブロードキャストドメインからポートを削除してから新しいブロードキャストドメインに割り当てする必要があります。
- LIF が割り当てられているポートをブロードキャストドメインから削除することはできません。
- クラスタ管理 LIF とノード管理 LIF はデフォルト IPspace 内のデフォルトブロードキャストドメインに割り当てられるため、これらの LIF に割り当てられているポートはデフォルトブロードキャストドメインから削除できません。

## 手順

1. 現在のポートの割り当てを確認します。

```
network port show
```

Node	Port	IPspace	Broadcast Domain	Link	MTU	Admin/Oper
-----						
node1						
	e0a	Cluster	Cluster	up	9000	auto/1000
	e0b	Cluster	Cluster	up	9000	auto/1000
	e0c	Default	Default	up	1500	auto/1000
	e0d	Default	Default	up	1500	auto/1000
	e0e	Default	Default	up	1500	auto/1000
	e0f	Default	Default	up	1500	auto/1000
	e0g	Default	Default	up	1500	auto/1000
node2						
	e0a	Cluster	Cluster	up	9000	auto/1000
	e0b	Cluster	Cluster	up	9000	auto/1000
	e0c	Default	Default	up	1500	auto/1000
	e0d	Default	Default	up	1500	auto/1000
	e0e	Default	Default	up	1500	auto/1000
	e0f	Default	Default	up	1500	auto/1000
	e0g	Default	Default	up	1500	auto/1000

この例では、コマンドの出力から次の情報が得られます。

- ポート e0c、e0d、e0e、e0f および e0g 各ノードにはデフォルトのブロードキャストドメインが割り当てられています。
  - これらのポートは、作成する IPspace のブロードキャストドメインで使用できる可能性があります。
2. デフォルトブロードキャストドメイン内の、LIF インターフェイスに割り当てられている、したがって新しいブロードキャストドメインに移動できないポートを確認します。

```
network interface show
```



Vserver	Logical Interface	Status Admin/Oper	Network Address/Mask	Current Node	Current Port	Is Home
Cluster						
	node1_clus1	up/up	10.0.2.40/24	node1	e0a	true
	node1_clus2	up/up	10.0.2.41/24	node1	e0b	true
	node2_clus1	up/up	10.0.2.42/24	node2	e0a	true
	node2_clus2	up/up	10.0.2.43/24	node2	e0b	true
cluster1						
	cluster_mgmt	up/up	10.0.1.41/24	node1	e0c	true
	node1_mgmt	up/up	10.0.1.42/24	node1	e0c	true
	node2_mgmt	up/up	10.0.1.43/24	node2	e0c	true

次の例では、コマンドの出力から次の情報が得られます。

- ノードポートがポートに割り当てられます e0c 各ノードで、クラスタ管理LIFのホームノードがオンになっている e0c オン node1。
- ポート e0d、e0e、e0f および e0g 各ノードがLIFをホストしていないため、デフォルトのブロードキャストドメインから削除して、新しいIPspaceの新しいブロードキャストドメインに追加できます。

#### ブロードキャストドメインの作成 (ONTAP 9.7以前)

ONTAP 9.7 以前では、同じレイヤ 2 ネットワークに属するクラスタのネットワークポートをグループ化するブロードキャストドメインを作成します。これらのポートは、SVMで使用されます。カスタム IPspace のブロードキャストドメインを作成する必要があります。IPspace に作成した SVM では、ブロードキャストドメイン内のポートを使用します。



このタスクは、ONTAP 9.8 ではなく、ONTAP 9.1-9.7 に関連しています。

作業を開始する前に

このタスクを実行するには、クラスタ管理者である必要があります。

ONTAP 9.8 以降では、ブロードキャストドメインはクラスタの作成処理または参加処理中に自動的に作成されます。ONTAP 9.8 以降を実行している場合は、これらの手順は必要ありません。

ONTAP 9.7 以前では、ブロードキャストドメインに追加するポートが別のブロードキャストドメインに属していない必要がありました。

このタスクについて

LIF のフェイルオーバー先のポートは、LIF のフェイルオーバーグループのメンバーである必要があります。ブロードキャストドメインを作成すると、ONTAP によって同じ名前のフェイルオーバーグループが自動的に作成されます。フェイルオーバーグループには、ブロードキャストドメインに割り当てられたすべてのポートが含まれます。

- すべてのブロードキャストドメイン名が IPspace 内で一意である必要があります。
- ブロードキャストドメインに追加できるポートは、物理ネットワークポート、VLAN、インターフェイスグループ（ifgrp）です。
- 使用するポートが別のブロードキャストドメインに属しているが、使用されていない場合は、を使用します `network port broadcast-domain remove-ports` 既存のブロードキャストドメインからポートを削除するコマンド。
- ブロードキャストドメインに追加したポートの MTU は、ブロードキャストドメインに設定されている MTU 値に更新されます。
- 管理トラフィックを処理する e0M ポートを除く、レイヤ 2 ネットワークに接続されているすべてのデバイスの MTU 値が一致している必要があります。
- IPspace 名を指定しない場合、ブロードキャストドメインは「Default」IPspace に作成されます。

システムの設定を簡単にするために、同じポートを含む同じ名前のフェイルオーバーグループが自動的に作成されます。

#### 手順

1. 現在ブロードキャストドメインに割り当てられていないポートを表示します。

```
network port show
```

ディスプレイが大きい場合は、を使用します `network port show -broadcast-domain` 未割り当てのポートのみを表示するコマンド。

2. ブロードキャストドメインを作成します。

```
network port broadcast-domain create -broadcast-domain broadcast_domain_name
-mtu mtu_value [-ipspace ipspace_name] [-ports ports_list]
```

◦ *broadcast\_domain\_name* は、作成するブロードキャストドメインの名前です。

◦ *mtu\_value* はIPパケットのMTUサイズです。通常は1500と9000です。

この値は、このブロードキャストドメインに追加するすべてのポートに適用されます。

◦ *ipspace\_name* は、このブロードキャストドメインを追加するIPspaceの名前です。

「default」IPspace は、このパラメータの値を指定しないかぎり使用されます。

◦ *ports\_list* は、ブロードキャストドメインに追加するポートのリストです。

ポートはという形式で追加されます *node\_name:port\_number* 例えば、`node1:e0c0`。

3. 必要に応じて、ブロードキャストドメインが作成されたことを確認します。

```
network port show -instance -broadcast-domain new_domain
```

#### 例

次のコマンドは、Default IPspace にブロードキャストドメイン bcast1 を作成し、MTU を 1500 に設定してポートを 4 つ追加します。

```
network port broadcast-domain create -broadcast-domain bcast1 -mtu 1500 -ports
```

cluster1-01:e0e,cluster1-01:e0f,cluster1-02:e0e,cluster1-02:e0f

完了後

この時点で、サブネットを作成してブロードキャストドメインで使用可能になる IP アドレスのプールを定義するか、SVM とインターフェイスを IPspace に割り当てることができます。詳細については、[を参照してください](#) "クラスタと SVM のピアリング"。

既存のブロードキャストドメインの名前を変更する必要がある場合は、を使用します network port broadcast-domain rename コマンドを実行します

ブロードキャストドメインのポートを追加または削除する（ONTAP 9.7以前）

ブロードキャストドメインの最初の作成時にネットワークポートを追加したり、既存のブロードキャストドメインに対してポートを追加または削除したりできます。これにより、クラスタ内のすべてのポートを効率的に使用できます。

新しいブロードキャストドメインに追加するポートがすでに別のブロードキャストドメインにある場合は、そのブロードキャストドメインからポートを削除してから新しいブロードキャストドメインに割り当てる必要があります。



このタスクは、ONTAP 9.8 ではなく、ONTAP 9.1-9.7 に関連しています。

作業を開始する前に

- このタスクを実行するには、クラスタ管理者である必要があります。
- ブロードキャストドメインに追加するポートは、他のブロードキャストドメインに属していないポートでなければなりません。
- すでにインターフェイスグループに属しているポートを個別にブロードキャストドメインに追加することはできません。

このタスクについて

ネットワークポートの追加と削除には、次のルールが適用されます。

ポートの追加	ポートの削除
追加できるポートは、ネットワークポート、VLAN、インターフェイスグループ（ifgrp）です。	N/A
ポートは、ブロードキャストドメインのシステム定義のフェイルオーバーグループに追加されます。	ポートは、ブロードキャストドメインのすべてのフェイルオーバーグループから削除されます。
ポートの MTU は、ブロードキャストドメインに設定されている MTU 値に更新されます。	ポートの MTU は変更されません。
ポートの IPspace は、ブロードキャストドメインの IPspace 値に更新されます。	ポートは「Default」IPspace に移動し、ブロードキャストドメイン属性はない。



を使用してインターフェイスグループの最後のメンバーポートを削除した場合 network port ifgrp remove-port このコマンドを実行すると、ブロードキャストドメインからインターフェイスグループポートが削除されます。これは、ブロードキャストドメインに空のインターフェイスグループポートが許可されていないためです。

手順

1. を使用して、ブロードキャストドメインに現在割り当てられているポートまたは割り当てられていないポートを表示します `network port show` コマンドを実行します
2. ブロードキャストドメインにポートを追加するか、ブロードキャストドメインからポートを削除します。

状況	使用
ブロードキャストドメインにポートを追加します	<code>network port broadcast-domain add-ports</code>
ブロードキャストドメインからポートを削除します	<code>network port broadcast-domain remove-ports</code>

3. ポートがブロードキャストドメインに対して追加または削除されたことを確認します。

```
network port show
```

これらのコマンドの詳細については、を参照してください ["ONTAP 9 のコマンド"](#)。

ポートの追加と削除の例

次のコマンドは、Default IPspace のブロードキャストドメイン `bcast1` に、ノード `cluster-1-01` のポート `e0g` と、ノード `cluster-1-02` の `e0g` を追加します。

```
cluster-1::> network port broadcast-domain add-ports -broadcast-domain bcast1  
-ports cluster-1-01:e0g,cluster1-02:e0g
```

次のコマンドは、Cluster IPspace のブロードキャストドメイン `Cluster` にクラスタポートを 2 つ追加します。

```
cluster-1::> network port broadcast-domain add-ports -broadcast-domain Cluster  
-ports cluster-2-03:e0f,cluster2-04:e0f -ipspace Cluster
```

次のコマンドは、Default IPspace のブロードキャストドメイン `bcast1` から、ノード `cluster1-01` のポート `e0e` を削除します。

```
cluster-1::> network port broadcast-domain remove-ports -broadcast-domain bcast1  
-ports cluster-1-01:e0e
```

ブロードキャストドメインのスプリット (ONTAP 9.7以前)

既存のブロードキャストドメインを 2 つにスプリットして、それぞれのドメインに、元のブロードキャストドメインに割り当てられていたポートのいくつかを含めることができます。

このタスクについて

- ポートがフェイルオーバーグループに含まれている場合は、グループ内のすべてのポートをスプリットする必要があります。

- ポートに LIF が関連付けられている場合は、LIF をサブネットの範囲に含めることはできません。

## ステップ

ブロードキャストドメインを 2 つのブロードキャストドメインにスプリットします。

```
network port broadcast-domain split -ipspace <ipspace_name> -broadcast  
-domain <broadcast_domain_name> -new-broadcast-domain  
<broadcast_domain_name> -ports <node:port,node:port>
```

- `ipspace_name` は、ブロードキャストドメインのある IPspace の名前です。
- `-broadcast-domain` は、スプリットするブロードキャストドメインの名前です。
- `-new-broadcast-domain` は、作成する新しいブロードキャストドメインの名前です。
- `-ports` は、新しいブロードキャストドメインに追加するノードの名前とポートです。

## ブロードキャストドメインのマージ (ONTAP 9.7 以前)

`merge` コマンドを使用して、1 つのブロードキャストドメインのすべてのポートを既存のブロードキャストドメインに移動することができます。

この方法を使用すると、ブロードキャストドメインのすべてのポートを削除してから、既存のブロードキャストドメインに追加するという手順を踏まなくて済みます。

## ステップ

1 つのブロードキャストドメインのポートを既存のブロードキャストドメインにマージします。

```
network port broadcast-domain merge -ipspace <ipspace_name> -broadcast  
-domain <broadcast_domain_name> -into-broadcast-domain  
<broadcast_domain_name>
```

- `ipspace_name` は、ブロードキャストドメインのある IPspace の名前です。
- `-broadcast-domain` は、マージするブロードキャストドメインの名前です。
- `-into-broadcast-domain` は、追加のポートを受け取るブロードキャストドメインの名前です。

## 例

次の例では、`bd-data1` というブロードキャストドメインを `bd-data2` というブロードキャストドメインにマージしています。

```
network port -ipspace Default broadcast-domain bd-data1 into-broadcast-domain bd-  
data2
```

## ブロードキャストドメイン (ONTAP 9.7 以前) のポートの MTU 値を変更する

あるブロードキャストドメインの MTU 値を変更することにより、そのブロードキャスト

トドメインのすべてのポートの MTU 値を変更できます。これは、ネットワークで行われたトポロジの変更をサポートするために実行できます。

作業を開始する前に

管理トラフィックを処理する e0M ポートを除く、レイヤ 2 ネットワークに接続されているすべてのデバイスの MTU 値が一致している必要があります。

このタスクについて

MTU 値を変更すると、影響を受けるポートを経由するトラフィックが一時的に中断されます。プロンプトが表示され、回答の MTU 値を変更するために「y」と入力する必要があります。

ステップ

ブロードキャストドメインのすべてのポートの MTU 値を変更します。

```
network port broadcast-domain modify -broadcast-domain  
<broadcast_domain_name> -mtu <mtu_value> [-ipspace <ipspace_name>]
```

- broadcast\_domain は、ブロードキャストドメインの名前です。
- mtu は IP パケットの MTU サイズです。通常は 1500 と 9000 です。
- ipspace は、このブロードキャストドメインが配置されている IPspace の名前です。「default」IPspace は、このオプションの値を指定しないかぎり使用されます。次のコマンドは、ブロードキャストドメイン「bcast1」のすべてのポートの MTU を 9000 に変更します。

```
network port broadcast-domain modify -broadcast-domain <Default-1> -mtu <  
9000 >  
Warning: Changing broadcast domain settings will cause a momentary data-  
serving interruption.  
Do you want to continue? {y|n}: <y>
```

ブロードキャストドメインを表示する (**ONTAP 9.7**以前)

クラスタの各 IPspace 内にあるブロードキャストドメインのリストを表示できます。この出力には、各ブロードキャストドメインのポートと MTU 値のリストも含まれます。

ステップ

クラスタのブロードキャストドメイン、および関連付けられているポートを表示します。

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

次のコマンドは、クラスタのすべてのブロードキャストドメイン、および関連付けられているポートを表示します。

```

network port broadcast-domain show
IPspace Broadcast
Name      Domain Name  MTU   Port List
-----
Cluster Cluster      9000
          cluster-1-01:e0a    complete
          cluster-1-01:e0b    complete
          cluster-1-02:e0a    complete
          cluster-1-02:e0b    complete
Default Default      1500
          cluster-1-01:e0c    complete
          cluster-1-01:e0d    complete
          cluster-1-02:e0c    complete
          cluster-1-02:e0d    complete
          bcast1      1500
          cluster-1-01:e0e    complete
          cluster-1-01:e0f    complete
          cluster-1-01:e0g    complete
          cluster-1-02:e0e    complete
          cluster-1-02:e0f    complete
          cluster-1-02:e0g    complete

```

次のコマンドは、bcast1 というブロードキャストドメインにある、更新ステータスがエラーのポートを表示します。このポートは、ポートを正しく更新できなかったことを示します。

```

network port broadcast-domain show -broadcast-domain bcast1 -port-update
-status error

IPspace Broadcast
Name      Domain Name  MTU   Port List
-----
Default bcast1      1500
          cluster-1-02:e0g    error

```

詳細については、を参照してください ["ONTAP 9 のコマンド"](#)。

ブロードキャストドメインを削除する

不要になったブロードキャストドメインは削除できます。削除することで、そのブロードキャストドメインに関連付けられていたポートは「Default」IPspace に移動します。

作業を開始する前に

削除するブロードキャストドメインに、関連付けられているサブネット、ネットワークインターフェイス、SVM がないようにします。

このタスクについて

- システムで作成された「Cluster」ブロードキャストドメインを削除することはできません。
- ブロードキャストドメインを削除すると、そのドメインに関連するフェイルオーバーグループもすべて削除されます。


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

#### System Manager の略

- ONTAP 9.12.0以降では、System Managerを使用してブロードキャストドメイン\*を削除できます

ブロードキャストドメインにポートが含まれている場合やサブネットに関連付けられている場合は、削除オプションは表示されません。

手順

1. [ネットワーク]>[概要]>[ブロードキャストドメイン\*]を選択します。
2. 選択するオプション  削除するブロードキャストドメインの横にある削除\*をクリックします。

#### CLI の使用

\*ブロードキャストドメイン\*を削除するには、CLIを使用してください

ステップ

ブロードキャストドメインを削除します。

```
network port broadcast-domain delete -broadcast-domain broadcast_domain_name
[-ipspace ipspace_name]
```

次のコマンドは、`ipspace1` という IPspace のブロードキャストドメイン `default-1` を削除します。

```
network port broadcast-domain delete -broadcast-domain Default-1 -ipspace
ipspace1
```

## フェイルオーバーグループとポリシー

### LIFフェイルオーバーの概要

LIF フェイルオーバーとは、LIF の現在のポートでリンク障害が発生した場合に別のネットワークポートに LIF を自動的に移行する機能です。これは、SVM との接続の高可用性を実現するための重要な機能です。LIF のフェイルオーバーを設定するには、フェイルオーバーグループを作成し、フェイルオーバーグループを使用するように LIF を変更してから、フェイルオーバーポリシーを指定します。

フェイルオーバーグループは、クラスタ内の 1 つ以上のノードのネットワークポート（物理ポート、VLAN、インターフェイスグループ）をまとめたものです。フェイルオーバーグループにあるネットワークポートによって、LIF で使用可能なフェイルオーバーターゲットが決まります。フェイルオーバーグループには、クラスタ管理 LIF、ノード管理 LIF、クラスタ間 LIF、および NAS データ LIF を割り当てることができます。





LIF に有効なフェイルオーバーターゲットを設定していないと、LIF がフェイルオーバーしようとしたときにシステムが停止します。フェイルオーバーの設定を確認するには、「`network interface show -failover`」コマンドを使用します。

ブロードキャストドメインを作成すると、同じネットワークポートを含む同じ名前のフェイルオーバーグループが自動的に作成されます。このフェイルオーバーグループはシステムによって自動的に管理されます。つまり、ブロードキャストドメインのポートが追加または削除されると、フェイルオーバーグループのポートも自動的に追加または削除されます。この機能により、管理者が自分のフェイルオーバーグループを管理する手間を省くことができます。

## フェイルオーバーグループを作成します

ネットワークポートのフェイルオーバーグループを作成して、LIF の現在のポートでリンク障害が発生した場合に、LIF が別のポートに自動的に移行できるようにします。これにより、システムのネットワークトラフィックがクラスタ内の使用可能な他のポートに再ルーティングされます。

このタスクについて

を使用します `network interface failover-groups create` コマンドを使用してグループを作成し、グループにポートを追加します。

- フェイルオーバーグループに追加できるポートは、ネットワークポート、VLAN、インターフェイスグループ（ifgrp）です。
- フェイルオーバーグループに追加するポートは、すべて同じブロードキャストドメインに属している必要があります。
- 1 つのポートを複数のフェイルオーバーグループに含めることができます。
- 異なる VLAN またはブロードキャストドメインに LIF がある場合は、VLAN またはブロードキャストドメインごとにフェイルオーバーグループを設定する必要があります。
- フェイルオーバーグループは、SAN の iSCSI 環境と FC 環境には適用されません。

### ステップ

フェイルオーバーグループを作成します。

```
network interface failover-groups create -vserver vs1 -failover-group failover_group_name -targets ports_list
```

- `vs1` は、フェイルオーバーグループを使用できるSVMの名前です。
- `failover_group_name` は、作成するフェイルオーバーグループの名前です。
- `ports_list` は、フェイルオーバーグループに追加するポートのリストです。  
`node_name > : <port_number>` という形式でポートを指定してください。たとえば、`node1 : e0c` のようになります。

次のコマンドは、SVM vs3 にフェイルオーバーグループ fg3 を作成してポートを 2 つ追加します。

```
network interface failover-groups create -vserver vs3 -failover-group fg3
-targets cluster1-01:e0e,cluster1-02:e0e
```

完了後

- フェイルオーバーグループを作成したら、LIF にフェイルオーバーグループを適用する必要があります。
- 有効なフェイルオーバーターゲットのないフェイルオーバーグループを LIF に設定すると、警告メッセージが表示されます。

有効なフェイルオーバーターゲットのない LIF がフェイルオーバーしようとする、システムが停止する可能性があります。

## LIF のフェイルオーバーを設定する

フェイルオーバーポリシーとフェイルオーバーグループを LIF に適用することにより、ネットワークポートの特定のグループに LIF がフェイルオーバーするように設定できます。また、LIF の別のポートへのフェイルオーバーを無効にすることもできます。

このタスクについて

- LIF を作成すると、LIF フェイルオーバーがデフォルトで有効になり、使用可能なターゲットポートのリストが、LIF のタイプとサービスポリシーに基づくデフォルトのフェイルオーバーグループとフェイルオーバーポリシーによって決まります。

9.5 以降では、LIF を使用できるネットワークサービスを定義するサービスポリシーを LIF に指定できます。一部のネットワークサービスでは、LIF のフェイルオーバーが制限されます。



フェイルオーバーをさらに制限する方法で LIF のサービスポリシーを変更すると、LIF のフェイルオーバーポリシーが自動的に更新されます。

- LIF のフェイルオーバーの動作は、`network interface modify` コマンドの `-failover-group` パラメータと `-failover-policy` パラメータの値を指定することによって変更することができます。
- LIF の変更によって、LIF に有効なフェイルオーバーターゲットがなくなる場合は警告メッセージが表示されます。

有効なフェイルオーバーターゲットのない LIF がフェイルオーバーしようとする、システムが停止する可能性があります。

- ONTAP 9.11.1以降のオールフラッシュSANアレイ（ASA）プラットフォームでは、新規に作成したStorage VMに新しく作成したiSCSI LIFでiSCSI LIFのフェイルオーバーが自動的に有効になります。

また、を使用することもできます **"既存のiSCSI LIFでiSCSI LIFフェイルオーバーを手動で有効にする"** ONTAP 9.11.1以降にアップグレードする前に作成されたLIFを意味します。

- 次に、`-failover-policy` の設定によって、フェイルオーバーグループからどのターゲットポートが選択されるかを示します。



iSCSI LIFのフェイルオーバーの場合は、フェイルオーバーポリシーのみ `local-only`、`sfo-partner-only` および `disabled` がサポートされます。

- broadcast-domain-wide フェイルオーバーグループ内のすべてのノードのすべてのポートを環境 にします。
- system-defined 環境 は、LIFのホームノードとクラスタ内の他の1つのノード（存在する場合は通常はSFO以外のパートナー）にあるポートのみを対象とします。
- local-only 環境 を実行するのは、LIFのホームノードのポートだけです。
- sfo-partner-only 環境 を実行するのは、LIFのホームノードとそのSFOパートナーのポートだけです。
- disabled LIFにフェイルオーバーが設定されていないことを示します。

## ステップ

既存のインターフェイスのフェイルオーバーを設定します。

```
network interface modify -vserver <vserver_name> -lif <lif_name> -failover
-policy <failover_policy> -failover-group <failover_group>
```

## フェイルオーバーの設定例、および無効化の例

次のコマンドは、フェイルオーバーポリシーを broadcast-domain-wide に設定し、SVM vs3 の data1 という LIF のフェイルオーバーターゲットとして、フェイルオーバーグループ fg3 のポートを使用します。

```
network interface modify -vserver vs3 -lif data1 failover-policy
broadcast-domain-wide - failover-group fg3
```

```
network interface show -vserver vs3 -lif * -fields failover-
group,failover-policy
```

vserver	lif	failover-policy	failover-group
vs3	data1	broadcast-domain-wide	fg3

次のコマンドは、SVM vs3 の data1 という LIF のフェイルオーバーを無効にします。

```
network interface modify -vserver vs3 -lif data1 failover-policy disabled
```

## フェイルオーバーグループとポリシーを管理するためのコマンドです

を使用できます network interface failover-groups フェイルオーバーグループを管理するためのコマンド。を使用します network interface modify コマンドを使用して、LIFに適用されるフェイルオーバーグループとフェイルオーバーポリシーを管理します。

状況	使用するコマンド
----	----------

フェイルオーバーグループにネットワークポートを追加します	<code>network interface failover-groups add-targets</code>
フェイルオーバーグループからネットワークポートを削除します	<code>network interface failover-groups remove-targets</code>
フェイルオーバーグループのネットワークポートを変更する	<code>network interface failover-groups modify</code>
現在のフェイルオーバーグループを表示します	<code>network interface failover-groups show</code>
LIF のフェイルオーバーを設定する	<code>network interface modify -failover -group -failover-policy</code>
各 LIF で使用されているフェイルオーバーグループとフェイルオーバーポリシーを表示します	<code>network interface show -fields failover-group, failover-policy</code>
フェイルオーバーグループの名前を変更します	<code>network interface failover-groups rename</code>
フェイルオーバーグループを削除します	<code>network interface failover-groups delete</code>



フェイルオーバーグループを変更した結果、クラスタ内のどの LIF も有効なフェイルオーバーターゲットを持たなくなってしまうと、LIF がフェイルオーバーしようとしたときにシステムが停止する可能性があります。

詳細については、のマニュアルページを参照してください `network interface failover-groups` および `network interface modify` コマンド

## サブネット（クラスタ管理者のみ）

### サブネットの概要

サブネットを使用すると、ONTAP ネットワーク設定用の IP アドレスの特定のブロックまたはプールを割り当てることができます。そのため、IP アドレスやネットワークマスク値を指定する代わりにサブネット名を指定して、LIF を簡単に作成できます。

サブネットはブロードキャストドメイン内に作成され、同じレイヤ 3 サブネットに属する IP アドレスのプールを含んでいます。サブネット内の IP アドレスは、LIF の作成時にブロードキャストドメインのポートに割り当てられます。LIF を削除すると、その IP アドレスはサブネットプールに返され、以降の LIF で使用できるようになります。

IP アドレスの管理が容易になり、LIF を簡単な手順で作成できるようになるため、サブネットを使用することを推奨します。また、サブネットを定義するときにゲートウェイを指定した場合、そのサブネットを使用して LIF を作成すると、そのゲートウェイへのデフォルトルートが SVM に自動的に追加されます。

## サブネットを作成

サブネットを作成してIPv4またはIPv6アドレスの特定のブロックを割り当て、あとでSVMのLIFを作成するときに使用できます。

そのため、各 LIF の IP アドレスやネットワークマスク値を指定する代わりに、サブネット名を指定して簡単に LIF を作成できます。

作業を開始する前に

このタスクを実行するには、クラスタ管理者である必要があります。

サブネットを追加するブロードキャストドメインと IPspace がすでに存在している必要があります。

このタスクについて

- すべてのサブネット名が IPspace 内で一意である必要があります。
- サブネットに IP アドレスの範囲を追加するときは、別々のサブネットまたはホストで同じ IP アドレスが使用されないように、ネットワーク内で IP アドレスの範囲が重複しないことを確認する必要があります。
- サブネットを定義するときにゲートウェイを指定した場合は、そのサブネットを使用して LIF を作成するときに、そのゲートウェイへのデフォルトルートが SVM に自動的に追加されます。サブネットを使用しない場合、またはサブネットを定義するときにゲートウェイを指定しない場合は、を使用する必要があります route create コマンドを使用してSVMにルートを手動で追加します。

手順

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

## System Manager の略

ONTAP 9.12.0以降では、System Managerを使用してサブネットを作成できます。

### 手順

1. [ネットワーク]>[概要]>[サブネット\*]を選択します。
2. をクリックします **+ Add** をクリックしてください。
3. サブネットに名前を付けます。
4. サブネットのIPアドレスを指定します。
5. サブネットマスクを設定します。
6. サブネットを構成するIPアドレスの範囲を定義します。
7. 必要に応じて、ゲートウェイを指定します。
8. サブネットが属しているブロードキャストドメインを選択します。
9. 変更を保存します。
  - a. 入力したIPアドレスまたは範囲がすでにインターフェイスで使用されている場合は、次のメッセージが表示されます。  
An IP address in this range is already in use by a LIF. Associate the LIF with this subnet?
  - b. OK \*をクリックすると、既存のLIFがサブネットに関連付けられます。

### CLI の使用

CLIを使用してサブネットを作成してください。

```
network subnet create -subnet-name subnet_name -broadcast-domain  
<broadcast_domain_name> [- ipspace <ipspace_name>] -subnet  
<subnet_address> [-gateway <gateway_address>] [-ip-ranges  
<ip_address_list>] [-force-update-lif-associations <true>]
```

- subnet\_name は、作成するレイヤ3サブネットの名前です。

「Mgmt」のようなテキスト文字列形式の名前を付けることも、192.0.2.0/24 などのサブネットのIPアドレスの値にすることもできます。

- broadcast\_domain\_name は、サブネットが配置されるブロードキャストドメインの名前です。
- ipspace\_name は、ブロードキャストドメインが属するIPspaceの名前です。

「default」 IPspace は、このオプションの値を指定しないかぎり使用されます。

- subnet\_address は、サブネットのIPアドレスとマスクです。たとえば、192.0.2.0/24のように指定します。
- gateway\_address は、サブネットのデフォルトルートのゲートウェイです。たとえば、192.0.2.1のように指定します。

- `ip_address_list` は、サブネットに割り当てるIPアドレスのリストまたは範囲です。

個別の IP アドレス、IP アドレスの範囲、またはその組み合わせをカンマで区切って指定できます。

- 値 `true` に設定できます `-force-update-lif-associations` オプション

指定した範囲の IP アドレスを現在使用しているサービスプロセッサまたはネットワークインターフェイスがある場合は、このコマンドが失敗します。この値を `true` に設定すると、手動でアドレスが指定されているインターフェイスが現在のサブネットに関連付けられ、コマンドは問題なく実行されます。

次のコマンドは、Default IPspace のブロードキャストドメイン `default-1` に `sub1` というサブネットを作成します。IPv4 のサブネット IP アドレスとマスク、ゲートウェイ、IP アドレスの範囲を指定しています。

```
network subnet create -subnet-name sub1 -broadcast-domain Default-1
-subnet 192.0.2.0/24 - gateway 192.0.2.1 -ip-ranges 192.0.2.1-
192.0.2.100, 192.0.2.122
```

次のコマンドは、「Default」IPspace のブロードキャストドメイン `Default` に `sub2` というサブネットを作成します。IPv6 アドレスの範囲を指定しています。

```
network subnet create -subnet-name sub2 -broadcast-domain Default
-subnet 3FFE::/64 - gateway 3FFE::1 -ip-ranges "3FFE::10-3FFE::20"
```

完了後

サブネット内のアドレスを使用して、SVM とインターフェイスを IPspace に割り当てることができます。

既存のサブネットの名前を変更する必要がある場合は、を使用します `network subnet rename` コマンドを実行します

## サブネットの IP アドレスを追加または削除します


新しくサブネットを作成するときに IP アドレスを追加したり、既存のサブネットに IP アドレスを追加したりできます。既存のサブネットから IP アドレスを削除することもできます。このようにして、SVM に必要な IP アドレスだけが割り当てられるようにします。

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

### System Manager の略

- ONTAP 9.12.0以降では、System Managerを使用して、サブネット\*に対してIPアドレスを追加または削除できます

#### 手順

1. [ネットワーク]>[概要]>[サブネット\*]を選択します。
2. 選択するオプション  \*>変更するサブネットの横にあるEdit \*をクリックします。
3. IPアドレスを追加または削除します。
4. 変更を保存します。
  - a. 入力したIPアドレスまたは範囲がすでにインターフェイスで使用されている場合は、次のメッセージが表示されます。  
An IP address in this range is already in use by a LIF. Associate the LIF with this subnet?
  - b. OK \*をクリックすると、既存のLIFがサブネットに関連付けられます。

#### CLI の使用

- CLIを使用して、IPアドレスをサブネットに追加したり、サブネットから削除したりします。\*

#### このタスクについて

IP アドレスを追加するときに、追加しようとしている範囲の IP アドレスを使用しているサービスプロセッサまたはネットワークインターフェイスがあるとエラーが表示されます。手動でアドレスを指定したインターフェイスを現在のサブネットに関連付ける場合は、を設定できます `-force-update-lif-associations` オプションをに設定します `true`。

IP アドレスを削除するときに、削除する IP アドレスを使用しているサービスプロセッサまたはネットワークインターフェイスがあるとエラーが表示されます。サブネットから削除したIPアドレスをインターフェイスで引き続き使用するには、を設定します `-force-update-lif-associations` オプションをに設定します `true`。

#### ステップ

サブネットの IP アドレスを追加または削除します。

状況	使用するコマンド
サブネットに IP アドレスを追加する	<code>network subnet add-ranges</code>
サブネットから IP アドレスを削除します	<code>network subnet remove-ranges</code>

これらのコマンドの詳細については、マニュアルページを参照してください。

次のコマンドは、192.0.2.82~192.0.2.85 の IP アドレスをサブネット sub1 に追加します。



```
network subnet add-ranges -subnet-name <sub1> -ip-ranges <192.0.2.82-192.0.2.85>
```

次のコマンドは、IP アドレス 198.51.100.9 をサブネット sub3 から削除します。

```
network subnet remove-ranges -subnet-name <sub3> -ip-ranges <198.51.100.9>
```

現在の範囲が 1~10 と 20~40 で、追加するアドレスが 11~19 と 41~50（つまり、1~50 を範囲にする）の場合は、次のコマンドを使用して既存のアドレス範囲と重複させることができます。このコマンドは新しいアドレスのみを追加し、既存のアドレスには影響しません。

```
network subnet add-ranges -subnet-name <sub3> -ip-ranges <198.51.10.1-198.51.10.50>
```

## サブネットのプロパティを変更します

既存のサブネットのアドレスとマスク値、ゲートウェイアドレス、IP アドレスの範囲を変更することができます。

このタスクについて


- IP アドレスを変更するときは、別々のサブネットまたはホストで同じ IP アドレスが使用されることのないように、ネットワーク内で IP アドレスの範囲が重複しないようにする必要があります。
- ゲートウェイの IP アドレスを追加または変更した場合は、LIF を作成するときに、変更したゲートウェイがサブネットを使用して新しい SVM に適用されます。SVM のゲートウェイへのルートがない場合は、デフォルトルートが作成されます。ゲートウェイの IP アドレスを変更した場合は、SVM に新しいルートを手動で追加する必要があります。

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

## System Manager の略

- ONTAP 9.12.0以降では、System Managerを使用してサブネットのプロパティを変更できます\*

### 手順

1. [ネットワーク]>[概要]>[サブネット\*]を選択します。
2. 選択するオプション  \*>変更するサブネットの横にあるEdit \*をクリックします。
3. 変更を加えます。
4. 変更を保存します。
  - a. 入力したIPアドレスまたは範囲がすでにインターフェイスで使用されている場合は、次のメッセージが表示されます。  
An IP address in this range is already in use by a LIF. Associate the LIF with this subnet?
  - b. OK \*をクリックすると、既存のLIFがサブネットに関連付けられます。

### CLI の使用

- CLIを使用して、サブネットのプロパティを変更します。\*

### ステップ

サブネットのプロパティを変更します。

```
network subnet modify -subnet-name <subnet_name> [-ip-space
<ip-space_name>] [-subnet <subnet_address>] [-gateway <gateway_address>]
[-ip-ranges <ip_address_list>] [-force-update-lif-associations <true>]
```

- subnet\_name は、変更するサブネットの名前です。
- ip-space は、サブネットのあるIPspaceの名前です。
- subnet は、サブネットの新しいアドレスとマスクです（該当する場合）。たとえば、192.0.2.0/24のように指定します。
- gateway は、サブネットの新しいゲートウェイです（該当する場合）。たとえば、192.0.2.1のように指定します。「\*」と入力すると、ゲートウェイのエントリが削除されます。
- ip\_ranges は、サブネットに割り当てる新しいIPアドレスのリストまたは範囲です（該当する場合）。個別のIPアドレス、IPアドレスの範囲、またはその組み合わせをカンマで区切って指定できます。ここで指定した範囲によって、既存のIPアドレスが置き換えられます。
- force-update-lif-associations は、IPアドレス範囲を変更する場合に必要です。IPアドレスの範囲を変更する場合、このオプションの値を \* true \* に設定できます。指定した範囲のIPアドレスを使用しているサービスプロセスまたはネットワークインターフェイスがある場合は、このコマンドが失敗します。この値を \* true に設定すると、手動でアドレスが指定されているインターフェイスが現在のサブネットに関連付けられ、コマンドは問題なく実行されます。

次のコマンドは、sub3 というサブネットのゲートウェイのIPアドレスを変更します。

```
network subnet modify -subnet-name <sub3> -gateway <192.0.3.1>
```

## サブネットを表示します

IPspace 内の各サブネットに割り当てられている IP アドレスのリストを表示することができます。この出力には、各サブネットの使用可能な IP アドレスの総数、および現在使用されているアドレスの数も表示されます。

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

### System Manager の略

- ONTAP 9.12.0以降では、System Managerでサブネットを表示できます\*

#### 手順

1. [ネットワーク]>[概要]>[サブネット\*]を選択します。
2. サブネットのリストを表示します。

### CLI の使用

- CLIを使用してサブネット\*を表示します

#### ステップ

サブネットのリスト、およびそれらのサブネットで使用されている関連付けられた IP アドレスの範囲を表示します。

```
network subnet show
```

次のコマンドは、サブネットおよびサブネットのプロパティを表示します。

```
network subnet show
```

IPspace: Default

Subnet		Broadcast		Avail/	
Name	Subnet	Domain	Gateway	Total	Ranges
sub1	192.0.2.0/24	bcast1	192.0.2.1	5/9	192.0.2.92-192.0.2.100
sub3	198.51.100.0/24	bcast3	198.51.100.1	3/3	198.51.100.7,198.51.100.9

## サブネットを削除します


サブネットが不要になり、そのサブネットの IP アドレスの割り当てを解除したい場合は、サブネットを削除します。

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

### System Manager の略

- ONTAP 9.12.0以降では、System Managerを使用してサブネット\*を削除できます

#### 手順

1. [ネットワーク]>[概要]>[サブネット\*]を選択します。
2. 選択するオプション  削除するサブネットの横にある削除\*をクリックします。
3. 変更を保存します。

### CLI の使用

- CLIを使用してサブネット\*を削除してください

#### このタスクについて

指定した範囲の IP アドレスを現在使用しているサービスプロセッサまたはネットワークインターフェイスがある場合は、エラーが表示されます。サブネットを削除したあとも、インターフェイスでその IP アドレスを使用する場合は、`-force-update-lif-associations` オプションを `true` に設定して、サブネットの LIF との割り当てを解除します。

#### ステップ

サブネットを削除します。

```
network subnet delete -subnet-name subnet_name [-ipspace ipspace_name] [-force-update-lif-associations true]
```

次のコマンドは、`ipspace1` という IPspace のサブネット `sub1` を削除します。

```
network subnet delete -subnet-name sub1 -ipspace ipspace1
```

## SVMs を作成します

クライアントにデータを提供するには、SVM を作成する必要があります。

#### 作業を開始する前に

- このタスクを実行するには、クラスタ管理者である必要があります。
- SVM のルートボリュームに設定するセキュリティ形式を決めておく必要があります。

この SVM に Hyper-V over SMB または SQL Server over SMB 解決策を実装する予定がある場合は、ルートボリュームに NTFS セキュリティ形式を使用してください。Hyper-V ファイルまたは SQL データベースファイルを格納するボリュームは、作成時に NTFS セキュリティ形式に設定する必要があります。ルートボリュームのセキュリティ形式を NTFS に設定しておく、UNIX セキュリティ形式または mixed セキ

ユリティ形式のデータボリュームを誤って作成することがありません。

- ONTAP 9.13.1以降では、Storage VMに最大容量を設定できます。また、SVMの容量レベルがしきい値に近づいたときにアラートを設定することもできます。詳細については、を参照してください [SVM容量の管理](#)。

## System Manager の略

System Managerを使用してStorage VMを作成できます。

### 手順

1. Storage VM\*を選択します。
2. をクリックします **+ Add** Storage VMを作成してください。
3. Storage VMの名前を指定
4. アクセスプロトコルを選択します。
  - SMB / CIFS、NFS
  - iSCSI
  - FC
  - NVMe
  - i. SMB / CIFSの有効化\*を選択した場合は、次の設定を行います。

フィールドまたはチェックボックス	説明
管理者の名前	SMB / CIFS Storage VMの管理者ユーザ名を指定してください。
パスワード	SMB / CIFS Storage VMの管理者パスワードを指定してください。
サーバー名	SMB / CIFS Storage VMのサーバ名を指定してください。
Active Directory ドメイン	SMB / CIFS Storage VMにユーザ認証を提供するActive Directory ドメインを指定してください。
組織単位	SMB / CIFSサーバに関連付けられたActive Directory ドメイン内の組織単位を指定します。「CN=Computers」はデフォルト値であり、変更できます。
Storage VM内の共有へのアクセス時にデータを暗号化する	SMB 3.0を使用してデータを暗号化し、SMB / CIFS Storage VM内の共有に対する不正なファイルアクセスを防止するには、このチェックボックスを選択します。
ドメイン	SMB / CIFS Storage VMに対して表示されているドメインを追加、削除、または順序変更する。
ネームサーバ	SMB / CIFS Storage VMのネームサーバの追加、削除、または順序変更

デフォルト言語	Storage VMとそのボリュームのデフォルトの言語エンコード設定を指定します。Storage VM内の個々のボリュームの設定を変更する場合はCLIを使用してください。
Network Interface の略	Storage VMに設定するネットワークインターフェイスごとに、既存のサブネットを選択するか（少なくとも1つ存在する場合）、または「サブネットなし」と指定し、「IPアドレス*」フィールドと「サブネットマスク」フィールドを入力します。 使用する場合は、* Use the same subnet mask and gateway for all of the following interfaces*チェックボックスをオンにします。 ホームポートを自動的に選択することも、リストから使用するポートを手動で選択することもできます。
管理者アカウントを管理する	Storage VM管理者アカウントを管理する場合は、このチェックボックスを選択します。選択すると、ユーザ名とパスワードを指定し、確認のためにパスワードをもう一度入力し、Storage VM管理用にネットワークインターフェイスを追加するかどうかを指定します。

1. NFSの有効化\*を選択した場合は、次の設定を行います。

フィールドまたはチェックボックス	説明
Allow NFS client accessチェックボックス	NFS Storage VMに作成されたすべてのボリュームで、ルートボリュームパス「/」を使用してマウントとトラバースを行う必要がある場合は、このチェックボックスを選択します。エクスポートポリシー「default」にルールを追加して、マウントを中断なくトラバースできるようにします。

ルール	<p>をクリックします <b>+ Add</b> ルールを作成します。</p> <ul style="list-style-type: none"> <li>クライアント仕様：ホスト名、IPアドレス、ネットグループ、またはドメインを指定します。</li> <li>Access Protocols：次のオプションを組み合わせで選択します。 <ul style="list-style-type: none"> <li>SMB/CIFS</li> <li>FlexCache</li> <li>NFS <ul style="list-style-type: none"> <li>NFSv3</li> <li>NFSv4</li> </ul> </li> </ul> </li> <li>アクセスの詳細：各タイプのユーザについて、読み取り専用、読み取り/書き込み、またはスーパーユーザのいずれかのアクセスレベルを指定します。ユーザタイプは次のとおりです。 <ul style="list-style-type: none"> <li>すべて</li> <li>すべて（匿名ユーザとして）</li> <li>「UNIX」</li> <li>Kerberos 5.</li> <li>Kerberos 5i</li> <li>Kerberos 5p</li> <li>NTLM</li> </ul> </li> </ul> <p>ルールを保存します。</p>
デフォルト言語	<p>Storage VMとそのボリュームのデフォルトの言語エンコード設定を指定します。Storage VM内の個々のボリュームの設定を変更する場合はCLIを使用してください。</p>
Network Interface の略	<p>Storage VMに設定するネットワークインターフェイスごとに、既存のサブネットを選択するか（少なくとも1つ存在する場合）、または「サブネットなし」と指定し、「IPアドレス*」フィールドと「サブネットマスク」フィールドを入力します。</p> <p>使用する場合は、* Use the same subnet mask and gateway for all of the following interfaces*チェックボックスをオンにします。</p> <p>ホームポートを自動的に選択することも、リストから使用するポートを手動で選択することもできます。</p>



管理者アカウントを管理する	Storage VM管理者アカウントを管理する場合は、このチェックボックスを選択します。選択すると、ユーザ名とパスワードを指定し、確認のためにパスワードをもう一度入力し、Storage VM管理用にネットワークインターフェイスを追加するかどうかを指定します。
---------------	---

1. [Enable iSCSI\*]を選択した場合は、次の設定を行います。

フィールドまたはチェックボックス	説明
Network Interface の略	Storage VMに設定するネットワークインターフェイスごとに、既存のサブネットを選択するか（少なくとも1つ存在する場合）、または「サブネットなし」と指定し、「IPアドレス*」フィールドと「サブネットマスク」フィールドを入力します。 使用する場合は、* Use the same subnet mask and gateway for all of the following interfaces*チェックボックスをオンにします。 ホームポートを自動的に選択することも、リストから使用するポートを手動で選択することもできます。
管理者アカウントを管理する	Storage VM管理者アカウントを管理する場合は、このチェックボックスを選択します。選択すると、ユーザ名とパスワードを指定し、確認のためにパスワードをもう一度入力し、Storage VM管理用にネットワークインターフェイスを追加するかどうかを指定します。

1. Enable FC（FCの有効化）を選択した場合は、次の設定を行います。

フィールドまたはチェックボックス	説明
FCポートを設定	Storage VMに含めるノードのネットワークインターフェイスを選択してください。ノードごとに2つのネットワークインターフェイスを推奨します。
管理者アカウントを管理する	Storage VM管理者アカウントを管理する場合は、このチェックボックスを選択します。選択すると、ユーザ名とパスワードを指定し、確認のためにパスワードをもう一度入力し、Storage VM管理用にネットワークインターフェイスを追加するかどうかを指定します。

1. Enable NVMe/FC \*を選択した場合は、次の設定を行います。

フィールドまたはチェックボックス	説明
------------------	----

FCポートを設定	Storage VMに含めるノードのネットワークインターフェイスを選択してください。ノードごとに2つのネットワークインターフェイスを推奨します。
管理者アカウントを管理する	Storage VM管理者アカウントを管理する場合は、このチェックボックスを選択します。選択すると、ユーザ名とパスワードを指定し、確認のためにパスワードをもう一度入力し、Storage VM管理用にネットワークインターフェイスを追加するかどうかを指定します。

1. [NVMe/TCPを有効にする]\*を選択した場合は、次の設定を行います。

フィールドまたはチェックボックス	説明
Network Interface の略	Storage VMに設定するネットワークインターフェイスごとに、既存のサブネットを選択するか（少なくとも1つ存在する場合）、または「サブネットなし」と指定し、「IPアドレス*」フィールドと「サブネットマスク」フィールドを入力します。 使用する場合は、* Use the same subnet mask and gateway for all of the following interfaces*チェックボックスをオンにします。 ホームポートを自動的に選択することも、リストから使用するポートを手動で選択することもできます。
管理者アカウントを管理する	Storage VM管理者アカウントを管理する場合は、このチェックボックスを選択します。選択すると、ユーザ名とパスワードを指定し、確認のためにパスワードをもう一度入力し、Storage VM管理用にネットワークインターフェイスを追加するかどうかを指定します。

1. 変更を保存します。

## CLI の使用

ONTAP CLIを使用してサブネットを作成してください。

## 手順

1. SVM のルートボリュームを格納するためのアグリゲートを決定します。

```
storage aggregate show -has-mroot false
```

ルートボリュームを格納するための空きスペースが 1GB 以上あるアグリゲートを選択する必要があります。SVM で NAS の監査を設定する場合は、ルートアグリゲートに少なくとも 3GB の追加の空きスペースと、監査を有効にしたときに監査ステー징ボリュームの作成に使用される追加のスペースが必要です。



既存の SVM で NAS の監査がすでに有効になっている場合は、アグリゲートの作成が完了したあとすぐにアグリゲートのステージングボリュームが作成されます。

2. SVM のルートボリュームを作成するアグリゲートの名前を控えます。
3. SVM を作成するときに言語を指定する予定であり、使用する値がわからない場合は、指定する言語の値を確認し、その値を控えます。

```
vserver create -language ?
```

4. SVM を作成するときに Snapshot ポリシーを指定する予定であり、ポリシーの名前がわからない場合は、使用可能なポリシーの一覧を表示し、使用する Snapshot ポリシーの名前を確認して、その名前を控えます。

```
volume snapshot policy show -vserver vserver_name
```

5. SVM を作成するときにクォータポリシーを指定する予定であり、ポリシーの名前がわからない場合は、使用可能なポリシーの一覧を表示し、使用するクォータポリシーの名前を確認して、その名前を控えます。

```
volume quota policy show -vserver vserver_name
```

6. SVM を作成します。

```
vserver create -vserver vserver_name -aggregate aggregate_name -rootvolume  
root_volume_name -rootvolume-security-style {unix|ntfs|mixed} [-ipspace  
IPspace_name] [-language <language>] [-snapshot-policy  
snapshot_policy_name] [-quota-policy quota_policy_name] [-comment comment]
```

```
vserver create -vserver vs1 -aggregate aggr3 -rootvolume vs1_root  
-rootvolume-security-style ntfs -ipspace ipspace1 -language  
en_US.UTF-8
```

```
[Job 72] Job succeeded: Vserver creation completed
```

7. SVM の設定が正しいことを確認します。

```
vserver show -vserver vs1
```

```
Vserver: vs1
Vserver Type: data
Vserver Subtype: default
Vserver UUID: 11111111-1111-1111-1111-111111111111
Root Volume: vs1_root
Aggregate: aggr3
NIS Domain: -
Root Volume Security Style: ntfs
LDAP Client: -
Default Volume Language Code: en_US.UTF-8
Snapshot Policy: default
Comment:
Quota Policy: default
List of Aggregates Assigned: -
Limit on Maximum Number of Volumes allowed: unlimited
Vserver Admin State: running
Vserver Operational State: running
Vserver Operational State Stopped Reason: -
Allowed Protocols: nfs, cifs, ndmp
Disallowed Protocols: fcp, iscsi
QoS Policy Group: -
Config Lock: false
IPspace Name: ipspace1
Is Vserver Protected: false
```

この例では、コマンドを実行すると「vs1」という名前の SVM が IPspace 「ipspace1」に作成されます。ルートボリュームは「vs1\_root」という名前で、NTFS セキュリティ形式を使用して aggr3 に作成されます。



ONTAP 9.13.1以降では、アダプティブQoSポリシーグループテンプレートを設定して、SVM内のボリュームにスループットの下限と上限の制限を適用できます。このポリシーはSVMの作成後にのみ適用できます。このプロセスの詳細については、[を参照してください アダプティブポリシーグループテンプレートを設定します。](#)

## 論理インターフェイス（LIF）

### LIFの概要

#### LIFの設定の概要

LIF（論理インターフェイス）は、クラスタ内のノードへのネットワークアクセスポイントを表します。LIF は、クラスタでネットワーク経由の通信の送受信に使用されるポートに設定できます。

クラスタ管理者は、次のものを作成、表示、変更、移行、リバートできます。 または LIF を削除します。SVM 管理者は、SVM に関連付けられている LIF だけを表示できます。

LIF は、サービスポリシー、ホームポート、ホームノード、フェイルオーバー先のポートのリスト、ファイアウォールポリシーなどの特性が関連付けられている IP アドレスまたは WWPN です。LIF は、クラスタでネットワーク経由の通信の送受信に使用されるポートに設定できます。



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

LIF をホストできるポートは次のとおりです。

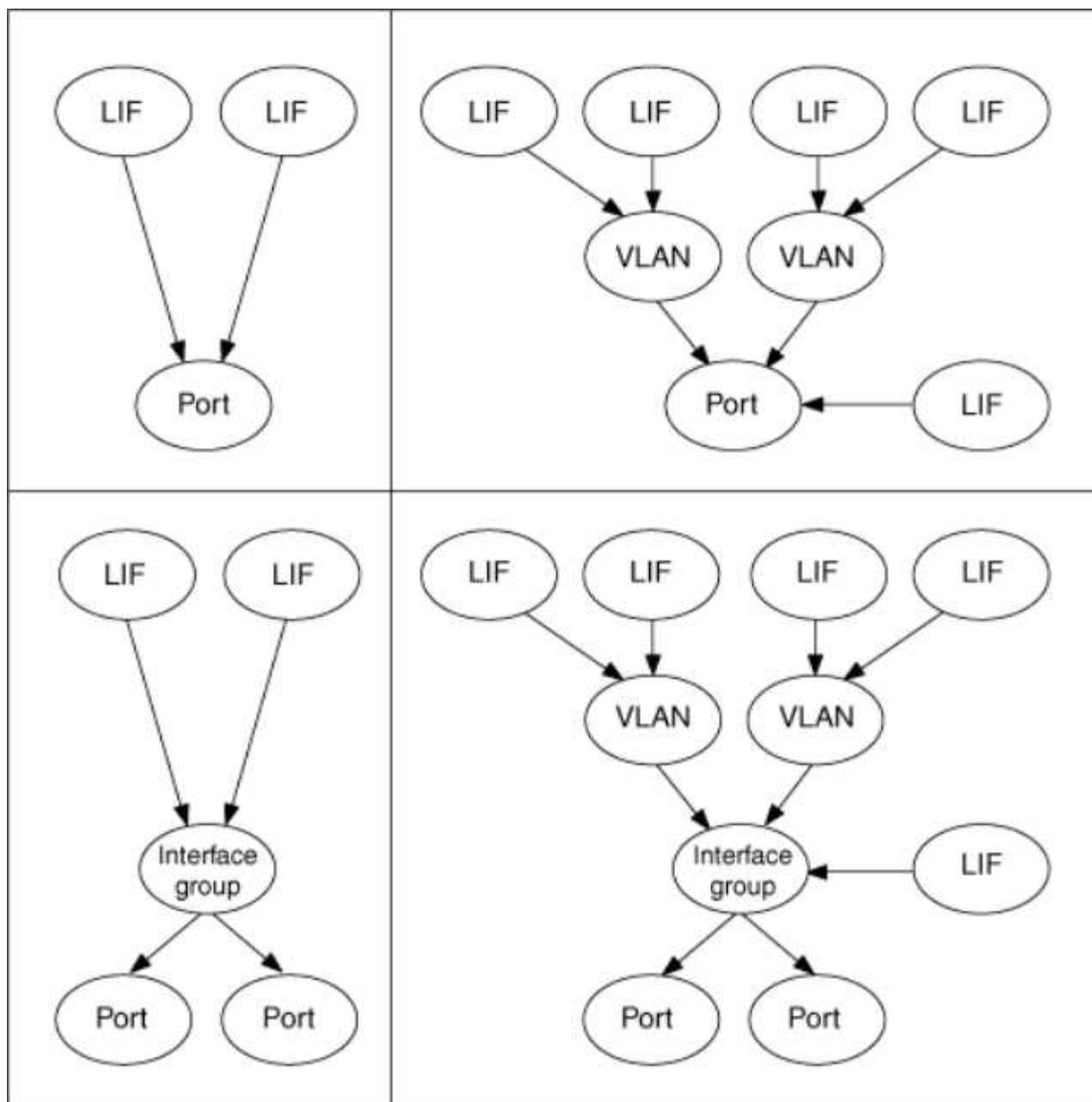
- インターフェイスグループに属していない物理ポート
- インターフェイスグループ
- VLAN
- VLAN をホストする物理ポートまたはインターフェイスグループ
- 仮想 IP （VIP）ポート

ONTAP 9.5 以降では、VIP LIF がサポートされており、VIP ポートでホストされます。

LIF で FC などの SAN プロトコルを設定する場合は、WWPN に関連付けられます。

## "SAN 管理"

次の図に、ONTAP システムのポート階層を示します。



#### LIFのフェイルオーバーとギブバック

LIFのフェイルオーバーは、LIFがホームノードまたはポートからHAパートナーノードまたはポートに移動したときに発生します。LIFのフェイルオーバーは、ONTAPによって自動的にトリガーされることも、クラスタ管理者が手動でトリガーして、物理イーサネットリンクの停止やノードのReplicated Database (RDB; レプリケートされたデータベース) クォーラムのメンバーでないノードなどのイベントが発生したときにトリガーされます。LIFのフェイルオーバーが発生した場合、フェイルオーバーの理由が解決されるまで、ONTAPはパートナーノードで通常の動作を継続します。ホームノードまたはホームポートの健全性が回復すると、LIFはHAパートナーからホームノードまたはホームポートにリバートされます。このリバートはギブバックと呼ばれます。

LIFのフェイルオーバーとギブバックを実行するには、各ノードのポートが同じブロードキャストドメインに属している必要があります。各ノードの関連するポートが同じブロードキャストドメインに属していることを確認するには、次の手順を参照してください。

- ONTAP 9.8以降: ["ポートの到達可能性を修復します"](#)

- ONTAP 9.7以前： "ブロードキャストドメインのポートを追加または削除します"

LIFのフェイルオーバーが（自動または手動で）有効になっているLIFの場合は、次の点に注意してください。

- データサービスポリシーを使用するLIFでは、フェイルオーバーポリシーの制限を確認できます。
  - ONTAP 9.6以降： "ONTAP 9.6 以降の LIF とサービスポリシー"
  - ONTAP 9.5以前： "ONTAP 9.5 以前の LIF のロール"
- LIFの自動リバートは、自動リバートをに設定した場合に実行されます true LIFのホームポートが正常に機能しており、LIFをホストできる場合。
- 計画的または計画外のノードのテイクオーバーでは、テイクオーバーされたノードのLIFがHAパートナーにフェイルオーバーされます。LIFのフェイルオーバー先のポートは、VIF Managerで決定されます。
- フェイルオーバーが完了すると、LIFは正常に動作します。
- auto-revertがに設定されている場合、ギブバックが開始されると、LIFはホームノードとホームポートにリバートされます。 true。
- 1つ以上のLIFをホストしているポートでイーサネットリンクが停止すると、VIF ManagerはLIFを停止しているポートから同じブロードキャストドメイン内の別のポートに移行します。新しいポートは、同じノードまたはそのHAパートナーに配置できます。リンクがリストアされ、auto-revertがに設定されている場合 `true` を選択すると、LIFがそれぞれのホームノードおよびホームポートにリバートされます。
- ノードがレプリケートされたデータベース（RDB）クォーラムのメンバーでなくなると、VIF ManagerはLIFをクォーラムのノードからHAパートナーに移行します。ノードがクォーラムに戻ったあと、およびauto-revertがに設定されている場合 `true` を選択すると、LIFがそれぞれのホームノードおよびホームポートにリバートされます。

ポートのタイプと **LIF** の互換性があります

LIF には、さまざまなポートタイプをサポートするための特性があります。



クラスタ間 LIF と管理 LIF が同じサブネットに設定されていると、管理トラフィックが外部のファイアウォールによってブロックされ、AutoSupport 接続と NTP 接続が失敗する可能性があります。システムをリカバリするには、を実行します `network interface modify -vserver vservice name -lif intercluster LIF -status-admin up|down` コマンドを入力してクラスタ間LIFを切り替えます。ただし、この問題を回避するには、クラスタ間 LIF と管理 LIF を別々のサブネットに設定する必要があります。

LIF	説明
データ LIF	<p>Storage Virtual Machine （ SVM ）に関連付けられた LIF で、クライアントとの通信に使用します。</p> <p>1 つのポートに複数のデータ LIF を設定できます。これらのインターフェイスは、クラスタ全体で移行またはフェイルオーバーできます。ファイアウォールポリシーを mgmt に変更すると、データ LIF を SVM 管理 LIF として使用できます。</p> <p>データ LIF は、NIS 、 LDAP 、 Active Directory 、 WINS 、および DNS の各サーバに対するセッションで使用されます。</p>

クラスタ LIF	<p>クラスタ内のノード間のクラスタ内トラフィックに使用される LIF です。クラスタ LIF は、必ずクラスタポート上に作成する必要があります。</p> <p>クラスタ LIF は、同じノードのクラスタポート間でフェイルオーバーできますが、リモートノードに移行またはフェイルオーバーすることはできません。新しいノードがクラスタに追加されると、IP アドレスは自動的に生成されます。ただし、クラスタ LIF に IP アドレスを手動で割り当てる場合は、新しい IP アドレスが既存のクラスタ LIF と同じサブネット範囲に含まれるようにする必要があります。</p>
クラスタ管理 LIF	<p>クラスタ全体に対する単一の管理インターフェイスを提供する LIF です。</p> <p>クラスタ管理 LIF は、クラスタ内の任意のノードにフェイルオーバーできます。クラスタポートまたはクラスタ間ポートにはフェイルオーバーできません</p>
クラスタ間 LIF	<p>クラスタ間の通信、バックアップ、およびレプリケーションに使用される LIF です。クラスタピア関係を確立する前に、クラスタ内の各ノードにクラスタ間 LIF を作成する必要があります。</p> <p>これらの LIF は、同じノードのポートにのみフェイルオーバーできます。クラスタ内の別のノードに移行またはフェイルオーバーすることはできません。</p>
ノード管理 LIF	<p>クラスタ内の特定のノードを管理するために専用の IP アドレスを提供する LIF です。クラスタの作成時またはクラスタへのノードの追加時に作成されます。これらの LIF は、クラスタからノードにアクセスできなくなった場合など、システムのメンテナンスに使用されます。</p>
VIP LIF	<p>VIP LIF は、VIP ポートで作成される任意のデータ LIF です。詳細については、<a href="#">を参照してください "仮想 IP（VIP）LIF を設定する"</a>。</p>

## LIFとサービスポリシー（ONTAP 9.6以降）

LIFのロールやファイアウォールポリシーの代わりに、LIFでサポートされるトラフィックの種類を決定するサービスポリシーをLIFに割り当てることができます。サービスポリシーは、LIFでサポートされる一連のネットワークサービスを定義します。ONTAPには、LIFに関連付けることができる一連の組み込みのサービスポリシーが用意されています。

サービスポリシーとその詳細を表示するには、次のコマンドを使用します。

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

特定のサービスにバインドされていない機能では、システム定義の動作を使用してアウトバウンド接続用のLIFが選択されます。

### システム SVM のサービスポリシー

管理 SVM とすべてのシステム SVM には、管理 LIF とクラスタ間 LIF を含む、その SVM の LIF に使用できるサービスポリシーが含まれています。これらのポリシーは、IPspace の作成時にシステムによって自動的に作成されます。

次の表に、ONTAP 9.12.1以降のシステムSVMのLIFの組み込みのポリシーを示します。その他のリリースでは、次のコマンドを使用してサービスポリシーとその詳細を表示します。



network interface service-policy show

ポリシー	含まれるサービス	同等のロール	説明
デフォルト - intercluster	インタークラスタコア、管理 - https : //	クラスタ間	クラスタ間トラフィックを処理する LIF で使用されます。 注：サービス intercluster-core は、net-intercluster サービスポリシーという名前で ONTAP 9.5 から提供されています。
default-route-announce	management-bgp	-	BGPピア接続を処理するLIFで使用されます。 注：ONTAP 9.5では、net-route-announce サービスポリシーという名前で提供されています。
default-management	management-core、management-https、management-http、management-ssh、management-autosupport、management-ems、management-dns-client、management-ad-client、management-ldap-client、management-nis-client、management-ntp-client、management-log-forwarding	ノード管理、またはクラスタ管理	システムを対象としたこの管理ポリシーを使用して、システムSVMが所有するノードとクラスタを対象とした管理LIFを作成します。これらのLIFは、DNS、AD、LDAP、またはNISサーバへのアウトバウンド接続や、システム全体に代わって実行されるアプリケーションをサポートするための追加の接続に使用できます。 ONTAP 9.12.1以降では、を使用できます management-log-forwarding 監査ログをリモートsyslogサーバに転送するために使用するLIFを制御するサービス。

次の表は、ONTAP 9.11.1以降、システムSVM上でLIFが使用できるサービスを示しています。

サービス	フェイルオーバーの制限	説明
intercluster-core	home-node-only	中核となるクラスタ間サービス
管理コア	-	中核となる管理サービス
management-ssh	-	SSH 管理アクセス用のサービス
Management - http : //	-	HTTP管理アクセス用のサービス
管理 - HTTPS	-	HTTPS管理アクセス用のサービス
management-autosupport	-	AutoSupport ペイロードの送信に関連するサービス

management-bgp	home-port - Only (ホームポートのみ)	BGP ピアのやり取りに関連するサービス
backup-ndmp-control の実行	-	NDMP バックアップ制御のためのサービス
管理 - EMS	-	管理メッセージアクセス用のサービス
management-ntp-client	-	ONTAP 9.10.1で導入されました。 NTP クライアントアクセス用のサービス。
management-ntp-server	-	ONTAP 9.11.1で導入されました。 NTP サーバ管理アクセス用のサービス
管理 - portmap	-	portmap 管理用のサービス
management-srsh -server です	-	rsh サーバ管理のためのサービス
management-snmp-server	-	SNMP サーバ管理用のサービス
management-telnet-server	-	Telnet サーバ管理用のサービス
管理-ログ転送	-	ONTAP 9.12.1で導入されました。 監査ログ転送用のサービス

#### データ **SVM** のサービスポリシー

すべてのデータ SVM に、その SVM の LIF で使用できるサービスポリシーが含まれています。

次の表に、ONTAP 9.11.1以降の、データSVMのLIFの組み込みのポリシーを示します。その他のリリースでは、次のコマンドを使用してサービスポリシーとその詳細を表示します。

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

ポリシー	含まれるサービス	同等のデータプロトコル	説明
------	----------	-------------	----

default-management	management-https、management-http、management-ssh、management-dns-client、management-ad-client、management-ldap-client、management-nis-client	なし	このSVMを対象とした管理ポリシーを使用して、データSVMが所有するSVM管理LIFを作成します。これらのLIFを使用して、SVM管理者にSSHまたはHTTPSアクセスを提供できます。これらのLIFは、必要に応じて、外部DNSサーバ、ADサーバ、LDAPサーバ、またはNISサーバへのアウトバウンド接続に使用できます。
default-data-blocks (デフォルトデータブロック)	データコア、データ - iSCSI	iSCSI	ブロックベースのSANデータトラフィックを処理するLIFで使用されます。ONTAP 9.10.1以降、「default-data-blocks」ポリシーは廃止されました。代わりに「default-data-iscsi」サービスポリシーを使用します。
default-data-files の形式で指定します	data-filc-client、data-dns-server、data-flexcache、data-cifs、data-nfs、management-dns-client、management-ad-client、management-ldap-client、management-nis-client	NFS、CIFS、fcache	default-data-filesポリシーを使用して、ファイルベースのデータプロトコルをサポートするNAS LIFを作成します。SVMにLIFが1つしかないことがあるため、このポリシーでは、外部のDNS、AD、LDAP、またはNISサーバへのアウトバウンド接続にLIFを使用することができます。これらの接続で管理LIFのみを使用する場合は、このポリシーからこれらのサービスを削除できます。
default-data-iscsi	データコア、データ - iSCSI	iSCSI	iSCSIデータトラフィックを処理するLIFで使用されます。
default-data-nvme-tcpです	データコア、データNVMe - TCP	nvme-tcpが表示されます	NVMe/FCデータトラフィックを処理するLIFで使用します。

次の表に、データSVMで使用できる各サービスをONTAP 9.11.1以降でLIFのフェイルオーバーポリシーに適用される制限とともに示します。

サービス	フェイルオーバーの制限	説明
management-ssh	-	SSH 管理アクセス用のサービス
Management - http : //	-	ONTAP 9.10.1で導入 HTTP管理アクセス用のサービス
管理 - HTTPS	-	HTTPS管理アクセス用のサービス
管理 - portmap	-	portmap 管理アクセス用のサービス

management-snmp-server	-	ONTAP 9.10.1で導入 SNMPサーバ管理アクセス用のサービス
データコア	-	コアデータサービス
データ NFS	-	NFS データサービス
データ - CIFS	-	CIFSデータサービス
データ FlexCache	-	FlexCache データサービス
データ - iSCSI	home-port - Only （ホームポートのみ）	iSCSI データサービス
backup-ndmp-control の実行	-	ONTAP 9.10.1で導入 Backup NDMP はデータサービスを制御します
data-dns-server	-	ONTAP 9.10.1で導入 DNS サーバデータサービス
data-fpolicy-client	-	ファイルスクリーニングポリシーデータサービス
data-nvme-tcp を選択します	home-port - Only （ホームポートのみ）	ONTAP 9.10.1で導入 NVMe TCP データサービス
data-s3-server のように指定します	-	Simple Storage Service （ S3 ）サーバデータサービス

データ SVM の LIF に対するサービスポリシーの割り当てについて、次の点に注意してください。

- データサービスのリストを指定してデータ SVM を作成した場合、その SVM には、指定したサービスを使用して組み込みの「 default-data-files 」サービスポリシーと「 default-data-blocks 」サービスポリシーが作成されます。
- データサービスのリストを指定せずにデータ SVM を作成した場合、その SVM にはデフォルトのデータサービスのリストを使用して組み込みの「 default-data-files 」サービスポリシーと「 default-data-blocks 」サービスポリシーが作成されます。

デフォルトのデータサービスのリストには、iSCSI、NFS、NVMe、SMB、FlexCache の各サービスが含まれます。

- データプロトコルのリストを指定して LIF を作成した場合、指定したデータプロトコルと同等のサービスポリシーが LIF に割り当てられます。
- 同等のサービスポリシーが存在しない場合は、カスタムサービスポリシーが作成されます。
- サービスポリシーやデータプロトコルのリストを指定せずに LIF を作成した場合、デフォルトで default-data-files サービスポリシーが LIF に割り当てられます。

## データコアサービス

コアサービスでは、データロールが割り当てられた LIF を使用していたコンポーネントを、LIF のロールではなくサービスポリシーを使用して LIF を管理するようにアップグレードされたクラスタで想定どおりに機能させることができます（ONTAP 9.6 では廃止）。

コアをサービスとして指定してもファイアウォール内のポートは開かれませんが、データ SVM のサービスポリシーにはこのサービスを含める必要があります。たとえば、default-data-files サービスポリシーには、デフォルトで次のサービスが含まれています。

- データコア
- データ NFS
- データ - CIFS
- データ FlexCache

LIF を使用するすべてのアプリケーションが想定どおりに機能するように、コアサービスをポリシーに含めます。ただし、必要に応じて、他の 3 つのサービスは削除できます。

## クライアント側の LIF サービス

ONTAP 9.10.1 以降の ONTAP は、複数のアプリケーションにクライアント側の LIF サービスを提供します。これらのサービスは、各アプリケーションの代わりにアウトバウンド接続に使用する LIF を制御します。

管理者は、次の新しいサービスを使用して、特定のアプリケーションのソースアドレスとして使用する LIF を制御できます。

サービス	SVM の制限事項	説明
management-ad-client	-	ONTAP 9.11.1以降では、ONTAP は外部ADサーバへのアウトバウンド接続にActive Directoryクライアントサービスを提供します。
management-dns-client	-	ONTAP 9.11.1以降では、ONTAP は外部DNSサーバへのアウトバウンド接続にDNSクライアントサービスを提供します。
management-ldap-clientの場合	-	ONTAP 9.11.1以降では、ONTAPが外部LDAPサーバへのアウトバウンド接続にLDAPクライアントサービスを提供しています。
management-nis-client	-	ONTAP 9.11.1以降では、ONTAPは外部のNISサーバへのアウトバウンド接続用にNISクライアントサービスを提供しています。
management-ntp-client	システムのみ	ONTAP 9.10.1 以降の ONTAP は、外部 NTP サーバへのアウトバウンド接続に NTP クライアントサービスを提供します。

data-fpolicy-client	データのみ	ONTAP 9.8 以降では、ONTAP はアウトバウンド FPolicy 接続のクライアントサービスを提供します。
---------------------	-------	--

新しいサービスはそれぞれ一部の組み込みのサービスポリシーに自動的に含まれますが、管理者はそれらのサービスを組み込みのポリシーから削除するか、カスタムポリシーに追加して、各アプリケーションの代わりにアウトバウンド接続に使用する LIF を制御できます。

### LIFのロール（ONTAP 9.5以前）

LIF の特性はロールごとに異なります。LIF のロールにより、インターフェイスでサポートされるトラフィックの種類のほか、適用されるフェイルオーバールール、適用されるファイアウォールの制限、セキュリティ、ロードバランシング、ルーティングの方法が決まります。LIF のロールには、cluster、cluster management、data、intercluster、node management、undef（未定義）です。undef ロールは、BGP LIF に使用されます。

ONTAP 9.6 以降では、LIF のロールは廃止されています。ロールの代わりに LIF のサービスポリシーを指定する必要があります。サービスポリシーを使用して LIF を作成する場合、LIF のロールを指定する必要はありません。

### LIF セキュリティ

	データ LIF	クラスタ LIF	ノード管理 LIF	クラスタ管理 LIF	クラスタ間 LIF
プライベート IP サブネットが必要かどうか	いいえ	はい。	いいえ	いいえ	いいえ
セキュアなネットワークが必要	いいえ	はい。	いいえ	いいえ	はい。
デフォルトのファイアウォールポリシー	非常に厳しい	完全にオープン	中	中	非常に厳しい
ファイアウォールをカスタマイズ可能	はい。	いいえ	はい。	はい。	はい。

### LIF フェイルオーバー

	データ LIF	クラスタ LIF	ノード管理 LIF	クラスタ管理 LIF	クラスタ間 LIF
--	---------	----------	-----------	------------	-----------

デフォルトの動作です	LIF のホームノードおよび SFO 以外のパートナーノードと同じフェイルオーバーグループ内のポートにフェイルオーバーします	LIF のホームノードと同じフェイルオーバーグループ内のポートにフェイルオーバーします	LIF のホームノードと同じフェイルオーバーグループ内のポートにフェイルオーバーします	同じフェイルオーバーグループ内の任意のポート	LIF のホームノードと同じフェイルオーバーグループ内のポートにフェイルオーバーします
カスタマイズ可能	はい。	いいえ	はい。	はい。	はい。

#### LIF のルーティング

	データ LIF	クラスタ LIF	ノード管理 LIF	クラスタ管理 LIF	クラスタ間 LIF
デフォルトルートが必要になる状況	クライアントまたはドメインコントローラが別の IP サブネットにある場合	なし	いずれかのプライマリトラフィックタイプで、別の IP サブネットへのアクセスが必要な場合	管理者が別の IP サブネットから接続している場合	他のクラスタ間 LIF が別の IP サブネットにある場合
特定の IP サブネットへの静的ルートが必要になる状況	まれです	なし	まれです	まれです	別のクラスタのノードのクラスタ間 LIF が異なる IP サブネットにある場合
特定のサーバへの静的ホストルートが必要になる状況	ノード管理 LIF の欄に記載されたいずれかのトラフィックタイプを使用するには、ノード管理 LIF ではなく、データ LIF を経由します。これには、対応するファイアウォールの変更が必要です。	なし	まれです	まれです	まれです

#### LIF のリバランシング

	データ LIF	クラスタ LIF	ノード管理 LIF	クラスタ管理 LIF	クラスタ間 LIF
DNS : DNS サーバとして使用	はい。	いいえ	いいえ	いいえ	いいえ

DNS：ゾーンとしてエクスポート	はい。	いいえ	いいえ	いいえ	いいえ
------------------	-----	-----	-----	-----	-----

## LIF のプライマリトラフィックタイプ

	データ LIF	クラスタ LIF	ノード管理 LIF	クラスタ管理 LIF	クラスタ間 LIF
主なトラフィックタイプ	NFS サーバ、CIFS サーバ、NIS クライアント、Active Directory、LDAP、WINS、DNS クライアントおよびサーバ、iSCSI および FC サーバ	クラスタ内	SSH サーバ、HTTPS サーバ、NTP クライアント、SNMP、AutoSupport クライアント、DNS クライアント、ソフトウェアアップデートのロード	SSH サーバ、HTTPS サーバ	クラスタ間レプリケーション

## LIFの管理

### LIF のサービスポリシーを設定

LIF のサービスポリシーを設定して、LIF を使用する単一のサービスまたは一連のサービスを指定できます。

### LIF のサービスポリシーを作成

LIF のサービスポリシーを作成することができます。1 つ以上の LIF にサービスポリシーを割り当てることで、1 つまたは一連のサービスのトラフィックの処理を LIF に許可することができます。

を実行するにはadvanced権限が必要です `network interface service-policy create` コマンドを実行します

### このタスクについて

データ SVM とシステム SVM の両方でデータトラフィックと管理トラフィックの管理に使用できる組み込みのサービスとサービスポリシーを用意しています。ほとんどのユースケースでは、カスタムサービスポリシーを作成するのではなく、組み込みのサービスポリシーを使用して対応できます。

これらの組み込みのサービスポリシーは必要に応じて変更できます。

### 手順

1. クラスタで使用可能なサービスを表示します。

```
network interface service show
```

サービスとは、LIF がアクセスするアプリケーション、およびクラスタで提供されるアプリケーションです。各サービスには、アプリケーションがリスンしている TCP ポートと UDP ポートが 0 個以上含まれます。



次のデータサービスと管理サービスも利用できます。

```
cluster1::> network interface service show
```

Service	Protocol:Ports
-----	-----
cluster-core	-
data-cifs	-
data-core	-
data-flexcache	-
data-iscsi	-
data-nfs	-
intercluster-core	tcp:11104-11105
management-autosupport	-
management-bgp	tcp:179
management-core	-
management-https	tcp:443
management-ssh	tcp:22
12 entries were displayed.	

2. クラスタに存在するサービスポリシーを表示します。

```
cluster1::> network interface service-policy show
```

Vserver	Policy	Service: Allowed Addresses
-----		
-----		
cluster1		
	default-intercluster	intercluster-core: 0.0.0.0/0 management-https: 0.0.0.0/0
	default-management	management-core: 0.0.0.0/0 management-autosupport: 0.0.0.0/0 management-ssh: 0.0.0.0/0 management-https: 0.0.0.0/0
	default-route-announce	management-bgp: 0.0.0.0/0
Cluster		
	default-cluster	cluster-core: 0.0.0.0/0
vs0		
	default-data-blocks	data-core: 0.0.0.0/0 data-iscsi: 0.0.0.0/0
	default-data-files	data-core: 0.0.0.0/0 data-nfs: 0.0.0.0/0 data-cifs: 0.0.0.0/0 data-flexcache: 0.0.0.0/0
	default-management	data-core: 0.0.0.0/0 management-ssh: 0.0.0.0/0 management-https: 0.0.0.0/0

```
7 entries were displayed.
```

### 3. サービスポリシーを作成します。

```
cluster1::> set -privilege advanced
```

```
Warning: These advanced commands are potentially dangerous; use them  
only when directed to do so by technical support.
```

```
Do you wish to continue? (y or n): y
```

```
cluster1::> network interface service-policy create -vserver <svm_name>  
-policy <service_policy_name> -services <service_name> -allowed  
-addresses <IP_address/mask,...>
```

- 「SERVICE\_NAME」は、ポリシーに含めるサービスのリストを指定します。
- 「ip\_address /mask」には、サービスポリシー内のサービスへのアクセスを許可するアドレスのサブネットマスクのリストを指定します。デフォルトでは、指定されたすべてのサービスがデフォルトの許可アドレスリスト 0.0.0.0/0 で追加され、すべてのサブネットからのトラフィックが許可されます。デフォルト以外の許可アドレスリストを指定した場合、そのポリシーを使用する LIF は、指定したマスクと一致しないソースアドレスを使用するすべての要求をブロックするように設定されます。

次の例は、\_nfs\_or\_SMB\_servicesを含むSVM用のデータサービスポリシーsvm1\_data\_policy\_\_を作成する方法を示しています。

```
cluster1::> set -privilege advanced
Warning: These advanced commands are potentially dangerous; use them
only when directed to do so by technical support.
Do you wish to continue? (y or n): y

cluster1::> network interface service-policy create -vserver svm1
-policy svm1_data_policy -services data-nfs,data-cifs,data-core
```

次の例は、クラスタ間サービスポリシーを作成する方法を示しています。

```
cluster1::> set -privilege advanced
Warning: These advanced commands are potentially dangerous; use them
only when directed to do so by technical support.
Do you wish to continue? (y or n): y

cluster1::> network interface service-policy create -vserver cluster1
-policy intercluster1 -services intercluster-core
```

#### 4. サービスポリシーが作成されたことを確認します。

```
cluster1::> network interface service-policy show
```

次の出力は、使用可能なサービスポリシーを示しています。

```
cluster1::> network interface service-policy show
```

Vserver	Policy	Service: Allowed Addresses
-----		
-----		
cluster1		
	default-intercluster	intercluster-core: 0.0.0.0/0 management-https: 0.0.0.0/0
	intercluster1	intercluster-core: 0.0.0.0/0
	default-management	management-core: 0.0.0.0/0 management-autosupport: 0.0.0.0/0 management-ssh: 0.0.0.0/0 management-https: 0.0.0.0/0
	default-route-announce	management-bgp: 0.0.0.0/0
Cluster		
	default-cluster	cluster-core: 0.0.0.0/0
vs0		
	default-data-blocks	data-core: 0.0.0.0/0 data-iscsi: 0.0.0.0/0
	default-data-files	data-core: 0.0.0.0/0 data-nfs: 0.0.0.0/0 data-cifs: 0.0.0.0/0 data-flexcache: 0.0.0.0/0
	default-management	data-core: 0.0.0.0/0 management-ssh: 0.0.0.0/0 management-https: 0.0.0.0/0
	svm1_data_policy	data-core: 0.0.0.0/0 data-nfs: 0.0.0.0/0 data-cifs: 0.0.0.0/0

```
9 entries were displayed.
```

完了後

LIF の作成時または既存の LIF の変更時にサービスポリシーを割り当てます。

LIF にサービスポリシーを割り当てます

LIF の作成時または変更時に、LIF にサービスポリシーを割り当てることができます。サービスポリシーは、LIF で使用できる一連のサービスを定義します。

このタスクについて

管理 SVM とデータ SVM の LIF にサービスポリシーを割り当てることができます。

ステップ

LIF にサービスポリシーをいつ割り当てるかに応じて、次のいずれかを実行します。

実行する作業	サービスポリシーを割り当てています ...
LIF を作成する	<code>network interface create -vserver SVM_name -lif &lt;LIF_name&gt; -home-node &lt;node_name&gt; -home-port &lt;port_name&gt; { ( -address &lt;IP_address&gt; -netmask &lt;IP_address&gt; ) -subnet-name &lt;subnet_name&gt; } -service-policy &lt;service_policy_name&gt;</code>
LIF の変更	<code>network interface modify -vserver &lt;svm_name&gt; -lif &lt;lif_name&gt; -service -policy &lt;service_policy_name&gt;</code>

LIF のサービスポリシーを指定する際に、LIF のデータプロトコルとロールを指定する必要はありません。ロールとデータプロトコルを指定して LIF を作成することもできます。



サービスポリシーは、サービスポリシーの作成時に指定した同じ SVM に含まれる LIF でのみ使用できます。

例

次の例は、LIF のサービスポリシーを default-management に変更する方法を示しています。

```
cluster1::> network interface modify -vserver cluster1 -lif lif1 -service -policy default-management
```

LIF のサービスポリシーを管理するためのコマンド

を使用します `network interface service-policy` LIFのサービスポリシーを管理するコマンド。

作業を開始する前に

アクティブなSnapMirror関係にあるLIFのサービスポリシーを変更すると、レプリケーションスケジュールが中断されます。LIFをクラスタ間から非クラスタ間（またはその逆）に変換した場合、変更はピアクラスタにレプリケートされません。LIFサービスポリシーの変更後にピアクラスタを更新するには、まず `snapmirror abort` 操作Then [レプリケーション関係を再同期する](#)。

状況	使用するコマンド
サービスポリシーを作成する（advanced権限が必要）	<code>network interface service-policy create</code>

状況	使用するコマンド
既存のサービスポリシーにサービスエントリを追加する（advanced権限が必要）	<code>network interface service-policy add-service</code>
既存のサービスポリシーのクローンを作成する（advanced権限が必要）	<code>network interface service-policy clone</code>
既存のサービスポリシーのサービスエントリを変更する（advanced権限が必要）	<code>network interface service-policy modify-service</code>
既存のサービスポリシーからサービスエントリを削除する（advanced権限が必要）	<code>network interface service-policy remove-service</code>
既存のサービスポリシーの名前を変更する（advanced権限が必要）	<code>network interface service-policy rename</code>
既存のサービスポリシーを削除する（advanced権限が必要）	<code>network interface service-policy delete</code>
組み込みのサービスポリシーを元の状態にリストアする（advanced権限が必要）	<code>network interface service-policy restore-defaults</code>
既存のサービスポリシーを表示します	<code>network interface service-policy show</code>

## LIFを作成する（ネットワークインターフェイス）

SVM は、1 つ以上のネットワーク論理インターフェイス（LIF）を通じてクライアントにデータを提供します。データへのアクセスに使用するポートに LIF を作成する必要があります。LIF（ネットワークインターフェイス）は、物理ポートまたは論理ポートに関連付けられた IP アドレスです。コンポーネントに障害が発生しても、LIF は別の物理ポートにフェイルオーバーまたは移行できるため、引き続きネットワークと通信できます。

### ベストプラクティス

ONTAPに接続されたスイッチポートは、LIFの移行時の遅延を軽減するために、スパニングツリーエッジポートとして設定する必要があります。

### 作業を開始する前に

- このタスクを実行するには、クラスタ管理者である必要があります。
- 基盤となる物理または論理ネットワークポートの管理ステータスが up に設定されている必要があります。
- サブネット名を使用して LIF の IP アドレスとネットワークマスク値を割り当てる場合は、そのサブネットがすでに存在している必要があります。

サブネットには、同じレイヤ 3 サブネットに属する IP アドレスのプールが含まれています。作成するに

は、System Managerまたははを使用します `network subnet create` コマンドを実行します

- LIF で処理するトラフィックのタイプを指定するメカニズムが変更されました。ONTAP 9.5 以前では、LIF はロールを使用して処理するトラフィックのタイプを指定していました。ONTAP 9.6 以降では、サービスポリシーを使用して、処理するトラフィックのタイプを指定します。

このタスクについて

- 同じ LIF に NAS プロトコルや SAN プロトコルを割り当てることはできません。

サポートされているプロトコルは、SMB、NFS、FlexCache、iSCSI、および FC です。iSCSI と FC を他のプロトコルと組み合わせることはできません。ただし、NAS プロトコルとイーサネットベースの SAN プロトコルは、同じ物理ポートで使用できます。

- SMBトラフィックを伝送するLIFを、ホームノードに自動的にリバートするように設定しないでください。Hyper-V over SMB または SQL Server over SMB でノンストップオペレーションを実現する解決策を SMB サーバでホストする場合、これは必須です。
- 同じネットワークポート上に IPv4 と IPv6 の両方の LIF を作成できます。
- DNS、NIS、LDAP、Active Directory など、SVM で使用されるすべてのネームマッピングサービスとホスト名解決サービス SVM のデータトラフィックを処理する少なくとも 1 つの LIF から到達可能である必要があります。
- ノード間のクラスタ内トラフィックを処理する LIF は、管理トラフィックを処理する LIF またはデータトラフィックを処理する LIF と同じサブネット上には存在しないようにしてください。
- 有効なフェイルオーバーターゲットのない LIF を作成すると、警告メッセージが表示されます。
- クラスタ内のLIFの数が多い場合は、クラスタでサポートされるLIFの容量を確認できます。
  - System Manager：ONTAP 9.12.0以降では、ネットワークインターフェイスグリッドのスループットを表示します。
  - CLI：を使用します `network interface capacity show` コマンドとを使用して、各ノードでサポートされるLIFの容量を確認します `network interface capacity details show` コマンド (advanced権限レベル)。
- ONTAP 9.7 以降では、同じサブネット内に SVM 用の他の LIF がすでに存在する場合、LIF のホームポートを指定する必要はありません。ONTAP は、同じサブネットにすでに設定されている他の LIF と同じブロードキャストドメインにある指定したホームノード上のランダムなポートを自動的に選択します。

ONTAP 9.4 以降では、FC-NVMe がサポートされます。FC-NVMe LIF を作成する場合は、次の点に注意してください。

- LIF を作成する FC アダプタで NVMe プロトコルがサポートされている必要があります。
- データ LIF で使用できるデータプロトコルは FC-NVMe のみです。
- SAN をサポートする Storage Virtual Machine (SVM) ごとに、管理トラフィックを処理する LIF を 1 つ 設定する必要があります。
- NVMe の LIF とネームスペースは、同じノードでホストする必要があります。
- データトラフィックを処理する NVMe LIF は SVM ごとに 1 つだけ設定できます。
- サブネットを使用してネットワークインターフェイスを作成すると、選択したサブネットから使用可能な IP アドレスが ONTAP によって自動的に選択され、ネットワークインターフェイスに割り当てられます。複数のサブネットがある場合はサブネットを変更できますが、IP アドレスを変更することはできません。

- ネットワークインターフェイスに対してSVMを作成（追加）するときに、既存のサブネットの範囲内のIPアドレスを指定することはできません。サブネットの競合エラーが表示されます。この問題は、SVM設定またはクラスタ設定でクラスタ間ネットワークインターフェイスを作成または変更するなど、ネットワークインターフェイスの他のワークフローで実行します。
- ONTAP 9.10.1以降の `network interface` CLI コマンドにはが含まれています `-rdma-protocols NFS over RDMA` 構成用のパラメータ。ONTAP 9.12.1以降では、System ManagerでRDMA構成を使用するNFS用ネットワークインターフェイスの作成がサポートされています。詳細については、[を参照してください NFS over RDMA用にLIFを設定します](#)。
- ONTAP 9.11.1以降では、オールフラッシュSANアレイ（ASA）プラットフォームでiSCSI LIFの自動フェイルオーバーを使用できます。

iSCSI LIFのフェイルオーバーは自動的に有効になります（フェイルオーバーポリシーはに設定されます）`sfo-partner-only auto-revert`の値はに設定されています `true`）。指定したSVMにiSCSI LIFが存在しない場合、または指定したSVMの既存のすべてのiSCSI LIFですでにiSCSI LIFのフェイルオーバーが有効になっている場合。

ONTAP 9.11.1以降にアップグレードしたあとに、iSCSI LIFのフェイルオーバー機能が有効になっていないSVMに既存のiSCSI LIFがある場合に、同じSVMに新しいiSCSI LIFを作成すると、新しいiSCSI LIFでも同じフェイルオーバーポリシーが適用されます (`disabled`) を作成します。

#### "ASA プラットフォームのiSCSI LIFのフェイルオーバー"

ONTAP 9.7 以降では、少なくとも 1 つの LIF が同じサブネットにすでに存在するかぎり、ONTAP によって LIF のホームポートが自動的に選択されます。ONTAP は、そのサブネット内の他の LIF と同じブロードキャストドメイン内のホームポートを選択します。ホームポートは指定できますが、指定した IPspace のサブネットにまだ LIF がない場合を除き、指定する必要はありません。

ONTAP 9.12.0以降では、使用するインターフェイスに応じて次の手順 が使用されます。System ManagerまたはCLI：



## System Manager の略

- System Managerを使用して、ネットワークインターフェイスを追加\*

### 手順

1. Network > Overview > Network Interfaces \*を選択します。
2. 選択するオプション **+ Add**。
3. 次のいずれかのインターフェイスロールを選択します。
  - a. データ
  - b. クラスタ間
  - c. SVM管理
4. プロトコルを選択します。
  - a. SMB / CIFSとNFS
  - b. iSCSI
  - c. FC
  - d. NVMe/FC
  - e. NVMe/FC
5. LIFに名前を付けるか、以前の選択内容から生成された名前をそのまま使用します。
6. ホームノードを受け入れるか、ドロップダウンを使用して選択します。
7. 選択したSVMのIPspaceに少なくとも1つのサブネットが設定されている場合は、サブネットのドロップダウンが表示されます。
  - a. サブネットを選択した場合は、ドロップダウンから選択します。
  - b. サブネットを指定せずに続行すると、ブロードキャストドメインのドロップダウンが表示されます。
    - i. IPアドレスを指定します。IPアドレスが使用中の場合は、警告メッセージが表示されます。
    - ii. サブネットマスクを指定します。
8. ブロードキャストドメインからホームポートを自動的に選択するか（推奨）、ドロップダウンメニューからホームポートを選択します。ホームポート制御は、ブロードキャストドメインまたはサブネットの選択に基づいて表示されます。
9. ネットワークインターフェイスを保存します。

### CLI の使用

- CLIを使用してLIFを作成してください\*

### 手順

1. LIF に使用するブロードキャストドメインのポートを決定します。

```
network port broadcast-domain show -ipspace ipspace1
```

IPspace	Broadcast			Update
Name	Domain name	MTU	Port List	Status Details
ipspacel	default	1500		
			node1:e0d	complete
			node1:e0e	complete
			node2:e0d	complete
			node2:e0e	complete

2. LIF に使用するサブネットに未使用の IP アドレスが十分にあることを確認します。

```
network subnet show -ipspacel ipspacel
```

3. データへのアクセスに使用するポートに 1 つ以上の LIF を作成します。

```
network interface create -vserver _SVM_name_ -lif _lif_name_
-service-policy _service_policy_name_ -home-node _node_name_ -home
-port port_name {-address _IP_address_ - netmask _Netmask_value_ |
-subnet-name _subnet_name_} -firewall- policy _policy_ -auto-revert
{true|false}
```

- -home-node は、の実行時にLIFが戻るノードです network interface revert LIFに対して コマンドを実行します。

auto-revert オプションを使用して、LIF をホームノードおよびホームポートに自動的にリポートするかどうかを指定することもできます。

- -home-port は、の実行時にLIFが戻る物理ポートまたは論理ポートです network interface revert LIFに対してコマンドを実行します。
- でIPアドレスを指定できます -address および -netmask オプションを使用するか、サブネットからの割り当てを有効にするには、-subnet\_name オプション
- サブネットを使用して IP アドレスとネットワークマスクを指定した場合、サブネットにゲートウェイが定義されていると、そのサブネットを使用して LIF を作成するときにゲートウェイへのデフォルトルートが SVM に自動的に追加されます。
- サブネットを使用せずに手動で IP アドレスを割り当てると、クライアントまたはドメインコントローラが別の IP サブネットにある場合にゲートウェイへのデフォルトルートの設定が必要になることがあります。。 network route create のマニュアルページには、SVM内での静的ルートの作成に関する情報が記載されています。
- -auto-revert 起動時、管理データベースのステータスが変ったとき、ネットワーク接続が確立されたときなどの状況で、データLIFがホームノードに自動的にリポートされるかどうかを指定できます。デフォルト設定はです false`に設定することもできます `true` 環境内のネットワーク管理ポリシーによって異なります。
- -service-policy ONTAP 9.5以降では、を使用してLIFのサービスポリシーを割り当てることができます -service-policy オプション  
LIF にサービスポリシーを指定すると、そのポリシーを使用して LIF のデフォルトロール、フェ

イルオーバーポリシー、データプロトコルのリストが作成されます。ONTAP 9.5 では、クラスター間および BGP ピアのサービスについてのみサービスポリシーがサポートされます。ONTAP 9.6 では、複数のデータサービスおよび管理サービスに対してサービスポリシーを作成できます。

- ° -data-protocol FCPまたはNVMe/FCプロトコルをサポートするLIFを作成できます。IP LIFを作成する場合、このオプションは必要ありません。

4. オプション：-addressオプションでIPv6アドレスを割り当てます。

- a. network ndp prefix show コマンドを使用し、各種インターフェイスで学習された RA プレフィックスのリストを表示します。

。 network ndp prefix show コマンドはadvanced権限レベルで使用できます。

- b. の形式を使用します prefix:: IPv6アドレスを手動で作成します。

prefix は、さまざまなインターフェイスで学習されたプレフィックスです。

を導出するため `id` で、ランダムな64ビット16進数を選択します。

5. LIF インターフェイスの設定が正しいことを確認します。

```
network interface show -vserver vs1
```

Vserver	Logical Interface	Status Admin/Oper	Network Address/Mask	Current Node	Current Port	Is
Home						
vs1	lif1	up/up	10.0.0.128/24	node1	e0d	true

6. フェイルオーバーグループの設定が適切であることを確認します。

```
network interface show -failover -vserver vs1
```

Vserver	Logical interface	Home Node:Port	Failover Policy	Failover Group
vs1	lif1	node1:e0d	system-defined	ipspace1

Failover Targets: node1:e0d, node1:e0e, node2:e0d, node2:e0e

7. 設定した IP アドレスに到達できることを確認します。

対象	使用
----	----

IPv4 アドレス	ネットワーク ping
IPv6アドレス	ネットワーク ping6

#### 例

次のコマンドでは、を使用してLIFを作成し、IPアドレスとネットワークマスク値を指定します  
-address および -netmask パラメータ：

```
network interface create -vserver vs1.example.com -lif datalif1
-service-policy default-data-files -home-node node-4 -home-port elc
-address 192.0.2.145 -netmask 255.255.255.0 -auto-revert true
```

次のコマンドは、LIF を作成し、IP アドレスとネットワークマスク値を指定したサブネット（`client1_sub`）から割り当てています。

```
network interface create -vserver vs3.example.com -lif datalif3
-service-policy default-data-files -home-node node-3 -home-port elc
-subnet-name client1_sub - auto-revert true
```

次のコマンドでは、NVMe/FC LIFを作成し、を指定します `nvme-fc` データプロトコル：

```
network interface create -vserver vs1.example.com -lif datalif1 -data
-protocol nvme-fc -home-node node-4 -home-port lc -address 192.0.2.145
-netmask 255.255.255.0 -auto-revert true
```

## LIF を変更する

LIF の属性は変更することができます。これには、ホームノードや現在のノード、管理ステータス、IP アドレス、ネットマスク、フェイルオーバーポリシー、ファイアウォールポリシー、およびサービスポリシーLIF のアドレスファミリーを IPv4 から IPv6 に変更することもできます。

#### このタスクについて

- LIF の管理ステータスを down に変更すると、再び up に戻るまで、現行の NFSv4 ロックが維持されたままになります。

ロックされたファイルに他の LIF がアクセスしようとしたときにロックの競合が発生するのを防ぐには、LIF の管理ステータスを down に設定する前に、NFSv4 クライアントを別の LIF に移動する必要があります。

- FC LIF で使用されるデータプロトコルは変更できません。ただし、サービスポリシーに割り当てられているサービスを変更したり、IP LIF に割り当てられているサービスポリシーを変更したりすることはできません。

FC LIF で使用されるデータプロトコルを変更するには、LIF を削除して作成し直す必要があります。IP

LIF にサービスポリシーを変更するには、更新が短時間停止します。

- ノードを対象とした管理 LIF のホームノードや現在のノードを変更することはできません。
- LIF の IP アドレスとネットワークマスク値を変更するためにサブネットを使用すると、指定したサブネットから IP アドレスが割り当てられます。LIF の以前の IP アドレスが別のサブネットから割り当てられた場合は、そのサブネットに IP アドレスが返されます。
- LIF のアドレスファミリーを IPv4 から IPv6 に変更するには、IPv6 アドレスのコロン表記を使用して、に新しい値を追加する必要があります `-netmask-length` パラメータ
- 自動構成されたリンクローカル IPv6 アドレスは変更できません。
- LIF の変更によって、LIF に有効なフェイルオーバーターゲットがなくなる場合は警告メッセージが表示されます。

有効なフェイルオーバーターゲットのない LIF がフェイルオーバーしようとする、システムが停止する可能性があります。

- ONTAP 9.5 以降では、LIF に関連付けられているサービスポリシーを変更できます。

ONTAP 9.5 では、クラスタ間および BGP ピアのサービスについてのみサービスポリシーがサポートされます。ONTAP 9.6 では、複数のデータサービスおよび管理サービスに対してサービスポリシーを作成できます。

- ONTAP 9.11.1 以降では、オールフラッシュ SAN アレイ (ASA) プラットフォームで iSCSI LIF の自動フェイルオーバーを使用できます。


既存の iSCSI LIF (9.11.1 以降へのアップグレード前に作成された LIF) の場合は、フェイルオーバーポリシーを ["iSCSI LIF の自動フェイルオーバーを有効にする"](#)。

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

**System Manager の略**

- ONTAP 9.12.0以降では、System Managerを使用してネットワークインターフェイス\*を編集できます

手順

1. Network > Overview > Network Interfaces \*を選択します。
2. 選択するオプション  \*>変更するネットワークインターフェイスの横にある[Edit]をクリックします。
3. ネットワークインターフェイスの設定を変更します。詳細については、を参照してください "[LIF を作成](#)"。
4. 変更を保存します。

**CLI の使用**

- LIFの変更にはCLIを使用してください\*

手順

1. を使用してLIFの属性を変更します `network interface modify` コマンドを実行します

次の例は、 `datalif2` という LIF の IP アドレスとネットワークマスクを、サブネット `client1_sub` の IP アドレスとネットワークマスク値に変更する例を示しています。

```
network interface modify -vserver vs1 -lif datalif2 -subnet-name client1_sub
```

次の例は、 LIF のサービスポリシーを変更する方法を示しています。

```
network interface modify -vserver siteA -lif node1_inter1 -service -policy example
```

2. IP アドレスに到達できることを確認します。

使用するポート	使用する方法
IPv4 アドレス	<code>network ping</code>
IPv6アドレス	<code>network ping6</code>

**LIF を移行**

ポートで障害が発生した場合やメンテナンスを行う場合など、同じノードの別のポートやクラスタ内の別のノードに LIF を移行しなければならないことがあります。LIF の移行は LIF のフェイルオーバーと似ていますが、 LIF の移行は手動で行います。 LIF のフ

フェイルオーバーは、LIF の現在のネットワークポートのリンク障害に対応して LIF を自動的に移行する機能です。

作業を開始する前に

- LIF のフェイルオーバーグループを設定しておく必要があります。
- デスティネーションのノードおよびポートが動作していて、ソースポートと同じネットワークにアクセスできる必要があります。

このタスクについて

- BGP LIF はホームポートに配置され、他のノードやポートに移行することはできません。
- ノードから NIC を削除する前に、NIC に属しているポートでホストされている LIF をクラスタ内の他のポートに移行する必要があります。
- クラスタ LIF を移行するコマンドは、そのクラスタ LIF がホストされているノードで実行する必要があります。
- ノードを対象とした管理 LIF、クラスタ LIF、クラスタ間 LIF など、ノードを対象とした LIF をリモートノードに移行することはできません。
- NFSv4 の LIF をノード間で移行する場合は、その LIF が新しいポートで使えるようになるまで、45 秒ほどかかります。

この問題を回避するには、NFSv4.1 を使用します。

- iSCSI LIFは、ONTAP 9.11.1以降を実行しているオールフラッシュSANアレイ（ASA）プラットフォームで移行できます。

iSCSI LIFの移行は、ホームノードまたはHAパートナーのポートに限定されます。

- ONTAPバージョン9.11.1以降を実行しているオールフラッシュSANアレイ（ASA）プラットフォームでないプラットフォームでは、ノード間でiSCSI LIFを移行することはできません。

この問題を回避するには、デスティネーションノードに iSCSI LIF を作成する必要があります。詳細はこちら ["iSCSI LIFを作成しています"](#)。

- NFS over RDMA用のLIF（ネットワークインターフェイス）を移行する場合は、デスティネーションポートがRoCEに対応していることを確認する必要があります。ONTAP 9.10.1以降を実行してCLIでLIFを移行するか、ONTAP 9.12.1を実行してSystem Managerで移行する必要があります。System ManagerでRoCE対応のデスティネーションポートを選択したら、\* RoCEポートを使用する\*の横にあるチェックボックスをオンにして、移行を正常に完了する必要があります。の詳細を確認してください ["NFS over RDMA用のLIFを設定しています"](#)。
- VMware VAAI のコピーオフロード処理は、ソース LIF またはデスティネーション LIF を移行すると失敗します。コピーオフロードについては、以下を参照してください。
  - ["NFS環境"](#)
  - ["SAN 環境"](#)

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

## System Manager の略

- System Managerを使用して、ネットワーク・インターフェイス\*を移行します

### 手順

1. Network > Overview > Network Interfaces \*を選択します。
2. 選択するオプション ⓘ \*>変更するネットワーク・インターフェイスの横にあるMigrate \*を選択します。



iSCSI LIFの場合、\*[インターフェイスの移行]\*ダイアログボックスで、HAパートナーのデスティネーションノードとポートを選択します。

iSCSI LIFを永続的に移行する場合は、チェックボックスを選択します。iSCSI LIFは完全に移行される前にオフラインにする必要があります。また、iSCSI LIFが完全に移行されたあとは、元に戻すことはできません。リバートオプションはありません。

3. [\* Migrate (移行) ] をクリックします
4. 変更を保存します。

### CLI の使用

- LIFの移行にはCLIを使用してください\*

### ステップ

特定の LIF を移行するかすべての LIF を移行するかに応じて、該当する操作を実行します。

移行する項目	入力するコマンド
特定の LIF	<code>network interface migrate</code>
ノードのすべてのデータ LIF とクラスタ管理 LIF	<code>network interface migrate-all</code>
ポートに接続していないすべての LIF です	<code>network interface migrate-all -node &lt;node&gt; -port &lt;port&gt;</code>

次の例は、という名前のLIFを移行する方法を示しています datalif1 指定します vs0 をポートに追加します e0d オン node0b :

```
network interface migrate -vserver vs0 -lif datalif1 -dest-node node0b  
-dest-port e0d
```

次の例は、現在（ローカル）のノードからすべてのデータ LIF とクラスタ管理 LIF を移行する方法を示しています。

```
network interface migrate-all -node local
```



**LIF をホームポートにリバートする**

別のポートにフェイルオーバーまたは移行された LIF を、手動または自動でホームポートにリバートできます。特定の LIF のホームポートを使用できない場合、その LIF は現在のポートにとどまり、リバートされません。

このタスクについて


- 自動リバートオプションを設定する前に LIF のホームポートの状態を up にすると、LIF はホームポートにリバートされません。
- 「auto-revert」オプションの値を true に設定しないかぎり、LIF は自動的にリバートされることはありません。
- LIF がホームポートにリバートされるように、「auto-revert」オプションを有効にしてください。

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

**System Manager の略**

- System Managerを使用して、ネットワークインターフェイスをホームポートに戻します。\*

手順

1. Network > Overview > Network Interfaces \*を選択します。
2. 選択するオプション  >変更するネットワークインターフェイスの横にある復帰。
3. ネットワークインターフェイスをホームポートに戻すには、\* Revert \*を選択します。

**CLI の使用**

- CLIを使用してLIFをホームポート\*にリバートします

ステップ

LIF をホームポートに手動または自動でリバートします。

ホームポートへの LIF のリバートの方法	入力するコマンド
手動で実行する	<code>network interface revert -vserver vservice_name -lif lif_name</code>
自動的に	<code>network interface modify -vserver vservice_name -lif lif_name -auto-revert true</code>

**ONTAP 9.8 以降：正しく設定されていないクラスタ LIF からリカバリします**

クラスタネットワークがスイッチにケーブル接続されているが、クラスタ IPspace に設定されたすべてのポートがクラスタ IPspace に設定された他のポートに到達できない場合は、クラスタを作成できません。

このタスクについて

スイッチクラスタで、クラスタネットワークインターフェイス（LIF）が間違っ

合、またはクラスタポートが間違ったネットワークに接続されている場合は、が表示されます `cluster create` 次のエラーが表示されてコマンドが失敗することがあります。

```
Not all local cluster ports have reachability to one another.  
Use the "network port reachability show -detail" command for more details.
```

の結果 `network port show` コマンドでは、クラスタLIFが設定されたポートに接続されているために、複数のポートがクラスタIPspaceに追加されたと表示されることがあります。ただし、の結果 `network port reachability show -detail` コマンドは、相互に接続されていないポートを表示します。

クラスタ LIF が設定された他のポートに到達できないポート上に設定されたクラスタ LIF をリカバリするには、次の手順を実行します。

#### 手順

1. クラスタ LIF のホームポートを正しいポートにリセットします。

```
network port modify -home-port
```

2. クラスタ LIF が設定されていないポートをクラスタブロードキャストドメインから削除します。

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

3. クラスタを作成します。

```
cluster create
```

#### 結果

クラスタの作成が完了すると、正しい設定が検出され、正しいブロードキャストドメインにポートが配置されます。

#### LIF を削除する

不要になったネットワークインターフェイス（LIF）を削除できます。

作業を開始する前に

削除する LIF が使用中でないことを確認します。

#### 手順

1. 次のコマンドを使用して、削除する LIF を意図的に停止したものとしてマークします。

```
network interface modify -vserver vservice_name -lif lif_name -status  
-admin down
```

2. を使用します `network interface delete` 1つまたはすべてのLIFを削除するコマンド：

削除の対象	入力するコマンド
特定の LIF	<code>network interface delete -vserver vs1 -lif lif_name</code>
すべての LIFs	<code>network interface delete -vserver vs1 -lif *</code>

次のコマンドは、`mgmtlif2` という LIF を削除します。

```
network interface delete -vserver vs1 -lif mgmtlif2
```

3. を使用します `network interface show` コマンドを入力して、LIFが削除されたことを確認します。

## ネットワーク負荷の分散

### Balanceネットワークの概要

負荷が適切に割り当てられた LIF でクライアント要求を処理するようにクラスタを設定することができます。その結果、LIF とポートがバランスよく使用されるようになり、クラスタのパフォーマンスが向上します。

DNS ロードバランシングを使用すると、負荷が適切なデータ LIF を選んで、使用可能なデータポートすべて（物理、インターフェイスグループ、VLAN）にユーザネットワークのトラフィックを分散させることができます。

DNS ロードバランシングでは、LIF が SVM のロードバランシングゾーンに関連付けられます。サイト規模の DNS サーバは、すべての DNS 要求を転送し、ネットワークトラフィックおよびポートのリソースの可用性（CPU 使用率、スループット、開いている接続など）に基づいて負荷の最も少ない LIF を返すように設定されています。DNS ロードバランシングのメリットは次のとおりです。

- 新しいクライアント接続が、使用可能なリソース全体に分散されます。
- 特定の SVM をマウントするときに使用する LIF を手動で決める必要がありません。
- DNSロードバランシングは、NFSv3、NFSv4、NFSv4.1、SMB 2.0、SMB 2.1、SMB 3.0、S3に対応しています。

### DNS ロードバランシングの仕組み

クライアントは、LIF に関連付けられた IP アドレス、または複数の IP アドレスに関連付けられたホスト名を指定することにより、SVM をマウントします。デフォルトでは、すべての LIF のワークロードのバランスが取れるように、サイト規模の DNS サーバによってラウンドロビン方式で LIF が選択されます。

ラウンドロビン方式のロードバランシングでは、LIF のいくつかが過負荷になることがあります。そのため、

SVM でホスト名の解決を取り扱う DNS のロードバランシングゾーンを使用するオプションがあります。DNS ロードバランシングゾーンを使用すると、新しいクライアント接続が使用可能なリソース間でバランスよく配分されるため、クラスタのパフォーマンスが向上します。

DNS ロードバランシングゾーンは、クラスタ内の DNS サーバであり、すべての LIF の負荷を動的に評価して、負荷を適切に割り当てる LIF を返します。ロードバランシングゾーンでは、DNS が負荷に基づいてそれぞれの LIF に重み（メトリック）を割り当てます。

すべての LIF に、ポートの負荷とホームノードの CPU 利用率に基づいて重みが割り当てられます。DNS クエリでは、負荷が低いポートの LIF から優先的に返されます。重みは手動で割り当てすることもできます。

## DNS ロードバランシングゾーンを作成します

DNS ロードバランシングゾーンを作成すると、LIF にマウントされているクライアントの数など、負荷に基づいて LIF を動的に選択できるようになります。ロードバランシングゾーンはデータ LIF の作成時に作成できます。

作業を開始する前に

サイト規模の DNS サーバ上に、設定した LIF にロードバランシングゾーンに対するすべての要求を転送する DNS フォワーダを設定しておく必要があります。

技術情報アーティクル "[clustered Data ONTAP での DNS ロードバランシングの設定方法](#)" NetApp Support Siteには、条件付き転送を使用する DNS ロードバランシングの設定に関する詳細が記載されています。

このタスクについて

- すべてのデータ LIF は、DNS ロードバランシングゾーン名の DNS クエリに応答できます。
- DNS ロードバランシングゾーンの名前はクラスタ内で一意でなければなりません。ゾーン名の要件は次のとおりです。
  - 256 文字以内にする必要があります。
  - ピリオドが少なくとも 1 つ必要です。
  - 先頭と末尾の文字をピリオドなどの特殊文字にすることはできません。
  - 文字間にスペースを使用することはできません。
  - DNS 名の各ラベルの最大文字数は 63 文字です。

ラベルは、ピリオドの前後のテキストです。たとえば、storage.company.com という名前の DNS ゾーンは 3 つのラベルで構成されています。

## ステップ

を使用します `network interface create` コマンドにを指定します `dns-zone` DNSロードバランシングゾーンを作成するオプション。

ロードバランシングゾーンがすでに存在する場合は、LIF がそのロードバランシングゾーンに追加されます。コマンドの詳細については、を参照してください "[ONTAP 9 のコマンド](#)"。

次の例は、LIFの作成時にstorage.company.comという名前のDNSロードバランシングゾーンを作成する方法を示しています `lif1`：

```
network interface create -vserver vs0 -lif lif1 -home-node node1
-home-port e0c -address 192.0.2.129 -netmask 255.255.255.128 -dns-zone
storage.company.com
```

## ロードバランシングゾーンに対して LIF を追加または削除する

仮想マシン（SVM）の DNS ロードバランシングゾーンに対して LIF を追加または削除できます。すべての LIF をロードバランシングゾーンから同時に削除することもできます。

作業を開始する前に

- ロードバランシングゾーンの LIF は、すべて同じ SVM に属している必要があります。
- 各 LIF は 1 つの DNS ロードバランシングゾーンにのみ含めることができます。
- サブネットの異なる LIF がある場合は、サブネットごとのフェイルオーバーグループが設定されている必要があります。

このタスクについて

管理ステータスが down の LIF は一時的に DNS ロードバランシングゾーンから削除されます。LIF の管理ステータスが up に戻ると、自動的に DNS ロードバランシングゾーンに追加されます。

ステップ

ロードバランシングゾーンに対して LIF を追加または削除します。

状況	入力するコマンド
LIF を追加する	<pre>network interface modify -vserver vs0 -lif lif1 -dns-zone zone1</pre> <p>例</p> <pre>network interface modify -vserver vs1 -lif data1 -dns-zone cifs.company.com</pre>
1 つの LIF を削除する	<pre>network interface modify -vserver vs0 -lif lif1 -dns-zone none</pre> <p>例</p> <pre>network interface modify -vserver vs1 -lif data1 -dns-zone none</pre>
すべての LIF を削除します	<pre>network interface modify -vserver vs0 -lif * -dns-zone none</pre> <p>例</p> <pre>network interface modify -vserver vs0 -lif * -dns-zone none</pre> <p>ロードバランシングゾーンからSVMのすべてのLIFを削除することで、そのゾーンからSVMを削除できます。</p>

## DNSサービスの設定（ONTAP 9.8以降）

NFS または SMB サーバを作成する前に、SVM 用の DNS サービスを設定する必要があります。通常、DNS ネームサーバは、NFS または SMB サーバが参加するドメインの Active Directory 統合 DNS サーバです。

このタスクについて

Active Directory 統合 DNS サーバには、ドメイン LDAP およびドメインコントローラサーバのサービスレコード（SRV）が格納されます。SVM が Active Directory LDAP サーバおよびドメインコントローラを見つけられない場合は、NFS または SMB サーバのセットアップに失敗します。

SVM は、ホストについての情報を検索する際に、hosts ネームサービス ns-switch データベースを使用してどのネームサービスを使用するか、どの順番で使用するかを決定します。hosts データベースでサポートされている 2 つのネームサービスは、files および dns です。

SMB サーバを作成する前に、dns がソースの 1 つであることを確認する必要があります。



mgwd プロセスと SecD プロセスについて DNS ネームサービスの統計を表示するには、統計画面を使用します。

### 手順

1. hosts ネームサービスデータベースの現在の設定を確認します。この例では、hosts ネームサービスデータベースはデフォルトの設定を使用しています。

```
vserver services name-service ns-switch show -vserver vs1 -database hosts
```

```
Vserver: vs1
Name Service Switch Database: hosts
Vserver: vs1 Name Service Switch Database: hosts
Name Service Source Order: files, dns
```

2. 必要に応じて、次の操作を実行します。

- a. DNS ネームサービスを希望の順序で hosts ネームサービスデータベースに追加するか、ソースの順序を変更します。

この例では、DNS ファイルとローカルファイルを順に使用するように hosts データベースを設定しています。

```
vserver services name-service ns-switch modify -vserver vs1 -database hosts
-sources dns,files
```

- b. ネームサービスの設定が正しいことを確認します。

```
vserver services name-service ns-switch show -vserver vs1 -database hosts
```

```
Vserver: vs1
Name Service Switch Database: hosts
Name Service Source Order: dns, files
```

### 3. DNS サービスを設定する

```
vserver services name-service dns create -vserver vs1 -domains
example.com,example2.com -name-servers 10.0.0.50,10.0.0.51
```



vserver services name-service dns create コマンドを使用すると、設定の自動検証が行われ、ONTAP がネームサーバに接続できない場合はエラーメッセージが報告されます。

### 4. DNS の設定が正しいことと、サービスが有効になっていることを確認してください。

```
Vserver: vs1
Domains: example.com, example2.com Name Servers: 10.0.0.50, 10.0.0.51
Enable/Disable DNS: enabled Timeout (secs): 2
Maximum Attempts: 1
```

### 5. ネームサーバのステータスを検証します。

```
vserver services name-service dns check -vserver vs1
```

Vserver	Name Server	Status	Status Details
vs1	10.0.0.50	up	Response time (msec): 2
vs1	10.0.0.51	up	Response time (msec): 2

## SVM に動的 DNS を設定します

Active Directory に統合された DNS サーバを DNS にある NFS または SMB サーバの DNS レコードに動的に登録する場合は、SVM で動的 DNS（DDNS）を設定する必要があります。

作業を開始する前に

SVM で DNS ネームサービスが設定されている必要があります。セキュア DDNS を使用する場合は、Active Directory 統合 DNS ネームサーバを使用して、SVM 用の NFS または SMB サーバまたは Active Directory アカウントを作成しておく必要があります。

このタスクについて

完全修飾ドメイン名（FQDN）は一意にする必要があります。

完全修飾ドメイン名（FQDN）は一意にする必要があります。

- NFSの場合は、で指定した値です -vserver-fqdn の一部として vserver services name-service dns dynamic-update コマンドがLIFの登録FQDNになります。

- SMB の場合、CIFS サーバの NetBIOS 名および CIFS サーバの完全修飾ドメイン名として指定された値が、LIF の登録済み FQDN になります。ONTAP では設定できません。次のシナリオでは、LIF FQDN は「CIFS\_VS1.EXAMPLE.COM」です

```
cluster1::> cifs server show -vserver vs1
```

```

                                Vserver: vs1
                                CIFS Server NetBIOS Name: CIFS_VS1
                                NetBIOS Domain/Workgroup Name: EXAMPLE
                                Fully Qualified Domain Name: EXAMPLE.COM
                                Organizational Unit: CN=Computers
Default Site Used by LIFs Without Site Membership:
                                Workgroup Name: -
                                Kerberos Realm: -
                                Authentication Style: domain
CIFS Server Administrative Status: up
CIFS Server Description:
List of NetBIOS Aliases: -

```



DDNS 更新の RFC ルールに準拠していない SVM FQDN の設定エラーを回避するには、RFC に準拠した FQDN 名を使用します。詳細については、[RFC 1123](#)を参照してください。

## 手順

### 1. SVM で DDNS を設定します。

```
vserver services name-service dns dynamic-update modify -vserver vserver_name
-is-enabled true [-use-secure {true|false} -vserver-fqdn
FQDN_used_for_DNS_updates
```

```
vserver services name-service dns dynamic-update modify -vserver vs1 -is
-enabled true - use-secure true -vserver-fqdn vs1.example.com
```

カスタマイズした FQDN の一部としてアスタリスクを使用することはできません。例：\*.netapp.com が無効です。

### 2. DDNS の設定が正しいことを確認します。

```
vserver services name-service dns dynamic-update show
```

Vserver	Is-Enabled	Use-Secure	Vserver FQDN	TTL
vs1	true	true	vs1.example.com	24h



## DNSサービスの設定（ONTAP 9.7以前）

NFS または SMB サーバを作成する前に、SVM 用の DNS サービスを設定する必要があります。通常、DNS ネームサーバは、NFS または SMB サーバが参加するドメインの Active Directory 統合 DNS サーバです。

このタスクについて

Active Directory 統合 DNS サーバには、ドメイン LDAP およびドメインコントローラサーバのサービスレコード（SRV）が格納されます。SVM が Active Directory LDAP サーバおよびドメインコントローラを見つけられない場合は、NFS または SMB サーバのセットアップに失敗します。

SVM は、ホストについての情報を検索する際に、hosts ネームサービス ns-switch データベースを使用してどのネームサービスを使用するか、どの順番で使用するかを決定します。hosts データベースでサポートされる2つのネームサービスは `files` および `dns`。

それを確認する必要があります `dns` は、SMBサーバを作成する前のソースの1つです。



mgwd プロセスと SecD プロセスについて DNS ネームサービスの統計を表示するには、統計画面を使用します。

### 手順

1. の現在の設定を確認します hosts ネームサービスデータベース

この例では、hosts ネームサービスデータベースはデフォルトの設定を使用しています。

```
vserver services name-service ns-switch show -vserver vs1 -database hosts
```

```
Vserver: vs1
Name Service Switch Database: hosts
Name Service Source Order: files, dns
```

2. 必要に応じて、次の操作を実行します。

- a. DNS ネームサービスを希望の順序で hosts ネームサービスデータベースに追加するか、ソースの順序を変更します。

この例では、DNS ファイルとローカルファイルを順に使用するように hosts データベースを設定しています。

```
vserver services name-service ns-switch modify -vserver vs1 -database hosts
-sources dns,files
```

- a. ネームサービスの設定が正しいことを確認します。

```
vserver services name-service ns-switch show -vserver vs1 -database hosts
```

3. DNS サービスを設定する

```
vserver services name-service dns create -vserver vs1 -domains
```

```
example.com,example2.com -name-servers 10.0.0.50,10.0.0.51
```



SVMサービス `name-service dns create` コマンドは設定の自動検証を実行し、ONTAP がネームサーバに接続できない場合はエラーメッセージを報告します。

4. DNS の設定が正しいことと、サービスが有効になっていることを確認してください。

```
Vserver: vs1
Domains: example.com, example2.com Name
Servers: 10.0.0.50, 10.0.0.51
Enable/Disable DNS: enabled Timeout (secs): 2
Maximum Attempts: 1
```

5. ネームサーバのステータスを検証します。

```
vserver services name-service dns check -vserver vs1
```

Vserver	Name Server	Status	Status Details
vs1	10.0.0.50	up	Response time (msec): 2
vs1	10.0.0.51	up	Response time (msec): 2

## SVM に動的 DNS を設定します

Active Directory に統合された DNS サーバを DNS にある NFS または SMB サーバの DNS レコードに動的に登録する場合は、SVM で動的 DNS (DDNS) を設定する必要があります。

作業を開始する前に

SVM で DNS ネームサービスが設定されている必要があります。セキュア DDNS を使用する場合は、Active Directory 統合 DNS ネームサーバを使用して、SVM 用の NFS または SMB サーバまたは Active Directory アカウントを作成しておく必要があります。

このタスクについて

完全修飾ドメイン名 (FQDN) は一意にする必要があります。

- NFSの場合は、で指定した値です `-vserver-fqdn` の一部として `vserver services name-service dns dynamic-update` コマンドがLIFの登録FQDNになります。
- SMB の場合、CIFS サーバの NetBIOS 名および CIFS サーバの完全修飾ドメイン名として指定された値が、LIF の登録済み FQDN になります。ONTAP では設定できません。次のシナリオでは、LIF FQDN は「CIFS\_VS1.EXAMPLE.COM」です

```
cluster1::> cifs server show -vserver vs1
```

```

Vserver: vs1
CIFS Server NetBIOS Name: CIFS_VS1
NetBIOS Domain/Workgroup Name: EXAMPLE
Fully Qualified Domain Name: EXAMPLE.COM
Organizational Unit: CN=Computers
Default Site Used by LIFs Without Site Membership:
Workgroup Name: -
Kerberos Realm: -
Authentication Style: domain
CIFS Server Administrative Status: up
CIFS Server Description:
List of NetBIOS Aliases: -
```



DDNS 更新の RFC ルールに準拠していない SVM FQDN の設定エラーを回避するには、RFC に準拠した FQDN 名を使用します。詳細については、[RFC 1123](#)を参照してください。

## 手順

1. SVM で DDNS を設定します。

```
vserver services name-service dns dynamic-update modify -vserver vs1 -is-  
-enabled true [-use-secure {true|false} -vserver-fqdn  
FQDN_used_for_DNS_updates
```

```
vserver services name-service dns dynamic-update modify -vserver vs1 -is-  
-enabled true - use-secure true -vserver-fqdn vs1.example.com
```

カスタマイズした FQDN の一部としてアスタリスクを使用することはできません。例：\*.netapp.com が無効です。

2. DDNS の設定が正しいことを確認します。

```
vserver services name-service dns dynamic-update show
```

Vserver	Is-Enabled	Use-Secure	Vserver FQDN	TTL
vs1	true	true	vs1.example.com	24h

## 動的 DNS サービスを設定する

Active Directory に統合された DNS サーバを DNS にある NFS または SMB サーバの DNS レコードに動的に登録する場合は、SVM で動的 DNS（DDNS）を設定する必要があります。

作業を開始する前に

SVM で DNS ネームサービスが設定されている必要があります。セキュア DDNS を使用する場合は、Active Directory 統合 DNS ネームサーバを使用して、SVM 用の NFS または SMB サーバまたは Active Directory アカウントを作成しておく必要があります。

このタスクについて

一意の FQDN を指定する必要があります。



DDNS 更新の RFC ルールに準拠していない SVM FQDN の設定エラーを回避するには、RFC に準拠した FQDN 名を使用します。

手順

1. SVM で DDNS を設定します。

```
vserver services name-service dns dynamic-update modify -vserver vserver_name
-is-enabled true [-use-secure {true|false}] -vserver-fqdn
FQDN_used_for_DNS_updates
```

```
vserver services name-service dns dynamic-update modify -vserver vs1 -is
-enabled true - use-secure true -vserver-fqdn vs1.example.com
```

カスタマイズした FQDN の一部としてアスタリスクを使用することはできません。例：\*.netapp.com が無効です。

2. DDNS の設定が正しいことを確認します。

```
vserver services name-service dns dynamic-update show
```

Vserver	Is-Enabled	Use-Secure	Vserver FQDN	TTL
vs1	true	true	vs1.example.com	24h

## ホストメイカイケツ

### ホストメイカイケツノカイヨウ

ONTAP では、クライアントにアクセスを提供したりサービスにアクセスしたりするために、ホスト名を数値の IP アドレスに変換できなければなりません。Storage Virtual Machine (SVM) でローカルまたは外部のネームサービスを使用してホスト情報を解決するように設定する必要があります。ONTAP では、ホスト名を解決するために外部 DNS サーバまたはローカルの hosts ファイルを使用するように設定できます。

外部 DNS サーバを使用する場合は、動的 DNS (DDNS) を設定できます。これにより、新規または変更された DNS 情報がストレージシステムから DNS サーバに自動的に送信されます。動的 DNS 更新を使用しない場合は、新しいシステムがオンラインになったときや既存の DNS 情報が変更されたときに、特定された DNS サーバに手動で DNS 情報 (DNS の名前と IP アドレス) を追加する必要があります。このプロセスは時間が

かかり、エラーが発生しやすくなります。ディザスタリカバリ時に手動で設定を行っていると、ダウンタイムが長くなる可能性があります。

## ホスト名解決に使用する **DNS** を設定します

ホスト情報を取得するには、DNS を使用してローカルソースまたはリモートソースにアクセスします。これらのソースのいずれかまたは両方にアクセスするために DNS を設定する必要があります。

ONTAP がクライアントに適切なアクセスを許可するには、ホスト情報を検索できなければなりません。ネームサービスを設定して、ONTAP がホスト情報を取得するためにローカルまたは外部の DNS サービスにアクセスできるようにします。

ONTAP では、に相当するテーブルにネームサービス設定情報が格納されます `/etc/nsswitch.conf` UNIX システム上のファイル。

外部 **DNS** サーバを使用して、ホスト名解決のために **SVM** とデータ **LIF** を設定する

使用できます `vserver services name-service dns` コマンドを使用してSVMでDNSを有効にし、ホスト名解決にDNSを使用するように設定します。ホスト名は外部 DNS サーバを使用して解決されます。

作業を開始する前に

ホスト名を検索するために、サイト規模の DNS サーバが使用可能である必要があります。

単一点障害を回避するには、複数の DNS サーバを設定する必要があります。。 `vserver services name-service dns create` 入力したDNSサーバ名が1つだけの場合は警告が表示されます。

このタスクについて

を参照してください [動的 DNS サービスを設定する](#) SVMでの動的DNSの設定に関する詳細については、を参照してください。

手順

1. SVM で DNS を有効にします。

```
vserver services name-service dns create -vserver <vserver_name>
-domains <domain_name> -name-servers <ip_addresses> -state enabled
```

次のコマンドは、SVM vs1 で外部 DNS サーバを有効にします。

```
vserver services name-service dns create -vserver vs1.example.com
-domains example.com -name-servers 192.0.2.201,192.0.2.202 -state
enabled
```



。 `vserver services name-service dns create` コマンドは設定の自動検証を実行し、ONTAP がネームサーバに接続できない場合はエラーメッセージを報告します。

2. を使用してネームサーバのステータスを検証します `vserver services name-service dns check` コマンドを実行します

```
vserver services name-service dns check -vserver vs1.example.com
```

Name Server			
Vserver	Name Server	Status	Status Details
vs1.example.com	10.0.0.50	up	Response time (msec): 2
vs1.example.com	10.0.0.51	up	Response time (msec): 2

DNSに関連するサービスポリシーの詳細については、を参照してください。 ["ONTAP 9.6 以降の LIF とサービスポリシー"](#)。

ホスト名解決用のネームサービススイッチテーブルを設定します

ONTAP がホスト情報を取得するためにローカルまたは外部のネームサービスにアクセスできるようにするには、ネームサービススイッチテーブルを正しく設定する必要があります。

作業を開始する前に

環境内のホストのマッピングでどのネームサービスを使用するかを決めておく必要があります。

手順

1. ネームサービススイッチテーブルに必要なエントリを追加します。

```
vserver services name-service ns-switch modify -vserver <vserver_name>  
-database <database_name> -source <source_names>
```

2. ネームサービススイッチテーブルに想定されるエントリが適切な順序で格納されていることを確認します。

```
vserver services name-service ns-switch show -vserver <vserver_name>
```

例

次の例は、SVM vs1のネームサービススイッチテーブル内のエントリを、ホスト名を解決するためにまずローカルのhostsファイルを使用し、次に外部DNSサーバを使用するように変更します。

```
vserver services name-service ns-switch modify -vserver vs1 -database  
hosts -sources files,dns
```

## hosts テーブルの管理（クラスタ管理者のみ）

クラスタ管理者は、管理 Storage Virtual Machine（SVM）の hosts テーブルのホスト名エントリを追加、変更、削除、表示できます。SVM 管理者は、割り当てられた SVM に対してのみホスト名エントリを設定できます。

ローカルホスト名エントリを管理するコマンド

を使用できます `vserver services name-service dns hosts` DNSホストテーブルエントリを作成、変更、または削除するコマンド。

DNS ホスト名エントリを作成または変更するときは、複数のエイリアスアドレスをカンマで区切って指定できます。

状況	使用するコマンド
DNS ホスト名エントリを作成します	<code>vserver services name-service dns hosts create</code>
DNS ホスト名エントリを変更する	<code>vserver services name-service dns hosts modify</code>
DNS ホスト名エントリを削除する	<code>vserver services name-service dns hosts delete</code>

詳細については、を参照してください ["ONTAP 9 のコマンド"](#) をクリックします `vserver services name-service dns hosts` コマンド

## ネットワークを保護します

連邦情報処理標準（**FIPS**）を使用したネットワークセキュリティの設定

ONTAP は、すべての SSL 接続に対する連邦情報処理標準（FIPS）140-2 に準拠しています。ONTAP では、SSL FIPS モードを有効または無効にしたり、SSL プロトコルをグローバルに設定したり、RC4 などの弱い暗号を無効にしたりできます。

デフォルトでは、ONTAP の SSL は、次のプロトコルを使用して FIPS 準拠が無効、SSL プロトコルが有効な状態で設定されます。

- TLSv1（ONTAP 9.11.1以降）
- TLSv1.2
- TLSv1.1
- TLSv1

SSL FIPS モードがイネーブルの場合、ONTAP から ONTAP 外部のクライアントまたはサーバコンポーネントへの SSL 通信には、FIPS 準拠の SSL 用暗号が使用されます。

管理者アカウントが SSH 公開鍵を使用して SVM にアクセスできるようにする場合は、SSL FIPS モードを有効にする前に、ホストキーアルゴリズムがサポートされていることを確認する必要があります。

\*注：ONTAP 9.11.1以降では、ホストキーアルゴリズムのサポートが変更されています。

ONTAP リリース	サポートされているキータイプ	サポートされていないキータイプです
9.11.1以降	ECDSA - sha2 - nistp256	rsa-sha2-512+ rsa-sha2-256+ SSH-ed25519以降 SSH-DSS+ SSH-RSA
9.10.1以前	ECDSA-sha2-nistp256+ SSH-ed25519	SSH-DSS+ SSH-RSA

FIPS を有効にする前に、サポートされるキーアルゴリズムを使用していない既存の SSH 公開鍵アカウントをサポート対象のキータイプで再設定する必要があります。再設定しないと、管理者認証は失敗します。

詳細については、を参照してください ["SSH 公開鍵アカウントを有効にします"](#)。

SSL FIPSモードの設定の詳細については、を参照してください `security config modify` のマニュアルページ。

## FIPSを有効にする

システムのインストールまたはアップグレードの直後に、すべてのセキュアユーザがセキュリティ設定を調整することを推奨します。SSL FIPS モードがイネーブルの場合、ONTAP から ONTAP 外部のクライアントまたはサーバコンポーネントへの SSL 通信には、FIPS 準拠の SSL 用暗号が使用されます。



FIPSが有効な場合、RSAキーの長さが4096の証明書をインストールまたは作成することはできません。

## 手順

1. advanced 権限レベルに切り替えます。

```
set -privilege advanced
```

2. FIPSを有効にします。

```
security config modify -interface SSL -is-fips-enabled true
```

3. 続行するかどうかを尋ねられたら、と入力します `y`
4. ONTAP 9.8 以前を実行している場合は、クラスタ内の各ノードを 1 つずつ手動でリブートします。ONTAP 9.9.1以降では、リブートは必要ありません。

## 例

ONTAP 9.9.1 以降を実行している場合は、警告メッセージは表示されません。



```
security config modify -interface SSL -is-fips-enabled true
```

Warning: This command will enable FIPS compliance and can potentially cause some non-compliant components to fail. MetroCluster and Vserver DR require FIPS to be enabled on both sites in order to be compatible.

Do you want to continue? {y|n}: y

Warning: When this command completes, reboot all nodes in the cluster. This is necessary to prevent components from failing due to an inconsistent security configuration state in the cluster. To avoid a service outage, reboot one node at a time and wait for it to completely initialize before rebooting the next node. Run "security config status show" command to monitor the reboot status.

Do you want to continue? {y|n}: y

## FIPS を無効にする

古いシステム構成を実行し続けている状態で、ONTAP の設定で下位互換性を確保する場合は、FIPS が無効な場合にのみ SSLv3 を有効にすることができます。

### 手順

1. advanced 権限レベルに切り替えます。

```
set -privilege advanced
```

2. 次のように入力して FIPS を無効に

```
security config modify -interface SSL -is-fips-enabled false
```

3. 続行するかどうかを尋ねられたら、と入力します y。
4. ONTAP 9.8 以前を実行している場合は、クラスタ内の各ノードを手動でリブートします。ONTAP 9.9.1以降では、リブートは必要ありません。

### 例

ONTAP 9.9.1 以降を実行している場合は、警告メッセージは表示されません。

```
security config modify -interface SSL -supported-protocols SSLv3
```

Warning: Enabling the SSLv3 protocol may reduce the security of the interface, and is not recommended.

Do you want to continue? {y|n}: y

Warning: When this command completes, reboot all nodes in the cluster. This is necessary to prevent components from failing due to an inconsistent security configuration state in the cluster. To avoid a service outage, reboot one node at a time and wait for it to completely initialize before rebooting the next node. Run "security config status show" command to monitor the reboot status.

Do you want to continue? {y|n}: y

## FIPS 準拠ステータスを表示します

クラスタ全体で現在のセキュリティ設定が実行されているかどうかを確認することができます。

### 手順

1. クラスタ内の各ノードを 1 つずつリブートします。

すべてのクラスタノードを同時にリブートしないでください。クラスタ内のすべてのアプリケーションで新しいセキュリティ設定が実行されていること、および FIPS のオン / オフモード、プロトコル、暗号に対する変更がすべて反映されていることを確認するには、リブートが必要です。

2. 現在の準拠ステータスを表示します。

```
security config show
```

```
security config show
```

	Cluster		Cluster
Security			
Interface	FIPS Mode	Supported Protocols	Supported Ciphers Config
Ready			
-----			
-----			
SSL	false	TLSv1_2, TLSv1_1, TLSv1	ALL:!LOW:!aNULL: yes !EXP:!eNULL

## ワイヤ暗号化を介した IP セキュリティ（IPsec）を設定します

ONTAP は、転送モードでインターネットプロトコルセキュリティ (IPsec) を使用して、転送中もデータの安全性と暗号化を継続的に確保します。IPsec では、NFS、iSCSI、

SMB の各プロトコルを含むすべての IP トラフィックを暗号化できます。

ONTAP 9.12.1以降では、フロントエンドホストプロトコルIPsecサポートは、MetroCluster IPおよびMetroCluster ファブリック接続構成で利用できます。  
MetroCluster クラスタでのIPSecのサポートは、フロントエンドのホストトラフィックに限定され、MetroCluster のクラスタ間LIFではサポートされません。

ONTAP 9.10.1 以降では、Pre-Shared Key（PSK; 事前共有キー）または証明書のいずれかを使用してIPSecでの認証を行うことができます。以前は、IPsecでサポートされていたのはPSKだけでした。

ONTAP 9.9.1以降では、IPsecで使用する暗号化アルゴリズムがFIPS 140-2に準拠しています。アルゴリズムは、ONTAP のNetApp Cryptographic Moduleによって生成され、FIPS 140-2認定を継承しています。

ONTAP 9.8以降では、ONTAPでトランスポートモードのIPsecがサポートされます。

IPSec の設定後は、リプレイ攻撃や中間者（MITM）攻撃に対抗するための予防措置を講じて、クライアントと ONTAP 間のネットワークトラフィックを保護します。

NetApp SnapMirror およびクラスタピアリングトラフィックの暗号化では、クラスタピアリング暗号化（CPE）の場合でも、IPSec 経由でセキュアな転送レイヤセキュリティ（TLS）を使用することを推奨します。これは、TLSの方がIPsecよりもパフォーマンスが優れているためです。

クラスタでIPSec機能が有効になっている場合、ネットワークでトラフィックを処理するには、保護対象のトラフィックと一致する Security Policy Database（SPD）エントリ、および保護の詳細（暗号スイートや認証方式など）を指定する必要があります。各クライアントには、対応する SPD エントリも必要です。

クラスタで **IPSec** を有効に設定します

クラスタのIPSecを有効にして、転送中もデータのセキュリティを継続的に確保し、暗号化することができます。

手順

1. IPSec がすでに有効になっているかどうかを検出します。

```
security ipsec config show
```

結果にが含まれている場合 `IPsec Enabled: false` 次の手順に進みます。

2. IPSec を有効にします。

```
security ipsec config modify -is-enabled true
```

3. 検出コマンドを再度実行します。

```
security ipsec config show
```

結果にが含まれるようになりました IPsec Enabled: true。

証明書認証を使用した**IPSec**ポリシーの作成の準備

認証に事前共有キー（PSK）のみを使用し、証明書認証を使用しない場合は、この手順を省略できます。

認証に証明書を使用するIPsecポリシーを作成する前に、次の前提条件を満たしていることを確認する必要があります。

- エンドエンティティ（ONTAPまたはクライアント）の証明書を両側で検証できるように、ONTAPとクライアントの両方に相手のCA証明書をインストールする必要があります。
- ポリシーに含まれる ONTAP LIF の証明書がインストールされます



ONTAP LIF は証明書を共有できます。証明書と LIF の間に 1 対 1 のマッピングは必要ありません。

#### 手順

1. 相互認証で利用したすべてのCA証明書（ONTAP側CAとクライアント側CAの両方を含む）をONTAP証明書管理にインストールします（ONTAPの自己署名ルートCAの場合など）。

##### サンプルコマンド

```
cluster::> security certificate install -vserver svm_name -type server-ca  
-cert-name my_ca_cert
```

2. インストールされているCAが認証時にIPsec CA検索パス内にあることを確認するには、を使用して、ONTAP証明書管理CAをIPsecモジュールに追加します。 security ipsec ca-certificate add コマンドを実行します

##### サンプルコマンド

```
cluster::> security ipsec ca-certificate add -vserver svm_name -ca-certs  
my_ca_cert
```

3. ONTAP LIF で使用する証明書を作成してインストールします。この証明書の発行元 CA がすでに ONTAP にインストールされ、IPSec に追加されている必要があります。

##### サンプルコマンド

```
cluster::> security certificate install -vserver svm_name -type server -cert  
-name my_nfs_server_cert
```

ONTAPの証明書の詳細については、ONTAP 9のドキュメントのsecurity certificateコマンドを参照してください。

#### セキュリティポリシーデータベース（SPD）の定義

IPSec では、トラフィックをネットワーク上に転送する前に SPD エントリが必要です。これは、認証に PSK と証明書のどちらを使用している場合にも当てはまります。

#### 手順

1. を使用します security ipsec policy create コマンドの宛先：
  - a. ONTAP IP アドレスまたは IP アドレスのサブネットを選択して、IPSec 転送に参加します。
  - b. ONTAP IP アドレスに接続するクライアント IP アドレスを選択します。



クライアントは、Pre-Shared Key（PSK）を使用して Internet Key Exchange バージョン 2（IKEv2）をサポートしている必要があります。

- c. 任意。上位層プロトコル（UDP、TCP、ICMPなど）など、きめ細かなトラフィックパラメータを選択します。）、ローカルポート番号、およびトラフィックを保護するリモートポート番号。対応するパラメータは `protocols`、`local-ports` および `remote-ports` それぞれ。

ONTAP IP アドレスとクライアント IP アドレスの間のすべてのトラフィックを保護するには、この手順を省略します。デフォルトでは、すべてのトラフィックを保護します。

- d. のPSKまたは公開キーインフラストラクチャ（PKI）を入力します。 `auth-method` 必要な認証方式のパラメータ。
  - i. PSKを入力する場合は、パラメータを指定し、<enter>キーを押して事前共有キーの入力と確認を求めるプロンプトを表示します。



`local-identity` および `remote-identity` ホストとクライアントの両方で**strongSwan**を使用し、ホストまたはクライアントに対してワイルドカードポリシーが選択されていない場合、パラメータはオプションです。

- ii. PKIを入力する場合は、も入力する必要があります `cert-name`、`local-identity`、`remote-identity` パラメータリモート側の証明書IDが不明な場合、または複数のクライアントIDが予想される場合は、特殊なIDを入力します。 `ANYTHING`。

```
security ipsec policy create -vserver vs1 -name test34 -local-ip-subnets
192.168.134.34/32 -remote-ip-subnets 192.168.134.44/32
Enter the preshared key for IPsec Policy _test34_ on Vserver _vs1_:
```

```
security ipsec policy create -vserver vs1 -name test34 -local-ip-subnets
192.168.134.34/32 -remote-ip-subnets 192.168.134.44/32 -local-ports 2049
-protocols tcp -auth-method PKI -cert-name my_nfs_server_cert -local
-identity CN=netapp.ipsec.lif1.vs0 -remote-identity ANYTHING
```

ONTAPとクライアントの両方が一致するIPsecポリシーを設定し、認証クレデンシャル（PSKまたは証明書）が両側に配置されるまで、IPトラフィックはクライアントとサーバの間を流れません。詳細については、クライアント側のIPsec設定を参照してください。

## IPsec ID を使用する

事前共有キー認証方式では、ホストとクライアントの両方で**strongSwan**を使用し、ホストまたはクライアントに対してワイルドカードポリシーが選択されていない場合、ローカルIDとリモートIDはオプションです。

PKI/ 証明書認証方式の場合、ローカル ID とリモート ID の両方が必須です。IDは、各側の証明書内で認証され、検証プロセスで使用されるIDを指定します。リモートIDが不明な場合、または多数の異なるIDである可能性がある場合は、特別なIDを使用します `ANYTHING`。

## このタスクについて

ONTAP では、SPD エントリを変更するか、または SPD ポリシーを作成する際に、ID を指定します。SPD には、IP アドレスまたは文字列形式の ID 名を使用できます。

## ステップ

既存のSPD ID設定を変更するには、次のコマンドを使用します。

```
security ipsec policy modify
```

コマンドの例を示します

```
security ipsec policy modify -vserver vs1 -name test34 -local-identity  
192.168.134.34 -remote-identity client.fooboo.com
```

## IPSec の複数クライアント設定

多数のクライアントで IPSec を利用する必要がある場合、クライアントごとに 1 つの SPD エントリを使用すれば十分です。ただし、数百、数千のクライアントで IPSec を利用する必要がある場合には、IPSec の複数クライアント設定を使用することを推奨します。

このタスクについて

ONTAP では、IPSec が有効な単一の SVM IP アドレスに、多数のネットワーク上にある複数のクライアントを接続できます。これを行うには、次のいずれかの方法を使用します。

### • \* サブネット構成 \*

特定のサブネット（192.168.134.0/24など）のすべてのクライアントが単一のSPDポリシーエントリを使用して単一のSVM IPアドレスに接続できるようにするには、を指定する必要があります remote-ip-subnets サブネット形式。また、を指定する必要があります remote-identity フィールドに正しいクライアント側IDを入力します。



サブネット設定で 1 つのポリシーエントリを使用する場合、そのサブネット内の IPsec クライアントは、IPsec ID と Pre-Shared Key（PSK；事前共有キー）を共有します。ただし、これは証明書認証には当てはまりません。証明書を使用する場合、各クライアントは独自の一意の証明書または共有証明書を使用して認証できます。ONTAP IPsec は、ローカルの信頼ストアにインストールされている CA に基づいて、証明書の有効性をチェックします。ONTAP は、証明書失効リスト (CRL) チェックもサポートしています。

### • \* すべてのクライアント設定を許可 \*

ソースIPアドレスに関係なくすべてのクライアントにSVMのIPsec対応IPアドレスへの接続を許可するには、を使用します 0.0.0.0/0 ワイルドカードワシテイスルバアイ remote-ip-subnets フィールド。

また、を指定する必要があります remote-identity フィールドに正しいクライアント側IDを入力します。証明書認証の場合は、と入力できます ANYTHING。

また、ときに 0.0.0.0/0 ワイルドカードを使用する場合は、使用する特定のローカルまたはリモートポート番号を設定する必要があります。例：NFS port 2049。

手順

a. 複数のクライアントに対してIPsecを設定するには、次のいずれかのコマンドを使用します。

i. サブネット設定\*を使用して複数のIPsecクライアントをサポートする場合：

```
security ipsec policy create -vserver vserver_name -name policy_name  
-local-ip-subnets IPsec_IP_address/32 -remote-ip-subnets  
IP_address/subnet -local-identity local_id -remote-identity remote_id
```

コマンドの例を示します

```
security ipsec policy create -vserver vs1 -name subnet134 -local-ip-subnets  
192.168.134.34/32 -remote-ip-subnets 192.168.134.0/24 -local-identity  
ontap_side_identity -remote-identity client_side_identity
```

- i. [すべてのクライアントの設定を許可する]\*を使用して複数のIPsecクライアントをサポートする場合は、次の手順を実行します。

```
security ipsec policy create -vserver vserver_name -name policy_name  
-local-ip-subnets IPsec_IP_address/32 -remote-ip-subnets 0.0.0.0/0 -local  
-ports port_number -local-identity local_id -remote-identity remote_id
```

コマンドの例を示します

```
security ipsec policy create -vserver vs1 -name test35 -local-ip-subnets  
IPsec_IP_address/32 -remote-ip-subnets 0.0.0.0/0 -local-ports 2049 -local  
-identity ontap_side_identity -remote-identity client_side_identity
```

## IPSec の統計情報

ネゴシエーションを使用すると、ONTAP SVM の IP アドレスとクライアントの IP アドレスの間に、IKE セキュリティアソシエーション（SA）と呼ばれるセキュリティチャネルを確立できます。IPsec SA は、実際のデータ暗号化および復号化を実行するために両方のエンドポイントにインストールされます。

statistics コマンドを使用して、IPsec SA と IKE SA の両方のステータスを確認できます。

コマンドの例を示します

IKE SA サンプルコマンド：

```
security ipsec show-ikesa -node hosting_node_name_for_svm_ip
```

IPSec SA サンプルコマンドおよび出力：

```
security ipsec show-ipseca -node hosting_node_name_for_svm_ip
```

```
cluster1::> security ipsec show-ikesa -node cluster1-node1
```

Vserver	Policy Name	Local Address	Remote Address	Initiator-SPI	State
vs1	test34	192.168.134.34	192.168.134.44	c764f9ee020cec69	ESTABLISHED

IPSec SA サンプルコマンドおよび出力：

```
security ipsec show-ipsecsa -node hosting_node_name_for_svm_ip

cluster1::> security ipsec show-ipsecsa -node cluster1-node1
      Policy   Local           Remote           Inbound   Outbound
Vserver  Name     Address          Address          SPI        SPI
State
-----
-----
vs1       test34
          192.168.134.34  192.168.134.44  c4c5b3d6  c2515559
INSTALLED
```

## LIF のファイアウォールポリシーを設定します

ファイアウォールを設定すると、クラスタのセキュリティを強化して、ストレージシステムへの不正アクセスを防止するのに役立ちます。デフォルトでは、オンボードファイアウォールは、データ LIF、管理 LIF、クラスタ間 LIF の特定の IP サービスへのリモートアクセスを許可するように設定されています。

ONTAP 9.10.1 以降：

- ファイアウォールポリシーは廃止され、LIFのサービスポリシーに置き換えられました。これまでは、オンボードファイアウォールはファイアウォールポリシーを使用して管理されていました。この機能は、LIF のサービスポリシーを使用して実行されるようになりました。
- すべてのファイアウォールポリシーが空であり、基盤となるファイアウォールのどのポートも開かない。代わりに、LIF のサービスポリシーを使用してすべてのポートを開く必要があります。
- ファイアウォールポリシーからLIFサービスポリシーに移行するために9.10.1以降にアップグレードしたあとは必要な処理はありません。以前のONTAP リリースで使用されていたファイアウォールポリシーと整合性のあるLIFサービスポリシーが自動的に構築されます。カスタムファイアウォールポリシーを作成および管理するスクリプトやその他のツールを使用している場合は、カスタムサービスポリシーを作成するスクリプトのアップグレードが必要になることがあります。

詳細については、を参照してください ["ONTAP 9.6 以降の LIF とサービスポリシー"](#)。

ファイアウォールポリシーを使用して、SSH、HTTP、HTTPS、Telnet、NTP などの管理サービスプロトコルへのアクセスを制御できます。NDMP、NDMPS、RSH、DNS、または SNMP。NFS や SMB などのデータプロトコル用にファイアウォールポリシーを設定することはできません。

ファイアウォールサービスとポリシーは、次の方法で管理できます。

- ファイアウォールサービスを有効または無効にします
- 現在のファイアウォールサービスの設定を表示しています
- ポリシー名とネットワークサービスを指定して新しいファイアウォールポリシーを作成してください
- ファイアウォールポリシーを論理インターフェイスに適用する
- 既存のファイアウォールポリシーとまったく同一の新しいポリシーを作成する



この機能は、同じ SVM 内でよく似たポリシーを作成するときや、別の SVM にポリシーをコピーするときに使用できます。

- ファイアウォールポリシーに関する情報を表示する
- ファイアウォールポリシーで使用する IP アドレスとネットマスクを変更する
- LIF で使用していないファイアウォールポリシーを削除する

## ファイアウォールポリシーと LIF

LIF のファイアウォールポリシーは、各 LIF を介したクラスタへのアクセスを制限するために使用します。デフォルトのファイアウォールポリシーが、各タイプの LIF を介したシステムアクセスにどのように影響するか、および LIF のセキュリティを強化または低下させるためにファイアウォールポリシーをカスタマイズする方法について理解しておく必要があります。

を使用して LIF を設定する場合 `network interface create` または `network interface modify` コマンドを入力します。に指定した値です `-firewall-policy` パラメータは、LIF へのアクセスを許可するサービスプロトコルと IP アドレスを決定します。

多くの場合、デフォルトのファイアウォールポリシーの値をそのまま使用できます。特定の IP アドレスや管理サービスプロトコルへのアクセスを制限しなければならない場合もあります。使用可能な管理サービスプロトコルは、SSH、HTTP、HTTPS、Telnet、NTP、NDMP、NDMPS、RSH、DNS、および SNMP。

すべてのクラスタ LIF のファイアウォールポリシーのデフォルトはです `""` およびは変更できません。

次の表に、LIF の作成時にそのロール（ONTAP 9.5 以前）またはサービスポリシー（ONTAP 9.6 以降）に応じて LIF に割り当てられるデフォルトのファイアウォールポリシーを示します。

ファイアウォールポリシー	デフォルトのサービスプロトコル	デフォルトのアクセス権	割り当て先の LIF
管理	DNS、http、https、ndmp、ndmps、NTP、SNMP、ssh	任意のアドレス（0.0.0.0/0）	クラスタ管理 LIF、SVM 管理 LIF、ノード管理 LIF
Mgmt - NFS を管理します	DNS、http、https、ndmp、ndmps、NTP、portmap、SNMP、ssh	任意のアドレス（0.0.0.0/0）	SVM 管理アクセスもサポートするデータ LIF
クラスタ間	HTTPS、NDMP、ndmps	任意のアドレス（0.0.0.0/0）	すべてのクラスタ間 LIF
データ	DNS、NDMP、ndmps、portmap	任意のアドレス（0.0.0.0/0）	すべてのデータ LIF

## portmap サービスの設定

portmap サービスは、RPC サービスを RPC サービスがリスンするポートにマッピングします。

ONTAP 9.3 以前では portmap サービスに常にアクセス可能で、ONTAP 9.4 では ONTAP 9.6 で設定可能になっており、ONTAP 9.7 以降では自動的に管理されます。

- ONTAP 9.3 までは、サードパーティのファイアウォールではなく組み込みの ONTAP ファイアウォールを使用するネットワーク構成では、ポート 111 で portmap サービス（rpcbind）へのアクセスが常に許可されていました。
- ONTAP 9.4 から ONTAP 9.6 までは、ファイアウォールポリシーを変更して、portmap サービスへのアクセスを許可するかどうかを LIF ごとに制御できます。
- ONTAP 9.7 以降では、portmap ファイアウォールサービスが廃止されています。代わりに、NFS サービスをサポートするすべての LIF に対して portmap ポートが自動的に開きます。
- ポートマップサービスは、ONTAP 9.4 ～ ONTAP 9.6\* のファイアウォールで設定可能です

このトピックの残りの部分では、ONTAP 9.4 リリースから ONTAP 9.6 リリースまでの portmap ファイアウォールサービスの設定方法について説明します。

設定によっては、特定のタイプの LIF、通常は管理 LIF とクラスタ間 LIF でのサービスへのアクセスを禁止できる場合があります。状況によっては、データ LIF からのアクセスも禁止できます。

#### 想定される動作

ONTAP 9.4 から ONTAP 9.6 への動作は、アップグレード時にシームレスに移行できるように設計されています。portmap サービスにすでに特定のタイプの LIF からアクセスしている場合、それらのタイプの LIF からは引き続きサービスにアクセスできます。ONTAP 9.3以前と同様に、ファイアウォール内でアクセス可能なサービスをLIFタイプのファイアウォールポリシーで指定できます。

この動作を有効にするには、クラスタ内のすべてのノードで ONTAP 9.4 ～ ONTAP 9.6 が実行されている必要があります。影響を受けるのはインバウンドトラフィックのみです。

新しいルールは次のとおりです。

- リリース 9.4 から 9.6 にアップグレードした場合、ONTAP は、既存のすべてのファイアウォールポリシー（デフォルトまたはカスタム）に portmap サービスを追加します。
- 新しいクラスタ ONTAP や IPspace を作成した場合、portmap サービスはデフォルトのデータポリシーにのみ追加され、デフォルトの管理ポリシーまたはクラスタ間ポリシーには追加されません。
- 必要に応じて、デフォルトまたはカスタムのポリシーに portmap サービスを追加したり削除したりできます。

#### portmapサービスを追加または削除する方法

SVM またはクラスタのファイアウォールポリシーに portmap サービスを追加する（ファイアウォール内でのアクセスを許可する）には、次のように入力します。

```
system services firewall policy create -vserver SVM -policy
mgmt|intercluster|data|custom -service portmap
```

SVM またはクラスタのファイアウォールポリシーから portmap サービスを削除する（ファイアウォール内でのアクセスを禁止する）には、次のように入力します。

```
system services firewall policy delete -vserver SVM -policy
mgmt|intercluster|data|custom -service portmap
```

既存の LIF にファイアウォールポリシーを適用するには、network interface modify コマンドを使用します。

コマンド構文全体については、を参照してください ["ONTAP 9 のコマンド"](#)。

ファイアウォールポリシーを作成して **LIF** に割り当てます

LIF を作成するときに、デフォルトのファイアウォールポリシーが割り当てられます。多くの場合、ファイアウォールのデフォルト設定をそのまま使用でき、変更する必要はありません。LIF にアクセスできるネットワークサービスや IP アドレスを変更する場合は、カスタムファイアウォールポリシーを作成して LIF に割り当てることができます。

このタスクについて

- でファイアウォールポリシーを作成することはできません policy 名前 data、intercluster、cluster、または `mgmt。

これらの値は、システム定義のファイアウォールポリシー用に予約されています。

- クラスタ LIF のファイアウォールポリシーを設定したり変更したりすることはできません。

クラスタ LIF のファイアウォールポリシーは、どのサービスタイプでも 0.0.0.0/0 に設定されます。

- ポリシーからサービスを削除する必要がある場合は、既存のファイアウォールポリシーを削除してから、新しいポリシーを作成する必要があります。
- クラスタで IPv6 が有効になっている場合は、IPv6 アドレスを使用してファイアウォールポリシーを作成できます。

IPv6を有効にすると、data、intercluster、および `mgmt ファイアウォールポリシーには、許可されるアドレスのリストにIPv6ワイルドカード:::/0が含まれます。

- System Manager を使用してクラスタ全体のデータ保護機能を設定するときは、許可されるアドレスのリストにクラスタ間 LIF の IP アドレスを含め、必ず、クラスタ間 LIF と会社所有のファイアウォールの両方で HTTPS サービスを許可してください。

デフォルトでは、が表示されます intercluster ファイアウォールポリシーは、すべてのIPアドレス（IPv6の場合は0.0.0.0/0、または:::/0）からのアクセスを許可し、HTTPS、NDMP、およびNDMPサービスは有効にします。このデフォルトポリシーを変更する場合や、クラスタ間 LIF の独自のファイアウォールポリシーを作成する場合は、許可されるアドレスのリストに各クラスタ間 LIF の IP アドレスを追加して、HTTPS サービスを有効にする必要があります。

- ONTAP 9.6 以降では、HTTPS および SSH のファイアウォールサービスはサポートされていません。

ONTAP 9.6では、management-https および management-ssh LIFサービスは、HTTPSとSSHの管理アクセスに使用できます。

手順

1. 特定の SVM の LIF で使用できるファイアウォールポリシーを作成します。

```
system services firewall policy create -vserver vserver_name -policy
policy_name -service network_service -allow-list ip_address/mask
```

ファイアウォールポリシーに追加するネットワークサービスごとに上記のコマンドを繰り返して、各サービスで許可される IP アドレスを指定できます。

2. を使用して、ポリシーが正しく追加されたことを確認します `system services firewall policy show` コマンドを実行します
3. ファイアウォールポリシーを LIF に適用します。

```
network interface modify -vserver vs1 -lif lif_name -firewall-policy policy_name
```

4. を使用して、ポリシーがLIFに正しく追加されたことを確認します `network interface show -fields firewall-policy` コマンドを実行します

ファイアウォールポリシーを作成して**LIF**に適用する例

次のコマンドは、 10.10 サブネットの IP アドレスからの HTTP および HTTPS プロトコルによるアクセスを許可する `data_http` というファイアウォールポリシーを作成し、 SVM vs1 の `data1` という LIF に適用してから、クラスタのすべてのファイアウォールポリシーを表示します。

```
system services firewall policy create -vserver vs1 -policy data_http  
-service http - allow-list 10.10.0.0/16
```

```
system services firewall policy show
```

Vserver	Policy	Service	Allowed
-----	-----	-----	-----
cluster-1			
	data		
		dns	0.0.0.0/0
		ndmp	0.0.0.0/0
		ndmps	0.0.0.0/0
cluster-1			
	intercluster		
		https	0.0.0.0/0
		ndmp	0.0.0.0/0
		ndmps	0.0.0.0/0
cluster-1			
	mgmt		
		dns	0.0.0.0/0
		http	0.0.0.0/0
		https	0.0.0.0/0
		ndmp	0.0.0.0/0
		ndmps	0.0.0.0/0
		ntp	0.0.0.0/0
		snmp	0.0.0.0/0
		ssh	0.0.0.0/0
vs1			
	data_http		
		http	10.10.0.0/16
		https	10.10.0.0/16

```
network interface modify -vserver vs1 -lif data1 -firewall-policy  
data_http
```

```
network interface show -fields firewall-policy
```

vserver	lif	firewall-policy
-----	-----	-----
Cluster	node1_clus_1	
Cluster	node1_clus_2	
Cluster	node2_clus_1	
Cluster	node2_clus_2	
cluster-1	cluster_mgmt	mgmt
cluster-1	node1_mgmt1	mgmt
cluster-1	node2_mgmt1	mgmt
vs1	data1	data_http
vs3	data2	data

## ファイアウォールサービスおよびポリシーを管理するためのコマンド

を使用できます `system services firewall` ファイアウォールサービスを管理するためのコマンド `system services firewall policy` ファイアウォールポリシーを管理するコマンド、および `network interface modify` LIFのファイアウォール設定を管理するコマンド。

状況	使用するコマンド
ファイアウォールサービスを有効または無効にします	<code>system services firewall modify</code>
ファイアウォールサービスの現在の設定を表示します	<code>system services firewall show</code>
ファイアウォールポリシーを作成するか、既存のファイアウォールポリシーにサービスを追加してください	<code>system services firewall policy create</code>
ファイアウォールポリシーを LIF に適用する	<code>network interface modify -lif lifname -firewall-policy</code>
ファイアウォールポリシーに関連付けられた IP アドレスとネットマスクを変更する	<code>system services firewall policy modify</code>
ファイアウォールポリシーに関する情報を表示する	<code>system services firewall policy show</code>
既存のファイアウォールポリシーとまったく同一の新しいポリシーを作成します	<code>system services firewall policy clone</code>
LIF で使用されていないファイアウォールポリシーを削除する	<code>system services firewall policy delete</code>

詳細については、のマニュアルページを参照してください `system services firewall`、`system services firewall policy` および `network interface modify` のコマンド "[ONTAP 9 のコマンド](#)"。

## QoSマーキング（クラスタ管理者のみ）

### QoSの概要

ネットワーク Quality of Service（QoS；サービス品質）マーキングを使用すると、ネットワークの状態に基づいて各トラフィックタイプに優先順位を付け、ネットワークリソースを効率的に利用できます。各 IPspace でサポートされるトラフィックタイプについて、送信 IP パケットの Differentiated Services Code Point（DSCP）値を設定できます。

## UC 準拠のための DSCP マーキング

デフォルトまたはユーザが指定した DSCP コードを使用して、特定のプロトコルの発信（出力）IP パケットトラフィックで Differentiated Services Code Point（DSCP）マーキングをイネーブルにできます。DSCP マーキングは、ネットワークトラフィックを分類および管理するためのメカニズムであり、Unified Capabilities（UC）準拠のコンポーネントです。

DSCP マーキング（\_QoS マーキング\_ または \_サービスマーキングの品質\_）は、IPspace、プロトコル、DSCP の値を指定することで有効になります。DSCP マーキングを適用できるプロトコルは、NFS、SMB、iSCSI、SnapMirror、NDMP、FTP、HTTP/HTTPS、SSH、Telnet、および SNMP。

特定のプロトコルに対して DSCP マーキングを有効にするときに DSCP 値を指定しない場合は、デフォルトが使用されます。

- データプロトコル/トラフィックのデフォルト値は 0x0A（10）です。
- 制御プロトコル/トラフィックのデフォルト値は 0x30（48）です。

## QoS マーキング値を変更します

IPspace ごとに、さまざまなプロトコルのサービス品質（QoS）マーキング値を変更できます。

作業を開始する前に

クラスタ内のすべてのノードで同じバージョンの ONTAP が実行されている必要があります。

ステップ

を使用して QoS マーキング値を変更します `network qos-marking modify` コマンドを実行します

- `-ipspace` パラメータは、QoS マーキングエントリを変更する IPspace を指定します。
- `-protocol` パラメータは、QoS マーキングエントリを変更するプロトコルを指定します。  
`network qos-marking modify` のマニュアルページに、プロトコルの指定可能な値が記載されています。
- `-dscp` パラメータには、Differentiated Services Code Point（DSCP）値を指定します。指定できる値の範囲は、0~63 です。
- `-is-enabled` パラメータを使用して、指定した IPspace 内の指定したプロトコルの QoS マーキングを有効または無効にします `-ipspace` パラメータ

次のコマンドは、デフォルトの IPspace の NFS プロトコルに対して QoS マーキングを有効にします。

```
network qos-marking modify -ipspace Default -protocol NFS -is-enabled true
```

次のコマンドは、デフォルトの IPspace の NFS プロトコルに対して DSCP 値を 20 に設定します。

```
network qos-marking modify -ipspace Default -protocol NFS -dscp 20
```

## QoS マーキング値を表示します

IPspace ごとに、さまざまなプロトコルの QoS マーキング値を表示できます。

### ステップ

を使用して、QoSマーキング値を表示します `network qos-marking show` コマンドを実行します

次のコマンドは、デフォルトの IPspace のすべてのプロトコルの QoS マーキングを表示します。

```
network qos-marking show -ipspace Default
IPspace          Protocol          DSCP    Enabled?
-----
Default
                  CIFS                10      false
                  FTP                48      false
                  HTTP-admin          48      false
                  HTTP-filesrv       10      false
                  NDMP                10      false
                  NFS                10      true
                  SNMP                48      false
                  SSH                48      false
                  SnapMirror       10      false
                  Telnet           48      false
                  iSCSI            10      false
11 entries were displayed.
```

## SNMPの管理（クラスタ管理者のみ）

### SNMPの概要

クラスタの SVM を監視するように SNMP を設定すると、問題を発生前に回避したり、発生時に対応したりすることができます。SNMP の管理には、SNMP ユーザを設定し、すべての SNMP イベントの SNMP トラップの送信先（管理ワークステーション）を設定する必要があります。データ LIF では、SNMP はデフォルトで無効になっています。

データ SVM に、読み取り専用 SNMP ユーザを作成して管理できます。データ LIF は、SVM で SNMP 要求を受信するように設定する必要があります。

SNMP ネットワーク管理ワークステーションまたはマネージャは、SVM SNMP エージェントに情報を照会できます。SNMP エージェントは情報を収集し、SNMP マネージャに転送します。SNMP エージェントは、特定のイベントが発生するたびにトラップ通知も生成します。SVM 上の SNMP エージェントの権限は読み取り専用権限であるため、設定操作や、トラップに回答して対処するために使用することはできません。ONTAP は SNMP バージョン v1、v2c、および v3 と互換性のある SNMP エージェントを備えています。SNMPv3 は、パスフレーズと暗号化を使用して高度なセキュリティを提供します。

ONTAP システムでの SNMP サポートの詳細については、を参照してください ["TR-4220 : 『SNMP Support](#)



in Data ONTAP 』"。

## MIBの概要

MIB（管理情報ベース）は、SNMP のオブジェクトとトラップが記述されたテキストファイルです。

MIB は、ストレージシステムの管理データの構造を表し、Object Identifier（OID；オブジェクト識別子）を含む階層状のネームスペースを使用します。各 OID は、SNMP を使用して読み取り可能な変数を識別します。

MIB は構成ファイルではなく、ONTAP はこれらのファイルを読み取らないため、SNMP 機能は MIB による影響を受けません。ONTAP には次の MIB ファイルがあります。

- ネットアップのカスタム MIB (netapp.mib)

ONTAP は、IPv6（RFC 2465）、TCP（RFC 4022）、UDP（RFC 4113）、および ICMP（RFC 2466）の MIB をサポートします。これらの MIB では IPv4 と IPv6 の両方のデータが表示されます。

ONTAP では、オブジェクト識別子（OID）とオブジェクトの簡略名の簡単な相互参照も提供されています。traps.dat ファイル。



ONTAP の MIB および「traps.dat」ファイルの最新バージョンは、NetApp Support Siteから入手できます。ただし、サポートサイトにあるファイルのバージョンが、お使いの ONTAP バージョンの SNMP 機能に必ずしも対応しているとは限りません。これらのファイルは、最新バージョンの ONTAP の SNMP 機能の評価用に提供されています。

## SNMP トラップ

SNMP トラップは、SNMP エージェントから SNMP マネージャに非同期通知として送信されたシステム監視情報をキャプチャします。

SNMP トラップには、標準、ビルトイン、およびユーザ定義の 3 種類があります。ユーザ定義トラップは、ONTAP ではサポートされていません。

トラップを使用して、MIB に定義された運用上のしきい値または障害を定期的にチェックすることができます。しきい値に到達するか、障害が検出されると、SNMP エージェントは、イベントを警告するメッセージ（トラップ）をトラップホストに送信します。



ONTAP は、SNMPv1 トラップ、および ONTAP 9.1 以降の SNMPv3 トラップをサポートしています。ONTAP は、SNMPv2c トラップおよび INFORM をサポートしていません。

## 標準 SNMP トラップ

これらのトラップは RFC 1215 で定義されています。ONTAP でサポートされている SNMP トラップは、coldStart、warmStart、linkDown、linkUp、および authenticationFailure の 5 つです。



authenticationFailure トラップは、デフォルトで無効になっています。を使用する必要があります。system snmp authtrap トラップをイネーブルにするコマンド。詳細については、次のマニュアルページを参照してください。"[ONTAP 9 のコマンド](#)"

## 組み込みの **SNMP** トラップ

ビルトイントラップは ONTAP に事前定義されたトラップで、イベントの発生時にトラップホストリストのネットワーク管理ステーションに自動的に送信されます。diskFailedShutdown、cpuTooBusy、volumeNearlyFull など、これらのトラップはカスタム MIB で定義されています。

各ビルトイントラップは、一意のトラップコードで識別されます。

## **SNMP** コミュニティを作成して **LIF** に割り当てます

SNMPv1 および SNMPv2c を使用する場合に管理ステーションと Storage Virtual Machine (SVM) 間の認証メカニズムとして機能する、SNMP コミュニティを作成できます。

データSVMにSNMPコミュニティを作成することで、などのコマンドを実行できます snmpwalk および snmpget (データLIF)。

このタスクについて

- ONTAP の新規インストールでは、SNMPv1 と SNMPv2c はデフォルトで無効になっています。

SNMPv1 と SNMPv2c は、SNMP コミュニティを作成すると有効になります。

- ONTAP でサポートされるのは、読み取り専用のコミュニティです。
- デフォルトでは、データLIFに割り当てられている「data」ファイアウォールポリシーでは、SNMPサービスがに設定されています deny。

新しいファイアウォールポリシーを作成し、SNMPサービスをに設定する必要があります allow データSVMのSNMPユーザを作成する場合。



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

- 管理 SVM とデータ SVM の両方に、SNMPv1 ユーザと SNMPv2c ユーザの SNMP コミュニティを作成できます。
- SVMはSNMP標準の一部ではないため、データLIFでのクエリにはネットアップのルートOID (1.3.6.1.4.1.789) を含める必要があります。次に例を示します。snmpwalk -v 2c -c snmpNFS 10.238.19.14 1.3.6.1.4.1.789。

## 手順

1. を使用してSNMPコミュニティを作成します system snmp community add コマンドを実行します次のコマンドは、管理 SVM cluster-1 に SNMP コミュニティを作成する方法を示しています。

```
system snmp community add -type ro -community-name comty1 -vserver cluster-1
```

次のコマンドは、データ SVM vs1 に SNMP コミュニティを作成する方法を示しています。

```
system snmp community add -type ro -community-name comty2 -vserver vs1
```

2. `system snmp community show` コマンドを使用して、コミュニティが作成されたことを確認します。

次のコマンドは、SNMPv1 および SNMPv2c 用に作成された 2 つのコミュニティを表示します。

```
system snmp community show
cluster-1
rocomty1
vs1
rocomty2
```

3. を使用して、「data」ファイアウォールポリシーでSNMPがサービスとして許可されているかどうかを確認します `system services firewall policy show` コマンドを実行します

次のコマンドは、デフォルトの「data」ファイアウォールポリシーでは SNMP サービスが許可されていないことを示しています（SNMP サービスは「mgmt」ファイアウォールポリシーでのみ許可されています）。

```
system services firewall policy show
Vserver Policy      Service      Allowed
-----
cluster-1
  data
    dns            0.0.0.0/0
    ndmp           0.0.0.0/0
    ndmps          0.0.0.0/0
cluster-1
  intercluster
    https          0.0.0.0/0
    ndmp           0.0.0.0/0
    ndmps          0.0.0.0/0
cluster-1
  mgmt
    dns            0.0.0.0/0
    http           0.0.0.0/0
    https          0.0.0.0/0
    ndmp           0.0.0.0/0
    ndmps          0.0.0.0/0
    ntp            0.0.0.0/0
    snmp           0.0.0.0/0
    ssh            0.0.0.0/0
```

4. を使用したアクセスを許可する新しいファイアウォールポリシーを作成します `snmp` を使用してサービス

を提供します system services firewall policy create コマンドを実行します

次のコマンドは、「data1」という名前の新しいデータファイアウォールポリシーを作成して、を許可します snmp

```
system services firewall policy create -policy data1 -service snmp
-vserver vs1 -allow-list 0.0.0.0/0
```

```
cluster-1::> system services firewall policy show -service snmp
```

Vserver	Policy	Service	Allowed
-----			
cluster-1			
	mgmt		
		snmp	0.0.0.0/0
vs1			
	data1		
		snmp	0.0.0.0/0

5. firewall-policy パラメータを指定して「network interface modify」コマンドを使用し、ファイアウォールポリシーをデータ LIF に適用します。

次のコマンドは、新しい「data1」ファイアウォールポリシーを LIF「datalif1」に割り当てます。

```
network interface modify -vserver vs1 -lif datalif1 -firewall-policy
data1
```

## クラスタに **SNMPv3** ユーザを設定します

SNMPv3 は、SNMPv1 や SNMPv2c に比べて安全なプロトコルです。SNMPv3 を使用するには、SNMP マネージャから SNMP ユーティリティを実行するための SNMPv3 ユーザを設定する必要があります。

### ステップ

「security login create コマンド」を使用して SNMPv3 ユーザを作成します。

次の情報を入力するように求められます。

- エンジン ID : デフォルトで、推奨値はローカルエンジン ID です
- 認証プロトコル
- 認証パスワード
- プライバシープロトコル
- プライバシープロトコルのパスワード

### 結果

SNMPv3 ユーザは、ユーザ名とパスワードを使用して SNMP マネージャからログインし、SNMP ユーティリティのコマンドを実行できます。

### SNMPv3 セキュリティパラメータ

SNMPv3 には認証機能が備わっており、この機能を選択すると、コマンドの呼び出し時に、ユーザ名、認証プロトコル、認証キー、および必要なセキュリティレベルの入力が必要になります。

次の表に、SNMPv3 セキュリティパラメータを示します。

パラメータ	コマンドラインオプション	説明
エンジン ID	-e engineID	SNMP エージェントのエンジン ID。デフォルト値はローカルのエンジン ID（推奨）です。
securityName の略	-u 名	ユーザ名は 32 文字以内にする必要があります。
authProtocol の略	• a { none	md5
sha	SHA-256 }	認証タイプには、none、md5、SHA、または SHA-256 を指定できます。
authKey	• パスフレーズ	8 文字以上の長さのパスフレーズ
セキュリティレベル	-l { authNoPriv	AuthPriv
noAuthNoPriv }	セキュリティレベルには、「Authentication、No Privacy」、「Authentication、Privacy」、「No Authentication、No Authentication」のいずれかを指定できます。プライバシーなし。	privProtocol の略
-x { none	des	aes128 }
プライバシープロトコルには、none、des、または aes128 を指定できます	プライベートパスワード	-X パスワード

### さまざまなセキュリティレベルの例

次に、さまざまなセキュリティレベルで作成された SNMPv3 ユーザが、などの SNMP クライアント側コマンドを使用する例を示します。`snmpwalk` をクリックして、クラスタオブジェクトを照会します。

パフォーマンスを高めるには、テーブルから単一または少数のオブジェクトを取得するのではなく、テーブル

内のすべてのオブジェクトを取得します。



を使用する必要があります snmpwalk 認証プロトコルがSHAの場合は5.3.1以降。

セキュリティレベル: **authPriv**

authPriv セキュリティレベルの SNMPv3 ユーザを作成した場合の出力を次に示します。

```
security login create -user-or-group-name snmpv3user -application snmp
-authentication-method usm
Enter the authoritative entity's EngineID [local EngineID]:
Which authentication protocol do you want to choose (none, md5, sha, sha2-
256) [none]: md5

Enter the authentication protocol password (minimum 8 characters long):
Enter the authentication protocol password again:
Which privacy protocol do you want to choose (none, des, aes128) [none]:
des
Enter privacy protocol password (minimum 8 characters long):
Enter privacy protocol password again:
```

## FIPS モード

```
security login create -username snmpv3user -application snmp -authmethod
usm
Enter the authoritative entity's EngineID [local EngineID]:
Which authentication protocol do you want to choose (sha, sha2-256) [sha]

Enter authentication protocol password (minimum 8 characters long):
Enter authentication protocol password again:
Which privacy protocol do you want to choose (aes128) [aes128]:
Enter privacy protocol password (minimum 8 characters long):
Enter privacy protocol password again:
```

## snmpwalk テストを実行します

この SNMPv3 ユーザが snmpwalk コマンドを実行した場合の出力を次に示します。

パフォーマンスを高めるには、テーブルから単一または少数のオブジェクトを取得するのではなく、テーブル内のすべてのオブジェクトを取得します。

```
$ snmpwalk -v 3 -u snmpv3user -a SHA -A password1! -x DES -X password1! -l
authPriv 192.0.2.62 .1.3.6.1.4.1.789.1.5.8.1.2
Enterprises.789.1.5.8.1.2.1028 = "vol0"
Enterprises.789.1.5.8.1.2.1032 = "vol0"
Enterprises.789.1.5.8.1.2.1038 = "root_vs0"
Enterprises.789.1.5.8.1.2.1042 = "root_vstrap"
Enterprises.789.1.5.8.1.2.1064 = "vol1"
```

セキュリティレベル: **authNoPriv**

authNoPriv セキュリティレベルの SNMPv3 ユーザを作成した場合の出力を次に示します。

```
security login create -username snmpv3user1 -application snmp -authmethod
usm -role admin
Enter the authoritative entity's EngineID [local EngineID]:
Which authentication protocol do you want to choose (none, md5, sha)
[none]: md5
```

## FIPS モード

FIPSでは、プライバシープロトコルに\* none \*を選択することはできません。そのため、authNoPriv SNMPv3 ユーザをFIPSモードで設定することはできません。

## snmpwalk テストを実行します

この SNMPv3 ユーザが snmpwalk コマンドを実行した場合の出力を次に示します。

パフォーマンスを高めるには、テーブルから単一または少数のオブジェクトを取得するのではなく、テーブル内のすべてのオブジェクトを取得します。

```
$ snmpwalk -v 3 -u snmpv3user1 -a MD5 -A password1! -l authNoPriv
192.0.2.62 .1.3.6.1.4.1.789.1.5.8.1.2
Enterprises.789.1.5.8.1.2.1028 = "vol0"
Enterprises.789.1.5.8.1.2.1032 = "vol0"
Enterprises.789.1.5.8.1.2.1038 = "root_vs0"
Enterprises.789.1.5.8.1.2.1042 = "root_vstrap"
Enterprises.789.1.5.8.1.2.1064 = "vol1"
```

セキュリティレベル: **noAuthNoPriv**

noAuthNoPriv セキュリティレベルの SNMPv3 ユーザを作成した場合の出力を次に示します。

```
security login create -username snmpv3user2 -application snmp -authmethod
usm -role admin
Enter the authoritative entity's EngineID [local EngineID]:
Which authentication protocol do you want to choose (none, md5, sha)
[none]: none
```

## FIPS モード

FIPSでは、プライバシープロトコルに\* none \*を選択することはできません。

## snmpwalk テストを実行します

この SNMPv3 ユーザが snmpwalk コマンドを実行した場合の出力を次に示します。

パフォーマンスを高めるには、テーブルから単一または少数のオブジェクトを取得するのではなく、テーブル内のすべてのオブジェクトを取得します。

```
$ snmpwalk -v 3 -u snmpv3user2 -l noAuthNoPriv 192.0.2.62
.1.3.6.1.4.1.789.1.5.8.1.2
Enterprises.789.1.5.8.1.2.1028 = "vol0"
Enterprises.789.1.5.8.1.2.1032 = "vol0"
Enterprises.789.1.5.8.1.2.1038 = "root_vs0"
Enterprises.789.1.5.8.1.2.1042 = "root_vstrap"
Enterprises.789.1.5.8.1.2.1064 = "vol1"
```

## SNMP 通知を受信するトラップホストを設定します

クラスタで SNMP トラップが生成されたときに通知（SNMP トラップ PDU）を受信するトラップホスト（SNMP マネージャ）を設定できます。SNMP トラップホストのホスト名または IP アドレス（IPv4 または IPv6）を指定できます。

作業を開始する前に

- ・クラスタで SNMP トラップと SNMP トラップが有効になっている必要があります。



SNMP トラップと SNMP トラップはデフォルトで有効になっています。

- ・クラスタでトラップホスト名を解決するように DNS が設定されている必要があります。
- ・IPv6 アドレスを使用して SNMP トラップホストを設定するには、クラスタで IPv6 を有効にする必要があります。
- ・ONTAP 9.1 以降のバージョンでは、トラップホストの作成時に、事前定義されているユーザベースのセキュリティモデル（USM）の認証とプライバシーのクレデンシャルを指定しておく必要があります。

## ステップ

SNMP トラップホストを追加します。



```
system snmp traphost add
```



トラップを送信できるのは、少なくとも 1 つの SNMP 管理ステーションがトラップホストとして指定されているときのみです。

次のコマンドは、yyy.example.com という新しい SNMPv3 トラップホストを既知の USM ユーザとともに追加します。

```
system snmp traphost add -peer-address yyy.example.com -usm-username  
MyUsmUser
```

次のコマンドは、トラップホストの IPv6 アドレスを指定して、そのホストを追加します。

```
system snmp traphost add -peer-address 2001:0db8:1:1:209:6bff:feae:6d67
```

## SNMP を管理するためのコマンド

を使用できます `system snmp` SNMP、トラップ、およびトラップホストを管理するコマンド。を使用できます `security SVM`ごとにSNMPユーザを管理するコマンド。を使用できます `event` SNMPトラップに関連するイベントを管理するコマンド。

### SNMP を設定するためのコマンド

状況	使用するコマンド
クラスタで SNMP を有効にします	<pre>options -option-name snmp.enable -option-value on</pre> <p>管理（mgmt）ファイアウォールポリシーで SNMP サービスが許可されている必要があります。SNMP が許可されているかどうかを確認するには、<code>system services firewall policy show</code> コマンドを使用します。</p>
クラスタで SNMP を無効にします	<pre>options -option-name snmp.enable -option-value off</pre>

### SNMP v1、v2c、および v3 ユーザを管理するコマンド

状況	使用するコマンド
SNMP ユーザを設定する	<pre>security login create</pre>

SNMP ユーザを表示します	<code>security snmpusers</code> and <code>security login show -application snmp</code>
SNMP ユーザを削除する	<code>security login delete</code>
SNMP ユーザのログイン方法のアクセス制御ロール名を変更します	<code>security login modify</code>

#### 連絡先と場所の情報を提供するコマンド

状況	使用するコマンド
クラスタの連絡先の詳細を表示または変更する	<code>system snmp contact</code>
クラスタの場所の詳細を表示または変更する	<code>system snmp location</code>

#### SNMP コミュニティを管理するコマンド

状況	使用するコマンド
1 つの SVM 、またはクラスタのすべての SVM に読み取り専用（ro）コミュニティを追加する	<code>system snmp community add</code>
1 つまたはすべてのコミュニティを削除します	<code>system snmp community delete</code>
すべてのコミュニティのリストを表示します	<code>system snmp community show</code>

SVMはSNMP標準の一部ではないため、データLIFでのクエリにはネットアップのルートOID（1.3.6.1.4.1.789）を含める必要があります。次に例を示します。 `snmpwalk -v 2c -c snmpNFS 10.238.19.14 1.3.6.1.4.1.789`。

#### SNMP オプションの値を表示するコマンド

状況	使用するコマンド
クラスタの連絡先、連絡先、トラップホストを送信するようにクラスタが設定されているかどうか、トラップホストのリスト、コミュニティとアクセス制御の種類のリストなど、すべての SNMP オプションの現在の値を表示します	<code>system snmp show</code>

#### SNMP のトラップおよびトラップホストを管理するコマンド

状況	使用するコマンド
----	----------

クラスタからの SNMP トラップの送信を有効にします	<code>system snmp init -init 1</code>
クラスタからの SNMP トラップの送信を無効にします	<code>system snmp init -init 0</code>
クラスタの特定のイベントに関する SNMP 通知を受信するトラップホストを追加します	<code>system snmp traphost add</code>
トラップホストを削除します	<code>system snmp traphost delete</code>
トラップホストのリストを表示します	<code>system snmp traphost show</code>

## SNMP トラップに関連するイベントを管理するコマンド

状況	使用するコマンド
SNMP トラップ（ビルトイン）が生成されたイベントを表示します	<code>event route show</code>  を使用します <code>-snmp-support true</code> SNMP 関連のイベントのみを表示するためのパラメータ。  を使用します <code>instance -messagename &lt;message&gt;</code> パラメータを使用して、イベントが発生した理由と対処方法の詳細な概要を表示します。  個々の SNMP トラップイベントを特定の送信先トラップホストにルーティングすることはできません。すべての SNMP トラップイベントが、すべての送信先トラップホストに送信されます。
SNMP トラップ履歴レコードのリストを表示します。 SNMP トラップに送信されたイベント通知です	<code>event snmphistory show</code>
SNMP トラップ履歴レコードを削除します	<code>event snmphistory delete</code>

詳細については、を参照してください `system snmp`、`security` および `event` コマンドについては、マニュアルページを参照してください。 ["ONTAP 9 のコマンド"](#)

## SVM のルーティングを管理します

### SVM ルーティングの概要

SVM のルーティングテーブルは、SVM がデスティネーションとの通信に使用するネットワークパスを決めるものです。ルーティングテーブルがどのように機能するかを理解し、ネットワークの問題が発生する前に防止することが重要です。

ルーティングルールは次のとおりです。

- ONTAP は、使用可能な最も限定的なルートでトラフィックをルーティングします。
- より限定的なルートがない場合、ONTAP は最後の手段としてデフォルトゲートウェイルート（0 ビットのネットマスク）でトラフィックをルーティングします。

デスティネーション、ネットマスク、メトリックが同じルートが複数ある場合、リブート後またはアップグレード後に同じルートが使用される保証はありません。複数のデフォルトルートを設定している場合、これは特に問題です。

SVM にはデフォルトルートを 1 つだけ設定することを推奨します。システム停止を回避するには、より限定的なルートでは到達できないネットワークアドレスにデフォルトルートが到達できることを確認する必要があります。詳細については、技術情報アートを参照してください ["SU134 : clustered ONTAP で誤ったルーティング設定が行われるとネットワークアクセスが中断される可能性があります"](#)

静的ルートを作成します。

Storage Virtual Machine（SVM）内で静的ルートを作成して、LIF が発信トラフィックをネットワークでどのように取り扱うかを制御できます。

SVM に関連するルートエントリを作成すると、そのルートが、ゲートウェイと同じサブネットにあり、指定した SVM に所有されているすべての LIF で使用されます。

ステップ

を使用します `network route create` ルートを作成するコマンド。

```
network route create -vserver vs0 -destination 0.0.0.0/0 -gateway
10.61.208.1
```

マルチパスルーティングを有効にします

複数のルートが同じメトリックを宛先に持つ場合、送信トラフィックには 1 つのルートのみが選択されます。これにより、他のルートが発信トラフィックの送信に使用されなくなります。マルチパスルーティングを有効にして、使用可能なすべてのルートを使用して負荷を分散することができます。

手順

1. advanced 権限レベルにログインします。

```
set -privilege advanced
```

2. マルチパスルーティングを有効にします。

```
network options multipath-routing modify -is-enabled true
```

クラスタ内のすべてのノードでマルチパスルーティングが有効になります。

```
network options multipath-routing modify -is-enabled true
```

## 静的ルートを削除します

不要な静的ルートを Storage Virtual Machine（SVM）から削除できます。

### ステップ

を使用します `network route delete` 静的ルートを削除するコマンド。

このコマンドの詳細については、を参照してください `network route` マニュアルページ：["ONTAP 9 のコマンド"](#)。

次の例では、SVM vs0 に関連付けられている、ゲートウェイ 10.63.0.1 とデスティネーション IP アドレス 0.0.0.0/0 の静的ルートを削除しています。

```
network route delete -vserver vs0 -gateway 10.63.0.1 -destination
0.0.0.0/0
```

## ルーティング情報を表示します

クラスタの各 SVM のルーティング設定に関する情報を表示することができます。この情報は、クライアントアプリケーションまたはサービスとクラスタ内のノード上の LIF との接続に関連するルーティングの問題を診断するのに役立ちます。

### 手順

1. を使用します `network route show` コマンドを使用して、1つ以上のSVM内のルートを表示します。次の例は、vs0 という SVM に設定されているルートを表示しています。

```
network route show
(network route show)
Vserver          Destination      Gateway          Metric
-----
vs0
                  0.0.0.0/0       172.17.178.1    20
```

2. を使用します `network route show-lifs` コマンドを使用して、1つ以上のSVM内のルートとLIFの関連付けを表示します。

次の例は、vs0 という SVM が所有しているルートと LIF の関連付けを表示しています。

```
network route show-lifs
(network route show-lifs)
```

```
Vserver: vs0
```

Destination	Gateway	Logical Interfaces
-----	-----	-----
0.0.0.0/0	172.17.178.1	cluster_mgmt, LIF-b-01_mgmt1, LIF-b-02_mgmt1

3. 使用します `network route active-entry show` コマンドを使用して、1つ以上のノード、SVM、サブネットに設定されているルート、または指定したデスティネーションに一致するルートを表示します。

次の例は、特定の SVM に設定されているすべてのルートを表示しています。

```
network route active-entry show -vserver Data0
```

```
Vserver: Data0
```

```
Node: node-1
```

```
Subnet Group: 0.0.0.0/0
```

Destination	Gateway	Interface	Metric	Flags
-----	-----	-----	-----	-----
127.0.0.1	127.0.0.1	lo	10	UHS
127.0.10.1	127.0.20.1	losk	10	UHS
127.0.20.1	127.0.20.1	losk	10	UHS

```
Vserver: Data0
```

```
Node: node-1
```

```
Subnet Group: fd20:8b1e:b255:814e::/64
```

Destination	Gateway	Interface	Metric	Flags
-----	-----	-----	-----	-----
default	fd20:8b1e:b255:814e::1	e0d	20	UGS
fd20:8b1e:b255:814e::/64	link#4	e0d	0	UC

```
Vserver: Data0
```

```
Node: node-2
```

```
Subnet Group: 0.0.0.0/0
```

Destination	Gateway	Interface	Metric	Flags
-----	-----	-----	-----	-----
127.0.0.1	127.0.0.1	lo	10	UHS

```
Vserver: Data0
```

```

Node: node-2
Subnet Group: 0.0.0.0/0
Destination          Gateway          Interface    Metric    Flags
-----
127.0.10.1           127.0.20.1      losk         10        UHS
127.0.20.1           127.0.20.1      losk         10        UHS

Vserver: Data0
Node: node-2
Subnet Group: fd20:8b1e:b255:814e::/64
Destination          Gateway          Interface    Metric    Flags
-----
default              fd20:8b1e:b255:814e::1
                                e0d            20        UGS

fd20:8b1e:b255:814e::/64
                                link#4         e0d         0         UC
fd20:8b1e:b255:814e::1 link#4          e0d         0         UHL
11 entries were displayed.

```

## ルーティングテーブルからダイナミックルートを削除します

IPv4 と IPv6 の ICMP リダイレクトを受信すると、動的ルートがルーティングテーブルに追加されます。デフォルトでは、動的ルートは 300 秒後に削除されます。動的ルートを維持する時間を変更する場合は、タイムアウト値を変更できます。

このタスクについて

0~65、535 秒のタイムアウト値を設定できます。値を 0 に設定すると、ルートは無期限になります。動的ルートを削除すると、無効なルートの永続性が原因で接続が切断されるのを防ぐことができます。

手順

1. 現在のタイムアウト値を表示します。

- IPv4 の場合：

```
network tuning icmp show
```

- IPv6 の場合：

```
network tuning icmp6 show
```

2. タイムアウト値を変更します。

- IPv4 の場合：

```
network tuning icmp modify -node node_name -redirect-timeout
timeout_value
```

◦ IPv6の場合：

```
network tuning icmp6 modify -node node_name -redirect-v6-timeout
timeout_value
```

3. タイムアウト値が正しく変更されたことを確認します。

◦ IPv4 の場合：

```
network tuning icmp show
```

◦ IPv6の場合：

```
network tuning icmp6 show
```

## ネットワーク情報を表示します

### ネットワーク情報の概要を表示する

CLIを使用すると、ポート、LIF、ルート、フェイルオーバールール、フェイルオーバーグループ、ファイアウォールルール、DNS、NIS、および接続。ONTAP 9.8以降では、使用しているネットワークについてSystem Managerに表示されるデータもダウンロードできます。

この情報は、ネットワークの再設定やクラスタのトラブルシューティングを行うときに役立ちます。

クラスタ管理者の場合は、使用可能なネットワーク情報をすべて表示できます。SVM 管理者は、割り当てられている SVM に関連する情報のみを表示できます。

System Managerの\_リスト表示\_に情報を表示するときに\*[ダウンロード]\*をクリックすると、表示されているオブジェクトのリストがダウンロードされます。

- このリストは、カンマ区切り値（CSV）形式でダウンロードされます。
- 表示されている列のデータのみがダウンロードされます。
- CSV ファイル名は、オブジェクト名とタイムスタンプでフォーマットされます。

### ネットワークポートの情報を表示します

クラスタ内の特定のポート、またはすべてのノードのすべてのポートに関する情報を表



示できます。

このタスクについて

次の情報が表示されます。

- ノード名
- ポート名
- IPspace 名
- ブロードキャストドメイン名
- リンクステータス（up または down）
- MTU を設定します
- ポート速度の設定と動作ステータス（毎秒 1 ギガビットまたは 10 ギガビット）
- 自動ネゴシエーション設定（true または false）
- 二重モードと動作ステータス（half または full）
- ポートのインターフェイスグループ（該当する場合）
- ポートの VLAN タグ情報（該当する場合）
- ポートのヘルスステータス（「正常」または「デグレード」）
- ポートがデグレードとマークされた理由

該当するデータがないフィールドにはという値が表示されます。たとえば、アクティブでないポートの二重モードの動作ステータスや速度の情報はありません。

#### ステップ

を使用して、ネットワークポートの情報を表示します `network port show` コマンドを実行します

各ポートの詳細情報を表示するには、を指定します `-instance` パラメータを指定するか、を使用してフィールド名を指定して特定の情報を取得します `-fields` パラメータ

```
network port show
```

```
Node: node1
```

```
Ignore
```

						Speed(Mbps)	Health
Health							
Port	IPspace	Broadcast	Domain	Link	MTU	Admin/Oper	Status
Status							
-----	-----	-----	----	----	----	-----	-----
-----							
e0a	Cluster	Cluster		up	9000	auto/1000	healthy
false							
e0b	Cluster	Cluster		up	9000	auto/1000	healthy
false							
e0c	Default	Default		up	1500	auto/1000	degraded
false							
e0d	Default	Default		up	1500	auto/1000	degraded
true							

```
Node: node2
```

```
Ignore
```

						Speed(Mbps)	Health
Health							
Port	IPspace	Broadcast	Domain	Link	MTU	Admin/Oper	Status
Status							
-----	-----	-----	----	----	----	-----	-----
-----							
e0a	Cluster	Cluster		up	9000	auto/1000	healthy
false							
e0b	Cluster	Cluster		up	9000	auto/1000	healthy
false							
e0c	Default	Default		up	1500	auto/1000	healthy
false							
e0d	Default	Default		up	1500	auto/1000	healthy
false							

```
8 entries were displayed.
```

## VLAN に関する情報を表示する（クラスタ管理者のみ）

クラスタ内の特定の VLAN またはすべての VLAN の情報を表示できます。

このタスクについて

を指定すると、各VLANの詳細情報を表示できます -instance パラメータでフィールド名を指定すると、特定の情報を表示できます -fields パラメータ

## ステップ

を使用して、VLANに関する情報を表示します `network port vlan show` コマンドを実行します 次のコマンドは、クラスタ内のすべての VLAN に関する情報を表示します。

```
network port vlan show
```

Node	VLAN Name	Port	Network VLAN ID	Network MAC Address
cluster-1-01				
	a0a-10	a0a	10	02:a0:98:06:10:b2
	a0a-20	a0a	20	02:a0:98:06:10:b2
	a0a-30	a0a	30	02:a0:98:06:10:b2
	a0a-40	a0a	40	02:a0:98:06:10:b2
	a0a-50	a0a	50	02:a0:98:06:10:b2
cluster-1-02				
	a0a-10	a0a	10	02:a0:98:06:10:ca
	a0a-20	a0a	20	02:a0:98:06:10:ca
	a0a-30	a0a	30	02:a0:98:06:10:ca
	a0a-40	a0a	40	02:a0:98:06:10:ca
	a0a-50	a0a	50	02:a0:98:06:10:ca

## インターフェイスグループ情報の表示（クラスタ管理者のみ）

インターフェイスグループに関する情報を表示して、その設定を確認できます。

このタスクについて

次の情報が表示されます。

- インターフェイスグループが配置されているノード
- インターフェイスグループに含まれているネットワークポートのリスト
- インターフェイスグループの名前
- 分散機能（MAC、IP、ポート、またはシーケンシャル）
- インターフェイスグループの Media Access Control（MAC；メディアアクセス制御）アドレス
- ポートのアクティビティステータス。集約されたポートがアクティブであるかどうか（すべてのポートがアクティブであるかどうか）、アクティブであるポートがないかどうか（一部のポートがアクティブであるかどうか）、アクティブでないかどうかを示します

## ステップ

を使用して、インターフェイスグループに関する情報を表示します `network port ifgrp show` コマンドを実行します

各ノードの詳細情報を表示するには、を指定します `-instance` パラメータでフィールド名を指定すると、特定の情報を表示できます `-fields` パラメータ

次のコマンドは、クラスタ内のすべてのインターフェイスグループに関する情報を表示します。

```
network port ifgrp show
```

	Port	Distribution		Active	
Node	IfGrp	Function	MAC Address	Ports	Ports
-----	-----	-----	-----	-----	-----
cluster-1-01	a0a	ip	02:a0:98:06:10:b2	full	e7a, e7b
cluster-1-02	a0a	sequential	02:a0:98:06:10:ca	full	e7a, e7b
cluster-1-03	a0a	port	02:a0:98:08:5b:66	full	e7a, e7b
cluster-1-04	a0a	mac	02:a0:98:08:61:4e	full	e7a, e7b

次のコマンドは、1つのノードのインターフェイスグループの詳細情報を表示します。

```
network port ifgrp show -instance -node cluster-1-01
```

```

Node: cluster-1-01
Interface Group Name: a0a
Distribution Function: ip
Create Policy: multimode
MAC Address: 02:a0:98:06:10:b2
Port Participation: full
Network Ports: e7a, e7b
Up Ports: e7a, e7b
Down Ports: -

```

## LIF 情報を表示します

LIF に関する詳細情報を表示して、その設定を確認できます。

この情報は、IP アドレスが重複していないか、ネットワークポートが正しいサブネットに属しているかなど、LIF の基本的な問題を診断するのに便利です。Storage Virtual Machine (SVM) 管理者は、SVM に関連付けられている LIF の情報だけを表示できます。

このタスクについて

次の情報が表示されます。

- LIF に関連付けられている IP アドレス
- LIF の管理ステータス
- LIF の動作ステータス

データ LIF の動作ステータスは、そのデータ LIF が関連付けられている SVM のステータスによって決まります。SVM が停止すると、LIF の動作ステータスが down に変わります。SVM が再び起動すると、動

作ステータスは up に変わります

- LIF が配置されているノードとポート

該当するデータがないフィールド（ステータスの詳しい情報がない場合など）については、と表示されます -。

ステップ

network interface show コマンドを使用して、LIF の情報を表示します。

各 LIF の詳しい情報を表示するには、-instance パラメータを指定します。特定の情報を表示するには、-fields パラメータを使用してフィールド名を指定します。

次のコマンドは、クラスタ内のすべての LIF に関する一般的な情報を表示します。

# network interface show

Vserver	Logical Interface	Status Admin/Oper	Network Address/Mask	Current Node	Current Is Port
Home					
-----	-----	-----	-----	-----	-----
example					
	lif1	up/up	192.0.2.129/22	node-01	e0d
false					
node	cluster_mgmt	up/up	192.0.2.3/20	node-02	e0c
false					
node-01	clus1	up/up	192.0.2.65/18	node-01	e0a
true					
	clus2	up/up	192.0.2.66/18	node-01	e0b
true					
	mgmt1	up/up	192.0.2.1/20	node-01	e0c
true					
node-02	clus1	up/up	192.0.2.67/18	node-02	e0a
true					
	clus2	up/up	192.0.2.68/18	node-02	e0b
true					
	mgmt2	up/up	192.0.2.2/20	node-02	e0d
true					
vs1	d1	up/up	192.0.2.130/21	node-01	e0d
false					
	d2	up/up	192.0.2.131/21	node-01	e0d
true					
	data3	up/up	192.0.2.132/20	node-02	e0c
true					

次のコマンドは、1つの LIF に関する詳細情報を表示します。

```
network interface show -lif data1 -instance

Vserver Name: vs1
Logical Interface Name: data1
Role: data
Data Protocol: nfs,cifs
Home Node: node-01
Home Port: e0c
Current Node: node-03
Current Port: e0c
Operational Status: up
Extended Status: -
Is Home: false
Network Address: 192.0.2.128
Netmask: 255.255.192.0
Bits in the Netmask: 18
IPv4 Link Local: -
Subnet Name: -
Administrative Status: up
Failover Policy: local-only
Firewall Policy: data
Auto Revert: false
Fully Qualified DNS Zone Name: xxx.example.com
DNS Query Listen Enable: false
Failover Group Name: Default
FCP WWPN: -
Address family: ipv4
Comment: -
IPspace of LIF: Default
```

ルーティング情報を表示します

SVM 内のルートに関する情報を表示できます。

ステップ

表示するルーティング情報のタイプに応じて、該当するコマンドを入力します。

表示する情報	入力するコマンド
SVM の静的ルート	network route show
SVM の各ルートの LIF	network route show-lifs

各ルートの詳細情報を表示するには、を指定します `-instance` パラメータ次のコマンドは、`cluster-1` の SVM 内の静的ルートを表示します。

```
network route show
Vserver          Destination      Gateway          Metric
-----
Cluster
0.0.0.0/0        10.63.0.1       10
cluster-1
0.0.0.0/0        198.51.9.1      10
vs1
0.0.0.0/0        192.0.2.1       20
vs3
0.0.0.0/0        192.0.2.1       20
```

次のコマンドは、`cluster-1` のすべての SVM 内の静的ルートと論理インターフェイス（LIF）の関連付けを表示します。

```
network route show-lifs
Vserver: Cluster
Destination      Gateway          Logical Interfaces
-----
0.0.0.0/0        10.63.0.1       -

Vserver: cluster-1
Destination      Gateway          Logical Interfaces
-----
0.0.0.0/0        198.51.9.1      cluster_mgmt,
cluster-1_mgmt1,

Vserver: vs1
Destination      Gateway          Logical Interfaces
-----
0.0.0.0/0        192.0.2.1       data1_1, data1_2

Vserver: vs3
Destination      Gateway          Logical Interfaces
-----
0.0.0.0/0        192.0.2.1       data2_1, data2_2
```

## DNS hosts テーブルエントリを表示する（クラスタ管理者のみ）

DNS hosts テーブルエントリは、ホスト名と IP アドレスのマッピングです。クラスタ内のすべての SVM のホスト名およびエイリアス名と IP アドレスのマッピングを表示する



ことができます。

#### ステップ

`vserver services name-service dns hosts show` コマンドを使用して、すべての SVM のホスト名エントリを表示します。

次の例は、ホストテーブルエントリを表示します。

```
vserver services name-service dns hosts show
Vserver      Address      Hostname      Aliases
-----
cluster-1
              10.72.219.36  lnx219-36     -
vs1
              10.72.219.37  lnx219-37     lnx219-37.example.com
```

使用できます `vserver services name-service dns` コマンドを使用してSVMでDNSを有効にし、ホスト名解決にDNSを使用するように設定します。ホスト名は外部 DNS サーバを使用して解決されます。

## DNS ドメイン設定を表示します

クラスタ内の 1 つ以上の Storage Virtual Machine （ SVM ） の DNS ドメイン設定を表示して、正しく設定されているかどうかを確認できます。

#### ステップ

を使用してDNSドメイン設定を表示します `vserver services name-service dns show` コマンドを実行します

次のコマンドは、クラスタ内のすべての SVM の DNS 設定を表示します。

```
vserver services name-service dns show
Vserver      State      Domains      Name Servers
-----
cluster-1    enabled    xyz.company.com  192.56.0.129,
192.56.0.130
vs1          enabled    xyz.company.com  192.56.0.129,
192.56.0.130
vs2          enabled    xyz.company.com  192.56.0.129,
192.56.0.130
vs3          enabled    xyz.company.com  192.56.0.129,
192.56.0.130
```

次のコマンドは、 SVM vs1 の DNS 設定の詳細を表示します。

```
vserver services name-service dns show -vserver vs1
Vserver: vs1
Domains: xyz.company.com
Name Servers: 192.56.0.129, 192.56.0.130
Enable/Disable DNS: enabled
Timeout (secs): 2
Maximum Attempts: 1
```

## フェイルオーバーグループに関する情報を表示します

フェイルオーバーグループに関する情報を表示することができます。これには、各フェイルオーバーグループ内のノードとポートのリスト、フェイルオーバーの有効 / 無効、各 LIF に適用されているフェイルオーバーポリシーの種類が含まれます。

### 手順

1. を使用して、各フェイルオーバーグループのターゲットポートを表示します `network interface failover-groups show` コマンドを実行します

次のコマンドは、2 ノードクラスタのすべてのフェイルオーバーグループに関する情報を表示します。

```
network interface failover-groups show
Vserver      Group      Failover
-----
Cluster
vs1          Cluster
              cluster1-01:e0a, cluster1-01:e0b,
              cluster1-02:e0a, cluster1-02:e0b
vs1          Default
              cluster1-01:e0c, cluster1-01:e0d,
              cluster1-01:e0e, cluster1-02:e0c,
              cluster1-02:e0d, cluster1-02:e0e
```

2. を使用して、特定のフェイルオーバーグループのターゲットポートとブロードキャストドメインを表示します `network interface failover-groups show` コマンドを実行します

次のコマンドは、SVM vs4 の data12 というフェイルオーバーグループに関する詳しい情報を表示します。

```
network interface failover-groups show -vserver vs4 -failover-group data12
```

```
Vserver Name: vs4
Failover Group Name: data12
Failover Targets: cluster1-01:e0f, cluster1-01:e0g, cluster1-02:e0f,
                  cluster1-02:e0g
Broadcast Domain: Default
```

3. を使用して、すべてのLIFで使用されているフェイルオーバー設定を表示します network interface show コマンドを実行します

次のコマンドは、各 LIF で使用されているフェイルオーバーポリシーとフェイルオーバーグループを表示します。

```
network interface show -vserver * -lif * -fields failover-
group,failover-policy
vserver    lif                failover-policy    failover-group
-----
Cluster    cluster1-01_clus_1  local-only         Cluster
Cluster    cluster1-01_clus_2  local-only         Cluster
Cluster    cluster1-02_clus_1  local-only         Cluster
Cluster    cluster1-02_clus_2  local-only         Cluster
cluster1    cluster_mgmt        broadcast-domain-wide Default
cluster1    cluster1-01_mgmt1   local-only         Default
cluster1    cluster1-02_mgmt1   local-only         Default
vs1         data1               disabled           Default
vs3         data2               system-defined     group2
```

## LIF のフェイルオーバーターゲットを表示します

LIF のフェイルオーバーポリシーとフェイルオーバーグループが正しく設定されているかどうかを確認しなければならない場合があります。フェイルオーバールールを間違っ  
て設定しないように、1 つまたはすべての LIF のフェイルオーバーターゲットを表示で  
きます。

このタスクについて

LIF のフェイルオーバーターゲットを表示すると、次のことを確認できます。

- LIF に正しいフェイルオーバーグループとフェイルオーバーポリシーが設定されているかどうか
- 表示されたフェイルオーバーターゲットのポートが LIF に適しているかどうか
- データ LIF のフェイルオーバーターゲットが管理ポート（e0M）でないかどうか

ステップ

を使用して、LIFのフェイルオーバーターゲットを表示します failover のオプション network interface show コマンドを実行します

次のコマンドは、2 ノードクラスタのすべての LIF のフェイルオーバーターゲットに関する情報を表示します。。 Failover Targets 行には、特定のLIFにおけるノードとポートの組み合わせの（優先順位の高い）リストが表示されます。

```
network interface show -failover
```

	Logical	Home	Failover	Failover
Vserver	Interface	Node:Port	Policy	Group
-----	-----	-----	-----	-----
Cluster				
	node1_clus1	node1:e0a	local-only	Cluster
		Failover Targets: node1:e0a,	node1:e0b	
	node1_clus2	node1:e0b	local-only	Cluster
		Failover Targets: node1:e0b,	node1:e0a	
	node2_clus1	node2:e0a	local-only	Cluster
		Failover Targets: node2:e0a,	node2:e0b	
	node2_clus2	node2:e0b	local-only	Cluster
		Failover Targets: node2:e0b,	node2:e0a	
cluster1				
	cluster_mgmt	node1:e0c	broadcast-domain-wide	Default
		Failover Targets: node1:e0c,	node1:e0d,	
		node2:e0c,	node2:e0d	
	node1_mgmt1	node1:e0c	local-only	Default
		Failover Targets: node1:e0c,	node1:e0d	
	node2_mgmt1	node2:e0c	local-only	Default
		Failover Targets: node2:e0c,	node2:e0d	
vs1				
	data1	node1:e0e	system-defined	bcast1
		Failover Targets: node1:e0e,	node1:e0f,	
		node2:e0e,	node2:e0f	

## ロードバランシングゾーンの LIF を表示します

ロードバランシングゾーンに属するすべての LIF を表示して、そのゾーンが正しく設定されているかどうかを確認できます。特定の LIF、またはすべての LIF のロードバランシングゾーンを表示することもできます。

### ステップ

次のいずれかのコマンドを使用して、LIF とロードバランシングの詳細を表示します

表示する内容	入力するコマンド
特定のロードバランシングゾーンに属する LIF	<code>network interface show -dns-zone zone_name</code>  zone_name ロードバランシングゾーンの名前を指定します。
特定の LIF のロードバランシングゾーン	<code>network interface show -lif lif_name -fields dns-zone</code>
すべての LIF のロードバランシングゾーン	<code>network interface show -fields dns-zone</code>

### LIF のロードバランシングゾーンを表示する例

次のコマンドは、SVM vs0 の storage.company.com というロードバランシングゾーンに属するすべての LIF の詳細を表示します。

```
net int show -vserver vs0 -dns-zone storage.company.com
```

Vserver	Logical Interface	Status Admin/Oper	Network Address/Mask	Current Node	Current Port	Is Home
vs0	lif3	up/up	10.98.226.225/20	ndeux-11	e0c	true
	lif4	up/up	10.98.224.23/20	ndeux-21	e0c	true
	lif5	up/up	10.98.239.65/20	ndeux-11	e0c	true
	lif6	up/up	10.98.239.66/20	ndeux-11	e0c	true
	lif7	up/up	10.98.239.63/20	ndeux-21	e0c	true
	lif8	up/up	10.98.239.64/20	ndeux-21	e0c	true

次のコマンドは、data3 という LIF の DNS ゾーンの詳細を表示します。

```
network interface show -lif data3 -fields dns-zone
Vserver    lif      dns-zone
-----
vs0        data3    storage.company.com
```

次のコマンドは、クラスタ内のすべての LIF、および対応する DNS ゾーンを表示します。

```
network interface show -fields dns-zone
Vserver    lif      dns-zone
-----
cluster    cluster_mgmt none
ndeux-21   clus1     none
ndeux-21   clus2     none
ndeux-21   mgmt1     none
vs0        data1     storage.company.com
vs0        data2     storage.company.com
```

## クラスタの接続を表示します

クラスタ内のすべてのアクティブな接続を表示したり、クライアント、論理インターフェイス、プロトコル、またはサービス別にノードのアクティブな接続を表示したりできます。クラスタ内のリスンしているすべての接続を表示することもできます。

クライアント別のアクティブな接続を表示する（クラスタ管理者のみ）

クライアント別にアクティブな接続を表示して、特定のクライアントで使用されているノードを確認したり、ノードあたりのクライアント数に不均衡がないかどうかを確認したりできます。

このタスクについて

クライアント別のアクティブな接続数の情報は、次のような場合に役立ちます。

- ビジー状態や過負荷のノードを特定する。
- 特定のクライアントからのボリュームへのアクセスが低速になっている理由を確認する。

クライアントがアクセスしているノードに関する詳細を表示し、ボリュームが配置されているノードと比較できます。ボリュームへのアクセスにクラスタネットワークのトラバースが必要な場合、オーバーサブスライブされたリモートノードにあるボリュームへのリモートアクセスにより、クライアントのパフォーマンスが低下することがあります。

- データアクセスにすべてのノードが均等に使用されていることを確認する。
- 接続数が予期せず多くなっているクライアントを特定する。
- 特定のクライアントがノードに接続しているかどうかを確認する。

ステップ

を使用して、ノードのアクティブな接続数をクライアント別に表示します `network connections active show-clients` コマンドを実行します

このコマンドの詳細については、マニュアルページを参照してください。 ["ONTAP 9 のコマンド"](#)

```
network connections active show-clients
Node      Vserver Name      Client IP Address      Count
-----
node0     vs0                192.0.2.253            1
          vs0                192.0.2.252            2
          Cluster         192.10.2.124           5
node1     vs0                192.0.2.250            1
          vs0                192.0.2.252            3
          Cluster         192.10.2.123           4
node2     vs1                customer.example.com    1
          vs1                192.0.2.245            3
          Cluster         192.10.2.122           4
node3     vs1                customer.example.org    1
          vs1                customer.example.net    3
          Cluster         192.10.2.121           4
```

プロトコル別のアクティブな接続を表示する（クラスタ管理者のみ）

ノードのアクティブな接続数をプロトコル（TCP または UDP）別に表示して、クラスタ内のプロトコルの使用状況を比較できます。

このタスクについて

プロトコル別のアクティブな接続数の情報は、次のような場合に役立ちます。

- 接続が切断されている UDP クライアントを探す。

ノードの接続数が制限に近づくと、UDP クライアントが最初に破棄されます。

- 他のプロトコルが使用されていないことを確認する。

ステップ

を使用して、ノードのアクティブな接続数をプロトコル別に表示します `network connections active show-protocols` コマンドを実行します

このコマンドの詳細については、マニュアルページを参照してください。

```

network connections active show-protocols
Node      Vserver Name  Protocol  Count
-----
node0
      vs0      UDP      19
      Cluster  TCP      11
node1
      vs0      UDP      17
      Cluster  TCP       8
node2
      vs1      UDP      14
      Cluster  TCP      10
node3
      vs1      UDP      18
      Cluster  TCP       4

```

サービス別のアクティブな接続を表示する（クラスタ管理者のみ）

クラスタ内の各ノードのアクティブな接続数をサービスタイプ（NFS、SMB、マウントなど）別に表示できます。これは、クラスタ内のサービスの使用状況を比較する際に役立ちます。これにより、ノードのプライマリワークロードを特定するのに役立ちます。

このタスクについて

サービス別のアクティブな接続数の情報は、次のような場合に役立ちます。

- すべてのノードが適切なサービス用に使用されていること、およびそのサービスのロードバランシングが機能していることを確認する。
- 他のサービスが使用されていないことを確認する。を使用して、ノードのアクティブな接続数をサービス別に表示します `network connections active show-services` コマンドを実行します

このコマンドの詳細については、マニュアルページを参照してください。 ["ONTAP 9 のコマンド"](#)



```

network connections active show-services
Node      Vserver Name      Service      Count
-----
node0
      vs0          mount         3
      vs0          nfs           14
      vs0          nlm_v4        4
      vs0          cifs_srv      3
      vs0          port_map      18
      vs0          rclopcp       27
      Cluster      ctlopcp       60
node1
      vs0          cifs_srv      3
      vs0          rclopcp       16
      Cluster      ctlopcp       60
node2
      vs1          rclopcp       13
      Cluster      ctlopcp       60
node3
      vs1          cifs_srv      1
      vs1          rclopcp       17
      Cluster      ctlopcp       60

```

ノードおよび **SVM** の **LIF** 別のアクティブな接続の情報を表示します

ノードおよび Storage Virtual Machine（SVM）の LIF 別のアクティブな接続数を表示して、クラスタ内の LIF 間で接続数の不均衡がないかどうかを確認できます。

このタスクについて

LIF 別のアクティブな接続数の情報は、次のような場合に役立ちます。

- 各 LIF の接続数を比較することで、過負荷の LIF を探す。
- すべてのデータ LIF に対して DNS ロードバランシングが機能していることを確認する。
- さまざまな SVM への接続数を比較して、最もよく使用されている SVM を特定する。

ステップ

を使用して、SVMおよびノードのアクティブな接続数をLIF別に表示します network connections active show-lifs コマンドを実行します

このコマンドの詳細については、マニュアルページを参照してください。 ["ONTAP 9 のコマンド"](#)

```

network connections active show-lifs
Node      Vserver Name  Interface Name  Count
-----
node0
    vs0        datalif1        3
    Cluster    node0_clus_1    6
    Cluster    node0_clus_2    5
node1
    vs0        datalif2        3
    Cluster    node1_clus_1    3
    Cluster    node1_clus_2    5
node2
    vs1        datalif2        1
    Cluster    node2_clus_1    5
    Cluster    node2_clus_2    3
node3
    vs1        datalif1        1
    Cluster    node3_clus_1    2
    Cluster    node3_clus_2    2

```

クラスタ内のアクティブな接続を表示します

クラスタ内のアクティブな接続に関する情報を表示して、それぞれの接続で使用されている LIF、ポート、リモートホスト、サービス、Storage Virtual Machine（SVM）、およびプロトコルを確認できます。

このタスクについて

クラスタ内のアクティブな接続の情報は、次のような場合に役立ちます。

- 個々のクライアントが正しいノードで正しいプロトコルとサービスを使用していることを確認する。
- クライアントで特定の組み合わせのノード、プロトコル、およびサービスを使用してデータにアクセスできない場合に、同様のクライアントを探して設定やパケットトレースを比較することができます。

ステップ

を使用して、クラスタ内のアクティブな接続を表示します `network connections active show` コマンドを実行します

このコマンドの詳細については、マニュアルページを参照してください。 ["ONTAP 9 のコマンド"](#)

次のコマンドは、node1 というノードのアクティブな接続の情報を表示します。

```
network connections active show -node node1
```

Vserver	Interface	Remote	
Name	Name:Local Port	Host:Port	Protocol/Service
-----	-----	-----	-----
Node: node1			
Cluster	node1_clus_1:50297	192.0.2.253:7700	TCP/ctlopcp
Cluster	node1_clus_1:13387	192.0.2.253:7700	TCP/ctlopcp
Cluster	node1_clus_1:8340	192.0.2.252:7700	TCP/ctlopcp
Cluster	node1_clus_1:42766	192.0.2.252:7700	TCP/ctlopcp
Cluster	node1_clus_1:36119	192.0.2.250:7700	TCP/ctlopcp
vs1	data1:111	host1.aa.com:10741	UDP/port-map
vs3	data2:111	host1.aa.com:10741	UDP/port-map
vs1	data1:111	host1.aa.com:12017	UDP/port-map
vs3	data2:111	host1.aa.com:12017	UDP/port-map

次のコマンドは、SVM vs1 のアクティブな接続の情報を表示します。

```
network connections active show -vserver vs1
```

Vserver	Interface	Remote	
Name	Name:Local Port	Host:Port	Protocol/Service
-----	-----	-----	-----
Node: node1			
vs1	data1:111	host1.aa.com:10741	UDP/port-map
vs1	data1:111	host1.aa.com:12017	UDP/port-map

クラスタ内のリスンしている接続を表示します

クラスタ内のリスンしている接続を表示して、特定のプロトコルとサービスの接続を受け入れている LIF とポートを確認することができます。

このタスクについて

クラスタ内のリスンしている接続の表示は、次のような場合に役立ちます。

- 特定の LIF へのクライアント接続が必ず失敗する場合に、その LIF を適切なプロトコルまたはサービスでリスンしていることを確認する。
- あるノードのボリュームのデータに別のノードの LIF を介してリモートアクセスできない場合に、それぞれのクラスタ LIF で UDP / rcllopcp リスナーが開いていることを確認する。
- 同じクラスタの 2 つのノード間での SnapMirror 転送に失敗した場合に、それぞれのクラスタ LIF で UDP / rcllopcp リスナーが開いていることを確認する。
- 異なるクラスタの 2 つのノード間での SnapMirror 転送に失敗した場合に、それぞれのインタークラスタ LIF で TCP / ctlopcp リスナーが開いていることを確認する。

ステップ

を使用して、ノードごとにリスンしている接続を表示します `network connections listening show コ`

マンドを実行します

```
network connections listening show
Vserver Name      Interface Name:Local Port      Protocol/Service
-----
Node: node0
Cluster           node0_clus_1:7700              TCP/ctlopcp
vs1               data1:4049                    UDP/unknown
vs1               data1:111                     TCP/port-map
vs1               data1:111                     UDP/port-map
vs1               data1:4046                    TCP/sm
vs1               data1:4046                    UDP/sm
vs1               data1:4045                    TCP/nlm-v4
vs1               data1:4045                    UDP/nlm-v4
vs1               data1:2049                    TCP/nfs
vs1               data1:2049                    UDP/nfs
vs1               data1:635                    TCP/mount
vs1               data1:635                    UDP/mount
Cluster           node0_clus_2:7700              TCP/ctlopcp
```

ネットワークの問題を診断するためのコマンドです

ネットワークの問題を診断するには、などのコマンドを使用します ping, traceroute, ndp, および tcpdump。などのコマンドを使用することもできます ping6 および traceroute6 IPv6の問題を診断する。

状況	入力するコマンド
ノードがネットワーク上の他のホストに到達できるかどうかをテストします	network ping
ノードが IPv6 ネットワーク上の他のホストに到達できるかどうかをテストします	network ping6
IPv4 パケットがネットワークノードまでたどったルートをトレースする	network traceroute
IPv6パケットがネットワークノードまでたどったルートをトレースする	network traceroute6
近接探索プロトコル（NDP）を管理する	network ndp
指定したネットワークインターフェイスまたはすべてのネットワークインターフェイスで送受信されたパケットの統計情報を表示する	run -node node_name ifstat 注：このコマンドはノードシェルから使用できます。
リモートデバイスタイプやデバイスプラットフォームなど、クラスタ内の各ノードとポートで検出されている隣接デバイスに関する情報を表示します	network device-discovery show

ノードの CDP 隣接デバイスを表示する（ONTAP は CDPv1 通知のみをサポート）	<pre>run -node node_name cdpd show-neighbors</pre> <p>注：このコマンドはノードシェルから使用できます。</p>
ネットワークで送受信されたパケットをトレースします	<pre>network tcpdump start -node node-name -port port_name</pre> <p>注：このコマンドはノードシェルから使用できます。</p>
クラスタ間またはクラスタ内のノード間のレイテンシとスループットを測定します	<pre>network test -path -source-node source_nodename local -destination -cluster destination_clustername -destination-node destination_nodename -session-type Default, AsyncMirrorLocal, AsyncMirrorRemote, SyncMirrorRemote, or RemoteDataTransfer</pre> <p>詳細については、を参照してください <a href="#">"パフォーマンス管理"</a>。</p>

これらのコマンドの詳細については、該当するマニュアルページを参照してください。 ["ONTAP 9 のコマンド"](#)

## 近接探索プロトコルによるネットワーク接続を表示します

近接探索プロトコルによるネットワーク接続を表示します

データセンターでは、近接探索プロトコルを使用して、物理または仮想システムのペアとそのネットワークインターフェイス間のネットワーク接続を表示できます。ONTAP では、2 つの近接探索プロトコルとして、Cisco Discovery Protocol（CDP）と Link Layer Discovery Protocol（LLDP）がサポートされます。

近接探索プロトコルを使用すると、ネットワーク内の直接接続されているプロトコル対応デバイスを自動的に検出し、その情報を表示できます。各デバイスは、ID、機能、および接続情報をアドバタイズします。この情報はイーサネットフレームでマルチキャスト MAC アドレスへ送信され、近接するすべてのプロトコル対応デバイスで受信されます。

2 つのデバイスがネイバーになるには、各デバイスでプロトコルが有効になっていて、正しく設定されている必要があります。検出プロトコルの機能は、直接接続されたネットワークに限定されます。近接機器には、スイッチ、ルータ、ブリッジなどのプロトコル対応デバイスが含まれます。ONTAP では、2 つの近接探索プロトコルがサポートされます。これらは個別に使用することも一緒に使用することもでき

- シスコ検出プロトコル（CDP）\*

CDP は、Cisco Systems が開発したリンクレイヤプロトコルです。ONTAP では、クラスタポートに対してこのプロトコルがデフォルトで有効になりますが、データポートに対しては明示的に有効にする必要があります。

- リンク層検出プロトコル（LLDP）\*

LLDP は、ベンダーに依存しないプロトコルであり、IEEE 802.1AB 規格のドキュメントで指定されています。すべてのポートに対して明示的にイネーブルにする必要があります。

**CDP** を使用してネットワーク接続を検出します

CDP を使用してネットワーク接続を検出するには、導入時の考慮事項を確認し、データポートで CDP を有効にし、ネイバーデバイスを表示し、必要に応じて CDP 設定値を調整します。クラスタポートでは、CDP はデフォルトで有効になります。

隣接デバイスに関する情報を表示するには、スイッチとルータでも CDP を有効にする必要があります。

ONTAP リリース	説明
9.10.1以前	CDP は、クラスタと管理ネットワークスイッチを自動的に検出するためにクラスタスイッチヘルスマニタでも使用されます。
9.11.1以降	CDPは、クラスタ、ストレージ、および管理ネットワークスイッチを自動的に検出するためにクラスタスイッチヘルスマニタでも使用されます。

関連情報

["システム管理"](#)

**CDP** を使用する場合の考慮事項

デフォルトでは、CDP 対応デバイスは CDPv2 通知を送信します。CDP 対応デバイスは、CDPv1 通知を受信した場合にのみ、CDPv1 通知を送信します。ONTAP は CDPv1 のみをサポートします。したがって、ONTAP ノードが CDPv1 通知を送信すると、CDP 対応の隣接デバイスが CDPv1 通知を返します。

ノードで CDP を有効にする前に、次の点を確認してください。

- CDP はすべてのポートでサポートされます。
- CDP 通知は、up 状態のポートから送受信されます。
- CDP 通知を送受信するには、送信デバイスと受信デバイスの両方で CDP を有効にする必要があります。
- CDP 通知は一定間隔で送信され、送信間隔は設定可能です。
- LIF の IP アドレスが変更されると、ノードは更新された情報を次の CDP 通知で送信します。
- ONTAP 9.10.1以前：
  - CDP はクラスタポートで常に有効になります。
  - 非クラスタポートでは、CDP はデフォルトで無効になります。
- ONTAP 9.11.1以降：
  - CDPは、クラスタポートとストレージポートで常に有効になります。
  - 非クラスタポートと非ストレージポートでは、CDPはデフォルトで無効になっています。



ノードで LIF が変更された場合、スイッチなどの受信デバイス側で CDP 情報が更新されないことがあります。このような問題が発生した場合は、ノードのネットワークインターフェイスをいったん down 状態にしてから、up 状態に設定してください。

- CDP 通知で送信されるのは IPv4 アドレスのみです。

- VLAN が設定されている物理ネットワークポートの場合、VLAN に設定されているすべての LIF が通知されます。
- インターフェイスグループの一部となっている物理ポートの場合、そのインターフェイスグループに設定されているすべての IP アドレスが、各物理ポートで通知されます。
- VLAN をホストするインターフェイスグループの場合、インターフェイスグループおよび VLAN に設定されているすべての LIF が各ネットワークポートで通知されます。
- CDP パケットが 1500 バイト以下に制限されているため、ポート上  
多数の LIF で構成されている場合、隣接するスイッチではこれらの IP アドレスの一部のみが報告されることがあります。

**CDP を有効または無効にします**

CDP 対応の隣接デバイスを検出して通知を送信するには、クラスタの各ノードで CDP が有効になっている必要があります。

ONTAP 9.10.1 以前のデフォルトでは、ノードのすべてのクラスタポートで CDP が有効になり、ノードのすべての非クラスタポートで無効になります。

ONTAP 9.11.1 以降では、デフォルトで、ノードのすべてのクラスタポートとストレージポートで CDP が有効になり、ノードの非クラスタポートと非ストレージポートで無効になっています。

このタスクについて

。 `cdpd.enable` オプションは、ノードのポートで CDP を有効にするか無効にするかを制御します。

- ONTAP 9.10.1 以前の場合、`on` を指定すると、非クラスタポートで CDP が有効になります。
- ONTAP 9.11.1 以降では、`on` を指定すると、非クラスタポートと非ストレージポートで CDP が有効になります。
- ONTAP 9.10.1 以前のバージョンでは、`off` を指定すると非クラスタポートで CDP が無効になります。クラスタポートの CDP を無効にすることはできません。
- ONTAP 9.11.1 以降では、`off` を指定すると、非クラスタポートと非ストレージポートで CDP が無効になります。クラスタポートの CDP を無効にすることはできません。

CDP 対応デバイスに接続されているポートで CDP を無効にすると、ネットワークトラフィックが最適化されない可能性があります。

手順

1. クラスタ内の 1 つまたはすべてのノードの、現在の CDP 設定を表示します。

CDP 設定を表示する対象	入力するコマンド
ノード	<code>run - node &lt;node_name&gt; options cdpd.enable</code>
クラスタ内のすべてのノード	<code>options cdpd.enable</code>

2. クラスタ内の 1 つまたはすべてのノードで、すべてのポートの CDP を有効または無効にします。

CDP を有効または無効にする対象	入力するコマンド
ノード	<code>run -node node_name options cdpd.enable {on or off}</code>
クラスタ内のすべてのノード	<code>options cdpd.enable {on or off}</code>

#### CDP ネイバー情報を表示します

クラスタのノードのポートに CDP 対応デバイスが接続されている場合は、そのポートの隣接デバイスの情報を表示することができます。を使用できます `network device-discovery show -protocol cdp` ネイバー情報を表示するコマンド。

#### このタスクについて

ONTAP 9.10.1以前では、クラスタポートでCDPが常に有効になっているため、これらのポートのCDPネイバー情報は常に表示されます。非クラスタポートの隣接情報を表示するには、これらのポートで CDP を有効にする必要があります。

ONTAP 9.11.1以降では、クラスタポートとストレージポートでCDPが常に有効になっているため、これらのポートのCDP隣接情報は常に表示されます。非クラスタポートおよび非ストレージポートでCDPを有効にして、これらのポートのネイバー情報を表示する必要があります。

#### ステップ

クラスタ内のノードのポートに接続されているすべての CDP 対応デバイスの情報を表示します。

```
network device-discovery show -node node -protocol cdp
```

次のコマンドは、ノードsti2650-212のポートに接続されているネイバーを表示します。



```

network device-discovery show -node sti2650-212 -protocol cdp
Node/          Local  Discovered
Protocol      Port   Device (LLDP: ChassisID)  Interface          Platform
-----
sti2650-212/cdp
              e0M    RTP-LF810-510K37.gdl.eng.netapp.com(SAL1942R8JS)
                                   Ethernet1/14        N9K-
C93120TX
              e0a    CS:RTP-CS01-510K35        0/8                CN1610
              e0b    CS:RTP-CS01-510K36        0/8                CN1610
              e0c    RTP-LF350-510K34.gdl.eng.netapp.com(FDO21521S76)
                                   Ethernet1/21        N9K-
C93180YC-FX
              e0d    RTP-LF349-510K33.gdl.eng.netapp.com(FDO21521S4T)
                                   Ethernet1/22        N9K-
C93180YC-FX
              e0e    RTP-LF349-510K33.gdl.eng.netapp.com(FDO21521S4T)
                                   Ethernet1/23        N9K-
C93180YC-FX
              e0f    RTP-LF349-510K33.gdl.eng.netapp.com(FDO21521S4T)
                                   Ethernet1/24        N9K-
C93180YC-FX

```

出力には、指定したノードの各ポートに接続されている Cisco デバイスが一覧表示されます。

#### CDP メッセージの保持時間を設定します

保持時間とは、CDP 通知が CDP 対応の隣接デバイスのキャッシュに格納される時間です。保持時間は各 CDPv1 パケットで通知され、ノードが CDPv1 パケットを受信するたびに更新されます。

- の値 `cdpd.holdtime` オプションの値は、HAペアの両方のノードで同じに設定する必要があります。
- デフォルトの保持時間は 180 ですが、10~255 秒の値を入力できます。
- 保持時間が切れる前に IP アドレスが削除された場合、CDP 情報は保持時間が切れるまでキャッシュされます。

#### 手順

1. クラスタ内の 1 つまたはすべてのノードの CDP メッセージの現在の保持時間を表示します。

保持時間を表示する対象	入力するコマンド
ノード	<code>run -node node_name options cdpd.holdtime</code>
クラスタ内のすべてのノード	<code>options cdpd.holdtime</code>

2. クラスタ内の 1 つまたはすべてのノードで、すべてのポートの CDP 通知の保持時間を設定します。

保持時間を設定する対象	入力するコマンド
ノード	<code>run -node node_name options cdpd.holdtime holdtime</code>
クラスタ内のすべてのノード	<code>options cdpd.holdtime holdtime</code>

#### CDP 通知の送信間隔を設定します

CDP 通知は、一定の間隔で CDP 隣接機器に送信されます。ネットワークトラフィックの量やネットワークポロジの変化に応じて、CDP 通知の送信間隔を調整することができます。

- の値 `cdpd.interval` オプションの値は、HAペアの両方のノードで同じに設定する必要があります。
- デフォルトの送信間隔は 60 秒ですが、5~900 秒の値を入力できます。

#### 手順

1. クラスタ内の 1 つまたはすべてのノードについて、CDP 通知の現在の送信間隔を表示します。

送信間隔を表示する対象	入力するコマンド
ノード	<code>run -node node_name options cdpd.interval</code>
クラスタ内のすべてのノード	<code>options cdpd.interval</code>

2. クラスタ内の 1 つまたはすべてのノードで、すべてのポートの CDP 通知の送信間隔を設定します。

送信間隔を設定する対象	入力するコマンド
ノード	<code>run -node node_name options cdpd.interval interval</code>
クラスタ内のすべてのノード	<code>options cdpd.interval interval</code>

#### CDP 統計情報を表示または消去します

ネットワーク接続に潜在的な問題を検出するために、各ノードのクラスタポートと非クラスタポートの CDP 統計を表示することができます。CDP 統計は、値が前回消去されたときからの累積値です。

#### このタスクについて

ONTAP 9.10.1以前では、ポートでCDPが常にイネーブルになっているため、これらのポート上のトラフィックに関するCDP統計情報は常に表示されます。これらのポートの統計情報を表示するには、ポート上でCDPを有効にする必要があります。

ONTAP 9.11.1以降では、クラスタポートとストレージポートでCDPが常に有効になっているため、これらのポートのトラフィックについてCDP統計情報が常に表示されます。非クラスタポートまたは非ストレージポートでCDP統計情報を表示するには、これらのポートでCDPを有効にする必要があります。

## ステップ

ノードのすべてのポートに関する現在の CDP 統計情報を表示または消去します。

状況	入力するコマンド
CDP 統計情報を表示します	<code>run -node node_name cdpd show-stats</code>
CDP 統計情報を消去します	<code>run -node node_name cdpd zero-stats</code>

### 統計情報の表示と消去の例

次のコマンドは、消去する前の CDP 統計情報を表示します。出力には、前回統計情報が消去されてから送受信されたパケットの合計数が表示されます。

```
run -node nodel cdpd show-stats
```

#### RECEIVE

Packets:	9116	Csum Errors:	0	Unsupported Vers:	4561
Invalid length:	0	Malformed:	0	Mem alloc fails:	0
Missing TLVs:	0	Cache overflow:	0	Other errors:	0

#### TRANSMIT

Packets:	4557	Xmit fails:	0	No hostname:	0
Packet truncated:	0	Mem alloc fails:	0	Other errors:	0

#### OTHER

Init failures:	0
----------------	---

次のコマンドは、CDP 統計情報を消去します。

```
run -node nodel cdpd zero-stats
```

```
run -node nodel cdpd show-stats
```

#### RECEIVE

Packets:	0		Csum Errors:	0		Unsupported Vers:	0
Invalid length:	0		Malformed:	0		Mem alloc fails:	0
Missing TLVs:	0		Cache overflow:	0		Other errors:	0

#### TRANSMIT

Packets:	0		Xmit fails:	0		No hostname:	0
Packet truncated:	0		Mem alloc fails:	0		Other errors:	0

#### OTHER

Init failures:	0
----------------	---

統計を消去すると、次回 CDP 通知を送信または受信したあとに統計が累積され始めます。

### LLDPを使用したネットワーク接続の検出

LLDP を使用してネットワーク接続を検出するには、導入時の考慮事項を確認し、すべてのポートで LLDP を有効にし、隣接デバイスを表示し、必要に応じて LLDP の設定値を調整します。

ネイバーデバイスに関する情報を表示するには、スイッチおよびルータでも LLDP をイネーブルにする必要があります。

ONTAP は現在、次の Type-Length-Value 構造（TLV）を報告します。

- シャーシ ID
- ポート ID
- Time-To-Live（TTL）
- システム名

システム名 TLV は、CNA デバイスでは送信されません。

X1143 アダプタや UTA2 オンボードポートなどの特定の統合ネットワークアダプタ（CNA）には LLDP のオフロードサポートが含まれています。

- LLDP のオフロードは、Data Center Bridging（DCB）に使用されます。
- 表示される情報がクラスタとスイッチで異なる場合があります。

CNAポートとCNA以外のポートについてスイッチで表示されるシャーシIDとポートIDのデータが異なる場合があります。

例：

- 非CNAポートの場合：
  - シャーシIDは、ノードのいずれかのポートの固定MACアドレスです
  - Port IDは、ノード上の対応するポートのポート名です
- CNAポートの場合：
  - シャーシIDとポートIDは、ノード上の対応するポートのMACアドレスです。

ただし、これらのポートタイプについては、クラスタで表示されるデータに整合性があることを示しています。



LLDP の仕様では、SNMP MIB による収集情報へのアクセスを定義します。ただし、現時点では、ONTAP は LLDP MIB をサポートしていません。

#### LLDPの有効化または無効化

LLDP対応の隣接デバイスを検出して通知を送信するには、クラスタの各ノードでLLDPが有効になっている必要があります。ONTAP 9.7 以降では、LLDP がノードのすべてのポートでデフォルトで有効になっています。

#### このタスクについて

ONTAP 9.10.1以前の場合は `lldp.enable` オプションは、ノードのポートでLLDPを有効にするか無効にするかを制御します。

- `on` すべてのポートでLLDPをイネーブルにします。
- `off` すべてのポートでLLDPをディセーブルにします。

ONTAP 9.11.1以降の場合は `lldp.enable` オプションは、ノードの非クラスタポートとストレージポートでLLDPを有効にするか無効にするかを制御します。

- `on` すべての非クラスタポートおよびストレージポートでLLDPをイネーブルにします。
- `off` すべての非クラスタポートおよびストレージポートでLLDPを無効にします。

#### 手順

1. クラスタ内の1つまたはすべてのノードの現在のLLDP設定を表示します。
  - シングルノード `run -node node_name options lldp.enable`
  - すべてのノード：`options lldp.enable`
2. クラスタ内の 1 つまたはすべてのノードで、すべてのポートの LLDP を有効または無効に設定します。

LLDPを有効または無効にする対象	入力するコマンド
ノード	<code>`run -node node_name options lldp.enable {on</code>
<code>off}`</code>	クラスタ内のすべてのノード
<code>`options lldp.enable {on</code>	<code>off}`</code>

- シングルノード

```
run -node node_name options lldp.enable {on|off}
```

- すべてのノード：

```
options lldp.enable {on|off}
```

## LLDPネイバー情報の表示

クラスタのノードのポートに LLDP 対応デバイスが接続されている場合は、そのポートの隣接デバイスの情報を表示することができます。ネイバー情報を表示するには、`network device-discovery show` コマンドを使用します。

### ステップ

1. クラスタ内のノードのポートに接続されているすべてのLLDP準拠デバイスの情報を表示します。

```
network device-discovery show -node node -protocol lldp
```

次のコマンドは、ノード `cluster-1_01` のポートに接続されている隣接デバイスの情報を表示します。この出力には、指定したノードの各ポートに接続されている LLDP 対応デバイスが一覧表示されます。状況に応じて `-protocol` オプションを省略すると、CDP対応デバイスも表示されます。

```
network device-discovery show -node cluster-1_01 -protocol lldp
Node/          Local   Discovered
Protocol       Port    Device                                Interface          Platform
-----
cluster-1_01/lldp
                e2a     0013.c31e.5c60                       GigabitEthernet1/36
                e2b     0013.c31e.5c60                       GigabitEthernet1/35
                e2c     0013.c31e.5c60                       GigabitEthernet1/34
                e2d     0013.c31e.5c60                       GigabitEthernet1/33
```

## LLDP 通知の送信間隔を調整します

LLDP通知は、一定の間隔でLLDPネイバーに送信されます。ネットワークトラフィックやネットワークポロジの変化に応じて、LLDP通知の送信間隔を増減できます。

### このタスクについて

IEEE が推奨するデフォルトの送信間隔は 30 秒ですが、5~300 秒の値を入力できます。

### 手順

1. クラスタ内の1つまたはすべてのノードについて、LLDP通知の現在の間隔を表示します。

◦ シングルノード

```
run -node <node_name> options lldp.xmit.interval
```

◦ すべてのノード：

```
options lldp.xmit.interval
```

2. クラスタ内の 1 つまたはすべてのノードで、すべてのポートの LLDP 通知の送信間隔を調整します。

◦ シングルノード

```
run -node <node_name> options lldp.xmit.interval <interval>
```

◦ すべてのノード：

```
options lldp.xmit.interval <interval>
```

#### LLDP 通知の TTL 値を調整します

Time-To-Live (TTL) とは、LLDP 通知が LLDP 対応の隣接デバイスのキャッシュに格納される時間です。TTL は各 LLDP パケットで通知され、ノードが LLDP パケットを受信するたびに更新されます。発信 LLDP フレームで TTL を変更できます。

このタスクについて

- TTLは計算された値であり、送信間隔の積です (lldp.xmit.interval) とホールド乗数 (lldp.xmit.hold) プラス1。
- デフォルトの保持の乗数値は 4 ですが、1~100 の値を入力できます。
- IEEE が推奨するデフォルトの TTL は 121 秒ですが、送信間隔と保持の乗数の値を調整することにより、発信フレームの値を 6~30001 秒に指定できます。
- TTL が期限切れになる前に IP アドレスが削除された場合、LLDP 情報は TTL が期限切れになるまでキャッシュされます。

手順

1. クラスタ内の 1 つまたはすべてのノードの現在の保持の乗数値を表示します。

◦ シングルノード

```
run -node <node_name> options lldp.xmit.hold
```

◦ すべてのノード：

```
options lldp.xmit.hold
```

2. クラスタ内の1つまたはすべてのノードで、すべてのポートの保持の乗数値を調整します。

◦ シングルノード

```
run -node <node_name> options lldp.xmit.hold <hold_value>
```

◦ すべてのノード：

```
options lldp.xmit.hold <hold_value>
```

#### LLDP統計情報を表示または消去します

ネットワーク接続に潜在的な問題を検出するために、各ノードのクラスタポートと非クラスタポートのLLDP統計を表示できます。LLDP統計は、前回消去されたときからの累積値です。

このタスクについて

ONTAP 9.10.1以前では、クラスタポートでLLDPが常に有効になっているため、これらのポートのトラフィックについては常にLLDP統計が表示されます。非クラスタポートでLLDP統計が表示されるようにするには、LLDPを有効にする必要があります。

ONTAP 9.11.1以降では、クラスタポートとストレージポートでLLDPが常に有効になっているため、これらのポートのトラフィックについてLLDP統計が常に表示されます。これらのポートに対して統計情報を表示するには、クラスタ以外のポートおよびストレージ以外のポートでLLDPを有効にする必要があります。

#### ステップ

ノードのすべてのポートの現在のLLDP統計を表示または消去します。

状況	入力するコマンド
LLDP統計を表示します	<code>run -node node_name lldp stats</code>
LLDP統計情報をクリアします	<code>run -node node_name lldp stats -z</code>

#### 統計の例を表示および消去します

次のコマンドは、LLDP統計をクリアする前に表示します。出力には、前回統計情報が消去されてから送受信されたパケットの合計数が表示されます。



```
cluster-1::> run -node vsim1 lldp stats
```

RECEIVE

```
Total frames:      190k | Accepted frames:  190k | Total drops:
0
```

TRANSMIT

```
Total frames:      5195 | Total failures:    0
```

OTHER

```
Stored entries:      64
```

次のコマンドは、LLDP統計をクリアします。

```
cluster-1::> The following command clears the LLDP statistics:
```

```
run -node vsim1 lldp stats -z
```

```
run -node node1 lldp stats
```

RECEIVE

```
Total frames:      0 | Accepted frames:  0 | Total drops:
0
```

TRANSMIT

```
Total frames:      0 | Total failures:    0
```

OTHER

```
Stored entries:      64
```

統計を消去すると、LLDP通知が次回送信または受信されたあとに統計が累積され始めます。

# NAS ストレージ管理

## System Manager を使用して NAS プロトコルを管理します

### System Manager による NAS 管理の概要

このセクションのトピックでは、ONTAP 9.7 以降のリリースの System Manager を使用して NAS 環境を構成および管理する方法を説明します。

従来の System Manager（ONTAP 9.7 以前でのみ使用可能）を使用している場合は、次のトピックを参照してください。

- ["NFS 構成の概要"](#)
- ["SMBセツテイノカイヨウ"](#)

System Manager では、以下のワークフローがサポートされ

- NAS ファイルサービスに使用するクラスタの初期設定。
- ストレージニーズを変更するための追加のボリュームプロビジョニング。
- 業界標準の認証およびセキュリティ機能の設定とメンテナンス。

System Manager を使用すると、NAS サービスをコンポーネントレベルで管理できます。

- プロトコル— NFS、SMB、またはその両方（NAS マルチプロトコル）
- ネームサービス— DNS、LDAP、NIS
- ネームサービススイッチ
- Kerberos セキュリティ
- エクスポートと共有
- qtree
- ユーザとグループのネームマッピング

### VMware データストア用の NFS ストレージのプロビジョニング

Virtual Storage Console for VMware vSphere（VSC）を使用して ESXi ホスト用の ONTAP ベースのストレージシステムに NFS ボリュームをプロビジョニングする前に、System Manager for ONTAP 9.7 以降を使用して NFS を有効にしてください。

を作成した後 ["NFS 対応の Storage VM"](#) System Manager で、VSC を使用して NFS ボリュームをプロビジョニングし、データストアを管理します。

VSC 7.0 以降、VSC はの一部です ["ONTAP Tools for VMware vSphere 仮想アプライアンス"](#)で、VSC、vStorage APIs for Storage Awareness（VASA）Provider、および Storage Replication Adapter（SRA）for VMware vSphere の機能を使用できます。

必ずを確認してください ["NetApp Interoperability Matrix を参照してください"](#) 現在の ONTAP リリースと VSC

リリースの互換性を確認するため。

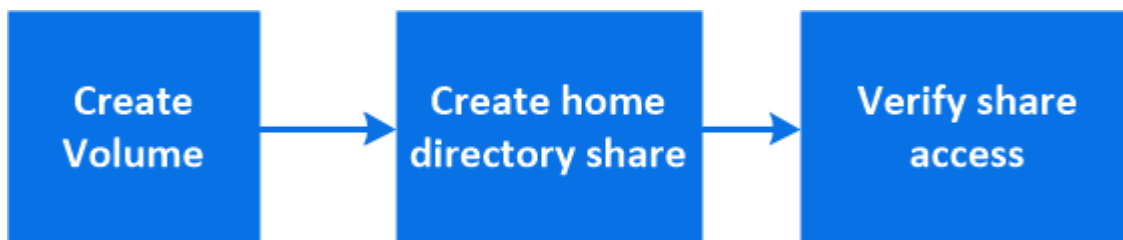
System Manager Classic（ONTAP 9.7 以前のリリース）を使用して、ESXi ホストからデータストアへの NFS アクセスを設定するには、を参照してください ["VSCを使用したESXi向けのNFS設定の概要"](#)

詳細については、を参照してください ["TR-4597：『VMware vSphere for ONTAP』"](#) および VSC リリースのドキュメントを参照してください。

## ホームディレクトリ用の **NAS** ストレージをプロビジョニングします

SMB プロトコルを使用してホームディレクトリにストレージを提供するボリュームを作成します。

この手順は、上にホームディレクトリ用の新しいボリュームを作成します ["SMB対応の既存のStorage VM"](#)。ボリュームの構成時にシステムのデフォルトをそのまま使用することも、カスタム構成を指定することもできます。



FlexVol ボリュームを作成することも、高いパフォーマンスが求められる大規模なファイルシステムには FlexGroup ボリュームを作成することもできます。も参照してください ["FlexGroup を使用して大規模ファイルシステム用の NAS ストレージをプロビジョニング"](#)。

このボリュームの仕様は Ansible Playbook に保存することもできます。詳細については、を参照してください ["Ansible Playbook を使用して、ボリュームや LUN を追加、編集できます"](#)。

### 手順

#### 1. SMB 対応 Storage VM に新しいボリュームを追加

- [ストレージ]>[ボリューム]を選択し、[追加]\*をクリックします。
- 名前を入力し、Storage VM を選択してサイズを入力します。

SMBプロトコルが設定されているStorage VMのみが表示されます。SMBプロトコルが設定されているStorage VMが1つしかない場合、\*[Storage VM]\*フィールドは表示されません。

- この時点で \* Save \* をクリックすると、System Manager はシステムデフォルトを使用して FlexVol ボリュームを作成および追加します。
- さらに \* その他のオプション \* をクリックしてボリュームの設定をカスタマイズし、許可、サービス品質、データ保護などのサービスを有効にすることができます。を参照してください [\[ボリュームの設定をカスタマイズする\]](#) をクリックし、次の手順を実行するためにここに戻ります。

#### 2. [ワークフローでステップ 2、ステップ 2][\* ストレージ]>[共有]をクリックし、[\* 追加]をクリックして、[\* ホームディレクトリ\*]を選択します。

#### 3. Windows クライアントで、次の手順を実行して、共有にアクセスできることを確認します。

- エクスプローラで、次の形式で共有にドライブをマッピングします。

\\\_SMB\_Server\_Name\_\_Share\_Name\_

変数（%w、%d、または%u）を使用して共有名が作成された場合は、解決済みの名前を使用してアクセスをテストする必要があります。

- b. 新しく作成したドライブで、テストファイルを作成し、作成できたら削除します。

## ボリュームの設定をカスタマイズする

システムのデフォルトを受け入れる代わりに、ボリュームを追加するときにボリューム構成をカスタマイズできます。

### 手順

[\* その他のオプション\*] をクリックした後、必要な機能を選択し、必要な値を入力します。

- リモートボリュームのキャッシュ。
- パフォーマンスサービスレベル（サービス品質、QoS）：

ONTAP 9.8以降では、デフォルト値に加えて、カスタムQoSポリシーを指定したりQoSを無効にしたりできます。

- QoS を無効にするには、「\* Custom \*」、「\* Existing \*」、「\* none \*」の順に選択します。
- 「\* Custom \*」を選択し、既存のサービスレベルを指定すると、ローカル階層が自動的に選択されます。
- ONTAP 9.9.1以降では、カスタムのパフォーマンスサービスレベルを作成するように選択した場合、System Managerを使用して、作成するボリュームを配置するローカル階層（手動配置）を手動で選択できます。

このオプションは、リモートキャッシュまたは FlexGroup ボリュームのオプションを選択した場合は使用できません。

- FlexGroup ボリューム（\* ボリュームデータをクラスタ全体に分散 \* を選択）。

このオプションは、パフォーマンスサービスレベル \* で手動配置 \* を選択した場合は使用できません。 そうしないと、追加するボリュームはデフォルトで FlexVol ボリュームになります。

- ボリュームが設定されているプロトコルのアクセス権限。
- SnapMirror によるデータ保護（ローカルまたはリモート）を実行してから、プルダウンリストからデステーションクラスタの保護ポリシーと設定を指定します。
- [保存]\*を選択してボリュームを作成し、クラスタとStorage VMに追加します。



ボリュームを保存したら、に戻ります [\[step2\]](#) ホームディレクトリのプロビジョニングを完了します。

## NFS を使用して Linux サーバ用の NAS ストレージをプロビジョニング

ONTAP System Manager（9.7 以降）で NFS プロトコルを使用して Linux サーバにストレージを提供するボリュームを作成します。

この手順は、に新しいボリュームを作成します ["NFS 対応の既存の Storage VM"](#)。ボリュームの設定時にシステムのデフォルトをそのまま使用することも、カスタム構成を指定することもできます。

FlexVol ボリュームを作成することも、高いパフォーマンスが求められる大規模なファイルシステムには FlexGroup ボリュームを作成することもできます。も参照してください ["FlexGroup を使用して大規模ファイルシステム用の NAS ストレージをプロビジョニング"](#)。

このボリュームの仕様は Ansible Playbook に保存することもできます。詳細については、を参照してください ["Ansible Playbook を使用して、ボリュームや LUN を追加、編集できます"](#)。

ONTAP NFS プロトコル機能の範囲の詳細については、を参照してください ["NFS のリファレンスの概要"](#)。

## 手順

1. NFS対応Storage VMに新しいボリュームを追加してください。
  - a. [\* ストレージ]、[ボリューム]の順にクリックし、[\* 追加]をクリックします。
  - b. 名前を入力し、Storage VM を選択してサイズを入力します。

NFS プロトコルが設定されている Storage VM のみが表示されます。SMBプロトコルが設定されているStorage VMが1つしかない場合、\*[Storage VM]\*フィールドは表示されません。

- この時点で \* Save \* をクリックすると、System Manager はシステムデフォルトを使用して FlexVol ボリュームを作成および追加します。



デフォルトのエクスポートポリシーでは、すべてのユーザにフルアクセスが許可されます。

- さらに \* その他のオプション \* をクリックしてボリュームの設定をカスタマイズし、許可、サービス品質、データ保護などのサービスを有効にすることができます。を参照してください [\[ボリュームの設定をカスタマイズする\]](#)をクリックし、次の手順を実行するためにここに戻ります。
2. [step2-complete-prov, Step 2 in the workflow]] Linuxクライアントで、次の手順を実行してアクセスを確認します。
    - a. Storage VM のネットワークインターフェイスを使用してボリュームを作成してマウントします。
    - b. 新しくマウントしたボリュームで、テストファイルを作成し、テキストを書き込んでから、ファイルを削除します。

アクセスを確認したら、を実行できます ["ボリュームのエクスポートポリシーを使用してクライアントアクセスを制限します"](#) マウントされたボリュームに対する必要な UNIX の所有権と権限を設定します。

## ボリュームの設定をカスタマイズする

システムのデフォルトを受け入れる代わりに、ボリュームを追加するときにボリューム構成をカスタマイズできます。

## 手順

[\* その他のオプション \*] をクリックした後、必要な機能を選択し、必要な値を入力します。

- リモートボリュームのキャッシュ。
- パフォーマンスサービスレベル（サービス品質、QoS）：

ONTAP 9.8以降では、デフォルト値に加えて、カスタムQoSポリシーを指定したりQoSを無効にしたりできます。

- QoS を無効にするには、「 \* Custom \* 」、「 \* Existing \* 」、「 \* none \* 」の順に選択します。
- 「 \* Custom \* 」を選択し、既存のサービスレベルを指定すると、ローカル階層が自動的に選択されます。
- ONTAP 9.9.1以降では、カスタムのパフォーマンスサービスレベルを作成するように選択した場合、System Managerを使用して、作成するボリュームを配置するローカル階層（手動配置）を手動で選択できます。

このオプションは、リモートキャッシュまたは FlexGroup ボリュームのオプションを選択した場合は使用できません。

- FlexGroup ボリューム（ \* ボリュームデータをクラスタ全体に分散 \* を選択）。

このオプションは、パフォーマンスサービスレベル \* で手動配置 \* を選択した場合は使用できません。 そうしないと、追加するボリュームはデフォルトで FlexVol ボリュームになります。

- ボリュームが設定されているプロトコルのアクセス権限。
- SnapMirror によるデータ保護（ローカルまたはリモート）を実行してから、プルダウンリストからデスティネーションクラスタの保護ポリシーと設定を指定します。
- [保存]\*を選択してボリュームを作成し、クラスタとStorage VMに追加します。



ボリュームを保存したら、に戻ります [\[step2-complete-prov\]](#) NFS を使用して Linux サーバのプロビジョニングを完了する方法

ONTAP でこれを行うその他の方法

実行するタスク	参照先
System Manager Classic （ ONTAP 9.7 以前）	<a href="#">"NFS 構成の概要"</a>
ONTAP コマンドラインインターフェイス（ CLI ）	<a href="#">"CLI を使用した NFS の設定の概要"</a>

エクスポートポリシーを使用してアクセスを管理します

エクスポートポリシーを使用した NFS サーバへの Linux クライアントアクセスの有効化

この手順は、のエクスポートポリシーを作成または変更します ["NFS 対応の既存の Storage VM"](#)。

手順

1. System Manager で、 \* Storage \* > \* Volumes \* をクリックします。
2. NFS 対応ボリュームをクリックし、 \* 詳細 \* をクリックします。
3. [ \* エクスポートポリシーの編集 \* ] をクリックし、 [ \* 既存のポリシーの選択 \* ] または [ \* 新しいポリシーの追加 \* ] をクリックします。

## SMB を使用して Windows サーバ用の NAS ストレージをプロビジョニングする

ONTAP 9.7 以降で使用可能な System Manager を使用して、SMB プロトコルを使用して Windows サーバにストレージを提供するボリュームを作成します。

この手順は、に新しいボリュームを作成します ["SMB対応の既存のStorage VM"](#) およびは、ボリュームのルート (/) ディレクトリ用の共有を作成します。ボリュームの構成時にシステムのデフォルトをそのまま使用することも、カスタム構成を指定することもできます。SMB の初期設定後に、追加の共有を作成したりプロパティを変更したりすることもできます。

FlexVol ボリュームを作成することも、高いパフォーマンスが求められる大規模なファイルシステムには FlexGroup ボリュームを作成することもできます。も参照してください ["FlexGroup を使用して大規模ファイルシステム用の NAS ストレージをプロビジョニング"](#)。

このボリュームの仕様は Ansible Playbook に保存することもできます。詳細については、を参照してください ["Ansible Playbook を使用して、ボリュームや LUN を追加、編集できます"](#)。

ONTAP の SMB プロトコル機能の範囲の詳細については、を参照してください ["SMB リファレンスの概要"](#)。

作業を開始する前に

- ONTAP 9.13.1以降では、新しいボリュームに対して容量分析とアクティビティ追跡をデフォルトで有効にすることができます。System Managerでは、クラスターレベルまたはStorage VMレベルでデフォルト設定を管理できます。詳細については、を参照してください [File System Analytics を有効にします](#)。

手順

### 1. SMB 対応 Storage VM に新しいボリュームを追加

- a. [\* ストレージ]、[ボリューム]の順にクリックし、[\* 追加]をクリックします。
- b. 名前を入力し、Storage VM を選択してサイズを入力します。

SMBプロトコルが設定されているStorage VMのみが表示されます。SMBプロトコルが設定されていないStorage VMが1つしかない場合、\*[Storage VM]\*フィールドは表示されません。

- この時点で\*[保存]\*を選択した場合、System Managerはデフォルトのシステム設定を使用してFlexVolボリュームを作成および追加します。
- [その他のオプション]\*を選択すると、ボリュームの構成をカスタマイズして、許可、サービス品質 (QoS)、データ保護などのサービスを有効にすることができます。を参照してください [\[ボリュームの設定をカスタマイズする\]](#)をクリックし、次の手順を実行するためにここに戻ります。

### 2. [step2-sat-prov-win, Step 2 in the workflow]共有がアクセス可能であることを確認するためにWindowsクライアントに切り替えます。

- a. エクスプローラで、次の形式で共有にドライブをマッピングします。  
\\\_SMB\_Server\_Name\_\_Share\_Name\_
- b. 新しく作成したドライブで、テストファイルを作成し、テキストを書き込み、ファイルを削除します。

アクセスを確認したら、共有 ACL によってクライアントアクセスを制限し、マッピングされたドライブに必要なセキュリティプロパティを設定できます。を参照してください ["SMB 共有を作成"](#) を参照してください。



## 共有を追加または変更する

SMB の初期設定後に共有を追加することができます。共有は、選択したデフォルト値とプロパティを使用して作成されます。これらは後で変更できます。

共有の設定時に次の共有プロパティを設定できます。


- アクセス権限
- 共有プロパティ
  - Hyper-V over SMB および SQL Server over SMB データを含む共有（ONTAP 9.10.1 以降）の継続的可用性を有効にします。次も参照してください。
    - ["Hyper-V over SMB での継続的な可用性を備えた共有の要件"](#)
    - ["SQL Server over SMB での継続的な可用性を備えた共有の要件"](#)
  - この共有へのアクセス時に SMB 3.0 でデータを暗号化する。

初期設定後に、次のプロパティを変更することもできます。

- シンボリックリンク
  - シンボリックリンクとワイドリンクを有効または無効にします
- 共有プロパティ
  - クライアントに Snapshot コピーディレクトリへのアクセスを許可します。
  - oplock を有効にして、クライアントがファイルをロックしてコンテンツをローカルにキャッシュできるようにします（デフォルト）。
  - Access-Based Enumeration（ABE；アクセスベースの列挙）を有効にすると、ユーザのアクセス権限に基づいて共有リソースが表示されます。

## の手順

SMB 対応ボリュームに新しい共有を追加するには、[ストレージ]、[共有]の順にクリックし、[追加]をクリックして[共有 \*\*]を選択します。

既存の共有を変更するには、[ストレージ]、[共有]の順にクリックし、をクリックします  をクリックして、[編集]を選択します

## ボリュームの設定をカスタマイズする

システムのデフォルトを受け入れる代わりに、ボリュームを追加するときにボリューム構成をカスタマイズできます。

## 手順

[\* その他のオプション\*] をクリックした後、必要な機能を選択し、必要な値を入力します。

- リモートボリュームのキャッシュ。
- パフォーマンスサービスレベル（サービス品質、QoS）：

ONTAP 9.8 以降では、デフォルト値の選択に加えて、カスタム QoS ポリシーを指定したり、QoS を無効にしたりできます。



- QoS を無効にするには、「\* Custom \*」、「\* Existing \*」、「\* none \*」の順に選択します。
- 「\* Custom \*」を選択し、既存のサービスレベルを指定すると、ローカル階層が自動的に選択されます。
- ONTAP 9.9.1以降では、カスタムのパフォーマンスサービスレベルを作成するように選択した場合、System Managerを使用して、作成するボリュームを配置するローカル階層（手動配置）を手動で選択できます。

このオプションは、リモートキャッシュまたは FlexGroup ボリュームのオプションを選択した場合は使用できません。

- FlexGroup ボリューム（\* ボリュームデータをクラスタ全体に分散 \* を選択）。

このオプションは、パフォーマンスサービスレベル \* で手動配置 \* を選択した場合は使用できません。そうしないと、追加するボリュームはデフォルトで FlexVol ボリュームになります。

- このオプションは、パフォーマンスサービスレベル \* で手動配置 \* を選択した場合は使用できません。そうしないと、追加するボリュームはデフォルトで FlexVol ボリュームになります。
- ボリュームが設定されているプロトコルに対するアクセス権限。
- SnapMirror によるデータ保護（ローカルまたはリモート）をプルダウンリストからデスティネーションクラスタの保護ポリシーと設定を指定します。
- 「保存」をクリックしてボリュームを作成し、クラスタと Storage VM に追加します。

システムのデフォルトを受け入れる代わりに、ボリュームを追加するときにボリューム構成をカスタマイズできます。

#### 手順

[\* その他のオプション \*] をクリックした後、必要な機能を選択し、必要な値を入力します。

- リモートボリュームのキャッシュ。
- パフォーマンスサービスレベル（サービス品質、QoS）：

ONTAP 9.8以降では、デフォルト値に加えて、カスタムQoSポリシーを指定したりQoSを無効にしたりできます。

- QoS を無効にするには、「\* Custom \*」、「\* Existing \*」、「\* none \*」の順に選択します。
- 「\* Custom \*」を選択し、既存のサービスレベルを指定すると、ローカル階層が自動的に選択されます。
- ONTAP 9.9.1以降では、カスタムのパフォーマンスサービスレベルを作成するように選択した場合、System Managerを使用して、作成するボリュームを配置するローカル階層（手動配置）を手動で選択できます。

このオプションは、リモートキャッシュまたは FlexGroup ボリュームのオプションを選択した場合は使用できません。

- FlexGroup ボリューム（\* ボリュームデータをクラスタ全体に分散 \* を選択）。

このオプションは、パフォーマンスサービスレベル \* で手動配置 \* を選択した場合は使用できません。そうしないと、追加するボリュームはデフォルトで FlexVol ボリュームになります。

- ボリュームが設定されているプロトコルのアクセス権限。
- SnapMirror によるデータ保護（ローカルまたはリモート）を実行してから、プルダウンリストからデステイネーションクラスタの保護ポリシーと設定を指定します。
- [保存]\*を選択してボリュームを作成し、クラスタとStorage VMに追加します。



ボリュームを保存したら、に戻ります [\[step2-compl-prov-win\]](#) SMB を使用した Windows サーバのプロビジョニングの完了

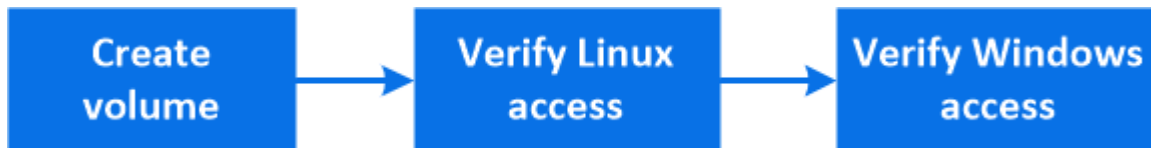
## ONTAP でこれを行うその他の方法

実行するタスク	参照先
System Manager Classic （ ONTAP 9.7 以前）	<a href="#">"SMBセツテイノカイヨウ"</a>
ONTAP のコマンドラインインターフェイス	<a href="#">"CLIヲシヨウシタSMBセツテイノカイヨウ"</a>

## NFS と SMB の両方を使用して Windows と Linux の両方に NAS ストレージをプロビジョニングする

NFS または SMB プロトコルを使用してクライアントにストレージを提供するボリュームを作成します。

この手順は、に新しいボリュームを作成します ["既存の Storage VM で NFS プロトコルと SMB プロトコルの両方が有効になっています"](#)。



NFSプロトコルは、一般にLinux環境で使用されます。 SMBプロトコルは、一般にWindows環境で使用されます。 ただし、 NFSとSMBはどちらもLinuxとWindowsのどちらでも使用できます。

FlexVol ボリュームを作成することも、高いパフォーマンスが求められる大規模なファイルシステムには FlexGroup ボリュームを作成することもできます。 を参照してください ["FlexGroup を使用して大規模ファイルシステム用の NAS ストレージをプロビジョニング"](#)。

このボリュームの仕様は Ansible Playbook に保存することもできます。 詳細については、を参照してください ["Ansible Playbook を使用して、ボリュームや LUN を追加、編集できます"](#)。

## 手順

1. NFS と SMB の両方に対して有効になっている Storage VM に新しいボリュームを追加します。
  - a. [\* ストレージ]、[ボリューム]の順にクリックし、[\* 追加]をクリックします。
  - b. 名前を入力し、Storage VM を選択してサイズを入力します。

NFS プロトコルと SMB プロトコルの両方が設定されている Storage VM のみが表示されます。 NFS プロトコルと SMB プロトコルが設定された Storage VM が 1 つしかない場合、「\* Storage VM \*」

フィールドは表示されません。

- c. をクリックし、[NFS経由でエクスポート]\*を選択します。

デフォルト設定では、すべてのユーザにフルアクセスが許可されます。エクスポートポリシーにはあとから制限付きルールを追加できます。

- d. [\* SMB / CIFS で共有 ] を選択します。

共有が作成され、デフォルトのアクセス制御リスト（ACL）が「Everyone」グループに「Full Control」に設定されます。ACLにはあとから制限を追加できます。

- e. この時点で \* Save \* をクリックすると、System Manager はシステムデフォルトを使用して FlexVol ボリュームを作成および追加します。

または、許可、サービス品質、データ保護など、必要な追加サービスを引き続き有効にすることもできます。を参照してください [\[ボリュームの設定をカスタマイズする\]](#) をクリックし、次の手順を実行するためにここに戻ります。

2. [step2-sed-prov-nfs-smb、ワークフローの手順2] Linuxクライアントで、エクスポートがアクセス可能であることを確認します。

- a. Storage VM のネットワークインターフェイスを使用してボリュームを作成してマウントします。
- b. 新しくマウントしたボリュームで、テストファイルを作成し、テキストを書き込んでから、ファイルを削除します。

3. Windows クライアントで、次の手順を実行して、共有にアクセスできることを確認します。

- a. エクスプローラで、次の形式で共有にドライブをマッピングします。

\\\_SMB\_Server\_Name\_\_Share\_Name\_

- b. 新しく作成したドライブで、テストファイルを作成し、テキストを書き込み、ファイルを削除します。

アクセスを確認したら、を実行できます ["ボリュームのエクスポートポリシーを使用してクライアントアクセスを制限し、共有 ACL を使用してクライアントアクセスを制限します"](#) をクリックし、エクスポートおよび共有ボリュームに対して必要な所有権と権限を設定します。

## ボリュームの設定をカスタマイズする

システムのデフォルトを受け入れる代わりに、ボリュームを追加するときにボリューム構成をカスタマイズできます。

### 手順

[\* その他のオプション \*] をクリックした後、必要な機能を選択し、必要な値を入力します。

- リモートボリュームのキャッシュ。
- パフォーマンスサービスレベル（サービス品質、QoS）：

ONTAP 9.8以降では、デフォルト値に加えて、カスタムQoSポリシーを指定したりQoSを無効にしたりできます。

- QoS を無効にするには、「\* Custom \*」、「\* Existing \*」、「\* none \*」の順に選択します。

- 「\* Custom \*」を選択し、既存のサービスレベルを指定すると、ローカル階層が自動的に選択されます。
- ONTAP 9.9.1以降では、カスタムのパフォーマンスサービスレベルを作成するように選択した場合、System Managerを使用して、作成するボリュームを配置するローカル階層（手動配置）を手動で選択できます。

このオプションは、リモートキャッシュまたは FlexGroup ボリュームのオプションを選択した場合は使用できません。

- FlexGroup ボリューム（\* ボリュームデータをクラスタ全体に分散 \* を選択）。

このオプションは、パフォーマンスサービスレベル \* で手動配置 \* を選択した場合は使用できません。 そうしないと、追加するボリュームはデフォルトで FlexVol ボリュームになります。

- ボリュームが設定されているプロトコルのアクセス権限。
- SnapMirror によるデータ保護（ローカルまたはリモート）を実行してから、プルダウンリストからデステイネーションクラスタの保護ポリシーと設定を指定します。
- [保存]\*を選択してボリュームを作成し、クラスタとStorage VMに追加します。

ボリュームを保存したら、に戻ります [\[step2-compl-prov-nfs-smb\]](#) Windows サーバおよび Linux サーバのマルチプロトコルプロビジョニングを完了するため。

## ONTAP でこれを行うその他の方法

実行するタスク	参照するコンテンツ
System Manager Classic （ ONTAP 9.7 以前）	"SMB と NFS のマルチプロトコル構成の概要"
ONTAP のコマンドラインインターフェイス	"CLIヲシヨウシタSMBセツテイノカイヨウ" [] link: <a href="https://docs.netapp.com/us-en/ontap/nfs-config/index.html">https://docs.netapp.com/us-en/ontap/nfs-config/index.html</a> ["CLI を使用した NFS の設定の概要"] [] "セキュリティ形式とその影響とは" [+] "マルチプロトコル環境でのファイル名とディレクトリ名の大文字と小文字の区別"

## Kerberos を使用してクライアントアクセスを保護

NAS クライアントのストレージアクセスを保護するには、Kerberos を有効にします。

この手順は、で有効になっている既存の Storage VM に Kerberos を設定します "NFS" または "SMB"。

開始する前に、DNS 、 NTP 、 およびを設定しておく必要があります "LDAP" ストレージシステム。



### 手順

1. ONTAP コマンドラインで、Storage VM ルートボリュームに対する UNIX 権限を設定します。

- a. Storage VMのルートボリュームに対する関連する権限を表示します。 `volume show -volume root_vol_name-fields user,group,unix-permissions`

Storage VM のルートボリュームを次のように設定しておく必要があります。

名前	設定
UID	root または ID 0
GID	root または ID 0
UNIX 権限	755

- a. これらの値が表示されない場合は、を使用します `volume modify` コマンドを使用して更新します。

## 2. Storage VM ルートボリュームに対するユーザ権限を設定します。

- a. ローカル UNIX ユーザを表示します。 `vserver services name-service unix-user show -vserver vserver_name`

Storage VM で次の UNIX ユーザを設定しておく必要があります。

ユーザ名	ユーザ ID	プライマリグループ ID
NFS	500ドル	0
ルート	0	0

+

- 。注： NFS クライアントユーザの SPN に対する Kerberos-UNIX ネームマッピングがある場合は、 nfs ユーザは必要ありません。手順 5 を参照してください。

- a. これらの値が表示されない場合は、を使用します `vserver services name-service unix-user modify` コマンドを使用して更新します。

## 3. Storage VM ルートボリュームに対するグループ権限を設定します。

- a. ローカル UNIX グループを表示します。 `vserver services name-service unix-group show -vserver vserver_name`

Storage VM で次の UNIX グループを設定しておく必要があります。

グループ名	グループ ID
デーモン	1.
ルート	0

- a. これらの値が表示されない場合は、を使用します `vserver services name-service unix-group modify` コマンドを使用して更新します。

## 4. Kerberos を設定するには、 System Manager に切り替えてください

## 5. System Manager で、 \* Storage > Storage VM\* をクリックし、 Storage VM を選択します。

## 6. [\* 設定 \*] をクリックします。

7. をクリックします → Kerberos を使用します。
8. Kerberos Realm の下の \* Add \* をクリックし、次のセクションを完了します。
  - Kerberos Realm を追加します  
  
KDC ベンダーに応じて設定の詳細を入力します。
  - Realm にネットワークインターフェイスを追加します  
  
[ \* 追加 ] をクリックし、ネットワーク・インターフェイスを選択します。
9. 必要に応じて、Kerberos プリンシパル名からローカルユーザ名へのマッピングを追加します。
  - a. [ストレージ]>[Storage VM]\*をクリックし、Storage VMを選択します。
  - b. [ \* 設定 \* ] をクリックし、をクリックします → [ \* ネームマッピング ( \* Name Mapping ) ] の下。
  - c. **Kerberos** から **UNIX** の下で、正規表現を使用してパターンと置換を追加します。



## ネームサービスを使用したクライアントアクセスの提供

ONTAP が LDAP または NIS を使用してホスト、ユーザ、グループ、またはネットグループ情報を検索し、NAS クライアントを認証できるようにします。

この手順は、に対して有効になっている既存の Storage VM の LDAP または NIS の設定を作成または変更します **"NFS"** または **"SMB"**。

LDAP 構成の場合は、環境に必要な LDAP の設定の詳細が必要であり、デフォルトの ONTAP LDAP スキーマを使用する必要があります。

### 手順

1. 必要なサービスを設定します。 \* Storage > Storage VM\* をクリックします。
2. Storage VM を選択し、 \* Settings \* をクリックして、をクリックします  LDAP または NIS 。
3. ネームサービススイッチに変更を追加します。クリックします  ネームサービススイッチの下。

## ディレクトリとファイルを管理します

System Manager のボリュームの表示を展開し、ディレクトリとファイルを表示および削除します。

ONTAP 9.9.1以降では、低レイテンシの高速ディレクトリ削除機能によってディレクトリが削除されます。

ONTAP 9.9.1 以降でのファイルシステムの表示の詳細については、を参照してください **"File System Analytics の概要"**。

### ステップ

1. Storage > Volumes （ストレージ）を選択します。ボリュームを展開して内容を表示します。

**System Manager** を使用して、ホスト固有のユーザとグループを管理します

ONTAP 9.10.1 以降では、System Manager を使用して、UNIX または Windows ホストに固有のユーザとグループを管理できます。

次の手順を実行できます。

Windows の場合	「 UNIX 」
<ul style="list-style-type: none"><li>• <a href="#">Windows のユーザとグループを表示します</a></li><li>• <a href="#">[add-edit-delete-Windows]</a></li><li>• <a href="#">[manage-windows-users]</a></li></ul>	<ul style="list-style-type: none"><li>• <a href="#">UNIX ユーザおよびグループを表示します</a></li><li>• <a href="#">[add-edit-delete-UNIX]</a></li><li>• <a href="#">[manage-unix-users]</a></li></ul>

**Windows** のユーザとグループを表示します

System Manager では、Windows ユーザとグループのリストを表示できます。

手順

1. System Manager で、 \* Storage > Storage VM\* をクリックします。
2. Storage VM を選択し、 \* Settings \* タブを選択します。
3. [\* Host Users and Groups\* （ホストユーザーとグループ\*） ] 領域までスクロールします。  
  
「 \* Windows \* 」セクションには、選択した Storage VM に関連付けられている各グループのユーザ数の概要が表示されます。
4. をクリックします → をクリックします。
5. [\* グループ\*] タブをクリックし、 をクリックします ▼ をクリックすると、そのグループに関する詳細が表示されます。
6. グループ内のユーザーを表示するには、グループを選択し、 \* ユーザー \* タブをクリックします。

**Windows** グループを追加、編集、または削除します

System Manager では、Windows グループを追加、編集、削除することで、グループを管理できます。

手順

1. System Manager で、Windows グループのリストを表示します。 を参照してください [Windows のユーザとグループを表示します](#)。
2. [\* グループ\*] タブでは、次のタスクを使用してグループを管理できます。

実行する処理	実行する手順
--------	--------

グループを追加します	<ol style="list-style-type: none"> <li>1. をクリックします <b>+</b> Add。</li> <li>2. グループ情報を入力します。</li> <li>3. 権限を指定します。</li> <li>4. グループメンバーの指定（ローカルユーザ、ドメインユーザ、またはドメイングループの追加）</li> </ol>
グループを編集します	<ol style="list-style-type: none"> <li>1. グループ名の横にあるをクリックします <b>:</b>をクリックし、* 編集 * をクリックします。</li> <li>2. グループ情報を変更します。</li> </ol>
グループを削除します	<ol style="list-style-type: none"> <li>1. 削除するグループの横にあるチェックボックスをオンにします。</li> <li>2. をクリックします <b>🗑</b> Delete。</li> </ol> <p>注： 1つのグループを削除するには、<b>:</b> グループ名の横にある * 削除 * をクリックします。</p>

## Windows ユーザを管理します

System Manager では、Windows ユーザを追加、編集、削除、有効化、無効化することで管理できます。Windows ユーザのパスワードを変更することもできます。

### 手順

1. System Manager で、グループのユーザのリストを表示します。 を参照してください [Windows のユーザとグループを表示します](#)。
2. [Users] タブでは、次のタスクを実行してユーザを管理できます。

実行する処理	実行する手順
ユーザを追加します	<ol style="list-style-type: none"> <li>1. をクリックします <b>+</b> Add。</li> <li>2. ユーザ情報を入力します。</li> </ol>
ユーザを編集します	<ol style="list-style-type: none"> <li>1. ユーザ名の横にあるをクリックします <b>:</b>をクリックし、* 編集 * をクリックします。</li> <li>2. ユーザ情報を変更します。</li> </ol>
ユーザを削除します	<ol style="list-style-type: none"> <li>1. 削除するユーザの横にあるチェックボックスをオンにします。</li> <li>2. をクリックします <b>🗑</b> Delete。</li> </ol> <p>。注： * をクリックして、1 人のユーザーを削除することもできます <b>:</b> ユーザー名の横にある * 削除 * をクリックします。</p>



ユーザパスワードを変更します	<ol style="list-style-type: none"> <li>1. ユーザ名の横にあるをクリックします  をクリックし、[パスワードの変更 *] をクリックします。</li> <li>2. 新しいパスワードを入力し、確認のためにもう一度入力します。</li> </ol>
ユーザを有効にします	<ol style="list-style-type: none"> <li>1. 有効にする各無効なユーザの横にあるチェックボックスをオンにします。</li> <li>2. をクリックします  Enable 。</li> </ol>
ユーザを無効にします	<ol style="list-style-type: none"> <li>1. 無効にする各有効なユーザの横にあるチェックボックスをオンにします。</li> <li>2. をクリックします  Disable 。</li> </ol>


### UNIX ユーザおよびグループを表示します

System Manager では、UNIX ユーザおよびグループのリストを表示できます。

#### 手順

1. System Manager で、 \* Storage > Storage VM\* をクリックします。
2. Storage VM を選択し、 \* Settings \* タブを選択します。
3. [\* Host Users and Groups\* (ホストユーザーとグループ\*)] 領域までスクロールします。

「 \* unix \* 」セクションには、選択した Storage VM に関連付けられた各グループのユーザ数の概要が表示されます。

4. をクリックします  をクリックします。
5. [\* グループ\*] タブをクリックすると、そのグループの詳細が表示されます。
6. グループ内のユーザーを表示するには、グループを選択し、 \* ユーザー \* タブをクリックします。

### UNIX グループを追加、編集、または削除します

System Manager では、UNIX グループを追加、編集、または削除することで、それらのグループを管理できます。

#### 手順

1. System Manager で、UNIX グループのリストを表示します。 を参照してください [UNIX ユーザおよびグループを表示します](#)。
2. [\* グループ\*] タブでは、次のタスクを使用してグループを管理できます。

実行する処理	実行する手順
--------	--------

グループを追加します	<ol style="list-style-type: none"> <li>1. をクリックします <b>+</b> Add。</li> <li>2. グループ情報を入力します。</li> <li>3. （任意）関連付けられたユーザを指定します。</li> </ol>
グループを編集します	<ol style="list-style-type: none"> <li>1. グループを選択します。</li> <li>2. をクリックします <b>✎</b> Edit。</li> <li>3. グループ情報を変更します。</li> <li>4. （オプション）ユーザを追加または削除します。</li> </ol>
グループを削除します	<ol style="list-style-type: none"> <li>1. 削除するグループを選択します。</li> <li>2. をクリックします <b>🗑</b> Delete。</li> </ol>

## UNIX ユーザを管理します

System Manager では、Windows ユーザを追加、編集、削除することで管理できます。

### 手順

1. System Manager で、グループのユーザのリストを表示します。 を参照してください [UNIX ユーザおよびグループを表示します](#)。
2. **[Users]** タブでは、次のタスクを実行してユーザを管理できます。

実行する処理	実行する手順
ユーザを追加します	<ol style="list-style-type: none"> <li>1. をクリックします <b>+</b> Add。</li> <li>2. ユーザ情報を入力します。</li> </ol>
ユーザを編集します	<ol style="list-style-type: none"> <li>1. 編集するユーザを選択します。</li> <li>2. をクリックします <b>✎</b> Edit。</li> <li>3. ユーザ情報を変更します。</li> </ol>
ユーザを削除します	<ol style="list-style-type: none"> <li>1. 削除するユーザを選択します。</li> <li>2. をクリックします <b>🗑</b> Delete。</li> </ol>

## NFS アクティブクライアントを監視します

ONTAP 9.8 以降では、クラスタ上で NFS のライセンスが有効になっている場合に、どの NFS クライアント接続がアクティブになっているかが表示されます。

この方法を使用すると、接続はされているがアイドル状態で切断されている Storage VM にアクティブに接続している NFS クライアントを簡単に確認できます。

各NFSクライアントのIPアドレスについて、\* NFSクライアント\*ディスプレイには次のように表示されます。

\*最終アクセス時刻

\*ネットワークインターフェースのIPアドレス

\* NFS接続のバージョン

\* Storage VM名

また、過去 48 時間にアクティブだった NFS クライアントのリストが \* Storage > Volumes \* の表示にも表示され、NFS クライアントの数は \* Dashboard \* 表示にも表示されます。

## ステップ

1. NFS クライアントアクティビティを表示します。[\*Hosts] > [NFS Clients] をクリックします。

## NAS ストレージを有効にします


NFS を使用して Linux サーバ用の NAS ストレージを有効にします





Storage VMを作成または変更して、NFSサーバがLinuxクライアントにデータを提供できるようにします。

この手順は、NFSプロトコル用に新規または既存のStorage VMを有効にします。ここでは、環境に必要なネットワークサービス、認証サービス、セキュリティサービスの構成の詳細を記載するものとします。



## 手順

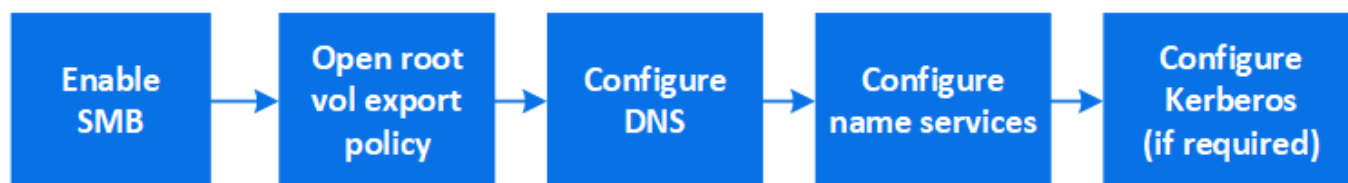
1. Storage VMでNFSを有効にします。
  - a. 新しいStorage VMの場合：\* Storage > Storage VM\*をクリックし、\* Add をクリックして**Storage VM**名を入力し、SMB / CIFS、NFS、S3 タブで NFSの有効化\*を選択します。
    - デフォルトの言語を確認します。
    - ネットワークインターフェースを追加
    - Storage VM管理者アカウント情報を更新する（オプション）。
  - b. 既存のStorage VMの場合：\* Storage > Storage VM\*をクリックし、Storage VMを選択して\* Settings \* をクリックし、をクリックします  NFS \*。
2. Storage VM ルートボリュームのエクスポートポリシーを開きます。
  - a. Storage > Volumes \* をクリックし、Storage VM のルートボリューム（デフォルトは \_volume-name\_root ）を選択して、\* Export Policy \* に表示されるポリシーをクリックします。
  - b. ルールを追加するには、[\* 追加 ] をクリックします。
    - クライアント仕様 = 0.0.0.0/0
    - アクセスプロトコル = nfs
    - アクセスの詳細 = UNIX 読み取り専用

3. ホスト名解決用の DNS の設定：「\* Storage」 > 「Storage VM\*」をクリックし、Storage VM を選択して「\* Settings」をクリックし、をクリックします  DNS の下。
4. 必要に応じてネームサービスを設定
  - a. Storage > Storage VM\* をクリックし、Storage VM を選択して \* Settings \* をクリックし、for をクリックします  LDAP または NIS。
  - b. ネームサービススイッチファイルに変更を加えた場合は追加します。をクリックします  ネームサービススイッチタイトル。
5. 必要に応じて Kerberos を設定します。
  - a. Storage > Storage VM\* をクリックし、Storage VM を選択して、\* Settings \* をクリックします。
  - b. をクリックします  Kerberos タイルで、\* Add \* をクリックします。


**SMB** を使用して **Windows** サーバ用の **NAS** ストレージを有効にします




Storage VMを作成または変更して、SMBサーバでWindowsクライアントにデータを提供できるようにします。

この手順 では、SMBプロトコル用の新規または既存のStorage VMを有効にします。ここでは、環境に必要なネットワークサービス、認証サービス、セキュリティサービスの構成の詳細を記載するものとします。



#### 手順

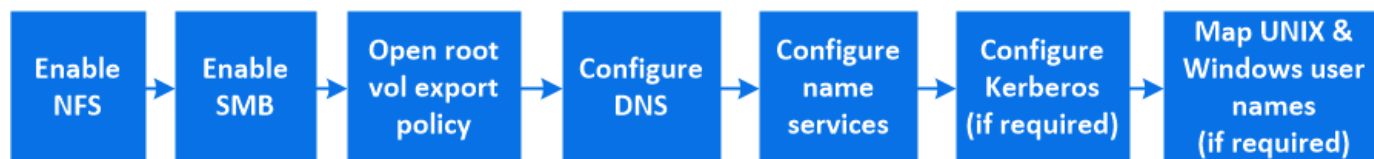
1. Storage VMでSMBを有効にします。
  - a. 新しいStorage VMの場合：\* Storage > Storage VM\*をクリックし、\* Add をクリックして**Storage VM** 名を入力し、SMB / CIFS、NFS、S3 タブで SMB / CIFSの有効化\*を選択します。
    - 次の情報を入力します。
      - 管理者の名前とパスワード
      - サーバ名
      - Active Directoryドメイン
    - 組織単位を確認します。
    - DNS値を確認します。
    - デフォルトの言語を確認します。
    - ネットワークインターフェイスを追加
    - Storage VM管理者アカウント情報を更新する（オプション）。
  - b. 既存のStorage VMの場合：\* Storage > Storage VM\*をクリックし、Storage VMを選択して\* Settings \*をクリックし、をクリックします  \* SMB \*。
2. Storage VM ルートボリュームのエクスポートポリシーを開きます。

- a. Storage > Volumes \* をクリックし、Storage VM のルートボリューム（デフォルトは *volume-name\_root*）を選択し、\* Export Policy \* に表示されるポリシーをクリックします。
  - b. ルールを追加するには、[ \* 追加 ] をクリックします。
    - クライアント仕様= 0.0.0.0/0
    - アクセスプロトコル = SMB
    - アクセスの詳細= NTFS読み取り専用
3. ホスト名解決に使用する DNS を設定します。
- a. Storage > Storage VM\* の順にクリックし、Storage VM を選択し、\* Settings \* をクリックして、をクリックします  **DNS** の下。
  - b. DNS サーバに切り替えて、SMB サーバをマッピングします。
    - フォワードルックアップ（A - アドレスレコード）とリバースルックアップ（PTR - ポインタレコード）のエントリを作成して、SMB サーバ名をデータネットワークインターフェイスの IP アドレスにマッピングします。
    - NetBIOS エイリアスを使用する場合は、エイリアスの正規名（CNAME リソースレコード）のルックアップエントリを作成して、各エイリアスを SMB サーバのデータネットワークインターフェイスの IP アドレスにマッピングします。
4. 必要に応じてネームサービスを設定
- a. Storage > Storage VM\* の順にクリックし、Storage VM を選択し、\* Settings \* をクリックして、をクリックします  「\* ldap \*」または「\* nis \*」の下。
  - b. ネームサービススイッチファイルに変更を加えた場合は追加します。をクリックします  ネームサービススイッチ \* の下。
5. 必要に応じて Kerberos を設定します。
- a. Storage > Storage VM\* をクリックし、Storage VM を選択して、\* Settings \* をクリックします。
  - b. をクリックします → **[Kerberos]** の下にある **[Add]** をクリックします。

**NFS** と **SMB** の両方を使用して、**Windows** と **Linux** の両方で **NAS** ストレージを有効にします








Storage VMを作成または変更して、NFSサーバとSMBサーバがLinuxクライアントやWindowsクライアントにデータを提供できるようにします。

この手順 では、新規または既存のStorage VMがNFSプロトコルとSMBプロトコルの両方を提供できます。ここでは、環境に必要なネットワークサービス、認証サービス、セキュリティサービスの構成の詳細を記載するものとします。



手順

1. Storage VMでNFSとSMBを有効にする
  - a. 新しいStorage VMの場合：\* Storage > Storage VM\* をクリックし、\* Add をクリックして **Storage VM** 名を入力し、SMB / CIFS、NFS、S3 タブで SMB / CIFSの有効化\*と\* NFSの有効化\*を選択します。

- 次の情報を入力します。
    - 管理者の名前とパスワード
    - サーバ名
    - Active Directory ドメイン
  - 組織単位を確認します。
  - DNS 値を確認します。
  - デフォルトの言語を確認します。
  - ネットワークインターフェイスを追加
  - Storage VM 管理者アカウント情報を更新する（オプション）。
- b. 既存の Storage VM の場合： \* Storage > Storage VM\* をクリックし、Storage VM を選択して \* Settings \* をクリックします。NFS または SMB がまだ有効になっていない場合は、次のサブ手順を実行します。
- をクリックします  NFS \*。
  - をクリックします  \* SMB \*。
2. Storage VM ルートボリュームのエクスポートポリシーを開きます。
- a. Storage > Volumes \* をクリックし、Storage VM のルートボリューム（デフォルトは *volume-name\_root*）を選択し、\* Export Policy \* に表示されるポリシーをクリックします。
- b. ルールを追加するには、[ \* 追加 ] をクリックします。
- クライアント仕様 = 0.0.0.0/0
  - アクセスプロトコル = nfs
  - アクセスの詳細 = NFS 読み取り専用
3. ホスト名解決に使用する DNS を設定します。
- a. Storage > Storage VM\* の順にクリックし、Storage VM を選択し、\* Settings \* をクリックして、をクリックします  **DNS** の下。
- b. DNS の設定が完了したら、DNS サーバに切り替えて SMB サーバをマッピングします。
- フォワードルックアップ（A - アドレスレコード）とリバースルックアップ（PTR - ポインタレコード）のエントリを作成して、SMB サーバ名をデータネットワークインターフェイスの IP アドレスにマッピングします。
  - NetBIOS エイリアスを使用する場合は、エイリアスの正規名（CNAME リソースレコード）のルックアップエントリを作成して、各エイリアスを SMB サーバのデータネットワークインターフェイスの IP アドレスにマッピングします。
4. 必要に応じてネームサービスを設定します。
- a. Storage > Storage VM\* の順にクリックし、Storage VM を選択し、\* Settings \* をクリックして、をクリックします  LDAP または NIS。
- b. ネームサービススイッチファイルに変更を加えた場合は追加します。をクリックします  ネームサービススイッチ \* の下。
5. 必要に応じて Kerberos を設定します。をクリックします  Kerberos タイルで、\* Add \* をクリックします。
6. 必要に応じて UNIX と Windows のユーザ名をマッピングします。をクリックします  [\* ネームマッピン

グ\*]で、[\*追加]をクリックします。

この手順は、Windows と UNIX のユーザアカウントが暗黙的にマッピングされない場合にのみ使用します。小文字の Windows ユーザ名が UNIX ユーザ名と一致していれば、ユーザ名は暗黙的にマッピングされます。この手順は、LDAP ユーザ、NIS ユーザ、またはローカルユーザを使用して実行できます。一致しない 2 組のユーザセットがある場合、ネームマッピングを設定する必要があります。

## CLI で NFS を設定

### CLI を使用した NFS の設定の概要

ONTAP 9 の CLI コマンドを使用して、新規または既存の Storage Virtual Machine (SVM) の新しいボリュームまたは qtree に格納されているファイルへの NFS クライアントアクセスを設定できます。

次の手順に従って、ボリュームまたは qtree へのアクセスを設定します。

- ONTAP で現在サポートされている次のいずれかのバージョンを使用する必要がある： NFSv3、NFSv4、NFSv4.1、NFSv4.2、または pNFS を使用する NFSv4.1。
- System Manager や自動スクリプトツールではなく、コマンドラインインターフェイス (CLI) を使用する必要がある。

System Manager を使用して NAS マルチプロトコルアクセスを設定するには、を参照してください ["NFS と SMB の両方を使用して Windows と Linux の両方に NAS ストレージをプロビジョニングする"](#)。

- すべての選択肢について検討するのではなく、ベストプラクティスに従う。

コマンド構文の詳細については、CLI ヘルプおよび ONTAP のマニュアルページを参照してください。

- 新しいボリュームを UNIX ファイル権限を使用して保護する。
- SVM 管理者権限ではなくクラスタ管理者権限を持っている。

ONTAP NFS プロトコル機能の範囲の詳細については、を参照してください ["NFS のリファレンスの概要"](#)。

### ONTAP でこれを行うその他の方法

実行するタスク	参照先
再設計された System Manager (ONTAP 9.7 以降で使用可能)	<a href="#">"NFS を使用して Linux サーバ用の NAS ストレージをプロビジョニング"</a>
System Manager Classic (ONTAP 9.7 以前で使用可能)	<a href="#">"NFS 構成の概要"</a>

### NFS の設定ワークフロー

NFS を設定するには、物理ストレージとネットワークの要件を評価して、目的に応じたワークフローを選択します。新規または既存の SVM への NFS アクセスを設定するか、すでに NFS アクセスの設定が完了している既存の SVM にボリュームまたは qtree を追



加するかによってワークフローが異なります。

準備

物理ストレージ要件を評価

クライアントの NFS ストレージをプロビジョニングする前に、既存のアグリゲート内に新しいボリュームのための十分なスペースがあることを確認する必要があります。十分なスペースがない場合は、既存のアグリゲートにディスクを追加するか、必要なタイプの新しいアグリゲートを作成することができます。

手順

- 1. 既存のアグリゲート内の使用可能なスペースを表示します。

```
storage aggregate show
```

十分なスペースを備えたアグリゲートがある場合は、その名前をワークシートに記録します。

```
cluster::> storage aggregate show
Aggregate      Size Available Used% State  #Vols  Nodes  RAID Status
-----
aggr_0         239.0GB    11.13GB   95% online    1 node1  raid_dp, normal
aggr_1         239.0GB    11.13GB   95% online    1 node1  raid_dp, normal
aggr_2         239.0GB    11.13GB   95% online    1 node2  raid_dp, normal
aggr_3         239.0GB    11.13GB   95% online    1 node2  raid_dp, normal
aggr_4         239.0GB   238.9GB   95% online    5 node3  raid_dp, normal
aggr_5         239.0GB   239.0GB   95% online    4 node4  raid_dp, normal
6 entries were displayed.
```

- 2. 十分なスペースを備えたアグリゲートがない場合は、を使用して既存のアグリゲートにディスクを追加します storage aggregate add-disks コマンドを実行するか、を使用して新しいアグリゲートを作成します storage aggregate create コマンドを実行します

関連情報

["ONTAP の概念"](#)

ネットワーク要件を評価

クライアントに NFS ストレージを提供する前に、 NFS プロビジョニングの要件を満た



すようにネットワークが正しく設定されていることを確認する必要があります。

必要なもの

次のクラスタネットワークオブジェクトを設定する必要があります。

- 物理ポートと論理ポート
- ブロードキャストドメイン
- サブネット（必要な場合）
- IPspace（必要に応じて、デフォルトの IPspace に追加）
- フェイルオーバーグループ（必要に応じて、各ブロードキャストドメインのデフォルトのフェイルオーバーグループに追加）
- 外部ファイアウォール

手順

1. 使用可能な物理ポートと仮想ポートを表示します。

```
network port show
```

- 可能な場合は、データネットワークの速度が最高であるポートを使用する必要があります。
- 最大限のパフォーマンスを得るためには、データネットワーク内のすべてのコンポーネントの MTU 設定が同じである必要があります。

2. サブネット名を使用して LIF の IP アドレスとネットワークマスク値を割り当てる場合は、そのサブネットが存在し、十分な数のアドレスが使用可能であることを確認してください： +

```
network subnet show
```

サブネットには、同じレイヤ 3 サブネットに属する IP アドレスのプールが含まれています。サブネットは、を使用して作成されます `network subnet create` コマンドを実行します

3. 使用可能な IPspace を表示します。

```
network ipspace show
```

デフォルトの IPspace またはカスタムの IPspace を使用できます。

4. IPv6 アドレスを使用する場合は、IPv6 がクラスタで有効になっていることを確認します。

```
network options ipv6 show
```

必要に応じて、を使用してIPv6を有効にできます `network options ipv6 modify` コマンドを実行します

新しい **NFS** ストレージ容量のプロビジョニング先を決定します

新しい NFS ボリュームまたは qtrees を作成する前に、そのボリュームを新規、既存のどちらの SVM に配置するかを決め、配置先の SVM でどのような設定が必要になるかを確認しておく必要があります。これにより、ワークフローが決まります。

## 選択肢

- 新しい SVM、または NFS が有効になっているものの設定されていない既存の SVM でボリュームまたは qtree をプロビジョニングする場合は、「SVM への NFS アクセスの設定」と「NFS 対応 SVM へのストレージ容量の追加」の両方の手順を完了します。

### SVM への NFS アクセスを設定

#### NFS対応SVMにNFSストレージを追加

次のいずれかに該当する場合は、新しい SVM を作成します。

- クラスタで NFS を初めて有効にする場合。
- クラスタ内の既存の SVM で NFS サポートを有効にするのが望ましくない場合。
- クラスタ内に NFS 対応の SVM が 1 つ以上あり、分離されたネームスペースに別の NFS サーバが必要な場合（マルチテナンシーシナリオ）。  
NFS が有効になっているものの設定されていない既存の SVM 上でストレージをプロビジョニングする場合にも、このオプションを選択する必要があります。これが当てはまるのは、SAN アクセス用の SVM を作成している場合や、SVM 作成時にどのプロトコルも有効になっていなかった場合です。

SVM で NFS を有効にしたあとに、ボリュームまたは qtree のプロビジョニングに進みます。

- NFS アクセスの設定が完了している既存の SVM でボリュームまたは qtree をプロビジョニングする場合は、「NFS 対応 SVM へのストレージ容量の追加」の手順を実行します。

#### NFS 対応 SVM にストレージを追加

## NFS 設定情報を収集するためのワークシート

NFS 設定ワークシートを使用すると、クライアントの NFS アクセスを設定するために必要な情報を収集できます。

ストレージをプロビジョニングする場所に関する決定に応じて、ワークシートのいずれかまたは両方のセクションを完了する必要があります。

SVM に対する NFS アクセスを設定する場合は、両方のセクションを完了する必要があります。

- SVM への NFS アクセスを設定する
- NFS 対応 SVM へのストレージ容量の追加

NFS対応SVMにストレージ容量を追加する場合は、次の作業のみを実行してください。

- NFS 対応 SVM へのストレージ容量の追加

パラメータの詳細については、コマンドのマニュアルページを参照してください。

### SVM への NFS アクセスを設定

- SVM を作成するためのパラメータ \*

では、次の値を指定します `vserver create` コマンド（新しいSVMを作成する場合）。

フィールド	説明	あなたの価値
-vserver	新しい SVM の名前を指定します。完全修飾ドメイン名（FQDN）を指定するか、クラスタ内で一意の SVM 名を適用する別の命名規則に従います。	
-aggregate	新しい NFS ストレージ容量に対応できる十分なスペースを持つクラスタ内のアグリゲートの名前を指定します。	
-rootvolume	SVM ルートボリュームの一意の名前を指定します。	
-rootvolume-security-style	SVM の UNIX セキュリティ形式を使用します。	unix
-language	このワークフローではデフォルトの言語設定を使用します。	C.UTF-8
ipspace	IPspace は、Storage Virtual Machine（SVM）が属する個別の IP アドレススペースです。	

• NFS サーバ作成用のパラメータ \*

では、次の値を指定します `vserver nfs create` コマンドは、新しい NFS サーバを作成し、サポートされている NFS バージョンを指定するときに使用します。

NFSv4 以降を有効にする場合は、セキュリティを強化するために LDAP を使用する必要があります。

フィールド	説明	あなたの価値
-v3、-v4.0、-v4.1、-v4.1 -pnfs	必要に応じて NFS バージョンを有効にします。  <div>  <p>ONTAP 9.8以降では、v4.2もサポートされます v4.1 が有効になります。</p> </div>	
-v4-id-domain	ID マッピングのドメイン名を指定します。	
-v4-numeric-ids	所有者 ID 番号のサポート（有効または無効）。	

• LIF 作成用のパラメータ \*

では、次の値を指定します `network interface create` コマンドを使用してLIFを作成します。

Kerberos を使用する場合は、複数の LIF で Kerberos を有効にする必要があります。

フィールド	説明	あなたの価値
<code>-lif</code>	新しい LIF の名前を指定します。	
<code>-role</code>	このワークフローではデータ LIF のロールを使用します。	data
<code>-data-protocol</code>	このワークフローでは NFS プロトコルのみを使用します。	nfs
<code>-home-node</code>	でLIFが戻るノードを指定します <code>network interface revert</code> LIFに対してコマンドを実行します。	
<code>-home-port</code>	の場合にLIFが戻るポートまたはインターフェイスグループ <code>network interface revert</code> LIFに対してコマンドを実行します。	
<code>-address</code>	新しい LIF によるデータアクセスに使用されるクラスタ上の IPv4 または IPv6 アドレスを指定します。	
<code>-netmask</code>	LIF のネットワークマスクとゲートウェイを指定します。	
<code>-subnet</code>	IP アドレスのプール。の代わりに使用されます <code>-address</code> および <code>-netmask</code> アドレスとネットワークを自動的に割り当てます。	
<code>-firewall-policy</code>	このワークフローではデフォルトのデータファイアウォールポリシーを使用します。	data

• DNS ホスト名解決のパラメータ \*

では、次の値を指定します `vserver services name-service dns create` コマンドを使用してDNSを設定します。

フィールド	説明	あなたの価値
-------	----	--------

-domains	最大 5 つの DNS ドメイン名。	
-name-servers	DNS ネームサーバごとに最大 3 つの IP アドレスを指定します。	

#### ネームサービス情報

##### • ローカルユーザー作成用のパラメータ \*

を使用してローカルユーザを作成する場合は、次の値を指定します `vserver services name-service unix-user create` コマンドを実行しますURI から UNIX ユーザを含むファイルをロードすることによってローカルユーザを設定する場合は、これらの値を手動で指定する必要はありません。

	ユーザ名 (-user)	ユーザ ID (-id)	グループ ID (-primary-gid)	フルネーム (-full-name)
例	johnm	一二三	100	ジョンミラー
1.				
2.				
3.				
...				
N				

##### • ローカルグループを作成するためのパラメータ \*

を使用してローカルグループを作成する場合は、次の値を指定します `vserver services name-service unix-group create` コマンドを実行しますURI から UNIX グループを含むファイルをロードすることによってローカルグループを設定する場合は、これらの値を手動で指定する必要はありません。

	グループ名 (-name)	グループ ID (-id)
例	エンジニアリング	100
1.		
2.		
3.		
...		

N		
---	--	--

# • NISのパラメータ\*

では、次の値を指定します `vserver services name-service nis-domain create` コマンドを実行します



ONTAP 9.2以降では、フィールドが表示されます `-nis-servers` フィールドを置き換えます `-servers`。この新しいフィールドには、NISサーバのホスト名またはIPアドレスを指定できます。

フィールド	説明	あなたの価値
<code>-domain</code>	SVM で名前検索に使用される NIS ドメインを指定します。	
<code>-active</code>	アクティブな NIS ドメインサーバを指定します。	true または false
<code>-servers</code>	ONTAP 9.0、9.1 : NIS ドメイン設定で使用される NIS サーバの 1 つ以上の IP アドレスを指定します。	
<code>-nis-servers</code>	ONTAP 9.2 : ドメイン設定で使用される NIS サーバの IP アドレスおよびホスト名をカンマで区切って指定します。	

# • LDAPのパラメータ\*

では、次の値を指定します `vserver services name-service ldap client create` コマンドを実行します

また、自己署名ルートCA証明書も必要です `.pem` ファイル。



ONTAP 9.2以降では、フィールドが表示されます `-ldap-servers` フィールドを置き換えます `-servers`。この新しいフィールドには、LDAP サーバのホスト名または IP アドレスを指定できます。

フィールド	説明	あなたの価値
<code>-vserver</code>	LDAP クライアント設定を作成する SVM の名前を指定します。	
<code>-client-config</code>	新しい LDAP クライアント設定に割り当てる名前。	

フィールド	説明	あなたの価値
-servers	ONTAP 9.0、9.1：1 つ以上の LDAP サーバの IP アドレスをカンマで区切って指定します。	
-ldap-servers	ONTAP 9.2：LDAP サーバの IP アドレスおよびホスト名をカンマで区切って指定します。	
-query-timeout	デフォルトを使用します 3 このワークフローの秒数。	3
-min-bind-level	最小バインド認証レベルを指定します。デフォルトはです anonymous。をに設定する必要があります sasl 署名と封印が設定されている場合。	
-preferred-ad-servers	カンマで区切った IP アドレスのリストによって、優先される Active Directory サーバを指定します。	
-ad-domain	Active Directory ドメインを指定します。	
-schema	使用するスキーマテンプレート。デフォルトまたはカスタムのスキーマを使用できます。	
-port	デフォルトのLDAPサーバポートを使用します 389 をクリックします。	389
-bind-dn	バインドユーザの識別名を指定します。	
-base-dn	ベース識別名。デフォルトはです ""（ルート）。	
-base-scope	デフォルトのベース検索範囲を使用します subnet をクリックします。	subnet
-session-security	LDAP 署名または署名と封印を有効にします。デフォルトはです none。	

フィールド	説明	あなたの価値
-use-start-tls	LDAP over TLS を有効にします。 デフォルトは false。	

• Kerberos 認証のパラメータ \*

では、次の値を指定します `vserver nfs kerberos realm create` コマンドを実行します。Microsoft Active Directory をキー配布センター（KDC）サーバとして使用するか、MIT やその他の UNIX KDC サーバとして使用するかによって、一部の値が異なります。

フィールド	説明	あなたの価値
-vserver	KDC と通信する SVM を指定します。	
-realm	Kerberos Realm を指定します。	
-clock-skew	クライアントとサーバ間で許可されているクロックスキューを指定します	
-kdc-ip	KDC の IP アドレスを指定します。	
-kdc-port	KDC のポート番号を指定します。	
-adserver-name	Microsoft KDC のみ：AD サーバ名を指定します。	
-adserver-ip	Microsoft KDC のみ：AD サーバの IP アドレスを指定します。	
-adminserver-ip	UNIX KDC のみ：管理サーバの IP アドレスを指定します。	
-adminserver-port	UNIX KDC のみ：管理サーバのポート番号を指定します。	
-passwordserver-ip	UNIX KDC のみ：パスワードサーバの IP アドレスを指定します。	
-passwordserver-port	UNIX KDC のみ：パスワードサーバのポートを指定します。	
-kdc-vendor	KDC ベンダーを指定します。	{ Microsoft



Other }	-comment	必要なコメントを指定します。
---------	----------	----------------

では、次の値を指定します `vserver nfs kerberos interface enable` コマンドを実行します

フィールド	説明	あなたの価値
-vserver	Kerberos 設定を作成する SVM の名前を指定します。	
-lif	Kerberos を有効にするデータ LIF を指定します。Kerberos は複数の LIF で有効にすることができます。	
-spn	サービスプリンシパル名 (SPN) を指定します。	
-permitted-enc-types	Kerberos over NFSで許可されている暗号化タイプ。aes-256 クライアントの機能に応じて推奨されます。	
-admin-username	KDC から SPN シークレットキーを直接取得するための KDC 管理者のクレデンシャルを指定します。パスワードは必須です	
-keytab-uri	KDC 管理者のクレデンシャルを持っていない場合は、SPN キーが含まれている KDC の keytab ファイルを指定します。	
-ou	Microsoft KDC の Realm を使用して Kerberos を有効にしたときに Microsoft Active Directory サーバアカウントが作成される組織単位 (OU) を指定します。	

#### NFS 対応 SVM へのストレージ容量の追加

- エクスポートポリシーおよびルールを作成するためのパラメータ \*

では、次の値を指定します `vserver export-policy create` コマンドを実行します

フィールド	説明	あなたの価値
-vserver	新しいボリュームをホストする SVM の名前を指定します。	

-policyname	新しいエクスポートポリシーの名前を指定します。	
-------------	-------------------------	--

では、各ルールに次の値を指定します `vserver export-policy rule create` コマンドを実行します

フィールド	説明	あなたの価値
-clientmatch	クライアント一致条件	
-ruleindex	ルールのリスト内でのエクスポートルールの位置。	
-protocol	このワークフローでは NFS を使用します。	nfs
-rorule	読み取り専用アクセスの認証方式を指定します。	
-rwrule	読み取り / 書き込みアクセスの認証方式を指定します。	
-superuser	スーパーユーザアクセスの認証方式を指定します。	
-anon	匿名ユーザをマッピングするユーザ ID を指定します。	

エクスポートポリシーごとにルールを 1 つ以上作成する必要があります。

-ruleindex	-clientmatch	-rorule	-rwrule	-superuser	-anon
例	0.0.0.0/0 、 @rootaccess_negroup	任意	krb5	システム	65534
1.					
2.					
3.					
...					
N					

• ボリュームを作成するためのパラメータ \*

では、次の値を指定します `volume create` コマンドは、`qtree`の代わりにボリュームを作成する場合に使用します。

フィールド	説明	あなたの価値
<code>-vserver</code>	新しいボリュームをホストする新規または既存の SVM の名前を指定します。	
<code>-volume</code>	新しいボリュームに対して、一意のわかりやすい名前を指定します。	
<code>-aggregate</code>	新しい NFS ボリュームに対応できる十分なスペースを持つクラスター内のアグリゲートの名前を指定します。	
<code>-size</code>	新しいボリュームのサイズとして任意の整数を指定します。	
<code>-user</code>	ボリュームのルートの所有者に設定するユーザの名前または ID を指定します。	
<code>-group</code>	ボリュームのルートの所有者に設定するグループの名前または ID を指定します。	
<code>--security-style</code>	このワークフローには UNIX セキュリティ形式を使用します。	unix
<code>-junction-path</code>	新しいボリュームをマウントするルート ( / ) の下の場所を指定します。	
<code>-export-policy</code>	既存のエクスポートポリシーを使用する場合は、ボリュームの作成時に名前を入力できます。	

• `qtree` を作成するためのパラメータ \*

では、次の値を指定します `volume qtree create` コマンドは、ボリュームではなく `qtree`を作成する場合に使用します。

フィールド	説明	あなたの価値
-------	----	--------

-vserver	qtree を含むボリュームが配置されている SVM の名前。	
-volume	新しい qtree を格納するボリュームの名前を指定します。	
-qtree	新しい qtree に対して、一意のわかりやすい名前を 64 文字以内で指定します。	
-qtree-path	qtreeパスの引数を指定します。形式はです /vol/volume_name/qtree_name\> ボリュームとqtreeを別々の引数として指定する代わりに指定できます。	
-unix-permissions	オプション： qtree の UNIX 権限を指定します。	
-export-policy	既存のエクスポートポリシーを使用する場合は、 qtree の作成時に名前を入力できます。	

## SVM への NFS アクセスを設定

**SVM** を作成します。

NFS クライアントへのデータアクセスを提供するための SVM がクラスタ内に 1 つもない場合は、作成する必要があります。

作業を開始する前に

- ONTAP 9.13.1以降では、Storage VMに最大容量を設定できます。また、SVMの容量レベルがしきい値に近づいたときにアラートを設定することもできます。詳細については、[を参照してください SVM容量の管理](#)。

手順

1. SVM を作成します。

```
vserver create -vserver vserver_name -rootvolume root_volume_name -aggregate aggregate_name -rootvolume-security-style unix -language C.UTF-8 -ipspace ipspace_name
```

- にUNIX設定を使用します -rootvolume-security-style オプション
- デフォルトのC.UTF-8を使用します -language オプション
- 。 ipspace 設定はオプションです。

## 2. 新しく作成した SVM の設定とステータスを確認します。

```
vserver show -vserver vserver_name
```

。 Allowed Protocols フィールドにはNFSを含める必要があります。このリストはあとで編集できます。

。 Vserver Operational State フィールドにはを表示する必要があります running 状態。が表示された場合 initializing 状態にすると、ルートボリュームの作成などの中間処理が失敗したため、SVM を削除して再作成する必要があります。

### 例

次のコマンドは、データアクセス用の SVM を IPspace ipspaceA 内に作成します。

```
cluster1::> vserver create -vserver vs1.example.com -rootvolume root_vs1  
-aggregate aggr1  
-rootvolume-security-style unix -language C.UTF-8 -ipspace ipspaceA
```

```
[Job 2059] Job succeeded:  
Vserver creation completed
```

次のコマンドは、1GBのルートボリュームでSVMが作成され、自動的に起動されて追加されたことを示しています running 状態。ルートボリュームには、ルールを含まないデフォルトのエクスポートポリシーがあるため、ルートボリュームは作成時にエクスポートされません。

```
cluster1::> vserver show -vserver vs1.example.com
Vserver: vs1.example.com
Vserver Type: data
Vserver Subtype: default
Vserver UUID: b8375669-19b0-11e5-b9d1-00a0983d9736
Root Volume: root_vs1
Aggregate: aggr1
NIS Domain: -
Root Volume Security Style: unix
LDAP Client: -
Default Volume Language Code: C.UTF-8
Snapshot Policy: default
Comment:
Quota Policy: default
List of Aggregates Assigned: -
Limit on Maximum Number of Volumes allowed: unlimited
Vserver Admin State: running
Vserver Operational State: running
Vserver Operational State Stopped Reason: -
Allowed Protocols: nfs, cifs, fcp, iscsi, ndmp
Disallowed Protocols: -
QoS Policy Group: -
Config Lock: false
IPspace Name: ipspaceA
```



ONTAP 9.13.1以降では、アダプティブQoSポリシーグループテンプレートを設定して、SVM内のボリュームにスループットの下限と上限の制限を適用できます。このポリシーはSVMの作成後にのみ適用できます。このプロセスの詳細については、[を参照してください アダプティブポリシーグループテンプレートを設定します](#)。

**SVM で NFS プロトコルが有効になっていることを確認します**

SVM で NFS を設定して使用する前に、プロトコルが有効になっていることを確認する必要があります。

このタスクについて

この作業は通常、SVMのセットアップ時に実行します。ただし、セットアップ時にプロトコルを有効にしなかった場合でも、を使用してあとから有効にすることができます `vserver add-protocols` コマンドを実行します



作成したプロトコルは、LIF から追加または削除することはできません。

を使用して、SVMのプロトコルを無効にすることもできます `vserver remove-protocols` コマンドを実行します

## 手順

1. 現在 SVM で有効になっているプロトコルと無効になっているプロトコルを確認します。

```
vserver show -vserver vserver_name -protocols
```

を使用することもできます `vserver show-protocols` コマンドを使用して、クラスタ内のすべての SVM で現在有効になっているプロトコルを表示します。

2. 必要に応じて、プロトコルを有効または無効にします。

- NFS プロトコルを有効にする手順は次のとおりです。

[+]

```
vserver add-protocols -vserver vserver_name -protocols nfs
```

- プロトコルを無効にするには：

[+]

```
vserver remove-protocols -vserver vserver_name -protocols protocol_name  
[,protocol_name,...]
```

3. 有効 / 無効なプロトコルが正しく更新されたことを確認します。

```
vserver show -vserver vserver_name -protocols
```

## 例

次のコマンドは、`vs1` という SVM で現在有効 / 無効（許可 / 不許可）になっているプロトコルを表示します。

```
vs1::> vserver show -vserver vs1.example.com -protocols
```

Vserver	Allowed Protocols	Disallowed Protocols
vs1.example.com	nfs	cifs, fcp, iscsi, ndmp

次のコマンドは、を追加することで NFS 経由のアクセスを許可します `nfs vs1` という SVM で有効になっているプロトコルのリストに移動します。

```
vs1::> vserver add-protocols -vserver vs1.example.com -protocols nfs
```

## SVM ルートボリュームのエクスポートポリシーを開きます

SVM ルートボリュームのデフォルトのエクスポートポリシーには、すべてのクライアントに NFS 経由のアクセスを許可するルールが含まれている必要があります。このようなルールを追加しないと、SVM とそのボリュームに対する NFS クライアントのアクセスがすべて拒否されます。

### このタスクについて

新しい SVM が作成されると、デフォルトのエクスポートポリシー（`default`）が、SVM のルートボリュームに対して自動的に作成されます。SVM 上のデータにクライアントからアクセスできるようにするには、デフォルトのエクスポートポリシーのルールを 1 つ以上作成する必要があります。

デフォルトのエクスポートポリシーを使用するすべての NFS クライアントに対してアクセスが許可されていることを確認してから、ボリュームまたは qtree ごとにカスタムのエクスポートポリシーを作成して各ボリュームへのアクセスを制限します。

#### 手順

1. 既存の SVM を使用している場合は、デフォルトのルートボリュームエクスポートポリシーを確認します。

```
vserver export-policy rule show
```

次のようなコマンド出力が表示されます。

```
cluster::> vserver export-policy rule show -vserver vs1.example.com
-policyname default -instance

Vserver: vs1.example.com
Policy Name: default
Rule Index: 1
Access Protocol: nfs
Client Match Hostname, IP Address, Netgroup, or Domain: 0.0.0.0/0
RO Access Rule: any
RW Access Rule: any
User ID To Which Anonymous Users Are Mapped: 65534
Superuser Security Types: any
Honor SetUID Bits in SETATTR: true
Allow Creation of Devices: true
```

オープンアクセスを許可するこのようなルールが存在する場合、このタスクは完了です。表示されない場合は、次の手順に進みます。

2. SVM ルートボリュームのエクスポートルールを作成します。

```
vserver export-policy rule create -vserver vserver_name -policyname default
-ruleindex 1 -protocol nfs -clientmatch 0.0.0.0/0 -rorule any -rwrule any
-superuser any
```

Kerberosで保護されたボリュームのみをSVMに含める場合は、エクスポートルールオプションを設定できます `-rorule`、`-rwrule` および `-superuser` ルートボリュームのをに設定します `krb5` または `krb5i`。例：

```
-rorule krb5i -rwrule krb5i -superuser krb5i
```

3. を使用してルールの作成を確認します `vserver export-policy rule show` コマンドを実行します

#### 結果

これで、SVM で作成されたすべてのボリュームまたは qtree に、すべての NFS クライアントからアクセスできるようになります。



## NFS サーバを作成します

クラスタでNFSのライセンスが有効であることを確認したら、を使用できます `vserver nfs create` コマンドを使用してSVMにNFSサーバを作成し、SVMがサポートするNFSのバージョンを指定します。

このタスクについて

SVM は、NFS の 1 つ以上のバージョンをサポートするように設定できます。NFSv4 以降をサポートする場合は、次の点に注意してください。

- NFSv4 ユーザ ID マッピングドメイン名が、NFSv4 サーバとターゲットクライアントで同じである必要があります。

NFSv4 サーバとクライアントで同じ名前が使用されていれば、LDAP または NIS のドメイン名と同じにする必要はありません。

- ターゲットクライアントで NFSv4 数値 ID 設定がサポートされている必要があります。
- セキュリティ上の理由から、NFSv4 環境では、LDAP をネームサービスに使用する必要があります。

作業を開始する前に

SVM を、NFS プロトコルを許可するように設定しておく必要があります。

手順

1. クラスタ上で NFS のライセンスが有効であることを確認します。

```
system license show -package nfs
```

表示されない場合は、営業担当者にお問い合わせください。

2. NFS サーバを作成します。

```
vserver nfs create -vserver vserver_name -v3 {enabled|disabled} -v4.0  
{enabled|disabled} -v4-id-domain nfsv4_id_domain -v4-numeric-ids  
{enabled|disabled} -v4.1 {enabled|disabled} -v4.1-pnfs {enabled|disabled}
```

NFS バージョンは任意の組み合わせで有効にすることができます。pNFSをサポートする場合は、両方を有効にする必要があります `-v4.1` および `-v4.1-pnfs` オプション (Options)

v4 以降を有効にする場合は、次のオプションが正しく設定されていることも確認する必要があります。

- `-v4-id-domain`

(オプション) このパラメータは、NFSv4 プロトコルの定義に応じて、ユーザ名およびグループ名の文字列形式のドメイン部分を指定します。デフォルト ONTAP では、NIS ドメインが設定されている場合は NIS ドメインを、設定されていない場合は DNS ドメインが使用されます。ターゲットクライアントで使用されているドメイン名に一致する値を指定する必要があります。

- `-v4-numeric-ids`

(オプション) このパラメータは、NFSv4 所有者属性で数値文字列識別子のサポートを有効にするかどうかを指定します。デフォルト設定は `enabled` ですが、ターゲットクライアントがこの設定をサポート

ートすることを確認する必要があります。

NFSのその他の機能は、を使用してあとから有効にすることができます `vserver nfs modify` コマンドを実行します

3. NFS が実行されていることを確認します。

```
vserver nfs status -vserver vserver_name
```

4. NFS が必要に応じて設定されていることを確認します。

```
vserver nfs show -vserver vserver_name
```

例

次のコマンドは、NFSv3 と NFSv4.0 が有効な `vs1` という名前の SVM 上に NFS サーバを作成します。

```
vs1::> vserver nfs create -vserver vs1 -v3 enabled -v4.0 enabled -v4-id  
-domain my_domain.com
```

次のコマンドは、`vs1` という名前の新しい NFS サーバのステータスと設定値を確認します。

```
vs1::> vserver nfs status -vserver vs1  
The NFS server is running on Vserver "vs1".  
  
vs1::> vserver nfs show -vserver vs1  
  
Vserver: vs1  
General NFS Access: true  
NFS v3: enabled  
NFS v4.0: enabled  
UDP Protocol: enabled  
TCP Protocol: enabled  
Default Windows User: -  
NFSv4.0 ACL Support: disabled  
NFSv4.0 Read Delegation Support: disabled  
NFSv4.0 Write Delegation Support: disabled  
NFSv4 ID Mapping Domain: my_domain.com  
...
```

## LIF を作成

LIF は、物理ポートまたは論理ポートに関連付けられた IP アドレスです。コンポーネントに障害が発生しても、LIF は別の物理ポートにフェイルオーバーまたは移行できるため、引き続きネットワークと通信できます。

必要なもの

- 基盤となる物理または論理ネットワークポートが管理用に設定されている必要があります up ステータス。
- サブネット名を使用して LIF の IP アドレスとネットワークマスク値を割り当てる場合は、そのサブネットがすでに存在している必要があります。

サブネットには、同じレイヤ 3 サブネットに属する IP アドレスのプールが含まれています。これらはを使用して作成されます `network subnet create` コマンドを実行します

- LIF で処理するトラフィックのタイプを指定するメカニズムが変更されました。ONTAP 9.5 以前では、LIF はロールを使用して処理するトラフィックのタイプを指定していました。ONTAP 9.6 以降では、サービスポリシーを使用して、処理するトラフィックのタイプを指定します。

#### このタスクについて

- 同じネットワークポート上に IPv4 と IPv6 の両方の LIF を作成できます。
- Kerberos 認証を使用する場合は、複数の LIF で Kerberos を有効にします。
- クラスタ内の LIF の数が多い場合は、を使用して、クラスタでサポートされる LIF の容量を確認できます `network interface capacity show` コマンドとを使用して、各ノードでサポートされる LIF の容量を確認します `network interface capacity details show` コマンド (advanced 権限レベル)。
- ONTAP 9.7 以降では、同じサブネット内に SVM 用の他の LIF がすでに存在する場合、LIF のホームポートを指定する必要はありません。ONTAP は、同じサブネットにすでに設定されている他の LIF と同じブロードキャストドメインにある指定したホームノード上のランダムなポートを自動的に選択します。

ONTAP 9.4 以降では、FC-NVMe がサポートされます。FC-NVMe LIF を作成する場合は、次の点に注意してください。

- LIF を作成する FC アダプタで NVMe プロトコルがサポートされている必要があります。
- データ LIF で使用できるデータプロトコルは FC-NVMe のみです。
- SAN をサポートする Storage Virtual Machine (SVM) ごとに、管理トラフィックを処理する LIF を 1 つ設定する必要があります。
- NVMe の LIF とネームスペースは、同じノードでホストする必要があります。
- データトラフィックを処理する NVMe LIF は SVM ごとに 1 つだけ設定できます。

#### 手順

##### 1. LIF を作成します。

```
network interface create -vserver vservice_name -lif lif_name -role data -data
-protocol nfs -home-node node_name -home-port port_name {-address IP_address
-netmask IP_address | -subnet-name subnet_name} -firewall-policy data -auto
-revert {true|false}
```

オプション	説明
• ONTAP 9.5 以前 *	<code>`network interface create -vserver vservice_name -lif lif_name -role data -data-protocol nfs -home-node node_name -home-port port_name {-address IP_address -netmask IP_address</code>

-subnet-name <i>subnet_name</i> } -firewall-policy data -auto-revert {true	false}`
• ONTAP 9.6 以降 *	`network interface create -vserver <i>vserver_name</i> -lif <i>lif_name</i> -role data -data-protocol nfs -home-node <i>node_name</i> -home-port <i>port_name</i> {-address <i>IP_address</i> -netmask <i>IP_address</i>
-subnet-name <i>subnet_name</i> } -firewall-policy data -auto-revert {true	false}`

- 。 -role サービスポリシーを使用してLIFを作成する場合はパラメータは必要ありません（ONTAP 9.6以降）。
- 。 -data-protocol パラメータはLIFの作成時に指定する必要があります。あとで変更するには、データLIFを削除して再作成する必要があります。
- 。 -data-protocol サービスポリシーを使用してLIFを作成する場合はパラメータは必要ありません（ONTAP 9.6以降）。
- 。 -home-node は、の実行時にLIFが戻るノードです network interface revert LIFに対してコマンドを実行します。

を使用して、LIFをホームノードおよびホームポートに自動的にリバートするかどうかを指定することもできます -auto-revert オプション

- 。 -home-port は、の実行時にLIFが戻る物理ポートまたは論理ポートです network interface revert LIFに対してコマンドを実行します。
- 。 でIPアドレスを指定できます -address および -netmask オプションを選択するか、を使用してサブネットからの割り当てを有効にします -subnet\_name オプション
- 。 サブネットを使用して IP アドレスとネットワークマスクを指定した場合、サブネットにゲートウェイが定義されていると、そのサブネットを使用して LIF を作成するときにゲートウェイへのデフォルトルートが SVM に自動的に追加されます。
- 。 サブネットを使用せずに手動で IP アドレスを割り当てると、クライアントまたはドメインコントローラが別の IP サブネットにある場合にゲートウェイへのデフォルトルートの設定が必要になることがあります。 network route create のマニュアルページには、SVM内での静的ルートの作成に関する情報が記載されています。
- 。 をクリックします -firewall-policy オプションで、同じデフォルトを使用します data をLIFのルールとして使用します。

必要に応じて、カスタムファイアウォールポリシーをあとから作成して追加できます。



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

- 。 -auto-revert 起動時、管理データベースのステータスが変化したとき、ネットワーク接続が確立されたときなどの状況で、データLIFがホームノードに自動的にリバートされるかどうかを指定できます。デフォルト設定はです false`に設定することもできます `false 環境内のネットワーク管理ポリシーによって異なります。

2. を使用して、LIFが正常に作成されたことを確認します `network interface show` コマンドを実行します
3. 設定した IP アドレスに到達できることを確認します。

対象	使用
IPv4 アドレス	<code>network ping</code>
IPv6アドレス	<code>network ping6</code>

4. Kerberos を使用する場合は、手順 1~3 を繰り返して追加の LIF を作成します。

これらの各 LIF で Kerberos を個別に有効にする必要があります。

#### 例

次のコマンドでは、を使用してLIFを作成し、IPアドレスとネットワークマスク値を指定します `-address` および `-netmask` パラメータ：

```
network interface create -vserver vs1.example.com -lif datalif1 -role data
-data-protocol nfs -home-node node-4 -home-port elc -address 192.0.2.145
-netmask 255.255.255.0 -firewall-policy data -auto-revert true
```

次のコマンドは、LIF を作成し、IP アドレスとネットワークマスク値を指定したサブネット（`client1_sub`）から割り当てています。

```
network interface create -vserver vs3.example.com -lif datalif3 -role data
-data-protocol nfs -home-node node-3 -home-port elc -subnet-name
client1_sub -firewall-policy data -auto-revert true
```

次のコマンドは、`cluster-1` 内のすべての LIF を表示します。`datalif1` および `datalif3` というデータ LIF には IPv4 アドレスを設定しています。一方、`datalif4` には IPv6 アドレスを設定しています。

```
network interface show
```

Vserver	Logical Interface	Status Admin/Oper	Network Address/Mask	Current Node	Current Port	Is
Home						
-----	-----	-----	-----	-----	-----	-----
cluster-1						
true	cluster_mgmt	up/up	192.0.2.3/24	node-1	e1a	
node-1						
true	clus1	up/up	192.0.2.12/24	node-1	e0a	
true	clus2	up/up	192.0.2.13/24	node-1	e0b	
true	mgmt1	up/up	192.0.2.68/24	node-1	e1a	
node-2						
true	clus1	up/up	192.0.2.14/24	node-2	e0a	
true	clus2	up/up	192.0.2.15/24	node-2	e0b	
true	mgmt1	up/up	192.0.2.69/24	node-2	e1a	
vs1.example.com						
true	datalif1	up/down	192.0.2.145/30	node-1	e1c	
vs3.example.com						
true	datalif3	up/up	192.0.2.146/30	node-2	e0c	
true	datalif4	up/up	2001::2/64	node-2	e0c	
5 entries were displayed.						

次のコマンドは、に割り当てられたNASデータLIFを作成する方法を示しています default-data-files サービスポリシー：

```
network interface create -vserver vs1 -lif lif2 -home-node node2 -homeport e0d -service-policy default-data-files -subnet-name ipspace1
```

ホスト名解決に使用する **DNS** を有効にします

を使用できます vsriver services name-service dns コマンドを使用してSVMでDNSを有効にし、ホスト名解決にDNSを使用するように設定します。ホスト名は外部

DNS サーバを使用して解決されます。

必要なもの

ホスト名を検索するために、サイト規模の DNS サーバが使用可能である必要があります。

単一点障害を回避するには、複数の DNS サーバを設定する必要があります。。 `vserver services name-service dns create` 入力したDNSサーバ名が1つだけの場合は警告が表示されます。

このタスクについて

SVM での動的 DNS の設定については、『ネットワーク管理ガイド』を参照してください。

手順

1. SVM で DNS を有効にします。

```
vserver services name-service dns create -vserver vserver_name -domains
domain_name -name-servers ip_addresses -state enabled
```

次のコマンドは、SVM vs1 で外部 DNS サーバを有効にします。

```
vserver services name-service dns create -vserver vs1.example.com
-domains example.com -name-servers 192.0.2.201,192.0.2.202 -state
enabled
```



ONTAP 9.2以降では、`vserver services name-service dns create` コマンドは設定の自動検証を実行し、ONTAP がネームサーバに接続できない場合はエラーメッセージを報告します。

2. を使用して、DNSドメイン設定を表示します `vserver services name-service dns show` コマンドを実行します

次のコマンドは、クラスタ内のすべての SVM の DNS 設定を表示します。

```
vserver services name-service dns show
```

Vserver	State	Domains	Name Servers
cluster1	enabled	example.com	192.0.2.201, 192.0.2.202
vs1.example.com	enabled	example.com	192.0.2.201, 192.0.2.202

次のコマンドは、SVM vs1 の DNS 設定の詳細を表示します。

```
vserver services name-service dns show -vserver vs1.example.com
Vserver: vs1.example.com
Domains: example.com
Name Servers: 192.0.2.201, 192.0.2.202
Enable/Disable DNS: enabled
Timeout (secs): 2
Maximum Attempts: 1
```

3. を使用してネームサーバのステータスを検証します `vserver services name-service dns check` コマンドを実行します

。 `vserver services name-service dns check` コマンドはONTAP 9.2以降で使用できます。

```
vserver services name-service dns check -vserver vs1.example.com
```

Vserver	Name Server	Status	Status Details
vs1.example.com	10.0.0.50	up	Response time (msec): 2
vs1.example.com	10.0.0.51	up	Response time (msec): 2

## ネームサービスを設定

### ネームサービスの概要を設定

ストレージシステムの構成によっては、クライアントに適切なアクセス権を提供するために ONTAP でホスト、ユーザ、グループ、またはネットグループ情報を検索できるようにする必要があります。この情報を取得するためには、ONTAP がローカルまたは外部のネームサービスにアクセスできるようにネームサービスを設定する必要があります。

NIS や LDAP などのネームサービスは、クライアント認証時の名前検索を容易にするために使用する必要があります。特に NFSv4 以降を導入する際は、セキュリティ強化のために、可能なかぎり LDAP を使用することを推奨します。外部ネームサーバが使用できない場合に備えて、ローカルのユーザとグループも設定する必要があります。

ネームサービス情報は、すべてのソースで同期を維持する必要があります。

### ネームサービススイッチテーブルを設定します

ONTAP がローカルまたは外部のネームサービスに問い合わせるホスト、ユーザ、グループ、ネットグループ、またはネームマッピングの情報を取得できるようにするには、ネームサービススイッチテーブルを正しく設定する必要があります。

### 必要なもの



ホスト、ユーザ、グループ、ネットグループ、またはネームマッピングで現在の環境に該当するように使用するネームサービスを決定しておく必要があります。

ネットグループの使用を計画する場合、ネットグループ内に指定されているすべての IPv6 アドレスは、RFC 5952 での指定どおりに短縮および圧縮されている必要があります。

このタスクについて

使用されていない情報ソースは含めないでください。たとえば、環境でNISが使用されていない場合は、を指定しないでください `-sources nis` オプション

手順

1. ネームサービススイッチテーブルに必要なエントリを追加します。

```
vserver services name-service ns-switch create -vserver vserver_name -database database_name -sources source_names
```

2. ネームサービススイッチテーブルに想定されるエントリが適切な順序で格納されていることを確認します。

```
vserver services name-service ns-switch show -vserver vserver_name
```

修正する場合は、を使用する必要があります `vserver services name-service ns-switch modify` または `vserver services name-service ns-switch delete` コマンド

例

次の例は、SVM vs1 がローカルネットグループファイルを使用し、外部 NIS サーバがネットグループ情報をこの順序で検索するように、ネームサービススイッチテーブルに新しいエントリを作成します。

```
cluster::> vserver services name-service ns-switch create -vserver vs1  
-database netgroup -sources files,nis
```

完了後

- データアクセスを提供するには、SVM 用に指定したネームサービスを設定する必要があります。
- SVM 用のネームサービスを削除する場合は、ネームサービススイッチテーブルからも削除する必要があります。

ネームサービススイッチテーブルからネームサービスを削除しないと、ストレージシステムへのクライアントアクセスが想定どおりに機能しない場合があります。

ローカル **UNIX** ユーザおよびグループを設定する

ローカル **UNIX** ユーザおよびグループの概要を設定する

SVM 上で、認証およびネームマッピングにローカル UNIX ユーザおよびグループを使用できます。UNIX ユーザおよびグループは、手動で作成することも、Uniform Resource Identifier (URI) から UNIX ユーザまたはグループを含むファイルをロードすることもできます。

クラスタ内のローカル UNIX ユーザグループおよびグループメンバーの合計数に対するデフォルトの上限値は 32、768 です。クラスタ管理者はこの制限を変更できます。

## ローカル **UNIX** ユーザを作成します

を使用できます `vserver services name-service unix-user create` コマンドを使用してローカルUNIXユーザを作成します。ローカル UNIX ユーザは、SVM 上に UNIX ネームサービスオプションとして作成し、ネームマッピングの処理で使用する UNIX ユーザです。

### ステップ

1. ローカル UNIX ユーザを作成します。

```
vserver services name-service unix-user create -vserver vserver_name -user user_name -id integer -primary-gid integer -full-name full_name
```

`-user user_name` ユーザ名を指定します。ユーザ名は 64 文字以内にする必要があります。

`-id integer` 割り当てるユーザIDを指定します。

`-primary-gid integer` プライマリグループIDを指定します。これにより、ユーザがプライマリグループに追加されます。ユーザを作成したあと、手動でユーザを目的の追加グループに追加できます。

### 例

次のコマンドは、johnm というローカル UNIX ユーザ（フルネームは「John Miller」）を vs1 という SVM 上に作成します。ユーザ ID は 123 で、プライマリグループ ID は 100 です。

```
node::> vserver services name-service unix-user create -vserver vs1 -user johnm -id 123 -primary-gid 100 -full-name "John Miller"
```

## URI からローカル **UNIX** ユーザをロードします

SVMで個々のローカルUNIXユーザを手動で作成する別の方法として、ローカルUNIXユーザのリストをUniform Resource Identifier (URI) からSVMにロードすることで、タスクを簡易化できます。(vserver services name-service unix-user load-from-uri)。

### 手順

1. ロードするローカル UNIX ユーザのリストが含まれているファイルを作成します。

ファイルには、UNIX内のユーザ情報が含まれている必要があります `/etc/passwd` 形式：

```
user_name: password: user_ID: group_ID: full_name
```

このコマンドにより、の値が破棄されます `password` フィールドと、の後のフィールドの値 `full_name` フィールド (`home_directory` および `shell`)。

サポートされる最大ファイルサイズは 2.5MB です。

2. リストに重複した情報が含まれていないことを確認します。

リストに重複したエントリが含まれている場合、リストのロードは失敗し、エラーメッセージが表示されます。

3. ファイルをサーバにコピーします。

サーバには、HTTP、HTTPS、FTP、または FTPS 経由でストレージシステムから到達できる必要があります。

4. ファイルの URI を確認します。

この URI は、ファイルの場所を示すためにストレージシステムに指定するアドレスです。

5. ローカル UNIX ユーザのリストが含まれているファイルを、URI から SVM にロードします。

```
vserver services name-service unix-user load-from-uri -vserver vserver_name  
-uri {ftp|http|https|https}://uri -overwrite {true|false}
```

`-overwrite {true false}` は、エントリを上書きするかどうかを指定します。デフォルトは `false`。

#### 例

次のコマンドは、ローカルUNIXユーザのリストをURIからロードします

`ftp://ftp.example.com/passwd` vs1 という名前の SVM に追加します。URI を使用してロードした情報によって SVM 内の既存のユーザが上書きされることはありません。

```
node::> vserver services name-service unix-user load-from-uri -vserver vs1  
-uri ftp://ftp.example.com/passwd -overwrite false
```

#### ローカル **UNIX** グループを作成します

を使用できます `vserver services name-service unix-group create` コマンドを使用して、SVM に対してローカルな UNIX グループを作成します。ローカル UNIX グループはローカル UNIX ユーザとともに使用されます。

#### ステップ

1. ローカル UNIX グループを作成します。

```
vserver services name-service unix-group create -vserver vserver_name -name  
group_name -id integer
```

`-name group_name` グループ名を指定します。グループ名は 64 文字以内にする必要があります。

`-id integer` 割り当てるグループIDを指定します。

例

次のコマンドは、vs1 という名前の SVM 上に eng という名前のローカルグループを作成します。グループ ID は 101 です。

```
vs1::> vserver services name-service unix-group create -vserver vs1 -name  
eng -id 101
```

ローカル **UNIX** グループにユーザを追加します

を使用できます `vserver services name-service unix-group adduser` コマンドを使用して、SVMに対してローカルなUNIXグループにユーザを追加します。

ステップ

1. ローカル UNIX グループにユーザを追加します。

```
vserver services name-service unix-group adduser -vserver vserver_name -name  
group_name -username user_name
```

`-name group_name` ユーザのプライマリグループに加えて、ユーザを追加するUNIXグループの名前を指定します。

例

次のコマンドは、vs1 という SVM の eng というローカル UNIX グループに、max という名前のユーザを追加します。

```
vs1::> vserver services name-service unix-group adduser -vserver vs1 -name  
eng  
-username max
```

**URI** からローカル **UNIX** グループをロードします

個々のローカルUNIXグループを手動で作成する別の方法として、を使用して、ローカルUNIXグループのリストをUniform Resource Identifier (URI) からSVMにロードすることができます `vserver services name-service unix-group load-from-uri` コマンドを実行します

手順

1. ロードするローカル UNIX グループのリストが含まれているファイルを作成します。

ファイルには、UNIX内のグループ情報が含まれている必要があります `/etc/group` 形式：

```
group_name: password: group_ID: comma_separated_list_of_users
```

このコマンドにより、の値が破棄されます `password` フィールド。

サポートされる最大ファイルサイズは 1MB です。

グループファイルの 1 行の最大長は、32、768 文字です。

2. リストに重複した情報が含まれていないことを確認します。

重複するエントリがリストに含まれていてはいけません。含まれていると、リストのロードに失敗します。SVMにすでにエントリがある場合は、を設定する必要があります `-overwrite` パラメータの値 `true` 既存のすべてのエントリを新しいファイルで上書きするか、または既存のエントリと重複するエントリが新しいファイルに含まれていないことを確認します。

3. ファイルをサーバにコピーします。

サーバには、HTTP、HTTPS、FTP、または FTPS 経由でストレージシステムから到達できる必要があります。

4. ファイルの URI を確認します。

この URI は、ファイルの場所を示すためにストレージシステムに指定するアドレスです。

5. ローカル UNIX グループのリストが含まれているファイルを、URI から SVM にロードします。

```
vserver services name-service unix-group load-from-uri -vserver vserver_name  
-uri {ftp|http|https|https}://uri -overwrite {true|false}
```

`-overwrite true false` は、エントリを上書きするかどうかを指定します。デフォルトは `false`。このパラメータを指定した場合 `true` と指定 ONTAP した SVM の既存のローカル UNIX グループ データベース全体が、ロードするファイルのエントリで置き換えられます。

## 例

次のコマンドは、ローカル UNIX グループのリストを URI からロードします

`ftp://ftp.example.com/group vs1` という名前の SVM に追加します。URI を使用してロードした情報によって SVM 内の既存のグループが上書きされることはありません。

```
vs1::> vserver services name-service unix-group load-from-uri -vserver vs1  
-uri ftp://ftp.example.com/group -overwrite false
```

## ネットグループの使用

### ネットグループの概要の使用

ネットグループは、ユーザ認証に使用でき、また、エクスポートポリシールールでクライアントを照合するためにも使用できます。を使用して、外部名前サーバ（LDAP または NIS）からネットグループへのアクセスを提供したり、Uniform Resource Identifier（URI）から SVM にネットグループをロードしたりできます `vserver services name-service netgroup load` コマンドを実行します

### 必要なもの

ネットグループを使用する前に、次の条件を満たしていることを確認する必要があります。

- ネットグループ内のすべてのホストは、ソース（NIS、LDAP、またはローカルファイル）に関係なく、フォワードおよびリバース DNS ルックアップの一貫性を提供するために、フォワード（A）およびリバース（PTR）の両方の DNS レコードを持つ必要があります。

また、クライアントの IP アドレスが複数の PTR レコードを持つ場合は、それらすべてのホスト名がネットグループのメンバーであり、対応する A レコードを持っている必要があります。

- ネットグループ内のすべてのホストの名前が、そのソース（NIS、LDAP、またはローカルファイル）に関係なく、正しいスペルで、かつ大文字 / 小文字を正しく使用している必要があります。ネットグループで使用されているホスト名に不整合があると、エクスポートチェックの失敗など、予期しない動作が発生する可能性があります。
- ネットグループ内に指定されているすべての IPv6 アドレスは、RFC 5952 での指定どおりに短縮および圧縮されている必要があります。

たとえば、2011 : hu9 : 0 : 0 : 0 : 0 : 3 : 1 は 2011 : hu9 : 3 : 1 に短縮する必要があります。

#### このタスクについて

ネットグループについては次の処理を実行できます。

- を使用できます `vserver export-policy netgroup check-membership` クライアントIPが特定のネットグループのメンバーであるかどうかを確認するためのコマンド。
- を使用できます `vserver services name-service getxxbyyy netgrp` コマンドを使用して、クライアントがネットグループの一部であるかどうかを確認します。

検索を実行する基盤となるサービスは、設定済みのネームサービススイッチの順序に基づいて選択されます。

#### ネットグループを **SVM** にロードする

エクスポートポリシールールでクライアントの照合に使用できる方法の 1 つは、ネットグループにリストされているホストを使用することです。ネットグループは、外部ネームサーバに格納されているネットグループを使用する代わりに、Uniform Resource Identifier (URI) を使用して SVM にロードすることもできます (`vserver services name-service netgroup load`)。

#### 必要なもの

ネットグループファイルは、SVM にロードする前に、次の要件を満たしている必要があります。

- ファイルは、NIS の設定に使用されるのと同じ適切なネットグループテキストファイル形式を使用する必要があります。

ONTAP は、ロードを行う前にネットグループテキストファイル形式をチェックします。ファイルにエラーが含まれている場合、ファイルはロードされず、ファイルで実行する必要のある修正を示すメッセージが表示されます。エラーを修正後に、ネットグループファイルを指定した SVM に再ロードできます。

- ネットグループファイル内のホスト名に含まれる英文字は、すべて小文字にする必要があります。
- サポートされる最大ファイルサイズは 5MB です。

- ネットグループでサポートされる最大ネストレベルは 1000 です。
- ネットグループファイルでホスト名を定義する際に使用できるのは、プライマリ DNS ホスト名のみです。

エクスポートへのアクセスに関する問題を回避するために、ホスト名の定義には DNS CNAME やラウンドロビンレコードを使用しないでください。

- ネットグループファイル内の 3 つの値のうちユーザおよびドメインの部分は、ONTAP でサポートされていないので空にしておく必要があります。

ホスト / IP の部分のみがサポートされます。

#### このタスクについて

ONTAP は、ローカルネットグループファイルを対象としたホスト単位のネットグループ検索をサポートしています。ネットグループファイルをロードしたあと、ホスト単位のネットグループ検索を有効にするために netgroup.byhost マップが ONTAP によって自動的に作成されます。これにより、エクスポートポリシールールを処理してクライアントアクセスを評価する際のローカルネットグループ検索にかかる時間が大幅に短縮されます。

#### ステップ

1. URI から SVM にネットグループをロードします。

```
vserver services name-service netgroup load -vserver vs1 -source
{ftp|http|https|https}://uri
```

ネットグループファイルのロードと netgroup.byhost マップの構築には、数分かかる場合があります。

ネットグループの更新が必要な場合は、ネットグループファイルを編集し、更新されたファイルを SVM にロードすることができます。

#### 例

次のコマンドは、HTTPのURLを使用して、ネットグループ定義をvs1というSVMにロードします  
http://intranet/downloads/corp-netgroup:

```
vs1::> vserver services name-service netgroup load -vserver vs1
-source http://intranet/downloads/corp-netgroup
```

ネットグループの定義の状態を確認します

ネットグループをSVMにロードしたら、を使用できます vserver services name-service netgroup status ネットグループの定義のステータスを確認するコマンド。これにより、ネットグループの定義が SVM の基盤となるすべてのノードで一貫した状態になっているかどうかを確認することができます。

#### 手順

1. 権限レベルを advanced に設定します。

```
set -privilege advanced
```

2. ネットグループの定義のステータスを確認します。

```
vserver services name-service netgroup status
```

追加情報をより詳細なビューで表示できます。

3. admin 権限レベルに戻ります。

```
set -privilege admin
```

#### 例

権限レベルを設定したあと、次のコマンドを実行すると、すべての SVM のネットグループのステータスが表示されます。

```
vs1::> set -privilege advanced
```

Warning: These advanced commands are potentially dangerous; use them only when

directed to do so by technical support.

Do you wish to continue? (y or n): y

```
vs1::*> vserver services name-service netgroup status
```

Virtual

Server	Node	Load Time	Hash Value
--------	------	-----------	------------

-----

-----

vs1

node1	9/20/2006 16:04:53
-------	--------------------

e6cb38ec1396a280c0d2b77e3a84eda2

node2	9/20/2006 16:06:26
-------	--------------------

e6cb38ec1396a280c0d2b77e3a84eda2

node3	9/20/2006 16:08:08
-------	--------------------

e6cb38ec1396a280c0d2b77e3a84eda2

node4	9/20/2006 16:11:33
-------	--------------------

e6cb38ec1396a280c0d2b77e3a84eda2

#### NIS ドメイン設定を作成します

現在の環境でネームサービスにNetwork Information Service (NIS；ネットワーク情報サービス) が使用されている場合は、を使用してSVMのNISドメイン設定を作成する必要があります vserver services name-service nis-domain create コマンドを実行します

必要なもの



SVM に NIS ドメインを設定するためには、設定済みのすべての NIS サーバが使用可能でアクセスできる状態になっている必要があります。

ディレクトリ検索での NIS の使用を予定している場合、NIS サーバ内のマップに 1、024 文字を超えるエントリを持たせることはできません。この制限に従っていない NIS サーバを指定しないでください。そうしないと、NIS エントリに依存したクライアントアクセスに失敗する可能性があります。

このタスクについて

複数の NIS ドメインを作成できます。ただし、に設定されているものだけを使用できます `active`。

NISデータベースにが含まれている場合 `netgroup.byhost` マップ、ONTAP は、検索を高速化するために使用できます。。 `netgroup.byhost` および `netgroup` クライアントアクセスの問題を回避するために、ディレクトリ内のマップは常に同期されている必要があります。ONTAP 9.7以降ではNISが使用されます

`netgroup.byhost` エントリはを使用してキャッシュできます `vserver services name-service nis-domain netgroup-database` コマンド

ホスト名解決にNISを使用することはサポートされていません。

手順

1. NIS ドメイン設定を作成します。

```
vserver services name-service nis-domain create -vserver vs1 -domain  
domain_name -active true -servers IP_addresses
```

最大 10 台の NIS サーバを指定できます。



ONTAP 9.2以降では、フィールドが表示されます `-nis-servers` フィールドを置き換えま  
す `-servers`。この新しいフィールドには、NISサーバのホスト名またはIPアドレスを指定  
できます。

2. ドメインが作成されたことを確認します。

```
vserver services name-service nis-domain show
```

例

次のコマンドは、IP アドレス 192.0.2.180 の NIS サーバを使用して、`vs1` という名前の SVM に、`nisdomain` という NIS ドメインのアクティブな NIS ドメイン設定を作成します。

```
vs1::> vserver services name-service nis-domain create -vserver vs1  
-domain nisdomain -active true -nis-servers 192.0.2.180
```

**LDAP** を使用する

**LDAP** の使用方法の概要

現在の環境で LDAP がネームサービス用に使用されている場合は、LDAP 管理者と協力して要件および適切なストレージシステム構成を決定し、SVM を LDAP クライアントとして有効にする必要があります。

ONTAP 9.10.1 以降では、LDAP チャンネルバインドがデフォルトで Active Directory とネームサービスの両方の LDAP 接続でサポートされます。ONTAP は、Start-TLS または LDAPS が有効で、セッションセキュリティが署名または封印に設定されている場合にのみ、LDAP 接続でチャンネルバインドを試行します。ネームサーバとの LDAP チャンネルバインディングを無効または再度有効にするには、を使用します `-try-channel-binding` パラメータと `ldap client modify` コマンドを実行します

詳細については、を参照してください

["2020 年の Windows 向け LDAP チャンネルバインドおよび LDAP 署名の要件"](#)。

- LDAP for ONTAP を設定する前に、サイト環境が LDAP サーバおよびクライアント設定のベストプラクティスを満たしていることを確認する必要があります。具体的には、次の条件を満たす必要があります。
  - LDAP サーバのドメイン名が LDAP クライアント上のエントリと一致している必要があります。
  - LDAP サーバでサポートされている LDAP ユーザパスワードハッシュタイプには、ONTAP でサポートされているハッシュタイプが含まれている必要があります。
    - crypt (すべてのタイプ) および SHA-1 (SHA、SSHA)
    - ONTAP 9.8 以降では、SHA-2 ハッシュ (SHA-256、SSH-384、SHA-512、SSHA-256、SSHA-384 および SSHA-512) もサポートされます。
  - LDAP サーバにセッションセキュリティ対策が必要な場合は、LDAP クライアントで設定する必要があります。

次のセッションセキュリティオプションを使用できます。

- LDAP 署名 (データの整合性チェックを提供) および LDAP の署名と封印 (データの整合性チェックと暗号化を提供)
- START TLS
- LDAPS (LDAP over TLS または SSL)
- 署名および封印された LDAP クエリを有効にするには、次のサービスが設定されている必要があります。
  - LDAP サーバで GSSAPI (Kerberos) SASL がサポートされている必要があります。
  - LDAP サーバに、DNS A/AAAA レコード、および DNS サーバで設定された PTR レコードが必要です。
  - Kerberos サーバに、DNS サーバ上に存在する SRV レコードが必要です。
- TLS または LDAPS を開始できるようにするには、次の点を考慮する必要があります。
  - ネットアップでは、LDAPS ではなく Start TLS を使用することを推奨します。
  - LDAPS を使用している場合は、ONTAP 9.5 以降で LDAP サーバの TLS または SSL が有効になっている必要があります。ONTAP 9.0~9.4 では SSL はサポートされません。
  - 証明書サーバがドメインで設定済みである必要があります。
- LDAP リファラール追跡を有効にするには (ONTAP 9.5 以降)、次の条件を満たしている必要があります。
  - 両方のドメインで、次のいずれかの信頼関係を設定する必要があります。
    - 双方向
    - 一方向。一次は紹介ドメインを信頼します

- 親子
- 参照されているすべてのサーバ名を解決するように DNS が設定されていること。
- bind-as-cifs-server が true に設定されている場合、認証には両ドメインのパスワードが同じである必要があります。

次の設定は LDAP リファラール追跡でサポートされません。



- すべての ONTAP バージョン：
  - 管理 SVM 上の LDAP クライアント
- ONTAP 9.8 以前では（9.9.1 以降でサポートされています）：
  - LDAP の署名と封印（-session-security オプション）
  - 暗号化された TLS 接続（-use-start-tls オプション）
  - LDAPS ポート 636（-use-ldaps-for-ad-ldap オプション）

- SVM で LDAP クライアントを設定するときは、LDAP スキーマを入力する必要があります。

ほとんどの場合、デフォルトの ONTAP スキーマのいずれかが適しています。ただし、環境で使用する LDAP スキーマがこれらと異なる場合は、LDAP クライアントを作成する前に、ONTAP 用の新しい LDAP クライアントスキーマを作成する必要があります。環境の要件については、LDAP 管理者にお問い合わせください。

- LDAP をホスト名解決に使用することはサポートされていません。

を参照してください。

- "ネットアップテクニカルレポート 4835：『How to Configure LDAP in ONTAP』"
- "自己署名ルート CA 証明書を SVM にインストールします"

新しい **LDAP** クライアントスキーマを作成します

環境で使用する LDAP スキーマが ONTAP のデフォルトと異なる場合は、LDAP クライアント設定を作成する前に、ONTAP 用の新しい LDAP クライアントスキーマを作成する必要があります。

このタスクについて

ほとんどの LDAP サーバでは、ONTAP が提供する次のデフォルトスキーマを使用できます。

- MS-AD-BIS（ほとんどの Windows Server 2012 以降の AD サーバで推奨されるスキーマ）
- AD-IDMU（Windows Server 2008、Windows Server 2012、およびそれ以降の AD サーバ）
- AD-SFU（Windows Server 2003 以前の AD サーバ）
- RFC-2307（UNIX LDAP サーバ）

デフォルト以外の LDAP スキーマを使用する必要がある場合は、LDAP クライアント設定を作成する前にスキーマを作成する必要があります。新しいスキーマを作成する前に、LDAP 管理者に問い合わせてください。

ONTAP に用意されているデフォルトの LDAP スキーマは変更できません。新しいスキーマを作成するには、コピーを作成し、それに応じてコピーを変更します。

#### 手順

1. 既存の LDAP クライアントスキーマテンプレートを表示して、コピーするスキーマを特定します。

```
vserver services name-service ldap client schema show
```

2. 権限レベルを advanced に設定します。

```
set -privilege advanced
```

3. 既存の LDAP クライアントスキーマのコピーを作成します。

```
vserver services name-service ldap client schema copy -vserver vserver_name  
-schema existing_schema_name -new-schema-name new_schema_name
```

4. 新しいスキーマを変更し、環境に合わせてカスタマイズします。

```
vserver services name-service ldap client schema modify
```

5. admin 権限レベルに戻ります。

```
set -privilege admin
```

#### LDAP クライアント設定を作成します

環境内の外部LDAPサービスまたはActive DirectoryサービスにONTAPからアクセスする場合は、まずストレージシステム上にLDAPクライアントを設定する必要があります。

#### 必要なもの

Active Directoryドメイン解決リストの最初の3つのサーバのいずれかが稼働し、データを提供している必要があります。そうしないと、このタスクは失敗します。



複数のサーバがあり、そのうちどの時点でも3台以上のサーバがダウンしています。

#### 手順

1. LDAP管理者に問い合わせ、適切な設定値を確認してください `vserver services name-service ldap client create` コマンドを実行します

- a. LDAP サーバへのドメインベースまたはアドレスベースの接続を指定します。

。 `-ad-domain` および `-servers` オプションを同時に指定することはできません。

- を使用します `-ad-domain` Active DirectoryドメインでLDAPサーバ検出を有効にするオプション。
- を使用できます `-restrict-discovery-to-site` LDAPサーバ検出を、指定したドメインのCIFSデフォルトサイトに制限するオプション。このオプションを使用する場合は、CIFSのデフォルトサイトも指定する必要があります。 `-default-site`。

- 使用できます `-preferred-ad-servers` カンマで区切ってIPアドレスで1つ以上の優先Active Directoryサーバを指定するオプション。クライアントが作成されたら、を使用してこのリストを変更できます `vserver services name-service ldap client modify` コマンドを実行します
- 使用します `-servers` カンマで区切ってIPアドレスで1つ以上のLDAPサーバ（Active DirectoryまたはUNIX）を指定するオプション。



。 `-servers` オプションはONTAP 9.2で廃止されました。ONTAP 9.2以降では、`-ldap-servers` フィールドがに置き換わります `-servers` フィールド。このフィールドには、LDAPサーバのホスト名またはIPアドレスを指定できます。

b. デフォルトまたはカスタムの LDAP スキーマを指定します。

ほとんどの LDAP サーバでは、ONTAP が提供するデフォルトの読み取り専用スキーマを使用できます。他のスキーマを使用する必要がある場合を除き、デフォルトのスキーマを使用することを推奨します。その場合は、デフォルトスキーマ（読み取り専用）をコピーし、コピーを変更することによって、独自のスキーマを作成できます。

デフォルトのスキーマ：

- MS-AD-BIS を参照してください

RFC 2307bis に基づいて、ほとんどの標準的な Windows 2012 以降の LDAP 環境で優先される LDAP スキーマです。

- AD-IDMU

Active Directory Identity Management for UNIX に基づいて、このスキーマは Windows Server 2008、Windows Server 2012、およびそれ以降のほとんどの AD サーバに適しています。

- AD-SFU

Active Directory Services for UNIX に基づいて、このスキーマは Windows 2003 以前のほとんどの AD サーバに適しています。

- RFC-2307

RFC-2307（ネットワーク情報サービスとして LDAP を使用するためのアプローチ）に基づいて、このスキーマはほとんどの UNIX AD サーバに適しています。

c. バインド値を選択します。

- `-min-bind-level {anonymous|simple|sas1}` 最小バインド認証レベルを指定します。

デフォルト値はです **anonymous**。

- `-bind-dn LDAP_DN` バインドユーザを指定します。

Active Directory サーバの場合は、アカウント（`DOMAIN\user`）またはプリンシパル（`user@domain.com`）の形式でユーザを指定する必要があります。それ以外の場合は、識別名（`CN=user`、`DC=domain`、`DC=com`）の形式でユーザを指定する必要があります。

- `-bind-password password` バインドパスワードを指定します。

d. 必要に応じて、セッションセキュリティオプションを選択します。

LDAP サーバで必要な場合は、LDAP の署名と封印または LDAP over TLS を有効にすることができます。

- `--session-security {none|sign|seal}`

署名を有効にできます (sign、データ整合性)、署名と封印 (seal、データ整合性と暗号化)、またはどちらでもない none、署名または封印なし)。デフォルト値はです none。

また、を設定する必要があります `-min-bind-level {sasl}` バインド認証をにフォールバックする場合を除きます **anonymous** または **simple** 署名と封印のバインドが失敗した場合。

- `-use-start-tls {true|false}`

に設定すると **true** LDAPサーバがサポートしており、LDAPクライアントはサーバへの暗号化されたTLS接続を使用します。デフォルト値はです **false**。このオプションを使用するには、LDAP サーバの自己署名ルート CA 証明書をインストールする必要があります。



Storage VMでSMBサーバがドメインに追加されており、LDAPサーバがSMBサーバのホームドメインのドメインコントローラの1つである場合は、`-session-security -for-ad-ldap` オプションを使用します `vserver cifs security modify` コマンドを実行します

e. ポート、クエリ、およびベースの値を選択します。

デフォルト値を推奨しますが、実際の環境に適しているかどうかを LDAP 管理者に確認する必要があります。

- `-port port` LDAPサーバポートを指定します。

デフォルト値はです 389。

Start TLS を使用した LDAP 接続の保護を予定している場合は、デフォルトのポート 389 を使用する必要があります。Start TLS は LDAP のデフォルトポート 389 経由でプレーンテキスト接続として開始され、その後 TLS 接続にアップグレードされます。ポートを変更すると、Start TLS は失敗します。

- `-query-timeout integer` クエリタイムアウトを秒単位で指定します。

指定できる範囲は 1~10 秒です。デフォルト値はです 3 秒。

- `-base-dn LDAP_DN` ベースDNを指定します。

必要に応じて複数の値を入力できます (LDAP リファラール追跡を有効にした場合など)。デフォルト値はです "" (ルート)。

- `-base-scope {base|onelevel|subtree}` は、ベース検索範囲を指定します。

デフォルト値はです subtree。



- `-referral-enabled {true|false}` LDAPリファール追跡を有効にするかどうかを指定します。

ONTAP 9.5 以降では、LDAP リファール追跡を有効にすると、必要なレコードが他の LDAP サーバにあることを示す LDAP リファール応答がプライマリ LDAP サーバから返された場合に、ONTAP LDAP クライアントがそれらの LDAP サーバに対してルックアップ要求を実行することができます。デフォルト値はです **false**。

参照された LDAP サーバにあるレコードを検索するには、参照されたレコードのベース DN を LDAP クライアント設定の一部としてベース DN に追加する必要があります。

## 2. Storage VMにLDAPクライアント設定を作成します。

```
vserver services name-service ldap client create -vserver vserver_name -client
-config client_config_name {-servers LDAP_server_list | -ad-domain ad_domain}
-preferred-ad-servers preferred_ad_server_list -restrict-discovery-to-site
{true|false} -default-site CIFS_default_site -schema schema -port 389 -query
-timeout 3 -min-bind-level {anonymous|simple|sasl} -bind-dn LDAP_DN -bind
-password password -base-dn LDAP_DN -base-scope subtree -session-security
{none|sign|seal} [-referral-enabled {true|false}]
```



LDAPクライアント設定を作成するときは、Storage VM名を指定する必要があります。

## 3. LDAP クライアント設定が正常に作成されたことを確認します。

```
vserver services name-service ldap client show -client-config
client_config_name
```

### 例

次のコマンドでは、LDAPのActive Directoryサーバと連携するために、Storage VM vs1でldap1という名前の新しいLDAPクライアント設定を作成します。

```
cluster1::> vserver services name-service ldap client create -vserver vs1
-client-config ldapclient1 -ad-domain addomain.example.com -schema AD-SFU
-port 389 -query-timeout 3 -min-bind-level simple -base-dn
DC=addomain,DC=example,DC=com -base-scope subtree -preferred-ad-servers
172.17.32.100
```

次のコマンドでは、署名と封印が必要なLDAPのActive Directoryサーバと連携するために、Storage VM vs1でldap1という名前の新しいLDAPクライアント設定を作成します。LDAPサーバの検出は指定したドメインの特定のサイトに制限されます。

```
cluster1::> vservice name-service ldap client create -vserver vs1
-client-config ldapclient1 -ad-domain addomain.example.com -restrict
-discovery-to-site true -default-site cifsdefaultsite.com -schema AD-SFU
-port 389 -query-timeout 3 -min-bind-level sasl -base-dn
DC=addomain,DC=example,DC=com -base-scope subtree -preferred-ad-servers
172.17.32.100 -session-security seal
```

次のコマンドでは、LDAPリファール追跡が必要なLDAPのActive Directoryサーバと連携するために、Storage VM vs1でldap1という名前の新しいLDAPクライアント設定を作成します。

```
cluster1::> vservice name-service ldap client create -vserver vs1
-client-config ldapclient1 -ad-domain addomain.example.com -schema AD-SFU
-port 389 -query-timeout 3 -min-bind-level sasl -base-dn
"DC=adbasedomain,DC=example1,DC=com; DC=adrefdomain,DC=example2,DC=com"
-base-scope subtree -preferred-ad-servers 172.17.32.100 -referral-enabled
true
```

次のコマンドでは、ベースDNを指定することで、Storage VM vs1のldap1という名前のLDAPクライアント設定を変更します。

```
cluster1::> vservice name-service ldap client modify -vserver vs1
-client-config ldap1 -base-dn CN=Users,DC=addomain,DC=example,DC=com
```

次のコマンドは、リファール追跡を有効にすることで、Storage VM vs1のldap1という名前のLDAPクライアント設定を変更します。

```
cluster1::> vservice name-service ldap client modify -vserver vs1
-client-config ldap1 -base-dn "DC=adbasedomain,DC=example1,DC=com;
DC=adrefdomain,DC=example2,DC=com" -referral-enabled true
```

## LDAP クライアント設定を SVM に関連付けます

SVMでLDAPを有効にするには、を使用する必要があります vservice name-service ldap create LDAPクライアント設定をSVMに関連付けるコマンド。

### 必要なもの

- LDAP ドメインがネットワーク内にすでに存在しており、SVM が配置されているクラスタからアクセスできる必要があります。
- LDAP クライアント設定が SVM に存在している必要があります。

### 手順

1. SVMでLDAPを有効にします。



```
vserver services name-service ldap create -vserver vserver_name -client-config client_config_name
```



ONTAP 9.2以降では、`vserver services name-service ldap create` コマンドは設定の自動検証を実行し、ONTAP がネームサーバに接続できない場合はエラーメッセージを報告します。

次のコマンドは、「vs1」という SVM で LDAP を有効にし、「ldap1」という LDAP クライアント設定を使用するように設定します。

```
cluster1::> vserver services name-service ldap create -vserver vs1  
-client-config ldap1 -client-enabled true
```

2. `vserver services name-service ldap check` コマンドを使用して、ネームサーバのステータスを検証します。

次のコマンドは、SVM vs1. 上の LDAP サーバを検証します。

```
cluster1::> vserver services name-service ldap check -vserver vs1  
  
| Vserver: vs1 |  
| Client Configuration Name: cl |  
| LDAP Status: up |  
| LDAP Status Details: Successfully connected to LDAP server |  
| "10.11.12.13". |
```

ネームサービスのチェックコマンドは ONTAP 9.2 以降で使用できます。

ネームサービススイッチテーブルで **LDAP** ソースを確認します

ネームサービスの LDAP ソースが SVM のネームサービススイッチテーブルに正しく表示されていることを確認する必要があります。

手順

1. 現在のネームサービススイッチテーブルの内容を表示します。

```
vserver services name-service ns-switch show -vserver svm_name
```

次のコマンドは、SVM My\_SVM の結果を表示します。

```
ie3220-a::> vserver services name-service ns-switch show -vserver My_SVM
```

Vserver	Database	Source
-----	-----	-----
My_SVM	hosts	files, dns
My_SVM	group	files,ldap
My_SVM	passwd	files,ldap
My_SVM	netgroup	files
My_SVM	namemap	files

5 entries were displayed.

namemap ネームマッピング情報を検索するソースとその検索順序を指定します。UNIX のみの環境では、このエントリは必要ありません。ネームマッピングは、UNIX と Windows の両方を使用する混在環境でのみ必要になります。

## 2. を更新します ns-switch 必要に応じて入力：

ns-switch エントリの更新対象	入力するコマンド
ユーザ情報	<code>vserver services name-service ns-switch modify -vserver vserver_name -database passwd -sources ldap,files</code>
グループ情報	<code>vserver services name-service ns-switch modify -vserver vserver_name -database group -sources ldap,files</code>
ネットグループ情報	<code>vserver services name-service ns-switch modify -vserver vserver_name -database netgroup -sources ldap,files</code>

## NFS で Kerberos を使用してセキュリティを強化します

### NFS での Kerberos 使用によるセキュリティ強化の概要

Kerberos を強力な認証に使用している環境では、Kerberos 管理者と協力して要件および適切なストレージシステム設定を決定し、SVM を Kerberos クライアントとして有効にする必要があります。

環境が次のガイドラインに従う必要があります。

- ONTAP で Kerberos を設定するには、Kerberos のサーバとクライアントの設定に適したベストプラクティスに従ってサイトが導入されている必要があります。
- Kerberos 認証を必須とする場合は、可能であれば NFSv4 以降を使用します。

NFSv3 でも Kerberos を使用できますが、Kerberos の高度なセキュリティ機能をフルに活用するには、ONTAP を NFSv4 以降に導入する必要があります。

- サーバアクセスの冗長化を促すため、同じ SPN を使ってクラスタ内の複数のノードのデータ LIF で Kerberos を有効にする必要があります。
- Kerberos を SVM で有効にする場合は、NFS クライアントの設定に応じて、次のいずれかのセキュリティ方式をボリュームまたは qtree のエクスポートルールに指定する必要があります。
  - krb5 (Kerberos v5プロトコル)
  - krb5i (Kerberos v5プロトコルとチェックサムによる整合性チェック)
  - krb5p (Kerberos v5プロトコルとプライバシーサービス)

Kerberos のサーバとクライアントのほかに、次の外部サービスを Kerberos を使用する ONTAP 用に設定する必要があります。

- ディレクトリサービス

Active Directory や OpenLDAP などのセキュアなディレクトリサービスを環境に導入し、SSL / TLS 経由の LDAP を使用するように設定してください。NIS を使用すると、要求がクリアテキストで送信されセキュアではないため、NIS は使用しないでください。

- NTP

タイムサーバで NTP を実行している必要があります。これは、時刻のずれによる Kerberos 認証の失敗を回避するために必要です。

- ドメイン名解決 (DNS)

それぞれの UNIX クライアントおよび SVM LIF について、KDC の前方参照ゾーンと逆引き参照ゾーンに適切なサービスレコード (SRV) が登録されている必要があります。すべてのコンポーネントを DNS で正しく解決できる必要があります。

**Kerberos 設定の権限を確認します**

Kerberos では、特定の UNIX 権限が SVM ルートボリューム用およびローカルユーザおよびグループ用に設定されている必要があります。

**手順**

1. SVM ルートボリュームについて、関連する権限を表示します。

```
volume show -volume root_vol_name-fields user,group,unix-permissions
```

SVM のルートボリュームを次のように設定しておく必要があります。

名前	設定
UID	root または ID 0
GID	root または ID 0

名前	設定
UNIX 権限	755

これらの値が表示されない場合は、を使用します `volume modify` コマンドを使用して更新します。

## 2. ローカル UNIX ユーザを表示します。

```
vserver services name-service unix-user show -vserver vserver_name
```

SVM で次の UNIX ユーザを設定しておく必要があります。

ユーザ名	ユーザ ID	プライマリグループ ID	コメント (Comment)
NFS	500ドル	0	GSS INIT フェーズで必要。  NFS クライアントユーザの SPN の最初のコンポーネントがユーザとして使用されます。  NFS クライアントユーザの SPN に対する Kerberos-UNIX ネームマッピングがある場合は、nfs ユーザは必要ありません。
ルート	0	0	マウントに必要。

これらの値が表示されていない場合は、を使用できます `vserver services name-service unix-user modify` コマンドを使用して更新します。

## 3. ローカル UNIX グループを表示します。

```
vserver services name-service unix-group show -vserver vserver_name
```

SVM で次の UNIX グループを設定しておく必要があります。

グループ名	グループ ID
デーモン	1.
ルート	0

これらの値が表示されていない場合は、を使用できます `vserver services name-service unix-group modify` コマンドを使用して更新します。

環境で ONTAP から外部 Kerberos サーバにアクセスする場合は、まず既存の Kerberos Realm を使用するように SVM を設定する必要があります。そのためには、Kerberos KDCサーバの設定値を収集し、を使用する必要があります `vserver nfs kerberos realm create` SVMにKerberos Realm設定を作成するコマンド。

#### 必要なもの

認証の問題を回避するために、クラスタ管理者はストレージシステム、クライアント、および KDC サーバ上で NTP を設定しておく必要があります。クライアントとサーバの時間差（クロックスキュー）は、認証エラーの一般的な原因です。

#### 手順

1. で指定する適切な設定値を決定するには、Kerberos管理者に問い合わせてください `vserver nfs kerberos realm create` コマンドを実行します
2. SVM で Kerberos Realm の設定を作成します。

```
vserver nfs kerberos realm create -vserver vserver_name -realm realm_name  
{AD_KDC_server_values |AD_KDC_server_values} -comment "text"
```

3. Kerberos Realm 設定が正常に作成されたことを確認します。

```
vserver nfs kerberos realm show
```

#### 例

次のコマンドは、Microsoft Active Directory サーバを KDC サーバとして使用する NFS Kerberos Realm 設定を SVM vs1 で作成します。Kerberos Realm は AUTH.EXAMPLE.COM です。Active Directory サーバの名前は ad-1 で、IP アドレスは 10.10.8.14 です。許容されるクロックスキューは 300 秒（デフォルト）です。KDC サーバの IP アドレスは 10.10.8.14 で、ポート番号は 88（デフォルト）です。「Microsoft Kerberos config」はコメントです。

```
vs1::> vserver nfs kerberos realm create -vserver vs1 -realm  
AUTH.EXAMPLE.COM -adserver-name ad-1  
-adserver-ip 10.10.8.14 -clock-skew 300 -kdc-ip 10.10.8.14 -kdc-port 88  
-kdc-vendor Microsoft  
-comment "Microsoft Kerberos config"
```

次のコマンドは、MIT KDC を使用する NFS Kerberos Realm 設定を SVM vs1 で作成します。Kerberos Realm は SECURITY.EXAMPLE.COM です。許容されるクロックスキューは 300 秒です。KDC サーバの IP アドレスは 10.10.9.1 で、ポート番号は 88 です。KDC ベンダーは UNIX ベンダーを示す Other です。管理サーバの IP アドレスは 10.10.9.1 で、ポート番号は 749（デフォルト）です。パスワードサーバの IP アドレスは 10.10.9.1 で、ポート番号は 464（デフォルト）です。「UNIX Kerberos config」はコメントです。

```
vs1::> vserver nfs kerberos realm create -vserver vs1 -realm
SECURITY.EXAMPLE.COM. -clock-skew 300
-kdc-ip 10.10.9.1 -kdc-port 88 -kdc-vendor Other -adminserver-ip 10.10.9.1
-adminserver-port 749
-passwordserver-ip 10.10.9.1 -passwordserver-port 464 -comment "UNIX
Kerberos config"
```

**NFS Kerberos** で許可されている暗号化タイプを設定する

デフォルトでは、ONTAP は、DES、3DES、AES-128、および AES-256 の暗号化タイプをサポートします。を使用して、SVMごとに許可される暗号化タイプを、特定の環境のセキュリティ要件に合わせて設定できます `vserver nfs modify` コマンドにを指定します `-permitted-enc-types` パラメータ

このタスクについて

クライアントの互換性を最大にするために、ONTAP はデフォルトで弱い DES 暗号化と強い AES 暗号化の両方をサポートしています。つまり、たとえば、セキュリティの向上を必要としていて環境でこの機能がサポートされている場合は、この手順を使用して、DES と 3DES を無効にしてクライアントに AES 暗号化のみの使用を要求できます。

使用可能な最も強力な暗号化を使用する必要があります。ONTAP の場合は AES-256 です。この暗号化レベルが環境でサポートされていることを、KDC 管理者に確認する必要があります。

- SVM 上で AES 全体（AES-128 と AES-256 の両方）を有効または無効にすると、システムが停止します。元の DES プリンシパル / keytab ファイルが削除され、SVM のすべての LIF 上で Kerberos 構成を無効にすることが必要になるからです。

この変更を行う前に、SVM 上で NFS クライアントが AES 暗号化に依存していないことを確認する必要があります。

- DES や 3DES の有効化または無効化は、LIF での Kerberos 設定の変更を一切必要としません。

ステップ

1. 許可されている必要な暗号化タイプを有効または無効にします。

有効または無効にする対象	実行する手順
DES または 3DES	<p>a. SVMのNFS Kerberosで許可される暗号化タイプを設定します。</p> <p>[+]</p> <pre>vserver nfs modify -vserver vserver_name -permitted-enc-types encryption_types</pre> <p>暗号化タイプが複数ある場合はカンマで区切ります。</p> <p>b. 変更が成功したことを確認します。</p> <p>[+]</p> <pre>vserver nfs show -vserver vserver_name -fields permitted-enc- types</pre>

有効または無効にする対象	実行する手順
AES-128またはAES-256	<p>a. Kerberosが有効になっているSVMとLIFを特定します。 [+] <code>vserver nfs kerberos interface show</code></p> <p>b. 変更対象のNFS Kerberosで許可されている暗号化タイプが設定されているSVM上のすべてのLIFでKerberosを無効にします。 [+] <code>vserver nfs kerberos interface disable -lif <i>lif_name</i></code></p> <p>c. SVMのNFS Kerberosで許可される暗号化タイプを設定します。 [+] <code>vserver nfs modify -vserver <i>vserver_name</i> -permitted-enc-types <i>encryption_types</i></code></p> <p>暗号化タイプが複数ある場合はカンマで区切ります。</p> <p>d. 変更が成功したことを確認します。 [+] <code>vserver nfs show -vserver <i>vserver_name</i> -fields permitted-enc-types</code></p> <p>e. SVM上のすべてのLIFでKerberosを再度有効にします。 [+] <code>vserver nfs kerberos interface enable -lif <i>lif_name</i> -spn <i>service_principal_name</i></code></p> <p>f. すべてのLIFでKerberosが有効になっていることを確認します。 [+] <code>vserver nfs kerberos interface show</code></p>

データ LIF で **Kerberos** を有効にします

を使用できます `vserver nfs kerberos interface enable` コマンドを使用してデータLIFでKerberosを有効にします。これにより、SVMでNFSのKerberosセキュリティサービスを使用できます。

このタスクについて

Active Directory KDC を使用する場合、使用される SPN の最初の 15 文字は Realm またはドメイン内の SVM 間で一意である必要があります。



手順

1. NFS Kerberos 設定を作成します。

```
vserver nfs kerberos interface enable -vserver vserver_name -lif
logical_interface -spn service_principal_name
```

ONTAP で Kerberos インターフェイスを有効にするには、KDC の SPN 用のシークレットキーが必要です。

Microsoft KDC の場合、KDC に接続があると、シークレットキーを取得するためのユーザ名とパスワードのプロンプトが CLI で発行されます。Kerberos Realmの別のOUでSPNを作成する必要がある場合は、オプションのを指定できます -ou パラメータ

Microsoft 以外の KDC の場合は、次の 2 つのうちいずれかの方法を使用してシークレットキーを取得できます。

状況	コマンドとともに含める必要のあるパラメータ
KDC からキーを直接取得するための KDC 管理者のクレデンシャルが必要です	-admin-username kdc_admin_username
KDC 管理者のクレデンシャルはないが、キーが含まれている、KDC の keytab ファイルはある	-keytab-uri {ftp

2. LIF で Kerberos が有効になっていることを確認します。

```
vserver nfs kerberos-config show
```

3. 複数の LIF で Kerberos を有効にするには、手順 1 と 2 を繰り返します。

例

次のコマンドは、vs1 という SVM の NFS Kerberos 設定を、OU lab2ou 内の SPN nfs/ves03-d1.lab.example.com@TEST.LAB.EXAMPLE.COM を使用して、ves03-d1 という論理インターフェイス ves03-d1 に対して作成して検証します。

```
vs1::> vserver nfs kerberos interface enable -lif ves03-d1 -vserver vs2
-spkn nfs/ves03-d1.lab.example.com@TEST.LAB.EXAMPLE.COM -ou "ou=lab2ou"

vs1::>vserver nfs kerberos-config show
      Logical
Vserver Interface Address      Kerberos  SPN
-----
vs0      ves01-a1
          10.10.10.30 disabled -
vs2      ves01-d1
          10.10.10.40 enabled  nfs/ves03-
d1.lab.example.com@TEST.LAB.EXAMPLE.COM
2 entries were displayed.
```

## NFS 対応 SVM にストレージ容量を追加

### NFS 対応 SVM の概要へのストレージ容量の追加

NFS 対応 SVM にストレージ容量を追加するには、ストレージコンテナを提供するボリュームまたは qtree を作成し、そのコンテナのエクスポートポリシーを作成または変更する必要があります。その後、クラスタからの NFS クライアントアクセスを確認し、クライアントシステムからのアクセスをテストできます。

#### 必要なもの

- SVM で NFS の設定が完了している必要があります。
- SVM ルートボリュームのデフォルトのエクスポートポリシーに、すべてのクライアントへのアクセスを許可するルールが含まれている必要があります。
- ネームサービス設定に対する更新が完了している必要があります。
- Kerberos 設定への追加または変更が完了している必要があります。

#### エクスポートポリシーを作成する

エクスポートルールを作成する前に、それらを保持するエクスポートポリシーを作成する必要があります。使用できます `vserver export-policy create` コマンドを使用してエクスポートポリシーを作成します。

#### 手順

1. エクスポートポリシーを作成する

```
vserver export-policy create -vserver vserver_name -policyname policy_name
```

ポリシー名に指定できる文字数は最大 256 文字です。

2. エクスポートポリシーが作成されたことを確認します。

```
vserver export-policy show -policyname policy_name
```

#### 例

次のコマンドは、vs1 という SVM で、exp1 という名前のエクスポートポリシーを作成し、作成を確認します。

```
vs1::> vserver export-policy create -vserver vs1 -policyname exp1

vs1::> vserver export-policy show -policyname exp1
Vserver          Policy Name
-----
vs1              exp1
```

## エクスポートポリシーにルールを追加する

エクスポートポリシーにルールが含まれていないと、クライアントはデータにアクセスできません。新しいエクスポートルールを作成するには、クライアントを特定してクライアント照合形式を選択し、アクセスとセキュリティの種類を選択し、匿名ユーザ ID マッピングを指定し、ルールインデックス番号を選択して、アクセスプロトコルを選択する必要があります。その後、を使用できます `vserver export-policy rule create` コマンドを使用して新しいルールをエクスポートポリシーに追加します。

### 必要なもの

- エクスポートルールを追加するエクスポートポリシーを用意しておく必要があります。
- データ SVM で DNS が正しく設定されている必要があります、DNS サーバに NFS クライアント用の正しいエントリが存在する必要があります。

その理由は、特定のクライアント照合形式で ONTAP がデータ SVM の DNS 設定を使用して DNS ルックアップを実行することと、エクスポートポリシールールの照合が失敗するとクライアントがデータにアクセスできなくなる可能性があることです。

- Kerberos で認証する場合は、NFS クライアントで次のうちのセキュリティ方式が使用されているかを特定しておく必要があります。
  - `krb5` (Kerberos v5プロトコル)
  - `krb5i` (Kerberos v5プロトコルとチェックサムによる整合性チェック)
  - `krb5p` (Kerberos v5プロトコルとプライバシーサービス)

### このタスクについて

エクスポートポリシーの既存のルールがクライアント照合とアクセスの要件を満たしている場合は、新しいルールを作成する必要はありません。

Kerberosで認証する場合に、SVMのすべてのボリュームにKerberos経由でアクセスできる場合は、エクスポートルールオプションを設定できます `-rorule`、`-rwrule` および `-superuser` ルートボリュームのをに設定します `krb5`、`krb5i` または `krb5p`。

### 手順

1. クライアントと、新しいルールのクライアント照合形式を特定します。

。 `-clientmatch` オプションは、ルールを適用するクライアントを指定します。クライアント照合の値は 1 つまたは複数指定できます。複数の値を指定する場合はカンマで区切る必要があります。次のいずれかの形式で指定できます。

クライアント照合形式	例
先頭に文字が付いたドメイン名	<code>.example.com</code> または <code>.example.com, .example.net, ...</code>
ホスト名	<code>host1</code> または <code>host1, host2, ...</code>

クライアント照合形式	例
IPv4 アドレス	10.1.12.24 または 10.1.12.24,10.1.12.25, ...
サブネットマスクをビット数で表した IPv4 アドレス	10.1.12.10/4 または 10.1.12.10/4,10.1.12.11/4,...
IPv4 アドレスとネットワークマスク	10.1.16.0/255.255.255.0 または 10.1.16.0/255.255.255.0,10.1.17.0/255. 255.255.0,...
ピリオド区切りの形式の IPv6 アドレス	::1.2.3.4 または ::1.2.3.4,::1.2.3.5,...
サブネットマスクをビット数で表したIPv6アドレス	ff::00/32 または ff::00/32,ff::01/32,...
ネットグループ名の前に @ 文字を付けた単一のネットグループ	@netgroup1 または @netgroup1,@netgroup2,...

クライアント定義のタイプを組み合わせることもできます。たとえば、.example.com,@netgroup1。

IP アドレスを指定する場合は、次の点に注意してください。

- 10.1.12.10-10.1.12.70 のように、IP アドレスの範囲を入力することはできません。

この形式のエントリはテキスト文字列と解釈され、ホスト名として扱われます。

- クライアントアクセスのきめ細かな管理のためにエクスポートルールで個々の IP アドレスを指定する際には、動的（DHCP など）または一時的（IPv6 など）に割り当てられている IP アドレスを指定しないでください。

そうしないと、IP アドレスが変更されるとクライアントはアクセスを失います。

- ff : 12/ff : 00 のように、IPv6 アドレスとネットワークマスクを入力することはできません。

## 2. クライアント照合のアクセスタイプとセキュリティタイプを選択します。

指定したセキュリティタイプで認証するクライアントに対して、次のアクセスモードを 1 つ以上指定できます。

- -rorule （読み取り専用アクセス）
- -rwrule （読み取り/書き込みアクセス）
- -superuser （ルートアクセス）



特定のセキュリティタイプに対する読み取り / 書き込みアクセスは、エクスポートルールでそのセキュリティタイプに対する読み取り専用アクセスも許可した場合にのみ許可されます。読み取り専用パラメータで読み取り / 書き込みパラメータよりも限定的なセキュリティタイプを指定した場合、クライアントに対して読み取り / 書き込みアクセスが許可されない可能性があります。スーパーユーザアクセスの場合も同様です。

カンマ区切りの形式を使用して、1つのルールに対して複数のセキュリティタイプを指定できます。セキュリティタイプとしてを指定する場合は `any` または `never`、その他のセキュリティタイプは指定しないでください。次の有効なセキュリティタイプから選択してください。

セキュリティタイプの設定	一致するクライアントからエクスポートされたデータへのアクセス
<code>any</code>	受信セキュリティタイプに関係なく、常に実行されます。
<code>none</code>	単独で指定した場合、どのセキュリティタイプのクライアントにも匿名アクセスが許可されます。他のセキュリティタイプと一緒に指定した場合、指定したセキュリティタイプのクライアントにアクセスが許可され、それ以外のセキュリティタイプのクライアントには匿名アクセスが許可されません。
<code>never</code>	受信セキュリティタイプに関係なく、絶対に使用しないでください。
<code>krb5</code>	Kerberos 5 によって認証されます。認証のみ：各要求および応答のヘッダーが署名されます。
<code>krb5i</code>	Kerberos 5i によって認証されます。認証および整合性：各要求および応答のヘッダーと本文が署名されます。
<code>krb5p</code>	Kerberos 5pによって認証されます。認証、整合性、およびプライバシー：各要求および応答のヘッダーと本文が署名され、NFS データペイロードが暗号化されます。
<code>ntlm</code>	CIFS NTLM によって認証されます。
<code>sys</code>	NFS AUTH_SYS によって認証されます。

推奨されるセキュリティタイプは `sys`、または Kerberos を使用する場合は、``krb5``、`krb5i`` または ``krb5p``。

NFSv3でKerberosを使用する場合は、エクスポートポリシールールで許可する必要があります `-rorule` および `-rwrule` へのアクセス `sys` に加えて `krb5`。これは、Network Lock Manager（NLM；ネットワークロックマネージャ）にエクスポートへのアクセスを許可するためです。

### 3. 匿名ユーザ ID マッピングを指定します。

。 `-anon` optionは、ユーザIDが0（ゼロ）で到着するクライアント要求にマッピングされるUNIXユーザIDまたはユーザ名を指定します。このユーザIDは通常ユーザ名rootに関連付けられています。デフォルト値は `65534`。NFS クライアントは通常、ユーザ ID `65534` をユーザ名 `nobody` と関連付けます（*root squashing*）。ONTAP では、このユーザ ID が `pcuser` というユーザに関連付けられています。ユーザIDが0のクライアントからのアクセスを無効にするには、の値を指定します `65535`。

### 4. ルールインデックスの順序を選択します。

。 `-ruleindex` optionには、ルールのインデックス番号を指定します。ルールはインデックス番号のリストの順序に従って評価され、インデックス番号の小さいルールが最初に評価されます。たとえば、インデックス番号が 1 のルールは、インデックス番号が 2 のルールよりも先に評価されます。

追加対象	作業
最初のルールをエクスポートポリシーに追加します	入力するコマンド 1。
追加のルールをエクスポートポリシーに追加	<p>a. ポリシー内の既存のルールを表示します。 [+] <code>vserver export-policy rule show -instance -policyname <i>your_policy</i></code></p> <p>b. 評価する順序に応じて、新しいルールのインデックス番号を選択します。</p>

### 5. 該当するNFSアクセス値を選択します。{`nfs`|`nfs3`|`nfs4`}。

`nfs` 任意のバージョンと一致します。 `nfs3` および `nfs4` 特定のバージョンのみを照合します。

### 6. エクスポートルールを作成して既存のエクスポートポリシーに追加します。

```
vserver export-policy rule create -vserver vserver_name -policyname policy_name -ruleindex integer -protocol {nfs|nfs3|nfs4} -clientmatch { text | "text,text,..." } -rorule security_type -rwrule security_type -superuser security_type -anon user_ID
```

### 7. エクスポートポリシーのルールを表示して新しいルールが存在することを確認します。

```
vserver export-policy rule show -policyname policy_name
```

このコマンドにより、エクスポートポリシーに適用されるルールの一覧を含む、エクスポートポリシーの概要が表示されます。ONTAP では、各ルールにルールインデックス番号が割り当てられます。ルールインデックス番号を確認したあと、その番号を使用して、指定したエクスポートルールの詳細情報を表示できます。

### 8. エクスポートポリシーに適用されたルールが正しく設定されていることを確認します。

```
vserver export-policy rule show -policyname policy_name -vserver vserver_name -ruleindex integer
```

例

次のコマンドは、rs1 というエクスポートポリシーで、vs1 という名前の SVM 上のエクスポートルールを作成し、作成を確認します。ルールのインデックス番号は 1 です。このルールは、ドメイン eng.company.com およびネットグループ @netgroup1 内のどのクライアントとも一致します。すべての NFS アクセスを有効にしています。AUTH\_SYS で認証されたユーザに対する読み取り専用および読み取り / 書き込みアクセスを有効にしています。UNIX ユーザ ID が 0（ゼロ）のクライアントは、Kerberos 以外で認証すると匿名化されます。

```
vs1::> vserver export-policy rule create -vserver vs1 -policyname expl
-ruleindex 1 -protocol nfs
-clientmatch .eng.company.com,@netgoup1 -rorule sys -rwrule sys -anon
65534 -superuser krb5
```

```
vs1::> vserver export-policy rule show -policyname nfs_policy
```

Virtual Server	Policy Name	Rule Index	Access Protocol	Client Match	RO Rule
vs1	expl	1	nfs	eng.company.com, @netgroup1	sys

```
vs1::> vserver export-policy rule show -policyname expl -vserver vs1
-ruleindex 1
```

```

Vserver: vs1
Policy Name: expl
Rule Index: 1
Access Protocol: nfs
Client Match Hostname, IP Address, Netgroup, or Domain:
eng.company.com,@netgroup1
RO Access Rule: sys
RW Access Rule: sys
User ID To Which Anonymous Users Are Mapped: 65534
Superuser Security Types: krb5
Honor SetUID Bits in SETATTR: true
Allow Creation of Devices: true
```

次のコマンドは、expol2 というエクスポートポリシーで vs2 という SVM に対するエクスポートルールを作成し、作成を確認します。このルールのインデックス番号は21です。このルールは、クライアントをネットグループ dev\_netgroup\_main のメンバーと照合します。すべての NFS アクセスを有効にしています。AUTH\_SYS によって認証されたユーザの読み取り専用アクセスを有効にし、読み取り / 書き込みおよびルートアクセスについては Kerberos 認証を要求します。UNIX ユーザ ID が 0（ゼロ）のクライアントは、Kerberos 以外で認証するとルートアクセスを拒否されます。

```
vs2::> vsserver export-policy rule create -vsserver vs2 -policyname expol2
-ruleindex 21 -protocol nfs
-clientmatch @dev_netgroup_main -rorule sys -rwrule krb5 -anon 65535
-superuser krb5
```

```
vs2::> vsserver export-policy rule show -policyname nfs_policy
```

Virtual Server	Policy Name	Rule Index	Access Protocol	Client Match	RO Rule
vs2	expol2	21	nfs	@dev_netgroup_main	sys

```
vs2::> vsserver export-policy rule show -policyname expol2 -vsserver vs1
-ruleindex 21
```

```

Vserver: vs2
Policy Name: expol2
Rule Index: 21
Access Protocol: nfs
Client Match Hostname, IP Address, Netgroup, or Domain:
                                         @dev_netgroup_main
RO Access Rule: sys
RW Access Rule: krb5
User ID To Which Anonymous Users Are Mapped: 65535
Superuser Security Types: krb5
Honor SetUID Bits in SETATTR: true
Allow Creation of Devices: true

```

ボリュームまたは **qtree** のストレージコンテナを作成します

ボリュームを作成します

を使用して、ボリュームを作成し、ジャンクションポイントやその他のプロパティを指定できます `volume create` コマンドを実行します

このタスクについて

クライアントがデータを使用できるようにするには、ボリュームに *junction path* を含める必要があります。ジャンクションパスは、新しいボリュームを作成するときに指定できます。ジャンクションパスを指定せずにボリュームを作成する場合は、を使用してSVMネームスペースにボリュームを `_mount_` する必要があります `volume mount` コマンドを実行します

作業を開始する前に

- NFSがセットアップされ、実行されている必要があります。
- SVMのセキュリティ形式がUNIXである必要があります。
- ONTAP 9.13.1以降では、容量分析とアクティビティ追跡を有効にしてボリュームを作成できます。容量またはアクティビティトラッキングを有効にするには、を問題します `volume create` コマンドにを指定



します `-analytics-state` または `-activity-tracking-state` をに設定します `on`。

容量分析とアクティビティ追跡の詳細については、を参照してください [File System Analytics](#) を有効にします。

## 手順

1. ジャンクションポイントを指定してボリュームを作成します。

```
volume create -vserver svm_name -volume volume_name -aggregate aggregate_name
-size {integer[KB|MB|GB|TB|PB]} -security-style unix -user user_name_or_number
-group group_name_or_number -junction-path junction_path [-policy
export_policy_name]
```

の選択 `-junction-path` 次のようなものがあります。

- ルートの直下。例： `/new_vol`

新しいボリュームを作成し、SVM のルートボリュームに直接マウントされるように指定することができます。

- 既存のディレクトリの下（例： `/existing_dir/new_vol`）

新しいボリュームを作成し、ディレクトリとして表現されている既存のボリューム（既存の階層内）にマウントされるように指定できます。

新しいディレクトリ（新しいボリュームの下の新しい階層）にボリュームを作成する場合は、次のように指定します。 `/new_dir/new_vol` その後、SVM ルートボリュームにジャンクションされた新しい親ボリュームを作成しておく必要があります。その後、新しい親ボリューム（新しいディレクトリ）のジャンクションパスに新しい子ボリュームを作成します。

[+]

既存のエクスポートポリシーを使用する場合は、ボリュームの作成時にそのポリシーを指定できます。エクスポートポリシーは、を使用してあとから追加することもできます `volume modify` コマンドを実行します

2. 目的のジャンクションポイントでボリュームが作成されたことを確認します。

```
volume show -vserver svm_name -volume volume_name -junction
```

## 例

次のコマンドは、SVM `vs1.example.com` およびアグリゲート `aggr1` 上に、`users1` という名前の新しいボリュームを作成します。新しいボリュームは、で使用できます `/users`。ボリュームのサイズは `750GB` で、ボリュームギャランティのタイプは `volume`（デフォルト）です。

```
cluster1::> volume create -vserver vs1.example.com -volume users
-aggregate aggr1 -size 750g -junction-path /users
[Job 1642] Job succeeded: Successful
```

```
cluster1::> volume show -vserver vs1.example.com -volume users -junction
```

Vserver	Volume	Active	Junction Path	Junction Path Source
vs1.example.com	users1	true	/users	RW_volume

次のコマンドは、SVM 「vs1.example.com」 およびアグリゲート「aggr1」に、「home4」という名前の新しいボリュームを作成します。ディレクトリ /eng/ はvs1 SVMのネームスペースにすでに存在し、新しいボリュームはで使えるようになります /eng/home`をクリックします。これがのホームディレクトリになります ` /eng/ ネームスペース：ボリュームのサイズは750GBで、ボリュームギャランティのタイプはです volume（デフォルト）。

```
cluster1::> volume create -vserver vs1.example.com -volume home4
-aggregate aggr1 -size 750g -junction-path /eng/home
[Job 1642] Job succeeded: Successful
```

```
cluster1::> volume show -vserver vs1.example.com -volume home4 -junction
```

Vserver	Volume	Active	Junction Path	Junction Path Source
vs1.example.com	home4	true	/eng/home	RW_volume

**qtree** を作成します

を使用して、データを含むqtreeを作成し、そのプロパティを指定できます volume qtree create コマンドを実行します

必要なもの

- SVM と新しい qtree を格納するボリュームがすでに存在している必要があります。
- SVM のセキュリティ形式が UNIX で、NFS が設定されて実行されている必要があります。

手順

1. qtree を作成します。

```
volume qtree create -vserver vserver_name { -volume volume_name -qtree
qtree_name | -qtree-path qtree path } -security-style unix [-policy
export_policy_name]
```

ボリュームとqtreeを別々の引数として指定するか、の形式でqtreeパスの引数を指定できます /vol/volume\_name/\_qtree\_name。

デフォルトでは、qtree は親ボリュームのエクスポートポリシーを継承しますが、独自のものを使用するように設定することもできます。既存のエクスポートポリシーを使用する場合は、qtree の作成時にポリシーを指定できます。エクスポートポリシーは、を使用してあとから追加することもできます volume qtree modify コマンドを実行します

2. qtree が必要なジャンクションパスで作成されたことを確認します。

```
volume qtree show -vserver vs1.example.com { -volume volume_name -qtree
qtree_name | -qtree-path qtree path }
```

#### 例

次の例は、ジャンクションパスがであるSVM vs1.example.com上に、qt01という名前のqtreeを作成します /vol/data1 :

```
cluster1::> volume qtree create -vserver vs1.example.com -qtree-path
/vol/data1/qt01 -security-style unix
[Job 1642] Job succeeded: Successful
```

```
cluster1::> volume qtree show -vserver vs1.example.com -qtree-path
/vol/data1/qt01
```

```

Vserver Name: vs1.example.com
Volume Name: data1
Qtree Name: qt01
Actual (Non-Junction) Qtree Path: /vol/data1/qt01
Security Style: unix
Oplock Mode: enable
Unix Permissions: ---rwxr-xr-x
Qtree Id: 2
Qtree Status: normal
Export Policy: default
Is Export Policy Inherited: true
```

エクスポートポリシーを使用して **NFS** アクセスを保護

エクスポートポリシーを使用して **NFS** アクセスを保護

エクスポートポリシーを使用することにより、ボリュームまたは qtree への NFS アクセスを特定のパラメータに一致するクライアントだけに制限することができます。新しいストレージをプロビジョニングするときに、既存のポリシーとルールを使用するか、既存のポリシーにルールを追加するか、新しいポリシーとルールを作成することができます。エクスポートポリシーの設定を確認することもできます



ONTAP 9.3 以降では、エクスポートポリシーの設定チェックをバックグラウンドジョブとして有効にし、すべてのルール違反をエラールールリストに記録することができます。 `vserver export-policy config-checker` コマンドはチェッカーを呼び出して結果を表示します。この結果を使用して、構成を検証し、誤ったルールをポリシーから削除できます。このコマンドで検証されるのは、エクスポート設定のホスト名、ネットグループ、匿名ユーザのみです。

エクスポートルールの処理順序を管理します

使用できます `vserver export-policy rule setindex` 既存のエクスポートルールのインデックス番号を手動で設定するコマンド。これにより、ONTAP がクライアント要求に対してエクスポートルールを適用する優先順位を指定できます。

このタスクについて

新しいインデックス番号がすでに使用されている場合は、指定した場所にルールが挿入され、それに応じてリストの順序が変更されます。

ステップ

1. 指定したエクスポートルールのインデックス番号を変更します。

```
vserver export-policy rule setindex -vserver virtual_server_name -policyname policy_name -ruleindex integer -newruleindex integer
```

例

次のコマンドは、`vs1` という SVM の `rs1` というエクスポートポリシーのインデックス番号を 3 から 2 に変更します。

```
vs1::> vserver export-policy rule setindex -vserver vs1  
-policyname rs1 -ruleindex 3 -newruleindex 2
```

エクスポートポリシーをボリュームに割り当てます

SVM 内の各ボリュームには、クライアントがボリューム内のデータにアクセスするためのエクスポートルールを含むエクスポートポリシーを関連付ける必要があります。

このタスクについて

エクスポートポリシーは、ボリュームの作成時、またはボリュームの作成後にいつでも、ボリュームに関連付けることができます。1 つのボリュームに関連付けることができるのは 1 つのエクスポートポリシーですが、1 つのポリシーを多数のボリュームに関連付けることができます。

手順

1. ボリュームの作成時にエクスポートポリシーを指定しなかった場合は、ボリュームにエクスポートポリシーを割り当てます。

```
volume modify -vserver vserver_name -volume volume_name -policy export_policy_name
```

2. ポリシーがボリュームに割り当てられたことを確認します。

```
volume show -volume volume_name -fields policy
```

#### 例

次のコマンドは、エクスポートポリシー `nfs_policy` を `vs1` という SVM 上のボリューム `vol1` に割り当てて、割り当てを確認します。

```
cluster::> volume modify -vserver vs1 -volume vol1 -policy nfs_policy

cluster::>volume show -volume vol -fields policy
vserver volume      policy
-----
vs1      vol1      nfs_policy
```

エクスポートポリシーを **qtree** に割り当てます

ボリューム全体をエクスポートする代わりに、ボリュームの特定の **qtree** をエクスポートしてクライアントから直接アクセスできるようにすることもできます。**qtree** をエクスポートするには、**qtree** にエクスポートポリシーを割り当てます。エクスポートポリシーの割り当ては、新しい **qtree** の作成時に行うことも、既存の **qtree** の変更によって行うこともできます。

#### 必要なもの

エクスポートポリシーが存在している必要があります。

#### このタスクについて

**qtree** では、作成時に指定しなかった場合、格納先ボリュームの親のエクスポートポリシーがデフォルトで継承されます。

エクスポートポリシーは、**qtree** の作成時、または **qtree** の作成後にいつでも、**qtree** に関連付けることができます。1 つの **qtree** に関連付けることができるのは 1 つのエクスポートポリシーですが、1 つのポリシーを多数の **qtree** と関連付けることができます。

#### 手順

1. **qtree** の作成時にエクスポートポリシーを指定しなかった場合は、**qtree** にエクスポートポリシーを割り当てます。

```
volume qtree modify -vserver vserver_name -qtree-path
/vol/volume_name/qtree_name -export-policy export_policy_name
```

2. ポリシーが **qtree** に割り当てられたことを確認します。

```
volume qtree show -qtree qtree_name -fields export-policy
```

#### 例

次のコマンドは、エクスポートポリシー `nfs_policy` を `vs1` という SVM 上の **qtree** `qt1` に割り当てて、割り当てを確認します。

```
cluster::> volume modify -vserver vs1 -qtree-path /vol/vol1/qt1 -policy
nfs_policy

cluster::>volume qtree show -volume vol1 -fields export-policy
vserver volume qtree export-policy
-----
vs1      data1  qt01  nfs_policy
```

## クラスタからの **NFS** クライアントアクセスを確認

UNIX 管理ホストで UNIX ファイル権限を設定することにより、選択したクライアントに共有へのアクセスを許可できます。を使用してクライアントアクセスを確認できます  
vserver export-policy check-access コマンドを実行し、必要に応じてエクスポートルールを調整します。

### 手順

1. クラスタで、を使用してエクスポートへのクライアントアクセスを確認します vserver export-policy check-access コマンドを実行します

次のコマンドは、IP アドレスが 1.2.3.4 の NFSv3 クライアントによるボリューム home2 への読み取り / 書き込みアクセスをチェックします。コマンド出力には、ボリュームでエクスポートポリシーが使用されていることが示されます exp-home-dir アクセスは拒否されます

```
cluster1::> vserver export-policy check-access -vserver vs1 -client-ip
1.2.3.4 -volume home2 -authentication-method sys -protocol nfs3 -access
-type read-write
```

Path	Policy	Policy Owner	Policy Owner Type	Rule Index	Access
/	default	vs1_root	volume	1	read
/eng	default	vs1_root	volume	1	read
/eng/home2	exp-home-dir	home2	volume	1	denied

3 entries were displayed.

2. 出力を確認して、エクスポートポリシーが意図したとおりに機能してクライアントアクセスが想定どおりに動作しているかどうかを判断します。

具体的には、ボリュームまたは qtree によって使用されたエクスポートポリシーと、結果としてクライアントが行ったアクセスのタイプを確認する必要があります。

3. 必要に応じて、エクスポートポリシールールを再設定します。

クライアントシステムからの **NFS** アクセスをテストします

新しいストレージオブジェクトに対する NFS アクセスの確認が完了したら、設定をテストする必要があります。設定をテストするには、NFS 管理ホストにログインし、SVM に対するデータの読み取りと書き込みが可能かどうかを確認します。その後、root 以外のユーザとしてクライアントシステム上で処理を繰り返します。

必要なもの

- クライアントシステムに、前に指定したエクスポートルールで許可されている IP アドレスが割り当てられている必要があります。
- root ユーザのログイン情報が必要です。

手順

1. クラスタで、新しいボリュームをホストしている LIF の IP アドレスを確認します。

```
network interface show -vserver svm_name
```

2. 管理ホストクライアントシステムに root ユーザとしてログインします。
3. ディレクトリをマウントフォルダに変更します。

```
cd /mnt/
```

4. 新しいフォルダを作成し、SVM の IP アドレスを使用してマウントします。

- a. 新しいフォルダを作成します。

[+]

```
mkdir /mnt/folder
```

- b. 次の新しいディレクトリに新しいボリュームをマウントします。

[+]

```
mount -t nfs -o hard IPAddress:/volume_name /mnt/folder
```

- c. ディレクトリを新しいフォルダに変更します。

[+]

```
cd folder
```

次のコマンドでは、test1 という名前のフォルダを作成し、IP アドレス 192.0.2.130 のボリューム vol1 をマウントフォルダ test1 にマウントして、ディレクトリを新しい test1 に変更しています。

```
host# mkdir /mnt/test1
host# mount -t nfs -o hard 192.0.2.130:/vol1 /mnt/test1
host# cd /mnt/test1
```

5. 新しいファイルを作成し、そのファイルが存在することを確認して、テキストを書き込みます。

- a. テストファイルを作成します。

[+]

```
touch filename
```

- b. ファイルが存在することを確認します。

```
[+]
ls -l filename
```

c. 入力するコマンド

```
[+]
cat > filename
```

テキストを入力してから Ctrl+D を押してテストファイルにテキストを書き込みます。

d. テストファイルの内容を表示します。

```
[+]
cat filename
```

e. テストファイルを削除します。

```
[+]
rm filename
```

f. 親ディレクトリに戻ります。

```
[+]
cd ..
```

```
host# touch myfile1
host# ls -l myfile1
-rw-r--r-- 1 root root 0 Sep 18 15:58 myfile1
host# cat >myfile1
This text inside the first file
host# cat myfile1
This text inside the first file
host# rm -r myfile1
host# cd ..
```

6. root として、マウントされたボリュームに対する必要な UNIX の所有権と権限を設定します。

7. エクスポートルールで特定されている UNIX クライアントシステムで、新しいボリュームへのアクセス権を持つ許可されたユーザとしてログインし、手順 3～5 を繰り返して、ボリュームのマウントとファイルの作成が可能なことを確認します。

## 追加情報の参照先

NFS クライアントアクセスをテストしたあと、NFS の追加設定を行ったり、SAN アクセスを追加したりできます。プロトコルアクセスが完了したら、Storage Virtual Machine (SVM) のルートボリュームを保護する必要があります。

### NFS構成

NFS アクセスについてさらに詳しく設定するには、以下の情報とテクニカルレポートを参照してください。

- ["NFS の管理"](#)

NFS を使用したファイルアクセスを設定および管理する方法について説明しています。



- ["ネットアップテクニカルレポート 4067 : 『 NFS Best Practice and Implementation Guide 』 "](#)

NFSv3 および NFSv4 の運用ガイドであり、NFSv4 を中心に ONTAP オペレーティングシステムの概要を説明しています。

- ["ネットアップテクニカルレポート 4073 : 『 Secure Unified Authentication 』 "](#)

NFS ストレージ認証用に UNIX ベースの Kerberos バージョン 5 ( krb5 ) サーバを使用する ONTAP の設定方法と、KDC および Lightweight Directory Access Protocol ( LDAP ) のアイデンティティプロバイダとして Windows Server Active Directory ( AD ) を使用するための の設定方法について説明しています。

- ["ネットアップテクニカルレポート 3580 : 『 NFSv4 の拡張内容とベスト・プラクティス・ガイド - Data ONTAP での実装 』 "](#)

ONTAP を実行するシステムに接続された AIX 、 Linux 、または Solaris クライアントに NFSv4 のコンポーネントを実装する際のベストプラクティスを紹介しています。

## ネットワーク構成

ネットワーク機能とネームサービスについてさらに詳しく設定するには、次の情報とテクニカルレポートを参照してください。

- ["NFS の管理"](#)

ONTAP ネットワークを設定および管理する方法について説明しています。

- ["ネットアップテクニカルレポート 4182 : 『 Clustered Data ONTAP 構成でのイーサネットストレージのベストプラクティス 』 "](#)

ONTAP ネットワーク設定の実装について説明し、一般的なネットワーク導入シナリオおよびベストプラクティスの推奨事項を提供しています。

- ["ネットアップテクニカルレポート 4668 : 『 Name Services Best Practices Guide 』 "](#)

認証用に LDAP 、 NIS 、 DNS 、およびローカルファイルの設定を行う方法について説明します。

## SAN プロトコルの設定

新しい SVM に対する SAN アクセスを提供または変更する場合は、FC または iSCSI の設定情報を使用できます。この情報は、複数のホストオペレーティングシステムに対応しています。

## ルートボリュームの保護

SVM でプロトコルを設定したら、ルートボリュームを保護してください。

- ["データ保護"](#)

負荷共有ミラーを作成して SVM ルートボリュームを保護する方法について説明しています。これは、NAS 対応の SVM に対するネットアップのベストプラクティスです。また、SVM ルートボリュームを負荷共有ミラーから昇格させてボリュームの障害や消失からリカバリする簡単な方法についても説明しています。

# ONTAP エクスポートと 7-Mode エクスポートの違い

## ONTAP エクスポートと 7-Mode エクスポートの違い

ONTAP でのNFSエクスポートの実装方法に詳しくない場合は、7-ModeとONTAP のエクスポート設定ツール、およびサンプルの7-Modeを比較してください /etc/exports クラスタ化されたポリシーとルールを含むファイル。

ONTAP ではありません /etc/exports ファイルではありません exportfs コマンドを実行します代わりに、エクスポートポリシーを定義する必要があります。エクスポートポリシーを使用すると、7-Mode の場合とほとんど同じ方法でクライアントアクセスを制御できます。また、1つのエクスポートポリシーを複数のボリュームに再利用できるなどの機能も追加されています。

### 関連情報

["NFS の管理"](#)

["ネットアップテクニカルレポート 4067：『NFS Best Practice and Implementation Guide』"](#)

## 7-Mode と ONTAP のエクスポートの比較

ONTAP でのエクスポートは、定義方法と使用方法が 7-Mode 環境とは異なります。

相違点	7-Mode	ONTAP
エクスポートの定義方法	エクスポートはで定義されます /etc/exports ファイル。	エクスポートは、SVM 内でエクスポートポリシーを作成することによって定義されます。SVM には複数のエクスポートポリシーを含めることができます。
エクスポートの範囲	<ul style="list-style-type: none"><li>エクスポートは指定したファイルパスまたは qtree に適用されます。</li><li>で別のエントリを作成する必要があります /etc/exports ファイルパスまたはqtreeごとに指定します。</li><li>エクスポートは、で定義されている場合にのみ保持されます /etc/exports ファイル。</li></ul>	<ul style="list-style-type: none"><li>エクスポートポリシーは、ボリューム内のすべてのファイルパスおよび qtree を含むボリューム全体に適用されます。</li><li>エクスポートポリシーは、必要に応じて複数のボリュームに適用できます。</li><li>システムの再起動後も、すべてのエクスポートポリシーが永続します。</li></ul>

フェンシング（特定のクライアントに対して同じリソースへの別のアクセスを指定すること）	特定のクライアントに単一のエクスポートされたリソースへの異なるアクセスを提供するには、で各クライアントとその許可されているアクセスをリストする必要があります /etc/exports ファイル。	エクスポートポリシーは、多数のエクスポートルールで構成されています。エクスポートルールごとに、リソースに対する特定のアクセス権限が定義され、該当する権限を持つクライアントが一覧表示されます。特定のクライアントに対して異なるアクセスを指定するには、特定のアクセス権限セットごとにエクスポートルールを作成し、それらの権限を持つクライアントをリストして、エクスポートポリシーにルールを追加する必要があります。
名前のエイリアス設定	エクスポートを定義するときに、エクスポートの名前として、ファイルパスとは異なる名前を選択できます。を使用する必要があります -actual でこのようなエクスポートを定義するときのパラメータ /etc/exports ファイル。	<p>エクスポートされたボリュームの名前として、実際のボリューム名とは異なる名前を選択できます。そのためには、カスタムジャンクションパス名を持つボリュームをSVMネームスペース内でマウントする必要があります。</p> <div>  <p>デフォルトでは、ボリュームは、それぞれのボリューム名でマウントされます。ボリュームのジャンクションパス名をカスタマイズするには、マウント解除し、名前を変更してから、再マウントする必要があります。</p> </div>

## ONTAP エクスポートポリシーの例

エクスポートポリシーの例を確認すると、ONTAP でのエクスポートポリシーの動作について理解を深めることができます。

### 7-Mode エクスポートの ONTAP 実装例

次の例は、に表示される7-Modeエクスポートを示しています /etc/export ファイル：

```
/vol/vol1 -sec=sys,ro=@readonly_netgroup,rw=@readwrite_netgroup1:
@readwrite_netgroup2:@rootaccess_netgroup,root=@rootaccess_netgroup
```

このエクスポートをクラスタエクスポートポリシーとして再現するには、3つのエクスポートルールを含むエクスポートポリシーを作成し、そのエクスポートポリシーをボリューム vol1 に割り当てる必要があります。

す。

ルール	要素（ <b>Element</b> ）	価値
ルール 1	-clientmatch（クライアント仕様）	@readonly_netgroup
-ruleindex（ルールリスト内でのエクスポートルールの位置）	1	-protocol
nfs	-rorule（読み取り専用アクセスを許可）	sys（クライアントはAUTH_SYSで認証されます）
-rwrule（読み取り/書き込みアクセスを許可）	never	-superuser（スーパーユーザアクセスを許可）
none（root_squashed_to anon）	ルール2	-clientmatch
@rootaccess_netgroup	-ruleindex	2
-protocol	nfs	-rorule
sys	-rwrule	sys
-superuser	sys	ルール3
-clientmatch	@readwrite_netgroup1,@readwrite_netgroup2	-ruleindex
3	-protocol	nfs
-rorule	sys	-rwrule
sys	-superuser	none

1. exp\_vol1 というエクスポートポリシーを作成します。

```
vserver export-policy create -vserver NewSVM -policyname exp_vol1
```

2. 基本コマンドに対して、次のパラメータを指定して 3 つのルールを作成します。

◦ 基本コマンド：

[+]

```
vserver export-policy rule create -vserver NewSVM -policyname exp_vol1
```

◦ ルールパラメータ：

```
[] -clientmatch @readonly_netgroup -ruleindex 1 -protocol nfs -rorule sys -rwrule never -superuser
```

```

none` []
-clientmatch @rootaccess_netgroup -ruleindex 2 -protocol nfs -rorule sys
-rwrule sys -superuser sys
[+]
-clientmatch @readwrite_netgroup1,@readwrite_netgroup2 -ruleindex 3
-protocol nfs -rorule sys -rwrule sys -superuser none

```

3. ボリューム vol1 にポリシーを割り当てます。

```
volume modify -vserver NewSVM -volume vol1 -policy exp_vol1
```

## 7-Mode エクスポートの統合の例

次の例は、7-Modeを示しています /etc/export 10個のqtreeごとに1行で構成されるファイル：

```

/vol/vol1/q_1472 -sec=sys,rw=host1519s,root=host1519s
/vol/vol1/q_1471 -sec=sys,rw=host1519s,root=host1519s
/vol/vol1/q_1473 -sec=sys,rw=host1519s,root=host1519s
/vol/vol1/q_1570 -sec=sys,rw=host1519s,root=host1519s
/vol/vol1/q_1571 -sec=sys,rw=host1519s,root=host1519s
/vol/vol1/q_2237 -sec=sys,rw=host2057s,root=host2057s
/vol/vol1/q_2238 -sec=sys,rw=host2057s,root=host2057s
/vol/vol1/q_2239 -sec=sys,rw=host2057s,root=host2057s
/vol/vol1/q_2240 -sec=sys,rw=host2057s,root=host2057s
/vol/vol1/q_2241 -sec=sys,rw=host2057s,root=host2057s

```

ONTAP では、qtreeごとに2つのポリシーのうちの1つ（を含むルールが設定されたポリシー）が必要です  
 -clientmatch host1519s、またはを含むルールを持つ1つ -clientmatch host2057s。

1. exp\_vol1q1 と exp\_vol1q2 という 2 つのエクスポートポリシーを作成します。

```

° vserver export-policy create -vserver NewSVM -policyname exp_vol1q1
° vserver export-policy create -vserver NewSVM -policyname exp_vol1q2

```

2. 各ポリシーのルールを作成します。

```

° vserver export-policy rule create -vserver NewSVM -policyname exp_vol1q1
  -clientmatch host1519s -rwrule sys -superuser sys
° vserver export-policy rule create -vserver NewSVM -policyname exp_vol1q2
  -clientmatch host1519s -rwrule sys -superuser sys

```

3. ポリシーを qtree に適用します。

```

° volume qtree modify -vserver NewSVM -qtree-path /vol/vol1/q_1472 -export
  -policy exp_vol1q1
° [ 続く 4 つの qtree ...]
° volume qtree modify -vserver NewSVM -qtree-path /vol/vol1/q_2237 -export
  -policy exp_vol1q2
° [ 続く 4 つの qtree ...]

```

これらのホスト用に qtree をあとから追加する必要がある場合は、同じエクスポートポリシーを使用します。

## CLIを使用したNFSの管理

### NFS のリファレンスの概要

ONTAP には、NFS プロトコルで利用できるファイルアクセス機能が含まれています。NFS サーバおよびエクスポートボリュームまたは qtree を有効にすることができます。

これらの手順は、次の状況で実行します。

- ONTAP NFSプロトコルの機能の範囲について理解する必要がある。
- NFSの基本的な設定ではなく、あまり一般的でない設定タスクとメンテナンスタスクを実行する。
- System Manager や自動スクリプトツールではなく、コマンドラインインターフェイス（CLI）を使用する必要がある。

### NAS ファイルアクセスを理解する

#### ネームスペースとジャンクションポイント

##### ネームスペースとジャンクションポイントの概要

`nas_namespace_` は、`_junction points_to` によって結合されたボリュームを論理的にグループ化して、単一のファイルシステム階層を作成します。十分な権限を持つクライアントは、ストレージ内のファイルの場所を指定せずにネームスペース内のファイルにアクセスできます。ジャンクションされたボリュームはクラスタ内の任意の場所に配置できます。

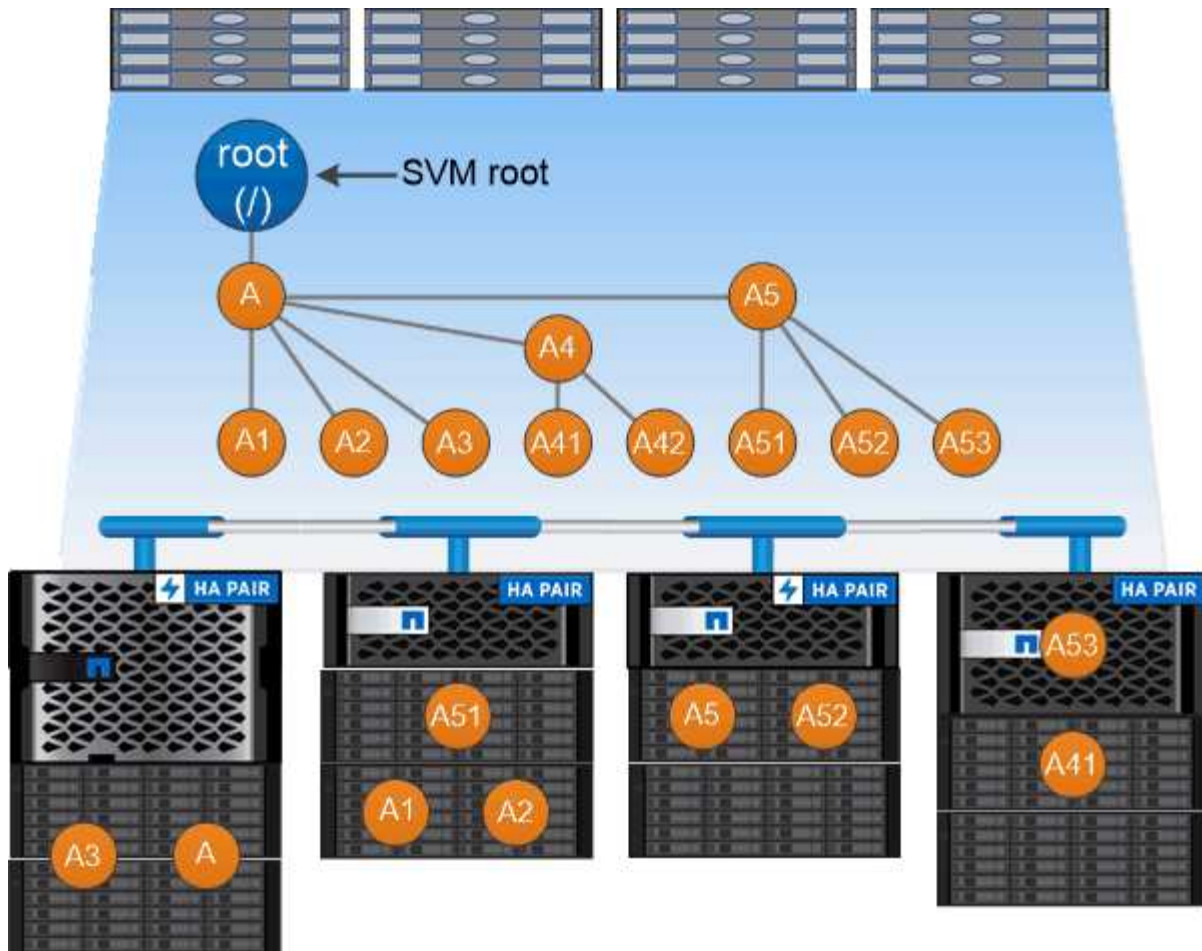
NAS クライアントは、目的のファイルを含むすべてのボリュームをマウントするのではなく、`nfs_export_` をマウントするか、`SMB_share` にアクセスします。`_エクスポート` または `共有` は、ネームスペース全体またはネームスペース内の中間的な場所を表します。クライアントは、アクセスポイントより下にマウントされたボリュームにのみアクセスします。

ネームスペースには必要に応じてボリュームを追加できます。ジャンクションポイントは、親ボリュームジャンクションのすぐ下に作成することも、ボリューム内のディレクトリに作成することもできます。「vol3」という名前のボリュームのボリュームジャンクションへのパスは、になることがあります `/vol1/vol2/vol3`` または ``/vol1/dir2/vol3`` あるいは ``/dir1/dir2/vol3`。このパスのことを `_junction` パスと呼びます。 \_

SVM には、それぞれ一意のネームスペースがあります。SVM ルートボリュームは、ネームスペース階層へのエントリポイントです。



ノードに障害やフェイルオーバーが発生したときにデータを引き続き利用できるようにするには、SVM ルートボリュームに `_load-sharing mirror_copy` を作成する必要があります。



*A namespace is a logical grouping of volumes joined together at junction points to create a single file system hierarchy.*

例

次の例は、ジャンクションパスがである「home4」という名前のボリュームをSVM vs1上に作成します  
/eng/home :

```
cluster1::> volume create -vserver vs1 -volume home4 -aggregate aggr1
-size 1g -junction-path /eng/home
[Job 1642] Job succeeded: Successful
```

一般的な **NAS** ネームスペースアーキテクチャとは

SVM ネームスペースを作成するときに使用できる一般的な NAS ネームスペースアーキテクチャがいくつかあります。ビジネスやワークフローのニーズに合わせて、ネームスペースアーキテクチャを選択できます。

ネームスペースの最上位は常にルートボリュームであり、スラッシュ (/) で表されます。ルートの下位のネームスペースアーキテクチャは、次の 3 つの基本カテゴリに分類されます。

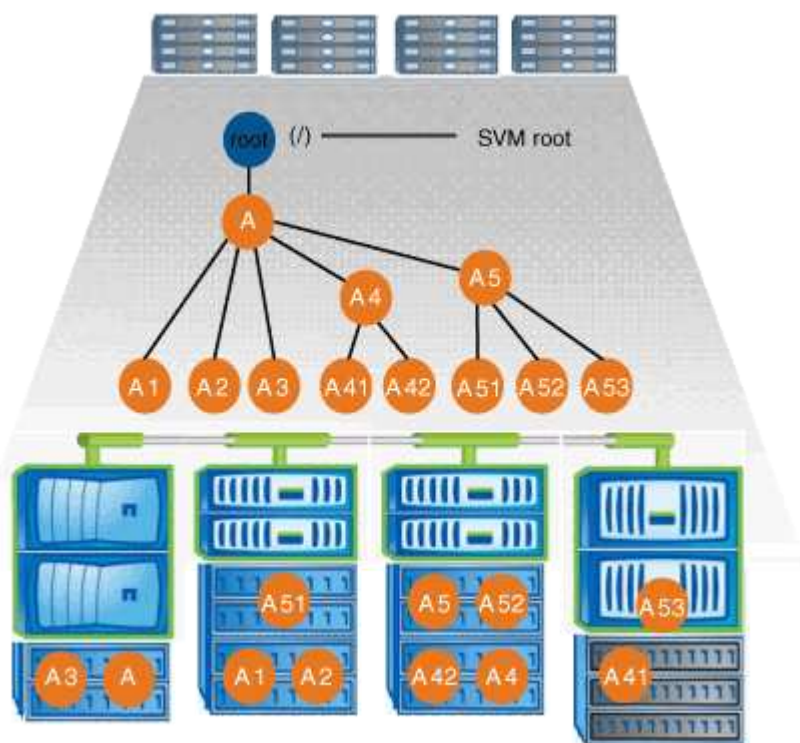
- ネームスペースのルートへのジャンクションポイントを 1 つ備えた単一のブランチツリー



- ネームスペースのルートへのジャンクションポイントを複数備えた複数分岐ツリー
- 複数のスタンドアロンボリュームがそれぞれ、ネームスペースのルートへの個別のジャンクションポイントを備えています

### 単一分岐ツリーを使用するネームスペース

単一分岐のツリーを使用するアーキテクチャには、SVM ネームスペースのルートへの単一の挿入ポイントがあります。単一の挿入ポイントは、結合されたボリュームまたはルートの下ディレクトリのどちらかになります。それ以外のすべてのボリュームは、単一の挿入ポイントの下のジャンクションポイント（ボリュームまたはディレクトリ）でマウントされます。



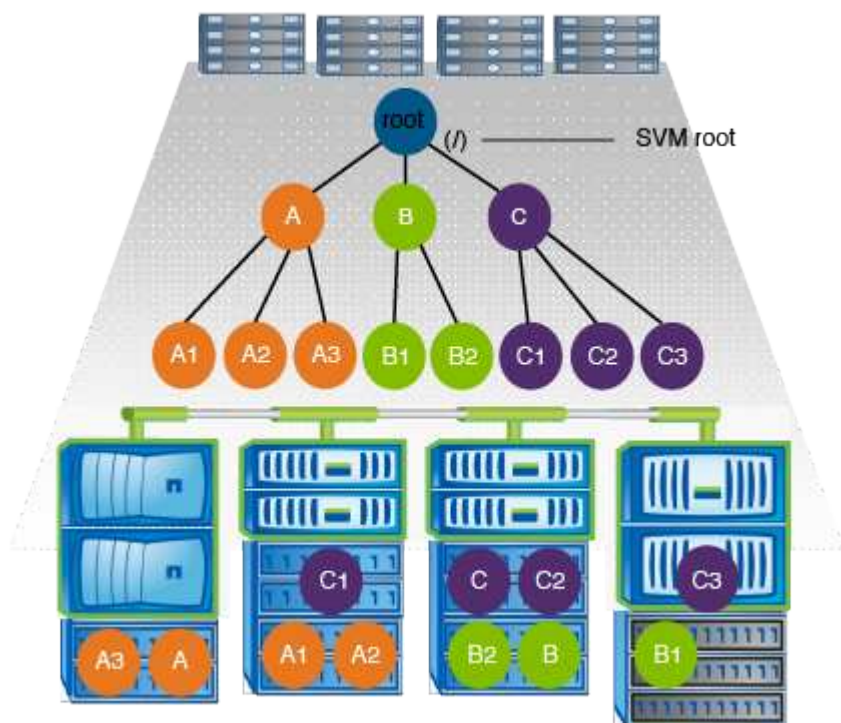
たとえば、上記のネームスペースアーキテクチャを使用する標準的なボリュームジャンクション構成は、すべてのボリュームが単一の挿入ポイントの下で結合された以下のような構成になります。これは「d ATA」というディレクトリです。



Vserver	Volume	Junction Active	Junction Path	Junction Path Source
vs1	corp1	true	/data/dir1/corp1	RW_volume
vs1	corp2	true	/data/dir1/corp2	RW_volume
vs1	data1	true	/data/data1	RW_volume
vs1	eng1	true	/data/data1/eng1	RW_volume
vs1	eng2	true	/data/data1/eng2	RW_volume
vs1	sales	true	/data/data1/sales	RW_volume
vs1	vol1	true	/data/vol1	RW_volume
vs1	vol2	true	/data/vol2	RW_volume
vs1	vol3	true	/data/vol3	RW_volume
vs1	vs1_root	-	/	-

## 複数分岐ツリーを使用するネームスペース

複数分岐のツリーを使用するネームスペースには、SVM ネームスペースのルートへの複数の挿入ポイントがあります。挿入ポイントは、ルート直下で結合されたボリュームまたはディレクトリのどちらかになります。それ以外のすべてのボリュームは、挿入ポイントの下のジャンクションポイント（ボリュームまたはディレクトリ）でマウントされます。

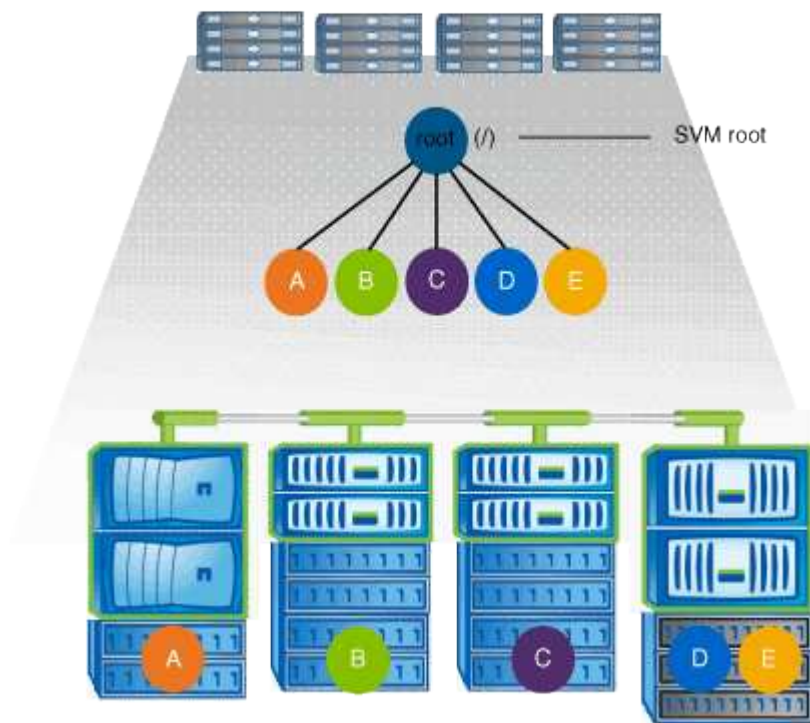


たとえば、上記のネームスペースアーキテクチャを使用する標準的なボリュームジャンクション構成は、SVM のルートボリュームへの 3 つの挿入ポイントがある以下のような構成になります。2 つの挿入ポイントは、「data」と「projects」という名前のディレクトリです。挿入ポイントの 1 つは「audit」という名前の結合されたボリュームです。

Vserver	Volume	Junction Active	Junction Path	Junction Path Source
vs1	audit	true	/audit	RW_volume
vs1	audit_logs1	true	/audit/logs1	RW_volume
vs1	audit_logs2	true	/audit/logs2	RW_volume
vs1	audit_logs3	true	/audit/logs3	RW_volume
vs1	eng	true	/data/eng	RW_volume
vs1	mktg1	true	/data/mktg1	RW_volume
vs1	mktg2	true	/data/mktg2	RW_volume
vs1	project1	true	/projects/project1	RW_volume
vs1	project2	true	/projects/project2	RW_volume
vs1	vs1_root	-	/	-

### 複数のスタンドアロンボリュームを含むネームスペース

スタンドアロンボリュームを使用するアーキテクチャでは、すべてのボリュームに SVM ネームスペースのルートへの挿入ポイントがありますが、それらのボリュームは別のボリュームの下でジャンクションされません。各ボリュームは一意的なパスを持ち、ルート直下で結合されているか、ルートより下のディレクトリで結合されています。



たとえば、上記のネームスペースアーキテクチャを使用する標準的なボリュームジャンクション構成は、SVM のルートボリュームへの 5 つの挿入ポイントがあり、それぞれが 1 つのボリュームへのパスを表す以下のような構成になります。

Vserver	Volume	Junction		Junction	
		Active	Junction Path	Path	Source
vs1	eng	true	/eng	RW_volume	
vs1	mktg	true	/vol/mktg	RW_volume	
vs1	project1	true	/project1	RW_volume	
vs1	project2	true	/project2	RW_volume	
vs1	sales	true	/sales	RW_volume	
vs1	vs1_root	-	/	-	

## ONTAP によるファイルアクセスの制御方法

### ONTAP によるファイルアクセスの制御の概要

ONTAP は、指定された認証ベースおよびファイルベースの制限に従って、ファイルアクセスを制御します。

クライアントがファイルにアクセスするためにストレージシステムに接続するとき、ONTAP は 2 つのタスクを実行する必要があります。

- 認証

ONTAP は、信頼できるソースで ID を検証して、クライアントを認証する必要があります。また、クライアントの認証タイプは、エクスポートポリシーの設定時にクライアントがデータにアクセスできるかどうかの判断に使用できる方法の 1 つです（CIFS の場合は省略可能）。

- 承認

ONTAP は、ユーザのクレデンシャルとファイルまたはディレクトリに設定されている権限を比較し、提供するアクセスのタイプ（ある場合）を判別することで、ユーザを許可する必要があります。

ファイルアクセス制御を適切に管理するため、ONTAP は、NIS、LDAP、および Active Directory サーバなどの外部サービスと通信します。CIFS または NFS を使用するストレージシステムのファイルアクセスを設定するには、ONTAP の環境に応じて、サービスを適切に設定する必要があります。

### 認証ベースの制限

認証ベースの制限を使用すると、Storage Virtual Machine（SVM）に接続できるクライアントマシンおよびユーザを指定できます。

ONTAP は、UNIX サーバおよび Windows サーバの両方からの Kerberos 認証をサポートします。

### ファイルベースの制限

ONTAP では、3 つのレベルのセキュリティを評価して、SVM 上にあるファイルおよびディレクトリに対して要求された処理を実行する権限がエンティティにあるかどうかを判断します。アクセスは、3 つのセキュリティレベルの評価後に有効な権限によって判断されます。

どのストレージオブジェクトにも、最大 3 種類のセキュリティレイヤを含めることができます。

- エクスポート（NFS）および共有（SMB）セキュリティ

指定された NFS エクスポートまたは SMB 共有へのエクスポートおよび共有セキュリティ環境クライアントアクセス管理者権限を持つユーザは、SMB クライアントと NFS クライアントからエクスポートおよび共有レベルのセキュリティを管理できます。

- ストレージレベルのアクセス保護のファイルおよびディレクトリセキュリティ

ストレージレベルのアクセス保護セキュリティ環境 SVM ボリュームへの SMB および NFS クライアントアクセス NTFS のアクセス権のみがサポートされています。ONTAP で、ストレージレベルのアクセス保護が適用されているボリューム上のデータにアクセスする UNIX ユーザのセキュリティチェックを行うには、UNIX ユーザがボリュームを所有する SVM 上の Windows ユーザにマッピングされている必要があります。



NFS または SMB クライアントからファイルまたはディレクトリのセキュリティ設定を表示した場合、ストレージレベルのアクセス保護セキュリティは表示されません。システム（Windows または UNIX）管理者であっても、ストレージレベルのアクセス保護セキュリティをクライアントから取り消すことはできません。

- NTFS、UNIX、および NFSv4 のネイティブのファイルレベルのセキュリティ

ストレージオブジェクトを表すファイルやディレクトリには、ネイティブのファイルレベルのセキュリティが存在します。ファイルレベルのセキュリティはクライアントから設定できます。ファイル権限は、データへのアクセスに SMB と NFS のどちらを使用するかに関係なく有効です。

## ONTAPによるNFSクライアント認証の処理

### ONTAP による NFS クライアント認証の処理の概要

NFS クライアントから SVM 上のデータにアクセスするためには、NFS クライアントが正しく認証されている必要があります。ONTAP では、UNIX クレデンシャルを設定されたネームサービスに照らしてチェックすることで、そのクライアントを認証します。

NFS クライアントが SVM に接続すると、ONTAP は、SVM のネームサービス設定に応じて複数のネームサービスをチェックし、そのユーザの UNIX クレデンシャルを取得します。ONTAP でチェックできるのは、ローカルの UNIX アカウント、NIS ドメイン、および LDAP ドメインのクレデンシャルです。ONTAP がユーザを認証できるように、このうちの少なくとも 1 つを設定しておく必要があります。複数 ONTAP のネームサービスと検索順序を指定できます。

UNIX のボリュームセキュリティ形式のみを使用する NFS 環境の場合、この設定だけで NFS クライアントから接続するユーザが認証され、適切なファイルアクセスが提供されます。

mixed、NTFS、またはunifiedのボリュームセキュリティ形式を使用している場合、ONTAPがUNIXユーザをWindowsドメインコントローラで認証するためにはSMBユーザ名を取得する必要があります。これには、ローカルのUNIXアカウントまたはLDAPドメインを使用して個々のユーザをマッピングするか、代わりにデフォルトのSMBユーザを使用します。ONTAPが検索するネームサービスの種類と検索順序を指定することも、デフォルトのSMBユーザを指定することもできます。

ONTAP は、ネームサービスを使用してユーザおよびクライアントに関する情報を取得します。ONTAP は、ストレージシステム上でデータにアクセスしたりストレージシステムを管理したりするユーザの認証や、混在環境でのユーザクレデンシャルのマッピングを行うために、この情報を使用します。

ストレージシステムを設定するときに、ONTAP が認証用のユーザクレデンシャルを取得するために使用するネームサービスを指定する必要があります。ONTAP では、次のネームサービスをサポートしています。

- ローカルユーザ（ファイル）
- 外部 NIS ドメイン（NIS）
- 外部LDAPドメイン（LDAP）

を使用します `vserver services name-service ns-switch` ネットワーク情報を検索するソースとソースの検索順序をSVMに設定するコマンドファミリー。これらのコマンドは、と同等の機能を提供します `/etc/nsswitch.conf` UNIXシステム上のファイル。

NFS クライアントが SVM に接続すると、ONTAP は指定されたネームサービスをチェックして、ユーザの UNIX クレデンシャルを取得します。ネームサービスが正しく設定されていて ONTAP が UNIX クレデンシャルを取得できる場合、ONTAP はユーザの認証に成功します。

mixed セキュリティ形式の環境では、ONTAP によるユーザクレデンシャルのマッピングが必要になる場合があります。ONTAP がユーザクレデンシャルを適切にマッピングできるようにするには、環境のネームサービスを適切に設定する必要があります。

ONTAP は、SVM 管理者アカウントの認証にもネームサービスを使用します。ネームサービススイッチを設定または変更する際にはこの点を念頭に置いて、SVM 管理者アカウントの認証を誤って無効にしないようにする必要があります。SVM管理ユーザの詳細については、[を参照してください "管理者認証と RBAC"](#)。

### ONTAP による NFS クライアントからの SMB ファイルアクセスの許可方法

ONTAP では、NTFS（Windows NT ファイルシステム）のセキュリティセマンティクスを利用して、NTFS アクセス権によるファイルへのアクセス権が、NFS クライアント上の UNIX ユーザにあるかどうかを判別されます。

ONTAP では、ユーザの UNIX User ID（UID；UNIX ユーザ ID）から変換された SMB クレデンシャルを使用して、ファイルに対するユーザのアクセス権の有無が確認されます。SMB クレデンシャルは、通常はユーザの Windows ユーザ名であるプライマリ Security Identifier（SID；セキュリティ識別子）と、ユーザがメンバーとなっている Windows グループに対応する 1 つ以上のグループ SID で構成されています。

ONTAP で UNIX UID を SMB クレデンシャルへ変換するときに要する時間は、数十ミリ秒から数百ミリ秒です。これは、この変換処理にドメインコントローラへの問い合わせも含まれるためです。ONTAP は UID を SMB クレデンシャルにマッピングします。このマッピングはクレデンシャルキャッシュ内に入力されるので、変換によって発生する検証時間が短縮されます。

### NFS クレデンシャルキャッシュの仕組み

NFS ユーザがストレージシステム上の NFS エクスポートへのアクセスを要求すると、ONTAP は、ユーザの認証を行うために外部ネームサーバまたはローカルファイルからユ

ーザクレデンシャルを取得する必要があります。その後、ONTAP は、以降の参照用にこれらのクレデンシャルを内部のクレデンシャルキャッシュに格納します。NFS クレデンシャルキャッシュの仕組みを理解しておく、パフォーマンスおよびアクセスに関する潜在的な問題に対処できます。

クレデンシャルキャッシュがないと、ONTAP ユーザは NFS ユーザからアクセスが要求されるたびにネームサービスを照会しなければなりません。多数のユーザがアクセスする使用頻度の高いストレージシステムでは、こうした状況がすぐに深刻なパフォーマンス上の問題につながり、不必要な遅延や、場合によっては NFS クライアントアクセスの拒否さえ引き起こす可能性があります。

クレデンシャルキャッシュがあれば、ONTAP は取得したユーザクレデンシャルをあらかじめ決められた期間だけ格納しておき、同じ NFS クライアントから再び要求があっても迅速かつ簡単にアクセスすることができます。この方法には、次の利点があります。

- 外部ネームサーバ（NIS や LDAP など）への要求の処理を減らすことで、ストレージシステムの負荷が軽減されます。
- 外部ネームサーバに送信する要求を減らすことで、外部ネームサーバの負荷が軽減されます。
- ユーザの認証を行う前に外部ソースからクレデンシャルを取得するための待ち時間をなくすることで、ユーザアクセスが高速になります。

ONTAP は、受理されたクレデンシャルと拒否されたクレデンシャルの両方をクレデン受理されたクレデンシャルとは、ユーザが認証されてアクセス権を付与されたこと拒否されたクレデンシャルとは、ユーザが認証されずにアクセスが拒否されたことを意味します

デフォルトでは、ONTAP は受理されたクレデンシャルを 24 時間保存します。つまり、ユーザの最初の認証から 24 時間は、そのユーザからのすべてのアクセス要求で ONTAP はキャッシュされたクレデンシャルを使用します。24 時間後にそのユーザからアクセスが要求された場合は、最初からやり直しになります。ONTAP はキャッシュされたクレデンシャルを破棄し、適切なネームサービスソースから再びクレデンシャルを取得します。それまでの 24 時間にネームサーバ上でクレデンシャルが変更された場合、ONTAP は、次の 24 時間での使用に備えて、更新されたクレデンシャルをキャッシュします。

デフォルトでは、ONTAP は拒否されたクレデンシャルを 2 時間保存します。つまり、ユーザに対する最初のアクセス拒否から 2 時間は、そのユーザからのすべてのアクセス要求を ONTAP は拒否し続けます。2 時間後にそのユーザからアクセスが要求された場合は、最初からやり直しになります。ONTAP は適切なネームサービスソースから再びクレデンシャルを取得します。それまでの 2 時間にネームサーバ上でクレデンシャルが変更された場合、ONTAP は、次の 2 時間での使用に備えて、更新されたクレデンシャルをキャッシュします。

## **NAS** ネームスペース内でデータボリュームを作成および管理します

ジャンクションポイントを指定してデータボリュームを作成します

ジャンクションポイントはデータボリュームの作成時に指定できます。作成したボリュームは、ジャンクションポイントに自動的にマウントされ、NAS アクセス用の設定にすぐに使用できます。

作業を開始する前に

- ボリュームを作成するアグリゲートがすでに存在している必要があります。
- ONTAP 9.13.1以降では、容量分析とアクティビティ追跡を有効にしてボリュームを作成できます。容量またはアクティビティトラッキングを有効にするには、を問題します volume create コマンドにを指定



します `-analytics-state` または `-activity-tracking-state` をに設定します `on`。

容量分析とアクティビティ追跡の詳細については、を参照してください [File System Analytics](#) を有効にします。



ジャンクションパスに次の文字を使用することはできません。 `*#<>|?\`

[+]

また、ジャンクションパスの長さは 255 文字以下にする必要があります。

#### 手順

1. ジャンクションポイントを指定してボリュームを作成します。

```
volume create -vserver vsilver_name -volume volume_name -aggregate
aggregate_name -size {integer[KB|MB|GB|TB|PB]} -security-style
{ntfs|unix|mixed} -junction-path junction_path
```

ジャンクションパスはルート (`/`) で始まる必要があり、ディレクトリおよび結合されたボリュームを含むことができます。ジャンクションパスにボリュームの名前を含める必要はありません。ジャンクションパスはボリューム名に依存しません。

ボリュームのセキュリティ形式の指定は任意です。セキュリティ形式を指定しない場合、ONTAP は、Storage Virtual Machine (SVM) のルートボリュームに適用されている形式と同じセキュリティ形式を使用してボリュームを作成します。ただし、ルートボリュームのセキュリティ形式が、作成するデータボリュームには適切でないセキュリティ形式である場合もあります。トラブルシューティングが困難なファイルアクセスの問題を最小限に抑えるため、ボリュームの作成時にセキュリティ形式を指定することを推奨します。

ジャンクションパスでは大文字と小文字が区別されません。 `/ENG` はと同じです `/eng`。CIFS 共有を作成する場合、Windows では、ジャンクションパスがあたかも大文字と小文字の区別があるかのように扱われます。たとえば、ジャンクションがの場合などです `/ENG`SMB共有のパスはで始まる必要があります`/ENG`ではありません`/eng`。

データボリュームのカスタマイズに使用できるオプションのパラメータが多数用意されています。これらの機能の詳細については、のマニュアルページを参照してください `volume create` コマンドを実行します

2. 目的のジャンクションポイントでボリュームが作成されたことを確認します。

```
volume show -vserver vsilver_name -volume volume_name -junction
```

#### 例

次の例は、ジャンクションパスがである「home4」という名前のボリュームをSVM vs1上に作成します `/eng/home` :

```
cluster1::> volume create -vserver vs1 -volume home4 -aggregate aggr1
-size 1g -junction-path /eng/home
[Job 1642] Job succeeded: Successful
```

```
cluster1::> volume show -vserver vs1 -volume home4 -junction
```

Vserver	Volume	Active	Junction Path	Junction Path Source
vs1	home4	true	/eng/home	RW_volume

ジャンクションポイントを指定せずにデータボリュームを作成

ジャンクションポイントを指定せずにデータボリュームを作成できます。作成したボリュームは自動的にマウントされず、NAS アクセス用の設定に使用することはできません。ボリュームの SMB 共有または NFS エクスポートを設定する前に、ボリュームをマウントする必要があります。

作業を開始する前に

- ボリュームを作成するアグリゲートがすでに存在する必要があります。
- ONTAP 9.13.1以降では、容量分析とアクティビティ追跡を有効にしてボリュームを作成できます。容量またはアクティビティトラッキングを有効にするには、`volume create` コマンドに `-analytics-state` または `-activity-tracking-state` を指定します `on`。

容量分析とアクティビティ追跡の詳細については、[を参照してください](#) [File System Analytics](#) を有効にします。

手順

1. 次のコマンドを使用して、ジャンクションポイントが設定されていないボリュームを作成します。

```
volume create -vserver vserver_name -volume volume_name -aggregate
aggregate_name -size {integer[KB|MB|GB|TB|PB]} -security-style
{ntfs|unix|mixed}
```

ボリュームのセキュリティ形式の指定は任意です。セキュリティ形式を指定しない場合、ONTAP は、Storage Virtual Machine (SVM) のルートボリュームに適用されている形式と同じセキュリティ形式を使用してボリュームを作成します。ただし、ルートボリュームのセキュリティ形式が、データボリュームには適切でないセキュリティ形式である場合もあります。トラブルシューティングが困難なファイルアクセスの問題を最小限に抑えるため、ボリュームの作成時にセキュリティ形式を指定することを推奨します。

データボリュームのカスタマイズに使用できるオプションのパラメータが多数用意されています。これらの機能の詳細については、[のマニュアルページを参照してください](#) `volume create` コマンドを実行します

2. ジャンクションポイントが設定されていないボリュームが作成されたことを確認します。

```
volume show -vserver vserver_name -volume volume_name -junction
```



## 例

次の例は、ジャンクションポイントにマウントされない「sales」という名前のボリュームを SVM vs1 上に作成します。

```
cluster1::> volume create -vserver vs1 -volume sales -aggregate aggr3
-size 20GB
[Job 3406] Job succeeded: Successful
```

```
cluster1::> volume show -vserver vs1 -junction
```

Vserver	Volume	Junction		Junction
		Active	Junction Path	Path Source
vs1	data	true	/data	RW_volume
vs1	home4	true	/eng/home	RW_volume
vs1	vs1_root	-	/	-
vs1	sales	-	-	-

**NAS** ネームスペース内の既存のボリュームをマウントまたはアンマウントします

Storage Virtual Machine (SVM) ボリュームに格納されたデータへの NAS クライアントアクセスを設定するには、ボリュームが NAS ネームスペースにマウントされている必要があります。現在マウントされていないボリュームは、ジャンクションポイントにマウントできます。ボリュームはアンマウントすることもできます。

このタスクについて

ボリュームをアンマウントしてオフラインにすると、アンマウントしたボリュームのネームスペース内に含まれていたジャンクションポイントのあるボリューム内のデータも含め、ジャンクションポイント内のすべてのデータに NAS クライアントからアクセスできなくなります。



NAS クライアントからのボリュームへのアクセスを中止するには、ボリュームを単純にアンマウントするだけでは不十分です。ボリュームをオフラインにするか、クライアント側のファイルハンドルキャッシュを確実に無効にするためのその他の手順を実行する必要があります。詳細については、次の技術情報アートを参照してください。

["ONTAP のネームスペースから NFSv3 クライアントを削除しても、ボリュームにアクセスできるようになります"](#)

ボリュームをアンマウントしてオフラインにしても、そのボリューム内のデータは失われません。また、既存のボリュームエクスポートポリシーおよびボリュームまたはディレクトリ上に作成された SMB 共有、およびアンマウントされたボリューム内のジャンクションポイントは保持されます。アンマウントしたボリュームを再マウントすれば、NAS クライアントは既存のエクスポートポリシーと SMB 共有を使用してボリューム内のデータにアクセスできるようになります。

## 手順

1. 必要な操作を実行します。

状況	入力するコマンド
ボリュームをマウント	<code>volume mount -vserver <i>svm_name</i> -volume <i>volume_name</i> -junction-path <i>junction_path</i></code>
ボリュームをアンマウントします	<code>volume unmount -vserver <i>svm_name</i> -volume <i>volume_name</i></code>  <code>volume offline -vserver <i>svm_name</i> -volume <i>volume_name</i></code>

2. ボリュームが目的のマウント状態になっていることを確認します。

```
volume show -vserver svm_name -volume volume_name -fields state,junction-
path,junction-active
```

例

次の例は、SVM「vs1」にある「sales」という名前のボリュームをジャンクションポイント「/sales」にマウントします。

```
cluster1::> volume mount -vserver vs1 -volume sales -junction-path /sales

cluster1::> volume show -vserver vs1 state,junction-path,junction-active
```

vserver	volume	state	junction-path	junction-active
vs1	data	online	/data	true
vs1	home4	online	/eng/home	true
vs1	sales	online	/sales	true

次の例は、SVM「vs1」にある「data」という名前のボリュームをアンマウントしてオフラインにします。

```
cluster1::> volume unmount -vserver vs1 -volume data
cluster1::> volume offline -vserver vs1 -volume data

cluster1::> volume show -vserver vs1 -fields state,junction-path,junction-
active
```

vserver	volume	state	junction-path	junction-active
vs1	data	offline	-	-
vs1	home4	online	/eng/home	true
vs1	sales	online	/sales	true

ボリュームマウントポイントとジャンクションポイントに関する情報を表示します

Storage Virtual Machine（SVM）のマウントボリューム、およびボリュームがマウントされているジャンクションポイントに関する情報を表示できます。また、ジャンクションポイントにマウントされていないボリュームを確認することもできます。この情報を使用して、SVM ネームスペースを理解し、管理することができます。

ステップ

- 1. 必要な操作を実行します。

表示する項目	入力するコマンド
SVM のマウントされたボリュームとマウントされていないボリュームに関する概要情報	<code>volume show -vserver vs1 -junction</code>
SVM のマウントされたボリュームとマウントされていないボリュームに関する詳細情報	<code>volume show -vserver vs1 -volume volume_name -instance</code>
SVM のマウントされたボリュームとマウントされていないボリュームに関する特定の情報	<div>a. 必要に応じて、の有効なフィールドを表示できます <code>-fields</code> パラメータを指定するには、次のコマンドを使用します。 <code>volume show -fields ?</code></div> <div>b. を使用して、必要な情報を表示します <code>-fields</code> パラメータ： <code>volume show -vserver vs1 -fields fieldname,...</code></div>

例

次の例は、SVM vs1 のマウントされたボリュームとマウントされていないボリュームの概要を表示します。

```
cluster1::> volume show -vserver vs1 -junction
```

Vserver	Volume	Active	Junction Path	Junction Path Source
vs1	data	true	/data	RW_volume
vs1	home4	true	/eng/home	RW_volume
vs1	vs1_root	-	/	-
vs1	sales	true	/sales	RW_volume

次の例は、SVM vs2 上に配置されたボリュームの指定したフィールドに関する情報を表示します。

```
cluster1::> volume show -vserver vs2 -fields
vserver,volume,aggregate,size,state,type,security-style,junction-
path,junction-parent,node
vserver volume    aggregate size state  type security-style junction-path
junction-parent node
-----
vs2      data1      aggr3    2GB  online RW    unix      -          -
node3
vs2      data2      aggr3    1GB  online RW    ntfs      /data2
vs2_root node3
vs2      data2_1    aggr3    8GB  online RW    ntfs      /data2/d2_1
data2    node3
vs2      data2_2    aggr3    8GB  online RW    ntfs      /data2/d2_2
data2    node3
vs2      pubs      aggr1    1GB  online RW    unix      /publications
vs2_root node1
vs2      images    aggr3    2TB  online RW    ntfs      /images
vs2_root node3
vs2      logs      aggr1    1GB  online RW    unix      /logs
vs2_root node1
vs2      vs2_root aggr3    1GB  online RW    ntfs      /          -
node3
```

## セキュリティ形式を設定する

### セキュリティ形式がデータアクセスに与える影響

セキュリティ形式とその影響とは

セキュリティ形式には、UNIX、NTFS、mixed、および unified の 4 種類があり、セキュリティ形式ごとにデータに対する権限の処理方法が異なります。目的に応じて適切なセキュリティ形式を選択できるように、それぞれの影響について理解しておく必要があります。

セキュリティ形式はデータにアクセスできるクライアントの種類には影響しないことに注意してください。セキュリティ形式で決まるのは、データアクセスの制御に ONTAP で使用される権限の種類と、それらの権限を変更できるクライアントの種類だけです。

たとえば、ボリュームで UNIX セキュリティ形式を使用している場合でも、ONTAP はマルチプロトコルに対応しているため、SMB クライアントから引き続きデータにアクセスできます（認証と許可が適切な場合）。ただし、ONTAP では、UNIX クライアントのみが標準のツールを使用して変更できる UNIX 権限が使用されます。

セキュリティ形式	権限を変更できるクライアント	クライアントが使用できる権限	有効になるセキュリティ形式	ファイルにアクセスできるクライアント
「UNIX」	NFS	NFSv3 モードビット NFSv4.x ACL	「UNIX」	NFS と SMB
NTFS	SMB	NTFS ACL	NTFS	
混在	NFS または SMB	NFSv3 モードビット NFSv4.x ACL	「UNIX」	
		NTFS ACL	NTFS	
統合： (ONTAP 9.4以前のリリースでは、Infinite Volumeのみ)。	NFS または SMB	NFSv3 モードビット NFSv4.1 ACL	「UNIX」	
		NTFS ACL	NTFS	

FlexVol ボリュームでは、UNIX、NTFS、および mixed のセキュリティ形式がサポートされます。セキュリティ形式が mixed または unified の場合は、ユーザがセキュリティ形式を各自設定するため、権限を最後に変更したクライアントの種類によって有効になる権限が異なります。権限を最後に変更したクライアントが NFSv3 クライアントの場合、権限は UNIX NFSv3 モードビットになります。最後のクライアントが NFSv4 クライアントの場合、権限は NFSv4 ACL になります。最後のクライアントが SMB クライアントの場合、権限は Windows NTFS ACL になります。

unified セキュリティ形式は、Infinite Volume でのみ使用できます。Infinite Volume は、ONTAP 9.5 以降のリリースではサポートされなくなりました。詳細については、[を参照してください FlexGroup ボリュームの管理の概要](#)。

ONTAP 9.2以降では、show-effective-permissions パラメータをに設定します vservers security file-directory コマンドを使用すると、指定したファイルまたはフォルダパスに対してWindowsユーザまたはUNIXユーザに付与されている有効な権限を表示できます。また、オプションのパラメータも指定します -share-name 有効な共有権限を表示できます。



ONTAP で、最初にデフォルトのファイル権限がいくつか設定されます。デフォルトでは、UNIX、mixed、および unified のセキュリティ形式のボリュームにあるデータについては、セキュリティ形式は UNIX、権限の種類は UNIX モードビット（特に指定しないかぎり 0755）が有効になります。これは、デフォルトのセキュリティ形式で許可されたクライアントで設定するまで変わりません。NTFS セキュリティ形式のボリュームにあるデータについては、デフォルトで NTFS セキュリティ形式が有効になり、すべてのユーザにフルコントロール権限を許可する ACL が割り当てられます。

セキュリティ形式を設定する場所とタイミング

セキュリティ形式は、FlexVol（ルートボリュームとデータボリュームの両方）および qtrees で設定できます。セキュリティ形式は、作成時に手動で設定することも、自動的に継承することも、あとで変更することもできます。

**SVM** で使用するセキュリティ形式を決定します

ボリュームで使用するセキュリティ形式を決定するには、2つの要素を考慮する必要があります

あります。第 1 の要素は、ファイルシステムを管理する管理者のタイプです。第 2 の要素は、ボリューム上のデータにアクセスするユーザまたはサービスのタイプです。

ボリュームのセキュリティ形式を設定するときは、最適なセキュリティ形式を選択して権限の管理に関する問題を回避するために、環境のニーズを考慮する必要があります。決定時には次の点を考慮すると役立ちます。

セキュリティ形式	以下の場合に選択
「UNIX」	<ul style="list-style-type: none"><li>• ファイルシステムが UNIX 管理者によって管理される。</li><li>• ユーザの大半が NFS クライアントである。</li><li>• データにアクセスするアプリケーションで、サービスアカウントとして UNIX ユーザが使用される。</li></ul>
NTFS	<ul style="list-style-type: none"><li>• ファイルシステムは Windows 管理者によって管理されます。</li><li>• ユーザの大部分が SMB クライアントです。</li><li>• データにアクセスするアプリケーションで、サービスアカウントとして Windows ユーザが使用される。</li></ul>
混在	<ul style="list-style-type: none"><li>• ファイルシステムが UNIX 管理者と Windows 管理者の両方によって管理され、ユーザが NFS クライアントと SMB クライアントの両方で構成される。</li></ul>

#### セキュリティ形式の継承の仕組み

新しい FlexVol または qtree の作成時にセキュリティ形式を指定しない場合、セキュリティ形式はさまざまな方法で継承されます。

セキュリティ形式は、次のように継承されます。

- FlexVol ボリュームは、そのボリュームを含む SVM のルートボリュームのセキュリティ形式を継承します。
- qtree は、その qtree を含む FlexVol ボリュームのセキュリティ形式を継承します。
- ファイルまたはディレクトリは、そのファイルまたはディレクトリを含む FlexVol ボリュームまたは qtree のセキュリティ形式を継承します。

#### ONTAP による UNIX アクセス権の維持方法

UNIX アクセス権を現在持っている FlexVol ボリューム内のファイルが Windows アプリケーションによって編集および保存されても、ONTAP は UNIX アクセス権を維持できます。

Windows クライアントのアプリケーションは、ファイルを編集して保存するときに、ファイルのセキュリティプロパティを読み取り、新しい一時ファイルを作成し、それらのプロパティを一時ファイルに適用してから、一時ファイルに元のファイル名を付けます。

セキュリティプロパティのクエリを実行すると、Windows クライアントは、UNIX アクセス権を正確に表す構築済み ACL を受け取ります。この構築済み ACL は、Windows アプリケーションによってファイルが更新されるときにファイルの UNIX アクセス権を維持し、生成されたファイルが同じ UNIX アクセス権を持つよう

にするためだけに使用されます。ONTAP は、構築済み ACL を使用して NTFS ACL を設定しません。

**Windows** のセキュリティタブを使用して **UNIX** アクセス権を管理します

SVM 上の mixed セキュリティ形式のボリリュームまたは qtree に含まれるファイルまたはフォルダの UNIX アクセス権を操作する場合は、Windows クライアントのセキュリティタブを使用できます。また、Windows ACL を照会および設定できるアプリケーションを使用することもできます。

- UNIX アクセス権の変更

Windows のセキュリティタブを使用して、mixed セキュリティ形式のボリリュームまたは qtree の UNIX アクセス権を表示および変更できます。メインの [Windows Security] タブを使用して UNIX アクセス権を変更する場合は、編集する既存の ACE を削除してから（モードビットを 0 に設定）、変更を行う必要があります。または、高度なエディタを使用して権限を変更することもできます。

モードのアクセス権を使用している場合は、リストされた UID、GID、およびその他（コンピュータにアカウントを持つその他すべてのユーザ）のモードアクセス権を直接変更できます。たとえば、表示された UID に r-x のアクセス権が設定されている場合、この UID のアクセス権を rwx に変更できます。

- UNIX アクセス権を NTFS アクセス権に変更しています

Windows のセキュリティタブを使用して、ファイルおよびフォルダのセキュリティ形式が UNIX 対応である mixed 型セキュリティ形式のボリリュームまたは qtree 上で、UNIX セキュリティオブジェクトを Windows セキュリティオブジェクトに置き換えることができます。

適切な Windows のユーザおよびグループのオブジェクトに置き換える前に、リストされている UNIX アクセス権のエントリをすべて削除しておく必要があります。次に、Windows のユーザおよびグループのオブジェクトに NTFS ベースの ACL を設定します。すべての UNIX セキュリティオブジェクトを削除し、Windows のユーザおよびグループのみを mixed セキュリティ形式のボリリュームまたは qtree 上のファイルまたはフォルダに追加すると、ファイルまたはフォルダのセキュリティ形式が UNIX から NTFS へ変換されます。

フォルダの権限を変更する場合、Windows のデフォルトの動作では、すべてのサブフォルダとファイルにこれらの変更が反映されます。したがって、セキュリティ形式の変更をすべての子フォルダ、サブフォルダ、およびファイルに反映したくない場合は、反映する範囲を希望の範囲に変更する必要があります。

## **SVM** ルートボリリュームのセキュリティ形式を設定する

Storage Virtual Machine（SVM）のルートボリリューム上のデータに使用するアクセス権のタイプを決定するには、SVM ルートボリリュームのセキュリティ形式を設定します。

### 手順

1. を使用します `vserver create` コマンドにを指定します `-rootvolume-security-style` セキュリティ形式を定義するパラメータ。

ルートボリリュームのセキュリティ形式に指定できるオプションは、です `unix`、`ntfs` または `mixed`。

2. 作成した SVM のルートボリリュームセキュリティ形式を含む設定を表示して確認します。

```
vserver show -vserver vserver_name
```

**FlexVol** ボリュームのセキュリティ形式を設定する

Storage Virtual Machine（SVM）の FlexVol 上のデータに使用するアクセス権のタイプを決定するには、FlexVol のセキュリティ形式を設定します。

手順

1. 次のいずれかを実行します。

FlexVol ボリュームの状況	使用するコマンド
はまだ存在しません	<code>volume create</code> を含めます <code>-security-style</code> セキュリティ形式を指定するパラメータ。
はすでに存在します	<code>volume modify</code> を含めます <code>-security-style</code> セキュリティ形式を指定するパラメータ。

FlexVol のセキュリティ形式に指定できるオプションは、です `unix`、`ntfs` または `mixed`。

FlexVol ボリュームの作成時にセキュリティ形式を指定しない場合、ボリュームはルートボリュームのセキュリティ形式を継承します。

詳細については、を参照してください `volume create` または `volume modify` コマンド、を参照してください ["論理ストレージ管理"](#)。

2. 作成した FlexVol ボリュームのセキュリティ形式を含む設定を表示するには、次のコマンドを入力します。

```
volume show -volume volume_name -instance
```

**qtree** にセキュリティ形式を設定する

qtree 上のデータに使用するアクセス権のタイプを決定するには、qtree のセキュリティ形式を設定します。

手順

1. 次のいずれかを実行します。

qtree の有無	使用するコマンド
はまだ存在しません	<code>volume qtree create</code> を含めます <code>-security-style</code> セキュリティ形式を指定するパラメータ。
はすでに存在します	<code>volume qtree modify</code> を含めます <code>-security-style</code> セキュリティ形式を指定するパラメータ。

qtreeセキュリティ形式に指定できるオプションは、です `unix`、`ntfs` または `mixed`。

qtreeの作成時にセキュリティ形式を指定しない場合、デフォルトのセキュリティ形式はです `mixed`。



詳細については、を参照してください `volume qtree create` または `volume qtree modify` コマンド、を参照してください "[論理ストレージ管理](#)"。

2. 作成したqtreeのセキュリティ形式を含む設定を表示するには、次のコマンドを入力します。 `volume qtree show -qtree qtree_name -instance`

## NFSを使用したファイルアクセスの設定

### NFS の概要を使用したファイルアクセスのセットアップ

クライアントが NFS を使用して Storage Virtual Machine （ SVM ） 上のファイルにアクセスできるようにするには、いくつかの手順を実行する必要があります。環境の現在の設定によっては、さらにいくつかの手順を実行することもできます。

クライアントが NFS を使用して SVM のファイルにアクセスできるようにするには、次の作業を行う必要があります。

1. SVM で NFS プロトコルを有効にします。

クライアントからの NFS 経由のデータアクセスを許可するように SVM を設定する必要があります。

2. SVM に NFS サーバを作成します。

NFS サーバは、 NFS 経由のファイル提供を可能にする SVM 上の論理エンティティです。NFS サーバを作成し、許可する NFS プロトコルのバージョンを指定する必要があります。

3. SVM でエクスポートポリシーを設定します。

クライアントがボリュームと qtree を使用できるようにするには、エクスポートポリシーを設定する必要があります。

4. ネットワークおよびストレージの環境に応じて、適切なセキュリティおよびその他の設定を使用して NFS サーバを設定します。

この手順には、Kerberos 、 LDAP 、 NIS 、 ネームマッピング、ローカルユーザの設定が含まれます。

### エクスポートポリシーを使用して **NFS** アクセスを保護

エクスポートポリシーがボリュームまたは **qtree** へのクライアントアクセスを制御する仕組み

エクスポートポリシーには、各クライアントアクセス要求を処理する 1 つ以上の `_ エクスポートルール _` が含まれています。このプロセスの結果、クライアントアクセスを許可するかどうか、およびアクセスのレベルが決まります。クライアントがデータにアクセスするためには、エクスポートルールを含むエクスポートポリシーが Storage Virtual Machine （ SVM ） 上に存在する必要があります。

ボリュームまたは qtree へのクライアントアクセスを設定するには、各ボリュームまたは qtree にポリシーを 1 つ関連付けます。SVM には複数のエクスポートポリシーを含めることができます。これにより、複数のボリュームまたは qtree を含む SVM に対して次の操作を実行できます。

- SVM のボリュームまたは qtree ごとに異なるエクスポートポリシーを割り当て、SVM の各ボリュームまたは qtree へのクライアントアクセスを個別に制御する。
- SVM の複数のボリュームまたは qtree に同じエクスポートポリシーを割り当て、同一のクライアントアクセス制御を実行する。ボリュームまたは qtree ごとに新しいエクスポートポリシーを作成する必要はありません。

クライアントが適用可能なエクスポートポリシーで許可されていないアクセス要求を行うと、権限拒否のメッセージが表示され、その要求は失敗します。クライアントがエクスポートポリシーのどのルールにも一致しない場合、アクセスは拒否されます。エクスポートポリシーが空の場合は、すべてのアクセスが暗黙的に拒否されます。

エクスポートポリシーは、ONTAP を実行しているシステム上で動的に変更できます。

#### SVM のデフォルトのエクスポートポリシー

各 SVM には、ルールが含まれていないデフォルトのエクスポートポリシーが用意されています。SVM 上のデータにクライアントからアクセスできるようにするには、ルールを備えたエクスポートポリシーを用意する必要があります。SVM 内の各 FlexVol にエクスポートポリシーを関連付ける必要があります。

SVMを作成すると、という名前のデフォルトのエクスポートポリシーがストレージシステムによって自動的に作成されます default SVMのルートボリュームに対して実行します。SVM 上のデータにクライアントからアクセスできるようにするには、デフォルトのエクスポートポリシーのルールを 1 つ以上作成する必要があります。または、ルールを備えたカスタムのエクスポートポリシーを作成することもできます。デフォルトのエクスポートポリシーは、変更および名前変更は可能ですが、削除することはできません。

SVM 内に FlexVol ボリュームを作成すると、作成されたボリュームには、SVM のルートボリュームのデフォルトのエクスポートポリシーが関連付けられます。デフォルトでは、SVM に作成した各ボリュームには、ルートボリュームのデフォルトのエクスポートポリシーが関連付けられます。SVM 内のすべてのボリュームでデフォルトのエクスポートポリシーを使用することも、ボリュームごとに独自のエクスポートポリシーを作成することもできます。複数のボリュームを同じエクスポートポリシーに関連付けることができます。

#### エクスポートルールの仕組み

エクスポートルールは、エクスポートポリシーの機能要素です。エクスポートルールでは、ボリュームへのクライアントアクセス要求が設定済みの特定のパラメータと照合され、クライアントアクセス要求の処理方法が決定されます。

エクスポートポリシーには、クライアントにアクセスを許可するエクスポートルールが少なくとも 1 つ含まれている必要があります。エクスポートポリシーに複数のルールが含まれている場合、ルールはエクスポートポリシーに表示される順に処理されます。ルールの順序は、ルールインデックス番号によって決まります。ルールがクライアントに一致すると、そのルールの権限が使用され、それ以降のルールは処理されません。一致するルールがない場合、クライアントはアクセスを拒否されます。

次の条件を使用して、クライアントのアクセス権限を決定するようにエクスポートルールを設定できます。

- クライアントが要求の送信に使用するファイルアクセスプロトコル。たとえば、NFSv4 や SMB などです。
- ホスト名や IP アドレスなどのクライアント識別子。

の最大サイズ -clientmatch フィールドは4096文字です。

- Kerberos v5、NTLM、AUTH\_SYS など、クライアントが認証に使用するセキュリティタイプ。

ルールで複数の条件が指定されている場合、クライアントがそれらのすべてに一致しないとルールは適用されません。



ONTAP 9.3 以降では、エクスポートポリシーの設定チェックをバックグラウンドジョブとして有効にし、すべてのルール違反をエラールールリストに記録することができます。。 `vserver export-policy config-checker` コマンドを実行するとチェッカーが呼び出されて結果が表示され、設定を検証したり、誤ったルールをポリシーから削除したりできます。

このコマンドで検証されるのは、エクスポート設定のホスト名、ネットグループ、匿名ユーザのみです。

例

エクスポートポリシーに、次のパラメータが指定されたエクスポートルールが含まれています。

- `-protocol nfs3`
- `-clientmatch 10.1.16.0/255.255.255.0`
- `-rorule any`
- `-rwrule any`

クライアントアクセス要求は NFSv3 プロトコルを使用して送信され、クライアントの IP アドレスは 10.1.17.37 です。

クライアントアクセスプロトコルが一致していても、クライアントの IP アドレスがエクスポートルールで指定されているアドレスとは別のサブネットに属しています。そのため、クライアントは一致なくなり、このルールはこのクライアントに適用されません。

例

エクスポートポリシーに、次のパラメータが指定されたエクスポートルールが含まれています。

- `-protocol nfs`
- `-clientmatch 10.1.16.0/255.255.255.0`
- `-rorule any`
- `-rwrule any`

クライアントアクセス要求は NFSv4 プロトコルを使用して送信され、クライアントの IP アドレスは 10.1.16.54 です。

クライアントアクセスプロトコルが一致し、クライアントの IP アドレスが指定したサブネット内にあります。そのため、クライアントは一致し、このルールはこのクライアントを環境します。セキュリティタイプに関係なく、クライアントは読み取り / 書き込みアクセス権を取得します。

例

エクスポートポリシーに、次のパラメータが指定されたエクスポートルールが含まれています。

- `-protocol nfs3`

- -clientmatch 10.1.16.0/255.255.255.0
- -rorule any
- -rwrule krb5,ntlm

クライアント #1 は、IP アドレスが 10.1.16.207 で、NFSv3 プロトコルを使用してアクセス要求を送信し、Kerberos v5 で認証されます。

クライアント #2 は、IP アドレスが 10.1.16.211 で、NFSv3 プロトコルを使用してアクセス要求を送信し、AUTH\_SYS で認証されます。

両方のクライアントで、クライアントアクセスプロトコルと IP アドレスは一致しています。読み取り専用パラメータでは、認証に使用するセキュリティタイプに関係なく、読み取り専用アクセスがすべてのクライアントに許可されています。したがって、両方のクライアントが読み取り専用アクセス権を取得します。ただし、読み取り / 書き込みアクセス権を取得するのはクライアント #1 だけです。これは、認証に承認されたセキュリティタイプ Kerberos v5 を使用したためです。クライアント #2 は読み取り / 書き込みアクセス権を取得できません。

リストにないセキュリティタイプを使用するクライアントを管理します

エクスポートルールのアクセスパラメータに指定されていないセキュリティタイプをクライアントが使用している場合は、オプションを使用して、クライアントへのアクセスを拒否するか、クライアントを匿名ユーザIDにマッピングするかを選択できます none にアクセスパラメータを指定します。

クライアントは、別のセキュリティタイプで認証されているか、まったく認証されていない（セキュリティタイプ AUTH\_NONE）場合に、アクセスパラメータで指定されていないセキュリティタイプを使用しているとみなされます。デフォルトでは、クライアントはそのレベルへのアクセスを自動的に拒否されます。ただし、オプションは追加できます none をアクセスパラメータに追加します。リストにないセキュリティ形式を使用するクライアントは、拒否されずに匿名ユーザ ID にマッピングされます。。 -anon パラメータは、これらのクライアントに割り当てるユーザIDを決定します。に指定されたユーザID -anon パラメータは、匿名ユーザに適していると思われる権限が設定されている有効なユーザである必要があります。

に有効な値 -anon パラメータの範囲はからです 0 終了： 65535。

に割り当てられたユーザID -anon	クライアントアクセス要求の処理結果
0 - 65533	クライアントアクセス要求は匿名ユーザ ID にマッピングされ、このユーザに対して設定された権限に応じてアクセスできるようになります。
65534	クライアントアクセス要求はユーザ nobody にマッピングされ、このユーザに対して設定されたアクセス権に応じてアクセスできるようになります。これがデフォルトです。

に割り当てられたユーザID -anon	クライアントアクセス要求の処理結果
65535	この ID にマッピングされていて、クライアントがセキュリティタイプ AUTH_NONE を使用している場合、クライアントからのアクセス要求は拒否されます。ユーザ ID が 0 のクライアントからのアクセス要求は、この ID にマッピングされ、他のセキュリティタイプをクライアントが使用している場合、拒否されます。

オプションを使用する場合 `none` では、最初に読み取り専用パラメータが処理されることを覚えておくことが重要です。リストにないセキュリティタイプを使用するクライアントのエクスポートルールを設定する際は、次のガイドラインを考慮してください。

読み取り専用には含まれます none	読み取り/書き込みに含まれます none	リストにないセキュリティタイプ を使用するクライアントのアクセ ス結果
いいえ	いいえ	拒否されました
いいえ	はい。	最初に読み取り専用が処理される ため、拒否されました
はい。	いいえ	匿名として読み取り専用です
はい。	はい。	匿名として読み書き可能です

#### 例

エクスポートポリシーに、次のパラメータが指定されたエクスポートルールが含まれています。

- `-protocol nfs3`
- `-clientmatch 10.1.16.0/255.255.255.0`
- `-rorule sys,none`
- `-rwrule any`
- `-anon 70`

クライアント #1 は、IP アドレスが 10.1.16.207 で、NFSv3 プロトコルを使用してアクセス要求を送信し、Kerberos v5 で認証されます。

クライアント #2 は、IP アドレスが 10.1.16.211 で、NFSv3 プロトコルを使用してアクセス要求を送信し、AUTH\_SYS で認証されます。

クライアント #3 は、IP アドレスが 10.1.16.234 で、NFSv3 プロトコルを使用してアクセス要求を送信し、認証は行われていません（セキュリティタイプ AUTH\_NONE）。

3 つすべてのクライアントで、クライアントアクセスプロトコルと IP アドレスは一致しています。読み取り専用パラメータでは、読み取り専用アクセスが、AUTH\_SYS で認証された、自身のユーザ ID を持つクライアントに許可されています。読み取り専用パラメータでは、ユーザ ID が 70 の匿名ユーザとしての読み取り

専用アクセスが、他のセキュリティタイプを使用して認証されたクライアントに許可されています。読み取り / 書き込みパラメータでは、読み取り / 書き込みアクセスがすべてのセキュリティタイプに許可されていますが、この場合は、読み取り専用ルールですでにフィルタされている環境クライアントのみが許可されます。

したがって、クライアント #1 とクライアント #3 は、ユーザ ID が 70 の匿名ユーザとしてのみ読み取り / 書き込みアクセス権を取得します。クライアント #2 は、自身のユーザ ID で読み取り / 書き込みアクセス権を取得します。

#### 例

エクスポートポリシーに、次のパラメータが指定されたエクスポートルールが含まれています。

- `-protocol nfs3`
- `-clientmatch 10.1.16.0/255.255.255.0`
- `-rorule sys,none`
- `-rwrule none`
- `-anon 70`

クライアント #1 は、IP アドレスが 10.1.16.207 で、NFSv3 プロトコルを使用してアクセス要求を送信し、Kerberos v5 で認証されます。

クライアント #2 は、IP アドレスが 10.1.16.211 で、NFSv3 プロトコルを使用してアクセス要求を送信し、AUTH\_SYS で認証されます。

クライアント #3 は、IP アドレスが 10.1.16.234 で、NFSv3 プロトコルを使用してアクセス要求を送信し、認証は行われていません（セキュリティタイプ AUTH\_NONE）。

3 つすべてのクライアントで、クライアントアクセスプロトコルと IP アドレスは一致しています。読み取り専用パラメータでは、読み取り専用アクセスが、AUTH\_SYS で認証された、自身のユーザ ID を持つクライアントに許可されています。読み取り専用パラメータでは、ユーザ ID が 70 の匿名ユーザとしての読み取り専用アクセスが、他のセキュリティタイプを使用して認証されたクライアントに許可されています。読み取り / 書き込みパラメータでは、匿名ユーザとしてのみ読み取り / 書き込みアクセスが許可されています。

したがって、クライアント #1 とクライアント #3 は、ユーザ ID が 70 の匿名ユーザとしてのみ読み取り / 書き込みアクセス権を取得します。クライアント #2 は、自身のユーザ ID で読み取り専用アクセス権を取得しますが、読み取り / 書き込みアクセスは拒否されます。

#### セキュリティタイプによるクライアントアクセスレベルの決定方法

クライアントの認証に使用されるセキュリティタイプは、エクスポートルールで特別な役割を果たします。クライアントがボリュームまたは qtree にアクセスする際のレベルがセキュリティタイプによってどのように決定されるかについて理解しておく必要があります。

アクセスレベルには、次の 3 つがあります。

1. 読み取り専用です
2. 読み書き可能です
3. superuser（ユーザ ID が 0 のクライアントの場合）

セキュリティタイプに基づくアクセスレベルはこの順序で評価されるため、エクスポートルールでアクセスレベルパラメータを作成するときは、次のルールに従う必要があります。

クライアントに必要なアクセスレベル	クライアントのセキュリティタイプと一致する必要があるアクセスパラメータ
標準ユーザの読み取り専用	読み取り専用です (-rorule)
標準ユーザの読み取り / 書き込み	読み取り専用です (-rorule) および読み取り/書き込み (-rwrule)
スーパーユーザの読み取り専用です	読み取り専用です (-rorule) および -superuser
スーパーユーザの読み取り / 書き込み	読み取り専用です (-rorule) および読み取り/書き込み (-rwrule) および -superuser

次に、これらの 3 つのアクセスパラメータのそれぞれで有効なセキュリティタイプを示します。

- any
- none
- never

このセキュリティタイプは、では使用できません -superuser パラメータ

- krb5
- krb5i
- krb5p
- ntlm
- sys

クライアントのセキュリティタイプを 3 つの各アクセスパラメータと照合したときの結果としては、次の 3 つが考えられます。

クライアントのセキュリティタイプ	クライアント
アクセスパラメータで指定されたタイプと一致する。	独自のユーザ ID を使用して、そのレベルのアクセス権を取得します。
指定したタイプと一致しないが、アクセスパラメータにオプションが指定されている none。	で指定されたユーザIDを持つ匿名ユーザとして、そのレベルのアクセス権を取得します -anon パラメータ

クライアントのセキュリティタイプ	クライアント
指定したタイプと一致しないため、アクセスパラメータにオプションが指定されていません none。	は、そのレベルのアクセス権を取得しません。これは、には適用されません -superuser パラメータには常にが含まれているためです none 指定されていない場合でも。

## 例

エクスポートポリシーに、次のパラメータが指定されたエクスポートルールが含まれています。

- -protocol nfs3
- -clientmatch 10.1.16.0/255.255.255.0
- -rorule any
- -rwrule sys,krb5
- -superuser krb5

クライアント #1 は、IP アドレスが 10.1.16.207、ユーザ ID が 0 で、NFSv3 プロトコルを使用してアクセス要求を送信し、Kerberos v5 で認証されます。

クライアント #2 は、IP アドレスが 10.1.16.211、ユーザ ID が 0 で、NFSv3 プロトコルを使用してアクセス要求を送信し、AUTH\_SYS で認証されます。

クライアント #3 は、IP アドレスが 10.1.16.234、ユーザ ID が 0 で、NFSv3 プロトコルを使用してアクセス要求を送信し、認証は行われていません（AUTH\_NONE）。

3 つすべてのクライアントで、クライアントアクセスプロトコルと IP アドレスは一致しています。読み取り専用パラメータでは、セキュリティタイプに関係なく、読み取り専用アクセスがすべてのクライアントに許可されています。読み取り / 書き込みパラメータでは、読み取り / 書き込みアクセスが、AUTH\_SYS または Kerberos v5 で認証された、自身のユーザ ID を持つクライアントに許可されています。スーパーユーザパラメータでは、スーパーユーザアクセスが、Kerberos v5 で認証された、ユーザ ID が 0 のクライアントに許可されています。

したがって、クライアント #1 は、3 つすべてのアクセスパラメータに一致するため、スーパーユーザの読み取り / 書き込みアクセス権を取得します。クライアント #2 は、読み取り / 書き込みアクセス権を取得しますが、スーパーユーザアクセス権は取得できません。クライアント #3 は、読み取り専用アクセス権を取得しますが、スーパーユーザアクセス権は取得できません。

スーパーユーザのアクセス要求を管理します

エクスポートポリシーを設定する際には、ストレージシステムがユーザ ID が 0 のクライアントアクセス要求をスーパーユーザとして受信し、それに応じてエクスポートルールを設定する場合に必要な処理を考慮する必要があります。

UNIX の世界では、ユーザ ID 0 のユーザがスーパーユーザと呼ばれ、通常は root と呼ばれます。このユーザにはシステム上で無制限のアクセス権が与えられています。スーパーユーザ権限の使用は、システムやデータセキュリティの侵害などのいくつかの理由によってリスクを伴う可能性があります。

デフォルトでは、ONTAP はユーザ ID が 0 のクライアントを匿名ユーザにマッピングします。ただし、は指定できます - superuser ユーザIDが0のクライアントの処理方法（セキュリティタイプに応じて）を決定す



るエクスポートルールのパラメータ。で有効なオプションは次のとおりです `-superuser` パラメータ：

- any
- none

これは、を指定しない場合のデフォルト設定です `-superuser` パラメータ

- krb5
- ntlm
- sys

ユーザIDが0のクライアントは、に応じて2つの方法で処理されます `-superuser` パラメータ設定：

状況に応じて <b>-superuser</b> パラメータおよびクライアントのセキュリティタイプ	クライアント
一致	ユーザ ID 0 でスーパーユーザアクセス権を取得します。
一致しません	で指定されたユーザIDを持つ匿名ユーザとしてアクセスを取得します <code>-anon</code> パラメータとその割り当てられた権限。これは、読み取り専用パラメータと読み取り/書き込みパラメータのどちらでオプションが指定されているかに関係ありません <code>none</code> 。

クライアントがNTFSセキュリティ形式およびのボリュームにアクセスするためにユーザID 0を提示する場合 `-superuser` パラメータはに設定されます `none` ONTAP では、匿名ユーザがネームマッピングを使用して適切なクレデンシャルを取得します。

例

エクスポートポリシーに、次のパラメータが指定されたエクスポートルールが含まれています。

- `-protocol nfs3`
- `-clientmatch 10.1.16.0/255.255.255.0`
- `-rorule any`
- `-rwrule krb5,ntlm`
- `-anon 127`

クライアント#1は、IPアドレスが10.1.16.207、ユーザIDが746で、NFSv3プロトコルを使用してアクセス要求を送信し、Kerberos v5で認証されます。

クライアント #2 は、IP アドレスが 10.1.16.211、ユーザ ID が 0 で、NFSv3 プロトコルを使用してアクセス要求を送信し、AUTH\_SYS で認証されます。

両方のクライアントで、クライアントアクセスプロトコルと IP アドレスは一致しています。読み取り専用パラメータでは、認証に使用するセキュリティタイプに関係なく、読み取り専用アクセスがすべてのクライアントに許可されています。ただし、読み取り / 書き込みアクセス権を取得するのはクライアント #1 だけです。

これは、認証に承認されたセキュリティタイプ Kerberos v5 を使用したためです。

クライアント #2 は、スーパーユーザアクセス権を取得できません。代わりに、が原因で匿名にマッピングされます `-superuser` パラメータが指定されていません。つまり、デフォルトは `none` ユーザID 0を匿名に自動的にマッピングします。また、クライアント #2 はセキュリティタイプが読み取り / 書き込みパラメータと一致しなかったため、読み取り専用アクセス権のみを取得します。

例

エクスポートポリシーに、次のパラメータが指定されたエクスポートルールが含まれています。

- `-protocol nfs3`
- `-clientmatch 10.1.16.0/255.255.255.0`
- `-rorule any`
- `-rwrule krb5,ntlm`
- `-superuser krb5`
- `-anon 0`

クライアント #1 は、IP アドレスが 10.1.16.207、ユーザ ID が 0 で、NFSv3 プロトコルを使用してアクセス要求を送信し、Kerberos v5 で認証されます。

クライアント #2 は、IP アドレスが 10.1.16.211、ユーザ ID が 0 で、NFSv3 プロトコルを使用してアクセス要求を送信し、AUTH\_SYS で認証されます。

両方のクライアントで、クライアントアクセスプロトコルと IP アドレスは一致しています。読み取り専用パラメータでは、認証に使用するセキュリティタイプに関係なく、読み取り専用アクセスがすべてのクライアントに許可されています。ただし、読み取り / 書き込みアクセス権を取得するのはクライアント #1 だけです。これは、認証に承認されたセキュリティタイプ Kerberos v5 を使用したためです。クライアント #2 は読み取り / 書き込みアクセス権を取得できません。

このエクスポートルールでは、ユーザ ID が 0 のクライアントにスーパーユーザアクセスが許可されています。クライアント#1は、読み取り専用およびのユーザIDおよびセキュリティタイプと一致するため、スーパーユーザアクセスを取得します `-superuser` パラメータクライアント#2のセキュリティタイプが読み取り/書き込みパラメータまたはと一致しないため、読み取り/書き込みアクセス権もスーパーユーザアクセス権も取得されません `-superuser` パラメータ代わりに、クライアント #2 は匿名ユーザにマッピングされます。この場合、ユーザ ID は 0 です。

**ONTAP** でのエクスポートポリシーキャッシュの使用方法

システムパフォーマンスを向上するために、ONTAP はローカルキャッシュを使用してホスト名やネットグループなどの情報を格納します。これにより、ONTAP は外部ソースから情報を取得するよりも迅速にエクスポートポリシールールを処理できます。キャッシュとは何か、またキャッシュによって何が行われるのかを理解すると、クライアントアクセスに関する問題のトラブルシューティングに役立ちます。

NFS エクスポートへのクライアントアクセスを制御するには、エクスポートポリシーを設定します。各エクスポートポリシーにはルールが含まれており、各ルールにはアクセスを要求しているクライアントに対するマッチングを行うパラメータが含まれています。これらのパラメータの一部では、ドメイン名、ホスト名、ネットグループなどのオブジェクトを解決するために ONTAP が DNS サーバや NIS サーバのような外部ソースと通信する必要があります。

外部ソースとの通信には少し時間がかかります。パフォーマンスを向上させるために、ONTAP は、各ノード上の複数のキャッシュに情報をローカルに格納して、エクスポートポリシールールオブジェクトの解決にかかる時間を短縮します。

キャッシュ名	保存される情報のタイプ
にアクセスします	対応するエクスポートポリシーへのクライアントのマッピング
名前	対応する UNIX ユーザ ID への UNIX ユーザ名のマッピング
ID	対応する UNIX ユーザ ID および拡張された UNIX グループ ID への UNIX ユーザ ID のマッピング
ホスト	対応する IP アドレスへのホスト名のマッピング
ネットグループ	メンバーの対応する IP アドレスへのネットグループのマッピング
showmount	SVM ネームスペースからエクスポートされたディレクトリのリスト

ONTAP が外部ネームサーバ上の情報を取得してローカルに格納したあとに、環境内の外部ネームサーバ上の情報を変更すると、キャッシュ内の情報が古くなる可能性があります。ONTAP は一定期間の経過後に自動的にキャッシュを更新しますが、有効期限や更新の時期およびアルゴリズムはキャッシュごとに異なります。

キャッシュに古くなった情報が含まれる理由としてもう 1 つ考えられるのは、ONTAP がキャッシュされた情報の更新を試みたにもかかわらずネームサーバと通信しようとしてエラーが発生した場合です。この場合、ONTAP は、クライアントの中断を避けるために現在ローカルキャッシュに格納されている情報を引き続き使用します。

その結果、成功することが想定されるクライアントアクセス要求が失敗し、エラーとなることが想定されるクライアントアクセス要求が成功する可能性があります。クライアントアクセスに関するこのような問題のトラブルシューティング時には、エクスポートポリシーキャッシュの一部を表示したり、手動でフラッシュしたりできます。

#### アクセスキャッシュの仕組み

ONTAP は、アクセスキャッシュを使用して、ボリュームまたは qtrees へのクライアントアクセス処理に対するエクスポートポリシールール評価の結果を格納します。これにより、クライアントから I/O 要求が送信されるたびにエクスポートポリシールール評価の処理を行う場合よりも、アクセスキャッシュから情報をはるかに短時間で取得できるため、パフォーマンスが向上します。

NFS クライアントがボリュームまたは qtrees 上のデータにアクセスするための I/O 要求を送信するたびに、ONTAP はそれぞれの I/O 要求を評価して、その I/O 要求を許可するか拒否するかを決定する必要があります。この評価には、そのボリュームまたは qtrees に関連付けられているすべてのエクスポートポリシールールのチェックが伴います。ボリュームまたは qtrees へのパスが 1 つ以上のジャンクションポイントと交差してい

る場合は、そのパスに付随する複数のエクスポートポリシーに対してこのチェックの実行が必要になる可能性があります。

なお、この評価は、最初のマウント要求についてだけでなく、読み取り、書き込み、リスト、コピーなどの処理を行う NFS クライアントから送信されたすべての I/O 要求について行われます。

ONTAP が適用可能なエクスポートポリシールールを特定して要求を許可するか拒否するかを決定すると、ONTAP はその情報を格納するためのエントリをアクセスキャッシュ内に作成します。

NFS クライアントが I/O 要求を送信すると、ONTAP は、そのクライアントの IP アドレス、SVM の ID、ターゲットボリュームまたは qtree に関連付けられているエクスポートポリシーを記録したうえで、まずアクセスキャッシュをチェックして一致するエントリがないか確認します。一致するエントリがアクセスキャッシュ内に存在する場合、ONTAP はそこに格納されている情報を使用して、I/O 要求を許可または拒否します。一致するエントリが存在しない場合、ONTAP は先ほど述べたすべての適用可能なポリシールールを評価する通常の処理を行います。

アクティブに使用されていないアクセスキャッシュエントリは更新されません。これにより、外部ネームサーバとの無駄な通信が削減されます。

アクセスキャッシュからの情報の取得は、I/O 要求のたびにエクスポートポリシールールを評価する全体的な処理よりもずっと高速です。そのため、アクセスキャッシュを使用すると、クライアントアクセスチェックのオーバーヘッドが軽減され、パフォーマンスが大幅に向上します。

アクセスキャッシュパラメータの仕組み

アクセスキャッシュ内のエントリの更新期間を制御するパラメータがいくつかあります。これらのパラメータの仕組みを理解すると、各パラメータを変更してアクセスキャッシュを調整し、パフォーマンスと格納される情報の鮮度のバランスを取ることができます。

アクセスキャッシュには、ボリュームまたは qtree へのアクセスを試みるクライアントに適用される 1 つ以上のエクスポートルールで構成されるエントリが格納されます。これらのエントリは、一定期間格納されたあと、更新されます。更新時間はアクセスキャッシュパラメータによって決定され、アクセスキャッシュエントリのタイプによって異なります。

アクセスキャッシュパラメータは、個々の SVM に対して指定できます。これにより、SVM のアクセス要件に応じてパラメータを変更できます。アクティブに使用されていないアクセスキャッシュエントリは更新されないため、外部ネームサーバとの無駄な通信が削減されます。

アクセスキャッシュエントリタイプ	説明	更新期間（秒）
正のエントリ	クライアントへのアクセス拒否を発生させなかったアクセスキャッシュエントリです。	最小値： 300  最大値： 86 、 400  デフォルト値は 3,600 です。

負のエントリ	クライアントへのアクセス拒否を発生させたアクセスキャッシュエントリです。	最小：60 最大値： 86、 400 デフォルト値は 3,600 です。
--------	--------------------------------------	--

## 例

NFS クライアントがクラスタ上のボリュームへのアクセスを試みます。ONTAP は、エクスポートポリシールールに対するクライアントのマッチングを行い、クライアントがエクスポートポリシールール設定に基づいてアクセスを行っていると判断します。ONTAP はエクスポートポリシールールを正のエントリとしてアクセスキャッシュに格納します。デフォルトでは、ONTAP は、この正のエントリを 1 時間（3、600 秒）アクセスキャッシュ内に保持したあと、情報を最新の状態にするためにこのエントリを自動的に更新します。

アクセスキャッシュが不必要にいっぱいになるのを防ぐために、クライアントアクセスの特定の期間使用されていない既存のアクセスキャッシュエントリをクリアするための追加のパラメータがあります。これ `-harvest-timeout` パラメータの有効範囲は60~2、592、000秒で、デフォルト設定は86、400秒です。

## qtree からエクスポートポリシーを削除する

qtree に割り当てられている特定のエクスポートポリシーが不要になった場合は、代わりに格納先ボリュームのエクスポートポリシーを継承するように qtree を変更することで、エクスポートポリシーを削除できます。これは、を使用して実行できます `volume qtree modify` コマンドにを指定します `-export-policy` パラメータと空の名前文字列（""）。

## 手順

1. qtree からエクスポートポリシーを削除するには、次のコマンドを入力します。

```
volume qtree modify -vserver vservers_name -qtree-path
/vol/volume_name/qtree_name -export-policy ""
```

2. qtree が適切に変更されたことを確認します。

```
volume qtree show -qtree qtree_name -fields export-policy
```

## qtree ファイル操作の qtree ID を検証します

ONTAP では、オプションで qtree ID の検証を追加で実行できます。この検証により、クライアントのファイル処理要求で有効な qtree ID が使用されるとともに、クライアントによるファイルの移動が同じ qtree 内でのみ行えるようになります。この検証を有効または無効にするには、を変更します `-validate-qtree-export` パラメータこのパラメータはデフォルトで有効になっています。

## このタスクについて

このパラメータは、Storage Virtual Machine （SVM）上の 1 つ以上の qtree にエクスポートポリシーを直接割り当てている場合にのみ有効です。

## 手順

1. 権限レベルを advanced に設定します。

```
set -privilege advanced
```

2. 次のいずれかを実行します。

検証する <b>qtree ID</b> の状態	入力するコマンド
有効	<pre>vserver nfs modify -vserver vserver_name -validate-qtree-export enabled</pre>
無効	<pre>vserver nfs modify -vserver vserver_name -validate-qtree-export disabled</pre>

3. admin 権限レベルに戻ります。

```
set -privilege admin
```

#### FlexVol のエクスポートポリシーの制限とネストされたジャンクション

上位レベルのジャンクションでネストされたジャンクションよりも制限が厳しいエクスポートポリシーを設定した場合は、下位レベルのジャンクションへのアクセスに失敗する可能性があります。

上位レベルのジャンクションには下位レベルのジャンクションよりも制限が厳しくないエクスポートポリシーを設定するようにしてください。

#### NFS で Kerberos を使用してセキュリティを強化する

##### ONTAP での Kerberos のサポート

Kerberos は、クライアント / サーバアプリケーションに対して強力でセキュアな認証を提供します。認証により、ユーザおよびプロセスの ID をサーバで検証できます。ONTAP 環境では、Storage Virtual Machine (SVM) と NFS クライアント間の認証を Kerberos で実行できます。

ONTAP 9 では、次の Kerberos 機能がサポートされます。

- 整合性チェック機能を備えた Kerberos 5 認証 (krb5i)

Krb5i では、チェックサムを使用して、クライアントとサーバ間で転送される各 NFS メッセージの整合性を検証します。これは、セキュリティ上の理由（データが改ざんされていないことの確認など）とデータ整合性に関する理由（信頼性の低いネットワークで NFS を使用する場合のデータ破損の防止など）の両方で有用です。

- プライバシーチェック機能を備えた Kerberos 5 認証 (krb5p)

krb5p では、クライアントとサーバ間のすべてのトラフィックがチェックサムで暗号化されます。これにより、安全性が向上し、負荷も増加します。

- 128 ビットおよび 256 ビットの AES 暗号化

Advanced Encryption Standard (AES) は、電子データを保護するための暗号化アルゴリズムです。ONTAPでは、セキュリティを強化するために、128ビットキーによるAES (AES-128) と256ビットキーによるAES (AES-256) がKerberosでサポートされます。

- SVM レベルの Kerberos Realm 設定

SVM 管理者は、Kerberos Realm 設定を SVM レベルで作成できるようになりました。つまり、SVM 管理者は、Kerberos Realm 設定に関してクラスタ管理者に頼る必要がなくなり、個別の Kerberos Realm 設定をマルチテナンシー環境で作成することができます。

## NFS で Kerberos を設定するための要件

NFS で Kerberos を使用するための設定をシステムで行う前に、ネットワークおよびストレージの環境のいくつかの項目について、適切に設定されていることを確認する必要があります。



環境を設定する手順は、使用しているクライアントオペレーティングシステム、ドメインコントローラ、Kerberos、DNS などのバージョンや種類によって異なります。これらのすべての変数については、本ドキュメントでは説明していません。詳細については、各コンポーネントの該当するドキュメントを参照してください。

Windows Server 2008 R2 の Active Directory および Linux ホストを使用する環境での ONTAP と Kerberos 5 および NFSv3 / NFSv4 の設定方法に関する詳しい例については、テクニカルレポート 4073 を参照してください。

次の項目を最初に設定する必要があります。

### ネットワーク環境の要件

- Kerberos

Kerberos を Key Distribution Center (KDC ; キー配布センター) で設定しておく必要があります (たとえば、Windows Active Directory ベースの Kerberos または MIT Kerberos) 。

NFSサーバはを使用する必要があります nfs マシンプリンシパルの主要コンポーネントとして使用します。

- ディレクトリサービス

Active Directory や OpenLDAP などのセキュアなディレクトリサービスを環境に導入し、SSL / TLS 経由の LDAP を使用するように設定する必要があります。

- NTP

タイムサーバで NTP を実行している必要があります。これは、時刻のずれによる Kerberos 認証の失敗を回避するために必要です。

- ドメイン名解決（DNS）

それぞれの UNIX クライアントおよび SVM LIF について、KDC の前方参照ゾーンと逆引き参照ゾーンに適切なサービスレコード（SRV）が登録されている必要があります。すべてのコンポーネントを DNS で正しく解決できる必要があります。

- ユーザアカウント

各クライアントについて、Kerberos Realm のユーザアカウントが必要です。NFS サーバでは 'マシン・プリンシパルの主要コンポーネントとして NFS' を使用する必要があります

## NFSクライアントの要件

- NFS

NFSv3 または NFSv4 を使用してネットワーク経由で通信するように各クライアントが適切に設定されている必要があります。

クライアントで RFC1964 および RFC2203 がサポートされている必要があります。

- Kerberos

Kerberos 認証を使用するように各クライアントが適切に設定されている必要があります。詳細は次のとおりです。

- TGS 通信の暗号化が有効です。

非常にセキュリティ性の高い AES-256。

- TGT 通信に対する最も安全な暗号化タイプが有効です。
- Kerberos Realm とドメインを正しく設定します。
- GSSはイネーブルです。

マシンのクレデンシャルを使用する場合：

- 走らないでください gssd を使用 -n パラメータ
- 走らないでください kinit をrootユーザとして指定します。

- 各クライアントは、最新かつ更新されたオペレーティングシステムバージョンを使用する必要があります。

これにより、Kerberos での AES 暗号化の互換性と信頼性が最大限確保されます。

- DNS

DNS を使用して名前が正しく解決されるように各クライアントが適切に設定されている必要があります。

- NTP

各クライアントが NTP サーバと同期されている必要があります。



- ホストおよびドメインの情報

各クライアントの `/etc/hosts` および `/etc/resolv.conf` ファイルには正しいホスト名とDNS情報が格納されている必要があります。

- keytab ファイル

各クライアントについて、KDC の keytab ファイルが必要です。Realm は大文字で指定する必要があります。最高レベルのセキュリティを得るために、暗号化タイプを AES-256 にする必要があります。

- オプション：パフォーマンスを最大限に高めるには、ローカルエリアネットワークとの通信用とストレージネットワークとの通信用に、少なくとも 2 つのネットワークインターフェイスを設定します。

## ストレージシステムの要件

- NFS ライセンス

ストレージシステムに有効な NFS ライセンスがインストールされている必要があります。

- CIFSライセンス

CIFS ライセンスはオプションです。マルチプロトコルのネームマッピングを使用する場合にのみ、Windows クレデンシャルをチェックする必要があります。純粋な UNIX のみの環境では必要ありません。

- SVM

システムで SVM を少なくとも 1 つ設定しておく必要があります。

- SVM で DNS を設定します

各 SVM で DNS を設定しておく必要があります。

- NFS サーバ

SVM で NFS を設定しておく必要があります。

- AES 暗号化

最高レベルのセキュリティを得るために、Kerberos で AES-256 暗号化のみを許可するように NFS サーバを設定する必要があります。

- SMBサーバ

マルチプロトコル環境の場合は、SVMでSMBを設定しておく必要があります。SMB サーバは、マルチプロトコルのネームマッピングに必要です。

- 個のボリューム

SVM で使用するルートボリュームと少なくとも 1 つのデータボリュームを設定しておく必要があります。

- ルートボリューム

SVM のルートボリュームを次のように設定しておく必要があります。

名前	設定
セキュリティ形式	「 UNIX 」
UID	root または ID 0
GID	root または ID 0
UNIX 権限	777

ルートボリュームとは異なり、データボリュームのセキュリティ形式は任意に設定できます。

- UNIXグループ

SVM で次の UNIX グループを設定しておく必要があります。

グループ名	グループ ID
デーモン	1.
ルート	0
pcuser	65534 （ SVM を作成すると ONTAP で自動的に作成されます）

- UNIXユーザ

SVM で次の UNIX ユーザを設定しておく必要があります。

ユーザ名	ユーザ ID	プライマリグループ ID	コメント（ <b>Comment</b> ）
NFS	500ドル	0	GSS INITフェーズで必要  NFS クライアントユーザの SPN の最初のコンポーネントがユーザとして使用されます。
pcuser	65534	65534	NFSトCIFSノマルチプロトコルノシヨウニヒツヨウ  SVMを作成すると、ONTAPで自動的に作成されてpcuserグループに追加されます。

ユーザ名	ユーザ ID	プライマリグループ ID	コメント (Comment)
ルート	0	0	マウントに必要

NFS クライアントユーザの SPN に対する Kerberos-UNIX ネームマッピングがある場合は、nfs ユーザは必要ありません。

- エクスポートポリシーとルール

ルートボリュームとデータボリュームおよび qtree に対するエクスポートポリシーと必要なエクスポートルールを設定しておく必要があります。SVMのすべてのボリュームへのアクセスにKerberosを使用する場合は、エクスポートルールのオプションを設定できます `-rorule`、`-rwrule` および `-superuser` ルートボリュームのをに設定します `krb5`、`krb5i` または `krb5p`。

- Kerberos-UNIX ネームマッピング

NFS クライアントユーザの SPN によって識別されたユーザに root 権限を持たせる場合は、root に対するネームマッピングを作成する必要があります。

## 関連情報

["ネットアップテクニカルレポート 4073 : 『 Secure Unified Authentication 』"](#)

["NetApp Interoperability Matrix Tool で確認できます"](#)

["システム管理"](#)

["論理ストレージ管理"](#)

**NFSv4** のユーザ ID ドメインを指定します

ユーザIDドメインを指定するには、を設定します `-v4-id-domain` オプション

このタスクについて

NFSv4 ユーザ ID のマッピングにデフォルトで使用されるドメインは、NIS ドメインが設定されている場合は NIS ドメインになります。ONTAPNIS ドメインが設定されていない場合は、DNS ドメインが使用されます。たとえば、複数のユーザ ID ドメインがある場合、ユーザ ID ドメインの設定が必要になることがあります。ドメイン名は、ドメインコントローラのドメイン設定と一致する必要があります。これは NFSv3 の場合は必要ありません。

ステップ

1. 次のコマンドを入力します。

```
vserver nfs modify -vserver vservice_name -v4-id-domain NIS_domain_name
```

ネームサービスを設定

**ONTAP** のネームサービススイッチ設定の仕組み

ONTAP では、に相当するテーブルにネームサービス設定情報が格納されます

/etc/nsswitch.conf UNIXシステム上のファイル。このテーブルを環境に応じて適切に設定するためには、その機能と ONTAP でテーブルがどのように使用されるかを理解しておく必要があります。

ONTAP ネームサービススイッチテーブルは、ONTAP が特定の種類のネームサービス情報を取得する際にどのネームサービスソースをどの順番で参照するかを決定します。ONTAP では、SVM ごとに個別のネームサービススイッチテーブルが保持されます。

## データベースタイプ

テーブルには、次の各データベースタイプについてネームサービスのリストが格納されます。

データベースタイプ	ネームサービスソースの用途	有効なソース
ホスト	ホスト名の IP アドレスへの変換	ファイル、DNS
グループ	ユーザグループ情報を検索しています	files 、 nis 、 ldap が表示されます
パスワード	ユーザ情報を検索しています	files 、 nis 、 ldap が表示されます
ネットグループ	ネットグループ情報の検索	files 、 nis 、 ldap が表示されます
namemap	ユーザ名のマッピング	ファイル、LDAP

## ソースタイプ

ソースタイプによって、該当する情報を取得するために使用するネームサービスソースが決まります。

ソースタイプ	情報の検索先	使用するコマンド
ファイル	ローカルのソースファイル	<pre>vserver services name-service unix-user vserver services name-service unix-group</pre> <pre>vserver services name-service netgroup</pre> <pre>vserver services name-service dns hosts</pre>
NIS	SVM の NIS ドメイン設定で指定された外部の NIS サーバ	<pre>vserver services name-service nis-domain</pre>
LDAP	SVM の LDAP クライアント設定で指定された外部の LDAP サーバ	<pre>vserver services name-service ldap</pre>

ソースタイプ	情報の検索先	使用するコマンド
DNS	SVM の DNS 設定で指定された外部の DNS サーバ	<code>vserver services name-service dns</code>

データアクセスとSVM管理者の両方の認証にNISまたはLDAPを使用する場合も、を追加する必要があります  
files また、NISまたはLDAP認証が失敗した場合のフォールバックとしてローカルユーザを設定します。

外部ソースへのアクセスに使用するプロトコル

ONTAP では、外部ソースのサーバへのアクセスに次のプロトコルを使用します。

外部のネームサービスソース	アクセスに使用するプロトコル
NIS	UDP
DNS	UDP
LDAP	TCP

例

次の例では、SVM svm\_1 のネームサービススイッチ情報を表示しています。

```
cluster1::*> vserver services name-service ns-switch show -vserver svm_1
```

Vserver	Database	Source	Order
svm_1	hosts	files,	
		dns	
svm_1	group	files	
svm_1	passwd	files	
svm_1	netgroup	nis,	
		files	

ホストの IP アドレスの検索では、ONTAP は最初にローカルのソースファイルを参照します。結果が返されない場合は、次に DNS サーバが照会されます。

ユーザまたはグループ情報の検索では、ONTAP はローカルのソースファイルだけを参照します。結果が返されない場合、検索は失敗します。

ネットグループ情報の検索では、ONTAP が最初に外部 NIS サーバを参照し、結果が返されない場合は、次にローカルネットグループファイルが照会されます。

SVM svm\_1 のテーブルには、ネームマッピング用のネームサービスエントリは含まれていません。そのため、ONTAP はデフォルトでローカルのソースファイルだけを参照します。

関連情報

LDAP を使用する

## LDAPの概要

LDAP（ Lightweight Directory Access Protocol ）サーバを使用すると、ユーザ情報を一元的に管理できます。ユーザデータベースを LDAP サーバに保存する場合、既存の LDAP データベースのユーザ情報を検索するようにストレージシステムを設定できます。

- LDAP for ONTAP を設定する前に、サイト環境が LDAP サーバおよびクライアント設定のベストプラクティスを満たしていることを確認する必要があります。具体的には、次の条件を満たす必要があります。
  - LDAP サーバのドメイン名が LDAP クライアント上のエントリと一致している必要があります。
  - LDAP サーバでサポートされている LDAP ユーザパスワードハッシュタイプには、ONTAP でサポートされているハッシュタイプが含まれている必要があります。
    - crypt（すべてのタイプ）および SHA-1（SHA、SSHA）
    - ONTAP 9.8 以降では、SHA-2 ハッシュ（SHA-256、SSH-384、SHA-512、SSHA-256、SSHA-384 および SSHA-512）もサポートされます。
  - LDAP サーバにセッションセキュリティ対策が必要な場合は、LDAP クライアントで設定する必要があります。

次のセッションセキュリティオプションを使用できます。

- LDAP 署名（データの整合性チェックを提供）および LDAP の署名と封印（データの整合性チェックと暗号化を提供）
- START TLS
- LDAPS（LDAP over TLS または SSL）
- 署名および封印された LDAP クエリを有効にするには、次のサービスが設定されている必要があります。
  - LDAP サーバで GSSAPI（Kerberos）SASL がサポートされている必要があります。
  - LDAP サーバに、DNS A/AAAA レコード、および DNS サーバで設定された PTR レコードが必要です。
  - Kerberos サーバに、DNS サーバ上に存在する SRV レコードが必要です。
- TLS または LDAPS を開始できるようにするには、次の点を考慮する必要があります。
  - ネットアップでは、LDAPS ではなく Start TLS を使用することを推奨します。
  - LDAPS を使用している場合は、ONTAP 9.5 以降で LDAP サーバの TLS または SSL が有効になっている必要があります。ONTAP 9.0~9.4 では SSL はサポートされません。
  - 証明書サーバがドメインで設定済みである必要があります。
- LDAP リファラール追跡を有効にするには（ONTAP 9.5 以降）、次の条件を満たしている必要があります。
  - 両方のドメインで、次のいずれかの信頼関係を設定する必要があります。

- 双方向
- 一方。一次は紹介ドメインを信頼します
- 親子
- 参照されているすべてのサーバ名を解決するように DNS が設定されていること。
- の認証では、ドメインパスワードが同じである必要があります `--bind-as-cifs-server true` に設定します。

次の設定は LDAP リファラール追跡でサポートされません。



- すべての ONTAP バージョン：
- 管理 SVM 上の LDAP クライアント
- ONTAP 9.8 以前では（9.9.1 以降でサポートされています）：
- LDAP の署名と封印（`-session-security` オプション）
- 暗号化された TLS 接続（`-use-start-tls` オプション）
- LDAPS ポート 636（`-use-ldaps-for-ad-ldap` オプション）

- ONTAP 9.11.1 以降では、を使用できます ["nsswitch 認証のための LDAP 高速バインド。"](#)
- SVM で LDAP クライアントを設定するときは、LDAP スキーマを入力する必要があります。

ほとんどの場合、デフォルトの ONTAP スキーマのいずれかが適しています。ただし、環境で使用する LDAP スキーマがこれらと異なる場合は、LDAP クライアントを作成する前に、ONTAP 用の新しい LDAP クライアントスキーマを作成する必要があります。環境の要件については、LDAP 管理者にお問い合わせください。

- LDAP をホスト名解決に使用することはサポートされていません。

追加情報の場合は、を参照してください ["ネットアップテクニカルレポート 4835：『How to Configure LDAP in ONTAP』"](#)。

## LDAP の署名と封印の概念

ONTAP 9 以降では、署名と封印を設定して、Active Directory（AD）サーバへの照会に対する LDAP セッションセキュリティを有効にすることができます。Storage Virtual Machine（SVM）の NFS サーバセキュリティ設定を LDAP サーバの設定に対応するように設定する必要があります。

署名は、シークレットキーのテクノロジーを使用して、LDAP ペイロードデータの整合性を確認します。封印は、LDAP ペイロードデータを暗号化して機密情報がクリアテキストで送信されないようにします。LDAP トラフィックについて、署名が必要か、署名と封印が必要か、どちらも必要ないかは、`Idap Security Level` オプションで指定します。デフォルトは `none`。テスト

SMB トラフィックに対する LDAP の署名と封印は、を使用して SVM で有効にします `-session-security -for-ad-ldap` オプションをに設定します `vserver cifs security modify` コマンドを実行します

## LDAPSの概念

ONTAP での LDAP 通信の保護方法に関する用語や概念を理解しておく必要があります。ONTAP は、Active Directory 統合 LDAP サーバ間または UNIX ベース LDAP サーバ間の認証されたセッションの設定に Start TLS または LDAPS を使用できます。

### 用語集

ONTAP での LDAP 通信の保護に LDAPS を使用方法に関して理解しておくべき用語があります。

- \* LDAP \*

（ Lightweight Directory Access Protocol ） 情報ディレクトリにアクセスして管理するためのプロトコルです。LDAP は、ユーザ、グループ、ネットグループなどのオブジェクトを格納するための情報ディレクトリとして使用されます。LDAP は、これらのオブジェクトを管理したり LDAP クライアントからの要求を満たしたりするディレクトリサービスも提供します。

- SSL

（ Secure Sockets Layer ） インターネット上で情報を安全に送信するために開発されたプロトコルです。SSLはONTAP 9以降でサポートされていますが、TLSの導入に伴い廃止されました。

- \* tls \*

（ Transport Layer Security ） 従来の SSL 仕様に基づいた IETF 標準の追跡プロトコルです。SSL の後継にあたります。TLSはONTAP 9.5以降でサポートされます。

- \* LDAPS （ LDAP over SSL または TLS ） \*

TLS または SSL を使用して LDAP クライアントと LDAP サーバ間の通信を保護するプロトコル。「*ldap over SSL*」と「*ldap over TLS*」は同じ意味で使用されることがあります。LDAPSはONTAP 9.5以降でサポートされます。

- ONTAP 9.5-9.8 では、LDAPS はポート 636 でのみ有効にできます。そのためには、を使用します `-use-ldaps-for-ad-ldap` パラメータと `vserver cifs security modify` コマンドを実行します
- ONTAP 9.9.1以降では、任意のポートでLDAPSを有効にできますが、デフォルトはポート636です。これを行うには、を設定します `-ldaps-enabled` パラメータの値 `true` そして目的のものを指定してください `-port` パラメータ詳細については、を参照してください `vserver services name-service ldap client create` のマニュアルページ



ネットアップでは、LDAPS ではなく Start TLS を使用することを推奨します。

- \* TLS を開始 \*

（ `START_TLS`、`STARTTLS`、`_StartTLS` と呼ばれます）。TLS プロトコルを使用してセキュアな通信を提供するメカニズムです。

ONTAP では、LDAP 通信を保護するために `STARTTLS` を使用し、デフォルトの LDAP ポート（389）を使用して LDAP サーバと通信します。LDAP サーバは、LDAP ポート 389 経由の接続を許可するように設定する必要があります。そうしないと、SVM から LDAP サーバへの LDAP TLS 接続が失敗します。



## ONTAP での LDAPS の使用方法

ONTAP は TLS サーバ認証をサポートしています。この認証により、SVM の LDAP クライアントは、バインド操作時に LDAP サーバの ID を確認できます。TLS に対応した LDAP クライアントは、公開鍵暗号化の標準的な技法を使用して、サーバの証明書および公開 ID が有効であり、かつクライアントの信頼できる Certificate Authority (CA ; 認証局) のリストにある CA によって発行されたものであるかどうかをチェックできます。

LDAP では、TLS を使用した通信の暗号化方法として STARTTLS がサポートさSTARTTLS は標準の LDAP ポート (389) 経由でプレーンテキスト接続として開始され、その後 TLS 接続にアップグレードされます。

ONTAP では次の機能がサポートされます

- Active Directory 統合 LDAP サーバと SVM の間の SMB 関連トラフィックに使用する LDAPS
- LDAPS : ネームマッピングやその他の UNIX 情報で使用する LDAP トラフィックに使用します

Active Directory 統合 LDAP サーバまたは UNIX ベース LDAP サーバのいずれかを使用して、LDAP ネームマッピングおよびユーザ、グループ、ネットグループなどのその他の UNIX 情報の格納に使用できます。

- 自己署名ルート CA 証明書

Active-Directory 統合 LDAP を使用している場合は、Windows Server 証明書サービスがドメインにインストールされていると自己署名ルート証明書が生成されます。UNIX ベースの LDAP サーバを LDAP ネームマッピングに使用している場合は、該当する LDAP アプリケーションに適切な手段を使用して、自己署名ルート証明書の生成と保存が行われます。

デフォルトでは、LDAPSは無効になっています。

### LDAP の RFC2307bis サポートを有効にする

LDAP を使用するとともに、ネストされたグループメンバーシップを使用するための追加機能を必要とする場合は、ONTAP を設定して LDAP の RFC2307bis サポートを有効にすることができます。

#### 必要なもの

デフォルトの LDAP クライアントスキーマのうち、使用するいずれか 1 つのコピーを作成しておく必要があります。

#### このタスクについて

LDAP クライアントスキーマでは、グループオブジェクトによって memberUid 属性が使用されます。この属性には複数の値を含めることができ、そのグループに属するユーザの名前を一覧表示できます。RFC2307bis 対応の LDAP クライアントスキーマでは、グループオブジェクトによって uniqueMember 属性が使用されます。この属性には、LDAP ディレクトリ内の別のオブジェクトの完全な Distinguished Name (DN ; 識別名) を含めることができます。これにより、グループに他のグループをメンバーとして追加できるため、ネストされたグループを使用できます。

このユーザは、ネストされたグループを含めて 256 を超えるグループのメンバーになることはできません。ONTAP は、この 256 グループの上限を超えるグループをすべて無視します。

デフォルトでは、RFC2307bis サポートが無効になっています。



MS-AD-BIS スキーマを使用して LDAP クライアントを作成すると、ONTAP では RFC2307bis サポートが自動的に有効になります。

追加情報の場合は、を参照してください "[ネットアップテクニカルレポート 4835](#) : 『How to Configure LDAP in ONTAP』"。

#### 手順

1. 権限レベルを advanced に設定します。

```
set -privilege advanced
```

2. コピーした RFC2307 LDAP クライアントスキーマを変更して、RFC2307bis のサポートを有効にします。

```
vserver services name-service ldap client schema modify -vserver vservice_name  
-schema schema_name -enable-rfc2307bis true
```

3. LDAP サーバでサポートされているオブジェクトクラスに一致するように、スキーマを変更します。

```
vserver services name-service ldap client schema modify -vserver vservice_name  
-schema schema_name -group-of-unique-names-object-class object_class
```

4. LDAP サーバでサポートされている属性名に一致するように、スキーマを変更します。

```
vserver services name-service ldap client schema modify -vserver vservice_name  
-schema schema_name -unique-member-attribute attribute_name
```

5. admin 権限レベルに戻ります。

```
set -privilege admin
```

#### LDAP ディレクトリ検索の設定オプション

環境にとって最も適切な方法で LDAP サーバに接続するように ONTAP LDAP クライアントを設定することで、ユーザ、グループ、およびネットグループ情報を含め、LDAP ディレクトリ検索を最適化することができます。デフォルトの LDAP ベースおよびスコープ検索値で十分な状況や、カスタム値のほうが適切な場合に指定すべきパラメータを理解しておく必要があります。

ユーザ、グループ、およびネットグループ情報の LDAP クライアント検索オプションは、LDAP クエリの失敗、ひいてはストレージシステムへのクライアントアクセスの失敗を回避するのに役立ちます。また、クライアントのパフォーマンスの問題を回避するために、検索をできるだけ効率的に行うことができます。

#### デフォルトのベースおよびスコープ検索値です

LDAP ベースは、LDAP クライアントが LDAP クエリを実行するために使用するデフォルトのベース DN です。ユーザ、グループ、ネットグループの検索を含むすべての検索は、ベース DN を使用して行われます。このオプションは、LDAP ディレクトリが比較的小さく、すべての関連エントリが同じ DN 内にある場合に適しています。

カスタムベースDNを指定しない場合、デフォルトはです `root`。つまり、各クエリでディレクトリ全体が検索されます。これにより、LDAP クエリが成功する見込みは最大になりますが、非効率的であったり、大規模な LDAP ディレクトリではパフォーマンスの大幅な低下につながったりする可能性があります。

LDAP ベーススコープは、LDAP クライアントが LDAP クエリを実行するために使用するデフォルトの検索スコープです。ユーザ、グループ、ネットグループの検索を含むすべての検索は、ベーススコープを使用して行われます。LDAP クエリによる検索範囲を、名前付きエントリのみ、DN の 1 レベル下にあるエントリ、または DN の下にあるサブツリー全体のどれにするかが決定されます。

カスタムベーススコープを指定しない場合、デフォルトはです `subtree`。つまり、各クエリで DN の下にあるサブツリー全体が検索されます。これにより、LDAP クエリが成功する見込みは最大になりますが、非効率的であったり、大規模な LDAP ディレクトリではパフォーマンスの大幅な低下につながったりする可能性があります。

#### カスタムベースおよびスコープ検索値

必要に応じて、ユーザ、グループ、およびネットグループ検索で、別々のベースおよびスコープ値を指定できます。クエリの検索ベースとクエリをこうした形で制限すると、検索対象が LDAP ディレクトリのより小さなサブセクションに制限されるため、パフォーマンスを大幅に向上させることができます。

カスタムベースおよびスコープ値を指定した場合、ユーザ、グループ、およびネットグループ検索の一般的なデフォルト検索ベースおよびスコープは無視されます。カスタムベースおよびスコープ値を指定するパラメータは、`advanced` 権限レベルで使用できます。

LDAP クライアントパラメータ	カスタム指定要素
<code>-base-dn</code>	すべての LDAP 検索のベース DN 複数の値を必要に応じて入力できます（ONTAP 9.5 以降のリリースで LDAP リファーラル追跡を有効にした場合など）。
<code>-base-scope</code>	すべての LDAP 検索のベーススコープ
<code>-user-dn</code>	すべての LDAP ユーザ検索のベース DN このパラメータは、環境ユーザ名マッピング検索も行います。
<code>-user-scope</code>	すべての LDAP ユーザ検索のベーススコープ：このパラメータは、環境ユーザ名マッピング検索も行います。
<code>-group-dn</code>	すべての LDAP グループ検索のベース DN
<code>-group-scope</code>	すべての LDAP グループ検索のベーススコープ
<code>-netgroup-dn</code>	すべての LDAP ネットグループ検索のベース DN
<code>-netgroup-scope</code>	すべての LDAP ネットグループ検索のベーススコープ

#### 複数のカスタムベース DN 値

LDAP ディレクトリが複雑な場合は、特定の情報を求めて LDAP ディレクトリの複数の部分を検索するため

に、複数のベース DN の指定が必要になることがあります。複数のユーザ、グループ、およびネットグループ DN パラメータを指定するには、各パラメータをセミコロン（;）で区切り、DN 検索リスト全体を二重引用符（"）で囲みます。DN にセミコロンが含まれている場合は、DN のセミコロンの直前にエスケープ文字（\）を追加する必要があります。

scope 環境は、対応するパラメータに指定されている のリスト全体を表します。たとえば、3 つの異なるユーザ DN のリストとサブツリーをユーザスコープで指定した場合は、LDAP ユーザ検索により、指定された 3 つの DN のそれぞれでサブツリー全体が検索されます。

また、ONTAP 9.5 以降では、LDAP\_referral\_c追いかけ\_を指定することもできます。これにより、プライマリ LDAP サーバから LDAP リファールル応答が返されなかった場合に、ONTAP LDAP クライアントがその他の LDAP サーバへのルックアップ要求を参照することができます。クライアントは、このリファールデータに記載されたサーバからターゲットオブジェクトを取得します。参照された LDAP サーバにあるオブジェクトを検索するには、参照されたオブジェクトのベース DN を LDAP クライアント設定の一部としてベース DN に追加します。ただし、参照されたオブジェクトは、（を使用して）リファール追跡が有効になっている場合にのみ検索されます -referral-enabled true オプション）LDAP クライアントの作成時または変更時

**LDAP** ディレクトリのホスト単位ネットグループ検索のパフォーマンスを向上させます

LDAP 環境がホスト単位のネットグループ検索を許可するように設定されている場合は、この機能を利用するように ONTAP を設定し、ホスト単位のネットグループ検索を実行することができます。これにより、ネットグループ検索の処理速度を大幅に引き上げ、ネットグループ検索時のレイテンシによる NFS クライアントアクセスの問題を減らすことができます。

必要なもの

LDAPディレクトリにはが含まれている必要があります netgroup.byhost 地図。

DNS サーバには、NFS クライアントのフォワード（A）およびリバース（PTR）ルックアップレコードの両方が含まれている必要があります。

ネットグループ内の IPv6 アドレスを指定するときは、常に RFC 5952 で指定されているとおりに各アドレスを短縮および圧縮する必要があります。

このタスクについて

NISサーバは、と呼ばれる3つの個別のマップにネットグループ情報を格納します netgroup、netgroup.byuser`および `netgroup.byhost。の目的 netgroup.byuser および netgroup.byhost マップはネットグループ検索を高速化するためのものです。ONTAP は、マウントの応答時間を短縮するために NIS サーバ上でホスト単位のネットグループ検索を実行できます。

デフォルトでは、LDAPディレクトリにはそのようなはありません netgroup.byhost NISサーバと同様のマッピングただし、サードパーティのツールを使用すると、NISをインポートできます netgroup.byhost LDAPディレクトリにマッピングして、ホスト単位的高速ネットグループ検索を有効にします。ホスト単位のネットグループ検索を許可するようにLDAP環境を設定している場合は、を使用してONTAP LDAPクライアントを設定できます netgroup.byhost ホスト単位のネットグループ検索を高速化するために、名前、DN、および検索範囲をマッピングします。

ホスト単位のネットグループ検索の結果をより迅速に受け取ることで、ONTAP クライアントがエクスポートへのアクセスを要求した場合、より高速にエクスポートルールを処理できます。これにより、ネットグループ検索による遅延の問題によってアクセスが遅延する可能性が低下します。

## 手順

1. NISの完全な識別名を取得します netgroup.byhost LDAPディレクトリにインポートしたマップ。

マップ DN は、インポートに使用したサードパーティツールによって異なります。最高のパフォーマンスを得るには、正確なマップ DN を指定する必要があります。

2. 権限レベルを advanced に設定します。set -privilege advanced

3. Storage Virtual Machine (SVM) のLDAPクライアント設定でホスト単位のネットグループ検索を有効にします。vserver services name-service ldap client modify -vserver vserver\_name -client-config config\_name -is-netgroup-byhost-enabled true -netgroup-byhost -dn netgroup-by-host\_map\_distinguished\_name -netgroup-byhost-scope netgroup-by-host\_search\_scope

-is-netgroup-byhost-enabled {true false} LDAPディレクトリのホスト単位のネットグループ検索を有効または無効にします。デフォルトは false。

-netgroup-byhost-dn netgroup-by-host\_map\_distinguished\_name の識別名を指定します netgroup.byhost LDAPディレクトリにマッピングします。これにより、ホスト単位のネットグループ検索のベース DN が無効になります。このパラメータを指定しない場合、ONTAP は代わりにベース DN を使用します。

-netgroup-byhost-scope {base|onelevel subtree} は、ホスト単位のネットグループ検索の検索範囲を指定します。このパラメータを指定しない場合、デフォルトのが使用されます subtree。

LDAPクライアント設定がまだ存在しない場合は、を使用して新しいLDAPクライアント設定を作成するときにこれらのパラメータを指定することで、ホスト単位のネットグループ検索を有効にできます vserver services name-service ldap client create コマンドを実行します



ONTAP 9.2以降では、フィールドが表示されます -ldap-servers フィールドを置き換えます -servers。この新しいフィールドには、LDAP サーバのホスト名または IP アドレスを指定できます。

4. admin 権限レベルに戻ります。set -privilege admin

## 例

次のコマンドは、「ldap\_corp」という名前の既存のLDAPクライアント設定を変更して、を使用したホスト単位のネットグループ検索を有効にします netgroup.byhost 「nisMapName="netgroup.byhost"、dc=corp、dc=example、dc=com」という名前のマップとデフォルトの検索範囲 subtree：

```
cluster1::*> vserver services name-service ldap client modify -vserver vs1
-client-config ldap_corp -is-netgroup-byhost-enabled true -netgroup-byhost
-dn nisMapName="netgroup.byhost",dc=corp,dc=example,dc=com
```

## 完了後

。netgroup.byhost および netgroup クライアントアクセスの問題を回避するために、ディレクトリ内のマップは常に同期されている必要があります。

## 関連情報

**nsswitch**認証に**LDAP**高速バインドを使用できます

ONTAP 9.11.1以降では、`ldap_fast bind_`ルキノウ（`_コンカレントbind_`とも呼ばれます）を利用して、クライアント認証要求を迅速かつ簡単に行うことができます。この機能を使用するには、LDAPサーバが高速バインド機能をサポートしている必要があります。

このタスクについて

高速バインドを使用しない場合、ONTAP はLDAP簡易バインドを使用して、LDAPサーバで管理ユーザを認証します。この認証方式では、ONTAP がユーザまたはグループの名前をLDAPサーバに送信し、保存されているハッシュパスワードを受信して、サーバのハッシュコードをユーザパスワードからローカルに生成されたハッシュパスコードと比較します。同一の場合、ONTAP はログイン権限を付与します。

高速バインド機能を使用すると、ONTAP はセキュアな接続を介してLDAPサーバにユーザクレデンシャル（ユーザ名とパスワード）のみを送信します。LDAPサーバはこれらのクレデンシャルを検証し、ONTAP にログイン権限を付与するように指示します。

高速バインドの利点の1つは、LDAPサーバでサポートされるすべての新しいハッシュアルゴリズムをONTAP でサポートする必要がないことです。パスワードハッシュはLDAPサーバによって実行されるためです。

"高速バインドの使用方法について説明します。"

LDAP高速バインドには、既存のLDAPクライアント設定を使用できます。ただし、LDAPクライアントがTLSまたはLDAPS用に設定されていることを強く推奨します。設定されていない場合は、パスワードがプレーンテキストでネットワーク経由で送信されます。

ONTAP 環境でLDAP高速バインドを有効にするには、次の要件を満たす必要があります。

- ONTAP 管理者ユーザは、高速バインドをサポートするLDAPサーバで設定する必要があります。
- ネームサービススイッチ（nsswitch）データベースにLDAP用にONTAP SVMが設定されている必要があります。
- 高速バインドを使用してnsswitch認証を行うには、ONTAP 管理者ユーザアカウントとグループアカウントを設定する必要があります。

手順

1. LDAPサーバでLDAP高速バインドがサポートされていることをLDAP管理者に確認してください。
2. ONTAP 管理者ユーザクレデンシャルがLDAPサーバで設定されていることを確認します。
3. 管理SVMまたはデータSVMにLDAP高速バインドが正しく設定されていることを確認します。
  - a. LDAP高速バインドサーバがLDAPクライアント設定にリストされていることを確認するには、次のように入力します。

```
vserver services name-service ldap client show
```

"LDAPクライアント設定について説明します。"

- b. 確認してください `ldap` は、nsswitchに設定されているソースの1つです `passwd` データベースに次のように入力します

```
vserver services name-service ns-switch show
```

"nsswitch設定の詳細は、[こちらをご覧ください。](#)"

4. 管理ユーザがnsswitchで認証されていること、およびアカウントでLDAP高速バインド認証が有効になっていることを確認します。

- 既存のユーザの場合は、と入力します security login modify 次のパラメータ設定を確認します。

```
-authentication-method nsswitch
```

```
-is-ldap-fastbind true
```

- 新しい管理者ユーザについては、を参照してください "[LDAPまたはNISアカウントアクセスを有効にします。](#)"

**LDAP統計を表示します。**

ONTAP 9.2 以降では、パフォーマンスを監視して問題を診断するために、ストレージシステム上の Storage Virtual Machine (SVM) の LDAP 統計を表示することができます。

必要なもの

- SVM で LDAP クライアントを設定しておく必要があります。
- データを表示できる LDAP オブジェクトを特定しておく必要があります。

ステップ

1. カウンタオブジェクトのパフォーマンスデータを表示します。

```
statistics show
```

例

次の例は、オブジェクトのパフォーマンスデータを表示します secd\_external\_service\_op :

```
cluster::*> statistics show -vserver vserverName -object
secd_external_service_op -instance "vserverName:LDAP (NIS & Name
Mapping):GetUserInfoFromName:1.1.1.1"
```

Object: secd\_external\_service\_op

Instance: vserverName:LDAP (NIS & Name

Mapping):GetUserInfoFromName:1.1.1.1

Start-time: 4/13/2016 22:15:38

End-time: 4/13/2016 22:15:38

Scope: vserverName

Counter	Value
instance_name	vserverName:LDAP (NIS & Name Mapping):GetUserInfoFromName: 1.1.1.1
last_modified_time	1460610787
node_name	nodeName
num_not_found_responses	1
num_request_failures	1
num_requests_sent	1
num_responses_received	1
num_successful_responses	0
num_timeouts	0
operation	GetUserInfoFromName
process_name	secd
request_latency	52131us

## ネームマッピングを設定する

### ネームマッピングの概要を設定する

ONTAPでは、ネームマッピングを使用して、SMB IDをUNIX IDに、Kerberos IDをUNIX IDに、UNIX IDをSMB IDにマッピングします。この情報は、NFSクライアントとSMBクライアントのどちらから接続しているかに関係なく、ユーザクレデンシャルを取得して適切なファイルアクセスを提供するために必要です。

ネームマッピングを使用する必要がない例外が2つあります。

- 純粋な UNIX 環境を構成しており、ボリュームに対して SMB アクセスや NTFS セキュリティ形式を使用する予定がない場合。
- 代わりにデフォルトユーザを使用するように設定している場合。

このシナリオでは、すべてのクライアントクレデンシャルを個別にマッピングするのではなく、すべてのクライアントクレデンシャルが同じデフォルトユーザにマッピングされるため、ネームマッピングは必要ありません。



ネームマッピングはユーザに対してのみ使用でき、グループに対しては使用できません。

ただし、個々のユーザのグループを特定のユーザにマッピングすることはできます。たとえば、SALES という単語が先頭または末尾に付くすべての AD ユーザを、特定の UNIX ユーザおよびそのユーザの UID にマッピングできます。

#### ネームマッピングの仕組み

ONTAP がユーザのクレデンシャルをマッピングする必要がある場合、最初に、ローカルのネームマッピングデータベースおよび LDAP サーバで既存のマッピングの有無をチェックします。一方をチェックするか両方をチェックするか、およびそのチェック順序は、SVM のネームサービスの設定で決まります。

- Windows から UNIX へのマッピングの場合

マッピングが見つからなかった場合、ONTAP は小文字の Windows ユーザ名が UNIX ドメインで有効なユーザ名かどうかをチェックします。設定されている場合は、デフォルトの UNIX ユーザが使用されます。デフォルトの UNIX ユーザが設定されておらず、この方法でも ONTAP がマッピングを取得できない場合、マッピングは失敗し、エラーが返されます。

- UNIX から Windows へのマッピングの場合

マッピングが見つからなかった場合、ONTAP は SMB ドメインで UNIX 名と一致する Windows アカウントを探します。正しく設定されていない場合は、デフォルトの SMB ユーザが使用されます。デフォルトの SMB ユーザが設定されておらず、この方法でも ONTAP がマッピングを取得できない場合、マッピングは失敗し、エラーが返されます。

マシンアカウントは、デフォルトでは、指定したデフォルトの UNIX ユーザにマッピングされます。デフォルトの UNIX ユーザを指定しないと、マシンアカウントのマッピングは失敗します。

- ONTAP 9.5 以降では、マシンアカウントをデフォルトの UNIX ユーザ以外のユーザにマッピングできます。
- ONTAP 9.4 以前では、マシンアカウントを他のユーザにマッピングすることはできません。

マシンアカウントに定義されているネームマッピングがあっても無視されます。

#### UNIX ユーザから Windows ユーザへのネームマッピングのためのマルチドメイン検索

ONTAP は、UNIX ユーザを Windows ユーザにマッピングする際のマルチドメイン検索をサポートしています。一致する結果が返されるまで、検出されたすべての信頼できるドメインで、変換後のパターンに一致する名前が検索されます。また、信頼できる優先ドメインのリストを設定することもできます。このリストは、検出された信頼できるドメインのリストの代わりに使用され、一致する結果が返されるまで順に検索されます。

#### ドメインの信頼性が UNIX ユーザから Windows ユーザへのネームマッピング検索に与える影響

マルチドメインのユーザ名マッピングの仕組みを理解するには、ドメインの信頼性が ONTAP に与える影響を理解しておく必要があります。SMB サーバのホームドメインとの Active Directory 信頼関係は、双方向の信頼にすることも、インバウンドまたはアウトバウンドの2種類の単方向の信頼のいずれかにすることもできます。ホームドメインは、SVM 上の SMB サーバが属しているドメインです。

• 双方向の信頼

双方向の信頼では、両方のドメインが相互に信頼しています。SMBサーバのホームドメインが別のドメインと双方向の信頼関係にある場合、ホームドメインは信頼できるドメインに属するユーザを認証および許可できます。その逆も同様です。

UNIX ユーザから Windows ユーザへのネームマッピング検索は、ホームドメインと他方のドメインの間に双方向の信頼関係が確立されたドメインでのみ実行できます。

• アウトバウンドの信頼

アウトバウンドの信頼では、ホームドメインが他方のドメインを信頼しています。この場合、ホームドメインはアウトバウンドの信頼できるドメインに属しているユーザを認証および認可できます。

ホームドメインとアウトバウンドの信頼関係にあるドメインは、UNIX ユーザから Windows ユーザへのネームマッピング検索の実行時に `_not_searched` になります。

• インバウンドの信頼

インバウンドの信頼では、もう一方のドメインがSMBサーバのホームドメインを信頼します。この場合、ホームドメインはインバウンドの信頼できるドメインに属しているユーザを認証または認可できません。

ホームドメインとインバウンドの信頼関係にあるドメインは、UNIX ユーザから Windows ユーザへのネームマッピング検索の実行時に `_not_searched` になります。

ワイルドカード（\*）を使用したネームマッピングのためのマルチドメイン検索の設定

マルチドメインネームマッピング検索は、Windows ユーザ名のドメインセクションにワイルドカードを使用することで容易になります。次の表に、マルチドメイン検索を有効にするためにネームマッピングエントリのドメイン部にワイルドカードを使用する方法を示します。

パターン（Pattern）	交換	結果
ルート	{ Asterisk } { backslash } { backslash } 管理者	UNIX ユーザ「root」は「administrator」という名前のユーザにマッピングされます。「administrator」という名前の最初の一致するユーザが見つかるまで、すべての信頼できるドメインが順に検索されます。

パターン ( <b>Pattern</b> )	交換	結果
*	<pre>{ Asterisk }   { backslash }   { backslash }   { Asterisk }</pre>	<p>有効な UNIX ユーザは、対応する Windows ユーザにマッピングされます。該当する名前のユーザとの最初の一致が見つかるまで、すべての信頼できるドメインが順に検索されます。</p> <div>  <p>パターン { Asterisk } { backslash } { backslash } { Asterisk } は、UNIX から Windows へのネームマッピングでのみ有効で、反対方向では無効です。</p> </div>

## マルチドメインの名前検索の実行方法

マルチドメインの名前検索に使用する信頼できるドメインのリストを決定する方法は 2 つあります。

- ONTAP で作成された自動検出された双方向の信頼リストを使用します
- 自分で作成した信頼できる優先ドメインリストを使用します

ユーザ名のドメインセクションにワイルドカードを使用して UNIX ユーザが Windows ユーザにマッピングされている場合、Windows ユーザはすべての信頼できるドメインで次のように検索されます。

- 信頼できるドメインの優先リストが設定されている場合、マッピング先の Windows ユーザはこの検索リスト内でのみ順に検索されます。
- 信頼できるドメインの優先リストが設定されていない場合は、ホームドメインと双方向の信頼関係にあるすべてのドメインで Windows ユーザの検索が行われます。
- ホームドメインと双方向の信頼関係にあるドメインが存在しない場合、ホームドメインでユーザの検索が行われます。

UNIX ユーザがユーザ名にドメインセクションのない Windows ユーザにマッピングされている場合は、ホームドメインで Windows ユーザの検索が行われます。

## ネームマッピングの変換ルール

ONTAP システムには、SVM ごとに一連の変換ルールが保存されています。各ルールは、`a_pattern_` と `a_replacement_` の 2 つの要素で構成されます。変換は該当するリストの先頭から開始され、最初に一致したルールに基づいて実行されます。パターンは UNIX 形式の正規表現です。リプレースメントは、UNIX のように、パターンのサブ式を表すエスケープシーケンスを含む文字列です `sed` プログラム。

ネームマッピングを作成します

を使用できます `vserver name-mapping create` コマンドを使用してネームマッピングを作成します。ネームマッピングを使用すると、Windows ユーザから UNIX セキュリティ形式のボリュームへのアクセスおよびその逆方向のアクセスが可能になります。

このタスクについて

ONTAP では、SVM ごとに、各方向について最大 12、500 個のネームマッピングがサポートされます。

ステップ

1. ネームマッピングを作成します。

```
vserver name-mapping create -vserver vserver_name -direction {krb-unix|win-unix|unix-win} -position integer -pattern text -replacement text
```



。 `-pattern` および `-replacement` ステートメントは正規表現として記述できます。を使用することもできます `-replacement null` 置換文字列を使用してユーザへのマッピングを明示的に拒否するステートメント " " (スペース文字)。を参照してください `vserver name-mapping create` のマニュアルページを参照してください。

Windows から UNIX へのマッピングを作成した場合、新しいマッピングが作成されたときに ONTAP システムに接続していたすべての SMB クライアントは、新しいマッピングを使用するために、一度ログアウトしてから、再度ログインする必要があります。

例

次のコマンドは、`vs1` という名前の SVM 上にネームマッピングを作成します。このマッピングは UNIX から Windows へのマッピングで、優先順位リスト内での位置は 1 番目です。UNIX ユーザ `johnd` を Windows ユーザ `ENG\JohnDoe` にマッピングします。

```
vs1::> vserver name-mapping create -vserver vs1 -direction unix-win
-position 1 -pattern johnd
-replacement "ENG\\JohnDoe"
```

次のコマンドは、`vs1` という名前の SVM 上に別のネームマッピングを作成します。このマッピングは Windows から UNIX へのマッピングで、優先順位リスト内での位置は 1 番目です。パターンとリプレースメントには正規表現が使用されています。このマッピングにより、ドメイン `ENG` 内のすべての CIFS ユーザが、SVM に関連付けられた LDAP ドメイン内のユーザにマッピングされます。

```
vs1::> vserver name-mapping create -vserver vs1 -direction win-unix
-position 1 -pattern "ENG\\(.+)"
-replacement "\\1"
```

次のコマンドは、`vs1` という名前の SVM 上に別のネームマッピングを作成します。このパターンには、エスケープする必要がある Windows ユーザ名の要素として「`$`」が含まれています。Windows ユーザ `ENG\john$ops` を UNIX ユーザ `john_ops` にマッピングします。

```
vs1::> vsriver name-mapping create -direction win-unix -position 1
-pattern ENG\\john\$ops
-replacement john_ops
```

デフォルトユーザを設定します。

ユーザに対する他のマッピングの試行がすべて失敗した場合や、UNIX と Windows の間で個々のユーザをマッピングしないようにする場合に使用するデフォルトユーザを設定できます。ただし、マッピングされていないユーザの認証を失敗にする場合は、デフォルトユーザを設定しないでください。

このタスクについて

CIFS 認証で、各 Windows ユーザを個別の UNIX ユーザにマッピングしないようにする場合は、代わりにデフォルトの UNIX ユーザを指定できます。

NFS 認証で、各 UNIX ユーザを個別の Windows ユーザにマッピングしないようにする場合は、代わりにデフォルトの Windows ユーザを指定できます。

ステップ

1. 次のいずれかを実行します。

状況	入力するコマンド
デフォルトの UNIX ユーザを設定する	<code>vsriver cifs options modify -default-unix-user user_name</code>
デフォルトの Windows ユーザを設定します	<code>vsriver nfs modify -default-win-user user_name</code>

ネームマッピングの管理用コマンド

ONTAP には、ネームマッピングを管理するためのコマンドが用意されています。

状況	使用するコマンド
ネームマッピングを作成します	<code>vsriver name-mapping create</code>
特定の位置にネームマッピングを挿入します	<code>vsriver name-mapping insert</code>
ネームマッピングを表示します	<code>vsriver name-mapping show</code>

2つのネームマッピングの位置を入れ替えます 注：ネームマッピングにIP修飾子エントリが設定されている場合、スワップは許可されません。	<code>vserver name-mapping swap</code>
ネームマッピングを変更する	<code>vserver name-mapping modify</code>
ネームマッピングを削除する	<code>vserver name-mapping delete</code>
ネームマッピングが正しいことを確認します	<code>vserver security file-directory show-effective-permissions -vserver vs1 -win-user-name user1 -path / -share-name sh1</code>

詳細については、各コマンドのマニュアルページを参照してください。

### Windows NFS クライアントのアクセスを有効にします

ONTAP は Windows NFSv3 クライアントからのファイルアクセスをサポートしています。つまり、NFSv3をサポートするWindowsオペレーティングシステムを実行しているクライアントは、クラスタのNFSv3エクスポートのファイルにアクセスできます。この機能を正しく使用するには、Storage Virtual Machine（SVM）を適切に設定し、一定の要件と制限事項に注意する必要があります。

このタスクについて

デフォルトでは、Windows NFSv3 クライアントサポートが無効になっています。

作業を開始する前に

SVM で NFSv3 が有効になっている必要があります。

手順

1. Windows NFSv3 クライアントのサポートを有効にします。

```
vserver nfs modify -vserver svm_name -v3-ms-dos-client enabled -mount-rootonly disabled
```

2. Windows NFSv3クライアントをサポートするすべてのSVMで、を無効にします `-enable-ejukebox` および `-v3-connection-drop` パラメータ：

```
vserver nfs modify -vserver vserver_name -enable-ejukebox false -v3-connection-drop disabled
```

これで、Windows NFSv3 クライアントがストレージシステムにエクスポートをマウントできるようになります。

3. を指定して、各Windows NFSv3クライアントがハードマウントを使用するようにします `-o mtype=hard` オプション

これは、マウントの信頼性を確保するために必要です。

```
mount -o mtype=hard \\10.53.33.10\vol\vol1 z:\
```

## NFS クライアントで NFS エクスポートの表示を有効にします

NFSクライアントはを使用できます `showmount -e` コマンドを使用して、ONTAP NFS サーバから使用可能なエクスポートのリストを表示します。これは、ユーザがマウントするファイルシステムを確認するのに役立ちます。

ONTAP 9.2 以降 ONTAP では、NFS クライアントでのエクスポートリストの表示がデフォルトで許可されます。以前のリリースでは `showmount` のオプション `vserver nfs modify` コマンドは明示的に有効にする必要があります。エクスポートリストを表示するには、SVM で NFSv3 が有効になっている必要があります。

### 例

次のコマンドは、`vs1` という SVM に対して `showmount` を実行します。

```
cluster1 : : > vserver nfs show -vserver vs1 -fields showmount
vserver showmount
-----
vs1      enabled
```

次のコマンドは、IP アドレスが 10.63.21.9 の NFS サーバ上のエクスポートのリストを表示します。

```
showmount -e 10.63.21.9
Export list for 10.63.21.9:
/unix      (everyone)
/unix/unix1 (everyone)
/unix/unix2 (everyone)
/          (everyone)
```

## NFSを使用したファイルアクセスの管理

### NFSv3 を有効または無効にします

NFSv3を有効または無効にするには、を変更します `-v3` オプションこれにより、NFSv3 プロトコルを使用してクライアントがファイルにアクセスできるようになります。デフォルトでは、NFSv3 が有効になっています。

### ステップ

1. 次のいずれかを実行します。

状況	入力するコマンド
----	----------

NFSv3 を有効にします	<code>vserver nfs modify -vserver vserver_name -v3 enabled</code>
NFSv3を無効にする	<code>vserver nfs modify -vserver vserver_name -v3 disabled</code>

#### NFSv4.0 を有効または無効にする

NFSv4.0を有効または無効にするには、`-v4.0` オプションこれにより、NFSv4.0 プロトコルを使用してクライアントがファイルにアクセスできるかどうかを指定できます。ONTAP 9.9.1では、NFSv4.0がデフォルトで有効になります。それより前のリリースでは、デフォルトで無効になっていました。

##### ステップ

1. 次のいずれかを実行します。

状況	入力するコマンド
NFSv4.0 を有効にする	<code>vserver nfs modify -vserver vserver_name -v4.0 enabled</code>
NFSv4.0 を無効にする	<code>vserver nfs modify -vserver vserver_name -v4.0 disabled</code>

#### NFSv4.1を有効または無効にする

NFSv4.1を有効または無効にするには、`-v4.1` オプションこれにより、NFSv4.1プロトコルを使用してクライアントがファイルにアクセスできるようになります。ONTAP 9.9.1では、NFSv4.1がデフォルトで有効になります。以前のリリースでは、デフォルトで無効になっていました。

##### ステップ

1. 次のいずれかを実行します。

状況	入力するコマンド
NFSv4.1を有効にする	<code>vserver nfs modify -vserver vserver_name -v4.1 enabled</code>
NFSv4.1を無効にする	<code>vserver nfs modify -vserver vserver_name -v4.1 disabled</code>



## NFSv4ストレージプールの制限を管理します

ONTAP 9.13以降では、クライアントあたりのストレージプールのリソース制限に達したときに、NFSv4サーバがNFSv4クライアントに対するリソースを拒否するように設定できます。クライアントがNFSv4ストレージプールリソースを大量に消費すると、NFSv4ストレージプールリソースが使用できないために他のNFSv4クライアントがブロックされる可能性があります。

この機能を有効にすると、各クライアントによるアクティブなストレージプールリソース消費量を表示することもできます。これにより、システムリソースを使い果たしているクライアントを識別しやすくなり、クライアントごとのリソース制限を課すことができます。

消費されたストレージプールリソースを表示します

。 `vserver nfs storepool show` コマンドは、消費されたストレージプールリソースの数を表示します。ストレージプールは、NFSv4クライアントが使用するリソースのプールです。

### ステップ

1. 管理者としてを実行します `vserver nfs storepool show` コマンドを使用してNFSv4クライアントのstorepool情報を表示します。

### 例

次の例は、NFSv4クライアントのストレージプール情報を表示します。

```
cluster1::*> vserver nfs storepool show

Node: node1

Vserver: vs1

Data-IP: 10.0.1.1

Client-IP Protocol IsTrunked OwnerCount OpenCount DelegCount LockCount
-----
-----
10.0.2.1      nfs4.1      true      2 1 0 4
10.0.2.2      nfs4.2      true      2 1 0 4

2 entries were displayed.
```

ストレージプール制限の制御を有効または無効にします

管理者は、次のコマンドを使用して、ストレージプールの制限制御を有効または無効にできます。

## ステップ

1. 管理者は、次のいずれかの操作を実行します。

状況	入力するコマンド
ストレージプール制限の制御を有効にします	<code>vserver nfs storepool config modify -limit-enforce enabled</code>
ストレージプール制限の制御を無効にします	<code>vserver nfs storepool config modify -limit-enforce disabled</code>

ブロックされたクライアントのリストを表示します

ストレージプール制限が有効になっている場合、管理者は、クライアントごとのリソースしきい値に達したときにブロックされたクライアントを確認できます。管理者は次のコマンドを使用して、ブロックされたクライアントとしてマークされているクライアントを確認できます。

## 手順

1. を使用します `vserver nfs storepool blocked-client show` コマンドを使用してNFSv4ブロッククライアントリストを表示します。

ブロックされたクライアントリストからクライアントを削除します

クライアントあたりのしきい値に達したクライアントは切断され、ブロッククライアントキャッシュに追加されます。管理者は次のコマンドを使用して、ブロッククライアントキャッシュからクライアントを削除できます。これにより、クライアントはONTAP NFSv4サーバに接続できるようになります。

## 手順

1. を使用します `vserver nfs storepool blocked-client flush -client-ip <ip address>` コマンドを実行して、storepoolブロックされたクライアントキャッシュをフラッシュします。
2. を使用します `vserver nfs storepool blocked-client show` コマンドを使用して、クライアントがブロッククライアントキャッシュから削除されたことを確認します。

## 例

この例では、IPアドレスが「10.2.1.1」のブロックされたクライアントがすべてのノードからフラッシュされています。

```
cluster1::*>vserver nfs storepool blocked-client flush -client-ip 10.2.1.1

cluster1::*>vserver nfs storepool blocked-client show

Node: node1

Client IP
-----
10.1.1.1

1 entries were displayed.
```

## pNFS を有効または無効にします

pNFS は、NFS クライアントがストレージデバイスに対する読み取り / 書き込み処理を直接かつ並行して実行し、ボトルネックとなる可能性がある NFS サーバをバイパスできるようにすることで、パフォーマンスを向上します。pNFS (Parallel NFS) を有効または無効にするには、を変更します `-v4.1-pnfs` オプション

ONTAP リリースの種類	pNFS のデフォルト値
9.8以降	無効
9.7以前	有効

## 必要なもの

pNFS を使用するには、NFSv4.1 のサポートが必要です。

pNFS を有効にする場合は、まず NFS リファラールを無効にする必要があります。両方を同時に有効にすることはできません。

SVM で pNFS と Kerberos を併用する場合は、SVM 上のすべての LIF で Kerberos を有効にする必要があります。

## ステップ

1. 次のいずれかを実行します。

状況	入力するコマンド
pNFS を有効にします	<code>vserver nfs modify -vserver vserver_name -v4.1-pnfs enabled</code>
pNFS を無効にします	<code>vserver nfs modify -vserver vserver_name -v4.1-pnfs disabled</code>

## 関連情報

## • NFS トランキングの概要

### TCP および UDP 経由の NFS アクセスを制御します

TCP および UDP 経由の Storage Virtual Machine (SVM) への NFS アクセスを有効または無効にするには、を変更します `-tcp` および `-udp` パラメータを指定します。これにより、環境で NFS クライアントが TCP または UDP 経由でデータにアクセスできるかどうかを制御できます。

このタスクについて

これらのパラメータは NFS のみに適用されます。補助プロトコルには影響しません。たとえば、TCP 経由の NFS が無効になっていても、TCP 経由でのマウント処理は成功します。TCP または UDP トラフィックを完全にブロックするには、エクスポートポリシールールを使用します。



コマンドの失敗を防ぐために、NFS に対して TCP を無効にする前に SnapDiff RPC サーバをオフにする必要があります。TCP を無効にするには、コマンドを使用します `vserver snapdiff-rpc-server off -vserver vserver name`。

### ステップ

1. 次のいずれかを実行します。

設定する NFS アクセスの状態	入力するコマンド
TCP 経由で有効化	<code>vserver nfs modify -vserver vserver_name -tcp enabled</code>
TCP 経由で無効化	<code>vserver nfs modify -vserver vserver_name -tcp disabled</code>
UDP 経由で有効化	<code>vserver nfs modify -vserver vserver_name -udp enabled</code>
UDP 経由で無効にしました	<code>vserver nfs modify -vserver vserver_name -udp disabled</code>

### 非予約ポートからの NFS 要求を制御します

非予約ポートからの NFS マウント要求を拒否するには、を有効にします `-mount -rootonly` オプション  
非予約ポートからのすべての NFS 要求を拒否するには、を有効にします `-nfs-rootonly` オプション

このタスクについて

デフォルトでは、オプションです `-mount-rootonly` はです `enabled`。

デフォルトでは、オプションです `-nfs-rootonly` はです `disabled`。

これらのオプションは、NULL 手順には適用されません。

### ステップ

1. 次のいずれかを実行します。

状況	入力するコマンド
非予約ポートからの NFS マウント要求を許可します	<code>vserver nfs modify -vserver vserver_name -mount -rootonly disabled</code>
非予約ポートからの NFS マウント要求を拒否します	<code>vserver nfs modify -vserver vserver_name -mount -rootonly enabled</code>
非予約ポートからのすべての NFS 要求を許可します	<code>vserver nfs modify -vserver vserver_name -nfs -rootonly disabled</code>
非予約ポートからのすべての NFS 要求を拒否します	<code>vserver nfs modify -vserver vserver_name -nfs -rootonly enabled</code>

不明な **UNIX** ユーザ向けに、**NTFS** ボリュームまたは **qtree** への **NFS** アクセスを処理する

ONTAP は、NTFS セキュリティ形式のボリュームまたは qtree への接続を試みる UNIX ユーザを識別できない場合、そのユーザを Windows ユーザに明示的にマッピングできません。ONTAP は、セキュリティを厳しくするためにそのようなユーザに対してアクセスを拒否するように設定することも、そうしたユーザをデフォルトの Windows ユーザにマッピングしてすべてのユーザに最小限のレベルのアクセスを保証するように設定することもできます。

必要なもの

このオプションを有効にする場合は、デフォルトの Windows ユーザを設定する必要があります。

このタスクについて

UNIX ユーザが NTFS セキュリティ形式のボリュームまたは qtree へのアクセスを試みる場合、その UNIX ユーザは、ONTAP が NTFS アクセス権を適切に評価できるように、まず Windows ユーザにマッピングされている必要があります。ただし、ONTAP は、設定されているユーザ情報ネームサービスソースでその UNIX ユーザの名前を検索できなかった場合、特定の Windows ユーザにその UNIX ユーザを明示的にマッピングすることができません。このような不明な UNIX ユーザの処理方法は、次の方法で決定できます。

- 不明な UNIX ユーザに対してアクセスを拒否する。

この場合、NTFS ボリュームまたは qtree へのアクセス権を取得するためにすべての UNIX ユーザに明示的なマッピングを要求することで、より厳しいセキュリティが適用されます。

- 不明な UNIX ユーザをデフォルトの Windows ユーザにマッピングする。

これにより、セキュリティは低下しますが、すべてのユーザがデフォルトの Windows ユーザを介して NTFS ボリュームまたは qtree への最小限のレベルのアクセス権を取得できるようになるため、利便性が向上します。

手順

1. 権限レベルを **advanced** に設定します。

```
set -privilege advanced
```

2. 次のいずれかを実行します。

不明な UNIX ユーザへのデフォルトの Windows ユーザのマッピング	入力するコマンド
有効	<code>vserver nfs modify -vserver vserver_name -map -unknown-uid-to-default-windows-user enabled</code>
無効	<code>vserver nfs modify -vserver vserver_name -map -unknown-uid-to-default-windows-user disabled</code>

3. admin 権限レベルに戻ります。

```
set -privilege admin
```

非予約ポートを使用して **NFS** エクスポートをマウントするクライアントに関する注意事項

。 `-mount-rootoonly` 非予約ポートを使用して NFS エクスポートをマウントするクライアントをサポートする必要があるストレージシステムでは、ユーザが root としてログインしている場合でも、オプションを無効にする必要があります。Hummingbird クライアントや Solaris NFS / IPv6 クライアントがこれに該当します。

状況に応じて `-mount-rootoonly` オプションが有効になっている場合、ONTAP では、非予約ポート（1、023 より大きいポート）を使用する NFS クライアントで NFS エクスポートをマウントすることはできません。

ドメインを検証してネットグループのより厳密なアクセスチェックを実行します

デフォルトでは、ONTAP はネットグループに対するクライアントアクセスを評価する際に追加の検証を実行します。この追加チェックにより、クライアントのドメインが Storage Virtual Machine（SVM）のドメイン設定に一致していることが確認されます。一致しない場合、ONTAP はクライアントアクセスを拒否します。

このタスクについて

ONTAP は、クライアントアクセス用のエクスポートポリシールールおよびネットグループが含まれているエクスポートポリシールールを評価する際に、クライアントの IP アドレスがそのネットグループに属しているかどうかを ONTAP が確認する必要があります。そのために、ONTAP は、DNS を使用してクライアントの IP アドレスをホスト名に変換し、Fully Qualified Domain Name（FQDN；完全修飾ドメイン名）を取得します。

ネットグループファイルにホストの短い名前のみがリストされていて、そのホストの短い名前が複数のドメインに存在している場合は、異なるドメインのクライアントがこのチェックなしでアクセス権を取得することが可能です。

この問題を回避するために、ONTAP は、ホストについて DNS から返されたドメインを SVM 用に設定されている DNS ドメイン名のリストと比較します。一致した場合は、アクセスが許可されます。一致しない場合、アクセスは拒否されます。

この検証はデフォルトで有効になっています。これを管理するには、を変更します `-netgroup-dns-domain-search` パラメータ。advanced権限レベルで使用できます。

#### 手順

1. 権限レベルを advanced に設定します。

```
set -privilege advanced
```

2. 必要な操作を実行します。

ネットグループのドメイン検証の設定	入力するコマンド
有効	<pre>vserver nfs modify -vserver vserver_name -netgroup-dns-domain -search enabled</pre>
無効	<pre>vserver nfs modify -vserver vserver_name -netgroup-dns-domain -search disabled</pre>

3. 権限レベルを admin に設定します。

```
set -privilege admin
```

#### NFSv3 サービスで使用するポートを変更します

ストレージシステム上の NFS サーバは、マウントデーモンや Network Lock Manager などのサービスを使用して、特定のデフォルトネットワークポート経由で NFS クライアントと通信します。デフォルトポートは、ほとんどの NFS 環境で正しく機能するので変更する必要はありませんが、別の NFS ネットワークポートを NFSv3 環境で使用する場合はそうすることができます。

#### 必要なもの

ストレージシステムで NFS ポートを変更するには、すべての NFS クライアントがシステムに再接続する必要があるため、変更前先立ってこの情報をユーザに伝えておく必要があります。

#### このタスクについて

NFS マウントデーモン、Network Lock Manager（NLM；ネットワークロックマネージャ）、Network Status Monitor（NSM；ネットワークステータスマニタ）、および NFS クォータデーモンの各サービスで使用するポートを Storage Virtual Machine（SVM）ごとに設定できます。ポート番号の変更は、TCP と UDP の両方でデータにアクセスする NFS クライアントに影響します。

NFSv4 および NFSv4.1 のポートは変更できません。

#### 手順

1. 権限レベルを advanced に設定します。

```
set -privilege advanced
```

2. NFS へのアクセスを無効にします。

```
vserver nfs modify -vserver vserver_name -access false
```

3. 特定の NFS サービスの NFS ポートを設定します。

```
vserver nfs modify -vserver vserver_name nfs_port_parameter port_number
```

NFS ポートのパラメータ	説明	デフォルトのポート
-mountd-port	NFS マウントデーモン	635
-nlm-port	Network Lock Manager の略	4045
-nsm-port	Network Status Monitor サービスの略	4046
-rquotad-port	NFS クォータデーモン	4049

デフォルトポートに加えて、1、024~65、535 の範囲のポート番号を使用できます。各 NFS サービスは一意のポートを使用する必要があります。

4. NFS へのアクセスを有効にします。

```
vserver nfs modify -vserver vserver_name -access true
```

5. を使用します network connections listening show ポート番号の変更を確認するコマンド。

6. admin 権限レベルに戻ります。

```
set -privilege admin
```

例

次のコマンドは、vs1 という SVM で NFS マウントデーモンのポートを 1113 に設定します。



```

vs1::> set -privilege advanced
Warning: These advanced commands are potentially dangerous; use
        them only when directed to do so by NetApp personnel.
Do you want to continue? {y|n}: y

vs1::*> vserver nfs modify -vserver vs1 -access false

vs1::*> vserver nfs modify -vserver vs1 -mountd-port 1113

vs1::*> vserver nfs modify -vserver vs1 -access true


vs1::*> network connections listening show
Vserver Name      Interface Name:Local Port      Protocol/Service
-----
Node: cluster1-01
Cluster           cluster1-01_clus_1:7700        TCP/ctlopccp
vs1               data1:4046                   TCP/sm
vs1               data1:4046                   UDP/sm
vs1               data1:4045                   TCP/nlm-v4
vs1               data1:4045                   UDP/nlm-v4
vs1               data1:1113                   TCP/mount
vs1               data1:1113                   UDP/mount
...
vs1::*> set -privilege admin

```

**NFS** サーバを管理するためのコマンドです

ONTAP には、NFS サーバを管理するためのコマンドが用意されています。

状況	使用するコマンド
NFS サーバを作成します	<code>vserver nfs create</code>
NFS サーバを表示する	<code>vserver nfs show</code>
NFS サーバを変更する	<code>vserver nfs modify</code>
NFS サーバを削除する	<code>vserver nfs delete</code>

を非表示にします .snapshot NFSv3マウントポイント下のディレクトリリスト	vserver nfs を使用したコマンド -v3-hide-snapshot オプションを有効にします
 <p>への明示的なアクセス .snapshot このオプションが有効になっていても、ディレクトリは許可されます。</p>	

詳細については、各コマンドのマニュアルページを参照してください。

## ネームサービスの問題をトラブルシューティングする

ネームサービスの問題でクライアントでアクセスエラーが発生した場合は、を使用できます `vserver services name-service getxxbyyy` さまざまなネームサービス検索を手動で実行し、検索の詳細と結果を調べてトラブルシューティングに役立てるためのコマンドファミリー。

このタスクについて

- 各コマンドでは、次の情報を指定できます。
    - 検索を実行するノードまたは Storage Virtual Machine （ SVM ） の名前。

これにより、特定のノードまたは SVM でネームサービス検索をテストして、想定されるネームサービス設定問題の検索を絞り込むことができます。

  - 検索に使用されるソースを表示するかどうか。
- これにより、正しいソースが使用されているかどうかを確認できます。
- ONTAP は、設定されているネームサービススイッチの順序に基づいて、検索を実行するためのサービスを選択します。
  - これらのコマンドは advanced 権限レベルで使用できます。

## 手順

- 次のいずれかを実行します。

取得する情報	使用するコマンド
ホスト名のIPアドレス	<code>vserver services name-service getxxbyyy getaddrinfo</code> <code>vserver services name-service getxxbyyy gethostbyname</code> (IPv4アドレスのみ)
グループIDごとのグループのメンバー	<code>vserver services name-service getxxbyyy getgrbygid</code>

グループ名ごとのグループのメンバー	<code>vserver services name-service getxxbyyy getgrbyname</code>
ユーザが属しているグループのリスト	<code>vserver services name-service getxxbyyy getgrlist</code>
IPアドレスのホスト名	<code>vserver services name-service getxxbyyy getnameinfo vserver services name- service getxxbyyy gethostbyaddr (IPv4アド レスのみ)</code>
ユーザ名別のユーザ情報	<code>vserver services name-service getxxbyyy getpwbyname</code> RBACユーザの名前解決をテストする には、を指定します <code>-use-rbac</code> パラメータの形式 <code>true</code> 。
ユーザIDごとのユーザ情報	<code>vserver services name-service getxxbyyy getpwbyuid</code> RBACユーザの名前解決をテストするには、を指定し ます <code>-use-rbac</code> パラメータの形式 <code>true</code> 。
クライアントのネットグループメンバーシップ	<code>vserver services name-service getxxbyyy netgrp</code>
ホスト単位のネットグループ検索を使用したクライ アントのネットグループメンバーシップ	<code>vserver services name-service getxxbyyy netgrpbyhost</code>

次の例は、ホスト `acast1.eng.example.com` のIPアドレスの取得を試みることでSVM `vs1` のDNSルックアップをテストします。

```
cluster1::*> vserver services name-service getxxbyyy getaddrinfo -vserver
vs1 -hostname acast1.eng.example.com -address-family all -show-source true
Source used for lookup: DNS
Host name: acast1.eng.example.com
Canonical Name: acast1.eng.example.com
IPv4: 10.72.8.29
```

次の例は、501768というUIDを持つユーザのユーザ情報の取得を試みることでSVM `vs1` のNIS検索をテストします。

```
cluster1::~*> vserver services name-service getxxbyyy getpwbyuid -vserver
vs1 -userID 501768 -show-source true
Source used for lookup: NIS
pw_name: jsmith
pw_passwd: $1$y8rA4XX7$/DDOXAvC2PC/IsNFozfIN0
pw_uid: 501768
pw_gid: 501768
pw_gecos:
pw_dir: /home/jsmith
pw_shell: /bin/bash
```

次の例は、ldap1というユーザのユーザ情報の取得を試みることでSVM vs1のLDAP検索をテストします。

```
cluster1::~*> vserver services name-service getxxbyyy getpwbyname -vserver
vs1 -username ldap1 -use-rbac false -show-source true
Source used for lookup: LDAP
pw_name: ldap1
pw_passwd: {crypt}JSPM6yc/ilIX6
pw_uid: 10001
pw_gid: 3333
pw_gecos: ldap1 user
pw_dir: /u/ldap1
pw_shell: /bin/csh
```

次の例は、クライアントdnshost0がネットグループlnetgroup136のメンバーであるかどうかを調べることでSVM vs1のネットグループ検索をテストします。

```
cluster1::~*> vserver services name-service getxxbyyy netgrp -vserver vs1
-netgroup lnetgroup136 -client dnshost0 -show-source true
Source used for lookup: LDAP
dnshost0 is a member of lnetgroup136
```

1. 実行したテストの結果を分析し、必要な措置を取ります。

状況	を確認します
ホスト名または IP アドレスの検索に失敗したか、 正しくない結果が得られました	DNS設定
検索で間違ったソースが照会されました	ネームサービススイッチの設定

状況	を確認します
ユーザまたはグループの検索に失敗したか、正しくない結果が得られた	<ul style="list-style-type: none"> <li>• ネームサービススイッチの設定</li> <li>• ソースの設定（ローカルファイル、NISドメイン、LDAPクライアント）</li> <li>• ネットワーク設定（LIF、ルートなど）</li> </ul>
ホスト名の検索に失敗したかタイムアウトになり、DNSの短縮名（例：host1）がDNSサーバで解決されない	Top-Level Domain（TLD；最上位レベルのドメイン）クエリのDNS設定。を使用して、TLDクエリを無効にできます <code>-is-tld-query-enabled false</code> オプションをに設定します <code>vserver services name-service dns modify</code> コマンドを実行します

## 関連情報

"[ネットアップテクニカルレポート 4668](#)：『[Name Services Best Practices Guide](#)』"

## ネームサービスの接続を確認

ONTAP 9.2 以降では、DNS ネームサーバと LDAP ネームサーバが ONTAP に接続されているかどうかを確認できます。これらのコマンドは admin 権限レベルで使用できます。

### このタスクについて

DNS または LDAP ネームサービスの設定が有効かどうかは、必要に応じてネームサービス設定チェックを使用して確認できます。この検証チェックは、コマンドラインまたは System Manager で実行できます。

DNS 設定の場合、すべてのサーバがテストされ、設定が有効とみなされるためにはすべてのサーバが動作している必要があります。LDAP 設定の場合は、いずれかのサーバが稼働していれば設定は有効です。ネームサービスコマンドでは、以外の設定チェックが適用されます `skip-config-validation` フィールドは `true`（デフォルトは `false`）です。

### ステップ

1. 適切なコマンドを使用して、ネームサービスの設定を確認します。設定されているサーバのステータスが UI に表示されます。

確認する項目	使用するコマンド
DNS の設定ステータス	<code>vserver services name-service dns check</code>
LDAPの設定ステータス	<code>vserver services name-service ldap check</code>

```
cluster1::> vserver services name-service dns check -vserver vs0
```

Vserver	Name Server	Status	Status Details
vs0	10.11.12.13	up	Response time (msec): 55
vs0	10.11.12.14	up	Response time (msec): 70
vs0	10.11.12.15	down	Connection refused.

```
cluster1::> vserver services name-service ldap check -vserver vs0
```

```
| Vserver: vs0 |
| Client Configuration Name: c1 |
| LDAP Status: up |
| LDAP Status Details: Successfully connected to LDAP server |
"10.11.12.13". |
```

設定されているサーバ（name-servers/ldap-servers）の少なくとも1つが到達可能でサービスを提供していれば、設定の検証は成功です。到達不能なサーバがある場合は、警告が表示されます。

ネームサービススイッチエントリを管理するコマンド

ネームサービススイッチエントリは、作成、表示、変更、および削除することで管理できます。

状況	使用するコマンド
ネームサービススイッチエントリを作成します	<code>vserver services name-service ns-switch create</code>
ネームサービススイッチエントリを表示します	<code>vserver services name-service ns-switch show</code>
ネームサービススイッチエントリを変更する	<code>vserver services name-service ns-switch modify</code>
ネームサービススイッチエントリを削除する	<code>vserver services name-service ns-switch delete</code>

詳細については、各コマンドのマニュアルページを参照してください。

関連情報

"[ネットアップテクニカルレポート 4668](#) : 『[Name Services Best Practices Guide](#)』"

## ネームサービスキャッシュを管理するコマンド

ネームサービスキャッシュは、Time-To-Live（TTL）値を変更することで管理できます。TTL 値は、ネームサービス情報がキャッシュに保持される期間です。

TTL 値を変更する対象	使用するコマンド
UNIX ユーザ	<code>vserver services name-service cache unix-user settings</code>
UNIX グループ	<code>vserver services name-service cache unix-group settings</code>
UNIX ネットグループ	<code>vserver services name-service cache netgroups settings</code>
ホスト	<code>vserver services name-service cache hosts settings</code>
グループメンバーシップ	<code>vserver services name-service cache group-membership settings</code>

## 関連情報

["ONTAP 9コマンド"](#)

## ネームマッピングの管理用コマンド

ONTAP には、ネームマッピングを管理するためのコマンドが用意されています。

状況	使用するコマンド
ネームマッピングを作成します	<code>vserver name-mapping create</code>
特定の位置にネームマッピングを挿入します	<code>vserver name-mapping insert</code>
ネームマッピングを表示します	<code>vserver name-mapping show</code>
2 つのネームマッピングの位置を入れ替えます 注：ネームマッピングに IP 修飾子エントリが設定されている場合、スワップは許可されません。	<code>vserver name-mapping swap</code>
ネームマッピングを変更する	<code>vserver name-mapping modify</code>
ネームマッピングを削除する	<code>vserver name-mapping delete</code>

ネームマッピングが正しいことを確認します	<code>vserver security file-directory show-effective-permissions -vserver vs1 -win-user-name user1 -path / -share-name sh1</code>
----------------------	---

詳細については、各コマンドのマニュアルページを参照してください。

ローカル **UNIX** ユーザを管理するためのコマンド

ONTAP には、ローカル UNIX ユーザを管理するための固有のコマンドが用意されています。

状況	使用するコマンド
ローカル UNIX ユーザを作成します	<code>vserver services name-service unix-user create</code>
URI からローカル UNIX ユーザをロードします	<code>vserver services name-service unix-user load-from-uri</code>
ローカル UNIX ユーザを表示します	<code>vserver services name-service unix-user show</code>
ローカル UNIX ユーザを変更する	<code>vserver services name-service unix-user modify</code>
ローカル UNIX ユーザを削除する	<code>vserver services name-service unix-user delete</code>

詳細については、各コマンドのマニュアルページを参照してください。

ローカル **UNIX** グループを管理するためのコマンド

ONTAP には、ローカル UNIX グループを管理するための固有のコマンドが用意されています。

状況	使用するコマンド
ローカル UNIX グループを作成します	<code>vserver services name-service unix-group create</code>
ローカル UNIX グループにユーザを追加します	<code>vserver services name-service unix-group adduser</code>
URI からローカル UNIX グループをロードします	<code>vserver services name-service unix-group load-from-uri</code>
ローカル UNIX グループを表示します	<code>vserver services name-service unix-group show</code>



ローカル UNIX グループを変更する	<code>vserver services name-service unix-group modify</code>
ローカル UNIX グループからユーザを削除します	<code>vserver services name-service unix-group deluser</code>
ローカル UNIX グループを削除する	<code>vserver services name-service unix-group delete</code>

詳細については、各コマンドのマニュアルページを参照してください。

ローカル **UNIX** ユーザ、グループ、およびグループメンバーに対する制限

ONTAP では、クラスタ内の UNIX ユーザおよびグループの最大数の制限と、この制限を管理するためのコマンドが導入されました。これらの制限は、管理者がクラスタ内にローカル UNIX ユーザおよびグループを過剰に作成できないようにすることで、パフォーマンスの問題を回避するのに役立ちます。

ローカル UNIX ユーザグループとグループメンバーの合計数には制限があります。ローカル UNIX ユーザについては別途制限があります。これらの制限はクラスタ全体に適用されます。これらの新しい制限はそれぞれデフォルト値に設定されており、あらかじめ割り当てられたハードリミットまで引き上げることができます。

データベース	デフォルトの制限です	ハードリミット
ローカル UNIX ユーザ	3 2、7 6 8	六五、五三六
ローカル UNIX グループおよびグループメンバー	3 2、7 6 8	六五、五三六

ローカル **UNIX** ユーザおよびグループの制限を管理します

ONTAP には、ローカル UNIX ユーザおよびグループに対する制限を管理するための固有のコマンドが用意されています。クラスタ管理者は、これらのコマンドを使用して、過剰な数のローカル UNIX ユーザおよびグループに関連していると考えられる、クラスタ内のパフォーマンスの問題のトラブルシューティングを行うことができます。

このタスクについて

これらのコマンドは、advanced 権限レベルのクラスタ管理者が使用できます。

ステップ

1. 次のいずれかを実行します。

状況	使用するコマンド
ローカル UNIX ユーザの制限に関する情報を表示する	<code>vserver services unix-user max-limit show</code>

状況	使用するコマンド
ローカル UNIX グループの制限に関する情報を表示します	<code>vserver services unix-group max-limit show</code>
ローカル UNIX ユーザの制限を変更する	<code>vserver services unix-user max-limit modify</code>
ローカル UNIX グループの制限を変更する	<code>vserver services unix-group max-limit modify</code>

詳細については、各コマンドのマニュアルページを参照してください。

#### ローカルネットグループの管理用コマンド

URI からのロード、ノード間でのステータスの確認、表示、削除を行うことで、ローカルネットグループを管理できます。

状況	使用するコマンド
URI からネットグループをロードします	<code>vserver services name-service netgroup load</code>
ノード間でのネットグループのステータスを確認します	<code>vserver services name-service netgroup status</code>  <code>advanced</code> 権限レベル以上で使用できます。
ローカルネットグループを表示します	<code>vserver services name-service netgroup file show</code>
ローカルネットグループを削除する	<code>vserver services name-service netgroup file delete</code>

詳細については、各コマンドのマニュアルページを参照してください。

#### NIS ドメイン設定を管理するコマンドです

ONTAP には、NIS ドメイン設定を管理するためのコマンドが用意されています。

状況	使用するコマンド
NIS ドメイン設定を作成します	<code>vserver services name-service nis-domain create</code>
NIS ドメイン設定を表示する	<code>vserver services name-service nis-domain show</code>

NIS ドメイン設定のバインドステータスを表示します	<code>vserver services name-service nis-domain show-bound</code>
NIS統計を表示する	<code>vserver services name-service nis-domain show-statistics advanced</code> 権限レベル以上で使用できます。
NIS の統計を消去します	<code>vserver services name-service nis-domain clear-statistics advanced</code> 権限レベル以上で使用できます。
NIS ドメイン設定を変更する	<code>vserver services name-service nis-domain modify</code>
NIS ドメイン設定を削除する	<code>vserver services name-service nis-domain delete</code>
ホスト単位のネットグループ検索でのキャッシュを有効にします	<code>vserver services name-service nis-domain netgroup-database config modify advanced</code> 権限レベル以上で使用できます。

詳細については、各コマンドのマニュアルページを参照してください。

#### LDAP クライアント設定の管理用コマンド

ONTAP には、LDAP クライアント設定を管理するためのコマンドが用意されています。



SVM 管理者は、クラスタ管理者が作成した LDAP クライアント設定を変更したり削除したりできません。

状況	使用するコマンド
LDAP クライアント設定を作成します	<code>vserver services name-service ldap client create</code>
LDAP クライアント設定を表示します	<code>vserver services name-service ldap client show</code>
LDAP クライアント設定を変更します	<code>vserver services name-service ldap client modify</code>
LDAP クライアントのバインドパスワードを変更します	<code>vserver services name-service ldap client modify-bind-password</code>
LDAP クライアント設定を削除します	<code>vserver services name-service ldap client delete</code>

詳細については、各コマンドのマニュアルページを参照してください。

## LDAP 設定を管理するためのコマンド

ONTAP には、LDAP 設定を管理するためのコマンドが用意されています。

状況	使用するコマンド
LDAP 設定を作成します	<code>vserver services name-service ldap create</code>
LDAP 設定を表示します	<code>vserver services name-service ldap show</code>
LDAP 設定を変更します	<code>vserver services name-service ldap modify</code>
LDAP 設定を削除します	<code>vserver services name-service ldap delete</code>

詳細については、各コマンドのマニュアルページを参照してください。

## LDAP クライアントスキーマテンプレートを管理するためのコマンド

ONTAP には、LDAP クライアントスキーマテンプレートを管理するための固有のコマンドが用意されています。



SVM 管理者は、クラスタ管理者が作成した LDAP クライアントスキーマを変更したり削除したりできません。

状況	使用するコマンド
既存の LDAP スキーマテンプレートをコピーします	<code>vserver services name-service ldap client schema copy advanced</code> 権限レベル以上で使用できます。
LDAP スキーマテンプレートを表示します	<code>vserver services name-service ldap client schema show</code>
LDAP スキーマテンプレートを変更します	<code>vserver services name-service ldap client schema modify advanced</code> 権限レベル以上で使用できます。
LDAP スキーマテンプレートを削除します	<code>vserver services name-service ldap client schema delete advanced</code> 権限レベル以上で使用できます。

詳細については、各コマンドのマニュアルページを参照してください。

## NFS Kerberos インターフェイス設定を管理するコマンドです

ONTAP には、NFS Kerberos インターフェイスの設定を管理するためのコマンドが用意されています。

状況	使用するコマンド
----	----------

LIF で NFS Kerberos を有効にします	<code>vserver nfs kerberos interface enable</code>
NFS Kerberos インターフェイスの設定を表示します	<code>vserver nfs kerberos interface show</code>
NFS Kerberos インターフェイスの設定を変更します	<code>vserver nfs kerberos interface modify</code>
LIF で NFS Kerberos を無効にします	<code>vserver nfs kerberos interface disable</code>

詳細については、各コマンドのマニュアルページを参照してください。

### NFS Kerberos Realm 設定を管理するコマンド

ONTAP には、NFS Kerberos Realm の設定を管理するための固有のコマンドが用意されています。

状況	使用するコマンド
NFS Kerberos Realm の設定を作成します	<code>vserver nfs kerberos realm create</code>
NFS Kerberos Realm の設定を表示します	<code>vserver nfs kerberos realm show</code>
NFS Kerberos Realm の設定を変更します	<code>vserver nfs kerberos realm modify</code>
NFS Kerberos Realm の設定を削除します	<code>vserver nfs kerberos realm delete</code>

詳細については、各コマンドのマニュアルページを参照してください。

### エクスポートポリシーを管理するためのコマンド

ONTAP には、エクスポートポリシーを管理するためのコマンドが用意されています。

状況	使用するコマンド
エクスポートポリシーに関する情報を表示します	<code>vserver export-policy show</code>
エクスポートポリシーの名前を変更します	<code>vserver export-policy rename</code>

エクスポートポリシーをコピーする	<code>vserver export-policy copy</code>
エクスポートポリシーを削除する	<code>vserver export-policy delete</code>

詳細については、各コマンドのマニュアルページを参照してください。

エクスポートルールを管理するためのコマンド

ONTAP には、エクスポートルールを管理するためのコマンドが用意されています。

状況	使用するコマンド
エクスポートルールを作成します	<code>vserver export-policy rule create</code>
エクスポートルールに関する情報を表示する	<code>vserver export-policy rule show</code>
エクスポートルールを変更する	<code>vserver export-policy rule modify</code>
エクスポートルールを削除する	<code>vserver export-policy rule delete</code>



異なるクライアントを照合する同一のエクスポートルールが複数設定されている場合は、エクスポートルールの管理時にそれらのルールの同期を必ず維持するようにしてください。

詳細については、各コマンドのマニュアルページを参照してください。

**NFS** クレデンシャルキャッシュを設定する

**NFS** クレデンシャルキャッシュの **Time-To-Live** を変更する理由

ONTAP は、アクセス高速化とパフォーマンス向上のために、クレデンシャルキャッシュを使用して、NFS エクスポートアクセスでのユーザ認証に必要な情報を格納します。情報がクレデンシャルキャッシュに格納される期間を設定して、環境に合わせてカスタマイズできます。

NFS クレデンシャルキャッシュの Time-To-Live (TTL) の変更が問題の解決に役立つ場合があります。どのような状況がこれに該当するか、またそうした変更がどのような影響を及ぼすかを理解しておく必要があります。

理由

次の状況では、デフォルト TTL の変更を検討してください。

問題	修正アクション
環境内のネームサーバで ONTAP からの要求の負荷が高いためにパフォーマンスが低下している。	キャッシュされている受理および拒否のクレデンシヤルに対する TTL を長くして、ONTAP からネームサーバへの要求数を減らします。
ネームサーバ管理者がこれまで拒否されていた NFS ユーザに対してアクセスを許可する変更を行った。	キャッシュされている拒否されたクレデンシヤルに対する TTL を短くして、ONTAP ユーザが新しいクレデンシヤルを外部ネームサーバに要求して NFS ユーザがアクセスできるようになるまでの待機時間を短縮します。
ネームサーバ管理者がこれまで許可されていた NFS ユーザに対してアクセスを拒否する変更を行った。	キャッシュされている受理されたクレデンシヤルに対する TTL を短くして、ONTAP が新しいクレデンシヤルを外部ネームサーバに要求して NFS ユーザがアクセスを拒否されるようになるまでの時間を短縮します。

## 結果

受理および拒否のクレデンシヤルをキャッシュしておく期間を個別に変更することができます。ただし、こうした変更の長所と短所の両方に注意する必要があります。

状況	利点は ...	欠点は ...
クレデンシヤルのキャッシュ時間を長くしてください	ONTAP がクレデンシヤルの要求をネームサーバに送信する頻度が低下し、ネームサーバの負荷が軽減されます。	それまではアクセスが許可されていたが今後は許可されなくなる NFS ユーザに対し、アクセスを拒否するのにかかる時間が長くなります。
受理されたクレデンシヤルのキャッシュ時間を短くします	それまではアクセスが許可されていたが今後は許可されなくなる NFS ユーザに対し、アクセスを拒否するのにかかる時間が短くなります。	ONTAP がクレデンシヤルの要求をネームサーバに送信する頻度が高くなり、ネームサーバの負荷が増大します。
拒否されたクレデンシヤルのキャッシュ時間を長くします	ONTAP がクレデンシヤルの要求をネームサーバに送信する頻度が低下し、ネームサーバの負荷が軽減されます。	それまではアクセスが許可されていなかったが今後は許可されるようになる NFS ユーザに対し、アクセスを許可するのにかかる時間が長くなります。
拒否されたクレデンシヤルのキャッシュ時間を短くします	それまではアクセスが許可されていなかったが今後は許可されるようになる NFS ユーザに対し、アクセスを許可するのにかかる時間が短くなります。	ONTAP がクレデンシヤルの要求をネームサーバに送信する頻度が高くなり、ネームサーバの負荷が増大します。

キャッシュされた **NFS** ユーザクレデンシャルの **Time-To-Live** を設定してください

Storage Virtual Machine（SVM）の NFS サーバを変更することで、ONTAP が NFS ユーザのクレデンシャルを内部キャッシュに格納する期間である Time-To-Live（TTL）を設定できます。これにより、ネームサーバの高負荷に関する問題や、NFS ユーザアクセスに影響を及ぼすクレデンシャルの変更に関する問題を軽減できます。

このタスクについて

これらのパラメータは advanced 権限レベルで使用できます。

手順

1. 権限レベルを advanced に設定します。

```
set -privilege advanced
```

2. 必要な操作を実行します。

TTL を変更するキャッシュ対象	使用するコマンド
受理のクレデンシャル	<pre>vserver nfs modify -vserver vserver_name -cached -cred-positive-ttl time_to_live</pre> <p>TTL の測定単位はミリ秒です。ONTAP 9.10.1以降では、デフォルトは1時間（3,600,000ミリ秒）です。ONTAP 9.9.1以前では、デフォルトは24時間（86,400,000ミリ秒）です。この値の許容範囲は1分（60,000ミリ秒）～7日間（604,800,000ミリ秒）です。</p>
拒否のクレデンシャルです	<pre>vserver nfs modify -vserver vserver_name -cached -cred-negative-ttl time_to_live</pre> <p>TTL の測定単位はミリ秒です。デフォルトは2時間（7,200,000ミリ秒）です。この値の許容範囲は1分（60,000ミリ秒）～7日間（604,800,000ミリ秒）です。</p>

3. admin 権限レベルに戻ります。

```
set -privilege admin
```

エクスポートポリシーキャッシュを管理します

エクスポートポリシーキャッシュをフラッシュします

ONTAP は、アクセスを高速化するために、エクスポートポリシーに関連する情報の格納に複数のエクスポートポリシーキャッシュを使用します。エクスポートポリシーキャッシュを手動でフラッシュします (vserver export-policy cache flush)古い可能性がある情報を削除し、ONTAP が適切な外部リソースから最新情報を取得するように強制します。これは、NFS エクスポートへのクライアントアクセスに関するさまざまな問



題の解決に役立ちます。

このタスクについて

エクスポートポリシーキャッシュの情報は、次の理由で古くなる可能性があります。

- エクスポートポリシールールが最近変更された
- ネームサーバでホスト名レコードが最近変更された
- ネームサーバでネットグループエントリが最近変更された
- ネットグループの完全なロードを妨げていたネットワーク停止からのリカバリが発生しました

手順

1. ネームサービスキャッシュを有効にしていない場合は、advanced 権限モードで次のいずれかを実行します。

フラッシュ対象	入力するコマンド
すべてのエクスポートポリシーキャッシュ（ showmount を除く）	<code>vserver export-policy cache flush -vserver vserver_name</code>
エクスポートポリシールールアクセスキャッシュ	<code>vserver export-policy cache flush -vserver vserver_name -cache access</code> オプションのを指定できます <code>-node</code> アクセスキャッシュをフラッシュするノードを指定するパラメータ。
ホスト名キャッシュ	<code>vserver export-policy cache flush -vserver vserver_name -cache host</code>
ネットグループキャッシュ	<code>vserver export-policy cache flush -vserver vserver name -cache netgroup</code> ネットグループの処理は大量のリソースを消費します。ネットグループキャッシュのフラッシュは、古いネットグループが原因で発生したクライアントアクセス問題の解決を試みる場合にのみ行ってください。
showmount キャッシュ	<code>vserver export-policy cache flush -vserver vserver_name -cache showmount</code>

2. ネームサービスキャッシュが有効になっている場合は、次のいずれかを実行します。

フラッシュ対象	入力するコマンド
エクスポートポリシールールアクセスキャッシュ	<code>vserver export-policy cache flush -vserver vserver_name -cache access</code> オプションのを指定できます <code>-node</code> アクセスキャッシュをフラッシュするノードを指定するパラメータ。

フラッシュ対象	入力するコマンド
ホスト名キャッシュ	<code>vserver services name-service cache hosts forward-lookup delete-all</code>
ネットグループキャッシュ	<code>vserver services name-service cache netgroups ip-to-netgroup delete-all</code> <code>vserver services name-service cache netgroups members delete-all</code> ネットグループの処理は大量のリソースを消費します。ネットグループキャッシュのフラッシュは、古いネットグループが原因で発生したクライアントアクセス問題の解決を試みる場合にのみ行ってください。
showmount キャッシュ	<code>vserver export-policy cache flush</code> <code>-vserver vserver_name -cache showmount</code>

エクスポートポリシーネットグループのキューとキャッシュを表示します

ONTAP では、ネットグループのインポート時および解決時にネットグループキューを使用し、結果として得られる情報を格納するためにネットグループキャッシュを使用します。エクスポートポリシーのネットグループ関連の問題をトラブルシューティングする場合は、を使用できます `vserver export-policy netgroup queue show` および `vserver export-policy netgroup cache show` ネットグループキューのステータスおよびネットグループキャッシュの内容を表示するコマンド。

#### ステップ

1. 次のいずれかを実行します。

エクスポートポリシーネットグループに関する表示対象	入力するコマンド
キュー	<code>vserver export-policy netgroup queue show</code>
キャッシュ	<code>vserver export-policy netgroup cache show -vserver vserver_name</code>

詳細については、各コマンドのマニュアルページを参照してください。

クライアント IP アドレスがネットグループのメンバーであるかどうかを確認します

ネットグループに関連するNFSクライアントアクセスの問題をトラブルシューティングする場合は、を使用できます `vserver export-policy netgroup check-membership` クライアントIPが特定のネットグループのメンバーであるかどうかを確認するためのコマンド。

## このタスクについて

ネットグループメンバーシップのチェックにより、クライアントがネットグループのメンバーであることまたはメンバーでないことを ONTAP が認識しているかどうかを確認できます。また、ネットグループ情報の更新中に ONTAP ネットグループキャッシュが一時的な状態にあるかどうかもわかります。この情報は、クライアントに対して予期せずアクセスが許可または拒否される理由を理解するのに役立ちます。

## ステップ

1. クライアントIPアドレスのネットグループメンバーシップを確認します。 `vserver export-policy netgroup check-membership -vserver vserver_name -netgroup netgroup_name -client-ip client_ip`

このコマンドによって次のような結果が返されることがあります。

- クライアントはネットグループのメンバーです。

これは、リバースルックアップスキャンまたはホスト単位のネットグループ検索によって確認されました。

- クライアントはネットグループのメンバーです。

クライアントが ONTAP のネットグループキャッシュに見つかりました。

- クライアントはネットグループのメンバーではありません。
- ONTAP が現在ネットグループキャッシュを更新中なので、まだクライアントのメンバーシップを決定できません。

これが完了するまで、メンバーシップの判断を明示的に下すことはできません。を使用します `vserver export-policy netgroup queue show` ネットグループのロードを監視し、完了後にチェックを再試行するコマンド。

## 例

次の例は、IP アドレスが 172.17.16.72 のクライアントが SVM vs1 上のネットグループ mercury のメンバーであるかどうかをチェックします。

```
cluster1::> vserver export-policy netgroup check-membership -vserver vs1
-netgroup mercury -client-ip 172.17.16.72
```

## アクセスキャッシュのパフォーマンスを最適化

複数のパラメータを設定して、アクセスキャッシュを最適化したり、パフォーマンスとアクセスキャッシュに格納される情報の鮮度とのバランスをとったりすることができます。

## このタスクについて

アクセスキャッシュの更新期間を設定するときは、次の点に注意してください。

- 値を大きくすると、アクセスキャッシュ内のエントリの保持期間が長くなります。

長所としては、ONTAP がアクセスキャッシュエントリの更新時に消費するリソースの減少によるパフォーマンスの向上が挙げられます。短所は、エクスポートポリシールールが変更されてアクセスキャッシュエントリが古くなった場合、エントリの更新にかかる時間が長くなることです。その結果、アクセスできないクライアントが拒否され、拒否されるはずのクライアントがアクセス権を取得する可能性があります。

- 値を小さくすると、ONTAP によるアクセスキャッシュエントリの更新頻度が高くなります。

長所は、エントリの鮮度が向上し、クライアントに対するアクセスの許可または拒否が正しく行われる可能性が高くなることです。短所としては、ONTAP がアクセスキャッシュエントリの更新時に消費するリソースの増加によるパフォーマンスの低下が挙げられます。

## 手順

1. 権限レベルを advanced に設定します。

```
set -privilege advanced
```

2. 必要な操作を実行します。

変更の対象	入力するコマンド
正のエントリの更新期間	<pre>vserver export-policy access-cache config modify-all-vservers -refresh -period-positive timeout_value</pre>
負のエントリの更新期間	<pre>vserver export-policy access-cache config modify-all-vservers -refresh -period-negative timeout_value</pre>
古いエントリのタイムアウト時間	<pre>vserver export-policy access-cache config modify-all-vservers -harvest -timeout timeout_value</pre>

3. 新しいパラメータ設定を確認します。

```
vserver export-policy access-cache config show-all-vservers
```

4. admin 権限レベルに戻ります。

```
set -privilege admin
```

## ファイルロックを管理します

### プロトコル間のファイルロックについて

ファイルロックは、あるユーザが以前に開いていたファイルに別のユーザがアクセスするのを防ぐために、クライアントアプリケーションで使用される方法です。ONTAP でファイルをロックする方法は、クライアントのプロトコルによって異なります。

クライアントが NFS クライアントである場合、ロックは任意に設定します。クライアントが SMB クライアントである場合、ロックは必須となります。

NFS ファイルと SMB ファイルのロックの違いのため、SMB アプリケーションですでに開いているファイルに NFS クライアントからアクセスすると、エラーになる場合があります。

NFS クライアントが SMB アプリケーションによってロックされたファイルにアクセスすると、次のいずれかの状態になります。

- mixed形式またはNTFS形式のボリュームでは、などのファイル操作が行われます `rm`、`rmdir` および `mv` NFS アプリケーションが失敗するように原因 できますか。
- NFS の読み取りと書き込みの処理は、SMB の読み取り拒否および書き込み拒否のオープンモードによってそれぞれ拒否されます。
- また、ファイルの書き込み対象となる範囲が、排他的な SMB バイトロックでロックされている場合も、NFS の書き込みの処理はエラーになります。

UNIX セキュリティ形式のボリュームでは、NFS のリンク解除および名前変更の処理で SMB のロック状態が無視され、ファイルへのアクセスが許可されます。UNIX セキュリティ形式のボリュームでのその他すべての NFS 処理では、SMB のロック状態が考慮されます。

#### ONTAP による読み取り専用ビットの処理方法

読み取り専用ビットは、ファイルが書き込み可能（無効）なのか読み取り専用（有効）なのかを示すために、ファイルごとに設定されます。

Windows を使用する SMB クライアントは、ファイルごとの読み取り専用ビットを設定できます。NFS クライアントは、ファイルごとの読み取り専用ビットを設定しません。NFS クライアントは、ファイルごとの読み取り専用ビットを使用するプロトコル操作を行わないためです。

ONTAP は、Windows を使用する SMB クライアントによってファイルが作成される際に、そのファイルに読み取り専用ビットを設定できます。ファイルが NFS クライアントと SMB クライアント間で共有されている場合も、ONTAP は読み取り専用ビットを設定できます。一部のソフトウェアは、NFS クライアントおよび SMB クライアントで使用される場合、読み取り専用ビットが有効になっている必要があります。

NFS クライアントと SMB クライアント間で共有されるファイルに対して、適切な読み取りおよび書き込み権限を保持するために、読み取り専用ビットが次の規則に従って処理されます。ONTAP

- NFS は、読み取り専用ビットが有効になっているファイルを書き込み権限ビットが無効になっているファイルとして扱います。
- NFS クライアントがすべての書き込み権限ビットを無効にしたときに、これらのうち少なくとも 1 つが以前有効であったら、ONTAP はそのファイルの読み取り専用ビットを有効にします。
- NFS クライアントがすべての書き込み権限ビットを有効にすると、ONTAP はそのファイルの読み取り専用ビットを無効にします。
- あるファイルの読み取り専用ビットが有効になっているときに、NFS クライアントがそのファイルの権限を調べようとすると、そのファイルの権限ビットは NFS クライアントには送信されず、代わりに書き込み権限ビットがマスクされた権限ビットが ONTAP クライアントに送信されます。
- ファイルの読み取り専用ビットが有効になっているときに、SMB クライアントがこの読み取り専用ビットを無効にすると、ONTAP はそのファイルに対する所有者の書き込み権限ビットを有効にします。
- 読み取り専用ビットが有効になっているファイルに書き込めるのは、`root` のみです。



ファイル権限の変更は、SMB クライアントではすぐに反映されますが、NFS クライアントが属性のキャッシュを有効にしている場合は NFS クライアントではすぐに反映されないことがあります。

共有パスコンポーネントのロックの処理に関する **ONTAP** と **Windows** の違い

Windows とは異なり、ONTAP では、ファイルが開いているときにそのファイルのパスの各コンポーネントがロックされません。この動作は SMB 共有パスにも影響します。

ONTAP 原因ではパスの各コンポーネントがロックされないため、開いているファイルまたは共有より上のパスコンポーネントの名前を変更できます。このため、特定のアプリケーションで原因の問題が発生したり、SMB 構成の共有パスを無効な名前に変更したりすることができます。原因によって共有にアクセスできなくなる可能性があります。

パスコンポーネントの名前変更による問題を回避するには、Windows Access Control List (ACL ; アクセス制御リスト) のセキュリティ設定を適用して、ユーザやアプリケーションが重要なディレクトリの名前を変更できないようにします。

の詳細を確認してください ["クライアントがアクセスしている間にディレクトリの名前を変更しないようにする方法"](#)。

ロックに関する情報を表示します

有効になっているロックの種類とロックの状態、バイト範囲ロック、共有ロックモード、委譲ロック、および便宜的ロックの詳細、永続性ハンドルを使用してロックが開かれているかどうかなど、現在のファイルロックに関する情報を表示できます。

このタスクについて

NFSv4 または NFSv4.1 を使用して確立されたロックについては、クライアント IP アドレスを表示できません。

デフォルトでは、すべてのロックに関する情報が表示されます。コマンドパラメータを使用すると、特定の Storage Virtual Machine (SVM) のロックに関する情報を表示したり、他の条件によってコマンドの出力をフィルタリングしたりできます。

。 `vserver locks show` コマンドは、次の4種類のロックに関する情報を表示します。

- バイト範囲ロック。ファイルの一部のみをロックします。
- 共有ロック。開いているファイルをロックします。
- 便宜的ロック。SMB を使用してクライアント側キャッシュを制御します。
- 委譲。NFSv4.x を使用してクライアント側キャッシュを制御します

オプションのパラメータを指定すると、各ロックタイプに関する重要な情報を確認できます。詳細については、コマンドのマニュアルページを参照してください。

ステップ

1. を使用して、ロックに関する情報を表示します `vserver locks show` コマンドを実行します

例

次の例は、パスのファイルに対するNFSv4ロックに関する概要情報を表示します /vol1/file1。共有ロックのアクセスモードは write-deny\_none であり、書き込み委譲でロックが許可されています。

```
cluster1::> vserver locks show

Vserver: vs0
Volume   Object Path                LIF          Protocol   Lock Type   Client
-----
-----
vol1      /vol1/file1                 lif1          nfsv4      share-level -
                Sharelock Mode: write-deny_none
                delegation -
                Delegation Type: write
```

次の例は、パスのファイルに対するSMBロックに関するoplockおよび共有ロックの詳細情報を表示します /data2/data2\_2/intro.pptx。IP アドレスが 10.3.1.3 のクライアントに対して、共有ロックのアクセスモードを write-deny\_none として、永続性ハンドルが許可されています。バッチの oplock レベルで oplock リースが許可されています。

```
cluster1::> vserver locks show -instance -path /data2/data2_2/intro.pptx

Vserver: vs1
Volume: data2_2
Logical Interface: lif2
Object Path: /data2/data2_2/intro.pptx
Lock UUID: 553cf484-7030-4998-88d3-1125adbba0b7
Lock Protocol: cifs
Lock Type: share-level
Node Holding Lock State: node3
Lock State: granted
Bytelock Starting Offset: -
Number of Bytes Locked: -
Bytelock is Mandatory: -
Bytelock is Exclusive: -
Bytelock is Superlock: -
Bytelock is Soft: -
Oplock Level: -
Shared Lock Access Mode: write-deny_none
Shared Lock is Soft: false
Delegation Type: -
Client Address: 10.3.1.3
SMB Open Type: durable
SMB Connect State: connected
SMB Expiration Time (Secs): -
SMB Open Group ID:
```

```
78a90c59d45ae211998100059a3c7a00a007f70da0f8ffffcd445b0300000000
```

```

Vserver: vs1
Volume: data2_2
Logical Interface: lif2
Object Path: /data2/data2_2/test.pptx
Lock UUID: 302fd7b1-f7bf-47ae-9981-f0dcb6a224f9
Lock Protocol: cifs
Lock Type: op-lock
Node Holding Lock State: node3
Lock State: granted
Bytelock Starting Offset: -
Number of Bytes Locked: -
Bytelock is Mandatory: -
Bytelock is Exclusive: -
Bytelock is Superlock: -
Bytelock is Soft: -
Oplock Level: batch
Shared Lock Access Mode: -
Shared Lock is Soft: -
Delegation Type: -
Client Address: 10.3.1.3
SMB Open Type: -
SMB Connect State: connected
SMB Expiration Time (Secs): -
SMB Open Group ID:
78a90c59d45ae211998100059a3c7a00a007f70da0f8ffffcd445b0300000000
```

ロックを解除します

ファイルロックが原因でクライアントがファイルにアクセスできなくなっている場合は、現在有効なロックの情報を表示して、特定のロックを解除することができます。ロックの解除が必要になるケースとしては、アプリケーションのデバッグなどが挙げられます。

このタスクについて

。vserver locks break コマンドは、advanced権限レベル以上でのみ使用できます。詳細については、コマンドのマニュアルページを参照してください。

手順

1. ロックを解除するために必要な情報を確認するには、を使用します vserver locks show コマンドを実行します

詳細については、コマンドのマニュアルページを参照してください。

2. 権限レベルを advanced に設定します。



```
set -privilege advanced
```

3. 次のいずれかを実行します。

ロックを解除するための指定項目	入力するコマンド
SVM 名、ボリューム名、LIF 名、およびファイルパス	<code>vserver locks break -vserver vserver_name -volume volume_name -path path -lif lif</code>
ロック ID	<code>vserver locks break -lockid UUID</code>

4. admin 権限レベルに戻ります。

```
set -privilege admin
```

## NFS での FPolicy の first-read および first-write フィルタの動作

外部 FPolicy サーバを使用して FPolicy が有効になっていて、読み取り / 書き込み処理が監視対象イベントの場合、読み取り / 書き込み要求のトラフィックが多いと NFS クライアントで応答時間が長くなります。NFS クライアントの場合、FPolicy で first-read フィルタと first-write フィルタを使用すると、FPolicy 通知の数が減り、パフォーマンスが向上します。

NFS では、クライアントはファイルに対して I/O を実行する際に、ファイルのハンドルを取得します。このハンドルは、サーバとクライアントのリブート後も有効なままになる場合があります。このため、クライアントはハンドルを自由にキャッシュし、ハンドルを再取得しなくてもハンドルに対する要求を送信できます。通常のセッションでは、大量の読み取り / 書き込み要求がファイルサーバに送信されます。これらのすべての要求について通知が生成されると、次の問題が発生する可能性があります。

- 追加の通知処理により負荷が増大し、応答時間が長くなります。
- サーバに影響のない通知も含め、多数の通知が FPolicy サーバに送信される。

クライアントから特定のファイルに対する最初の読み取り / 書き込み要求を受信すると、キャッシュエントリが作成され、読み取り / 書き込みの数が増分されます。この要求は初回読み取り / 書き込み処理とマークされ、FPolicy イベントが生成されます。NFS クライアント用の FPolicy フィルタを計画して作成する前に、FPolicy フィルタの基本的な仕組みを理解しておく必要があります。

- first-read : 初回読み取りのクライアント要求をフィルタリングします。

このフィルタは NFS イベントに使用されます `-file-session-io-grouping-count` および `-file-session-io-grouping-duration` FPolicy が処理される初回読み取り要求は、設定によって決まります。

- first-write : 初回書き込みのクライアント要求をフィルタリングします。

このフィルタは NFS イベントに使用されます `-file-session-io-grouping-count` および `-file-session-io-grouping-duration` 設定により、FPolicy が処理された初回書き込み要求が決まります。

NFS サーバのデータベースには、次のオプションが追加されます。

```
file-session-io-grouping-count: Number of I/O Ops on a File to Be Clubbed
and Considered as One Session
for Event Generation
file-session-io-grouping-duration: Duration for Which I/O Ops on a File to
Be Clubbed and Considered as
One Session for Event Generation
```

**NFSv4.1 サーバ実装 ID を変更する**

NFSv4.1 プロトコルには、サーバのドメイン、名前、および日付を記録したサーバ実装 ID が含まれています。サーバ実装 ID のデフォルト値は変更できます。デフォルト値を変更すると、たとえば、使用率の統計を収集したり、相互運用性の問題をトラブルシューティングしたりするときに役立ちます。詳細については、RFC 5661 を参照してください。

このタスクについて  
3 つのオプションのデフォルト値は次のとおりです。

オプション	オプション名	デフォルト値
NFSv4.1 実装 ID - ドメイン	-v4.1-implementation -domain	NetApp.com にアクセスします
NFSv4.1 実装 ID の名前	-v4.1-implementation-name	クラスタバージョンの名前
NFSv4.1 実装 ID - 日付	-v4.1-implementation-date	クラスタバージョンの日付

**手順**

- 1. 権限レベルを advanced に設定します。

```
set -privilege advanced
```

- 2. 次のいずれかを実行します。

変更する <b>NFSv4.1</b> 実装 ID のオプション	入力するコマンド
ドメイン	vserver nfs modify -v4.1 -implementation-domain domain
名前	vserver nfs modify -v4.1 -implementation-name name

変更する <b>NFSv4.1</b> 実装 ID のオプション	入力するコマンド
日付	<code>vserver nfs modify -v4.1 -implementation-date date</code>

3. admin 権限レベルに戻ります。

```
set -privilege admin
```

## NFSv4 ACLs を管理します

### NFSv4 ACL を有効化する利点

NFSv4 ACL を有効化すると多くの利点を得られます。

NFSv4 ACL を有効にする利点は次のとおりです。

- ファイルやディレクトリへのユーザアクセスのより詳細な制御
- NFS セキュリティが向上します
- CIFS との相互運用性の向上
- NFS のユーザあたりの最大グループ数は 16 でなくなりました

### NFSv4 ACL の仕組み

NFSv4 ACL を使用しているクライアントは、システム上のファイルとディレクトリに ACL を設定し、その ACL を表示することができます。ACL が設定されているディレクトリ内にファイルやサブディレクトリを新しく作成すると、新しいファイルやサブディレクトリには、その ACL 内の ACE のうち、該当する継承フラグが指定された ACL エントリ（ACE）がすべて継承されます。

ファイルやディレクトリが NFSv4 要求によって作成される場合、作成されるファイルやディレクトリの ACL は、ファイル作成要求に ACL が含まれているか、または標準の UNIX ファイルアクセス権限のみが含まれているか、および親ディレクトリに ACL が設定されているかどうかによって異なります。

- 要求に ACL が含まれる場合は、その ACL が使用されます。
- 要求に標準 UNIX ファイルアクセス権限のみが含まれ、親ディレクトリに ACL がある場合、親ディレクトリの ACL の ACE に適切な継承フラグのタグが付けられていれば、それらの ACE が新しいファイルやディレクトリに継承されます。



親ACLは、の場合でも継承されます `-v4.0-acl` がに設定されます `off`。

- 要求に標準の UNIX ファイルアクセス権限のみが含まれ、親ディレクトリに ACL がない場合は、クライアントのファイルモードを使用して標準の UNIX ファイルアクセス権限が設定されます。
- 要求に標準 UNIX ファイルアクセス権限のみが含まれ、親ディレクトリに継承できない ACL がある場合は、モードビットのみを使用して新しいオブジェクトが作成されます。



状況に応じて `-chown-mode` パラメータがに設定されました `restricted` でコマンドを使用します `vserver nfs` または `vserver export-policy rule` ファミリーの場合、NFSv4 ACLで設定されたディスク上の権限でroot以外のユーザがファイル所有権を変更できる場合でも、スーパーユーザのみがファイル所有権を変更できます。詳細については、関連するマニュアルページを参照してください。

#### NFSv4 ACL の変更を有効または無効にします

ONTAP がを受信したとき `chmod` ACLが設定されたファイルまたはディレクトリに対するコマンド。デフォルトでは、ACLは保持され、モードビットの変更を反映するように変更されます。を無効にすることができます `-v4-acl-preserve` 代わりにACLをドロップする場合に動作を変更するパラメータ。

このタスクについて

unified セキュリティ形式を使用している場合、このパラメータは、クライアントがファイルまたはディレクトリに対する `chmod`、`chgroup`、または `chown` コマンドを送信したときに NTFS ファイルアクセス権が保持されるか破棄されるかの指定も行います。

このパラメータのデフォルトは `enabled` です。

手順

1. 権限レベルを `advanced` に設定します。

```
set -privilege advanced
```

2. 次のいずれかを実行します。

状況	入力するコマンド
既存の NFSv4 ACL の保持と変更を有効にする（デフォルト）	<code>vserver nfs modify -vserver vserver_name -v4-acl -preserve enabled</code>
保持を無効にして、モードビットを変更するときに NFSv4 ACL を破棄します	<code>vserver nfs modify -vserver vserver_name -v4-acl -preserve disabled</code>

3. `admin` 権限レベルに戻ります。

```
set -privilege admin
```

#### ONTAP での NFSv4 ACL を使用したファイル削除の可否の判別方法

ファイルを削除できるかどうかを判別するために、ONTAP は、そのファイルの `DELETE` ビットと、ファイルが含まれるディレクトリの `DELETE_CHILD` ビットの組み合わせを使用します。詳細については、NFS 4.1 RFC 5661 を参照してください。

**NFSv4 ACL を有効または無効にします**

NFSv4 ACLを有効または無効にするには、を変更します `-v4.0-acl` および `-v4.1-acl` オプション（Options）これらのオプションは、デフォルトでは無効になっています。

このタスクについて

。 `-v4.0-acl` または `-v4.1-acl` オプションは、NFSv4 ACLの設定と表示を制御します。アクセスチェックでのNFSv4 ACLの適用は制御しません。

ステップ

- 1. 次のいずれかを実行します。

状況	作業
NFSv4.0 ACL を有効にする	次のコマンドを入力します。  <code>vserver nfs modify -vserver vserver_name -v4.0-acl enabled</code>
NFSv4.0 ACL を無効にする	次のコマンドを入力します。  <code>vserver nfs modify -vserver vserver_name -v4.0-acl disabled</code>
NFSv4.1 ACLを有効にする	次のコマンドを入力します。  <code>vserver nfs modify -vserver vserver_name -v4.1-acl enabled</code>
NFSv4.1 ACLを無効にする	次のコマンドを入力します。  <code>vserver nfs modify -vserver vserver_name -v4.1-acl disabled</code>

**NFSv4 ACL の ACE の最大数を変更する**

パラメータを変更すると、各NFSv4 ACLに許可されるACEの最大数を変更できます `-v4-acl-max-aces`。デフォルトでは、ACLあたりのACE の数は 400 個に制限されています。この制限を引き上げることで、400 個を超える ACE を含む ACL のデータを、ONTAP を実行するストレージシステムに移行できるようになります。

このタスクについて

この制限値を増やすと、NFSv4 ACL を含むファイルにアクセスするクライアントのパフォーマンスが低下することがあります。

手順

1. 権限レベルを advanced に設定します。

```
set -privilege advanced
```

2. NFSv4 ACL の ACE の最大数を変更します。

```
vserver nfs modify -v4-acl-max-aces max_ace_limit
```

の有効な範囲

```
max_ace_limit はです 192 終了： 1024.
```

3. admin 権限レベルに戻ります。

```
set -privilege admin
```

**NFSv4 ファイル委譲を管理します**

**NFSv4** 読み取りファイル委譲を有効または無効にします

NFSv4読み取りファイル委譲を有効または無効にするには、を変更します -v4.0-read-delegationまたは オプション読み取りファイル委譲を有効にすると、ファイルのオープンとクローズに伴うメッセージのオーバーヘッドを大幅に軽減できます。

このタスクについて

デフォルトでは、読み取りファイル委譲は無効です。

読み取りファイル委譲を有効にした場合の欠点は、サーバのリブートまたはリスタート後、クライアントのリブートまたはリスタート後、あるいはネットワークを分割したあとに、サーバおよびそのクライアントが委譲をリカバリする必要があることです。

ステップ

1. 次のいずれかを実行します。

状況	作業
NFSv4 読み取りファイル委譲を有効にする	次のコマンドを入力します。  vserver nfs modify -vserver vserver_name -v4.0-read-delegation enabled
NFSv4.1 読み取りファイル委譲を有効にします	次のコマンドを入力します。  [+] vserver nfs modify -vserver vserver_name -v4.1-read-delegation enabled

NFSv4 読み取りファイル委譲を無効にする	次のコマンドを入力します。  vserver nfs modify -vserver vserver_name -v4.0 -read-delegation disabled
NFSv4.1読み取りファイル委譲を無効にする	次のコマンドを入力します。  vserver nfs modify -vserver vserver_name -v4.1 -read-delegation disabled

## 結果

ファイル委譲オプションの変更はすぐに反映されます。NFS のリブートやリスタートは必要ありません。

### NFSv4 書き込みファイル委譲を有効または無効にします

書き込みファイル委譲を有効または無効にするには、を変更します `-v4.0-write-delegation`または オプション書き込みファイル委譲を有効にすると、ファイルのオープンとクローズだけでなく、ファイルおよびレコードのロックに関連するメッセージのオーバーヘッドを大幅に軽減できます。

このタスクについて

デフォルトでは、書き込みファイル委譲は無効です。

書き込みファイル委譲を有効にした場合の欠点は、サーバのリブートまたはリスタート後、クライアントのリブートまたはリスタート後、あるいはネットワークを分割したあとに、サーバおよびそのクライアントが委譲をリカバリするための追加タスクを実行する必要があることです。

## ステップ

1. 次のいずれかを実行します。

状況	作業
NFSv4 書き込みファイル委譲を有効にします	次のコマンドを入力します。 vserver nfs modify -vserver vserver_name -v4.0 -write-delegation enabled
NFSv4.1書き込みファイル委譲を有効にする	次のコマンドを入力します。 vserver nfs modify -vserver vserver_name -v4.1 -write-delegation enabled
NFSv4 書き込みファイル委譲を無効にする	次のコマンドを入力します。 vserver nfs modify -vserver vserver_name -v4.0 -write-delegation disabled

状況	作業
NFSv4.1 書き込みファイル委譲を無効にします	次のコマンドを入力します。vserver nfs modify -vserver vserver_name -v4.1 -write-delegation disabled

## 結果

ファイル委譲オプションの変更はすぐに反映されます。NFS のリブートやリスタートは必要ありません。

## NFSv4 ファイルおよびレコードロックを設定する

### NFSv4 ファイルおよびレコードロックについて

NFSv4 クライアントの場合、ONTAP は NFSv4 のファイルロックメカニズムをサポートしているため、すべてのファイルのロック状態がリースベースモデルで保持されます。

["ネットアップテクニカルレポート 3580 : 『NFSv4 の拡張内容とベスト・プラクティス・ガイド - Data ONTAP での実装』"](#)

### NFSv4 ロックリース期間を指定します

NFSv4 ロックリース期間（ONTAP がクライアントに解除不能なロックを付与する期間）を指定するには、を変更します -v4-lease-seconds オプションリース期間を短くするとサーバのリカバリにかかる時間が短縮され、リース期間を長くすると、大量のクライアントを処理するサーバに効果的です。

### このタスクについて

デフォルトでは、このオプションはに設定されています 30。このオプションの最小値はです 10。このオプションの最大値はロック猶予期間です。この期間は、で設定できます locking.lease\_seconds オプション

## 手順

1. 権限レベルを advanced に設定します。

```
set -privilege advanced
```

2. 次のコマンドを入力します。

```
vserver nfs modify -vserver vserver_name -v4-lease-seconds number_of_seconds
```

3. admin 権限レベルに戻ります。

```
set -privilege admin
```

### NFSv4 ロック猶予期間を指定します

NFSv4 ロック猶予期間（サーバリカバリ中にクライアントがロック状態をONTAP に再要求する期間）を指定するには、を変更します -v4-grace-seconds オプション



このタスクについて

デフォルトでは、このオプションはに設定されています 45。

手順

1. 権限レベルを advanced に設定します。

```
set -privilege advanced
```

2. 次のコマンドを入力します。

```
vserver nfs modify -vserver vserver_name -v4-grace-seconds number_of_seconds
```

3. admin 権限レベルに戻ります。

```
set -privilege admin
```

## NFSv4 リファールルの仕組み

NFSv4 リファールルを有効にすると、ONTAP は NFSv4 クライアントに対して「SVM 内」のリファールルを提供します。SVM 内リファールルでは、NFSv4 要求を受け取ったクラスタノードが、NFSv4 クライアントに Storage Virtual Machine (SVM) の別の論理インターフェイス (LIF) を紹介します。

NFSv4 クライアントは、それ以降、ターゲット LIF でリファールルを受け取ったパスにアクセスする必要があります。元のクラスタノードがこのようなリファールルを返すのは、データボリュームが存在するクラスタノード上の SVM に LIF があるため、クライアントがデータにより高速にアクセスでき、余分なクラスタ通信が回避されると判断された場合です。

## NFSv4 リファールルを有効または無効にします

Storage Virtual Machine (SVM) で NFSv4 リファールルを有効にするには、オプションを有効にします `-v4-fsid-change` および `-v4.0-referrals` または。NFSv4 リファールルを有効にすると、この機能をサポートする NFSv4 クライアントのデータへのアクセス速度を向上させることができます。

必要なもの

NFS リファールルを有効にする場合は、まず Parallel NFS を無効にする必要があります。両方を同時に有効にすることはできません。

手順

1. 権限レベルを advanced に設定します。

```
set -privilege advanced
```

2. 次のいずれかを実行します。

状況	入力するコマンド
----	----------

NFSv4 リファールを有効にする	<code>vserver nfs modify -vserver vserver_name -v4-fsid -change enabled vserver nfs modify -vserver vserver_name -v4.0-referrals enabled</code>
NFSv4 リファールを無効にする	<code>vserver nfs modify -vserver vserver_name -v4.0 -referrals disabled</code>
NFSv4.1リファールを有効にする	<code>vserver nfs modify -vserver vserver_name -v4-fsid -change enabled vserver nfs modify -vserver vserver_name -v4.1-referrals enabled</code>
NFSv4.1リファールを無効にする	<code>vserver nfs modify -vserver vserver_name -v4.1 -referrals disabled</code>

3. admin 権限レベルに戻ります。

```
set -privilege admin
```

## NFS統計の表示

パフォーマンスを監視して問題を診断するために、ストレージシステム上の Storage Virtual Machine（SVM）の NFS 統計を表示することができます。

### 手順

1. を使用します `statistics catalog object show` コマンドを使用して、データを表示できるNFSオブジェクトを特定します。

```
statistics catalog object show -object nfs*
```

2. を使用します `statistics start` およびオプションです `statistics stop` 1つ以上のオブジェクトからデータサンプルを収集するコマンド。
3. を使用します `statistics show` コマンドを使用してサンプルデータを表示します。

### 例：NFSv3のパフォーマンスの監視

次の例は、NFSv3 プロトコルのパフォーマンスデータを表示します。

次のコマンドは、新しいサンプルのデータ収集を開始します。

```
vs1::> statistics start -object nfsv3 -sample-id nfs_sample
```

次のコマンドは、正常に行われた読み取り要求および書き込み要求の数と読み取り要求と書き込み要求の総数を比較するカウンタを指定して、サンプルからデータを表示します。

```
vs1::> statistics show -sample-id nfs_sample -counter
read_total|write_total|read_success|write_success
```

```
Object: nfsv3
Instance: vs1
Start-time: 2/11/2013 15:38:29
End-time: 2/11/2013 15:38:41
Cluster: cluster1
```

Counter	Value
read_success	40042
read_total	40042
write_success	1492052
write_total	1492052

## 関連情報

["パフォーマンス監視のセットアップ"](#)

**DNS**統計を表示します。

パフォーマンスを監視して問題を診断するために、ストレージシステム上のStorage Virtual Machine (SVM) のDNS統計を表示することができます。

## 手順

1. を使用します `statistics catalog object show` コマンドを使用して、データを表示できるDNSオブジェクトを特定します。

```
statistics catalog object show -object external_service_op*
```

2. を使用します `statistics start` および `statistics stop` 1つ以上のオブジェクトからデータサンプルを収集するコマンド。
3. を使用します `statistics show` コマンドを使用してサンプルデータを表示します。

## DNS 統計を監視しています

次の例は、DNS クエリのパフォーマンスデータを表示します。次のコマンドは、新しいサンプルのデータ収集を開始します。

```
vs1::*> statistics start -object external_service_op -sample-id
dns_sample1
vs1::*> statistics start -object external_service_op_error -sample-id
dns_sample2
```

次のコマンドは、送信した DNS クエリの数と、受信した / 失敗した / タイムアウトになった DNS クエリの数

を比較するカウンタを指定して、サンプルからデータを表示します。

```
vs1::*> statistics show -sample-id dns_sample1 -counter
num_requests_sent|num_responses_received|num_successful_responses|num_time
outs|num_request_failures|num_not_found_responses
```

```
Object: external_service_op
Instance: vs1:DNS:Query:10.72.219.109
Start-time: 3/8/2016 11:15:21
End-time: 3/8/2016 11:16:52
Elapsed-time: 91s
Scope: vs1
```

Counter	Value
num_not_found_responses	0
num_request_failures	0
num_requests_sent	1
num_responses_received	1
num_successful_responses	1
num_timeouts	0

6 entries were displayed.

次のコマンドは、特定のサーバの DNS クエリに対して特定のエラーを受信した回数を示すカウンタを指定して、サンプルからデータを表示します。

```
vs1::*> statistics show -sample-id dns_sample2 -counter
server_ip_address|error_string|count
```

```
Object: external_service_op_error
Instance: vs1:DNS:Query:NXDOMAIN:10.72.219.109
Start-time: 3/8/2016 11:23:21
End-time: 3/8/2016 11:24:25
Elapsed-time: 64s
Scope: vs1
```

Counter	Value
count	1
error_string	NXDOMAIN
server_ip_address	10.72.219.109

3 entries were displayed.

関連情報

["パフォーマンス監視のセットアップ"](#)

## NIS統計を表示する

パフォーマンスを監視して問題を診断するために、ストレージシステム上のStorage Virtual Machine (SVM) のNIS統計を表示することができます。

### 手順

1. を使用します `statistics catalog object show` コマンドを使用して、データを表示できるNISオブジェクトを特定します。

```
statistics catalog object show -object external_service_op*
```

2. を使用します `statistics start` および `statistics stop` 1つ以上のオブジェクトからデータサンプルを収集するコマンド。
3. を使用します `statistics show` コマンドを使用してサンプルデータを表示します。

### NIS 統計を監視する

次の例は、NIS クエリのパフォーマンスデータを表示します。次のコマンドは、新しいサンプルのデータ収集を開始します。

```
vs1::*> statistics start -object external_service_op -sample-id  
nis_sample1  
vs1::*> statistics start -object external_service_op_error -sample-id  
nis_sample2
```

次のコマンドは、送信した NIS クエリの数と、受信した / 失敗した / タイムアウトになった NIS クエリの日数を比較するカウンタを指定して、サンプルからデータを表示します。

```
vs1::*> statistics show -sample-id nis_sample1 -counter
instance|num_requests_sent|num_responses_received|num_successful_responses
|num_timeouts|num_request_failures|num_not_found_responses
```

```
Object: external_service_op
Instance: vs1:NIS:Query:10.227.13.221
Start-time: 3/8/2016 11:27:39
End-time: 3/8/2016 11:27:56
Elapsed-time: 17s
Scope: vs1
```

Counter	Value
num_not_found_responses	0
num_request_failures	1
num_requests_sent	2
num_responses_received	1
num_successful_responses	1
num_timeouts	0

6 entries were displayed.

次のコマンドは、特定のサーバの NIS クエリに対して特定のエラーを受信した回数を示すカウンタを指定して、サンプルからデータを表示します。

```
vs1::*> statistics show -sample-id nis_sample2 -counter
server_ip_address|error_string|count
```

```
Object: external_service_op_error
Instance: vs1:NIS:Query:YP_NOTFOUND:10.227.13.221
Start-time: 3/8/2016 11:33:05
End-time: 3/8/2016 11:33:10
Elapsed-time: 5s
Scope: vs1
```

Counter	Value
count	1
error_string	YP_NOTFOUND
server_ip_address	10.227.13.221

3 entries were displayed.

## 関連情報

["パフォーマンス監視のセットアップ"](#)

**VMware vStorage over NFS** がサポートされるようになりました

ONTAP は、NFS 環境で特定の VMware vStorage API for Array Integration （VAAI）機能をサポートしています。

サポートされている機能

次の機能がサポートされます。

- コピーオフロード

ESXi ホストで、仮想マシンや仮想マシンディスク（VMDK）のコピーを、ホストを介さずにソースとデスティネーションのデータストア間で直接実行できます。これにより、ESXi ホストの CPU サイクルやネットワーク帯域幅を節約できます。ソースボリュームがスパースボリュームの場合、コピーオフロードでスペース効率が保持されます。

- スペースリザベーション

スペースをリザーブして VMDK ファイル用のストレージスペースを確保します。

制限

NFS で VMware vStorage を使用する際には、次の制限事項があります。

- 次の場合にコピーオフロード処理が失敗することがあります。
  - ソースボリュームまたはデスティネーションボリュームで wafiron を実行中に、ボリュームが一時的にオフラインになっている
  - ソースボリュームまたはデスティネーションボリュームを移動しているとき
  - ソースまたはデスティネーションの LIF を移動しているとき
  - テイクオーバーまたはギブバック処理を実行しているとき
  - スイッチオーバーまたはスイッチバック処理を実行しているとき
- 次のシナリオでは、ファイルハンドル形式の違いが原因でサーバ側のコピーが失敗する可能性があります。

qtree のエクスポートを現在行っているか、以前行っていた SVM から、これまでに qtree をエクスポートしたことがない SVM へのデータのコピーを試みます。上記の制限を回避するために、デスティネーション SVM で少なくとも 1 つの qtree をエクスポートすることができます。

関連情報

"Data ONTAP では、VAAI オフロード処理はどのようにサポートされていますか。"

**VMware vStorage over NFS** を有効または無効にします

を使用して、Storage Virtual Machine（SVM）で VMware vStorage over NFS のサポートを有効または無効にできます `vserver nfs modify` コマンドを実行します

このタスクについて

デフォルトでは、VMware vStorage over NFS のサポートは無効になっています。

#### 手順

1. SVM での現在の vStorage のサポートステータスを表示します。

```
vserver nfs show -vserver vserver_name -instance
```

2. 次のいずれかを実行します。

状況	入力するコマンド
VMware vStorage のサポートを有効にします	<pre>vserver nfs modify -vserver vserver_name -vstorage enabled</pre>
VMware vStorage のサポートを無効にします	<pre>vserver nfs modify -vserver vserver_name -vstorage disabled</pre>

#### 完了後

この機能を使用する前に、NFS Plug-in for VMware VAAI をインストールしておく必要があります。詳細については、「[NetApp NFS Plug-in for VMware VAAI のインストール](#)」を参照してください。

#### 関連情報

["ネットアップのマニュアル：NetApp NFS Plug-in for VMware VAAI"](#)

#### **rquota** のサポートを有効または無効にします

ONTAP は、remote quota protocol バージョン 1（rquota v1）をサポートしています。rquota プロトコルを使用すると、NFS クライアントは、リモートマシンからユーザのクォータ情報を取得できます。Storage Virtual Machine（SVM）で rquota を有効にするには、を使用します `vserver nfs modify` コマンドを実行します

#### このタスクについて

デフォルトでは、rquota は無効です。

#### ステップ

1. 次のいずれかを実行します。

状況	入力するコマンド
SVM で rquota のサポートを有効にします	<pre>vserver nfs modify -vserver vserver_name -rquota enable</pre>
SVM で rquota のサポートを無効にします	<pre>vserver nfs modify -vserver vserver_name -rquota disable</pre>

クォータの詳細については、を参照してください ["論理ストレージ管理"](#)。



**TCP 転送サイズを変更することで NFSv3 / NFSv4 のパフォーマンスが向上します**

TCP 最大転送サイズを変更することで、高レイテンシのネットワーク経由でストレージシステムに接続する NFSv3 / NFSv4 クライアントのパフォーマンスを向上させることができます。

レイテンシが 10 ミリ秒を超えるワイドエリアネットワーク（WAN）またはメトロエリアネットワーク（MAN）などの高レイテンシネットワークを介してクライアントがストレージシステムにアクセスしている場合は、TCP 最大転送サイズを変更することで、ネットワーク接続のパフォーマンスを向上させることができます。ローカルエリアネットワーク（LAN）などの低レイテンシネットワークでストレージシステムにアクセスするクライアントは、これらのパラメータを変更してもパフォーマンスの向上はあまり期待できません。スループットの向上がレイテンシの影響を上回らない場合は、これらのパラメータを使用しないでください。

ストレージ環境がこれらのパラメータの変更の恩恵を受けるかどうかを判断するには、まずパフォーマンスの低い NFS クライアントで総合的なパフォーマンス評価を行ってください。パフォーマンスの低さが、クライアント上の過剰なラウンドトリップによるレイテンシとデータ量の少ない要求によるものかどうかを確認します。このような状況では、クライアントとサーバは、接続を介して送信される小さな要求と応答を待機するデューティサイクルの大部分を消費するため、使用可能な帯域幅を完全に使用することはできません。

NFSv3 と NFSv4 の要求サイズを大きくすることで、クライアントとサーバは使用可能な帯域幅をより効果的に使用できるようになり、単位時間あたりの移動データ量が多くなります。そのため、接続の全体的な効率が増加します。

ストレージシステムとクライアントの間で設定が異なる場合があることに注意してください。ストレージシステムとクライアントでサポートされる転送処理の最大サイズは 1MB です。ただし、ストレージシステムで最大転送サイズを 1MB に設定しても、クライアントがサポートするサイズが 64KB であると、マウントの転送サイズは 64KB 以下に制限されます。

これらのパラメータを変更する前に注意しなければならないのは、変更すると、大量の応答をアセンブルして送信するのに時間がかかり、ストレージシステムでメモリ消費が増えるということです。ストレージシステムへの高レイテンシ接続が増えるほど、メモリ消費量も増加します。メモリ容量が多いストレージシステムでは、この変更による影響はほとんどありません。メモリ容量が少ないストレージシステムでは、パフォーマンスが著しく低下する可能性があります。

これらのパラメータを効果的に使用するには、クラスタの複数のノードからデータを取得する必要があります。クラスタネットワーク固有のレイテンシによって、応答の全体的なレイテンシが増加する可能性があります。これらのパラメータを使用するときに、全体的なレイテンシが増大する傾向があります。そのため、レイテンシの影響を受けやすいワークロードは悪影響を受ける可能性があります。

### **NFSv3 と NFSv4 の TCP 最大転送サイズを変更する**

を変更できます `-tcp-max-xfer-size` NFSv3 および NFSv4.x プロトコルを使用するすべての TCP 接続の最大転送サイズを設定するオプション。

このタスクについて

これらのオプションは Storage Virtual Machine （SVM）ごとに変更できます。

ONTAP 9以降では、を参照してください `v3-tcp-max-read-size` および `v3-tcp-max-write-size` オプションは廃止されました。を使用する必要があります `-tcp-max-xfer-size` 代わりにオプション。

手順

1. 権限レベルを advanced に設定します。

```
set -privilege advanced
```

2. 次のいずれかを実行します。

状況	入力するコマンド
NFSv3 または NFSv4 の TCP 最大転送サイズを変更する	<pre>vserver nfs modify -vserver vserver_name -tcp-max-xfer-size integer_max_xfer_size</pre>

オプション	範囲	デフォルト
-tcp-max-xfer-size	8192~1048576 バイト	65536バイト



最大転送サイズには、4KB（4096 バイト）の倍数を入力する必要があります。要求が要件を満たしていない場合は、パフォーマンスが低下します。

3. を使用します `vserver nfs show -fields tcp-max-xfer-size` コマンドを使用して変更を確認します。
4. 静的マウントを使用しているクライアントがある場合、新しいパラメータサイズを有効にするには、いったんアンマウントしてから再度マウントします。

#### 例

次のコマンドは、vs1 という SVM で NFSv3 と NFSv4.x の TCP 最大転送サイズを 1、048、576 バイトに設定します。

```
vs1::> vserver nfs modify -vserver vs1 -tcp-max-xfer-size 1048576
```

#### NFS ユーザに許可するグループ ID の数を設定します

ONTAP は、Kerberos（RPCSEC\_GSS）認証を使用して NFS ユーザクレデンシャルを処理する場合、デフォルトで最大 32 個のグループ ID をサポートしています。AUTH\_SYS 認証を使用する場合は、RFC 5331 で定義されているとおり、グループ ID のデフォルトの最大数は 16 個です。デフォルト数を超えるグループに属しているユーザがいる場合は、この最大数を 1、024 まで増やすことができます。

#### このタスクについて

デフォルト数を超えるグループ ID がクレデンシャルに設定されている場合、残りのグループ ID は切り捨てられ、そのユーザがストレージシステムのファイルにアクセスしようとするエラーが発生する可能性があります。SVM あたりの最大グループ数は、環境内の最大グループ数と同じ数に設定する必要があります。

次の表に、の2つのパラメータを示します `vserver nfs modify` 3つの設定例でグループIDの最大数を決定するコマンド。

パラメータ	設定	結果として得られるグループ ID の上限数
-extended-groups-limit	32	RPCSEC_GSS : 32
-auth-sys-extended-groups	disabled	AUTH_SYS : 16
	これらはデフォルト設定です。	
-extended-groups-limit	256	RPCSEC_GSS : 256
-auth-sys-extended-groups	disabled	AUTH_SYS : 16
-extended-groups-limit	512	RPCSEC_GSS : 512
-auth-sys-extended-groups	enabled	AUTH_SYS : 512

## 手順

1. 権限レベルを advanced に設定します。

```
set -privilege advanced
```

2. 必要な操作を実行します。

許可される補助グループの最大数の設定対象	入力するコマンド
RPCSEC_GSS の場合のみ、AUTH_SYS はデフォルト値の 16 に設定されます	<pre>vserver nfs modify -vserver vserver_name -extended-groups-limit {32-1024} -auth-sys-extended-groups disabled</pre>
RPCSEC_GSS と AUTH_SYS の両方	<pre>vserver nfs modify -vserver vserver_name -extended-groups-limit {32-1024} -auth-sys-extended-groups enabled</pre>

3. を確認します -extended-groups-limit AUTH\_SYS が拡張グループを使用しているかどうかを確認します。 `vserver nfs show -vserver vserver_name -fields auth-sys-extended-groups,extended-groups-limit`
4. admin 権限レベルに戻ります。

```
set -privilege admin
```

## 例

次の例は、拡張されたグループを AUTH\_SYS 認証で有効にし、AUTH\_SYS 認証と RPCSEC\_GSS 認証の両方で拡張グループの最大数を 512 に設定します。これらの変更は、vs1 という SVM にアクセスするクライアントに対してのみ行われます。

```

vs1::> set -privilege advanced
Warning: These advanced commands are potentially dangerous; use
        them only when directed to do so by NetApp personnel.
Do you want to continue? {y|n}: y

vs1::*> vservers nfs modify -vservers vs1 -auth-sys-extended-groups enabled
-extended-groups-limit 512

vs1::*> vservers nfs show -vservers vs1 -fields auth-sys-extended-
groups,extended-groups-limit
vservers auth-sys-extended-groups extended-groups-limit
-----
vs1      enabled                      512

vs1::*> set -privilege admin

```

## NTFS セキュリティ形式のデータへの root ユーザアクセスを制御する

NTFS セキュリティ形式のデータへの NFS クライアントアクセスを許可したり、NTFS クライアントによる NFS セキュリティ形式データへのアクセスを許可したりするように ONTAP を設定することができます。NFS データストアで NTFS セキュリティ形式を使用する際には、root ユーザによるアクセスの処理方法を決定し、それに応じて Storage Virtual Machine (SVM) を設定する必要があります。

このタスクについて

root ユーザが NTFS セキュリティ形式のデータにアクセスする際には、次の 2 つのオプションがあります。

- 他の NFS ユーザと同様に root ユーザを Windows ユーザにマッピングし、NTFS ACL に従ってアクセスを管理する。
- NTFS ACL を無視してフルアクセスを root に対して提供する。

手順

1. 権限レベルを advanced に設定します。

```
set -privilege advanced
```

2. 必要な操作を実行します。

root ユーザへの対処方法	入力するコマンド
Windows ユーザにマッピングする	<code>vservers nfs modify -vservers vservers_name -ignore-nt-acl-for-root disabled</code>
NT ACL チェックをバイパスします	<code>vservers nfs modify -vservers vservers_name -ignore-nt-acl-for-root enabled</code>

デフォルトでは、このパラメータは無効になっています。

このパラメータが有効になっていても root ユーザに対するネームマッピングが存在しない場合、ONTAP はデフォルトの SMB 管理者のクレデンシャルを監査に使用します。

3. admin 権限レベルに戻ります。

```
set -privilege admin
```

## サポート対象のNFSバージョンとクライアント

サポートされる**NFS**のバージョンとクライアントの概要

ネットワークで NFS を使用する前に、ONTAP でサポートされる NFS のバージョンとクライアントを確認しておく必要があります。

この表は、NFSプロトコルのメジャーバージョンとマイナーバージョンがONTAP でデフォルトでサポートされる場合を示しています。デフォルトでは、このNFSプロトコルをサポートするONTAP の最も古いバージョンがサポートされているわけではありません。

バージョン	デフォルトは有効です
NFSv3	はい。
NFSv4.0	はい、ONTAP 9.9.1 以降でサポートされています
NFSv4.1	はい、ONTAP 9.9.1 以降でサポートされています
NFSv4.2	はい、ONTAP 9.9.1 以降でサポートされています
pNFS	いいえ

ONTAP でサポートされる NFS クライアントに関する最新情報については、Interoperability Matrix を参照してください。

["NetApp Interoperability Matrix Tool で確認できます"](#)

**ONTAP** でサポートされる **NFSv4.0** の機能

ONTAP は、SPKM3 および LIPKEY のセキュリティ機能を除く NFSv4.0 の必須機能をすべてサポートしています。

次の NFSv4 機能がサポートされます。

- \* コンパウンド \*

クライアントは、1つのリモート手順呼び出し（RPC）要求で複数のファイル操作を要求できます。

- \* ファイル委譲 \*

サーバは、一部のタイプのクライアントにファイル制御を委譲して読み取りおよび書き込みアクセスを許可します。

- \* 擬似 fs \*

NFSv4 サーバでストレージシステム上のマウントポイントの決定に使用します。NFSv4 にはマウントプロトコルはありません。

- \* ロック \*

リースベース。NFSv4 には独立した Network Lock Manager (NLM ; ネットワークロックマネージャ) または Network Status Monitor (NSM ; ネットワークステータスマニタ) プロトコルはありません。

NFSv4.0 プロトコルの詳細については、RFC 3530 を参照してください。

## NFSv4 の ONTAP サポートの制限事項

NFSv4 の ONTAP サポートにはいくつかの制限があることに注意してください。

- 委譲機能はすべてのクライアントタイプでサポートされているわけではありません。
- ONTAP 9.4 以前のリリースでは、UTF8 以外のボリュームで ASCII 以外の文字が含まれている名前はストレージシステムで拒否されます。

ONTAP 9.5 以降のリリースでは、utf8mb4 言語設定で作成され NFSv4 を使用してマウントされたボリュームはこの制限を受けなくなります。

- すべてのファイルハンドルは永続的です。サーバは揮発性のファイルハンドルを提供しません。
- 移行とレプリケーションはサポートされていません。
- NFSv4 クライアントは、読み取り専用負荷共有ミラーでサポートされていません。

ONTAP は、NFSv4 クライアントを直接読み取りおよび書き込みアクセスの負荷共有ミラーのソースにルーティングします。

- 名前付き属性はサポートされていません。
- 次の属性を除くすべての推奨属性がサポートされています。

- archive
- hidden
- homogeneous
- mimetype
- quota\_avail\_hard
- quota\_avail\_soft
- quota\_used
- system

◦ time\_backup



ただし、はサポートされていません quota\* 属性では、ONTAP はRQUOTA側のバンド プロトコルを介してユーザクォータとグループクォータをサポートします。

## ONTAP での NFSv4.1 のサポート

ONTAP 9.8 以降では、NFSv4.1 が有効になっている場合、nconnect 機能がデフォルトで使用できます。

以前の NFS クライアント実装では、マウントを使用する TCP 接続は 1 つだけです。ONTAP では、1 つの TCP 接続が IOPS の増加に伴うボトルネックになることがあります。ただし、nConnect 対応クライアントでは、1 つの NFS マウントに複数の TCP 接続（最大 16 個）を関連付けることができます。このような NFS クライアントは、ファイル操作を複数の TCP 接続にラウンドロビン方式で多重化し、使用可能なネットワーク帯域幅からより高いスループットを取得します。nConnect は、NFSv3 マウントと NFSv4.1 マウントでのみ推奨されます。

NFS クライアントのマニュアルを参照して、nConnect がクライアントバージョンでサポートされているかどうかを確認してください。

ONTAP 9.9.1 以降では、NFSv4.1 がデフォルトで有効になっています。以前のリリースでは、を指定して有効にすることができました `-v4.1` オプションを選択し、に設定します `enabled Storage Virtual Machine (SVM)` に NFS サーバを作成する場合。

ONTAP は、NFSv4.1 のディレクトリレベルおよびファイルレベルの委譲をサポートしていません。

## NFSv4 4.2 の ONTAP サポート

ONTAP 9.8 以降では、ONTAP で NFSv4.2 プロトコルがサポートされ、NFSv4.2 対応クライアントのアクセスが許可されます。

ONTAP 9.9.1 以降では、NFSv4 4.2 がデフォルトで有効になっています。ONTAP 9.8 では、`-v4.1` オプションを選択し、に設定します `enabled Storage Virtual Machine (SVM)` に NFS サーバを作成する場合。NFSv4.1 を有効にすると、クライアントが v4.2 としてマウントされた状態で NFSv4.1 の機能を使用することもできます。

ONTAP の以降のリリースでは、NFSv4.2 のオプション機能のサポートが拡張されています。

先頭のドキュメント	NFSv4.2 のオプションの機能
ONTAP 9.12.1	<ul style="list-style-type: none"><li>• NFS 拡張属性</li><li>• スパースファイル</li><li>• スペースリザベーション</li></ul>
ONTAP 9.9.1	NFS とラベルされた MAC（必須アクセス制御

## NFS v4.2 セキュリティラベル

ONTAP 9.9.1 以降では、NFS セキュリティラベルを有効にできます。デフォルトでは無効になっています。

NFS v4.2 セキュリティラベルでは、ONTAP NFS サーバは必須アクセス制御（MAC）対応であり、クライアントから送信された sec\_label 属性を保存および取得します。

詳細については、を参照してください ["RFC 7240"](#)。

ONTAP 9.12.1以降では、NDMPダンプ処理でNFS v4.2セキュリティラベルがサポートされます。以前のリリースのファイルまたはディレクトリでセキュリティラベルが検出された場合、ダンプは失敗します。

#### 手順

1. 権限の設定を advanced に変更します。

```
set -privilege advanced
```

2. セキュリティラベルを有効にする：

```
vserver nfs modify -vserver _svm_name_ -v4.2-seclabel enabled
```

#### NFS拡張属性

ONTAP 9.12.1以降では、NFS拡張属性（xattrs）がデフォルトで有効になっています。

拡張属性は、で定義される標準のNFS属性です ["RFC 8276"](#) 最新のNFSクライアントで有効になっています。ユーザ定義のメタデータをファイルシステムオブジェクトに添付するために使用でき、高度なセキュリティの導入に役立ちます。

現在のところ、NDMPダンプ処理では、NFS拡張属性はサポートされていません。ファイルまたはディレクトリで拡張属性が検出された場合、ダンプは続行されますがこれらのファイルまたはディレクトリの拡張属性はバックアップされません

拡張属性を無効にする必要がある場合は、を使用します vserver nfs modify -v4.2-xattrs disabled コマンドを実行します

#### Parallel NFS の ONTAP サポート

ONTAP は、Parallel NFS（pNFS；パラレル NFS）をサポートします。pNFS プロトコルは、クラスタの複数のノードに分散されたファイルセットのデータにクライアントが直接アクセスできるようにして、パフォーマンスを向上します。これにより、クライアントはボリュームへの最適なパスを見つけることができます。

#### ハードマウントの使用

マウントの問題をトラブルシューティングするときは、正しい種類のマウントを使用していることを確認する必要があります。NFS は、ソフトマウントとハードマウントの2つのマウントタイプをサポートしています。信頼性を確保するために、ハードマウントのみを使用してください。

特に NFS タイムアウトが頻繁に発生する可能性がある場合は、ソフトマウントは使用しないでください。タ



イムアウトによって競合状態が発生し、データが破損する可能性があります。

## NFS と SMB のファイルとディレクトリの命名規則

NFSとSMBのファイルとディレクトリの命名規則について説明します

ファイルとディレクトリの命名規則は、ONTAP クラスタおよびクライアントの言語設定に加え、ネットワーククライアントのオペレーティングシステムとファイル共有プロトコルによって異なります。

オペレーティングシステムとファイル共有のプロトコルによって、次の要素が決定します。

- ファイル名に使用できる文字
- ファイル名での大文字と小文字の区別

ONTAP では、ONTAP のリリースに応じて、ファイル、ディレクトリ、qtree の名前でマルチバイト文字がサポートされます。

ファイル名またはディレクトリ名に使用できる文字

異なるオペレーティングシステムのクライアントからファイルやディレクトリにアクセスする場合は、どちらのオペレーティングシステムでも有効な文字を使用します。

たとえば、UNIX を使用してファイルやディレクトリを作成する場合は、ファイル名やディレクトリ名にコロン (:) を使用しないでください。コロンは、MS-DOS ファイル名やディレクトリ名では使用できないためです。有効な文字の制限はオペレーティングシステムごとに異なります。使用できない文字の詳細については、クライアントのオペレーティングシステムのマニュアルを参照してください。

マルチプロトコル環境でのファイル名とディレクトリ名の大文字と小文字の区別

ファイル名とディレクトリ名では、NFSクライアントでは大文字と小文字が区別されますが、SMBクライアントでは大文字と小文字が区別されません。この違いがマルチプロトコル環境に及ぼす影響と、SMB 共有の作成時にパスを指定するときや、共有内のデータにアクセスするときなどのような対処が必要になるかを理解しておく必要があります。

SMBクライアントがという名前のディレクトリを作成する場合 `testdir`SMBクライアントとNFSクライアントのどちらでも、ファイル名はと表示されます`testdir。ただし、SMBユーザがあとでディレクトリ名を作成しようとした場合`TESTDIR`を指定することはできません。SMBクライアントでは、その名前がすでに存在しているとみなされます。NFSユーザがあとでという名前のディレクトリを作成する場合`TESTDIR`では、NFSクライアントとSMBクライアントで表示されるディレクトリ名は次のように異なります。`

- NFSクライアントでは、両方のディレクトリ名が作成したとおりに表示されます（例：） `testdir` および ``TESTDIR`` ディレクトリ名では大文字と小文字が区別されるためです。
- SMB クライアントでは、2つのディレクトリを区別するために 8.3 形式の名前が使用されます。1つのディレクトリにはベースファイル名が付けられます。追加のディレクトリには 8.3 形式のファイル名が割り当てられます。
  - SMBクライアントでは、が表示されます `testdir` および `TESTDI~1`。

- ONTAP によってが作成されます TESTDI~1 2つのディレクトリを区別するディレクトリ名。

この場合、Storage Virtual Machine (SVM) での共有の作成時または変更時に共有パスを指定するときは、8.3 形式の名前を使用する必要があります。

ファイルについても、SMBクライアントでが作成された場合と同様です `test.txt` `SMBクライアントとNFSクライアントのどちらでも、ファイル名はと表示されます` `test.txt`。ただし、SMBユーザがあとでを作成しようとした場合 `Test.txt` を指定することはできません。SMBクライアントでは、その名前がすでに存在しているとみなされます。NFSユーザがあとでという名前のファイルを作成した場合 `Test.txt` では、NFSクライアントとSMBクライアントで表示されるファイル名は次のように異なります。

- NFSクライアントでは、両方のファイル名が作成されたとおりに表示され、`test.txt` および `Test.txt` ファイル名では大文字と小文字が区別されるためです。
- SMBクライアントでは、2つのファイルを区別するために8.3形式の名前が使用されます。1つのファイルにはベースファイル名が付けられます。追加のファイルには8.3形式のファイル名が割り当てられます。
  - SMBクライアントでは、が表示されます `test.txt` および `TEST~1.TXT`。
  - ONTAP によってが作成されます `TEST~1.TXT` 2つのファイルを区別するためのファイル名。



Vserver cifs character-mappingコマンドを使用して文字マッピングを作成した場合、通常は大文字と小文字が区別されないWindows検索では大文字と小文字が区別される可能性があります。これは、文字マッピングが作成されていて、ファイル名がその文字マッピングを使っている場合にのみ、ファイル名のルックアップで大文字小文字が区別されることを意味します。

## ONTAP によるファイル名とディレクトリ名の作成方法

ONTAP は、SMBクライアントからアクセスされるすべてのディレクトリ内にあるファイルまたはディレクトリに対して2つの名前が作成され、保持されます。元の長い名前と8.3形式の名前です。

名前が8文字を超える、または拡張子が3文字を超える（ファイルの場合）ファイル名やディレクトリ名について、ONTAP は次のように8.3形式の名前を生成します。

- 名前が6文字を超える場合は、元のファイル名またはディレクトリ名が6文字に切り捨てられます。
- 切り捨て後に一意でなくなったファイル名またはディレクトリ名には、チルダ（~）と1~5の数字が追加されます。

同様の名前が6つ以上存在するため数字が足りなくなった場合には、元の名前とは無関係な一意の名前が作成されます。

- ファイルの場合は、ファイル名の拡張子が3文字に切り捨てられます。

たとえば、NFSクライアントがという名前のファイルを作成するとします `specifications.html` `ONTAPで作成される8.3形式のファイル名はです` `specif~1.htm`。この名前がすでに存在する場合、ONTAP はファイル名の最後に別の番号を使用します。たとえば、NFSクライアントがという名前の別のファイルを作成したとします `specifications_new.html`、8.3形式の `specifications_new.html` はです `specif~2.htm`。

マルチバイトを含むファイル名、ディレクトリ名、 **qtree** 名の **ONTAP** での処理

ONTAP 9.5 以降では、4 バイトの UTF-8 エンコード形式の名前がサポートされるようになり、Basic Multilingual Plane（BMP；基本多言語面）以外の Unicode 補助文字を含むファイル、ディレクトリ、ツリーの名前を作成および表示できるようになりました。以前のリリースでは、これらの補助文字はマルチプロトコル環境では正しく表示されませんでした。

4バイトのUTF-8エンコード名のサポートを有効にするには、`new_utf8mb4_言語コード`を使用できます `vserver` および `volume` コマンド・ファミリー。

- 次のいずれかの方法で新しいボリュームを作成する必要があります。
- ボリュームを設定しています `-language` 明示的なオプション：

```
volume create -language utf8mb4 {...}
```

- ボリュームを継承しています `-language` オプションを指定して作成または変更したSVMから、次のオプションを選択します。

```
vserver [create|modify] -language utf8mb4 {...}``volume create {...}
```

- ONTAP 9.6以前を使用している場合、utf8mb4をサポートするために既存のボリュームを変更することはできません。utf8mb4対応の新しいボリュームを作成し、クライアントベースのコピーツールを使用してデータを移行する必要があります。

ONTAP 9.7P1以降を使用している場合は、utf8mb4の既存ボリュームをサポートリクエストで変更できます。詳細については、[を参照してください "ONTAPでの作成後にボリュームの言語を変更できますか。"](#)。

[+]

SVM は utf8mb4 をサポートするように更新できますが、既存のボリュームの言語コードは元の設定のままです。

[+]



現在のところ、4 バイトの UTF-8 文字を含む LUN 名はサポートされていません。

- 一般に、Unicode 文字データは、Windows ファイルシステムアプリケーションでは 16-bit Unicode Transformation Format（UTF-16）、NFS ファイルシステムでは 8-bit Unicode Transformation Format（UTF-8）を使用して表現されます。

ONTAP 9.5 よりも前のリリースでは、Windows クライアントで作成された UTF-16 の補助文字を含む名前は、他の Windows クライアントには正しく表示されましたが、NFS クライアントでは UTF-8 に正しく変換されませんでした。同様に、NFS クライアントで作成された UTF-8 の補助文字を含む名前は、Windows クライアントで UTF-16 に正しく変換されませんでした。

- ONTAP 9.4 以前を実行しているシステムで作成したファイル名に有効な追加文字が含まれている場合や無効な追加文字が含まれている場合、ONTAP はそれらのファイル名を拒否し、ファイル名が無効であることを示すエラーを返します。

この問題を回避するには、ファイル名に BMP 文字のみを使用して補助文字は使用しないようにするか、ONTAP 9.5 以降にアップグレードしてください。

Unicode 文字は qtree 名で使用できます。

- どちらかを使用できます volume qtree qtree名を設定または変更するには、コマンドファミリーまたは System Manager を使用します。
- 日本語や中国語などの Unicode 形式のマルチバイト文字を qtree 名に含めることができます。
- ONTAP 9.5 よりも前のリリースでは、BMP 文字（つまり 3 バイトで表現可能な文字）のみがサポートされます。



ONTAP 9.5 よりも前のリリースでは、qtree の親ボリュームのジャンクションパスに、Unicode 文字を使用した qtree 名やディレクトリ名を含めることができます。 volume show 親ボリュームの言語設定が UTF-8 の場合は、コマンドでこれらの名前が正しく表示されます。ただし、親ボリュームの言語設定が UTF-8 のいずれかでない場合は、ジャンクションパスの一部が数値の NFS 名に置き換えられて表示されます。

- 9.5 以降のリリースでは、qtree が utf8mb4 に対応したボリュームに含まれていれば、qtree 名で 4 バイト文字がサポートされます。

ボリュームでの **SMB** ファイル名の変換のための文字マッピングを設定します

NFS クライアントは、SMB クライアントと特定の Windows アプリケーションでは無効な文字を含むファイル名を作成できます。ボリュームにおけるファイル名の変換のための文字マッピングを設定できます。これにより、そのままでは無効な NFS 名を持つファイルに SMB クライアントからアクセスできます。

このタスクについて

SMB クライアントが NFS クライアントによって作成されたファイルにアクセスすると、ONTAP はファイル名を調べます。ファイル名が有効な SMB ファイル名でない場合は（たとえば、コロンが含まれている場合）、ONTAP は各ファイルに対して保持されている 8.3 形式のファイル名を返します。ただし、これにより、長いファイル名に重要な情報をエンコードするアプリケーションで問題が発生します。

したがって、異なるオペレーティングシステムを使用するクライアント間でファイルを共有する場合は、両方のオペレーティングシステムで有効な文字をファイル名に使用する必要があります。

ただし、SMB クライアントで有効でない文字を含む NFS クライアントが作成したファイル名がある場合は、無効な NFS の文字を、SMB と特定の Windows アプリケーションの両方で有効な Unicode 文字に変換するマッピングを定義できます。たとえば、この機能は CATIAR MCAD および Mathematica アプリケーションをサポートしていますが、同じ要件を持つほかのアプリケーションでも使用できます。

文字マッピングはボリューム単位で設定できます。

ボリュームで文字マッピングを設定する場合は、次の点に注意する必要があります。

- 文字マッピングは、ジャンクションポイントをまたいで適用されません。

文字マッピングは、各ジャンクションボリュームに対して明示的に設定する必要があります。

- 無効な文字を表す Unicode 文字が、通常はファイル名に使用されないようにする必要があります。これらの文字が使用されていた場合、不要なマッピングが発生します。

たとえば ' コロン (:) をハイフン (-) にマップしようとした場合 ' ファイル名にハイフン (-) が正しく使用さ

れていれば 'Windows クライアントが "a-b" という名前のファイルにアクセスしようとする' その要求は NFS 名 "a:b" にマップされます ( 望ましい結果ではありません )

- 文字マッピングを適用してもまだマッピングに無効な Windows 文字が含まれている場合、ONTAP は Windows 8.3 ファイル名にフォールバックします。
- FPolicy 通知、NAS 監査ログ、セキュリティトレースメッセージでは、マッピングされたファイル名が表示されます。
- タイプが DP である SnapMirror 関係が作成されても、ソースボリュームの文字マッピングはデスティネーション DP ボリュームにレプリケートされません。
- 大文字と小文字の区別：マッピングされた Windows 名は NFS 名に変換されるため、名前の検索は NFS のセマンティクスに従います。NFS ルックアップでは大文字と小文字が区別されるという事実も含まれます。つまり、マッピングされた共有にアクセスするアプリケーションは、Windows の大文字と小文字を区別しない動作に依存しません。ただし、8.3 形式の名前は大文字と小文字が区別されません。
- 部分マッピングまたは無効なマッピング：ディレクトリ列挙 ( 「dir」 ) を実行しているクライアントに返すように名前をマッピングしたあと、結果の Unicode 名について Windows の有効性がチェックされます。その名前にまだ無効な文字が含まれている場合、または Windows で無効な文字が含まれている場合 ( 「.」または空白で終わる場合など ) は、無効な名前の代わりに 8.3 形式の名前が返されます。

## ステップ

### 1. 文字マッピングを設定します。

```
vserver cifs character-mapping create -vserver vserver_name -volume  
volume_name -mapping mapping_text, ...
```

マッピングは、「:」で区切られたソース文字とターゲット文字のペアのリストで構成されます。文字は、16 進数値で入力された Unicode 文字です。例：3C : E03C

それぞれの最初の値 mapping\_text コロンで区切られたペアは、変換する NFS 文字の 16 進値です。2 番目の値は、SMB で使用される Unicode 値です。マッピングのペアは一意である必要があります ( 1 対 1 のマッピングが存在する必要があります ) 。

#### ◦ ソースマッピング

次の表に、ソースマッピングで許可されている Unicode 文字セットを示します。

Unicode 文字	印刷された文字	説明
0x01-0x19	該当なし	印刷されない制御文字
0x5C	\	バックスラッシュ
0x3a	:	コロン
0x2A	*	アスタリスク
0x3f	?	疑問符
0x22	"	引用符

0x3C	<	より小さい
0x3E	>	が次の値より大きい
0x7C		
縦線	0xb1	±

。ターゲットマッピング

ターゲット文字には、U+E0000...U+F8FF の範囲の Unicode の「私用領域」を指定できます。

例

次のコマンドは、Storage Virtual Machine（SVM）vs1 上の「data」という名前のボリュームに文字マッピングを作成します。

```
cluster1::> vsriver cifs character-mapping create -volume data -mapping
3c:e17c,3e:f17d,2a:f745
cluster1::> vsriver cifs character-mapping show
```

Vserver	Volume Name	Character Mapping
vs1	data	3c:e17c, 3e:f17d, 2a:f745

**SMB** ファイル名の変換のための文字マッピングを管理するコマンド

FlexVol での SMB ファイル名の変換に使用する情報を作成、変更、表示したり、ファイル文字マッピングを削除したりすることで、文字マッピングを管理できます。

状況	使用するコマンド
新しいファイル文字マッピングを作成します	<code>vsriver cifs character-mapping create</code>
ファイル文字マッピングに関する情報を表示する	<code>vsriver cifs character-mapping show</code>
既存のファイル文字マッピングを変更します	<code>vsriver cifs character-mapping modify</code>
ファイル文字マッピングを削除します	<code>vsriver cifs character-mapping delete</code>

詳細については、各コマンドのマニュアルページを参照してください。

# NFS トランキングを管理します。

## NFS トランキングの概要

ONTAP 9.14.1以降では、セッショントランキングを利用してNFSサーバ上の異なるLIFへの複数の接続を開くことができるため、データ転送速度が向上し、マルチパスによる耐障害性が実現します。

トランキングは、FlexVolボリュームをトランキング対応のクライアント（特にVMwareおよびLinuxクライアント）にエクスポートする場合や、NFS over RDMA、TCP、pNFSにエクスポートする場合に便利です。

ONTAP 9.14.1では、トランキングは1つのノードのLIFに制限されます。トランキングは複数のノードにまたがるLIFにはできません。

FlexGroupボリュームはトランキングでサポートされています。これによりパフォーマンスは向上しますが、FlexGroupボリュームへのマルチパスアクセスはシングルノードでしか設定できません。

このリリースのマルチパスでは、セッショントランキングのみがサポートされます。

## トランキングの使用方法

トランキングによるマルチパスのメリットを活用するには、トランキング対応NFSサーバがあるSVMに関連付けられた一連のLIF（\_trunking group\_と呼ばれます）が必要です。トランキンググループ内のLIFは、クラスタの同じノードにホームポートがあり、それらのホームポートに配置されている必要があります。トランキンググループ内のすべてのLIFが同じフェイルオーバーグループのメンバーであることを推奨します。

ONTAPでは、1つのクライアントからノードあたり最大16のトランク接続がサポートされます。

クライアントがトランキング対応サーバからエクスポートをマウントする場合、クライアントはトランキンググループ内のLIFのIPアドレスの数を指定します。クライアントが最初のLIFに接続したあとに追加されたLIFは、NFSv4.1セッションに追加され、トランキンググループの要件を満たしている場合にのみトランキングに使用されます。クライアントは、独自のアルゴリズム（ラウンドロビンなど）に基づいて、複数の接続にNFS処理を分散します。

最大のパフォーマンスを得るには、シングルパスエクスポートではなく、マルチパスエクスポート専用のSVMでトランキングを設定します。つまり、トランキングが有効なクライアントのみにエクスポートが提供されているSVM内のNFSサーバでのみトランキングを有効にします。

## サポートされるクライアント

ONTAP NFSv4.1サーバは、NFSv4.1セッショントランキングに対応したすべてのクライアントとのトランキングをサポートしています。

次のクライアントは、ONTAP 9.14.1でテスト済みです。

- VMware-ESXi 7.0U3F以降
- Linux - Red Hat Enterprise Linux (RHEL) 8.8および9.3



NFSサーバでトランキングが有効になっている場合、トランキングをサポートしていないNFSクライアントでエクスポートされた共有にアクセスすると、パフォーマンスが低下することがあります。これは、SVMデータLIFへの複数のマウントに使用されるTCP接続が1つだけであるためです。

## NFSトランキングとnconnectの違い

ONTAP 9.8 以降では、NFSv4.1 が有効になっている場合、nconnect 機能がデフォルトで使用できます。nconnect対応クライアントでは、1つのNFSマウントで、1つのLIFを介して複数のTCP接続（最大16）を確立できます。

一方、トランキングは\_multipathing\_functionalityで、複数のLIFを介して複数のTCP接続を提供します。環境に追加のNICを使用できる場合は、トランキングによってnconnectの機能を越えた並列処理とパフォーマンスが向上します。

の詳細を確認してください ["nconnect : "](#)

## トランキング用に新しいNFSサーバとエクスポートを設定する

トランキングが有効なNFSサーバを作成する

ONTAP 9.14.1以降では、NFSサーバでトランキングを有効にできます。NFSv4.1 は、NFSサーバの作成時にデフォルトで有効になります。

作業を開始する前に

SVMの条件：

- クライアントのデータ要件に対応する十分なストレージを基盤としています。
- NFSに対して有効にします。
- NFSトランキング専用。他のクライアントは設定しないでください。

手順

1. 適切なSVMが存在しない場合は作成します。

```
vserver create -vserver svm_name -rootvolume root_volume_name -aggregate aggregate_name -rootvolume-security-style unix -language C.UTF-8
```

2. 新しく作成した SVM の設定とステータスを確認します。

```
vserver show -vserver svm_name
```

の詳細を確認してください ["SVMを作成する。"](#)

3. NFSサーバを作成します。

```
vserver nfs create -vserver svm_name -v3 disabled -v4.0 disabled -v4.1 enabled -v4.1-trunking enabled -v4-id-domain my_domain.com
```

4. NFS が実行されていることを確認します。



```
vserver nfs status -vserver svm_name
```

5. NFS が必要に応じて設定されていることを確認します。

```
vserver nfs show -vserver svm_name
```

の詳細を確認してください ["NFSサーバの設定"](#)

完了後

必要に応じて次のサービスを設定します。

- ["DNS"](#)
- ["LDAP"](#)
- ["Kerberos"](#)

ネットワークをトランキング用に準備する

NFSv4.1 トランキングを利用するには、トランキンググループ内のLIFが同じノードに配置され、同じノードにホームポートがある必要があります。LIFは、同じノードのフェイルオーバーグループに設定する必要があります。

このタスクについて

LIFとNICを1対1でマッピングするとパフォーマンスが最大限に向上しますが、トランキングを有効にする必要はありません。少なくとも2つのNICをインストールするとパフォーマンスが向上しますが、必須ではありません。

複数のフェイルオーバーグループを設定できますが、トランキングのフェイルオーバーグループにはトランキンググループに含めるLIFだけを指定する必要があります。

フェイルオーバーグループの接続（および基盤となるNIC）を追加または削除するときは、常にトランキングフェイルオーバーグループを調整する必要があります。

作業を開始する前に

- フェイルオーバーグループを作成する場合は、NICに関連付けられているポート名を確認しておく必要があります。
- すべてのポートが同じノード上にある必要があります。

手順

1. 使用するネットワークポートの名前とステータスを確認します。

```
network port status
```

2. フェイルオーバーグループを作成します。

```
network interface failover-groups create -vserver svm_name -failover-group failover_group_name -targets ports_list
```



フェイルオーバーグループは必須ではありませんが、使用することを強く推奨します。

- `svm_name` は、NFSサーバが含まれているSVMの名前です。
- `ports_list` は、フェイルオーバーグループに追加するポートのリストです。

ポートは `_node_name : port_number_` の形式で追加します（例：node1 : e0c）。

次のコマンドは、SVM vs1にフェイルオーバーグループfg3を作成し、ポートを3つ追加します。

```
network interface failover-groups create -vserver vs1 -failover-group fg3
-targets cluster1-01:e0c,cluster1-01:e0d,cluster1-01:e0e
```

の詳細を確認してください ["フェイルオーバーグループ："](#)

### 3. 必要に応じて、トランキンググループのメンバー用のLIFを作成します。

```
network interface create -vserver svm_name -lif lif_name -home-node node_name
-home-port port_name -address IP_address -netmask IP_address [-service-policy
policy] [-auto-revert {true|false}]
```

- `-home-node` - `network interface revert` コマンドをLIFで実行したときにLIFに戻るノード。

を使用して、LIFをホームノードおよびホームポートに自動的にリバートするかどうかを指定することもできます `-auto-revert` オプション

- `-home-port` は、`network interface revert` コマンドをLIFに対して実行したときにLIFに戻る物理ポートまたは論理ポートです。
- でIPアドレスを指定できます `-address` および `-netmask` オプション（ではなく） `-subnet` オプション
- 別のIPサブネットにクライアントまたはドメインコントローラがある場合は、IPアドレスを割り当てるときに、ゲートウェイへのデフォルトルートの設定が必要になることがあります。。 `network route create` のマニュアルページには、SVM内での静的ルートの作成に関する情報が記載されています。
- `-service-policy` - LIFのサービスポリシー。ポリシーを指定しない場合、デフォルトのポリシーが自動的に割り当てられます。を使用します `network interface service-policy show` 使用可能なサービスポリシーを確認するためのコマンド。
- `-auto-revert` - 起動時、管理データベースのステータスが変化したとき、ネットワーク接続が確立されたときなどの状況で、データLIFがホームノードに自動的にリバートされるかどうかを指定します。デフォルト設定はfalseですが、環境内のネットワーク管理ポリシーに応じてtrueに設定できます。

トランキンググループ内のすべてのLIFに対してこの手順を繰り返します。

次のコマンドを実行すると、lif-A SVM用 vs1、ポート e0c ノード cluster1\_01：

```
network interface create -vserver vs1 -lif lif-A -service-policy ??? -home
-node cluster1_01 -home-port e0c -address 192.0.2.0
```

の詳細を確認してください ["LIFの作成"](#)

### 4. LIFが作成されたことを確認します。

```
network interface show
```

5. 設定したIPアドレスに到達できることを確認します。

対象	使用
IPv4 アドレス	network ping
IPv6アドレス	network ping6

クライアントアクセス用のデータのエクスポート

データ共有へのクライアントアクセスを許可するには、ボリュームを1つ以上作成し、ボリュームに少なくとも1つのルールが設定されたエクスポートポリシーを設定する必要があります。

クライアントのエクスポート要件：

- Linuxクライアントでは、トランキング接続ごと（つまりLIFごと）に、個別のマウントと個別のマウントポイントが必要です。
- VMwareクライアントでは、複数のLIFを指定したエクスポートされたボリュームに対してマウントポイントが1つだけ必要です。

VMwareクライアントには、エクスポートポリシーでルートアクセスが必要です。

手順

1. エクスポートポリシーを作成する

```
vserver export-policy create -vserver svm_name -policyname policy_name
```

ポリシー名に指定できる文字数は最大 256 文字です。

2. エクスポートポリシーが作成されたことを確認します。

```
vserver export-policy show -policyname policy_name
```

例

次のコマンドは、vs1 という SVM で、exp1 という名前のエクスポートポリシーを作成し、作成を確認します。

```
vs1::> vserver export-policy create -vserver vs1 -policyname exp1
```

3. エクスポートルールを作成して既存のエクスポートポリシーに追加します。

```
vserver export-policy rule create -vserver svm_name -policyname policy_name  
-ruleindex integer -protocol nfs4 -clientmatch { text | "text,text,..." }  
-rorule security_type -rwrule security_type -superuser security_type -anon  
user_ID
```

- 。 -clientmatch パラメータには、エクスポートをマウントするトランキング対応のLinuxまた

はVMwareクライアントを指定する必要があります。

の詳細を確認してください ["エクスポートルールを作成しています。"](#)

#### 4. ジャンクションポイントを指定してボリュームを作成します。

```
volume create -vserver svm_name -volume volume_name -aggregate aggregate_name  
-size {integer[KB|MB|GB|TB|PB]} -security-style unix -user user_name_or_number  
-group group_name_or_number -junction-path junction_path -policy  
export_policy_name
```

詳細はこちら ["ボリュームを作成します。"](#)

#### 5. 目的のジャンクションポイントでボリュームが作成されたことを確認します。

```
volume show -vserver svm_name -volume volume_name -junction-path
```

### クライアントマウントの作成

トランキングをサポートするLinuxおよびVMwareクライアントは、トランキングが有効になっているONTAP NFSv4.1サーバからボリュームまたはデータ共有をマウントできます。

クライアントでmountコマンドを入力する場合は、トランキンググループ内の各LIFのIPアドレスを入力する必要があります。

詳細はこちら ["サポートされるクライアント"](#)。

#### Linuxクライアントの要件

トランキンググループ内の接続ごとに、個別のマウントポイントが必要です。

次のようなコマンドを使用して、エクスポートしたボリュームをマウントします。

```
mount lif1_ip:/vol-test /mnt/test1 -o vers=4.1,max_connect=16
```

```
mount lif2_ip:/vol-test /mnt/test2 -o vers=4.1,max_connect=16
```

バージョン (vers) の値は次のとおりです。 4.1 以降が必要です。

。 max\_connect 値は、トランキンググループ内の接続数に対応します。

#### VMwareクライアントの要件

トランキンググループ内の各接続のIPアドレスを含むMOUNTステートメントが必要です。

次のようなコマンドを使用して、エクスポートしたデータストアをマウントします。

```
#esxcli storage nfs41 -H lif1_ip, lif2_ip -s /mnt/sh are1 -v nfs41share
```

。 -H 値はトランキンググループの接続に対応します。

## 既存のNFSエクスポートをトランキングに適合させる

### シングルパスエクスポートの適応の概要

既存のシングルパス（非トランキング）のNFSv4.1エクスポートでトランキングを使用するように設定できます。トランキング対応のクライアントは、サーバとクライアントの前提条件を満たしていれば、サーバでトランキングが有効になるとすぐにパフォーマンスの向上を利用できます。

シングルパスエクスポートをトランキング用に適応させると、エクスポートされたデータセットを既存のボリュームおよびSVMに保持できます。これを行うには、NFSサーバでトランキングを有効にし、ネットワーク設定とエクスポート設定を更新し、エクスポートされた共有をクライアントに再マウントする必要があります。

トランキングをイネーブルにすると、サーバが再起動されます。VMwareクライアントでは、エクスポートしたデータストアを再マウントする必要があります。Linuxクライアントでは、エクスポートしたボリュームを `max_connect` オプション

### NFSサーバでトランキングを有効にする

トランキングはNFSサーバで明示的に有効にする必要があります。NFSv4.1は、NFSサーバの作成時にデフォルトで有効になります。

トランキングを有効にしたら、次のサービスが必要に応じて設定されていることを確認します。

- ["DNS"](#)
- ["LDAP"](#)
- ["Kerberos"](#)

### 手順

1. トランキングを有効にし、NFSv4.1が有効になっていることを確認します。

```
vserver nfs create -vserver svm_name -v4.1 enabled -v4.1-trunking enabled
```

2. NFS が実行されていることを確認します。

```
vserver nfs status -vserver svm_name
```

3. NFS が必要に応じて設定されていることを確認します。

```
vserver nfs show -vserver svm_name
```

の詳細を確認してください ["NFSサーバの設定"](#)

。このSVMからWindowsクライアントにデータを提供する場合は、共有を移動してからサーバを削除します。

```
vserver cifs show -vserver svm_name
```

[+]

```
vserver cifs delete -vserver svm_name
```

NFSv4.1 トランキングを使用するには、トランキンググループ内のLIFが同じノードに配置され、同じノードにホームポートがある必要があります。すべてのLIFは、同じノードのフェイルオーバーグループに設定する必要があります。

このタスクについて

LIFとNICを1対1でマッピングするとパフォーマンスが最大限に向上しますが、トランキングを有効にするためには必要ありません。

複数のフェイルオーバーグループを設定できますが、トランキングのフェイルオーバーグループにはトランキンググループに含まれるLIFだけを指定する必要があります。

フェイルオーバーグループの接続（および基盤となるNIC）を追加または削除するときは、常にトランキングフェイルオーバーグループを調整する必要があります。

作業を開始する前に

- フェイルオーバーグループを作成するには、NICに関連付けられているポート名を確認しておく必要があります。
- すべてのポートが同じノード上にある必要があります。

手順

1. 使用するネットワークポートの名前とステータスを確認します。

```
network port show
```

2. トランキングフェイルオーバーグループを作成するか、既存のフェイルオーバーグループを変更します。

```
network interface failover-groups create -vserver svm_name -failover-group failover_group_name -targets ports_list
```

```
network interface failover-groups modify -vserver svm_name -failover-group failover_group_name -targets ports_list
```



フェイルオーバーグループは必須ではありませんが、使用することを強く推奨します。

- ° `svm_name` は、NFSサーバが含まれているSVMの名前です。
- ° `ports_list` は、フェイルオーバーグループに追加するポートのリストです。

ポートは次の形式で追加されます。 `node_name:port_number` 例えば、 ``node1:e0c`。

次のコマンドは、フェイルオーバーグループを作成します。 fg3 SVM vs1にポートを3つ追加します。

```
network interface failover-groups create -vserver vs1 -failover-group fg3 -targets cluster1-01:e0c,cluster1-01:e0d,cluster1-01:e0e
```

の詳細を確認してください ["フェイルオーバーグループ："](#)

### 3. 必要に応じて、トランキンググループのメンバー用に追加のLIFを作成します。

```
network interface create -vserver svm_name -lif lif_name -home-node node_name
-home-port port_name -address IP_address -netmask IP_address [-service-policy
policy] [-auto-revert {true|false}]
```

- -home-node - network interface revertコマンドをLIFで実行したときにLIFが戻るノード。

LIFをホームノードとホームポートに自動的にリバートするかどうかを指定するには、 -auto  
-revert オプション

- -home-port は、network interface revertコマンドをLIFに対して実行したときにLIFが戻る物理ポートまたは論理ポートです。
- でIPアドレスを指定できます -address および -netmask オプション（Options）
- IPアドレスを手動で（サブネットを使用せずに）割り当てるときに、クライアントまたはドメインコントローラが別のIPサブネットにある場合は、ゲートウェイへのデフォルトルートの設定が必要になることがあります。SVM内で静的ルートを作成する方法については、network route createのマニュアルページを参照してください。
- -service-policy - LIFのサービスポリシー。ポリシーを指定しない場合、デフォルトのポリシーが自動的に割り当てられます。を使用します network interface service-policy show 使用可能なサービスポリシーを確認するためのコマンド。
- -auto-revert -起動時、管理データベースのステータスが変化したとき、ネットワーク接続が確立されたときなどの状況で、データLIFがホームノードに自動的にリバートされるかどうかを指定します。\*デフォルト設定はfalse \*ですが、環境内のネットワーク管理ポリシーに応じてtrueに設定できます。

トランキンググループに追加するLIFごとに、この手順を繰り返します。

次のコマンドは、ノードcluster1\_01のポートe0cにSVM vs1用のlif-aを作成します。

```
network interface create -vserver vs1 -lif lif-A -service-policy default-
intercluster -home-node cluster1_01 -home-port e0c -address 192.0.2.0
```

の詳細を確認してください "[LIFの作成](#)"

### 4. LIFが作成されたことを確認します。

```
network interface show
```

### 5. 設定した IP アドレスに到達できることを確認します。

対象	使用
IPv4 アドレス	network ping
IPv6アドレス	network ping6

クライアントアクセス用のデータエクスポートを変更します。

クライアントが既存のデータ共有のトランキングを利用できるようにするには、エクス

ポートポリシーとルール、およびそれらが接続されているボリュームの変更が必要になる場合があります。LinuxクライアントとVMwareデータストアには、エクスポートに関するさまざまな要件があります。

クライアントのエクスポート要件：

- Linuxクライアントでは、トランキング接続ごと（つまりLIFごと）に、個別のマウントと個別のマウントポイントが必要です。

ONTAP 9.14.1にアップグレードしていて、すでにボリュームをエクスポートしている場合は、そのボリュームをトランキンググループで引き続き使用できます。

- VMwareクライアントでは、複数のLIFを指定したエクスポートされたボリュームに対してマウントポイントが1つだけが必要です。

VMwareクライアントには、エクスポートポリシーでルートアクセスが必要です。

手順

1. 既存のエクスポートポリシーが設定されていることを確認します。

```
vserver export-policy show
```

2. 既存のエクスポートポリシールールがトランキング構成に適していることを確認します。

```
vserver export-policy rule show -policyname policy_name
```

特に、`-clientmatch` パラメータを指定すると、エクスポートをマウントするトランキング対応のLinuxクライアントまたはVMwareクライアントが正しく識別されます。

調整が必要な場合は、`vserver export-policy rule modify` コマンドを実行するか、新しいルールを作成します。

```
vserver export-policy rule create -vserver svm_name -policyname policy_name
-ruleindex integer -protocol nfs4 -clientmatch { text | "text,text,..." }
-rorule security_type -rwrule security_type -superuser security_type -anon
user_ID
```

の詳細を確認してください ["エクスポートルールを作成しています。"](#)

3. エクスポートした既存のボリュームがオンラインであることを確認します。

```
volume show -vserver svm_name
```

クライアントマウントの再確立

トランキングされていないクライアント接続をトランキングされた接続に変換するには、LinuxクライアントおよびVMwareクライアントの既存のマウントを、LIFに関する情報を使用してアンマウントし、再マウントする必要があります。

クライアントでmountコマンドを入力する場合は、トランキンググループ内の各LIFのIPアドレスを入力する



必要があります。

詳細はこちら ["サポートされるクライアント"](#)。



VMwareクライアントをアンマウントすると、データストア上のVMが停止します。別の方法として、トランキングを有効にした新しいデータストアを作成し、\* Storage VMotion \*を使用してVMを古いデータストアから新しいデータストアに移動します。詳細については、VMwareのドキュメントを参照してください。

#### Linuxクライアントの要件

トランキンググループ内の接続ごとに、個別のマウントポイントが必要です。

次のようなコマンドを使用して、エクスポートしたボリュームをマウントします。

```
mount lif1_ip:/vol-test /mnt/test1 -o vers=4.1,max_connect=2
```

```
mount lif2_ip:/vol-test /mnt/test2 -o vers=4.1,max_connect=2
```

- 。 vers 値は次のでなければなりません： 4.1 以降が必要です。
- 。 max\_connect 値は、トランキンググループ内の接続数に対応している必要があります。

#### VMwareクライアントの要件

トランキンググループ内の各接続のIPアドレスを含むMOUNTステートメントが必要です。

次のようなコマンドを使用して、エクスポートしたデータストアをマウントします。

```
#esxcli storage nfs41 -H lif1_ip, lif2_ip -s /mnt/sh are1 -v nfs41share
```

- 。 -H 値はトランキンググループの接続に対応している必要があります。

## RDMA 経由の NFS を管理します

### RDMA経由のNFS

NFS over RDMA は RDMA アダプタを使用し、ストレージシステムメモリとホストシステムメモリの間でデータを直接コピーできるため、CPU の中断やオーバーヘッドは発生しません。

NFS over RDMA 構成は、レイテンシの影響を受けやすいワークロードや、マシンラーニングや分析などの広帯域幅ワークロードを使用するお客様向けに設計されています。NVIDIA は、GPU Direct Storage (GDS) を有効にするために RDMA 経由の NFS を拡張しました。GDSはRDMAを使用してストレージシステムとGPUメモリ間でデータを直接転送することで、CPUとメインメモリを完全にバイパスすることで、GPU対応のワークロードをさらに高速化します。

ONTAP 9.14.1以降では、RDMA経由のNFS構成がNFSv4.1プロトコルでサポートされます。

ONTAP 9.10.1以降では、RDMA経由のNFS構成が、Mellanox CX-5またはCX-6アダプタと一緒に使用した場

合にNFSv4.0プロトコルでサポートされます。このアダプタでは、バージョン2のRoCEプロトコルを使用するRDMAがサポートされます。GDS は、 Mellanox NIC カードと MOFED ソフトウェアを搭載した NVIDIA Tesla および Ampere ファミリー GPU のみを使用してサポートされます。

NFS over RDMA のサポートは、ノードローカルトラフィックのみに限定されます。同じノード上のすべてのコンスチチュエントがサポートされ、同じノード上の LIF からアクセスできる標準の FlexVol または FlexGroup。NFS マウントのサイズが 64k を超えると、NFS over RDMA 構成でパフォーマンスが不安定になります。

#### 要件

- ストレージシステムでONTAP 9.10.1以降が実行されている必要があります
  - ONTAP 9.12.1以降では、System Managerを使用してRDMA経由のNFSを設定できます。ONTAP 9.10.1および9.11.1では、CLIを使用してRDMA上のNFSを設定する必要があります。
- HAペアの両方のノードのバージョンを同じにする必要があります。
- ストレージシステムコントローラにはRDMAがサポートされている必要があります。

ONTAPで開始しています...	次のコントローラがRDMAをサポートしています...
9.10.1以降	<ul style="list-style-type: none"><li>• A400</li><li>• A700</li><li>• A800</li></ul>
ONTAP 9.14.1以降	<ul style="list-style-type: none"><li>• AFF Cシリーズ</li><li>• A900</li></ul>

- RDMAでサポートされるハードウェア（例 Mellanox CX-5またはCX-6）
- RDMA をサポートするには、データ LIF を設定する必要があります。
- クライアントで Mellanox RDMA 対応 NIC カードと Mellanox OFED （ MOFED ） ネットワークソフトウェアを使用している必要があります。



インターフェイスグループはNFS over RDMAではサポートされません。

#### 次のステップ

- [NFS over RDMA 用に NIC を設定します](#)
- [NFS over RDMA 用に LIF を設定します](#)
- [NFS over RDMA の NFS 設定](#)

#### 関連情報

- ["RDMA"](#)
- [NFSトランキングの概要](#)
- ["RFC 7530 ： NFS バージョン 4 プロトコル"](#)
- ["RFC 8166 ： リモート手順コールバージョン 1 用のリモートダイレクトメモリアクセストランスポート"](#)
- ["RFC 8167 ： RPC-over-RDMA トランスポート上の双方向リモート手順コール"](#)

- ["RFC 8267 : RPC-over-RDMA バージョン 1 への NFS 上位レイヤバインディング"](#)

## NFS over RDMA 用に NIC を設定します

NFS over RDMA では、クライアントシステムとストレージプラットフォームの両方に NIC を設定する必要があります。

### ストレージプラットフォームの構成

サーバに X1148 RDMA アダプタをインストールする必要があります。HA 構成を使用している場合は、フェイルオーバーパートナーに対応する X1148 アダプタを用意して、フェイルオーバー中も RDMA サービスを継続できるようにする必要があります。NIC は ROCE 対応である必要があります。

ONTAP 9.10.1以降では、次のコマンドを使用して、RDMAオフロードプロトコルのリストを表示できます。

```
network port show -rdma-protocols roce
```

### クライアントシステム構成

クライアントで Mellanox RDMA 対応 NIC カード（例 X1148）および Mellanox OFED ネットワークソフトウェア。サポートされるモデルとバージョンについては、Mellanox のドキュメントを参照してください。クライアントとサーバは直接接続できますが、スイッチのフェイルオーバーパフォーマンスが向上するため、スイッチの使用を推奨します。

クライアント、サーバ、およびスイッチ、およびスイッチ上のすべてのポートは、ジャンボフレームを使用して設定する必要があります。また、すべてのスイッチでプライオリティフロー制御が有効であることを確認します。

この設定を確認したら、NFS をマウントできます。

## System Manager の略

System Managerを使用してRDMA経由のNFSでネットワークインターフェイスを設定するには、ONTAP 9.12.1以降を使用している必要があります。

### 手順

1. RDMAがサポートされるかどうかを確認します。[Network]>[Ethernet Ports]に移動し、グループビューで適切なノードを選択します。ノードを拡張する際には、所定のポートについて\* rdma protocols フィールドを確認します。値 RoCE は**RDMA**がサポートされていることを示し、ダッシュ (-\*) はサポートされていないことを示します。
2. VLANを追加するには、**+VLAN\***を選択します。適切なノードを選択します。**RDMA**をサポートしているポートは、「Port」ドロップダウンメニューに「RoCE Enabled \*」というテキストが表示されます。RDMAをサポートしていないポートについては、テキストは表示されません。
3. のワークフローに従ってください [NFS を使用して Linux サーバ用の NAS ストレージを有効にします](#) 新しいNFSサーバを設定します。

ネットワークインターフェイスを追加する際には、「\* RoCEポートを使用\*」を選択できます。RDMA経由のNFSを使用するすべてのネットワークインターフェイスで、このオプションを選択します。

### CLI の使用

1. 次のコマンドを使用して、NFS サーバで RDMA アクセスが有効になっているかどうかを確認します。

```
vserver nfs show -vserver SVM_name
```

デフォルトでは、-rdma を有効にする必要があります。サポートされていない場合は、NFS サーバで RDMA アクセスを有効にします。

```
vserver nfs modify -vserver SVM_name -rdma enabled
```

2. クライアントを RDMA 経由で NFSv4.0 にマウントします。
  - a. proto パラメータの入力は、サーバの IP プロトコルのバージョンによって異なります。IPv4の場合は、を使用します proto=rdma。IPv6の場合は、proto=rdma6。
  - b. NFSターゲットポートをと指定します port=20049 標準ポート2049ではなく、次の手順を実行します。

```
mount -o vers=4,minorversion=0,proto=rdma,port=20049 Server_IP_address  
:/volume_path mount_point
```

3. オプション：クライアントをアンマウントする必要がある場合は、コマンドを実行します unmount mount\_path

### 詳細情報

- [NFS サーバを作成します](#)
- [NFS を使用して Linux サーバ用の NAS ストレージを有効にします](#)

## NFS over RDMA 用に LIF を設定します

NFS over RDMAを利用するには、LIF（ネットワークインターフェイス）をRDMA互換性を確保するように設定する必要があります。LIFとそのフェイルオーバーペアの両方がRDMAをサポートしている必要があります。

新しい LIF を作成

### System Manager の略

System ManagerでRDMA経由のNFS用のネットワークインターフェイスを作成するには、ONTAP 9.12.1以降を実行している必要があります。

手順

1. Network > Overview > Network Interfaces \*を選択します。
2. 選択するオプション **+ Add**。
3. NFS、SMB / CIFS、S3 \*を選択すると、RoCEポートを使用するオプションがあります。「RoCEポートを使用する」のチェックボックスをオンにします。
4. Storage VMとホームノードを選択します。名前を割り当てます。IPアドレスとサブネットマスクを入力します。
5. IPアドレスとサブネットマスクを入力すると、System Managerによって、ブロードキャストドメインのリストがRoCE対応ポートを持つドメインにフィルタリングされます。ブロードキャストドメインを選択してください。必要に応じて、ゲートウェイを追加できます。
6. [ 保存（ Save ） ] を選択します。

### CLI の使用

手順

1. LIF を作成します。

```
network interface create -vserver SVM_name -lif lif_name -service-policy
service_policy_name -home-node node_name -home-port port_name {-address
IP_address -netmask netmask_value | -subnet-name subnet_name} -firewall
-policy policy_name -auto-revert {true|false} -rdma-protocols roce
```


- サービスポリシーには、 default-data-files または dataNFS-NFS ネットワークインターフェイス サービスを含むカスタムポリシーを指定する必要があります。
- -rdma-protocols パラメータにはリストを指定できます。このリストはデフォルトでは空です。いつ roce また、LIFはRoCEオフロードをサポートしているポートでのみ設定でき、Bot LIFの移行とフェイルオーバーに影響します。

LIF を変更する

## System Manager の略

System ManagerでRDMA経由のNFS用のネットワークインターフェイスを作成するには、ONTAP 9.12.1以降を実行している必要があります。

### 手順

1. Network > Overview > Network Interfaces \*を選択します。
2. 選択するオプション  \*>変更するネットワークインターフェイスの横にある[Edit]をクリックします。
3. RoCEポートを使用する\*をオンにしてNFS over RDMAを有効にするか、オフにして無効にしてください。ネットワークインターフェイスがRoCE対応ポート上にある場合は、「RoCEポートを使用する」の横にチェックボックスが表示されます。
4. 必要に応じて、その他の設定を変更します。
5. 「\* Save \*（保存）」を選択して、変更を確定します。

### CLI の使用

1. LIFのステータスは、で確認できます `network interface show` コマンドを実行しますサービスポリシーに `data-nfs` ネットワークインターフェイスサービスを含める必要があります。。 `-rdma -protocols` リストにはと入力します `roce`。上記のいずれかの条件に該当しない場合は、LIF を変更します。
2. LIF を変更するには、次のコマンドを実行します。

```
network interface modify vservers SVM_name -lif lif_name -service-policy
service_policy_name -home-node node_name -home-port port_name {-address
IP_address -netmask netmask_value | -subnet-name subnet_name} -firewall
-policy policy_name -auto-revert {true|false} -rdma-protocols roce
```



特定のオフロードプロトコルを必要とするように LIF を変更した場合に、そのプロトコルをサポートするポートに LIF が割り当てられていないとエラーが発生します。

## LIF を移行

ONTAP では、RDMAを介したNFSを利用するために、ネットワークインターフェイス（LIF）を移行することもできます。この移行を実行する場合は、デスティネーションポートがRoCEに対応していることを確認する必要があります。ONTAP 9.12.1以降では、この手順をSystem Managerで実行できます。System Managerでネットワークインターフェイスのデスティネーションポートを選択すると、ポートがRoCEに対応しているかどうか指定されます。

次の場合にのみ、LIFをNFS over RDMA構成に移行できます。

- RoCE対応ポートでホストされるNFS RDMAネットワークインターフェイス（LIF）です。
- RoCE対応ポートでホストされるNFS TCPネットワークインターフェイス（LIF）です。
- RoCE非対応ポートでホストされるNFS TCPネットワークインターフェイス（LIF）です。

ネットワークインターフェイスの移行の詳細については、を参照してください [LIF を移行](#)。

## 詳細情報

- [LIF を作成](#)
- [LIF を作成](#)
- [LIF を変更する](#)
- [LIF を移行](#)

## NFS 設定を変更します

ほとんどの場合、NFS over RDMA用にNFS対応Storage VMの設定を変更する必要はありません。

ただし、Mellanox チップと LIF の移行に関する問題に対処するには、NFSv4 のロック猶予期間を延長する必要があります。デフォルトでは、猶予期間は 45 秒に設定されています。ONTAP 9.10.1以降の猶予期間の最大値は180（秒）です。

### 手順

1. 権限レベルを advanced に設定します。

```
set -privilege advanced
```

2. 次のコマンドを入力します。

```
vserver nfs modify -vserver SVM_name -v4-grace-seconds number_of_seconds
```

このタスクの詳細については、を参照してください [NFSv4 ロック猶予期間の指定](#)。

## CLI を使用して SMB を設定します

### CLIヲシヨウシタSMBセツテイノカイヨウ

ONTAP 9 の CLI コマンドを使用して、新規または既存の SVM の新しいボリュームまたは qtree に格納されているファイルへの SMB クライアントアクセスを設定できます。



SMB(Server Message Block) は、Common Internet File System (CIFS) プロトコルの最新のダイアレクトです。ONTAP コマンドラインインターフェイス（CLI）および OnCommand 管理ツールでは、\_cifs\_というメッセージが引き続き表示されます。

次の手順に従って、ボリュームまたは qtree への SMB アクセスを設定します。

- SMB のバージョン 2 以降を使用する必要がある。
- NFS クライアントではなく、SMB クライアントのみを対象とする（マルチプロトコル構成ではない）。
- 新しいボリュームはNTFSファイル権限を使用して保護されます。
- SVM 管理者権限ではなくクラスタ管理者権限を持っている。

SVM と LIF を作成するにはクラスタ管理者権限が必要です。他の SMB 設定タスクには、SVM 管理者権限で十分です。

- System Manager や自動スクリプトツールではなく、CLI を使用する。

System Manager を使用して NAS マルチプロトコルアクセスを設定するには、を参照してください ["NFS と SMB の両方を使用して Windows と Linux の両方に NAS ストレージをプロビジョニングする"](#)。

- すべての選択肢について検討するのではなく、ベストプラクティスに従う。

コマンド構文の詳細については、CLI ヘルプおよび ONTAP のマニュアルページを参照してください。

ONTAP の SMB プロトコル機能の範囲の詳細については、を参照してください ["SMB リファレンスの概要"](#)。

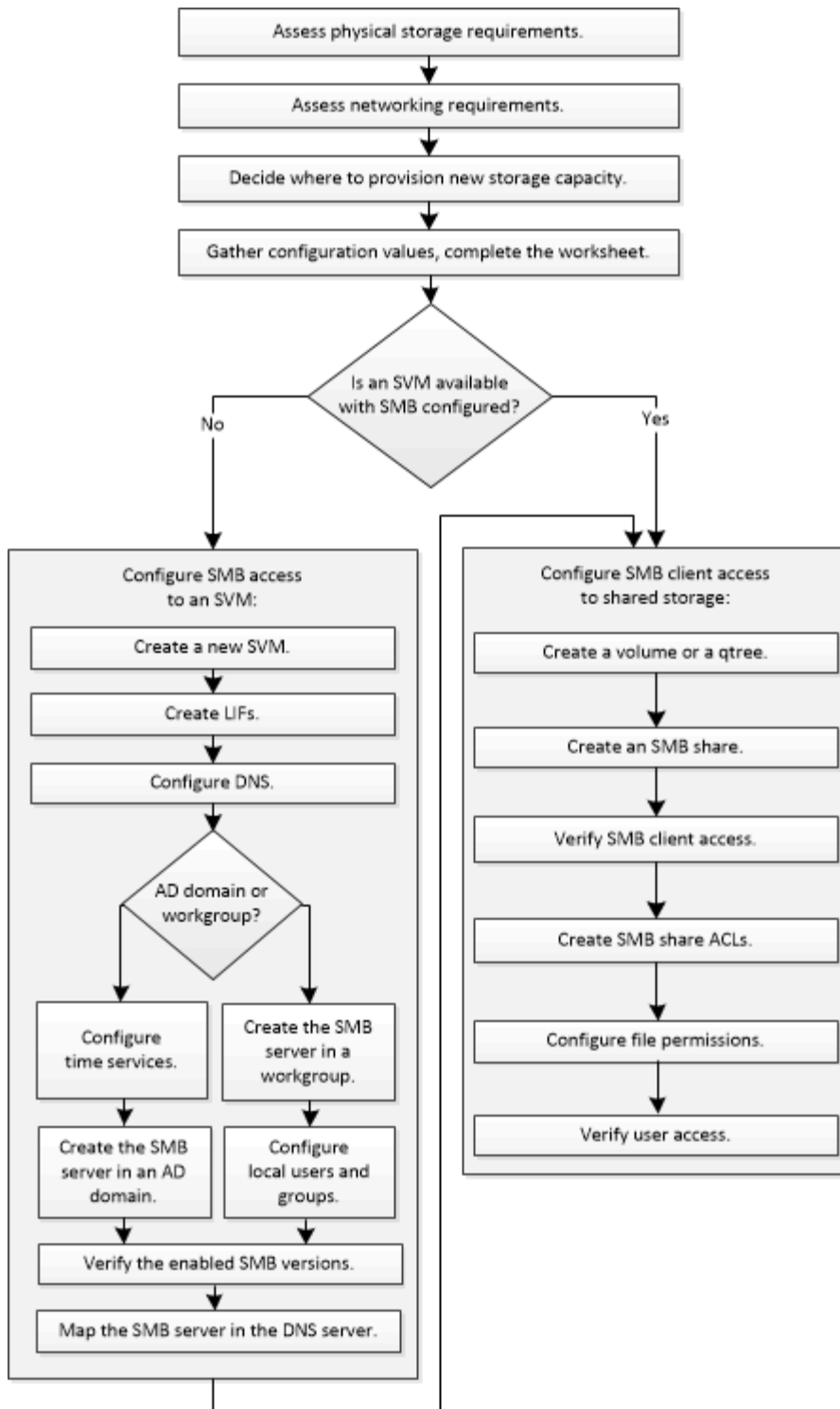
#### ONTAP でこれを行うその他の方法

実行するタスク	参照先
再設計された System Manager （ ONTAP 9.7 以降で使用可能）	<a href="#">"SMB を使用して Windows サーバ用の NAS ストレージをプロビジョニングする"</a>
System Manager Classic （ ONTAP 9.7 以前で使用可能）	<a href="#">"SMB セツテイ ノ カイ ヨウ"</a>

#### SMB の設定ワークフロー

SMB を設定するには、物理ストレージとネットワークの要件を評価して、目的に応じたワークフローを選択します。新規または既存の SVM への SMB アクセスを設定するか、すでに SMB アクセスの設定が完了している既存の SVM にボリュームまたは qtrees を追加するかによってワークフローが異なります。





## 準備

物理ストレージ要件を評価

クライアント用の SMB ストレージをプロビジョニングする前に、既存のアグリゲート内に新しいボリューム用の十分なスペースがあることを確認する必要があります。十分なスペースがない場合は、既存のアグリゲートにディスクを追加するか、必要なタイプの新しいアグリゲートを作成することができます。

## 手順

1. 既存のアグリゲート内の使用可能なスペースを表示します。 `storage aggregate show`

十分なスペースを備えたアグリゲートがある場合は、その名前をワークシートに記録します。

```
cluster::> storage aggregate show
Aggregate      Size Available Used% State  #Vols  Nodes  RAID Status
-----
aggr_0         239.0GB   11.13GB   95% online    1 node1  raid_dp, normal
aggr_1         239.0GB   11.13GB   95% online    1 node1  raid_dp, normal
aggr_2         239.0GB   11.13GB   95% online    1 node2  raid_dp, normal
aggr_3         239.0GB   11.13GB   95% online    1 node2  raid_dp, normal
aggr_4         239.0GB   238.9GB   95% online    5 node3  raid_dp, normal
aggr_5         239.0GB   239.0GB   95% online    4 node4  raid_dp, normal
6 entries were displayed.
```

2. 十分なスペースを備えたアグリゲートがない場合は、を使用して既存のアグリゲートにディスクを追加します `storage aggregate add-disks` コマンドを実行するか、を使用して新しいアグリゲートを作成します `storage aggregate create` コマンドを実行します

## ネットワーク要件を評価

クライアントにSMBストレージを提供する前に、SMBプロビジョニングの要件を満たすようにネットワークが正しく設定されていることを確認する必要があります。

作業を開始する前に

次のクラスタネットワークオブジェクトを設定する必要があります。

- 物理ポートと論理ポート
- ブロードキャストドメイン
- サブネット（必要な場合）
- IPspace（必要に応じて、デフォルトの IPspace に追加）
- フェイルオーバーグループ（必要に応じて、各ブロードキャストドメインのデフォルトのフェイルオーバーグループに追加）
- 外部ファイアウォール

## 手順

1. 使用可能な物理ポートと仮想ポートを表示します。 `network port show`

- 可能な場合は、データネットワークの速度が最高であるポートを使用する必要があります。
  - 最大限のパフォーマンスを得るためには、データネットワーク内のすべてのコンポーネントの MTU 設定が同じである必要があります。
2. サブネット名を使用して LIF の IP アドレスとネットワークマスク値を割り当てる場合は、そのサブネットが存在し、十分な数のアドレスが使用可能であることを確認します。 `network subnet show`

サブネットには、同じレイヤ 3 サブネットに属する IP アドレスのプールが含まれています。サブネットは、を使用して作成されます `network subnet create` コマンドを実行します

3. 使用可能な IPspace を表示します。 `network ipspace show`

デフォルトの IPspace またはカスタムの IPspace を使用できます。

4. IPv6 アドレスを使用する場合は、IPv6 がクラスタで有効になっていることを確認します。 `network options ipv6 show`

必要に応じて、を使用してIPv6を有効にできます `network options ipv6 modify` コマンドを実行します

新しい**SMB**ストレージ容量のプロビジョニング先を決定する

新しい SMB ボリュームまたは qtree を作成する前に、その配置先を新規、既存のどちらの SVM にするかを決め、SVM にどのような設定が必要になるかを確認しておく必要があります。これにより、ワークフローが決まります。

選択肢

- 新しい SVM、または SMB が有効になっているものの設定されていない既存の SVM 上でボリュームまたは qtree をプロビジョニングする場合は、「SVM への SMB アクセスの設定」と「SMB 対応 SVM へのストレージ容量の追加」の両方の手順を実行します。

### SVMへのSMBアクセスの設定

#### 共有ストレージへの SMB クライアントアクセスの設定

次のいずれかに該当する場合は、新しい SVM を作成します。

- クラスタでSMBを初めて有効にする場合。
- クラスタ内の既存のSVMでSMBサポートを有効にするのが望ましくない場合。
- クラスタ内に SMB 対応 SVM が 1 つ以上あり、次のいずれかの接続が必要な場合。
  - ワークグループ内の別の Active Directory フォレストへの接続。
  - 分離されたネームスペース内の SMB サーバへの接続（マルチテナンシーシナリオ）。SMBが有効になっているが設定はまだ完了していない既存のSVMでストレージをプロビジョニングする場合も、このオプションを選択する必要があります。これが当てはまるのは、SAN アクセス用の SVM を作成している場合や、SVM 作成時にどのプロトコルも有効になっていなかった場合です。

SVMでSMBを有効にしたあとに、ボリュームまたはqtreeのプロビジョニングに進みます。

- SMB アクセスの設定が完了している既存の SVM でボリュームまたは qtree をプロビジョニングする場合は、「SMB 対応 SVM へのストレージ容量の追加」の手順を実行します。

#### 共有ストレージへの SMB クライアントアクセスの設定

### SMB設定情報を収集するためのワークシート

SMB設定ワークシートを使用すると、クライアントのSMBアクセスを設定するために必要な情報を収集できます。

ストレージをプロビジョニングする場所に関する決定に応じて、ワークシートのいずれかまたは両方のセクションを完了する必要があります。

- SVMへのSMBアクセスを設定する場合は、両方のセクションを完了する必要があります。

#### SVMへのSMBアクセスの設定

#### 共有ストレージへの SMB クライアントアクセスの設定

- SMB対応SVMにストレージ容量を追加する場合は、2番目のセクションのみを完了する必要があります。

#### 共有ストレージへの SMB クライアントアクセスの設定

パラメータの詳細については、コマンドのマニュアルページを参照してください。

### SVMへのSMBアクセスの設定

- SVM を作成するためのパラメータ \*

では、次の値を指定します `vserver create` コマンド（新しいSVMを作成する場合）。

フィールド	説明	あなたの価値
<code>-vserver</code>	新しい SVM の名前を指定します。完全修飾ドメイン名（FQDN）を指定するか、クラスタ内で一意の SVM 名を適用する別の命名規則に従います。	
<code>-aggregate</code>	新しいSMBストレージ容量に対応できる十分なスペースを持つクラスタ内のアグリゲートの名前を指定します。	
<code>-rootvolume</code>	SVM ルートボリュームの一意の名前を指定します。	
<code>-rootvolume-security-style</code>	SVMのNTFSセキュリティ形式を使用します。	<code>ntfs</code>

フィールド	説明	あなたの価値
-language	このワークフローではデフォルトの言語設定を使用します。	C.UTF-8
ipspace	オプション：IPspace は、SVM が配置される個別の IP アドレススペースです。	

• LIF 作成用のパラメータ \*

では、次の値を指定します `network interface create` コマンドを使用してLIFを作成します。

フィールド	説明	あなたの価値
-lif	新しい LIF の名前を指定します。	
-role	このワークフローではデータ LIF のロールを使用します。	data
-data-protocol	このワークフローではSMBプロトコルのみを使用します。	cifs
-home-node	でLIFが戻るノードを指定します <code>network interface revert</code> LIFに対してコマンドを実行します。	
-home-port	の場合にLIFが戻るポートまたはインターフェイスグループ <code>network interface revert</code> LIFに対してコマンドを実行します。	
-address	新しい LIF によるデータアクセスに使用されるクラスタ上の IPv4 または IPv6 アドレスを指定します。	
-netmask	LIF のネットワークマスクとゲートウェイを指定します。	
-subnet	IP アドレスのプール。の代わりに使用されます -address および -netmask アドレスとネットワークを自動的に割り当てます。	

フィールド	説明	あなたの価値
-firewall-policy	このワークフローではデフォルトのデータファイアウォールポリシーを使用します。	data
-auto-revert	オプション：起動時またはその他の状況下でデータ LIF がホームノードに自動的にリバートされるかどうかを指定します。デフォルト設定はです false。	

• DNS ホスト名解決のパラメータ \*

では、次の値を指定します `vserver services name-service dns create` コマンドを使用してDNSを設定します。

フィールド	説明	あなたの価値
-domains	最大 5 つの DNS ドメイン名。	
-name-servers	DNS ネームサーバごとに最大 3 つの IP アドレスを指定します。	

**Active Directory** ドメインで **SMB** サーバをセットアップする

• タイムサービス設定のパラメータ \*

では、次の値を指定します `cluster time-service ntp server create` コマンド（タイムサービスを設定する場合）。

フィールド	説明	あなたの価値
-server	Active Directory ドメイン用の NTP サーバのホスト名または IP アドレスを指定します。	

• Active Directory ドメイン内に SMB サーバを作成するためのパラメータ \*

では、次の値を指定します `vserver cifs create` コマンドは、新しいSMBサーバを作成し、ドメイン情報を指定するときに使用します。

フィールド	説明	あなたの価値
-vserver	SMB サーバを作成する SVM の名前を指定します。	

フィールド	説明	あなたの価値
-cifs-server	SMB サーバの名前（最大 15 文字）を指定します。	
-domain	SMB サーバに関連付ける Active Directory ドメインの完全修飾ドメイン名（FQDN）を指定します。	
-ou	オプション：SMB サーバに関連付ける Active Directory ドメイン内の組織単位を指定します。デフォルトでは、このパラメータは CN=Computers に設定されます。	
-netbios-aliases	オプション：NetBIOS エイリアスのリストを指定します。NetBIOS エイリアスは、SMB サーバ名の別名です。	
-comment	オプション：サーバのテキストコメントを指定します。Windows クライアントは、ネットワーク上のサーバを参照するとき、この SMB サーバ概要を確認できます。	

ワークグループに **SMB** サーバをセットアップする

- ワークグループで SMB サーバーを作成するためのパラメータ \*

では、次の値を指定します `vserver cifs create` コマンドは、新しいSMBサーバを作成し、サポートされるSMBバージョンを指定するときに使用します。

フィールド	説明	あなたの価値
-vserver	SMB サーバを作成する SVM の名前を指定します。	
-cifs-server	SMB サーバの名前（最大 15 文字）を指定します。	
-workgroup	ワークグループの名前（最大 15 文字）を指定します。	
-comment	オプション：サーバのテキストコメントを指定します。Windows クライアントは、ネットワーク上のサーバを参照するとき、この SMB サーバ概要を確認できます。	

• ローカルユーザー作成用のパラメータ \*

を使用してローカルユーザを作成する場合は、次の値を指定します `vserver cifs users-and-groups local-user create` コマンドを実行しますこれらの値は、ワークグループ内、およびオプションで AD ドメイン内の SMB サーバに必要です。

フィールド	説明	あなたの価値
<code>-vserver</code>	ローカルユーザを作成する SVM の名前を指定します。	
<code>-user-name</code>	ローカルユーザの名前（最大 20 文字）を指定します。	
<code>-full-name</code>	オプション：ユーザのフルネームを指定します。フルネームにスペースが含まれる場合は、フルネームを 2 重引用符で囲みます。	
<code>-description</code>	オプション：ローカルユーザの概要。概要にスペースが含まれる場合は、パラメータを引用符で囲みます。	
<code>-is-account-disabled</code>	オプション：ユーザアカウントが有効か無効かを指定します。このパラメータを指定しない場合、ユーザアカウントはデフォルトで有効になります。	

• ローカルグループを作成するためのパラメータ \*

を使用してローカルグループを作成する場合は、次の値を指定します `vserver cifs users-and-groups local-group create` コマンドを実行しますAD ドメインおよびワークグループ内の SMB サーバの場合はオプションです。

フィールド	説明	あなたの価値
<code>-vserver</code>	ローカルグループを作成する SVM の名前を指定します。	
<code>-group-name</code>	ローカルグループの名前（最大 256 文字）を指定します。	
<code>-description</code>	オプション：ローカルグループの概要。概要にスペースが含まれる場合は、パラメータを引用符で囲みます。	



## SMB対応SVMへのストレージ容量の追加

### • ボリュームを作成するためのパラメータ \*

では、次の値を指定します `volume create` コマンドは、`qtree`の代わりにボリュームを作成する場合に使用します。

フィールド	説明	あなたの価値
<code>-vserver</code>	新しいボリュームをホストする新規または既存の SVM の名前を指定します。	
<code>-volume</code>	新しいボリュームに対して、一意のわかりやすい名前を指定します。	
<code>-aggregate</code>	新しいSMBボリューム用の十分なスペースがあるクラスタ内のアグリゲートの名前を指定します。	
<code>-size</code>	新しいボリュームのサイズとして任意の整数を指定します。	
<code>-security-style</code>	このワークフローにはNTFSセキュリティ形式を使用します。	<code>ntfs</code>
<code>-junction-path</code>	新しいボリュームをマウントするルート（/）の下場所を指定します。	

### • `qtree` を作成するためのパラメータ \*

では、次の値を指定します `volume qtree create` コマンドは、ボリュームではなく`qtree`を作成する場合に使用します。

フィールド	説明	あなたの価値
<code>-vserver</code>	<code>qtree</code> を含むボリュームが配置されている SVM の名前。	
<code>-volume</code>	新しい <code>qtree</code> を格納するボリュームの名前を指定します。	
<code>-qtree</code>	新しい <code>qtree</code> に対して、一意のわかりやすい名前を 64 文字以内で指定します。	

フィールド	説明	あなたの価値
-qtree-path	qtreeパスの引数を指定します。形式はです /vol/volume_name/qtree_name\ > ボリュームとqtreeを別々の引数として指定する代わりに指定できます。	

• SMB 共有作成のパラメータ \*

では、次の値を指定します `vserver cifs share create` コマンドを実行します

フィールド	説明	あなたの価値
-vserver	SMB 共有を作成する SVM の名前を指定します。	
-share-name	作成する SMB 共有の名前（最大 256 文字）を指定します。	
-path	SMB 共有へのパスの名前（最大 256 文字）を指定します。このパスは、共有を作成する前にボリューム内に存在している必要があります。	
-share-properties	オプション：共有プロパティのリストを指定します。デフォルト設定はです <code>oplocks</code> 、 <code>browsable</code> 、 <code>changenotify</code> および <code>show-previous-versions</code> 。	
-comment	オプション：サーバのテキストコメント（最大 256 文字）を指定します。Windows クライアントは、ネットワーク上で参照するとき、この SMB 共有概要を確認できます。	

• SMB 共有アクセス制御リスト（ACL）を作成するためのパラメータ \*

では、次の値を指定します `vserver cifs share access-control create` コマンドを実行します

フィールド	説明	あなたの価値
-vserver	SMB ACL を作成する SVM の名前を指定します。	

フィールド	説明	あなたの価値
-share	作成先の SMB 共有の名前を指定します。	
-user-group-type	共有の ACL に追加するユーザまたはグループのタイプを指定します。デフォルトのタイプは windows	windows
-user-or-group	共有の ACL に追加するユーザまたはグループを指定します。ユーザ名を指定する場合は、「ドメイン名」の形式でユーザのドメインを含める必要があります。	
-permission	ユーザまたはグループの権限を指定します。	`[ No_access
Read	Change	Full_Control ]`

## SVMへのSMBアクセスの設定

### SVMへのSMBアクセスの設定

SMB クライアントアクセス用に SVM を設定していない場合は、新しい SVM を作成して設定するか、既存の SVM を設定する必要があります。SMB を設定する場合は、SVM ルートボリュームへのアクセスを許可し、SMB サーバを作成し、LIF を作成し、ホスト名解決を有効にし、ネームサービスを設定し、必要に応じて Kerberos セキュリティの有効化。

**SVM** を作成します。

SMBクライアントにデータアクセスを提供するSVMがクラスタ内に1つもない場合は、SVMを作成する必要があります。

作業を開始する前に

- ONTAP 9.13.1以降では、Storage VMに最大容量を設定できます。また、SVMの容量レベルがしきい値に近づいたときにアラートを設定することもできます。詳細については、[を参照してください SVM容量の管理](#)。

手順

1. SVM を作成します。
 

```
vserver create -vserver svm_name -rootvolume root_volume_name
-aggregate aggregate_name -rootvolume-security-style ntfs -language C.UTF-8
-ipospace ipospace_name
```

  - のNTFS設定を使用します。-rootvolume-security-style オプション
  - デフォルトのC.UTF-8を使用します -language オプション

。 ipspace 設定はオプションです。

2. 新しく作成した SVM の設定とステータスを確認します。 `vserver show -vserver vserver_name`

。 Allowed Protocols フィールドにはCIFSを含める必要があります。このリストはあとで編集できます。

。 Vserver Operational State フィールドにはを表示する必要があります running 状態。が表示された場合 initializing 状態にすると、ルートボリュームの作成などの中間処理が失敗したため、SVM を削除して再作成する必要があります。

#### 例

次のコマンドは、データアクセス用のSVMをIPspace内に作成します ipspaceA：

```
cluster1::> vserver create -vserver vs1.example.com -rootvolume root_vs1
-aggregate aggr1
-rootvolume-security-style ntfs -language C.UTF-8 -ipspace ipspaceA
```

```
[Job 2059] Job succeeded:
Vserver creation completed
```

次のコマンドは、1GBのルートボリュームでSVMが作成され、自動的に起動されて追加されたことを示しています running 状態。ルートボリュームには、ルールを含まないデフォルトのエクスポートポリシーがあるため、ルートボリュームは作成時にエクスポートされません。

```
cluster1::> vserver show -vserver vs1.example.com
Vserver: vs1.example.com
Vserver Type: data
Vserver Subtype: default
Vserver UUID: b8375669-19b0-11e5-b9d1-00a0983d9736
Root Volume: root_vs1
Aggregate: aggr1
NIS Domain: -
Root Volume Security Style: ntfs
LDAP Client: -
Default Volume Language Code: C.UTF-8
Snapshot Policy: default
Comment:
Quota Policy: default
List of Aggregates Assigned: -
Limit on Maximum Number of Volumes allowed: unlimited
Vserver Admin State: running
Vserver Operational State: running
Vserver Operational State Stopped Reason: -
Allowed Protocols: nfs, cifs, fcp, iscsi, ndmp
Disallowed Protocols: -
QoS Policy Group: -
Config Lock: false
IPspace Name: ipspaceA
```



ONTAP 9.13.1以降では、アダプティブQoSポリシーグループテンプレートを設定して、SVM内のボリュームにスループットの下限と上限の制限を適用できます。このポリシーはSVMの作成後にのみ適用できます。このプロセスの詳細については、[を参照してください アダプティブポリシーグループテンプレートを設定します](#)。

**SVMでSMBプロトコルが有効になっていることを確認する**

SVMでSMBを設定して使用する前に、プロトコルが有効になっていることを確認する必要があります。

このタスクについて

この作業は通常、SVMのセットアップ時に実行します。ただし、セットアップ時にプロトコルを有効にしなかった場合でも、を使用してあとから有効にすることができます `vserver add-protocols` コマンドを実行します



作成したプロトコルは、LIF から追加または削除することはできません。

を使用して、SVMのプロトコルを無効にすることもできます `vserver remove-protocols` コマンドを実行します

## 手順

1. 現在 SVM で有効になっているプロトコルと無効になっているプロトコルを確認します。 `vserver show -vserver vserver_name -protocols`

を使用することもできます `vserver show-protocols` コマンドを使用して、クラスタ内のすべてのSVMで現在有効になっているプロトコルを表示します。

2. 必要に応じて、プロトコルを有効または無効にします。

- SMBプロトコルを有効にする手順は次のとおりです。 `vserver add-protocols -vserver vserver_name -protocols cifs`
- プロトコルを無効にするには： `vserver remove-protocols -vserver vserver_name -protocols protocol_name[,protocol_name,...]`

3. 有効 / 無効なプロトコルが正しく更新されたことを確認します。 `vserver show -vserver vserver_name -protocols`

## 例

次のコマンドは、 `vs1` という SVM で現在有効 / 無効（許可 / 不許可）になっているプロトコルを表示します。

```
vs1::> vserver show -vserver vs1.example.com -protocols
Vserver           Allowed Protocols           Disallowed Protocols
-----
vs1.example.com   cifs                         nfs, fcp, iscsi, ndmp
```

次のコマンドは、を追加してSMB経由のアクセスを許可します `cifs vs1` というSVMで有効になっているプロトコルのリストに移動します。

```
vs1::> vserver add-protocols -vserver vs1.example.com -protocols cifs
```

## SVM ルートボリュームのエクスポートポリシーを開きます

SVMルートボリュームのデフォルトのエクスポートポリシーには、すべてのクライアントにSMB経由のアクセスを許可するルールが含まれている必要があります。このようなルールを追加しないと、SVMとそのボリュームに対するSMBクライアントのアクセスがすべて拒否されます。

### このタスクについて

新しい SVM が作成されると、デフォルトのエクスポートポリシー（default）が、SVM のルートボリュームに対して自動的に作成されます。SVM 上のデータにクライアントからアクセスできるようにするには、デフォルトのエクスポートポリシーのルールを 1 つ以上作成する必要があります。

デフォルトのエクスポートポリシーですべての SMB アクセスが許可されていることを確認してから、ボリュームまたは `qtree` ごとにカスタムのエクスポートポリシーを作成して各ボリュームへのアクセスを制限します。

## 手順

1. 既存の SVM を使用している場合は、デフォルトのルートボリュームエクスポートポリシーを確認します。 `vserver export-policy rule show`

次のようなコマンド出力が表示されます。

```
cluster::> vserver export-policy rule show -vserver vs1.example.com
-policyname default -instance

Vserver: vs1.example.com
Policy Name: default
Rule Index: 1
Access Protocol: cifs
Client Match Hostname, IP Address, Netgroup, or Domain: 0.0.0.0/0
RO Access Rule: any
RW Access Rule: any
User ID To Which Anonymous Users Are Mapped: 65534
Superuser Security Types: any
Honor SetUID Bits in SETATTR: true
Allow Creation of Devices: true
```

オープンアクセスを許可するこのようなルールが存在する場合、このタスクは完了です。表示されない場合は、次の手順に進みます。

2. SVM ルートボリュームのエクスポートルールを作成します。 `vserver export-policy rule create -vserver vserver_name -policyname default -ruleindex 1 -protocol cifs -clientmatch 0.0.0.0/0 -rorule any -rwrule any -superuser any`
3. を使用してルールの作成を確認します `vserver export-policy rule show` コマンドを実行します

## 結果

これで、SVM で作成されたすべてのボリュームまたは qtrees に SMB クライアントからアクセスできるようになります。

## LIF を作成

LIF は、物理ポートまたは論理ポートに関連付けられた IP アドレスです。コンポーネントに障害が発生しても、LIF は別の物理ポートにフェイルオーバーまたは移行できるため、引き続きネットワークと通信できます。

### 作業を開始する前に

- 基盤となる物理または論理ネットワークポートが管理用に設定されている必要があります up ステータス。
- サブネット名を使用して LIF の IP アドレスとネットワークマスク値を割り当てる場合は、そのサブネットがすでに存在している必要があります。

サブネットには、同じレイヤ 3 サブネットに属する IP アドレスのプールが含まれています。これらはを使用して作成されます `network subnet create` コマンドを実行します

- LIF で処理するトラフィックのタイプを指定するメカニズムが変更されました。ONTAP 9.5 以前では、LIF はロールを使用して処理するトラフィックのタイプを指定していました。ONTAP 9.6 以降では、サービスポリシーを使用して、処理するトラフィックのタイプを指定します。

このタスクについて

- 同じネットワークポート上に IPv4 と IPv6 の両方の LIF を作成できます。
- クラスタ内のLIFの数が多い場合は、を使用して、クラスタでサポートされるLIFの容量を確認できます `network interface capacity show` コマンドとを使用して、各ノードでサポートされるLIFの容量を確認します `network interface capacity details show` コマンド（advanced権限レベル）。
- ONTAP 9.7 以降では、同じサブネット内に SVM 用の他の LIF がすでに存在する場合、LIF のホームポートを指定する必要はありません。ONTAP は、同じサブネットにすでに設定されている他の LIF と同じブロードキャストドメインにある指定したホームノード上のランダムなポートを自動的に選択します。

手順

#### 1. LIF を作成します。

```
network interface create -vserver vservice_name -lif lif_name -role data -data-protocol cifs -home-node node_name -home-port port_name {-address IP_address -netmask IP_address | -subnet-name subnet_name} -firewall-policy data -auto-revert {true|false}
```

\* ONTAP 9.5 以前 \*

```
`network interface create -vserver vservice_name -lif lif_name -role data -data-protocol cifs -home-node node_name -home-port port_name {-address IP_address -netmask IP_address -subnet-name subnet_name} -firewall-policy data -auto-revert {true false}`
```

\* ONTAP 9.6 以降 \*

```
`network interface create -vserver vservice_name -lif lif_name -service-policy service_policy_name -home-node node_name -home-port port_name {-address IP_address -netmask IP_address -subnet-name subnet_name} -firewall-policy data -auto-revert {true false}`
```

- 。 `-role` サービスポリシーを使用してLIFを作成する場合はパラメータは必要ありません（ONTAP 9.6以降）。
- 。 `-data-protocol` サービスポリシーを使用してLIFを作成する場合はパラメータは必要ありません（ONTAP 9.6以降）。ONTAP 9.5以前を使用している場合 `-data-protocol` パラメータはLIFの作成時に指定する必要があります。あとで変更するには、データLIFを削除して再作成する必要があります。
- `-home-node` は、の実行時にLIFが戻るノードです `network interface revert LIF` に対してコマンドを実行します。

を使用して、LIFをホームノードおよびホームポートに自動的にリポートするかどうかを指定することもできます `-auto-revert` オプション



- `-home-port` は、の実行時にLIFが戻る物理ポートまたは論理ポートです `network interface revert` LIFに対してコマンドを実行します。
- でIPアドレスを指定できます `-address` および `-netmask` オプションを選択するか、を使用してサブネットからの割り当てを有効にします `-subnet_name` オプション
- サブネットを使用して IP アドレスとネットワークマスクを指定した場合、サブネットにゲートウェイが定義されていると、そのサブネットを使用して LIF を作成するときにゲートウェイへのデフォルトルートが SVM に自動的に追加されます。
- サブネットを使用せずに手動で IP アドレスを割り当てると、クライアントまたはドメインコントローラが別の IP サブネットにある場合にゲートウェイへのデフォルトルートの設定が必要になることがあります。。 `network route create` のマニュアルページには、SVM内での静的ルートの作成に関する情報が記載されています。
- をクリックします `-firewall-policy` オプションで、同じデフォルトを使用します `data` をLIFのロールとして使用します。

必要に応じて、カスタムファイアウォールポリシーをあとから作成して追加できます。



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

- `-auto-revert` 起動時、管理データベースのステータスが変化したとき、ネットワーク接続が確立されたときなどの状況で、データLIFがホームノードに自動的にリバートされるかどうかを指定できます。デフォルト設定は `false` に設定することもできます `false` 環境内のネットワーク管理ポリシーによって異なります。

## 2. LIF が正常に作成されたことを確認します。

```
network interface show
```

## 3. 設定した IP アドレスに到達できることを確認します。

対象	使用
IPv4 アドレス	<code>network ping</code>
IPv6アドレス	<code>network ping6</code>

### 例

次のコマンドでは、を使用してLIFを作成し、IPアドレスとネットワークマスク値を指定します `-address` および `-netmask` パラメータ：

```
network interface create -vserver vs1.example.com -lif datalif1 -role data
-data-protocol cifs -home-node node-4 -home-port elc -address 192.0.2.145
-netmask 255.255.255.0 -firewall-policy data -auto-revert true
```

次のコマンドは、LIF を作成し、IP アドレスとネットワークマスク値を指定したサブネット（`client1_sub`

) から割り当てています。

```
network interface create -vserver vs3.example.com -lif datalif3 -role data
-data-protocol cifs -home-node node-3 -home-port elc -subnet-name
client1_sub -firewall-policy data -auto-revert true
```

次のコマンドは、cluster-1 内のすべての LIF を表示します。datalif1 および datalif3 というデータ LIF には IPv4 アドレスを設定しています。一方、datalif4 には IPv6 アドレスを設定しています。

```
network interface show
```

Vserver	Logical Interface	Status Admin/Oper	Network Address/Mask	Current Node	Current Is Port
Home					
-----	-----	-----	-----	-----	-----
----					
cluster-1					
	cluster_mgmt	up/up	192.0.2.3/24	node-1	e1a
true					
node-1					
	clus1	up/up	192.0.2.12/24	node-1	e0a
true					
	clus2	up/up	192.0.2.13/24	node-1	e0b
true					
	mgmt1	up/up	192.0.2.68/24	node-1	e1a
true					
node-2					
	clus1	up/up	192.0.2.14/24	node-2	e0a
true					
	clus2	up/up	192.0.2.15/24	node-2	e0b
true					
	mgmt1	up/up	192.0.2.69/24	node-2	e1a
true					
vs1.example.com					
	datalif1	up/down	192.0.2.145/30	node-1	e1c
true					
vs3.example.com					
	datalif3	up/up	192.0.2.146/30	node-2	e0c
true					
	datalif4	up/up	2001::2/64	node-2	e0c
true					
5 entries were displayed.					

次のコマンドは、に割り当てられたNASデータLIFを作成する方法を示しています default-data-files サービスポリシー：

```
network interface create -vserver vs1 -lif lif2 -home-node node2 -homeport
e0d -service-policy default-data-files -subnet-name ipspace1
```

ホスト名解決に使用する **DNS** を有効にします

を使用できます `vserver services name-service dns` コマンドを使用してSVMでDNSを有効にし、ホスト名解決にDNSを使用するように設定します。ホスト名は外部DNS サーバを使用して解決されます。

作業を開始する前に

ホスト名を検索するために、サイト規模の DNS サーバが使用可能である必要があります。

単一点障害を回避するには、複数の DNS サーバを設定する必要があります。。 `vserver services name-service dns create` 入力したDNSサーバ名が1つだけの場合は警告が表示されます。

このタスクについて

SVM での動的 DNS の設定については、『ネットワーク管理ガイド』を参照してください。

手順

1. SVM で DNS を有効にします。 `vserver services name-service dns create -vserver vs1 -domains example.com -name-servers 192.0.2.201,192.0.2.202 -state enabled`

次のコマンドは、SVM vs1 で外部 DNS サーバを有効にします。

```
vserver services name-service dns create -vserver vs1.example.com
-domains example.com -name-servers 192.0.2.201,192.0.2.202 -state
enabled
```



ONTAP 9.2以降では、 `vserver services name-service dns create` コマンドは設定の自動検証を実行し、ONTAP がネームサーバに接続できない場合はエラーメッセージを報告します。

2. を使用して、DNSドメイン設定を表示します `vserver services name-service dns show` コマンドを実行します

次のコマンドは、クラスタ内のすべての SVM の DNS 設定を表示します。

```
vserver services name-service dns show
```

Vserver	State	Domains	Name Servers
cluster1	enabled	example.com	192.0.2.201, 192.0.2.202
vs1.example.com	enabled	example.com	192.0.2.201, 192.0.2.202

次のコマンドは、SVM vs1 の DNS 設定の詳細を表示します。

```
vserver services name-service dns show -vserver vs1.example.com
Vserver: vs1.example.com
Domains: example.com
Name Servers: 192.0.2.201, 192.0.2.202
Enable/Disable DNS: enabled
Timeout (secs): 2
Maximum Attempts: 1
```

3. を使用してネームサーバのステータスを検証します `vserver services name-service dns check` コマンドを実行します

。 `vserver services name-service dns check` コマンドはONTAP 9.2以降で使用できます。

```
vserver services name-service dns check -vserver vs1.example.com
```

Vserver	Name Server	Status	Status Details
vs1.example.com	10.0.0.50	up	Response time (msec): 2
vs1.example.com	10.0.0.51	up	Response time (msec): 2

## Active Directory ドメイン内に SMB サーバをセットアップする

タイムサービスを設定

Active Directory ドメインコントローラで SMB サーバを作成する前に、クラスタ時間と SMB サーバが所属するドメインのドメインコントローラの時間のずれが 5 分以内であることを確認する必要があります。

このタスクについて

Active Directory ドメインと同じ NTP サーバを使用して時刻を同期するようにクラスタ NTP サービスを設定する必要があります。

ONTAP 9.5 以降では、対称認証を使用するように NTP サーバをセットアップできます。

手順

1. を使用してタイムサービスを設定します `cluster time-service ntp server create` コマンドを実行します
  - 対称認証を使用せずにタイムサービスを設定するには、次のコマンドを入力します。 `cluster time-service ntp server create -server server_ip_address`
  - 対称認証を使用してタイムサービスを設定するには、次のコマンドを入力します。 `cluster time-service ntp server create -server server_ip_address -key-id key_id`  
`cluster time-service ntp server create -server 10.10.10.1 cluster time-service ntp server create -server 10.10.10.2`
2. を使用して、タイムサービスが正しく設定されていることを確認します `cluster time-service ntp server show` コマンドを実行します

```
cluster time-service ntp server show
```

Server	Version
-----	-----
10.10.10.1	auto
10.10.10.2	auto

**NTP** サーバの対称認証を管理するコマンドです

ONTAP 9.5 以降では、ネットワークタイムプロトコル（NTP）バージョン 3 がサポートされます。NTPv3 には SHA-1 鍵を使用した対称認証機能が含まれ、ネットワークセキュリティが強化されます。

作業	使用するコマンド
対称認証を使用せずに NTP サーバを設定する	<code>cluster time-service ntp server create -server server_name</code>
対称認証を使用して NTP サーバを設定する	<code>cluster time-service ntp server create -server server_ip_address -key-id key_id</code>
既存の NTP サーバに対して対称認証を有効にする必要なキー ID を追加することで、既存の NTP サーバを変更して認証を有効にすることができます	<code>cluster time-service ntp server modify -server server_name -key-id key_id</code>

作業	使用するコマンド
共有 NTP キーを設定する	<pre>cluster time-service ntp key create -id shared_key_id -type shared_key_type -value shared_key_value</pre> <div>  <p>共有キーは ID で参照されます。ID、そのタイプ、および値が、ノードと NTP サーバで同じである必要があります</p> </div>
不明なキー ID で NTP サーバを設定する	<pre>cluster time-service ntp server create -server server_name -key-id key_id</pre>
NTP サーバで設定されていないキー ID でサーバを設定する。	<pre>cluster time-service ntp server create -server server_name -key-id key_id</pre> <div>  <p>キー ID、タイプ、および値が、NTP サーバで設定されたキー ID、タイプ、および値と同じである必要があります。</p> </div>
対称認証を無効にします	<pre>cluster time-service ntp server modify -server server_name -authentication disabled</pre>

**Active Directory** ドメイン内に **SMB** サーバを作成します

使用できます `vserver cifs create` コマンドを使用して SVM 上に SMB サーバを作成し、所属先の Active Directory (AD) ドメインを指定します。

作業を開始する前に

データ処理に使用している SVM および LIF が、SMB プロトコルを許可するように設定されている必要があります。LIF は、SVM 上で設定されている DNS サーバ、および SMB サーバの追加先ドメインの AD ドメインコントローラに接続する必要があります。

SMB サーバの追加先となる AD ドメイン内のマシンアカウントの作成を許可されているユーザなら誰でも、SVM 上に SMB サーバを作成できます。これには、他のドメインのユーザを含めることができます。

ONTAP 9.7 以降では、権限がある Windows アカウントの名前とパスワードの代わりに、keytab ファイルの URI を AD 管理者から提供される場合があります。URI を受け取ったら、に含めます `-keytab-uri` パラメータと `vserver cifs` コマンド

このタスクについて

Active Directory ドメインで SMB サーバを作成する場合の条件は次のとおりです。

- ドメインを指定するときは Fully Qualified Domain Name (FQDN ; 完全修飾ドメイン名) を使用する必要があります。

- デフォルト設定では、SMB サーバマシンアカウントは Active Directory CN=Computer オブジェクトに追加されます。
- を使用して、SMBサーバを別の組織単位（OU）に追加することもできます `-ou` オプション
- 必要に応じて、SMB サーバの 1 つ以上の NetBIOS エイリアス（最大 200 個）をカンマで区切って追加できます。

SMB サーバの NetBIOS エイリアスを設定すると、他のファイルサーバのデータを SMB サーバに統合して、SMB サーバが元のファイルサーバの名前に応答するようにする場合に役立ちます。

。 `vserver cifs` マニュアルページには、追加のオプションパラメータと命名要件が記載されています。



ONTAP 9.1 以降では、SMB バージョン 2.0 からドメインコントローラ（DC）への接続を有効にすることができます。これは、ドメインコントローラで SMB 1.0 を無効にしている場合は必須です。ONTAP 9.2 以降では、SMB 2.0 がデフォルトで有効になります。

ONTAP 9.8 以降では、ドメインコントローラへの接続を暗号化するように指定できます。ONTAP では、ドメインコントローラの通信に暗号化が必要です `-encryption-required-for-dc-connection` オプションはに設定されています `true`; デフォルトは `false`。このオプションを設定すると、SMB3 でのみ暗号化がサポートされるため、SMB3 プロトコルのみが使用されます。。

**"SMBの管理"** SMB サーバ設定オプションの詳細については、を参照してください。

#### 手順

1. クラスタでSMBのライセンスが有効になっていることを確認します。 `system license show -package cifs`

SMBライセンスはに含まれています。 **"ONTAP One"**。ONTAP Oneをお持ちでなく、ライセンスがインストールされていない場合は、営業担当者にお問い合わせください。

SMB サーバを認証のみに使用する場合は、CIFS ライセンスは必要ありません。

2. ADドメインにSMBサーバを作成します。 `vserver cifs create -vserver vserver_name -cifs -server smb_server_name -domain FQDN [-ou organizational_unit] [-netbios-aliases NetBIOS_name, ...] [-keytab-uri {(ftp|http)://hostname|IP_address}] [-comment text]`

ドメインに参加する場合、このコマンドの実行には数分かかることがあります。

次のコマンドは、ドメイン「`example.com`」に SMB サーバ「`'smb_server01'`」を作成します

```
cluster1::> vserver cifs create -vserver vs1.example.com -cifs-server
smb_server01 -domain example.com
```

次のコマンドは、ドメイン「`mydomain.com`」に SMB サーバ「`'smb_server02'`」を作成し、keytab ファイルを使用して ONTAP 管理者を認証します。

```
cluster1::> vsserver cifs create -vsserver vs1.mydomain.com -cifs-server
smb_server02 -domain mydomain.com -keytab-uri
http://admin.mydomain.com/ontap1.keytab
```

3. を使用してSMBサーバの設定を確認します vsserver cifs show コマンドを実行します

この例では、「sMB\_SERVER01」という名前の SMB サーバが SVM vs1.example.com 上に作成され、「example.com」ドメイン」に追加されたことがコマンド出力に示されています。

```
cluster1::> vsserver cifs show -vsserver vs1

Vserver: vs1.example.com
CIFS Server NetBIOS Name: SMB_SERVER01
NetBIOS Domain/Workgroup Name: EXAMPLE
Fully Qualified Domain Name: EXAMPLE.COM
Default Site Used by LIFs Without Site Membership:
Authentication Style: domain
CIFS Server Administrative Status: up
CIFS Server Description: -
List of NetBIOS Aliases: -
```

4. 必要に応じて、ドメインコントローラとの暗号化通信を有効にします (ONTAP 9.8以降)。vsserver cifs security modify -vsserver svm\_name -encryption-required-for-dc-connection true

例

次のコマンドは、SVM vs2.example.com の「example.com」ドメインに「MB\_Server02」という名前の SMB サーバを作成します。マシン・アカウントは「OU=eng、OU=corp、DC=example、DC=com」コンテナに作成されますSMB サーバには NetBIOS エイリアスが割り当てられます。

```
cluster1::> vsserver cifs create -vsserver vs2.example.com -cifs-server
smb_server02 -domain example.com -ou OU=eng,OU=corp -netbios-aliases
old_cifs_server01

cluster1::> vsserver cifs show -vsserver vs1

Vserver: vs2.example.com
CIFS Server NetBIOS Name: SMB_SERVER02
NetBIOS Domain/Workgroup Name: EXAMPLE
Fully Qualified Domain Name: EXAMPLE.COM
Default Site Used by LIFs Without Site Membership:
Authentication Style: domain
CIFS Server Administrative Status: up
CIFS Server Description: -
List of NetBIOS Aliases: OLD_CIFS_SERVER01
```



次のコマンドは、別のドメインのユーザ（ここでは信頼できるドメインの管理者）が、SVM vs3.example.com 上に「smb\_server03」という名前の SMB サーバを作成できるようにします。。  
-domain オプションは、SMBサーバを作成するホームドメイン（DNSの設定で指定）の名前を指定します。。  
username オプションは、信頼できるドメインの管理者を指定します。

- ホームドメイン： example.com
- 信頼できるドメイン： trust.lab.com
- 信頼できるドメインのユーザ名： Administrator1

```
cluster1::> vsserver cifs create -vsriver vs3.example.com -cifs-server  
smb_server03 -domain example.com
```

```
Username: Administrator1@trust.lab.com  
Password: . . .
```

**SMB 認証用の keytab ファイルを作成します**

ONTAP 9.7 以降 ONTAP では、keytab ファイルを使用した Active Directory（AD）サーバとの SVM 認証がサポートされます。AD管理者はkeytabファイルを生成し、Uniform Resource Identifier（URI;ユニフォームリソース識別子）としてONTAP 管理者が使用できるようにします。このファイルは、に指定します vsriver cifs コマンドを実行するには、ADドメインとのKerberos認証が必要です。

AD管理者は、標準のWindows Serverを使用してkeytabファイルを作成できます ktpass コマンドを実行しますこのコマンドは、認証が必要なプライマリドメインで実行する必要があります。。 ktpass コマンドを使用してkeytabファイルを生成できるのはプライマリドメインユーザのみです。信頼できるドメインユーザを使用して生成されたキーはサポートされていません。

keytab ファイルは、特定の ONTAP 管理者ユーザ用に生成されます。管理者ユーザのパスワードが変更されないかぎり、特定の暗号化タイプとドメインに対して生成されたキーは変更されません。したがって、管理者ユーザのパスワードを変更した場合は、そのたびに新しい keytab ファイルが必要になります。

次の暗号化タイプがサポートされています。

- AES256-SHA1
- des-cbc-md5



ONTAP では、DES-CBC-CRC 暗号化タイプはサポートされていません。

- RC4-HMAC

最も高度な暗号化タイプはAES256 です。ONTAP システムで有効な場合はAES256 を使用してください。

keytab ファイルは、管理パスワードを指定して生成するか、ランダムに生成されたパスワードを使用して生成できます。ただし、keytab ファイル内のキーを復号化するために AD サーバ側で管理者ユーザに固有な秘密鍵が必要になるため、ある時点で使用できるパスワードオプションはどちらか 1 つだけです。特定の管理者の秘密鍵を変更すると、keytab ファイルは無効になります。

ワークグループ内に **SMB** サーバをセットアップする

ワークグループの概要で **SMB** サーバをセットアップする

ワークグループ内のメンバーとして SMB サーバをセットアップするには、SMB サーバを作成してから、ローカルユーザとローカルグループを作成します。

Microsoft Active Directory ドメインインフラを使用できない場合は、ワークグループに SMB サーバを設定できます。

ワークグループモードの SMB サーバでは NTLM 認証のみがサポートされ、Kerberos 認証はサポートされません。

ワークグループ内に **SMB** サーバを作成

を使用できます `vserver cifs create` コマンドを使用してSVM上にSMBサーバを作成し、所属先のワークグループを指定します。

作業を開始する前に

データ処理に使用している SVM および LIF が、SMB プロトコルを許可するように設定されている必要があります。LIF は、SVM で設定されている DNS サーバに接続する必要があります。

このタスクについて

ワークグループモードの SMB サーバでは、次の SMB 機能はサポートされません。

- SMB3 監視プロトコル
- SMB3 CA 共有
- SQL over SMB
- フォルダリダイレクト
- 移動プロファイル
- グループポリシーオブジェクト（GPO）
- ボリューム Snapshot サービス（VSS）

。 `vserver cifs` その他のオプションの設定パラメータと命名要件については、マニュアルページを参照してください。

手順

1. クラスタでSMBのライセンスが有効になっていることを確認します。 `system license show -package cifs`

SMBライセンスには含まれています。 **"ONTAP One"**。ONTAP Oneをお持ちでなく、ライセンスがインストールされていない場合は、営業担当者にお問い合わせください。

SMB サーバを認証のみに使用する場合は、CIFS ライセンスは必要ありません。

2. ワークグループ内にSMBサーバを作成します。 `vserver cifs create -vserver vserver_name -cifs-server cifs_server_name -workgroup workgroup_name [-comment text]`

次のコマンドは 'ワークグループ "workgroup01" 内に SMB サーバ "smb\_server01" を作成します

```
cluster1::> vservers cifs create -vservers vs1.example.com -cifs-server
SMB_SERVER01 -workgroup workgroup01
```

3. を使用してSMBサーバの設定を確認します vservers cifs show コマンドを実行します

次の例では、コマンド出力は、ワークグループ「workgroup01」内の SVM vs1.example.com 上に「smb\_server01」という名前の SMB サーバが作成されたことを示しています。

```
cluster1::> vservers cifs show -vservers vs0

Vserver: vs1.example.com
CIFS Server NetBIOS Name: SMB_SERVER01
NetBIOS Domain/Workgroup Name: workgroup01
Fully Qualified Domain Name: -
Organizational Unit: -
Default Site Used by LIFs Without Site Membership: -
Workgroup Name: workgroup01
Authentication Style: workgroup
CIFS Server Administrative Status: up
CIFS Server Description:
List of NetBIOS Aliases: -
```

完了後

ワークグループ内の CIFS サーバについては、SVM 上でローカルユーザ、およびオプションでローカルグループを作成する必要があります。

関連情報

["SMBの管理"](#)

ローカルユーザアカウントを作成します

SVM に格納されたデータへの SMB 接続によるアクセスの許可に使用できるローカルユーザアカウントを作成できます。ローカルユーザアカウントは、SMB セッションを作成する際の認証にも使用できます。

このタスクについて

ローカルユーザの機能は、SVM の作成時にデフォルトで有効になります。

ローカルユーザアカウントを作成するときは、ユーザ名を指定する必要があり、アカウントを関連付ける SVM を指定する必要があります。

。vservers cifs users-and-groups local-user マニュアルページには、オプションのパラメータと命名要件の詳細が記載されています。

## 手順

1. ローカルユーザを作成します。 `vserver cifs users-and-groups local-user create -vserver vserver_name -user-name user_name optional_parameters`

次のオプションのパラメータが役に立つ場合があります。

- `-full-name`

ユーザのフルネーム。

- `-description`

ローカルユーザの概要。

- `-is-account-disabled {true|false}`

ユーザアカウントが有効になっているか無効になっているかを示します。このパラメータを指定しない場合、ユーザアカウントはデフォルトで有効になります。

ローカルユーザのパスワードを入力するように求められます。

2. ローカルユーザのパスワードを入力し、確認のためにもう一度入力します。
3. ユーザが正常に作成されたことを確認します。 `vserver cifs users-and-groups local-user show -vserver vserver_name`

## 例

次の例では、SVM `vs1.example.com` に関連付けられた「`SMB_SERVER1\Sue`」という完全な名前のローカルユーザ「`Sue Chang`」を作成します。

```
cluster1::> vserver cifs users-and-groups local-user create -vserver
vs1.example.com -user-name SMB_SERVER01\sue -full-name "Sue Chang"

Enter the password:
Confirm the password:

cluster1::> vserver cifs users-and-groups local-user show
Vserver  User Name                      Full Name  Description
-----
vs1      SMB_SERVER01\Administrator          Built-in administrator
account
vs1      SMB_SERVER01\sue                   Sue Chang
```

ローカルグループを作成します

SVM に関連付けられたデータへの SMB 接続によるアクセスの許可に使用できるローカルグループを作成できます。また、グループのメンバーに付与するユーザ権限と機能を定義した権限を割り当てることもできます。

このタスクについて

ローカルグループの機能は、SVM の作成時にデフォルトで有効になります。

ローカルグループを作成するときは、グループの名前を指定する必要があり、グループに関連付ける SVM を指定する必要があります。グループ名を指定する際、ローカルドメイン名は指定してもしなくても構いません。また、オプションで、ローカルグループの概要を指定することもできます。別のローカルグループにローカルグループを追加することはできません。

。 `vserver cifs users-and-groups local-group` マニュアルページには、オプションのパラメータと命名要件の詳細が記載されています。

#### 手順

1. ローカルグループを作成します。 `vserver cifs users-and-groups local-group create`  
`-vserver vserver_name -group-name group_name`

次のオプションのパラメータが役に立つ場合があります。

- `-description`

ローカルグループの概要。

2. グループが正常に作成されたことを確認します。 `vserver cifs users-and-groups local-group show -vserver vserver_name`

#### 例

次の例では、SVM `vs1` に関連付けられるローカルグループ「`s MB_SERVER01\engineering`」を作成します。

```
cluster1::> vserver cifs users-and-groups local-group create -vserver
vs1.example.com -group-name SMB_SERVER01\engineering
```

```
cluster1::> vserver cifs users-and-groups local-group show -vserver
vs1.example.com
```

Vserver	Group Name	Description
vs1.example.com	BUILTIN\Administrators	Built-in Administrators
vs1.example.com	BUILTIN\Backup Operators	Backup Operators group
vs1.example.com	BUILTIN\Power Users	Restricted administrative privileges
vs1.example.com	BUILTIN\Users	All users
vs1.example.com	SMB_SERVER01\engineering	
vs1.example.com	SMB_SERVER01\sales	

#### 完了後

新しいグループにメンバーを追加する必要があります。

ローカルグループメンバーシップの管理では、ローカルユーザやドメインユーザの追加と削除、ドメイングループの追加と削除ができます。この機能は、特定のグループに対するアクセス制御に基づいてデータへのアクセスを制御したり、グループに関連した権限をユーザに付与したりする上で役に立ちます。

#### このタスクについて

特定のグループのメンバーシップに基づいてローカルユーザ、ドメインユーザ、またはドメイングループに付与されたアクセス権や権限を取り消す場合に、メンバーをグループから削除できます。

メンバーをローカルグループに追加する場合は、次の点に注意する必要があります。

- 特殊なグループ `_Everyone` にユーザを追加することはできません。
- 別のローカルグループにローカルグループを追加することはできません。
- ローカルグループにドメインユーザまたはグループを追加するには、ONTAP で名前を SID に解決できる必要があります。

メンバーをローカルグループから削除する場合は、次の点に注意する必要があります。

- 特殊なグループ `_Everyone` からメンバーを削除することはできません。
- ローカルグループからメンバーを削除するには、ONTAP で名前を SID に解決できる必要があります。

#### 手順

##### 1. メンバーをグループに追加するか、グループから削除します。

- メンバーを追加します。 `vserver cifs users-and-groups local-group add-members -vserver vserver_name -group-name group_name -member-names name[,...]`

カンマ区切りのリストに記載されたローカルユーザ、ドメインユーザ、ドメイングループを指定し、特定のローカルグループに追加します。

- メンバーを削除します。 `vserver cifs users-and-groups local-group remove-members -vserver vserver_name -group-name group_name -member-names name[,...]`

カンマ区切りのリストに記載されたローカルユーザ、ドメインユーザ、ドメイングループを指定し、特定のローカルグループから削除します。

#### 例

次の例では、SVM `vs1.example.com` 上のローカルグループ「`s MB_SERVER01\engineering`」にローカルユーザ「`""s MB_SERVER01\engineering`」を追加します。

```
cluster1::> vserver cifs users-and-groups local-group add-members -vserver
vs1.example.com -group-name SMB_SERVER01\engineering -member-names
SMB_SERVER01\sue
```

次の例では、SVM `vs1.example.com` 上のローカルグループ「`s MB_SERVER1\engineering`」からローカルユーザ「`s MB_SERVER01\Sue`」および「`s MB_SERVER01\engineering`」を削除します。

```
cluster1::> vsriver cifs users-and-groups local-group remove-members  
-vsriver vs1.example.com -group-name SMB_SERVER\engineering -member-names  
SMB_SERVER\sue,SMB_SERVER\james
```

有効な **SMB** のバージョンを確認

ONTAP 9 のリリースによって、クライアントおよびドメインコントローラとの接続に対してデフォルトで有効になっている SMB のバージョンが決まります。ご使用の環境で必要なクライアントと機能を、SMB サーバがサポートしていることを確認する必要があります。

このタスクについて

クライアントとドメインコントローラの両方と接続するために、可能な限り SMB 2.0 以降を有効にする必要があります。セキュリティ上の理由から、SMB 1.0 の使用は避け、お使いの環境で不要であることを確認した場合は無効にする必要があります。

ONTAP 9 では、SMB バージョン 2.0 以降がクライアント接続用にデフォルトで有効になっていますが、デフォルトで有効になっている SMB 1.0 のバージョンは ONTAP リリースによって異なります。

- ONTAP 9.1 P8 以降では、SVM で SMB 1.0 を無効にすることができます。
  - 。 -smb1-enabled オプションをに設定します vsriver cifs options modify コマンドは、SMB 1.0 を有効または無効にします。
- ONTAP 9.3 以降では、新しい SVM でデフォルトで無効になっています。

SMB サーバが Active Directory (AD) ドメイン内にある場合、ONTAP 9.1 以降では、ドメインコントローラ (DC) に接続するために SMB 2.0 を有効にすることができます。DC 上で SMB 1.0 を無効にしている場合は、この処理は必須です。ONTAP 9.2 以降では、SMB 2.0 が DC 接続用にデフォルトで有効になります。



状況 -smb1-enabled-for-dc-connections がに設定されます false 間 -smb1-enabled がに設定されます true`ONTAP では、クライアントとしての SMB 1.0 の接続は拒否されますが、サーバとしての SMB 1.0 のインバウンド接続は引き続き受け入れます。

"[SMBの管理](#)" サポートされる SMB のバージョンと機能に関する詳細が記載されています。

手順

1. 権限レベルを advanced に設定します。

```
set -privilege advanced
```

2. 有効になっている SMB のバージョンを確認します。

```
vsriver cifs options show
```

リストを下にスクロールすると、クライアント接続用に有効になっている SMB のバージョンを表示できます。また、AD ドメイン内の SMB サーバを設定している場合は、AD ドメイン接続用に有効になっているバージョンを表示できます。

3. 必要に応じて、クライアント接続用の SMB プロトコルを有効または無効にします。

- SMBバージョンを有効にするには：

```
vserver cifs options modify -vserver vserver_name smb_version true
```

- SMBバージョンを無効にするには：

```
vserver cifs options modify -vserver vserver_name smb_version false
```

に指定できる値 smb\_version：

- -smb1-enabled
- -smb2-enabled
- -smb3-enabled
- -smb31-enabled

次のコマンドは、SVM vs1.example.comでSMB 3.1を有効にします。

```
cluster1::*> vserver cifs options modify -vserver vs1.example.com -smb31-enabled true
```

1. SMB サーバが Active Directory ドメイン内にある場合は、必要に応じて、DC 接続用の SMB プロトコルを有効または無効にします。

- SMBバージョンを有効にするには：

```
vserver cifs security modify -vserver vserver_name -smb2-enabled-for-dc-connections true
```

- SMBバージョンを無効にするには：

```
vserver cifs security modify -vserver vserver_name -smb2-enabled-for-dc-connections false
```

2. admin 権限レベルに戻ります。



```
set -privilege admin
```

## DNS サーバでの SMB サーバのマッピング

Windows ユーザがドライブを SMB サーバ名にマッピングできるように、サイトの DNS サーバに、SMB サーバ名および NetBIOS エイリアスをデータ LIF の IP アドレスにマッピングしたエントリを設定する必要があります。

作業を開始する前に

サイトの DNS サーバに対する管理アクセス権が必要です。管理アクセス権がない場合は、DNS 管理者にこのタスクの実行を依頼する必要があります。

このタスクについて

SMB サーバ名に NetBIOS エイリアスを使用する場合は、各エイリアスに DNS サーバのエントリポイントを作成することを推奨します。

手順

1. DNS サーバにログインします。
2. フォワードルックアップ（A - アドレスレコード）とリバースルックアップ（PTR - ポインタレコード）のエントリを作成して、SMB サーバ名をデータ LIF の IP アドレスにマッピングします。
3. NetBIOS エイリアスを使用する場合は、エイリアスの正規名（CNAME リソースレコード）のルックアップエントリを作成して、各エイリアスを SMB サーバのデータ LIF の IP アドレスにマッピングします。

結果

ネットワーク全体にマッピングが反映されると、Windows ユーザがドライブを SMB サーバ名またはその NetBIOS エイリアスにマッピングできるようになります。

## 共有ストレージへの SMB クライアントアクセスを設定します

共有ストレージへの **SMB** クライアントアクセスを設定します

SVM 上の共有ストレージに対する SMB クライアントアクセスを許可するには、ストレージコンテナを提供するボリュームまたは qtree を作成し、そのコンテナの共有を作成または変更する必要があります。その後、共有およびファイルの権限を設定し、クライアントシステムからのアクセスをテストできます。

作業を開始する前に

- SVMでSMBの設定が完了している必要があります。
- ネームサービス設定に対する更新が完了している必要があります。
- Active Directory ドメインまたはワークグループ設定への追加または変更が完了している必要があります。

ボリュームまたは **qtree** のストレージコンテナを作成します

ボリュームを作成します

を使用して、ボリュームを作成し、ジャンクションポイントやその他のプロパティを指定できます `volume create` コマンドを実行します

このタスクについて

クライアントがデータを使用できるようにするには、ボリュームに *junction path* を含める必要があります。ジャンクションパスは、新しいボリュームを作成するときに指定できます。ジャンクションパスを指定せずにボリュームを作成する場合は、を使用してSVMネームスペースにボリュームを `_mount_` する必要があります `volume mount` コマンドを実行します

作業を開始する前に

- SMBがセットアップされて実行されている必要があります。
- SVMのセキュリティ形式はNTFSである必要があります。
- ONTAP 9.13.1以降では、容量分析とアクティビティ追跡を有効にしてボリュームを作成できます。容量またはアクティビティトラッキングを有効にするには、を問題します `volume create` コマンドにを指定します `-analytics-state` または `-activity-tracking-state` をに設定します `on`。

容量分析とアクティビティ追跡の詳細については、を参照してください [File System Analytics](#) を有効にします。

手順

1. ジャンクションポイントを指定してボリュームを作成します。 `volume create -vserver svm_name -volume volume_name -aggregate aggregate_name -size {integer[KB|MB|GB|TB|PB]} -security-style ntfs -junction-path junction_path`

の選択 `-junction-path` 次のようなものがあります。

- ルートの直下。例： `/new_vol`

新しいボリュームを作成し、SVMのルートボリュームに直接マウントされるように指定することができます。

- 既存のディレクトリの下（例： `/existing_dir/new_vol`

新しいボリュームを作成し、ディレクトリとして表現されている既存のボリューム（既存の階層内）にマウントされるように指定できます。

新しいディレクトリ（新しいボリュームの下の新しい階層）にボリュームを作成する場合は、次のように指定します。 `/new_dir/new_vol` その後、SVMルートボリュームにジャンクションされた新しい親ボリュームを作成しておく必要があります。その後、新しい親ボリューム（新しいディレクトリ）のジャンクションパスに新しい子ボリュームを作成します。

2. 目的のジャンクションポイントでボリュームが作成されたことを確認します。 `volume show -vserver svm_name -volume volume_name -junction`

例

次のコマンドは、SVM `vs1.example.com` およびアグリゲート `aggr1` 上に、`users1` という名前の新しいボリュームを作成します。新しいボリュームは、で使用できます `/users`。ボリュームのサイズは750GBで、ボリュームギャランティのタイプは `volume`（デフォルト）です。

```
cluster1::> volume create -vserver vs1.example.com -volume users
-aggregate aggr1 -size 750g -junction-path /users
[Job 1642] Job succeeded: Successful
```

```
cluster1::> volume show -vserver vs1.example.com -volume users -junction
```

Vserver	Volume	Active	Junction Path	Junction Path Source
vs1.example.com	users1	true	/users	RW_volume

次のコマンドでは、「home4」という名前の新しいボリュームを SVM 「vs1.example.com」 およびアグリゲート「aggr1」に作成します。ディレクトリ /eng/ はvs1 SVMのネームスペースにすでに存在し、新しいボリュームは使用できるようになります /eng/home をクリックします。これがのホームディレクトリになります /eng/ ネームスペース：ボリュームのサイズは750GBで、ボリュームギャランティのタイプは volume（デフォルト）。

```
cluster1::> volume create -vserver vs1.example.com -volume home4
-aggregate aggr1 -size 750g -junction-path /eng/home
[Job 1642] Job succeeded: Successful
```

```
cluster1::> volume show -vserver vs1.example.com -volume home4 -junction
```

Vserver	Volume	Active	Junction Path	Junction Path Source
vs1.example.com	home4	true	/eng/home	RW_volume

qtree を作成します

を使用して、データを含むqtreeを作成し、そのプロパティを指定できます volume qtree create コマンドを実行します

作業を開始する前に

- SVM と新しい qtree を格納するボリュームがすでに存在している必要があります。
- SVM のセキュリティ形式は NTFS である必要があります。また、SMB が設定されて実行されている必要があります。

手順

1. qtree を作成します。 volume qtree create -vserver vserver\_name { -volume volume\_name -qtree qtree\_name | -qtree-path qtree path } -security-style ntfs

ボリュームとqtreeを別々の引数として指定するか、の形式でqtreeパスの引数を指定できます /vol/volume\_name/\_qtree\_name。

2. qtree が必要なジャンクションパスで作成されたことを確認します。 volume qtree show -vserver vserver\_name { -volume volume\_name -qtree qtree\_name | -qtree-path qtree path

```
}
```

## 例

次の例は、ジャンクションパスがであるSVM vs1.example.com上に、qt01という名前のqtreeを作成します  
/vol/data1:

```
cluster1::> volume qtree create -vserver vs1.example.com -qtree-path  
/vol/data1/qt01 -security-style ntfs  
[Job 1642] Job succeeded: Successful
```

```
cluster1::> volume qtree show -vserver vs1.example.com -qtree-path  
/vol/data1/qt01
```

```
                Vserver Name: vs1.example.com  
                Volume Name: data1  
                Qtree Name: qt01  
Actual (Non-Junction) Qtree Path: /vol/data1/qt01  
                Security Style: ntfs  
                Oplock Mode: enable  
                Unix Permissions: ---rwxr-xr-x  
                Qtree Id: 2  
                Qtree Status: normal  
                Export Policy: default  
Is Export Policy Inherited: true
```

## SMB 共有の作成に関する要件と考慮事項

SMB 共有を作成する前に、特にホームディレクトリに関して、共有パスと共有プロパティの要件を理解しておく必要があります。

SMB共有を作成するには、を使用してディレクトリパス構造を指定します -path のオプションを選択します vserver cifs share create クライアントがアクセスするコマンド)。ディレクトリパスは、SVM ネームスペース内に作成したボリュームまたは qtree のジャンクションパスに相当します。ディレクトリパスと対応するジャンクションパスは、共有を作成する前に存在している必要があります。

共有パスには次の要件があります。

- ディレクトリパス名は 255 文字以内で指定します。
- パス名にスペースが含まれている場合は、文字列全体を引用符で囲む必要があります（例： "/new volume/mount here"）。
- UNCパスの場合 (\\servername\sharename\filepath (UNCパスの先頭のを除く) が256文字を超えている場合、Windowsの[プロパティ]ボックスの\*[セキュリティ]\*タブは使用できません。

これは、ONTAP 問題ではなく Windows クライアント問題です。この問題を回避するには、UNC パスが 256 文字を超える共有を作成しないでください。

共有プロパティのデフォルト値は変更できます。

- すべての共有のデフォルトの初期プロパティはです `oplocks`、`browsable`、`changenotify` および `show-previous-versions`。
- 共有の作成時、共有プロパティの指定はオプションです。

ただし、共有の作成時に共有プロパティを指定した場合、デフォルト値は使用されません。を使用する場合 `-share-properties` パラメータ共有を作成するときは、共有に適用するすべての共有プロパティをカンマで区切って指定する必要があります。

- ホームディレクトリ共有を指定するには、を使用します `homedirectory` プロパティ。

この機能を使用すると、接続するユーザと一連の変数に基づいてさまざまなディレクトリにマッピングされる共有を設定できます。ユーザごとに別個の共有を作成する必要はありません。1つの共有を設定し、いくつかのホームディレクトリパラメータを指定して、エントリポイント（共有）とユーザのホームディレクトリ（SVM上のディレクトリ）間のユーザの関係を定義します。



共有の作成後にこのプロパティを追加または削除することはできません。

ホームディレクトリの共有には次の要件があります。

- SMBホームディレクトリを作成する前に、を使用して、ホームディレクトリ検索パスを少なくとも1つ追加する必要があります `vserver cifs home-directory search-path add` コマンドを実行します
- の値で指定したホームディレクトリ共有 `homedirectory` をクリックします `-share-properties` パラメータにはを含める必要があります `%w`（Windowsユーザ名）共有名の動変数。

共有名にはさらにを含めることができます `%d`（ドメイン名）動変数（例：`%d/%w`）または共有名の静的な部分（例：`home1_%w`）。

- 共有が他のユーザのホームディレクトリに接続するために管理者またはユーザによって使用されている場合（のオプションを使用） `vserver cifs home-directory modify` 動的な共有名のパターンの前にチルダを付ける必要があります（`~`）。

["SMBの管理"](#) および `vserver cifs share` マニュアルページには追加情報があります。

## SMB 共有を作成

SMB サーバのデータを SMB クライアントと共有するには、SMB 共有を作成する必要があります。共有を作成するときは、共有をホームディレクトリとして指定するなど、共有プロパティを設定できます。オプションの設定により、共有をカスタマイズすることもできます。

作業を開始する前に

共有を作成する前に、ボリュームまたは `qtree` のディレクトリパスが SVM ネームスペース内に存在している必要があります。

このタスクについて

共有を作成するときのデフォルトの共有ACL（デフォルトの共有権限）はです `Everyone / Full Control`。共有へのアクセスをテストしたら、デフォルトの共有 ACL を削除し、より安全な方法で置き換え

る必要があります。

#### 手順

1. 必要に応じて、共有のディレクトリパス構造を作成します。
  - 。 `vserver cifs share create` コマンドはで指定されたパスをチェックします `-path` オプション（共有の作成時）。指定したパスが存在しない場合、コマンドは失敗します。
2. 指定したSVMに関連付けられているSMB共有を作成します。 `vserver cifs share create -vserver vserver_name -share-name share_name -path path [-share-properties share_properties,...] [other_attributes] [-comment text]`
3. 共有が作成されたことを確認します。 `vserver cifs share show -share-name share_name`

#### 例

次のコマンドは、「SHARE1」という名前のSMB共有をSVM上に作成します `vs1.example.com`。ディレクトリパスはです `/users` をクリックすると、デフォルトのプロパティで作成されます。

```
cluster1::> vserver cifs share create -vserver vs1.example.com -share-name
SHARE1 -path /users

cluster1::> vserver cifs share show -share-name SHARE1
```

Vserver	Share	Path	Properties	Comment	ACL
vs1.example.com	SHARE1	/users	oplocks	-	Everyone / Full
Control			browsable		
			changenotify		
			show-previous-versions		

#### SMB クライアントアクセスを確認

共有にアクセスしてデータを書き込むことで、SMB が正しく設定されていることを確認する必要があります。SMB サーバ名と NetBIOS エイリアスを使用してアクセスをテストします。

#### 手順

1. Windows クライアントにログインします。
2. SMB サーバ名を使用してアクセスをテストします。
  - a. エクスプローラで、次の形式で共有にドライブをマッピングします。 `\\SMB_Server_Name\Share_Name`

正常にマッピングされない場合は、DNS マッピングがネットワーク全体にまだ反映されていない可能性があります。しばらく待ってから、再度 SMB サーバ名を使用してアクセスをテストしてください。

SMBサーバの名前がvs1.example.comで、共有の名前がSHARE1の場合は、次のように入力します。  
\\vs0.example.com\SHARE1

b. 新しく作成したドライブで、テストファイルを作成し、作成できたら削除します。

SMB サーバ名を使用した共有への書き込みアクセスが可能であることを確認できました。

3. NetBIOS エイリアスについて手順 2 を繰り返します。

**SMB 共有のアクセス制御リストを作成**

SMB 共有の Access Control List （ACL ；アクセス制御リスト）を作成して共有権限を設定すると、ユーザとグループの共有へのアクセスレベルを制御できます。

作業を開始する前に

共有へのアクセスを許可するユーザまたはグループを決めておく必要があります。

このタスクについて

ローカルまたはドメインの Windows ユーザまたはグループ名を使用して共有レベルの ACL を設定できます。

新しいACLを作成する前に、デフォルトの共有ACLを削除する必要があります `Everyone / Full Control` は、セキュリティリスクをもたらします。

ワークグループモードでは、ローカルドメイン名は SMB サーバ名です。

**手順**

- 1. デフォルトの共有ACLを削除します。 `vserver cifs share access-control delete -vserver vserver_name -share share_name -user-or-group everyone`
- 2. 新しい ACL を設定します。

設定する <b>ACL</b> に使用するアカウント	入力するコマンド
Windows ユーザ	<code>vserver cifs share access-control create -vserver vserver_name -share share_name -user-group-type windows -user-or-group Windows_domain_name\\user_name -permission access_right</code>
Windows グループ	<code>vserver cifs share access-control create -vserver vserver_name -share share_name -user-group-type windows -user-or-group Windows_group_name -permission access_right</code>

- 3. を使用して、共有に適用されたACLが正しいことを確認します `vserver cifs share access-control show` コマンドを実行します

**例**

次のコマンドは、を示しています Change 「vs1.example.com」"SVM:" 上の「sales」共有に対する「Sales Team」 Windowsグループへの権限

```
cluster1::> vsserver cifs share access-control create -vsserver
vs1.example.com -share sales -user-or-group "Sales Team" -permission
Change

cluster1::> vsserver cifs share access-control show
```

Vserver	Share Name	User/Group Name	User/Group Type	Access Permission
vs1.example.com	c\$	BUILTIN\Administrators	windows	Full_Control
vs1.example.com	sales	DOMAIN\"Sales Team"	windows	Change

以下のコマンドで説明します Change 「Tiger Team」という名前のローカルWindowsグループおよびへの権限 Full\_Control SVM 「vs1」 の「datavol5」共有に対する「Sue Chang」という名前のWindowsローカルユーザの権限：

```
cluster1::> vsserver cifs share access-control create -vsserver vs1 -share
datavol5 -user-group-type windows -user-or-group "Tiger Team" -permission
Change

cluster1::> vsserver cifs share access-control create -vsserver vs1 -share
datavol5 -user-group-type windows -user-or-group "Sue Chang" -permission
Full_Control

cluster1::> vsserver cifs share access-control show -vsserver vs1
```

Vserver	Share Name	User/Group Name	User/Group Type	Access Permission
vs1	c\$	BUILTIN\Administrators	windows	Full_Control
vs1	datavol5	DOMAIN\"Tiger Team"	windows	Change
vs1	datavol5	DOMAIN\"Sue Chang"	windows	Full_Control

共有内で **NTFS** ファイル権限を設定する

共有にアクセスできるユーザまたはグループにファイルアクセスを許可するには、Windows クライアントで、その共有内のファイルおよびディレクトリに対して NTFS フ



ファイルアクセス権を設定する必要があります。

作業を開始する前に

このタスクを実行する管理者は、選択したオブジェクトに対する権限を変更するための十分な NTFS 権限を持っている必要があります。

このタスクについて

"[SMBの管理](#)" また、標準および詳細な NTFS アクセス権の設定方法については、Windows のマニュアルを参照してください。

手順

1. Windows クライアントに管理者としてログインします。
2. Windows Explorer の \* ツール \* メニューから、\* ネットワークドライブのマップ \* を選択します。
3. [ ネットワークドライブの割り当て \* ] ボックスに入力します。
  - a. ドライブ文字を選択します。
  - b. [ \* フォルダ \* ] ボックスに、権限を適用するデータと共有名を含む共有を含む SMB サーバー名を入力します。

SMBサーバ名がSMB\_SERVER01で、共有の名前が「SHARE1」の場合は、と入力します  
\\SMB\_SERVER01\SHARE1。



SMBサーバ名の代わりに、SMBサーバのデータインターフェイスのIPアドレスを指定できます。

- c. [ 完了 ] をクリックします。

選択したドライブがマウントされて使用可能な状態になり、共有内に格納されているファイルやフォルダが Windows エクスプローラウィンドウに表示されます。

4. NTFS ファイル権限を設定するファイルまたはディレクトリを選択します。
5. ファイルまたはディレクトリを右クリックし、\* プロパティ \* を選択します。
6. [ \* セキュリティ \* ] タブを選択します。

Security タブには、NTFS 権限が設定されているユーザとグループのリストが表示されます。[ < オブジェクト > のアクセス許可 ] ボックスには、選択したユーザーまたはグループの有効なアクセス許可と拒否のアクセス許可のリストが表示されます。

7. [ 編集 ( Edit ) ] をクリックします。

[ < オブジェクト > のアクセス許可 ] ボックスが開きます。

8. 次のうち必要な操作を実行します。

状況	実行する処理
新しいユーザまたはグループに対する標準の NTFS 権限を設定します	<p>a. [ 追加 ( Add ) ] をクリックします。</p> <p>[ ユーザー、コンピュータ、サービスアカウント、またはグループの選択 ] ウィンドウが開きます。</p> <p>b. [ 選択するオブジェクト名を入力してください * ] ボックスに、 NTFS アクセス権を追加するユーザまたはグループの名前を入力します。</p> <p>c. [OK] をクリックします。</p>
ユーザまたはグループに対する標準の NTFS 権限を変更または削除する	[ * グループ名またはユーザー名 * ] ボックスで、変更または削除するユーザーまたはグループを選択します。

9. 次のうち必要な操作を実行します。

状況	実行する処理
新規または既存のユーザまたはグループに対する標準の NTFS 権限を設定する	[ * パーミッション for < オブジェクト > * ] ボックスで、選択したユーザーまたはグループに対して許可または許可しないアクセスのタイプの [ 許可 * ] または [ 拒否 * ] ボックスを選択します。
ユーザまたはグループを削除します	[ 削除 ( Remove ) ] をクリックします。



標準の権限ボックスの一部またはすべてを選択できない場合、権限は親オブジェクトから継承されます。[ \* 特別な権限 \* ] ボックスは選択できません。選択されている場合は、選択したユーザまたはグループに対して詳細な権限が 1 つ以上設定されていることを意味します。

10. そのオブジェクトの NTFS アクセス権の追加、削除、または編集が完了したら、 **OK** をクリックします。

ユーザアクセスを確認

設定したユーザが、 SMB 共有およびその中に含まれるファイルにアクセスできることをテストする必要があります。

手順

- Windows クライアントで、共有へのアクセスを許可したいいずれかのユーザとしてログインします。
- Windows Explorer の \* ツール \* メニューから、 \* ネットワークドライブのマップ \* を選択します。
- [ ネットワークドライブの割り当て \* ] ボックスに入力します。
  - ドライブ文字を選択します。
  - [ \* フォルダー \* ] ボックスに、ユーザーに提供する共有名を入力します。

SMBサーバ名がSMB\_SERVER01で、共有の名前が「SHARE1」の場合は、と入力します  
\\SMB\_SERVER01\share1。

c. [完了] をクリックします。

選択したドライブがマウントされて使用可能な状態になり、共有内に格納されているファイルやフォルダが Windows エクスプローラウィンドウに表示されます。

4. テストファイルを作成し、その存在を確認し、テキストを書き込んで、テストファイルを削除します。

## CLIを使用したSMBの管理

### SMB リファレンスの概要

SMB プロトコルで ONTAP ファイルアクセス機能を使用できます。CIFS サーバを有効にしたり、共有を作成したり、Microsoft サービスを有効にしたりできます。



SMB(Server Message Block) は、Common Internet File System (CIFS) プロトコルの最新のダイレクトです。ONTAP コマンドラインインターフェイス（CLI）および OnCommand 管理ツールでは、\_cifs\_ というメッセージが引き続き表示されます。

これらの手順は、次のような状況で使用する必要があります。

- ONTAP の SMB プロトコル機能の範囲について理解する必要がある。
- SMBの基本的な設定ではなく、あまり一般的でない設定タスクとメンテナンスタスクを実行する。
- System Manager や自動スクリプトツールではなく、コマンドラインインターフェイス（CLI）を使用する必要がある。

### SMB サーバのサポート

#### SMB サーバのサポートの概要

Storage Virtual Machine（SVM）上で SMB サーバを有効にして設定し、SMB クライアントがクラスタ上のファイルにアクセスできるようにすることができます。

- クラスタ内のデータ SVM は、それぞれ 1 つの Active Directory ドメインにバインドできます。
- データ SVM は、必ずしも同じドメインにバインドする必要はありません。
- 複数の SVM を同じドメインにバインドできます。

SMB サーバを作成する前に、データの提供に使用する SVM と LIF を設定しておく必要があります。データネットワークがフラットでない場合は、IPspace、ブロードキャストドメイン、およびサブネットの設定も必要になることがあります。詳細については、『ネットワーク管理ガイド』を参照してください。

関連情報

["Network Management の略"](#)

[SMB サーバを変更](#)

サポートされる **SMB** のバージョンと機能

Server Message Block （ **SMB** ；サーバメッセージブロック）は、 Microsoft Windows クライアントおよびサーバで使用されるリモートファイル共有プロトコルです。 ONTAP 9 ではすべての **SMB** のバージョンがサポートされますが、デフォルトである **SMB 1.0** がサポートされるかどうかは ONTAP のバージョンによって異なります。 ONTAP **SMB** サーバが、ご使用の環境で必要なクライアントと機能をサポートしていることを確認する必要があります。

ONTAP がサポートする **SMB** クライアントおよびドメインコントローラの最新情報については、 Interoperability Matrix Tool を参照してください。

**SMB 2.0** 以降のバージョンは ONTAP 9 の **SMB** サーバではデフォルトで有効になっており、必要に応じて有効または無効を切り替えることができます。 次の表に、 **SMB 1.0** のサポートとデフォルト設定を示します。

<b>SMB 1.0</b> の機能：	<b>ONTAP 9</b> のリリース：			
	9.0	9.1	9.2.	9.3以降
はデフォルトで有効になっています	はい。	はい。	はい。	いいえ
有効または無効にすることができます	いいえ	はい * 9.1 P8 以降が必要です。	はい。	はい。



**SMB 1.0** および **2.0** のドメインコントローラへの接続に関するデフォルト設定も ONTAP のバージョンによって異なります。 詳細については、[vserver cifs security modify](#) のマニュアルページ。 既存の **CIFS** サーバで **SMB 1.0** を実行している環境では、できるだけ早く最新の **SMB** バージョンに移行して、セキュリティとコンプライアンスを強化する必要があります。 詳細については、ネットアップの担当者にお問い合わせください。

次の表に、 **SMB** でサポートされる機能と対応するバージョンを示します。 **SMB** の機能には、デフォルトで有効になるものと追加の設定が必要なものがあります。

* この機能：	* 有効化が必要：	* <b>ONTAP 9</b> では、以下のバージョンの <b>SMB</b> がサポートされています。 *				
		1.0	"2.0"	2.1	3.0	3.1.1
従来の <b>SMB 1.0</b> の機能		X	X	X	X	X
永続性ハンドル			X	X	X	X

* この機能： *	* 有効化が必要 ： *	* ONTAP 9 では、以下のバージョンの <b>SMB</b> がサポートされています。 *				
複合操作			X	X	X	X
非同期操作			X	X	X	X
読み取り / 書き込みバッファのサイズが増加します			X	X	X	X
拡張性の向上			X	X	X	X
SMB 署名	X	X	X	X	X	X
代替データストリーム（ADS）ファイル形式	X	X	X	X	X	X
Large MTU（ONTAP 9.7 以降ではデフォルトで有効）	X			X	X	X
oplock リース				X	X	X
共有の継続的な可用性	X				X	X
永続的ハンドル					X	X
監視					X	X
SMB 暗号化：AES-128-CCM	X				X	X
スケールアウト（CA 共有で必要）					X	X
透過的なフェイルオーバー					X	X

* この機能： *	* 有効化が必要 ： *	* <b>ONTAP 9</b> では、以下のバージョンの <b>SMB</b> がサポートされています。 *				
SMB マルチチャネル（ ONTAP 9.4 以降）	X				X	X
事前認証の整合性						X
クラスタ・クライアント・フェイルオーバー v.2（ CCFv2）						X
SMB 暗号化： AES-128-GCM（ ONTAP 9.1 以降）	X					X

## 関連情報

[SMB 署名を使用したネットワークセキュリティの強化](#)

[SMBサーバの最小認証セキュリティレベルの設定](#)

[SMB を介したデータ転送での SMB サーバの SMB 暗号化要求の設定](#)

"[ネットアップテクニカルレポート 4543：『SMB Protocol Best Practices』](#)"

"[ネットアップの相互運用性](#)"

サポートされない **Windows** の機能

ネットワークで CIFS を使用する場合は、一部の Windows の機能が ONTAP ではサポートされないことに注意する必要があります。

ONTAP では、次の Windows 機能はサポートされません。

- Encrypted File System（EFS；暗号化ファイルシステム）
- 変更ジャーナルでの NT File System（NTFS）イベントのロギング
- Microsoft File Replication Service（FRS；ファイルレプリケーションサービス）
- Microsoft Windows インデックスサービス
- Hierarchical Storage Management（HSM；階層型ストレージ管理）経由のリモートストレージ

- Windows クライアントからのクォータ管理
- Windows のクォータのセマンティクス
- LMHOSTS ファイル
- NTFS のネイティブ圧縮機能です

**SVM に NIS または LDAP ネームサービスを設定します**

SMB アクセスでは、NTFS セキュリティ形式のボリューム内のデータにアクセスする場合でも、UNIX ユーザへのユーザマッピングが常に実行されます。NIS または LDAP ディレクトリストアにその情報が格納されている UNIX ユーザに Windows ユーザをマッピングする場合や、ネームマッピングに LDAP を使用する場合は、SMB のセットアップ時にこのネームサービスを設定する必要があります。

作業を開始する前に

ネームサービスデータベース設定をネームサービスインフラに合わせてカスタマイズしておく必要があります。

このタスクについて

SVM は、ネームサービス ns-switch データベースを使用して、指定されたネームサービスデータベースを検索するソースの順番を決定します。ns-switch ソースには、「files」、「nis」、または「ldap」を任意に組み合わせて使用できます。グループデータベースの場合、ONTAP は設定されたすべてのソースからグループメンバーシップを取得し、統合されたグループメンバーシップ情報をアクセスチェックに使用します。UNIX グループ情報の取得時にこれらのいずれかのソースを使用できないと、ONTAP は完全な UNIX クレデンシャルを取得できず、アクセスチェックが失敗することがあります。そのため、ns-switch 設定にグループデータベースのすべての ns-switch ソースが設定されていることを必ず確認する必要があります。

デフォルトでは、SMBサーバは、すべてのWindowsユーザをローカルに格納されているデフォルトのUNIXユーザにマッピングします passwd データベース：デフォルトの設定を使用する場合、SMB アクセスに対する、NIS または LDAP UNIX ユーザおよびグループのネームサービスまたは LDAP ユーザマッピングの設定は省略可能です。

手順

1. UNIX ユーザ、グループ、ネットグループ情報が NIS ネームサービスによって管理されている場合、NIS ネームサービスを次のように設定します。
  - a. を使用して、ネームサービスの現在の順序を確認します `vserver services name-service ns-switch show` コマンドを実行します

この例では、3つのデータベースを示します (group、passwd および netgroup) を使用できます `nis` ネームサービスソースがのみを使用している files 情報源として

```
vserver services name-service ns-switch show -vserver vs1
```

Vserver	Database	Enabled	Source Order
-----	-----	-----	-----
vs1	hosts	true	dns, files
vs1	group	true	files
vs1	passwd	true	files
vs1	netgroup	true	files
vs1	namemap	true	files

を追加する必要があります `nis` を参照してください `group` および `passwd` データベース、およびオプションでにアクセスできます `netgroup` データベース：

- b. を使用して、ネームサービス `ns-switch` データベースを必要な順序で調整します `vserver services name-service ns-switch modify` コマンドを実行します

パフォーマンスを最大にするためには、SVM に設定する予定のないネームサービスデータベースにはネームサービスを追加しないでください。

複数のネームサービスデータベースの設定を変更する場合、変更するそれぞれのネームサービスデータベースに対して別々にコマンドを実行する必要があります。

この例では、`nis` および `files` は、のソースとして設定されています `group` および `passwd` この順番でデータベースを作成します。その他のネームサービスデータベースは変更されません。

```
vserver services name-service ns-switch modify -vserver vs1 -database group
-sources nis,files vserver services name-service ns-switch modify -vserver
vs1 -database passwd -sources nis,files
```

- c. を使用して、ネームサービスの順序が正しいことを確認します `vserver services name-service ns-switch show` コマンドを実行します

```
vserver services name-service ns-switch show -vserver vs1
```

Vserver	Database	Enabled	Source Order
-----	-----	-----	-----
vs1	hosts	true	dns, files
vs1	group	true	nis, files
vs1	passwd	true	nis, files
vs1	netgroup	true	files
vs1	namemap	true	files



d. NISネームサービス設定を作成します。+

```
vserver services name-service nis-domain create -vserver vserver_name
-domain NIS_domain_name -servers NIS_server_IPaddress,... -active true+

vserver services name-service nis-domain create -vserver vs1 -domain
example.com -servers 10.0.0.60 -active true
```



ONTAP 9.2以降では、フィールドが表示されます -nis-servers フィールドを置き換えます -servers。この新しいフィールドには、NISサーバのホスト名またはIPアドレスを指定できます。

e. NISネームサービスが適切に設定され、アクティブになっていることを確認します。 vserver

```
services name-service nis-domain show vserver vserver_name

vserver services name-service nis-domain show vserver vs1
```

Vserver	Domain	Active	Server
vs1	example.com	true	10.0.0.60

2. UNIX ユーザ、グループ、ネットグループ情報またはネームマッピングが LDAP ネームサービスによって管理されている場合は、格納されている情報を使用して LDAP ネームサービスを設定します ["NFS の管理"](#)。

## ONTAP のネームサービススイッチ設定の仕組み

ONTAP では、に相当するテーブルにネームサービス設定情報が格納されます /etc/nsswitch.conf UNIXシステム上のファイル。このテーブルを環境に応じて適切に設定するためには、その機能と ONTAP でテーブルがどのように使用されるかを理解しておく必要があります。

ONTAP ネームサービススイッチテーブルは、ONTAP が特定の種類のネームサービス情報を取得する際にどのネームサービスソースをどの順番で参照するかを決定します。ONTAP では、SVM ごとに個別のネームサービススイッチテーブルが保持されます。

### データベースタイプ

テーブルには、次の各データベースタイプについてネームサービスのリストが格納されます。

データベースタイプ	ネームサービスソースの用途	有効なソース
ホスト	ホスト名の IP アドレスへの変換	ファイル、DNS
グループ	ユーザグループ情報を検索しています	files 、 nis 、 ldap が表示されます
パスワード	ユーザ情報を検索しています	files 、 nis 、 ldap が表示されます

データベースタイプ	ネームサービスソースの用途	有効なソース
ネットグループ	ネットグループ情報の検索	files 、 nis 、 ldap が表示されます
namemap	ユーザ名のマッピング	ファイル、 LDAP

## ソースタイプ

ソースタイプによって、該当する情報を取得するために使用するネームサービスソースが決まります。

ソースタイプ	情報の検索先	使用するコマンド
ファイル	ローカルのソースファイル	<pre>vserver services name- service unix-user vserver services name-service unix-group</pre> <pre>vserver services name- service netgroup</pre> <pre>vserver services name- service dns hosts</pre>
NIS	SVM の NIS ドメイン設定で指定された外部の NIS サーバ	<pre>vserver services name- service nis-domain</pre>
LDAP	SVM の LDAP クライアント設定で指定された外部の LDAP サーバ	<pre>vserver services name- service ldap</pre>
DNS	SVM の DNS 設定で指定された外部の DNS サーバ	<pre>vserver services name- service dns</pre>

データアクセスとSVM管理者の両方の認証にNISまたはLDAPを使用する場合も、を追加する必要があります  
files また、NISまたはLDAP認証が失敗した場合のフォールバックとしてローカルユーザを設定します。

## 外部ソースへのアクセスに使用するプロトコル

ONTAP では、外部ソースのサーバへのアクセスに次のプロトコルを使用します。

外部のネームサービスソース	アクセスに使用するプロトコル
NIS	UDP
DNS	UDP
LDAP	TCP

## 例

次の例は、SVMのネームサービススイッチ設定を表示します svm\_1 :

```
cluster1::*> vserver services name-service ns-switch show -vserver svm_1
```

Vserver	Database	Source Order
svm_1	hosts	files, dns
svm_1	group	files
svm_1	passwd	files
svm_1	netgroup	nis, files

ユーザまたはグループ情報の検索では、ONTAP はローカルのソースファイルだけを参照します。結果が返されない場合、検索は失敗します。

ネットグループ情報の検索では、ONTAP が最初に外部 NIS サーバを参照し、結果が返されない場合は、次にローカルネットグループファイルが照会されます。

SVM svm\_1 のテーブルには、ネームマッピング用のネームサービスエントリは含まれていません。そのため、ONTAP はデフォルトでローカルのソースファイルだけを参照します。

## SMB サーバを管理します

### SMB サーバを変更

を使用して、ワークグループからActive Directoryドメイン、ワークグループから別のワークグループ、またはActive DirectoryドメインからワークグループにSMBサーバを移動できます `vserver cifs modify` コマンドを実行します

このタスクについて

SMB サーバ名や管理ステータスなど、SMB サーバのその他の属性を変更することもできます。詳細については、のマニュアルページを参照してください。

#### 選択肢

- ワークグループから Active Directory ドメインに SMB サーバを移動するには、次の手順を実行します。
  - SMBサーバの管理ステータスをに設定します `down`。

```
Cluster1::>vserver cifs modify -vserver vs1 -status-admin down
```

- ワークグループから Active Directory ドメインに SMB サーバを移動するには、次の手順を実行します。 `vserver cifs modify -vserver vserver_name -domain domain_name`

```
Cluster1::>vserver cifs modify -vserver vs1 -domain example.com
```

SMBサーバのActive Directoryマシンアカウントを作成するには、にコンピュータを追加するための十分な権限があるWindowsアカウントの名前とパスワードを指定する必要があります `ou=example` ou 内のコンテナ `example.com`ドメイン。

ONTAP 9.7 以降では、権限がある Windows アカウントの名前とパスワードの代わりに、`keytab` ファイルの URI を AD 管理者から提供される場合があります。URIを受け取ったら、に含めます `-keytab-uri` パラメータと `vserver cifs` コマンド

- ワークグループから別のワークグループに SMB サーバを移動します。

- a. SMBサーバの管理ステータスをに設定します `down`。

```
Cluster1::>vserver cifs modify -vserver vs1 -status-admin down
```

- b. SMBサーバのワークグループを変更します。 `vserver cifs modify -vserver vserver_name -workgroup new_workgroup_name`

```
Cluster1::>vserver cifs modify -vserver vs1 -workgroup workgroup2
```

- Active Directory ドメインからワークグループに SMB サーバを移動するには、次の手順を実行します。

- a. SMBサーバの管理ステータスをに設定します `down`。

```
Cluster1::>vserver cifs modify -vserver vs1 -status-admin down
```

- b. Active DirectoryドメインからワークグループにSMBサーバを移動します。 `vserver cifs modify -vserver vserver_name -workgroup workgroup_name`

```
cluster1::> vserver cifs modify -vserver vs1 -workgroup workgroup1
```



ワークグループモードに切り替えるには、継続的可用性を備えた共有、シャドウコピー、AES など、ドメインベースの機能をすべて無効にし、該当する設定がシステムによって自動的に削除されるようにする必要があります。ただし、「`EXAMPLE.COM\userName`」などのドメインで設定された共有 ACL は正しく機能しませんが、ONTAP で削除することはできません。このような共有 ACL は、コマンドの完了後できるだけ早く外部ツールを使用して削除してください。AES が有効になっている場合は、「`example.com`」ドメインで AES を無効にするための十分な権限を持つ Windows アカウントの名前とパスワードの入力を求められることがあります。

- の該当するパラメータを使用して、他の属性を変更します `vserver cifs modify` コマンドを実行します

オプションを使用した**SMB**サーバのカスタマイズ

SMB サーバのカスタマイズ方法について検討する場合は、使用できるオプションを把握しておくと便利です。一部のオプションは汎用的なものですが、SMB の特定の機能を有効にして設定するためのオプションも複数あります。SMBサーバオプションは、で制御します `vserver cifs options modify` オプション

以下に、admin 権限レベルで使用できる SMB サーバオプションについて説明します。

• \* SMB セッションタイムアウト値の設定 \*

このオプションでは、SMB セッションが切断されるまでのアイドル時間を秒数で指定できます。アイドルセッションとは、ユーザがクライアントでファイルもディレクトリも開いていないセッションのことです。デフォルト値は900秒です。

• \* デフォルトの UNIX ユーザーの構成 \*

このオプションでは、SMB サーバで使用されるデフォルトの UNIX ユーザを指定できます。ONTAP はデフォルトユーザ「pcuser」（UID は 65534）を自動的に作成し、グループ「pcuser」（GID は 65534）を作成して、デフォルトユーザを「pcuser」グループに追加します。SMB サーバを作成すると、ONTAP は自動的に「pcuser」をデフォルトの UNIX ユーザとして設定します。

• \* ゲスト UNIX ユーザの設定 \*

このオプションでは、信頼されていないドメインからログインしたユーザをマッピングする UNIX ユーザの名前を指定できます。これにより、信頼されていないドメインのユーザが SMB サーバに接続できるようになります。デフォルトでは、このオプションは設定されていません（デフォルト値はありません）。このため、信頼されていないドメインのユーザは SMB サーバへの接続を許可されません。

• \* モードビットの読み取り権限付与の実行の有効化または無効化 \*

このオプションを有効または無効にすると、UNIX 実行可能ビットが設定されていない場合でも、UNIX モードビットが設定された実行可能ファイルの実行を、ファイルへの読み取り権限を持つ SMB クライアントに許可するかどうかを指定できます。このオプションは、デフォルトでは無効になっています。

• \* NFS クライアントからの読み取り専用ファイルの削除機能の有効化または無効化 \*

このオプションを有効または無効にすると、読み取り専用属性が設定されたファイルやフォルダの削除を NFS クライアントに許可するかどうかを指定できます。NTFS の削除では、読み取り専用属性が設定されたファイルやフォルダの削除は許可されません。UNIX の削除では読み取り専用ビットが無視され、ファイルやフォルダを削除できるかどうかは親ディレクトリの権限によって判断されます。デフォルト設定はです `disabled` これにより、NTFSの削除セマンティクスが発生します。

• \* Windows Internet Name Service サーバーアドレスの設定 \*

このオプションでは、複数の Windows Internet Name Service（WINS）サーバアドレスをカンマで区切って指定できます。IPv4 アドレスを指定する必要があります。IPv6 アドレスはサポートされません。デフォルト値はありません。

以下に、advanced 権限レベルで使用できる SMB サーバオプションについて説明します。

• \* CIFS ユーザーへの UNIX グループ権限の付与 \*

このオプションは、ファイルの所有者ではない CIFS ユーザにグループ権限を付与するかどうかを指定します。CIFSユーザがUNIXセキュリティ形式のファイルの所有者ではない場合に、このパラメータがに設定されます `true`` をクリックすると、ファイルに対するグループ権限が付与されます。CIFSユーザがUNIXセキュリティ形式のファイルの所有者ではない場合に、このパラメータがに設定されます `false`` を指定すると、通常のUNIXルールを適用してファイル権限が付与されます。このパラメータは、権限がに設定されているUNIXセキュリティ形式のファイルに適用されます ``mode bits` セキュリティモードがNTFSまたはNFSv4のファイルには適用されません。デフォルト設定は `false`` です。

- \* SMB 1.0 の有効化または無効化 \*

ONTAP 9.3 で SMB サーバが作成された SVM では、SMB 1.0 がデフォルトで無効になります。



ONTAP 9.3 以降では、ONTAP 9.3 で新しく作成された SMB サーバについては SMB 1.0 がデフォルトで無効になります。できるだけ早く最新の SMB バージョンに移行して、セキュリティとコンプライアンスを強化してください。詳細については、ネットアップの担当者にお問い合わせください。

- \* SMB 2.x の有効化または無効化 \*

SMB 2.0 は、LIF フェイルオーバーをサポートする SMB の最小バージョンです。SMB 2.x を無効にした場合、ONTAP では SMB 3.x も自動的に無効になります

SMB 2.0 は SVM でのみサポートされます。このオプションは、SVM ではデフォルトで有効になります

- \* SMB 3.0の有効化または無効化\*

SMB 3.0 は、継続的可用性を備えた共有をサポートする SMB の最小バージョンです。Windows Server 2012 および Windows 8 は、SMB 3.0 をサポートする Windows の最小バージョンです。

SMB 3.0はSVMでのみサポートされます。このオプションは、SVM ではデフォルトで有効になります

- \* SMB 3.1 を有効または無効にします

Windows 10 は、SMB 3.1 をサポートする Windows の唯一のバージョンです。

SMB 3.1はSVMでのみサポートされます。このオプションは、SVM ではデフォルトで有効になります

- \* ODX コピーオフロードの有効化または無効化 \*

ODX コピーオフロードは、対応する Windows クライアントで自動的に使用されます。このオプションはデフォルトで有効になっています。

- \* ODX コピーオフロードの直接コピーメカニズムの有効化または無効化 \*

直接コピーメカニズムは、コピー中のファイル変更を禁止するモードで Windows クライアントがコピー元のファイルを開こうとした場合に、コピーオフロード処理のパフォーマンスを向上させます。デフォルトでは、直接コピーメカニズムは有効になっています。

- \* 自動ノードリファラルの有効化または無効化 \*

自動ノードリファラルでは、SMB サーバはクライアントに対して、要求した共有を介してアクセスするデータのホストノードに対してローカルなデータ LIF を自動的に参照することになります。

- \* SMB \* のエクスポート・ポリシーの有効化または無効化

このオプションは、デフォルトでは無効になっています。

- \* ジャンクションポイントのリパースポイントとしての使用の有効化または無効化 \*

このオプションを有効にすると、SMB サーバはジャンクションポイントをリパースポイントとして SMB クライアントに公開します。このオプションは、SMB 2.x 接続または SMB 3.0 接続のみで有効です。このオプションはデフォルトで有効になっています。

このオプションは SVM でのみサポートされます。このオプションは、SVM ではデフォルトで有効になります

- \* TCP 接続ごとの最大同時操作数の設定 \*

デフォルト値は255です。

- \* ローカルの Windows ユーザーとグループ機能の有効化または無効化 \*

このオプションはデフォルトで有効になっています。

- \* ローカル Windows ユーザー認証の有効化または無効化 \*

このオプションはデフォルトで有効になっています。

- \* VSS シャドウ・コピー機能の有効化または無効化 \*

ONTAP では、シャドウコピー機能によって、Hyper-V over SMB 解決策を使用して格納されたデータのリモートバックアップを実行します。

このオプションは、SVM、および Hyper-V over SMB 構成でのみサポートされます。このオプションは、SVM ではデフォルトで有効になります

- \* シャドウ・コピーのディレクトリ階層の設定 \*

このオプションでは、シャドウコピー機能を使用するときに、シャドウコピーを作成するディレクトリの最大階層を定義できます。

このオプションは、SVM、および Hyper-V over SMB 構成でのみサポートされます。このオプションは、SVM ではデフォルトで有効になります

- \* マルチドメインネームマッピングの検索機能の有効化または無効化 \*

有効にすると、UNIX ユーザが Windows ユーザ名のドメイン部分にワイルドカード (\*) を使用して Windows ドメインユーザにマッピングされている場合に (\*\joe など)、ONTAP はホームドメインと双方向の信頼関係が確立されたすべてのドメインで、指定したユーザを検索します。ホームドメインとは、SMB サーバのコンピュータアカウントが含まれるドメインです。

双方向の信頼関係が確立されたすべてのドメインを検索する代わりに、信頼できるドメインのリストを設定することもできます。このオプションを有効にして、優先リストを設定すると、マルチドメインネームマッピングの検索を実行するために優先リストが使用されます。

デフォルトでは、マルチドメインネームマッピングの検索は有効になります。

- \* ファイルシステムセクターサイズの設定 \*

このオプションでは、ONTAP から SMB クライアントに報告されるファイルシステムセクターサイズをバイト単位で設定できます。このオプションには2つの有効な値があります。4096 および 512。デフォルト値はです 4096。この値をに設定する必要がある場合があります 512 Windowsアプリケーションが512バイトのセクターサイズのみをサポートしている場合。

- \* ダイナミックアクセス制御の有効化または無効化 \*

このオプションを有効にすると、監査を使用した集約型アクセスポリシーのステージングや、グループポリシーオブジェクトを使用した集約型アクセスポリシーの実装を含めて、ダイナミックアクセス制御を使用して SMB サーバのオブジェクトを保護できます。このオプションは、デフォルトでは無効になっています。

このオプションは SVM でのみサポートされます。

- \* 認証されていないセッションのアクセス制限の設定（restrict anonymous） \*

このオプションでは、認証されていないセッションのアクセス制限を指定します。制限は匿名ユーザに適用されます。デフォルトでは、匿名ユーザに対するアクセス制限はありません。

- \* UNIX 対応のセキュリティを使用するボリューム（UNIX セキュリティ形式のボリューム、または UNIX 対応のセキュリティを使用する mixed セキュリティ形式のボリューム）での NTFS ACL の提供を有効または無効にする \*

このオプションを有効または無効にして、UNIX セキュリティ形式のファイルやフォルダのファイルセキュリティが SMB クライアントに表示される方法を指定します。有効 ONTAP にすると、UNIX セキュリティ形式のボリューム内のファイルやフォルダは、NTFS ACL を使用する NTFS ファイルセキュリティが設定されたファイルやフォルダとして SMB クライアントに表示されます。無効 ONTAP にすると、UNIX セキュリティ形式のボリュームは、ファイルセキュリティのない FAT ボリュームとして表示されます。デフォルトでは、ボリュームは NTFS ACL を使用する NTFS ファイルセキュリティが設定されたボリュームとして表示されます。

- \* SMB 擬似オープン機能の有効化または無効化 \*

この機能を有効にすると、ONTAP がファイルやディレクトリの属性情報を照会する際のオープン要求とクローズ要求の方法が最適化されて、SMB 2.x および SMB 3.0 のパフォーマンスが向上します。デフォルトでは、SMB 擬似オープン機能は有効になっています。このオプションは、SMB 2.x 以降を使用する接続にのみ有効です。

- \* UNIX 拡張の有効化または無効化 \*

このオプションを有効にすると、SMB サーバで UNIX 拡張が有効になります。UNIX 拡張を使用すると、SMB プロトコルを介して POSIX/UNIX 形式のセキュリティを表示できます。デフォルトでは、このオプションは無効になっています。

Mac OSX クライアントなど、UNIX ベースの SMB クライアントが環境内にある場合は、UNIX 拡張を有効にしてください。UNIX 拡張を有効にすると、SMB サーバは POSIX/UNIX セキュリティ情報を SMB 経由で UNIX ベースのクライアントに送信できるようになります。クライアントは、受け取ったセキュリティ情報を POSIX/UNIX セキュリティに変換します。

- \* 略称を使用した検索のサポートの有効化または無効化 \*



このオプションを有効にすると、SMB サーバは短縮名に対して検索を実行できます。このオプションを有効にした場合の検索では、長いファイル名に加えて 8.3 形式のファイル名も照合されます。このパラメータのデフォルト値は `false`。

• \* DFS 対応の自動通知のサポートの有効化または無効化 \*

このオプションを有効または無効にして、共有に接続する SMB 2.x および SMB 3.0 クライアントに SMB サーバから DFS 対応を自動的に通知するかどうかを指定します。ONTAP では、SMB アクセス用のシンボリックリンクの実装で DFS リファールが使用されます。有効にすると、シンボリックリンクアクセスが有効かどうかに関係なく、SMB サーバは常に DFS 対応を通知します。無効にすると、シンボリックリンクアクセスが有効になっている共有にクライアントが接続する場合にのみ、SMB サーバは DFS 対応を通知します。

• \* SMB クレジットの最大数の設定 \*

ONTAP 9.4以降ではを設定します `-max-credits` オプションを使用すると、クライアントとサーバがSMBバージョン2以降を実行している場合に、SMB接続に付与するクレジットの数を制限できます。デフォルト値は128です。

• \* SMB マルチチャネルのサポートの有効化または無効化 \*

を有効にします `-is-multichannel-enabled` ONTAP 9.4以降のリリースのオプションを使用すると、クラスタとそのクライアントに適切なNICが導入されている場合に、SMBサーバは単一のSMBセッションに対して複数の接続を確立できます。これにより、スループットとフォールトトレランスが向上します。このパラメータのデフォルト値は `false`。

SMB マルチチャネルが有効な場合、次のパラメータも指定できます。

- 各マルチチャネルセッションに許可される最大接続数。このパラメータのデフォルト値は 32 です。
- 各マルチチャネルセッションで通知されるネットワークインターフェイスの最大数。このパラメータのデフォルト値は256です。

## SMBサーバオプションの設定

SMBサーバオプションは、Storage Virtual Machine (SVM) でのSMBサーバの作成後にいつでも設定できます。

### ステップ

1. 必要な操作を実行します。

SMBサーバオプションの設定	入力するコマンド
admin 権限レベルで設定します	<pre>vserver cifs options modify -vserver vserver_name options</pre>
advanced 権限レベルで設定します	<pre>a. set -privilege advanced b. vserver cifs options modify -vserver vserver_name options c. set -privilege admin</pre>

SMBサーバオプションの設定の詳細については、のマニュアルページを参照してください `vserver cifs options modify` コマンドを実行します

#### SMBユーザへのUNIXグループ権限付与の設定

このオプションを使用すると、ファイルの所有者でない SMB ユーザもファイルやディレクトリにアクセスする権限をグループに付与することができます。

##### 手順

1. 権限レベルを `advanced` に設定します。 `set -privilege advanced`
2. UNIX グループ権限付与を必要に応じて設定します。

状況	入力するコマンド
ユーザがファイルの所有者でない場合にもファイルやディレクトリにアクセスするためのグループ権限を付与する	<code>vserver cifs options modify -grant-unix-group-perms-to-others true</code>
ユーザがファイルの所有者でない場合はファイルやディレクトリにアクセスするためのグループ権限を付与しないようにします	<code>vserver cifs options modify -grant-unix-group-perms-to-others false</code>

3. オプションが目的の値に設定されていることを確認します。 `vserver cifs options show -fields grant-unix-group-perms-to-others`
4. `admin` 権限レベルに戻ります。 `set -privilege admin`

#### 匿名ユーザのアクセス制限を設定します

デフォルトでは、認証されていない匿名ユーザ（`_null` ユーザ）はネットワーク上の特定の情報にアクセスできます。SMBサーバオプションを使用して、匿名ユーザに対するアクセス制限を設定できます。

##### このタスクについて

。 `-restrict-anonymous` SMBサーバオプションはに対応します `RestrictAnonymous` Windowsのレジストリエントリ。

匿名ユーザは、ユーザ名、詳細、アカウントポリシー、共有名など、ネットワーク上の Windows ホストから特定のタイプのシステム情報をリストまたは列挙できます。次の 3 つのうち、いずれかのアクセス制限設定を指定して、匿名ユーザのアクセスを制御することができます。

価値	説明
<code>no-restriction</code> （デフォルト）	匿名ユーザにアクセス制限を設定しません。
<code>no-enumeration</code>	匿名ユーザに対して列挙だけを制限します。

価値	説明
no-access	匿名ユーザに対してアクセスを制限します。

## 手順

1. 権限レベルを **advanced** に設定します。 `set -privilege advanced`
2. **restrict anonymous**を設定します。 `vserver cifs options modify -vserver vserver_name -restrict-anonymous {no-restriction|no-enumeration|no-access}`
3. オプションが目的の値に設定されていることを確認します。 `vserver cifs options show -vserver vserver_name`
4. **admin** 権限レベルに戻ります。 `set -privilege admin`

## 関連情報

### 使用できる SMB サーバオプション

**UNIX** セキュリティ形式のデータに対するファイルセキュリティの **SMB** クライアントへの提供方法を管理します

**UNIX** セキュリティ形式のデータの概要で、ファイルセキュリティが **SMB** クライアントにどのように提供されるかを管理します

SMB クライアントへの NTFS ACL の提供を有効または無効にすることによって、UNIX セキュリティ形式のデータに対するファイルセキュリティの SMB クライアントへの提供方法を選択できます。それぞれの設定には利点があり、ビジネス要件に最適な設定を選択するために理解しておく必要があります。

デフォルトでは、ONTAP は、UNIX セキュリティ形式のボリュームに対する UNIX アクセス権を NTFS ACL として SMB クライアントに提供します。これは次のような場合に適しています。

- Windows の [ プロパティ ] ボックスの [ セキュリティ \* ] タブを使用して、UNIX アクセス権を表示および編集する。

処理が UNIX システムで許可されていない場合、Windows クライアントからアクセス権を変更することはできません。たとえば、所有していないファイルの所有権を変更することはできません。これは、UNIX システムではこの処理が許可されていないためです。この制限により、SMB クライアントは、ファイルやフォルダに対して設定された UNIX アクセス権をバイパスできないようになっています。

- ユーザは、Microsoft Office などの特定の Windows アプリケーションを使用して UNIX セキュリティ形式のボリューム上でファイルを編集および保存します。ONTAP では、保存処理中に UNIX アクセス権を保持する必要があります。
- 使用するファイルの NTFS ACL を読み取ることを想定した特定の Windows アプリケーションが環境にある場合。

状況によっては、NTFS ACL としての UNIX アクセス権の提供を無効にすることもできます。この機能を無効にすると、ONTAP は UNIX セキュリティ形式のボリュームを FAT ボリュームとして SMB クライアントに提供します。UNIX セキュリティ形式のボリュームを FAT ボリュームとして SMB クライアントに提供するのは、次のような場合です。

- UNIX アクセス権の変更は、マウントを使用して UNIX クライアントでのみ行うことができます。

SMB クライアントで UNIX セキュリティ形式のボリュームがマッピングされている場合は、Security タブを使用できません。マッピングされたドライブは、ファイル権限がない FAT ファイルシステムでフォーマットされたドライブとして表示されます。

- SMB を使用するアプリケーションでアクセスするファイルやフォルダに NTFS ACL を設定しており、データが UNIX セキュリティ形式のボリュームにあると失敗する可能性がある場合。

ONTAP がボリュームを FAT として報告する場合、アプリケーションは ACL の変更を試みません。

## 関連情報

[FlexVol でのセキュリティ形式の設定](#)

[qtree でのセキュリティ形式の設定](#)

**UNIX セキュリティ形式のデータに対する NTFS ACL の提供を有効または無効にします**

UNIX セキュリティ形式のデータ（UNIX セキュリティ形式のボリュームと UNIX 対応のセキュリティを使用する mixed セキュリティ形式のボリューム）に対する NTFS ACL の SMB クライアントへの提供を有効または無効にできます。

## このタスクについて

このオプションを有効にすると、ONTAP は、UNIX 対応のセキュリティ形式を使用するボリュームのファイルおよびフォルダを NTFS ACL を使用するように SMB クライアントに提供します。このオプションを無効にした場合は、ボリュームが SMB クライアントに FAT ボリュームとして提供されます。デフォルトでは、NTFS ACL が SMB クライアントに提供されます。

## 手順

1. 権限レベルを advanced に設定します。 `set -privilege advanced`
2. UNIX NTFS ACL オプションを設定します。 `vserver cifs options modify -vserver vserver_name -is-unix-nt-acl-enabled {true|false}`
3. オプションが目的の値に設定されていることを確認します。 `vserver cifs options show -vserver vserver_name`
4. admin 権限レベルに戻ります。 `set -privilege admin`

## ONTAP による UNIX アクセス権の維持方法

UNIX アクセス権を現在持っている FlexVol ボリューム内のファイルが Windows アプリケーションによって編集および保存されても、ONTAP は UNIX アクセス権を維持できます。

Windows クライアントのアプリケーションは、ファイルを編集して保存するときに、ファイルのセキュリティプロパティを読み取り、新しい一時ファイルを作成し、それらのプロパティを一時ファイルに適用してから、一時ファイルに元のファイル名を付けます。

セキュリティプロパティのクエリを実行すると、Windows クライアントは、UNIX アクセス権を正確に表す構築済み ACL を受け取ります。この構築済み ACL は、Windows アプリケーションによってファイルが更新されるときにファイルの UNIX アクセス権を維持し、生成されたファイルが同じ UNIX アクセス権を持つようにするためだけに使用されます。ONTAP は、構築済み ACL を使用して NTFS ACL を設定しません。

**Windows** のセキュリティタブを使用して **UNIX** アクセス権を管理します

SVM 上の mixed セキュリティ形式のボリュームまたは qtree に含まれるファイルまたはフォルダの UNIX アクセス権を操作する場合は、Windows クライアントのセキュリティタブを使用できます。また、Windows ACL を照会および設定できるアプリケーションを使用することもできます。

- UNIX アクセス権の変更

Windows のセキュリティタブを使用して、mixed セキュリティ形式のボリュームまたは qtree の UNIX アクセス権を表示および変更できます。メインの [Windows Security] タブを使用して UNIX アクセス権を変更する場合は、編集する既存の ACE を削除してから（モードビットを 0 に設定）、変更を行う必要があります。または、高度なエディタを使用して権限を変更することもできます。

モードのアクセス権を使用している場合は、リストされた UID、GID、およびその他（コンピュータにアカウントを持つその他すべてのユーザ）のモードアクセス権を直接変更できます。たとえば、表示された UID に r-x のアクセス権が設定されている場合、この UID のアクセス権を rwx に変更できます。

- UNIX アクセス権を NTFS アクセス権に変更しています

Windows のセキュリティタブを使用して、ファイルおよびフォルダのセキュリティ形式が UNIX 対応である mixed 型セキュリティ形式のボリュームまたは qtree 上で、UNIX セキュリティオブジェクトを Windows セキュリティオブジェクトに置き換えることができます。

適切な Windows のユーザおよびグループのオブジェクトに置き換える前に、リストされている UNIX アクセス権のエントリをすべて削除しておく必要があります。次に、Windows のユーザおよびグループのオブジェクトに NTFS ベースの ACL を設定します。すべての UNIX セキュリティオブジェクトを削除し、Windows のユーザおよびグループのみを mixed セキュリティ形式のボリュームまたは qtree 上のファイルまたはフォルダに追加すると、ファイルまたはフォルダのセキュリティ形式が UNIX から NTFS へ変換されます。

フォルダの権限を変更する場合、Windows のデフォルトの動作では、すべてのサブフォルダとファイルにこれらの変更が反映されます。したがって、セキュリティ形式の変更をすべての子フォルダ、サブフォルダ、およびファイルに反映したくない場合は、反映する範囲を希望の範囲に変更する必要があります。

## **SMB** サーバのセキュリティ設定を管理します

### **ONTAP** による **SMB** クライアント認証の処理

SMB接続を確立してSVMに格納されているデータにアクセスする前に、ユーザはSMBサーバが属しているドメインで認証される必要があります。SMBサーバでは、Kerberos とNTLM（NTLMv1またはNTLMv2）の2つの認証方式がサポートされます。ドメインユーザの認証に使用されるデフォルトの方法は Kerberos です。

### **Kerberos** 認証

ONTAP は、許可された SMB セッションの作成時に Kerberos 認証をサポートします。

Kerberos は Active Directory のプライマリ認証サービスです。Kerberos サーバの Kerberos Key Distribution Center（KDC；キー配布センター）サービスは、Active Directory に対してセキュリティプリンシパルに関する情報の格納や取得を行います。NTLM モデルとは異なり、SMB サーバなどの別のコンピュータとのセッ

セッションを確立する Active Directory クライアントは、直接 KDC にアクセスしてセッションのクレデンシャルを取得します。

NTLM認証

NTLM クライアント認証は、パスワードに基づくユーザ固有のシークレットを共有し、チャレンジ - 応答プロトコルを使用して行われます。

ユーザがローカルのWindowsユーザアカウントを使用してSMB接続を作成した場合、認証はSMBサーバによってNTLMv2を使用してローカルに行われます。

SVM ディザスタリカバリ構成での SMB サーバセキュリティ設定に関するガイドライン

IDが保持されないディザスタリカバリデスティネーションとして設定されたSVMを作成する前に（を参照） `-identity-preserve` オプションはに設定されています `false`（SnapMirror構成の場合）デスティネーションSVMでのSMBサーバセキュリティ設定の管理方法について理解しておく必要があります。

- デフォルト以外の SMB サーバセキュリティ設定はデスティネーションにレプリケートされません。

デスティネーション SVM 上に SMB サーバを作成した場合、すべての SMB サーバセキュリティ設定はデフォルト値に設定されます。SVM のディザスタリカバリ先を初期化、更新、再同期した場合、ソース上の SMB サーバのセキュリティ設定はデスティネーションにレプリケートされません。

- デフォルト以外の SMB サーバセキュリティ設定は手動で設定する必要があります。

ソース SVM 上で SMB サーバセキュリティ設定をデフォルト以外にしている場合、デスティネーションが読み書き可能になったあと（SnapMirror 関係が解除されたあと）にデスティネーション SVM 上で手動で同じ設定を行う必要があります。

SMBサーバのセキュリティ設定に関する情報を表示する

Storage Virtual Machine（SVM）上の SMB サーバセキュリティ設定に関する情報を表示できます。この情報は、セキュリティ設定が正しいかどうかを確認する際に役立ちます。

このタスクについて

表示されるセキュリティ設定は、そのオブジェクトのデフォルト値か、ONTAP CLI または Active Directory グループポリシーオブジェクト（GPO）を使用して設定されたデフォルト以外の値です。

を使用しないでください `vserver cifs security show` 一部のオプションが無効なため、ワークグループモードのSMBサーバに対してコマンドを実行します。

ステップ

- 次のいずれかを実行します。

表示する情報	入力するコマンド
指定した SVM のすべてのセキュリティ設定	<code>vserver cifs security show -vserver vserver_name</code>

表示する情報	入力するコマンド
SVM の特定のセキュリティ設定	<code>vserver cifs security show -vserver <u>vserver_name</u> -fields [fieldname,...]</code> 入ることができます -fields ? 使用できるフィールドを決定します。

例

次の例は、SVM vs1 のすべてのセキュリティ設定を表示します。

```
cluster1::> vserver cifs security show -vserver vs1

Vserver: vs1

                Kerberos Clock Skew:           5 minutes
                Kerberos Ticket Age:            10 hours
                Kerberos Renewal Age:            7 days
                Kerberos KDC Timeout:           3 seconds
                Is Signing Required:            false
                Is Password Complexity Required: true
                Use start_tls For AD LDAP connection: false
                Is AES Encryption Enabled:       false
                LM Compatibility Level:          lm-ntlm-ntlmv2-krb
                Is SMB Encryption Required:      false
                Client Session Security:         none
                SMB1 Enabled for DC Connections: false
                SMB2 Enabled for DC Connections: system-default
                LDAP Referral Enabled For AD LDAP connections: false
                Use LDAPS for AD LDAP connection: false
                Encryption is required for DC Connections: false
                AES session key enabled for NetLogon channel: false
                Try Channel Binding For AD LDAP Connections: false
```

表示される設定は、実行中の ONTAP のバージョンによって異なります。

次の例は、SVM vs1 の Kerberos のクロックスキューを表示します。

```
cluster1::> vserver cifs security show -vserver vs1 -fields kerberos-
clock-skew


                vserver kerberos-clock-skew
                -----
                vs1      5
```

ローカル **SMB** ユーザに対するパスワードの複雑さの要件を有効または無効にします

パスワードの複雑さの要件を有効にすると、Storage Virtual Machine（SVM）上のローカル SMB ユーザに対するセキュリティを強化できます。パスワードの複雑さの要件はデフォルトでは有効になっています。この機能は、いつでも無効にして再度有効にすることができます。

作業を開始する前に

CIFS サーバでローカルユーザ、ローカルグループ、およびローカルユーザ認証が有効になっている必要があります。



このタスクについて

を使用しないでください `vserver cifs security modify` 一部のオプションが無効なため、ワークグループモードのCIFSサーバに対してコマンドを実行します。

手順

- 1. 次のいずれかを実行します。

ローカル <b>SMB</b> ユーザに対するパスワードの複雑さの要件の設定	入力するコマンド
有効	<code>vserver cifs security modify -vserver vserver_name -is-password-complexity -required true</code>
無効	<code>vserver cifs security modify -vserver vserver_name -is-password-complexity -required false</code>

- 2. パスワードの複雑さの要件に関するセキュリティ設定を確認します。 `vserver cifs security show -vserver vserver_name`

例

次の例は、SVM vs1 のローカル SMB ユーザに対してパスワードの複雑さの要件を有効にします。

```
cluster1::> vserver cifs security modify -vserver vs1 -is-password
-complexity-required true

cluster1::> vserver cifs security show -vserver vs1 -fields is-password-
complexity-required
vserver is-password-complexity-required
-----
vs1      true
```



関連情報

[CIFS サーバのセキュリティ設定に関する情報を表示する](#)

[ローカルユーザおよびローカルグループを使用した認証と許可](#)

[ローカルユーザパスワードの要件](#)

[ローカルユーザのアカウントパスワードを変更しています](#)

**CIFS** サーバの **Kerberos** セキュリティ設定を変更します

Kerberos クロックスキュー時間の許容最大値、Kerberos チケットの有効期間、チケットの更新日の最大数など、CIFS サーバの Kerberos セキュリティ設定の一部を変更できます。

このタスクについて

を使用したCIFSサーバのKerberos設定の変更 `vserver cifs security modify` コマンドでは、で指定した単一のStorage Virtual Machine (SVM) の設定のみを変更できます `-vserver` パラメータActive Directory の Group Policy Object ( GPO ; グループポリシーオブジェクト) を使用すると、同一の Active Directory ドメインに属するクラスタ上の SVM すべてについて、Kerberos セキュリティ設定を集中管理できます。

手順

- 1. 次の操作を 1 つ以上実行します。

状況	入力するコマンド
Kerberosクロックスキューの許容最大時間を分（9.13.1以降）または秒（9.12.1以前）で指定します。	<pre>vserver cifs security modify -vserver vserver_name -kerberos-clock-skew integer_in_minutes</pre> <p>デフォルトの設定は 5 分です。</p>
Kerberos チケットの有効期間を時間で指定します。	<pre>vserver cifs security modify -vserver vserver_name -kerberos-ticket-age integer_in_hours</pre> <p>デフォルトの設定は 10 時間です。</p>
チケットの更新日の最大数を指定します。	<pre>vserver cifs security modify -vserver vserver_name -kerberos-renew-age integer_in_days</pre> <p>デフォルトの設定は 7 日です。</p>
KDC のソケットのタイムアウトを指定します。この時間を過ぎるとすべての KDC が到達不能とマークされます。	<pre>vserver cifs security modify -vserver vserver_name -kerberos-kdc-timeout integer_in_seconds</pre> <p>デフォルトの設定は 3 秒です。</p>

## 2. Kerberos セキュリティ設定を確認します。

```
vserver cifs security show -vserver vserver_name
```

### 例

次の例では、SVM vs1 の Kerberos セキュリティ設定を「Kerberos Clock Skew」に 3 分、「Kerberos Ticket Age」に 8 時間に変更しています。

```
cluster1::> vserver cifs security modify -vserver vs1 -kerberos-clock-skew
3 -kerberos-ticket-age 8

cluster1::> vserver cifs security show -vserver vs1

Vserver: vs1

                Kerberos Clock Skew:                3 minutes
                Kerberos Ticket Age:                  8 hours
                Kerberos Renewal Age:                  7 days
                Kerberos KDC Timeout:                  3 seconds
                Is Signing Required:                   false
                Is Password Complexity Required:       true
                Use start_tls For AD LDAP connection:  false
                Is AES Encryption Enabled:             false
                LM Compatibility Level: lm-ntlm-ntlmv2-krb
                Is SMB Encryption Required:            false
```

### 関連情報

["CIFS サーバのセキュリティ設定に関する情報を表示する"](#)

["サポートされる GPO"](#)

["CIFS サーバへのグループポリシーオブジェクトの適用"](#)

**SMBサーバの最小認証セキュリティレベルを設定する**

SMB サーバの *LMCompatibilityLevel* と呼ばれる SMB サーバの最小セキュリティレベルを設定することで、SMB クライアントアクセスのビジネスセキュリティ要件を満たすことができます。最小セキュリティレベルは、SMBサーバによって許可されるSMBクライアントからのセキュリティトークンの最小レベルです。



#### このタスクについて

- ワークグループモードのSMBサーバでは、NTLM認証のみがサポートされます。Kerberos 認証はサポートされません。
- LMCompatibilityLevel は SMB クライアント認証にのみ適用され、admin 認証には適用されません。

最低限の認証セキュリティレベルは、サポートされている 4 つのセキュリティレベルのうちの 1 つに設定することができます。

価値	説明
lm-ntlm-ntlmv2-krb（デフォルト）	Storage Virtual Machine（SVM）は、LM、NTLM、NTLMv2、Kerberos 認証セキュリティを許可します。
ntlm-ntlmv2-krb	SVM は、NTLM、NTLMv2、Kerberos 認証セキュリティを許可します。SVM は LM 認証を拒否します。
ntlmv2-krb	SVM は、NTLMv2 と Kerberos 認証セキュリティを許可します。SVM は LM と NTLM 認証を拒否します。
krb	SVM は、Kerberos 認証セキュリティのみを許可します。SVM は LM、NTLM、NTLMv2 認証を拒否します。

#### 手順

1. 最小認証セキュリティレベルを設定します。 `vserver cifs security modify -vserver vserver_name -lm-compatibility-level {lm-ntlm-ntlmv2-krb|ntlm-ntlmv2-krb|ntlmv2-krb|krb}`
2. 認証セキュリティレベルが目的のレベルに設定されていることを確認します。 `vserver cifs security show -vserver vserver_name`

#### 関連情報

[Kerberos ベースの通信用の AES 暗号化を有効または無効にします](#)

**AES** 暗号化を使用して **Kerberos** ベースの通信のセキュリティを強化できます

Kerberos ベースの通信による最も強固なセキュリティを実現するために、AES-256 暗号化と AES-128 暗号化を SMB サーバで有効にすることができます。デフォルトでは、SVMでのSMBサーバの作成時にAdvanced Encryption Standard（AES）暗号化は無効になっています。AES暗号化が提供する強固なセキュリティを活用するには、AES暗号化を有効にする必要があります。

SMB の Kerberos 関連の通信は、SVM で SMB サーバを作成する際や、SMB セッションの設定フェーズで使用されます。SMB サーバでは、Kerberos 通信で次の暗号化タイプがサポートされます。

- AES 256
- AES 128
- DES（デス
- RC4-HMAC

Kerberos 通信で最高のセキュリティを持つ暗号化タイプを使用する場合は、SVM の Kerberos 通信で AES

暗号化を有効にする必要があります。

SMB サーバを作成すると、ドメインコントローラによって Active Directory にコンピュータマシンアカウントが作成されます。この時点で、KDC は特定のマシンアカウントの暗号化機能を認識するようになります。その後、認証時にクライアントがサーバに提示するサービスチケットを暗号化するために、特定の暗号化タイプが選択されます。

ONTAP 9.12.1以降では、Active Directory (AD) KDCにアドバタイズする暗号化タイプを指定できます。を使用できます `-advertised-enc-types` 推奨される暗号化タイプを有効にするオプション。また、弱い暗号化タイプを無効にする場合にも使用できます。方法をご確認ください ["Kerberosベースの通信の暗号化タイプを有効または無効にします"](#)。



SMB 3.0 で利用可能な Intel AES New Instructions (Intel AES NI) は AES アルゴリズムの改良版で、サポート対象のプロセッサファミリーでのデータ暗号化処理を高速化します。SMB 3.1.1 以降では、SMB 暗号化で使用されるハッシュアルゴリズムとして AES-128-CCM に代わって AES-128-GCM が使用されます。

関連情報

[CIFS サーバの Kerberos セキュリティ設定の変更](#)

**Kerberos ベースの通信用の AES 暗号化を有効または無効にします**

Kerberosベースの通信で最も強力なセキュリティを活用するには、SMBサーバでAES-256暗号化とAES-128暗号化を使用する必要があります。ONTAP 9.13.1以降では、AES暗号化がデフォルトで有効になります。Active Directory (AD) KDC との Kerberos ベースの通信に AES 暗号化タイプを SMB サーバで選択したくない場合は、AES 暗号化を無効にすることができます。

AES暗号化がデフォルトで有効になっているかどうか、および暗号化タイプを指定できるかどうかは、ONTAPのバージョンによって異なります。

ONTAPバージョン	AES暗号化が有効になっている...	暗号化タイプを指定できますか。
9.13.1以降	デフォルトでは	はい。
9.12.1:	手動で実行する	はい。
9.11.1以前	手動で実行する	いいえ

ONTAP 9.12.1以降では、を使用してAES暗号化を有効または無効にします `-advertised-enc-types` オプション。AD KDCにアドバタイズする暗号化タイプを指定できます。デフォルト設定は `rc4` および `des`、ただし、AESタイプを指定すると、AES暗号化が有効になります。オプションを使用して、弱いRC4暗号化タイプとDES暗号化タイプを明示的に無効にすることもできます。ONTAP 9.11.1以前では、`-is-aes-encryption-enabled` AES暗号化を有効または無効にするオプションを指定できません。また、暗号化タイプは指定できません。

セキュリティを強化するため、Storage Virtual Machine (SVM) は AES セキュリティオプションが変更されるたびに、AD 内のマシンアカウントのパスワードを変更します。パスワードの変更には、マシンアカウントが含まれる組織単位 (OU) の管理 AD クレデンシャルが必要になることがあります。

IDが保持されないディザスタリカバリデステーションとしてSVMが設定されている場合 (`-identity-preserve` オプションはに設定されています `false` SnapMirrorの設定では、デフォルト以外のSMBサーバ

セキュリティ設定はデスティネーションにレプリケートされません。ソースSVMでAES暗号化を有効にした場合は、AES暗号化を手動で有効にする必要があります。

**ONTAP 9.12.1以降**

1. 次のいずれかを実行します。

Kerberos 通信の AES 暗号化タイプの設定	入力するコマンド
有効	<pre>vserver cifs security modify -vserver vserver_name -advertised -enc-types aes-128,aes-256</pre>
無効	<pre>vserver cifs security modify -vserver vserver_name -advertised -enc-types des,rc4</pre>

注： `-is-aes-encryption-enabled` オプションはONTAP 9.12.1では廃止され、以降のリリースでは削除される可能性があります。

2. AES暗号化が設定どおり有効または無効になっていることを確認します。 `vserver cifs security show -vserver vserver_name -fields advertised-enc-types`

例

次の例は、SVM vs1のSMBサーバでAES暗号化タイプを有効にします。

```
cluster1::> vserver cifs security modify -vserver vs1 -advertised-enc
-types aes-128,aes-256

cluster1::> vserver cifs security show -vserver vs1 -fields advertised-
enc-types

vserver   advertised-enc-types
-----
vs1       aes-128,aes-256
```

次の例は、SVM vs2のSMBサーバでAES暗号化タイプを有効にします。管理者は、SMB サーバを含む OU の管理 AD クレデンシャルを入力するように求められます。

```
cluster1::> vsriver cifs security modify -vsriver vs2 -advertised-enc
-types aes-128,aes-256
```

Info: In order to enable SMB AES encryption, the password for the SMB server machine account must be reset. Enter the username and password for the SMB domain "EXAMPLE.COM".

Enter your user ID: administrator

Enter your password:

```
cluster1::> vsriver cifs security show -vsriver vs2 -fields advertised-
enc-types
```

```
vsriver  advertised-enc-types
-----  -----
vs2      aes-128,aes-256
```

## ONTAP 9.11.1以前

1. 次のいずれかを実行します。

Kerberos 通信の AES 暗号化タイプの設定	入力するコマンド
有効	<pre>vsriver cifs security modify -vsriver vsriver_name -is-aes -encryption-enabled true</pre>
無効	<pre>vsriver cifs security modify -vsriver vsriver_name -is-aes -encryption-enabled false</pre>

2. AES暗号化が設定どおり有効または無効になっていることを確認します。 `vsriver cifs security show -vsriver vsriver_name -fields is-aes-encryption-enabled`

。 `is-aes-encryption-enabled` フィールドが表示されます `true` AES暗号化が有効になっている場合と `false` 無効になっている場合。

## 例

次の例は、SVM vs1のSMBサーバでAES暗号化タイプを有効にします。

```
cluster1::> vserver cifs security modify -vserver vs1 -is-aes
-encryption-enabled true

cluster1::> vserver cifs security show -vserver vs1 -fields is-aes-
encryption-enabled

vserver  is-aes-encryption-enabled
-----
vs1      true
```

次の例は、SVM vs2のSMBサーバでAES暗号化タイプを有効にします。管理者は、SMB サーバを含む OU の管理 AD クレデンシャルを入力するように求められます。

```
cluster1::> vserver cifs security modify -vserver vs2 -is-aes
-encryption-enabled true

Info: In order to enable SMB AES encryption, the password for the CIFS
server
machine account must be reset. Enter the username and password for the
SMB domain "EXAMPLE.COM".

Enter your user ID: administrator

Enter your password:

cluster1::> vserver cifs security show -vserver vs2 -fields is-aes-
encryption-enabled

vserver  is-aes-encryption-enabled
-----
vs2      true
```

**SMB** 署名を使用してネットワークのセキュリティを強化します

**SMB** 署名を使用してネットワークセキュリティの概要を強化します

SMB 署名は、リプレイアタックを防止することで、SMB サーバとクライアント間のネットワークトラフィックが危険にさらされることのないようにします。デフォルト ONTAP では、クライアントから要求されたときに SMB 署名がサポートされます。ストレージ管理者は、必要に応じて、SMB 署名を必須にするように SMB サーバを設定できます。



## SMB 署名ポリシーが CIFS サーバとの通信に与える影響

CIFS サーバの SMB 署名セキュリティ設定に加えて、クライアントと CIFS サーバ間の通信のデジタル署名を制御する Windows クライアント上の SMB 署名ポリシーが 2 つあります。ビジネス要件に合わせて設定を行うことができます。

クライアント SMB ポリシーは、Microsoft 管理コンソール（MMC）または Active Directory の GPO を使用して設定した Windows ローカルセキュリティポリシー設定で制御されます。クライアントの SMB 署名とセキュリティ問題の詳細については、Microsoft Windows のマニュアルを参照してください。

ここでは、Microsoft クライアントの 2 つの SMB 署名ポリシーについて説明します。

- Microsoft network client: Digitally sign communications (if server agrees)

この設定は、クライアントの SMB 署名機能を有効にするかどうかを制御します。デフォルトでは有効になっています。この設定をクライアントで無効にすると、クライアントの CIFS サーバとの通信は、CIFS サーバ上の SMB 署名の設定によって異なります。

- Microsoft network client: Digitally sign communications (always)

この設定は、クライアントがサーバとの通信に SMB 署名を必要とするかどうかを制御します。デフォルトでは無効になっています。この設定がクライアントで無効になっている場合、SMB 署名の動作はのポリシー設定に基づきます Microsoft network client: Digitally sign communications (if server agrees) および CIFS サーバの設定。



ご使用の環境に、SMB 署名を必要とするように設定された Windows クライアントが含まれる場合、CIFS サーバ上の SMB 署名を有効にする必要があります。有効にしないと、CIFS サーバはこれらのシステムにデータを提供できません。

クライアントと CIFS サーバの SMB 署名設定の有効な結果は、SMB セッションで SMB 1.0 が使用されるか SMB 2.x 以降が使用されるかによって異なります。

次の表に、セッションで SMB 1.0 が使用される場合の有効な SMB 署名の動作を示します。

クライアント	ONTAP — 署名は不要	ONTAP — 署名が必要
署名は無効になっており、不要です	署名されません	署名
署名が有効になっており、不要である	署名されません	署名
署名が無効になっており、必要です	署名	署名
署名が有効になっており、必要です	署名	署名



古いバージョンの Windows の SMB 1 クライアントや一部の Windows 以外の SMB 1 クライアントでは、署名がクライアントでは無効になっていて CIFS サーバでは必要な場合、接続に失敗することがあります。

次の表に、セッションで SMB 2.x または SMB 3.0 が使用される場合の有効な SMB 署名の動作を示します。



SMB 2.x クライアントと SMB 3.0 クライアントでは、SMB 署名は常に有効になります。無効にすることはできません。

クライアント	ONTAP — 署名は不要	ONTAP — 署名が必要
署名は不要です	署名されません	署名
署名が必要です	署名	署名

次の表に、Microsoft クライアントおよびサーバの SMB 署名のデフォルト動作を示します。

プロトコル	ハッシュアルゴリズム	有効 / 無効を切り替えられます	必須 / 不要	クライアントのデフォルト	サーバのデフォルト	DC のデフォルト
SMB 1.0	MD5	はい。	はい。	有効（不要）	無効（不要）	必須
SMB 2.x	HMAC SHA-256	いいえ	はい。	必要ありません	必要ありません	必須
SMB 3.0	AES-CMAC :	いいえ	はい。	必要ありません	必要ありません	必須



Microsoftではの使用を推奨していません Digitally sign communications (if client agrees) または Digitally sign communications (if server agrees) グループポリシーの設定。Microsoftでは、の使用も推奨していません EnableSecuritySignature レジストリ設定。これらのオプションはSMB 1の動作にのみ影響し、で置き換えることができます Digitally sign communications (always) グループポリシー設定または RequireSecuritySignature レジストリ設定。詳細については、Microsoftのブログを参照してください。 <http://blogs.technet.com/b/josebda/archive/2010/12/01/the-basics-of-smb-signing-covering-both-smb1-and-smb2.aspx>[The SMB署名の基礎（SMB1とSMB2の両方をカバー）]

## SMB 署名のパフォーマンスへの影響

SMB セッションで SMB 署名を使用すると、Windows クライアントとのすべての SMB 通信でパフォーマンスが低下し、クライアントとサーバ（SMB サーバを含む SVM を実行しているクラスタ上のノード）の両方に影響します。

パフォーマンスへの影響は、CPU 使用率の増加としてクライアントとサーバの両方に表示されますが、ネットワークトラフィックの量は変わりません。

パフォーマンスへの影響の程度は、実行している ONTAP 9 のバージョンによって異なります。ONTAP 9.7 以降では、新しい暗号化のオフロードアルゴリズムによって、署名済み SMB トラフィックのパフォーマンスが向上します。SMB 署名オフロードは、SMB 署名が有効になっている場合にデフォルトで有効になります。

SMB 署名のパフォーマンスを向上させるには、AES-NI オフロード機能が必要です。お使いのプラットフォームで AES-NI オフロードがサポートされていることを確認するには、Hardware Universe（HWU）を参照してください。

はるかに高速なGCMアルゴリズムをサポートするSMBバージョン3.11を使用できる場合は、さらにパフォーマンスが向上します。

ネットワーク、ONTAP 9 のバージョン、SMB のバージョン、および SVM の実装方法に応じて SMB 署名のパフォーマンスへの影響には幅があるため、影響の程度はご使用のネットワーク環境でのテストによってのみ検証可能です。

ほとんどの Windows クライアントは、サーバで SMB 署名が有効になっている場合は、SMB 署名をデフォルトでネゴシエートします。一部の Windows クライアントで SMB 保護が必要で、SMB 署名がパフォーマンスの問題を引き起こしている場合は、リプレイアタックからの保護を必要としない Windows クライアントに対して SMB 署名を無効にすることができます。Windows クライアントでの SMB 署名の無効化については、Microsoft Windows のマニュアルを参照してください。

#### SMB 署名の設定に関する推奨事項

SMB クライアントと CIFS サーバの間の SMB 署名の動作は、セキュリティ要件に応じて設定することができます。CIFS サーバでの SMB 署名の設定は、セキュリティ要件の内容によって異なります。

SMB 署名は、クライアントと CIFS サーバのどちらでも設定できます。SMB 署名を設定する際の推奨事項を次に示します。

状況	推奨事項
クライアントとサーバの間の通信のセキュリティを強化する必要がある	を有効にして、クライアントでSMB署名を必須にします Require Option (Sign always) クライアントのセキュリティ設定。
特定の Storage Virtual Machine（SVM）へのすべての SMB トラフィックに署名する	セキュリティ設定で SMB 署名を必須にするように設定して、CIFS サーバで SMB 署名を必須にします。

Windows クライアントのセキュリティ設定の詳細については、Microsoft のマニュアルを参照してください。

#### 複数のデータ LIF が設定されている場合の SMB 署名に関するガイドライン

SMB サーバで SMB 署名要求を有効または無効にするときは、SVM に複数のデータ LIF が設定されている場合のガイドラインに注意する必要があります。

SMB サーバを設定する際に、複数のデータ LIF が設定されていることがあります。その場合、DNSサーバに複数のが含まれています A CIFSサーバのエントリを記録します。SMBサーバホスト名はすべて同じですが、IPアドレスはそれぞれ一意です。たとえば、2つのデータLIFが設定されているSMBサーバのDNSは次のようになります A レコードエントリ：

```
10.1.1.128 A VS1.IEPUB.LOCAL VS1
10.1.1.129 A VS1.IEPUB.LOCAL VS1
```

通常の動作では、SMB 署名要求の設定を変更すると、クライアントからの新しい接続だけが SMB 署名の設定変更の影響を受けます。ただし、この動作には例外があります。クライアントに共有への既存の接続がある場合、設定の変更後、クライアントは元の接続を維持しながら同じ共有への新しい接続を作成します。この場合、新規と既存の SMB 接続の両方で新しい SMB 署名の要件が適用されます。

次の例を考えてみましょう。

1. client1は、パスを使用してSMB署名を必要とせずに共有に接続します o:\。
2. ストレージ管理者が、SMB 署名を要求するように SMB サーバの設定を変更したとします。
3. client1は、パスを使用してSMB署名要求で同じ共有に接続します s:\ （パスを使用して接続を維持します o:\）。
4. その結果、両方でデータにアクセスするときにSMB署名が使用されます o:\ および s:\ ドライブ。

受信 **SMB** トラフィックの **SMB** 署名要求を有効または無効にします

SMB メッセージへのクライアントによる署名を強制するには、SMB 署名要求を有効にします。有効にすると、ONTAP は有効な署名のある SMB メッセージのみを受け入れます。SMB 署名を許可するが要求しない場合は、SMB 署名要求を無効にできます。

このタスクについて

デフォルトでは、SMB 署名要求は無効になっています。SMB 署名要求はいつでも有効または無効にできます。

次の状況では、SMB 署名はデフォルトで無効になりません。



1. SMB 署名要求が有効になっており、クラスタが SMB 署名をサポートしていないバージョンの ONTAP にリバートされた。
2. その後、クラスタが SMB 署名をサポートするバージョンの ONTAP にアップグレードされた。

このような場合は、サポートされているバージョンの ONTAP で最初に行われた SMB 署名の設定が、リバートとその後のアップグレードを通して維持されます。

Storage Virtual Machine (SVM) ディザスタリカバリ関係を設定する際にで選択した値 `-identity` `-preserve` のオプション `snapmirror create` コマンドは、デスティネーションSVMにレプリケートされる設定の詳細を決定します。

を設定した場合は `-identity-preserve` オプションをに設定します `true` (ID保持)。SMB署名のセキュリティ設定がデスティネーションにレプリケートされます。

を設定した場合は `-identity-preserve` オプションをに設定します `false` (ID保持なし)。SMB署名のセキュリティ設定はデスティネーションにレプリケートされません。この場合、デスティネーションの CIFS サーバセキュリティ設定はデフォルト値に設定されます。ソース SVM で SMB 署名要求を有効にしている場合は、デスティネーション SVM で SMB 署名要求を手動で有効にする必要があります。

## 手順

1. 次のいずれかを実行します。

SMB 署名要求の設定	入力するコマンド
有効	<code>vserver cifs security modify -vserver vserver_name -is-signing-required true</code>
無効	<code>vserver cifs security modify -vserver vserver_name -is-signing-required false</code>

2. での値を確認して、SMB署名要求が有効か無効かを確認します Is Signing Required 次のコマンドの出力のフィールドは、目的の値に設定されます。 `vserver cifs security show -vserver vserver_name -fields is-signing-required`

## 例

次の例は、SVM vs1 で SMB 署名要求を有効にします。

```
cluster1::> vserver cifs security modify -vserver vs1 -is-signing-required true

cluster1::> vserver cifs security show -vserver vs1 -fields is-signing-required
vserver  is-signing-required
-----
vs1      true
```



暗号化設定への変更は、新しい接続に対して有効になります。既存の接続は影響を受けません。

## SMB セッションが署名されているかどうかを確認します

CIFS サーバで接続中の SMB セッションに関する情報を表示できます。この情報を使用して、SMB セッションが署名されているかどうかを確認できます。これは、必要なセキュリティ設定を使用して SMB クライアントセッションが接続されているかどうかを確認する場合に役立ちます。

## 手順

1. 次のいずれかを実行します。

表示する情報	入力するコマンド
指定した Storage Virtual Machine (SVM) 上の署名されたすべてのセッション	<code>vserver cifs session show -vserver vserver_name -is-session-signed true</code>

表示する情報	入力するコマンド
SVM 上の指定したセッション ID を持つ署名されたセッションの詳細です	<code>vserver cifs session show -vserver <i>vserver_name</i> -session-id integer -instance</code>

## 例

次のコマンドを実行すると、SVM vs1 上の署名されたセッションに関するセッション情報が表示されます。デフォルトのサマリー出力には 'Is Session Signed' 出力フィールドは表示されません

```
cluster1::> vserver cifs session show -vserver vs1 -is-session-signed true
Node:      node1
Vserver:   vs1
Connection Session
ID          ID          Workstation      Windows User      Open      Idle
-----
3151272279  1          10.1.1.1        DOMAIN\joe        2         23s
```

次のコマンドを実行すると、セッション ID 2 の SMB セッションに関する、セッションが署名されているかどうかを含む詳細なセッション情報が表示されます。

```
cluster1::> vserver cifs session show -vserver vs1 -session-id 2 -instance
Node: node1
Vserver: vs1
Session ID: 2
Connection ID: 3151274158
Incoming Data LIF IP Address: 10.2.1.1
Workstation: 10.1.1.2
Authentication Mechanism: Kerberos
Windows User: DOMAIN\joe
UNIX User: pcuser
Open Shares: 1
Open Files: 1
Open Other: 0
Connected Time: 10m 43s
Idle Time: 1m 19s
Protocol Version: SMB3
Continuously Available: No
Is Session Signed: true
User Authenticated as: domain-user
NetBIOS Name: CIFS_ALIAS1
SMB Encryption Status: Unencrypted
```

## 関連情報

SMB 署名済みセッションの統計を監視します

SMB セッションの統計を監視し、確立されたセッションのうち、署名されたセッションと署名されていないセッションを区別できます。

このタスクについて

。 `statistics advanced` 権限レベルでコマンドを実行すると、が表示されます `signed_sessions` 署名済みSMBセッションの数を監視するために使用できるカウンタ。。 `signed_sessions` カウンタには、次の統計オブジェクトがあります。

- `cifs` すべてのSMBセッションについてSMB署名を監視できます。
- `smb1` SMB 1.0セッションのSMB署名を監視できます。
- `smb2` SMB 2.xセッションとSMB 3.0セッションのSMB署名を監視できます。

SMB 3.0の統計はの出力に表示されます `smb2` オブジェクト。

署名されたセッションの数をセッションの合計数と比較する場合は、の出力を比較できます `signed_sessions` の出力でカウンタに設定します `established_sessions` カウンタ。

データを取得して表示するには、統計サンプルの収集を開始する必要があります。データ収集を停止しなければ、サンプルからデータを表示できます。データ収集を停止すると、サンプルが固定された状態になります。データ収集を停止しないと、以前のクエリとの比較に使用できる更新されたデータを取得できます。この比較は、傾向を確認するのに役立ちます。

手順

1. 権限レベルを `advanced` に設定+  
`set -privilege advanced`
2. データ収集を開始します：+  
`statistics start -object {cifs|smb1|smb2} -instance instance -sample-id sample_ID [-node node_name]`

指定しない場合は、を実行します `-sample-id` パラメータを指定すると、サンプルIDが生成され、このサンプルがCLIセッションのデフォルトのサンプルとして定義されます。の値 `-sample-id` はテキスト文字列です。同じCLIセッションでこのコマンドを実行する場合に、を指定しないでください `-sample-id` パラメータを指定すると、前のデフォルトサンプルが上書きされます。

必要に応じて、統計を収集するノードを指定できます。ノードを指定しない場合、サンプルは、クラスタ内のすべてのノードについて統計情報を収集します。

3. を使用します `statistics stop` サンプルのデータ収集を停止するコマンド。
4. SMB 署名統計情報を表示します。

表示する情報	入力するコマンド
署名されたセッション	<code>`show -sample-id sample_ID -counter signed_sessions</code>

表示する情報	入力するコマンド
<code>node_name [-node node_name]</code>	署名されたセッションと確立されたセッション
<code>`show -sample-id sample_ID -counter signed_sessions</code>	<code>established_sessions</code>

単一のノードの情報のみを表示する場合は、オプションのを指定します `-node` パラメータ

5. admin権限レベルに戻ります。+  
`set -privilege admin`



次の例では、「vs1」という Storage Virtual Machine（SVM）について、SMB 2.x と SMB 3.0 のそれぞれの署名統計情報を監視する方法を示します。

次のコマンドは、advanced 権限レベルへの変更を行います。

```
cluster1::> set -privilege advanced
```

```
Warning: These advanced commands are potentially dangerous; use them  
only when directed to do so by support personnel.  
Do you want to continue? {y|n}: y
```

次のコマンドは、新しいサンプルのデータ収集を開始します。

```
cluster1::*> statistics start -object smb2 -sample-id smbsigning_sample  
-vserver vs1  
Statistics collection is being started for Sample-id: smbsigning_sample
```

次のコマンドは、サンプルのデータ収集を停止します。

```
cluster1::*> statistics stop -sample-id smbsigning_sample  
Statistics collection is being stopped for Sample-id: smbsigning_sample
```

次のコマンドは、ノードが署名した SMB セッションと確立されたセッションをサンプルから表示します。

```
cluster1::*> statistics show -sample-id smbSigning_sample -counter
signed_sessions|established_sessions|node_name
```

Object: smb2

Instance: vs1

Start-time: 2/6/2013 01:00:00

End-time: 2/6/2013 01:03:04

Cluster: cluster1

Counter	Value
-----	-----
established_sessions	0
node_name	node1
signed_sessions	0
established_sessions	1
node_name	node2
signed_sessions	1
established_sessions	0
node_name	node3
signed_sessions	0
established_sessions	0
node_name	node4
signed_sessions	0

次のコマンドでは、ノード 2 が署名した SMB セッションをサンプルから表示します。

```
cluster1::*> statistics show -sample-id smbSigning_sample -counter
signed_sessions|node_name -node node2
```

Object: smb2

Instance: vs1

Start-time: 2/6/2013 01:00:00

End-time: 2/6/2013 01:22:43

Cluster: cluster1

Counter	Value
-----	-----
node_name	node2
signed_sessions	1

次のコマンドは、admin 権限レベルに戻ります。

```
cluster1::*> set -privilege admin
```

SMB を介したデータ転送に必要な SMB 暗号化を SMB サーバで設定します

## SMB暗号化の概要

SMB を介したデータ転送での SMB 暗号化は、SMB サーバで有効化または無効化できるセキュリティ強化です。共有プロパティ設定を使用して共有ごとに必要な SMB 暗号化を設定することもできます。

デフォルトでは、Storage Virtual Machine (SVM) でのSMBサーバの作成時にSMB暗号化は無効になっています。SMB 暗号化が提供する高度なセキュリティを活用するには、SMB 暗号化を有効にする必要があります。

暗号化された SMB セッションを作成するには、SMB クライアントが SMB 暗号化をサポートしている必要があります。Windows Server 2012 および Windows 8 以降の Windows クライアントでは、SMB 暗号化がサポートされます。

SVM での SMB 暗号化は、次の 2 つの設定によって制御されます。

- SVMの機能を有効にするSMBサーバセキュリティオプション
- 共有ごとにSMB暗号化を設定するSMB共有プロパティ

SVM 上のすべてのデータへのアクセスに暗号化を要求するか、選択した共有のデータにアクセスする場合のみに SMB 暗号化を要求するかを決定できます。SVM レベルの設定は、共有レベルの設定よりも優先されます。

次の表に示す 2 つの設定の組み合わせを使用すると、効果的な SMB 暗号化設定を行うことができます。

SMB サーバ SMB 暗号化が有効	共有暗号化データ設定が有効です	サーバ側の暗号化の動作
正しいです	いいえ	SVM のすべての共有でサーバレベルの暗号化が有効です。この設定では、SMB セッション全体で暗号化が行われます。
正しいです	正しいです	共有レベルの暗号化には関係なく SVM のすべての共有でサーバレベルの暗号化が有効です。この設定では、SMB セッション全体で暗号化が行われます。
いいえ	正しいです	特定の共有で共有レベルの暗号化が有効です。この設定では、ツリー接続から暗号化が行われます。

<b>SMB サーバ SMB 暗号化が有効</b>	共有暗号化データ設定が有効です	サーバ側の暗号化の動作
いいえ	いいえ	暗号化は有効になっていません。

暗号化をサポートしていないSMBクライアントは、暗号化が必要なSMBサーバや共有には接続できません。

暗号化設定への変更は、新しい接続に対して有効になります。既存の接続は影響を受けません。

### SMB 暗号化のパフォーマンスへの影響

SMB セッションで SMB 暗号化を使用すると、Windows クライアントとのすべての SMB 通信でパフォーマンスが低下し、クライアントとサーバ（SMB サーバを含む SVM を実行しているクラスタ上のノード）の両方に影響します。

パフォーマンスへの影響は、CPU 使用率の増加としてクライアントとサーバの両方に表示されますが、ネットワークトラフィックの量は変わりません。

パフォーマンスへの影響の程度は、実行している ONTAP 9 のバージョンによって異なります。ONTAP 9.7 以降では、新しい暗号化のオフロードアルゴリズムによって、暗号化された SMB トラフィックのパフォーマンスが向上します。SMB 暗号化オフロードは、SMB 暗号化が有効になっている場合にデフォルトで有効になります。

SMB 暗号化のパフォーマンスを高めるには、AES-NI オフロード機能が必要です。お使いのプラットフォームで AES-NI オフロードがサポートされていることを確認するには、Hardware Universe（HWU）を参照してください。

はるかに高速なGCMアルゴリズムをサポートするSMBバージョン3.11を使用できる場合は、さらにパフォーマンスが向上します。

ネットワーク、ONTAP 9 のバージョン、SMB のバージョン、および SVM の実装方法に応じて SMB 暗号化のパフォーマンスへの影響には幅があるため、影響の程度はご使用のネットワーク環境でのテストによるのみ検証可能です。

SMB 暗号化は、SMB サーバではデフォルトで無効になっています。SMB 暗号化は、暗号化を必要とする SMB 共有または SMB サーバでのみ有効にしてください。SMB 暗号化を有効にすると、ONTAP はすべての要求に対して要求を復号化して応答を暗号化する必要があります。そのため、SMB 暗号化は必要な場合にのみ有効にしてください。

受信 **SMB** トラフィックの **SMB** 暗号化要求を有効または無効にします

受信 SMB トラフィックに SMB 暗号化を必須にする場合は、CIFS サーバ上または共有レベルで有効にすることができます。デフォルトでは、SMB 暗号化は必須ではありません。

このタスクについて

CIFS サーバ上で SMB 暗号化を有効にすることができます。この場合、CIFS サーバ上のすべての共有が環境によって暗号化されます。CIFS サーバ上のすべての共有で SMB 暗号化要求を有効にしない場合、または受信 SMB トラフィックの SMB 暗号化要求を共有ごとに有効にする場合は、CIFS サーバ上で SMB 暗号化要求を無効にすることができます。

Storage Virtual Machine (SVM) ディザスタリカバリ関係をセットアップするときには選択した値 `-identity-preserve` のオプション `snapmirror create` コマンドは、デスティネーションSVMにレプリケートされる設定の詳細を決定します。

を設定した場合は `-identity-preserve` オプションをに設定します `true` (ID保持) では、SMB暗号化のセキュリティ設定がデスティネーションにレプリケートされます。

を設定した場合は `-identity-preserve` オプションをに設定します `false` (ID保持なし)。SMB暗号化のセキュリティ設定はデスティネーションにレプリケートされません。この場合、デスティネーションの CIFS サーバセキュリティ設定はデフォルト値に設定されます。ソース SVM で SMB 暗号化を有効にしている場合は、デスティネーションで CIFS サーバの SMB 暗号化を手動で有効にする必要があります。

手順

- 1. 次のいずれかを実行します。

CIFS サーバでの受信 SMB トラフィックの SMB 暗号化要求の設定	入力するコマンド
有効	<code>vserver cifs security modify -vserver vserver_name -is-smb-encryption -required true</code>
無効	<code>vserver cifs security modify -vserver vserver_name -is-smb-encryption -required false</code>

- 2. CIFSサーバでのSMB暗号化要求が必要に応じて有効または無効になっていることを確認します。

```
vserver cifs security show -vserver vserver_name -fields is-smb-encryption-required
```

。 `is-smb-encryption-required` フィールドが表示されます `true` CIFSサーバおよびでSMB暗号化要求が有効になっている場合 `false` 無効になっている場合。

例

次の例は、SVM vs1 で CIFS サーバの受信 SMB トラフィックの SMB 暗号化要求を有効にします。

```
cluster1::> vserver cifs security modify -vserver vs1 -is-smb-encryption -required true

cluster1::> vserver cifs security show -vserver vs1 -fields is-smb-encryption-required
vserver  is-smb-encryption-required
-----  -----
vs1      true
```

クライアントが暗号化 **SMB** セッションを使用して接続しているかどうかを確認します

接続中の SMB セッションに関する情報を表示して、クライアントが暗号化された SMB 接続を使用しているかどうかを確認できます。これは、必要なセキュリティ設定を使用して SMB クライアントセッションが接続されているかどうかを確認する場合に役立ちます。

このタスクについて

SMB クライアントセッションには、次の 3 つのいずれかの暗号化レベルを設定できます。

- unencrypted

SMB セッションは暗号化されません。Storage Virtual Machine （SVM）レベルの暗号化も共有レベルの暗号化も設定されません。

- partially-encrypted

ツリー接続が行われると、暗号化が開始されます。共有レベルの暗号化が設定されています。SVM レベルの暗号化は有効になりません。

- encrypted

SMB セッションは完全に暗号化されます。SVM レベルの暗号化が有効です。共有レベルの暗号化は、有効になる場合とならない場合があります。SVM レベルの暗号化設定は、共有レベルの暗号化設定よりも優先されます。

手順

1. 次のいずれかを実行します。

表示する情報	入力するコマンド
指定した SVM のセッションで、指定した暗号化設定を使用するセッション	<code>`vserver cifs session show -vserver vserver_name {unencrypted</code>
partially-encrypted	<code>encrypted} -instance`</code>
指定した SVM の特定のセッション ID の暗号化設定	<code>vserver cifs session show -vserver vserver_name -session-id integer -instance</code>

例

次のコマンドを実行すると、セッション ID 2 の SMB セッションに関する、暗号化設定を含む詳細なセッション情報が表示されます。

```

cluster1::> vserver cifs session show -vserver vs1 -session-id 2 -instance
Node: node1
Vserver: vs1
Session ID: 2
Connection ID: 3151274158
Incoming Data LIF IP Address: 10.2.1.1
Workstation: 10.1.1.2
Authentication Mechanism: Kerberos
Windows User: DOMAIN\joe
UNIX User: pcuser
Open Shares: 1
Open Files: 1
Open Other: 0
Connected Time: 10m 43s
Idle Time: 1m 19s
Protocol Version: SMB3
Continuously Available: No
Is Session Signed: true
User Authenticated as: domain-user
NetBIOS Name: CIFS_ALIAS1
SMB Encryption Status: Unencrypted

```

## SMB 暗号化統計情報を監視する

SMB 暗号化の統計を監視し、確立されたセッションおよび共有接続のうち、暗号化されたものと暗号化されていないものを区別できます。

このタスクについて

。statistics advanced権限レベルでコマンドを実行すると次のカウンタが表示され、暗号化されたSMBセッションおよび共有接続の数を監視できます。

カウンタ名	説明
encrypted_sessions	暗号化された SMB 3.0 セッションの数
encrypted_share_connections	ツリー接続が行われた暗号化された共有の数
rejected_unencrypted_sessions	クライアントに暗号化機能がないために拒否されたセッションセットアップ数を示します
rejected_unencrypted_shares	クライアントに暗号化機能がないために拒否された共有マッピング数

これらのカウンタでは、次の統計オブジェクトを使用できます。

- `cifs` すべてのSMB 3.0セッションについてSMB暗号化を監視できます。

SMB 3.0の統計はの出力に表示されます `cifs` オブジェクト。暗号化されたセッションの数をセッションの合計数と比較する場合は、の出力を比較できます `encrypted_sessions` の出力でカウンタに設定します `established_sessions` カウンタ。

暗号化された共有接続数を共有接続の合計数と比較する場合は、の出力を比較します `encrypted_share_connections` の出力でカウンタに設定します `connected_shares` カウンタ。

- `rejected_unencrypted_sessions` SMB暗号化をサポートしていないクライアントから暗号化を必要とするSMBセッションの確立が試行された回数を示します。
- `rejected_unencrypted_shares` SMB暗号化をサポートしていないクライアントから暗号化が必要なSMB共有への接続が試行された回数を示します。

データを取得して表示するには、統計サンプルの収集を開始する必要があります。データ収集を停止しなければ、サンプルからデータを表示できます。データ収集を停止すると、サンプルが固定された状態になります。データ収集を停止しないと、以前のクエリとの比較に使用できる更新されたデータを取得できます。この比較は、傾向を確認するのに役立ちます。

#### 手順

1. 権限レベルをadvancedに設定+  
`set -privilege advanced`
2. データ収集を開始します：+  
`statistics start -object {cifs|smb1|smb2} -instance instance -sample-id sample_ID [-node node_name]`

指定しない場合は、を実行します `-sample-id` パラメータを指定すると、サンプルIDが生成され、このサンプルがCLIセッションのデフォルトのサンプルとして定義されます。の値 `-sample-id` はテキスト文字列です。同じCLIセッションでこのコマンドを実行する場合に、を指定しないでください `-sample-id` パラメータを指定すると、前のデフォルトサンプルが上書きされます。

必要に応じて、統計を収集するノードを指定できます。ノードを指定しない場合、サンプルは、クラスター内のすべてのノードについて統計情報を収集します。

3. を使用します `statistics stop` サンプルのデータ収集を停止するコマンド。
4. SMB 暗号化統計情報を表示します。

表示する情報	入力するコマンド
暗号化されたセッション	<code>`show -sample-id sample_ID -counter encrypted_sessions</code>
<code>node_name [-node node_name]`</code>	暗号化されたセッションと確立されたセッション
<code>`show -sample-id sample_ID -counter encrypted_sessions</code>	<code>established_sessions</code>
<code>node_name [-node node_name]`</code>	暗号化された共有接続



表示する情報	入力するコマンド
<code>`show -sample-id <i>sample_ID</i> -counter encrypted_share_connections</code>	<code><i>node_name</i> [-node <i>node_name</i>]</code>
暗号化された共有接続と接続された共有	<code>`show -sample-id <i>sample_ID</i> -counter encrypted_share_connections</code>
connected_shares	<code><i>node_name</i> [-node <i>node_name</i>]</code>
暗号化されていないセッションは	<code>`show -sample-id <i>sample_ID</i> -counter rejected_unencrypted_sessions</code>
<code><i>node_name</i> [-node <i>node_name</i>]</code>	拒否された暗号化されていない
<code>`show -sample-id <i>sample_ID</i> -counter rejected_unencrypted_share</code>	<code><i>node_name</i> [-node <i>node_name</i>]</code>

単一のノードの情報のみを表示する場合は、オプションのを指定します `-node` パラメータ

5. admin権限レベルに戻ります。+  
`set -privilege admin`

次の例は、「vs1」という Storage Virtual Machine（SVM）について、SMB 3.0 の暗号化統計情報を監視する方法を示します。

次のコマンドは、advanced 権限レベルへの変更を行います。

```
cluster1::> set -privilege advanced
```

```
Warning: These advanced commands are potentially dangerous; use them  
only when directed to do so by support personnel.  
Do you want to continue? {y|n}: y
```

次のコマンドは、新しいサンプルのデータ収集を開始します。

```
cluster1::*> statistics start -object cifs -sample-id  
smbencryption_sample -vserver vs1  
Statistics collection is being started for Sample-id:  
smbencryption_sample
```

次のコマンドは、サンプルのデータ収集を停止します。

```
cluster1::*> statistics stop -sample-id smbencryption_sample  
Statistics collection is being stopped for Sample-id:  
smbencryption_sample
```

次のコマンドは、指定したノードについて、暗号化された SMB セッション数と確立されたセッション数をサンプルから表示します。

```
cluster2::*> statistics show -object cifs -counter
established_sessions|encrypted_sessions|node_name -node node_name
```

Object: cifs

Instance: [proto\_ctx:003]

Start-time: 4/12/2016 11:17:45

End-time: 4/12/2016 11:21:45

Scope: vsim2

Counter	Value
established_sessions	1
encrypted_sessions	1

2 entries were displayed

次のコマンドは、指定したノードについて、拒否された暗号化されていない SMB セッション数をサンプルから表示します。

```
clus-2::*> statistics show -object cifs -counter
rejected_unencrypted_sessions -node node_name
```

Object: cifs

Instance: [proto\_ctx:003]

Start-time: 4/12/2016 11:17:45

End-time: 4/12/2016 11:21:51

Scope: vsim2

Counter	Value
rejected_unencrypted_sessions	1

1 entry was displayed.

次のコマンドは、指定したノードについて、接続された SMB 共有数と暗号化された SMB 共有数をサンプルから表示します。

```
clus-2::*> statistics show -object cifs -counter
connected_shares|encrypted_share_connections|node_name -node node_name
```

Object: cifs  
Instance: [proto\_ctx:003]  
Start-time: 4/12/2016 10:41:38  
End-time: 4/12/2016 10:41:43  
Scope: vsim2

Counter	Value
connected_shares	2
encrypted_share_connections	1

2 entries were displayed.

次のコマンドは、指定したノードについて、拒否された暗号化されていない SMB 共有接続数をサンプルから表示します。

```
clus-2::*> statistics show -object cifs -counter
rejected_unencrypted_shares -node node_name
```

Object: cifs  
Instance: [proto\_ctx:003]  
Start-time: 4/12/2016 10:41:38  
End-time: 4/12/2016 10:42:06  
Scope: vsim2

Counter	Value
rejected_unencrypted_shares	1

1 entry was displayed.

## 関連情報

[使用可能な統計オブジェクトと統計カウンタの確認](#)

["パフォーマンスの監視と管理の概要"](#)

セキュアな **LDAP** セッション通信

**LDAP** の署名と封印の概念

ONTAP 9 以降では、署名と封印を設定して、Active Directory（AD）サーバへの照会

に対する LDAP セッションセキュリティを有効にすることができます。Storage Virtual Machine (SVM) の CIFS サーバセキュリティ設定を LDAP サーバの設定に対応するように設定する必要があります。

署名は、シークレットキーのテクノロジーを使用して、LDAP ペイロードデータの整合性を確認します。封印は、LDAP ペイロードデータを暗号化して機密情報がクリアテキストで送信されないようにします。LDAP トラフィックについて、署名が必要か、署名と封印が必要か、どちらも必要ないかは、*ldap Security Level* オプションで指定します。デフォルトは `none`。

SVMでCIFSトラフィックに対するLDAPの署名と封印が `-session-security-for-ad-ldap` オプションに設定します `vserver cifs security modify` コマンドを実行します

### CIFS サーバで LDAP の署名と封印を有効にする

CIFS サーバで Active Directory LDAP サーバとのセキュアな通信に署名と封印を使用するためには、CIFS サーバのセキュリティ設定を変更して LDAP の署名と封印を有効にする必要があります。

作業を開始する前に

AD サーバ管理者に問い合わせて、適切なセキュリティ設定値を決定する必要があります。

手順

1. Active Directory LDAPサーバとのトラフィックの署名と封印を有効にするCIFSサーバのセキュリティ設定を行います。 `vserver cifs security modify -vserver vserver_name -session-security -for-ad-ldap {none|sign|seal}`

署名を有効にできます (sign、データ整合性)、署名と封印 (seal、データ整合性と暗号化)、またはどちらもない `none`、署名または封印なし)。デフォルト値は `none`。

2. LDAPの署名と封印のセキュリティ設定が正しく設定されていることを確認します。 `vserver cifs security show -vserver vserver_name`



SVMがネームマッピングやその他のUNIX情報（ユーザ、グループ、ネットグループなど）の照会に同じLDAPサーバを使用する場合は、で対応する設定を有効にする必要があります `-session-security` のオプション `vserver services name-service ldap client modify` コマンドを実行します

### LDAP over TLS を設定する

自己署名ルート CA 証明書のコピーをエクスポートします

Active Directory 通信の保護に LDAP over SSL/TLS を使用するには、まず Active Directory 証明書サービスの自己署名ルート CA 証明書のコピーを証明書ファイルにエクスポートし、それを ASCII テキストファイルに変換する必要があります。ONTAP は、このテキストファイルを使用して証明書を Storage Virtual Machine (SVM) にインストールします。

作業を開始する前に

Active Directory 証明書サービスがすでにインストールされ、CIFS サーバが属しているドメイン用に設定されている必要があります。Active Directory 証明書サービスのインストールと設定の詳細については、Microsoft TechNet ライブラリを参照してください。

"Microsoft TechNet ライブラリ : [technet.microsoft.com](https://technet.microsoft.com)"

#### ステップ

1. 内のドメインコントローラのルートCA証明書を取得します .pem テキスト形式。

"Microsoft TechNet ライブラリ : [technet.microsoft.com](https://technet.microsoft.com)"

#### 完了後

SVM に証明書をインストールします。

#### 関連情報

"Microsoft TechNet ライブラリ"

自己署名ルート **CA** 証明書を **SVM** にインストールします

LDAP サーバにバインドするときに TLS を使用した LDAP 認証が必要な場合は、まず自己署名ルート CA 証明書を SVM にインストールする必要があります。

#### このタスクについて

LDAP over TLS が有効な場合、SVM 上の ONTAP LDAP クライアントでは、ONTAP 9.0 および 9.1 の破棄された証明書はサポートされません。

ONTAP 9.2 以降では、TLS 通信を使用する ONTAP 内のすべてのアプリケーションで、Online Certificate Status Protocol (OCSP) を使用してデジタル証明書のステータスを確認できます。OCSP が LDAP over TLS に対して有効になっている場合、失効した証明書は拒否され、接続は失敗します。

#### 手順

1. 自己署名ルート CA 証明書をインストールします。
  - a. 証明書のインストールを開始します。 `security certificate install -vserver vservice_name -type server-ca`
  - コンソール出力に次のメッセージが表示されます。 Please enter Certificate: Press <Enter> when done
  - b. 証明書を開きます .pem ファイルテキストエディタを使用して、で始まる行を含めて証明書をコピーします -----BEGIN CERTIFICATE----- で終わる `-----END CERTIFICATE-----` をクリックし、コマンドプロンプトのあとに証明書を貼り付けます。
  - c. 証明書が正しく表示されることを確認します。
  - d. Enter キーを押してインストールを完了します。
2. 証明書がインストールされていることを確認します。 `security certificate show -vserver vservice_name`

サーバで **LDAP over TLS** を有効にします

SMBサーバでActive Directory LDAPサーバとのセキュアな通信にTLSを使用するには、SMBサーバのセキュリティ設定を変更してLDAP over TLSを有効にする必要があります。

ONTAP 9.10.1 以降では、Active Directory（AD）とネームサービスの両方の LDAP 接続で、LDAP チャネルバインドがデフォルトでサポートされます。ONTAP は、Start-TLS または LDAPS が有効で、セッションセキュリティが署名または封印に設定されている場合にのみ、LDAP 接続でチャネルバインドを試行します。ADサーバとのLDAPチャネルバインディングを無効または再度有効にするには、を使用します `-try -channel-binding-for-ad-ldap` パラメータと `vserver cifs security modify` コマンドを実行します

詳細については、以下を参照してください。

- ["LDAPの概要"](#)
- ["2020 年の Windows 向け LDAP チャネルバインドおよび LDAP 署名の要件"](#)。

手順

1. Active Directory LDAPサーバとのセキュアなLDAP通信を許可するSMBサーバのセキュリティ設定を行います。 `vserver cifs security modify -vserver vserver_name -use-start-tls-for-ad-ldap true`
2. LDAP over TLSのセキュリティ設定がに設定されていることを確認します `true` : `vserver cifs security show -vserver vserver_name`



SVMがネームマッピングやその他のUNIX情報（ユーザ、グループ、ネットグループなど）の照会に同じLDAPサーバを使用する場合は、も変更する必要があります `-use-start-tls` オプションを使用します `vserver services name-service ldap client modify` コマンドを実行します

パフォーマンスと冗長性を高めるために **SMB** マルチチャネルを設定します

ONTAP 9.4 以降では、SMB マルチチャネルを設定して、1つのSMBセッションでONTAPとクライアントの間に複数の接続を確立することができます。これにより、スループットとフォールトトレランスが向上します。

作業を開始する前に

SMB マルチチャネル機能は、クライアントがSMB 3.0 以降のバージョンでネゴシエートする場合にのみ使用できます。ONTAP SMB サーバでは、SMB 3.0 以降がデフォルトで有効になっています。

このタスクについて

SMB クライアントは、ONTAP クラスタで適切な設定が見つかり、複数のネットワーク接続を自動的に検出して使用します。

SMB セッションでの同時接続数は、導入しているNICによって異なります。

- \* クライアントおよびONTAP クラスタに 1G NIC を搭載 \*

クライアントから確立される接続数は NIC ごとに 1 つで、すべての接続にセッションがバインドされます。

- \* クライアントおよび ONTAP クラスタ上の 10G 以上の NIC \*

クライアントから確立される接続数は NIC ごとに最大 4 つで、すべての接続にセッションがバインドされます。クライアントは 10G 以上の複数の NIC で接続を確立できます。

また、次のパラメータを変更することもできます（advanced 権限）。

- **-max-connections-per-session**

各マルチチャネルセッションに許可される最大接続数。デフォルトの接続数は 32 です。

デフォルトよりも多くの接続を有効にする場合は、クライアントの設定に対して同等の調整を行う必要があります。これには、デフォルトの接続数は 32 です。

- **-max-lifs-per-session**

各マルチチャネルセッションで通知されるネットワークインターフェイスの最大数。デフォルトのネットワークインターフェイス数は 256 です。

#### 手順

1. 権限レベルを advanced に設定します。 `set -privilege advanced`
2. SMB サーバで SMB マルチチャネルを有効にします。 `vserver cifs options modify -vserver vserver_name -is-multichannel-enabled true`
3. ONTAP が SMB マルチチャネルセッションを報告していることを確認します。 `vserver cifs session show options`
4. admin 権限レベルに戻ります。 `set -privilege admin`

#### 例

次の例は、すべての SMB セッションに関する情報を表示します。1 つのセッションに対して複数の接続が表示されています。



```
cluster1::> vserver cifs session show
Node:    node1
Vserver: vs1
Connection Session                                Open
Idle
IDs      ID      Workstation      Windows User      Files
Time
-----
-----
138683,
138684,
138685    1      10.1.1.1      DOMAIN\
4s
Administrator
```

次の例は、セッション ID 1 が割り当てられた SMB セッションに関する詳細情報を表示します。

```
cluster1::> vserver cifs session show -session-id 1 -instance

Vserver: vs1

Node: node1
Session ID: 1
Connection IDs: 138683,138684,138685
Connection Count: 3
Incoming Data LIF IP Address: 192.1.1.1
Workstation IP Address: 10.1.1.1
Authentication Mechanism: NTLMv1
User Authenticated as: domain-user
Windows User: DOMAIN\administrator
UNIX User: root
Open Shares: 2
Open Files: 5
Open Other: 0
Connected Time: 5s
Idle Time: 5s
Protocol Version: SMB3
Continuously Available: No
Is Session Signed: false
NetBIOS Name: -
```

**SMB** サーバでのデフォルト **Windows** ユーザから **UNIX** ユーザへのマッピングを設定する

ユーザに対する他のマッピングの試行がすべて失敗した場合や、UNIX と Windows の間で個々のユーザをマッピングしないようにする場合に使用するデフォルトの UNIX ユーザを設定できます。ただし、マッピングされていないユーザの認証を失敗にする必要がある場合は、デフォルト UNIX ユーザを設定しないでください。

このタスクについて

デフォルトでは、デフォルト UNIX ユーザの名前は「pcuser」です。これは、デフォルトで、デフォルト UNIX ユーザへのユーザマッピングが有効になっていることを意味します。デフォルトの UNIX ユーザとして使用する別の名前を指定することもできます。指定する名前は、Storage Virtual Machine（SVM）用に設定されているネームサービスデータベース内に存在する必要があります。このオプションを null 文字列に設定すると、どのユーザも UNIX デフォルトユーザとして CIFS サーバにアクセスできません。つまり、CIFS サーバにアクセスするためには、各ユーザがパスワードデータベースにアカウントを持つ必要があります。

ユーザがデフォルトの UNIX ユーザアカウントを使用して CIFS サーバに接続するには、次の前提条件を満たす必要があります。

- ユーザが認証されていること。
- ユーザが、CIFS サーバのローカル Windows ユーザデータベース、CIFS サーバのホームドメイン、信頼できるドメイン（CIFS サーバでマルチドメインネームマッピング検索が有効な場合）のいずれかにあること
- ユーザ名が明示的に null 文字列にマッピングされることはありません。

手順

1. デフォルトの UNIX ユーザを設定します。

状況	入力するコマンド
デフォルトの UNIX ユーザ「pcuser」を使用する	<code>vserver cifs options modify -default -unix-user pcuser</code>
別の UNIX ユーザアカウントをデフォルトユーザとして使用します	<code>vserver cifs options modify -default -unix-user user_name</code>
デフォルトの UNIX ユーザを無効にします	<code>vserver cifs options modify -default -unix-user ""</code>

```
vserver cifs options modify -default-unix-user pcuser
```

2. デフォルトの UNIX ユーザが正しく設定されていることを確認します。 `vserver cifs options show -vserver vserver_name`

次の例では、SVM vs1 のデフォルト UNIX ユーザとゲスト UNIX ユーザの両方が UNIX ユーザ「pcuser」を使用するように設定されています。

```
vserver cifs options show -vserver vs1
```

```
Vserver: vs1

Client Session Timeout : 900
Default Unix Group      : -
Default Unix User       : pcuser
Guest Unix User         : pcuser
Read Grants Exec        : disabled
Read Only Delete        : disabled
WINS Servers            : -
```

ゲスト **UNIX** ユーザを設定します

ゲスト UNIX ユーザを設定すると、信頼されていないドメインからログインしたユーザがゲスト UNIX ユーザにマッピングされ、CIFS サーバに接続できるようになります。ただし、信頼されていないドメインのユーザの認証を失敗にする場合は、ゲスト UNIX ユーザを設定しないでください。デフォルトでは、信頼されていないドメインのユーザによる CIFS サーバへの接続は許可されません（ゲスト UNIX アカウントは設定されません）。

このタスクについて

ゲスト UNIX アカウントを設定する場合は、次の点に注意する必要があります。

- CIFS サーバがホームドメインまたは信頼できるドメインのドメインコントローラ、ローカルデータベースのどちらかに対してユーザを認証できず、このオプションが有効である場合、CIFS サーバはユーザをゲストユーザとみなし、そのユーザを指定した UNIX ユーザにマッピングします。
- このオプションを null 文字列に設定すると、ゲスト UNIX ユーザは無効になります。
- いずれかの Storage Virtual Machine（SVM）ネームサービスデータベースで、ゲスト UNIX ユーザとして使用する UNIX ユーザを作成する必要があります。
- ゲストユーザとしてログインしたユーザは、自動的に CIFS サーバの BUILTIN\guests グループのメンバーになります。
- 「homedirs-public」オプションは、認証されたユーザにのみ適用されます。ゲストユーザとしてログインしたユーザは、ホームディレクトリを持ちません。また、他のユーザのホームディレクトリにアクセスすることはできません。

手順

1. 次のいずれかを実行します。

状況	入力するコマンド
ゲスト UNIX ユーザを設定します	<pre>vserver cifs options modify -guest -unix-user <i>unix_name</i></pre>
ゲスト UNIX ユーザを無効にします	<pre>vserver cifs options modify -guest -unix-user ""</pre>

```
vserver cifs options modify -guest-unix-user pcuser
```

2. ゲストUNIXユーザが正しく設定されていることを確認します。 `vserver cifs options show -vserver vserver_name`

次の例では、SVM vs1 のデフォルト UNIX ユーザとゲスト UNIX ユーザの両方が UNIX ユーザ「pcuser」を使用するように設定されています。

```
vserver cifs options show -vserver vs1
```

```
Vserver: vs1

Client Session Timeout : 900
Default Unix Group      : -
Default Unix User       : pcuser
Guest Unix User         : pcuser
Read Grants Exec        : disabled
Read Only Delete        : disabled
WINS Servers            : -
```

**Administrators** グループをルートにマッピングします

環境内のクライアントがすべて CIFS クライアントで、Storage Virtual Machine（SVM）がマルチプロトコルストレージシステムとしてセットアップされている場合は、SVM上のファイルにアクセスするための root 権限を持つ Windows アカウントが少なくとも 1 つ必要です。十分なユーザ権限がないため、この SVM を管理できません。

このタスクについて

ただし、ストレージシステムがNTFS専用としてセットアップされている場合は /etc ディレクトリには、AdministratorsグループがONTAP 構成ファイルにアクセスできるようにするファイルレベルのACLが設定されています。

手順

1. 権限レベルを advanced に設定します。 `set -privilege advanced`
2. 必要に応じて、Administrators グループをルートにマッピングする CIFS サーバオプションを設定します。

状況	作業
管理者グループメンバーをルートにマッピングします	<code>vserver cifs options modify -vserver vserver_name -is-admin-users-mapped-to -root-enabled true</code> がなくても、Administratorsグループ内のすべてのアカウントはrootとみなされます。/etc/usermap.cfg アカウントをrootにマッピングするエントリ。Administrators グループに属するアカウントを使用してファイルを作成する場合、UNIX クライアントからファイルを表示するときに、ファイルはルートによって所有されます。
Administrators グループメンバーのルートへのマッピングを無効にします	<code>vserver cifs options modify -vserver vserver_name -is-admin-users-mapped-to -root-enabled false</code> Administratorsグループ内のアカウントがrootにマッピングされなくなります。ルートへのマッピングは、単一のユーザに対して明示的にのみ実行できます。

- オプションが目的の値に設定されていることを確認します。 `vserver cifs options show -vserver vserver_name`
- admin 権限レベルに戻ります。 `set -privilege admin`

**SMB** セッションを介して接続しているユーザのタイプに関する情報を表示します

SMB セッションを介して接続しているユーザのタイプに関する情報を表示できます。これは、適切なタイプのユーザのみが Storage Virtual Machine （SVM）上の SMB セッションを介して接続していることを確認するのに役立ちます。

このタスクについて

SMB セッションを介して接続できるユーザのタイプは次のとおりです。

- local-user

ローカル CIFS ユーザとして認証されている

- domain-user

ドメインユーザとして（CIFS サーバのホームドメインまたは信頼できるドメインから）認証されている

- guest-user

ゲストユーザとして認証されています

- anonymous-user

匿名ユーザまたは null ユーザとして認証されています

手順

1. SMBセッションを介して接続しているユーザのタイプを確認します。vserver cifs session show -vserver vserver\_name -windows-user windows\_user\_name -fields windows-user,address,lif-address,user-type

確立されたセッションのユーザタイプ情報を表示する対象	入力するコマンド
指定したユーザタイプのすべてのセッション	`vserver cifs session show -vserver vserver_name -user-type {local-user
domain-user	guest-user
anonymous-user}`	特定のユーザの場合

例

次のコマンドを実行すると、ユーザ「iepubs\user1」によって確立された SVM vs1 上のセッションのユーザタイプに関するセッション情報が表示されます。

```
cluster1::> vserver cifs session show -vserver pub1 -windows-user
iepubs\user1 -fields windows-user,address,lif-address,user-type
node      vserver session-id connection-id lif-address  address
windows-user      user-type
-----
-----
pub1node1 pub1      1          3439441860      10.0.0.1      10.1.1.1
IEPUBS\user1      domain-user
```

Windows クライアントの過剰なリソース消費を制限するコマンドオプション

をクリックします vserver cifs options modify コマンドを使用すると、Windowsクライアントのリソース消費を制御できます。ファイルオープン、セッションオープン、変更通知要求が異常に多い場合など、正常な範囲を超えてリソースを消費しているクライアントがある場合に便利です。

には次のオプションがあります vserver cifs options modify Windowsクライアントのリソース消費を制御するコマンドが追加されました。これらのオプションの最大値を超えると、要求は拒否され、EMS メッセージが送信されます。これらのオプションで設定された上限の 80% に達したときにも EMS 警告メッセージが送信されます。

- -max-opens-same-file-per-tree  
CIFS ツリーあたりの同じファイルの最大オープン数
- -max-same-user-sessions-per-connection  
同じユーザが接続ごとに開いたセッションの最大数

- `-max-same-tree-connect-per-session`

同じ共有に対するセッションあたりの最大ツリー接続数

- `-max-watches-set-per-tree`

ツリーごとに確立されるウォッチの最大数（別名 *change notifier*）

デフォルトの制限および現在の設定を表示する方法については、マニュアルページを参照してください。

ONTAP 9.4 以降では、SMB バージョン 2 以降を実行しているサーバで、クライアントからサーバに SMB 接続で送信できる未処理要求（`_SMB クレジット`）の数を制限することができます。SMB クレジットの管理はクライアント側で開始され、サーバ側で制御されます。

SMB接続で許可できる未処理要求の最大数は、で制御されます `-max-credits` オプションこのオプションのデフォルト値は 128 です。

従来の **oplock** および **oplock** リースでクライアントのパフォーマンスを向上

従来の **oplock** および **oplock** リースの概要でクライアントのパフォーマンスを向上

便宜的 **oplock** と **oplock** リースでは、先読み、あと書き、ロックの各情報を SMB クライアント側でキャッシングできるよう、特定のファイル共有シナリオでそのクライアントを有効にします。これにより、クライアントは、目的のファイルへのアクセス要求をサーバに定期的に通知しなくても、ファイルの読み書きを実行できます。これにより、ネットワークトラフィックが軽減され、パフォーマンスが向上します。

**oplock** リースは **oplock** を強化したもので、SMB 2.1 以降のプロトコルで使用できます。**oplock** リースでは、クライアントが、自身による複数の SMB オープンにおいてキャッシュ状態を取得し、保持できます。

**oplock** は次の 2 つの方法で制御できます。

- 共有プロパティで、を使用します `vserver cifs share create` 共有の作成時にコマンドを実行するか、またはを実行します `vserver share properties` 作成後のコマンド。
- **qtree**プロパティ。を使用します `volume qtree create` コマンドを使用して**qtree**を作成するか、コマンドを使用します `volume qtree oplock` 作成後のコマンド。

**oplock** を使用するときの書き込みキャッシュデータ消失に関する考慮事項

状況によっては、あるプロセスがファイルに対して排他的な **oplock** を保持している場合に、別のプロセスがそのファイルを開こうとすると、最初のプロセスはキャッシュされたデータを無効にし、書き込みとロックをフラッシュする必要があります。クライアントは **oplock** を放棄し、ファイルにアクセスする必要があります。このフラッシュ時にネットワーク障害が発生すると、キャッシュされた書き込みデータが失われる可能性があります。

- データ損失の可能性

データの書き込みがキャッシュされるアプリケーションでは、次の場合にそのデータを失う可能性があります

ます。

- 接続は SMB 1.0 を使用して確立されます。
  - ファイルに対して排他的な oplock を使用している場合
  - oplock を解除するか、ファイルを閉じるように指示された場合
  - 書き込みキャッシュをフラッシュするプロセスで、ネットワークまたはターゲットシステムにエラーが発生した場合
- エラー処理および書き込みの完了

キャッシュ自体にはエラー処理がありません。アプリケーションがエラー処理を行います。アプリケーションがキャッシュへの書き込みを行うと、書き込みは常に完了します。キャッシュがネットワーク経由でターゲットシステムに書き込みを行う場合、書き込みは完了していると仮定する必要があります。これは、完了していない場合、データが失われるためです。

**SMB 共有の作成時に oplock を有効または無効にします**

oplock を使用すると、クライアントによってファイルがロックされてコンテンツがローカルにキャッシュされるため、ファイル操作のパフォーマンスが向上します。Storage Virtual Machine（SVM）上にある SMB 共有では、oplock が有効になっています。場合によっては、oplock の無効化が必要になることがあります。oplock は共有ごとに有効または無効にできます。

このタスクについて

共有を含むボリュームで oplock が有効になっているが、その共有の oplock 共有プロパティが無効になっている場合、その共有の oplock は無効になります。共有での oplock の無効化は、ボリュームの oplock の設定よりも優先されます。共有で oplock を無効にすると、便宜的 oplock と oplock リースの両方が無効になります。

oplock 共有プロパティに加えて、その他の共有プロパティをカンマで区切って指定できます。その他の共有パラメータを指定することもできます。

手順

1. 該当する操作を実行します。



状況	作業
共有の作成時に共有で oplock を有効にします	<p>次のコマンドを入力します。vserver cifs share create -vserver _vserver_name_ -share-name share_name -path path_to_share -share-properties [oplocks,...]</p> <div>  <p>共有にデフォルトの共有プロパティのみを設定する場合は、です oplocks、browsable および `changenotify` 有効にすると、を指定する必要はありません -share -properties SMB共有を作成するときのパラメータ。デフォルト以外の共有プロパティを組み合わせる場合は、を指定する必要があります -share-properties パラメータに指定し、その共有に使用する共有プロパティのリストを指定します。</p> </div>
共有の作成時に共有で oplock を無効にします	<p>次のコマンドを入力します。vserver cifs share create -vserver _vserver_name_ -share-name _share_name_ -path _path_to_share_ -share-properties [other_share_property,...]</p> <div>  <p>oplockを無効にする場合は、共有の作成時に共有プロパティのリストを指定する必要がありますが、を指定することはできません oplocks プロパティ。</p> </div>

## 関連情報

[既存の SMB 共有で oplock を有効または無効にします](#)

[oplock ステータスを監視しています](#)

ボリュームおよび **qtree** で **oplock** を有効または無効にするためのコマンド

oplock を使用すると、クライアントによってファイルがロックされてコンテンツがローカルにキャッシュされるため、ファイル操作のパフォーマンスが向上します。ボリュームや qtree の oplock を有効または無効にするためのコマンドを理解しておく必要があります。また、いつボリュームおよび qtree で oplock を有効または無効にできるかについても理解しておく必要があります。

- ボリュームではデフォルトで oplock が有効になっています。

- ボリュームの作成時に oplock を無効にすることはできません。
- 既存の SVM のボリュームでは、oplock をいつでも有効または無効にできます。
- SVM の qtree では oplock を有効にできます。

oplock モードの設定は、すべてのボリュームのデフォルトの qtree である qtree ID 0 のプロパティです。qtree の作成時に oplock 設定を指定しない場合、qtree は親ボリュームの oplock 設定を継承します。この設定はデフォルトで有効になっています。ただし、新しい qtree に oplock 設定を指定すると、ボリュームの oplock 設定よりも優先されます。

状況	使用するコマンド
ボリュームまたは qtree の oplock を有効にします	volume qtree oplocks を使用 -oplock-mode パラメータをに設定します enable
ボリュームまたは qtree の oplock を無効にします	volume qtree oplocks を使用 -oplock-mode パラメータをに設定します disable

## 関連情報

[oplock ステータスを監視しています](#)

既存の SMB 共有で **oplock** を有効または無効にします

Storage Virtual Machine（SVM）上の SMB 共有では、oplock がデフォルトで有効になっています。場合によっては、oplock の無効化が必要になることがあります。または、以前に共有で oplock を無効にした場合に、oplock を再度有効にすることもできます。

## このタスクについて

共有を含むボリュームで oplock が有効になっているが、その共有の oplock 共有プロパティが無効になっている場合、その共有の oplock は無効になります。共有での oplock の無効化は、ボリュームでの oplock の有効化よりも優先されます。共有で oplock を無効にすると、便宜的 oplock と oplock リースの両方が無効になります。既存の共有での oplock の有効化と無効化はいつでも実行できます。

## ステップ

1. 該当する操作を実行します。

状況	作業
既存の共有を変更して、共有で oplock を有効にします	<p>次のコマンドを入力します。vserver cifs share properties add -vserver vserver_name -share-name share_name -share-properties oplocks</p> <div>  <p>追加する共有プロパティをカンマで区切って追加指定できます。</p> </div> <p>新しく追加したプロパティは、共有プロパティの既存のリストに追加されます。以前に指定した共有プロパティは有効なままです。</p>
既存の共有を変更して共有で oplock を無効にします	<p>次のコマンドを入力します。vserver cifs share properties remove -vserver vserver_name -share-name share_name -share-properties oplocks</p> <div>  <p>削除する共有プロパティをカンマで区切って追加指定できます。</p> </div> <p>削除した共有プロパティは既存の共有プロパティリストから削除されますが、削除しなかった設定済みの共有プロパティは有効なままです。</p>

## 例

次のコマンドは、Storage Virtual Machine（SVM、旧 Vserver）vs1 上の「Engineering」という名前の共有の oplock を有効にします。

```
cluster1::> vserver cifs share properties add -vserver vs1 -share-name Engineering -share-properties oplocks
```

```
cluster1::> vserver cifs share properties show
```

Vserver	Share	Properties
-----	-----	-----
vs1	Engineering	oplocks browsable changenotify showsnapshot

次のコマンドは、SVM vs1 上の「Engineering」という名前の共有の oplock を無効にします。

```
cluster1::> vservers cifs share properties remove -vservers vs1 -share-name Engineering -share-properties oplocks
```

```
cluster1::> vservers cifs share properties show
```

Vserver	Share	Properties
vs1	Engineering	browsable changenotify showsnapshot

## 関連情報

### SMB 共有の作成時における oplock の有効化と無効化

#### oplock ステータスを監視しています

#### 既存の SMB 共有に対する共有プロパティの追加または削除

#### oplock ステータスを監視します

oplock ステータスについて、情報を監視、表示できます。この情報を使用して、oplock が設定されたファイル、oplock のレベルや oplock の状態レベル、oplock リースの使用の有無を確認できます。また、手動での解除が必要となる可能性のあるロックについて、情報を確認することもできます。

#### このタスクについて

すべての oplock についての情報を要約形式または詳細なリスト形式で表示できます。オプションのパラメータを使用すると、既存のロックの一部について情報を表示することもできます。たとえば、クライアントの IP アドレスやパスを指定して、該当するロックのみを返すように指定できます。

従来の oplock および oplock リースについて、次の情報を表示できます。

- oplock が有効な SVM、ノード、ボリューム、LIF
- ロック UUID
- oplock が有効なクライアントの IP アドレス
- oplock が有効なパス
- ロックのプロトコル（SMB）およびロックのタイプ（oplock）
- ロックの状態
- oplock レベル
- 接続の状態および SMB の有効期限
- oplock リースが許可されている場合は、Open Group ID

を参照してください `vservers oplocks show` 各パラメータの詳細な概要 のマニュアルページ

## 手順

1. を使用してoplockステータスを表示します `vserver locks show` コマンドを実行します

例

次のコマンドは、すべてのロックに関するデフォルトの情報を表示します。表示されたファイルのoplockは、で許可されています `read-batch oplock`レベル：

```
cluster1::> vserver locks show
```

```
Vserver: vs0
```

Volume	Object Path	LIF	Protocol	Lock Type	Client
vol1	/vol1/notes.txt	node1_data1			
			cifs	share-level	192.168.1.5
	Sharelock Mode: read_write-deny_delete				
				op-lock	192.168.1.5
	Oplock Level: read-batch				

次の例は、パスのファイルに対するロックに関する詳細情報を表示します

`/data2/data2_2/intro.pptx`。を使用してファイルにoplockリースが許可されています `batch` IPアドレスがのクライアントに対するoplockレベル `10.3.1.3`：



詳細情報を表示する場合に、このコマンドを使用すると、oplock の情報と共有ロックの情報を別々に表示できます。この例では、oplock の情報のみが表示されています。

```
cluster1::> vserver lock show -instance -path /data2/data2_2/intro.pptx
```

```

    Vserver: vs1
    Volume: data2_2
Logical Interface: lif2
    Object Path: /data2/data2_2/intro.pptx
    Lock UUID: ff1cbf29-bfef-4d91-ae06-062bf69212c3
    Lock Protocol: cifs
    Lock Type: op-lock
Node Holding Lock State: node3
    Lock State: granted
Bytelock Starting Offset: -
    Number of Bytes Locked: -
    Bytelock is Mandatory: -
    Bytelock is Exclusive: -
    Bytelock is Superlock: -
    Bytelock is Soft: -
    Oplock Level: batch
Shared Lock Access Mode: -
    Shared Lock is Soft: -
    Delegation Type: -
    Client Address: 10.3.1.3
    SMB Open Type: -
    SMB Connect State: connected
SMB Expiration Time (Secs): -
    SMB Open Group ID:
78a90c59d45ae211998100059a3c7a00a007f70da0f8ffffcd445b0300000000
```

## 関連情報

[SMB 共有の作成時における oplock の有効化と無効化](#)

[既存の SMB 共有で oplock を有効または無効にします](#)

[ボリュームおよび qtree で oplock を有効または無効にするためのコマンド](#)

## SMB サーバへのグループポリシーオブジェクトの適用

**SMB** サーバへのグループポリシーオブジェクトの適用の概要の説明を参照してください

SMBサーバは、グループポリシーオブジェクト（GPO）をサポートしています。GPO は、Active Directory環境のコンピュータに適用される\_グループポリシー属性\_と呼ばれる一連のルールです。GPO を使用して、同じ Active Directory ドメインに属するクラスター上のすべての Storage Virtual Machine （SVM）の設定を一元管理できます。

SMBサーバでGPOが有効になっている場合、ONTAPはActive DirectoryサーバにLDAPクエリを送信してGPO情報を要求します。SMBサーバに適用可能なGPO定義がある場合、Active Directoryサーバは次のGPO情報を

返します。

- GPO 名
- 現在の GPO バージョン
- GPO 定義の場所
- GPO ポリシーセットの Universally Unique Identifier (UUID) 一覧

#### 関連情報

[DAC（ダイナミックアクセス制御）を使用したファイルアクセスの保護](#)

["SMB および NFS の監査とセキュリティトレース"](#)

#### サポートされる GPO

すべてのグループポリシーオブジェクト（GPO）を CIFS 対応の Storage Virtual Machine（SVM）に適用できるわけではありませんが、SVM では関連する GPO を認識して処理することができます。

SVM で現在サポートされている GPO は次のとおりです。

- 高度な監査ポリシー設定：

オブジェクトへのアクセス：集約型アクセスポリシーのステージング

次の設定を含む集約型アクセスポリシー（CAP）のステージングで監査対象となるイベントのタイプを指定します。

- 監査しないでください
- 成功イベントのみ監査
- 失敗イベントのみ監査
- 成功イベントと失敗イベントの両方を監査します



3つの監査オプション（成功イベントのみ監査、失敗イベントのみ監査、成功イベントと失敗イベントの両方を監査）のいずれかが設定されている場合、ONTAP は成功イベントと失敗イベントの両方を監査します。

を使用して設定します Audit Central Access Policy Staging を設定します Advanced Audit Policy Configuration/Audit Policies/Object Access GPO：



高度な監査ポリシー構成 GPO 設定を使用するには、その設定を適用する CIFS 対応の SVM 上で監査を構成する必要があります。SVM で監査が構成されていない場合、GPO 設定は適用されず、破棄されます。

- レジストリ設定：
  - CIFS 対応の SVM のグループポリシーの更新間隔

を使用して設定します Registry GPO：

- グループポリシーの更新間隔のランダムオフセット

を使用して設定します Registry GPO :

- BranchCache のハッシュの発行

BranchCache のハッシュの発行 GPO は、BranchCache の動作モードに対応します。次の 3 つの動作モードがサポートされています。

- 共有ごと
- all-shares

- 無効

を使用して設定します Registry GPO :

- BranchCache のハッシュバージョンサポート

次の 3 つのハッシュバージョン設定がサポートされています。

- BranchCache バージョン 1.7
  - BranchCache バージョン 1.7
  - BranchCacheバージョン1および2
- を使用して設定します Registry GPO :



BranchCache GPO 設定を使用するには、その設定を適用する CIFS 対応の SVM 上で BranchCache を構成する必要があります。SVM で BranchCache が構成されていない場合、GPO 設定は適用されず、破棄されます。

- セキュリティ設定

- 監査ポリシーとイベントログ

- ログオンイベントを監査します

次の設定を含む監査対象となるログオンイベントの種類を指定します。

- 監査しないでください
  - 成功イベントのみ監査
  - 障害イベントの監査
  - 成功イベントと失敗イベントの両方を監査します
- を使用して設定します Audit logon events を設定します Local Policies/Audit Policy GPO :



3 つの監査オプション（成功イベントのみ監査、失敗イベントのみ監査、成功イベントと失敗イベントの両方を監査）のいずれかが設定されている場合、ONTAP は成功イベントと失敗イベントの両方を監査します。

- オブジェクトへのアクセスを監査する

次の設定を含む監査対象となるオブジェクトアクセスの種類を指定します。



- 監査しないでください
- 成功イベントのみ監査
- 障害イベントの監査
- 成功イベントと失敗イベントの両方を監査します  
を使用して設定します Audit object access を設定します Local Policies/Audit Policy GPO :



3つの監査オプション（成功イベントのみ監査、失敗イベントのみ監査、成功イベントと失敗イベントの両方を監査）のいずれかが設定されている場合、ONTAPは成功イベントと失敗イベントの両方を監査します。

#### ▪ ログの保持方法

次の設定を含む監査ログの保持方法を指定します。

- ログファイルのサイズが最大ログサイズを超えたら、イベントログを上書きします
- イベントログを上書きしない（手動でログを消去）  
を使用して設定します Retention method for security log を設定します Event Log GPO :

#### ▪ 最大ログサイズ

監査ログの最大サイズを指定します。

を使用して設定します Maximum security log size を設定します Event Log GPO :



監査ポリシーとイベントログ GPO 設定を使用するには、その設定を適用する CIFS 対応の SVM 上で監査を構成する必要があります。SVM で監査が構成されていない場合、GPO 設定は適用されず、破棄されます。

#### ◦ ファイルシステムのセキュリティ

GPO を通してファイルセキュリティを適用するファイルまたはディレクトリのリストを指定します。

を使用して設定します File System GPO :



SVM 内にファイルシステムセキュリティ GPO を構成するボリュームパスが存在している必要があります。

#### ◦ Kerberos ポリシー

##### ▪ 最大クロックスキュー

コンピュータクロック同期の最大許容誤差を分単位で指定します。

を使用して設定します Maximum tolerance for computer clock synchronization を設定します Account Policies/Kerberos Policy GPO :

##### ▪ チケットの有効期間

ユーザチケットの最大有効期間を時間単位で指定します。

を使用して設定します Maximum lifetime for user ticket を設定します Account Policies/Kerberos Policy GPO :

- チケットの更新の有効期間

ユーザチケットの更新の最大有効期間を日単位で指定します。

を使用して設定します Maximum lifetime for user ticket renewal を設定します Account Policies/Kerberos Policy GPO :

- ユーザ権限の割り当て (権限)

- 所有権を取得します

セキュリティ保護が可能なオブジェクトの所有権を持つユーザとグループのリストを指定します。

を使用して設定します Take ownership of files or other objects を設定します Local Policies/User Rights Assignment GPO :

- セキュリティ権限

ファイル、フォルダ、Active Directory オブジェクトなどの個々のリソースへのオブジェクトアクセスの監査オプションを指定できるユーザとグループのリストを指定します。

を使用して設定します Manage auditing and security log を設定します Local Policies/User Rights Assignment GPO :

- 通知権限の変更 (トラバースチェックのバイパス)

ユーザとグループがトラバースするディレクトリに対する権限を持っていなくても、ディレクトリツリーをトラバースできるユーザとグループのリストを指定します。

ファイルやディレクトリの変更通知を受け取るユーザにも同じ権限が必要です。を使用して設定します Bypass traverse checking を設定します Local Policies/User Rights Assignment GPO :

- レジストリ値

- 署名要求設定

SMB 署名要求が有効になっているか無効になっているかを示します。

を使用して設定します Microsoft network server: Digitally sign communications (always) を設定します Security Options GPO :

- restrict anonymous (匿名の制限)

匿名ユーザの制限内容に次の 3 つの GPO 設定を指定します。

- Security Account Manager (SAM) アカウントを列挙しない :

このセキュリティ設定は、コンピュータへの匿名接続に付与される追加の権限を決定します。このオプションはと表示されます no-enumeration ONTAP（有効になっている場合）。

を使用して設定します Network access: Do not allow anonymous enumeration of SAM accounts を設定します Local Policies/Security Options GPO：

- SAM アカウントと共有は列挙しません

このセキュリティ設定で、匿名による SAM アカウントと共有の列挙を許可するかどうかを決定します。このオプションはと表示されます no-enumeration ONTAP（有効になっている場合）。

を使用して設定します Network access: Do not allow anonymous enumeration of SAM accounts and shares を設定します Local Policies/Security Options GPO：

- 共有と名前付きパイプへの匿名アクセスを制限します

共有とパイプへの匿名アクセスを制限します。このオプションはと表示されます no-access ONTAP（有効になっている場合）。

を使用して設定します Network access: Restrict anonymous access to Named Pipes and Shares を設定します Local Policies/Security Options GPO：

定義済みおよび適用済みのグループポリシーに関する情報を表示する場合は、Resultant restriction for anonymous user Outputフィールドには、3つのrestrict anonymous GPO設定による制限に関する情報が表示されます。表示される可能性がある制限結果は、次のとおりです。

- no-access

匿名ユーザは、指定された共有と名前付きパイプへのアクセスを拒否され、SAM アカウントと共有を列挙できません。この制限結果は、の場合に表示されます Network access: Restrict anonymous access to Named Pipes and Shares GPOが有効になっている。

- no-enumeration

匿名ユーザは、指定された共有と名前付きパイプにアクセスできますが、SAM アカウントと共有は列挙できません。この制限は、次の両方の条件に該当する場合に適用されます。

- 。 Network access: Restrict anonymous access to Named Pipes and Shares GPOが無効になっています。
- またはをクリックします Network access: Do not allow anonymous enumeration of SAM accounts または Network access: Do not allow anonymous enumeration of SAM accounts and shares GPOが有効になっている。

- no-restriction

匿名ユーザにはフルアクセスが付与され、列挙できます。この制限は、次の両方の条件に該当する場合に適用されます。

- 。 Network access: Restrict anonymous access to Named Pipes and Shares GPOが無効になっています。
- 両方とも Network access: Do not allow anonymous enumeration of SAM accounts

および Network access: Do not allow anonymous enumeration of SAM accounts and shares GPOが無効になっている。

- 制限されたグループ

制限されたグループを設定して、組み込みまたはユーザ定義のグループのメンバーシップを一元管理することができます。グループポリシーを通して制限されたグループを適用する場合、CIFS サーバローカルグループのメンバーシップは、適用されるグループポリシーで定義されているメンバーリスト設定に一致するように自動的に設定されます。

を使用して設定します Restricted Groups GPO :

- 集約型アクセスポリシーの設定

集約型アクセスポリシーのリストを指定します。集約型アクセスポリシーと関連付けられた集約型アクセスポリシールールによって、SVM 上の複数のファイルに対するアクセス権限が決定されます。

## 関連情報

[CIFS サーバ上で GPO サポートを有効または無効にします](#)

[DAC（ダイナミックアクセス制御）を使用したファイルアクセスの保護](#)

["SMB および NFS の監査とセキュリティトレース"](#)

[CIFS サーバの Kerberos セキュリティ設定の変更](#)

[BranchCache を使用したブランチオフィスでの SMB 共有のコンテンツのキャッシュ](#)

[SMB 署名を使用したネットワークセキュリティの強化](#)

[トラバースチェックのバイパスの設定](#)

[匿名ユーザのアクセス制限を設定します](#)

**SMB** サーバで **GPO** を使用するための要件

SMB サーバでグループポリシーオブジェクト（GPO）を使用するには、いくつかの要件を満たしている必要があります。

- クラスタで SMB のライセンスが有効になっている必要があります。SMBライセンスには含まれていません。"ONTAP One"。ONTAP Oneをお持ちでなく、ライセンスがインストールされていない場合は、営業担当者にお問い合わせください。
- SMB サーバが設定され、Windows Active Directory ドメインに参加している必要があります。
- SMB サーバ管理ステータスがオンになっている必要があります。
- GPO が設定され、SMB サーバコンピュータオブジェクトを含む Windows Active Directory の組織単位（OU）に適用されている必要があります。
- SMB サーバで GPO のサポートが有効になっている必要があります。

CIFS サーバ上で GPO のサポートを有効または無効にします

CIFS サーバでグループポリシーオブジェクト（GPO）のサポートを有効または無効にできます。CIFS サーバ上で GPO のサポートを有効にすると、グループポリシー（CIFS サーバコンピュータオブジェクトを含む組織単位に適用されるポリシー）に定義されている該当する GPO が CIFS サーバに適用されます。



このタスクについて  
GPO はワークグループモードの CIFS サーバでは有効にできません。

手順

- 1. 次のいずれかを実行します。

状況	入力するコマンド
GPOs を有効にします。	<code>vserver cifs group-policy modify -vserver vserver_name -status enabled</code>
GPOs を無効にする	<code>vserver cifs group-policy modify -vserver vserver_name -status disabled</code>

- 2. GPOサポートが目的の状態になっていることを確認します。 `vserver cifs group-policy show -vserver +vserver_name_`

ワークグループモードの CIFS サーバのグループポリシーステータスは「disabled」と表示されます。

例

次の例は、Storage Virtual Machine（SVM）vs1 で GPO サポートを有効にします。

```
cluster1::> vserver cifs group-policy modify -vserver vs1 -status enabled

cluster1::> vserver cifs group-policy show -vserver vs1

                Vserver: vs1
Group Policy Status: enabled
```

関連情報

- [サポートされる GPO](#)
- [CIFSサーバでGPOを使用するための要件](#)
- [CIFS サーバでの GPO の更新方法](#)
- [CIFS サーバ上の GPO 設定を手動で更新します](#)
- [GPO 設定に関する情報を表示します](#)

CIFS サーバでの GPO の更新方法の概要

デフォルトでは、ONTAP はグループポリシーオブジェクト（GPO）の変更を 90 分に 1 回取得して適用します。セキュリティ設定は 16 時間ごとに更新されます。ONTAP で自動的に更新される前に GPO を更新し、新しい GPO ポリシー設定を適用するには、ONTAP コマンドを使用して CIFS サーバで手動更新をトリガーします。


- デフォルトでは、すべての GPO を 90 分に 1 回確認し、必要に応じて更新。

この間隔は設定可能で、を使用して設定できます Refresh interval および Random offset GPO 設定。

ONTAP は、GPO の変更がないかどうかを Active Directory に照会します。Active Directory に記録されている GPO のバージョン番号が CIFS サーバ上の GPO のバージョン番号より大きい場合、ONTAP は新しい GPO を取得して適用します。バージョン番号が同じ場合、CIFS サーバ上の GPO は更新されません。

- セキュリティ設定の GPO を 16 時間に 1 回更新。

ONTAP は、変更の有無にかかわらず、16 時間に 1 回セキュリティ設定の GPO を取得して適用します。



デフォルト値の 16 時間は、現在の ONTAP バージョンでは変更できません。これは Windows クライアントのデフォルト設定です。

- ONTAP コマンドを使用して手動ですべての GPO を更新。

このコマンドは、ウィンドウをシミュレートします gpupdate.exe /force コマンド。

関連情報

CIFS サーバ上の GPO 設定を手動で更新します

CIFS サーバ上の GPO 設定を手動で更新します

CIFS サーバの Group Policy Object（GPO；グループポリシーオブジェクト）設定を直ちに更新するには、設定を手動で更新します。変更された設定のみを更新することも、以前に適用されていて変更されていない設定を含めてすべての設定を強制的に更新することもできます。

ステップ

- 適切な操作を実行します。

更新する項目	入力するコマンド
GPO 設定が変更されました	<code>vserver cifs group-policy update -vserver vserver_name</code>

更新する項目	入力するコマンド
すべての GPO 設定	<code>vserver cifs group-policy update -vserver vserver_name -force-reapply -all-settings true</code>

## 関連情報

### CIFS サーバでの GPO の更新方法

GPO 設定に関する情報を表示します

Active Directory で定義されているグループポリシーオブジェクト（GPO）設定および CIFS サーバに適用されている GPO 設定に関する情報を表示できます。

このタスクについて

CIFS サーバが属しているドメインの Active Directory で定義されているすべての GPO 設定に関する情報を表示するか、または CIFS サーバに適用されている GPO 設定に関する情報のみを表示することができます。

## 手順

1. 次のいずれかの操作を実行し、GPO 設定に関する情報を表示します。

情報を表示するグループポリシー設定	入力するコマンド
Active Directory で定義されています	<code>vserver cifs group-policy show-defined -vserver vserver_name</code>
CIFS 対応の Storage Virtual Machine（SVM）に適用されている	<code>vserver cifs group-policy show-applied -vserver vserver_name</code>

## 例

次の例は、vs1 という CIFS 対応の SVM が属する Active Directory で定義されている GPO 設定を表示します。

```
cluster1::> vserver cifs group-policy show-defined -vserver vs1
```

```
Vserver: vs1
```

```
-----
```

```
    GPO Name: Default Domain Policy
```

```
    Level: Domain
```

```
    Status: enabled
```

```
Advanced Audit Settings:
```

```
    Object Access:
```

```
        Central Access Policy Staging: failure
```

```
Registry Settings:
```

```
    Refresh Time Interval: 22
```

```
Refresh Random Offset: 8
Hash Publication Mode for BranchCache: per-share
Hash Version Support for BranchCache : version1
Security Settings:
  Event Audit and Event Log:
    Audit Logon Events: none
    Audit Object Access: success
    Log Retention Method: overwrite-as-needed
    Max Log Size: 16384
  File Security:
    /vol1/home
    /vol1/dir1
  Kerberos:
    Max Clock Skew: 5
    Max Ticket Age: 10
    Max Renew Age: 7
  Privilege Rights:
    Take Ownership: usr1, usr2
    Security Privilege: usr1, usr2
    Change Notify: usr1, usr2
  Registry Values:
    Signing Required: false
  Restrict Anonymous:
    No enumeration of SAM accounts: true
    No enumeration of SAM accounts and shares: false
    Restrict anonymous access to shares and named pipes: true
    Combined restriction for anonymous user: no-access
  Restricted Groups:
    gpr1
    gpr2
Central Access Policy Settings:
  Policies: cap1
           cap2

  GPO Name: Resultant Set of Policy
  Status: enabled
Advanced Audit Settings:
  Object Access:
    Central Access Policy Staging: failure
Registry Settings:
  Refresh Time Interval: 22
  Refresh Random Offset: 8
  Hash Publication for Mode BranchCache: per-share
  Hash Version Support for BranchCache: version1
Security Settings:
  Event Audit and Event Log:
```



```

    Audit Logon Events: none
    Audit Object Access: success
    Log Retention Method: overwrite-as-needed
    Max Log Size: 16384
File Security:
    /vol1/home
    /vol1/dir1
Kerberos:
    Max Clock Skew: 5
    Max Ticket Age: 10
    Max Renew Age: 7
Privilege Rights:
    Take Ownership: usr1, usr2
    Security Privilege: usr1, usr2
    Change Notify: usr1, usr2
Registry Values:
    Signing Required: false
Restrict Anonymous:
    No enumeration of SAM accounts: true
    No enumeration of SAM accounts and shares: false
    Restrict anonymous access to shares and named pipes: true
    Combined restriction for anonymous user: no-access
Restricted Groups:
    gpr1
    gpr2
Central Access Policy Settings:
    Policies: cap1
               cap2

```

次の例は、CIFS 対応の SVM vs1 に適用されている GPO 設定を表示します。

```

cluster1::> vserver cifs group-policy show-applied -vserver vs1

Vserver: vs1
-----
    GPO Name: Default Domain Policy
        Level: Domain
        Status: enabled
Advanced Audit Settings:
    Object Access:
        Central Access Policy Staging: failure
Registry Settings:
    Refresh Time Interval: 22
    Refresh Random Offset: 8
    Hash Publication Mode for BranchCache: per-share

```

```
Hash Version Support for BranchCache: all-versions
Security Settings:
  Event Audit and Event Log:
    Audit Logon Events: none
    Audit Object Access: success
    Log Retention Method: overwrite-as-needed
    Max Log Size: 16384
  File Security:
    /vol1/home
    /vol1/dir1
  Kerberos:
    Max Clock Skew: 5
    Max Ticket Age: 10
    Max Renew Age: 7
  Privilege Rights:
    Take Ownership: usr1, usr2
    Security Privilege: usr1, usr2
    Change Notify: usr1, usr2
  Registry Values:
    Signing Required: false
  Restrict Anonymous:
    No enumeration of SAM accounts: true
    No enumeration of SAM accounts and shares: false
    Restrict anonymous access to shares and named pipes: true
    Combined restriction for anonymous user: no-access
  Restricted Groups:
    gpr1
    gpr2
Central Access Policy Settings:
  Policies: cap1
           cap2

GPO Name: Resultant Set of Policy
Level: RSOP
Advanced Audit Settings:
  Object Access:
    Central Access Policy Staging: failure
Registry Settings:
  Refresh Time Interval: 22
  Refresh Random Offset: 8
  Hash Publication Mode for BranchCache: per-share
  Hash Version Support for BranchCache: all-versions
Security Settings:
  Event Audit and Event Log:
    Audit Logon Events: none
    Audit Object Access: success
```

```
Log Retention Method: overwrite-as-needed
Max Log Size: 16384
File Security:
    /vol1/home
    /vol1/dir1
Kerberos:
    Max Clock Skew: 5
    Max Ticket Age: 10
    Max Renew Age: 7
Privilege Rights:
    Take Ownership: usr1, usr2
    Security Privilege: usr1, usr2
    Change Notify: usr1, usr2
Registry Values:
    Signing Required: false
Restrict Anonymous:
    No enumeration of SAM accounts: true
    No enumeration of SAM accounts and shares: false
    Restrict anonymous access to shares and named pipes: true
    Combined restriction for anonymous user: no-access
Restricted Groups:
    gpr1
    gpr2
Central Access Policy Settings:
    Policies: cap1
             cap2
```

## 関連情報

### CIFS サーバ上で GPO サポートを有効または無効にします

制限されたグループの **GPO** に関する詳細情報を表示します

Active Directory でグループポリシーオブジェクト（GPO）として定義されている制限されたグループ、および CIFS サーバに適用されている制限されたグループに関する詳細情報を表示できます。

このタスクについて

デフォルトでは、次の情報が表示されます。

- グループポリシー名
- グループポリシーのバージョン
- リンク

グループポリシーを設定するレベルを指定します。出力される値は次のとおりです。

- Local グループポリシーがONTAP で設定されている場合

- Site グループポリシーがドメインコントローラのサイトレベルで設定されている場合
- Domain グループポリシーがドメインコントローラのドメインレベルで設定されている場合
- OrganizationalUnit グループポリシーがドメインコントローラの組織単位（OU）レベルで設定されている場合
- RSOP さまざまなレベルで定義されたすべてのグループポリシーから派生した一連のポリシー

- 制限されたグループ名です
- 制限されたグループに属するユーザとグループ、および属さないユーザとグループ
- 制限されたグループが追加されているグループのリスト

グループは、ここに記載されているグループ以外のグループのメンバーになることもできます。

## ステップ

1. 次のいずれかの操作を実行し、制限されたグループのすべての GPO に関する情報を表示します。

情報を表示する制限されたグループのすべての GPO	入力するコマンド
Active Directory で定義されています	<code>vserver cifs group-policy restricted-group show-defined -vserver vserver_name</code>
CIFS サーバに適用されます	<code>vserver cifs group-policy restricted-group show-applied -vserver vserver_name</code>

## 例

次の例は、CIFS 対応の vs1 という名前の SVM が属する Active Directory ドメインで定義されている、制限されたグループの GPO に関する情報を表示します。

```
cluster1::> vsriver cifs group-policy restricted-group show-defined  
-vsriver vs1
```

```
Vsriver: vs1
```

```
-----
```

```
Group Policy Name: gp01  
Version: 16  
Link: OrganizationalUnit  
Group Name: group1  
Members: user1  
MemberOf: EXAMPLE\group9
```

```
Group Policy Name: Resultant Set of Policy  
Version: 0  
Link: RSOP  
Group Name: group1  
Members: user1  
MemberOf: EXAMPLE\group9
```

次の例は、CIFS 対応の SVM vs1 に適用されている、制限されたグループの GPO に関する情報を表示します。

```
cluster1::> vsriver cifs group-policy restricted-group show-applied  
-vsriver vs1
```

```
Vsriver: vs1
```

```
-----
```

```
Group Policy Name: gp01  
Version: 16  
Link: OrganizationalUnit  
Group Name: group1  
Members: user1  
MemberOf: EXAMPLE\group9
```

```
Group Policy Name: Resultant Set of Policy  
Version: 0  
Link: RSOP  
Group Name: group1  
Members: user1  
MemberOf: EXAMPLE\group9
```


GPO 設定に関する情報を表示します

集約型アクセスポリシーに関する情報を表示します

Active Directory で定義されている集約型アクセスポリシーに関する詳細情報を表示できます。また、グループポリシーオブジェクト（GPO）を介して CIFS サーバに適用されている集約型アクセスポリシーに関する情報も表示できます。

このタスクについて  
デフォルトでは、次の情報が表示されます。

- SVM 名
- 集約型アクセスポリシーの名前
- SID
- 説明
- 作成時間
- 修正日時
- メンバールール



ワークグループモードの CIFS サーバについては、GPO をサポートしていないため情報は表示されません。

ステップ

1. 次のいずれかの操作を実行し、集約型アクセスポリシーに関する情報を表示します。

情報を表示するすべての集約型アクセスポリシー	入力するコマンド
Active Directory で定義されています	<code>vserver cifs group-policy central-access-policy show-defined -vserver vserver_name</code>
CIFS サーバに適用されます	<code>vserver cifs group-policy central-access-policy show-applied -vserver vserver_name</code>

例

次の例は、Active Directory で定義されているすべての集約型アクセスポリシーの情報を表示します。

```
cluster1::> vserver cifs group-policy central-access-policy show-defined
```

```
Vserver   Name                               SID
-----
-----
vs1       p1                               S-1-17-3386172923-1132988875-3044489393-
3993546205
        Description: policy #1
        Creation Time: Tue Oct 22 09:34:13 2013
        Modification Time: Wed Oct 23 08:59:15 2013
        Member Rules: r1

vs1       p2                               S-1-17-1885229282-1100162114-134354072-
822349040
        Description: policy #2
        Creation Time: Tue Oct 22 10:28:20 2013
        Modification Time: Thu Oct 31 10:25:32 2013
        Member Rules: r1
                        r2
```

次の例は、クラスタ上の Storage Virtual Machine（SVM）に適用されているすべての集約型アクセスポリシーの情報を表示します。

```
cluster1::> vserver cifs group-policy central-access-policy show-applied
```

```
Vserver   Name                               SID
-----
-----
vs1       p1                               S-1-17-3386172923-1132988875-3044489393-
3993546205
        Description: policy #1
        Creation Time: Tue Oct 22 09:34:13 2013
        Modification Time: Wed Oct 23 08:59:15 2013
        Member Rules: r1

vs1       p2                               S-1-17-1885229282-1100162114-134354072-
822349040
        Description: policy #2
        Creation Time: Tue Oct 22 10:28:20 2013
        Modification Time: Thu Oct 31 10:25:32 2013
        Member Rules: r1
                        r2
```

DAC（ダイナミックアクセス制御）を使用したファイルアクセスの保護

GPO 設定に関する情報を表示します

集約型アクセスポリシールールに関する情報を表示します

集約型アクセスポリシールールに関する情報を表示します

Active Directory で定義されている集約型アクセスポリシーに関連付けられた集約型アクセスポリシールールに関する詳細情報を表示できます。また、集約型アクセスポリシーの GPO（グループポリシーオブジェクト）を介して CIFS サーバに適用されている集約型アクセスポリシールールに関する情報も表示できます。

このタスクについて

定義および適用されている集約型アクセスポリシールールに関する詳細情報を表示できます。デフォルトでは、次の情報が表示されます。

- SVM 名です
- 集約型アクセスルールの名前
- 説明
- 作成時間
- 修正日時
- 現在の権限
- 推奨される権限
- ターゲットリソース

集約型アクセスポリシーに関連付けられた、情報を表示するすべての集約型アクセスポリシールール	入力するコマンド
Active Directory で定義されています	<code>vserver cifs group-policy central-access-rule show-defined -vserver vserver_name</code>
CIFS サーバに適用されます	<code>vserver cifs group-policy central-access-rule show-applied -vserver vserver_name</code>

例

次の例は、Active Directory で定義されている集約型アクセスポリシーに関連付けられたすべての集約型アクセスポリシールールの情報を表示します。



```
cluster1::> vservers cifs group-policy central-access-rule show-defined
```

```
Vserver      Name
-----
vs1          r1
            Description: rule #1
            Creation Time: Tue Oct 22 09:33:48 2013
            Modification Time: Tue Oct 22 09:33:48 2013
            Current Permissions: O:SYG:SYD:AR(A;;FA;;;WD)
            Proposed Permissions: O:SYG:SYD:(A;;FA;;;OW)(A;;FA;;;BA)(A;;FA;;;SY)

vs1          r2
            Description: rule #2
            Creation Time: Tue Oct 22 10:27:57 2013
            Modification Time: Tue Oct 22 10:27:57 2013
            Current Permissions: O:SYG:SYD:AR(A;;FA;;;WD)
            Proposed Permissions: O:SYG:SYD:(A;;FA;;;OW)(A;;FA;;;BA)(A;;FA;;;SY)
```

次の例は、クラスタ上で Storage Virtual Machine（SVM）に適用されている集約型アクセスポリシーに関連付けられたすべての集約型アクセスポリシールールの情報を表示します。

```
cluster1::> vservers cifs group-policy central-access-rule show-applied
```

```
Vserver      Name
-----
vs1          r1
            Description: rule #1
            Creation Time: Tue Oct 22 09:33:48 2013
            Modification Time: Tue Oct 22 09:33:48 2013
            Current Permissions: O:SYG:SYD:AR(A;;FA;;;WD)
            Proposed Permissions: O:SYG:SYD:(A;;FA;;;OW)(A;;FA;;;BA)(A;;FA;;;SY)

vs1          r2
            Description: rule #2
            Creation Time: Tue Oct 22 10:27:57 2013
            Modification Time: Tue Oct 22 10:27:57 2013
            Current Permissions: O:SYG:SYD:AR(A;;FA;;;WD)
            Proposed Permissions: O:SYG:SYD:(A;;FA;;;OW)(A;;FA;;;BA)(A;;FA;;;SY)
```

## 関連情報

[DAC（ダイナミックアクセス制御）を使用したファイルアクセスの保護](#)

[GPO 設定に関する情報を表示します](#)

[集約型アクセスポリシーに関する情報を表示します](#)

**SMBサーバコンピュータアカウントパスワードの管理用コマンド**

パスワードの変更、リセット、無効化、および自動更新スケジュールの設定に使用するコマンドについて説明します。SMBサーバでスケジュールを設定して自動的に更新することもできます。

状況	使用するコマンド
ドメインアカウントのパスワードを変更またはリセットします。パスワードがわかっている場合	<code>vserver cifs domain password change</code>
ドメインアカウントパスワードをリセットします。パスワードがわからない場合	<code>vserver cifs domain password reset</code>
コンピュータアカウントパスワードの自動変更を行うために SMB サーバを設定する	<code>vserver cifs domain password schedule modify -vserver vserver_name -is -schedule-enabled true</code>
SMBサーバでのコンピュータアカウントパスワードの自動変更の無効化	<code>vserver cifs domain password schedule modify -vserver vs1 -is-schedule-enabled false</code>

詳細については、各コマンドのマニュアルページを参照してください。

ドメインコントローラ接続を管理します

検出されたサーバに関する情報を表示します

CIFS サーバで検出された LDAP サーバおよびドメインコントローラに関する情報を表示できます。

**ステップ**

1. 検出されたサーバに関する情報を表示するには、次のコマンドを入力します。 `vserver cifs domain discovered-servers show`

**例**

次の例は、SVM vs1 で検出されたサーバを表示します。

```
cluster1::> vserver cifs domain discovered-servers show
```

```
Node: node1  
Vserver: vs1
```

Domain Name	Type	Preference	DC-Name	DC-Address	Status
example.com	MS-LDAP	adequate	DC-1	1.1.3.4	OK
example.com	MS-LDAP	adequate	DC-2	1.1.3.5	OK
example.com	MS-DC	adequate	DC-1	1.1.3.4	OK
example.com	MS-DC	adequate	DC-2	1.1.3.5	OK

## 関連情報

### サーバのリセットおよび再検出

#### CIFS サーバを停止または起動しています

サーバをリセットおよび再検出します

CIFS サーバでサーバのリセットと再検出を行うと、LDAP サーバおよびドメインコントローラに格納されている情報が CIFS サーバに破棄されます。サーバの情報が破棄されたあと、それらの外部サーバに関する最新の情報が再取得されます。これは、接続されているサーバが適切に応答しない場合に役立ちます。

## 手順

1. 次のコマンドを入力します。 `vserver cifs domain discovered-servers reset-servers -vserver vserver_name`
2. 再検出されたサーバに関する情報を表示します。 `vserver cifs domain discovered-servers show -vserver vserver_name`

## 例

次の例は、Storage Virtual Machine（SVM、旧 Vserver）vs1 のサーバをリセットして再検出します。

```
cluster1::> vservers cifs domain discovered-servers reset-servers -vservers vs1
```

```
cluster1::> vservers cifs domain discovered-servers show
```

```
Node: node1  
Vserver: vs1
```

Domain Name	Type	Preference	DC-Name	DC-Address	Status
example.com	MS-LDAP	adequate	DC-1	1.1.3.4	OK
example.com	MS-LDAP	adequate	DC-2	1.1.3.5	OK
example.com	MS-DC	adequate	DC-1	1.1.3.4	OK
example.com	MS-DC	adequate	DC-2	1.1.3.5	OK

## 関連情報

[検出されたサーバに関する情報を表示する](#)

[CIFS サーバを停止または起動しています](#)

ドメインコントローラの検出を管理します

ONTAP 9.3 以降では、ドメインコントローラ（DC）の検出に使用するデフォルトプロセスを変更できます。サイトまたは優先 DC のプールに検出を制限できるため、環境によってはパフォーマンスの向上につながります。

### このタスクについて

デフォルトでは、任意の優先 DC、ローカルサイト内のすべての DC、およびすべてのリモート DC を含めて、使用可能なすべての DC が検出されます。そのため、一部の環境では、認証時および共有へのアクセス時にレイテンシが発生する可能性があります。使用する DC のプールが決まっている場合、またはリモート DC が不適切またはアクセスできない場合は、検出方法を変更できます。

ONTAP 9.3以降のリリースでは、`discovery-mode` のパラメータ `cifs domain discovered-servers` コマンドでは、次のいずれかの検出オプションを選択できます。

- ドメイン内のすべての DC が検出されます。
- ローカルサイト内の DC だけが検出されます。
  - `default-site` SMBサーバのパラメータは、`sites-and-services` でサイトに割り当てられていない LIF でこのモードを使用するように定義できます。
- サーバの検出は実行せず、優先 DC のみを使用するように SMB サーバを設定します。

このモードを使用するには、最初に SMB サーバに対して優先 DC を定義する必要があります。

## ステップ

1. 目的の検出オプションを指定します。 `vservers cifs domain discovered-servers discovery-`

```
mode modify -vserver vs1 -mode {all|site|none}
```

のオプション mode パラメータ：

- ° all

使用可能なすべての DC を検出します（デフォルト）。

- ° site

DC の検出対象をサイトに制限します。

- ° none

優先 DC のみを使用し、検出は実行しません。

優先ドメインコントローラを追加する

ONTAP は DNS を介してドメインコントローラを自動的に検出します。必要に応じて、特定のドメインに対する優先ドメインコントローラのリストにドメインコントローラを追加することができます。

このタスクについて

指定したドメインに優先ドメインコントローラリストがすでに存在する場合、新しいリストが既存のリストに統合されます。

ステップ

1. 優先ドメインコントローラのリストに追加するには、次のコマンドを入力します。+

```
vserver cifs domain preferred-dc add -vserver vs1 -domain cifs.lab.example.com  
-preferred-dc 172.17.102.25, 172.17.102.24
```

-vserver vs1 Storage Virtual Machine (SVM) 名を示します。

-domain cifs.lab.example.com 指定したドメインコントローラが属するドメインの完全修飾Active Directory名を指定します。

-preferred-dc 172.17.102.25, 172.17.102.24 は、優先ドメインコントローラの1つ以上のIPアドレスを優先順にカンマで区切って指定します。

例

次のコマンドでは、SVM vs1上のSMBサーバがcifs.lab.example.comドメインへの外部アクセスを管理するために使用する優先ドメインコントローラのリストに、ドメインコントローラ172.17.102.25と172.17.102.24を追加します。

```
cluster1::> vserver cifs domain preferred-dc add -vserver vs1 -domain  
cifs.lab.example.com -preferred-dc 172.17.102.25,172.17.102.24
```

関連情報

優先ドメインコントローラの管理用コマンド

優先ドメインコントローラの管理用コマンド

優先ドメインコントローラの追加、表示、削除を行うコマンドについて説明します。

状況	使用するコマンド
優先ドメインコントローラを追加する	<code>vserver cifs domain preferred-dc add</code>
優先ドメインコントローラを表示する	<code>vserver cifs domain preferred-dc show</code>
優先ドメインコントローラを削除する	<code>vserver cifs domain preferred-dc remove</code>

詳細については、各コマンドのマニュアルページを参照してください。

関連情報

優先ドメインコントローラの追加

ドメインコントローラへの **SMB2** 接続を有効にします

ONTAP 9.1 以降では、SMB バージョン 2.0 からドメインコントローラへの接続を有効にすることができます。これは、ドメインコントローラで SMB 1.0 を無効にしている場合は必須です。ONTAP 9.2 以降では、SMB2 がデフォルトで有効になります。


このタスクについて

。 `smb2-enabled-for-dc-connections` コマンドオプションを使用すると、使用しているONTAP のリリースに応じたシステムデフォルトが有効になります。ONTAP 9.1 のシステムデフォルトでは、SMB 1.0 が有効、SMB 2.0 が無効になります。ONTAP 9.2 のシステムデフォルトでは、SMB 1.0 が有効になり、SMB 2.0 が有効になります。ドメインコントローラは、最初に SMB 2.0 をネゴシエートし、失敗した場合は SMB 1.0 を使用します。

SMB 1.0 は、ONTAP からドメインコントローラに対して無効にすることができます。ONTAP 9.1 では、SMB 1.0 を無効にした場合、ドメインコントローラと通信するために SMB 2.0 を有効にする必要があります。

詳細情報：

- "有効なSMBのバージョンの確認"。
- "サポートされる SMB のバージョンと機能"。



状況 `-smb1-enabled-for-dc-connections` がに設定されます `false` 間 `-smb1-enabled` がに設定されます `true` ONTAP では、クライアントとしてのSMB 1.0の接続は拒否されますが、サーバとしてのSMB 1.0のインバウンド接続は引き続き受け入れます。

手順

1. SMBセキュリティ設定を変更する前に、有効になっているSMBのバージョンを確認します。 `vserver cifs security show`

2. リストを下にスクロールして SMB のバージョンを確認します。
3. を使用して、該当するコマンドを実行します `smb2-enabled-for-dc-connections` オプション

SMB2 の設定	入力するコマンド
有効	<code>vserver cifs security modify -vserver vserver_name -smb2-enabled-for-dc-connections true</code>
無効	<code>vserver cifs security modify -vserver vserver_name -smb2-enabled-for-dc-connections false</code>

ドメインコントローラへの暗号化接続を有効にします

ONTAP 9.8 以降では、ドメインコントローラへの接続を暗号化するように指定できます。

このタスクについて

ONTAP では、ドメインコントローラ (DC) 通信の暗号化が必要です `-encryption-required-for-dc-connection` オプションはに設定されています `true`; デフォルトは `false` です。このオプションを設定すると、SMB3 でのみ暗号化がサポートされるため、SMB3 プロトコルのみが使用されます。

暗号化された DC 通信が必要な場合は、を参照してください `-smb2-enabled-for-dc-connections` ONTAP は SMB3 接続のみをネゴシエートするため、このオプションは無視されます。DC が SMB3 と暗号化をサポートしていない場合、ONTAP は接続しません。

ステップ

1. DC との暗号化通信を有効にします。 `vserver cifs security modify -vserver svm_name -encryption-required-for-dc-connection true`

非 **Kerberos** 環境のストレージにアクセスするには、**null** セッションを使用します

非 **Kerberos** 環境でストレージにアクセスする場合は、**null** セッションを使用します

**null** セッションアクセスは、ローカルシステムで稼働しているクライアントベースのサービスにストレージシステムデータなどのネットワークリソースへのアクセスを提供します。**null** セッションは、クライアントプロセスが「システム」アカウントを使用してネットワークリソースにアクセスするときに発生します。**null** セッション設定は非 **Kerberos** 認証に固有です。

ストレージシステムによる **null** セッションアクセスの実現方法

**null** セッション共有には認証が必要ないため、**null** セッションアクセスが必要なクライアントは、その IP アドレスがストレージシステムにマッピングされている必要があります。

デフォルトでは、マッピングされていない **null** セッションクライアントは、共有の列挙など一部の ONTAP シ

システムサービスにはアクセスできますが、ストレージシステムデータへのアクセスは制限されます。



ONTAP は、でWindows RestrictAnonymousレジストリ設定値をサポートしています  
-restrict-anonymous オプションこれにより、マッピングされていない null ユーザが表示  
またはアクセスできるシステムリソースの範囲を制御できます。たとえば、共有の一覧や IPC\$  
共有（非表示の名前付きパイプ共有）へのアクセスを無効にできます。。 vserver cifs  
options modify および vserver cifs options show の詳細については、のマニュアル  
ページを参照してください -restrict-anonymous オプション

特に設定がないかぎり、null セッションでストレージシステムアクセスを要求するローカルプロセスを実行しているクライアントは、「everyone」などの制限のないグループのみのメンバーとなります。null セッションアクセスを選択したストレージシステムリソースに制限するには、すべての null セッションクライアントが属するグループを作成します。このグループを作成すると、ストレージシステムアクセスを制限したり、null セッションクライアントのみに適用されるストレージシステムリソース権限を設定したりできます。

ONTAP には、マッピング構文が用意されています vserver name-mapping nullユーザセッションを使用したストレージシステムリソースへのアクセスを許可するクライアントのIPアドレスを指定するコマンドセット。null ユーザ用のグループを作成したら、null セッションのみに適用されるストレージシステムリソースのアクセス制限およびリソース権限を指定できます。null ユーザは匿名ログオンとみなされます。null ユーザは、ホームディレクトリにアクセスできません。

マッピングされた IP アドレスからストレージシステムにアクセスするすべての null ユーザには、マッピングされたユーザ権限が付与されます。null ユーザにマッピングされたストレージシステムへの不正なアクセスを防止するため、適切な予防措置を検討してください。最大限の保護を実現するには、ストレージシステムと null ユーザによるストレージシステムアクセスが必要なすべてのクライアントを別のネットワークに配置し、IP アドレス「SVM」の問題を解消します。

## 関連情報

### 匿名ユーザのアクセス制限を設定します

null ユーザにファイルシステム共有へのアクセスを許可します

null セッションクライアントによるストレージシステムリソースへのアクセスを許可するには、null セッションクライアントに使用するグループを割り当てて null セッションクライアントの IP アドレスを記録し、ストレージシステム上の、null セッションを使用したデータアクセスを許可するクライアントリストにその IP アドレスを追加します。

## 手順

1. を使用します vserver name-mapping create IP修飾子を使用して、nullユーザを任意の有効なWindowsユーザにマッピングするコマンド。

次のコマンドは、有効なホスト名 google.com で user1 に null ユーザをマッピングします。

```
vserver name-mapping create -direction win-unix -position 1 -pattern  
"ANONYMOUS LOGON" -replacement user1 - hostname google.com
```

次のコマンドは、有効な IP アドレス 10.238.2.54/32 で user1 に null ユーザをマッピングします。



```
vserver name-mapping create -direction win-unix -position 2 -pattern
"ANONYMOUS LOGON" -replacement user1 -address 10.238.2.54/32
```

2. を使用します `vserver name-mapping show` コマンドを入力してネームマッピングを確認します。

```
vserver name-mapping show

Vserver:    vs1
Direction:  win-unix
Position Hostname      IP Address/Mask
-----
1          -           10.72.40.83/32      Pattern: anonymous logon
                                   Replacement: user1
```

3. を使用します `vserver cifs options modify -win-name-for-null-user` nullユーザにWindowsメンバーシップを割り当てるコマンド。

このオプションは、null ユーザに有効なネームマッピングが設定されている場合にのみ使用できます。

```
vserver cifs options modify -win-name-for-null-user user1
```

4. を使用します `vserver cifs options show` コマンドを使用して、nullユーザのWindowsユーザまたはグループへのマッピングを確認します。

```
vserver cifs options show

Vserver :vs1

Map Null User to Windows User of Group: user1
```

## SMB サーバの NetBIOS エイリアスを管理します

### SMB サーバ用の NetBIOS エイリアスの概要を管理します

NetBIOS エイリアスは、SMB クライアントが SMB サーバに接続するときに使用できる SMB サーバの別名です。SMB サーバの NetBIOS エイリアスを設定すると、他のファイルサーバのデータを SMB サーバに統合して、SMB サーバが元のファイルサーバの名前に応答するようにする場合に役立ちます。

SMB サーバの作成時または SMB サーバ作成後の任意の時点で、NetBIOS エイリアスのリストを指定できます。リストへの NetBIOS エイリアスの追加や削除は、いつでも行うことができます。SMB サーバには NetBIOS エイリアスリスト内のどの名前を使用しても接続できます。

## 関連情報

### NetBIOS over TCP 接続に関する情報を表示する

#### SMBサーバにNetBIOSエイリアスのリストを追加する

エイリアスを使用してSMBサーバに接続できるようにするには、NetBIOSエイリアスのリストを作成するか、既存のNetBIOSエイリアスのリストにNetBIOSエイリアスを追加します。

#### このタスクについて

- NetBIOS エイリアス名は 15 文字以内にする必要があります。
- SMBサーバには最大200個のNetBIOSエイリアスを設定できます。
- 次の文字は使用できません。

@#\* () =+[] ; : " , <> \ ?

#### 手順

1. NetBIOSエイリアスを追加します。+

```
vserver cifs add-netbios-aliases -vserver vserver_name -netbios-aliases  
NetBIOS_alias,...
```

```
vserver cifs add-netbios-aliases -vserver vs1 -netbios-aliases  
alias_1,alias_2,alias_3
```

- 1 つ以上の NetBIOS エイリアスをカンマで区切って指定します。
- 指定した NetBIOS エイリアスが既存のリストに追加されます。
- 現在のリストが空である場合、NetBIOS エイリアスの新しいリストが作成されます。

2. NetBIOSエイリアスが正しく追加されたことを確認します。 `vserver cifs show -vserver vserver_name -display-netbios-aliases`

```
vserver cifs show -vserver vs1 -display-netbios-aliases
```

```
Vserver: vs1
```

```
Server Name: CIFS_SERVER
```

```
NetBIOS Aliases: ALIAS_1, ALIAS_2, ALIAS_3
```

## 関連情報

### NetBIOS エイリアスリストからの NetBIOS エイリアスの削除

#### CIFS サーバの NetBIOS エイリアスのリストを表示する

#### NetBIOS エイリアスリストから NetBIOS エイリアスを削除します

CIFS サーバで特定の NetBIOS エイリアスが不要な場合、その NetBIOS エイリアスをリ

ストから削除できます。リストからすべての NetBIOS エイリアスを削除することもできます。

このタスクについて

複数の NetBIOS エイリアスを削除するには、カンマで区切って指定します。を指定すると、CIFSサーバ上のすべてのNetBIOSエイリアスを削除できます - をの値として指定します -netbios-aliases パラメータ

手順

1. 次のいずれかを実行します。

削除する項目	入力するコマンド
リスト内の特定の NetBIOS エイリアス	<pre>vserver cifs remove-netbios-aliases -vserver _vserver_name_ -netbios -aliases _NetBIOS_alias_,...</pre>
リスト内のすべての NetBIOS エイリアス	<pre>vserver cifs remove-netbios-aliases -vserver vserver_name -netbios-aliases -</pre>

```
vserver cifs remove-netbios-aliases -vserver vs1 -netbios-aliases alias_1
```

2. 指定したNetBIOSエイリアスが削除されたことを確認します。 `vserver cifs show -vserver vserver_name -display-netbios-aliases`

```
vserver cifs show -vserver vs1 -display-netbios-aliases
```

```
Vserver: vs1
```

```
Server Name: CIFS_SERVER
```

```
NetBIOS Aliases: ALIAS_2, ALIAS_3
```

**CIFS** サーバの **NetBIOS** エイリアスのリストを表示します

NetBIOS エイリアスのリストを表示できます。これは、SMB クライアントが CIFS サーバへの接続に使用できる名前を確認する場合に役立ちます。

ステップ

1. 次のいずれかを実行します。

表示する情報	入力するコマンド
CIFS サーバの NetBIOS エイリアス	<pre>vserver cifs show -display-netbios -aliases</pre>

表示する情報	入力するコマンド
NetBIOS エイリアスのリストを含む詳細な CIFS サーバ情報	<code>vserver cifs show -instance</code>

次の例は、CIFS サーバの NetBIOS エイリアスに関する情報を表示します。

```
vserver cifs show -display-netbios-aliases
```

```
Vserver: vs1

      Server Name: CIFS_SERVER
      NetBIOS Aliases: ALIAS_1, ALIAS_2, ALIAS_3
```

次の例は、NetBIOS エイリアスのリストを CIFS サーバの詳細情報の一部として表示します。

```
vserver cifs show -instance
```

```

                                Vserver: vs1
                                CIFS Server NetBIOS Name: CIFS_SERVER
                                NetBIOS Domain/Workgroup Name: EXAMPLE
                                Fully Qualified Domain Name: EXAMPLE.COM
Default Site Used by LIFs Without Site Membership:
                                Authentication Style: domain
                                CIFS Server Administrative Status: up
                                CIFS Server Description:
                                List of NetBIOS Aliases: ALIAS_1, ALIAS_2,
ALIAS_3
```

詳細については、コマンドのマニュアルページを参照してください。

## 関連情報

[CIFS サーバへの NetBIOS エイリアスのリストの追加](#)

[CIFS サーバの管理用コマンド](#)

**SMB** クライアントが **NetBIOS** エイリアスを使用して接続しているかどうかを確認します

SMB クライアントが NetBIOS エイリアスを使用して接続しているかどうか、および使用している場合はその NetBIOS エイリアスを確認できます。これは、接続の問題のトラブルシューティングを行う場合に役立ちます。

## このタスクについて

を使用する必要があります `-instance` SMB 接続に関連付けられている NetBIOS エイリアス（ある場合）を表示するためのパラメータ。CIFS サーバの名前または IP アドレスを使用して SMB 接続を確立している場合は、

の出力が表示されます NetBIOS Name フィールドはです - (ハイフン)。

## ステップ

1. 必要な操作を実行します。

表示する <b>NetBIOS</b> 情報	入力するコマンド
SMBセツソク	<code>vserver cifs session show -instance</code>
指定した NetBIOS エイリアスを使用する接続：	<code>vserver cifs session show -instance -netbios-name netbios_name</code>

次の例は、セッション ID 1 の SMB 接続に使用されている NetBIOS エイリアスに関する情報を表示します。

```
vserver cifs session show -session-id 1 -instance
```

```
Node: node1
Vserver: vs1
Session ID: 1
Connection ID: 127834
Incoming Data LIF IP Address: 10.1.1.25
Workstation: 10.2.2.50
Authentication Mechanism: NTLMv2
Windows User: EXAMPLE\user1
UNIX User: user1
Open Shares: 2
Open Files: 2
Open Other: 0
Connected Time: 1d 1h 10m 5s
Idle Time: 22s
Protocol Version: SMB3
Continuously Available: No
Is Session Signed: true
User Authenticated as: domain-user
NetBIOS Name: ALIAS1
SMB Encryption Status: Unencrypted
```

その他の **SMB** サーバタスクを管理します

**CIFS** サーバを停止または起動します

ユーザが SMB 共有を介してデータにアクセスしていない間に作業を行う場合は、SVM 上の CIFS サーバを停止すると便利です。SMB アクセスを再開するには、CIFS サーバを起動します。CIFS サーバを停止することによって、Storage Virtual Machine (SVM

）で許可されているプロトコルを変更できます。

手順

1. 次のいずれかを実行します。

状況	入力するコマンド
CIFS サーバを停止します	<code>`vserver cifs stop -vserver vserver_name [-foreground {true</code>
<code>false}]`</code>	CIFS サーバを起動します
<code>`vserver cifs start -vserver vserver_name [-foreground {true</code>	<code>false}]`</code>

`-foreground` コマンドをフォアグラウンドとバックグラウンドのどちらで実行するかを指定します。省略した場合、このパラメータはに設定されます ``true`` コマンドはフォアグラウンドで実行されます。

2. を使用して、CIFSサーバの管理ステータスが正しいことを確認します `vserver cifs show` コマンドを実行します

例

次のコマンドは、SVM vs1 の CIFS サーバを起動します。

```
cluster1::> vserver cifs start -vserver vs1

cluster1::> vserver cifs show -vserver vs1

Vserver: vs1
CIFS Server NetBIOS Name: VS1
NetBIOS Domain/Workgroup Name: DOMAIN
Fully Qualified Domain Name: DOMAIN.LOCAL
Default Site Used by LIFs Without Site Membership:
Authentication Style: domain
CIFS Server Administrative Status: up
```

関連情報

[検出されたサーバに関する情報を表示する](#)

[サーバのリセットおよび再検出](#)

**CIFS** サーバを別の **OU** に移動します

CIFS サーバの create プロセスでは、別の OU を指定しないかぎり、セットアップ時にデフォルトの Organizational Unit （OU；組織単位）CN=Computers が使用されます。CIFS サーバはセットアップ後でも別の OU に移動できます。

## 手順

1. Windows サーバーで、 \* Active Directory ユーザーとコンピューター \* ツリーを開きます。
2. Storage Virtual Machine （ SVM ） の Active Directory オブジェクトを見つけます。
3. オブジェクトを右クリックし、 \* 移動 \* （ \* Move \* ） を選択します。
4. SVM に関連付ける OU を選択します

## 結果

選択した OU に、 SVM オブジェクトが移動します。

**SMB** サーバを移動する前に、 **SVM** 上の動的 **DNS** ドメインを変更します

SMB サーバを別のドメインに移動する際に、 SMB サーバの DNS レコードが Active Directory に統合された DNS サーバによって DNS に動的に登録されるようにするには、 SMB サーバを移動する前に Storage Virtual Machine （ SVM ） 上の動的 DNS （ DDNS ） を変更する必要があります。

### 作業を開始する前に

SMB サーバコンピュータアカウントを含む新しいドメインのサービスロケーションレコードを含む DNS ドメインを使用するには、 SVM で DNS ネームサービスを変更する必要があります。セキュア DDNS を使用している場合は、 Active Directory に統合された DNS ネームサーバを使用する必要があります。

### このタスクについて

DDNS （ SVM 上で設定されている場合）はデータ LIF の DNS レコードを新しいドメインに自動的に追加しますが、元のドメインの DNS レコードは元の DNS サーバから自動的に削除されません。手動で削除する必要があります。

SMB サーバを移動する前に DDNS の変更を完了するには、次のトピックを参照してください。

### "動的 DNS サービスを設定する"

**SVM** を **Active Directory** ドメインに追加します

を使用してドメインを変更すると、既存のSMBサーバを削除することなくStorage Virtual Machine（SVM）をActive Directoryドメインに追加できます `vserver cifs modify` コマンドを実行します現在のドメインに参加しなおすことも、新しいドメインに参加することもできます。

### 作業を開始する前に

- SVM の DNS 設定が完了している必要があります。
- SVM の DNS 設定がターゲットドメインを提供できる必要があります。

DNS サーバには、ドメイン LDAP およびドメインコントローラサーバのサービスロケーションレコード（ SRV ） が含まれている必要があります。

### このタスクについて

- Active Directory ドメインの変更を続行するには、 CIFS サーバの管理ステータスを「所有」に設定する必要があります。

- コマンドが正常に完了すると、管理ステータスは自動的に「up」に設定されます。
- ドメインに参加する場合、このコマンドの実行には数分かかることがあります。

#### 手順

1. SVMをCIFSサーバドメインに追加します。 `vserver cifs modify -vserver vserver_name -domain domain_name -status-admin down`

詳細については、のマニュアルページを参照してください `vserver cifs modify` コマンドを実行します新しいドメイン用にDNSを再設定する必要がある場合は、のマニュアルページを参照してください `vserver dns modify` コマンドを実行します

SMBサーバのActive Directoryマシンアカウントを作成するには、にコンピュータを追加するための十分な権限があるWindowsアカウントの名前とパスワードを指定する必要があります `ou= example ou` 内のコンテンツ `example.com` ドメイン。

ONTAP 9.7 以降では、権限がある Windows アカウントの名前とパスワードの代わりに、 `keytab` ファイルの URI を AD 管理者から提供される場合があります。URIを受け取ったら、に含めます `-keytab-uri` パラメータと `vserver cifs` コマンド

2. CIFSサーバが目的のActive Directoryドメイン内にあることを確認します。 `vserver cifs show`

#### 例

次の例では、SVM `vs1` 上にある SMB サーバ「`CIFSSERVER1`」を `keytab` 認証を使用して `example.com` ドメインに追加します。

```
cluster1::> vserver cifs modify -vserver vs1 -domain example.com -status
-admin down -keytab-uri http://admin.example.com/ontap1.keytab
```

```
cluster1::> vserver cifs show
```

	Server	Status	Domain/Workgroup	Authentication
Vserver	Name	Admin	Name	Style
-----	-----	-----	-----	-----
vs1	CIFSSERVER1	up	EXAMPLE	domain

#### NetBIOS over TCP 接続に関する情報を表示します

NetBIOS over TCP（NBT）接続に関する情報を表示できます。これは、NetBIOSに関連する問題のトラブルシューティングを行う場合に役立ちます。

#### ステップ

1. を使用します `vserver cifs nbtstat` NetBIOS over TCP接続に関する情報を表示するコマンド。



IPv6 経由の NetBIOS ネームサービス（NBNS）はサポートされていません。

#### 例



次の例は、「cluster1」について表示される NetBIOS ネームサービスの情報を示しています。

```
cluster1::> vservice cifs nbtstat

Vservice: vs1
Node:      cluster1-01
Interfaces:
            10.10.10.32
            10.10.10.33
Servers:
            17.17.1.2  (active  )
NBT Scope:
            [ ]
NBT Mode:
            [h]
NBT Name    NetBIOS Suffix    State    Time Left    Type
-----
CLUSTER_1   00                          wins     57
CLUSTER_1   20                          wins     57

Vservice: vs1
Node:      cluster1-02
Interfaces:
            10.10.10.35
Servers:
            17.17.1.2  (active  )
CLUSTER_1   00                          wins     58
CLUSTER_1   20                          wins     58
4 entries were displayed.
```

**SMBサーバの管理用コマンド**

作成、表示、変更、停止、開始、 およびSMBサーバを削除しています。また、サーバのリセットと再検出、マシンアカウントパスワードの変更またはリセット、マシンアカウントパスワードのスケジュール変更、 NetBIOS エイリアスの追加または削除を行うコマンドもあります。

状況	使用するコマンド
SMB サーバを作成	vservice cifs create
SMB サーバに関する情報を表示する	vservice cifs show
SMBサーバを変更する	vservice cifs modify

SMB サーバを別のドメインに移動する	<code>vserver cifs modify</code>
SMB サーバを停止	<code>vserver cifs stop</code>
SMB サーバを起動	<code>vserver cifs start</code>
SMBサーバを削除する	<code>vserver cifs delete</code>
SMBサーバ用のサーバのリセットと再検出	<code>vserver cifs domain discovered-servers reset-servers</code>
SMBサーバのマシンアカウントパスワードを変更する	<code>vserver cifs domain password change</code>
SMBサーバのマシンアカウントパスワードをリセットする	<code>vserver cifs domain password change</code>
SMBサーバのマシンアカウントの自動パスワード変更のスケジュールを設定する	<code>vserver cifs domain password schedule modify</code>
SMBサーバ用のNetBIOSエイリアスを追加する	<code>vserver cifs add-netbios-aliases</code>
SMBサーバのNetBIOSエイリアスを削除する	<code>vserver cifs remove-netbios-aliases</code>

詳細については、各コマンドのマニュアルページを参照してください。

#### 関連情報

["SMB サーバを削除したときにローカルユーザとローカルグループが受ける影響"](#)

#### NetBIOS ネームサービスを有効にします

ONTAP 9 以降では、NetBIOS ネームサービス（NBNS、Windows Internet Name Service または WINS と呼ばれることもあります）はデフォルトで無効になっています。以前は、WINS がネットワークで有効かどうかに関係なく、CIFS 対応 Storage Virtual Machine（SVM）が名前登録のブロードキャストを送信していました。NBNS が必須の構成でのみこのブロードキャストが送信されるようにするには、新しい CIFS サーバに対して NBNS を明示的に有効にする必要があります。

#### 作業を開始する前に

- すでに NBNS を使用しているシステムを ONTAP 9 にアップグレードした場合、このタスクを実行する必要はありません。NBNS はそれまでと同様に機能します。
- NBNS は UDP（ポート 137）経由で有効になります。
- IPv6 経由の NBNS はサポートされていません。

## 手順

1. 権限レベルを advanced に設定します。

```
set -privilege advanced
```

2. CIFS サーバで NBNS を有効にします。

```
vserver cifs options modify -vserver <vserver name> -is-nbns-enabled  
true
```

3. admin 権限レベルに戻ります。

```
set -privilege admin
```

## SMB アクセスと SMB サービスに IPv6 を使用します

### IPv6 を使用するための要件

SMB サーバで IPv6 を使用する前に、この機能をサポートする ONTAP および SMB のバージョンとライセンスの要件について確認しておく必要があります。

### ONTAP ライセンスの要件：

SMB のライセンスがあれば、IPv6 を使用するために特別なライセンスは必要ありません。SMB ライセンスはに含まれています。"ONTAP One"。ONTAP Oneをお持ちでなく、ライセンスがインストールされていない場合は、営業担当者にお問い合わせください。

### SMB プロトコルのバージョン

- SVM について ONTAP は、すべてのバージョンの SMB プロトコルで IPv6 がサポートされます。



IPv6 経由の NetBIOS ネームサービス（NBNS）はサポートされていません。

### SMB アクセスと CIFS サービスでの IPv6 のサポート

CIFS サーバで IPv6 を使用する場合は、ONTAP による SMB アクセスや CIFS サービスとのネットワーク通信での IPv6 のサポートについて確認しておく必要があります。

### Windows クライアントおよびサーバのサポート

ONTAP では、IPv6 をサポートする Windows サーバおよびクライアントをサポートしています。次に、Microsoft Windows クライアントおよびサーバによる IPv6 のサポートについて説明します。

- Windows 7、Windows 8、Windows Server 2008、Windows Server 2012 以降では、SMB ファイル共有と、DNS、LDAP、CLDAP、Kerberos サービスなどの Active Directory サービスの両方で IPv6 が

サポートされます。

IPv6 アドレスが設定されている場合、Windows 7 および Windows Server 2008 以降のリリースでは、Active Directory サービスに対してデフォルトで IPv6 が使用されます。IPv6 接続による NTLM 認証と Kerberos 認証の両方がサポートされます。

ONTAP でサポートされる Windows クライアントでは、いずれも IPv6 アドレスを使用して SMB 共有に接続できます。

ONTAPがサポートするWindowsクライアントに関する最新情報については、を参照してください。"[互換性マトリックス](#)"。



NT ドメインは IPv6 ではサポートされません。

その他の **CIFS** サービスもサポートされます

ONTAP では、SMB ファイル共有と Active Directory サービスに加え、以下に対しても IPv6 をサポートしています。

- クライアント側のサービス：オフラインフォルダ、移動プロファイル、フォルダリダイレクト、以前のバージョン機能など
- サーバ側のサービス：動的ホームディレクトリの有効化（ホームディレクトリ機能）、シンボリックリンクとワイドリンク、BranchCache、ODX コピーオフロード、自動ノードリファラール、および以前のバージョン
- ファイルアクセス管理用のサービス：Windows のローカルユーザやローカルグループを使用したアクセス制御と権限の管理、CLI を使用したファイル権限や監査ポリシーの設定、セキュリティトレース、ファイルロックの管理、SMB アクティビティの監視などが可能です
- NAS のマルチプロトコルの監査
- FPolicy の
- 共有の継続的な可用性、監視プロトコル、およびリモート VSS（Hyper-V over SMB 構成で使用）

ネームサービスおよび認証サービスのサポート

次のネームサービスとの通信が IPv6 でサポートされます。

- ドメインコントローラ
- DNS サーバ
- LDAPサーバ
- KDCサーバ
- NISサーバ

**CIFS** サーバが **IPv6** を使用して外部サーバに接続する方法

要件に対応した設定を作成するには、CIFS サーバが外部サーバへの接続を確立するときに IPv6 がどのように使用されるかを確認しておく必要があります。

- 送信元アドレスの選択

外部サーバへの接続を試行する場合、選択する送信元アドレスは宛先アドレスと同じタイプでなければなりません。たとえば、IPv6 アドレスに接続する場合、CIFS サーバをホストする Storage Virtual Machine (SVM) には、送信元アドレスとして使用する IPv6 アドレスを持つデータ LIF または管理 LIF が必要です。同様に、IPv4 アドレスに接続する場合、SVM には、送信元アドレスとして使用する IPv4 アドレスを持つデータ LIF または管理 LIF が必要です。

- DNS を使用して動的に検出されるサーバの場合、サーバ検出は次のように実行されます。

- クラスタで IPv6 が無効になっている場合は、IPv4 サーバアドレスのみが検出されます。
- クラスタで IPv6 が有効になっている場合は、IPv4 と IPv6 の両方のサーバアドレスが検出されます。アドレスが属するサーバが適切かどうかと、IPv6 または IPv4 のデータ LIF または管理 LIF が使用可能かどうかに応じて、いずれかのタイプが使用されます。動的サーバ検出は、ドメインコントローラとその関連サービス (LSA、NETLOGON、Kerberos、LDAP など) の検出に使用されます。

- DNS サーバへの接続

SVM が DNS サーバに接続するときに IPv6 を使用するかどうかは、DNS ネームサービスの設定によって決まります。IPv6 アドレスを使用するように DNS サービスが設定されている場合は、IPv6 を使用して接続が確立されます。必要に応じて、DNS サーバへの接続に引き続き IPv4 アドレスが使用されるようにするため、DNS ネームサービスの設定で IPv4 アドレスを使用できます。DNS ネームサービスの設定時に、IPv4 アドレスと IPv6 アドレスを組み合わせて指定できます。

- LDAPサーバへの接続

SVM が LDAP サーバに接続するときに IPv6 を使用するかどうかは、LDAP クライアントの設定によって決まります。IPv6 アドレスを使用するように LDAP クライアントが設定されている場合は、IPv6 を使用して接続が確立されます。必要に応じて、LDAP サーバへの接続に引き続き IPv4 アドレスが使用されるようにするため、LDAP クライアントの設定で IPv4 アドレスを使用できます。LDAP クライアントの設定時に、IPv4 アドレスと IPv6 アドレスを組み合わせて指定できます。



LDAP クライアントの設定は、UNIX ユーザ、グループ、およびネットグループのネームサービス用に LDAP を設定するときに使用されます。

- NISサーバへの接続

SVMがNISサーバに接続するときにIPv6を使用するかどうかは、NISネームサービスの設定によって決まります。IPv6アドレスを使用するようにNISサービスが設定されている場合は、IPv6を使用して接続が確立されます。必要に応じて、NISサーバへの接続で引き続きIPv4アドレスを使用できるように、NISネームサービスの設定でIPv4アドレスを使用できます。NISネームサービスの設定時に、IPv4アドレスとIPv6アドレスを組み合わせて指定できます。



NIS ネームサービスは、UNIX ユーザ、グループ、ネットグループ、およびホスト名オブジェクトを格納および管理するために使用されます。

## 関連情報

[SMB での IPv6 の有効化 \(クラスタ管理者のみ\)](#)

[IPv6 SMB セッション情報の監視および表示](#)

IPv6 ネットワークはクラスタのセットアップ時には有効になりません。SMB で IPv6 を使用するには、クラスタのセットアップ後にクラスタ管理者が IPv6 を有効にする必要があります。クラスタ管理者が IPv6 を有効にすると、IPv6 はクラスタ全体で有効になります。

ステップ

1. IPv6を有効にします。 `network options ipv6 modify -enabled true`

クラスタでの IPv6 の有効化と IPv6 LIF の設定の詳細については、 [\\_ ネットワーク管理ガイド \\_](#) を参照してください。

IPv6 が有効になっている。SMB アクセス用の IPv6 データ LIF を設定できます。

関連情報

[IPv6 SMB セッション情報の監視および表示](#)

["Network Management の略"](#)

SMB で IPv6 を無効にします

クラスタで IPv6 を有効にするにはネットワークオプションを使用しますが、同じコマンドを使用して SMB での IPv6 を無効にすることはできません。代わりに、クラスタ管理者がクラスタで最後に IPv6 を有効にしたインターフェイスを無効にすると、ONTAP は IPv6 を無効にします。IPv6 を有効にしたインターフェイスの管理については、クラスタ管理者と連絡を取る必要があります。

クラスタでの IPv6 の無効化の詳細については、 [\\_ ネットワーク管理ガイド \\_](#) を参照してください。

関連情報

["Network Management の略"](#)

IPv6 SMB セッション情報を監視および表示します

IPv6 ネットワークで接続されている SMB セッション情報を監視および表示できます。この情報は、IPv6 SMB セッションに関する他の有用な情報と同様、IPv6 を使用して接続するクライアントを決定する上で役に立ちます。

ステップ

1. 必要な操作を実行します。

確認する項目	入力するコマンド
Storage Virtual Machine （SVM）への SMB セッションは、IPv6 を使用して接続されます	<code>vserver cifs session show -vserver vserver_name -instance</code>

確認する項目	入力するコマンド
特定の LIF アドレスにより、SMB セッションに IPv6 を使用します	<pre>vserver cifs session show -vserver vserver_name -lif-address LIF_IP_address -instance</pre> <p><i>LIF_IP_address</i> は、データLIFのIPv6アドレスです。</p>

## SMB を使用したファイルアクセスをセットアップする

### セキュリティ形式を設定する

セキュリティ形式がデータアクセスに与える影響

### セキュリティ形式とその影響とは

セキュリティ形式には、UNIX、NTFS、mixed、および unified の 4 種類があり、セキュリティ形式ごとにデータに対する権限の処理方法が異なります。目的に応じて適切なセキュリティ形式を選択できるように、それぞれの影響について理解しておく必要があります。

セキュリティ形式はデータにアクセスできるクライアントの種類には影響しないことに注意してください。セキュリティ形式で決まるのは、データアクセスの制御に ONTAP で使用される権限の種類と、それらの権限を変更できるクライアントの種類だけです。

たとえば、ボリュームで UNIX セキュリティ形式を使用している場合でも、ONTAP はマルチプロトコルに対応しているため、SMB クライアントから引き続きデータにアクセスできます（認証と許可が適切な場合）。ただし、ONTAP では、UNIX クライアントのみが標準のツールを使用して変更できる UNIX 権限が使用されます。

セキュリティ形式	権限を変更できるクライアント	クライアントが使用できる権限	有効になるセキュリティ形式	ファイルにアクセスできるクライアント
「UNIX」	NFS	NFSv3 モードビット	「UNIX」	NFS と SMB
NFSv4.x ACL	「UNIX」	NTFS	SMB	NTFS ACL
NTFS	混在	NFS または SMB	NFSv3 モードビット	「UNIX」
NFSv4.x ACL	「UNIX」	NTFS ACL	NTFS	統合：
NFS または SMB	NFSv3 モードビット	「UNIX」	NFSv4.1 ACL	「UNIX」

セキュリティ形式	権限を変更できるクライアント	クライアントが使用できる権限	有効になるセキュリティ形式	ファイルにアクセスできるクライアント
NTFS ACL	NTFS	統合： (ONTAP 9.4以前のリリースでは、Infinite Volumeのみ)。	NFS または SMB	NFSv3 モードビット
「UNIX」	NFSv4.1 ACL			NTFS ACL

FlexVol ボリュームでは、UNIX、NTFS、および mixed のセキュリティ形式がサポートされます。セキュリティ形式が mixed または unified の場合は、ユーザがセキュリティ形式を各自設定するため、権限を最後に変更したクライアントの種類によって有効になる権限が異なります。権限を最後に変更したクライアントが NFSv3 クライアントの場合、権限は UNIX NFSv3 モードビットになります。最後のクライアントが NFSv4 クライアントの場合、権限は NFSv4 ACL になります。最後のクライアントが SMB クライアントの場合、権限は Windows NTFS ACL になります。

unified セキュリティ形式は、Infinite Volume でのみ使用できます。Infinite Volume は、ONTAP 9.5 以降のリリースではサポートされなくなりました。詳細については、を参照してください "[FlexGroup ボリュームの管理の概要](#)"。

ONTAP 9.2以降では、show-effective-permissions パラメータをに設定します vserver security file-directory コマンドを使用すると、指定したファイルまたはフォルダパスに対してWindowsユーザまたはUNIXユーザに付与されている有効な権限を表示できます。また、オプションのパラメータも指定します -share-name 有効な共有権限を表示できます。



ONTAP で、最初にデフォルトのファイル権限がいくつか設定されます。デフォルトでは、UNIX、mixed、および unified のセキュリティ形式のボリュームにあるデータについては、セキュリティ形式は UNIX、権限の種類は UNIX モードビット（特に指定しないかぎり 0755）が有効になります。これは、デフォルトのセキュリティ形式で許可されたクライアントで設定するまで変わりません。NTFS セキュリティ形式のボリュームにあるデータについては、デフォルトで NTFS セキュリティ形式が有効になり、すべてのユーザにフルコントロール権限を許可する ACL が割り当てられます。

## セキュリティ形式を設定する場所とタイミング

セキュリティ形式は、FlexVol（ルートボリュームとデータボリュームの両方）および qtrees で設定できます。セキュリティ形式は、作成時に手動で設定することも、自動的に継承することも、あとで変更することもできます。

### SVM で使用するセキュリティ形式を決定します

ボリュームで使用するセキュリティ形式を決定するには、2つの要素を考慮する必要があります。第1の要素は、ファイルシステムを管理する管理者のタイプです。第2の要素は、ボリューム上のデータにアクセスするユーザまたはサービスのタイプです。

ボリュームのセキュリティ形式を設定するときは、最適なセキュリティ形式を選択して権限の管理に関する問題を回避するために、環境のニーズを考慮する必要があります。決定時には次の点を考慮すると役立ちます。



セキュリティ形式	以下の場合に選択
「UNIX」	<ul style="list-style-type: none"> <li>• ファイルシステムが UNIX 管理者によって管理される。</li> <li>• ユーザの大半が NFS クライアントである。</li> <li>• データにアクセスするアプリケーションで、サービスアカウントとして UNIX ユーザが使用される。</li> </ul>
NTFS	<ul style="list-style-type: none"> <li>• ファイルシステムは Windows 管理者によって管理されます。</li> <li>• ユーザの大部分がSMBクライアントです。</li> <li>• データにアクセスするアプリケーションで、サービスアカウントとして Windows ユーザが使用される。</li> </ul>
混在	ファイルシステムが UNIX 管理者と Windows 管理者の両方によって管理され、ユーザが NFS クライアントと SMB クライアントの両方で構成される。

#### セキュリティ形式の継承の仕組み

新しい FlexVol または qtree の作成時にセキュリティ形式を指定しない場合、セキュリティ形式はさまざまな方法で継承されます。

セキュリティ形式は、次のように継承されます。

- FlexVol ボリュームは、そのボリュームを含む SVM のルートボリュームのセキュリティ形式を継承します。
- qtree は、その qtree を含む FlexVol ボリュームのセキュリティ形式を継承します。
- ファイルまたはディレクトリは、そのファイルまたはディレクトリを含む FlexVol ボリュームまたは qtree のセキュリティ形式を継承します。

#### ONTAP による UNIX アクセス権の維持方法

UNIX アクセス権を現在持っている FlexVol ボリューム内のファイルが Windows アプリケーションによって編集および保存されても、ONTAP は UNIX アクセス権を維持できます。

Windows クライアントのアプリケーションは、ファイルを編集して保存するときに、ファイルのセキュリティプロパティを読み取り、新しい一時ファイルを作成し、それらのプロパティを一時ファイルに適用してから、一時ファイルに元のファイル名を付けます。

セキュリティプロパティのクエリを実行すると、Windows クライアントは、UNIX アクセス権を正確に表す構築済み ACL を受け取ります。この構築済み ACL は、Windows アプリケーションによってファイルが更新されるときにファイルの UNIX アクセス権を維持し、生成されたファイルが同じ UNIX アクセス権を持つようにするためだけに使用されます。ONTAP は、構築済み ACL を使用して NTFS ACL を設定しません。

**Windows** のセキュリティタブを使用して **UNIX** アクセス権を管理します

SVM 上の mixed セキュリティ形式のボリュームまたは qtree に含まれるファイルまたはフォルダの UNIX アクセス権を操作する場合は、Windows クライアントのセキュリティタブを使用できます。また、Windows ACL を照会および設定できるアプリケーションを使用することもできます。

- UNIX アクセス権の変更

Windows のセキュリティタブを使用して、mixed セキュリティ形式のボリュームまたは qtree の UNIX アクセス権を表示および変更できます。メインの [Windows Security] タブを使用して UNIX アクセス権を変更する場合は、編集する既存の ACE を削除してから（モードビットを 0 に設定）、変更を行う必要があります。または、高度なエディタを使用して権限を変更することもできます。

モードのアクセス権を使用している場合は、リストされた UID、GID、およびその他（コンピュータにアカウントを持つその他すべてのユーザ）のモードアクセス権を直接変更できます。たとえば、表示された UID に r-x のアクセス権が設定されている場合、この UID のアクセス権を rwx に変更できます。

- UNIX アクセス権を NTFS アクセス権に変更しています

Windows のセキュリティタブを使用して、ファイルおよびフォルダのセキュリティ形式が UNIX 対応である mixed 型セキュリティ形式のボリュームまたは qtree 上で、UNIX セキュリティオブジェクトを Windows セキュリティオブジェクトに置き換えることができます。

適切な Windows のユーザおよびグループのオブジェクトに置き換える前に、リストされている UNIX アクセス権のエントリをすべて削除しておく必要があります。次に、Windows のユーザおよびグループのオブジェクトに NTFS ベースの ACL を設定します。すべての UNIX セキュリティオブジェクトを削除し、Windows のユーザおよびグループのみを mixed セキュリティ形式のボリュームまたは qtree 上のファイルまたはフォルダに追加すると、ファイルまたはフォルダのセキュリティ形式が UNIX から NTFS へ変換されます。

フォルダの権限を変更する場合、Windows のデフォルトの動作では、すべてのサブフォルダとファイルにこれらの変更が反映されます。したがって、セキュリティ形式の変更をすべての子フォルダ、サブフォルダ、およびファイルに反映したくない場合は、反映する範囲を希望の範囲に変更する必要があります。

## **SVM** ルートボリュームのセキュリティ形式を設定する

Storage Virtual Machine（SVM）のルートボリューム上のデータに使用するアクセス権のタイプを決定するには、SVM ルートボリュームのセキュリティ形式を設定します。

### 手順

1. を使用します `vserver create` コマンドにを指定します `-rootvolume-security-style` セキュリティ形式を定義するパラメータ。

ルートボリュームのセキュリティ形式に指定できるオプションは、です `unix`、`ntfs` または `mixed`。

2. 作成した SVM のルートボリュームセキュリティ形式を含む設定を表示して確認します。 `vserver show -vserver vserver_name`

## FlexVol ボリュームのセキュリティ形式を設定する

Storage Virtual Machine（SVM）の FlexVol 上のデータに使用するアクセス権のタイプを決定するには、FlexVol のセキュリティ形式を設定します。

### 手順

1. 次のいずれかを実行します。

FlexVol ボリュームの状況	使用するコマンド
はまだ存在しません	<code>volume create</code> を含めます <code>-security-style</code> セキュリティ形式を指定するパラメータ。
はすでに存在します	<code>volume modify</code> を含めます <code>-security-style</code> セキュリティ形式を指定するパラメータ。

FlexVol のセキュリティ形式に指定できるオプションは、です `unix`、`ntfs` または `mixed`。

FlexVol ボリュームの作成時にセキュリティ形式を指定しない場合、ボリュームはルートボリュームのセキュリティ形式を継承します。

詳細については、を参照してください `volume create` または `volume modify` コマンド、を参照してください ["論理ストレージ管理"](#)。

2. 作成した FlexVol ボリュームのセキュリティ形式を含む設定を表示するには、次のコマンドを入力します。

```
volume show -volume volume_name -instance
```

## qtree にセキュリティ形式を設定する

qtree 上のデータに使用するアクセス権のタイプを決定するには、qtree のセキュリティ形式を設定します。

### 手順

1. 次のいずれかを実行します。

qtree の有無	使用するコマンド
はまだ存在しません	<code>volume qtree create</code> を含めます <code>-security-style</code> セキュリティ形式を指定するパラメータ。
はすでに存在します	<code>volume qtree modify</code> を含めます <code>-security-style</code> セキュリティ形式を指定するパラメータ。

qtreeセキュリティ形式に指定できるオプションは、です `unix`、`ntfs` または `mixed`。

qtreeの作成時にセキュリティ形式を指定しない場合、デフォルトのセキュリティ形式はです `mixed`。

詳細については、を参照してください `volume qtree create` または `volume qtree modify` コマンド、を参照してください "[論理ストレージ管理](#)"。

- 作成したqtreeのセキュリティ形式を含む設定を表示するには、次のコマンドを入力します。 `volume qtree show -qtree qtree_name -instance`

**NAS** ネームスペース内でデータボリュームを作成および管理します

**NAS** ネームスペースでのデータボリュームの作成と管理の概要

NAS 環境でファイルアクセスを管理するには、Storage Virtual Machine（SVM）上でデータボリュームおよびジャンクションポイントを管理する必要があります。これには、ネームスペースアーキテクチャの計画、ジャンクションポイントが設定されたボリュームまたはジャンクションポイントが設定されていないボリュームの作成、ボリュームのマウントまたはアンマウント、およびデータボリュームや NFS サーバまたは CIFS サーバのネームスペースに関する情報の表示が含まれます。

ジャンクションポイントを指定してデータボリュームを作成します

ジャンクションポイントはデータボリュームの作成時に指定できます。作成したボリュームは、ジャンクションポイントに自動的にマウントされ、NAS アクセス用の設定にすぐに使用できます。

作業を開始する前に

ボリュームを作成するアグリゲートがすでに存在している必要があります。



ジャンクションパスに次の文字を使用することはできません。 `*#<><|?\\`

また、ジャンクションパスの長さは 255 文字以下にする必要があります。

手順

- ジャンクションポイントを指定してボリュームを作成します。 `volume create -vserver vsERVER_name -volume volume_name -aggregate aggregate_name -size {integer[KB|MB|GB|TB|PB]} -security-style {ntfs|unix|mixed} -junction-path junction_path`

ジャンクションパスはルート（/）で始まる必要があり、ディレクトリおよび結合されたボリュームを含むことができます。ジャンクションパスにボリュームの名前を含める必要はありません。ジャンクションパスはボリューム名に依存しません。

ボリュームのセキュリティ形式の指定は任意です。セキュリティ形式を指定しない場合、ONTAP は、Storage Virtual Machine（SVM）のルートボリュームに適用されている形式と同じセキュリティ形式を使用してボリュームを作成します。ただし、ルートボリュームのセキュリティ形式が、作成するデータボリュームには適切でないセキュリティ形式である場合もあります。トラブルシューティングが困難なファイルアクセスの問題を最小限に抑えるため、ボリュームの作成時にセキュリティ形式を指定することを推奨します。

ジャンクションパスでは大文字と小文字が区別されません。/ENG はと同じです /eng。CIFS 共有を作成する場合、Windows では、ジャンクションパスがあたかも大文字と小文字の区別があるかのように扱わ

れます。たとえば、ジャンクションがの場合などです /ENG、CIFS共有のパスは次の文字で始まる必要があります。 /ENG`ではありません `/eng。

データボリュームのカスタマイズに使用できるオプションのパラメータが多数用意されています。これらの機能の詳細については、のマニュアルページを参照してください volume create コマンドを実行します

2. 目的のジャンクションポイントでボリュームが作成されたことを確認します。 volume show -vserver vs1 -volume volume\_name -junction

#### 例

次の例は、ジャンクションパスがである「home4」という名前のボリュームをSVM vs1上に作成します /eng/home :

```
cluster1::> volume create -vserver vs1 -volume home4 -aggregate aggr1
-size 1g -junction-path /eng/home
[Job 1642] Job succeeded: Successful

cluster1::> volume show -vserver vs1 -volume home4 -junction
```

Vserver	Volume	Active	Junction Path	Junction Path Source
vs1	home4	true	/eng/home	RW_volume

ジャンクションポイントを指定せずにデータボリュームを作成

ジャンクションポイントを指定せずにデータボリュームを作成できます。作成したボリュームは自動的にマウントされず、NAS アクセス用の設定に使用することはできません。ボリュームの SMB 共有または NFS エクスポートを設定する前に、ボリュームをマウントする必要があります。

作業を開始する前に

ボリュームを作成するアグリゲートがすでに存在している必要があります。

#### 手順

1. 次のコマンドを使用して、ジャンクションポイントが設定されていないボリュームを作成します。

```
volume create -vserver vs1 -volume volume_name -aggregate
aggregate_name -size {integer[KB|MB|GB|TB|PB]} -security-style
{ntfs|unix|mixed}
```

ボリュームのセキュリティ形式の指定は任意です。セキュリティ形式を指定しない場合、ONTAP は、Storage Virtual Machine (SVM) のルートボリュームに適用されている形式と同じセキュリティ形式を使用してボリュームを作成します。ただし、ルートボリュームのセキュリティ形式が、データボリュームには適切でないセキュリティ形式である場合もあります。トラブルシューティングが困難なファイルアクセスの問題を最小限に抑えるため、ボリュームの作成時にセキュリティ形式を指定することを推奨します。

データボリュームのカスタマイズに使用できるオプションのパラメータが多数用意されています。これら

の機能の詳細については、のマニュアルページを参照してください volume create コマンドを実行します

2. ジャンクションポイントが設定されていないボリュームが作成されたことを確認します。 volume show -vserver vs1 -volume volume\_name -junction

例

次の例は、ジャンクションポイントにマウントされない「sales」という名前のボリュームを SVM vs1 上に作成します。

```
cluster1::> volume create -vserver vs1 -volume sales -aggregate aggr3
-size 20GB
[Job 3406] Job succeeded: Successful
```

```
cluster1::> volume show -vserver vs1 -junction
```

Vserver	Volume	Active	Junction Path	Junction Path Source
vs1	data	true	/data	RW_volume
vs1	home4	true	/eng/home	RW_volume
vs1	vs1_root	-	/	-
vs1	sales	-	-	-

**NAS** ネームスペース内の既存のボリュームをマウントまたはアンマウントします

Storage Virtual Machine（SVM）ボリュームに格納されたデータへの NAS クライアントアクセスを設定するには、ボリュームが NAS ネームスペースにマウントされている必要があります。現在マウントされていないボリュームは、ジャンクションポイントにマウントできます。ボリュームはアンマウントすることもできます。

このタスクについて

ボリュームをアンマウントしてオフラインにすると、アンマウントしたボリュームのネームスペース内に含まれていたジャンクションポイントのあるボリューム内のデータも含め、ジャンクションポイント内のすべてのデータに NAS クライアントからアクセスできなくなります。



NAS クライアントからのボリュームへのアクセスを中止するには、ボリュームを単純にアンマウントするだけでは不十分です。ボリュームをオフラインにするか、クライアント側のファイルハンドルキャッシュを確実に無効にするためのその他の手順を実行する必要があります。詳細については、次の技術情報アートを参照してください。"[ONTAP のネームスペースから NFSv3 クライアントを削除しても、ボリュームにアクセスできるようになります](#)"

ボリュームをアンマウントしてオフラインにしても、ボリューム内のデータは失われません。また、既存のボリュームエクスポートポリシーおよびボリュームまたはディレクトリ上に作成された SMB 共有、およびアンマウントされたボリューム内のジャンクションポイントは保持されます。アンマウントしたボリュームを再マウントすれば、NAS クライアントは既存のエクスポートポリシーと SMB 共有を使用してボリューム内のデータにアクセスできるようになります。

手順

1. 必要な操作を実行します。

状況	入力するコマンド
ボリュームをマウント	<code>volume mount -vserver svm_name -volume volume_name -junction-path junction_path</code>
ボリュームをアンマウントします	<code>volume unmount -vserver svm_name -volume volume_name</code>  <code>volume offline -vserver svm_name -volume volume_name</code>

2. ボリュームが目的のマウント状態になっていることを確認します。

```
volume show -vserver svm_name -volume volume_name -fields state,junction-path,junction-active
```

例

次の例は、SVM「vs1」にある「sales」という名前のボリュームをジャンクションポイント「/sales」にマウントします。

```
cluster1::> volume mount -vserver vs1 -volume sales -junction-path /sales

cluster1::> volume show -vserver vs1 state,junction-path,junction-active
```

vserver	volume	state	junction-path	junction-active
-----	-----	-----	-----	-----
vs1	data	online	/data	true
vs1	home4	online	/eng/home	true
vs1	sales	online	/sales	true

次の例は、SVM「vs1」にある「data」という名前のボリュームをアンマウントしてオフラインにします。

```
cluster1::> volume unmount -vserver vs1 -volume data
cluster1::> volume offline -vserver vs1 -volume data

cluster1::> volume show -vserver vs1 -fields state,junction-path,junction-
active
```

vserver	volume	state	junction-path	junction-active
vs1	data	offline	-	-
vs1	home4	online	/eng/home	true
vs1	sales	online	/sales	true

ボリュームマウントポイントとジャンクションポイントに関する情報を表示します

Storage Virtual Machine（SVM）のマウントボリューム、およびボリュームがマウントされているジャンクションポイントに関する情報を表示できます。また、ジャンクションポイントにマウントされていないボリュームを確認することもできます。この情報を使用して、SVM ネームスペースを理解し、管理することができます。

#### 手順

1. 必要な操作を実行します。

表示する項目	入力するコマンド
SVM のマウントされたボリュームとマウントされていないボリュームに関する概要情報	<code>volume show -vserver vs1 -junction</code>
SVM のマウントされたボリュームとマウントされていないボリュームに関する詳細情報	<code>volume show -vserver vs1 -volume volume_name -instance</code>
SVM のマウントされたボリュームとマウントされていないボリュームに関する特定の情報	<p>a. 必要に応じて、の有効なフィールドを表示できます <code>-fields</code> パラメータを指定するには、次のコマンドを使用します。 <code>volume show -fields ?</code></p> <p>b. を使用して、必要な情報を表示します <code>-fields</code> パラメータ：<code>volume show -vserver vs1 -fields fieldname、.....</code></p>

#### 例

次の例は、SVM vs1 のマウントされたボリュームとマウントされていないボリュームの概要を表示します。



```
cluster1::> volume show -vserver vs1 -junction
```

Vserver	Volume	Active	Junction Path	Junction Path Source
vs1	data	true	/data	RW_volume
vs1	home4	true	/eng/home	RW_volume
vs1	vs1_root	-	/	-
vs1	sales	true	/sales	RW_volume

次の例は、SVM vs2 上に配置されたボリュームの指定したフィールドに関する情報を表示します。

```
cluster1::> volume show -vserver vs2 -fields
vserver,volume,aggregate,size,state,type,security-style,junction-
path,junction-parent,node
```

vserver	volume	aggregate	size	state	type	security-style	junction-path	junction-parent	node
vs2	data1	aggr3	2GB	online	RW	unix	-	-	node3
vs2	data2	aggr3	1GB	online	RW	ntfs	/data2		
vs2	data2_root	aggr3	8GB	online	RW	ntfs	/data2/d2_1		
vs2	data2_1	aggr3	8GB	online	RW	ntfs	/data2/d2_2		
vs2	data2_2	aggr3	8GB	online	RW	ntfs	/data2/d2_2		
vs2	pubs	aggr1	1GB	online	RW	unix	/publications		
vs2	images	aggr3	2TB	online	RW	ntfs	/images		
vs2	logs	aggr1	1GB	online	RW	unix	/logs		
vs2	vs2_root	aggr3	1GB	online	RW	ntfs	/	-	node3

## ネームマッピングを設定する

### ネームマッピングの概要を設定する

ONTAP では、ネームマッピングを使用して、CIFS ID を UNIX ID に、Kerberos ID を UNIX ID に、UNIX ID を CIFS ID にマッピングします。この情報は、NFS クライアントからの接続か CIFS クライアントからの接続かに関係なく、ユーザクレデンシャルを取得して適切なファイルアクセスを提供するために必要になります。

ネームマッピングを使用する必要がない例外が 2 つあります。

- 純粋な UNIX 環境を構成した場合、ボリュームに対して CIFS アクセスまたは NTFS セキュリティ形式を使用する予定はありません。
- 代わりにデフォルトユーザを使用するように設定している場合。

このシナリオでは、すべてのクライアントクレデンシャルを個別にマッピングするのではなく、すべてのクライアントクレデンシャルが同じデフォルトユーザにマッピングされるため、ネームマッピングは必要ありません。

ネームマッピングはユーザに対してのみ使用でき、グループに対しては使用できません。

ただし、個々のユーザのグループを特定のユーザにマッピングすることはできます。たとえば、SALES という単語が先頭または末尾に付くすべての AD ユーザを、特定の UNIX ユーザおよびそのユーザの UID にマッピングできます。

#### ネームマッピングの仕組み

ONTAP がユーザのクレデンシャルをマッピングする必要がある場合、最初に、ローカルのネームマッピングデータベースおよび LDAP サーバで既存のマッピングの有無をチェックします。一方をチェックするか両方をチェックするか、およびそのチェック順序は、SVM のネームサービスの設定で決まります。

- Windows から UNIX へのマッピングの場合

マッピングが見つからなかった場合、ONTAP は小文字の Windows ユーザ名が UNIX ドメインで有効なユーザ名かどうかをチェックします。設定されている場合は、デフォルトの UNIX ユーザが使用されます。デフォルトの UNIX ユーザが設定されておらず、この方法でも ONTAP がマッピングを取得できない場合、マッピングは失敗し、エラーが返されます。

- UNIX から Windows へのマッピングの場合

マッピングが見つからなかった場合、ONTAP は SMB ドメインで UNIX 名と一致する Windows アカウントを探します。正しく設定されていない場合は、デフォルトの SMB ユーザが使用されます。デフォルトの CIFS ユーザが設定されておらず、この方法でも ONTAP がマッピングを取得できない場合、マッピングは失敗し、エラーが返されます。

マシンアカウントは、デフォルトでは、指定したデフォルトの UNIX ユーザにマッピングされます。デフォルトの UNIX ユーザを指定しないと、マシンアカウントのマッピングは失敗します。

- ONTAP 9.5 以降では、マシンアカウントをデフォルトの UNIX ユーザ以外のユーザにマッピングできます。
- ONTAP 9.4 以前では、マシンアカウントを他のユーザにマッピングすることはできません。

マシンアカウントに定義されているネームマッピングがあっても無視されます。

#### UNIX ユーザから Windows ユーザへのネームマッピングのためのマルチドメイン検索

ONTAP は、UNIX ユーザを Windows ユーザにマッピングする際のマルチドメイン検索をサポートしています。一致する結果が返されるまで、検出されたすべての信頼できる

ドメインで、変換後のパターンに一致する名前が検索されます。また、信頼できる優先ドメインのリストを設定することもできます。このリストは、検出された信頼できるドメインのリストの代わりに使用され、一致する結果が返されるまで順に検索されます。

ドメインの信頼性が **UNIX** ユーザから **Windows** ユーザへのネームマッピング検索に与える影響

マルチドメインのユーザ名マッピングの仕組みを理解するには、ドメインの信頼性が ONTAP に与える影響を理解しておく必要があります。CIFS サーバのホームドメインとの Active Directory 信頼関係は、双方向の信頼にすることも、インバウンドとアウトバウンドの 2 つのタイプがある単方向の信頼のどちらかにすることもできます。ホームドメインは、SVM の CIFS サーバが属しているドメインです。

- 双方向の信頼

双方向の信頼では、両方のドメインが相互に信頼しています。CIFS サーバのホームドメインが別のドメインと双方向の信頼関係にある場合、このホームドメインは信頼できるドメインに属しているユーザを認証および認可でき、その反対に、この信頼できるドメインはホームドメインに属しているユーザを認証および認可することができます。

UNIX ユーザから Windows ユーザへのネームマッピング検索は、ホームドメインと他方のドメインの間に双方向の信頼関係が確立されたドメインでのみ実行できます。

- アウトバウンドの信頼

アウトバウンドの信頼では、ホームドメインが他方のドメインを信頼しています。この場合、ホームドメインはアウトバウンドの信頼できるドメインに属しているユーザを認証および認可できます。

ホームドメインとアウトバウンドの信頼関係にあるドメインは、UNIX ユーザから Windows ユーザへのネームマッピング検索の実行時に `_not_searched` になります。

- インバウンドの信頼

インバウンドの信頼では、CIFS サーバのホームドメインが他方のドメインによって信頼されています。この場合、ホームドメインはインバウンドの信頼できるドメインに属しているユーザを認証または認可できません。

ホームドメインとインバウンドの信頼関係にあるドメインは、UNIX ユーザから Windows ユーザへのネームマッピング検索の実行時に `_not_searched` になります。

ワイルドカード（\*）を使用したネームマッピングのためのマルチドメイン検索の設定

マルチドメインネームマッピング検索は、Windows ユーザ名のドメインセクションにワイルドカードを使用することで容易になります。次の表に、マルチドメイン検索を有効にするためにネームマッピングエントリのドメイン部にワイルドカードを使用する方法を示します。

パターン（ <b>Pattern</b> ）	交換	結果
ルート	<ul style="list-style-type: none"> <li>• \\ 管理者</li> </ul>	UNIX ユーザ「 root 」は「 administrator 」という名前のユーザにマッピングされます。「 administrator 」という名前の最初の一致するユーザが見つかるまで、すべての信頼できるドメインが順に検索されます。
*	\\*\\*	<p>有効な UNIX ユーザは、対応する Windows ユーザにマッピングされます。該当する名前のユーザとの最初の一致が見つかるまで、すべての信頼できるドメインが順に検索されます。</p> <div>  <p>パターン「\\*\\*」は、UNIX から Windows へのネームマッピングでのみ有効であり、反対方向では無効です。</p> </div>

## マルチドメインの名前検索の実行方法

マルチドメインの名前検索に使用する信頼できるドメインのリストを決定する方法は 2 つあります。

- ONTAP で作成された自動検出された双方向の信頼リストを使用します
- 自分で作成した信頼できる優先ドメインリストを使用します

ユーザ名のドメインセクションにワイルドカードを使用して UNIX ユーザが Windows ユーザにマッピングされている場合、Windows ユーザはすべての信頼できるドメインで次のように検索されます。

- 信頼できるドメインの優先リストが設定されている場合、マッピング先の Windows ユーザはこの検索リスト内でのみ順に検索されます。
- 信頼できるドメインの優先リストが設定されていない場合は、ホームドメインと双方向の信頼関係にあるすべてのドメインで Windows ユーザの検索が行われます。
- ホームドメインと双方向の信頼関係にあるドメインが存在しない場合、ホームドメインでユーザの検索が行われます。

UNIX ユーザがユーザ名にドメインセクションのない Windows ユーザにマッピングされている場合は、ホームドメインで Windows ユーザの検索が行われます。

## ネームマッピングの変換ルール

ONTAP システムには、SVM ごとに一連の変換ルールが保存されています。各ルールは、`a_pattern_` と `a_replacement_` の 2 つの要素で構成されます。変換は該当するリストの先頭から開始され、最初に一致したルールに基づいて実行されます。パターンは

UNIX 形式の正規表現です。リプレースメントは、UNIXのように、パターンのサブ式を表すエスケープシーケンスを含む文字列です sed プログラム。

ネームマッピングを作成します

を使用できます `vserver name-mapping create` コマンドを使用してネームマッピングを作成します。ネームマッピングを使用すると、Windows ユーザから UNIX セキュリティ形式のボリュームへのアクセスおよびその逆方向のアクセスが可能になります。

このタスクについて

ONTAP では、SVM ごとに、各方向について最大 12、500 個のネームマッピングがサポートされます。

ステップ

1. ネームマッピングを作成します。 `vserver name-mapping create -vserver vserver_name -direction {krb-unix|win-unix|unix-win} -position integer -pattern text -replacement text`



。 `-pattern` および `-replacement` ステートメントは正規表現として記述できます。を使用することもできます `-replacement null` 置換文字列を使用してユーザへのマッピングを明示的に拒否するステートメント " " (スペース文字)。を参照してください `vserver name-mapping create` のマニュアルページを参照してください。

Windows から UNIX へのマッピングを作成した場合、新しいマッピングが作成されたときに ONTAP システムに接続していたすべての SMB クライアントは、新しいマッピングを使用するために、一度ログアウトしてから、再度ログインする必要があります。

例

次のコマンドは、`vs1` という名前の SVM 上にネームマッピングを作成します。このマッピングは UNIX から Windows へのマッピングで、優先順位リスト内での位置は 1 番目です。UNIX ユーザ `johnd` を Windows ユーザ `ENG\JohnDoe` にマッピングします。

```
vs1::> vserver name-mapping create -vserver vs1 -direction unix-win
-position 1 -pattern johnd
-replacement "ENG\\JohnDoe"
```

次のコマンドは、`vs1` という名前の SVM 上に別のネームマッピングを作成します。このマッピングは Windows から UNIX へのマッピングで、優先順位リスト内での位置は 1 番目です。パターンとリプレースメントには正規表現が使用されています。このマッピングにより、ドメイン `ENG` 内のすべての CIFS ユーザが、SVM に関連付けられた LDAP ドメイン内のユーザにマッピングされます。

```
vs1::> vserver name-mapping create -vserver vs1 -direction win-unix
-position 1 -pattern "ENG\\(.+)"
-replacement "\\1"
```

次のコマンドは、`vs1` という名前の SVM 上に別のネームマッピングを作成します。このパターンには、エスケープする必要がある Windows ユーザ名の要素として「\$」が含まれています。Windows ユーザ

ENG\john\$ops を UNIX ユーザ john\_ops にマッピングします。

```
vs1::> vsriver name-mapping create -direction win-unix -position 1
-pattern ENG\\john\$ops
-replacement john_ops
```

デフォルトユーザを設定します。

ユーザに対する他のマッピングの試行がすべて失敗した場合や、UNIX と Windows の間で個々のユーザをマッピングしないようにする場合に使用するデフォルトユーザを設定できます。ただし、マッピングされていないユーザの認証を失敗にする場合は、デフォルトユーザを設定しないでください。

このタスクについて

CIFS 認証で、各 Windows ユーザを個別の UNIX ユーザにマッピングしないようにする場合は、代わりにデフォルトの UNIX ユーザを指定できます。

NFS 認証で、各 UNIX ユーザを個別の Windows ユーザにマッピングしないようにする場合は、代わりにデフォルトの Windows ユーザを指定できます。

手順

- 1. 次のいずれかを実行します。

状況	入力するコマンド
デフォルトの UNIX ユーザを設定する	<code>vsriver cifs options modify -default -unix-user user_name</code>
デフォルトの Windows ユーザを設定します	<code>vsriver nfs modify -default-win-user user_name</code>

ネームマッピングの管理用コマンド

ONTAP には、ネームマッピングを管理するためのコマンドが用意されています。

状況	使用するコマンド
ネームマッピングを作成します	<code>vsriver name-mapping create</code>
特定の位置にネームマッピングを挿入します	<code>vsriver name-mapping insert</code>
ネームマッピングを表示します	<code>vsriver name-mapping show</code>

状況	使用するコマンド
2 つのネームマッピングの位置を入れ替えます   ネームマッピングが IP 修飾子エントリで設定されている場合は交換できません。	<code>vserver name-mapping swap</code>
ネームマッピングを変更する	<code>vserver name-mapping modify</code>
ネームマッピングを削除する	<code>vserver name-mapping delete</code>
ネームマッピングが正しいことを確認します	<code>vserver security file-directory show-effective-permissions -vserver vs1 -win-user-name user1 -path / -share-name sh1</code>

詳細については、各コマンドのマニュアルページを参照してください。

## マルチドメインネームマッピング検索を設定する

マルチドメインネームマッピングの検索を有効または無効にします

マルチドメインネームマッピングの検索では、UNIX ユーザから Windows ユーザへのネームマッピングを設定するときに、Windows 名のドメイン部分にワイルドカード（\\*）を使用できます。名前のドメイン部分にワイルドカード（\*）を使用すると、ONTAP で、CIFS サーバのコンピュータアカウントが含まれるドメインと双方向の信頼関係が確立されているすべてのドメインを検索できるようになります。

### このタスクについて

双方向の信頼関係が確立されたすべてのドメインを検索する代わりに、信頼できるドメインのリストを設定することもできます。信頼できるドメインのリストを設定すると、ONTAP は双方向の信頼関係が確立された検出ドメインの代わりに、信頼できるドメインのリストを使用してマルチドメインネームマッピングの検索を実行します。

- マルチドメインネームマッピングの検索は、デフォルトで有効になっています。
- このオプションは、advanced 権限レベルで使用できます。

### 手順

1. 権限レベルを advanced に設定します。 `set -privilege advanced`
2. 次のいずれかを実行します。

マルチドメインネームマッピングの検索の設定	入力するコマンド
有効	<code>vserver cifs options modify -vserver vserver_name -is-trusted-domain-enum -search-enabled true</code>
無効	<code>vserver cifs options modify -vserver vserver_name -is-trusted-domain-enum -search-enabled false</code>

3. admin 権限レベルに戻ります。 `set -privilege admin`

## 関連情報

### 使用できる SMB サーバオプション

信頼できるドメインをリセットして再検出します

すべての信頼できるドメインを強制的に再検出することができます。これは、信頼できるドメインサーバが適切に応答しない場合や、信頼関係が変更された場合に役立ちます。CIFS サーバのコンピュータアカウントを含むドメインであるホームドメインと双方向の信頼が確立されたドメインのみが検出されます。

## ステップ

1. を使用して信頼できるドメインをリセットし、再検出します `vserver cifs domain trusts rediscover` コマンドを実行します

```
vserver cifs domain trusts rediscover -vserver vs1
```

## 関連情報

### 検出された信頼できるドメインに関する情報を表示する

検出された信頼できるドメインに関する情報を表示します

CIFS サーバのホームドメインで検出された信頼できるドメインに関する情報を表示できます。ホームドメインとは、CIFS サーバのコンピュータアカウントが含まれるドメインです。これは、検出される信頼できるドメインと、検出された信頼できるドメインのリスト内でのそれらの順序を把握する場合に役立ちます。

## このタスクについて

ホームドメインと双方向の信頼関係が確立されたドメインのみが検出されます。ホームドメインのドメインコントローラ（DC）は信頼できるドメインのリストを DC が決めた順序で返すため、リスト内のドメインの順序は予測できません。信頼できるドメインのリストを表示すると、マルチドメインネームマッピングの検索の検索順序を確認できます。

表示される信頼できるドメインの情報は、ノードおよび Storage Virtual Machine（SVM）別にグループ化されます。

## ステップ



1. を使用して、検出された信頼できるドメインに関する情報を表示します `vserver cifs domain trusts show` コマンドを実行します

```
vserver cifs domain trusts show -vserver vs1
```

```
Node: node1
Vserver: vs1

Home Domain          Trusted Domain
-----
EXAMPLE.COM          CIFS1.EXAMPLE.COM,
                     CIFS2.EXAMPLE.COM
                     EXAMPLE.COM

Node: node2
Vserver: vs1

Home Domain          Trusted Domain
-----
EXAMPLE.COM          CIFS1.EXAMPLE.COM,
                     CIFS2.EXAMPLE.COM
                     EXAMPLE.COM
```

## 関連情報

### 信頼できるドメインのリセットおよび再検出

信頼できるドメインの優先リストに含まれる信頼できるドメインを追加、削除、または置換します

SMBサーバの信頼できるドメインの優先リストに対して信頼できるドメインを追加または削除したり、現在のリストを変更したりできます。信頼できるドメインの優先リストを設定すると、マルチドメインネームマッピングの検索を実行するときに、検出された双方向の信頼関係にあるドメインの代わりにこのリストが使用されます。

#### このタスクについて

- 信頼できるドメインを既存のリストに追加すると、新しいリストが既存のリストにマージされ、新しいエントリが末尾に追加されます。信頼できるドメインは、リスト内の順序で検索されます。
- 信頼できるドメインを既存のリストから削除する際にリストを指定しないと、指定した Storage Virtual Machine (SVM) の信頼できるドメインのリスト全体が削除されます。
- 信頼できるドメインの既存のリストを変更すると、新しいリストで上書きされます。



信頼できるドメインのリストには、双方向の信頼関係にあるドメインのみを入力してください。アウトバウンドまたはインバウンドの信頼ドメインを優先ドメインリストに入力することはできませんが、マルチドメインネームマッピングの検索では使用されません。ONTAP は単方向ドメインのエントリをスキップし、リスト内の次の双方向の信頼関係にあるドメインに移動します。

## ステップ

1. 次のいずれかを実行します。

信頼できるドメインのリストに対して行う操作	使用するコマンド
信頼できるドメインをリストに追加します	<code>vserver cifs domain name-mapping-search add -vserver _vserver_name_ -trusted-domains FQDN, ...</code>
信頼できるドメインをリストから削除します	<code>vserver cifs domain name-mapping-search remove -vserver _vserver_name_ [-trusted-domains FQDN, ...]</code>
既存のリストを変更します	<code>vserver cifs domain name-mapping-search modify -vserver _vserver_name_ -trusted-domains FQDN, ...</code>

## 例

次のコマンドは、SVM vs1 が使用する信頼できるドメインの優先リストに 2 つの信頼できるドメイン（cifs1.example.com および cifs2.example.com）を追加します。

```
cluster1::> vserver cifs domain name-mapping-search add -vserver vs1
-trusted-domains cifs1.example.com, cifs2.example.com
```

次のコマンドを実行すると、SVM vs1 で使用されるリストから信頼できるドメインが 2 つ削除されます。

```
cluster1::> vserver cifs domain name-mapping-search remove -vserver vs1
-trusted-domains cifs1.example.com, cifs2.example.com
```

次のコマンドは、SVM vs1 で使用されている信頼できるドメインのリストを変更します。元のリストが新しいリストに置き換えられます。

```
cluster1::> vserver cifs domain name-mapping-search modify -vserver vs1
-trusted-domains cifs3.example.com
```

## 関連情報

[信頼できるドメインの優先リストに関する情報を表示する](#)

信頼できるドメインの優先リストに関する情報を表示します

信頼できるドメインの優先リストに含まれる信頼できるドメインに関する情報、およびマルチドメインネームマッピングの検索が有効な場合の信頼できるドメインの検索順序に関する情報を表示できます。自動検出された信頼できるドメインのリストを使用する

代わりに、信頼できるドメインの優先リストを設定することもできます。

#### 手順

1. 次のいずれかを実行します。

表示する情報	使用するコマンド
Storage Virtual Machine （SVM）ごとにグループ化されたクラスタ内のすべての信頼できる優先ドメイン	<code>vserver cifs domain name-mapping-search show</code>
指定した SVM のすべての信頼できる優先ドメインを指定します	<code>vserver cifs domain name-mapping-search show -vserver vserver_name</code>

次のコマンドは、クラスタ上のすべての信頼できる優先ドメインに関する情報を表示します。

```
cluster1::> vserver cifs domain name-mapping-search show
Vserver          Trusted Domains
-----
vs1              CIFS1.EXAMPLE.COM
```

#### 関連情報

[信頼できるドメインの優先リストに含まれる信頼できるドメインの追加、削除、または置換](#)

### SMB 共有を作成および設定

#### SMB 共有の作成と設定の概要

ユーザやアプリケーションが SMB 経由で CIFS サーバ上のデータにアクセスできるようにするには、SMB 共有を作成して設定する必要があります。SMB 共有とは、ボリューム内に指定されたアクセスポイントです。共有をカスタマイズするには、共有パラメータと共有プロパティを指定します。既存の共有はいつでも変更できます。

SMB 共有を作成すると、すべてのメンバーにフルコントロール権限が設定された ACL が ONTAP によって作成されます。

SMB 共有は、Storage Virtual Machine （SVM）上の CIFS サーバに関連付けられます。SVM が削除された場合、または関連付けられている CIFS サーバが SVM から削除された場合、SMB 共有は削除されます。SVM に CIFS サーバを再作成する場合は、SMB 共有を再作成する必要があります。

#### 関連情報

[SMB を使用したファイルアクセスの管理](#)

["Microsoft Hyper-V および SQL Server 向けの SMB の設定"](#)

[ボリュームでの SMB ファイル名の変換のための文字マッピングを設定します](#)

Storage Virtual Machine (SVM) 上にCIFSサーバを作成すると、デフォルトの管理共有が自動的に作成されます。これらのデフォルトの共有とその用途について理解しておく必要があります。

CIFS サーバを作成すると、ONTAP によって次のデフォルトの管理共有が作成されます。



ONTAP 9.8以降では、admin\$共有はデフォルトでは作成されなくなりました。

- IPC \$
- admin\$ (ONTAP 9.7以前のみ)
- c\$

末尾が \$ 文字である共有は非表示の共有であるため、デフォルトの管理共有はマイコンピュータには表示されませんが、共有フォルダを使用して表示することはできます。

### ipc\$ および admin\$ デフォルト管理共有の用途

ipc\$ および admin\$ 共有は ONTAP が使用するものであり、Windows 管理者が SVM 上にあるデータにアクセスするために使用することはできません。

- ipc\$ 共有

ipc\$ 共有は、プログラム間通信に必要な名前付きパイプを共有するリソースです。ipc\$ 共有はコンピュータのリモート管理や、コンピュータの共有リソースを表示する際に使用されます。ipc\$ 共有の共有設定、共有プロパティ、ACL は変更できません。また、ipc\$ 共有の名前の変更や削除もできません。

- admin\$共有 (ONTAP 9.7以前のみ)



ONTAP 9.8以降では、admin\$共有はデフォルトでは作成されなくなりました。

admin\$ 共有は、SVM のリモート管理に使用されます。このリソースのパスは、常に SVM ルートへのパスです。admin\$ 共有の共有設定、共有プロパティ、ACL は変更できません。また、admin\$ 共有の名前の変更や削除もできません。

### c\$ デフォルト共有の用途

c\$ 共有は、クラスタまたは SVM の管理者が SVM のルートボリュームへのアクセスおよび管理に使用できる管理共有です。

c\$ 共有には、次のような特徴があります。

- この共有へのパスは、常に SVM ルートボリュームへのパスで、変更することはできません。
- c\$ 共有のデフォルト ACL は、Administrator / Full Control です。

このユーザは、BUILTIN\administrator です。デフォルトで、BUILTIN\administrator を共有にマッピングでき、マッピングされたルートディレクトリ内のファイルやフォルダの表示、作成、変更、削除が可能です。このディレクトリ内のファイルおよびフォルダを管理する場合は、注意が必要です。

- c\$ 共有の ACL は変更できます。
- c\$ 共有の設定や共有プロパティは変更できます。
- c\$ 共有は削除できません。
- SVM 管理者は、ネームスペースジャンクションを横断することによって、マッピングされた c\$ 共有から残りの SVM ネームスペースにアクセスできます。
- c\$ 共有には、Microsoft 管理コンソールを使用してアクセスできます。

#### 関連情報

[Windows ノセキュリティタブラシヨウシタショウサイナ NTFS ファイルアクセスケンノセツテイ](#)

#### SMB 共有の命名要件

SMB サーバで SMB 共有を作成するときは、ONTAP の共有の命名要件に注意してください。

ONTAP の共有の命名規則は Windows の命名規則と同じであり、次の要件が含まれています。

- 共有名は SMB サーバでそれぞれ一意にする必要があります。
- 共有名では大文字と小文字は区別されません。
- 共有名の最大長は 80 文字です。
- 共有名では Unicode がサポートされます。
- \$ 記号で終わる共有名は非表示の共有です。
- ONTAP 9.7 以前の場合、admin\$、ipc\$、c\$ 管理共有は、すべての CIFS サーバ上に自動的に作成され、共有名が予約されます。ONTAP 9.8 以降では、admin\$ 共有は自動的に作成されなくなりました。
- 共有の作成時に ONTAP\_ADMIN\$ という共有名は使用できません。
- 共有名ではスペースの使用がサポートされます。
  - 共有名の先頭または末尾の文字をスペースにすることはできません。
  - スペースを含む共有名は引用符で囲む必要があります。



単一引用符は共有名の一部とみなされ、引用符の代わりに使用することはできません。

- SMB 共有の名前では次の特殊文字の使用がサポートされます。

! @ # \$ % & ' \_ . ~ ( ) { }

- SMB 共有の名前では次の特殊文字の使用はサポートされません。
  - " / \ : ; | < > 、 ? \* =

マルチプロトコル環境で共有を作成する際のディレクトリの大文字と小文字の区別

名前に大文字と小文字の違いしかないディレクトリ名を区別するために 8.3 の命名方法が使用されている SVM に共有を作成する場合は、クライアントが必要なディレクトリパスに接続できるように共有パスに 8.3 の名前を使用する必要があります。

次の例では、Linux クライアント上に「testdir」と「testdir」という名前の2つのディレクトリが作成されています。ディレクトリを含むボリュームのジャンクションパスは、です /home。最初の出力はLinux クライアントで、2 番目の出力はSMB クライアントで行います。

```
ls -l
drwxrwxr-x 2 user1 group1 4096 Apr 17 11:23 testdir
drwxrwxr-x 2 user1 group1 4096 Apr 17 11:24 TESTDIR
```

```
dir

Directory of Z:\

04/17/2015  11:23 AM    <DIR>          testdir
04/17/2015  11:24 AM    <DIR>          TESTDI~1
```

2 番目のディレクトリへの共有を作成する場合、共有パスに 8.3 の名前を使用する必要があります。この例では、最初のディレクトリの共有パスはです /home/testdir 2番目のディレクトリの共有パスはです /home/TESTDI~1。

**SMB 共有プロパティを使用する**

**SMB 共有プロパティの概要を使用する**

SMB 共有のプロパティをカスタマイズすることができます。

使用可能な共有プロパティは次のとおりです。

共有プロパティ	説明
oplocks	共有で便宜的ロックを使用することを指定します。これはクライアント側キャッシュとも呼ばれます。
browsable	Windows クライアントが共有を参照することを許可します。
showsnapshot	クライアントが Snapshot コピーを表示およびトラバースできることを指定します。
changenotify	共有が変更通知要求をサポートすることを指定します。SVM 上の共有では、これはデフォルトの初期プロパティです。

共有プロパティ	説明
attributecache	属性にすばやくアクセスできるように SMB 共有でのファイル属性のキャッシュを有効にします。デフォルトでは、属性のキャッシュは無効になっています。このプロパティは、SMB 1.0 経由で共有に接続するクライアントがある場合にのみ有効にしてください。クライアントが SMB 2.x または SMB 3.0 経由で共有に接続している場合、この共有プロパティは適用されません。
continuously-available	SMB クライアントが永続的な方法でファイルを開くことを許可します。この方法で開いたファイルは、フェイルオーバーやギブバックなど、システムを停止させるイベントから保護されます。
branchcache	共有内のファイルに対する BranchCache ハッシュの要求をクライアントに許可します。このオプションが役立つのは、CIFS の BranchCache 設定で動作モードとして「共有ごと」を指定した場合だけです。
access-based-enumeration	このプロパティは、この共有で _ アクセスベースの列挙 _ (ABE) を有効にするように指定します。各ユーザのアクセス権に基づいて ABE フィルタを適用した共有フォルダがユーザに表示され、そのユーザがアクセス権を持たないフォルダやその他の共有リソースは表示されないようにします。
namespace-caching	このプロパティは、この共有に接続する SMB クライアントが、CIFS サーバから返されたディレクトリの列挙結果をキャッシュできることを指定します。これにより、パフォーマンスが向上します。デフォルトでは、SMB 1 のクライアントはディレクトリの列挙結果をキャッシュしません。SMB 2 および SMB 3 クライアントはデフォルトでディレクトリ列挙結果をキャッシュするため、この共有プロパティを指定してパフォーマンスが向上するのは SMB 1 クライアント接続のみです。
encrypt-data	この共有へのアクセス時に SMB 暗号化の使用を義務付けます。SMB データへのアクセスで暗号化をサポートしていない SMB クライアントは、この共有にアクセスできません。

既存の **SMB** 共有に対する共有プロパティを追加または削除します

共有プロパティを追加または削除することで、既存の SMB 共有をカスタマイズできます。この方法は、環境内での要件の変化に合わせて共有の設定を変更する場合に便利です。

作業を開始する前に  
プロパティを変更する共有が存在している必要があります。

このタスクについて  
共有プロパティの追加に関するガイドラインは次のとおりです。

- カンマで区切って指定することで、1つ以上の共有プロパティを追加できます。
- 以前に指定した共有プロパティは有効なままです。

新しく追加したプロパティは、共有プロパティの既存のリストに追加されます。

- 共有にすでに適用されている共有プロパティに新しい値を指定した場合は、元の値が新たに指定した値に置き換えられます。
- を使用して共有プロパティを削除することはできません `vserver cifs share properties add` コマンドを実行します

を使用できます `vserver cifs share properties remove` 共有プロパティを削除するコマンド。

共有プロパティの削除に関するガイドラインは次のとおりです。

- カンマで区切って指定することで、1つ以上の共有プロパティを削除できます。
- 以前に指定した共有プロパティは、削除しないかぎり有効なままです。

手順

1. 適切なコマンドを入力します。

状況	入力するコマンド
共有プロパティを追加します	<code>vserver cifs share properties add -vserver _vserver_name_ -share-name _share_name_ -share-properties _properties_,...</code>
共有プロパティを削除します	<code>vserver cifs share properties remove -vserver _vserver_name_ -share-name _share_name_ -share-properties _properties_,...</code>

2. 共有プロパティの設定を確認します。 `vserver cifs share show -vserver vserver_name -share-name share_name`

例

次のコマンドは、を追加します `showsnapshot SVM vs1`上の「share1」という名前の共有に共有プロパティを設定します。



```
cluster1::> vservers cifs share properties add -vservers vs1 -share-name
share1 -share-properties showsnapshot
```

```
cluster1::> vservers cifs share show -vservers vs1
```

Vserver	Share	Path	Properties	Comment	ACL
vs1	share1	/share1	oplocks	-	Everyone / Full
Control			browsable changenotify showsnapshot		

次のコマンドでは、が削除されます browsable SVM vs1上の「share2」という名前の共有から共有プロパティを指定します。

```
cluster1::> vservers cifs share properties remove -vservers vs1 -share-name
share2 -share-properties browsable
```

```
cluster1::> vservers cifs share show -vservers vs1
```

Vserver	Share	Path	Properties	Comment	ACL
vs1	share2	/share2	oplocks	-	Everyone / Full
Control			changenotify		

## 関連情報

### SMB 共有の管理用コマンド

**force-group** 共有設定を使用して、**SMB** ユーザアクセスを最適化します

ONTAP コマンドラインから、UNIX 対応のセキュリティを使用するデータへの共有を作成するときに、SMB ユーザがその共有内に作成するすべてのファイルが、*force-group* と呼ばれる同じグループに属するように指定できます。このグループは、UNIX グループデータベースで事前に定義されている必要があります。*force-group* を使用すると、さまざまなグループに属する SMB ユーザがファイルに確実にアクセスできるようになります。

*force-group* の指定は、共有が UNIX または mixed qtree 内にある場合にのみ有効です。NTFS セキュリティ形式のボリュームまたは qtree にある共有内のファイルへのアクセスは、UNIX の GID ではなく Windows の権限によって判断されるため、これらの共有に *force-group* を設定する必要はありません。

共有に *force-group* が指定されている場合、次のようになります。

- この共有にアクセスする *force-group* 内の SMB ユーザは、*force-group* の GID に一時的に変更されます。

この GID を使用すると、通常はプライマリ GID または UID を使用してアクセスできないファイルにこの共有内のファイルにアクセスできるようになります。

- SMB ユーザがこの共有内に作成するすべてのファイルは、ファイル所有者のプライマリ GID に関係なく、同じフォースグループに属します。

SMB ユーザが、NFS ユーザによって作成されたファイルにアクセスしようとする、SMB ユーザのプライマリ GID によって、権限があるかどうか判断されます。

force-group は、NFS ユーザがこの共有内のファイルにアクセスする方法には影響を与えません。NFS ユーザが作成したファイルは、ファイル所有者から GID を取得します。アクセス権限の決定は、ファイルにアクセスしようとしている NFS ユーザの UID およびプライマリ GID に基づきます。

force-group を使用すると、さまざまなグループに属する SMB ユーザがファイルに確実にアクセスできるようになります。たとえば、会社の Web ページを保存する共有を作成し、Engineering グループと Marketing グループのユーザに書き込みアクセス権を付与する必要がある場合、共有を作成して、「webgroup1」という名前の force-group に書き込み権限を与えます。force-group が指定されているため、SMB ユーザがこの共有内に作成するすべてのファイルは「webgroup1」グループによって所有されます。また、ユーザが共有にアクセスするときは、「webgroup1」グループの GID が自動的に割り当てられます。そのため、Engineering グループと Marketing グループのユーザの権限を管理しなくても、すべてのユーザがこの共有に書き込むことができます。

## 関連情報

### force-group 共有設定を使用した SMB 共有の作成

**force-group** 共有設定を使用して **SMB** 共有を作成します

UNIX ファイルセキュリティ形式のボリュームや qtree にあるデータにアクセスする SMB ユーザが、同じ UNIX グループに属していると ONTAP でみなされるようにするには、force-group 共有設定を使用して SMB 共有を作成します。

## ステップ

1. SMB共有を作成します。 `vserver cifs share create -vserver vserver_name -share-name share_name -path path -force-group-for-create UNIX_group_name`

UNCパスの場合 (\\servername\sharename\filepath) が256文字を超えています (先頭の「\\Windowsの[プロパティ]ボックスの\*[セキュリティ]タブは使用できません。これは、ONTAP 問題ではなく Windows クライアント問題です。この問題を回避するには、UNC パスが 256 文字を超える共有を作成しないでください。

共有の作成後にforce-groupを削除する場合は、共有をいつでも変更し、の値として空の文字列("")を指定できます -force-group-for-create パラメータ共有を変更して force-group を削除した場合、この共有への既存のすべての接続には、引き続き以前に設定された force-group がプライマリ GID として使用されます。

## 例

次のコマンドを実行すると、Webからアクセスできる「webpages」共有が作成されます  
/corp/companyinfo SMBユーザが作成するすべてのファイルがwebgroup1グループに割り当てられているディレクトリ：

```
vserver cifs share create -vserver vs1 -share-name webpages -path
```

```
/corp/companyinfo -force-group-for-create webgroup1
```

## 関連情報

[force-group 共有設定を使用して、SMB ユーザアクセスを最適化します](#)

**MMC** を使用して **SMB** 共有情報を表示します

Microsoft 管理コンソール（MMC）を使用して SVM の SMB 共有情報を表示し、いくつかの管理タスクを実行できます。共有を表示する前に、MMC を SVM に接続する必要があります。

このタスクについて

MMC を使用すると、SVM 内の共有に対して次のタスクを実行できます。

- 共有を表示します
- アクティブなセッションを表示します
- 開いているファイルを表示します
- システムのセッション、ファイル、およびツリー接続のリストを列挙します
- 開いているファイルを閉じます
- 開いているセッションを閉じます
- 共有を作成 / 管理します



上記の機能によって表示されるビューは、クラスタではなくノードに固有のものです。そのため、MMC を使用して SMB サーバホスト名（cifs01.domain.local）に接続すると、DNS の設定に基づいてクラスタ内の単一の LIF にルーティングされます。

次の機能は、MMC for ONTAP ではサポートされていません。

- 新しいローカルユーザ / グループを作成しています
- 既存のローカルユーザ / グループの管理 / 表示
- イベントまたはパフォーマンスログを表示する
- ストレージ
- サービスとアプリケーション

この処理がサポートされていない場合は、が表示されることがあります `remote procedure call failed` エラー。

## "FAQ：ONTAP で Windows MMC を使用する"

### 手順

1. 任意の Windows サーバーでコンピュータの管理 MMC を開くには、[コントロールパネル]で、[管理ツール]>[コンピュータの管理\*]を選択します。
2. 「\*アクション\*>\*別のコンピューターに接続\*」を選択します。

[コンピュータの選択]ダイアログボックスが表示されます。

3. ストレージ・システムの名前を入力するか、または \* Browse \* をクリックしてストレージ・システムを検索します。
4. [OK] をクリックします。

MMC が SVM に接続します。

5. ナビゲーションペインで、 \* 共有フォルダ \* > \* 共有 \* をクリックします。

右側の表示ペインに SVM の共有のリストが表示されます。

6. 共有の共有プロパティを表示するには、共有をダブルクリックして \* プロパティ \* ダイアログボックスを開きます。
7. MMC を使用してストレージシステムに接続できない場合は、ストレージシステムで次のいずれかのコマンドを使用して、 BUILTIN\Administrators グループまたは BUILTIN\Power Users グループにユーザを追加できます。

```
cifs users-and-groups local-groups add-members -vserver <vserver_name>
-group-name BUILTIN\Administrators -member-names <domainuser>

cifs users-and-groups local-groups add-members -vserver <vserver_name>
-group-name "BUILTIN\Power Users" -member-names <domainuser>
```

#### SMB 共有の管理用コマンド

を使用します `vserver cifs share` および `vserver cifs share properties` SMB共有を管理するコマンド。

状況	使用するコマンド
SMB 共有を作成	<code>vserver cifs share create</code>
SMB 共有を表示する	<code>vserver cifs share show</code>
SMB 共有を変更する	<code>vserver cifs share modify</code>
SMB 共有を削除する	<code>vserver cifs share delete</code>
既存の共有に共有プロパティを追加する	<code>vserver cifs share properties add</code>
既存の共有から共有プロパティを削除します	<code>vserver cifs share properties remove</code>
共有プロパティに関する情報を表示します	<code>vserver cifs share properties show</code>

詳細については、各コマンドのマニュアルページを参照してください。

## SMB 共有の ACL を使用してファイルアクセスを保護

SMB 共有レベル ACL の管理に関するガイドラインを次に示します

共有レベルの ACL を変更すると、共有に設定するアクセス権を強化したり、軽減したりできます。Windows のユーザとグループまたは UNIX のユーザとグループのいずれかを使用して共有レベルの ACL を設定できます。

共有を作成すると、共有レベルの ACL のデフォルトでは、Everyone という名前の標準グループに読み取りアクセス権が与えられます。ACL に読み取りアクセス権が設定されているため、ドメイン内およびすべての信頼できるドメイン内のすべてのユーザに共有への読み取り専用アクセス権が与えられます。

共有レベルの ACL を変更するには、Windows クライアントの Microsoft 管理コンソール（MMC）または ONTAP コマンドラインを使用します。

MMC を使用する際には、次の点に留意してください。

- 指定するユーザ名およびグループ名は Windows 名である必要があります。
- Windows の権限だけを指定できます。

ONTAP コマンドラインを使用する際には、次の点に留意してください。

- ユーザ名およびグループ名には、Windows 名または UNIX 名を使用できます。

ACL の作成時または変更時に指定されない場合、デフォルトのタイプは Windows のユーザとグループです。

- Windows の権限だけを指定できます。

## SMB 共有のアクセス制御リストを作成

SMB 共有の Access Control List（ACL；アクセス制御リスト）を作成して共有権限を設定すると、ユーザとグループの共有へのアクセスレベルを制御できます。

このタスクについて

ローカルまたはドメインの Windows ユーザまたはグループ名、あるいは UNIX ユーザまたはグループ名を使用して共有レベルの ACL を設定できます。

新しいACLを作成する前に、デフォルトの共有ACLを削除する必要があります。`Everyone / Full Control`は、セキュリティリスクをもたらします。

ワークグループモードでは、ローカルドメイン名は SMB サーバ名です。

## 手順

1. デフォルトの共有ACLを削除します。`vserver cifs share access-control delete -vserver \_vserver\_name \_-share\_share\_name \_-user-or-group everyone`
2. 新しい ACL を設定します。

設定する <b>ACL</b> に使用するアカウント	入力するコマンド
Windows ユーザ	<pre>vserver cifs share access-control create -vserver vserver_name -share share_name -user-group-type windows -user-or-group Windows_domain_name\user_name -permission access_right</pre>
Windows グループ	<pre>vserver cifs share access-control create -vserver vserver_name -share share_name -user-group-type windows -user-or-group Windows_domain_name\group_name -permission access_right</pre>
UNIX ユーザ	<pre>vserver cifs share access-control create -vserver vserver_name -share share_name -user-group-type unix-user -user-or-group UNIX_user_name -permission access_right</pre>
UNIX グループ	<pre>vserver cifs share access-control create -vserver vserver_name -share share_name -user-group-type unix-group -user-or-group UNIX_group_name -permission access_right</pre>

3. を使用して、共有に適用されたACLが正しいことを確認します `vserver cifs share access-control show` コマンドを実行します

#### 例

次のコマンドは、を示しています Change SVM 「vs1.example.com」 上の「sales」共有に対する「Sales Team」 Windowsグループへの権限：

```
cluster1::> vsserver cifs share access-control create -vsserver
vs1.example.com -share sales -user-or-group "DOMAIN\Sales Team"
-permission Change

cluster1::> vsserver cifs share access-control show -vsserver
vs1.example.com
```

Vserver	Share Name	User/Group Name	User/Group Type	Access Permission
vs1.example.com	c\$	BUILTIN\Administrators	windows	Full_Control
vs1.example.com	sales	DOMAIN\Sales Team	windows	Change

次のコマンドは、を示しています Read SVM 「vs2.example.com」 上の 「eng」 共有の 「engineering」 UNIX グループへの権限：

```
cluster1::> vsserver cifs share access-control create -vsserver
vs2.example.com -share eng -user-group-type unix-group -user-or-group
engineering -permission Read

cluster1::> vsserver cifs share access-control show -vsserver
vs2.example.com
```

Vserver	Share Name	User/Group Name	User/Group Type	Access Permission
vs2.example.com	c\$	BUILTIN\Administrators	windows	Full_Control
vs2.example.com	eng	engineering	unix-group	Read

以下のコマンドで説明します Change 「Tiger Team」という名前のローカルWindowsグループおよびへの権限 Full\_Control SVM 「vs1」 の 「datavol5」 共有に対する 「Sue Chang」という名前のWindowsローカルユーザの権限：

```
cluster1::> vsriver cifs share access-control create -vsriver vs1 -share
datavol5 -user-group-type windows -user-or-group "Tiger Team" -permission
Change

cluster1::> vsriver cifs share access-control create -vsriver vs1 -share
datavol5 -user-group-type windows -user-or-group "Sue Chang" -permission
Full_Control

cluster1::> vsriver cifs share access-control show -vsriver vs1
```

Vsriver	Share	User/Group	User/Group	Access
Permission	Name	Name	Type	
-----	-----	-----	-----	
vs1	c\$	BUILTIN\Administrators	windows	
Full_Control				
vs1	datavol5	Tiger Team	windows	Change
vs1	datavol5	Sue Chang	windows	Full_Control

## SMB 共有アクセス制御リストの管理用コマンド

アクセス制御リスト（ACL）の作成、表示、変更、削除など、SMB の ACL を管理するためのコマンドについて説明します。

状況	使用するコマンド
新しいACLを作成する	<code>vsriver cifs share access-control create</code>
ACL を表示します	<code>vsriver cifs share access-control show</code>
ACL を変更します	<code>vsriver cifs share access-control modify</code>
ACL を削除します	<code>vsriver cifs share access-control delete</code>

## ファイル権限を使用してファイルアクセスを保護

**Windows** のセキュリティタブを使用して、詳細な **NTFS** ファイル権限を設定します

Windows の [プロパティ] ウィンドウの [Windows セキュリティ \*] タブを使用して、ファイルおよびフォルダの標準 NTFS ファイルアクセス権を構成できます。

作業を開始する前に



このタスクを実行する管理者は、選択したオブジェクトに対する権限を変更するための十分な NTFS 権限を持っている必要があります。

このタスクについて

NTFS ファイル権限を設定するには、Windows ホストで、NTFS セキュリティ記述子に関連付けられている NTFS Discretionary Access Control List (DACL ; 随意アクセス制御リスト) にエントリを追加します。その後、セキュリティ記述子を NTFS ファイルおよびディレクトリに適用します。これらのタスクは Windows GUI によって自動的に処理されます。

手順

1. Windows Explorer の \* ツール \* メニューから、\* ネットワークドライブのマップ \* を選択します。
2. [\* ネットワークドライブの割り当て \*] ダイアログボックスに入力します。
  - a. ドライブ文字を選択します。
  - b. [\* フォルダー \*] ボックスに、許可を適用するデータと共有名を含む共有を含む CIFS サーバー名を入力します。

CIFSサーバ名が「CIFS\_SERVER」で、共有の名前が「share1」の場合は、と入力します  
\\CIFS\_SERVER\share1。



CIFS サーバ名の代わりに、CIFS サーバのデータインターフェイスの IP アドレスを指定することもできます。

- c. [完了] をクリックします。

選択したドライブがマウントされて使用可能な状態になり、共有内に格納されているファイルやフォルダが Windows エクスプローラウィンドウに表示されます。

3. NTFS ファイル権限を設定するファイルまたはディレクトリを選択します。
4. ファイルまたはディレクトリを右クリックし、\* プロパティ \* を選択します。
5. [\* セキュリティ \*] タブを選択します。

**Security** タブには、NTFS アクセス権が設定されているユーザーおよびグループのリストが表示されます。[\* アクセス許可の対象 \*] ボックスには、選択した各ユーザーまたはグループに対して有効な [許可] と [拒否] のアクセス許可のリストが表示されます。

6. 「\* 詳細設定 \*」をクリックします。

Windows の [プロパティ] ウィンドウには、ユーザーおよびグループに割り当てられている既存のファイルアクセス権に関する情報が表示されます。

7. [権限の変更 \*] をクリックします。

[アクセス権] ウィンドウが開きます

8. 次のうち必要な操作を実行します。

状況	実行する処理
新しいユーザまたはグループの詳細な NTFS 権限を設定します	a. [ 追加 (Add) ] をクリックします。 b. [ * 選択するオブジェクト名を入力してください * ] ボックスに、追加するユーザーまたはグループの名前を入力します。 c. [OK] をクリックします。
ユーザまたはグループの詳細な NTFS アクセス権を変更します	a. [ * アクセス権エントリ: * ] ボックスで、詳細なアクセス権を変更するユーザーまたはグループを選択します。 b. [ 編集 (Edit) ] をクリックします。
ユーザまたはグループの詳細な NTFS 権限を削除する	a. [ * アクセス許可エントリ: * ] ボックスで、削除するユーザーまたはグループを選択します。 b. [ 削除 (Remove) ] をクリックします。 c. 手順 13 に進みます。

新しいユーザまたはグループに詳細な NTFS 権限を追加する場合、または既存のユーザまたはグループの NTFS 詳細権限を変更する場合は、<Object> の権限エントリボックスが開きます。

9. [ \* 適用先 \* ] ボックスで、この NTFS ファイル許可エントリを適用する方法を選択します。

1 つのファイルに NTFS ファイル権限を設定する場合、\* Apply to \* ボックスはアクティブになりません。[ \* 適用先 \* (Apply to) ] 設定のデフォルトは、\* このオブジェクトのみ \* です。

10. [ \* アクセス許可 \* ] ボックスで、このオブジェクトに設定する詳細なアクセス許可の [ \* 許可 \* ] または [ \* 拒否 \* ] ボックスを選択します。

- 指定したアクセスを許可するには、\* 許可 \* ボックスを選択します。
- 指定されたアクセスを許可しない場合は、\* Deny \* ボックスを選択します。  
次の詳細な権限に関する権限を設定できます。
- \* フルコントロール \*

この詳細な権限を選択すると、他のすべての詳細な権限が自動的に選択されます（それらの権限が許可または拒否されます）。

- \* フォルダの移動 / ファイルの実行 \*
- \* フォルダのリスト / データの読み取り \*
- \* 属性の読み取り \*
- \* 拡張属性の読み取り \*
- \* ファイルの作成 / データの書き込み \*
- \* フォルダの作成 / データの追加 \*
- \* 属性の書き込み \*

- \* 拡張属性の書き込み \*
- \* サブフォルダとファイルの削除 \*
- \* 削除 \*
- \* 読み取り許可 \*
- \* 権限の変更 \*
- \* 所有権を取りなさい \*



いずれかの詳細な権限ボックスを選択できない場合、その権限は親オブジェクトから継承されます。

- このオブジェクトのサブフォルダとファイルにこれらのアクセス権を継承させる場合は、[このコンテナ内のオブジェクトまたはコンテナにこれらのアクセス権を適用する \*] ボックスをオンにします。
- [OK] をクリックします。
- NTFS 権限の追加、削除、または編集が完了したら、このオブジェクトの継承設定を指定します。

- [このオブジェクトの親から継承可能な権限を含める \*] ボックスをオンにします。

これがデフォルトです。

- [このオブジェクトから継承可能な権限ですべての子オブジェクトを置換する \*] ボックスをオンにします。

この設定は、1つのファイルに NTFS ファイルアクセス権を設定する場合は、[アクセス権] ボックスには表示されません。



この設定を選択する場合は注意が必要です。この設定を選択すると、すべての子オブジェクトの既存の権限がすべて削除され、このオブジェクトの権限設定に置き換えられます。削除する必要がなかった権限が誤って削除される可能性があります。これは、mixed セキュリティ形式のボリュームまたは qtree でアクセス権を設定する場合に特に重要です。子オブジェクトが UNIX 対応のセキュリティ形式を使用している場合に、このような子オブジェクトに NTFS 権限を適用すると、ONTAP によってこれらのオブジェクトが UNIX セキュリティ形式から NTFS セキュリティ形式に変更され、これらの子オブジェクトのすべての UNIX 権限が NTFS 権限に置き換えられます。

- 両方のボックスを選択します。
- どちらのボックスも選択しない。

- OK** をクリックして、\*Permissions\* ボックスを閉じます。
- OK \* をクリックして、\* <Object>\* の高度なセキュリティ設定ボックスを閉じます。

詳細な NTFS 権限の設定方法の詳細については、Windows のマニュアルを参照してください。

## 関連情報

[CLI を使用して、NTFS ファイルおよびフォルダに対してファイルセキュリティを設定および適用します](#)

[NTFSセキュリティ形式のボリュームのファイルセキュリティに関する情報の表示](#)

[mixed セキュリティ形式のボリュームのファイルセキュリティに関する情報を表示する](#)

[UNIX セキュリティ形式のボリュームのファイルセキュリティに関する情報を表示する](#)

**ONTAP CLI** を使用して **NTFS** ファイル権限を設定します

ONTAP CLI を使用して、ファイルおよびディレクトリに対して NTFS ファイル権限を設定できます。これにより、Windows クライアントで SMB 共有を使用してデータに接続することなく NTFS ファイル権限を設定できます。

NTFS ファイル権限を設定するには、NTFS セキュリティ記述子に関連付けられている NTFS Discretionary Access Control List (DACL ; 随意アクセス制御リスト) にエントリを追加します。その後、セキュリティ記述子を NTFS ファイルおよびディレクトリに適用します。

コマンドラインで設定できるのは NTFS ファイルアクセス権だけです。CLI で NFSv4 ACL を設定することはできません。

手順

1. NTFSセキュリティ記述子を作成します。

```
vserver security file-directory ntfs create -vserver svm_name -ntfs-sd  
ntfs_security_descriptor_name -owner owner_name -group primary_group_name  
-control-flags-raw raw_control_flags
```

2. NTFSセキュリティ記述子にDACLを追加します。

```
vserver security file-directory ntfs dacl add -vserver svm_name -ntfs-sd  
ntfs_security_descriptor_name -access-type {deny|allow} -account account_name  
-rights {no-access|full-control|modify|read-and-execute|read|write} -apply-to  
{this-folder|sub-folders|files}
```

3. ファイル/ディレクトリのセキュリティポリシーを作成します。

```
vserver security file-directory policy create -vserver svm_name -policy-name  
policy_name
```

**SMB** 経由でファイルにアクセスする際の **UNIX** ファイルアクセス権によるアクセス制御方法

FlexVol ボリュームのセキュリティ形式は、NTFS、UNIX、mixed の3種類のいずれかにすることができます。セキュリティ形式に関係なく SMB 経由でデータにアクセスできますが、UNIX 対応のセキュリティを使用するデータにアクセスするには、適切な UNIX ファイル権限が必要になります。

SMB 経由でのデータへのアクセス時には、いくつかのアクセス制御を使用して、要求した操作を実行する権限がユーザにあるかどうか判断されます。

- エクスポート権限

SMB アクセスに関するエクスポート権限の設定はオプションです。

- 共有権限
- ファイル権限

ユーザが操作を実行するデータには、次のタイプのファイル権限を適用できます。

- NTFS
- UNIX NFSv4 ACL
- UNIX モードビット

NFSv4 ACL または UNIX モードビットが設定されたデータの場合は、UNIX 形式のアクセス権を使用してデータへのファイルアクセス権が決定されます。SVM 管理者は、適切なファイル権限を設定して、ユーザに目的のアクションを実行する権限が付与されるようにする必要があります。



mixed セキュリティ形式のボリューム内のデータでは、NTFS または UNIX 対応のセキュリティ形式を使用できます。UNIX 対応のセキュリティ形式を使用するデータの場合は、データに対するファイル権限を判断するときに NFSv4 権限または UNIX モードビットが使用されます。

## DAC（ダイナミックアクセス制御）を使用したファイルアクセスの保護

**Dynamic Access Control**（**DAC**；ダイナミックアクセス制御）の概要を使用したファイルアクセスの保護

ダイナミックアクセス制御を使用してアクセスを保護できます。Active Directory で集約型アクセスポリシーを作成し、適用された GPO を使用して SVM 上のファイルとフォルダにそのポリシーを適用します。集約型アクセスポリシーのステージングイベントを使用するように監査を設定すると、集約型アクセスポリシーの変更を適用する前にその影響を確認できます。

## CIFS クレデンシャルの追加

ダイナミックアクセス制御が導入される前は、CIFS クレデンシャルにセキュリティプリンシパル（ユーザ）の ID と Windows グループメンバーシップが含まれていました。ダイナミックアクセス制御では、デバイス ID、デバイスの信頼性、ユーザの信頼性という 3 種類の情報がクレデンシャルに追加されます。

- デバイス ID

ユーザ ID 情報に似ていますが、ユーザがログインに使用しているデバイスの ID とグループメンバーシップは例外です。

- デバイスの信頼性

デバイスのセキュリティプリンシパルに関するアサーションです。たとえば、デバイスの信頼性として特定の OU のメンバーであることなどがあります。

- ユーザの信頼性

ユーザのセキュリティプリンシパルに関するアサーションです。たとえば、ユーザの信頼性として AD アカウントが特定の OU のメンバーであることなどがあります。

## 集約型アクセスポリシー

ファイルの集約型アクセスポリシーを使用すると、ユーザグループ、ユーザの信頼性、デバイスの信頼性、およびリソースのプロパティを使用した条件式を含む許可ポリシーを一元的に導入して管理できます。

たとえば、ビジネスへの影響が大きいデータにアクセスする場合、ユーザーはフルタイムの従業員であり、管理対象デバイスからのみデータにアクセスできる必要があります。集約型アクセスポリシーは Active Directory で定義され、GPO メカニズムを介してファイルサーバに配布されます。

### 高度な監査機能を備えた集約型アクセスポリシーのステージング

集約型アクセスポリシーは「集約型」にすることができます。この場合、ファイルアクセスチェック時に「what if」方式で評価されます。ポリシーが適用されていた場合の結果と、現在の設定との違いが、監査イベントとして記録されます。管理者は、実際にポリシーを有効にする前に、監査イベントログを使用してアクセスポリシーの変更による影響を確認できます。アクセスポリシーの変更による影響を評価したあと、ポリシーを目的の SVM に GPO 経由で導入できます。

### 関連情報

[サポートされる GPO](#)

[CIFS サーバへのグループポリシーオブジェクトの適用](#)

[CIFS サーバ上で GPO サポートを有効または無効にします](#)

[GPO 設定に関する情報を表示します](#)

[集約型アクセスポリシーに関する情報を表示します](#)

[集約型アクセスポリシールールに関する情報を表示します](#)

[CIFS サーバ上のデータを保護する集約型アクセスポリシーの設定](#)

[ダイナミックアクセス制御セキュリティに関する情報を表示する](#)

["SMB および NFS の監査とセキュリティトレース"](#)

[サポートされるダイナミックアクセス制御機能](#)

CIFS サーバ上で DAC（ダイナミックアクセス制御）を使用する場合、Active Directory 環境での ONTAP によるダイナミックアクセス制御機能のサポートについて理解しておく必要があります。

[ダイナミックアクセス制御でサポートされます](#)

CIFS サーバでダイナミックアクセス制御が有効になっている場合、ONTAP は次の機能をサポートします。

機能性	コメント
ファイルシステムへの請求	請求とは、ユーザに関する何らかの真実を表す単純な名前と値のペアです。ユーザクレデンシャルにはクレーム情報が含まれており、ファイルのセキュリティ記述子はクレームチェックを含むアクセスチェックを実行できます。これにより、管理者は誰がファイルにアクセスできるかを細かく制御できます。
ファイルアクセスチェック用の条件式	ファイルのセキュリティパラメータを変更する場合、ユーザは任意に複雑な条件式をファイルのセキュリティ記述子に追加できます。条件式には、クレームのチェックを含めることができます。
集約型アクセスポリシーによるファイルアクセスの集中管理	集約型アクセスポリシーは、ファイルへのタグ付けが可能な Active Directory 内に格納される一種の ACL です。ファイルへのアクセスは、ディスク上のセキュリティ記述子とタグ付きの集約型アクセスポリシーの両方のアクセスチェックでアクセスが許可されている場合にのみ許可されます。これにより、管理者はディスク上のセキュリティ記述子を変更することなく、一元的な場所（AD）からファイルへのアクセスを制御できます。
集約型アクセスポリシーのステージング	集約型アクセスポリシーへの変更を「集約型アクセスポリシー」し、監査レポートで変更の影響を確認することで、実際のファイルアクセスに影響を与えずにセキュリティの変更を試す機能を追加します。
ONTAP CLI を使用した集約型アクセスポリシーセキュリティに関する情報の表示のサポート	を拡張します <code>vserver security file-directory show</code> 適用されている集約型アクセスポリシーに関する情報を表示するコマンド。
集約型アクセスポリシーを含むセキュリティトレース	を拡張します <code>vserver security trace</code> 適用されている集約型アクセスポリシーに関する情報を含む結果を表示するコマンドファミリー。

ダイナミックアクセス制御ではサポートされません

CIFS サーバでダイナミックアクセス制御が有効になっている場合、ONTAP は次の機能をサポートしません。

機能性	コメント
NTFS ファイルシステムオブジェクトの自動分類	これは、ONTAP でサポートされていない Windows ファイル分類インフラストラクチャの拡張機能です。

機能性	コメント
集約型アクセスポリシーのステージング以外の高度な監査	高度な監査では、集約型アクセスポリシーのステージングのみがサポートされます。

**CIFS** サーバでダイナミックアクセス制御と集約型アクセスポリシーを使用する際の考慮事項

CIFS サーバ上のファイルとフォルダを保護するために Dynamic Access Control （DAC；ダイナミックアクセス制御）と集約型アクセスポリシーを使用する際は、一定の考慮事項に注意する必要があります。

ポリシールール「環境 **domain\administrator user**」の場合、**root** に対して **NFS** アクセスが拒否されることがあります

特定の状況では、**root** ユーザがアクセスしようとしているデータに集約型アクセスポリシーセキュリティが適用されていると、**root** に対して **NFS** アクセスが拒否されることがあります。問題は、集約型アクセスポリシーに **domain\administrator** に適用されるルールが含まれており、**root** アカウントが **domain\administrator** アカウントにマッピングされている場合に実行されます。

**domain\administrator** ユーザにルールを適用する代わりに、**domain\administrators** グループなど、管理者権限を持つグループにルールを適用してください。これにより、**root** を **domain\administrator** アカウントにマッピングしても、**root** はこの問題の影響を受けなくなります。

適用された集約型アクセスポリシーが **Active Directory** に見つからないと、**CIFS** サーバの **BUILTIN\Administrators** グループにリソースへのアクセスが許可されます

CIFS サーバに格納されたリソースに集約型アクセスポリシーが適用されている場合に、CIFS サーバが集約型アクセスポリシーの SID を使用して Active Directory から情報を取得しようとしても、SID が Active Directory 内の既存の集約型アクセスポリシーの SID と一致しないことがあります。このような場合、CIFS サーバはそのリソースにローカルのデフォルトのリカバリポリシーを適用します。

ローカルのデフォルトのリカバリポリシーでは、CIFS サーバの **BUILTIN\Administrators** グループにそのリソースへのアクセスが許可されます。

ダイナミックアクセス制御の概要を有効または無効にします

Dynamic Access Control （DAC；ダイナミックアクセス制御）を使用して CIFS サーバ上のオブジェクトを保護するオプションは、デフォルトでは無効になっています。CIFS サーバでダイナミックアクセス制御を使用する場合は、このオプションを有効にする必要があります。CIFS サーバに格納されたオブジェクトの保護にダイナミックアクセス制御を使用する必要がなくなった場合は、このオプションを無効にすることができます。

このタスクについて

ダイナミックアクセス制御を有効にすると、ダイナミックアクセス制御関連のエントリを使用する ACL をファイルシステムに含めることができます。ダイナミックアクセス制御を無効にすると、現在のダイナミックアクセス制御エントリは無視され、新しいエントリは許可されません。

このオプションは、advanced 権限レベルでのみ使用できます。



## ステップ

1. 権限レベルを advanced に設定します。 `set -privilege advanced`
2. 次のいずれかを実行します。

ダイナミックアクセス制御の設定	入力するコマンド
有効	<code>vserver cifs options modify -vserver vserver_name -is-dac-enabled true</code>
無効	<code>vserver cifs options modify -vserver vserver_name -is-dac-enabled false</code>

3. 管理者権限レベルに戻ります。 `set -privilege admin`

## 関連情報

### CIFS サーバ上のデータを保護する集約型アクセスポリシーの設定

ダイナミックアクセス制御が無効な場合に、ダイナミックアクセス制御 **ACE** を含む **ACL** を管理します

ダイナミックアクセス制御 ACE が適用された ACL が割り当てられたリソースがある場合に Storage Virtual Machine （SVM）でダイナミックアクセス制御を無効にすると、ダイナミックアクセス制御 ACE を削除するまではそのリソースの非ダイナミックアクセス制御 ACE を管理できません。

#### このタスクについて

ダイナミックアクセス制御を無効にした場合、既存のダイナミックアクセス制御 ACE を削除するまでは、既存の非ダイナミックアクセス制御 ACE の削除や新しい非ダイナミックアクセス制御 ACE の追加はできません。

これらの手順は、通常 ACL の管理に使用している任意のツールを使用して実行できます。

#### 手順

1. リソースに適用されているダイナミックアクセス制御 ACE を確認します。
2. リソースからダイナミックアクセス制御 ACE を削除します。
3. 必要に応じて、リソースに対して非ダイナミックアクセス制御 ACE を追加または削除します。

**CIFS** サーバ上のデータを保護する集約型アクセスポリシーを設定します

集約型アクセスポリシーを使用した CIFS サーバ上のデータへのアクセスを保護するためには、CIFS サーバでの Dynamic Access Control （DAC；ダイナミックアクセス制御）の有効化、Active Directory での集約型アクセスポリシーの設定、GPO を使用した Active Directory コンテナへの集約型アクセスポリシーの適用、CIFS サーバで GPO を有効にします。

#### 作業を開始する前に

- 集約型アクセスポリシーを使用するには、Active Directory を設定する必要があります。

- 集約型アクセスポリシーを作成し、CIFS サーバを含むコンテナに GPO の作成と適用を行うには、Active Directory ドメインコントローラに対して十分なアクセスが必要です。
- 必要なコマンドを実行するためには、Storage Virtual Machine （SVM）で十分な管理アクセスが必要です。

このタスクについて

集約型アクセスポリシーは、Active Directory のグループポリシーオブジェクト（GPO）に対して定義および適用されます。集約型アクセスポリシーと GPO の設定については、Microsoft TechNet ライブラリを参照してください。

## "Microsoft TechNet ライブラリ"

### 手順

1. を使用してSVMのダイナミックアクセス制御を有効にしていない場合は、有効にします `vserver cifs options modify` コマンドを実行します

```
vserver cifs options modify -vserver vs1 -is-dac-enabled true
```

2. を使用してCIFSサーバでグループポリシーオブジェクト（GPO）を有効にしていない場合は、有効にします `vserver cifs group-policy modify` コマンドを実行します

```
vserver cifs group-policy modify -vserver vs1 -status enabled
```

3. Active Directory で集約型アクセスルールと集約型アクセスポリシーを作成します。
4. グループポリシーオブジェクト（GPO）を作成して Active Directory に集約型アクセスポリシーを導入します。
5. CIFS サーバコンピュータアカウントが存在するコンテナに GPO を適用します。
6. を使用して、CIFSサーバに適用されたGPOを手動で更新します `vserver cifs group-policy update` コマンドを実行します

```
vserver cifs group-policy update -vserver vs1
```

7. を使用して、GPO集約型アクセスポリシーがCIFSサーバ上のリソースに適用されていることを確認します `vserver cifs group-policy show-applied` コマンドを実行します

次の例は、デフォルトのドメインポリシーに、CIFS サーバに適用される 2 つの集約型アクセスポリシーがあることを示しています。

```
vserver cifs group-policy show-applied
```

```
Vserver: vs1
-----
GPO Name: Default Domain Policy
Level: Domain
Status: enabled
Advanced Audit Settings:
Object Access:
Central Access Policy Staging: failure
```

Registry Settings:

Refresh Time Interval: 22  
Refresh Random Offset: 8  
Hash Publication Mode for BranchCache: per-share  
Hash Version Support for BranchCache: all-versions

Security Settings:

Event Audit and Event Log:  
Audit Logon Events: none  
Audit Object Access: success  
Log Retention Method: overwrite-as-needed  
Max Log Size: 16384

File Security:

/vol1/home  
/vol1/dir1

Kerberos:

Max Clock Skew: 5  
Max Ticket Age: 10  
Max Renew Age: 7

Privilege Rights:

Take Ownership: usr1, usr2  
Security Privilege: usr1, usr2  
Change Notify: usr1, usr2

Registry Values:

Signing Required: false

Restrict Anonymous:

No enumeration of SAM accounts: true  
No enumeration of SAM accounts and shares: false  
Restrict anonymous access to shares and named pipes: true  
Combined restriction for anonymous user: no-access

Restricted Groups:

gpr1  
gpr2

Central Access Policy Settings:

Policies: cap1  
cap2

GPO Name: Resultant Set of Policy

Level: RSOP

Advanced Audit Settings:

Object Access:  
Central Access Policy Staging: failure

Registry Settings:

Refresh Time Interval: 22  
Refresh Random Offset: 8  
Hash Publication Mode for BranchCache: per-share  
Hash Version Support for BranchCache: all-versions

#### Security Settings:

##### Event Audit and Event Log:

Audit Logon Events: none  
Audit Object Access: success  
Log Retention Method: overwrite-as-needed  
Max Log Size: 16384

##### File Security:

/vol1/home  
/vol1/dirl

##### Kerberos:

Max Clock Skew: 5  
Max Ticket Age: 10  
Max Renew Age: 7

##### Privilege Rights:

Take Ownership: usr1, usr2  
Security Privilege: usr1, usr2  
Change Notify: usr1, usr2

##### Registry Values:

Signing Required: false

##### Restrict Anonymous:

No enumeration of SAM accounts: true  
No enumeration of SAM accounts and shares: false  
Restrict anonymous access to shares and named pipes: true  
Combined restriction for anonymous user: no-access

##### Restricted Groups:

gpr1  
gpr2

##### Central Access Policy Settings:

Policies: cap1  
cap2

2 entries were displayed.

#### 関連情報

[GPO 設定に関する情報を表示します](#)

[集約型アクセスポリシーに関する情報を表示します](#)

[集約型アクセスポリシールールに関する情報を表示します](#)

[ダイナミックアクセス制御の有効化と無効化](#)

[ダイナミックアクセス制御セキュリティに関する情報を表示します](#)

NTFS ボリューム、および mixed セキュリティ形式のボリューム上の NTFS 対応セキュリティを使用するデータについて、ダイナミックアクセス制御（DAC）セキュリティに関する情報を表示できます。これには、条件付き ACE、リソース ACE、および集約

型アクセスポリシー ACE に関する情報が含まれます。この結果を使用して、セキュリティ設定の検証や、ファイルアクセスに関する問題のトラブルシューティングを行うことができます。

このタスクについて

Storage Virtual Machine（SVM）の名前、およびファイルまたはフォルダのセキュリティ情報を表示するデータのパスを入力する必要があります。出力は要約形式または詳細なリストで表示できます。

ステップ

- 1. ファイルとディレクトリのセキュリティ設定を必要な詳細レベルで表示します。

表示する情報	入力するコマンド
要約形式で表示されます	<code>vserver security file-directory show -vserver vserver_name -path path</code>
詳細が表示されます	<code>vserver security file-directory show -vserver vserver_name -path path -expand-mask true</code>
出力は、グループ SID とユーザ SID とともに表示されます	<code>vserver security file-directory show -vserver vserver_name -path path -lookup-names false</code>
16 進数のビットマスクをテキスト形式に変換するファイルとディレクトリのセキュリティについて	<code>vserver security file-directory show -vserver vserver_name -path path -textual-mask true</code>

例

次の例は、パスに関するダイナミックアクセス制御セキュリティの情報を表示します /vol1 SVM vs1：

```

cluster1::> vserver security file-directory show -vserver vs1 -path /vol1
      Vserver: vs1
      File Path: /vol1
      File Inode Number: 112
      Security Style: mixed
      Effective Style: ntfs
      DOS Attributes: 10
      DOS Attributes in Text: ----D---
      Expanded Dos Attribute: -
      Unix User Id: 0
      Unix Group Id: 1
      Unix Mode Bits: 777
      Unix Mode Bits in Text: rwxrwxrwx
      ACLs: NTFS Security Descriptor
            Control:0xbf14
            Owner:CIFS1\Administrator
            Group:CIFS1\Domain Admins
            SACL - ACEs
                  ALL-Everyone-0xf01ff-OI|CI|SA|FA
                  RESOURCE ATTRIBUTE-Everyone-0x0

      ("Department_MS",TS,0x10020,"Finance")
            POLICY ID-All resources - No Write-
0x0-OI|CI
            DACL - ACEs
                  ALLOW-CIFS1\Administrator-0x1f01ff-
OI|CI
                  ALLOW-Everyone-0x1f01ff-OI|CI
                  ALLOW CALLBACK-DAC\user1-0x1200a9-
OI|CI

      ((@User.department==@Resource.Department_MS&&@Resource.Impact_MS>1000)&&@D
evice.department==@Resource.Department_MS)

```

## 関連情報

[GPO 設定に関する情報を表示します](#)

[集約型アクセスポリシーに関する情報を表示します](#)

[集約型アクセスポリシールールに関する情報を表示します](#)

ダイナミックアクセス制御のリバートに関する考慮事項

ダイナミックアクセス制御（DAC）をサポートしないバージョンの ONTAP にリバートする場合に発生する状況と、リバートの前後に必要な処理を把握しておく必要があります。

ダイナミックアクセス制御がサポートされていないバージョンの ONTAP にクラスタをリバートし、1 つ以上の Storage Virtual Machine ( SVM ) でダイナミックアクセス制御が有効になっている場合、リバート前に次の処理を実行する必要があります。

- クラスタでダイナミックアクセス制御が有効になっているすべての SVM で、ダイナミックアクセス制御を無効にする必要があります。
- を含むクラスタで監査の設定を変更する必要があります `cap-staging` のみを使用するイベントタイプ `file-op` イベントタイプ。

ダイナミックアクセス制御 ACE が設定されているファイルやフォルダについて、リバートに関する重要な考慮事項を理解し、対応する必要があります。

- クラスタをリバートした場合、既存のダイナミックアクセス制御 ACE は削除されませんが、ファイルアクセスチェックで無視されます。
- リバート後はダイナミックアクセス制御 ACE は無視されるため、ダイナミックアクセス制御 ACE が設定されたファイルへのアクセスには変更が発生します。

これにより、ユーザは以前にアクセスできなかったファイルにアクセスできるようになり、以前にアクセスできたファイルにアクセスできなくなる可能性があります。

- 以前のセキュリティレベルに戻すには、影響を受けるファイルに非ダイナミックアクセス制御 ACE を適用する必要があります。

この処理は、リバート前またはリバート完了直後に実行できます。



リバート後はダイナミックアクセス制御 ACE は無視されるため、影響を受けるファイルに非ダイナミックアクセス制御 ACE を適用する際にダイナミックアクセス制御 ACE を削除する必要はありません。ただし、必要に応じて手動で削除することもできます。

ダイナミックアクセス制御と集約型アクセスポリシーの設定方法および使用方法に関する追加情報の参照先

ダイナミックアクセス制御と集約型アクセスポリシーを設定および使用する際には、参考資料を利用することができます。

Active Directory のダイナミックアクセス制御と集約型アクセスポリシーの設定方法についての情報は、Microsoft TechNet ライブラリにあります。

["Microsoft TechNet : 「ダイナミックアクセス制御のシナリオの概要」](#)

["Microsoft TechNet : 「集約型アクセスポリシーのシナリオ」](#)

ダイナミックアクセス制御と集約型アクセスポリシーを使用およびサポートするように SMB サーバを設定するには、次の参考資料を使用することができます。

- \* SMBサーバーでのGPOの使用\*

[SMBサーバへのグループポリシーオブジェクトの適用](#)

- \* SMBサーバでのNAS監査の設定\*

### エクスポートポリシーを使用したSMBアクセスの保護

#### SMB アクセスでのエクスポートポリシーの使用方法

SMBサーバでSMBアクセスに関するエクスポートポリシーが有効になっている場合は、SMBクライアントによるSVMボリュームへのアクセスを制御するときにエクスポートポリシーが使用されます。データにアクセスするには、SMB アクセスを許可するエクスポートポリシーを作成し、SMB 共有を含むボリュームにそのポリシーを関連付けます。

エクスポートポリシーには1つ以上のルールが適用されており、このルールで、データへのアクセスを許可されるクライアントと、読み取り専用アクセスと読み取り/書き込みアクセスでサポートされる認証プロトコルを指定します。エクスポートポリシーを設定して、すべてのクライアント、クライアントのサブネット、または特定のクライアントにSMB経由のアクセスを許可し、データへの読み取り専用アクセスと読み取り/書き込みアクセスを決定する際にKerberos 認証、NTLM 認証、またはKerberos 認証とNTLM 認証の両方を使用した認証を許可できます。

ONTAPでエクスポートポリシーに適用されたすべてのエクスポートルールを処理したら、クライアントアクセスを許可するかどうか、および許可するアクセスのレベルを決定できます。エクスポートルールは、Windowsのユーザとグループではなくクライアントマシンに適用されます。エクスポートルールは、Windowsのユーザおよびグループベースの認証と許可に代わるものではありません。共有とファイルのアクセス権限に加えて、エクスポートルールはもう1つのアクセスセキュリティレイヤを提供します。

ボリュームへのクライアントアクセスを設定するには、ボリュームごとにエクスポートポリシーを1つ関連付けます。各SVMには複数のエクスポートポリシーを含めることができます。これにより、複数のボリュームを備えたSVMに対して次の操作を実行できます。

- SVMのボリュームごとに異なるエクスポートポリシーを割り当て、SVMの各ボリュームへのクライアントアクセスを個別に制御する。
- SVMの複数のボリュームに同じエクスポートポリシーを割り当て、同一のクライアントアクセス制御を実行する。ボリュームごとに新しいエクスポートポリシーを作成する必要はありません。

各SVMには、「デフォルト」という名前のエクスポートポリシーが少なくとも1つあります。これにはルールは含まれません。このエクスポートポリシーは削除できませんが、名前や内容は変更できます。デフォルトでは、SVM上の各ボリュームはデフォルトのエクスポートポリシーに関連付けられています。SVMでSMBアクセスのエクスポートポリシーが無効になっている場合、「default」エクスポートポリシーはSMBアクセスには影響しません。

NFSホストとSMBホストの両方にアクセスを提供するルールを設定し、そのルールをエクスポートポリシーに関連付けることができます。このポリシーを、NFSホストとSMBホストの両方がアクセスする必要があるデータを含むボリュームに関連付けることができます。または、SMBクライアントのみがアクセスする必要があるボリュームがある場合は、SMBプロトコルを使用したアクセスのみを許可するルール、および読み取り専用アクセスと書き込みアクセスの認証にKerberosまたはNTLMのみ（あるいはその両方）を使用するルールを含むエクスポートポリシーを設定できます。その後、このエクスポートポリシーをSMBアクセスのみが必要なボリュームに関連付けます。

SMBに関するエクスポートポリシーが有効になっている場合に、クライアントが適用可能なエクスポートポリシーで許可されていないアクセス要求を行うと、権限拒否のメッセージが表示され、その要求は失敗します。クライアントがボリュームのエクスポートポリシーのどのルールにも一致しない場合、アクセスは拒否さ



れます。エクスポートポリシーが空の場合は、すべてのアクセスが暗黙的に拒否されます。これは、共有とファイルの権限によってアクセスが許可されている場合にも当てはまります。つまり、SMB 共有を含むボリュームで少なくとも以下を許可するようにエクスポートポリシーを設定する必要があります。

- すべてのクライアント、またはクライアントの適切なサブセットへのアクセスを許可します
- SMB 経由のアクセスを許可する
- Kerberos 認証または NTLM 認証（あるいはその両方）を使用した適切な読み取り専用アクセスと書き込みアクセスを許可する

詳細はこちら ["エクスポートポリシーの設定と管理"](#)。

#### エクスポートルール仕組み

エクスポートルールは、エクスポートポリシーの機能要素です。エクスポートルールでは、ボリュームへのクライアントアクセス要求が設定済みの特定のパラメータと照合され、クライアントアクセス要求の処理方法が決定されます。

エクスポートポリシーには、クライアントにアクセスを許可するエクスポートルールが少なくとも 1 つ含まれている必要があります。エクスポートポリシーに複数のルールが含まれている場合、ルールはエクスポートポリシーに表示される順に処理されます。ルールの順序は、ルールインデックス番号によって決まります。ルールがクライアントに一致すると、そのルールの権限が使用され、それ以降のルールは処理されません。一致するルールがない場合、クライアントはアクセスを拒否されます。

次の条件を使用して、クライアントのアクセス権限を決定するようにエクスポートルールを設定できます。

- クライアントが要求の送信に使用するファイルアクセスプロトコル。たとえば、NFSv4 や SMB などです。
- ホスト名や IP アドレスなどのクライアント識別子。

の最大サイズ `-clientmatch` フィールドは4096文字です。

- Kerberos v5、NTLM、AUTH\_SYS など、クライアントが認証に使用するセキュリティタイプ。

ルールで複数の条件が指定されている場合、クライアントがそれらのすべてに一致しないとルールは適用されません。

#### 例

エクスポートポリシーに、次のパラメータが指定されたエクスポートルールが含まれています。

- `-protocol nfs3`
- `-clientmatch 10.1.16.0/255.255.255.0`
- `-rorule any`
- `-rwrule any`

クライアントアクセス要求は NFSv3 プロトコルを使用して送信され、クライアントの IP アドレスは 10.1.17.37 です。

クライアントアクセスプロトコルが一致していても、クライアントの IP アドレスがエクスポートルールで指定されているアドレスとは別のサブネットに属しています。そのため、クライアントは一致なくなり、この

ルールはこのクライアントに適用されません。

例

エクスポートポリシーに、次のパラメータが指定されたエクスポートルールが含まれています。

- `-protocol nfs`
- `-clientmatch 10.1.16.0/255.255.255.0`
- `-rorule any`
- `-rwrule any`

クライアントアクセス要求はNFSv4プロトコルを使用して送信され、クライアントのIPアドレスは10.1.16.54です。

クライアントアクセスプロトコルが一致し、クライアントのIPアドレスが指定したサブネット内にあります。そのため、クライアントは一致し、このルールはこのクライアントを環境します。セキュリティタイプに関係なく、クライアントは読み取り / 書き込みアクセス権を取得します。

例

エクスポートポリシーに、次のパラメータが指定されたエクスポートルールが含まれています。

- `-protocol nfs3`
- `-clientmatch 10.1.16.0/255.255.255.0`
- `-rorule any`
- `-rwrule krb5,ntlm`

クライアント #1 は、IP アドレスが 10.1.16.207 で、NFSv3 プロトコルを使用してアクセス要求を送信し、Kerberos v5 で認証されます。

クライアント #2 は、IP アドレスが 10.1.16.211 で、NFSv3 プロトコルを使用してアクセス要求を送信し、AUTH\_SYS で認証されます。

両方のクライアントで、クライアントアクセスプロトコルとIPアドレスは一致しています。読み取り専用パラメータでは、認証に使用するセキュリティタイプに関係なく、読み取り専用アクセスがすべてのクライアントに許可されています。したがって、両方のクライアントが読み取り専用アクセス権を取得します。ただし、読み取り / 書き込みアクセス権を取得するのはクライアント #1 だけです。これは、認証に承認されたセキュリティタイプ Kerberos v5 を使用したためです。クライアント #2 は読み取り / 書き込みアクセス権を取得できません。

**SMB** 経由のアクセスを制限または許可するエクスポートポリシールールの例

以下の例は、SMB アクセスのエクスポートポリシーが有効になっている SVM で SMB 経由のアクセスを制限または許可するエクスポートポリシールールを作成する方法を示しています。

SMB アクセスに関するエクスポートポリシーは、デフォルトでは無効になっています。SMB 経由のアクセスを制限または許可するエクスポートポリシールールは、SMB アクセスのエクスポートポリシーを有効にしている場合にのみ設定する必要があります。

## SMB アクセスのみのエクスポートルール

次のコマンドでは、「vs1」という名前の SVM に、次の構成のエクスポートルールが作成されます。

- ポリシー名：cifs1
- インデックス番号：1
- クライアント一致：192.168.1.0/24 ネットワーク上のクライアントにのみ一致します
- プロトコル：SMB アクセスのみを有効にします
- 読み取り専用アクセス：NTLM 認証または Kerberos 認証を使用するクライアントに許可します
- 読み取り / 書き込みアクセス：Kerberos 認証を使用するクライアントに許可します

```
cluster1::> vserver export-policy rule create -vserver vs1 -policyname  
cifs1 -ruleindex 1 -protocol cifs -clientmatch 192.168.1.0/255.255.255.0  
-rorule krb5,ntlm -rwrule krb5
```

## SMB および NFS アクセスのエクスポートルール

次のコマンドでは、「vs1」という名前の SVM に、次の構成のエクスポートルールが作成されます。

- ポリシー名：cifs nfs1
- インデックス番号：2.
- クライアント一致：すべてのクライアントに一致します
- プロトコル：SMB アクセスと NFS アクセス
- 読み取り専用アクセス：すべてのクライアントに許可します
- 読み取り / 書き込みアクセス：Kerberos 認証（NFS および SMB）または NTLM 認証（SMB）を使用するクライアントに許可
- UNIX ユーザ ID 0（ゼロ）のマッピング：ユーザ ID 65534（通常ユーザ名 nobody にマッピングされる）にマッピング
- suid と sgid のアクセス：許可しています

```
cluster1::> vserver export-policy rule create -vserver vs1 -policyname  
cifs nfs1 -ruleindex 2 -protocol cifs,nfs -clientmatch 0.0.0.0/0 -rorule  
any -rwrule krb5,ntlm -anon 65534 -allow-suid true
```

## NTLM のみを使用する SMB アクセスのエクスポートルール

次のコマンドでは、「vs1」という名前の SVM に、次の構成のエクスポートルールが作成されます。

- ポリシー名：ntlm1
- インデックス番号：1
- クライアント一致：すべてのクライアントに一致します

- プロトコル：SMB アクセスのみを有効にします
- 読み取り専用アクセス：NTLM を使用するクライアントにのみ許可されます
- 読み取り / 書き込みアクセス：NTLM を使用するクライアントにのみ許可されます



NTLM のみを使用するアクセスに読み取り専用オプションまたは読み取り / 書き込みオプションを設定する場合は、クライアント一致オプションで IP アドレスベースのエントリを使用する必要があります。それ以外の場合は、受信します access denied エラー。これは、ONTAP がホスト名を使用してクライアントの権限を確認するときに、Kerberos Service Principal Name (SPN ; サービスプリンシパル名) を使用するためです。NTLM 認証では、SPN 名はサポートされません。

```
cluster1::> vservers export-policy rule create -vservers vs1 -policyname
ntlm1 -ruleindex 1 -protocol cifs -clientmatch 0.0.0.0/0 -rorule ntlm
-rwrule ntlm
```

**SMB** アクセスに関するエクスポートポリシーを有効または無効にします

Storage Virtual Machine (SVM) での SMB アクセスに関するエクスポートポリシーを有効または無効にすることができます。エクスポートポリシーを使用したリソースへの SMB アクセスの制御はオプションです。

作業を開始する前に

SMB のエクスポートポリシーを有効にするための要件は次のとおりです。

- クライアントのエクスポートルールを作成する前に、そのクライアントの「PTR」レコードが DNS に登録されている必要があります。
- SVM が NFS クライアントにアクセスを提供し、NFS アクセスに使用するホスト名が CIFS サーバ名と異なる場合は、ホスト名に対して「A」レコードと「PTR」レコードのセットが追加が必要です。

このタスクについて

SVM に新しい CIFS サーバをセットアップするとき、SMB アクセスに関するエクスポートポリシーの使用はデフォルトで無効になります。認証プロトコル、クライアント IP アドレス、またはホスト名に基づいてアクセスを制御する場合は、SMB アクセスのエクスポートポリシーを有効にできます。SMB アクセスに関するエクスポートポリシーはいつでも有効または無効にできます。

手順

1. 権限レベルを advanced に設定します。set -privilege advanced
2. エクスポートポリシーを有効または無効にします。
  - エクスポートポリシーを有効にします。vservers cifs options modify -vservers vservers\_name -is-exportpolicy-enabled true
  - エクスポートポリシーを無効にします。vservers cifs options modify -vservers vservers\_name -is-exportpolicy-enabled false
3. admin 権限レベルに戻ります。set -privilege admin

例

次の例は、エクスポートポリシーを使用した SVM vs1 上のリソースへの SMB クライアントアクセスの制御を有効にします。

```
cluster1::> set -privilege advanced
Warning: These advanced commands are potentially dangerous; use them
only when directed to do so by technical support personnel.
Do you wish to continue? (y or n): y

cluster1::*> vserver cifs options modify -vserver vs1 -is-exportpolicy
-enabled true

cluster1::*> set -privilege admin
```

ストレージレベルのアクセス保護を使用してファイルアクセスを保護

ストレージレベルのアクセス保護を使用してファイルアクセスを保護

ネイティブファイルレベルのセキュリティとエクスポートおよび共有のセキュリティを使用したアクセスの保護に加えて、ボリュームレベルで ONTAP によって適用される第 3 のセキュリティレイヤとしてストレージレベルのアクセス保護を設定できます。ストレージレベルのアクセス保護：すべての NAS プロトコルから適用されるストレージオブジェクトへの環境アクセスを保護します。

NTFS のアクセス権のみがサポートされています。ONTAP で、ストレージレベルのアクセス保護が適用されているボリューム上のデータにアクセスする UNIX ユーザのセキュリティチェックを行うには、UNIX ユーザがボリュームを所有する SVM 上の Windows ユーザにマッピングされている必要があります。

ストレージレベルのアクセス保護の動作

- ストレージレベル環境のアクセス保護：ストレージオブジェクト内のすべてのファイルまたはすべてのディレクトリを保護します。

ボリューム内のすべてのファイルまたはディレクトリがストレージレベルのアクセス保護設定の影響を受けるため、伝播による継承は必要ありません。

- ストレージレベルのアクセス保護は、ボリューム内のファイルのみ、ディレクトリのみ、またはファイルとディレクトリの両方に適用されるように設定できます。

- ファイルとディレクトリのセキュリティ

ストレージオブジェクト内のすべてのディレクトリとファイルを環境に格納します。これがデフォルト設定です。

- ファイルセキュリティ

ストレージオブジェクト内のすべてのファイルを環境します。このセキュリティを適用しても、ディレクトリへのアクセスとディレクトリの監査には影響しません。

- ディレクトリセキュリティ

ストレージオブジェクト内のすべてのディレクトリを環境します。このセキュリティを適用しても、ファイルへのアクセスとファイルの監査には影響しません。

- ストレージレベルのアクセス保護は、権限の制限に使用します。

アクセス権限は付与されません。

- NFS または SMB クライアントからファイルまたはディレクトリのセキュリティ設定を表示した場合、ストレージレベルのアクセス保護のセキュリティは表示されません。

このセキュリティは、有効な権限を決定するために、ストレージオブジェクトレベルで適用され、メタデータ内に格納されます。

- システム（Windows または UNIX）管理者であっても、ストレージレベルのセキュリティをクライアントから取り消すことはできません。

このセキュリティは、ストレージ管理者のみが変更できるように設計されています。

- ストレージレベルのアクセス保護は、NTFS または mixed セキュリティ形式のボリュームに適用できません。
- ストレージレベルのアクセス保護を UNIX セキュリティ形式のボリュームに適用できるのは、そのボリュームが含まれている SVM で CIFS サーバが設定されている場合に限られます。
- ボリュームがボリュームジャンクションパス以下にマウントされていて、そのパスにストレージレベルのアクセス保護が存在している場合、その下にマウントされているボリュームには伝播されません。
- ストレージレベルのアクセス保護のセキュリティ記述子は、SnapMirror データレプリケーションおよび SVM レプリケーションによってレプリケートされます。
- ウィルススキャンについては特別な免除があります。

ファイルやディレクトリのスクリーニングを行うこれらのサーバに対しては、ストレージレベルのアクセス保護によってオブジェクトへのアクセスが拒否されていても、例外的なアクセスが許可されます。

- ストレージレベルのアクセス保護によってアクセスが拒否された場合、FPolicy 通知は送信されません。

## アクセスチェックの順序

ファイルまたはディレクトリへのアクセスは、エクスポートまたは共有の権限、ボリュームで設定されているストレージレベルのアクセス保護権限、ファイルやディレクトリに適用されるネイティブのファイル権限の各影響の組み合わせによって決まります。すべてのレベルのセキュリティが評価されて、ファイルまたはディレクトリの有効な権限が決定されます。セキュリティアクセスチェックは、次の順序で実行されます。

1. SMB 共有または NFS エクスポートレベルの権限
2. ストレージレベルのアクセス保護
3. NTFS のファイルやフォルダの Access Control List（ACL；アクセス制御リスト）、NFSv4 ACL、または UNIX モードのビット

## ストレージレベルのアクセス保護の使用のユースケース

ストレージレベルのアクセス保護は、ストレージレベルでの追加セキュリティを提供します。このセキュリティはクライアント側からは見えないため、ユーザや管理者がデス

クトップから取り消すことはできません。一部のユースケースでは、ストレージレベルでアクセス制御を行える機能が役立ちます。

この機能の一般的なユースケースとしては、次のようなシナリオがあります。

- すべてのユーザーのアクセスをストレージ・レベルで監査および制御することにより、知的財産を保護します
- 銀行や証券会社など、金融サービス企業のストレージの場合
- 部門ごとに個別のファイルストレージを使用する行政サービス
- すべての学生のファイルを保護する大学

ストレージレベルのアクセス保護を設定するためのワークフロー

ストレージレベルのアクセス保護（SLAG）を設定するワークフローでは、NTFS ファイル権限や監査ポリシーを設定する際に使用する ONTAP CLI コマンドと同じコマンドを使用します。対象のファイルやディレクトリのアクセスを設定する代わりに、対象の Storage Virtual Machine（SVM）ボリュームの SLAG を設定します。



#### 関連情報

[ストレージレベルのアクセス保護の設定](#)



ボリュームまたは qtree にストレージレベルのアクセス保護を設定するためには、いくつかの手順に従う必要があります。ストレージレベルのアクセス保護は、ストレージレベルで設定されるアクセスセキュリティを提供します。環境がすべての NAS プロトコルからその適用先のストレージオブジェクトにアクセスするセキュリティを提供します。

#### 手順

1. を使用して、セキュリティ記述子を作成します `vserver security file-directory ntfs create` コマンドを実行します

```
vserver security file-directory ntfs create -vserver vs1 -ntfs-sd sd1 vserver
security file-directory ntfs show -vserver vs1
```

```
Vserver: vs1
```

NTFS Security Descriptor Name	Owner Name
-----	-----
sd1	-

セキュリティ記述子は、次の 4 つのデフォルト DACL アクセス制御エントリ（ACE）を持つように作成されます。

```
Vserver: vs1
```

```
NTFS Security Descriptor Name: sd1
```

Account Name	Access Type	Access Rights	Apply To
-----	-----	-----	-----
BUILTIN\Administrators	allow	full-control	this-folder, sub-folders, files
BUILTIN\Users	allow	full-control	this-folder, sub-folders, files
CREATOR OWNER	allow	full-control	this-folder, sub-folders, files
NT AUTHORITY\SYSTEM	allow	full-control	this-folder, sub-folders, files

ストレージレベルのアクセス保護を設定するときにデフォルトのエントリを使用しない場合は、セキュリティ記述子に独自の ACE を作成して追加する前に、デフォルトのエントリを削除できます。

2. セキュリティ記述子から、ストレージレベルのアクセス保護セキュリティに設定したくないデフォルトの DACL ACE を削除します。

- a. を使用して、不要なDACL ACEを削除します `vserver security file-directory ntfs dacl remove` コマンドを実行します

この例では、セキュリティ記述子から `BUILTIN\Administrators`、`BUILTIN\Users`、`CREATOR OWNER` の3つのデフォルト DACL ACE を削除しています。

```
vserver security file-directory ntfs dacl remove -vserver vs1 -ntfs-sd sd1
-access-type allow -account builtin\users vserver security file-directory
ntfs dacl remove -vserver vs1 -ntfs-sd sd1 -access-type allow -account
builtin\administrators vserver security file-directory ntfs dacl remove
-vserver vs1 -ntfs-sd sd1 -access-type allow -account "creator owner"
```

- b. を使用して、ストレージレベルのアクセス保護セキュリティに使用しないDACL ACEがセキュリティ記述子から削除されたことを確認します `vserver security file-directory ntfs dacl show` コマンドを実行します

この例では、コマンドからの出力により、セキュリティ記述子から3つのデフォルト DACL ACE が削除され、`NT AUTHORITY\SYSTEM` のデフォルト DACL ACE エントリのみが残されていることを確認できます。

```
vserver security file-directory ntfs dacl show -vserver vs1
```

Vserver: vs1

NTFS Security Descriptor Name: sd1

Account Name	Access Type	Access Rights	Apply To
-----	-----	-----	-----
NT AUTHORITY\SYSTEM	allow	full-control	this-folder, sub-folders, files

3. を使用して、セキュリティ記述子に1つ以上のDACL エントリを追加します `vserver security file-directory ntfs dacl add` コマンドを実行します

この例では、セキュリティ記述子に2つの DACL ACE を追加しています。

```
vserver security file-directory ntfs dacl add -vserver vs1 -ntfs-sd sd1
-access-type allow -account example\engineering -rights full-control -apply-to
this-folder,sub-folders,files vserver security file-directory ntfs dacl add
-vserver vs1 -ntfs-sd sd1 -access-type allow -account "example\Domain Users"
-rights read -apply-to this-folder,sub-folders,files
```

4. を使用して、セキュリティ記述子に1つ以上のSACL エントリを追加します。 `vserver security file-directory ntfs sacl add` コマンドを実行します

この例では、セキュリティ記述子に2つのSACL ACE を追加しています。

```
vserver security file-directory ntfs sacl add -vserver vs1 -ntfs-sd sd1
-access-type failure -account "example\Domain Users" -rights read -apply-to
```

```
this-folder,sub-folders,files vserver security file-directory ntfs sac1 add
-vserver vs1 -ntfs-sd sd1 -access-type success -account example\engineering
-rights full-control -apply-to this-folder,sub-folders,files
```

5. を使用して、DACLおよびSACLのACEが正しく設定されていることを確認します vserver security file-directory ntfs dacl show および vserver security file-directory ntfs sac1 show コマンドを指定します。

この例では、次のコマンドはセキュリティ記述子「`d1`」の DACL エントリに関する情報を表示します。

```
vserver security file-directory ntfs dacl show -vserver vs1 -ntfs-sd sd1
```

```
Vserver: vs1
```

```
NTFS Security Descriptor Name: sd1
```

Account Name	Access Type	Access Rights	Apply To
EXAMPLE\Domain Users	allow	read	this-folder, sub-folders, files
EXAMPLE\engineering	allow	full-control	this-folder, sub-folders, files
NT AUTHORITY\SYSTEM	allow	full-control	this-folder, sub-folders, files

この例では、次のコマンドを実行すると、セキュリティ記述子「`d1`」の SACL エントリに関する情報が表示されます。

```
vserver security file-directory ntfs sac1 show -vserver vs1 -ntfs-sd sd1
```

```
Vserver: vs1
```

```
NTFS Security Descriptor Name: sd1
```

Account Name	Access Type	Access Rights	Apply To
EXAMPLE\Domain Users	failure	read	this-folder, sub-folders, files
EXAMPLE\engineering	success	full-control	this-folder, sub-folders, files

6. を使用して、セキュリティポリシーを作成します `vserver security file-directory policy create` コマンドを実行します

次に、「policy1」という名前のポリシーを作成する例を示します。

```
vserver security file-directory policy create -vserver vs1 -policy-name policy1
```

7. を使用して、ポリシーが正しく設定されていることを確認します `vserver security file-directory policy show` コマンドを実行します

```
vserver security file-directory policy show
```

Vserver	Policy Name
-----	-----
vs1	policy1

8. を使用して、セキュリティ記述子が関連付けられたタスクをセキュリティポリシーに追加します `vserver security file-directory policy task add` コマンドにを指定します `-access -control` パラメータをに設定します `slag`。

ポリシーには複数のストレージレベルのアクセス保護タスクを含めることができますが、ポリシーにファイルとディレクトリのタスクとストレージレベルのアクセス保護タスクの両方を含めることはできません。ポリシーに含めるタスクは、すべてストレージレベルのアクセス保護タスクにするか、すべてファイルとディレクトリのタスクにする必要があります。

この例では 'セキュリティ記述子 "d1" に割り当てられている "policy1 " という名前のポリシーにタスクが追加されますこれはに割り当てられます `/datavol1` アクセス制御タイプが「slag」に設定されているパス。

```
vserver security file-directory policy task add -vserver vs1 -policy-name policy1 -path /datavol1 -access-control slag -security-type ntfs -ntfs-mode propagate -ntfs-sd sd1
```

9. を使用して、タスクが正しく設定されていることを確認します `vserver security file-directory policy task show` コマンドを実行します

```
vserver security file-directory policy task show -vserver vs1 -policy-name policy1
```

```
Vserver: vs1
Policy: policy1
```

Index	File/Folder	Access	Security	NTFS	NTFS
Security	Path	Control	Type	Mode	Descriptor
Name					
-----	-----	-----	-----	-----	
1	/datavol1	slag	ntfs	propagate	sd1

10. を使用して、ストレージレベルのアクセス保護セキュリティポリシーを適用します `vserver security file-directory apply` コマンドを実行します

```
vserver security file-directory apply -vserver vs1 -policy-name policy1
```

セキュリティポリシーを適用するジョブがスケジュールされます。

11. を使用して、適用されたストレージレベルのアクセス保護セキュリティ設定が正しいことを確認します `vserver security file-directory show` コマンドを実行します

この例では、コマンドの出力から、ストレージレベルのアクセス保護セキュリティがNTFSボリュームに適用されていることがわかります `/datavol1`。Everyone に Full Control を許可するデフォルト DACL は残っていますが、ストレージレベルのアクセス保護セキュリティによって、ストレージレベルのアクセス保護設定で定義されたグループにアクセスが制限（および監査）されます。

```
vserver security file-directory show -vserver vs1 -path /datavol1
```

```

        Vserver: vs1
        File Path: /datavol1
File Inode Number: 77
        Security Style: ntfs
        Effective Style: ntfs
        DOS Attributes: 10
DOS Attributes in Text: ----D---
Expanded Dos Attributes: -
        Unix User Id: 0
        Unix Group Id: 0
        Unix Mode Bits: 777
Unix Mode Bits in Text: rwxrwxrwx
        ACLs: NTFS Security Descriptor
              Control:0x8004
              Owner: BUILTIN\Administrators
              Group: BUILTIN\Administrators
              DACL - ACEs
                  ALLOW-Everyone-0x1f01ff
                  ALLOW-Everyone-0x10000000-OI|CI|IO

Storage-Level Access Guard security
SACL (Applies to Directories):
    AUDIT-EXAMPLE\Domain Users-0x120089-FA
    AUDIT-EXAMPLE\engineering-0x1f01ff-SA
DACL (Applies to Directories):
    ALLOW-EXAMPLE\Domain Users-0x120089
    ALLOW-EXAMPLE\engineering-0x1f01ff
    ALLOW-NT AUTHORITY\SYSTEM-0x1f01ff
SACL (Applies to Files):
    AUDIT-EXAMPLE\Domain Users-0x120089-FA
    AUDIT-EXAMPLE\engineering-0x1f01ff-SA
DACL (Applies to Files):
    ALLOW-EXAMPLE\Domain Users-0x120089
    ALLOW-EXAMPLE\engineering-0x1f01ff
    ALLOW-NT AUTHORITY\SYSTEM-0x1f01ff

```

## 関連情報

[CLI を使用して、SVM の NTFS ファイルセキュリティ、NTFS 監査ポリシー、ストレージレベルのアクセス保護を管理します](#)

[ストレージレベルのアクセス保護を設定するためのワークフロー](#)

[ストレージレベルのアクセス保護に関する情報の表示](#)

## ストレージレベルのアクセス保護の削除

### SLAG の適用に関する一覧表

SLAG は、ボリューム、 qtree 、またはその両方に対して設定できます。次の表に、さまざまな状況について、ボリュームまたは qtree に SLAG 構成を適用できるかどうかを示します。

	<b>AFS 内のボリューム SLAG</b>	<b>Snapshot コピー内のボリューム SLAG</b>	<b>AFS 内の qtree SLAG</b>	<b>Snapshot コピー内の qtree SLAG</b>
AFS 内のボリューム へのアクセス	はい。	いいえ	N/A	N/A
Snapshot コピー内 のボリュームへのア クセス	はい。	いいえ	N/A	N/A
AFS 内の qtree への アクセス（ qtree に SLAG が設定されて いる場合）	いいえ	いいえ	はい。	いいえ
AFS 内の qtree への アクセス（ qtree に SLAG が設定されて いない場合）	はい。	いいえ	いいえ	いいえ
Snapshot コピー内 の qtree へのアクセ ス（ qtree に SLAG が設定されている場 合）	いいえ	いいえ	はい。	いいえ
Snapshot コピー内 の qtree へのアクセ ス（ qtree に SLAG が設定されていない 場合）	はい。	いいえ	いいえ	いいえ

ストレージレベルのアクセス保護に関する情報を表示します

ストレージレベルのアクセス保護は、ボリュームまたは qtree に適用される 3 番目のセキュリティレイヤです。ストレージレベルのアクセス保護設定は、Windows のプロパティウィンドウでは表示できません。ストレージレベルのアクセス保護セキュリティに関する情報を表示するには、ONTAP CLI を使用する必要があります。この情報を使用して、構成の検証や、アクセスに関する問題のトラブルシューティングを行うことができ

ます。

このタスクについて

Storage Virtual Machine（SVM）の名前、およびストレージレベルのアクセス保護セキュリティ情報を表示するボリュームまたは qtree のパスを入力する必要があります。出力は要約形式または詳細なリストで表示できます。

ステップ

1. ストレージレベルのアクセス保護セキュリティ設定を必要な詳細レベルで表示します。

表示する情報	入力するコマンド
要約形式で表示されます	<code>vserver security file-directory show -vserver vserver_name -path path</code>
詳細が表示されます	<code>vserver security file-directory show -vserver vserver_name -path path -expand-mask true</code>

例

次の例は、パスにあるNTFSセキュリティ形式のボリュームのストレージレベルのアクセス保護セキュリティ情報を表示します /datavol1 SVM vs1：



```
cluster::> vsriver security file-directory show -vsriver vs1 -path
/datavol1
```

```

    Vserver: vs1
    File Path: /datavol1
    File Inode Number: 77
    Security Style: ntfs
    Effective Style: ntfs
    DOS Attributes: 10
    DOS Attributes in Text: ----D---
    Expanded Dos Attributes: -
    Unix User Id: 0
    Unix Group Id: 0
    Unix Mode Bits: 777
    Unix Mode Bits in Text: rwxrwxrwx
    ACLs: NTFS Security Descriptor
          Control:0x8004
          Owner:BUILTIN\Administrators
          Group:BUILTIN\Administrators
          DACL - ACEs
                ALLOW-Everyone-0x1f01ff
                ALLOW-Everyone-0x10000000-OI|CI|IO

    Storage-Level Access Guard security
    SACL (Applies to Directories):
          AUDIT-EXAMPLE\Domain Users-0x120089-FA
          AUDIT-EXAMPLE\engineering-0x1f01ff-SA
    DACL (Applies to Directories):
          ALLOW-EXAMPLE\Domain Users-0x120089
          ALLOW-EXAMPLE\engineering-0x1f01ff
          ALLOW-NT AUTHORITY\SYSTEM-0x1f01ff
    SACL (Applies to Files):
          AUDIT-EXAMPLE\Domain Users-0x120089-FA
          AUDIT-EXAMPLE\engineering-0x1f01ff-SA
    DACL (Applies to Files):
          ALLOW-EXAMPLE\Domain Users-0x120089
          ALLOW-EXAMPLE\engineering-0x1f01ff
          ALLOW-NT AUTHORITY\SYSTEM-0x1f01ff
```

次の例は、パスにあるmixedセキュリティ形式のボリュームに関するストレージレベルのアクセス保護の情報を表示します /datavol5 (SVM vs1)。このボリュームの最上位には、UNIX 対応のセキュリティが設定されています。ボリュームにはストレージレベルのアクセス保護セキュリティが設定されています。

```

cluster1::> vserver security file-directory show -vserver vs1 -path
/datavol5

      Vserver: vs1
      File Path: /datavol5
      File Inode Number: 3374
      Security Style: mixed
      Effective Style: unix
      DOS Attributes: 10
      DOS Attributes in Text: ----D---
      Expanded Dos Attributes: -
      Unix User Id: 0
      Unix Group Id: 0
      Unix Mode Bits: 755
      Unix Mode Bits in Text: rwxr-xr-x
      ACLs: Storage-Level Access Guard security
      SACL (Applies to Directories):
        AUDIT-EXAMPLE\Domain Users-0x120089-FA
        AUDIT-EXAMPLE\engineering-0x1f01ff-SA
      DACL (Applies to Directories):
        ALLOW-EXAMPLE\Domain Users-0x120089
        ALLOW-EXAMPLE\engineering-0x1f01ff
        ALLOW-NT AUTHORITY\SYSTEM-0x1f01ff
      SACL (Applies to Files):
        AUDIT-EXAMPLE\Domain Users-0x120089-FA
        AUDIT-EXAMPLE\engineering-0x1f01ff-SA
      DACL (Applies to Files):
        ALLOW-EXAMPLE\Domain Users-0x120089
        ALLOW-EXAMPLE\engineering-0x1f01ff
        ALLOW-NT AUTHORITY\SYSTEM-0x1f01ff

```

ストレージレベルのアクセス保護を削除します

ストレージレベルのアクセスセキュリティの設定が不要になった場合は、ボリュームや qtree からストレージレベルのアクセス保護を削除できます。ストレージレベルのアクセス保護を削除しても、通常の NTFS のファイルやディレクトリのセキュリティは変更されたり削除されたりしません。

#### 手順

1. を使用して、ボリュームまたは qtree にストレージレベルのアクセス保護が設定されていることを確認します vserver security file-directory show コマンドを実行します

```
vserver security file-directory show -vserver vs1 -path /datavol2
```

```

        Vserver: vs1
        File Path: /datavol2
    File Inode Number: 99
        Security Style: ntfs
        Effective Style: ntfs
        DOS Attributes: 10
    DOS Attributes in Text: ----D---
    Expanded Dos Attributes: -
        Unix User Id: 0
        Unix Group Id: 0
        Unix Mode Bits: 777
    Unix Mode Bits in Text: rwxrwxrwx
        ACLs: NTFS Security Descriptor
            Control:0xbf14
            Owner:BUILTIN\Administrators
            Group:BUILTIN\Administrators
            SACL - ACEs
                AUDIT-EXAMPLE\Domain Users-0xf01ff-OI|CI|FA
            DACL - ACEs
                ALLOW-EXAMPLE\Domain Admins-0x1f01ff-OI|CI
                ALLOW-EXAMPLE\Domain Users-0x1301bf-OI|CI

        Storage-Level Access Guard security
        DACL (Applies to Directories):
            ALLOW-BUILTIN\Administrators-0x1f01ff
            ALLOW-CREATOR OWNER-0x1f01ff
            ALLOW-EXAMPLE\Domain Admins-0x1f01ff
            ALLOW-EXAMPLE\Domain Users-0x120089
            ALLOW-NT AUTHORITY\SYSTEM-0x1f01ff
        DACL (Applies to Files):
            ALLOW-BUILTIN\Administrators-0x1f01ff
            ALLOW-CREATOR OWNER-0x1f01ff
            ALLOW-EXAMPLE\Domain Admins-0x1f01ff
            ALLOW-EXAMPLE\Domain Users-0x120089
            ALLOW-NT AUTHORITY\SYSTEM-0x1f01ff

```

2. を使用して、ストレージレベルのアクセス保護を削除します vserver security file-directory remove-slag コマンドを実行します

```
vserver security file-directory remove-slag -vserver vs1 -path /datavol2
```

3. を使用して、ボリュームまたはqtreeからストレージレベルのアクセス保護が削除されたことを確認します vserver security file-directory show コマンドを実行します

```
vserver security file-directory show -vserver vs1 -path /datavol2
```

```

Vserver: vs1
File Path: /datavol2
File Inode Number: 99
Security Style: ntfs
Effective Style: ntfs
DOS Attributes: 10
DOS Attributes in Text: ----D---
Expanded Dos Attributes: -
Unix User Id: 0
Unix Group Id: 0
Unix Mode Bits: 777
Unix Mode Bits in Text: rwxrwxrwx
ACLs: NTFS Security Descriptor
Control:0xbf14
Owner:BUILTIN\Administrators
Group:BUILTIN\Administrators
SACL - ACEs
AUDIT-EXAMPLE\Domain Users-0xf01ff-OI|CI|FA
DACL - ACEs
ALLOW-EXAMPLE\Domain Admins-0x1f01ff-OI|CI
ALLOW-EXAMPLE\Domain Users-0x1301bf-OI|CI

```

## SMB を使用したファイルアクセスの管理

ローカルユーザおよびローカルグループを使用して認証と許可を行います

**ONTAP** でのローカルユーザとローカルグループの使用方法

ローカルユーザとローカルグループの概念

ローカルユーザとローカルグループを設定して使用するかどうかを決定する前に、ローカルユーザとローカルグループの定義を理解し、基本的ないくつかの情報を理解しておく必要があります。

### • \* ローカルユーザー \*

一意の Security Identifier (SID ; セキュリティ識別子) を持つユーザアカウント。そのユーザアカウントを作成した Storage Virtual Machine (SVM) 上でのみ認識されます。ローカルユーザアカウントには、ユーザ名や SID などの一連の属性があります。ローカルユーザアカウントは、NTLM 認証を使用して CIFS サーバ上でローカルに認証します。

ユーザアカウントには次のような用途があります。

- ユーザに `_ ユーザ権限の管理 _` 権限を付与するために使用します。
- SVM が所有するファイルリソースおよびフォルダリソースに対する共有レベルとファイルレベルのアクセスを制御する。

- \* ローカルグループ \*

一意の SID を持つグループ。そのグループを作成した SVM 上でのみ認識が可能です。グループには一連のメンバーが含まれます。メンバーは、ローカルユーザ、ドメインユーザ、ドメイングループ、およびドメインマシンアカウントです。グループは、作成、変更、または削除できます。

グループにはいくつかの用途があります。

- メンバーに `_User Rights Management_Privileges` を付与するために使用します。
- SVM が所有するファイルリソースおよびフォルダリソースに対する共有レベルとファイルレベルのアクセスを制御する。

- \* ローカルドメイン \*

ローカルスコープを持つドメイン。SVM によりバインドされています。ローカルドメインの名前は CIFS サーバの名前です。ローカルユーザとローカルグループはローカルドメインに含まれています。

- \* Security Identifier (SID ; セキュリティ識別子) \*

SID は、Windows 形式のセキュリティプリンシパルを識別する可変長の数値です。たとえば、通常の SID の場合は、次のような形式になります。S-1-5-21-3139654847-1303905135-2517279418-123456。

- \* NTLM 認証 \*

CIFS サーバ上のユーザの認証で使用される、Microsoft Windows のセキュリティ方式。

- \* 複製されたクラスタデータベース (RDB) \*

クラスタ内の各ノードのインスタンスを持つ複製されたデータベース。ローカルユーザとローカルグループのオブジェクトは、RDB に格納されます。

ローカルユーザおよびローカルグループを作成する理由

Storage Virtual Machine (SVM) でローカルユーザやローカルグループを作成する理由はいくつかあります。たとえば、ドメインコントローラ (DC) を使用できないときでも、ローカルユーザアカウントを使用して SMB サーバにアクセスできます。ローカルグループを使用して権限を割り当てる場合や、SMB サーバがワークグループにある場合もあります。

ローカルユーザアカウントを作成する理由には、次のようなものがあります。

- SMB サーバがワークグループにあり、ドメインユーザを使用できない。

ワークグループ設定にはローカルユーザが必要です。

- ドメインコントローラを使用できないときに、SMB サーバで認証してログインできるようにする。

ドメインコントローラがダウンしている場合や、ネットワークの問題によって SMB サーバからドメインコントローラに接続できない場合でも、ローカルユーザであれば、NTLM 認証を使用して SMB サーバに認証できます。

- ローカル・ユーザに `_ ユーザ権限の管理 _` 権限を割り当てる

*User Rights Management* は、ユーザとグループに付与する SVM の権限を SMB サーバ管理者が制御できる機能です。ユーザに権限を割り当てるには、ユーザのアカウントにそれらの権限を割り当てるか、ユーザをそれらの権限が割り当てられたローカルグループのメンバーにします。

ローカルグループを作成する理由には、次のようなものがあります。

- SMB サーバがワークグループにあり、ドメイングループを使用できない。

ワークグループにローカルグループを設定する必要はありませんが、設定するとローカルワークグループユーザのアクセス権限を管理するのに役立ちます。

- 共有やファイルアクセスの制御にローカルグループを使用して、ファイルやフォルダのリソースへのアクセスを制御する。
- カスタマイズした `_ ユーザ権限の管理 _` 権限を持つローカルグループを作成する。

権限があらかじめ定義された組み込みのユーザグループがいくつか用意されています。カスタマイズした一連の権限を割り当てるには、ローカルグループを作成し、そのグループに必要な権限を割り当てます。その後、ローカルグループにローカルユーザ、ドメインユーザ、およびドメイングループを追加します。

## 関連情報

[ローカルユーザ認証の仕組み](#)

[サポートされる権限のリスト](#)

## ローカルユーザ認証の仕組み

CIFS サーバのデータにアクセスする前に、ローカルユーザは認証されたセッションを作成する必要があります。

SMB はセッションベースであるため、ユーザの ID は、最初にセッションがセットアップされたときに一度だけ確認できます。CIFS サーバでは、ローカルユーザの認証時に NTLM ベースの認証が使用されます。NTLMv1 と NTLMv2 の両方がサポートされています。

ONTAP では、3 つの事例でローカル認証が使用されます。各事例は、ユーザ名のドメイン部分（`DOMAIN\user` 形式）が CIFS サーバのローカルドメイン名（CIFS サーバ名）と一致するかどうかによって異なります。

- ドメイン部分が一致します

データへのアクセスを要求するときにローカルユーザクレデンシャルを指定したユーザが、CIFS サーバでローカルに認証されます。

- ドメイン部分が一致しません

ONTAP は、CIFS サーバが属しているドメインのドメインコントローラで NTLM 認証を試行します。認証に成功した場合は、ログインが完了します。成功しなかった場合は、認証が失敗した理由によって次の動作が異なります。

たとえば、ユーザは Active Directory 内に存在するが、パスワードが無効であるか期限切れになっている

場合は、ONTAP は CIFS サーバ上の対応するローカルユーザアカウントの使用を試みません。代わりに、認証は失敗します。その他にも、ONTAP が CIFS サーバ上の対応するローカルアカウントを使用している場合、そのアカウントが存在するときは、NetBIOS ドメイン名が一致していなくても認証に使用する場合があります。たとえば、一致するドメインアカウントが存在するが無効になっている場合、ONTAP は、CIFS サーバ上の対応するローカルアカウントを認証に使用します。

- ドメイン部分は指定されません

ONTAP はまず、ローカルユーザとしての認証を試行します。ローカルユーザとしての認証に失敗した場合は、ONTAP が、CIFS サーバが属しているドメインのドメインコントローラでユーザを認証します。

ローカルユーザまたはドメインユーザの認証が完了したら、ONTAP でローカルグループメンバーシップおよび権限が考慮される完全なユーザアクセストークンが構成されます。

ローカルユーザの NTLM 認証の詳細については、Microsoft Windows のマニュアルを参照してください。

## 関連情報

### ローカルユーザ認証の有効化と無効化

## ユーザアクセストークンの構成方法

ユーザが共有をマッピングすると、認証された SMB セッションが確立され、ユーザアクセストークンが構成されます。このトークンには、ユーザ、ユーザのグループメンバーシップ、累積権限、マッピングされた UNIX ユーザのそれぞれについて、情報が格納されています。

この機能が無効になっていないかぎり、ローカルユーザとローカルグループの両方の情報がユーザアクセストークンに追加されます。アクセストークンの構成方法は、ローカルユーザのログインと Active Directory ドメインユーザのログインでは、方法が異なります。

- ローカルユーザログイン

ローカルユーザは複数のローカルグループのメンバーになることができますが、ローカルグループを他のローカルグループのメンバーにすることはできません。ローカルユーザアクセストークンは、その特定のローカルユーザが属するグループに割り当てられたすべての権限の組み合わせから構成されます。

- ドメイン・ユーザ・ログイン

ドメインユーザのログインでは、ONTAP は、ユーザの SID と、そのユーザが属するすべてのドメイングループの SID が格納されたユーザアクセストークンを取得します。ONTAP は、ユーザドメイングループのローカルメンバーシップ（存在する場合）が提供するアクセストークンとドメインユーザアクセストークンとの組み合わせを使用します。また、ドメインユーザに割り当てられた直接権限や、ドメイングループメンバーシップの直接権限も使用します。

ローカルユーザとドメインユーザの両方のログインで、プライマリグループ RID もユーザアクセストークン用に設定されています。デフォルトのRIDはです Domain Users (RID 513)。デフォルトは変更できません。

Windows から UNIX へのネームマッピングと、UNIX から Windows へのネームマッピングのプロセスでは、ローカルアカウントとドメインアカウントのどちらについても同じルールが適用されます。



UNIX ユーザがローカルアカウントに自動的にマッピングされることはありません。このマッピングが必要な場合は、既存のネームマッピングコマンドを使用して明示的なマッピングルールを指定する必要があります。

ローカルグループを含む SVM での SnapMirror の使用に関するガイドラインを次に示します

ローカルグループを含む SVM によって所有されているボリュームで SnapMirror を設定する際は、一定のガイドラインに注意する必要があります。

SnapMirror によって別の SVM にレプリケートされるファイル、ディレクトリ、または共有に適用する ACE ではローカルグループを使用できません。SnapMirror 機能を使用して別の SVM 上のボリュームに対する DR ミラーを作成する場合に、そのボリュームにローカルグループの ACE があるときは、ミラーには ACE は適用されません。データが別の SVM にレプリケートされる場合、実質的に、そのデータは別のローカルドメインに格納されることになります。ローカルユーザとローカルグループに付与されるアクセス権は、そのオブジェクトが最初に作成された SVM のスコープ内でのみ有効です。

**CIFS** サーバを削除したときのローカルユーザとローカルグループに対する影響

CIFS サーバを作成すると、デフォルトの一連のローカルユーザとローカルグループが作成され、CIFS サーバをホストする Storage Virtual Machine (SVM) に関連付けられます。SVM 管理者は、ローカルユーザやローカルグループをいつでも作成することができます。CIFS サーバを削除するときは、それを実行した場合のローカルユーザとローカルグループに対する影響について理解しておく必要があります。

ローカルユーザとローカルグループは SVM に関連付けられます。そのため、セキュリティの観点から、CIFS サーバを削除してもそれらが削除されることはありません。CIFS サーバを削除してもローカルユーザとローカルグループは削除されませんが、表示されなくなります。SVM で CIFS サーバを再作成するまで、表示したり管理したりすることはできません。



CIFS サーバの管理ステータスは、ローカルユーザやローカルグループが表示されるかどうかには影響しません。

**Microsoft** 管理コンソールでのローカルユーザとローカルグループの情報の表示

Microsoft 管理コンソールを使用して、ローカルユーザとローカルグループのそれぞれの情報を表示できます。ONTAP の今回のリリースでは、Microsoft 管理コンソールで、ローカルユーザとローカルグループに対する上記以外の管理タスクを実行することはできません。

リポートに関するガイドライン

ローカルユーザとグループを使用してファイルアクセスまたはユーザ権限を管理している場合に、ローカルユーザとグループをサポートしない ONTAP リリースにクラスタをリポートするときは、一定の考慮事項に注意する必要があります。

- セキュリティ上の理由から、ONTAP をローカルユーザとグループの機能をサポートしないバージョンにリポートしても、設定されているローカルユーザ、グループ、および権限に関する情報は削除されません。



- ONTAP の以前のメジャーバージョンにリバートする際、ONTAP では認証とクレデンシャルの作成時にローカルユーザとローカルグループは使用されません。
- ローカルユーザとローカルグループは、ファイルおよびフォルダの ACL から削除されません。
- ローカルユーザまたはローカルグループに付与された権限に基づいて許可されるアクセスに依存するファイルアクセス要求は拒否されます。

アクセスを許可するには、ローカルユーザとローカルグループオブジェクトではなく、ドメインオブジェクトに基づいてアクセスを許可するようにファイル権限を再設定する必要があります。

ローカル権限とは

サポートされる権限のリスト

ONTAP には、一連のサポートされる権限があらかじめ定義されています特定の事前定義されたローカルグループには、これらの権限の一部がデフォルトで追加されています。事前定義グループの権限は追加または削除できます。また、新しいローカルユーザまたはローカルグループを作成して、そのグループや、既存のドメインユーザおよびグループに権限を追加することもできます。

次の表に、Storage Virtual Machine（SVM）でサポートされる権限の一覧と、その権限が割り当てられている BUILTIN グループを示します。

権限の名前	デフォルトのセキュリティ設定	説明
SeTcbPrivilege	なし	オペレーティングシステムの一部として機能します
SeBackupPrivilege	BUILTIN\Administrators、 BUILTIN\Backup Operators	ACL を無視してファイルとディレクトリをバックアップします
SeRestorePrivilege	BUILTIN\Administrators、 BUILTIN\Backup Operators	ファイルおよびディレクトリをリストアし、ACL を上書きすべての有効なユーザまたはグループの SID をファイル所有者として設定します
SeTakeOwnershipPrivilege	BUILTIN\Administrators	ファイルまたはその他のオブジェクトの所有権を取得します
SeSecurityPrivilege	BUILTIN\Administrators	監査の管理  これには、セキュリティログの表示、ダンプ、およびクリアが含まれます。

権限の名前	デフォルトのセキュリティ設定	説明
SeChangeNotifyPrivilege	BUILTIN\Administrators、 BUILTIN\Backup Operators、 BUILTIN\Power Users、 BUILTIN\Users、 Everyone	トラバースチェックのバイパス  この権限を持つユーザには、フォルダ、シンボリックリンク、ジャンクションをトラバースするためのトラバース (x) 権限は必要ありません。

#### 関連情報

- [ローカル権限を割り当てます](#)
- [トラバースチェックのバイパスの設定](#)

#### 権限を割り当てます

ローカルユーザまたはドメインユーザに権限を直接割り当てることができます。また、ユーザに付与する権限と一致する権限が割り当てられているローカルグループにユーザを割り当てることができます。

- 作成したグループに一連の権限を割り当てることができます。

その後、ユーザに付与する権限が割り当てられているグループにユーザを追加します。

- また、ローカルユーザおよびドメインユーザを、デフォルトの権限がユーザに付与する権限と一致している事前定義グループに割り当てることができます。

#### 関連情報

- [ローカルまたはドメインのユーザまたはグループに対する権限の追加](#)
- [ローカルまたはドメインのユーザまたはグループの権限を削除しています](#)
- [ローカルまたはドメインのユーザまたはグループの権限をリセットしています](#)
- [トラバースチェックのバイパスの設定](#)

**BUILTIN** グループとローカル管理者アカウントの使用に関するガイドラインを次に示します

**BUILTIN** グループとローカル管理者アカウントを使用する場合は、一定のガイドラインに注意する必要があります。たとえば、ローカル管理者アカウントは、名前の変更は可能ですが、削除はできません。

- Administrator アカウントは、名前の変更は可能ですが、削除はできません。
- Administrator アカウントは BUILTIN\Administrators グループから削除できません。
- BUILTIN グループは、名前の変更は可能ですが、削除はできません。

BUILTIN グループの名前を変更したあと、よく知られた名前を使用して別のローカルオブジェクトを作成できますが、そのオブジェクトには新しい RID が割り当てられます。

- ローカルゲストアカウントがありません。

## 関連情報

### 事前定義の BUILTIN グループとそのデフォルトの権限

#### ローカルユーザパスワードの要件

デフォルトでは、ローカルユーザのパスワードは複雑さの要件を満たしている必要があります。パスワードの複雑さの要件は、Microsoft Windows\_Local セキュリティポリシー \_ で定義されている要件に似ています。

パスワードは次の基準を満たしている必要があります。

- 6 文字以上にする必要があります
- ユーザアカウント名を含めることはできません
- 次の 4 種類のうちの 3 種類以上の文字を含める必要があります。
  - 大文字のアルファベット (A~Z)
  - 小文字のアルファベット (a~z)
  - 数字 (0~9)
  - 特殊文字：

~@#\$% { キャレット } & \* \_ + = \ | ( ) [] ; " < > , . ? /

## 関連情報

### ローカル SMB ユーザに対するパスワードの複雑さの要件の有効化と無効化

#### CIFS サーバのセキュリティ設定に関する情報を表示する

#### ローカルユーザのアカウントパスワードを変更しています

#### 事前定義の BUILTIN グループとそのデフォルトの権限

ローカルユーザまたはドメインユーザのメンバーシップを、ONTAP の事前定義された一連の BUILTIN グループに割り当てることができます。事前定義グループには、事前定義された権限が割り当てられ

次の表に、事前定義グループを示します。

事前定義の <b>BUILTIN</b> グループ	デフォルトの権限
<p>BUILTIN\Administrators544番</p> <p>最初に作成されたとき、ローカル Administrator RIDが500のアカウントは、自動的にこのグループのメンバーになります。Storage Virtual Machine (SVM) がドメインに参加している場合は、domain\Domain Admins グループがグループに追加されます。SVMがドメインから削除された場合は domain\Domain Admins グループがグループから削除されます。</p>	<ul style="list-style-type: none"> <li>• SeBackupPrivilege</li> <li>• SeRestorePrivilege</li> <li>• SeSecurityPrivilege</li> <li>• SeTakeOwnershipPrivilege</li> <li>• SeChangeNotifyPrivilege</li> </ul>
<p>BUILTIN\Power Users547番地</p> <p>このグループには、最初に作成された時点ではメンバーはありません。このグループのメンバーには、次のような特徴があります。</p> <ul style="list-style-type: none"> <li>• ローカルユーザとローカルグループを作成および管理できます。</li> <li>• 自分自身や他のオブジェクトをに追加することはできません BUILTIN\Administrators グループ：</li> </ul>	SeChangeNotifyPrivilege
<p>BUILTIN\Backup Operators住所は551</p> <p>このグループには、最初に作成された時点ではメンバーはありません。このグループのメンバーは、バックアップ目的で開いたファイルやフォルダの読み取りおよび書き込み権限を上書きできます。</p>	<ul style="list-style-type: none"> <li>• SeBackupPrivilege</li> <li>• SeRestorePrivilege</li> <li>• SeChangeNotifyPrivilege</li> </ul>
<p>BUILTIN\UsersRID 545</p> <p>最初に作成された時点では、このグループには（暗黙の以外に）メンバーはありません Authenticated Users 特殊グループ）。SVMがドメインに参加すると、が表示されます domain\Domain Users グループがこのグループに追加されます。SVMがドメインから削除された場合は domain\Domain Users グループがこのグループから削除されます。</p>	SeChangeNotifyPrivilege
<p>EveryoneSID S-1-1-0</p> <p>このグループには、ゲストを含むすべてのユーザが含まれます（ただし匿名ユーザは含まれません）。このグループは、暗黙のメンバーシップを持つ暗黙のグループです。</p>	SeChangeNotifyPrivilege

## 関連情報

[BUILTIN グループとローカル管理者アカウントの使用に関するガイドラインを次に示します](#)

[サポートされる権限のリスト](#)

[トラバースチェックのバイパスの設定](#)

ローカルユーザとローカルグループ機能を有効または無効にします

ローカルユーザとローカルグループ機能の概要を有効または無効にします

NTFS セキュリティ形式データのアクセス制御にローカルユーザとローカルグループを使用する前に、ローカルユーザとローカルグループ機能を有効にする必要があります。また、SMB 認証にローカルユーザを使用する場合は、ローカルユーザ認証機能を有効にする必要があります。

ローカルユーザとローカルグループ機能とローカルユーザ認証はデフォルトで有効になっています。有効になっていない場合は、ローカルユーザとローカルグループを設定して使用する前に有効にする必要があります。ローカルユーザとローカルグループ機能はいつでも無効にすることができます。

ローカルユーザとローカルグループ機能の明示的な無効化に加えて、ONTAP では、クラスタ内のノードがローカルユーザとローカルグループ機能をサポートしていないリリースの ONTAP にリバートされた場合にその機能が無効になります。クラスタ内のすべてのノードでその機能をサポートするバージョンの ONTAP が実行されるまで、ローカルユーザとローカルグループ機能は有効になりません。

## 関連情報

[ローカルユーザアカウントを変更します](#)

[ローカルグループを変更します](#)

[ローカルまたはドメインのユーザまたはグループに権限を追加します](#)

ローカルユーザとローカルグループを有効または無効にします

Storage Virtual Machine (SVM) での SMB アクセスに使用するローカルユーザとローカルグループを有効または無効にすることができます。ローカルユーザとローカルグループ機能はデフォルトで有効になっています。

このタスクについて

SMB 共有および NTFS ファイル権限の設定時にローカルユーザとローカルグループを使用でき、必要に応じて、SMB 接続の作成時の認証のためにローカルユーザを使用できます。認証にローカルユーザを使用するには、ローカルユーザとローカルグループ認証オプションも有効にする必要があります。

## 手順

1. 権限レベルを advanced に設定します。 `set -privilege advanced`
2. 次のいずれかを実行します。

ローカルユーザとローカルグループの設定	入力するコマンド
有効	<code>vserver cifs options modify -vserver vserver_name -is-local-users-and-groups-enabled true</code>
無効	<code>vserver cifs options modify -vserver vserver_name -is-local-users-and-groups-enabled false</code>

3. admin 権限レベルに戻ります。 `set -privilege admin`

#### 例

次の例は、SVM vs1 でローカルユーザとローカルグループ機能を有効にします。

```
cluster1::> set -privilege advanced
Warning: These advanced commands are potentially dangerous; use them
only when directed to do so by technical support personnel.
Do you wish to continue? (y or n): y

cluster1::*> vserver cifs options modify -vserver vs1 -is-local-users-and
-groups-enabled true

cluster1::*> set -privilege admin
```

#### 関連情報

[ローカルユーザ認証を有効または無効にします](#)

[ローカルユーザアカウントを有効または無効にします](#)

[ローカルユーザ認証を有効または無効にします](#)

Storage Virtual Machine（SVM）での SMB アクセスに関するローカルユーザ認証を有効または無効にすることができます。デフォルトでは、ローカルユーザ認証は許可されます。これは、SVM がドメインコントローラにアクセスできない場合、またはドメインレベルのアクセス制御を使用しない場合に役立ちます。

#### 作業を開始する前に

CIFS サーバでローカルユーザとローカルグループ機能を有効にする必要があります。

#### このタスクについて

ローカルユーザ認証はいつでも有効または無効にできます。SMB 接続の作成時の認証のためにローカルユーザを使用する場合は、CIFS サーバのローカルユーザとローカルグループオプションも有効にする必要があります。

#### 手順

1. 権限レベルを advanced に設定します。set -privilege advanced

2. 次のいずれかを実行します。

ローカル認証の設定	入力するコマンド
有効	<code>vserver cifs options modify -vserver vserver_name -is-local-auth-enabled true</code>
無効	<code>vserver cifs options modify -vserver vserver_name -is-local-auth-enabled false</code>

3. admin 権限レベルに戻ります。set -privilege admin

#### 例

次の例は、SVM vs1 でローカルユーザ認証を有効にします。

```
cluster1::>set -privilege advanced
Warning: These advanced commands are potentially dangerous; use them
only when directed to do so by technical support personnel.
Do you wish to continue? (y or n): y

cluster1::*> vserver cifs options modify -vserver vs1 -is-local-auth
-enabled true

cluster1::*> set -privilege admin
```

#### 関連情報

[ローカルユーザ認証の仕組み](#)

[ローカルユーザとローカルグループの有効化と無効化](#)

[ローカルユーザアカウントを管理します](#)

[ローカルユーザアカウントを変更します](#)

既存のユーザのフルネームや概要を変更したり、ユーザアカウントを有効または無効にしたりする場合は、ローカルユーザアカウントを変更します。また、ユーザ名が侵害を受けたり、管理上の目的で名前の変更が必要になった場合にも、ローカルユーザアカウントの名前を変更できます。

状況	入力するコマンド
ローカルユーザのフルネームの変更	<code>vserver cifs users-and-groups local-user modify -vserver vserver_name -user -name user_name -full-name text</code> フルネームにスペースが含まれている場合は、二重引用符で囲む必要があります。
ローカルユーザの概要を変更します	<code>vserver cifs users-and-groups local-user modify -vserver vserver_name -user -name user_name -description text</code> 概要にスペースが含まれている場合は、二重引用符で囲む必要があります。
ローカルユーザアカウントを有効または無効にします	<code>`vserver cifs users-and-groups local-user modify -vserver vserver_name -user-name user_name -is-account-disabled {true</code>
<code>false}`</code>	ローカルユーザアカウントの名前を変更します

#### 例

次の例は、Storage Virtual Machine（SVM、旧 Vserver）vs1 上のローカルユーザ「CIFS\_SERVER\sue」の名前を「CIFS\_SERVER\sue\_new」に変更します。

```
cluster1::> vserver cifs users-and-groups local-user rename -user-name
CIFS_SERVER\sue -new-user-name CIFS_SERVER\sue_new -vserver vs1
```

ローカルユーザアカウントを有効または無効にします

ユーザが Storage Virtual Machine（SVM）に格納されたデータに SMB 接続経由でアクセスできるようにするには、ローカルユーザアカウントを有効にします。また、そのユーザが SVM のデータに SMB 経由でアクセスできないようにするには、ローカルユーザアカウントを無効にします。

このタスクについて

ユーザアカウントを変更してローカルユーザを有効にします。

#### ステップ

1. 適切な操作を実行します。

状況	入力するコマンド
ユーザアカウントを有効にします	<code>vserver cifs users-and-groups local-user modify -vserver vserver_name -user-name user_name -is-account-disabled false</code>



状況	入力するコマンド
ユーザアカウントを無効にします	<pre>vserver cifs users-and-groups local-user modify -vserver vserver_name -user-name user_name -is-account -disabled true</pre>

## ローカルユーザのアカウントパスワードを変更する

ローカルユーザのアカウントパスワードを変更できます。これは、ユーザのパスワードが侵害された場合やユーザがパスワードを忘れた場合に役立ちます。

### ステップ

- 適切な操作を実行してパスワードを変更します。 `vserver cifs users-and-groups local-user set-password -vserver vserver_name -user-name user_name`

### 例

次の例は、Storage Virtual Machine（SVM、旧 Vserver） `vs1` に関連付けられたローカルユーザ「`CIFS_SERVER\sue`」のパスワードを設定します。

```
cluster1::> vserver cifs users-and-groups local-user set-password -user
-name CIFS_SERVER\sue -vserver vs1
```

Enter the new password:

Confirm the new password:

## 関連情報

[ローカル SMB ユーザに対するパスワードの複雑さの要件の有効化と無効化](#)

[CIFS サーバのセキュリティ設定に関する情報を表示する](#)

## ローカルユーザに関する情報を表示します

すべてのローカルユーザのリストを要約形式で表示できます。特定のユーザに対して設定されているアカウント設定を確認するには、そのユーザの詳細なアカウント情報、および複数のユーザのアカウント情報を表示します。この情報は、ユーザの設定を変更する必要があるかどうかを判断する場合に加えて、認証やファイルアクセスに関する問題のトラブルシューティングを行う場合にも役立ちます。

### このタスクについて

ユーザのパスワードに関する情報は表示されません。

### ステップ

- 次のいずれかを実行します。

状況	入力するコマンド
Storage Virtual Machine（SVM）のすべてのユーザに関する情報を表示する	<code>vserver cifs users-and-groups local-user show -vserver <i>vserver_name</i></code>
特定のユーザの詳細なアカウント情報を表示する	<code>vserver cifs users-and-groups local-user show -instance -vserver <i>vserver_name</i> -user-name <i>user_name</i></code>

コマンドの実行時に選択できるオプションのパラメータがほかにもあります。詳細については、のマニュアルページを参照してください。

## 例

次の例は、SVM vs1 のすべてのローカルユーザに関する情報を表示します。

```
cluster1::> vserver cifs users-and-groups local-user show -vserver vs1
Vserver  User Name                               Full Name      Description
-----
vs1      CIFS_SERVER\Administrator    James Smith    Built-in administrator
account
vs1      CIFS_SERVER\sue              Sue    Jones
```

ローカルユーザのグループメンバーシップに関する情報を表示します

ローカルユーザが属しているローカルグループに関する情報を表示できます。この情報を使用して、ユーザに付与する必要があるファイルやフォルダへのアクセスを確認できます。この情報は、ユーザに付与する必要があるファイルやフォルダへのアクセス権や、ファイルアクセスに関する問題のトラブルシューティングを行うタイミングを判断するのに役立ちます。

このタスクについて

コマンドをカスタマイズして、必要な情報のみを表示することができます。

## ステップ

1. 次のいずれかを実行します。

状況	入力するコマンド
指定したローカルユーザのローカルユーザメンバーシップに関する情報を表示します	<code>vserver cifs users-and-groups local-user show-membership -user-name <i>user_name</i></code>
このローカルユーザが属しているローカルグループのローカルユーザメンバーシップに関する情報を表示します	<code>vserver cifs users-and-groups local-user show-membership -membership <i>group_name</i></code>

状況	入力するコマンド
指定した Storage Virtual Machine（SVM）に関連付けられているローカルユーザのユーザメンバーシップに関する情報を表示する	<code>vserver cifs users-and-groups local-user show-membership -vserver vserver_name</code>
指定した SVM 上のすべてのローカルユーザに関する詳細情報を表示する	<code>vserver cifs users-and-groups local-user show-membership -instance -vserver vserver_name</code>

## 例

次の例は、SVM vs1 上のすべてのローカルユーザのメンバーシップ情報を表示します。ユーザ「CIFS\_SERVER\Administrator」は「BUILTIN\Administrators」グループのメンバーで、「CIFS\_SERVER\sue」は「CIFS\_SERVER\g1」グループのメンバーです。

```
cluster1::> vserver cifs users-and-groups local-user show-membership
-vserver vs1
Vserver      User Name                               Membership
-----
vs1          CIFS_SERVER\Administrator              BUILTIN\Administrators
              CIFS_SERVER\sue                      CIFS_SERVER\g1
```

## ローカルユーザアカウントを削除します

CIFS サーバに対するローカル SMB 認証や、SVM に格納されたデータへのアクセス権の定義に使用するローカルユーザアカウントが不要になった場合は、Storage Virtual Machine（SVM）から削除することができます。

### このタスクについて

ローカルユーザを削除する場合は、次の点に注意してください。

- ファイルシステムは変更されません。

このユーザを参照するファイルやディレクトリに対する Windows セキュリティ記述子は調整されません。

- ローカルユーザへのすべての参照がメンバーシップおよび権限のデータベースから削除されます。
- Administrator などの標準的な既知のユーザは削除できません。

## 手順

1. 削除するローカルユーザアカウントの名前を確認します。 `vserver cifs users-and-groups local-user show -vserver vserver_name`
2. ローカルユーザを削除します。 `vserver cifs users-and-groups local-user delete -vserver vserver_name -user-name username_name`
3. ユーザアカウントが削除されたことを確認します。 `vserver cifs users-and-groups local-user`

```
show -vserver vs1
```

例

次の例は、SVM vs1 に関連付けられたローカルユーザ「CIFS\_SERVER\sue」を削除します。

```
cluster1::> vs1 cifs users-and-groups local-user show -vserver vs1
Vserver  User Name                               Full Name           Description
-----  -
vs1      CIFS_SERVER\Administrator               James Smith        Built-in administrator
account
vs1      CIFS_SERVER\sue                        Sue    Jones

cluster1::> vs1 cifs users-and-groups local-user delete -vserver vs1
-user-name CIFS_SERVER\sue

cluster1::> vs1 cifs users-and-groups local-user show -vserver vs1
Vserver  User Name                               Full Name           Description
-----  -
vs1      CIFS_SERVER\Administrator               James Smith        Built-in administrator
account
```

ローカルグループを管理します

ローカルグループを変更します

既存のローカルグループの概要を変更するには、既存のローカルグループの名前を変更するか、グループの名前を変更します。

状況	使用するコマンド
ローカルグループの概要を変更します	<code>vs1 cifs users-and-groups local-group modify -vserver vs1 -group-name group_name -description text</code> 概要 にスペースが含まれている場合は、二重引用符で囲む必要があります。
ローカルグループの名前を変更します	<code>vs1 cifs users-and-groups local-group rename -vserver vs1 -group-name group_name -new-group-name new_group_name</code>

例

次の例では、ローカル・グループの名前を 'CIFS\_server\engineering' から 'CIFS\_server\engineering\_new' に変更します

```
cluster1::> vsserver cifs users-and-groups local-group rename -vsserver vs1
-group-name CIFS_SERVER\engineering -new-group-name
CIFS_SERVER\engineering_new
```

次の例では ' ローカル・グループの概要を変更します

```
cluster1::> vsserver cifs users-and-groups local-group modify -vsserver vs1
-group-name CIFS_SERVER\engineering -description "New Description"
```

ローカルグループに関する情報を表示します

クラスタまたは指定した Storage Virtual Machine （ SVM ） で設定されているすべてのローカルグループの一覧を表示できます。この情報は、 SVM に格納されているデータに対するファイルアクセスに関する問題や、 SVM のユーザ権限に関する問題のトラブルシューティングに役立ちます。

ステップ

1. 次のいずれかを実行します。

必要な情報	入力するコマンド
クラスタのすべてのローカルグループ	<code>vsserver cifs users-and-groups local-group show</code>
SVM のすべてのローカルグループ	<code>vsserver cifs users-and-groups local-group show -vsserver vsserver_name</code>

このコマンドを実行するときに選択できるオプションのパラメータがほかにもあります。詳細については、のマニュアルページを参照してください。

例

次の例は、 SVM vs1 のすべてのローカルグループに関する情報を表示します。

```
cluster1::> vsserver cifs users-and-groups local-group show -vsserver vs1
Vserver  Group Name                                Description
-----  -
vs1      BUILTIN\Administrators                     Built-in Administrators group
vs1      BUILTIN\Backup Operators                   Backup Operators group
vs1      BUILTIN\Power Users                       Restricted administrative privileges
vs1      BUILTIN\Users                             All users
vs1      CIFS_SERVER\engineering
vs1      CIFS_SERVER\sales
```

## ローカルグループメンバーシップを管理します

ローカルグループメンバーシップの管理では、ローカルユーザやドメインユーザの追加と削除、ドメイングループの追加と削除ができます。この機能は、特定のグループに対するアクセス制御に基づいてデータへのアクセスを制御したり、グループに関連した権限をユーザに付与したりする上で役に立ちます。

### このタスクについて

ローカルグループへのメンバーの追加に関するガイドラインを次に示します。

- 特殊なグループ `_Everyone` にユーザを追加することはできません。
- ローカルグループにユーザを追加する前に、あらかじめそのグループが存在している必要があります。
- ローカルグループにユーザを追加する前に、あらかじめそのユーザが存在している必要があります。
- 別のローカルグループにローカルグループを追加することはできません。
- ローカルグループにドメインユーザまたはグループを追加するには、Data ONTAP で名前を SID に解決できる必要があります。

ローカルグループからのメンバーの削除に関するガイドラインを次に示します。

- 特殊なグループ `_Everyone` からメンバーを削除することはできません。
- メンバーを削除するグループが存在している必要があります。
- ONTAP は、グループから削除するメンバーの名前を、対応する SID に対して解決できる必要があります。

### ステップ

1. グループのメンバーを追加または削除します。

状況	使用するコマンド
グループにメンバーを追加します	<pre>vserver cifs users-and-groups local-group add-members -vserver _vserver_name_ -group-name _group_name_ -member-names name[,...]</pre> カンマ区切りのリストに記載されたローカルユーザ、ドメインユーザ、ドメイングループを指定し、特定のローカルグループに追加します。
グループからメンバーを削除します	<pre>vserver cifs users-and-groups local-group remove-members -vserver _vserver_name_ -group-name _group_name_ -member-names name[,...]</pre> カンマ区切りのリストに記載されたローカルユーザ、ドメインユーザ、ドメイングループを指定し、特定のローカルグループから削除します。

次の例は、SVM vs1 上のローカルグループ「`S MB_server\sue`」とドメイングループ「`AD_DOM\dom_eng`」をローカルグループ「`S MB_server\engineering`」に追加します。

```
cluster1::> vserver cifs users-and-groups local-group add-members  
-vserver vs1 -group-name SMB_SERVER\engineering -member-names  
SMB_SERVER\sue,AD_DOMAIN\dom_eng
```

次の例は、SVM vs1 上のローカルグループ「SMB\_server\sue」と「SMB\_server\james」からローカルユーザ「SMB\_server\engineering」を削除します。

```
cluster1::> vserver cifs users-and-groups local-group remove-members  
-vserver vs1 -group-name SMB_SERVER\engineering -member-names  
SMB_SERVER\sue,SMB_SERVER\james
```

## 関連情報

### [ローカルグループのメンバーに関する情報を表示する](#)

ローカルグループのメンバーに関する情報を表示します

クラスタまたは指定した Storage Virtual Machine（SVM）で設定されているローカルグループのすべてのメンバーの一覧を表示できます。この情報は、ファイルアクセスに関する問題やユーザ権限に関する問題のトラブルシューティングに役立ちます。

## ステップ

1. 次のいずれかを実行します。

表示する情報	入力するコマンド
クラスタのすべてのローカルグループのメンバー	<code>vserver cifs users-and-groups local-group show-members</code>
SVM のすべてのローカルグループのメンバー	<code>vserver cifs users-and-groups local-group show-members -vserver vserver_name</code>

## 例

次の例は、SVM vs1 のすべてのローカルグループのメンバーに関する情報を表示します。

```
cluster1::> vsriver cifs users-and-groups local-group show-members
-vsvrrer vs1
Vsvrrer   Group Name                               Members
-----
vs1       BUILTIN\Administrators                     CIFS_SERVER\Administrator
                                                AD_DOMAIN\Domain Admins
                                                AD_DOMAIN\dom_grp1
                                                AD_DOMAIN\Domain Users
                                                AD_DOMAIN\dom_usr1
                                                CIFS_SERVER\james
BUILTIN\Users
CIFS_SERVER\engineering
```

ローカルグループを削除します

Storage Virtual Machine（SVM）に関連付けられたデータへのアクセス権を決定するのに必要なくなった場合や、SVM ユーザ権限をグループメンバーに割り当てての必要なくなった場合は、SVM からローカルグループを削除できます。

このタスクについて

ローカルグループを削除する場合は、次の点に注意してください。

- ファイルシステムは変更されません。

このグループを参照するファイルやディレクトリに対する Windows セキュリティ記述子は調整されません。

- グループが存在しない場合は、エラーが返されます。
- special\_every\_group は削除できません。
- BUILTIN\Administrators *BUILTIN\Users* などの組み込みのグループは削除できません。

手順

1. SVM上のローカルグループのリストを表示して、削除するローカルグループの名前を確認します。  
vsriver cifs users-and-groups local-group show -vsvrrer vsvrrer\_name
2. ローカルグループを削除します。 vsriver cifs users-and-groups local-group delete -vsvrrer vsvrrer\_name -group-name group\_name
3. グループが削除されたことを確認します。 vsriver cifs users-and-groups local-user show -vsvrrer vsvrrer\_name

例

次の例は、SVM vs1 に関連付けられたローカルグループ「CIFS\_SERVER\sales」を削除します。



```

cluster1::> vsriver cifs users-and-groups local-group show -vsriver vs1
Vserver      Group Name                Description
-----
vs1          BUILTIN\Administrators    Built-in Administrators group
vs1          BUILTIN\Backup Operators  Backup Operators group
vs1          BUILTIN\Power Users       Restricted administrative
privileges
vs1          BUILTIN\Users             All users
vs1          CIFS_SERVER\engineering
vs1          CIFS_SERVER\sales

cluster1::> vsriver cifs users-and-groups local-group delete -vsriver vs1
-group-name CIFS_SERVER\sales

cluster1::> vsriver cifs users-and-groups local-group show -vsriver vs1
Vserver      Group Name                Description
-----
vs1          BUILTIN\Administrators    Built-in Administrators group
vs1          BUILTIN\Backup Operators  Backup Operators group
vs1          BUILTIN\Power Users       Restricted administrative
privileges
vs1          BUILTIN\Users             All users
vs1          CIFS_SERVER\engineering

```

ローカルデータベースのドメインユーザおよびグループ名を更新します

CIFS サーバのローカルグループにドメインユーザやドメイングループを追加することができます。これらのドメインオブジェクトは、クラスタのローカルデータベースに登録されます。ドメインオブジェクトの名前を変更した場合は、ローカルデータベースを手動で更新する必要があります。

このタスクについて

ドメイン名を更新する Storage Virtual Machine （SVM）の名前を指定する必要があります。

手順

1. 権限レベルを advanced に設定します。 `set -privilege advanced`
2. 適切な操作を実行します。

ドメインユーザおよびドメイングループの更新後の処理	使用するコマンド
ドメインユーザとドメイングループについて、正常に更新されたものと更新できなかったものを表示する	<code>vsriver cifs users-and-groups update-names -vsriver vsriver_name</code>

ドメインユーザおよびドメイングループの更新後の処理	使用するコマンド
ドメインユーザとドメイングループについて、正常に更新されたものを表示する	<code>vserver cifs users-and-groups update-names -vserver vserver_name -display -failed-only false</code>
更新できなかったドメインユーザとドメイングループのみを表示します	<code>vserver cifs users-and-groups update-names -vserver vserver_name -display -failed-only true</code>
更新に関するすべてのステータス情報を非表示にします	<code>vserver cifs users-and-groups update-names -vserver vserver_name -suppress -all-output true</code>

3. admin 権限レベルに戻ります。 `set -privilege admin`

#### 例

次の例は、Storage Virtual Machine（SVM、旧 Vserver）vs1 に関連付けられているドメインユーザおよびグループの名前を更新します。前回の更新には依存する一連の名前を更新する必要があります。

```

cluster1::> set -privilege advanced
Warning: These advanced commands are potentially dangerous; use them
only when directed to do so by technical support personnel.
Do you wish to continue? (y or n): y

cluster1::*> vsserver cifs users-and-groups update-names -vsserver vs1

Vserver:          vs1
SID:              S-1-5-21-123456789-234565432-987654321-12345
Domain:          EXAMPLE1
Out-of-date Name: dom_user1
Updated Name:     dom_user2
Status:          Successfully updated

Vserver:          vs1
SID:              S-1-5-21-123456789-234565432-987654322-23456
Domain:          EXAMPLE2
Out-of-date Name: dom_user1
Updated Name:     dom_user2
Status:          Successfully updated

Vserver:          vs1
SID:              S-1-5-21-123456789-234565432-987654321-123456
Domain:          EXAMPLE1
Out-of-date Name: dom_user3
Updated Name:     dom_user4
Status:          Successfully updated; also updated SID "S-1-5-21-
123456789-234565432-987654321-123457"
                  to name "dom_user5"; also updated SID "S-1-5-21-
123456789-234565432-987654321-123458"
                  to name "dom_user6"; also updated SID "S-1-5-21-
123456789-234565432-987654321-123459"
                  to name "dom_user7"; also updated SID "S-1-5-21-
123456789-234565432-987654321-123460"
                  to name "dom_user8"

The command completed successfully. 7 Active Directory objects have been
updated.

cluster1::*> set -privilege admin

```

ローカル権限を管理します

ローカルまたはドメインのユーザまたはグループに権限を追加します

ローカルまたはドメインのユーザやグループのユーザ権限を管理できます。追加した権限は、これらのオブジェクトに割り当てられていたデフォルトの権限よりも優先されます。これにより、ユーザまたはグループに付与する権限をカスタマイズして、セキュリティを強化できます。

作業を開始する前に

権限を追加する対象となるローカルまたはドメインのユーザまたはグループがすでに存在している必要があります。

このタスクについて

オブジェクトに権限を追加すると、そのユーザまたはグループのデフォルトの権限は無効になります。権限を追加しても、以前に追加した権限は削除されません。

ローカルまたはドメインのユーザまたはグループに権限を追加する場合は、次の点に注意する必要があります。

- 権限は 1 つ以上追加できます。
- ドメインユーザまたはグループへの権限の追加時、ONTAP では、ドメインコントローラに接続してそのドメインユーザまたはグループを検証することがあります。

ONTAP からドメインコントローラに接続できない場合、コマンドが失敗することがあります。

手順

1. ローカルまたはドメインのユーザまたはグループに1つ以上の権限を追加します。 `vserver cifs users-and-groups privilege add-privilege -vserver _vserver_name_ -user-or-group-name name -privileges _privilege_[,...]`
2. 必要な権限がオブジェクトに適用されていることを確認します。 `vserver cifs users-and-groups privilege show -vserver vserver_name -user-or-group-name name`

例

次の例は、Storage Virtual Machine（SVM、旧 Vserver）vs1 上の「CIFS\_SERVER\sueo」ユーザに「`SeTcbPrivilege」権限と「`seeOwnershipPrivilege」権限を追加します。

```
cluster1::> vserver cifs users-and-groups privilege add-privilege -vserver
vs1 -user-or-group-name CIFS_SERVER\sue -privileges
SeTcbPrivilege,SeTakeOwnershipPrivilege

cluster1::> vserver cifs users-and-groups privilege show -vserver vs1
Vserver      User or Group Name      Privileges
-----
vs1          CIFS_SERVER\sue        SeTcbPrivilege
                                   SeTakeOwnershipPrivilege
```

ローカルまたはドメインのユーザまたはグループから権限を削除します

ローカルまたはドメインのユーザやグループのユーザ権限を管理するには、権限を削除します。これにより、ユーザとグループに付与される最大権限をカスタマイズして、セキュリティを強化できます。

作業を開始する前に

権限を削除する対象となるローカルまたはドメインのユーザまたはグループがすでに存在している必要があります。

このタスクについて

ローカルまたはドメインのユーザやグループの権限を削除するときは、次の点に注意してください。

- 1 つ以上の権限を削除できます。
- ドメインのユーザまたはグループの権限を削除する場合、ONTAP でそれらのユーザやグループを検証するために、ドメインコントローラに接続することがあります。

ONTAP からドメインコントローラに接続できない場合、コマンドが失敗することがあります。

手順

1. ローカルまたはドメインのユーザまたはグループから1つ以上の権限を削除します。 `vserver cifs users-and-groups privilege remove-privilege -vserver _vserver_name_ -user-or-group-name _name_ -privileges _privilege_[,...]`
2. 必要な権限がオブジェクトから削除されていることを確認します。 `vserver cifs users-and-groups privilege show -vserver vserver_name -user-or-group-name name`

例

次の例は、Storage Virtual Machine（SVM、旧 Vserver）vs1 上のユーザ「CIFS\_SERVER\sueo」から「`s eTcbPrivilege」および「`s eTakeOwnershipPrivilege」権限を削除します。

```
cluster1::> vserver cifs users-and-groups privilege show -vserver vs1
Vserver    User or Group Name      Privileges
-----
vs1        CIFS_SERVER\sue        SeTcbPrivilege
                                SeTakeOwnershipPrivilege

cluster1::> vserver cifs users-and-groups privilege remove-privilege
-vserver vs1 -user-or-group-name CIFS_SERVER\sue -privileges
SeTcbPrivilege,SeTakeOwnershipPrivilege

cluster1::> vserver cifs users-and-groups privilege show -vserver vs1
Vserver    User or Group Name      Privileges
-----
vs1        CIFS_SERVER\sue        -
```

ローカルまたはドメインのユーザとグループの権限をリセットします

ローカルまたはドメインのユーザやグループの権限をリセットできます。これは、ローカルまたはドメインのユーザやグループの権限に対して行った変更が不要になった場合や必要がなくなった場合に役立ちます。

このタスクについて

ローカルまたはドメインのユーザまたはグループの権限をリセットすると、そのオブジェクトの権限のエントリがすべて削除されます。

手順

1. ローカルまたはドメインのユーザまたはグループの権限をリセットします。 `vserver cifs users-and-groups privilege reset-privilege -vserver vserver_name -user-or-group-name name`
2. オブジェクトの権限がリセットされたことを確認します。 `vserver cifs users-and-groups privilege show -vserver vserver_name -user-or-group-name name`

例

次の例は、Storage Virtual Machine（SVM、旧 Vserver）vs1 上のユーザ「CIFS\_SERVER\sue」の権限をリセットしています。デフォルトでは、標準ユーザのアカウントには権限は関連付けられません。

```
cluster1::> vserver cifs users-and-groups privilege show
Vserver      User or Group Name      Privileges
-----
vs1          CIFS_SERVER\sue        SeTcbPrivilege
                                   SeTakeOwnershipPrivilege

cluster1::> vserver cifs users-and-groups privilege reset-privilege
-vserver vs1 -user-or-group-name CIFS_SERVER\sue

cluster1::> vserver cifs users-and-groups privilege show
This table is currently empty.
```

次の例では 'グループ ""BUILTIN\Administrators ""' の特権をリセットし '実質的に特権エントリを削除します

```
cluster1::> vserver cifs users-and-groups privilege show
Vserver      User or Group Name      Privileges
-----
vs1          BUILTIN\Administrators  SeRestorePrivilege
                                   SeSecurityPrivilege
                                   SeTakeOwnershipPrivilege

cluster1::> vserver cifs users-and-groups privilege reset-privilege
-vserver vs1 -user-or-group-name BUILTIN\Administrators

cluster1::> vserver cifs users-and-groups privilege show
This table is currently empty.
```

権限の上書きに関する情報を表示します

ドメインまたはローカルのユーザアカウントまたはグループに割り当てられているカスタムの権限に関する情報を表示できます。この情報は、必要なユーザ権限が適用されているかどうかを確認するのに役立ちます。

#### ステップ

1. 次のいずれかを実行します。

表示する情報	入力するコマンド
Storage Virtual Machine （SVM）上のすべてのドメインおよびローカルのユーザとグループのカスタム権限	<code>vserver cifs users-and-groups privilege show -vserver vserver_name</code>
SVM 上の特定のドメインまたはローカルのユーザとグループのカスタム権限	<code>vserver cifs users-and-groups privilege show -vserver vserver_name -user-or-group-name name</code>

このコマンドを実行するときに選択できるオプションのパラメータがほかにもあります。詳細については、のマニュアルページを参照してください。

#### 例

次のコマンドを実行すると、SVM vs1 のローカルまたはドメインのユーザとグループに明示的に関連付けられているすべての権限が表示されます。

```
cluster1::> vserver cifs users-and-groups privilege show -vserver vs1
```

Vserver	User or Group Name	Privileges
vs1	BUILTIN\Administrators	SeTakeOwnershipPrivilege SeRestorePrivilege
vs1	CIFS_SERVER\sue	SeTcbPrivilege SeTakeOwnershipPrivilege

## トラバースチェックのバイパスを設定する

### トラバースチェックのバイパスの設定の概要

トラバースチェックのバイパスは、トラバースするディレクトリに対する権限がユーザにない場合でも、ファイルのパスに含まれるすべてのディレクトリをユーザがトラバースできるかどうかを判断するユーザ権限です。トラバースチェックのバイパスを許可または拒否した場合の動作と、Storage Virtual Machine（SVM）でのユーザに対するトラバースチェックのバイパスの設定方法を理解しておく必要があります。

### トラバースチェックのバイパスを許可または拒否した場合の動作

- 許可した場合、ユーザがファイルにアクセスしようとする、中間ディレクトリのトラバース権限が ONTAP でチェックされないで、ファイルへのアクセスの可否が判別されます。
- 拒否した場合、ONTAP はファイルのパスにあるすべてのディレクトリでトラバース（実行）権限をチェックします。

中間ディレクトリのいずれかに「X」（トラバース権限）がない場合、ONTAP はファイルへのアクセスを拒否します。

## トラバースチェックのバイパスを設定する

ONTAP CLI を使用するか、Active Directory グループポリシーにこのユーザ権限を設定すると、トラバースチェックのバイパスを設定できます。

。SeChangeNotifyPrivilege 権限は、ユーザにトラバースチェックのバイパスを許可するかどうかを制御します。

- この権限を SVM のローカル SMB ユーザまたはグループ、ドメインユーザまたはグループに追加すると、トラバースチェックのバイパスを許可できます。
- この権限を SVM のローカル SMB ユーザまたはグループ、ドメインユーザまたはグループから削除すると、トラバースチェックのバイパスを拒否できます。

SVM の次の BUILTIN グループには、デフォルトでトラバースチェックのバイパス権限が割り当てられています。

- BUILTIN\Administrators
- BUILTIN\Power Users



- BUILTIN\Backup Operators
- BUILTIN\Users
- Everyone

これらのいずれかのグループのメンバーにトラバースチェックのバイパスを許可したくない場合は、グループからこの権限を削除する必要があります。

CLI を使用して SVM のローカル SMB ユーザおよびグループのトラバースチェックのバイパスを設定する場合は、次の点に注意する必要があります。

- カスタムのローカルグループまたはドメイングループのメンバーにトラバースチェックのバイパスを許可する場合は、を追加する必要があります SeChangeNotifyPrivilege そのグループへの特権。
- ローカルユーザまたはドメインユーザにトラバースチェックのバイパスを個別に許可する場合に、そのユーザがその権限を持つグループのメンバーでないときは、を追加できます SeChangeNotifyPrivilege そのユーザアカウントに対する権限。
- ローカルまたはドメインのユーザまたはグループのトラバースチェックのバイパスを無効にするには、を削除します SeChangeNotifyPrivilege いつでも特権。



特定のローカルまたはドメインのユーザまたはグループに対してトラバースチェックのバイパスを無効にするには、も削除する必要があります SeChangeNotifyPrivilege 権限を取得します Everyone グループ：

## 関連情報

[ユーザまたはグループにディレクトリのトラバースチェックのバイパスを許可する](#)

[ユーザまたはグループに対してディレクトリのトラバースチェックのバイパスを禁止します](#)

[ボリュームでの SMB ファイル名の変換のための文字マッピングを設定します](#)

[SMB 共有のアクセス制御リストを作成](#)

[ストレージレベルのアクセス保護を使用してファイルアクセスを保護](#)

[サポートされる権限のリスト](#)

[ローカルまたはドメインのユーザまたはグループに権限を追加します](#)

[ユーザまたはグループにディレクトリのトラバースチェックのバイパスを許可する](#)

トラバースするディレクトリに対する権限がユーザにない場合でも、ファイルへのパスに含まれるすべてのディレクトリをユーザがトラバースできるようにするには、を追加します SeChangeNotifyPrivilege Storage Virtual Machine (SVM) 上のローカルSMBユーザまたはグループに対する権限。デフォルトでは、ユーザはディレクトリのトラバースチェックをバイパスできます。

## 作業を開始する前に

- SVM上にSMBサーバが存在している必要があります。

- ローカルユーザとローカルグループのSMBサーバオプションが有効になっている必要があります。
- が格納されているローカルまたはドメインのユーザまたはグループ SeChangeNotifyPrivilege 追加する権限はすでに存在している必要があります。

#### このタスクについて

ドメインユーザまたはグループへの権限の追加時、ONTAP では、ドメインコントローラに接続してそのドメインユーザまたはグループを検証することがあります。ONTAP からドメインコントローラに接続できない場合、コマンドが失敗することがあります。

#### 手順

1. を追加して、トラバースチェックのバイパスを有効にします SeChangeNotifyPrivilege ローカルまたはドメインのユーザまたはグループに対する権限： `vserver cifs users-and-groups privilege add-privilege -vserver vserver_name -user-or-group-name name -privileges SeChangeNotifyPrivilege`

の値 `-user-or-group-name` パラメータは、ローカルユーザまたはローカルグループ、ドメインユーザまたはグループです。

2. 指定したユーザまたはグループでトラバースチェックのバイパスが有効になっていることを確認します。  
`vserver cifs users-and-groups privilege show -vserver vserver_name -user-or-group-name name`

#### 例

次のコマンドは、「example\eng」グループに属するユーザがを追加してディレクトリのトラバースチェックをバイパスできるようにします SeChangeNotifyPrivilege グループに対する権限：

```
cluster1::> vserver cifs users-and-groups privilege add-privilege -vserver
vs1 -user-or-group-name EXAMPLE\eng -privileges SeChangeNotifyPrivilege

cluster1::> vserver cifs users-and-groups privilege show -vserver vs1
Vserver      User or Group Name      Privileges
-----
vs1          EXAMPLE\eng             SeChangeNotifyPrivilege
```

#### 関連情報

[ユーザまたはグループに対するディレクトリのトラバースチェックのバイパスを禁止する](#)

ユーザまたはグループに対してディレクトリのトラバースチェックのバイパスを禁止します

トラバースするディレクトリに対する権限がユーザにないために、ファイルのパスに含まれるすべてのディレクトリをユーザがトラバースできないようにするには、を削除します SeChangeNotifyPrivilege Storage Virtual Machine (SVM) 上のローカルSMB ユーザまたはグループからの権限。

#### 作業を開始する前に

権限を削除する対象となるローカルまたはドメインのユーザまたはグループがすでに存在している必要があります。

## このタスクについて

ドメインのユーザまたはグループの権限を削除する場合、ONTAP でそれらのユーザやグループを検証するために、ドメインコントローラに接続することがあります。ONTAP からドメインコントローラに接続できない場合、コマンドが失敗することがあります。

## 手順

1. トラバースチェックのバイパスを禁止します。 `vserver cifs users-and-groups privilege remove-privilege -vserver vserver_name -user-or-group-name name -privileges SeChangeNotifyPrivilege`

コマンドは、を削除します `SeChangeNotifyPrivilege` の値で指定したローカルまたはドメインのユーザまたはグループの権限 `-user-or-group-name name` パラメータ

2. 指定したユーザまたはグループに対してトラバースチェックのバイパスが無効になっていることを確認します。 `vserver cifs users-and-groups privilege show -vserver vserver_name -user-or-group-name name`

## 例

次のコマンドを実行すると、「EXAMPLE\eng」グループに属するユーザに対して、ディレクトリのトラバースチェックのバイパスが禁止されます。

```
cluster1::> vserver cifs users-and-groups privilege show -vserver vs1
Vserver      User or Group Name      Privileges
-----
vs1          EXAMPLE\eng              SeChangeNotifyPrivilege

cluster1::> vserver cifs users-and-groups privilege remove-privilege
-vserver vs1 -user-or-group-name EXAMPLE\eng -privileges
SeChangeNotifyPrivilege

cluster1::> vserver cifs users-and-groups privilege show -vserver vs1
Vserver      User or Group Name      Privileges
-----
vs1          EXAMPLE\eng              -
```

## 関連情報

[ユーザまたはグループに対するディレクトリのトラバースチェックのバイパスを許可する](#)

ファイルセキュリティと監査ポリシーに関する情報を表示します

ファイルセキュリティと監査ポリシーの概要に関する情報を表示します

Storage Virtual Machine（SVM）上のボリュームに格納されたファイルとディレクトリのファイルセキュリティに関する情報を表示できます。FlexVol の監査ポリシーに関する情報を表示できます。設定されている場合、FlexVol ボリュームのストレージレベルのアクセス保護およびダイナミックアクセス制御セキュリティの設定に関する情報を表示できます。

ファイルセキュリティに関する情報を表示する

次のセキュリティ形式のボリュームと（ FlexVol の） qtree に格納されたデータに適用されているファイルセキュリティに関する情報を表示できます。

- NTFS
- 「 UNIX 」
- 混在

監査ポリシーに関する情報を表示する

次の NAS プロトコルを介した FlexVol ボリューム上のアクセスイベントを監査する監査ポリシーに関する情報を表示できます。

- SMB （すべてのバージョン）
- NFSv4.x に対応している

**Storage-Level Access Guard** （ **SLAG** ；ストレージレベルのアクセス保護）セキュリティに関する情報を表示する

ストレージレベルのアクセス保護セキュリティは、次のセキュリティ形式の FlexVol および qtree オブジェクトに適用できます。

- NTFS
- 混在
- UNIX （ボリュームが含まれる SVM で CIFS サーバが設定されている場合）

ダイナミックアクセス制御（ **DAC** ）セキュリティに関する情報を表示する

ダイナミックアクセス制御セキュリティは、次のセキュリティ形式の FlexVol ボリューム内のオブジェクトに適用できます。

- NTFS
- Mixed （オブジェクトに NTFS 対応のセキュリティが設定されている場合）

関連情報

[ストレージレベルのアクセス保護を使用したファイルアクセスの保護](#)

[ストレージレベルのアクセス保護に関する情報の表示](#)

**NTFS** セキュリティ形式のボリュームのファイルセキュリティに関する情報を表示します

セキュリティ形式と有効なセキュリティ形式、適用されている権限、DOS 属性に関する情報など、NTFS セキュリティ形式のボリューム上にあるファイルやディレクトリのセキュリティに関する情報を表示できます。この結果を使用して、セキュリティ設定の検証や、ファイルアクセスに関する問題のトラブルシューティングを行うことができます。

このタスクについて

Storage Virtual Machine（SVM）の名前、およびファイルまたはフォルダのセキュリティ情報を表示するデータのパスを入力する必要があります。出力は要約形式または詳細なリストで表示できます。

- NTFS セキュリティ形式のボリュームおよび qtree では、NTFS ファイルアクセス権と Windows のユーザおよびグループのみを使用してファイルアクセス権を決定するため、UNIX 関連の出力フィールドには表示専用の UNIX ファイルアクセス権情報が格納されます。
- ACL 出力は、NTFS セキュリティが適用されたファイルとフォルダについて表示されます。
- ストレージレベルのアクセス保護セキュリティは、ボリュームのルートまたは qtree で設定できるため、ストレージレベルのアクセス保護が設定されているボリュームまたは qtree パスの出力には、通常のファイル ACL とストレージレベルのアクセス保護 ACL の両方が表示されることがあります。
- 指定したファイルまたはディレクトリパスにダイナミックアクセス制御が設定されている場合は、ダイナミックアクセス制御 ACE に関する情報も出力に表示されます。

ステップ

1. ファイルとディレクトリのセキュリティ設定を必要な詳細レベルで表示します。

表示する情報	入力するコマンド
要約形式で表示されます	<code>vserver security file-directory show -vserver vs1 -path /</code>
詳細が表示されます	<code>vserver security file-directory show -vserver vs1 -path / -expand-mask true</code>

例

次の例は、パスに関するセキュリティ情報を表示します `/vol1 SVM vs1`：

```
cluster::> vserver security file-directory show -vserver vs1 -path /vol4
```

```

Vserver: vs1
File Path: /vol4
File Inode Number: 64
Security Style: ntfs
Effective Style: ntfs
DOS Attributes: 10
DOS Attributes in Text: ----D---
Expanded Dos Attributes: -
Unix User Id: 0
Unix Group Id: 0
Unix Mode Bits: 777
Unix Mode Bits in Text: rwxrwxrwx
ACLs: NTFS Security Descriptor
Control:0x8004
Owner:BUILTIN\Administrators
Group:BUILTIN\Administrators
DACL - ACEs
ALLOW-Everyone-0x1f01ff
ALLOW-Everyone-0x10000000-
```

OI|CI|IO

次の例は、マスクを展開してパスに関するセキュリティ情報を表示します /data/engineering SVM vs1 :

```
cluster::> vserver security file-directory show -vserver vs1 -path -path
/data/engineering -expand-mask true
```

```

Vserver: vs1
File Path: /data/engineering
File Inode Number: 5544
Security Style: ntfs
Effective Style: ntfs
DOS Attributes: 10
DOS Attributes in Text: ----D---
Expanded Dos Attributes: 0x10
...0 .... = Offline
.... ..0. .... = Sparse
.... .... 0... .... = Normal
.... .... ..0. .... = Archive
.... .... ...1 .... = Directory
.... .... .... .0.. = System
.... .... .... ..0. = Hidden
.... .... .... ...0 = Read Only
```

```

    Unix User Id: 0
    Unix Group Id: 0
    Unix Mode Bits: 777
Unix Mode Bits in Text: rwxrwxrwx
    ACLs: NTFS Security Descriptor
    Control:0x8004

```

```

    1... .. = Self Relative
    .0.. .. = RM Control Valid
    ..0. .. = SACL Protected
    ...0 .. = DACL Protected
    .... 0... .. = SACL Inherited
    .... .0.. .. = DACL Inherited
    .... ..0. .. = SACL Inherit Required
    .... ...0 .. = DACL Inherit Required
    .... .... .0. .... = SACL Defaulted
    .... .... ...0 .... = SACL Present
    .... .... .... 0... = DACL Defaulted
    .... .... .... .1.. = DACL Present
    .... .... .... ..0. = Group Defaulted
    .... .... .... ...0 = Owner Defaulted

```

```

Owner:BUILTIN\Administrators
Group:BUILTIN\Administrators
DACL - ACEs

```

```

    ALLOW-Everyone-0x1f01ff

```

	0... .. =
Generic Read	
	.0.. .. =
Generic Write	
	..0. .... =
Generic Execute	
	...0 .... =
Generic All	
	.... ..0 .... =
System Security	
	.... .... 1 .... =
Synchronize	
	.... .... 1... .. =
Write Owner	
	.... .... .1. .... =
Write DAC	
	.... .... ..1. .... =
Read Control	
	.... .... ...1 .... =
Delete	

	.....1..... =
Write Attributes	
	.....1.... =
Read Attributes	
	.....1... =
Delete Child	
	.....1. .... =
Execute	
	.....1 .... =
Write EA	
	.....1... =
Read EA	
	.....1... =
Append	
	.....1. .... =
Write	
	.....1 =
Read	
	ALLOW-Everyone-0x10000000-OI CI IO
	0.... .... =
Generic Read	
	.0... .... =
Generic Write	
	..0. .... =
Generic Execute	
	...1 .... =
Generic All	
	.....0 .... =
System Security	
	.....0 .... =
Synchronize	
	.....0 .... =
Write Owner	
	.....0... .... =
Write DAC	
	.....0. .... =
Read Control	
	.....0 .... =
Delete	
	.....0 .... =
Write Attributes	
	.....0... .... =
Read Attributes	
	.....0... .... =
Delete Child	



Execute	.....0..... =
Write EA	.....0..... =
Read EA	.....0..... =
Append	.....0..... =
Write	.....0..... =
Read	.....0..... =

次の例は、パスにあるボリュームの、ストレージレベルのアクセス保護セキュリティ情報を含むセキュリティ情報を表示します /datavol1 SVM vs1：

```
cluster::> vserver security file-directory show -vserver vs1 -path  
/datavol1
```

```
      Vserver: vs1  
      File Path: /datavol1  
File Inode Number: 77  
      Security Style: ntfs  
      Effective Style: ntfs  
      DOS Attributes: 10  
DOS Attributes in Text: ----D---  
Expanded Dos Attributes: -  
      Unix User Id: 0  
      Unix Group Id: 0  
      Unix Mode Bits: 777  
Unix Mode Bits in Text: rwxrwxrwx  
      ACLs: NTFS Security Descriptor  
            Control:0x8004  
            Owner: BUILTIN\Administrators  
            Group: BUILTIN\Administrators  
            DACL - ACEs  
                  ALLOW-Everyone-0x1f01ff  
                  ALLOW-Everyone-0x10000000-OI|CI|IO  
  
Storage-Level Access Guard security  
SACL (Applies to Directories):  
      AUDIT-EXAMPLE\Domain Users-0x120089-FA  
      AUDIT-EXAMPLE\engineering-0x1f01ff-SA  
DACL (Applies to Directories):  
      ALLOW-EXAMPLE\Domain Users-0x120089  
      ALLOW-EXAMPLE\engineering-0x1f01ff  
      ALLOW-NT AUTHORITY\SYSTEM-0x1f01ff  
SACL (Applies to Files):  
      AUDIT-EXAMPLE\Domain Users-0x120089-FA  
      AUDIT-EXAMPLE\engineering-0x1f01ff-SA  
DACL (Applies to Files):  
      ALLOW-EXAMPLE\Domain Users-0x120089  
      ALLOW-EXAMPLE\engineering-0x1f01ff  
      ALLOW-NT AUTHORITY\SYSTEM-0x1f01ff
```

#### 関連情報

[mixed セキュリティ形式のボリュームのファイルセキュリティに関する情報を表示する](#)

[UNIX セキュリティ形式のボリュームのファイルセキュリティに関する情報を表示する](#)

**mixed** セキュリティ形式のボリューム上のファイルセキュリティに関する情報を表示します

セキュリティ形式と有効なセキュリティ形式、適用されている権限、UNIXの所有者とグループに関する情報など、mixed セキュリティ形式のボリューム上にあるファイルやディレクトリのセキュリティに関する情報を表示できます。この結果を使用して、セキュリティ設定の検証や、ファイルアクセスに関する問題のトラブルシューティングを行うことができます。

このタスクについて

Storage Virtual Machine（SVM）の名前、およびファイルまたはフォルダのセキュリティ情報を表示するデータのパスを入力する必要があります。出力は要約形式または詳細なリストで表示できます。

- mixed セキュリティ形式のボリュームおよび qtree には、UNIX ファイル権限、モードビットまたは NFSv4 ACL、および NTFS ファイル権限を使用する一部のファイルおよびディレクトリを含めることができます。
- mixed セキュリティ形式のボリュームの最上位には、UNIX 対応のセキュリティまたは NTFS 対応のセキュリティを設定できます。
- ACL 出力は、NTFS または NFSv4 セキュリティが適用されたファイルとフォルダについてのみ表示されます。

このフィールドは、モードビットのアクセス権のみ（NFSv4 ACL はなし）が適用されている UNIX セキュリティ形式のファイルおよびディレクトリでは空になります。

- ACL 出力の所有者とグループの出力フィールドは、NTFS セキュリティ記述子の場合にのみ適用されます。
- ストレージレベルのアクセス保護セキュリティは、ボリュームのルートまたは qtree の有効なセキュリティ形式が UNIX であっても、mixed セキュリティ形式のボリュームまたは qtree で設定できるため、ストレージレベルのアクセス保護が設定されているボリュームまたは qtree パスの出力には、UNIX ファイル権限とストレージレベルのアクセス保護 ACL の両方が表示されることがあります。
- コマンドで入力したパスが、NTFS 対応のセキュリティを使用するデータへのパスである場合、そのファイルまたはディレクトリパスにダイナミックアクセス制御が設定されていれば、ダイナミックアクセス制御 ACE に関する情報も出力に表示されます。

ステップ

1. ファイルとディレクトリのセキュリティ設定を必要な詳細レベルで表示します。

表示する情報	入力するコマンド
要約形式で表示されます	<code>vserver security file-directory show -vserver vs1 -path /path</code>
詳細が表示されます	<code>vserver security file-directory show -vserver vs1 -path /path -expand-mask true</code>

例

次の例は、パスに関するセキュリティ情報を表示します /projects マスクを展開した形式でSVM vs1に格納します。この mixed セキュリティ形式のパスには、UNIX 対応のセキュリティが設定されています。

```
cluster1::> vserver security file-directory show -vserver vs1 -path  
/projects -expand-mask true
```

```
        Vserver: vs1  
        File Path: /projects  
File Inode Number: 78  
    Security Style: mixed  
    Effective Style: unix  
    DOS Attributes: 10  
DOS Attributes in Text: ----D---  
Expanded Dos Attributes: 0x10  
    ...0 .... = Offline  
    .... ..0. .... = Sparse  
    .... .... 0... .... = Normal  
    .... .... ..0. .... = Archive  
    .... .... ...1 .... = Directory  
    .... .... .... .0.. = System  
    .... .... .... ..0. = Hidden  
    .... .... .... ...0 = Read Only  
        Unix User Id: 0  
        Unix Group Id: 1  
        Unix Mode Bits: 700  
Unix Mode Bits in Text: rwx-----  
        ACLs: -
```

次の例は、パスに関するセキュリティ情報を表示します /data (SVM vs1)。この mixed セキュリティ形式のパスには、NTFS 対応のセキュリティが設定されています。

```
cluster1::> vserver security file-directory show -vserver vs1 -path /data
```

```

        Vserver: vs1
        File Path: /data
    File Inode Number: 544
        Security Style: mixed
        Effective Style: ntfs
        DOS Attributes: 10
    DOS Attributes in Text: ----D---
Expanded Dos Attributes: -
        Unix User Id: 0
        Unix Group Id: 0
        Unix Mode Bits: 777
    Unix Mode Bits in Text: rwxrwxrwx
        ACLs: NTFS Security Descriptor
            Control:0x8004
            Owner:BUILTIN\Administrators
            Group:BUILTIN\Administrators
            DACL - ACEs
                ALLOW-Everyone-0x1f01ff
                ALLOW-Everyone-0x10000000-
```

OI|CI|IO

次の例は、パスにあるボリュームに関するセキュリティ情報を表示します /datavol5 (SVM vs1)。この mixed セキュリティ形式のボリュームの最上位には、UNIX 対応のセキュリティが設定されています。ボリュームにはストレージレベルのアクセス保護セキュリティが設定されています。

```
cluster1::> vserver security file-directory show -vserver vs1 -path /datavol5
```

```
      Vserver: vs1
      File Path: /datavol5
      File Inode Number: 3374
      Security Style: mixed
      Effective Style: unix
      DOS Attributes: 10
      DOS Attributes in Text: ----D---
      Expanded Dos Attributes: -
      Unix User Id: 0
      Unix Group Id: 0
      Unix Mode Bits: 755
      Unix Mode Bits in Text: rwxr-xr-x
      ACLs: Storage-Level Access Guard security
      SACL (Applies to Directories):
        AUDIT-EXAMPLE\Domain Users-0x120089-FA
        AUDIT-EXAMPLE\engineering-0x1f01ff-SA
        AUDIT-EXAMPLE\market-0x1f01ff-SA
      DACL (Applies to Directories):
        ALLOW-BUILTIN\Administrators-0x1f01ff
        ALLOW-CREATOR OWNER-0x1f01ff
        ALLOW-EXAMPLE\Domain Users-0x120089
        ALLOW-EXAMPLE\engineering-0x1f01ff
        ALLOW-EXAMPLE\market-0x1f01ff
      SACL (Applies to Files):
        AUDIT-EXAMPLE\Domain Users-0x120089-FA
        AUDIT-EXAMPLE\engineering-0x1f01ff-SA
        AUDIT-EXAMPLE\market-0x1f01ff-SA
      DACL (Applies to Files):
        ALLOW-BUILTIN\Administrators-0x1f01ff
        ALLOW-CREATOR OWNER-0x1f01ff
        ALLOW-EXAMPLE\Domain Users-0x120089
        ALLOW-EXAMPLE\engineering-0x1f01ff
        ALLOW-EXAMPLE\market-0x1f01ff
```

## 関連情報

[NTFSセキュリティ形式のボリュームのファイルセキュリティに関する情報の表示](#)

[UNIX セキュリティ形式のボリュームのファイルセキュリティに関する情報を表示する](#)

**UNIX** セキュリティ形式のボリューム上のファイルセキュリティに関する情報を表示します

セキュリティ形式と有効なセキュリティ形式、適用されている権限、UNIX の所有者とグループに関する情報など、UNIX セキュリティ形式のボリューム上にあるファイルや

ディレクトリのセキュリティに関する情報を表示できます。この結果を使用して、セキュリティ設定の検証や、ファイルアクセスに関する問題のトラブルシューティングを行うことができます。

このタスクについて

Storage Virtual Machine（SVM）の名前、およびファイルまたはディレクトリのセキュリティ情報を表示するデータのパスを入力する必要があります。出力は要約形式または詳細なリストで表示できます。

- UNIX セキュリティ形式のボリュームおよび qtree では、ファイルアクセス権の決定時に、UNIX ファイルアクセス権のみが使用されます。モードビットまたは NFSv4 ACL です。
- ACL 出力は、NFSv4 セキュリティが適用されたファイルとフォルダについてのみ表示されます。

このフィールドは、モードビットのアクセス権のみ（NFSv4 ACL はなし）が適用されている UNIX セキュリティ形式のファイルおよびディレクトリでは空になります。

- ACL 出力の所有者とグループの出力フィールドは、NFSv4 セキュリティ記述子には該当しません。

これらのフィールドが意味があるのは、NTFS セキュリティ記述子の場合のみです。

- ストレージレベルのアクセス保護セキュリティは、SVMでCIFSサーバが設定されている場合、UNIXのボリュームまたはqtreeでサポートされるため、で指定したボリュームまたはqtreeに適用されるストレージレベルのアクセス保護セキュリティに関する情報が出力に含まれることがあります -path パラメータ

ステップ

1. ファイルとディレクトリのセキュリティ設定を必要な詳細レベルで表示します。

表示する情報	入力するコマンド
要約形式で表示されます	<code>vserver security file-directory show -vserver vserver_name -path path</code>
詳細が表示されます	<code>vserver security file-directory show -vserver vserver_name -path path -expand-mask true</code>

例

次の例は、パスに関するセキュリティ情報を表示します /home SVM vs1：

```
cluster1::> vserver security file-directory show -vserver vs1 -path /home
```

```

        Vserver: vs1
        File Path: /home
    File Inode Number: 9590
        Security Style: unix
        Effective Style: unix
        DOS Attributes: 10
    DOS Attributes in Text: ----D---
Expanded Dos Attributes: -
        Unix User Id: 0
        Unix Group Id: 1
        Unix Mode Bits: 700
    Unix Mode Bits in Text: rwx-----
        ACLs: -
```

次の例は、パスに関するセキュリティ情報を表示します /home マスクを展開した形式のSVM vs1 :

```
cluster1::> vserver security file-directory show -vserver vs1 -path /home
-expand-mask true
```

```

        Vserver: vs1
        File Path: /home
    File Inode Number: 9590
        Security Style: unix
        Effective Style: unix
        DOS Attributes: 10
    DOS Attributes in Text: ----D---
Expanded Dos Attributes: 0x10
    ...0 .... .... = Offline
    .... ..0. .... = Sparse
    .... .... 0... = Normal
    .... .... ..0. = Archive
    .... .... ...1 .... = Directory
    .... .... .... .0.. = System
    .... .... .... ..0. = Hidden
    .... .... .... ...0 = Read Only
        Unix User Id: 0
        Unix Group Id: 1
        Unix Mode Bits: 700
    Unix Mode Bits in Text: rwx-----
        ACLs: -
```



## NTFSセキュリティ形式のボリュームのファイルセキュリティに関する情報の表示

### mixed セキュリティ形式のボリュームのファイルセキュリティに関する情報を表示する

CLI を使用して、FlexVol の NTFS 監査ポリシーに関する情報を表示する

セキュリティ形式と有効なセキュリティ形式、適用されているアクセス権、システムアクセス制御リストに関する情報など、FlexVol の NTFS 監査ポリシーに関する情報を表示できます。この結果を使用して、セキュリティ設定の検証や、監査に関する問題のトラブルシューティングを行うことができます。

このタスクについて

Storage Virtual Machine (SVM) の名前、および監査情報を表示するファイルまたはフォルダのパスを指定する必要があります。出力は要約形式または詳細なリストで表示できます。

- NTFS セキュリティ形式のボリュームおよび qtree では、NTFS のシステムアクセス制御リスト (SACL) のみが監査ポリシーに使用されます。
- NTFS 対応のセキュリティが有効な mixed セキュリティ形式のボリューム内のファイルおよびフォルダには、NTFS 監査ポリシーを適用できます。

mixed セキュリティ形式のボリュームおよび qtree には、UNIX ファイル権限、モードビットまたは NFSv4 ACL、および NTFS ファイル権限を使用する一部のファイルおよびディレクトリを含めることができます。

- mixed セキュリティ形式のボリュームの最上位では、UNIX または NTFS 対応のセキュリティを有効にすることができ、そこには NTFS SACL が格納されている場合も、格納されていない場合もあります。
- ストレージレベルのアクセス保護セキュリティは、ボリュームのルートまたは qtree の有効なセキュリティ形式が UNIX であっても、mixed セキュリティ形式のボリュームまたは qtree で設定できるため、ストレージレベルのアクセス保護が設定されているボリュームまたは qtree パスの出力には、通常のファイルおよびフォルダの NFSv4 SACL とストレージレベルのアクセス保護の NTFS SACL の両方が表示される場合があります。
- コマンドで入力したパスが、NTFS 対応のセキュリティを使用するデータへのパスである場合、そのファイルまたはディレクトリパスにダイナミックアクセス制御が設定されていれば、ダイナミックアクセス制御 ACE に関する情報も出力に表示されます。
- NTFS 対応のセキュリティが有効なファイルおよびフォルダに関するセキュリティ情報を表示する場合、UNIX 関連の出力フィールドには表示専用の UNIX ファイル権限情報が格納されます。

ファイルアクセス権の決定時、NTFS セキュリティ形式のファイルおよびフォルダでは、NTFS ファイルアクセス権と Windows ユーザおよびグループのみが使用されます。

- ACL 出力は、NTFS または NFSv4 セキュリティが適用されたファイルとフォルダについてのみ表示されます。

このフィールドは、モードビットのアクセス権のみ (NFSv4 ACL はなし) が適用されている UNIX セキュリティ形式のファイルおよびフォルダでは空になります。

- ACL 出力の所有者とグループの出力フィールドは、NTFS セキュリティ記述子の場合にのみ適用されません。

ステップ

1. ファイルおよびディレクトリ監査ポリシー設定を必要な詳細レベルで表示します。

表示する情報	入力するコマンド
要約形式で表示されます	<code>vserver security file-directory show -vserver vserver_name -path path</code>
詳細なリストとして	<code>vserver security file-directory show -vserver vserver_name -path path -expand-mask true</code>

例

次の例は、パスの監査ポリシーの情報を表示します /corp (SVM vs1)。パスで NTFS 対応のセキュリティが有効になっています。NTFS セキュリティ記述子には、SUCCESS および SUCCESS/FAIL SACL エントリの両方が含まれています。

```
cluster::> vserver security file-directory show -vserver vs1 -path /corp
      Vserver: vs1
      File Path: /corp
      File Inode Number: 357
      Security Style: ntfs
      Effective Style: ntfs
      DOS Attributes: 10
      DOS Attributes in Text: ----D---
      Expanded Dos Attributes: -
      Unix User Id: 0
      Unix Group Id: 0
      Unix Mode Bits: 777
      Unix Mode Bits in Text: rwxrwxrwx
      ACLs: NTFS Security Descriptor
      Control:0x8014
      Owner:DOMAIN\Administrator
      Group:BUILTIN\Administrators
      SACL - ACEs
      ALL-DOMAIN\Administrator-0x100081-OI|CI|SA|FA
      SUCCESSFUL-DOMAIN\user1-0x100116-OI|CI|SA
      DACL - ACEs
      ALLOW-BUILTIN\Administrators-0x1f01ff-OI|CI
      ALLOW-BUILTIN\Users-0x1f01ff-OI|CI
      ALLOW-CREATOR OWNER-0x1f01ff-OI|CI
      ALLOW-NT AUTHORITY\SYSTEM-0x1f01ff-OI|CI
```

次の例は、パスの監査ポリシーの情報を表示します /datavol1 (SVM vs1)。このパスには、標準ファイルおよびフォルダの SACL とストレージレベルのアクセス保護の SACL の両方が格納されています。

```

cluster::> vserver security file-directory show -vserver vs1 -path
/datavol1

      Vserver: vs1
      File Path: /datavol1
      File Inode Number: 77
      Security Style: ntfs
      Effective Style: ntfs
      DOS Attributes: 10
      DOS Attributes in Text: ----D---
      Expanded Dos Attributes: -
      Unix User Id: 0
      Unix Group Id: 0
      Unix Mode Bits: 777
      Unix Mode Bits in Text: rwxrwxrwx
      ACLs: NTFS Security Descriptor
            Control:0xaa14
            Owner: BUILTIN\Administrators
            Group: BUILTIN\Administrators
            SACL - ACEs
              AUDIT-EXAMPLE\marketing-0xf01ff-OI|CI|FA
            DACL - ACEs
              ALLOW-EXAMPLE\Domain Admins-0x1f01ff-OI|CI
              ALLOW-EXAMPLE\marketing-0x1200a9-OI|CI

      Storage-Level Access Guard security
      SACL (Applies to Directories):
        AUDIT-EXAMPLE\Domain Users-0x120089-FA
        AUDIT-EXAMPLE\engineering-0x1f01ff-SA
      DACL (Applies to Directories):
        ALLOW-EXAMPLE\Domain Users-0x120089
        ALLOW-EXAMPLE\engineering-0x1f01ff
        ALLOW-NT AUTHORITY\SYSTEM-0x1f01ff
      SACL (Applies to Files):
        AUDIT-EXAMPLE\Domain Users-0x120089-FA
        AUDIT-EXAMPLE\engineering-0x1f01ff-SA
      DACL (Applies to Files):
        ALLOW-EXAMPLE\Domain Users-0x120089
        ALLOW-EXAMPLE\engineering-0x1f01ff
        ALLOW-NT AUTHORITY\SYSTEM-0x1f01ff

```

CLI を使用して、FlexVol の NFSv4 監査ポリシーに関する情報を表示する

セキュリティ形式と有効なセキュリティ形式、適用されている権限、システムアクセス制御リスト（SACL）に関する情報など、ONTAP CLI を使用して FlexVol の NFSv4 監

査ポリシーに関する情報を表示できます。この結果を使用して、セキュリティ設定の検証や、監査に関する問題のトラブルシューティングを行うことができます。

このタスクについて

Storage Virtual Machine（SVM）の名前、および監査情報を表示するファイルまたはディレクトリのパスを入力する必要があります。出力は要約形式または詳細なリストで表示できます。

- UNIX セキュリティ形式のボリュームおよび qtree では、監査ポリシーに NFSv4 SACL のみが使用されます。
- mixed セキュリティ形式のボリュームにある UNIX セキュリティ形式のファイルとディレクトリには、NFSv4 監査ポリシーを適用できます。

mixed セキュリティ形式のボリュームおよび qtree には、UNIX ファイル権限、モードビットまたは NFSv4 ACL、および NTFS ファイル権限を使用する一部のファイルおよびディレクトリを含めることができます。

- mixed セキュリティ形式のボリュームの最上位では、UNIX または NTFS 対応のセキュリティを有効にすることができ、NFSv4 SACL が含まれる場合と含まれない場合があります。
- ACL 出力は、NTFS または NFSv4 セキュリティが適用されたファイルとフォルダについてのみ表示されます。

このフィールドは、モードビットのアクセス権のみ（NFSv4 ACL はなし）が適用されている UNIX セキュリティ形式のファイルおよびフォルダでは空になります。

- ACL 出力の所有者とグループの出力フィールドは、NTFS セキュリティ記述子の場合にのみ適用されます。
- ストレージレベルのアクセス保護セキュリティは、ボリュームのルートまたは qtree の有効なセキュリティ形式が UNIX であっても、mixed セキュリティ形式のボリュームまたは qtree で設定できるため、ストレージレベルのアクセス保護が設定されているボリュームまたは qtree パスの出力には、標準の NFSv4 ファイルおよびディレクトリの SACL とストレージレベルのアクセス保護の NTFS SACL の両方が表示される場合があります。
- ストレージレベルのアクセス保護セキュリティは、SVMでCIFSサーバが設定されている場合、UNIXのボリュームまたはqtreeでサポートされるため、で指定したボリュームまたはqtreeに適用されるストレージレベルのアクセス保護セキュリティに関する情報が出力に含まれることがあります -path パラメータ

手順

1. ファイルとディレクトリのセキュリティ設定を必要な詳細レベルで表示します。

表示する情報	入力するコマンド
要約形式で表示されます	<code>vserver security file-directory show -vserver vserver_name -path path</code>
詳細が表示されます	<code>vserver security file-directory show -vserver vserver_name -path path -expand-mask true</code>

例

次の例は、パスに関するセキュリティ情報を表示します /lab (SVM vs1)。この UNIX セキュリティ形式のパスには NFSv4 SACL が設定されています。

```
cluster::> vserver security file-directory show -vserver vs1 -path /lab

      Vserver: vs1
      File Path: /lab
      File Inode Number: 288
      Security Style: unix
      Effective Style: unix
      DOS Attributes: 11
      DOS Attributes in Text: ----D--R
      Expanded Dos Attributes: -
      Unix User Id: 0
      Unix Group Id: 0
      Unix Mode Bits: 0
      Unix Mode Bits in Text: -----
      ACLs: NFSV4 Security Descriptor
            Control:0x8014
            SACL - ACEs
                  SUCCESSFUL-S-1-520-0-0xf01ff-SA
                  FAILED-S-1-520-0-0xf01ff-FA
            DACL - ACEs
                  ALLOW-S-1-520-1-0xf01ff
```

ファイルセキュリティと監査ポリシーに関する情報を表示する方法

ワイルドカード文字（\*）を使用すると、特定のパスまたはルートボリリュームの下にあるすべてのファイルおよびディレクトリのファイルセキュリティと監査ポリシーに関する情報を表示できます。

ワイルドカード文字（\*）は、すべてのファイルおよびディレクトリの情報を表示する特定のディレクトリパスの最後のサブコンポーネントとして使用できます。「\*」という名前の特定のファイルまたはディレクトリの情報を表示する場合は、二重引用符（「`」）で完全なパスを指定する必要があります。

例

次のコマンドにワイルドカード文字を指定すると、パスの下にあるすべてのファイルとディレクトリに関する情報が表示されます /1/ SVM vs1：

```

cluster::> vserver security file-directory show -vserver vs1 -path /1/*

      Vserver: vs1
      File Path: /1/1
      Security Style: mixed
      Effective Style: ntfs
      DOS Attributes: 10
      DOS Attributes in Text: ----D---
      Expanded Dos Attributes: -
      Unix User Id: 0
      Unix Group Id: 0
      Unix Mode Bits: 777
      Unix Mode Bits in Text: rwxrwxrwx
      ACLs: NTFS Security Descriptor
            Control:0x8514
            Owner:BUILTIN\Administrators
            Group:BUILTIN\Administrators
            DACL - ACEs
            ALLOW-Everyone-0x1f01ff-OI|CI (Inherited)

      Vserver: vs1
      File Path: /1/1/abc
      Security Style: mixed
      Effective Style: ntfs
      DOS Attributes: 10
      DOS Attributes in Text: ----D---
      Expanded Dos Attributes: -
      Unix User Id: 0
      Unix Group Id: 0
      Unix Mode Bits: 777
      Unix Mode Bits in Text: rwxrwxrwx
      ACLs: NTFS Security Descriptor
            Control:0x8404
            Owner:BUILTIN\Administrators
            Group:BUILTIN\Administrators
            DACL - ACEs
            ALLOW-Everyone-0x1f01ff-OI|CI (Inherited)

```

次のコマンドは、パスの下に「\*」という名前のファイルの情報を表示します /vol1/a SVM vs1の。パスは二重引用符 ("" ) で囲まれます。

```
cluster::> vservers security file-directory show -vservers vs1 -path  
"/vol1/a/*"
```

```
      Vserver: vs1  
      File Path: "/vol1/a/*"  
      Security Style: mixed  
      Effective Style: unix  
      DOS Attributes: 10  
      DOS Attributes in Text: ----D---  
      Expanded Dos Attributes: -  
          Unix User Id: 1002  
          Unix Group Id: 65533  
          Unix Mode Bits: 755  
      Unix Mode Bits in Text: rwxr-xr-x  
          ACLs: NFSV4 Security Descriptor  
              Control:0x8014  
              SACL - ACEs  
                  AUDIT-EVERYONE@-0x1f01bf-FI|DI|SA|FA  
              DACL - ACEs  
                  ALLOW-EVERYONE@-0x1f00a9-FI|DI  
                  ALLOW-OWNER@-0x1f01ff-FI|DI  
                  ALLOW-GROUP@-0x1200a9-IG
```

**CLI** を使用して、**SVM** の **NTFS** ファイルセキュリティ、**NTFS** 監査ポリシー、ストレージレベルのアクセス保護を管理します

**CLI** の概要を使用して、**SVM** の **NTFS** ファイルセキュリティ、**NTFS** 監査ポリシー、ストレージレベルのアクセス保護を管理します

**CLI** を使用して、Storage Virtual Machine（SVM）の **NTFS** ファイルセキュリティ、**NTFS** 監査ポリシー、ストレージレベルのアクセス保護を管理できます。

**NTFS** ファイルセキュリティと監査ポリシーは、SMB クライアントから、または **CLI** を使用して管理できます。ただし、**CLI** を使用してファイルセキュリティと監査ポリシーを設定する場合、リモートクライアントを使用せずにファイルセキュリティを管理できます。**CLI** を使用すると、多数のファイルやフォルダに対してセキュリティを適用する場合でも 1 つのコマンドで実行できるため、所要時間を大幅に短縮できます。

**ONTAP** から **SVM** ボリュームに適用されるもう 1 つのセキュリティレイヤであるストレージレベルのアクセス保護を設定できます。ストレージレベルのアクセス保護環境は、すべての **NAS** プロトコルからストレージレベルのアクセス保護が適用されているストレージオブジェクトへのアクセスを保護します。

ストレージレベルのアクセス保護は **ONTAP CLI** からのみ設定および管理できます。ストレージレベルのアクセス保護設定を **SMB** クライアントから管理することはできません。また、**NFS** または **SMB** クライアントからファイルまたはディレクトリのセキュリティ設定を表示した場合、ストレージレベルのアクセス保護のセキュリティは表示されません。システム（**Windows** または **UNIX**）管理者であっても、ストレージレベルのアクセス保護セキュリティをクライアントから取り消すことはできません。そのため、ストレージレベルのアクセス保護は、ストレージ管理者が独立して設定および管理できるセキュリティレイヤをデータアクセスに追加で提供します。



ストレージレベルのアクセス保護では NTFS のアクセス権のみがサポートされます。ただし、ストレージレベルのアクセス保護が適用されているボリューム上のデータへの NFS 経由のアクセスに対しても、そのボリュームを所有する SVM 上の Windows ユーザに UNIX ユーザがマッピングされている場合は、ONTAP でセキュリティチェックを実行できます。

## NTFS セキュリティ形式のボリューム

NTFS セキュリティ形式のボリュームや qtree に格納されているファイルやフォルダはすべて、NTFS 対応のセキュリティが有効になります。を使用できます `vserver security file-directory` NTFSセキュリティ形式のボリュームに次の種類のセキュリティを実装するためのコマンドファミリー。

- ボリュームに格納されているファイルとフォルダに対するファイル権限と監査ポリシー
- ボリュームに対するストレージレベルのアクセス保護セキュリティ

## mixed セキュリティ形式のボリューム

mixed セキュリティ形式のボリュームおよび qtree には、UNIX 対応のセキュリティを備え、UNIX ファイルアクセス権を使用する一部のファイルおよびフォルダ、モードビットまたは NFSv4.x ACL と NFSv4.x 監査ポリシー、および NTFS 対応のセキュリティを有効にして NTFS ファイルアクセス権と監査ポリシーを使用する一部のファイルおよびフォルダを含めることができます。を使用できます `vserver security file-directory` mixedセキュリティ形式のデータに次の種類のセキュリティを適用するコマンドファミリー。

- mixed 形式のボリュームや qtree での NTFS 対応のセキュリティ形式のファイルおよびフォルダに対するファイル権限と監査ポリシー
- ストレージレベルのアクセス保護：NTFS 対応または UNIX 対応のセキュリティ形式のボリューム

## UNIXセキュリティ形式のボリューム

UNIX セキュリティ形式のボリュームと qtree には、UNIX 対応のセキュリティ（モードビットまたは NFSv4.x ACL）を備えたファイルとフォルダが含まれます。を使用する場合は、次の点に注意する必要があります `vserver security file-directory` UNIXセキュリティ形式のボリュームにセキュリティを実装するコマンドファミリー：

- `vserver security file-directory` UNIXセキュリティ形式のボリュームおよび qtree では、コマンドファミリーを使用して UNIX ファイルセキュリティおよび監査ポリシーを管理することはできません。
- を使用できます `vserver security file-directory` UNIXセキュリティ形式のボリュームを含む SVM に CIFS サーバが含まれている場合に、そのボリュームにストレージレベルのアクセス保護を設定するコマンドファミリー。

## 関連情報

[ファイルセキュリティと監査ポリシーに関する情報を表示します](#)

[CLI を使用して、NTFS ファイルおよびフォルダに対してファイルセキュリティを設定および適用します](#)

[CLI を使用して、NTFS ファイルおよびフォルダに対して監査ポリシーを設定および適用する](#)

[ストレージレベルのアクセス保護を使用してファイルアクセスを保護](#)



CLI を使用してファイルおよびフォルダのセキュリティを設定するユースケース

ファイルおよびフォルダのセキュリティは、リモートクライアントを使用せずにローカルで適用および管理できるため、多数のファイルまたはフォルダに対して一括でセキュリティを設定する場合に比べて大幅に時間を短縮できます。

CLI を使用してファイルおよびフォルダのセキュリティを設定すると効果的な状況として、次のようなユースケースがあります。

- ホームディレクトリ内のファイルストレージなど、大規模なエンタープライズ環境のファイルの格納
- データの移行
- Windows ドメインの変更
- NTFS ファイルシステムのファイルセキュリティと監査ポリシーの標準化

CLI を使用してファイルおよびフォルダのセキュリティを設定する場合の制限事項

ファイルおよびフォルダのセキュリティ設定で CLI を使用する際には、一定の制限事項を知っておく必要があります。

- `vserver security file-directory` コマンドファミリーは NFSv4 ACL の設定をサポートしていません。

NTFS のセキュリティ記述子は NTFS ファイルと NTFS フォルダにのみ適用できます。

セキュリティ記述子を使用したファイルおよびフォルダのセキュリティの適用方法

セキュリティ記述子には、ユーザがファイルやフォルダに対して実行できる操作、およびユーザがファイルやフォルダにアクセスするときに監査される内容を決定するアクセス制御リストが含まれます。

#### • \* 権限 \*

権限は、オブジェクトの所有者によって許可または拒否され、指定されたファイルまたはフォルダに対してオブジェクト（ユーザ、グループ、またはコンピュータオブジェクト）が実行できる操作を決定します。

#### • \* セキュリティ記述子 \*

セキュリティ記述子は、ファイルまたはフォルダに関連付けられた権限を定義するセキュリティ情報を含むデータ構造です。

#### • \* アクセス制御リスト (ACL) \*

アクセス制御リストは、セキュリティ記述子内に含まれるリストです。セキュリティ記述子が適用されるファイルまたはフォルダに対してユーザ、グループ、またはコンピュータオブジェクトが実行できる操作に関する情報が含まれます。セキュリティ記述子には、次の 2 種類の ACL を含めることができます。

- Discretionary Access Control List （ DACL ； 随意アクセス制御リスト）
- システムアクセスセイギョリスト SACL

- \* 随意アクセス制御リスト (DACL) \*

DACL には、ファイルまたはフォルダに対して操作を実行するためのアクセスを許可または拒否するユーザ、グループ、およびコンピュータオブジェクトの SID リストが含まれます。DACL には、0 個以上の Access Control Entry (ACE ; アクセス制御エントリ) が含まれます。

- \* システム・アクセス・コントロール・リスト (SACL) \*

SACL には、成功または失敗した監査イベントがログに記録されるユーザ、グループ、およびコンピュータオブジェクトの SID リストが含まれます。SACL には、0 個以上の Access Control Entry (ACE ; アクセス制御エントリ) が含まれます。

- \* アクセス制御エントリ (ACE) \*

ACE は、DACL または SACL 内の個々のエントリです。

- DACL アクセス制御エントリは、特定のユーザ、グループ、またはコンピュータオブジェクトに対して許可または拒否されるアクセス権を指定します。
- SACL アクセス制御エントリは、特定のユーザ、グループ、またはコンピュータオブジェクトによって実行される指定された操作の監査時にログに記録される成功または失敗イベントを指定します。

- \* 権限の継承 \*

権限の継承は、セキュリティ記述子で定義された権限が親オブジェクトからオブジェクトにどのように伝播されるかを示します。子オブジェクトには継承可能な権限のみが継承されます。親オブジェクトのアクセス権を設定する際に、フォルダ、サブフォルダ、およびファイルがそのアクセス権を継承できるかどうかを「適用先」で決定することができます this-folder、sub-folders、および files`」を指定します。

## 関連情報

["SMB および NFS の監査とセキュリティトレース"](#)

[CLI を使用した NTFS ファイルおよびフォルダに対する監査ポリシーの設定および適用](#)

**SVM** ディザスタリカバリデスティネーションでローカルユーザまたはグループを使用するファイルとディレクトリのポリシーを適用する際のガイドライン

ファイルとディレクトリのポリシー設定がセキュリティ記述子、DACL、SACL エントリのいずれかでローカルユーザまたはグループを使用する場合、ID 破棄設定の Storage Virtual Machine (SVM) ディザスタリカバリデスティネーションでファイルとディレクトリのポリシーを適用する前に注意すべきいくつかのガイドラインがあります。

ソースクラスタのソース SVM が、ソース SVM からデスティネーションクラスタのデスティネーション SVM にデータと設定をレプリケートする SVM ディザスタリカバリ構成を設定できます。

SVM ディザスタリカバリの 2 つのタイプのうち 1 つを設定できます。

- ID が保持されます

この設定では、SVM と CIFS サーバの ID が維持されます。

- ID が破棄されました

この設定では、SVM と CIFS サーバの ID が維持されません。このシナリオでは、デスティネーション SVM の SVM と CIFS サーバの名前は、ソース SVM の SVM と CIFS サーバの名前と異なります。

## ID 破棄設定に関するガイドライン

ID 破棄設定では、ローカルユーザ、グループ、権限設定を含む SVM ソースを SVM デスティネーションの CIFS サーバ名に一致するようにローカルドメインの名前（ローカル CIFS サーバ名）を変更する必要があります。たとえば、ソース SVM 名が「vs1」で CIFS サーバ名が「CIFS1」、デスティネーション SVM 名が「vs1\_dst」で CIFS サーバ名が「CIFS1\_DST」の場合、ローカルユーザ「CIFS1\user1」のローカルドメイン名は「CIFS1\_DST デスティネーション SVM」で自動的に「CIFS1\_DST\user1」に変更されます。

```
cluster1::> vsriver cifs users-and-groups local-user show -vsriver vs1_dst
```

Vsriver	User Name	Full Name	Description
vs1	CIFS1\Administrator		Built-in
administrator account			
vs1	CIFS1\user1	-	-

```
cluster1dst::> vsriver cifs users-and-groups local-user show -vsriver vs1_dst
```

Vsriver	User Name	Full Name	Description
vs1_dst	CIFS1_DST\Administrator		Built-in
administrator account			
vs1_dst	CIFS1_DST\user1	-	-

ローカルユーザおよびグループデータベースでローカルユーザおよびグループ名が自動的に変更されても、ファイルとディレクトリのポリシー設定（を使用してCLIで設定するポリシー）のローカルユーザまたはグループ名は自動的に変更されません vsriver security file-directory コマンドファミリー）。

たとえば、「vs1」の場合、が配置されているDACLエントリを設定しているとします -account パラメータが「CIFS1\user1」に設定されている場合、デスティネーションSVMでデスティネーションのCIFSサーバ名が反映されて設定が自動的に変更されることはありません。

```
cluster1::> vserver security file-directory ntfs dacl show -vserver vs1
```

Vserver: vs1

NTFS Security Descriptor Name: sd1

Account Name	Access Type	Access Rights	Apply To
-----	-----	-----	-----
CIFS1\user1	allow	full-control	this-folder

```
cluster1::> vserver security file-directory ntfs dacl show -vserver vs1_dst
```

Vserver: vs1\_dst

NTFS Security Descriptor Name: sd1

Account Name	Access Type	Access Rights	Apply To
-----	-----	-----	-----
**CIFS1**\user1	allow	full-control	this-folder

を使用する必要があります vserver security file-directory modify CIFSサーバ名を手動でデスティネーションCIFSサーバ名に変更するコマンド

アカウントパラメータを含むファイルとディレクトリのポリシー設定コンポーネント

ローカルユーザまたはグループを含むパラメータ設定を使用できるファイルとディレクトリのポリシー設定コンポーネントは3つあります。

- セキュリティ記述子

必要に応じて、セキュリティ記述子の所有者とセキュリティ記述子の所有者のプライマリグループを指定できます。セキュリティ記述子で所有者とプライマリグループのエントリにローカルユーザまたはグループを使用する場合、デスティネーション SVM にアカウント名を使用するようにセキュリティ記述子を変更する必要があります。を使用できます vserver security file-directory ntfs modify コマンドを使用してアカウント名に必要な変更を行います。

- DACL エントリ

各 DACL エントリは、アカウントと関連付ける必要があります。ローカルユーザまたはグループアカウントを使用する DACL は、すべてデスティネーション SVM 名を使用するように変更する必要があります。既存の DACL エントリのアカウント名は変更できないため、ローカルユーザまたはグループが設定されたすべての DACL エントリをセキュリティ記述子から削除し、訂正したデスティネーションアカウント名を設定した新しい DACL エントリを作成し、その新しい DACL エントリを適切なセキュリティ記述子と関連付ける必要があります。

- SACL エントリ

各 SACL エントリは、アカウントに関連付ける必要があります。ローカルユーザまたはグループアカウント

トを使用する SACL は、すべてデスティネーション SVM 名を使用するように変更する必要があります。既存の SACL エントリのアカウント名は変更できないため、ローカルユーザまたはグループが設定されたすべての SACL エントリをセキュリティ記述子から削除し、修正したデスティネーションアカウント名を使用して新しい SACL エントリを作成し、それらの新しい SACL エントリを適切なセキュリティ記述子と関連付ける必要があります。

ポリシーを適用する前に、ファイルとディレクトリのポリシー設定で使用されているローカルユーザまたはグループに必要な変更を行う必要があります。そうしないと、適用ジョブは失敗します。

CLI を使用して、NTFS ファイルおよびフォルダに対してファイルセキュリティを設定および適用します

## NTFS セキュリティ記述子を作成します

NTFS セキュリティ記述子（ファイルセキュリティポリシー）の作成は、Storage Virtual Machine （SVM）内のファイルやフォルダの NTFS Access Control List （ACL；アクセス制御リスト）を設定および適用するための最初のステップです。セキュリティ記述子をポリシータスクでファイルパスまたはフォルダパスに関連付けることができます。

このタスクについて

NTFS セキュリティ形式のボリューム内に存在するファイルやフォルダ、または mixed セキュリティ形式のボリューム上に存在するファイルやフォルダに対して、NTFS セキュリティ記述子を作成できます。

デフォルトでは、セキュリティ記述子を作成すると、Discretionary Access Control List （DACL；随意アクセス制御リスト）の 4 つの Access Control Entry （ACE；アクセス制御エントリ）がそのセキュリティ記述子に追加されます。4 つのデフォルトの ACE は次のとおりです。

オブジェクト	アクセスタイプ	アクセス権	権限の適用先
組み込み管理者	許可（Allow）	フルコントロール	このフォルダ、サブフォルダ、ファイル
組み込みユーザ	許可（Allow）	フルコントロール	このフォルダ、サブフォルダ、ファイル
作成者の所有者	許可（Allow）	フルコントロール	このフォルダ、サブフォルダ、ファイル
NT AUTHORITY\SYSTEM	許可（Allow）	フルコントロール	このフォルダ、サブフォルダ、ファイル

次のオプションのパラメータを使用して、セキュリティ記述子の設定をカスタマイズできます。

- セキュリティ記述子の所有者
- 所有者のプライマリグループ
- raw 制御フラグ

オプションのパラメータの値はストレージレベルのアクセス保護では無視されます。詳細については、マニユ

アルページを参照してください。

## NTFSセキュリティ記述子へのNTFS DACLアクセス制御エントリの追加

NTFS セキュリティ記述子への随意アクセス制御リスト（DACL）のアクセス制御エントリ（ACE）の追加は、ファイルまたはフォルダに対する NTFS ACL の設定および適用における 2 番目の手順です。各エントリによって、アクセスが許可または拒否されるオブジェクトが識別され、ACE で定義されているファイルまたはフォルダに対してオブジェクトが実行できる操作または実行できない操作が定義されます。

このタスクについて

セキュリティ記述子のDACLには1つ以上のACEを追加できます。

セキュリティ記述子に含まれるDACLに既存のACEがある場合は、新しいACEがDACLに追加されます。セキュリティ記述子に DACL が含まれていない場合は、DACL が作成され、その DACL に新しい ACE が追加されます。

必要に応じて、で指定したアカウントに対して許可または拒否する権限を指定することで、DACLエントリをカスタマイズできます -account パラメータ権限を指定する場合、次の 3 つの相互に排他的な方法があります。

- 権利
- 詳細な権限
- raw 権限（advanced 権限）



DACLエントリの権限を指定しない場合、権限はデフォルトでに設定されます Full Control。

必要に応じて、継承の適用方法を指定することで、DACL エントリをカスタマイズできます。

オプションのパラメータの値はストレージレベルのアクセス保護では無視されます。詳細については、マニュアルページを参照してください。

### 手順

1. セキュリティ記述子にDACLエントリを追加します。 `vserver security file-directory ntfs dacl add -vserver vserver_name -ntfs-sd SD_name -access-type {allow|deny} -account name_or_SIDoptional_parameters`

```
vserver security file-directory ntfs dacl add -ntfs-sd sd1 -access-type deny
-account domain\joe -rights full-control -apply-to this-folder -vserver vs1
```

2. DACLエントリが正しいことを確認します。 `vserver security file-directory ntfs dacl show -vserver vserver_name -ntfs-sd SD_name -access-type {allow|deny} -account name_or_SID`

```
vserver security file-directory ntfs dacl show -vserver vs1 -ntfs-sd sd1
-access-type deny -account domain\joe
```

```

Vserver: vs1
Security Descriptor Name: sd1
  Allow or Deny: deny
    Account Name or SID: DOMAIN\joe
      Access Rights: full-control
Advanced Access Rights: -
  Apply To: this-folder
    Access Rights: full-control

```

## セキュリティポリシーを作成する

SVM のファイルセキュリティポリシーの作成は、ファイルまたはフォルダに対して ACL を設定および適用する 3 番目のステップです。ポリシーは、さまざまなタスクのコンテナとして機能します。各タスクは、ファイルまたはフォルダに適用できる単一のエントリです。あとで、このセキュリティポリシーにタスクを追加できます。

### このタスクについて

セキュリティポリシーに追加するタスクには、NTFS セキュリティ記述子とファイルパスまたはフォルダパスとの間の関連付けが含まれます。そのため、セキュリティポリシーは、NTFS セキュリティ形式または mixed セキュリティ形式のボリュームを含む SVM にそれぞれ関連付ける必要があります。

### 手順

1. セキュリティポリシーを作成します。 `vserver security file-directory policy create -vserver vserver_name -policy-name policy_name`

```
vserver security file-directory policy create -policy-name policy1 -vserver vs1
```

2. セキュリティポリシーを確認します。 `vserver security file-directory policy show`

```

vserver security file-directory policy show
      Vserver      Policy Name
-----
      vs1          policy1

```

## セキュリティポリシーにタスクを追加します

ACL を設定し、SVM 内のファイルやフォルダへ適用する 4 番目のステップでは、ポリシータスクを作成してセキュリティポリシーに追加します。ポリシータスクを作成するときに、セキュリティポリシーとタスクを関連付けます。セキュリティポリシーには、1 つ以上のタスクエントリを追加できます。

### このタスクについて

セキュリティポリシーはタスクのコンテナです。タスクとは、NTFS または mixed セキュリティが設定され

たファイルまたはフォルダ（ストレージレベルのアクセス保護を設定する場合はボリュームオブジェクト）へのセキュリティポリシーによって実行できる単一の処理を指します。

タスクには次の 2 つのタイプがあります。

- ファイルとディレクトリのタスク

指定されたファイルやフォルダにセキュリティ記述子を適用するタスクの指定に使用します。ファイルとディレクトリのタスクによって適用される ACL は、SMB クライアントまたは ONTAP CLI で管理できます。

- ストレージレベルのアクセス保護タスク

指定されたボリュームにストレージレベルのアクセス保護のセキュリティ記述子を適用するタスクの指定に使用します。ストレージレベルのアクセス保護タスクで適用される ACL は ONTAP CLI からのみ管理できます。

タスクには、ファイル（またはフォルダ）やファイルセット（またはフォルダセット）のセキュリティ構成の定義が含まれています。ポリシー内のすべてのタスクは、一意のパスによって識別されます。1 つのポリシー内の 1 つのパスに含められるのは 1 つのタスクだけです。ポリシーに重複するタスクエントリを含めることはできません。

ポリシーへのタスクの追加に関するガイドラインを次に示します。

- ポリシーあたりのタスクエントリは最大 10、000 個です。
- ポリシーには 1 つ以上のタスクを含めることができます。

ポリシーには複数のタスクを含めることができますが、ポリシーにファイルとディレクトリのタスクとストレージレベルのアクセス保護タスクの両方を含めることはできません。ポリシーに含めるタスクは、すべてストレージレベルのアクセス保護タスクにするか、すべてファイルとディレクトリのタスクにする必要があります。

- ストレージレベルのアクセス保護は、権限の制限に使用します。

アクセス権限は付与されません。

セキュリティポリシーにタスクを追加する際には、次の 4 つの必須パラメータを指定する必要があります。

- SVM 名
- ポリシー名
- パス
- パスに関連付けるセキュリティ記述子

次のオプションのパラメータを使用して、セキュリティ記述子の設定をカスタマイズできます。

- セキュリティタイプ
- プロパゲーションモード
- インデックス位置
- アクセス制御の種類



オプションのパラメータの値はストレージレベルのアクセス保護では無視されます。詳細については、マニュアルページを参照してください。

## 手順

1. セキュリティ記述子が関連付けられているタスクをセキュリティポリシーに追加します。 `vserver security file-directory policy task add -vserver vserver_name -policy-name policy_name -path path -ntfs-sd SD_nameoptional_parameters`

`file-directory` は、のデフォルト値です `-access-control` パラメータファイルとディレクトリのアクセスタスクを設定する場合、アクセス制御の種類の指定は任意です。

```
vserver security file-directory policy task add -vserver vs1 -policy-name policy1 -path /home/dir1 -security-type ntfs -ntfs-mode propagate -ntfs-sd sd2 -index-num 1 -access-control file-directory
```

2. ポリシータスクの設定を確認します。 `vserver security file-directory policy task show -vserver vserver_name -policy-name policy_name -path path`

```
vserver security file-directory policy task show
```

Vserver: vs1

Policy: policy1

Index	File/Folder	Access	Security	NTFS	NTFS
Security	Path	Control	Type	Mode	
Descriptor	Name				
-----	-----	-----	-----	-----	
-----					
1	/home/dir1	file-directory	ntfs	propagate	sd2

## セキュリティポリシーを適用する

SVM へのファイルセキュリティポリシーの適用は、ファイルまたはフォルダに対して NTFS ACL を作成および適用する最後のステップです。

### このタスクについて

セキュリティポリシーに定義されているセキュリティ設定を、FlexVol ボリューム（NTFS または mixed セキュリティ形式）内の NTFS ファイルおよびフォルダに適用できます。



監査ポリシーと関連する SACL を適用すると、既存の DACL は上書きされます。セキュリティポリシーとそれに関連付けられた DACL が適用されると、既存の DACL はすべて上書きされます。新しいセキュリティポリシーを作成して適用する前に、既存のセキュリティポリシーを確認してください。

## ステップ

1. セキュリティポリシーを適用します。 `vserver security file-directory apply -vserver`

```
vserver_name -policy-name policy_name
```

```
vserver security file-directory apply -vserver vs1 -policy-name policy1
```

ポリシーを適用するジョブがスケジュールされ、ジョブ ID が返されます。

```
[Job 53322]Job is queued: Fsecurity Apply. Use the "Job show 53322 -id 53322" command to view the status of the operation
```

セキュリティポリシージョブを監視します

Storage Virtual Machine（SVM）にセキュリティポリシーを適用する場合、セキュリティポリシージョブを監視してその進行状況を監視できます。これは、セキュリティポリシーの適用が成功したかどうかを確認するのに役立ちます。また、多数のファイルやフォルダに一括してセキュリティ設定を適用するような長時間のジョブを実行する場合にも、この方法が便利です。

このタスクについて

セキュリティポリシージョブに関する詳細情報を表示するには、を使用します -instance パラメータ

ステップ

1. セキュリティポリシージョブを監視します。 `vserver security file-directory job show -vserver vserver_name`

```
vserver security file-directory job show -vserver vs1
```

Job ID	Name	Vserver	Node	State
53322	Fsecurity Apply	vs1	node1	Success
Description: File Directory Security Apply Job				

適用したファイルセキュリティを確認します

Storage Virtual Machine（SVM）のファイルやフォルダにセキュリティポリシーを適用した場合に、それらの設定が意図したとおりになっているかを確認するには、ファイルのセキュリティ設定を確認します。

このタスクについて

データが格納されている SVM の名前、およびセキュリティ設定を確認するファイルとフォルダのパスを指定する必要があります。オプションのを使用できます -expand-mask セキュリティ設定に関する詳細情報を表示するためのパラメータ。

ステップ

1. ファイルとフォルダのセキュリティ設定を表示します。 `vserver security file-directory show`

```
-vserver vserver_name -path path [-expand-mask true]
```

```
vserver security file-directory show -vserver vs1 -path /data/engineering  
-expand-mask true
```

```
Vserver: vs1  
    File Path: /data/engineering  
File Inode Number: 5544  
    Security Style: ntfs  
    Effective Style: ntfs  
    DOS Attributes: 10  
DOS Attributes in Text: ----D---  
Expanded Dos Attributes: 0x10  
    ...0 .... = Offline  
    .... ..0. .... = Sparse  
    .... .... 0... .... = Normal  
    .... .... ..0. .... = Archive  
    .... .... ...1 .... = Directory  
    .... .... .... .0.. = System  
    .... .... .... ..0. = Hidden  
    .... .... .... ...0 = Read Only  
    Unix User Id: 0  
    Unix Group Id: 0  
    Unix Mode Bits: 777  
Unix Mode Bits in Text: rwxrwxrwx  
    ACLs: NTFS Security Descriptor  
    Control:0x8004  
  
    1... .... = Self Relative  
    .0.. .... = RM Control Valid  
    ..0. .... = SACL Protected  
    ...0 .... = DACL Protected  
    .... 0... .... = SACL Inherited  
    .... .0.. .... = DACL Inherited  
    .... ..0. .... = SACL Inherit Required  
    .... ...0 .... = DACL Inherit Required  
    .... .... ..0. .... = SACL Defaulted  
    .... .... ...0 .... = SACL Present  
    .... .... .... 0... = DACL Defaulted  
    .... .... .... .1.. = DACL Present  
    .... .... .... ..0. = Group Defaulted  
    .... .... .... ...0 = Owner Defaulted  
  
Owner: BUILTIN\Administrators  
Group: BUILTIN\Administrators  
DACL - ACEs
```

	ALLOW-Everyone-0x1f01ff	
	0... .. =	
Generic Read		
	.0... .. =	
Generic Write		
	..0. .... =	
Generic Execute		
	...0 .... =	
Generic All		
	.... ..0 .... =	
System Security		
	.... ....1 .... =	
Synchronize		
	.... ....1... .. =	
Write Owner		
	.... ....1... .. =	
Write DAC		
	.... ....1. .... =	
Read Control		
	.... ....1 .... =	
Delete		
	.... ....1 .... =	
Write Attributes		
	.... ....1... .. =	
Read Attributes		
	.... ....1... .. =	
Delete Child		
	.... ....1... .. =	
Execute		
	.... ....1 .... =	
Write EA		
	.... ....1... .. =	
Read EA		
	.... ....1... .. =	
Append		
	.... ....1. .... =	
Write		
	.... ....1 =	
Read		
	ALLOW-Everyone-0x10000000-OI CI IO	
	0... .. =	
Generic Read		
	.0... .. =	
Generic Write		
	..0. .... =	

[illegible]

**CLI** の概要を使用して、**NTFS** ファイルおよびフォルダに対して監査ポリシーを設定および適用する

ONTAP CLI を使用して NTFS ファイルおよびフォルダに監査ポリシーを適用するには、いくつかの手順を実行する必要があります。まず、NTFS セキュリティ記述子を作成し、SACL をセキュリティ記述子に追加します。次に、セキュリティポリシーを作成してポリシータスクを追加します。その後、Storage Virtual Machine (SVM) にセキュリティポリシーを適用します。

このタスクについて

セキュリティポリシーを適用したら、セキュリティポリシージョブを監視して、適用した監査ポリシーの設定を確認することができます。



監査ポリシーと関連する SACL を適用すると、既存の DACL は上書きされます。新しいセキュリティポリシーを作成して適用する前に、既存のセキュリティポリシーを確認してください。

## 関連情報

[ストレージレベルのアクセス保護を使用したファイルアクセスの保護](#)

[CLI を使用してファイルおよびフォルダのセキュリティを設定する場合の制限事項](#)

[セキュリティ記述子を使用したファイルおよびフォルダのセキュリティの適用方法](#)

["SMB および NFS の監査とセキュリティトレース"](#)

[CLI を使用して、NTFS ファイルおよびフォルダに対してファイルセキュリティを設定および適用します](#)

## NTFS セキュリティ記述子を作成します

NTFS セキュリティ記述子監査ポリシーの作成は、SVM 内のファイルやフォルダの NTFS Access Control List (ACL ; アクセス制御リスト) を設定および適用するための最初のステップです。このセキュリティ記述子をポリシータスクでファイルパスまたはフォルダパスに関連付けます。

### このタスクについて

NTFS セキュリティ形式のボリューム内に存在するファイルやフォルダ、または mixed セキュリティ形式のボリューム上に存在するファイルやフォルダに対して、NTFS セキュリティ記述子を作成できます。

デフォルトでは、セキュリティ記述子を作成すると、Discretionary Access Control List (DACL ; 随意アクセス制御リスト) の 4 つの Access Control Entry (ACE ; アクセス制御エントリ) がそのセキュリティ記述子に追加されます。4 つのデフォルトの ACE は次のとおりです。

オブジェクト	アクセスタイプ	アクセス権	権限の適用先
組み込み管理者	許可 (Allow)	フルコントロール	このフォルダ、サブフォルダ、ファイル
組み込みユーザ	許可 (Allow)	フルコントロール	このフォルダ、サブフォルダ、ファイル
作成者の所有者	許可 (Allow)	フルコントロール	このフォルダ、サブフォルダ、ファイル
NT AUTHORITY\SYSTEM	許可 (Allow)	フルコントロール	このフォルダ、サブフォルダ、ファイル

次のオプションのパラメータを使用して、セキュリティ記述子の設定をカスタマイズできます。

- セキュリティ記述子の所有者
- 所有者のプライマリグループ

- raw 制御フラグ

オプションのパラメータの値はストレージレベルのアクセス保護では無視されます。詳細については、マニュアルページを参照してください。

#### 手順

1. advancedパラメータを使用する場合は、権限レベルをadvancedに設定します。 `set -privilege advanced`
2. セキュリティ記述子を作成します。 `vserver security file-directory ntfs create -vserver vserver_name -ntfs-sd SD_nameoptional_parameters`  
  
`vserver security file-directory ntfs create -ntfs-sd sd1 -vserver vs1 -owner DOMAIN\joe`
3. セキュリティ記述子の設定が正しいことを確認します。 `vserver security file-directory ntfs show -vserver vserver_name -ntfs-sd SD_name`

```
vserver security file-directory ntfs show -vserver vs1 -ntfs-sd sd1
```

```
Vserver: vs1
Security Descriptor Name: sd1
Owner of the Security Descriptor: DOMAIN\joe
```

4. advanced権限レベルの場合は、admin権限レベルに戻ります。 `set -privilege admin`

#### NTFS セキュリティ記述子に NTFS SACL アクセス制御エントリを追加します

NTFS セキュリティ記述子への SACL（システムアクセス制御リスト）アクセス制御エントリ（ACE）の追加は、SVM 内のファイルやフォルダに対する NTFS 監査ポリシーを作成する 2 番目のステップです。エントリごとに、監査するユーザまたはグループを指定します。SACL エントリは、成功したアクセス試行と失敗したアクセス試行のどちらを監査するかを定義します。

#### このタスクについて

セキュリティ記述子の SACL には、1 つ以上の ACE を追加できます。

セキュリティ記述子に含まれている SACL に既存の ACE がある場合は、新しい ACE が SACL に追加されます。セキュリティ記述子に SACL が含まれていない場合は、SACL が作成され、その SACL に新しい ACE が追加されます。

SACLエントリを設定するには、で指定したアカウントの成功イベントまたは失敗イベントについて監査する権限を指定します -account パラメータ権限を指定する場合、次の 3 つの相互に排他的な方法があります。

- 権利
- 詳細な権限

- raw 権限（advanced 権限）



SACL エントリの権限を指定しない場合のデフォルト設定はです Full Control。

必要に応じて、で継承を適用する方法を指定して、SACL エントリをカスタマイズできます apply to パラメータこのパラメータを指定しない場合、デフォルトでは、この SACL エントリがこのフォルダ、サブフォルダ、およびファイルに適用されます。

#### 手順

1. SACL エントリをセキュリティ記述子に追加します。vserver security file-directory ntfs sacl add -vserver vs1 -ntfs-sd sd1 -access-type {failure|success} -account name\_or\_SID optional\_parameters

```
vserver security file-directory ntfs sacl add -ntfs-sd sd1 -access-type failure -account domain\joe -rights full-control -apply-to this-folder -vserver vs1
```

2. SACL エントリが正しいことを確認します。vserver security file-directory ntfs sacl show -vserver vs1 -ntfs-sd sd1 -access-type {failure|success} -account name\_or\_SID

```
vserver security file-directory ntfs sacl show -vserver vs1 -ntfs-sd sd1 -access-type deny -account domain\joe
```

```
Vserver: vs1
Security Descriptor Name: sd1
Access type for Specified Access Rights: failure
Account Name or SID: DOMAIN\joe
Access Rights: full-control
Advanced Access Rights: -
Apply To: this-folder
Access Rights: full-control
```

#### セキュリティポリシーを作成する

Storage Virtual Machine（SVM）の監査ポリシーの作成は、ファイルまたはフォルダに対して ACL を設定および適用する 3 番目のステップです。ポリシーは、さまざまなタスクのコンテナとして機能します。各タスクは、ファイルまたはフォルダに適用できる単一のエントリです。あとで、このセキュリティポリシーにタスクを追加できます。

#### このタスクについて

セキュリティポリシーに追加するタスクには、NTFS セキュリティ記述子とファイルパスまたはフォルダパスとの間の関連付けが含まれます。そのため、セキュリティポリシーは、NTFS セキュリティ形式または mixed セキュリティ形式のボリュームを含む各 Storage Virtual Machine（SVM）に関連付ける必要があります。

#### 手順



1. セキュリティポリシーを作成します。 `vserver security file-directory policy create -vserver vserver_name -policy-name policy_name`

```
vserver security file-directory policy create -policy-name policy1 -vserver vs1
```

2. セキュリティポリシーを確認します。 `vserver security file-directory policy show`

```
vserver security file-directory policy show
Vserver      Policy Name
-----
vs1          policy1
```

セキュリティポリシーにタスクを追加します

ACL を設定し、SVM 内のファイルやフォルダへ適用する 4 番目のステップでは、ポリシータスクを作成してセキュリティポリシーに追加します。ポリシータスクを作成するときに、セキュリティポリシーとタスクを関連付けます。セキュリティポリシーには、1 つ以上のタスクエントリを追加できます。

このタスクについて

セキュリティポリシーはタスクのコンテナです。タスクとは、NTFS または mixed セキュリティが設定されたファイルまたはフォルダ（ストレージレベルのアクセス保護を設定する場合はボリュームオブジェクト）へのセキュリティポリシーによって実行できる単一の処理を指します。

タスクには次の 2 つのタイプがあります。

- ファイルとディレクトリのタスク

指定されたファイルやフォルダにセキュリティ記述子を適用するタスクの指定に使用します。ファイルとディレクトリのタスクによって適用される ACL は、SMB クライアントまたは ONTAP CLI で管理できます。

- ストレージレベルのアクセス保護タスク

指定されたボリュームにストレージレベルのアクセス保護のセキュリティ記述子を適用するタスクの指定に使用します。ストレージレベルのアクセス保護タスクで適用される ACL は ONTAP CLI からのみ管理できます。

タスクには、ファイル（またはフォルダ）やファイルセット（またはフォルダセット）のセキュリティ構成の定義が含まれています。ポリシー内のすべてのタスクは、一意のパスによって識別されます。1 つのポリシー内の 1 つのパスに含められるのは 1 つのタスクだけです。ポリシーに重複するタスクエントリを含めることはできません。

ポリシーへのタスクの追加に関するガイドラインを次に示します。

- ポリシーあたりのタスクエントリは最大 10、000 個です。
- ポリシーには 1 つ以上のタスクを含めることができます。

ポリシーには複数のタスクを含めることができますが、ポリシーにファイルとディレクトリのタスクとストレージレベルのアクセス保護タスクの両方を含めることはできません。ポリシーに含めるタスクは、すべてストレージレベルのアクセス保護タスクにするか、すべてファイルとディレクトリのタスクにする必要があります。

- ストレージレベルのアクセス保護は、権限の制限に使用します。

アクセス権限は付与されません。

次のオプションのパラメータを使用して、セキュリティ記述子の設定をカスタマイズできます。

- セキュリティタイプ
- プロパゲーションモード
- インデックス位置
- アクセス制御の種類

オプションのパラメータの値はストレージレベルのアクセス保護では無視されます。詳細については、マニュアルページを参照してください。

手順

1. セキュリティ記述子が関連付けられているタスクをセキュリティポリシーに追加します。  
`vserver security file-directory policy task add -vserver vserver_name -policy-name policy_name -path path -ntfs-sd SD_nameoptional_parameters`

`file-directory` は、のデフォルト値です `-access-control` パラメータファイルとディレクトリのアクセスタスクを設定する場合、アクセス制御の種類の指定は任意です。

```
vserver security file-directory policy task add -vserver vs1 -policy-name policy1 -path /home/dir1 -security-type ntfs -ntfs-mode propagate -ntfs-sd sd2 -index-num 1 -access-control file-directory
```

2. ポリシータスクの設定を確認します。  
`vserver security file-directory policy task show -vserver vserver_name -policy-name policy_name -path path`

```
vserver security file-directory policy task show
```

Vserver: vs1					
Policy: policy1					
Index	File/Folder	Access	Security	NTFS	NTFS
Security	Path	Control	Type	Mode	
Descriptor	Name				
-----	-----	-----	-----	-----	
1	/home/dir1	file-directory	ntfs	propagate	sd2

## セキュリティポリシーを適用する

SVMへの監査ポリシーの適用は、ファイルまたはフォルダに対してNTFS ACLを作成および適用する最後のステップです。

### このタスクについて

セキュリティポリシーに定義されているセキュリティ設定を、FlexVol ボリューム（NTFS または mixed セキュリティ形式）内の NTFS ファイルおよびフォルダに適用できます。



監査ポリシーと関連する SACL を適用すると、既存の DACL は上書きされます。セキュリティポリシーとそれに関連付けられたDACLが適用されると、既存のDACLはすべて上書きされます。新しいセキュリティポリシーを作成して適用する前に、既存のセキュリティポリシーを確認してください。

### ステップ

1. セキュリティポリシーを適用します。 `vserver security file-directory apply -vserver vserver_name -policy-name policy_name`

```
vserver security file-directory apply -vserver vs1 -policy-name policy1
```

ポリシーを適用するジョブがスケジュールされ、ジョブ ID が返されます。

```
[Job 53322]Job is queued: Fsecurity Apply. Use the "Job show 53322 -id 53322" command to view the status of the operation
```

## セキュリティポリシージョブを監視します

Storage Virtual Machine（SVM）にセキュリティポリシーを適用する場合、セキュリティポリシージョブを監視してその進行状況を監視できます。これは、セキュリティポリシーの適用が成功したかどうかを確認するのに役立ちます。また、多数のファイルやフォルダに一括してセキュリティ設定を適用するような長時間のジョブを実行する場合にも、この方法が便利です。

### このタスクについて

セキュリティポリシージョブに関する詳細情報を表示するには、`show` を使用します `-instance` パラメータ

### ステップ

1. セキュリティポリシージョブを監視します。 `vserver security file-directory job show -vserver vserver_name`

```
vserver security file-directory job show -vserver vs1
```

Job ID	Name	Vserver	Node	State
53322	Fsecurity Apply	vs1	node1	Success
Description: File Directory Security Apply Job				

適用した監査ポリシーを確認します

Storage Virtual Machine（SVM）のファイルやフォルダにセキュリティポリシーを適用した場合に、それらの監査セキュリティの設定が意図したとおりになっているかを確認するには、監査ポリシーを確認します。

このタスクについて

を使用します `vserver security file-directory show` コマンドを使用して監査ポリシーの情報を表示します。データが格納されている SVM の名前、およびファイルまたはフォルダの監査ポリシーの情報を表示するデータのパスを指定する必要があります。

ステップ

1. 監査ポリシーの設定を表示します。 `vserver security file-directory show -vserver vserver_name -path path`

例

次のコマンドは、SVM vs1 のパス「/corp」に適用されている監査ポリシーの情報を表示します。このパスには、SUCCESS と SUCCESS/FAIL SACL の両方のエントリが適用されています。

```

cluster::> vsriver security file-directory show -vsriver vs1 -path /corp

      Vserver: vs1
      File Path: /corp
      Security Style: ntfs
      Effective Style: ntfs
      DOS Attributes: 10
      DOS Attributes in Text: ----D---
      Expanded Dos Attributes: -
      Unix User Id: 0
      Unix Group Id: 0
      Unix Mode Bits: 777
      Unix Mode Bits in Text: rwxrwxrwx
      ACLs: NTFS Security Descriptor
            Control:0x8014
            Owner:DOMAIN\Administrator
            Group:BUILTIN\Administrators
            SACL - ACEs
                  ALL-DOMAIN\Administrator-0x100081-OI|CI|SA|FA
                  SUCCESSFUL-DOMAIN\user1-0x100116-OI|CI|SA
            DACL - ACEs
                  ALLOW-BUILTIN\Administrators-0x1f01ff-OI|CI
                  ALLOW-BUILTIN\Users-0x1f01ff-OI|CI
                  ALLOW-CREATOR OWNER-0x1f01ff-OI|CI
                  ALLOW-NT AUTHORITY\SYSTEM-0x1f01ff-OI|CI

```

#### セキュリティポリシージョブの管理に関する考慮事項

セキュリティポリシージョブが存在する場合、特定の状況下では、そのセキュリティポリシーやポリシーに割り当てられたタスクを変更できません。セキュリティポリシーの変更が確実に成功するように、ポリシーを変更できる条件やできない条件を理解しておく必要があります。ポリシーの変更には、ポリシーに割り当てられたタスクの追加、削除、変更と、ポリシーの削除または変更が含まれます。

セキュリティポリシーにジョブが存在し、そのジョブが次の状態の場合、そのポリシーまたはポリシーに割り当てられたタスクは変更できません。

- ジョブが実行中または実行中です。
- ジョブが一時停止中の場合
- ジョブが再開され、実行中の状態になります。
- ジョブが別のノードへのフェイルオーバーを待機中の場合。

セキュリティポリシーにジョブが存在する場合、次の状況下では、そのセキュリティポリシーまたはポリシーに割り当てられたタスクを正常に変更できます。

- ポリシージョブが停止されました。
- ポリシージョブが正常に終了しました。

#### NTFS セキュリティ記述子を管理するコマンド

ONTAP には、セキュリティ記述子を管理するためのコマンドが用意されています。セキュリティ記述子に関する情報を作成、変更、削除、および表示できます。

状況	使用するコマンド
NTFS セキュリティ記述子を作成します	<code>vserver security file-directory ntfs create</code>
既存の NTFS セキュリティ記述子を変更します	<code>vserver security file-directory ntfs modify</code>
既存の NTFS セキュリティ記述子に関する情報を表示します	<code>vserver security file-directory ntfs show</code>
NTFS セキュリティ記述子を削除します	<code>vserver security file-directory ntfs delete</code>

のマニュアルページを参照してください `vserver security file-directory ntfs` 詳細情報を表示するコマンドです。

#### NTFS DACL アクセス制御エントリを管理するコマンド

ONTAP には、DACL のアクセス制御エントリ（ACE）を管理するためのコマンドが用意されています。ACE はいつでも NTFS DACL に追加できます。また、NTFS DACL の ACE に関する情報を変更、削除、表示するなどで、既存の DACL を管理できます。

状況	使用するコマンド
ACE を作成して NTFS DACL に追加します	<code>vserver security file-directory ntfs dacl add</code>
NTFS DACL の既存の ACE の変更	<code>vserver security file-directory ntfs dacl modify</code>
NTFS DACL の既存の ACE に関する情報を表示します	<code>vserver security file-directory ntfs dacl show</code>
NTFS DACL から既存の ACE を削除します	<code>vserver security file-directory ntfs dacl remove</code>

のマニュアルページを参照してください `vserver security file-directory ntfs dacl` 詳細情報を

表示するコマンドです。

#### NTFS SACLアクセス制御エントリの管理用コマンド

ONTAPには、SACLのアクセス制御エントリ（ACE）を管理するためのコマンドが用意されています。ACE はいつでも NTFS SACL に追加できます。また、NTFS SACL の ACE に関する情報を変更、削除、表示するなどで、既存の SACL を管理することができます。

状況	使用するコマンド
ACE を作成して NTFS SACL に追加します	<code>vserver security file-directory ntfs sacl add</code>
NTFS SACL の既存の ACE の変更	<code>vserver security file-directory ntfs sacl modify</code>
NTFS SACL の既存の ACE に関する情報を表示します	<code>vserver security file-directory ntfs sacl show</code>
NTFS SACL から既存の ACE を削除します	<code>vserver security file-directory ntfs sacl remove</code>

のマニュアルページを参照してください `vserver security file-directory ntfs sacl` 詳細情報を表示するコマンドです。

#### セキュリティポリシーを管理するためのコマンド

ONTAP には、セキュリティポリシーを管理するためのコマンドが用意されています。ポリシーに関する情報を表示したり、ポリシーを削除したりできます。セキュリティポリシーを変更することはできません。

状況	使用するコマンド
セキュリティポリシーを作成する	<code>vserver security file-directory policy create</code>
セキュリティポリシーに関する情報を表示します	<code>vserver security file-directory policy show</code>
セキュリティポリシーを削除する	<code>vserver security file-directory policy delete</code>

のマニュアルページを参照してください `vserver security file-directory policy` 詳細情報を表示するコマンドです。

ONTAP には、セキュリティポリシータスクを追加、変更、削除、および関連する情報表示するためのコマンドが用意されています。

状況	使用するコマンド
セキュリティポリシータスクを追加する	<code>vserver security file-directory policy task add</code>
セキュリティポリシータスクを変更する	<code>vserver security file-directory policy task modify</code>
セキュリティポリシータスクに関する情報を表示します	<code>vserver security file-directory policy task show</code>
セキュリティポリシータスクを削除する	<code>vserver security file-directory policy task remove</code>

のマニュアルページを参照してください `vserver security file-directory policy task` 詳細情報を表示するコマンドです。

ONTAP には、セキュリティポリシージョブを一時停止、再開、停止、および関連する情報表示するためのコマンドが用意されています。

状況	使用するコマンド
セキュリティポリシージョブを一時停止します	<code>vserver security file-directory job pause -vserver vserver_name -id integer</code>
セキュリティポリシージョブを再開します	<code>vserver security file-directory job resume -vserver vserver_name -id integer</code>
セキュリティポリシージョブに関する情報を表示します	<code>vserver security file-directory job show -vserver vserver_name</code> このコマンドを使用して、ジョブのジョブIDを確認できます。
セキュリティポリシージョブを停止します	<code>vserver security file-directory job stop -vserver vserver_name -id integer</code>

のマニュアルページを参照してください `vserver security file-directory job` 詳細情報を表示するコマンドです。



**SMB 共有のメタデータキャッシュを設定します**

**SMB メタデータのキャッシングの仕組み**

メタデータのキャッシングにより、SMB 1.0 クライアントでファイル属性をキャッシュして、ファイル属性およびフォルダ属性にすばやくアクセスできるようになります。属性のキャッシュは、共有ごとに有効または無効にすることができます。メタデータのキャッシングが有効な場合は、キャッシュされたエントリの TTL を設定することもできます。クライアントが SMB 2.x または SMB 3.0 で共有に接続している場合は、メタデータキャッシュの設定は必要ありません。

SMB メタデータのキャッシングを有効にすると、パスとファイルの属性データが一定期間保存されます。これにより、一般的なワークロードでの SMB 1.0 クライアントの SMB パフォーマンスを向上させることができます。

特定のタスクでは、SMB によって大量のトラフィックが作成され、そのトラフィックにはパスとファイルのメタデータに対する複数の同一クエリが含まれることがあります。代わりに、SMB メタデータのキャッシングを使用してキャッシュから情報を読み込むことで、重複するクエリ数を減らし、SMB 1.0 クライアントのパフォーマンスを向上させることができます。



メタデータのキャッシングを使用すると、ごくまれに、古い情報が SMB 1.0 クライアントに提供されることがあります。ご使用の環境でこのリスクを回避する必要がある場合は、この機能を有効にしないでください。

**SMB メタデータのキャッシングを有効にします**

SMB メタデータのキャッシングを有効にすることで、SMB 1.0 クライアントの SMB パフォーマンスを向上させることができます。デフォルトでは、SMB メタデータのキャッシングは無効になっています。

**ステップ**

- 1. 必要な操作を実行します。

状況	入力するコマンド
共有の作成時に SMB メタデータのキャッシングを有効にする	<code>vserver cifs share create -vserver vserver_name -share-name share_name -path path -share-properties attributecache</code>
既存の共有で SMB メタデータのキャッシングを有効にします	<code>vserver cifs share properties add -vserver vserver_name -share-name share_name -share-properties attributecache</code>

**関連情報**

[SMB メタデータキャッシュエントリの有効期間の設定](#)

既存の SMB 共有に対する共有プロパティの追加または削除

**SMB** メタデータキャッシュエントリの有効期間を設定します

SMB メタデータキャッシュエントリの有効期間を設定できます。これにより、環境内での SMB メタデータキャッシュのパフォーマンスを最適化できます。デフォルトは10秒です。

作業を開始する前に

SMB メタデータキャッシュ機能を有効にしている必要があります。SMB メタデータのキャッシングが有効でない場合、SMB キャッシュの TTL 設定は使用されません。

ステップ

- 1. 必要な操作を実行します。

SMB メタデータキャッシュエントリの有効期間を設定する 際の方法	入力するコマンド
共有を作成します	<code>vserver cifs share -create -vserver vserver_name -share-name share_name -path path -attribute-cache-ttl [integerh][integerm][integers]</code>
既存の共有を変更する	<code>vserver cifs share -modify -vserver vserver_name -share-name share_name -attribute-cache-ttl [integerh][integerm][integers]</code>

共有を作成または変更するときに、追加の共有設定オプションおよび共有プロパティを指定できます。詳細については、マニュアルページを参照してください。

ファイルロックを管理します

プロトコル間のファイルロックについて

ファイルロックは、あるユーザが以前に開いていたファイルに別のユーザがアクセスするのを防ぐために、クライアントアプリケーションで使用される方法です。ONTAP でファイルをロックする方法は、クライアントのプロトコルによって異なります。

クライアントが NFS クライアントである場合、ロックは任意に設定します。クライアントが SMB クライアントである場合、ロックは必須となります。

NFS ファイルと SMB ファイルのロックの違いのため、SMB アプリケーションですでに開いているファイルに NFS クライアントからアクセスすると、エラーになる場合があります。

NFS クライアントが SMB アプリケーションによってロックされたファイルにアクセスすると、次のいずれかの状態になります。

- mixed形式またはNTFS形式のボリュームでは、などのファイル操作が行われます `rm`、`rmdir` および `mv` NFSアプリケーションが失敗するように原因 できますか。
- NFS の読み取りと書き込みの処理は、SMB の読み取り拒否および書き込み拒否のオープンモードによってそれぞれ拒否されます。
- また、ファイルの書き込み対象となる範囲が、排他的な SMB バイトロックでロックされている場合も、NFS の書き込みの処理はエラーになります。
- リンク解除

- NTFSファイルシステムでは、SMBとCIFSの削除処理がサポートされます。

ファイルは最後に閉じた後に削除されます。

- NFSのリンク解除処理はサポートされていません。

NTFSセマンティクスとSMBセマンティクスが必要であり、NFSでは前回の削除時のクローズ処理がサポートされないため、この処理はサポートされません。

- UNIXファイルシステムでは、リンク解除操作がサポートされます。

NFSとUNIXのセマンティクスが必要なため、サポートされています。

- 名前を変更する

- NTFSファイルシステムの場合、デスティネーションファイルがSMBまたはCIFSから開かれていれば、デスティネーションファイルの名前を変更できます。

- NFSの名前変更はサポートされていません。

NTFSセマンティクスとSMBセマンティクスが必要なため、サポートされていません。

UNIX セキュリティ形式のボリュームでは、NFS のリンク解除および名前変更の処理で SMB のロック状態が無視され、ファイルへのアクセスが許可されます。UNIX セキュリティ形式のボリュームでのその他すべての NFS 処理では、SMB のロック状態が考慮されます。

#### ONTAP による読み取り専用ビットの処理方法

読み取り専用ビットは、ファイルが書き込み可能（無効）なのか読み取り専用（有効）なのかを示すために、ファイルごとに設定されます。

Windows を使用する SMB クライアントは、ファイルごとの読み取り専用ビットを設定できます。NFS クライアントは、ファイルごとの読み取り専用ビットを設定しません。NFS クライアントは、ファイルごとの読み取り専用ビットを使用するプロトコル操作を行わないためです。

ONTAP は、Windows を使用する SMB クライアントによってファイルが作成される際に、そのファイルに読み取り専用ビットを設定できます。ファイルが NFS クライアントと SMB クライアント間で共有されている場合も、ONTAP は読み取り専用ビットを設定できます。一部のソフトウェアは、NFS クライアントおよび SMB クライアントで使用される場合、読み取り専用ビットが有効になっている必要があります。

NFS クライアントと SMB クライアント間で共有されるファイルに対して、適切な読み取りおよび書き込み権限を保持するために、読み取り専用ビットが次の規則に従って処理されます。 ONTAP

- NFS は、読み取り専用ビットが有効になっているファイルを書き込み権限ビットが無効になっているファ

イルとして扱います。

- NFS クライアントがすべての書き込み権限ビットを無効にしたときに、これらのうち少なくとも 1 つが以前有効であったら、ONTAP はそのファイルの読み取り専用ビットを有効にします。
- NFS クライアントがすべての書き込み権限ビットを有効にすると、ONTAP はそのファイルの読み取り専用ビットを無効にします。
- あるファイルの読み取り専用ビットが有効になっているときに、NFS クライアントがそのファイルの権限を調べようとすると、そのファイルの権限ビットは NFS クライアントには送信されず、代わりに書き込み権限ビットがマスクされた権限ビットが ONTAP クライアントに送信されます。
- ファイルの読み取り専用ビットが有効になっているときに、SMB クライアントがこの読み取り専用ビットを無効にすると、ONTAP はそのファイルに対する所有者の書き込み権限ビットを有効にします。
- 読み取り専用ビットが有効になっているファイルに書き込めるのは、root のみです。



ファイル権限の変更は、SMB クライアントではすぐに反映されますが、NFS クライアントが属性のキャッシュを有効にしている場合は NFS クライアントではすぐに反映されないことがあります。

共有パスコンポーネントのロックの処理に関する **ONTAP** と **Windows** の違い

Windows とは異なり、ONTAP では、ファイルが開いているときにそのファイルのパスの各コンポーネントがロックされません。この動作は SMB 共有パスにも影響します。

ONTAP 原因ではパスの各コンポーネントがロックされないため、開いているファイルまたは共有より上のパスコンポーネントの名前を変更できます。このため、特定のアプリケーションで原因の問題が発生したり、SMB 構成の共有パスを無効な名前に変更したりすることができます。原因によって共有にアクセスできなくなる可能性があります。

パスコンポーネントの名前変更による問題を回避するには、ユーザまたはアプリケーションが重要なディレクトリの名前を変更できないようにするセキュリティ設定を適用します。

ロックに関する情報を表示します

有効になっているロックの種類とロックの状態、バイト範囲ロック、共有ロックモード、委譲ロック、および便宜的ロックの詳細、永続性ハンドルを使用してロックが開かれているかどうかなど、現在のファイルロックに関する情報を表示できます。

このタスクについて

NFSv4 または NFSv4.1 を使用して確立されたロックについては、クライアント IP アドレスを表示できません。

デフォルトでは、すべてのロックに関する情報が表示されます。コマンドパラメータを使用すると、特定の Storage Virtual Machine (SVM) のロックに関する情報を表示したり、他の条件によってコマンドの出力をフィルタリングしたりできます。

。 `vserver locks show` コマンドは、次の4種類のロックに関する情報を表示します。

- バイト範囲ロック。ファイルの一部のみをロックします。
- 共有ロック。開いているファイルをロックします。

- 便宜的ロック。SMB を使用してクライアント側キャッシュを制御します。
- 委譲。NFSv4.x を使用してクライアント側キャッシュを制御します

オプションのパラメータを指定すると、各ロックタイプに関する重要な情報を確認できます。詳細については、コマンドのマニュアルページを参照してください。

## ステップ

1. を使用して、ロックに関する情報を表示します vservers locks show コマンドを実行します

## 例

次の例は、パスのファイルに対するNFSv4ロックに関する概要情報を表示します /vol1/file1。共有ロックのアクセスモードは write-deny\_none であり、書き込み委譲でロックが許可されています。

```
cluster1::> vservers locks show

Vserver: vs0
Volume  Object Path          LIF          Protocol  Lock Type  Client
-----
-----
vol1    /vol1/file1             lif1         nfsv4     share-level -
                Sharelock Mode: write-deny_none
                delegation -
                Delegation Type: write
```

次の例は、パスのファイルに対するSMBロックに関するoplockおよび共有ロックの詳細情報を表示します /data2/data2\_2/intro.pptx。IP アドレスが 10.3.1.3 のクライアントに対して、共有ロックのアクセスモードを write-deny\_none として、永続性ハンドルが許可されています。バッチの oplock レベルで oplock リースが許可されています。

```
cluster1::> vservers locks show -instance -path /data2/data2_2/intro.pptx

Vserver: vs1
Volume: data2_2
Logical Interface: lif2
Object Path: /data2/data2_2/intro.pptx
Lock UUID: 553cf484-7030-4998-88d3-1125adbba0b7
Lock Protocol: cifs
Lock Type: share-level
Node Holding Lock State: node3
Lock State: granted
Bytelock Starting Offset: -
Number of Bytes Locked: -
Bytelock is Mandatory: -
Bytelock is Exclusive: -
Bytelock is Superlock: -
```

```

    Bytelock is Soft: -
        Oplock Level: -
Shared Lock Access Mode: write-deny_none
    Shared Lock is Soft: false
        Delegation Type: -
            Client Address: 10.3.1.3
                SMB Open Type: durable
                    SMB Connect State: connected
SMB Expiration Time (Secs): -
    SMB Open Group ID:
78a90c59d45ae211998100059a3c7a00a007f70da0f8ffffcd445b0300000000

        Vserver: vs1
            Volume: data2_2
Logical Interface: lif2
    Object Path: /data2/data2_2/test.pptx
        Lock UUID: 302fd7b1-f7bf-47ae-9981-f0dcb6a224f9
            Lock Protocol: cifs
                Lock Type: op-lock
Node Holding Lock State: node3
    Lock State: granted
Bytelock Starting Offset: -
    Number of Bytes Locked: -
        Bytelock is Mandatory: -
        Bytelock is Exclusive: -
        Bytelock is Superlock: -
            Bytelock is Soft: -
                Oplock Level: batch
Shared Lock Access Mode: -
    Shared Lock is Soft: -
        Delegation Type: -
            Client Address: 10.3.1.3
                SMB Open Type: -
                    SMB Connect State: connected
SMB Expiration Time (Secs): -
    SMB Open Group ID:
78a90c59d45ae211998100059a3c7a00a007f70da0f8ffffcd445b0300000000

```

ロックを解除します

ファイルロックが原因でクライアントがファイルにアクセスできなくなっている場合は、現在有効なロックの情報を表示して、特定のロックを解除することができます。ロックの解除が必要になるケースとしては、アプリケーションのデバッグなどが挙げられます。

このタスクについて

。 `vserver locks break` コマンドは、`advanced`権限レベル以上でのみ使用できます。詳細については、コマンドのマニュアルページを参照してください。

手順

- 1. ロックを解除するために必要な情報を確認するには、を使用します `vserver locks show` コマンドを実行します

詳細については、コマンドのマニュアルページを参照してください。

- 2. 権限レベルを `advanced` に設定します。 `set -privilege advanced`
- 3. 次のいずれかを実行します。

ロックを解除するための指定項目	入力するコマンド
SVM 名、ボリリューム名、 LIF 名、およびファイルパス	<code>vserver locks break -vserver vserver_name -volume volume_name -path path -lif lif</code>
ロック ID	<code>vserver locks break -lockid UUID</code>

- 4. `admin` 権限レベルに戻ります。 `set -privilege admin`

SMB のアクティビティを監視する

SMB セッション情報を表示します

SMB 接続、SMB セッション ID 、セッションを使用しているワークステーションの IP アドレスなど、確立された SMB セッションに関する情報を表示できます。セッションの SMB プロトコルバージョンや継続的可用性を備えた保護のレベルに関する情報を表示できます。この情報は、セッションでノンストップオペレーションがサポートされているかどうか確認するのに役立ちます。

このタスクについて

SVM 上のすべてのセッションに関する情報を要約形式で表示できます。ただし、多くの場合、大量の出力が返されます。オプションのパラメータを指定すると、出力に表示される情報をカスタマイズできます。

- オプションのを使用できます `-fields` 選択したフィールドに関する出力を表示するためのパラメータ。  
入ることができます `-fields ?` 使用できるフィールドを決定します。
- を使用できます `-instance` 確立されたSMBセッションに関する詳細情報を表示するためのパラメータ。
- を使用できます `-fields` パラメータまたは `-instance` パラメータのみ、または他のオプションパラメータと組み合わせて指定します。

ステップ

- 1. 次のいずれかを実行します。

表示する <b>SMB</b> セッション情報	入力するコマンド
SVM 上のすべてのセッションを要約形式で表示します	<code>vserver cifs session show -vserver vserver_name</code>
指定した接続 ID のセッション	<code>vserver cifs session show -vserver vserver_name -connection-id integer</code>
指定したワークステーションの IP アドレスからのセッションです	<code>vserver cifs session show -vserver vserver_name -address workstation_IP_address</code>
指定した LIF IP アドレスのセッションを表示します	<code>vserver cifs session show -vserver vserver_name -lif-address LIF_IP_address</code>
指定したノード上のセッションを表示します	<code>`vserver cifs session show -vserver vserver_name -node {node_name</code>
<code>local}`</code>	指定した Windows ユーザからのセッションです
<code>vserver cifs session show -vserver vserver_name -windows-user domain_name\\user_name</code>	を指定します
<code>`vserver cifs session show -vserver vserver_name -auth-mechanism {NTLMv1</code>	NTLMv2
Kerberos	Anonymous}`
指定したプロトコルバージョンを使用しているセッションです	<code>`vserver cifs session show -vserver vserver_name -protocol-version {SMB1</code>
SMB2	SMB2_1
SMB3	SMB3_1}`  [NOTE] ==== 継続的可用性を備えた保護と SMB マルチチャネルは、SMB 3.0 以降のセッションでのみ利用できます。該当するすべてのセッションのステータスを表示するには、このパラメータの値をに設定します SMB3 以降が必要です。  =====
指定したレベルの継続的可用性を備えた保護を使用しているセッション	<code>`vserver cifs session show -vserver vserver_name -continuously-available {No</code>



表示する <b>SMB</b> セッション情報	入力するコマンド
Yes	Partial}`  [NOTE] ==== 継続的可用性のステータスがの場合 Partial`つまり、継続的可用性を備えた開いているファイルがセッションに少なくとも1つ含まれていますが、継続的可用性を備えた保護を使用して開かれていないファイルがセッションに含まれています。を使用できます `vserver cifs sessions file show コマンドを使用して、確立されたセッションのどのファイルが継続的可用性を備えた保護で開かれていないかを確認します。  ====
指定した SMB 署名セッションステータスのセッション	`vserver cifs session show -vserver vs1 -is-session-signed {true

## 例

次のコマンドを実行すると、IP アドレスが 10.1.1.1 のワークステーションから確立された SVM vs1 上のセッションに関するセッション情報が表示されます。

```
cluster1::> vserver cifs session show -address 10.1.1.1
Node:    node1
Vserver: vs1
Connection Session
ID        ID        Workstation    Windows User    Open    Idle
-----  -
3151272279,
3151272280,
3151272281  1        10.1.1.1        DOMAIN\joe        2        23s
```

次のコマンドを実行すると、SVM vs1 上の継続的可用性を備えた保護を使用するセッションに関する詳細なセッション情報が表示されます。この接続はドメインアカウントを使用して確立されています。

```
cluster1::> vsriver cifs session show -instance -continuously-available  
Yes
```

```
Node: node1  
Vserver: vs1  
Session ID: 1  
Connection ID: 3151274158  
Incoming Data LIF IP Address: 10.2.1.1  
Workstation IP address: 10.1.1.2  
Authentication Mechanism: Kerberos  
Windows User: DOMAIN\SERVER1$  
UNIX User: pcuser  
Open Shares: 1  
Open Files: 1  
Open Other: 0  
Connected Time: 10m 43s  
Idle Time: 1m 19s  
Protocol Version: SMB3  
Continuously Available: Yes  
Is Session Signed: false  
User Authenticated as: domain-user  
NetBIOS Name: -  
SMB Encryption Status: Unencrypted
```

次のコマンドは、SVM vs1 上の SMB 3.0 と SMB マルチチャネルを使用しているセッションに関する情報を表示します。この例では、ユーザは LIF IP アドレスを使用して SMB 3.0 対応のクライアントからこの共有に接続しています。そのため、認証メカニズムはデフォルトの NTLMv2 になっています。継続的可用性を備えた保護を使用して接続するためには、Kerberos 認証を使用して接続を確立する必要があります。

```
cluster1::> vserver cifs session show -instance -protocol-version SMB3
```

```

Node: node1
Vserver: vs1
Session ID: 1
**Connection IDs: 3151272607,31512726078,3151272609
Connection Count: 3**
Incoming Data LIF IP Address: 10.2.1.2
Workstation IP address: 10.1.1.3
Authentication Mechanism: NTLMv2
Windows User: DOMAIN\administrator
UNIX User: pcuser
Open Shares: 1
Open Files: 0
Open Other: 0
Connected Time: 6m 22s
Idle Time: 5m 42s
Protocol Version: SMB3
Continuously Available: No
Is Session Signed: false
User Authenticated as: domain-user
NetBIOS Name: -
SMB Encryption Status: Unencrypted
```

## 関連情報

### 開いている SMB ファイルに関する情報を表示する

開いている **SMB** ファイルに関する情報を表示します

SMB 接続、SMB セッション ID、ホスティングボリューム、共有名、共有パスなど、開いている SMB ファイルに関する情報を表示できます。ファイルの継続的可用性を備えた保護のレベルに関する情報を表示できます。この情報は、開いているファイルがノンストップオペレーションをサポートする状態であるかどうか確認するのに役立ちます。

#### このタスクについて

確立された SMB セッションで開いているファイルに関する情報を表示できます。これは、SMB セッション内の特定のファイルに関する SMB セッション情報を確認する必要がある場合に役立ちます。

たとえば、SMBセッションで、開いているファイルの一部が継続的可用性を備えた保護を使用して開いている場合と、残りのファイルが継続的可用性を備えた保護を使用して開かれていない場合（の値）`-continuously-available` フィールドに入力します `vserver cifs session show` コマンド出力はです `Partial`）の場合は、このコマンドを使用して、継続的可用性に対応していないファイルを確認できます。

を使用して、Storage Virtual Machine（SVM）上の確立されたSMBセッションのすべての開いているファイル

に関する情報を要約形式で表示できます `vserver cifs session file show` オプションのパラメータを指定しないコマンド。

ただし、多くの場合、大量の出力が返されます。オプションのパラメータを指定すると、出力に表示される情報をカスタマイズできます。これは、開いているファイルの一部のみにに関する情報を表示する場合に便利です。

- オプションのを使用できます `-fields` 選択したフィールドの出力を表示するためのパラメータ。

このパラメータは、単独で使用することも、他のオプションのパラメータと組み合わせて使用することもできます。

- を使用できます `-instance` 開いているSMBファイルに関する詳細情報を表示するためのパラメータ。

このパラメータは、単独で使用することも、他のオプションのパラメータと組み合わせて使用することもできます。

## ステップ

1. 次のいずれかを実行します。

表示する開いている <b>SMB</b> ファイル	入力するコマンド
をクリックします	<code>vserver cifs session file show -vserver vserver_name</code>
指定したノード上のセッションを表示します	<code>`vserver cifs session file show -vserver vserver_name -node {node_name</code>
<code>local}`</code>	指定したファイル ID のファイル
<code>vserver cifs session file show -vserver vserver_name -file-id integer</code>	指定した SMB 接続 ID のファイル
<code>vserver cifs session file show -vserver vserver_name -connection-id integer</code>	指定した SMB セッション ID のファイル
<code>vserver cifs session file show -vserver vserver_name -session-id integer</code>	指定したホスティングアグリゲートのファイル
<code>vserver cifs session file show -vserver vserver_name -hosting -aggregate aggregate_name</code>	指定したボリュームのファイルです
<code>vserver cifs session file show -vserver vserver_name -hosting-volume volume_name</code>	指定した SMB 共有のファイル

表示する開いている <b>SMB</b> ファイル	入力するコマンド
<code>vserver cifs session file show -vserver vserver_name -share share_name</code>	指定した SMB パスのオブジェクト
<code>vserver cifs session file show -vserver vserver_name -path path</code>	指定したレベルの継続的可用性を備えた保護を使用しているファイル
<code>`vserver cifs session file show -vserver vserver_name -continuously-available {No</code>	Yes}`  [NOTE] ==== 継続的可用性のステータスがこの場合 `No` つまり、 これらの開いているファイルは、テイクオーバーや ギブバックからの無停止でのリカバリには対応して いません。また、可用性の高い関係にあるパートナ ー間での一般的なアグリゲートの再配置からリカバ リすることもできません。  ====
指定した再接続の状態のファイル	<code>`vserver cifs session file show -vserver vserver_name -reconnected {No</code>

ほかにも、出力結果の絞り込みに使用できるオプションのパラメータがあります。詳細については、のマニュアルページを参照してください。

## 例

次の例は、SVM vs1 の開いているファイルに関する情報を表示します。

```
cluster1::> vserver cifs session file show -vserver vs1
Node:      node1
Vserver:    vs1
Connection: 3151274158
Session:    1
File        File        Open Hosting      Continuously
ID          Type          Mode Volume      Share      Available
-----
41          Regular    r      data        data        Yes
Path: \mytest.rtf
```

次の例は、SVM vs1 のファイル ID 82 の開いている SMB ファイルに関する詳細情報を表示します。

```
cluster1::> vsriver cifs session file show -vsriver vs1 -file-id 82
-instance
```

```
Node: node1
Vserver: vs1
File ID: 82
Connection ID: 104617
Session ID: 1
File Type: Regular
Open Mode: rw
Aggregate Hosting File: aggr1
Volume Hosting File: data1
CIFS Share: data1
Path from CIFS Share: windows\win8\test\test.txt
Share Mode: rw
Range Locks: 1
Continuously Available: Yes
Reconnected: No
```

## 関連情報

### SMB セッション情報の表示

使用可能な統計オブジェクトと統計カウンタを確認します

CIFS、SMB、監査、および BranchCache ハッシュの統計に関する情報を取得してパフォーマンスを監視する前に、データの取得に使用できるオブジェクトとカウンタを確認しておく必要があります。

## 手順

1. 権限レベルを advanced に設定します。set -privilege advanced
2. 次のいずれかを実行します。

確認する項目	入力するコマンド
使用可能なオブジェクト	statistics catalog object show
使用可能な特定のオブジェクト	statistics catalog object show object object_name
使用可能なカウンタ	statistics catalog counter show object object_name

使用可能なオブジェクトとカウンタの詳細については、マニュアルページを参照してください。

3. admin 権限レベルに戻ります。set -privilege admin

## 例

次のコマンドを実行すると、advanced 権限レベルで表示したときの、クラスタ内の CIFS および SMB アクセスに関連する特定の統計オブジェクトの説明が表示されます。

```
cluster1::> set -privilege advanced

Warning: These advanced commands are potentially dangerous; use them only
when directed to do so by support personnel.
Do you want to continue? {y|n}: y

cluster1::*> statistics catalog object show -object audit
    audit_ng                      CM object for exporting audit_ng
performance counters

cluster1::*> statistics catalog object show -object cifs
    cifs                          The CIFS object reports activity of the
                                Common Internet File System protocol
                                ...

cluster1::*> statistics catalog object show -object nblade_cifs
    nblade_cifs                  The Common Internet File System (CIFS)
                                protocol is an implementation of the
Server
                                ...

cluster1::*> statistics catalog object show -object smb1
    smb1                         These counters report activity from the
SMB
                                revision of the protocol. For information
                                ...

cluster1::*> statistics catalog object show -object smb2
    smb2                         These counters report activity from the
                                SMB2/SMB3 revision of the protocol. For
                                ...

cluster1::*> statistics catalog object show -object hashd
    hashd                       The hashd object provides counters to
measure
                                the performance of the BranchCache hash
daemon.
cluster1::*> set -privilege admin
```

次のコマンドは、の一部のカウンタに関する情報を表示します cifs advanced権限レベルで表示されるオブジェクト。



この例では、で使用可能なカウンタの一部が表示されているわけではありません cifs オブジェクト。出力は切り捨てられます。

```
cluster1::> set -privilege advanced
```

Warning: These advanced commands are potentially dangerous; use them only when directed to do so by support personnel.

Do you want to continue? {y|n}: y

```
cluster1::*> statistics catalog counter show -object cifs
```

Object: cifs

Counter	Description
active_searches	Number of active searches over SMB and SMB2
auth_reject_too_many	Authentication refused after too many requests were made in rapid succession
avg_directory_depth	Average number of directories crossed by SMB and SMB2 path-based commands
...	...

```
cluster2::> statistics start -object client -sample-id
```

Object: client

Counter	Value
cifs_ops	0
cifs_read_ops	0
cifs_read_recv_ops	0
cifs_read_recv_size	0B
cifs_read_size	0B
cifs_write_ops	0
cifs_write_recv_ops	0
cifs_write_recv_size	0B
cifs_write_size	0B
instance_name	vserver_1:10.72.205.179
instance_uuid	2:10.72.205.179
local_ops	0
mount_ops	0

[...]



関連情報

[統計情報を表示します](#)

統計情報を表示します

CIFS と SMB 、監査、および BranchCache ハッシュに関する統計など、さまざまな統計を表示して、パフォーマンスを監視し、問題を診断することができます。

作業を開始する前に

を使用してデータサンプルを収集しておく必要があります `statistics start` および `statistics stop` オブジェクトに関する情報を表示する前のコマンド。

手順

- 1. 権限レベルを `advanced` に設定します。 `set -privilege advanced`
- 2. 次のいずれかを実行します。

統計を表示する対象	入力するコマンド
SMB のすべてのバージョン	<code>statistics show -object cifs</code>
SMB 1.0	<code>statistics show -object smb1</code>
SMB 2.x と SMB 3.0	<code>statistics show -object smb2</code>
ノードの CIFS サブシステム	<code>statistics show -object nblade_cifs</code>
マルチプロトコルの監査	<code>statistics show -object audit_ng</code>
BranchCache ハッシュサービス	<code>statistics show -object hashd</code>
動的 DNS	<code>statistics show -object ddns_update</code>

詳細については、各コマンドのマニュアルページを参照してください。

- 3. `admin` 権限レベルに戻ります。 `set -privilege admin`

関連情報

[使用可能な統計オブジェクトと統計カウンタの確認](#)

[SMB 署名済みセッションの統計の監視](#)

[BranchCache 統計を表示します](#)

[統計を使用した自動ノードリファラルのアクティビティの監視](#)

["Microsoft Hyper-V および SQL Server 向けの SMB の設定"](#)

## SMB クライアントベースのサービスを導入する

オフラインファイルを使用して、オフラインで使用するファイルをキャッシュできます

オフラインファイルを使用して、オフラインで使用するためのファイルのキャッシュの概要を確認します

ONTAP では、Microsoft のオフラインファイル機能（\_クライアント側キャッシュ\_）をサポートしています。これにより、オフラインで使用するファイルをローカルホストにキャッシュできます。オフラインファイル機能を使用すると、ネットワークから切断されているファイルでも作業を継続できます。

Windows のユーザドキュメントやプログラムを共有に自動的にキャッシュするかどうか、またはキャッシュするファイルを手動で選択するかどうかを指定できます。新しい共有では、手動キャッシュがデフォルトで有効になります。オフラインで利用可能となったファイルは、Windows クライアントのローカルディスクと同期されます。同期は、特定のストレージシステム共有へのネットワーク接続がリストアされたときに実行されます。

オフラインのファイルおよびフォルダに対するアクセス権限は CIFS サーバに保存されているファイルおよびフォルダと同じであるため、オフラインのファイルおよびフォルダに対して処理を実行するには、CIFS サーバに保存されているファイルおよびフォルダに対する十分な権限が必要です。

ユーザとネットワーク上の他のユーザが同じファイルに変更を加えた場合、ユーザはネットワークにローカルバージョンのファイルを保存するか、別のバージョンを保持するか、または両方を保存できます。両方のバージョンを残す場合は、ローカルユーザが変更した新しいファイルがローカルに保存され、キャッシュされたファイルは CIFS サーバに保存されたバージョンの変更が反映されて上書きされます。

オフラインファイルは、共有ごとに共有の設定を行うことができます。共有を作成または変更するときに、次の 4 つのオフラインフォルダ設定のいずれかを選択できます。

- キャッシュなし

共有のクライアント側キャッシュを無効にします。クライアントのローカルにファイルやフォルダが自動的にキャッシュされず、ユーザがファイルやフォルダをローカルにキャッシュすることもできません。

- 手動キャッシュ

共有にキャッシュするファイルを手動で選択できるようにします。これがデフォルト設定です。デフォルトでは、ファイルやフォルダはローカルクライアントにキャッシュされません。オフラインで使用するためにローカルにキャッシュするファイルやフォルダをユーザが選択できます。

- ドキュメントの自動キャッシュ

ユーザのドキュメントが共有に自動的にキャッシュされるようにします。ローカルにキャッシュされるのは、アクセスしたファイルとフォルダだけです。

- プログラムの自動キャッシュ

プログラムとユーザのドキュメントが共有に自動的にキャッシュされるようにします。ローカルにキャッシュされるのは、アクセスしたファイル、フォルダ、およびプログラムだけです。また、この設定を有効にすると、ネットワークに接続されている場合でも、クライアントはローカルにキャッシュされた実行フ

ファイルを実行できます。

Windows サーバおよびクライアントでのオフラインファイルの設定の詳細については、Microsoft TechNet ライブラリを参照してください。

#### 関連情報

[移動プロファイルを使用した SVM に関連付けられた CIFS サーバへのユーザプロファイルの一元的な格納](#)

[フォルダリダイレクトを使用した CIFS サーバへのデータの格納](#)

[BranchCache を使用したブランチオフィスでの SMB 共有のコンテンツのキャッシュ](#)

"Microsoft TechNet ライブラリ： [technet.microsoft.com/en-us/library/](https://technet.microsoft.com/en-us/library/)"

オフラインファイルを使用するための要件

CIFS サーバで Microsoft のオフラインファイル機能を使用する前に、この機能をサポートする ONTAP および SMB のバージョンと Windows クライアントの種類について確認しておく必要があります。

#### ONTAP のバージョンの要件

ONTAP の各リリースでオフラインファイルがサポートされます。

#### SMB プロトコルのバージョン

Storage Virtual Machine （SVM ONTAP）については、すべてのバージョンの SMB でオフラインファイルがサポートされます。

#### Windows クライアントの要件

Windows クライアントでオフラインファイルがサポートされている必要があります。

オフラインファイル機能をサポートする Windows クライアントに関する最新情報については、Interoperability Matrix を参照してください。

["mysupport.netapp.com/matrix"](https://mysupport.netapp.com/matrix)

オフラインファイルの導入に関するガイドラインを参照してください

が搭載されたホームディレクトリ共有にオフラインファイルを導入する場合は、いくつかの重要なガイドラインについて理解しておく必要があります。showsnapshot ホームディレクトリに設定された共有プロパティ。

状況に応じて showsnapshot オフラインファイルが設定されているホームディレクトリ共有で共有プロパティが設定されている場合、Windows クライアントはすべての Snapshot コピーをの下にキャッシュします ~snapshot ユーザのホームディレクトリ内のフォルダ。

次のいずれかに該当する場合、Windows クライアントでは、すべての Snapshot コピーがホームディレクトリの下にキャッシュされます。

- ユーザが、ホームディレクトリをクライアントからオフラインで利用できるようにしている。

の内容 ~snapshot ホームディレクトリ内のフォルダが含まれ、オフラインで使用できるようになります。

- ユーザは、などのフォルダをリダイレクトするようにフォルダリダイレクトを設定します My Documents CIFSサーバ共有上のホームディレクトリのルートに移動します。

Windows クライアントによっては、リダイレクトされたフォルダが自動的にオフラインで利用できるようになる場合があります。フォルダがホームディレクトリのルートにリダイレクトされる場合は ~snapshot フォルダは、キャッシュされたオフラインコンテンツに含まれます。



ファイル導入をオフラインにします ~snapshot フォルダはオフラインファイルに含まれないようにしてください。内のSnapshotコピー ~snapshot フォルダには、ONTAP がSnapshotコピーを作成した時点のボリューム上のすべてのデータが格納されます。そのため、のオフラインコピーを作成します ~snapshot フォルダは、クライアント上のローカルストレージを大量に消費し、オフラインファイルの同期中にネットワーク帯域幅を消費します。また、オフラインファイルの同期にかかる時間も長くなります。

CLI を使用して **SMB** 共有でオフラインファイルサポートを設定します

SMB 共有の作成時に、または既存の SMB 共有の変更時にいつでも、ONTAP CLI を使用して、4 つのオフラインファイル設定のいずれかを指定することによって、オフラインファイルのサポートを設定できます。手動オフラインファイルのサポートがデフォルト設定です。

このタスクについて

オフラインファイルのサポートを設定する場合は、次の 4 つのオフラインファイル設定のいずれかを選択できます。

設定	説明
none	Windows クライアントがこの共有のファイルをキャッシュすることを禁止します。
manual	Windows クライアントのユーザが、キャッシュするファイルを手動で選択できるようにします。
documents	Windows クライアントがオフラインアクセスのために使用するユーザのドキュメントをキャッシュすることを許可します。
programs	Windows クライアントがオフラインアクセスのために使用するプログラムをキャッシュすることを許可します。クライアントは、共有が使用可能な場合でも、キャッシュしたプログラムファイルをオフラインモードで使用できます。

選択できるオフラインファイル設定は 1 つだけです。既存の SMB 共有でオフラインファイル設定を変更する

と、元の設定が新しいオフラインファイル設定に置き換えられます。その他の既存の SMB 共有設定および共有プロパティは、削除も置換もされません。明示的に削除または変更しないかぎり、有効なままです。

手順

- 1. 適切な操作を実行します。

オフラインファイルを設定する対象	入力するコマンド
新しい SMB 共有	<code>`vserver cifs share create -vserver vserver_name -share-name share_name -path path -offline-files {none</code>
manual	documents
programs}`	既存の SMB 共有
<code>`vserver cifs share modify -vserver vserver_name -share-name share_name -offline-files {none</code>	manual
documents	programs}`

- 2. SMB共有の設定が正しいことを確認します。 `vserver cifs share show -vserver vserver_name -share-name share_name -instance`

例

次のコマンドでは、オフラインファイルをに設定して「data1」という名前のSMB共有を作成します documents：

```
cluster1::> vsserver cifs share create -vsserver vs1 -share-name data1 -path
/data1 -comment "Offline files" -offline-files documents

cluster1::> vsserver cifs share show -vsserver vs1 -share-name data1
-instance

                Vserver: vs1
                Share: data1
CIFS Server NetBIOS Name: VS1
                Path: /data1
        Share Properties: oplocks
                        browsable
                        changenotify
        Symlink Properties: enable
        File Mode Creation Mask: -
        Directory Mode Creation Mask: -
                Share Comment: Offline files
                Share ACL: Everyone / Full Control
        File Attribute Cache Lifetime: -
                Volume Name: -
                Offline Files: documents
        Vscan File-Operations Profile: standard
        Maximum Tree Connections on Share: 4294967295
                UNIX Group for File Create: -
```

次のコマンドは、オフラインファイルの設定をに変更することで、「data1」という名前の既存のSMB共有を変更します manual ファイルモードとディレクトリモードの作成マスクの値を追加します。

```
cluster1::> vsserver cifs share modify -vsserver vs1 -share-name data1
-offline-files manual -file-umask 644 -dir-umask 777
```

```
cluster1::> vsserver cifs share show -vsserver vs1 -share-name data1
-instance
```

```

                Vserver: vs1
                Share: data1
    CIFS Server NetBIOS Name: VS1
                Path: /data1
    Share Properties: oplocks
                    browsable
                    changenotify
    Symlink Properties: enable
    File Mode Creation Mask: 644
    Directory Mode Creation Mask: 777
    Share Comment: Offline files
    Share ACL: Everyone / Full Control
    File Attribute Cache Lifetime: -
    Volume Name: -
    Offline Files: manual
    Vscan File-Operations Profile: standard
    Maximum Tree Connections on Share: 4294967295
    UNIX Group for File Create: -
```

## 関連情報

### 既存の SMB 共有に対する共有プロパティの追加または削除

コンピュータの管理 MMC を使用して、SMB 共有でオフラインファイルサポートを設定します

オフラインで使用するためにファイルをローカルにキャッシュすることをユーザに許可する場合は、コンピュータの管理 MMC（Microsoft 管理コンソール）を使用してオフラインファイルのサポートを設定できます。

## 手順

1. Windows サーバー上の MMC を開くには、Windows エクスプローラで、ローカルコンピューターのアイコンを右クリックし、\* 管理 \* を選択します。
2. 左側のパネルで、「\* コンピュータの管理 \*」を選択します。
3. 「\* アクション \* > \* 別のコンピューターに接続 \*」を選択します。

[ コンピュータの選択 ] ダイアログボックスが表示されます。

4. CIFS サーバの名前を入力するか、\* Browse \* をクリックして CIFS サーバを指定します。

CIFS サーバの名前が Storage Virtual Machine（SVM）ホスト名と同じである場合は、SVM 名を入力し

ます。CIFS サーバの名前が SVM ホスト名と異なる場合は、CIFS サーバの名前を入力します。

5. [OK] をクリックします。
6. コンソールツリーで、\* システムツール \* > \* 共有フォルダー \* をクリックします。
7. [\* 共有] をクリックします。
8. 結果ペインで、共有を右クリックします。
9. \* プロパティ \* をクリックします。

選択した共有のプロパティが表示されます。

10. [一般\*] タブで、[\* オフライン設定\*] をクリックします。

[オフライン設定] ダイアログボックスが表示されます。

11. 必要に応じて、オフラインの可用性オプションを設定します。
12. [OK] をクリックします。

移動プロファイルを使用すると、**SVM** に関連付けられた **SMB** サーバにユーザプロファイルを一元的に格納できます

移動プロファイルを使用すると、**SVM** の概要に関連付けられた **SMB** サーバにユーザプロファイルを一元的に格納できます

ONTAP では、Windows の移動プロファイルの格納をサポートしており、それらを Storage Virtual Machine (SVM) に関連付けられた CIFS サーバに格納することができます。ユーザ移動プロファイルを設定すると、ユーザはログイン先に関係なく自動でリソースを利用できるようになります。また、移動プロファイルを使用すると、ユーザプロファイルの管理と管理が簡単になります。

移動ユーザプロファイルには、次のような利点があります。

- 自動でリソースを利用できる

Windows 8、Windows 7、Windows 2000、または Windows XP を実行しているコンピュータであれば、ネットワーク上のどのコンピュータにログインしても、各ユーザの一意のプロファイルを自動的に利用できます。ネットワーク上で使用するコンピュータごとにプロファイルを作成する必要はありません。

- コンピュータの交換が簡単

ユーザのプロファイル情報はすべてネットワークに別途保存されるため、交換後の新しいコンピュータにユーザのプロファイルを簡単にダウンロードできます。ユーザが新しいコンピュータに初めてログインしたときに、サーバに保存されているユーザのプロファイルが新しいコンピュータにコピーされます。

## 関連情報

[オフラインファイルを使用したオフラインで使用するファイルのキャッシュ](#)

[フォルダリダイレクトを使用した CIFS サーバへのデータの格納](#)



CIFS サーバで Microsoft の移動プロファイルを使用する前に、この機能をサポートする ONTAP および SMB のバージョンと Windows クライアントの種類について確認しておく必要があります。

### ONTAP のバージョンの要件

ONTAP では移動プロファイルをサポートしています

### SMB プロトコルのバージョン

Storage Virtual Machine (SVM ONTAP) については、すべてのバージョンの SMB で移動プロファイルがサポートされます。

### Windows クライアントの要件

移動プロファイルを使用するには、Windows クライアントでこの機能がサポートされている必要があります。

移動プロファイルをサポートする Windows クライアントに関する最新情報については、Interoperability Matrix を参照してください。

["NetApp Interoperability Matrix Tool で確認できます"](#)

移動プロファイルを設定する

ネットワーク上の任意のコンピュータにユーザがログオンするときに、そのユーザのプロファイルを自動的に使用できるようにするには、Active Directory ユーザとコンピュータ MMC スナップインを使用して移動プロファイルを設定します。Windows Serverで移動プロファイルを設定する場合は、Active Directory管理センターを使用できます。

### 手順

1. Windowsサーバーで、Active DirectoryユーザーとコンピュータMMC（またはWindowsサーバーのActive Directory管理センター）を開きます。
2. 移動プロファイルを設定するユーザを見つけます。
3. ユーザーを右クリックし、\* プロパティ \* をクリックします。
4. [プロファイル]\*タブで、ユーザの移動プロファイルを保存する共有のプロファイルパスを入力し、続けてを入力します %username%。

たとえば、プロファイルパスは次のようになります。

\\vs1.example.com\profiles\%username%。ユーザが初めてログインしたとき、%username% がユーザの名前に置き換えられます。



パス内 \\vs1.example.com\profiles\%username%、profiles は、すべてのメンバーにフルコントロール権限があるStorage Virtual Machine (SVM) vs1上の共有の共有名です。

5. [OK] をクリックします。

フォルダリダイレクトを使用して、**SMB** サーバにデータを格納します

フォルダリダイレクトを使用して、**SMB** サーバの概要にデータを格納します

ONTAP では、Microsoft のフォルダリダイレクトをサポートしています。ユーザや管理者は、この機能を使用して、ローカルフォルダのパスを CIFS サーバの場所にリダイレクトできます。リダイレクトされたフォルダは、データが SMB 共有に格納されていても、ローカルの Windows クライアントに格納されたフォルダのように扱うことができます。

フォルダリダイレクトは、主に、ホームディレクトリをすでに導入しており、既存のホームディレクトリ環境との互換性を維持したい組織を対象としています。

- Documents、Desktop、および Start Menu は、リダイレクト可能なフォルダの例です。
- ユーザは、各自の Windows クライアントからフォルダをリダイレクトできます。
- 管理者は、Active Directory で GPO を設定することで、フォルダリダイレクトを一元的に設定および管理できます。
- 移動プロファイルを設定している場合は、管理者がユーザデータとプロファイルデータを分けることができます。
- 管理者は、フォルダリダイレクトとオフラインファイルを使用して、ローカルフォルダのデータストレージを CIFS サーバにリダイレクトし、ユーザはコンテンツをローカルにキャッシュできます。

## 関連情報

[オフラインファイルを使用したオフラインで使用するファイルのキャッシュ](#)

[移動プロファイルを使用した SVM に関連付けられた CIFS サーバへのユーザプロファイルの一元的な格納](#)

フォルダリダイレクトを使用するための要件

CIFS サーバで Microsoft のフォルダリダイレクトを使用する前に、この機能をサポートする ONTAP および SMB のバージョンと Windows クライアントの種類について確認しておく必要があります。

## ONTAP のバージョンの要件

ONTAP は、Microsoft のフォルダリダイレクトをサポートしています

## SMB プロトコルのバージョン

Storage Virtual Machine (SVM) については、ONTAP のすべてのバージョンの SMB で Microsoft のフォルダリダイレクトがサポートされます。

## Windows クライアントの要件

Microsoft のフォルダリダイレクトを使用するには、Windows クライアントでこの機能がサポートされている必要があります。

フォルダリダイレクトをサポートする Windows クライアントに関する最新情報については、Interoperability Matrix を参照してください。

フォルダリダイレクトを設定します

Windows の [ プロパティ ] ウィンドウを使用して、フォルダリダイレクトを設定できます。この方法を使用する利点は、Windows ユーザが SVM 管理者のサポートがなくてもフォルダリダイレクトを設定できることです。

手順

1. エクスプローラで、ネットワーク共有にリダイレクトするフォルダを右クリックします。
2. \* プロパティ \* をクリックします。

選択した共有のプロパティが表示されます。

3. [\* ショートカット \*] タブで、[\* ターゲット \*] をクリックし、選択したフォルダーをリダイレクトするネットワーク上の場所へのパスを指定します。

たとえば、フォルダをにリダイレクトする場合などです data にマッピングされているホームディレクトリ内のフォルダ Q:\、を指定します Q:\data ターゲットとして。

4. [OK] をクリックします。

オフラインフォルダの設定の詳細については、Microsoft TechNet ライブラリを参照してください。

関連情報

["Microsoft TechNet ライブラリ : technet.microsoft.com/en-us/library/"](https://technet.microsoft.com/en-us/library/)

**SMB 2.x** を使用する **Windows** クライアントから **~snapshot** ディレクトリにアクセスします

へのアクセスに使用する方法 ~snapshot SMB 2.xを使用するWindowsクライアントのディレクトリは、SMB 1.0の場合とは異なります。にアクセスする方法を理解しておく必要があります ~snapshot SMB 2.x接続を使用してSnapshotコピーに格納されたデータに正常にアクセスする場合のディレクトリ。

SVM管理者は、Windowsクライアントのユーザがに表示およびアクセスできるかどうかを制御します ~snapshot 共有上のディレクトリを有効または無効にします showsnapshot vserver cifs share properties familiesコマンドを使用した共有プロパティ。

をクリックします showsnapshot 共有プロパティが無効になっているため、SMB 2.xを使用するWindowsクライアントのユーザはを表示できません ~snapshot ディレクトリにあり、内のSnapshotコピーにはアクセスできません ~snapshot ディレクトリ（へのパスを手動で入力した場合も含む） ~snapshot またはディレクトリ内の特定のSnapshotコピーにコピーします。

をクリックします showsnapshot 共有プロパティが有効になっています。SMB 2.xを使用するWindowsクライアントのユーザは引き続きを表示できません ~snapshot 共有のルート、または共有のルートより下のジャンクションまたはディレクトリ内のディレクトリ。ただし、共有に接続したユーザは非表示のにアクセスできます ~snapshot ディレクトリを手動で追加します \~snapshot 共有パスの末尾に移動します。隠れた者だ ~snapshot ディレクトリには、次の2つのエントリポイントからアクセスできます。

- を共有のルートに追加します
- を共有スペースのすべてのジャンクションポイントでクリックします

隠れた者だ ~snapshot 共有内のジャンクション以外のサブディレクトリからディレクトリにアクセスすることはできません。

例

次の例に示す設定では、「eng」共有へのSMB 2.x接続を使用するWindowsクライアントのユーザがにアクセスできます ~snapshot ディレクトリを手動で追加します ~snapshot を共有パス（共有のルート、およびパス内のすべてのジャンクションポイント）に設定します。隠れた者だ ~snapshot ディレクトリには、次の3つのパスからアクセスできます。

- \\vs1\eng\~snapshot
- \\vs1\eng\projects1\~snapshot
- \\vs1\eng\projects2\~snapshot

```
cluster1::> volume show -vserver vs1 -fields volume,junction-path
vserver volume          junction-path
-----
vs1      vs1_root        /
vs1      vs1_vol1        /eng
vs1      vs1_vol2        /eng/projects1
vs1      vs1_vol3        /eng/projects2

cluster1::> vsserver cifs share show
Vserver  Share  Path    Properties      Comment  ACL
-----
vs1      eng    /eng    oplocks         -        Everyone / Full Control
          changenotify
          browsable
          showsnapshot
```

以前のバージョン機能を使用してファイルとフォルダをリカバリする

以前のバージョン機能の概要を使用したファイルとフォルダのリカバリ

Microsoft の以前のバージョン機能は、Snapshot コピーを何らかの形でサポートしているファイルシステムで、それらが有効になっている場合に使用できます。Snapshot テクノロジは ONTAP に不可欠なテクノロジーの 1 つです。ユーザは、Windows クライアントで Microsoft の以前のバージョン機能を使用して、Snapshot コピーからファイルとフォルダをリカバリできます。

以前のバージョン機能を使用すると、ストレージ管理者の手を借りなくても、一連の Snapshot コピーを参照したり、Snapshot コピーからデータをリストアしたりできます。以前のバージョン機能は設定できません。常に有効になります。ストレージ管理者が Snapshot コピーを共有でできるようにした場合、ユーザは以前のバージョン機能を使用して次の作業を実行できます。

- 誤って削除したファイルをリカバリする。
- 誤って上書きしたファイルをリカバリする。
- 作業中にファイルのバージョンを比較します。

Snapshot コピーに格納されているデータは読み取り専用です。ファイルに変更を加えるには、ファイルのコピーを別の場所に保存する必要があります。Snapshot コピーは定期的に削除されるため、以前のバージョンのファイルを残しておく場合は、以前のバージョン機能で格納されたファイルのコピーを作成しておく必要があります。

**Microsoft** の以前のバージョン機能を使用するための要件

CIFS サーバで Microsoft の以前のバージョン機能を使用する前に、この機能をサポートする ONTAP および SMB のバージョンと Windows クライアントの種類について確認しておく必要があります。また、Snapshot コピーの設定の要件についても確認しておく必要があります。

### **ONTAP** のバージョンの要件

は、以前のバージョンをサポートします

### **SMB** プロトコルのバージョン

Storage Virtual Machine （SVM ONTAP）については、すべてのバージョンの SMB で以前のバージョン機能がサポートされます。

### **Windows** クライアントの要件

ユーザが以前のバージョン機能を使用して Snapshot コピー内のデータにアクセスするには、Windows クライアントでこの機能がサポートされている必要があります。

以前のバージョンをサポートする Windows クライアントに関する最新情報については、Interoperability Matrix を参照してください。

["NetApp Interoperability Matrix Tool で確認できます"](#)

### **Snapshot** コピーの設定の要件

以前のバージョン機能を使用して Snapshot コピー内のデータにアクセスするには、有効な Snapshot ポリシーがデータを含むボリュームに関連付けられ、クライアントが Snapshot データにアクセスできるようになっていて、Snapshot コピーが存在している必要があります。

**Snapshot** コピーのデータを表示および管理するには、イゼンノバージョンタブを使用します

Windows クライアントマシンのユーザは、Windows のプロパティウィンドウの以前のバージョンタブを使用して、Storage Virtual Machine （SVM）管理者を介さずに Snapshot コピーに格納されたデータをリストアできます。

このタスクについて

管理者が共有を含むボリュームで Snapshot コピーを有効にしている場合、および管理者が Snapshot コピー

を表示するように共有を設定している場合は、以前のバージョンタブで SVM に格納されているデータの Snapshot コピーのデータを表示および管理することしかできません。

#### 手順

1. エクスプローラで、CIFS サーバに格納されたデータのマッピングされたドライブの内容を表示します。
2. Snapshot コピーを表示または管理するマッピングされたネットワークドライブのファイルまたはフォルダを右クリックします。
3. \* プロパティ \* をクリックします。

選択したファイルまたはフォルダのプロパティが表示されます。

4. [ 以前のバージョン \* ] タブをクリックします。

選択したファイルまたはフォルダの使用可能な Snapshot コピーのリストが [ フォルダバージョン : ] ボックスに表示されます。表示された Snapshot コピーは、Snapshot コピー名のプレフィックスと作成時のタイムスタンプで識別できます。

5. [ \* フォルダーバージョン : \* ] ボックスで、管理するファイルまたはフォルダーのコピーを右クリックします。
6. 適切な操作を実行します。

状況	実行する処理
Snapshot コピーのデータを表示します	• 開く * をクリックします。
Snapshot コピーからデータのコピーを作成します	[ * コピー ( Copy ) ] をクリックします

Snapshot コピーのデータは読み取り専用です。[ 以前のバージョン ] タブにリストされているファイルやフォルダを変更する場合は、変更するファイルやフォルダのコピーを書き込み可能な場所に保存し、コピーを変更する必要があります。

7. スナップショット・データの管理が終了したら **OK** をクリックして \* プロパティ \* ダイアログ・ボックスを閉じます

以前のバージョンタブを使用して Snapshot データを表示および管理する方法の詳細については、Microsoft TechNet ライブラリを参照してください。

#### 関連情報

"Microsoft TechNet ライブラリ : [technet.microsoft.com/en-us/library/](http://technet.microsoft.com/en-us/library/)"

**Snapshot** コピーが以前のバージョン機能で使えるかどうかを確認します

有効な Snapshot ポリシーが共有を含むボリュームに適用されていて、ボリューム設定で Snapshot コピーへのアクセスが許可されている場合にのみ、以前のバージョンタブで Snapshot コピーを表示できます。Snapshot コピーの使用可否を確認すると、以前のバージョン機能を使用してアクセス可能かどうか確認できます。

#### 手順

1. 共有データが存在するボリュームで自動Snapshotコピーが有効になっているかどうか、およびクライアントがSnapshotディレクトリにアクセスできるかどうかを確認します。`volume show -vserver vserver-name -volume volume-name -fields vserver,volume,snapdir-access,snapshot-policy,snapshot-count`

出力には、ボリュームに関連付けられている Snapshot ポリシー、クライアントの Snapshot ディレクトリアクセスが有効かどうか、および使用可能な Snapshot コピーの数が表示されます。

2. 関連付けられているSnapshotポリシーが有効になっているかどうかを確認します。`volume snapshot policy show -policy policy-name`
3. 使用可能なSnapshotコピーの一覧を表示します。`volume snapshot show -volume volume_name`

Snapshot ポリシーおよび Snapshot スケジュールの設定と管理の詳細については、を参照してください "[データ保護](#)"。

#### 例

次の例は、「data」上の共有データと使用可能な Snapshot コピーを含む「data」という名前のボリュームに関連付けられている Snapshot ポリシーに関する情報を表示します。

```
cluster1::> volume show -vserver vs1 -volume data1 -fields
vserver,volume,snapshot-policy,snapdir-access,snapshot-count
vserver  volume snapdir-access snapshot-policy snapshot-count
-----
vs1      data1  true                default                10

cluster1::> volume snapshot policy show -policy default
Vserver: cluster1

Number of Is
Policy Name    Schedules Enabled Comment
-----
default        3 true    Default policy with hourly, daily &
weekly schedules.

Schedule      Count    Prefix    SnapMirror Label
-----
hourly         6    hourly    -
daily          2    daily      daily
weekly         2    weekly     weekly

cluster1::> volume snapshot show -volume data1

Vserver  Volume  Snapshot                                State    Size  Total%  Used%
-----
vs1      data1

weekly.2012-12-16_0015    valid    408KB    0%    1%
daily.2012-12-22_0010    valid    420KB    0%    1%
daily.2012-12-23_0010    valid    192KB    0%    0%
weekly.2012-12-23_0015    valid    360KB    0%    1%
hourly.2012-12-23_1405    valid    196KB    0%    0%
hourly.2012-12-23_1505    valid    196KB    0%    0%
hourly.2012-12-23_1605    valid    212KB    0%    0%
hourly.2012-12-23_1705    valid    136KB    0%    0%
hourly.2012-12-23_1805    valid    200KB    0%    0%
hourly.2012-12-23_1905    valid    184KB    0%    0%
```

## 関連情報

[以前のバージョン機能のアクセスを有効にする Snapshot 設定の作成](#)

## "データ保護"

以前のバージョン機能のアクセスを有効にする **Snapshot** 設定を作成します

Snapshot コピーへのクライアントアクセスが有効で、Snapshot コピーが存在する場合は、常に以前のバージョン機能を使用できます。Snapshot コピーの設定がこれらの要件を満たしていない場合は、要件を満たすように Snapshot コピーの設定を作成できます



す。

#### 手順

1. [以前のバージョン機能]からのアクセスを許可する共有が含まれているボリュームにSnapshotポリシーが関連付けられていない場合は、を使用してSnapshotポリシーをボリュームに関連付けて有効にします  
`volume modify` コマンドを実行します

を使用する方法の詳細については、を参照してください `volume modify` コマンドについては、マニュアルページを参照してください。

2. を使用して、Snapshotコピーへのアクセスを有効にします `volume modify` コマンドを使用してを設定します `-snap-dir` オプションをに設定します `true`。

を使用する方法の詳細については、を参照してください `volume modify` コマンドについては、マニュアルページを参照してください。

3. を使用して、Snapshotポリシーが有効になっていること、およびSnapshotディレクトリへのアクセスが有効になっていることを確認します `volume show` および `volume snapshot policy show` コマンド

を使用する方法の詳細については、を参照してください `volume show` および `volume snapshot policy show` コマンドについては、マニュアルページを参照してください。

Snapshot ポリシーおよび Snapshot スケジュールの設定と管理の詳細については、を参照してください "[データ保護](#)"。

#### 関連情報

["データ保護"](#)

ジャンクションを含むディレクトリのリストアに関するガイドライン

以前のバージョンを使用してジャンクションポイントを含むフォルダをリストアする場合は、一定のガイドラインに注意する必要があります。

以前のバージョンを使用して、ジャンクションポイントである子フォルダを含むフォルダをリストアすると、が表示されてリストアに失敗することがあります Access Denied エラー。

リストアしようとしているフォルダにジャンクションが含まれているかどうかは、を使用して確認できます `vol show` コマンドにを指定します `-parent` オプションを使用することもできます `vserver security trace` ファイルおよびフォルダのアクセス問題に関する詳細なログを作成するコマンド。

#### 関連情報

[NAS ネームスペース内でのデータボリュームの作成と管理](#)

## SMB サーバベースのサービスを導入

ホームディレクトリを管理します

ONTAP で動的ホームディレクトリを有効にする方法

ONTAP ホームディレクトリを使用すると、SMB 共有を設定し、ユーザと一連の変数に

基づいてさまざまなディレクトリにマッピングすることができます。ユーザごとに別個の共有を作成するのではなく、1つの共有を設定し、いくつかのホームディレクトリパラメータを指定して、エントリポイント（共有）とホームディレクトリ（SVM上のディレクトリ）間の関係をユーザ単位で定義します。

ゲストユーザとしてログインしたユーザは、ホームディレクトリを持ちません。また、他のユーザのホームディレクトリにアクセスすることはできません。ユーザとディレクトリのマッピング方法を決定する4つの変数があります。

#### • \* 共有名 \*

ユーザの接続先として作成する共有の名前です。この共有にはホームディレクトリのプロパティを設定する必要があります。

共有名には、次の動的な名前を使用できます。

- %w （ユーザのWindowsユーザ名）
  - %d （ユーザのWindowsドメイン名）
  - %u （ユーザのマッピングされたUNIXユーザ名）
- すべてのホームディレクトリ間で共有名を一意にするには、共有名に/%w または %u 変数（Variable）：共有名には両方を使用できます %d および/%w 変数（例： %d/%w` または、共有名に静的な部分と変数の部分（home\_ など）を含めることができます /%w`）。

#### • \* 共有パス \*

共有によって定義される、つまり、共有名の1つに関連付けられる相対パスです。各検索パスに付加されて、SVMのルートからのユーザのホームディレクトリの完全パスを生成します。静的（例：home）、動的（例：%w）、または2つの組み合わせ（例：eng/%w）。

#### • \* 検索パス \*

SVMのルートからの絶対パスのセットで、ONTAPではこのパスに基づいてホームディレクトリが検索されます。を使用して、1つ以上の検索パスを指定できます `vserver cifs home-directory search-path add` コマンドを実行します複数ONTAPの検索パスを指定すると、有効なパスが見つかるまで、指定された順に各検索パスが試行されます。

#### • \* ディレクトリ \*

ユーザに対して作成する、そのユーザのホームディレクトリです。通常、ディレクトリ名はユーザの名前です。ホームディレクトリは、検索パスで定義されるいずれかのディレクトリに作成する必要があります。

たとえば、次のように設定します。

- ユーザ： John Smith
- ユーザのドメイン： acme
- ユーザ名： jsmith
- SVM名： vs1
- ホームディレクトリ共有名#1：home\_ %w -共有パス： %w

- ホームディレクトリ共有名#2: %w-共有パス: %d/%w
- 検索パス#1: /vol0home/home
- 検索パス#2: /vol1home/home
- 検索パス#3: /vol2home/home
- ホームディレクトリ: /vol1home/home/jsmith

シナリオ1: ユーザーがに接続します \\vs1\home\_jsmith。これは最初のホームディレクトリ共有名に一致し、相対パスが生成されます jsmith。ONTAP がというディレクトリを検索するようになりました jsmith 各検索パスを順にチェックするには、次の手順に従います。

- /vol0home/home/jsmith は存在しません。検索パス#2に進みます。
- /vol1home/home/jsmith は存在します。したがって、検索パス#3はチェックされません。これで、ユーザは自分のホームディレクトリに接続されました。

シナリオ2: ユーザーがに接続する \\vs1\jsmith。これは2番目のホームディレクトリ共有名に一致し、相対パスが生成されます acme/jsmith。ONTAP がというディレクトリを検索するようになりました acme/jsmith 各検索パスを順にチェックするには、次の手順に従います。

- /vol0home/home/acme/jsmith は存在しません。検索パス#2に進みます。
- /vol1home/home/acme/jsmith は存在しません。検索パス#3に進みます。
- /vol2home/home/acme/jsmith は存在しません。ホームディレクトリが存在しないため、接続は失敗します。

ホームディレクトリ共有

ホームディレクトリ共有を追加します

SMB ホームディレクトリ機能を使用する場合、共有プロパティにホームディレクトリプロパティを含む共有を少なくとも 1 つ追加する必要があります。

このタスクについて

ホームディレクトリ共有は、共有の作成時にを使用して作成できます vserver cifs share create コマンドを入力するか、を使用して、既存の共有をいつでもホームディレクトリ共有に変更できます vserver cifs share modify コマンドを実行します

ホームディレクトリ共有を作成するには、を含める必要があります homedirectory の値 -share -properties オプションは、共有を作成または変更するときに使用します。共有名と共有パスは変数を使用して指定できます。変数はユーザがそれぞれのホームディレクトリに接続するときに動的に変換されます。パスで使用できる変数はです %w、`%d`および `%u` Windows ユーザ名、ドメイン、マッピングされたUNIX ユーザ名にそれぞれ対応します。

手順

1. ホームディレクトリ共有を追加: +

```
vserver cifs share create -vserver vs1 -share-name share_name -path path -share-properties homedirectory[,...]
```

-vserver vs1 検索パスを追加するCIFS対応のStorage Virtual Machine (SVM) を指定します。

`-share-name share-name` ホームディレクトリ共有名を指定します。

共有名にリテラル文字列が含まれている場合は、必須の変数の1つに加えて、必要な変数も含まれています `%w`、`%u` または ``%d`ONTAP` がリテラル文字列を変数として処理しないようにするには、リテラル文字列の前に`%`（パーセント）文字を付ける必要があります（例： ``%%w`）。

- 共有名にはどちらかを使用する必要があります `%w` または `%u` 変数（Variable）：
- 共有名にはさらにを含めることができます `%d` 変数（例： `%d/%w`）または共有名の静的な部分（例：  
：`home1_/%w`）。
- 管理者が、他のユーザのホームディレクトリに接続するために、またはユーザが他のユーザのホームディレクトリに接続するのを許可するために共有を使用する場合は、動的な共有名のパターンの先頭にチルダ（`~`）を付ける必要があります。

◦ `vserver cifs home-directory modify` は、を設定してこのアクセスを有効にする場合に使用します `-is-home-dirs-access-for-admin-enabled` オプションをに設定します `true`) または `advanced` オプションを設定します `-is-home-dirs-access-for-public-enabled` 終了：  
`true`。

`-path path` ホームディレクトリの相対パスを指定します。

`-share-properties homedirectory[,...]` その共有の共有プロパティを指定します。を指定する必要があります `homedirectory` 価値。追加の共有プロパティをカンマで区切って指定できます。

1. を使用して、ホームディレクトリ共有が追加されたことを確認します `vserver cifs share show` コマンドを実行します

例

次のコマンドは、という名前のホームディレクトリ共有を作成します `%w`。 `oplocks`、`browsable` および `changenotify` 共有プロパティは、に加えて設定します `homedirectory` 共有プロパティ。



この例で表示されているのは、SVM の共有の出力の一部です。出力は省略されています。

```
cluster1::> vserver cifs share create -vserver vs1 -share-name %w -path %w
-share-properties oplocks,browsable,changenotify,homedirectory
```

```
vs1::> vserver cifs share show -vserver vs1
```

Vserver	Share	Path	Properties	Comment	ACL
vs1	%w	%w	oplocks	-	Everyone / Full
Control			browsable		
			changenotify		
			homedirectory		

関連情報

[ホームディレクトリ検索パスを追加しています](#)

## 自動ノードリファラルの使用に関する要件とガイドライン

### ユーザのホームディレクトリへのアクセスの管理

ホームディレクトリ共有には、一意なユーザ名が必要です

を使用してホームディレクトリ共有を作成する場合は、一意のユーザ名を割り当てるように注意してください `%w` (Windows ユーザ名) または `%u` (UNIX ユーザ名) 変数。共有を動的に生成します。共有名はユーザ名にマッピングされます。

静的共有の名前とユーザの名前が同じ場合、次の 2 つの問題が発生する可能性があります。

- ユーザがを使用してクラスタ上の共有のリストを表示したとき `net view` コマンドを実行すると、同じユーザ名を持つ 2 つの共有が表示されます。
- ユーザがその共有名に接続すると、常に静的共有に接続され、同じ名前のホームディレクトリ共有にはアクセスできません。

たとえば、「`administrator`」という名前の共有があり、「`administrator`」という名前の Windows ユーザ名が割り当てられているとします。ホーム・ディレクトリ共有を作成し、その共有に接続すると、「管理者」のホーム・ディレクトリ共有ではなく、「管理者」の静的共有に接続されます。

共有名が重複している問題を解決するには、次のいずれかの手順を実行します。

- 静的共有の名前を変更し、ユーザのホームディレクトリ共有と競合しないようにします。
- ユーザに新しいユーザ名を割り当てて、静的共有名と競合しないようにします。
- を使用する代わりに、「`home`」などの静的な名前を使用して CIFS ホームディレクトリ共有を作成します `%w` 共有名との競合を回避するためのパラメータ。

### アップグレード後に静的ホームディレクトリ共有名が受ける影響

ホームディレクトリ共有名にはのどちらかが含まれている必要があります `%w` または `%u` 動的変数。新しい要件がある ONTAP のバージョンにアップグレードしたあとに、既存の静的ホームディレクトリ共有名が受ける影響について理解しておく必要があります。

ホームディレクトリの設定に静的共有名が含まれている場合に ONTAP にアップグレードしても、静的ホームディレクトリ共有名は変更されず、共有も有効なままです。ただし、どちらも含まない新しいホームディレクトリ共有を作成することはできません `%w` または `%u` 変数 (Variable) :

ユーザのホームディレクトリ共有名にどちらかの変数を含めるという必須条件によって、すべての共有名がホームディレクトリ設定全体で一意であることが保証されます。必要に応じて、静的ホームディレクトリ共有名を、どちらかを含む名前に変更できます `%w` または `%u` 変数 (Variable) :

ホームディレクトリ検索パスを追加します

ONTAP の SMB ホームディレクトリを使用する場合は、ホームディレクトリ検索パスを少なくとも 1 つ追加する必要があります。

このタスクについて

を使用して、ホームディレクトリ検索パスを追加できます `vserver cifs home-directory search-`

path add コマンドを実行します

。vserver cifs home-directory search-path add コマンドはで指定されたパスをチェックします -path オプション（コマンド実行時）。指定したパスが存在しない場合は、続行するかどうかを確認するメッセージが表示されます。お前が選べ y または n。をクリックします y 続行するには、ONTAP が検索パスを作成します。ただし、ホームディレクトリ設定で検索パスを使用するには、あらかじめディレクトリ構造を作成しておく必要があります。続行しない場合、コマンドは失敗し、検索パスは作成されません。その後、パスディレクトリ構造を作成し、を再実行できます vs1 cifs home-directory search-path add コマンドを実行します

#### 手順

1. ホームディレクトリ検索パスを追加します。vserver cifs home-directory search-path add -vserver vs1 -path /home1
2. を使用して、検索パスが正常に追加されたことを確認します vs1 cifs home-directory search-path show コマンドを実行します

#### 例

次の例は、パスを追加します /home1 SVM vs1のホームディレクトリ設定に移動します。

```
cluster::> vs1 cifs home-directory search-path add -vserver vs1 -path /home1

vs1::> vs1 cifs home-directory search-path show
Vserver      Position Path
-----
vs1          1      /home1
```

次の例は、パスの追加を試みます /home2 SVM vs1のホームディレクトリ設定に移動します。パスが存在しません。続行しないように選択します。

```
cluster::> vs1 cifs home-directory search-path add -vserver vs1 -path /home2
Warning: The specified path "/home2" does not exist in the namespace
        belonging to Vserver "vs1".
Do you want to continue? {y|n}: n
```

#### 関連情報

##### ホームディレクトリ共有の追加

%w 変数と %d 変数を使用して、ホームディレクトリの設定を作成します

を使用して、ホームディレクトリ設定を作成できます %w および %d 変数。ユーザは、動的に作成された共有を使用してホームディレクトリ共有に接続できます。

#### 手順

1. ユーザのホームディレクトリを含むqtreeを作成します。 `volume qtree create -vserver vserver_name -qtree-path qtree_path`
2. qtreeで正しいセキュリティ形式が使用されていることを確認します。 `volume qtree show`
3. 適切なセキュリティ形式がqtreeで使用されていない場合は、を使用してセキュリティ形式を変更します `volume qtree security` コマンドを実行します
4. ホームディレクトリ共有を追加します。 `vserver cifs share create -vserver vserver -share-name %w -path %d/%w -share-properties homedirectory\[,...\]`  
  
`-vserver vserver` 検索パスを追加するCIFS対応のStorage Virtual Machine (SVM) を指定します。  
  
`-share-name %w` ホームディレクトリ共有名を指定します。ユーザがホームディレクトリに接続すると、ONTAP によって共有名が動的に作成されます。共有名の形式は `_windows_user_name` です。  
  
`-path %d/%w` ホームディレクトリの相対パスを指定します。ユーザがホームディレクトリに接続すると、ユーザごとに `_domain/windows_user_name` の形式で相対パスが動的に作成されます。  
  
`-share-properties homedirectory\[,...\]` その共有の共有プロパティを指定します。を指定する必要があります `homedirectory` 価値。追加の共有プロパティをカンマで区切って指定できます。
5. を使用して、共有が目的の設定になっていることを確認します `vserver cifs share show` コマンドを実行します
6. ホームディレクトリ検索パスを追加します。 `vserver cifs home-directory search-path add -vserver vserver -path path`  
  
`-vserver vserver-name` 検索パスを追加するCIFS対応のSVMを指定します。  
  
`-path path` 検索パスの絶対ディレクトリパスを指定します。
7. を使用して、検索パスが正常に追加されたことを確認します `vserver cifs home-directory search-path show` コマンドを実行します
8. ユーザにホームディレクトリがある場合は、ホームディレクトリを含むように指定した qtree またはボリュームに対応するディレクトリを作成します。  
  
たとえば、パスがqtreeを作成したとします `/vol/vol1/users` ディレクトリを作成するユーザ名は `mydomain\user1` で、次のパスでディレクトリを作成します。  
`/vol/vol1/users/mydomain/user1`。  
  
にマウントされた「home1」という名前のボリュームを作成した場合 `/home1`` では、次のパスでディレクトリを作成します。 ``/home1/mydomain/user1`。
9. ドライブをマッピングするか、UNC パスを使用して、ユーザがホームディレクトリ共有に正常に接続できることを確認します。  
  
たとえば、ユーザ `mydomain\user1` が、SVM `vs1` 上にあるディレクトリ（手順8で作成）に接続する場合は、UNCパスを使用して接続します `\\vs1\user1`。

#### 例

次の例のコマンドでは、次の設定を使用してホームディレクトリを設定を作成します。

- 共有名は %w です
- 相対ホームディレクトリパスは %d/%w です
- ホームディレクトリを含むために使用される検索パス /home1、は、NTFSセキュリティ形式で設定されているボリュームです。
- 設定は SVM vs1 上に作成されます。

ユーザが Windows ホストからホームディレクトリにアクセスする場合には、このようなホームディレクトリ設定を使用できます。また、ユーザが Windows ホストと UNIX ホストからホームディレクトリにアクセスし、ファイルシステム管理者が Windows ベースのユーザおよびグループを使用してファイルシステムへのアクセスを制御する場合にも、このような設定を使用できます。

```
cluster::> vsriver cifs share create -vsriver vs1 -share-name %w -path
%d/%w -share-properties oplocks,browsable,changesotify,homedirectory

cluster::> vsriver cifs share show -vsriver vs1 -share-name %w

                Vserver: vs1
                Share: %w
CIFS Server NetBIOS Name: VS1
                Path: %d/%w
                Share Properties: oplocks
                                browsable
                                changesotify
                                homedirectory
                Symlink Properties: enable
                File Mode Creation Mask: -
                Directory Mode Creation Mask: -
                Share Comment: -
                Share ACL: Everyone / Full Control
File Attribute Cache Lifetime: -
                Volume Name: -
                Offline Files: manual
Vscan File-Operations Profile: standard

cluster::> vsriver cifs home-directory search-path add -vsriver vs1 -path
/home1

cluster::> vsriver cifs home-directory search-path show
Vserver      Position Path
-----
vs1          1        /home1
```

## 関連情報

[%u 変数を使用してホームディレクトリを設定します](#)



## 追加のホームディレクトリの設定

### SMB ユーザのホームディレクトリパスに関する情報を表示する

%u 変数を使用してホームディレクトリを設定します

を使用して、ホームディレクトリの設定を作成し、共有名を指定できます %w 変数ですが、を使用します %u ホームディレクトリ共有の相対パスを指定する変数。これにより、ユーザは、ホームディレクトリの実際の名前やパスを意識することなく、Windows ユーザ名を使用して動的に作成された共有を使用してホームディレクトリ共有に接続できます。

#### 手順

1. ユーザのホームディレクトリを含むqtreeを作成します。 `volume qtree create -vserver vsver_name -qtree-path qtree_path`
2. qtreeで正しいセキュリティ形式が使用されていることを確認します。 `volume qtree show`
3. 適切なセキュリティ形式がqtreeで使用されていない場合は、を使用してセキュリティ形式を変更します `volume qtree security` コマンドを実行します
4. ホームディレクトリ共有を追加します。 `vserver cifs share create -vserver vsver_name -share-name %w -path %u -share-properties homedirectory ,...]`

-vserver vsver\_name 検索パスを追加するCIFS対応のStorage Virtual Machine (SVM) を指定します。

-share-name %w ホームディレクトリ共有名を指定します。ユーザがホームディレクトリに接続すると、ユーザごとに \_windows\_user\_name の形式で共有名が動的に作成されます。



を使用することもできます %u の変数 -share-name オプションこれにより、マッピング先の UNIX ユーザ名を使用して相対共有パスが作成されます。

-path %u ホームディレクトリの相対パスを指定します。ユーザがホームディレクトリに接続すると、ユーザごとに \_mapped\_UNIX\_user\_name の形式で共有名が動的に作成されます。



このオプションの値には静的な要素も含めることができます。例： eng/%u。

-share-properties homedirectory\[,...\] その共有の共有プロパティを指定します。を指定する必要があります homedirectory 価値。追加の共有プロパティをカンマで区切って指定できます。

5. を使用して、共有が目的の設定になっていることを確認します `vserver cifs share show` コマンドを実行します
6. ホームディレクトリ検索パスを追加します。 `vserver cifs home-directory search-path add -vserver vsver_name -path path`

-vserver vsver\_name 検索パスを追加するCIFS対応のSVMを指定します。

-path path 検索パスの絶対ディレクトリパスを指定します。

7. を使用して、検索パスが正常に追加されたことを確認します `vserver cifs home-directory`

search-path show コマンドを実行します

8. UNIXユーザが存在しない場合は、を使用してUNIXユーザを作成します vserver services unix-user create コマンドを実行します



ユーザをマッピングするには、Windows ユーザ名のマッピング先となる UNIX ユーザ名があらかじめ存在している必要があります。

9. 次のコマンドを使用して、UNIXユーザへのWindowsユーザのネームマッピングを作成します。 vserver name-mapping create -vserver vserver\_name -direction win-unix -priority integer -pattern windows\_user\_name -replacement unix\_user\_name



Windows ユーザを UNIX ユーザにマッピングするネームマッピングがすでに存在する場合は、このマッピング手順を実行する必要はありません。

Windows ユーザ名は対応する UNIX ユーザ名にマッピングされます。Windows ユーザは、ホームディレクトリ共有に接続すると、Windows ユーザ名に対応する共有名を使用して動的に作成されたホームディレクトリに接続することになります。その際、ディレクトリ名が UNIX ユーザ名に対応していることはユーザにはわかりません。

10. ユーザにホームディレクトリがある場合は、ホームディレクトリを含むように指定した qtree またはボリュームに対応するディレクトリを作成します。

たとえば、パスがのqtreeを作成したとします /vol/vol1/users ディレクトリを作成するユーザのマッピングされたUNIXユーザ名が「unixuser1」である場合は、次のパスでディレクトリを作成します。

/vol/vol1/users/unixuser1。

にマウントされた「home1」という名前のボリュームを作成した場合 /home1`では、次のパスでディレクトリを作成します。 `/home1/unixuser1。

11. ドライブをマッピングするか、UNC パスを使用して、ユーザがホームディレクトリ共有に正常に接続できることを確認します。

たとえば、UNIXユーザunixuser1にマッピングされるユーザmydomain\user1が、SVM vs1上にあるディレクトリ（手順10で作成）に接続する場合は、UNCパスを使用して接続します \\vs1\user1。

## 例

次の例のコマンドでは、次の設定を使用してホームディレクトリの設定を作成します。

- 共有名は %w です
- 相対ホームディレクトリパスは %u です
- ホームディレクトリを含むために使用される検索パス /home1、は、UNIXセキュリティ形式で設定されたボリュームです。
- 設定は SVM vs1 上に作成されます。

ユーザが Windows ホストから、または Windows ホストと UNIX ホストからホームディレクトリにアクセスし、ファイルシステム管理者が UNIX ベースのユーザおよびグループを使用してファイルシステムへのアクセスを制御する場合には、このようなホームディレクトリ設定を使用できます。

```
cluster::> vsriver cifs share create -vsriver vs1 -share-name %w -path %u
-share-properties oplocks,browsable,changenotify,homedirectory
```

```
cluster::> vsriver cifs share show -vsriver vs1 -share-name %u
```

```

                Vserver: vs1
                Share: %w
CIFS Server NetBIOS Name: VS1
                Path: %u
        Share Properties: oplocks
                        browsable
                        changenotify
                        homedirectory
        Symlink Properties: enable
        File Mode Creation Mask: -
        Directory Mode Creation Mask: -
                Share Comment: -
                Share ACL: Everyone / Full Control
File Attribute Cache Lifetime: -
                Volume Name: -
                Offline Files: manual
Vscan File-Operations Profile: standard
```

```
cluster::> vsriver cifs home-directory search-path add -vsriver vs1 -path
/home1
```

```
cluster::> vsriver cifs home-directory search-path show -vsriver vs1
```

```
Vserver      Position Path
-----
vs1          1          /home1
```

```
cluster::> vsriver name-mapping create -vsriver vs1 -direction win-unix
-position 5 -pattern user1 -replacement unixuser1
```

```
cluster::> vsriver name-mapping show -pattern user1
```

```
Vserver      Direction Position
-----
vs1          win-unix  5          Pattern: user1
                                Replacement: unixuser1
```

## 関連情報

[%w 変数と %d 変数を使用したホームディレクトリ設定の作成](#)

[追加のホームディレクトリの設定](#)

## SMB ユーザのホームディレクトリパスに関する情報を表示する

### 追加のホームディレクトリの設定

を使用して、追加のホームディレクトリ設定を作成できます `%w`、`%d` および `%u` 変数。必要に応じてホームディレクトリの設定をカスタマイズできます。

共有名と検索パスで変数と静的文字列の組み合わせを使用して、多数のホームディレクトリの設定を作成できます。次の表に、さまざまなホームディレクトリ設定を作成する例を示します。

で作成されるパス /vol1/user ホームディレクトリを含む...	share コマンド
をクリックして共有パスを作成します \\vs1\~win_username これにより、ユーザがに誘導されます /vol1/user/win_username	<code>vserver cifs share create -share-name ~%w -path %w -share-properties oplocks,browsable,changenotify,homedirectory</code>
をクリックして共有パスを作成します \\vs1\win_username これにより、ユーザがに誘導されます /vol1/user/domain/win_username	<code>vserver cifs share create -share-name %w -path %d/%w -share-properties oplocks,browsable,changenotify,homedirectory</code>
をクリックして共有パスを作成します \\vs1\win_username これにより、ユーザがに誘導されます /vol1/user/unix_username	<code>vserver cifs share create -share-name %w -path %u -share-properties oplocks,browsable,changenotify,homedirectory</code>
をクリックして共有パスを作成します \\vs1\unix_username これにより、ユーザがに誘導されます /vol1/user/unix_username	<code>vserver cifs share create -share-name %u -path %u -share-properties oplocks,browsable,changenotify,homedirectory</code>

### 検索パスを管理するコマンド

ONTAPには、SMBホームディレクトリ設定の検索パスを管理するためのコマンドが用意されています。たとえば、検索パスに関する情報を追加、削除、表示するためのコマンドがあります。また、検索パスの順序を変更するためのコマンドもあります。

状況	使用するコマンド
検索パスを追加します	<code>vserver cifs home-directory search-path add</code>
検索パスを表示します	<code>vserver cifs home-directory search-path show</code>

状況	使用するコマンド
検索パスの順序を変更します	<code>vserver cifs home-directory search-path reorder</code>
検索パスを削除します	<code>vserver cifs home-directory search-path remove</code>

詳細については、各コマンドのマニュアルページを参照してください。

**SMB ユーザのホームディレクトリパスに関する情報を表示します**

Storage Virtual Machine（SVM）上の SMB ユーザのホームディレクトリパスを表示できます。これは、複数の CIFS ホームディレクトリパスが設定されている場合に、ユーザのホームディレクトリが含まれるパスを確認するときに役立ちます。

#### ステップ

1. を使用して、ホームディレクトリパスを表示します `vserver cifs home-directory show-user` コマンドを実行します

```
vserver cifs home-directory show-user -vserver vs1 -username user1
```

Vserver	User	Home Dir Path
-----	-----	-----
vs1	user1	/home/user1

#### 関連情報

[ユーザのホームディレクトリへのアクセスの管理](#)

ユーザのホームディレクトリへのアクセスを管理します

デフォルトでは、ユーザのホームディレクトリにはそのユーザしかアクセスできません。動的な共有名の前にチルダ（ { チルダ } ）が付いている共有の場合、Windows 管理者や他のユーザ（パブリックアクセス）によるユーザのホームディレクトリへのアクセスを有効または無効にできます。

作業を開始する前に

Storage Virtual Machine（SVM）のホームディレクトリ共有に、動的な共有名の前にチルダ（ { チルダ } ）を追加した共有名を設定する必要があります。共有の命名要件は次のとおりです。

ホームディレクトリの共有名	共有に接続するコマンドの例
{ チルダ } %d { チルダ } %w	<code>net use * \\IPAddress\~domain~user/u:credentials</code>

ホームディレクトリの共有名	共有に接続するコマンドの例
{ チルダ } %w	net use * \\IPAddress\~user/u:credentials
{ チルダ } abc { チルダ } %w	net use * \\IPAddress\abc~user/u:credentials

## ステップ

1. 適切な操作を実行します。

ユーザのホームディレクトリへのアクセスを有効または無効にする対象	入力するコマンド
Windows 管理者	vserver cifs home-directory modify -vserver vserver_name -is-home-dirs -access-for-admin-enabled {true false} デフォルトはです true。
任意のユーザ（パブリックアクセス）	a. 権限レベルをadvancedに設定+ set -privilege advanced  b. アクセスを有効または無効にします。`vserver cifs home-directory modify -vserver vserver_name -is-home-dirs-access-for-public -enabled {true

次の例は、ユーザのホームディレクトリへのパブリックアクセスを有効にします。+

```
set -privilege advanced [] `vserver cifs home-directory modify -vserver vs1 -is-home-dirs-access-for
-public-enabled true` []
set -privilege admin
```

## 関連情報

[SMB ユーザのホームディレクトリパスに関する情報を表示する](#)

## UNIX シンボリックリンクへの SMB クライアントアクセスを設定する

ONTAP を使用して UNIX シンボリックリンクへの SMB クライアントアクセスを提供する方法

シンボリックリンクは UNIX 環境で作成されるファイルで、別のファイルまたはディレクトリへの参照が含まれます。シンボリックリンクにアクセスしたクライアントは、シンボリックリンクが参照するターゲットファイルまたはディレクトリにリダイレクトされます。ONTAP は、ワイドリンク（ローカルファイルシステムの外部にあるターゲットとの絶対リンク）を含む、相対および絶対シンボリックリンクをサポートしています。

ONTAP には、SMB クライアントが SVM で設定されている UNIX のシンボリックリンクをたどるための機能が用意されています。この機能はオプションであり、を使用して共有ごとに設定できます `-symlink` `-properties` のオプション `vserver cifs share create` 次のいずれかの設定を指定してコマンドを実行します。

- 読み取り / 書き込みアクセスで有効化
- 読み取り専用アクセスで有効化
- SMB クライアントに対してシンボリックリンクを非表示にして無効にしました
- SMB クライアントからシンボリックリンクへのアクセス権なしで無効になりました

共有でシンボリックリンクを有効にした場合、相対シンボリックリンクは追加の設定なしで機能します。

共有でシンボリックリンクを有効にただけでは、絶対シンボリックリンクは機能しません。最初に、シンボリックリンクの UNIX パスからデスティネーション SMB パスへのマッピングを作成する必要があります。絶対シンボリックリンクのマッピングを作成する場合、ローカルリンクが `a_widelink` ; ワイドリンクを他のストレージデバイス上のファイルシステムにリンクするか、同じ ONTAP システム上の別々の SVM でホストされているファイルシステムにリンクするかを指定できます。widelink を作成するときは、そのクライアントが参照するための情報を含める必要があります。つまり、クライアントがディレクトリのリパースジャンクションポイントを検出するためのポイントを作成します。ローカル共有外のファイルまたはディレクトリへの絶対シンボリックリンクを作成しても、局所性をローカルに設定すると、ONTAP はターゲットへのアクセスを許可しません。



クライアントがローカルシンボリックリンク（絶対または相対）を削除しようとした場合、シンボリックリンクのみが削除され、ターゲットファイルまたはターゲットディレクトリは削除されません。それに対して、クライアントがワイドリンクを削除しようとした場合には、ワイドリンクが参照する実際のターゲットファイルやターゲットディレクトリが削除されることがあります。クライアントは SVM 外のターゲットファイルまたはディレクトリを明示的に開いて削除できるため、ONTAP ではこの操作を制御できません。

#### • \* リパースポイントと ONTAP ファイルシステムサービス \*

`a_reparse point_` は、オプションでファイルとともにボリュームに格納できる NTFS ファイルシステムオブジェクトです。リパースポイントは、SMB クライアントが NTFS 形式のボリュームで作業する際に、拡張ファイルシステムサービスを受け取る機能を提供します。リパースポイントは、リパースポイントのタイプを識別する標準のタグと、クライアントがさらに処理するために SMB クライアントが取得できるリパースポイントのコンテンツで構成されます。ファイルシステムの拡張機能で利用できるオブジェクトタイプの中で、ONTAP は、リパースポイントタグを使用した NTFS シンボリックリンクとディレクトリジャンクションポイントのサポートを実装しています。リパースポイントの内容を認識できない SMB クライアントは、単に無視し、リパースポイントで有効になる可能性がある拡張ファイルシステムサービスを提供しません。

#### • \* ディレクトリジャンクションポイントおよびシンボリックリンクの ONTAP サポート \*

ディレクトリジャンクションポイントは、ファイルが格納されている別の場所（別のパス（シンボリックリンク）または別のストレージデバイス（ワイドリンク）を参照できる、ファイルシステムディレクトリ構造内の場所です。ONTAP SMB サーバでは、ディレクトリのジャンクションポイントをリパースポイントとして Windows クライアントに公開し、ディレクトリのジャンクションポイントがトラバースされたときに対応したクライアントが ONTAP からリパースポイントのコンテンツを取得できるようにします。その結果、異なるパスやストレージデバイスを、同じファイルシステムに属しているかのように移動して接続することができます。

#### • \* リパースポイントオプションを使用したワイドリンクサポートの有効化 \*

`-is-use-junctions-as-reparse-points-enabled` ONTAP 9では、オプションはデフォルトで有効になっています。すべての SMB クライアントがワイドリンクをサポートしているわけではないため、情報を有効にするオプションはプロトコルバージョンごとに設定可能であり、サポート対象とサポー



ト対象外の両方の SMB クライアントに対応できるようにします。ONTAP 9.2以降のリリースでは、オプションを有効にする必要があります `-widelink-as-reparse-point-versions` ワイドリンクを使用して共有にアクセスする各クライアントプロトコル（デフォルトはSMB1）。以前のリリースでは、デフォルトの SMB1 を使用してアクセスされるワイドリンクのみがレポートされ、SMB2 または SMB3 を使用するシステムはワイドリンクにアクセスできませんでした。

詳細については、Microsoft NTFS のマニュアルを参照してください。

## "Microsoft のドキュメント：「Reparse Points」

**SMB** アクセス用に **UNIX** シンボリックリンクを設定する場合の制限

SMB アクセス用に UNIX シンボリックリンクを設定する際には、一定の制限事項を理解しておく必要があります。

制限（Limit）	説明
4時45分	CIFS サーバ名の FQDN を使用して指定できる CIFS サーバ名の最大文字数。 <div> 代わりに、CIFS サーバ名を NetBIOS 名として指定できますが、その場合は 15 文字に制限されます。</div>
80	共有名の最大文字数。
256	シンボリックリンクを作成するとき、または既存のシンボリックリンクのUNIXパスを変更するときに指定できるUNIXパスの最大長。UNIXパスはで始まる必要があります/" (slash) and end with a "/"。先頭と末尾のスラッシュは、256 文字の制限に含まれます。
256	シンボリックリンクの作成時または既存のシンボリックリンクのCIFSパスの変更時に指定できるCIFSパスの最大長。CIFSパスはで始まる必要があります/" (slash) and end with a "/"。先頭と末尾のスラッシュは、256 文字の制限に含まれます。

## 関連情報

### SMB 共有のシンボリックリンクマッピングの作成

**CIFS** サーバオプションを使用して、**ONTAP** で **DFS** の自動通知を制御する

共有に接続する SMB クライアントに DFS 対応を通知する方法は、CIFS サーバオプションで制御されます。ONTAP では、クライアントが SMB 経由でシンボリックリンクにアクセスするときに DFS リファールを使用するため、このオプションを無効または有効にしたときの影響を理解しておく必要があります。



DFS に対応していることを CIFS サーバが SMB クライアントに自動的に通知するかどうかは、CIFS サーバオプションで指定します。デフォルトでは、このオプションは有効になっており、CIFS サーバは DFS に対応していることを常に SMB クライアントに（たとえシンボリックリンクへのアクセスが無効になっている共有に接続する場合でも）通知します。シンボリックリンクへのアクセスが有効になっている共有にクライアントが接続する場合にのみ、DFS に対応していることを CIFS サーバがクライアントに通知するようにするには、このオプションを無効にします。

このオプションを無効にすると次のような影響があることに注意してください。

- シンボリックリンクの共有設定は変更されません。
- シンボリックリンクアクセス（読み取り / 書き込みアクセスまたは読み取り専用アクセス）を許可するように共有パラメータが設定されている場合、CIFS サーバは、その共有に接続するクライアントに DFS 対応を通知します。

シンボリックリンクへのクライアントの接続とアクセスは中断されることなく続行されます。

- シンボリックリンクアクセスを許可しないように共有パラメータが設定されている場合（アクセスを無効にしているか共有パラメータの値が null の場合）、CIFS サーバは、その共有に接続するクライアントに DFS 対応を通知しません。

クライアントは、CIFS サーバが DFS に対応しているというキャッシュされた情報を保持しており、CIFS サーバはそのことを通知しなくなるので、シンボリックリンクアクセスが無効になっている共有に接続されたクライアントは、CIFS サーバオプションが無効になったあとでそれらの共有にアクセスできなくなることがあります。オプションが無効になったあとで、それらの共有に接続されたクライアントをリポートし、キャッシュされた情報を消去する必要があります。

これらの変更は SMB 1.0 の接続には適用されません。

**SMB 共有で UNIX シンボリックリンクサポートを設定する**

SMB 共有の作成時に、または既存の SMB 共有の変更によっていつでも、シンボリックリンクの共有プロパティ設定を指定することによって、SMB 共有で UNIX シンボリックリンクのサポートを設定できます。UNIX シンボリックリンクのサポートはデフォルトで有効になっています。UNIX シンボリックリンクのサポートを共有で無効にすることもできます。

このタスクについて

SMB 共有で UNIX シンボリックリンクのサポートを設定する場合は、次の設定のいずれかを選択できます。

設定	説明
enable（廃止予定*）	読み取り / 書き込みアクセスに対してシンボリックリンクを有効にします。
read_only（廃止予定*）	読み取り専用アクセスに対してシンボリックリンクを有効にします。この設定はワイドリンクには適用されません。ワイドリンクアクセスは常に読み取り / 書き込みです。

設定	説明
hide (廃止予定*)	SMB クライアントにシンボリックリンクが表示されないようにします。
no-strict-security	クライアントに共有の範囲を越えるシンボリックリンクの参照を許可します。
symlinks	読み取り / 書き込みアクセスに対してローカルシンボリックリンクを有効にします。CIFSオプションが設定されていても、DFS通知は生成されません is-advertise-dfs-enabled がに設定されます true。これがデフォルト設定です。
symlinks-and-widelinks	読み取り / 書き込みアクセスに対してローカルシンボリックリンクとワイドリンクの両方を有効にします。DFS通知は、CIFSオプションが指定されている場合でも、ローカルシンボリックリンクとワイドリンクの両方に対して生成されます is-advertise-dfs-enabled がに設定されます false。
disable	シンボリックリンクとワイドリンクを無効にします。CIFSオプションが設定されていても、DFS通知は生成されません is-advertise-dfs-enabled がに設定されます true。
"" (null、未設定)	シンボリックリンクを共有で無効にします。
- (未設定)	シンボリックリンクを共有で無効にします。



- ONTAP の今後のリリースでは、`enable,hide,_read-only` パラメータは廃止されており、削除される可能性があります。

## 手順

1. シンボリックリンクのサポートを設定または無効化します。

条件	入力するコマンド
新しい SMB 共有	<code>`+vserver cifs share create -vserver vserver_name -share-name share_name -path path -symlink -properties {enable</code>
hide	<code>read-only</code>
""	<code>-</code>
symlinks	<code>symlinks-and-widelinks</code>

条件	入力するコマンド
disable},...]+`	既存の SMB 共有
`+vserver cifs share modify -vserver vs1 -share-name share_name -symlink-properties {enable	hide
read-only	""
-	symlinks
symlinks-and-widelinks	disable},...]+`

2. SMB共有の設定が正しいことを確認します。 `vserver cifs share show -vserver vs1 -share-name share_name -instance`

例

次のコマンドでは、UNIXシンボリックリンク設定をに設定して、「data1」という名前のSMB共有を作成します enable：

```
cluster1::> vserver cifs share create -vserver vs1 -share-name data1 -path /data1 -symlink-properties enable

cluster1::> vserver cifs share show -vserver vs1 -share-name data1 -instance

Vserver: vs1
Share: data1
CIFS Server NetBIOS Name: VS1
Path: /data1
Share Properties: oplocks
                  browsable
                  changenotify
Symlink Properties: enable
File Mode Creation Mask: -
Directory Mode Creation Mask: -
Share Comment: -
Share ACL: Everyone / Full Control
File Attribute Cache Lifetime: -
Volume Name: -
Offline Files: manual
Vscan File-Operations Profile: standard
Maximum Tree Connections on Share: 4294967295
UNIX Group for File Create: -
```

関連情報

## SMB 共有のシンボリックリンクマッピングの作成

**SMB 共有のシンボリックリンクマッピングを作成します**

SMB 共有に対する UNIX シンボリックリンクのマッピングを作成できます。親フォルダに対して相対的なファイルまたはフォルダを参照する相対シンボリックリンクを作成することも、絶対パスを使用してファイルまたはフォルダを参照する絶対シンボリックリンクを作成することもできます。

このタスクについて

SMB 2.x を使用している場合、Mac OS X クライアントからワイドリンクにアクセスすることはできません。Mac OS X クライアントからワイドリンクを使用して共有に接続しようとする、接続に失敗します。ただし、SMB 1 を使用している場合は、Mac OS X クライアントでワイドリンクを使用できます。

手順

1. SMB共有のシンボリックリンクマッピングを作成するには：

```
vserver cifs symlink create  
-vserver virtual_server_name -unix-path path -share-name share_name -cifs-path  
path [-cifs-server server_name] [-locality {local|free|widelink}] [-home-  
directory {true|false}]
```

`-vserver virtual_server_name` Storage Virtual Machine (SVM) 名を示します。

`-unix-path path` UNIXパスを指定します。UNIXパスはスラッシュで始まる必要があります (/) とスラッシュで終わる必要があります (/)。

`-share-name share_name` マッピングするSMB共有の名前を指定します。

`-cifs-path path` CIFSパスを指定します。CIFSパスはスラッシュで始まる必要があります (/) とスラッシュで終わる必要があります (/)。

`-cifs-server server_name` CIFSサーバ名を指定します。CIFS サーバ名は、DNS 名 ( `mynetwork.cifs.server.com` など)、IP アドレス、または NetBIOS 名として指定できます。NetBIOS名は、を使用して確認できます `vserver cifs show` コマンドを実行しますこのオプションパラメータを指定しない場合、デフォルト値のローカル CIFS サーバの NetBIOS 名が使用されます。

`-locality local|free|widelink}`は、ローカルリンク、フリーリンク、ワイドシンボリックリンクのいずれを作成するかを指定します。ローカルシンボリックリンクはローカル SMB 共有にマッピングされます。フリーシンボリックリンクはローカル SMB サーバ上の任意の場所にマッピングできます。ワイドシンボリックリンクはネットワーク上の任意の SMB 共有にマッピングされます。このオプションパラメータを指定しない場合、デフォルト値は `local` です。

`-home-directory true false}` ターゲットの共有がホームディレクトリかどうかを指定します。このパラメータはオプションですが、このパラメータをに設定する必要があります `true` ターゲットの共有がホームディレクトリとして設定されている場合。デフォルトは `false` です。

例

次のコマンドは、`vs1` という名前の SVM 上にシンボリックリンクマッピングを作成します。UNIXパスが設定されている `/src/`、SMB共有名「ソース」、CIFSパス `/mycompany/source/` およびCIFSサーバのIPアドレス123.123.123.123。ワイドリンクです。

```
cluster1::> vserver cifs symlink create -vserver vs1 -unix-path /src/  
-share-name SOURCE -cifs-path "/mycompany/source/" -cifs-server  
123.123.123.123 -locality widelink
```

## 関連情報

### SMB 共有での UNIX シンボリックリンクサポートの設定

シンボリックリンクのマッピングを管理するコマンド

ONTAP には、シンボリックリンクのマッピングを管理するためのコマンドが用意されています。

状況	使用するコマンド
シンボリックリンクのマッピングを作成します	<code>vserver cifs symlink create</code>
シンボリックリンクのマッピングに関する情報を表示する	<code>vserver cifs symlink show</code>
シンボリックリンクのマッピングを変更する	<code>vserver cifs symlink modify</code>
シンボリックリンクのマッピングを削除する	<code>vserver cifs symlink delete</code>

詳細については、各コマンドのマニュアルページを参照してください。

### BranchCache を使用してブランチオフィスで SMB 共有のコンテンツをキャッシュする

BranchCache を使用してブランチオフィスの概要で SMB 共有のコンテンツをキャッシュする

BranchCache は、要求元のクライアントのローカルコンピュータにコンテンツをキャッシュできるようにするために Microsoft が開発した機能です。ONTAP に BranchCache を実装すると、Storage Virtual Machine（SVM）に格納されたコンテンツに SMB を使用してブランチオフィスのユーザがアクセスする際に、広域ネットワーク（WAN）の使用量を抑え、アクセス応答時間を短縮することができます。

BranchCache を設定すると、Windows BranchCache クライアントはまず SVM のコンテンツを取得し、次に取得したコンテンツをブランチオフィスのコンピュータにキャッシュします。ブランチオフィスの別の BranchCache 対応クライアントが同じコンテンツを要求すると、SVM は最初に要求元ユーザの認証と許可を実行します。次に SVM は、キャッシュされたコンテンツが最新のものであるかどうかを確認し、最新のものである場合はそのコンテンツに関するメタデータをクライアントに送信します。クライアントは、そのメタデータを使用して、ローカルのキャッシュから直接コンテンツを取得します。

## 関連情報

### オフラインファイルを使用したオフラインで使用するファイルのキャッシュ

## BranchCache バージョンのサポート

ONTAP でサポートされる BranchCache のバージョンを確認しておく必要があります。

ONTAP では、BranchCache 1 と強化された BranchCache 2 がサポートされています。

- Storage Virtual Machine (SVM) の SMB サーバで BranchCache を設定するときに、BranchCache 1、BranchCache 2、またはすべてのバージョンを有効にすることができます。

デフォルトでは、すべてのバージョンが有効になっています。

- BranchCache 2 のみを有効にする場合は、リモートオフィスの Windows クライアントマシンで BranchCache 2 がサポートされている必要があります。

BranchCache 2 をサポートするのは SMB 3.0 以降のクライアントだけです。

BranchCache のバージョンの詳細については、Microsoft TechNet ライブラリを参照してください。

### 関連情報

"Microsoft TechNet ライブラリ: [technet.microsoft.com/en-us/library/](https://technet.microsoft.com/en-us/library/)"

## ネットワークプロトコルのサポート要件

ONTAP BranchCache を実装するときは、ネットワークプロトコルの要件を考慮する必要があります。

ONTAP BranchCache 機能は、SMB 2.1 以降を使用して、IPv4 および IPv6 のネットワークに実装できます。

BranchCache の実装に含まれるすべての CIFS サーバとブランチオフィスのマシンで、SMB 2.1 以降のプロトコルを有効にする必要があります。SMB 2.1 では、プロトコルの機能拡張により、クライアントを BranchCache 環境に含めることができます。SMB プロトコルとして BranchCache をサポートするために必要な最小バージョンを指定してください。SMB 2.1 は、BranchCache バージョン 1 をサポートします。

BranchCache バージョン 2 を使用する場合は、サポートする SMB の最小バージョンは SMB 3.0 になります。BranchCache 2 の実装に含まれるすべての CIFS サーバとブランチオフィスのマシンで、SMB 3.0 以降を有効にする必要があります。

リモートオフィスで SMB 2.1 のみサポートするクライアント、SMB 3.0 をサポートするクライアントが混在する場合は、BranchCache 1 と BranchCache 2 の両方のキャッシングをサポートする CIFS サーバに BranchCache 構成を実装することができます。



Microsoft BranchCache 機能ではファイルアクセスプロトコルとして HTTP / HTTPS と SMB プロトコルの両方がサポートされますが、ONTAP BranchCache でサポートされるのは SMB のみです。

## ONTAP および Windows ホストのバージョン要件

BranchCache を設定するには、ONTAP やブランチオフィスの Windows ホストが特定

のバージョン要件を満たしている必要があります。

BranchCache を設定するには、クラスタの ONTAP のバージョンや対象となるブランチオフィスのクライアントで、SMB 2.1 以降と BranchCache の機能をサポートしている必要があります。また、ホスト型キャッシュモードを設定する場合は、サポートされているホストをキャッシュサーバに使用する必要があります。

BranchCache 1 は、次の ONTAP バージョンと Windows ホストでサポートされています。

- コンテンツサーバ：ONTAP を備えた Storage Virtual Machine (SVM)
- キャッシュサーバ：Windows Server 2008 R2 または Windows Server 2012 以降
- ピアまたはクライアント：Windows 7 Enterprise、Windows 7 Ultimate、Windows 8、Windows Server 2008 R2、または Windows Server 2012 以降

BranchCache 2は、次のONTAPバージョンおよびWindowsホストでサポートされています。

- コンテンツサーバ：ONTAP を備えた SVM
- キャッシュサーバ：Windows Server 2012 以降
- ピアまたはクライアント：Windows 8 または Windows Server 2012 以降

#### ONTAP で BranchCache ハッシュが無効になる理由

ONTAP でどのような場合にハッシュが無効になるかを理解すると、BranchCache の設定を計画するときに役立ちます。この情報に基づいて、設定する必要がある動作モードの決定と、BranchCache を有効にする共有を選択するかどうかの検討の助けになります。

ONTAP は、BranchCache ハッシュが有効なものであるかを管理しています。ハッシュが無効な場合、ONTAP は次にコンテンツが要求されたときにハッシュを無効にして新しいハッシュを計算します。これは、BranchCache が有効なままであることを前提としています。

ONTAP は、以下の場合にハッシュを無効にします。

- サーバキーが変更された場合。

サーバキーが変更された場合は、ONTAP によってハッシュストア内のすべてのハッシュが無効になります。

- BranchCache のハッシュストアの最大サイズに達したために、ハッシュがキャッシュからフラッシュされた場合。

このパラメータは調整可能で、ビジネス要件に合わせて変更することができます。

- SMB または NFS 経由のアクセスでファイルが変更された場合。
- 有効なハッシュが適用されたファイルがを使用してリストアされた場合 `snap restore` コマンドを実行します
- BranchCache対応のSMB共有を含むボリュームがを使用してリストアされた場合 `snap restore` コマンドを実行します

BranchCache を設定する場合は、ハッシュを格納する場所とハッシュストアのサイズを選択します。ハッシュストアの場所とサイズに関するガイドラインについて理解しておく、CIFS 対応の SVM で BranchCache の設定を計画するのに役立ちます。

- ハッシュストアは、atime アップデートが許可されるボリューム上に配置する必要があります。

ハッシュストアでは、ハッシュファイルへのアクセス時間を使用して、アクセス頻度の高いファイルを管理します。atime アップデートが無効になっている場合、作成時間がこの目的に使用されます。使用頻度の高いファイルを追跡するために atime を使用することを推奨します。

- SnapMirror デスティネーションや SnapLock ボリュームなどの読み取り専用のファイルシステムにはハッシュを格納できません。
- ハッシュストアが最大サイズに達すると、新しいハッシュを格納するスペースを確保するために古いハッシュがフラッシュされます。

ハッシュストアの最大サイズを増やすと、キャッシュからフラッシュされるハッシュの量を減らすことができます。

- ハッシュを格納するボリュームが使用できないか、いっぱいである場合、またはクラスタ内通信に BranchCache サービスがハッシュ情報を取得できない問題がある場合、BranchCache サービスは使用できません。

ボリュームは、オフラインであるため、またはストレージ管理者がハッシュストアの新しい場所を指定したために、使用できないことがあります。

これは、ファイルアクセスに関する原因の問題ではありません。ハッシュストアに正常にアクセスできない場合は、ONTAP からクライアントに Microsoft 定義のエラーが返され、クライアントは通常の SMB 読み取り要求を使用してファイルを要求します。

### 関連情報

#### [SMBサーバでのBranchCacheの設定](#)

#### [BranchCache の設定を変更します](#)

### BranchCache の推奨事項

BranchCache を設定する前に、BranchCache キャッシュを有効にする SMB 共有の決定時に考慮する必要がある推奨事項がいくつかあります。

使用する動作モードと BranchCache を有効にする SMB 共有の決定時には、次の推奨事項を考慮してください。

- リモートからキャッシュするデータが頻繁に変更されると、BranchCache の利点が十分には生かされません。
- BranchCache サービスは、複数のリモートオフスクライアントによって再利用されるファイルコンテンツ、または単一のリモートユーザが繰り返しアクセスするファイルコンテンツを含む共有の場合に役立ちます。
- Snapshot コピーのデータや SnapMirror デスティネーションのデータなどの読み取り専用コンテンツのキ



キャッシュを有効にすることを検討してください。

**BranchCache** を設定します

## **BranchCache** の概要を設定

SMB サーバで BranchCache を設定するには、ONTAP コマンドを使用します。BranchCache を実装するには、クライアント、および必要に応じてコンテンツをキャッシュするブランチオフィスにホストされるキャッシュサーバも設定する必要があります。

共有ごとにキャッシュを有効にするように BranchCache を設定する場合は、BranchCache キャッシュサービスの対象となる SMB 共有で BranchCache を有効にする必要があります。

## **BranchCache** を設定するための要件

BranchCache のセットアップを開始する前に、いくつかの前提条件を満たす必要があります。

SVM の CIFS サーバで BranchCache を設定するには、次の要件を満たしている必要があります。

- クラスタ内のすべてのノードに ONTAP がインストールされている必要があります。
- CIFS のライセンスが有効になっていて、SMB サーバが設定されている必要があります。SMB ライセンスには含まれています。"ONTAP One"。ONTAP One をお持ちでなく、ライセンスがインストールされていない場合は、営業担当者にお問い合わせください。
- IPv4 または IPv6 のネットワーク接続が設定されている必要があります。
- BranchCache 1 の場合、SMB 2.1 以降が有効になっている必要があります。
- BranchCache 2 の場合、SMB 3.0 が有効になっていて、リモートの Windows クライアントで BranchCache 2 がサポートされている必要があります。

## **SMB**サーバでの**BranchCache**の設定

BranchCache サービスを共有ごとに提供するように BranchCache を設定できます。また、すべての SMB 共有でキャッシュを自動的に有効にするように BranchCache を設定することもできます。

このタスクについて

BranchCache は SVM で設定できます。

- CIFS サーバ上のすべての SMB 共有に格納されたすべてのコンテンツに対してキャッシュサービスを提供する場合は、すべての共有の BranchCache 設定を作成できます。
- CIFS サーバ上の選択した SMB 共有に格納されたコンテンツに対してキャッシュサービスを提供する場合は、共有ごとの BranchCache 設定を作成できます。

BranchCache の設定時には、次のパラメータを指定する必要があります。

必須パラメータ	説明
SVM 名 _	BranchCache は SVM ごとに設定します。BranchCache サービスを設定する CIFS 対応の SVM を指定する必要があります。
ハッシュストアへのパス _	<p>BranchCache ハッシュは SVM ボリューム上の通常のファイルに格納されます。ONTAP にハッシュデータを格納する既存のディレクトリのパスを指定する必要があります。BranchCache ハッシュパスは読み取り / 書き込み可能である必要があります。Snapshot ディレクトリなどの読み取り専用パスは指定できません。他のデータが格納されているボリュームにハッシュデータを格納するか、ハッシュデータを格納するための別のボリュームを作成することができます。</p> <p>SVM が SVM ディザスタリカバリソースである場合、ハッシュパスをルートボリューム上にすることはできません。これは、ルートボリュームがディザスタリカバリデスティネーションにレプリケートされないためです。</p> <p>ハッシュパスには、ファイル名に使用できる文字と空白を含めることができます。</p>

必要に応じて、次のパラメータを指定できます。

オプションのパラメータ	説明
サポートされているバージョン _	ONTAP では BranchCache 1 および 2 がサポートされています。バージョン 1、バージョン 2、または両方のバージョンを有効にできます。デフォルトでは、両方のバージョンが有効になります。
_ ハッシュストアの最大サイズ _	ハッシュデータストアに使用するサイズを指定できます。ハッシュデータがこの値を超えると、ONTAP は古いハッシュを削除し、新しいハッシュを格納するスペースを確保します。ハッシュストアのデフォルトサイズは 1GB です。ハッシュが過剰に破棄されない方が、BranchCache のパフォーマンスは向上します。ハッシュストアがいっぱいになるのが原因でハッシュが頻繁に破棄されていると判断した場合は、BranchCache の設定を変更して、ハッシュストアのサイズを大きくすることができます。

オプションのパラメータ	説明
_ サーバキー _	クライアントが BranchCache サーバを偽装できないようにするために BranchCache サービスによって使用されるサーバキーを指定できます。指定しない場合、サーバキーは BranchCache の設定の作成時にランダムに生成されます。サーバキーを特定の値に設定すると、複数のサーバが同じファイルの BranchCache データを提供している場合に、クライアントがその同じサーバキーを使用してサーバのハッシュを使用できるようになります。サーバキーにスペースを含める場合は、サーバキーを引用符で囲む必要があります。
オペレーティングモード _	<p>デフォルトでは、BranchCache は共有ごとに有効になります。</p> <ul style="list-style-type: none"> <li>• BranchCacheを共有ごとに有効にするBranchCacheの設定を作成するには、このオプションパラメータを指定しないか、を指定します per-share。</li> <li>• すべての共有でBranchCacheを自動的に有効にするには、動作モードをに設定する必要があります all-shares。</li> </ul>

## 手順

1. 必要に応じて SMB 2.1 および 3.0 を有効にします。
  - a. 権限レベルを advanced に設定します。 `set -privilege advanced`
  - b. SVMのSMB設定を確認して、必要なすべてのバージョンのSMBが有効になっているかどうかを確認します。 `vserver cifs options show -vserver vserver_name`
  - c. 必要に応じて、SMB 2.1を有効にします。 `vserver cifs options modify -vserver vserver_name -smb2-enabled true`

このコマンドを実行すると、SMB 2.0 と SMB 2.1 の両方が有効になります。

- d. 必要に応じて、SMB 3.0を有効にします。 `vserver cifs options modify -vserver vserver_name -smb3-enabled true`
  - e. admin 権限レベルに戻ります。 `set -privilege admin`
2. BranchCacheを設定します。 `vserver cifs branchcache create -vserver vserver_name -hash-store-path path [-hash-store-max-size {integer[KB|MB|GB|TB|PB]}] [-versions {v1-enable|v2-enable|enable-all}] [-server-key text] -operating-mode {per-share|all-shares}`

指定したハッシュストレージのパスが存在し、SVMによって管理されているボリューム上にある必要があります。また、パスは読み取り / 書き込み可能なボリュームにある必要があります。パスが読み取り専用であるか、または存在しない場合、コマンドは失敗します。

SVM BranchCache の追加設定で同じサーバキーを使用する場合は、サーバキーとして入力した値を記録

しておきます。BranchCache の設定に関する情報を表示するときに、サーバキーは表示されません。

3. BranchCache の設定が正しいことを確認します。 `vserver cifs branchcache show -vserver vserver_name`

例

次のコマンドを実行すると、SMB 2.1 と 3.0 の両方が有効になっていることが確認され、SVM vs1 上のすべての SMB 共有でキャッシュを自動的に有効にするように BranchCache が設定されます。

```
cluster1::> set -privilege advanced
Warning: These advanced commands are potentially dangerous; use them
only when directed to do so by technical support personnel.
Do you wish to continue? (y or n): y

cluster1::*> vserver cifs options show -vserver vs1 -fields smb2-
enabled,smb3-enabled
vserver smb2-enabled smb3-enabled
-----
vs1      true      true

cluster1::*> set -privilege admin

cluster1::> vserver cifs branchcache create -vserver vs1 -hash-store-path
/hash_data -hash-store-max-size 20GB -versions enable-all -server-key "my
server key" -operating-mode all-shares

cluster1::> vserver cifs branchcache show -vserver vs1

                                Vserver: vs1
        Supported BranchCache Versions: enable_all
                                Path to Hash Store: /hash_data
        Maximum Size of the Hash Store: 20GB
Encryption Key Used to Secure the Hashes: -
        CIFS BranchCache Operating Modes: all_shares
```

次のコマンドを実行すると、SMB 2.1 と 3.0 の両方が有効になっていることが確認され、SVM vs1 上の共有ごとにキャッシュを有効にするように BranchCache が設定されて、BranchCache の設定が確認されます。

```

cluster1::> set -privilege advanced
Warning: These advanced commands are potentially dangerous; use them
only when directed to do so by technical support personnel.
Do you wish to continue? (y or n): y

cluster1::*> vsserver cifs options show -vsserver vs1 -fields smb2-
enabled,smb3-enabled
vsserver smb2-enabled smb3-enabled
-----
vs1      true      true

cluster1::*> set -privilege admin

cluster1::> vsserver cifs branchcache create -vsserver vs1 -hash-store-path
/hash_data -hash-store-max-size 20GB -versions enable-all -server-key "my
server key"

cluster1::> vsserver cifs branchcache show -vsserver vs1

                                Vserver: vs1
        Supported BranchCache Versions: enable_all
                                Path to Hash Store: /hash_data
        Maximum Size of the Hash Store: 20GB
Encryption Key Used to Secure the Hashes: -
        CIFS BranchCache Operating Modes: per_share

```

## 関連情報

[要件とガイドライン：BranchCache バージョンのサポート](#)

[リモートオフィスでの BranchCache の設定に関する情報の参照先を指定します](#)

[BranchCache が有効な SMB 共有を作成](#)

[既存の SMB 共有で BranchCache を有効にします](#)

[BranchCache の設定を変更します](#)

[SMB 共有で BranchCache を無効にする手順の概要](#)

[SVM の BranchCache 設定を削除します](#)

リモートオフィスでの **BranchCache** の設定に関する情報の参照先を指定します

SMB サーバで BranchCache を設定したら、クライアントコンピュータに BranchCache をインストールして設定する必要があります。また、必要に応じて、リモートオフィスのキャッシュサーバにも BranchCache をインストールして設定する必要があります。リ

モートオフィスで BranchCache を設定する手順については、Microsoft から説明が提供されています。

ブランチオフィスのクライアントを設定する手順、および必要に応じて BranchCache を使用するキャッシュサーバを Microsoft BranchCache の Web サイトで設定する手順について説明します。

["Microsoft BranchCache のドキュメント：「What's New」](#)

**BranchCache が有効な SMB 共有を設定**

**BranchCache が有効な SMB 共有の概要を設定**

SMB サーバとブランチオフィスで BranchCache を設定したら、ブランチオフィスのクライアントによるコンテンツのキャッシュを許可する SMB 共有で BranchCache を有効にすることができます。

BranchCache キャッシュは、SMB サーバ上のすべての SMB 共有で有効にするか、共有ごとに有効にすることができます。

- BranchCache を共有ごとに有効にする場合、BranchCache は共有の作成時に有効にするか、既存の共有を変更して有効にすることができます。

既存の SMB 共有でキャッシュを有効にすると、その共有で BranchCache を有効にした時点で、ONTAP によるハッシュの計算と要求元クライアントへのメタデータの送信が開始されます。

- 共有への SMB 接続をすでに確立しているクライアントは、それ以降にその共有で BranchCache が有効になった場合、BranchCache のサポートを得ることができません。

ONTAP は、SMB セッションがセットアップされたときに共有の BranchCache のサポートを通知します。BranchCache が有効なときにすでにセッションを確立していたクライアントは、キャッシュされている内容をこの共有で使用するために、いったん切断してから再接続する必要があります。



その後 SMB 共有に対する BranchCache を無効にすると、ONTAP による要求元クライアントへのメタデータの送信が中止されます。データが必要なクライアントは、コンテンツサーバ（SMB サーバ）から直接データを取得します。

**BranchCache が有効な SMB 共有を作成**

SMB 共有の作成時にを設定して、共有で BranchCache を有効にすることができます  
branchcache 共有プロパティ。

このタスクについて

- SMB 共有で BranchCache を有効にする場合は、共有のオフラインファイル設定を手動キャッシュに設定する必要があります。

これは、共有を作成するときのデフォルト設定です。

- BranchCache が有効な共有を作成するときに、オプションの共有パラメータを追加で指定することもできます。

- を設定できます `branchcache` Storage Virtual Machine (SVM) で `BranchCache` が設定されておらず有効になっていない場合も含む共有のプロパティ。

ただし、共有でキャッシュされたコンテンツを提供するには、SVM で `BranchCache` を設定して有効にする必要があります。

- を使用するとき共有に適用されるデフォルトの共有プロパティはないためです `-share-properties` パラメータを指定する場合は、に加えて共有に適用する他のすべての共有プロパティを指定する必要があります `branchcache` プロパティを共有するには、カンマで区切って指定します。
- 詳細については、のマニュアルページを参照してください `vserver cifs share create` コマンドを実行します

## ステップ

1. `BranchCache` が有効な SMB 共有を作成します。+  
`vserver cifs share create -vserver vserver_name -share-name share_name -path path -share-properties branchcache[,...]`
2. を使用して、SMB 共有に対して `BranchCache` 共有プロパティが設定されていることを確認します  
`vserver cifs share show` コマンドを実行します

## 例

次のコマンドでは、「data」という名前の `BranchCache` が有効な SMB 共有をパスに作成します `/data` SVM `vs1` 上。デフォルトでは、オフラインファイルの設定はに設定されています `manual` :

```
cluster1::> vserver cifs share create -vserver vs1 -share-name data -path
/data -share-properties branchcache,oplocks,browsable,changenotify

cluster1::> vserver cifs share show -vserver vs1 -share-name data
      Vserver: vs1
      Share: data
CIFS Server NetBIOS Name: VS1
      Path: /data
      Share Properties: branchcache
                        oplocks
                        browsable
                        changenotify
      Symlink Properties: enable
      File Mode Creation Mask: -
      Directory Mode Creation Mask: -
      Share Comment: -
      Share ACL: Everyone / Full Control
      File Attribute Cache Lifetime: -
      Volume Name: data
      Offline Files: manual
      Vscan File-Operations Profile: standard
```

## 関連情報

## 単一の SMB 共有での BranchCache の無効化

既存の **SMB** 共有で **BranchCache** を有効にします

既存のSMB共有でBranchCacheを有効にするには、を追加します `branchcache` 共有プロパティを既存の共有プロパティリストに追加します。

このタスクについて

- SMB 共有で BranchCache を有効にする場合は、共有のオフラインファイル設定を手動キャッシュに設定する必要があります。

既存の共有のオフラインファイル設定が手動キャッシュに設定されていない場合は、共有を変更して設定する必要があります。

- を設定できます `branchcache Storage Virtual Machine (SVM)` でBranchCacheが設定されておらず有効になっていない場合も含む共有のプロパティ。

ただし、共有でキャッシュされたコンテンツを提供するには、SVM で BranchCache を設定して有効にする必要があります。

- を追加したとき `branchcache` 共有プロパティ共有に対する既存の共有設定と共有プロパティは維持されます。

BranchCache 共有プロパティは既存の共有プロパティリストに追加されます。を使用する方法の詳細については、を参照してください `vserver cifs share properties add` コマンドについては、マニュアルページを参照してください。

### 手順

1. 必要に応じて、オフラインファイルの共有設定を手動キャッシュに設定します。
  - a. を使用して、オフラインファイルの共有設定を確認します `vserver cifs share show` コマンドを実行します
  - b. オフラインファイルの共有設定が `manual` に設定されていない場合は、必要な値に変更します。

```
vserver cifs share modify -vserver vserver_name -share-name share_name -offline-files manual
```
2. 既存のSMB共有でBranchCacheを有効にします。 `vserver cifs share properties add -vserver vserver_name -share-name share_name -share-properties branchcache`
3. SMB共有でBranchCache共有プロパティが設定されていることを確認します。 `vserver cifs share show -vserver vserver_name -share-name share_name`

### 例

次のコマンドは、「data2」という名前の既存のSMB共有（パス）でBranchCacheを有効にします `/data2 SVM vs1` :



```
cluster1::> vservice cifs share show -vservice vs1 -share-name data2
```

```

    Vservice: vs1
    Share: data2
    CIFS Server NetBIOS Name: VS1
    Path: /data2
    Share Properties: oplocks
                     browsable
                     changenotify
                     showsnapshot
    Symlink Properties: -
    File Mode Creation Mask: -
    Directory Mode Creation Mask: -
    Share Comment: -
    Share ACL: Everyone / Full Control
File Attribute Cache Lifetime: 10s
    Volume Name: -
    Offline Files: manual
Vscan File-Operations Profile: standard
```

```
cluster1::> vservice cifs share properties add -vservice vs1 -share-name
data2 -share-properties branchcache
```

```
cluster1::> vservice cifs share show -vservice vs1 -share-name data2
```

```

    Vservice: vs1
    Share: data2
    CIFS Server NetBIOS Name: VS1
    Path: /data2
    Share Properties: oplocks
                     browsable
                     showsnapshot
                     changenotify
                     branchcache
    Symlink Properties: -
    File Mode Creation Mask: -
    Directory Mode Creation Mask: -
    Share Comment: -
    Share ACL: Everyone / Full Control
File Attribute Cache Lifetime: 10s
    Volume Name: -
    Offline Files: manual
Vscan File-Operations Profile: standard
```

BranchCache の設定を管理および監視する

BranchCache 設定を変更

SVM 上の BranchCache サービスの設定では、ハッシュストアディレクトリのパス、最大サイズ、動作モード、サポートする BranchCachet のバージョンなどの設定を変更できます。ハッシュストアを含めるボリュームのサイズを拡張することもできます。

手順

- 1. 適切な操作を実行します。

状況	入力するコマンド
ハッシュストアディレクトリのサイズを変更する	<code>`vserver cifs branchcache modify -vserver vservice_name -hash-store-max-size {integer}[KB</code>
MB	GB
TB	PB]}`
ハッシュストアを含めるボリュームのサイズを増やします	<code>`volume size -vserver vservice_name -volume volume_name -new-size new_size[k</code>
m	g
t]` ハッシュストアを含むボリュームがいっぱいになった場合は、ボリュームのサイズを拡張できます。新しいボリュームサイズは、数字と単位で指定できます。  の詳細を確認してください " <a href="#">FlexVol ボリュームの管理</a> "	ハッシュストアディレクトリのパスを変更します

状況	入力するコマンド
<code>`vserver cifs branchcache modify -vserver vserver_name -hash-store-path path -flush-hashes {true</code>	<p><code>false}`</code> SVM が SVM ディザスタリカバリソースである場合、ハッシュパスをルートボリューム上にはできません。これは、ルートボリュームがディザスタリカバリデスティネーションにレプリケートされないためです。</p> <p>BranchCache ハッシュパスには、ファイル名に使用できる文字と空白を含めることができます。</p> <p>ハッシュパスを変更する場合は、<code>-flush-hashes</code> は、ONTAP で元のハッシュストアの場所からハッシュをフラッシュするかどうかを指定する必須パラメータです。には次の値を設定できます <code>-flush -hashes</code> パラメータ：</p> <p>を指定する場合 <code>`true`</code> ONTAP では、元の場所にあるハッシュが削除され、<b>BranchCache</b>対応クライアントから新しい要求が行われると、新しい場所に新しいハッシュが作成されます。</p> <p>を指定する場合 <code>`false`</code>を指定すると、ハッシュはフラッシュされません。</p> <p>+</p> <p>この場合、後でハッシュストアパスを元の場所に戻して、既存のハッシュを再利用することができます。</p>
動作モードを変更します	<code>`vserver cifs branchcache modify -vserver vserver_name -operating-mode {per-share</code>
<code>all-shares</code>	<p><code>disable}`</code></p> <p>動作モードを変更するときは、次の点に注意してください。</p> <p><b>SMB</b>セッションのセットアップ時に、<b>ONTAP</b>によって、<b>BranchCache</b>の共有のサポートが通知されます。</p> <p>BranchCache が有効なときにすでにセッションを確立していたクライアントは、キャッシュされている内容をこの共有で使用するために、いったん切断してから再接続する必要があります。</p>
サポートする BranchCache バージョンを変更します	<code>`vserver cifs branchcache modify -vserver vserver_name -versions {v1-enable</code>
<code>v2-enable</code>	<code>enable-all}`</code>

2. を使用して、設定の変更を確認します `vserver cifs branchcache show` コマンドを実行します

**BranchCache** 設定に関する情報を表示します

Storage Virtual Machine （SVM）の BranchCache 設定に関する情報を表示できます。

この情報は、設定を検証する場合や、設定を変更する前に現在の設定を確認する場合に役立ちます。

ステップ

- 1. 次のいずれかを実行します。

表示する項目	入力するコマンド
すべての SVM の BranchCache 設定に関する概要情報	<code>vserver cifs branchcache show</code>
特定の SVM の設定に関する詳細情報	<code>vserver cifs branchcache show -vserver vserver_name</code>

例

次の例は、SVM vs1 の BranchCache 設定に関する情報を表示します。

```
cluster1::> vserver cifs branchcache show -vserver vs1

                                Vserver: vs1
        Supported BranchCache Versions: enable_all
                Path to Hash Store: /hash_data
        Maximum Size of the Hash Store: 20GB
Encryption Key Used to Secure the Hashes: -
        CIFS BranchCache Operating Modes: per_share
```

BranchCache サーバキーを変更します

BranchCache サーバキーを変更するには、Storage Virtual Machine （SVM）で BranchCache の設定を変更し、別のサーバキーを指定します。

このタスクについて

サーバキーを特定の値に設定すると、複数のサーバが同じファイルの BranchCache データを提供している場合に、クライアントがその同じサーバキーを使用してサーバのハッシュを使用できるようになります。

サーバキーを変更する場合は、ハッシュキャッシュをフラッシュすることにも必要になります。ハッシュのフラッシュ後、BranchCache 対応クライアントによって新しい要求が行われると、ONTAP によって新しいハッシュが作成されます。

手順

- 1. 次のコマンドを使用して、サーバキーを変更します。`vserver cifs branchcache modify -vserver vserver_name -server-key text -flush-hashes true`  
  
新しいサーバキーを設定する場合は、も指定する必要があります `-flush-hashes` に設定します `true`。
- 2. を使用して、BranchCache の設定が正しいことを確認します `vserver cifs branchcache show` コマ

ンドを実行します

## 例

次の例は、SVM vs1 でスペースを含む新しいサーバキーを設定し、ハッシュキャッシュをフラッシュします。

```
cluster1::> vserver cifs branchcache modify -vserver vs1 -server-key "new
vserver secret" -flush-hashes true

cluster1::> vserver cifs branchcache show -vserver vs1

                Vserver: vs1
Supported BranchCache Versions: enable_all
                Path to Hash Store: /hash_data
Maximum Size of the Hash Store: 20GB
Encryption Key Used to Secure the Hashes: -
CIFS BranchCache Operating Modes: per_share
```

## 関連情報

[ONTAP で BranchCache ハッシュが無効になる理由](#)

指定したパスの **BranchCache** ハッシュを事前に計算します

単一のファイル、ディレクトリ、またはディレクトリ構造内のすべてのファイルのハッシュを事前に計算するように BranchCache サービスを設定できます。これは、BranchCache 対応の共有にあるデータのハッシュをピーク以外の時間帯に計算するのに役立ちます。

## このタスクについて

ハッシュの統計を表示する前にデータサンプルを収集する場合は、を使用する必要があります `statistics start` およびオプションです `statistics stop` コマンド

- ハッシュを事前に計算する対象の Storage Virtual Machine （SVM）とパスを指定する必要があります。
- また、ハッシュを再帰的に計算するかどうかも指定する必要があります。
- ハッシュを再帰的に計算する場合、BranchCache サービスでは、指定されたパスの下のディレクトリツリー全体を参照し、対象となる各オブジェクトのハッシュを計算します。

## 手順

1. 必要に応じてハッシュを事前に計算します。

ハッシュを事前に計算する対象	入力するコマンド
単一のファイルまたはディレクトリ	<pre>vserver cifs branchcache hash-create -vserver vserver_name -path path -recurse false</pre>

ハッシュを事前に計算する対象	入力するコマンド
ディレクトリ構造内のすべてのファイルを再帰的に処理します	<pre>vserver cifs branchcache hash-create -vserver vserver_name -path absolute_path -recurse true</pre>

2. を使用して、ハッシュが計算されていることを確認します `statistics` コマンドを実行します

- a. の統計を表示します `hashd` 目的のSVMインスタンスのオブジェクト。 `statistics show -object hashd -instance vserver_name`
- b. コマンドを繰り返し実行して、作成済みのハッシュの数が増加していることを確認します。

#### 例

次の例は、パスにハッシュを作成します `/data SVM vs1`に格納されているすべてのファイルとサブディレクトリで、次のコマンドを実行します。

```
cluster1::> vserver cifs branchcache hash-create -vserver vs1 -path /data
-recurse true
```

```
cluster1::> statistics show -object hashd -instance vs1
```

Object: hashd

Instance: vs1

Start-time: 9/6/2012 19:09:54

End-time: 9/6/2012 19:11:15

Cluster: cluster1

Counter	Value
branchcache_hash_created	85
branchcache_hash_files_replaced	0
branchcache_hash_rejected	0
branchcache_hash_store_bytes	0
branchcache_hash_store_size	0
instance_name	vs1
node_name	node1
node_uuid	11111111-1111-1111-1111-111111111111
process_name	-

```
cluster1::> statistics show -object hashd -instance vs1
```

Object: hashd

Instance: vs1

Start-time: 9/6/2012 19:09:54

End-time: 9/6/2012 19:11:15

Cluster: cluster1

Counter	Value
branchcache_hash_created	92
branchcache_hash_files_replaced	0
branchcache_hash_rejected	0
branchcache_hash_store_bytes	0
branchcache_hash_store_size	0
instance_name	vs1
node_name	node1
node_uuid	11111111-1111-1111-1111-111111111111
process_name	-

## 関連情報

["パフォーマンス監視のセットアップ"](#)

## SVM BranchCache ハッシュストアからハッシュをフラッシュします

Storage Virtual Machine (SVM) 上の BranchCache ハッシュストアから、キャッシュされたハッシュをすべてフラッシュできます。これは、ブランチオフィスの BranchCache の設定を変更した場合に役立ちます。たとえば、最近キャッシュモードを分散キャッシュからホスト型キャッシュモードに再設定した場合は、ハッシュストアをフラッシュする必要があります。

このタスクについて

ハッシュのフラッシュ後、BranchCache 対応クライアントによって新しい要求が行われると、ONTAP によって新しいハッシュが作成されます。

ステップ

1. BranchCacheハッシュストアからハッシュをフラッシュします。 `vserver cifs branchcache hash-flush -vserver vserver_name`

```
vserver cifs branchcache hash-flush -vserver vs1
```

## BranchCache 統計を表示します

BranchCache 統計を表示すると、さまざまな目的の中でも、キャッシュが適切に機能しているかどうかの確認、キャッシュコンテンツをクライアントに提供しているかどうかの確認、新しいハッシュデータのスペースを確保するためにハッシュファイルが削除されたかどうかの確認に特に役立ちます。

このタスクについて

。 `hashd statistic` オブジェクトには、BranchCacheハッシュに関する統計情報を提供するカウンタが含まれます。。 `cifs statistic` オブジェクトには、BranchCache関連のアクティビティに関する統計情報を提供するカウンタが含まれます。これらのオブジェクトに関する情報は、 `advanced` 権限レベルで収集して表示できます。

手順

1. 権限レベルを `advanced` に設定します。 `set -privilege advanced`

```
cluster1::> set -privilege advanced
```

```
Warning: These advanced commands are potentially dangerous; use them  
only when directed to do so by support personnel.  
Do you want to continue? {y|n}: y
```

2. を使用して、BranchCache関連のカウンタを表示します `statistics catalog counter show` コマンドを実行します

統計カウンタの詳細については、このコマンドのマニュアルページを参照してください。

```
cluster1::*> statistics catalog counter show -object hashd
```



Object: hashd

Counter	Description
-----	-----
branchcache_hash_created	Number of times a request to generate BranchCache hash for a file succeeded.
branchcache_hash_files_replaced	Number of times a BranchCache hash file was deleted to make room for more recent hash data. This happens if the hash store size is exceeded.
branchcache_hash_rejected	Number of times a request to generate BranchCache hash data failed.
branchcache_hash_store_bytes	Total number of bytes used to store hash data.
branchcache_hash_store_size	Total space used to store BranchCache hash data for the Vserver.
instance_name	Instance Name
instance_uuid	Instance UUID
node_name	System node name
node_uuid	System node id

9 entries were displayed.

cluster1::\*> statistics catalog counter show -object cifs

Object: cifs

Counter	Description
-----	-----
active_searches	Number of active searches over SMB and SMB2
auth_reject_too_many	Authentication refused after too many requests were made in rapid succession
avg_directory_depth	Average number of directories crossed by SMB and SMB2 path-based commands
avg_junction_depth	Average number of junctions crossed by SMB and SMB2 path-based commands
branchcache_hash_fetch_fail	Total number of times a request to fetch

```

hash
data failed. These are failures when
attempting to read existing hash data.
It
does not include attempts to fetch hash
data
that has not yet been generated.
branchcache_hash_fetch_ok Total number of times a request to fetch
hash
data succeeded.
branchcache_hash_sent_bytes Total number of bytes sent to clients
requesting hashes.
branchcache_missing_hash_bytes
Total number of bytes of data that had
to be
read by the client because the hash for
that
content was not available on the server.
....Output truncated....

```

3. を使用して、BranchCache関連の統計を収集します `statistics start` および `statistics stop` コマンド

```

cluster1::*> statistics start -object cifs -vserver vs1 -sample-id 11
Statistics collection is being started for Sample-id: 11

cluster1::*> statistics stop -sample-id 11
Statistics collection is being stopped for Sample-id: 11

```

4. を使用して、収集したBranchCache統計を表示します `statistics show` コマンドを実行します

```
cluster1::*> statistics show -object cifs -counter  
branchcache_hash_sent_bytes -sample-id 11
```

```
Object: cifs  
Instance: vs1  
Start-time: 12/26/2012 19:50:24  
End-time: 12/26/2012 19:51:01  
Cluster: cluster1
```

Counter	Value
branchcache_hash_sent_bytes	0
branchcache_hash_sent_bytes	0
branchcache_hash_sent_bytes	0
branchcache_hash_sent_bytes	0

```
cluster1::*> statistics show -object cifs -counter  
branchcache_missing_hash_bytes -sample-id 11
```

```
Object: cifs  
Instance: vs1  
Start-time: 12/26/2012 19:50:24  
End-time: 12/26/2012 19:51:01  
Cluster: cluster1
```

Counter	Value
branchcache_missing_hash_bytes	0
branchcache_missing_hash_bytes	0
branchcache_missing_hash_bytes	0
branchcache_missing_hash_bytes	0

5. admin 権限レベルに戻ります。set -privilege admin

```
cluster1::*> set -privilege admin
```

## 関連情報

[統計情報を表示します](#)

["パフォーマンス監視のセットアップ"](#)

**BranchCache** グループポリシーオブジェクトがサポートされます

ONTAP BranchCache では、BranchCache のグループポリシーオブジェクト（GPO）

をサポートしており、特定の BranchCache の設定パラメータを一元的に管理できます。BranchCache の GPO には、BranchCache のハッシュの発行 GPO と BranchCache のハッシュバージョンサポート GPO の 2 つがあります。

- \* BranchCache のハッシュの発行 GPO \*

BranchCacheのハッシュの発行GPOはに対応します `-operating-mode` パラメータGPO の更新が行われると、グループポリシーが適用される組織単位（OU）に含まれる Storage Virtual Machine（SVM）オブジェクトにこの値が適用されます。

- \* BranchCache のハッシュバージョンサポート \*

BranchCacheのハッシュバージョンサポートGPOはに対応します `-versions` パラメータGPO の更新が行われると、グループポリシーが適用される組織単位に含まれる SVM オブジェクトにこの値が適用されます。

## 関連情報

### CIFS サーバへのグループポリシーオブジェクトの適用

**BranchCache** グループポリシーオブジェクトに関する情報を表示します

CIFS サーバの Group Policy Object（GPO；グループポリシーオブジェクト）設定に関する情報を表示して、CIFS サーバが属しているドメインで BranchCache GPO が定義されているかどうか、定義されている場合は許可されている設定を確認できます。また、BranchCache GPO 設定が CIFS サーバに適用されているかどうかも確認できます。

#### このタスクについて

CIFS サーバが属しているドメイン内で GPO 設定が定義されていても、CIFS 対応の Storage Virtual Machine（SVM）が含まれる Organizational Unit（OU；組織単位）に適用されているとは限りません。適用される GPO 設定は、CIFS 対応の SVM に適用されているすべての定義済み GPO の一部です。GPO を介して適用された BranchCache 設定は、CLI を介して適用された設定よりも優先さ

#### 手順

1. を使用して、Active Directoryドメインに対して定義されているBranchCache GPO設定を表示します  
`vserver cifs group-policy show-defined` コマンドを実行します



この例で表示されているのは、コマンドで出力されるフィールドの一部です。出力は省略されています。

```
cluster1::> vserver cifs group-policy show-defined -vserver vs1
```

```
Vserver: vs1
```

```
-----
```

```
    GPO Name: Default Domain Policy
```

```
    Level: Domain
```

```
    Status: enabled
```

```
Advanced Audit Settings:
```

```
    Object Access:
```

```
        Central Access Policy Staging: failure
```

```
Registry Settings:
```

```
    Refresh Time Interval: 22
```

```
    Refresh Random Offset: 8
```

```
    Hash Publication Mode for BranchCache: per-share
```

```
    Hash Version Support for BranchCache: version1
```

```
[...]
```

```
    GPO Name: Resultant Set of Policy
```

```
    Status: enabled
```

```
Advanced Audit Settings:
```

```
    Object Access:
```

```
        Central Access Policy Staging: failure
```

```
Registry Settings:
```

```
    Refresh Time Interval: 22
```

```
    Refresh Random Offset: 8
```

```
    Hash Publication for Mode BranchCache: per-share
```

```
    Hash Version Support for BranchCache: version1
```

```
[...]
```

2. を使用して、CIFSサーバに適用されているBranchCache GPO設定を表示します vserver cifs group-policy show-applied コマンドを実行します`



この例で表示されているのは、コマンドで出力されるフィールドの一部です。出力は省略されています。

```
cluster1::> vsriver cifs group-policy show-applied -vsriver vs1
```

```
Vsriver: vs1
```

```
-----
```

```
    GPO Name: Default Domain Policy
```

```
        Level: Domain
```

```
        Status: enabled
```

```
Advanced Audit Settings:
```

```
    Object Access:
```

```
        Central Access Policy Staging: failure
```

```
Registry Settings:
```

```
    Refresh Time Interval: 22
```

```
    Refresh Random Offset: 8
```

```
    Hash Publication Mode for BranchCache: per-share
```

```
    Hash Version Support for BranchCache: version1
```

```
[...]
```

```
    GPO Name: Resultant Set of Policy
```

```
        Level: RSOP
```

```
Advanced Audit Settings:
```

```
    Object Access:
```

```
        Central Access Policy Staging: failure
```

```
Registry Settings:
```

```
    Refresh Time Interval: 22
```

```
    Refresh Random Offset: 8
```

```
    Hash Publication Mode for BranchCache: per-share
```

```
    Hash Version Support for BranchCache: version1
```

```
[...]
```

## 関連情報

[CIFS サーバ上で GPO サポートを有効または無効にします](#)

**SMB** 共有で **BranchCache** を無効にします

**SMB** 共有で **BranchCache** を無効にする手順の概要

特定の SMB 共有で BranchCache キャッシュサービスを提供する必要がなくなったが、あとでそれらの共有でキャッシュサービスが必要になる可能性がある場合は、共有ごとに BranchCache を無効にすることができます。すべての共有でキャッシュを提供するように BranchCache を設定しているが、一時的にすべてのキャッシュサービスを無効にする必要がある場合は、BranchCache 設定を変更してすべての共有で自動キャッシュを停止することができます。

SMB 共有で有効になっていた BranchCache をあとから無効にすると、ONTAP による要求元クライアントへのメタデータの送信が中止されます。データが必要なクライアントは、コンテンツサーバ (Storage Virtual

Machine（SVM）上の CIFS サーバ）から直接データを取得します。

関連情報

[BranchCache が有効な SMB 共有の設定](#)

単一の **SMB** 共有で **BranchCache** を無効にします

キャッシュコンテンツを使用できるようにしていた特定の共有でキャッシュサービスを提供する必要がなくなった場合は、既存の SMB 共有で BranchCache を無効にすることができます。

ステップ

1. 次のコマンドを入力します。

```
vserver cifs share properties remove -vserver  
vserver_name -share-name share_name -share-properties branchcache
```

BranchCache 共有プロパティが削除されます。適用されているその他の共有プロパティは有効なままです。

例

次のコマンドは、「data2」という名前の既存の SMB 共有で BranchCache を無効にします。

```
cluster1::> vservice cifs share show -vservice vs1 -share-name data2
```

```

        Vservice: vs1
        Share: data2
CIFS Server NetBIOS Name: VS1
        Path: /data2
    Share Properties: oplocks
                     browsable
                     changenotify
                     attributecache
                     branchcache
    Symlink Properties: -
    File Mode Creation Mask: -
    Directory Mode Creation Mask: -
        Share Comment: -
            Share ACL: Everyone / Full Control
File Attribute Cache Lifetime: 10s
        Volume Name: -
        Offline Files: manual
Vscan File-Operations Profile: standard
```

```
cluster1::> vservice cifs share properties remove -vservice vs1 -share-name
data2 -share-properties branchcache
```

```
cluster1::> vservice cifs share show -vservice vs1 -share-name data2
```

```

        Vservice: vs1
        Share: data2
CIFS Server NetBIOS Name: VS1
        Path: /data2
    Share Properties: oplocks
                     browsable
                     changenotify
                     attributecache
    Symlink Properties: -
    File Mode Creation Mask: -
    Directory Mode Creation Mask: -
        Share Comment: -
            Share ACL: Everyone / Full Control
File Attribute Cache Lifetime: 10s
        Volume Name: -
        Offline Files: manual
Vscan File-Operations Profile: standard
```



すべての **SMB** 共有での自動キャッシュを停止します

Storage Virtual Machine（SVM）のすべての SMB 共有に対して BranchCache キャッシュを自動的に有効にするように設定している場合、BranchCache の設定を変更することで、すべての SMB 共有に対するコンテンツの自動キャッシュを停止することができます。

このタスクについて

すべての SMB 共有に対する自動キャッシュを停止するには、BranchCache の動作モードを共有ごとのキャッシュに変更します。

手順

1. すべてのSMB共有で自動キャッシュを停止するようにBranchCacheを設定します。 `vserver cifs branchcache modify -vserver vserver_name -operating-mode per-share`
2. BranchCacheの設定が正しいことを確認します。 `vserver cifs branchcache show -vserver vserver_name`

例

次のコマンドは、Storage Virtual Machine（SVM、旧 Vserver）vs1 の BranchCache 設定を変更して、すべての SMB 共有に対する自動キャッシュを停止します。

```
cluster1::> vserver cifs branchcache modify -vserver vs1 -operating-mode
per-share

cluster1::> vserver cifs branchcache show -vserver vs1

                                Vserver: vs1
        Supported BranchCache Versions: enable_all
                                Path to Hash Store: /hash_data
        Maximum Size of the Hash Store: 20GB
Encryption Key Used to Secure the Hashes: -
        CIFS BranchCache Operating Modes: per_share
```

**SVM** で **BranchCache** を有効または無効にします

**CIFS** サーバで **BranchCache** を無効または再度有効にしたときの動作

BranchCache を設定したあとに、ブランチオフィスのクライアントがキャッシュされたコンテンツを使用できないようにするには、CIFS サーバでキャッシュを無効にします。BranchCache を無効にするときは、それを実行した場合の動作について理解しておく必要があります

BranchCache を無効にすると、ONTAP によるハッシュの計算や要求元クライアントへのメタデータの送信が行われなくなります。ただし、ファイルアクセスは中断されません。以降に、BranchCache 対応クライアント ONTAP からアクセスするコンテンツのメタデータ情報を要求すると、Microsoft のエラーが返されます。この場合は、クライアントでもう一度要求を送信して、実際のコンテンツを要求します。これに対する応


答として、CIFS サーバから Storage Virtual Machine（SVM）に格納されている実際のコンテンツが送信されます。

CIFS サーバで BranchCache を無効にしたあとは、SMB 共有で BranchCache の機能がアドバタイズされなくなります。新しい SMB 接続でデータにアクセスするには、通常の SMB 読み取り要求を行います。

BranchCache は、CIFS サーバでいつでも再度有効にすることができます。

- BranchCache ONTAP を無効にしてもハッシュストアは削除されないため、要求されたハッシュがまだ有効であれば、BranchCache を再度有効にしたあとに、格納されたハッシュを使用してハッシュの要求に応答することができます。
- BranchCache 対応の共有に対する SMB 接続を確立したクライアントで接続を確立したときに BranchCache が無効になっていたクライアントの場合には、以降に BranchCache を再度有効にしても、BranchCache のサポートは有効になりません。

これは、SMB セッションのセットアップ時に共有に対する BranchCache のサポートが通知されるから ONTAP です。BranchCache を無効にしたときに BranchCache 対応の共有に対するセッションを確立していた場合、その共有のキャッシュされたコンテンツを使用するには、いったん切断してから再接続する必要があります。



CIFS サーバで BranchCache を無効にしたあとにハッシュストアを保存しておく必要がない場合は、手動で削除することができます。BranchCache を再度有効にするときは、ハッシュストアのディレクトリが存在することを確認する必要があります。BranchCache を再度有効にすると、BranchCache 対応の共有で BranchCache の機能がアドバタイズされるようになります。BranchCache 対応クライアントから新しい要求が行われると、ONTAP によって新しいハッシュが作成されます。

**BranchCache を有効または無効にします**

Storage Virtual Machine（SVM）で BranchCache を無効にするには、BranchCache の動作モードをに変更します disabled。BranchCache サービスを共有単位で提供するか、すべての共有で自動的に提供するように動作モードを変更すると、いつでも BranchCache を有効にすることができます。

手順

1. 該当するコマンドを実行します。

状況	入力するコマンド
BranchCache を無効にする	<code>vserver cifs branchcache modify -vserver vserver_name -operating-mode disable</code>
共有ごとに BranchCache を有効にします	<code>vserver cifs branchcache modify -vserver vserver_name -operating-mode per-share</code>

状況	入力するコマンド
すべての共有で BranchCache を有効にします	<code>vserver cifs branchcache modify -vserver vs1 -operating-mode all-shares</code>

2. BranchCacheの動作モードが目的の設定になっていることを確認します。 `vserver cifs branchcache show -vserver vs1`

例

次の例は、SVM vs1 で BranchCache を無効にします。

```
cluster1::> vserver cifs branchcache modify -vserver vs1 -operating-mode
disable

cluster1::> vserver cifs branchcache show -vserver vs1

Vserver: vs1
Supported BranchCache Versions: enable_all
Path to Hash Store: /hash_data
Maximum Size of the Hash Store: 20GB
Encryption Key Used to Secure the Hashes: -
CIFS BranchCache Operating Modes: disable
```

**SVM の BranchCache 設定を削除します**

**BranchCache 設定を削除した場合の動作**

BranchCache を設定したあとに、Storage Virtual Machine（SVM）からのキャッシュされたコンテンツの提供を中止する場合は、CIFS サーバで BranchCache 設定を削除します。設定を削除するときは、それを実行した場合の動作について理解しておく必要があります。

設定を削除すると、ONTAP によってその SVM の設定情報がクラスタから削除され、BranchCache サービスが停止します。SVM のハッシュストアについては、ONTAP で削除するかどうかを選択することができます。

BranchCache 設定を削除しても、BranchCache 対応クライアントによるアクセスは中断されません。以降に、BranchCache 対応クライアントから既存の SMB 接続でキャッシュ済みのコンテンツのメタデータ情報を要求すると、ONTAP は Microsoft のエラーを返します。この場合は、クライアントでもう一度要求を送信して、実際のコンテンツを要求します。これに対する応答として、CIFS サーバから SVM に格納されている実際のコンテンツが送信されます。

BranchCache 設定を削除すると、SMB 共有で BranchCache の機能がアドバタイズされなくなります。キャッシュされていないコンテンツに新しい SMB 接続でアクセスするには、通常の SMB 読み取り要求を行います。

**BranchCache** 設定を削除します

Storage Virtual Machine（SVM）で BranchCache サービスの削除に使用するコマンドは、既存のハッシュを削除するか、保持するかによって異なります。

ステップ

1. 該当するコマンドを実行します。

状況	入力するコマンド
BranchCache 設定を削除し、既存のハッシュを削除します	<code>vserver cifs branchcache delete -vserver vserver_name -flush-hashes true</code>
BranchCache 設定を削除するが、既存のハッシュは保持する	<code>vserver cifs branchcache delete -vserver vserver_name -flush-hashes false</code>

例

次の例は、SVM vs1 で BranchCache 設定を削除し、既存のハッシュをすべて削除します。

```
cluster1::> vserver cifs branchcache delete -vserver vs1 -flush-hashes  
true
```

リバートした場合の **BranchCache** の動作

ONTAP を BranchCache がサポートされないリリースにリバートするときは、それを実行した場合の動作について理解しておくことが重要です。

- ONTAP を BranchCache がサポートされないバージョンにリバートすると、BranchCache 対応クライアントに対して SMB 共有で BranchCache の機能がアドバタイズされなくなります。そのため、クライアントからハッシュ情報が要求されることはありません。

代わりに、通常の SMB 読み取り要求を使用して実際のコンテンツを要求します。これに対する応答として、SMBサーバからStorage Virtual Machine（SVM）に格納されている実際のコンテンツが送信されます。

- ハッシュストアをホストするノードを BranchCache がサポートされないリリースにリバートする場合、リバート時に出力されるコマンドを使用して、ストレージ管理者が手動で BranchCache の設定をリバートする必要があります。

このコマンドは、BranchCache の設定とハッシュを削除します。

リバートの完了後、必要に応じて、ハッシュストアが格納されていたディレクトリを手動で削除できます。

関連情報

### Microsoft リモートコピーのパフォーマンスを向上

Microsoft リモートコピーのパフォーマンスの概要を改善します

Microsoft Offloaded Data Transfer (ODX ; オフロードデータ転送) は、\_コピーオフロード\_とも呼ばれ、この機能を使用すると、互換性があるストレージデバイス内やストレージデバイス間で、ホストコンピュータを介さずにデータを直接転送できます。

ONTAPでは、SMBプロトコルとSANプロトコルの両方でODXがサポートされます。ソースとデスティネーションのどちらについても、CIFS サーバと LUN の両方に対応しています。

ODX 以外のファイル転送では、ソースからデータが読み取られ、ネットワーク経由でクライアントコンピュータに転送されます。クライアントコンピュータは、データをネットワーク経由でデスティネーションに転送します。つまり、クライアントコンピュータはソースからデータを読み取り、デスティネーションに書き込みます。ODX ファイル転送では、データはソースからデスティネーションに直接コピーされます。

ODX オフロードコピーはソースストレージとデスティネーションストレージの間で直接実行されるため、パフォーマンスが大幅に向上します。実現するパフォーマンスの向上には、ソースとデスティネーションの間のコピー時間の短縮、クライアントでのリソース使用量 (CPU、メモリ) の削減、ネットワーク I/O 帯域幅の使用量の削減などが挙げられます。

SMB 環境では、この機能は、クライアントとストレージサーバの両方で SMB 3.0 および ODX 機能がサポートされている場合にのみ使用できます。SAN 環境では、この機能は、クライアントとストレージサーバの両方で ODX 機能がサポートされている場合にのみ使用できます。ODX がサポートされていて有効になっているクライアントコンピュータでは、ファイルの移動やコピーを行う際に、オフロードファイル転送が自動的にかつ透過的に使用されます。ODX は、ファイルをエクスプローラでドラッグアンドドロップしたか、コマンドラインのファイルコピーコマンドを使用したか、クライアントアプリケーションによってファイルコピー要求が開始されたかに関係なく使用されます。

### 関連情報

[Auto Location で SMB 自動ノードリファールを提供することで、クライアントの応答時間を改善します](#)

["Microsoft Hyper-V および SQL Server 向けの SMB の設定"](#)

### ODX の仕組み

ODX コピーオフロードでは、トークンベースのメカニズムを使用して、ODX 対応の CIFS サーバ内または CIFS サーバ間でデータの読み取りおよび書き込みを行います。CIFS サーバは、ホストを介してデータをルーティングするのではなく、データを表す小さなトークンをクライアントに送信します。ODX クライアントがそのトークンをデスティネーションサーバに提示すると、サーバはそのトークンで表されるデータをソースからデスティネーションに転送できます。

ODX クライアントは、CIFS サーバが ODX 対応であると認識すると、ソースファイルを開いて CIFS サーバのトークンを要求します。デスティネーションファイルを開いたあと、クライアントはトークンを使用して、データをソースからデスティネーションに直接コピーするようにサーバに指示します。

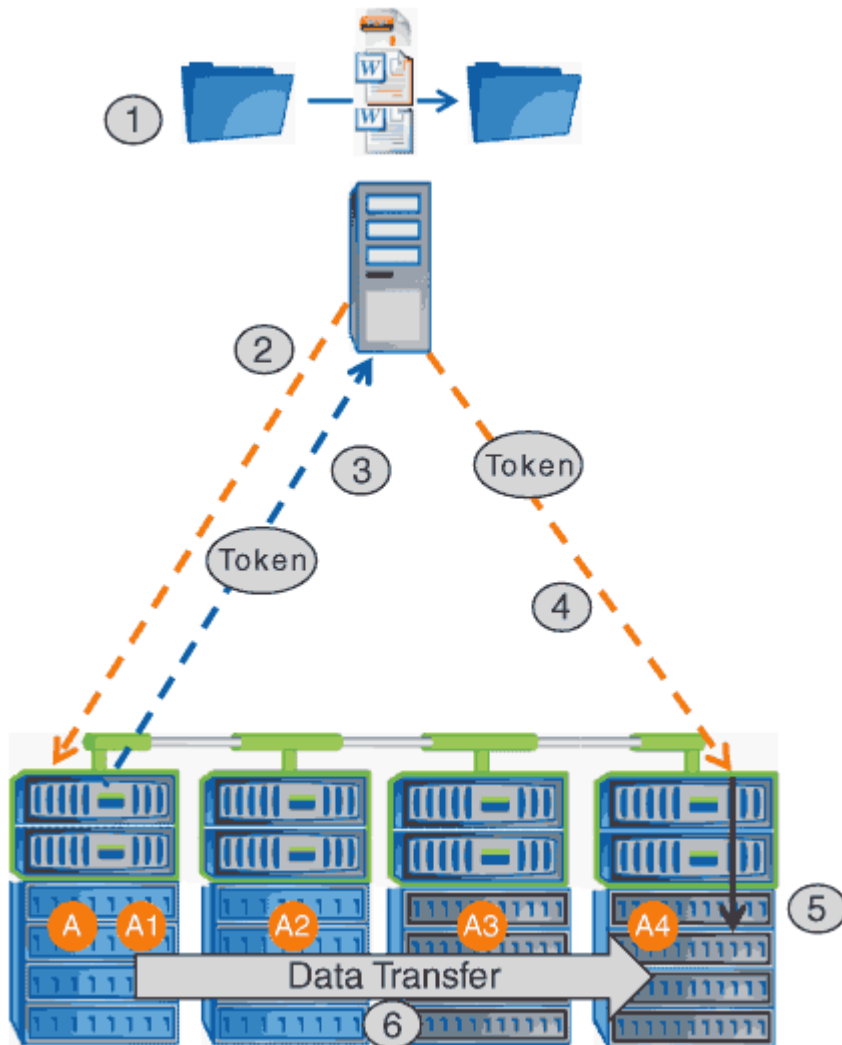


ソースとデスティネーションは、コピー処理の範囲に応じて、同じ Storage Virtual Machine (SVM) 上に存在する場合も異なる SVM 上に存在する場合もあります。

トークンは、データのポイントインタイム表現として機能します。たとえば、ストレージ間でデータをコピーする場合、データセグメントを表すトークンが要求元クライアントに返され、そのトークンをクライアントがデスティネーションにコピーするため、クライアントを介して基盤となるデータをコピーする必要があります。

ONTAP では、8MB のデータを表すトークンがサポートされます。8MB を超える ODX コピーは、8MB のデータを表すトークンを複数使用して実行されます。

次の図で、ODX コピー処理に関連する手順について説明します。



1. エクスプローラを使用するか、コマンドラインインターフェイスを使用するか、仮想マシンの移行の一環として、ユーザがファイルをコピーまたは移動します。または、アプリケーションによってファイルのコピーまたは移動が開始されます。
2. ODX 対応のクライアントが、この転送要求を ODX 要求に自動的に変換します。

CIFS サーバに送信される ODX 要求には、トークン要求が含まれています。

3. CIFS サーバで ODX が有効になっていて、接続が SMB 3.0 経由の場合は、ソースのデータを論理的に表したものであるトークンが CIFS サーバによって生成されます。

4. クライアントは、データを表すトークンを受信し、書き込み要求を使用してそのトークンをデスティネーション CIFS サーバに送信します。

ネットワーク経由でソースからクライアントにコピーされ、クライアントからデスティネーションにコピーされるのは、このデータだけです。

5. トークンがストレージサブシステムに送信されます。
6. コピーまたは移動が SVM によって内部的に実行されます。

コピーまたは移動されるファイルが 8MB より大きい場合、コピーを実行するには複数のトークンが必要になります。コピーが完了するまで、必要に応じて手順 2~6 を実行します。



ODX オフロードコピーで障害が発生した場合、コピーまたは移動処理は、その処理の従来の読み取りおよび書き込みにフォールバックされます。同様に、デスティネーション CIFS サーバで ODX がサポートされていない場合、または ODX が無効になっている場合は、コピーまたは移動処理は、その処理の従来の読み取りおよび書き込みにフォールバックされます。

#### ODX を使用するための要件

Storage Virtual Machine (SVM) で ODX によるコピーオフロードを使用する前に、一定の要件について確認しておく必要があります。

#### ONTAP のバージョンの要件

ONTAP の各リリースで ODX によるコピーオフロードがサポートされます。

#### SMB のバージョンの要件

- ONTAP では、SMB 3.0 以降で ODX がサポートされます。
- ODX を有効にする前に、CIFS サーバで SMB 3.0 を有効にしておく必要があります。
  - ODX を有効にすると、SMB 3.0 も有効になります（まだ有効になっていない場合）。
  - SMB 3.0 を無効にすると ODX も無効になります。

#### Windows サーバとクライアントの要件

ODX によるコピーオフロードを使用するには、Windows クライアントでこの機能がサポートされている必要があります。

。"NetApp Interoperability Matrix を参照してください"サポートされているWindowsクライアントに関する最新情報が含まれています。

#### ボリューム要件：

- ソースボリュームは 1.25GB 以上でなければなりません。
- 圧縮されたボリュームを使用する場合は、圧縮形式をアダプティブにする必要があります。サポートされる圧縮グループサイズは 8K のみです。

二次圧縮形式はサポートされません

コピーオフロードに ODX を使用する場合は、一定のガイドラインについて理解しておく必要があります。たとえば、ODX を使用できるボリュームのタイプや、クラスタ内およびクラスタ間の ODX に関する考慮事項を把握しておく必要があります。

#### ボリュームガイドライン

- 次のようなボリューム設定では、コピーオフロードに ODX を使用できません。

- ソースボリュームサイズが 1.25GB 未満である必要があります

ODX を使用するには、ボリュームサイズが 1.25GB 以上である必要があります。

- 読み取り専用ボリューム

負荷共有ミラー、SnapMirror デスティネーションボリューム、または SnapVault デスティネーションボリュームに存在するファイルやフォルダには ODX を使用できません。

- ソースボリュームが重複排除されていない場合

- ODX コピーはクラスタ内のコピーにのみ対応しています。

ODX を使用して、ファイルまたはフォルダを別のクラスタ内のボリュームにコピーすることはできません。

#### その他のガイドライン

- SMB 環境では、コピーオフロードに ODX を使用するには、256KB 以上のファイルである必要があります。

サイズの小さいファイルは、従来のコピー処理を使用して転送されます。

- ODX コピーオフロードでは、コピープロセスの一環として重複排除が実行されます。

データのコピーまたは移動時に SVM のボリュームで重複排除が発生しないようにする場合は、その SVM で ODX コピーオフロードを無効にする必要があります。

- データ転送を実行するアプリケーションは、ODX をサポートするように記述する必要があります。

ODX がサポートされるアプリケーション処理は次のとおりです。

- Virtual Hard Disk（VHD；仮想ハードディスク）の作成および変換、Snapshot コピーの管理、仮想マシン間でのファイルのコピーなど、Hyper-V の管理処理
- エクスプローラでの操作
- Windows PowerShell の copy コマンド
- Windows コマンドプロンプトの copy コマンド

Windows コマンドプロンプトの Robocopy は ODX をサポートしています。





ODX をサポートする Windows サーバまたはクライアント上でアプリケーションを実行する必要があります。

+

Windows サーバおよびクライアントでサポートされる ODX アプリケーションの詳細については、Microsoft TechNet ライブラリを参照してください。

#### 関連情報

"Microsoft TechNet ライブラリ : [technet.microsoft.com/en-us/library/](https://technet.microsoft.com/en-us/library/)"

#### ODX のユースケース

SVM で ODX を使用する前に、どのような場合にパフォーマンスを向上できるかを判断できるようにユースケースについて確認しておく必要があります。

ODX をサポートする Windows サーバおよびクライアントでは、リモートサーバ間でデータをコピーする際に、デフォルトでコピーオフロードが使用されます。Windows サーバまたはクライアントで ODX がサポートされていない場合や、ODX コピーオフロードが任意の時点で失敗した場合は、コピーまたは移動処理が従来の読み取りと書き込みの処理を使用して実行されます。

ODX コピーおよび移動の使用は、以下のユースケースでサポートされます。

- ボリューム内

ソースとデスティネーションのファイルまたは LUN は、同じボリューム内にあります。

- ボリュームが異なり、ノードと SVM は同じです

ソースとデスティネーションのファイルまたは LUN は、同じノード上の異なるボリュームにあります。データは同じ SVM に所有されます。

- ボリュームとノードが異なり、SVM は同じです

ソースとデスティネーションのファイルまたは LUN は、異なるノード上の異なるボリュームにあります。データは同じ SVM に所有されます。

- SVM が異なり、ノードは同じです

ソースとデスティネーションのファイルまたは LUN は、同じノード上の異なるボリュームにあります。データは異なる SVM に所有されます。

- SVM とノードが異なります

ソースとデスティネーションのファイルまたは LUN は、異なるノード上の異なるボリュームにあります。データは異なる SVM に所有されます。

- クラスタ間

ソース LUN とデスティネーション LUN は、異なるクラスタの異なるノード上の異なるボリュームにあります。これは SAN でのみサポートされ、CIFS では機能しません。

その他にも、いくつかの特殊なユースケースがあります。

- ONTAP の ODX の実装で ODX を使用すると、SMB 共有と FC / iSCSI で接続された仮想ドライブとの間でファイルをコピーできます。

SMB 共有と LUN が同じクラスタにある場合は、Windows エクスプローラ、Windows CLI または PowerShell、Hyper-V、または ODX をサポートするその他のアプリケーションを使用して、SMB 共有と接続された LUN 間の ODX コピーオフロードを使用してファイルをシームレスにコピーまたは移動できます。

- Hyper-V では、さらに次のようなユースケースでも ODX コピーオフロードが使用されます。
  - Hyper-V で ODX コピーオフロードのパススルーを使用して、仮想ハードディスク（VHD）ファイル内および VHD ファイル間でのデータのコピー、または同じクラスタ内のマッピングされた SMB 共有と接続された iSCSI LUN の間でのデータのコピーを実行できます。

これにより、ゲストオペレーティングシステムからのコピーを基盤となるストレージに渡すことができます。

- 容量固定 VHD を作成する際に、ODX を使用して、既知の初期化済みトークンによってディスクを初期化します。
- ソースとデスティネーションのストレージが同じクラスタにある場合に、ODX コピーオフロードを使用して、仮想マシンのストレージを移行します。



Hyper-V での ODX コピーオフロードのパススルーの用途を活用するには、ゲストオペレーティングシステムで ODX がサポートされている必要があります。また、ゲストオペレーティングシステムのディスクが、ODX をサポートするストレージ（SMB または SAN）から作成された SCSI ディスクである必要があります。ゲストオペレーティングシステムのディスクが IDE ディスクの場合、ODX のパススルーはサポートされません。

## ODXの有効化または無効化

Storage Virtual Machine（SVM）で ODX を有効または無効にすることができます。デフォルトでは、SMB 3.0 が有効になっている場合は ODX コピーオフロードのサポートも有効になります。

作業を開始する前に

SMB 3.0 が有効になっている必要があります。

このタスクについて

SMB 3.0 を無効にすると、ONTAP でも SMB ODX が無効になります。SMB 3.0 を再度有効にする場合は、SMB ODX を手動で再度有効にする必要があります。

手順

1. 権限レベルを advanced に設定します。 `set -privilege advanced`
2. 次のいずれかを実行します。

ODX コピーオフロードの設定	入力するコマンド
有効	<code>vserver cifs options modify -vserver vserver_name -copy-offload-enabled true</code>
無効	<code>vserver cifs options modify -vserver vserver_name -copy-offload-enabled false</code>

3. admin 権限レベルに戻ります。 `set -privilege admin`

例

次の例は、SVM vs1 で ODX コピーオフロードを有効にします。

```
cluster1::> set -privilege advanced
Warning: These advanced commands are potentially dangerous; use them
only when directed to do so by technical support personnel.
Do you wish to continue? (y or n): y

cluster1::*> vserver cifs options modify -vserver vs1 -copy-offload
-enabled true

cluster1::*> set -privilege admin
```

関連情報

[使用できる SMB サーバオプション](#)

**Auto Location** で **SMB 自動ノードリファール**を提供することで、クライアントの応答時間を短縮します

**Auto Location** の概要を示す **SMB 自動ノードリファール**を提供することで、クライアントの応答時間を改善します

Auto Location は、SMB 自動ノードリファールを使用して Storage Virtual Machine (SVM) での SMB クライアントのパフォーマンスを向上します。自動ノードリファールは、要求しているクライアントを、データが存在するボリュームをホストしているノード SVM 上の LIF に自動的にリダイレクトします。これにより、クライアントの応答時間を改善できます。

SMB クライアントが SVM 上でホストされている SMB 共有に接続するときに、要求されたデータを所有していないノード上の LIF を使用して接続することがあります。クライアントが接続しているノードは、クラスタネットワークを使用して別のノードが所有しているデータにアクセスします。SMB 接続が要求されたデータを含むノード上にある LIF を使用している場合、クライアントへの応答時間が短縮されます。

- ONTAP では、Microsoft の DFS リファールを使用して、要求されたファイルやフォルダがネームスペース内の別の場所でホストされていることを SMB クライアントに通知することで、この機能を実現します。

ノードがリファールを作成するのは、データを含むノード上に SVM の LIF が 1 つあることを特定した場合です。

- 自動ノードリファールでは、IPv4 と IPv6 の LIF の IP アドレスがサポートされます。
- リファールは、クライアントの接続に使用されている共有のルートの場所に基づいて作成されます。
- リファールは SMB ネゴシエーション中に発生します。

リファールは、接続が確立される前に作成されます。ONTAP がターゲットノードに参照先の SMB クライアントを通知したあと、接続が確立され、それ以降、クライアントはその参照先 LIF パスを介してデータにアクセスします。これにより、クライアントにはより高速なデータアクセスが提供され、クラスタの余分な通信も回避されます。



共有が複数のジャンクションポイントにまたがっていて、ジャンクションの一部が他のノードに格納されているボリュームを参照する場合、共有内のデータは複数のノードに分散されます。ONTAP は共有のルートに対してローカルなリファールを提供するため、ONTAP では、これらのローカルでないボリュームに含まれるデータを取得する際にクラスタネットワークを使用する必要があります。このタイプのネームスペースアーキテクチャでは、自動ノードリファールによる大幅なパフォーマンス向上は望めない場合があります。

データをホストするノードに使用可能な LIF がない場合、ONTAP は、クライアントが選択した LIF を使用して接続を確立します。ファイルが SMB クライアントによって開かれると、クライアントは参照された同じ接続を介してファイルへのアクセスを継続します。

何らかの理由で CIFS サーバがリファールを作成できない場合でも、SMB サービスが中断されることはありません。自動ノードリファールが有効でない場合と同様に SMB 接続が確立されます。

#### 関連情報

#### [Microsoft リモートコピーのパフォーマンスの向上](#)

#### 自動ノードリファールの使用に関する要件とガイドライン

SMB 自動ノードリファール（別名 `_autolocation_`）を使用する前に、この機能をサポートする ONTAP のバージョンなど、一定の要件について理解しておく必要があります。サポートされる SMB プロトコルのバージョンやその他の特別なガイドラインについても確認しておく必要があります。

#### ONTAP のバージョンとライセンスの要件

- クラスタ内のすべてのノードで、自動ノードリファールがサポートされているバージョンの ONTAP が実行されている必要があります。
- オートロケーションを使用する SMB 共有でワイドリンクが有効になっている必要があります。
- CIFS のライセンスが有効になっていて、SVM に SMB サーバが配置されている必要があります。SMB ライセンスは含まれています。"ONTAP One"。ONTAP Oneをお持ちでなく、ライセンスがインストールされていない場合は、営業担当者にお問い合わせください。

## SMB プロトコルのバージョン

- SVM について ONTAP は、すべてのバージョンの SMB で自動ノードリファールがサポートされます。

## SMB クライアントの要件

SMB 自動ノードリファールは、ONTAP でサポートされるすべての Microsoft クライアントでサポートされます。

ONTAP でサポートされる Windows クライアントの最新情報については、Interoperability Matrix を参照してください。

["NetApp Interoperability Matrix Tool で確認できます"](#)

## データ LIF の要件

データ LIF を SMB クライアントのリファールとして使用する可能性がある場合は、NFS と CIFS の両方を有効にしたデータ LIF を作成する必要があります。

自動ノードリファールは、ターゲットノードのデータ LIF で NFS プロトコルまたは SMB プロトコルのどちらかが有効になっていない場合は機能しないことがあります。

この要件が満たされない場合でも、データアクセスには影響しません。SMB クライアントは、SVM への接続に使用した元の LIF を使用して共有をマッピングします。

## 参照された SMB 接続を確立する際の NTLM 認証の要件

CIFS サーバを含むドメインと自動ノードリファールを使用するクライアントを含むドメインで、NTLM 認証が許可されている必要があります。

リファールを作成する際には、SMB サーバから Windows クライアントに参照先の IP アドレスが渡されます。IP アドレスを使用した接続には NTLM 認証が使用されるため、参照された接続に対しては Kerberos 認証は実行されません。

これは、Windows クライアントが Kerberos で使用されるサービスプリンシパル名（の形式）を作成できないためです（service/NetBIOS name および service/FQDN）。これは、クライアントがサービスに Kerberos チケットを要求できないことを意味します。

自動ノードリファールでホームディレクトリ機能を使用する場合のガイドラインを次に示します

ホームディレクトリ共有プロパティを有効にして共有を設定した場合、ホームディレクトリの設定で 1 つ以上のホームディレクトリ検索パスを設定できます。この検索パスで、SVM のボリュームを含む各ノードに格納されているボリュームを指定できます。クライアントはリファールを受け取り、使用できるアクティブなローカルデータ LIF があれば、ホームユーザのホームディレクトリに対してローカルな、参照された LIF を介して接続します。

SMB 1.0 クライアントで自動ノードリファールを有効にして動的ホームディレクトリにアクセスする場合は注意が必要です。SMB 1.0 クライアントでは、認証を行う前、つまり SMB サーバに対してユーザの名前が指定されていない段階で自動ノードリファールが必要になるからです。SMB 1.0 クライアントで SMB ホームディレクトリへのアクセスが正常に機能するのは、次の条件に該当する場合です。

- SMB ホームディレクトリは、「%w」（Windows ユーザ名）または「%u」（マッピングされた UNIX ユーザ名）のような単純な名前を使用するように設定されており、「%d\%w」（ドメイン名\ユーザ名

) のようなドメイン名形式の名前では使用されません。

- ・ホーム・ディレクトリ共有を作成するときに、CIFS ホーム・ディレクトリ共有名は変数（「%w」または「%u」）で設定され、「home」などの静的な名前では設定されません。

SMB 2.x クライアントと SMB 3.0 クライアントの場合は、自動ノードリファールを使用してホームディレクトリにアクセスする際に特別なガイドラインはありません。

参照接続が確立されている **CIFS** サーバで自動ノードリファールを無効にする場合のガイドラインを次に示します

オプションを有効にしたあとに自動ノードリファールを無効にした場合、参照 LIF に現在接続されているクライアントでは参照接続が維持されます。ONTAP では SMB 自動ノードリファールのメカニズムとして DFS リファールを使用しているため、オプションを無効にしたあとも、参照接続用にクライアントにキャッシュされている DFS リファールがタイムアウトするまでは参照 LIF に再接続できます。これは、自動ノードリファールがサポートされないバージョンの ONTAP にリポートした場合も同様です。クライアントは、クライアントのキャッシュから DFS リファールがタイムアウトするまで、引き続きリファールを使用します。

オートロケーションは、SMB 自動ノードリファールを使用してクライアントに SVM のデータボリュームを所有しているノード上の LIF を参照させることで、SMB クライアントのパフォーマンスを向上させます。SMB クライアントが SVM 上でホストされている SMB 共有に接続するときに、要求されたデータを所有しておらず、クラスタインターコネクトネットワークを使用してデータを取得しているノード上の LIF を使用して接続することがあります。SMB 接続が要求されたデータを含むノード上にある LIF を使用している場合、クライアントへの応答時間が短縮されます。

ONTAP では、Microsoft の分散ファイルシステム（DFS）リファールを使用して、要求されたファイルやフォルダがネームスペース内の別の場所でホストされていることを SMB クライアントに通知することで、この機能を実現します。ノードがリファールを作成するのは、データを含むノード上に SVM の LIF があることを特定した場合です。リファールは、クライアントの接続に使用されている共有のルートの場所に基づいて作成されます。

リファールは SMB ネゴシエーション中に発生します。リファールは、接続が確立される前に作成されます。ONTAP がターゲットノードに参照先の SMB クライアントを通知したあと、接続が確立され、それ以降、クライアントはその参照先 LIF パスを介してデータにアクセスします。これにより、クライアントにはより高速なデータアクセスが提供され、クラスタの余分な通信も回避されます。

**Mac OS** クライアントで自動ノードリファールを使用する際のガイドラインを次に示します

Mac OS では Microsoft の Distributed File System（DFS；分散ファイルシステム）がサポートされていますが、Mac OS X クライアントは SMB 自動ノードリファールをサポートしていません。Windows クライアントは、SMB 共有に接続する前に DFS リファール要求を行います。ONTAP は、要求されたデータをホストしているノード上で見つかったデータ LIF へのリファールを提供します。これにより、クライアントの応答時間が短縮されます。Mac OS でも DFS はサポートされますが、Mac OS クライアントの動作は Windows クライアントとまったく同じではありません。

関連情報

[ONTAP で動的ホームディレクトリを有効にする方法](#)

["Network Management の略"](#)

["NetApp Interoperability Matrix Tool で確認できます"](#)



SMB 自動ノードリファーラルを有効にする際に、ONTAP の一部の機能ではリファーラルがサポートされない点に注意してください。

- SMB 自動ノードリファーラルは、次の種類のボリュームではサポートされません。
  - 負荷共有ミラーの読み取り専用のメンバー
  - データ保護ミラーのデスティネーションボリューム
- LIF が移動してもノードリファーラルは移動しません。

クライアントが SMB 2.x または SMB 3.0 接続を介した参照接続を使用している場合、データ LIF が無停止で移動してもクライアントは引き続き同じ参照接続を使用します。LIF がデータに対してローカルでなくなった場合も同様です。

- ボリュームが移動してもノードリファーラルは移動しません。

クライアントがいずれかの SMB 接続による参照接続を使用している場合、ボリュームが移動してもクライアントは引き続き同じ参照接続を使用します。ボリュームがデータ LIF と異なるノードに移動した場合も同様です。

**SMB 自動ノードリファーラルを有効または無効にします**

SMB 自動ノードリファーラルを有効にして、SMB クライアントアクセスのパフォーマンスを向上させることができます。ONTAP で SMB クライアントを参照しないようにするには、自動ノードリファーラルを無効にします。

作業を開始する前に

Storage Virtual Machine （SVM）で CIFS サーバが設定されて実行されている必要があります。

このタスクについて

SMB 自動ノードリファーラル機能は、デフォルトでは無効になっています。必要に応じて、各 SVM で有効または無効にすることができます。

このオプションは、advanced 権限レベルで使用できます。

手順

1. 権限レベルを advanced に設定します。set -privilege advanced
2. SMB 自動ノードリファーラルを必要に応じて有効または無効にします。

SMB 自動ノードリファーラルの設定	入力するコマンド
有効	<code>vserver cifs options modify -vserver vserver_name -is-referral-enabled true</code>
無効	<code>vserver cifs options modify -vserver vserver_name -is-referral-enabled false</code>

このオプション設定は、新しい SMB セッションで有効になります。既存の接続を使用しているクライアントは、その既存のキャッシュがタイムアウトになった場合にのみノードリファールを利用できます

3. admin権限レベルに切り替えます。 `set -privilege admin`

## 関連情報

### 使用できる SMB サーバオプション

統計を使用して、自動ノードリファールのアクティビティを監視します

参照されるSMB接続の数を確認するには、を使用して自動ノードリファールのアクティビティを監視します `statistics` コマンドを実行しますリファールを監視することで、自動リファールによって共有をホストするノードに対して接続が割り当てられている範囲を把握し、データ LIF を再配分して CIFS サーバの共有へのローカルアクセスを向上させるべきかどうかを判断することができます。

#### このタスクについて

。 `cifs` オブジェクトには、SMB自動ノードリファールの監視に役立つadvanced権限レベルのカウンタがいくつか用意されています。

- `node_referral_issued`

共有のルートとは別のノードでホストされる LIF を使用して接続したクライアントのうち、共有のルートへのリファールが発行されたクライアントの数。

- `node_referral_local`

共有のルートと同じノードでホストされる LIF を使用して接続したクライアントの数。一般に、ローカルアクセスを使用するとパフォーマンスが最適化され

- `node_referral_not_possible`

共有のルートとは別のノードでホストされる LIF を使用して接続したクライアントのうち、共有のルートをホストするノードへのリファールが発行されていないクライアントの数。これは、共有のルートのノードに対するアクティブなデータ LIF が見つからないためです。

- `node_referral_remote`

共有のルートとは別のノードでホストされる LIF を使用して接続したクライアントの数。リモートアクセスを使用するとパフォーマンスが低下する可能性があります。

一定期間内のデータ（サンプル）を収集して表示することにより、Storage Virtual Machine（SVM）の自動ノードリファール統計を監視できます。データ収集を停止しなければ、サンプルからデータを表示できます。データ収集を停止すると、サンプルが固定された状態になります。データ収集を停止しないと、以前のクエリとの比較に使用できる更新されたデータを取得できます。この比較は、パフォーマンスの傾向を確認するのに役立ちます。



から収集した情報を評価および使用するため `statistics` コマンドを使用する場合は、環境内のクライアントの分散状況について理解しておく必要があります。



## 手順

1. 権限レベルを advanced に設定します。 `set -privilege advanced`
2. を使用して、自動ノードリファールルの統計を表示します `statistics` コマンドを実行します

次に、一定のサンプリング時間におけるデータを収集して表示することにより、自動ノードリファールルの統計を表示する例を示します。

- a. 収集を開始します。 `statistics start -object cifs -instance vs1 -sample-id sample1`

```
Statistics collection is being started for Sample-id: sample1
```

- b. 目的の収集時間が経過するまで待ちます。
- c. 収集を停止します。 `statistics stop -sample-id sample1`

```
Statistics collection is being stopped for Sample-id: sample1
```

- d. 自動ノードリファールルの統計を表示します。 `statistics show -sample-id sample1 -counter node`

```
Object: cifs
Instance: vs1
Start-time: 2/4/2013 19:27:02
End-time: 2/4/2013 19:30:11
Cluster: cluster1
```

Counter	Value
node_name	node1
node_referral_issued	0
node_referral_local	1
node_referral_not_possible	2
node_referral_remote	2
...	
node_name	node2
node_referral_issued	2
node_referral_local	1
node_referral_not_possible	0
node_referral_remote	2
...	

出力には、SVM vs1 に含まれるすべてのノードのカウンタが表示されます。この例では、わかりやす

いように、自動ノードリファールルの統計に関連する出力フィールドだけを示しています。

3. admin 権限レベルに戻ります。 `set -privilege admin`

関連情報

[統計情報を表示します](#)

["パフォーマンス監視のセットアップ"](#)

**Windows** クライアントを使用して、クライアント側の **SMB** 自動ノードリファールル情報を監視します

クライアント側から発行されているリファールルを確認するには、Windowsを使用します `dfsutil.exe` ユーティリティ。

Windows 7以降のクライアントで使用できるRemote Server Administration Tools (RSAT) キットには、が含まれています `dfsutil.exe` ユーティリティ。このユーティリティを使用すると、リファールルキャッシュの内容に関する情報を表示できるほか、クライアントで現在使用されている各リファールルに関する情報を表示できます。また、このユーティリティを使用して、クライアントのリファールルキャッシュをクリアすることもできます。詳細については、Microsoft TechNet ライブラリを参照してください。

関連情報

["Microsoft TechNet ライブラリ： `technet.microsoft.com/en-us/library/`"](https://technet.microsoft.com/en-us/library/)

アクセスベースの列挙を使用して共有のフォルダのセキュリティを確保します

アクセスベースの列挙の概要を使用して、共有のフォルダのセキュリティを提供します

Access-Based Enumeration が SMB 共有で有効になっていると、共有内のフォルダまたはファイルに（個人またはグループの権限制限により）アクセスする権限がないユーザーの環境には、その共有リソースは表示されませんが、共有自体は表示されたままです。

従来の共有プロパティでは、共有内のファイルやフォルダの表示や変更権限を持つユーザー（個人またはグループ）を指定できます。ただし、権限のないユーザーに対して共有内のフォルダやファイルを表示可能とするかどうかを制御することはできません。この状態だと、共有内のこれらのフォルダ名またはファイル名に、顧客名や開発中の製品などの重要な情報が記述されている場合に問題になることがあります。

ABE では、共有プロパティが強化され、共有内のファイルやフォルダの列挙表示も対象になりました。このため、ABE を使用して、ユーザーのアクセス権に基づいて共有内のファイルとフォルダの表示をフィルタリングすることができます。つまり、共有自体はすべてのユーザーに表示されますが、共有内のファイルやフォルダは、指定したユーザーに対して表示したり非表示にしたりすることができます。職場の機密情報を保護するだけでなく、ABE を使用すると大きなディレクトリ構造の表示を簡略化できるため、あらゆるコンテンツにアクセスする必要がないユーザーにメリットがあります。たとえば、共有自体はすべてのユーザーに表示されますが、共有内のファイルやフォルダは表示または非表示にすることができます。

詳細はこちら ["SMB / CIFSアクセスベースの列挙を使用する際のパフォーマンスへの影響"](#)。

**SMB** 共有でのアクセスベースの列挙を有効または無効にします

SMB 共有で Access-Based Enumeration を有効または無効にすると、ユーザーがアクセス権のない共有リソースを表示することを許可または禁止できます。

このタスクについて  
デフォルトでは、ABEは無効になっています。

#### 手順

1. 次のいずれかを実行します。

状況	入力するコマンド
新しい共有で ABE を有効にします	<code>vserver cifs share create -vserver vserver_name -share-name share_name -path path -share-properties access-based-enumeration</code> SMB共有の作成時に、追加のオプションの共有設定および追加の共有プロパティを指定できます。詳細については、のマニュアルページを参照してください <code>vserver cifs share create</code> コマンドを実行します
既存の共有で ABE を有効にします	<code>vserver cifs share properties add -vserver vserver_name -share-name share_name -share-properties access-based-enumeration</code> 既存の共有プロパティは維持されます。ABE 共有プロパティは既存の共有プロパティリストに追加されます。
既存の共有で ABE を無効にします	<code>vserver cifs share properties remove -vserver vserver_name -share-name share_name -share-properties access-based-enumeration</code> その他の共有プロパティは維持されます。ABE 共有プロパティのみが共有プロパティリストから削除されます。

2. を使用して、共有設定が正しいことを確認します `vserver cifs share show` コマンドを実行します

#### 例

次の例は、「sales」という名前のABE SMB共有をパスに作成します `/sales SVM vs1`上。共有はを使用して作成されます `access-based-enumeration` 共有プロパティとして：

```
cluster1::> vsriver cifs share create -vsriver vs1 -share-name sales -path
/sales -share-properties access-based-
enumeration,oplocks,browsable,changenotify

cluster1::> vsriver cifs share show -vsriver vs1 -share-name sales

                Vserver: vs1
                Share: sales
CIFS Server NetBIOS Name: VS1
                Path: /sales
                Share Properties: access-based-enumeration
                                oplocks
                                browsable
                                changenotify
                Symlink Properties: enable
                File Mode Creation Mask: -
                Directory Mode Creation Mask: -
                Share Comment: -
                Share ACL: Everyone / Full Control
File Attribute Cache Lifetime: -
                Volume Name: -
                Offline Files: manual
Vscan File-Operations Profile: standard
```

次の例は、を追加します access-based-enumeration 「data2」という名前のSMB共有への共有プロパティ:

```
cluster1::> vsriver cifs share properties add -vsriver vs1 -share-name
data2 -share-properties access-based-enumeration

cluster1::> vsriver cifs share show -vsriver vs1 -share-name data2 -fields
share-name,share-properties
server  share-name share-properties
-----
vs1     data2      oplocks,browsable,changenotify,access-based-enumeration
```

## 関連情報

[既存の SMB 共有に対する共有プロパティの追加または削除](#)

**Windows** クライアントからのアクセスベースの列挙を有効または無効にします

SMB 共有での Access-Based Enumeration の有効化と無効化は Windows クライアントから実行できるため、この共有設定は CIFS サーバに接続することなく編集できます。



。 abecmd ユーティリティは、Windows ServerおよびWindowsクライアントの新しいバージョンでは使用できません。Windows Server 2008の一部としてリリースされました。Windows Server 2008のサポートは2020年1月14日をもって終了しました。

## 手順

1. ABEをサポートするWindowsクライアントで、次のコマンドを入力します。 `abecmd [/enable | /disable] [/server CIFS_server_name] {/all | share_name}`

詳細については、を参照してください abecmd コマンドについては、Windowsクライアントのマニュアルを参照してください。

## NFS と SMB のファイルとディレクトリの命名規則

NFS と SMB のファイルとディレクトリの命名規則について概要を示します

ファイルとディレクトリの命名規則は、ONTAP クラスタおよびクライアントの言語設定に加え、ネットワーククライアントのオペレーティングシステムとファイル共有プロトコルによって異なります。

オペレーティングシステムとファイル共有のプロトコルによって、次の要素が決定します。

- ファイル名に使用できる文字
- ファイル名での大文字と小文字の区別

ONTAP では、ONTAP のリリースに応じて、ファイル、ディレクトリ、qtree の名前でマルチバイト文字がサポートされます。

ファイル名またはディレクトリ名に使用できる文字

異なるオペレーティングシステムのクライアントからファイルやディレクトリにアクセスする場合は、どちらのオペレーティングシステムでも有効な文字を使用します。

たとえば、UNIX を使用してファイルやディレクトリを作成する場合は、ファイル名やディレクトリ名にコロン (:) を使用しないでください。コロンは、MS-DOS ファイル名やディレクトリ名では使用できないためです。有効な文字の制限はオペレーティングシステムごとに異なります。使用できない文字の詳細については、クライアントのオペレーティングシステムのマニュアルを参照してください。

マルチプロトコル環境でのファイル名とディレクトリ名の大文字と小文字の区別

ファイル名とディレクトリ名では、NFSクライアントでは大文字と小文字が区別されますが、SMBクライアントでは大文字と小文字が区別されません。この違いがマルチプロトコル環境に及ぼす影響と、SMB 共有の作成時にパスを指定するときや、共有内のデータにアクセスするときにはどのような対処が必要になるかを理解しておく必要があります。

SMBクライアントがという名前のディレクトリを作成する場合 `testdir`` SMBクライアントとNFSクライアントのどちらでも、ファイル名はと表示されます ``testdir`。ただし、SMBユーザがあとでディレクトリ名を作成しようとした場合 ``TESTDIR`` を指定することはできません。SMBクライアントでは、その名前がすでに

存在しているとみなされます。NFSユーザがあとでという名前のディレクトリを作成する場合 `TESTDIR` では、NFSクライアントとSMBクライアントで表示されるディレクトリ名は次のように異なります。

- NFSクライアントでは、両方のディレクトリ名が作成したとおりに表示されます（例：） `testdir` および `TESTDIR` ディレクトリ名では大文字と小文字が区別されるためです。
- SMB クライアントでは、2つのディレクトリを区別するために 8.3 形式の名前が使用されます。1つのディレクトリにはベースファイル名が付けられます。追加のディレクトリには 8.3 形式のファイル名が割り当てられます。
  - SMBクライアントでは、が表示されます `testdir` および `TESTDI~1`。
  - ONTAP によってが作成されます `TESTDI~1` 2つのディレクトリを区別するディレクトリ名。

この場合、Storage Virtual Machine（SVM）での共有の作成時または変更時に共有パスを指定するときは、8.3 形式の名前を使用する必要があります。

ファイルについても、SMBクライアントでが作成された場合と同様です `test.txt` `SMBクライアントとNFSクライアントのどちらでも、ファイル名はと表示されます` `text.txt`。ただし、SMBユーザがあとでを作成しようとした場合 `Test.txt` を指定することはできません。SMBクライアントでは、その名前がすでに存在しているとみなされます。NFSユーザがあとでという名前のファイルを作成した場合 `Test.txt` では、NFSクライアントとSMBクライアントで表示されるファイル名は次のように異なります。

- NFSクライアントでは、両方のファイル名が作成されたとおりに表示され、 `test.txt` および `Test.txt` ファイル名では大文字と小文字が区別されるためです。
- SMB クライアントでは、2つのファイルを区別するために 8.3 形式の名前が使用されます。1つのファイルにはベースファイル名が付けられます。追加のファイルには 8.3 形式のファイル名が割り当てられます。
  - SMBクライアントでは、が表示されます `test.txt` および `TEST~1.TXT`。
  - ONTAP によってが作成されます `TEST~1.TXT` 2つのファイルを区別するためのファイル名。



SVM `cifs character-mapping` コマンドを使用して文字マッピングを有効または変更した場合、通常、大文字と小文字は区別されない Windows ルックアップは大文字と小文字が区別されません。

## ONTAP によるファイル名とディレクトリ名の作成方法

ONTAP は、SMB クライアントからアクセスされるすべてのディレクトリ内にあるファイルまたはディレクトリに対して 2つの名前が作成され、保持されます。元の長い名前と 8.3 形式の名前です。

名前が 8 文字を超える、または拡張子が 3 文字を超える（ファイルの場合）ファイル名やディレクトリ名について、ONTAP は次のように 8.3 形式の名前を生成します。

- 名前が 6 文字を超える場合は、元のファイル名またはディレクトリ名が 6 文字に切り捨てられます。
- 切り捨て後に一意でなくなったファイル名またはディレクトリ名には、チルダ（~）と 1~5 の数字が追加されます。

同様の名前が 6 つ以上存在するため数字が足りなくなった場合には、元の名前とは無関係な一意の名前が作成されます。

- ファイルの場合は、ファイル名の拡張子が 3 文字に切り捨てられます。

たとえば、NFSクライアントがという名前のファイルを作成するとします `specifications.html`ONTAP` で作成される 8.3 形式のファイル名はです ``specif~1.htm`。この名前がすでに存在する場合、ONTAP はファイル名の最後に別の番号を使用します。たとえば、NFSクライアントがという名前の別のファイルを作成したとします `specifications_new.html`、8.3 形式の `specifications_new.html` はです `specif~2.htm`。

マルチバイトを含むファイル名、ディレクトリ名、**qtree** 名の **ONTAP** での処理

ONTAP 9.5 以降では、4 バイトの UTF-8 エンコード形式の名前がサポートされるようになり、Basic Multilingual Plane（BMP；基本多言語面）以外の Unicode 補助文字を含むファイル、ディレクトリ、ツリーの名前を作成および表示できるようになりました。以前のリリースでは、これらの補助文字はマルチプロトコル環境では正しく表示されませんでした。

4 バイトの UTF-8 エンコード名のサポートを有効にするには、`new_utf8mb4_` 言語コードを使用できます `vserver` および `volume` コマンド・ファミリー。

次のいずれかの方法で新しいボリュームを作成する必要があります。

- ボリュームを設定しています `-language` 明示的なオプション：`volume create -language utf8mb4 {...}`
- ボリュームを継承しています `-language` オプションを指定して作成または変更した SVM から、次のオプションを選択します。`vserver [create|modify] -language utf8mb4 {...}``volume create {...}`
- ONTAP 9.6 以前では、`utf8mb4` をサポートするために既存のボリュームを変更することはできません。`utf8mb4` 対応の新しいボリュームを作成し、クライアントベースのコピーツールを使用してデータを移行する必要があります。

SVM は `utf8mb4` をサポートするように更新できますが、既存のボリュームの言語コードは元の設定のままです。

ONTAP 9.7P1 以降を使用している場合は、`utf8mb4` の既存ボリュームをサポートリクエストで変更できます。詳細については、を参照してください ["ONTAP での作成後にボリュームの言語を変更できますか。"](#)。

- ONTAP 9.8 以降では、`[-language <Language code>]` ボリュームの言語を\*。`utf-8` から `utf8mb4` に変更するためのパラメータ。ボリュームの言語を変更するには、["ネットアップサポート"](#)。



現在のところ、4 バイトの UTF-8 文字を含む LUN 名はサポートされていません。

- 一般に、Unicode 文字データは、Windows ファイルシステムアプリケーションでは 16-bit Unicode Transformation Format（UTF-16）、NFS ファイルシステムでは 8-bit Unicode Transformation Format（UTF-8）を使用して表現されます。

ONTAP 9.5 よりも前のリリースでは、Windows クライアントで作成された UTF-16 の補助文字を含む名前は、他の Windows クライアントには正しく表示されましたが、NFS クライアントでは UTF-8 に正しく変換されませんでした。同様に、NFS クライアントで作成された UTF-8 の補助文字を含む名前は、Windows クライアントで UTF-16 に正しく変換されませんでした。



- ONTAP 9.4 以前を実行しているシステムで作成したファイル名に有効な追加文字が含まれている場合や無効な追加文字が含まれている場合、ONTAP はそれらのファイル名を拒否し、ファイル名が無効であることを示すエラーを返します。

この問題を回避するには、ファイル名に BMP 文字のみを使用して補助文字は使用しないようにするか、ONTAP 9.5 以降にアップグレードしてください。

ONTAP 9 以降では、Unicode 文字を qtree 名に使用できます。

- どちらかを使用できます volume qtree qtree名を設定または変更するには、コマンドファミリーまたは System Manager を使用します。
- 日本語や中国語などの Unicode 形式のマルチバイト文字を qtree 名に含めることができます。
- ONTAP 9.5 よりも前のリリースでは、BMP 文字（つまり 3 バイトで表現可能な文字）のみがサポートされます。



ONTAP 9.5 よりも前のリリースでは、qtree の親ボリュームのジャンクションパスに、Unicode 文字を使用した qtree 名やディレクトリ名を含めることができます。 volume show 親ボリュームの言語設定が UTF-8 の場合は、コマンドでこれらの名前が正しく表示されます。ただし、親ボリュームの言語設定が UTF-8 のいずれかでない場合は、ジャンクションパスの一部が数値の NFS 名に置き換えられて表示されます。

- 9.5 以降のリリースでは、qtree が utf8mb4 に対応したボリュームに含まれていれば、qtree 名で 4 バイト文字がサポートされます。

ボリュームでの **SMB** ファイル名の変換のための文字マッピングを設定します

NFS クライアントは、SMB クライアントと特定の Windows アプリケーションでは無効な文字を含むファイル名を作成できます。ボリュームにおけるファイル名の変換のための文字マッピングを設定できます。これにより、そのままでは無効な NFS 名を持つファイルに SMB クライアントからアクセスできます。

このタスクについて

SMB クライアントが NFS クライアントによって作成されたファイルにアクセスすると、ONTAP はファイル名を調べます。ファイル名が有効な SMB ファイル名でない場合は（たとえば、コロンが含まれている場合）、ONTAP は各ファイルに対して保持されている 8.3 形式のファイル名を返します。ただし、これにより、長いファイル名に重要な情報をエンコードするアプリケーションで問題が発生します。

したがって、異なるオペレーティングシステムを使用するクライアント間でファイルを共有する場合は、両方のオペレーティングシステムで有効な文字をファイル名に使用する必要があります。

ただし、SMB クライアントで有効でない文字を含む NFS クライアントが作成したファイル名がある場合は、無効な NFS の文字を、SMB と特定の Windows アプリケーションの両方で有効な Unicode 文字に変換するマッピングを定義できます。たとえば、この機能は CATIAR MCAD および Mathematica アプリケーションをサポートしていますが、同じ要件を持つほかのアプリケーションでも使用できます。

文字マッピングはボリューム単位で設定できます。

ボリュームで文字マッピングを設定する場合は、次の点に注意する必要があります。

- 文字マッピングは、ジャンクションポイントをまたいで適用されません。



文字マッピングは、各ジャンクションボリュームに対して明示的に設定する必要があります。

- 無効な文字を表す Unicode 文字が、通常はファイル名に使用されないようにする必要があります。これらの文字が使用されていた場合、不要なマッピングが発生します。

たとえば ' コロン (:) をハイフン (-) にマッピングしようとした場合 ' ファイル名にハイフン (-) が正しく使用されていれば 'Windows クライアントが "a-b" という名前のファイルにアクセスしようとする' その要求は NFS 名 "a:b" にマッピングされます ( 望ましい結果ではありません )

- 文字マッピングを適用してもまだマッピングに無効な Windows 文字が含まれている場合、ONTAP は Windows 8.3 ファイル名にフォールバックします。
- FPolicy 通知、NAS 監査ログ、セキュリティトレースメッセージでは、マッピングされたファイル名が表示されます。
- タイプが DP である SnapMirror 関係が作成されても、ソースボリュームの文字マッピングはデスティネーション DP ボリュームにレプリケートされません。
- 大文字と小文字の区別：マッピングされた Windows 名は NFS 名に変換されるため、名前の検索は NFS のセマンティクスに従います。NFS ルックアップでは大文字と小文字が区別されるという事実も含まれます。つまり、マッピングされた共有にアクセスするアプリケーションは、Windows の大文字と小文字を区別しない動作に依存しません。ただし、8.3 形式の名前は大文字と小文字が区別されません。
- 部分マッピングまたは無効なマッピング：ディレクトリ列挙（「dir」）を実行しているクライアントに返すように名前をマッピングしたあと、結果の Unicode 名について Windows の有効性がチェックされます。その名前にまだ無効な文字が含まれている場合、または Windows で無効な文字が含まれている場合（「.」または空白で終わる場合など）は、無効な名前の代わりに 8.3 形式の名前が返されます。

## ステップ

### 1. 文字マッピング「+」を設定します

```
vserver cifs character-mapping create -vserver vserver_name -volume volume_name  
-mapping mapping_text, ...[+]
```

マッピングは、「:」で区切られたソース文字とターゲット文字のペアのリストで構成されます。文字は、16 進数値で入力された Unicode 文字です。例：3C : E03C[+]

それぞれの最初の値 mapping\_text コロンで区切られたペアは、変換する NFS 文字の 16 進値です。2 番目の値は、SMB で使用される Unicode 値です。マッピングのペアは一意である必要があります（1 対 1 のマッピングが存在する必要があります）。

- ソースマッピング +

次の表に、ソースマッピングで許可されている Unicode 文字セットを示します。

[+]

Unicode 文字	印刷された文字	説明
0x01-0x19	該当なし	印刷されない制御文字
0x5C		バックスラッシュ

Unicode 文字	印刷された文字	説明
0x3a	:	コロン
0x2A	*	アスタリスク
0x3f	?	疑問符
0x22	"	引用符
0x3C	<	より小さい
0x3E	>	が次の値より大きい
0x7C		
縦線	0xb1	±

- ターゲットマッピング

ターゲット文字には、U+E0000...U+F8FF の範囲の Unicode の「私用領域」を指定できます。

#### 例

次のコマンドは、Storage Virtual Machine （SVM） vs1 上の「data」という名前のボリュームに文字マッピングを作成します。

```
cluster1::> vsserver cifs character-mapping create -volume data -mapping
3c:e17c,3e:f17d,2a:f745
cluster1::> vsserver cifs character-mapping show
```

Vserver	Volume Name	Character Mapping
vs1	data	3c:e17c, 3e:f17d, 2a:f745

#### 関連情報

[NAS ネームスペース内でのデータボリュームの作成と管理](#)

#### SMB ファイル名の変換のための文字マッピングを管理するコマンド

FlexVol での SMB ファイル名の変換に使用する情報を作成、変更、表示したり、ファイル文字マッピングを削除したりすることで、文字マッピングを管理できます。

状況	使用するコマンド
新しいファイル文字マッピングを作成します	<code>vserver cifs character-mapping create</code>
ファイル文字マッピングに関する情報を表示する	<code>vserver cifs character-mapping show</code>
既存のファイル文字マッピングを変更します	<code>vserver cifs character-mapping modify</code>
ファイル文字マッピングを削除します	<code>vserver cifs character-mapping delete</code>

詳細については、各コマンドのマニュアルページを参照してください。

#### 関連情報

[ボリュームでの SMB ファイル名の変換のための文字マッピングを設定する](#)

## NASデータへのS3クライアントアクセスを提供

### S3マルチプロトコルの概要

ONTAP 9.12.1以降では、S3プロトコルを実行するクライアントが、NFSプロトコルおよびSMBプロトコルを使用するクライアントに提供されているデータに再フォーマットせずにアクセスできるようにすることができます。この機能により、NASデータは引き続きNASクライアントに提供され、S3アプリケーション（データマイニングや人工知能など）を実行するS3クライアントにオブジェクトデータが提供されます。

S3マルチプロトコル機能は次の2つのユースケースに対応します。

#### 1. S3クライアントを使用した既存のNASデータへのアクセス

既存のデータが従来のNASクライアント（NFSまたはSMB）を使用して作成され、NASボリューム（FlexVol またはFlexGroup ボリューム）にある場合、S3クライアント上の分析ツールを使用してこのデータにアクセスできるようになりました。

#### 2. NASとS3の両方のプロトコルを使用したI/O処理に対応できる、最新のクライアント用のバックエンドストレージです

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

### S3マルチプロトコルの仕組み

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

このマッピングは、指定されたNASディレクトリ階層をS3バケットとして提供することで実現されます。ディレクトリ階層内の各ファイルは、マップされたディレクトリから下の位置に相対的な名前を持つS3オブジェクトとして表され、ディレクトリ境界はスラッシュ文字 (/) で表されます。

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

SMBクライアントまたはNFSクライアントが作成すると、ファイルはすぐにディレクトリに配置され、クライアントからはデータが書き込まれる前に参照できます。S3クライアントはセマンティクスが異なることを要求します。セマンティクスでは、新しいオブジェクトはすべてのデータが書き込まれるまでネームスペースに表示されません。S3からNASストレージへのマッピングではS3のセマンティクスを使用してファイルが作成され、S3の作成コマンドが完了するまでファイルは外部には表示されません。

### S3 NASバケットのデータ保護

S3 NAS「バケット」は、S3クライアントのNASデータをマッピングするだけで、標準のS3バケットではありません。したがって、NetApp S3 SnapMirror機能を使用してS3 NASバケットを保護する必要はありません。代わりに、非同期SnapMirrorボリュームレプリケーションを使用して、S3 NASバケットを含むボリュームを保護できます。SnapMirror SynchronousおよびSVMディザスタリカバリはサポートされていません。

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

詳細はこちら ["非同期SnapMirror"](#)。

### S3 NASバケットの監査

S3 NASバケットは従来のS3バケットではないため、S3監査を設定してアクセスを監査することはできません。の詳細を確認してください ["S3監査"](#)。

ただし、S3 NASバケットにマッピングされているNASファイルとディレクトリは、従来のONTAP 監査手順を使用してアクセスイベントを監査できます。したがって、S3処理ではNAS監査イベントがトリガーされますが、次の例外があります。

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

詳細はこちら ["SVMでNASイベントを監査する"](#)。

### S3およびNASの相互運用性

ONTAP S3 NASバケットは、ここに記載されている点を除いて、NASとS3の標準機能をサポートします。

NAS機能は、現在**S3 NAS**バケットではサポートされていません

## FabricPool の大容量階層

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

**S3 NAS**バケットでは現在、**S3**機能はサポートされていません

## AWSユーザメタデータ

- S3ユーザメタデータの一部として受信したキーと値のペアは、現在のリリースのオブジェクトデータと一緒にディスクに格納されません。
- プレフィックスが「x-amz-meta」の要求ヘッダーは無視されます。

## AWSタグ

- PUT Object要求とMultipart Initiate要求では、プレフィックスが「x-amz-tagging」のヘッダーは無視されます。
- 既存のファイル（つまり、「tagging」クエリー文字列を持つPUT、GET、Deleteの各要求）でタグを更新する要求は、エラーで拒否されます。

## バージョン管理

バージョン管理をバケットのマッピング設定で指定することはできません。

- バージョンがnullでない仕様（versionId=xyzクエリ文字列）を含む要求は、エラー応答を受信します。
- バケットのバージョン管理状態に影響する要求は拒否され、エラーが発生します。

## マルチパート処理

次の操作はサポートされません。

- AbortMultipartUpload の略
- CompleteMultipartUpload
- CreateMultipartUpload を実行します
- ListMultipartUpload の略

## NASデータの**S3**クライアントアクセス要件

NASファイルとディレクトリをS3アクセス用にマッピングする場合は、互換性が確保されていない問題がいくつかあることに注意してください。NASファイル階層は、S3 NASバケットを使用して階層を提供する前に調整しなければならない場合があります。

S3 NASバケットは、S3バケット構文を使用してディレクトリをマッピングすることでNASディレクトリへのS3アクセスを提供し、ディレクトリツリー内のファイルはオブジェクトとみなされます。オブジェクト名は、S3バケットの設定で指定されたディレクトリに相対的な、ファイルのスラッシュで区切られたパス名です。

このマッピングは、S3 NASバケットを使用してファイルとディレクトリにサービスを提供する際にいくつかの要件を適用します。

- S3の名前は1024バイトに制限されているため、長いパス名を持つファイルにS3を使用してアクセスすることはできません。

- ファイル名とディレクトリ名は255文字に制限されているため、オブジェクト名には、連続する255文字以外の文字（「/」）を使用できません
- バックスラッシュ（「\」）で区切られたSMBパス名は、s3にはスラッシュ（「/」）ではなく、オブジェクト名として表示されます。
- 有効なS3オブジェクト名のペアの一部は、マッピングされたNASディレクトリツリーに共存できません。たとえば、有効なS3オブジェクト名「part1/part2」と「part1/part2/part3」は、NASディレクトリツリーに同時に存在できないファイルにマッピングされます。「part1/part2」は、最初の名前に含まれるファイルで、もう一方の名前に含まれるディレクトリです。
  - 「part1/part2」が既存のファイルの場合、「part1/part2/part3」のS3作成は失敗します。
  - "part1/part2/part3"が既存のファイルの場合、"part1/part2"のS3作成または削除が失敗します。
  - 既存のオブジェクトの名前と一致するS3オブジェクトの作成によって、（バージョン管理されていないバケット内の）既存のオブジェクトが置き換えられます。これはNASを保持するが、完全に一致する必要があります。上記の例では、名前が競合している間は原因によって既存のオブジェクトが削除されないため、これらのオブジェクトは削除されません。

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

## NASデータへのS3プロトコルアクセスを有効にします

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

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

- ["NFS構成"](#)
- ["SMBの設定"](#)

作業を開始する前に

S3プロトコルを有効にする前に、次の項目を設定する必要があります。

- S3プロトコルおよび目的のNASプロトコル（NFS、SMB、またはその両方）のライセンスが設定されている。
- SVMが目的のNASプロトコル用に設定されている。
- NFSサーバとSMBサーバが存在します。
- DNSおよびその他の必要なサービスが設定されていること。
- NASデータをクライアントシステムにエクスポートまたは共有しています。

このタスクについて

S3 クライアントから S3 対応 SVM への HTTPS トラフィックを有効にするには、認証局（CA）証明書が必


要です。次の3つのソースのCA証明書を使用できます。

- 新しいONTAP 自己署名証明書をSVMに作成します。
- 既存のONTAP 自己署名証明書がSVMに存在している。
- サードパーティの証明書。

NASデータの提供に使用するS3 / NASバケットにも同じデータLIFを使用できます。特定のIPアドレスが必要な場合は、を参照してください ["データ LIF を作成します。"](#)。S3データトラフィックをLIFで有効にするには、S3サービスデータポリシーが必要です。SVMの既存のサービスポリシーを変更して、S3を含めることができます。

S3オブジェクトサーバを作成するときは、クライアントがS3アクセスに使用する完全修飾ドメイン名（FQDN）としてS3サーバ名を入力できるように準備しておく必要があります。S3サーバのFQDNの先頭をバケット名にすることはできません。

## System Manager の略

1. NASプロトコルが設定されているStorage VMでS3を有効にします。
  - a. Storage > Storage VM\*の順にクリックし、NAS対応のStorage VMを選択して、Settings（設定）をクリックし、をクリックします  S3 の下。
  - b. 証明書のタイプを選択します。システムで生成された証明書と独自の証明書のどちらを選択した場合も、クライアントアクセスには証明書が必要です。
  - c. ネットワークインターフェイスを入力してください。
2. システムで生成された証明書を選択した場合は、新しい Storage VM の作成を確認すると証明書情報が表示されます。[ダウンロード]をクリックし、クライアントアクセス用に保存します。
  - シークレットキーは今後表示されません。
  - 証明書情報が再度必要な場合は、[\* ストレージ]、[Storage VMs]の順にクリックし、Storage VM を選択して、[\* 設定]をクリックします。

## CLI の使用

1. SVMでS3プロトコルが許可されていることを確認します。+  
`vserver show -fields allowed-protocols`
2. このSVMの公開鍵証明書を記録します。[+]  
新しいONTAP自己署名証明書が必要な場合は、を参照してください。 ["CA 証明書を作成して SVM にインストールします"](#)。
3. サービスデータポリシーを更新します
  - a. SVMのサービスデータポリシーを表示します。+  
`network interface service-policy show -vserver svm_name`
  - b. を追加します data-core および data-s3-server services 表示されない場合は、[+]  
`network interface service-policy add-service -vserver svm_name -policy policy_name -services data-core,data-s3-server`
4. SVMのデータLIFが要件を満たしていることを確認します。+  
`network interface show -vserver svm_name`
5. S3サーバを作成します：+  
`vserver object-store-server create -vserver svm_name -object-store-server s3_server_fqdn -certificate-name ca_cert_name -comment text [additional_options]`

S3 サーバの作成時またはあとからいつでも追加のオプションを指定できます。

- HTTPS は、ポート 443 でデフォルトで有効になっています。ポート番号は、-secure-listener-port オプションを使用して変更できます。[+]  
HTTPS を有効にすると、SSL/TLS との適切な統合に CA 証明書が必要になります。
- HTTP はデフォルトではディセーブルです。イネーブルにすると、サーバはポート 80 をリスンします。is-http-enabledオプションを指定して有効にするか、-listener-portオプションを使用してポート番号を変更できます。[+]  
HTTP が有効な場合は、すべての要求と応答がクリアテキストでネットワーク経由で送信されます。
  1. S3が必要に応じて設定されていることを確認します。+  
`vserver object-store-server show`



例+

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

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

```
Vserver: vs1
```

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

## S3 NASバケットを作成する

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

作業を開始する前に

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

このタスクについて

S3 NASバケットは、SVMのルートディレクトリ内のすべてのファイルとディレクトリのセットを指定するように設定できます。

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

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

たとえば、大規模なユーザグループに読み取り専用データアクセスを許可するバケットポリシーと、そのデータのサブセットに対して処理を実行する権限を制限するグループが別々に必要になることがあります。

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

- \* aggr-list\aggr-list-multiplier\storage-service-level\volume\size\exclude-aggr-list\qos-policy-group \*+  
S3 NASバケットの設定時にボリュームまたはqtreeが作成されません。
- \* role\is-protected\is-protected-on-ontap\is-protected-on-cloud \*+

S3 NASバケットは、S3 SnapMirrorを使用して保護またはミラーリングされませんが、代わりにボリューム単位で使用する通常のSnapMirror保護を使用します。

- バージョン管理状態+  
NASボリュームには通常、異なるバージョンを保存するためのSnapshotテクノロジーが用意されています。ただし、バージョン管理は現在S3 NASバケットでは使用できません。
- \* logical-used\ object-count \*+  
NASボリュームについては、volumeコマンドを使用して同等の統計情報を使用できます。

### System Manager の略

NAS対応Storage VMに新しいS3 NASバケットを追加

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

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

### CLI の使用

NASファイルシステムを含むSVMにS3 NASバケットを作成します。[+]

```
vserver object-store-server bucket create -vserver svm_name -bucket  
bucket_name -type nas -nas-path junction_path [-comment text]
```

例：+

```
cluster1::> vserver object-store-server bucket create -bucket testbucket -type  
nas -path /vol1
```

## S3クライアントユーザを有効にします

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

作業を開始する前に

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

このタスクについて

S3ユーザ名を対応するLinux/UNIXまたはWindowsユーザにマッピングすると、NASファイルに対する許可チェックがS3クライアントからアクセスされたときに実施されます。S3からNASへのマッピングは、単一の名前またはPOSIXの正規表現で指定できるS3ユーザ名\_Pattern\_、およびLinux/UNIXまたはWindowsのユーザ名\_Replacement\_を指定して指定します。

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

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

S3ユーザをNASユーザにマッピングすると、ユーザにアクセスを許可するリソース（ディレクトリとファイル）と、ユーザがアクセスを許可された操作、または許可されなかった操作を指定する権限を付与できます。

## System Manager の略

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

## CLI の使用

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

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

  - ° -position -マッピング評価の優先順位番号。1または2を入力します。
  - ° -pattern - S3ユーザ名または正規表現
  - ° -replacement - WindowsまたはUNIXのユーザ名

### 例+

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

1. クライアントアクセスを許可するバケットポリシーを作成します。[+]  

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

  - ° -effect {deny|allow} -ユーザがアクションを要求したときにアクセスを許可するか拒否するかを指定します。

- `-action <Action>`, ... -許可または拒否されるリソース操作を指定しますオブジェクトストアサーバで現在S3 NAS/バケットに対してサポートされているリソース処理のセットは、`GetObject`、`PutObject`、`DeleteObject`、`ListBucket`、`GetBucketAcl`、`GetObjectAcl`、`GetObjectTagging`、`PutObjectTagging`、`DeleteObjectTagging`、`GetBucketLocation`、`GetBucketVersioning`、`PutBucketVersioning`、`ListBucketVersions`の各メソッドに対応しています。このパラメータではワイルドカードを使用できます。
- `-principal <Objectstore Principal>`, ... -オブジェクトストアサーバのユーザまたはグループに対してアクセスを要求するユーザを検証します。
  - オブジェクトストアサーバグループは、グループ名にプレフィックスグループ/を追加することによって指定します。
  - `-principal -` (ハイフン文字) は、すべてのユーザにアクセスを許可します。
- `-resource <text>`, ... -許可または拒否の権限を設定するバケット、フォルダ、またはオブジェクトを指定します。このパラメータではワイルドカードを使用できます。
- `[-sid <SID>]` -オブジェクトストアサーバのバケットポリシーステートメントのオプションのテキストコメントを指定します。

例+

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

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

## Microsoft Hyper-V および SQL Server 向けの SMB の設定

### Microsoft Hyper-V および SQL Server 向けの SMB の設定の概要

ONTAP の機能を使用すると、SMB プロトコルを介した Microsoft アプリケーション、Microsoft Hyper-V および Microsoft SQL Server の 2 つのノンストップオペレーションを有効にできます。

SMB のノンストップオペレーションを実装する場合は、次の手順を使用する必要があります。

- SMB プロトコルの基本的なファイルアクセスが設定されている。
- SVM にある SMB 3.0 以降のファイル共有を有効にして次のオブジェクトを格納する。
  - Hyper-V 仮想マシンファイル
  - SQL Server システムデータベース

#### 関連情報

ONTAP テクノロジーおよび外部サービスとのやり取りに関する追加情報については、次のテクニカルレポート (TR) を参照してください。

"ネットアップテクニカルレポート 4172 : 『 Microsoft Hyper-V over SMB 3.0 with ONTAP Best Practices 』 "

"ネットアップテクニカルレポート 4369 : 『 Best Practices for Microsoft SQL Server and SnapManager 7.2 for SQL Server with Clustered Data ONTAP 』 "

## Microsoft Hyper-V および SQL Server over SMB ソリューション用に ONTAP を設定する

継続的な可用性が確保された SMB 3.0 以降のファイル共有を使用して、Hyper-V 仮想マシンファイルまたは SQL Server システムデータベースとユーザデータベースを SVM 内のボリュームに格納し、同時に計画的イベントと計画外イベントの間のノンストップオペレーション（NDO）を実現できます。

### SMB を介した Microsoft Hyper-V

Hyper-V over SMB 解決策を作成するには、まず、Microsoft Hyper-V サーバにストレージサービスを提供するように ONTAP を設定する必要があります。また、Microsoft クラスタ（クラスタ構成を使用する場合）、Hyper-V サーバ、CIFS サーバによってホストされている共有への継続的な可用性が確保された SMB 3.0 接続、および必要に応じて、SVM ボリュームに格納されている仮想マシンファイルを保護するためのバックアップサービスも設定する必要があります。



Hyper-V サーバは、Windows Server 2012 以降で設定する必要があります。Hyper-V サーバの構成については、スタンドアロンの構成とクラスタ化された構成の両方がサポートされます。

- Microsoft クラスタおよび Hyper-V サーバの作成については、Microsoft の Web サイトを参照してください。
- SnapManager for Hyper-V は、Snapshot コピーベースの高速バックアップサービスを容易に実現できるホストベースのアプリケーションで、Hyper-V over SMB 構成と統合できるように設計されています。

Hyper-V over SMB 構成での SnapManager の使用については、SnapManager for Hyper-V インストールとアドミニストレーションガイドを参照してください。

### Microsoft SQL Server over SMB

SQL Server over SMB 解決策を作成するには、まず、Microsoft SQL Server アプリケーションにストレージサービスを提供するように ONTAP を設定する必要があります。さらに、Microsoft クラスタも設定する必要があります（クラスタ構成を使用する場合）。その後、Windows サーバに SQL Server をインストールして設定し、CIFS サーバにホストされている共有への継続的な可用性を備えた SMB 3.0 接続を作成します。SVM ボリュームに格納されているデータベースファイルを保護するオプションで、バックアップサービスを設定することもできます。



SQL Server は、Windows Server 2012 以降にインストールし、設定する必要があります。スタンドアロン構成とクラスタ構成の両方がサポートされます。

- Microsoft クラスタの作成および SQL Server のインストールと設定については、Microsoft の Web サイトを参照してください。
- SnapCenter Plug-in for Microsoft SQL Serverは、Snapshotコピーベースの高速バックアップサービスを容易に実現できるホストベースのアプリケーションで、SQL Server over SMB構成と統合できるように設計されています。

## Hyper-V および SQL Server over SMB でのノンストップオペレーション

Hyper-V および SQL Server over SMB のノンストップオペレーションとは何ですか

Hyper-V および SQL Server over SMB のノンストップオペレーションとは、さまざまな管理作業の間も、アプリケーションサーバおよびそれに格納された仮想マシンやデータベースをオンラインのまま維持して、継続的な可用性を実現できる機能の組み合わせのことです。これには、ストレージインフラの計画的停止と計画外停止の両方が含まれます。

SMB を介したアプリケーションサーバのノンストップオペレーションでは、次のような操作がサポートされます。

- 計画的なテイクオーバーとギブバック
- 計画外のテイクオーバー
- アップグレード
- 計画的なアグリゲートの再配置（ARL）
- LIF の移行とフェイルオーバー
- 計画的なボリュームの移動

**SMB** を介したノンストップオペレーションを可能にするプロトコル

SMB 3.0 のリリースに伴い、Microsoft から、Hyper-V および SQL Server over SMB のノンストップオペレーションのサポートに必要な機能を備えた新しいプロトコルがリリースされました。

ONTAP では、SMB を介したアプリケーションサーバのノンストップオペレーションを実現するために、それらのプロトコルを使用しています。

- SMB 3.0
- 監視

Hyper-V および SQL Server over SMB のノンストップオペレーションの主要な概念

Hyper-V over SMB または SQL Server over SMB 解決策を設定する前に理解しておくべきノンストップオペレーション（NDO）の概念があります。

- \* 共有の継続的な可用性 \*

継続的可用性プロパティが設定されている SMB 3.0 共有。継続的可用性を備えた共有を介して接続しているクライアントは、テイクオーバー、ギブバック、およびアグリゲート移転などのシステム停止を伴うイベントが発生しても、

- \* ノード \*

クラスタのメンバーである単一のコントローラ。SFO ペアの 2 つのノードを区別するために、1 つのノードを `_local node_name` と呼び、もう 1 つのノードを `_partner node_or_remote node_name` と呼ぶことがあります。ストレージのプライマリ所有者はローカルノードです。セカンダリ所有者は、プライマリ所有者に障害が発生したストレージを制御するパートナーノードです。各ノードは、そのストレージのプライマリ所有者と、そのパートナーストレージのセカンダリ所有者です。

- \* 無停止でのアグリゲートの再配置 \*

クライアントアプリケーションを中断することなく、クラスタの SFO ペア内のパートナーノード間でアグリゲートを移動できること。

- \* 無停止フェイルオーバー \*

テイクオーバーを参照してください。

- \* 無停止での LIF の移行 \*

LIF を介してクラスタに接続されたクライアントアプリケーションを中断することなく、LIF を移行できること。SMB 接続の場合は、SMB 2.0 以降を使用して接続するクライアントでのみ可能です。

- \* ノンストップオペレーション \*

クライアントアプリケーションを中断することなく、ONTAP の主な管理およびアップグレード操作を実行でき、ノード障害に耐えられること。全体として、この用語は、無停止テイクオーバー、無停止アップグレード、および無停止移行の各機能を指します。

- \* 無停止アップグレード \*

アプリケーションを中断することなくノードのハードウェアまたはソフトウェアをアップグレードできること。

- \* 無停止ボリューム移動 \*

ボリュームを使用しているすべてのアプリケーションを中断することなく、クラスタ内で自由にボリュームを移動できること。SMB 接続の場合、SMB のすべてのバージョンで無停止でのボリューム移動がサポートされます。

- \* 永続的ハンドル \*

接続が切断した場合に、継続的可用性を備えた接続が透過的に CIFS サーバに再接続できるように設定する SMB 3.0 のプロパティ。永続性ハンドルと同様に、接続中のクライアントとの通信が失われたあとの一定期間、CIFS サーバによって永続的ハンドルが維持されます。ただし、永続的ハンドルは、永続性ハンドルよりも弾力性があります。CIFS サーバは、再接続後のクライアントにハンドルを 60 秒間使用する猶予を与え、その 60 秒間は、ファイルへのアクセスを要求する他のクライアントからのアクセスを拒否します。

永続的ハンドルに関する情報は SFO パートナーの永続的ストレージにミラー化されます。これにより、永続的ハンドルを切断したクライアントが、SFO パートナーによってノードのストレージの所有権が引き継がれた後に、永続性ハンドルを再利用できるようになります。永続的ハンドルは、LIF の移動（永続性ハンドルによってサポートされる）だけでなく、テイクオーバー、ギブバック、およびアグリゲートの再配置についても無停止での処理を提供します。



- \* SFO ギブバック \*

テイクオーバーイベントから戻るときにホーム位置にアグリゲートを戻します。

- \* SFO ペア \*

2つのノードのどちらかが機能を停止した場合に相互にデータを処理するようにコントローラが設定されたノードのペア。システムモデルに応じて、両方のコントローラを1つのシャーシに配置することも、別々のシャーシに配置することもできます。2ノードクラスターでの HA ペアを指します。

- \* テイクオーバー \*

ストレージのプライマリ所有者が失敗したときに、パートナーがストレージの制御を引き継ぐプロセス。SFO の文脈では、フェイルオーバーとテイクオーバーは同義です。

### SMB 3.0 の機能が SMB 共有を介したノンストップオペレーションをサポートする仕組み

SMB 3.0 には、Hyper-V over SMB および SQL Server over SMB 共有のノンストップオペレーションをサポートするためのきわめて重要な機能があります。これにはが含まれます `continuously-available` 共有プロパティおよび `_persistent handle` と呼ばれるファイルハンドルの一種。SMBクライアントは、ファイルオープン状態を再要求し、SMB接続を透過的に再確立できます。

永続的ハンドルは、継続的な可用性が設定された共有に接続する SMB 3.0 対応のクライアントに付与できます。SMB セッションが切断された場合、CIFS サーバは永続的ハンドルの状態に関する情報を保持します。CIFS サーバは、クライアントが再接続できる 60 秒間は他のクライアント要求をブロックするため、永続的ハンドルを持つクライアントは、ネットワークの切断後にハンドルを再要求できます。永続的ハンドルを持つクライアントは、Storage Virtual Machine (SVM) のデータ LIF のいずれかを使用して、同じ LIF または別の LIF を介して再接続できます。

アグリゲートの再配置、テイクオーバー、およびギブバックはすべて、SFO ペア間で行われます。永続的ハンドルを持つファイルを使用したセッションの切断と再接続をシームレスに管理するために、パートナーノードでは、すべての永続的ハンドルのロック情報のコピーが保持されます。イベントが計画的か計画外かに関係なく、SFO パートナーは、永続的ハンドルの再接続を無停止で管理できます。この新機能を使用すると、従来では業務が停止する状況となるイベントでも、CIFS サーバへの SMB 3.0 接続を、SVM に割り当てられた別のデータ LIF に透過的に無停止でフェイルオーバーできます。

永続的ハンドルを使用すると、CIFS サーバで SMB 3.0 接続を透過的にフェイルオーバーできるようになりますが、障害が発生したために Hyper-V アプリケーションが Windows Server クラスター内の別のノードにフェイルオーバーされる場合、クライアントは切断されたハンドルのファイルハンドルを再要求できません。このシナリオでは、切断された状態のファイルハンドルによって、別のノードで再起動した Hyper-V アプリケーションのアクセスがブロックされる可能性があります。「フェイルオーバークラスタリング」は、SMB 3.0 の一部で、古い競合するハンドルを無効にするメカニズムを提供して、このシナリオに対処します。このメカニズムを使用すると、Hyper-V クラスターノードに障害が発生した場合に、Hyper-V クラスターを迅速にリカバリできます。

### 透過的なフェイルオーバーを強化するための監視プロトコルの機能

監視プロトコルにより、SMB 3.0 の継続的な可用性が確保された共有 (CA 共有) に対するクライアントフェイルオーバー機能が強化されます。監視を使用すると、LIF のフェイルオーバーのリカバリがバイパスされるため、フェイルオーバーにかかる時間が短

縮されます。ノードを使用できなくなると、SMB 3.0 接続のタイムアウトを待たずにアプリケーションサーバに通知されます。

フェイルオーバーはシームレスです。クライアント上で実行されているアプリケーションは、フェイルオーバーが発生したことを認識しません。監視プロトコルを使用できなくてもフェイルオーバー処理に影響はありませんが、監視プロトコルを使用しないフェイルオーバーは効率が落ちます。

監視プロトコルを使用する高度なフェイルオーバーは、次の要件が満たされた場合に実行できます。

- SMB 3.0 が有効になっている SMB 3.0 対応の CIFS サーバでのみ使用できる。
- 共有で、共有の継続的な可用性プロパティが設定されている SMB 3.0 を使用している必要があります。
- アプリケーションサーバの接続先のノードの SFO パートナーに、少なくとも 1 つ以上、アプリケーションサーバのデータをホスティングする Storage Virtual Machine (SVM) に割り当てられた運用中のデータ LIF がある。



監視プロトコルは、SFO ペアの間で実行されます。LIF はクラスタ内の任意のノードに移行できるため、すべてのノードがその SFO パートナーの監視プロトコルであることが必要になる場合があります。アプリケーションサーバのデータをホスティングしている SVM がパートナーノード上にアクティブなデータ LIF を持っていない場合、監視プロトコルは、指定されたノード上で SMB 接続の迅速なフェイルオーバーを提供することはできません。したがって、そのような構成の 1 つをホスティングしている SVM には、クラスタ内のすべてのノードに少なくとも 1 つ以上のデータ LIF が必要です。

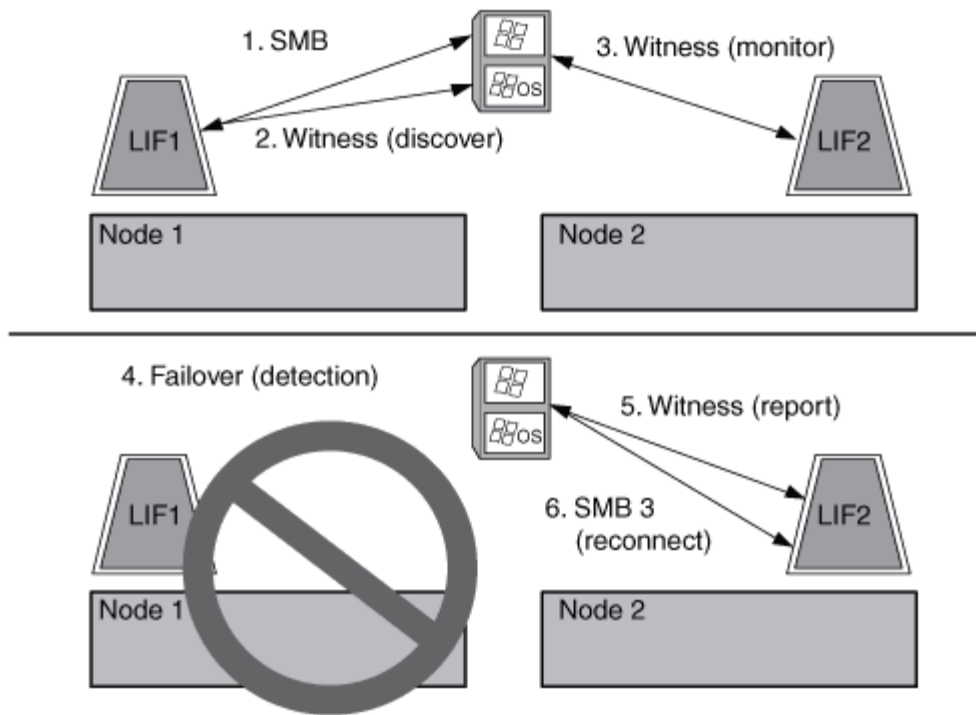
- アプリケーションサーバは、個々の LIF IP アドレスではなく、DNS に格納されている CIFS サーバ名を使用して CIFS サーバに接続する必要があります。

#### 監視プロトコルの仕組み

ONTAP では、ノードの SFO パートナーを監視役として使用して、監視プロトコルが実装されます。障害が発生すると、パートナーが障害を迅速に検出し、SMB クライアントに通知します。

監視プロトコルでは、次のプロセスを使用してフェイルオーバーが強化されます。

1. アプリケーションサーバがノード 1 への継続的な可用性が確保された SMB 接続を確立すると、CIFS サーバからアプリケーションサーバに監視が利用可能であることが通知されます。
2. アプリケーションサーバは、ノード 1 に監視サーバの IP アドレスを要求し、Storage Virtual Machine (SVM) に割り当てられたノード 2 (SFO パートナー) のデータ LIF の IP アドレスリストを受け取ります。
3. アプリケーションサーバは、いずれかの IP アドレスを選択し、ノード 2 への監視接続を作成して、ノード 1 の継続的な可用性が確保された接続を移行する必要がある場合に通知されるように登録します。
4. ノード 1 でフェイルオーバーが発生した場合、監視によってフェイルオーバーが容易になりますが、ギブバックには影響しません。
5. 監視によってフェイルオーバーイベントが検出され、監視接続を介してアプリケーションサーバに、SMB 接続をノード 2 に移行する必要があることが通知されます。
6. アプリケーションサーバは、SMB セッションをノード 2 に移行し、クライアントアクセスを中断することなく接続をリカバリします。



## リモート VSS による共有ベースのバックアップ

### リモート VSS による共有ベースのバックアップの概要

リモート VSS を使用して、CIFS サーバに格納された Hyper-V 仮想マシンファイルの共有ベースのバックアップを実行できます。

Microsoft リモート VSS（ボリュームシャドウコピーサービス）は、既存の Microsoft VSS インフラを拡張したものです。リモート VSS では、SMB 共有のシャドウコピーにも対応するように VSS インフラが拡張され、また、Hyper-V などのサーバアプリケーションでは、SMB ファイル共有に VHD ファイルを格納できます。これらの拡張機能を使用すると、データと構成ファイルを共有に格納する仮想マシンに対して、アプリケーションと整合性のあるシャドウコピーを作成できます。

### リモート VSS の概念

ここでは、リモート VSS（ボリュームシャドウコピーサービス）の概念について説明します。リモート VSS が Hyper-V over SMB 構成でバックアップサービスによってどのように使用されるかを理解するには、これらの概念を理解しておく必要があります。

#### • \* VSS（ボリューム・シャドウ・コピー・サービス） \*

特定の時点で特定のボリュームのバックアップコピーまたはデータの Snapshot を作成するために使用される Microsoft のテクノロジー。VSS は、データサーバ、バックアップアプリケーション、およびストレージ管理ソフトウェアを調整して、整合性のあるバックアップの作成と管理をサポートします。

#### • \* リモート VSS（リモートボリュームシャドウコピーサービス） \*

SMB 3.0 共有を介してデータにアクセスした特定の時点における整合性が取れた共有ベースのバックアップコピーを作成する Microsoft のテクノロジーです。Volume Shadow Copy Service と呼ばれることもあります。

- \* シャドウコピー \*

共有に含まれるデータセットの明確に定義された特定の時点における複製です。シャドウコピーを使用すると、システムやアプリケーションによる元のボリュームのデータ更新を継続したまま、整合性が取れたポイントインタイムバックアップを作成できます。

- \* シャドウ・コピー・セット \*

1 つ以上のシャドウコピーの集合です。各シャドウコピーが 1 つの共有に対応します。シャドウコピーセット内のシャドウコピーに対応する共有は、すべて同じ処理でバックアップする必要があります。セットに含めるシャドウコピーは、VSS に対応したアプリケーションの VSS クライアントで識別されます。

- \* シャドウ・コピー・セットの自動リカバリ \*

リモート VSS に対応したバックアップアプリケーションのバックアッププロセスの一環として実行される、シャドウコピーを格納するレプリカディレクトリの整合性が取れたポイントインタイムコピーを作成する処理です。バックアップの開始時に、アプリケーションの VSS クライアントで、バックアップ対象としてスケジュールされたデータ（Hyper-V の場合は仮想マシンファイル）にソフトウェアチェックポイントを設定する処理が開始されます。これにより、VSS クライアントでアプリケーションの続行が許可されます。シャドウコピーセットが作成されると、リモート VSS によってシャドウコピーセットが書き込み可能にされ、書き込み可能なコピーがアプリケーションに公開されます。アプリケーションでは、シャドウコピーセットをバックアップする準備として、前の処理で作成されたソフトウェアチェックポイントを使用して自動リカバリを実行します。自動リカバリでは、チェックポイントの作成後にファイルやディレクトリに対して行われた変更を元に戻すことで、シャドウコピーを整合性のある状態にします。自動リカバリは、VSS に対応したバックアップのオプションの手順です。

- \* シャドウ・コピー ID \*

シャドウコピーを一意に識別する GUID です。

- \* シャドウ・コピー・セット ID \*

同じサーバに対する一連のシャドウコピー ID を一意に識別する GUID です。

- \* SnapManager for Hyper-V \*

Microsoft Windows Server 2012 Hyper-V のバックアップとリストアの処理を自動化して簡単に実行できるようにするソフトウェアです。SnapManager for Hyper-V では、リモート VSS と自動リカバリを使用して、SMB 共有を介して Hyper-V ファイルをバックアップします。

## 関連情報

[Hyper-V および SQL Server over SMB のノンストップオペレーションの主要な概念](#)

[リモート VSS による共有ベースのバックアップ](#)

リモート **VSS** で使用されるディレクトリ構造の例

リモート VSS は、シャドウコピーの作成時に、Hyper-V 仮想マシンファイルが格納されているディレクトリ構造をトラバースします。仮想マシンファイルのバックアップを正しく作成できるように、適切なディレクトリ構造について理解しておくことが重要です。

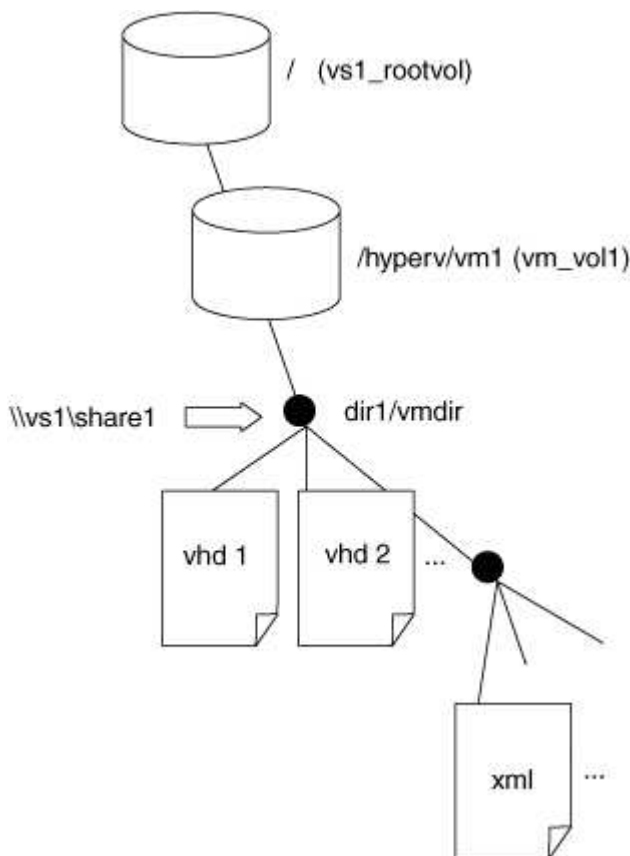
シャドウコピーを正常に作成するためにサポートされるディレクトリ構造は、次の要件を満たしています。

- 仮想マシンファイルの格納に使用されるディレクトリ構造内に存在するのは、ディレクトリと通常のファイルだけです。

ディレクトリ構造には、ジャンクション、リンク、通常以外のファイルは含まれません。

- 仮想マシンのファイルはすべて単一の共有内に存在します。
- 仮想マシンファイルの格納に使用されるディレクトリ構造は、設定されたシャドウコピーディレクトリの階層より深くなりません。
- 共有のルートディレクトリには、仮想マシンファイルまたはディレクトリのみが含まれます。

次の図では、ジャンクションポイントがであるvm\_vol1という名前のボリュームが作成されています /hyperv/vm1 Storage Virtual Machine (SVM) vs1上。ジャンクションポイントの下には、仮想マシンファイルを格納するサブディレクトリが作成されます。Hyper-Vサーバの仮想マシンファイルには、パスのshare1を介してアクセスします /hyperv/vm1/dir1/vmdir。シャドウコピーサービスによって、share1 の下のディレクトリ構造内（設定されたシャドウコピーのディレクトリ階層まで）に格納されたすべての仮想マシンファイルのシャドウコピーが作成されます。



#### SnapManager for Hyper-V による Hyper-V over SMB のリモート VSS ベースのバックアップの管理方法

SnapManager for Hyper-V を使用して、リモート VSS ベースのバックアップサービス进行管理できます。スペース効率に優れたバックアップセットを作成するには、SnapManager for Hyper-V で管理されているバックアップサービスを使用すると効果的です。

Hyper-V で管理されているバックアップ向けに SnapManager を最適化するには、次のようなものがあります。

- SnapDrive と ONTAP の統合により、SMB 共有の場所を検出する際のパフォーマンスが最適化されます。

ONTAP は、共有が存在するボリュームの名前を SnapDrive に提供します。

- SnapManager for Hyper-V は、シャドウコピーサービスでコピーする必要がある SMB 共有内の仮想マシンファイルのリストを指定します。

仮想マシンファイルの対象リストを指定することで、シャドウコピーサービスで、共有内のすべてのファイルのシャドウコピーを作成する必要がなくなります。

- Storage Virtual Machine (SVM) に、Hyper-V がリストアに使用するための SnapManager の Snapshot コピーが保持されます。

バックアップフェーズはありません。バックアップは、スペース効率に優れた Snapshot コピーです。

SnapManager for Hyper-V は、次のプロセスを使用して、Hyper-V over SMB のバックアップとリストアの機能を提供します。

#### 1. シャドウコピー処理を準備しています

SnapManager for Hyper-V アプリケーションの VSS クライアントが、シャドウコピーセットを設定します。VSS クライアントは、どの共有をシャドウコピーセットに含めるかに関する情報を収集し、この情報を ONTAP に提供します。セットには 1 つ以上のシャドウコピーが含まれる場合があり、1 つのシャドウコピーが 1 つの共有に対応します。

#### 2. シャドウコピーセットの作成（自動リカバリが使用される場合）

シャドウコピーセットに含まれている共有ごとに、ONTAP がシャドウコピーを作成し、シャドウコピーを書き込み可能にします。

#### 3. シャドウコピーセットの公開

ONTAP によって作成されたシャドウコピーが Hyper-V 用の SnapManager に公開され、アプリケーションの VSS ライターが自動リカバリを実行できるようになります。

#### 4. シャドウコピーセットを自動的にリカバリします

シャドウコピーセットの作成中に、バックアップセットに含まれているファイルにアクティブな変更が発生する時間帯があります。アプリケーションの VSS ライターは、シャドウコピーを更新して、バックアップ前に完全な整合性が確保された状態にする必要があります。



自動リカバリの実行方法はアプリケーションに固有です。リモート VSS はこのフェーズには関連しません。

#### 5. シャドウコピーセットの完了とクリーンアップを行います

自動リカバリの完了後に、VSS クライアントが ONTAP に通知します。シャドウコピーセットが読み取り専用になり、バックアップできる状態になります。バックアップに SnapManager for Hyper-V を使用する場合は、Snapshot コピー内のファイルがバックアップになるため、バックアップフェーズでは、バック

クアッパセット内の共有を含むボリュームごとに Snapshot コピーが作成されます。バックアップが完了すると、シャドウコピーセットが CIFS サーバから削除されます。

## Hyper-V over SMB および SQL Server over SMB 共有での ODX コピーオフロードの使用 方法

Offloaded Data Transfer (ODX ; オフロードデータ転送) は `_copy offloaded_` と呼ばれ、この機能を使用すると、互換性があるストレージデバイス内やストレージデバイス間で、ホストコンピュータを介さずにデータを直接転送できます。ONTAP ODX コピーオフロードを使用すると、アプリケーションサーバで SMB 環境経由のコピー処理を実行する際のパフォーマンスが向上します。

ODX 以外のファイル転送では、ソース CIFS サーバからデータが読み取られ、ネットワーク経由でクライアントコンピュータに転送されます。クライアントコンピュータは、データをネットワーク経由でデスティネーション CIFS サーバに転送します。つまり、クライアントコンピュータはソースからデータを読み取り、デスティネーションに書き込みます。ODX ファイル転送では、データはソースからデスティネーションに直接コピーされます。

ODX オフロードコピーはソースストレージとデスティネーションストレージの間で直接実行されるため、パフォーマンスが大幅に向上します。実現するパフォーマンスの向上には、ソースとデスティネーションの間のコピー時間の短縮、クライアントでのリソース使用量 (CPU、メモリ) の削減、ネットワーク I/O 帯域幅の使用量の削減などが挙げられます。

```
ONTAP ODX copy offload is supported on both SAN LUNs and SMB 3.0  
continuously available connections.
```

ODX コピーおよび移動の使用は、以下のユースケースでサポートされます。

- ボリューム内

ソースとデスティネーションのファイルまたは LUN は、同じボリューム内にあります。

- ボリュームが異なり、ノードと Storage Virtual Machine (SVM) は同じ

ソースとデスティネーションのファイルまたは LUN は、同じノード上の異なるボリュームにあります。データは同じ SVM に所有されます。

- ボリュームとノードが異なり、SVM は同じです

ソースとデスティネーションのファイルまたは LUN は、異なるノード上の異なるボリュームにあります。データは同じ SVM に所有されます。

- SVM が異なり、ノードは同じです

ソースとデスティネーションのファイルまたは LUN は、同じノード上の異なるボリュームにあります。データは異なる SVM に所有されます。

- SVM とノードが異なります

ソースとデスティネーションのファイルまたは LUN は、異なるノード上の異なるボリュームにありま



す。データは異なる SVM に所有されます。

Hyper-V ソリューションでの ODX コピーオフロードの具体的な用途には、次のようなものがあります。

- Hyper-V で ODX コピーオフロードのパススルーを使用して、仮想ハードディスク（VHD）ファイル内および VHD ファイル間でのデータのコピー、または同じクラスタ内のマッピングされた SMB 共有と接続された iSCSI LUN の間でのデータのコピーを実行できます。

これにより、ゲストオペレーティングシステムからのコピーを基盤となるストレージに渡すことができます。

- 容量固定 VHD を作成する際に、ODX を使用して、既知の初期化済みトークンによってディスクを初期化します。
- ソースとデスティネーションのストレージが同じクラスタにある場合に、ODX コピーオフロードを使用して、仮想マシンのストレージを移行します。



Hyper-V での ODX コピーオフロードのパススルーの用途を活用するには、ゲストオペレーティングシステムで ODX がサポートされている必要があります。また、ゲストオペレーティングシステムのディスクが、ODX をサポートするストレージ（SMB または SAN）から作成された SCSI ディスクである必要があります。ゲストオペレーティングシステムのディスクが IDE ディスクの場合、ODX のパススルーはサポートされません。

SQL Server ソリューションでの ODX コピーオフロードの具体的な用途には、次のようなものがあります。

- ODX コピーオフロードを使用して、マッピングされた SMB 共有間、または同じクラスタ内の SMB 共有と接続された iSCSI LUN の間で SQL Server データベースのエクスポートとインポートを行うことができます。
- ソースとデスティネーションのストレージが同じクラスタにある場合に、ODX コピーオフロードを使用して、データベースのエクスポートとインポートを行います。

## 設定に関する要件と考慮事項

### ONTAP とライセンスの要件

SVM でノンストップオペレーションを実現する SQL Server over SMB または Hyper-V over SMB ソリューションを作成するときは、ONTAP とライセンスの特定の要件について理解しておく必要があります。

#### ONTAP のバージョンの要件

- Hyper-V over SMB

ONTAP では、Windows Server 2012 以降で実行される Hyper-V での SMB 共有を介したノンストップオペレーションがサポートされます。

- SQL Server over SMB

ONTAP では、Windows Server 2012 以降で実行される SQL Server 2012 以降での SMB 共有を介したノンストップオペレーションがサポートされます。



SMB 共有を介したノンストップオペレーションがサポートされる ONTAP、Windows Server、および SQL Server のバージョンの最新情報については、Interoperability Matrix を参照してください。

## "NetApp Interoperability Matrix Tool で確認できます"

### ライセンス要件

次のライセンスが必要です。

- CIFS
- FlexClone （Hyper-V over SMB のみ）

このライセンスは、バックアップにリモート VSS を使用する場合に必要になります。シャドウコピーサービスでは、バックアップの作成時に使用されるファイルのポイントインタイムコピーを作成するために FlexClone が使用されます。

リモート VSS を使用しないバックアップ方式を使用する場合、FlexClone ライセンスはオプションです。

FlexCloneのライセンスは、["ONTAP One"](#)。ONTAP Oneをお持ちでない場合は、["必要なライセンスがインストールされていることを確認する"](#)、および必要に応じて、["インストールする"](#)。

### ネットワークとデータ LIF の要件

ノンストップオペレーション用に SQL Server または Hyper-V over SMB 構成を作成する場合、一定のネットワークとデータ LIF 要件について理解しておく必要があります。

#### ネットワークプロトコルの要件

- IPv4 および IPv6 のネットワークがサポートされています。
- SMB 3.0 以降が必要です。

SMB 3.0 には、ノンストップオペレーションを実現するために必要となる継続的可用性を備えた SMB 接続の確立に欠かせない機能が備わっています。

- DNS サーバには、CIFS サーバ名を Storage Virtual Machine （SVM）上のデータ LIF に割り当てられた IP アドレスにマッピングするエントリが格納されている必要があります。

通常、Hyper-V または SQL Server アプリケーションサーバは、仮想マシンまたはデータベースファイルへのアクセス時に複数のデータ LIF を介して複数の接続を確立します。正常に機能するには、アプリケーションサーバは、複数の一意の IP アドレスへの複数の接続を確立するのではなく、CIFS サーバ名を使用してこのような複数の SMB 接続を確立する必要があります。

監視でも、個々の LIF の IP アドレスではなく CIFS サーバの DNS 名を使用する必要があります。

ONTAP 9.4 以降では、SMB マルチチャネルを有効にすることで、Hyper-V over SMB 構成と SQL Server over SMB 構成のスループットとフォールトトレランスを向上させることができます。そのためには、クラスタとクライアントに 1G、10G、またはそれ以上の NIC を複数導入しておく必要があります。

## データ LIF の要件

- SMB 解決策経由のアプリケーションサーバをホストする SVM には、クラスタ内のすべてのノードに稼働しているデータ LIF が少なくとも 1 つ必要です。

SVM データ LIF は、アプリケーションサーバがアクセスするデータを現在ホストしていないノードを含む、クラスタ内の他のデータポートにフェイルオーバーできます。さらに、監視ノードは常に、アプリケーションサーバが接続されているノードの SFO パートナーであるため、クラスタ内のどのノードも監視ノードになる可能性があります。

- データ LIF は、自動リバートするように設定されていない必要があります。

テイクオーバーまたはギブバックの発生後は、データ LIF をホームポートに手動でリバートする必要があります。

- データ LIF のすべての IP アドレスが DNS 内にエントリを保持する必要があり、すべてのエントリが CIFS サーバ名に解決される必要があります。

アプリケーションサーバは、CIFS サーバ名を使用して SMB 共有に接続する必要があります。LIF IP アドレスを使用して接続を確立するようにアプリケーションサーバを設定しないでください。

- CIFS サーバ名が SVM 名と異なる場合は、DNS エントリが CIFS サーバ名に解決される必要があります。

## Hyper-V over SMB 用の SMB サーバとボリュームの要件

ノンストップオペレーション用に Hyper-V over SMB 構成を作成する場合、一定の SMB サーバとボリュームの要件について理解しておく必要があります。

### SMBサーバの要件

- SMB 3.0 が有効になっている必要があります。

これはデフォルトで有効になっています。

- デフォルトの UNIX ユーザの CIFS サーバオプションが、有効な UNIX ユーザアカウントを使用して設定されている必要があります。

アプリケーションサーバでは、SMB 接続を確立する際にマシンアカウントが使用されます。すべての SMB アクセスで、Windows ユーザが任意の UNIX ユーザアカウントまたはデフォルトの UNIX ユーザアカウントに正常にマッピングされる必要があるため、ONTAP は、アプリケーションサーバのマシンアカウントをデフォルトの UNIX ユーザアカウントにマッピングできる必要があります。

- 自動ノードリファラールを無効にする必要があります（この機能はデフォルトで無効になります）。

Hyper-V マシンファイル以外のデータにアクセスするために自動ノードリファラールを使用する場合は、そのデータ用に別の SVM を作成する必要があります。

- SMB サーバが属しているドメインで、Kerberos と NTLM の両方の認証が許可されている必要があります。

ONTAP ではリモート VSS に対して Kerberos サービスがアドバタイズされないため、ドメインが NTLM を許可するように設定されている必要があります。

- ・シャドウコピー機能を有効にする必要があります。

この機能はデフォルトで有効になっています。

- ・シャドウコピーサービスでシャドウコピーの作成時に使用される Windows ドメインアカウントが、SMB サーバのローカルの BUILTIN\Administrators グループまたは BUILTIN\Backup Operators グループに属している必要があります。

ボリューム要件：

- ・仮想マシンファイルを格納するためのボリュームは、NTFS セキュリティ形式のボリュームとして作成されている必要があります。

継続的な可用性が確保された SMB 接続を使用してアプリケーションサーバの NDO を実現するには、共有を含むボリュームが NTFS ボリュームである必要があります。さらに、そのボリュームが常に NTFS ボリュームである必要があります。mixed セキュリティ形式のボリュームまたは UNIX セキュリティ形式のボリュームを NTFS セキュリティ形式のボリュームに変更し、そのボリュームを SMB 共有を介して直接 NDO に使用することはできません。mixed セキュリティ形式のボリュームを NTFS セキュリティ形式のボリュームに変更し、SMB 共有を介して NDO に使用する場合は、ボリュームの一番上に ACL を手動で配置し、格納されているすべてのファイルおよびフォルダにその ACL を適用する必要があります。そうしないと、ソースボリュームまたはデスティネーションボリュームが最初は mixed セキュリティ形式または UNIX セキュリティ形式のボリュームとして作成され、あとで NTFS セキュリティ形式に変更された場合は、ファイルを別のボリュームに移動する仮想マシンの移行またはデータベースファイルのエクスポートとインポートに失敗する可能性があります。

- ・シャドウコピー処理を正常に実行するには、ボリュームに十分な利用可能スペースが必要です。

使用可能なスペースは、シャドウコピーバックアップセットに含まれている共有内のすべてのファイル、ディレクトリ、およびサブディレクトリによって使用される合計スペースと同サイズ以上である必要があります。この要件は、自動リカバリを使用する環境シャドウコピーのみです。

## 関連情報

"Microsoft TechNet ライブラリ： [technet.microsoft.com/en-us/library/](https://technet.microsoft.com/en-us/library/)"

## SQL Server over SMB 用の SMB サーバとボリュームの要件

ノンストップオペレーション用に SQL Server over SMB 構成を作成する場合、SMB サーバとボリュームの要件について理解しておく必要があります。

### SMBサーバの要件

- ・SMB 3.0 が有効になっている必要があります。

これはデフォルトで有効になっています。

- ・デフォルトの UNIX ユーザの CIFS サーバオプションが、有効な UNIX ユーザアカウントを使用して設定されている必要があります。

アプリケーションサーバでは、SMB 接続を確立する際にマシンアカウントが使用されます。すべての SMB アクセスで、Windows ユーザが任意の UNIX ユーザアカウントまたはデフォルトの UNIX ユーザアカウントに正常にマッピングされる必要があるため、ONTAP は、アプリケーションサーバのマシンアカウントをデフォルトの UNIX ユーザアカウントにマッピングできる必要があります。

さらに、SQL Server はドメインユーザを SQL Server サービスアカウントとして使用します。サービスアカウントは、デフォルトの UNIX ユーザにもマッピングする必要があります。

- 自動ノードリファールを無効にする必要があります（この機能はデフォルトで無効になります）。

SQL Server データベースファイル以外のデータへのアクセスに自動ノードリファールを使用する場合、そのデータ用の SVM を個別に作成する必要があります。

- ONTAP への SQL Server のインストールに使用する Windows ユーザアカウントには、SeSecurityPrivilege 権限を割り当てる必要があります。

この権限は、SMB サーバのローカル BUILTIN\Administrators グループに割り当てられます。

ボリューム要件：

- 仮想マシンファイルを格納するためのボリュームは、NTFS セキュリティ形式のボリュームとして作成されている必要があります。

継続的な可用性が確保された SMB 接続を使用してアプリケーションサーバの NDO を実現するには、共有を含むボリュームが NTFS ボリュームである必要があります。さらに、そのボリュームが常に NTFS ボリュームである必要があります。mixed セキュリティ形式のボリュームまたは UNIX セキュリティ形式のボリュームを NTFS セキュリティ形式のボリュームに変更し、そのボリュームを SMB 共有を介して直接 NDO に使用することはできません。mixed セキュリティ形式のボリュームを NTFS セキュリティ形式のボリュームに変更し、SMB 共有を介して NDO に使用する場合は、ボリュームの一番上に ACL を手動で配置し、格納されているすべてのファイルおよびフォルダにその ACL を適用する必要があります。そうしないと、ソースボリュームまたはデスティネーションボリュームが最初は mixed セキュリティ形式または UNIX セキュリティ形式のボリュームとして作成され、あとで NTFS セキュリティ形式に変更された場合は、ファイルを別のボリュームに移動する仮想マシンの移行またはデータベースファイルのエクスポートとインポートに失敗する可能性があります。

- データベースファイルが格納されたボリュームにジャンクションを含めることはできますが、SQL Server はデータベースディレクトリ構造の作成時にジャンクションを横断しません。
- SnapCenter Plug-in for Microsoft SQL Serverのバックアップ処理が成功するためには、ボリュームに十分な利用可能スペースが必要です。

SQL Server データベースファイルを格納するボリュームには、共有内にあるデータベースディレクトリ構造と、格納されているすべてのファイルを格納できる十分な容量が必要です。

関連情報

"Microsoft TechNet ライブラリ：[technet.microsoft.com/en-us/library/](https://technet.microsoft.com/en-us/library/)"

**Hyper-V over SMB** での継続的可用性を備えた共有の要件と考慮事項

ノンストップオペレーションをサポートする Hyper-V over SMB 構成で継続的可用性を備えた共有を設定する場合は、一定の要件と考慮事項に注意する必要があります。

共有の要件

- アプリケーションサーバが使用する共有には、継続的可用性が設定されている必要があります。

継続的可用性を備えた共有に接続するアプリケーションサーバは永続的ハンドルを受け取ります。永続的

ハンドルを使用すると、テイクオーバー、ギブバック、アグリゲートの再配置などの停止イベントのあとに SMB 共有に無停止で再接続し、ファイルロックを再取得することができます。

- リモート VSS に対応したバックアップサービスを使用する場合は、ジャンクションを含む共有に Hyper-V ファイルを配置することはできません。

自動リカバリの場合、共有のトラバース時にジャンクションが見つかった場合、シャドウコピーの作成は失敗します。自動リカバリではない場合、シャドウコピーの作成は失敗しませんが、ジャンクションは何も参照しません。

- リモート VSS に対応したバックアップサービスと自動リカバリを使用する場合は、以下を含む共有に Hyper-V ファイルを配置することはできません。

- シンボリックリンク、ハードリンク、またはワイドリンク
- 通常以外のファイル

シャドウコピーを実行する共有にリンクまたは通常以外のファイルが含まれている場合は、シャドウコピーの作成に失敗します。この要件は、自動リカバリを使用する環境シャドウコピーのみです。

- シャドウコピー処理を正常に実行するには、ボリュームに十分な利用可能スペースが必要です（Hyper-V over SMB の場合のみ）。

使用可能なスペースは、シャドウコピーバックアップセットに含まれている共有内のすべてのファイル、ディレクトリ、およびサブディレクトリによって使用される合計スペースと同サイズ以上である必要があります。この要件は、自動リカバリを使用する環境シャドウコピーのみです。

- アプリケーションサーバが使用する継続的可用性を備えた共有では、次の共有プロパティを設定しないでください。
  - ホームディレクトリ
  - 属性のキャッシュ
  - BranchCache

#### 考慮事項

- クォータは継続的可用性を備えた共有でサポートされます。
- Hyper-V over SMB の構成では、次の機能はサポートされません。
  - 監査
  - FPolicy の
- を使用した SMB 共有ではウィルススキャンは実行されません continuously-availability パラメータをに設定します Yes。

#### SQL Server over SMB での継続的可用性を備えた共有の要件と考慮事項

ノンストップオペレーションをサポートする SQL Server over SMB 構成で継続的可用性を備えた共有を設定する場合は、一定の要件と考慮事項に注意する必要があります。

## 共有の要件

- 仮想マシンファイルを格納するためのボリュームは、NTFS セキュリティ形式のボリュームとして作成されている必要があります。

継続的な可用性が確保された SMB 接続を使用してアプリケーションサーバのノンストップオペレーションを実現するには、共有を含むボリュームが NTFS ボリュームである必要があります。さらに、そのボリュームが常に NTFS ボリュームである必要があります。mixed セキュリティ形式のボリュームまたは UNIX セキュリティ形式のボリュームを NTFS セキュリティ形式のボリュームに変更し、そのボリュームを SMB 共有を介したノンストップオペレーションに直接使用することはできません。mixed セキュリティ形式のボリュームを NTFS セキュリティ形式のボリュームに変更し、そのボリュームを SMB 共有を介したノンストップオペレーションに使用する場合は、ボリュームの一番上に ACL を手動で配置し、格納されているすべてのファイルおよびフォルダにその ACL を適用する必要があります。そうしないと、ソースボリュームまたはデスティネーションボリュームが最初は mixed セキュリティ形式または UNIX セキュリティ形式のボリュームとして作成され、あとで NTFS セキュリティ形式に変更された場合は、ファイルを別のボリュームに移動する仮想マシンの移行またはデータベースファイルのエクスポートとインポートに失敗する可能性があります。

- アプリケーションサーバが使用する共有には、継続的可用性が設定されている必要があります。

継続的可用性を備えた共有に接続するアプリケーションサーバは永続的ハンドルを受け取ります。永続的ハンドルを使用すると、テイクオーバー、ギブバック、アグリゲートの再配置などの停止イベントのあとに SMB 共有に無停止で再接続し、ファイルロックを再取得することができます。

- データベースファイルが格納されたボリュームにジャンクションを含めることはできますが、SQL Server はデータベースディレクトリ構造の作成時にジャンクションを横断しません。
- SnapCenter Plug-in for Microsoft SQL Server の処理が成功するためには、ボリュームに十分な利用可能スペースが必要です。

SQL Server データベースファイルを格納するボリュームには、共有内にあるデータベースディレクトリ構造と、格納されているすべてのファイルを格納できる十分な容量が必要です。

- アプリケーションサーバが使用する継続的可用性を備えた共有では、次の共有プロパティを設定しないでください。
  - ホームディレクトリ
  - 属性のキャッシュ
  - BranchCache

## 共有に関する考慮事項

- クォータは継続的可用性を備えた共有でサポートされます。
- SQL Server over SMB 構成では、次の機能はサポートされません。
  - 監査
  - FPolicy の
- を使用した SMB 共有ではウィルススキャンは実行されません continuously-availability 共有プロパティが設定されました。

## Hyper-V over SMB 構成用のリモート VSS に関する考慮事項

Hyper-V over SMB 構成用のリモート VSS に対応したバックアップソリューションを使用する場合は、一定の考慮事項について理解しておく必要があります。

### 一般的なリモート VSS の考慮事項

- Microsoft のアプリケーションサーバ 1 つにつき、最大 64 の共有を設定できます。

1 つのシャドウコピーセットに 64 個を超える共有がある場合、シャドウコピー処理は失敗します。これは Microsoft の要件です。

- アクティブなシャドウコピーセットは、1 台の CIFS サーバで 1 つしか許可されません。

シャドウコピー処理は、同じ CIFS サーバ上で別のシャドウコピー処理が進行中である場合には失敗します。これは Microsoft の要件です。

- リモート VSS によってシャドウコピーが作成されるディレクトリ構造内では、ジャンクションは許可されません。
  - 自動リカバリの場合、共有のトラバース時にジャンクションが見つかり、シャドウコピーの作成は失敗します。
  - 自動リカバリではない場合、シャドウコピーの作成は失敗しませんが、ジャンクションは何も参照しません。

### 自動リカバリを行うシャドウコピーのみに適用されるリモート VSS の考慮事項

一部の制限は、自動リカバリを行うシャドウコピーにのみ適用されます。

- シャドウコピーの作成で許可される最大サブディレクトリ階層は 5 層です。

これは、シャドウコピーサービスによってシャドウコピーバックアップセットが作成されるディレクトリ階層です。仮想マシンのファイルを含むディレクトリのネストレベルが 5 よりも深い場合、シャドウコピーの作成は失敗します。この目的は、共有のクローニング時におけるディレクトリのトラバースを制限することです。最大ディレクトリ階層は CIFS サーバオプションを使用して変更できます。

- ボリューム上に利用可能なスペースが十分ある必要があります。

使用可能なスペースは、シャドウコピーバックアップセットに含まれている共有内のすべてのファイル、ディレクトリ、およびサブディレクトリによって使用される合計スペースと同サイズ以上である必要があります。

- リモート VSS によってシャドウコピーが作成されるディレクトリ構造内では、リンクまたは通常以外のファイルは許可されません。

シャドウコピーの作成は、そのシャドウコピーに対応する共有内にリンクまたは通常以外のファイルがある場合には失敗します。これらのファイルはクローニングプロセスでサポートされていません。

- ディレクトリに対する NFSv4 ACL は許可されません。

シャドウコピーの作成では、ファイルの NFSv4 ACL は維持されますが、ディレクトリの NFSv4 ACL は失われます。

- ・シャドウコピーセットの作成に許可される時間は最大 60 秒です。

Microsoft の仕様により、シャドウコピーセットの作成に許可される時間は最大 60 秒です。この時間内に VSS クライアントでシャドウコピーセットを作成できない場合、シャドウコピー処理は失敗します。したがって、シャドウコピーセット内のファイル数には制限があります。バックアップセットに含めることができる実際のファイル数または仮想マシン数は、一定ではなく、多くの要因に依存するため、お客様の環境ごとに判断する必要があります。

## SQL Server および Hyper-V over SMB 用の ODX コピーオフロード要件

アプリケーションサーバ経由でデータを送信せずに、仮想マシンファイルを移行する場合や、データベースファイルをソースストレージからデスティネーションストレージに直接エクスポートおよびインポートする場合は、ODX コピーオフロードが有効になっている必要があります。ODX コピーオフロードと SQL Server および Hyper-V over SMB ソリューションを使用する場合は、理解しておくべきいくつかの要件があります。

ODX コピーオフロードを使用すると、パフォーマンスが大幅に向上します。この CIFS サーバオプションは、デフォルトで有効に設定されています。

- ・ODX コピーオフロードを使用するには、SMB 3.0 が有効になっている必要があります。
- ・ソースボリュームは 1.25GB 以上でなければなりません。
- ・コピーオフロードに使用するボリュームで重複排除を有効にする必要があります。
- ・圧縮されたボリュームを使用する場合は、圧縮形式をアダプティブにする必要があります。サポートされる圧縮グループサイズは 8K のみです。

二次圧縮形式はサポートされません

- ・ODX コピーオフロードを使用して Hyper-V ゲストをディスク内やディスク間で移行するには、Hyper-V サーバが SCSI ディスクを使用するように設定されている必要があります。

デフォルトでは IDE ディスクが設定されますが、ディスクが IDE ディスクを使用して作成されている場合は、ゲストの移行時に ODX コピーオフロードは機能しません。

## SQL Server および Hyper-V over SMB 構成に関する推奨事項

SQL Server over SMB および Hyper-V over SMB 構成が安定して機能するようにするには、ソリューションの設定に関する推奨されるベストプラクティスについて理解しておく必要があります。

### 一般的な推奨事項

- ・アプリケーションサーバのファイルは一般的なユーザデータとは別に格納します。

可能な場合は、Storage Virtual Machine (SVM) とそのストレージ全体をアプリケーションサーバのデータ専用にします。

- ・パフォーマンスを最大限に高めるには、アプリケーションサーバのデータを格納する SVM で SMB 署名を無効にします。



- パフォーマンスの最適化とフォールトトレランスの向上を図るためには、SMB マルチチャネルを有効にして、1 つの SMB セッションで ONTAP とクライアントの間に複数の接続を確立できるようにします。
- Hyper-V または SQL Server over SMB 構成で使用する共有以外では、継続的可用性を備えた共有を作成しないようにします。
- 継続的な可用性を確保するために使用される共有については、変更通知を無効に
- アグリゲートの再配置（ARL）には一部の処理が一時停止するフェーズがあるため、ARL と同時にボリュームの移動を実行しないようにします。
- Hyper-V over SMB ソリューションでは、クラスタ化された仮想マシンを作成する際にゲスト内 iSCSI ドライブを使用します。共有 .VHDX ONTAP SMB共有のHyper-V over SMBではファイルがサポートされません。

## Hyper-V または SQL Server over SMB 構成を計画

ボリューム設定ワークシートに記入

このワークシートを使用すると、SQL Server および Hyper-V over SMB 構成用のボリュームを作成する際に必要となる値を簡単に記録できます。

ボリュームごとに、次の情報を指定する必要があります。

- Storage Virtual Machine （SVM）名

SVM 名はすべてのボリュームで同じです。

- ボリューム名
- アグリゲート名

ボリュームは、クラスタ内のノード上のアグリゲートに作成できます。

- サイズ
- ジャンクションパス

アプリケーションサーバのデータを格納するボリュームの作成時には、次の事項を考慮してください。

- ルートボリュームのセキュリティ形式が NTFS でない場合は、ボリュームの作成時にセキュリティ形式を NTFS として指定する必要があります。

デフォルトで、ボリュームは SVM ルートボリュームのセキュリティ形式を継承します。

- ボリュームには、デフォルトのボリュームスペースギャランティを設定する必要があります。
- 必要に応じて、スペースのオートサイズ管理を設定できます。
- Snapshotコピーのスペースリザベーションを決定するオプションは、に設定する必要があります 0。
- ボリュームに適用される Snapshot ポリシーを無効にする必要があります。

SVM の Snapshot ポリシーが無効になっている場合は、ボリュームの Snapshot ポリシーを指定する必要はありません。ボリュームは SVM の Snapshot ポリシーを継承します。SVM の Snapshot ポリシーが無効になっておらず、Snapshot コピーを作成するように設定されている場合は、Snapshot ポリシーをボ

リウムレベルで指定し、そのポリシーを無効にする必要があります。Snapshot コピーの作成と削除は、シャドウコピーサービス対応のバックアップと SQL Server バックアップによって管理されます。

- ボリュームに負荷共有ミラーを設定することはできません。

アプリケーションサーバで使用される共有を作成するジャンクションパスを選択する際は、共有エントリポイントの下に結合されたボリュームが含まれないようにする必要があります。

たとえば、仮想マシンファイルを「vol1」、「vol2」、「vol3」、および「vol4」という名前の4つのボリュームに格納する場合は、例に示すネームスペースを作成できます。その後、次のパスにアプリケーションサーバの共有を作成できます。 /data1/vol1、 /data1/vol2、 /data2/vol3`および ` /data2/vol4。

Vserver	Volume	Junction		Junction Path Source
		Active	Junction Path	
vs1	data1	true	/data1	RW_volume
vs1	vol1	true	/data1/vol1	RW_volume
vs1	vol2	true	/data1/vol2	RW_volume
vs1	data2	true	/data2	RW_volume
vs1	vol3	true	/data2/vol3	RW_volume
vs1	vol4	true	/data2/vol4	RW_volume

情報の種類	値
Volume 1：ボリューム名、アグリゲート、サイズ、ジャンクションパス _	
_ ボリューム 2：ボリューム名、アグリゲート、サイズ、ジャンクションパス _	
ボリューム3：ボリューム名、アグリゲート、サイズ、ジャンクションパス	
ボリューム4：ボリューム名、アグリゲート、サイズ、ジャンクションパス	
ボリューム5：ボリューム名、アグリゲート、サイズ、ジャンクションパス	
ボリューム6：ボリューム名、アグリゲート、サイズ、ジャンクションパス	
追加ボリューム：ボリューム名、アグリゲート、サイズ、ジャンクションパス _	

## SMB 共有設定ワークシートに記入

このワークシートを使用して、SQL Server および Hyper-V over SMB 構成用に継続的可用性を備えた SMB 共有を作成する際に必要となる値を記録してください。

### SMB 共有のプロパティおよび設定に関する情報

共有ごとに、次の情報を指定する必要があります。

- Storage Virtual Machine (SVM) 名

SVM 名はすべての共有で同じです

- 共有名
- パス
- 共有プロパティ

次の 2 つの共有プロパティを設定する必要があります。

- oplocks
- continuously-available

次の共有プロパティは設定しないでください。

- homedirectory attributecache
- branchcache
- access-based-enumeration
  - シンボリックリンクが無効になっている必要があります (の値) `-symlink-properties` パラメータは null にする必要があります[""] ) 。

### 共有パスに関する情報

リモート VSS を使用して Hyper-V ファイルをバックアップする場合は、Hyper-V サーバから仮想マシンファイルの格納場所への SMB 接続を確立する際に使用する共有パスの選択が重要になります。共有はネームスペース内の任意のポイントに作成できますが、Hyper-V サーバで使われる共有のパスに結合されたボリュームを含めることはできません。ジャンクションポイントを含む共有パスでシャドウコピー処理を実行することはできません。

データベースディレクトリ構造を作成する場合、SQL Server はジャンクションを横断できません。ジャンクションポイントを含む SQL Server の共有パスは作成しないでください。

たとえば、次に示すネームスペースを例にとると、仮想マシンファイルまたはデータベースファイルをボリューム「vol1」、「vol2」、「vol3」、および「vol4」に格納する場合は、アプリケーションサーバの共有を次のパスに作成する必要があります。/data1/vol1、/data1/vol2、/data2/vol3`および`/data2/vol4。

Vserver	Volume	Junction		Junction Path Source
		Active	Junction Path	
vs1	data1	true	/data1	RW_volume
vs1	vol1	true	/data1/vol1	RW_volume
vs1	vol2	true	/data1/vol2	RW_volume
vs1	data2	true	/data2	RW_volume
vs1	vol3	true	/data2/vol3	RW_volume
vs1	vol4	true	/data2/vol4	RW_volume



共有は上で作成できますが /data1 および /data2 パス管理管理用に、これらの共有を使用してデータを格納するようにアプリケーションサーバを設定しないでください。

#### 計画ワークシート

情報の種類	値
_ ボリューム 1 : SMB 共有名およびパス _	
ボリューム2: <i>SMB</i> 共有名とパス	
ボリューム3: <i>SMB</i> 共有名とパス	
ボリューム4: <i>SMB</i> 共有名とパス	
ボリューム5: <i>SMB</i> 共有名とパス	
ボリューム6: <i>SMB</i> 共有名とパス	
ボリューム7: <i>SMB</i> 共有名とパス	
追加ボリューム: SMB 共有名およびパス _	

## Hyper-V over SMB および SQL Server over SMB でノンストップオペレーションを実現するための ONTAP 設定を作成します

**Hyper-V** および **SQL Server over SMB** の概要を使用して、ノンストップオペレーション用の **ONTAP** 設定を作成します

SMB を介したノンストップオペレーションを実現する Hyper-V および SQL Server 環境を使用するためには、ONTAP の設定手順をいくつか実行する必要があります。

Hyper-V over SMB および SQL Server over SMB でノンストップオペレーションを実現する ONTAP 構成を作成する前に、次の作業を完了する必要があります。

- クラスタでタイムサービスがセットアップされている必要があります。
- SVM 用のネットワークをセットアップします。
- SVM を作成します。
- SVM でデータ LIF インターフェイスを設定します。
- SVM で DNS を設定します。
- SVM に必要なネームサービスをセットアップします。
- SMBサーバを作成しておく必要があります。

## 関連情報

[Hyper-V または SQL Server over SMB 構成を計画](#)

## 設定に関する要件と考慮事項

**Kerberos** 認証および **NTLMv2** 認証の両方が許可されていることを確認する（**Hyper-V over SMB** 共有）

Hyper-V over SMB のノンストップオペレーションを実行する場合、データ SVM の CIFS サーバおよび Hyper-V サーバで Kerberos 認証と NTLMv2 認証の両方が許可されていなければなりません。CIFS サーバと Hyper-V サーバの両方について、使用できる認証方法を制御する設定を確認する必要があります。

### このタスクについて

Kerberos 認証は、継続的可用性を備えた共有への接続を確立する際に必要になります。また、リモート VSS のプロセスで NTLMv2 認証が使用されます。そのため、Hyper-V over SMB 構成に対しては、両方の認証方法を使用した接続がサポートされている必要があります。

Kerberos 認証と NTLMv2 認証の両方が許可されるように、次の設定を行う必要があります。

- Storage Virtual Machine （SVM）で SMB のエクスポートポリシーが無効になっている必要があります。

SVM では、Kerberos 認証と NTLMv2 認証がどちらも常に有効になりますが、エクスポートポリシーを使用することで認証方法に基づいてアクセスを制限することが可能です。

SMB のエクスポートポリシーは省略可能で、デフォルトでは無効になっています。エクスポートポリシーが無効になっている場合、CIFS サーバでは Kerberos 認証と NTLMv2 認証の両方がデフォルトで許可されます。

- CIFS サーバと Hyper-V サーバが属するドメインで、Kerberos 認証と NTLMv2 認証の両方を許可する必要があります。

Kerberos 認証は、Active Directory ドメインではデフォルトで有効になります。ただし、NTLMv2 認証は、セキュリティポリシーの設定またはグループポリシーで禁止されている場合があります。

## 手順

1. 次の手順に従って、SVM でエクスポートポリシーが無効になっていることを確認します。
  - a. 権限レベルを advanced に設定します。

```
set -privilege advanced
```

- b. を確認します `-is-exportpolicy-enabled` CIFSサーバオプションがに設定されている `false` :

```
vserver cifs options show -vserver vserver_name -fields vserver,is-exportpolicy-enabled
```

- c. admin 権限レベルに戻ります。

```
set -privilege admin
```

2. SMB のエクスポートポリシーが無効になっていない場合は無効にします。

```
vserver cifs options modify -vserver vserver_name -is-exportpolicy-enabled false
```

3. ドメインで NTLMv2 認証と Kerberos 認証の両方が許可されていることを確認します。

ドメインで許可されている認証方法を確認する方法については、Microsoft TechNet ライブラリを参照してください。

4. ドメインで NTMLv2 認証が許可されていない場合は、Microsoft のドキュメントに記載されたいずれかの方法で NTLMv2 認証を有効にします。

#### 例

次に、SVM vs1 で SMB のエクスポートポリシーが無効になっていることを確認するコマンドの例を示します。

```
cluster1::> set -privilege advanced
Warning: These advanced commands are potentially dangerous; use them
only when directed to do so by technical support personnel.
Do you wish to continue? (y or n): y

cluster1::*> vserver cifs options show -vserver vs1 -fields vserver,is-
exportpolicy-enabled

vserver  is-exportpolicy-enabled
-----
vs1      false

cluster1::*> set -privilege admin
```

ドメインアカウントがデフォルトの **UNIX** ユーザにマッピングされていることを確認します

Hyper-V および SQL Server では、継続的可用性を備えた共有への SMB 接続を作成する際にドメインアカウントを使用します。接続を作成するには、コンピュータアカウントが UNIX ユーザに正しくマッピングされている必要があります。そのための最も便利な方法は、コンピュータアカウントをデフォルトの UNIX ユーザにマッピングすることです。

このタスクについて

Hyper-V および SQL Server は、ドメインコンピュータアカウントを使用して SMB 接続を作成します。また、SQL Server は、SMB 接続を作成するサービスアカウントとしてドメインユーザアカウントを使用します。

Storage Virtual Machine (SVM) を作成すると、「pcuser」という名前のデフォルトユーザがONTAP によって自動的に作成されます (UIDはになります) 65534) および「pcuser」という名前のグループ (GIDはです `65534` をクリックし、デフォルトユーザを"pcuser"グループに追加します。クラスタを Data ONTAP 8.2 にアップグレードする前に使用していた SVM で Hyper-V over SMB 解決策を設定する場合は、デフォルトのユーザとグループが存在していない可能性があります。デフォルトの UNIX ユーザを設定していない場合は、CIFS サーバのデフォルトの UNIX ユーザを設定する前に、デフォルトのユーザとグループを作成する必要があります。

手順

1. デフォルトの UNIX ユーザが存在するかどうかを確認します。

```
vserver cifs options show -vserver vserver_name
```

2. デフォルトユーザオプションが設定されていない場合は、デフォルトの UNIX ユーザとして指定できる UNIX ユーザが存在するかどうかを確認します。

```
vserver services unix-user show -vserver vserver_name
```

3. デフォルトユーザオプションが設定されておらず、デフォルトの UNIX ユーザとして指定できる UNIX ユーザも存在しない場合は、デフォルトの UNIX ユーザとデフォルトのグループを作成し、デフォルトのユーザをそのグループに追加します。

通常、デフォルトユーザにはユーザ名「pcuser」が与えられ、のUIDを割り当てる必要があります 65534。デフォルトのグループには '通常' グループ名として pcuser が与えられますグループに割り当てるGIDはである必要があります 65534。

- a. デフォルトグループを作成します。

[+]

```
vserver services unix-group create -vserver vserver_name -name pcuser -id 65534
```

- b. デフォルトユーザを作成し、デフォルトグループに追加します。

[+]

```
vserver services unix-user create -vserver vserver_name -user pcuser -id 65534 -primary-gid 65534
```

- c. デフォルトのユーザとデフォルトグループが正しく設定されていることを確認します。

```
[] `vserver services unix-user show -vserver _vserver_name_*` []
```

```
vserver services unix-group show -vserver vserver_name -members
```

4. CIFS サーバのデフォルトのユーザが設定されていない場合は、次の手順を実行します。

- a. デフォルトユーザを設定します。

```
vserver cifs options modify -vserver *vserver_name -default-unix-user pcuser*
```

- b. デフォルトの UNIX ユーザが正しく設定されていることを確認します。

## **vserver cifs options show -vserver vserver\_name**

5. アプリケーションサーバのコンピュータアカウントがデフォルトのユーザに正しくマッピングされていることを確認するには、SVMの共有にドライブをマッピングし、を使用してWindowsユーザとUNIXユーザのマッピングを確認します `vserver cifs session show` コマンドを実行します

このコマンドの使用の詳細については、マニュアルページを参照してください。

### 例

次のコマンドでは、CIFS サーバのデフォルトのユーザが設定されていないことがわかりますが、「pcuser」ユーザと「pcuser」グループは存在します。「pcuser」ユーザは、SVM vs1 上の CIFS サーバのデフォルトのユーザとして割り当てられています。

```
cluster1::> vserver cifs options show
```

```
Vserver: vs1
```

```
Client Session Timeout : 900
Default Unix Group      : -
Default Unix User       : -
Guest Unix User         : -
Read Grants Exec        : disabled
Read Only Delete        : disabled
WINS Servers            : -
```

```
cluster1::> vserver services unix-user show
```

Vserver	User Name	User ID	Group ID	Full Name
vs1	nobody	65535	65535	-
vs1	pcuser	65534	65534	-
vs1	root	0	1	-

```
cluster1::> vserver services unix-group show -members
```

Vserver	Name	ID
vs1	daemon	1
	Users: -	
vs1	nobody	65535
	Users: -	
vs1	pcuser	65534
	Users: -	
vs1	root	0
	Users: -	

```
cluster1::> vserver cifs options modify -vserver vs1 -default-unix-user
```



```
pcuser

cluster1:> vsriver cifs options show

Vserver: vs1

Client Session Timeout : 900
Default Unix Group      : -
Default Unix User       : pcuser
Guest Unix User         : -
Read Grants Exec        : disabled
Read Only Delete        : disabled
WINS Servers            : -
```

**SVM** のルートボリュームのセキュリティ形式が **NTFS** に設定されていることを確認します

Hyper-V および SQL Server over SMB のノンストップオペレーションを実行する場合は、ボリュームを NTFS セキュリティ形式で作成する必要があります。ルートボリュームのセキュリティ形式には、Storage Virtual Machine (SVM) で作成されたボリュームのデフォルトが適用されるため、ルートボリュームのセキュリティ形式は NTFS に設定する必要があります。

このタスクについて

- ルートボリュームのセキュリティ形式は SVM の作成時に指定できます。
- SVM の作成時にルートボリュームのセキュリティ形式を NTFS 以外に設定した場合は、を使用してあとからセキュリティ形式を変更できます `volume modify` コマンドを実行します

手順

1. SVM のルートボリュームの現在のセキュリティ形式を確認します。

```
volume show -vserver vsriver_name -fields vsriver,volume,security-style
```

2. ルートボリュームのセキュリティ形式が NTFS 以外になっている場合は、セキュリティ形式を NTFS に変更します。

```
volume modify -vserver vsriver_name -volume root_volume_name -security-style ntfs
```

3. SVM のルートボリュームのセキュリティ形式が NTFS に設定されていることを確認します。

```
volume show -vserver vsriver_name -fields vsriver,volume,security-style
```

例

次に、SVM vs1 のルートボリュームのセキュリティ形式が NTFS になっていることを確認するコマンドの例を示します。

```
cluster1::> volume show -vserver vs1 -fields vserver,volume,security-style
vserver  volume      security-style
-----  -
vs1      vs1_root     unix

cluster1::> volume modify -vserver vs1 -volume vs1_root -security-style
ntfs

cluster1::> volume show -vserver vs1 -fields vserver,volume,security-style
vserver  volume      security-style
-----  -
vs1      vs1_root     ntfs
```

必要な **CIFS** サーバオプションが設定されていることを確認する

Hyper-V および SQL Server over SMB のノンストップオペレーションを実行する場合、必要な CIFS サーバオプションが有効になっており、要件に従って適切に設定されていることを確認する必要があります。

このタスクについて

- SMB 2.x と SMB 3.0 が有効になっている必要があります。
- パフォーマンスが向上したコピーオフロードを使用するには、ODX コピーオフロードが有効になっている必要があります。
- Hyper-V over SMB 解決策でリモート VSS に対応したバックアップサービスを使用する場合は、VSS シャドウコピーサービスが有効になっている必要があります（Hyper-V のみ）。

手順

1. Storage Virtual Machine （SVM）で必要な CIFS サーバオプションが有効になっていることを確認します。

- a. 権限レベルを advanced に設定します。

```
set -privilege advanced
```

- b. 次のコマンドを入力します。

```
vserver cifs options show -vserver vserver_name
```

次のオプションはに設定する必要があります true：

- -smb2-enabled
- -smb3-enabled
- -copy-offload-enabled
- -shadowcopy-enabled（Hyper-Vのみ）

2. いずれかのオプションがに設定されていない場合 `true` 次の手順を実行します。

- a. に設定します `true` を使用します `vserver cifs options modify` コマンドを実行します
  - b. オプションがに設定されていることを確認します `true` を使用します `vserver cifs options show` コマンドを実行します
3. `admin` 権限レベルに戻ります。

```
set -privilege admin
```

#### 例

次に、SVM `vs1` について、Hyper-V over SMB 構成に必要なオプションが有効になっていることを確認するコマンドの例を示します。この例の要件では、ODX コピーオフロードのオプションを有効にする必要があります。

```
cluster1::> set -privilege advanced
Warning: These advanced commands are potentially dangerous; use them
only when directed to do so by technical support personnel.
Do you wish to continue? (y or n): y

cluster1::*> vserver cifs options show -vserver vs1 -fields smb2-
enabled,smb3-enabled,copy-offload-enabled,shadowcopy-enabled
vserver smb2-enabled smb3-enabled copy-offload-enabled shadowcopy-enabled
-----
vs1      true          true          false          true

cluster-1::*> vserver cifs options modify -vserver vs1 -copy-offload
-enabled true

cluster-1::*> vserver cifs options show -vserver vs1 -fields copy-offload-
enabled
vserver  copy-offload-enabled
-----
vs1      true

cluster1::*> set -privilege admin
```

パフォーマンスと冗長性を高めるために **SMB** マルチチャネルを設定します

ONTAP 9.4 以降では、SMB マルチチャネルを設定して、1 つの SMB セッションで ONTAP とクライアントの間に複数の接続を確立することができます。これにより、Hyper-V および SQL Server over SMB 構成のスループットとフォールトトレランスが向上します。

#### 必要なもの

SMB マルチチャネル機能は、クライアントが SMB 3.0 以降のバージョンでネゴシエートする場合にのみ使用できます。ONTAP SMB サーバでは、SMB 3.0 以降がデフォルトで有効になっています。

このタスクについて

SMB クライアントは、ONTAP クラスタで適切な設定が見つかり、複数のネットワーク接続を自動的に検出して使用します。

SMB セッションでの同時接続数は、導入している NIC によって異なります。

- \* クライアントおよび ONTAP クラスタに 1G NIC を搭載 \*

クライアントから確立される接続数は NIC ごとに 1 つで、すべての接続にセッションがバインドされません。

- \* クライアントおよび ONTAP クラスタ上の 10G 以上の NIC \*

クライアントから確立される接続数は NIC ごとに最大 4 つで、すべての接続にセッションがバインドされます。クライアントは 10G 以上の複数の NIC で接続を確立できます。

また、次のパラメータを変更することもできます（advanced 権限）。

- **-max-connections-per-session**

各マルチチャネルセッションに許可される最大接続数。デフォルトの接続数は 32 です。

デフォルトよりも多くの接続を有効にする場合は、クライアントの設定に対して同等の調整を行う必要があります。これには、デフォルトの接続数は 32 です。

- **-max-lifs-per-session**

各マルチチャネルセッションで通知されるネットワークインターフェイスの最大数。デフォルトのネットワークインターフェイス数は 256 です。

## 手順

1. 権限レベルを advanced に設定します。

```
set -privilege advanced
```

2. SMB サーバで SMB マルチチャネルを有効にします。

```
vserver cifs options modify -vserver vserver_name -is-multichannel-enabled true
```

3. ONTAP が SMB マルチチャネルセッションを報告していることを確認します。

```
vserver cifs session options show
```

4. admin 権限レベルに戻ります。

```
set -privilege admin
```

## 例

次の例は、すべての SMB セッションに関する情報を表示します。1 つのセッションに対して複数の接続が表示されています。

```
cluster1::> vserver cifs session show
Node:    node1
Vserver: vs1
Connection Session                                Open
Idle
IDs      ID      Workstation      Windows User      Files
Time
-----
-----
138683,
138684,
138685    1      10.1.1.1      DOMAIN\
4s                                     Administrator
0
```

次の例は、セッション ID 1 が割り当てられた SMB セッションに関する詳細情報を表示します。

```
cluster1::> vserver cifs session show -session-id 1 -instance

Vserver: vs1

Node: node1
Session ID: 1
Connection IDs: 138683,138684,138685
Connection Count: 3
Incoming Data LIF IP Address: 192.1.1.1
Workstation IP Address: 10.1.1.1
Authentication Mechanism: NTLMv1
User Authenticated as: domain-user
Windows User: DOMAIN\administrator
UNIX User: root
Open Shares: 2
Open Files: 5
Open Other: 0
Connected Time: 5s
Idle Time: 5s
Protocol Version: SMB3
Continuously Available: No
Is Session Signed: false
NetBIOS Name: -
```

## NTFS データボリュームを作成

Hyper-V over SMB または SQL Server over SMB アプリケーションサーバで使用する継続的可用性を備えた共有を設定する前に、Storage Virtual Machine (SVM) 上に


NTFS データボリュームを作成する必要があります。ボリューム構成ワークシートを使用して、データボリュームを作成します。

このタスクについて

データボリュームのカスタマイズに使用できるオプションのパラメータが用意されています。ボリュームのカスタマイズの詳細については、[xref:./smb-hyper-v-sql/"論理ストレージ管理"](#)を参照してください。

データボリュームの作成時に、次の項目を含むボリューム内にはジャンクションポイントを作成しないでください。

- ONTAP によってシャドウコピーが生成される Hyper-V ファイル
- SQL Server を使用してバックアップされる SQL Server データベースファイル



mixed セキュリティ形式または UNIX セキュリティ形式を使用するボリュームを誤って作成した場合、そのボリュームを NTFS セキュリティ形式のボリュームに変更して、ノンストップオペレーション用の継続的可用性を備えた共有の作成に直接使用することはできません。Hyper-V over SMB および SQL Server over SMB のノンストップオペレーションが正しく機能しないのは、この構成で使用するボリュームを NTFS セキュリティ形式のボリュームとして作成した場合だけです。ボリュームを削除し、NTFS セキュリティ形式でボリュームを再作成する必要があります。または、Windows ホストでボリュームをマッピングし、ボリュームの最上位に ACL を適用して、ボリューム内のすべてのファイルとフォルダに ACL を適用することもできます。

手順

1. 適切なコマンドを入力して、データボリュームを作成します。

ボリュームを作成する SVM のルートボリュームのセキュリティ形式	入力するコマンド
NTFS	<code>volume create -vserver vsERVER_name -volume volume_name -aggregate aggregate_name -size integer[KB MB GB TB PB] -junction-path path</code>
NTFS ではありません	<code>volume create -vserver vsERVER_name -volume volume_name -aggregate aggregate_name -size integer[KB MB GB TB PB] -security-style ntfs -junction-path path</code>

2. ボリュームの設定が正しいことを確認します。

```
volume show -vserver vsERVER_name -volume volume_name
```

継続的可用性を備えた **SMB** 共有を作成

データボリュームを作成したら、アプリケーションサーバが Hyper-V 仮想マシンおよび構成ファイルと SQL Server データベースファイルにアクセスするために使用する継続的可用性を備えた共有を作成できます。SMB 共有を作成する場合と同様に、共有設定ワ

ークシートを使用する必要があります。

#### 手順

1. 既存のデータボリュームとそのジャンクションパスに関する情報を表示します。

```
volume show -vserver vs1 -junction
```

2. 継続的可用性を備えた SMB 共有を作成します。

```
vserver cifs share create -vserver vs1 -share-name share_name -path  
path -share-properties oplocks,continuously-available -symlink "" [-comment  
text]
```

- 必要に応じて、コメントを共有設定に追加することもできます。
  - デフォルトでは、オフラインファイル共有プロパティは共有に設定され、に設定されます manual。
  - ONTAP によって、Windowsのデフォルトの共有権限で共有が作成されます Everyone / Full Control。
3. 共有設定ワークシートのすべての共有について同じ手順を繰り返します。
  4. を使用して、設定が正しいことを確認します vserver cifs share show コマンドを実行します
  5. 継続的な可用性が確保された共有に NTFS ファイル権限を設定するには、各共有にドライブをマッピングし、Windows のプロパティ \* ウィンドウを使用してファイル権限を設定します。

#### 例

次のコマンドを実行すると、Storage Virtual Machine（SVM、旧 Vserver）vs1 上に「data2」という名前の継続的可用性を備えた共有が作成されます。シンボリックリンクを無効にするには、を設定します -symlink パラメータの値 ""：

```
cluster1::> volume show -vserver vs1 -junction
```

Vserver	Volume	Active	Junction Path	Junction Path Source
vs1	data	true	/data	RW_volume
vs1	data1	true	/data/data1	RW_volume
vs1	data2	true	/data/data2	RW_volume
vs1	vs1_root	-	/	-

```
cluster1::> vsserver cifs share create -vserver vs1 -share-name data2 -path
/data/data2 -share-properties oplocks,continuously-available -symlink ""

cluster1::> vsserver cifs share show -vserver vs1 -share-name data2
```

```

Vserver: vs1
Share: data2
CIFS Server NetBIOS Name: VS1
Path: /data/data2
Share Properties: oplocks
                  continuously-available
Symlink Properties: -
File Mode Creation Mask: -
Directory Mode Creation Mask: -
Share Comment: -
Share ACL: Everyone / Full Control
File Attribute Cache Lifetime: -
Volume Name: -
Offline Files: manual
Vscan File-Operations Profile: standard

```

ユーザアカウント（**SMB 共有の SQL Server 用**）に **SeSecurityPrivilege** 権限を追加する

SQL Server のインストールに使用するドメインユーザアカウントには、デフォルトではドメインユーザに割り当てられていない権限を必要とする特定の操作を CIFS サーバで実行するために、「すべてのユーザ」権限を割り当てる必要があります。

必要なもの

SQL Server のインストールに使用するドメインアカウントがすでに存在している必要があります。

このタスクについて

SQL Server インストーラのアカウントに権限を追加するときに、ONTAP がドメインコントローラに照会してアカウントを検証することがあります。ONTAP からドメインコントローラに接続できない場合、コマンドが失敗することがあります。

手順



1. “s eepleed” 権限を追加します。

```
vserver cifs users-and-groups privilege add-privilege -vserver vserver_name  
-user-or-group-name account_name -privileges SeSecurityPrivilege
```

の値 `-user-or-group-name` パラメータは、SQL Serverのインストールに使用するドメインユーザアカウントの名前です。

2. 権限がアカウントに適用されていることを確認します。

```
vserver cifs users-and-groups privilege show -vserver vserver_name -user-or-  
group-name account_name
```

#### 例

次のコマンドでは、Storage Virtual Machine（SVM）vs1 のEXAMPLE ドメインにある SQL Server インストーラのアカウントに「s eepleed」権限を追加しています。

```
cluster1::> vserver cifs users-and-groups privilege add-privilege -vserver  
vs1 -user-or-group-name EXAMPLE\SQLInstaller -privileges  
SeSecurityPrivilege  
  
cluster1::> vserver cifs users-and-groups privilege show -vserver vs1  
Vserver      User or Group Name      Privileges  
-----  
vs1          EXAMPLE\SQLInstaller    SeSecurityPrivilege
```

### VSS シャドウコピーのディレクトリ階層を設定する（Hyper-V over SMB 共有の場合）

必要に応じて、シャドウコピーを作成する SMB 共有のディレクトリの最大階層を設定できます。このパラメータは、ONTAP によってシャドウコピーが作成されるサブディレクトリの最大レベルを手動で制御する場合に役立ちます。

#### 必要なもの

VSS シャドウコピー機能を有効にする必要があります。

#### このタスクについて

デフォルトでは、最大 5 つのサブディレクトリにシャドウコピーが作成されます。値がに設定されている場合 `0`ONTAP では、すべてのサブディレクトリに対してシャドウコピーが作成されます。



シャドウコピーセットのディレクトリ階層は 6 個以上のサブディレクトリまたはすべてのサブディレクトリを含むことができますが、シャドウコピーセットの作成は 60 秒以内に完了しなければならないという Microsoft の要件があります。この時間内に完了できない場合、シャドウコピーセットの作成は失敗します。作成時間が制限時間を超えないようにシャドウコピーのディレクトリ階層原因を設定しないでください。

#### 手順

1. 権限レベルを advanced に設定します。

```
set -privilege advanced
```

2. VSS シャドウコピーのディレクトリ階層を目的のレベルに設定します。

```
vserver cifs options modify -vserver vserver_name -shadowcopy-dir-depth  
integer
```

```
vserver cifs options modify -vserver vs1 -shadowcopy-dir-depth 6
```

3. admin 権限レベルに戻ります。

```
set -privilege admin
```

## Hyper-V および SQL Server over SMB 構成を管理します

既存の共有を継続的な可用性を確保するように設定し

既存の共有を変更して、継続的な可用性が確保された共有にすることができます。この共有は、Hyper-V および SQL Server アプリケーションサーバが Hyper-V 仮想マシンおよび構成ファイルや SQL Server データベースファイルに無停止でアクセスするために使用します。

このタスクについて

既存の共有に次のような特徴がある場合、SMB を介したアプリケーションサーバでその共有をノンストップオペレーション用の継続的可用性を備えた共有として使用することはできません。

- 状況に応じて homedirectory この共有に共有プロパティが設定されます
- 共有に有効なシンボリックリンクまたはワイドリンクが含まれている場合
- 共有のルート配下にジャンクションボリュームが含まれている場合

次の 2 つの共有パラメータが正しく設定されていることを確認する必要があります。

- `-offline-files` パラメータは Either に設定されます `manual` (デフォルト) または `none`。
- シンボリックリンクは無効にする必要があります。

次の共有プロパティを設定する必要があります。

- `continuously-available`
- `oplocks`

次の共有プロパティは設定しないでください。現在の共有プロパティのリストに含まれている場合は、継続的可用性を備えた共有から削除する必要があります。

- `attributecache`
- `branchcache`

手順

1. 現在の共有パラメータの設定と、設定済みの共有プロパティの現在のリストを表示します。

```
vserver cifs share show -vserver vserver_name -share-name share_name
```

2. 必要に応じて、を使用して共有パラメータを変更してシンボリックリンクを無効にし、オフラインファイルをmanualに設定します vserver cifs share properties modify コマンドを実行します

シンボリックリンクを無効にするには、の値を設定します -symlink パラメータの値 ""。

- シンボリックリンクを無効にするには、の値を設定します -symlink パラメータの値 ""。

- を設定できます -offline-files を指定して正しい設定に変更します manual。

3. を追加します continuously-available 共有プロパティ、および必要に応じてを共有します oplocks 共有プロパティ：

```
vserver cifs share properties add -vserver vserver_name -share-name share_name  
-share-properties continuously-available[,oplock]
```

状況に応じて oplocks 共有プロパティがまだ設定されていないため、と一緒に追加する必要があります continuously-available 共有プロパティ。

4. 継続的な可用性が確保された共有でサポートされていない共有プロパティを削除します。

```
vserver cifs share properties remove -vserver vserver_name -share-name  
share_name -share-properties properties[,...]
```

共有プロパティをカンマで区切って指定して、1 つ以上の共有プロパティを削除することができます。

5. を確認します -symlink および -offline-files パラメータが正しく設定されている。

```
vserver cifs share show -vserver vserver_name -share-name share_name -fields  
symlink-properties,offline-files
```

6. 設定済みの共有プロパティのリストが正しいことを確認します。

```
vserver cifs shares properties show -vserver vserver_name -share-name  
share_name
```

## 例

次の例は、Storage Virtual Machine (SVM) vs1 上の「share1」という名前の既存の共有を SMB を介したアプリケーションサーバでの NDO 用に設定する方法を示しています。

- を設定すると、共有でシンボリックリンクが無効になります -symlink パラメータを""に設定します。
- ◦ -offline-file パラメータが変更され、に設定されます manual。
- ◦ continuously-available 共有プロパティが共有に追加されます。
- ◦ oplocks 共有プロパティはすでに共有プロパティのリストに含まれているため、追加する必要はありません。
- ◦ attributecache 共有プロパティが共有から削除されます。

- 。 browsable 共有プロパティは、SMBを介したアプリケーションサーバでのNDOに使用される継続的可用性を備えた共有では省略可能で、共有プロパティの1つとして保持されます。

```
cluster1:> vsserver cifs share show -vsserver vs1 -share-name share1
```

```

        Vserver: vs1
        Share: share1
    CIFS Server NetBIOS Name: vs1
        Path: /data
    Share Properties: oplocks
                    browsable
                    attributecache
    Symlink Properties: enable
    File Mode Creation Mask: -
    Directory Mode Creation Mask: -
        Share Comment: -
        Share ACL: Everyone / Full Control
File Attribute Cache Lifetime: 10s
        Volume Name: data
        Offline Files: documents
Vscan File-Operations Profile: standard
```

```
cluster1:> vsserver cifs share modify -vsserver vs1 -share-name share1
-offline-file manual -symlink ""
```

```
cluster1:> vsserver cifs share properties add -vsserver vs1 -share-name
share1 -share-properties continuously-available
```

```
cluster1:> vsserver cifs share properties remove -vsserver vs1 -share-name
share1 -share-properties attributecache
```

```
cluster1:> vsserver cifs share show -vsserver vs1 -share-name share1
-fields symlink-properties,offline-files
vsserver  share-name symlink-properties offline-files
```

```
-----
vs1      share1      -                      manual
```

```
cluster1:> vsserver cifs share properties show -vsserver vs1 -share-name
share1
```

```

        Vserver: vs1
        Share: share1
    Share Properties: oplocks
                    browsable
                    continuously-available
```

**Hyper-V over SMB バックアップで VSS シャドウコピーを有効または無効にします**

VSS 対応バックアップアプリケーションを使用して、SMB 共有に格納された Hyper-V 仮想マシンファイルをバックアップする場合は、VSS シャドウコピーを有効にする必要があります。VSS 対応バックアップアプリケーションを使用しない場合は、VSS シャドウコピーを無効にできます。デフォルトでは、VSS シャドウコピーは有効になっています。

このタスクについて

VSS シャドウコピーはいつでも有効または無効にできます。

手順

- 1. 権限レベルを advanced に設定します。

```
set -privilege advanced
```

- 2. 次のいずれかを実行します。

VSS シャドウコピーの設定	入力するコマンド
有効	<code>vserver cifs options modify -vserver vserver_name -shadowcopy-enabled true</code>
無効	<code>vserver cifs options modify -vserver vserver_name -shadowcopy-enabled false</code>

- 3. admin 権限レベルに戻ります。

```
set -privilege admin
```

例

次のコマンドを実行すると、SVM vs1 で VSS シャドウコピーが有効になります。

```
cluster1::> set -privilege advanced
Warning: These advanced commands are potentially dangerous; use them
only when directed to do so by technical support personnel.
Do you wish to continue? (y or n): y

cluster1::*> vserver cifs options modify -vserver vs1 -shadowcopy-enabled
true

cluster1::*> set -privilege admin
```

統計を使用して、 **Hyper-V** および **SQL Server over SMB** のアクティビティを監視します

使用可能な統計オブジェクトと統計カウンタを確認します

CIFS、SMB、監査、および BranchCache ハッシュの統計に関する情報を取得してパフォーマンスを監視する前に、データの取得に使用できるオブジェクトとカウンタを確認しておく必要があります。

手順

- 1. 権限レベルを advanced に設定します。

```
set -privilege advanced
```

- 2. 次のいずれかを実行します。

確認する項目	入力するコマンド
使用可能なオブジェクト	<code>statistics catalog object show</code>
使用可能な特定のオブジェクト	<code>statistics catalog object show object <i>object_name</i></code>
使用可能なカウンタ	<code>statistics catalog counter show object <i>object_name</i></code>

使用可能なオブジェクトとカウンタの詳細については、マニュアルページを参照してください。

- 3. admin 権限レベルに戻ります。

```
set -privilege admin
```

例

次のコマンドを実行すると、advanced 権限レベルで表示したときの、クラスタ内の CIFS および SMB アクセスに関連する特定の統計オブジェクトの説明が表示されます。

```
cluster1::> set -privilege advanced
```

Warning: These advanced commands are potentially dangerous; use them only when directed to do so by support personnel.

Do you want to continue? {y|n}: y

```
cluster1::*> statistics catalog object show -object audit
      audit_ng          CM object for exporting audit_ng
performance counters
```

```
cluster1::*> statistics catalog object show -object cifs
      cifs              The CIFS object reports activity of the
                        Common Internet File System protocol
                        ...
```

```
cluster1::*> statistics catalog object show -object nblade_cifs
      nblade_cifs       The Common Internet File System (CIFS)
                        protocol is an implementation of the
Server
                        ...
```

```
cluster1::*> statistics catalog object show -object smb1
      smb1              These counters report activity from the
SMB
                        revision of the protocol. For information
                        ...
```

```
cluster1::*> statistics catalog object show -object smb2
      smb2              These counters report activity from the
                        SMB2/SMB3 revision of the protocol. For
                        ...
```

```
cluster1::*> statistics catalog object show -object hashd
      hashd             The hashd object provides counters to
measure
                        the performance of the BranchCache hash
daemon.
```

```
cluster1::*> set -privilege admin
```

次のコマンドは、の一部のカウンタに関する情報を表示します `cifs advanced`権限レベルで表示されるオブジェクト。



この例では、で使用可能なカウンタの一部が表示されているわけではありません `cifs` オブジェクト。出力は切り捨てられます。

```
cluster1::> set -privilege advanced
```

Warning: These advanced commands are potentially dangerous; use them only when directed to do so by support personnel.

Do you want to continue? {y|n}: y

```
cluster1::*> statistics catalog counter show -object cifs
```

Object: cifs

Counter	Description
active_searches	Number of active searches over SMB and SMB2
auth_reject_too_many	Authentication refused after too many requests were made in rapid succession
avg_directory_depth	Average number of directories crossed by SMB and SMB2 path-based commands
...	...

```
cluster2::> statistics start -object client -sample-id
```

Object: client

Counter	Value
cifs_ops	0
cifs_read_ops	0
cifs_read_recv_ops	0
cifs_read_recv_size	0B
cifs_read_size	0B
cifs_write_ops	0
cifs_write_recv_ops	0
cifs_write_recv_size	0B
cifs_write_size	0B
instance_name	vserver_1:10.72.205.179
instance_uuid	2:10.72.205.179
local_ops	0
mount_ops	0

[...]

## SMB 統計を表示します

パフォーマンスの監視と問題の診断用に、さまざまな SMB 統計を表示することができ



ます。

#### 手順

1. 使用します `statistics start` およびオプションです `statistics stop` データサンプルを収集するコマンド。
2. 次のいずれかを実行します。

統計を表示する対象	入力するコマンド
SMB のすべてのバージョン	<code>statistics show -object cifs</code>
SMB 1.0	<code>statistics show -object smb1</code>
SMB 2.x と SMB 3.0	<code>statistics show -object smb2</code>
ノードのSMBサブシステム	<code>statistics show -object nblade_cifs</code>

の詳細については、を参照してください `statistics` コマンド：

- "statistics showの画面には次"
- "統計が開始されます"
- "統計が停止しました"

### 設定がノンストップオペレーションに対応していることを確認します

ヘルスマニタを使用して、ノンストップオペレーションのステータスが正常かどうかを確認します

ヘルスマニタを使用すると、クラスタ全体のシステムヘルスステータスに関する情報が得られます。ヘルスマニタは Hyper-V over SMB および SQL Server over SMB 構成を監視して、アプリケーションサーバの Nondisruptive Operation（NDO；ノンストップオペレーション）を実現します。ステータスがデグレードになっている場合は、考えられる原因や推奨されるリカバリアクションなど、問題の詳細を表示できます。

ヘルスマニタはいくつかあります。ONTAP では、システム全体の健全性と個々のヘルスマニタの健全性の両方が監視されます。ノード接続ヘルスマニタには、CIFS-NDO サブシステムが含まれています。モニタには一連のヘルスポリシーがあり、特定の物理的な条件によってシステムが停止する可能性がある場合にアラートをトリガーするポリシーと、システム停止が発生している場合にアラートが生成し、対処方法に関する情報を提供するポリシーがあります。SMB を介した NDO 構成では、アラートは次の 2 つの状態で生成されます。

アラート ID	重大度	条件
<b>HaNotReadyCifsNdo_Alert</b>	メジャー（Major）	ノード上のアグリゲート内のボリュームでホストされている 1 つ以上のファイルが、継続的可用性を備えた SMB 共有を介して開かれており、障害が発生した場合でも継続性が保証されるはずだが、パートナーとの HA 関係が設定されていないか正常でない。
<b>NoStandbyLifCifsNdo_Alert</b>	マイナー	Storage Virtual Machine（SVM）はノードから SMB を介してアクティブにデータを提供しており、SMB ファイルは継続的可用性を備えた共有を介して継続的に開かれているが、そのパートナーノードが SVM のアクティブなデータ LIF を公開していない。

システムヘルスの監視を使用して、ノンストップオペレーションのステータスを表示します

を使用できます `system health` クラスタのシステムヘルス全体および CIFS-NDO サブシステムのヘルスに関する情報の表示、アラートへの応答、以降のアラートの設定、ヘルスマニタの設定に関する情報の表示を行うコマンド。

#### 手順

1. 適切な操作を実行して、ヘルスステータスを監視します。

表示する項目	入力するコマンド
個々のヘルスマニタのステータス全体が反映された、システムのヘルスステータス	<b>system health status show</b>
CIFS-NDO サブシステムのヘルスステータスに関する情報	<b>system health subsystem show -subsystem CIFS-NDO -instance</b>

2. 適切な操作を実行して、CIFS-NDO アラートの監視がどのように設定されているかに関する情報を表示します。

表示する情報	入力するコマンド
監視対象のノード、初期化状態、ステータスなど、CIFS-NDO サブシステムのヘルスマニタの設定とステータス	<b>system health config show -subsystem CIFS-NDO</b>
ヘルスマニタで生成される可能性がある CIFS-NDO アラート	<b>system health alert definition show -subsystem CIFS-NDO</b>

表示する情報	入力するコマンド
アラートが発行されるタイミングを決定する、CIFS-NDO ヘルスモニタのポリシー	<b>system health policy definition show -monitor node-connect</b>



を使用します `-instance` 詳細情報を表示するためのパラメータ。

#### 例

次の出力は、クラスタおよび CIFS-NDO サブシステムのヘルスステータス全体に関する情報を示しています。

```
cluster1::> system health status show
Status
-----
ok

cluster1::> system health subsystem show -instance -subsystem CIFS-NDO

                Subsystem: CIFS-NDO
                  Health: ok
      Initialization State: initialized
Number of Outstanding Alerts: 0
  Number of Suppressed Alerts: 0
                        Node: node2
  Subsystem Refresh Interval: 5m
```

次の出力は、CIFS-NDO サブシステムのヘルスモニタの設定とステータスに関する詳細な情報を示しています。

```

cluster1::> system health config show -subsystem CIFS-NDO -instance

Node: node1
Monitor: node-connect
Subsystem: SAS-connect, HA-health, CIFS-NDO
Health: ok
Monitor Version: 2.0
Policy File Version: 1.0
Context: node_context
Aggregator: system-connect
Resource: SasAdapter, SasDisk, SasShelf,
HaNodePair,
HaICMailbox, CifsNdoNode,
CifsNdoNodeVserver
Subsystem Initialization Status: initialized
Subordinate Policy Versions: 1.0 SAS, 1.0 SAS multiple adapters, 1.0,
1.0

Node: node2
Monitor: node-connect
Subsystem: SAS-connect, HA-health, CIFS-NDO
Health: ok
Monitor Version: 2.0
Policy File Version: 1.0
Context: node_context
Aggregator: system-connect
Resource: SasAdapter, SasDisk, SasShelf,
HaNodePair,
HaICMailbox, CifsNdoNode,
CifsNdoNodeVserver
Subsystem Initialization Status: initialized
Subordinate Policy Versions: 1.0 SAS, 1.0 SAS multiple adapters, 1.0,
1.0

```

継続的可用性を備えた **SMB** 共有の設定を確認します

ノンストップオペレーションをサポートするには、Hyper-V および SQL Server の SMB 共有が継続的可用性を備えた共有として設定されている必要があります。また、それ以外にも、いくつかの共有設定について確認が必要になります。計画的または計画外の停止が発生する状況でアプリケーションサーバのノンストップオペレーションをシームレスに実行できるように、共有が適切に設定されていることを確認してください。

このタスクについて

次の 2 つの共有パラメータが正しく設定されていることを確認する必要があります。

- 。 -offline-files パラメータはEitherに設定されます manual （デフォルト） または none。
- シンボリックリンクは無効にする必要があります。

ノンストップオペレーションが適切に実行されるようにするには、次の共有プロパティを設定する必要があります。

- continuously-available
- oplocks

次の共有プロパティは設定しないでください。

- homedirectory
- attributecache
- branchcache
- access-based-enumeration

#### 手順

1. オフラインファイルがに設定されていることを確認します manual または disabled シンボリックリンクが無効になっています。

```
vserver cifs shares show -vserver vserver_name
```

2. SMB 共有が継続的可用性を確保するように設定されていることを確認します。

```
vserver cifs shares properties show -vserver vserver_name
```

#### 例

次の例は、Storage Virtual Machine （SVM、旧 Vserver） vs1 上の「share1」という名前の共有の共有設定を表示します。オフラインファイルはに設定されます manual シンボリックリンクは無効になっています（でハイフンで指定） Symlink Properties フィールド出力）：

```
cluster1::> vsriver cifs share show -vsriver vs1 -share-name share1
      Vserver: vs1
      Share: share1
      CIFS Server NetBIOS Name: VS1
      Path: /data/share1
      Share Properties: oplocks
                      continuously-available
      Symlink Properties: -
      File Mode Creation Mask: -
      Directory Mode Creation Mask: -
      Share Comment: -
      Share ACL: Everyone / Full Control
      File Attribute Cache Lifetime: -
      Volume Name: -
      Offline Files: manual
      Vscan File-Operations Profile: standard
```

次の例は、SVM vs1 上の「share1」という名前の共有の共有プロパティを表示します。

```
cluster1::> vsriver cifs share properties show -vsriver vs1 -share-name
share1
Vserver      Share      Properties
-----
vs1          share1    oplocks
                      continuously-available
```

## LIF のステータスを確認

Hyper-V および SQL Server over SMB 構成の Storage Virtual Machine（SVM）がクラスタ内の各ノードに LIF を配置するように設定しても、日々の業務を行っているうちに、一部の LIF が他のノードのポートに移動してしまうことがあります。LIF のステータスを確認して、必要な措置を講じる必要があります。

### このタスクについて

シームレスなノンストップオペレーションの運用支援を提供するには、クラスタ内の各ノードの SVM に少なくとも 1 つの LIF を配置し、すべての LIF をホームポートに関連付ける必要があります。設定されている LIF の中に現在ホームポートに関連付けられていないものがある場合は、ポートの問題を修正してから、対応するホームポートに LIF をリポートする必要があります。

### 手順

1. 設定されている SVM の LIF に関する情報を表示します。

```
network interface show -vsriver vsriver_name
```

この例では、「lif1」はホームポートに配置されていません。

```
network interface show -vserver vs1
```

Vserver	Logical Interface	Status Admin/Oper	Network Address/Mask	Current Node	Current Is Port
Home					
-----	-----	-----	-----	-----	-----
vs1	lif1	up/up	10.0.0.128/24	node2	e0d
false	lif2	up/up	10.0.0.129/24	node2	e0d
true					

2. 対応するホームポートに関連付けられていない LIF がある場合は、次の手順を実行します。

a. それぞれの LIF について、LIF のホームポートを確認します。

```
network interface show -vserver vs1 -lif lif1 -fields home-node,home-port
```

```
network interface show -vserver vs1 -lif lif1 -fields home-node,home-port
```

vserver	lif	home-node	home-port
-----	----	-----	-----
vs1	lif1	node1	e0d

b. それぞれの LIF について、LIF のホームポートが up 状態になっているかどうかを確認します。

```
network port show -node node1 -port e0d -fields port,link
```

```
network port show -node node1 -port e0d -fields port,link
```

node	port	link
-----	----	----
node1	e0d	up

+  
この例では、「lif1」をホームポートに戻す必要があります。node1:e0d。

3. LIFを関連付けるホームポートのネットワークインターフェイスがない場合 up 状態にして、問題を解決して、これらのインターフェイスがアップ状態になるようにします。

4. 必要に応じて、ホームポートに LIF をリバートします。

```
network interface revert -vserver vs1 -lif lif1
```

```
network interface revert -vserver vs1 -lif lif1
```

5. クラスタ内の各ノードにアクティブな SVM の LIF があることを確認します。

```
network interface show -vserver vs1
```

```
network interface show -vserver vs1
```

Vserver	Logical Interface	Status Admin/Oper	Network Address/Mask	Current Node	Current Port	Is
Home						
vs1	lif1	up/up	10.0.0.128/24	node1	e0d	
true	lif2	up/up	10.0.0.129/24	node2	e0d	
true						

**SMB** セッションの継続的可用性を確認します

**SMB** セッション情報を表示します

SMB 接続、SMB セッション ID、セッションを使用しているワークステーションの IP アドレスなど、確立された SMB セッションに関する情報を表示できます。セッションの SMB プロトコルバージョンや継続的可用性を備えた保護のレベルに関する情報を表示できます。この情報は、セッションでノンストップオペレーションがサポートされているかどうか確認するのに役立ちます。

このタスクについて

SVM 上のすべてのセッションに関する情報を要約形式で表示できます。ただし、多くの場合、大量の出力が返されます。オプションのパラメータを指定すると、出力に表示される情報をカスタマイズできます。

- オプションのを使用できます `-fields` 選択したフィールドに関する出力を表示するためのパラメータ。

入ることができます `-fields` ? 使用できるフィールドを決定します。

- を使用できます `-instance` 確立されたSMBセッションに関する詳細情報を表示するためのパラメータ。
- を使用できます `-fields` パラメータまたは `-instance` パラメータのみ、または他のオプションパラメータと組み合わせて指定します。


手順

1. 次のいずれかを実行します。



表示する <b>SMB</b> セッション情報	入力するコマンド
SVM 上のすべてのセッションを要約形式で表示します	<b>vserver cifs session show -vserver vserver_name</b>
指定した接続 ID のセッション	<b>vserver cifs session show -vserver vserver_name -connection-id integer</b>
指定したワークステーションの IP アドレスからのセッションです	<b>vserver cifs session show -vserver vserver_name -address workstation_IP_address</b>
指定した LIF IP アドレスのセッションを表示します	<b>vserver cifs session show -vserver vserver_name -lif -address LIF_IP_address</b>
指定したノード上のセッションを表示します	<b>*vserver cifs session show -vserver vserver_name -node {node_name</b>
local}*`	指定した Windows ユーザからのセッションです
<b>vserver cifs session show -vserver vserver_name -windows-user user_name</b>  の形式 user_name はです [domain]\user。	を指定します

表示する <b>SMB</b> セッション情報	入力するコマンド
<b>vserver cifs session show -vserver vserver_name -auth -mechanism authentication_mec hanism</b>  の値 -auth -mechanism 次のい ずれかです。  • NTLMv1  • NTLMv2  • Kerberos  • Anonymous	指定したプロトコルバージョンを使用しているセッションです

表示する <b>SMB</b> セッション情報	入力するコマンド
<div data-bbox="180 195 469 401"> <pre> <b>vserver cifs</b> <b>session show</b> <b>-vserver</b> <b>vserver_name</b> <b>-protocol-version</b> <b>protocol_version</b> </pre> </div> <div data-bbox="180 441 493 541"> <p>の値 <code>-protocol</code> <code>-version</code> 次のいずれか です。</p> </div> <div data-bbox="207 581 329 835"> <ul style="list-style-type: none"> <li>• SMB1</li> <li>• SMB2</li> <li>• SMB2_1</li> <li>• SMB3</li> <li>• SMB3_1</li> </ul> </div> <div data-bbox="261 1451 315 1507">  </div> <div data-bbox="378 884 464 2074"> <p>継続的 可用性 を備え た保護 と SMB マルチ チャネ ルは、 SMB 3.0 以 降のセ ッションでの み利用 できま す。該 当する すべてのセッ ションのステ ータス を表示 するに は、こ のパラ メータ の値を に設定 します SMB3 以降が 必要で す。</p> </div>	<div data-bbox="511 195 1403 222"> <p>指定したレベルの継続的可用性を備えた保護を使用しているセッション</p> </div>

表示する <b>SMB</b> セッション情報	入力するコマンド
<pre> <b>vserver cifs</b> <b>session show</b> <b>-vserver</b> <b>vserver_name</b> <b>-continuously</b> <b>-available</b> <b>continuously_avail</b> <b>able_protection_le</b> <b>vel</b> </pre> <p>           の値 -continuously            -available 次のいず            れかです。         </p> <ul style="list-style-type: none"> <li>• No</li> <li>• Yes</li> <li>• Partial</li> </ul>	<p>指定した SMB 署名セッションステータスのセッション</p>

例

次のコマンドを実行すると、IP アドレスが 10.1.1.1 のワークステーションから確立された SVM vs1 上のセッションに関するセッション情報が表示されます。

継続的  
可用性

```
cluster1::> vserver cifs session show -address 10.1.1.1
Node:      node1
Vserver:   vs1
Connection Session
ID          ID          Workstation      Windows User      Open      Idle
-----
3151272279,
3151272280,
3151272281  1          10.1.1.1        DOMAIN\joe        2         23s
```

次のコマンドを実行すると、SVM vs1 上の継続的可用性を備えた保護を使用するセッションに関する詳細なセッション情報が表示されます。この接続はドメインアカウントを使用して確立されています。

含まれて  
います  
が、継続  
的可用性

```
cluster1::> vserver cifs session show -instance -continuously-available
Yes

Node: node1
Vserver: vs1
Session ID: 1
Connection ID: 3151274158
Incoming Data LIF IP Address: 10.2.1.1
Workstation IP address: 10.1.1.2
Authentication Mechanism: Kerberos
Windows User: DOMAIN\SERVER1$
UNIX User: pcuser
Open Shares: 1
Open Files: 1
Open Other: 0
Connected Time: 10m 43s
Idle Time: 1m 19s
Protocol Version: SMB3
Continuously Available: Yes
Is Session Signed: false
User Authenticated as: domain-user
NetBIOS Name: -
SMB Encryption Status: Unencrypted
```

ないかを

次のコマンドは、SVM vs1 上の SMB 3.0 と SMB マルチチャネルを使用しているセッションに関する情報を表示します。この例では、ユーザは LIF IP アドレスを使用して SMB 3.0 対応のクライアントからこの共有に接続しています。そのため、認証メカニズムはデフォルトの NTLMv2 になっています。継続的可用性を備えた保護を使用して接続するためには、Kerberos 認証を使用して接続を確立する必要があります。

```
cluster1::> vserver cifs session show -instance -protocol-version SMB3
```

```
Node: node1
Vserver: vs1
Session ID: 1
**Connection IDs: 3151272607,31512726078,3151272609
Connection Count: 3**
Incoming Data LIF IP Address: 10.2.1.2
Workstation IP address: 10.1.1.3
Authentication Mechanism: NTLMv2
Windows User: DOMAIN\administrator
UNIX User: pcuser
Open Shares: 1
Open Files: 0
Open Other: 0
Connected Time: 6m 22s
Idle Time: 5m 42s
Protocol Version: SMB3
Continuously Available: No
Is Session Signed: false
User Authenticated as: domain-user
NetBIOS Name: -
SMB Encryption Status: Unencrypted
```

開いている **SMB** ファイルに関する情報を表示します

SMB 接続、SMB セッション ID、ホスティングボリューム、共有名、共有パスなど、開いている SMB ファイルに関する情報を表示できます。ファイルの継続的可用性を備えた保護のレベルに関する情報も表示できます。この情報は、開いているファイルがノンストップオペレーションをサポートする状態であるかどうか確認するのに役立ちます。

このタスクについて

確立された SMB セッションで開いているファイルに関する情報を表示できます。これは、SMB セッション内の特定のファイルに関する SMB セッション情報を確認する必要がある場合に役立ちます。

たとえば、SMBセッションで、開いているファイルの一部が継続的可用性を備えた保護を使用して開いている場合と、残りのファイルが継続的可用性を備えた保護を使用して開かれていない場合（の値 `-continuously-available` フィールドに入力します `vserver cifs session show` コマンド出力はです `Partial`）の場合は、このコマンドを使用して、継続的可用性に対応していないファイルを確認できます。

を使用して、Storage Virtual Machine (SVM) 上の確立されたSMBセッションのすべての開いているファイルに関する情報を要約形式で表示できます `vserver cifs session file show` オプションのパラメータを指定しないコマンド。

ただし、多くの場合、大量の出力が返されます。オプションのパラメータを指定すると、出力に表示される情

報をカスタマイズできます。これは、開いているファイルの一部のみに関する情報を表示する場合に便利です。

- オプションのを使用できます `-fields` 選択したフィールドの出力を表示するためのパラメータ。

このパラメータは、単独で使用することも、他のオプションのパラメータと組み合わせて使用することもできます。


- を使用できます `-instance` 開いているSMBファイルに関する詳細情報を表示するためのパラメータ。

このパラメータは、単独で使用することも、他のオプションのパラメータと組み合わせて使用することもできます。

## 手順

1. 次のいずれかを実行します。

表示する開いている <b>SMB</b> ファイル	入力するコマンド
をクリックします	<b><code>vserver cifs session file show -vserver vserver_name</code></b>
指定したノード上のセッションを表示します	<code>*vserver cifs session file show -vserver vserver_name -node {node_name</code>
<code>local}*</code>	指定したファイル ID のファイル
<b><code>vserver cifs session file show -vserver vserver_name -file-id integer</code></b>	指定した SMB 接続 ID のファイル
<b><code>vserver cifs session file show -vserver vserver_name -connection-id integer</code></b>	指定した SMB セッション ID のファイル
<b><code>vserver cifs session file show -vserver vserver_name -session-id integer</code></b>	指定したホスティングアグリゲートのファイル
<b><code>vserver cifs session file show -vserver vserver_name -hosting -aggregate aggregate_name</code></b>	指定したボリュームのファイルです
<b><code>vserver cifs session file show -vserver vserver_name -hosting-volume volume_name</code></b>	指定した SMB 共有のファイル
<b><code>vserver cifs session file show -vserver vserver_name -share share_name</code></b>	指定した SMB パスのオブジェクト

表示する開いている <b>SMB</b> ファイル	入力するコマンド
<b>vserver cifs session file show</b> <b>-vserver vserver_name -path path</b>	指定したレベルの継続的可用性を備えた保護を使用しているファイル
<b>vserver cifs session file show</b> <b>-vserver vserver_name -continuously</b> <b>-available</b> <b>continuously_available_status</b>  の値 -continuously-available 次のいずれかです。 <ul style="list-style-type: none"> <li>• No</li> <li>• Yes</li> </ul> <div>  <p>継続的可用性のステータスの場合 `No` つまり、これらの開いているファイルは、テイクオーバーやギブバックからの無停止でのリカバリには対応していません。また、可用性の高い関係にあるパートナー間での一般的なアグリゲートの再配置からリカバリすることもできません。</p> </div>	指定した再接続の状態のファイル

ほかにも、出力結果の絞り込みに使用できるオプションのパラメータがあります。詳細については、のマニュアルページを参照してください。

例

次の例は、SVM vs1 の開いているファイルに関する情報を表示します。

```
cluster1::> vserver cifs session file show -vserver vs1
Node:      node1
Vserver:   vs1
Connection: 3151274158
Session:    1
File      File      Open Hosting      Continuously
ID        Type        Mode Volume      Share      Available
-----
41        Regular    r      data      data      Yes
Path: \mytest.rtf
```

次の例は、SVM vs1 のファイル ID 82 の開いている SMB ファイルに関する詳細情報を表示します。



```
cluster1::> vserver cifs session file show -vserver vs1 -file-id 82  
-instance
```

```
      Node: node1  
      Vserver: vs1  
      File ID: 82  
      Connection ID: 104617  
      Session ID: 1  
      File Type: Regular  
      Open Mode: rw  
Aggregate Hosting File: aggr1  
  Volume Hosting File: data1  
      CIFS Share: data1  
Path from CIFS Share: windows\win8\test\test.txt  
      Share Mode: rw  
      Range Locks: 1  
Continuously Available: Yes  
      Reconnected: No
```

# SANストレージ管理

## SANの概念

### iSCSI を使用した SAN プロビジョニング

SAN 環境において、ストレージシステムはストレージターゲットデバイスを含むターゲットです。iSCSI および FC では、ストレージターゲットデバイスを LUN（論理ユニット）と呼びます。Non-Volatile Memory Express（NVMe）over Fibre Channel では、ストレージターゲットデバイスをネームスペースと呼びます。

iSCSI および FC の場合は LUN、NVMe の場合はネームスペースを作成することでストレージを構成します。これらの LUN またはネームスペースに、ホストから Internet Small Computer System Interface（iSCSI）または Fibre Channel（FC；ファイバチャネル）プロトコルネットワーク経由でアクセスします。

iSCSI ネットワークに接続するために、ホストでは標準のイーサネットネットワークアダプタ（NIC）、ソフトウェアイニシエータを搭載した TOE カード、CNA、または専用の iSCSI Host Bus Adapter（HBA；ホストバスアダプタ）を使用します。

FC ネットワークに接続する場合、ホストでは FC HBA または CNA が必要です。

サポートされる FC プロトコルは次のとおりです。

- FC
- FCoE
- NVMe

### iSCSI ターゲットノードのネットワーク接続と名前

iSCSI ターゲットノードは、いくつかの方法でネットワークに接続できます。

- ONTAP に統合されているソフトウェアを使用して、イーサネットインターフェイスを介して接続する。
- 複数のシステムインターフェイス上。iSCSI に使用されるインターフェイスで、SMB や NFS などの他のプロトコルのトラフィックも転送できます。
- ユニファイドターゲットアダプタ（UTA）または Converged Network Adapter（CNA；統合ネットワークアダプタ）を使用する。

すべての iSCSI ノードには、ノード名が必要です。

iSCSI ノード名の 2 つの形式、つまり、タイプ指定子は、\_iqn と \_eui\_ です。SVM iSCSI ターゲットでは、常に iqn タイプの指定子が使用されます。イニシエータでは、iqn タイプ指定子と eui タイプ指定子のどちらも使用できます。

### ストレージシステムのノード名

iSCSI を実行している各 SVM には、逆ドメイン名と一意のエンコード番号から成るデフォルトのノード名が付いています。

ノード名は次の形式で表示されます。

`iqn.1992-08.com.netapp:sn.unique-encoding-number`

次の例は、一意のエンコード番号を持つストレージシステムのデフォルトのノード名です。

```
iqn.1992-08.com.netapp:sn.812921059e6c11e097b3123478563412:vs.6
```

## iSCSI の TCP ポート

iSCSI プロトコルは、TCP ポート番号 3260 を使用するように、ONTAP で設定されています。

ONTAP では、iSCSI のポート番号の変更がサポートされていません。ポート番号 3260 は iSCSI 仕様の一部として登録されており、他のアプリケーションやサービスでは使用できません。

### 関連情報

["ネットアップのマニュアル：ONTAP SAN ホスト構成"](#)

## iSCSI サービスの管理

### iSCSI サービスの管理

Storage Virtual Machine (SVM) の iSCSI 論理インターフェイスで iSCSI サービスの可用性を管理するには、を使用します `vserver iscsi interface enable` または `vserver iscsi interface disable` コマンド

デフォルトでは、すべての iSCSI 論理インターフェイスで iSCSI サービスが有効になっています。

### ホストに iSCSI を実装する方法

iSCSI は、ハードウェアまたはソフトウェアを使用してホストに実装できます。

iSCSI は、次のいずれかの方法で実装できます。

- ホストの標準イーサネットインターフェイスを使用するイニシエータソフトウェアを使用する。
- iSCSI Host Bus Adapter (HBA ; ホストバスアダプタ) を使用する。ホストオペレーティングシステムでは、iSCSI HBA をローカルディスクを搭載した SCSI ディスクアダプタとみなします。
- TCP / IP 処理をオフロードする TCP Offload Engine (TOE ; TCP オフロードエンジン) アダプタを使用する。

iSCSI プロトコルの処理は、引き続きホストソフトウェアによって実行されます。

### iSCSI 認証の仕組み

iSCSI セッションの第 1 段階では、イニシエータがストレージシステムにログイン要求を送信して、iSCSI セッションを開始します。ストレージシステムは、このログイン要求を許可または拒否するか、またはログインが不要であると判断します。

iSCSI 認証方法は次のとおりです。

- Challenge Handshake Authentication Protocol (CHAP) - イニシエータは CHAP ユーザ名およびパスワードを使用してログインします。

CHAP パスワードを指定するか、16 進数のシークレットパスワードを生成できます。CHAP ユーザ名およびパスワードには、次の 2 種類があります。

- インバウンド - ストレージシステムがイニシエータを認証します。

CHAP 認証を使用する場合は、インバウンド設定が必要です。

- アウトバウンド - イニシエータがストレージシステムを認証できるようにするオプションの設定です。

インバウンドユーザ名およびパスワードをストレージシステムで定義した場合にのみ、アウトバウンド設定を使用できます。

- deny — イニシエータはストレージシステムへのアクセスを拒否されます。
- none — イニシエータの認証は必要ありません

イニシエータとその認証方法の一覧を定義できます。このリストにない環境イニシエータに対して、デフォルトの認証方法を定義することもできます。

#### 関連情報

["Data ONTAP での Windows マルチパス・オプション：ファイバ・チャネルおよび iSCSI"](#)

### iSCSI イニシエータのセキュリティ管理

ONTAP は、iSCSI イニシエータのセキュリティを管理するためのさまざまな機能を備えています。iSCSI イニシエータのリストと各イニシエータに対する認証方法の定義、認証リスト内のイニシエータと関連する認証方法の表示、認証リストに対するイニシエータの追加と削除、リストにないイニシエータに対するデフォルトの iSCSI イニシエータ認証方法の定義を行うことができます。

### iSCSI エンドポイントの分離

ONTAP 9.1 以降では、既存の iSCSI セキュリティコマンドが拡張され、IP アドレスの範囲や複数の IP アドレスを受け入れることができるようになりました。

すべての iSCSI イニシエータは、ターゲットとのセッションまたは接続を確立するときに、発信元 IP アドレスを提供する必要があります。元の IP アドレスがサポート対象外または不明な場合にイニシエータがクラスタにログインできないようにすることで、独自の識別を実現します。サポート対象外または不明な IP アドレスを発信したイニシエータは、iSCSI セッションレイヤでログインが拒否されるため、クラスタ内の LUN やボリュームにアクセスできません。

この新しい機能を 2 つの新しいコマンドで実装して、既存のエントリを管理します。

イニシエータのアドレス範囲を追加する

でIPアドレス範囲を追加するか、複数のIPアドレスを追加して、iSCSIイニシエータのセキュリティ管理を改善します `vserver iscsi security add-initiator-address-range` コマンドを実行します

```
cluster1::> vserver iscsi security add-initiator-address-range
```

イニシエータのアドレス範囲を削除する

を使用して、IPアドレス範囲または複数のIPアドレスを削除します `vserver iscsi security remove-initiator-address-range` コマンドを実行します

```
cluster1::> vserver iscsi security remove-initiator-address-range
```

## CHAP 認証とは

Challenge Handshake Authentication Protocol（CHAP）により、iSCSI イニシエータとターゲットの間で認証に基づいたやり取りが可能になります。CHAP 認証を使用する場合は、イニシエータとストレージシステムの両方で、CHAP ユーザ名およびパスワードを定義します。

iSCSI セッションの第 1 段階では、イニシエータがストレージシステムにログイン要求を送信して、セッションを開始します。ログイン要求には、イニシエータの CHAP ユーザ名および CHAP アルゴリズムが含まれています。ストレージシステムは CHAP チャレンジで応答します。イニシエータは CHAP 応答を返します。ストレージシステムは応答を検証し、イニシエータを認証します。CHAP パスワードは、応答の計算に使用されます。

### CHAP 認証を使用する場合のガイドライン

CHAP 認証を使用する場合は、一定のガイドラインに従う必要があります。

- インバウンドユーザ名およびパスワードをストレージシステムで定義している場合は、イニシエータのアウトバウンド CHAP 設定にも同じユーザ名およびパスワードを使用する必要があります。ストレージシステムでアウトバウンドユーザ名およびパスワードも定義して、双方向認証を可能にしている場合は、イニシエータのインバウンド CHAP 設定にも同じユーザ名およびパスワードを使用する必要があります。
- ストレージシステムのインバウンド設定とアウトバウンド設定には、同じユーザ名およびパスワードを使用できません。
- CHAP ユーザ名には 1~128 バイトを使用できます。

ユーザ名を null にすることはできません。

- CHAP パスワード（secrets）には 1~512 バイトを使用できます。

パスワードには、16 進数値または文字列を使用できます。16 進数値を使用する場合は、プレフィックス「0x」または「0X」を付けた値を入力する必要があります。パスワードを null にすることはできません。

ONTAP では、CHAPパスワード（シークレット）に特殊文字、英語以外の文字、数字、およびスペースを使用できます。ただし、これにはホストの制限があります。これらのいずれかが特定のホストで許可されていない場合は、使用できません。



たとえば、Microsoft iSCSI ソフトウェアイニシエータでは、IPSec 暗号化を使用しない場合、イニシエータとターゲットの両方の CHAP パスワードを 12 バイト以上に設定する必要があります。パスワードの最大長は、IPSec を使用するかどうかに関係なく 16 バイトです。

その他の制限事項については、イニシエータのマニュアルを参照してください。

イニシエータのインターフェイスを制限する **iSCSI** インターフェイスアクセスリストの使用方法によって、パフォーマンスとセキュリティが向上する可能性があります

iSCSI インターフェイスアクセスリストを使用して、イニシエータがアクセスできる SVM 内の LIF の数を制限できます。これにより、パフォーマンスとセキュリティが向上します。

イニシエータが iSCSI を使用して検出セッションを開始したとき `SendTargets` コマンドを実行すると、アクセスリストにある LIF（ネットワークインターフェイス）に関連付けられている IP アドレスが受信されます。デフォルトでは、すべてのイニシエータが SVM 内のすべての iSCSI LIF にアクセスできます。アクセスリストを使用すると、イニシエータがアクセスできる SVM 内の LIF の数を制限できます。

### Internet Storage Name Service (iSNS)

Internet Storage Name Service（iSNS）は、TCP/IP ストレージネットワークで iSCSI デバイスを自動的に検出して管理できるプロトコルです。iSNS サーバは、IP アドレス、iSCSI ノード名 IQN、ポータルグループなど、ネットワーク上のアクティブな iSCSI デバイスに関する情報を維持します。

iSNS サーバは、サードパーティベンダーから入手できます。ネットワーク内に iSNS サーバがあり、イニシエータとターゲットで使用するよう設定および有効化されている場合、Storage Virtual Machine（SVM）の管理 LIF を使用して、その SVM のすべての iSCSI LIF を iSNS サーバに登録できます。登録が完了すると、iSCSI イニシエータは iSNS サーバを照会して、その SVM のすべての LIF を検出できるようになります。

iSNS サービスを使用する場合は、Storage Virtual Machine（SVM）を Internet Storage Name Service（iSNS）サーバに適切に登録する必要があります。

iSNS サーバがネットワークにない場合は、各ターゲットがホストで認識できるように、ターゲットを手動で設定する必要があります。

#### iSNS サーバの機能

iSNS サーバは、Internet Storage Name Service（iSNS）プロトコルを使用して、IP アドレス、iSCSI ノード名（IQN）、ポータルグループなど、ネットワーク上のアクティブな iSCSI デバイスに関する情報を維持します。

iSNS プロトコルを使用すると、IP ストレージネットワークで iSCSI デバイスを自動的に検出して管理できます。iSCSI イニシエータは、iSNS サーバに照会して iSCSI ターゲットデバイスを検出します。

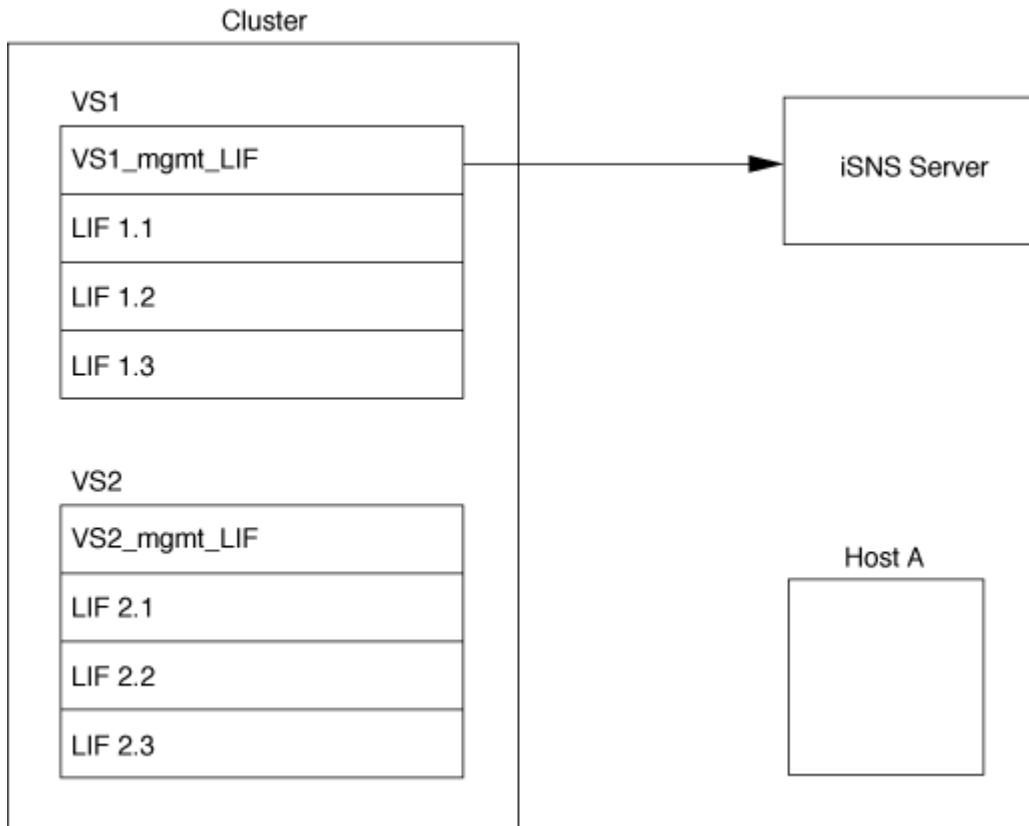
ネットアップでは、iSNS サーバの提供や再販は行っていません。これらのサーバは、ネットアップがサポー

トするベンダーから入手できます。

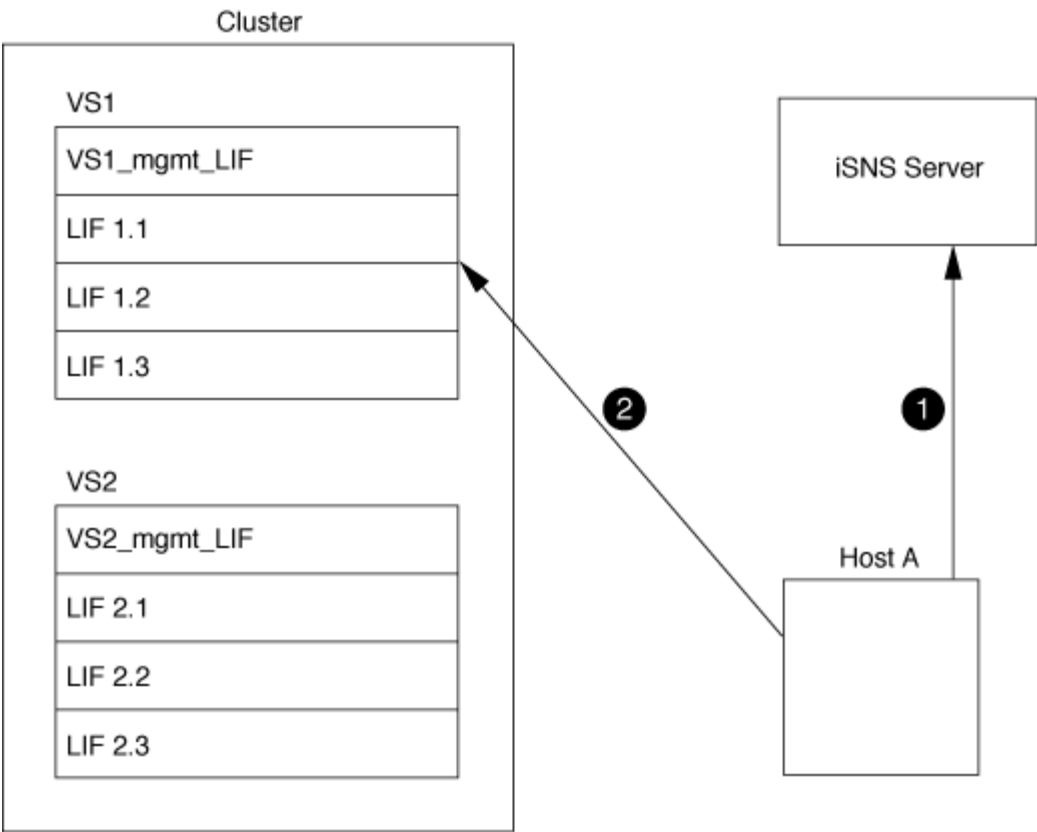
#### SVMs と iSNS サーバの連動

iSNS サーバは、Storage Virtual Machine（SVM）の管理 LIF を介して各 SVM と通信します。管理 LIF は、特定の SVM のすべての iSCSI ターゲットのノード名、エイリアス、およびポータル情報を iSNS サーバに登録します。

次の例では、SVM「VS1」はSVM管理LIF「VS1\_mgmt\_LIF」を使用してiSNSサーバに登録しています。iSNSに登録中、SVMはすべてのiSCSI LIFをSVM管理LIFを介してiSNSサーバに送信します。iSNSの登録が完了すると、iSNSサーバには「VS1」でiSCSIを提供するすべてのLIFのリストが格納されます。複数のSVMsがあるクラスタでは、iSNSサービスを使用する個々のSVMがiSNSサーバに登録する必要があります。



次の例では、iSNSサーバによるターゲットへの登録が完了すると、ホストAがiSNSサーバを介して「VS1」のすべてのLIFを検出できるようになります（手順1を参照）。ホストAが「VS1」のLIFの検出を完了すると、ホストAは「VS1」の任意のLIFとの接続を確立できます（手順2を参照）。「VS2」の管理LIF「VS2\_mgmt\_LIF」がiSNSサーバに登録されるまで、ホストAは「VS2」内のLIFを認識しません。



ただし、インターフェイスアクセスリストを定義すると、ホストがターゲットへのアクセスに使用できるのはインターフェイスアクセスリストに定義された LIF のみになります。

一度 iSNS が設定されると、SVM の設定を変更するたびに ONTAP によって iSNS サーバが自動的に更新されます。

設定を変更してから ONTAP から iSNS サーバに更新情報が送信されるまでには、数分程度の遅れが生じる可能性があります。iSNS サーバの iSNS 情報を強制的に更新します。 `vserver iscsi isns update`

**iSNS** を管理するためのコマンド

ONTAP には、iSNS サービスを管理するコマンドが用意されています。

状況	使用するコマンド
iSNS サービスを設定する	<code>vserver iscsi isns create</code>
iSNS サービスを開始する	<code>vserver iscsi isns start</code>
iSNS サービスを変更する	<code>vserver iscsi isns modify</code>
iSNS サービス設定を表示します	<code>vserver iscsi isns show</code>
登録済みの iSNS 情報を強制的に更新します	<code>vserver iscsi isns update</code>



iSNS サービスを停止します	<code>vserver iscsi isns stop</code>
iSNS サービスを削除します	<code>vserver iscsi isns delete</code>
コマンドのマニュアルページを表示します	<code>man command name</code>

詳細については、各コマンドのマニュアルページを参照してください。

## FC を使用した SAN プロビジョニング

ONTAP で FC SAN を実装する方法について理解する際に必要となる重要な概念について説明します。

### FC ターゲットノードをネットワークに接続する方法

ストレージシステムとホストはいずれもアダプタを備えており、ケーブルを使用して FC スイッチに接続できます。

ノードを FC SAN に接続すると、各 SVM の LIF の World Wide Port Name（WWPN；ワールドワイドポート名）がスイッチのファブリックネームサービスに登録されます。SVM の WWNN と各 LIF の WWPN は、ONTAP によって自動的に割り当てられます。



FC を使用してホストから直接ノードに接続することはできません。NPIV が必要なため、スイッチを使用する必要があります。iSCSI セッションでは、ネットワークルーティングされた接続または直接接続された接続で通信が可能です。ただし、どちらの方法も ONTAP でサポートされています。

### FC ノードの識別方法

FC を使用して設定された各 SVM は、World Wide Node Name（WWNN）で識別されます。

### WWPN の使用方法

WWPN により、FC をサポートするように設定されている SVM 内の各 LIF が識別されます。これらの LIF はクラスタ内の各ノードの物理 FC ポートを利用します。これらのポートには、FC ターゲットカード、UTA、または UTA2 としてノードの FC または FCoE として設定することができます。

- **igroup** を作成します

ホストの HBA の WWPN は、igroup の作成に使用します。igroup は、特定 LUN へのホストアクセスの制御に使用します。igroup を作成するには、FC ネットワーク内の一連のイニシエータの WWPN を指定します。ストレージシステム上の LUN を igroup にマッピングすると、グループ内のすべてのイニシエータに対し、その LUN へのアクセスを許可することができます。LUN にマッピングされている igroup に WWPN が含まれていないホストは、その LUN にアクセスできません。つまり、そのホストでは、LUN がディスクとして表示されません。

ポートセットを作成して、特定のターゲットポートでのみ LUN を表示することもできます。ポートセットは、FC ターゲットポートをグループ化したものです。ポートセットには igroup をバインドできます。この igroup 内のすべてのホストは、ポートセット内のターゲットポートからのみ各 LUN にアクセスでき

ます。

- FC LIF を一意に識別します

WWPN は、FC 論理インターフェイスを一意に識別します。ホストの OS は、WWNN と WWPN を組み合わせて使用して、SVM および FC LIF を識別します。一部のオペレーティングシステムでは、パーシスタントバインディングがないと、ホスト上の同じターゲット ID に LUN が表示されません。

## WWN の割り当ての仕組み

WWN は、ONTAP でシーケンシャルに作成されます。ただし、ONTAP による割り当て方法が原因で、WWN がシーケンシャルに割り当てられていないように見える場合があります。

各アダプタには WWPN および WWNN があらかじめ設定されていますが、ONTAP ではあらかじめ設定された値が使用されません。その代わりに、ONTAP はオンボードイーサネットポートの MAC アドレスに基づいて、固有の WWPN または WWNN を割り当てます。

WWN が割り当て時にシーケンシャルでないように見える理由は次のとおりです。

- WWN は、クラスタ内のすべてのノードと Storage Virtual Machine (SVM) で一意に割り当てられます。
- 解放された WWN はリサイクルされ、利用可能な名前のプールに再び追加されます。

## FC スイッチの識別方法

ファイバチャネルスイッチでは、デバイス自体に 1 つの Worldwide Node Name (WWNN ; ワールドワイドノード名) があり、デバイスの各ポートに 1 つの Worldwide Port Name (WWPN ; ワールドワイドポート名) があります。

たとえば、次の図は、16 ポート Brocade スイッチの各ポートに WWPN がどのように割り当てられているかを示しています。特定のスイッチのポートの番号付けについては、そのスイッチ用にベンダーが提供するマニュアルを参照してください。



ポート \* 0 \*, WWPN 20 : **00** : 00 : 60 : 69 : 51 : 06 : b4

ポート \* 1 \*, WWPN 20 : **01** : 00 : 60 : 69 : 51 : 06 : b4

ポート \* 14 \*, WWPN 20 : **0e** 00 : 60 : 69 : 51 : 06 : b4

ポート \* 15 \*, WWPN 20 : **0f** : 00 : 60 : 69 : 51 : 06 : B4

## NVMe を使用した SAN プロビジョニング

ONTAP 9.4 以降では、SAN 環境で NVMe/FC がサポートされます。NVMe/FC では、

FC および iSCSI で LUN をプロビジョニングして igroup にマッピングするのと同様に、ネームスペースとサブシステムをプロビジョニングし、ネームスペースをサブシステムにマッピングすることができます。

NVMe ネームスペースは、論理ブロックにフォーマット可能な不揮発性メモリの容量です。ネームスペースは FC および iSCSI プロトコルの LUN に相当し、NVMe サブシステムは igroup に相当します。NVMe サブシステムはイニシエータに関連付けることができ、これにより関連付けられたイニシエータからサブシステム内のネームスペースにアクセスできるようになります。



NVMe ネームスペースは、機能的には LUN に似ていますが、LUN でサポートされるすべての機能がサポートされるわけではありません。

ONTAP 9.5 以降では、NVMe を使用したホスト側のデータアクセスをサポートするにはライセンスが必要です。ONTAP 9.4 で NVMe が有効になっている場合、ONTAP 9.5 へのアップグレード後に 90 日間の猶予期間中にライセンスを取得する必要があります。ある場合 ["ONTAP One"](#)にはNVMeライセンスが含まれています。ライセンスを有効にするには、次のコマンドを使用します。

```
system license add -license-code NVMe_license_key
```

#### 関連情報

["ネットアップテクニカルレポート 4684 : 『Implementing and Configuring Modern SANs with NVMe/FC』"](#)

## SANホリユウム

### SAN ボリュームについての概要

ONTAP には、基本的なボリュームプロビジョニングオプションとして、シックプロビジョニング、シンプロビジョニング、セミシックプロビジョニングの 3 つが用意されています。各オプションでは、ボリュームスペースおよび ONTAP ブロック共有テクノロジーでのスペース要件がさまざまな方法で管理されます。これらのオプションの仕組みを理解することで、環境に最も適したオプションを選択できるようになります。



SAN LUN と NAS 共有を同じ FlexVol に配置することは推奨されません。SAN LUN と FlexVol NAS 共有それぞれに専用の FlexVol ボリュームをプロビジョニングしてください。これにより、管理とレプリケーションの導入が簡易化され、Active IQ Unified Manager (旧 OnCommand Unified Manager) での FlexVol ボリュームのサポート方法が統一されます。

#### ボリュームのシンプロビジョニング

シンプロビジョニングボリュームは、作成時に ONTAP によって追加のスペースが確保されることはありません。ボリュームにデータが書き込まれるときに、書き込み処理に対応するために必要なアグリゲート内のストレージをボリュームが要求します。シンプロビジョニングボリュームを使用する場合はアグリゲートをオーバーコミットできますが、アグリゲートの空きスペースが不足すると、必要なスペースをボリュームが確保できなくなる可能性があります。

シンプロビジョニング FlexVol を作成するには、そのボリュームを設定します `-space-guarantee` オプションをに設定します `none`。

## ボリュームのシックプロビジョニング

シックプロビジョニングボリュームを作成すると、ボリューム内のブロックにいつでも書き込むことができるように、ONTAP はアグリゲートから十分なストレージを確保します。シックプロビジョニングを使用するようにボリュームを構成する場合は、圧縮や重複排除などの ONTAP の Storage Efficiency 機能を使用して、事前に必要となる大容量のストレージをオフセットすることができます。

シックプロビジョニング FlexVol ボリュームを作成するには、そのボリュームを設定します `-space-slo`（サービスレベル目標）オプションをに設定します `thick`。

## ボリュームのセミシックプロビジョニング

セミシックプロビジョニングを利用するボリュームを作成すると、ONTAP はボリュームサイズに相当するストレージスペースをアグリゲートから確保します。ブロック共有テクノロジーでブロックが使用されているためにボリュームの空きスペースが不足しそうになると、ONTAP は保護データオブジェクト（Snapshot コピー、FlexClone ファイル、FlexClone LUN）を削除して、該当するオブジェクトが保持しているスペースを解放します。上書きに必要なスペースを確保できる速度で ONTAP が保護データオブジェクトを削除できるかぎり、書き込み処理は続行されます。これは「ベストエフォート」書き込み保証と呼ばれます。

- ・注：\* セミシックプロビジョニングを使用するボリュームでは、次の機能はサポートされていません。
- ・重複排除、圧縮、コンパクションなどの Storage Efficiency テクノロジー
- ・Microsoft オフロードデータ転送（ODX）

セミシックプロビジョニング FlexVol ボリュームを作成するには、そのボリュームを設定します `-space-slo`（サービスレベル目標）オプションをに設定します `semi-thick`。

スペースリザーブファイルおよびスペースリザーブ LUN で使用します

スペースリザーブファイルまたはスペースリザーブ LUN は、ストレージの作成時にそのストレージに割り当てられるものです。ネットアップではこれまで、スペース・リザーベーションが無効になっている LUN（スペース・リザーブなしの LUN）を「シン・プロビジョニング LUN」と呼んできました。

- ・注意：\* スペースリザーブなしのファイルは、一般的に「シンプロビジョニングされたファイル」とは呼ばれません。

次の表に、スペースリザーブファイルおよびスペースリザーブ LUN で使用できる 3 つのボリュームプロビジョニングオプションの主な違いを示します。

ボリュームのプロビジョニング	LUN/file のスペースリザーベーション	上書きします	保護データ <sup>2</sup>	ストレージ効率 <sup>3</sup>
厚み（Thick）	サポートされます	保証された <sup>1</sup>	保証	サポートされます
シン	効果はありません	なし	保証	サポートされます
セミシック	サポートされます	ベストエフォート <sup>1</sup> ^	ベストエフォート	サポート対象外

- ・メモ \*

1. 上書きの保証またはベストエフォートの上書き保証が行われるには、LUN またはファイルでスペースリザーベーションが有効になっている必要があります。
2. 保護データには、Snapshot コピーおよび自動削除の対象とマークされた FlexClone ファイルと FlexClone LUN（バックアップクローン）が含まれます。
3. Storage Efficiency には、重複排除、圧縮、自動削除の対象とマークされていない FlexClone ファイルと FlexClone LUN（アクティブクローン）、および FlexClone サブファイル（コピーオフロードに使用）が含まれます。

## SCSI シンプロビジョニング LUN のサポート

ONTAP は、T10 SCSI シンプロビジョニング LUN に加え、ネットアップのシンプロビジョニング LUN もサポートしています。T10 SCSI シンプロビジョニングを使用すると、ホストアプリケーションで、LUN のスペース再生やブロック環境の LUN スペース監視機能などの SCSI 機能をサポートできます。使用する SCSI ホストソフトウェアも、T10 SCSI シンプロビジョニングをサポートしている必要があります。

ONTAP を使用します space-allocation LUNでのT10シンプロビジョニングのサポートを有効または無効にするための設定。ONTAP を使用します space-allocation enable LUNでT10 SCSIシンプロビジョニングを有効にするための設定。

。 [-space-allocation {enabled|disabled}] ONTAP でT10シンプロビジョニングのサポートを有効または無効にする方法、およびT10 SCSIシンプロビジョニングを有効にする方法の詳細については、『Command Reference Manual』のコマンドを参照してください。

## "ONTAP 9 のコマンド"

### ボリュームのプロビジョニングオプションを設定

ボリュームにシンプロビジョニング、シックプロビジョニング、またはセミシックプロビジョニングを設定できます。

このタスクについて

を設定します -space-slo オプションをに設定します thick 次のことを確認します。

- ボリューム全体がアグリゲートに事前に割り当てられます。を使用することはできません volume create または volume modify ボリュームを設定するコマンド -space-guarantee オプション
- 上書きに必要なスペースの 100% がリザーブされます。を使用することはできません volume modify ボリュームを設定するコマンド -fractional-reserve オプション

を設定します -space-slo オプションをに設定します semi-thick 次のことを確認します。

- ボリューム全体がアグリゲートに事前に割り当てられます。を使用することはできません volume create または volume modify ボリュームを設定するコマンド -space-guarantee オプション
- スペースは上書き用にリザーブされません。を使用できます volume modify ボリュームを設定するコマンド -fractional-reserve オプション
- Snapshot コピーの自動削除が有効になります。

### ステップ

1. ボリュームのプロビジョニングオプションを設定します。

```
volume create -vsriver vsriver_name -volume volume_name -aggregate  
aggregate_name -space-slo none|thick|semi-thick -space-guarantee none|volume
```

。-space-guarantee オプションのデフォルトはです none（AFF システムの場合）およびAFF以外のDPボリュームの場合。それ以外の場合は、デフォルトでになります volume。既存のFlexVol ボリュームの場合は、を使用します volume modify プロビジョニングオプションを設定するコマンド。

次のコマンドを使うと、SVM vs1 上の vol1 にシンプロビジョニングが設定されます。

```
cluster1::> volume create -vsriver vs1 -volume vol1 -space-guarantee  
none
```

次のコマンドを使うと、SVM vs1 上の vol1 にシックプロビジョニングが設定されます。

```
cluster1::> volume create -vsriver vs1 -volume vol1 -space-slo thick
```

次のコマンドを使うと、SVM vs1 上の vol1 にセミシックプロビジョニングが設定されます。

```
cluster1::> volume create -vsriver vs1 -volume vol1 -space-slo semi-  
thick
```

## SAN ボリュームの構成オプション

LUN が含まれているボリュームに対してさまざまなオプションを設定する必要があります。ボリュームオプションの設定方法によって、ボリューム内の LUN で使用可能なスペースの量が決まります。

### 自動拡張

自動拡張は有効または無効にすることができます。有効にすると、ONTAP では、ボリュームのサイズを事前設定した最大サイズまで自動的に拡張できます。ボリュームの自動拡張をサポートするには、使用可能なスペースを包含アグリゲートに確保する必要があります。そのため、自動拡張を有効にする場合は、包含アグリゲートの空きスペースを監視し、必要に応じて追加してください。

自動拡張は、Snapshot の作成時にはトリガーできません。自動拡張が有効になっていても、ボリュームに十分なスペースがないと Snapshot の作成は失敗します。

自動拡張が無効な場合、ボリュームのサイズに変更はありません。

### 自動縮小

自動縮小は有効または無効にすることができます。有効にすると、ONTAP では、ボリュームで消費されたスペースの量が事前設定したしきい値を下回った場合に、ボリューム全体のサイズを自動的に縮小できます。これにより、ボリュームで未使用の空きスペースの自動的な解放が開始されて、ストレージ効率が向上します。

## Snapshot の自動削除

Snapshot の自動削除では、次のいずれかの場合に、Snapshot コピーが自動的に削除されます。

- ボリュームがフルに近い状態の場合
- Snapshot リザーブスペースがフルに近い状態の場合
- オーバーライトリザーブスペースがフルの場合

古いものから順に、または新しいものから順に Snapshot コピーを削除するように Snapshot の自動削除を設定できます。Snapshot の自動削除では、クローンボリュームや LUN 内の Snapshot コピーにリンクされている Snapshot コピーは削除されません。

自動拡張と Snapshot の自動削除の両方が有効な場合にボリュームで追加のスペースが必要になると、デフォルトでは、ONTAP は最初に自動拡張をトリガーして、必要なスペースを確保しようとします。自動拡張で十分なスペースを確保できない場合は、Snapshot の自動削除がトリガーされます。

## Snapshot リザーブ

Snapshot リザーブは、Snapshot コピー用にリザーブされるボリューム内のスペースの量を定義します。Snapshot リザーブに割り当てられたスペースを他の目的に使用することはできません。Snapshot リザーブ用に割り当てられたすべてのスペースが使用された場合、Snapshot コピーはボリューム上の追加スペースを消費します。

## SAN 環境でのボリューム移動に関する要件

LUN またはネームスペースを含むボリュームを移動する場合は、一定の要件を満たす必要があります。

- ボリュームに 1 つ以上の LUN が含まれている場合は、クラスタ内の各ノードに接続する LUN（LIF）ごとに少なくとも 2 つのパスが必要です。

これにより、単一点障害が排除され、コンポーネント障害に備えてシステムの運用を継続することができま

- ボリュームにネームスペースが含まれている場合は、クラスタで ONTAP 9.6 以降が実行されている必要があります。

ONTAP 9.5 を実行する NVMe 構成では、ボリューム移動はサポートされません。

## フラクショナルリザーブの設定に関する考慮事項

フラクショナルリザーブは、`_lun overwrite reserve` と呼ばれ、FlexVol ボリューム内のスペースリザーブ LUN およびファイルのオーバーライトリザーブを無効にすることができます。これはストレージ利用率を最大限に高めるのに役立ちますが、スペース不足による書き込みエラーが悪影響を及ぼす環境では、この設定を利用する場合の要件を確認しておく必要があります。

フラクショナルリザーブ設定はパーセンテージで表され、有効な値はのみです 0 および 100 パーセントフラクショナルリザーブ設定はボリュームの属性です。

フラクショナルリザーブをに設定しています 0 ストレージ利用率が向上します。ただし、ボリュームの空きスペースがなくなると、ボリュームギャランティがに設定されていても、ボリュームに格納されたデータにアクセスするアプリケーションでデータを利用できなくなる可能性があります volume。ただし、ボリュームを適切に設定して使用することで、書き込みが失敗する可能性を最小限に抑えることができます。ONTAP では、フラクショナルリザーブがに設定されたボリュームに対して「ベストエフォート」の書き込み保証が提供されます 0 次の要件の\_all\_が満たされている場合：

- 重複排除を使用していません
- 圧縮を使用していません
- FlexClone サブファイルが使用されていません
- すべての FlexClone ファイルと FlexClone LUN で自動削除が有効になっています

これはデフォルト設定ではありません。FlexClone ファイルや FlexClone LUN の自動削除は、作成時に設定するか作成後に変更して明示的に有効にする必要があります。

- ODX コピーオフロードと FlexClone コピーオフロードは使用されていません
- ボリュームギャランティがに設定されている volume
- ファイルまたはLUNのスペースリザーベーションはです enabled
- ボリュームのSnapshotリザーブがに設定されている 0
- ボリュームSnapshotコピーの自動削除はです enabled を使用しています destroy`を削除します`lun\_clone,vol\_clone,cifs\_share,file\_clone,sfsr`をクリックします `volume

この設定では、必要に応じて FlexClone ファイルと FlexClone LUN も削除されます。

変更率が高いと、上記の必要な設定をすべて行っても、まれに Snapshot コピーの自動削除が追いつかなくなり、ボリュームのスペースが不足することがあります。

また、必要に応じてボリュームの自動拡張機能を使用することで、ボリュームの Snapshot コピーの自動削除が発生する可能性を抑えることができます。自動拡張機能を有効にする場合は、関連付けられたアグリゲートの空きスペースを監視する必要があります。アグリゲートの空きスペースがなくなり、ボリュームを拡張できなくなると、ボリュームの空きスペースがなくなったときに削除される Snapshot コピーが増える可能性があります。

上記の設定要件をすべて満たすことができず、ボリュームのスペース不足を防ぐ必要がある場合は、ボリュームのフラクショナルリザーブ設定をに設定する必要があります 100。これにより、事前に確保する必要がある空きスペースは増えますが、上記のテクノロジーを使用する場合でもデータ変更処理が確実に実行されるようになります。

フラクショナルリザーブ設定のデフォルト値と有効値は、ボリュームのギャランティによって異なります。

ボリュームギャランティ	デフォルトのフラクショナルリザーブ	使用できる値
ボリューム	100	0、100
なし	0	0、100



## SANホスト側のスペース管理

シンプロビジョニング環境において、ホストファイルシステムで解放されたスペースをストレージシステム側で管理するプロセスを担っているのがホスト側のスペース管理です。

ホストファイルシステムでは、新しいデータの格納に使用できるブロックはどれか、また、有効なデータを含んでいるため上書きしてはならないブロックはどれかを追跡するための情報がメタデータに記録されます。このメタデータは LUN 内に格納されます。ホストファイルシステム内でファイルが削除されると、ファイルシステムのメタデータが更新され、削除されたファイルのブロックが空きスペースとしてマークされます。ファイルシステム内の合計空きスペースが再計算され、新しく解放されたブロック分のスペースが組み入れられます。ストレージシステム側では、こうしたメタデータの更新が、ホストによって実行される他の書き込みとまったく相違ないものとして認識されます。このため、ストレージシステム側では、削除が行われた事実が検知されません。

その結果、ホスト側と基盤のストレージシステム側で報告される空きスペース容量に不一致が生じます。たとえば、新しくプロビジョニングされた 200GB の LUN がストレージシステムによってホストに割り当てられているとします。ホストとストレージシステムの両方で、200GB の空きスペースが報告されます。ホストに 100GB のデータが書き込まれた場合。この時点で、ホストとストレージシステムの両方で、使用済みスペースが 100GB 、未使用スペースが 100GB と報告されます。

次に、ホストから 50GB のデータが削除されました。この時点で、ホストは使用済みスペースが 50GB 、未使用スペースが 150GB であると報告します。ただし、ストレージシステムから報告される使用済みスペースは 100GB 、未使用スペースは 100GB です。

ホスト側のスペース管理では、さまざまな方法を使用して、ホストとストレージシステム間のスペースの差分を調整します。

### SnapCenter によるホスト管理の簡易化

SnapCenter ソフトウェアを使用すると、iSCSI ストレージや FC ストレージに関連する管理作業とデータ保護作業を簡単に行うことができます。SnapCenter は、Windows ホストと UNIX ホストに対応するオプションの管理パッケージです。

SnapCenter ソフトウェアを使用すると、ストレージプールから簡単に仮想ディスクを作成して複数のストレージシステムに分散したり、ストレージのプロビジョニングタスクを自動化したりできます。また、ホストのデータと整合性のある Snapshot コピーや Snapshot コピーからのクローンの作成プロセスが簡易化されます。

詳細については、ネットアップ製品のドキュメントを参照してください "[SnapCenter](#)"。

関連リンク

"[SCSI シンプロビジョニング LUN のスペース割り当てを有効にします](#)"

### igroup について

initiator group (igroup ; イニシエータグループ) は、FC プロトコルホスト WWPN または iSCSI ホストノード名のテーブルです。igroup を定義して LUN にマッピングし、どのイニシエータが LUN にアクセスできるかを制御できます。

通常は、ホストのイニシエータポートまたはソフトウェアイニシエータがすべて LUN にアクセスできること

が必要とされます。マルチパスソフトウェアを使用しているか、またはクラスタホストがある場合、各イニシエータポートまたは各クラスタホストのソフトウェアイニシエータは同じ LUN への冗長パスを必要とします。

LUN にアクセスできるイニシエータを指定する igroup は LUN の作成前後どちらでも作成できますが、LUN を igroup にマッピングするには igroup を作成しておく必要があります。

igroup には複数のイニシエータを含めることができ、複数の igroup に同じイニシエータを含めることができます。ただし、同じイニシエータを持つ複数の igroup に 1 つの LUN をマッピングすることはできません。1 つのイニシエータを、ostype が異なる複数の igroup のメンバーにすることはできません。

**igroup による LUN アクセスの提供例**

複数の igroup を作成して、ホストで利用できる LUN を定義することができます。たとえば、ホストクラスタを使用している場合、いくつかの igroup を使用して、クラスタ内の 1 つのホストだけ、またはすべてのホストに特定の LUN が認識されるように設定できます。

次の表に、ストレージシステムにアクセスする 4 つのホストについて、4 つの igroup によって LUN にアクセスできるようにする方法を示します。クラスタ化したホスト（Host3 および Host4）は、両方とも同一 igroup（group3）のメンバーであり、この igroup にマッピングされている LUN にアクセスできます。group4 という igroup には Host4 の WWPN が含まれ、パートナーには表示されないローカルな情報が格納されます。

HBA WWPN、IQN 、または EUI のホスト	igroup 数	igroup に追加されている WWPN、IQN、EUI	igroup にマッピングされている LUN
Host1、シングルパス（ iSCSI ソフトウェアイニ シエータ）  iqn.1991- 05.com.microsoft:host1	グループ 1	iqn.1991- 05.com.microsoft:host1	/vol/vol2/lun1
Host2、マルチパス（ HBA × 2）  10 : 00 : 00 : 00 : c9 : 2b : 6b : 3c  10 : 00 : 00 : 00 : c9 : 2b : 02 : 3c	グループ2	10 : 00 : 00 : 00 : c9 : 2b : 6b : 3c  10 : 00 : 00 : 00 : c9 : 2b : 02 : 3c	/vol/vol2/lun2

HBA WWPN、IQN、または EUI のホスト	igroup 数	igroup に追加されている WWPN、IQN、EUI	igroup にマッピングされている LUN
Host3、マルチパス、ホスト 4 でクラスタ構成  10 : 00 : 00 : 00 : c9 : 2b : 32 : 1b  10 : 00 : 00 : 00 : c9 : 2b : 41 : 02	グループ 3	10 : 00 : 00 : 00 : c9 : 2b : 32 : 1b  10 : 00 : 00 : 00 : c9 : 2b : 41 : 02  10 : 00 : 00 : 00 : c9 : 2b : 51 : 2c  10 : 00 : 00 : 00 : c9 : 2b : 47 : A2	/vol/vol2/qtrees1/lun3
Host4、マルチパス、クラスタ構成（Host3 には認識されない）  10 : 00 : 00 : 00 : c9 : 2b : 51 : 2c  10 : 00 : 00 : 00 : c9 : 2b : 47 : A2	グループ 4	10 : 00 : 00 : 00 : c9 : 2b : 51 : 2c  10 : 00 : 00 : 00 : c9 : 2b : 47 : A2	/vol/vol2/qtrees2/lun4 /vol/vol2/qtrees1/lun5

## igroup のイニシエータの WWPN と iSCSI ノード名を指定します

igroup の作成時に、イニシエータの iSCSI ノード名と WWPN を指定できます。それらをあとから指定することもできます。LUN の作成時にイニシエータの iSCSI ノード名と WWPN を指定するように選択した場合は、必要に応じてそれらをあとから削除できます。

Host Utilities のマニュアルに記載されている手順に従って、WWPN を取得し、特定のホストに関連付けられている iSCSI ノード名を確認します。ESX ソフトウェアを実行しているホストでは、Virtual Storage Console を使用します。

## VMware と Microsoft のコピーオフロードによるストレージ仮想化

### VMware と Microsoft のコピーオフロードによるストレージ仮想化の概要

VMware と Microsoft は、パフォーマンスとネットワークスループットを向上させるために、コピーオフロード処理をサポートしています。VMware と Windows それぞれのオペレーティングシステム環境で、コピーオフロード機能を使用するための要件を満たすように、システムを設定する必要があります。

VMware と Microsoft のコピーオフロードを仮想環境で使用する場合は、LUN をアライメントする必要があります。LUN がアライメントされていないと、パフォーマンスが低下

## 仮想 SAN 環境を使用する利点

Storage Virtual Machine（SVM）と LIF を使用して仮想環境を作成すると、SAN 環境をクラスタ内のすべてのノードに拡張できます。

- 分散管理

SVM の任意のノードにログインして、クラスタ内のすべてのノードを管理できます。

- データアクセスの向上

MPIO と ALUA を使用することで、SVM のどのアクティブな iSCSI LIF または FC LIF からでもデータにアクセスできます。

- LUN アクセスの制御

SLM とポートセットを使用すると、イニシエータによって LUN へのアクセスに使用される LIF を制限できます。

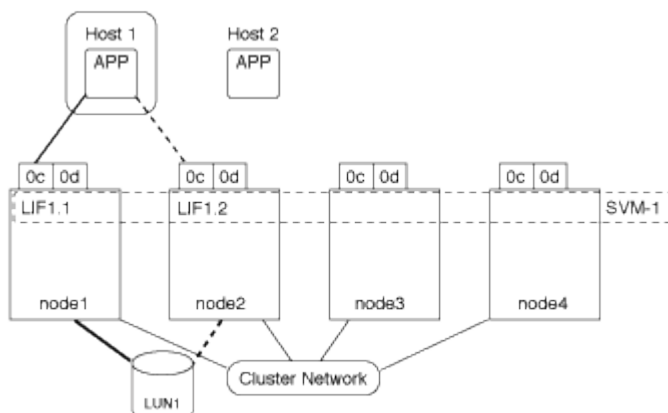
## 仮想環境での LUN へのアクセスの仕組み

仮想環境では、ホスト（クライアント）は LIF を使用して、最適パスおよび非最適パス経路で LUN にアクセスします。

LIF は、SVM を物理ポートに接続する論理インターフェイスです。複数の SVMs で同じポート上に複数の LIF を設定できますが、1 つの LIF は 1 つの SVM に属します。LUN には、SVM の LIF を介してアクセスできます。

### クラスタ内の1つのSVMを使用したLUNへのアクセス例

次の例では、ホスト 1 が SVM-1 の LIF1.1 と LIF1.2 に接続して LUN1 にアクセスします。LIF1.1 は物理ポート node1 : 0c を、LIF1.2 は node2 : 0c を使用します。LIF1.1 と LIF1.2 は SVM-1 のみに属しています。SVM-1 のノード 1 またはノード 2 で新しい LUN を作成した場合は、その LUN でもこれらの同じ LIF を使用できます。新しい SVM を作成した場合は、両方のノードの物理ポート 0c または 0d を使用して新しい LIF を作成できます。



### クラスタ内の複数のSVMを使用したLUNへのアクセス例

1 つの物理ポートに複数の LIF を設定して、異なる SVM を接続できます。LIF は特定の SVM に関連付けられているため、クラスタノードは受信データトラフィックを正しい SVM に送信できます。次の例では、1~4 の

各ノードに、各ノードの物理ポート 0c を使用して SVM-2 用の LIF を 1 つずつ設定しています。ホスト 1 は SVM-1 の LIF1.1 と LIF1.2 に接続して LUN1 にアクセスします。ホスト 2 は、SVM-2 の LIF2.1 と LIF2.2 に接続して LUN2 にアクセスします。両方の SVM がノード 1 とノード 2 の物理ポート 0c を共有しています。SVM-2 には追加の LIF があり、ホスト 2 はこの LIF を使用して LUN3 と LUN4 にアクセスします。これらの LIF はノード 3 とノード 4 の物理ポート 0c を使用します。複数の SVMs でそれらのノードの物理ポートを共有できます。



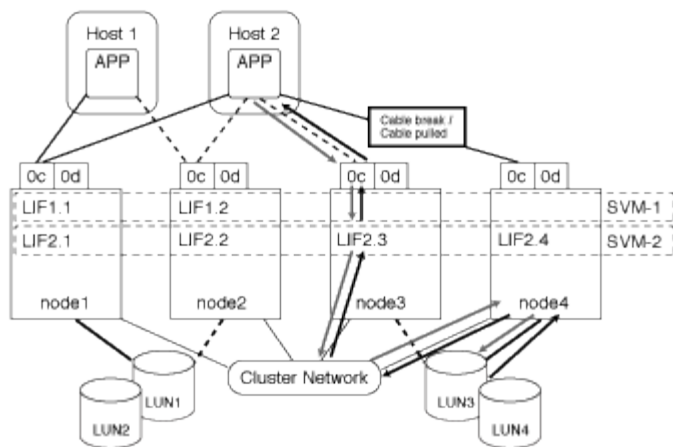
#### ホストシステムからLUNへのアクティブパスまたは最適パスの例

アクティブパスまたは最適パスでは、データトラフィックはクラスタネットワークを経由せずに、LUN への最短ルートをとります。LUN1 へのアクティブパスまたは最適パスは、物理ポート 0c を使用してノード 1 の LUN1.1 を経由します。ホスト 2 には、アクティブパスまたは最適パスが 2 つあります。1 つは node1 へのパスで、LIF2.1 は物理ポート 0c を共有し、もう 1 つは node4、LIF2.4 は物理ポート 0c を使用します。



#### ホストシステムからLUNへのアクティブパスまたは非最適（間接）パスの例

アクティブパスまたは非最適（間接）パスでは、データトラフィックはクラスタネットワークを経由します。この問題は、ホストからのアクティブパスまたは最適パスがすべて使用できず、トラフィックを処理できない場合にのみ発生します。ホスト 2 から SVM-2 LIF2.4 へのパスが失われた場合は、クラスタネットワークを経由して LUN3 と LUN4 にアクセスします。ホスト 2 からのアクセスには、ノード 3 の LIF2.3 が使用されます。トラフィックは、クラスタネットワークスイッチに入ったあと、LUN3 と LUN4 にアクセスできるようノード 4 にバックアップされます。次に、クラスタネットワークスイッチ経由で逆方向に戻り、LIF2.3 経由でホスト 2 にバックアウトされます。このアクティブパスまたは非最適パスは、LIF2.4 へのパスがリストアされるか、ノード 4 のもう 1 つの物理ポートで SVM-2 の新しい LIF が確立されるまで使用されます。



=  
:allow-uri-read:

### ESX ホストの VMware VAAI パフォーマンスを向上させます

ONTAP では、ESX ホストで ESX 4.1 以降が実行されている場合、VMware vStorage APIs for Array Integration（VAAI）の一部の機能がサポートされます。これらの機能を使用すると、ESX ホストからストレージシステムに処理の負荷をオフロードし、ネットワークスループットを向上させることができます。これらの機能は、正しい環境の ESX ホストで自動的に有効になります。

VAAI 機能は、次の SCSI コマンドをサポートします。

- EXTENDED\_COPY

この機能により、ホストは、データ転送の際にホストに影響を与えることなく、LUN 間または LUN 内のデータ転送を開始できます。その結果、ESX CPU サイクルが節約され、ネットワークスループットが増加します。拡張コピー機能は「コピーオフロード」とも呼ばれ、仮想マシンのクローニングなどで使用されます。ESX ホストからコピーオフロード機能が呼び出されると、ホストネットワークを経由せずにストレージシステム内でデータがコピーされます。コピーオフロードでは、次の方法でデータが転送されます。

- LUN 内で組み合わせることができます
- ボリューム内の LUN 間
- Storage Virtual Machine（SVM）内の異なるボリューム上の LUN 間
- クラスタ内の異なる SVM 上の LUN 間

この機能呼び出すことができない場合、ESX ホストは自動的に標準の読み取りコマンドと書き込みコマンドをコピー処理に使用します。

- WRITE\_SAME

この機能により、すべてゼロなどの繰り返しパターンをストレージアレイに書き込む処理がオフロードされます。この機能は、ファイルをゼロで埋める場合などに使用されます。

- COMPARE\_AND\_WRITE

特定のファイルへの同時アクセス制限がバイパスされ、仮想マシンのブートなどの処理が高速になります。

す。

#### VAAI 環境を使用するための要件

VAAI 機能は ESX オペレーティングシステムの一部であり、環境を正しく設定すると、ESX ホストによって自動的に起動されます。

環境の要件は次のとおりです。

- ESX ホストで ESX 4.1 以降が実行されている必要があります。
- VMware データストアをホストするネットアップストレージシステムで ONTAP を実行する。
- (コピーオフロードのみ) VMware コピー操作のソースとデスティネーションの両方が同じクラスタ内の同じストレージシステムでホストされている。



コピーオフロード機能は、現時点では、異なるストレージシステムでホストされている VMware データストア間のコピーに対応していません。

VAAI 機能が ESX でサポートされているかどうかを確認します

ESX オペレーティングシステムで VAAI 機能がサポートされているかどうかを確認するには、vSphere Client を確認するか、他の方法でホストにアクセスします。ONTAP はデフォルトで SCSI コマンドをサポートします。

ESX ホストの詳細設定を確認して、VAAI 機能が有効になっているかどうかを確認できます。次の表に、SCSI コマンドと対応する ESX コントロールの名前を示します。

SCSIコマンド	ESX コントロール名 (VAAI 機能)
extended_copy の実行が可能です	HardwareAcceleratedMove
WRITE_Same	HardwareAcceleratedInit
_ と _ を比較します	HardwareAcceleratedLocking

#### Microsoft オフロードデータ転送 (ODX)

Microsoft Offloaded Data Transfer (ODX ; オフロードデータ転送) は \_ コピーオフロード \_ とも呼ばれ、この機能を使用すると、ストレージデバイス内または互換性があるストレージデバイス間で、ホストコンピュータを介さずにデータを直接転送できます。

ONTAPでは、SMBプロトコルとSANプロトコルの両方でODXがサポートされます。

ODX 以外のファイル転送では、ソースからデータが読み取られ、ネットワーク経由でホストに転送されます。ホストは、データをネットワーク経由でデスティネーションに転送します。ODX ファイル転送では、ホストを経由せずに、データがソースからデスティネーションに直接コピーされます。

ODXオフロードコピーはソースとデスティネーションの間で直接実行されるため、同じボリューム内でコピーを実行するとパフォーマンスが大幅に向上します。たとえば、同じボリュームコピーのコピー時間の短縮、



クライアントでのCPUとメモリの使用量の削減、ネットワークI/O帯域幅の使用量の削減などが挙げられます。複数のボリュームにコピーが存在する場合は、ホストベースのコピーに比べてパフォーマンスが大幅に向上することはありません。

SAN 環境で ODX を使用できるのは、ホストとストレージシステムの両方で ODX がサポートされている場合のみです。ODX がサポートされていて有効になっているクライアントコンピュータでは、ファイルの移動やコピーを行う際に、オフロードファイル転送が自動的にかつ透過的に使用されます。ODX は、ファイルをエクスプローラでドラッグアンドドロップしたか、コマンドラインのファイルコピーコマンドを使用したか、クライアントアプリケーションによってファイルコピー要求が開始されたかに関係なく使用されます。

#### ODX を使用するための要件

コピーオフロードに ODX を使用する場合は、ボリュームのサポートに関する考慮事項、システム要件、およびソフトウェア機能の要件について理解しておく必要があります。

ODX を使用するためのシステム要件は次のとおりです。

- ONTAP

サポート対象のバージョンの ONTAP では、ODX が自動的に有効になります。

- ソースボリュームの最小サイズは 2GB です

最適なパフォーマンスを確保するには、260GB 以上のソースボリュームが必要です。

- Windows クライアントでの ODX のサポート

ODX は、Windows Server 2012 以降および Windows 8 以降でサポートされます。サポート対象の Windows クライアントの最新情報については、Interoperability Matrix を参照してください。

["NetApp Interoperability Matrix Tool で確認できます"](#)

- コピーアプリケーションによる ODX のサポート

データ転送を実行するアプリケーションが ODX をサポートする必要があります。ODX がサポートされるアプリケーション処理は次のとおりです。

- Virtual Hard Disk (VHD ; 仮想ハードディスク) の作成および変換、Snapshot コピーの管理、仮想マシン間でのファイルのコピーなど、Hyper-V の管理処理
  - エクスプローラでの操作
  - Windows PowerShell の copy コマンド
  - Windows コマンドプロンプトの copy コマンド
- Windows サーバおよびクライアントでサポートされる ODX アプリケーションの詳細については、Microsoft TechNet ライブラリを参照してください。

- 圧縮されたボリュームを使用する場合は、圧縮グループサイズを 8K にする必要があります。

32K の圧縮グループサイズはサポートされていません。

ODX を次のタイプのボリュームで使用することはできません。

- 容量が 2GB 未満のソースボリューム



- 読み取り専用ボリューム
- "FlexCache ボリューム"



ODXはFlexCache元のボリュームでサポートされます。

- "セミシックプロビジョニングされたボリューム"

#### 特別なシステムファイルの要件

qtree で見つかった ODX ファイルを削除できます。テクニカルサポートから指示されないかぎり、他の ODX システムファイルは削除または変更しないでください。

ODX 機能を使用する場合、システムのすべてのボリュームに ODX システムファイルが存在します。これらのファイルによって、ODX 転送時に使用されるデータのポイントインタイムビューが有効になります。次のシステムファイルは、データのオフロード先となる LUN またはファイルがある各ボリュームのルートレベルにあります。

- .copy-offload （非表示のディレクトリ）
- .tokens （非表示の下のファイル .copy-offload ディレクトリ）

を使用できます `copy-offload delete-tokens -path dir_path -node node_name` ODXファイルを含むqtreeを削除するコマンド。

#### ODX のユースケース

SVM で ODX を使用する前に、どのような場合にパフォーマンスを向上できるかを判断できるようにユースケースについて確認しておく必要があります。

ODX をサポートする Windows サーバおよびクライアントでは、リモートサーバ間でデータをコピーする際に、デフォルトでコピーオフロードが使用されます。Windows サーバまたはクライアントで ODX がサポートされていない場合や、ODX コピーオフロードが任意の時点で失敗した場合は、コピーまたは移動処理が従来の読み取りと書き込みの処理を使用して実行されます。

ODX コピーおよび移動の使用は、以下のユースケースでサポートされます。

- ボリューム内

ソースとデスティネーションのファイルまたは LUN は、同じボリューム内にあります。

- ボリュームが異なり、ノードと SVM は同じです

ソースとデスティネーションのファイルまたは LUN は、同じノード上の異なるボリュームにあります。データは同じ SVM に所有されます。

- ボリュームとノードが異なり、SVM は同じです

ソースとデスティネーションのファイルまたは LUN は、異なるノード上の異なるボリュームにあります。データは同じ SVM に所有されます。

- SVM が異なり、ノードは同じです

ソースとデスティネーションのファイルまたは LUN は、同じノード上の異なるボリュームにあります。データは異なる SVM に所有されます。

- SVM とノードが異なります

ソースとデスティネーションのファイルまたは LUN は、異なるノード上の異なるボリュームにあります。データは異なる SVM に所有されます。

- クラスタ間

ソース LUN とデスティネーション LUN は、異なるクラスタの異なるノード上の異なるボリュームにあります。これは SAN でのみサポートされ、SMB では機能しません。

その他にも、いくつかの特殊なユースケースがあります。

- ONTAP の ODX の実装で ODX を使用すると、SMB 共有と FC / iSCSI で接続された仮想ドライブとの間でファイルをコピーできます。

SMB 共有と LUN が同じクラスタにある場合は、Windows エクスプローラ、Windows CLI または PowerShell、Hyper-V、または ODX をサポートするその他のアプリケーションを使用して、SMB 共有と接続された LUN 間の ODX コピーオフロードを使用してファイルをシームレスにコピーまたは移動できます。

- Hyper-V では、さらに次のようなユースケースでも ODX コピーオフロードが使用されます。
    - Hyper-V で ODX コピーオフロードのパススルーを使用して、仮想ハードディスク（VHD）ファイル内および VHD ファイル間でのデータのコピー、または同じクラスタ内のマッピングされた SMB 共有と接続された iSCSI LUN の間でのデータのコピーを実行できます。
- これにより、ゲストオペレーティングシステムからのコピーを基盤となるストレージに渡すことができます。
- 容量固定 VHD を作成する際に、ODX を使用して、既知の初期化済みトークンによってディスクを初期化します。
  - ソースとデスティネーションのストレージが同じクラスタにある場合に、ODX コピーオフロードを使用して、仮想マシンのストレージを移行します。



Hyper-V での ODX コピーオフロードのパススルーの用途を活用するには、ゲストオペレーティングシステムで ODX がサポートされている必要があります。また、ゲストオペレーティングシステムのディスクが、ODX をサポートするストレージ（SMB または SAN）から作成された SCSI ディスクである必要があります。ゲストオペレーティングシステムのディスクが IDE ディスクの場合、ODX のパススルーはサポートされません。

## SAN 管理

### SAN プロビジョニング

#### SAN の管理の概要

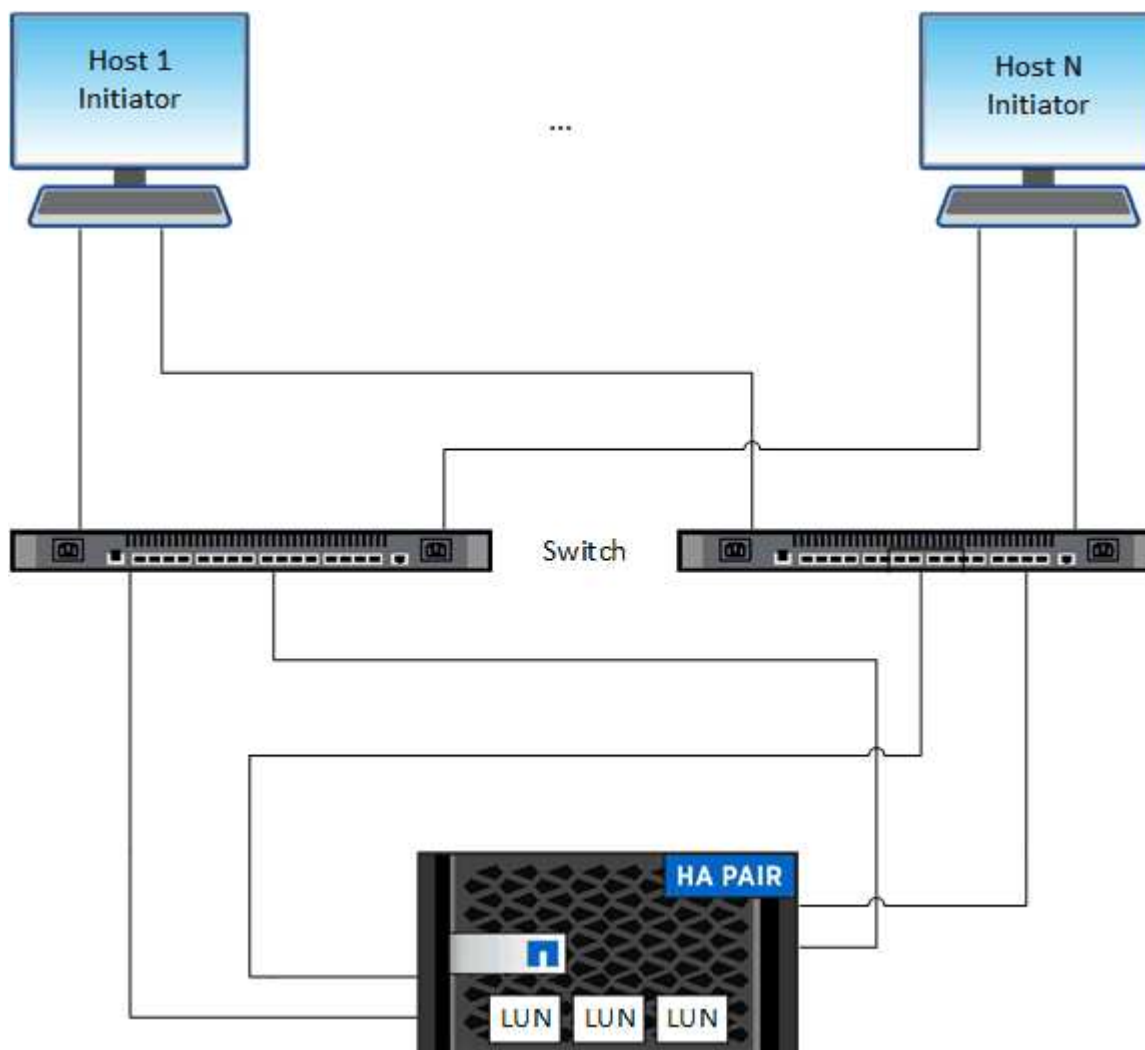
このセクションの内容では、ONTAP 9.7以降のリリースのONTAP コマンドラインイン

ターフェイス（CLI）およびSystem Managerを使用してSAN環境を構成および管理する方法を説明します。

従来の System Manager（ONTAP 9.7 以前でのみ使用可能）を使用している場合は、次のトピックを参照してください。

- ["iSCSI プロトコル"](#)
- ["FC/FCoE プロトコル"](#)

iSCSI プロトコルと FC プロトコルを使用して、SAN 環境にストレージを提供できます。



iSCSI および FC では、ストレージターゲットは LUN（論理ユニット）と呼ばれ、標準のブロックデバイスとしてホストに提示されます。LUN を作成して、イニシエータグループ（igroup）にマッピングします。イニシエータグループは、FC ホスト WWPS と iSCSI ホストノード名の表であり、どのイニシエータがどの LUN にアクセスできるかを制御します。

FC ターゲットは FC スイッチおよびホスト側アダプタを介してネットワークに接続され、World Wide Port Name（WWPN；ワールドワイドポート名）で識別されます。iSCSI ターゲットは、標準のイーサネットネットワークアダプタ（NIC）、ソフトウェアイニシエータを搭載した TCP オフロードエンジン（TOE）カード、統合ネットワークアダプタ（CNA）または専用のホストバスアダプタ（HBA）を介してネットワークに接続し、iSCSI 修飾名（IQN）で識別されます。

## FCoE 用にスイッチを設定します

既存のイーサネットインフラで FC サービスを実行するには、FCoE 用にスイッチを設定する必要があります。

### 必要なもの

- SAN 構成がサポートされている必要があります。

サポートされている構成の詳細については、を参照してください ["NetApp Interoperability Matrix Tool で確認できます"](#)。

- Unified Target Adapter （UTA ; ユニファイドターゲットアダプタ）をストレージシステムに設置する必要があります。

UTA2を使用する場合は、に設定する必要があります cna モード（Mode）：

- Converged Network Adapter （CNA ; 統合ネットワークアダプタ）をホストにインストールする必要があります。

### 手順

1. スイッチのマニュアルを使用して、FCoE 用にスイッチを設定します。
2. クラスタ内の各ノードのDCB設定が正しく設定されていることを確認します。

```
run -node node1 -command dcb show
```

DCB 設定はスイッチに対して行われます。設定が正しくない場合は、スイッチのマニュアルを参照してください。

3. FCターゲットポートのオンラインステータスがのときにFCoEログインが機能していることを確認する true。

```
fcip adapter show -fields node,adapter,status,state,speed,fabric-established,physical-protocol
```

FCターゲットポートのオンラインステータスがの場合 `false` スイッチのマニュアルを参照してください。

### 関連情報

- ["NetApp Interoperability Matrix Tool で確認できます"](#)
- ["ネットアップテクニカルレポート 3800 : 『Fibre Channel over Ethernet（FCoE）End-to-End Deployment Guide』"](#)
- ["Cisco MDS 9000 NX-OS および SAN-OS ソフトウェアの構成ガイド"](#)
- ["Brocade 製品"](#)

## システム要件

LUN のセットアップでは、LUN を作成し、igroup を作成して、LUN を igroup にマッピングします。LUN をセットアップするには、システムが特定の前提条件を満たしている必要があります。

- Interoperability Matrix にサポート対象として掲載されている SAN 構成を使用する。
- で指定した SAN ホストとコントローラの構成の制限を SAN 環境が満たしている必要があります ["NetApp Hardware Universe の略"](#) ONTAP ソフトウェアのバージョンに対応している必要があります。
- サポートされているバージョンの Host Utilities がインストールされている。

詳細については、Host Utilities のマニュアルを参照してください。

- LUN の所有者ノードと所有者ノードの HA パートナーに SAN LIF がある。

## 関連情報

- ["NetApp Interoperability Matrix Tool で確認できます"](#)
- ["ONTAP SAN ホスト構成"](#)
- ["ネットアップテクニカルレポート 4017 : 『ファイバチャネル SAN のベストプラクティス』"](#)

## LUNを作成する前に理解しておくべきこと

### LUNの実際のサイズが少し異なる理由

LUNのサイズについては、次の点に注意してください。

- LUNを作成する場合、LUNの実際のサイズはLUNのOSタイプによって多少異なります。LUN の作成後に LUN の OS タイプを変更することはできません。
- 最大LUNサイズでLUNを作成する場合は、LUNの実際のサイズが若干小さくなる可能性があることに注意してください。ONTAP では、制限値の端数が切り捨てられます。
- 各 LUN のメタデータ用として、LUN を含むアグリゲートに約 64KB のスペースが必要です。LUN の作成時には、LUN を含むアグリゲートに LUN のメタデータ用の十分なスペースがあることを確認する必要があります。アグリゲートに LUN のメタデータ用のスペースが十分ないと、一部のホストが LUN にアクセスできなくなる可能性があります。

### LUN ID の割り当てに関するガイドライン

通常、デフォルトの LUN ID は 0 で始まり、LUN をマッピングするたびに 1 ずつ増加します。LUN ID は、ホストによって LUN の場所とパス名に関連付けられます。有効な LUN ID 番号の範囲は、ホストによって異なります。詳細については、Host Utilities のマニュアルを参照してください。

### LUN を igroup にマッピングする場合のガイドラインを次に示します

- LUNは、igroupに一度だけマッピングできます。
- ベストプラクティスとして、1つのLUNをigroupを介して1つの特定のイニシエータにのみマッピングすることを推奨します。
- 1つのイニシエータを複数の igroup に追加できますが、そのイニシエータをマッピングできる LUN は 1 つだけです。

- 同じ igroup にマッピングされている 2 つの LUN に、同じ LUN ID を使用することはできません。
- igroup およびポートセットには、同じ種類のプロトコルを使用する必要があります。

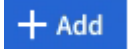
プロトコル**FC**または**iSCSI**ライセンスを確認して追加します

FC または iSCSI で Storage Virtual Machine （ SVM ） のブロックアクセスを有効にするには、ライセンスが必要です。FCライセンスとiSCSIライセンスは、に含まれています。 **"ONTAP One"**。

## 例 6. 手順

### System Manager の略

ONTAP Oneをお持ちでない場合は、ONTAP System Manager（9.7以降）でFCまたはiSCSIのライセンスを確認して追加します。

1. System Managerで、\*[クラスタ]>[設定]>[ライセンス]\*を選択します
2. ライセンスが表示されない場合は、を選択します  をクリックし、ライセンスキーを入力します。
3. 「\* 追加」を選択します。

### CLI の使用

ONTAP Oneをお持ちでない場合は、ONTAP CLIを使用してFCまたはiSCSIのライセンスを確認して追加します。

1. FCまたはiSCSIのアクティブなライセンスがあることを確認します。

```
system license show
```

Package	Type	Description	Expiration
Base	site	Cluster Base License	-
NFS	site	NFS License	-
CIFS	site	CIFS License	-
iSCSI	site	iSCSI License	-
FCP	site	FCP License	-

2. FCまたはiSCSIのアクティブなライセンスがない場合は、ライセンスコードを追加します。

```
license add -license-code <your_license_code>
```

## SAN ストレージをプロビジョニング

この手順 では、すでにFCプロトコルまたはiSCSIプロトコルが設定されている既存のStorage VMに新しいLUNが作成されます。

新しいStorage VMを作成してFCプロトコルまたはiSCSIプロトコルを設定する必要がある場合は、を参照してください ["FC 用に SVM を設定"](#) または ["SVM を iSCSI 用に設定"](#)。

FCライセンスが有効になっていない場合、LIFとSVMはオンラインとして表示されますが、動作ステータスはdownになります。

LUNは、ホストではディスクデバイスとして表示されます。



LUN の作成時、Asymmetric Logical Unit Access (ALUA ; 非対称論理ユニットアクセス) は常に有効になります。ALUA の設定は変更できません。

イニシエータをホストするには、SVM 内のすべての FC LIF で単一イニシエータゾーニングを使用する必要があります。

ONTAP 9.8 以降では、ストレージをプロビジョニングすると QoS がデフォルトで有効になります。QoS を無効にするか、プロビジョニングプロセス中またはあとからカスタムの QoS ポリシーを選択できます。

**System Manager の略**

ONTAP System Manager (9.7以降) でFCまたはiSCSIプロトコルを使用してSANホストにストレージを提供するためのLUNを作成します。

System Manager Classic (9.7以前で使用可能) を使用してこのタスクを完了するには、を参照してください ["Red Hat Enterprise Linux 向けの iSCSI の設定"](#)

**手順**

1. 該当するをインストールします ["SANホストユーティリティ"](#) ホスト。
2. System Manager で、 \* Storage > LUNs \* をクリックし、 \* Add \* をクリックします。
3. LUN の作成に必要な情報を入力します。
4. ONTAP のバージョンに応じて、「その他のオプション」をクリックすると、次のいずれかの操作を実行できます。

オプション	以降で使用できません
<ul style="list-style-type: none"><li>• 親ボリュームではなく LUN に QoS ポリシーを割り当て<ul style="list-style-type: none"><li>◦ * その他のオプション &gt; ストレージと最適化 *</li><li>◦ パフォーマンスサービスレベル * を選択します。</li><li>◦ ボリューム全体ではなく個々の LUN に QoS ポリシーを適用するには、 * これらのパフォーマンス制限を各 LUN に適用 * を選択します。</li></ul></li></ul> <p>デフォルトでは、パフォーマンス制限がボリュームレベルで適用されます。</p>	ONTAP 9.10.1
<ul style="list-style-type: none"><li>• 既存の igroup を使用して新しいイニシエータグループを作成します<ul style="list-style-type: none"><li>◦ * 「その他のオプション」 &gt; 「ホスト情報」 *</li><li>◦ 既存のイニシエータグループを使用して新しいイニシエータグループを選択します *。<ul style="list-style-type: none"><li>▪ 注：他の igroup を含む igroup の OS タイプは、作成後に変更することはできません。</li></ul></li></ul></li></ul>	ONTAP 9.9.1
<ul style="list-style-type: none"><li>• 概要を igroup またはホストイニシエータに追加します</li></ul> <p>概要は、igroup またはホストイニシエータのエイリアスとして機能します。</p> <ul style="list-style-type: none"><li>◦ * 「その他のオプション」 &gt; 「ホスト情報」 *</li></ul>	ONTAP 9.9.1



<ul style="list-style-type: none"> <li>• 既存のボリュームに LUN を作成します</li> </ul> <p>デフォルトでは、新しいボリュームに新しい LUN が作成されます。</p> <ul style="list-style-type: none"> <li>◦ * その他のオプション &gt; LUN の追加 *</li> <li>◦ [ * グループ関連の LUN * ] を選択します。</li> </ul>	ONTAP 9.9.1
<ul style="list-style-type: none"> <li>• QoS を無効にするか、カスタムの QoS ポリシーを選択します</li> <li>◦ * その他のオプション &gt; ストレージと最適化 *</li> <li>◦ パフォーマンスサービスレベル * を選択します。</li> <li>▪ 注： ONTAP 9.9.1 以降では、カスタム QoS ポリシーを選択した場合、指定したローカル階層への手動配置を選択することもできます。</li> </ul>	ONTAP 9.8

5. FC の場合は、FC スイッチを WWPN でゾーニングします。イニシエータごとに 1 つのゾーンを使用し、各ゾーンにすべてのターゲットポートを含めます。

6. ホストでLUNを検出します。

VMware vSphereでは、Virtual Storage Console (VSC) を使用してLUNを検出して初期化します。

7. LUNを初期化し、必要に応じてファイルシステムを作成します。

8. ホストがLUNのデータの書き込みと読み取りを実行できることを確認します。

## CLI の使用

ONTAP CLIでFCまたはiSCSIプロトコルを使用してSANホストにストレージを提供するためのLUNを作成します。

1. FCまたはiSCSIのライセンスがあることを確認します。

```
system license show
```

Package	Type	Description	Expiration
Base	site	Cluster Base License	-
NFS	site	NFS License	-
CIFS	site	CIFS License	-
iSCSI	site	iSCSI License	-
FCP	site	FCP License	-

2. FCまたはiSCSIのライセンスがない場合は、を使用します license add コマンドを実行します

```
license add -license-code <your_license_code>
```

3. SVMでプロトコルサービスを有効にします。

- iSCSIの場合：\*

```
vserver iscsi create -vserver <svm_name> -target-alias <svm_name>
```

- FCの場合：\*

```
vserver fcp create -vserver <svm_name> -status-admin up
```

4. 各ノードにSVM用のLIFを2つ作成します。

```
network interface create -vserver <svm_name> -lif <lif_name> -role  
data -data-protocol <iscsi|fc> -home-node <node_name> -home-port  
<port_name> -address <ip_address> -netmask <netmask>
```

ネットアップでは、データを提供するSVMごとに、ノードごとに少なくとも1つのiSCSIまたはFC LIFをサポートしています。ただし、冗長性を確保するには、ノードごとに2つのLIFが必要です。iSCSIの場合は、別々のイーサネットネットワークにあるノードごとに少なくとも2つのLIFを設定することを推奨します。

5. LIFが作成され、動作ステータスがになっていることを確認します online：

```
network interface show -vserver <svm_name> <lif_name>
```

6. LUN を作成します。

```
lun create -vserver <svm_name> -volume <volume_name> -lun <lun_name>  
-size <lun_size> -ostype linux -space-reserve <enabled|disabled>
```

LUN 名は 255 文字以内で、スペースは使用できません。



NVFAIL オプションは、ボリュームで LUN が作成されると、自動的に有効になります。

7. igroup を作成します。

```
igroup create -vserver <svm_name> -igroup <igroup_name> -protocol  
<fcp|iscsi|mixed> -ostype linux -initiator <initiator_name>
```

8. LUN を igroup にマッピングします。

```
lun mapping create -vserver <svm_name> -volume <volume_name> -lun  
<lun_name> -igroup <igroup_name>
```

9. LUN が正しく設定されていることを確認します。

```
lun show -vserver <svm_name>
```

10. 必要に応じて、["ポートセットを作成してigroupにバインドします"](#)。
11. ホストのマニュアルに記載されている手順に従って、特定のホストでブロックアクセスを有効にします。
12. Host Utilities を使用して FC または iSCSI マッピングを完了し、ホスト上の LUN を検出します。

#### 関連情報

- ["SAN の管理の概要"](#)
- ["ONTAP SAN ホスト構成"](#)
- ["System ManagerでSANイニシエータグループを表示および管理します"](#)
- ["ネットアップテクニカルレポート 4017 : 『ファイバチャネル SAN のベストプラクティス』"](#)

## NVMeプロビジョニング

### NVMe の概要

NVMe ( Non-Volatile Memory Express ) プロトコルを使用して、 SAN 環境にストレージを提供できます。 NVMe プロトコルは、ソリッドステートストレージのパフォーマンスを高めるために最適化されています。

NVMe のストレージターゲットはネームスペースと呼ばれます。 NVMe ネームスペースは、論理ブロックにフォーマットして標準ブロックデバイスとしてホストに提供できる不揮発性ストレージの容量です。 FC および iSCSI で LUN をプロビジョニングして igroup にマッピングする場合と同様に、ネームスペースとサブシステムを作成し、ネームスペースをサブシステムにマッピングします。

NVMe ターゲットは、FC スイッチを使用する標準的な FC インフラ、またはイーサネットスイッチとホスト側アダプタを使用する標準の TCP インフラを通じてネットワークに接続されます。

NVMeのサポートは、ONTAP のバージョンによって異なります。 を参照してください ["NVMeのサポートと制限"](#) を参照してください。

## NVMe とは

Nonvolatile Memory Express（NVMe）プロトコルは、不揮発性ストレージメディアへのアクセスに使用する転送プロトコルです。

NVMe over Fabrics（NVMeoF）は仕様で定義された NVMe の拡張機能であり、PCIe 以外の接続経路による NVMe ベースの通信を実現します。このインターフェイスを使用すると、外部のストレージエンクロージャをサーバに接続できます。

NVMe は、フラッシュテクノロジーから高性能な永続的メモリテクノロジーまで、不揮発性メモリを搭載したストレージデバイスに効率的にアクセスできるように設計されています。そのため、ハードディスクドライブ用に設計されたストレージプロトコルのような制限はありません。フラッシュデバイスとソリッドステートデバイス（SSD）は、不揮発性メモリ（NVM）の一種です。NVM では停電時にもデータが失われません。NVMe はそのメモリにアクセスするための手段です。

NVMe のメリットには、データ転送の速度、生産性、スループット、容量の向上があります。具体的には次のような特性があります。

- NVMe は最大 64、000 のキューを使用できるように設計されています。

各キューには、最大 64、000 個のコマンドを同時に保持できます。

- NVMe は、複数のハードウェアベンダーとソフトウェアベンダーでサポートされています
- フラッシュテクノロジーを使用すると NVMe の生産性が向上し、応答時間が短縮されます
- NVMe では、SSD に送信される「検索」ごとに複数のデータ要求を行うことができます。

NVMe は「要求」のデコードにかかる時間が短く、マルチスレッドプログラムでスレッドロックを必要としません。

- CPU レベルでのボトルネックを防止する機能をサポートし、システムの拡張に応じて並外れた拡張性を実現します。

## NVMe ネームスペースについて

NVMe ネームスペースは、論理ブロックにフォーマット可能な不揮発性メモリ（NVM）の容量です。ネームスペースは、Storage Virtual Machine で NVMe プロトコルが設定されている場合に使用され、FC および iSCSI プロトコルの LUN に相当します。

NVMe ホストには、1 つ以上のネームスペースがプロビジョニングされて接続されます。各ネームスペースがさまざまなブロックサイズをサポートできます。

NVMe プロトコルは、複数のコントローラ経由でネームスペースへのアクセスを提供します。ほとんどのオペレーティングシステムでサポートされている NVMe ドライバを使用すると、Solid State Drive（SSD；ソリッドステートドライブ）ネームスペースは標準ブロックデバイスとして表示され、そのままファイルシステムとアプリケーションを導入できます。

ネームスペース ID（NSID）は、コントローラがネームスペースへのアクセスを提供するために使用する識別子です。ホストまたはホストグループに対して NSID を設定する場合は、ホストからボリュームへのアクセスも設定します。論理ブロックは一度に 1 つのホストグループにのみマッピングでき、同じホストグループに複数の NSID が割り当てられることはありません。

## NVMe サブシステムについて

NVMe サブシステムには、1 つ以上の NVMe コントローラ、ネームスペース、NVM サブシステムポート、NVM ストレージメディア、およびコントローラと NVM ストレージメディア間のインターフェイスが含まれます。NVMe ネームスペースを作成すると、デフォルトではサブシステムにマッピングされません。新しいサブシステムまたは既存のサブシステムをマッピングすることもできます。

### 関連情報

- ["NVMe ストレージをプロビジョニングする"](#)
- ["NVMe ネームスペースをサブシステムにマッピングする"](#)
- ["SAN ホストとクラウドクライアントを設定"](#)

## NVMe のライセンス要件

ONTAP 9.5 以降では、NVMe をサポートするにはライセンスが必要です。ONTAP 9.4 で NVMe が有効になっている場合、ONTAP 9.5 へのアップグレード後に 90 日間の猶予期間中にライセンスを取得する必要があります。

ライセンスを有効にするには、次のコマンドを使用します。

```
system license add -license-code NVMe_license_key
```

## NVMe の構成、サポート、制限事項

ONTAP 9.4 以降では **"Non-Volatile Memory Express (NVMe)"** SAN 環境ではプロトコルを使用できます。NVMe で使用される物理的なセットアップとゾーニングの手法は従来の FC ネットワークと同じですが、NVMe は FC-SCSI と比べて帯域幅が広く、IOPS が高く、レイテンシも低減されます。

NVMe のサポートと制限事項は、ONTAP のバージョン、プラットフォーム、構成によって異なります。具体的な構成の詳細については、を参照してください ["NetApp Interoperability Matrix Tool で確認できます"](#)。サポートされる制限については、["Hardware Universe"](#)。



クラスタあたりの最大ノード数は、Hardware Universe の\*サポートされるプラットフォームの混在\*で確認できます。

### 設定

- NVMe 構成は、単一ファブリックまたはマルチファブリックを使用してセットアップできます。
- SAN をサポートする SVM ごとに管理 LIF を 1 つ設定する必要があります。
- 異機種混在の FC スイッチファブリックの使用は、組み込みのブレードスイッチ以外はサポートされていません。

特定の例外については、を参照してください ["NetApp Interoperability Matrix Tool で確認できます"](#)。

- カスケードファブリック、部分メッシュファブリック、フルメッシュファブリック、コアエッジファブリック、およびディレクタファブリックは、FC スイッチをファブリックに接続する業界標準の方法であり、いずれもサポートされます。

ファブリックは 1 つまたは複数のスイッチで構成できます。また、ストレージコントローラは複数のスイッチに接続することができます。

## の機能

ONTAPのバージョンに応じて、次のNVMe機能がサポートされます。

ONTAP で開始しています...	NVMeのサポート
9.12.1:	NVMe/FCでの4ノードMetroCluster IP構成 <ul style="list-style-type: none"> <li>9.12.1よりも前のNVMeでは、MetroCluster 構成はサポートされません。</li> <li>MetroCluster構成はNVMe/TCPではサポートされません。</li> </ul>
9.10.1	<a href="#">ネームスペースのサイズを変更する</a>
9.9.1	<ul style="list-style-type: none"> <li>ネームスペースとLUNは同じボリュームに共存できます。</li> </ul>
9.8	<ul style="list-style-type: none"> <li>プロトコルの共存</li> </ul> SCSI、NAS、NVMeの各プロトコルを同じStorage Virtual Machine（SVM）に配置できます。  ONTAP 9.8より前のバージョンでは、SVMで利用できるプロトコルはNVMeだけです。 *
9.6	<ul style="list-style-type: none"> <li>ネームスペース用に512バイトブロック、4096バイトブロック</li> </ul> デフォルト値は 4096 です。ホストオペレーティングシステムで 4096 バイトブロックがサポートされていない場合のみ、 512 を使用してください。  <ul style="list-style-type: none"> <li>ネームスペースがマッピングされたボリュームの移動</li> </ul>
9.5	マルチパスHAペアのフェイルオーバー/ギブバック：

## プロトコル

次のNVMeプロトコルがサポートされます。

プロトコル	ONTAP で開始しています...	許可者
TCP	9.10.1	デフォルト

FC	9.4	デフォルト
----	-----	-------

ONTAP 9.8以降では、同じStorage Virtual Machine (SVM) にSCSI、NAS、NVMeの各プロトコルを設定できます。

ONTAP 9.7以前では、SVMで利用できるプロトコルはNVMeのみです。

#### ネームスペース

NVMeネームスペースを使用する場合は、次の点に注意する必要があります。

- LUN のデータが失われた場合、ネームスペースからリストアすることはできません。また、その逆も同様です。
- ネームスペースのスペースギャランティはそれを含むボリュームのスペースギャランティと同じになります。
- 7-ModeのData ONTAPからのボリューム移行では、ネームスペースを作成できません。
- ネームスペースでは、次のものはサポートされません。
  - 名前変更中です
  - ボリューム間での移動
  - ボリューム間でのコピー
  - オンデマンドコピー

#### その他の制限事項

**ONTAP** の次の機能は、**NVMe** 構成ではサポートされません。

- 同期
- Virtual Storage Console の略

次の説明は、**ONTAP 9.4** を実行しているノードのみに該当します。

- NVMe の LIF とネームスペースは、同じノードでホストする必要があります。
- NVMe LIF を作成する前に、NVMe サービスを作成する必要があります。

#### 関連情報

["最新SANのベストプラクティス"](#)

#### NVMe用のStorage VMを設定する

ノードで NVMe プロトコルを使用する場合は、SVM を NVMe 専用に設定する必要があります。


#### 作業を開始する前に

FC アダプタまたはイーサネットアダプタで NVMe がサポートされている必要があります。サポートされるアダプタの一覧については、を参照してください ["NetApp Hardware Universe の略"](#)。

## 例 8. 手順

### System Manager の略

ONTAP System Manager（9.7以降）でNVMe用のStorage VMを設定します。

新しい <b>Storage VM</b> に <b>NVMe</b> を設定してください	既存の <b>Storage VM</b> に <b>NVMe</b> を設定
<ol style="list-style-type: none"><li>1. System Managerで、* Storage &gt; Storage VM* をクリックし、* Add *をクリックします。</li><li>2. Storage VMの名前を入力してください。</li><li>3. アクセスプロトコル*として「* nvme」を選択します。</li><li>4. 「* NVMe/FCを有効にする」または「* NVMe/FCを有効にする」および「*保存」を選択します。</li></ol>	<ol style="list-style-type: none"><li>1. System Manager で、* Storage &gt; Storage VM* をクリックします。</li><li>2. 設定するStorage VMをクリックします。</li><li>3. [設定]タブをクリックし、をクリックします  をクリックします。</li><li>4. 「* NVMe/FCを有効にする」または「* NVMe/FCを有効にする」および「*保存」を選択します。</li></ol>

### CLI の使用

ONTAP CLIを使用して、NVMe用のStorage VMを設定します。

1. 既存の SVM を使用しない場合は、作成します。

```
vserver create -vserver <SVM_name>
```

- a. SVM が作成されたことを確認します。

```
vserver show
```

2. クラスタに NVMe または TCP 対応アダプタがインストールされていることを確認します。

NVMeの場合：

```
network fcp adapter show -data-protocols-supported fc-nvme
```

TCPの場合：

```
network port show
```

3. ONTAP 9.7 以前を実行している場合は、SVM からすべてのプロトコルを削除します。

```
vserver remove-protocols -vserver <SVM_name> -protocols  
iscsi,fcp,nfs,cifs,ndmp
```



ONTAP 9.8 以降では、NVMe を追加するときに他のプロトコルを削除する必要はありません。

4. SVM に NVMe プロトコルを追加します。

```
vserver add-protocols -vserver <SVM_name> -protocols nvme
```

5. ONTAP 9.7 以前を実行している場合は、SVM で許可されているプロトコルが NVMe だけであることを確認します。

```
vserver show -vserver <SVM_name> -fields allowed-protocols
```

に表示されるプロトコルはNVMeのみです `allowed protocols` 列 (Column) :

6. NVMe サービスを作成します。

```
vserver nvme create -vserver <SVM_name>
```

7. NVMe サービスが作成されたことを確認します。

```
vserver nvme show -vserver <SVM_name>
```

。 Administrative Status SVMのがと表示されている必要があります `up`。

8. NVMe/FC LIF を作成します。

◦ ONTAP 9.9.1以前の場合、FC :

```
network interface create -vserver <SVM_name> -lif <lif_name>  
-role data -data-protocol fc-nvme -home-node <home_node> -home  
-port <home_port>
```

◦ ONTAP 9.10.1以降、FCまたはTCPの場合 :

```
network interface create -vserver <SVM_name> -lif <lif_name>  
-service-policy <default-data-nvme-tcp | default-data-nvme-fc>  
-data-protocol <fcp | fc-nvme | nvme-tcp> -home-node <home_node>  
-home-port <home_port> -status-admin up -failover-policy disabled  
-firewall-policy data -auto-revert false -failover-group  
<failover_group> -is-dns-update-enabled false
```

9. HA パートナーノードに NVMe/FC LIF を作成します。

- ONTAP 9.9.1以前の場合、FC：

```
network interface create -vserver <SVM_name> -lif <lif_name>
-role data -data-protocol fc-nvme -home-node <home_node> -home
-port <home_port>
```

- ONTAP 9.10.1以降、FCまたはTCPの場合：

```
network interface create -vserver <SVM_name> -lif <lif_name>
-service-policy <default-data-nvme-tcp | default-data-nvme-fc>
-data-protocol <fcp | fc-nvme | nvme-tcp> -home-node <home_node>
-home-port <home_port> -status-admin up -failover-policy disabled
-firewall-policy data -auto-revert false -failover-group
<failover_group> -is-dns-update-enabled false
```

10. NVMe/FC LIF が作成されたことを確認します。

```
network interface show -vserver <SVM_name>
```

11. LIF と同じノードにボリュームを作成します。

```
vol create -vserver <SVM_name> -volume <vol_name> -aggregate
<aggregate_name> -size <volume_size>
```

自動効率化ポリシーに関する警告メッセージが表示された場合は無視してかまいません。

## NVMe ストレージをプロビジョニングする

次の手順に従って、既存のStorage VMでNVMe対応ホスト用のネームスペースを作成し、ストレージをプロビジョニングします。

ONTAP 9.8 以降では、ストレージをプロビジョニングすると QoS がデフォルトで有効になります。QoS を無効にするか、プロビジョニングプロセス中またはあとからカスタムの QoS ポリシーを選択できます。

作業を開始する前に

Storage VM が NVMe 用に設定され、FC または TCP 転送がすでにセットアップされている必要があります。

## System Manager の略

ONTAP System Manager (9.7以降) を使用して、NVMeプロトコルを使用してストレージを提供するネームスペースを作成します。

### 手順

1. System Manager で、 \* Storage > NVMe 名前空間 \* をクリックし、 \* Add \* をクリックします。

新しいサブシステムを作成する必要がある場合は、 \* その他のオプション \* をクリックします。

2. ONTAP 9.8 以降を実行していて、QoS を無効にする場合やカスタムの QoS ポリシーを選択する場合は、「その他のオプション」をクリックし、「 \* ストレージおよび最適化 \* 」で「 \* パフォーマンスサービスレベル \* 」を選択します。
3. FC スイッチを WWPN でゾーニングイニシエータごとに 1 つのゾーンを使用し、各ゾーンにすべてのターゲットポートを含めます。
4. ホストで、新しいネームスペースを検出します。
5. ネームスペースを初期化し、ファイルシステムでフォーマットします。
6. ホストがネームスペースに対してデータの書き込みと読み取りを実行できることを確認します。

### CLI の使用

ONTAP のCLIを使用して、NVMeプロトコルを使用してストレージを提供するネームスペースを作成します。

この手順 は、NVMeプロトコル用に設定済みの既存のStorage VMにNVMeネームスペースとサブシステムを作成し、ネームスペースをサブシステムにマッピングしてホストシステムからのデータアクセスを許可します。

NVMe用にStorage VMを設定する必要がある場合は、を参照してください ["NVMe 用に SVM を設定します"](#)。

### 手順

1. SVM が NVMe 用に設定されていることを確認します。

```
vserver show -vserver <svm_name> -fields allowed-protocols
```

NVMe がの下に表示されます allowed-protocols 列 (Column) :

2. NVMe ネームスペースを作成します。

```
vserver nvme namespace create -vserver <svm_name> -path <path> -size  
<size_of_namespace> -ostype <OS_type>
```

3. NVMe サブシステムを作成します。

```
vserver nvme subsystem create -vserver <svm_name> -subsystem  
<name_of_subsystem> -ostype <OS_type>
```

NVMe サブシステムの名前では大文字と小文字が区別されます。1~96文字で指定する必要があります。特殊文字を使用できます。

4. サブシステムが作成されたことを確認します。

```
vserver nvme subsystem show -vserver <svm_name>
```

。 nvme の下にサブシステムが表示されます Subsystem 列 (Column) :

5. ホストから NQN を取得します。
6. ホストの NQN をサブシステムに追加します。

```
vserver nvme subsystem host add -vserver <svm_name> -subsystem  
<subsystem_name> -host-nqn <Host_NQN>
```

7. ネームスペースをサブシステムにマッピングします。

```
vserver nvme subsystem map add -vserver <svm_name> -subsystem  
<subsystem_name> -path <path>
```

ネームスペースは、1つのサブシステムにのみマッピングできます。

8. ネームスペースがサブシステムにマッピングされていることを確認します。

```
vserver nvme namespace show -vserver <svm_name> -instance
```

サブシステムがと表示されます Attached subsystem。

## NVMe ネームスペースをサブシステムにマッピングする

NVMeネームスペースをサブシステムにマッピングすると、ホストからのデータアクセスが可能になります。NVMeネームスペースは、ストレージのプロビジョニング時にサブシステムにマッピングすることも、ストレージのプロビジョニング後にマッピングすることもできます。

ONTAP 9.14.1以降では、特定のホストに対するリソース割り当てに優先順位を付けることができます。デフォルトでは、NVMeサブシステムに追加されたホストには標準優先度が与えられます。ONTAPのコマンドラインインターフェイス (CLI) を使用して、デフォルト優先度を手動で標準から高に変更できます。高い優先

度を割り当てられたホストには、より多くのI/Oキュー数とキュー深度が割り当てられます。



ONTAP 9.13.1以前でサブシステムに追加されたホストを高い優先度で指定するには、次の手順を実行します。 [ホスト優先度の変更](#)。

作業を開始する前に

ネームスペースとサブシステムはすでに作成されている必要があります。ネームスペースとサブシステムを作成する必要がある場合は、[を参照してください "NVMe ストレージをプロビジョニングする"](#)。

手順

1. ホストから NQN を取得します。
2. ホストの NQN をサブシステムに追加します。

```
vserver nvme subsystem host add -vserver <SVM_name> -subsystem  
<subsystem_name> -host-nqn <Host_NQN_:subsystem._subsystem_name>
```

ホストのデフォルト優先度をregularからhighに変更する場合は、`-priority high` オプションこのオプションは、ONTAP 9.14.1以降で使用できます。

3. ネームスペースをサブシステムにマッピングします。

```
vserver nvme subsystem map add -vserver <SVM_name> -subsystem  
<subsystem_name> -path <path>
```

ネームスペースは、1つのサブシステムにのみマッピングできます。

4. ネームスペースがサブシステムにマッピングされていることを確認します。

```
vserver nvme namespace show -vserver <SVM_name> -instance
```

サブシステムがと表示されます Attached subsystem。

## LUNを管理します

**LUN QoS** ポリシーグループを編集します

ONTAP 9.10.1 以降の System Manager を使用して、複数の LUN のサービス品質（QoS）ポリシーを同時に割り当てたり削除したりできます。



QoSポリシーがボリュームレベルで割り当てられている場合は、ボリュームレベルで変更する必要があります。QoS ポリシーは、もともと LUN レベルで割り当てられていた場合にのみ、LUN レベルで編集できます。

手順

1. System Manager で、 \* Storage > LUNs \* をクリックします。

2. 編集する LUN を選択します。

一度に複数の LUN を編集する場合は、その LUN が同じ Storage Virtual Machine （ SVM ） に属している必要があります。同じ SVM に属していない LUN を選択した場合は、 QoS ポリシーグループを編集するオプションは表示されません。

3. [ \* その他 \* ] をクリックし、 [ \* QoS ポリシーグループの編集 \* ] を選択します。

#### LUNをネームスペースに変換します

ONTAP 9.11.1以降では、ONTAP CLIを使用して、既存のLUNをNVMeネームスペースにインプレース変換できます。

#### 必要なもの

- 指定したLUNには、igroupにマッピングされている既存のLUNを含めることはできません。
- MetroCluster が設定されたSVM内やSM-BC関係にあるLUNは使用できません。
- LUNをプロトコルエンドポイントにしたり、プロトコルエンドポイントにバインドしたりすることはできません。
- LUNにゼロ以外のプレフィックスやサフィックスストリームを含めることはできません。
- LUNをSnapshotの一部にしたり、SnapMirror関係のデスティネーション側に読み取り専用LUNとして配置したりすることはできません。

#### ステップ

1. LUNをNVMeネームスペースに変換します。

```
vserver nvme namespace convert-from-lun -vserver -lun-path
```

#### LUN をオフラインにします

ONTAP 9.10.1 以降の場合、 System Manager を使用して LUN をオフラインにできます。ONTAP 9.10.1 より前のバージョンでは、 ONTAP CLI を使用して LUN をオフラインにする必要があります。

## System Manager の略

### 手順

1. System Manager で、 \* Storage > LUNs \* をクリックします。
2. 1 つまたは複数の LUN をオフラインにします

実行する処理	操作
単一の LUN をオフラインにします	LUN 名の横にある をクリックします。 をクリックし、 * オフラインにする * を選択します。
複数の LUN をオフラインにします	<ol style="list-style-type: none"><li>1. オフラインにする LUN を選択します。</li><li>2. 「 * 詳細」 をクリックし、 「 * オフラインにする * 」 を選択します。</li></ol>

### CLI の使用

CLI を使用する場合、一度にオフラインにできる LUN は 1 つだけです。

### ステップ

1. LUN をオフラインにします。

```
lun offline <lun_name> -vserver <SVM_name>
```

## LUN のサイズを変更します

LUN のサイズは増やすことも減らすこともできます。



Solaris LUN のサイズは変更できません。

### LUN のサイズを拡張する

LUN の拡張後のサイズは、ONTAP のバージョンによって異なります。

ONTAPバージョン	LUN の最大サイズ
ONTAP 9.12.1P2以降	AFF、FAS、ASAプラットフォームの場合は128TB
ONTAP 9.8以降	<ul style="list-style-type: none"><li>• オールフラッシュSANアレイ（ASA）プラットフォームの場合は128TB</li><li>• ASA以外のプラットフォームの場合は16TB</li></ul>
ONTAP 9.5、9.6、9.7	16TB

ONTAP 9.4 以前	<p>元のLUNサイズの10倍ですが、最大LUNサイズである16TBを超えることはありません。</p> <p>たとえば、100GBで作成したLUNは1、000GBまでしか拡張できません。</p> <p>LUNの実際の最大サイズが正確に16TBであるとは限りません。ONTAP では、制限値の端数が切り捨てられます。</p>
--------------	---


サイズを拡張するときに、LUN をオフラインにする必要はありません。ただし、サイズを拡張したあとでホストがサイズの変更を認識するには、ホスト上の LUN を再スキャンする必要があります。

のコマンドリファレンスページを参照してください `lun resize` コマンドを使用してLUNのサイズ変更の詳細を確認してください。

## 例 9. 手順

### System Manager の略

ONTAP System Managerを使用してLUNのサイズを拡張する（9.7以降）。

1. System Manager で、 \* Storage > LUNs \* をクリックします。
2. をクリックします  をクリックし、 \* Edit \* を選択します。
3. Storage and Optimization では、**LUN**のサイズが拡張され、 Save \*が表示されます。

### CLI の使用

ONTAP CLIを使用してLUNのサイズを拡張する。

1. LUN のサイズを拡張します。

```
lun resize -vserver <SVM_name> -volume <volume_name> -lun <lun_name>
-size <lun_size>
```

2. 拡張した LUN のサイズを確認します。

```
lun show -vserver <SVM_name_>
```

ONTAP の処理では、LUN の実際の最大サイズが端数を切り捨てられるため、想定値よりも少し小さくなります。また、LUN の実際のサイズは、LUN の OS タイプによって多少異なります。サイズの正確な値を取得するには、advanced モードで次のコマンドを実行します。

```
set -unit B
```

```
lun show -fields max-resize-size -volume volume_name -lun lun_name
```



1. ホスト上の LUN を再スキャンします。
2. ホストのマニュアルに従って、新しく作成した LUN のサイズをホストファイルシステムに認識させます。

#### LUN のサイズを縮小します

LUN のサイズを縮小する前に、ホストが LUN データを含むブロックを小さい LUN サイズの境界に移行する必要があります。LUN データを含むブロックを切り捨てずに LUN を適切に縮小するには、SnapCenterなどのツールを使用する必要があります。LUN のサイズを手動で縮小することは推奨されません。

LUN のサイズを縮小すると、サイズが縮小されたことが ONTAP からイニシエータに自動的に通知されます。ただし、ホストが新しい LUN サイズを認識するには、ホストで追加の手順が必要になる場合があります。ホストのファイル構造のサイズの縮小に固有の情報については、ホストのマニュアルを参照してください。

#### LUN を移動します

Storage Virtual Machine （SVM）内のボリューム間で LUN を移動できますが、SVM 間で LUN を移動することはできません。SVM 内のボリューム間で移動される LUN はただちに移動され、接続が失われることはありません。

#### 必要なもの

LUN で Selective LUN Map（SLM；選択的 LUN マップ）を使用している場合は、["SLM レポート ノード リストの変更"](#) LUN を移動する前に、デスティネーション ノードとその HA パートナーを追加します。

#### このタスクについて

重複排除、圧縮、コンパクションなどの Storage Efficiency 機能は、LUN の移動時には保持されません。これらは、LUN の移動の完了後に再適用する必要があります。

Snapshot コピーによるデータ保護はボリュームレベルで行われます。そのため、移動した LUN にはデスティネーション ボリュームのデータ保護形式が適用されます。デスティネーション ボリューム用の Snapshot コピーが確立されていない場合、LUN の Snapshot コピーは作成されません。また、LUN のすべての Snapshot コピーは、これらの Snapshot コピーが削除されないかぎり、元のボリュームに保持されます。

次のボリュームに LUN を移動することはできません。

- SnapMirror デスティネーション ボリューム
- SVM ルート ボリューム

次のタイプの LUN は移動できません。

- ファイルから作成された LUN
- NVFail 状態の LUN
- 負荷共有関係にある LUN
- プロトコル エンドポイント クラスの LUN



サイズが 1TB 以上で os\_type が Solaris の LUN では、LUN の移動時にホストでタイムアウトが発生する場合があります。このタイプの LUN では、移動を開始する前に LUN をアンマウントする必要があります。


## 例 10. 手順

### System Manager の略

ONTAP System Manager (9.7以降) を搭載したLUNを移動します。

ONTAP 9.10.1 以降では、単一の LUN を移動するときに System Manager で新しいボリュームを作成できます。ONTAP 9.8 および 9.9.8.1 では、LUN の移動を開始する前に、LUN の移動先のボリュームが存在している必要があります。

#### 手順

1. System Manager で、\* Storage > LUNs \* をクリックします。
2. 移動するLUNを右クリックし、 をクリックし、\* LUN の移動 \* を選択します。

ONTAP 9.10.1 では、LUN を既存のボリューム \* または新しいボリューム \* に移動するように選択します。

新しいボリュームを作成する場合は、ボリュームの仕様を指定します。

3. [ 移動 ( Move ) ] をクリックします。

### CLI の使用

ONTAP CLIを使用してLUNを移動します。

1. LUN を移動します。

```
lun move start
```

ごく短時間、移動した LUN が元のボリュームと移動後のボリュームの両方に表示されます。これは移動が完了するまでの一時的な状態で、想定内の動作です。

2. 移動のステータスを追跡し、正常に完了したことを確認します。

```
lun move show
```

## 関連情報

- ["選択的 LUN マップ"](#)

## LUN を削除します

不要になった LUN は Storage Virtual Machine ( SVM ) から削除できます。

必要なもの

LUN を削除する前に、その igroup から LUN のマッピングを解除する必要があります。

手順

1. アプリケーションやホストが LUN を使用していないことを確認します。
2. igroup から LUN のマッピングを解除します。

```
lun mapping delete -vserver <SVM_name> -volume <volume_name> -lun  
<LUN_name> -igroup <igroup_name>
```

3. LUNを削除します。

```
lun delete -vserver <SVM_name> -volume <volume_name> -lun <LUN_name>
```

4. LUNが削除されたことを確認します。

```
lun show -vserver <SVM_name>
```

Vserver	Path	State	Mapped	Type	Size
vs5	/vol/vol16/lun8	online	mapped	windows	10.00GB

**LUNをコピーする前に理解しておくべきこと**

**LUNをコピーする前に、次の点に注意してください。**

クラスタ管理者は、を使用して、クラスタ内のStorage Virtual Machine (SVM) 間でLUNをコピーできます lun copy コマンドを実行しますクラスタ管理者は、を使用してStorage Virtual Machine (SVM) ピア関係を確立する必要があります vsserver peer create SVM間のLUNコピー処理を実行する前のコマンド。ソースボリューム内に SIS クローン用の十分なスペースが必要です。

Snapshotコピー内のLUNをのソースLUNとして使用できます lun copy コマンドを実行しますを使用してLUNをコピーする場合 lun copy コマンドを実行すると、LUNコピーの読み取りと書き込みがすぐに可能になります。LUN コピーの作成によってソース LUN が変更されることはありません。ソース LUN と LUN コピーは、LUN シリアル番号の異なる一意の LUN として存在します。ソース LUN に対する変更は LUN コピーに反映されず、LUN コピーに対する変更はソース LUN に反映されません。ソース LUN の LUN マッピングは新しい LUN にコピーされないため、LUN コピーをマッピングする必要があります。

Snapshot コピーによるデータ保護はボリュームレベルで行われます。そのため、ソース LUN のボリュームとは異なるボリュームに LUN をコピーする場合、デスティネーション LUN にはデスティネーションボリュームのデータ保護形式が適用されます。デスティネーションボリューム用の Snapshot コピーが確立されていない場合、LUN コピーの Snapshot コピーは作成されません。

LUN のコピーはノンストップオペレーションです。

次の種類の LUN はコピーできません。

- ファイルから作成された LUN
- NVFAIL 状態の LUN
- 負荷共有関係にある LUN
- プロトコルエンドポイントクラスの LUN

**LUN** の設定済みスペースと使用済みスペースを確認します

LUN の設定済みスペースと実際に使用されているスペースを把握しておく、スペース再生時に再生可能なスペースの量、データを含むリザーブスペースの量、および LUN の設定済みの合計サイズと実際に使用されているサイズを特定するのに役立ちます。

ステップ

1. LUN の設定済みスペースと実際に使用されているスペースを表示します。

```
lun show
```

次の例は、vs3 という Storage Virtual Machine (SVM) 内の LUN の設定済みスペースと実際に使用されているスペースを示しています。

```
lun show -vserver vs3 -fields path, size, size-used, space-reserve
```

vserver	path	size	space-reserve	size-used
vs3	/vol/vol0/lun1	50.01GB	disabled	25.00GB
vs3	/vol/vol0/lun1_backup	50.01GB	disabled	32.15GB
vs3	/vol/vol0/lun2	75.00GB	disabled	0B
vs3	/vol/volspace/lun0	5.00GB	enabled	4.50GB

4 entries were displayed.

**SCSI シンプロビジョニング LUN** のスペース割り当てを有効にします

SCSI シンプロビジョニングがホストでサポートされている場合は、ONTAP で SCSI シンプロビジョニング LUN のスペース割り当てを有効にすることができます。スペース割り当てを有効にすると、ボリュームのスペースが不足し、ボリューム内の LUN が書き込みを受け付けられなくなったときに、ONTAP からホストに通知されます。ONTAP は、ホストでデータが削除されたときにも自動的にスペースを再生します。

SCSI シンプロビジョニングをサポートしないホスト上では、LUN が含まれているボリューム内のスペースが不足し自動拡張できなくなったときに、ONTAP によってその LUN はオフラインになります。SCSI シンプロビジョニングをサポートするホストでは、スペースが不足しても ONTAP は LUN をオフラインにしません。LUN は読み取り専用モードでオンライン状態を維持し、LUN が書き込みを受け付けられなくなったことがホストに通知されます。

また、SCSI シンプロビジョニングをサポートするホストでデータが削除されると、ホスト側のスペース管理

によって、ホストファイルシステムで削除されたデータのブロックが識別され、自動的に1つ以上の SCSI UNMAP ストレージシステム上の対応するブロックを解放するコマンド。

作業を開始する前に

スペース割り当てを有効にするには、SCSIシンプロビジョニングがホストでサポートされている必要があります。SCSIシンプロビジョニングは、SCSI SBC-3標準で定義されている論理ブロックプロビジョニングを使用します。この標準をサポートするホストだけが、ONTAP の SCSI シンプロビジョニングを使用できます。

現在、スペース割り当てを有効にした場合の SCSI シンプロビジョニングに対応しているホストは次のとおりです。

- Citrix XenServer 6.5以降
- ESXi 5.0以降
- Oracle Linux 6.2 UEKカーネル以降
- RHEL 6.2以降
- SLES11以降
- Solaris 11.1以降
- Windows の場合

このタスクについて

デフォルトでは、スペース割り当てはすべてのLUNに対して無効になっています。LUNをオフラインにしてスペース割り当てを有効にしてから、ホストがスペース割り当てが有効になったことを認識するには、ホストで検出を実行する必要があります。

手順

1. LUNをオフラインにします。

```
lun modify -vserver vservice_name -volume volume_name -lun lun_name
-state offline
```

2. スペース割り当てを有効にします。

```
lun modify -vserver _vservice_name_ -volume _volume_name_ -lun _lun_name_
-space-allocation enabled
```

3. スペース割り当てが有効になっていることを確認します。

```
lun show -vserver _vservice_name_ -volume _volume_name_ -lun _lun_name_
-fields space-allocation
```

4. LUN をオンラインにします。

```
lun modify -vserver _vserver_name_ -volume _volume_name_ -lun _lun_name_  
-state online
```

5. ホストですべてのディスクを再スキャンして、が変更されたことを確認します -space-allocation オプションが正しく検出されました。

**LUN** に対する **I/O** パフォーマンスは、ストレージ **QoS** を使用して制御および監視できます

LUN への入出力（I/O）パフォーマンスは、LUN をストレージ QoS ポリシーグループに割り当てることによって制御できます。I/O パフォーマンスを制御することで、ワークロードが特定のパフォーマンス目標を達成できるようにしたり、他のワークロードに悪影響を与えるワークロードを抑制したりできます。

このタスクについて

ポリシーグループは最大スループット制限（100MB/s など）を適用します。ポリシーグループは最大スループットを指定せずに作成することもでき、ワークロードの制御に先立ってパフォーマンスを監視できます。

FlexVol および LUN が含まれている Storage Virtual Machine（SVM）をポリシーグループに割り当てることもできます。

ポリシーグループへの LUN の割り当てについては、次の要件に注意してください。

- LUN は、ポリシーグループが属する SVM に含まれている必要があります。
- SVM は、ポリシーグループを作成するときに指定します。
- LUN をポリシーグループに割り当てた場合、その LUN を含むボリュームまたは SVM をポリシーグループに割り当てることはできなくなります。

ストレージ QoS の使用方法の詳細については、を参照してください ["システムアドミニストレーションリファレンス"](#)。

手順

1. を使用します qos policy-group create コマンドを使用してポリシーグループを作成します。
2. を使用します lun create コマンドまたはを実行します lun modify コマンドにを指定します -qos -policy-group LUNをポリシーグループに割り当てるためのパラメータ。
3. を使用します qos statistics パフォーマンスデータを表示するためのコマンド。
4. 必要に応じて、を使用します qos policy-group modify コマンドを使用してポリシーグループの最大スループット制限を調整します。

**LUN** を効果的に監視するためのツール

LUN を効果的に監視し、スペース不足になるのを防ぐためのツールが用意されています。

- Active IQ Unified Manager は、環境内のすべてのクラスタのすべてのストレージを管理するための無償ツールです。

- System Manager は、ONTAP に組み込まれているグラフィカルユーザーインターフェイスです。クラスターレベルに必要なストレージを手動で管理できます。
- OnCommand Insight を使用すると、ストレージインフラの状況を一元的に確認できます。また、自動監視やアラートの機能、および LUN、ボリューム、アグリゲートでストレージスペース不足が発生したときにレポートする機能を設定できます。

## 移行した LUN の機能と制限

SAN 環境では、7-Mode ボリュームを ONTAP に移行する際にサービスの中断が必要です。移行を完了するには、ホストをシャットダウンする必要があります。移行後は、ホスト構成を更新してから、ONTAP でデータの提供を開始する必要があります

ホストをシャットダウンできる時間帯にメンテナンスのスケジュールを設定して、移行を完了する必要があります。

Data ONTAP 7-Mode から ONTAP に移行された LUN には、LUN の管理方法に影響を及ぼす特定の機能と制限があります。

移行した LUN では、次の操作を実行できます。

- を使用して LUN を表示します `lun show` コマンドを実行します
- を使用して、7-Mode ボリュームから移行した LUN のインベントリを表示します `transition 7-mode show` コマンドを実行します
- 7-Mode Snapshot コピーからボリュームをリストアします

ボリュームをリストアすると、Snapshot コピーにキャプチャされたすべての LUN が移行されます

- を使用して、7-Mode Snapshot コピーから単一の LUN をリストアします `snapshot restore-file` コマンドを実行します
- 7-Mode Snapshot コピー内の LUN のクローンを作成します
- 7-Mode Snapshot コピーにキャプチャされた LUN から特定の範囲のブロックをリストアする
- 7-Mode Snapshot コピーを使用して、ボリュームの FlexClone を作成します

移行した LUN では、次の操作を実行することはできません。

- ボリューム内にキャプチャされた Snapshot コピーでバックアップされた LUN クローンにアクセスします

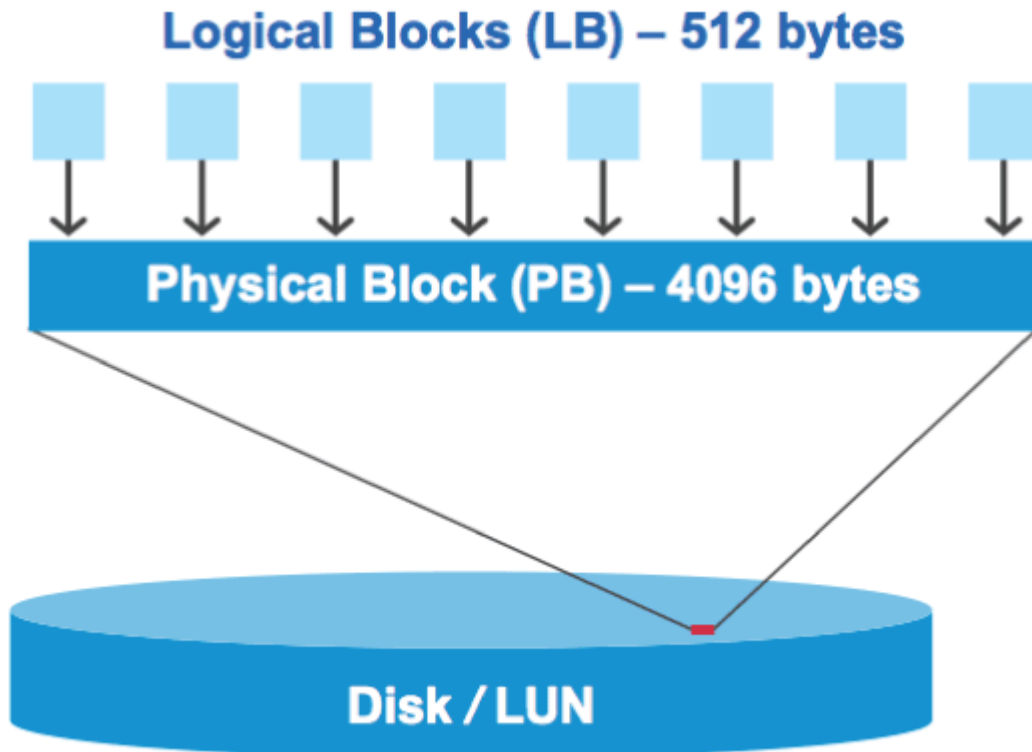
## 関連情報

["コピーベースの移行"](#)

## 適切にアライメントされた LUN における I/O のミスアライメントの概要

ONTAP では、適切にアライメントされた LUN における I/O のミスアライメントが報告されることがあります。一般に、このようなミスアライメントの警告は、LUN が適切にプロビジョニングされていて、パーティションテーブルが適正であることに確信があれば無視してかまいません。

LUN とハードディスクはどちらもストレージをブロックとして提供します。ホスト上のディスクのブロックサイズは 512 バイトなので、LUN はそのサイズのブロックをホストに提供しますが、実際はよりサイズの大きい 4KB のブロックを使用してデータを格納します。ホストで使用される 512 バイトのデータブロックは論理ブロックと呼ばれ、LUN がデータの格納に使用する 4KB のデータブロックは物理ブロックと呼ばれます。つまり、4KB の各物理ブロックに 512 バイトの論理ブロックが 8 個あります。



ホストオペレーティングシステムは、任意の論理ブロックで読み取りまたは書き込みの I/O 処理を開始できます。I/O 処理がアライメントされているとみなされるのは、I/O 処理が物理ブロック内の最初の論理ブロックで開始される場合のみです。I/O 処理が物理ブロックの最初の論理ブロック以外のブロックで開始される場合は、I/O がミスアライメントされているとみなされます。ONTAP は、LUN におけるミスアライメントを自動検出して報告します。ただし、ミスアライメント I/O が検出されたからといって、LUN もミスアライメントされているとは限りません。適切にアライメントされた LUN でも、ミスアライメント I/O が報告される場合があります。

さらに調査が必要な場合は、Knowledge Baseの記事を参照してください ["LUNのミスアライメントされたIOを特定する方法"](#)

アライメントの問題を修正するためのツールの詳細については、+ を参照してください

- ["Windows Unified Host Utilities 7.1"](#)
- ["Virtual Storage Console for VMware vSphere インストレーションアドミニストレーションガイド"](#)

**LUN の OS タイプを使用して I/O アライメントを実行する**

ONTAP 9.7以前では、推奨されるONTAP LUNを使用する必要があります。ostype OSパーティショニングスキームとのI/Oアライメントを実現するために、オペレーティングシステムに最も近い値。

ホスト OS で採用されるパーティショニングスキームは I/O のミスアライメントの大きな要因です。一部のONTAP LUN ostype 値は、ホストオペレーティングシステムがアライメントするデフォルトのパーティシ



ヨニングスキームを有効にするために、「プレフィックス」と呼ばれる特別なオフセットを使用します。



場合によっては、I/O アライメントを実行するためにカスタムパーティションテーブルが必要になることがあります。ただし、の場合 `ostype "prefix"` の値がより大きい値 `0` カスタムパーティションを使用すると、ミスアライメントI/Oが発生する可能性があります。

ONTAP 9.7以前でプロビジョニングされたLUNの詳細については、技術情報アートを参照してください。"[LUNでアライメントされていないIOを特定する方法](#)"。



ONTAP 9.8以降でプロビジョニングされる新しいLUNには、すべてのLUN OSタイプでプレフィックスとサフィックスサイズが0に設定されます。I/Oは、デフォルトでサポートされるホストOSとアライメントされている必要があります。

**Linux 固有の I/O アライメントに関する注意事項があります**

Linux ディストリビューションでは、データベース、各種ボリュームマネージャ、ファイルシステム用の raw デバイスなど、さまざまな方法で LUN を使用できます。raw デバイスまたは論理ボリューム内の物理ボリュームとして使用する場合は、LUN にパーティションを作成する必要はありません。

RHEL 5 以前および SLES 10 以前の場合、ボリュームマネージャを使用せずに LUN を使用する場合は、LUN をパーティショニングして、アライメントされたオフセットから始まる 1 つのパーティションを設定する必要があります。これは、8 つの論理ブロックの偶数の倍数であるセクターです。

**Solaris LUN 固有の I/O アライメントに関する注意事項があります**

を使用するかどうかを決定する際には、さまざまな要因を考慮する必要があります `solaris ostype` または `solaris_efi ostype`

を参照してください "[Solaris Host Utilities Installation and Administration Guide](#)" を参照してください。

**ESX ブート LUN はミスアライメントとしてレポートされます**

ESX ブート LUN として使用される LUN は通常、ミスアライメントとして ONTAP から報告されます。ESX は、ブート LUN 上に複数のパーティションを作成するため、アライメントが非常に困難です。ミスアライメント I/O の合計容量は小さいため、ミスアライメントされた ESX ブート LUN は通常、パフォーマンス上の問題を生じません。VMwareでLUNが正しくプロビジョニングされていることを前提とします `ostype` アクションは必要ありません。

関連情報

"[VMware vSphere、その他の仮想環境、およびネットアップストレージシステム用のゲスト VM ファイルシステムのパーティションとディスクのアライメント](#)"

**LUN がオフラインになった場合の問題への対処方法**

書き込みに使用できるスペースがない場合、LUN はデータの整合性を保持するためにオフラインになります。LUN がスペース不足やオフラインになる原因はさまざまですが、いくつかの方法で問題に対処できます。

状況	可能です
アグリゲートがいっぱいです	<ul style="list-style-type: none"> <li>• ディスクを追加します。</li> <li>• を使用します <code>volume modify</code> 使用可能なスペースがあるボリュームを縮小するコマンド。</li> <li>• 使用可能なスペースがあるスペースギャランティボリュームがある場合は、ボリュームのスペースギャランティをに変更します <code>none</code> を使用 <code>volume modify</code> コマンドを実行します</li> </ul>
ボリュームがフルの状態であるが、包含アグリゲートに利用可能なスペースがある	<ul style="list-style-type: none"> <li>• スペースギャランティボリュームの場合は、を使用します <code>volume modify</code> コマンドを使用してボリュームのサイズを拡張します。</li> <li>• シンプロビジョニングボリュームの場合は、を使用します <code>volume modify</code> コマンドを使用して、ボリュームの最大サイズを拡張します。</li> </ul> <p>ボリュームの自動拡張が有効になっていない場合は、を使用します <code>volume modify -autogrow -mode</code> 有効にします。</p> <ul style="list-style-type: none"> <li>• を使用して、Snapshotコピーを手動で削除します <code>volume snapshot delete</code> コマンドを入力するか、を使用します <code>volume snapshot autodelete modify</code> Snapshotコピーを自動的に削除するコマンド。</li> </ul>

#### 関連情報

["ディスクとローカル階層（アグリゲート）の管理"](#)

["論理ストレージ管理"](#)

ホストで **iSCSI LUN** が表示されない場合のトラブルシューティング

ホストでは、iSCSI LUN がローカルディスクとして表示されます。ストレージシステムの LUN をホストがディスクとして使用できない場合は、構成設定を確認してください。

設定	対処方法：
ケーブル配線	ホストとストレージシステムの間のケーブルが適切に接続されていることを確認します。

設定	対処方法：
ネットワーク接続	<p>ホストとストレージシステムの間に TCP / IP 接続が確立されていることを確認します。</p> <ul style="list-style-type: none"> <li>• ストレージシステムのコマンドラインから、iSCSI に使用されているホストインターフェイスを ping します。</li> </ul> <pre>ping -node node_name -destination host_ip_address_for_iSCSI</pre> <ul style="list-style-type: none"> <li>• ホストのコマンドラインから、iSCSI に使用されているストレージシステムインターフェイスを ping します。</li> </ul> <pre>ping -node node_name -destination host_ip_address_for_iSCSI</pre>
システム要件	各構成コンポーネントが、認定された製品であることを確認します。ホスト OS のサービスパックレベル、イニシエータバージョン、ONTAP バージョンなどのシステム要件を満たしていることも確認してください。Interoperability Matrix に最新のシステム要件が記載されています。
ジャンボフレーム	構成でジャンボフレームを使用している場合は、ネットワークパス内のすべてのデバイスでジャンボフレームが有効になっていることを確認します。ホストイーサネット NIC、ストレージシステム、およびすべてのスイッチです。
iSCSI サービスのステータス	iSCSI サービスのライセンスがあり、ストレージシステムで開始されていることを確認します。
イニシエータログイン	イニシエータがストレージシステムにログインしていることを確認します。状況に応じて <code>iscsi initiator show</code> コマンド出力にログインしているイニシエータが表示されないため、ホストのイニシエータ設定をチェックしてください。イニシエータのターゲットとしてストレージシステムが設定されていることも確認してください。
iSCSI ノード名 (IQN)	正しいイニシエータのノード名を <code>igroup</code> 設定で使用していることを確認します。イニシエータのツールおよびコマンドをホストで使用し、イニシエータのノード名を表示できます。 <code>igroup</code> およびホストで設定したイニシエータのノード名は、互いに一致する必要があります。
LUN マッピング	<p>LUN が <code>igroup</code> にマッピングされていることを確認します。ストレージ・システムのコンソールで、次のいずれかのコマンドを使用できます。</p> <ul style="list-style-type: none"> <li>• <code>lun mapping show</code> すべてのLUN、およびLUNがマッピングされている <code>igroup</code> を表示します。</li> <li>• <code>lun mapping show -igroup</code> 特定の <code>igroup</code> にマッピングされているLUNを表示します。</li> </ul>

設定	対処方法：
iSCSI LIF が有効になります	iSCSI 論理インターフェイスが有効になっていることを確認する。

#### 関連情報

["NetApp Interoperability Matrix Tool で確認できます"](#)

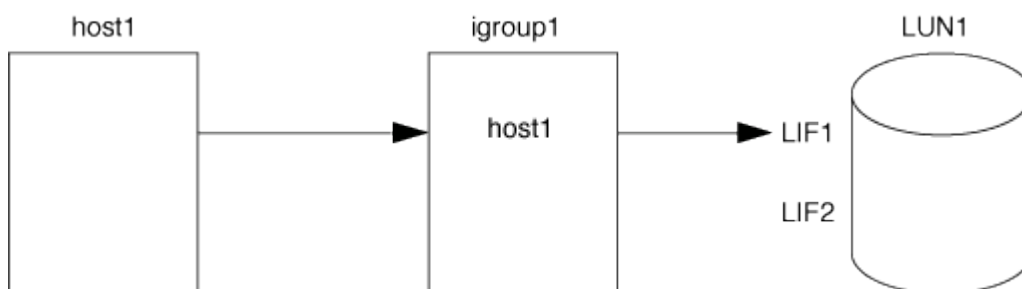
## igroupとポートセットを管理します

ポートセットと**igroup**によって**LUN**アクセスを制限する方法

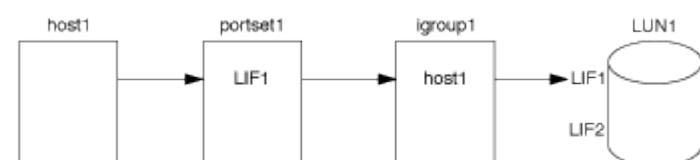
Selective LUN Map (SLM；選択的なLUNマップ) に加えて、igroupおよびポートセットを使用してLUNへのアクセスを制限することもできます。

ポートセットとSLMを併用すると、特定のターゲットのアクセスを特定のイニシエータのみに制限できます。SLM とポートセットを併用する場合、LUN には、その LUN を所有するノードおよびノードの HA パートナーのポートセットに含まれる一連の LIF 経由でアクセス可能になります。

次の例で、initiator1にはポートセットがありません。ポートセットがない場合、initiator1はLIF1とLIF2の両方を經由してLUN1にアクセスできます。



ポートセットを使用すると、LUN1へのアクセスを制限できます。次の例では、initiator1 は LIF1 経由でのみ LUN1 にアクセスできます。ただし、LIF2はportset1に含まれないため、LIF2経由でLUN1にアクセスすることはできません。



#### 関連情報

- [選択的 LUN マップ](#)
- [ポートセットを作成して igroup にバインドします](#)

## SANイニシエータとigroupを表示および管理します

System Managerを使用して、イニシエータグループ (igroup) とイニシエータを表示および管理できます。

このタスクについて

- イニシエータグループは、ストレージシステム上の特定のLUNにアクセスできるホストを識別します。
- イニシエータグループとイニシエータグループは、作成後に編集または削除することもできます。
- SANイニシエータグループとイニシエータを管理するには、次のタスクを実行します。
  - [\[view-manage-san-igroups\]](#)
  - [\[view-manage-san-inits\]](#)

**SANイニシエータグループを表示および管理します**

System Managerを使用して、イニシエータグループ (igroup) のリストを表示できます。 リストから追加の処理を実行できます。

手順

1. System Managerで、\* Hosts > SAN Initiator Groups \*をクリックします。

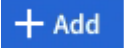
イニシエータグループ (igroup) のリストが表示されます。 リストが大きい場合は、ページの右下隅にあるページ番号をクリックすると、リストの追加ページを表示できます。

列には、igroupに関するさまざまな情報が表示されます。 9.11.1以降では、igroupの接続ステータスも表示されます。 ステータスアラートにカーソルを合わせると詳細が表示されます。


2. (オプション) : リストの右上にあるアイコンをクリックすると、次のタスクを実行できます。

- \* 検索 \*
- \*ダウンロード\*リスト。
- \*リストの\*または\*隠す\*列を表示します。
- \*リスト内のデータをフィルタリングします。

3. リストから操作を実行できます。

- をクリックします  をクリックしてigroupを追加します。
- igroup名をクリックすると、そのigroupの詳細が表示されます。 \* Overview \* ページが表示されます。

概要\*ページでは、igroupに関連付けられているLUNを確認できます。 また、処理を開始してLUNの作成やLUNのマッピングを行うこともできます。 「\*すべてのSANイニシエータ」をクリックしてメインリストに戻ります。

- igroupにカーソルを合わせ、をクリックします  をクリックしてigroupを編集または削除します。
- igroup名の左側の領域にカーソルを合わせ、チェックボックスをオンにします。 イニシエータグループに追加をクリックすると、そのigroupを別のigroupに追加できます。
- Storage VM \*列で、Storage VMの名前をクリックして詳細を確認します。

**SANイニシエータを表示および管理します**

System Managerを使用して、イニシエータのリストを表示できます。 リストから追加の処理を実行できます。

手順

1. System Managerで、\* Hosts > SAN Initiator Groups \*をクリックします。

イニシエータグループ (igroup) のリストが表示されます。

2. イニシエータを表示するには'次の手順に従います

- FCイニシエータの一覧を表示するには、\* FCイニシエータ\*タブをクリックします。
- iSCSIイニシエータのリストを表示するには、\* iSCSIイニシエータ\*タブをクリックします。

各列には、イニシエータに関するさまざまな情報が表示されます。

9.11.1以降では、イニシエータの接続ステータスも表示されます。ステータスアラートにカーソルを合わせると詳細が表示されます。

3. (オプション) : リストの右上にあるアイコンをクリックすると、次のタスクを実行できます。

- \* Search \* : 特定のイニシエータを一覧表示します。
- \*ダウンロード\*リスト。
- \*リストの\*または\*隠す\*列を表示します。
- \*リスト内のデータをフィルタリングします。

ネストされた**igroup**を作成する

ONTAP 9.9.1以降では、他の既存のigroupで構成されるigroupを作成できます。

1. System Manager で、\* Host > SAN Initiator Groups \* をクリックし、\* Add \* をクリックします。
2. igroup 名 \* と \* 概要 \* を入力します。

概要は igroup のエイリアスとして機能します。

3. Storage VM \* および \* Host Operating System \* を選択します。



ネストされた igroup の OS タイプは、igroup の作成後は変更できません。

4. イニシエータグループメンバー \* で、\* 既存のイニシエータグループ \* を選択します。
  - Search \* を使用して、追加する igroup を検索して選択できます。

**igroup** を複数の **LUN** にマッピングします

ONTAP 9.9.1以降では、igroupを複数のLUNに同時にマッピングできます。

1. System Manager で、\* Storage > LUNs \* をクリックします。
2. マッピングする LUN を選択します。
3. [\* 詳細 \*] をクリックし、[\* イニシエータ・グループへのマップ \*] をクリックします。



選択した igroup が、選択した LUN に追加されます。既存のマッピングは上書きされません。

ポートセットを作成して **igroup** にバインドします

の使用に加えて、を使用します "**センタクテキ LUN マップ SLM**"では、ポートセットを作成し、ポートセットをigroupにバインドして、イニシエータがLUNへのアクセスに使用するLIFをさらに制限できます。

ポートセットをigroupにバインドしない場合、igroup内のすべてのイニシエータが、LUNを所有するノードおよび所有者ノードのHAパートナーのすべてのLIFからマップ済みのLUNにアクセスできます。

必要なもの

少なくとも 1 つの LIF と 1 つの igroup が必要です。

インターフェイスグループを使用しないかぎり、iSCSI と FC の冗長性を確保するために推奨される LIF の数は 2 個です。インターフェイスグループを使用する場合に推奨される LIF の数は 1 個です。

このタスクについて


ノード上にLIFが3つ以上あり、特定のイニシエータを一部のLIFに制限する場合は、ポートセットとSLMを併用の方が効果的です。ポートセットを使用しない場合は、LUNへのアクセス権を持つすべてのイニシエータが、LUNを所有するノードおよび所有者ノードのHAパートナー経由でノード上のすべてのターゲットにアクセスできます。

### System Manager の略

ONTAP 9.10.1 以降の System Manager を使用して、ポートセットを作成し、igroup にバインドできます。

ONTAP 9.10.1より前のリリースでポートセットを作成してigroupにバインドする必要がある場合は、ONTAP CLI手順 を使用する必要があります。

1. System Manager で、 \* Network > Overview > portsets \* をクリックし、 \* Add \* をクリックします。
2. 新しいポートセットの情報を入力し、 \* Add \* をクリックします。
3. [\*Hosts] > [SAN Initiator Groups] をクリックします
4. ポートセットを新しい igroup にバインドするには、 \* Add \* をクリックします。

ポートセットを既存の igroup にバインドするには、igroup を選択し、をクリックします  をクリックし、 \* イニシエータグループの編集 \* をクリックします。

### 関連情報

["イニシエータとigroupを表示および管理します"](#)

### CLI の使用

1. 適切な LIF を含むポートセットを作成します。

```
portset create -vserver vs1 -portset portset_name -protocol
protocol -port-name port_name
```

FCを使用する場合は、を指定します protocol パラメータの形式 fcp。iSCSIを使用している場合は、を指定します protocol パラメータの形式 iscsi。

2. igroup をポートセットにバインドします。

```
lun igroup bind -vserver vs1 -igroup igroup_name -portset
portset_name
```

3. ポートセットと LIF が正しいことを確認します。

```
portset show -vserver vs1
```

Vserver	Portset	Protocol	Port Names	Igroups
vs3	portset0	iscsi	lif0,lif1	igroup1


### ポートセットを管理します

に加えて ["センタクテキ LUN マップ SLM"](#)では、ポートセットを使用して、イニシエータが LUN へのアクセスに使用する LIF をさらに制限できます。




ONTAP 9.10.1以降のSystem Managerを使用して、ポートセットに関連付けられているネットワークインターフェイスを変更し、ポートセットを削除できます。

ポートセットに関連付けられているネットワークインターフェイスを変更します

1. System Managerで、\*[ネットワーク]>[概要]>[ポートセット]\*を選択します。
2. 編集するポートセットを選択します  をクリックし、「\* ポートセットの編集」を選択します。

ポートセットを削除します

1. System Manager で、 \* Network > Overview > portsets \* をクリックします。
2. 単一のポートセットを削除するには、ポートセットを選択し、を選択します  次に、[ ポートセットの削除 ] を選択します。

複数のポートセットを削除するには、ポートセットを選択し、\* 削除 \* をクリックします。

## 選択的 LUN マップの概要

選択的 LUN マップ（SLM）を使用すると、ホストから LUN へのパスの数を減らすことができます。SLM を使用して新しい LUN マップを作成すると、LUN を所有するノードとその HA パートナーのパス経由でのみ LUN にアクセスできます。

SLM を使用すると、ホストごとに 1 つの igroup を管理でき、システム停止を伴わない LUN の移動処理がサポートされます。ポートセットの操作や LUN の再マッピングは不要です。

"ポートセット" SLMと併用すると、特定のターゲットのアクセスを特定のイニシエータだけに制限できます。SLM とポートセットを併用する場合、LUN には、その LUN を所有するノードおよびノードの HA パートナーのポートセットに含まれる一連の LIF 経由でアクセス可能になります。

新しい LUN マップでは SLM がデフォルトで有効になります。

**SLM が LUN マップで有効かどうかを判断します**

ONTAP 9リリースで作成されたLUNと以前のバージョンから移行されたLUNが環境内に混在している場合は、特定のLUNで選択的LUNマップ（SLM）が有効になっているかどうかを確認しなければならないことがあります。

の出力に表示される情報を使用できます `lun mapping show -fields reporting-nodes, node` コマンドを使用して、LUNマップでSLMが有効になっているかどうかを確認します。SLMが有効になっていない場合は、コマンド出力の「reporting-nodes」列の下セルにと表示されます。SLMが有効な場合、「nodes」列の下に表示されるノードのリストが「reporting-nodes」列に複製されます。

**SLM レポートノードリストを変更します**

LUN または LUN が含まれているボリュームを同じクラスタ内の別のハイアベイラビリティ（HA）ペアに移動する場合は、移動を開始する前に選択的 LUN マップ（SLM）のレポートノードリストを変更して、最適化されたアクティブな LUN パスを維持する必要があります。

手順

1. デスティネーションノードとそのパートナーノードをアグリゲートまたはボリュームのレポートノードリ

ストに追加します。

```
lun mapping add-reporting-nodes -vserver _vserver_name_ -path _lun_path_  
-igroup _igroup_name_ [-destination-aggregate _aggregate_name_|-  
destination-volume _volume_name_]
```

一貫した命名規則がある場合は、を使用して複数のLUNマッピングを同時に変更できます  
*igroup\_prefix\**ではなく *igroup\_name*。

2. ホストを再スキャンして、新しく追加したパスを検出します。
3. OS で必要な場合は、マルチパスネットワーク I/O （MPIO）構成に新しいパスを追加します。
4. 必要な移動処理のためのコマンドを実行して、処理が完了するまで待ちます。
5. I/O がアクティブパスまたは最適パス経由で処理されていることを確認します。

```
lun mapping show -fields reporting-nodes
```

6. レポートノードリストから、前の LUN 所有者とそのパートナーノードを削除します。

```
lun mapping remove-reporting-nodes -vserver _vserver_name_ -path  
_lun_path_ -igroup _igroup_name_ -remote-nodes
```

7. 既存の LUN マップから LUN が削除済みであることを確認します。

```
lun mapping show -fields reporting-nodes
```

8. ホスト OS の古いデバイスのエントリを削除します。
9. 必要に応じて、マルチパス構成ファイルを変更します。
10. ホストを再スキャンして古いパスが削除されたことを確認します。[+]  
ホストを再スキャンする手順については、ホストのマニュアルを参照してください。

## iSCSI プロトコルを管理します

最適なパフォーマンスを実現できるようにネットワークを設定します

イーサネットネットワークによってパフォーマンスは大きく変わります。特定の設定値を選択することで、iSCSI に使用するネットワークのパフォーマンスを最大限に高めることができます。

### 手順

1. ホストポートとストレージポートを同じネットワークに接続します。

同じスイッチに接続することを推奨します。ルーティングは絶対に使用しないでください。

2. 最も速度の速いポートを選択して、それらを iSCSI 専用にします。

10GbE ポートが最適です。最小要件は 1GbE ポートです。

3. すべてのポートでイーサネットフロー制御を無効にします。

が表示されます **"Network Management の略"** CLI を使用してイーサネットポートのフロー制御を設定するため。

4. ジャンボフレームを有効にします（通常は MTU が 9000 ）。

イニシエータ、ターゲット、スイッチを含む、データパス内のすべてのデバイスでジャンボフレームがサポートされている必要があります。サポートされていない場合にジャンボフレームを有効にすると、ネットワークのパフォーマンスが大幅に低下

## **SVM** を **iSCSI** 用に設定


iSCSI 用に Storage Virtual Machine （ SVM ）を設定するには、SVM 用の LIF を作成し、それらの LIF に iSCSI プロトコルを割り当てる必要があります。

このタスクについて

iSCSI プロトコルを使用してデータを提供するそれぞれの SVM について、各ノードに少なくとも 1 つの iSCSI LIF が必要です。冗長性を確保するには、各ノードに少なくとも 2 つの LIF を作成する必要があります。

**System Manager の略**

ONTAP System Manager (9.7以降) でiSCSI用のStorage VMを設定します。

新しい <b>Storage VM</b> で <b>iSCSI</b> を設定	既存の <b>Storage VM</b> で <b>iSCSI</b> を設定
<ol style="list-style-type: none"><li>1. System Managerで、* Storage &gt; Storage VM* をクリックし、* Add *をクリックします。</li><li>2. Storage VMの名前を入力してください。</li><li>3. アクセスプロトコル*として「* iSCSI *」を選択します。</li><li>4. Enable iSCSI (iSCSIを有効にする) をクリックし、ネットワークインタフェースのIPアドレスとサブネットマスクを入力します。 +各ノードに少なくとも2つのネットワークインターフェイスが必要です。</li><li>5. [ 保存 ( Save ) ] をクリックします。</li></ol>	<ol style="list-style-type: none"><li>1. System Manager で、* Storage &gt; Storage VM* をクリックします。</li><li>2. 設定するStorage VMをクリックします。</li><li>3. [設定]タブをクリックし、をクリックします  をクリックします。</li><li>4. Enable iSCSI (iSCSIを有効にする) をクリックし、ネットワークインタフェースのIPアドレスとサブネットマスクを入力します。 +各ノードに少なくとも2つのネットワークインターフェイスが必要です。</li><li>5. [ 保存 ( Save ) ] をクリックします。</li></ol>

**CLI の使用**

ONTAP CLIを使用してiSCSI用のStorage VMを設定します。

1. SVM が iSCSI トラフィックをリスンするようにします。

```
vserver iscsi create -vserver vserver_name -target-alias vserver_name
```

2. iSCSI に使用する各ノードに、SVM 用の LIF を作成します。

◦ ONTAP 9.6以降：

```
network interface create -vserver vserver_name -lif lif_name -data  
-protocol iscsi -service-policy default-data-iscsi -home-node node_name  
-home-port port_name -address ip_address -netmask netmask
```

◦ ONTAP 9.5以前：

```
network interface create -vserver vserver_name -lif lif_name -role data  
-data-protocol iscsi -home-node node_name -home-port port_name -address  
ip_address -netmask netmask
```

3. LIF が正しく設定されたことを確認します。

```
network interface show -vserver vserver_name
```

4. iSCSI が正常に稼働していること、およびその SVM のターゲット IQN を確認します。

```
vserver iscsi show -vserver vserver_name
```

5. ホストから、LIF への iSCSI セッションを作成します。

## 関連情報

"NetAppテクニカルレポート4080：『Best Practices for Modern SAN』"

イニシエータのセキュリティポリシー方式を定義します

イニシエータとその認証方法の一覧を定義できます。ユーザ定義の認証方法がない環境イニシエータに対するデフォルトの認証方法を変更することもできます。

このタスクについて

製品のセキュリティポリシールゴリズムを使用して一意のパスワードを生成することも、使用するパスワードを手動で指定することもできます。



すべてのイニシエータが 16 進数 CHAP シークレットパスワードをサポートしているわけ

## 手順

1. を使用します `vserver iscsi security create` イニシエータのセキュリティポリシー方式を作成するコマンド。

```
vserver iscsi security create -vserver vs2 -initiator iqn.1991-05.com.microsoft:host1 -auth-type CHAP -user-name bob1 -outbound-user-name bob2
```

2. 画面に表示されるコマンドに従ってパスワードを追加します。

インバウンドとアウトバウンドの CHAP ユーザ名およびパスワードを使用して、イニシエータ `iqn.1991-05.com.microsoft:host1` のセキュリティポリシー方式を作成します。

## 関連情報

- [iSCSI 認証の仕組み](#)
- [CHAP認証](#)

## SVM の iSCSI サービスを削除します

Storage Virtual Machine（SVM）の不要になった iSCSI サービスは削除できます。

### 必要なもの

iSCSI サービスを削除するには、iSCSI サービスの管理ステータスが「所有」状態である必要があります。を使用すると、管理ステータスをdownに切り替えることができます `vserver iscsi modify` コマンドを実行します

## 手順

1. を使用します `vserver iscsi modify` コマンドを使用してLUNへのI/Oを停止します。

```
vserver iscsi modify -vserver vs1 -status-admin down
```

2. を使用します `vserver iscsi delete` コマンドを使用してSVMからiSCSIサービスを削除します。

```
vserver iscsi delete -vserver vs_1
```

3. を使用します `vserver iscsi show command` をクリックして、SVMからiSCSIサービスが削除されたことを確認します。

```
vserver iscsi show -vserver vs1
```

**iSCSI セッションのエラーリカバリの詳細については、こちらを参照してください**

iSCSI セッションのエラーリカバリレベルを上げると、iSCSI エラーリカバリの詳細情報を確認できます。高いレベルのエラーリカバリを使用すると、原因で iSCSI セッションのパフォーマンスが少し低下する可能性があります。

このタスクについて

デフォルトでは、ONTAP は iSCSI セッションに対してエラーリカバリレベル 0 を使用するよう設定されています。エラーリカバリレベル 1 または 2 に対応したイニシエータを使用している場合は、エラーリカバリレベルを上げるように選択できます。変更したセッションのエラーリカバリレベルは、新しく作成するセッションにのみ影響し、既存のセッションには影響しません。

ONTAP 9.4以降では `max-error-recovery-level` オプションはではサポートされていません `iscsi show` および `iscsi modify` コマンド

手順

1. advanced モードに切り替えます。

```
set -privilege advanced
```

2. を使用して現在の設定を確認します `iscsi show` コマンドを実行します

```
iscsi show -vserver vs3 -fields max-error-recovery-level
```

```
vserver max-error-recovery-level
-----
vs3      0
```

3. を使用してエラーリカバリレベルを変更します `iscsi modify` コマンドを実行します

```
iscsi modify -vserver vs3 -max-error-recovery-level 2
```

## SVM を iSNS サーバに登録する

を使用できます `vserver iscsi isns` iSNSサーバに登録するようにStorage Virtual Machine (SVM) を設定するコマンド。

このタスクについて

。 `vserver iscsi isns create` コマンドは、SVMをiSNSサーバに登録するように設定します。SVM には、iSNS サーバの設定や管理を行うコマンドはありません。iSNS サーバを管理するには、iSNS サーバのベンダーが提供するサーバ管理ツールまたはインターフェイスを使用します。

## 手順

1. iSNS サーバで、iSNS サービスが開始しており、サービスを提供可能な状態であることを確認します。
2. データポートに SVM 管理 LIF を作成します。

```
network interface create -vserver SVM_name -lif lif_name -role data -data  
-protocol none -home-node home_node_name -home-port home_port -address  
IP_address -netmask network_mask
```

3. SVM に iSCSI サービスがない場合は作成します。

```
vserver iscsi create -vserver SVM_name
```

4. iSCSI サービスが正常に作成されたことを確認します。

```
iscsi show -vserver SVM_name
```

5. SVM のデフォルトルートが存在していることを確認します。

```
network route show -vserver SVM_name
```

6. SVM のデフォルトルートが存在しない場合は、デフォルトルートを作成します。

```
network route create -vserver SVM_name -destination destination -gateway  
gateway
```

7. iSNS サービスに登録するように SVM を設定します。

```
vserver iscsi isns create -vserver SVM_name -address IP_address
```

IPv4 アドレスファミリーと IPv6 アドレスファミリーの両方がサポートされています。iSNS サーバのアドレスファミリーは、SVM 管理 LIF のアドレスファミリーと同じである必要があります。

たとえば、IPv4 アドレスを使用する SVM 管理 LIF を、IPv6 アドレスを使用する iSNS サーバに接続することはできません。

8. iSNS サービスが実行されていることを確認します。

```
vserver iscsi isns show -vserver SVM_name
```

9. iSNS サービスが実行されていない場合は、iSNS サービスを開始します。

```
vserver iscsi isns start -vserver SVM_name
```

## ストレージシステム上の **iSCSI** エラーメッセージを解決します

iSCSI関連の一般的なエラーメッセージは、で確認できます event log show コマンドを実行しますこれらのメッセージの意味と、特定された問題の解決方法を把握する必要があります。

次の表に、最も一般的なエラーメッセージと、それらを解決する手順を示します。

メッセージ	説明	対処方法：
ISCSI: network interface identifier disabled for use; incoming connection discarded	このインターフェイスの iSCSI サービスが有効になっていません。	<p>を使用できます <code>iscsi interface enable</code> コマンドを実行してインターフェイスで iSCSI サービスを有効にします。例：</p> <pre>iscsi interface enable -vserver vs1 -lif lif1</pre>
ISCSI: Authentication failed for initiator nodename	指定されたイニシエータに対して CHAP が正しく設定されていません。	<p>CHAP 設定をチェックします。ストレージシステムのインバウンド設定とアウトバウンド設定には、同じユーザ名およびパスワードを使用できません。</p> <ul style="list-style-type: none"> <li>• ストレージシステムのインバウンドクレデンシャルは、イニシエータのアウトバウンドクレデンシャルと一致する必要があります</li> <li>• ストレージシステムのアウトバウンドクレデンシャルは、イニシエータのインバウンドクレデンシャルと一致する必要があります</li> </ul>

### iSCSI LIFの自動フェイルオーバーの有効化または無効化

ONTAP 9.11.1以降にアップグレードした場合は、ONTAP 9.10.1以前で作成したすべての iSCSI LIF で LIF の自動フェイルオーバーを手動で有効にする必要があります。

ONTAP 9.11.1以降では、オールフラッシュ SAN アレイプラットフォームで iSCSI LIF の LIF の自動フェイルオーバーを有効にすることができます。ストレージフェイルオーバーが発生すると、iSCSI LIF はホームノードまたはポートから HA パートナーノードまたはポートに自動的に移行され、フェイルオーバーの完了後に再び移行されます。または、iSCSI LIF のポートが正常な状態でなくなった場合、その LIF は現在のホームノードの正常なポートに自動的に移行され、ポートが正常な状態に戻った時点で元のポートに戻ります。を使用すると、iSCSI で実行されている SAN ワークロードは、フェイルオーバー後に I/O サービスを迅速に再開できます。

ONTAP 9.11.1以降では、次のいずれかの条件に該当する場合、新しく作成した iSCSI LIF で LIF の自動フェイルオーバーがデフォルトで有効になります。

- SVM に iSCSI LIF がありません
- LIF の自動フェイルオーバーが SVM のすべての iSCSI LIF で有効になっている

### iSCSI LIFの自動フェイルオーバーを有効にする

デフォルトでは、ONTAP 9.10.1以前で作成した iSCSI LIF では、LIF の自動フェイルオーバーは有効になりません。SVM 上に LIF の自動フェイルオーバーが有効になっていない iSCSI LIF がある場合、新しく作成した LIF でも LIF の自動フェイルオーバーは有効になりません。LIF の自動フェイルオーバーが有効になっておらず、



フェイルオーバーが発生するとiSCSI LIFは移行されません。

の詳細を確認してください ["LIFのフェイルオーバーとギブバック"](#)。

#### ステップ

1. iSCSI LIFの自動フェイルオーバーを有効にします。

```
network interface modify -vserver SVM_name -lif iscsi_lif -failover-policy sfo-partner-only -auto-revert true
```

SVMのすべてのiSCSI LIFを更新するには、`-lif*` ではなく `lif`。

#### iSCSI LIFの自動フェイルオーバーを無効にする

ONTAP 9.10.1以前で作成したiSCSI LIFに対するiSCSI LIFの自動フェイルオーバーを以前に有効にしていた場合は、無効にすることもできます。

#### ステップ

1. iSCSI LIFの自動フェイルオーバーを無効にします。

```
network interface modify -vserver SVM_name -lif iscsi_lif -failover-policy disabled -auto-revert false
```

SVMのすべてのiSCSI LIFを更新するには、`-lif*` ではなく `lif`。

#### 関連情報

- ["LIFを作成"](#)
- 手動で実行する ["LIFを移行する"](#)
- 手動で実行する ["LIFをホームポートにリポートします。"](#)
- ["LIFのフェイルオーバーを設定する"](#)

## FC プロトコルを管理する

### FC 用に SVM を設定

FC 用に Storage Virtual Machine (SVM) を設定するには、SVM 用の LIF を作成し、それらの LIF に FC プロトコルを割り当てる必要があります。

#### 作業を開始する前に

FCライセンス (["ONTAP Oneに付属"](#)) を使用し、有効にする必要があります。FCライセンスが有効になっていない場合、LIFとSVMはオンラインとして表示されますが、動作ステータスはになります `down`。LIF と SVM を動作状態にするには、FC サービスを有効にする必要があります。イニシエータをホストするには、SVM 内のすべての FC LIF で単一イニシエータゾーニングを使用する必要があります。

このタスクについて

ネットアップでは、FC プロトコルを使用してデータを提供するそれぞれの SVM について、各ノードに少なくとも 1 つの FC LIF をサポートしています。 ノードごとに 1 つの LIF を接続した構成では、ノードごとに 2 つの LIF と 2 つのファブリックを使用する必要があります。これにより、ノードレイヤとファブリックで冗長性が確保されます。

例 13. 手順

System Manager の略

ONTAP System Manager (9.7以降) でiSCSI用のStorage VMを設定します。

をクリックして新しい <b>Storage VM</b> に <b>FC</b> を設定してください	既存の <b>Storage VM</b> に <b>FC</b> を設定
<div>1. System Managerで、 * Storage &gt; Storage VM* をクリックし、 * Add *をクリックします。</div> <div>2. Storage VMの名前を入力してください。</div> <div>3. アクセスプロトコル*として「* FC」を選択します。</div> <div>4. [FCを有効にする]をクリックします。 + FCポートが自動的に割り当てられます。</div> <div>5. [ 保存 ( Save ) ] をクリックします。</div>	<div>1. System Manager で、 * Storage &gt; Storage VM* をクリックします。</div> <div>2. 設定するStorage VMをクリックします。</div> <div>3. [設定]タブをクリックし、 をクリックします  をクリックします。</div> <div>4. Enable FC (FCを有効にする) をクリックし、ネットワークインタフェースのIPアドレスとサブネットマスクを入力します。 + FCポートが自動的に割り当てられます。</div> <div>5. [ 保存 ( Save ) ] をクリックします。</div>

CLI の使用

1. SVM で FC サービスを有効にします。

```
vserver fcp create -vserver vserver_name -status-admin up
```

2. FC を提供する各ノードの SVM 用に 2 つの LIF を作成します。

◦ ONTAP 9.6以降：

```
network interface create -vserver vserver_name -lif lif_name -data  
-protocol fcp -service-policy default-data-fcp -home-node node_name  
-home-port port_name -address ip_address -netmask netmask -status-admin  
up
```

◦ ONTAP 9.5以前：

```
network interface create -vserver vserver_name -lif lif_name -role data  
-data-protocol fcp -home-node node_name -home-port port
```

3. LIFが作成され、動作ステータスがになっていることを確認します online：

```
network interface show -vserver vserver_name lif_name
```

## SVM の FC サービスを削除する

Storage Virtual Machine （ SVM ） の不要になった FC サービスは削除できます。

### 必要なもの

SVM の FC サービスを削除するには、事前に管理ステータスを「所有」にする必要があります。管理ステータスをdownに設定するには、を使用します `vserver fcp modify` コマンドまたはを実行します `vserver fcp stop` コマンドを実行します

### 手順

1. を使用します `vserver fcp stop` コマンドを使用してLUNへのI/Oを停止します。

```
vserver fcp stop -vserver vs_1
```

2. を使用します `vserver fcp delete` SVMからサービスを削除するコマンド。

```
vserver fcp delete -vserver vs_1
```

3. を使用します `vserver fcp show` SVMからFCサービスが削除されたことを確認します。

```
vserver fcp show -vserver vs_1
```

## FCoE ジャンボフレーム用の MTU の推奨設定

Fibre Channel over Ethernet （ FCoE ） の場合、 CNA のイーサネットアダプタ部分については、ジャンボフレームを 9000 MTU で設定する必要があります。CNA の FCoE アダプタ部分については、ジャンボフレームを 1500 以上の MTU で設定する必要があります。イニシエータ、ターゲット、および介在するすべてのスイッチがジャンボフレームをサポートしており、ジャンボフレーム用に設定されている場合にのみ、ジャンボフレームを設定します。

## NVMe プロトコルを管理します

### SVM の NVMe サービスを開始します

Storage Virtual Machine （ SVM ） で NVMe プロトコルを使用する前に、 SVM で NVMe サービスを開始しておく必要があります。

### 作業を開始する前に

システムで NVMe プロトコルが許可されている必要があります。

サポートされる NVMe プロトコルは次のとおりです。

プロトコル	先頭のドキュメント	許可者
TCP	ONTAP 9.10.1	デフォルト
FCP	ONTAP 9.4	デフォルト

#### 手順

1. 権限の設定を advanced に変更します。

```
set -privilege advanced
```

2. NVMe プロトコルが許可されていることを確認します。

```
vserver nvme show
```

3. NVMe プロトコルサービスを作成します。

```
vserver nvme create
```

4. SVM で NVMe プロトコルサービスを開始します。

```
vserver nvme modify -status -admin up
```

#### SVM から NVMe サービスを削除します

必要に応じて、Storage Virtual Machine （ SVM ） から NVMe サービスを削除できます。

#### 手順

1. 権限の設定を advanced に変更します。

```
set -privilege advanced
```

2. SVM で NVMe サービスを停止します。

```
vserver nvme modify -status -admin down
```


3. NVMe サービスを削除します。

```
vserver nvme delete
```

#### ネームスペースのサイズを変更する

ONTAP 9.10.1 以降では、ONTAP CLI を使用して NVMe ネームスペースのサイズを拡張または縮小できます。System Manager を使用して、NVMe ネームスペースのサイズを拡張できます。

#### System Manager の略

1. Storage > NVMe Namespaces \* をクリックします。
2. 拡張するネームスペースの上にあるをクリックします  をクリックし、\* 編集 \* をクリックします。
3. 容量 \* で、ネームスペースのサイズを変更します。

#### CLI の使用

1. 次のコマンドを入力します。 `vserver nvme namespace modify -vserver SVM_name -path path -size new_size_of_namespace`

#### ネームスペースのサイズを縮小します

NVMe ネームスペースのサイズを縮小するには、ONTAP CLI を使用する必要があります。

1. 権限の設定を advanced に変更します。

```
set -privilege advanced
```

2. ネームスペースのサイズを縮小します。

```
vserver nvme namespace modify -vserver SVM_name -path namespace_path -size new_size_of_namespace
```

#### ネームスペースをLUNに変換する

ONTAP 9.11.1以降では、ONTAP CLIを使用して、既存のNVMeネームスペースをインプレーズでLUNに変換できます。

を開始する前に

- 指定したNVMeネームスペースにはサブシステムへの既存のマッピングがありません。
- ネームスペースをSnapshotコピーの一部にしたり、SnapMirror関係のデスティネーション側で読み取り専用ネームスペースとして使用したりすることはできません。
- NVMeネームスペースは特定のプラットフォームとネットワークカードでのみサポートされるため、この機能は特定のハードウェアでのみ機能します。

#### 手順

1. 次のコマンドを入力して、NVMeネームスペースをLUNに変換します。

```
lun convert-from-namespace -vserver -namespace-path
```

#### NVMe経由のインバンド認証の設定

ONTAP 9.12.1以降では、ONTAPコマンドラインインターフェイス（CLI）を使用して、DH-HMAC-CHAP認証を使用して、NVMe/TCPおよびNVMe/FCプロトコルを介し

たNVMeホストとコントローラ間のインバンド（セキュア）双方向および単方向認証を設定できます。ONTAP 9.14.1以降では、インバンド認証をSystem Managerで設定できます。

インバンド認証を設定するには、各ホストまたはコントローラにDH-HMAC-CHAPキーを関連付ける必要があります。DH-HMAC-CHAPキーは、NVMeホストまたはコントローラのNQNと管理者が設定した認証シークレットを組み合わせたものです。NVMeホストまたはコントローラがピアを認証するには、ピアに関連付けられたキーを認識する必要があります。

単方向認証では、コントローラではなくホストにシークレットキーが設定されます。双方向認証では、ホストとコントローラの両方にシークレットキーが設定されます。

SHA-256がデフォルトのハッシュ関数で、2048ビットがデフォルトのDHグループです。

## System Manager の略

ONTAP 9.14.1以降では、NVMeサブシステムの作成または更新、NVMeネームスペースの作成またはクローニング、新しいNVMeネームスペースを使用した整合グループの追加時に、System Managerを使用してインバンド認証を設定できます。

### 手順

1. System Managerで、[ホスト]>[NVMeサブシステム]\*をクリックし、[追加]\*をクリックします。
2. NVMeサブシステム名を追加し、Storage VMとホストオペレーティングシステムを選択します。
3. ホストのNQNを入力します。
4. [Host NQN]の横にある\*[Use in-band authentication]\*を選択します。
5. ホストシークレットとコントローラシークレットを指定します。

DH-HMAC-CHAPキーは、NVMeホストまたはコントローラのNQNと管理者が設定した認証シークレットを組み合わせたものです。

6. ホストごとに使用するハッシュ関数とDHグループを選択します。

ハッシュ関数とDHグループを選択しない場合、SHA-256がデフォルトのハッシュ関数として割り当てられ、2048ビットがデフォルトのDHグループとして割り当てられます。

7. 必要に応じて、\*[追加]\*をクリックし、必要に応じて手順を繰り返してホストを追加します。
8. [保存 ( Save ) ]をクリックします。
9. インバンド認証が有効になっていることを確認するには、\*[システムマネージャ]>[ホスト]>[NVMeサブシステム]>[グリッド]>[ピークビュー]\*をクリックします。

ホスト名の横にあるトランスペアレントキーアイコンは、単方向モードがイネーブルであることを示します。 ホスト名の横にある不透明キーは、双方向モードが有効であることを示します。

## CLI の使用

### 手順

1. NVMeサブシステムにDH-MHMAC-CHAP認証を追加します。

```
vserver nvme subsystem host add -vserver <svm_name> -subsystem
<subsystem> -host-nqn <host_nqn> -dhchap-host-secret
<authentication_host_secret> -dhchap-controller-secret
<authentication_controller_secret> -dhchap-hash-function <sha-
256|sha-512> -dhchap-group <none|2048-bit|3072-bit|4096-bit|6144-
bit|8192-bit>
```

2. DH-MHMAC CHAP認証プロトコルがホストに追加されていることを確認します。

```
vserver nvme subsystem host show
```

```

[ -dhchap-hash-function {sha-256|sha-512} ] Authentication Hash
Function
[ -dhchap-dh-group {none|2048-bit|3072-bit|4096-bit|6144-bit|8192-
bit} ]
Diffie-Hellman
Group
[ -dhchap-mode {none|unidirectional|bidirectional} ]
Authentication Mode

```

### 3. NVMeコントローラの作成時にDH-MHMAC CHAP認証が実行されたことを確認します。

```
vserver nvme subsystem controller show
```

```

[ -dhchap-hash-function {sha-256|sha-512} ] Authentication Hash
Function
[ -dhchap-dh-group {none|2048-bit|3072-bit|4096-bit|6144-bit|8192-
bit} ]
Diffie-Hellman
Group
[ -dhchap-mode {none|unidirectional|bidirectional} ]
Authentication Mode

```

## NVMe経由のインバンド認証を無効にする

DH-HMAC-CHAPを使用してNVMe経由のインバンド認証を設定している場合は、いつでも無効にすることができます。

ONTAP 9.12.1以降からONTAP 9.12.0以前にリバートする場合は、リバート前にインバンド認証を無効にする必要があります。DH-HMAC-CHAPを使用するインバンド認証が無効になっていない場合、リバートは失敗します。

### 手順

1. サブシステムからホストを削除して、DH-MHMAC-CHAP認証を無効にします。

```
vserver nvme subsystem host remove -vserver <svm_name> -subsystem
<subsystem> -host-nqn <host_nqn>
```

2. DH-MHMAC-CHAP認証プロトコルがホストから削除されたことを確認します。



```
vserver nvme subsystem host show
```

3. 認証を行わずにホストをサブシステムに再度追加します。

```
vserver nvme subsystem host add vserver <svm_name> -subsystem  
<subsystem> -host-nqn <host_nqn>
```

## NVMeホスト優先度の変更

ONTAP 9.14.1以降では、特定のホストに対するリソース割り当ての優先順位を設定するようにNVMeサブシステムを設定できます。デフォルトでは、ホストがサブシステムに追加されると、通常の優先度が割り当てられます。高い優先度を割り当てられたホストには、より多くのI/Oキュー数とキュー深度が割り当てられます。

ONTAPのコマンドラインインターフェイス（CLI）を使用して、デフォルト優先度を手動で標準から高に変更できます。ホストに割り当てられている優先度を変更するには、サブシステムからホストを削除してから再度追加する必要があります。

### 手順

1. ホストプライオリティがRegularに設定されていることを確認します。

```
vserver nvme show-host-priority
```

2. サブシステムからホストを削除します。

```
vserver nvme subsystem host remove -vserver <svm_name> -subsystem  
<subsystem> -host-nqn <host_nqn>
```

3. ホストがサブシステムから削除されたことを確認します。

```
vserver nvme subsystem host show
```

4. 優先度が高いサブシステムにホストを再度追加します。

```
vserver nvme subsystem host add -vserver <SVM_name> -subsystem  
<subsystem_name> -host-nqn <Host_NQN_:subsystem._subsystem_name>  
-priority high
```

**NVMe / TCP**コントローラのホストの自動検出を管理します。

ONTAP 9.14.1以降、IPベースのファブリックでは、NVMe/TCPプロトコルを使用するコントローラのホスト検出がデフォルトで自動化されます。

#### NVMe / TCPコントローラのホスト検出を自動化

以前に自動ホスト検出を無効にしていたが、ニーズが変わった場合は、再度有効にすることができます。

##### 手順

1. advanced 権限モードに切り替えます。

```
set -privilege advanced
```

2. 自動検出を有効にします。

```
vserver nvme modify -vserver <vserver_name> -mdns-service-discovery  
-enabled true
```

3. NVMe/TCPコントローラの自動検出が有効になっていることを確認します。

```
vserver nvme show
```

#### NVMe / TCPコントローラのホストの自動検出を無効にする

NVMe / TCPコントローラをホストで自動的に検出する必要がなく、ネットワークで不要なマルチキャストトラフィックが検出された場合は、この機能を無効にする必要があります。

##### 手順

1. advanced 権限モードに切り替えます。

```
set -privilege advanced
```

2. 自動検出を無効にします。

```
vserver nvme modify -vserver <vserver_name> -mdns-service-discovery  
-enabled false
```

3. NVMe/TCPコントローラの自動検出が無効になっていることを確認します。

```
vserver nvme show
```

## NVMeホスト仮想マシン識別子の無効化

ONTAP 9.14.1以降では、デフォルトで、ONTAPでNVMe/FCホストが一意的識別子で仮想マシンを識別し、NVMe/FCホストが仮想マシンのリソース利用率を監視する機能がサポートされます。これにより、ホスト側のレポート作成とトラブルシューティングが強化されます。

この機能は、bootargを使用して無効にできます。

### ステップ

1. 仮想マシンIDを無効にします。

```
bootargs set fct_sli_appid_off <port>, <port>
```

次の例は、ポート0gとポート0iのVMIDを無効にします。

```
bootargs set fct_sli_appid_off 0g,0i

fct_sli_appid_off == 0g,0i
```

## FC アダプタを搭載したシステムを管理する

### FC アダプタを搭載したシステムを管理する

オンボード FC アダプタと FC アダプタカードの管理に使用できるコマンドが用意されています。これらのコマンドを使用して、アダプタモードの設定、アダプタ情報の表示、および速度の変更を行うことができます。

ほとんどのストレージシステムには、イニシエータまたはターゲットとして設定できるオンボード FC アダプタが搭載されています。イニシエータまたはターゲットとして設定された FC アダプタカードを使用することもできます。イニシエータはバックエンドディスクシェルフに接続します。場合によっては、外部ストレージアレイ（FlexArray）にも接続します。ターゲットは FC スイッチのみに接続します。FC ターゲットの HBA ポートとスイッチポートの速度は、両方とも同じ値に設定し、auto には設定しないでください。

### 関連情報

["SAN構成"](#)

### FC アダプタの管理用コマンド

FC コマンドを使用して、ストレージコントローラの FC ターゲットアダプタ、FC イニシエータアダプタ、およびオンボード FC アダプタを管理できます。FC アダプタの管理に使用するコマンドは、FC プロトコルと FC-NVMe プロトコルで同じです。

FC イニシエータアダプタのコマンドは、ノードレベルでのみ機能します。を使用する必要があります `run -node node_name` FCイニシエータアダプタのコマンドを使用する前のコマンド。

## FC ターゲットアダプタの管理用コマンド

状況	使用するコマンド
ノードの FC アダプタ情報を表示する	<code>network fcp adapter show</code>
FC ターゲットアダプタのパラメータを変更する	<code>network fcp adapter modify</code>
FC プロトコルトラフィック情報を表示します	<code>run -node <i>node_name</i> sysstat -f</code>
FC プロトコルの実行時間を表示します	<code>run -node <i>node_name</i> uptime</code>
アダプタの設定とステータスを表示します	<code>run -node <i>node_name</i> sysconfig -v adapter</code>
拡張カードが取り付けられていること、および構成にエラーがないかどうかを確認します	<code>run -node <i>node_name</i> sysconfig -ac</code>
コマンドのマニュアルページを表示します	<code>man <i>command_name</i></code>

## FC イニシエータアダプタの管理用コマンド

状況	使用するコマンド
ノードのすべてのイニシエータおよびそのアダプタの情報を表示する	<code>run -node <i>node_name</i> storage show adapter</code>
アダプタの設定とステータスを表示します	<code>run -node <i>node_name</i> sysconfig -v adapter</code>
拡張カードが取り付けられていること、および構成にエラーがないかどうかを確認します	<code>run -node <i>node_name</i> sysconfig -ac</code>

## オンボード FC アダプタの管理用コマンド

状況	使用するコマンド
オンボード FC ポートのステータスを表示します	<code>run -node <i>node_name</i> system hardware unified-connect show</code>

## FCアダプタを設定

オンボードの FC ポートは、それぞれイニシエータまたはターゲットとして個別に構成できます。一部の FC アダプタのポートについては、オンボードの FC ポートと同様に、それぞれターゲットポートまたはイニシエータポートとして個別に構成することもできます。ターゲットモードに設定できるアダプタのリストは、で確認できます

## "NetApp Hardware Universe の略"。

ターゲットモードは、ポートを FC イニシエータに接続するために使用します。イニシエータモードは、テープドライブやテープライブラリへのポートの接続、または FlexArray 仮想化や Foreign LUN Import (FLI) を使用するサードパーティストレージへのポートの接続に使用されます。

FC アダプタを構成する手順は、FC プロトコルでも FC-NVMe プロトコルでも同じです。ただし、FC-NVMe をサポートする FC アダプタは限られています。を参照してください ["NetApp Hardware Universe の略"](#) FC-NVMe プロトコルをサポートするアダプタの一覧が表示されます。

**FC アダプタをターゲットモードに設定します**

手順

1. アダプタをオフラインにします。

```
node run -node node_name storage disable adapter adapter_name
```

アダプタがオフラインにならない場合は、システムの該当するアダプタポートからケーブルを取り外すこともできます。

2. アダプタをイニシエータからターゲットに変更します。

```
system hardware unified-connect modify -t target -node node_name adapter adapter_name
```

3. 変更したアダプタをホストしているノードをリブートします。

4. ターゲットポートの設定が正しいことを確認します。

```
network fcp adapter show -node node_name
```

5. アダプタをオンラインにします。

```
network fcp adapter modify -node node_name -adapter adapter_port -state up
```

**FC アダプタをイニシエータモードに設定します**

必要なもの

- アダプタの LIF を、メンバーとして属するすべてのポートセットから削除する必要があります。
- 物理ポートのパーソナリティをターゲットからイニシエータに変更する前に、変更する物理ポートを使用するすべての Storage Virtual Machine (SVM) のすべての LIF を、移行するか破棄する必要があります。



NVMe/FC ではイニシエータモードがサポートされます。

手順

1. アダプタからすべての LIF を削除します。

```
network interface delete -vserver SVM_name -lif LIF_name,LIF_name
```

2. アダプタをオフラインにします。

```
network fcp adapter modify -node node_name -adapter adapter_port -status-admin down
```

アダプタがオフラインにならない場合は、システムの該当するアダプタポートからケーブルを取り外すこともできます。

3. アダプタをターゲットからイニシエータに変更します。

```
system hardware unified-connect modify -t initiator adapter_port
```

4. 変更したアダプタをホストしているノードをリブートします。
5. 構成に対して FC ポートが正しい状態で設定されていることを確認します。

```
system hardware unified-connect show
```

6. アダプタをオンラインに戻します。

```
node run -node node_name storage enable adapter adapter_port
```

アダプタの設定を確認します

特定のコマンドを使用して、FC / UTAアダプタに関する情報を表示できます。

#### FCターゲットアダプタ

##### ステップ

1. を使用します `network fcp adapter show` アダプタ情報を表示するコマンド：`network fcp adapter show -instance -node node1 -adapter 0a`

使用されている各スロットのシステム設定情報とアダプタ情報が出力に表示されます。

#### ユニファイドターゲットアダプタ (UTA) のX1143A-R6

##### 手順

1. ケーブルを接続していない状態でコントローラをブートします。
2. を実行します `system hardware unified-connect show` コマンドを使用して、ポートの設定とモジュールを確認します。
3. ポート情報を確認してから、CNA とポートを設定します。

#### UTA2 ポートを CNA モードから FC モードに変更します

Fibre Channel (FC ; ファイバチャネル) イニシエータモードと FC ターゲットモードをサポートするには、UTA2 ポートを Converged Network Adapter (CNA ; 統合ネットワークアダプタ) モードから FC モードに変更する必要があります。ポートをネットワークに接続する物理メディアを変更する必要がある場合は、パーソナリティを CNA モードから FC モードに変更します。

##### 手順

1. アダプタをオフラインにします。

```
network fcp adapter modify -node node_name -adapter adapter_name -status-admin
down
```

2. ポートのモードを変更します。

```
ucadmin modify -node node_name -adapter adapter_name -mode fcp
```

3. ノードをリブートし、アダプタをオンラインにします。

```
network fcp adapter modify -node node_name -adapter adapter_name -status-admin
up
```

4. 状況に応じて、管理者にポートの削除を依頼するか、VIF マネージャでポートを削除します。

- 。ポートが LIF のホームポートとして使用されている場合、インターフェイスグループ（ifgrp）のメンバーである場合、または VLAN をホストしている場合は、管理者は次の作業を行う必要があります。

- i. LIF を移動するか、ifgrp からポートを削除する、または VLAN をそれぞれ削除します。
- ii. を実行して、ポートを手動で削除します network port delete コマンドを実行します

状況に応じて network port delete コマンドが失敗した場合は、エラーに対処してからもう一度コマンドを実行する必要があります。

- 。ポートが LIF のホームポートとして使用されていない場合、ifgrp のメンバーでない場合、および VLAN をホストしていない場合は、リブート時に VIF マネージャのレコードからポートが削除されます。

VIF マネージャでポートが削除されない場合は、管理者がリブート後にを使用してポートを手動で削除する必要があります network port delete コマンドを実行します

```
net-f8040-34::> network port show
```

```
Node: net-f8040-34-01
```

Port	IPspace	Broadcast	Domain	Link	MTU	Speed (Mbps) Admin/Oper	Health Status
...							
e0i	Default	Default		down	1500	auto/10	-
e0f	Default	Default		down	1500	auto/10	-
...							

```
net-f8040-34::> ucadmin show
```

Admin	Current	Current	Pending	Pending
Node	Adapter	Mode	Type	Type
Status				

```

-----
-----
net-f8040-34-01 0e cna target - -
offline
net-f8040-34-01 0f cna target - -
offline
...

net-f8040-34::> network interface create -vs net-f8040-34 -lif m
-role
node-mgmt-home-node net-f8040-34-01 -home-port e0e -address 10.1.1.1
-netmask 255.255.255.0

net-f8040-34::> network interface show -fields home-port, curr-port

vserver lif home-port curr-port
-----
Cluster net-f8040-34-01_clus1 e0a e0a
Cluster net-f8040-34-01_clus2 e0b e0b
Cluster net-f8040-34-01_clus3 e0c e0c
Cluster net-f8040-34-01_clus4 e0d e0d
net-f8040-34
cluster_mgmt e0M e0M
net-f8040-34
m e0e e0i
net-f8040-34
net-f8040-34-01_mgmt1 e0M e0M
7 entries were displayed.

net-f8040-34::> ucadmin modify local 0e fc

Warning: Mode on adapter 0e and also adapter 0f will be changed to
fc.
Do you want to continue? {y|n}: y
Any changes will take effect after rebooting the system. Use the
"system node reboot" command to reboot.

net-f8040-34::> reboot local
(system node reboot)

Warning: Are you sure you want to reboot node "net-f8040-34-01"?
{y|n}: y

```

5. 適切な SFP+ が取り付けられていることを確認します。



```
network fcp adapter show -instance -node -adapter
```

CNA の場合は、10Gb イーサネット SFP を使用します。FC の場合は、ノードで構成を変更する前に、8Gb SFP または 16Gb SFP を使用します。

## CNA / UTA2 ターゲットアダプタの光モジュールを変更します

ユニファイドターゲットアダプタ（CNA / UTA2）用に選択したパーソナリティモードをサポートするには、そのアダプタで光モジュールを変更する必要があります。

### 手順

1. カードで使用されている現在の SFP+ を確認します。次に、現在の SFP+ を、優先して使用するパーソナリティ（FC または CNA）に適した SFP+ に差し替えます。
2. X1143A-R6 アダプタから現在の光モジュールを取り外します。
3. 優先して使用するパーソナリティモード（FC または CNA）の光ファイバに適したモジュールを挿入します。
4. 適切な SFP+ が取り付けられていることを確認します。

```
network fcp adapter show -instance -node -adapter
```

サポートされている SFP+ モジュールと Cisco ブランドの銅線（Twinax）ケーブルについては、Hardware Universe を参照してください。

### 関連情報

["NetApp Hardware Universe の略"](#)

## X1143A-R6 アダプタでサポートされるポート設定

FC ターゲットモードは、X1143A-R6 アダプタポートのデフォルト設定です。ただし、このアダプタのポートは、10Gb イーサネットおよび FCoE ポートまたは 16Gb FC ポートとして設定できます。

イーサネットおよび FCoE 用に設定した場合、X1143A-R6 アダプタは、同じ 10GbE ポートの NIC および FCoE のターゲットトラフィックを同時にサポートします。FC 用に設定した場合、同じ ASIC を共有する 2 ポートの各ペアを FC ターゲットまたは FC イニシエータモード用に個別に設定できます。つまり、単一の X1143A-R6 アダプタが、1 つの 2 ポートペアで FC ターゲットモードをサポートし、もう 1 つの 2 ポートペアで FC イニシエータモードをサポートできます。

### 関連情報

["NetApp Hardware Universe の略"](#)

["SAN構成"](#)

### ポートを設定します

ユニファイドターゲットアダプタ（X1143A-R6）を設定するには、同じチップ上の隣接する 2 個のポートを同じパーソナリティモードで設定する必要があります。

## 手順

1. を使用して、必要に応じてFibre Channel（FC；ファイバチャネル）またはConverged Network Adapter（CNA；統合ネットワークアダプタ）にポートを設定します system node hardware unified-connect modify コマンドを実行します
2. FC または 10Gb イーサネットに適したケーブルを接続します。
3. 適切な SFP+ が取り付けられていることを確認します。

```
network fcp adapter show -instance -node -adapter
```

CNA の場合は、10Gb イーサネット SFP を使用します。FC の場合は、接続先の FC ファブリックに応じて 8Gb SFP または 16Gb SFP を使用します。

## X1133A-R6 アダプタ使用時の接続の切断を回避します

別の X1133A-R6 HBA への冗長パスを構成することにより、ポート障害時に接続が切断されないようにすることができます。

X1133A-R6 HBA は、4 ポート 16Gb の FC アダプタで、2 組の 2 ポートペアで構成されます。X1133A-R6 アダプタは、ターゲットモードまたはイニシエータモードとして設定できます。2 ポートペアはそれぞれ 1 つの ASIC でサポートされます（たとえば、ポート 1 とポート 2 は ASIC 1、ポート 3 とポート 4 は ASIC 2）。単一の ASIC の両方のポートを、ターゲットモードまたはイニシエータモードのどちらかで動作するように設定する必要があります。ペアをサポートする ASIC でエラーが発生すると、そのペアの両方のポートがオフラインになります。

接続が切断されないようにするには、別の X1133A-R6 HBA への冗長パスか、HBA の別の ASIC でサポートされるポートへの冗長パスを構成します。

## すべての SAN プロトコルの LIF を管理します

すべての **SAN** プロトコルの **LIF** を管理します

SAN環境でクラスタのフェイルオーバー機能を利用するには、イニシエータでMultipath I/O（MPIO；マルチパスI/O）とAsymmetric Logical Unit Access（ALUA；非対称論理ユニットアクセス）を使用する必要があります。ノードで障害が発生した場合、LIF は障害が発生したパートナーノードの IP アドレスを引き継ぎません。代わりに、MPIO ソフトウェアが、ホストの ALUA を使用して、LIF 経由で LUN にアクセスするための適切なパスを選択します。

HA ペアの各ノードから 1 つ以上の iSCSI パスを作成し、HA ペアで処理する LUN に論理インターフェイス（LIF）を使用してアクセスできるようにする必要があります。SAN をサポートする Storage Virtual Machine（SVM）ごとに管理 LIF を 1 つ設定する必要があります。

直接接続またはイーサネットスイッチの使用がサポートされています。両方のタイプの接続用にLIFを作成する必要があります。

- SAN をサポートする Storage Virtual Machine（SVM）ごとに管理 LIF を 1 つ設定する必要があります。ノードごとに 2 つの LIF を設定できます。LIF は、iSCSI 用のイーサネットネットワークを分離するために、FC で使用するファブリックごとに 1 つずつ使用します。

作成したLIFは、ポートセットから削除したり、Storage Virtual Machine (SVM) 内の別のノードに移動したり、LIFを削除したりできます。

#### 関連情報

- ["LIFを上書き設定"](#)
- ["LIF を作成"](#)

#### NVMe LIF を設定します

NVMe LIF を設定するときは、特定の要件を満たす必要があります。

作業を開始する前に

LIF を作成する FC アダプタで NVMe がサポートされている必要があります。サポートされているアダプタについては、["Hardware Universe"](#)。

このタスクについて

ONTAP 9.12.1以降では、ノードごとに最大12ノードのNVMe LIFを2つ設定できます。ONTAP 9.11.1以前では、ノードあたり2つのNVMe LIFを、最大2つのノードで設定できます。

NVMe LIF を作成するときのルールは次のとおりです。

- データ LIF で使用できるデータプロトコルは NVMe のみです。
- SAN をサポートする SVM ごとに管理 LIF を 1 つ設定する必要があります。
- ONTAP 9.5以降では、ネームスペースを含むノードとそのHAパートナーにNVMe LIFを設定する必要があります。
- ONTAP 9.4 のみ：
  - NVMe の LIF とネームスペースは、同じノードでホストする必要があります。
  - 設定できる NVMe データ LIF は SVM ごとに 1 つだけです。

#### 手順

1. LIF を作成します。

```
network interface create -vserver <SVM_name> -lif <LIF_name> -role  
<LIF_role> -data-protocol {fc-nvme|nvme-tcp} -home-node <home_node>  
-home-port <home_port>
```



NVMe/TCPはONTAP 9.10.1以降で使用できます。

2. LIF が作成されたことを確認します。

```
network interface show -vserver <SVM_name>
```

作成後、NVMe/TCP LIFはポート8009で検出をリスンします。

## SAN LIFを移動する前に理解しておくべきこと

クラスタにノードを追加したりクラスタからノードを削除するなど、クラスタの構成を変更する場合は、LIF を移動するだけで済みます。LIF を移動すれば、FC ファブリックを再ゾーニングしたり、クラスタに接続されたホストとその新しいターゲットインターフェイスとの間に新しい iSCSI セッションを作成したりする必要がありません。

を使用してSAN LIFを移動することはできません `network interface move` コマンドを実行しますSAN LIF を移動するには、まず目的の LIF をオフラインにし、別のホームノードやポートに移動させてから、移動先の新しい場所で LIF をオンラインに戻します。Asymmetric Logical Unit Access（ALUA；非対称論理ユニットアクセス）は、任意の ONTAP 解決策の一部として冗長パスと自動選択を提供します。このため、移動時に LIF がオフライン状態になっても、I/O の中断は生じません。ホストは再試行してから、I/O を別の LIF に移動するだけです。

LIF の移動を使用すると、システムを停止することなく次の操作を実行できます。

- クラスタの 1 つの HA ペアを、LUN データにアクセスするホストにはまったく支障のない形で、アップグレードした HA ペアに置き換えます
- ターゲットインターフェイスカードをアップグレードします
- Storage Virtual Machine（SVM）のリソースをクラスタ内のノードセットから別のノードセットに移行する

## ポートセットから **SAN LIF** を削除する

削除または移動する LIF がポートセットに含まれている場合、LIF を削除または移動する前に、ポートセットから LIF を削除する必要があります。

### このタスクについて

次の手順の手順 1 は、LIF が 1 つだけポートセットにある場合にのみ実行する必要があります。ポートセットがイニシエータグループにバインドされている場合、そのポートセット内の最後の LIF は削除できません。複数の LIF がポートセットにある場合は、手順 2 から開始できます。

### 手順

1. ポートセットにLIFが1つしかない場合は、を使用します `lun igroup unbind` イニシエータグループからポートセットのバインドを解除するコマンド。



イニシエータグループとポートセットのバインドを解除すると、イニシエータグループ内のすべてのイニシエータは、すべてのネットワークインターフェイス上の、そのイニシエータグループにマッピングされたすべてのターゲット LUN にアクセスできるようになります。

```
cluster1::>lun igroup unbind -vserver vs1 -igroup ig1
```

2. を使用します `lun portset remove` コマンドを使用してポートセットからLIFを削除します。

```
cluster1::> port set remove -vserver vs1 -portset ps1 -port-name lif1
```

## SAN LIF を移動します

ノードをオフラインにする必要がある場合、SAN LIF を移動して WWPN などの設定情報を保持しておけば、スイッチファブリックの再ゾーニングを行わずに済みます。SAN LIF は移動前にオフラインにする必要があるため、ホストトラフィックについては、ホストマルチパスソフトウェアを使用して、LUN への無停止アクセスを確保する必要があります。SAN LIF はクラスタ内の任意のノードに移動できますが、SAN LIF を別の Storage Virtual Machine (SVM) に移動することはできません。

### 必要なもの

LIF がポートセットのメンバーである場合、LIF を別のノードに移動する前に、その LIF をポートセットから削除しておく必要があります。

### このタスクについて

移動する LIF のデスティネーションノードおよび物理ポートは、同じ FC ファブリック上またはイーサネットネットワーク上に存在する必要があります。適切にゾーニングされていない別のファブリック上に LIF を移動したり、iSCSI イニシエータとターゲットを接続していないイーサネットネットワーク上に LIF を移動したりすると、その LIF をオンラインに戻しても接続できなくなります。

### 手順

1. LIF の管理ステータスと動作ステータスを表示します。

```
network interface show -vserver vservice_name
```

2. LIF のステータスを `down` に変更します (オフライン) :

```
network interface modify -vserver vservice_name -lif LIF_name -status-admin down
```

3. LIF を新しいノードとポートに割り当てます。

```
network interface modify -vserver vservice_name -lif LIF_name -home-node node_name -home-port port_name
```

4. LIF のステータスを `up` に変更します (オンライン) :

```
network interface modify -vserver vservice_name -lif LIF_name -status-admin up
```

5. 変更内容を確認します。

```
network interface show -vserver vservice_name
```

## SAN 環境の LIF を削除する

LIF を削除する前に、LIF に接続しているホストが、別のパスを介して LUN にアクセスできることを確認してください。

### 必要なもの


削除する LIF がポートセットのメンバーである場合、LIF を削除する前に、まずポートセットから LIF を削除

する必要があります。

### System Manager の略

ONTAP System Manager (9.7以降) を使用してLIFを削除します。

#### 手順

1. System Managerで、\* Network > Overview をクリックし、Network Interfaces \*を選択します。
2. LIFを削除するStorage VMを選択します。
3. をクリックします  をクリックし、\* Delete \* を選択します。

### CLI の使用

ONTAP CLIを使用してLIFを削除する

#### 手順

1. 削除する LIF の名前と現在のポートを確認します。

```
network interface show -vserver vs1
```

2. LIF を削除します。

```
network interface delete
```

```
network interface delete -vserver vs1 -lif lif1
```

3. LIF が削除されたことを確認します。

```
network interface show
```

```
network interface show -vserver vs1
```

Logical Status	Network	Current	Current Is
Vserver Interface	Admin/Oper	Node	Port
Home			
-----	-----	-----	-----
vs1			
lif2	up/up	192.168.2.72/24	node-01 e0b
true			
lif3	up/up	192.168.2.73/24	node-01 e0b
true			

クラスタにノードを追加するための**SAN LIF**の要件

クラスタにノードを追加する場合は、一定の考慮事項について理解しておく必要があります。

- 新しいノードに LUN を作成する前に、必要に応じてそれらのノードに LIF を作成する必要があります。
- ホストスタックとプロトコルの指示に従って、作成した LIF をホストから検出する必要があります。
- クラスタインターコネクトネットワークを使用しないでも LUN やボリュームを移動できるようにするには、新しいノード上に LIF を作成する必要があります。

ホストによる **iSCSI SendTargets** 検出処理に対して **FQDN** を返すように **iSCSI LIF** を設定します

ONTAP 9 以降では、ホスト OS から送信された iSCSI SendTargets 検出処理に対して Fully Qualified Domain Name（FQDN；完全修飾ドメイン名）を返すように iSCSI LIF を設定できます。FQDN を返すように設定すると、ホスト OS とストレージサービスの間にネットワークアドレス変換（NAT）デバイスがある場合に便利です。

このタスクについて

IP アドレスは NAT デバイスを挟んだ反対側では認識されませんが、FQDN であれば両方で認識されます。



FQDN 値の互換性のある最大文字数は、すべてのホスト OS で 128 文字です。

手順

1. 権限の設定を advanced に変更します。

```
set -privilege advanced
```

2. FQDN を返すように iSCSI LIF を設定します。

```
vserver iscsi interface modify -vserver SVM_name -lif iscsi_LIF_name
-sendtargets_fqdn FQDN
```

次の例では、FQDN として storagehost-005.example.com を返すように iSCSI LIF を設定しています。

```
vserver iscsi interface modify -vserver vs1 -lif vs1_iscsi1 -sendtargets-fqdn
storagehost-005.example.com
```

3. sendtargets が FQDN になっていることを確認します。

```
vserver iscsi interface show -vserver SVM_name -fields sendtargets-fqdn
```

この例では、sendtargets-fqdn 出力フィールドに storagehost-005.example.com が表示されています。

```
cluster::vserver*> vserver iscsi interface show -vserver vs1 -fields
sendtargets-fqdn
vserver lif          sendtargets-fqdn
-----
vs1      vs1_iscsi1  storagehost-005.example.com
vs1      vs1_iscsi2  storagehost-006.example.com
```

関連情報

## 推奨されるボリュームとファイルまたは LUN の設定の組み合わせ

推奨されるボリュームとファイルまたは LUN の設定の組み合わせの概要

使用可能な FlexVol の設定とファイルまたは LUN の設定の組み合わせは、使用するアプリケーションと管理要件によって異なります。これらの組み合わせのメリットとデメリットを理解しておく、環境に適したボリュームと LUN の設定の組み合わせを決定する際に役立ちます。

推奨されるボリュームと LUN の設定の組み合わせは次のとおりです。

- スペースリザーブファイルまたはスペースリザーブ LUN とシックボリュームプロビジョニング
- スペースリザーブなしのファイルまたはスペースリザーブなしの LUN とシンボリュームプロビジョニング
- スペースリザーブファイルまたはスペースリザーブ LUN とセミシックボリュームプロビジョニング

これらのいずれかの設定の組み合わせとともに、LUN で SCSI シンプロビジョニングを使用できます。

スペースリザーブファイルまたはスペースリザーブ LUN とシックボリュームプロビジョニング

- 利点 :\*
- スペースリザーブファイルでのすべての書き込み処理が保証されます。スペース不足のために失敗することはありません。
- ボリュームでの Storage Efficiency テクノロジとデータ保護テクノロジに関する制限はありません。
- コストと制限 : \*
- シックプロビジョニングボリュームをサポートするための十分なスペースをアグリゲートから事前に確保しておく必要があります。
- LUN 作成時に、LUN の 2 倍のサイズのスペースがボリュームから割り当てられます。

スペースリザーブなしのファイルまたはスペースリザーブなしの LUN とシンボリュームプロビジョニング

- 利点 :\*
- ボリュームでの Storage Efficiency テクノロジとデータ保護テクノロジに関する制限はありません。
- スペースは使用時に初めて割り当てられます。
- 費用および制限 :\*
- 書き込み処理は保証されず、ボリュームの空きスペースが不足すると失敗する場合があります。
- アグリゲートの空きスペースを効果的に管理して、空きスペースが不足しないようにする必要があります。

スペースリザーブファイルまたはスペースリザーブ LUN とセミシックボリュームプロビジョニング

- 利点 :\*



事前に確保されるスペースがシックボリュームプロビジョニングの場合よりも少なく、ベストエフォートの書き込み保証も提供されます。

- 費用および制限 :\*
- このオプションを指定すると、書き込み処理が失敗することがあります。

このリスクは、ボリュームの空きスペースとデータの揮発性の適切なバランスを維持することで軽減できます。

- Snapshot コピー、FlexClone ファイル、FlexClone LUN などのデータ保護オブジェクトは保持できません。
- 重複排除、圧縮、ODX / コピーオフロードなど、自動で削除できない ONTAP のブロック共有ストレージ効率化機能は使用できません。

環境に適したボリュームと **LUN** の構成の組み合わせを決定します

環境に関するいくつかの基本的な質問に答えることで、環境に最も適した FlexVol ボリュームと LUN の設定を決定できます。

このタスクについて

LUN とボリュームの設定は、ストレージ利用率を最大限に高めるため、または書き込みを確実に保証するために最適化することができます。ストレージの利用要件と、空きスペースを監視し迅速に補充するための要件に基づいて、ご使用の環境に適した FlexVol ボリュームと LUN ボリュームを決める必要があります。



LUN ごとに個別のボリュームを設定する必要はありません。

ステップ

1. 次のデシジョンツリーを使用して、環境に最も適したボリュームと LUN の設定の組み合わせを決定してください。



LUN のデータの増加率を計算します

スペースリザーブ LUN とスペースリザーブなしの LUN のどちらが適切かを判断するには、時間の経過に伴う LUN データの増加率を把握する必要があります。

このタスクについて

データの増加率が一定して高い場合、スペースリザーブ LUN の使用が適しています。データの増加率が低い場合は、スペースリザーブなしの LUN を検討してください。

OnCommand Insight などのツールを使用してデータの増加率を計算することも、手動で計算することもできます。手動計算の手順を次に示します。

手順

1. スペースリザーブ LUN をセットアップします。
2. 一定期間、たとえば 1 週間、LUN 上のデータを監視します。

データの増加が定期的に発生する代表的なサンプルを形成するために、十分な監視期間を確保してください。たとえば、毎月末には大量のデータが常に増加する可能性があります。

3. 毎日、増加したデータの量を GB 単位で記録します。
4. 監視期間の最後に、1 日ごとの合計を合算し、監視期間中の総日数で割ります。

この計算で、平均増加率が導かれます。

例

この例では、200GB の LUN が必要です。1 週間 LUN を監視し、毎日のデータの変更を記録しました。記録は次のとおりです。

- 日曜日：20GB
- 月曜日：18GB
- 火曜日：17GB
- 水曜日：20GB
- 木曜日：20GB
- 金曜日：23GB
- 土曜日：22GB

この例では、増加率は  $(20+18+17+20+20+23+22) / 7$  で求めることができ、1 日あたり 20GB となります。

スペースリザーブファイルまたはスペースリザーブ **LUN** とシックプロビジョニングボリュームを組み合わせた場合の構成設定

この FlexVol とファイルまたは LUN の設定の組み合わせでは、Storage Efficiency テクノロジーを使用できます。また、事前に十分なスペースが割り当てられるため、空きスペースを能動的に監視する必要がありません。

シックプロビジョニングを使用するボリュームでスペースリザーブファイルまたはスペースリザーブ LUN を設定するには、次の設定が必要です。

音量設定	価値
保証	ボリューム
フラクショナルリザーブ	100
Snapshot リザーブ	任意
Snapshot の自動削除	任意。
自動拡張	オプション。有効にした場合は、アグリゲートの空きスペースを能動的に監視する必要があります。

ファイルまたは <b>LUN</b> の設定	価値
スペースリザーベーション	有効

スペースリザーブなしのファイルまたはスペースリザーブなしの **LUN** とシンプロビジョニングボリュームを組み合わせた場合の構成設定

この FlexVol とファイルまたは LUN の設定の組み合わせでは、事前に割り当てられるス

ストレージの量が最小になりますが、スペース不足によるエラーを回避するために空きスペースを能動的に管理する必要があります。

シンプロビジョニングボリュームでスペースリザーブなしのファイルまたはスペースリザーブなしの LUN を設定するには、次の設定が必要です。

音量設定	価値
保証	なし
フラクショナルリザーブ	0
Snapshot リザーブ	任意
Snapshot の自動削除	任意。
自動拡張	任意。

ファイルまたは <b>LUN</b> の設定	価値
スペースリザーベーション	無効

その他の考慮事項については

ボリュームまたはアグリゲートのスペースが不足すると、ファイルまたは LUN への書き込み処理が失敗する場合があります。

ボリュームとアグリゲートの両方の空きスペースを能動的に監視しない場合は、ボリュームの自動拡張を有効にして、ボリュームの最大サイズをアグリゲートのサイズに設定してください。この設定では、アグリゲートの空きスペースを能動的に監視する必要がありますが、ボリュームの空きスペースを監視する必要はありません。

スペースリザーブファイルまたはスペースリザーブ **LUN** とセミシックボリュームプロビジョニングを組み合わせた場合の構成設定

この FlexVol とファイルまたは LUN の設定の組み合わせでは、フルプロビジョニングとの組み合わせに比べて事前に割り当てるストレージが少なく済みますが、ボリュームに使用できる効率化テクノロジーが制限されます。この設定の組み合わせでは、上書きがベストエフォートベースで行われます。

セミシックプロビジョニングを使用するボリュームでスペースリザーブ LUN を設定するには、次の設定が必要です。

音量設定	価値
保証	ボリューム

音量設定	価値
フラクショナルリザーブ	0
Snapshot リザーブ	0
Snapshot の自動削除	オン。この場合、コミットメントレベルを destroy に設定し、削除リストにすべてのオブジェクトを追加し、トリガーを volume に設定し、すべての FlexClone LUN と FlexClone ファイルの自動削除を有効にします。
自動拡張	オプション。有効にした場合は、アグリゲートの空きスペースを能動的に監視する必要があります。

ファイルまたは <b>LUN</b> の設定	価値
スペースリザーベーション	有効

#### テクノロジーの制限事項

この設定の組み合わせでは、次のボリュームの Storage Efficiency テクノロジーを使用できません。

- 圧縮
- 重複排除
- ODX コピーオフロードと FlexClone コピーオフロード
- 自動削除の対象としてマークされていない FlexClone LUN と FlexClone ファイル（アクティブクローン）
- FlexClone サブファイル
- ODX / コピーオフロード

その他の考慮事項については

この設定の組み合わせを使用する場合は、次の点を考慮する必要があります。

- 対象の LUN をサポートするボリュームのスペースが不足した場合は、保護データ（FlexClone LUN、FlexClone ファイル、および Snapshot コピー）が削除されます。
- ボリュームの空きスペースが不足すると、書き込み処理がタイムアウトして失敗することがあります。

AFF プラットフォームではデフォルトで圧縮が有効になります。AFF プラットフォームのセミシックプロビジョニングを使用するボリュームに対しては、明示的に圧縮を無効にする必要があります。

## SANのデータ保護

## SAN 環境でのデータ保護方法の概要

データを保護するには、データのコピーを作成して、誤ってデータを削除した場合、アプリケーションがクラッシュした場合、データが破損した場合、災害が発生した場合にそのコピーをリストアできるようにします。データ保護およびバックアップのニーズに応じて、ONTAP では、データを保護するためのさまざまな方法を提供しています。

### SnapMirror のビジネス継続性（SM-BC）

ONTAP 9.9.1の一般提供開始以降では、目標復旧時間ゼロ（ゼロRTO）または透過的アプリケーションフェイルオーバー（TAF）によって、SAN環境でビジネスクリティカルなアプリケーションを自動的にフェイルオーバーできます。SM-BCを使用するには、2つのAFFクラスタまたは2つのオールフラッシュSANアレイ（ASA）クラスタを使用する構成にONTAPメディエーター1.2がインストールされている必要があります。

["ネットアップのマニュアル：SnapMirror Business Continuity"](#)

### Snapshot コピー

LUN の複数のバックアップを手動または自動で作成、スケジュール、および保守できます。Snapshot コピーは、最小限のボリュームスペースしか使用せず、パフォーマンスコストもかかりません。LUN データを誤って変更または削除した場合は、最新のいずれかの Snapshot コピーからデータをすばやく簡単にリストアできます。

### FlexClone LUN（FlexClone のライセンスが必要）

アクティブボリューム内や Snapshot コピー内にある別の LUN の書き込み可能なポイントインタイムコピーを提供します。クローンとその親は、相互に影響を及ぼさずに個別に変更できます。

### SnapRestore（ライセンスが必要）

ボリューム全体の Snapshot コピーから高速かつスペース効率に優れたデータリカバリを必要に応じて実行できます。SnapRestore を使用すると、ストレージシステムをリブートしなくても、LUN を以前保存した状態にリストアできます。

### データ保護ミラーコピー（SnapMirror のライセンスが必要）

非同期のディザスタリカバリを提供します。そのために、ボリューム上にあるデータの Snapshot コピーを定期的に作成し、それらの Snapshot コピーを通常は別のクラスタ上にあるパートナーボリュームにローカルエリアネットワークまたはワイドエリアネットワーク経由でコピーして保持します。ソースボリューム上のデータが破損した場合や失われた場合には、パートナーボリューム上のミラーコピーにより、最新の Snapshot コピーの時点におけるデータをすぐに使用およびリストアすることができます。

### SnapVault バックアップ（SnapMirror のライセンスが必要）

ストレージ効率に優れた、長期間保持できるバックアップを提供します。SnapVault 関係により、ボリュームの選択した Snapshot コピーをデスティネーションボリュームにバックアップし、保持することができます。

テープバックアップおよびアーカイブ処理を行っている場合は、SnapVault セカンダリボリュームにすでにバックアップされているデータに対してそれらの処理を実行できます。

## SnapDrive for Windows または UNIX （ SnapDrive ライセンスが必要）

LUN へのアクセスを設定し、LUN を管理し、ストレージシステムの Snapshot コピーを Windows ホストまたは UNIX ホストから直接管理します。

### ネイティブテープバックアップ / リカバリ

ONTAP はほとんどの既存のテープドライブに対応しており、テープベンダーが新しいデバイスのサポートを動的に追加するための方策も用意されています。ONTAP は Remote Magnetic Tape （ RMT ） プロトコルもサポートしているため、RMT 対応システムへのバックアップやリカバリも可能です。

### 関連情報

["ネットアップのマニュアル： SnapDrive for UNIX"](#)

["ネットアップのマニュアル： SnapDrive for Windows （現在のリリース）"](#)

["テープバックアップによるデータ保護"](#)

## LUN の移動またはコピーが Snapshot コピーに及ぼす影響

### LUN の移動またはコピーが Snapshot コピーに及ぼす影響の概要

Snapshot コピーはボリュームレベルで作成します。LUN を別のボリュームにコピーまたは移動すると、デスティネーションボリュームの Snapshot コピーポリシーがコピーまたは移動されたボリュームに適用されます。デスティネーションボリュームの Snapshot コピーが確立されていない場合、移動またはコピーされた LUN の Snapshot コピーは作成されません。

### Snapshot コピーから単一の LUN をリストアします

ボリューム全体をリストアすることなく、ボリューム内の単一 LUN のみを Snapshot コピーからリストアできます。LUN は、元の場所またはボリューム内の新しいパスにリストアできます。この処理では、ボリューム内の他のファイルまたは LUN に影響を与えることなく、単一の LUN だけがリストアされます。ファイルは、ストリームを使用してリストアすることもできます。

### 必要なもの

- リストア処理を完了するには、ボリュームに十分なスペースが必要です。
  - フラクショナルリザーブが 0% のスペースリザーブ LUN をリストアする場合、リストアする LUN と同じサイズのスペースが必要です。
  - フラクショナルリザーブが 100% のスペースリザーブ LUN をリストアする場合、リストアする LUN の 2 倍のサイズのスペースが必要です。
  - スペースリザーブなしの LUN をリストアする場合、リストアする LUN が実際に使用しているスペースのみが必要です。
- デスティネーション LUN の Snapshot コピーを作成しておく必要があります。

リストア処理が失敗すると、デスティネーション LUN が切り捨てられる可能性があります。このような

場合は、Snapshot コピーを使用してデータ損失を防ぐことができます。

- ソース LUN の Snapshot コピーを作成しておく必要があります。

まれに、LUN のリストアに失敗したときに、ソース LUN が使用不能になることがあります。この場合、Snapshot コピーを使用して、リストアを試みる直前の状態に LUN を復帰させることができます。

- デスティネーション LUN とソース LUN の OS タイプが同じである必要があります。

デスティネーション LUN の OS タイプがソース LUN の OS タイプと異なる場合は、リストア処理後、ホストからデスティネーション LUN へのデータアクセスが失われる可能性があります。

## 手順

1. ホストから、LUN へのホストアksesをすべて停止します。
2. ホスト上の LUN をアンマウントして、ホストが LUN にアクセスできないようにします。
3. LUN のマッピングを解除します。

```
lun mapping delete -vserver vservice_name -volume volume_name -lun lun_name  
-igroup igroup_name
```

4. LUN のリストア先にする Snapshot コピーを決定します。

```
volume snapshot show -vserver vservice_name -volume volume_name
```

5. LUN をリストアする前に、LUN の Snapshot コピーを作成します。

```
volume snapshot create -vserver vservice_name -volume volume_name -snapshot  
snapshot_name
```

6. ボリューム内の指定した LUN をリストアします。

```
volume snapshot restore-file -vserver vservice_name -volume volume_name  
-snapshot snapshot_name -path lun_path
```

7. 画面の手順に従います。
8. 必要に応じて、LUN をオンラインにします。

```
lun modify -vserver vservice_name -path lun_path -state online
```

9. 必要に応じて、LUN を再マッピングします。

```
lun mapping create -vserver vservice_name -volume volume_name -lun lun_name  
-igroup igroup_name
```

10. ホストから、LUN を再マウントします。
11. ホストから、LUN へのアクセスを再開します。



## Snapshot コピーからボリューム内のすべての LUN をリストアします

を使用できます `volume snapshot restore` 指定したボリューム内のすべてのLUNをSnapshotコピーからリストアするコマンド。

### 手順

1. ホストから、LUN へのホストアクセスをすべて停止します。

SnapRestore を使用している場合は、ボリューム内の LUN へのすべてのホストアクセスを停止しないと、原因によるデータの破損やシステムエラーが発生する可能性があります

2. ホスト上の LUN をアンマウントして、ホストが LUN にアクセスできないようにします。
3. LUN のマッピングを解除します。

```
lun mapping delete -vserver vservice_name -volume volume_name -lun lun_name  
-igroup igroup_name
```

4. ボリュームのリストア先にする Snapshot コピーを決定します。

```
volume snapshot show -vserver vservice_name -volume volume_name
```

5. 権限の設定を `advanced` に変更します。

```
set -privilege advanced
```

6. データをリストアします。

```
volume snapshot restore -vserver vservice_name -volume volume_name -snapshot  
snapshot_name
```

7. 画面の指示に従います。

8. LUN を再マッピングします。

```
lun mapping create -vserver vservice_name -volume volume_name -lun lun_name  
-igroup igroup_name
```

9. LUN がオンラインであることを確認します。

```
lun show -vserver vservice_name -path lun_path -fields state
```

10. LUN がオンラインになっていない場合は、オンラインにします。

```
lun modify -vserver vservice_name -path lun_path -state online
```

11. 権限の設定を `admin` に変更します。

```
set -privilege admin
```

12. ホストから、LUN を再マウントします。

13. ホストから、LUN へのアクセスを再開します。

ボリュームから既存の **Snapshot** コピーを削除します

ボリュームから既存の Snapshot コピーを手動で削除できます。この処理は、ボリュームのスペースを増やす必要がある場合などに実行します。

手順

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

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

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

10 entries were displayed.

- 2. を使用します `volume snapshot delete` Snapshotコピーを削除するコマンド。

状況	入力するコマンド
1 つの Snapshot コピーを削除します	<code>volume snapshot delete -vserver svm_name -volume vol_name -snapshot snapshot_name</code>
複数の Snapshot コピーを削除する	<code>volume snapshot delete -vserver svm_name -volume vol_name -snapshot snapshot_name1[, snapshot_name2,...]</code>
すべての Snapshot コピーを削除します	<code>volume snapshot delete -vserver svm_name -volume vol_name -snapshot *</code>

次の例は、ボリューム vol3 上のすべての Snapshot コピーを削除します。

```
cluster::> volume snapshot delete -vserver vs3 -volume vol3 *  
  
10 entries were acted on.
```

## FlexClone LUN を使用してデータを保護します

### FlexClone LUN を使用してデータの概要を保護します

FlexClone LUN は、アクティブボリューム内や Snapshot コピー内にある別の LUN の書き込み可能なポイントインタイムコピーです。クローンとその親は、相互に影響を及ぼさずに個別に変更できます。

FlexClone LUN は、最初は親 LUN とスペースを共有します。デフォルトでは、FlexClone LUN は親 LUN のスペースリザーブ属性を継承します。たとえば、親 LUN がスペースリザーブなしの場合は、FlexClone LUN もデフォルトでスペースリザーブなしになります。ただし、スペースリザーブ LUN である親から、スペースリザーブなしの FlexClone LUN を作成することもできます。

LUN クローンの作成時にはバックグラウンドでブロック共有が発生し、ブロック共有が終了するまでボリュームの Snapshot コピーは作成できません。

で FlexClone LUN の自動削除機能を有効にするには、ボリュームを設定する必要があります `volume snapshot autodelete modify` コマンドを実行します有効にしない場合、FlexClone LUN を自動削除したくても、ボリュームで FlexClone の自動削除が有効になっていないため、FlexClone LUN は削除されません。

FlexClone LUN を作成すると、FlexClone LUN の自動削除機能がデフォルトで無効になります。FlexClone LUN を自動削除できるようにするには、FlexClone LUN ごとに FlexClone LUN を手動で有効にする必要があります。ボリュームのセミシックプロビジョニングを使用している場合に、このオプションが提供する「ベストエフォート」の書き込み保証が必要な場合は、`_ALL_FlexClone LUN` を自動削除できるようにする必要があります。



Snapshot コピーから FlexClone LUN を作成すると、スペース効率に優れたバックグラウンドプロセスを使用して、LUN が自動的に Snapshot コピーからスプリットされます。そのため、LUN が Snapshot コピーに依存したり、追加スペースを消費したりすることはなくなります。このバックグラウンドスプリットが終了する前に Snapshot コピーが自動的に削除された場合、その FlexClone LUN は、FlexClone LUN の自動削除機能が無効になっていても削除されます。バックグラウンドスプリットが完了したあとは、Snapshot コピーが削除されても、FlexClone LUN は削除されません。

### 関連情報

["論理ストレージ管理"](#)

### FlexClone LUN を使用する理由

FlexClone LUN を使用すると、LUN の読み書き可能なコピーを複数作成できます。

これは、次のような場合に行います。

- テストを目的として LUN の一時的なコピーを作成する必要があります。

- 本番環境のデータへのアクセスを許可することなく、追加のユーザがデータのコピーを利用できるようにする必要があります。
- 変更および開発作業用にデータベースのクローンを作成し、元のデータを未変更のまま残す場合
- LUN データの特定のサブセット（ボリュームグループ内の特定の論理ボリュームまたはファイルシステム）にアクセスする場合。またはファイルシステム内の特定のファイルまたはファイルセット）を選択し、元の LUN の残りのデータをリストアせずに、元の LUN にコピーします。これは、LUN とその LUN クローンを同時にマウントできるオペレーティングシステムで機能します。SnapDrive for UNIXはでこれをサポートしています `snap connect` コマンドを実行します
- 同じオペレーティングシステム上に複数の SAN ブートホストが必要な場合。

自動削除設定を使用して **FlexVol** ボリュームの空きスペースを再生する方法

FlexVol の自動削除設定を有効にすると、FlexClone ファイルおよび FlexClone LUN を自動的に削除できます。自動削除を有効にすると、ボリュームがフルに近くなったときに、指定した量の空きスペースをボリューム内に再生できます。

ボリュームの空きスペースが一定のしきい値を下回ったときに FlexClone ファイルおよび FlexClone LUN の削除を自動的に開始し、ボリュームの空きスペースを指定の量だけ再生したらクローンの削除を自動的に中止するように設定できます。クローンの自動削除を開始するしきい値を指定することはできませんが、それぞれのクローンを削除対象に含めるかどうかと、ボリュームの空きスペースの目標量を指定することができます。

ボリュームの空きスペースが一定のしきい値を下回ったとき、および次の要件の両方に達したときに、FlexClone ファイルおよび FlexClone LUN が自動的に削除されます。

- FlexClone ファイルおよび FlexClone LUN が格納されているボリュームに対して自動削除機能が有効になっている。

FlexVol に対して自動削除機能を有効にするには、を使用します `volume snapshot autodelete modify` コマンドを実行します。設定する必要があります `-trigger` パラメータの値 `volume` または `snap_reserve` ボリュームが FlexClone ファイルおよび FlexClone LUN を自動的に削除するように設定します。

- FlexClone ファイルおよび FlexClone LUN に対して自動削除機能が有効になっている。

FlexClone ファイルまたは FlexClone LUN に対して自動削除を有効にするには、を使用します `file clone create` コマンドにを指定します `-autodelete` パラメータこのクローン設定はボリュームの他の設定よりも優先されるため、この設定で個別に自動削除を無効にすることで、特定の FlexClone ファイルや FlexClone LUN を保持することができます。

**FlexClone** ファイルおよび **FlexClone LUN** を自動的に削除するように **FlexVol** を設定する

ボリュームの空きスペースが特定のしきい値を下回った場合に、自動削除を有効にした FlexClone ファイルおよび FlexClone LUN を自動的に削除するように FlexVol を設定できます。

必要なもの

- FlexVol ボリュームに FlexClone ファイルおよび FlexClone LUN が含まれていて、オンラインになっている必要があります。

- FlexVol ボリュームを読み取り専用ボリュームにすることはできません。

## 手順

1. を使用して、FlexVol ボリューム内のFlexCloneファイルおよびFlexClone LUNの自動削除を有効にします  
volume snapshot autodelete modify コマンドを実行します

- をクリックします -trigger パラメータを指定することもできます volume または snap\_reserve。
- をクリックします -destroy-list パラメータは常に指定する必要があります lun\_clone, file\_clone 削除するクローンのタイプが1つだけであるかどうかは関係ありません。  
[+]

次の例は、ボリューム vol1 で FlexClone ファイルおよび FlexClone LUN の自動削除を有効にし、ボリュームの 25% が空きスペースになるまでスペースが再生されるようにします。

```
cluster1::> volume snapshot autodelete modify -vserver vs1 -volume
vol1 -enabled true -commitment disrupt -trigger volume -target-free
-space 25 -destroy-list lun_clone,file_clone
```

```
Volume modify successful on volume:vol1
```



FlexVol ボリュームの自動削除を有効にする際に、の値を設定した場合 -commitment パラメータの値 destroy`を使用して、すべてのFlexCloneファイルおよびFlexClone LUNを削除します`-autodelete パラメータをに設定します true ボリュームの空きスペースが指定したしきい値を下回った場合に削除されることがあります。ただし、FlexCloneファイルとFlexClone LUNはを使用します -autodelete パラメータをに設定します false は削除されません。

2. を使用して、FlexVol ボリュームでFlexCloneファイルおよびFlexClone LUNの自動削除が有効になっていることを確認します volume snapshot autodelete show コマンドを実行します

次の例では、ボリューム vol1 で FlexClone ファイルおよび FlexClone LUN の自動削除が有効になっています。

```
cluster1::> volume snapshot autodelete show -vserver vs1 -volume vol1
```

```

Vserver Name: vs1
Volume Name: vol1
Enabled: true
Commitment: disrupt
Defer Delete: user_created
Delete Order: oldest_first
Defer Delete Prefix: (not specified)*
Target Free Space: 25%
Trigger: volume
Destroy List: lun_clone,file_clone
Is Constituent Volume: false
```

3. 次の手順を実行して、ボリューム内の削除対象とする FlexClone ファイルおよび FlexClone LUN の自動削除を有効にします。

- a. を使用して、特定の FlexClone ファイルまたは FlexClone LUN の自動削除を有効にします `volume file clone autodelete` コマンドを実行します

を使用して、特定の FlexClone ファイルまたは FlexClone LUN を強制的に自動削除することができます `volume file clone autodelete` コマンドに `-force` パラメータ

次の例は、ボリューム `vol1` に含まれる FlexClone LUN `lun1_clone` の自動削除が有効になっていることを示します。

```
cluster1::> volume file clone autodelete -vserver vs1 -clone-path  
/vol/vol1/lun1_clone -enabled true
```

FlexClone ファイルおよび FlexClone LUN の作成時に自動削除を有効にすることができます。

- b. を使用して、FlexClone ファイルまたは FlexClone LUN で自動削除が有効になっていることを確認します `volume file clone show-autodelete` コマンドを実行します

次の例は、FlexClone LUN `lun1_clone` で自動削除が有効になっていることを示します。

```
cluster1::> volume file clone show-autodelete -vserver vs1 -clone  
-path vol/vol1/lun1_clone  
  
Name: vs1  
Path: vol/vol1/lun1_clone  
  
**Autodelete Enabled: true**
```

コマンドの使用の詳細については、該当するマニュアルページを参照してください。

アクティブボリュームから **LUN** のクローンを作成します

アクティブボリュームの LUN をクローニングして、LUN のコピーを作成できます。こうして作成された FlexClone LUN は、アクティブボリューム内の元の LUN の読み書き可能なコピーです。

必要なもの

FlexClone ライセンスがインストールされている必要があります。このライセンスには、["ONTAP One"](#)。

このタスクについて

スペースリザーブされた FlexClone LUN には、親のスペースリザーブ LUN と同量のスペースが必要です。FlexClone LUN のスペースをリザーブしない場合は、FlexClone LUN に対する変更を保存するために十分なスペースがボリュームにあることを確認する必要があります。

## 手順

1. クローンを作成する前に、LUN が igroup にマッピングされていないこと、またはに書き込まれていないことを確認する必要があります。
2. を使用します `lun show` コマンドを実行してLUNが存在することを確認します。

```
lun show -vserver vs1
```

Vserver	Path	State	Mapped	Type	Size
vs1	/vol/vol1/lun1	online	unmapped	windows	47.07MB

3. を使用します `volume file clone create` コマンドを使用してFlexClone LUNを作成します。

```
volume file clone create -vserver vs1 -volume vol1 -source-path lun1  
-destination-path/lun1_clone
```

FlexClone LUNを自動削除に使用できるようにする必要がある場合は、を含めます `-autodelete true`。セミシックプロビジョニングを使用してこの FlexClone LUN をボリューム内に作成する場合は、すべての FlexClone LUN で自動削除を有効にする必要があります。

4. を使用します `lun show` コマンドを実行して、LUNが作成されたことを確認します。

```
lun show -vserver vs1
```

Vserver	Path	State	Mapped	Type	Size
vs1	/vol/volX/lun1	online	unmapped	windows	47.07MB
vs1	/vol/volX/lun1_clone	online	unmapped	windows	47.07MB

## ボリューム内の **Snapshot** コピーから **FlexClone LUN** を作成します

ボリューム内の Snapshot コピーを使用して、LUN の FlexClone コピーを作成できます。LUN の FlexClone コピーは読み書き可能です。

### 必要なもの

FlexClone ライセンスがインストールされている必要があります。このライセンスは、["ONTAP One"](#)。

### このタスクについて

FlexClone LUN は、親 LUN のスペースリザーベーション属性を継承します。スペースリザーブされた FlexClone LUN には、親のスペースリザーブ LUN と同量のスペースが必要です。FlexClone LUN のスペースをリザーブしない場合は、クローンに対する変更を保存するために十分なスペースがボリュームに必要です。

## 手順

1. LUN がマッピングされていないか、書き込まれていないことを確認します。
2. LUN が含まれているボリュームの Snapshot コピーを作成します。

```
volume snapshot create -vserver vs1 -volume vol1 -snapshot snap1
```

クローニングする LUN の Snapshot コピー（元の Snapshot コピー）を作成する必要があります。

### 3. Snapshot コピーから FlexClone LUN を作成します。

```
file clone create -vserver vs1 -volume vol1 -source-path source_path -snapshot-name snap1 -destination-path dest_path
```

FlexClone LUNを自動削除に使用できるようにする必要がある場合は、を含めます `-autodelete true`。セミシックプロビジョニングを使用してこの FlexClone LUN をボリューム内に作成する場合は、すべての FlexClone LUN で自動削除を有効にする必要があります。

### 4. FlexClone LUN が正しいことを確認します。

```
lun show -vserver vs1
```

Vserver	Path	State	Mapped	Type	Size
vs1	/vol/vol1/lun1_clone	online	unmapped	windows	47.07MB
vs1	/vol/vol1/lun1_snap_clone	online	unmapped	windows	47.07MB

特定の **FlexClone** ファイルまたは **FlexClone LUN** を自動削除の対象から除外します

FlexClone ファイルおよび FlexClone LUN を自動的に削除するように FlexVol を設定すると、指定した条件を満たすすべてのクローンが削除される可能性があります。特定の FlexClone ファイルまたは FlexClone LUN を残したい場合は、それらを FlexClone の自動削除プロセスから除外できます。

必要なもの

FlexClone ライセンスがインストールされている必要があります。このライセンスは、["ONTAP One"](#)。

このタスクについて

FlexClone ファイルまたは FlexClone LUN を作成すると、クローンの自動削除設定がデフォルトで無効になります。自動削除を無効にした FlexClone ファイルと FlexClone LUN は、ボリュームのスペースを再生するためにクローンを自動的に削除するように FlexVol を設定しても保持されます。



を設定した場合は `commitment` ボリュームのレベルをに設定します `try` または `disrupt`。特定の FlexClone ファイルまたは FlexClone LUN を個別に保持するには、それらのクローンの自動削除を無効にします。ただし、を設定した場合 `commitment` ボリュームのレベルをに設定します `destroy` 削除リストには次のものが含まれます ``lun_clone,file_clone`` では、ボリューム設定はクローン設定よりも優先され、クローンの自動削除設定に関係なく、すべての FlexClone ファイルと FlexClone LUN が削除されます。

手順

1. を使用して、特定の FlexClone ファイルまたは FlexClone LUN を自動的に削除しないように設定します



volume file clone autodelete コマンドを実行します

次の例は、vol1 に含まれている FlexClone LUN lun1\_clone の自動削除を無効にする方法を示しています。

```
cluster1::> volume file clone autodelete -vserver vs1 -volume vol1  
-clone-path lun1_clone -enable false
```

自動削除を無効にした FlexClone ファイルまたは FlexClone LUN は、ボリュームのスペース再生を目的とした自動削除の対象になりません。

2. を使用して、FlexClone ファイルまたは FlexClone LUN で自動削除が無効になっていることを確認します  
volume file clone show-autodelete コマンドを実行します

次の例では、FlexClone LUN lun1\_clone の自動削除が false になっています。

```
cluster1::> volume file clone show-autodelete -vserver vs1 -clone-path  
vol/vol1/lun1_clone  
  
Name: vs1  
Clone Path:  
vol/vol1/lun1_clone  
Autodelete  
Enabled: false
```

## SAN 環境で SnapVault バックアップを構成して使用する

### SAN 環境での SnapVault バックアップの構成と使用の概要

SAN 環境で SnapVault を設定して使用方法は、NAS 環境の場合とほぼ同じですが、SAN 環境で LUN をリストアする場合は、いくつか特別な手順を踏む必要があります。

SnapVault バックアップには、ソースボリュームの読み取り専用コピーのセットが含まれています。SAN 環境では、必ず、個々の LUN ではなくボリューム全体を SnapVault のセカンダリボリュームにバックアップします。

LUN を含むプライマリボリュームと、SnapVault バックアップとして動作するセカンダリボリュームの間に SnapVault 関係を作成して初期化する手順は、ファイルプロトコルに使用される FlexVol ボリュームで使われる手順と同じです。この手順の詳細については、を参照してください ["データ保護"](#)。

Snapshot コピーを作成して SnapVault セカンダリボリュームにコピーする前に、LUN がバックアップされ、一貫した状態であることを確認することが重要です。Snapshot コピーの作成を SnapCenter で自動化すると、バックアップされた LUN が確実に過不足なく、元のアプリケーションで使用可能な状態になります。

SnapVault セカンダリボリュームから LUN をリストアする場合には、3 つの基本の選択肢があります。

- SnapVault セカンダリボリュームから LUN を直接マッピングし、ホストを LUN に接続して LUN の内容にアクセスできます。

この LUN は読み取り専用であり、SnapVault バックアップ内の最新の Snapshot コピーからのみマッピングできます。永続的予約およびその他の LUN のメタデータは失われます。必要に応じて、元の LUN に引き続きアクセス可能であれば、ホスト上でコピープログラムを使用して LUN の内容を元の LUN にコピーすることができます。

LUN のシリアル番号がソース LUN のものと異なります。

- SnapVault セカンダリボリューム内の任意の Snapshot コピーを、新しい読み書き可能ボリュームにクローニングします。

その後、ボリューム内の任意の LUN をマッピングし、ホストを LUN に接続して LUN の内容にアクセスできます。必要に応じて、元の LUN に引き続きアクセス可能であれば、ホスト上でコピープログラムを使用して LUN の内容を元の LUN にコピーすることができます。

- SnapVault セカンダリボリューム内の任意の Snapshot コピーから、LUN が含まれているボリューム全体をリストアできます。

ボリューム全体をリストアすると、ボリューム内のすべての LUN とすべてのファイルが置き換えられます。Snapshot コピーの作成後に作成された新しい LUN はすべて失われます。

LUN では、マッピング、シリアル番号、UUID、永続的予約が維持されます。

## SnapVault バックアップから読み取り専用の LUN コピーにアクセスする

LUN の読み取り専用コピーには、SnapVault バックアップ内の最新の Snapshot コピーからアクセスできます。LUN の ID、パス、およびシリアル番号はソース LUN のものと異なり、あらかじめマッピングしておく必要があります。永続的予約、LUN マッピング、および igroup は、SnapVault セカンダリボリュームにレプリケートされません。

### 必要なもの

- SnapVault 関係が初期化されていて、SnapVault セカンダリボリューム内の最新の Snapshot コピーに目的の LUN が含まれている必要があります。
- SnapVault バックアップがある Storage Virtual Machine (SVM) に、適切な SAN プロトコル対応の LIF が 1 個以上あり、LUN コピーへのアクセスに使用するホストからこの LIF にアクセスできることが必要です。
- SnapVault セカンダリボリュームから LUN コピーに直接アクセスする場合、SnapVault SVM に事前に igroup を作成しておく必要があります。

LUN には SnapVault セカンダリボリュームから直接アクセスできます。LUN を含むボリュームのリストアやクローニングを行う必要はありません。

### このタスクについて

SnapVault セカンダリボリュームに新しい Snapshot コピーが追加されたときに、以前の Snapshot コピーに LUN がマッピングされている場合、マッピングされた LUN の内容が変更されます。LUN は引き続き同じ ID でマッピングされますが、データは新しい Snapshot コピーから取得されます。LUN のサイズが変更された場合、一部のホストはサイズの変更を自動的に検出します。Windows ホストでは、サイズ変更を検知するためにディスクの再スキャンが必要です。

## 手順

1. を実行します `lun show` コマンドを実行して、SnapVault セカンダリボリューム内の使用可能なLUNをリスト表示します。

この例では、プライマリボリューム `srcvolA` 内の元の LUN と、 SnapVault セカンダリボリューム `dstvolB` 内のコピーされた LUN の両方が表示されています。

```
cluster::> lun show
```

Vserver	Path	State	Mapped	Type	Size
-----	-----	-----	-----	-----	-----
vserverA	/vol/srcvolA/lun_A	online	mapped	windows	300.0GB
vserverA	/vol/srcvolA/lun_B	online	mapped	windows	300.0GB
vserverA	/vol/srcvolA/lun_C	online	mapped	windows	300.0GB
vserverB	/vol/dstvolB/lun_A	online	unmapped	windows	300.0GB
vserverB	/vol/dstvolB/lun_B	online	unmapped	windows	300.0GB
vserverB	/vol/dstvolB/lun_C	online	unmapped	windows	300.0GB

```
6 entries were displayed.
```

2. 目的のホストのigroupが、 SnapVault セカンダリボリュームがあるSVM内にまだ存在していない場合は、を実行します `igroup create igroup`を作成するコマンドです。

このコマンドでは、 iSCSI プロトコルを使用する Windows ホスト用の igroup を作成します。

```
cluster::> igroup create -vserver vserverB -igroup temp_igroup
               -protocol iscsi -ostype windows
               -initiator iqn.1991-05.com.microsoft:hostA
```

3. を実行します `lun mapping create` コマンドを実行して、目的のLUNコピーをigroupにマッピングします。

```
cluster::> lun mapping create -vserver vserverB -path /vol/dstvolB/lun_A
               -igroup temp_igroup
```

4. ホストを LUN に接続し、適宜 LUN の内容にアクセスします。

## SnapVault バックアップから単一の LUN をリストアする

単一の LUN を新しい場所または元の場所にリストアできます。 SnapVault セカンダリボリューム内の任意の Snapshot コピーを使用してリストアできます。 LUN を元の場所にリストアするには、まず新しい場所にリストアしてから、元の場所にコピーします。

必要なもの

- SnapVault 関係が初期化されていて、SnapVault セカンダリボリュームに、リストアに使用する適切な Snapshot コピーが含まれている必要があります。
- SnapVault セカンダリボリュームがある Storage Virtual Machine (SVM) に、適切な SAN プロトコル対応の LIF が 1 個以上あり、LUN コピーへのアクセスに使用するホストからこの LIF にアクセスできることが必要です。
- igroup が SnapVault SVM 上にすでに存在している必要があります。

#### このタスクについて

このプロセスでは、SnapVault セカンダリボリューム内の Snapshot コピーから、読み書き可能なボリュームクローンを作成します。このクローン内の LUN を直接使用することも、必要に応じて LUN の内容を元の LUN の場所にコピーすることもできます。

クローン内の LUN のパスとシリアル番号は、元の LUN のものとは異なります。永続的予約は維持されません。

#### 手順

1. を実行します `snapmirror show` コマンドを使用して、SnapVault バックアップが含まれているセカンダリボリュームを検証します。

```
cluster::> snapmirror show
```

Source Path	Dest Type	Mirror Path	Relation State	Total Progress	Healthy	Last Updated
vserverA:srcvolA	XDP	vserverB:dstvolB	Snapmirrored Idle	-	true	-

2. を実行します `volume snapshot show` コマンドを使用して、LUNのリストア元となるSnapshotコピーを特定します。

```
cluster::> volume snapshot show
```

Vserver	Volume	Snapshot	State	Size	Total%	Used%
vserverB	dstvolB	snap2.2013-02-10_0010	valid	124KB	0%	0%
		snap1.2013-02-10_0015	valid	112KB	0%	0%
		snap2.2013-02-11_0010	valid	164KB	0%	0%

3. を実行します `volume clone create` 目的のSnapshotコピーから読み書き可能クローンを作成するコマンド。

ボリュームクローンは、SnapVault バックアップと同じアグリゲート内に作成されます。アグリゲート内

に、クローンを格納できるだけの十分なスペースが必要です。

```
cluster::> volume clone create -vserver vserverB
      -flexclone dstvolB_clone -type RW -parent-volume dstvolB
      -parent-snapshot daily.2013-02-10_0010
[Job 108] Job succeeded: Successful
```

4. を実行します `lun show` コマンドを実行して、ボリュームクローン内のLUNをリスト表示します。

```
cluster::> lun show -vserver vserverB -volume dstvolB_clone
```

Vserver	Path	State	Mapped	Type
vserverB	/vol/dstvolB_clone/lun_A	online	unmapped	windows
vserverB	/vol/dstvolB_clone/lun_B	online	unmapped	windows
vserverB	/vol/dstvolB_clone/lun_C	online	unmapped	windows

3 entries were displayed.

5. 目的のホストのigroupがSnapVault バックアップがあるSVMにまだ存在していない場合は、を実行します `igroup create` groupを作成するコマンドです。

この例では、iSCSI プロトコルを使用する Windows ホスト用の igroup を作成しています。

```
cluster::> igroup create -vserver vserverB -igroup temp_igroup
      -protocol iscsi -ostype windows
      -initiator iqn.1991-05.com.microsoft:hostA
```

6. を実行します `lun mapping create` コマンドを実行して、目的のLUNコピーをigroupにマッピングします。

```
cluster::> lun mapping create -vserver vserverB
      -path /vol/dstvolB_clone/lun_C -igroup temp_igroup
```

7. ホストを LUN に接続し、適宜 LUN の内容にアクセスします。

この LUN は読み書き可能であり、元の LUN の代わりに使用できます。LUN のシリアル番号が異なるため、ホストはこの LUN が元の LUN とは別の LUN であると解釈します。

8. ホスト上でコピープログラムを使用して、LUN の内容を元の LUN にコピーします。

ボリューム内のすべての **LUN** を **SnapVault** バックアップからリストアします

ボリューム内の 1 つ以上の LUN を SnapVault バックアップからリストアする必要があります

る場合は、ボリューム全体をリストアできます。ボリュームをリストアする場合は、ボリューム内のすべての LUN が対象になります。

#### 必要なもの

SnapVault 関係が初期化されていて、SnapVault セカンダリボリュームに、リストアに使用する適切な Snapshot コピーが含まれている必要があります。

#### このタスクについて

ボリューム全体をリストアすると、ボリュームの状態は、リストアに使用した Snapshot コピーが作成された時点の状態に戻ります。Snapshot コピーの作成後にボリュームに追加された LUN がある場合、その LUN はリストアの過程で削除されます。

ボリュームのリストア後も、LUN と igroup とのマッピングはリストアの直前と同じ状態が維持されます。LUN のマッピングは、Snapshot コピー作成時点のマッピングとは異なる場合があります。ホストクラスタによる LUN の永続的予約は維持されます。

#### 手順

1. ボリューム内のすべての LUN に対する I/O を停止します。
2. を実行します `snapmirror show` コマンドを実行して、SnapVault セカンダリボリュームが含まれているセカンダリボリュームを確認します。

```
cluster::> snapmirror show
```

Source Path	Type	Dest Path	Mirror State	Relation Status	Total Progress	Healthy	Last Updated
-----							
vserverA:srcvolA							
	XDP	vserverB:dstvolB					
			Snapmirrored				
			Idle		-	true	-

3. を実行します `volume snapshot show` コマンドを使用して、リストア元の Snapshot コピーを特定します。

```
cluster::> volume snapshot show
```

Vserver	Volume	Snapshot	State	Size	Total%	Used%
-----						
vserverB						
	dstvolB					
		snap2.2013-02-10_0010	valid	124KB	0%	0%
		snap1.2013-02-10_0015	valid	112KB	0%	0%
		snap2.2013-02-11_0010	valid	164KB	0%	0%

4. を実行します `snapmirror restore` コマンドを入力し、を指定します `-source-snapshot` 使用する Snapshot コピーを指定するオプション。

リストア先として指定するのは、リストア先の元のボリュームです。

```
cluster::> snapmirror restore -destination-path vserverA:srcvolA  
-source-path vserverB:dstvolB -source-snapshot daily.2013-02-10_0010
```

```
Warning: All data newer than Snapshot copy hourly.2013-02-11_1205 on  
volume vserverA:src_volA will be deleted.
```

```
Do you want to continue? {y|n}: y
```

```
[Job 98] Job is queued: snapmirror restore from source  
"vserverB:dstvolB" for the snapshot daily.2013-02-10_0010.
```

5. ホストクラスタ間で LUN を共有している場合は、影響を受けるホストから LUN に対する永続的予約をリストアします。

#### **SnapVault** バックアップからのボリュームのリストア

次の例では、Snapshot コピーの作成後に lun\_D という名前の LUN がボリュームに追加されています。Snapshot コピーからボリューム全体をリストアしたあと、lun\_D は表示されなくなります。

を参照してください lun show コマンドの出力では、プライマリボリュームsrcvolA内のLUNと、SnapVault セカンダリボリュームdstvolB内のそれらのLUNの読み取り専用コピーを確認できます。SnapVault バックアップに lun\_D のコピーはありません。

```
cluster::> lun show
```

Vserver	Path	State	Mapped	Type	Size
vserverA	/vol/srcvolA/lun_A	online	mapped	windows	300.0GB
vserverA	/vol/srcvolA/lun_B	online	mapped	windows	300.0GB
vserverA	/vol/srcvolA/lun_C	online	mapped	windows	300.0GB
vserverA	/vol/srcvolA/lun_D	online	mapped	windows	250.0GB
vserverB	/vol/dstvolB/lun_A	online	unmapped	windows	300.0GB
vserverB	/vol/dstvolB/lun_B	online	unmapped	windows	300.0GB
vserverB	/vol/dstvolB/lun_C	online	unmapped	windows	300.0GB

7 entries were displayed.

```
cluster::> snapmirror restore -destination-path vserverA:srcvolA
-source-path vserverB:dstvolB
-source-snapshot daily.2013-02-10_0010
```

Warning: All data newer than Snapshot copy hourly.2013-02-11\_1205  
on volume vserverA:src\_volA will be deleted.  
Do you want to continue? {y|n}: y  
[Job 98] Job is queued: snapmirror restore from source  
"vserverB:dstvolB" for the snapshot daily.2013-02-10\_0010.

```
cluster::> lun show
```

Vserver	Path	State	Mapped	Type	Size
vserverA	/vol/srcvolA/lun_A	online	mapped	windows	300.0GB
vserverA	/vol/srcvolA/lun_B	online	mapped	windows	300.0GB
vserverA	/vol/srcvolA/lun_C	online	mapped	windows	300.0GB
vserverB	/vol/dstvolB/lun_A	online	unmapped	windows	300.0GB
vserverB	/vol/dstvolB/lun_B	online	unmapped	windows	300.0GB
vserverB	/vol/dstvolB/lun_C	online	unmapped	windows	300.0GB

6 entries were displayed.

ボリュームが SnapVault セカンダリボリュームからリストアされると、ソースボリュームには lun\_D が存在しなくなりますリストア後もソースボリューム内の LUN のマッピングは維持されるため、再マッピングする必要はありません。

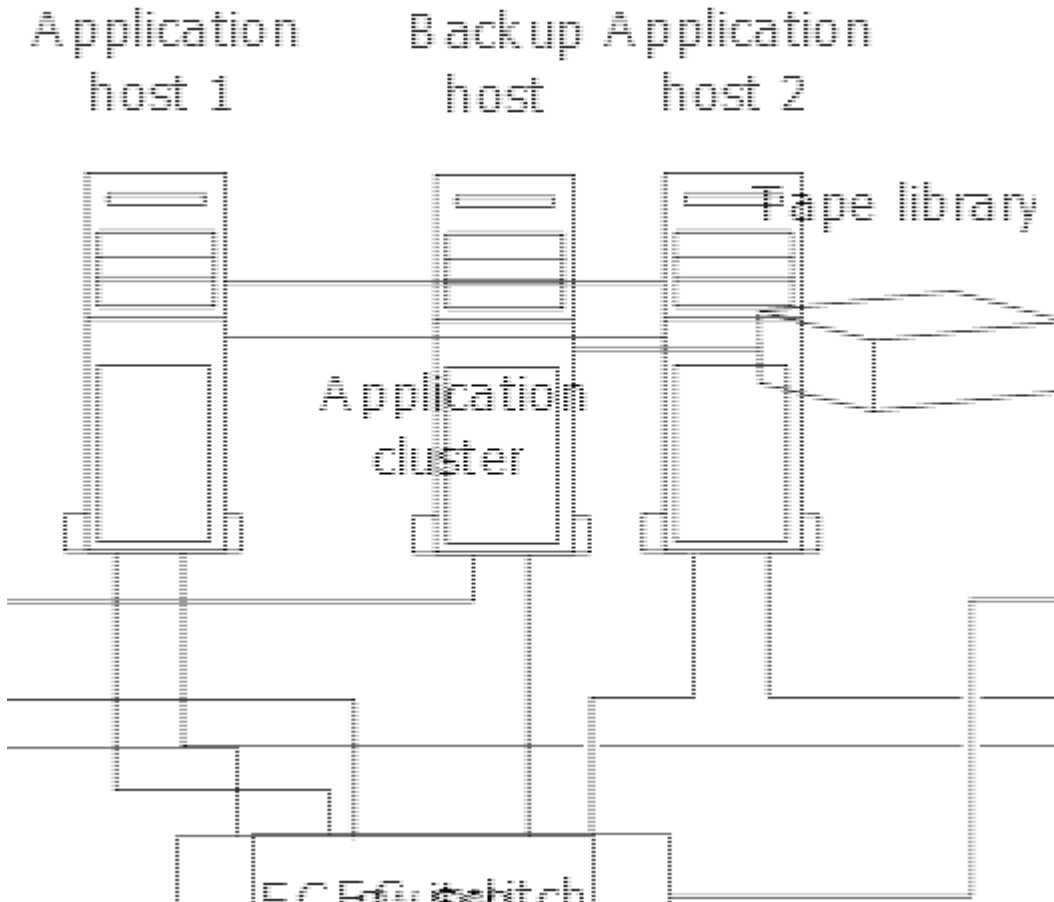
## ホストバックアップシステムをプライマリストレージシステムに接続する方法

テープへの SAN システムのバックアップは、アプリケーションホストのパフォーマンス低下を避けるため、別のバックアップホストで実行できます。

SAN と NAS のデータは、バックアップ目的で分けておくことが必須です。次の図に、プライマリストレージシステムに接続するホストバックアップシステムに推奨される物理構成を示します。ボリュームは SAN 専用



として設定する必要があります。LUN は単一のボリュームに限定することも、複数のボリュームまたはストレージシステムに分散して設定することもできます。



ホスト上のボリュームは、ストレージシステムからマッピングされた単一の LUN、または HP-UX システム上の VxVM などのボリュームマネージャを使用して複数の LUN で構成できます。

## ホストバックアップシステムを介して **LUN** をバックアップする

ホストバックアップシステムのソースデータとして、Snapshot コピー内のクローン LUN を使用できます。

### 必要なもの

本番用 LUN が必要です。アプリケーションサーバの WWPN またはイニシエータノード名を含む igroup にマッピングされている必要があります。また、LUN がフォーマット済みで、ホストにアクセスする必要があります。

### 手順

1. ホストファイルシステムバッファの内容をディスクに保存します。

ホストオペレーティングシステムのコマンドを使用するか、SnapDrive for Windows または SnapDrive for UNIX を使用できます。この手順を SAN バックアップのプリプロセススクリプトに含めることもできます。

2. を使用します volume snapshot create コマンドを使用して本番用 LUN の Snapshot コピーを作成します。

```
volume snapshot create -vserver vs0 -volume vol3 -snapshot vol3_snapshot  
-comment "Single snapshot" -foreground false
```

3. を使用します volume file clone create 本番用LUNのクローンを作成するコマンド。

```
volume file clone create -vserver vs3 -volume vol3 -source-path lun1 -snapshot  
-name snap_vol3 -destination-path lun1_backup
```

4. を使用します lun igroup create バックアップサーバのWWPNを含むigroupを作成するコマンド。

```
lun igroup create -vserver vs3 -igroup igroup3 -protocol fc -ostype windows  
-initiator 10:00:00:00:c9:73:5b:91
```

5. を使用します lun mapping create 手順3で作成したLUNクローンをバックアップホストにマッピングするコマンド。

```
lun mapping create -vserver vs3 -volume vol3 -lun lun1_backup -igroup igroup3
```

この手順を SAN バックアップアプリケーションのポストプロセススクリプトに含めることができます。

6. ホストから、新しい LUN を検出し、ファイルシステムをホストで使用できるようにします。

この手順を SAN バックアップアプリケーションのポストプロセススクリプトに含めることができます。

7. SAN バックアップアプリケーションを使用して、バックアップホストの LUN クローン内のデータをテープにバックアップします。

8. を使用します lun modify LUNクローンをオフラインにするコマンド。

```
lun modify -vserver vs3 -path /vol/vol3/lun1_backup -state offline
```

9. を使用します lun delete をクリックしてLUNクローンを削除します。

```
lun delete -vserver vs3 -volume vol3 -lun lun1_backup
```

10. を使用します volume snapshot delete コマンドを実行してSnapshotコピーを削除します。

```
volume snapshot delete -vserver vs3 -volume vol3 -snapshot vol3_snapshot
```

## SAN 構成リファレンス

### SANコウセイノカイヨウ

Storage Area Network (SAN ; ストレージエリアネットワーク) は、iSCSIやFCなどのSAN転送プロトコルを使用してホストに接続されるストレージ解決策で構成されます。ストレージ解決策が1つ以上のスイッチを介してホストに接続されるようにSANを設定できます。iSCSIを使用している場合は、スイッチを使用せずにストレージ解決策がホストに直接接続されるようにSANを設定することもできます。

SANでは、Windows、Linux、UNIXなど、異なるオペレーティングシステムを使用する複数のホストからスト

レーズ解決策に同時にアクセスできます。 を使用できます ["選択的LUNマッピング"](#) および ["ポートセット"](#) ホストとストレージの間のデータアクセスを制限します。

iSCSIの場合、ストレージ解決策とホスト間のネットワークポロジをネットワークと呼びます。 FC、FC / NVMe、FCoEの場合、ストレージ解決策とホストの間のネットワークポロジをファブリックと呼びます。 冗長性を確保してデータアクセスの中断からデータを保護するには、マルチネットワークまたはマルチファブリック構成のHAペアを使用してSANをセットアップする必要があります。 シングルノードまたはシングルネットワーク/ファブリックを使用する構成は完全な冗長性がないため、推奨されません。

SANの設定が完了したら、次の操作を実行できます。 ["iSCSIまたはFC用のストレージのプロビジョニング"](#) または、次の操作を実行できます ["FC / NVMe用のストレージのプロビジョニング"](#)。 その後、ホストに接続してデータの提供を開始できます。

SANプロトコルのサポートは、ONTAPのバージョン、プラットフォーム、構成によって異なります。 具体的な構成の詳細については、を参照してください ["NetApp Interoperability Matrix Tool で確認できます"](#)。

#### 関連情報

- ["SAN の管理の概要"](#)
- ["NVMeの構成、サポート、制限事項"](#)

## iSCSIコウセイ

### iSCSI SANホストの構成方法

iSCSI構成では、iSCSI SANホストに直接接続するか、1つ以上のIPスイッチを介してホストに接続するハイアベイラビリティ（HA）ペアを使用します。

["HA ペア"](#) ホストがLUNへのアクセスに使用するアクティブ/最適化パスとアクティブ/非最適パスのレポートノードとして定義されます。 Windows、Linux、UNIXなど、異なるオペレーティングシステムを使用する複数のホストから同時にストレージにアクセスできます。 ホストでは、ALUAをサポートするサポート対象のマルチパス解決策がインストールおよび設定されている必要があります。 サポートされるオペレーティングシステムとマルチパスソリューションは、 ["NetApp Interoperability Matrix Tool で確認できます"](#)。

マルチネットワーク構成では、ホストをストレージシステムに接続するスイッチが複数あります。 完全な冗長性を備えたマルチネットワーク構成を推奨します。 シングルネットワーク構成では、1台のスイッチでホストをストレージシステムに接続します。 シングルネットワーク構成では完全な冗長性は確保されません。



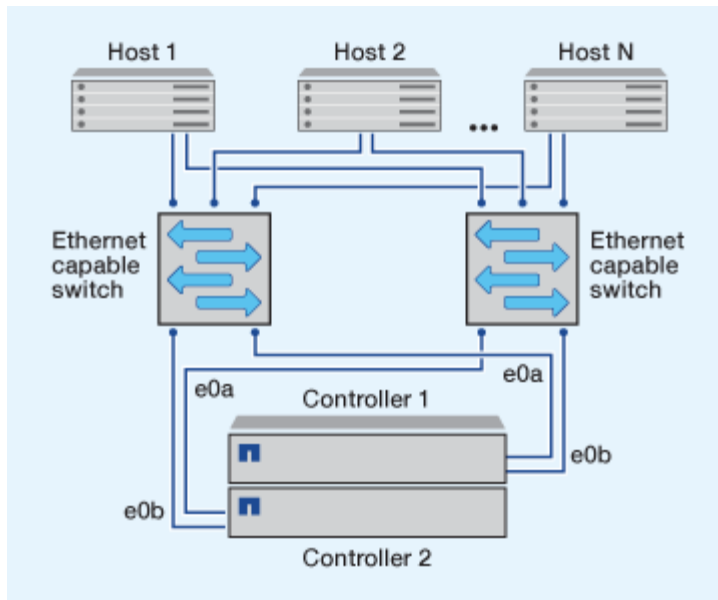
["シングルノードコウセイ"](#) は、フォールトトレランスやノンストップオペレーションのサポートに必要な冗長性が確保されないため、推奨されません。

#### 関連情報

- 詳細をご確認ください ["選択的LUNマッピング（SLM）"](#) HAペアが所有するLUNへのアクセスに使用するパスを制限します。
- 詳細はこちら ["SAN LIF"](#)。
- の詳細を確認してください ["iSCSIにおけるVLANの利点"](#)。

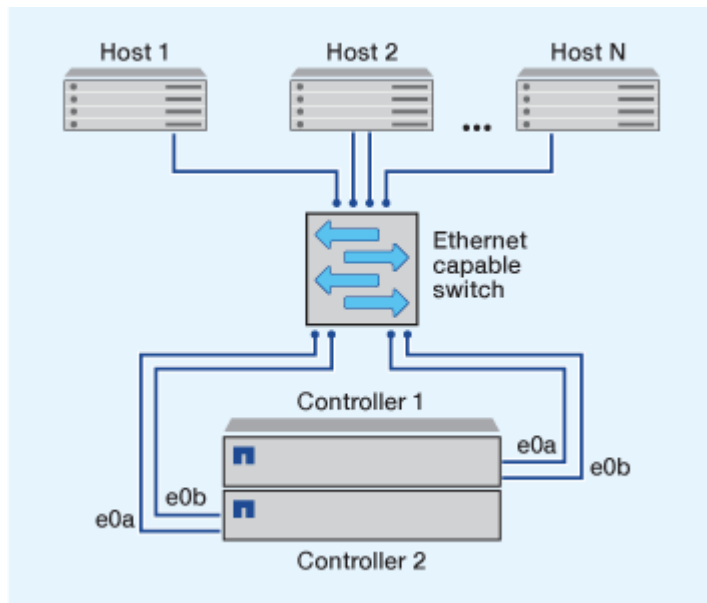
### マルチネットワークiSCSIコウセイ

マルチネットワークの HA ペア構成では、HA ペアを複数のスイッチで 1 つまたは複数のホストに接続します。 スwitchが複数あるため、この構成では完全な冗長性が確保されます。



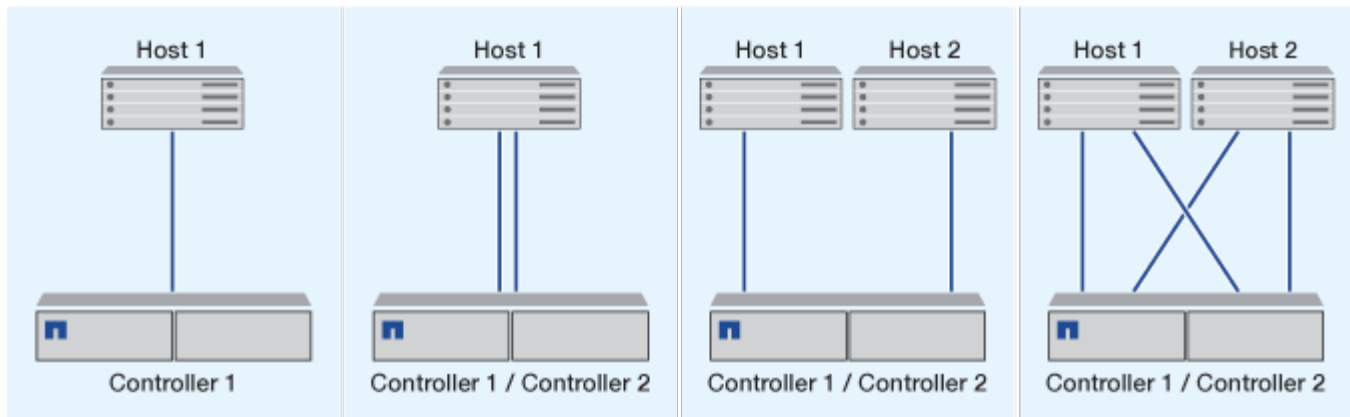
#### タンイチネットワークアクノiSCSIコウセイ

単一ネットワークの HA ペア構成では、HA ペアを 1 台のスイッチで 1 つまたは複数のホストに接続します。スイッチが 1 台しかないため、この構成では完全な冗長性は確保されません。



#### 直接接続型iSCSI構成

直接接続型の構成では、1 つ以上のホストをコントローラに直接接続します。



## iSCSI 構成で VLAN を使用する利点

VLAN は、ブロードキャストドメインにグループ化されたスイッチポートのグループで構成されます。VLAN は、単一のスイッチに設定することも、複数のスイッチシャーシにまたがって設定することもできます。静的な VLAN と動的な VLAN を使用すると、IP ネットワークインフラ内でのセキュリティの強化、問題の切り分け、および使用可能なパスの制限が可能になります。

大規模な IP ネットワークインフラに VLAN を実装する利点は次のとおりです。

- セキュリティの向上：

VLAN を使用すると、イーサネットネットワークまたは IP SAN のノード間のアクセスが制限されるため、既存のインフラを利用しながらセキュリティを強化できます。

- 問題を切り分けることで、イーサネットネットワークや IP SAN の信頼性が高まります。
- 問題の範囲を制限することで、問題解決時間を短縮できます。
- 特定の iSCSI ターゲットポートへの使用可能なパスの数が削減されます。
- ホストで使用するパスの最大数が削減されます。

パスが多すぎると再接続の時間が遅くなります。ホストにマルチパス解決策がない場合は、VLAN を使用して 1 つのパスのみを許可できます。

## 動的 VLANs

動的な VLAN は MAC アドレスに基づいています。VLAN は、VLAN に含めるメンバーの MAC アドレスを指定して定義できます。

動的な VLAN は柔軟性に優れており、デバイスがスイッチに物理的に接続されている物理ポートにマッピングする必要はありません。ケーブルを別のポートに接続するときに VLAN を再構成する必要はありません。

## 静的な VLAN

静的な VLAN はポートベースです。スイッチポートとスイッチポートを使用して、VLAN とそのメンバーを定義します。

静的な VLAN を使用すると、MAC（メディアアクセス制御）のスプーフィングを使用した VLAN への不正

アクセスを防止できるため、セキュリティが向上します。ただし、第三者がスイッチに物理的にアクセスできる場合は、ケーブルを交換してネットワークアドレスを再設定することでアクセスが可能になります。

環境によっては、静的な VLAN は動的な VLAN よりも簡単に作成および管理できます。静的な VLAN では、48 ビットの MAC アドレスではなく、スイッチとポートの識別子のみを指定する必要があるからです。また、VLAN の識別子をスイッチのポート範囲のラベルとして設定することもできます。

## FC コウセイ

### FC および FC-NVMe SAN ホストの構成方法

FC および FC-NVMe SAN ホストは、HA ペアと少なくとも 2 つのスイッチを使用して設定することを推奨します。これにより、ファブリックレイヤとストレージシステムレイヤで冗長性が確保され、フォールトトレランスとノンストップオペレーションがサポートされます。FC または FC-NVMe SAN ホストをスイッチを使用せずに HA ペアに直接接続することはできません。

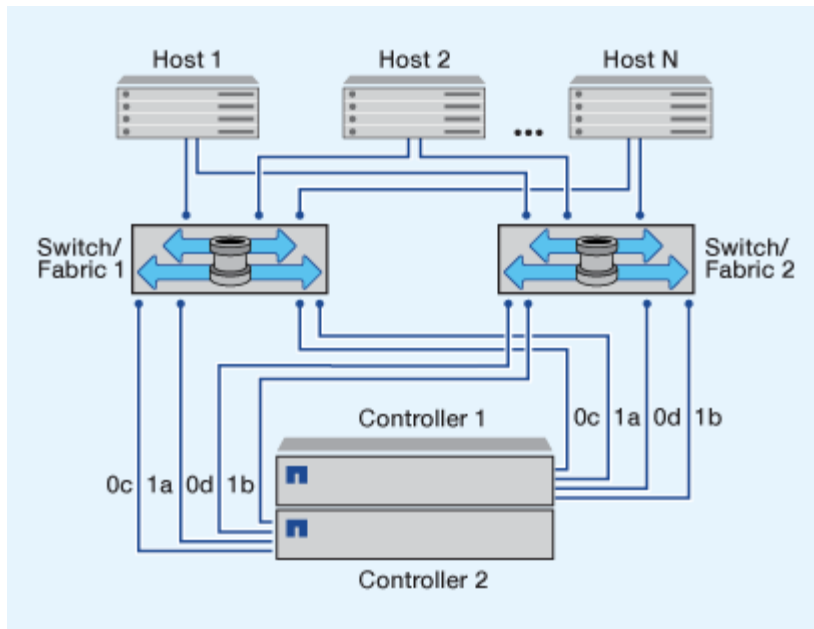
カスケードファブリック、部分メッシュファブリック、フルメッシュファブリック、コアエッジファブリック、およびディレクタファブリックは、FC スwitch をファブリックに接続する業界標準の方法であり、いずれもサポートされます。異機種混在の FC スwitch ファブリックの使用は、組み込みのブレードスイッチ以外はサポートされていません。特定の例外については、を参照してください ["Interoperability Matrix Tool で確認してください"](#)。ファブリックは 1 つまたは複数のスイッチで構成できます。また、ストレージコントローラは複数のスイッチに接続することができます。

Windows、Linux、UNIX など、異なるオペレーティングシステムを使用する複数のホストから、ストレージコントローラに同時にアクセスできます。ホストには、サポートされるマルチパス解決策をインストールおよび設定する必要があります。サポートされるオペレーティングシステムとマルチパスソリューションは、Interoperability Matrix Tool で確認できます。

### マルチファブリックノ FC コウセイ オヨビ FC-NVMe コウセイ

マルチファブリックの HA ペア構成では、HA ペアを複数のスイッチで 1 つ以上のホストに接続します。次の図は、マルチファブリックの HA ペアを示しています。わかりやすいように、この図ではファブリックが 2 つだけになっていますが、マルチファブリック構成は 2 つ以上の任意の数のファブリックで構成できます。

次の図の FC ターゲットポート番号 (0c、0d、1a、1b) は一例です。実際のポート番号は、使用しているストレージノードのモデル、および拡張アダプタを使用しているかどうかによって異なります。

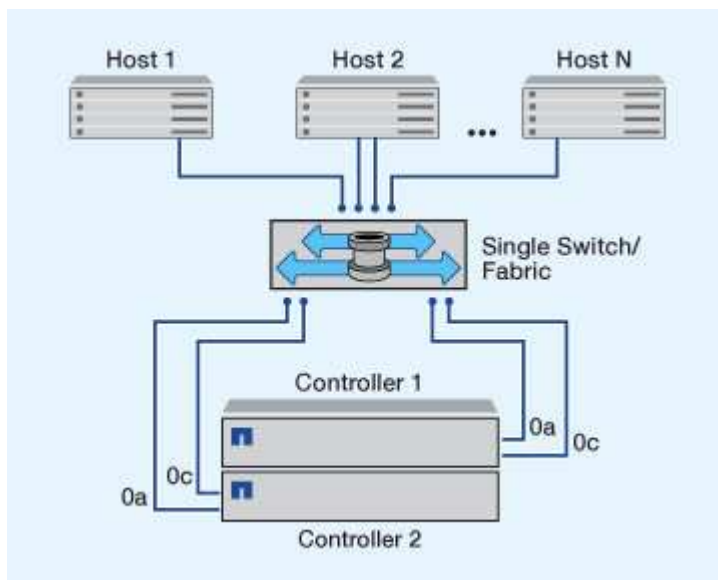


#### タンイツファブリックノFCコウセイオヨビFC-NVMeコウセイ

単一ファブリックの HA ペア構成では、HA ペアの両方のコントローラを 1 つのファブリックで 1 つまたは複数のホストに接続します。ホストとコントローラは単一のスイッチを介して接続されるため、単一ファブリックの HA ペア構成では完全な冗長性は確保されません。

次の図の FC ターゲットポート番号 (0a、0c) は一例です。実際のポート番号は、使用しているストレージノードのモデル、および拡張アダプタを使用しているかどうかによって異なります。

単一ファブリックの HA ペア構成は、FC 構成をサポートするすべてのプラットフォームでサポートされます。



"シングルノードコウセイ" は、フォールトトレランスやノンストップオペレーションのサポートに必要な冗長性が確保されないため、推奨されません。

#### 関連情報

- 詳細をご確認ください ["選択的LUNマッピング \(SLM\)"](#) HA ペアが所有する LUN へのアクセスに使用する

パスを制限します。

- 詳細はこちら ["SAN LIF"](#)。

## FC スイッチ構成のベストプラクティス

FC スイッチを構成するときは、パフォーマンスを最大限に高めるために一定のベストプラクティスに従うことを推奨します。

FC スイッチの構成では、リンク速度を固定の値に設定すると効果的です。これは大規模なファブリックに特に適した方法で、ファブリックを再構築する際のパフォーマンスが最大限に高まり、時間を大幅に短縮することができます。自動ネゴシエーションは柔軟性に優れていますが、FC スイッチの構成では期待したパフォーマンスを常に得られるとはかぎらないため、全体の構築時間は長くなります。

ファブリックに接続されているすべてのスイッチで、N\_Port ID Virtualization (NPIV) がサポートされていて有効になっている必要があります。ONTAP は、NPIV を使用して FC ターゲットをファブリックに提示します。

サポートされている環境の詳細については、を参照してください ["NetApp Interoperability Matrix Tool で確認できます"](#)。

FC および iSCSI のベストプラクティスについては、を参照してください ["NetAppテクニカルレポート4080：『Best Practices for Modern SAN』"](#)。

## サポートされる FC ホップ数

ホストとストレージシステムの間でサポートされる FC の最大ホップ数は、スイッチベンダーとストレージシステムによる FC 構成のサポート内容によって異なります。

ホップ数とは、イニシエータ（ホスト）とターゲット（ストレージシステム）の間のパスにあるスイッチ数です。Cisco では、この値を「SAN ファブリックの直径」とも呼びます。

スイッチベンダー	サポートされるホップ数
Brocade	FCでは7、FCoEでは5
シスコ	7 FCの場合、最大3つのスイッチをFCoEスイッチにすることができます。

## 関連情報

["ネットアップのダウンロード： Brocade 拡張性マトリックスのドキュメント"](#)

["ネットアップのダウンロード： Cisco 拡張性マトリックスのドキュメント"](#)

## サポートされる FC ターゲットポートの速度

FC ターゲットポートは、さまざまな速度で実行するように構成できます。ターゲットポートの速度は接続先デバイスの速度と同じにする必要があります。同じホストで使用するターゲットポートは、すべて同じ速度に設定する必要があります。



FC-NVMe 構成の場合も、FC 構成の場合とまったく同じ方法で FC ターゲットポートを使用できます。

ターゲットポートの速度は、自動ネゴシエーションを使わずに、接続先デバイスの速度と同じにすることを推奨します。自動ネゴシエーションを設定したポートの方が、ギブバックやテイクオーバーなどの中断後の再接続に時間がかかる可能性があります。

オンボードポートと拡張アダプタは、次の速度で実行するように構成できます。コントローラと拡張アダプタのポートは、必要に応じて、さまざまな速度で実行するように個別に構成することができます。

4Gb ポート	8Gb ポート	16Gb ポート	32Gb ポート
<ul style="list-style-type: none"><li>• 4 GB</li><li>• 2 Gb</li><li>• 1 Gb</li></ul>	<ul style="list-style-type: none"><li>• 8 Gb</li><li>• 4 GB</li><li>• 2 Gb</li></ul>	<ul style="list-style-type: none"><li>• 16Gb</li><li>• 8 Gb</li><li>• 4 GB</li></ul>	<ul style="list-style-type: none"><li>• 32Gb</li><li>• 16Gb</li><li>• 8 Gb</li></ul>



UTA2 ポートでは、必要に応じて、8Gb の SFP+ アダプタを使用して 8Gb、4Gb、2Gb の速度をサポートできます。

#### FC のターゲットポート構成に関する推奨事項

最大のパフォーマンスと可用性を得るためには、推奨される FC ターゲットポート構成を使用します。

次の表に、オンボード FC および FC-NVMe ターゲットポートの使用優先順位を示します。拡張アダプタの場合は、接続に同じ ASIC を使用しないように FC ポートを分散させます。優先スロットの順序については、を参照してください ["NetApp Hardware Universe の略"](#) コントローラで使用する ONTAP ソフトウェアのバージョンに対応しています。

FC-NVMe は次のモデルでサポートされます。

- AFF A300



AFF A300 オンボードポートでは FC-NVMe がサポートされません。

- AFF A700の略
- AFF A700s
- AFF A800



FAS2520システムにはオンボードのFCポートはなく、アドオンのアダプタもサポートされません。

コントローラ	ASIC を共有するポートペア	ターゲットポートの数：優先ポート
FAS9000、AFF A700、AFF A700s、AFF A800	なし	すべてのデータポートが拡張アダプタにあります。を参照してください <a href="#">"NetApp Hardware Universe の略"</a> を参照してください。

コントローラ	ASIC を共有するポートペア	ターゲットポートの数：優先ポート
8080、8060、8040	0E+0f 0g+0h	1 : 0e 2 : 0e、0g 3 : 0e、0g、0h 4 : 0e、0g、0f、0h
FAS8200 と AFF A300	0g+0h	1 : 0g 2 : 0g、0h
8020	0c+0d	1 : 0c 2 : 0c、0d
62xx	0a+0b 0c+0d	1 : 0A 2 : 0a、0c 3 : 0a、0c、0b 4 : 0a、0c、0b、0d
32xx	0c+0d	1 : 0c 2 : 0c、0d
FAS2554、FAS2552、FAS2600 シリーズ、FAS2720、FAS2750 、AFF A200、AFF A220	0c+0d 0E+0f	1 : 0c 2 : 0c、0e 3 : 0c、0e、0d 4 : 0c、0e、0d、0f

## FC アダプタを搭載したシステムを管理する

### FC アダプタを搭載したシステムの管理の概要

オンボード FC アダプタと FC アダプタカードの管理に使用できるコマンドが用意されています。これらのコマンドを使用して、アダプタモードの設定、アダプタ情報の表示、および速度の変更を行うことができます。

ほとんどのストレージシステムには、イニシエータまたはターゲットとして設定できるオンボード FC アダプタが搭載されています。イニシエータまたはターゲットとして設定された FC アダプタカードを使用すること

もできます。イニシエータはバックエンドディスクシェルフに接続します。場合によっては、外部ストレージアレイ（FlexArray）にも接続します。ターゲットはFC スイッチのみに接続します。FC ターゲットの HBA ポートとスイッチポートの速度は、両方とも同じ値に設定し、auto には設定しないでください。

#### FC アダプタの管理用コマンド

FC コマンドを使用して、ストレージコントローラの FC ターゲットアダプタ、FC イニシエータアダプタ、およびオンボード FC アダプタを管理できます。FC アダプタの管理に使用するコマンドは、FC プロトコルと FC-NVMe プロトコルで同じです。

FC イニシエータアダプタのコマンドは、ノードレベルでのみ機能します。を使用する必要があります `run -node node_name` FCイニシエータアダプタのコマンドを使用する前のコマンド。

#### FC ターゲットアダプタの管理用コマンド

状況	使用するコマンド
ノードの FC アダプタ情報を表示する	<code>network fcp adapter show</code>
FC ターゲットアダプタのパラメータを変更する	<code>network fcp adapter modify</code>
FC プロトコルトラフィック情報を表示します	<code>run -node node_name sysstat -f</code>
FC プロトコルの実行時間を表示します	<code>run -node node_name uptime</code>
アダプタの設定とステータスを表示します	<code>run -node node_name sysconfig -v adapter</code>
拡張カードが取り付けられていること、および構成にエラーがないかどうかを確認します	<code>run -node node_name sysconfig -ac</code>
コマンドのマニュアルページを表示します	<code>man command_name</code>

#### FC イニシエータアダプタの管理用コマンド

状況	使用するコマンド
ノードのすべてのイニシエータおよびそのアダプタの情報を表示する	<code>run -node node_name storage show adapter</code>
アダプタの設定とステータスを表示します	<code>run -node node_name sysconfig -v adapter</code>
拡張カードが取り付けられていること、および構成にエラーがないかどうかを確認します	<code>run -node node_name sysconfig -ac</code>

## オンボード FC アダプタの管理用コマンド

状況	使用するコマンド
オンボード FC ポートのステータスを表示します	<code>system node hardware unified-connect show</code>

FC アダプタをイニシエータモードに設定します

オンボードアダプタの個々の FC ポートや特定の FC アダプタカードをイニシエータモードに設定することができます。イニシエータモードは、テープドライブやテープライブラリへのポートの接続、または FlexArray 仮想化や Foreign LUN Import（FLI）を使用するサードパーティストレージへのポートの接続に使用されます。

必要なもの

- アダプタの LIF を、メンバーとして属するすべてのポートセットから削除する必要があります。
- 物理ポートのパーソナリティをターゲットからイニシエータに変更する前に、変更する物理ポートを使用するすべての Storage Virtual Machine（SVM）のすべての LIF を、移行するか破棄する必要があります。

このタスクについて

オンボードの FC ポートは、それぞれイニシエータまたはターゲットとして個別に構成できます。一部の FC アダプタのポートについては、オンボードの FC ポートと同様に、それぞれターゲットポートまたはイニシエータポートとして個別に構成することもできます。ターゲットモードに設定できるアダプタのリストは、確認できます ["NetApp Hardware Universe の略"](#)。



NVMe/FC ではイニシエータモードがサポートされます。

手順

1. アダプタからすべての LIF を削除します。

```
network interface delete -vserver SVM_name -lif lif_name,lif_name
```

2. アダプタをオフラインにします。

```
network fcp adapter modify -node node_name -adapter adapter_port -status-admin down
```

アダプタがオフラインにならない場合は、システムの該当するアダプタポートからケーブルを取り外すこともできます。

3. アダプタをターゲットからイニシエータに変更します。

```
system hardware unified-connect modify -t initiator adapter_port
```

4. 変更したアダプタをホストしているノードをリブートします。
5. 構成に対して FC ポートが正しい状態で設定されていることを確認します。

```
system hardware unified-connect show
```

## 6. アダプタをオンラインに戻します。

```
node run -node node_name storage enable adapter adapter_port
```

### FC アダプタをターゲットモードに設定します

オンボードアダプタの個々の FC ポートや特定の FC アダプタカードをターゲットモードに設定できます。ターゲットモードは、ポートを FC イニシエータに接続するために使用します。

このタスクについて

オンボードの FC ポートは、それぞれイニシエータまたはターゲットとして個別に構成できます。一部の FC アダプタのポートについては、オンボードの FC ポートと同様に、それぞれターゲットポートまたはイニシエータポートとして個別に構成することもできます。ターゲットモードに設定できるアダプタのリストは、で確認できます ["NetApp Hardware Universe の略"](#)。

FC アダプタを構成する手順は、FC プロトコルでも FC-NVMe プロトコルでも同じです。ただし、FC-NVMe をサポートする FC アダプタは限られています。を参照してください ["NetApp Hardware Universe の略"](#) FC-NVMe プロトコルをサポートするアダプタの一覧が表示されます。

### 手順

#### 1. アダプタをオフラインにします。

```
node run -node node_name storage disable adapter adapter_name
```

アダプタがオフラインにならない場合は、システムの該当するアダプタポートからケーブルを取り外すこともできます。

#### 2. アダプタをイニシエータからターゲットに変更します。

```
system node hardware unified-connect modify -t target -node node_name adapter adapter_name
```

#### 3. 変更したアダプタをホストしているノードをリブートします。

#### 4. ターゲットポートの設定が正しいことを確認します。

```
network fcp adapter show -node node_name
```

#### 5. アダプタをオンラインにします。

```
network fcp adapter modify -node node_name -adapter adapter_port -state up
```

### FC ターゲットアダプタに関する情報を表示する

を使用できます `network fcp adapter show` コマンドを使用して、システム内の FC アダプタのシステム設定およびアダプタ情報を表示します。

### ステップ

#### 1. を使用して、FCアダプタに関する情報を表示します `network fcp adapter show` コマンドを実行しま

す

使用されている各スロットのシステム設定情報とアダプタ情報が出力に表示されます。

```
network fcp adapter show -instance -node node1 -adapter 0a
```

#### FC アダプタの速度を変更します

自動ネゴシエーションを使わずに、アダプタのターゲットポートの速度を接続先デバイスの速度と同じにすることを推奨します。自動ネゴシエーションを設定したポートの方が、ギブバックやテイクオーバーなどの中断後の再接続に時間がかかる可能性があります。

#### 必要なもの

このアダプタをホームポートとして使用しているすべての LIF をオフラインにする必要があります。

#### このタスクについて

このタスクではクラスタ内のすべてのStorage Virtual Machine (SVM) とLIFが対象となるため、を使用する必要があります `-home-port` および `-home-lif` この操作の範囲を制限するパラメータ。これらのパラメータを使用しないと、処理環境によってクラスタ内のすべての LIF が処理によって使用されなくなる可能性があります。

#### 手順

1. アダプタのすべての LIF をオフラインにします。

```
network interface modify -vserver * -lif * { -home-node node1 -home-port 0c }  
-status-admin down
```

2. アダプタをオフラインにします。

```
network fcp adapter modify -node node1 -adapter 0c -state down
```

アダプタがオフラインにならない場合は、システムの該当するアダプタポートからケーブルを取り外すこともできます。

3. ポートアダプタの最大速度を確認します。

```
fcp adapter show -instance
```

アダプタ速度を最大速度よりも速くすることはできません。

4. アダプタ速度を変更します。

```
network fcp adapter modify -node node1 -adapter 0c -speed 16
```

5. アダプタをオンラインにします。

```
network fcp adapter modify -node node1 -adapter 0c -state up
```

6. アダプタのすべての LIF をオンラインにします。

```
network interface modify -vserver * -lif * { -home-node node1 -home-port 0c }  
-status-admin up
```

#### サポートされる FC ポート

オンボードの FC ポートと FC 用の CNA / UTA2 ポートの数は、コントローラのモデルによって異なります。また、FC ポートは、サポートされている FC ターゲット拡張アダプタのほか、FC SFP+ アダプタ用の追加の UTA2 カードからも提供されます。

オンボードの **FC**、**UTA**、および **UTA2** ポートを使用できます

- オンボードポートは、ターゲットまたはイニシエータのどちらかの FC ポートとして個別に構成できます。
- オンボードの FC ポートの数はコントローラのモデルによって異なります。  
  
。 ["NetApp Hardware Universe の略"](#) に、各コントローラモデルのオンボード FC ポートの一覧を示します。
- FAS2520システムはFCをサポートしていません。

#### ターゲット拡張アダプタの FC ポート

- 使用可能なターゲット拡張アダプタは、コントローラのモデルによって異なります。  
  
。 ["NetApp Hardware Universe の略"](#) に、各コントローラモデルのターゲット拡張アダプタの一覧を示します。
- 一部の FC 拡張アダプタのポートは、工場出荷時にイニシエータまたはターゲットのどちらかとして構成されており、変更することはできません。

その他のポートについては、オンボードの FC ポートと同様に、それぞれターゲットまたはイニシエータどちらかの FC ポートとして個別に構成できます。完全なリストは、で入手できます ["NetApp Hardware Universe の略"](#)。

#### **X1133A-R6** アダプタ使用時の接続の切断を回避します

別の X1133A-R6 HBA への冗長パスを構成することにより、ポート障害時に接続が切断されないようにすることができます。

X1133A-R6 HBA は、4 ポート 16Gb の FC アダプタで、2 組の 2 ポートペアで構成されます。X1133A-R6 アダプタは、ターゲットモードまたはイニシエータモードとして設定できます。2 ポートペアはそれぞれ 1 つの ASIC でサポートされます（たとえば、ポート 1 とポート 2 は ASIC 1、ポート 3 とポート 4 は ASIC 2）。単一の ASIC の両方のポートを、ターゲットモードまたはイニシエータモードのどちらかで動作するように設定する必要があります。ペアをサポートする ASIC でエラーが発生すると、そのペアの両方のポートがオフラインになります。

接続が切断されないようにするには、別の X1133A-R6 HBA への冗長パスか、HBA の別の ASIC でサポートされるポートへの冗長パスを構成します。

## X1143A-R6 アダプタでサポートされるポート設定の概要

X1143A-R6 アダプタのポートは、デフォルトでは FC ターゲットモードで構成されますが、10Gb イーサネットポートおよび FCoE ポート（CNA ポート）、あるいは 16Gb FC イニシエータポートまたはターゲットポートとして構成することもできます。これには、SFP+ アダプタが必要です。

イーサネットおよび FCoE 用に設定した場合、X1143A-R6 アダプタは、同じ 10GbE ポートの NIC および FCoE のターゲットトラフィックを同時にサポートします。FC 用に設定した場合、同じ ASIC を共有する 2 ポートの各ペアを FC ターゲットまたは FC イニシエータモード用に個別に設定できます。つまり、単一の X1143A-R6 アダプタが、1 つの 2 ポートペアで FC ターゲットモードをサポートし、もう 1 つの 2 ポートペアで FC イニシエータモードをサポートできます。同じ ASIC に接続するポートペアは、同じモードで設定する必要があります。

X1143A-R6 アダプタは、FC モードでは既存の FC デバイスと同じように動作し、最大速度は 16Gbps になります。X1143A-R6 アダプタを CNA モードで使用する、同じ 10GbE ポートを共有する NIC および FCoE のトラフィックを同時に処理することができます。CNA モードでは、FCoE の機能については FC ターゲットモードのみがサポートされます。

ポートを設定します

ユニファイドターゲットアダプタ（X1143A-R6）を設定するには、同じチップ上の隣接する 2 個のポートを同じパーソナリティモードで設定する必要があります。

手順

1. を使用して、必要に応じて Fibre Channel（FC；ファイバチャネル）または Converged Network Adapter（CNA；統合ネットワークアダプタ）にポートを設定します `system node hardware unified-connect modify` コマンドを実行します
2. FC または 10Gb イーサネットに適したケーブルを接続します。
3. 適切な SFP+ が取り付けられていることを確認します。

```
network fcp adapter show -instance -node -adapter
```

CNA の場合は、10Gb イーサネット SFP を使用します。FC の場合は、接続先の FC ファブリックに応じて 8Gb SFP または 16Gb SFP を使用します。

## UTA2 ポートを CNA モードから FC モードに変更します

Fibre Channel（FC；ファイバチャネル）イニシエータモードと FC ターゲットモードをサポートするには、UTA2 ポートを Converged Network Adapter（CNA；統合ネットワークアダプタ）モードから FC モードに変更する必要があります。ポートをネットワークに接続する物理メディアを変更する必要がある場合は、パーソナリティを CNA モードから FC モードに変更します。

手順

1. アダプタをオフラインにします。



```
network fcp adapter modify -node node_name -adapter adapter_name -status-admin
down
```

2. ポートのモードを変更します。

```
ucadmin modify -node node_name -adapter adapter_name -mode fcp
```

3. ノードをリブートし、アダプタをオンラインにします。

```
network fcp adapter modify -node node_name -adapter adapter_name -status-admin
up
```

4. 状況に応じて、管理者にポートの削除を依頼するか、VIF マネージャでポートを削除します。

- 。ポートが LIF のホームポートとして使用されている場合、インターフェイスグループ（ifgrp）のメンバーである場合、または VLAN をホストしている場合は、管理者は次の作業を行う必要があります。

- i. LIF を移動するか、ifgrp からポートを削除する、または VLAN をそれぞれ削除します。
- ii. を実行して、ポートを手動で削除します network port delete コマンドを実行します

状況に応じて network port delete コマンドが失敗した場合は、エラーに対処してからもう一度コマンドを実行する必要があります。

- 。ポートが LIF のホームポートとして使用されていない場合、ifgrp のメンバーでない場合、および VLAN をホストしていない場合は、リブート時に VIF マネージャのレコードからポートが削除されます。

VIF マネージャでポートが削除されない場合は、管理者がリブート後にを使用してポートを手動で削除する必要があります network port delete コマンドを実行します

```
net-f8040-34::> network port show
```

```
Node: net-f8040-34-01
```

Port	IPspace	Broadcast	Domain	Link	MTU	Speed (Mbps) Admin/Oper	Health Status
...							
e0i	Default	Default		down	1500	auto/10	-
e0f	Default	Default		down	1500	auto/10	-
...							

```
net-f8040-34::> ucadmin show
```

Node	Adapter	Current Mode	Current Type	Pending Mode	Pending Type	Admin
Status						
net-f8040-34-01						

```

                                0e      cna      target      -      -
offline
    net-f8040-34-01
                                0f      cna      target      -      -
offline
    ...

    net-f8040-34::> network interface create -vs net-f8040-34 -lif m
    -role
    node-mgmt-home-node net-f8040-34-01 -home-port e0e -address 10.1.1.1
    -netmask 255.255.255.0

    net-f8040-34::> network interface show -fields home-port, curr-port

    vserver lif                                home-port curr-port
    -----
    Cluster net-f8040-34-01_clus1 e0a          e0a
    Cluster net-f8040-34-01_clus2 e0b          e0b
    Cluster net-f8040-34-01_clus3 e0c          e0c
    Cluster net-f8040-34-01_clus4 e0d          e0d
    net-f8040-34
        cluster_mgmt          e0M          e0M
    net-f8040-34
        m                      e0e          e0i
    net-f8040-34
        net-f8040-34-01_mgmt1 e0M          e0M
    7 entries were displayed.

    net-f8040-34::> ucaadmin modify local 0e fc

    Warning: Mode on adapter 0e and also adapter 0f will be changed to
    fc.

    Do you want to continue? {y|n}: y
    Any changes will take effect after rebooting the system. Use the
    "system node reboot" command to reboot.

    net-f8040-34::> reboot local
    (system node reboot)

    Warning: Are you sure you want to reboot node "net-f8040-34-01"?
    {y|n}: y

```

##### 5. 適切な SFP+ が取り付けられていることを確認します。

```
network fcp adapter show -instance -node -adapter
```

CNA の場合は、10Gb イーサネット SFP を使用します。FC の場合は、ノードで構成を変更する前に、8Gb SFP または 16Gb SFP を使用します。

## CNA / UTA2 ターゲットアダプタの光モジュールを変更します

ユニファイドターゲットアダプタ（CNA / UTA2）用に選択したパーソナリティモードをサポートするには、そのアダプタで光モジュールを変更する必要があります。

### 手順

1. カードで使用されている現在の SFP+ を確認します。次に、現在の SFP+ を、優先して使用するパーソナリティ（FC または CNA）に適した SFP+ に差し替えます。
2. X1143A-R6 アダプタから現在の光モジュールを取り外します。
3. 優先して使用するパーソナリティモード（FC または CNA）の光ファイバに適したモジュールを挿入します。
4. 適切な SFP+ が取り付けられていることを確認します。

```
network fcp adapter show -instance -node -adapter
```

サポートされている SFP+ モジュールと Cisco ブランドの銅線（Twinax）ケーブルについては、を参照してください "[NetApp Hardware Universe の略](#)"。

## アダプタの設定を確認します

ユニファイドターゲットアダプタ（X1143A-R6）の設定を確認するには、を実行する必要があります `system hardware unified-connect show` コマンドを使用してコントローラ上のすべてのモジュールを表示します。

### 手順

1. ケーブルを接続していない状態でコントローラをブートします。
2. を実行します `system hardware unified-connect show` コマンドを使用して、ポートの設定とモジュールを確認します。
3. ポート情報を確認してから、CNA とポートを設定します。

## FCoE コウセイ

### FCoE の設定方法の概要

FCoE は、FCoE スイッチを使用してさまざまな方法で構成できます。直接接続型の構成は FCoE ではサポートされません。

FCoE 構成はすべてデュアルファブリックです。完全な冗長性を提供し、ホスト側でマルチパスソフトウェアが必要です。すべての FCoE 構成で、イニシエータとターゲット間のパスには、最大ホップ数内であればいくつでも FCoE スイッチと FC スイッチを配置できます。スイッチ同士を接続するためには、イーサネット ISL をサポートするファームウェアバージョンがスイッチで実行されている必要があります。FCoE 構成の各ホストでオペレーティングシステムが同じである必要はありません。

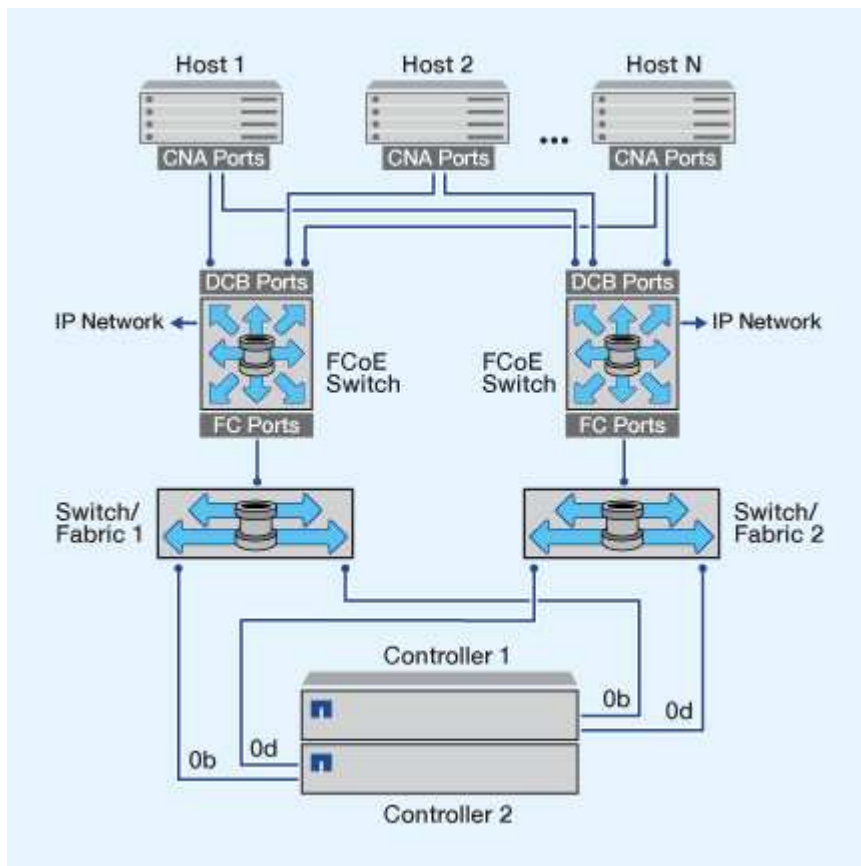
FCoE 構成では、FCoE の機能を明示的にサポートするイーサネットスイッチが必要です。FCoE 構成は、FC スイッチと同じ相互運用性と品質管理プロセスに照らして検証されます。サポートされる構成の一覧については、Interoperability Matrix を参照してください。これらのサポートされる構成には、スイッチモデル、単一ファブリックに導入可能なスイッチの数、サポートされるスイッチファームウェアのバージョンなどのパラメータが含まれています。

次の図の FC ターゲット拡張アダプタのポート番号は一例です。実際のポート番号は、FCoE ターゲット拡張アダプタがインストールされている拡張スロットによって変わる場合があります。

#### FCoE イニシエータから FC ターゲット

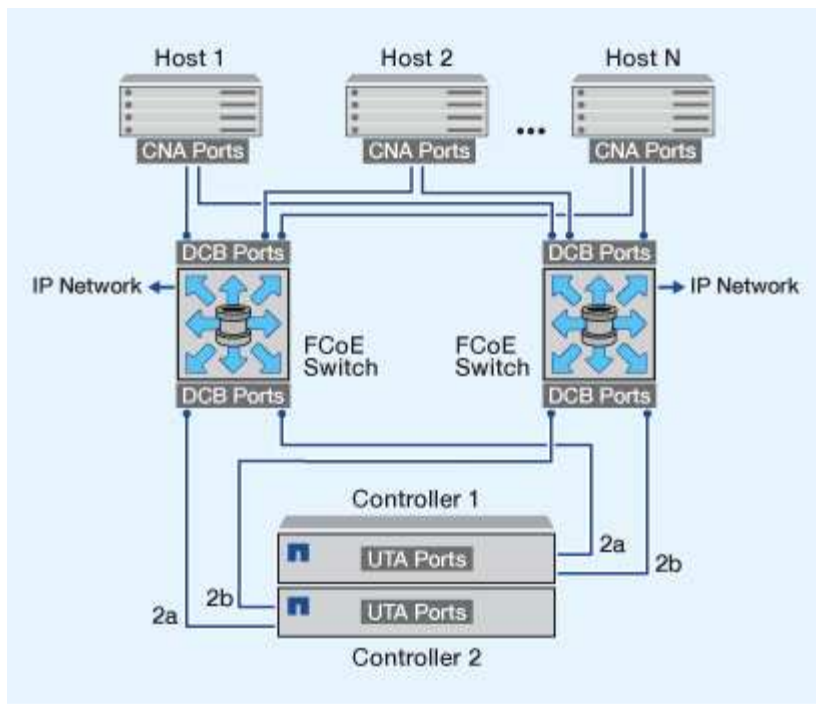
FCoE イニシエータ（CNA）を使用すると、FCoE スイッチを介して、ホストを HA ペアの両方のコントローラの FC ターゲットポートに接続できます。FCoE スイッチには FC ポートも必要です。ホストの FCoE イニシエータは、常に FCoE スイッチに接続されます。FCoE スイッチは、FC ターゲットに直接接続することも、FC スイッチを介して FC ターゲットに接続することもできます。

次の図では、ホストの CNA を FCoE スイッチに接続し、FC スイッチを HA ペアに接続しています。



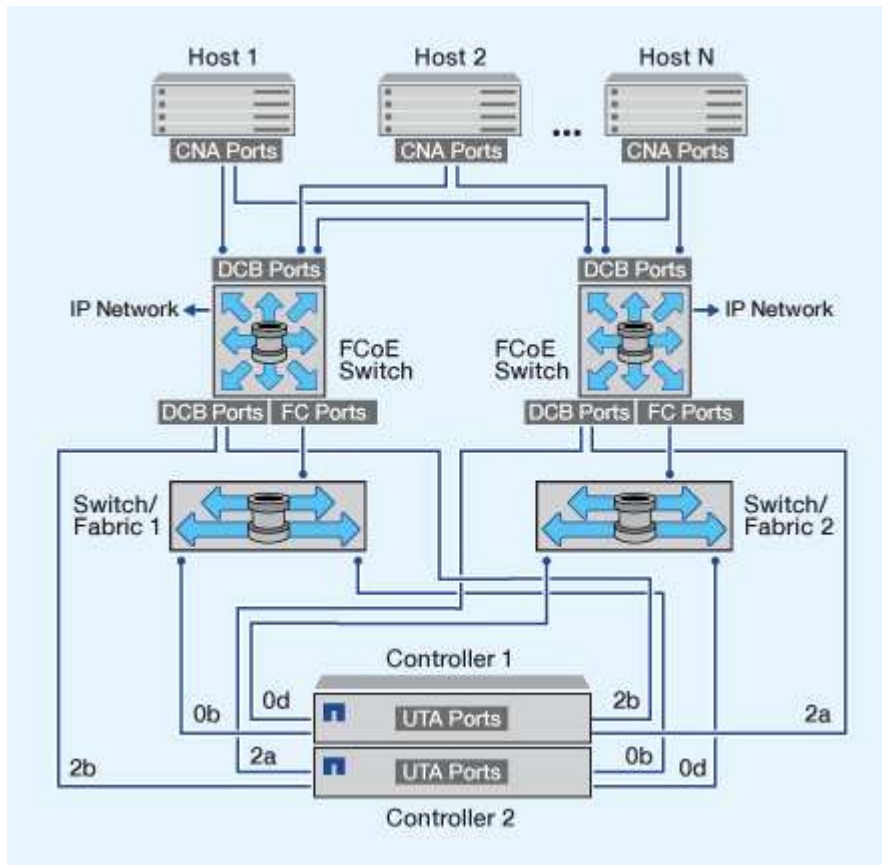
#### FCoE イニシエータから FCoE ターゲット

ホストの FCoE イニシエータ（CNA）を使用すると、FCoE スイッチを介して、ホストを HA ペアの両方のコントローラの FCoE ターゲットポート（UTA または UTA2 と呼ばれる）に接続できます。



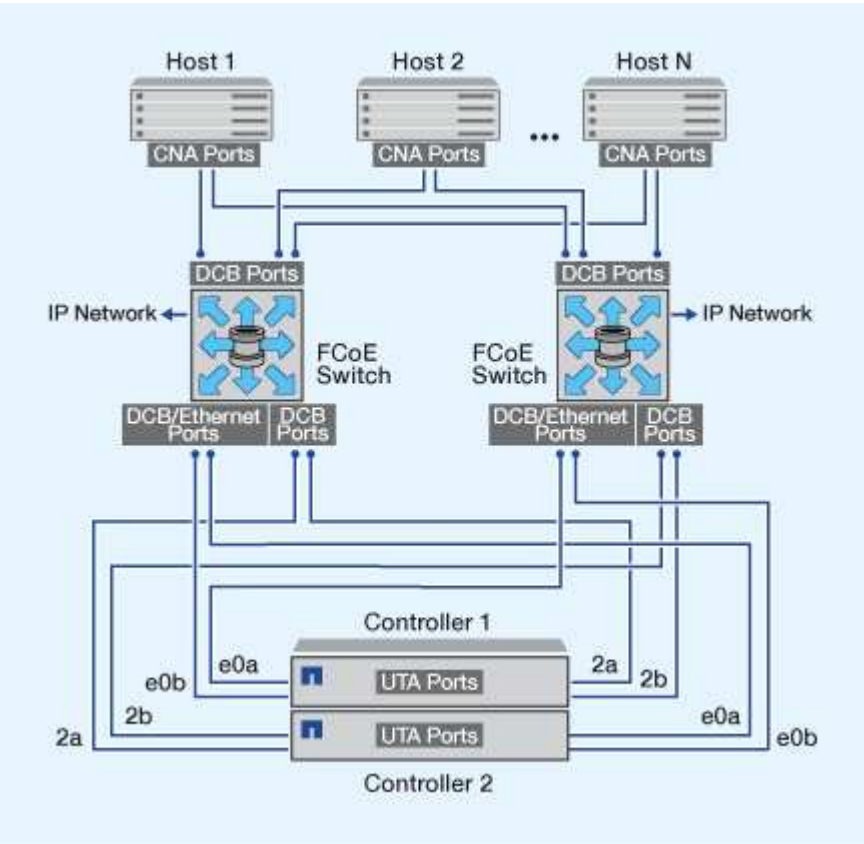
#### FCoE イニシエータから FCoE および FC ターゲット

ホストの FCoE イニシエータ（CNA）を使用すると、FCoE スイッチを介して、ホストを HA ペアの両方のコントローラの FCoE および FC ターゲットポート（UTA または UTA2 と呼ばれる）に接続できます。



FCoE と IP ストレージプロトコルの混在

ホストの FCoE イニシエータ（CNA）を使用すると、FCoE スイッチを介して、ホストを HA ペアの両方のコントローラの FCoE ターゲットポート（UTA または UTA2 と呼ばれる）に接続できます。FCoE ポートでは、単一のスイッチへの従来のリンクアグリゲーションは使用できません。Cisco スイッチは、FCoE をサポートする特別なタイプのリンクアグリゲーション（仮想ポートチャネル）をサポートします。仮想ポートチャネルは、2つのスイッチへの個別のリンクを集約します。仮想ポートチャネルは他のイーサネットトラフィックにも使用できます。NFS、SMB、iSCSI、およびその他のイーサネットトラフィックなど、FCoE以外のトラフィックに使用されるポートでは、FCoEスイッチの通常のイーサネットポートを使用できます。



FCoE イニシエータとターゲットの組み合わせ

FCoE および従来の FC のイニシエータとターゲットの特定の組み合わせがサポートされます。

FCoE イニシエータ

ホストコンピュータの FCoE イニシエータは、ストレージコントローラの FCoE ターゲットと従来の FC ターゲットの両方で使用できます。ホストの FCoE イニシエータは FCoE DCB（Data Center Bridging）スイッチに接続する必要があります。ターゲットに直接接続することはできません。

次の表に、サポートされる組み合わせを示します。

イニシエータ	ターゲット	サポートされます
FC	FC	はい。

イニシエータ	ターゲット	サポートされます
FC	FCoE	はい。
FCoE	FC	はい。
FCoE	FCoE	はい。

## FCoE ターゲット

ストレージコントローラで FCoE ターゲットポートと 4Gb、8Gb、16Gb の FC ポートを混在させることができます。FC ポートがアドインのターゲットアダプタであるかオンボードのポートであるかは関係ありません。FCoE と FC の両方のターゲットアダプタを同じストレージコントローラに搭載できます。



FC のオンボードポートと拡張ポートの組み合わせルールが引き続き適用されます。

## FCoE でサポートされるホップ数

ホストとストレージシステムの間でサポートされる Fibre Channel over Ethernet (FCoE) の最大ホップ数は、スイッチベンダー、およびストレージシステムでの FCoE 構成のサポート内容によって異なります。

ホップ数とは、イニシエータ（ホスト）とターゲット（ストレージシステム）の間のパスにあるスイッチ数です。Cisco Systems のマニュアルでは、この値のことを「SAN fabric\_ の直径」とも呼んでいます。

FCoE では、FCoE スイッチを FC スイッチに接続することができます。

エンドツーエンドの FCoE 接続では、イーサネットの Inter-Switch Link (ISL ; スイッチ間リンク) に対応したバージョンのファームウェアが FCoE スイッチで実行されている必要があります。

次の表に、サポートされる最大ホップ数を示します。

スイッチベンダー	サポートされるホップ数
Brocade	FCの場合は7  FCoE の場合は 5
シスコ	7.  FCoE スイッチは 3 台まで使用できます。

## ファイバチャネルおよび FCoE のゾーニング

### ファイバチャネルおよび FCoE のゾーニングの概要

FC ゾーン、FC-NVMe ゾーン、または FCoE ゾーンは、ファブリック内の 1 つ以上のポートを論理的にグループ化したものです。デバイス同士が互いを認識し、接続し、相

互にセッションを確立して通信できるようにするには、両方のポートに共通のゾーンメンバーシップが必要です。シングルイニシエータのゾーニングを推奨します。

#### ゾーニングを行う理由

- ・ イニシエータ HBA 間のクロストークを削減または解消できます。

これは小規模な環境でも発生し、ゾーニングを実装する最大の理由の 1 つです。ゾーニングによってファブリックの論理サブセットを作成することで、クロストークの問題が解消されます。

- ・ 特定の FC、FC-NVMe、または FCoE ポートへの使用可能なパスの数と、ホストと特定の LUN の間に認識されるパスの数を減らすことができます。

たとえば、一部のホスト OS のマルチパスソリューションには、管理できるパスの数に制限があります。ゾーニングを使用すると、OS のマルチパスドライバで認識されるパスの数を減らすことができます。ホストにマルチパス解決策がインストールされていない場合は、ファブリックのゾーニングまたは SVM の選択的 LUN マッピング（SLM）とポートセットの組み合わせを使用して、認識される LUN へのパスが 1 つだけであることを確認する必要があります。

- ・ ゾーンを共有するエンドポイントへのアクセスと接続を制限することで、セキュリティを強化します。

共通のゾーンがないポート同士が通信することはできません。

- ・ 発生する問題を切り離すことで SAN の信頼性が高まり、問題の範囲を限定することで解決時間を短縮する効果があります。

#### ゾーニングに関する推奨事項

- ・ 1 つの SAN にホストを 4 つ以上接続する場合や SAN に接続されたノードで SLM が実装されていない場合は、常にゾーニングを実装してください。
- ・ 一部のスイッチベンダーでは World Wide Node Name のゾーニングも使用できますが、特定のポートを正しく定義し、NPIV を効果的に利用するには、World Wide Port Name のゾーニングを使用する必要があります。
- ・ 管理性を損なわない範囲でゾーンサイズを制限することを推奨します。

複数のゾーンを重複させてサイズを制限することができます。ホストまたはホストクラスタごとにゾーンを定義することを推奨します。

- ・ イニシエータ HBA 間のクロストークを解消するために、単一イニシエータのゾーニングを使用してください。

#### World Wide Name に基づくゾーニング

World Wide Name（WWN；ワールドワイド名）に基づくゾーニングでは、ゾーンに含めるメンバーの WWN を指定します。ONTAP でのゾーニングでは、World Wide Port Name（WWPN）ゾーニングを使用する必要があります。

WWPN ゾーニングは柔軟性に優れており、デバイスをファブリックに接続する物理的な場所によってアクセスが制限されることがありません。ケーブルを別のポートに接続するときにゾーンを再設定する必要はありません。



ONTAP を実行するストレージコントローラへのファイバチャネルパスでは、ノードの物理ポートの WWPN ではなく、ターゲットの論理インターフェイス（LIF）の WWPN を使用して FC スイッチをゾーニングしてください。LIF の詳細については、『ONTAP ネットワーク管理ガイド』を参照してください。

## "Network Management の略"

### 個々のゾーン

推奨されるゾーニング設定では、ゾーンごとに 1 つのホストイニシエータを配置します。ゾーンは、ホストイニシエータポートとストレージノード上の 1 つ以上のターゲット LIF で構成され、ターゲットあたりの希望する数のパスまで LUN へのアクセスを提供します。つまり、同じノードにアクセスする複数のホストはお互いのポートを認識できませんが、各イニシエータはすべてのノードにアクセスできます。

Storage Virtual Machine（SVM）のすべての LIF を、ホストイニシエータがあるゾーンに追加する必要があります。これにより、既存のゾーンを編集したり、新しいゾーンを作成したりせずに、ボリュームや LUN を移動できます。

ONTAP を実行するノードへのファイバチャネルパスでは、ノードの物理ポートの WWPN ではなく、ターゲットの論理インターフェイス（LIF）の WWPN を使用して FC スイッチをゾーニングしてください。物理ポートの WWPN は「50」で始まり、LIF の WWPN は「20」で始まります。

### 単一ファブリックゾーニング

単一ファブリック構成でも、各ホストイニシエータを各ストレージノードに接続できます。複数のパスを管理するには、ホストにマルチパスソフトウェアが必要です。マルチパスで解決策の耐障害性を確保するには、各ホストに 2 つのイニシエータが必要です。

各イニシエータには、アクセス可能なノードの LIF を少なくとも 1 つ割り当てる必要があります。ホストイニシエータからクラスタ内の HA ペアのノードへのパスが少なくとも 1 つあるようにゾーニングを設定して、LUN 接続用のパスを提供する必要があります。つまり、ホスト上の各イニシエータには、そのゾーン構成内のノードごとにターゲット LIF が 1 つだけ割り当てられます。クラスタ内の同じノードまたは複数のノードへのパスが複数必要な場合は、ゾーン構成内の各ノードに複数の LIF を割り当てます。これにより、あるノードに障害が発生した場合や、LUN を含むボリュームが別のノードに移動した場合も、ホストは引き続き LUN にアクセスできます。この場合、レポートノードを適切に設定する必要があります。

単一ファブリック構成はサポートされていますが、可用性に優れているとはみなされません。1 つのコンポーネントで障害が発生すると、原因によるデータアクセスが失われる可能性があります。

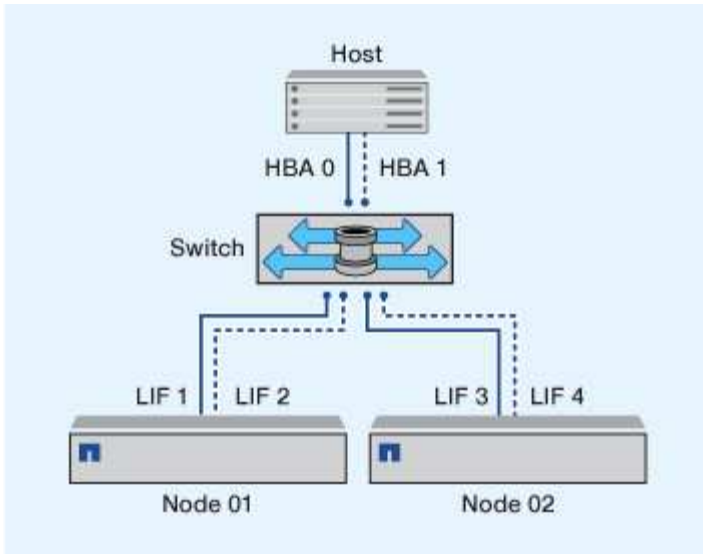
次の図では、ホストに 2 つのイニシエータがあり、マルチパスソフトウェアを実行しています。次の 2 つのゾーンがあります。



この図で使用されている命名規則は、ONTAP 解決策で使用できる一例です。

- ゾーン 1：HBA 0、LIF\_1、および LIF\_3
- ゾーン 2：HBA 1、LIF\_2、および LIF\_4

これよりもノード数が多い構成では、追加のノードの LIF がこれらのゾーンに配置されます。



この例では、各ゾーンに 4 つの LIF をすべて配置することもできます。その場合のゾーンは次のようになります。

- ゾーン 1：HBA 0、LIF\_1、LIF\_2、LIF\_3、および LIF\_4
- ゾーン 2：HBA 1、LIF\_1、LIF\_2、LIF\_3、および LIF\_4



ホスト OS とマルチパスソフトウェアが、ノード上の LUN へのアクセスに使用される数のパスをサポートしている必要があります。ノードの LUN へのアクセスに使用するパスの数については、SAN 構成の制限に関するセクションを参照してください。

#### 関連情報

["NetApp Hardware Universe の略"](#)

#### デュアルファブリックの HA ペアのゾーニング

デュアルファブリック構成では、各ホストイニシエータを各クラスタノードに接続できます。各ホストイニシエータは、異なるスイッチを使用してクラスタノードにアクセスできます。複数のパスを管理するには、ホストにマルチパスソフトウェアが必要です。

1 つのコンポーネントで障害が発生してもデータへのアクセスは維持されるため、デュアルファブリック構成はハイアベイラビリティとみなされます。

次の図では、ホストに 2 つのイニシエータがあり、マルチパスソフトウェアを実行しています。2 つのゾーンがあります。SLM では、すべてのノードがレポートノードとなるように設定されています。



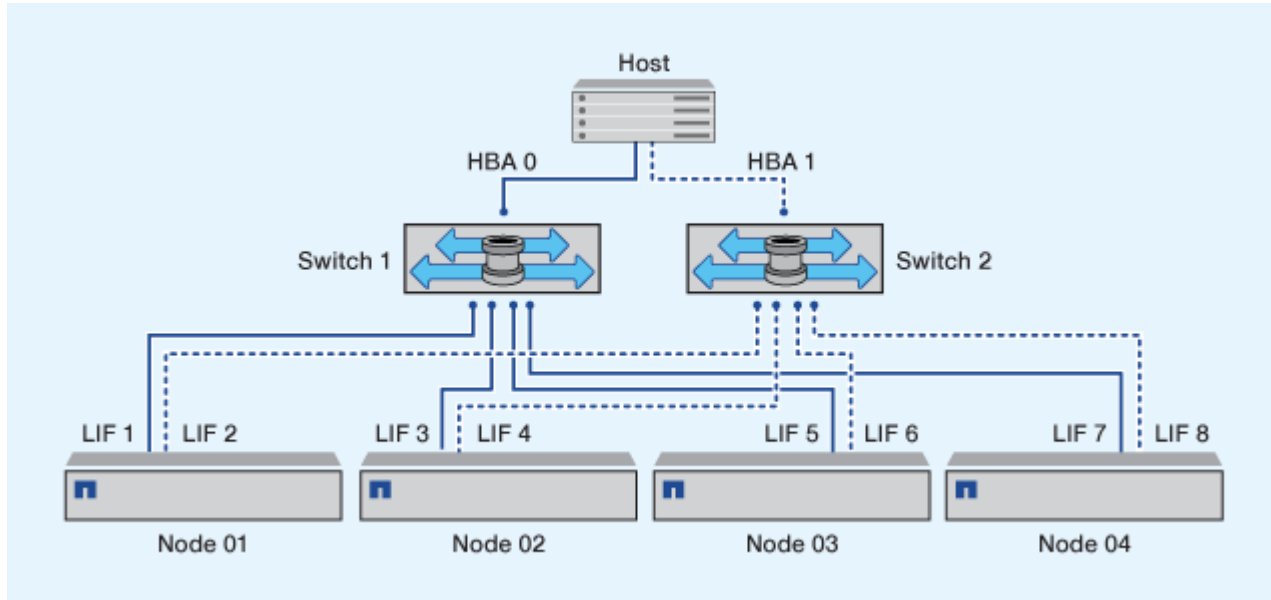
この図で使用されている命名規則は、ONTAP 解決策で使用できる一例です。

- ゾーン 1：HBA 0、LIF\_1、LIF\_3、LIF\_5、および LIF\_7
- ゾーン 2：HBA 1、LIF\_2、LIF\_4、LIF\_6、および LIF\_8

各ホストイニシエータは、異なるスイッチを使用してゾーニングされています。ゾーン 1 には、スイッチ 1 からアクセスします。ゾーン 2 にはスイッチ 2 からアクセスします。

各イニシエータは、すべてのノードの LIF にアクセスできます。これにより、あるノードで障害が発生しても、ホストは引き続き LUN にアクセスできます。SVM は、選択的 LUN マップ（SLM）とレポートノードの設定に基づいて、clustered 解決策のすべてのノードのすべての iSCSI LIF と FC LIF にアクセスできます。SLM、ポートセット、または FC スイッチゾーニングを使用することで、SVM からホストへのパスの数と SVM から LUN へのパスの数を少なくすることができます。

これよりもノード数が多い構成では、追加のノードの LIF がこれらのゾーンに配置されます。



ホスト OS とマルチパスソフトウェアが、ノード上の LUN へのアクセスに使用される数のパスをサポートしている必要があります。

#### 関連情報

["NetApp Hardware Universe の略"](#)

#### Cisco FC および FCoE スイッチのゾーニング制限

Cisco FC スイッチおよび FCoE スイッチを使用する場合、1つのファブリックゾーンに同じ物理ポートのターゲット LIF を複数含めることはできません。同じポートの LIF を同じゾーンに複数配置すると、接続が失われた場合に LIF ポートがリカバリできなくなる可能性があります。

FC-NVMe プロトコルには、通常の FC スイッチが FC プロトコルとまったく同じ方法で使用されます。

- FC および FCoE プロトコルの複数の LIF は、ゾーンが同じでなければノード上の物理ポートを共有することができます。
- FC-NVMe と FCoE は、同じ物理ポートを共有できません。
- FC と FC-NVMe は、同じ 32Gb 物理ポートを共有できます。
- Cisco FC スイッチおよび FCoE スイッチでは、特定のポートの各 LIF をそのポートの他の LIF とは別のゾーンに配置する必要があります。
- 1つのゾーンに FC と FCoE 両方の LIF を配置することができます。ゾーンにはクラスタ内のすべてのターゲットポートの LIF を配置することができますが、ホストのパス制限を超えないように注意し、SLM

の設定を確認してください。

- 物理ポートが異なる LIF は、同じゾーンに配置することもできます。
- Cisco スイッチを使用する場合は、LIF を分離する必要があります。

必須ではありませんが、LIF の分離はすべてのスイッチで推奨されます

## 共有 SAN 構成の要件

共有 SAN 構成とは、ホストを ONTAP ストレージシステムと他社のストレージシステムの両方に接続する構成です。単一のホストから ONTAP ストレージシステムと他社のストレージシステムにアクセスする場合は、いくつかの要件を満たす必要があります。

いずれのホストオペレーティングシステムでも、各ベンダーのストレージシステムへの接続には別々のアダプタを使用することを推奨します。別々のアダプタを使用すると、ドライバや設定が競合する可能性が低くなります。ONTAP ストレージシステムへの接続には、NetApp Interoperability Matrix Tool にサポート対象として記載されたアダプタモデル、BIOS、ファームウェア、ドライバを使用する必要があります。

必須または推奨のタイムアウト値やホストのその他のストレージパラメータを設定します。ネットアップソフトウェアのインストールやネットアップ設定の適用は必ず最後に行ってください。

- AIX の場合、構成に対応する AIX Host Utilities バージョンの値を Interoperability Matrix Tool で確認して適用します。
- ESX の場合、Virtual Storage Console for VMware vSphere を使用してホスト設定を適用します。
- HP-UX の場合、HP-UX のデフォルトのストレージ設定を使用します。
- Linux の場合、構成に対応する Linux Host Utilities バージョンの値を Interoperability Matrix Tool で確認して適用します。
- Solaris の場合、構成に対応する Solaris Host Utilities バージョンの値を Interoperability Matrix Tool で確認して適用します。
- Windows の場合、構成に対応する Windows Host Utilities のバージョンを Interoperability Matrix Tool で確認してインストールします。

### 関連情報

["NetApp Interoperability Matrix Tool で確認できます"](#)

## MetroCluster 環境の SAN 構成

### MetroCluster 環境の SAN 構成

MetroCluster 環境で SAN 構成を使用する際の注意事項は次のとおりです。

- MetroCluster 構成では ' フロントエンド FC ファブリックのルーテッド VSAN 構成はサポートされません
- ONTAP 9.12.1以降では、NVMe/FCで4ノードMetroCluster IP構成がサポートされます。MetroCluster構成はNVMe/TCPではサポートされません。MetroCluster 構成はONTAP 9.12.1よりも前のNVMeではサポートされません。
- MetroCluster 構成では、iSCSI、FC、FCoEなどの他のSANプロトコルがサポートされます。

- SANクライアント構成を使用している場合は、に記載されているメモにMetroCluster 構成に関する特別な考慮事項がないかどうかを確認する必要があります ["NetApp Interoperability Matrix Tool で確認できます"](#) IMT
- オペレーティングシステムとアプリケーションでは、MetroCluster の自動計画外スイッチオーバーとTiebreakerまたはメディエーターから開始されたスイッチオーバーをサポートするために、120秒のI/O耐障害性を提供する必要があります。
- フロントエンド SAN の両側で MetroCluster が同じ WWPN を使用している。

#### 関連情報

- ["MetroCluster のデータ保護とディザスタリカバリについて理解する"](#)
- ["技術情報アーティクル：「What are AIX Host support considerations in a MetroCluster configuration？」"](#)
- ["技術情報アーティクル：「Solaris host support considerations in a MetroCluster configuration」"](#)

スイッチオーバーとスイッチバックの間でポートが重複しないようにする

SAN環境では、古いポートがオフラインになって新しいポートがオンラインになったときに重複しないように、フロントエンドスイッチを設定できます。

スイッチオーバーの実行中に、ディザスタサイトの FC ポートがオフラインで、このポートがネームサービスとディレクトリサービスから削除されたことをファブリックが検出するまで、サバイバーサイトの FC ポートがファブリックにログインすることがあります。

災害時に FC ポートがまだ削除されていないと、WWPN の重複が原因で、サバイバーサイトでの FC ポートのファブリックログインが拒否される可能性があります。FC スイッチのこの動作は、既存のデバイスではなく、前のデバイスのログインに合わせて変更できます。この動作が他のファブリックデバイスに与える影響を確認してください。詳細については、スイッチベンダーにお問い合わせください。

スイッチのタイプに応じて、適切な手順 を選択します。

## 例 14. 手順

### Cisco スイッチ

1. スイッチに接続してログインします。
2. コンフィギュレーションモードを開始します。

```
switch# config t
switch(config)#
```

3. ネームサーバデータベースの最初のデバイスエントリを新しいデバイスで上書きします。

```
switch(config)# no fcns reject-duplicate-pwwn vsan 1
```

4. NX-OS 8.x を実行しているスイッチで、flogi quiesce タイムアウトが 0 に設定されていることを確認します。

- a. 休止期間を表示します。

```
switch(config)# show flogi interval info \ i quiesce
```

```
Stats:  fs flogi quiesce timerval:  0
```

- b. 前の手順の出力で時刻がゼロであることが示されない場合は、0 に設定します。

```
switch(config)# flogi scale enable
```

```
switch(config)$ flogi quiesce timeout 0
```

### Brocade スイッチ

1. スイッチに接続してログインします。
2. を入力します switchDisable コマンドを実行します
3. を入力します configure コマンドを入力し、を押します y をクリックします。

```
F-Port login parameters (yes, y, no, n): [no] y
```

4. 設定 1 を選択：

```
- 0: First login take precedence over the second login (default)
- 1: Second login overrides first login.
- 2: the port type determines the behavior
Enforce FLOGI/FDISC login: (0..2) [0] 1
```

5. 残りのプロンプトに応答するか、\* Ctrl+D\* を押します。

6. を入力します switchEnable コマンドを実行します

## 関連情報

["テストまたはメンテナンスのためのスイッチオーバーの実行"](#)

## ホストでのマルチパスのサポート

### ホストでのマルチパスのサポートの概要

ONTAP では、FC と iSCSI のどちらのパスにも必ず Asymmetric Logical Unit Access （ALUA；非対称論理ユニットアクセス）が使用されます。FC プロトコルと iSCSI プロトコルに対して ALUA をサポートするホスト構成を使用してください。

ONTAP 9.5 以降では、Asynchronous Namespace Access （ANA）を使用する NVMe 構成で、マルチパス HA ペアのフェイルオーバー / ギブバックがサポートされます。ONTAP 9.4 では、NVMe でサポートされるホストからターゲットへのパスは 1 つだけです。アプリケーションホストは、ハイアベイラビリティ（HA）パートナーへのパスのフェイルオーバーを管理する必要があります。

ALUA または ANA をサポートする具体的なホスト設定については、を参照してください ["NetApp Interoperability Matrix Tool で確認できます"](#) および ["ONTAP SAN ホスト構成"](#) ホストオペレーティングシステムに応じて異なります。

### ホストのマルチパスソフトウェアが必要になる状況

Storage Virtual Machine （SVM）の論理インターフェイス（LIF）からファブリックへのパスが複数ある場合、マルチパスソフトウェアが必要です。ホストが複数のパスで LUN にアクセスできる場合は、ホストにマルチパスソフトウェアが必要です。

マルチパスソフトウェアは、LUN へのすべてのパスを単一のディスクとしてオペレーティングシステムに表示します。マルチパスソフトウェアがない場合、各パスが別々のディスクとしてオペレーティングシステムに認識されるため、データの破損を招くことがあります。

次のいずれかに該当する場合、解決策に複数のパスがあるとみなされます。

- ホストの 1 つのイニシエータポートを SVM の複数の SAN LIF に接続している場合
- 複数のイニシエータポートを SVM の単一の SAN LIF に接続しています
- 複数のイニシエータポートを SVM の複数の SAN LIF に接続しています

HA 構成では、マルチパスソフトウェアの使用を推奨します。選択的 LUN マップに加え、FC スイッチのゾーニングまたはポートセットを使用して、LUN へのアクセスに使用するパスを制限することを推奨します。



マルチパスソフトウェアは、マルチパス I/O（MPIO）ソフトウェアとも呼ばれます。

ホストからクラスタ内のノードへの推奨されるパス数

ホストからクラスタ内の各ノードへのパスは 8 個までにすることを推奨します。ホスト OS やホストで使用されるマルチパスでサポートされるパスの総数に注意が必要です。

選択的 LUN マップ（SLM）を使用して、クラスタ内の Storage Virtual Machine（SVM）で使用される各レポートノードへのパスを LUN ごとに少なくとも 2 つ確保します。これにより、単一点障害が排除され、コンポーネント障害に備えてシステムの運用を継続することができます。

クラスタにノードが 4 つ以上ある場合、またはいずれかのノードの SVM で 5 つ以上のターゲットポートを使用している場合は、ノード上の LUN へのアクセスに使用できるパスの数を制限し、推奨される最大数である 8 個以内にするには、次の方法を使用します。

- SLM

SLM は、ホストから LUN へのパスを、LUN を所有するノード上のパスと所有者ノードの HA パートナーのパスだけに制限します。SLM はデフォルトでは有効になっています。

- iSCSI のポートセット
- ホストの FC igroup マッピング
- FC スイッチゾーニング

関連情報

["SAN 管理"](#)

## 構成の制限

**SAN** 構成でサポートされるノード数を確認

ONTAP でサポートされるクラスタあたりのノード数は、ONTAP のバージョン、クラスタ内のストレージコントローラのモデル、およびクラスタノードのプロトコルによって異なります。

このタスクについて

FC、FC-NVMe、FCoE、または iSCSI が設定されたノードがクラスタにある場合、そのクラスタには SAN ノードの制限が適用されます。クラスタ内のコントローラに基づくノードの制限については、[Hardware Universe](#) を参照してください。

手順

1. に進みます ["NetApp Hardware Universe の略"](#)。
2. 左上の [\* ホーム] ボタンの横にある [\* プラットフォーム] をクリックし、プラットフォームの種類を選択します。
3. 使用している ONTAP のバージョンの横にあるチェックボックスをオンにします。

プラットフォームを選択するための新しい列が表示されます。



4. 解決策で使用しているプラットフォームの横にあるチェックボックスをオンにします。
5. [仕様を選択] 列の [すべて選択 \*] チェックボックスをオフにします。
6. [クラスタあたりの最大ノード数 (NAS / SAN) \*] チェックボックスをオンにします。
7. [結果を表示 (Show Results)] をクリックする。

#### 関連情報

["NetApp Hardware Universe の略"](#)

**FC 構成および FC-NVMe 構成**におけるクラスタあたりのサポートされるホスト数を確認します

クラスタに接続できる SAN ホストの最大数は、クラスタの各ノードに接続されるホストの数、ホストあたりのイニシエータ数、ホストあたりのセッション数、クラスタ内のノード数など、クラスタのさまざまな属性の組み合わせによって大きく異なります。

#### このタスクについて

FC 構成および FC-NVMe 構成では、システムの Initiator-Target Nexus (ITN ; イニシエータ - ターゲット接続) の数に基づいて、クラスタにホストを追加できるかどうかを判断します。

1 つの ITN は、ホストのイニシエータからストレージシステムのターゲットへの 1 つのパスに該当します。FC 構成および FC-NVMe 構成のノードあたりの最大 ITN 数は 2、048 です。ITN がこの最大数を超えない限り、クラスタにホストを追加することができます。

クラスタで使用されている ITN の数を確認するには、クラスタの各ノードで次の手順を実行します。

#### 手順

1. ノードの LIF をすべて特定します。
2. ノードのすべての LIF に対して次のコマンドを実行します。

```
fcf initiator show -fields wwpn, lif
```

コマンド出力の一番下に表示されたエントリ数が、その LIF の ITN 数です。

3. それぞれの LIF について、表示された ITN 数を記録します。
4. クラスタのすべてのノードの各 LIF の ITN 数を合計します。

この値がクラスタの ITN の総数になります。

**iSCSI 構成**でサポートされるホスト数を確認します

iSCSI 構成で接続できる SAN ホストの最大数は、クラスタの各ノードに接続されるホストの数、ホストあたりのイニシエータ数、ホストあたりのログイン数、クラスタ内のノード数など、クラスタのさまざまな属性の組み合わせによって大きく異なります。

#### このタスクについて

ノードに直接または 1 つ以上のスイッチを介して接続できるホストの数は、使用可能なイーサネットポートの数で決まります。使用可能なイーサネットポートの数は、コントローラのモデル、およびコントローラにインストールされているアダプタの数とタイプによって決まります。コントローラおよびアダプタでサポートさ

れるイーサネットポートの数は、\_ Hardware Universe \_ で確認できます。

マルチノードクラスタ構成の場合は、ノードあたりの iSCSI セッションの数に基づいて、クラスタにホストを追加できるかどうかを判断する必要があります。ノードあたりの iSCSI セッションの最大数をクラスタが下回っている場合は、引き続きクラスタにホストを追加できます。ノードあたりの iSCSI セッションの最大数は、クラスタ内のコントローラのタイプによって異なります。

#### 手順

1. ノードのターゲットポータルグループをすべて特定します。
2. ノードのすべてのターゲットポータルグループについて、それぞれ iSCSI セッションの数を確認します。

```
iscsi session show -tpgroup tpgroup
```

コマンド出力の一番下に表示されたエントリ数が、そのターゲットポータルグループの iSCSI セッション数です。

3. 各ターゲットポータルグループについて、表示された iSCSI セッション数を記録します。
4. ノードの各ターゲットポータルグループの iSCSI セッション数を追加します。

この値がノードの iSCSI セッションの総数になります。

#### FC スイッチの構成の制限

ファイバチャネルスイッチには、ポート、ポートグループ、ブレード、およびスイッチごとにサポートされるログイン数など、最大構成制限があります。サポートされる制限については、スイッチベンダーから文書化されています

各 FC の Logical Interface (LIF ; 論理インターフェイス) が FC のスイッチポートにログインします。ノードの 1 つのターゲットからのログインの総数は、LIF の数に、基盤となる物理ポートへのログイン数として 1 を足した数です。スイッチベンダーが設定しているログインやその他の構成値の制限を超えないようにしてください。これは、NPIV が有効な仮想環境のホスト側で使用されているイニシエータにも当てはまります。解決策で使用されているターゲットまたはイニシエータのログインについては、スイッチベンダーが設定している制限を超えないようにしてください。

#### Brocade スイッチの最大数

Brocade スイッチの最大構成数は、\_ Brocade 拡張性ガイドライン \_ で確認できます。

#### Cisco Systems スイッチの最大数

Cisco スイッチの構成の制限については、を参照してください "[Cisco の設定の制限](#)" 使用している Cisco スイッチソフトウェアのバージョンに対応したガイドです。

#### キュー深度の算出の概要

ノードあたりおよび FC ポートのファンインあたりの ITN 数を最大にするために、ホストの FC キュー深度の調整が必要になる場合があります。LUN の最大数と 1 つの FC ポートに接続できる HBA の数は、FC ターゲットポートで使用可能なキューの深さによって制限されます。

このタスクについて

キュー深度は、ストレージコントローラで一度にキューに格納することができる、I/O 要求（SCSI コマンド）の数です。ホストのイニシエータ HBA からストレージコントローラのターゲットアダプタへの I/O 要求ごとに、キューエントリが 1 つ作成されます。一般に、キュー深度を大きくするとパフォーマンスが向上します。ただし、ストレージコントローラの最大キュー深度に達すると、ストレージコントローラは QFULL 応答を返して受け取ったコマンドを拒否します。QFULL 状態はシステムパフォーマンスの大幅な低下を招き、一部のシステムではエラーを引き起こすこともあります。そのため、1 台のストレージコントローラに多数のホストがアクセスしている環境では、QFULL が発生しないように慎重に計画してください。

複数のイニシエータ（ホスト）を含む構成では、すべてのホストでキュー深度を同程度に設定する必要があります。同じターゲットポートを介してストレージコントローラに接続されたホスト間では、キュー深度に応じてリソースへのアクセスに差があり、キュー深度が小さいホストよりもキュー深度の大きいホストのアクセスが優先されます。

キュー深度を「チューニング」する場合は、次の一般的な推奨事項を考慮してください。

- 小規模から中規模のシステムでは、HBA キュー深度を 32 にする。
- 大規模のシステムでは、HBA キュー深度を 128 にする。
- 例外的なケースまたはパフォーマンステストでは、キュー深度を 256 にしてキュー関連の問題の発生を回避します。
- すべてのホストにアクセスが均等になるように、すべてのホストでキュー深度を同程度に設定する必要があります。
- パフォーマンスの低下やエラーを回避するために、ストレージコントローラのターゲット FC ポートのキュー深度を超えないようにする。

#### 手順

1. 1 つの FC ターゲットポートに接続しているすべてのホストの FC イニシエータの数を数えます。
2. 128 をかけます。
  - 2、048 より小さい場合は、すべてのイニシエータのキュー深度を 128 に設定します。  
15 台のホストがあり、1 つのイニシエータがストレージコントローラ上の 2 つのターゲットポートのそれぞれに接続されています。 $15 \times 128 = 1,920$ 。これは合計最大キュー深度の 2、048 より少ないため、すべてのイニシエータのキュー深度を 128 に設定できます。
  - この値が 2、048 よりも大きい場合は、手順 3 に進みます。  
30 台のホストがあり、1 つのイニシエータがストレージコントローラ上の 2 つのターゲットポートのそれぞれに接続されています。 $30 \times 128 = 3,840$ 。これは合計最大キュー深度の 2、048 より大きいため、手順 3 に記載されているいずれかのオプションを実行して調整します。
3. 次のいずれかのオプションを選択して、ストレージコントローラにホストを追加します。
  - オプション 1：
    - i. FC ターゲットポートを追加します。
    - ii. FC イニシエータを再配分します。
  - iii. 手順 1 と 2. を繰り返します。  
[+]  
必要とされるキュー深度 3、840 は、ポートあたりの使用可能なキュー深度を超えています。この状態を解決するために、各コントローラに 2 ポートの FC ターゲットアダプタを追加し、30 台のホストのうち 15 台が 1 つのポートセットに接続され、残りの 15 台のホストが 2 つ目のポートセットに接続されるように FC スイッチをゾーニングし直します。これで、ポートあたりのキュー

深度は  $15 \times 128 = 1,920$  となります。

。オプション2：

- i. 各ホストを「ラージ」または「モール」として指定します。これは、予想される I/O ニーズに基づいています。
- ii. 大規模イニシエータの台数に 128 をかけます。
- iii. 小規模イニシエータの台数に 32 をかけます。
- iv. 2 つの結果をまとめて追加します。
- v. 2,048 より小さい場合は、大規模ホストのキュー深度を 128 に、小規模ホストのキュー深度を 32 に設定します。
- vi. 2,048 よりも大きい場合は、合計キュー深度が 2,048 以下になるまで各イニシエータのキュー深度を下げます。

特定の 1 秒あたりの I/O スループットに必要なキュー深度を算出するには、次の式を使用します。



必要なキュー深度 = (IOPS) × (応答時間)

たとえば、応答時間 3 ミリ秒で 40,000 IOPS のスループットに必要なキュー深度は、 $40,000 \times (.003) = 120$  です。

基本的な推奨構成である 32 個にキュー深度を制限した場合、ターゲットポートに接続できるホストの最大数は 64 です。ただし、キュー深度を 128 にした場合は、1 つのターゲットポートに接続できるホストの最大数は 16 になります。キュー深度が大きいほど、1 つのターゲットポートでサポートできるホストの数は少なくなります。キュー深度を小さくできないような要件がある場合は、ターゲットポートを増やしてください。

必要とされるキュー深度 3,840 は、ポートあたりの使用可能なキュー深度を超えています。ストレージ I/O のニーズが高い「大規模」ホストが 10 台あり、I/O のニーズが低い「モール」ホストが 20 台あります。大規模ホストのイニシエータのキュー深度を 128 に、小規模ホストのイニシエータのキュー深度を 32 に設定します。

その結果、合計キュー深度は  $(10 \times 128) + (20 \times 32) = 1,920$  になります。

使用可能なキュー深度を、各イニシエータに均等に分配できます。

そのため、イニシエータあたりのキュー深度は  $2,048 \div 30 = 68$  となります。

### SAN ホストでキュー深度を設定します

ノードあたりおよび FC ポートのファンインあたりの ITN 数を最大にするために、ホストのキュー深度の変更が必要になる場合があります。

#### AIX ホスト

を使用して、AIXホストのキュー深度を変更できます chdev コマンドを実行しますを使用して行った変更 chdev コマンドはリブート後も維持されます。

#### 例

- `hdisk7` デバイスのキュー深度を変更するには、次のコマンドを使用します。

```
chdev -l hdisk7 -a queue_depth=32
```

- `fcs0` HBA のキュー深度を変更するには、次のコマンドを使用します。

```
chdev -l fcs0 -a num_cmd_elems=128
```

のデフォルト値 `num_cmd_elems` 200です最大値は 2、048 です。



変更するには、必要に応じてHBAをオフラインにします `num_cmd_elems` を使用してオンラインに戻します `rmdev -l fcs0 -R` および `makdev -l fcs0 -P` コマンド

## HP-UX ホスト

HP-UXホストのLUNまたはデバイスのキュー深度は、`kernel`パラメータを使用して変更できます `scsi_max_qdepth`。HBAのキュー深度は、カーネルパラメータを使用して変更できます `max_fcp_reqs`。

- のデフォルト値 `scsi_max_qdepth` 8です最大値は255です。

`scsi_max_qdepth` を使用して、実行中のシステムで動的に変更できます `-u` オプションを選択します `kmtune` コマンドを実行します変更は、システム上のすべてのデバイスに有効です。たとえば、LUN のキュー深度を 64 に増やすには、次のコマンドを使用します。

```
kmtune -u -s scsi_max_qdepth=64
```

を使用して、個々のデバイスファイルのキュー深度を変更できます `scsictl` コマンドを実行しますを使用して変更を行います `scsictl` コマンドの設定は、システムのリブート後は維持されません。特定のデバイスファイルのキュー深度を表示および変更するには、次のコマンドを実行します。

```
scsictl -a /dev/rdisk/c2t2d0
```

```
scsictl -m queue_depth=16 /dev/rdisk/c2t2d0
```

- のデフォルト値 `max_fcp_reqs` 512です最大値は 1024 です。

を変更するには、カーネルを再構築し、システムを再起動する必要があります `max_fcp_reqs` 有効にします。たとえば、HBA のキュー深度を 256 に変更するには、次のコマンドを使用します。

```
kmtune -u -s max_fcp_reqs=256
```

## Solaris ホストの場合

Solaris ホストの LUN および HBA のキュー深度を設定できます。

- LUN のキュー深度の場合：ホストで使用中の LUN の数に LUN あたりのスロットル (`lun-queue-depth`) をかけた値が、ホストの `tgt-queue-depth` の値以下になる必要があります。
- Sunスタックのキュー深度の場合：標準ドライバでは、LUN単位またはターゲット単位ではサポートされていません `max_throttle` HBAレベルの設定。を設定するための推奨方法 `max_throttle` ネイティブドライバの値は、のデバイスタイプごと (`VID_PID`) レベルです `/kernel/drv/sd.conf` および

/kernel/drv/ssd.conf ファイル。ホストユーティリティでは、この値が MPxIO 構成では 64、Veritas DMP 構成では 8 に設定されます。

#### 手順

1. # cd/kernel/drv
2. # vi lpfc.conf
3. を検索します /tgt-queue (/tgt-queue)

```
tgt-queue-depth=32
```



デフォルト値はインストール時に 32 に設定されています。

4. 環境の構成に基づいて目的の値を設定します。
5. ファイルを保存します。
6. を使用してホストをリブートします sync; sync; sync; reboot -- -r コマンドを実行します

#### QLogic HBA の VMware ホスト

を使用します esxcfg-module HBAタイムアウト設定を変更するコマンド。を手動で更新します esx.conf ファイルは推奨されません。

#### 手順

1. root ユーザとしてサービスコンソールにログオンします。
2. を使用します #vmkload\_mod -l 現在ロードされているQlogic HBAモジュールを確認するコマンド。
3. Qlogic HBA の単一インスタンスの場合は、次のコマンドを実行します。

```
#esxcfg-module -s ql2xmaxqdepth=64 qla2300_707
```



この例では qla2300\_707 が使用されています。の出力に基づいて、適切なモジュールを使用します vmkload\_mod -l。

4. 次のコマンドを使用して変更を保存します。

```
#!/usr/sbin/esxcfg-boot -b
```

5. 次のコマンドを使用してサーバをリブートします。

```
#reboot
```

6. 次のコマンドを使用して変更を確認します。

a. #esxcfg-module -g qla2300\_707

b. qla2300\_707 enabled = 1 options = 'ql2xmaxqdepth=64'

#### Emulex HBA の VMware ホスト

を使用します esxcfg-module HBAタイムアウト設定を変更するコマンド。を手動で更新します esx.conf

ファイルは推奨されません。

#### 手順

1. root ユーザとしてサービスコンソールにログオンします。
2. を使用します `#vmkload_mod -l grep lpfc` コマンドを実行して、どのEmulex HBAが現在ロードされているかを確認します。
3. Emulex HBA の単一インスタンスの場合は、次のコマンドを入力します。

```
#esxcfg-module -s lpfc0_lun_queue_depth=16 lpfcdd_7xx
```



HBA のモジュールに応じて、最後の部分には `lpfcdd_7xx` または `lpfcdd_732` を指定します。このコマンドでは `lpfcdd_7xx` モジュールを指定しています。の結果に基づいて、適切なモジュールを使用する必要があります `vmkload_mod -l`。

このコマンドを実行すると、`lpfc0` で表される HBA に対して LUN のキュー深度を 16 に設定します。

4. Emulex HBA の複数のインスタンスの場合は、次のコマンドを実行します。

```
a esxcfg-module -s "lpfc0_lun_queue_depth=16 lpfc1_lun_queue_depth=16"
lpfcdd_7xx
```

`lpfc0` に対する LUN のキュー深度と `lpfc1` に対する LUN のキュー深度が 16 に設定されます。

5. 次のコマンドを入力します。

```
#esxcfg-boot -b
```

6. を使用してリブートします `#reboot`。

#### Emulex HBA の Windows ホスト

Windowsホストでは、を使用できます `LPUTILNT` Emulex HBAのキュー深度を更新するユーティリティ。

#### 手順

1. を実行します `LPUTILNT` にあるユーティリティ `C:\WINNT\system32` ディレクトリ。
2. 右側のメニューから `* Drive Parameters *` (ドライブパラメータ) を選択します。
3. スクロールダウンして、`[QueueDepth]` をダブルクリックします。



150 より大きい `* QueueDepth *` を設定する場合は、次の Windows レジストリ値も適切に増やす必要があります。

```
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\lpxnds\Parameters\Device\NumberOfRequests
```

#### Qlogic HBA の Windows ホスト

Windowsホストでは、およびを使用できます `SANsurfer` Qlogic HBAのキュー深度を更新するHBAマネージャユーティリティ。



## 手順

1. を実行します SANsurfer HBAマネージャユーティリティ。
2. [\* HBA ポート > 設定] をクリックします。
3. リスト・ボックスの \* HBA ポートの詳細設定 \* をクリックします。
4. を更新します Execution Throttle パラメータ

## Emulex HBA の Linux ホスト

Linux ホストでは Emulex HBA のキュー深度を更新できます。更新をリブート後も維持するには、新しい RAM ディスクイメージを作成してホストをリブートする必要があります。

## 手順

1. 変更するキュー深度パラメータを特定します。

```
modinfo lpfc|grep queue_depth
```

キュー深度パラメータとその概要のリストが表示されます。使用しているオペレーティングシステムのバージョンに応じて、次のキュー深度パラメータを 1 つ以上変更できます。

- lpfc\_lun\_queue\_depth：特定のLUNのキューに格納できるFCコマンドの最大数 (uint)
  - lpfc\_hba\_queue\_depth：lpfc HBAのキューに格納できるFCコマンドの最大数 (uint)
  - lpfc\_tgt\_queue\_depth：特定のターゲットポートのキューに格納できるFCコマンドの最大数 (uint)
- 。 lpfc\_tgt\_queue\_depth パラメータは、Red Hat Enterprise Linux 7.xシステム、SUSE Linux Enterprise Server 11 SP4システム、および12.xシステムにのみ適用されます。

2. にキュー深度パラメータを追加して、キュー深度を更新します /etc/modprobe.conf ファイル (Red Hat Enterprise Linux 5.xシステム用) を参照してください /etc/modprobe.d/scsi.conf ファイル (Red Hat Enterprise Linux 6.xまたは7.xシステム、またはSUSE Linux Enterprise Server 11.xまたは12.xシステム用)

使用しているオペレーティングシステムのバージョンに応じて、次のコマンドを 1 つ以上追加できます。

- options lpfc lpfc\_hba\_queue\_depth=new\_queue\_depth
- options lpfc lpfc\_lun\_queue\_depth=new\_queue\_depth
- options lpfc lpfc\_tgt\_queue\_depth=new\_queue\_depth

3. 新しい RAM ディスクイメージを作成し、ホストをリブートして、リブート後も更新内容を維持します。

詳細については、を参照してください ["システム管理"](#) を参照してください。

4. 変更したキュー深度パラメータの値が更新されていることを確認します。

```
root@localhost ~]#cat /sys/class/scsi_host/host5/lpfc_lun_queue_depth
30
```



キュー深度の現在の値が表示されます。

## QLogic HBA の Linux ホスト

Linux ホストでは QLogic ドライバのデバイスキュー深度を更新できます。更新をリブート後も維持するには、新しい RAM ディスクイメージを作成してホストをリブートする必要があります。QLogic HBA のキュー深度を変更するには、QLogic HBA の管理 GUI またはコマンドラインインターフェイス（CLI）を使用します。

このタスクでは、QLogic HBA の CLI を使用して QLogic HBA のキュー深度を変更する方法を示します

### 手順

1. 変更するデバイスキュー深度パラメータを確認します。

```
modinfo qla2xxx | grep ql2xmaxqdepth
```

変更できるのはのみです ql2xmaxqdepth キュー深度パラメータ。各LUNに設定できる最大キュー深度を指定します。RHEL 7.5 以降のデフォルト値は 64 です。RHEL 7.4 以前のデフォルト値は 32 です。

```
root@localhost ~]# modinfo qla2xxx|grep ql2xmaxqdepth
parm:          ql2xmaxqdepth:Maximum queue depth to set for each LUN.
Default is 64. (int)
```

2. デバイスのキュー深度の値を更新します。

- 永続的に変更する場合は、次の手順を実行します。
  - i. にキュー深度パラメータを追加して、キュー深度を更新します /etc/modprobe.conf ファイル（Red Hat Enterprise Linux 5.xシステム用）を参照してください  
/etc/modprobe.d/scsi.conf Red Hat Enterprise Linux 6.xまたは7.xシステム、またはSUSE Linux Enterprise Server 11.xまたは12.xシステムのファイル： options qla2xxx  
ql2xmaxqdepth=new\_queue\_depth
  - ii. 新しい RAM ディスクイメージを作成し、ホストをリブートして、リブート後も更新内容を維持します。

詳細については、を参照してください "[システム管理](#)" を参照してください。

- 現在のセッションだけでパラメータを変更する場合は、次のコマンドを実行します。

```
echo new_queue_depth > /sys/module/qla2xxx/parameters/ql2xmaxqdepth
```

次の例では、キュー深度を 128 に設定します。

```
echo 128 > /sys/module/qla2xxx/parameters/ql2xmaxqdepth
```

3. キュー深度の値が更新されたことを確認します。

```
cat /sys/module/qla2xxx/parameters/ql2xmaxqdepth
```

キュー深度の現在の値が表示されます。

4. ファームウェアパラメータを更新してQLogic HBAのキュー深度を変更します Execution Throttle  
QLogic HBA BIOSからアクセスします。

- a. QLogic HBA の管理 CLI にログインします。

```
/opt/QLogic_Corporation/QConvergeConsoleCLI/qauccli
```

- b. メインメニューからを選択します Adapter Configuration オプション

```
[root@localhost ~]#  
/opt/QLogic_Corporation/QConvergeConsoleCLI/qauccli  
Using config file:  
/opt/QLogic_Corporation/QConvergeConsoleCLI/qauccli.cfg  
Installation directory: /opt/QLogic_Corporation/QConvergeConsoleCLI  
Working dir: /root
```

```
QConvergeConsole
```

```
CLI - Version 2.2.0 (Build 15)
```

```
Main Menu
```

```
1: Adapter Information  
**2: Adapter Configuration**  
3: Adapter Updates  
4: Adapter Diagnostics  
5: Monitoring  
6: FabricCache CLI  
7: Refresh  
8: Help  
9: Exit
```

```
Please Enter Selection: 2
```

- c. アダプタ設定パラメータのリストからを選択します HBA Parameters オプション

```

1:  Adapter Alias
2:  Adapter Port Alias
**3:  HBA Parameters**
4:  Persistent Names (udev)
5:  Boot Devices Configuration
6:  Virtual Ports (NPIV)
7:  Target Link Speed (iidDMA)
8:  Export (Save) Configuration
9:  Generate Reports
10:  Personality
11:  FEC
(p or 0: Previous Menu; m or 98: Main Menu; ex or 99: Quit)
Please Enter Selection: 3

```

d. HBA ポートのリストから、必要な HBA ポートを選択します。

```

Fibre Channel Adapter Configuration

HBA Model QLE2562 SN: BFD1524C78510
1: Port 1: WWPN: 21-00-00-24-FF-8D-98-E0 Online
2: Port 2: WWPN: 21-00-00-24-FF-8D-98-E1 Online
HBA Model QLE2672 SN: RFE1241G81915
3: Port 1: WWPN: 21-00-00-0E-1E-09-B7-62 Online
4: Port 2: WWPN: 21-00-00-0E-1E-09-B7-63 Online

(p or 0: Previous Menu; m or 98: Main Menu; ex or 99: Quit)
Please Enter Selection: 1

```

HBA ポートの詳細が表示されます。

e. [HBA Parameters]メニューからを選択します Display HBA Parameters オプションを選択すると、の現在の値が表示されます Execution Throttle オプション

のデフォルト値 Execution Throttle オプションは65535です。

```

HBA Parameters Menu

=====
HBA          : 2 Port: 1
SN           : BFD1524C78510
HBA Model    : QLE2562
HBA Desc.    : QLE2562 PCI Express to 8Gb FC Dual Channel
FW Version   : 8.01.02

```

```
WWPN          : 21-00-00-24-FF-8D-98-E0
WWNN          : 20-00-00-24-FF-8D-98-E0
Link          : Online
=====
```

- 1: Display HBA Parameters
- 2: Configure HBA Parameters
- 3: Restore Defaults

(p or 0: Previous Menu; m or 98: Main Menu; x or 99: Quit)  
Please Enter Selection: 1

```
-----
HBA Instance 2: QLE2562 Port 1 WWPN 21-00-00-24-FF-8D-98-E0 PortID 03-
07-00
Link: Online
-----
```

```
-----
Connection Options          : 2 - Loop Preferred, Otherwise Point-to-
Point
Data Rate                   : Auto
Frame Size                   : 2048
Hard Loop ID                 : 0
Loop Reset Delay (seconds)  : 5
Enable Host HBA BIOS        : Enabled
Enable Hard Loop ID         : Disabled
Enable FC Tape Support      : Enabled
Operation Mode               : 0 - Interrupt for every I/O completion
Interrupt Delay Timer (100us) : 0
**Execution Throttle        : 65535**
Login Retry Count           : 8
Port Down Retry Count       : 30
Enable LIP Full Login       : Enabled
Link Down Timeout (seconds) : 30
Enable Target Reset         : Enabled
LUNs Per Target             : 128
Out Of Order Frame Assembly : Disabled
Enable LR Ext. Credits      : Disabled
Enable Fabric Assigned WWN  : N/A
```

Press <Enter> to continue:

- a. Enter \* を押して続行します。
- b. [HBA Parameters]メニューからを選択します Configure HBA Parameters HBAパラメータを変更するオプション。

- c. [Configure Parameters]メニューからを選択します Execute Throttle オプションを選択し、このパラメータの値を更新します。

#### Configure Parameters Menu

```
=====
HBA          : 2 Port: 1
SN           : BFD1524C78510
HBA Model    : QLE2562
HBA Desc.    : QLE2562 PCI Express to 8Gb FC Dual Channel
FW Version   : 8.01.02
WWPN         : 21-00-00-24-FF-8D-98-E0
WWNN         : 20-00-00-24-FF-8D-98-E0
Link         : Online
=====

1: Connection Options
2: Data Rate
3: Frame Size
4: Enable HBA Hard Loop ID
5: Hard Loop ID
6: Loop Reset Delay (seconds)
7: Enable BIOS
8: Enable Fibre Channel Tape Support
9: Operation Mode
10: Interrupt Delay Timer (100 microseconds)
11: Execution Throttle
12: Login Retry Count
13: Port Down Retry Count
14: Enable LIP Full Login
15: Link Down Timeout (seconds)
16: Enable Target Reset
17: LUNs per Target
18: Enable Receive Out Of Order Frame
19: Enable LR Ext. Credits
20: Commit Changes
21: Abort Changes

(p or 0: Previous Menu; m or 98: Main Menu; x or 99: Quit)
Please Enter Selection: 11
Enter Execution Throttle [1-65535] [65535]: 65500
```

- d. Enter \* を押して続行します。
- e. [Configure Parameters]メニューからを選択します Commit Changes 変更を保存するオプション。

f. メニューを終了します。

# S3 オブジェクトストレージの管理

## ONTAP 9でのS3サポートの詳細

### S3構成の概要

ONTAP 9.8 以降では、ONTAP クラスタ内で ONTAP Simple Storage Service (S3) オブジェクトストレージサーバを有効にすることができます。

ONTAP では、S3オブジェクトストレージを提供するオンプレミスのユースケースを2つサポートしています。

- FabricPool 階層をローカルクラスタ（ローカルバケットへの階層）またはリモートクラスタ（クラウド階層）のバケットに配置します。
- S3 クライアントアプリケーションからローカルクラスタまたはリモートクラスタのバケットへのアクセス。

ONTAP 9.14.1以降では、MetroCluster IP構成およびFC構成のミラーされたアグリゲートまたはミラーされていないアグリゲートのSVMでS3オブジェクトストレージサーバを有効にすることができます。

ONTAP 9.12.1以降では、MetroCluster IP構成のミラーされていないアグリゲート内のSVMでS3オブジェクトストレージサーバを有効にできます。MetroCluster IP構成でのミラーされていないアグリゲートの制限事項の詳細については、を参照してください "[ミラーされていないアグリゲートに関する考慮事項](#)"。

S3 オブジェクトストレージを設定する場合は、次の手順を実行する必要があります。

- ONTAP を実行している既存のクラスタから S3 オブジェクトストレージを提供する。

ONTAP S3 は、ハードウェアや管理の追加なしで既存のクラスタの S3 機能を利用する場合に適しています。ただし、NetApp StorageGRIDソフトウェアは、引き続きNetAppの主力製品であるオブジェクトストレージ向け解決策です。詳細については、を参照してください "[StorageGRID のドキュメント](#)"。

- SVM 管理者権限ではなくクラスタ管理者権限を持っている。

### System ManagerおよびONTAP CLIを使用したS3の設定

ONTAP S3は、System ManagerおよびONTAP CLIを使用して設定および管理できます。System Managerを使用してS3を有効にしてバケットを作成する際、ONTAP では、シンプルな設定を実現するためのデフォルトのベストプラクティスが選択されます。設定パラメータを指定する必要がある場合は、ONTAP CLIを使用できます。CLIからS3サーバとバケットを設定した場合は、必要に応じてSystem Managerで管理することもできます。逆も同様です。

System Manager を使用して S3 バケットを作成すると、ONTAP によって、システムで最も使用可能なパフォーマンスサービスレベルがデフォルトで設定されます。たとえば、AFF システムでは、デフォルト設定は \* Extreme \* になります。パフォーマンスサービスレベルは、事前定義されたアダプティブ QoS ポリシーグループです。カスタムの QoS ポリシーグループを指定する場合は、デフォルトのサービスレベルのいずれかを指定する代わりに、ポリシーグループを指定しなくてもかまいません。

事前定義されたアダプティブ QoS ポリシーグループは次のとおりです。

- \* Extreme \* : 最高レベルのレイテンシと最高レベルのパフォーマンスを求められるアプリケーションに使用されます。
- \* パフォーマンス \* : 適度なパフォーマンスとレイテンシが求められるアプリケーションに使用します。
- \* Value \* : スループットと容量がレイテンシよりも重視されるアプリケーションに使用します。
- \* カスタム \* : カスタムの QoS ポリシーを指定するか、QoS ポリシーなしで指定します。

[階層化に使用する \*] を選択した場合、パフォーマンスサービスレベルは選択されず、階層化データに最適なパフォーマンスを備えた低コストのメディアを選択しようとしています。

次も参照してください。 ["アダプティブ QoS ポリシーグループを使用する"](#)。

ONTAP は、選択したサービスレベルを満たす最も適切なディスクを含むローカル階層でこのバケットをプロビジョニングしようとしています。ただし、バケットに含めるディスクを指定する必要がある場合は、CLI でローカル階層（アグリゲート）を指定して S3 オブジェクトストレージを設定することを検討してください。CLI から S3 サーバを設定した場合も、必要に応じて System Manager で管理できます。

バケットに使用するアグリゲートを指定できるようにするには、CLI を使用する必要があります。

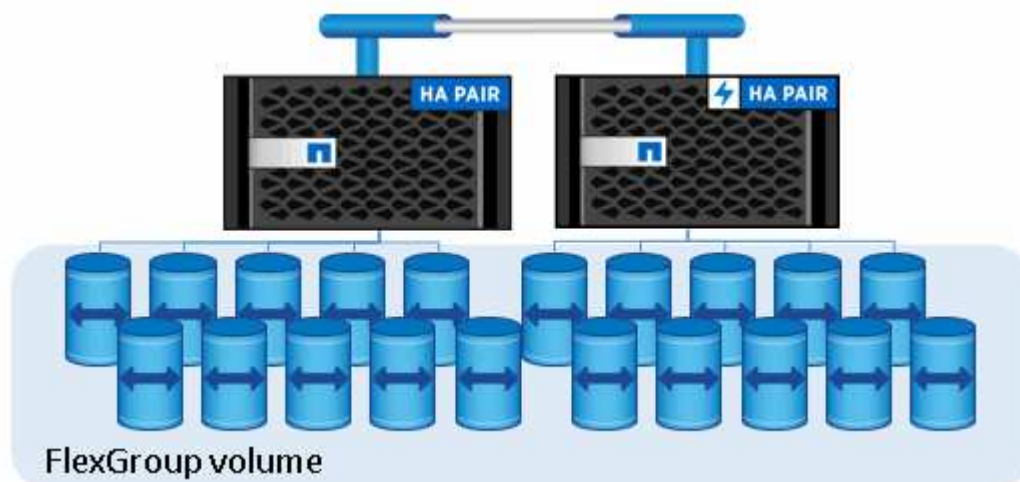
### Cloud Volumes ONTAP での S3 バケットの設定

Cloud Volumes ONTAP からバケットを提供する場合は、基盤となるアグリゲートを手動で選択して、いずれかのノードだけを使用するようにすることを強く推奨します。両方のノードのアグリゲートを使用すると、ノードが地理的に分離された可用性ゾーンに配置されるため、レイテンシの問題の影響を受けやすくなるため、パフォーマンスに影響を及ぼす可能性があります。したがって、Cloud Volumes ONTAP 環境では、を実行する必要があります [CLIからS3バケットを設定する](#)。

そうしないと、Cloud Volumes ONTAP 上の S3 サーバが、Cloud Volumes ONTAP 内とオンプレミス環境で同じように設定および管理されます。

### アーキテクチャ

ONTAP では、バケットの基盤となるアーキテクチャは FlexGroup ボリュームです。複数のコンスティチュエントメンバーボリュームで構成される単一のネームスペースで、単一のボリュームとして管理されます。



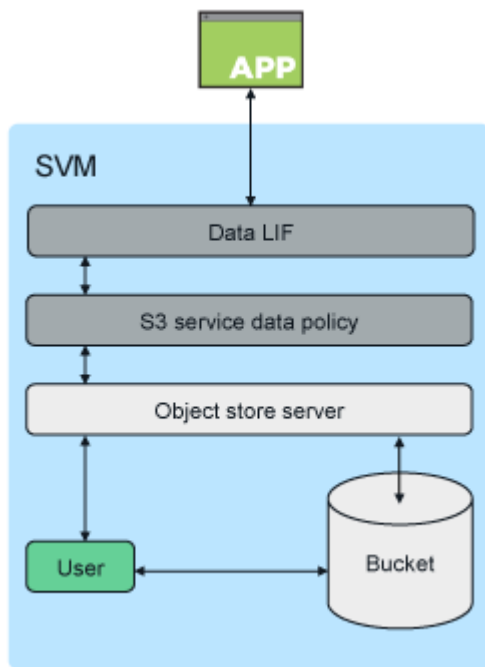


バケットの最大値は基盤となるハードウェアの物理的な最大値によってのみ制限され、アーキテクチャの最大値が高くなる可能性があります。バケットでは、FlexGroup エラスティックサイジングを利用して、スペースが不足した FlexGroup ボリュームのコンスチチュエントを自動的に拡張できます。FlexGroup ボリュームあたりの最大バケット数は 1000、FlexGroup ボリュームの容量の 1/3（バケット内のデータ増加に対応）に制限されています。



S3 バケットを含む FlexGroup ボリュームへの NAS プロトコルまたは SAN プロトコルアクセスは許可されません。

バケットへのアクセスは、許可されたユーザとクライアントアプリケーションから提供されます。



## ユースケース

ONTAP S3 サービスへのクライアントアクセスの主なユースケースは 3 つあります。

- FabricPool S3 をリモートの ONTAP 大容量（クラウド）階層として使用する ONTAP システムでは  
大容量階層を含む S3 サーバとバケット（\_cold\_data 用）は、パフォーマンス階層（hot\_data 用）とは別のクラスタにあります。
- FabricPool S3 をローカル ONTAP 階層として使用する ONTAP システムでは  
大容量階層を含む S3 サーバとバケットは、パフォーマンス階層と同じクラスタにありますが、別の HA ペアにあります。
- 外部の S3 クライアントアプリケーション用  
ONTAP S3 は、ネットアップ以外のシステムで実行される S3 クライアントアプリケーションに対応します。

ONTAP S3 バケットへのアクセスには、HTTPS を使用することを推奨します。HTTPS を有効にすると、SSL/TLS との適切な統合のためにセキュリティ証明書が必要になります。これにより、クライアントユー

「アクセスキーとシークレットキー」は、ONTAP S3 でユーザを認証するとともに、ONTAP S3 内での処理に対するユーザのアクセス権限を許可するために必要になります。また、クライアントアプリケーションがサーバを認証してクライアントとサーバの間にセキュアな接続を確立できるように、ルート CA 証明書（ONTAP S3 サーバの署名済み証明書）にもアクセスする必要があります。

ユーザは S3 対応 SVM 内に作成され、アクセス権限はバケットレベルまたは SVM レベルで制御できます。つまり、SVM 内の 1 つ以上のバケットへのアクセスを許可できます。

ONTAP S3 サーバでは、HTTPS がデフォルトで有効になっています。HTTPS を無効にして、クライアントアクセスに対して HTTP を有効にすることができます。その場合、CA 証明書を使用した認証は必要ありません。ただし、HTTP が有効で HTTPS が無効な場合、ONTAP S3 サーバとのすべての通信がクリアテキストでネットワーク経由で送信されます。

追加情報の場合は、を参照してください ["テクニカルレポート：『 S3 in ONTAP Best Practices 』"](#)

関連情報

["FlexGroup ボリューム管理"](#)

## 計画

### S3 オブジェクトストレージでの ONTAP バージョンのサポート

ONTAP 9.8以降、オンプレミス環境でS3オブジェクトストレージをサポート。Cloud Volumes ONTAP では、ONTAP 9.9.1以降のクラウド環境でS3オブジェクトストレージがサポートされます。

#### Cloud Volumes ONTAP によるS3のサポート

ONTAP S3はオンプレミス環境と同じようにCloud Volumes ONTAP で設定、機能します。ただし、次の点が異なります。

- 基盤となるアグリゲートは1つのノードだけで構成する必要があります。の詳細を確認してください ["CVO 環境でのバケットの作成"](#)。

クラウドプロバイダ	ONTAPバージョン
Azure	ONTAP 9.9.1以降
AWS	ONTAP 9.11.0以降
Google Cloud	ONTAP 9.12.1以降

### ONTAP 9.7のS3パブリックプレビュー

ONTAP 9.7 では、S3 オブジェクトストレージがパブリックプレビューとして導入されました。このバージョンは本番環境用ではなく、ONTAP 9.8 以降では更新されません。本番環境で S3 オブジェクトストレージをサポートするのは、ONTAP 9.8 以降のリリースだけです。

9.7 パブリックプレビューで作成した S3 バケットは、ONTAP 9.8 以降で使用できますが、機能拡張は利用できません。9.7 パブリックプレビューで作成したバケットがある場合は、それらのバケットの内容を 9.8 バケットに移行して、機能のサポート、セキュリティ、パフォーマンスの強化を行う必要があります。

## ONTAP S3 でサポートされている処理

ONTAP S3アクションは、以下に示す場合を除き、標準のS3 REST APIでサポートされています。詳細については、を参照してください ["Amazon S3 APIリファレンス"を参照してください](#)。

### バケットの処理

AWS S3 APIを使用するONTAPでサポートされる処理は次のとおりです。

バケットの処理	<b>ONTAP</b> のサポートはから始まります
CreateBucketを選択します	ONTAP 9.11.1
DeleteBucketの場合	ONTAP 9.11.1
DeleteBucketPolicyのようになります	ONTAP 9.12.1
GetBucketAcl	ONTAP 9.8
GetBucketLifecycleConfiguration	ONTAP 9.13.1以降 *有効期限アクションのみがサポートされています。
GetBucketLocation	ONTAP 9.10.1
GetBucketPolicyのようになります	ONTAP 9.12.1
ヘッドバケット	ONTAP 9.8
ListBuckets	ONTAP 9.8
ListBucketVersioning	ONTAP 9.11.1
ListObjectVersions	ONTAP 9.11.1
PutBucket	• ONTAP 9.11.1 • ONTAP 9.8 - ONTAP REST APIのみでサポート
PutBucketLifecycleConfigurationの略	ONTAP 9.13.1以降 *有効期限アクションのみがサポートされています。
PutBucketPolicyのように指定します	ONTAP 9.12.1

### オブジェクトの処理

ONTAP 9.9.1以降では、ONTAP S3でオブジェクトメタデータとタグ付けがサポートされます。

- PutObjectとCreateMultipartUploadには、 x-amz-meta-<key>.

例： x-amz-meta-project: ontap\_s3。

- GetObject。およびHeadObjectはユーザ定義のメタデータを返します。
- メタデータとは異なり、タグは次の機能を使用してオブジェクトから独立して読み取ることができます。
  - PutObjectTagging の 2 つのグループが
  - GetObjectTagging の 2 つの機能を

◦ DeleteObjectTagging の場合

ONTAP 9.11.1以降のONTAP S3では、オブジェクトのバージョン管理と以下のONTAP APIによる関連アクションがサポートされます。

- GetBucketVersioningの各ノードの設定
- ListBucketVersionsの1つ
- PutBucketVersioningの各ノードの設定

オブジェクトの処理	<b>ONTAP</b> のサポートはから始まります
AbortMultipartUpload の略	ONTAP 9.8
CompleteMultipartUpload	ONTAP 9.8
CopyObject	ONTAP 9.12.1
CreateMultipartUpload を実行します	ONTAP 9.8
deleteObject	ONTAP 9.8
オブジェクトを削除します	ONTAP 9.11.1
DeleteObjectTagging の場合	ONTAP 9.9.1
GetBucketVersioningの各ノードの設定	ONTAP 9.11.1
GetObject	ONTAP 9.8
GetObjectAcl	ONTAP 9.8
GetObjectRetentionの略	ONTAP 9.14.1
GetObjectTagging の 2 つの機能を	ONTAP 9.9.1
HeadObject （ヘッドオブジェクト）	ONTAP 9.8
ListMultipartUpload の略	ONTAP 9.8
ListObjects	ONTAP 9.8
ListObjectsV2	ONTAP 9.8
ListBucketVersionsの1つ	ONTAP 9.11.1
ListParts	ONTAP 9.8
PutBucketVersioningの各ノードの設定	ONTAP 9.11.1
PutObject	ONTAP 9.8
PutObjectLockConfigurationの略	ONTAP 9.14.1
PutObjectRetentionの略	ONTAP 9.14.1
PutObjectTagging の 2 つのグループが	ONTAP 9.9.1
UploadPart のアップロード	ONTAP 9.8
UploadPartCopyをクリックします	ONTAP 9.12.1

## グループポリシー

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

- ポリシーの作成
- AttachGroup ポリシー

## ユーザ管理

これらの処理は S3 に固有のものではなく、一般に IAM プロセスに関連付けられています。

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

## ONTAP S3 の相互運用性

ONTAP S3 サーバは、この表に記載されている機能を除き、他の ONTAP 機能と正常に通信します。

フィーチャー領域（ <b>Feature area</b> ）	サポートされます	サポート対象外
Cloud Volumes ONTAP	<ul style="list-style-type: none"><li>• ONTAP 9.9.1 以降のリリースの Azure クライアント</li><li>• ONTAP 9.11.0以降のリリースのAWSクライアント</li><li>• ONTAP 9.12.1以降のリリースのGoogle Cloudクライアント</li></ul>	<ul style="list-style-type: none"><li>• ONTAP 9.8 以前のリリースの任意のクライアントの Cloud Volumes ONTAP</li></ul>
データ保護	<ul style="list-style-type: none"><li>• Cloud Sync</li><li>• "オブジェクトのバージョン管理"（ONTAP 9.11.1以降）</li><li>• "S3 SnapMirrorの略"（ONTAP 9.10.1以降）</li><li>• MetroCluster IP設定（ONTAP 9.12.1以降）</li><li>• SnapLock（ONTAP 9.14.1以降）</li><li>• WORM（ONTAP 9.14.1以降）</li></ul>	<ul style="list-style-type: none"><li>• イレイジャーコーディング</li><li>• 情報ライフサイクル管理</li><li>• NDMP</li><li>• SMTape の場合</li><li>• SnapMirror クラウド</li><li>• SVM ディザスタリカバリ</li><li>• SyncMirror</li><li>• ユーザが作成した Snapshot コピー</li></ul>

フィーチャー領域（ <b>Feature area</b> ）	サポートされます	サポート対象外
暗号化	<ul style="list-style-type: none"> <li>• NetApp Aggregate Encryption （ NAE ）</li> <li>• NetApp Volume Encryption （ NVE ）</li> <li>• NetApp Storage Encryption （ NSE ）</li> <li>• TLS/SSL</li> </ul>	<ul style="list-style-type: none"> <li>• SLAG</li> </ul>
ストレージ効率	<ul style="list-style-type: none"> <li>• 重複排除</li> <li>• 圧縮</li> <li>• コンパクション</li> </ul>	<ul style="list-style-type: none"> <li>• アグリゲートレベルの効率化</li> <li>• ONTAP S3 バケットを含む FlexGroup ボリュームのボリュームクローン</li> </ul>
ストレージ仮想化	-	NetApp FlexArray 仮想化
サービス品質（ QoS ）	<ul style="list-style-type: none"> <li>• QoS の最大数（上限）</li> <li>• QoS の最小値（下限）</li> </ul>	-
その他の機能	<ul style="list-style-type: none"> <li>• "S3 イベントを監査します"（ONTAP 9.10.1以降）</li> </ul>	<ul style="list-style-type: none"> <li>• FlexCache ボリューム</li> <li>• FPolicy の</li> <li>• qtree</li> <li>• クォータ</li> </ul>

## ONTAP S3の検証済みサードパーティソリューション

NetAppは、ONTAP S3で使用する以下のサードパーティソリューションを検証しました。

お探しの解決策が表示されない場合は、NetAppのアカウント担当者にお問い合わせください。

### ONTAP S3で検証済みの他社製ソリューション

NetAppは、それぞれのパートナーと協力してこれらのソリューションをテストしました。

- Amazon SageMaker
- Apache Hadoop S3Aクライアント
- Apache Kafka です
- Commvault（V11）
- 矛盾したカフカ

- レッドハットキー
- ルブリク
- 雪の結晶
- トリノ
- Veeam (V12)

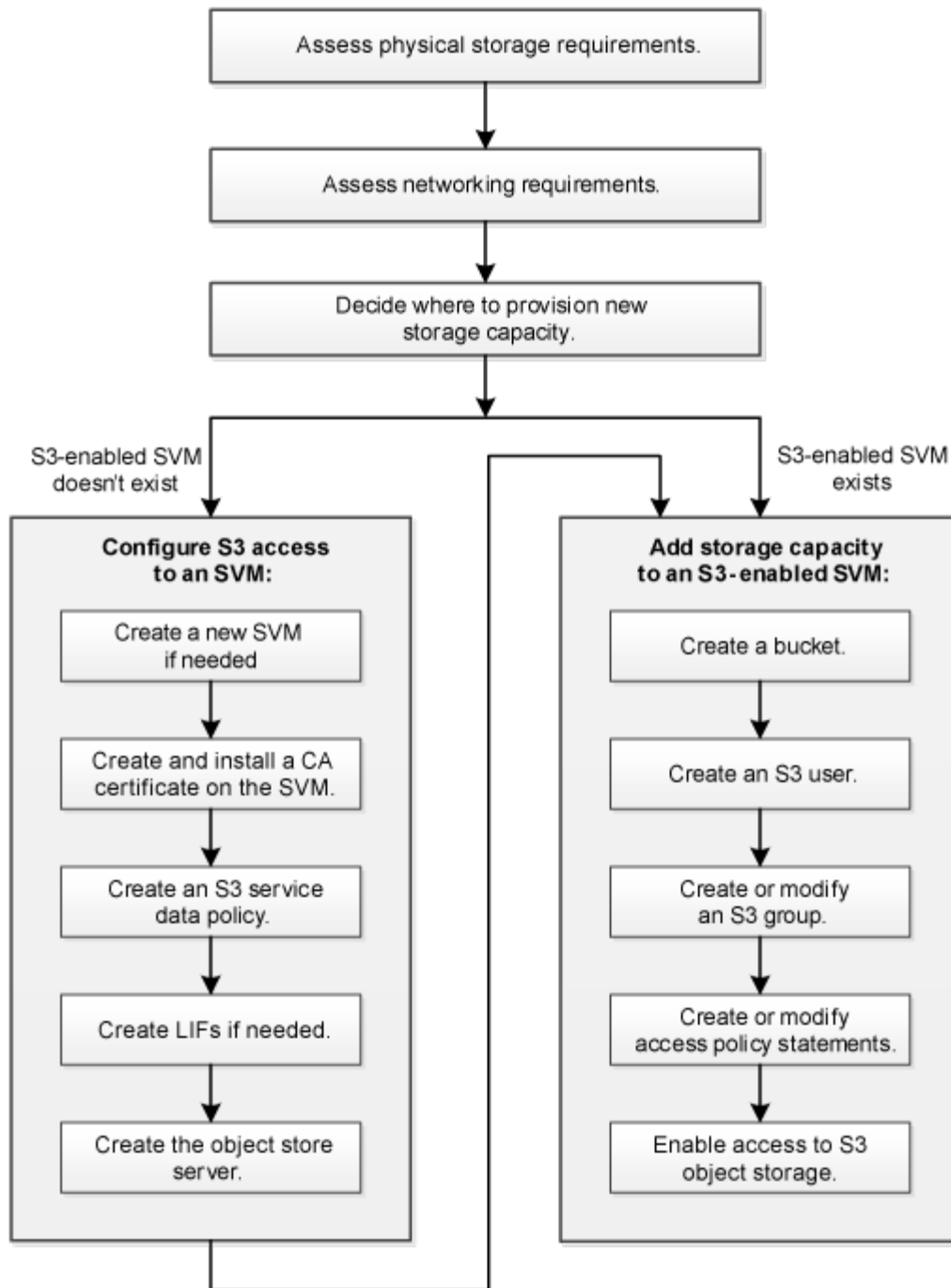
## 設定

### S3 の設定プロセスについて

#### S3 の設定ワークフロー

S3 を設定するには、物理ストレージとネットワークの要件を評価して、目的に応じたワークフローを選択します。新規または既存の SVM への S3 アクセスを設定するか、すでに S3 アクセスの設定が完了している既存の SVM にバケットとユーザを追加するかによってワークフローが異なります。

System Managerを使用して新しいStorage VMへのS3アクセスを設定すると、証明書とネットワークの情報を入力するように求められ、Storage VMとS3オブジェクトストレージサーバは一度に作成されます。



#### 物理ストレージ要件を評価

クライアントの S3 ストレージをプロビジョニングする前に、既存のアグリゲート内に新しいオブジェクトストア用の十分なスペースがあることを確認する必要があります。十分なスペースがない場合は、既存のアグリゲートにディスクを追加するか、必要なタイプと場所で新しいアグリゲートを作成することができます。

#### このタスクについて

S3 対応 SVM で S3 バケットを作成すると、バケットをサポートする FlexGroup ボリュームが自動的に作成されます。基盤となるアグリゲートや FlexGroup コンポーネントを ONTAP Select で自動的に（デフォルト）選択するか、基盤となるアグリゲートや FlexGroup コンポーネントを手動で選択することができます。



アグリゲートと FlexGroup コンポーネントを指定する場合は、たとえば基盤となるディスクに固有のパフォーマンス要件がある場合などに、アグリゲートの構成が FlexGroup ボリュームのプロビジョニングに関するベストプラクティスのガイドラインに従っていることを確認する必要があります。詳細はこちら。

- ["FlexGroup ボリューム管理"](#)
- ["ネットアップテクニカルレポート 4571-A : 『 NetApp ONTAP FlexGroup Volume Top Best Practices 』"](#)

バケットを Cloud Volumes ONTAP から提供している場合は、基盤となるアグリゲートを手動で選択して、使用するノードが1つだけになるようにすることを強く推奨します。両方のノードのアグリゲートを使用すると、ノードが地理的に分離された可用性ゾーンに配置されるため、レイテンシの問題の影響を受けやすくなるため、パフォーマンスに影響を及ぼす可能性があります。詳細はこちら ["Cloud Volumes ONTAP 用バケットの作成"](#)。

ONTAP S3 サーバを使用して、ローカルの FabricPool 大容量階層、つまり高パフォーマンス階層と同じクラスタに作成できます。これは、SSD ディスクが1つの HA ペアに接続されている状態で、別の HA ペアの HDD ディスクに階層化 `_cold_data` を設定する場合などに便利です。このユースケースでは、S3 サーバとローカルの大容量階層を含むバケットを、パフォーマンス階層とは別の HA ペアに配置する必要があります。ローカル階層化は、1 ノードクラスタと2 ノードクラスタではサポートされていません。

## 手順

1. 既存のアグリゲート内の使用可能なスペースを表示します。

```
storage aggregate show
```

十分なスペースがあるアグリゲートや必要なノードの場所がある場合は、S3構成用のアグリゲートの名前を記録します。

```
cluster-1::> storage aggregate show
Aggregate      Size Available Used% State   #Vols  Nodes  RAID Status
-----
aggr_0         239.0GB    11.13GB   95% online      1 node1  raid_dp, normal
aggr_1         239.0GB    11.13GB   95% online      1 node1  raid_dp, normal
aggr_2         239.0GB    11.13GB   95% online      1 node2  raid_dp, normal
aggr_3         239.0GB    11.13GB   95% online      1 node2  raid_dp, normal
aggr_4         239.0GB    238.9GB   95% online      5 node3  raid_dp, normal
aggr_5         239.0GB    239.0GB   95% online      4 node4  raid_dp, normal
6 entries were displayed.
```

2. 十分なスペースまたは必要なノードの場所を備えたアグリゲートがない場合は、を使用して既存のアグリゲートにディスクを追加します `storage aggregate add-disks` コマンドを実行するか、を使用して新しいアグリゲートを作成します `storage aggregate create` コマンドを実行します

## ネットワーク要件を評価

クライアントに S3 ストレージを提供する前に、S3 プロビジョニングの要件を満たすようにネットワークが正しく設定されていることを確認する必要があります。

作業を開始する前に

次のクラスタネットワークオブジェクトを設定する必要があります。

- 物理ポートと論理ポート
- ブロードキャストドメイン
- サブネット（必要な場合）
- IPspace（必要に応じて、デフォルトの IPspace に追加）
- フェイルオーバーグループ（必要に応じて、各ブロードキャストドメインのデフォルトのフェイルオーバーグループに追加）
- 外部ファイアウォール

このタスクについて

リモートの FabricPool 容量（クラウド）階層およびリモートの S3 クライアントの場合は、データ SVM を使用してデータ LIF を設定する必要があります。FabricPool クラウド階層の場合は、クラスタ間 LIF も設定する必要があります。クラスタピアリングは必要ありません。

ローカル FabricPool の大容量階層には、システム SVM（「Cluster」）を使用する必要がありますが、LIF を設定する方法は 2 つあります。

- クラスタ LIF を使用できます。

このオプションでは、これ以上 LIF を設定する必要はありませんが、クラスタ LIF のトラフィックが増加します。また、他のクラスタからローカル階層にアクセスできなくなります。

- データ LIF とクラスタ間 LIF を使用できます。

このオプションを使用するには追加の設定が必要です。たとえば、S3 プロトコルの LIF を有効にする必要がありますが、ローカル階層には他のクラスタのリモート FabricPool クラウド階層としてもアクセスできます。

## 手順

1. 使用可能な物理ポートと仮想ポートを表示します。

```
network port show
```

- 可能な場合は、データネットワークの速度が最高であるポートを使用する必要があります。
- 最大限のパフォーマンスを得るためには、データネットワーク内のすべてのコンポーネントの MTU 設定が同じである必要があります。

2. サブネット名を使用して LIF の IP アドレスとネットワークマスク値を割り当てる場合は、そのサブネットが存在し、十分な数のアドレスが使用可能であることを確認します。

```
network subnet show
```

サブネットには、同じレイヤ 3 サブネットに属する IP アドレスのプールが含まれています。サブネットは、を使用して作成されます `network subnet create` コマンドを実行します

### 3. 使用可能な IPspace を表示します。

```
network ipspace show
```

デフォルトの IPspace またはカスタムの IPspace を使用できます。

### 4. IPv6 アドレスを使用する場合は、IPv6 がクラスタで有効になっていることを確認します。

```
network options ipv6 show
```

必要に応じて、を使用してIPv6を有効にできます `network options ipv6 modify` コマンドを実行します

新しい **S3** ストレージ容量のプロビジョニング先を決定します

新しい S3 バケットを作成する前に、そのバケットを新規と既存のどちらの SVM に配置するかを決めておく必要があります。これにより、ワークフローが決まります。

#### 選択肢

- 新しい SVM または S3 に対して有効になっていない SVM にバケットをプロビジョニングする場合は、次のトピックに記載された手順を実行します。

"S3 用の SVM を作成します"

"S3のバケットを作成します"

S3 は NFS と SMB を備えた SVM 内にも共存できますが、次のいずれかに該当する場合は、新しい SVM を作成することもできます。

- クラスタで S3 を初めて有効にする場合。
- クラスタ内の既存の SVM で S3 サポートを有効にするのが望ましくない場合。
- クラスタ内に S3 対応 SVM が 1 つ以上あり、パフォーマンス特性が異なる別の S3 サーバが必要な場合。  
SVM で S3 を有効にしたあとに、バケットのプロビジョニングに進みます。
- 既存の S3 対応 SVM に初期バケットまたは追加のバケットをプロビジョニングする場合は、次のトピックに記載された手順を実行します。

"S3のバケットを作成します"

## SVM への S3 アクセスを設定する

### S3 用の SVM を作成します

S3はSVM内で他のプロトコルと共存できますが、新しいSVMを作成してネームスペースとワークロードを分離することもできます。

このタスクについて

SVMからS3オブジェクトストレージのみを提供する場合は、S3サーバでDNS設定を行う必要はありません。ただし、他のプロトコルを使用する場合は、SVMにDNSを設定できます。

System Managerを使用して新しいStorage VMへのS3アクセスを設定すると、証明書とネットワークの情報を入力するように求められ、Storage VMとS3オブジェクトストレージサーバは一度に作成されます。

### System Manager の略

S3サーバ名を完全修飾ドメイン名 (FQDN) として入力できるようにして、クライアントがS3アクセスに使用できるようにしておく必要があります。S3サーバのFQDNの先頭をバケット名にすることはできません。


インターフェイスロールデータ用のIPアドレスを入力する準備をしておく必要があります。

外部 CA 署名証明書を使用している場合は、この手順中に証明書の入力を求められます。システムで生成された証明書を使用することもできます。

#### 1. Storage VM で S3 を有効にします。

- a. 新しいStorage VMを追加します。[\* Storage (ストレージ)]>[Storage VMs]をクリックし、[\* Add (追加)]をクリックします。

既存のStorage VMがない新しいシステムの場合は、\*ダッシュボード>プロトコルの設定\*をクリックします。

S3サーバを既存のStorage VMに追加する場合は、\* Storage > Storage VM\*をクリックし、Storage VMを選択して\* Settings \*をクリックし、をクリックします  \* S3 の下 \*。

- a. Enable S3 \* をクリックし、S3 Server Name を入力します。

- b. 証明書のタイプを選択します。

システムで生成された証明書と独自の証明書のどちらを選択した場合も、クライアントアクセスには証明書が必要です。

- c. ネットワークインターフェイスを入力してください。

#### 2. システムで生成された証明書を選択した場合は、新しい Storage VM の作成を確認すると証明書情報が表示されます。[ダウンロード]をクリックし、クライアントアクセス用に保存します。

- シークレットキーは今後表示されません。
- 証明書情報が再度必要な場合は、[\*ストレージ]、[Storage VMs]の順にクリックし、Storage VMを選択して、[\*設定]をクリックします。

### CLI の使用

#### 1. クラスタ上で S3 のライセンスが有効であることを確認します。

```
system license show -package s3
```

表示されない場合は、営業担当者にお問い合わせください。

#### 2. SVM を作成します。

```
vserver create -vserver <svm_name> -subtype default -rootvolume  
<root_volume_name> -aggregate <aggregate_name> -rootvolume-security  
-style unix -language C.UTF-8 -data-services <data-s3-server>  
-ipSPACE <ipSPACE_name>
```

- にUNIX設定を使用します -rootvolume-security-style オプション
- デフォルトのC.UTF-8を使用します -language オプション
- ipSPACE 設定はオプションです。

### 3. 新しく作成した SVM の設定とステータスを確認します。

```
vserver show -vserver <svm_name>
```

。 Vserver Operational State フィールドにはを表示する必要があります running 状態。が表示された場合 initializing 状態にすると、ルートボリュームの作成などの中間処理が失敗したため、SVMを削除して再作成する必要があります。

#### 例

次のコマンドは、データアクセス用の SVM を IPspace ipSPACEA 内に作成します。

```
cluster-1::> vserver create -vserver svm1.example.com -rootvolume  
root_svm1 -aggregate aggr1 -rootvolume-security-style unix -language  
C.UTF-8 -data-services _data-s3-server_ -ipSPACE ipSPACEA
```

```
[Job 2059] Job succeeded:  
Vserver creation completed
```

次のコマンドは、1GBのルートボリュームでSVMが作成され、自動的に起動されて追加されたことを示しています running 状態。ルートボリュームには、ルールを含まないデフォルトのエクスポートポリシーがあるため、ルートボリュームは作成時にエクスポートされません。デフォルトでは、vsadminユーザアカウントが作成され、に配置されます locked 状態。vsadmin ロールがデフォルトの vsadmin ユーザアカウントに割り当てられます。

```

cluster-1::> vserver show -vserver svm1.example.com
                                Vserver: svm1.example.com
                                Vserver Type: data
                                Vserver Subtype: default
                                Vserver UUID: b8375669-19b0-11e5-b9d1-
00a0983d9736

                                Root Volume: root_svm1
                                Aggregate: aggr1
                                NIS Domain: -
                                Root Volume Security Style: unix
                                LDAP Client: -
                                Default Volume Language Code: C.UTF-8
                                Snapshot Policy: default
                                Comment:
                                Quota Policy: default
                                List of Aggregates Assigned: -
                                Limit on Maximum Number of Volumes allowed: unlimited
                                Vserver Admin State: running
                                Vserver Operational State: running
                                Vserver Operational State Stopped Reason: -
                                Allowed Protocols: nfs, cifs
                                Disallowed Protocols: -
                                QoS Policy Group: -
                                Config Lock: false
                                IPspace Name: ipspaceA

```

**CA 証明書を作成して SVM にインストールします**

S3 クライアントから S3 対応 SVM への HTTPS トラフィックを有効にするには、認証局（CA）証明書が必要です。

このタスクについて

HTTP のみを使用するように S3 サーバを設定することは可能ですが、CA 証明書が不要なクライアントを設定することも可能です。ただし、ONTAP S3 サーバへの HTTPS トラフィックを CA 証明書を使用して保護することを推奨します。

IP トラフィックがクラスタ LIF のみを経由するローカル階層化の場合、CA 証明書は必要ありません。

この手順に記載されている手順では、ONTAP 自己署名証明書を作成してインストールします。サードパーティベンダーの CA 証明書もサポートされています。詳細については、管理者認証のドキュメントを参照してください。

["管理者認証と RBAC"](#)

を参照してください `security certificate` 追加の設定オプションのマニュアルページ

## 手順

### 1. 自己署名デジタル証明書を作成します。

```
security certificate create -vserver svm_name -type root-ca -common-name  
ca_cert_name
```

。 -type root-ca オプションは、認証局（CA）として機能して他の証明書に署名するための自己署名デジタル証明書を作成してインストールします。

。 -common-name オプションを指定すると、SVMの認証局（CA）名が作成され、証明書の完全な名前を生成するときに使用されます。

デフォルトの証明書サイズは 2048 ビットです。

## 例

```
cluster-1::> security certificate create -vserver svm1.example.com -type  
root-ca -common-name svm1_ca
```

```
The certificate's generated name for reference:  
svm1_ca_159D1587CE21E9D4_svm1_ca
```

生成された証明書の名前が表示されたら、この手順の以降の手順で名前を保存してください。

### 2. 証明書署名要求を生成します。

```
security certificate generate-csr -common-name s3_server_name  
[additional_options]
```

。 -common-name 署名要求のパラメータには、S3サーバ名（FQDN）を指定する必要があります。

必要に応じて、SVM の場所やその他の詳細情報を指定できます。

今後の参照用に、証明書要求と秘密鍵のコピーを保管するように求められます。

### 3. SVM\_CA を使用して CSR に署名し、S3 サーバの証明書を作成します。

```
security certificate sign -vserver svm_name -ca ca_cert_name -ca-serial  
ca_cert_serial_number [additional_options]
```

前の手順で使用したコマンドオプションを入力します。

- 。 -ca --ステップ1で入力したCAの共通名。
- 。 -ca-serial --ステップ1のCAシリアル番号。たとえば、CA 証明書の名前が svm1\_ca\_159D1587CE21E9D4\_svm1\_ca の場合、シリアル番号は 159D1587CE21E9D4 です。

デフォルトでは、署名済み証明書の有効期限は 365 日です。別の値を選択し、他の署名の詳細を指定できます。

プロンプトが表示されたら、手順 2 で保存した証明書要求文字列をコピーして入力します。



署名済み証明書が表示されます。あとで使えるように保存しておきます。

4. S3 対応 SVM に署名済み証明書をインストールします。

```
security certificate install -type server -vserver svm_name
```

プロンプトが表示されたら、証明書と秘密鍵を入力します。

証明書チェーンが必要な場合は、中間証明書を入力できます。

秘密鍵と CA 署名デジタル証明書が表示されたら、あとで参照できるように保存します。

5. 公開鍵証明書を取得します。

```
security certificate show -vserver svm_name -common-name ca_cert_name -type  
root-ca -instance
```

公開鍵証明書を保存しておき、以降のクライアント側の設定に使用します。

例

```
cluster-1::> security certificate show -vserver svm1.example.com -common  
-name svm1_ca -type root-ca -instance  
  
Name of Vserver: svm1.example.com  
FQDN or Custom Common Name: svm1_ca  
Serial Number of Certificate: 159D1587CE21E9D4  
Certificate Authority: svm1_ca  
Type of Certificate: root-ca  
(DEPRECATED)-Certificate Subtype: -  
Unique Certificate Name: svm1_ca_159D1587CE21E9D4_svm1_ca  
Size of Requested Certificate in Bits: 2048  
Certificate Start Date: Thu May 09 10:58:39 2020  
Certificate Expiration Date: Fri May 08 10:58:39 2021  
Public Key Certificate: -----BEGIN CERTIFICATE-----  
MIIDZ ...==  
-----END CERTIFICATE-----  
  
Country Name: US  
State or Province Name:  
Locality Name:  
Organization Name:  
Organization Unit:  
Contact Administrator's Email Address:  
Protocol: SSL  
Hashing Function: SHA256  
Self-Signed Certificate: true  
Is System Internal Certificate: false
```

## S3 サービスデータポリシーを作成する

S3 のデータサービスと管理サービスのサービスポリシーを作成できます。LIF 上の S3 データトラフィックを有効にするには、S3 サービスデータポリシーが必要です。

### このタスクについて

データ LIF とクラスタ間 LIF を使用する場合は、S3 サービスデータポリシーが必要です。ローカル階層化のユースケースにクラスタ LIF を使用している場合は必要ありません。

LIF にサービスポリシーを指定すると、そのポリシーを使用して LIF のデフォルトロール、フェイルオーバーポリシー、データプロトコルのリストが作成されます。

SVM と LIF には複数のプロトコルを設定できますが、オブジェクトデータを提供する際には S3 だけを使用することを推奨します。

### 手順

1. 権限の設定を advanced に変更します。

```
set -privilege advanced
```

2. サービスデータポリシーを作成します。

```
network interface service-policy create -vserver svm_name -policy policy_name  
-services data-core,data-s3-server
```

。data-core および data-s3-server ONTAP S3を有効にするために必要なサービスはサービスだけです。必要に応じて他のサービスも含めることができます。

データ LIF を作成します。

新しい SVM を作成した場合、S3 アクセス用に作成する専用の LIF はデータ LIF です。

### 作業を開始する前に

- 基盤となる物理または論理ネットワークポートが管理用に設定されている必要があります up ステータス。
- サブネット名を使用して LIF の IP アドレスとネットワークマスク値を割り当てる場合は、そのサブネットがすでに存在している必要があります。

サブネットには、同じレイヤ 3 サブネットに属する IP アドレスのプールが含まれています。これらはを使用して作成されます network subnet create コマンドを実行します

- LIF サービスポリシーがすでに存在している必要があります。

### このタスクについて

- 同じネットワークポート上に IPv4 と IPv6 の両方の LIF を作成できます。
- クラスタ内の LIF の数が多い場合は、を使用して、クラスタでサポートされる LIF の容量を確認できます network interface capacity show コマンドとを使用して、各ノードでサポートされる LIF の容量を確認します network interface capacity details show コマンド (advanced 権限レベル)。
- リモートの FabricPool 容量 (クラウド) 階層化を有効にする場合は、クラスタ間 LIF も設定する必要があります。

ります。

## 手順

### 1. LIF を作成します。

```
network interface create -vserver svm_name -lif lif_name -service-policy
service_policy_names -home-node node_name -home-port port_name {-address
IP_address -netmask IP_address | -subnet-name subnet_name} -firewall-policy
data -auto-revert {true|false}
```

- -home-node は、の実行時にLIFが戻るノードです network interface revert LIFに対してコマンドを実行します。

を使用して、LIFをホームノードおよびホームポートに自動的にリバートするかどうかを指定することもできます -auto-revert オプション

- -home-port は、の実行時にLIFが戻る物理ポートまたは論理ポートです network interface revert LIFに対してコマンドを実行します。
- でIPアドレスを指定できます -address および -netmask オプションを選択するか、を使用してサブネットからの割り当てを有効にします -subnet\_name オプション
- サブネットを使用して IP アドレスとネットワークマスクを指定した場合、サブネットにゲートウェイが定義されていると、そのサブネットを使用して LIF を作成するときにゲートウェイへのデフォルトルートが SVM に自動的に追加されます。
- サブネットを使用せずに手動で IP アドレスを割り当てると、クライアントまたはドメインコントローラが別の IP サブネットにある場合にゲートウェイへのデフォルトルートの設定が必要になることがあります。。 network route create のマニュアルページには、SVM内での静的ルートの作成に関する情報が記載されています。
- をクリックします -firewall-policy オプションで、同じデフォルトを使用します data をLIFのルールとして使用します。

必要に応じて、カスタムファイアウォールポリシーをあとから作成して追加できます。



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

- -auto-revert 起動時、管理データベースのステータスが変化したとき、ネットワーク接続が確立されたときなどの状況で、データLIFがホームノードに自動的にリバートされるかどうかを指定できます。デフォルト設定はです false`に設定することもできます `false 環境内のネットワーク管理ポリシーによって異なります。
- 。 -service-policy optionは、作成したデータサービスポリシーと管理サービスポリシー、およびその他の必要なポリシーを指定します。

### 2. でIPv6アドレスを割り当てる場合 -address オプション：

- a. を使用します network ndp prefix show ささまざまなインターフェイスで学習されたRAプレフィックスのリストを表示するコマンド。

- network ndp prefix show コマンドはadvanced権限レベルで使用できます。

b. の形式を使用します `prefix:id` IPv6アドレスを手動で作成します。

`prefix` は、さまざまなインターフェイスで学習されたプレフィックスです。

を導出するため `id` で、ランダムな64ビット16進数を選択します。

3. を使用して、LIFが正常に作成されたことを確認します `network interface show` コマンドを実行します
4. 設定した IP アドレスに到達できることを確認します。

対象	使用
IPv4 アドレス	<code>network ping</code>
IPv6アドレス	<code>network ping6</code>

#### 例

次のコマンドは、に割り当てられたS3データLIFを作成する方法を示しています `my-S3-policy` サービスポリシー：

```
network interface create -vserver svml.example.com -lif lif2 -home-node  
node2 -homeport e0d -service-policy my-S3-policy -subnet-name ipspace1
```

次のコマンドは、`cluster-1` 内のすべての LIF を表示します。`datlif1` および `datlif3` というデータ LIF には IPv4 アドレスを設定しています。一方、`datlif4` には IPv6 アドレスを設定しています。

```
cluster-1::> network interface show
```

Vserver	Logical Interface	Status Admin/Oper	Network Address/Mask	Current Node	Current Is Port
Home					
-----					
cluster-1	cluster_mgmt	up/up	192.0.2.3/24	node-1	e1a
true					
node-1	clus1	up/up	192.0.2.12/24	node-1	e0a
true					
	clus2	up/up	192.0.2.13/24	node-1	e0b
true					
	mgmt1	up/up	192.0.2.68/24	node-1	e1a
true					
node-2	clus1	up/up	192.0.2.14/24	node-2	e0a
true					
	clus2	up/up	192.0.2.15/24	node-2	e0b
true					
	mgmt1	up/up	192.0.2.69/24	node-2	e1a
true					
vs1.example.com	datalif1	up/down	192.0.2.145/30	node-1	e1c
true					
vs3.example.com	datalif3	up/up	192.0.2.146/30	node-2	e0c
true					
	datalif4	up/up	2001::2/64	node-2	e0c
true					

5 entries were displayed.

リモートの **FabricPool** 階層化用にクラスタ間 **LIF** を作成する

ONTAP S3 を使用してリモートの FabricPool 容量（クラウド）階層化を有効にする場合は、クラスタ間 LIF を設定する必要があります。データネットワークと共有するポートにクラスタ間 LIF を設定できます。これにより、クラスタ間ネットワークに必要なポート数を減らすことができます。

作業を開始する前に

- 基盤となる物理または論理ネットワークポートが管理用に設定されている必要があります up ステータス。
- LIF サービスポリシーがすでに存在している必要があります。

このタスクについて

ローカルのファブリックプールの階層化や外部の S3 アプリケーションへの提供にクラスタ間 LIF は必要ありません。

手順

1. クラスタ内のポートの一覧を表示します。

```
network port show
```

次の例は、のネットワークポートを示しています cluster01：

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

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

2. システム SVM にクラスタ間 LIF を作成します。

```
network interface create -vserver Cluster -lif LIF_name -service-policy  
default-intercluster -home-node node -home-port port -address port_IP -netmask  
netmask
```

次の例は、クラスタ間LIFを作成します cluster01\_icl01 および cluster01\_icl02：

```

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

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

```

### 3. クラスタ間 LIF が作成されたことを確認します。

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

```

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

```

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

### 4. クラスタ間 LIF が冗長構成になっていることを確認します。

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

次の例は、クラスタ間LIFを示しています cluster01\_icl01 および cluster01\_icl02 をクリックします e0c ポートはにフェイルオーバーします e0d ポート：

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

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

### S3 オブジェクトストアサーバを作成します

ONTAP オブジェクトストアサーバは、ONTAP NAS サーバおよび SAN サーバが提供するファイルストレージまたはブロックストレージではなく、データを S3 オブジェクトとして管理します。

作業を開始する前に

S3サーバ名を完全修飾ドメイン名 (FQDN) として入力できるようにして、クライアントがS3アクセスに使用できるようにしておく必要があります。バケット名の先頭にFQDNを使用することはできません。

自己署名 CA 証明書（前の手順で作成）または外部 CA ベンダーが署名した証明書が必要です。IP トラフィックがクラスタ LIF のみを経由するローカル階層化の場合、CA 証明書は必要ありません。

このタスクについて

オブジェクトストアサーバを作成すると、UID 0 の root ユーザが作成されます。この root ユーザに対してアクセスキーもシークレットキーも生成されません。ONTAP 管理者はを実行する必要があります `object-store-server users regenerate-keys` コマンドを使用して、このユーザのアクセスキーとシークレットキーを設定します。



ネットアップのベストプラクティスとして、この root ユーザは使用しないでください。root ユーザのアクセスキーまたはシークレットキーを使用するクライアントアプリケーションは、オブジェクトストア内のすべてのバケットとオブジェクトにフルアクセスできます。

を参照してください `vserver object-store-server` 追加の設定オプションおよび表示オプションのマニュアルページ




**System Manager の略**

既存のStorage VMにS3サーバを追加する場合は、この手順を使用します。新しいStorage VMにS3サーバを追加する方法については、を参照してください ["S3用のストレージSVMを作成します"](#)。

インターフェイスロールデータ用のIPアドレスを入力する準備をしておく必要があります。

## 1. 既存のStorage VMでS3を有効にします。

- a. Storage VMを選択します。\* Storage > Storage VM\*をクリックし、Storage VMを選択して\* Settings \*をクリックし、をクリックします  \* S3 の下 \*。
- b. Enable S3 \* をクリックし、 S3 Server Name を入力します。
- c. 証明書のタイプを選択します。

システムで生成された証明書と独自の証明書のどちらを選択した場合も、クライアントアクセスには証明書が必要です。

- d. ネットワークインターフェイスを入力してください。

## 2. システムで生成された証明書を選択した場合は、新しい Storage VM の作成を確認すると証明書情報が表示されます。[ダウンロード]をクリックし、クライアントアクセス用に保存します。

- シークレットキーは今後表示されません。
- 証明書情報が再度必要な場合は、[\* ストレージ]、[Storage VMs]の順にクリックし、Storage VMを選択して、[\* 設定]をクリックします。

**CLI の使用**

## 1. S3 サーバを作成します。

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

S3 サーバの作成時またはあとからいつでも追加のオプションを指定できます。

- ローカルの階層化を設定する場合は、SVM名にデータSVM名またはシステムSVM（クラスタ）名を指定できます。
- 証明書名は、サーバCA証明書（中間またはルートCA証明書）ではなく、サーバ証明書（エンドユーザまたはリーフ証明書）の名前にする必要があります。
- HTTPS は、ポート 443 でデフォルトで有効になっています。ポート番号はを使用して変更できます `-secure-listener-port` オプション

HTTPSを有効にすると、SSL/TLSと正しく統合するためにCA証明書が必要になります。

- HTTPはデフォルトで無効になっています。有効にすると、サーバはポート80でリスンします。を使用して有効にできます `-is-http-enabled` オプションを選択するか、ポート番号を `-listener-port` オプション

HTTPが有効な場合、要求と応答はクリアテキストでネットワーク経由で送信されます。

2. S3が設定されていることを確認します。

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

例

このコマンドは、すべてのオブジェクトストレージサーバの設定値を検証します。

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

Vserver: vs1

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

## S3 対応 SVM にストレージ容量を追加

バケットを作成する

S3オブジェクトは `_Buckets_` に保持されます。他のディレクトリ内のディレクトリ内にファイルとしてネストされることはありません。

作業を開始する前に

S3サーバを含むStorage VMがすでに存在している必要があります。

このタスクについて

- ONTAP 9.14.1以降では、S3 FlexGroupボリュームでバケットが作成されたときに自動サイズ変更が有効になりました。これにより、既存および新規のFlexGroupボリュームでバケットを作成する際の過剰な容量割り当てが解消されます。FlexGroupボリュームのサイズは、次のガイドラインに基づいて、必要な最小サイズに変更されます。必要な最小サイズは、FlexGroupボリューム内のすべてのS3バケットの合計サイズです。
  - ONTAP 9.14.1以降では、新しいバケットの作成時にS3 FlexGroupボリュームを作成すると、必要な最小サイズでFlexGroupボリュームが作成されます。
  - S3 FlexGroupボリュームがONTAP 9.14.1より前に作成された場合は、ONTAP 9.14.1のあとに最初に作成または削除されたバケットによって、FlexGroupボリュームのサイズが必要な最小サイズに変更されます。
  - ONTAP 9.14.1より前に作成されたS3 FlexGroupボリュームに必要な最小サイズがすでに設定されている場合は、ONTAP 9.14.1以降のバケットの作成または削除でS3 FlexGroupボリュームのサイズが維持されます。

- ストレージサービスレベルは、事前定義されたアダプティブ QoS ポリシーグループで、*value*、*performion*、*\_extreme* デフォルトレベルがあります。カスタムの QoS ポリシーグループを定義してバケットに適用すると、デフォルトのストレージサービスレベルのいずれかを使用する代わりに、そのグループを定義して使用することもできます。ストレージサービスの定義の詳細については、を参照してください。"[ストレージサービスの定義](#)"。パフォーマンス管理の詳細については、を参照してください。"[パフォーマンス管理](#)"。  
ONTAP 9.8 以降では、ストレージをプロビジョニングすると QoS がデフォルトで有効になります。QoS を無効にするか、プロビジョニングプロセス中またはあとからカスタムの QoS ポリシーを選択できます。
- ローカルの容量階層化を設定する場合は、S3サーバが配置されているシステムStorage VMではなく、データStorage VMIにバケットとユーザを作成します。
- リモートクライアントアクセスの場合は、S3 対応の Storage VM でバケットを設定する必要があります。S3 対応でない Storage VM にバケットを作成した場合、そのバケットはローカル階層化にのみ使用できます。
- ONTAP 9.14.1以降では、次のことが可能です。"[MetroCluster構成のミラーされたアグリゲートまたはミラーされていないアグリゲートにバケットを作成する](#)"。
- CLIでは、バケットを作成する際に、次の2つのプロビジョニングオプションを選択できます。

- 基盤となるアグリゲートと FlexGroup コンポーネントを ONTAP Select に提供（デフォルト）

- ONTAP は、アグリゲートを自動的に選択することで、最初のバケット用の FlexGroup ボリュームを作成して設定します。プラットフォームに使用できる最も高いサービスレベルが自動的に選択されるほか、ストレージサービスレベルを指定することもできます。あとでStorage VMに追加するバケットには、同じFlexGroupボリュームが使用されます。
- また、バケットを階層化に使用するかどうかを指定することもできます。この場合、ONTAP は階層化データのパフォーマンスが最適な低コストのメディアを選択しようとします。

- 使用するアグリゲートとFlexGroupコンポーネントを選択します（advanced権限のコマンドオプションが必要です）。バケットと包含FlexGroupボリュームを作成するアグリゲートを手動で選択し、各アグリゲートのコンスティチュエントの数を指定できます。バケットを追加する場合：

- 新しいバケットにアグリゲートとコンスティチュエントを指定すると、新しいバケット用の新しい FlexGroup が作成されます。
- 新しいバケットにアグリゲートとコンスティチュエントを指定しない場合、新しいバケットが既存の FlexGroup に追加されます。  
を参照してください [FlexGroup ボリューム管理](#) を参照してください。

バケットの作成時にアグリゲートとコンスティチュエントを指定した場合、デフォルトまたはカスタムの QoS ポリシーグループは適用されません。これは、を使用してあとで実行できます  
`vserver object-store-server bucket modify` コマンドを実行します

を参照してください "[vserver object-store-serverバケットmodifyの数が変更されました](#)" を参照してください。

注： Cloud Volumes ONTAP からバケットを処理する場合は、CLI手順 を使用してください。基盤となるアグリゲートを手動で選択し、いずれかのノードだけを使用することを強く推奨します。両方のノードのアグリゲートを使用すると、ノードが地理的に分離された可用性ゾーンに配置されるため、レイテンシの問題の影響を受けやすくなるため、パフォーマンスに影響を及ぼす可能性があります。

## ONTAP CLIを使用したS3バケットの作成

1. アグリゲートとFlexGroup コンポーネントを自分で選択する場合は、権限レベルをadvancedに設定します（それ以外の場合はadmin権限レベルで十分です）。 `set -privilege advanced`
2. バケットを作成します。

```
vserver object-store-server bucket create -vserver svm_name -bucket
bucket_name [-size integer[KB|MB|GB|TB|PB]] [-comment text]
[additional_options]
```

Storage VM名には、データStorage VMまたは Cluster（システムStorage VM名）（ローカルの階層化を設定する場合）。

オプションを指定しない場合、ONTAPは800GBのバケットを作成し、サービスレベルをシステムで使用可能な最も高いレベルに設定します。

パフォーマンスまたは使用量に基づいて ONTAP でバケットを作成する場合は、次のいずれかのオプションを使用します。

- サービスレベル

を含めます `-storage-service-level` オプションに次のいずれかの値を指定します。 `value`、`performance` または `extreme`。

- 階層化

を含めます `-used-as-capacity-tier true` オプション

基盤となる FlexGroup ボリュームを作成するアグリゲートを指定する場合は、次のオプションを使用します。

- 。 `-aggr-list` パラメータは、FlexGroup ボリュームのコンスティチュエントに使用するアグリゲートのリストを指定します。

指定したエントリごとに、そのアグリゲート上にコンスティチュエントが1つ作成されます。同じアグリゲートを複数回指定すると、そのアグリゲート上に複数のコンスティチュエントを作成できます。

FlexGroup 全体で一貫したパフォーマンスが得られるように、すべてのアグリゲートで同じディスクタイプと RAID グループ構成を使用する必要があります。

- 。 `-aggr-list-multiplier` パラメータは、に表示されるアグリゲートを反復する回数を指定します `-aggr-list` FlexGroup ボリューム作成時のパラメータ。

のデフォルト値 `-aggr-list-multiplier` パラメータは4です。

3. 必要に応じて QoS ポリシーグループを追加します。

```
vserver object-store-server bucket modify -bucket bucket_name -qos-policy
-group qos_policy_group
```

4. バケットの作成を確認します。

```
vserver object-store-server bucket show [-instance]
```

## 例

次の例は、Storage VMのバケットを作成します。vs1 サイズ 1TB アグリゲートを指定する場合

```
cluster-1::*> vserver object-store-server bucket create -vserver  
svml.example.com -bucket testbucket -aggr-list aggr1 -size 1TB
```

## System Managerを使用したS3バケットの作成

### 1. S3 対応 Storage VM に新しいバケットを追加

- a. [\* ストレージ]、[バケット]の順にクリックし、[\* 追加]をクリックします。
- b. 名前を入力し、Storage VM を選択してサイズを入力します。
  - この時点で \* Save \* をクリックすると、次のデフォルト設定でバケットが作成されます。
  - どのグループポリシーも有効になっていないかぎり、バケットへのアクセスはユーザに許可されません。



S3 root ユーザを使用して ONTAP オブジェクトストレージを管理したり権限を共有したりしないでください。オブジェクトストアに無制限にアクセスできます。代わりに、割り当てた管理者権限を持つユーザまたはグループを作成してください。

- システムで最も利用可能なサービス品質（パフォーマンス）レベル。
- [保存]\*をクリックして、これらのデフォルト値でバケットを作成します。

## 追加の権限と制限を設定する

バケットの設定時に[\*その他のオプション]\*をクリックすると、オブジェクトロック、ユーザ権限、パフォーマンスレベルを設定できます。設定はあとで変更することもできます。

S3 オブジェクトストアを FabricPool の階層化に使用する場合は、パフォーマンスサービスレベルではなく、階層化に \* 使用（階層化データのパフォーマンスが最適な低コストのメディアを使用）を選択することを確認してください。

後でリカバリするためにオブジェクトのバージョン管理を有効にする場合は、\*バージョン管理を有効にする\*を選択します。バケットでオブジェクトのロックを有効にすると、バージョン管理がデフォルトで有効になります。オブジェクトのバージョン管理の詳細については、[を参照してください。"AmazonのS3バケットでのバージョン管理の使用"](#)。

9.14.1以降では、S3バケットでオブジェクトロックがサポートされます。S3オブジェクトロックには標準のSnapLockライセンスが必要です。このライセンスは、["ONTAP One"](#)。

ONTAP Oneよりも前のリリースでは、SnapLockライセンスはSecurity and Compliance Bundleに含まれていました。Security and Compliance Bundleの提供は終了しましたが、引き続き有効です。現在は必須ではありませんが、既存のお客様は ["ONTAP Oneへのアップグレード"](#)。

バケットでオブジェクトのロックを有効にする場合は、次の手順を実行します。 ["SnapLockライセンスがインストールされていることの確認"](#)。SnapLockライセンスがインストールされていない場合は、["をインストールします"](#) オブジェクトロックを有効にする前に有効にします。

SnapLockライセンスがインストールされていることを確認したら、バケット内のオブジェクトが削除または上書きされないように保護するには、\*[オブジェクトのロックを有効にする]\*を選択します。ロックは、すべてのバージョンまたは特定のバージョンのオブジェクトで有効にできます。また、クラスタノードのSnapLockコンプライアンスロックが初期化されている場合にのみ有効にできます。次の手順を実行します。

1. クラスターのいずれのノードでもSnapLockコンプライアンスロックが初期化されていない場合は、**[Initialize SnapLock Compliance Clock]\***ボタンが表示されます。クラスタノードの**SnapLock**コンプライアンスロックを初期化するには、**[ SnapLockコンプライアンスロックの初期化]\***をクリックします。
2. オブジェクトに対して **\_ Write Once、Read Many (WORM) \_** 権限を許可する時間ベースのロックを有効にするには、**\* Governance \***モードを選択します。Governance\_modeであっても、特定の権限を持つ管理者ユーザがオブジェクトを削除できます。
3. オブジェクトに対してより厳密な削除ルールと更新ルールを割り当てる場合は、**\* 準拠 \***モードを選択します。このモードのオブジェクトロックでは、指定した保持期間が終了した時点でのみオブジェクトを期限切れにできます。保持期間を指定しないかぎり、オブジェクトは無期限にロックされたままになります。
4. 一定期間ロックを有効にする場合は、ロックの保持期間を日単位または年単位で指定します。



ロックは、バージョン管理に対応しているS3バケットとバージョン管理に対応していないS3バケットに適用されます。オブジェクトのロックは、NASオブジェクトには適用されません。

バケットの保護と権限の設定、およびパフォーマンスサービスレベルを設定できます。



権限を設定する前に、ユーザとグループを作成しておく必要があります。

詳細については、を参照してください **"新しいバケット用のミラーを作成します"**。

バケットへのアクセスを確認

S3クライアントアプリケーション（ONTAP S3または外部のサードパーティアプリケーション）では、次のように入力して、新しく作成したバケットへのアクセスを確認できます。

- S3 サーバの CA 証明書。
- ユーザのアクセスキーとシークレットキー。
- S3 サーバの FQDN 名とバケット名。

**MetroCluster**構成のミラーされたアグリゲートまたはミラーされていないアグリゲートにバケットを作成する

ONTAP 9.14.1以降では、MetroCluster FC構成およびIP構成のミラーされたアグリゲートまたはミラーされていないアグリゲートにバケットをプロビジョニングできます。

このタスクについて

- デフォルトでは、バケットはミラーされたアグリゲート上にプロビジョニングされます。
- プロビジョニングのガイドラインは、と同じです。 **"バケットを作成する"** MetroCluster環境でのバケットの作成に適用

- MetroCluster環境では、S3オブジェクトストレージの次の機能は\*サポートされません\*。

- S3 SnapMirrorの略
- S3バケットのライフサイクル管理
- Compliance \*モードでのS3オブジェクトのロック



\*ガバナンス\*モードでのS3オブジェクトのロックがサポートされています。

- ローカルFabricPool階層化

作業を開始する前に

S3 サーバを含む SVM がすでに存在している必要があります。

バケットを作成するプロセス

## CLI の使用

1. アグリゲートとFlexGroup コンポーネントを自分で選択する場合は、権限レベルをadvancedに設定します（それ以外の場合はadmin権限レベルで十分です）。`set -privilege advanced`
2. バケットを作成します。

```
vserver object-store-server bucket create -vserver <svm_name> -bucket  
<bucket_name> [-size integer[KB|MB|GB|TB|PB]] [-use-mirrored-aggregates  
true/false]
```

を設定します `-use-mirrored-aggregates` オプションをに設定します `true` または `false` ミラーされたアグリゲートとミラーされていないアグリゲートのどちらを使用するかによって異なります。



デフォルトでは、が表示されます `-use-mirrored-aggregates` オプションはに設定されています `true`。

- SVM名はデータSVMである必要があります。
- オプションを指定しない場合、ONTAPは800GBのバケットを作成し、サービスレベルをシステムで使用可能な最も高いレベルに設定します。
- パフォーマンスまたは使用量に基づいて ONTAP でバケットを作成する場合は、次のいずれかのオプションを使用します。

- サービスレベル

を含めます `-storage-service-level` オプションに次のいずれかの値を指定します。  
`value`、`performance` または `extreme`。

- 階層化

を含めます `-used-as-capacity-tier true` オプション

- 基盤となる FlexGroup ボリュームを作成するアグリゲートを指定する場合は、次のオプションを使用します。

- `-aggr-list` パラメータは、FlexGroup ボリュームのコンスティチュエントに使用するアグリゲートのリストを指定します。

指定したエントリごとに、そのアグリゲート上にコンスティチュエントが1つ作成されます。同じアグリゲートを複数回指定すると、そのアグリゲート上に複数のコンスティチュエントを作成できます。

FlexGroup 全体で一貫したパフォーマンスが得られるように、すべてのアグリゲートで同じディスクタイプと RAID グループ構成を使用する必要があります。

- `-aggr-list-multiplier` パラメータは、に表示されるアグリゲートを反復する回数を指定します `-aggr-list` FlexGroup ボリューム作成時のパラメータ。

のデフォルト値 `-aggr-list-multiplier` パラメータは4です。

3. 必要に応じて QoS ポリシーグループを追加します。



```
vserver object-store-server bucket modify -bucket bucket_name -qos-policy  
-group qos_policy_group
```

#### 4. バケットの作成を確認します。

```
vserver object-store-server bucket show [-instance]
```

#### 例

次の例では、ミラーされたアグリゲート上に1TBのSVM vs1のバケットを作成します。

```
cluster-1::*> vserver object-store-server bucket create -vserver  
svm1.example.com -bucket testbucket -size 1TB -use-mirrored-aggregates  
true
```

### System Manager の略

#### 1. S3 対応 Storage VM に新しいバケットを追加

- a. [ \* ストレージ ]、[ バケット ] の順にクリックし、[ \* 追加 ] をクリックします。
- b. 名前を入力し、Storage VM を選択してサイズを入力します。

デフォルトでは、バケットはミラーされたアグリゲートにプロビジョニングされます。ミラーされていないアグリゲートにバケットを作成する場合は、[その他のオプション]\*を選択し、[保護]の[ SyncMirror階層を使用する]\*ボックスをオフにします（次の図を参照）。

## Add bucket

NAME

To use this bucket from a remote cluster, configure S3 service on storage VM "vs1".

FOLDER (OPTIONAL)

Specify the folder to map to this bucket. [Know more](#)

CAPACITY

Size
GB

☐ Use tiering  
If you select this option, the system will try to select low-cost media with optimal performance for the tiered data.

☐ Enable versioning  
Versioning-enabled buckets allow you to recover objects that were accidentally deleted or overwritten. After versioning is enabled, it can't be disabled. However, you can suspend versioning.

PERFORMANCE SERVICE LEVEL

Value

Not sure? [Get help selecting type](#)

Permissions
☐ Copy access permissions from an existing bucket

Principal	Effect	Actions	Resources	Conditions
All users of this stor...	allow	ListBucket	*	

+ Add

Object locking
☐ Enable object locking  
Object locking utilizes the "Write Once, Read Many" (WORM) model in which objects or their versions are protected from being deleted or overwritten during the specified retention period.

Protection
☒ Use the S3x3l0n0r10n

- この時点で \* Save \* をクリックすると、次のデフォルト設定でバケットが作成されます。
  - どのグループポリシーも有効になっていないかぎり、バケットへのアクセスはユーザに許可されません。



S3 root ユーザを使用して ONTAP オブジェクトストレージを管理したり権限を共有したりしないでください。オブジェクトストアに無制限にアクセスできます。代わりに、割り当てた管理者権限を持つユーザまたはグループを作成してください。

- システムで最も利用可能なサービス品質（パフォーマンス）レベル。
- バケットの設定時にユーザの権限やパフォーマンスレベルを設定するには、「\* More Options \*」をクリックします。あとで設定を変更することもできます。

- 権限を設定するために \* More Options \* を使用する前に、ユーザーとグループを作成しておく必要があります。
  - S3 オブジェクトストアを FabricPool の階層化に使用する場合は、パフォーマンスサービスレベルではなく、階層化に \* 使用（階層化データのパフォーマンスが最適な低コストのメディアを使用）を選択することを検討してください。
2. 別の ONTAP システムまたは外部のサードパーティ製アプリケーションである S3 クライアントアプリケーションで、次のように入力して新しいバケットへのアクセスを確認します。
- S3 サーバの CA 証明書。
  - ユーザーのアクセスキーとシークレットキー。
  - S3 サーバの FQDN 名とバケット名。

バケットライフサイクル管理ルールを作成します

ONTAP 9.13.1以降では、S3バケット内のオブジェクトライフサイクルを管理するためのライフサイクル管理ルールを作成できます。バケット内の特定のオブジェクトに対して削除ルールを定義し、それらのルールを使用してバケットオブジェクトを期限切れにすることができます。これにより、保持要件を満たし、S3オブジェクトストレージ全体を効率的に管理できます。



バケットオブジェクトに対してオブジェクトロックが有効になっている場合、オブジェクトの有効期限に関するライフサイクル管理ルールはロックされたオブジェクトには適用されません。オブジェクトのロックについては、[を参照してください](#)。"[バケットを作成する](#)"。

作業を開始する前に

S3 サーバとバケットを含む S3 対応の SVM がすでに存在している必要があります。を参照してください "[S3 用の SVM を作成します](#)" を参照してください。

このタスクについて

ライフサイクル管理ルールを作成する際に、バケットオブジェクトに次の削除操作を適用できます。

- 現在のバージョンの削除-このアクションは、ルールで指定されたオブジェクトを期限切れにします。バケットでバージョン管理が有効になっている場合は、S3によって、期限切れになったすべてのオブジェクトが使用できなくなります。バージョン管理が有効になっていない場合は、オブジェクトが永続的に削除されます。CLIの操作は次のとおりです。 `Expiration`。
- Deletion of non-current versions - S3が最新でないオブジェクトを完全に削除できるタイミングを指定します。CLIの操作は次のとおりです。 `NoncurrentVersionExpiration`。
- 期限切れ削除マーカーの削除-このアクションは、期限切れのオブジェクト削除マーカーを削除します。バージョン管理が有効なバケットでは、削除マーカーが付いたオブジェクトがオブジェクトの現在のバージョンになります。オブジェクトは削除されず、アクションを実行することはできません。これらのオブジェクトに現在のバージョンが関連付けられていない場合、これらのオブジェクトは期限切れになります。CLIの操作は次のとおりです。 `Expiration`。
- [Deletion of incomplete multipart uploads]-マルチパートアップロードを実行中のままにする最大時間（日数）を設定します。その後、それらは削除されます。CLIの操作は次のとおりです。 `AbortIncompleteMultipartUpload`。

使用する手順は、使用するインターフェイスによって異なります。ONTAP 9.13、1では、CLIを使用する必要があります。ONTAP 9.14.1以降では、System Managerも使用できます。

CLIを使用したライフサイクル管理ルール of 管理

ONTAP 9.13.1以降では、ONTAP CLIを使用してライフサイクル管理ルールを作成し、S3バケット内のオブジェクトを期限切れにすることができます。

作業を開始する前に

CLIでは、バケットライフサイクル管理ルールを作成するときに、有効期限アクションタイプごとに必須フィールドを定義する必要があります。これらのフィールドは、最初の作成後に変更できます。次の表に、アクションタイプごとに固有のフィールドを示します。

アクションタイプ	一意のフィールド
NonCurrentVersionExpiration	<ul style="list-style-type: none"><li>• -non-curr-days -最新でないバージョンが削除されるまでの日数</li><li>• -new-non-curr-versions -保持する最新の非最新バージョンの数</li></ul>
有効期限	<ul style="list-style-type: none"><li>• -obj-age-days -オブジェクトの現在のバージョンを削除できるようになるまでの作成からの日数</li><li>• -obj-exp-date -オブジェクトが期限切れになる日付</li><li>• -expired-obj-del-markers -オブジェクト削除マーカースクリーンアップします</li></ul>
AbortIncompleteMultipartUpload の略	<ul style="list-style-type: none"><li>• -after-initiation-days -アップロードを中止できる開始日数。この日数を過ぎるとアップロードが中止されます</li></ul>

バケットライフサイクル管理ルールを特定のオブジェクトのサブセットにのみ適用するには、管理者はルールの作成時に各フィルタを設定する必要があります。ルールの作成時にこれらのフィルタが設定されていない場合、ルールはバケット内のすべてのオブジェクトに適用されます。

以下の場合、すべてのフィルタを最初に作成した後\_except\_に変更できます。+

- -prefix
- -tags
- -obj-size-greater-than
- -obj-size-less-than

手順

1. を使用します `vserver object-store-server bucket lifecycle-management-rule create` バケットライフサイクル管理ルールを作成するためのexpirationアクションタイプの必須フィールドを含むコマンド。

例

次のコマンドは、NonCurrentVersionExpirationバケットライフサイクル管理ルールを作成します。

```
vserver object-store-server bucket lifecycle-management-rule create
-vserver <svm_name> -bucket <bucket_name> -rule-id <rule_name> -action
NonCurrentVersionExpiration -index <lifecycle_rule_index_integer> -is
-enabled {true|false} -prefix <object_name> -tags <text> -obj-size-greater
-than {<integer>[KB|MB|GB|TB|PB]} -obj-size-less-than
{<integer>[KB|MB|GB|TB|PB]} -new-non-curr-versions <integer> -non-curr
-days <integer>
```

#### 例

次のコマンドは、Expirationバケットライフサイクル管理ルールを作成します。

```
vserver object-store-server bucket lifecycle-management-rule create
-vserver <svm_name> -bucket <bucket_name> -rule-id <rule_name> -action
Expiration -index <lifecycle_rule_index_integer> -is-enabled {true|false}
-prefix <object_name> -tags <text> -obj-size-greater-than
{<integer>[KB|MB|GB|TB|PB]} -obj-size-less-than
{<integer>[KB|MB|GB|TB|PB]} -obj-age-days <integer> -obj-exp-date
<"MM/DD/YYYY HH:MM:SS"> -expired-obj-del-marker {true|false}
```

#### 例


次のコマンドは、AbortIncompleteMultipartUploadバケットライフサイクル管理ルールを作成します。


```
vserver object-store-server bucket lifecycle-management-rule create
-vserver <svm_name> -bucket <bucket_name> -rule-id <rule_name> -action
AbortIncompleteMultipartUpload -index <lifecycle_rule_index_integer> -is
-enabled {true|false} -prefix <object_name> -tags <text> -obj-size-greater
-than {<integer>[KB|MB|GB|TB|PB]} -obj-size-less-than
{<integer>[KB|MB|GB|TB|PB]} -after-initiation-days <integer>
```

### System Managerを使用したライフサイクル管理ルールの管理

ONTAP 9.14.1以降では、System Managerを使用してS3オブジェクトを期限切れにすることができます。S3オブジェクトのライフサイクル管理ルールを追加、編集、削除できます。また、あるバケット用に作成されたライフサイクルルールをインポートして、別のバケット内のオブジェクトに使用することもできます。アクティブなルールは、あとで無効にして有効にすることができます。


ライフサイクル管理ルールを追加します。

1. [ストレージ]>[バケット]\*をクリックします。
2. 有効期限ルールを指定するバケットを選択します。
3. をクリックします  アイコンをクリックし、\*[ライフサイクルルールの管理]\*を選択します。
4. [追加]>[ライフサイクルルール]\*をクリックします。

5. [ライフサイクルルールの追加]ページで、ルールの名前を追加します。
  6. ルールの範囲を定義します。ルールをバケット内のすべてのオブジェクトに適用するか、特定のオブジェクトに適用するかを指定します。オブジェクトを指定する場合は、次のいずれかのフィルタ条件を少なくとも1つ追加します。
    - a. prefix：ルールを適用するオブジェクトキー名のプレフィックスを指定します。通常は、オブジェクトのパスまたはフォルダです。ルールごとに1つのプレフィックスを入力できます。有効なプレフィックスが指定されていないかぎり、ルールはバケット内のすべてのオブジェクトを環境にします。
    - b. tags：ルールを適用するオブジェクトのキーと値のペア（タグ）を3つまで指定します。フィルタリングには有効なキーのみが使用されます。この値はオプションです。ただし、値を追加する場合は、対応するキーに有効な値のみを追加してください。
    - c. サイズ：オブジェクトの最小サイズと最大サイズの間でスコープを制限できます。どちらかまたは両方の値を入力できます。デフォルトの単位はMIBです。
  7. アクションを指定します。
    - a. オブジェクトの現在のバージョンを期限切れにする：現在のオブジェクトが作成されてから一定の日数が経過した後、または特定の日付に、すべてのオブジェクトを永続的に使用不可にするルールを設定します。このオプションは、\*期限切れのオブジェクト削除マーカーを削除\*オプションが選択されている場合は使用できません。
    - b. 最新でないバージョンを完全に削除：バージョンが最新でなくなってから削除できるようになるまでの日数と、保持するバージョンの数を指定します。
    - c. 期限切れのオブジェクト削除マーカーを削除：期限切れの削除マーカーを持つオブジェクト、つまり現在のオブジェクトが関連付けられていないマーカーを削除するには、このアクションを選択します。
- 

このオプションは、保持期間後にすべてのオブジェクトを自動的に削除する\*[現在のバージョンのオブジェクトを期限切れにする]\*オプションを選択すると使用できなくなります。オブジェクトタグをフィルタリングに使用している場合も、このオプションは使用できません。
- d. 未完了のマルチパートアップロードを削除：未完了のマルチパートアップロードを削除するまでの日数を設定します。指定した保持期間内に実行中のマルチパートアップロードが失敗した場合は、完了していないマルチパートアップロードを削除できます。オブジェクトタグをフィルタリングに使用すると、このオプションは使用できなくなります。
  - e. [保存（Save）]をクリックします。

## ライフサイクルルールのインポート


1. [ストレージ]>[バケット]\*をクリックします。
2. 有効期限ルールをインポートするバケットを選択します。
3. をクリックします  アイコンをクリックし、\*[ライフサイクルルールの管理]\*を選択します。
4. [追加]>[ルールのインポート]\*をクリックします。
5. ルールのインポート元のバケットを選択します。選択したバケットに対して定義されているライフサイクル管理ルールが表示されます。
6. インポートするルールを選択します。一度に1つのルールを選択できます。デフォルトでは最初のルールが選択されます。

7. [\* インポート \*] をクリックします。

## ルールの編集、削除、または無効化

編集できるのは、ルールに関連付けられているライフサイクル管理アクションのみです。ルールがオブジェクトタグでフィルタされている場合は、[期限切れのオブジェクト削除マーカーを削除する]\*オプションと[不完全なマルチパートアップロードを削除する]\*オプションは使用できません。

ルールを削除すると、そのルールは以前に関連付けられていたオブジェクトには適用されなくなります。

1. [ストレージ]>[バケット]\*をクリックします。
2. ライフサイクル管理ルールを編集、削除、または無効にするバケットを選択します。
3. をクリックします  アイコンをクリックし、\*[ライフサイクルルールの管理]\*を選択します。
4. 必要なルールを選択します。一度に1つのルールを編集および無効にすることができます。一度に複数のルールを削除できます。
5. 、[削除]、または[無効化]\*を選択し、手順を完了します。

## S3 ユーザを作成します

許可されたクライアントだけに接続を制限するには、すべてのONTAPオブジェクトストアでユーザ認証が必要です。

始める前に。

S3対応Storage VMがすでに存在する必要があります。

このタスクについて

S3ユーザにはStorage VM内の任意のバケットへのアクセスを許可できます。S3ユーザを作成すると、そのユーザのアクセスキーとシークレットキーも生成されます。オブジェクトストアのFQDNとバケット名をユーザと共有する必要があります。S3ユーザのキーは、`vserver object-store-server user show` コマンドを実行します

バケットポリシーまたはオブジェクトサーバポリシーで、S3 ユーザに特定のアクセス権限を付与できます。



新しいオブジェクトストアサーバを作成すると、ONTAPによってrootユーザ（UID 0）が作成されます。rootユーザは、すべてのバケットにアクセスできる権限を持つユーザです。NetAppでは、ONTAP S3をrootユーザとして管理するのではなく、特定の権限を指定してadminユーザロールを作成することを推奨します。

## CLI の使用

### 1. S3 ユーザを作成します。

```
vserver object-store-server user create -vserver svm_name -user user_name  
-comment [-comment text] -key-time-to-live time
```


- コメントの追加は任意です。
- ONTAP 9.14.1以降では、キーが有効になる期間を `-key-time-to-live` パラメータ保持期間を次の形式で追加して、アクセスキーの有効期限が切れるまでの期間を指定できます。  
`P[<integer>D]T[<integer>H][<integer>M][<integer>S] | P<integer>W`  
たとえば、1日、2時間、3分、4秒の保持期間を入力する場合は、次のように入力します。  
`P1DT2H3M4S`。指定されていないかぎり、キーは無期限に有効です。

次の例では、という名前のユーザを作成します。 `sm_user1` Storage VM上 `vs0` キーの保持期間は1週間です。

```
vserver object-store-server user create -vserver vs0 -user sm_user1  
-key-time-to-live P1W
```

### 2. アクセスキーとシークレットキーは必ず保存してください。S3クライアントからのアクセスに必要になります。

## System Manager の略

1. Storage > Storage VM\* をクリックします。ユーザを追加する必要があるStorage VMを選択し、\*[設定]\*を選択して  S3 の下。
2. ユーザを追加するには、\*[ユーザ]>[追加]\*をクリックします。
3. ユーザの名前を入力します。
4. ONTAP 9.14.1以降では、ユーザに対して作成されるアクセスキーの保持期間を指定できます。キーが自動的に期限切れになるまでの保持期間を、日、時間、分、または秒で指定できます。デフォルトでは、この値は 0 これは、キーが無期限に有効であることを示します。
5. [保存 (Save)] をクリックします。ユーザが作成され、そのユーザのアクセスキーとシークレットキーが生成されます。
6. アクセスキーとシークレットキーをダウンロードまたは保存します。S3クライアントからのアクセスに必要になります。

## 次のステップ

- [S3 グループを作成または変更します](#)

## S3 グループを作成または変更します

適切なアクセス許可を持つユーザのグループを作成することで、バケットへのアクセスを簡易化できます。

作業を開始する前に

S3 対応 SVM の S3 ユーザがすでに存在している必要があります。



このタスクについて

S3 グループのユーザには、SVM 内の任意のバケットへのアクセスを許可できますが、複数の SVM のユーザには許可できません。グループアクセス権限は、次の 2 つの方法で設定できます。


- をバケットレベルで指定します

S3 ユーザのグループを作成したら、バケットポリシーステートメントでグループ権限を指定します。この権限は、そのバケットにのみ適用されます。

- をクリックします

S3 ユーザのグループを作成したら、グループ定義でオブジェクトサーバのポリシー名を指定します。これらのポリシーによって、バケットとグループメンバーのアクセスが決まります。

#### System Manager の略

1. Storage VM を編集します。\* Storage > Storage VM\* をクリックし、Storage VM をクリックして \* Settings \* をクリックし、をクリックします  S3 の下。
2. グループを追加：\* Groups を選択し、Add \*を選択します。
3. グループ名を入力し、ユーザのリストから選択します。
4. 既存のグループポリシーを選択するか、今すぐ追加するか、あとからポリシーを追加できます。

#### CLI の使用

1. S3 グループを作成します。

```
vserver object-store-server group create -vserver svm_name -name group_name -users user_name\(s\) [-policies policy_names] [-comment text\]
```

  - 。 -policies オプションは、オブジェクトストアにバケットが1つしかない設定では省略できます。グループ名はバケットポリシーに追加できます。
  - 。 -policies オプションは、を使用してあとで追加できます `vserver object-store-server group modify` オブジェクトストレージサーバポリシーの作成後に実行するコマンドです。

キーを再生成して保持期間を変更する

アクセスキーとシークレットキーは、S3クライアントアクセスを有効にするためのユーザの作成時に自動的に生成されます。キーの有効期限が切れた場合や、キーが侵害された場合に、ユーザのキーを再生成できます。

アクセスキーの生成については、を参照してください。 ["S3 ユーザを作成します"](#)。



## CLI の使用

1. 次のコマンドを実行して、ユーザのアクセスキーとシークレットキーを再生成します。 `vserver object-store-server user regenerate-keys` コマンドを実行します
2. デフォルトでは、生成されたキーは無期限に有効です。9.14.1以降では、キーの保持期間を変更できます。この期間が過ぎると、キーは自動的に期限切れになります。保持期間は次の形式で追加できます。 `P[<integer>D]T[<integer>H][<integer>M][<integer>S] | P<integer>W`  
たとえば、1日、2時間、3分、4秒の保持期間を入力する場合は、次のように入力します。  
`P1DT2H3M4S。`

```
vserver object-store-server user regenerate-keys -vserver svm_name  
-user user -key-time-to-live 0
```

3. アクセスキーとシークレットキーを保存します。S3クライアントからのアクセスに必要なになります。

## System Manager の略

1. Storage > Storage VM\* をクリックし、Storage VM を選択します。
2. [\* 設定 \*] タブで、をクリックします  を \* S3 \* タイルに追加します。
3. [ユーザ]タブで、アクセスキーがないか、ユーザのキーの有効期限が切れていることを確認します。
4. キーを再生成する必要がある場合は、  アイコン"] ユーザーの横にある\*[キーの再生成]\*をクリックします。
5. デフォルトでは、生成されたキーは無期限に有効です。9.14.1以降では、キーの保持期間を変更できます。この期間が過ぎると、キーは自動的に期限切れになります。保持期間を日、時間、分、または秒単位で入力します。
6. [保存 ( Save ) ] をクリックします。キーが再生成されます。キーの保持期間の変更はすぐに反映されます。
7. アクセスキーとシークレットキーをダウンロードまたは保存します。S3クライアントからのアクセスに必要なになります。

## アクセスポリシーステートメントを作成または変更します

### バケットとオブジェクトストアのサーバポリシーについて

S3 リソースへのユーザとグループのアクセスは、バケットとオブジェクトストアのサーバポリシーによって制御されます。ユーザまたはグループの数が少ない場合はバケットレベルでアクセスを制御すれば十分であると考えられますが、ユーザやグループが多数ある場合はオブジェクトストアサーバレベルでアクセスを制御する方が簡単です。

### バケットポリシーを変更する

デフォルトのバケットポリシーにアクセスルールを追加できます。アクセス制御の範囲はコンテナバケットなので、バケットが1つしかない場合は最も適しています。

作業を開始する前に

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

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

このタスクについて

新しいユーザとグループに新しいステートメントを追加したり、既存のステートメントの属性を変更したりできます。その他のオプションについては、を参照してください `vserver object-store-server bucket policy` マニュアルページ

ユーザとグループの権限は、バケットの作成時または必要に応じてあとから付与できます。バケットの容量とQoS ポリシーグループの割り当てを変更することもできます。

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

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

## System Manager の略

### 手順

1. バケットを編集します。 \* Storage > Bucket\* をクリックし、目的のバケットをクリックして \* Edit \* をクリックします。

権限を追加または変更するときに、次のパラメータを指定できます。

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

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

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



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

## CLI の使用

### 手順

1. バケットポリシーにステートメントを追加します。

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

次のパラメータでアクセス権限を定義します。

-effect	この文では ' アクセスを許可または拒否できます
-action	を指定できます * すべてのアクション、または次の1つ以上のリストを意味します。GetObject, PutObject, DeleteObject, ListBucket, GetBucketAcl, GetObjectAcl, ListBucketMultipartUploads, および ListMultipartUploadParts。

-principal	<p>1 つ以上の S3 ユーザまたはグループのリスト。</p> <ul style="list-style-type: none"> <li>• 最大 10 のユーザまたはグループを指定できます。</li> <li>• S3グループを指定する場合は、の形式で指定する必要があります group/group_name.</li> <li>• * には、パブリックアクセス（アクセスキーとシークレットキーを使用しないアクセス）を指定できます。</li> <li>• プリンシパルを指定しない場合、Storage VM内のすべてのS3ユーザにアクセスが許可されます。</li> </ul>
-resource	<p>バケットとバケットに含まれるすべてのオブジェクト。ワイルドカード文字 * および ? リソースを指定するための正規表現を作成するために使用できます。リソースについては、ポリシーで変数を指定できます。これらのポリシー変数は、ポリシーが評価されるときにコンテキスト値に置き換えられるプレースホルダです。</p>

オプションで、テキスト文字列をコメントとして指定できます -sid オプション

#### 例

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

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

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

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

ONTAP 9.14.1以降では、バケットポリシーの変数を指定できます。次の例は、Storage VM用のサーババケットポリシーステートメントを作成します。svm1 および bucket1、およびを指定します。

`${aws:username}` ポリシーリソースの変数として指定します。ポリシーが評価されると、ポリシー変数は要求コンテキストのユーザ名に置き換えられ、そのユーザに対して設定されたとおりにポリシーアクションを実行できます。たとえば、次のポリシーステートメントが評価されると、`${aws:username}` は、S3処理を実行するユーザに置き換えられます。ユーザが user1 操作を実行し、そのユーザにアクセスを許可します。bucket1 として bucket1/user1/\*。

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

オブジェクトストアサーバポリシーを作成または変更する

オブジェクトストア内の 1 つ以上のバケットに適用できるポリシーを作成できます。オブジェクトストアサーバのポリシーをユーザのグループに関連付けることで、複数のバケット間のリソースアクセスの管理を簡易化することができます。

作業を開始する前に

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

このタスクについて

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



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

ONTAP S3 リソースへのアクセスに使用する読み取り専用のデフォルトポリシーは 3 つあります。

- フルアクセス
- NoS3アクセス
- ReadOnlyAccess の略

また、新しいカスタムポリシーを作成し、新しいユーザとグループに新しいステートメントを追加したり、既存のステートメントの属性を変更したりすることもできます。その他のオプションについては、を参照してください `vserver object-store-server policy` ["コマンドリファレンス"](#)。


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

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

## System Manager の略

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

### 手順

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

グループポリシーを追加または変更する際には、次のパラメータを指定できます。

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

## CLI の使用

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

### 手順

1. オブジェクトストレージサーバポリシーを作成します。

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

2. ポリシーのステートメントを作成します。

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

次のパラメータでアクセス権限を定義します。

-effect	この文では ' アクセスを許可または拒否できません
---------	---------------------------

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

オプションで、テキスト文字列をコメントとして指定できます -sid オプション

デフォルトでは、新しいステートメントはステートメントのリストの末尾に追加され、順番に処理されます。後でステートメントを追加または変更する場合は、ステートメントのを変更するオプションがあります -index 処理順序を変更するための設定。

## 外部ディレクトリサービス用のS3アクセスの設定

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

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

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

作業を開始する前に

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

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



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

外部ディレクトリサービス用の**S3**アクセスの設定

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

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

このコマンドの詳細については、を参照してください ["vserver services name-service ns-switch modify"](#) コマンドを実行します

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

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

例：次の例では、buck1。このポリシーは、LDAPグループへのアクセスを許可します。group1 リソース（バケットとそのオブジェクト）に buck1。

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

3. LDAPグループのユーザが group1 S3クライアントからS3処理を実行できます。

認証に**LDAP**高速バインドモードを使用する

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

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

このコマンドの詳細については、を参照してください ["vserver services name-service ns-switch modify"](#) コマンドを実行します

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

- a. S3クライアントでアクセスキーを次の形式で設定します。

"NTAPFASTBIND" + base64-encode(user-name:password)

例 "NTAPFASTBIND" +base64 -エンコード(ldapuser:password)。結果は次のようになります。

NTAPFASTBINDbGRhcHVzZXI6cGFzc3dvcmQ=



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

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

**LDAP**ユーザまたはドメインユーザが自分の**S3**アクセスキーを生成できるようにする

ONTAP 9.14.1以降では、ONTAP管理者がカスタムロールを作成してローカルグループ、ドメイングループ、またはLightweight Directory Access Protocol (LDAP) グループに付与し、それらのグループに属するユーザがS3クライアントアクセス用に独自のアクセスキーとシークレットキーを生成できるようにすることができます。

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

作業を開始する前に

次の点を確認します。

1. S3サーバを含むS3対応Storage VMが作成されている。を参照してください ["S3 用の SVM を作成します"](#)。
2. そのStorage VMにバケットが作成されている。を参照してください ["バケットを作成する"](#)。
3. Storage VMにDNSが設定されています。を参照してください ["DNS サービスを設定する"](#)。
4. LDAPサーバの自己署名ルート認証局 (CA) 証明書がStorage VMにインストールされている。を参照してください ["自己署名ルート CA 証明書を SVM にインストールします"](#)。
5. Storage VMでTLSが有効になっているLDAPクライアントが設定されています。を参照してください ["LDAP クライアント設定を作成します"](#) および。
6. クライアント設定をSVMに関連付けます。を参照してください ["LDAP クライアント設定を SVM に関連付けます"](#) および ["vserver services name-service ldap createを使用して"](#)。
7. データStorage VMを使用している場合は、管理ネットワークインターフェイス (LIF) とVM上に、LIFのサービスポリシーを作成します。を参照してください ["ネットワークインターフェイスの作成"](#) および ["network interface service-policy createを実行します"](#) コマンド

アクセスキー生成のためのユーザの設定

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

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

このコマンドの詳細については、を参照してください ["vserver services name-service ns-switch modify"](#) コマンドを実行します

2. S3ユーザREST APIエンドポイントへのアクセスを含むカスタムロールを作成します。

```
security login rest-role create -vserver <vserver-name> -role <custom-role-
name> -api "/api/protocols/s3/services/*/users" -access <access-type>
```

この例では、を使用しています s3-role Storage VMのユーザ用にロールが生成されました `svm-1` をクリックします。読み取り、作成、更新のすべてのアクセス権が付与されます。

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

このコマンドの詳細については、を参照してください ["security login rest -role create"](#) コマンドを実行します

3. security login コマンドを使用してLDAPユーザグループを作成し、S3ユーザREST APIエンドポイントにアクセスするための新しいカスタムロールを追加します。このコマンドの詳細については、を参照してください ["security login create を実行します"](#) コマンドを実行します

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

この例では、LDAPグループ ldap-group-1 が作成された場所 svm-1、およびカスタムロール s3role APIエンドポイントにアクセスするために追加され、高速バインドモードでLDAPアクセスを有効にします。

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

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

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

**S3**ユーザまたは**LDAP**ユーザとして、独自のアクセスキーを生成

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

**HTTP**メソッドとエンドポイント

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

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

カールの例

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

## JSON 出力例

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

## S3 オブジェクトストレージへのクライアントアクセスを有効にします

リモートの **FabricPool** 階層化のために **ONTAP S3** アクセスを有効にします

FabricPool S3 をリモートの ONTAP 大容量（クラウド）階層として使用するには、ONTAP S3 管理者が S3 サーバの設定に関する情報をリモートの ONTAP クラスタ管理者に提供する必要があります。

このタスクについて

FabricPool クラウド階層を設定するには、次の S3 サーバ情報が必要です。

- サーバ名（FQDN）
- バケット名
- CA 証明書
- アクセスキー
- パスワード（シークレットアクセスキー）

さらに、次のネットワーク設定が必要です。

- 管理 SVM 用に設定された DNS サーバ内のリモート ONTAP S3 サーバのホスト名のエントリに、S3 サ

ーバの FQDN 名と LIF の IP アドレスが含まれている必要があります。

- クラスタピアリングは必要ありませんが、ローカルクラスタにクラスタ間LIFを設定する必要があります。

ONTAP S3 をクラウド階層として設定する方法については、FabricPool のドキュメントを参照してください。

## "FabricPool を使用したストレージ階層の管理"

ローカルの **FabricPool** 階層化のために **ONTAP S3** アクセスを有効にします

ONTAP S3 をローカルの FabricPool 大容量階層として使用するには、作成したバケットに基づいてオブジェクトストアを定義し、パフォーマンス階層のアグリゲートにオブジェクトストアを接続して FabricPool を作成する必要があります。

作業を開始する前に

ONTAP S3サーバ名とバケット名を確認し、（と）クラスタLIFを使用してS3サーバを作成しておく必要があります `-vserver Cluster` パラメータ）。

このタスクについて

オブジェクトストアの設定には、S3 サーバとバケットの名前や認証要件など、ローカルの大容量階層の情報が含まれています。

作成したオブジェクトストア設定は、別のオブジェクトストアまたはバケットに再関連付けしないでください。ローカル階層には複数のバケットを作成できますが、1つのバケットに複数のオブジェクトストアを作成することはできません。

ローカルの大容量階層には FabricPool ライセンスは必要ありません。

手順

1. ローカルの大容量階層用のオブジェクトストアを作成します。

```
storage aggregate object-store config create -object-store-name store_name
-ipospace Cluster -provider-type ONTAP_S3 -server S3_server_name -container
-name bucket_name -access-key access_key -secret-password password
```

- 。 `-container-name` は、作成したS3バケットです。
- 。 `-access-key` パラメータは、ONTAP S3サーバへの要求を承認します。
- 。 `-secret-password` パラメータ（シークレットアクセスキー）は、ONTAP S3サーバへの要求を認証します。
- を設定できます `-is-certificate-validation-enabled` パラメータの値 `false` をクリックしてONTAP S3の証明書のチェックを無効にします。

```
cluster1::> storage aggregate object-store config create
-object-store-name MyLocalObjStore -ipospace Cluster -provider-type
ONTAP_S3 -server s3.example.com
-container-name bucket1 -access-key myS3key -secret-password myS3pass
```

- オブジェクトストアの設定情報を表示して確認します。

```
storage aggregate object-store config show
```

- オプション：ボリューム内のアクセス頻度の低いデータの量を確認するには、の手順に従います ["Inactive Data Reporting によるボリューム内のアクセス頻度の低いデータ量の確認"](#)。

ボリューム内のアクセス頻度の低いデータの量を確認すると、FabricPool のローカル階層化にどのアグリゲートを使用するかを決定するのに役立ちます。

- オブジェクトストアをアグリゲートに接続します。

```
storage aggregate object-store attach -aggregate aggr_name -object-store-name store_name
```

を使用できます `allow-flexgroup true` FlexGroup ボリュームのコンスティチュエントを含むアグリゲートを接続するオプション。

```
cluster1::> storage aggregate object-store attach
-aggregate aggr1 -object-store-name MyLocalObjStore
```

- オブジェクトストアの情報を表示し、接続したオブジェクトストアが使用可能であることを確認します。

```
storage aggregate object-store show
```

```
cluster1::> storage aggregate object-store show
```

Aggregate	Object Store Name	Availability State
-----	-----	-----
aggr1	MyLocalObjStore	available

## S3 アプリケーションからのクライアントアクセスを有効にします

S3 クライアントアプリケーションが ONTAP S3 サーバにアクセスするためには、ONTAP S3 管理者が S3 ユーザに設定情報を指定する必要があります。

作業を開始する前に

S3クライアントアプリケーションが、次のAWS署名バージョンを使用してONTAP S3サーバで認証する必要があります。

- 署名バージョン4、ONTAP 9.8以降
- シグニチャバージョン2、ONTAP 9.11.1以降

それ以外のシグニチャバージョンは、ONTAP S3でサポートされていません。

ONTAP S3 管理者は、S3 ユーザを作成し、個々のユーザまたはグループメンバーとして、バケットポリシーまたはオブジェクトストレージサーバポリシーでアクセス権限を付与しておく必要があります。

S3 クライアントアプリケーションで ONTAP S3 サーバ名を解決できる必要があります。そのためには、ONTAP S3 管理者が S3 サーバの LIF の S3 サーバ名（FQDN）と IP アドレスを指定する必要があります。

このタスクについて

ONTAP S3 バケットにアクセスするには、S3 クライアントアプリケーションのユーザが ONTAP S3 管理者から提供された情報を入力します。

ONTAP 9.9.1以降では、ONTAP S3サーバで次のAWSクライアント機能がサポートされます。

- ユーザ定義のオブジェクトメタデータ

キーと値のペアのセットは、PUT（または POST）を使用してオブジェクトを作成するときに、メタデータとして割り当てることができます。オブジェクトに対して GET / HEAD 処理が実行されると、システムメタデータとともにユーザ定義のメタデータが返されます。

- オブジェクトのタグ付け

キーと値のペアのセットは、オブジェクトを分類するためのタグとして個別に割り当てることができます。メタデータとは異なり、タグは REST API でオブジェクトから独立して作成および読み取りされ、オブジェクトの作成時または作成後にいつでも実装されます。



クライアントがタグ情報を取得および取得できるようにするには、アクションを実行します `GetObjectTagging`、`PutObjectTagging` および `DeleteObjectTagging` バケットまたはグループポリシーを使用して許可されている必要があります。

詳細については、AWS S3 のドキュメントを参照してください。

手順

1. S3 サーバ名と CA 証明書を入力して、S3 クライアントアプリケーションを ONTAP S3 サーバで認証します。
2. 次の情報を入力して、S3 クライアントアプリケーションでユーザを認証します。
  - S3 サーバ名（FQDN）とバケット名
  - ユーザのアクセスキーとシークレットキー

## ストレージサービスの定義

ONTAP には、対応する最小パフォーマンス要因にマッピングされた事前定義されたストレージサービスが含まれています。

クラスタまたは SVM で実際に使用可能なストレージサービスは、SVM 内のアグリゲートを構成するストレージのタイプによって決まります。

次の表に、定義済みのストレージサービスと対応する最小パフォーマンス要因を示します。



ストレージサービス	想定 IOPS （SLA）	最大 IOPS （SLO）	最小ボリューム IOPS	推定レイテンシ	想定 IOPS の適用
価値	TBあたり128	TBあたり512	七五	17 ミリ秒	AFF の場合：はい  それ以外の場合：いいえ
パフォーマンス	TB あたり 2、048	TB あたり 4096	500ドル	2 ミリ秒	はい。
最高レベル	TBあたり6、144	TB あたり 12288 回	1000	1 ミリ秒	はい。

次の表に、メディアまたはノードのタイプごとに使用可能なストレージサービスレベルを示します。

メディアまたはノード	使用可能なストレージサービスレベル
ディスク	価値
仮想マシンディスク	価値
FlexArray LUN の略	価値
ハイブリッド	価値
大容量フラッシュ	価値
ソリッドステートドライブ（SSD） - AFF 以外のドライブです	価値
パフォーマンスが最適化されたフラッシュ - SSD （AFF）	最高レベル、パフォーマンス、バリュー

## S3 SnapMirror でバケットを保護します

### S3 SnapMirror の概要

ONTAP 9.10.1以降では、SnapMirrorのミラーリングとバックアップの機能を使用してONTAP S3オブジェクトストアのバケットを保護できます。標準のSnapMirrorとは異なり、S3 SnapMirrorでは、AWS S3などのネットアップ以外のデスティネーションへのミラーリングとバックアップが可能です。

S3 SnapMirror は、ONTAP S3 バケットから次のデスティネーションへのアクティブなミラー階層とバックアップ階層をサポートしています。

ターゲット	アクティブなミラーとテイクオーバーをサポートしているか	バックアップとリストアをサポートするかどうか
ONTAP S3の略 <ul style="list-style-type: none"> <li>• 同じ SVM 内のバケット</li> <li>• 同一クラスタ上の異なる SVM にあるバケット</li> <li>• 異なるクラスタの SVM のバケット</li> </ul>	✓	✓
StorageGRID		✓
AWS S3		✓
Cloud Volumes ONTAP for Azure	✓	✓
Cloud Volumes ONTAP for AWS	✓	✓
Cloud Volumes ONTAP for Google Cloud の略	✓	✓

ONTAP S3 サーバ上の既存のバケットを保護することも、データ保護をすぐに有効にして新しいバケットを作成することもできます。

### S3 SnapMirror の要件

- ONTAPバージョン  
ソースクラスタとデスティネーションクラスタでONTAP 9.10.1以降が実行されている必要があります。
- ライセンス  
ONTAPのソースシステムとデスティネーションシステムには、次のライセンスバンドルが必要です。
  - Core Bundle  
(ONTAP S3プロトコルおよびストレージ用)。
  - データ保護バンドル  
S3 SnapMirrorの場合、他のNetAppオブジェクトストアターゲット（ONTAP S3、StorageGRID、Cloud Volumes ONTAP）をターゲットにします。
  - Data Protection BundleとHybrid Cloud Bundle  
S3の場合は、AWS S3などのサードパーティのオブジェクトストアをターゲットにします。
- ONTAP S3の略
  - ONTAP S3 サーバでソースとデスティネーションの SVM が実行されている必要があります。
  - TLS アクセス用の CA 証明書は、S3 サーバをホストするシステムにインストールすることを推奨しますが、必須ではありません。
    - S3 サーバの証明書への署名に使用する CA 証明書は、S3 サーバをホストするクラスタの管理 Storage VM にインストールする必要があります。
    - 自己署名 CA 証明書、または外部 CA ベンダーが署名した証明書を使用できます。
    - ソースまたはデスティネーションの Storage VM が HTTPS をリスンしていない場合は、CA 証明書をインストールする必要はありません。
- ピアリング（ONTAP S3 ターゲット用）
  - クラスタ間 LIF が設定されている必要があります（リモート ONTAP ターゲット用）。

- ソースクラスタとデスティネーションクラスタ間にピア関係が設定されている（リモート ONTAP ターゲットの場合）。
- ソースとデスティネーションの Storage VM 間にピア関係が設定されている（すべての ONTAP ターゲット用）。
- SnapMirror ポリシー
  - S3 固有の SnapMirror ポリシーはすべての S3 SnapMirror 関係に必要ですが、複数の関係に同じポリシーを使用することができます。
  - 独自のポリシーを作成するか、次の値を含むデフォルトの \* Continuous \* ポリシーをそのまま使用できます。
    - スロットル（スループット / 帯域幅の上限） - 無制限
    - 目標復旧時点までの時間： 1 時間（ 3600 秒）
- root ユーザーキー  
S3 SnapMirror 関係では Storage VM の root ユーザーアクセスキーが必要です。ONTAP ではデフォルトでは割り当てられません。S3 SnapMirror 関係を初めて作成するときは、ソースとデスティネーションの Storage VM の両方にキーが存在することを確認し、存在しない場合は再生成する必要があります。再生成する必要がある場合は、アクセスキーとシークレットキーのペアを使用するすべてのクライアントおよび SnapMirror オブジェクトストアのすべての設定が新しいキーで更新されていることを確認する必要があります。

S3 サーバの設定については、次のトピックを参照してください。

- ["Storage VM で S3 サーバを有効にします"](#)
- ["S3 の設定プロセスについて"](#)

クラスタと Storage VM のピアリングについては、次のトピックを参照してください。

- ["ミラーとバックアップの準備（ System Manager 、手順 1~6 ）"](#)
- ["クラスタと SVM のピアリング（ CLI ）"](#)

## サポートされる SnapMirror 関係

S3 SnapMirror は、ファンアウト関係とカスケード関係をサポートしています。概要については、[を参照してください "ファンアウト構成およびカスケード構成のデータ保護"](#)。

S3 SnapMirror では、ファンイン環境（複数のソースバケットと1つのデスティネーションバケット間のデータ保護関係）はサポートされません。S3 SnapMirror では、複数のクラスタから単一のセカンダリクラスタへの複数のバケットミラーをサポートできますが、各ソースバケットにはセカンダリクラスタ上に独自のデスティネーションバケットが必要です。

## S3 バケットへのアクセスを制御

新しいバケットを作成するときは、ユーザとグループを作成してアクセスを制御できます。詳細については、[次のトピックを参照してください](#)。

- ["S3 ユーザとグループの追加（ System Manager ）"](#)
- ["S3 ユーザを作成（ CLI ）"](#)
- ["S3 グループの作成または変更（ CLI ）"](#)

## リモートクラスタでのミラーとバックアップの保護

新しいバケットのミラー関係の作成（リモートクラスタ）

新しい S3 バケットを作成する場合、リモートクラスタの S3 SnapMirror デスティネーションですぐに保護することができます。



このタスクについて


タスクはソースシステムとデスティネーションシステムの両方で実行する必要があります。

作業を開始する前に

- ONTAP のバージョン、ライセンス、S3 サーバの設定に関する要件を満たしている必要があります。
- ソースクラスタとデスティネーションクラスタの間にピア関係が存在し、ソース Storage VM とデスティネーション Storage VM の間にピア関係が存在します。
- CA 証明書は、ソース VM とデスティネーション VM に必要です。自己署名 CA 証明書または外部 CA ベンダーが署名した証明書を使用できます。

## System Manager の略

1. この Storage VM の最初の S3 SnapMirror 関係である場合は、ソースとデスティネーションの Storage VM の両方に root ユーザーキーが存在することを確認し、存在しない場合は再生成します。
  - a. Storage > Storage VM\* をクリックし、Storage VM を選択します。
  - b. [\* 設定 \*] タブで、をクリックします  を \* S3 \* タイルに追加します。
  - c. [Users] タブで、root ユーザーのアクセスキーがあることを確認します。
  - d. 表示されていない場合は、をクリックします  アイコン"] [root] の横にある [\*Regenerate Key] をクリックします。  
キーがすでに存在する場合は、キーを再生成しないでください。
2. ソースとデスティネーションの Storage VM の両方で、Storage VM を編集してユーザーを追加し、グループにユーザーを追加します。

Storage > Storage VM\* の順にクリックし、Storage VM をクリックして、\* Settings \* をクリックし、をクリックします  S3 の下。

を参照してください "[S3 ユーザーとグループを追加](#)" を参照してください。

3. ソースクラスタに S3 SnapMirror ポリシーを作成します。これは、既存のポリシーがなく、デフォルトポリシーを使用しない場合に行います。
  - a. [\* 保護]、[概要 \*] の順にクリックし、[ローカルポリシーの設定 \*] をクリックします。
  - b. をクリックします → [\* 保護ポリシー \*] の横にある [\* 追加] をクリックします。
    - ポリシー名と概要を入力します。
    - ポリシーの範囲として、クラスタまたは SVM を選択します
    - S3 SnapMirror 関係には「\* Continuous \*」を選択します。
    - スロットル値および \* 目標復旧時点 \* 値を入力します。
4. SnapMirror 保護を使用してバケットを作成します。
  - a. [\* ストレージ]、[バケット] の順にクリックし、[\* 追加] をクリックします。権限の確認は任意ですが、推奨されます。
  - b. 名前を入力し、Storage VM を選択してサイズを入力し、\* その他のオプション \* をクリックします。
  - c. [Permissions] で、[Add] をクリックします。
    - \* Principal \* および \* Effect \* - ユーザーグループの設定に対応する値を選択するか、デフォルト値をそのまま使用します。
    - アクション-次の値が表示されていることを確認します。

```
GetObject,PutObject,DeleteObject,ListBucket,GetBucketAcl,GetObjectAcl,ListBucketMultipartUploads,ListMultipartUploadParts
```

- リソース-デフォルトを使用します (*bucketname*, *bucketname/\**) または必要なその他の値。

を参照してください ["バケットへのユーザアクセスを管理します"](#) これらのフィールドの詳細については、[を参照してください](#)。

- d. **[Protection]** で、 **[Enable SnapMirror (ONTAP or Cloud)]** をオンにします。次に、次の値を入力します。

- デスティネーション

- \* ターゲット： ONTAP システム \*
- \* cluster \*：リモートクラスタを選択します。
- \* Storage VM \*：リモートクラスタの Storage VM を選択します。
- \* S3 サーバ CA 証明書 \*： \_source\_certificate の内容をコピーして貼り付けます。

- ソース

- \* S3 サーバ CA 証明書： \* destination\_certificate の内容をコピーして貼り付けます。

5. チェック \* 外部 CA ベンダーが署名した証明書を使用している場合は、宛先で同じ証明書を使用します。
6. [\* Destination Settings] をクリックすると、バケット名、容量、およびパフォーマンスサービスレベルのデフォルト値の代わりに独自の値を入力することもできます。
7. [保存 (Save)] をクリックします。ソースStorage VMに新しいバケットが作成され、デスティネーションStorage VMに作成された新しいバケットにミラーリングされます。

#### ロックされたバケットのバックアップ

ONTAP 9.14.1以降では、ロックされたS3バケットをバックアップし、必要に応じてリストアできます。

新規または既存のバケットの保護設定を定義する際に、ソースクラスタとデスティネーションクラスタでONTAP 9.14.1以降を実行し、ソースバケットでオブジェクトのロックが有効になっている場合は、デスティネーションバケットでオブジェクトのロックを有効にすることができます。ソースバケットのオブジェクトロックモードとロックの保持期間が、デスティネーションバケットのレプリケートオブジェクトに適用されるようになります。また、\*[Destination Settings]\*セクションで、デスティネーションバケットに対して別のロック保持期間を定義することもできます。この保持期間は、ソースバケットとS3インターフェイスからレプリケートされたロックされていないオブジェクトにも適用されます。

バケットでオブジェクトロックを有効にする方法については、[を参照してください](#)。 ["バケットを作成する"](#)。

#### CLI の使用

1. この SVM の最初の S3 SnapMirror 関係の場合は、ソースとデスティネーションの両方の SVM に root ユーザキーが存在することを確認し、存在しない場合は再生成します。

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

root ユーザのアクセスキーがあることを確認します。表示されない場合は、次のように入力します。

```
vserver object-store-server user regenerate-keys -vserver svm_name -user root
```

キーがすでに存在する場合は、キーを再生成しないでください。

2. ソースとデスティネーションの両方の SVM でバケットを作成します。

```
vserver object-store-server bucket create -vserver svm_name -bucket
bucket_name [-size integer[KB|MB|GB|TB|PB]] [-comment text]
[additional_options]
```

3. ソースとデスティネーションの両方の SVM で、デフォルトのバケットポリシーにアクセスルールを追加します。

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

例

```
src_cluster::> vserver object-store-server bucket policy add-
statement -bucket test-bucket -effect allow -action
GetObject,PutObject,DeleteObject,ListBucket,GetBucketAcl,GetObjectAc
l,ListBucketMultipartUploads,ListMultipartUploadParts -principal -
-resource test-bucket, test-bucket /*
```

4. 既存のSnapMirrorポリシーがなく、デフォルトポリシーを使用しない場合は、ソースSVMでS3 SnapMirrorポリシーを作成します。

```
snapmirror policy create -vserver svm_name -policy policy_name -type
continuous [-rpo integer] [-throttle throttle_type] [-comment text]
[additional_options]
```

パラメータ

- を入力します continuous - S3 SnapMirror関係の唯一のポリシータイプ（必須）。
- -rpo -目標復旧時点の時間を秒単位で指定します（オプション）。
- -throttle -スループット/帯域幅の上限をキロバイト/秒単位で指定します（オプション）。

例

```
src_cluster::> snapmirror policy create -vserver vs0 -type
continuous -rpo 0 -policy test-policy
```

5. ソースクラスタとデスティネーションクラスタの管理 SVM に CA サーバ証明書をインストールします。
  - a. ソースクラスタで、*destination\_S3*サーバ証明書に署名したCA証明書をインストールします。

```
security certificate install -type server-ca -vserver _src_admin_svm -cert
-name dest_server_certificate
```
  - b. デスティネーションクラスタで、*source\_S3*サーバ証明書に署名したCA証明書をインストールします。

```
security certificate install -type server-ca -vserver _dest_admin_svm
-cert-name src_server_certificate
```

外部の CA ベンダーが署名した証明書を使用している場合は、ソースとデスティネーションの管理 SVM に同じ証明書をインストールします。

を参照してください security certificate install のマニュアルページを参照してください。

#### 6. ソース SVM で、S3 SnapMirror 関係を作成します。

```
snapmirror create -source-path src_svm_name:/bucket/bucket_name  
-destination-path dest_peer_svm_name:/bucket/bucket_name, ...} [-policy  
policy_name]
```

作成したポリシーを使用することも、デフォルトのポリシーをそのまま使用することもできます。

例

```
src_cluster::> snapmirror create -source-path vs0-src:/bucket/test-  
bucket -destination-path vs1-dest:bucket/test-bucket-mirror -policy  
test-policy
```

#### 7. ミラーリングがアクティブであることを確認します。

```
snapmirror show -policy-type continuous -fields status
```

既存のバケットのミラー関係を作成する（リモートクラスタ）

既存の S3 バケットの保護はいつでも開始できます。たとえば、S3 設定を ONTAP 9.10.1 より前のリリースからアップグレードした場合などです。

このタスクについて

タスクはソースクラスタとデスティネーションクラスタの両方で実行する必要があります。

作業を開始する前に





- ONTAP のバージョン、ライセンス、S3 サーバの設定に関する要件を満たしている必要があります。
- ソースクラスタとデスティネーションクラスタの間にピア関係が存在し、ソース Storage VM とデスティネーション Storage VM の間にピア関係が存在します。
- CA 証明書は、ソース VM とデスティネーション VM に必要です。自己署名 CA 証明書または外部 CA ベンダーが署名した証明書を使用できます。

手順

ミラー関係は、System Manager または ONTAP CLI を使用して作成できます。



## System Manager の略

- この Storage VM の最初の S3 SnapMirror 関係である場合は、ソースとデスティネーションの Storage VM の両方に root ユーザキーが存在することを確認し、存在しない場合は再生成します。
  - [ストレージ]>[Storage VM]\*を選択し、Storage VMを選択します。
  - [\* 設定 \*] タブで、をクリックします  を \* S3 \* タイルに追加します。
  - [Users] タブで、root ユーザのアクセスキーがあることを確認します。
  - 表示されていない場合は、をクリックします  アイコン"] の横にある[Regenerate Key]をクリックします。\*  
キーがすでに存在する場合は、キーを再生成しないでください。
- ソースとデスティネーションの Storage VM 両方でユーザおよびグループのアクセスが正しいことを確認します。  
[ストレージ]>[Storage VM]を選択し、**Storage VM**を選択して[設定]\*を選択します。最後に、  \* S3 の下\*。  
  
を参照してください "[S3 ユーザとグループを追加](#)" を参照してください。
- ソースクラスタに S3 SnapMirror ポリシーを作成します。これは、既存のポリシーがなく、デフォルトポリシーを使用しない場合に行います。
  - [保護]>[概要]を選択し、[ローカルポリシー設定]\*をクリックします。
  - 選択するオプション → [\* 保護ポリシー \*] の横にある [\* 追加] をクリックします。
  - ポリシー名と概要を入力します。
  - ポリシーのスコップとして、クラスタまたは SVM を選択します
  - S3 SnapMirror 関係には「\* Continuous \*」を選択します。
  - スロットル値および \* 目標復旧時点 \* 値を入力します。
- 既存のバケットのバケットアクセスポリシーが引き続きニーズを満たしていることを確認します。
  - [\* ストレージ]、[バケット] の順にクリックし、保護するバケットを選択します。
  - [\* アクセス許可] タブで、をクリックします  [\*編集]\*をクリックし、[権限]の[追加]\*をクリックします。
    - \* 主な内容と効果 \* : ユーザーグループの設定に対応する値を選択するか、デフォルト値をそのまま使用します。
    - \* アクション : 次の値が表示されていることを確認します。

```
GetObject, PutObject, DeleteObject, ListBucket, GetBucketAcl, GetObjectAcl, ListBucketMultipartUploads, ListMultipartUploadParts
```

- リソース:デフォルトを使用します (*bucketname*, *bucketname/\**) または必要なその他の値。

を参照してください "[バケットへのユーザアクセスを管理します](#)" これらのフィールドの詳細については、を参照してください。

5. S3 SnapMirror 保護を使用して既存のバケットを保護します。
  - a. [\* ストレージ \*] > [\* バケット \*] をクリックし、保護するバケットを選択します。
  - b. [\* Protect] をクリックして、次の値を入力します。
    - デスティネーション
      - \* ターゲット \* : ONTAP システム
      - \* cluster \* : リモートクラスタを選択します。
      - \* Storage VM \* : リモートクラスタの Storage VM を選択します。
      - \* S3 サーバ CA 証明書 \* : \_source\_certificate の内容をコピーして貼り付けます。
    - ソース
      - \* S3 サーバ CA 証明書 \* : \_destination\_certificate の内容をコピーして貼り付けます。
6. チェック \* 外部 CA ベンダーが署名した証明書を使用している場合は、宛先で同じ証明書を使用します。
7. [\* Destination Settings] をクリックすると、バケット名、容量、およびパフォーマンスサービスレベルのデフォルト値の代わりに独自の値を入力することもできます。
8. [保存 (Save)] をクリックします。既存のバケットがデスティネーション Storage VM の新しいバケットにミラーリングされます。

#### ロックされたバケットのバックアップ

ONTAP 9.14.1以降では、ロックされたS3バケットをバックアップし、必要に応じてリストアできます。

新規または既存のバケットの保護設定を定義する際に、ソースクラスタとデスティネーションクラスタでONTAP 9.14.1以降を実行し、ソースバケットでオブジェクトのロックが有効になっている場合は、デスティネーションバケットでオブジェクトのロックを有効にすることができます。ソースバケットのオブジェクトロックモードとロックの保持期間が、デスティネーションバケットのレプリケートオブジェクトに適用されるようになります。また、\*[Destination Settings]\*セクションで、デスティネーションバケットに対して別のロック保持期間を定義することもできます。この保持期間は、ソースバケットとS3インターフェイスからレプリケートされたロックされていないオブジェクトにも適用されます。

バケットでオブジェクトロックを有効にする方法については、を参照してください。 ["バケットを作成する"](#)。

#### CLI の使用

1. この SVM の最初の S3 SnapMirror 関係の場合は、ソースとデスティネーションの両方の SVM に root ユーザキーが存在することを確認し、存在しない場合は再生成します。

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

[] root ユーザのアクセスキーがあることを確認します。表示されない場合は、次のように入力します。`vserver object-store-server user regenerate-keys -vserver \_svm\_name\_ -user \_root\_` [] キーがすでに存在する場合は、キーを再生成しないでください。

2. ミラーターゲットにするバケットをデスティネーション SVM 上に作成します。

```
vserver object-store-server bucket create -vserver svm_name -bucket dest_bucket_name [-size integer[KB|MB|GB|TB|PB]] [-comment text] [additional_options]
```

3. ソースとデスティネーションの両方のSVMで、デフォルトのバケットポリシーのアクセスルールが正しいことを確認します。

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

例

```
src_cluster::> vserver object-store-server bucket policy add-
statement -bucket test-bucket -effect allow -action
GetObject,PutObject,DeleteObject,ListBucket,GetBucketAcl,GetObjectAc
l,ListBucketMultipartUploads,ListMultipartUploadParts -principal -
-resource test-bucket, test-bucket /*
```

4. ソース SVM に S3 SnapMirror ポリシーを作成します。これは、既存のポリシーがなく、デフォルトポリシーを使用しない場合に行います。

```
snapmirror policy create -vserver svm_name -policy policy_name -type
continuous [-rpo integer] [-throttle throttle_type] [-comment text]
[additional_options]
```

パラメータ

- ° continuous –S3 SnapMirror関係の唯一のポリシータイプ（必須）。
- ° -rpo –目標復旧時点の時間を秒単位で指定します（オプション）。
- ° -throttle –スループット/帯域幅の上限をキロバイト/秒単位で指定します（オプション）。

例

```
src_cluster::> snapmirror policy create -vserver vs0 -type
continuous -rpo 0 -policy test-policy
```

5. ソースクラスタとデスティネーションクラスタの管理 SVM に CA 証明書をインストールします。
  - a. ソースクラスタで、*destination\_S3*サーバ証明書に署名したCA証明書をインストールします。  
`security certificate install -type server-ca -vserver _src_admin_svm -cert -name dest_server_certificate`
  - b. デスティネーションクラスタで、*source\_S3*サーバ証明書に署名したCA証明書をインストールします。  
`security certificate install -type server-ca -vserver _dest_admin_svm -cert-name src_server_certificate`  
[+]  
外部の CA ベンダーが署名した証明書を使用している場合は、ソースとデスティネーションの管理 SVM に同じ証明書をインストールします。

を参照してください `security certificate install` のマニュアルページを参照してください。

6. ソース SVM で、S3 SnapMirror 関係を作成します。

```
snapmirror create -source-path src_svm_name:/bucket/bucket_name  
-destination-path dest_peer_svm_name:/bucket/bucket_name, ...} [-policy  
policy_name]
```

作成したポリシーを使用することも、デフォルトのポリシーをそのまま使用することもできます。

例

```
src_cluster::> snapmirror create -source-path vs0:/bucket/test-  
bucket -destination-path vs1:/bucket/test-bucket-mirror -policy  
test-policy
```

#### 7. ミラーリングがアクティブであることを確認します。

```
snapmirror show -policy-type continuous -fields status
```

デスティネーションバケットからデータをテイクオーバーして提供（リモートクラスタ）

ソースバケットのデータを使用できなくなった場合は、SnapMirror 関係を解除してデスティネーションバケットを書き込み可能にし、データの提供を開始できます。

このタスクについて


テイクオーバー処理が実行されると、ソースバケットが読み取り専用に変換され、元のデスティネーションバケットが読み取り / 書き込みに変換されて S3 SnapMirror 関係が反転されます。

無効にしたソースバケットを再び使用できるようになると、S3 SnapMirror は 2 つのバケットの内容を自動的に再同期します。Volume SnapMirror の導入に必要な場合と同様に、関係を明示的に再同期する必要はありません。

リモートクラスタからテイクオーバー処理を開始する必要があります。

## System Manager の略

使用できないバケットからフェイルオーバーし、データの提供を開始します。

1. 保護 > 関係 \* をクリックし、\* S3 SnapMirror \* を選択します。
2. をクリックします  アイコン] をクリックし、\* フェイルオーバー \* を選択して、\* フェイルオーバー \* をクリックします。

## CLI の使用

1. デスティネーションバケットのフェイルオーバー処理を開始します。  
`snapmirror failover start -destination-path svm_name:/bucket/bucket_name`
2. フェイルオーバー処理のステータスを確認します。  
`snapmirror show -fields status`

### 例

```
dest_cluster::> snapmirror failover start -destination-path  
dest_svm1:/bucket/test-bucket-mirror
```

デスティネーション **Storage VM**（リモートクラスタ）からバケットをリストアする

ソースバケットのデータが失われたり破損したりした場合は、デスティネーションバケットからオブジェクトをリストアすることでデータを再取り込みできます。

### このタスクについて


デスティネーションバケットは既存のバケットまたは新しいバケットにリストアできます。リストア処理のターゲットバケットは、デスティネーションバケットの使用済み論理スペースよりも大きくする必要があります。

既存のバケットを使用する場合は、リストア処理の開始時に空にする必要があります。Restore は、あるバケットを「ロールバック」するのではなく、空のバケットに以前の内容を取り込みます。

リストア処理はリモートクラスタから開始する必要があります。

## System Manager の略

バックアップしたデータをリストアします。

1. 保護 > 関係 \* をクリックし、\* S3 SnapMirror \* を選択します。
2. をクリックします  アイコン] 次に、[\* Restore] を選択します。
3. 「\* ソース \*」で、「\* 既存バケット」(デフォルト) または「\* 新規バケット」を選択します。
  - 既存の Bucket \* (デフォルト) にリストアするには、次の操作を実行します。
    - 既存のバケットを検索するクラスタと Storage VM を選択します。
    - 既存のバケットを選択します。
    - destination\_S3 サーバ CA 証明書の内容をコピーして貼り付けます。
  - 新しいバケットへのリストアを実行するには、次の値を入力します。
    - 新しいバケットをホストするクラスタと Storage VM。
    - 新しいバケットの名前、容量、パフォーマンスサービスレベル。  
を参照してください ["ストレージサービスレベル"](#) を参照してください。
    - destination\_S3 サーバ CA 証明書の内容。
4. 「\* Destination \*」の下にある \_source\_S3 サーバ CA 証明書の内容をコピーして貼り付けます。
5. [保護]、[関係] の順にクリックして、復元の進行状況を監視します。

### ロックされたバケットの復元

ONTAP 9.14.1以降では、ロックされたバケットをバックアップし、必要に応じてリストアできます。

オブジェクトロックされたバケットは、新規または既存のバケットにリストアできます。次のシナリオでは、オブジェクトロックバケットをデスティネーションとして選択できます。

- 新しいバケットにリストア：オブジェクトのロックが有効になっている場合、オブジェクトのロックも有効になっているバケットを作成することで、バケットをリストアできます。ロックされたバケットをリストアすると、元のバケットのオブジェクトロックモードと保持期間がレプリケートされます。新しいバケットに対して別のロック保持期間を定義することもできます。この保持期間は、他のソースからのロックされていないオブジェクトに適用されます。
- 既存のバケットにリストア：オブジェクトロックバケットは、既存のバケットでバージョン管理および同様のオブジェクトロックモードが有効になっていれば、既存のバケットにリストアできます。元のバケットの保持期間が維持されます。
- ロックされていないバケットのリストア：バケットでオブジェクトロックが有効になっていない場合でも、ソースクラスタにあるオブジェクトロックが有効になっているバケットにリストアできます。バケットをリストアすると、ロックされていないオブジェクトがすべてロックされ、デスティネーションバケットの保持モードと保持期間がそれらのオブジェクトに適用されます。

### CLI の使用

1. リストア用の新しいデスティネーションバケットを作成します。詳細については、[を参照してください "新しいバケットのバックアップ関係の作成 \(クラウドターゲット\)"](#)。
2. デスティネーションバケットのリストア処理を開始します。

```
snapmirror restore -source-path svm_name:/bucket/bucket_name -destination  
-path svm_name:/bucket/bucket_name
```

例

```
dest_cluster::> snapmirror restore -source-path src_vs1:/bucket/test-  
bucket -destination-path dest_vs1:/bucket/test-bucket-mirror
```

## ローカルクラスタでのミラー保護とバックアップ保護




新しいバケットのミラー関係の作成（ローカルクラスタ）

新しい S3 バケットを作成すると、そのバケットを同じクラスタ上の S3 SnapMirror デスティネーションですぐに保護することができます。データは、別の Storage VM のバケットまたはソースと同じ Storage VM にミラーリングできます。

作業を開始する前に

- ONTAP のバージョン、ライセンス、S3 サーバの設定に関する要件を満たしている必要があります。
- ソース Storage VM とデスティネーション Storage VM の間にピア関係が存在します。
- CA 証明書は、ソース VM とデスティネーション VM に必要です。自己署名 CA 証明書または外部 CA ベンダーが署名した証明書を使用できます。

## System Manager の略

1. この Storage VM の最初の S3 SnapMirror 関係である場合は、ソースとデスティネーションの Storage VM の両方に root ユーザキーが存在することを確認し、存在しない場合は再生成します。
  - a. Storage > Storage VM\* をクリックし、Storage VM を選択します。
  - b. [\* 設定 \*] タブで、をクリックします  を S3 のタイルに表示します。
  - c. [Users] タブで、root ユーザのアクセスキーがあることを確認します
  - d. 表示されていない場合は、をクリックします  アイコン"] [root] の横にある [\*Regenerate Key] をクリックします。  
キーがすでに存在する場合は、キーを再生成しないでください。
2. ソースとデスティネーションの Storage VM の両方で、Storage VM を編集してユーザを追加し、グループにユーザを追加します。  
Storage > Storage VM\* の順にクリックし、Storage VM をクリックして、\* Settings \* をクリックし、をクリックします  S3 の下。

を参照してください ["S3 ユーザとグループを追加"](#) を参照してください。

3. S3 SnapMirror ポリシーを作成します。これは、既存のポリシーがなく、デフォルトポリシーを使用しない場合に行います。
  - a. [保護]>[概要]をクリックし、[ローカルポリシー設定]\*をクリックします。
  - b. をクリックします → [\* 保護ポリシー \*] の横にある [\* 追加] をクリックします。
    - ポリシー名と概要を入力します。
    - ポリシーのスコープとして、クラスタまたは SVM を選択します
    - S3 SnapMirror 関係には「\* Continuous \*」を選択します。
    - スロットル値および \* 目標復旧時点 \* 値を入力します。
4. SnapMirror 保護を使用してバケットを作成します。
  - a. [\* ストレージ]、[バケット] の順にクリックし、[\* 追加] をクリックします。
  - b. 名前を入力し、Storage VM を選択してサイズを入力し、\* その他のオプション \* をクリックします。
  - c. [Permissions] で、[Add] をクリックします。権限の確認は任意ですが、推奨されます。
    - \* Principal \* および \* Effect \* - ユーザグループの設定に対応する値を選択するか、デフォルト値をそのまま使用します。
    - アクション-次の値が表示されていることを確認します。

```
GetObject, PutObject, DeleteObject, ListBucket, GetBucketAcl, GetObjectAcl, ListBucketMultipartUploads, ListMultipartUploadParts
```

- リソース-デフォルトを使用します (bucketname, bucketname/\*) または必要なその他の値

を参照してください ["バケットへのユーザアクセスを管理します"](#) これらのフィールドの詳細については、を参照してください。



- d. **[Protection]** で、 **[Enable SnapMirror (ONTAP or Cloud)]** をオンにします。次に、次の値を入力します。

- デスティネーション

- \* ターゲット \* : ONTAP システム
- \* cluster \* : ローカルクラスタを選択します。
- \* Storage VM \* : ローカルクラスタのStorage VMを選択します。
- \* S3 サーバ CA 証明書 \* : ソース証明書の内容をコピーして貼り付けます。

- ソース

- \* S3 サーバ CA 証明書 \* : デスティネーション証明書の内容をコピーして貼り付けます。

5. チェック \* 外部 CA ベンダーが署名した証明書を使用している場合は、宛先で同じ証明書を使用します。
6. [\* Destination Settings] をクリックすると、バケット名、容量、およびパフォーマンスサービスレベルのデフォルト値の代わりに独自の値を入力することもできます。
7. [保存 (Save)] をクリックします。ソースStorage VMに新しいバケットが作成され、デスティネーションStorage VMに作成された新しいバケットにミラーリングされます。

#### ロックされたバケットのバックアップ

ONTAP 9.14.1以降では、ロックされたS3バケットをバックアップし、必要に応じてリストアできます。

新規または既存のバケットの保護設定を定義する際に、ソースクラスタとデスティネーションクラスタでONTAP 9.14.1以降を実行し、ソースバケットでオブジェクトのロックが有効になっている場合は、デスティネーションバケットでオブジェクトのロックを有効にすることができます。ソースバケットのオブジェクトロックモードとロックの保持期間が、デスティネーションバケットのレプリケートオブジェクトに適用されるようになります。また、\*[Destination Settings]\*セクションで、デスティネーションバケットに対して別のロック保持期間を定義することもできます。この保持期間は、ソースバケットとS3インターフェイスからレプリケートされたロックされていないオブジェクトにも適用されます。

バケットでオブジェクトロックを有効にする方法については、[を参照してください。"バケットを作成する"](#)。

#### CLI の使用

1. この SVM の最初の S3 SnapMirror 関係の場合は、ソースとデスティネーションの両方の SVM に root ユーザキーが存在することを確認し、存在しない場合は再生成します。

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

root ユーザのアクセスキーがあることを確認します。表示されない場合は、次のように入力します。

```
vserver object-store-server user regenerate-keys -vserver svm_name -user root
```

キーがすでに存在する場合は、キーを再生成しないでください。

2. ソースとデスティネーションの両方の SVM でバケットを作成します。

```
vserver object-store-server bucket create -vserver svm_name -bucket bucket_name [-size integer[KB|MB|GB|TB|PB]] [-comment text] [additional_options]
```

3. ソースとデスティネーションの両方の SVM で、デフォルトのバケットポリシーにアクセスルールを追加します。

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

```
src_cluster::> vserver object-store-server bucket policy add-
statement -bucket test-bucket -effect allow -action
GetObject,PutObject,DeleteObject,ListBucket,GetBucketAcl,GetObjectAc
l,ListBucketMultipartUploads,ListMultipartUploadParts -principal -
-resource test-bucket, test-bucket /*
```

4. S3 SnapMirror ポリシーを作成します。これは、既存のポリシーがなく、デフォルトポリシーを使用しない場合に行います。

```
snapmirror policy create -vserver svm_name -policy policy_name -type
continuous [-rpo integer] [-throttle throttle_type] [-comment text]
[additional_options]
```

#### パラメータ

- continuous –S3 SnapMirror関係の唯一のポリシータイプ（必須）。
- -rpo –目標復旧時点の時間を秒単位で指定します（オプション）。
- -throttle –スループット/帯域幅の上限をキロバイト/秒単位で指定します（オプション）。

#### 例

```
src_cluster::> snapmirror policy create -vserver vs0 -type
continuous -rpo 0 -policy test-policy
```

5. 管理 SVM に CA サーバ証明書をインストールします。

- a. *source\_S3*サーバの証明書に署名したCA証明書を管理SVMにインストールします。  
`security certificate install -type server-ca -vserver _admin_svm -cert`  
`-name src_server_certificate`

- b. *destination\_S3*サーバの証明書に署名したCA証明書を管理SVMにインストールします。  
`security certificate install -type server-ca -vserver _admin_svm -cert`  
`-name dest_server_certificate`

[+]

外部のCAベンダーによって署名された証明書を使用している場合は、管理SVMにこの証明書をインストールするだけで済みます。

を参照してください `security certificate install` のマニュアルページを参照してください。

6. S3 SnapMirror関係を作成します。

```
snapmirror create -source-path src_svm_name:/bucket/bucket_name
```

```
-destination-path dest_peer_svm_name:/bucket/bucket_name, ...} [-policy policy_name]`
```

作成したポリシーを使用することも、デフォルトのポリシーをそのまま使用することもできます。

```
src_cluster::> snapmirror create -source-path vs0-src:/bucket/test-bucket -destination-path vs1-dest:/vs1/bucket/test-bucket-mirror -policy test-policy
```

7. ミラーリングがアクティブであることを確認します。

```
snapmirror show -policy-type continuous -fields status
```




既存のバケットのミラー関係を作成する（ローカルクラスタ）

同じクラスタ上の既存の S3 バケットの保護はいつでも開始できます。たとえば、S3 設定を ONTAP 9.10.1 より前のリリースからアップグレードした場合などです。データは、別の Storage VM のバケットまたはソースと同じ Storage VM にミラーリングできます。


作業を開始する前に

- ONTAP のバージョン、ライセンス、S3 サーバの設定に関する要件を満たしている必要があります。
- ソース Storage VM とデスティネーション Storage VM の間にピア関係が存在します。
- CA 証明書は、ソース VM とデスティネーション VM に必要です。自己署名 CA 証明書または外部 CA ベンダーが署名した証明書を使用できます。

## System Manager の略

1. この Storage VM の最初の S3 SnapMirror 関係である場合は、ソースとデスティネーションの Storage VM の両方に root ユーザーキーが存在することを確認し、存在しない場合は再生成します。
  - a. Storage > Storage VM\* をクリックし、Storage VM を選択します。
  - b. [\* 設定 \*] タブで、をクリックします  を \* S3 \* タイルに追加します。
  - c. [Users] タブで、root ユーザーのアクセスキーがあることを確認します。
  - d. 表示されていない場合は、をクリックします  アイコン"] [root] の横にある [\*Regenerate Key] をクリックします。  
キーがすでに存在する場合は、キーを再生成しないでください
2. ソースとデスティネーションの Storage VM 両方でユーザーおよびグループのアクセスが正しいことを確認します。
  - Storage > Storage VM\* の順にクリックし、Storage VM をクリックして、\* Settings \* をクリックし、をクリックします  S3 の下。

を参照してください "[S3 ユーザーとグループを追加](#)" を参照してください。

3. S3 SnapMirror ポリシーを作成します。これは、既存のポリシーがなく、デフォルトポリシーを使用しない場合に行います。
  - a. [\* 保護]、[概要 \*] の順にクリックし、[ローカルポリシーの設定 \*] をクリックします。
  - b. をクリックします → [\* 保護ポリシー \*] の横にある [\* 追加] をクリックします。
    - ポリシー名と概要を入力します。
    - ポリシーの範囲として、クラスターまたは SVM を選択します
    - S3 SnapMirror 関係には「\* Continuous \*」を選択します。
    - スロットル値および \* 目標復旧時点 \* 値を入力します。
4. 既存のバケットのバケットアクセスポリシーが引き続きニーズを満たしていることを確認します。
  - a. [\* ストレージ]、[バケット] の順にクリックし、保護するバケットを選択します。
  - b. [\* アクセス許可 \*] タブで、をクリックします  \* 編集 \* をクリックし、\* 権限 \* の下の \* 追加 \* をクリックします。
    - \* Principal \* および \* Effect \* - ユーザーグループの設定に対応する値を選択するか、デフォルト値をそのまま使用します。
    - アクション-次の値が表示されていることを確認します。

```
GetObject, PutObject, DeleteObject, ListBucket, GetBucketAcl, GetObjectAcl, ListBucketMultipartUploads, ListMultipartUploadParts
```

- リソース-デフォルトを使用します (*bucketname*, *bucketname/\**) または必要なその他の値。

を参照してください "[バケットへのユーザーアクセスを管理します](#)" これらのフィールドの詳細については、を参照してください。

5. S3 SnapMirror を使用して既存のバケットを保護します。
  - a. [\* Storage \* > \* Buckets] をクリックして、保護するバケットを選択します。
  - b. [\*Protect] をクリックして、次の値を入力します。
    - デスティネーション
      - \* ターゲット \* : ONTAP システム
      - \* cluster \* : ローカルクラスタを選択します。
      - \* Storage VM \* : 同じ Storage VM または別の Storage VM を選択します。
      - \* S3 サーバ CA 証明書 \* : \_source\_certificate の内容をコピーして貼り付けます。
    - ソース
      - \* S3 サーバ CA 証明書 \* : \_destination\_certificate の内容をコピーして貼り付けます。
6. チェック \* 外部 CA ベンダーが署名した証明書を使用している場合は、宛先で同じ証明書を使用します。
7. [\* Destination Settings] をクリックすると、バケット名、容量、およびパフォーマンスサービスレベルのデフォルト値の代わりに独自の値を入力することもできます。
8. [保存 (Save)] をクリックします。既存のバケットがデスティネーションStorage VMの新しいバケットにミラーリングされます。

#### ロックされたバケットのバックアップ

ONTAP 9.14.1以降では、ロックされたS3バケットをバックアップし、必要に応じてリストアできます。

新規または既存のバケットの保護設定を定義する際に、ソースクラスタとデスティネーションクラスタでONTAP 9.14.1以降を実行し、ソースバケットでオブジェクトのロックが有効になっている場合は、デスティネーションバケットでオブジェクトのロックを有効にすることができます。ソースバケットのオブジェクトロックモードとロックの保持期間が、デスティネーションバケットのレプリケートオブジェクトに適用されるようになります。また、\*[Destination Settings]\*セクションで、デスティネーションバケットに対して別のロック保持期間を定義することもできます。この保持期間は、ソースバケットとS3インターフェイスからレプリケートされたロックされていないオブジェクトにも適用されます。

バケットでオブジェクトロックを有効にする方法については、を参照してください。 ["バケットを作成する"](#)。

#### CLI の使用

1. この SVM の最初の S3 SnapMirror 関係の場合は、ソースとデスティネーションの両方の SVM に root ユーザーキーが存在することを確認し、存在しない場合は再生成します。

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

root ユーザーのアクセスキーがあることを確認します。表示されない場合は、次のように入力します。

```
vserver object-store-server user regenerate-keys -vserver svm_name -user root
```

キーがすでに存在する場合は、キーを再生成しないでください。

2. ミラーターゲットにするバケットをデスティネーション SVM 上に作成します。

```
vserver object-store-server bucket create -vserver svm_name -bucket dest_bucket_name [-size integer[KB|MB|GB|TB|PB]] [-comment text]
```

[*additional\_options*]

3. ソースとデスティネーションの両方の SVM で、デフォルトのバケットポリシーに対するアクセスルールが正しいことを確認します。

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

例

```
clusterA::> vserver object-store-server bucket policy add-statement
-bucket test-bucket -effect allow -action
GetObject,PutObject,DeleteObject,ListBucket,GetBucketAcl,GetObjectAc
l,ListBucketMultipartUploads,ListMultipartUploadParts -principal -
-resource test-bucket, test-bucket /*
```

4. S3 SnapMirror ポリシーを作成します。これは、既存のポリシーがなく、デフォルトポリシーを使用しない場合に行います。

```
snapmirror policy create -vserver svm_name -policy policy_name -type
continuous [-rpo _integer] [-throttle throttle_type] [-comment text]
[additional_options]
```

パラメータ

- *continuous* –S3 SnapMirror関係の唯一のポリシータイプ（必須）。
- *-rpo* –目標復旧時点の時間を秒単位で指定します（オプション）。
- *-throttle* –スループット/帯域幅の上限をキロバイト/秒単位で指定します（オプション）。

例

```
clusterA::> snapmirror policy create -vserver vs0 -type
continuous -rpo 0 -policy test-policy
```

5. 管理 SVM に CA サーバ証明書をインストールします。

- a. *source\_S3*サーバの証明書に署名したCA証明書を管理SVMにインストールします。  
*security certificate install -type server-ca -vserver \_admin\_svm -cert*  
*-name src\_server\_certificate*

- b. *destination\_S3*サーバの証明書に署名したCA証明書を管理SVMにインストールします。  
*security certificate install -type server-ca -vserver \_admin\_svm -cert*  
*-name dest\_server\_certificate*

[+]

外部のCAベンダーによって署名された証明書を使用している場合は、管理SVMにこの証明書をインストールするだけで済みます。

を参照してください *security certificate install* のマニュアルページを参照してください

い。

#### 6. S3 SnapMirror関係を作成します。

```
snapmirror create -source-path src_svm_name:/bucket/bucket_name  
-destination-path dest_peer_svm_name:/bucket/bucket_name, ...} [-policy  
policy_name]
```

作成したポリシーを使用することも、デフォルトのポリシーをそのまま使用することもできます。

例

```
src_cluster::> snapmirror create -source-path vs0-src:/bucket/test-  
bucket -destination-path vs1-dest:/bucket/test-bucket-mirror -policy  
test-policy
```

#### 7. ミラーリングがアクティブであることを確認します。

```
snapmirror show -policy-type continuous -fields status
```

デスティネーションバケットからテイクオーバーしてデータを提供（ローカルクラスタ）

ソースバケットのデータを使用できなくなった場合は、SnapMirror 関係を解除してデスティネーションバケットを書き込み可能にし、データの提供を開始できます。

このタスクについて


テイクオーバー処理が実行されると、ソースバケットが読み取り専用に変換され、元のデスティネーションバケットが読み取り / 書き込みに変換されて S3 SnapMirror 関係が反転されます。

無効にしたソースバケットを再び使用できるようになると、S3 SnapMirror は 2 つのバケットの内容を自動的に再同期します。Volume SnapMirror の標準的な導入の場合と同様に、関係を明示的に再同期する必要はありません。

デスティネーションバケットがリモートクラスタにある場合は、リモートクラスタからテイクオーバー処理を開始する必要があります。

## System Manager の略

使用できないバケットからフェイルオーバーし、データの提供を開始します。

1. 保護 > 関係 \* をクリックし、\* S3 SnapMirror \* を選択します。
2. をクリックします  アイコン] をクリックし、\* フェイルオーバー \* を選択して、\* フェイルオーバー \* をクリックします。

## CLI の使用

1. デスティネーションバケットのフェイルオーバー処理を開始します。  
`snapmirror failover start -destination-path svm_name:/bucket/bucket_name`
2. フェイルオーバー処理のステータスを確認します。  
`snapmirror show -fields status`

## 例

```
clusterA::> snapmirror failover start -destination-path vs1:/bucket/test-bucket-mirror
```

デスティネーション**Storage VM**（ローカルクラスタ）からバケットをリストアする

ソースバケットのデータが失われたり破損したりした場合は、デスティネーションバケットからオブジェクトをリストアすることでデータを再取り込みできます。

## このタスクについて

デスティネーションバケットは既存のバケットまたは新しいバケットにリストアできます。リストア処理のターゲットバケットは、デスティネーションバケットの使用済み論理スペースよりも大きくする必要があります。


既存のバケットを使用する場合は、リストア処理の開始時に空にする必要があります。Restore は、あるバケットを「ロールバック」するのではなく、空のバケットに以前の内容を取り込みます。

リストア処理はローカルクラスタから開始する必要があります。



## System Manager の略

バックアップデータをリストアします。

1. [ \* 保護 ]、[ 関係 ] の順にクリックし、バケットを選択します。
2. をクリックします  アイコン] 次に、[ \* Restore ] を選択します。
3. 「 \* ソース \* 」で、「 \* 既存バケット」 (デフォルト) または「 \* 新規バケット」を選択します。
  - 既存の Bucket \* (デフォルト) にリストアするには、次の操作を実行します。
    - 既存のバケットを検索するクラスタと Storage VM を選択します。
    - 既存のバケットを選択します。
4. デスティネーション S3 サーバ CA 証明書の内容をコピーして貼り付けます。
  - 新しいバケットへのリストアを実行するには、次の値を入力します。
    - 新しいバケットをホストするクラスタと Storage VM。
    - 新しいバケットの名前、容量、パフォーマンスサービスレベル。  
を参照してください ["ストレージサービスレベル"](#) を参照してください。
    - デスティネーション S3 サーバ CA 証明書の内容。
5. 「 \* Destination \* 」の下にあるソース S3 サーバ CA 証明書の内容をコピーして貼り付けます。
6. [ \* 保護 \* ] > [ 関係 ] の順にクリックして、リストアの進行状況を監視します。

### ロックされたバケットの復元

ONTAP 9.14.1以降では、ロックされたバケットをバックアップし、必要に応じてリストアできます。

オブジェクトロックされたバケットは、新規または既存のバケットにリストアできます。次のシナリオでは、オブジェクトロックバケットをデスティネーションとして選択できます。

- 新しいバケットにリストア：オブジェクトのロックが有効になっている場合、オブジェクトのロックも有効になっているバケットを作成することで、バケットをリストアできます。ロックされたバケットをリストアすると、元のバケットのオブジェクトロックモードと保持期間がレプリケートされます。新しいバケットに対して別のロック保持期間を定義することもできます。この保持期間は、他のソースからのロックされていないオブジェクトに適用されます。
- 既存のバケットにリストア：オブジェクトロックバケットは、既存のバケットでバージョン管理および同様のオブジェクトロックモードが有効になっていれば、既存のバケットにリストアできます。元のバケットの保持期間が維持されます。
- ロックされていないバケットのリストア：バケットでオブジェクトロックが有効になっていない場合でも、ソースクラスタにあるオブジェクトロックが有効になっているバケットにリストアできます。バケットをリストアすると、ロックされていないオブジェクトがすべてロックされ、デスティネーションバケットの保持モードと保持期間がそれらのオブジェクトに適用されます。

### CLI の使用

1. オブジェクトを新しいバケットにリストアする場合は、新しいバケットを作成します。詳細については、[を参照してください "新しいバケットのバックアップ関係の作成 \(クラウドターゲット\)"](#)。
2. デスティネーションバケットのリストア処理を開始します。

```
snapmirror restore -source-path svm_name:/bucket/bucket_name -destination  
-path svm_name:/bucket/bucket_name
```

例

```
clusterA::> snapmirror restore -source-path vs0:/bucket/test-bucket  
-destination-path vs1:/bucket/test-bucket-mirror
```

## クラウドターゲットを使用したバックアップ保護

### クラウドターゲットの関係の要件

ソースとターゲットの環境が、クラウドターゲットに対する S3 SnapMirror バックアップ保護の要件を満たしていることを確認します。

データバケットにアクセスするには、オブジェクトストアプロバイダとの有効なアカウントクレデンシャルが必要です。

クラスタをクラウドオブジェクトストアに接続するためには、クラスタ間ネットワークインターフェイスと IPspace がクラスタに設定されている必要があります。ローカルストレージからクラウドオブジェクトストアにデータをシームレスに転送するには、各ノードにクラスタネットワークインターフェイスを作成してください。

StorageGRID ターゲットの場合は、次の情報を確認しておく必要があります。

- サーバ名。完全修飾ドメイン名（FQDN）または IP アドレスで表されます
- バケット名。バケットはすでに存在する必要があります
- アクセスキー
- シークレットキー

また、StorageGRID サーバ証明書への署名に使用したCA証明書が、を使用してONTAP S3クラスタの管理Storage VMにインストールされている必要があります `security certificate install command`。詳細については、を参照してください ["CA 証明書をインストールしています"](#) StorageGRID を使用する場合。

AWS S3 ターゲットの場合は、次の情報を確認しておく必要があります。

- サーバ名。完全修飾ドメイン名（FQDN）または IP アドレスで表されます
- バケット名。バケットはすでに存在する必要があります
- アクセスキー
- シークレットキー

ONTAP クラスタの管理 Storage VM 用の DNS サーバは、FQDN（使用する場合）を IP アドレスに解決する必要があります。

### 新しいバケットのバックアップ関係の作成（クラウドターゲット）


新しいS3バケットを作成すると、オブジェクトストアプロバイダ（StorageGRIDシステムまたはAmazon S3環境）上のS3 SnapMirrorターゲットバケットにすぐにバックアップ

できます。

作業を開始する前に

- オブジェクトストアプロバイダの有効なアカウントクレデンシャルと設定情報が必要です。
- ソースシステムにクラスタ間ネットワークインターフェイスと IPspace が設定されている。
- ソースStorage VMのDNS設定で、ターゲットのFQDNを解決できる必要があります。

## System Manager の略

1. Storage VM を編集してユーザを追加し、グループにユーザを追加します。
  - a. Storage > Storage VM\* の順にクリックし、Storage VM をクリックして、\* Settings \* をクリックし、をクリックします  \* S3 の下 \*。  
  
を参照してください ["S3 ユーザとグループを追加"](#) を参照してください。
2. ソースシステムに Cloud Object Store を追加します。
  - a. [ 保護 ( Protection ) ] > [ 概要 ( Overview ) ] \* をクリックし、[ クラウドオブジェクトストア ( Cloud Object Stores ) ] を
  - b. [ \* 追加 ] をクリックし、[ \* Amazon S3 \* ] または [ \* StorageGRID \* ] を選択します。
  - c. 次の値を入力します。
    - クラウドオブジェクトストアの名前
    - URL 形式 (パスまたは仮想ホスト)
    - Storage VM ( S3 に対して有効)
    - オブジェクトストアサーバ名 ( FQDN )
    - オブジェクトストアの証明書
    - アクセスキー
    - シークレットキー
    - コンテナ (バケット) 名
3. S3 SnapMirror ポリシーを作成します。これは、既存のポリシーがなく、デフォルトポリシーを使用しない場合に行います。
  - a. [ \* 保護 ]、[ 概要 \* ] の順にクリックし、[ ローカルポリシーの設定 \* ] をクリックします。
  - b. をクリックします → [ \* 保護ポリシー \* ] の横にある [ \* 追加 ] をクリックします。
    - ポリシー名と概要を入力します。
    - ポリシーの範囲として、クラスタまたは SVM を選択します
    - S3 SnapMirror 関係には「 \* Continuous \* 」を選択します。
    - スロットル値および \* 目標復旧時点 \* 値を入力します。
4. SnapMirror 保護を使用してバケットを作成します。
  - a. [ \* ストレージ ]、[ バケット ] の順にクリックし、[ \* 追加 ] をクリックします。
  - b. 名前を入力し、Storage VM を選択してサイズを入力し、\* その他のオプション \* をクリックします。
  - c. [Permissions] で、[Add] をクリックします。権限の確認は任意ですが、推奨されます。
    - \* Principal \* および \* Effect \* - ユーザグループの設定に対応する値を選択するか、デフォルト値をそのまま使用します。
    - アクション-次の値が表示されていることを確認します。

```
`GetObject,PutObject,DeleteObject,ListBucket,GetBucketAcl,GetObjectAcl,ListBucketMultipartUploads,ListMultipartUploadParts`
```

- ・ リソース-デフォルトを使用します `_(bucketname, bucketname/*)` または必要なその他の値。

を参照してください ["バケットへのユーザアクセスを管理します"](#) これらのフィールドの詳細については、[を参照してください](#)。

- d. `[* 保護*]` で、`[* SnapMirror ( ONTAP またはクラウド) を有効にする*]` をオンにし、`[* クラウドストレージ*]` を選択して、`[* クラウドオブジェクトストア*]` を選択します。

[Save] をクリックすると、ソース Storage VM に新しいバケットが作成され、クラウドオブジェクトストアにバックアップされます。

## CLI の使用

1. この SVM の最初の S3 SnapMirror 関係の場合は、ソースとデスティネーションの両方の SVM に root ユーザキーが存在することを確認し、存在しない場合は再生成します。

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

[] rootユーザのアクセスキーがあることを確認します。表示されない場合は、次のように入力します。`vserver object-store-server user regenerate-keys -vserver svm\_name -user \_root\_` [] キーがすでに存在する場合は、キーを再生成しないでください。

2. ソースSVMにバケットを作成します。

```
vserver object-store-server bucket create -vserver svm_name -bucket  
bucket_name [-size integer[KB|MB|GB|TB|PB]] [-comment text]  
[additional_options]
```

3. デフォルトのバケットポリシーにアクセスルールを追加します。

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

## 例

```
clusterA::> vserver object-store-server bucket policy add-statement  
-bucket test-bucket -effect allow -action  
GetObject,PutObject,DeleteObject,ListBucket,GetBucketAcl,GetObjectAcl,  
ListBucketMultipartUploads,ListMultipartUploadParts -principal -  
-resource test-bucket, test-bucket /*
```

4. S3 SnapMirror ポリシーを作成します。これは、既存のポリシーがなく、デフォルトポリシーを使用しない場合に行います。

```
snapmirror policy create -vserver svm_name -policy policy_name -type  
continuous [-rpo integer] [-throttle throttle_type] [-comment text]  
[additional_options]
```

## パラメータ

\* type continuous –S3 SnapMirror関係の唯一のポリシータイプ（必須）。

- \* `-rpo` -目標復旧時点の時間を秒単位で指定します（オプション）。
- \* `-throttle` -スループット/帯域幅の上限をキロバイト/秒単位で指定します（オプション）。

例

```
clusterA::> snapmirror policy create -vserver vs0 -type continuous
-rpo 0 -policy test-policy
```

- ターゲットがStorageGRID システムの場合は、ソースクラスタの管理SVMにStorageGRID CAサーバ証明書をインストールします。

```
security certificate install -type server-ca -vserver src_admin_svm -cert
-name storage_grid_server_certificate
```

を参照してください `security certificate install` のマニュアルページを参照してください。

- S3 SnapMirrorデスティネーションオブジェクトストアを定義します。

```
snapmirror object-store config create -vserver svm_name -object-store-name
target_store_name -usage data -provider-type {AWS_S3|SGWS} -server
target_FQDN -container-name remote_bucket_name -is-ssl-enabled true -port
port_number -access-key target_access_key -secret-password
target_secret_key
```

パラメータ

- \* `-object-store-name` -ローカルONTAP システム上のオブジェクトストアターゲットの名前。
- \* `-usage` -使用します `data` をクリックします。
- \* `-provider-type` -AWS\_S3 および SGWS（StorageGRID）ターゲットがサポートされます。
- \* `-server` -ターゲットサーバのFQDNまたはIPアドレス。
- \* `-is-ssl-enabled` -SSLの有効化はオプションですが、推奨されます。

[+]

を参照してください `snapmirror object-store config create` のマニュアルページを参照してください。

例

```
src_cluster::> snapmirror object-store config create -vserver vs0
-object-store-name sgws-store -usage data -provider-type SGWS
-server sgws.example.com -container-name target-test-bucket -is-ssl
-enabled true -port 443 -access-key abc123 -secret-password xyz890
```

- S3 SnapMirror関係を作成します。

```
snapmirror create -source-path svm_name:/bucket/bucket_name -destination
-path object_store_name:/objstore -policy policy_name
```

パラメータ

- \* `-destination-path` -前の手順で作成したオブジェクトストアの名前と固定値 `objstore`。

[+]

作成したポリシーを使用することも、デフォルトのポリシーをそのまま使用することもできます。

例

```
src_cluster::> snapmirror create -source-path vs0:/bucket/test-  
bucket -destination-path sgws-store:/objstore -policy test-policy
```

8. ミラーリングがアクティブであることを確認します。

```
snapmirror show -policy-type continuous -fields status
```




既存のバケットのバックアップ関係の作成（クラウドターゲット）

既存の S3 バケットのバックアップはいつでも開始できます。たとえば、ONTAP 9.10.1 よりも前のリリースから S3 設定をアップグレードした場合などです。

作業を開始する前に

- オブジェクトストアプロバイダの有効なアカウントクレデンシャルと設定情報が必要です。
- ソースシステムにクラスタ間ネットワークインターフェイスと IPspace が設定されている。
- ソース Storage VM の DNS 設定でターゲットの FQDN を解決できる必要があります。

## System Manager の略

1. ユーザとグループが正しく定義されていることを確認します。  
Storage > Storage VM\* の順にクリックし、Storage VM をクリックして、\* Settings \* をクリックし、をクリックします  S3 の下。  
  
を参照してください "[S3 ユーザとグループを追加](#)" を参照してください。
2. S3 SnapMirror ポリシーを作成します。これは、既存のポリシーがなく、デフォルトポリシーを使用しない場合に行います。
  - a. [\* 保護]、[概要\*] の順にクリックし、[ローカルポリシーの設定\*] をクリックします。
  - b. をクリックします  [\* 保護ポリシー\*] の横にある [\* 追加] をクリックします。
  - c. ポリシー名と概要を入力します。
  - d. ポリシーのスコップとして、クラスタまたは SVM を選択します
  - e. S3 SnapMirror 関係には「\* Continuous \*」を選択します。
  - f. スロットル\* とリカバリ・ポイントの目標値\* を入力します。
3. ソースシステムに Cloud Object Store を追加します。
  - a. [保護 (Protection)] > [概要 (Overview)] \* をクリックし、[クラウドオブジェクトストア (Cloud Object Store)] を選択
  - b. [\* 追加] をクリックし、[\* Amazon S3 \* または \* その他 \* (StorageGRID Webscale)] を選択します。
  - c. 次の値を入力します。
    - クラウドオブジェクトストアの名前
    - URL 形式 (パスまたは仮想ホスト)
    - Storage VM (S3 に対して有効)
    - オブジェクトストアサーバ名 (FQDN)
    - オブジェクトストアの証明書
    - アクセスキー
    - シークレットキー
    - コンテナ (バケット) 名
4. 既存のバケットのバケットアクセスポリシーが引き続きニーズを満たしていることを確認します。
  - a. [\* Storage \* > \* Buckets] をクリックして、保護するバケットを選択します。
  - b. [\* アクセス許可\*] タブで、をクリックします  \* 編集 \* をクリックし、\* 権限 \* の下の \* 追加 \* をクリックします。
    - \* Principal \* および \* Effect \* - ユーザグループの設定に対応する値を選択するか、デフォルト値をそのまま使用します。
    - アクション-次の値が表示されていることを確認します。  
GetObject, PutObject, DeleteObject, ListBucket, GetBucketAcl, GetObjectAcl, ListBucketMultipartUploads, ListMultipartUploadParts



- ・ リソース-デフォルトを使用します (*bucketname*, *bucketname/\**) または必要なその他の値。

を参照してください ["バケットへのユーザアクセスを管理します"](#) これらのフィールドの詳細については、[を参照してください](#)。

## 5. S3 SnapMirror を使用してバケットをバックアップします。

- [ \* Storage \* ] > [ \* Buckets ] をクリックし、バックアップするバケットを選択します。
- [ \* Protect (保護) ] をクリックし、[ \* Target (ターゲット) ] の下の [ \* Cloud Storage (クラウドストレージ) ] を選択してから、[ \* Cloud Object Store (クラウドオブジェクトストア) ]

Save をクリックすると、既存のバケットがクラウドオブジェクトストアにバックアップされます。

## CLI の使用

### 1. デフォルトのバケットポリシーのアクセスルールが正しいことを確認します。

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

#### 例

```
clusterA::> vservers object-store-server bucket policy add-statement
-bucket test-bucket -effect allow -action
GetObject,PutObject,DeleteObject,ListBucket,GetBucketAcl,GetObjectAcl,
ListBucketMultipartUploads,ListMultipartUploadParts -principal -
-resource test-bucket, test-bucket /*
```

### 2. S3 SnapMirror ポリシーを作成します。これは、既存のポリシーがなく、デフォルトポリシーを使用しない場合に行います。

```
snapmirror policy create -vserver svm_name -policy policy_name -type
continuous [-rpo integer] [-throttle throttle_type] [-comment text]
[additional_options]
```

#### パラメータ

- \* `type continuous` –S3 SnapMirror関係の唯一のポリシータイプ (必須)。
- \* `-rpo` –目標復旧時点の時間を秒単位で指定します (オプション)。
- \* `-throttle` –スループット/帯域幅の上限をキロバイト/秒単位で指定します (オプション)。

#### 例

```
clusterA::> snapmirror policy create -vserver vs0 -type continuous
-rpo 0 -policy test-policy
```

### 3. ターゲットがStorageGRID システムの場合は、ソースクラスタの管理SVMにStorageGRID CA証明書を実装します。

```
security certificate install -type server-ca -vserver src_admin_svm -cert
-name storage_grid_server_certificate
```

を参照してください security certificate install のマニュアルページを参照してください。

#### 4. S3 SnapMirrorデスティネーションオブジェクトストアを定義します。

```
snapmirror object-store config create -vserver svm_name -object-store-name
target_store_name -usage data -provider-type {AWS_S3|SGWS} -server
target_FQDN -container-name remote_bucket_name -is-ssl-enabled true -port
port_number -access-key target_access_key -secret-password
target_secret_key
```

##### パラメータ

- \* -object-store-name -ローカルONTAP システム上のオブジェクトストアターゲットの名前。
- \* -usage -使用します data をクリックします。
- \* -provider-type -AWS\_S3 および SGWS (StorageGRID) ターゲットがサポートされます。
- \* -server -ターゲットサーバのFQDNまたはIPアドレス。
- \* -is-ssl-enabled -SSLの有効化はオプションですが、推奨されます。

[+]

を参照してください snapmirror object-store config create のマニュアルページを参照してください。

##### 例

```
src_cluster::> snapmirror object-store config create -vserver vs0
-object-store-name sgws-store -usage data -provider-type SGWS
-server sgws.example.com -container-name target-test-bucket -is-ssl
-enabled true -port 443 -access-key abc123 -secret-password xyz890
```

#### 5. S3 SnapMirror関係を作成します。

```
snapmirror create -source-path svm_name:/bucket/bucket_name -destination
-path object_store_name:/objstore -policy policy_name
```

##### パラメータ

- \* -destination-path -前の手順で作成したオブジェクトストアの名前と固定値 objstore。

[+]

作成したポリシーを使用することも、デフォルトのポリシーをそのまま使用することもできます。

```
src_cluster::> snapmirror create -source-path vs0:/bucket/buck-evp
-destination-path sgws-store:/objstore -policy test-policy
```

#### 6. ミラーリングがアクティブであることを確認します。

```
snapmirror show -policy-type continuous -fields status
```

クラウドターゲットからバケットをリストアする

ソースバケットのデータが失われたり破損したりした場合は、デスティネーションバケットからリストアしてデータを再取り込みできます。


このタスクについて

デスティネーションバケットは既存のバケットまたは新しいバケットにリストアできます。リストア処理のターゲットバケットは、デスティネーションバケットの使用済み論理スペースよりも大きくする必要があります。

既存のバケットを使用する場合は、リストア処理の開始時に空にする必要があります。Restore は、あるバケットを「ロールバック」するのではなく、空のバケットに以前の内容を取り込みます。

#### System Manager の略

バックアップデータをリストアします。

1. 保護 > 関係 \* をクリックし、\* S3 SnapMirror \* を選択します。
2. をクリックします  アイコン] 次に、[\* Restore] を選択します。
3. 「\* ソース \*」で、「\* 既存バケット」（デフォルト）または「\* 新規バケット」を選択します。
  - 既存の Bucket \* （デフォルト）にリストアするには、次の操作を実行します。
    - 既存のバケットを検索するクラスタと Storage VM を選択します。
    - 既存のバケットを選択します。
    - destination\_S3 サーバ CA 証明書の内容をコピーして貼り付けます。
  - 新しいバケットへのリストアを実行するには、次の値を入力します。
    - 新しいバケットをホストするクラスタと Storage VM。
    - 新しいバケットの名前、容量、およびパフォーマンスサービスレベル。  
を参照してください ["ストレージサービスレベル"](#) を参照してください。
    - デスティネーション S3 サーバ CA 証明書の内容。
4. 「\* Destination \*」の下にある \_source\_S3 サーバ CA 証明書の内容をコピーして貼り付けます。
5. [保護]、[関係] の順にクリックして、復元の進行状況を監視します。

#### CLI 手順の略

1. リストア用の新しいデスティネーションバケットを作成します。詳細については、[を参照してください](#) ["バケットのバックアップ関係の作成（クラウドターゲット）"](#)。

2. デスティネーションバケットのリストア処理を開始します。

```
snapmirror restore -source-path object_store_name:/objstore -destination  
-path svm_name:/bucket/bucket_name
```

#### 例

次の例は、デスティネーションバケットを既存のバケットにリストアします。


```
clusterA::> snapmirror restore -source-path sgws.store:/objstore  
-destination-path vs0:/bucket/test-bucket
```

## ミラーポリシーを変更する

S3 ミラーポリシーを変更できます。たとえば、RPO とスロットルの値を調整する場合などです。

## System Manager の略

これらの値を調整するには、既存の保護ポリシーを編集します。

1. [保護]>[関係]\*をクリックし、変更する関係の保護ポリシーを選択します。
2. をクリックします  アイコン"] ポリシー名の横にある \* Edit \* をクリックします。

## CLI の使用

S3 SnapMirrorポリシーを変更します。

```
snapmirror policy modify -vserver svm_name -policy policy_name [-rpo integer]
[-throttle throttle_type] [-comment text]
```

## パラメータ

- -rpo -目標復旧時点の時間を秒単位で指定します。
- -throttle -スループット/帯域幅の上限をキロバイト/秒単位で指定します。

```
clusterA::> snapmirror policy modify -vserver vs0 -policy test-policy
-rpo 60
```

# S3 イベントを監査します

## S3 イベントを監査します

ONTAP 9.10.1 以降の ONTAP S3 環境でデータイベントと管理イベントを監査できるようになりました。S3 監査機能は既存の NAS 監査機能とほぼ同じであり、S3 および NAS の監査機能はクラスタ内で共存できます。

SVM で S3 監査の設定を作成して有効にすると、S3 イベントがログファイルに記録されます。ログに記録するイベントは次のとおりです。

- オブジェクトアクセス（データ）イベント  
GetObject、PutObject、および DeleteObject
- 管理イベント  
PutBucket および DeleteBucket

ログ形式は JavaScript Object Notation（JSON）です。

S3 および NFS の監査の設定の合計は、クラスタあたり 50 個の SVM です。

次のライセンスバンドルが必要です。

- ONTAP S3プロトコルおよびストレージ向けのCore Bundleです

詳細については、を参照してください ["ONTAP 監査プロセスの仕組み"](#)。

## 監査の保証

デフォルトでは、S3 および NAS の監査が保証されます。ONTAP では、あるノードが利用できない場合でも、監査可能なバケットアクセスイベントがすべて記録されることが保証されます。要求されたバケット処理は、その処理の監査レコードが永続的ストレージのステージングボリュームに保存されるまで完了できません。スペース不足またはその他の問題が原因で監査レコードをステージングファイルにコミットできない場合は、クライアント処理が拒否されます。

## 監査用のスペース要件

ONTAP 監査システムでは、最初に監査レコードが個々のノードのバイナリステージングファイルに格納されます。定期的に統合され、ユーザが読解可能なイベントログに変換されて、SVM の監査イベントログディレクトリに格納されます。

ステージングファイルは専用のステージングボリュームに格納されます。ステージングボリュームは、監査の設定が作成されるときに ONTAP によって作成されます。各アグリゲートに 1 つのステージングボリュームがあります。

監査の設定に十分な利用可能スペースを計画する必要があります。

- 監査対象バケットを含むアグリゲート内のステージングボリューム。
- 変換されたイベントログの格納先ディレクトリを含むボリューム用。

S3 監査の設定を作成する際には、次の 2 つの方法のいずれかを使用して、イベントログの数とボリューム内の利用可能なスペースを制御できます。

- 数値制限 `-rotate-limit` パラメータは、保持する監査ファイルの最小数を制御します。
- 時間制限; `-retention-duration` パラメータは、ファイルを保持できる最大期間を制御します。

どちらのパラメータを使用しても、設定済みの値を超えると古い監査ファイルを削除して新しい監査ファイル用のスペースを確保できます。両方のパラメータの値が 0 の場合、すべてのファイルを保持する必要があります。したがって、十分なスペースを確保するために、パラメータの 1 つをゼロ以外の値に設定することを推奨します。

監査が保証されるため、ローテーションの上限までに監査データに使用できるスペースが不足した場合、新しい監査データを作成することはできず、クライアントがデータにアクセスできなくなります。したがって、この値の選択と監査に割り当てるスペースは慎重に選択する必要があり、また、監査システムの使用可能なスペースに関する警告に対応する必要があります。

詳細については、を参照してください ["監査の基本概念"](#)。

## S3 監査の設定を計画します

S3 監査の設定用にいくつかのパラメータを指定するか、デフォルトを受け入れる必要があります。特に、適切な空きスペースを確保するために、どのログローテーションパラメータを使用するかを検討する必要があります。

を参照してください `*vserver object-store-server audit create*` 構文の詳細については、マニュアルページを参照してください。

## 一般パラメーター

監査の設定の作成時に指定する必要がある 2 つの必須パラメータがあります。また、指定できるオプションのパラメータが 3 つあります。

情報のタイプ	オプション	必須
SVM 名 _  監査の設定を作成する SVM の名前。  SVM がすでに存在し、S3 に対して有効になっている必要があります。	<code>-verserver svm_name</code>	はい。
_ ログデスティネーションパス _  変換された監査ログを格納する場所を指定します。パスが SVM 上に存在している必要があります。  パスには、最大 864 文字の文字列を指定できます。パスには読み取り / 書き込みアクセス権が必要です。  パスが有効でない場合、監査の設定コマンドは失敗します。	<code>-destination text</code>	はい。
_ 監査するイベントのカテゴリ _  監査できるイベントカテゴリは次のとおりです。 <ul style="list-style-type: none"><li>• データ GetObject、PutObject、およびDeleteObjectイベント</li><li>• 管理 PutBucketイベントとDeleteBucketイベント</li></ul> デフォルトでは、データイベントのみが監査されます。	<code>-events {data management}, ...</code>	いいえ

監査ログファイルの数を制御するには、次のいずれかのパラメータを入力します。値を入力しない場合は、すべてのログファイルが保持されます。

情報のタイプ	オプション	必須
ログファイルのローテーションの上限 _  保持する監査ログファイルの数を指定します。これにより、その数からあふれた最も古いログファイルがローテーションから外されます。たとえば、5 という値を入力すると、最後の 5 つのログファイルが保持されます。  値を 0 に設定すると、すべてのログファイルが保持されます。デフォルト値は0です。	<code>-rotate-limit integer</code>	いいえ

<p>ログファイル継続時間制限</p> <p>ログファイルを削除するまでの保持期間を指定します。たとえば、5d0h0m という値を入力すると、5 日を超える古いログが削除されます。</p> <p>値を 0 に設定すると、すべてのログファイルが保持されます。デフォルト値は0です。</p>	<pre>-retention duration integer_time</pre>	<p>いいえ</p>
---	---	------------

## 監査ログローテーションのパラメータ

監査ログのローテーションは、サイズやスケジュールに基づいて実行できます。デフォルトでは、サイズに基づいた監査ログのローテーションが行われます。

ログサイズに基づいてログをローテーションします

デフォルトのログローテーション方法とデフォルトのログサイズを使用する場合、ログローテーションに関する特定のパラメータを設定する必要はありません。デフォルトのログサイズは 100MB です。

デフォルトのログサイズを使用しない場合は、を設定できます `-rotate-size` カスタムログサイズを指定するパラメータ。

ログサイズのみに基づいてローテーションをリセットする場合は、次のコマンドを使用しての設定を解除します `-rotate-schedule-minute` パラメータ：

```
vserver audit modify -vserver svm_name -destination / -rotate-schedule-minute -
```

## スケジュールに基づいたログのローテーション

スケジュールに基づいた監査ログのローテーションを選択した場合は、時間に基づくローテーションパラメータを任意に組み合わせて使用することで、ログのローテーションをスケジュールすることができます。

- 時間に基づくローテーションを使用する場合は、`-rotate-schedule-minute` パラメータは必須です。
- それ以外の時間ベースのローテーションパラメータは、すべてオプションです。
  - `-rotate-schedule-month`
  - `-rotate-schedule-dayofweek`
  - `-rotate-schedule-day`
  - `-rotate-schedule-hour`
- ローテーションスケジュールは、時間に関連するすべての値を使用して計算されます。たとえば、のみを指定した場合 `-rotate-schedule-minute` パラメータを指定すると、監査ログファイルのローテーションは、毎月のすべての曜日の毎時間、指定した分に行われます。
- 時間ベースのローテーションパラメータを1つまたは2つだけ指定した場合（例： `-rotate-schedule-month` および `-rotate-schedule-minutes`）を指定すると、ログファイルのローテーションは、指定した月にのみ、すべての曜日の毎時間、指定した分に行われます。

たとえば、監査ログのローテーションを、1月、3月、8月の毎週月曜日、水曜日、土曜日の10時30分に実行するように指定できます

- 両方に値を指定する場合は `-rotate-schedule-dayofweek` および ``-rotate-schedule-day`` では、これらは独立して考慮されます。

たとえば、を指定した場合などです `-rotate-schedule-dayofweek` 金曜日およびとして `-rotate-schedule-day` 13と指定すると、監査ログのローテーションは、13日の金曜日だけでなく、毎週金曜日と指定した月の13日にも実行されます。

- スケジュールのみに基づいてローテーションをリセットする場合は、次のコマンドを使用しての設定を解除します `-rotate-size` parameter:

```
vserver audit modify -vserver svm_name -destination / -rotate-size -
```

#### ログのサイズとスケジュールに基づいたログのローテーション

`rotate-size` パラメータと時間ベースのローテーションパラメータを任意の組み合わせで設定することで、ログファイルのローテーションをログサイズとスケジュールに基づいて行うことができます。例: `if -rotate-size` は10 MBに設定されており `-rotate-schedule-minute` が15に設定されている場合、ログファイルのサイズが10MBに達したとき、または1時間15分ごと（いずれか早い方）にログファイルがローテーションされます。

## S3 監査の設定を作成して有効にします

S3 監査を実装するには、まず S3 対応 SVM 上に永続的オブジェクトストアの監査の設定を作成し、その設定を有効にします。

必要なもの

- S3 対応の SVM。
- アグリゲートにステージングボリューム用の十分なスペースがあります。

このタスクについて

監査の設定は、監査する S3 バケットを含む SVM ごとに必要です。新規または既存の S3 サーバで S3 監査を有効にすることができます。監査の設定は、`* vserver object-store-server audit delete *` コマンドで削除されるまで S3 環境で維持されます。

S3 監査の設定では、監査対象として選択した SVM 内のすべてのバケットが環境に設定されます。監査が有効な SVM には、監査対象のバケットと監査対象外のバケットを含めることができます。

ログサイズやスケジュールに基づいて、自動ログローテーションの S3 監査を設定することを推奨します。自動ログローテーションを設定しない場合、デフォルトではすべてのログファイルが保持されます。S3 ログファイルのローテーションは、`* vserver object-store-server audit rotate-log *` コマンドを使用して手動で実行することもできます。

SVM が SVM ディザスタリカバリソースである場合、デスティネーションパスをルートボリューム上にすることはできません。

手順

1. 監査の設定を作成し、ログサイズまたはスケジュールに基づいて監査ログのローテーションを実行します。



監査ログのローテーションの基準	入力するコマンド
ログサイズ	<pre>vserver object-store-server audit create -vserver svm_name -destination path [[-events] {data management}, ...] [[-rotate-limit integer]   [- retention-duration [integer_d] [_integer_h][_integer_m][_integers]]] [-rotate-size {integer[KB MB GB TB PB]}]</pre>
スケジュール	<pre>vserver object-store-server audit create -vserver svm_name -destination path [[-events] {data management}, ...] [[-rotate-limit integer]   [- retention-duration [integerd][integerh] [integerm ][_integers]] ] [-rotate-schedule-month chron_month] [-rotate-schedule-dayofweek chron_dayofweek] [- rotate-schedule-day chron_dayofmonth] [-rotate- schedule-hour chron_hour] -rotate-schedule-minute chron_minute</pre> <p>。 -rotate-schedule-minute 時間に基づく監査ログのローテーションを設定する場合は、パラメータが必須です。</p>

## 2. S3 監査を有効にします。

```
vserver object-store-server audit enable -vserver svm_name
```

### 例

次の例は、サイズに基づくローテーションを使用してすべての S3 イベント（デフォルト）を監査する監査の設定を作成します。ログは /audit\_log ディレクトリに格納されます。ログファイルサイズの上限は 200MB です。ログのサイズが 200MB になると、ログのローテーションが実行されます。

```
cluster1::> vserver audit create -vserver vs1 -destination /audit_log -rotate
-size 200MB
```

次の例は、サイズに基づくローテーションを使用してすべての S3 イベント（デフォルト）を監査する監査の設定を作成します。ログファイルサイズの上限は 100MB（デフォルト）で、削除するまで 5 日間保持されます。

```
cluster1::> vserver audit create -vserver vs1 -destination /audit_log -retention
-duration 5d0h0m
```

次の例は、S3 管理イベントを監査する監査の設定と、時間に基づくローテーションを使用した集約型アクセスポリシーのステージングイベントを作成します。監査ログのローテーションが毎月、午後 12 時 30 分に行われますそして毎日、午後 12 : 30 に実行されます。ログのローテーション回数の上限は 5 回です。

```
cluster1::> vserver audit create -vserver vs1 -destination /audit_log -events
management -rotate-schedule-month all -rotate-schedule-dayofweek all -rotate
-schedule-hour 12 -rotate-schedule-minute 30 -rotate-limit 5
```

### S3 監査に使用するバケットを選択します

監査を有効にした SVM で監査するバケットを指定する必要があります。

必要なもの

- SVM で S3 監査が有効になっている。

このタスクについて

S3監査の設定はSVM単位で有効になりますが、監査が有効になっているSVMSでバケットを選択する必要があります。SVM にバケットを追加し、新しいバケットを監査する場合は、この手順でバケットを選択する必要があります。SVM の監査対象外のバケットで S3 監査を有効にすることもできます。

監査の設定は、で削除されるまでバケットの設定が維持されます `vserver object-store-server audit object-select delete` コマンドを実行します

手順

S3 監査用のバケットを選択します。

```
vserver object-store-server audit event-selector create -vserver svm_name -bucket bucket_name [[-access] {read-only|write-only|all}] [[-permission] {allow-only|deny-only|all}]
```

- `-access` -監査するイベントアクセスのタイプを指定します。 `read-only`、 `write-only` または `all` (デフォルトは `all`)。
- `-permission` -監査するイベント権限のタイプを指定します。 `allow-only`、 `deny-only` または `all` (デフォルトは `all`)。

例

次の例は、読み取り専用アクセスで許可されたイベントのみをログするバケットの監査設定を作成します。

```
cluster1::> vserver object-store-server audit event-selector create -vserver vs1 -bucket test-bucket -access read-only -permission allow-only
```

### S3 監査の設定を変更します

個々のバケットの監査パラメータ、または SVM で監査対象として選択されたすべてのバケットの監査設定を変更できます。

監査設定を変更する対象	入力するコマンド
個々のバケット	<code>vserver object-store-server audit event-selector modify -vserver svm_name [-bucket bucket_name] [parameters to modify]</code>
SVM 内のすべてのバケット	<code>vserver object-store-server audit modify -vserver svm_name [parameters to modify]</code>

例

次の例は、書き込み専用のアクセスイベントのみを監査するように個々のバケットの監査設定を変更します。

```
cluster1::> vserver object-store-server audit event-selector modify
-vserver vs1 -bucket test-bucket -access write-only
```

次の例は、SVM内のすべてのバケットの監査設定を変更し、ログサイズの上限を10MBに変更し、ローテーション前にログファイルを3つ保持するようにします。

```
cluster1::> vserver object-store-server audit modify -vserver vs1 -rotate
-size 10MB -rotate-limit 3
```

### S3 監査の設定を表示します

監査の設定が完了したら、監査が適切に設定されて有効になっていることを確認できます。また、クラスタ内のすべてのオブジェクトストアの監査の設定に関する情報を表示することもできます。

このタスクについて

バケットと SVM の監査の設定に関する情報を表示できます。

- バケット–を使用します `vserver object-store-server audit event-selector show` コマンドを実行します

パラメータを何も指定しないと、オブジェクトストアの監査設定があるクラスタ内のすべての SVM 内のバケットに関する次の情報が表示されます。

- SVM 名
- バケット名
- アクセスと権限の値

- SVM–を使用します `vserver object-store-server audit show` コマンドを実行します

パラメータを何も指定しないと、オブジェクトストアの監査の設定があるクラスタ内のすべての SVM に関する次の情報が表示されます。

- SVM 名
- 監査の状態
- ターゲットディレクトリ

を指定できます `-fields` 表示する監査設定情報を指定するパラメータ。

手順

S3 監査の設定に関する情報を表示します。

設定を変更する対象	入力するコマンド
バケット	<code>vserver object-store-server audit event-selector show</code> <code>[-vserver svm_name] [parameters]</code>

設定を変更する対象	入力するコマンド
SVM	<code>vserver object-store-server audit show [-vserver <i>svm_name</i>] [<i>parameters</i>]</code>

例

次の例は、単一のバケットの情報を表示します。

```
cluster1::> vserver object-store-server audit event-selector show -vserver
vs1 -bucket test-bucket
```

Vserver	Bucket	Access	Permission
-----	-----	-----	-----
vs1	bucket1	read-only	allow-only

次の例は、SVM 上のすべてのバケットに関する情報を表示します。

```
cluster1::> vserver object-store-server audit event-selector show -vserver
vs1
```

Vserver	:vs1
Bucket	:test-bucket
Access	:all
Permission	:all

次の例は、すべての SVM の名前、監査の状態、イベントの種類、ログ形式、およびターゲットディレクトリを表示します。

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

Vserver	State	Event Types	Log Format	Target Directory
-----	-----	-----	-----	-----
vs1	false	data	json	/audit_log

次の例は、すべての SVM の SVM 名および監査ログに関する詳細を表示します。

```
cluster1::> vserver object-store-server audit show -log-save-details
```

Vserver	Rotation File Size	Rotation Schedule	Rotation Limit
-----	-----	-----	-----
vs1	100MB	-	0

次の例は、すべての SVM に関するすべての監査設定情報をリスト形式で表示したものです。

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

```

        Vserver: vs1
      Auditing state: true
    Log Destination Path: /audit_log
Categories of Events to Audit: data
        Log Format: json
      Log File Size Limit: 100MB
    Log Rotation Schedule: Month: -
Log Rotation Schedule: Day of Week: -
      Log Rotation Schedule: Day: -
      Log Rotation Schedule: Hour: -
    Log Rotation Schedule: Minute: -
        Rotation Schedules: -
      Log Files Rotation Limit: 0
      Log Retention Time: 0s
```

# 認証とアクセス制御

## ニンシヨウトアクセスセイキヨノカイヨウ

ONTAP クラスタの認証とONTAP Webサービスへのアクセス制御を管理できます。

System Manager または CLI を使用して、クライアントや管理者によるクラスタやストレージへのアクセスを制御し、保護することができます。

従来の System Manager（ONTAP 9.7 以前でのみ使用可能）を使用している場合は、[を参照してください](#)  
"System Manager Classic（ONTAP 9.0 から 9.7）"

### クライアントの認証と許可

ONTAP では、信頼できるソースで ID を検証してクライアントマシンおよびユーザを認証します。ONTAP は、ユーザのクレデンシャルとファイルまたはディレクトリに対して設定されている権限を比較して、ユーザにファイルまたはディレクトリへのアクセスを許可します。

### 管理者認証と RBAC

管理者は、ローカルまたはリモートのログインアカウントを使用してクラスタおよび Storage VM に対して自身を認証します。管理者がアクセスできるコマンドは、ロールベースアクセス制御（RBAC）に基づいて決まります。

## 管理者認証とRBACの管理

管理者認証と RBAC の概要については、**CLI** を使用してください

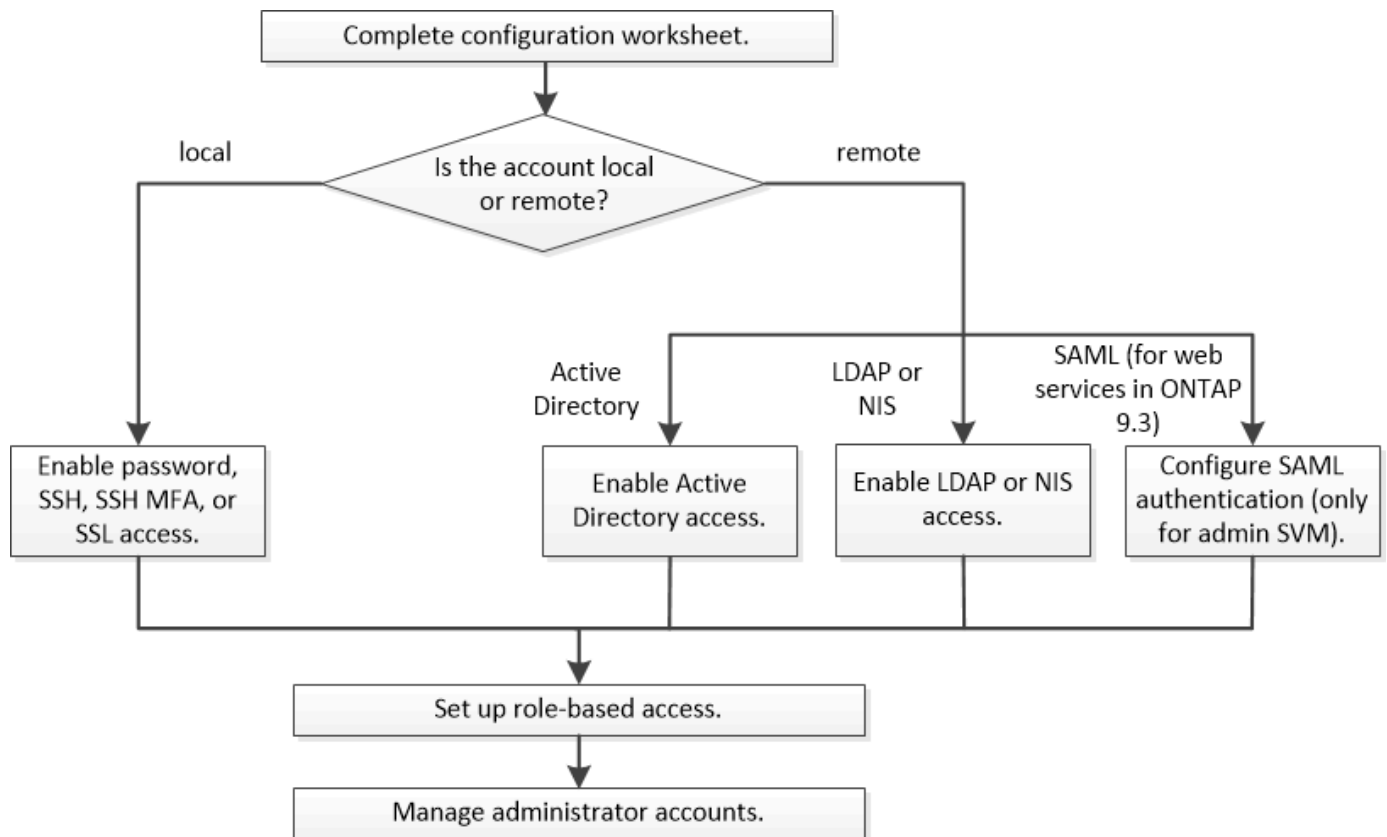
ONTAP クラスタ管理者および Storage Virtual Machine（SVM）管理者のログインアカウントを有効にすることができます。管理者が実行できる機能は、ロールベースアクセス制御（RBAC）を使用して定義することもできます。

ログインアカウントと RBAC は次の方法で有効にします。

- System Manager や自動スクリプトツールではなく、ONTAP コマンドラインインターフェイス（CLI）を使用する必要がある。
- すべての選択肢について検討するのではなく、ベストプラクティスに従う。
- クラスタに関する情報の収集に SNMP を使用しない。

### 管理者認証と RBAC のワークフロー

ローカルまたはリモートの管理者アカウントに対して認証を有効にすることができます。ローカルアカウントのアカウント情報はストレージシステムに、リモートアカウントのアカウント情報はストレージシステム以外の場所に格納されます。各アカウントには、事前定義されたロールまたはカスタムロールを割り当てることができます。



ローカル管理者アカウントには、次の種類の認証を使用した管理 Storage Virtual Machine（SVM）またはデータ SVM へのアクセスを許可できます。

- パスワード
- SSH 公開鍵
- SSL証明書
- SSH 多要素認証（MFA）

ONTAP 9.3 以降では、パスワードと公開鍵による認証がサポートされます。

リモートの管理者アカウントには、次の種類の認証を使用した管理 SVM またはデータ SVM へのアクセスを許可できます。

- Active Directory
- SAML 認証（管理 SVM のみ）

ONTAP 9.3 以降では、Service Processor Infrastructure、ONTAP API、または System Manager のいずれかの Web サービスを使用することで、管理 SVM へのアクセスに Security Assertion Markup Language（SAML）認証を使用できます。

- ONTAP 9.4 以降では、LDAP サーバまたは NIS サーバ上のリモートユーザに SSH MFA を使用できます。nsswitch と公開鍵による認証がサポートされます。

## 管理者認証と **RBAC** 設定用のワークシートです

ログインアカウントを作成してロールベースアクセス制御（RBAC）を設定する前に、設定ワークシートの各項目について情報を収集しておく必要があります。

ログインアカウントを作成または変更します

次の値はで指定します `security login create` コマンドは、ログインアカウントによるStorage VMへのアクセスを有効にする場合に使用します。にも同じ値を指定します `security login modify` コマンドは、アカウントによるStorage VMへのアクセス方法を変更するときに使用します。

フィールド	説明	あなたの価値
<code>-vserver</code>	アカウントがアクセスするStorage VMの名前。デフォルト値はクラスタの管理Storage VMの名前です。	
<code>-user-or-group-name</code>	アカウントのユーザ名またはグループ名。グループ名を指定すると、そのグループ内の各ユーザのアクセスが有効になります。ユーザ名またはグループ名を複数のアプリケーションに関連付けることができます。	
<code>-application</code>	Storage VMへのアクセスに使用されるアプリケーション： <ul style="list-style-type: none"><li>• <code>http</code></li><li>• <code>ontapi</code></li><li>• <code>snmp</code></li><li>• <code>ssh</code></li></ul>	



-authmethod	<p>アカウントの認証に使用する 方法。</p> <ul style="list-style-type: none"> <li>• cert SSL証明書認証用</li> <li>• domain Active Directory認証用</li> <li>• nsswitch LDAPまたはNIS認 証に使用します</li> <li>• password ユーザパスワード認 証用</li> <li>• publickey 公開鍵認証用</li> <li>• community (SNMPコミュニ ティストリング)</li> <li>• usm SNMPユーザセキュリティ モデルの場合</li> <li>• saml Security Assertion Markup Language (SAML) 認 証に使用します</li> </ul>	
-remote-switch-ipaddress	<p>リモートスイッチの IP アドレスで す。リモートスイッチは、クラス タスイッチヘルスマニタ (CSHM ) で監視されるクラスタスイッ チ、または MetroCluster ヘルスマ ニタ (MCC-HM) で監視される Fibre Channel (FC) スイッチで す。このオプションは、アプリケ ーションがの場合にのみ適用され ます snmp 認証方法はです usm。</p>	
-role	<p>アカウントに割り当てられている アクセス制御ロール。</p> <ul style="list-style-type: none"> <li>• クラスタ (管理Storage VM) のデフォルト値はです。 admin。</li> <li>• データStorage VMの場合、デ フォルト値はです。 vsadmin。</li> </ul>	
-comment	<p>(オプション) アカウントの説 明。テキストは二重引用符 (") で囲む必要があります。</p>	

-is-ns-switch-group	アカウントがLDAPグループアカウントかNISグループアカウントか (yes または no) 。	
-second-authentication-method	<p>多要素認証の場合の2番目の認証方式：</p> <ul style="list-style-type: none"> <li>• none 多要素認証を使用しない場合は、デフォルト値</li> <li>• publickey 公開鍵認証の場合 authmethod は、password または nsswitch です</li> <li>• password でのユーザパスワード認証に使用します authmethod は公開鍵です</li> <li>• nsswitch authmethod が publickey の場合のユーザパスワード認証用</li> </ul> <p>認証の順序は、常に公開鍵が先でパスワードがあとです。</p>	
-is-ldap-fastbind	<p>ONTAP 9.11.1以降では、trueに設定すると、nsswitch認証に対してLDAPファストバインドが有効になります。デフォルトはfalseです。LDAP高速バインドを使用するには、を使用します</p> <p>-authentication-method 値はに設定する必要があります nsswitch。 <a href="#">"nsswitch認証のLDAP fastbindについて説明します。"</a></p>	

## Cisco Duoセキュリティ情報の設定

次の値はで指定します security login duo create コマンドは、Storage VMに対してSSHログインを使用したCisco Duoツーフアクタ認証を有効にする場合に使用します。

フィールド	説明	あなたの価値
-vserver	Duo認証設定を適用するStorage VM（ONTAP CLIではVserver）。	
-integration-key	DuoにSSHアプリケーションを登録するときに取得した統合キー。	

-secret-key	DuoにSSHアプリケーションを登録するときに取得した秘密キー。	
-api-host	<p>SSHアプリケーションをDuoに登録するときに取得されるAPIホスト名。例：</p> <pre>api- &lt;HOSTNAME&gt;.duosecurity.com</pre>	
-fail-mode	Duo認証を妨げるサービスまたは構成エラーの場合は、失敗します。 safe （アクセスを許可）または secure （アクセスを拒否）。デフォルトはです `safe`これは、Duo APIサーバーにアクセスできないなどのエラーが原因で失敗した場合、Duo認証がバイパスされることを意味します。	
-http-proxy	<p>指定したHTTPプロキシを使用します。HTTPプロキシで認証が必要な場合は、プロキシURLにクレデンシャルを含めます。例：</p> <pre>http- proxy=http://username :password@proxy.example.org:8080</pre>	
-autopush	<p>または true または false。デフォルトはです false。状況 `true`Duoは、プッシュログイン要求をユーザーの電話に自動的に送信し、プッシュが利用できない場合は通話に戻ります。これにより、パスコード認証が実質的に無効になります。状況 `false`を選択すると、認証方法を選択するように求められます。</p> <p>セツテイシタシヨウコウ autopush = true`を設定することをお勧めします `max-prompts = 1。</p>	

-max-prompts	<p>ユーザーが2番目のファクターで認証に失敗した場合、Duoはユーザーに再度認証を求めるプロンプトを表示します。このオプションは、アクセスを拒否する前にDuoが表示するプロンプトの最大数を設定します。でなければなりません 1、 2`または `3。デフォルト値はです 1。</p> <p>例えば、`max-prompts = 1`ユーザーは最初のプロンプトで正常に認証される必要がありますが、次の場合は`max-prompts = 2`ユーザーが最初のプロンプトで誤った情報を入力すると、再度認証を求めるプロンプトが表示されます。</p> <p>セツテイシタシヨウコウ autopush = true`を設定することをお勧めします `max-prompts = 1。</p> <p>最高のエクスペリエンスを得るために、公開鍵認証のみを使用するユーザーには、常に max-prompts をに設定します 1。</p>	
-enabled	<p>Duo 2要素認証を有効にします。をに設定します true デフォルトでは有効にすると、設定されているパラメータに従って、SSHログイン時にDuo 2要素認証が実行されます。Duoが無効になっている場合 ( false)、Duo認証は無視されます。</p>	

## カスタムロールを定義する

次の値はで指定します security login role create コマンドは、カスタムロールを定義するときに使用します。

フィールド	説明	あなたの価値
-vserver	(オプション) ロールに関連付けられているStorage VM (ONTAP CLIではVserverと表示されます) の名前。	
-role	ロールの名前。	

-cmddirname	<p>ロールでアクセスできるコマンドまたはコマンドディレクトリ。コマンドサブディレクトリの名前は二重引用符 (") で囲む必要があります。例: "volume snapshot"。入る必要があります DEFAULT すべてのコマンドディレクトリを指定します。</p>	
-access	<p>(任意) ロールのアクセスレベル。コマンドディレクトリの場合:</p> <ul style="list-style-type: none"> <li>• none (カスタムロールのデフォルト値) は、コマンドディレクトリ内のコマンドへのアクセスを拒否します</li> <li>• readonly へのアクセスを許可します show コマンドディレクトリとそのサブディレクトリ内のコマンド</li> <li>• all コマンドディレクトリとそのサブディレクトリ内のすべてのコマンドへのアクセスを許可します</li> </ul> <p>for_nonintrinsic commands_ (末尾がでないコマンド create、modify、delete`または `show) :</p> <ul style="list-style-type: none"> <li>• none (カスタムロールのデフォルト値) は、コマンドへのアクセスを拒否します</li> <li>• readonly は適用されません</li> <li>• all コマンドへのアクセスを許可します</li> </ul> <p>組み込みコマンドへのアクセスを許可または拒否するには、コマンドディレクトリを指定する必要があります。</p>	

-query	<p>(任意) アクセスレベルのフィルタリングに使用されるクエリーオブジェクト。コマンドの有効なオプションまたはコマンドディレクトリ内のコマンドの形式で指定します。クエリーオブジェクトは二重引用符 (") で囲む必要があります。たとえば、コマンドディレクトリがの場合などです volume、クエリーオブジェクト "-aggr aggr0" のアクセスを有効にします aggr0 アグリゲートのみ：</p>	
--------	--	--

ユーザアカウントに公開鍵を関連付けます

次の値はで指定します security login publickey create コマンドは、SSH公開鍵をユーザアカウントに関連付けるときに使用します。

フィールド	説明	あなたの価値
-vserver	(オプション) アカウントがアクセスするStorage VMの名前。	
-username	アカウントのユーザ名。デフォルト値 `admin` に変更します。これは、クラスタ管理者のデフォルト名です。	
-index	公開鍵のインデックス番号。デフォルト値は、アカウントに対して最初に作成されたキーの場合は 0 です。それ以外の場合、デフォルト値は、そのアカウントに対して既存の最も大きいインデックス番号の 1 つ以上になります。	
-publickey	OpenSSH 公開鍵。キーは二重引用符 (") で囲む必要があります。	
-role	アカウントに割り当てられているアクセス制御ロール。	
-comment	(オプション) 公開鍵についての説明。テキストは二重引用符 (") で囲む必要があります。	

-x509-certificate	<p>(任意) ONTAP 9.13.1以降では、SSH公開鍵とのX.509証明書の関連付けを管理できます。</p> <p>X.509証明書をSSH公開鍵に関連付けると、ONTAPはSSHログイン時にこの証明書が有効かどうかを確認します。有効期限が切れているか失効している場合、ログインは許可されず、関連するSSH公開鍵は無効になります。有効な値は次のとおり</p> <ul style="list-style-type: none"> <li>• <code>install</code>：指定したPEMでエンコードされたX.509証明書をインストールし、SSH公開鍵に関連付けます。インストールする証明書の全文を含めます。</li> <li>• <code>modify</code>：PEMでエンコードされた既存のX.509証明書を指定された証明書に更新し、SSH公開鍵に関連付けます。新しい証明書の全文を含めます。</li> <li>• <code>delete</code>：既存のX.509証明書とSSH公開鍵の関連付けを削除します。</li> </ul>	
-------------------	--	--

## CA 署名済みサーバデジタル証明書をインストールする。

次の値はで指定します `security certificate generate-csr` Storage VMをSSLサーバとして認証するために使用するデジタル証明書署名要求（CSR）を生成するときにコマンドを実行します。

フィールド	説明	あなたの価値
-common-name	証明書の名前。完全修飾ドメイン名（FQDN）またはカスタム共通名を指定できます。	
-size	秘密鍵のビット数。値が大きいほど、キーのセキュリティは向上します。デフォルト値はです 2048。指定できる値はです 512、1024、1536、および 2048。	
-country	Storage VMの国（2文字のコード）。デフォルト値はです us。コードの一覧については、マニュアルページを参照してください。	

-state	Storage VMの都道府県。	
-locality	Storage VMの局所性。	
-organization	Storage VMの組織。	
-unit	Storage VMの組織内の単位。	
-email-addr	Storage VMの管理者連絡先のEメールアドレス。	
-hash-function	証明書の署名に使用する暗号化ハッシュ関数。デフォルト値はですSHA256。指定できる値はですSHA1、SHA256およびMD5。	

次の値はで指定します security certificate install コマンドは、クラスタまたはStorage VMをSSLサーバとして認証するためにCA署名デジタル証明書をインストールするときに使用します。次の表には、アカウント設定に関連するオプションのみを示します。

フィールド	説明	あなたの価値
-vserver	証明書をインストールするStorage VMの名前。	
-type	証明書のタイプ。 <ul style="list-style-type: none"> <li>• server (サーバ証明書と中間証明書)</li> <li>• client-ca SSLクライアントのルートCAの公開鍵証明書用</li> <li>• server-ca ONTAP がクライアントであるSSLサーバのルートCAの公開鍵証明書用</li> <li>• client ONTAP をSSLクライアントとして使用するための自己署名またはCA署名のデジタル証明書および秘密鍵</li> </ul>	

## Active Directory ドメインコントローラアクセスを設定する

次の値はで指定します security login domain-tunnel create コマンドは、データStorage VM用のSMBサーバがすでに設定されていて、Storage VMをゲートウェイまたは\_tunnel\_ (Active Directory ドメインコントローラによるクラスタへのアクセスの場合) として設定する場合に使用します。

フィールド	説明	あなたの価値
-------	----	--------



-vserver	SMBサーバが設定されているStorage VMの名前。	
----------	------------------------------	--

次の値はで指定します `vserver active-directory create` コマンドは、SMBサーバを設定しておらず、Active DirectoryドメインにStorage VMコンピュータアカウントを作成する場合に使用します。

フィールド	説明	あなたの価値
-vserver	Active Directoryコンピュータアカウントを作成するStorage VMの名前。	
-account-name	コンピュータアカウントのNetBIOS 名。	
-domain	完全修飾ドメイン名（FQDN）。	
-ou	ドメイン内の組織単位。デフォルト値はです <code>CN=Computers</code> 。ONTAPはこの値をドメイン名に付加して、Active Directory 識別名を生成します。	

## LDAP サーバまたは NIS サーバのアクセスを設定

次の値はで指定します `vserver services name-service ldap client create` コマンドは、Storage VMのLDAPクライアント設定を作成するときに使用します。

次の表には、アカウント設定に関連するオプションのみを示します。

フィールド	説明	あなたの価値
-vserver	クライアント設定のStorage VMの名前。	
-client-config	クライアント設定の名前。	
-ldap-servers	クライアントの接続先LDAPサーバのIPアドレスとホスト名をカンマで区切ったリスト。	
-schema	クライアントが LDAP クエリの作成に使用するスキーマ。	

-use-start-tls	<p>クライアントがStart TLSを使用してLDAPサーバとの通信を暗号化するかどうか (true または false) 。</p> <div>  <p>Start TLSは、データStorage VMへのアクセスでのみサポートされます。管理Storage VMへのアクセスではサポートされていません。</p> </div>	
----------------	---	--

次の値はで指定します `vserver services name-service ldap create` コマンドは、LDAPクライアント設定をStorage VMに関連付けるときに使用します。

フィールド	説明	あなたの価値
-vserver	クライアント設定を関連付けるStorage VMの名前。	
-client-config	クライアント設定の名前。	
-client-enabled	Storage VMでLDAPクライアント設定を使用できるかどうか (true または false) 。	

次の値はで指定します `vserver services name-service nis-domain create` コマンドは、Storage VMにNISドメイン設定を作成するとき使用します。

フィールド	説明	あなたの価値
-vserver	ドメイン設定を作成するStorage VMの名前。	
-domain	ドメインの名前。	
-active	ドメインがアクティブかどうか (true または false) 。	
-servers	<ul style="list-style-type: none"> <li>ONTAP 9.0、9.1 * : ドメイン設定で使用される NIS サーバの IP アドレスをカンマで区切って指定します。</li> </ul>	

-nis-servers	ドメイン設定で使用するNISサーバのIPアドレスとホスト名をカンマで区切ったリスト。	
--------------	--	--

次の値はで指定します `vserver services name-service ns-switch create` コマンドは、ネームサービスソースの参照順序を指定するときに使用します。

フィールド	説明	あなたの価値
-vserver	ネームサービスの参照順序を設定するStorage VMの名前。	
-database	ネームサービスデータベース。  <ul style="list-style-type: none"> <li>• <code>hosts</code> (ファイルおよびDNS ネームサービス)</li> <li>• <code>group</code> (ファイル、LDAP、およびNISの各ネームサービス)</li> <li>• <code>passwd</code> (ファイル、LDAP、およびNISの各ネームサービス)</li> <li>• <code>netgroup</code> (ファイル、LDAP、およびNISの各ネームサービス)</li> <li>• <code>namemap</code> ファイルとLDAPネームサービス</li> </ul>	
-sources	ネームサービスソースを検索する順序 (カンマで区切ったリスト)。  <ul style="list-style-type: none"> <li>• <code>files</code></li> <li>• <code>dns</code></li> <li>• <code>ldap</code></li> <li>• <code>nis</code></li> </ul>	

## SAML アクセスを設定する

ONTAP 9.3以降では、で次の値を指定します `security saml-sp create` SAML認証を設定するコマンド。

フィールド	説明	あなたの価値
-------	----	--------

<code>-idp-uri</code>	アイデンティティプロバイダ（IdP）メタデータのダウンロード元である IdP ホストの FTP アドレスまたは HTTP アドレス。	
<code>-sp-host</code>	SAML サービスプロバイダホスト（ONTAP システム）のホスト名または IP アドレス。デフォルトでは、クラスタ管理 LIF の IP アドレスが使用されます。	
<code>-cert-ca</code> および <code>-cert-serial</code> または <code>-cert-common-name</code>	サービスプロバイダホスト（ONTAP システム）のサーバ証明書の詳細。サービスプロバイダの証明書発行認証局（CA）と証明書のシリアル番号、またはサーバ証明書の共通名を入力できます。	
<code>-verify-metadata-server</code>	IdPメタデータサーバのIDを検証するかどうか <code>true</code> または <code>false</code> ）。この値は常にに設定することを推奨します <code>true</code> 。	

## ログインアカウントを作成します

### ログインアカウントの作成の概要

クラスタおよび SVM の管理者アカウントは、ローカルまたはリモートのいずれかとして有効にできます。ローカルアカウントでは、アカウント情報、公開鍵、セキュリティ証明書がストレージシステムに格納されます。AD アカウント情報はドメインコントローラに格納されます。LDAP および NIS アカウントは LDAP サーバおよび NIS サーバ上に存在します。

#### クラスタ管理者と **SVM** 管理者

クラスタ管理者は、クラスタの管理 SVM にアクセスします。管理SVMとクラスタ管理者（予約された名前）`admin` は、クラスタのセットアップ時に自動的に作成されます。

デフォルトを持つクラスタ管理者 `admin` ロールは、クラスタ全体とそのリソースを管理できます。クラスタ管理者は、必要に応じて別のロールを割り当てた別のクラスタ管理者を作成することができます。

SVM administrator は、データ SVM にアクセスします。クラスタ管理者は、必要に応じてデータ SVM と SVM 管理者を作成します。

SVM管理者には、が割り当てられます `vsadmin` デフォルトではロール。クラスタ管理者は、必要に応じて SVM 管理者に別のロールを割り当てることができます。

## 命名規則

リモートクラスタおよびSVMの管理者アカウントには、次の汎用名は使用できません。

- "adm"
- "ビン"
- "CLI"
- "デーモン"
- "ftp"
- "ゲーム"
- "停止"
- "LP"
- "メール"
- "男"
- "naroot"
- " NetApp "
- "ニュース"
- "誰もいない"
- "演算子"
- "ルート"
- "シャットダウン"
- "sshd"
- "同期"
- "sys"
- " uucp"
- "WWW"

## マージされたロール

同じユーザに対して複数のリモートアカウントを有効にすると、そのユーザには各アカウントに対して指定されたロールがすべて割り当てられます。つまり、LDAPまたはNISアカウントにが割り当てられている場合です `vsadmin` ロールが割り当てられ、同じユーザのADグループアカウントにが割り当てられます `vsadmin-volume` ロール。ADユーザは、より包括的なを使用してログインします `vsadmin` 機能：ロールは、 `_merged__` と呼ばれます。

## ローカルアカウントアクセスを有効にします

### ローカルアカウントアクセスの有効化の概要

ローカルアカウントでは、アカウント情報、公開鍵、セキュリティ証明書がストレージシステムに格納されます。を使用できます `security login create` コマンドを使用して、ローカルアカウントが管理またはデータSVMにアクセスできるようにします。

パスワードアカウントアクセスを有効にします

を使用できます `security login create` コマンドを使用して、管理者アカウントがパスワードを使用して管理またはデータSVMにアクセスできるようにします。コマンドを入力するとパスワードの入力を求められます。

このタスクについて

ログインアカウントに割り当てるアクセス制御ロールが不明な場合は、を使用します `security login modify` コマンドを使用してあとでロールを追加します。

作業を開始する前に

このタスクを実行するには、クラスタ管理者である必要があります。

ステップ

1. ローカル管理者アカウントがパスワードを使用して SVM にアクセスできるようにします。

```
security login create -vserver SVM_name -user-or-group-name user_or_group_name  
-application application -authmethod authentication_method -role role -comment  
comment
```

コマンド構文全体については、を参照してください ["ワークシート"](#)。

次のコマンドは、クラスタ管理者アカウントを有効にします `admin1` を使用します `backup` 管理SVMにアクセスするためのロール `engCluster` パスワードを使用する。コマンドを入力するとパスワードの入力を求められます。

```
cluster1::>security login create -vserver engCluster -user-or-group-name  
admin1 -application ssh -authmethod password -role backup
```

**SSH** 公開鍵アカウントを有効にします

を使用できます `security login create` コマンドを使用して、管理者アカウントがSSH公開鍵を使用して管理またはデータSVMにアクセスできるようにします。

このタスクについて

- アカウントが SVM にアクセスするためには、アカウントに公開鍵を関連付けておく必要があります。

[ユーザアカウントへの公開鍵の関連付け](#)

このタスクは、アカウントアクセスを有効にする前後どちらでも実行できます。

- ログインアカウントに割り当てるアクセス制御ロールが不明な場合は、を使用します `security login modify` コマンドを使用してあとでロールを追加します。

クラスタでFIPSモードを有効にする場合は、サポートされているキーアルゴリズムのない既存のSSH公開鍵アカウントを、サポートされるキータイプで再設定する必要があります。FIPSを有効にする前にアカウントを再設定する必要があります。そうしないと、管理者認証が失敗します。

次の表に、ONTAP SSH接続でサポートされるホストキータイプアルゴリズムを示します。これらのキータイプは、SSH公開認証の設定には適用されません。

ONTAP リリース	FIPSモードでサポートされるキータイプ	FIPS以外のモードでサポートされるキータイプ
9.11.1以降	ECDSA - sha2 - nistp256	ECDSA-sha2-nistp256+ rsa-sha2-512+ rsa-sha2-256+ SSH-ed25519以降 SSH-DSS+ SSH-RSA
9.10.1以前	ECDSA-sha2-nistp256+ SSH-ed25519	ECDSA-sha2-nistp256+ SSH-ed25519以降 SSH-DSS+ SSH-RSA



ONTAP 9.11.1以降では、ssh-ed25519ホストキーアルゴリズムのサポートが廃止されました。

詳細については、を参照してください ["FIPS を使用してネットワークセキュリティを設定する"](#)。

作業を開始する前に

このタスクを実行するには、クラスタ管理者である必要があります。

#### ステップ

1. ローカル管理者アカウントが SSH 公開鍵を使用して SVM にアクセスできるようにします。

```
security login create -vserver SVM_name -user-or-group-name user_or_group_name  
-application application -authmethod authentication_method -role role -comment  
comment
```

コマンド構文全体については、を参照してください ["ワークシート"](#)。

次のコマンドは、SVM管理者アカウントを有効にします `svmadmin1` を使用します `vsadmin-volume` SVMにアクセスするためのロール `engData1` SSH公開鍵の使用：

```
cluster1::>security login create -vserver engData1 -user-or-group-name  
svmadmin1 -application ssh -authmethod publickey -role vsadmin-volume
```

完了後

管理者アカウントに公開鍵が関連付けられていない場合は、アカウントが SVM にアクセスする前に関連付けておく必要があります。

[ユーザアカウントへの公開鍵の関連付け](#)

多要素認証（MFA）アカウントを有効にします

多要素認証の概要

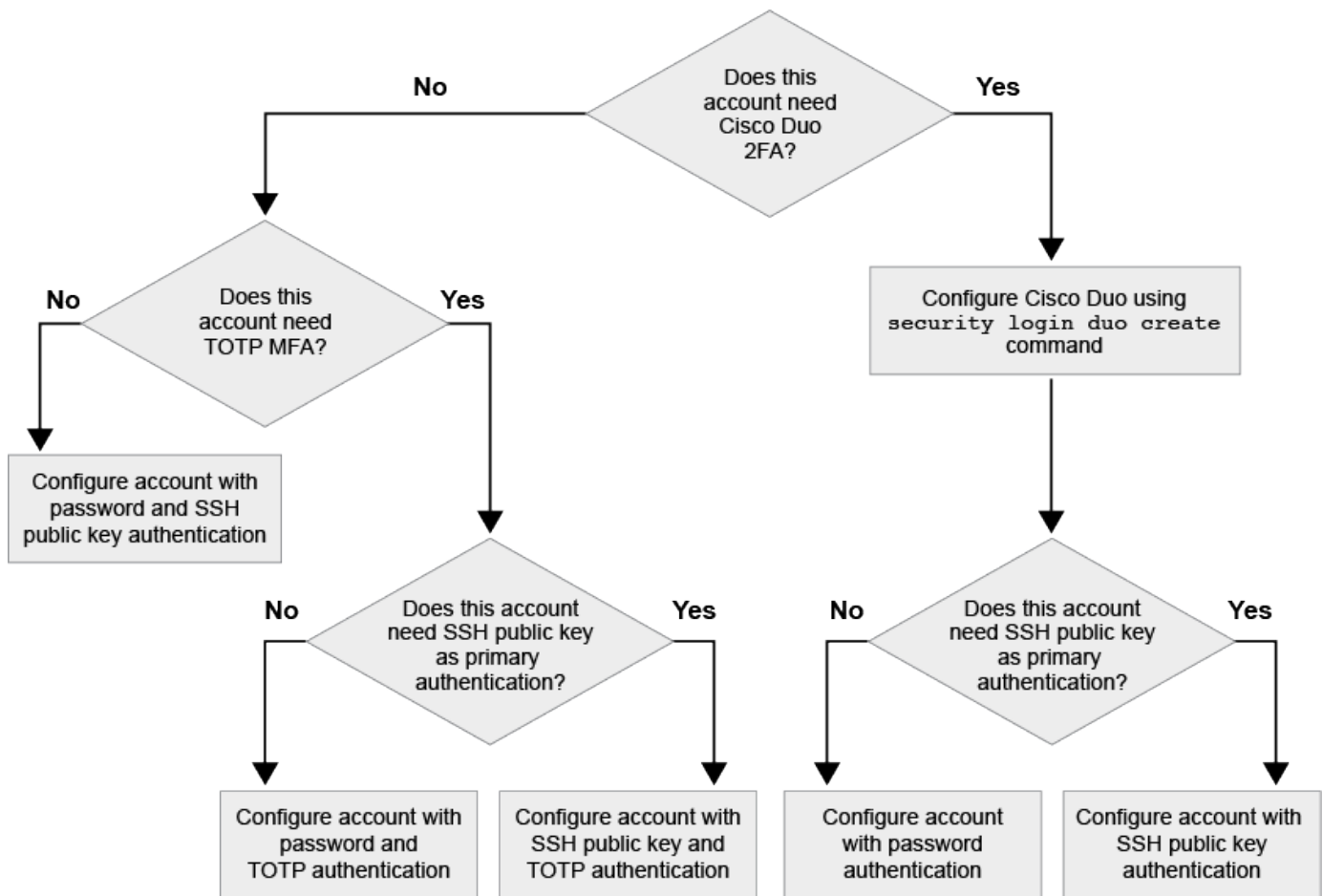
多要素認証（MFA）を使用すると、ユーザが管理Storage VMまたはデータStorage VMにログインする際に2つの認証方法を指定する必要があるため、セキュリティを強化できます。

ONTAPのバージョンに応じて、SSH公開鍵、ユーザパスワード、および時間ベースのワンタイムパスワード（TOTP）を組み合わせることで多要素認証に使用できます。Cisco Duo（ONTAP 9.14.1以降）をイネーブルにして設定すると、追加の認証方式として機能し、すべてのユーザの既存の方式を補完します。

使用可能なバージョン	最初の認証方法	2番目の認証方法
ONTAP 9.14.1	SSH 公開鍵	TOTP
	ユーザパスワード	TOTP
	SSH 公開鍵	Cisco Duo
	ユーザパスワード	Cisco Duo
ONTAP 9.13.1	SSH 公開鍵	TOTP
	ユーザパスワード	TOTP
ONTAP 9.3	SSH 公開鍵	ユーザパスワード

MFAが設定されている場合は、クラスタ管理者が最初にローカルユーザアカウントを有効にしてから、ローカルユーザがアカウントを設定する必要があります。





多要素認証を有効にします

多要素認証（MFA）を使用すると、管理SVMまたはデータSVMにログインする際にユーザに2つの認証方式の指定を要求することで、セキュリティを強化できます。

このタスクについて

- このタスクを実行するには、クラスタ管理者である必要があります。
- ログインアカウントに割り当てるアクセス制御ロールが不明な場合は、を使用します `security login modify` コマンドを使用してあとでロールを追加します。

#### "管理者に割り当てられているロールの変更"

- 認証に公開鍵を使用している場合は、アカウントがSVMにアクセスする前にアカウントに公開鍵を関連付ける必要があります。

#### "ユーザアカウントに公開鍵を関連付けます"

このタスクは、アカウントアクセスを有効にする前後どちらでも実行できます。

- ONTAP 9.12.1以降では、FIDO2（Fast Identity Online）またはPIV（Personal Identity Verification）認証標準を使用して、SSHクライアントMFAにYubikeyハードウェア認証デバイスを使用できます。

## SSH公開鍵とユーザパスワードを使用してMFAを有効にします

ONTAP 9.3以降では、クラスタ管理者がSSH公開鍵とユーザパスワードを使用してMFAを使用してログインするためのローカルユーザアカウントを設定できます。

1. ローカルユーザアカウントでSSH公開鍵とユーザパスワードを使用してMFAを有効にします。

```
security login create -vserver <svm_name> -user-or-group-name  
<user_name> -application ssh -authentication-method <password|publickey>  
-role admin -second-authentication-method <password|publickey>
```

次のコマンドを実行するには、SVM管理者アカウントが必要です `admin2` を使用します `admin` SVMにログインするためのロール `engData1` SSH公開鍵とユーザパスワードの両方を使用して、次の手順を実行します。

```
cluster-1::> security login create -vserver engData1 -user-or-group-name  
admin2 -application ssh -authentication-method publickey -role admin  
-second-authentication-method password  
  
Please enter a password for user 'admin2':  
Please enter it again:  
Warning: To use public-key authentication, you must create a public key  
for user "admin2".
```

## TOTPでMFAを有効にする

ONTAP 9.13.1以降では、SSH公開鍵またはユーザパスワードと時間ベースのワンタイムパスワード（TOTP）の両方を使用してローカルユーザに管理SVMまたはデータSVMへのログインを要求することで、セキュリティを強化できます。TOTPを使用してMFAのアカウントを有効にしたあと、ローカルユーザはにログインする必要があります ["設定を完了します"](#)。

TOTPは、現在の時刻を使用してワンタイムパスワードを生成するコンピュータアルゴリズムです。TOTPを使用する場合は、常にSSH公開鍵またはユーザパスワードに続く2番目の認証形式になります。

作業を開始する前に

これらのタスクを実行するには、ストレージ管理者である必要があります。

手順

最初の認証方法としてユーザパスワードまたはSSH公開鍵を使用し、2番目の認証方法としてTOTPを使用してMFAを設定できます。

## ユーザパスワードとTOTPでMFAを有効にします

1. ユーザパスワードとTOTPを使用して、ユーザアカウントで多要素認証を有効にします。

### 新規ユーザーアカウントの場合

```
security login create -vserver <svm_name> -user-or-group-name  
<user_or_group_name> -application ssh -authentication-method  
password -second-authentication-method totp -role <role> -comment  
<comment>
```

### 既存のユーザーアカウントの場合

```
security login modify -vserver <svm_name> -user-or-group-name  
<user_or_group_name> -application ssh -authentication-method  
password -second-authentication-method totp -role <role> -comment  
<comment>
```

2. TOTPを使用したMFAが有効になっていることを確認します。

```
security login show
```

## SSH公開鍵とTOTPを使用してMFAを有効にします

1. SSH公開鍵とTOTPを使用した多要素認証のユーザアカウントを有効にします。

### 新規ユーザーアカウントの場合

```
security login create -vserver <svm_name> -user-or-group-name  
<user_or_group_name> -application ssh -authentication-method  
publickey -second-authentication-method totp -role <role> -comment  
<comment>
```

### 既存のユーザーアカウントの場合

```
security login modify -vserver <svm_name> -user-or-group-name  
<user_or_group_name> -application ssh -authentication-method  
publickey -second-authentication-method totp -role <role> -comment  
<comment>
```

2. TOTPを使用したMFAが有効になっていることを確認します。

```
security login show
```

#### 完了後

- 管理者アカウントに公開鍵が関連付けられていない場合は、アカウントが SVM にアクセスする前に関連付けておく必要があります。

#### "ユーザアカウントへの公開鍵の関連付け"

- TOTPを使用したMFAの設定を完了するには、ローカルユーザがログインする必要があります。

#### "TOTPを使用してMFA用のローカルユーザアカウントを設定します"

#### 関連情報

の詳細を確認してください ["ONTAP 9での多要素認証 \(TR-4647\) "](#)。

#### TOTPを使用してMFA用のローカルユーザアカウントを設定します

ONTAP 9.13.1以降では、時間ベースのワンタイムパスワード (TOTP) を使用して多要素認証 (MFA) でユーザアカウントを設定できます。

#### 作業を開始する前に

- ストレージ管理者が必要です ["TOTPでMFAを有効にする"](#) ユーザーアカウントの2番目の認証方法として。
- プライマリユーザアカウントの認証方法は、ユーザパスワードまたは公開SSHキーである必要があります。
- スマートフォンと連携するようにTOTPアプリを設定し、TOTPシークレットキーを作成する必要があります。

TOTPは、Google Authenticatorなどのさまざまな認証アプリでサポートされています。

#### 手順

1. 現在の認証方法でユーザーアカウントにログインします。

現在の認証方法は、ユーザパスワードまたはSSH公開鍵である必要があります。

2. アカウントでTOTP設定を作成します。

```
security login totp create -vserver "<svm_name>" -username  
"<account_username >"
```

3. アカウントでTOTP設定が有効になっていることを確認します。

```
security login totp show -vserver "<svm_name>" -username  
"<account_username>"
```

### TOTPシークレットキーをリセットします

アカウントのセキュリティを保護するために、TOTPシークレットキーが侵害されたり紛失したりした場合は、それを無効にして新しいシークレットキーを作成する必要があります。

キーが侵害された場合は**TOTP**をリセットします

TOTPシークレットキーが侵害されたにもかかわらずアクセスできる場合は、侵害されたキーを削除して新しいキーを作成できます。

1. ユーザパスワードまたはSSH公開鍵と侵害されたTOTPシークレットキーを使用してユーザアカウントにログインします。
2. 侵害されたTOTPシークレットキーを削除します。

```
security login totp delete -vserver <svm_name> -username  
<account_username>
```

3. 新しいTOTPシークレットキーを作成します。

```
security login totp create -vserver <svm_name> -username  
<account_username>
```

4. アカウントでTOTP設定が有効になっていることを確認します。

```
security login totp show -vserver <svm_name> -username  
<account_username>
```

キーを紛失した場合は**TOTP**をリセットします

TOTPシークレットキーが失われた場合は、ストレージ管理者に問い合わせてください "[キーを無効にします](#)"。キーが無効になったら、最初の認証方法を使用してログインし、新しいTOTPを設定できます。

作業を開始する前に

ストレージ管理者がTOTPシークレットキーを無効にする必要があります。  
ストレージ管理者アカウントがない場合は、ストレージ管理者に連絡してキーを無効にしてください。

手順

1. ストレージ管理者がTOTPシークレットを無効にしたら、プライマリの認証方法を使用してローカルアカ

ウントにログインします。

## 2. 新しいTOTPシークレットキーを作成します。

```
security login totp create -vserver <svm_name> -username  
<account_username >
```

## 3. アカウントでTOTP設定が有効になっていることを確認します。

```
security login totp show -vserver <svm_name> -username  
<account_username>
```

ローカルアカウントの**TOTP**シークレットキーを無効にします

ローカルユーザの時間ベースのワンタイムパスワード（TOTP）シークレットキーが失われた場合、失われたキーをストレージ管理者が無効にしてからユーザが新しいTOTPシークレットキーを作成する必要があります。

このタスクについて

このタスクは、クラスタ管理者アカウントからのみ実行できます。

ステップ

### 1. TOTPシークレットキーを無効にします。

```
security login totp delete -vserver "<svm_name>" -username  
"<account_username>"
```

**SSL 証明書**アカウントを有効にします

を使用できます security login create コマンドを使用して、管理者アカウントがSSL証明書を使用して管理またはデータSVMにアクセスできるようにします。

このタスクについて

- アカウントが SVM にアクセスするためには、CA 署名済みサーバデジタル証明書をインストールしておく必要があります。

[CA 署名済みサーバ証明書を生成し、インストールする](#)

このタスクは、アカウントアクセスを有効にする前後どちらでも実行できます。

- ログインアカウントに割り当てるアクセス制御ロールが不明な場合は、を使用してあとでロールを追加できます security login modify コマンドを実行します

[管理者に割り当てられているロールの変更](#)



クラスタ管理者アカウントの場合、証明書認証はサポートされます。http、ontapi および rest アプリケーション：SVM管理者アカウントの場合、でのみ証明書認証がサポートされます ontapi および rest アプリケーション：

## ステップ

1. ローカル管理者アカウントが SSL 証明書を使用して SVM にアクセスできるようにします。

```
security login create -vserver SVM_name -user-or-group-name user_or_group_name  
-application application -authmethod authentication_method -role role -comment  
comment
```

コマンド構文全体については、を参照してください ["ONTAP のマニュアルページ - リリース別"](#)。

次のコマンドは、SVM管理者アカウントを有効にします svmadmin2 デフォルトで設定されています vsadmin SVMにアクセスするためのロールengData2 SSLデジタル証明書を使用する。

```
cluster1::>security login create -vserver engData2 -user-or-group-name  
svmadmin2 -application ontapi -authmethod cert
```

## 完了後

CA 署名済みサーバデジタル証明書がインストールされていない場合は、アカウントが SVM にアクセスする前にインストールしておく必要があります。

## CA 署名済みサーバ証明書を生成し、インストールする

### Active Directory アカウントアクセスを有効にします

を使用できます security login create コマンドを使用して、Active Directory (AD) ユーザまたはグループアカウントが管理またはデータSVMにアクセスできるようにします。AD グループのすべてのユーザは、グループに割り当てられたロールを使用して SVM にアクセスできます。

### このタスクについて

- アカウントが SVM にアクセスするためには、AD ドメインコントローラからクラスタまたは SVM へのアクセスを設定しておく必要があります。

### Active Directory ドメインコントローラアクセスを設定しています

このタスクは、アカウントアクセスを有効にする前後どちらでも実行できます。


- ONTAP 9.13.1以降では、ADユーザパスワードを使用して、SSH公開鍵をプライマリまたはセカンダリの認証方式として使用できます。

SSH公開鍵をプライマリ認証として使用することを選択した場合、AD認証は行われません。

- ONTAP 9.11.1以降では、を使用できます ["nsswitch認証のためのLDAP高速バインド"](#) AD LDAPサーバでサポートされている場合。

- ログインアカウントに割り当てるアクセス制御ロールが不明な場合は、を使用します security login modify コマンドを使用してあとでロールを追加します。

管理者に割り当てられているロールの変更



ADグループアカウントへのアクセスは、でのみサポートされます SSH、ontapi および `rest アプリケーション：ADグループは、多要素認証に一般的に使用されるSSH公開鍵認証ではサポートされません。

作業を開始する前に

- クラスタ時間と AD ドメインコントローラの時刻を、誤差が 5 分以内となるように同期する必要があります。
- このタスクを実行するには、クラスタ管理者である必要があります。

ステップ

1. AD のユーザまたはグループ管理者アカウントが SVM にアクセスできるようにします。
  - ADユーザの場合：\*

ONTAPバージョン	プライマリ認証	セカンダリ認証	コマンドを実行します
9.13.1以降	公開鍵	なし	<pre>security login create -vserver &lt;svm_name&gt; -user-or-group-name &lt;user_name&gt; -application ssh -authentication-method publickey -role &lt;role&gt;</pre>



ONTAPバージョン	プライマリ認証	セカンダリ認証	コマンドを実行します
9.13.1以降	ドメイン	公開鍵	<p>新規ユーザーの場合</p> <pre>security login create -vserver &lt;svm_name&gt; -user-or-group-name &lt;user_name&gt; -application ssh -authentication-method domain -second -authentication-method publickey -role &lt;role&gt;</pre> <p>既存のユーザーの場合</p> <pre>security login modify -vserver &lt;svm_name&gt; -user-or-group-name &lt;user_name&gt; -application ssh -authentication-method domain -second -authentication-method publickey -role &lt;role&gt;</pre>
9.0以降	ドメイン	なし	<pre>security login create -vserver &lt;svm_name&gt; -user-or-group-name &lt;user_name&gt; -application &lt;application&gt; -authentication-method domain -role &lt;role&gt; -comment &lt;comment&gt; [-is-ldap-fastbind true]</pre>

。ADグループの場合：\*

ONTAPバージョン	プライマリ認証	セカンダリ認証	コマンドを実行します
9.0以降	ドメイン	なし	<pre>security login create -vserver &lt;svm_name&gt; -user-or-group-name &lt;user_name&gt; -application &lt;application&gt; -authentication-method domain -role &lt;role&gt; -comment &lt;comment&gt; [-is-ldap- fastbind true]</pre>

+

コマンド構文全体については、を参照してください ["管理者認証およびRBAC設定用のワークシート"](#)

完了後

AD ドメインコントローラからクラスタまたは SVM へのアクセスを設定していない場合は、アカウントが SVM にアクセスする前に設定しておく必要があります。

### Active Directory ドメインコントローラアクセスを設定しています

**LDAP** または **NIS** アカウントアクセスを有効にします

を使用できます `security login create` LDAP または NIS のユーザアカウントが管理またはデータ SVM にアクセスできるようにするコマンド。LDAP サーバまたは NIS サーバから SVM へのアクセスを設定していない場合は、アカウントが SVM にアクセスする前に設定しておく必要があります。

このタスクについて

- グループアカウントはサポートされていません。
- アカウントが SVM にアクセスするためには、LDAP サーバまたは NIS サーバから SVM へのアクセスを設定しておく必要があります。

### LDAP サーバまたは NIS サーバのアクセスを設定する

このタスクは、アカウントアクセスを有効にする前後どちらでも実行できます。

- ログインアカウントに割り当てるアクセス制御ロールが不明な場合は、を使用します `security login modify` コマンドを使用してあとでロールを追加します。

### 管理者に割り当てられているロールの変更

- ONTAP 9.4 以降では、LDAP サーバまたは NIS サーバを経由するリモートユーザに対して多要素認証（MFA）がサポートされます。
- ONTAP 9.11.1 以降では、を使用できます "[nsswitch 認証のための LDAP 高速バインド](#)" LDAP サーバでサポートされている場合。
- LDAP 問題は既知のものであるため、は使用しないでください。LDAP ユーザアカウント情報の任意のフィールドの（コロン）文字（例： `gecos`、``userPassword`` など）。そうしないと、そのユーザの検索操作が失敗します。

作業を開始する前に

このタスクを実行するには、クラスタ管理者である必要があります。

手順

1. LDAP または NIS のユーザアカウントまたはグループアカウントが SVM にアクセスできるようにします。

```
security login create -vserver SVM_name -user-or-group-name user_name
-application application -authmethod nsswitch -role role -comment comment -is
-ns-switch-group yes|no [-is-ldap-fastbind true]
```

コマンド構文全体については、を参照してください "[ワークシート](#)"。

"[ログインアカウントを作成または変更する](#)"

次のコマンドは、LDAPまたはNISのクラスタ管理者アカウントを有効にします `guest2` を使用します `backup` 管理SVMにアクセスするためのロール `engCluster`。

```
cluster1::>security login create -vserver engCluster -user-or-group-name
guest2 -application ssh -authmethod nsswitch -role backup
```

## 2. LDAP ユーザまたは NIS ユーザに対して MFA ログインを有効にします。

```
security login modify -user-or-group-name rem_usr1 -application ssh
-authentication-method nsswitch -role admin -is-ns-switch-group no -second
-authentication-method publickey
```

認証方法はと指定できます `publickey` および2番目の認証方法をに設定します `nsswitch`。

次の例では MFA 認証を有効にしています。

```
cluster-1::*> security login modify -user-or-group-name rem_usr2
-application ssh -authentication-method nsswitch -vserver
cluster-1 -second-authentication-method publickey"
```

完了後

LDAP サーバまたは NIS サーバから SVM へのアクセスを設定していない場合は、アカウントが SVM にアクセスする前に設定しておく必要があります。

## LDAP サーバまたは NIS サーバのアクセスを設定する

### アクセス制御ロールを管理します

#### アクセス制御ロールの概要

管理者がアクセスできるコマンドは、管理者に割り当てられたロールで決まります。ロールは管理者のアカウントを作成するときに割り当てます。必要に応じて、別のロールを割り当てたりカスタムロールを定義したりできます。

管理者に割り当てられているロールを変更します

を使用できます `security login modify` コマンドを使用して、クラスタ管理者アカウントまたはSVM管理者アカウントのロールを変更します。事前定義またはカスタムのロールを割り当てることができます。

作業を開始する前に

このタスクを実行するには、クラスタ管理者である必要があります。

#### ステップ

1. クラスタ管理者または SVM 管理者のロールを変更します。

```
security login modify -vserver SVM_name -user-or-group-name user_or_group_name  
-application application -authmethod authentication_method -role role -comment  
comment
```

コマンド構文全体については、を参照してください ["ワークシート"](#)。

### "ログインアカウントを作成または変更する"

次のコマンドは、ADクラスタ管理者アカウントのロールを変更します DOMAIN1\guest1 に移動します readonly ロール。

```
cluster1::>security login modify -vserver engCluster -user-or-group-name  
DOMAIN1\guest1 -application ssh -authmethod domain -role readonly
```

次のコマンドは、ADグループアカウントのSVM管理者アカウントのロールを変更します DOMAIN1\adgroup カスタムに vol\_role ロール。

```
cluster1::>security login modify -vserver engData -user-or-group-name  
DOMAIN1\adgroup -application ssh -authmethod domain -role vol_role
```

### カスタムロールを定義する

を使用できます security login role create カスタムロールを定義するコマンド。このコマンドを必要な回数だけ実行して、ロールに関連付ける機能の正確な組み合わせを実現できます。

#### このタスクについて

- 事前定義かカスタムかにかかわらず、ロールは ONTAP コマンドまたはコマンドディレクトリへのアクセスを許可または拒否します。

コマンドディレクトリ ('volume' など) は、関連するコマンドとコマンドサブディレクトリのグループです。この手順で説明されている場合を除き、コマンドディレクトリへのアクセスを許可または拒否すると、ディレクトリとそのサブディレクトリに含まれる各コマンドへのアクセスが許可または拒否されます。

- 特定のコマンドまたはサブディレクトリへのアクセスは、親ディレクトリへのアクセスよりも優先されます。

あるロールにコマンドディレクトリを定義し、そのあとに親ディレクトリの特定のコマンドまたはサブディレクトリに対して異なるアクセスレベルを定義した場合、そのコマンドまたはサブディレクトリに指定したアクセスレベルが親のアクセスレベルよりも優先されます。



でのみ使用可能なコマンドやコマンドディレクトリへのアクセスを許可するロールをSVM管理者に割り当てることはできません admin クラスタ管理者 (例:) security コマンドディレクトリ。

作業を開始する前に

このタスクを実行するには、クラスタ管理者である必要があります。

## ステップ

### 1. カスタムロールを定義します。

```
security login role create -vserver SVM_name -role role -cmddirname  
command_or_directory_name -access access_level -query query
```

コマンド構文全体については、を参照してください ["ワークシート"](#)。

次のコマンドは、を許可します vol\_role ロールに内のコマンドへのフルアクセス権が付与されます volume コマンドディレクトリ、および内のコマンドへの読み取り専用アクセス volume snapshot サブディレクトリ。

```
cluster1::>security login role create -role vol_role -cmddirname  
"volume" -access all  
  
cluster1::>security login role create -role vol_role -cmddirname "volume  
snapshot" -access readonly
```

次のコマンドは、を許可します SVM\_storage ロール内のコマンドへの読み取り専用アクセス storage コマンドディレクトリ。内のコマンドにはアクセスできません storage encryption サブディレクトリにアクセスし、へのフルアクセスを許可します storage aggregate plex offline 非組み込みコマンド。

```
cluster1::>security login role create -role SVM_storage -cmddirname  
"storage" -access readonly  
  
cluster1::>security login role create -role SVM_storage -cmddirname  
"storage encryption" -access none  
  
cluster1::>security login role create -role SVM_storage -cmddirname  
"storage aggregate plex offline" -access all
```

## クラスタ管理者の事前定義されたロール

ほとんどの場合、クラスタ管理者用に事前定義されたロールで十分です。必要に応じて、カスタムロールを作成することができます。デフォルトでは、クラスタ管理者には事前定義されたが割り当てられます admin ロール。

次の表に、クラスタ管理者用の事前定義されたロールを示します。

ロール	アクセスレベル	コマンドまたはコマンドディレクトリに移動します
-----	---------	-------------------------

管理	すべて	すべてのコマンドディレクトリ (DEFAULT)
Admin-no-FSA (ONTAP 9.12.1以降で利用可能)	読み取り / 書き込み	<ul style="list-style-type: none"> <li>• すべてのコマンドディレクトリ (DEFAULT)</li> <li>• security login rest-role</li> <li>• security login role</li> </ul>
読み取り専用です	<ul style="list-style-type: none"> <li>• security login rest-role create</li> <li>• security login rest-role delete</li> <li>• security login rest-role modify</li> <li>• security login rest-role show</li> <li>• security login role create</li> <li>• security login role create</li> <li>• security login role delete</li> <li>• security login role modify</li> <li>• security login role show</li> <li>• volume activity-tracking</li> <li>• volume analytics</li> </ul>	なし
volume file show-disk-usage	AutoSupport	すべて
<ul style="list-style-type: none"> <li>• set</li> <li>• system node autosupport</li> </ul>	なし	その他すべてのコマンドディレクトリ (DEFAULT)
バックアップ	すべて	vserver services ndmp
<ul style="list-style-type: none"> <li>• 読み取り専用</li> </ul>	volume	なし

その他すべてのコマンドディレクトリ (DEFAULT)	• 読み取り専用	すべて
<ul style="list-style-type: none"> <li>• security login password</li> </ul> <p>自身のユーザアカウントのローカルパスワードとキー情報のみを管理する場合</p> <ul style="list-style-type: none"> <li>• set</li> </ul>	なし	security
• 読み取り専用	その他すべてのコマンドディレクトリ (DEFAULT)	なし



。 autosupport ロールは事前定義されたに割り当てられます autosupport AutoSupport OnDemandで使用されるアカウント。ONTAP では、を変更または削除することはできません autosupport アカウント：また、ONTAP ではを割り当てることもできません autosupport 他のユーザアカウントへのロール。

#### SVM 管理者の事前定義されたロール

SVM 管理者用に、ほとんどのニーズに合わせて事前定義されたロールが用意されています。必要に応じて、カスタムロールを作成することができます。デフォルトでは、SVM 管理者には事前定義されたが割り当てられます vsadmin ロール。

次の表に、SVM 管理者用の事前定義されたロールを示します。

ロール名	機能
vsadmin	<ul style="list-style-type: none"> <li>• 自身のユーザアカウントのローカルパスワードとキー情報を管理します</li> <li>• ボリューム移動を除くボリュームの管理</li> <li>• クォータ、mtree、Snapshot コピー、およびファイルの管理</li> <li>• LUN の管理</li> <li>• privileged delete を除く SnapLock 処理の実行</li> <li>• プロトコルの設定：NFS、SMB、iSCSI、FC、FCoE、NVMe/FCとNVMe/TCP</li> <li>• サービスの設定：DNS、LDAP、NIS</li> <li>• ジョブの監視</li> <li>• ネットワーク接続およびネットワークインターフェイスの監視</li> <li>• SVM の健全性を監視</li> </ul>

vsadmin-volume	<ul style="list-style-type: none"> <li>• 自身のユーザアカウントのローカルパスワードとキー情報を管理します</li> <li>• ボリュームの移動を含む、ボリュームの管理</li> <li>• クォータ、qtree、Snapshot コピー、およびファイルの管理</li> <li>• LUN の管理</li> <li>• プロトコルの設定：NFS、SMB、iSCSI、FC、FCoE、NVMe/FCとNVMe/TCP</li> <li>• サービスの設定：DNS、LDAP、NIS</li> <li>• ネットワークインターフェースの監視</li> <li>• SVM の健全性を監視</li> </ul>
vsadmin-protocol のいずれかです	<ul style="list-style-type: none"> <li>• 自身のユーザアカウントのローカルパスワードとキー情報を管理します</li> <li>• プロトコルの設定：NFS、SMB、iSCSI、FC、FCoE、NVMe/FCとNVMe/TCP</li> <li>• サービスの設定：DNS、LDAP、NIS</li> <li>• LUN の管理</li> <li>• ネットワークインターフェースの監視</li> <li>• SVM の健全性を監視</li> </ul>
vsadmin-backup のストレージシステムで	<ul style="list-style-type: none"> <li>• 自身のユーザアカウントのローカルパスワードとキー情報を管理します</li> <li>• NDMP 処理の管理</li> <li>• リストアしたボリュームを読み取り / 書き込み可能にします</li> <li>• SnapMirror 関係と Snapshot コピーの管理</li> <li>• ボリュームとネットワーク情報の表示</li> </ul>



vsadmin-snaplock	<ul style="list-style-type: none"> <li>• 自身のユーザアカウントのローカルパスワードとキー情報を管理します</li> <li>• ボリューム移動を除くボリュームの管理</li> <li>• クォータ、qtree、Snapshot コピー、およびファイルの管理</li> <li>• privileged delete などの SnapLock 処理の実行</li> <li>• プロトコルの設定：NFSとSMB</li> <li>• サービスの設定：DNS、LDAP、NIS</li> <li>• ジョブの監視</li> <li>• ネットワーク接続およびネットワークインターフェイスの監視</li> </ul>
vsadmin-readonly（読み取り専用	<ul style="list-style-type: none"> <li>• 自身のユーザアカウントのローカルパスワードとキー情報を管理します</li> <li>• SVM の健全性を監視</li> <li>• ネットワークインターフェイスの監視</li> <li>• ボリュームと LUN を表示します</li> <li>• サービスとプロトコルの表示</li> </ul>

## 管理者アクセスの制御

管理者に割り当てるロールによって、System Manager で実行できる機能が決まります。クラスタ管理者と Storage VM 管理者の事前定義されたロールは System Manager から提供されます。ロールは、管理者のアカウントを作成するときに割り当てるか、後で別のロールを割り当てることができます。

アカウントアクセスを有効にした方法によっては、次のいずれかを実行する必要があります。

- ローカルアカウントに公開鍵を関連付けます。
- CA 署名済みサーバデジタル証明書をインストールする。
- AD、LDAP、または NIS アクセスを設定

これらのタスクは、アカウントアクセスを有効にする前後どちらでも実行できます。

管理者にロールを割り当てます

次のように、管理者にロールを割り当てます。

### 手順


1. [\* Cluster]>[Settings]（設定）\*を選択します。
2. 選択するオプション → をクリックします。

3. 選択するオプション **+ Add** [\* ユーザー \*] の下。
4. ユーザー名を指定し、\* 役割 \* のドロップダウンメニューで役割を選択します。
5. ユーザのログイン方法およびパスワードを指定します。

管理者のロールを変更する

管理者のロールを次のように変更します。

手順

1. **[Cluster] > [Settings]** の順にクリックします。
2. ロールを変更するユーザの名前を選択し、をクリックします  ユーザ名の横に表示されます。
3. **[編集 (Edit)]** をクリックします。
4. **[\*Role]** のドロップダウンメニューで、ロールを選択します。

## 管理者アカウントを管理する

管理者アカウントの管理の概要

アカウントアクセスを有効にした方法によっては、ローカルアカウントへの公開鍵の関連付け、CA 署名済みサーバデジタル証明書のインストール、AD、LDAP、NIS のアクセスの設定などが必要になる場合があります。これらのタスクはすべて、アカウントアクセスを有効にする前後どちらでも実行できます。

管理者アカウントに公開鍵を関連付けます

SSH 公開鍵認証を使用する場合、アカウントが SVM にアクセスするためには、管理者アカウントに公開鍵を関連付ける必要があります。を使用できます `security login publickey create` 管理者アカウントにキーを関連付けるコマンド。

このタスクについて

SSH でのアカウントの認証にパスワードと SSH 公開鍵の両方を使用する場合、アカウントはまず公開鍵を使用して認証されます。

作業を開始する前に

- SSH キーを生成しておく必要があります。
- このタスクを実行するには、クラスタ管理者または SVM の管理者である必要があります。

手順

1. 管理者アカウントに公開鍵を関連付けます。

```
security login publickey create -vserver SVM_name -username user_name -index  
index -publickey certificate -comment comment
```

コマンド構文全体については、のワークシートリファレンスを参照してください ["ユーザアカウントへの公開鍵の関連付け"](#)。

## 2. 公開鍵を表示して変更を確認します。

```
security login publickey show -vserver SVM_name -username user_name -index index
```

### 例

次のコマンドは、SVM管理者アカウントに公開鍵を関連付けます `svmadmin1` SVM用 `engData1`。公開鍵のインデックス番号は 5 です。

```
cluster1::> security login publickey create -vserver engData1 -username svmadmin1 -index 5 -publickey "<key text>"
```

## 管理者アカウントのSSH公開鍵とX.509証明書を管理します

管理者アカウントによるSSH認証のセキュリティを強化するには、を使用します

`security login publickey` SSH公開鍵およびそのX.509証明書との関連付けを管理するための一連のコマンド。

公開鍵とX.509証明書を管理者アカウントに関連付けます

ONTAP 9.13.1以降では、管理者アカウントに関連付けた公開鍵にX.509証明書を関連付けることができます。これにより、そのアカウントのSSHログイン時の証明書の有効期限または失効チェックのセキュリティが強化されます。

### このタスクについて

SSH公開鍵とX.509証明書の両方を使用してSSH経由でアカウントを認証する場合、ONTAPは、SSH公開鍵を使用して認証する前にX.509証明書の有効性をチェックします。証明書の有効期限が切れているか失効している場合、SSHログインは拒否され、公開鍵は自動的に無効になります。

### 作業を開始する前に

- このタスクを実行するには、クラスタ管理者または SVM の管理者である必要があります。
- SSH キーを生成しておく必要があります。
- X.509証明書の有効期限のみを確認する必要がある場合は、自己署名証明書を使用できます。
- X.509証明書の有効期限と失効を確認する必要がある場合は、次の手順を実行します。
  - 認証局（CA）から証明書を受け取っておく必要があります。
  - を使用して証明書チェーン（中間およびルートCA証明書）をインストールする必要があります  
`security certificate install` コマンド
  - SSHに対してOCSPを有効にする必要があります。を参照してください ["OCSP を使用してデジタル証明書が有効であることを確認します"](#) 手順については、を参照し

### 手順

#### 1. 公開鍵とX.509証明書を管理者アカウントに関連付けます。

```
security login publickey create -vserver SVM_name -username user_name -index
```

```
index -publickey certificate -x509-certificate install
```

コマンド構文全体については、のワークシートリファレンスを参照してください ["ユーザアカウントへの公開鍵の関連付け"](#)。

2. 公開鍵を表示して変更を確認します。

```
security login publickey show -vserver SVM_name -username user_name -index  
index
```

#### 例

次のコマンドは、公開鍵とX.509証明書をSVM管理者アカウントに関連付けます svmadmin2 SVM用 engData2。公開鍵にはインデックス番号6が割り当てられます。

```
cluster1::> security login publickey create -vserver engData2 -username  
svmadmin2 -index 6 -publickey  
"<key text>" -x509-certificate install  
Please enter Certificate: Press <Enter> when done  
<certificate text>
```

管理者アカウントの**SSH**公開鍵から証明書の関連付けを削除します

公開鍵を保持したまま、アカウントのSSH公開鍵から現在の証明書の関連付けを削除できます。

作業を開始する前に

このタスクを実行するには、クラスタ管理者または SVM の管理者である必要があります。

#### 手順

1. 管理者アカウントからX.509証明書の関連付けを削除し、既存のSSH公開鍵を保持します。

```
security login publickey modify -vserver SVM_name -username user_name -index  
index -x509-certificate delete
```

2. 公開鍵を表示して変更を確認します。

```
security login publickey show -vserver SVM_name -username user_name -index  
index
```

#### 例

次のコマンドは、X.509証明書の関連付けをSVM管理者アカウントから削除します svmadmin2 SVM用 engData2 インデックス番号6です。

```
cluster1::> security login publickey modify -vserver engData2 -username  
svmadmin2 -index 6 -x509-certificate delete
```

管理者アカウントから公開鍵と証明書に関連付けを削除します

アカウントから現在の公開鍵と証明書の設定を削除できます。

作業を開始する前に

このタスクを実行するには、クラスタ管理者または SVM の管理者である必要があります。

手順

1. 管理者アカウントから公開鍵とX.509証明書の関連付けを削除します。

```
security login publickey delete -vserver SVM_name -username user_name -index index
```

2. 公開鍵を表示して変更を確認します。

```
security login publickey show -vserver SVM_name -username user_name -index index
```

例

次のコマンドは、SVM管理者アカウントから公開鍵とX.509証明書を削除します `svmadmin3` SVM用 `engData3` インデックス番号7です。

```
cluster1::> security login publickey delete -vserver engData3 -username svmadmin3 -index 7
```

## SSHログイン用のCisco Duo 2FAの設定

ONTAP 9.14.1以降では、SSHログイン時に2要素認証（2FA）にCisco Duoを使用するようにONTAPを設定できます。Duoはクラスタレベルで設定し、IT環境はデフォルトですべてのユーザーアカウントを設定します。また、Storage VM（旧称Vserver）のレベルでDuoを設定することもできます。その場合は、そのStorage VMのユーザにのみ適用されます。Duoを有効にして設定すると、追加の認証方式として機能し、すべてのユーザの既存の方式を補完します。

SSHログインでDuo認証を有効にした場合、ユーザは次回SSHを使用してログインするときにデバイスを登録する必要があります。登録情報については、『Cisco Duo ["登録に関するドキュメント"](#)』。

Cisco Duoでは、ONTAPコマンドラインインターフェイスを使用して次のタスクを実行できます。

- [Cisco Duoの設定](#)
- [Cisco Duo設定の変更](#)
- [Cisco Duo設定の削除](#)
- [Cisco Duo設定の表示](#)
- [Duoグループの削除](#)
- [Duoグループの表示](#)

- [ユーザーのDuo認証をバイパスする](#)

## Cisco Duoの設定

Cisco Duo構成は、クラスタ全体または特定のStorage VM（ONTAP CLIではVserverと呼ばれます）に対して、次のコマンドを使用して作成できます。 `security login duo create` コマンドを実行しますこれを行うと、このクラスタまたはStorage VMのSSHログインでCisco Duoが有効になります。

### 手順

1. Cisco Duo管理パネルにログインします。
2. [アプリケーション]>[UNIXアプリケーション]\*に移動します。
3. 統合キー、シークレットキー、およびAPIホスト名を記録します。
4. SSHを使用してONTAPアカウントにログインします。
5. このStorage VMに対してCisco Duo認証を有効にし、環境の情報を括弧内の値に置き換えます。

```
security login duo create \  
-vserver <STORAGE_VM_NAME> \  
-integration-key <INTEGRATION_KEY> \  
-secret-key <SECRET_KEY> \  
-apihost <API_HOSTNAME>
```

このコマンドの必須パラメータおよびオプションパラメータの詳細については、[を参照してください。 "管理者認証と RBAC 設定用のワークシートです"](#)。

## Cisco Duo設定の変更

Cisco Duoがユーザを認証する方法（指定される認証プロンプトの数、使用されるHTTPプロキシなど）を変更できます。Storage VM（ONTAP CLIではVserver）のCisco Duo設定を変更する必要がある場合は、`security login duo modify` コマンドを実行します

### 手順

1. Cisco Duo管理パネルにログインします。
2. [アプリケーション]>[UNIXアプリケーション]\*に移動します。
3. 統合キー、シークレットキー、およびAPIホスト名を記録します。
4. SSHを使用してONTAPアカウントにログインします。
5. このStorage VMのCisco Duo構成を変更します。括弧内の値は、環境から更新された情報に置き換えてください。

```
security login duo modify \  
-vserver <STORAGE_VM_NAME> \  
-integration-key <INTEGRATION_KEY> \  
-secret-key <SECRET_KEY> \  
-apihost <API_HOSTNAME> \  
-pushinfo true|false \  
-http-proxy <HTTP_PROXY_URL> \  
-autopush true|false \  
-prompts 1|2|3 \  
-max-unenrolled-logins <NUM_LOGINS> \  
-is-enabled true|false \  
-fail-mode safe|secure
```

### Cisco Duo設定の削除

Cisco Duo設定を削除すると、SSHユーザがログイン時にDuoを使用して認証する必要がなくなります。Storage VM（ONTAP CLIではVserverと呼ばれます）のCisco Duo設定を削除するには、`security login duo delete` コマンドを実行します

#### 手順

1. SSHを使用してONTAPアカウントにログインします。
2. このStorage VMのCisco Duo設定を削除します。Storage VM名は <STORAGE\_VM\_NAME>：

```
security login duo delete -vserver <STORAGE_VM_NAME>
```

これにより、このStorage VMのCisco Duo設定が完全に削除されます。

### Cisco Duo設定の表示

Storage VM（ONTAP CLIではVserverと表示されます）の既存のCisco Duo構成を表示するには、`security login duo show` コマンドを実行します

#### 手順

1. SSHを使用してONTAPアカウントにログインします。
2. このStorage VMのCisco Duo設定を表示します。必要に応じて、を使用できます `vserver` Storage VMを指定するパラメータ。Storage VM名は <STORAGE\_VM\_NAME>：

```
security login duo show -vserver <STORAGE_VM_NAME>
```

次のような出力が表示されます。

```
Vserver: testcluster
Enabled: true

Status: ok
INTEGRATION-KEY: DI89811J9JWMJCCO7IOH
SKEY SHA Fingerprint:
b79ffa4b1c50b1c747fbacdb34g671d4814
API Host: api-host.duosecurity.com
Autopush: true
Push info: true
Failmode: safe
Http-proxy: 192.168.0.1:3128
Prompts: 1
Comments: -
```

### Duoグループの作成

Cisco Duoでは、特定のActive Directory、LDAP、またはローカルユーザグループのユーザだけをDuo認証プロセスに含めるように設定できます。Duoグループを作成すると、そのグループ内のユーザーのみがDuo認証を求められます。Duoグループを作成するには、`security login duo group create` コマンドを実行します。グループを作成するときに、必要に応じて、そのグループ内の特定のユーザーをDuo認証プロセスから除外することができます。

#### 手順

1. SSHを使用してONTAPアカウントにログインします。
2. Duoグループを作成し、環境の情報を括弧内の値に置き換えます。を省略した場合は、`-vserver` パラメータを指定すると、グループはクラスタレベルで作成されます。

```
security login duo group create -vserver <STORAGE_VM_NAME> -group-name
<GROUP_NAME> -exclude-users <USER1, USER2>
```

Duoグループの名前は、Active Directory、LDAP、またはローカルグループと一致している必要があります。オプションで指定するユーザ `-exclude-users` パラメータはDuo認証プロセスに含まれません。

### Duoグループの表示

既存のCisco Duoグループエントリを表示するには、`security login duo group show` コマンドを実行します。

#### 手順

1. SSHを使用してONTAPアカウントにログインします。
2. Duoグループのエントリを表示します。括弧内の値は、環境の情報に置き換えてください。を省略した場合は、`-vserver` パラメータを指定すると、グループはクラスタレベルで表示されます。



```
security login duo group show -vserver <STORAGE_VM_NAME> -group-name  
<GROUP_NAME> -exclude-users <USER1, USER2>
```

Duoグループの名前は、Active Directory、LDAP、またはローカルグループと一致している必要があります。オプションで指定するユーザ `-exclude-users` パラメータは表示されません。

### Duoグループの削除

Duoグループのエントリを削除するには、`security login duo group delete` コマンドを実行します。グループを削除すると、そのグループのユーザはDuo認証プロセスに含まれなくなります。

#### 手順

1. SSHを使用してONTAPアカウントにログインします。
2. Duoグループエントリを削除し、環境内の情報を括弧内の値に置き換えます。を省略した場合は、`-vserver` パラメータを指定すると、グループはクラスタレベルで削除されます。

```
security login duo group delete -vserver <STORAGE_VM_NAME> -group-name  
<GROUP_NAME>
```

Duoグループの名前は、Active Directory、LDAP、またはローカルグループと一致している必要があります。

### ユーザーのDuo認証をバイパスする

すべてのユーザーまたは特定のユーザーをDuo SSH認証プロセスから除外できます。

#### すべてのDuoユーザーを除外

すべてのユーザに対してCisco Duo SSH認証をディセーブルにできます。

#### 手順

1. SSHを使用してONTAPアカウントにログインします。
2. SSHユーザに対してCisco Duo認証を無効にします（SVM名をに置き換えてください）。  
`<STORAGE_VM_NAME>`：

```
security login duo -vserver <STORAGE_VM_NAME> -is-duo-enabled-false
```

### Duoグループユーザーを除外

Duoグループの一部である特定のユーザーを、Duo SSH認証プロセスから除外できます。

#### 手順

1. SSHを使用してONTAPアカウントにログインします。

2. グループ内の特定のユーザに対してCisco Duo認証をディセーブルにします。括弧内の値は、除外するグループ名とユーザのリストに置き換えてください。

```
security login group modify -group-name <GROUP_NAME> -exclude-users  
<USER1, USER2>
```

Duoグループの名前は、Active Directory、LDAP、またはローカルグループと一致している必要があります。で指定するユーザ `-exclude-users` パラメータはDuo認証プロセスに含まれません。

## ローカルDuoユーザを除外

Cisco Duo管理パネルを使用すると、特定のローカルユーザをDuo認証の使用から除外できます。手順については、を参照してください "[Cisco Duoマニュアル](#)"。

## CA 署名済みサーバ証明書の概要を生成してインストールする

本番用システムでは、クラスタまたは SVM を SSL サーバとして認証する際に使用する CA 署名デジタル証明書をインストールすることを推奨します。を使用できます `security certificate generate-csr` 証明書署名要求（CSR）を生成するコマンドと `security certificate install` 認証局から返された証明書をインストールするコマンド。

### 証明書署名要求を生成します

を使用できます `security certificate generate-csr` 証明書署名要求（CSR）を生成するコマンド。要求が処理されると、署名済みのデジタル証明書が認証局（CA）から送信されます。

### 作業を開始する前に

このタスクを実行するには、クラスタ管理者または SVM の管理者である必要があります。

### 手順

1. CSR を生成します

```
security certificate generate-csr -common-name FQDN_or_common_name -size  
512|1024|1536|2048 -country country -state state -locality locality  
-organization organization -unit unit -email-addr email_of_contact -hash  
-function SHA1|SHA256|MD5
```

次のコマンドでは、米国カリフォルニア州サニーベールにある企業（カスタム共通名「`server1.companyname.com`」）の「IT」部門の「ソフトウェア」グループが使用する、「SHA256」ハッシュ関数で生成される2,048ビット秘密鍵を使用してCSRを作成します。SVM担当管理者のEメールアドレスは「[web@example.com](mailto:web@example.com)」です。CSR と秘密鍵が出力に表示されます。

```
cluster1::>security certificate generate-csr -common-name
server1.companyname.com -size 2048 -country US -state California
-locality Sunnyvale -organization IT -unit Software -email-addr
web@example.com -hash-function SHA256
```

Certificate Signing Request :

-----BEGIN CERTIFICATE REQUEST-----

```
MIIBGjCBxQIBADBgMRQwEgYDVQQDEwtleGFtcGxlLmNvbTElMAkGA1UEBhMCVVMx
CTAHBgNVBAGTADEJMAcGA1UEBxMAMQkwBwYDVQQKEwAxCTAHBgNVBAsTADEPMA0G
CSqGSIB3DQEJARYAMFwwDQYJKoZIhvcNAQEBBQADSwAwSAJBAPXFanNoJApTlnzS
xOcxixqImRRGZCR7tVmTYyqPSuTvfVtWdJbmXuj6U3alwoUsb13wfEvQnHVFNCi
2ninsJ8CAwEAAaAAMA0GCSqGSIB3DQEBChUAA0EA6EagLfso5+4g+ejiRKKTUPQO
UqOUeOkuvxhOvPC2w7b//fNSFsFHvXloqEOhYECn/NX9h8mbphCoM5YZ4OfnKw==
-----END CERTIFICATE REQUEST-----
```

Private Key :

-----BEGIN RSA PRIVATE KEY-----

```
MIIBOwIBAAJBAPXFanNoJApTlnzSxOcxixqImRRGZCR7tVmTYyqPSuTvfVtWdJb
mXuj6U3alwoUsb13wfEvQnHVFNCi2ninsJ8CAwEAAQJAWt2AO+bW3FKezEuIrQlu
KoMyRYK455wtMk8BrOyJfhYsB20B28eifjJvRWdTOBEav99M7cEzgPv+p5kaZTTM
gQIhAPsp+j1hrUXSRj979LIJY0sNez397i7ViFXWQScx/ehAiEA+oDbOooWlVvu
xj4aitxVBu6ByVckYU8LbsfeRNsZwD8CIQCbZ1/ENvmlJ/P7N9Exj2NCtEYxd0Q5
cwBZ5NfZeMBpwQIhAPk0KWQSLadGfsKO077itF+h9FGFNHbtuNTrVq4vPW3nAiAA
peMBQgEv28y2r8D4dkYzxcXmjzJluUSZSZ9c/wS6fA==
```

-----END RSA PRIVATE KEY-----

Note: Please keep a copy of your certificate request and private key for future reference.

2. CSR 出力の証明書要求をデジタル形式（Eメールなど）で信頼できるサードパーティの CA に送信し、署名を求めます。

要求が処理されると、署名済みのデジタル証明書が CA から送信されます。秘密鍵と CA 署名デジタル証明書のコピーは保管する必要があります。

#### CA 署名済みサーバ証明書をインストールします

を使用できます security certificate install CA署名済みサーバ証明書をSVMにインストールするコマンドONTAP は、サーバ証明書の証明書チェーンを形成する、認証局（CA）のルート証明書と中間証明書の入力求めます。

作業を開始する前に

このタスクを実行するには、クラスタ管理者または SVM の管理者である必要があります。

#### ステップ

1. CA署名済みサーバ証明書をインストールします。

```
security certificate install -vserver SVM_name -type certificate_type
```

コマンド構文全体については、を参照してください "[ワークシート](#)"。



ONTAP から、サーバ証明書の証明書チェーンを形成する CA ルート証明書と中間証明書の入力を求められます。チェーンは、サーバ証明書を発行した CA の証明書から始まり、CA のルート証明書まで続く場合があります。中間証明書が 1 つでも抜けていると、サーバ証明書のインストールに失敗します。

次のコマンドは、CA署名済みサーバ証明書と中間証明書をSVM「engData2」にインストールします。

```
cluster1::>security certificate install -vserver engData2 -type
server
Please enter Certificate: Press <Enter> when done
-----BEGIN CERTIFICATE-----
MIIB8TCCA ZugAwIBAwIBADANBgkqhkiG9w0BAQQFADBfMRMwEQYDVQQDEwpuZXRh
cHAuY29tMQswCQYDVQQGEwJVUzEJMACGA1UECBMAMQkwBwYDVQQHEwAxCTAHBgNV
BAoTADBJMACGA1UECzMAMQ8wDQYJKoZIhvcNAQkBFgAwHhcNMTAwNDI2MTk0OTI4
WhcNMTAwNTI2MTk0OTI4WjBfMRMwEQYDVQQDEwpuZXRhcHAuY29tMQswCQYDVQQG
EwJVUzEJMACGA1UECBMAMQkwBwYDVQQHEwAxCTAHBgNVBAoTADBJMACGA1UECzMA
MQ8wDQYJKoZIhvcNAQkBFgAwXDANBgkqhkiG9w0BAQEFAANLADBIaKEAyXrK2sry
-----END CERTIFICATE-----
```

```
Please enter Private Key: Press <Enter> when done
-----BEGIN RSA PRIVATE KEY-----
MIIBPAIBAAJBAMl6ytrK8nQj82UsWeHOeT8gk0BPX+Y5MLyCsUdXA7hXhumHNpvF
C61X2G32Sx8VEa1th94tx+vOEzq+UaqHlt0CAwEAAQJBAMZjDWlgmlm3qIr/n8VT
PFnnZnbVcXVM70tbUsgPKw+QCCh9dF1jmuQKeDr+wUMWkn1DeGrfhILpzfJGHRlJ
z7UCIQDr8d3gOG71UyX+BbFmo/N0uAKjS2cvUU+Y8a8pDxGLLwIhANqa99SuS18U
DiPvdaKTj6+EcGuXfCXz+G0rfgTZK8uzAiEArlmnrFYC8KwE9k7A0ylRzBLdUwK9
AvuJDn+/z+H1Bd0CIQDD93P/xpaJETNz53Au49VE5Jba/Jugckrbosd/lSd7nQIg
aEMAZt6qHHT4mndi8Bo8sDGedG2SKx6Qbn2IpuNZ7rc=
-----END RSA PRIVATE KEY-----
```

Do you want to continue entering root and/or intermediate  
certificates {y|n}: y

```
Please enter Intermediate Certificate: Press <Enter> when done
-----BEGIN CERTIFICATE-----
MIIE+zCCBGsgAwIBAgICAQ0wDQYJKoZIhvcNAQEFBQAwwbsxJDAiBgNVBAcTG1Zh
bGlDZXJ0IFZhbGlkYXRpb24gTmV0d29yazEXMBUGA1UEChMOVmFsaUNlcnQsIElu
Yy4xNTAzBgNVBAsTTFZhbGlDZXJ0IENsYXNzIDIGUG9saWN5IFZhbGlkYXRpb24g
QXV0aG9yaXR5MSEwHwYDVQQDEwhodHRwOi8vd3d3LnZhbGljZXJ0LmNvbS8xIDAe
BgkqhkiG9w0BCQEWEluZm9AdmFsaWNlcnQuY29tMB4XDTA0MDYyOTE3MDYyMFoX
DTI0MDYyOTE3MDYyMFowYzELMAkGA1UEBhMCVVMxITAfBgNVBAoTGFroZSBHbyBE
YWRkeSBHcm91cCwgSW5jLjExMC8GA1UECzMOR28gRGFkZkZkkgQ2xhc3MgMiBDZXJ0
-----END CERTIFICATE-----
```

Do you want to continue entering root and/or intermediate  
certificates {y|n}: y

```
Please enter Intermediate Certificate: Press <Enter> when done
-----BEGIN CERTIFICATE-----
```

```
MIIC5zCCAlACAQEwDQYJKoZIhvcNAQEFBQAwbgsxJDAiBgNVBACGTG1ZhbG1DZXJ0
IFZhbG1kYXRpb24gTmV0d29yazEXMBUGA1UEChMOVmFsaUNlcnQsIEluYy4xNTAz
BgNVBAsTTFZhbG1DZXJ0IENsYXNzIDIGUG9saWN5IFZhbG1kYXRpb24gQXV0aG9y
aXR5MSEwHwYDVQQDEExodHRwOi8vd3d3LnZhbG1jZXJ0LmNvbS8xIDAeBgkqhkiG
9w0BCQEWEluZm9AdmFsaWNlcnQuY29tMB4XDtk5MDYyNjAwMTk1NFoXDTE5MDYy
NjAwMTk1NFowgbsxJDAiBgNVBACGTG1ZhbG1DZXJ0IFZhbG1kYXRpb24gTmV0d29y
azEXMBUGA1UEChMOVmFsaUNlcnQsIEluYy4xNTAzBgNVBAsTTFZhbG1DZXJ0IENs
YXNzIDIGUG9saWN5IFZhbG1kYXRpb24gQXV0aG9yaXR5MSEwHwYDVQQDEExodHRw
-----END CERTIFICATE-----
```

Do you want to continue entering root and/or intermediate  
certificates {y|n}: n

You should keep a copy of the private key and the CA-signed digital  
certificate for future reference.

## System Manager を使用して証明書を管理します


ONTAP 9.10.1 以降では、System Manager を使用して、信頼される認証局、クライアント / サーバ証明書、ローカル（オンボード）認証局を管理できます。

System Manager では、他のアプリケーションから受信した証明書を管理して、それらのアプリケーションからの通信を認証できます。システムを他のアプリケーションに識別する独自の証明書を管理することもできます。

証明書情報を表示します

System Manager を使用すると、信頼された認証局、クライアント / サーバ証明書、およびクラスタに格納されているローカルの認証局を表示できます。

手順

1. System Manager で、\* Cluster > Settings \* の順に選択します。
2. [\* セキュリティ \* (\* Security \*) ] 領域までスクロールします。  
[\* 証明書 \*] セクションには、次の詳細が表示されます。
  - 保存されている信頼された認証局の数。
  - 保存されているクライアント / サーバ証明書の数。
  - 保存されているローカル認証局の数。
3. 任意の数を選択して証明書のカテゴリの詳細を表示するか、 をクリックして \* 証明書 \* ページを開きます。このページには、すべてのカテゴリに関する情報が含まれています。  
リストには、クラスタ全体の情報が表示されます。特定の Storage VM の情報のみを表示する場合は、次の手順を実行します。
  - a. [ストレージ]>[Storage VM]\* を選択します。
  - b. Storage VM を選択してください。

- c. [設定]タブに切り替えます。
- d. [証明書]セクションに表示されている番号を選択します。

次に何をするか

- [ \* 証明書 \* ] ページでは、次の操作を実行できます [\[証明書署名要求を生成します\]](#)。
- 証明書の情報は、カテゴリごとに 1 つずつ、3 つのタブに分けられます。各タブでは、次のタスクを実行できます。

タブ	実行できる手順
<ul style="list-style-type: none"> <li>• 信頼された認証機関 *</li> </ul>	<ul style="list-style-type: none"> <li>• <a href="#">[install-trusted-cert]</a></li> <li>• <a href="#">[信頼された認証局を削除します]</a></li> <li>• <a href="#">[信頼された認証局を更新してください]</a></li> </ul>
<ul style="list-style-type: none"> <li>• クライアント / サーバ証明書 *</li> </ul>	<ul style="list-style-type: none"> <li>• <a href="#">[install-cs-cert]</a></li> <li>• <a href="#">[gen-cs-cert]</a></li> <li>• <a href="#">[delete-cs-cert]</a></li> <li>• <a href="#">[renew-cs-cert]</a></li> </ul>
<ul style="list-style-type: none"> <li>• ローカル認証局 *</li> </ul>	<ul style="list-style-type: none"> <li>• <a href="#">[新しいローカル認証局を作成します]</a></li> <li>• <a href="#">[ローカルの認証局を使用して証明書に署名します]</a></li> <li>• <a href="#">[ローカル認証局を削除します]</a></li> <li>• <a href="#">[ローカルの認証局を更新してください]</a></li> </ul>

証明書署名要求を生成します

証明書署名要求（CSR）は、Certificate \* ページの任意のタブから System Manager で生成できます。秘密鍵と対応する CSR が生成されます。これには認証局を使用して署名し、パブリック証明書を生成できます。


手順

1. [ \* 証明書 \* ] ページを表示します。を参照してください [\[証明書情報を表示します\]](#)。
2. [+ CSRの生成]\*を選択します。
3. 件名の情報を入力します。
  - a. \* 共通名 \* を入力します。
  - b. \* 国 \* を選択します。
  - c. \* 組織 \* を入力します。
  - d. \* 組織単位 \* を入力します。
4. デフォルト値を上書きする場合は、\* その他のオプション \* を選択して追加情報を指定します。

信頼できる認証局をインストール（追加）します

System Manager に信頼された追加の認証局をインストールできます。

#### 手順

1. **[Trusted Certificate Authorities]** タブを表示します。を参照してください [\[証明書情報を表示します\]](#)。
2. 選択するオプション  **+ Add**。
3. **[Add Trusted Certificate Authority\*]** パネルで、次の手順を実行します。
  - \* 名 \* を入力します。
  - スコープ \* には、Storage VM を選択します。
  - \* 共通名 \* を入力します。
  - \* タイプ \* を選択します。
  - 証明書の詳細を入力またはインポートします。 \*


信頼された認証局を削除します

System Manager を使用して、信頼された認証局を削除できます。



ONTAPがプリインストールされている信頼された認証局は削除できません。


#### 手順

1. **[Trusted Certificate Authorities]** タブを表示します。を参照してください [\[証明書情報を表示します\]](#)。
2. 信頼された認証局の名前を選択します。
3. 選択するオプション  名前の横にある\*[削除]\*を選択します。

信頼された認証局を更新してください

System Manager を使用すると、有効期限が切れている、または有効期限が近づいている信頼された認証局を更新できます。


#### 手順

1. **[Trusted Certificate Authorities]** タブを表示します。を参照してください [\[証明書情報を表示します\]](#)。
2. 信頼された認証局の名前を選択します。
3. 選択するオプション  証明書名の横にある\*更新\*。

クライアント / サーバ証明書をインストール（追加）します

System Manager では、追加のクライアント / サーバ証明書をインストールできます。

#### 手順

1. クライアント / サーバ証明書 \* タブを表示します。を参照してください [\[証明書情報を表示します\]](#)。
2. 選択するオプション  **+ Add**。
3. **[Add Client/Server Certificate]** パネルで、次の手順を実行します。



- \* 証明書名 \* を入力します。
- スコープ \* には、Storage VM を選択します。
- \* 共通名 \* を入力します。
- \* タイプ \* を選択します。
- 証明書の詳細を入力またはインポートします。 \*  
 テキストファイルから証明書の詳細を入力またはコピーして貼り付けることも、\* Import \* をクリックして証明書ファイルからテキストをインポートすることもできます。
- 秘密鍵\*を入力します。  
 テキストファイルから秘密キーを入力するか、コピーして貼り付けるか、\* インポート \* をクリックして秘密キーファイルからテキストをインポートすることができます。

自己署名クライアント / サーバ証明書を生成（追加）します

System Manager では、追加の自己署名クライアント / サーバ証明書を生成できます。


手順

1. クライアント / サーバ証明書 \* タブを表示します。を参照してください [\[証明書情報を表示します\]](#)。
2. [+自己署名証明書の生成]\*を選択します。
3. 自己署名証明書の生成 \* パネルで、次の手順を実行します。
  - \* 証明書名 \* を入力します。
  - スコープ \* には、Storage VM を選択します。
  - \* 共通名 \* を入力します。
  - \* タイプ \* を選択します。
  - \* ハッシュ関数 \* を選択します。
  - \* キーサイズ \* を選択します。
  - Storage VM \* を選択します。

クライアント / サーバ証明書を削除します

System Manager では、クライアント / サーバ証明書を削除できます。

手順


1. クライアント / サーバ証明書 \* タブを表示します。を参照してください [\[証明書情報を表示します\]](#)。
2. クライアント / サーバ証明書の名前を選択します。
3. 選択するオプション  名前の横にある \* 削除 \* をクリックします。

クライアント / サーバ証明書を更新します

System Manager を使用して、有効期限が切れている、または有効期限が近づいているクライアント / サーバ証明書を更新できます。

手順

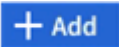
1. クライアント / サーバ証明書 \* タブを表示します。を参照してください [\[証明書情報を表示します\]](#)。

2. クライアント/サーバ証明書の名前を選択します。
3. 選択するオプション  名前の横にある \* Renew \*（更新）をクリックします。

新しいローカル認証局を作成します

System Manager を使用して、新しいローカル認証局を作成できます。


手順

1. [ ローカル証明機関 \* ] タブを表示します。 を参照してください [\[証明書情報を表示します\]](#)。
2. 選択するオプション  **+ Add**。
3. [Add Local Certificate Authority\*] パネルで、次の手順を実行します。
  - \* 名 \* を入力します。
  - スコープ \* には、Storage VM を選択します。
  - \* 共通名 \* を入力します。
4. デフォルト値を上書きする場合は、\* その他のオプション \* を選択して追加情報を指定します。

ローカルの認証局を使用して証明書に署名します

System Manager では、ローカルの認証局を使用して証明書に署名できます。

手順

1. [ ローカル証明機関 \* ] タブを表示します。 を参照してください [\[証明書情報を表示します\]](#)。
2. ローカル認証局の名前を選択します。
3. 選択するオプション  名前の横にある\*証明書に署名\*。
4. [ 証明書署名要求に署名する \* ] フォームに入力します。
  - 証明書署名のコンテンツを貼り付けるか、\* Import \* をクリックして証明書署名要求ファイルをインポートできます。
  - 証明書を有効にする日数を指定します。

ローカル認証局を削除します

System Manager では、ローカルの認証局を削除できます。


手順

1. [ ローカル認証局 ] タブを表示します。 を参照してください [\[証明書情報を表示します\]](#)。
2. ローカル認証局の名前を選択します。
3. 選択するオプション  名前の横にある\* Delete \*をクリックします。

ローカルの認証局を更新してください

System Manager を使用して、有効期限が切れた、または有効期限が近づいているローカルの認証局を更新できます。

手順

1. [ ローカル認証局 ] タブを表示します。を参照してください [\[証明書情報を表示します\]](#)。
2. ローカル認証局の名前を選択します。
3. 選択するオプション  名前の横にある \* Renew \* （更新）をクリックします。

#### Active Directory ドメインコントローラアクセスの概要を設定する

AD アカウントから SVM にアクセスするためには、AD ドメインコントローラからクラスタまたは SVM へのアクセスを設定しておく必要があります。データ SVM 用に SMB サーバをすでに設定している場合は、クラスタへの AD アクセス用に SVM をゲートウェイまたは *tunnel* として設定できます。SMB サーバを設定していない場合は、AD ドメインに SVM 用のコンピュータアカウントを作成できます。

ONTAP は、次のドメインコントローラ認証サービスをサポートしています。

- Kerberos
- LDAP
- Netlogon
- ローカルセキュリティ局（LSA）

ONTAP は、次のセッションキーアルゴリズムをサポートしており、セキュアな Netlogon 接続を実現します。

セッションキーアルゴリズム	使用可能なバージョン
HMAC-SHA256（Advanced Encryption Standard（AES）に基づく）  クラスタでONTAP 9.9.1以前が実行されていて、ドメインコントローラでセキュアなネットログオンサービスにAESが適用されている場合は、接続が失敗します。この場合、代わりにONTAPとの強力なキー接続を受け入れるようにドメインコントローラを再設定する必要があります。	ONTAP 9.10.1
DES および HMAC-MD5（強力なキーが設定されている場合）	ONTAP 9 のすべてのリリース

ネットログオンでのセキュアチャネルの確立中にAESセッションキーを使用する場合は、SVMでAESが有効になっていることを確認する必要があります。

- ONTAP 9.14.1以降では、SVMの作成時にAESがデフォルトで有効になり、ネットログオンでのセキュアチャネルの確立時にAESセッションキーを使用するようにSVMのセキュリティ設定を変更する必要はありません。
- ONTAP 9.10.1~9.13.1では、SVMの作成時にAESがデフォルトで無効になります。次のコマンドを使用してAESを有効にする必要があります。

```
cifs security modify -vserver vs1 -aes-enabled-for-netlogon-channel true
```



ONTAP 9.14.1以降にアップグレードした場合、以前のリリースのONTAPで作成された既存のSVMのAES設定は自動的に変更されません。これらのSVMでAESを有効にするには、引き続きこの設定の値を更新する必要があります。

認証トンネルを設定します

データSVM用のSMBサーバがすでに設定されている場合は、を使用できます `security login domain-tunnel create` コマンドを使用して、SVMをADによるクラスタへのアクセス用のゲートウェイ (*tunnel*) として設定します。

作業を開始する前に

- データSVM用のSMBサーバを設定しておく必要があります。
- AD ドメインのユーザアカウントによるクラスタの管理 SVM へのアクセスを有効にしておく必要があります。
- このタスクを実行するには、クラスタ管理者である必要があります。

ONTAP 9.10.1 以降では、AD アクセス用の SVM ゲートウェイ (ドメイントンネル) がある場合に、AD ドメインで NTLM を無効にしていれば、管理認証に Kerberos を使用できます。以前のリリースでは、SVM ゲートウェイの管理者認証で Kerberos がサポートされていませんでした。この機能はデフォルトで有効になっており、設定は必要ありません。



Kerberos 認証は常に最初に試行されます。失敗すると、NTLM 認証が試行されます。

ステップ

1. SMB 対応データ SVM を AD ドメインコントローラがクラスタにアクセスするための認証トンネルとして設定します。

```
security login domain-tunnel create -vserver svm_name
```

コマンド構文全体については、を参照してください ["ワークシート"](#)。



ユーザを認証するには、SVM が実行されている必要があります。

次のコマンドは、SMB対応のデータSVM「engData」を認証トンネルとして設定します。

```
cluster1::>security login domain-tunnel create -vserver engData
```

ドメインに **SVM** コンピュータアカウントを作成します

データSVM用のSMBサーバを設定していない場合は、を使用できます `vserver active-directory create` コマンドを使用して、ドメインにSVM用のコンピュータアカウントを作成します。

このタスクについて

を入力した後 `vserver active-directory create` コマンドを実行すると、ドメイン内の指定した組織単位にコンピュータを追加するための十分な権限を持つADユーザアカウントのクレデンシャルを入力するように求められます。アカウントのパスワードは空にできません。

作業を開始する前に

このタスクを実行するには、クラスタ管理者または SVM の管理者である必要があります。

## ステップ

1. AD ドメインに SVM 用のコンピュータアカウントを作成します。

```
vserver active-directory create -vserver SVM_name -account-name  
NetBIOS_account_name -domain domain -ou organizational_unit
```

コマンド構文全体については、を参照してください ["ワークシート"](#)。

次のコマンドは、SVM 「engData」 のドメイン 「example.com」 に 「ADSERVER1」 という名前のコンピュータアカウントを作成します。コマンドを入力すると、AD ユーザアカウントのクレデンシャルの入力を求められます。

```
cluster1::>vserver active-directory create -vserver engData -account  
-name ADSERVER1 -domain example.com
```

In order to create an Active Directory machine account, you must supply the name and password of a Windows account with sufficient privileges to add computers to the "CN=Computers" container within the "example.com" domain.

Enter the user name: Administrator

Enter the password:

## LDAP サーバまたは NIS サーバのアクセスの概要を設定

LDAP アカウントまたは NIS アカウントから SVM にアクセスするためには、LDAP サーバまたは NIS サーバから SVM へのアクセスを設定しておく必要があります。スイッチ機能を使用すると、LDAP または NIS を代替ネームサービスソースとして使用できます。

### LDAP サーバアクセスを設定する

LDAP アカウントが SVM にアクセスするためには、LDAP サーバから SVM へのアクセスを設定しておく必要があります。を使用できます `vserver services name-service ldap client create` コマンドを使用して SVM に LDAP クライアント設定を作成します。その後、を使用できます `vserver services name-service ldap create` コマンドを使用して LDAP クライアント設定を SVM に関連付けます。

### このタスクについて

ほとんどの LDAP サーバでは、ONTAP が提供する次のデフォルトスキーマを使用できます。

- MS-AD-BIS （ほとんどの Windows Server 2012 以降の AD サーバで推奨されるスキーマ）
- AD-IDMU （Windows 2008、Windows 2016、およびそれ以降の AD サーバ）

- AD-SFU (Windows Server 2003 以前の AD サーバ)
- RFC-2307 (UNIX LDAP サーバ)

他のスキーマを使用する必要がある場合を除き、デフォルトのスキーマを使用することを推奨します。その場合は、デフォルトスキーマをコピーし、コピーを変更することによって、独自のスキーマを作成できます。詳細については、を参照してください

- ["NFS構成"](#)
- ["ネットアップテクニカルレポート 4835 : 『How to Configure LDAP in ONTAP 』"](#)

作業を開始する前に

- をインストールしておく必要があります ["CA 署名済みサーバデジタル証明書"](#) 指定します。
- このタスクを実行するには、クラスタ管理者または SVM の管理者である必要があります。

手順

1. SVMにLDAPクライアント設定を作成します。

```
vserver services name-service ldap client create -vserver SVM_name -client
-config client_configuration -servers LDAP_server_IPs -schema schema -use
-start-tls true|false
```



Start TLS は、データ SVM へのアクセスでのみサポートされます。管理 SVM へのアクセスではサポートされません。

コマンド構文全体については、を参照してください ["ワークシート"](#)。

次のコマンドは、SVM「engData」上に「corp」という名前のLDAPクライアント設定を作成します。クライアントは、IPアドレスが172.160.0.100および172.16.0.101のLDAPサーバに匿名でバインドします。クライアントはRFC-2307スキーマを使用してLDAPクエリを実行します。クライアントとサーバ間の通信は Start TLS を使用して暗号化されます。

```
cluster1::> vserver services name-service ldap client create
-vserver engData -client-config corp -servers 172.16.0.100,172.16.0.101
-schema RFC-2307 -use-start-tls true
```



ONTAP 9.2以降では、フィールドが表示されます `-ldap-servers` フィールドを置き換えます `-servers`。この新しいフィールドには、LDAP サーバのホスト名または IP アドレスを指定できます。

2. LDAPクライアント設定をSVMに関連付けます。 `vserver services name-service ldap create -vserver SVM_name -client-config client_configuration -client-enabled true|false`

コマンド構文全体については、を参照してください ["ワークシート"](#)。

次のコマンドは、LDAPクライアント設定を関連付けます `corp` SVMを使用します `engData`、SVMでLDAPクライアントを有効にします。

```
cluster1::>vserver services name-service ldap create -vserver engData  
-client-config corp -client-enabled true
```



ONTAP 9.2以降では、`vserver services name-service ldap create` コマンドは設定の自動検証を実行し、ONTAP がネームサーバに接続できない場合はエラーメッセージを報告します。

3. `vserver services name-service ldap check` コマンドを使用して、ネームサーバのステータスを検証します。

次のコマンドは、SVM vs0 上の LDAP サーバを検証します。

```
cluster1::> vserver services name-service ldap check -vserver vs0  
  
| Vserver: vs0 |  
| Client Configuration Name: c1 |  
| LDAP Status: up |  
| LDAP Status Details: Successfully connected to LDAP server |  
"10.11.12.13". |
```

ネームサービスのチェックコマンドは ONTAP 9.2 以降で使用できます。

## NIS サーバアクセスの設定

NISアカウントがSVMにアクセスするためには、NISサーバからSVMへのアクセスを設定しておく必要があります。使用できます `vserver services name-service nis-domain create` コマンドを使用してSVMにNISドメイン設定を作成します。

このタスクについて

複数の NIS ドメインを作成できます。に設定できるNISドメインは1つだけです active 一度に。

作業を開始する前に

- SVM に NIS ドメインを設定するためには、設定済みのすべてのサーバが使用可能でアクセスできる状態になっている必要があります。
- このタスクを実行するには、クラスタ管理者または SVM の管理者である必要があります。

ステップ

1. SVMにNISドメイン設定を作成します。

```
vserver services name-service nis-domain create -vserver SVM_name -domain  
client_configuration -active true|false -nis-servers NIS_server_IPs
```

コマンド構文全体については、を参照してください ["ワークシート"](#)。





ONTAP 9.2以降では、フィールドが表示されます `-nis-servers` フィールドを置き換えます `-servers`。この新しいフィールドには、NISサーバのホスト名またはIPアドレスを指定できます。

次のコマンドは、SVM「engData」にNISドメイン設定を作成します。NISドメイン `nisdomain` は作成時にアクティブになり、IPアドレスが192.0.2.180のNISサーバと通信します。

```
cluster1::>vserver services name-service nis-domain create
-vserver engData -domain nisdomain -active true -nis-servers 192.0.2.180
```

ネームサービススイッチを作成します

ネームサービススイッチ機能を使用すると、LDAP または NIS を代替ネームサービスソースとして使用できます。を使用できます `vserver services name-service ns-switch modify` コマンドを使用して、ネームサービスソースの参照順序を指定します。

作業を開始する前に

- LDAP サーバおよび NIS サーバのアクセスを設定しておく必要があります。
- このタスクを実行するには、クラスタ管理者または SVM 管理者である必要があります。

ステップ

1. ネームサービスソースの参照順序を指定します。

```
vserver services name-service ns-switch modify -vserver SVM_name -database
name_service_switch_database -sources name_service_source_order
```

コマンド構文全体については、を参照してください ["ワークシート"](#)。

次のコマンドは、SVM「engData」上の「passwd」データベースのLDAPおよびNISネームサービスソースの検索順序を指定します。

```
cluster1::>vserver services name-service ns-switch
modify -vserver engData -database passwd -source files ldap,nis
```

管理者パスワードを変更します

初期パスワードは、システムへの初回ログイン後すぐに変更してください。SVM管理者は、を使用できます `security login password` コマンドを使用して自分のパスワードを変更します。クラスタ管理者は、を使用できます `security login password` コマンドを使用して管理者のパスワードを変更します。

このタスクについて

新しいパスワードは次のルールに従う必要があります。

- ユーザ名を含めることはできません



- 8 文字以上である必要があります
- アルファベットと数字がそれぞれ 1 文字以上含まれている必要があります
- 直近の 6 つのパスワードと同じパスワードは使用できません



を使用できます `security login role config modify` コマンドを使用して、特定のロールに関連付けられているアカウントのパスワードルールを変更します。詳細については、を参照してください ["コマンドリファレンス"](#)。

作業を開始する前に

- 自分のパスワードを変更するには、クラスタ管理者または SVM 管理者である必要があります。
- 他の管理者のパスワードを変更するには、クラスタ管理者である必要があります。

ステップ

1. 管理者パスワードを変更します。 `security login password -vserver svm_name -username user_name`

管理者のパスワードを変更するコマンドの例を次に示します `admin1` SVM用 `vs1.example.com`。現在のパスワードの入力を求められたら、新しいパスワードを入力して、もう一度入力します。

```
vs1.example.com::>security login password -vserver engData -username
admin1
Please enter your current password:
Please enter a new password:
Please enter it again:
```

管理者アカウントをロックおよびロック解除します

を使用できます `security login lock` 管理者アカウントをロックするコマンド、および `security login unlock` コマンドを使用してアカウントのロックを解除します。

作業を開始する前に

これらのタスクを実行するには、クラスタ管理者である必要があります。

手順

1. 管理者アカウントをロックします。

```
security login lock -vserver SVM_name -username user_name
```

次のコマンドは、管理者アカウントをロックします `admin1` SVM用 `vs1.example.com` :

```
cluster1::>security login lock -vserver engData -username admin1
```

2. 管理者アカウントのロックを解除します。

```
security login unlock -vserver SVM_name -username user_name
```

次のコマンドは、管理者アカウントのロックを解除します admin1 SVM用 vs1.example.com：

```
cluster1::>security login unlock -vserver engData -username admin1
```

失敗したログインを管理します

ログイン試行が繰り返し失敗する場合、侵入者がストレージシステムへのアクセスを試みていることが疑われます。侵入を防ぐためにさまざまな対策を講じることができます。

失敗したログインを確認する方法

イベント管理システム（EMS）では 1 時間ごとに失敗したログイン試行を通知します。失敗したログインの記録は、で確認できます audit.log ファイル。

ログイン試行が繰り返し失敗する場合の対処方法

侵入を防ぐための短期的な対策としては、次のような方法があります。

- パスワードに大文字、小文字、特殊文字、数字を最低何文字か含めるように要求します
- ログインに失敗したあとに間隔を設定します
- 許容されるログイン失敗回数を制限し、指定した回数を超えたユーザをロックアウトします
- 指定した日数アクティブでないアカウントを期限切れにしてロックアウトします

を使用できます security login role config modify コマンドを使用してこれらのタスクを実行します。

長期的に見て、次の手順を実行することもできます。

- を使用します security ssh modify コマンドを使用して、新しく作成するすべてのSVMに対してログインの失敗回数を制限します。
- ユーザにパスワードの変更を求めることで、既存の MD5 アルゴリズムのアカウントをより安全な SHA-512 アルゴリズムに移行する。

管理者アカウントのパスワードに **SHA-2** を適用します

ONTAP 9.0 より前のバージョンで作成した管理者アカウントでは、パスワードが手動で変更されるまで、アップグレード後も引き続き MD5 パスワードが使用されます。MD5 は SHA-2 よりも安全性が低くなります。そのため、アップグレード後は、MD5 アカウントのユーザに対してパスワードを変更してデフォルトの SHA-512 ハッシュ関数を使用するよう促す必要があります。

このタスクについて

パスワードハッシュ機能を使用すると、次の操作を実行できます。

- 指定したハッシュ関数に一致するユーザアカウントを表示する。
- 指定したハッシュ関数（MD5 など）を使用するアカウントを期限切れにして、次のログイン時にユーザにパスワードの変更を強制します。
- 指定したハッシュ関数を使用するパスワードが指定されたアカウントをロックする。
- ONTAP 9 より前のリリースにリバートする場合は、クラスタ管理者のパスワードを以前のリリースでサポートされているハッシュ関数（MD5）と互換性があるパスワードにリセットします。

ONTAPは、NetApp Manageability SDKを使用する場合にのみ、事前にハッシュされたSHA-2パスワードを受け入れます。(security-login-create および security-login-modify-password)。

#### 手順

1. MD5 管理者アカウントを SHA-512 パスワードハッシュ関数に移行します。

- a. すべてのMD5管理者アカウントを期限切れにします。 `security login expire-password -vserver * -username * -hash-function md5`

これにより、MD5 アカウントのユーザは、次のログイン時にパスワードの変更が必要になります。

- b. MD5 アカウントのユーザに、コンソールまたは SSH セッションを使用してログインするよう依頼します。

アカウントの有効期限が切れていることが検出され、ユーザにパスワードの変更を求めるメッセージが表示されます。変更されたパスワードでは、デフォルトで SHA-512 が使用されます。

2. ユーザが一定期間ログインしていないためにパスワードが変更されない MD5 アカウントについては、強制的にアカウントを移行します。


- a. まだMD5ハッシュ関数を使用しているアカウントをロックします（advanced権限レベル）。  
`security login expire-password -vserver * -username * -hash-function md5 -lock-after integer`

で指定した日数が経過した後、`-lock-after` ユーザーはMD5アカウントにアクセスできません。

- b. ユーザがパスワードを変更する準備ができたなら、アカウントのロックを解除します。 `security login unlock -vserver svm_name -username user_name`
- c. ユーザに、コンソールまたは SSH セッションからアカウントにログインし、表示される指示に従ってパスワードを変更するよう促します。


#### ファイルアクセスの問題を診断して修正

#### 手順

1. System Manager で、\* Storage > Storage VM\* を選択します。
2. トレースを実行する Storage VM を選択してください。
3. をクリックします  \* その他 \*。
4. ファイルアクセスのトレース \* をクリックします。
5. ユーザー名とクライアントの IP アドレスを入力し、\* トレースを開始 \* をクリックします。

トレース結果が表形式で表示されます。[\* 理由] 列には、ファイルにアクセスできなかった理由が表示さ

れます。

6. をクリックします  ファイルアクセス権限を表示するには、結果テーブルの左側の列を参照してください。

## 管理者による検証を管理します

### マルチ管理者検証の概要

ONTAP 9.11.1以降では、マルチ管理検証（MAV）を使用して、ボリュームやSnapshotコピーの削除などの特定の処理を、指定した管理者からの承認がないと実行できないようにすることができます。これにより、侵害を受けた管理者、悪意のある管理者、または経験の浅い管理者が、望ましくない変更やデータの削除を行うことを防止でき

マルチ管理者検証の設定は、次のとおりです。

- "1つ以上の管理者承認グループを作成します。"
- "マルチ管理者検証機能の有効化。"
- "ルールを追加または変更する。"

初期設定後、これらの要素はMAV承認グループ（MAV管理者）の管理者のみが変更できます。

マルチ管理者検証を有効にすると、保護されたすべての処理が完了するために次の3つの手順が必要となります。

- ユーザが処理を開始すると、が実行されます "要求が生成されます。"
- 実行する前に、少なくとも1つは必要です "MAV管理者は承認する必要があります。"
- 承認されると、ユーザーは操作を完了します。

複数管理者による検証は、自動化の負荷が大きいボリュームやワークフローでは使用しないことを想定しています。自動化された各タスクを完了するには承認が必要なためです。オートメーションとMAVを併用する場合は、MAVの特定の操作にクエリを使用することをお勧めします。たとえば、適用できます `volume delete` MAVルールは、自動化が関係しないボリュームにのみ適用され、特定の命名規則を使用して指定できます。



MAVの管理者の承認なしでマルチ管理者検証機能を無効にする必要がある場合は、ネットアップサポートに連絡して、次の技術情報アートを記載します。 "MAV管理者が利用できない場合にマルチ管理者検証を無効にする方法"。

### マルチ管理者検証の仕組み

マルチ管理者検証は、次の要素で構成されます。

- 承認権限と拒否権を持つ1人以上の管理者のグループ。
- 保護された操作またはコマンドのセット（`a_rules table`）
- `a_rules`エンジン\_保護されたオペレーションの実行を識別および制御します

MAVルールは、Role-Based Access Control（RBAC；ロールベースアクセス制御）ルールのあとに評価されま

す。このため、保護された操作を実行または承認する管理者は、それらの操作に対する最低限のRBAC権限を持っている必要があります。 ["RBACの詳細については、こちらをご覧ください。"](#)

## システム定義のルール

マルチ管理者検証を有効にすると、システム定義のルール（`_guard-rule_rules`とも呼ばれます）によってMAV処理のセットが確立され、MAVプロセス自体が回避されるリスクが含まれます。これらの操作をルールテーブルから削除することはできません。MAVを有効にすると、アスタリスク（`*`）で指定された操作は、実行前に1人以上の管理者による承認を必要とします。ただし、`show *`コマンドは除きます。

- `security multi-admin-verify modify` 操作\*

管理者による検証機能の設定を制御します。

- `security multi-admin-verify approval-group` 操作\*

管理者による検証クレデンシャルを使用して、一連の管理者のメンバーシップを制御します。

- `security multi-admin-verify rule` 操作\*

管理者による検証が必要な一連のコマンドを制御します。

- `security multi-admin-verify request` 操作

承認プロセスを制御します。

## ルールで保護されたコマンド

マルチ管理者検証を有効にした場合、システム定義のコマンドに加えて次のコマンドもデフォルトで保護されますが、これらのコマンドの保護を解除するようにルールを変更することができます。

- `security login password`
- `security login unlock`
- `set`

ONTAP 9.11.1以降のリリースでは、次のコマンドを保護できます。

cluster peer delete	volume snapshot autodelete modify
event config modify	volume snapshot delete
security login create	volume snapshot policy add-schedule
security login delete	volume snapshot policy create
security login modify	volume snapshot policy delete
system node run	volume snapshot policy modify
system node systemshell	volume snapshot policy modify-schedule
volume delete	volume snapshot policy remove-schedule
volume flexcache delete	volume snapshot restore
	vserver peer delete

ONTAP 9.13.1以降では、次のコマンドを保護できます。

- volume snaplock modify
- security anti-ransomware volume attack clear-suspect
- security anti-ransomware volume disable
- security anti-ransomware volume pause

ONTAP 9.14.1以降では、次のコマンドを保護できます。

- volume recovery-queue modify
- volume recovery-queue purge
- volume recovery-queue purge-all
- vserver modify

複数管理者による承認の仕組み

保護された操作がMAV保護されたクラスタで入力されると、操作の実行要求が指定されたMAV管理者グループに送信されます。

次の項目を設定できます。

- MAVグループ内の管理者の名前、連絡先情報、および数。

MAV管理者には、クラスタ管理者権限を持つRBACロールが必要です。

- MAV管理者グループの数。
  - MAVグループは、保護された各操作ルールに割り当てられます。

。複数のMAVグループの場合、どのMAVグループが特定のルールを承認するかを設定できます。

- 保護された操作を実行するために必要なMAV承認の数。
- MAV管理者が承認要求に応答する必要がある\_承認の失効\_期間。
- 要求元の管理者が処理を完了する必要がある\_実行のexpiry\_period。

これらのパラメータを設定したら、MAV承認が必要です。

MAV管理者は、保護された操作を実行するための独自の要求を承認できません。そのため、次の

- 管理者が1人だけのクラスタではMAVを有効にしないでください。
- MAVグループにユーザーが1人しかいない場合、MAV管理者は保護された操作を入力できません。通常の管理者は、これらの操作を入力する必要があり、MAV管理者は承認のみを行えます。
- MAV管理者が保護された操作を実行できるようにするには、MAV管理者の数が、必要な承認数よりも1人大きくなければなりません。  
たとえば、保護された操作に2つの承認が必要で、MAV管理者がそれらを実行する場合、MAV管理者グループには3人の承認が必要です。

MAV管理者は、（EMSを使用して）Eメールアラートで承認要求を受信するか、要求キューを照会できます。リクエストを受け取った場合、次の3つのアクションのいずれかを実行できます。

- 承認します
- 拒否（拒否）
- 無視（操作なし）

MAVルールに関連付けられているすべての承認者に電子メール通知が送信されるのは、次の場合です。

- リクエストが作成されました。
- リクエストが承認または拒否された場合。
- 承認されたリクエストが実行されます。

リクエスト者が同じ承認グループに属している場合は、リクエストが承認されると電子メールが送信されます。

\*注：\*リクエスト者は、承認グループに属している場合でも、リクエスト者自身のリクエストを承認できません。ただし、Eメール通知を受け取ることはできます。承認グループに属していない（つまり、MAV管理者ではない）リクエストは、電子メール通知を受信しません。

保護された操作の実行の仕組み

保護された操作の実行が承認されると、要求されたユーザーは操作を続行します。処理が拒否された場合、要求元ユーザーは処理を続行する前に要求を削除する必要があります。

MAVルールはRBAC権限の後に評価されます。そのため、操作の実行に十分なRBACアクセス許可がないユーザーはMAV要求プロセスを開始できません。

管理者の承認グループを管理します

Multi-Admin Verification（MAV；マルチ管理者検証）を有効にする前に、1人以上の管理

者が承認権限または拒否権限を付与される管理者承認グループを作成する必要があります。マルチ管理者検証を有効にすると、承認グループのメンバーシップを変更した場合には、既存の資格のある管理者の承認が必要になります。

このタスクについて

既存の管理者をMAVグループに追加したり、新しい管理者を作成したりできます。

MAV機能は、既存のロールベースアクセス制御（RBAC）設定に対応しています。MAV管理者は、MAV管理者グループに追加する前に、保護された操作を実行するための十分な権限を持っている必要があります。  
"RBACの詳細については、[こちらをご覧ください。](#)"

MAVを設定して、承認リクエストが保留中であることをMAV管理者に通知できます。そのためには、Eメール通知（特に）を設定する必要があります Mail From および Mail Server パラメーターまたは、これらのパラメータをクリアして通知を無効にすることもできます。MAV管理者は、電子メールアラートを使用しないで、承認キューを手動でチェックする必要があります。



#### System Manager の手順の略

MAV承認グループを初めて作成する場合は、「System Manager手順 to」を参照してください "[マルチ管理者検証を有効にします。](#)"

既存の承認グループを変更する、または追加の承認グループを作成するには、次の手順を実行します。

1. 管理者による検証を受ける管理者を特定します。
  - a. **[Cluster]>[Settings.]**をクリックします
  - b. をクリックします  をクリックします
  - c. をクリックします  **Add [Users.]**の下にあります
  - d. 必要に応じて名簿を変更します。

詳細については、を参照してください "[管理者アクセスの制御](#)"

2. MAV承認グループを作成または変更します。
  - a. **[Cluster]>[Settings.]**をクリックします
  - b. をクリックします  「セキュリティ」セクションの「\*マルチ管理者承認」の横。  
(が表示されます  アイコン（MAVがまだ設定されていない場合）。
    - Name：グループ名を入力します。
    - 承認者：ユーザーのリストから承認者を選択します。
    - Eメールアドレス：Eメールアドレスを入力します。
    - デフォルトグループ：グループを選択します。

MAVを有効にした後、既存の設定を編集するにはMAV承認が必要です。

#### CLI 手順の略

1. に値が設定されていることを確認します Mail From および Mail Server パラメータ入力するコマンド

```
event config show
```



次のような情報が表示されます。

```
cluster01::> event config show
                Mail From:  admin@localhost
                Mail Server: localhost
                Proxy URL:  -
                Proxy User:  -
                Publish/Subscribe Messaging Enabled: true
```

次のパラメータを入力して設定します。

```
event config modify -mail-from email_address -mail-server server_name
```

## 2. 管理者による検証を受ける管理者を特定します

実行する処理	入力するコマンド
現在の管理者を表示します	<code>security login show</code>
現在の管理者のクレデンシャルの変更	<code>security login modify &lt;parameters&gt;</code>
新しい管理者アカウントを作成します	<code>security login create -user-or-group -name <i>admin_name</i> -application ssh -authentication-method password</code>

## 3. MAV承認グループを作成します。

```
security multi-admin-verify approval-group create [ -vserver svm_name] -name  
group_name -approvers approver1[,approver2...] [[-email address1], address1...]
```

- `-vserver` -このリリースでは管理SVMのみがサポートされます。
- `-name` - MAVグループ名（最大64文字）。
- `-approvers` - 1人以上の承認者のリスト。
- `-email` - リクエストが作成、承認、拒否、または実行されたときに通知される1つ以上の電子メールアドレス。

\*例：\*次のコマンドは、2つのメンバーと関連付けられたEメールアドレスを持つMAVグループを作成します。

```
cluster-1::> security multi-admin-verify approval-group create -name  
mav-grp1 -approvers pavan,julia -email pavan@myfirm.com,julia@myfirm.com
```

## 4. グループの作成とメンバーシップを確認します。

```
security multi-admin-verify approval-group show
```

。例：＊

```
cluster-1::> security multi-admin-verify approval-group show
Vserver   Name           Approvers      Email
-----
-----
svm-1     mav-grp1      pavan,julia    email
pavan@myfirm.com,julia@myfirm.com
```

MAVグループの初期設定を変更するには、次のコマンドを使用します。

\*注意：\*すべての場合、MAV管理者による承認が必要です。

実行する処理	入力するコマンド
グループの特性を変更するか、既存のメンバー情報を変更します	<code>security multi-admin-verify approval-group modify [parameters]</code>
メンバーを追加または削除します	<code>security multi-admin-verify approval-group replace [-vserver svm_name] -name group_name [-approvers-to-add approver1[,approver2...]] [-approvers-to-remove approver1[,approver2...]]</code>
グループを削除します	<code>security multi-admin-verify approval-group delete [-vserver svm_name] -name group_name</code>

マルチ管理者検証を有効または無効にします

Multi-admin Verification (MAV；マルチ管理者検証) は明示的に有効にする必要があります。マルチ管理者検証を有効にした後は、MAV承認グループ (MAV管理者) の管理者による承認が必要になります。

このタスクについて

MAVを有効にすると、MAVを変更または無効にするには、MAV管理者の承認が必要になります。



MAVの管理者の承認なしでマルチ管理者検証機能を無効にする必要がある場合は、ネットアップサポートに連絡して、次の技術情報アートを記載します。"[MAV管理者が利用できない場合にマルチ管理者検証を無効にする方法](#)"。

MAVをイネーブルにすると、次のパラメータをグローバルに指定できます。

#### 承認グループ

グローバル承認グループのリスト。MAV機能を有効にするには、少なくとも1つのグループが必要です。



MAVとAutonomous Ransomware Protection (ARP) を使用している場合は、ARPの一時停止、無効化、および疑わしい要求のクリアを担当する新規または既存の承認グループを定義します。

## 必須の承認者

保護された操作を実行するために必要な承認者の数。デフォルトの最小数は1です。



必要な承認者の数は、デフォルトの承認グループ内の一意の承認者の総数よりも少なくする必要があります。

## 承認の有効期限（時間、分、秒）

MAV管理者が承認要求に応答する必要がある期間。デフォルト値は1時間（1h）、サポートされる最小値は1秒（1s）、サポートされる最大値は14日（14d）です。


## 実行の有効期限（時間、分、秒）

要求元の管理者が::operationを完了する必要がある期間。デフォルト値は1時間（1h）、サポートされる最小値は1秒（1s）、サポートされる最大値は14日（14d）です。

特定のパラメータについて、これらのパラメータを上書きすることもできます ["操作ルール。"](#)



## System Manager の手順の略

### 1. 管理者による検証を受ける管理者を特定します。

- [\[Cluster\]>\[Settings.\]](#)をクリックします
- をクリックします  をクリックします
- をクリックします  [Add \[Users.\]](#)の下にあります
- 必要に応じて名簿を変更します。

詳細については、[を参照してください "管理者アクセスの制御"](#)

### 2. 少なくとも1つの承認グループを作成し、少なくとも1つのルールを追加して、マルチ管理者検証を有効にします。

- [\[Cluster\]>\[Settings.\]](#)をクリックします
- をクリックします  「セキュリティ」セクションの「\*マルチ管理者承認」の横。
- をクリックします  [Add](#) 1つ以上の承認グループを追加します。
  - 名前-グループ名を入力します。
  - 承認者-ユーザーのリストから承認者を選択します。
  - Eメールアドレス-Eメールアドレスを入力します。
  - デフォルトグループ-グループを選択します。
- ルールを少なくとも1つ追加してください。
  - operation-サポートされているコマンドをリストから選択します。
  - Query-必要なコマンドオプションと値を入力します。

- オプションのパラメータ。グローバル設定を適用する場合は空白のままにします。グローバル設定を上書きする場合は、特定のルールに別の値を割り当てます。
- 必要な承認者の数
- 承認グループ

e. [詳細設定\*]をクリックして、デフォルトを表示または変更します。

- 必要な承認者数（デフォルト：1）
- 実行要求の有効期限（デフォルト：1時間）
- 承認リクエストの有効期限（デフォルト：1時間）
- メールサーバ\*
- 送信元Eメールアドレス\*

\*これらは、「通知管理」で管理されている電子メール設定を更新します。まだ設定されていない場合は、設定を求めるプロンプトが表示されます。


f. Enable（有効）\*をクリックしてMAV初期設定を完了します。

初期設定後、現在のMAVステータスが\* Multi-Admin Approval \*（マルチ管理者承認）タイルに表示されます。

- ステータス（有効または無効）
- 承認が必要なアクティブな操作
- 保留状態のオープン要求の数

をクリックすると、既存の設定を表示できます →。既存の構成を編集するにはMAV承認が必要です。

マルチ管理者検証を無効にする場合：

1. [Cluster]>[Settings.]をクリックします
2. をクリックします  「セキュリティ」セクションの「\*マルチ管理者承認」の横。
3. [有効]トグルボタンをクリックします。

この操作を完了するにはMAV承認が必要です。

#### CLI 手順の略

CLIでMAV機能をイネーブルにする前に、少なくとも1つ "MAV管理者グループ" を作成しておく必要があります。

実行する処理	入力するコマンド
MAV機能を有効にします	<pre>security multi-admin-verify modify -approval-groups group1[,group2...] [- required-approvers nn ] -enabled true [ -execution-expiry [nnh][nmm][nns]] [ -approval-expiry [nnh][nmm][nns]]</pre> <p>例：次のコマンドは、MAVを1つの承認グループ、2つの必須承認者、およびデフォルトの有効期限で有効にします。</p> <pre>cluster-1::&gt; security multi-admin- verify modify -approval-groups mav-grp1 -required-approvers 2 -enabled true</pre> <p>1つ以上を追加して初期設定を完了します <a href="#">"操作ルール。"</a></p>
MAV設定の変更（MAVの承認が必要）	<pre>security multi-admin-verify approval- group modify [-approval-groups group1 [,group2...]] [-required-approvers nn ] [ -execution-expiry [nnh][nmm][nns]] [ -approval-expiry [nnh][nmm][nns]]</pre>
MAV機能を確認します	<pre>security multi-admin-verify show</pre> <p>• 例： *</p> <pre>cluster-1::&gt; security multi-admin- verify show Is          Required  Execution Approval Approval Enabled Approvers Expiry      Expiry Groups ----- true      2          1h        1h mav-grp1</pre>
MAV機能を無効にする（MAVの承認が必要）	<pre>security multi-admin-verify modify -enabled false</pre>

保護された操作ルールを管理します

MAV (Multi-admin Verification) ルールを作成して、承認が必要な操作を指定します。操作が開始されるたびに、保護された操作が妨害され、承認の要求が生成されます。

ルールは任意の管理者が適切なRBAC機能を使用してMAVを有効にする前に作成できますが、MAVを有効にすると、ルールセットを変更するにはMAV承認が必要になります。

1回の操作で作成できるMAVルールは1つだけです。たとえば、複数のMAVルールを作成することはできません。 volume-snapshot-delete ルール。必要なルール制約は1つのルール内に含める必要があります。

ルールで保護されたコマンド

ONTAP 9.11.1以降では、次のコマンドを保護するルールを作成できます。

cluster peer delete	volume snapshot autodelete modify
event config modify	volume snapshot delete
security login create	volume snapshot policy add-schedule
security login delete	volume snapshot policy create
security login modify	volume snapshot policy delete
system node run	volume snapshot policy modify
system node systemshell	volume snapshot policy modify-schedule
volume delete	volume snapshot policy remove-schedule
volume flexcache delete	volume snapshot restore
	vserver peer delete

ONTAP 9.13.1以降では、次のコマンドを保護するルールを作成できます。

- volume snaplock modify
- security anti-ransomware volume attack clear-suspect
- security anti-ransomware volume disable
- security anti-ransomware volume pause

ONTAP 9.14.1以降では、次のコマンドを保護するルールを作成できます。

- volume recovery-queue modify
- volume recovery-queue purge
- volume recovery-queue purge-all

- `vserver modify`

MAV system-defaultコマンドのルール `security multi-admin-verify` "コマンド"を変更することはできません。

マルチ管理者検証を有効にした場合、システム定義のコマンドに加えて次のコマンドもデフォルトで保護されますが、これらのコマンドの保護を解除するようにルールを変更することができます。

- `security login password`
- `security login unlock`
- `set`

#### ルール制約

ルールを作成するときに、オプションで指定できます `-query` 要求をコマンド機能のサブセットに制限するオプション。。 `-query` オプションを使用すると、SVM、ボリューム、Snapshot名などの構成要素を制限することもできます。

例えば、`volume snapshot delete` コマンド、`-query` 次のように設定できます。 `-snapshot !hourly*,!daily*,!weekly*` つまり、`hourly`、`daily`、または`weekly`属性のプレフィックスが付いたボリュームSnapshotは、MAV保護から除外されます。

```
smci-vsrm20::> security multi-admin-verify rule show
```

		Required	Approval
Vserver	Operation	Approvers	Groups
vs01	volume snapshot delete	-	-
	Query: -snapshot !hourly*,!daily*,!weekly*		



除外された構成要素はMAVによって保護されず、管理者はそれらを削除または名前変更できます。

デフォルトでは、ルールは対応するを指定します `security multi-admin-verify request create` "`protected_operation`" 保護されたオペレーションが入力されると、コマンドが自動的に生成されます。このデフォルトを変更して、が必要になるようにすることができます `request create` コマンドは別々に入力します。

デフォルトでは、ルール固有の例外を指定できますが、ルールは次のグローバルMAV設定を継承します。



- 承認者の必要数
- 承認グループ
- 承認の有効期限
- 実行の有効期限

#### System Manager の手順の略

保護された処理ルールを初めて追加する場合は、System Managerの手順 を参照してください "[マルチ管理者](#)"

検証を有効にします。"

既存のルールセットを変更するには：

- 1. [\* Cluster]>[Settings]（設定）\*を選択します。
- 2. 選択するオプション  「セキュリティ」セクションの「\*マルチ管理者承認」の横。
- 3. 選択するオプション  Add ルールを追加するには、既存のルールを変更または削除することもできます。
  - operation-サポートされているコマンドをリストから選択します。
  - Query-必要なコマンドオプションと値を入力します。
  - オプションのパラメータ-グローバル設定を適用する場合は空欄のままにします。グローバル設定を上書きする場合は、特定のルールに別の値を割り当てます。
    - 必要な承認者の数
    - 承認グループ

CLI 手順の略



すべて security multi-admin-verify rule コマンドを実行するには、以外のMAV管理者の承認が必要です security multi-admin-verify rule show。

実行する処理	入力するコマンド
ルールを作成します	<code>security multi-admin-verify rule create -operation "protected_operation" [- query operation_subset] [parameters]</code>
現在の管理者のクレデンシャルの変更	<code>security login modify &lt;parameters&gt;</code>  例：次のルールでは、ルートボリュームの削除が承認されている必要があります。  <code>security multi-admin-verify rule create -operation "volume delete" -query "- vserver vs0"</code>
ルールを変更します	<code>security multi-admin-verify rule modify -operation "protected_operation" [parameters]</code>
ルールを削除します	<code>security multi-admin-verify rule delete -operation "protected_operation"</code>
ルールを表示します	<code>security multi-admin-verify rule show</code>

コマンド構文の詳細については、を参照してください security multi-admin-verify rule マニュアルページ



保護された操作の実行を要求します

マルチ管理者検証（MAV）が有効になっているクラスタで保護された操作またはコマンドを開始すると、ONTAP は自動的に操作を代行受信し、要求を生成するよう要求します。この要求は、MAV承認グループ（MAV管理者）の1人以上の管理者によって承認される必要があります。または、ダイアログなしでMAV要求を作成することもできます。

承認された場合は、クエリに応答して、要求の有効期限内に処理を完了する必要があります。拒否された場合、または要求や有効期限を超えた場合は、要求を削除して再送信する必要があります。

MAV機能は既存のRBAC設定に対応しています。つまり、管理者ロールには、MAV設定に関係なく、保護された操作を実行するための十分な権限が必要です。"[RBACの詳細については、こちらをご覧ください](#)"。

MAV管理者の場合、保護された操作を実行する要求もMAV管理者によって承認される必要があります。

#### System Manager の手順の略

ユーザーがメニュー項目をクリックして操作を開始し、操作が保護されると、承認要求が生成され、次のような通知がユーザーに送信されます。

```
Approval request to delete the volume was sent.  
Track the request ID 356 from Events & Jobs > Multi-Admin Requests.
```

[\*Multi-Admin Requests]ウィンドウは、MAVが有効な場合に使用できます。このウィンドウには、ユーザのログインIDとMAVロール（承認者または未承認）に基づいて保留中のリクエストが表示されます。保留中の要求ごとに、次のフィールドが表示されます。

- 操作
- インデックス（数値）
- ステータス（[保留中]、[承認済み]、[却下済み]、[実行済み]、または[期限切れ]）

リクエストが1人の承認者によって却下された場合、それ以上のアクションは実行できません。

- query（要求された処理のパラメータまたは値）
- ユーザーを要求しています
- 要求の有効期限はです
- （の数）保留中の承認者
- （数）承認者の候補

要求が承認されると、要求元ユーザは有効期限内に処理を再試行できます。

ユーザが承認なしで操作を再試行すると、次のような通知が表示されます。

```
Request to perform delete operation is pending approval.  
Retry the operation after request is approved.
```

## CLI 手順の略

1. 保護された操作を直接入力するか、MAV requestコマンドを使用します。

例-ボリュームを削除するには、次のいずれかのコマンドを入力します。

° volume delete

```
cluster-1::*> volume delete -volume voll -vserver vs0
```

```
Warning: This operation requires multi-admin verification. To create a
```

```
        verification request use "security multi-admin-verify request create".
```

```
        Would you like to create a request for this operation?
```

```
        {y|n}: y
```

```
Error: command failed: The security multi-admin-verify request (index 3) is auto-generated and requires approval.
```

° security multi-admin-verify request create "volume delete"

```
Error: command failed: The security multi-admin-verify request (index 3) requires approval.
```

2. リクエストのステータスを確認し、MAV通知に応答します。

- a. 要求が承認されたら、CLIメッセージに応答して処理を完了します。

▪ 例: \*

```
cluster-1::> security multi-admin-verify request show 3
```

```
Request Index: 3
  Operation: volume delete
    Query: -vserver vs0 -volume voll
    State: approved
Required Approvers: 1
Pending Approvers: 0
  Approval Expiry: 2/25/2022 14:32:03
  Execution Expiry: 2/25/2022 14:35:36
    Approvals: admin2
    User Vetoed: -
      Vserver: cluster-1
User Requested: admin
  Time Created: 2/25/2022 13:32:03
  Time Approved: 2/25/2022 13:35:36
    Comment: -
  Users Permitted: -
```

```
cluster-1::*> volume delete -volume voll -vserver vs0
```

Info: Volume "voll" in Vserver "vs0" will be marked as deleted and placed in the volume recovery queue. The space used by the volume will be recovered only after the retention period of 12 hours has completed. To recover the space immediately, get the volume name using (privilege:advanced) "volume recovery-queue show voll\_\*" and then "volume recovery-queue purge -vserver vs0 -volume <volume\_name>" command. To recover the volume use the (privilege:advanced) "volume recovery-queue recover -vserver vs0 -volume <volume\_name>" command.

Warning: Are you sure you want to delete volume "voll" in Vserver "vs0" ?  
{y|n}: y

- b. 要求が拒否された場合、または有効期限が過ぎた場合は、要求を削除し、再送信するか、MAV管理者に連絡してください。

▪ 例: \*

```
cluster-1::> security multi-admin-verify request show 3
```

```
Request Index: 3
  Operation: volume delete
    Query: -vserver vs0 -volume voll1
    State: vetoed
Required Approvers: 1
Pending Approvers: 1
  Approval Expiry: 2/25/2022 14:38:47
  Execution Expiry: -
    Approvals: -
    User Vetoed: admin2
    Vserver: cluster-1
User Requested: admin
  Time Created: 2/25/2022 13:38:47
  Time Approved: -
    Comment: -
Users Permitted: -
```

```
cluster-1::*> volume delete -volume voll1 -vserver vs0
```

```
Error: command failed: The security multi-admin-verify request (index 3)
hasbeen vetoed. You must delete it and create a new verification
request.
To delete, run "security multi-admin-verify request delete 3".
```

保護された操作要求を管理します

MAV承認グループ（MAV管理者）の管理者に保留中の操作実行要求が通知された場合、一定の期間（承認期限）内に承認または拒否のメッセージで応答する必要があります。十分な数の承認が得られない場合、リクエスト者はリクエストを削除して、別のリクエストを作成する必要があります。

このタスクについて

承認リクエストはインデックス番号で識別されます。インデックス番号は電子メールメッセージに含まれ、リクエストキューの表示にも含まれます。

要求キューからは、次の情報を表示できます。

操作

要求が作成される保護された操作。

クエリ

ユーザーが操作を適用するオブジェクト。

## 状態

リクエストの現在の状態（保留中、承認済み、却下済み、期限切れ） 実行済み。リクエストが1人の承認者によって却下された場合、それ以上のアクションは実行できません。

## 必須の承認者

リクエストを承認するために必要なMAV管理者の数。ユーザは、操作ルールのrequired-approversパラメータを設定できます。ユーザーが必須承認者をルールに設定していない場合は、グローバル設定の必須承認者が適用されます。

## 保留中の承認者

リクエストを承認済みとしてマークするためにリクエストを承認する必要があるMAV管理者の数。

## 承認の有効期限

MAV管理者が承認要求に応答する必要がある期間。許可されたユーザーは、操作ルールの承認期限を設定できます。承認期限がルールに設定されていない場合は、グローバル設定の承認期限が適用されます。

## 実行の有効期限

要求元の管理者が処理を完了する必要がある期間。許可された任意のユーザーは、操作ルールの実行有効期限を設定できます。実行有効期限がルールに設定されていない場合は、グローバル設定の実行有効期限が適用されます。

## ユーザーが承認しました

リクエストを承認したMAV管理者。

## ユーザが拒否しました

リクエストを拒否したMAV管理者。

## Storage VM（SVM）

要求が関連付けられているSVM。このリリースでは、管理SVMのみがサポートされます。

## ユーザが要求しました

要求を作成したユーザのユーザ名。

## 作成時刻

リクエストが作成された時刻。

## 承認された時間

リクエストの状態が承認済みに変更された時刻。

## コメント（Comment）

リクエストに関連付けられているコメント。

## ユーザが許可されました

リクエストが承認された保護された操作の実行を許可されているユーザーのリスト。状況 `users-permitted` が空の場合、適切な権限を持つすべてのユーザが処理を実行できます。

期限切れの要求または実行された要求は、制限が1000件に達したとき、または期限切れの要求が8時間を超えたときにすべて削除されます。拒否された要求は、期限切れとしてマークされると削除されます。

**System Manager** の手順の略

MAV管理者は、承認リクエストの詳細、リクエストの有効期限、リクエストを承認または却下するためのリンクが記載された電子メールメッセージを受信します。承認ダイアログにアクセスするには、Eメール内のリンクをクリックするか、System Managerで\* Events & Jobs > Requests \*（イベントとジョブ>要求）に移動します。

[\*Requests]ウィンドウは、マルチ管理者検証がイネーブルの場合に使用でき、ユーザのログインIDおよびMAVロール（アプルーバまたはそれ以外）に基づいて保留中の要求が表示されます。

- 操作
- インデックス（数値）
- ステータス（ [保留中] 、 [承認済み] 、 [却下済み] 、 [実行済み] 、または [期限切れ] ）

リクエストが1人の承認者によって却下された場合、それ以上のアクションは実行できません。

- query（要求された処理のパラメータまたは値）
- ユーザーを要求しています
- 要求の有効期限はです
- （の数） 保留中の承認者
- （数） 承認者の候補

MAV管理者は、この画面に追加のコントロールを設定できます。管理者は、個々の操作または操作の選択したグループを承認、拒否、または削除できます。ただし、MAV管理者が要求元ユーザである場合は、独自の要求を承認、拒否、または削除することはできません。

**CLI** 手順の略

1. 保留中のリクエストが電子メールで通知された場合は、リクエストのインデックス番号と承認期限をメモします。インデックス番号は、以下の\* show または show-pending \*オプションを使用して表示することもできます。
2. 要求を承認または拒否します。

実行する処理	入力するコマンド
リクエストを承認します	<code>security multi-admin-verify request approve nn</code>
要求を拒否します	<code>security multi-admin-verify request veto nn</code>
すべての要求、保留中の要求、または単一の要求を表示します	<code>`security multi-admin-verify request { show</code>

実行する処理	入力するコマンド
show-pending } [nn] { -fields field1[,field2...]	[-instance ]}`  キュー内のすべての要求を表示することも、保留中の要求だけを表示することもできます。インデックス番号を入力すると、その情報のみが表示されます。特定のフィールドに関する情報を表示するには、を使用します -fields パラメータ) またはすべてのフィールドについて (を使用 -instance パラメータ) 。
リクエストを削除します	security multi-admin-verify request delete nn

## 例

次のシーケンスでは、MAV管理者がインデックス番号3のリクエストメールを受信した後、リクエストが承認されます。これはすでに1つの承認を持っています。

```
cluster1::> security multi-admin-verify request show-pending
Pending
Index Operation      Query State  Approvers Requestor
-----
3 volume delete -    pending 1      julia

cluster-1::> security multi-admin-verify request approve 3

cluster-1::> security multi-admin-verify request show 3

Request Index: 3
Operation: volume delete
Query: -
State: approved
Required Approvers: 2
Pending Approvers: 0
Approval Expiry: 2/25/2022 14:32:03
Execution Expiry: 2/25/2022 14:35:36
Approvals: mav-admin2
User Vetoed: -
Vserver: cluster-1
User Requested: julia
Time Created: 2/25/2022 13:32:03
Time Approved: 2/25/2022 13:35:36
Comment: -
Users Permitted: -
```

例

次のシーケンスは、MAV管理者がインデックス番号3の要求メールを受信した後、すでに1つの承認がある要求を拒否します。

```
cluster1::> security multi-admin-verify request show-pending
Pending
Index Operation      Query State   Approvers Requestor
-----
3 volume delete - pending 1 pavan

cluster-1::> security multi-admin-verify request veto 3

cluster-1::> security multi-admin-verify request show 3

Request Index: 3
Operation: volume delete
Query: -
State: vetoed
Required Approvers: 2
Pending Approvers: 0
Approval Expiry: 2/25/2022 14:32:03
Execution Expiry: 2/25/2022 14:35:36
Approvals: mav-admin1
User Vetoed: mav-admin2
Vserver: cluster-1
User Requested: pavan
Time Created: 2/25/2022 13:32:03
Time Approved: 2/25/2022 13:35:36
Comment: -
Users Permitted: -
```

## OAuth 2.0を使用した認証と許可

### ONTAP OAuth 2.0実装の概要

ONTAP 9.14以降では、Open Authorization (OAuth 2.0) フレームワークを使用し、ONTAP クラスタへのアクセスを制御できます。この機能は、ONTAP CLI、System Manager、REST APIなど、ONTAP 管理インターフェイスを使用して設定できます。ただし、OAuth 2.0の承認とアクセス制御の決定は、クライアントがREST APIを使用し、ONTAPにアクセスする場合にのみ適用できます。



OAuth 2.0のサポートはONTAP 9.14.0で初めて導入されたため、使用しているONTAPリリースに依存します。を参照してください ["ONTAP リリースノート"](#) を参照してください。



## 機能とメリット

ONTAPでOAuth 2.0を使用する主な機能と利点を以下に説明します。

### OAuth 2.0標準のサポート

OAuth 2.0は業界標準の認可フレームワークです。署名付きアクセストークンを使用して、保護されたリソースへのアクセスを制限および制御するために使用されます。OAuth 2.0を使用すると、次のような利点があります。

- 認証設定の多くのオプション
- パスワードを含むクライアントのクレデンシャルは絶対に公開しない
- トークンは構成に基づいて有効期限が切れるように設定できます
- REST APIでの使用に最適

### いくつかの一般的な承認サーバーでテスト済み

ONTAPの実装は、OAuth 2.0準拠の認可サーバーと互換性があるように設計されています。次の一般的なサーバーまたはサービスでテスト済みです。

- Auth0
- Active Directory フェデレーション サービス (ADFS)
- キークロック

### 複数の同時認証サーバーのサポート

1つのONTAPクラスタに対して最大8つの許可サーバーを定義できます。これにより、多様なセキュリティ環境のニーズに柔軟に対応できます。

### REST ロール トノ トウゴウ

ONTAP認証の決定は、最終的にはユーザまたはグループに割り当てられたRESTロールに基づいて行われます。これらのロールは、自己完結型スコープとしてアクセストークン内で伝送されるか、Active DirectoryまたはLDAPグループとともにローカルONTAP定義に基づいて伝送されます。

### 送信者に制約されたアクセストークンを使用するオプション

クライアント認証を強化するMutual Transport Layer Security (MTLS) を使用するようにONTAPおよび認可サーバーを設定できます。これにより、OAuth 2.0アクセストークンが最初に発行されたクライアントによってのみ使用されることが保証されます。この機能は、FAPIやMITERによって確立されたものを含む、いくつかの一般的なセキュリティ推奨事項をサポートし、それらと一致しています。

## 実装と構成

大まかに言えば、OAuth 2.0の実装と構成にはいくつかの側面があり、開始時に考慮する必要があります。

### ONTAP内のOAuth 2.0エンティティ

OAuth 2.0認証フレームワークは、データセンターまたはネットワーク内の実際の要素または仮要素にマッピングできる複数のエンティティを定義します。OAuth 2.0エンティティとそのONTAPへの適応を以下の表に示します。

OAuth 2.0エンティティ	説明
リソース	内部ONTAPコマンドを使用してONTAPリソースへのアクセスを提供するREST APIエンドポイント。
リソース所有者	保護されたリソースを作成した、またはデフォルトでそのリソースを所有しているONTAPクラスタユーザ。
リソースサーバ	保護されているリソースのホスト（ONTAPクラスタ）。
クライアント	リソース所有者に代わって、または権限を持ってREST APIエンドポイントへのアクセスを要求するアプリケーション。
許可サーバ	通常、アクセストークンの発行と管理ポリシーの適用を担当する専用サーバです。

## コアONTAP構成

OAuth 2.0を有効にして使用するようにONTAPクラスタを設定する必要があります。これには、認可サーバへの接続の確立と、必要なONTAP認可設定の定義が含まれます。この設定は、次のいずれかの管理インターフェイスを使用して実行できます。

- ONTAP コマンドラインインターフェイス
- System Manager の略
- ONTAP REST API

## 環境およびサポートサービス

ONTAP定義に加えて、認可サーバも設定する必要があります。グループとロールのマッピングを使用している場合は、Active DirectoryグループまたはLDAPに相当するものも設定する必要があります。

## サポートされるONTAPクライアント

ONTAP 9.14以降では、REST APIクライアントからOAuth 2.0を使用してONTAPにアクセスできます。REST API呼び出しを実行する前に、認証サーバからアクセストークンを取得する必要があります。次に、クライアントは、HTTP認証要求ヘッダーを使用して、このトークンを\_bearer token\_としてONTAPクラスタに渡します。必要なセキュリティのレベルに応じて、クライアントで証明書を作成してインストールし、MTLSに基づいて送信者に制約されたトークンを使用することもできます。

## 選択した用語

ONTAPを使用したOAuth 2.0デプロイメントの検討を開始する際には、いくつかの用語について理解しておく役立ちます。を参照してください ["その他のリソース"](#) OAuth 2.0に関する詳細情報へのリンクについては、を参照してください。

## アクセストークン

認証サーバによって発行され、保護されたリソースへのアクセス要求を行うためにOAuth 2.0クライアントアプリケーションによって使用されるトークン。

## JSON Webトークン

アクセストークンのフォーマットに使用される標準。JSONは、OAuth 2.0の要求を3つの主要セクションに配置したコンパクトな形式で表現するために使用されます。

## 送信者に制約されたアクセストークン

Mutual Transport Layer Security (MTLS) プロトコルに基づくオプションの機能。トークンで追加の確認要求を使用することで、アクセストークンが最初に発行されたクライアントによってのみ使用されるようになります。

## JSON Webキーセット

JWKSは、ONTAPがクライアントから提示されたJWTトークンを検証するために使用する公開鍵の集まりです。キーセットは、通常、認証サーバで専用のURIを使用して使用できます。

## 適用範囲

スコープは、ONTAP REST APIなどの保護されたリソースへのアプリケーションのアクセスを制限または制御する手段を提供します。これらは、アクセストークン内の文字列として表されます。

## ONTAP RESTロール

RESTロールはONTAP 9.6で導入され、ONTAP RBACフレームワークの中核をなす機能です。これらのロールは、ONTAPで引き続きサポートされている以前の従来のロールとは異なります。ONTAPのOAuth 2.0実装では、RESTロールのみがサポートされています。

## HTTP認証ヘッダー

REST API呼び出しの一部としてクライアントと関連する権限を識別するためのHTTP要求に含まれるヘッダー。認証と認可の実行方法に応じて、いくつかの種類または実装があります。OAuth 2.0アクセストークンをONTAPに提示する場合、トークンは\_bearer token\_として識別されます。

## HTTPベーシック認証

初期のHTTP認証技術はまだONTAPでサポートされています。プレーンテキストのクレデンシャル（ユーザー名とパスワード）はコロンで連結され、base64でエンコードされます。文字列は認可要求ヘッダーに配置され、サーバに送信されます。

## FAPI

OpenID Foundationのワーキンググループで、金融業界向けにプロトコル、データスキーマ、およびセキュリティに関する推奨事項を提供しています。このAPIは元々 Financial Grade APIとして知られていた。

## マイター

米国空軍と米国政府に技術的および安全保障上のガイダンスを提供する民間の非営利企業。

## その他のリソース

いくつかの追加リソースを以下に示します。OAuth 2.0と関連規格の詳細については、これらのサイトを参照してください。

## プロトコルと標準

- ["RFC 6749: OAuth 2.0認可フレームワーク"](#)
- ["RFC 7519: JSON Webトークン \(JWT\) "](#)
- ["RFC 7523: OAuth 2.0クライアントの認証と承認のためのJSON Webトークン \(JWT\) プロファイル"](#)
- ["RFC 7662: 『OAuth 2.0 Token Introspection』 "](#)
- ["RFC 7800: 『Proof-of-Possession Key for JWT』 "](#)
- ["RFC 8705: 『OAuth 2.0 Mutual-TLS Client Authentication and Certificate-Bound Access Tokens』 "](#)

## 組織

- ["OpenID基盤"](#)
- ["FAPIワーキンググループ"](#)
- ["マイター"](#)
- ["IANA-JWT"](#)

## 製品とサービス

- ["Auth0"](#)
- ["ADFSの概要"](#)
- ["キークローク"](#)

## その他のツールとユーティリティ

- ["Auth0によるJWT"](#)
- ["OpenSSL"](#)

## NetAppのドキュメントとリソース

- ["ONTAPの自動化"](#) ドキュメント

## 概念

### 認証サーバとアクセストークン

認可サーバーは、OAuth 2.0 Authorizationフレームワーク内の中心的なコンポーネントとしていくつかの重要な機能を実行します。

### OAuth 2.0認可サーバ

認証サーバは、主にアクセストークンの作成と署名を行います。これらのトークンには、クライアントアプリケーションが保護されたリソースに選択的にアクセスできるように、IDおよび承認情報が含まれています。これらのサーバは通常、相互に分離されており、スタンドアロンの専用サーバとして、またはより大きなIDおよびアクセス管理製品の一部として、いくつかの異なる方法で実装できます。



OAuth 2.0の機能がより大きなIDおよびアクセス管理製品または解決策内にパッケージ化されている場合は特に、認可サーバーに異なる用語が使用されることがあります。たとえば、\*アイデンティティプロバイダ (IdP) \*という用語は、\*認証サーバ\*と同じ意味でよく使用されます。

## 管理

アクセストークンの発行に加えて、認可サーバーは一般的にWebユーザーインターフェイスを介して関連する管理サービスも提供します。たとえば、次の項目を定義および管理できます。

- ユーザおよびユーザ認証
- スコープ
- テナントとレルムによる管理の分離
- ポリシーの適用

- さまざまな外部サービスへの接続
- その他のIDプロトコル（SAMLなど）のサポート

ONTAPは、OAuth 2.0標準に準拠した認可サーバーと互換性があります。

## ONTAPニテイキ

1つ以上の認可サーバをONTAPに定義する必要があります。ONTAPは、各サーバとセキュアに通信してトークンを検証し、クライアントアプリケーションをサポートするその他の関連タスクを実行します。

ONTAP構成の主な側面を以下に示します。も参照してください "[OAuth 2.0の導入シナリオ](#)" を参照してください。

### アクセストークンの検証方法と検証場所

アクセストークンを検証するには、2つのオプションがあります。

- ローカル検証

ONTAPは、トークンを発行した認可サーバーから提供された情報に基づいて、アクセストークンをローカルで検証できます。認証サーバから取得された情報はONTAPによってキャッシュされ、定期的に更新されます。

- リモートイントロスペクション

リモートイントロスペクションを使用して、認証サーバーでトークンを検証することもできます。イントロスペクションは、許可された当事者がアクセストークンについて認可サーバーに問い合わせることを可能にするプロトコルです。ONTAPは、アクセストークンから特定のメタデータを抽出し、トークンを検証する方法を提供します。ONTAPは、パフォーマンス上の理由から一部のデータをキャッシュします。

### ネットワークの場所

ONTAPはファイアウォールの背後にある可能性があります。この場合は、設定の一部としてプロキシを指定する必要があります。

### 許可サーバの定義方法

ONTAPに対する認証サーバは、CLI、System Manager、REST APIなどの任意の管理インターフェイスを使用して定義できます。たとえば、CLIでは次のコマンドを使用します。 `security oauth2 client create`。

### 認証サーバの数

1つのONTAPクラスタに対して最大8つの許可サーバを定義できます。発行者または発行者/オーディエンスの要求が一意である限り、同じ認証サーバを同じONTAPクラスタに複数回定義できます。たとえば、Keycloakでは、異なるレルムを使用する場合は常にこのようになります。

### OAuth 2.0アクセストークンの使用

認証サーバによって発行されたOAuth 2.0アクセストークンはONTAPによって検証され、REST APIクライアント要求のロールベースアクセスの決定に使用されます。

## アクセストークンの取得

REST APIを使用するONTAPクラスタに定義されている認証サーバからアクセストークンを取得する必要があります。トークンを取得するには、認可サーバに直接問い合わせる必要があります。



ONTAPは、問題アクセストークンを使用したり、クライアントからの要求を認可サーバにリダイレクトしたりすることはありません。

トークンの要求方法は、次のようないくつかの要因によって異なります。

- 認可サーバとその設定オプション
- OAuth 2.0認可タイプ
- 要求の問題に使用するクライアントまたはソフトウェアツール

## 付与タイプ

`a_grant` は、OAuth 2.0アクセストークンの要求と受信に使用される、ネットワークフローのセットを含む明確に定義されたプロセスです。クライアント、環境、およびセキュリティの要件に応じて、いくつかの異なる権限付与タイプを使用できます。一般的な付与タイプの一覧を以下の表に示します。

許可タイプ	説明
クライアントクレデンシャル	クレデンシャル（IDや共有シークレットなど）のみを使用する一般的な付与タイプ。クライアントは、リソース所有者と密接な信頼関係を持っていると想定されます。
パスワード	リソース所有者パスワード資格情報付与タイプは、リソース所有者がクライアントとの信頼関係を確立している場合に使用できます。また、レガシーHTTPクライアントをOAuth 2.0に移行する場合にも役立ちます。
認証コード	これは機密クライアントにとって理想的な認可タイプであり、リダイレクトベースのフローに基づいています。アクセストークンとリフレッシュトークンの両方を取得するために使用できます。

## JWTの内容

OAuth 2.0アクセストークンはJWT形式です。コンテンツは、設定に基づいて認可サーバによって作成されます。ただし、トークンはクライアントアプリケーションには不透明です。クライアントには、トークンを検査したり、コンテンツを認識したりする理由はありません。

各JWTアクセストークンには、クレームのセットが含まれています。クレームは、発行者の特性と認可サーバでの管理定義に基づいた認可を記述します。この規格に登録されている請求の一部は、次の表に記載されています。すべての文字列で大文字と小文字が区別されます。

請求	キーワード	説明
発行者	ISS	トークンを発行したプリンシパルを識別します。請求処理はアプリケーション固有です。
件名	サブ	トークンのサブジェクトまたはユーザ。名前のスコープは、グローバルまたはローカルで一意になります。
対象者	豪ドル	トークンの対象となる受信者。文字列の配列として実装されます。

請求	キーワード	説明
有効期限	有効期限	トークンが期限切れになり、拒否されるまでの時間。

を参照してください ["RFC 7519：JSON Webトークン"](#) を参照してください。

## ONTAPクライアント許可のオプション

ONTAPクライアント許可をカスタマイズするには、いくつかのオプションを使用できます。承認の決定は、最終的には、アクセストークンに含まれるか、アクセストークンから派生したONTAP RESTロールに基づいて行われます。



使用できるのは ["ONTAP RESTロール"](#) OAuth 2.0の認可を設定する場合。以前のONTAPの従来のロールはサポートされていません。

はじめに

ONTAP内のOAuth 2.0の実装は、柔軟性と堅牢性を考慮して設計されており、ONTAP環境を保護するために必要なオプションを提供します。大まかには、ONTAPクライアント許可を定義するための3つの主要な設定カテゴリがあります。これらの設定オプションを同時に指定することはできません。

ONTAPでは、構成に応じて最適な1つのオプションが適用されます。を参照してください ["ONTAPニヨルアクセスノケツテイハウハウ"](#) を参照して、アクセスを決定するためにONTAPで構成定義をどのように処理するかを確認してください。

## OAuth 2.0の自己完結型スコープ

これらのスコープには、1つ以上のカスタムRESTロールが含まれており、それぞれが1つの文字列にカプセル化されています。ONTAPロールの定義には依存しません。認可サーバーでこれらのスコープ文字列を定義する必要があります。

### ローカルのONTAP固有のRESTロールとユーザ

設定に基づいて、ローカルONTAP ID定義を使用してアクセスを決定できます。オプションは次のとおりです。

- 単一のネームドRESTロール
- ユーザ名とローカルONTAPユーザの照合

指定したロールのscope構文は、`* ontap-role-URL-encoded-ONTAP-role-name`です。たとえば、ロールが「admin」の場合、スコープ文字列は「ontap-role-admin」になります。

## Active DirectoryまたはLDAPグループ

ローカルONTAPの定義を調べても、アクセスを決定できない場合は、Active Directory（「domain」）またはLDAP（「nsswitch」）グループが使用されます。グループ情報は、次の2つの方法のいずれかで指定できます。

- OAuth 2.0スコープ文字列

グループメンバーシップを持つユーザがない場合、クライアントのクレデンシャルフローを使用して機密アプリケーションをサポートします。スコープには`* ontap-group-URL-encoded-ONTAP-group-name`という名前を付けます。たとえば、グループが「development」の場合、スコープ文字列は「ontap-group-development」になります。

- 「グループ」の主張

これは、リソース所有者(パスワード付与)フローを使用してADFSによって発行されるアクセストークンを対象としています。

#### 自己完結型OAuth 2.0スコープ

自己完結型スコープは、アクセストークンで伝送される文字列です。各ロールは完全なカスタムロール定義であり、アクセスを決定するためにONTAPが必要とするすべての機能が含まれています。スコープは、ONTAP内で定義されているRESTロールとは別のものです。

#### スコープ文字列の形式

基本レベルでは、スコープは連続した文字列として表され、コロンで区切られた6つの値で構成されます。スコープ文字列で使用するパラメータについては、以下で説明します。

#### ONTAPリテラル

スコープはリテラル値で始まる必要があります `ontap` 小文字で入力します。これにより、範囲がONTAPに固有であることが識別されます。

#### クラスタ

スコープ環境となるONTAPクラスタを定義します。次の値を指定できます。

- クラスタUUID

単一のクラスタを識別します。

- アスタリスク(\*)

スコープ環境のすべてのクラスタを示します。

ONTAP CLIコマンドを使用できます。 `cluster identity show` をクリックしてクラスタのUUIDを表示します。指定しない場合は、スコープ環境 `all clusters` になります。

#### ロール

自己完結型スコープに含まれるRESTロールの名前。この値は、ONTAPで検証されたり、ONTAPに定義されている既存のRESTロールと照合されたりすることはありません。この名前はロギングに使用されます。

#### アクセスレベル

この値は、スコープ内でAPIエンドポイントを使用するときにクライアントアプリケーションに適用されるアクセスレベルを示します。次の表に示す6つの値があります。

アクセスレベル	説明
なし	指定したエンドポイントへのすべてのアクセスを拒否します。
- 読み取り専用	GETを使用した読み取りアクセスのみを許可します。



アクセスレベル	説明
READ_CREATE	POSTを使用して、読み取りアクセスと新しいリソースインスタンスの作成を許可します。
READ_MODIFY	読み取りアクセスを許可し、PATCHを使用して既存のリソースを更新する機能を許可します。
READ_CREATE_MODIFY	削除以外のすべてのアクセスを許可します。許可される処理は、GET（読み取り）、POST（作成）、およびPATCH（更新）です。
すべて	フルアクセスを許可します。

## SVM

クラスタ内のスコープ環境内のSVMの名前。すべてのSVMを示すために、\*（アスタリスク）を使用します。



この機能は、ONTAP 9.14.1では完全にはサポートされていません。SVMのパラメータは無視して、プレースホルダにアスタリスクを使用できます。を確認します ["ONTAP リリースノート"](#) をクリックしてSVMの今後のサポートを確認してください。

## REST API URI

リソースまたは関連リソースのセットへの完全パスまたは部分パス。文字列は次で始まる必要があります：  
/api。値を指定しない場合は、スコープ環境All APIエンドポイントがONTAPクラスタで指定されます。

### 範囲の例

自己完結型スコープの例を以下に示します。

**ONTAP : : joes-role : read\_create\_modify : : /api/cluster**

このロールを割り当てられたユーザに、 /cluster エンドポイント。

## CLI管理ツール

自己完結型スコープの管理を容易にし、エラーが発生しにくくするために、ONTAPにはCLIコマンドが用意されています。 security oauth2 scope 入力パラメータに基づいてスコープ文字列を生成します。

コマンド security oauth2 scope 入力内容に基づいて、次の2つのユースケースがあります。

- 文字列をスコープするCLIパラメータ

このバージョンのコマンドを使用すると、入力パラメータに基づいてスコープ文字列を生成できます。

- scope string to CLIパラメータ

このバージョンのコマンドを使用すると、入力スコープ文字列に基づいてコマンドパラメータを生成できます。

### 例

次の例では、次のコマンド例のあとに出力が含まれたスコープ文字列を生成します。定義は、すべてのクラスタを環境します。

```
security oauth2 scope cli-to-scope -role joes-role -access readonly -api  
/api/cluster
```

```
ontap:*:joes-role:readonly:*:/api/cluster
```

## ONTAPニヨルアクセスノケツテイハウハウ

OAuth 2.0を適切に設計および実装するには、ONTAPが許可設定を使用してクライアントのアクセスを決定する方法を理解する必要があります。

### ステップ1：自己完結型スコープ

アクセストークンに自己完結型のスコープが含まれている場合、ONTAPは最初にそれらのスコープを調べます。自己完結型スコープがない場合は、ステップ2に進みます。

1つ以上の自己完結型スコープが存在する場合、ONTAPは明示的な\*allow\*または\*deny\*決定が行われるまで、各スコープを適用します。明示的な決定が行われた場合、処理は終了します。

ONTAPが明示的にアクセスを決定できない場合は、手順2に進みます。

### 手順2：ローカルロールフラグを確認する

ONTAPがフラグの値を調べる `use-local-roles-if-present`。このフラグの値は、ONTAPに定義された認可サーバーごとに個別に設定されます。

- の場合 `true` 手順3に進みます。
- の場合 `false` 処理が終了し、アクセスが拒否されます。

### 手順3：名前付きONTAP RESTロール

アクセストークンに名前付きRESTロールが含まれている場合、ONTAPはそのロールを使用してアクセスを決定します。これにより、常に\* allow または deny \*の決定が行われ、処理が終了します。

名前付きRESTロールがない場合、またはロールが見つからない場合は、手順4に進みます。

### 手順4：ローカルONTAPユーザ

アクセストークンからユーザ名を抽出し、ローカルONTAPユーザと照合してみます。

ローカルONTAPユーザが一致した場合、ONTAPはそのユーザ用に定義されたロールを使用してアクセスを決定します。これにより、常に\* allow または deny \*の決定が行われ、処理が終了します。

ローカルONTAPユーザが一致しない場合、またはアクセストークンにユーザ名がない場合は、手順5に進みます。

### 手順5：グループとロールのマッピング

アクセストークンからグループを抽出し、グループと照合してみます。グループは、Active Directoryまたは同等のLDAPサーバを使用して定義します。

一致するグループがある場合、ONTAPはそのグループに定義されたロールを使用してアクセスを決定します。これにより、常に\* allow または deny \*の決定が行われ、処理が終了します。

一致するグループがない場合、またはアクセストークンにグループがない場合、アクセスは拒否され、処理は

終了します。

## OAuth 2.0の導入シナリオ

ONTAPに認可サーバーを定義するときに使用できる設定オプションはいくつかあります。これらのオプションに基づいて、展開環境に適した承認サーバーを作成できます。

### 設定パラメータの概要

ONTAPに認可サーバーを定義する際には、いくつかの設定パラメータを使用できます。これらのパラメータは、一般にすべての管理インターフェイスでサポートされています。

パラメータ名は、ONTAP管理インターフェイスによって多少異なります。たとえば、リモートイントロスペクションを設定する場合、エンドポイントはCLIコマンドパラメータを使用して識別されます。  
-introspection-endpoint。ただし、System Managerでは、同等のフィールドは\_AuthorizationサーバトークンイントロスペクションURI\_です。すべてのONTAP管理インターフェイスに対応するために、パラメータの一般的な概要が用意されています。正確なパラメータまたはフィールドは、コンテキストに基づいて明確にする必要があります。

パラメータ	説明
名前	ONTAPで認識されている認可サーバの名前。
アプリケーション	ONTAP内部アプリケーション定義環境。これは* http *である必要があります。
発行者URI	トークンを発行するサイトまたは組織を識別するパスを持つFQDN。
プロバイダJWKS URI	ONTAPがアクセストークンの検証に使用するJSON Webキーセットを取得するパスとファイル名を含むFQDN。
JWKS更新間隔	ONTAPがプロバイダJWKS URIから証明書情報を更新する頻度を決定する時間間隔。値はISO-8601形式で指定します。
イントロスペクションエンドポイント	ONTAPがイントロスペクションを通じてリモートトークン検証を実行するために使用するパスを持つFQDN。
クライアント ID	認可サーバで定義されているクライアントの名前。この値が含まれている場合は、インターフェイスに基づいて関連付けられたクライアントシークレットも指定する必要があります。
発信プロキシ	これは、ONTAPがファイアウォールの背後にある場合に、認可サーバへのアクセスを提供するためです。URIはcurl形式で指定する必要があります。
ローカルロールがある場合は使用	ローカルONTAP定義が使用されているかどうかを判断するブーリアンフラグ（名前付きRESTロールとローカルユーザを含む）。
ユーザ要求の削除	ONTAPがローカルユーザとの照合に使用する別名。を使用します sub ローカルユーザ名と一致するアクセストークンのフィールド。

### 導入シナリオ

いくつかの一般的な導入シナリオを次に示します。これらは、トークン検証がONTAPによってローカルで実行されるか、認証サーバによってリモートで実行されるかに基づいて編成されます。各シナリオには、必要な設定オプションのリストが含まれています。を参照してください ["ONTAPでのOAuth 2.0の導入"](#) コンフィギュレーションコマンドの例については、を参照してください。



認可サーバを定義したら、ONTAP管理インターフェイスを使用してその設定を表示できます。たとえば、次のコマンドを使用します。 `security oauth2 client show` ONTAP CLIを使用します。

## ローカル検証

次の導入シナリオは、ローカルでトークン検証を実行するONTAPに基づいています。

### プロキシなしで自己完結型スコープを使用する

これは、OAuth 2.0の自己完結型スコープのみを使用する最も単純な展開です。ローカルONTAP ID定義は使用されません。次のパラメータを指定する必要があります。

- 名前
- アプリケーション (http)
- プロバイダJWKS URI
- 発行者URI

また、認可サーバーでスコープを追加する必要があります。

### プロキシで自己完結型スコープを使用する

この展開シナリオでは、OAuth 2.0の自己完結型スコープを使用します。ローカルONTAP ID定義は使用されません。ただし、認可サーバはファイアウォールの内側にあるため、プロキシを設定する必要があります。次のパラメータを指定する必要があります。

- 名前
- アプリケーション (http)
- プロバイダJWKS URI
- 発信プロキシ
- 発行者URI
- 対象者

また、認可サーバーでスコープを追加する必要があります。

### ローカルユーザロールとデフォルトユーザ名のマッピングをプロキシで使用する

この導入シナリオでは、ローカルユーザロールとデフォルトのネームマッピングを使用します。リモートユーザ要求では、のデフォルト値が使用されます。 `sub` アクセストークンのこのフィールドはローカルユーザー名と一致するために使用されます。ユーザ名は40文字以下にする必要があります。認証サーバはファイアウォールの内側にあるため、プロキシを設定する必要もあります。次のパラメータを指定する必要があります。

- 名前
- アプリケーション (http)
- プロバイダJWKS URI
- ローカルロールがある場合は使用 (true)
- 発信プロキシ

- 発行者

ローカルユーザがONTAPに定義されていることを確認する必要があります。

ローカルユーザロールと代替ユーザ名マッピングをプロキシで使用する

この導入シナリオでは、ローカルユーザロールと代替ユーザ名を使用して、ローカルONTAPユーザを照合します。認証サーバはファイアウォールの背後にあるため、プロキシを設定する必要があります。次のパラメータを指定する必要があります。

- 名前
- アプリケーション (http)
- プロバイダJWKS URI
- ローカルロールがある場合は使用 (true)
- リモートユーザの要求
- 発信プロキシ
- 発行者URI
- 対象者

ローカルユーザがONTAPに定義されていることを確認する必要があります。

リモートイントロスペクション

次の展開構成は、イントロスペクションを介してリモートでトークン検証を実行するONTAPに基づいています。

プロキシなしで自己完結型スコープを使用する

これは、OAuth 2.0の自己完結型スコープを使用したシンプルな展開です。ONTAP ID定義は使用されません。次のパラメータを指定する必要があります。

- 名前
- アプリケーション (http)
- イントロスペクションエンドポイント
- クライアント ID
- 発行者URI

認可サーバーでは、スコープ、およびクライアントシークレットを定義する必要があります。

相互TLSを使用したクライアント認証

セキュリティのニーズに応じて、オプションでMutual TLS (MTLS) を設定して強力なクライアント認証を実装できます。OAuth 2.0展開の一部としてONTAPで使用される場合、MTLSはアクセストークンが最初に発行されたクライアントによってのみ使用されることを保証します。

## OAuth 2.0を使用した相互TLS

Transport Layer Security (TLS) は、2つのアプリケーション（通常はクライアントブラウザとWebサーバ）間にセキュアな通信チャネルを確立するために使用されます。相互TLSは、クライアント証明書を介してクライアントを強力に識別できるようにすることで、これを拡張します。OAuth 2.0を使用したONTAPクラスタで使用する場合、送信者に制約されたアクセストークンを作成して使用することで、基本的なMTLS機能が拡張されます。

送信者に制約されたアクセストークンは、最初に発行されたクライアントのみが使用できます。この機能をサポートするために、新しい確認請求 (cnf) がトークンに挿入されます。フィールドにプロパティが含まれています `x5t#S256` アクセストークンを要求するときに使用されるクライアント証明書のダイジェストを保持します。この値は、トークンの検証の一環としてONTAPによって検証されます。送信者に制約されていない許可サーバによって発行されたアクセストークンには、追加の確認要求は含まれません。

認可サーバごとにMTLSを個別に使用するようにONTAPを設定する必要があります。たとえば、CLIコマンド `security oauth2 client` パラメータを含む `use-mutual-tls` 次の表に示す3つの値に基づいてMTLS処理を制御します。



各構成で、ONTAPによって実行される結果とアクションは、構成パラメータの値、およびアクセストークンとクライアント証明書の内容によって異なります。テーブル内のパラメータは、最小から最も制限の厳しいものに分類されています。

パラメータ	説明
なし	OAuth 2.0相互TLS認証は、認可サーバでは完全に無効になっています。ONTAPは、確認要求がトークンに含まれている場合やクライアント証明書がTLS接続で提供されている場合でも、MTLSクライアント証明書認証を実行しません。
リクエスト	OAuth 2.0相互TLS認証は、送信者に制約されたアクセストークンがクライアントによって提示された場合に適用されます。つまり、MTLSは、確認請求（財産を含む）の場合にのみ適用されます。 <code>x5t#S256</code> がアクセストークンに含まれています。これがデフォルト設定です。
必須	OAuth 2.0相互TLS認証は、認可サーバによって発行されたすべてのアクセストークンに適用されます。したがって、すべてのアクセストークンは送信者に制約される必要があります。アクセストークンに確認要求がない場合、または無効なクライアント証明書がある場合、認証およびREST API要求は失敗します。

### 導入フローの概要

ONTAP環境でOAuth 2.0でMTLSを使用する場合の一般的な手順を以下に示します。を参照してください  
["RFC 8705：『OAuth 2.0 Mutual-TLS Client Authentication and Certificate-Bound Access Tokens』"](#) 詳細：

#### 手順1：クライアント証明書を作成してインストールする

クライアントIDの確立は、クライアントの秘密鍵に関する知識の証明に基づいています。対応する公開鍵は、クライアントから提示された署名付きX.509証明書に配置されます。クライアント証明書の作成手順の概要は次のとおりです。

1. 公開鍵と秘密鍵のペアを生成する
2. 証明書署名要求を作成する
3. CSRファイルを既知のCAに送信する

#### 4. CAが要求を検証し、署名済み証明書を発行

通常、クライアント証明書はローカルのオペレーティングシステムにインストールするか、curlなどの一般的なユーティリティを使用して直接使用できます。

##### ステップ2：MTLSを使用するようにONTAPを設定する

MTLSを使用するようにONTAPを設定する必要があります。この設定は、認可サーバごとに個別に行われます。たとえば、CLIでは次のコマンドを使用します。security oauth2 client は、オプションのパラメータとともに使用されます。use-mutual-tls。を参照してください "[ONTAPでのOAuth 2.0の導入](#)" を参照してください。

##### 手順3：クライアントがアクセストークンを要求する

クライアントは、ONTAPに設定された認証サーバからアクセストークンを要求する必要があります。クライアントアプリケーションは、手順1で作成およびインストールした証明書でMTLSを使用する必要があります。

##### ステップ4: 認証サーバがアクセストークンを生成する

認可サーバはクライアント要求を検証し、アクセストークンを生成します。この一部として、クライアント証明書のメッセージダイジェストが作成されます。このダイジェストは、トークンに確認要求として含まれます（フィールド cnf）。

##### 手順5：クライアントアプリケーションがONTAPにアクセストークンを提示する

クライアントアプリケーションは、ONTAPクラスタへのREST API呼び出しを実行し、アクセストークンを\* bearerトークン\*として承認要求ヘッダーに含めます。クライアントは、アクセストークンの要求に使用したのと同じ証明書を持つMTLSを使用する必要があります。

##### ステップ6: ONTAPはクライアントとトークンを検証します。

ONTAPは、HTTP要求でアクセストークンと、MTLS処理の一部として使用されるクライアント証明書を受信します。ONTAPは最初にアクセストークンの署名を検証します。設定に基づいて、ONTAPはクライアント証明書のメッセージダイジェストを生成し、トークン内の確認要求\* cnf\*と比較します。2つの値が一致する場合、ONTAPは、API要求を行うクライアントがアクセストークンが最初に発行されたクライアントと同じであることを確認しました。

## 構成と導入

### ONTAPを使用したOAuth 2.0の導入準備

ONTAP環境でOAuth 2.0を構成する前に、展開の準備をする必要があります。主なタスクと決定事項の概要を以下に示します。セクションの配置は、通常、従うべき順序に沿って配置されます。ただし、ほとんどの環境に適用できますが、必要に応じて環境に適応する必要があります。また、正式な導入計画の作成も検討する必要があります。



環境に応じて、ONTAPに定義されている認証サーバの設定を選択できます。これには、導入のタイプごとに指定する必要があるパラメータ値も含まれます。を参照してください "[OAuth 2.0の導入シナリオ](#)" を参照してください。

### リソースとクライアントアプリケーションを保護

OAuth 2.0は、保護されたリソースへのアクセスを制御するための承認フレームワークです。このため、導入

の最初の重要なステップは、使用可能なリソースと、それらにアクセスする必要があるクライアントを特定することです。

クライアントアプリケーションを特定する

REST API呼び出しを発行するときにOAuth 2.0を使用するクライアントと、アクセスが必要なAPIエンドポイントを決定する必要があります。

既存のONTAP RESTロールとローカルユーザの確認

RESTロールやローカルユーザなど、既存のONTAP IDの定義を確認する必要があります。OAuth 2.0の設定方法によっては、これらの定義を使用してアクセスを決定できます。

**OAuth 2.0**へのグローバルな移行

OAuth 2.0認証を段階的に実装することもできますが、各認証サーバーにグローバルフラグを設定することで、すべてのREST APIクライアントをOAuth 2.0にすぐに移動することもできます。これにより、自己完結型スコープを作成することなく、既存のONTAP構成に基づいてアクセスを決定できます。

認証サーバ

認証サーバーは、アクセストークンを発行し、管理ポリシーを適用することで、OAuth 2.0の展開において重要な役割を果たします。

認可サーバーを選択してインストールします。

1つ以上の認可サーバーを選択してインストールする必要があります。スコープの定義方法など、アイデンティティプロバイダの設定オプションと手順を理解することが重要です。

認証ルート**CA**証明書をインストールする必要があるかどうかを判断する

ONTAPでは、認証サーバの証明書を使用して、クライアントから提示された署名済みアクセストークンを検証します。これを行うには、ONTAPにルートCA証明書と中間証明書が必要です。ONTAPがプリインストールされている場合があります。そうでない場合は、インストールする必要があります。

ネットワークの場所と構成の評価

認証サーバがファイアウォールの背後にある場合は、プロキシサーバを使用するようにONTAPを設定する必要があります。

クライアントの認証と許可

クライアントの認証と許可には、いくつかの側面を考慮する必要があります。

自己完結型スコープまたはローカル**ONTAP ID**定義

大まかに言えば、認可サーバーで定義された自己完結型スコープを定義することも、役割やユーザーを含む既存のローカルONTAP ID定義に依存することもできます。

ローカル**ONTAP**処理を使用するオプション

ONTAP ID定義を使用する場合は、適用するものを次のように決定する必要があります。

- ネームドRESTロール
- ローカルユーザの一致
- Active DirectoryまたはLDAPグループ

ローカル検証またはリモートイントロスペクション



アクセストークンがONTAPによってローカルで検証されるか、イントロスペクションによって認可サーバーで検証されるかを決定する必要があります。また、更新間隔など、いくつかの関連する値も考慮する必要があります。

#### 送信者に制約されたアクセストークン

高度なセキュリティが必要な環境では、MTLSに基づいて送信制限付きアクセストークンを使用できます。これには、クライアントごとに証明書が必要です。

#### 管理インターフェイス

OAuth 2.0の管理は、次のいずれかのONTAPインターフェイスを使用して実行できます。

- コマンドラインインターフェイス
- System Manager の略
- REST API

#### クライアントニヨルアクセストークンノヨウキュウホウホウ

クライアントアプリケーションは、許可サーバからアクセストークンを直接要求する必要があります。許可の種類を含め、これをどのように行うかを決定する必要があります。

#### ONTAPの設定

ONTAPのいくつかの設定タスクを実行する必要があります。

#### RESTロールとローカルユーザを定義する

認証設定に基づいて、ローカルのONTAP識別処理を使用できます。この場合は、RESTロールとユーザ定義を確認して定義する必要があります。

#### コア構成

コアONTAP構成の実行には、主に次の3つの手順が必要です。

- 必要に応じて、認証サーバの証明書に署名したCAのルート証明書（および中間証明書）をインストールします。
- 認可サーバを定義します。
- クラスタに対してOAuth 2.0の処理を有効にします。

#### ONTAPでのOAuth 2.0の導入

OAuth 2.0のコア機能の展開には、主に3つのステップがあります。

##### 作業を開始する前に

ONTAPを設定する前に、OAuth 2.0の展開を準備する必要があります。たとえば、証明書がどのように署名されたか、ファイアウォールの内側にあるかなど、承認サーバを評価する必要があります。を参照してください ["ONTAPを使用したOAuth 2.0の導入準備"](#) を参照してください。

##### 手順1：認証サーバ証明書をインストールする

ONTAPには、多数のルートCA証明書が事前にインストールされています。そのため、多くの場合、認証サーバの証明書は追加の設定なしでONTAPによってすぐに認識されます。ただし、許可サーバ証明書の署名方法

によっては、ルートCA証明書と中間証明書のインストールが必要になる場合があります。

必要に応じて、次の手順に従って証明書をインストールします。必要な証明書はすべてクラスタレベルでインストールする必要があります。

ONTAPへのアクセス方法に基づいて、正しい手順を選択します。

#### 例 17. 手順

##### System Manager の略

1. System Managerで、[クラスタ]>\*[設定]\*を選択します。
2. [セキュリティ]\*セクションまで下にスクロールします。
3. の横にある→\*をクリックします。
4. タブで[追加]\*をクリックします。
5. [インポート]\*をクリックし、証明書ファイルを選択します。
6. 環境に合わせて設定パラメータを設定します。
7. [ 追加（Add） ] をクリックします。

##### CLI の使用

1. インストールを開始します。

```
security certificate install -type server-ca
```

2. 次のコンソールメッセージを確認します。

```
Please enter Certificate: Press <Enter> when done
```

3. 証明書ファイルをテキストエディタで開きます。
4. 次の行を含む証明書全体をコピーします。

```
-----BEGIN CERTIFICATE-----
```

```
-----END CERTIFICATE-----
```

5. コマンドプロンプトの後に証明書を端末に貼り付けます。
6. Enter\*キーを押してインストールを完了します。
7. 次のいずれかを使用して証明書がインストールされていることを確認します。

```
security certificate show-user-installed
```

```
security certificate show
```

#### 手順2：認証サーバを設定する

ONTAPに対する認可サーバを少なくとも1つ定義する必要があります。設定と導入計画に基づいてパラメータ値を選択する必要があります。レビュー "[OAuth2導入シナリオ](#)" をクリックして、構成に必要な正確なパラ

メータを決定します。



認可サーバー定義を変更するには、既存の定義を削除して新しい定義を作成します。

次の例は、最初のシンプルな導入シナリオに基づいています。"ローカル検証"。自己完結型スコープはプロキシなしで使用されます。

ONTAPへのアクセス方法に基づいて、正しい手順を選択します。CLI手順では、コマンドを実行する前に置き換える必要があるシンボリック変数を使用します。

#### 例 18. 手順

##### System Manager の略

1. System Managerで、[クラスタ]>[設定]\*を選択します。
2. [セキュリティ]\*セクションまで下にスクロールします。
3. \* OAuth 2.0 authorization の横にある+\*をクリックします。
4. [その他のオプション]\*を選択します。
5. 導入に必要な値を次のように指定します。
  - 名前
  - アプリケーション (http)
  - プロバイダJWKS URI
  - 発行者URI
6. [追加 (Add) ]をクリックします。

##### CLI の使用

1. 定義を再作成します。

```
security oauth2 client create -config-name <NAME> -provider-jwks-uri  
<URI_JWKS> -application http -issuer <URI_ISSUER>
```

例：

```
security oauth2 client create \  
-config-name auth0 \  
-provider-jwks-uri https://superzap.dev.netapp.com:8443/realms/my-  
realm/protocol/openid-connect/certs \  
-application http \  
-issuer https://superzap.dev.netapp.com:8443/realms/my-realm
```

### 手順3：OAuth 2.0を有効にする

最後のステップは、OAuth 2.0を有効にすることです。これはONTAPクラスタのグローバル設定です。



ONTAP、認可サーバー、およびサポートサービスがすべて正しく設定されていることを確認するまで、OAuth 2.0の処理を有効にしないでください。

ONTAPへのアクセス方法に基づいて、正しい手順を選択します。

#### 例 19. 手順

##### System Manager の略

1. System Managerで、[クラスタ]>[設定]\*を選択します。
2. [セキュリティ]セクション\*まで下にスクロールします。
3. \* OAuth 2.0 authorization の横にある→\*をクリックします。
4. \* OAuth 2.0認証\*を有効にします。

##### CLI の使用

1. OAuth 2.0を有効にします。

```
security oauth2 modify -enabled true
```

2. OAuth 2.0が有効になっていることを確認します。

```
security oauth2 show  
Is OAuth 2.0 Enabled: true
```

### OAuth 2.0を使用したREST API呼び出しの問題

ONTAPのOAuth 2.0実装では、REST APIクライアントアプリケーションがサポートされています。curlを使用して簡単なREST API呼び出しを問題し、OAuth 2.0の使用を開始できます。次の例は、ONTAPクラスタのバージョンを取得します。

作業を開始する前に

ONTAPクラスタに対してOAuth 2.0機能を設定して有効にする必要があります。これには、認可サーバーの定義が含まれます。

#### ステップ1：アクセストークンを取得する

REST API呼び出しで使用するアクセストークンを取得する必要があります。トークン要求はONTAPの外部で実行され、正確な手順は認可サーバとその設定によって異なります。Webブラウザ、curlコマンド、またはプログラミング言語を使用してトークンを要求できます。

説明のために、curlを使用してKeycloakからアクセストークンを要求する方法の例を以下に示します。

## キークロークの例

```
curl --request POST \  
--location  
'https://superzap.dev.netapp.com:8443/realms/peterson/protocol/openid-  
connect/token' \  
--header 'Content-Type: application/x-www-form-urlencoded' \  
--data-urlencode 'client_id=dp-client-1' \  
--data-urlencode 'grant_type=client_credentials' \  
--data-urlencode 'client_secret=5iTUf9QKLGxAoYaliR33v1D5A2xq09V7'
```

返されたトークンをコピーして保存する必要があります。

### 手順2：REST API呼び出しを問題する

有効なアクセストークンを取得したら、curlコマンドとアクセストークンを使用してREST API呼び出しを問題できます。

### パラメータと変数

curlの例の2つの変数について、次の表で説明します。

変数（ <b>Variable</b> ）	説明
\$FQDN_IP	ONTAP管理LIFの完全修飾ドメイン名またはIPアドレス。
\$access_token	認可サーバーによって発行されたOAuth 2.0アクセストークン。

curlの例を発行する前に、まずBashシェル環境でこれらの変数を設定する必要があります。たとえば、Linux CLIで次のコマンドを入力して、FQDN変数を設定および表示します。

```
FQDN_IP=172.14.31.224  
echo $FQDN_IP  
172.14.31.224
```

両方の変数をローカルのBashシェルで定義したら、curlコマンドをコピーしてCLIに貼り付けることができます。Enter \*を押して変数を置き換え、コマンドを問題します。

### カールの例

```
curl --request GET \  
--location "https://$FQDN_IP/api/cluster?fields=version" \  
--include \  
--header "Accept: */*" \  
--header "Authorization: Bearer $ACCESS_TOKEN"
```

# SAML 認証を設定する

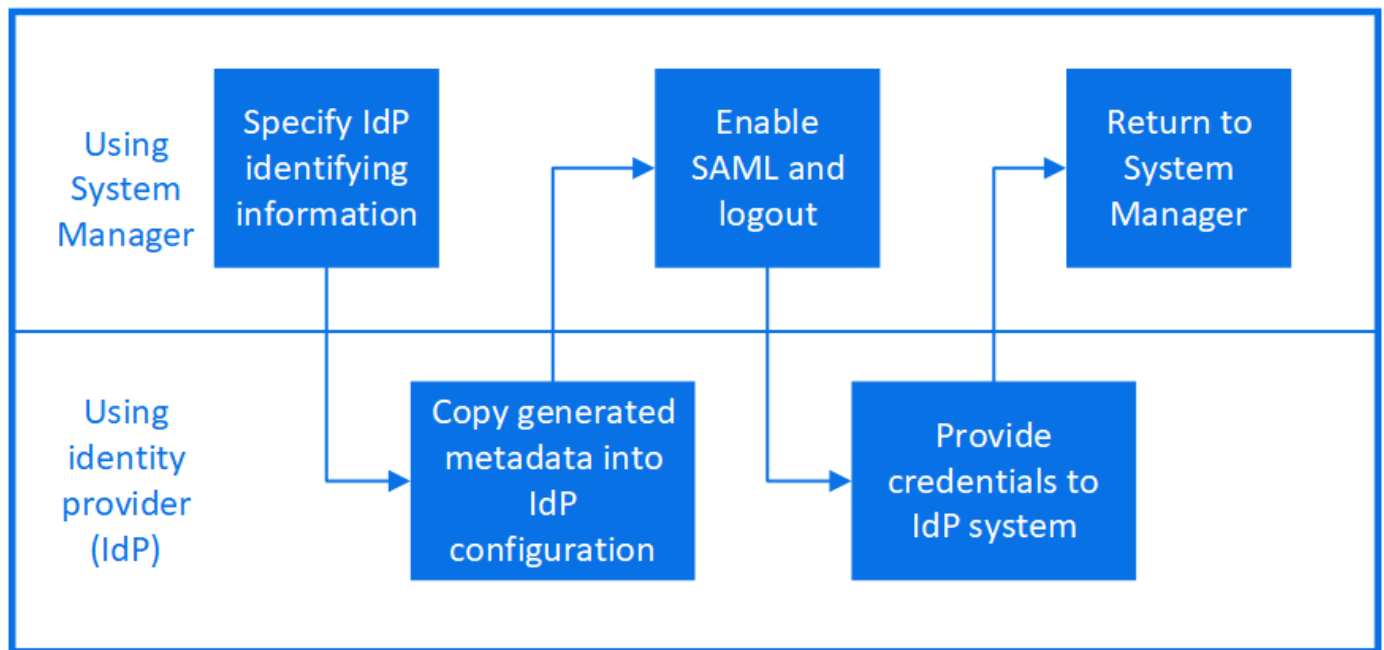
ONTAP 9.3 以降では、Web サービスに Security Assertion Markup Language (SAML) 認証を設定できます。SAML 認証を設定して有効にすると、Active Directory や LDAP などのディレクトリサービスプロバイダではなく、外部のアイデンティティプロバイダ (IdP) によってユーザが認証されます。

## SAML 認証を有効にする

System Manager または CLI を使用して SAML 認証を有効にするには、次の手順を実行します。クラスターで ONTAP 9.7 以前が実行されている場合は、System Manager で実行する手順が異なります。ご使用のシステムで利用可能な System Manager のオンラインヘルプを参照してください。



SAML 認証を有効にすると、System Manager の GUI にアクセスできるのはリモートユーザだけになります。ローカルユーザは、SAML 認証を有効にしたあとで System Manager GUI にアクセスできません。



作業を開始する前に

- リモート認証に使用する IdP を設定する必要があります。



設定済みの IdP から提供されたドキュメントを参照してください。

- IdP の URI が必要です。

このタスクについて

- SAML 認証は、にのみ適用されます http および ontapi アプリケーション：
  - 。 http および ontapi アプリケーションは、サービスプロセッサインフラ、ONTAP API、または System Manager の Web サービスで使用されます。


- SAML 認証は、管理 SVM へのアクセス時にのみ適用できます。

次のIdPがSystem Managerで検証されました。

- Active Directory フェデレーションサービス
- Cisco Duo（次のONTAPバージョンで検証済み）
  - 9.7P21以降の9.7リリース（"[System Managerのクラシックドキュメント](#)")
  - 9.8P17以降の9.8リリース
  - 9.9.1P13以降の9.9リリース
  - 9.10.1P9以降の9.10リリース
  - 9.11.1P4以降の9.11リリース
  - 9.12.1以降のリリース
- Shibboleth

環境に応じて、次の手順を実行します。

### System Manager の略

1. [Cluster] > [Settings] の順にクリックします。
2. SAML 認証 \* の横にあるをクリックします .
3. SAML 認証を有効にする \* チェックボックスがオンになっていることを確認します。
4. IdP URI の URL (を含む) を入力します "<a href="https://"" class="bare">https://"</a>)。
5. 必要に応じて、ホストシステムのアドレスを変更します。
6. 正しい証明書が使用されていることを確認します。
  - タイプが「server」の証明書が1つだけシステムにマッピングされている場合、その証明書はデフォルトとみなされ、表示されません。
  - システムが「server」タイプの複数の証明書にマッピングされている場合は、いずれかの証明書が表示されます。別の証明書を選択するには、\* Change \* をクリックします。
7. [保存 (Save)] をクリックします。確認ウィンドウには、自動的にクリップボードにコピーされたメタデータ情報が表示されます。
8. 指定した IdP システムに移動し、クリップボードからメタデータをコピーしてシステムメタデータを更新します。
9. 確認ウィンドウ (System Manager) に戻り、チェックボックスをオンにします。\* ホスト URI またはメタデータで IdP を設定しました。\*
10. Logout \* をクリックして、SAML ベースの認証を有効にします。IdP システムに認証画面が表示されます。
11. IdP システムで、SAML ベースのクレデンシャルを入力します。クレデンシャルを確認すると、System Manager のホームページが表示されます。

### CLI の使用

1. SAML の設定を作成して、ONTAP が IdP メタデータにアクセスできるようにします。

```
security saml-sp create -idp-uri idp_uri -sp-host ontap_host_name
```

idp\_uri は、IdP メタデータのダウンロード元の IdP ホストの FTP アドレスまたは HTTP アドレスです。

ontap\_host\_name は、SAML サービスプロバイダホスト (ここでは ONTAP システム) のホスト名または IP アドレスです。デフォルトでは、クラスタ管理 LIF の IP アドレスが使用されます。

必要に応じて、ONTAP サーバ証明書の情報を指定できます。デフォルトでは、ONTAP Web サーバ証明書の情報が使用されます。



```
cluster_12::> security saml-sp create -idp-uri  
https://example.url.net/idp/shibboleth
```

Warning: This restarts the web server. Any HTTP/S connections that are active

will be disrupted.

Do you want to continue? {y|n}: y

[Job 179] Job succeeded: Access the SAML SP metadata using the URL:  
https://10.0.0.1/saml-sp/Metadata

Configure the IdP and Data ONTAP users for the same directory server domain to ensure that users are the same for different authentication methods. See the "security login show" command for the Data ONTAP user configuration.

ONTAP ホストメタデータにアクセスするための URL が表示されます。

2. IdP ホストから、ONTAP ホストメタデータを使用して IdP を設定します。

IdP の設定の詳細については、IdP のマニュアルを参照してください。

3. SAML の設定を有効にします。

```
security saml-sp modify -is-enabled true
```

にアクセスする既存のユーザ http または ontapi アプリケーションで SAML 認証が自動的に設定されます。

4. のユーザを作成する場合 http または ontapi アプリケーション SAML の設定後、新しいユーザの認証方式として SAML を指定します。

- a. SAML 認証を使用する新しいユーザのログイン方法を作成します。

[+]

```
security login create -user-or-group-name user_name -application [http |  
ontapi] -authentication-method saml -vserver svm_name
```

```
cluster_12::> security login create -user-or-group-name admin1  
-application http -authentication-method saml -vserver  
cluster_12
```

- b. ユーザエントリが作成されたことを確認します。

```
security login show
```

```
cluster_12::> security login show
```

```
Vserver: cluster_12
```

```
Second
```

User/Group	Authentication	Acct
Name	Application Method	Role Name
Method		Locked
admin	console	password
none		admin
admin	http	password
none		admin
admin	http	saml
none		admin
admin	ontapi	password
none		admin
admin	ontapi	saml
none		admin
admin	service-processor	password
none		admin
admin	ssh	password
none		admin
admin1	http	password
none		backup
**admin1	http	saml
none**		backup


## SAML 認証を無効にする

外部のアイデンティティプロバイダ（IdP）を使用して Web ユーザの認証を停止する場合は、SAML 認証を無効にすることができます。SAML 認証が無効な場合は、Active Directory や LDAP などの設定済みのディレクトリサービスプロバイダが認証に使用されます。

環境に応じて、次の手順を実行します。

## 例 21. 手順

### System Manager の略

1. [Cluster] > [Settings] の順にクリックします。
2. [\* SAML Authentication\* ( SAML 認証) ] で、[\* Enabled \* (有効\*) ] トグルボタンをクリックします。
3. オプション:  [SAML 認証\*] の横にある [SAML 認証を有効にする\*] チェックボックスをオフにします

### CLI の使用

1. SAML 認証を無効にする

```
security saml-sp modify -is-enabled false
```

2. SAML 認証を使用しなくなった場合や IdP を変更する場合は、SAML の設定を削除します。

```
security saml-sp delete
```

## SAML の設定に関する問題のトラブルシューティング

Security Assertion Markup Language ( SAML ) 認証の設定に失敗した場合は、SAML の設定に失敗した各ノードを手動で修復して、障害からリカバリできます。修復プロセスの実行中は、Web サーバが再起動され、アクティブな HTTP 接続または HTTPS 接続が中断されます。

### このタスクについて

SAML 認証の設定時に、ONTAP は SAML の設定をノード単位で適用します。SAML 認証を有効にすると、ONTAP は設定の問題がある場合に自動的に各ノードを修復しようとします。いずれかのノードで SAML の設定に関する問題がある場合は、SAML 認証を無効にしてから再度有効にすることができます。SAML 認証を再度有効にしたあとも、1 つ以上のノードに SAML の設定を適用できない場合があります。SAML の設定に失敗したノードを特定し、そのノードを手動で修復できます。

### 手順

1. advanced 権限レベルにログインします。

```
set -privilege advanced
```

2. SAML の設定に失敗したノードを特定します。

```
security saml-sp status show -instance
```

```
cluster_12::~*> security saml-sp status show -instance

Node: node1
Update Status: config-success
Database Epoch: 9
Database Transaction Count: 997
Error Text:
SAML Service Provider Enabled: false
ID of SAML Config Job: 179

Node: node2
Update Status: config-failed
Database Epoch: 9
Database Transaction Count: 997
Error Text: SAML job failed, Reason: Internal error.
Failed to receive the SAML IDP Metadata file.
SAML Service Provider Enabled: false
ID of SAML Config Job: 180
2 entries were displayed.
```

3. 障害が発生したノードで SAML の設定を修復します。

**security saml-sp repair -node *node\_name***

```
cluster_12::~*> security saml-sp repair -node node2

Warning: This restarts the web server. Any HTTP/S connections that are
active
will be disrupted.
Do you want to continue? {y|n}: y
[Job 181] Job is running.
[Job 181] Job success.
```

Web サーバが再起動され、アクティブな HTTP 接続または HTTPS 接続が中断されます。

4. すべてのノードで SAML が正常に設定されたことを確認します。

**security saml-sp status show -instance**

```
cluster_12::*> security saml-sp status show -instance

Node: node1
Update Status: config-success
Database Epoch: 9
Database Transaction Count: 997
Error Text:
SAML Service Provider Enabled: false
ID of SAML Config Job: 179

Node: node2
Update Status: **config-success**
Database Epoch: 9
Database Transaction Count: 997
Error Text:
SAML Service Provider Enabled: false
ID of SAML Config Job: 180
2 entries were displayed.
```

#### 関連情報

["ONTAP 9コマンド"](#)

## Web サービスを管理します

### Manage Web Services の概要

クラスタまたは Storage Virtual Machine（SVM）の Web サービスを有効または無効にしたり、Web サービスの設定を表示したり、ロールのユーザが Web サービスにアクセスできるかどうかを管理したりできます。

クラスタまたは SVM の Web サービスは次の方法で管理できます。

- 特定の Web サービスを有効または無効にします
- Web サービスへのアクセスを暗号化された HTTP（SSL）のみに制限するかどうかを指定する
- Web サービスの可用性を表示します
- あるロールのユーザに Web サービスへのアクセスを許可するかどうか
- Web サービスへのアクセスが許可されているロールを表示する

ユーザが Web サービスにアクセスするには、次の条件をすべて満たしている必要があります。

- ユーザが認証されている必要があります。

たとえば、Web サービスからユーザ名とパスワードの入力を求められる場合があります。ユーザの応答は有効なアカウントと一致する必要があります。

- ユーザに正しいアクセス方法が設定されていること。

指定された Web サービスの正しいアクセス方法が設定されたユーザのみが正常に認証されます。ONTAP API Webサービス用 (ontapi) を使用する場合は、を使用する必要があります ontapi アクセス方法。その他のすべてのWebサービスの場合は、が必要です http アクセス方法。



を使用します security login ユーザのアクセス方法と認証方法を管理するコマンド。

- Web サービスがユーザのアクセス制御ルールを許可するように設定されている必要があります。



を使用します vservice services web access ルールのWebサービスへのアクセスを制御するコマンド。

ファイアウォールが有効になっている場合は、Web サービスに使用する LIF のファイアウォールポリシーを設定して、HTTP または HTTPS を許可する必要があります。

Web サービスアクセスに HTTPS を使用する場合は、Web サービスを提供するクラスタまたは SVM の SSL を有効にし、そのクラスタまたは SVM のデジタル証明書を提供する必要もあります。

## Web サービスへのアクセスを管理します

Web サービスは、HTTP または HTTPS を使用してユーザがアクセスできるアプリケーションです。クラスタ管理者は Web プロトコルエンジンをセットアップし、SSL を設定し、Web サービスを有効にし、ロールのユーザが Web サービスにアクセスできるようにします。

ONTAP 9.6 以降では、次の Web サービスがサポートされます。

- サービスプロセッサインフラ (spi)

このサービスによって、ノードのログファイル、コアダンプファイル、および MIB ファイルに、クラスタ管理 LIF またはノード管理 LIF から HTTP または HTTPS でアクセスできるようになります。デフォルト設定はです enabled。

ノードのログファイルまたはコアダンプファイルへのアクセス要求が発生すると、が表示されます spi Webサービスは、あるノードからファイルが存在する別のノードのルートボリュームへのマウントポイントを自動的に作成します。マウントポイントを手動で作成する必要はありません。。

- ONTAP API (ontapi)

このサービスでは、ONTAP API を実行し、リモートプログラムで管理機能を実行できます。デフォルト設定はです enabled。

一部の外部管理ツールではこのサービスが必要になる場合があります。たとえば、System Manager を使用する場合、このサービスを有効にしておく必要があります。

- Data ONTAP 検出 (disco)

このサービスは、外部の管理アプリケーションがネットワーク内のクラスタを検出できるようにします。デフォルト設定はです enabled。

- Support Diagnostics（診断）の略 (supdiag)

このサービスは、問題の分析と解決を支援するために、システム上の権限が設定された環境へのアクセスを制御します。デフォルト設定はです `disabled`。このサービスは、テクニカルサポートから指示があった場合にのみ有効にしてください。

- System Manager の略 (sysmgr)

このサービスは、ONTAP に組み込まれている System Manager の可用性を管理します。デフォルト設定はです `enabled`。このサービスはクラスタでのみサポートされます。

- ファームウェアベースボード管理コントローラ（BMC）の更新 (FW\_BMC)

このサービスを使用すると、BMC ファームウェアファイルをダウンロードできます。デフォルト設定はです `enabled`。

- ONTAP のドキュメント (docs)

このサービスでは、ONTAP のドキュメントにアクセスできます。デフォルト設定はです `enabled`。

- ONTAP RESTful API (docs\_api)

このサービスを使用すると、ONTAP RESTful API のドキュメントにアクセスできます。デフォルト設定はです `enabled`。

- ファイルのアップロードとダウンロード (fud)

このサービスは、ファイルのアップロードとダウンロードを提供します。デフォルト設定はです `enabled`。

- ONTAP メッセージング (ontapmsg)

このサービスでは、イベントをサブスクライブできるパブリッシュおよびサブスクライブインターフェイスがサポートされています。デフォルト設定はです `enabled`。

- ONTAP ポータル (portal)

このサービスは、ゲートウェイを仮想サーバに実装します。デフォルト設定はです `enabled`。

- ONTAP RESTful インターフェイス (rest)

このサービスは、クラスティンフラのすべての要素をリモートで管理するために使用する RESTful インターフェイスをサポートします。デフォルト設定はです `enabled`。

- Security Assertion Markup Language（SAML）サービスプロバイダのサポート (saml)

このサービスは、SAML サービスプロバイダをサポートするためのリソースを提供します。デフォルト設定はです `enabled`。

- SAML サービスプロバイダ (saml-sp)

このサービスは、SP メタデータやアサーションコンシューマサービスなどのサービスをサービスプロバイダに提供します。デフォルト設定はです `enabled`。

ONTAP 9.7 以降では、次の追加サービスがサポートされます。

- 設定バックアップファイル (backups)

このサービスでは、構成バックアップファイルをダウンロードできます。デフォルト設定はです `enabled`。

- ONTAPのセキュリティ (security)

このサービスでは、CSRF トークン管理をサポートして認証を強化しています。デフォルト設定はです `enabled`。

## Web プロトコルエンジンを管理します

クラスタ上で Web プロトコルエンジンを設定し、Web アクセスを許可するかどうか、およびどの SSL のバージョンが使用可能かを制御できます。Web プロトコルエンジンの設定を表示することもできます。

Web プロトコルエンジンは、次の方法でクラスタレベルで管理できます。

- を使用して、リモートクライアントがHTTPまたはHTTPSを使用してWebサービスコンテンツにアクセスできるかどうかを指定できます `system services web modify` コマンドにを指定します `-external` パラメータ
- を使用して、セキュアなWebアクセスにSSLv3を使用するかどうかを指定できます `security config modify` コマンドにを指定します `-supported-protocol` パラメータ  
デフォルトでは、SSLv3 は無効になっています。Transport Layer Security 1.0 (TLSv1.0) は有効になっており、必要に応じて無効にすることができます。
- クラスタ全体のコントロールプレーン Web サービスインターフェイスに対して、Federal Information Processing Standard (FIPS) 140-2 準拠モードを有効にすることができます。



FIPS 140-2 準拠モードは、デフォルトでは無効になっています。

- \* FIPS 140-2 準拠モードが無効な場合 \*

FIPS 140-2準拠モードを有効にするには、`is-fips-enabled` パラメータの値 `true` をクリックします `security config modify` コマンドを実行し、を使用します `security config show` コマンドを使用してオンラインステータスを確認します。

- \* FIPS 140-2 準拠モードが有効な場合 \*

- ONTAP 9.11.1以降では、TLSv1、TLSv1.1、およびSSLv3は無効になり、TLSv1.2とTLSv1.3のみが有効なままになります。ONTAP 9の内部および外部にある他のシステムや通信に影響します。FIPS 140-2準拠モードを有効にし、その後無効にした場合、TLSv1、TLSv1.1、およびSSLv3は無効のままになります。TLSV.1またはTLSv1 1.3は、前の設定に応じて有効のままになります。
- 9.11.1より前のバージョンのONTAP では、TLSv1とSSLv3は無効になり、TLSv1.1とTLSv1.2のみが引き続き有効になります。ONTAP では、FIPS 140-2 準拠モードが有効な場合、TLSv1 と SSLv3 を有効にすることはできません。FIPS 140-2 準拠モードを有効にし、その後無効にした場合、TLSv1 と SSLv3 は無効なままですが、以前の設定によっては、TLSv1.2 または TLSv1.1 と



TLSv1.2 の両方が有効になります。

- を使用して、クラスタ全体のセキュリティの設定を表示できます `system security config show` コマンドを実行します

ファイアウォールが有効になっている場合は、Web サービスに使用する論理インターフェイス（LIF）のファイアウォールポリシーを設定して、HTTP または HTTPS アクセスを許可する必要があります。

Web サービスアクセスに HTTPS を使用する場合は、Web サービスを提供するクラスタまたは Storage Virtual Machine（SVM）の SSL を有効にし、そのクラスタまたは SVM のデジタル証明書を提供する必要があります。

MetroCluster 構成では、クラスタ上の Web プロトコルエンジンの設定に対する変更内容は、パートナークラスタにレプリケートされません。

## Web プロトコルエンジンを管理するためのコマンド

を使用します `system services web` Web プロトコルエンジンを管理するコマンド。  
を使用します `system services firewall policy create` および `network interface modify` Web アクセス要求がファイアウォールを通過できるようにするコマンド。

状況	使用するコマンド
クラスタレベルで Web プロトコルエンジンを設定します。 <ul style="list-style-type: none"><li>• クラスタの Web プロトコルエンジンを有効または無効にします</li><li>• クラスタの SSLv3 を有効または無効にします</li><li>• セキュアな Web サービス（HTTPS）に対する FIPS 140-2 準拠を有効または無効にする</li></ul>	<code>system services web modify</code>
クラスタレベルの Web プロトコルエンジンの設定を表示し、Web プロトコルがクラスタ全体で機能しているかどうかを確認し、FIPS 140-2 準拠が有効でオンラインになっているかどうかを表示します	<code>system services web show</code>
ノードレベルの Web プロトコルエンジンの設定と、クラスタ内のノードに対する Web サービス処理のアクティビティを表示します	<code>system services web node show</code>
ファイアウォールポリシーを作成するか、既存のファイアウォールポリシーに HTTP または HTTPS プロトコルサービスを追加して、Web アクセス要求がファイアウォールを通過できるようにします	<code>system services firewall policy create</code> を設定します <code>-service</code> パラメータの値 <code>http</code> または <code>https</code> Web アクセス要求がファイアウォールを通過できるようにします。

状況	使用するコマンド
ファイアウォールポリシーを LIF と関連付ける	<pre>network interface modify</pre> <p>を使用できます <code>-firewall-policy</code> LIFのファイアウォールポリシーを変更するためのパラメータ。</p>

## Web サービスへのアクセスを設定する

Web サービスへのアクセスを設定することで、許可されたユーザが、HTTP または HTTPS を使用してクラスタまたは Storage Virtual Machine （SVM）のサービスコンテンツにアクセスできるようになります。

### 手順

1. ファイアウォールが有効になっている場合は、Web サービスで使用される LIF のファイアウォールポリシーで HTTP または HTTPS のアクセスがセットアップされていることを確認してください。



ファイアウォールが有効になっているかどうかは、を使用して確認できます `system services firewall show` コマンドを実行します

- a. ファイアウォールポリシーでHTTPまたはHTTPSが設定されていることを確認するには、を使用します `system services firewall policy show` コマンドを実行します

を設定します `-service` のパラメータ `system services firewall policy create` コマンドをに送信します `http` または `https` ポリシーでWebアクセスをサポートできるようにします。

- b. HTTPまたはHTTPSをサポートしているファイアウォールポリシーが、Webサービスを提供するLIFに関連付けられていることを確認するには、を使用します `network interface show` コマンドにを指定します `-firewall-policy` パラメータ

を使用します `network interface modify` コマンドにを指定します `-firewall-policy` LIFに対してファイアウォールポリシーを有効にするためのパラメータ。

2. クラスタレベルのWebプロトコルエンジンを設定してWebサービスのコンテンツにアクセスできるようにするには、を使用します `system services web modify` コマンドを実行します
3. セキュアなWebサービス（HTTPS）を使用する場合は、SSLを有効にし、を使用してクラスタまたはSVMのデジタル証明書情報を入力します `security ssl modify` コマンドを実行します
4. クラスタまたはSVMでWebサービスを有効にするには、を使用します `vserver services web modify` コマンドを実行します

この手順は、クラスタまたは SVM に対して有効にする各サービスについて繰り返す必要があります。

5. 特定のロールにクラスタまたはSVMのWebサービスへのアクセスを許可するには、を使用します `vserver services web access create` コマンドを実行します

アクセスを許可するロールはすでに存在している必要があります。を使用して、既存のロールを表示できます `security login role show` コマンドを実行するか、を使用して新しいロールを作成します `security login role create` コマンドを実行します

6. Webサービスへのアクセスが許可されているロールについては、の出力を確認して、ユーザにも正しいアクセス方法が設定されていることを確認してください `security login show` コマンドを実行します

をクリックしてONTAP API Webサービスにアクセスします `ontapi`）を使用してユーザを設定する必要があります `ontapi` アクセス方法。他のすべてのWebサービスにアクセスするには、ユーザがで設定されている必要があります `http` アクセス方法。



を使用します `security login create` コマンドを使用して、ユーザのアクセス方法を追加します。

## Web サービスを管理するためのコマンド

を使用します `vserver services web` クラスタまたはStorage Virtual Machine (SVM) のWebサービスの可用性を管理するためのコマンド。を使用します `vserver services web access` ロールのWebサービスへのアクセスを制御するコマンド。

状況	使用するコマンド
クラスタまたは SVM の Web サービスを次のように設定する  • Web サービスを有効または無効にします • Web サービスへのアクセスに HTTPS だけを使用できるようにするかどうかを指定します	<code>vserver services web modify</code>
クラスタまたは SVM の Web サービスの設定と可用性を表示する	<code>vserver services web show</code>
特定のロールに対して、クラスタまたは SVM の Web サービスへのアクセスを許可します	<code>vserver services web access create</code>
クラスタまたは SVM の Web サービスへのアクセスが許可されているロールを表示する	<code>vserver services web access show</code>
特定のロールに対して、クラスタまたは SVM の Web サービスへのアクセスを禁止する	<code>vserver services web access delete</code>

### 関連情報

["ONTAP 9コマンド"](#)

## ノード上のマウントポイントを管理するためのコマンド

。 `spi` Webサービスは、ノードのログファイルまたはコアファイルへのアクセス要求に応じて、1つのノードから別のノードのルートボリュームへのマウントポイントを自動的に作成します。マウントポイントを手動で管理する必要はありませんが、を使用して管理できます `system node root-mount` コマンド

状況	使用するコマンド
ノードから別のノードのルートボリュームへのマウントポイントを手動で作成します	<code>system node root-mount create</code> ノード間で作成できるマウントポイントは1つだけです。
クラスタ内のノード上の既存のマウントポイントを、マウントポイントが作成された時刻と現在の状態を含めて表示します	<code>system node root-mount show</code>
ノードから別のノードのルートボリュームへのマウントポイントを削除し、そのマウントポイントへの接続を強制的に終了します	<code>system node root-mount delete</code>

#### 関連情報

["ONTAP 9コマンド"](#)

## SSLの管理

SSL プロトコルは、デジタル証明書を使用して Web サーバとブラウザの間に暗号化された接続を確立することで、Web アクセスのセキュリティを向上させます。

クラスタまたは Storage Virtual Machine（SVM）の SSL は次の方法で管理できます。

- SSL の有効化
- デジタル証明書を生成してインストールし、クラスタまたは SVM と関連付ける
- SSL 設定を表示して SSL が有効かどうかを確認し、可能な場合は SSL 証明書名を表示します
- クラスタまたは SVM のファイアウォールポリシーを設定し、Web アクセス要求が通過できるようにします
- 使用できる SSL のバージョンを定義します
- Web サービスの HTTPS 要求のみにアクセスを制限する

## SSLの管理用コマンド



を使用します `security ssl` クラスタまたはStorage Virtual Machine（SVM）のSSLプロトコルを管理するコマンド。



状況	使用するコマンド
クラスタまたは SVM の SSL を有効にし、デジタル証明書を関連付けます	<code>security ssl modify</code>
クラスタまたは SVM の SSL 設定と証明書の名前を表示する	<code>security ssl show</code>

## Web サービスへのアクセスに関する問題のトラブルシューティングを行う

設定エラー原因 Web サービスへのアクセスに関する問題が発生します。このエラーに対応するには、LIF、ファイアウォールポリシー、Web プロトコルエンジン、Web サービス、デジタル証明書、すべてのユーザアクセス許可が正しく設定されていることを確認します。

次の表は、Web サービスの設定エラーを特定して対処する際に役立ちます。

アクセスに関する問題	原因となる設定エラー	エラーに対処する方法
Webブラウザからが返されます unable to connect または failure to establish a connection Web サービスにア クセスしようとするとエラーが発生 します。	LIF が正しく設定されていない可能 性があります。	Web サービスを配信する LIF に ping を送信できることを確認しま す。   を使用します network ping コ マンドを使用し てLIFにpingを送信 します。ネットワー ク設定の詳細につい ては、『ネットワー ク管理ガイド』を参 照してください。
ファイアウォールが正しく設定さ れていない可能性があります。	HTTP または HTTPS をサポートす るようファイアウォールポリシ ーが設定されていて、ポリシーが Web サービスを配信する LIF に割 り当てられていることを確認しま す。   を使用します system services firewall policy ファイアウォールポ リシーを管理するた めのコマンド。を使 用します network interface modify コマンドに を指定します -firewall -policy ポリシー をLIFに関連付ける ためのパラメータ。	Web プロトコルエンジンが無効に なっている可能性があります。

アクセスに関する問題	原因となる設定エラー	エラーに対処する方法
<p>Web プロトコルエンジンが有効になっていて、Web サービスがアクセス可能であることを確認します。</p> <div data-bbox="167 411 220 468">  </div> <div data-bbox="277 338 537 541"> <p>を使用します system services web クラスタのWeb プロトコルエンジン を管理するコマン ド。</p> </div>	<p>Webブラウザからが返されます not found Webサービスにアクセ スしようとするエラーが発生し ます。</p>	<p>Web サービスが無効になっている 可能性があります。</p>
<p>アクセスを許可する各 Web サービスが個別に有効になっていることを確認します。</p> <div data-bbox="167 831 220 888">  </div> <div data-bbox="277 753 537 957"> <p>を使用します vserver services web modify Webサービ スへのアクセスを有 効にするコマンド。</p> </div>	<p>Web ブラウザで、ユーザのアカウ ント名とパスワードを使用して Web サービスにログインできな い。</p>	<p>ユーザを認証できない、アクセス 方法が正しくない、またはユーザ に Web サービスへのアクセスが許 可されていない</p>

アクセスに関する問題	原因となる設定エラー	エラーに対処する方法
<p>ユーザアカウントが存在し、正しいアクセス方法と認証方法が設定されていることを確認します。また、ユーザのロールに Web サービスへのアクセスが許可されていることを確認します。</p> <div data-bbox="167 743 220 800">  </div> <p>を使用します  <code>security login</code>  ユーザアカウント、そのアクセス方法、および認証方法を管理するコマンド。ONTAP API Web サービスにアクセスするにはが必要です <code>ontapi</code> アクセス方法。他のすべての Web サービスにアクセスするにはが必要です <code>http</code> アクセス方法。を使用します <code>vserver services web access</code> ロールの Web サービスへのアクセスを管理するコマンド。</p>	<p>HTTPS を使用して Web サービスに接続すると、接続が中断されることが Web ブラウザに表示されません。</p>	<p>Web サービスを配信するクラスタまたは Storage Virtual Machine (SVM) で SSL が有効になっていない可能性がある</p>
<p>クラスタまたは SVM で SSL が有効になっていて、デジタル証明書が有効であることを確認します。</p> <div data-bbox="167 1493 220 1549">  </div> <p>を使用します  <code>security ssl</code>  HTTP サーバおよびの SSL 設定を管理するコマンド  <code>security certificate show</code> デジタル証明書情報を表示するコマンド。</p>	<p>HTTPS を使用して Web サービスに接続すると、信頼されていない接続であると Web ブラウザに表示されます。</p>	<p>自己署名デジタル証明書を使用している可能性があります。</p>

証明書を使用してリモートサーバの ID を確認します

証明書の概要を使用してリモートサーバの **ID** を確認します

ONTAP は、リモートサーバの ID を検証するセキュリティ証明書機能をサポートしています。

ONTAP ソフトウェアでは、次のデジタル証明書機能とプロトコルを使用して安全に接続できます。

- Online Certificate Status Protocol (OCSP) は、SSL 接続と Transport Layer Security (TLS) 接続を使用して、ONTAP サービスからのデジタル証明書要求のステータスを検証します。この機能はデフォルトでは無効になっています。
- ONTAP ソフトウェアには、信頼されたルート証明書のデフォルトセットが付属しています。
- Key Management Interoperability Protocol (KMIP) の証明書を使用して、クラスタと KMIP サーバの相互認証を有効にできます。

**OCSP** を使用してデジタル証明書が有効であることを確認します

ONTAP 9.2 以降では、Online Certificate Status Protocol (OCSP) を有効にすることで、Transport Layer Security (TLS) 通信を使用する ONTAP アプリケーションでデジタル証明書のステータスを受信できます。OCSP による証明書のステータスチェックは、特定のアプリケーションに対していつでも有効または無効にできます。デフォルトでは、OCSP による証明書のステータスチェックは無効になっています。

必要なもの

このタスクを実行するには、advanced権限レベルのアクセス権が必要です。

このタスクについて

OCSP は、次のアプリケーションをサポートしています。

- AutoSupport
- イベント管理システム (EMS)
- LDAP over TLS
- Key Management Interoperability Protocol (KMIP)
- 監査ログ
- FabricPool
- SSH (ONTAP 9.13.1以降)

手順

1. 権限レベルを advanced に設定します。 `set -privilege advanced`。
2. 特定の ONTAP アプリケーションで OCSP による証明書のステータスチェックを有効または無効にするには、次の該当するコマンドを使用します。



一部のアプリケーションで <b>OCSP</b> による証明書のステータスチェックを有効または無効にする場合	使用するコマンド
有効	<code>security config ocsp enable -app app name</code>
無効	<code>security config ocsp disable -app app name</code>

次のコマンドは、AutoSupport および EMS の OCSP サポートを有効にします。

```
cluster::*> security config ocsp enable -app asup,ems
```

OCSP を有効にすると、アプリケーションは次のいずれかの応答を受信します。

- Good - 証明書は有効で、通信可能な状態です。
- Revoked - 証明書は発行元の認証局によって永続的に信頼できないと判断されており、通信不可能な状態です。
- Unknown - サーバが証明書に関するステータス情報を持っていないため、通信不可能な状態です。
- OCSP server information is missing in the certificate - TLS 通信は続行していますが、サーバで OCSP が無効であると判断されているため、ステータスチェックは実行されません。
- No response from OCSP server - アプリケーションを実行できない状態です。

3. TLS を使用するすべてのアプリケーションで OCSP による証明書のステータスチェックを有効または無効にするには、次の該当するコマンドを使用します。

すべてのアプリケーションで <b>OCSP</b> による証明書のステータスチェックを有効または無効にする場合	使用するコマンド
有効	<code>security config ocsp enable</code>  <code>-app all</code>
無効	<code>security config ocsp disable</code>  <code>-app all</code>

有効にすると、指定した証明書が「有効」、「失効」、「不明」のいずれであるかを示す署名済みの応答が、すべてのアプリケーションに送信されます。証明書のステータスが `revoked` の場合は、アプリケーションは実行できません。アプリケーションが OCSP サーバから応答を受信できない場合、または OCSP サーバにアクセスできない場合、アプリケーションは続行できません。

4. を使用します `security config ocsp show` コマンドを使用して、OCSPをサポートするすべてのアプリケーションとそのサポートステータスを表示します。

```
cluster::*> security config ocsp show
Application                                OCSP Enabled?
-----
autosupport                               false
audit_log                                 false
fabricpool                                false
ems                                        false
kmip                                       false
ldap_ad                                   true
ldap_nis_namemap                          true
ssh                                        true

8 entries were displayed.
```

## TLS ベースのアプリケーションのデフォルト証明書を表示します

ONTAP 9.2 以降では、ONTAP に、Transport Layer Security（TLS）を使用する ONTAP アプリケーション用の信頼されたルート証明書のデフォルトセットが付属しています。

### 必要なもの

デフォルトの証明書は、管理 SVM の作成時、または ONTAP 9.2 へのアップグレード時に、管理 SVM にのみインストールされます。

### このタスクについて

現在クライアントとして機能し、証明書の検証が必要なアプリケーションは、AutoSupport、EMS、LDAP、監査ログ、FabricPool、および KMIP を使用できます。

証明書の有効期限が切れると、ユーザに証明書を削除するよう要求する EMS メッセージが起動します。デフォルトの証明書は、advanced 権限レベルでのみ削除できます。



デフォルトの証明書を削除すると、一部の ONTAP アプリケーションが正常に機能しなくなる場合があります（AutoSupport、監査ログなど）。

### ステップ

1. 管理 SVM にインストールされているデフォルトの証明書を表示するには、`security certificate show` コマンドを使用します。

```
security certificate show -vserver -type server-ca
```

```
fas2552-2n-abc-3::*> security certificate show -vserver fas2552-2n-abc-3
-type server-ca
Vserver      Serial Number  Common Name                                     Type
-----
fas2552-2n-abc-3
01           AACertificateServices
server-ca
Certificate Authority: AAA Certificate Services
Expiration Date: Sun Dec 31 18:59:59 2028
```

## クラスタとKMIPサーバの相互認証

### クラスタと KMIP サーバの相互認証の概要

Key Management Interoperability Protocol（KMIP）サーバなど、クラスタと外部キー管理ツールを相互認証することで、キー管理ツールが SSL を介した KMIP を使用してクラスタと通信できるようになります。この設定は、特定のアプリケーションや機能（ストレージ暗号化機能など）で、データアクセスの安全性を確保するためにセキュアなキーが必要とされる場合に使用します。

### クラスタの証明書署名要求を生成します

セキュリティ証明書を使用できます `generate-csr` 証明書署名要求（CSR）を生成するコマンド。要求が処理されると、署名済みのデジタル証明書が認証局（CA）から送信されます。

#### 必要なもの

このタスクを実行するには、クラスタ管理者または SVM 管理者である必要があります。

#### 手順

1. CSR を生成します

```
security certificate generate-csr -common-name FQDN_or_common_name -size
512|1024|1536|2048 -country country -state state -locality locality
-organization organization -unit unit -email-addr email_of_contact -hash
-function SHA1|SHA256|MD5
```

コマンド構文全体については、マニュアルページを参照してください。

次のコマンドは、SHA256 ハッシュ関数で生成される 2、048 ビット秘密鍵を使用して CSR を作成します。この CSR は、米国カリフォルニア州のサンニールにある `server1.companyname.com` というカスタム共通名の企業の IT 部門のソフトウェアグループが使用します。SVM 担当管理者の E メールアドレスは `web@example.com` です。CSR と秘密鍵が出力に表示されます。

```

cluster1::>security certificate generate-csr -common-name
server1.companyname.com -size 2048 -country US -state California -
locality Sunnyvale -organization IT -unit Software -email-addr
web@example.com -hash-function SHA256
Certificate Signing Request :
-----BEGIN CERTIFICATE REQUEST-----
MIIBGjCBxQIBADBqMRQwEgYDVQQDEwtleGFtcGx1LmNvbTELMakGA1UEBhMCVVMx
CTAHBgNVBAgtADEJMAcGA1UEBxMAMQkwBwYDVQQKEwAxCtAHBgNVBAStADEPMA0G
CSqGSIB3DQEJARYAMFwwDQYJKoZIhvcNAQEBBQADSwAwSAJBAPXFanNoJApTlnzS
xOcxixqImRRGZCR7tVmTYyqPSuTvfhVtwDJbmXuj6U3alwoUsb13wfEvQnHVFNCi
2ninsJ8CAwEAAaAAMA0GCSqGSIB3DQEBCwUAA0EA6EagLfso5+4g+ejiRKKTUPQO
UqOUEoKuvxhOvPC2w7b//fNSFsFHvXloqEOhYECn/NX9h8mbphCoM5YZ4OfnKw==
-----END CERTIFICATE REQUEST-----
Private Key :
24 | Administrator Authentication and RBAC
-----BEGIN RSA PRIVATE KEY-----
MIIBOwIBAAJBAPXFanNoJApTlnzSxOcxixqImRRGZCR7tVmTYyqPSuTvfhVtwDJb
mXuj6U3alwoUsb13wfEvQnHVFNCi2ninsJ8CAwEAAQJAWt2AO+bW3FKezEuIrQlu
KoMyRYK455wtMk8BrOyJfhYsB20B28eifjJvRWdTOBEav99M7cEzgpV+p5kaZTTM
gQIhAPsp+j1hrUXSRj979LIJJY0sNez397i7ViFXWQScx/ehAiEA+oDbOooWlVvu
xj4aitxVBu6ByVckYU8LbsfeRNsZwD8CIQCbZ1/ENvmlJ/P7N9Exj2NCtEYxd0Q5
cwBZ5NfZeMBpwQIhAPk0KWQSLadGfsKO077itF+h9FGFNHbtuNTrVq4vPW3nAiAA
peMBQgEv28y2r8D4dkYzxcXmjzJluUSZSZ9c/wS6fA==
-----END RSA PRIVATE KEY-----
Note: Please keep a copy of your certificate request and private key
for future reference.

```

2. CSR 出力の証明書要求をデジタル形式（E メールなど）で信頼できるサードパーティの CA に送信し、署名を求めます。

要求が処理されると、署名済みのデジタル証明書が CA から送信されます。秘密鍵と CA 署名デジタル証明書のコピーは保管する必要があります。

## クラスタの **CA** 署名済みサーバ証明書をインストールします

SSL サーバでクラスタまたは Storage Virtual Machine（SVM）を SSL クライアントとして認証するためには、client タイプのデジタル証明書をクラスタまたは SVM にインストールします。次に、client-ca 証明書をその SSL サーバの管理者に渡してインストールしてもらいます。

### 必要なもの

を使用してクラスタまたは SVM に SSL サーバのルート証明書をインストールしておく必要があります  
server-ca 証明書のタイプ。

### 手順

1. クライアント認証に自己署名デジタル証明書を使用するには、を使用します `security certificate create` コマンドにを指定します `type client` パラメータ
2. クライアント認証に CA 署名デジタル証明書を使用するには、次の手順を実行します。

- a. セキュリティ証明書を使用して、証明書署名要求（CSR）を生成します `generate-csr` コマンドを実行します

証明書要求と秘密鍵を含む CSR 出力が表示され、今後の参照用にファイルにコピーするよう求められます。ONTAP

- b. CSR 出力の証明書要求をデジタル形式（E メールなど）で信頼できる CA に送信し、署名を求めます。

秘密鍵と CA 署名証明書のコピーは今後の参照用として保管しておいてください。

要求が処理されると、署名済みのデジタル証明書が CA から送信されます。

- a. を使用してCA署名証明書をインストールします `security certificate install` コマンドにを指定します `-type client` パラメータ
- b. プロンプトが表示されたら証明書と秘密鍵を入力し、\* Enter \* キーを押します。
- c. プロンプトが表示されたら追加のルート証明書または中間証明書を入力し、\* Enter \* キーを押します。

信頼できるルート CA から発行された SSL 証明書に至る証明書チェーンに中間証明書がない場合は、クラスタまたは SVM に中間証明書をインストールします。中間証明書は、問題のエンドエンティティのサーバ証明書専用に信頼できるルートから発行される、副次的な証明書です。この結果、信頼できるルート CA から始まり、中間証明書を経て、発行された SSL 証明書で終わる証明書チェーンが形成されます。

3. を指定します `client-ca` クラスタまたはSVMの証明書。サーバにインストールするためのSSLサーバの管理者への証明書。

`security certificate show`コマンドとを使用します `-instance` および `-type client-ca` が表示されます `client-ca` 証明書情報。

## KMIP サーバの CA 署名済みクライアント証明書をインストールします

Key Management Interoperability Protocol（KMIP）の証明書サブタイプ（`-subtype kmip-cert` パラメータ）は、`client` および `server-ca` のタイプと組み合わせて適用され、クラスタと外部キー管理ツール（KMIP サーバなど）の相互認証に使用される証明書であることを示します。

このタスクについて

KMIP サーバをクラスタに対して SSL サーバとして認証する KMIP 証明書をインストールします。

手順

1. を使用します `security certificate install` コマンドにを指定します `-type server-ca` および `-subtype kmip-cert` KMIPサーバ用のKMIP証明書をインストールするためのパラメータ。

2. プロンプトが表示されたら、証明書を入力して Enter キーを押します。

今後の参照用として証明書のコピーを保管するように ONTAP から求められます。

```
cluster1::> security certificate install -type server-ca -subtype kmip-  
cert  
-vserver cluster1
```

```
Please enter Certificate: Press <Enter> when done
```

```
-----BEGIN CERTIFICATE-----
```

```
MIICPDCCAaUCEDyRMcsf9tAbDpq40ES/Er4wDQYJKoZIhvcNAQEFBQAwxELMAkG  
2JhucwNhkcV8sEVAbkSdjbCxlRhLQ2pRdKkkirWmnWXbj9T/UWZYB2oK0z5XqcJ  
2HUw19JlYDln1khVdWk/kfVIC0dpImmClr7JyDiGSnoscxlIaU5rfGW/D/xwzoiQ
```

```
...
```

```
-----END CERTIFICATE-----
```

You should keep a copy of the CA-signed digital certificate for future reference.

```
cluster1::>
```

# セキュリティとデータ暗号化

## System Manager によるセキュリティ管理の概要

ONTAP 9.7 以降では、System Manager を使用してクラスタセキュリティを管理できます。

System Manager では、ONTAP 標準の方法を使用して、クライアントや管理者によるストレージへのアクセスを保護し、ウィルスから保護します。保存データの暗号化や WORM ストレージでは、高度なテクノロジーも使用できます。

従来の System Manager （ONTAP 9.7 以前でのみ使用可能）を使用している場合は、[を参照してください](#) "[System Manager Classic （ONTAP 9.0 から 9.7）](#)"

### ウィルススキャン

ストレージシステムに統合されたウィルス対策機能を使用して、ウィルスやその他の悪意のあるプログラムからデータを保護することができます。ONTAP ウィルススキャン（\_vscan）は、クラス最高のサードパーティ製ウィルス対策ソフトウェアと ONTAP 機能を組み合わせたもので、どのファイルをスキャンするか、いつスキャンするかを柔軟に制御できます。

### 暗号化

ONTAP は、ストレージメディアの転用、返却、置き忘れ、盗難に際して保存データが読み取られることがないようにソフトウェアベースとハードウェアベースの暗号化テクノロジーを提供します。

### WORM ストレージ

\_ 解決策 \_ は、規制やガバナンスに準拠するために変更不可能な状態で重要なファイルを保管するために *write once, read many* （WORM）\_storage を使用する組織向けの、ハイパフォーマンスなコンプライアンス SnapLock です。

## ランサムウェアからデータを保護

### Autonomous Ransomware Protection Overview

ONTAP 9.10.1以降のAutonomous RansProtection（ARP）機能では、NAS（NFSおよびSMB）環境のワークロード分析を使用して、ランサムウェア攻撃を示す可能性のある異常なアクティビティをプロアクティブに検出して警告します。

攻撃の疑いがある場合、ARPは、スケジュールされたSnapshotコピーからの既存の保護に加えて、新しいSnapshotコピーも作成します。

### ライセンスとイネーブルメント

ARPにはライセンスが必要です。ARPは、["ONTAP 1ライセンス"](#)。ONTAP Oneライセンスがない場合は、使用しているONTAPのバージョンによって異なる他のライセンスを使用してARPを使用できます。

ONTAP リリース	使用許諾
ONTAP 9.11.1以降	anti_Ransomware
ONTAP 9.10.1	MT_EK_MGMT（マルチテナントキー管理）

- ONTAP 9.11.1以降にアップグレードしていて、ARPがすでにシステムに設定されている場合は、新しいアンチランサムウェアライセンスを購入する必要はありません。新しいARP設定の場合、新しいライセンスが必要です。
- ONTAP 9.11.1以降からONTAP 9.10.1にリバートする際に、ランサムウェア対策ライセンスでARPを有効にしていると、警告メッセージが表示され、ARPの再設定が必要になる場合があります。"[ARPのリバートについて説明します](#)"。

System ManagerまたはONTAP CLIを使用して、ボリューム単位でARPを設定できます。

## ONTAP ランサムウェア攻撃からの保護戦略

ランサムウェアの効果的な検出戦略には、複数の保護レイヤを含める必要があります。

例えば、車両の安全機能です。シートベルトなどの単一の機能に頼らず、事故時に完全に身を守ることができます。エアバッグ、アンチロックブレーキ、および前方衝突警告はすべて、より良い結果をもたらす追加の安全機能です。ランサムウェア攻撃からの保護は、同様の方法で確認する必要があります。

ONTAP には、ランサムウェアからの保護に役立つFPolicy、Snapshotコピー、SnapLock、Active IQ デジタルアドバイザーなどの機能が含まれていますが、以下では機械学習機能を備えたARP搭載機能に焦点を当てて説明します。

ONTAPのその他のランサムウェア対策機能の詳細については、を参照してください "[TR-4572](#) : 『[NetApp Solution for Ransomware](#)』 "

## ARPが検出するもの

ARPは、身代金が支払われるまで攻撃者がデータを保留するサービス拒否攻撃から保護するように設計されています。ARPは、以下に基づくランサムウェア対策検出を提供します。

- 受信データを暗号化データまたはプレーンテキストとして識別する。
- 検出する分析
  - **Entropy** : ファイル内のデータのランダム性の評価
  - ファイル拡張子タイプ: 通常の拡張子タイプと一致しない拡張子
  - ファイルIOPS : データ暗号化による異常なボリュームアクティビティの急増 (ONTAP 9.11.1以降)

ARPは、少数のファイルのみが暗号化された後、ほとんどのランサムウェア攻撃の拡散を検出し、データを保護するためのアクションを自動的に実行し、攻撃の疑いがあることを警告します。



ランサムウェア攻撃の安全性を完全に保証できるランサムウェア検出や防御システムはありません。攻撃が検出されない可能性はありますが、アンチウイルスソフトウェアが侵入を検出できなかった場合、ARPは重要な追加防御層として機能します。



## 学習モードとアクティブモード

ARPには2つのモードがあります。

- 学習（または「ドライラン」モード）
- アクティブ（または「有効」モード）

ARPをイネーブルにすると、`_learning mode_`で実行されます。学習モードでは、ONTAPシステムは、エンタロピー、ファイル拡張子タイプ、ファイルIOPSなどの分析領域に基づいてアラートプロファイルを作成します。ARPをラーニングモードで実行して、ワークロード特性を評価するのに十分な時間が経過したら、アクティブモードに切り替えてデータの保護を開始できます。ARPがアクティブモードに切り替わると、ONTAPはARP Snapshotコピーを作成して、脅威が検出された場合にデータを保護します。

ARPを学習モードのまま30日間放置することをお勧めします。ONTAP 9.13.1以降では、ARPによって最適な学習期間間隔が自動的に決定され、30日前にスイッチが自動化されます。

アクティブモードで、ファイル拡張子が異常としてフラグされている場合は、アラートを評価する必要があります。アラートに対処してデータを保護したり、アラートを誤検出としてマークしたりできます。アラートをfalse positiveとしてマークすると、アラートプロファイルが更新されます。たとえば、新しいファイル拡張子によってアラートがトリガーされ、アラートをfalse positiveとしてマークした場合、次回そのファイル拡張子が監視されたときにアラートは受信されません。コマンド `security anti-ransomware volume workload-behavior show` ボリュームで検出されたファイル拡張子が表示されます。（このコマンドをラーニングモードの早い段階で実行し、ファイルタイプが正確に表現されている場合は、ONTAPが他のメトリックを収集しているため、そのデータをアクティブモードに移行するためのベースとして使用しないでください）。

ONTAP 9.11.1以降では、ARPの検出パラメータをカスタマイズできます。詳細については、を参照してください [ARP攻撃検出パラメータを管理します。](#)。

## 脅威の評価とARP Snapshotコピー

アクティブモードでは、ARPは学習した分析に対して測定された受信データに基づいて脅威の確率を評価します。ARPが脅威を検出すると、測定値が割り当てられます。

- 低：ボリュームの異常をいち早く検出したもの（たとえば、新しいファイル拡張子がボリュームに観察された場合）。
- 中程度:同じファイル拡張子を持つ複数のファイルが観察されます。
  - ONTAP 9.10.1では、中程度へのエスカレーションのしきい値は100個以上です。ONTAP 9.11.1以降では、ファイル数を変更できます。デフォルト値は20です。

脅威が低い状況では、ONTAPが異常を検出し、ボリュームのSnapshotコピーを作成して最適なりカバリポイントを作成します。ONTAPでは、ARP Snapshotコピーの名前の先頭に次の文字が付加されます。 `Anti-ransomware-backup` 簡単に識別できるようにするために `Anti_ransomware_backup.2022-12-20_1248`。

ONTAPがランサムウェアのプロファイルに異常が一致しているかどうかを判断する分析レポートを実行すると、脅威は「中程度」にエスカレーションされます。下位レベルの脅威はログに記録され、System Managerの[\*イベント]セクションに表示されます。攻撃の可能性が中程度の場合、ONTAPによってEMS通知が生成され、脅威を評価するように求められます。ONTAPは低脅威に関するアラートを送信しませんが、ONTAP 9.14.1以降では、次のことが可能です。 [アラート設定の変更](#)。詳細については、を参照してください [異常な活動に対応する。](#)。

脅威に関する情報は、レベルに関係なく、System Managerの[\*イベント]セクションまたはを使用して表示できます `security anti-ransomware volume show` コマンドを実行します

ARP Snapshotコピーは最低2日間保持されます。ONTAP 9.11.1以降では、保持設定を変更できます。詳細については、[を参照してください Snapshotコピーのオプションを変更します](#)。

ランサムウェア攻撃のあとに **ONTAP** でデータをリカバリする方法

攻撃の疑いがある場合、システムはその時点でボリュームの Snapshot コピーを作成し、そのコピーをロックします。あとで攻撃が確認された場合は、ARP Snapshotコピーを使用してボリュームをリストアできます。

ロックされた Snapshot コピーは、通常の方法で削除できません。ただし、後で攻撃をフォールスポジティブとしてマークする場合、ロックされたコピーは削除されます。

影響を受けるファイルと攻撃時刻を把握していれば、ボリューム全体をSnapshotコピーの1つにリバートするだけでなく、さまざまなSnapshotコピーから影響を受けるファイルを選択してリカバリできます。

ARPは、実績のあるONTAP データ保護とディザスタリカバリテクノロジーを基盤として、ランサムウェア攻撃に対応しています。データのリカバリの詳細については、次のトピックを参照してください。

- ["Snapshot コピーからのリカバリ（System Manager）"](#)
- ["Snapshot コピーからのファイルのリストア（CLI）"](#)
- ["スマートなランサムウェアリカバリ"](#)

## 自動ランサムウェア対策による保護のユースケースと考慮事項

ONTAP 9.10.1以降では、自律型ランサムウェア対策（ARP）をNASワークロードで使用できます。ARPを導入する前に、推奨される使用方法とサポートされる設定、およびパフォーマンスへの影響について理解しておく必要があります。

サポートされる構成とサポートされない構成

ARPの使用を決定する際には、ボリュームのワークロードがARPに適していること、および必要なシステム構成を満たしていることを確認することが重要です。

最適なワークロード

ARPは次の用途に適しています。

- NFS ストレージ上のデータベース
- Windows または Linux のホームディレクトリ

学習期間中に検出されなかった拡張子のファイルが作成される可能性があるため、このワークロードでは誤検出の可能性が高くなります。

- 画像とビデオ

たとえば、医療記録やElectronic Design Automation（EDA）データなどです。

不適切なワークロード

ARPは次の用途には適していません。

- ファイルの作成や削除が頻繁に発生するワークロード（テスト/開発ワークロードなど、数秒で数十万個のファイル进行处理）
- ARPの脅威検出機能は、ファイルの作成、名前変更、または削除アクティビティの異常な急増を認識できるかどうか依存します。アプリケーション自体がファイルアクティビティのソースである場合、ランサムウェアのアクティビティと効果的に区別することはできません。
- アプリケーションまたはホストがデータを暗号化するワークロード。  
ARPは、着信データを暗号化されたものと暗号化されていないものと区別します。アプリケーション自体がデータを暗号化している場合は、機能の有効性が低下します。ただし、この機能は、ファイルアクティビティ（削除、上書き、作成、または新しいファイル拡張子を使用した作成または名前変更）およびファイルタイプに基づいて動作します。

サポートされている構成

ONTAP 9.10.1以降では、オンプレミスのONTAPシステムのNFSボリュームとSMBボリュームにARPを使用できます。

次のONTAPバージョンでは、その他の構成とボリュームタイプがサポートされます。

	ONTAP 9.14.1	ONTAP 9.13.1	ONTAP 9.12.1	ONTAP 9.11.1	ONTAP 9.10.1
非同期SnapMirrorで保護されているボリューム	✓	✓	✓		
非同期SnapMirror（SVMディザスタリカバリ）で保護されるSVM	✓	✓	✓		
SVM のデータ移動 (vserver migrate)	✓	✓	✓		
FlexGroup ボリューム	✓	✓			
管理者による検証が複数必要です	✓	✓			

## SnapMirrorとARPの相互運用性

ONTAP 9.12.1以降では、非同期SnapMirrorデスティネーションボリュームでARPがサポートされます。ARPはSnapMirror Synchronousでサポートされていません\*\*。

SnapMirrorソースボリュームがARP対応の場合、SnapMirrorデスティネーションボリュームには、ARP設定状態（ラーニング、有効化など）、ARPトレーニングデータ、およびARPで作成されたソースボリュームのSnapshotが自動的に取得されます。明示的な有効化は必要ありません。

デスティネーションボリュームは読み取り専用（RO）Snapshotコピーで構成されていますが、データに対してARP処理は実行されません。ただし、SnapMirrorデスティネーションボリュームが読み書き可能（rw）に変換されると、ARPはRW変換されたデスティネーションボリュームで自動的に有効になります。デスティネーションボリュームでは、ソースボリュームにすでに記録されている情報に加えて、ラーニング手順を追加する必要はありません。

ONTAP 9.10.1および9.11.1では、ARP設定の状態、トレーニングデータ、およびSnapshotコピーがソースボリュームからデスティネーションボリュームに転送されません。したがって、SnapMirrorデスティネーションボリュームがRWに変換されると、変換後にデスティネーションボリュームのARPがラーニングモードで明示的に有効になる必要があります。

## ARPと仮想マシン

ARPは仮想マシン（VM）でサポートされます。ARP検出の動作は、VMの内部と外部の変更で異なります。ARPは、エントロピーの高いファイルがVM内にあるワークロードには推奨されません。

### VM以外での変更

ARPは、新しい拡張子が暗号化されたボリュームに入った場合やファイル拡張子に変更された場合に、VMの外部にあるNFSボリュームでのファイル拡張子の変更を検出できます。検出可能なファイル拡張子の変更は次のとおりです。

- .vmx
- .vmxf
- .vmdk
- -flat.vmdk
- .nvram
- .vMem
- .vmsd
- .vmsn
- .vswp
- .vmss
- .log
- -\#.log

### VM内での変更

ランサムウェア攻撃がVMをターゲットにし、VMの外部で変更を行わずにVM内のファイルが変更された場合、ARPはVMのデフォルトエントロピーが低い場合（.txt、.docx、.mp4ファイルなど）に脅威を検出します。このシナリオではARPは保護スナップショットを作成しますが、VMの外部にあるファイル拡張子が改ざんされていないため、脅威アラートは生成されません。

デフォルトでは、ファイルが高エントロピー（.gzipやパスワードで保護されたファイルなど）の場合、ARPの検出機能は制限されます。ARPはこの場合でもプロアクティブなSnapshotを取得できますが、ファイル拡張子が外部から改ざんされていない場合、アラートはトリガーされません。

サポートされない構成です

ARPは、次のシステム設定ではサポートされていません。

- ONTAP S3 環境
- SAN 環境

ARPでは、次のボリューム構成はサポートされません。

- FlexGroupボリューム（ONTAP 9.10.1~9.12.1の場合）ONTAP 9.13.1以降では、FlexGroupボリュームがサポートされます）。
- FlexCacheボリューム（ARPは元のFlexVolボリュームではサポートされますが、キャッシュボリュームではサポートされません）
- ボリュームをオフラインにします
- SAN-only ボリューム
- SnapLock ボリューム
- SnapMirror Synchronous
- 非同期SnapMirror（ONTAP 9.10.1および9.11.1でのみサポートされません。非同期SnapMirrorは、ONTAP 9.12.1以降でサポートされます。詳細については、[\[snapmirror\]](#)を参照してください。）
- 制限されたボリューム
- Storage VMのルートボリューム
- 停止しているStorage VMのボリューム

#### ARPのパフォーマンスと周波数に関する考慮事項

ARPは、スループットとピークIOPSで測定した場合、システムパフォーマンスへの影響を最小限に抑えることができます。ARP機能の影響は、ボリュームのワークロードによって異なります。一般的なワークロードに推奨される構成の制限は次のとおりです。

ワークロードの特性	ノードあたりの推奨されるボリューム数の上限	ノード単位のボリューム制限を超えたときのパフォーマンスの低下：[*]
大量の読み取り処理や、データの圧縮が可能です。	一五〇	最大IOPSの4%
大量の書き込みが発生し、データを圧縮することはできません。	60ドルだ	最大IOPSの10%

合格：[\*]推奨制限を超過したボリュームの数に関係なく、システムパフォーマンスはこれらの割合を超えて低下することはありません。

ARP分析は優先順位付けされた順序で実行されるため、保護されたボリュームの数が増えるにつれて、各ボリュームでの分析の実行頻度は低下します。

#### ARPで保護されたボリュームを使用したマルチ管理者検証

ONTAP 9.13.1以降では、マルチ管理者検証（MAV）をイネーブルにしてARPによるセキュリティを強化できます。MAVを使用すると、少なくとも2人以上の認証された管理者が、保護されたボリュームでARPをオフにしたり、ARPを一時停止したり、疑わしい攻撃をfalse positiveとしてマークしたりする必要があります。方法をご確認ください ["ARPで保護されたボリュームのMAVを有効にします"](#)。

MAVグループの管理者を定義し、のMAVルールを作成する必要があります security anti-ransomware

volume disable、security anti-ransomware volume pause`および `security anti-ransomware volume attack clear-suspect 保護するARPコマンド。MAVグループの各管理者は、新しいルール要求とを承認する必要があります ["MAVルールを再度追加します"](#) MAV設定内。

ONTAP 9.14.1以降では、ARPスナップショットの作成および新しいファイル拡張子の監視に関するアラートが提供されます。これらのイベントのアラートは、デフォルトでは無効になっています。アラートはボリュームレベルまたはSVMレベルで設定できます。MAVルールは、次のコマンドを使用してSVMレベルで作成できます。security anti-ransomware vserver event-log modify またはボリュームレベルで、security anti-ransomware volume event-log modify。

次のステップ

- ["自動ランサムウェア対策を有効化"](#)
- ["ARPで保護されたボリュームのMAVを有効にする"](#)

## 自動ランサムウェア対策を有効化

ONTAP 9.10.1以降のAutonomous Ransomware Protection (ARP) は、新規または既存のボリュームで有効にできます。最初にARPをラーニングモードでイネーブルにします。このモードでは、システムがワークロードを分析して、通常の動作の特性を特定します。既存のボリュームでARPを有効にしたり、新しいボリュームを作成してARPを有効にしたりすることができます。

このタスクについて

ARPは、必ず最初にラーニング（またはドライラン）モードでイネーブルにする必要があります。アクティブモードで開始すると、過剰なfalse positiveレポートが発生する可能性があります。

ARPを学習モードで最低30日間実行することをお勧めします。ONTAP 9.13.1以降では、ARPによって最適な学習期間間隔が自動的に決定され、30日前にスイッチが自動化されます。詳細については、[を参照してください](#) ["学習モードとアクティブモード"](#)。



既存のボリュームでは、ラーニングモードとアクティブモードは新しく書き込まれたデータにのみ適用され、ボリューム内の既存のデータには適用されません。既存のデータはスキャンおよび分析されません。これは、以前の通常のデータトラフィックの特性が、ARPでボリュームを有効にした後の新しいデータに基づいていると見なされるためです。

作業を開始する前に

- NFSまたはSMB（またはその両方）に対してStorage VM (SVM) が有効になっている必要があります。
- [正しいライセンス](#) ONTAP のバージョンに対応するがインストールされている必要があります。
- クライアントでNASワークロードを設定しておく必要があります。
- ARPを設定するボリュームは保護されており、アクティブなボリュームである必要があります ["ジャンクションパス"](#)。
- ボリュームの使用率が100%未満である必要があります。
- ARPアクティビティの通知を含む電子メール通知を送信するようにEMSシステムを設定することをお勧めします。詳細については、[を参照してください](#) ["E メール通知を送信するように EMS イベントを設定します"](#)。
- ONTAP 9.13.1以降では、Autonomous Ransomware Protection (ARP；自律ランサムウェア対策) 設定に

複数の認証済みユーザ管理者が必要になるように、Multi-admin Verification（MAV；マルチ管理者検証）を有効にすることを推奨します。詳細については、を参照してください ["マルチ管理者検証を有効にします"](#)。

### **ARP**を有効にする

ARPは、System ManagerまたはONTAP CLIを使用して有効にできます。



## System Manager の略

### 手順

1. [ストレージ]>[ボリューム]\*を選択し、保護するボリュームを選択します。
2. [Volumes]の概要の\*タブで、[Status]を選択し、[Anti-ransomware]\*ボックスで[Disabled]から[Enabled in learning-mode]に切り替えます。
3. 学習期間が終了したら、ARPをアクティブモードに切り替えます。



ONTAP 9.13.1以降では、ARPによって最適な学習期間間隔が自動的に決定され、スイッチが自動化されます。可能です ["関連付けられているStorage VMでこの設定を無効にしてください"](#) ラーニングモードをアクティブモードに切り替える場合は、手動で切り替えます。

- a. [ストレージ]>[ボリューム]\*を選択し、アクティブモードにする準備ができたボリュームを選択します。
  - b. [Volumes]概要の\*タブで、**[Anti-ransomware]**ボックスで[Switch \* to active mode]を選択します。
4. ボリュームのARP状態は、\* Anti-ransomware \*ボックスで確認できます。

すべてのボリュームのARPステータスを表示するには、\* Volumes ペインで Show/Hide を選択し、Anti-ransomware \*ステータスがチェックされていることを確認します。

### CLI の使用

CLIを使用してARPを有効にするプロセスは、既存のボリュームで有効にする場合と新しいボリュームで有効にする場合で異なります。

既存のボリュームで**ARP**を有効にします

1. 既存のボリュームを変更して、学習モードでランサムウェアからの保護を有効にします。

```
security anti-ransomware volume dry-run -volume vol_name -vserver svm_name
```

ONTAP 9.13.1以降を実行している場合は、アクティブ状態への変更が自動的に行われるように、アダプティブラーニングがイネーブルになります。この動作を自動的に有効にしない場合は、関連付けられているすべてのボリュームでSVMレベルの設定を変更します。

```
vserver modify svm_name -anti-ransomware-auto-switch-from-learning-to-enabled false
```

2. 学習期間が終了したら、保護ボリュームを変更してアクティブモードに切り替えます（まだ自動的に行われていない場合）。

```
security anti-ransomware volume enable -volume vol_name -vserver svm_name
```

volume modify コマンドを使用して、アクティブモードに切り替えることもできます。

```
volume modify -volume vol_name -vserver svm_name -anti-ransomware-state active
```



3. ボリュームのARP状態を確認します。

```
security anti-ransomware volume show
```

新しいボリュームでARPを有効にします

1. データをプロビジョニングする前に、ランサムウェア対策を有効にした新しいボリュームを作成する。

```
volume create -volume vol_name -vserver svm_name -aggregate aggr_name -size nn -anti-ransomware-state dry-run -junction-path /path_name
```

ONTAP 9.13.1以降を実行している場合は、アクティブ状態への変更が自動的に行われるように、アダプティブラーニングがイネーブルになります。この動作を自動的に有効にしない場合は、関連付けられているすべてのボリュームでSVMレベルの設定を変更します。

```
vserver modify svm_name -anti-ransomware-auto-switch-from-learning-to-enabled false
```

2. 学習期間が終了したら、保護ボリュームを変更してアクティブモードに切り替えます（まだ自動的に行われていない場合）。

```
security anti-ransomware volume enable -volume vol_name -vserver svm_name
```

volume modify コマンドを使用して、アクティブモードに切り替えることもできます。

```
volume modify -volume vol_name -vserver svm_name -anti-ransomware-state active
```

3. ボリュームのARP状態を確認します。

```
security anti-ransomware volume show
```

## 新規ボリュームでの**Autonomous Ransomware Protection**のデフォルト設定の有効化

ONTAP 9.10.1以降のStorage VM (SVM) を設定して、学習モードのAutonomous Ransomware Protection (ARP) に対して新しいボリュームがデフォルトで有効になるようにすることができます。

### このタスクについて

デフォルトでは、新しいボリュームは無効モードでARPを使用して作成されます。この設定は、System ManagerおよびCLIを使用して変更できます。デフォルトで有効になっているボリュームは、ラーニング（またはドライラン）モードでARPに設定されます。

ARPは、設定の変更後にSVMで作成されたボリュームでのみ有効になります。既存のボリュームではARPは有効になりません。方法をご確認ください ["既存のボリュームでARPを有効にします"](#)。

ONTAP 9.13.1以降、アダプティブラーニングがARP分析に追加され、ラーニングモードからアクティブモードへの切り替えが自動的行われます。詳細については、[を参照してください "学習モードとアクティブモード"](#)。

作業を開始する前に

- [正しいライセンス](#) ONTAP のバージョンに対応するがインストールされている必要があります。
- ボリュームの使用率が100%未満である必要があります。
- ジャンクシヨンパスがアクティブである必要があります。
- ONTAP 9.13.1以降では、マルチ管理者認証（MAV）を有効にして、ランサムウェア対策に2人以上の認証済みユーザ管理者が必要になるようにすることをお勧めします。 ["詳細はこちら。"](#)

ARPをラーニングモードからアクティブモードに切り替えます。

ONTAP 9.13.1以降、アダプティブラーニングがARP分析に追加されました。学習モードからアクティブモードへの切り替えは自動的に行われます。ARPによるラーニングモードからアクティブモードへの自動切り替えは、次のオプションの設定に基づいて決定されます。

```
-anti-ransomware-auto-switch-minimum-incoming-data-percent  
-anti-ransomware-auto-switch-duration-without-new-file-extension  
-anti-ransomware-auto-switch-minimum-learning-period  
-anti-ransomware-auto-switch-minimum-file-count  
-anti-ransomware-auto-switch-minimum-file-extension
```


30日間の学習後、これらの条件の1つまたは複数が満たされていない場合でも、ボリュームは自動的にアクティブモードに切り替わります。つまり、自動切り替えが有効な場合、ボリュームは最大30日後にアクティブモードに切り替わります。最大値の30日は固定であり、変更できません。

デフォルト値を含むARP設定オプションの詳細については、[を参照してください。](#) ["ONTAP コマンドリファレンス"](#)。

手順

デフォルトでは、System ManagerまたはONTAP CLIを使用してARPを有効にできます。

## System Manager の略

1. [ストレージ]>[Storage VM]\*を選択し、ARPで保護するボリュームを含むStorage VMを選択します。
2. \*[設定]\*タブに移動します。[Security（セキュリティ）]\*で、[Anti-ransomware（ランサムウェア対策）]\*\*タイルを探し、
3. NASボリュームのARPを有効にするには、このボックスをオンにします。Storage VM内の対応するすべてのNASボリュームでARPを有効にするには、追加のボックスをオンにします。



ONTAP 9.13.1にアップグレードした場合は、\*十分な学習後に自動的に学習モードからアクティブモードに切り替える\*設定が自動的に有効になります。これにより、ARPは最適な学習期間間隔を決定し、アクティブモードへの切り替えを自動化できます。手動でアクティブモードに移行する場合は、この設定をオフにします。

## CLI の使用

1. 既存のSVMを変更して、新しいボリュームでデフォルトでARPを有効にします。

```
vserver modify -vserver svm_name -anti-ransomware-default-volume-state dry-run
```

CLIでは、新しいボリュームに対してARPがデフォルトで有効になっている新しいSVMを作成することもできます。

```
vserver create -vserver svm_name -anti-ransomware-default-volume-state dry-run [other parameters as needed]
```

ONTAP 9.13.1以降にアップグレードした場合は、アクティブ状態への変更が自動的に行われるように、アダプティブラーニングがイネーブルになります。この動作を自動的に有効にしない場合は、次のコマンドを使用します。

```
vserver modify svm_name -anti-ransomware-auto-switch-from-learning-to-enabled false
```

## Autonomous Ransomware Protectionを一時停止して、ワークロードイベントを分析対象から除外します

通常とは異なるワークロードイベントが発生すると予想される場合は、一時的にRansomware Protection（ARP）分析を一時的に一時停止して再開できます。

ONTAP 9.13.1以降では、マルチ管理者検証（MAV）をイネーブルにして、複数の認証済みユーザ管理者がARPを一時停止する必要があります。["詳細はこちら。"](#)。

### このタスクについて

ARPの一時停止中は、イベントはログに記録されず、新しい書き込みに対するアクションも記録されません。ただし、分析処理はバックグラウンドで以前のログに対して続行されます。



ARP無効機能を使用して分析を一時停止しないでください。これにより、ボリュームのARPが無効になり、学習されたワークロードの動作に関する既存の情報はすべて失われます。これには学習期間の再開が必要です。

ARPは、System ManagerまたはONTAP CLIを使用して一時停止できます。

### System Manager の略

1. [ストレージ]>[ボリューム]\*を選択し、ARPを一時停止するボリュームを選択します。
2. [Volumes]の概要の[\* **Security**]タブで、[Anti-ransomware]ボックスの\*[Pause anti-ransomware]\*を選択します。



ONTAP 9.13.1以降では、MAVを使用してARP設定を保護している場合、一時停止操作によって、1人以上の追加管理者の承認を得るように求められます。"すべての管理者から承認を受ける必要があります" MAV承認グループに関連付けられているか、操作が失敗します。

### CLI の使用

1. ボリュームのARPを一時停止します。

```
security anti-ransomware volume pause -vserver svm_name -volume vol_name
```

2. 処理を再開するには、を使用します resume パラメータ

```
security anti-ransomware volume resume -vserver svm_name -volume vol_name
```

3. \*ARP設定を保護するためにMAV（ONTAP 9.13.1以降で使用可能）を使用している場合は、一時停止操作によって、1人以上の追加管理者の承認を得るように求められます。MAV承認グループに関連付けられているすべての管理者から承認を受ける必要があります。そうしないと、操作は失敗します。

MAVを使用していて、予定されている一時停止操作で追加の承認が必要な場合は、各MAVグループ承認者が次の処理を行います。

- a. 要求を表示します。

```
security multi-admin-verify request show
```

- b. リクエストを承認します。

```
security multi-admin-verify request approve -index[number returned from show request]
```

最後のグループ承認者に対する応答は、ボリュームが変更され、ARPの状態が一時停止されたことを示します。

MAVを使用していて、MAVグループ承認者である場合は、一時停止操作要求を拒否できます。

```
security multi-admin-verify request veto -index[number returned from show request]
```

## 自律型ランサムウェア対策攻撃検出パラメータの管理

ONTAP 9.11.1以降では、特定の自律型ランサムウェア対策が有効なボリュームでランサムウェア検出のパラメータを変更し、通常のファイルアクティビティとして既知の急増を報告できます。検出パラメータを調整すると、特定のボリュームワークロードに基づいてレポートの精度が向上します。

### 攻撃検出の仕組み

Autonomous Ransomware Protection (ARP; 自律型ランサムウェア対策) がラーニングモードの場合、ボリューム動作のベースライン値が設定されます。これらはエントロピー、ファイル拡張子、およびONTAP 9.11.1以降のIOPSです。これらのベースラインは、ランサムウェアの脅威を評価するために使用されます。これらの条件の詳細については、[を参照してください](#)。 [ARPが検出するもの](#)。

ONTAP 9.10.1では、次の両方の条件が検出されると、ARPは警告を発行します。

- 以前にボリュームで認識されなかったファイル拡張子を持つファイルが20個を超える
- 高エントロピーデータ

ONTAP 9.11.1以降では、`_only_one`条件が満たされた場合にARPから脅威警告が発行されます。たとえば、ボリュームで以前に観察されることがないファイル拡張子を持つ20を超えるファイルが24時間以内に観察された場合、ARPはこれを`threat_expended_of_observed_entropy`に分類します。（24時間と20ファイルの値はデフォルトであり、変更可能です）。

ONTAP 9.14.1以降では、ARPが新しいファイル拡張子を監視したとき、およびARPがスナップショットを作成したときにアラートを設定できます。詳細については、[を参照してください](#) [\[modify-alerts\]](#)

特定のボリュームやワークロードでは、異なる検出パラメータが必要です。たとえば、ARP対応ボリュームで多数の種類のファイル拡張子がホストされている場合、以前に見たことのないファイル拡張子のしきい値をデフォルトの20よりも大きい値に変更したり、以前に見たことのないファイル拡張子に基づいて警告を無効にしたりすることができます。ONTAP 9.11.1以降では、特定のワークロードに適した攻撃検出パラメータを変更できます。

### 攻撃検出パラメータの変更

ARP対応ボリュームの想定される動作によっては、攻撃検出パラメータを変更することができます。

#### 手順

1. 既存の攻撃検出パラメータを表示します。

```
security anti-ransomware volume attack-detection-parameters show -vserver  
svm_name -volume volume_name
```

```
security anti-ransomware volume attack-detection-parameters show
-vserver vs1 -volume vol1
```

```

Vserver Name : vs1
Volume Name : vol1
Is Detection Based on High Entropy Data Rate? : true
Is Detection Based on Never Seen before File Extension? : true
Is Detection Based on File Create Rate? : true
Is Detection Based on File Rename Rate? : true
Is Detection Based on File Delete Rate? : true
Is Detection Relaxing Popular File Extensions? : true
High Entropy Data Surge Notify Percentage : 100
File Create Rate Surge Notify Percentage : 100
File Rename Rate Surge Notify Percentage : 100
File Delete Rate Surge Notify Percentage : 100
Never Seen before File Extensions Count Notify Threshold : 20
Never Seen before File Extensions Duration in Hour : 24
```

2. 表示されているフィールドはすべて、ブール値または整数値で変更できます。フィールドを変更するには、`security anti-ransomware volume attack-detection-parameters modify` コマンドを実行します

パラメータの完全なリストについては、を参照してください。 ["ONTAP コマンドリファレンス"](#)。

## 既知のサージを報告

ARPは、アクティブモードでも検出パラメータのベースライン値の変更を継続します。1回限りのサージ、または新しい日常の特徴であるサージのいずれかのボリュームアクティビティのサージを知っている場合は、それを安全として報告する必要があります。これらの急増を安全として手動で報告することは、ARPの脅威評価の精度を向上させるのに役立ちます。

### 1回限りの急増を報告する

1. 既知の状況で1回限りのサージが発生していて、ARPで将来の状況でも同様のサージを報告する場合は、ワークロードの動作からサージをクリアします。

```
security anti-ransomware volume workload-behavior clear-surge -vserver
svm_name -volume volume_name
```

## ベースラインサージの修正

1. 報告されたサージを通常のアプリケーション動作と見なす必要がある場合は、サージを報告してベースラインサージ値を変更します。

```
security anti-ransomware volume workload-behavior update-baseline-from-surge
-vserver svm_name -volume volume_name
```

## ARPアラートの設定

ONTAP 9.14.1以降では、ARPで2つのARPイベントのアラートを指定できます。

- ボリューム上の新しいファイル拡張子の観察
- ARPスナップショットの作成

これら2つのイベントのアラートは、個々のボリュームまたはSVM全体に対して設定できます。SVMでアラートを有効にした場合、アラートの設定は有効にしたあとに作成されたボリュームにのみ継承されます。デフォルトでは、アラートはどのボリュームでも有効になっていません。


イベントアラートは、マルチ管理者検証で制御できます。詳細については、を参照してください [ARPで保護されたボリュームを使用したマルチ管理者検証](#)。

## System Manager の略

### ボリュームのアラートの設定

1. ボリュームに移動します。設定を変更するボリュームを個別に選択します。
2. セキュリティタブを選択し、イベントセキュリティ設定を選択します。
3. 新しいファイル拡張子が検出されましたおよびランサムウェアスナップショットが作成されましたのアラートを受信するには、**Severity**見出しの下のドロップダウンメニューを選択します。イベントを生成しないから通知に設定を変更します。
4. 保存を選択します。

### SVMのアラートを設定する

1. [Storage VM]\*に移動し、設定を有効にするSVMを選択します。
2. [**Security**]\*見出しの下で、[Anti-ransomware]\*カードを探します。選択するオプション  次に、ランサムウェアイベントの重大度を編集します。
3. 新しいファイル拡張子が検出されましたおよびランサムウェアスナップショットが作成されましたのアラートを受信するには、**Severity**見出しの下のドロップダウンメニューを選択します。イベントを生成しないから通知に設定を変更します。
4. 保存を選択します。

## CLI の使用

### ボリュームのアラートの設定

- 新しいファイル拡張子にアラートを設定するには、次の手順を実行します。

```
security anti-ransomware volume event-log modify -vserver svm_name -is
-enabled-on-new-file-extension-seen true
```

- ARPスナップショットの作成に関するアラートを設定するには、次の手順を実行します。

```
security anti-ransomware volume event-log modify -vserver svm_name -is
-enabled-on-snapshot-copy-creation true
```

- を使用して設定を確認します。 anti-ransomware volume event-log show コマンドを実行します

### SVMのアラートを設定する

- 新しいファイル拡張子にアラートを設定するには、次の手順を実行します。

```
security anti-ransomware vserver event-log modify -vserver svm_name -is
-enabled-on-new-file-extension-seen true
```

- ARPスナップショットの作成に関するアラートを設定するには、次の手順を実行します。

```
security anti-ransomware vserver event-log modify -vserver svm_name -is
-enabled-on-snapshot-copy-creation true
```

- を使用して設定を確認します。 security anti-ransomware vserver event-log show コマンドを実行します



## 詳細情報

- ["Autonomous Ransomware Protection AttacksとAutonomous Ransomware Protectionのスナップショットについて理解する"](#)

異常な活動に対応する。

Autonomous Ransomware Protection (ARP) は、保護されたボリュームで異常なアクティビティを検出すると、警告を発行します。通知を評価して、アクティビティが許容可能か (false positive) 、または攻撃が悪意のあるものと思われるかどうかを判断する必要があります。

このタスクについて

ARPは、高データエントロピー、データ暗号化による異常なボリュームアクティビティ、および異常なファイル拡張子の組み合わせを検出すると、疑わしいファイルのリストを表示します。

警告が発行されると、次の 2 つの方法のいずれかでファイルアクティビティにマークを付けることによって応答できます。

- 偽陽性

特定されたファイルタイプはワークロードに想定されているため、無視してかまいません。

- ランサムウェア攻撃の可能性

特定されたファイルタイプは、ワークロード内で予期せぬものであり、攻撃の可能性として扱う必要があります。

どちらの場合も、通知を更新してクリアすると、通常のモニタリングが再開されます。ARPは、選択したファイルアクティビティを使用して、脅威評価プロファイルに評価を記録します。

攻撃の疑いがある場合は、通知をクリアする前に、攻撃であるかどうかを確認し、攻撃である場合はそれに対応し、保護されたデータを復元する必要があります。 ["ランサムウェア攻撃から回復する方法の詳細をご覧ください"](#)。



ボリューム全体をリストアする場合、クリアする通知はありません。

作業を開始する前に

ARPはアクティブモードで実行されている必要があります。

手順

異常なタスクには、System ManagerまたはONTAP CLIを使用して対応できます。

## System Manager の略

1. 「異常なアクティビティ」通知が表示されたら、リンクをクリックするか、【ボリューム】\*概要の[セキュリティ]\*タブに移動します。

警告は\*メニューの[概要]\*ペインに表示されます。

2. 「Detected Abnormal volume activity（異常ボリュームアクティビティの検出）」というメッセージが表示されたら、疑わしいファイルを確認します。

タブで、[疑わしいファイルの種類を表示]\*を選択します。

3. [疑わしいファイルの種類 \*] ダイアログボックスで、各ファイルの種類を調べて、「False Positive」または「Potential Ransomware Attack」としてマークします。

選択した値	対処方法
誤検出	<div><div></div><div>ONTAP 9.13.1以降では、MAVを使用してARP設定を保護している場合、clear-suspect操作によって、1人以上の追加管理者の承認を得るように求められます。"すべての管理者から承認を受ける必要があります" MAV承認グループに関連付けられているか、操作が失敗します。</div></div> <div>[Update]*および[Clear Suspect File Types]*を選択して、決定を記録し、通常のARPモニタリングを再開します。</div>
潜在的なランサムウェア攻撃	攻撃に対応し、保護されたデータを復元します。次に、* Update および Clear Suspect File Types *を選択して、決定を記録し、通常のARPモニタリングを再開します。[+] ボリューム全体をリストアした場合、クリアされる疑わしいファイルタイプは存在しません。

## CLI の使用

1. ランサムウェア攻撃の疑いがある場合は、攻撃の時間と重大度を確認します。

```
security anti-ransomware volume show -vserver svm_name -volume vol_name
```

出力例：

```
Vserver Name: vs0
Volume Name: vol1
State: enabled
Attack Probability: moderate
Attack Timeline: 9/14/2021 01:03:23
Number of Attacks: 1
```

EMS メッセージを確認することもできます。

```
event log show -message-name callhome.arw.activity.seen
```

## 2. 攻撃レポートを生成し、出力先をメモします。

```
security anti-ransomware volume attack generate-report -volume vol_name  
-dest-path file_location/
```

出力例：

```
Report "report_file_vs0_vol1_14-09-2021_01-21-08" available at path  
"vs0:vol1/"
```

## 3. 管理クライアントシステムのレポートを表示します。例：

```
[root@rhel8 mnt]# cat report_file_vs0_vol1_14-09-2021_01-21-08  
  
19  "9/14/2021 01:03:23"    test_dir_1/test_file_1.jpg.lckd  
20  "9/14/2021 01:03:46"    test_dir_2/test_file_2.jpg.lckd  
21  "9/14/2021 01:03:46"    test_dir_3/test_file_3.png.lckd`
```

## 4. ファイル拡張子の評価に基づいて、次のいずれかの操作を実行します。

### ◦ 誤検出

次のコマンドを入力して決定を記録し、許可された拡張子のリストに新しい拡張子を追加して、通常のランサムウェア対策の監視を再開します。

```
anti-ransomware volume attack clear-suspect -vserver svm_name -volume  
vol_name [extension identifiers] -false-positive true
```

拡張機能を識別するには、次のいずれかのパラメータを使用します。

`[-seq-no integer]` 疑わしいリスト内のファイルのシーケンス番号。

`[-extension text, ... ]` ファイル拡張子

`[-start-time date_time -end-time date_time]` 消去されるファイル範囲の開始時刻と終了時刻。形式は「MM/DD/YYYY HH:MM:SS」です。

### ◦ ランサムウェア攻撃の可能性

攻撃に応答し **"ARPによって作成されたバックアップスナップショットからデータをリカバリします"**。データがリカバリされたら、次のコマンドを入力して決定事項を記録し、通常のARPモニタリングを再開します。

```
anti-ransomware volume attack clear-suspect -vserver svm_name -volume  
vol_name [extension identifiers] -false-positive false
```

拡張機能を識別するには、次のいずれかのパラメータを使用します。

`[-seq-no integer]` 疑わしいリスト内のファイルのシーケンス番号

`[-extension text, ... ]` ファイル拡張子

`[-start-time date_time -end-time date_time]` 消去されるファイル範囲の開始時刻と終了時刻。形式は「MM/DD/YYYY HH:MM:SS」です。

ボリューム全体をリストアした場合、クリアされる疑わしいファイルタイプは存在しません。ARPによって作成されたバックアップスナップショットが削除され、攻撃レポートがクリアされます。

5. MAVと予想されるを使用している場合 `clear-suspect` 操作には追加の承認が必要です。各MAVグループ承認者は次のことを行います。

- a. 要求を表示します。

```
security multi-admin-verify request show
```

- b. 通常のランサムウェア対策監視の再開要求を承認します。

```
security multi-admin-verify request approve -index[number returned from show request]
```

最後のグループ承認者に対する応答は、ボリュームが変更され、誤検出が記録されたことを示します。

6. MAVを使用していて、MAVグループ承認者である場合は、疑わしいリクエストを却下することもできます。

```
security multi-admin-verify request veto -index[number returned from show request]
```

#### 詳細情報

- ["KB：自律型ランサムウェア対策攻撃と自律型ランサムウェア対策スナップショットについて"](#)。

## ランサムウェア攻撃のあとにデータをリストア

Autonomous Ransomware Protection (ARP；自律型ランサムウェア対策) で、`Anti_ransomware_backup` ランサムウェアの潜在的な脅威を検出した場合。これらのARP Snapshotコピーまたはボリュームの別のSnapshotコピーのいずれかを使用して、データをリストアできます。

#### このタスクについて

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

以外のSnapshotからリストアするには `Anti_ransomware_backup` スナップショットシステム攻撃が特定された後、最初にARPスナップショットを解放する必要があります。

システム攻撃が報告されていない場合は、最初に `Anti_ransomware_backup` その後、Snapshotコピーを使用して、選択したSnapshotコピーからボリュームをリストアします。

#### 手順


データは、System ManagerまたはONTAP CLIを使用してリストアできます。

## System Manager の略

### システム攻撃後の復元

1. ARPスナップショットから復元するには、手順2に進みます。以前のSnapshotコピーからリストアするには、まずARP Snapshotのロックを解除する必要があります。
  - a. Storage > Volumes（ストレージ）を選択します。
  - b. を選択し、[疑わしいファイルタイプの表示]\*を選択します。
  - c. ファイルを「False Positive」としてマークします。
  - d. [更新]\*および[疑わしいファイルの種類をクリア]\*を選択します。
2. ボリューム内のSnapshotコピーを表示します。


[ストレージ]>[ボリューム]を選択し、ボリュームと Snapshotコピー\*を選択します。

3. 選択するオプション  をクリックし、\*[リストア]\*を選択します。

### システム攻撃が特定されなかった場合のリストア

1. ボリューム内のSnapshotコピーを表示します。

[ストレージ]>[ボリューム]を選択し、ボリュームと Snapshotコピー\*を選択します。

2. 選択するオプション  お客様は、Anti\_ransomware\_backup スナップショット：
3. [\* Restore] を選択します。
4. メニューに戻り、使用する**Snapshot**コピーを選択します。[ Restore] を選択します。

## CLI の使用

### システム攻撃後の復元

1. ARP Snapshotコピーからリストアするには、手順2に進みます。以前のSnapshotコピーからデータをリストアするには、ARP Snapshotのロックを解除する必要があります。



を使用している場合にのみ、以前のSnapshotコピーからリストアする前にAnti-Ransomware SnapLockを解放する必要があります volume snap restore 以下のコマンドを実行します。 FlexClone、Single File Snap Restore、またはその他の方法を使用してデータをリストアする場合は、この作業は必要ありません。

攻撃を「誤検知」および「疑いのないもの」としてマークします。

```
anti-ransomware volume attack clear-suspect -vserver svm_name -volume vol_name [extension identifiers] -false-positive true
```

拡張機能を識別するには、次のいずれかのパラメータを使用します。

[-seq-no integer] 疑わしいリスト内のファイルのシーケンス番号。

[-extension text, ... ] ファイル拡張子

[-start-time date\_time -end-time date\_time] 消去されるファイル範囲の開始時刻と終了時刻。形式は「MM/DD/YYYY HH:MM:SS」です。

2. ボリューム内の Snapshot コピーの一覧を表示します。

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

次の例は、のSnapshotコピーを示しています vol1:

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

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

7 entries were displayed.

### 3. Snapshot コピーからボリュームの内容をリストアします。

```
volume snapshot restore -vserver SVM -volume volume -snapshot snapshot
```

次の例は、の内容をリストアします vol1:

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

システム攻撃が特定されなかった場合のリストア

#### 1. ボリューム内の Snapshot コピーの一覧を表示します。

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

次の例は、のSnapshotコピーを示しています vol1:

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

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

7 entries were displayed.

## 2. Snapshot コピーからボリュームの内容をリストアします。

```
volume snapshot restore -vserver SVM -volume volume -snapshot snapshot
```

次の例は、の内容をリストアします vol1 :

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

## 3. 必要なSnapshotコピーを使用してボリュームをリストアする場合は、手順1と2を繰り返します。

### 詳細情報

- ["KB : ONTAPでのランサムウェア対策とリカバリ"](#)

## 自動Snapshotコピーのオプションを変更します

ONTAP 9.11.1以降では、ランサムウェア攻撃の疑いがある場合に自動的に生成されるAutonomous Ransomware Protection (ARP) Snapshotコピーの保持設定をCLIで制御できます。

作業を開始する前に

変更できるのはノードSVM上のARP Snapshotオプションだけです。

### 手順

1. 現在のARP Snapshotコピー設定をすべて表示するには、次のように入力します。

```
vserver options -vserver svm_name arw*
```



。 vserver options コマンドは非表示のコマンドです。マニュアルページを表示するには、と入力します man vserver options ONTAP CLIで実行します。


2. 選択した現在のARP Snapshotコピー設定を表示するには、次のように入力します。

```
vserver options -vserver svm_name -option-name arw_setting_name
```

3. ARP Snapshotコピーの設定を変更するには、次のように入力します。

```
vserver options -vserver svm_name -option-name arw_setting_name -option-value arw_setting_value
```

次の設定を変更できます。

ARW設定	説明
* arw.snap.maxcount *	指定した時間に1つのボリューム内に存在可能なARP Snapshotコピーの最大数を指定します。古いコピーは、ARP Snapshotコピーの総数がこの指定した制限内に収まるように削除されます。
* arw.snap.create.interval.hours*	ARP Snapshotコピーの間隔（hours_between）を指定します。攻撃が疑われる場合、新しいSnapshotコピーが作成されます。以前に作成されたコピーは、この指定した間隔よりも古いものです。
* arw.snap.normal.retain.interval.hours*	ARP Snapshotコピーを保持する期間（時間）を指定します。ARP Snapshotコピーがこの古いものになると、この経過時間に達するために最新のコピーよりも前に作成された他のARP Snapshotコピーは削除されます。この期間よりも古いARP Snapshotコピーはありません。
* arw.snap.max.retain.interval.days*	<p>ARP Snapshotコピーを保持できる最大期間（日数）を指定します。ボリュームで攻撃が報告されていない場合、指定した期間よりも古いARP Snapshotコピーは削除されます。</p> <p>[+]</p> <div>  <p>中程度の脅威が検出された場合、ARP Snapshotコピーの最大保持間隔は無視されます。脅威に対応して作成されたARP Snapshotコピーは、脅威に対応するまで保持されます。脅威を誤検出としてマークすると、ボリューム上のARP Snapshotコピーが削除されます。</p> </div>
* arw.snap.create.interval.hours.post.max.count*	ボリュームにすでに最大数のARP Snapshotコピーが含まれている場合、ARP Snapshotコピーの間隔（interval_in hours_between）を指定します。最大数に達すると、ARP Snapshotコピーが削除されて、新しいコピー用のスペースが確保されます。このオプションを使用すると、新しいARP Snapshotコピーの作成速度を下げて、古いコピーを保持することができます。ボリュームにARP Snapshotコピーの最大数がすでに含まれている場合、このオプションで指定した間隔が、arw.snap.create.interval.hoursではなく、次のARP Snapshotコピー作成に使用されます。
* arw.surge.snap.interval.days*	ARPサージSnapshotコピーの間隔（日数）を指定します。ONTAPは、IOトラフィックが急増し、最後に作成されたARP Snapshotコピーがこの指定された間隔よりも古い場合に、ARP Snapshotサージコピーを作成します。このオプションは、ARPサージスナップショットの保持期間（日数_）も指定します。

## ウイルスから保護



## ウィルス対策の設定の概要

Vscanは、NetAppが開発したウィルス対策スキャン解決策です。ウィルスやその他の悪意のあるコードからデータを保護できます。

Vscanは、クライアントがSMB経由でファイルにアクセスするときにウィルススキャンを実行します。Vscanは、オンデマンドまたはスケジュールに基づいてスキャンするように設定できます。Vscanは、ONTAPのコマンドラインインターフェイス（CLI）またはONTAPのアプリケーションプログラミングインターフェイス（API）を使用して操作できます。

### 関連情報

["Vscanパートナーソリューション"](#)

## ネットアップのウィルス対策機能について

### ネットアップのウィルススキャンについて

Vscanは、NetAppが開発したウィルス対策スキャン解決策です。ウィルスやその他の悪意のあるコードからデータを保護できます。パートナーが提供するウィルス対策ソフトウェアとONTAPの機能を組み合わせることで、お客様はファイルスキャンの管理に必要な柔軟性を得ることができます。

### ウィルススキャンの仕組み

スキャン処理は、サードパーティベンダーのウィルス対策ソフトウェアをホストする外部サーバで実行されます。

ONTAPは、アクティブなスキャンモードに基づいて、クライアントがSMB経由でファイルにアクセスする場合（オンアクセス）、または特定の場所にあるファイルにスケジュールに従ってアクセスする場合、またはただちに（オンデマンドで）アクセスする場合にスキャン要求を送信します。

- ・クライアントがSMB経由でファイルを開く、読み取る、名前を変更する、閉じるたびにウィルスチェックを行うには、`_on_access_scanning_to`を使用します。ファイル操作は、外部サーバからファイルのスキャンステータスが報告されるまで中断されます。ファイルがすでにスキャンされている場合、ONTAPはファイル操作を許可します。それ以外の場合は、サーバからのスキャンを要求します。

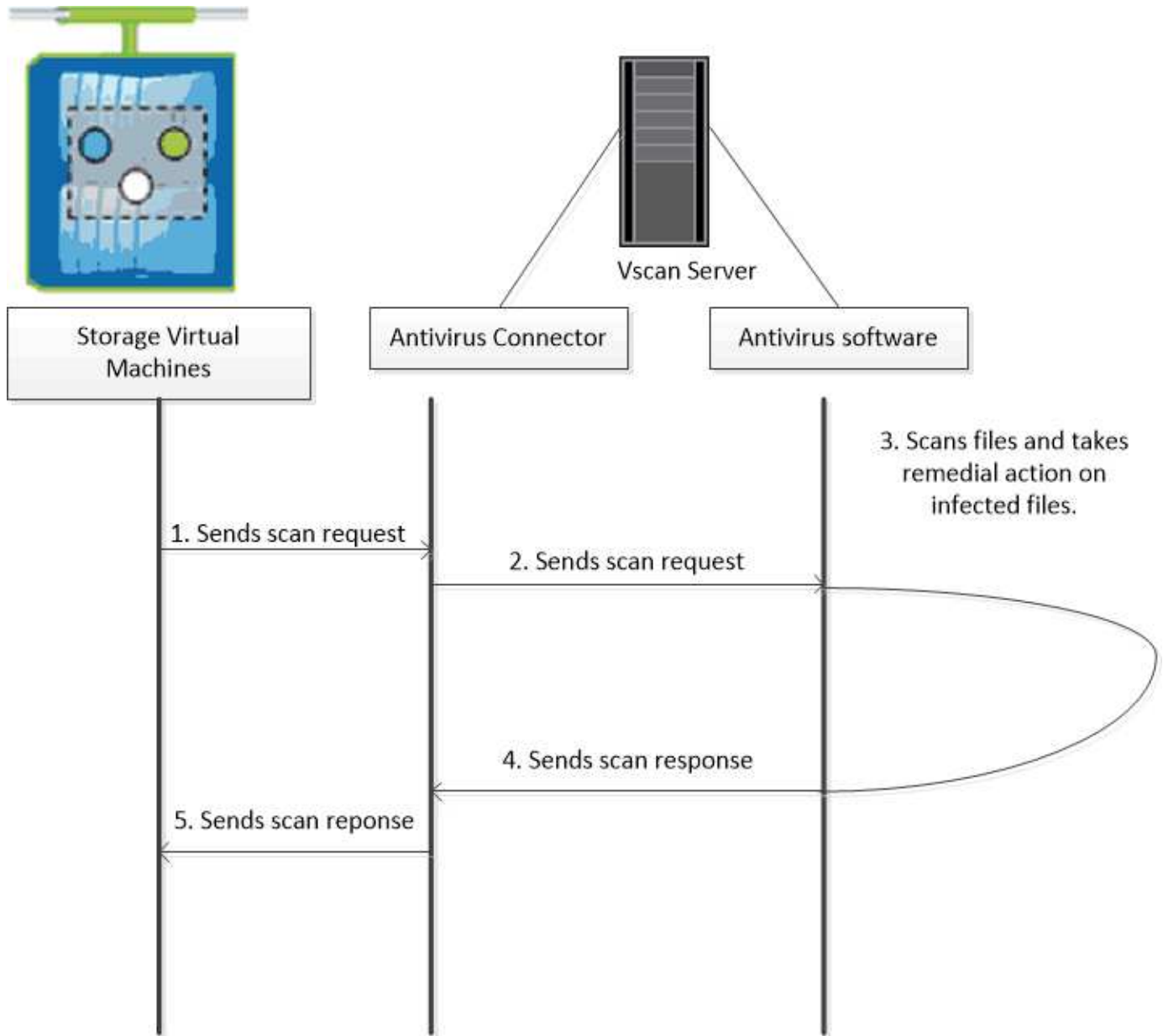
オンアクセススキャンはNFSではサポートされていません。

- ・オンデマンドスキャン`_`を使用すると、ファイルのウィルスチェックをただちにまたはスケジュールに基づいて実行できます。通常はオンアクセススキャン用にサイジングされている既存のAVインフラが過負荷にならないように、オンデマンドスキャンはオフピークの時間帯にのみ実行することを推奨します。外部サーバはチェックしたファイルのスキャンステータスを更新するため、SMB経由でのファイルアクセスのレイテンシが低減されます。ファイルの変更またはソフトウェアバージョンの更新があった場合は、外部サーバから新しいファイルスキャンを要求します。

オンデマンドスキャンは、NFS経由でのみエクスポートされたボリュームも含め、SVMネームスペース内のすべてのパスに対して使用できます。

通常は、SVMでオンアクセスモードとオンデマンドスキャンモードの両方を有効にします。どちらのモードでも、ウィルス対策ソフトウェアはソフトウェアの設定に基づいて感染したファイルに対して修復アクションを実行します。

ネットアップが提供し、外部サーバにインストールされる ONTAP Antivirus Connector が、ストレージシステムとウィルス対策ソフトウェア間の通信を処理します。

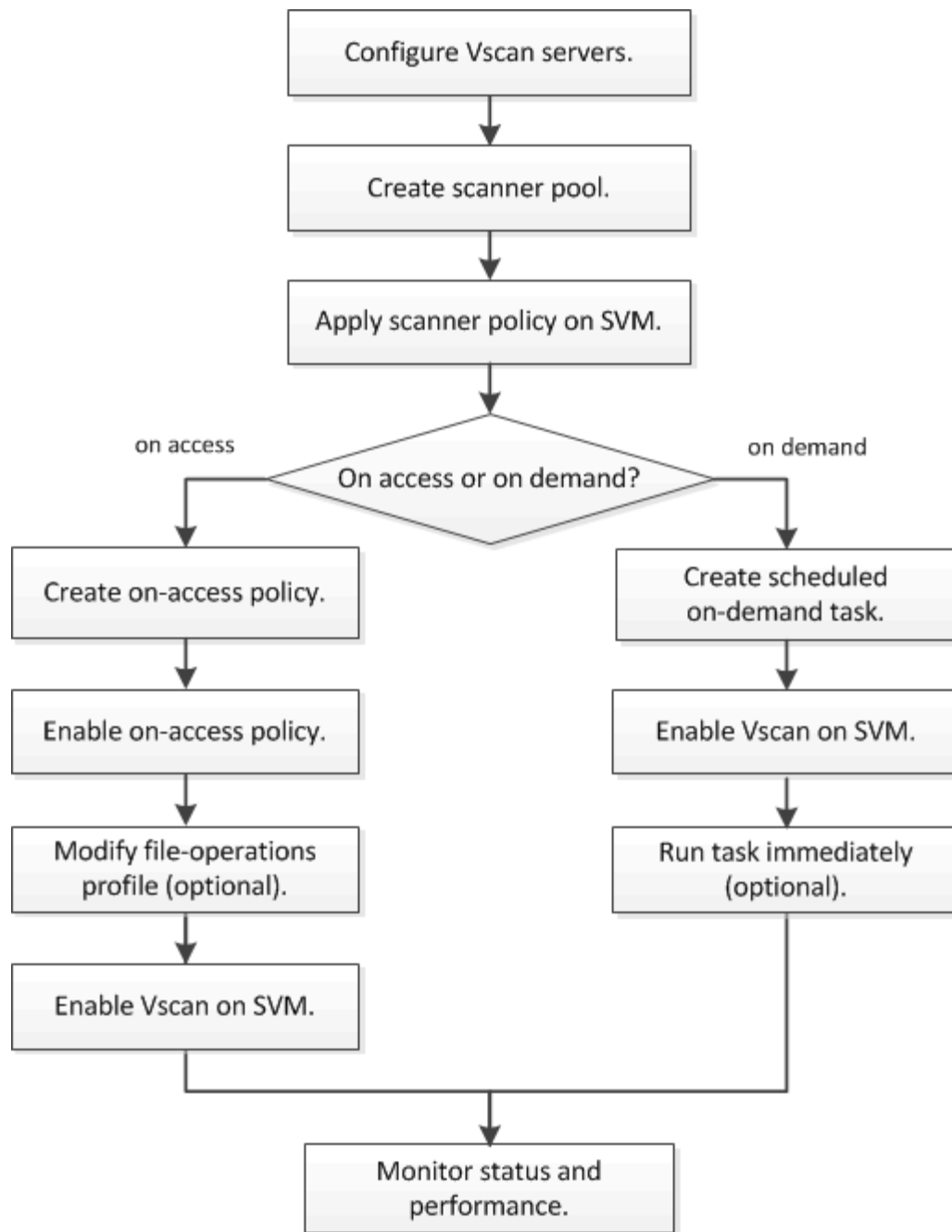


#### ウィルススキャンのワークフロー

スキャンを有効にする前に、スキャナプールを作成し、スキャナポリシーを適用する必要があります。通常は、SVMでオンアクセスモードとオンデマンドスキャンモードの両方を有効にします。



CIFS の設定を完了しておく必要があります。



#### 次のステップ

- [単一クラスタにスキャナプールを作成する](#)
- [単一のクラスタにスキャナポリシーを適用する](#)
- [オンアクセスポリシーを作成します](#)

#### ウィルス対策アーキテクチャ

NetAppウィルス対策アーキテクチャは、Vscanサーバソフトウェアと関連する設定で構成されます。

## Vscanサーバソフトウェア

このソフトウェアはVscanサーバにインストールする必要があります。

- \* ONTAP Antivirus Connector \*

ネットアップが提供するソフトウェアで、SVMとウィルス対策ソフトウェア間のスキャン要求と応答の通信を処理します。仮想マシン上で実行できますが、最高のパフォーマンスを得るには物理マシンを使用します。このソフトウェアは、NetApp Support Siteからダウンロードできます（ログインが必要です）。

- \* アンチウイルスソフトウェア \*

これは、ウィルスやその他の悪意のあるコードのファイルをスキャンするパートナー提供のソフトウェアです。ソフトウェアを設定する際に、感染したファイルに対して実行する処理を指定します。

## Vscanソフトウェア設定

これらのソフトウェアをVscanサーバで設定する必要があります。

- \* スキャナプール \*

この設定では、SVMに接続できるVscanサーバと特権ユーザを定義します。また、スキャン要求のタイムアウト時間も定義します。この時間が経過すると、代替の Vscan サーバがある場合はそのサーバにスキャン要求が送信されます。



Vscanサーバ上のウィルス対策ソフトウェアのタイムアウト時間は、scanner-poolのスキャン要求タイムアウト時間よりも5秒短く設定する必要があります。これにより、ソフトウェアのタイムアウト時間がスキャン要求のタイムアウト時間よりも長いため、ファイルアクセスが遅延または拒否される状況を回避できます。

- \* 特権ユーザ \*

この設定は、VscanサーバがSVMへの接続に使用するドメインユーザアカウントです。スキャナプール内の特権ユーザのリストにアカウントが存在している必要があります。

- \* スキャナポリシー \*

この設定では、スキャナプールをアクティブにするかどうかを指定します。スキャナポリシーはシステムで定義されるため、カスタムのスキャナポリシーを作成することはできません。次の3つのポリシーのみを使用できます。

- Primary スキャナプールをアクティブにします。
- Secondary プライマリスキャナプールのVscanサーバが1つも接続されていない場合にのみスキャナプールをアクティブにします。
- Idle スキャナプールを非アクティブにします。

- \* オンアクセスポリシー \*

この設定では、オンアクセススキャンの範囲を定義します。スキャンする最大ファイルサイズ、スキャンに含めるファイル拡張子とパス、およびスキャンから除外するファイル拡張子とパスを指定できます。

デフォルトでは、読み取り / 書き込みボリュームのみがスキャンされます。読み取り専用ボリュームのス

キャンを有効にするフィルタや、実行アクセス権で開かれたファイルのみにスキャンを制限するフィルタを指定することができます。

- `scan-ro-volume` 読み取り専用ボリュームのスキャンを有効にします。
- `scan-execute-access` 実行アクセス権で開かれたファイルにスキャンを制限します。



「アクセスの実行」と「アクセスの実行」は「アクセスの実行」とは異なります。指定されたクライアントは、実行ファイルが「実行意図」で開かれている場合にのみ、実行ファイルに対して「実行アクセス」を持つことになります。

を設定できます `scan-mandatory` オフにすると、ウィルススキャンに使用できるVscanサーバがない場合にファイルアクセスが許可されます。オンアクセスモードでは、次の2つのオプションのいずれかを選択できます。

- 必須：このオプションを指定すると、タイムアウト時間が経過するまで、Vscanはサーバへのスキャン要求の配信を試みます。サーバがスキャン要求を受け入れなかった場合、クライアントアクセス要求は拒否されます。
- 必須以外：このオプションを使用すると、Vscanサーバがウィルススキャンに使用できるかどうかに関係なく、Vscanでクライアントアクセスが常に許可されます。

#### • \* オンデマンドタスク \*

この設定では、オンデマンドスキャンの範囲を定義します。スキャンする最大ファイルサイズ、スキャンに含めるファイル拡張子とパス、およびスキャンから除外するファイル拡張子とパスを指定できます。デフォルトでは、サブディレクトリ内のファイルがスキャンされます。

`cron` スケジュールを使用していつタスクを実行するかを指定できます。を使用できます `vserver vscan on-demand-task run` タスクをすぐに実行するコマンド。

#### • \* Vscan ファイル処理プロファイル（オンアクセススキャンのみ） \*

◦ `vscan-fileop-profile` のパラメータ `vserver cifs share create` コマンドは、ウィルススキャンをトリガーするSMBファイル処理を定義します。デフォルトでは、パラメータはに設定されています `'standard'` NetAppのベストプラクティスです。このパラメータは、SMB共有を作成または変更するときに必要に応じて調整できます。

- `no-scan` 共有に対してウィルススキャンを一切トリガーしません。
- `standard` 開く、閉じる、および名前変更の各処理でウィルススキャンをトリガーします。
- `strict` 開く、読み取る、閉じる、および名前変更の各処理でウィルススキャンをトリガーします。

◦ `strict` プロファイルを使用すると、複数のクライアントが同時に1つのファイルにアクセスする状況でセキュリティが強化されます。あるクライアントがウィルスを書き込んだあとにファイルを閉じたときに、別のクライアントで同じファイルが開いたままになっている場合は、`strict` 2番目のクライアントでの読み取り処理で、ファイルが閉じる前にスキャンがトリガーされるようにします。

の制限に注意する必要があります `strict`` 同時にアクセスされる可能性があるファイルを含む共有にプロファイルを設定します。このプロファイルはより多くのスキャン要求を生成するため、パフォーマンスに影響を与える可能性があります。

- `writes-only` 変更されたファイルが閉じられたときにのみウィルススキャンをトリガーします。

以来 writes-only 生成されるスキャン要求が少なくなり、通常はパフォーマンスが向上します。

このプロファイルを使用する場合は、修復不可能な感染ファイルを削除または隔離するようにスキャナを設定して、アクセスできないようにする必要があります。たとえば、クライアントがウイルスを書き込んだあとにファイルを閉じた場合、そのファイルにアクセスしたクライアントが修復、削除、または隔離されていない without それへの書き込みは感染します。



クライアントアプリケーションが名前変更操作を実行すると、ファイルは新しい名前で閉じられ、スキャンされません。このような処理がセキュリティ上の問題になる場合は、を使用して ください standard または strict プロファイル (Profile) :

## Vscanパートナーソリューション

NetAppは、Trellix、Symantec、Trend Micro、およびSentinel Oneと協力して、ONTAP Vscanテクノロジーを基盤とする業界をリードするアンチマルウェアおよびアンチウイルスソリューションを提供しています。これらのソリューションは、ファイルをスキャンしてマルウェアを検出し、影響を受けるファイルを修正するのに役立ちます。

次の表に示すように、Trellix、Symantec、Trend Microの相互運用性の詳細については、NetAppのInteroperability Matrixを参照してください。TrellixとSymantecの相互運用性の詳細については、パートナーのWebサイトを参照してください。Sentinel Oneおよびその他の新しいパートナーの相互運用性の詳細は、パートナーのWebサイトで管理されます。

パートナー	解決策のドキュメント	相互運用性の詳細
Trellix (旧McAfee)	"Trellix製品ドキュメント"	<ul style="list-style-type: none"><li>• "<a href="#">NetApp Interoperability Matrix Tool</a> で確認できます"</li><li>• "<a href="#">Endpoint Security Storage Protection</a>でサポートされるプラットフォーム (<a href="#">trellix.com</a>) "</li></ul>
シマンテック	" <a href="#">Symantec Protection Engine 9.0.0</a> "	<ul style="list-style-type: none"><li>• "<a href="#">NetApp Interoperability Matrix Tool</a> で確認できます"</li><li>• "<a href="#">Symantec Protection Engine (SPE) for Network Attached Storage (NAS) 9.x.x</a>と認定されたパートナーデバイスのサポートマトリックス"</li><li>• "<a href="#">Symantec Protection Engine (SPE) for Network Attached Storage (NAS) 8.x</a>認定パートナーデバイスのサポートマトリックス (<a href="#">broadcom.com</a>) "</li></ul>
トレンドマイクロ	"『 <a href="#">Trend Micro ServerProtect for Storage 6.0 Getting Started Guide</a> 』 "	" <a href="#">NetApp Interoperability Matrix Tool</a> で確認できます"

パートナー	解決策のドキュメント	相互運用性の詳細
センチネル1	<ul style="list-style-type: none"> <li>• <a href="#">"SentinelOne Singularityクラウドデータセキュリティ"</a></li> <li>• <a href="#">"SentinelOneのサポート"</a></li> </ul> <p>このリンクにはユーザーログインが必要です。Sentinel Oneからアクセス権をリクエストできます。</p>	深い本能

## Vscan サーバのインストールと設定

### Vscan サーバのインストールと設定

1つ以上のVscanサーバを設定して、システム上のファイルがウィルススキャンされるようにします。サーバにウィルス対策ソフトウェアをインストールして設定するには、ベンダーからの指示に従ってください。

NetAppが提供するREADMEファイルの手順に従って、ONTAP Antivirus Connectorをインストールして設定します。または、["\[Install ONTAP Antivirus Connectorページ\]"](#)。



ディザスタリカバリおよびMetroCluster構成の場合は、プライマリ/ローカルおよびセカンダリ/パートナーのONTAPクラスタ用に個別のVscanサーバをセットアップして設定する必要があります。

### ウィルス対策ソフトウェアの要件

- ウィルス対策ソフトウェアの要件については、ベンダーのドキュメントを参照してください。
- Vscan でサポートされるベンダー、ソフトウェア、およびバージョンについては、["Vscanパートナーソリューション"](#) ページ

### ONTAP Antivirus Connector の要件

- ONTAP Antivirus Connectorは、NetApp Support Siteの[\\*ソフトウェアダウンロード\\*ページ](#)からダウンロードできます。 ["ネットアップのダウンロード：ソフトウェア"](#)
- ONTAP Antivirus ConnectorでサポートされるWindowsのバージョンと相互運用性の要件については、["Vscanパートナーソリューション"](#)。



クラスタ内の Vscan サーバによってインストールする Windows サーバのバージョンは同じでなくても構いません。

- Windows サーバに .NET 3.0 以降がインストールされている必要があります。
- Windows サーバで SMB 2.0 が有効になっている必要があります。



## ONTAP Antivirus Connectorのインストール

ONTAP Antivirus ConnectorをVscanサーバにインストールして、ONTAPを実行しているシステムとVscanサーバの間の通信を有効にします。ONTAP Antivirus Connectorをインストールすると、ウィルス対策ソフトウェアは1つ以上のStorage Virtual Machine（SVM）と通信できるようになります。

### このタスクについて

- を参照してください "[Vscanパートナーソリューション](#)" サポートされるプロトコル、ウィルス対策ベンダーのソフトウェアのバージョン、ONTAPのバージョン、相互運用性の要件、およびWindowsサーバについては、ページを参照してください。
- .NET 4.5.1以降がインストールされている必要があります。
- ONTAP Antivirus Connectorは仮想マシンで実行できます。ただし、パフォーマンスを最大限に高めるために、NetAppではアンチウイルススキャンに専用の仮想マシンを使用することを推奨しています。
- ONTAP Antivirus Connectorをインストールして実行するWindowsサーバでSMB 2.0が有効になっている必要があります。

### 作業を開始する前に

- サポートサイトからONTAP Antivirus Connectorセットアップファイルをダウンロードし、ハードドライブのディレクトリに保存します。
- ONTAP Antivirus Connectorをインストールするための要件を満たしていることを確認します。
- Antivirus Connectorをインストールするための管理者権限があることを確認します。

### 手順

1. 適切なセットアップファイルを実行して、Antivirus Connectorインストールウィザードを開始します。
2. [次へ] を選択します。[インストール先フォルダ]ダイアログボックスが開きます。
3. 表示されているフォルダにAntivirus Connectorをインストールするには、\_Next\_を選択します。別のフォルダにインストールするには、\_Change\_\_を選択します。
4. [Windows AV Connector ONTAPサービスのクレデンシャル]ダイアログボックスが開きます。
5. Windowsサービスのクレデンシャルを入力するか、\*[追加]\*を選択してユーザを選択します。ONTAPシステムの場合、このユーザは有効なドメインユーザであり、SVMのスキャナプール設定に存在している必要があります。
6. 「\* 次へ \*」を選択します。[プログラムをインストールする準備ができました]ダイアログボックスが開きます。
7. インストールを開始するには\*を選択します。設定を変更する場合は[戻る]\*を選択します。ステータス・ボックスが開き'インストールの進行状況が表示され'InstallShield Wizard Completedダイアログ・ボックスが表示されます
8. ONTAP ONTAP管理LIFまたはデータLIFの設定を続行する場合は、[LIFの設定]チェックボックスを選択します。  
このVscanサーバを使用するには、ONTAP管理LIFまたはデータLIFを少なくとも1つ設定する必要があります。
9. インストールログを表示する場合は、[Windowsインストーラログを表示する]チェックボックスをオンにします。
10. を選択してインストールを終了し、**InstallShield**ウィザードを閉じます。



ONTAP LIFを設定するための[Configure ONTAP LIFs]\*アイコンがデスクトップに保存されます。

11. Antivirus ConnectorにSVMを追加します。

SVMをAntivirus Connectorに追加するには、データLIFのリストを取得するようにポーリングされるONTAP管理LIFを追加するか、またはデータLIFを直接設定します。

ONTAP管理LIFが設定されている場合は、ポーリング情報とONTAP管理者アカウントのクレデンシャルも指定する必要があります。

- SVMの管理LIFまたはIPアドレスが management-https。これは、データLIFのみを設定する場合は必要ありません。
- HTTPアプリケーション用のユーザアカウントを作成し、（少なくとも読み取り専用）アクセスを持つロールを割り当てたことを確認します。 /api/network/ip/interfaces REST API：ユーザの作成の詳細については、を参照してください。 ["Security login role create を実行します"](#) および ["security login create を実行します"](#) ONTAPのマニュアルページ



管理SVM用に認証トンネルSVMを追加して、ドメインユーザをアカウントとして使用することもできます。詳細については、を参照してください ["security login domain-tunnel createのように設定します"](#) ONTAPのマニュアルページまたは /api/security/acccounts および /api/security/roles adminアカウントとロールを設定するためのREST API。

手順

1. Antivirus Connectorのインストールの完了時にデスクトップに保存されていた\*アイコンを右クリックし、[Run as Administrator]\*を選択します。
2. [Configure ONTAP LIFs]ダイアログボックスで、優先する設定タイプを選択し、次の操作を実行します。

作成するLIFのタイプ	実行する手順
データ LIF	<ol style="list-style-type: none"><li>a. 「role」を「data」に設定</li><li>b. 「data protocol」を「cifs」に設定</li><li>c. 「firewall policy」を「data」に設定する</li><li>d. 「service policy」を「default-data-files」に設定</li></ol>
管理LIF	<ol style="list-style-type: none"><li>a. 「role *」を「data」に設定</li><li>b. 「data protocol」を「none」に設定します。</li><li>c. 「firewall policy」を「mgmt」に設定</li><li>d. 「service policy」を「default-management」に設定</li></ol>

詳細については、をご覧ください ["LIFの作成"](#)。

LIFを作成したら、追加するSVMのデータLIF、管理LIF、またはIPアドレスを入力します。クラスタ管理LIFを入力することもできます。クラスタ管理LIFを指定すると、そのクラスタ内でSMBを提供しているすべてのSVMがVscanサーバを使用できます。



VscanサーバでKerberos認証が必要な場合は、各SVMデータLIFに一意的DNS名を付ける必要があります。その名前をWindows Active DirectoryでServer Principal Name (SPN; サーバプリンシパル名) として登録する必要があります。各データLIFで一意的DNS名を使用できない場合、またはSPNとして登録されていない場合、VscanサーバはNT LAN Managerメカニズムを使用して認証します。Vscanサーバを接続したあとにDNS名とSPNを追加または変更した場合は、VscanサーバでAntivirus Connectorサービスを再起動して変更を適用する必要があります。

3. 管理LIFを設定するには、ポーリング期間を秒単位で入力します。ポーリング期間は、Antivirus ConnectorがSVMまたはクラスタのLIF設定に対する変更をチェックする頻度です。デフォルトのポーリング間隔は60秒です。
4. ONTAP管理者アカウント名とパスワードを入力して、管理LIFを設定します。
5. [テスト]\*をクリックして接続を確認し、認証を確認します。認証は管理LIFの設定でのみ検証されます。
6. ポーリングまたは接続先のLIFのリストにLIFを追加するには、\*[更新]\*をクリックします。
7. [保存]\*をクリックして、レジストリへの接続を保存します。
8. 接続のリストをレジストリインポートまたはレジストリエクスポートファイルにエクスポートする場合は、\*エクスポート\*をクリックします。これは、複数のVscanサーバが同じ管理LIFまたはデータLIFのセットを使用する場合に便利です。

を参照してください ["ONTAP Antivirus Connectorページの設定"](#) を参照してください。

## ONTAP Antivirus Connectorの設定

ONTAP管理LIF、ポーリング情報、およびONTAP管理者アカウントのクレデンシャルを入力するか、データLIFだけを入力して、接続先のStorage Virtual Machine (SVM) を指定するようにONTAP Antivirus Connectorを設定します。また、SVM接続の詳細を変更したり、SVM接続を削除したりすることもできます。ONTAP管理LIFが設定されている場合、デフォルトでは、ONTAP Antivirus ConnectorはREST APIを使用してデータLIFのリストを取得します。

### SVM接続の詳細を変更する

Antivirus Connectorに追加されたStorage Virtual Machine (SVM) 接続の詳細を更新するには、ONTAP管理LIFとポーリング情報を変更します。データLIFの追加後に更新することはできません。データLIFを更新するには、まずデータLIFを削除してから、新しいLIFまたはIPアドレスを使用して再度追加する必要があります。

### 作業を開始する前に

HTTPアプリケーション用のユーザアカウントを作成し、(少なくとも読み取り専用) アクセスを持つロールを割り当てたことを確認します。 /api/network/ip/interfaces REST API :

ユーザの作成の詳細については、を参照してください。 ["Security login role create を実行します"](#) および ["security login create を実行します"](#) コマンド

管理SVM用に認証トンネルSVMを追加して、ドメインユーザをアカウントとして使用することもできます。詳細については、を参照してください ["security login domain-tunnel createのように設定します"](#) ONTAPのマニュアルページ

### 手順

1. Antivirus Connectorのインストールの完了時にデスクトップに保存されていた\*アイコンを右クリック

し、[Run as Administrator]\*を選択します。[Configure ONTAP LIF]ダイアログボックスが開きます。

2. SVMのIPアドレスを選択し、\*[更新]\*をクリックします。
3. 必要に応じて情報を更新します。
4. [保存]\*をクリックして、レジストリの接続の詳細を更新します。
5. 接続のリストをレジストリインポートまたはレジストリエクスポートファイルにエクスポートする場合は、\*エクスポート\*をクリックします。  
これは、複数のVscanサーバが同じ管理LIFまたはデータLIFのセットを使用する場合に便利です。

#### Antivirus ConnectorからSVM接続を削除する

不要になったSVM接続は削除できます。

#### 手順

1. Antivirus Connectorのインストールの完了時にデスクトップに保存されていた\*アイコンを右クリックし、[Run as Administrator]\*を選択します。[Configure ONTAP LIF]ダイアログボックスが開きます。
2. SVMのIPアドレスを1つ以上選択し、\*[削除]\*をクリックします。
3. [保存]\*をクリックして、レジストリの接続の詳細を更新します。
4. 接続のリストをレジストリインポートまたはレジストリエクスポートファイルにエクスポートする場合は、\*エクスポート\*をクリックします。  
これは、複数のVscanサーバが同じ管理LIFまたはデータLIFのセットを使用する場合に便利です。

#### トラブルシューティングを行う

#### 作業を開始する前に

この手順でレジストリ値を作成する場合は、右側のペインを使用します。

診断目的でAntivirus Connectorログを有効または無効にすることができます。デフォルトでは、これらのログは無効になっています。パフォーマンスを強化するには、Antivirus Connectorのログを無効なままにし、重大イベントに対してのみ有効にする必要があります。

#### 手順

1. [スタート]\*を選択し、検索ボックスに「regedit」と入力して、regedit.exe をクリックします。
2. レジストリエディタ\*で、ONTAP Antivirus Connectorの次のサブキーを探します。  
HKEY\_LOCAL\_MACHINE\SOFTWARE\Wow6432Node\Data ONTAP\Clustered Data ONTAP Antivirus Connector\v1.0
3. 次の表に示すタイプ、名前、および値を指定して、レジストリ値を作成します。

を入力します	名前	値
文字列	トレースパス	C:\avshim.log

このレジストリ値には、他の有効なパスを指定できます。

4. 次の表に示すタイプ、名前、値、およびログ情報を指定して、別のレジストリ値を作成します。

を入力します	名前	重要なロギング	中間ロギング	詳細なロギング
--------	----	---------	--------	---------

DWORD	トレースレベル	1.	2または3	4.
-------	---------	----	-------	----

これにより、手順3でTracePathに指定したパス値に保存されるAntivirus Connectorログが有効になります。

- 手順3および4で作成したレジストリ値を削除して、Antivirus Connectorログを無効にします。
- 「LogRotation」という名前でタイプ「multi\_sz」の別のレジストリ値を作成します（引用符なし）。"LogRotation"で、ローテーションサイズのエントリとして「logFileSize:1」を指定し（1は1MBを表します）、次の行では「logFileCount:5」をローテーションの制限（5が制限）を入力します。



これらの値はオプションです。指定しない場合は、ローテーションサイズとローテーションの上限にそれぞれデフォルト値の20MBと10ファイルが使用されます。指定された整数値には、小数または小数の値は指定されません。デフォルト値よりも大きい値を指定した場合は、代わりにデフォルト値が使用されます。

- ユーザー設定のログローテーションを無効にするには、手順6で作成したレジストリ値を削除します。

#### カスタマイズ可能なバナー

カスタムバナーを使用すると、法的拘束力のあるステートメントとシステムアクセスに関する免責事項を\_Configure ONTAP LIFAPI\_windowに配置できます。

#### ステップ

1. の内容を更新してデフォルトバナーを変更します。 banner.txt ファイルをインストールディレクトリに保存し、変更を保存します。  
変更内容がバナーに反映されるようにするには、[Configure ONTAP LIF]ウィンドウを再度開いてください。

#### Extended Ordinance (EO) モードを有効にする

セキュアな運用のために、拡張規則 (EO) モードを有効または無効にすることができます。

#### 手順

1. [スタート]\*を選択し、検索ボックスに「regedit」と入力して、 regedit.exe をクリックします。
2. レジストリエディタ\*で、ONTAP Antivirus Connectorの次のサブキーを探します。  
HKEY\_LOCAL\_MACHINE\SOFTWARE\Wow6432Node\Data ONTAP\Clustered Data ONTAP Antivirus Connector\v1.0
3. 右側のペインで、EOモードを有効にするには「EO\_Mode」（引用符なし）と値「1」（引用符なし）という名前の「DWORD」タイプの新しいレジストリ値を作成し、EOモードを無効にするには「0」（引用符なし）を作成します。



デフォルトでは、EO\_Mode レジストリエントリがありません。EOモードは無効です。EOモードをイネーブルにする場合は、外部syslogサーバと相互証明書認証の両方を設定する必要があります。

## 外部syslogサーバの設定

作業を開始する前に

この手順でレジストリ値を作成する場合は、右側のペインを使用することに注意してください。

手順

1. [スタート]\*を選択し、検索ボックスに「regedit」と入力して、regedit.exe をクリックします。
2. レジストリエディタ\*で、syslog設定用のONTAP Antivirus Connector用の次のサブキーを作成します。  
HKEY\_LOCAL\_MACHINE\SOFTWARE\Wow6432Node\Data ONTAP\Clustered Data ONTAP  
Antivirus Connector\v1.0\syslog
3. 次の表に示すように、タイプ、名前、および値を指定してレジストリ値を作成します。

を入力します	名前	価値
DWORD	syslog_enabled	1または0

値「1」はsyslogを有効にし、値「0」はsyslogを無効にすることに注意してください。

4. 次の表に示す情報を指定して、別のレジストリ値を作成します。

を入力します	名前
REG_SZ	syslog_host

[Value]フィールドにsyslogホストのIPアドレスまたはドメイン名を入力します。

5. 次の表に示す情報を指定して、別のレジストリ値を作成します。

を入力します	名前
REG_SZ	syslog_port

[Value]フィールドに、syslogサーバが実行されているポート番号を入力します。

6. 次の表に示す情報を指定して、別のレジストリ値を作成します。

を入力します	名前
REG_SZ	syslog_protocol

syslogサーバで使用中のプロトコル（「tcp」または「udp」）を[Value]フィールドに入力します。

7. 次の表に示す情報を指定して、別のレジストリ値を作成します。

を入力します	名前	LOG_CRIT	LOG_NOTICE	ログ情報	LOG_DEBUG
DWORD	syslog_level	2.	5.	6.	7.

8. 次の表に示す情報を指定して、別のレジストリ値を作成します。

を入力します	名前	価値
DWORD	syslog_tls	1または0

値「1」はTransport Layer Security (TLS) でsyslogを有効にし、値「0」はTLSでsyslogを無効にすることに注意してください。

設定された外部**syslog**サーバがスムーズに動作することを確認する

- キーが存在しない場合、またはnull値がある場合は、次の手順を実行します。
  - プロトコルのデフォルトは「TCP」です。
  - ポートのデフォルトは、プレーンな「TCP/UDP」の場合は「514」、TLSの場合は「6514」です。
  - syslogレベルのデフォルト値は5 (log\_notice) です。
- syslogが有効になっていることを確認するには、syslog\_enabled 値は「1」です。をクリックします syslog\_enabled 値は「1」です。EOモードが有効かどうかに関係なく、設定されたリモートサーバにログインできます。
- EOモードが「1」に設定されていて、syslog\_enabled 「1」から「0」までの値。以下が適用されます。
  - syslogがEOモードでイネーブルになっていない場合は、サービスを開始できません。
  - システムが安定した状態で実行されている場合は、EOモードでsyslogを無効にできず、syslogが強制的に「1」に設定されていることを示す警告が表示されます。これはレジストリに表示されます。この場合は、まずEOモードをディセーブルにしてから、syslogをディセーブルにする必要があります。
- EOモードおよびsyslogが有効になっているときにsyslogサーバが正常に実行できない場合、サービスの実行は停止します。これは、次のいずれかの理由で発生する可能性があります。
  - syslog\_hostが無効であるか、設定されていません。
  - UDPまたはTCP以外の無効なプロトコルが設定されています。
  - ポート番号が無効です。
- TCPまたはTLS over TCP構成では、サーバがIPポートをリスンしていない場合、接続は失敗し、サービスはシャットダウンします。

#### X.509相互証明書認証の設定

管理パス内のAntivirus ConnectorとONTAP間のSecure Sockets Layer (SSL) 通信では、X.509証明書ベースの相互認証が可能です。EOモードが有効になっていて証明書が見つからない場合、AVコネクタは終了します。Antivirus Connectorで次の手順を実行します。

#### 手順

1. Antivirus Connectorは、Antivirus Connectorのインストールディレクトリを実行するディレクトリパスで、Antivirus Connectorクライアント証明書とNetAppサーバの認証局 (CA) 証明書を検索します。証明書をこの固定ディレクトリパスにコピーします。
2. クライアント証明書とその秘密鍵をPKCS12形式で埋め込み、「av\_client.p12」という名前を付けます。
3. NetAppサーバの証明書への署名に使用したCA証明書 (およびルートCAまでの中間署名機関)

が、Privacy Enhanced Mail (PEM) 形式で「ontap\_CA.pem」という名前のものであることを確認します。Antivirus Connectorインストールディレクトリに配置します。NetApp ONTAPシステムで、Antivirus Connectorのクライアント証明書に「client-ca」タイプの証明書として署名するためのCA証明書（およびルートCAまでの中間署名機関）を「ONTAP」にインストールします。

## スキャナプールを設定

### スキャナプールの概要の設定

スキャナプールは、SVM に接続できる Vscan サーバと特権ユーザを定義します。スキャナポリシーは、スキャナプールがアクティブかどうかを決定します。



SMBサーバでエクスポートポリシーを使用する場合は、各Vscanサーバをエクスポートポリシーに追加する必要があります。

### 単一クラスタにスキャナプールを作成する

スキャナプールは、SVM に接続できる Vscan サーバと特権ユーザを定義します。個々のSVM用またはクラスタ内のすべてのSVM用のスキャナプールを作成できます。

#### 必要なもの

- SVM と Vscan サーバは同じドメインに属しているか、信頼されたドメインに属している必要があります。
- 個々のSVM用のスキャナプールを定義する場合は、SVM管理LIFまたはSVMデータLIFにONTAP Antivirus Connectorを設定しておく必要があります。
- クラスタ内のすべてのSVM用のスキャナプールを定義する場合は、クラスタ管理LIFにONTAP Antivirus Connectorを設定しておく必要があります。
- 特権ユーザのリストには、Vscan サーバが SVM への接続に使用するドメインユーザアカウントが含まれている必要があります。
- スキャナプールの設定が完了したら、サーバへの接続ステータスを確認します。

#### 手順

1. スキャナプールを作成します。

```
vserver vscan scanner-pool create -vserver data_SVM|cluster_admin_SVM -scanner-pool scanner_pool -hostnames Vscan_server_hostnames -privileged-users privileged_users
```

- 個々の SVM 用のプールの場合はデータ SVM、クラスタ内のすべての SVM 用のプールの場合はクラスタ管理 SVM を指定します。
- 各 Vscan サーバのホスト名には IP アドレスまたは FQDN を指定します。
- 各特権ユーザのドメイン名とユーザ名を指定します。  
すべてのオプションの一覧については、コマンドのマニュアルページを参照してください。

次のコマンドは、という名前のスキャナプールを作成します SP をクリックします vs1 SVM :

```
cluster1::> vserver vscan scanner-pool create -vserver vs1 -scanner-pool
SP -hostnames 1.1.1.1,vmwin204-27.fsct.nb -privileged-users
cifs\u1,cifs\u2
```

## 2. スキャナプールが作成されたことを確認します。

```
vserver vscan scanner-pool show -vserver data_SVM|cluster_admin_SVM -scanner
-pool scanner_pool
```

すべてのオプションの一覧については、コマンドのマニュアルページを参照してください。

次のコマンドは、の詳細を表示します SP スキャナプール：

```
cluster1::> vserver vscan scanner-pool show -vserver vs1 -scanner-pool
SP

Vserver: vs1
Scanner Pool: SP
Applied Policy: idle
Current Status: off
Cluster on Which Policy Is Applied: -
Scanner Pool Config Owner: vserver
List of IPs of Allowed Vscan Servers: 1.1.1.1, 10.72.204.27
List of Host Names of Allowed Vscan Servers: 1.1.1.1, vmwin204-
27.fsct.nb
List of Privileged Users: cifs\u1, cifs\u2
```

を使用することもできます `vserver vscan scanner-pool show` コマンドを使用してSVMのすべてのスキャナプールを表示します。コマンド構文全体については、コマンドのマニュアルページを参照してください。

## MetroCluster 構成でスキャナプールを作成

MetroCluster 構成の各クラスタには、クラスタのプライマリとセカンダリの SVM に対応するプライマリとセカンダリのスキャナプールを作成する必要があります。

### 必要なもの

- SVM と Vscan サーバは同じドメインに属しているか、信頼されたドメインに属している必要があります。
- 個々のSVM用のスキャナプールを定義する場合は、SVM管理LIFまたはSVMデータLIFにONTAP Antivirus Connectorを設定しておく必要があります。
- クラスタ内のすべてのSVM用のスキャナプールを定義する場合は、クラスタ管理LIFにONTAP Antivirus Connectorを設定しておく必要があります。
- 特権ユーザのリストには、Vscan サーバが SVM への接続に使用するドメインユーザアカウントが含まれている必要があります。



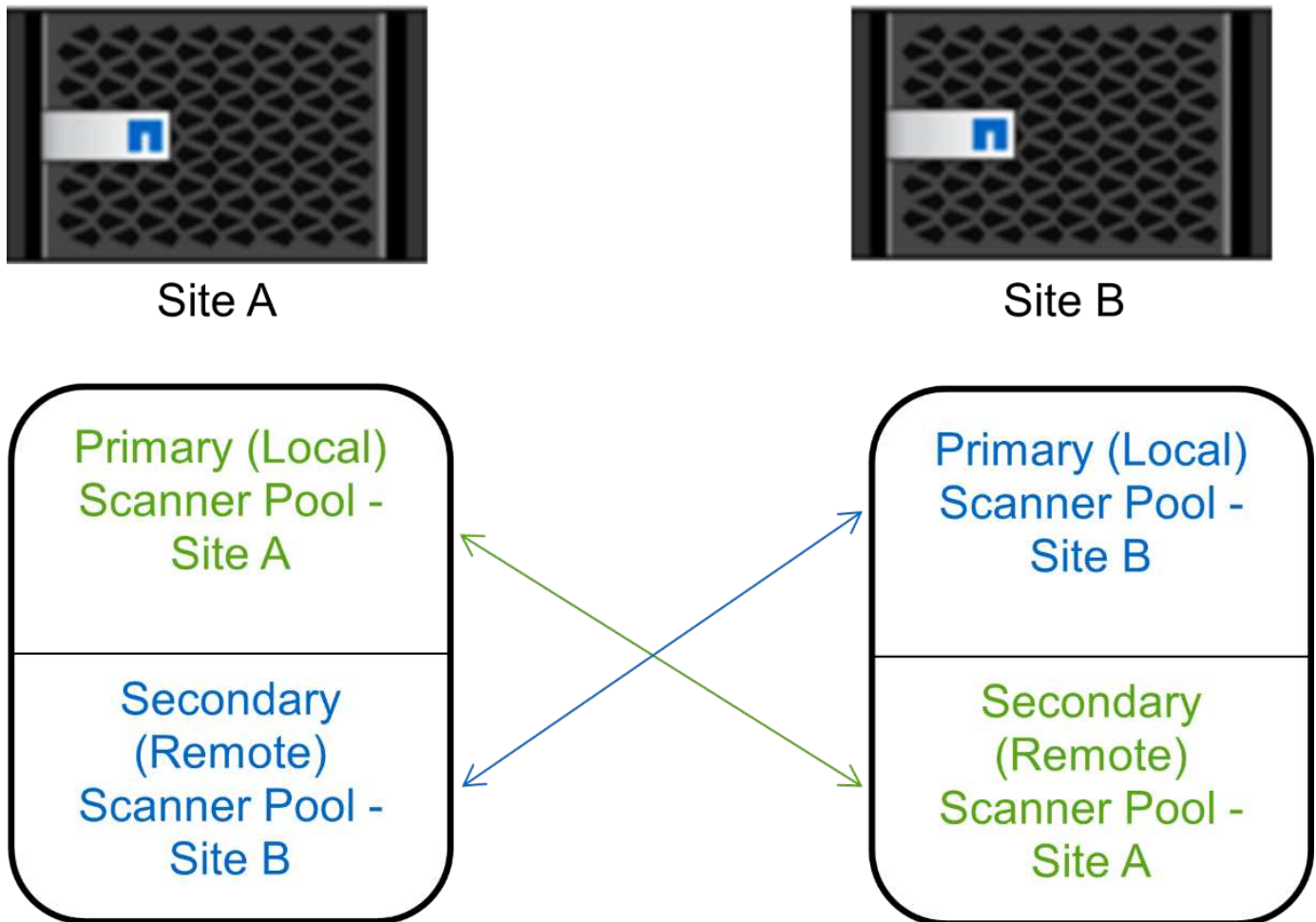
- スキャナプールの設定が完了したら、サーバへの接続ステータスを確認します。

このタスクについて

MetroCluster 構成は、物理的に分離された 2 つのミラークラスタを実装することでデータを保護します。各クラスタが、もう一方のクラスタのデータおよび SVM 設定を同期的にレプリケートします。クラスタがオンラインのときは、ローカルクラスタのプライマリ SVM がデータを提供します。リモートクラスタがオフラインのときは、ローカルクラスタのセカンダリ SVM がデータを提供します。

つまり、MetroCluster構成の各クラスタにプライマリとセカンダリのスキャナプールを作成する必要があり、クラスタがセカンダリSVMからデータの提供を開始すると、セカンダリプールがアクティブになります。ディザスタリカバリ（DR）の設定はMetroClusterと同様です。

この図は、一般的なMetroCluster / DR構成を示しています。



手順

1. スキャナプールを作成します。

```
vserver vscan scanner-pool create -vserver data_SVM|cluster_admin_SVM -scanner
-pool scanner_pool -hostnames Vscan_server_hostnames -privileged-users
privileged_users
```

- 個々の SVM 用のプールの場合はデータ SVM、クラスタ内のすべての SVM 用のプールの場合はクラスタ管理 SVM を指定します。

- 各 Vscan サーバのホスト名には IP アドレスまたは FQDN を指定します。
- 各特権ユーザのドメイン名とユーザ名を指定します。



スキャナプールの作成は、すべてプライマリ SVM を含むクラスタから実行する必要があります。

すべてのオプションの一覧については、コマンドのマニュアルページを参照してください。

次のコマンドは、MetroCluster 構成の各クラスタにプライマリとセカンダリのスキャナプールを作成します。

```
cluster1::> vserver vscan scanner-pool create -vserver cifssvm1 -
scanner-pool pool1_for_site1 -hostnames scan1 -privileged-users cifs
\u1,cifs\u2

cluster1::> vserver vscan scanner-pool create -vserver cifssvm1 -
scanner-pool pool1_for_site2 -hostnames scan1 -privileged-users cifs
\u1,cifs\u2

cluster1::> vserver vscan scanner-pool create -vserver cifssvm1 -
scanner-pool pool2_for_site1 -hostnames scan2 -privileged-users cifs
\u1,cifs\u2

cluster1::> vserver vscan scanner-pool create -vserver cifssvm1 -
scanner-pool pool2_for_site2 -hostnames scan2 -privileged-users cifs
\u1,cifs\u2
```

## 2. スキャナプールが作成されたことを確認します。

```
vserver vscan scanner-pool show -vserver data_SVM|cluster_admin_SVM -scanner
-pool scanner_pool
```

すべてのオプションの一覧については、コマンドのマニュアルページを参照してください。

次のコマンドは、スキャナプールの詳細を表示します pool1 :

```
cluster1::> vserver vscan scanner-pool show -vserver cifssvm1 -scanner
-pool pool1_for_site1
```

```

Vserver: cifssvm1
Scanner Pool: pool1_for_site1
Applied Policy: idle
Current Status: off
Cluster on Which Policy Is Applied: -
Scanner Pool Config Owner: vserver
List of IPs of Allowed Vscan Servers:
List of Host Names of Allowed Vscan Servers: scan1
List of Privileged Users: cifs\u1,cifs\u2
```

を使用することもできます `vserver vscan scanner-pool show` コマンドを使用してSVMのすべてのスキャナプールを表示します。コマンド構文全体については、コマンドのマニュアルページを参照してください。

#### 単一のクラスタにスキャナポリシーを適用する

スキャナポリシーは、スキャナプールがアクティブかどうかを決定します。スキャナプールが定義するVscanサーバがSVMに接続できるようにするには、スキャナプールをアクティブ化する必要があります。

#### このタスクについて

- 1つのスキャナプールに適用できるスキャナポリシーは1つだけです。
- クラスタ内のすべてのSVM用のスキャナプールを作成した場合は、各SVMにスキャナポリシーを個別に適用する必要があります。

#### 手順

1. スキャナポリシーを適用します。

```
vserver vscan scanner-pool apply-policy -vserver data_SVM -scanner-pool
scanner_pool -scanner-policy primary|secondary|idle -cluster
cluster_to_apply_policy_on
```

スキャナポリシーには次のいずれかの値が設定されます。

- Primary スキャナプールをアクティブにします。
- Secondary プライマリスキャナプールのVscanサーバが1つも接続されていない場合にのみスキャナプールをアクティブにします。
- Idle スキャナプールを非アクティブにします。

次の例は、というスキャナプールを示しています SP をクリックします vs1 SVMがアクティブ：

```
cluster1::> vserver vscan scanner-pool apply-policy -vserver vs1
-scanner-pool SP -scanner-policy primary
```

## 2. スキャナプールがアクティブであることを確認します。

```
vserver vscan scanner-pool show -vserver data_SVM|cluster_admin_SVM -scanner
-pool scanner_pool
```

すべてのオプションの一覧については、コマンドのマニュアルページを参照してください。

次のコマンドは、の詳細を表示します SP スキャナプール：

```
cluster1::> vserver vscan scanner-pool show -vserver vs1 -scanner-pool
SP

Vserver: vs1
Scanner Pool: SP
Applied Policy: primary
Current Status: on
Cluster on Which Policy Is Applied: cluster1
Scanner Pool Config Owner: vserver
List of IPs of Allowed Vscan Servers: 1.1.1.1, 10.72.204.27
List of Host Names of Allowed Vscan Servers: 1.1.1.1, vmwin204-
27.fsct.nb
List of Privileged Users: cifs\u1, cifs\u2
```

を使用できます `vserver vscan scanner-pool show-active` コマンドを使用して、SVMのアクティブなスキャナプールを表示します。コマンド構文全体については、コマンドのマニュアルページを参照してください。

## MetroCluster 構成でスキャナポリシーを適用

スキャナポリシーは、スキャナプールがアクティブかどうかを決定します。MetroCluster 構成では、各クラスタのプライマリとセカンダリのスキャナプールにスキャナポリシーを適用する必要があります。

このタスクについて

- 1つのスキャナプールに適用できるスキャナポリシーは1つだけです。
- クラスタ内のすべてのSVM用のスキャナプールを作成した場合は、各SVMにスキャナポリシーを個別に適用する必要があります。
- ディザスタリカバリおよびMetroCluster構成では、ローカルクラスタとリモートクラスタ内のすべてのスキャナプールにスキャナポリシーを適用する必要があります。
- ローカルクラスタ用に作成するポリシーでは、でローカルクラスタを指定する必要があります `cluster` パラメータリモートクラスタ用に作成するポリシーでは、 `cluster` パラメータこれにより、災害発生時

にリモートクラスタがウィルススキャン処理をテイクオーバーできるようになります。

## 手順

### 1. スキャナポリシーを適用します。

```
vserver vscan scanner-pool apply-policy -vserver data_SVM -scanner-pool  
scanner_pool -scanner-policy primary|secondary|idle -cluster  
cluster_to_apply_policy_on
```

スキャナポリシーには次のいずれかの値が設定されます。

- Primary スキャナプールをアクティブにします。
- Secondary プライマリスキャナプールのVscanサーバが1つも接続されていない場合にのみスキャナプールをアクティブにします。
- Idle スキャナプールを非アクティブにします。



スキャナポリシーの適用は、すべてプライマリ SVM を含むクラスタから実行する必要があります。

次のコマンドは、MetroCluster 構成の各クラスタのプライマリとセカンダリのスキャナプールにスキャナポリシーを適用します。

```
cluster1::>vserver vscan scanner-pool apply-policy -vserver cifssvm1  
-scanner-pool pool1_for_site1 -scanner-policy primary -cluster cluster1  
  
cluster1::>vserver vscan scanner-pool apply-policy -vserver cifssvm1  
-scanner-pool pool2_for_site1 -scanner-policy secondary -cluster  
cluster1  
  
cluster1::>vserver vscan scanner-pool apply-policy -vserver cifssvm1  
-scanner-pool pool1_for_site2 -scanner-policy primary -cluster cluster2  
  
cluster1::>vserver vscan scanner-pool apply-policy -vserver cifssvm1  
-scanner-pool pool2_for_site2 -scanner-policy secondary -cluster  
cluster2
```

### 2. スキャナプールがアクティブであることを確認します。

```
vserver vscan scanner-pool show -vserver data_SVM|cluster_admin_SVM -scanner  
-pool scanner_pool
```

すべてのオプションの一覧については、コマンドのマニュアルページを参照してください。

次のコマンドは、スキャナプールの詳細を表示します pool1：

```

cluster1::> vserver vscan scanner-pool show -vserver cifssvm1 -scanner
-pool pool1_for_site1

Vserver: cifssvm1
Scanner Pool: pool1_for_site1
Applied Policy: primary
Current Status: on
Cluster on Which Policy Is Applied: cluster1
Scanner Pool Config Owner: vserver
List of IPs of Allowed Vscan Servers:
List of Host Names of Allowed Vscan Servers: scan1
List of Privileged Users: cifs\u1,cifs\u2

```

を使用できます `vserver vscan scanner-pool show-active` コマンドを使用して、SVMのアクティブなスキャナプールを表示します。コマンド構文全体については、コマンドのマニュアルページを参照してください。

## スキャナプールの管理用コマンド

スキャナプールを変更および削除し、スキャナプールの特権ユーザと Vscan サーバを管理できます。また、スキャナプールに関する概要情報を確認することもできます。

状況	入力するコマンド
スキャナプールを変更	<code>vserver vscan scanner-pool modify</code>
スキャナプールを削除します	<code>vserver vscan scanner-pool delete</code>
スキャナプールに特権ユーザを追加する	<code>vserver vscan scanner-pool privileged-users add</code>
スキャナプールから特権ユーザを削除します	<code>vserver vscan scanner-pool privileged-users remove</code>
スキャナプールに Vscan サーバを追加する	<code>vserver vscan scanner-pool servers add</code>
スキャナプールから Vscan サーバを削除します	<code>vserver vscan scanner-pool servers remove</code>
スキャナプールの概要と詳細を表示します	<code>vserver vscan scanner-pool show</code>
スキャナプールの特権ユーザを表示します	<code>vserver vscan scanner-pool privileged-users show</code>

すべてのスキャナプールの Vscan サーバを表示します	<code>vserver vscan scanner-pool servers show</code>
------------------------------	--

これらのコマンドの詳細については、マニュアルページを参照してください。

## オンアクセススキャンを設定します

オンアクセスポリシーを作成します

オンアクセスポリシーはオンアクセススキャンの範囲を定義します。オンアクセスポリシーは、個々の SVM 用またはクラスタ内のすべての SVM 用に作成できます。クラスタ内のすべての SVM 用のオンアクセスポリシーを作成した場合は、各 SVM でポリシーを個別に有効にする必要があります。

このタスクについて

- スキャンする最大ファイルサイズ、スキャンに含めるファイル拡張子とパス、およびスキャンから除外するファイル拡張子とパスを指定できます。
- を設定できます `scan-mandatory` オフにすると、ウィルススキャンに使用できるVscanサーバがない場合にファイルアクセスが許可されます。
- デフォルトでは、ONTAPは「default\_cifs」という名前のオンアクセスポリシーを作成し、クラスタ内のすべてのSVMに対して有効にします。
- に基づいてスキャン除外の対象となるすべてのファイル `paths-to-exclude`、`file-ext-to-exclude` または `max-file-size` パラメータは、`scan-mandatory` オプションがonに設定されている。（これをチェックしてください "[トラブルシューティング](#)" セクションに関連する接続の問題 `scan-mandatory` オプション）
- デフォルトでは、読み取り / 書き込みボリュームのみがスキャンされます。読み取り専用ボリュームのスキャンを有効にするフィルタや、実行アクセス権で開かれたファイルのみにスキャンを制限するフィルタを指定することができます。
- `continuously-available` パラメータがYesに設定されているSMB共有ではウィルススキャンは実行されません。
- を参照してください "[ウィルス対策アーキテクチャ](#)" セクションで、`_vscan` ファイル処理プロファイルの詳細を確認してください。
- SVMごとに最大10個のオンアクセスポリシーを作成できます。ただし、一度に有効にできるオンアクセスポリシーは1つだけです。
  - オンアクセスポリシーでは、最大100個のパスとファイル拡張子をウィルススキャンの対象から除外できます。
- ファイル除外の推奨事項：
  - 大容量ファイル（ファイルサイズを指定可能）は、CIFSユーザの応答に時間がかかるか、スキャン要求がタイムアウトする可能性があるため、ウィルススキャンの対象から除外することを検討してください。除外するデフォルトのファイルサイズは2GBです。
  - 次のようなファイル拡張子を除外することを検討 `.vhd` および `.tmp` これらの拡張子を持つファイルはスキャンに適していない可能性があるためです。
  - 隔離ディレクトリなどのファイルパスや、仮想ハードドライブまたはデータベースのみが格納されているパスを除外することを検討してください。

。一度に有効にできるポリシーは1つだけであるため、すべての除外が同じポリシーに指定されていることを確認します。NetAppでは、アンチウイルスエンジンで指定されているのと同じ除外を設定することを強く推奨します。

- ・ オンアクセスポリシーは、 [オンデマンドスキャン](#)。のオンアクセススキャンを回避するには、 `-scan-files-with-no-ext` を `false` に設定し、 `-file-ext-to-exclude` すべての拡張子を除外するには、を指定します。

## 手順

### 1. オンアクセスポリシーを作成します。

```
vserver vscan on-access-policy create -vserver data_SVM|cluster_admin_SVM
-policy-name policy_name -protocol CIFS -max-file-size
max_size_of_files_to_scan -filters [scan-ro-volume,][scan-execute-access]
-file-ext-to-include extensions_of_files_to_include -file-ext-to-exclude
extensions_of_files_to_exclude -scan-files-with-no-ext true|false -paths-to
exclude paths_of_files_to_exclude -scan-mandatory on|off
```

。 個々の SVM 用のポリシーの場合はデータ SVM、クラスタ内のすべての SVM 用のポリシーの場合はクラスタ管理 SVM を指定します。

。 -file-ext-to-exclude を設定すると、が上書きされます -file-ext-to-include 設定：

。 設定 -scan-files-with-no-ext true に設定すると、拡張子のないファイルがスキャンされます。次のコマンドは、という名前のオンアクセスポリシーを作成します Policy1 をクリックします vs1 SVM：

```
cluster1::> vserver vscan on-access-policy create -vserver vs1 -policy
-name Policy1 -protocol CIFS -filters scan-ro-volume -max-file-size 3GB
-file-ext-to-include "mp*", "tx*" -file-ext-to-exclude "mp3", "txt" -scan
-files-with-no-ext false -paths-to-exclude "\\vol\ a b\\", "\\vol\ a, b\\"
```

### 2. オンアクセスポリシーが作成されたことを確認します。 `vserver vscan on-access-policy show -instance data_SVM|cluster_admin_SVM -policy-name name`

すべてのオプションの一覧については、コマンドのマニュアルページを参照してください。

次のコマンドは、の詳細を表示します Policy1 ポリシー：



```
cluster1::> vserver vscan on-access-policy show -instance vs1 -policy
-name Policy1
```

```

Vserver: vs1
Policy: Policy1
Policy Status: off
Policy Config Owner: vserver
File-Access Protocol: CIFS
Filters: scan-ro-volume
Mandatory Scan: on
Max File Size Allowed for Scanning: 3GB
File Paths Not to Scan: \vol\ a b\, \vol\ a,b\
File Extensions Not to Scan: mp3, txt
File Extensions to Scan: mp*, tx*
Scan Files with No Extension: false
```

オンアクセスポリシーを有効にします

オンアクセスポリシーはオンアクセススキャンの範囲を定義します。SVM のファイルをスキャンするには、その SVM でオンアクセスポリシーを有効にする必要があります。

クラスタ内のすべての SVM 用のオンアクセスポリシーを作成した場合は、各 SVM でポリシーを個別に有効にする必要があります。SVM で一度に有効にできるオンアクセスポリシーは 1 つだけです。

手順

1. オンアクセスポリシーを有効にします。

```
vserver vscan on-access-policy enable -vserver data_SVM -policy-name
policy_name
```

次のコマンドは、という名前のオンアクセスポリシーを有効にします Policy1 をクリックします vs1 SVM :

```
cluster1::> vserver vscan on-access-policy enable -vserver vs1 -policy
-name Policy1
```

2. オンアクセスポリシーが有効になっていることを確認します。

```
vserver vscan on-access-policy show -instance data_SVM -policy-name
policy_name
```

すべてのオプションの一覧については、コマンドのマニュアルページを参照してください。

次のコマンドは、の詳細を表示します Policy1 オンアクセスポリシー :

```
cluster1::> vserver vscan on-access-policy show -instance vs1 -policy
-name Policy1
```

```

Vserver: vs1
Policy: Policy1
Policy Status: on
Policy Config Owner: vserver
File-Access Protocol: CIFS
Filters: scan-ro-volume
Mandatory Scan: on
Max File Size Allowed for Scanning: 3GB
File Paths Not to Scan: \vol\ a b\, \vol\ a,b\
File Extensions Not to Scan: mp3, txt
File Extensions to Scan: mp*, tx*
Scan Files with No Extension: false
```

### SMB 共有の Vscan ファイル処理プロファイルを変更します

SMB共有の\_vscanファイル処理プロファイル\_は、スキャンをトリガーできる共有に対する処理を定義します。デフォルトでは、パラメータはに設定されています standard。このパラメータは、SMB 共有を作成または変更するときに必要に応じて調整できます。

を参照してください ["ウィルス対策アーキテクチャ"](#) セクションで、\_vscanファイル処理プロファイル\_の詳細を確認してください。



が含まれているSMB共有ではウィルススキャンは実行されません。 continuously-available パラメータをに設定します Yes。

### ステップ

1. SMB共有のVscanファイル処理プロファイルの値を変更します。

```
vserver cifs share modify -vserver data_SVM -share-name share -path share_path
-vscan-fileop-profile no-scan|standard|strict|writes-only
```

すべてのオプションの一覧については、コマンドのマニュアルページを参照してください。

次のコマンドは、SMB共有のVscanファイル処理プロファイルをに変更します。 strict :

```
cluster1::> vserver cifs share modify -vserver vs1 -share-name
SALES_SHARE -path /sales -vscan-fileop-profile strict
```

## オンアクセスポリシーを管理するためのコマンド

オンアクセスポリシーは変更、無効化、または削除できます。ポリシーの概要と詳細を表示できます。

状況	入力するコマンド
オンアクセスポリシーを作成します	<code>vserver vscan on-access-policy create</code>
オンアクセスポリシーを変更する	<code>vserver vscan on-access-policy modify</code>
オンアクセスポリシーを有効にします	<code>vserver vscan on-access-policy enable</code>
オンアクセスポリシーを無効にします	<code>vserver vscan on-access-policy disable</code>
オンアクセスポリシーを削除する	<code>vserver vscan on-access-policy delete</code>
オンアクセスポリシーの概要と詳細を表示します	<code>vserver vscan on-access-policy show</code>
対象から除外するパスをリストに追加します	<code>vserver vscan on-access-policy paths-to-exclude add</code>
対象から除外するパスをリストから削除します	<code>vserver vscan on-access-policy paths-to-exclude remove</code>
対象から除外するパスのリストを表示します	<code>vserver vscan on-access-policy paths-to-exclude show</code>
対象から除外するファイル拡張子をリストに追加します	<code>vserver vscan on-access-policy file-ext-to-exclude add</code>
対象から除外するファイル拡張子をリストから削除します	<code>vserver vscan on-access-policy file-ext-to-exclude remove</code>
対象から除外するファイル拡張子のリストを表示します	<code>vserver vscan on-access-policy file-ext-to-exclude show</code>
対象に含めるファイル拡張子をリストに追加します	<code>vserver vscan on-access-policy file-ext-to-include add</code>
対象に含めるファイル拡張子をリストから削除します	<code>vserver vscan on-access-policy file-ext-to-include remove</code>
対象に含めるファイル拡張子のリストを表示します	<code>vserver vscan on-access-policy file-ext-to-include show</code>

これらのコマンドの詳細については、マニュアルページを参照してください。

## オンデマンドスキャンを設定する

### オンデマンドスキャンの概要を設定する

オンデマンドスキャンを使用すると、ファイルのウィルスチェックをただちにまたはスケジュールに基づいて実行できます。

たとえば、ピーク時を避けてスキャンを実行する場合や、オンアクセススキャンの対象外の大容量ファイルのスキャンを実行する場合などに便利です。cronスケジュールを使用して、タスクを実行するタイミングを指定できます。

### このトピックについて

- スケジュールはタスクの作成時に割り当てることができます。
- SVM で同時にスケジュールできるタスクは1つだけです。
- オンデマンドスキャンでは、シンボリックリンクやストリームファイルのスキャンはサポートされません。



オンデマンドスキャンでは、シンボリックリンクやストリームファイルのスキャンはサポートされません。



オンデマンドタスクを作成するには、少なくとも1つのオンアクセスポリシーを有効にする必要があります。デフォルトポリシーまたはユーザが作成したオンアクセスポリシーを使用できます。

### オンデマンドタスクを作成する

オンデマンドタスクは、オンデマンドウィルススキャンの範囲を定義します。スキャンするファイルの最大サイズ、スキャン対象に含めるファイルの拡張子とパス、およびスキャン対象から除外するファイルの拡張子とパスを指定できます。デフォルトでは、サブディレクトリ内のファイルがスキャンされます。

### このタスクについて

- SVMごとに最大10個のオンデマンドタスクを作成できますが、アクティブにできるのは1つだけです。
- オンデマンドタスクは、スキャンに関連する統計情報を含むレポートを作成します。このレポートには、コマンドを使用するか、タスクによって作成されたレポートファイルを定義された場所にダウンロードしてアクセスできます。

### 作業を開始する前に

- が必要です [オンアクセスポリシーを作成しました。](#)。デフォルトのポリシーでもユーザが作成したポリシーでもかまいません。オンアクセスポリシーがないと、スキャンを有効にできません。

### 手順

1. オンデマンドタスクを作成します。

```
vserver vscan on-demand-task create -vserver data_SVM -task-name task_name
```

```
-scan-paths paths_of_files_to_scan -report-directory report_directory_path  
-report-expiry-time expiration_time_for_report -schedule cron_schedule -max  
-file-size max_size_of_files_to_scan -paths-to-exclude paths -file-ext-to  
-exclude file_extensions -file-ext-to-include file_extensions -scan-files-with  
-no-ext true|false -directory-recursion true|false
```

- °。 -file-ext-to-exclude を設定すると、が上書きされます -file-ext-to-include 設定：
- ° 設定 -scan-files-with-no-ext trueに設定すると、拡張子のないファイルがスキャンされます。

すべてのオプションの一覧については、を参照してください。 ["コマンドリファレンス"](#)。

次のコマンドは、という名前のオンデマンドタスクを作成します。 Task1 vs1 VMで次の手順を実行します。

```
cluster1::> vsserver vscan on-demand-task create -vsserver vs1 -task-name  
Task1 -scan-paths "/vol1/", "/vol2/cifs/" -report-directory "/report"  
-schedule daily -max-file-size 5GB -paths-to-exclude "/vol1/cold-files/"  
-file-ext-to-include "vmdk?", "mp*" -file-ext-to-exclude "mp3", "mp4"  
-scan-files-with-no-ext false  
[Job 126]: Vscan On-Demand job is queued. Use the "job show -id 126"  
command to view the status.
```

+



を使用できます job show コマンドを使用してジョブのステータスを表示します。を使用  
できます job pause および job resume ジョブを一時停止および再開するコマンド、ま  
たは job stop コマンドを使用してジョブを終了します。

## 2. オンデマンドタスクが作成されたことを確認します。

```
vsserver vscan on-demand-task show -instance data_SVM -task-name task_name
```

すべてのオプションの一覧については、コマンドのマニュアルページを参照してください。

次のコマンドは、の詳細を表示します Task1 タスク：

```
cluster1::> vserver vscan on-demand-task show -instance vs1 -task-name Task1

Vserver: vs1
Task Name: Task1
List of Scan Paths: /vol1/, /vol2/cifs/
Report Directory Path: /report
Job Schedule: daily
Max File Size Allowed for Scanning: 5GB
File Paths Not to Scan: /vol1/cold-files/
File Extensions Not to Scan: mp3, mp4
File Extensions to Scan: vmdk?, mp*
Scan Files with No Extension: false
Request Service Timeout: 5m
Cross Junction: true
Directory Recursion: true
Scan Priority: low
Report Log Level: info
Expiration Time for Report: -
```

完了後

タスクの実行をスケジュールする前に、SVM でスキャンを有効にする必要があります。

オンデマンドタスクのスケジュールを設定します

スケジュールを割り当てずにタスクを作成し、`vserver vscan on-demand-task schedule` コマンドを使用してスケジュールを割り当てるか、タスクの作成時にスケジュールを追加します。

このタスクについて

で割り当てられたスケジュール `vserver vscan on-demand-task schedule` このコマンドは、ですすでに割り当てられているスケジュールを上書きします `vserver vscan on-demand-task create` コマンドを実行します

手順

1. オンデマンドタスクのスケジュールを設定します。

```
vserver vscan on-demand-task schedule -vserver data_SVM -task-name task_name -schedule cron_schedule
```

次のコマンドは、という名前のオンアクセスタスクをスケジュールします Task2 をクリックします vs2 SVM :

```
cluster1::> vserver vscan on-demand-task schedule -vserver vs2 -task
-name Task2 -schedule daily
[Job 142]: Vscan On-Demand job is queued. Use the "job show -id 142"
command to view the status.
```

ジョブのステータスを表示するには、`job show` コマンドを実行します。`job pause` および `job resume` ジョブをそれぞれ一時停止および再開するコマンド。`job stop` コマンドを実行すると、ジョブが終了します。

## 2. オンデマンドタスクがスケジュールされていることを確認します。

```
vserver vscan on-demand-task show -instance data_SVM -task-name task_name
```

すべてのオプションの一覧については、コマンドのマニュアルページを参照してください。

次のコマンドは、の詳細を表示します Task 2 タスク：

```
cluster1::> vserver vscan on-demand-task show -instance vs2 -task-name
Task2

Vserver: vs2
Task Name: Task2
List of Scan Paths: /vol1/, /vol2/cifs/
Report Directory Path: /report
Job Schedule: daily
Max File Size Allowed for Scanning: 5GB
File Paths Not to Scan: /vol1/cold-files/
File Extensions Not to Scan: mp3, mp4
File Extensions to Scan: vmdk, mp*
Scan Files with No Extension: false
Request Service Timeout: 5m
Cross Junction: true
Directory Recursion: true
Scan Priority: low
Report Log Level: info
```

完了後

タスクの実行をスケジュールする前に、SVM でスキャンを有効にする必要があります。

オンデマンドタスクをただちに実行します

オンデマンドタスクは、スケジュールが割り当てられているかどうかに関係なく、ただちに実行することもできます。

作業を開始する前に

SVM でスキャンを有効にしておく必要があります。


ステップ

1. オンデマンドタスクをただちに実行します。

```
vserver vscan on-demand-task run -vserver data_SVM -task-name task_name
```

次のコマンドは、という名前のオンアクセスタスクを実行します Task1 をクリックします vs1 SVM :

```
cluster1::> vserver vscan on-demand-task run -vserver vs1 -task-name Task1
[Job 161]: Vscan On-Demand job is queued. Use the "job show -id 161" command to view the status.
```



を使用できます job show コマンドを使用してジョブのステータスを表示します。を使用  
できます job pause および job resume ジョブを一時停止および再開するコマンド、ま  
たは job stop コマンドを使用してジョブを終了します。

オンデマンドタスクを管理するためのコマンドです

オンデマンドタスクを変更、削除、またはスケジュールを解除できます。タスクの概要  
と詳細を表示し、タスクのレポートを管理できます。

状況	入力するコマンド
オンデマンドタスクを作成する	vserver vscan on-demand-task create
オンデマンドタスクを変更する	vserver vscan on-demand-task modify
オンデマンドタスクを削除する	vserver vscan on-demand-task delete
オンデマンドタスクを実行する	vserver vscan on-demand-task run
オンデマンドタスクのスケジュールを設定します	vserver vscan on-demand-task schedule
オンデマンドタスクのスケジュールを解除します	vserver vscan on-demand-task unschedule
オンデマンドタスクの概要と詳細を表示する	vserver vscan on-demand-task show
オンデマンドレポートを表示します	vserver vscan on-demand-task report show
オンデマンドレポートを削除する	vserver vscan on-demand-task report delete



これらのコマンドの詳細については、マニュアルページを参照してください。

## ONTAPで外部接続式のウィルス対策機能を設定するためのベストプラクティス

ONTAPでオフボックス機能を設定する場合は、次の推奨事項を考慮してください。

- 特権ユーザのウィルススキャン処理を制限します。通常のユーザは、特権ユーザクレデンシャルを使用しないでください。この制限は、Active Directoryの特権ユーザのログイン権限を無効にすることで実現できます。
- AdministratorsグループやBackup Operatorsグループなど、ドメイン内で多数の権限を持つユーザグループには、特権ユーザを含める必要はありません。特権ユーザは、Vscanサーバ接続の確立およびウィルススキャン用ファイルへのアクセスを許可するために、ストレージシステムでのみ検証する必要があります。
- Vscanサーバを実行しているコンピュータは、ウィルススキャンの目的でのみ使用してください。一般的な使用を避けるには、これらのマシンのWindowsターミナルサービスおよびその他のリモートアクセスプロビジョニングを無効にし、これらのマシンに新しいソフトウェアをインストールする権利を管理者のみに付与します。
- Vscanサーバはウィルススキャン専用にし、バックアップなどの他の処理には使用しないでください。Vscanサーバを仮想マシン（VM）として実行することもできます。VscanサーバをVMとして実行する場合は、VMに割り当てられているリソースが共有されておらず、ウィルススキャンを実行するのに十分であることを確認してください。
- Vscanサーバに適切なCPU、メモリ、およびディスク容量を提供して、リソースの過剰割り当てを回避します。ほとんどのVscanサーバは、複数のCPUコアサーバを使用してCPU間で負荷を分散するように設計されています。
- SVMからVscanサーバへの接続には、スキャントラフィックが他のクライアントネットワークトラフィックの影響を受けないように、専用ネットワークとプライベートVLANを使用することを推奨します。NetApp Vscanサーバ上のウィルス対策VLAN専用およびSVM上のデータLIF専用の、独立したネットワークインターフェイスカード（NIC）を作成します。この手順により、ネットワークの問題が発生した場合の管理とトラブルシューティングが簡単になります。アンチウイルストラフィックは、プライベートネットワークを使用して分離する必要があります。ウィルス対策サーバは、次のいずれかの方法でドメインコントローラ（DC）およびONTAPと通信するように設定する必要があります。
  - DCは、トラフィックの分離に使用されるプライベートネットワークを介してアンチウイルスサーバと通信する必要があります。
  - DCサーバとウィルス対策サーバは、CIFSクライアントネットワークとは異なる別のネットワーク（前述のプライベートネットワークではない）を介して通信する必要があります。
  - ウィルス対策通信でKerberos認証を有効にするには、プライベートLIF用のDNSエントリと、プライベートLIF用に作成したDNSエントリに対応するサービスプリンシパル名をDC上に作成します。この名前は、Antivirus ConnectorにLIFを追加するときに使用します。DNSは、Antivirus Connectorに接続されている各プライベートLIFに対して一意の名前を返すことができる必要があります。



Vscanトラフィック用のLIFがクライアントトラフィック用のLIFとは別のポートに設定されている場合、ポート障害が発生したときにVscan LIFが別のノードにフェイルオーバーする可能性があります。変更によって新しいノードからVscanサーバに到達できなくなり、ノード上のファイル処理に関するスキャン通知が失敗します。ノード上の少なくとも1つのLIFを介してVscanサーバにアクセスできることを確認し、そのノードで実行されたファイル処理のスキャン要求を処理できるようにします。

- 少なくとも1GbEネットワークを使用して、NetAppストレージシステムとVscanサーバを接続します。

- 複数のVscanサーバがある環境では、同様の高パフォーマンスネットワーク接続があるすべてのサーバを接続します。Vscanサーバを接続すると、負荷を分散できるためパフォーマンスが向上します。
- リモートサイトやブランチオフィスには、NetAppではリモートのVscanサーバではなくローカルのVscanサーバを使用することを推奨します。これは、Vscanサーバが高レイテンシの場合に最適なサーバであるためです。コストが要因の場合は、中程度のウイルス保護のためにラップトップまたはPCを使用してください。ボリュームまたはqtreeを共有し、リモートサイトの任意のシステムからスキャンすることで、ファイルシステム全体の定期的なスキャンをスケジュールできます。
- 複数のVscanサーバを使用してSVM上のデータをスキャンし、ロードバランシングと冗長性を確保します。CIFSワークロードとその結果のウイルス対策トラフィックの量は、SVMごとに異なります。ストレージコントローラでCIFSとウイルススキャンのレイテンシを監視します。時間の経過に伴う結果の傾向を監視します。VscanサーバのCPUキューやアプリケーションキューが原因でCIFSのレイテンシやウイルススキャンのレイテンシがトレンドのしきい値を超えて上昇すると、CIFSクライアントの待機時間が長くなることがあります。Vscanサーバを追加する負荷を分散するため。
- 最新バージョンのONTAP Antivirus Connectorをインストールします。
- ウィルス対策エンジンと定義を最新の状態に維持します。更新頻度に関する推奨事項については、パートナーにお問い合わせください。
- マルチテナンシー環境では、VscanサーバとSVMが同じドメインまたは信頼されたドメインに属している場合は、スキャナプール（Vscanサーバのプール）を複数のSVMで共有できます。
- 感染したファイルのウイルス対策ソフトウェアポリシーは、ほとんどのウイルス対策ベンダーで設定されているデフォルト値である「delete」または「quarantine」に設定する必要があります。「vscan-fileop-profile」が「write\_only」に設定されていて、感染したファイルが見つかった場合、ファイルは共有に残り、ファイルを開いてもスキャンはトリガーされないため開くことができます。アンチウイルススキャンは、ファイルが閉じられた後にのみトリガーされます。
- scan-engine timeout 値は次の値より小さくする必要があります： scanner-pool request-timeout 価値。  
この値を大きい値に設定すると、ファイルへのアクセスに遅延が生じ、最終的にタイムアウトする可能性があります。  
これを回避するには、scan-engine timeout 5秒未満 scanner-pool request-timeout 価値。の変更方法については、スキャンエンジンベンダーのマニュアルを参照してください。scan-engine timeout 設定：。scanner-pool timeout 次のコマンドをアドバンスモードで使用し、request-timeout パラメータ：  
vserver vscan scanner-pool modify。
- オンアクセススキャンのワークロード向けにサイジングされていて、オンデマンドスキャンの使用が必要な環境では、NetAppでは、既存のウイルス対策インフラへの負荷の増大を避けるために、オンデマンドスキャンジョブをオフピークの時間帯にスケジュールすることを推奨しています。

パートナー様固有のベストプラクティスの詳細については、"[Vscanパートナーソリューション](#)"。

## SVM でウイルススキャンを有効にします

オンアクセススキャンまたはオンデマンドスキャンを実行するには、SVM でウイルススキャンを有効にする必要があります。

### 手順

1. SVM でウイルススキャンを有効にします。

```
vserver vscan enable -vserver data_SVM
```



を使用できます `vserver vscan disable` ウィルススキャンを無効にするコマンド（必要な場合）。

次のコマンドは、でウィルススキャンを有効にします `vs1` SVM：

```
cluster1::> vserver vscan enable -vserver vs1
```

2. SVM でウィルススキャンが有効になっていることを確認します。

```
vserver vscan show -vserver data_SVM
```

すべてのオプションの一覧については、コマンドのマニュアルページを参照してください。

次のコマンドは、のVscanステータスを表示します `vs1` SVM：

```
cluster1::> vserver vscan show -vserver vs1
```

```
Vserver: vs1
Vscan Status: on
```

## スキャン済みファイルのステータスをリセットします

SVMでスキャンに成功したファイルのスキャンステータスををを使用してリセットすることもできます `vserver vscan reset` コマンドを使用して、ファイルのキャッシュされた情報を破棄します。このコマンドを使用すると、たとえばスキャン設定に誤りがあった場合にウィルススキャン処理を再開できます。

このタスクについて

を実行したあと `vserver vscan reset` コマンドを実行すると、対象となるすべてのファイルが次回アクセスされたときにスキャンされます。



このコマンドを使用すると、再スキャンするファイルの数やサイズによっては、パフォーマンスが低下する可能性があります。

必要なもの

このタスクを実行するには `advanced` 権限が必要です。

手順

1. `advanced` 権限レベルに切り替えます。

```
set -privilege advanced
```

2. スキャン済みファイルのステータスをリセットします。

```
vserver vscan reset -vserver data_SVM
```

次のコマンドは、のスキャン済みファイルのステータスをリセットします vs1 SVM：

```
cluster1::> vserver vscan reset -vserver vs1
```

## Vscan イベントログ情報を表示します

使用できます `vserver vscan show-events` コマンドを使用して、感染したファイル、Vscanサーバの更新などに関するイベントログ情報を表示します。クラスタ、特定のノード、SVM、またはVscanサーバについてのイベント情報を表示できます。

作業を開始する前に

Vscanイベントログを表示するにはadvanced権限が必要です。

手順

1. advanced 権限レベルに切り替えます。

```
set -privilege advanced
```

2. Vscan イベントログ情報を表示します。

```
vserver vscan show-events
```

すべてのオプションの一覧については、コマンドのマニュアルページを参照してください。

次のコマンドは、クラスタのイベントログ情報を表示します cluster1：

```
cluster1::*> vserver vscan show-events
```

Vserver	Node	Server	Event Type	Event Time
vs1	Cluster-01	192.168.1.1	file-infected	9/5/2014 11:37:38
vs1	Cluster-01	192.168.1.1	scanner-updated	9/5/2014 11:37:08
vs1	Cluster-01	192.168.1.1	scanner-connected	9/5/2014 11:34:55

3 entries were displayed.

## 接続の問題の監視とトラブルシューティング

**scan-mandatory** オプションの使用時に発生する可能性がある接続の問題

使用できます `vserver vscan connection-status show` 接続の問題のトラブル

シューティングに役立つVscanサーバ接続に関する情報を表示するコマンド。

デフォルトでは、が表示されます `scan-mandatory` オンアクセススキャンのオプションを指定すると、Vscanサーバ接続をスキャンに使用できない場合にファイルアクセスが拒否されます。このオプションは重要な安全機能を備えていますが、いくつかの状況で問題が発生する可能性があります。

- ・クライアントアクセスを有効にする前に、LIF が設定された各ノードの SVM に少なくとも 1 つの Vscan サーバが接続されていることを確認する必要があります。クライアントアクセスを有効にしたあとにサーバをSVMに接続する必要がある場合は、をオフにする必要があります `scan-mandatory` オプションを使用して、Vscanサーバ接続を使用できないためにファイルアクセスが拒否されないようにします。サーバの接続が完了したら、オプションをオンに戻すことができます。
- ・1 つのターゲット LIF で SVM のすべての Vscan サーバ接続をホストしている場合、その LIF を移行するとサーバと SVM の間の接続が失われます。Vscanサーバ接続を使用できないためにファイルアクセスが拒否されないようにするには、をオフにする必要があります `scan-mandatory` オプションを選択してください。LIF の移行が完了したら、オプションをオンに戻すことができます。

各 SVM に少なくとも 2 つの Vscan サーバを割り当てる必要があります。ストレージシステムへの Vscan サーバの接続には、クライアントアクセスとは別のネットワークを使用することを推奨します。

#### Vscan サーバの接続ステータスを表示するコマンド

を使用できます `vserver vscan connection-status show` Vscanサーバの接続ステータスに関する概要と詳細情報を表示するコマンド。

状況	入力するコマンド
Vscan サーバ接続の概要を表示します	<code>vserver vscan connection-status show</code>
Vscan サーバ接続の詳細を表示します	<code>vserver vscan connection-status show-all</code>
接続されている Vscan サーバの詳細を表示します	<code>vserver vscan connection-status show-connected</code>
接続されていない使用可能な Vscan サーバの詳細を表示します	<code>vserver vscan connection-status show-not-connected</code>

これらのコマンドの詳細については、を参照してください ["ONTAP のマニュアルページ"](#)。

#### ウィルススキャンのトラブルシューティング

一般的なウィルススキャンの問題については、考えられる原因と解決方法があります。ウィルススキャンはVscanとも呼ばれます。

問題	解決方法
----	------

Vscanサーバがに接続できない clustered ONTAPストレージシステム。	スキャナプールの設定でVscanサーバのIPアドレスが指定されているかどうかを確認します。また、スキャナプールのリストで許可されている特権ユーザがアクティブかどうかを確認します。スキャナプールを確認するには、 <code>vserver vscan scanner-pool show</code> コマンドをストレージシステムのコマンドプロンプトで実行します。それでもVscanサーバが接続できない場合は、ネットワークに問題がある可能性があります。
クライアントで高レイテンシが観察されます。	スキャナプールにVscanサーバを追加するタイミングが来たと考えられます。
トリガーされたスキャンが多すぎます。	の値を変更します。 <code>vscan-fileop-profile</code> パラメータを指定して、ウィルススキャンの対象として監視するファイル操作の数を制限します。
一部のファイルがスキャンされていません。	オンアクセスポリシーを確認します。これらのファイルのパスがパス除外リストに追加されているか、ファイルのサイズが除外の設定値を超えている可能性があります。オンアクセスポリシーを確認するには、 <code>vserver vscan on-access-policy show</code> コマンドをストレージシステムのコマンドプロンプトで実行します。
ファイルアクセスが拒否されました。	ポリシー設定で <code>_scan-mandatory_setting</code> が指定されているかどうかを確認します。この設定では、Vscanサーバが接続されていない場合にデータアクセスが拒否されます。必要に応じて設定を変更します。

## ステータスとパフォーマンスアクティビティの監視

Vscanサーバの接続ステータス、  
Vscanサーバの健全性、およびスキャンされたファイルの数。この情報は、  
Vscanサーバに関連する問題を診断します。

### Vscanサーバの接続情報の表示

Vscanサーバの接続ステータスを表示して、使用中の接続を管理できます。  
使用可能な接続が表示されます。さまざまなコマンドで情報を表示  
Vscanサーバの接続ステータスについて

コマンド...	表示される情報...
<code>vserver vscan connection-status show</code>	接続ステータスの概要
<code>vserver vscan connection-status show-all</code>	接続ステータスに関する詳細情報

<code>vserver vscan connection-status show-not-connected</code>	使用可能だが接続されていない接続のステータス
<code>vserver vscan connection-status show-connected</code>	接続されているVscanサーバに関する情報

これらのコマンドの詳細については、を参照してください ["マニュアルページ"](#)。

#### Vscanサーバの統計の表示

Vscanサーバ固有の統計を表示して、パフォーマンスを監視し、関連する問題を診断できます。  
 ウィルススキャン：を使用する前に、データサンプルを収集する必要があります。 `statistics show` コマンドをに送信します  
 Vscanサーバの統計を表示します。  
 データサンプルを完了するには、次の手順を実行します。

#### ステップ

1. を実行します `statistics start` コマンドとを実行します `optional statistics` 停止コマンド。

#### Vscanサーバ要求とレイテンシの統計を表示する

ONTAPを使用できます。 `offbox vscan` SVM単位でカウンタを実行してVscan速度を監視  
 すべてのVscanで1秒あたりに送出および受信されるサーバ要求とサーバレイテンシ  
 サーバ：これらの統計を表示するには、次の手順を実行します。

#### ステップ

1. `statistics show`を実行します。 `object offbox_vscan -instance SVM` コマンドにを指定します  
 次のカウンタ

カウンタ...	表示される情報...
<code>scan_request_dispatched_rate</code>	ONTAPからVscanサーバに送信される1秒あたりのウィルススキャン要求数
<code>scan_noti_received_rate</code>	ONTAPがVscanサーバから受信した1秒あたりのウィルススキャン要求数
<code>dispatch_latency</code>	使用可能なVscanサーバを特定してそのVscanサーバに要求を送信するためのONTAP内のレイテンシ
<code>scan_latency</code>	ONTAPからVscanサーバへのラウンドトリップレイテンシ（スキャンの実行時間を含む）

#### ONTAP外部Vscanカウンタから生成される統計の例

```
Object: offbox_vscan
Instance: SVM
Start-time: 10/16/2013 10:13:25
End-time: 10/16/2013 10:25:11
Cluster: cluster01
Number of Constituents: 2 (complete_aggregation)
Counter Value
```

```
-----
scan_request_dispatched_rate 291
scan_noti_received_rate 292
dispatch_latency 43986us
scan_latency 3433501us
-----
```

## 個々のVscanサーバ要求とレイテンシの統計を表示する

ONTAPを使用できます。offbox\_vscan\_server SVMごと、オフボックスのVscanサーバごとにカウンタノード単位で監視し、ディスパッチされたVscanサーバ要求の速度とサーバレイテンシを各Vscanサーバを個別に指定します。この情報を収集するには、次の手順を実行します。

### ステップ

1. を実行します `statistics show -object offbox_vscan -instance SVM:servername:nodename` 次のカウンタを指定してコマンドを実行します。

カウンタ...	表示される情報...
scan_request_dispatched_rate	ONTAPから送信されたウィルススキャン要求の数
scan_latency	ONTAPからVscanサーバへのラウンドトリップレイテンシ（スキャンの実行時間を含む） 1秒あたりのVscanサーバへの転送

## ONTAP offbox\_vscan\_serverカウンタで生成される統計の例



```
Object: offbox_vscan_server
Instance: SVM:vscan_server:node
Start-time: 10/16/2013 10:13:25
End-time: 10/16/2013 10:25:11
Cluster: cluster01
Number of Constituents: 1 (complete_aggregation)
Counter Value
```

```
-----
scan_request_dispatched_rate 291
scan_latency 3433830us
-----
```

## Vscanサーバ使用率の統計を表示する

ONTAPを使用することもできます。offbox\_vscan\_server Vscanサーバ側の使用率を収集するカウンタ統計：これらの統計は、SVM単位、オフボックスのVscanサーバ単位、ノード単位で追跡されます。彼らはVscanサーバのCPU利用率、Vscanサーバでのスキャン処理のキュー深度を記載

（現在と最大の両方）、使用済みメモリ、および使用済みネットワーク。

これらの統計は、Antivirus ConnectorによってONTAP内の統計カウンタに転送されます。彼らは20秒ごとにポーリングされ、正確性を保つために複数回収集する必要があるデータに基づいている。それ以外の場合、統計に表示される値は最後のポーリングのみを反映します。CPUの利用率とキューは特に監視と分析に重要です。平均キューの値が大きい場合、

Vscanサーバがボトルネックになります。

SVMごと、オフボックスVscanサーバごと、およびノードごとのVscanサーバの使用率の統計を収集するにはBasisで、次の手順を実行します。

### ステップ

1. Vscanサーバの使用率の統計を収集します。

を実行します `statistics show -object offbox_vscan_server -instance SVM:servername:nodename` コマンドと次のコマンド `offbox_vscan_server` カウンタ：

カウンタ...	表示される情報...
<code>scanner_stats_pct_cpu_used</code>	VscanサーバのCPU利用率
<code>scanner_stats_pct_input_queue_avg</code>	Vscanサーバ上のスキャン要求の平均キュー
<code>scanner_stats_pct_input_queue_hiwatemark</code>	Vscanサーバでのスキャン要求のピークキュー
<code>scanner_stats_pct_mem_used</code>	Vscanサーバで使用されているメモリ
<code>scanner_stats_pct_network_used</code>	Vscanサーバで使用されるネットワーク

```
Object: offbox_vscan_server
Instance: SVM:vscan_server:node
Start-time: 10/16/2013 10:13:25
End-time: 10/16/2013 10:25:11
Cluster: cluster01
Number of Constituents: 1 (complete_aggregation)
Counter Value
-----
scanner_stats_pct_cpu_used 51
scanner_stats_pct_dropped_requests 0
scanner_stats_pct_input_queue_avg 91
scanner_stats_pct_input_queue_hiwatermark 100
scanner_stats_pct_mem_used 95
scanner_stats_pct_network_used 4
-----
```

## SVM で NAS イベントを監査します

### SMB および NFS の監査とセキュリティトレース

SMB プロトコルと NFS プロトコルで利用できるファイルアクセス監査機能は、ONTAP で使用できます。たとえば、FPolicy を使用した標準の監査やファイルポリシー管理などです。

SMB と NFS のファイルアクセスイベントの監査は、次のような状況で設計および実装する必要があります。

- SMB および NFS プロトコルの基本的なファイルアクセスが設定されている。
- 次のいずれかの方法で監査の設定を作成して管理する。
  - ONTAP の標準機能
  - 外部 FPolicy サーバ

### SVM で NAS イベントを監査します

NAS イベントの監査は、Storage Virtual Machine (SVM) で特定の SMB および NFS イベントを追跡してログに記録できるセキュリティ対策です。これは、潜在的なセキュリティの問題を追跡するのに役立ち、セキュリティ違反が発生した場合の証拠になります。Active Directory の集約型アクセスポリシーのステージングおよび監査によってこれらを実装した場合の結果を確認することもできます。

#### SMB イベント

次のイベントを監査できます。

- SMB ファイルおよびフォルダのアクセスイベント

監査が有効になっている SVM に属する FlexVol ボリュームに格納されているオブジェクトに対する SMB によるファイルおよびフォルダアクセスイベントを監査できます。

- SMB ログオンおよびログオフイベント

SVM 上の SMB サーバでの SMB ログオンおよびログオフイベントを監査できます。

- 集約型アクセスポリシーのステージングイベント

提案された集約型アクセスポリシーによって適用された権限を使用して、SMB サーバ上のオブジェクトの有効なアクセスを監査できます。集約型アクセスポリシーのステージングによって監査を行うと、集約型アクセスポリシーを導入する前に、その影響を確認できます。

集約型アクセスポリシーのステージングによる監査は、Active Directory の GPO を使用してセットアップされます。ただし、SVM の監査の設定は、集約型アクセスポリシーステージングイベントを監査するように設定されている必要があります。

SMB サーバでダイナミックアクセス制御を有効にせずに、監査の設定で集約型アクセスポリシーのステージングを有効にすることはできますが、集約型アクセスポリシーのステージングイベントが生成されるのは、ダイナミックアクセス制御が有効になっている場合のみです。ダイナミックアクセス制御は SMB サーバオプションを使用して有効にします。デフォルトでは有効になっていません。

## NFS イベント

ファイルおよびディレクトリイベントを監査するには、SVM に格納されているオブジェクトで NFSv4 ACL を使用します。

## 監査の仕組み

### 監査の基本概念

ONTAP の監査について理解するために、監査の基本概念を確認しておく必要があります。

- \* ステージングファイル \*

統合および変換の前に監査レコードが格納される、個々のノード上の中間バイナリファイル。ステージングファイルはステージングボリュームに格納されます。

- \* ステージングボリューム \*

ステージングファイルを格納するために ONTAP によって作成される専用ボリューム。各アグリゲートに 1 つのステージングボリュームがあります。ステージングボリュームは、そのアグリゲート内のデータボリュームを対象としたデータアクセスの監査レコードを格納するために、監査が有効なすべての Storage Virtual Machine (SVM) で共有されます。各 SVM の監査レコードは、ステージングボリューム内の個別のディレクトリに格納されます。

クラスタ管理者はステージングボリュームに関する情報を表示できますが、それ以外のほとんどのボリューム操作は実行できません。ステージングボリュームを作成できるのは ONTAP のみです。ONTAP では、ステージングボリュームに自動的に名前が割り当てられます。すべてのステージングボリューム名はで始まります MDV\_aud\_ そのあとに、ステージングボリュームを含むアグリゲートの UUID (例: MDV\_aud\_1d0131843d4811e296fc123478563412.)

- \* システムボリューム \*

ファイルサービスや監査ログのメタデータなど、特別なメタデータを格納する FlexVol ボリューム。システムボリュームの所有者は管理 SVM であり、システムボリュームはクラスタ全体で表示されます。ステージングボリュームはシステムボリュームの一種です。

- \* 統合タスク \*

監査が有効になったときに作成されるタスク。各 SVM で長時間にわたって実行されるこのタスクは、SVM のメンバーノード全体のステージングファイルから監査レコードを取得します。このタスクは、監査レコードを時間順にソートされた状態でマージしたうえで、これらのレコードを監査の設定で指定されたユーザが読解可能なイベントログ形式に変換します。変換されたイベントログは、SVM 監査の設定で指定された監査イベントログディレクトリに格納されます。

## ONTAP 監査プロセスの仕組み

ONTAP の監査プロセスは、Microsoft の監査プロセスとは異なります。監査を設定する前に、ONTAP の監査プロセスの仕組みについて理解しておく必要があります。

監査レコードは、最初に個々のノードのバイナリステージングファイルに格納されます。ある SVM で監査が有効になると、すべてのメンバーノードでその SVM のステージングファイルが保持されます。定期的に統合され、ユーザが読解可能なイベントログに変換されて、SVM の監査イベントログディレクトリに格納されます。

ある SVM で監査が有効になっている場合の処理

監査は、SVM でのみ有効にできます。ストレージ管理者が SVM で監査を有効にすると、監査サブシステムによってステージングボリュームが存在するかどうかを確認されます。ステージングボリュームは、SVM に所有されているデータボリュームを含むアグリゲートごとが必要です。存在しない場合は、監査サブシステムによって必要なステージングボリュームが作成されます。

また、監査が有効になる前に、前提条件となるその他のタスクが実行されます。

- 監査サブシステムによって、ログディレクトリのパスが使用可能でシンボリックリンクが含まれていないことが検証されます。

ログディレクトリは、SVM のネームスペース内のパスとしてすでに存在している必要があります。監査ログファイルを格納する新しいボリュームまたは qtrees を作成することを推奨します。監査サブシステムは、デフォルトのログファイルの場所を割り当てません。監査の設定で指定されているログディレクトリのパスが有効なパスでない場合は、監査の設定の作成に失敗します The specified path "/path" does not exist in the namespace belonging to Vserver "Vserver\_name" エラー。

ディレクトリは存在するがシンボリックリンクが含まれている場合は、設定の作成に失敗します。

- 監査によって統合タスクがスケジュールされます。

このタスクがスケジュールされると、監査が有効になります。SVM の監査の設定とログファイルは、リブート後も、NFS サーバまたは SMB サーバが停止したり再起動したりしても維持されます。

## イベントログの統合

ログの統合は、監査が無効になるまで定期的に行われるスケジュール済みタスクです。監査が無効になると、統合タスクによって残りのすべてのログが統合されたことが検証されます。

### 監査の保証

デフォルトでは、監査が保証されています。ONTAP では、あるノードが利用できない場合でも、監査可能なファイルアクセスイベント（設定された監査ポリシーの ACL で指定されている）がすべて記録されることが保証されます。要求されたファイル操作は、その操作の監査レコードが永続的ストレージのステージングボリュームに保存されるまで完了できません。スペース不足またはその他の問題が原因で監査レコードをステージングファイルのディスクにコミットできない場合は、クライアント処理が拒否されます。



管理者または権限レベルのアクセス権を持つアカウントユーザは、NetApp Manageability SDK または REST API を使用してファイル監査ログ処理を省略できます。NetApp Manageability SDK または REST API を使用してファイル操作が行われたかどうかを確認するには、に格納されているコマンド履歴ログを確認します `audit.log` ファイル。

コマンド履歴監査ログの詳細については、の「管理アクティビティの監査ログの管理」セクションを参照してください ["システム管理"](#)。

### ノードが利用できない場合の統合プロセス

監査が有効になっている SVM に属するボリュームを含むノードが利用できない場合、監査の統合タスクの動作は、そのノードのストレージフェイルオーバー（SFO）パートナー（2 ノードクラスタの場合は HA パートナー）が利用可能かどうかによって異なります。

- ステージングボリュームが SFO パートナーを介して利用可能な場合は、ノードから最後に報告されたステージングボリュームがスキャンされ、統合が正常に行われます。
- SFO パートナーが利用できない場合は、タスクによって部分的なログファイルが作成されます。

あるノードにアクセスできない場合は、統合タスクによって、その SVM の利用可能な他のノードの監査レコードが統合されます。完了していないことを識別するために、サフィックスが追加されます `.partial` を統合ファイル名に変更します。

- 利用できないノードが利用可能になったら、そのノードの監査レコードが、その時点における他のノードの監査レコードと統合されます。
- 監査レコードはすべて維持されます。

### イベントログのローテーション

監査イベントログファイルは、設定されたログサイズしきい値に達した場合、または設定されたスケジュールに従ってローテーションされます。イベントログファイルがローテーションされると、スケジュールされた統合タスクによって、まず、アクティブな変換済みファイルの名前がタイムスタンプのあるアーカイブファイルに変更され、そのあとで新しいアクティブな変換済みイベントログファイルが作成されます。

### SVM で監査が無効になっている場合の処理

SVM で監査が無効になると、もう一度統合タスクがトリガーされます。未処理の記録済みの監査レコードはすべて、ユーザが読解可能な形式でログに記録されます。SVM で監査が無効になっても、イベントログディレクトリに格納されている既存のイベントログは削除されず、参照が可能です。

その SVM の既存のステージングファイルがすべて統合されたら、スケジュールから統合タスクが削除されます。SVM の監査の設定を無効にしても、監査の設定は削除されません。ストレージ管理者は、監査をいつでも再度有効にできます。

監査の統合ジョブは、監査が有効になったときに作成され、統合タスクを監視して、統合タスクがエラーによって終了した場合に統合タスクを再作成します。ユーザは監査の統合ジョブを削除できません。

## 監査の要件と考慮事項

Storage Virtual Machine （SVM）で監査を設定して有効にする前に、一定の要件と考慮事項について理解しておく必要があります。

- 監査を有効にしたSVMの最大サポート数は、ONTAPのバージョンによって異なります。

ONTAPバージョン	最大
9.8以前	50です
9.9.1 以降	400

- 監査は、SMB または NFS のライセンスとは関係ありません。

クラスタにSMBとNFSのライセンスがインストールされていない場合でも、監査を設定して有効にすることができます。

- NFS 監査では、セキュリティ ACE （タイプ U）をサポートしています。
- NFS 監査では、モードビットと監査 ACE の間のマッピングはありません。

ACL をモードビットに変換する場合、監査 ACE はスキップされます。モードビットを ACL に変換する場合、監査 ACE は生成されません。

- 監査の設定で指定するディレクトリが存在している必要があります。

存在しない場合、監査の設定を作成するコマンドは失敗します。

- 監査の設定で指定するディレクトリは、次の要件を満たしている必要があります。

- ディレクトリにシンボリックリンクを含めることはできません。

監査の設定で指定するディレクトリにシンボリックリンクが含まれている場合、監査の設定を作成するコマンドは失敗します。

- 絶対パスを使用してディレクトリを指定する必要があります。

相対パスは指定しないでください（例：）。 /vs1/../../。

- 監査は、ステージングボリューム内に利用可能なスペースがあるかどうか依存します。

監査対象のボリュームを含むアグリゲートのステージングボリュームに十分なスペースを確保できるよう注意する必要があります。

- 監査は、変換されたイベントログの格納先ディレクトリを含むボリューム内に利用可能なスペースがあるかどうか依存します。

イベントログの格納に使用するボリュームに十分なスペースを確保できるよう注意する必要があります。を使用して、監査ディレクトリに保持するイベントログの数を指定できます `-rotate-limit` 監査の設定を作成する際のパラメータ。これは、ボリューム内のイベントログ用に十分なスペースを確保するのに役立ちます。

- 監査の設定では、SMBサーバでダイナミックアクセス制御を有効にしなくても集約型アクセスポリシーのステージングを有効にできますが、集約型アクセスポリシーのステージングイベントを生成するには、ダイナミックアクセス制御を有効にする必要があります。

ダイナミックアクセス制御は、デフォルトでは有効になっていません。

#### 監査を有効にする際のアグリゲートスペースに関する考慮事項

監査の設定が作成されていてクラスタ内の少なくとも 1 つの Storage Virtual Machine (SVM) で監査が有効になっている場合、監査サブシステムは、既存のすべてのアグリゲートと、作成されるすべての新しいアグリゲートにステージングボリュームを作成します。クラスタ上で監査を有効にする際は、アグリゲートスペースに関する考慮事項に注意する必要があります。

アグリゲートに十分な空き容量がない場合、ステージングボリュームの作成に失敗することがあります。これは、監査の設定を作成したときに、既存のアグリゲートにステージングボリュームを格納するための十分なスペースがない場合に発生することがあります。

SVM で監査を有効にする前に、既存のアグリゲート上にステージングボリューム用の十分なスペースがあることを確認する必要があります。

#### ステージングファイルの監査レコードのサイズに関する制限

ステージングファイルの監査レコードのサイズは、32KB 以下にする必要があります。

大規模な監査レコードが発生する可能性がある場合

次のいずれかのシナリオで、管理の監査時に大規模な監査レコードが発生することがあります。

- 多数のユーザを含むグループに対してユーザを追加または削除する。
- 多数のファイル共有ユーザを含むファイル共有に対して、ファイル共有アクセス制御リスト (ACL) を追加または削除する。
- その他のシナリオ。

この問題を回避するには、管理監査を無効にしてください。これを行うには、監査設定を変更し、監査イベントタイプのリストから次の項目を削除します。

- ファイル共有
- ユーザアカウント
- セキュリティグループ
- 認証ポリシー変更

削除すると、ファイルサービスの監査サブシステムで監査されなくなります。

## 大きすぎる監査レコードの影響

- 監査レコードのサイズが大きすぎる（32KB を超える）場合、監査レコードは作成されず、監査サブシステムによって次のような Event Management System（EMS；イベント管理システム）メッセージが生成されます。

```
File Services Auditing subsystem failed the operation or truncated an audit
record because it was greater than max_audit_record_size value. Vserver
UUID=%s, event_id=%u, size=%u
```

監査が保証されている場合は、監査レコードを作成できないためにファイル処理が失敗します。

- 監査レコードのサイズが 9、999 バイトを超える場合は、上記と同じ EMS メッセージが表示されます。部分的な監査レコードが作成され、指定した値よりも大きな値が欠落します。
- 監査レコードが 2、000 文字を超えている場合は、実際の値ではなく次のエラーメッセージが表示されます。

```
The value of this field was too long to display.
```

## サポートされる監査イベントログの形式

変換された監査イベントログでサポートされるファイル形式はです EVTX および XML ファイル形式。

監査の設定を作成する際には、ファイル形式の種類を指定できます。デフォルトでは、ONTAP はバイナリログをに変換します EVTX ファイル形式。

## 監査イベントログを表示する

監査イベントログを使用して、ファイルセキュリティが適切であるかどうか、ファイルやフォルダへの不適切なアクセス試行がなかったかどうかを確認できます。に保存された監査イベントログを表示および処理できます EVTX または XML ファイル形式。

- EVTX ファイル形式

変換されたを開くことができます EVTX Microsoft イベントビューアを使用して、保存されたファイルとしてイベントログを監査します。

イベントビューアでイベントログを表示する際に使用できるオプションは 2 つあります。

- 全般表示

イベントレコードには、すべてのイベントに共通する情報が表示されます。このバージョンの ONTAP では、イベントレコードに関するイベント固有のデータは表示されません。詳細表示を使用して、イベント固有のデータを表示できます。

- 詳細ビュー

フレンドリ表示と XML 表示を使用できます。フレンドリ表示と XML 表示には、すべてのイベントに共通の情報とイベントレコードのイベント固有のデータの両方が表示されます。



- XML ファイル形式

表示と処理が可能です XML をサポートする他社製アプリケーションの監査イベントログ XML ファイル形式。XML スキーマと XML フィールドの定義に関する情報があれば、XML 表示ツールを使用して監査ログを表示できます。XML スキーマおよび定義の詳細については、を参照してください "[ONTAP 監査スキーマリファレンス](#)"。

## イベントビューアを使用したアクティブな監査ログの表示方法

クラスターで監査の統合プロセスを実行している場合、統合プロセスにより、監査を有効にした SVM のアクティブな監査ログファイルに新しいレコードが追加されます。このアクティブな監査ログは、SMB 共有でアクセスして Microsoft イベントビューアで開くことができます。

イベントビューアには、既存の監査レコードが表示されるだけでなく、コンソールウィンドウの内容を更新するオプションもあります。アクティブな監査ログにアクセスするために使用される共有で oplock が有効になっているかどうかに応じて、新たに追加されたログをイベントビューアで表示できるかどうか異なります。

共有での oplock の設定	動作
有効	その時点までに書き込まれたイベントを含むログがイベントビューアに表示されます。更新処理を実行してもログは更新されず、統合プロセスで追加された新しいイベントは表示されません。
無効	その時点までに書き込まれたイベントを含むログがイベントビューアに表示されます。更新処理を実行すると、ログが更新され、統合プロセスで追加された新しいイベントが表示されます。



この情報は、にのみ適用されます EVTX イベントログ。XML イベントログは、SMBを介してブラウザで、または任意のXMLエディタまたはビューアを使用してNFSで表示できます。

## 監査できる SMB イベント

### 監査できる SMB イベントの概要

ONTAP は、ファイルおよびフォルダのアクセスイベント、ログオンおよびログオフイベント、集約型アクセスポリシーのステージングイベントなどの SMB イベントを監査できます。どのようなアクセスイベントを監査できるか理解しておく、イベントログの結果を解釈するときに役立ちます。

ONTAP 9.2 以降では、次の SMB イベントが監査対象として追加されました。

イベント ID (EVT / イベント EVTX)	説明	カテゴリ
4670	オブジェクト権限が変更されました	ファイルアクセス

4907	オブジェクトの監査設定が変更されました	オブジェクトアクセス：監査設定が変更された。	ファイルアクセス
4913	オブジェクトの集約型アクセスポリシーが変更されました	オブジェクトへのアクセス：CAP が変更された。	ファイルアクセス

ONTAP 9.0 以降では、次の SMB イベントを監査できます。

イベント ID (EVT / EVTX)	イベント	説明	カテゴリ
540/4624	アカウントがログオンに成功しました	ログオン/ログオフ：ネットワーク (SMB) ログオン。	ログオンおよびログオフ
529/4625	アカウントがログオンに失敗しました	ログオン/ログオフ：ユーザ名が不明またはパスワードが無効です。	ログオンおよびログオフ
530/4625	アカウントがログオンに失敗しました	ログオン/ログオフ：アカウントログオンの時間制限です。	ログオンおよびログオフ
531/4625	アカウントがログオンに失敗しました	ログオン/ログオフ：アカウントは現在無効になっています。	ログオンおよびログオフ
532/4625	アカウントがログオンに失敗しました	ログオン/ログオフ：ユーザアカウントの有効期限が切れています。	ログオンおよびログオフ
533/4625	アカウントがログオンに失敗しました	ログオン/ログオフ：ユーザはこのコンピュータにログオンできません。	ログオンおよびログオフ
534/4625	アカウントがログオンに失敗しました	ログオン/ログオフ：ユーザはログオンを許可されていません。	ログオンおよびログオフ
535/4625	アカウントがログオンに失敗しました	ログオン/ログオフ：ユーザのパスワードが期限切れです。	ログオンおよびログオフ
537/4625	アカウントがログオンに失敗しました	ログオン/ログオフ：上記以外の理由でログオンが失敗しました。	ログオンおよびログオフ
539/4625	アカウントがログオンに失敗しました	ログオン/ログオフ：アカウントのロックアウト。	ログオンおよびログオフ
538/4634	アカウントがログオフされました	ログオン/ログオフ：ローカルまたはネットワークユーザのログオフ。	ログオンおよびログオフ

560/4656	オブジェクトを開く / オブジェクトを作成	オブジェクトへのアクセス：オブジェクト（ファイルまたはディレクトリ）が開きます。	ファイルアクセス
563/4659.	削除するためにオブジェクトを開く	オブジェクトへのアクセス：削除するためにオブジェクト（ファイルまたはディレクトリ）へのハンドルが要求された。	ファイルアクセス
564 / 4660	オブジェクトを削除します	オブジェクトへのアクセス：オブジェクト（ファイルまたはディレクトリ）を削除します。ONTAP は、Windows クライアントがオブジェクト（ファイルまたはディレクトリ）の削除を試みるとこのイベントを生成します。	ファイルアクセス
567/4663	オブジェクトの読み取り / オブジェクトの書き込み / オブジェクトの属性の取得 / オブジェクトの属性の設定	<p>オブジェクトへのアクセス：オブジェクトへのアクセスの試み（読み取り、書き込み、属性の取得、属性の設定）。</p> <ul style="list-style-type: none"> <li>注：* このイベントでは、ONTAP はオブジェクトに対する最初の SMB 読み取り操作と SMB 書き込み操作（の成功または失敗）を監査します。これにより、1 つのクライアントが、あるオブジェクトを開き、そのオブジェクトに対して連続的に多数の読み取りまたは書き込みを行っても、ONTAP が余計にログエントリを書き込むことがなくなります。</li> </ul>	ファイルアクセス
NA / 4664	ハードリンク	オブジェクトへのアクセス：ハードリンクの作成が試行されました。	ファイルアクセス
NA / 4818	提案された集約型アクセスポリシーでは、現在の集約型アクセスポリシーと同じアクセス権限が付与されません	オブジェクトへのアクセス：集約型アクセスポリシーのステージング。	ファイルアクセス
NA / NA Data ONTAP イベント ID 9999	オブジェクト名を変更します	オブジェクトへのアクセス：オブジェクトの名前変更。これは ONTAP イベントです。Windows では現在、単一イベントとしてサポートされていません。	ファイルアクセス

NA/NA Data ONTAP イベントID 9998	オブジェクトのリンク解除	オブジェクトへのアクセス：オブジェクトのリンクが解除される。これは ONTAP イベントです。Windows では現在、単一イベントとしてサポートされていません。	ファイルアクセス
---------------------------------	--------------	---	----------

#### イベント 4656 に関する追加情報

。 HandleID 監査でタグを付けます XML イベントには、アクセスされたオブジェクト（ファイルまたはディレクトリ）のハンドルが含まれます。 HandleID EVTX 4656 イベントのタグには、オープンイベントが新しいオブジェクトを作成するためのものか、既存のオブジェクトを開くためのものかによって、異なる情報が含まれます。

- open イベントが新しいオブジェクト（ファイルまたはディレクトリ）を作成するためのオープン要求である場合は、 HandleID 監査 XML イベントのタグに空が表示されます HandleID （例： `<Data Name="HandleID">0000000000000000;00;00000000;00000000</Data>` ）。

。 HandleID が空の理由は、（新しいオブジェクトを作成するための） OPEN 要求が、実際のオブジェクトの作成が行われる前、およびハンドルが存在する前に監査されるためです。同じオブジェクトの後続の監査対象イベントは、適切なオブジェクトハンドルを持ちます HandleID タグ。

- オープンイベントが既存のオブジェクトを開くためのオープン要求である場合、監査イベントには、そのオブジェクトの割り当てられたハンドルが割り当てられます HandleID タグ（例： `<Data Name="HandleID">000000000000401;00;000000ea;00123ed4</Data>` ）。

#### 監査対象オブジェクトへの完全なパスを決定します

に出力されたオブジェクトパス `<ObjectName>` 監査レコードのタグには、ボリュームの名前（カッコ内）と、そのボリュームを含むボリュームのルートからの相対パスが表示されます。ジャンクションパスを含む監査対象オブジェクトの完全パスを決定する場合には、実行する必要がある特定の手順があります。

#### 手順

1. を参照して、ボリューム名と監査対象オブジェクトへの相対パスを確認します `<ObjectName>` 監査イベントのタグ。

この例では、ボリューム名は「data1」で、ファイルへの相対パスはです `/dir1/file.txt`：

```
<Data Name="ObjectName"> (data1);/dir1/file.txt </Data>
```

2. 前の手順で確認したボリューム名を使用して、監査対象オブジェクトが含まれているボリュームのジャンクションパスを確認します。

この例では、ボリューム名は「data1」、監査対象オブジェクトが含まれるボリュームのジャンクションパスはです `/data/data1`：

```
volume show -junction -volume data1
```

Vserver	Volume	Junction		Junction Path	Junction Path Source
		Language	Active		
vs1	data1	en_US.UTF-8	true	/data/data1	RW_volume

3. で見つかった相対パスを追加して、監査対象オブジェクトへの完全パスを決定します <ObjectName> ボリュームのジャンクションパスにタグを付けます。

この例では、ボリュームのジャンクションパスは次のようになります。

```
/data/data1/dir1/file.text
```

## シンボリックリンクおよびハードリンクを監査する際の考慮事項

シンボリックリンクおよびハードリンクを監査する場合は、一定の考慮事項に注意する必要があります。

監査レコードには、で識別される監査対象オブジェクトへのパスなど、監査対象オブジェクトに関する情報が含まれます ObjectName タグ。シンボリックリンクおよびハードリンクのパスがどのように記録されるかを確認しておく必要があります ObjectName タグ。

### シンボリックリンク

シンボリックリンクとは、ターゲットと呼ばれるデスティネーションオブジェクトの場所へのポインタを含む、独立した inode を持つファイルです。シンボリックリンクを介してオブジェクトにアクセスする際、ONTAP は、シンボリックリンクを自動的に解釈し、ボリューム内のターゲットオブジェクトへの、プロトコルに依存しない本来のパスに従います。

次の出力例には、2つのシンボリックリンクがあり、どちらもという名前のファイルを指しています target.txt。一方のシンボリックリンクは相対シンボリックリンクであり、他方は絶対シンボリックリンクです。どちらかのシンボリックリンクが監査された場合は、が実行されます ObjectName 監査イベントのタグにファイルへのパスが含まれています target.txt：

```
[root@host1 audit]# ls -l
total 0
lrwxrwxrwx 1 user1 group1 37 Apr  2 10:09 softlink_fullpath.txt ->
/data/audit/target.txt
lrwxrwxrwx 1 user1 group1 10 Apr  2 09:54 softlink.txt -> target.txt
-rwxrwxrwx 1 user1 group1 16 Apr  2 10:05 target.txt
```

### ハードリンク

ハードリンクは、ファイルシステム上の既存のファイルに名前を関連付けるディレクトリエントリです。ハードリンクは元のファイルの inode の場所を指しています。ONTAP ONTAP は、シンボリックリンクの解釈方法と同様に、ハードリンクを解釈し、ボリューム内のターゲットオブジェクトへの本来のパスに従います。ハードリンクオブジェクトへのアクセスが監査されると、監査イベントはこの正規の絶対パスをに記録します

ObjectName ハードリンクパスではなくタグ付けます。

## 代替 NTFS データストリームを監査する際の考慮事項

NTFS 代替データストリームを持つファイルを監査する場合は、一定の考慮事項に注意する必要があります。

監査対象のオブジェクトの場所は、2つのタグ ( ) を使用してイベントレコードに記録されます ObjectName タグ (パス) および HandleID タグ (ハンドル)。ログに記録されるストリーム要求を適切に識別するには、NTFS 代替データストリームでこれらのフィールドに記録される ONTAP レコードを把握しておく必要があります。

- EVTX ID : 4656 のイベント (オープンおよび作成の監査イベント)
  - 代替データストリームのパスはに記録されます ObjectName タグ。
  - 代替データストリームのハンドルはに記録されます HandleID タグ。
- EVTX ID : 4663 のイベント (読み取り、書き込み、属性の取得など、その他すべての監査イベント)
  - 代替データストリームではなく、ベースファイルのパスがに記録されます ObjectName タグ。
  - 代替データストリームのハンドルはに記録されます HandleID タグ。

### 例

次の例は、を使用して代替データストリームの EVTX ID : 4663 イベントを特定する方法を示しています HandleID タグ。にもかかわらず ObjectName 読み取り監査イベントで記録されるタグ (パス) は、ベースファイルパスであるへのパスです HandleID タグを使用すると、イベントを代替データストリームの監査レコードとして識別できます。

ストリームファイル名はの形式になります `base_file_name:stream_name`。この例では、を使用しています `dir1` ディレクトリには、次のパスを持つ代替データストリームを持つベースファイルが含まれています。

```
/dir1/file1.txt  
/dir1/file1.txt:stream1
```



次のイベント例の出力はご覧のように省略されています。この出力にはイベントで使用可能なすべての出力タグが表示されているわけではありません。

EVTX ID 4656 (オープン監査イベント) の場合、代替データストリームの監査レコード出力に代替データストリーム名が記録されます ObjectName タグ：

```

- <Event>
- <System>
  <Provider Name="Netapp-Security-Auditing" />
  <EventID>4656</EventID>
  <EventName>Open Object</EventName>
  [...]
</System>
- <EventData>
  [...]
  **<Data Name="ObjectType">Stream</Data>
  <Data Name="HandleID">00000000000401;00;000001e4;00176767</Data>
  <Data Name="ObjectName">\\(data1\);/dir1/file1.txt:stream1</Data>
  **
  [...]
</EventData>
</Event>
- <Event>

```

EVTX ID 4663（読み取り監査イベント）の場合、同じ代替データストリームの監査レコード出力にベースファイル名が記録されます ObjectName タグ。ただし、のハンドル HandleID タグは代替データストリームのハンドルであり、このイベントを代替データストリームと関連付けるために使用できます。

```

- <Event>
- <System>
  <Provider Name="Netapp-Security-Auditing" />
  <EventID>4663</EventID>
  <EventName>Read Object</EventName>
  [...]
</System>
- <EventData>
  [...]
  **<Data Name="ObjectType">Stream</Data>
  <Data Name="HandleID">00000000000401;00;000001e4;00176767</Data>
  <Data Name="ObjectName">\\(data1\);/dir1/file1.txt</Data> **
  [...]
</EventData>
</Event>
- <Event>

```

## 監査できる NFS ファイルおよびディレクトリのアクセスイベント

ONTAP は、特定の NFS ファイルおよびディレクトリへのアクセスイベントを監査できます。どのようなアクセスイベントを監査できるか理解しておく、変換された監査イベントログの結果を解釈するときに役立ちます。

次の NFS ファイルおよびディレクトリへのアクセスイベントを監査できます。

- 読み取り
- を開きます
- を閉じます
- ディレクトリの読み取り
- 書き込み
- 属性の設定
- 作成
- リンク
- 属性を開く（OPENATTR）
- 取り外します
- 属性の取得
- 確認します
- 非検証
- 名前を変更する

NFS の名前変更イベントを確実に監査するには、ファイルではなくディレクトリに監査 ACE を設定する必要があります。これは、ディレクトリへのアクセス権がある場合に、名前変更の操作でファイルのアクセス権が確認されないためです。

## 監査の設定を計画

Storage Virtual Machine（SVM）で監査を設定する前に、使用可能な設定オプションを理解し、各オプションに設定する値を計画する必要があります。この情報は、ビジネスニーズを満たす監査の設定に役立ちます。

すべての監査の設定に共通する設定パラメータがあります。

また、統合および変換された監査ログのローテーション時に使用する方法を指定するために使用できるパラメータもあります。監査の設定を行う際には、次の 3 つの方法のいずれかを指定できます。

- ログサイズに基づいてログをローテーションします

ログのローテーションに使用されるデフォルトの方法です。

- スケジュールに基づいたログのローテーション
- ログのサイズとスケジュール（先にイベントが発生した方）に基づいてログのローテーションを実行

ログローテーションの方法を少なくとも 1 つ設定する必要があります。



## すべての監査設定に共通するパラメータ

監査の設定の作成時に指定する必要がある 2 つの必須パラメータがあります。また、指定できるオプションのパラメータが 3 つあります。

情報のタイプ	オプション	必須	含める	値を入力 します
SVM 名 _  監査の設定を作成する SVM の名前。SVM はすでに存在する必要があります。	-vserver vserver_name	はい。	はい。	
_ ログデスティネーションパス _  変換された監査ログを格納するディレクトリ を指定します。通常は専用のボリューム または qtree です。パスは SVM ネームス ペースにすでに存在する必要があります。  パスには、最大 864 文字の文字列を指定 できます。パスには読み取り / 書き込みア クセス権が必要です。  パスが有効でない場合、監査の設定コマン ドは失敗します。  SVM が SVM ディザスタリカバリソース である場合、ログのデスティネーションパ スをルートボリュームにすることはできま せん。これは、ルートボリュームのコンテ ンツがディザスタリカバリ先にレプリケー トされないためです。  FlexCache ボリュームをログのデスティネ ーション（ONTAP 9.7 以降）として使用 することはできません。	-destination text	はい。	はい。	

<p><u> 監査するイベントのカテゴリ </u></p> <p>監査するイベントのカテゴリを指定します。監査できるイベントカテゴリは次のとおりです。</p> <ul style="list-style-type: none"> <li>• ファイルアクセスイベント（SMB と NFSv4 の両方）</li> <li>• SMBログオンおよびログオフイベント</li> <li>• 集約型アクセスポリシーのステージングイベント</li> </ul> <p>集約型アクセスポリシーのステージングイベントは、Windows Server 2012 Active Directoryドメイン以降で使用できます。</p> <ul style="list-style-type: none"> <li>• ファイル共有カテゴリイベント</li> <li>• ポリシー変更イベントの監査</li> <li>• ローカルユーザアカウント管理イベント</li> <li>• セキュリティグループ管理イベント</li> <li>• 認証ポリシー変更イベント</li> </ul> <p>デフォルトでは、ファイルアクセスイベントとSMBログオンおよびログオフイベントが監査されます。</p> <p>*注：*を指定する前に cap-staging イベントカテゴリとしては、SVMにSMBサーバが存在する必要があります。SMBサーバでダイナミックアクセス制御を有効にせずに、監査の設定で集約型アクセスポリシーのステージングを有効にすることはできますが、集約型アクセスポリシーのステージングイベントが生成されるのは、ダイナミックアクセス制御が有効になっている場合のみです。ダイナミックアクセス制御はSMBサーバオプションを使用して有効にします。デフォルトでは有効になっていません。</p>	<p>-events {file-ops</p>	<p>cifs- logon- logoff</p>	<p>cap- staging</p>	<p>file- share</p>
<p>audit-policy-change</p>	<p>user-account</p>	<p>security-group</p>	<p>authorization-policy-change }</p>	<p>いいえ</p>

		<p>_ ログフ ァイル出 力形式 _</p> <p>監査ログ の出力形 式を指定 します。 出力形式 に はONTA P固有の ものを指 定できま す XML また はMicros oft Windows EVTX ロ グ形式。 デフォル トの出力 形式はで す EVTX。</p>	<p>-format {xml</p>	<p>evtx}</p>
--	--	--	-------------------------	--------------

いいえ			<p>ログファイルのローテーションの上限 <code>_</code></p> <p>保持する監査ログファイルの数を指定します。これにより、その数からあふれた最も古いログファイルがローテーションから外されます。たとえば、の値を入力した場合などで `5` では、最後の5つのログファイルが保持されます。</p> <p>の値 0 すべてのログファイルが保持されることを示します。デフォルト値は0です。</p>	<p><code>-rotate</code>  <code>-limit</code>  integer</p>
-----	--	--	--	---

監査イベントログのローテーションをいつ行うかを決定するためのパラメータ

- ログサイズに基づいてログを回転 \*

デフォルトでは、サイズに基づいた監査ログのローテーションが行われます。

- デフォルトのログサイズは 100MB です。

- デフォルトのログローテーション方法とデフォルトのログサイズを使用する場合、ログローテーションに関する特定のパラメータを設定する必要はありません。
- ログサイズのみに基づいて監査ログのローテーションを行う場合は、次のコマンドを使用しての設定を解除します `-rotate-schedule-minute` パラメータ：`vserver audit modify -vserver vs0 -destination / -rotate-schedule-minute -`

デフォルトのログサイズを使用しない場合は、を設定できます `-rotate-size` カスタムログサイズを指定するパラメータ：

情報のタイプ	オプション	必須	含める	値を入力します
<code>_ ログファイルサイズ制限 _</code>  監査ログファイルの最大サイズを指定します。	<code>-rotate-size {integer}[KB</code>	MB	GB	TB

- スケジュールに基づいてログを回転 \*

スケジュールに基づいた監査ログのローテーションを選択した場合は、時間に基づくローテーションパラメータを任意に組み合わせて使用することで、ログのローテーションをスケジュールすることができます。

- 時間に基づくローテーションを使用する場合は、`-rotate-schedule-minute` パラメータは必須です。
- それ以外の時間ベースのローテーションパラメータは、すべてオプションです。
- ローテーションスケジュールは、時間に関連するすべての値を使用して計算されます。

たとえば、のみを指定した場合 `-rotate-schedule-minute` パラメータを指定すると、監査ログファイルのローテーションは、毎月のすべての曜日の毎時間、指定した分に行われます。

- 時間ベースのローテーションパラメータを1つまたは2つだけ指定した場合（例：`-rotate-schedule-month` および `-rotate-schedule-minutes`）を指定すると、ログファイルのローテーションは、指定した月にのみ、すべての曜日の毎時間、指定した分に行われます。

たとえば、監査ログのローテーションを、1月、3月、8月の毎週月曜日、水曜日、土曜日の10時30分に実行するように指定できます

- 両方に値を指定する場合は `-rotate-schedule-dayofweek` および `-rotate-schedule-day` では、これらは独立して考慮されます。

たとえば、を指定した場合などです `-rotate-schedule-dayofweek` 金曜日およびとして `-rotate-schedule-day 13`と指定すると、監査ログのローテーションは、13日の金曜日だけでなく、毎週金曜日と指定した月の13日にも実行されます。

- スケジュールのみに基づいて監査ログのローテーションを行う場合は、次のコマンドを使用しての設定を解除します `-rotate-size` パラメータ：`vserver audit modify -vserver vs0 -destination / -rotate-size -`

次に示す使用可能な監査パラメータのリストを使用して、監査イベントログのローテーションのスケジュール設定に使用する値を決定できます。

情報のタイプ	オプション	必須	含める	値を入力 します
<p>ログローテーションスケジュール：Month_</p> <p>監査ログのローテーションを実行する月を指定します。</p> <p>有効な値はです January から December`および `all。たとえば、監査ログのローテーションが 1 月、3 月、8 月に行われるように指定できます。</p>	-rotate-schedule-month chron_month	いいえ		
<p>ログローテーションスケジュール：曜日 _</p> <p>監査ログのローテーションを実行する日（曜日）を指定します。</p> <p>有効な値はです Sunday から Saturday`および `all。たとえば、監査ログのローテーションを火曜日と金曜日に、またはすべての曜日に実行するように指定できます。</p>	-rotate-schedule-dayofweek chron_dayofweek	いいえ		
<p>ログローテーションスケジュール：Day _</p> <p>監査ログのローテーションを実行する日にちを指定します。</p> <p>指定できる値の範囲は、です 1 から 31。たとえば、監査ログのローテーションを毎月 10 日と 20 日に、またはすべての日に実行するように指定できます。</p>	-rotate-schedule-day chron_dayofmonth	いいえ		
<p>ログローテーションスケジュール：Hour _</p> <p>監査ログのローテーションを実行する時間を決めます。</p> <p>指定できる値の範囲は、です 0（午前0時）から 23（午後11時）。を指定します all 監査ログのローテーションを1時間ごとに実行します。たとえば、監査ログのローテーションが 6（午前 6 時）と 18（午後 6 時）に行われるように指定できます。</p>	-rotate-schedule-hour chron_hour	いいえ		

<p>ログローテーションスケジュール：分 _</p> <p>監査ログのローテーションを実行する分を決めます。</p> <p>指定できる値の範囲は、です 0 終了：59。たとえば、監査ログのローテーションが 30 分に行われるように指定できます。</p>	<p>-rotate-schedule-minute chron_minute</p>	<p>スケジュールベースのログローテーションを設定している場合は Yes、それ以外の場合は No にします</p>		
--	---	---	--	--

- ログサイズとスケジュールに基づいてログを回転 \*

両方を設定すると、ログサイズとスケジュールに基づいてログファイルのローテーションを行うことができます -rotate-size パラメータと時間ベースのローテーションパラメータを任意の組み合わせで指定できます。例：if -rotate-size は10 MBに設定されており -rotate-schedule-minute が15に設定されている場合、ログファイルのサイズが10MBに達したとき、または1時間15分ごと（いずれか早い方）にログファイルがローテーションされます。

## SVM 上にファイルとディレクトリの監査の設定を作成します

監査の設定を作成します

Storage Virtual Machine （SVM）上でファイルとディレクトリの監査の設定を作成する作業には、使用可能な設定オプションの理解、設定の計画、設定の実行および有効化が含まれます。その後、監査の設定に関する情報を表示して、設定した内容が適切であることを確認できます。

ファイルおよびディレクトリイベントの監査を開始する前に、監査の設定を Storage Virtual Machine （SVM）で作成する必要があります。

作業を開始する前に

集約型アクセスポリシーステージングの監査の設定を作成する場合は、SVM上にSMBサーバが存在している必要があります。



- SMB サーバでダイナミックアクセス制御を有効にせずに、監査の設定で集約型アクセスポリシーのステージングを有効にすることはできますが、集約型アクセスポリシーのステージングイベントが生成されるのは、ダイナミックアクセス制御が有効になっている場合のみです。

ダイナミックアクセス制御はSMBサーバオプションを使用して有効にします。デフォルトでは有効になっていません。

- コマンド内のフィールドの引数が無効な場合、たとえばフィールドの無効なエントリ、重複するエントリ、存在しないエントリなどが考えられます。その場合、監査フェーズの前にコマンドが失敗します。

この場合、監査レコードは生成されません。

## このタスクについて

SVM が SVM ディザスタリカバリソースである場合、デスティネーションパスをルートボリューム上にすることはできません。

## ステップ

1. 計画ワークシートの情報を使用して、ログサイズまたはスケジュールに基づいて監査ログのローテーションを行うための監査の設定を作成します。

監査ログのローテーションの基準	入力するコマンド
ログサイズ	`vserver audit create -vserver vserver_name -destination path -events [{file-ops
cifs-logon-logoff	cap-staging
file-share	authorization-policy-change
user-account	security-group
authorization-policy-change}] [-format {xml	evtx}] [-rotate-limit integer] [-rotate-size {integer[KB
MB	GB
TB	PB]]`
スケジュール	`vserver audit create -vserver vserver_name -destination path -events [{file-ops
cifs-logon-logoff	cap-staging}] [-format {xml

## 例

次の例は、サイズに基づくローテーションを使用してファイル操作とSMBログオンおよびログオフイベント（デフォルト）を監査する監査の設定を作成します。ログの形式はです EVTX （デフォルト）。ログはに保存されます /audit\_log ディレクトリ。ログファイルの最大サイズはです 200 MB。ログのサイズが 200MB になると、ログのローテーションが実行されます。



```
cluster1::> vsserver audit create -vsserver vs1 -destination /audit_log
-rotate-size 200MB
```

次の例は、サイズに基づくローテーションを使用してファイル操作とSMBログオンおよびログオフイベント（デフォルト）を監査する監査の設定を作成します。ログの形式はです EVTX（デフォルト）。ログはに保存されます /cifs\_event\_logs ディレクトリ。ログファイルの最大サイズはです 100 MB（デフォルト）。ログのローテーションの上限はです 5：

```
cluster1::> vsserver audit create -vsserver vs1 -destination
/cifs_event_logs -rotate-limit 5
```

次の例は、時間に基づくローテーションを使用してファイル操作、CIFS ログオンおよびログオフイベント、集約型アクセスポリシーのステージングイベントを監査する監査の設定を作成します。ログの形式はです EVTX（デフォルト）。監査ログのローテーションが毎月、午後 12 時 30 分に実行されますそして毎日、午後 12 : 30 に実行されます。ログのローテーションの上限はです 5：

```
cluster1::> vsserver audit create -vsserver vs1 -destination /audit_log
-events file-ops,cifs-logon-logoff,file-share,audit-policy-change,user-
account,security-group,authorization-policy-change,cap-staging -rotate
-schedule-month all -rotate-schedule-dayofweek all -rotate-schedule-hour
12 -rotate-schedule-minute 30 -rotate-limit 5
```

## SVM で監査を有効にします

監査の設定が完了したら、Storage Virtual Machine（SVM）で監査を有効にする必要があります。

必要なもの

SVM の監査設定がすでに存在している必要があります。

このタスクについて

SVM ディザスタリカバリ ID 破棄の設定が（SnapMirror 初期化完了後に）初めて開始され、SVM に監査の設定がある場合、ONTAP は監査の設定を自動的に無効にします。読み取り専用 SVM では、ステージングボリュームがいっぱいにならないように監査が無効になっています。SnapMirror 関係が解除されて SVM が読み書き可能になったあとでないと、監査を有効にすることはできません。

ステップ

1. SVM で監査を有効にします。

```
vsserver audit enable -vsserver vsserver_name
```

```
vsserver audit enable -vsserver vs1
```

監査の設定を確認します

監査の設定が完了したら、監査が適切に設定されて有効になっていることを確認する必要があります。

手順

1. 監査の設定を確認します。

```
vserver audit show -instance -vserver vserver_name
```

次のコマンドは、Storage Virtual Machine（SVM）vs1 のすべての監査の設定の情報をリスト形式で表示します。

```
vserver audit show -instance -vserver vs1
```

```

                Vserver: vs1
            Auditing state: true
        Log Destination Path: /audit_log
Categories of Events to Audit: file-ops
                Log Format: evtX
            Log File Size Limit: 200MB
        Log Rotation Schedule: Month: -
Log Rotation Schedule: Day of Week: -
            Log Rotation Schedule: Day: -
            Log Rotation Schedule: Hour: -
Log Rotation Schedule: Minute: -
            Rotation Schedules: -
        Log Files Rotation Limit: 0
```

## ファイルおよびフォルダの監査ポリシーを設定

ファイルおよびフォルダの監査ポリシーを設定

ファイルおよびフォルダのアクセスイベントの監査は、2つのステップで実装します。まず、Storage Virtual Machine（SVM）で監査設定を作成し、有効にする必要があります。次に、監視するファイルとフォルダに対して監査ポリシーを設定する必要があります。成功したアクセス試行と失敗したアクセス試行の両方を監視するように監査ポリシーを設定できます。

SMB と NFS の両方の監査ポリシーを設定できます。SMB と NFS の監査ポリシーでは、設定の要件や監査の機能が異なります。

適切な監査ポリシーが設定されている場合、ONTAP は、SMB または NFS サーバの稼働中に限り、監査ポリシーでの指定に従って SMB および NFS アクセスイベントを監視します。

## NTFS セキュリティ形式のファイルおよびディレクトリに監査ポリシーを設定する

ファイルおよびディレクトリ操作を監査する前に、監査情報を収集するファイルおよびディレクトリに対して監査ポリシーを設定する必要があります。これは、監査の設定と有効化に加えて行います。NTFS 監査ポリシーを設定するには、Windows のセキュリティタブを使用するか、ONTAP の CLI を使用します。

### Windows のセキュリティタブを使用した NTFS 監査ポリシーの設定

Windows の [ プロパティ ] ウィンドウの [Windows セキュリティ \*] タブを使用して、ファイルおよびディレクトリの NTFS 監査ポリシーを構成できます。これは Windows クライアント上に存在するデータの監査ポリシーを設定する場合と同じ方法であり、ユーザは使い慣れたものと同じ GUI インターフェイスを使用できます。

#### 必要なもの

監査は、System Access Control List (SACL ; システムアクセス制御リスト) を適用するデータが格納されている Storage Virtual Machine (SVM) で設定する必要があります。

#### このタスクについて

NTFS 監査ポリシーの設定は、NTFS セキュリティ記述子に関連付けられている NTFS SACL にエントリを追加することによって行います。その後、セキュリティ記述子を NTFS ファイルおよびディレクトリに適用します。これらのタスクは Windows GUI によって自動的に処理されます。セキュリティ記述子には、ファイルやフォルダのアクセス権を適用するための Discretionary Access Control List (DACL ; 随意アクセス制御リスト)、ファイルやフォルダを監査するための SACL、または SACL と DACL の両方を含めることができます。

Windows のセキュリティタブを使用して NTFS 監査ポリシーを設定するには、Windows ホストで次の手順を実行します。

#### 手順

1. Windows Explorer の \* ツール \* メニューから、\* ネットワークドライブのマップ \* を選択します。
2. [ ネットワークドライブの割り当て \* ] ボックスに入力します。
  - a. ドライブ文字を選択します。
  - b. [\* フォルダ \* ] ボックスに、監査するデータと共有名を保持して、共有を含む SMB サーバー名を入力します。

SMBサーバ名の代わりに、SMBサーバのデータインターフェイスのIPアドレスを指定できます。

SMBサーバ名が「smb\_server」で、共有の名前が「share1」の場合は、と入力します  
\\SMB\_SERVER\share1。

- c. [ 完了 ] をクリックします。

選択したドライブがマウントされて使用可能な状態になり、共有内に格納されているファイルやフォルダが Windows エクスプローラウィンドウに表示されます。

3. アクセスの監査を有効にするファイルまたはディレクトリを選択します。
4. ファイルまたはディレクトリを右クリックし、\* プロパティ \* を選択します。
5. [\* セキュリティ \* ] タブを選択します。

6. 「\* 詳細設定 \*」をクリックします。
7. [ 監査 \* ] タブを選択します。
8. 次のうち必要な操作を実行します。

状況	実行する処理
新しいユーザまたはグループの監査を設定します	<ol style="list-style-type: none"> <li>a. [ 追加 ( Add ) ] をクリックします。</li> <li>b. [ 選択するオブジェクト名を入力してください ] ボックスに、追加するユーザーまたはグループの名前を入力します。</li> <li>c. [OK] をクリックします。</li> </ol>
ユーザまたはグループから監査を削除します	<ol style="list-style-type: none"> <li>a. [ 選択するオブジェクト名を入力してください ] ボックスで、削除するユーザーまたはグループを選択します。</li> <li>b. [ 削除 ( Remove ) ] をクリックします。</li> <li>c. [OK] をクリックします。</li> <li>d. この手順の残りの部分はスキップします。</li> </ol>
ユーザまたはグループの監査を変更します	<ol style="list-style-type: none"> <li>a. [ 選択するオブジェクト名を入力してください ] ボックスで、変更するユーザーまたはグループを選択します。</li> <li>b. [ 編集 ( Edit ) ] をクリックします。</li> <li>c. [OK] をクリックします。</li> </ol>

ユーザーまたはグループの監査を設定したり、既存のユーザーまたはグループの監査を変更したりする場合は、[ < オブジェクト > の監査エントリ ] ボックスが開きます。

9. [ \* 適用先 \* ] ボックスで、この監査エントリの適用方法を選択します。

次のいずれかを選択できます。

- \* このフォルダ、サブフォルダ、ファイル \*
- \* このフォルダとサブフォルダ \*
- \* このフォルダのみ \*
- \* このフォルダとファイル \*
- \* サブフォルダとファイルのみ \*
- \* サブフォルダのみ \*

- ファイルのみ

単一ファイルに対して監査を設定している場合、\*適用先\*ボックスはアクティブになりません。[ \* 適用先 \* ( Apply to \* ) ] ボックスの設定は、デフォルトで \* このオブジェクトのみ \* に設定されています。



監査では SVM リソースが使用されるので、セキュリティ要件を満たす監査イベントにするために必要な最小レベルを選択してください。

10. [ \* アクセス \* ] ボックスで、監査する対象と、成功したイベント、失敗イベント、またはその両方を監査するかどうかを選択します。

- 成功したイベントを監査するには、成功ボックスを選択します。
- 障害イベントを監査するには、[ 障害 ] ボックスを選択します。

セキュリティ要件を満たすために監視する必要がある操作のみを選択してください。これらの監査可能なイベントの詳細については、Windows のマニュアルを参照してください。次のイベントを監査できます。

- \* フルコントロール \*
- \* フォルダの移動 / ファイルの実行 \*
- \* フォルダのリスト / データの読み取り \*
- \* 属性の読み取り \*
- \* 拡張属性の読み取り \*
- \* ファイルの作成 / データの書き込み \*
- \* フォルダの作成 / データの追加 \*
- \* 属性の書き込み \*
- \* 拡張属性の書き込み \*
- \* サブフォルダとファイルの削除 \*
- \* 削除 \*
- \* 読み取り許可 \*
- \* 権限の変更 \*
- \* 所有権を取りなさい \*

11. 監査設定を元のコンテナの後続のファイルとフォルダに反映させない場合は、[ このコンテナ内のオブジェクトまたはコンテナにのみ監査エントリを適用する \* ] ボックスを選択します。

12. [ 適用 ( Apply ) ] をクリックします。

13. 監査エントリの追加、削除、または編集が完了したら、**OK** をクリックします。

[Auditing Entry for <object>] ボックスが閉じます。

14. [ 監査 \* ] ボックスで、このフォルダの継承設定を選択します。

セキュリティ要件を満たす監査イベントにするために必要な最小レベルを選択してください。次のいずれかを選択できます。

- このオブジェクトの親から継承可能な監査エントリを含めるボックスを選択します
- [ このオブジェクトから継承可能な監査エントリをすべての子の既存の継承可能な監査エントリをすべて置換する ] ボックスをオンにします
- 両方のボックスを選択します。
- どちらのボックスも選択しない。  
1 つのファイルに SACL を設定する場合は [ このオブジェクトから継承可能な監査エントリをすべての子の既存のすべての監査エントリを置換 ] ボックスが [ 監査 ] ボックスに表示されません

15. [OK] をクリックします。

[ 監査 ] ボックスが閉じます。

#### ONTAP CLI を使用して NTFS 監査ポリシーを設定する

ONTAP CLI を使用して、ファイルおよびフォルダに対して監査ポリシーを設定できます。これにより、Windows クライアントで SMB 共有を使用してデータに接続することなく NTFS 監査ポリシーを設定できます。

を使用してNTFS監査ポリシーを設定できます `vserver security file-directory` コマンドファミリー。

CLI で設定できるのは NTFS SACL だけです。NFSv4 SACL の設定は、この ONTAP コマンドファミリーではサポートされていません。これらのコマンドを使用して NTFS SACL を設定し、ファイルおよびフォルダに追加する方法については、マニュアルページを参照してください。

#### UNIX セキュリティ形式のファイルおよびディレクトリの監査を設定します

UNIX セキュリティ形式のファイルおよびディレクトリの監査を設定するには、NFSv4.x ACL に監査 ACE を追加します。これにより、セキュリティの目的で特定の NFS ファイルおよびディレクトリのアクセスイベントを監視できます。

このタスクについて

NFSv4.x では、随意 ACE とシステム ACE の両方が同じ ACL に格納されます。個別の DACL と SACL には格納されません。したがって、既存の ACL に監査 ACE を追加する場合は、既存の ACL を上書きして失われることがないように、細心の注意を払う必要があります。既存の ACL に監査 ACE を追加する順序は重要ではありません。

手順

1. を使用して、ファイルまたはディレクトリの既存のACLを取得します `nfs4_getfacl` または同等のコマンド。

ACL の操作の詳細については、NFS クライアントのマニュアルページを参照してください。

2. 目的の監査 ACE を追加します。
3. を使用して、更新したACLをファイルまたはディレクトリに適用します `nfs4_setfacl` または同等のコマンド。

ファイルおよびディレクトリに適用されている監査ポリシーに関する情報を表示します

#### Windows のセキュリティタブを使用して、監査ポリシーに関する情報を表示します

Windows のプロパティウィンドウのセキュリティタブを使用して、ファイルおよびディレクトリに適用されている監査ポリシーに関する情報を表示できます。これは Windows サーバ上に存在するデータの場合と同じ方法であり、ユーザは使い慣れたものと同じ GUI インターフェイスを使用できます。

このタスクについて

ファイルやディレクトリに適用されている監査ポリシーに関する情報を表示すると、指定したファイルやフォルダに適切なシステムアクセス制御リスト（SACL）が設定されていることを確認できます。

NTFS ファイルおよびフォルダに適用されている SACL に関する情報を表示するには、Windows ホストで次の手順を実行します。

#### 手順

1. Windows Explorer の \* ツール \* メニューから、\* ネットワークドライブのマップ \* を選択します。
2. [\* ネットワークドライブの割り当て \*] ダイアログボックスに入力します。
  - a. ドライブ文字を選択します。
  - b. [フォルダ]ボックスに、監査するデータが格納されている共有を含むStorage Virtual Machine（SVM）のIPアドレスまたはSMBサーバ名と、共有の名前を入力します。

SMBサーバ名が「smb\_server」で、共有の名前が「share1」の場合は、と入力します  
\\SMB\_SERVER\share1。



SMBサーバ名の代わりに、SMBサーバのデータインターフェイスのIPアドレスを指定できます。

- c. [完了] をクリックします。

選択したドライブがマウントされて使用可能な状態になり、共有内に格納されているファイルやフォルダが Windows エクスプローラウィンドウに表示されます。

3. 監査情報を表示するファイルまたはディレクトリを選択します。
4. ファイルまたはディレクトリを右クリックし、\* プロパティ \* を選択します。
5. [\* セキュリティ \*] タブを選択します。
6. 「\* 詳細設定 \*」をクリックします。
7. [監査 \*] タブを選択します。
8. [\* Continue（続行）] をクリックします

[監査] ボックスが開きます。[監査エントリ \*] ボックスには、SACL が適用されているユーザーとグループの概要が表示されます。

9. [\* 監査エントリ \*] ボックスで、SACL エントリを表示するユーザーまたはグループを選択します。
10. [編集（Edit）] をクリックします。

[< オブジェクト > の監査エントリ] ボックスが開きます。

11. [\* アクセス \*（\* Access \*）] ボックスで、選択したオブジェクトに適用されている現在の SACL を表示します。
12. [\* キャンセル \*] をクリックして、[\* 監査エントリ for < オブジェクト > \*] ボックスを閉じます。
13. [\* キャンセル \*] をクリックして、[\* 監査 \*] ボックスを閉じます。

CLI を使用して、FlexVol の NTFS 監査ポリシーに関する情報を表示する

セキュリティ形式と有効なセキュリティ形式、適用されているアクセス権、システムアクセス制御リストに関する情報など、FlexVol の NTFS 監査ポリシーに関する情報を表示できます。この情報を使用して、セキュリティ設定の検証や、監査に関する問題のトラブルシューティングを行うことができます。

このタスクについて

ファイルやディレクトリに適用されている監査ポリシーに関する情報を表示すると、指定したファイルやフォルダに適切なシステムアクセス制御リスト（SACL）が設定されていることを確認できます。

Storage Virtual Machine（SVM）の名前、および監査情報を表示するファイルまたはフォルダのパスを指定する必要があります。出力は要約形式または詳細なリストで表示できます。

- NTFS セキュリティ形式のボリュームおよび qtree では、NTFS のシステムアクセス制御リスト（SACL）のみが監査ポリシーに使用されます。
- NTFS 対応のセキュリティが有効な mixed セキュリティ形式のボリューム内のファイルおよびフォルダには、NTFS 監査ポリシーを適用できます。

mixed セキュリティ形式のボリュームおよび qtree には、UNIX ファイル権限、モードビットまたは NFSv4 ACL、および NTFS ファイル権限を使用する一部のファイルおよびディレクトリを含めることができます。

- mixed セキュリティ形式のボリュームの最上位では、UNIX または NTFS 対応のセキュリティを有効にすることができ、そこには NTFS SACL が格納されている場合も、格納されていない場合もあります。
- ストレージレベルのアクセス保護セキュリティは、ボリュームのルートまたは qtree の有効なセキュリティ形式が UNIX であっても、mixed セキュリティ形式のボリュームまたは qtree で設定できるため、ストレージレベルのアクセス保護が設定されているボリュームまたは qtree パスの出力には、通常のファイルおよびフォルダの NFSv4 SACL とストレージレベルのアクセス保護の NTFS SACL の両方が表示される場合があります。
- コマンドで入力したパスが、NTFS 対応のセキュリティを使用するデータへのパスである場合、そのファイルまたはディレクトリパスにダイナミックアクセス制御が設定されていれば、ダイナミックアクセス制御 ACE に関する情報も出力に表示されます。
- NTFS 対応のセキュリティが有効なファイルおよびフォルダに関するセキュリティ情報を表示する場合、UNIX 関連の出力フィールドには表示専用の UNIX ファイル権限情報が格納されます。

ファイルアクセス権の決定時、NTFS セキュリティ形式のファイルおよびフォルダでは、NTFS ファイルアクセス権と Windows ユーザおよびグループのみが使用されます。

- ACL 出力は、NTFS または NFSv4 セキュリティが適用されたファイルとフォルダについてのみ表示されます。

このフィールドは、モードビットのアクセス権のみ（NFSv4 ACL はなし）が適用されている UNIX セキュリティ形式のファイルおよびフォルダでは空になります。

- ACL 出力の所有者とグループの出力フィールドは、NTFS セキュリティ記述子の場合にのみ適用されず。

ステップ

1. ファイルおよびディレクトリ監査ポリシー設定を必要な詳細レベルで表示します。



表示する情報	入力するコマンド
要約形式で表示されます	<code>vserver security file-directory show -vserver vserver_name -path path</code>
詳細なリストとして	<code>vserver security file-directory show -vserver vserver_name -path path -expand-mask true</code>

## 例

次の例は、パスの監査ポリシーの情報を表示します /corp (SVM vs1)。パスで NTFS 対応のセキュリティが有効になっています。NTFS セキュリティ記述子には、SUCCESS および SUCCESS/FAIL SACL エントリの両方が含まれています。

```
cluster::> vserver security file-directory show -vserver vs1 -path /corp
      Vserver: vs1
      File Path: /corp
      File Inode Number: 357
      Security Style: ntfs
      Effective Style: ntfs
      DOS Attributes: 10
      DOS Attributes in Text: ----D---
      Expanded Dos Attributes: -
      Unix User Id: 0
      Unix Group Id: 0
      Unix Mode Bits: 777
      Unix Mode Bits in Text: rwxrwxrwx
      ACLs: NTFS Security Descriptor
      Control:0x8014
      Owner:DOMAIN\Administrator
      Group:BUILTIN\Administrators
      SACL - ACEs
      ALL-DOMAIN\Administrator-0x100081-OI|CI|SA|FA
      SUCCESSFUL-DOMAIN\user1-0x100116-OI|CI|SA
      DACL - ACEs
      ALLOW-BUILTIN\Administrators-0x1f01ff-OI|CI
      ALLOW-BUILTIN\Users-0x1f01ff-OI|CI
      ALLOW-CREATOR OWNER-0x1f01ff-OI|CI
      ALLOW-NT AUTHORITY\SYSTEM-0x1f01ff-OI|CI
```

次の例は、パスの監査ポリシーの情報を表示します /datavol1 (SVM vs1)。このパスには、標準ファイルおよびフォルダの SACL とストレージレベルのアクセス保護の SACL の両方が格納されています。

```

cluster::> vsriver security file-directory show -vsriver vs1 -path
/datavol1

      Vserver: vs1
      File Path: /datavol1
      File Inode Number: 77
      Security Style: ntfs
      Effective Style: ntfs
      DOS Attributes: 10
      DOS Attributes in Text: ----D---
      Expanded Dos Attributes: -
      Unix User Id: 0
      Unix Group Id: 0
      Unix Mode Bits: 777
      Unix Mode Bits in Text: rwxrwxrwx
      ACLs: NTFS Security Descriptor
            Control:0xaa14
            Owner: BUILTIN\Administrators
            Group: BUILTIN\Administrators
            SACL - ACEs
              AUDIT-EXAMPLE\marketing-0xf01ff-OI|CI|FA
            DACL - ACEs
              ALLOW-EXAMPLE\Domain Admins-0x1f01ff-OI|CI
              ALLOW-EXAMPLE\marketing-0x1200a9-OI|CI

      Storage-Level Access Guard security
      SACL (Applies to Directories):
        AUDIT-EXAMPLE\Domain Users-0x120089-FA
        AUDIT-EXAMPLE\engineering-0x1f01ff-SA
      DACL (Applies to Directories):
        ALLOW-EXAMPLE\Domain Users-0x120089
        ALLOW-EXAMPLE\engineering-0x1f01ff
        ALLOW-NT AUTHORITY\SYSTEM-0x1f01ff
      SACL (Applies to Files):
        AUDIT-EXAMPLE\Domain Users-0x120089-FA
        AUDIT-EXAMPLE\engineering-0x1f01ff-SA
      DACL (Applies to Files):
        ALLOW-EXAMPLE\Domain Users-0x120089
        ALLOW-EXAMPLE\engineering-0x1f01ff
        ALLOW-NT AUTHORITY\SYSTEM-0x1f01ff

```

ファイルセキュリティと監査ポリシーに関する情報を表示する方法

ワイルドカード文字（\*）を使用すると、特定のパスまたはルートボリュームの下にあるすべてのファイルおよびディレクトリのファイルセキュリティと監査ポリシーに関する

る情報を表示できます。

ワイルドカード文字（\*）は、すべてのファイルおよびディレクトリの情報を表示する特定のディレクトリパスの最後のサブコンポーネントとして使用できます。

という名前の特定のファイルまたはディレクトリの情報を表示する場合は、パス全体を二重引用符（" "）で囲む必要があります。

例

次のコマンドにワイルドカード文字を指定すると、パスの下にあるすべてのファイルとディレクトリに関する情報が表示されます /1/ SVM vs1：

```

cluster::> vserver security file-directory show -vserver vs1 -path /1/*

      Vserver: vs1
      File Path: /1/1
      Security Style: mixed
      Effective Style: ntfs
      DOS Attributes: 10
      DOS Attributes in Text: ----D---
      Expanded Dos Attributes: -
      Unix User Id: 0
      Unix Group Id: 0
      Unix Mode Bits: 777
      Unix Mode Bits in Text: rwxrwxrwx
      ACLs: NTFS Security Descriptor
            Control:0x8514
            Owner:BUILTIN\Administrators
            Group:BUILTIN\Administrators
            DACL - ACEs
            ALLOW-Everyone-0x1f01ff-OI|CI (Inherited)

      Vserver: vs1
      File Path: /1/1/abc
      Security Style: mixed
      Effective Style: ntfs
      DOS Attributes: 10
      DOS Attributes in Text: ----D---
      Expanded Dos Attributes: -
      Unix User Id: 0
      Unix Group Id: 0
      Unix Mode Bits: 777
      Unix Mode Bits in Text: rwxrwxrwx
      ACLs: NTFS Security Descriptor
            Control:0x8404
            Owner:BUILTIN\Administrators
            Group:BUILTIN\Administrators
            DACL - ACEs
            ALLOW-Everyone-0x1f01ff-OI|CI (Inherited)

```

次のコマンドは、パスの下に「\*」という名前のファイルの情報を表示します /vol1/a SVM vs1の。パスは二重引用符 ("" ) で囲まれます。

```
cluster::> vservers security file-directory show -vservers vs1 -path  
"/vol1/a/*"
```

```
      Vserver: vs1  
      File Path: "/vol1/a/*"  
      Security Style: mixed  
      Effective Style: unix  
      DOS Attributes: 10  
      DOS Attributes in Text: ----D---  
      Expanded Dos Attributes: -  
      Unix User Id: 1002  
      Unix Group Id: 65533  
      Unix Mode Bits: 755  
      Unix Mode Bits in Text: rwxr-xr-x  
      ACLs: NFSV4 Security Descriptor  
      Control:0x8014  
      SACL - ACEs  
      AUDIT-EVERYONE@-0x1f01bf-FI|DI|SA|FA  
      DACL - ACEs  
      ALLOW-EVERYONE@-0x1f00a9-FI|DI  
      ALLOW-OWNER@-0x1f01ff-FI|DI  
      ALLOW-GROUP@-0x1200a9-IG
```

## 監査できる CLI 変更イベント

### 監査可能な CLI 変更イベントの概要

ONTAP は、特定の SMB 共有イベント、監査ポリシーイベント、ローカルセキュリティグループイベント、ローカルユーザグループイベント、認証ポリシーイベントなどの CLI 変更イベントを監査できます。どのような変更イベントを監査できるか理解しておく、イベントログの結果を解釈するときに役立ちます。

Storage Virtual Machine（SVM）で監査する CLI 変更イベントの管理作業として、手動での監査ログのローテーション、監査の有効化と無効化、監査対象変更イベントに関する情報の表示、監査対象変更イベントの変更、監査対象変更イベントの削除が可能です。

管理者が、SMB 共有、ローカルユーザグループ、ローカルセキュリティグループ、認証ポリシー、および監査ポリシーのイベントに関連する設定を変更するコマンドを実行する場合、レコードが生成され、対応するイベントが監査されます。

監査カテゴリ	イベント	イベント IDs	実行するコマンド
Mhost 監査	ポリシー変更	[4719] 監査設定が変更されました	`vservers audit disable`

enable	modify`	ファイル共有	[5142] ネットワーク共有が追加されました
vserver cifs share create	[5143] ネットワーク共有の変更	vserver cifs share modify `vserver cifs share create	modify
delete` `vserver cifs share add	remove`	[5144] ネットワーク共有が削除されました	vserver cifs share delete
監査	ユーザアカウント	[4720] ローカルユーザの作成	vserver cifs users-and-groups local-user create vserver services name-service unix-user create
[4722] ローカルユーザの有効化	`vserver cifs users-and-groups local-user create	modify`	[4724] ローカルユーザのパスワードのリセット
vserver cifs users-and-groups local-user set-password	[4725] ローカルユーザの無効化	`vserver cifs users-and-groups local-user create	modify`
[4726] ローカルユーザの削除	vserver cifs users-and-groups local-user delete vserver services name-service unix-user delete	[4738] ローカルユーザの変更	vserver cifs users-and-groups local-user modify vserver services name-service unix-user modify
[4781] ローカルユーザの名前変更	vserver cifs users-and-groups local-user rename	セキュリティグループ	[4731] ローカルセキュリティグループが作成されました
vserver cifs users-and-groups local-group create vserver services name-service unix-group create	[4734] ローカルセキュリティグループが削除されました	vserver cifs users-and-groups local-group delete vserver services name-service unix-group delete	[4735] ローカルセキュリティグループの変更

<code>`vserver cifs users-and-groups local-group rename</code>	<code>modify` vserver services name-service unix-group modify</code>	[4732] ローカルグループへのユーザの追加	<code>vserver cifs users-and-groups local-group add-members vserver services name-service unix-group adduser</code>
[4733] ローカルグループからユーザが削除されました	<code>vserver cifs users-and-groups local-group remove-members vserver services name-service unix-group deluser</code>	認証ポリシー変更	[4704] ユーザ権限の割り当て
<code>vserver cifs users-and-groups privilege add-privilege</code>	[4705] ユーザ権限が削除されました	<code>`vserver cifs users-and-groups privilege remove-privilege</code>	<code>reset-privilege`</code>

## ファイル共有イベントの管理

Storage Virtual Machine（SVM）に対してファイル共有イベントが設定されている場合、監査を有効にしたときに、それらについての監査イベントが生成されます。ファイル共有イベントは、を使用してSMBネットワーク共有が変更された場合に生成されます `vserver cifs share` 関連コマンド。

ファイル共有イベントは、SVMに対してSMBネットワーク共有が追加、変更、または削除されたときに生成されます。イベントIDは5142、5143、および5144です。SMBネットワーク共有の設定はを使用して変更します `cifs share access control create|modify|delete` コマンド

次の例では、「audit\_dest」という名前の共有オブジェクトが作成され、ID 5143 のファイル共有イベントが生成されています。

```

netapp-clus1::*> cifs share create -share-name audit_dest -path
/audit_dest
- System
  - Provider
    [ Name]   NetApp-Security-Auditing
    [ Guid]   {3CB2A168-FE19-4A4E-BDAD-DCF422F13473}
    EventID   5142
    EventName  Share Object Added
    ...
    ...
    ShareName  audit_dest
    SharePath  /audit_dest
    ShareProperties oplocks;browsable;changenotify;show-previous-versions;
    SD O:BAG:S-1-5-21-2447422786-1297661003-4197201688-513D:(A;;FA;;;WD)

```

## 監査ポリシー変更イベントの管理

Storage Virtual Machine（SVM）に対して監査ポリシー変更イベントが設定されている場合、監査を有効にしたときに、それらについての監査イベントが生成されます。監査ポリシー変更イベントは、を使用して監査ポリシーが変更されたときに生成されます  
vserver audit 関連コマンド。

監査ポリシー変更イベントは、監査ポリシーが無効化、有効化、または変更されたときに生成されます。イベント ID は 4719 です。このイベントは、ユーザが監査を無効にしようとしたときに状況を追跡するのに役立ちます。このイベントはデフォルトで設定されており、無効にするには diagnostic 権限が必要です。

次の例では、監査が無効になったときに、ID 4719 の監査ポリシー変更イベントが生成されています。

```

netapp-clus1::*> vserver audit disable -vserver vserver_1
- System
  - Provider
    [ Name]   NetApp-Security-Auditing
    [ Guid]   {3CB2A168-FE19-4A4E-BDAD-DCF422F13473}
    EventID   4719
    EventName  Audit Disabled
    ...
    ...
    SubjectUserName admin
    SubjectUserSid 65533-1001
    SubjectDomainName ~
    SubjectIP console
    SubjectPort

```



ユーザアカウントイベントを管理します

Storage Virtual Machine（SVM）に対してユーザアカウントイベントが設定されている場合、監査を有効にしたときに、それらについての監査イベントが生成されます。

イベントID 4720、4722、4724、4725、4726のユーザアカウントイベント 4738および4781は、ローカルSMBまたはNFSユーザがシステムから作成または削除されたとき、ローカルユーザアカウントが有効化、無効化または変更されたとき、ローカルSMBユーザパスワードがリセットまたは変更されたときに生成されます。ユーザアカウントイベントは、を使用してユーザアカウントが変更されたときに生成されます  
vserver cifs users-and-groups <local user> および vserver services name-service <unix user> コマンド

次の例では、ローカルSMBユーザが作成され、ID 4720のユーザアカウントイベントが生成されています。

```
netapp-clus1::*> vserver cifs users-and-groups local-user create -user
-name testuser -is-account-disabled false -vserver vserver_1
Enter the password:
Confirm the password:

- System
- Provider
  [ Name]   NetApp-Security-Auditing
  [ Guid]   {3CB2A168-FE19-4A4E-BDAD-DCF422F13473}
EventID 4720
EventName Local Cifs User Created
...
...
TargetUserName testuser
TargetDomainName NETAPP-CLUS1
TargetSid S-1-5-21-2447422786-1297661003-4197201688-1003
TargetType CIFS
DisplayName testuser
PasswordLastSet 1472662216
AccountExpires NO
PrimaryGroupId 513
UserAccountControl %%0200
SidHistory ~
PrivilegeList ~
```

次の例では、上記の例で作成されたローカルSMBユーザの名前が変更され、ID 4781のユーザアカウントイベントが生成されています。

```

netapp-clus1::*> vserver cifs users-and-groups local-user rename -user
-name testuser -new-user-name testuser1
- System
- Provider
  [ Name]   NetApp-Security-Auditing
  [ Guid]   {3CB2A168-FE19-4A4E-BDAD-DCF422F13473}
  EventID  4781
  EventName Local Cifs User Renamed
  ...
  ...
  OldTargetUserName testuser
  NewTargetUserName testuser1
  TargetDomainName NETAPP-CLUS1
  TargetSid S-1-5-21-2447422786-1297661003-4197201688-1000
  TargetType CIFS
  SidHistory ~
  PrivilegeList ~

```

## セキュリティグループイベントの管理

Storage Virtual Machine（SVM）に対してセキュリティグループイベントが設定されている場合、監査を有効にしたときに、それらについての監査イベントが生成されます。

セキュリティグループイベントは、システムのローカル SMB グループまたは NFS グループが作成または削除されたとき、それらのグループのローカルユーザが追加または削除されたときに生成されます。イベント ID は 4731、4732、4733、4734、および 4735 です。セキュリティグループイベントは、を使用してユーザアカウントが変更された場合に生成されます `vserver cifs users-and-groups <local-group>` および `vserver services name-service <unix-group>` コマンド

次の例では、ローカル UNIX セキュリティグループが作成され、ID 4731 のセキュリティグループイベントが生成されています。

```
netapp-clus1::*> vserver services name-service unix-group create -name
testunixgroup -id 20
- System
- Provider
  [ Name]   NetApp-Security-Auditing
  [ Guid]   {3CB2A168-FE19-4A4E-BDAD-DCF422F13473}
  EventID  4731
  EventName Local Unix Security Group Created
  ...
  ...
  SubjectUserName admin
  SubjectUserSid 65533-1001
  SubjectDomainName ~
  SubjectIP console
  SubjectPort
  TargetUserName testunixgroup
  TargetDomainName
  TargetGid 20
  TargetType NFS
  PrivilegeList ~
  GidHistory ~
```

認証ポリシー変更イベントを管理します

Storage Virtual Machine（SVM）に対して認証ポリシー変更イベントが設定されている場合、監査を有効にしたときに、それらについての監査イベントが生成されます。

認証ポリシー変更イベントは、SMB ユーザおよび SMB グループに対する認証権限が付与または取り消されたときに生成されます。イベント ID は 4704 および 4705 です。認証ポリシー変更イベントは、を使用して認証権限が割り当てられた場合または取り消された場合に生成されます `vserver cifs users-and-groups privilege` 関連コマンド。

次の例では、SMB ユーザグループの認証権限が割り当てられている場合に、ID 4704 の認証ポリシーイベントが生成されています。

```

netapp-clus1::*> vserver cifs users-and-groups privilege add-privilege
-user-or-group-name testcifslocalgroup -privileges *
- System
- Provider
  [ Name]   NetApp-Security-Auditing
  [ Guid]   {3CB2A168-FE19-4A4E-BDAD-DCF422F13473}
  EventID  4704
  EventName User Right Assigned
  ...
  ...
  TargetUserOrGroupName testcifslocalgroup
  TargetUserOrGroupName NETAPP-CLUS1
  TargetUserOrGroupSid  S-1-5-21-2447422786-1297661003-4197201688-1004;
  PrivilegeList
  SeTcbPrivilege;SeBackupPrivilege;SeRestorePrivilege;SeTakeOwnershipPrivile
ge;SeSecurityPrivilege;SeChangeNotifyPrivilege;
  TargetType  CIFS

```

## 監査の設定を管理します

監査イベントログの手動ローテーションを行います

監査イベントログは、表示する前に、ユーザが読解可能な形式に変換する必要があります。ONTAP によるログの自動ローテーション前に、特定の Storage Virtual Machine (SVM) のイベントログを表示する場合は、その SVM で監査イベントログの手動ローテーションを行うことができます。

### ステップ

1. を使用して、監査イベントログのローテーションを行います `vserver audit rotate-log` コマンドを実行します

```
vserver audit rotate-log -vserver vs1
```

監査イベントログは、監査の設定で指定されている形式で、SVMの監査イベントログディレクトリに保存されます (XML または EVTX) をクリックし、適切なアプリケーションを使用して表示できます。

### SVM での監査を有効または無効にします

Storage Virtual Machine (SVM) での監査を有効または無効にすることができます。必要に応じて、監査を無効にすることで、ファイルおよびディレクトリの監査を一時的に停止できます。監査はいつでも有効にできます (監査の設定が存在する場合)。

### 必要なもの

SVM で監査を有効にするには、SVM の監査の設定がすでに存在する必要があります。

"監査の設定を作成します"

このタスクについて  
監査を無効にしても、監査の設定は削除されません。

手順

- 1. 適切なコマンドを実行します。

監査の設定	入力するコマンド
有効	<code>vserver audit enable -vserver vserver_name</code>
無効	<code>vserver audit disable -vserver vserver_name</code>

- 2. 監査が目的の状態になっていることを確認します。

```
vserver audit show -vserver vserver_name
```

例

次の例は、SVM vs1 で監査を有効にします。

```
cluster1::> vserver audit enable -vserver vs1

cluster1::> vserver audit show -vserver vs1

Vserver: vs1
Auditing state: true
Log Destination Path: /audit_log
Categories of Events to Audit: file-ops, cifs-logon-logoff
Log Format: evtv
Log File Size Limit: 100MB
Log Rotation Schedule: Month: -
Log Rotation Schedule: Day of Week: -
Log Rotation Schedule: Day: -
Log Rotation Schedule: Hour: -
Log Rotation Schedule: Minute: -
Rotation Schedules: -
Log Files Rotation Limit: 10
```

次の例は、SVM vs1 で監査を無効にします。

```
cluster1::> vserver audit disable -vserver vs1

Vserver: vs1
Auditing state: false
Log Destination Path: /audit_log
Categories of Events to Audit: file-ops, cifs-logon-logoff
Log Format: evtv
Log File Size Limit: 100MB
Log Rotation Schedule: Month: -
Log Rotation Schedule: Day of Week: -
Log Rotation Schedule: Day: -
Log Rotation Schedule: Hour: -
Log Rotation Schedule: Minute: -
Rotation Schedules: -
Log Files Rotation Limit: 10
```

監査の設定に関する情報を表示します

監査の設定に関する情報を表示できます。この情報は、各 SVM で適切な設定が使用されているかどうか確認するのに役立ちます。また、表示される情報から、監査の設定が有効になっているかどうかを確認することもできます。

このタスクについて

すべての SVM の監査の設定に関する詳細情報を表示することも、オプションのパラメータを指定して、出力に表示される情報をカスタマイズすることもできます。オプションのパラメータを何も指定しない場合、次の情報が表示されます。

- 監査の設定が適用される SVM の名前
- 監査の状態。になります true または false

監査の状態がの場合 `true` 監査が有効になっています。監査の状態がの場合 `false` 監査は無効になっています。

- 監査するイベントのカテゴリ
- 監査ログの形式
- 統合および変換された監査ログが監査サブシステムによって格納されるターゲットディレクトリ

ステップ

1. を使用して、監査の設定に関する情報を表示します `vserver audit show` コマンドを実行します

コマンドの使用の詳細については、マニュアルページを参照してください。

例

次の例は、すべての SVM の監査の設定の概要を表示したものです。

```
cluster1::> vsserver audit show
```

Vserver	State	Event Types	Log Format	Target Directory
vs1	false	file-ops	evtx	/audit_log

次の例は、すべての SVM の監査の設定情報をリスト形式で表示したものです。

```
cluster1::> vsserver audit show -instance
```

```
                Vserver: vs1
            Auditing state: true
        Log Destination Path: /audit_log
Categories of Events to Audit: file-ops
            Log Format: evtx
            Log File Size Limit: 100MB
    Log Rotation Schedule: Month: -
Log Rotation Schedule: Day of Week: -
        Log Rotation Schedule: Day: -
        Log Rotation Schedule: Hour: -
    Log Rotation Schedule: Minute: -
            Rotation Schedules: -
        Log Files Rotation Limit: 0
```

#### 監査の設定を変更するコマンド

監査設定を変更する場合は、ログのデスティネーションパスおよび形式の変更、監査するイベントのカテゴリの変更、ログファイルの自動保存方法、保存するログファイルの最大数の指定など、現在の設定をいつでも変更できます。

状況	使用するコマンド
ログデスティネーションパスを変更します	<code>vsserver audit modify</code> を使用 <code>-destination</code> パラメータ
監査するイベントのカテゴリを変更します	<code>vsserver audit modify</code> を使用 <code>-events</code> パラメータ <div> 集約型アクセスポリシーのステージングイベントを監査するには、Dynamic Access Control (DAC; ダイナミックアクセス制御) SMBサーバオプションがStorage Virtual Machine (SVM) で有効になっている必要があります。</div>

ログ形式を変更します	<code>vserver audit modify</code> を使用 <code>-format</code> パラメータ
内部的な一時ログファイルサイズに基づいた自動保存の有効化	<code>vserver audit modify</code> を使用 <code>-rotate-size</code> パラメータ
時間間隔に基づいた自動保存の有効化	<code>vserver audit modify</code> を使用 <code>-rotate -schedule-month</code> 、 <code>-rotate-schedule-dayofweek</code> 、 <code>-rotate-schedule-day</code> 、 <code>-rotate-schedule-hour`および`-rotate-schedule-minute</code> パラメータ
保存されるログファイルの最大数の指定	<code>vserver audit modify</code> を使用 <code>-rotate-limit</code> パラメータ

監査の設定を削除します

Storage Virtual Machine（SVM）でのファイルおよびディレクトリイベントの監査が必要なくなり、SVM で監査の設定を維持する必要がなくなった場合は、監査の設定を削除できます。

手順

1. 監査の設定を無効にします。

```
vserver audit disable -vserver vserver_name

vserver audit disable -vserver vs1
```

2. 監査の設定を削除します。

```
vserver audit delete -vserver vserver_name

vserver audit delete -vserver vs1
```

クラスタリバートの影響を理解する

クラスタのリバートを予定している場合は、監査が有効になっている Storage Virtual Machine（SVM）がクラスタ内に存在するときに ONTAP が従うリバートのプロセスに注意する必要があります。リバートを行う前に特定の操作を実行する必要があります。

**SMB**のログオンおよびログオフイベントと集約型アクセスポリシーのステージングイベントの監査をサポートしていないバージョンの**ONTAP**へのリバート

SMBのログオンおよびログオフイベントと集約型アクセスポリシーのステージングイベントのサポートは、clustered Data ONTAP 8.3から開始されました。これらのイベントタイプをサポートしていないバージョンの ONTAP へのリバートを予定していて、これらのイベントタイプを監視する監査が設定されている場合は、リバートを行う前に、監査が有効になっている SVM の監査の設定を変更する必要があります。設定は、



ファイル操作イベントのみが監査されるように変更する必要があります。

## 監査およびステージング用のボリュームのスペースに関する問題のトラブルシューティングを行います

ステージングボリュームや監査イベントログを格納するボリュームに十分なスペースがない場合、問題が発生することがあります。十分なスペースがないと新しい監査レコードを作成できないため、クライアントからデータにアクセスできず、アクセス要求が失敗します。ボリュームのスペースに関するこれらの問題について、トラブルシューティングを行って解決する方法を確認しておく必要があります。

### イベントログボリュームに関連するスペースの問題のトラブルシューティングを行います

イベントログファイルを含むボリュームでスペースが不足すると、監査でログレコードをログファイルに変換できなくなります。その結果、クライアントアクセスに失敗します。イベントログボリュームのスペースに関する問題のトラブルシューティング方法を把握しておく必要があります。

- Storage Virtual Machine (SVM) 管理者およびクラスタ管理者は、ボリュームとアグリゲートの使用量と設定に関する情報を表示して、ボリュームでスペースが不足していないかを確認できます。
- イベントログを含むボリュームでスペースが不足している場合、SVM 管理者およびクラスタ管理者は、いくつかのイベントログファイルを削除するかボリュームのサイズを大きくすることで、スペースに関する問題を解決できます。



イベントログボリュームを含むアグリゲートがいっぱいになっている場合は、ボリュームのサイズを大きくする前に、アグリゲートのサイズを大きくする必要があります。アグリゲートのサイズを大きくすることができるのは、クラスタ管理者だけです。

- 監査の設定を変更して、イベントログファイルのデスティネーションパスを別のボリューム上のディレクトリに変更できます。

次の場合、データアクセスは拒否されます。



- デスティネーションディレクトリが削除されている場合。
- デスティネーションディレクトリをホストするボリュームのファイルリミットが最大レベルに達している場合。

### 詳細情報：

- ["ボリュームに関する情報の表示方法とボリュームサイズの拡張方法"](#)。
- ["アグリゲートに関する情報の表示方法とアグリゲートの管理方法"](#)。

### ステージングボリュームに関するスペースの問題のトラブルシューティングを行います

Storage Virtual Machine (SVM) のステージングファイルを含むボリュームのいずれかでスペースが不足すると、監査でログレコードをステージングファイルに書き込むことができなくなります。その結果、クライアントアクセスに失敗します。この問題のトラブルシューティングを行うには、ボリュームの使用量に関する情報を表示して、SVM で使用されているステージングボリュームのいずれかがいっぱいになっていないかを確認する必要があります。

統合イベントログファイルを含むボリュームに十分なスペースがあるにもかかわらず、スペース不足が原因でクライアントアクセスに失敗する場合は、ステージングボリュームでスペースが不足している可能性があります。SVM 管理者は、クラスタ管理者に問い合わせ、SVM のステージングファイルを含むステージングボリュームでスペースが不足していないかを確認する必要があります。ステージングボリュームのスペース不足が原因で監査イベントを生成できない場合は、監査サブシステムによって EMS イベントが生成されます。次のメッセージが表示されます。No space left on device。ステージングボリュームに関する情報を表示できるのは、クラスタ管理者だけです。SVM 管理者はこの操作を実行できません

すべてのステージングボリューム名はで始まります MDV\_aud\_ そのあとに、ステージングボリュームを含むアグリゲートのUUIDが続きます。次に、管理 SVM 上にある 4 個のシステムボリュームの例を示します。これらのボリュームは、クラスタ内でデータ SVM のファイルサービスの監査の設定の作成時に自動的に作成されたものです。

```
cluster1:> volume show -vserver cluster1
```

Vserver	Volume	Aggregate	State	Type	Size	Available
Used%						
-----	-----	-----	-----	-----	-----	-----
-----						
cluster1	MDV_aud_1d0131843d4811e296fc123478563412					
		aggr0	online	RW	2GB	1.90GB
5%						
cluster1	MDV_aud_8be27f813d7311e296fc123478563412					
		root_vs0	online	RW	2GB	1.90GB
5%						
cluster1	MDV_aud_9dc4ad503d7311e296fc123478563412					
		aggr1	online	RW	2GB	1.90GB
5%						
cluster1	MDV_aud_a4b887ac3d7311e296fc123478563412					
		aggr2	online	RW	2GB	1.90GB
5%						

4 entries were displayed.

ステージングボリュームでスペースが不足している場合は、ボリュームのサイズを大きくすることで、スペースに関する問題を解決できます。



ステージングボリュームを含むアグリゲートがいっぱいになっている場合は、ボリュームのサイズを大きくする前に、アグリゲートのサイズを大きくする必要があります。アグリゲートのサイズを拡張できるのは、クラスタ管理者だけです。SVM 管理者はこの操作を行うことができません

使用可能なスペースが 2GB 未満のアグリゲートがあると、SVM の監査の作成に失敗します。SVM の監査の作成に失敗した場合、作成されたステージングボリュームは削除されます。

## SVM で FPolicy を使用してファイルを監視および管理します

## FPolicyについて

### FPolicy 解決策の 2 つの要素とは何ですか

FPolicyは、パートナーソリューションを通じてStorage Virtual Machine（SVM）上のファイルアクセスイベントの監視と管理に使用されるファイルアクセス通知フレームワークです。パートナーソリューションは、データガバナンスとコンプライアンス、ランサムウェア対策、データモビリティなど、さまざまなユースケースへの対応を支援します。

パートナーソリューションには、NetAppがサポートするサードパーティソリューションとNetApp製品のワークロードセキュリティとCloud Data Senseの両方が含まれます。

FPolicy 解決策は 2 つの部分で構成されます。ONTAP FPolicyフレームワークは、クラスタでのアクティビティを管理し、パートナーアプリケーション（外部FPolicyサーバ）に通知を送信します。外部FPolicyサーバは、お客様のユースケースに対応するために、ONTAP FPolicyから送信された通知を処理します。

ONTAP フレームワークは、FPolicy の設定の作成と管理、ファイルイベントの監視、および外部 FPolicy サーバへの通知の送信を行います。ONTAP FPolicy は、外部 FPolicy サーバと Storage Virtual Machine （SVM）ノードの間の通信を可能にするインフラを提供します。

FPolicy フレームワークでは、外部 FPolicy サーバへの接続を確立し、クライアントアクセスによって特定のファイルシステムイベントが発生した場合に FPolicy サーバに通知を送信します。外部 FPolicy サーバは、それらの通知を処理し、ノードに応答を送信します。通知処理の結果として実行される処理は、アプリケーションごとに異なるほか、ノードと外部サーバの間の通信が非同期と同期のどちらであるかによっても異なります。

### 同期通知および非同期通知とは

FPolicy は、FPolicy インターフェイスを介して外部 FPolicy サーバに通知を送信します。通知は同期モードまたは非同期モードで送信されます。通知モードによって、FPolicy サーバへの通知送信後の ONTAP の動作が決まります。

#### • \* 非同期通知 \*

非同期通知では、FPolicy サーバからの応答を待たずにノードでの処理を継続できるため、システムの全体的なスループットが向上します。この種類の通知は、通知の評価結果に基づいて FPolicy サーバで処理を行う必要がないアプリケーションに適しています。たとえば、Storage Virtual Machine （SVM）管理者がファイルアクセスのアクティビティを監視および監査する場合などに使用されます。

非同期モードで動作している FPolicy サーバでネットワーク停止が発生した場合、停止中に生成された FPolicy 通知はストレージノードに格納されます。FPolicy サーバがオンラインに戻ると、サーバは格納された通知に関するアラートを受け取り、ストレージノードから通知を読み込むことができます。停止中に通知を保存できる期間は、最大 10 分に設定できます。

ONTAP 9.14.1以降では、FPolicyで永続的ストアを設定して、SVM内の非同期（必須ではない）ポリシーのファイルアクセスイベントをキャプチャすることができます。永続的ストアを使用すると、クライアントI/O処理とFPolicy通知処理を分離して、クライアントのレイテンシを低減できます。同期（必須または必須でない）および非同期の必須構成はサポートされていません。

#### • \* 同期通知 \*

同期モードで実行するように設定した場合は、すべての通知について FPolicy サーバからの確認応答を受け取ってからでないと、クライアントの処理を続行できません。このタイプの通知は、通知の評価結果に基づいて処理を行う必要がある場合に使用されます。たとえば、要求を許可するかどうかを外部 FPolicy サーバで指定された条件に基づいて判断する場合などに使用されます。

#### 同期アプリケーションおよび非同期アプリケーション

FPolicy アプリケーションにはさまざまな用途があり、非同期と同期の両方に対応しています。

非同期アプリケーションとは、ファイルまたはディレクトリへのアクセスや Storage Virtual Machine（SVM）上のデータが外部 FPolicy サーバによって変更されないアプリケーションです。例：

- ファイルアクセスと監査ログ
- ストレージリソース管理

同期アプリケーションとは、データアクセスやデータが外部 FPolicy サーバによって変更されるアプリケーションです。例：

- クォータ管理
- ファイルアクセスブロッキング
- ファイル・アーカイブと階層型ストレージ管理
- 暗号化サービスと復号化サービス
- 圧縮サービスと展開サービス

#### FPolicyの永続的ストア

ONTAP 9.14.1以降では、FPolicyで永続的ストアを設定して、SVM内の非同期（必須ではない）ポリシーのファイルアクセスイベントをキャプチャすることができます。永続的ストアを使用すると、クライアントI/O処理とFPolicy通知処理を分離して、クライアントのレイテンシを低減できます。同期（必須または必須でない）および非同期の必須構成はサポートされていません。

この機能は、FPolicy外部モードでのみ使用できます。この機能をサポートするには、使用するパートナーアプリケーションが必要です。このFPolicy設定がサポートされていることをパートナーと協力して確認する必要があります。

#### ベストプラクティス

クラスタ管理者は、FPolicyが有効になっている各SVMで永続的ストア用のボリュームを設定する必要があります。永続ストアが設定されている場合、一致するすべてのFPolicyイベントがキャプチャされ、FPolicyパイプライン内でさらに処理されて外部サーバに送信されます。

永続ストアは、予期しないリブートが発生した場合、またはFPolicyを無効にして再度有効にした場合に、最後のイベントを受信した時点のままになります。テイクオーバー処理が完了すると、新しいイベントがパートナーノードに格納されて処理されます。ギブバック処理のあと、ノードのテイクオーバーの発生時に残っている可能性がある未処理のイベントの処理が永続的ストアで再開されます。ライブイベントは、未処理のイベントよりも優先されます。

永続的ストアボリュームが同じSVM内のノード間で移動した場合、まだ処理されていない通知も新しいノー

ドに移動します。再実行する必要があります `fpolicy persistent-store create` ボリュームの移動後にいずれかのノードでコマンドを実行し、保留中の通知が外部サーバに配信されるようにします。

永続的ストアボリュームはSVM単位でセットアップします。FPolicyが有効なSVMごとに、永続的ストアボリュームを作成する必要があります。

FPolicyで最大トラフィック量を監視すると想定されるLIFがあるノードに永続的ストアボリュームを作成します。

永続的ストアに蓄積された通知がプロビジョニングされたボリュームのサイズを超えると、FPolicyは該当するEMSメッセージを含む受信通知を破棄し始めます。

永続的なストアのボリューム名とボリューム作成時に指定したジャンクションパスが一致している必要があります。

Snapshotポリシーをに設定 `none` 対象のボリュームではなく `default`。これは、Snapshotが誤ってリストアされて現在のイベントが失われることがないようにし、イベント処理が重複しないようにするためです。

永続的なイベントレコードが誤って破損したり削除されたりしないように、外部ユーザプロトコルアクセス（CIFS / NFS）で永続的ストアボリュームにアクセスできないようにします。これには、FPolicyを有効にしたあとにONTAPでボリュームをアンマウントしてジャンクションパスを削除すると、ユーザプロトコルアクセスができなくなります。

詳細については、を参照してください ["永続ストアの作成"](#)。

## FPolicy の設定タイプ

FPolicy の基本設定には 2 つのタイプがあります。一方の設定では、通知を受けて処理と対応を行う外部 FPolicy サーバを使用します。もう一方の設定では外部 FPolicy サーバを使用しません。代わりに、ONTAP 内部のネイティブ FPolicy サーバを使用して、拡張子に基づく単純なファイルブロッキングを行います。

### • \* 外部 FPolicy サーバ構成 \*

FPolicy サーバに通知が送信され、そのサーバが要求をスクリーニングし、要求されたファイル操作をノードで許可するかどうかを決定するルールを適用します。同期ポリシーの場合、FPolicy サーバは、要求されたファイル操作を許可またはブロックする応答をノードに送信します。

### • \* ネイティブ FPolicy サーバ構成 \*

通知は内部的にスクリーニングされます。要求は、FPolicy スコープで設定されているファイル拡張子に基づいて許可または拒否されます。

\*注：拒否されたファイル拡張子要求はログに記録されません。

を使用してネイティブ **FPolicy** 設定を作成する場合

ネイティブの FPolicy 設定では、ONTAP に組み込まれている FPolicy エンジンを使用して、ファイルの拡張子に基づいてファイル操作を監視およびブロックします。この解決策には、外部 FPolicy サーバ（FPolicy サーバ）は必要ありません。ネイティブファイルブロッキングの設定は、このシンプルな解決策がすべての場合に適しています。

ネイティブファイルブロッキングを使用すると、設定した処理およびフィルタリングイベントに一致するすべてのファイル処理を監視したうえで、特定の拡張子を持つファイルへのアクセスを拒否することができます。これがデフォルトの設定です。

この設定では、ファイルの拡張子のみに基づいてファイルへのアクセスをブロックすることができます。たとえば、を含むファイルをブロックします mp3 拡張子を使用すると、ターゲットのファイル拡張子がの特定の処理に関する通知を送信するようにポリシーを設定できます mp3。ポリシーは拒否するように設定されています mp3 通知を生成する操作に対するファイル要求。

次の環境ネイティブ FPolicy の設定：

- FPolicy サーバベースファイルスクリーニングでサポートされているフィルタとプロトコルのセットが、ネイティブファイルブロッキングでもサポートされます。
- ネイティブファイルブロッキングと FPolicy サーバベースファイルスクリーニングアプリケーションは同時に設定できます。

そのためには、Storage Virtual Machine（SVM）に2つの FPolicy ポリシーを設定します。1つはネイティブファイルブロッキングのために設定したポリシーで、もう1つは FPolicy のサーバベースのファイルスクリーニングのために設定したポリシーです。

- ネイティブファイルブロッキング機能では、ファイルの内容ではなく、拡張子のみに基づいてファイルがスクリーニングされます。
- シンボリックリンクの場合、ネイティブファイルブロッキングは、ルートファイルのファイル拡張子を使用します。

の詳細を確認してください ["FPolicy：ネイティブファイルブロッキング"](#)。

外部 FPolicy サーバを使用する設定を作成する状況

通知の処理と管理に外部 FPolicy サーバを使用する FPolicy 設定は、ファイル拡張子に基づく単純なファイルブロッキング以上が必要なユースケースに対して、堅牢なソリューションを提供します。

ファイルアクセスイベントの監視と記録、クォータサービスの提供、単純なファイル拡張子以外の条件に基づくファイルブロッキング、階層型ストレージ管理アプリケーションを使用したデータ移行サービスの提供など、目的に応じて外部 FPolicy サーバを使用する設定を作成する必要があります。または、Storage Virtual Machine（SVM）の一部のデータのみを監視するきめ細かいポリシーセットを提供することもできます。

**FPolicy 実装でクラスタコンポーネントが果たす役割**

FPolicy の実装においては、クラスタ、それに含まれる Storage Virtual Machine（SVM）、およびデータ LIF のそれぞれに役割があります。

• \* クラスタ \*

クラスタに含まれる FPolicy の管理フレームワークで、クラスタ内のすべての FPolicy の設定に関する情報の保守と管理を行います。

• \* SVM \*

FPolicy の設定は SVM レベルで定義されます。設定の範囲は SVM であり、SVM リソースにのみ適用されます。1つの SVM 設定で、別の SVM にあるデータに対するファイルアクセス要求を監視して通知を送信することはできません。

FPolicy の設定は管理 SVM で定義できます。管理 SVM で定義した設定は、すべての SVM で表示および使用できます。

#### • \* データ LIF \*

FPolicy サーバへの接続は、FPolicy の設定が格納された SVM に属するデータ LIF を通じて行われます。これらの接続に使用されるデータ LIF は、通常のクライアントアクセスに使用されるデータ LIF と同じ方法でフェイルオーバーできます。

### FPolicy と外部 FPolicy サーバの連携

Storage Virtual Machine（SVM）で FPolicy を設定して有効にすると、SVM に含まれているすべてのノードで FPolicy が実行されるようになります。FPolicy は、外部 FPolicy サーバ（FPolicy サーバ）との接続の確立と維持、通知の処理、および FPolicy サーバとやり取りする通知メッセージの管理を行います。

また、接続管理の一環として、FPolicy は次の役割を果たします。

- ファイル通知が正しい LIF を通過して FPolicy サーバに送信されるようにする。
- ポリシーに複数の FPolicy サーバが関連付けられている場合に、FPolicy サーバへの通知の送信時にロードバランシングが行われるようにする。
- FPolicy サーバへの接続が切断された場合、再接続を試行します。
- 認証されたセッションを介して FPolicy サーバに通知を送信します。
- パススルーリードが有効になっている場合にクライアント要求を処理するために FPolicy サーバによって確立されたパススルーリードデータ接続を管理します。

#### 制御チャネルを使用した FPolicy 通信

FPolicy は、Storage Virtual Machine（SVM）に含まれている各ノードのデータ LIF から外部 FPolicy サーバへの制御チャネル接続を開始します。FPolicy は制御チャネルを使用してファイル通知を送信するため、FPolicy サーバでは、SVM のトポロジに基づいて複数の制御チャネル接続が認識される場合があります。

#### 権限付きデータアクセスチャネルを使用した同期通信

同期通信では、FPolicy サーバは、権限付きデータアクセスパスを介して Storage Virtual Machine（SVM）上のデータにアクセスします。権限付きパスを介したアクセスでは、FPolicy サーバにファイルシステム全体が公開されます。データファイルにアクセスして、情報の収集、ファイルのスキャン、ファイルの読み取り、ファイルへの書き込みを行うことができます。

外部 FPolicy サーバが権限付きデータチャネルを介して SVM のルートからファイルシステム全体にアクセスできるため、権限付きデータチャネル接続はセキュアである必要があります。

#### 権限付きデータアクセスチャネルでの FPolicy 接続クレデンシャルの使用方法

FPolicy サーバは、FPolicy の設定で保存されている特定の Windows ユーザクレデンシャルを使用して、クラスタノードへの権限付きデータアクセス接続を確立します。権限付きデータアクセスチャネル接続の確立用としてサポートされているプロトコルは、SMB だけです。

FPolicy サーバで権限付きデータアクセスが必要とされる場合は、次の条件を満たす必要があります。



- クラスタでSMBライセンスが有効になっている必要があります。
- FPolicy サーバが FPolicy の設定で指定されたクレデンシャルで実行されている。

データチャネル接続を確立するとき、FPolicy では、指定された Windows ユーザ名のクレデンシャルが使用されます。データアクセスは、管理共有 ONTAP\_ADMIN\$ を介して確立されます。

権限付きデータアクセスのためのスーパーユーザクレデンシャルの付与とは何ですか

ONTAP は、IP アドレスと FPolicy 設定で設定されたユーザクレデンシャルを組み合わせ、FPolicy サーバにスーパーユーザクレデンシャルを付与します。

スーパーユーザには、FPolicy サーバでデータにアクセスする際に次の権限が付与されます。

- 権限チェックの省略

ファイルやディレクトリへのアクセスのチェックが省略されます。

- 特殊なロック権限

ONTAP では、ロックが設定されていても、ファイルへの読み取り、書き込み、変更が許可されます。バイト単位のロックが設定されたファイルを FPolicy サーバで取得した場合、ファイルに対する既存のロックはすぐに解除されます。

- すべての FPolicy チェックを省略します

アクセス時に FPolicy 通知が生成されません。

#### FPolicy によるポリシーの処理の管理方法

Storage Virtual Machine（SVM）には、優先度が異なる複数の FPolicy ポリシーが割り当てられる場合があります。SVM で適切な FPolicy の設定を作成するには、FPolicy によるポリシーの処理の管理方法を理解しておくことが重要です。

最初に各ファイルアクセス要求が評価され、このイベントを監視するポリシーが決定されます。監視対象イベントの場合は、関連するポリシーとともにそのイベントに関する情報が評価を行う FPolicy に渡されます。各ポリシーは、割り当てられた優先度の順に評価されます。

ポリシーを設定する際には、次の推奨事項を考慮してください。

- あるポリシーが常に他のポリシーよりも先に評価されるようにするには、そのポリシーの優先度を高く設定します。
- 監視対象イベントで要求されたファイルアクセス処理が正常に実行されることが、別のポリシーに対して評価されるファイル要求の前提条件となる場合は、最初のファイル処理の成功または失敗を制御するポリシーの優先度を高く設定します。

たとえば、1つのポリシーで FPolicy のファイルのアーカイブとリストアの機能を管理し、2つ目のポリシーでオンラインファイルのファイルアクセス処理を管理する場合、ファイルのリストアを管理するポリシーの優先度を高くして、2番目のポリシーで管理されている処理を実行する前にファイルをリストアするようにする必要があります。

- ファイルアクセス処理に適用される可能性があるすべてのポリシーを評価するには、同期ポリシーの優先度を低く設定します。



既存のポリシーの優先度を変更するには、ポリシーのシーケンス番号を変更します。ただし、変更した優先度に基づいてポリシーを評価するには、変更したシーケンス番号を持つポリシーを無効にしてから再度有効にする必要があります。

## ノードと外部 FPolicy サーバの間の通信プロセス

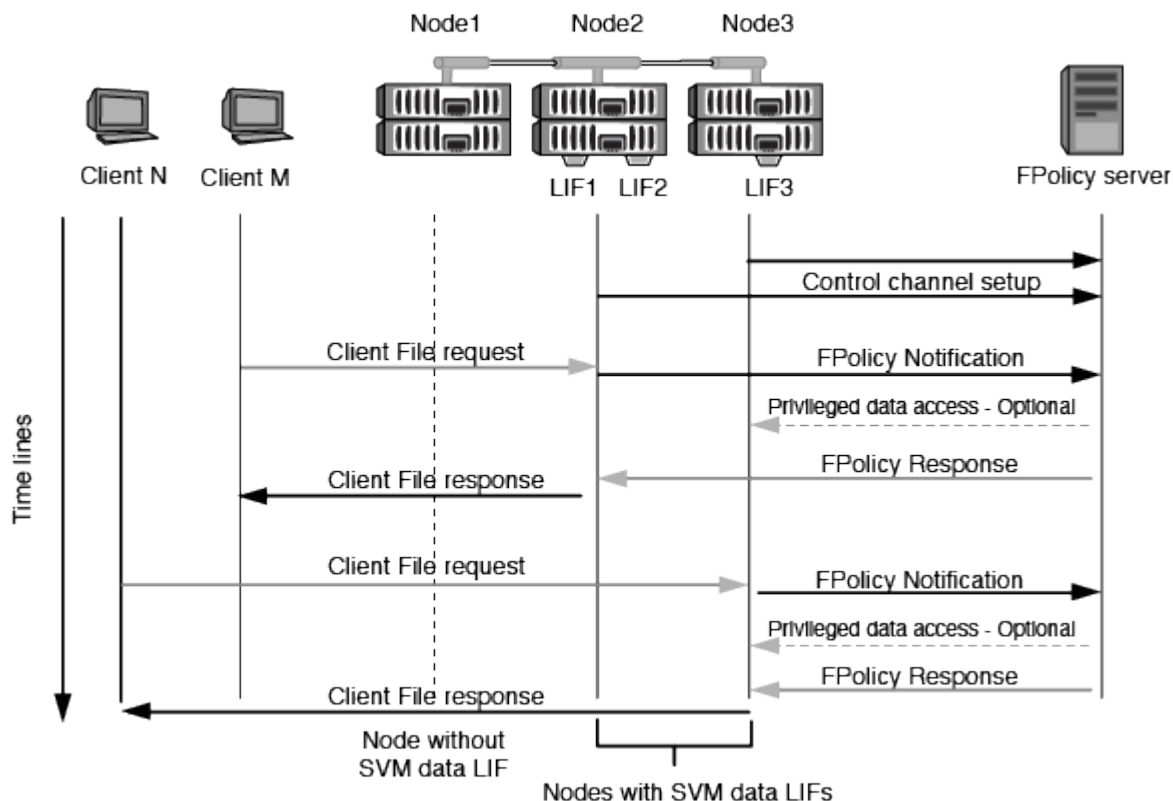
FPolicy の設定を適切に計画するには、ノードと外部 FPolicy サーバの間の通信プロセスについて理解しておく必要があります。

Storage Virtual Machine (SVM) に属しているすべてのノードは、TCP/IP を使用して外部 FPolicy サーバへの接続を開始します。FPolicy サーバへの接続のセットアップには、ノードのデータ LIF を使用します。そのため、接続のセットアップは、ノードで SVM のデータ LIF が稼働している場合しか実行できません。

ポリシーが有効になっている場合は、各ノードのそれぞれの FPolicy プロセスで、FPolicy サーバとの接続の確立が試行されます。ポリシー設定で指定された FPolicy 外部エンジンの IP アドレスとポートが使用されます。

この接続により、SVM に属する各ノードから FPolicy サーバへのデータ LIF を介した制御チャンネルが確立されます。また、データ LIF のアドレスとして同じノードで IPv4 と IPv6 の両方が設定されている場合、FPolicy は IPv4 と IPv6 の両方の接続の確立を試みます。そのため、SVM が複数のノードに展開されている場合、または IPv4 と IPv6 の両方のアドレスが設定されている場合は、SVM で FPolicy ポリシーを有効にしたあとに、クラスタからの複数の制御チャンネルのセットアップ要求に対応する必要があります。

たとえば、クラスタのノードが3つ（ノード1、ノード2、ノード3）ある場合に、SVM のデータ LIF がノード2とノード3にのみ分散されていると、データボリュームの分散に関係なく、制御チャンネルはノード2とノード3からのみ開始されます。ノード2には LIF1 と LIF2 の2つのデータ LIF があり、これらは SVM に属しており、初期接続は LIF1 からであるとします。FPolicy は、LIF1 で障害が発生した場合に LIF2 からの制御チャンネルの確立を試みます。



データ LIF は、同じノードのデータポート、またはリモートノードのデータポートに移行できます。

データ LIF がフェイルオーバーまたは移行されると、FPolicy サーバへの新しい制御チャネル接続が確立されます。その後、FPolicy は SMB クライアントおよび NFS クライアントのタイムアウトした要求を再試行でき、新しい通知が外部 FPolicy サーバに送信されます。ノードは、SMB と NFS の元のタイムアウトした要求に対する FPolicy サーバの応答を拒否します。

#### ノードのフェイルオーバー時における FPolicy による外部通信の管理方法

FPolicy 通信に使用されるデータポートをホストするクラスタノードに障害が発生した場合は、ONTAP サーバとノードの間の接続が切断されます。

クラスタフェイルオーバーが FPolicy サーバに及ぼす影響は、FPolicy 通信に使用されるデータポートを別のアクティブノードに移行するようにフェイルオーバーポリシーを設定することで軽減できます。移行が完了すると、新しいデータポートを使用して新しい接続が確立されます。

データポートを移行するようにフェイルオーバーポリシーが設定されていない場合、FPolicy サーバは障害が発生したノードが稼働するまで待機する必要があります。ノードが稼働したら、新しいセッション ID を使用してそのノードから新しい接続が開始されます。



FPolicy サーバでは、切断された接続を検出するためにキープアライブプロトコルメッセージが使用されます。セッション ID をパージするためのタイムアウトは、FPolicy の設定時に決定します。デフォルトのキープアライブタイムアウトは 2 分です。

#### SVM ネームスペースにおける FPolicy サービスの仕組み

ONTAP は、統合 Storage Virtual Machine (SVM) ネームスペースを提供します。ジャンクションによってクラスタ全体のボリュームを統合し、単一の論理ファイルシステムを実現します。FPolicy サーバはネームスペーストポロジを認識し、ネームスペース全体に FPolicy サービスを提供します。

ネームスペースは SVM に固有のもので、その内部に含まれています。したがって、ネームスペースは SVM コンテキストからのみ表示できます。ネームスペースには次のような特徴があります。

- 各 SVM には単一のネームスペースが存在します。ネームスペースのルートはルートボリュームで、ネームスペース内ではスラッシュ (/) で表されます。
- それ以外のボリュームには、ルート (/) より下のジャンクションポイントがあります。
- ボリュームジャンクションは、クライアントに対して透過的です。
- 単一の NFS エクスポートは、ネームスペース全体へのアクセスを提供できます。あるいは、エクスポートポリシーで特定のボリュームをエクスポートできます。
- ネームスペース内のボリューム、ボリューム内の qtree、またはディレクトリに SMB 共有を作成できます。
- ネームスペースアーキテクチャは柔軟です。

一般的なネームスペースアーキテクチャの例を次に示します。

- ルートからの分岐が 1 つだけのネームスペース

- ルートからの分岐が複数あるネームスペース
- ルートから分岐していないボリュームが複数あるネームスペース

## FPolicy のパススルーリードによる階層型ストレージ管理の利便性向上

パススルーリードを使用すると、移行されたオフラインファイルに対する読み取りアクセスを（階層型ストレージ管理（HSM）サーバとして機能している）FPolicy サーバから提供できます。セカンダリストレージシステムからプライマリストレージシステムにファイルをリコールする必要はありません。

SMBサーバ上にあるファイルにHSMを提供するようにFPolicyサーバが設定されている場合、ポリシーベースのファイル移行が実行されます。この場合、ファイルはセカンダリストレージにオフラインで保存され、スタブファイルのみがプライマリストレージに残ります。スタブファイルはクライアントからは通常のファイルとして認識されますが、実際には元のファイルと同じサイズのスパースファイルです。スパースファイルはSMBのオフラインビットが設定されており、セカンダリストレージに移行された実際のファイルを参照しています。

通常、オフラインファイルの読み取り要求を受信した場合は、要求されたコンテンツをプライマリストレージにリコールしてから、プライマリストレージからアクセスする必要があります。データをプライマリストレージにリコールする必要があることから、いくつかの好ましくない影響が生じます。特に、コンテンツをリコールしてから要求に応じる必要があるためにクライアント要求に対するレイテンシが大きくなる点と、プライマリストレージで必要となる領域の使用量がリコールされるファイルのサイズだけ増える点が挙げられます。

FPolicy のパススルーリードを使用すると、移行されたオフラインファイルに対する読み取りアクセスを HSM サーバ（FPolicy サーバ）から提供できます。セカンダリストレージシステムからプライマリストレージシステムにファイルをリコールする必要はありません。プライマリストレージにファイルをリコールして戻す代わりに、読み取り要求をセカンダリストレージから直接処理できます。



FPolicy のパススルーリード処理では、コピーオフロード（ODX）はサポートされません。

パススルーリードは、次のような利点を提供してユーザビリティを向上します。

- 要求されたデータをリコールするための十分なスペースがプライマリストレージになくても、読み取り要求を処理できます。
- スクリプトやバックアップ解決策で多数のオフラインファイルへのアクセスが必要になる場合など、データのリコールが急増した場合でも容量やパフォーマンスの管理を適切に行うことができます。
- Snapshot コピー内のオフラインファイルに対する読み取り要求を処理できます。

Snapshot コピーは読み取り専用であるため、スタブファイルが Snapshot コピー内にある場合、FPolicy サーバは元のファイルをリストアできません。パススルーリードを使用すると、この問題は解消されます。

- セカンダリストレージ上のファイルへのアクセスによって読み取り要求が処理されるタイミングや、オフラインファイルをプライマリストレージにリコールするタイミングを制御するポリシーを設定できます。

たとえば、オフラインファイルがプライマリストレージに移行されるまでの指定した期間内にオフラインファイルにアクセスできる回数を指定するポリシーを HSM サーバ上に作成できます。このタイプのポリシーにより、滅多にアクセスされないファイルのリコールを回避できます。

Storage Virtual Machine（SVM）および FPolicy サーバ間の接続を最適な形で設定できるように、FPolicy パススルーリードが有効になっている場合の読み取り要求の管理方法を理解しておく必要があります。

FPolicy パススルーリードが有効になっている場合に SVM がオフラインのファイルに対する要求を受け取ると、FPolicy によって標準の接続チャンネル経由で FPolicy サーバ（HSM サーバ）に通知が送信されます。

通知を受け取ったあと、FPolicy サーバはその通知で送信されたファイルパスからデータを読み取り、要求されたデータを SVM および FPolicy 間に確立されたパススルーリード権限付きデータ接続を介して SVM に送信します。

データが送信されると、FPolicy サーバは読み取り要求に allow または deny として応答します。読み取り要求が許可されたか拒否されたかによって、ONTAP は要求された情報またはエラーメッセージをクライアントに送信します。

## FPolicy の設定を計画

FPolicy を設定するための要件、考慮事項、およびベストプラクティス

SVMでFPolicyの設定を作成して設定する前に、FPolicyの設定に関する一定の要件、考慮事項、およびベストプラクティスについて確認しておく必要があります。

FPolicy機能は、コマンドラインインターフェイス（CLI）またはREST APIを使用して設定します。

FPolicy を設定するための要件

Storage Virtual Machine（SVM）で FPolicy を設定して有効にする前に、一定の要件について確認しておく必要があります。

- ・ クラスタ内のすべてのノードで、FPolicy がサポートされているバージョンの ONTAP が実行されている必要があります。
- ・ ONTAP の標準の FPolicy エンジンを使用しない場合は、外部 FPolicy サーバ（FPolicy サーバ）をインストールしておく必要があります。
- ・ FPolicy ポリシーが有効になっている SVM のデータ LIF からアクセスできるサーバに、FPolicy サーバがインストールされている必要があります。



ONTAP 9.8以降では、ONTAP により、を追加して、アウトバウンドFPolicy接続用のクライアントLIFサービスを利用できます data-fpolicy-client サービス "[LIFとサービスポリシーの詳細については、こちらをご覧ください](#)"。

- ・ FPolicy ポリシーの外部エンジンの設定で、FPolicy サーバの IP アドレスがプライマリサーバまたはセカンダリサーバとして設定されている必要があります。
- ・ FPolicy サーバで権限付きデータチャンネルを使用してデータにアクセスする場合は、次の追加要件を満たす必要があります。
  - クラスタで SMB のライセンスが有効になっている必要があります。

権限付きデータアクセスは SMB 接続を使用して実行されます。

- 権限付きデータチャンネルを使用してファイルにアクセスするためのユーザクレデンシャルが設定され

ている必要があります。

- FPolicy サーバが FPolicy の設定で指定されたクレデンシャルで実行されている。
- FPolicyサーバとの通信に使用されるすべてのデータLIFをで設定する必要があります `cifs` 許可されているプロトコルの1つとして指定します。

これには、パススルーリード接続で使用される LIF も含まれます。

- ONTAP 9.14.1以降では、FPolicyで永続的ストアを設定して、SVM内の非同期（必須ではない）ポリシーのファイルアクセスイベントをキャプチャすることができます。永続的ストアを使用すると、クライアントI/O処理とFPolicy通知処理を分離して、クライアントのレイテンシを低減できます。同期（必須または必須でない）および非同期の必須構成はサポートされていません。

#### FPolicy を設定する際のベストプラクティスと推奨事項

Storage Virtual Machine (SVM) でFPolicyを設定する場合は、FPolicyの設定によって監視のパフォーマンスが向上し、要件を満たす結果が得られるようにするために、設定に関する一般的なベストプラクティスと推奨事項を理解してください。

パフォーマンス、サイジング、および設定に関する具体的なガイドラインについては、FPolicyパートナーアプリケーションを参照してください。

#### ポリシー設定

FPolicy外部エンジン、イベント、SVM用のスコープを設定することで、全体的なエクスペリエンスとセキュリティが向上する可能性があります。

- SVM用のFPolicy外部エンジンの設定：
  - セキュリティを強化するには、パフォーマンスコストがかかります。Secure Sockets Layer (SSL) 通信を有効にすると、共有へのアクセスのパフォーマンスに影響します。
  - FPolicyサーバの通知処理の耐障害性と高可用性を確保するには、FPolicy外部エンジンに複数のFPolicyサーバを設定する必要があります。

- SVMのFPolicyイベントの設定

ファイル操作の監視は、エクスペリエンス全体に影響します。たとえば、ストレージ側で不要なファイル操作をフィルタリングすると、操作性が向上します。NetAppでは、次の設定を推奨しています。

- ユースケースを壊さずに、最小タイプのファイル処理を監視し、最大数のフィルタを有効にする。
- 属性取得、読み取り、書き込み、オープン、クローズの各処理にフィルタを使用する。SMBおよびNFSホームディレクトリ環境では、これらの処理の割合が高くなっています。

- SVMのFPolicyスコープの設定

ポリシーの範囲を、SVM全体ではなく、関連するストレージオブジェクト（共有、ボリューム、エクスポートなど）に制限します。NetAppでは、ディレクトリ拡張子の確認を推奨しています状況に応じて `is-file-extension-check-on-directories-enabled` パラメータはに設定されます `true` の場合、ディレクトリオブジェクトには、通常のファイルと同じ拡張子チェックが適用されます。

#### ネットワーク構成：

FPolicyサーバとコントローラ間のネットワーク接続のレイテンシを低くする必要があります。NetAppで



は、プライベートネットワークを使用してFPolicyトラフィックをクライアントトラフィックから分離することを推奨しています。

また、レイテンシを最小限に抑え、広帯域接続を実現するために、外部FPolicyサーバ（FPolicyサーバ）を広帯域接続が可能なクラスターの近くに配置する必要があります。



FPolicyトラフィック用のLIFがクライアントトラフィック用のLIFとは別のポートに設定されている場合、ポートの障害が原因でFPolicy LIFがもう一方のノードにフェイルオーバーすることがあります。その結果、ノードからFPolicyサーバに到達できなくなり、ノードでのファイル操作に関するFPolicy通知は失敗します。この問題を回避するには、ノード上の少なくとも1つのLIFからFPolicyサーバにアクセスして、そのノードで実行されるファイル操作のFPolicy要求を処理できることを確認します。

## ハードウェア構成

FPolicyサーバは物理サーバと仮想サーバのどちらにも配置できます。FPolicyサーバが仮想環境にある場合は、仮想サーバに専用のリソース（CPU、ネットワーク、およびメモリ）を割り当てる必要があります。

SVM がクライアント要求に応答する際のレイテンシの原因となる可能性がある FPolicy サーバの過負荷状態を防ぐために、クラスターノードと FPolicy サーバの比率を最適化する必要があります。最適な比率は、FPolicyサーバが使用されているパートナーアプリケーションによって異なります。NetAppでは、パートナーと協力して適切な価値を判断することを推奨しています。

## 複数ポリシーの設定

ネイティブブロッキング用のFPolicyポリシーはシーケンス番号に関係なく最も優先され、意思決定変更ポリシーは他のポリシーよりも優先されます。ポリシーの優先度はユースケースによって異なります。NetAppは、パートナーと協力して適切な優先順位を決定することを推奨します。

## サイズに関する考慮事項

FPolicyは、SMB処理とNFS処理のインライン監視を実行し、外部サーバに通知を送信し、外部エンジンの通信モード（同期または非同期）に応じて応答を待機します。このプロセスは、SMBとNFSのアクセスおよびCPUリソースのパフォーマンスに影響します。

NetAppでは、問題を軽減するために、FPolicyを有効にする前に、パートナーと協力して環境を評価し、サイジングすることを推奨しています。パフォーマンスは、ユーザ数、ユーザあたりの処理数やデータサイズなどのワークロード特性、ネットワークレイテンシ、障害やサーバの速度低下など、いくつかの要因によって影響を受けます。

## パフォーマンスを監視

FPolicyは通知ベースのシステムです。通知は、処理およびONTAPへの応答を生成するために外部サーバに送信されます。このラウンドトリッププロセスにより、クライアントアクセスのレイテンシが増加します。

FPolicyサーバとONTAPのパフォーマンスカウンタを監視すると、解決策のボトルネックを特定し、解決策を最適化するために必要に応じてパラメータを調整できます。たとえば、FPolicyのレイテンシの増加は、SMBとNFSのアクセスレイテンシに連鎖的に影響します。そのため、ワークロード（SMBとNFS）とFPolicyの両方のレイテンシを監視する必要があります。また、ONTAPのQoSポリシーを使用して、FPolicyが有効になっているボリュームまたはSVMごとにワークロードを設定できます。

NetAppは、を実行することを推奨します `statistics show -object workload` コマンドを使用してワークロード統計を表示します。さらに、次のパラメータを監視する必要があります。

- 平均レイテンシ、読み取りレイテンシ、書き込みレイテンシ
- 処理の総数
- 読み取りカウンタと書き込みカウンタ

FPolicyサブシステムのパフォーマンスを監視するには、次のFPolicyカウンタを使用します。



FPolicyに関連する統計を収集するには、診断モードにする必要があります。

#### 手順

##### 1. FPolicyカウンタを収集します。

- `statistics start -object fpolicy -instance instance_name -sample-id ID`
- `statistics start -object fpolicy_policy -instance instance_name -sample-id ID`

##### 2. FPolicyカウンタを表示します。

- `statistics show -object fpolicy -instance instance_name -sample-id ID`
- `statistics show -object fpolicy_server -instance instance_name -sample-id ID`

。 `fpolicy` および `fpolicy_server` カウンタは、次の表で説明されている複数のパフォーマンスパラメータに関する情報を提供します。

カウンタ	説明
「 <b>fpolicy</b> 」カウンタ	<code>aborted_requests</code>
SVMで処理が中止されたスクリーニング要求の数	<code>event_count</code>
通知の原因となるイベントのリスト	<code>max_request_latency</code> の略
最大スクリーン要求遅延	<code>outstanding_requests</code>
処理中のスクリーン要求の総数	<code>processed_requests</code>
SVMでfpolicy処理が実行されたスクリーニング要求の総数	<code>request_latency_hist</code>
画面要求のレイテンシのヒストグラム	<code>requests_dispatched_rate</code>
1秒あたりに送出されるスクリーン要求の数	<code>requests_received_rate</code>
1秒あたりに受信された画面要求の数	「 <b>fpolicy_server</b> 」カウンタ
<code>max_request_latency</code> の略	画面要求の最大遅延
<code>outstanding_requests</code>	応答を待機している画面要求の総数

カウンタ	説明
request_latency	画面要求の平均遅延
request_latency_hist	画面要求のレイテンシのヒストグラム
request_sent_rate	FPolicyサーバに送信された1秒あたりのスクリーニング要求数
response_received_rate	FPolicyサーバから受信した1秒あたりのスクリーニング応答数

## FPolicyワークフローと他のテクノロジーへの依存関係を管理します

NetAppでは、設定を変更する前にFPolicyポリシーを無効にすることを推奨しています。たとえば、有効なポリシーに設定されている外部エンジンのIPアドレスを追加または変更する場合は、最初にポリシーを無効にします。

NetApp FlexCacheボリュームを監視するようにFPolicyを設定する場合は、NetApp読み取りおよび属性取得ファイル操作を監視するようにFPolicyを設定しないことを推奨します。ONTAPでこれらの処理を監視するには、inode-to-path (I2P) データを取得する必要があります。I2PデータはFlexCacheボリュームから取得できないため、元のボリュームから取得する必要があります。そのため、これらの処理を監視することで、FlexCacheが提供するパフォーマンス上のメリットが排除されます。

FPolicyと外部のウィルス対策解決策の両方が導入されている場合、最初にウィルス対策解決策が通知を受信します。FPolicyの処理は、ウィルス対策スキャンの完了後に開始されます。低速のウィルス対策スキャナは全体的なパフォーマンスに影響する可能性があるため、ウィルス対策ソリューションのサイズを正しく設定することが重要です。

### パススルーリードのアップグレードおよびリバートに関する考慮事項

パススルーリードをサポートしている ONTAP リリースへのアップグレードまたはパススルーリードをサポートしていないリリースへのリバートを行う前に、アップグレードおよびリバートに関する考慮事項を把握しておく必要があります。

#### をアップグレードして

FPolicy パススルーリードをサポートしている ONTAP のバージョンにすべてのノードをアップグレードしたあと、クラスタはパススルーリードを使用できるようになります。ただし、既存の FPolicy 設定ではパススルーリードがデフォルトで無効になっています。既存の FPolicy 設定でパススルーリードを使用するには、FPolicy ポリシーを無効にして設定を変更してから、設定を再度有効にする必要があります。

#### 復元しています

FPolicyパススルーリードをサポートしていないバージョンのONTAPにリバートする前に、次の条件を満たす必要があります。

- パススルーリードを使用してすべてのポリシーを無効にし、パススルーリードを使用しないように影響を受ける設定を変更します。
- クラスタのすべてのFPolicyポリシーを無効にして、クラスタのFPolicy機能を無効にします。

永続的ストアをサポートしないバージョンのONTAPにリバートする前に、FPolicyポリシーに永続的ストアが設定されていないことを確認してください。永続ストアが設定されている場合、リバートは失敗します。



## FPolicy の設定手順は何ですか

FPolicy でファイルアクセスを監視するには、FPolicy の設定を作成し、FPolicy サービスが必要な Storage Virtual Machine (SVM) で有効にする必要があります。

SVM で FPolicy 設定をセットアップして有効にする手順は次のとおりです。

### 1. FPolicy 外部エンジンを作成します。

FPolicy 外部エンジンでは、特定の FPolicy の設定に関連付けられた外部 FPolicy サーバ（FPolicy サーバ）を識別します。内部の「ネイティブ」FPolicy エンジンを使用してネイティブ・ファイル・ブロッキング構成を作成する場合は、FPolicy 外部エンジンを作成する必要はありません。

### 2. FPolicy イベントを作成します。

FPolicy イベントでは、FPolicy ポリシーで監視する対象を定義します。監視対象のプロトコルとファイル操作を指定し、一連のフィルタを含めることができます。それらのフィルタを使用して、監視対象イベントの中から、FPolicy 外部エンジンで通知を送信する必要があるイベントだけを抽出できます。イベントでは、ポリシーでボリューム操作を監視するかどうかも指定します。

### 3. FPolicy ポリシーを作成します。

FPolicy ポリシーでは、監視する必要がある一連のイベントと、指定の FPolicy サーバ（FPolicy サーバが設定されていない場合は標準のエンジン）に通知を送信する必要がある監視対象イベントを、適切な範囲で関連付けます。また、通知を受信するデータへの権限付きアクセスを FPolicy サーバに許可するかどうかも定義します。FPolicy サーバからデータにアクセスする必要がある場合は、権限付きアクセスが必要になります。権限付きアクセスが必要になる一般的なユースケースとしては、ファイルブロッキング、クォータ管理、階層型ストレージ管理などがあります。ポリシーは、このポリシーの設定で FPolicy サーバを使用するか、内部の「ネイティブ」FPolicy サーバを使用するかを指定します。

スクリーニングを必須にするかどうかはポリシーで指定します。スクリーニングを必須にすると、すべての FPolicy サーバが停止した場合や定義された時間内に FPolicy サーバからの応答を得られない場合に、ファイルアクセスが拒否されます。

ポリシーは SVM 単位で適用されます。1 つのポリシーを複数の SVM に適用することはできません。ただし、SVM には複数の FPolicy ポリシーを設定でき、各ポリシーのスコープ、イベント、外部サーバの設定を同じ組み合わせにすることも、それぞれで異なる組み合わせにすることもできます。

### 4. ポリシーのスコープを設定します。

FPolicy スコープでは、ポリシーで監視するボリューム、共有、またはエクスポートポリシーを指定します。また、FPolicy による監視対象に含めるファイル拡張子や除外するファイル拡張子も指定します。



除外リストは、対象リストよりも優先されます。

### 5. FPolicy ポリシーを有効にします。

ポリシーを有効にすると、制御チャネルおよびオプションで権限付きデータチャネルが接続されます。SVM が属するノードの FPolicy プロセスで、ファイルおよびフォルダに対するアクセスの監視が開始され、設定された条件に当てはまるイベントが見つかったら、FPolicy サーバ（FPolicy サーバが設定されていない場合は標準のエンジン）に通知が送信されます。



ポリシーでネイティブファイルブロッキングを使用する場合は、外部エンジンは設定されず、関連付けられることもありません。

## FPolicy 外部エンジンの設定を計画します

### FPolicy 外部エンジンの設定を計画します

FPolicy 外部エンジンを設定する前に、外部エンジンを作成することの意味を理解し、使用可能な設定パラメータを理解する必要があります。この情報は、各パラメータに設定する値を決定するのに役立ちます。

### FPolicy 外部エンジンの作成時に定義される情報

外部エンジンの設定では、外部 FPolicy サーバ（FPolicy サーバ）への接続を作成および管理するために FPolicy が必要とする、次のような情報を定義します。

- SVM 名
- エンジン名
- FPolicy サーバへの接続時に使用するプライマリおよびセカンダリ FPolicy サーバの IP アドレスと TCP ポート番号
- エンジンタイプが非同期か同期か
- ノードと FPolicy サーバ間の接続を認証する方法

相互 SSL 認証を設定することを選択した場合は、SSL 証明書情報を提供するパラメータも設定する必要があります。

- 各種の高度な権限設定を使用して接続を管理する方法


これには、タイムアウト値、リトライ値、キープアライブ値、最大要求値、送信および受信バッファサイズ値、セッションタイムアウト値などを定義するパラメータが含まれます。

。 `vserver fpolicy policy external-engine create` コマンドは、FPolicy外部エンジンの作成に使用します。

### 外部エンジンの基本パラメータ

次に示す FPolicy 基本設定パラメータの一覧は、構成を計画するのに役立ちます。

情報のタイプ	オプション
<p>SVM</p> <p>この外部エンジンに関連付ける SVM の名前を指定します。</p> <p>各 FPolicy 設定は、単一の SVM 内で定義されます。FPolicy ポリシーの構成要素となる外部エンジン、ポリシーイベント、ポリシーのスコープ、およびポリシーを、すべて同じ SVM に関連付ける必要があります。</p>	<p><code>-vserver vserver_name</code></p>

<p><b>_ エンジン名 _</b></p> <p>外部エンジンの設定に割り当てる名前を指定します。FPolicy ポリシーを作成した場合、あとで外部エンジンの名前を指定する必要があります。これにより、外部エンジンがポリシーに関連付けられます。</p> <p>この名前に指定できる文字数は最大 256 文字です。</p> <div>  <p>MetroCluster または SVM ディザスタリカバリ設定で外部エンジンの名前を設定する場合、この名前は最大 200 文字にする必要があります。</p> </div> <p>名前には、次の ASCII 文字の任意の組み合わせを含めることができます。</p> <ul style="list-style-type: none"> <li>• a から z</li> <li>• A から Z</li> <li>• 0 から 9</li> <li>• 「_」、「-」, and “.”</li> </ul>	<p>-engine-name engine_name</p>
<p><b>プライマリ FPolicy サーバ _</b></p> <p>所定の FPolicy ポリシーに関してノードが送信する通知の宛先となるプライマリ FPolicy サーバを指定します。IP アドレスをカンマで区切って指定します。</p> <p>複数のプライマリサーバの IP アドレスを指定した場合、SVM が参加しているすべてのノードに、ポリシーが有効にされたときに指定されたすべてのプライマリ FPolicy サーバへの制御接続が作成されます。複数のプライマリ FPolicy サーバを設定した場合、通知は各 FPolicy サーバにラウンドロビン方式で送信されます。</p> <p>外部エンジンが MetroCluster または SVM ディザスタリカバリ設定で使用されている場合は、ソースサイトでの FPolicy サーバの IP アドレスをプライマリサーバとして指定する必要があります。デスティネーションサイトでの FPolicy サーバの IP アドレスは、セカンダリサーバとして指定する必要があります。</p>	<p>-primary-servers `IP_address`はい。</p>
<p><b>ポート番号 _</b></p> <p>FPolicy サービスのポート番号を指定します。</p>	<p>-port integer</p>

<p><u>_ セカンダリ FPolicy サーバ _</u></p> <p>所定の FPolicy ポリシーに関して、ファイルアクセスイベントの送信先となるセカンダリ FPolicy サーバを指定します。IP アドレスをカンマで区切って指定します。</p> <p>セカンダリサーバは、いずれのプライマリにも到達できない場合にのみ使用されます。ポリシーが有効になっている場合はセカンダリサーバへの接続が確立されますが、通知はいずれのプライマリサーバにも到達できない場合にのみセカンダリサーバに送信されます。複数のセカンダリ FPolicy サーバを設定した場合、通知は各 FPolicy サーバにラウンドロビン方式で送信されます。</p>	<pre>-secondary-servers `IP_address`はい。</pre>
<p><u>_ 外部エンジンタイプ _</u></p> <p>外部エンジンが同期モードで動作するか非同期モードで動作するかを指定します。デフォルトでは、FPolicy は同期モードで動作します。</p> <p>に設定すると `synchronous` ファイル要求処理では FPolicy サーバに通知が送信されますが、その後 FPolicy サーバから応答を受信するまでは通知は送信されません。この時点で、FPolicy サーバからの応答が要求されたアクションを許可するかどうかによって、要求フローが続行されるか処理が拒否されるかが決まります。</p> <p>に設定すると `asynchronous` ファイル要求処理は、FPolicy サーバに通知を送信したあとも続行します。</p>	<pre>-extern-engine-type external_engine_type このパラメータには、次のいずれかの値を指定できます。</pre> <ul style="list-style-type: none"> <li>• synchronous</li> <li>• asynchronous</li> </ul>
<p><u>_ SSL オプションを使用して FPolicy サーバと通信します</u></p> <p>FPolicy サーバとの通信のための SSL オプションを指定します。これは必須パラメータです。次の情報に基づいて、いずれかのオプションを選択できます。</p> <ul style="list-style-type: none"> <li>• に設定すると `no-auth` 認証は行われません。</li> </ul> <p>通信リンクは TCP を介して確立されます。</p> <ul style="list-style-type: none"> <li>• に設定すると `server-auth` SVM は、SSL サーバ認証を使用して FPolicy サーバを認証します。</li> <li>• に設定すると `mutual-auth` では、SVM と FPolicy サーバの間で相互認証が行われ、SVM は FPolicy サーバを認証し、FPolicy サーバは SVM を認証します。</li> </ul> <p>相互 SSL 認証を設定する場合は、も設定する必要があります</p> <pre>-certificate-common-name、-certificate-serial`および `-certificate-ca パラメータ</pre>	<pre>-ssl-option {no-auth</pre>
<pre>server-auth</pre>	<pre>mutual-auth}</pre>

<p>_ 証明書 FQDN またはカスタム共通名 _</p> <p>SVM と FPolicy サーバ間の SSL 認証が設定されている場合、使用される証明書の名前を指定します。証明書の名前は、FQDN またはカスタム共通名として指定できます。</p> <p>を指定する場合 mutual-auth をクリックします -ssl-option パラメータを使用する場合は、に値を指定する必要があります -certificate -common-name パラメータ</p>	<p>-certificate-common -name text</p>
<p>証明書シリアル番号 _</p> <p>SVM と FPolicy サーバ間の SSL 認証が設定されている場合、認証に使用される証明書のシリアル番号を指定します。</p> <p>を指定する場合 mutual-auth をクリックします -ssl-option パラメータを使用する場合は、に値を指定する必要があります -certificate -serial パラメータ</p>	<p>-certificate-serial text</p>
<p>_ 認証局 _</p> <p>SVM と FPolicy サーバ間の SSL 認証が設定されている場合、認証に使用される証明書の CA 名を指定します。</p> <p>を指定する場合 mutual-auth をクリックします -ssl-option パラメータを使用する場合は、に値を指定する必要があります -certificate-ca パラメータ</p>	<p>-certificate-ca text</p>

## 外部エンジンの詳細オプション

高度な FPolicy 設定パラメータの次の表は、高度なパラメータを使用して設定をカスタマイズするかどうかを計画する際に使用できます。これらのパラメータは、クラスターノードと FPolicy サーバ間の通信動作を変更するために使用します。

情報のタイプ	オプション
--------	-------

<p><u> リクエストをキャンセルするためのタイムアウト </u></p> <p>時間間隔を時間単位で指定します (h) 、分 (m) 、または秒 (s) ノードはFPolicyサーバからの応答を待機します。</p> <p>タイムアウト間隔が経過すると、ノードは FPolicy サーバにキャンセル要求を送信します。その後、ノードから代替 FPolicy サーバに通知が送信されます。このタイムアウトは、応答しない FPolicy サーバを処理するのに役立ちます。これにより SMB / NFS クライアントの応答を向上させることができます。また、通知要求がパフォーマンスの低い、またはダウンした FPolicy サーバから代替 FPolicy サーバへ移されているため、タイムアウトによってリクエストをキャンセルすることは、システムリソースを解放するのに役立ちます。</p> <p>この値の範囲はです 0 から 100。値がに設定されている場合 0 オプションは無効になり、キャンセル要求メッセージはFPolicyサーバに送信されません。デフォルトはです `20s。</p>	<p>-reqs-cancel-timeout integer[h</p>
<p>m</p>	<p>s]</p>
<p><u> 要求を破棄するためのタイムアウト </u></p> <p>タイムアウトを時間単位で指定します (h) 、分 (m) 、または秒 (s) をクリックして、要求を中止します。</p> <p>この値の範囲はです 0 から 200。</p>	<p>-reqs-abort-timeout ` integer[h</p>
<p>m</p>	<p>s]</p>
<p><u> ステータス要求の送信間隔 </u></p> <p>間隔を時間単位で指定します (h) 、分 (m) 、または秒 (s) をクリックすると、FPolicyサーバにステータス要求が送信されます。</p> <p>この値の範囲はです 0 から 50。値がに設定されている場合 0 オプションは無効になり、ステータス要求メッセージはFPolicyサーバに送信されません。デフォルトはです `10s。</p>	<p>-status-req-interval integer[h</p>
<p>m</p>	<p>s]</p>
<p>FPolicy サーバの未処理要求の最大数 <u> </u></p> <p>FPolicy サーバのキューに登録できる未処理要求の最大数を指定します。</p> <p>この値の範囲はです 1 から 10000。デフォルトはです 500。</p>	<p>-max-server-reqs integer</p>

<p><u> 応答しない FPolicy サーバを切断するタイムアウト </u></p> <p>時間間隔を時間単位で指定します (h) 、分 (m) 、または秒 (s) をクリックすると、FPolicyサーバへの接続が終了します。</p> <p>FPolicy サーバのキューに許容される最大要求数が含まれていて、タイムアウト期間内に応答がない場合のみ、タイムアウト期間が経過したあとに接続を終了します。許可される要求の最大数はどちらかです 50 （デフォルト）またはで指定された番号 max-server-reqs- パラメータ</p> <p>この値の範囲はです 1 から 100。デフォルトはです 60s。</p>	<pre>-server-progress -timeout integer[h</pre>
<p>m</p>	<p>s]</p>
<p><u> FPolicy サーバにキープアライブメッセージを送信する間隔 </u></p> <p>時間間隔を時間単位で指定します (h) 、分 (m) 、または秒 (s) をクリックすると、FPolicyサーバにキープアライブメッセージが送信されます。</p> <p>キープアライブメッセージはハーフオープン接続を検出します。</p> <p>この値の範囲はです 10 から 600。値がに設定されている場合 0 オプションは無効になり、キープアライブメッセージはFPolicyサーバに送信されません。デフォルトはです 120s。</p>	<pre>-keep-alive-interval-integer[h</pre>
<p>m</p>	<p>s]</p>
<p><u> 最大再接続試行回数 </u></p> <p>接続が切断されたあと、SVM が FPolicy サーバへの再接続を試行できる最大回数を指定します。</p> <p>この値の範囲はです 0 から 20。デフォルトはです 5。</p>	<pre>-max-connection-retries integer</pre>
<p><u> 受信バッファサイズ </u></p> <p>FPolicy サーバの接続ソケットの受信バッファサイズを指定します。</p> <p>デフォルト値は 256KB に設定されています。値が 0 に設定されている場合、受信バッファのサイズはシステムによって定義されている値に設定されます。</p> <p>たとえば、ソケットのデフォルト受信バッファサイズが 65 、 536 バイトの場合、この調整可能な値を 0 に設定すると、ソケットのバッファサイズは 65 、 536 バイトに設定されます。デフォルト値以外の任意の値を使用して、受信バッファのサイズ（バイト単位）を設定できます。</p>	<pre>-recv-buffer-size integer</pre>

<p>送信バッファサイズ _</p> <p>FPolicy サーバの接続ソケットの送信バッファサイズを指定します。</p> <p>デフォルト値は 256KB に設定されています。値が 0 に設定されている場合、送信バッファのサイズはシステムによって定義されている値に設定されます。</p> <p>たとえば、ソケットのデフォルト送信バッファサイズが 65、536 バイトの場合、この調整可能な値を 0 に設定すると、ソケットのバッファサイズは 65、536 バイトに設定されます。デフォルト値以外の任意の値を使用して、送信バッファのサイズ（バイト単位）を設定できます。</p>	<pre>-send-buffer-size integer</pre>
<p>_ 再接続中にセッション ID を消去するためのタイムアウト _</p> <p>間隔を時間単位で指定します (h)、分 (m)、または秒 (s) をクリックすると、再接続の試行時に FPolicy サーバに新しいセッション ID が送信されます。</p> <p>ストレージコントローラと FPolicy サーバとの間の接続が終了して、で再接続が行われた場合 -session-timeout 間隔：古い通知に対する応答を送信できるように、古いセッション ID が FPolicy サーバに送信されます。</p> <p>デフォルト値は 10 秒に設定されています。</p>	<pre>-session-timeout [integerH][integerM][integerS]</pre>

追加情報 **SSL** 認証接続を使用するための **FPolicy** 外部エンジンの設定について

SSL サーバへの接続時に追加情報を使用するように FPolicy 外部エンジンを設定する場合は、いくつかの FPolicy を把握しておく必要があります。

## SSL サーバ認証

SSL サーバ認証用の FPolicy 外部エンジンを設定する場合には、外部エンジンを作成する前に、FPolicy サーバ証明書の署名を行った認証局（CA）のパブリック証明書をインストールする必要があります。

## 相互認証

Storage Virtual Machine（SVM）のデータ LIF を外部 FPolicy サーバに接続する際に SSL 相互認証を使用するように FPolicy 外部エンジンを設定する場合は、外部エンジンを作成する前に、次の手順を実行します。FPolicy サーバ証明書に署名した CA のパブリック証明書を、SVM の認証用のパブリック証明書およびキーファイルとともにインストールする必要があります。インストールした証明書を FPolicy ポリシーが使用している間は、この証明書を削除しないでください。

FPolicy が相互認証に使用している間に証明書を削除すると、その証明書を使用する、無効になった FPolicy ポリシーを再度有効にすることはできません。この状況では、同じ設定で証明書を新規作成して SVM にインストールしても、FPolicy ポリシーを再度有効にすることはできません。

証明書が削除されている場合は、新しい証明書をインストールして、その新しい証明書を使用する FPolicy 外部エンジンを新規作成し、FPolicy ポリシーを変更して再度有効にする FPolicy ポリシーに、新しい外部エンジンを関連付ける必要があります。



## SSL の証明書をインストールします

FPolicyサーバ証明書への署名に使用したCAのパブリック証明書は、を使用してインストールします security certificate install コマンドにを指定します -type パラメータをに設定します client-ca。SVMの認証に必要な秘密鍵とパブリック証明書は、を使用してインストールします security certificate install コマンドにを指定します -type パラメータをに設定します server。

ID が保持されない設定の SVM ディザスタリカバリ関係では、証明書がレプリケートされません

FPolicy サーバへの接続確立時の SSL 認証に使用されるセキュリティ証明書は、ID が保持されない設定の SVM ディザスタリカバリ先に複製されません。SVM 上の FPolicy 外部エンジンの設定は複製されますが、セキュリティ証明書は複製されません。セキュリティ証明書をデスティネーションに手動でインストールする必要があります。

SVMディザスタリカバリ関係を設定するときには選択した値 -identity-preserve のオプション snapmirror create コマンドは、デスティネーションSVMにレプリケートされる設定の詳細を決定します。

を設定した場合は -identity-preserve オプションをに設定します true (ID保持)。セキュリティ証明書の情報を含むFPolicy設定の詳細がすべてレプリケートされます。セキュリティ証明書をデスティネーションにインストールする必要があるのは、オプションをに設定した場合だけです false (非ID保持)。

### MetroCluster および SVM ディザスタリカバリ設定を含むクラスタ対象 FPolicy 外部エンジンの制限事項

クラスタを対象とした FPolicy 外部エンジンは、クラスタ Storage Virtual Machine (SVM) をそのエンジンに割り当てることで作成できます。ただし、クラスタ対象の外部エンジンを MetroCluster または SVM ディザスタリカバリ設定で作成する場合は、SVM が FPolicy サーバとの外部通信で使用する認証方式を選択する際にある種の制限が存在します。

外部 FPolicy サーバの作成時に選択できる認証オプションは、認証なし、SSL サーバ認証、SSL 相互認証の 3 つです。外部 FPolicy サーバがデータ SVM に割り当てられている場合は認証オプションを選択する際の制限事項はありませんが、クラスタ対象の FPolicy 外部エンジンを作成する際には制限事項があります。

設定	許可されるかどうか
MetroCluster または SVM ディザスタリカバリと、認証を行わないクラスタ対象 FPolicy 外部エンジン (SSL 未設定)	はい。
MetroCluster または SVM ディザスタリカバリと、SSL サーバ認証または SSL 相互認証を行うクラスタ対象 FPolicy 外部エンジン	いいえ

- SSL 認証を行うクラスタ対象 FPolicy 外部エンジンが存在し、MetroCluster または SVM ディザスタリカバリ設定を作成する場合は、認証をまったく使用しないようにこの外部エンジンを変更するか、MetroCluster または SVM ディザスタリカバリ設定を作成する前に外部エンジンを削除する必要があります。
- MetroCluster または SVM ディザスタリカバリ設定がすでに存在する場合は、ONTAP により、SSL 認証を行うクラスタ対象 FPolicy 外部エンジンの作成が阻止されます。

このワークシートを使用して、FPolicy 外部エンジンの設定プロセス中に必要となる値を記録できます。パラメータ値が必須の場合は、外部エンジンを設定する前に、そのパラメータに使用する値を決定する必要があります。

#### 外部エンジンの基本的な設定に関する情報

外部エンジンの設定に各パラメータ設定を含めるかどうかを記録し、含めるパラメータの値を記録しておく必要があります。

情報のタイプ	必須	含める	値を入力します
Storage Virtual Machine （SVM）名	はい。	はい。	
エンジン名	はい。	はい。	
プライマリ FPolicy サーバ	はい。	はい。	
ポート番号	はい。	はい。	
セカンダリ FPolicy サーバ	いいえ		
外部エンジンタイプ	いいえ		
外部 FPolicy サーバとの通信のための SSL オプション	はい。	はい。	
証明書の FQDN またはカスタム共通名	いいえ		
証明書のシリアル番号	いいえ		
認証局	いいえ		

#### 外部エンジンの詳細パラメータに関する情報

外部エンジンを詳細パラメータで設定するには、advanced 権限モードで設定コマンドを入力する必要があります。

情報のタイプ	必須	含める	値を入力します
要求をキャンセルするためのタイムアウト	いいえ		
要求を破棄するためにタイムアウトしました	いいえ		

ステータス要求の送信間隔	いいえ		
FPolicy サーバの未処理要求の最大数	いいえ		
応答しない FPolicy サーバを切断するタイムアウト	いいえ		
FPolicy サーバへのキープアライブメッセージの送信間隔	いいえ		
再接続の最大試行回数	いいえ		
受信バッファサイズ	いいえ		
送信バッファサイズ	いいえ		
再接続時にセッション ID を破棄するためのタイムアウト	いいえ		

## FPolicy イベントの設定を計画します

### FPolicy イベントの設定の概要を計画します

FPolicy イベントを設定する前に、FPolicy イベントを作成することの意味を理解する必要があります。イベントで監視するプロトコル、監視するイベント、使用するイベントフィルタを決定する必要があります。この情報は、設定する値を計画するのに役立ちます。

### FPolicy イベントを作成することの意味

FPolicy イベントを作成することは、どのファイルアクセス操作を監視するか、またどの監視対象イベント通知を外部 FPolicy サーバに送信するかを決定するために、FPolicy プロセスで必要となる情報を定義することを意味します。FPolicy イベントの設定では、次の設定情報を定義します。

- Storage Virtual Machine （SVM）名
- イベント名
- 監視するプロトコル

FPolicy は、SMB、NFSv3、および NFSv4 のファイルアクセス処理を監視できます。

- 監視するファイル操作

すべてのファイル操作が各プロトコルに対して有効であるとは限りません。

- 構成するファイルフィルタ

ファイル操作とフィルタの特定の組み合わせのみが有効です。各プロトコルには、サポートされる独自の組み合わせがあります。

- ボリュームのマウントおよびアンマウント操作を監視するかどうか




3つのパラメータには依存関係があります (-protocol、-file-operations、-filters)。以下の組み合わせが3つのパラメータで有効です。

- を指定できます -protocol および -file-operations パラメータ
- 3つのパラメータをすべて同時に指定することもできます。
- いずれのパラメータも指定しないでください。

**FPolicy イベント構成に含まれるもの**

次に示す使用可能な FPolicy イベント設定パラメータの一覧は、構成を計画するのに役立ちます。

情報のタイプ	オプション
<p>SVM</p> <p>この FPolicy イベントに関連付ける SVM の名前を指定します。</p> <p>各 FPolicy 設定は、単一の SVM 内で定義されます。FPolicy ポリシーの構成要素となる外部エンジン、ポリシーイベント、ポリシーのスコープ、およびポリシーを、すべて同じ SVM に関連付ける必要があります。</p>	<p>-vserver vservice_name</p>
<p>_ イベント名 _</p> <p>FPolicy イベントに割り当てる名前を指定します。FPolicy ポリシーを作成する際には、イベント名を使用して FPolicy イベントをポリシーに関連付けます。</p> <p>この名前に指定できる文字数は最大 256 文字です。</p> <div><div></div><div>MetroCluster または SVM ディザスタリカバリ設定でイベントを設定する場合、この名前は最大 200 文字にする必要があります。</div></div> <p>名前には、次の ASCII 文字の任意の組み合わせを含めることができます。</p> <ul style="list-style-type: none"><li>• a から z</li><li>• A から Z</li><li>• 0 から 9</li><li>• " _ "、" - "、" . "、and " . "</li></ul>	<p>-event-name event_name</p>

<p>プロトコル _</p> <p>FPolicy イベント用に設定するプロトコルを指定します。のリスト -protocol 次のいずれかの値を指定できます。</p> <ul style="list-style-type: none"> <li>• cifs</li> <li>• nfsv3</li> <li>• nfsv4</li> </ul> <div data-bbox="167 520 220 573">  </div> <div data-bbox="284 478 1044 615"> <p>を指定する場合 -protocol`をクリックした場合は、で有効な値を指定する必要があります ` -file-operations パラメータプロトコルのバージョンによって、有効な値が変わる可能性があります。</p> </div>	<p>-protocol protocol</p>
---	---------------------------

## \_ ファイル操作 \_

FPolicy イベントのファイル操作のリストを指定します。

イベントは、で指定されたプロトコルを使用して、すべてのクライアント要求からこのリストに指定された操作をチェックします `-protocol` パラメータ1つ以上のファイル操作をカンマで区切って指定できます。のリスト `-file-operations` 次の値を1つ以上指定できます。

- `close` ファイルクローズ操作の場合
- `create` ファイル作成操作の場合
- `create-dir` ディレクトリ作成操作に使用します
- `delete` ファイル削除操作に使用します
- `delete_dir` ディレクトリ削除操作の場合
- `getattr` 属性取得操作の場合
- `link` リンク操作の場合
- `lookup` 検索操作に使用します
- `open` ファイルオープン操作の場合
- `read` ファイル読み取り操作に使用します
- `write` ファイル書き込み操作の場合
- `rename` ファイル名変更操作の場合
- `rename_dir` ディレクトリ名変更操作
- `setattr` 属性設定操作の場合
- `symlink` シンボリックリンク操作に使用します



を指定する場合 `-file-operations`` をクリックした場合は、で有効なプロトコルを指定する必要があります ``-protocol` パラメータ

`-file-operations`file_operations`` はい。

## \_ フィルタ \_

-filters `filter`はい。

指定したプロトコルにおける所定のファイル操作に対するフィルタのリストを指定します。の値を指定します -filters パラメータは、クライアント要求をフィルタリングするために使用します。リストには次の値を 1 つ以上指定できます。



を指定する場合は -filters パラメータを指定すると、の有効な値も指定する必要があります -file-operations および -protocol パラメータ

- monitor-ads 代替データストリームを要求するクライアント要求をフィルタリングするオプション。
- close-with-modification 変更してクローズ操作を要求するクライアント要求をフィルタリングするオプション。
- close-without-modification 変更せずにクローズ操作を要求するクライアント要求をフィルタリングするオプション。
- first-read 初回の読み取りを要求するクライアント要求をフィルタリングするオプション。
- first-write 初回の書き込みを要求するクライアント要求をフィルタリングするオプション。
- offline-bit オフラインビットの設定を要求するクライアント要求をフィルタリングするオプション。

このフィルタを設定すると、オフラインのファイルがアクセスされた場合のみ FPolicy サーバが通知を受信します。

- open-with-delete-intent 削除するためにファイルのオープンを要求するクライアント要求をフィルタリングするオプション。

このフィルタを設定すると、削除するためにファイルが開かれた場合のみ FPolicy サーバが通知を受信します。これは、ファイルシステムでが使用されるときに使用されます FILE\_DELETE\_ON\_CLOSE フラグが指定されています。

- open-with-write-intent 書き込み目的でのオープン操作を要求するクライアント要求をフィルタリングするオプション。

このフィルタを設定すると、書き込むためにファイルを開いた場合のみ FPolicy サーバが通知を受信します。

- write-with-size-change 書き込みと同時にサイズの変更を要求するクライアント要求をフィルタリングするオプション。

## \_ フィルタ \_ 続き

-filters `filter`はい。

- `setattr-with-owner-change` ファイルまたはディレクトリの所有者を変更するクライアント属性設定要求をフィルタリングするオプション。
- `setattr-with-group-change` ファイルまたはディレクトリのグループを変更するクライアント属性設定要求をフィルタリングするオプション。
- `setattr-with-sacl-change` ファイルまたはディレクトリのSACLを変更するクライアント属性設定要求をフィルタリングします。

このフィルタは、SMBプロトコルとNFSv4プロトコルでのみ使用できます。

- `setattr-with-dacl-change` ファイルまたはディレクトリのDACLを変更するクライアント属性設定要求をフィルタリングします。

このフィルタは、SMBプロトコルとNFSv4プロトコルでのみ使用できます。

- `setattr-with-modify-time-change` ファイルまたはディレクトリの変更日時を変更するクライアント属性設定要求をフィルタリングするオプション。
- `setattr-with-access-time-change` ファイルまたはディレクトリのアクセス時間を変更するクライアント属性設定要求をフィルタリングするオプション。
- `setattr-with-creation-time-change` ファイルまたはディレクトリの作成日時を変更するクライアント属性設定要求をフィルタリングするオプション。

このオプションは、SMBプロトコルに対してのみ使用できます。

- `setattr-with-mode-change` オプション：ファイルまたはディレクトリのモードビットを変更するクライアント属性設定要求をフィルタリングします。
- `setattr-with-size-change` ファイルサイズを変更するクライアント属性設定要求をフィルタリングするオプション。
- `setattr-with-allocation-size-change` ファイルの割り当てサイズを変更するクライアント属性設定要求をフィルタリングするオプション。

このオプションは、SMBプロトコルに対してのみ使用できます。

- `exclude-directory` ディレクトリ操作を要求するクライアント要求をフィルタリングするオプション。

このフィルタを指定すると、ディレクトリ操作は監視されません。



は、ボリューム処理が必要です _	-volume-operation {true
ボリュームのマウントおよびアンマウント操作に対して監視が必要かどうかを指定します。デフォルトはです false。	
false}	<i>FPolicy</i> アクセスが通知を拒否しました
-filters `filter`はい。	ONTAP 9.13.1以降では、権限がないためにファイル処理が失敗した場合に通知を受け取ることができます。これらの通知は、セキュリティ、ランサムウェア対策、ガバナンスに役立ちます。権限がないためにファイル操作が失敗した場合は、次のような通知が生成されます。
	<ul style="list-style-type: none"> <li>• NTFS権限が原因でエラーが発生しました。</li> <li>• UNIXモードビットによるエラー。</li> <li>• NFSv4 ACLに起因するエラー。</li> </ul>
-monitor-fileop-failure {true	false}

**FPolicy**で監視可能な、サポートされるファイル処理とフィルタの組み合わせ（SMB）

FPolicy イベントを設定する場合、SMB のファイルアクセスの監視では、サポートされるファイル操作とフィルタの組み合わせに制限があることを考慮する必要があります。

以下の表に、FPolicy による SMB ファイルアクセスイベントの監視でサポートされるファイル操作とフィルタの組み合わせを示します。

サポートされているファイル操作	サポートされているフィルタ
を閉じます	monitor-ads 、 offline-bit 、 close-with-modification 、 close-without-modification 、 close-with-read 、 exclude-directory
作成	monitor-ads 、 offline-bit
create_dir	現在、このファイル操作ではフィルタはサポートされていません。
削除	monitor-ads 、 offline-bit

delete_dir	現在、このファイル操作ではフィルタはサポートされていません。
属性の取得	offline-bit 、 exclud-dir のいずれかを指定します
を開きます	monitor-ads 、 offline-bit 、 open-with-delete-intent 、 open-with-write-intent 、 exclud-dir
読み取り	monitor-ads 、 offline-bit 、 first-read
書き込み	monitor-ads 、 offline-bit 、 first-write 、 write-with-size-change
名前を変更する	monitor-ads 、 offline-bit
rename_dir	現在、このファイル操作ではフィルタはサポートされていません。
属性の設定	monitor-ads 、 offline-bit 、 setattr_-with-owner_change 、 setattr_-with-group_change 、 setattr_-with-mode_change 、 setattr_-with_sacl_change 、 setattr_-with_dacl_change 、 setattr_-with-mody_time-change 、 setattr_-with-access-name_time-change 、 setattr_-with-creation_time-change 、 setattr-with_size_change 、 setattr_-with-allocation_size_change 、 exclude_directory

ONTAP 9.13.1以降では、権限がないためにファイル処理が失敗した場合に通知を受け取ることができます。次の表に、FPolicyによるSMBファイルアクセスイベントの監視でサポートされるアクセス拒否ファイル操作とフィルタの組み合わせを示します。

サポートされるアクセス拒否ファイル操作	サポートされているフィルタ
を開きます	NA

**FPolicy**で監視可能なサポートされるファイル処理とフィルタの組み合わせ（**NFSv3**）

FPolicyイベントを設定する場合、NFSv3のファイルアクセス操作の監視では、サポートされるファイル操作とフィルタの組み合わせに制限があることに注意する必要があります。

次の表に、FPolicyによるNFSv3ファイルアクセスイベントの監視でサポートされるファイル処理とフィルタの組み合わせを示します。

サポートされているファイル操作	サポートされているフィルタ
作成	オフラインビット
create_dir	現在、このファイル操作ではフィルタはサポートされていません。

削除	オフラインビット
delete_dir	現在、このファイル操作ではフィルタはサポートされていません。
リンク	オフラインビット
検索	offline-bit 、 exclud-dir のいずれかを指定します
読み取り	オフラインビット、初回読み取り
書き込み	オフラインビット、初回書き込み、 write-with-size-change
名前を変更する	オフラインビット
rename_dir	現在、このファイル操作ではフィルタはサポートされていません。
属性の設定	offline-bit 、 setattr_-with-owner_change 、 setattr_name_group-change 、 setattr_-with-mode_change 、 setattr_-with-mode_change 、 setattr_-with-mode_time-change 、 setattr_-with-access-time-change 、 setattr_-with-size_change 、 exclude_directory
シンボリックリンク	オフラインビット

ONTAP 9.13.1以降では、権限がないためにファイル処理が失敗した場合に通知を受け取ることができます。次の表に、FPolicyによるNFSv3ファイルアクセスイベントの監視でサポートされるアクセス拒否ファイル処理とフィルタの組み合わせを示します。

サポートされるアクセス拒否ファイル操作	サポートされているフィルタ
にアクセスします	NA
作成	NA
create_dir	NA
削除	NA
delete_dir	NA
リンク	NA
読み取り	NA

名前を変更する	NA
rename_dir	NA
属性の設定	NA
書き込み	NA

**FPolicy** で **NFSv4** を監視するために、サポートされるファイル操作とフィルタの組み合わせ

FPolicy イベントを設定する場合、NFSv4 のファイルアクセス操作の監視では、サポートされるファイル操作とフィルタの組み合わせに制限があることを考慮する必要があります。

以下の表に、FPolicy による NFSv4 ファイルアクセスイベントの監視でサポートされるファイル操作とフィルタの組み合わせを示します。

サポートされているファイル操作	サポートされているフィルタ
を閉じます	offline-bit 、 exclude-directory
作成	オフラインビット
create_dir	現在、このファイル操作ではフィルタはサポートされていません。
削除	オフラインビット
delete_dir	現在、このファイル操作ではフィルタはサポートされていません。
属性の取得	offline-bit 、 exclude-directory
リンク	オフラインビット
検索	offline-bit 、 exclude-directory
を開きます	offline-bit 、 exclude-directory
読み取り	オフラインビット、初回読み取り
書き込み	オフラインビット、初回書き込み、 write-with-size-change
名前を変更する	オフラインビット

rename_dir	現在、このファイル操作ではフィルタはサポートされていません。
属性の設定	offline-bit 、 setattr_-with-owner_change 、 setattr_-with-group_change 、 setattr_-with-mode_change 、 setattr_-with-acl_change 、 setattr_-with_dacl_change 、 setattr_on_mode_time-change 、 setattr_-with-access-time-change 、 setattr_-with_size_change 、 exclude_directory
シンボリックリンク	オフラインビット

ONTAP 9.13.1以降では、権限がないためにファイル処理が失敗した場合に通知を受け取ることができます。次の表に、FPolicyによるNFSv4ファイルアクセスイベントの監視でサポートされるアクセス拒否ファイル操作とフィルタの組み合わせを示します。

サポートされるアクセス拒否ファイル操作	サポートされているフィルタ
にアクセスします	NA
作成	NA
create_dir	NA
削除	NA
delete_dir	NA
リンク	NA
を開きます	NA
読み取り	NA
名前を変更する	NA
rename_dir	NA
属性の設定	NA
書き込み	NA

**FPolicy イベントの設定ワークシートに記入**

このワークシートを使用して、FPolicy イベントの設定プロセス中に必要となる値を記録できます。パラメータ値が必須の場合は、FPolicy イベントを設定する前に、そのパラメータに使用する値を決定する必要があります。

FPolicy イベントの設定に各パラメータ設定を含めるかどうかを記録し、含めるパラメータの値を記録しておく必要があります。

情報のタイプ	必須	含める	値を入力します
Storage Virtual Machine （ SVM ） 名	はい。	はい。	
イベント名	はい。	はい。	
プロトコル	いいえ		
ファイル操作	いいえ		
フィルタ	いいえ		
ボリューム操作	いいえ		
アクセス拒否イベント+ （ONTAP 9.13以降でサポート）	いいえ		

## FPolicy ポリシーの設定を計画します

### FPolicy ポリシーの設定の概要を計画

FPolicy ポリシーを設定する前に、ポリシーの作成時に必要なパラメータや、特定のオプションパラメータを設定する理由について理解しておく必要があります。この情報は、各パラメータに設定する値を決定するのに役立ちます。

FPolicy ポリシーを作成する際には、このポリシーと次のポリシーを関連付けます。

- Storage Virtual Machine （ SVM ）
- 1 つ以上の FPolicy イベント
- FPolicy 外部エンジン

いくつかのオプションポリシー設定を構成することもできます。

### FPolicy ポリシーの設定項目

FPolicy ポリシーで使用できる必須パラメータとオプションパラメータを次に示します。これは設定について計画するときに役立ちます。

情報のタイプ	オプション	必須	デフォルト
--------	-------	----	-------

<p>SVM 名 _</p> <p>FPolicy ポリシーを作成する SVM の名前を指定します。</p>	<p>-vserver vserver_name</p>	<p>はい。</p>	<p>なし</p>
<p>_ ポリシー名 _</p> <p>FPolicy ポリシーの名前を指定します。</p> <p>この名前に指定できる文字数は最大 256 文字です。</p> <div>  <p>MetroCluster または SVM ディザスタリカバリ設定でポリシーを設定する場合、この名前は最大 200 文字にする必要があります。</p> </div> <p>名前には、次の ASCII 文字の任意の組み合わせを含めることができます。</p> <ul style="list-style-type: none"> <li>• a から z</li> <li>• A から Z</li> <li>• 0 から 9</li> <li>• 「_」、「-」, and “.”</li> </ul>	<p>-policy-name policy_name</p>	<p>はい。</p>	<p>なし</p>
<p>_ イベント名 _</p> <p>FPolicy ポリシーに関連付けるイベントをカンマ区切りのリストで指定します。</p> <ul style="list-style-type: none"> <li>• 1 つのポリシーに複数のイベントに関連付けることができます。</li> <li>• イベントはプロトコルに固有です。</li> <li>• 1 つのポリシーで複数のプロトコルのファイルアクセスイベントを監視するには、ポリシーで監視する各プロトコルのイベントを作成し、それらのイベントをポリシーに関連付けます。</li> <li>• 既存のイベントを指定する必要があります。</li> </ul>	<p>-events `event_name`はい。</p>	<p>はい。</p>	<p>なし</p>

<p><u>外部エンジン名</u></p> <p>FPolicy ポリシーに関連付ける外部エンジンの名前を指定します。</p> <ul style="list-style-type: none"> <li>外部エンジンには、ノードから FPolicy サーバに通知を送信するための必要な情報が格納されています。</li> <li>単純なファイルブロッキングを行うために ONTAP の標準の外部エンジンを使用したり、より高度なファイルブロッキングとファイル管理を行うために外部 FPolicy サーバ（FPolicy サーバ）を使用するように設定された外部エンジンを使用したりするように FPolicy を設定できます。</li> <li>標準の外部エンジンを使用する場合は、このパラメータの値を指定しないか、を指定できます native を値として入力します。</li> <li>FPolicy サーバを使用する場合は、外部エンジンの設定がすでに存在している必要があります。</li> </ul>	<p>-engine engine_name</p>	<p>○（ポリシーで内部の ONTAP 標準エンジンを使用しない場合）</p>	<p>native</p>
<p><u>は必須のスクリーニングです</u></p> <p>必須のファイルアクセススクリーニングを要求するかどうかを指定します。</p> <ul style="list-style-type: none"> <li>必須のスクリーニング設定は、プライマリサーバとセカンダリサーバがすべて停止した場合や、指定した時間内に FPolicy サーバからの応答を得られない場合に、ファイルアクセスイベントをどのように処理するかを決定します。</li> <li>に設定すると `true` に設定すると、ファイルアクセスイベントが拒否されます。</li> <li>に設定すると `false` に設定すると、ファイルアクセスイベントが許可されます。</li> </ul>	<p>-is-mandatory {true</p>	<p>false}</p>	<p>いいえ</p>



true	<p>権限付きアクセスを許可する _</p> <p>権限付きデータ接続による監視対象のファイルやフォルダに対する権限付きアクセスを FPolicy サーバに許可するかどうかを指定します。</p> <p>設定されている場合、FPolicy サーバは権限付きデータ接続を使用して、監視対象データが格納されている SVM のルートにあるファイルにアクセスできます。</p> <p>権限付きデータアクセスの場合は、クラスタでSMBのライセンスが有効になっていて、FPolicyサーバへの接続に使用されるすべてのデータLIFがに設定されている必要があります。cifs 許可されているプロトコルの1つとして指定します。</p> <p>ポリシーで権限付きアクセスを許可する場合は、FPolicy サーバで権限付きアクセスに使用するアカウントのユーザ名も指定する必要があります。</p>	<pre>-allow -privileged -access {yes</pre>	no}
------	---	--	-----

No (パススルーリードが有効になっていない場合)	no	<p>_ 特権ユーザ名 _</p> <p>FPolicy サーバが権限付きデータアクセスで使用するアカウントのユーザ名を指定します。</p> <ul style="list-style-type: none"> <li>• このパラメータの値は、「ドメイン\ユーザ名」の形式にする必要があります。</li> <li>• 状況 -allow -privileged -access がに設定されます`no`を指定すると、このパラメータに設定された値は無視されます。</li> </ul>	<p>-privileged -user-name user_name</p>
---------------------------	----	--	---

<p>No（権限付きアクセスが有効になっていない場合）</p>	<p>なし</p>	<p><code>_allow passthrough-read _</code></p> <p>FPolicy サーバによってセカンダリストレージ（オフラインファイル）にアーカイブされているファイルを対象としたパススルーリードサービスを FPolicy サーバが提供できるかどうかを指定します。</p> <ul style="list-style-type: none"> <li>パススルーリードは、オフラインファイルのデータをプライマリストレージにリストアすることなく読み取るための手段です。</li> </ul> <p>パススルーリードでは、読み取り要求に応答する前にファイルをプライマリストレージにリコールする必要がないため、応答遅延が短縮されます。また、パススルーリードでは、読み取り要求を満たすためだけにリコールされるファイルによってストレージ領域を浪費する必要がなくなるため、ストレージ効率が最適化されます。</p> <ul style="list-style-type: none"> <li>有効になっている場合、FPolicy サーバはパススルーリード専用に開かれている別の権限付きデータチャネルを使用してファイルにデータを提供します。</li> </ul>	<pre>-is-passthrough -read-enabled {true</pre>
---------------------------------	-----------	--	--

FPolicy ポリシーで標準のエンジンを使用する場合の FPolicy スコープ設定の要件

標準のエンジンを使用するように FPolicy ポリシーを設定する場合、ポリシーで設定される FPolicy スコープの定義方法に関して特定の要件があります。

FPolicy スコープは、FPolicy 環境で指定されたボリュームや共有などシ FPolicy が適用される範囲の境界を定義します。FPolicy ポリシーが適用されるスコープをさらに制限するためのパラメータが多数あります。次のいずれかのパラメータ `-is-file-extension-check-on-directories-enabled` では、ディレクトリのファイル拡張子をチェックするかどうかを指定します。デフォルト値はです `false` これは、ディレクトリ上のファイル拡張子はチェックされないことを意味します。

標準のエンジンを使用する FPolicy ポリシーが共有またはボリュームおよびで有効になっている場合 `-is-file-extension-check-on-directories-enabled` パラメータはに設定されます `false` ポリシーのスコープでは、ディレクトリへのアクセスは拒否されます。この設定では、ディレクトリのファイル拡張子はチェックされないため、ポリシーのスコープ下にあるディレクトリ操作はすべて拒否されます。

標準のエンジンを使用している場合にディレクトリへのアクセスを成功させるには、を設定する必要があります `-is-file-extension-check-on-directories-enabled` parameter 終了: `true` 有効範囲の作成時。

(このパラメータはに設定されています) `true` では、ディレクトリ操作に対して拡張子のチェックが実行され、アクセスを許可するか拒否するかは、FPolicy スコープ設定に含まれている拡張子または除外されている拡張子に基づいて決定されます。

FPolicy ポリシーのワークシートに記入

このワークシートを使用して、FPolicy ポリシー設定プロセス中に必要となる値を記録できます。FPolicy ポリシーの設定に各パラメータ設定を含めるかどうかを記録し、含めるパラメータの値を記録しておく必要があります。

情報のタイプ	含める	値を入力します
Storage Virtual Machine （ SVM ） 名	はい。	
ポリシー名	はい。	
イベント名	はい。	
外部エンジンの名前		
スクリーニングを必須にするかどうか		
権限付きアクセスを許可します		
権限を持つユーザの名前		
パススルーリードが有効かどうか		

## FPolicy スコープの設定を計画します

### FPolicy スコープの設定の概要を計画します

FPolicy スコープを設定する前に、スコープを作成することの意味を理解する必要があります。スコープの構成要素を理解する必要があります。また、スコープの優先規則についても理解する必要があります。この情報は、設定する値を計画するのに役立ちます。

### FPolicy スコープを作成することの意味

FPolicy スコープを作成することは、FPolicy ポリシーの適用範囲を定義することを意味します。Storage Virtual Machine (SVM) は基本の適用範囲です。FPolicy ポリシーのスコープを作成する場合、スコープが適用される FPolicy ポリシーを定義する必要があり、さらにスコープを適用する SVM を指定する必要があります。

指定した SVM 内にスコープをさらに制限するためのパラメータが数多くあります。スコープに含めるものを指定したり、スコープから除外するものを指定したりすることでスコープを制限することができます。有効なポリシーにスコープを適用すると、ポリシーイベントのチェックがこのコマンドで定義したスコープに適用されます。

「include」オプションで一致するファイルアクセスイベントが見つかった場合に、通知が生成されます。「EXCLUDE」オプションで一致するファイルアクセスイベントについては、通知は生成されません。

FPolicy スコープの構成では、次の設定情報を定義します。

- SVM 名
- ポリシー名
- 監視対象に含めるまたは監視対象から除外する共有
- 監視対象に含めるまたは監視対象から除外するエクスポートポリシー
- 監視対象に含めるまたは監視対象から除外するボリューム
- 監視対象に含めるまたは監視対象から除外するファイル拡張子
- ディレクトリオブジェクトに対してファイル拡張子を監視するかどうか



クラスタの FPolicy ポリシーのスコープには、特に考慮すべき事項があります。クラスタの FPolicy ポリシーは、クラスタ管理者が管理 SVM 用に作成するポリシーです。クラスタ管理者がそのクラスタの FPolicy ポリシーのスコープも作成する場合、SVM 管理者はそれと同じポリシーのスコープを作成することはできません。ただし、クラスタ管理者がクラスタの FPolicy ポリシーのスコープを作成しない場合は、すべての SVM 管理者がそのクラスタポリシーのスコープを作成することができます。SVM 管理者がそのクラスタの FPolicy ポリシーのスコープを作成した場合、クラスタ管理者はそれ以降、その同じクラスタポリシーのクラスタスコープを作成することはできません。これは、クラスタ管理者が同じクラスタポリシーのスコープを上書きできないためです。

### スコープの優先規則

スコープの設定には、次の優先規則が適用されます。

- 共有がに含まれる場合 `-shares-to-include` 共有のパラメータと親ボリュームがに含まれます

-volumes-to-exclude パラメータ -volumes-to-exclude が優先されます -shares-to-include。

- エクスポートポリシーがに含まれている場合 -export-policies-to-include エクスポートポリシーのパラメータと親ボリュームがに含まれます -volumes-to-exclude パラメータ -volumes-to-exclude が優先されます -export-policies-to-include。

- 管理者は両方を指定できます -file-extensions-to-include および -file-extensions-to-exclude リスト。

。 -file-extensions-to-exclude パラメータは、の前にチェックされます -file-extensions-to-include パラメータがチェックされています。

## FPolicy スコープの構成要素を次に示します

次に示す使用可能な FPolicy スコープの設定パラメータの一覧は、構成を計画するのに役立ちます。



スコープに含めるか除外する共有、エクスポートポリシー、ボリューム、およびファイル拡張子を設定する際に、includeパラメータとexcludeパラメータにメタ文字（「|」など）を含めることができます?" and "\*"。正規表現の使用はサポートされていません。

情報のタイプ	オプション
<b>SVM</b>  FPolicy スコープを作成する SVM の名前を指定します。  各 FPolicy 設定は、単一の SVM 内で定義されます。FPolicy ポリシーの構成要素となる外部エンジン、ポリシーイベント、ポリシーのスコープ、およびポリシーを、すべて同じ SVM に関連付ける必要があります。	-vserver vserver_name
<b>_ ポリシー名 _</b>  スコープをアタッチする FPolicy ポリシーの名前を指定します。FPolicy ポリシーがすでに存在している必要があります。	-policy-name policy_name
<b>含める共有 _</b>  カンマで区切って複数の共有を指定し、FPolicy ポリシーの監視対象となるスコープに含めます。	-shares-to-include 'share_name'はい。
<b>_ 除外する共有 _</b>  カンマで区切って複数の共有を指定し、FPolicy ポリシーの監視対象となるスコープから除外します。	-shares-to-exclude 'share_name'はい。
<b>対象に含めるボリューム： FPolicy ポリシーの監視対象となるボリュームをカンマで区切って指定します。</b>	-volumes-to-include 'volume_name'はい。

<p>除外するボリューム <code>_</code></p> <p>カンマで区切って複数のボリュームを指定し、FPolicy ポリシーの監視対象となるスコープから除外します。</p>	<pre>-volumes-to-exclude `volume_name`はい。</pre>
<p>ポリシーを含めるには <code>_</code> をエクスポートします</p> <p>カンマで区切って複数のエクスポートポリシーを指定し、FPolicy ポリシーの監視対象となるスコープに含めます。</p>	<pre>-export-policies-to -include `export_policy_name`はい。</pre>
<p>ポリシーを <code>exclude_</code> にエクスポートします</p> <p>カンマで区切って複数のエクスポートポリシーを指定し、FPolicy ポリシーの監視対象となるスコープから除外します。</p>	<pre>-export-policies-to -exclude `export_policy_name`はい。</pre>
<p><code>_include</code> するファイル拡張子 <code>_</code></p> <p>カンマで区切って複数のファイル拡張子を指定し、FPolicy ポリシーの監視対象となるスコープに含めます。</p>	<pre>-file-extensions-to -include `file_extensions`はい。</pre>
<p><code>_</code> ファイル拡張子を <code>exclude_</code> に設定します</p> <p>カンマで区切って複数のファイル拡張子を指定し、FPolicy ポリシーの監視対象となるスコープから除外します。</p>	<pre>-file-extensions-to -exclude `file_extensions`はい。</pre>
<p><code>_</code> ディレクトリのファイル拡張子チェックは有効になっていますか？ <code>_</code></p> <p>ファイル名の拡張子の監視をディレクトリオブジェクトに適用するかどうかを指定します。このパラメータがに設定されている場合 <code>`true`</code> の場合、ディレクトリオブジェクトには、通常のファイルと同じ拡張子チェックが適用されます。このパラメータがに設定されている場合 <code>`false`</code> では、ディレクトリ名の拡張子は照合されず、名前の拡張子が一致しない場合でも、ディレクトリに関する通知が送信されます。</p> <p>スコープの割り当て先のFPolicyポリシーが標準のエンジンを使用するように設定されている場合は、このパラメータをに設定する必要があります <code>true</code>。</p>	<pre>-is-file-extension -check-on-directories -enabled {true</pre>
<p><code>false</code></p>	<pre>}</pre>

**FPolicy** スコープのワークシートに情報を記入します

このワークシートを使用して、FPolicy スコープの設定プロセス中に必要となる値を記録できます。パラメータ値が必須の場合は、FPolicy スコープを設定する前に、そのパラメータに使用する値を決定する必要があります。

FPolicy スコープの設定に各パラメータ設定を含めるかどうかを記録し、含めるパラメータの値を記録しておく必要があります。

情報のタイプ	必須	含める	値を入力します
Storage Virtual Machine （ SVM ） 名	はい。	はい。	
ポリシー名	はい。	はい。	
対象に含める共有	いいえ		
対象から除外する共有	いいえ		
対象に含めるボリューム	いいえ		
ボリュームを除外する	いいえ		
エクスポートポリシーを含める	いいえ		
エクスポートポリシーを除外する	いいえ		
対象に含めるファイル拡張子	いいえ		
対象から除外するファイル拡張子	いいえ		
ディレクトリのファイル拡張子の監視が有効かどうか	いいえ		

## FPolicy の設定を作成します

### FPolicy 外部エンジンを作成します

FPolicy の設定を作成するには、最初に外部エンジンを作成する必要があります。外部エンジンは、FPolicy で外部 FPolicy サーバへの接続を確立および管理する方法を定義します。内部の ONTAP エンジン（標準の外部エンジン）を単純なファイルブロッキングに使用している設定の場合は、FPolicy 外部エンジンを別途設定する必要がないため、この手順の実行は不要です。

必要なもの

。"外部エンジン" ワークシートを記入する必要があります。

このタスクについて

外部エンジンが MetroCluster 構成で使用されている場合は、ソースサイトでの FPolicy サーバの IP アドレスをプライマリサーバとして指定する必要があります。デスティネーションサイトでの FPolicy サーバの IP アドレスは、セカンダリサーバとして指定する必要があります。

手順

1. を使用して FPolicy 外部エンジンを作成します `vserver fpolicy policy external-engine`



create コマンドを実行します

次のコマンドは、Storage Virtual Machine（SVM）vs1.example.com 上に外部エンジンを作成します。FPolicy サーバとの外部通信に認証は必要ありません。

```
vserver fpolicy policy external-engine create -vserver-name vs1.example.com
-engine-name engine1 -primary-servers 10.1.1.2,10.1.1.3 -port 6789 -ssl-option
no-auth
```

- 2. を使用してFPolicy外部エンジンの設定を確認します vserver fpolicy policy external-engine show コマンドを実行します

次のコマンドは、SVM vs1.example.com で設定されているすべての外部エンジンに関する情報を表示します。

```
vserver fpolicy policy external-engine show -vserver vs1.example.com
```

		Primary	Secondary	
External Vserver Type	Engine	Servers	Servers	Port Engine
-----	-----	-----	-----	-----
vs1.example.com synchronous	engine1	10.1.1.2, 10.1.1.3	-	6789

次のコマンドは、SVM vs1.example.com 上の「engine1」という外部エンジンに関する詳細情報を表示します。

```
vserver fpolicy policy external-engine show -vserver vs1.example.com -engine
-name engine1
```

Vserver:	vs1.example.com
Engine:	engine1
Primary FPolicy Servers:	10.1.1.2, 10.1.1.3
Port Number of FPolicy Service:	6789
Secondary FPolicy Servers:	-
External Engine Type:	synchronous
SSL Option for External Communication:	no-auth
FQDN or Custom Common Name:	-
Serial Number of Certificate:	-
Certificate Authority:	-

**FPolicy イベントを作成します**

FPolicy ポリシーの設定を作成する手順の一環として、FPolicy イベントを作成する必要があります。FPolicy ポリシーを作成するときに、このイベントをポリシーに関連付けます。イベントは、監視するプロトコルと、監視およびフィルタリングするファイルアクセスイベントを定義します。

作業を開始する前に

FPolicy イベントを完了する必要があります ["ワークシート"](#)。

**FPolicy イベントを作成します**

- 1. を使用してFPolicyイベントを作成します vservers fpolicy policy event create コマンドを実行します

```
vservers fpolicy policy event create -vservers vs1.example.com -event-name event1 -protocol cifs -file-operations open,close,read,write
```

- 2. を使用してFPolicyイベントの設定を確認します vservers fpolicy policy event show コマンドを実行します

```
vservers fpolicy policy event show -vservers vs1.example.com
```

Vservers	Event Name	Protocols	File Operations	Filters	Is Volume Operation
vs1.example.com	event1	cifs	open, close, read, write	-	false

**FPolicy アクセス拒否イベントを作成します**

ONTAP 9.13.1以降では、権限がないためにファイル処理が失敗した場合に通知を受け取ることができます。これらの通知は、セキュリティ、ランサムウェア対策、ガバナンスに役立ちます。

- 1. を使用してFPolicyイベントを作成します vservers fpolicy policy event create コマンドを実行します

```
vservers fpolicy policy event create -vservers vs1.example.com -event-name event1 -protocol cifs -monitor-fileop-failure true -file-operations open
```

**永続ストアの作成**

ONTAP 9.14.1以降では、FPolicyを使用して ["永続的ストア"](#) SVM内の非同期非必須ポリシーのファイルアクセスイベントをキャプチャする。永続的ストアを使用すると、クライアントI/O処理とFPolicy通知処理を分離して、クライアントのレイテンシを低減できます。同期（必須または必須でない）および非同期の必須構成はサポートされていませ

ん。

## ベストプラクティス

- ・ 永続ストア機能を使用する前に、パートナーアプリケーションがこの構成をサポートしていることを確認してください。
- ・ 永続的ストアボリュームはSVM単位でセットアップします。FPolicyが有効なSVMごとに、永続的ストアボリュームが必要です。
- ・ 永続的ストアのボリューム名とボリューム作成時に指定したジャンクションパスが一致している必要があります。
- ・ FPolicyで最大トラフィック量を監視すると想定されるLIFがあるノードに永続的ストアボリュームを作成します。
- ・ Snapshotポリシーをに設定 `none` 対象のボリュームではなく `default`。これは、Snapshotが誤ってリストアされて現在のイベントが失われることがないようにし、イベント処理が重複しないようにするためです。
- ・ 永続的なイベントレコードが誤って破損したり削除されたりしないように、外部ユーザプロトコルアクセス (CIFS / NFS) で永続的ストアボリュームにアクセスできないようにします。これには、FPolicyを有効にしたあとにONTAPでボリュームをアンマウントしてジャンクションパスを削除すると、ユーザプロトコルアクセスができなくなります。

## 手順

1. 永続ストア用にプロビジョニング可能な空のボリュームをSVMに作成します。

```
volume create -vserver <SVM Name> -volume <volume> -state <online> -junction  
-path <path> -policy <default> -unix-permissions <777> -size <value>  
-aggregate <aggregate name> -snapshot-policy <none>
```

- 永続的ストアボリュームのサイズは、外部サーバ（パートナーアプリケーション）に配信されないイベントを維持する期間に基づいています。

たとえば、1秒あたり30Kの通知があるクラスターで30分間のイベントを維持する場合は、次のコマンドを実行します。

必要なボリュームサイズ =  $30000 \times 30 \times 60 \times 0.6\text{KB}$ （平均通知レコードサイズ） = 32400000 KB  
≈ 32GB

おおよその通知速度を確認するには、FPolicyパートナーアプリケーションに連絡するか、FPolicyカウンタを利用します。 `requests_dispatched_rate`。

- （ボリュームを作成するための）十分なRBAC権限を持つ管理者ユーザが、必要なサイズのボリュームを（volume CLIコマンドまたはREST APIを使用して）作成し、そのボリュームの名前を `-volume` 永続的ストアでは、CLIコマンドまたはREST APIを作成します。

2. 永続ストアを作成します。

```
vserver fpolicy persistent store create -vserver <SVM> -persistent-store  
<PS_name> -volume <volume>
```

- `persistent-store`：永続ストアの名前
- `volume`：永続的ストアボリューム

3. 永続的ストアが作成されたら、FPolicyポリシーを作成し、そのポリシーに永続的ストア名を追加できます。  
詳細については、を参照してください ["FPolicy ポリシーを作成します"](#)。

## FPolicy ポリシーを作成します

FPolicy ポリシーを作成する際には、外部エンジンと 1 つ以上のイベントをこのポリシーに関連付けます。このポリシーでは、必須のスクリーニングが要求されるかどうか、FPolicy サーバに Storage Virtual Machine (SVM) 上のデータへの権限付きアクセスが許可されているかどうか、オフラインファイルのパススルーリードが有効かどうかも指定します。

### 必要なもの

- FPolicy ポリシーワークシートを完成させる必要があります。
- FPolicy サーバを使用するようにポリシーを設定する場合は、外部エンジンが存在している必要があります。
- FPolicy ポリシーに関連付ける FPolicy イベントが少なくとも 1 つは存在している必要があります。
- 権限付きデータアクセスを設定する場合は、SVM上にSMBサーバが存在している必要があります。
- ポリシーの永続ストアを設定するには、エンジンタイプを\* async にし、ポリシーを non-mandatory \*にする必要があります。

詳細については、を参照してください ["永続ストアの作成"](#)。

### 手順

1. FPolicy ポリシーを作成します。

```
vserver fpolicy policy create -vserver-name vserver_name -policy-name  
policy_name -engine engine_name -events event_name, [-persistent-store  
PS_name] [-is-mandatory {true|false}] [-allow-privileged-access {yes|no}] [-  
privileged-user-name domain\user_name] [-is-passthrough-read-enabled  
{true|false}]
```

- FPolicy ポリシーには 1 つ以上のイベントを追加できます。
- デフォルトでは、必須のスクリーニングが有効になっています。
- 権限付きアクセスを許可する場合は、を設定します -allow-privileged-access パラメータの値 `yes` また、特権アクセスの特権ユーザ名を設定する必要があります。
- パススルーリードを設定する場合は、を設定します -is-passthrough-read-enabled パラメータの値 `true` 権限付きデータアクセスも設定する必要があります。

次のコマンドは、"event1" というイベントと、"engine1" という外部エンジンが関連付けられた "policy1 " という名前のポリシーを作成します。このポリシーでは、ポリシー設定にデフォルト値を使用します。

```
`vserver fpolicy policy create -vserver vs1.example.com -policy-name policy1  
-events event1 -engine engine1
```

次のコマンドは、"event2" というイベントと、"engine2" という外部エンジンが関連付けられた "policy2" というポリシーを作成します。このポリシーは、指定されたユーザ名を使用して権限付きア

クセスを使用するように設定されています。パススルーリードが有効になっています。

```
vserver fpolicy policy create -vserver vs1.example.com -policy-name policy2
-events event2 -engine engine2 -allow-privileged-access yes -privileged-
user-name example\archive_acct -is-passthrough-read-enabled true
```

次のコマンドは 'event3' というイベントが関連付けられた 'native1' という名前のポリシーを作成しますこのポリシーでは標準のエンジンを使用し、デフォルト値をポリシー設定に使用しています。

```
vserver fpolicy policy create -vserver vs1.example.com -policy-name native1
-events event3 -engine native
```

2. を使用してFPolicyポリシーの設定を確認します vserver fpolicy policy show コマンドを実行します

次のコマンドは、次の情報を含む、設定された 3 つの FPolicy ポリシーに関する情報を表示します。

- ポリシーに関連付けられている SVM
- ポリシーに関連付けられている外部エンジン
- ポリシーに関連付けられているイベント
- スクリーニングを必須にするかどうか
- 権限付きアクセスが必要かどうか

```
vserver fpolicy policy show
```

Vserver	Policy Name	Events	Engine	Is Mandatory	Privileged Access
-----	-----	-----	-----	-----	
vs1.example.com	policy1	event1	engine1	true	no
vs1.example.com	policy2	event2	engine2	true	yes
vs1.example.com	native1	event3	native	true	no

## FPolicy スコープを作成します

FPolicy ポリシーを作成したら、FPolicy スコープを作成する必要があります。スコープを作成するときに、スコープを FPolicy ポリシーに関連付けます。スコープは、FPolicy ポリシーを適用する範囲を定義します。共有、エクスポートポリシー、ボリューム、およびファイル拡張子に基づいて、対象とするファイルまたは除外するファイルを指定できます。

### 必要なもの

FPolicy スコープワークシートを完成させる必要があります。FPolicy ポリシーには、関連付けられた外部エンジンが存在する必要があります（外部 FPolicy サーバを使用するようにポリシーを設定する場合）、FPolicy イベントを少なくとも 1 つは関連付ける必要があります。

### 手順

1. を使用してFPolicyスコープを作成します `vserver fpolicy policy scope create` コマンドを実行します

```
vserver fpolicy policy scope create -vserver-name vs1.example.com -policy-name policy1 -volumes-to-include datavol1,datavol2
```

2. を使用してFPolicyスコープの設定を確認します `vserver fpolicy policy scope show` コマンドを実行します

```
vserver fpolicy policy scope show -vserver vs1.example.com -instance
```

```
Vserver: vs1.example.com
Policy: policy1
Shares to Include: -
Shares to Exclude: -
Volumes to Include: datavol1, datavol2
Volumes to Exclude: -
Export Policies to Include: -
Export Policies to Exclude: -
File Extensions to Include: -
File Extensions to Exclude: -
```

## FPolicy ポリシーを有効にします

FPolicy ポリシーの設定が完了したら、FPolicy ポリシーを有効にします。ポリシーを有効にすると優先度が設定され、そのポリシーのファイルアクセスの監視が開始されます。

### 必要なもの

FPolicy ポリシーには、関連付けられた外部エンジンが存在する必要があります（外部 FPolicy サーバを使用するようにポリシーを設定する場合）、FPolicy イベントを少なくとも 1 つは関連付ける必要があります。FPolicy ポリシースコープが存在し、FPolicy ポリシーに割り当てられている必要があります。

### このタスクについて

Storage Virtual Machine（SVM）で複数のポリシーを有効にし、複数のポリシーを同じファイルアクセスイベントに登録している場合は、優先度が使用されます。標準のエンジンの設定を使用するポリシーは、ポリシーを有効にするときに割り当てられたシーケンス番号に関係なく、他のエンジンのポリシーよりも優先度が高くなります。



管理 SVM ではポリシーを有効にできません。

### 手順

1. を使用して、FPolicyポリシーを有効にします `vserver fpolicy enable` コマンドを実行します

```
vserver fpolicy enable -vserver-name vs1.example.com -policy-name policy1 -sequence-number 1
```

2. を使用して、FPolicyポリシーが有効になっていることを確認します `vserver fpolicy show` コマンドを実行します

```
vserver fpolicy show -vserver vs1.example.com
```

Vserver	Policy Name	Sequence Number	Status	Engine
vs1.example.com	policy1	1	on	engine1

## FPolicy設定を管理します。

### FPolicy の設定を変更します

FPolicy の設定を変更するためのコマンド

FPolicy の設定を変更するには、設定の各要素を変更します。外部エンジン、FPolicy イベント、FPolicy スコープ、および FPolicy ポリシーを変更できます。FPolicy ポリシーを有効または無効にすることもできます。FPolicy ポリシーを無効にすると、そのポリシーのファイル監視が中止されます。

設定を変更する前に、FPolicy ポリシーを無効にすることを推奨します。

変更する項目	使用するコマンド
外部エンジン	<code>vserver fpolicy policy external-engine modify</code>
イベント	<code>vserver fpolicy policy event modify</code>
スコープ	<code>vserver fpolicy policy scope modify</code>
ポリシー	<code>vserver fpolicy policy modify</code>

詳細については、コマンドのマニュアルページを参照してください。

### FPolicy ポリシーを有効または無効にします

設定の完了後に、FPolicy ポリシーを有効にできます。ポリシーを有効にすると優先度が設定され、そのポリシーのファイルアクセスの監視が開始されます。そのポリシーのファイルアクセスの監視を停止するには、FPolicy ポリシーを無効にします。

#### 必要なもの

FPolicy ポリシーを有効にする前に、FPolicy の設定が完了している必要があります。

このタスクについて

- Storage Virtual Machine（SVM）で複数のポリシーを有効にし、複数のポリシーを同じファイルアクセスイベントに登録している場合は、優先度が使用されます。
- 標準のエンジンの設定を使用するポリシーは、ポリシーを有効にするときに割り当てられたシーケンス番号に関係なく、他のエンジンのポリシーよりも優先度が高くなります。
- FPolicy ポリシーの優先度を変更する場合は、ポリシーを無効にしてから、新しいシーケンス番号を使用して再度有効にする必要があります。

## ステップ

1. 適切な操作を実行します。

状況	入力するコマンド
FPolicy ポリシーを有効にします	<code>vserver fpolicy enable -vserver-name vserver_name -policy-name policy_name -sequence-number integer</code>
FPolicy ポリシーを無効にします	<code>vserver fpolicy disable -vserver-name vserver_name -policy-name policy_name</code>

## FPolicy の設定に関する情報を表示します

### show コマンドの仕組み

FPolicyの設定に関する情報を表示する際には、の仕組みを理解しておくと役立ちます  
show コマンドは機能します。

A show パラメータを追加せずにコマンドを実行すると、情報が要約形式で表示されます。さらに、すべて show コマンドには、同じ2つのオプションパラメータを同時に指定することはできません。-instance および -fields。

を使用する場合 -instance パラメータにを指定します show コマンドを使用すると、詳細情報がリスト形式で表示されます。場合によっては、詳細出力には時間がかかることがあり、不要な情報が含まれることもあります。を使用できます -fields fieldname[,fieldname...] 指定したフィールドの情報のみが表示されるように出力をカスタマイズするためのパラメータ。指定できるフィールドを確認するには、と入力します？の後 -fields パラメータ



の出力 show コマンドにを指定します -fields パラメータには、要求されたフィールドに関連する他の関連フィールドや必要なフィールドが表示される場合があります。

間隔 show コマンドには、その出力をフィルタリングして、コマンド出力に表示される情報の範囲を絞り込むことができる1つ以上のオプションパラメータがあります。コマンドで使用できるオプションパラメータを確認するには、と入力します？の後 show コマンドを実行します

。show コマンドでは、UNIX形式のパターンおよびワイルドカードがサポートされ、コマンドパラメータ引数の複数の値を照合できます。たとえば、ワイルドカード演算子（\*）、NOT 演算子（!）、OR 演算子（|）、範囲演算子（integer...integer）、less-than 演算子（<）、greater-than 演算子（>）、less-than-or-equal-to 演算子（<=）、greater-than-or-equal-to 演算子（>=）を指定する場合に使用できます。

UNIX形式のパターンおよびワイルドカードの使用の詳細については、を参照してください [ONTAP コマンド](#)



ラインインターフェイスを使用する。

**FPolicy** 設定に関する情報を表示するコマンドです

を使用します `fpolicy show` **FPolicy**外部エンジン、イベント、スコープ、およびポリシーに関する情報など、**FPolicy**の設定に関する情報を表示するコマンド。

FPolicy に関する情報の表示	使用するコマンド
外部エンジン	<code>vserver fpolicy policy external-engine show</code>
イベント	<code>vserver fpolicy policy event show</code>
スコープ	<code>vserver fpolicy policy scope show</code>
ポリシー	<code>vserver fpolicy policy show</code>

詳細については、コマンドのマニュアルページを参照してください。

**FPolicy** ポリシーのステータスに関する情報を表示します

**FPolicy** ポリシーのステータスに関する情報を表示して、ポリシーが有効になっているかどうか、使用するよう設定されている外部エンジン、ポリシーのシーケンス番号、および **FPolicy** ポリシーが関連付けられている **Storage Virtual Machine**（**SVM**）を確認できます。

このタスクについて

いずれのパラメータも指定しない場合、次の情報が表示されます。

- **SVM** 名
- ポリシー名
- ポリシーのシーケンス番号
- ポリシーのステータス

クラスタまたは特定の **SVM** で設定されている **FPolicy** ポリシーのステータスに関する情報の表示に加え、コマンドパラメータを使用して、他の条件によってコマンドの出力をフィルタリングすることができます。

を指定できます `-instance` パラメータを指定して、リストしたポリシーに関する詳細情報を表示します。または、を使用することもできます `-fields` パラメータを指定して、コマンド出力に指定されたフィールドのみを表示します。または `-fields ?` 使用できるフィールドを決定します。

ステップ

1. 適切なコマンドを使用して、**FPolicy** ポリシーのステータスに関する情報をフィルタリングして表示します。

ステータス情報を表示するポリシー	入力するコマンド
------------------	----------

クラスタのポリシーを確認してください	vserver fpolicy show
指定したステータスのポリシーを適用します	`vserver fpolicy show -status {on
off}`	指定した SVM のポリシーを適用します
vserver fpolicy show -vserver vserver_name	指定したポリシー名のポリシーを使用します
vserver fpolicy show -policy-name policy_name	指定した外部エンジンを使用するポリシーを定義します

## 例

次の例は、クラスタの FPolicy ポリシーに関する情報を表示します。

```
cluster1::> vserver fpolicy show
```

Vserver	Policy Name	Sequence Number	Status	Engine
-----	-----	-----	-----	-----
FPolicy	cserver_policy	-	off	eng1
vs1.example.com	v1p1	-	off	eng2
vs1.example.com	v1p2	-	off	native
vs1.example.com	v1p3	-	off	native
vs1.example.com	cserver_policy	-	off	eng1
vs2.example.com	v1p1	3	on	native
vs2.example.com	v1p2	1	on	eng3
vs2.example.com	cserver_policy	2	on	eng1

有効な **FPolicy** ポリシーに関する情報を表示します

有効な FPolicy ポリシーに関する情報を表示して、使用するよう設定されている外部エンジン、ポリシーの優先順位、および FPolicy ポリシーが関連付けられている Storage Virtual Machine （ SVM ）を確認できます。

このタスクについて

いずれのパラメータも指定しない場合、次の情報が表示されます。

- SVM 名
- ポリシー名
- ポリシーの優先度

コマンドパラメータを使用すると、指定した条件によってコマンドの出力をフィルタリングできます。

ステップ

- 適切なコマンドを使用して、有効な FPolicy ポリシーに関する情報を表示します。

情報を表示する有効なポリシー	入力するコマンド
クラスタのポリシーを確認してください	<code>vserver fpolicy show-enabled</code>
指定した SVM のポリシーを適用します	<code>vserver fpolicy show-enabled -vserver vs1.example.com</code>
指定したポリシー名のポリシーを使用します	<code>vserver fpolicy show-enabled -policy-name policy_name</code>
指定したシーケンス番号のもの	<code>vserver fpolicy show-enabled -priority integer</code>

例

次の例は、クラスタの有効な FPolicy ポリシーに関する情報を表示します。

```
cluster1::> vserver fpolicy show-enabled
Vserver                Policy Name                Priority
-----
vs1.example.com        pol_native                  native
vs1.example.com        pol_native2                 native
vs1.example.com        pol1                        2
vs1.example.com        pol2                        4
```

FPolicy サーバの接続を管理します

外部 FPolicy サーバに接続します

接続がすでに終了している場合、ファイル処理を有効にするために外部 FPolicy サーバへの手動での接続が必要になることがあります。接続は、サーバのタイムアウトに達した場合、または何らかのエラーが原因で終了します。または、管理者が接続を手動で終了することもできます。

このタスクについて

致命的なエラーが発生した場合、FPolicy サーバへの接続が終了することがあります。致命的なエラーの原因となった問題を解決したあと、FPolicy サーバに手動で再接続する必要があります。

手順

- を使用して外部FPolicyサーバに接続します `vserver fpolicy engine-connect` コマンドを実行しま

す

コマンドの詳細については、マニュアルページを参照してください。

2. を使用して、外部FPolicyサーバが接続されていることを確認します `vserver fpolicy show-engine` コマンドを実行します

コマンドの詳細については、マニュアルページを参照してください。

外部 **FPolicy** サーバを切断します

外部 FPolicy サーバからの手動での切断が必要になることがあります。これは、FPolicy サーバで通知要求の処理に関する問題が発生した場合や、FPolicy サーバでメンテナンスを実施する必要がある場合に役立つことがあります。

手順

1. を使用して外部FPolicyサーバから切断します `vserver fpolicy engine-disconnect` コマンドを実行します

コマンドの詳細については、マニュアルページを参照してください。

2. を使用して、外部FPolicyサーバから切断されたことを確認します `vserver fpolicy show-engine` コマンドを実行します

コマンドの詳細については、マニュアルページを参照してください。

外部 **FPolicy** サーバへの接続に関する情報を表示します

クラスタまたは指定した Storage Virtual Machine (SVM) の外部 FPolicy サーバ (FPolicy サーバ) への接続に関するステータス情報を表示できます。この情報は、接続されている FPolicy サーバを確認するのに役立ちます。

このタスクについて

いずれのパラメータも指定しない場合、次の情報が表示されます。

- SVM 名
- ノード名
- FPolicy ポリシー名
- FPolicy サーバの IP アドレス
- FPolicy サーバのステータス
- FPolicy サーバのタイプ

クラスタまたは特定の SVM の FPolicy 接続に関する情報の表示に加え、コマンドパラメータを使用して、他の条件によってコマンドの出力をフィルタリングすることができます。

を指定できます `-instance` パラメータを指定して、リストしたポリシーに関する詳細情報を表示します。または、を使用することもできます `-fields` パラメータを指定して、コマンド出力の指定されたフィールドの

みを表示します。入ることができます？の後 -fields パラメータを使用して、使用できるフィールドを確認します。

ステップ

- 適切なコマンドを使用して、ノードと FPolicy サーバの間の接続ステータスに関する情報をフィルタリングして表示します。

接続ステータス情報を表示する FPolicy サーバ	入力するコマンド
を指定します	<code>vserver fpolicy show-engine -server IP_address</code>
指定した SVM のものです	<code>vserver fpolicy show-engine -vserver vserver_name</code>
指定したポリシーに関連付けられているもの	<code>vserver fpolicy show-engine -policy-name policy_name</code>
指定したサーバステータスを使用します	<code>vserver fpolicy show-engine -server-status status</code>  サーバのステータスは、次のいずれかになります。 <ul style="list-style-type: none"><li>• connected</li><li>• disconnected</li><li>• connecting</li><li>• disconnecting</li></ul>
を指定します	<code>vserver fpolicy show-engine -server-type type</code>  FPolicy サーバのタイプとしては、次のいずれかを指定できます。 <ul style="list-style-type: none"><li>• primary</li><li>• secondary</li></ul>

指定した理由で切断されたもの	<pre>vserver fpolicy show-engine -disconnect-reason text</pre> <p>切断の理由はさまざまです。切断の一般的な理由は次のとおりです。</p> <ul style="list-style-type: none"> <li>• Disconnect command received from CLI.</li> <li>• Error encountered while parsing notification response from FPolicy server.</li> <li>• FPolicy Handshake failed.</li> <li>• SSL handshake failed.</li> <li>• TCP Connection to FPolicy server failed.</li> <li>• The screen response message received from the FPolicy server is not valid.</li> </ul>
----------------	---

## 例

次の例は、SVM vs1.example.com 上の FPolicy サーバへの外部エンジン接続に関する情報を表示したものです。

```
cluster1::> vserver fpolicy show-engine -vserver vs1.example.com
FPolicy
Vserver          Policy      Node        Server      Server-
-----
vs1.example.com policy1    node1       10.1.1.2    connected   primary
vs1.example.com policy1    node1       10.1.1.3    disconnected  primary
vs1.example.com policy1    node2       10.1.1.2    connected   primary
vs1.example.com policy1    node2       10.1.1.3    disconnected  primary
```

この例は、接続されている FPolicy サーバに関する情報のみを表示したものです。

```
cluster1::> vserver fpolicy show-engine -fields server -server-status
connected
node      vserver      policy-name  server
-----
node1     vs1.example.com policy1      10.1.1.2
node2     vs1.example.com policy1      10.1.1.2
```

**FPolicy** パススルーリード接続のステータスに関する情報を表示します

クラスタまたは指定した Storage Virtual Machine （SVM）の外部 FPolicy サーバ（ FPolicy サーバ） への FPolicy パススルーリード接続のステータスに関する情報を表示で

きます。この情報は、パススルーリードデータ接続を持つ FPolicy サーバや、パススルーリード接続が切断されている FPolicy サーバを確認するのに役立ちます。

このタスクについて

いずれのパラメータも指定しない場合、次の情報が表示されます。

- SVM 名
- FPolicy ポリシー名
- ノード名
- FPolicy サーバの IP アドレス
- FPolicy パススルーリード接続のステータス

クラスタまたは特定の SVM の FPolicy 接続に関する情報の表示に加え、コマンドパラメータを使用して、他の条件によってコマンドの出力をフィルタリングすることができます。

を指定できます `-instance` パラメータを指定して、リストしたポリシーに関する詳細情報を表示します。または、を使用することもできます `-fields` パラメータを指定して、コマンド出力の指定されたフィールドのみを表示します。入ることができます？の後 `-fields` パラメータを使用して、使用できるフィールドを確認します。

ステップ

1. 適切なコマンドを使用して、ノードと FPolicy サーバの間の接続ステータスに関する情報をフィルタリングして表示します。

表示する接続ステータス情報	入力するコマンド
クラスタの FPolicy パススルーリード接続のステータス	<code>vserver fpolicy show-passthrough-read-connection</code>
指定した SVM の FPolicy パススルーリード接続ステータス	<code>vserver fpolicy show-passthrough-read-connection -vserver vserver_name</code>
指定したポリシーの FPolicy パススルーリード接続ステータス	<code>vserver fpolicy show-passthrough-read-connection -policy-name policy_name</code>
指定したポリシーの詳細な FPolicy パススルーリード接続ステータス	<code>vserver fpolicy show-passthrough-read-connection -policy-name policy_name -instance</code>
指定したステータスの FPolicy パススルーリード接続ステータス	<code>vserver fpolicy show-passthrough-read-connection -policy-name policy_name -server-status status</code> サーバのステータスは、次のいずれかになります。 <ul style="list-style-type: none"><li>• <code>connected</code></li><li>• <code>disconnected</code></li></ul>

例

次のコマンドは、クラスタ上のすべての FPolicy サーバからのパススルーリード接続に関する情報を表示します。

```
cluster1::> vservers fpolicy show-passthrough-read-connection
```

Vserver	Policy Name	Node	FPolicy Server	Server Status
vs2.example.com	pol_cifs_2	FPolicy-01	2.2.2.2	disconnected
vs1.example.com	pol_cifs_1	FPolicy-01	1.1.1.1	connected

次のコマンドは、「pol\_cifs\_1」ポリシーに設定されている FPolicy サーバからのパススルーリード接続に関する詳細情報を表示します。

```
cluster1::> vservers fpolicy show-passthrough-read-connection -policy-name pol_cifs_1 -instance
```

Node: FPolicy-01  
Vserver: vs1.example.com  
Policy: pol\_cifs\_1  
Server: 1.1.1.1  
Session ID of the Control Channel: 8cef052e-2502-11e3-88d4-123478563412  
Server Status: connected  
Time Passthrough Read Channel was Connected: 9/24/2013 10:17:45  
Time Passthrough Read Channel was Disconnected: -  
Reason for Passthrough Read Channel Disconnection: none

## セキュリティトレースを使用したアクセスの確認

### セキュリティトレースの仕組み

パーミッショントレーシングフィルタを追加すると、Storage Virtual Machine（SVM）の SMB サーバおよび NFS サーバに対するクライアントまたはユーザによる処理要求が許可または拒否された理由が ONTAP で記録されるようになります。これは、ファイルアクセスのセキュリティ形式が適切であることを確認する場合や、ファイルアクセスに関する問題のトラブルシューティングを行う場合に役立ちます。

セキュリティトレースを使用すると、SVM 上での SMB および NFS 経由のクライアント処理を検出するフィルタを設定して、フィルタに一致するすべてのアクセスチェックをトレースできます。トレース結果には、アクセスが許可または拒否された理由がわかりやすくまとめられています。

SVM のファイルやフォルダに対する SMB / NFS アクセスのセキュリティ設定を確認する場合や、アクセスに関する問題がある場合は、パーミッショントレーシングを有効にするフィルタを短時間で追加できます。



次のリストに、セキュリティトレースの仕組みに関する重要な特性を示します。

- ONTAP は、セキュリティトレースを SVM レベルで適用します。
- 各受信要求がスクリーニングされ、有効になっているセキュリティトレースのフィルタ条件に一致するかどうかを確認されます。
- トレースは、ファイルとフォルダの両方のアクセス要求に対して実行されます。
- トレースでは、次の条件に基づいてフィルタリングできます。
  - クライアントIP
  - SMB または NFS パス
  - Windows 名
  - UNIX 名
- 要求は、\_allowed\_or\_Denied\_access 応答結果でスクリーニングされます。
- 有効なトレースのフィルタ条件に一致する各要求が、トレース結果ログに記録されます。
- ストレージ管理者は、フィルタが自動的に無効になるようにタイムアウトを設定できます。
- 要求が複数のフィルタに一致する場合は、インデックス番号が最も大きいフィルタの結果が記録されます。
- ストレージ管理者は、トレース結果ログを出力し、アクセス要求が許可または拒否された理由を確認できます。

アクセスのタイプによって、セキュリティトレースモニタがチェックされます

ファイルやフォルダに対するアクセスチェックは、複数の条件に基づいて行われます。これらすべての基準について、セキュリティトレースで操作を監視できます。

セキュリティトレースで監視されるアクセスチェックの種類は次のとおりです。

- ボリュームと qtree のセキュリティ形式
- 処理が要求されるファイルやフォルダを含むファイルシステムの効果的なセキュリティ
- ユーザマッピング
- 共有レベルの権限
- エクスポートレベルの権限
- ファイルレベルの権限
- ストレージレベルのアクセス保護セキュリティ

セキュリティトレースを作成する際の考慮事項

Storage Virtual Machine (SVM) でセキュリティトレースを作成する場合は、以下の考慮事項に注意する必要があります。たとえば、トレースを作成できるプロトコル、サポートされるセキュリティ形式、アクティブなトレースの最大数を把握しておく必要があります。

- セキュリティトレースは SVM 上でしか作成できません。
- セキュリティトレースフィルタの各エントリは SVM 固有です。

トレースを実行する SVM を指定する必要があります。

- パーミッショントレーシングフィルタは SMB 要求と NFS 要求についてのみ追加できます。
- トレースフィルタを作成するSVM上にSMBサーバまたはNFSサーバをセットアップする必要があります。
- NTFS、UNIX、mixed セキュリティ形式のボリュームおよび qtree 上に存在するファイルやフォルダに対してセキュリティトレースを作成できます。
- パーミッショントレーシングフィルタは SVM ごとに 10 個まで追加できます。
- フィルタを作成または変更するときは、フィルタインデックス番号を指定する必要があります。

フィルタはインデックス番号順に処理されます。インデックス番号の大きいフィルタの条件は、インデックス番号の小さい条件よりも先に処理されます。トレースされている要求が、複数の有効なフィルタの条件に一致する場合は、インデックス番号が最も大きいフィルタだけがトリガーされます。

- セキュリティトレースフィルタを作成して有効にしたあと、トレースフィルタでキャプチャしてトレース結果ログに記録できるアクティビティを生成するために、クライアントシステムでファイル要求またはフォルダ要求をいくつか実行する必要があります。
- ファイルアクセスの検証またはトラブルシューティングの目的でのみ、パーミッショントレーシングフィルタを追加してください。

パーミッショントレーシングフィルタを追加すると、コントローラのパフォーマンスが若干低下します。

検証またはトラブルシューティングが完了したら、すべてのパーミッショントレーシングフィルタを無効にするか、削除する必要があります。さらに ONTAP、ログに大量のトレース結果が送信されないように、できるだけ具体的なフィルタ条件を指定する必要があります。

## セキュリティトレースを実行します

### セキュリティトレースの概要を実行します

セキュリティトレースの実行では、セキュリティトレースフィルタの作成、フィルタ条件の確認、フィルタ条件に一致する SMB クライアントまたは NFS クライアントへのアクセス要求の生成、トレース結果の表示などを行います。

セキュリティフィルタを使用してトレース情報をキャプチャしたあと、フィルタを変更して再利用するか、不要になった場合は無効にすることができます。フィルタトレース結果を表示および分析したあと、その結果が不要になった場合は削除できます。

### セキュリティトレースフィルタを作成します


Storage Virtual Machine（SVM）で SMB および NFS のクライアント処理を検出し、フィルタに一致するすべてのアクセスチェックをトレースするセキュリティトレースフィルタを作成できます。セキュリティトレースの結果を使用して、構成の検証や、アクセスに関する問題のトラブルシューティングを行うことができます。

## このタスクについて

vserver security trace filter create コマンドには 2 つの必須パラメータがあります。

必須パラメータ	説明
-vserver vserver_name	SVM 名 _  セキュリティトレースフィルタを適用するファイルやフォルダが格納されている SVM の名前。
-index index_number	フィルタインデックス番号 _  フィルタに適用するインデックス番号。トレースフィルタは SVM ごとに 10 個まで使用できます。このパラメータに指定できる値は 1~10 です。

さまざまなオプションのフィルタパラメータでセキュリティトレースフィルタをカスタマイズして、セキュリティトレースによって生成された結果を絞り込むことができます。

フィルタパラメータ	説明
-client-ip IP_Address	IP アドレスを指定します。この IP アドレスから SVM にアクセスしているユーザが対象となります。
-path path	パーミッショントレースフィルタを適用するパスを指定します。の値 -path 次のいずれかの形式を使用できます。 <ul style="list-style-type: none"><li>共有またはエクスポートのルートから始まる完全なパス</li><li>共有のルートに対する相対パス</li></ul> パス値では、NFS 形式のディレクトリ UNIX 形式のディレクトリ区切り文字を使用する必要があります。
-windows-name win_user_name または -unix -name ``unix_user_name	アクセス要求をトレースする対象の Windows ユーザ名または UNIX ユーザ名を指定できます。ユーザ名変数では大文字と小文字は区別されません。同じフィルタで Windows ユーザ名と UNIX ユーザ名の両方を指定することはできません。 <div> トレースできるのは SMB と NFS のアクセスイベントですが、mixed セキュリティ形式または UNIX セキュリティ形式のデータに対してアクセスチェックを実行するときに、マッピングされた UNIX ユーザおよび UNIX グループが使用されることがあります。</div>
-trace-allow {yes	no}

セキュリティトレースフィルタでは、拒否イベントのトレースは常に有効です。必要に応じて、許可イベントをトレースすることもできます。許可イベントをトレースするには、このパラメータをに設定します yes。	-enabled {enabled
disabled}	セキュリティトレースフィルタを有効または無効にすることができます。デフォルトでは、セキュリティトレースフィルタは有効になっています。
-time-enabled integer	フィルタのタイムアウトを指定できます。指定した時間が経過すると、フィルタは無効になります。

手順

1. セキュリティトレースフィルタを作成します。

```
vserver security trace filter create -vserver vserver_name -index
index_numberfilter_parameters
```

filter\_parameters は、オプションのフィルタパラメータのリストです。

詳細については、コマンドのマニュアルページを参照してください。

2. セキュリティトレースフィルタのエントリを確認します。

```
vserver security trace filter show -vserver vserver_name -index index_number
```

例

次のコマンドは、共有パスのファイルにアクセスするすべてのユーザを対象とするセキュリティトレースフィルタを作成します \\server\share1\dir1\dir2\file.txt IPアドレス10.10.10.7から。フィルタはに完全なパスを使用します -path オプションデータへのアクセスに使用されるクライアントの IP アドレスは 10.10.10.7 です。フィルタは 30 分後にタイムアウトします。

```
cluster1::> vserver security trace filter create -vserver vs1 -index 1
-path /dir1/dir2/file.txt -time-enabled 30 -client-ip 10.10.10.7
cluster1::> vserver security trace filter show -index 1
Vserver  Index    Client-IP          Path                Trace-Allow
Windows-Name
-----  -
vs1      1      10.10.10.7      /dir1/dir2/file.txt      no      -
```

次のコマンドは、の相対パスを使用してセキュリティトレースフィルタを作成します -path オプションこのフィルタは、「joe」という名前の Windows ユーザのアクセスをトレースします。Joeは共有パスのファイルにアクセスしています \\server\share1\dir1\dir2\file.txt。許可イベントと拒否イベントをトレ

ースします。

```
cluster1::> vsserver security trace filter create -vsserver vs1 -index 2
-path /dir1/dir2/file.txt -trace-allow yes -windows-name mydomain\joe

cluster1::> vsserver security trace filter show -vsserver vs1 -index 2
      Vserver: vs1
      Filter Index: 2
      Client IP Address to Match: -
      Path: /dir1/dir2/file.txt
      Windows User Name: mydomain\joe
      UNIX User Name: -
      Trace Allow Events: yes
      Filter Enabled: enabled
      Minutes Filter is Enabled: 60
```

セキュリティトレースフィルタに関する情報を表示します

Storage Virtual Machine（SVM）で設定されているセキュリティトレースフィルタに関する情報を表示できます。これにより、各フィルタがトレースするアクセスイベントのタイプを確認できます。

#### ステップ

1. を使用して、セキュリティトレースフィルタエントリに関する情報を表示します vsserver security trace filter show コマンドを実行します

このコマンドの使用の詳細については、マニュアルページを参照してください。

#### 例

次のコマンドを実行すると、SVM vs1 のすべてのセキュリティトレースフィルタに関する情報が表示されます。

```
cluster1::> vsserver security trace filter show -vsserver vs1
Vserver  Index  Client-IP          Path                Trace-Allow
Windows-Name
-----
vs1      1      -                /dir1/dir2/file.txt    yes      -
vs1      2      -                /dir3/dir4/            no
mydomain\joe
```

セキュリティトレースの結果を表示します

セキュリティトレースフィルタに一致するファイル操作に対して生成されたセキュリテ

イトレースの結果を表示できます。この結果を使用して、ファイルアクセスセキュリティ設定の検証や、SMB および NFS のファイルアクセスに関する問題のトラブルシューティングを行うことができます。

#### 必要なもの

有効なセキュリティトレースフィルタが存在している必要があり、セキュリティトレースの結果が生成されるように、セキュリティトレースフィルタに一致する SMB クライアントまたは NFS クライアントから操作が実行されている必要があります。

#### このタスクについて

すべてのセキュリティトレースの結果の概要を表示することも、オプションのパラメータを指定して、出力に表示される情報をカスタマイズすることもできます。これは、多数のレコードがセキュリティトレースの結果に含まれている場合に便利です。

オプションのパラメータを何も指定しない場合、次の情報が表示されます。

- Storage Virtual Machine （SVM）名
- ノード名
- セキュリティトレースのインデックス番号
- セキュリティ形式
- パス
- 理由
- ユーザ名

トレースフィルタの設定に応じて、ユーザ名が表示されます。

フィルタの設定方法	作業
UNIX ユーザ名を使用する場合	UNIX ユーザ名が表示されます。
Windows ユーザ名を使用	Windows ユーザ名が表示されます。
ユーザ名を使用しない	Windows ユーザ名が表示されます。

オプションのパラメータを使用して、出力をカスタマイズできます。コマンド出力で返される結果を絞り込むために使用できるオプションのパラメータには、次のようなものがあります。

オプションのパラメータ	説明
<code>-fields 'field_name'</code> はい。	選択したフィールドの出力を表示します。このパラメータは、単独で使用することも、他のオプションのパラメータと組み合わせて使用することもできます。

-instance	セキュリティトレースイベントに関する詳細情報を表示します。このパラメータを他のオプションのパラメータとともに使用して、特定のフィルタ結果に関する詳細情報を表示します。
-node node_name	指定したノード上のイベントに関する情報のみを表示します。
-vserver vservice_name	指定した SVM 上のイベントに関する情報のみを表示します。
-index integer	指定したインデックス番号に対応するフィルタの結果として発生したイベントに関する情報を表示します。
-client-ip IP_address	指定したクライアント IP アドレスからのファイルアクセスの結果として発生したイベントに関する情報を表示します。
-path path	指定したパスへのファイルアクセスの結果として発生したイベントに関する情報を表示します。
-user-name user_name	指定した Windows ユーザまたは UNIX ユーザによるファイルアクセスの結果として発生したイベントに関する情報を表示します。
-security-style security_style	指定したセキュリティ形式のファイルシステムで発生したイベントに関する情報を表示します。

コマンドで使用できる他のオプションのパラメータについては、マニュアルページを参照してください。

## ステップ

1. を使用して、セキュリティトレースフィルタの結果を表示します `vserver security trace trace-result show` コマンドを実行します

```
vserver security trace trace-result show -user-name domain\user
```

```
Vserver: vs1
```

Node	Index	Filter Details	Reason
node1	3	User:domain\user Security Style:mixed Path:/dir1/dir2/	Access denied by explicit ACE
node1	5	User:domain\user Security Style:unix Path:/dir1/	Access denied by explicit ACE

## セキュリティトレースフィルタを変更する

トレースされたアクセスイベントを特定する際に使用するオプションのフィルタパラメータを変更するには、既存のセキュリティトレースフィルタを変更します。

### このタスクについて

変更するセキュリティトレースフィルタを特定するには、フィルタを適用した Storage Virtual Machine (SVM) の名前とフィルタのインデックス番号を指定します。オプションのフィルタパラメータはすべて変更できます。

### 手順

1. セキュリティトレースフィルタを変更します。

```
vserver security trace filter modify -vserver vserver_name -index  
index_numberfilter_parameters
```

- ° `vserver_name` は、セキュリティトレースフィルタを適用するSVMの名前です。
- ° `index_number` は、フィルタに適用するインデックス番号です。このパラメータに指定できる値は 1~10 です。
- ° `filter_parameters` は、オプションのフィルタパラメータのリストです。

2. セキュリティトレースフィルタのエントリを確認します。

```
vserver security trace filter show -vserver vserver_name -index index_number
```

### 例

次の例は、インデックス番号 1 のセキュリティトレースフィルタを変更します。このフィルタは、共有パスのファイルにアクセスしているすべてのユーザのイベントをトレースします

\\server\share1\dir1\dir2\file.txt 任意のIPアドレスから。フィルタはに完全なパスを使用します  
-path オプション許可イベントと拒否イベントをトレースします。

```
cluster1::> vserver security trace filter modify -vserver vs1 -index 1  
-path /dir1/dir2/file.txt -trace-allow yes
```

```
cluster1::> vserver security trace filter show -vserver vs1 -index 1  
Vserver: vs1  
Filter Index: 1  
Client IP Address to Match: -  
Path: /dir1/dir2/file.txt  
Windows User Name: -  
UNIX User Name: -  
Trace Allow Events: yes  
Filter Enabled: enabled  
Minutes Filter is Enabled: 60
```



セキュリティトレースフィルタを削除します

セキュリティトレースフィルタエントリが不要になった場合は削除できます。セキュリティトレースフィルタは Storage Virtual Machine（SVM）ごとに 10 個までしか使用できないので、上限に達した場合は、不要なフィルタを削除すると、新しいフィルタを作成できます。

このタスクについて

削除するセキュリティトレースフィルタを一意に識別するには、次の項目を指定する必要があります。

- トレースフィルタが適用されている SVM の名前
- トレースフィルタのフィルタインデックス番号

手順

1. 削除するセキュリティトレースフィルタエントリのフィルタインデックス番号を確認します。

```
vserver security trace filter show -vserver vserver_name
```

```
vserver security trace filter show -vserver vs1
```

Vserver	Index	Client-IP	Path	Trace-Allow
Windows-Name				
-----	-----	-----	-----	-----
vs1	1	-	/dir1/dir2/file.txt	yes
vs1	2	-	/dir3/dir4/	no
mydomain\joe				

2. 前の手順で確認したフィルタインデックス番号を使用して、フィルタエントリを削除します。

```
vserver security trace filter delete -vserver vserver_name -index index_number
```

```
vserver security trace filter delete -vserver vs1 -index 1
```

3. セキュリティトレースフィルタエントリが削除されたことを確認します。

```
vserver security trace filter show -vserver vserver_name
```

```
vserver security trace filter show -vserver vs1
```

Vserver	Index	Client-IP	Path	Trace-Allow
Windows-Name				
-----	-----	-----	-----	-----
vs1	2	-	/dir3/dir4/	no
mydomain\joe				

セキュリティトレースレコードを削除します

セキュリティトレースレコードを使用したファイルアクセスセキュリティの検証や、SMB または NFS のクライアントアクセスに関する問題のトラブルシューティングが完了したら、セキュリティトレースのログからセキュリティトレースレコードを削除できます。

このタスクについて

セキュリティトレースレコードを削除する前に、レコードのシーケンス番号を確認しておく必要があります。



各 Storage Virtual Machine (SVM) には、最大 128 件のトレースレコードを保存できます。SVM でこの上限に達した場合、最も古いトレースレコードが自動的に削除されて、新しいレコードが追加されます。したがって、SVM のトレースレコードを手動で削除しなくても、上限に達したときに、ONTAP によって自動的に最も古いトレース結果を削除して新しい結果用のスペースを確保することができます。

手順

1. 削除するレコードのシーケンス番号を指定します。

```
vserver security trace trace-result show -vserver vserver_name -instance
```

2. セキュリティトレースレコードを削除します。

```
vserver security trace trace-result delete -node node_name -vserver  
vserver_name -seqnum integer
```

```
vserver security trace trace-result delete -vserver vs1 -node node1 -seqnum  
999
```

- ° -node node\_name は、削除するパーミッショントレーシングイベントが発生したクラスタノードの名前です。

これは必須パラメータです。

- ° -vserver vserver\_name は、削除対象のパーミッショントレーシングイベントが発生したSVMの名前です。

これは必須パラメータです。

- ° -seqnum integer は、削除するログイベントのシーケンス番号です。

これは必須パラメータです。

すべてのセキュリティトレースレコードを削除します

既存のセキュリティトレースレコードが不要である場合は、1つのコマンドで特定のノード上のレコードをすべて削除できます。

ステップ

## 1. すべてのセキュリティトレースレコードを削除します。

```
vserver security trace trace-result delete -node node_name -vserver  
vserver_name *
```

- ° -node node\_name は、削除するパーミッショントレーシングイベントが発生したクラスタノードの名前です。
- ° -vserver vserver\_name は、削除するパーミッショントレーシングイベントが発生したStorage Virtual Machine (SVM) の名前です。

## セキュリティトレースの結果を解釈する

セキュリティトレースの結果には、要求が許可または拒否された理由が示されます。出力には、アクセスが許可または拒否された理由と、アクセスが許可または拒否されたアクセスチェック経路内の場所を組み合わせた結果が表示されます。この結果を使用して、アクションが許可された理由または許可されなかった理由を特定できます。

### 結果タイプとフィルタの詳細のリストに関する情報を検索する

セキュリティトレースの結果に表示できる結果タイプとフィルタの詳細のリストは、のマニュアルページで確認できます vserver security trace trace-result show コマンドを実行します

の出力例を示します Reason のフィールド Allow 結果タイプ

次に、の出力例を示します Reason のトレース結果ログに表示されるフィールド Allow 結果タイプ：

```
Access is allowed because SMB implicit permission grants requested  
access while opening existing file or directory.
```

```
Access is allowed because NFS implicit permission grants requested  
access while opening existing file or directory.
```

の出力例を示します Reason のフィールド Allow 結果タイプ

次に、の出力例を示します Reason のトレース結果ログに表示されるフィールド Deny 結果タイプ：

```
Access is denied. The requested permissions are not granted by the  
ACE while checking for child-delete access on the parent.
```

の出力例を示します Filter details フィールド

次に、の出力例を示します Filter details トレース結果ログのフィールド。フィルタ条件に一致するファイルやフォルダが格納されているファイルシステムの有効なセキュリティ形式が表示されます。

```
Security Style: MIXED and ACL
```

## 追加情報の参照先

SMBクライアントアクセスをテストしたあと、SMBの高度な設定を行ったり、SANアクセスを追加したりできます。NFS クライアントアクセスをテストしたあと、NFS の高度な設定を行ったり、SAN アクセスを追加したりできます。プロトコルアクセスが完了したら、SVM のルートボリュームを保護する必要があります。

### SMBの設定

SMBアクセスについてさらに詳しく設定するには、次のコマンドを使用します。

- ["SMBの管理"](#)

SMBプロトコルを使用したファイルアクセスを設定および管理する方法について説明します。

- ["ネットアップテクニカルレポート 4191 : 『 Best Practices Guide for clustered Data ONTAP 8.2 Windows File Services 』 "](#)

SMB の導入やその他の Windows ファイルサービスの機能の概要に加え、ONTAP に関する推奨事項や基本的なトラブルシューティング情報を紹介しています。

- ["ネットアップテクニカルレポート 3740 : 『 SMB 2 Next-Generation CIFS Protocol in Data ONTAP 』 "](#)

SMB 2 の機能について、設定に関する詳細や ONTAP での実装に関する情報を紹介しています。

### NFS構成

NFS アクセスについてさらに詳しく設定するには、以下を使用します。

- ["NFS の管理"](#)

NFS プロトコルを使用したファイルアクセスを設定および管理する方法について説明しています。

- ["ネットアップテクニカルレポート 4067 : 『 NFS Best Practice and Implementation Guide 』 "](#)

NFSv3 および NFSv4 の運用ガイドであり、NFSv4 を中心に ONTAP オペレーティングシステムの概要を説明しています。

- ["ネットアップテクニカルレポート 4668 : 『 Name Services Best Practices Guide 』 "](#)

LDAP、NIS、DNS、およびローカルユーザ / グループファイルを認証用に設定する際の、ベストプラクティス、制限、推奨事項、および考慮事項をまとめています。

- ["ネットアップテクニカルレポート 4616 : 『 NFS Kerberos in ONTAP with Microsoft Active Directory 』 "](#)

- ["ネットアップテクニカルレポート 4835 : 『 How to Configure LDAP in ONTAP 』 "](#)

- ["ネットアップテクニカルレポート 3580 : 『 NFSv4 の拡張内容とベスト・プラクティス・ガイド - Data ONTAP での実装』 "](#)

ONTAP を実行するシステムに接続された AIX、Linux、または Solaris クライアントに NFSv4 のコンポーネントを実装する際のベストプラクティスを紹介しています。

## ルートボリュームの保護

SVM でプロトコルを設定したら、ルートボリュームを保護してください。

- ["データ保護"](#)

負荷共有ミラーを作成して SVM ルートボリュームを保護する方法について説明しています。これは、NAS 対応の SVM に対するネットアップのベストプラクティスです。また、SVM ルートボリュームを負荷共有ミラーから昇格させてボリュームの障害や消失からリカバリする簡単な方法についても説明しています。

## System Manager を使用して暗号化を管理します



### ソフトウェアベースの暗号化を使用して格納データを暗号化

ボリューム暗号化を使用して、基盤となるデバイスの転用、返却、置き忘れ、盗難に際してボリュームのデータが読み取られないようにします。ボリューム暗号化は特殊なディスクを必要としません。HDD および SSD でのみ使用できます。

ボリューム暗号化にはキー管理ツールが必要です。System Manager を使用してオンボードキーマネージャを設定できます。外部キー管理ツールも使用できますが、最初に ONTAP CLI を使用して設定する必要があります。

キー管理ツールを設定すると、新しいボリュームはデフォルトで暗号化されます。

#### 手順

1. **[Cluster] > [Settings]** の順にクリックします。
2. **[Encryption]**( 暗号化 ) で、をクリックします  オンボードキーマネージャを初めて設定する場合。
3. 既存のボリュームを暗号化するには、**\* Storage > Volumes (ボリューム) \*** をクリックします。
4. 目的のボリュームで、をクリックします  次に、**\* Edit \*** をクリックします。
5. **[ 暗号化を有効にする ]** を選択します。


### 自己暗号化ドライブを使用して格納データを暗号化


ディスク暗号化を使用して、基盤となるデバイスの転用、返却、置き忘れ、盗難に際してローカル階層のすべてのデータが読み取られないようにします。ディスク暗号化には、特別な自己暗号化 HDD または SSD が必要です。

ディスク暗号化にはキー管理ツールが必要です。オンボードキーマネージャは System Manager を使用して設定できます。外部キー管理ツールも使用できますが、最初に ONTAP CLI を使用して設定する必要があります。

ONTAP で自己暗号化ディスクが検出された場合は、ローカル階層の作成時にオンボードキーマネージャを設定するよう求めるプロンプトが表示されます。

#### 手順

1. **[Encryption]**( 暗号化 ) で、をクリックします  オンボードキーマネージャを設定します。

2. ディスクのキー変更が必要であることを示すメッセージが表示されたら、をクリックします  をクリックし、 \* Rekey Disks \* をクリックします。

## CLI を使用して暗号化を管理します

### NetApp暗号化の概要

NetApp は、ストレージメディアの転用、返却、置き忘れ、盗難に際して保存データが読み取られないようにソフトウェアベースとハードウェアベースの暗号化テクノロジーを提供します。

- NetApp Volume Encryption (NVE) を使用したソフトウェアベースの暗号化では、一度に1つのボリュームのデータ暗号化がサポートされます
- NetApp Storage Encryption (NSE) を使用したハードウェアベースの暗号化では、データ書き込み時の Full Disk Encryption (FDE；フルディスク暗号化) がサポートされます。

### NetApp Volume Encryption を設定する

#### NetApp Volume Encryption の設定の概要

NetApp Volume Encryption (NVE) は、一度に 1 ボリュームずつ保管データを暗号化するためのソフトウェアベースのテクノロジーです。暗号化キーにはストレージシステムからしかアクセスできないため、基盤のデバイスの転用、返却、置き忘れ、盗難に際してボリュームのデータが読み取られることはありません。

#### NVE の概要

NVEでは、メタデータとデータ (Snapshotコピーを含む) の両方が暗号化されます。データへのアクセスには、ボリュームごとに 1 つずつ、一意の XTS-AES-256 キーを使用します。外部キー管理サーバまたはオンボードキーマネージャ (OKM) がノードにキーを提供します。

- 外部キー管理サーバはストレージ環境に配置されたサードパーティのシステムで、Key Management Interoperability Protocol (KMIP) を使用してノードにキーを提供します。外部キー管理サーバは、データとは別のストレージシステムで設定することを推奨します。
- オンボードキーマネージャは組み込みのツールで、データと同じストレージシステムからノードにキーを提供します。

ONTAP 9.7 以降では、ボリューム暗号化 (VE) ライセンスがあり、オンボードキーマネージャまたは外部キーマネージャを使用している場合、アグリゲートとボリューム暗号化がデフォルトで有効になります。VE ライセンスは、**"ONTAP One"**。外部キー管理ツールまたはオンボードキーマネージャを設定した場合、新しいアグリゲートおよび新しいボリューム用に保存データの暗号化の設定に変更があります。新しいアグリゲートでは、NetApp Aggregate Encryption (NAE) がデフォルトで有効になります。NAE アグリゲートに含まれない新しいボリュームでは、NetApp Volume Encryption (NVE) がデフォルトで有効になります。マルチテナントキー管理を使用してデータ Storage Virtual Machine (SVM) を独自のキー管理機能で設定した場合は、その SVM 用に作成されたボリュームに自動的に NVE が設定されます。

新規または既存のボリュームで暗号化を有効にできます。NVE は、重複排除や圧縮など、ストレージ効率化のためのさまざまな機能をサポートしています。ONTAP 9.14.1以降では、次のことが可能です。 [既存のSVMルートボリュームでNVEを有効にする](#)。



SnapLock を使用している場合は、新しい空の SnapLock ボリュームでのみ暗号化を有効にできます。既存の SnapLock ボリュームで暗号化を有効にすることはできません。

NVE は、アグリゲートのタイプ（HDD、SSD、ハイブリッド、アレイ LUN）や RAID タイプを問わず、サポートされるすべての ONTAP 環境（ONTAP Select を含む）で使用できます。NVE をハードウェアベースの暗号化と併用すれば、自己暗号化ドライブ上のデータを「暗号化」することもできます。

NVE を有効にすると、コアダンプも暗号化されます。

#### アグリゲートレベルの暗号化

通常、暗号化されたすべてのボリュームには一意のキーが割り当てられます。このキーは、ボリュームを削除すると一緒に削除されます。

ONTAP 9.6 以降では、`_NetApp Aggregate Encryption (NAE)` \_ を使用して、暗号化するボリュームの包含アグリゲートにキーを割り当てることができます。暗号化されたボリュームを削除しても、アグリゲートのキーは削除されません。アグリゲート全体が削除されると、キーは削除されます。

アグリゲートレベルの重複排除をインラインまたはバックグラウンドで実行する場合は、アグリゲートレベルの暗号化を使用する必要があります。そうしないと、NVE でアグリゲートレベルの重複排除がサポートされません。

ONTAP 9.7 以降では、ボリューム暗号化（VE）ライセンスがあり、オンボードキーマネージャまたは外部キーマネージャを使用している場合、アグリゲートとボリューム暗号化がデフォルトで有効になります。

NVE ボリュームと NAE ボリュームは同一アグリゲート内で共存できます。アグリゲートレベルの暗号化で暗号化されたボリュームは、デフォルトで NAE ボリュームになります。このデフォルトの設定は、ボリュームを暗号化するときに無効にすることができます。

を使用できます `volume move` コマンドを使用して NVE ボリュームを NAE ボリュームに変換します。その逆も同様です。NAE ボリュームは NVE ボリュームにレプリケートできます。

を使用することはできません `secure purge` NAE ボリュームに対するコマンド。

#### 外部キー管理サーバを使用する状況

オンボードキーマネージャを使用した方がコストもかからず一般的には便利ですが、次のいずれかに当てはまる場合は KMIP サーバを用意する必要があります。

- 連邦情報処理標準（FIPS）140-2 または OASIS KMIP 標準に準拠した暗号化キー管理解決策が必要な場合。
- 暗号化キーを一元管理するマルチクラスタ解決策が必要です。
- 認証キーをデータとは別のシステムや場所に格納してセキュリティを強化する必要がある場合。

#### 外部キー管理の範囲

外部キー管理のスコープによって、キー管理サーバの保護対象がクラスタ内のすべての SVM になるか、選択した SVM のみになるかが決まります。

- クラスタ内のすべての SVM に対して外部キー管理を設定するには、`cluster scop` を使用します。クラスタ管理者は、サーバに格納されているすべてのキーにアクセスできます。



- ONTAP 9.6 以降では、`svm scop` を使用して、クラスタ内の指定した SVM に外部キー管理を設定できます。各テナントが異なる SVM（または SVM のセット）を使用してデータを提供するマルチテナント環境には、この方法が最適です。特定のテナントの SVM 管理者だけが、そのテナントのキーにアクセスできます。
- ONTAP 9.10.1 以降では、を使用できます [Azure Key Vault](#) と [Google Cloud KMS](#) データSVMのNVEキーのみを保護する。これは、9.12.0以降のAWS KMSで利用できるようになりました。

同じクラスタで両方のスコープを使用できます。1 つの SVM に対してキー管理サーバが設定されている場合、ONTAP はそれらのサーバのみを使用してキーを保護します。それ以外 ONTAP の場合は、クラスタに対して設定されたキー管理サーバでキーが保護されます。

検証済みの外部キー管理ツールのリストは、にあります ["ネットアップの Interoperability Matrix Tool（IMT）"](#)。このリストを確認するには、IMTの検索機能に「キー管理ツール」と入力します。

#### サポートの詳細

次の表に、NVE のサポートの詳細を示します。

リソースまたは機能	サポートの詳細
プラットフォーム	AES-NI オフロード機能が必要です。ご使用のプラットフォームで NVE と NAE がサポートされていることを確認するには、Hardware Universe（HWU）を参照してください。
暗号化	<p>ONTAP 9.7 以降では、ボリューム暗号化（VE）ライセンスを追加し、オンボードキーマネージャまたは外部キーマネージャを設定すると、新しく作成したアグリゲートとボリュームがデフォルトで暗号化されます。暗号化されていないアグリゲートを作成する必要がある場合は、次のコマンドを使用します。</p> <pre>storage aggregate create -encrypt-with-aggr-key false</pre> <p>プレーンテキストのボリュームを作成する必要がある場合は、次のコマンドを使用します。</p> <pre>volume create -encrypt false</pre> <p>次の場合、暗号化はデフォルトでは有効になりません。</p> <ul style="list-style-type: none"> <li>• VE ライセンスがインストールされていません。</li> <li>• キー管理ツールが設定されていません</li> <li>• プラットフォームまたはソフトウェアは暗号化をサポートしていません</li> <li>• ハードウェアの暗号化が有効です</li> </ul>
ONTAP	すべての ONTAP 実装。ONTAP 9.5 以降では、ONTAP クラウドがサポートされます。
デバイス	HDD、SSD、ハイブリッド、アレイ LUN



RAID の場合	RAID0、RAID 4、RAID-DP、RAID-TEC のいずれかです。
個のボリューム	データボリュームと既存のSVMルートボリューム。MetroClusterメタデータボリュームのデータは暗号化できません。9.14.1より前のバージョンのONTAPでは、NVEを使用してSVMルートボリュームのデータを暗号化できません。ONTAP 9.14.1以降では、ONTAPでサポートされます。 <a href="#">SVMルートボリュームのNVE</a> 。
アグリゲートレベルの暗号化	<p>ONTAP 9.6 以降では、NVE でアグリゲートレベルの暗号化（NAE）がサポートされます。</p> <ul style="list-style-type: none"> <li>・アグリゲートレベルの重複排除をインラインまたはバックグラウンドで実行する場合は、アグリゲートレベルの暗号化を使用する必要があります。</li> <li>・アグリゲートレベルで暗号化されたボリュームのキーは変更できません。</li> <li>・アグリゲートレベルで暗号化されたボリュームでは、セキュアページがサポートされません。</li> <li>・NAE では、データボリュームに加えて、SVM ルートボリュームと MetroCluster メタデータボリュームの暗号化がサポートされます。ただし、ルートボリュームの暗号化はサポートされません。</li> </ul>
SVM スコープ	ONTAP 9.6 以降では、NVE で外部キー管理のみを対象に SVM スコープがサポートされます。オンボードキーマネージャに対してはサポートされません。MetroCluster は ONTAP 9.8 以降でサポートされています。
ストレージ効率	<p>重複排除、圧縮、コンパクション、FlexClone。</p> <p>クローンでは、親からスプリットしたあとも親と同じキーを使用します。を実行する必要があります volume move スプリットクローンの場合、スプリットクローンには別のキーが割り当てられます。</p>
レプリケーション	<ul style="list-style-type: none"> <li>・ボリュームレプリケーションでは、ソースボリュームとデスティネーションボリュームで異なる暗号化設定を使用できます。暗号化は、送信元に対して設定することも、宛先に対して設定解除することもできます。逆も同様です。</li> <li>・SVM レプリケーションの場合、デスティネーションボリュームは自動的に暗号化されます。ただし、ボリューム暗号化をサポートするノードがデスティネーションに含まれていない場合、レプリケーションは成功しますが、デスティネーションボリュームは暗号化されません。</li> <li>・MetroCluster 構成では、各クラスタが設定されたキーサーバから外部キー管理のキーを取得します。OKM キーは、構成レプリケーションサービスによってパートナーサイトにレプリケートされます。</li> </ul>
コンプライアンス	ONTAP 9.2 以降では、新しいボリュームのみを対象に、SnapLock が Compliance モードと Enterprise モードの両方でサポートされます。既存の SnapLock ボリュームで暗号化を有効にすることはできません。

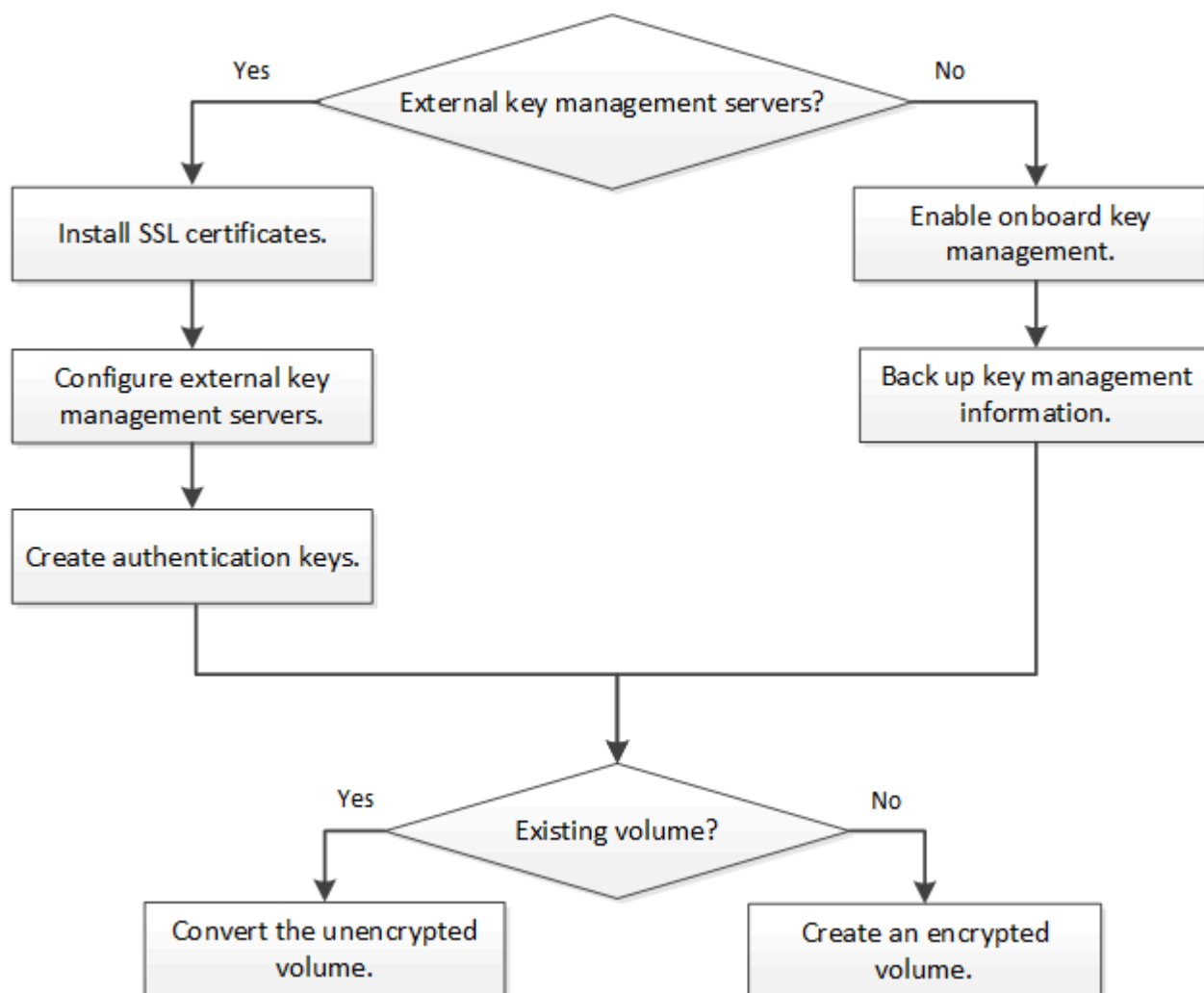
FlexGroup	ONTAP 9.2 以降では、FlexGroup がサポートされます。デスティネーションアグリゲートのタイプは、ボリュームレベルまたはアグリゲートレベルのソースアグリゲートと同じである必要があります。ONTAP 9.5 以降では、FlexGroup ボリュームのキーをインプレースで変更できます。
7-Mode からの移行	7-Mode Transition Tool 3.3 以降では、7-Mode Transition Tool CLI を使用して、クラスタシステムの NVE 対応デスティネーションボリュームへのコピーベースの移行を実行できます。

## 関連情報

["FAQ - NetApp Volume EncryptionおよびNetApp Aggregate Encryption"](#)

## NetApp Volume Encryption のワークフロー

ボリューム暗号化を有効にする前に、キー管理サービスを設定する必要があります。暗号化は新しいボリュームでも既存のボリュームでも有効にすることができます。



"VEライセンスをインストールする必要があります。" NVEでデータを暗号化する前に、キー管理サービスを設定しておく必要があります。ライセンスをインストールする前に、を実行する必要があります "ONTAP のバージョンが NVE をサポートしているかどうかを確認します"。

## NVEの設定

クラスタのバージョンが **NVE** をサポートしているかどうかを確認します

ライセンスをインストールする前に、クラスタのバージョンが NVE をサポートしているかどうかを確認する必要があります。を使用できます `version` コマンドを使用してクラスタのバージョンを確認します。

このタスクについて

クラスタのバージョンは、クラスタ内のいずれかのノードで実行されている ONTAP の最下位のバージョンです。

ステップ

1. クラスタのバージョンが NVE をサポートしているかどうかを確認します。

```
version -v
```

コマンドの出力に「1Ono-dARE」というテキスト（「no Data at Rest Encryption」の場合）、またはに記載されていないプラットフォームを使用している場合は、NVE はサポートされません "[サポートの詳細](#)"。

次のコマンドは、でNVEがサポートされるかどうかを確認します `cluster1`。

```
cluster1::> version -v
NetApp Release 9.1.0: Tue May 10 19:30:23 UTC 2016 <1Ono-DARE>
```

の出力 1Ono-DARE クラスタのバージョンでNVEがサポートされていないことを示します。

ライセンスをインストール

VE ライセンスでは、クラスタ内のすべてのノードでこの機能を使用できます。このライセンスは、NVEでデータを暗号化する前に必要です。に含まれている "[ONTAP One](#)"。

ONTAP Oneより前のバージョンでは、VEライセンスは暗号化バンドルに含まれていました。Encryptionバンドルは提供されなくなりましたが、引き続き有効です。現在は必須ではありませんが、既存のお客様は "[ONTAP Oneへのアップグレード](#)"。

作業を開始する前に

- このタスクを実行するには、クラスタ管理者である必要があります。
- 営業担当者からVEライセンスキーを入手するか、ONTAP Oneをインストールしておく必要があります。

手順

1. "[VEライセンスがインストールされていることを確認します。](#)"。

VEライセンスパッケージ名は `VE`。

2. ライセンスがインストールされていない場合は、 "[System ManagerまたはONTAP CLIを使用してインストール](#)"。

## 外部キー管理の概要の設定

1 つ以上の外部キー管理サーバを使用して、暗号化されたデータにアクセスする際にクラスタで使用するキーを安全に保管できます。外部キー管理サーバはストレージ環境に配置されたサードパーティのシステムで、Key Management Interoperability Protocol (KMIP) を使用してノードにキーを提供します。



ONTAP 9.1 以前のバージョンでは、外部キー管理ツールを使用する前に、ノード管理ロールが設定されたポートにノード管理 LIF を割り当てる必要があります。

ONTAP 9.1 以降では、NetApp Volume Encryption (NVE) によってオンボードキーマネージャがサポートされます。ONTAP 9.3以降では、NVEで外部キー管理 (KMIP) とオンボードキーマネージャがサポートされます。ONTAP 9.10.1 以降では、を使用できます [Azure Key Vaultサービス](#)または[Google Cloud Key Managerサービス](#) NVEキーを保護するため。ONTAP 9.11.1以降では、1つのクラスタに複数の外部キー管理ツールを設定できます。を参照してください [クラスタ化されたキーサーバを設定](#)

**System Manager**を使用して外部キー管理ツールを管理します。

ONTAP 9.7以降では、オンボードキーマネージャを使用して認証キーと暗号化キーを格納および管理できます。ONTAP 9.13.1以降では、外部キー管理ツールを使用してこれらのキーを格納および管理することもできます。

オンボードキーマネージャは、クラスタ内のセキュアなデータベースにキーを格納および管理します。スコープはクラスタです。外部キー管理ツールは、クラスタの外部にキーを格納および管理します。スコープには、クラスタまたはStorage VMを指定できます。1つ以上の外部キー管理ツールを使用できます。次の条件が適用されます。

- ・ オンボードキーマネージャが有効になっている場合、外部キー管理ツールをクラスタレベルで有効にすることはできませんが、Storage VMレベルで有効にすることはできます。
- ・ 外部キー管理ツールがクラスタレベルで有効になっている場合、オンボードキーマネージャを有効にすることはできません。

外部キー管理ツールを使用する場合は、Storage VMおよびクラスタごとに最大4つのプライマリキーサーバを登録できます。各プライマリキーサーバは、最大3台のセカンダリキーサーバでクラスタ化できます。

## 外部キー管理ツールを設定する

Storage VMに外部キー管理ツールを追加するには、Storage VMのネットワークインターフェイスの設定時にオプションのゲートウェイを追加する必要があります。Storage VMをネットワークルートなしで作成した場合は、外部キー管理ツール用のルートを明示的に作成する必要があります。を参照してください ["LIFを作成する \(ネットワークインターフェイス\)"](#)。

### 手順

外部キー管理ツールは、System Managerの別の場所から設定できます。




1. 外部キー管理ツールを設定するには、次のいずれかの開始手順を実行します。

ワークフロー

ナビゲーション

開始ステップ

キーマネージャを設定します	[クラスタ]>*[設定]*	[セキュリティ]*セクションまでスクロールします。[暗号化]*で、を選択します  。[外部キーマネージャ]*を選択します。
ローカル階層を追加してください	ストレージ>*[階層]*	[+ローカル階層の追加]*を選択します。[Configure Key Manager]チェックボックスをオンにします。[外部キーマネージャ]*を選択します。
ストレージを準備	ダッシュボード	セクションで、[ストレージの準備]*を選択します。次に、[Configure Key Manager]を選択します。[外部キーマネージャ]*を選択します。
暗号化を設定（キー管理ツールをStorage VMスコープでのみ使用）	ストレージ>*[Storage VM]*	Storage VM を選択してください。[設定]タブを選択します。の[暗号化]*セクションで、を選択します  。


- プライマリキーサーバを追加するには、  **Add** をクリックし、[IPアドレス]または[ホスト名]\*および[ポート]\*フィールドに入力します。
- インストールされている既存の証明書は、[KMIP Server CA Certificates]\*フィールドと[KMIP Client Certificate]\*フィールドに表示されます。次のいずれかの操作を実行できます。
  - 選択するオプション  をクリックして、キー管理ツールにマッピングするインストール済み証明書を選択します。（複数のサービスCA証明書を選択できますが、選択できるクライアント証明書は1つだけです）。
  - まだインストールされていない証明書を追加して外部キー管理ツールにマッピングする場合は、\*[新しい証明書の追加]\*を選択します。
  - 選択するオプション  をクリックして、インストールされている証明書のうち外部キー管理ツールにマッピングしない証明書を削除します。
- セカンダリキーサーバを追加するには、[セカンダリキーサーバ]\*列で[追加]\*を選択し、詳細を指定します。
- [保存]\*を選択して設定を完了します。

既存の外部キー管理ツールを編集します

すでに外部キー管理ツールを設定している場合は、その設定を変更できます。

#### 手順

- 外部キー管理ツールの設定を編集するには、次のいずれかの開始手順を実行します。

適用範囲	ナビゲーション	開始ステップ
クラスタスコープの外部キー管理ツール	[クラスタ]>*[設定]*	セクションまでスクロールします。[暗号化]*で、を選択します  をクリックし、[外部キーマネージャの編集]*を選択します。

Storage VMスコープの外部キー管理ツール	ストレージ>* Storage VM *	Storage VM を選択してください。[設定]タブを選択します。の[暗号化]セクションで、を選択します。 をクリックし、[外部キーマネージャの編集]*を選択します。
--------------------------	----------------------	--

2. 既存のキーサーバは\*[キーサーバ]\*の表に表示されます。次の操作を実行できます。

- 次を選択して新しいキーサーバを追加します。 **+ Add**。
- キーサーバを削除するには、 **⋮** キーサーバの名前を含むテーブルセルの最後に表示されます。そのプライマリキーサーバに関連付けられているセカンダリキーサーバも設定から削除されます。

外部キー管理ツールを削除します

ボリュームが暗号化されていない場合は、外部キー管理ツールを削除できます。

手順

1. 外部キー管理ツールを削除するには、次のいずれかの手順を実行します。

適用範囲	ナビゲーション	開始ステップ
クラスタスコープの外部キー管理ツール	【クラスタ】>*[設定]*	セクションまでスクロールします。[暗号化]*で、を選択します。 をクリックし、[外部キーマネージャの削除]*を選択します。
Storage VMスコープの外部キー管理ツール	ストレージ>* Storage VM *	Storage VM を選択してください。[設定]タブを選択します。の[暗号化]セクションで、を選択します。 をクリックし、[外部キーマネージャの削除]*を選択します。

キー管理ツール間でキーを移行する

クラスタで複数のキー管理ツールを有効にしている場合は、キー管理ツール間でキーを移行する必要があります。このプロセスはSystem Managerで自動的に完了します。

- オンボードキーマネージャまたは外部キーマネージャがクラスタレベルで有効になっていて、一部のボリュームが暗号化されている場合は、その後、Storage VMレベルで外部キー管理ツールを設定する際には、それらのキーをクラスタレベルのオンボードキーマネージャまたは外部キー管理ツールからStorage VMレベルの外部キー管理ツールに移行する必要があります。このプロセスは、System Managerによって自動的に実行されます。
- Storage VMで暗号化なしでボリュームを作成した場合は、キーを移行する必要はありません。

クラスタに **SSL** 証明書をインストールします

クラスタと KMIP サーバの間では、相互の ID を検証して SSL 接続を確立するために KMIP SSL 証明書を使用します。KMIP サーバとの SSL 接続を設定する前に、クラスタの KMIP クライアント SSL 証明書、および KMIP サーバのルート Certificate Authority（CA；認証局）の SSL パブリック証明書をインストールする必要があります。



## このタスクについて

HA ペア構成では、両方のノードで同じ SSL KMIP パブリック証明書とプライベート証明書を使用する必要があります。複数の HA ペアを同じ KMIP サーバに接続する場合は、HA ペアのすべてのノードで同じ SSL KMIP パブリック証明書とプライベート証明書を使用する必要があります。

## 作業を開始する前に

- 証明書を作成するサーバ、KMIP サーバ、およびクラスタの時刻が同期されている必要があります。
- クラスタのパブリック SSL KMIP クライアント証明書を入手しておく必要があります。
- クラスタの SSL KMIP クライアント証明書に関連付けられた秘密鍵を入手しておく必要があります。
- SSL KMIP クライアント証明書は、パスワードで保護しないでください。
- KMIP サーバのルート認証局（CA）の SSL パブリック証明書を入手しておく必要があります。
- MetroCluster環境では、両方のクラスタに同じKMIP SSL証明書をインストールする必要があります。



KMIP サーバへのクライアント証明書とサーバ証明書のインストールは、クラスタに証明書をインストールする前でもインストールしたあとでもかまいません。

## 手順

1. クラスタに SSL KMIP クライアント証明書をインストールします。

```
security certificate install -vserver admin_svm_name -type client
```

SSL KMIP パブリック証明書とプライベート証明書を入力するように求められます。

```
cluster1::> security certificate install -vserver cluster1 -type client
```

2. KMIP サーバのルート認証局（CA）の SSL パブリック証明書をインストールします。

```
security certificate install -vserver admin_svm_name -type server-ca
```

```
cluster1::> security certificate install -vserver cluster1 -type server-ca
```

## ONTAP 9.6 以降で外部キー管理を有効にする（NVE）

1 つ以上の KMIP サーバを使用して、暗号化されたデータにアクセスする際にクラスタで使用するキーを安全に保管できます。ONTAP 9.6以降では、データSVMが暗号化されたデータにアクセスする際に使用するキーを保護するための独立した外部キー管理ツールを設定できます。

ONTAP 9.11.1以降では、プライマリキーサーバごとに最大3つのセカンダリキーサーバを追加してクラスタ化されたキーサーバを作成できます。詳細については、[を参照してください クラスタ構成の外部キーサーバを構成](#)。

## このタスクについて

1 つのクラスタまたは SVM に最大 4 つの KMIP サーバを接続できます。冗長性とディザスタリカバリのために、少なくとも 2 台のサーバを使用することを推奨します。

外部キー管理のスコープによって、キー管理サーバの保護対象がクラスタ内のすべての SVM になるか、選択

した SVM のみになるかが決まります。

- クラスタ内のすべての SVM に対して外部キー管理を設定するには、*cluster scop* を使用します。クラスタ管理者は、サーバに格納されているすべてのキーにアクセスできます。
- ONTAP 9.6 以降では、*svm scop* を使用して、クラスタ内のデータ SVM に外部キー管理を設定できます。各テナントが異なる SVM（または SVM のセット）を使用してデータを提供するマルチテナント環境には、この方法が最適です。特定のテナントの SVM 管理者だけが、そのテナントのキーにアクセスできます。
- マルチテナント環境の場合は、次のコマンドを使用して、*MT\_EK\_MGMT* のライセンスをインストールします。

```
system license add -license-code <MT_EK_MGMT license code>
```

コマンド構文全体については、コマンドのマニュアルページを参照してください。

同じクラスタで両方のスコープを使用できます。1 つの SVM に対してキー管理サーバが設定されている場合、ONTAP はそれらのサーバのみを使用してキーを保護します。それ以外 ONTAP の場合は、クラスタに対して設定されたキー管理サーバでキーが保護されます。

オンボードキー管理はクラスタスコープで設定でき、外部キー管理は SVM スコープで設定できます。を使用できます `security key-manager key migrate` コマンドを使用して、クラスタスコープのオンボードキー管理から SVM スコープの外部キー管理ツールにキーを移行します。

作業を開始する前に

- KMIP SSL クライアント証明書とサーバ証明書をインストールしておく必要があります。
- このタスクを実行するには、クラスタ管理者または SVM の管理者である必要があります。
- MetroCluster 環境で外部キー管理を有効にする場合は、外部キー管理を有効にする前に MetroCluster が完全に設定されている必要があります。
- MetroCluster 環境では、両方のクラスタに KMIP SSL 証明書をインストールする必要があります。

手順

1. クラスタのキー管理ツールの接続を設定します。

```
security key-manager external enable -vserver admin_SVM -key-servers  
host_name|IP_address:port,... -client-cert client_certificate -server-ca-cert  
server_CA_certificates
```



- °。 `security key-manager external enable` コマンドは、に置き換わるものです `security key-manager setup` コマンドを実行しますクラスタのログインプロンプトでコマンドを実行すると、*admin\_SVM* デフォルトでは、現在のクラスタの管理 SVM が使用されます。クラスタスコープを設定するには、クラスタ管理者である必要があります。を実行できます `security key-manager external modify` コマンドを使用して、外部キー管理の設定を変更します。
- ° MetroCluster 環境で管理 SVM に外部キー管理を設定する場合は、を繰り返す必要があります `security key-manager external enable` パートナークラスタに対して実行します。

次のコマンドは、の外部キー管理を有効にします `cluster1` 3 つの外部キーサーバで構成されます。最初



のキーサーバはホスト名とポートで指定し、2 番目のキーサーバは IP アドレスとデフォルトポートで指定し、3 番目のキーサーバは IPv6 アドレスとポートで指定します。

```
cluster1::> security key-manager external enable -vserver cluster1 -key
-servers
ks1.local:15696,10.0.0.10,[fd20:8b1e:b255:814e:32bd:f35c:832c:5a09]:1234
-client-cert AdminVserverClientCert -server-ca-certs
AdminVserverServerCaCert
```

## 2. キー管理ツールとして SVM を設定します。

```
security key-manager external enable -vserver SVM -key-servers
host_name|IP_address:port,... -client-cert client_certificate -server-ca-cert
server_CA_certificates
```



- SVM のログインプロンプトでコマンドを実行すると、SVM デフォルトは現在の SVM です。SVM スコープを設定するには、クラスタ管理者または SVM 管理者である必要があります。を実行できます `security key-manager external modify` コマンドを使用して、外部キー管理の設定を変更します。
- MetroCluster 環境でデータ SVM に外部キー管理を設定する場合は、の手順を繰り返す必要はありません `security key-manager external enable` パートナークラスタに対して実行します。

次のコマンドは、の外部キー管理を有効にします `svm1` 単一のキーサーバがデフォルトポート 5696 でリスンしている場合：

```
svm11::> security key-manager external enable -vserver svm1 -key-servers
keyserver.svm1.com -client-cert SVM1ClientCert -server-ca-certs
SVM1ServerCaCert
```

## 3. 最後の手順をその他の SVM に対して繰り返します。



を使用することもできます `security key-manager external add-servers` コマンドを使用して追加の SVM を設定します。。 `security key-manager external add-servers` コマンドは、に置き換わるものです `security key-manager add` コマンドを実行しますコマンド構文全体については、マニュアルページを参照してください。

## 4. 設定したすべての KMIP サーバが接続されていることを確認します。

```
security key-manager external show-status -node node_name
```



。 `security key-manager external show-status` コマンドは、に置き換わるものです `security key-manager show -status` コマンドを実行しますコマンド構文全体については、マニュアルページを参照してください。

```
cluster1::> security key-manager external show-status
```

Node	Vserver	Key Server	Status
-----			
node1			
	svm1	keyserver.svm1.com:5696	available
	cluster1	10.0.0.10:5696	available
		fd20:8b1e:b255:814e:32bd:f35c:832c:5a09:1234	available
		ks1.local:15696	available
node2			
	svm1	keyserver.svm1.com:5696	available
	cluster1	10.0.0.10:5696	available
		fd20:8b1e:b255:814e:32bd:f35c:832c:5a09:1234	available
		ks1.local:15696	available

8 entries were displayed.

5. 必要に応じて、プレーンテキストボリュームを暗号化ボリュームに変換します。

```
volume encryption conversion start
```

ボリュームを変換する前に、外部キー管理ツールの設定をすべて完了しておく必要があります。MetroCluster環境では、両方のサイトに外部キー管理ツールを設定する必要があります。

#### ONTAP 9.5 以前で外部キー管理を有効にします

1 つ以上の KMIP サーバを使用して、暗号化されたデータにアクセスする際にクラスタで使用するキーを安全に保管できます。1 つのノードに最大 4 つの KMIP サーバを接続できます。冗長性とディザスタリカバリのために、少なくとも 2 台のサーバを使用することを推奨します。

このタスクについて

ONTAP は、クラスタ内のすべてのノードについて KMIP サーバの接続を設定します。

作業を開始する前に

- KMIP SSL クライアント証明書とサーバ証明書をインストールしておく必要があります。
- このタスクを実行するには、クラスタ管理者である必要があります。
- 外部キー管理ツールを設定する前に、MetroCluster 環境を設定する必要があります。
- MetroCluster 環境では、両方のクラスタにKMIP SSL証明書をインストールする必要があります。

## 手順

1. クラスタノードのキー管理ツールの接続を設定します。

```
security key-manager setup
```

キー管理ツールのセットアップが開始されます。



MetroCluster 環境では、このコマンドを両方のクラスタで実行する必要があります。

2. 各プロンプトで適切な応答を入力します。
3. KMIP サーバを追加します。

```
security key-manager add -address key_management_server_ipaddress
```

```
cluster1::> security key-manager add -address 20.1.1.1
```



MetroCluster 環境では、このコマンドを両方のクラスタで実行する必要があります。

4. 冗長性を確保するために KMIP サーバをもう 1 つ追加します。

```
security key-manager add -address key_management_server_ipaddress
```

```
cluster1::> security key-manager add -address 20.1.1.2
```



MetroCluster 環境では、このコマンドを両方のクラスタで実行する必要があります。

5. 設定したすべての KMIP サーバが接続されていることを確認します。

```
security key-manager show -status
```

コマンド構文全体については、マニュアルページを参照してください。

```
cluster1::> security key-manager show -status
```

Node	Port	Registered Key Manager	Status
-----	----	-----	-----
cluster1-01	5696	20.1.1.1	available
cluster1-01	5696	20.1.1.2	available
cluster1-02	5696	20.1.1.1	available
cluster1-02	5696	20.1.1.2	available

6. 必要に応じて、プレーンテキストボリュームを暗号化ボリュームに変換します。

```
volume encryption conversion start
```

ボリュームを変換する前に、外部キー管理ツールの設定をすべて完了しておく必要があります。MetroCluster環境では、両方のサイトに外部キー管理ツールを設定する必要があります。

クラウドプロバイダを使用してキーを管理します

ONTAP 9.10.1 以降では、を使用できます **"Azure キーボールド (AKV)"** および **"Google Cloud Platform のキー管理サービス (Cloud KMS)"** クラウドでホストされるアプリケーションでONTAP暗号化キーを保護する。ONTAP 9.12.0以降では、を使用してNVEキーを保護することもできます **"AWS KMS"**。

AWS KMS、AKV、Cloud KMSを使用して保護できます **"NetApp Volume Encryption (NVE) キー"** データSVMの場合のみ。

このタスクについて

クラウドプロバイダを使用したキー管理は、CLIまたはONTAP REST APIを使用して有効にできます。

クラウドプロバイダを使用してキーを保護する場合は、デフォルトではデータSVM LIFがクラウドキー管理エンドポイントとの通信に使用されることに注意してください。ノード管理ネットワークは、クラウドプロバイダの認証サービス (login.microsoftonline.com for Azure ; oauth2.googleapis.com for Cloud KMS) との通信に使用されます。クラスタネットワークが正しく設定されていないと、クラスタでキー管理サービスが適切に利用されません。

クラウドプロバイダのキー管理サービスを利用する場合は、次の制限事項に注意してください。

- クラウドプロバイダのキー管理は、NetApp Storage Encryption (NSE) およびNetApp Aggregate Encryption (NAE) では使用できません。 **"外部 KMIP"** 代わりに使用できます。
- クラウドプロバイダのキー管理はMetroCluster構成では使用できません。
- クラウドプロバイダのキー管理は、データSVMでのみ設定できます。

作業を開始する前に

- 適切なクラウドプロバイダでKMSを設定しておく必要があります。
- ONTAPクラスタのノードでNVEがサポートされている必要があります。
- **"Volume Encryption (VE) ライセンスとマルチテナントEncryption Key Management (MTEKM) ライセンスをインストールしておく必要があります。"**。これらのライセンスは、**"ONTAP One"**。
- クラスタ管理者またはSVM管理者である必要があります。
- データSVMに暗号化されたボリュームが含まれていないか、キー管理ツールを使用していないことを確認してください。データSVMに暗号化されたボリュームが含まれている場合は、KMSを設定する前にそれらのボリュームを移行する必要があります。

外部キー管理を有効にします

外部キー管理を有効にする方法は、使用するキー管理ツールによって異なります。該当するキー管理ツールと環境のタブを選択します。

## AWS

作業を開始する前に

- 暗号化を管理するIAMロールで使用されるAWS KMSキーの付与を作成する必要があります。IAMロールには、次の処理を許可するポリシーが含まれている必要があります。

- DescribeKey
  - Encrypt
  - Decrypt
- [+]

詳細については、AWSのドキュメントを参照してください ["助成金"](#)。

### ONTAP SVMでAWS KMSを有効にします

1. 作業を開始する前に、AWS KMSからアクセスキーIDとシークレットキーの両方を取得します。

2. 権限レベルを `advanced` に設定します。

```
set -priv advanced
```

3. AWS KMSを有効にします。

```
security key-manager external aws enable -vserver svm_name -region  
AWS_region -key-id key_ID -encryption-context encryption_context
```

4. プロンプトが表示されたら、シークレットキーを入力します。

5. AWS KMSが正しく設定されたことを確認します。

```
security key-manager external aws show -vserver svm_name
```

## Azure

### ONTAP SVMでAzure Key Vaultを有効にします

1. 作業を開始する前に、クライアントシークレットまたは証明書のいずれかで、Azure アカウントから適切な認証クレデンシャルを取得する必要があります。  
また、クラスタ内のすべてのノードが正常であることを確認する必要があります。これを確認するには、コマンドを使用します `cluster show`。

2. 特権レベルを `advanced` に設定します

```
set -priv advanced
```

3. SVMでAKVを有効にします

```
security key-manager external azure enable -client-id client_id -tenant-id  
tenant_id -name -key-id key_id -authentication-method {certificate|client-  
secret}
```

プロンプトが表示されたら、Azure アカウントからクライアント証明書またはクライアントシークレットを入力します。

4. AKVが正しく有効になっていることを確認します。

```
security key-manager external azure show vserver svm_name
```

サービスの到達可能性がOKでない場合は、データSVM LIFを介したAKVキー管理サービスへの接続を確立します。

## Google Cloud

### ONTAP SVMでCloud KMSを有効にします

1. 開始する前に、Google Cloud KMSアカウントキーファイルの秘密鍵をJSON形式で取得します。これは GCP アカウントにあります。

また、クラスタ内のすべてのノードが正常であることを確認する必要があります。これを確認するには、コマンドを使用します `cluster show`。

2. 特権レベルをadvancedに設定します。

```
set -priv advanced
```

3. SVMでCloud KMSを有効にします

```
security key-manager external gcp enable -vserver svm_name -project-id  
project_id-key-ring-name key_ring_name -key-ring-location key_ring_location  
-key-name key_name
```

プロンプトが表示されたら、サービスアカウントの秘密鍵を使用して JSON ファイルの内容を入力します

4. Cloud KMSが正しいパラメータで構成されていることを確認します。

```
security key-manager external gcp show vservers svm_name
```

のステータス `kms_wrapped_key_status` になります "UNKNOWN" 暗号化されたボリュームが作成されていない場合。

サービスへの到達可能性がOKでない場合は、データSVM LIFを介してGCPキー管理サービスへの接続を確立します。

データSVM用にすでに暗号化されたボリュームが1つ以上設定され、管理SVMのオンボードキーマネージャで対応するNVEキーが管理されている場合は、それらのキーを外部キー管理サービスに移行する必要があります。CLIでこれを行うには、次のコマンドを実行します。

```
security key-manager key migrate -from-Vserver admin_SVM -to-Vserver data_SVM
```

データSVMのすべてのNVEキーが正常に移行されるまで、テナントのデータSVM用に暗号化された新しいボリュームを作成することはできません。

#### 関連情報

- ["ネットアップのCloud Volumes ONTAP向け暗号化ソリューションを使用したボリュームの暗号化"](#)

#### ONTAP 9.6 以降でオンボードキー管理を有効にする (NVE)

オンボードキーマネージャを使用して、暗号化されたデータにアクセスする際にクラスタで使用するキーを安全に保管できます。オンボードキーマネージャは、暗号化されたボリュームまたは自己暗号化ディスクにアクセスする各クラスタで有効にする必要があります。

#### このタスクについて

を実行する必要があります `security key-manager onboard sync` コマンドはクラスタにノードを追加するたびに実行します。

MetroCluster構成を使用している場合は、`security key-manager onboard enable` 最初にローカルクラスタでコマンドを実行してから、`security key-manager onboard sync` リモートクラスタで同じパスフレーズを使用してコマンドを実行します。を実行すると `security key-manager onboard enable` ローカルクラスタからコマンドを実行し、リモートクラスタで同期する必要はありません。enable リモートクラスタからコマンドを再実行します。

デフォルトでは、ノードのリブート時にキー管理ツールのパスフレーズを入力する必要はありません。を使用できます `cc-mode-enabled=yes` リブート後にユーザにパスフレーズの入力を求めるオプション。

NVEの場合は、を設定します `cc-mode-enabled=yes` `を使用して作成したボリューム `volume create および `volume move start` コマンドは自動的に暗号化されます。の場合 `volume create` `を指定する必

要はありません ``-encrypt true``。の場合 `volume move start``を指定する必要はありません ``-encrypt-destination true``。

保管データの ONTAP 暗号化を設定する場合、CSfC（Commercial Solutions for Classified）の要件を満たすために、NVE で NSE を使用し、Common Criteria モードでオンボードキーマネージャが有効になっていることを確認する必要があります。を参照してください ["CSfC 解決策 Brief（CSfC の概要）"](#) CSfC の詳細については、を参照してください。

オンボードキーマネージャがCCモードで有効になっている場合 (`cc-mode-enabled=yes`) では、システムの動作は次のように変更されます。

- Common Criteria モードで動作している場合、クラスタパスフレーズの試行に連続して失敗したかどうか監視されます。

ブート時に正しいクラスタパスフレーズを入力しなかった場合、暗号化されたボリュームはマウントされません。これを修正するには、ノードをリブートし、正しいクラスタパスフレーズを入力する必要があります。ブート後、パラメータとしてクラスタパスフレーズを必要とするコマンドに対して、最大 5 回連続してクラスタパスフレーズを 24 時間以内に入力することができます。制限に達した場合（たとえば、クラスタのパスフレーズを 5 回連続して正しく入力できなかった場合など）は、24 時間のタイムアウトが経過するまで待つか、ノードをリブートして制限をリセットする必要があります。

- システムイメージの更新では、NetApp RSA-3072 コード署名証明書と SHA-384 コード署名ダイジェストを使用して、通常の NetApp RSA-2048 コード署名証明書および SHA-256 コード署名ダイジェストではなく、イメージの整合性をチェックします。

`upgrade` コマンドは、さまざまなデジタル署名をチェックして、イメージの内容が変更されていないか、壊れていないかを確認します。検証に成功した場合は、イメージの更新プロセスが次の手順に進みます。成功しなかった場合は、イメージの更新が失敗します。を参照してください `cluster image` のマニュアルページを参照してください。

オンボードキーマネージャは、揮発性メモリにキーを格納します。揮発性メモリの内容は、システムのリブート時または停止時にクリアされます。通常の動作条件下では、システムが停止すると 30 秒以内に揮発性メモリの内容がクリアされます。

作業を開始する前に

- このタスクを実行するには、クラスタ管理者である必要があります。
- オンボードキーマネージャを設定する前に、MetroCluster 環境を設定する必要があります。

手順

1. キー管理ツールのセットアップを開始します。

```
security key-manager onboard enable -cc-mode-enabled yes|no
```

設定 `cc-mode-enabled=yes` リブート後にユーザにキー管理ツールのパスフレーズの入力を求める場合。NVEの場合は、を設定します `cc-mode-enabled=yes``を使用して作成したボリューム ``volume create` および `volume move start` コマンドは自動的に暗号化されます。。 - `cc-mode-enabled` オプションはMetroCluster 構成ではサポートされません。。 `security key-manager onboard enable` コマンドは、に置き換わるものです `security key-manager setup` コマンドを実行します



次の例では、リブートのたびにパスフレーズの入力を求めずに、cluster1 でキー管理ツールの setup コマンドを開始します。

```
cluster1::> security key-manager onboard enable
```

```
Enter the cluster-wide passphrase for onboard key management in Vserver
"cluster1"::    <32..256 ASCII characters long text>
Reenter the cluster-wide passphrase:    <32..256 ASCII characters long
text>
```

2. パスフレーズのプロンプトで 32 ～ 256 文字のパスフレーズを入力します。または、64 ～ 256 文字のパスフレーズを「cc-mode」に入力します。



指定された "cc-mode" パスフレーズが 64 文字未満の場合、キー管理ツールのセットアップ操作によってパスフレーズのプロンプトが再表示されるまでに 5 秒の遅延が発生します。

3. パスフレーズの確認のプロンプトでパスフレーズをもう一度入力します。
4. 認証キーが作成されたことを確認します。

```
security key-manager key query -key-type NSE-AK
```



。 security key-manager key query コマンドは、に置き換わるものです security key-manager query key コマンドを実行しますコマンド構文全体については、マニュアルページを参照してください。

次の例は、の認証キーが作成されたことを確認します cluster1 :



```
cluster1::> security key-manager key query -key-type NSE-AK
Node: node1
Vserver: cluster1
Key Manager: onboard
Key Manager Type: OKM
Key Manager Policy: -
```

Key Tag	Key Type	Encryption	Restored
node1	NSE-AK	AES-256	true
Key ID: 00000000000000000000200000000000100056178fc6ace6d91472df8a9286daacc00000000 00000000			
node1	NSE-AK	AES-256	true
Key ID: 00000000000000000000200000000000100df1689a148fdfbf9c2b198ef974d0baa00000000 00000000			

2 entries were displayed.

5. 必要に応じて、プレーンテキストボリュームを暗号化ボリュームに変換します。

```
volume encryption conversion start
```

ボリュームを変換する前に、オンボードキーマネージャの設定が完了している必要があります。MetroCluster環境では、両方のサイトでオンボードキーマネージャを設定する必要があります。

完了後

あとで使用できるように、ストレージシステムの外部の安全な場所にパスフレーズをコピーしておきます。

オンボードキーマネージャのパスフレーズを設定するときは、災害時に備えて、ストレージシステムの外部の安全な場所にも手動で情報をバックアップしておく必要があります。を参照してください ["オンボードキー管理情報を手動でバックアップ"](#)。

**ONTAP 9.5** 以前でオンボードキー管理を有効にする（**NVE**）

オンボードキーマネージャを使用して、暗号化されたデータにアクセスする際にクラスタで使用するキーを安全に保管できます。オンボードキーマネージャは、暗号化されたボリュームや自己暗号化ディスクにアクセスする各クラスタで有効にする必要があります。

このタスクについて

を実行する必要があります `security key-manager setup` コマンドはクラスタにノードを追加するたびに実行します。

MetroCluster 構成を使用する場合は、次のガイドラインを確認してください。

- ONTAP 9.5では、を実行する必要があります `security key-manager setup` ローカルクラスタおよび `security key-manager setup -sync-metrocluster-config yes` リモートクラスタで、それぞれ同じパスフレーズを使用します。
- ONTAP 9.5より前のバージョンでは、を実行する必要があります `security key-manager setup` ローカルクラスタで、約20秒待ってからを実行します `security key-manager setup` リモートクラスタで、それぞれで同じパスフレーズを使用します。

デフォルトでは、ノードのリブート時にキー管理ツールのパスフレーズを入力する必要はありません。ONTAP 9.4以降では、`-enable-cc-mode yes` リブート後にユーザにパスフレーズの入力を求めるオプション。

NVEの場合は、を設定します `-enable-cc-mode yes` を使用して作成したボリューム ``volume create` および `volume move start` コマンドは自動的に暗号化されます。の場合 `volume create` を指定する必要はありません ``-encrypt true`。の場合 `volume move start` を指定する必要はありません ``-encrypt-destination true`。



パスフレーズの試行に失敗した場合は、ノードを再起動する必要があります。

作業を開始する前に

- 外部キー管理 (KMIP) サーバでNSEまたはNVEを使用している場合は、外部キー管理ツールのデータベースを削除しておく必要があります。

#### "外部キー管理からオンボードキー管理への移行"

- このタスクを実行するには、クラスタ管理者である必要があります。
- オンボードキーマネージャを設定する前に、MetroCluster 環境を設定する必要があります。

手順

1. キー管理ツールのセットアップを開始します。

```
security key-manager setup -enable-cc-mode yes|no
```



ONTAP 9.4以降では、`-enable-cc-mode yes` リブート後にユーザにキー管理ツールのパスフレーズの入力を求めるオプション。NVEの場合は、を設定します `-enable-cc-mode yes` を使用して作成したボリューム ``volume create` および `volume move start` コマンドは自動的に暗号化されます。

次の例では、リブートのたびにパスフレーズの入力を求めずに、`cluster1` でキー管理ツールをセットアップします。

• • •

- 

指定された "cc-mode" パスフレーズが 64 文字未満の場合、キー管理ツールのセットアップ操作によってパスフレーズのプロンプトが再表示されるまでに 5 秒の遅延が発生します。

- 一がすべてのノードに設定されていることを確認します。

```
security key-manager key show
```

マンド構文全体については、マニュアルページを参照してください。

Key ID	Used By
--------	---------

6. 必要に応じて、プレーンテキストボリュームを暗号化ボリュームに変換します。

```
volume encryption conversion start
```

ボリュームを変換する前に、オンボードキーマネージャの設定が完了している必要があります。MetroCluster環境では、両方のサイトでオンボードキーマネージャを設定する必要があります。

完了後

あとで使用できるように、ストレージシステムの外部の安全な場所にパスフレーズをコピーしておきます。

オンボードキーマネージャのパスフレーズを設定するときは、災害時に備えて、ストレージシステムの外部の安全な場所にも手動で情報をバックアップしておく必要があります。を参照してください ["オンボードキー管理情報を手動でバックアップ"](#)。

新しく追加したノードでオンボードキー管理を有効にします

オンボードキーマネージャを使用して、暗号化されたデータにアクセスする際にクラスタで使用するキーを安全に保管できます。オンボードキーマネージャは、暗号化されたボリュームや自己暗号化ディスクにアクセスする各クラスタで有効にする必要があります。



ONTAP 9.5以前の場合は、を実行する必要があります security key-manager setup コマンドはクラスタにノードを追加するたびに実行します。

ONTAP 9.6以降の場合は、を実行する必要があります security key-manager sync コマンドはクラスタにノードを追加するたびに実行します。

オンボードキー管理が設定されているクラスタにノードを追加した場合は、このコマンドを実行して不足しているキーを更新します。

MetroCluster 構成を使用する場合は、次のガイドラインを確認してください。

- ONTAP 9.6以降では、を実行する必要があります security key-manager onboard enable を実行してから、を実行します security key-manager onboard sync リモートクラスタで、それぞれで同じパスフレーズを使用します。
- ONTAP 9.5では、を実行する必要があります security key-manager setup ローカルクラスタおよび security key-manager setup -sync-metrocluster-config yes リモートクラスタで、それぞれで同じパスフレーズを使用します。
- ONTAP 9.5より前のバージョンでは、を実行する必要があります security key-manager setup ローカルクラスタで、約20秒待ってからを実行します security key-manager setup リモートクラスタで、それぞれで同じパスフレーズを使用します。

デフォルトでは、ノードのリブート時にキー管理ツールのパスフレーズを入力する必要はありません。ONTAP 9.4以降では、-enable-cc-mode yes リブート後にユーザにパスフレーズの入力を求めるオプション。

NVEの場合は、を設定します -enable-cc-mode yes`を使用して作成したボリューム `volume create` および volume move start コマンドは自動的に暗号化されます。の場合 volume create`を指定する必要はありません -encrypt true。の場合 volume move start`を指定する必要はありません -encrypt-destination true。



パスフレーズの試行に失敗した場合は、ノードを再起動する必要があります。

## NVE を使用してボリュームデータを暗号化する

### NVE を使用したボリュームデータの暗号化の概要

ONTAP 9.7 以降では、VE ライセンスとオンボードキー管理または外部キー管理を使用している場合、アグリゲートとボリューム暗号化がデフォルトで有効になります。ONTAP 9.6 以前では、新しいボリュームまたは既存のボリュームで暗号化を有効にできます。ボリューム暗号化を有効にする前に、VEライセンスをインストールし、キー管理を有効にしておく必要があります。NVE は FIPS-140-2 レベル 1 に準拠しています。

### VEライセンスでアグリゲートレベルの暗号化を有効にする

ONTAP 9.7以降では、新規に作成したアグリゲートとボリュームがデフォルトで暗号化されます。"VEライセンス" およびオンボードまたは外部のキー管理ONTAP 9.6 以降では、アグリゲートレベルの暗号化を使用して、暗号化するボリュームの包含アグリゲートにキーを割り当てることができます。

### このタスクについて

アグリゲートレベルの重複排除をインラインまたはバックグラウンドで実行する場合は、アグリゲートレベルの暗号化を使用する必要があります。そうしないと、NVE でアグリゲートレベルの重複排除がサポートされません。

アグリゲートレベルの暗号化が有効になっているアグリゲートは、\_NAE アグリゲートと呼ばれます（NetApp Aggregate Encryption の場合）。NAEアグリゲート内のすべてのボリュームは、NAEまたはNVE暗号化を使用して暗号化する必要があります。アグリゲートレベルの暗号化では、アグリゲート内に作成したボリュームはデフォルトでNAE暗号化を使用して暗号化されます。デフォルトの設定を変更して、NVE暗号化を使用することもできます。

NAE アグリゲートではプレーンテキストボリュームがサポートされません。

### 作業を開始する前に

このタスクを実行するには、クラスタ管理者である必要があります。

### 手順

1. アグリゲートレベルの暗号化を有効または無効にします。

目的	使用するコマンド
ONTAP 9.7 以降で NAE アグリゲートを作成します	<code>storage aggregate create -aggregate aggregate_name -node node_name</code>
ONTAP 9.6 で NAE アグリゲートを作成します	<code>storage aggregate create -aggregate aggregate_name -node node_name -encrypt-with -aggr-key true</code>

非 NAE アグリゲートを NAE アグリゲートに変換します	<code>storage aggregate modify -aggregate aggregate_name -node node_name -encrypt-with -aggr-key true</code>
NAE アグリゲートを非 NAE アグリゲートに変換します	<code>storage aggregate modify -aggregate aggregate_name -node node_name -encrypt-with -aggr-key false</code>

コマンド構文全体については、マニュアルページを参照してください。

次のコマンドは、でアグリゲートレベルの暗号化を有効にします `aggr1` :

- ONTAP 9.7 以降

```
cluster1::> storage aggregate create -aggregate aggr1
```

- ONTAP 9.6 以前 :

```
cluster1::> storage aggregate create -aggregate aggr1 -encrypt-with
-aggr-key true
```

## 2. アグリゲートで暗号化が有効になっていることを確認します。

```
storage aggregate show -fields encrypt-with-aggr-key
```

コマンド構文全体については、マニュアルページを参照してください。

次のコマンドは、を確認します `aggr1` 暗号化が有効 :

```
cluster1::> storage aggregate show -fields encrypt-with-aggr-key
aggregate          encrypt-aggr-key
-----
aggr0_vsim4        false
aggr1               true
2 entries were displayed.
```

完了後

を実行します `volume create` コマンドを使用して暗号化ボリュームを作成します。

ノードの暗号化キーを保存するために KMIP サーバを使用している場合、ボリュームを暗号化すると、ONTAP によって暗号化キーがサーバに自動的に「プッシュ」されます。

新しいボリュームで暗号化を有効にします

を使用できます `volume create` コマンドを使用して新しいボリュームで暗号化を有効にします。

このタスクについて

NetApp Volume Encryption (NVE) を使用してボリュームを暗号化できます。また、ONTAP 9.6以降では、NetApp Aggregate Encryption (NAE) を使用できます。NAEおよびNVEの詳細については、を参照してください [ボリューム暗号化の概要](#)。

ONTAP の新しいボリュームで暗号化を有効にする手順 は、使用するONTAP のバージョンと構成によって異なります。

- ONTAP 9.4以降では、を有効にした場合 `cc-mode` オンボードキーマネージャをセットアップする場合は、でボリュームを作成します `volume create` コマンドは、指定したかどうかに関係なく自動的に暗号化されます `-encrypt true`。
- ONTAP 9.6以前のリリースでは、を使用する必要があります `-encrypt true` を使用 `volume create` 暗号化を有効にするコマンド（を有効にしていない場合） `cc-mode`）。
- ONTAP 9.6でNAEボリュームを作成するには、アグリゲートレベルでNAEを有効にする必要があります。を参照してください [VEライセンスでアグリゲートレベルの暗号化を有効にします](#) 詳細については、を参照してください。
- ONTAP 9.7以降では、新規作成したボリュームがデフォルトで暗号化されます。"VEライセンス" および オンボードまたは外部のキー管理デフォルトでは、NAEアグリゲートに作成される新しいボリュームのタイプは、NVEではなくNAEになります。
  - ONTAP 9.7以降のリリースでは、を追加した場合 `-encrypt true` に移動します `volume create` NAEアグリゲート内にボリュームを作成するコマンドは、NAEではなくNVE暗号化を使用します。NAEアグリゲート内のすべてのボリュームは、NVEまたはNAEを使用して暗号化する必要があります。




NAE アグリゲートではプレーンテキストボリュームがサポートされません。

手順

1. 新しいボリュームを作成し、そのボリュームで暗号化を有効にするかどうかを指定します。新しいボリュームがNAEアグリゲートに含まれている場合、デフォルトではボリュームがNAEボリュームになります。

作成対象	使用するコマンド
NAEボリューム	<code>volume create -vserver SVM_name -volume volume_name -aggregate aggregate_name</code>

NVEボリューム	<pre>volume create -vserver SVM_name -volume volume_name -aggregate aggregate_name -encrypt true [+]</pre> <div>  <p>NAEがサポートされないONTAP 9.6以前では、<code>-encrypt true</code> ボリュームをNVEで暗号化するように指定します。NAE アグリゲートでボリュームが作成されるONTAP 9.7以降では、<code>-encrypt true</code> 代わりにデフォルトの暗号化タイプが無効になり、NVEボリュームが作成されます。</p> </div>
プレーンテキストのボリューム	<pre>volume create -vserver SVM_name -volume volume_name -aggregate aggregate_name -encrypt false</pre>

コマンド構文の詳細については、コマンドリファレンスページのリンク：<https://docs.netapp.com/us-en/ontap-cli-9141/volume-create.html>を参照してください。[`volume create`]をクリックします。

## 2. ボリュームで暗号化が有効になっていることを確認します。

```
volume show -is-encrypted true
```

コマンド構文全体については、を参照してください ["コマンドリファレンス"](#)。

## 結果

ノードの暗号化キーの格納にKMIPサーバを使用している場合は、ボリュームを暗号化するとONTAP によって暗号化キーがサーバに自動的に「プッシュ」されます。

```
=
:allow-uri-read:
```

既存のボリュームで暗号化を有効にする

どちらかを使用できます `volume move start` または `volume encryption conversion start` コマンドを使用して、既存のボリュームで暗号化を有効にします。

このタスクについて

- ONTAP 9.3以降では、を使用できます `volume encryption conversion start` 既存のボリュームの暗号化を「インプレース」で有効にするコマンド。ボリュームを別の場所に移動する必要はありません。または、`volume move start` コマンドを実行します
- ONTAP 9.2以前では、`volume move start` コマンドを使用して既存のボリュームを移動して暗号化を有効にします。

**volume encryption conversion start** コマンドを使用して既存のボリュームの暗号化を有効にします

ONTAP 9.3以降では、を使用できます `volume encryption conversion start` 既存のボリュームの暗号化を「インプレース」で有効にするコマンド。ボリュームを別の場所に移動する必要はありません。

変換処理を開始したら、完了する必要があります。処理中にパフォーマンス問題 が発生した場合は、を実行できます `volume encryption conversion pause` 処理を一時停止するコマンド、および `volume`



encryption conversion resume コマンドを実行して処理を再開します。



を使用することはできません volume encryption conversion start SnapLock ボリュームを変換します。

#### 手順

1. 既存のボリュームで暗号化を有効にします。

```
volume encryption conversion start -vserver SVM_name -volume volume_name
```

コマンド構文全体については、コマンドのマニュアルページを参照してください。

次のコマンドは、既存のボリュームで暗号化を有効にします。 vol1 :

```
cluster1::> volume encryption conversion start -vserver vs1 -volume vol1
```

ボリュームの暗号化キーが作成されます。ボリュームのデータが暗号化されます。

2. 変換処理のステータスを確認します。

```
volume encryption conversion show
```

コマンド構文全体については、コマンドのマニュアルページを参照してください。

次のコマンドは、変換処理のステータスを表示します。

```
cluster1::> volume encryption conversion show
```

Vserver	Volume	Start Time	Status
vs1	vol1	9/18/2017 17:51:41	Phase 2 of 2 is in progress.

3. 変換処理が完了したら、ボリュームで暗号化が有効になっていることを確認します。

```
volume show -is-encrypted true
```

コマンド構文全体については、コマンドのマニュアルページを参照してください。

次のコマンドは、の暗号化されたボリュームを表示します cluster1 :

```
cluster1::> volume show -is-encrypted true
```

Vserver	Volume	Aggregate	State	Type	Size	Available	Used
vs1	vol1	aggr2	online	RW	200GB	160.0GB	20%

結果

ノードの暗号化キーを保存するために KMIP サーバを使用している場合、ボリュームを暗号化すると、ONTAP によって暗号化キーがサーバに自動的に「プッシュ」されます。

volume move start コマンドを使用して、既存のボリュームの暗号化を有効にします

使用できます volume move start コマンドを使用して既存のボリュームを移動して暗号化を有効にします。を使用する必要があります volume move start ONTAP 9.2以前では、使用するアグリゲートは同じアグリゲートでも別のアグリゲートでもかまいません。

このタスクについて

- ONTAP 9.8以降では、を使用できます volume move start SnapLock またはFlexGroup ボリュームで暗号化を有効にします。
- ONTAP 9.4以降では、オンボードキーマネージャのセットアップ時に「cc-mode」を有効にすると、を使用してボリュームを作成できます volume move start コマンドは自動的に暗号化されます。指定する必要はありません -encrypt-destination true。
- ONTAP 9.6 以降では、アグリゲートレベルの暗号化を使用して、移動するボリュームの包含アグリゲートにキーを割り当てることができます。一意のキーで暗号化されたボリュームは、\_NVEボリューム\_と呼ばれます（NetAppボリューム暗号化を使用することを意味します）。アグリゲートレベルのキーで暗号化されたボリュームは、\_NAE ボリューム（ NetApp Aggregate Encryption の場合）と呼ばれます。NAE アグリゲートではプレーンテキストボリュームがサポートされません。
- ONTAP 9.14.1以降では、NVEでSVMルートボリュームを暗号化できます。詳細については、を参照してください [SVMルートボリュームでのNetAppボリューム暗号化の設定](#)。

作業を開始する前に

このタスクを実行するには、クラスタ管理者であるか、クラスタ管理者から権限を委譲された SVM 管理者である必要があります。

"volume move コマンドの実行権限の委譲"

手順

1. 既存のボリュームを移動し、そのボリュームで暗号化を有効にするかどうかを指定します。

変換対象	使用するコマンド
プレーンテキストボリュームから NVE ボリューム	<code>volume move start -vserver SVM_name -volume volume_name -destination-aggregate aggregate_name -encrypt-destination true</code>
NVE ボリュームまたはプレーンテキストボリュームから NAE ボリューム（デスティネーションでアグリゲートレベルの暗号化が有効になっている場合）	<code>volume move start -vserver SVM_name -volume volume_name -destination-aggregate aggregate_name -encrypt-with-aggr-key true</code>
NAE ボリュームから NVE ボリューム	<code>volume move start -vserver SVM_name -volume volume_name -destination-aggregate aggregate_name -encrypt-with-aggr-key false</code>

NAE ボリュームからプレーンテキストボリューム	<code>volume move start -vserver SVM_name -volume volume_name -destination-aggregate aggregate_name -encrypt-destination false -encrypt-with-aggr-key false</code>
NVEボリュームからプレーンテキストボリューム	<code>volume move start -vserver SVM_name -volume volume_name -destination-aggregate aggregate_name -encrypt-destination false</code>

コマンド構文全体については、コマンドのマニュアルページを参照してください。

次のコマンドは、という名前のプレーンテキストボリュームを変換します vol1 NVEボリュームへの移動：

```
cluster1::> volume move start -vserver vs1 -volume vol1 -destination
-aggregate aggr2 -encrypt-destination true
```

次のコマンドは、デスティネーションでアグリゲートレベルの暗号化が有効になっている場合に、という名前のNVEボリュームまたはプレーンテキストボリュームを変換します vol1 NAEボリュームへ：

```
cluster1::> volume move start -vserver vs1 -volume vol1 -destination
-aggregate aggr2 -encrypt-with-aggr-key true
```

次のコマンドは、という名前のNAEボリュームを変換します vol2 NVEボリュームへの移動：

```
cluster1::> volume move start -vserver vs1 -volume vol2 -destination
-aggregate aggr2 -encrypt-with-aggr-key false
```

次のコマンドは、という名前のNAEボリュームを変換します vol2 プレーンテキストボリュームへ：

```
cluster1::> volume move start -vserver vs1 -volume vol2 -destination
-aggregate aggr2 -encrypt-destination false -encrypt-with-aggr-key false
```

次のコマンドは、次の名前のNVEボリュームを変換します。 vol2 プレーンテキストボリュームへ：

```
cluster1::> volume move start -vserver vs1 -volume vol2 -destination
-aggregate aggr2 -encrypt-destination false
```

## 2. クラスタボリュームの暗号化タイプを表示します。

```
volume show -fields encryption-type none|volume|aggregate
```

。 encryption-type フィールドはONTAP 9.6以降で使用できます。

コマンド構文全体については、コマンドのマニュアルページを参照してください。

次のコマンドは、のボリュームの暗号化タイプを表示します cluster2：

```
cluster2::> volume show -fields encryption-type
```

vserver	volume	encryption-type
-----	-----	-----
vs1	vol1	none
vs2	vol2	volume
vs3	vol3	aggregate

3. ボリュームで暗号化が有効になっていることを確認します。

```
volume show -is-encrypted true
```

コマンド構文全体については、コマンドのマニュアルページを参照してください。

次のコマンドは、の暗号化されたボリュームを表示します cluster2：

```
cluster2::> volume show -is-encrypted true
```

Vserver	Volume	Aggregate	State	Type	Size	Available	Used
-----	-----	-----	-----	-----	-----	-----	-----
vs1	vol1	aggr2	online	RW	200GB	160.0GB	20%

## 結果

ノードの暗号化キーの格納にKMIPサーバを使用している場合、ボリュームの暗号化時にONTAPからサーバに暗号化キーが自動的にプッシュされます。

## SVMルートボリュームでのNetAppボリューム暗号化の設定

ONTAP 9.14.1以降では、Storage VM（SVM）のルートボリュームでNetApp Volume Encryption（NVE）を有効にすることができます。NVEでは、ルートボリュームが一意的なキーで暗号化されるため、SVMのセキュリティが向上します。

### このタスクについて

SVMルートボリューム上のNVEは、SVMの作成後にのみ有効にできます。

### 作業を開始する前に

- NetAppアグリゲート暗号化（NAE）で暗号化されたアグリゲートにSVMルートボリュームを配置しないでください。
- オンボードキーマネージャまたは外部キーマネージャを使用した暗号化を有効にしておく必要があります。

す。

- ONTAP 9.14.1以降が実行されている必要があります。
- NVEで暗号化されたルートボリュームを含むSVMを移行するには、移行の完了後にSVMルートボリュームをプレーンテキストボリュームに変換し、SVMルートボリュームを再暗号化する必要があります。
  - SVM移行のデスティネーションアグリゲートでNAEを使用する場合、ルートボリュームはデフォルトでNAEを継承します。
- SVMがSVMディザスタリカバリ関係にある場合は、次の手順を実行します。
  - ミラーされたSVMの暗号化設定はデスティネーションにコピーされません。ソースまたはデスティネーションでNVEを有効にする場合は、ミラーされたSVMルートボリュームでNVEを個別に有効にする必要があります。
  - デスティネーションクラスタ内のすべてのアグリゲートがNAEを使用する場合、SVMルートボリュームはNAEを使用します。

## 手順

ONTAP CLIまたはSystem Managerを使用して、SVMルートボリュームでNVEを有効にできます。

### CLI の使用

NVEは、SVMルートボリュームでインプレースで有効にすることも、アグリゲート間でボリュームを移動することによって有効にすることもできます。

ルートボリュームをインプレースで暗号化

1. ルートボリュームを暗号化されたボリュームに変換します。

```
volume encryption conversion start -vserver svm_name -volume volume
```

2. 暗号化が成功したことを確認します。 `volume show -encryption-type volume` NVEを使用しているすべてのボリュームのリストを表示します。

### SVMルートボリュームの移動による暗号化


1. ボリュームの移動を開始します。

```
volume move start -vserver svm_name -volume volume -destination-aggregate aggregate -encrypt-with-aggr-key false -encrypt-destination true
```

詳細情報 `volume move` を参照してください [ボリュームを移動する](#)。

2. を確認します。 `volume move` で操作が成功しました `volume move show` コマンドを実行します。 `volume show -encryption-type volume` NVEを使用しているすべてのボリュームのリストを表示します。

### System Manager の略

1. ストレージ>ボリュームに移動します。
2. 暗号化するSVMルートボリュームの名前の横にあるを選択します。  次に、編集を実行します。
3. [ **Storage and Optimization\*** ]見出しで、[ **Enable encryption\*** ]を選択します。
4. 保存を選択します。

ノードのルートボリューム暗号化を有効にします

ONTAP 9.8 以降では、ネットアップのボリューム暗号化を使用してノードのルートボリュームを保護できます。



このタスクについて

この手順環境はノードのルートボリュームを表します。SVM のルートボリュームには適用されません。SVMルートボリュームは、アグリゲートレベルの暗号化で保護できます。 [ONTAP 9.14.1以降、NVE](#)。

ルートボリュームの暗号化を開始したら、暗号化を完了する必要があります。処理を一時停止することはできません。暗号化が完了すると、ルートボリュームに新しいキーを割り当てることができなくなり、セキュアページ処理を実行することもできなくなります。

作業を開始する前に

- システムで HA 構成を使用している必要があります。
- ノードのルートボリュームを作成しておく必要があります。
- システムに、Key Management Interoperability Protocol (KMIP) を使用したオンボードキーマネージャまたは外部キー管理サーバが必要です。

手順

1. ルートボリュームを暗号化します。

```
volume encryption conversion start -vserver SVM_name -volume root_vol_name
```

2. 変換処理のステータスを確認します。

```
volume encryption conversion show
```

3. 変換処理が完了したら、ボリュームが暗号化されていることを確認します。

```
volume show -fields
```

次の例は、暗号化されたボリュームの出力を示しています。

```
::> volume show -vserver xyz -volume vol0 -fields is-encrypted
vserver      volume is-encrypted
-----
xyz          vol0    true
```

## ネットアップのハードウェアベースの暗号化を設定

ネットアップのハードウェアベースの暗号化の概要を設定

ネットアップのハードウェアベースの暗号化は、データ書き込み時の Full Disk Encryption (FDE) をサポートします。ファームウェアに格納された暗号化キーがない

とデータを読み取ることはできません。暗号化キーには認証されたノードからしかアクセスできません。

ネットアップのハードウェアベースの暗号化について理解する

ノードは、外部キー管理サーバまたはオンボードキーマネージャから取得した認証キーを使用して自己暗号化ドライブへの認証を行います。

- 外部キー管理サーバはストレージ環境に配置されたサードパーティのシステムで、Key Management Interoperability Protocol (KMIP) を使用してノードにキーを提供します。外部キー管理サーバは、データとは別のストレージシステムで設定することを推奨します。
- オンボードキーマネージャは組み込みのツールで、データと同じストレージシステムからノードに認証キーを提供します。

NetApp Volume Encryption をハードウェアベースの暗号化とともに使用すると、自己暗号化ドライブのデータを「暗号化」できます。

自己暗号化ドライブが有効な場合は、コアダンプも暗号化されます。



HA ペアが SAS ドライブまたは NVMe ドライブ (SED、NSE、FIPS) の暗号化を使用している場合は、トピックの手順に従う必要があります [FIPS ドライブまたは SED を非保護モードに戻します](#) システムを初期化する前の HA ペア内のすべてのドライブ (ブートオプション 4 または 9)。そうしないと、ドライブを転用した場合にデータが失われる可能性があります。

サポートされている自己暗号化ドライブのタイプ

2種類の自己暗号化ドライブがサポートされています。

- すべての FAS システムおよび AFF システムで、自己暗号化機能を備えた FIPS 認定の SAS ドライブまたは NVMe ドライブがサポートされます。これらのドライブは [FIPS ドライブ](#) と呼ばれ、Federal Information Processing Standard Publication 140-2 レベル 2 の要件に準拠しています。認定された機能により、ドライブに対する DoS 攻撃を防止するなど、暗号化に加えて保護が可能になります。FIPS ドライブは、同じノードまたは HA ペアで他のタイプのドライブと混在させることはできません。
- ONTAP 9.6以降では、AFF A800、A320、およびそれ以降のシステムで、FIPSのテストを実施していない自己暗号化NVMeドライブがサポートされます。これらのドライブは [SED](#) と呼ばれ、FIPSドライブと同じ暗号化機能を提供しますが、同じノードまたはHAペアで非暗号化ドライブと混在させることもできます。
- すべてのFIPS検証済みドライブは、FIPS検証に合格したファームウェア暗号化モジュールを使用します。FIPSドライブ暗号化モジュールは、ドライブの外部で生成されたキーを使用しません (ドライブに入力された認証パスフレーズは、ドライブのファームウェア暗号化モジュールでキー暗号化キーの取得に使用されます)。



非暗号化ドライブとは、SEDやFIPSドライブではないドライブです。



Flash Cacheモジュールを搭載したシステムでNSEを使用する場合は、NVEまたはNAEも有効にする必要があります。NSEは、Flash Cacheモジュール上のデータを暗号化しません。

オンボードキーマネージャを使用した方がコストもかからず一般的には便利ですが、次のいずれかに当てはまる場合は外部キー管理を使用することを推奨します。

- 組織のポリシーには、FIPS 140-2レベル2以上の暗号化モジュールを使用するキー管理解決策 が必要です。
- 暗号化キーを一元管理するマルチクラスタ解決策が必要です。
- 認証キーをデータとは別のシステムや場所に格納してセキュリティを強化する必要がある場合。

#### サポートの詳細

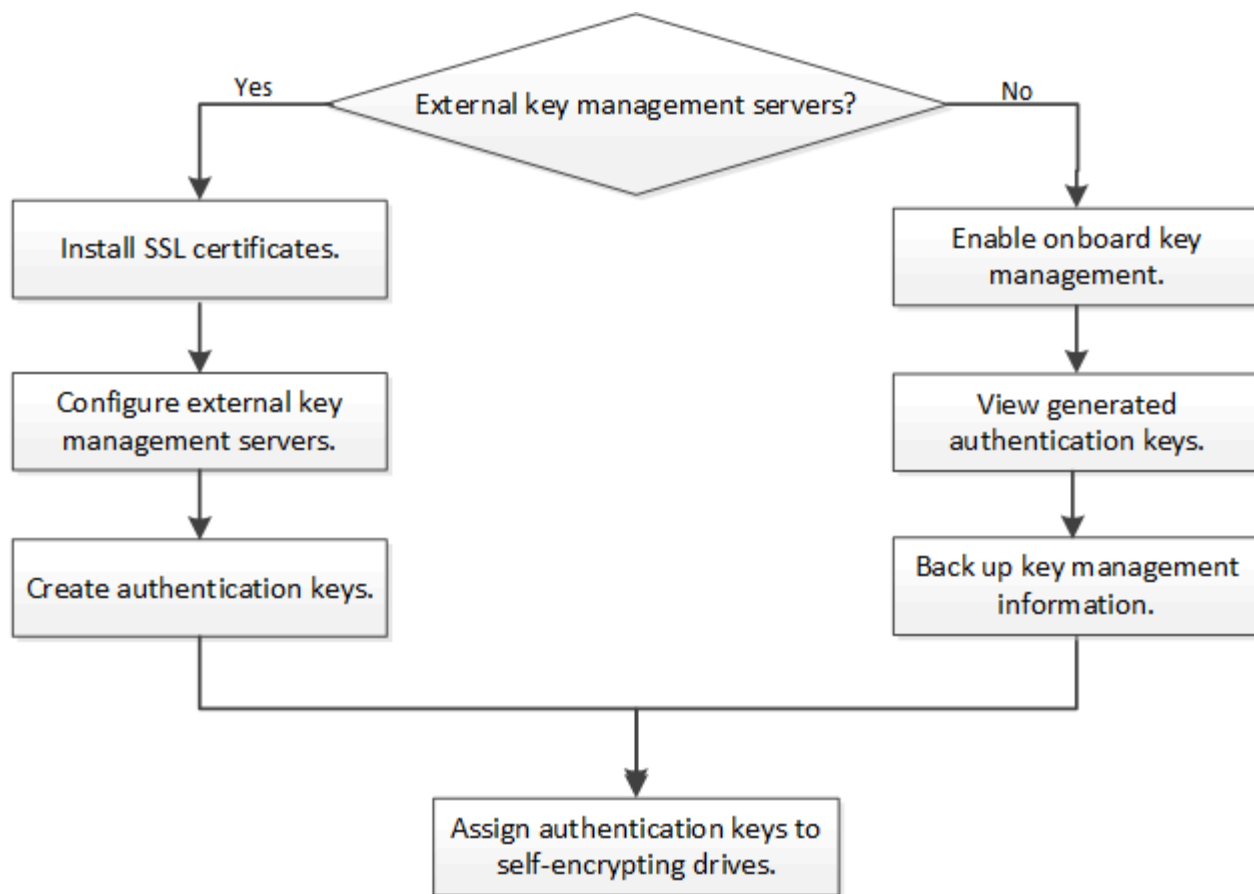
次の表に、重要なハードウェア暗号化のサポートの詳細を示します。サポートされている KMIP サーバ、ストレージシステム、ディスクシェルフの最新情報については、Interoperability Matrix を参照してください。

リソースまたは機能	サポートの詳細
異なるタイプのディスクの混在	<ul style="list-style-type: none"> <li>• FIPS ドライブは、同じノードまたは HA ペアで他のタイプのドライブと混在させることはできません。準拠した HA ペアと準拠していない HA ペアを同じクラスタに共存させることは可能です。</li> <li>• SEDは、同じノードまたはHAペアで暗号化されていないドライブと混在させることができます。</li> </ul>
ドライブタイプ	<ul style="list-style-type: none"> <li>• FIPS ドライブには、SAS ドライブまたは NVMe ドライブを使用できます。</li> <li>• SED は NVMe ドライブである必要があります。</li> </ul>
10Gb ネットワークインターフェイス	ONTAP 9.3 以降では、KMIP を使用したキー管理の設定で外部キー管理サーバとの通信に 10Gb ネットワークインターフェイスがサポートされます。
キー管理サーバとの通信に使用するポートを指定します	ONTAP 9.3 以降では、任意のストレージコントローラポートを使用してキー管理サーバと通信できます。それ以外の場合は、キー管理サーバとの通信にポートe0mを使用する必要があります。ストレージコントローラのモデルによっては、ブートプロセス時に一部のネットワークインターフェイスをキー管理サーバとの通信に使用できない場合があります。
MetroCluster （MCC）	<ul style="list-style-type: none"> <li>• NVMe ドライブでは MCC がサポートされます。</li> <li>• SAS ドライブでは MCC がサポートされません。</li> </ul>

#### ハードウェアベースの暗号化のワークフロー

自己暗号化ドライブに対してクラスタを認証するには、キー管理サービスを設定する必要があります。外部キー管理サーバまたはオンボードキーマネージャを使用できます。





#### 関連情報

- ["NetApp Hardware Universe の略"](#)
- ["NetApp Volume Encryption および NetApp Aggregate Encryption の略"](#)

#### 外部キー管理を設定

##### 外部キー管理の概要の設定

1 つ以上の外部キー管理サーバを使用して、暗号化されたデータにアクセスする際にクラスタで使用するキーを安全に保管できます。外部キー管理サーバはストレージ環境に配置されたサードパーティのシステムで、Key Management Interoperability Protocol（KMIP）を使用してノードにキーを提供します。

ONTAP 9.1 以前のバージョンでは、外部キー管理ツールを使用する前に、ノード管理ロールが設定されたポートにノード管理 LIF を割り当てる必要があります。

ONTAP 9.1 以降では、オンボードキーマネージャを使用して NetApp Volume Encryption（NVE）を実装できます。ONTAP 9.3 以降では、NVE を外部キー管理（KMIP）およびオンボードキーマネージャとともに実装できます。ONTAP 9.11.1以降では、1つのクラスタに複数の外部キー管理ツールを設定できます。を参照してください [クラスタ化されたキーサーバを設定](#)

##### ONTAP 9.2 以前でネットワーク情報を収集

ONTAP 9.2 以前を使用している場合は、外部キー管理を有効にする前にネットワーク設

定ワークシートに情報を記入してください。



ONTAP 9.3 以降では、必要なすべてのネットワーク情報が自動的に検出されます。

項目	注：	価値
キー管理ネットワークインターフェイスの名前		
キー管理ネットワークインターフェイスの IP アドレス	ノード管理 LIF の IPv4 形式または IPv6 形式の IP アドレス	
キー管理ネットワークインターフェイスの IPv6 ネットワークプレフィックス長	IPv6 を使用している場合、IPv6 ネットワークプレフィックス長	
キー管理ネットワークインターフェイスのサブネットマスク		
キー管理ネットワークインターフェイスのゲートウェイの IP アドレス		
クラスタネットワークインターフェイスの IPv6 アドレス	キー管理ネットワークインターフェイスに IPv6 を使用している場合にのみ必要です	
各 KMIP サーバのポート番号	任意。すべての KMIP サーバで同じポート番号を使用してください。ポート番号を指定しなかった場合は、デフォルトでポート 5696 が使用されます。これは、Internet Assigned Numbers Authority (IANA) が KMIP に割り当てているポートです。	
キータグ名	任意。キータグ名は、ノードに属するすべてのキーを識別するために使用されます。デフォルトのキータグ名はノード名です。	

#### 関連情報

"[ネットアップテクニカルレポート 3954](#) : 『[NetApp Storage Encryption Preinstallation Requirements and Procedures for IBM Tivoli Lifetime Key Manager](#)』"

"[ネットアップテクニカルレポート 4074](#) : 『[NetApp Storage Encryption Preinstallation Requirements and Procedures for SafeNet KeySecure](#)』"

クラスタに **SSL** 証明書をインストールします

クラスタと KMIP サーバの間では、相互の ID を検証して SSL 接続を確立するために KMIP SSL 証明書を使用します。KMIP サーバとの SSL 接続を設定する前に、クラスタの KMIP クライアント SSL 証明書、および KMIP サーバのルート Certificate Authority（CA；認証局）の SSL パブリック証明書をインストールする必要があります。

このタスクについて

HA ペア構成では、両方のノードで同じ SSL KMIP パブリック証明書とプライベート証明書を使用する必要があります。複数の HA ペアを同じ KMIP サーバに接続する場合は、HA ペアのすべてのノードで同じ SSL KMIP パブリック証明書とプライベート証明書を使用する必要があります。

作業を開始する前に

- 証明書を作成するサーバ、KMIP サーバ、およびクラスタの時刻が同期されている必要があります。
- クラスタのパブリック SSL KMIP クライアント証明書を入手しておく必要があります。
- クラスタの SSL KMIP クライアント証明書に関連付けられた秘密鍵を入手しておく必要があります。
- SSL KMIP クライアント証明書は、パスワードで保護しないでください。
- KMIP サーバのルート認証局（CA）の SSL パブリック証明書を入手しておく必要があります。
- MetroCluster環境では、両方のクラスタに同じKMIP SSL証明書をインストールする必要があります。



KMIP サーバへのクライアント証明書とサーバ証明書のインストールは、クラスタに証明書をインストールする前でもインストールしたあとでもかまいません。

手順

1. クラスタに SSL KMIP クライアント証明書をインストールします。

```
security certificate install -vserver admin_svm_name -type client
```

SSL KMIP パブリック証明書とプライベート証明書を入力するように求められます。

```
cluster1::> security certificate install -vserver cluster1 -type client
```

2. KMIP サーバのルート認証局（CA）の SSL パブリック証明書をインストールします。

```
security certificate install -vserver admin_svm_name -type server-ca
```

```
cluster1::> security certificate install -vserver cluster1 -type server-ca
```

**ONTAP 9.6** 以降で外部キー管理を有効にする（ハードウェアベース）

1 つ以上の KMIP サーバを使用して、暗号化されたデータにアクセスする際にクラスタで使用するキーを安全に保管できます。1 つのノードに最大 4 つの KMIP サーバを接続できます。冗長性とディザスタリカバリのために、少なくとも 2 台のサーバを使用することを推奨します。

ONTAP 9.11.1以降では、プライマリキーサーバごとに最大3つのセカンダリキーサーバを追加して、クラスタ化されたキーサーバを作成できます。詳細については、を参照してください [クラスタ構成の外部キーサーバ](#)

を構成。

作業を開始する前に

- KMIP SSL クライアント証明書とサーバ証明書をインストールしておく必要があります。
- このタスクを実行するには、クラスタ管理者である必要があります。
- 外部キー管理ツールを設定する前に、MetroCluster 環境を設定する必要があります。
- MetroCluster 環境では、両方のクラスタにKMIP SSL証明書をインストールする必要があります。

手順

1. クラスタのキー管理ツールの接続を設定します。

```
security key-manager external enable -vserver admin_SVM -key-servers  
host_name|IP_address:port,... -client-cert client_certificate -server-ca-cert  
server_CA_certificates
```



- security key-manager external enable コマンドは、に置き換わるものです security key-manager setup コマンドを実行しますを実行できます security key-manager external modify コマンドを使用して、外部キー管理の設定を変更します。コマンド構文全体については、マニュアルページを参照してください。
- MetroCluster 環境で管理SVMに外部キー管理を設定する場合は、を繰り返す必要があります security key-manager external enable パートナークラスタに対して実行します。

次のコマンドは、の外部キー管理を有効にします cluster1 3つの外部キーサーバで構成されます。最初のキーサーバはホスト名とポートで指定し、2番目のキーサーバはIPアドレスとデフォルトポートで指定し、3番目のキーサーバはIPv6アドレスとポートで指定します。

```
cluster1::> security key-manager external enable -key-servers  
ks1.local:15696,10.0.0.10,[fd20:8b1e:b255:814e:32bd:f35c:832c:5a09]:1234  
-client-cert AdminVserverClientCert -server-ca-certs  
AdminVserverServerCaCert
```

2. 設定したすべての KMIP サーバが接続されていることを確認します。

```
security key-manager external show-status -node node_name -vserver SVM -key  
-server host_name|IP_address:port -key-server-status available|not-  
responding|unknown
```



- security key-manager external show-status コマンドは、に置き換わるものです security key-manager show -status コマンドを実行しますコマンド構文全体については、マニュアルページを参照してください。

```
cluster1::> security key-manager external show-status
```

Node	Vserver	Key Server	Status
-----			
node1			
	cluster1	10.0.0.10:5696	available
		fd20:8b1e:b255:814e:32bd:f35c:832c:5a09:1234	available
		ks1.local:15696	available
node2			
	cluster1	10.0.0.10:5696	available
		fd20:8b1e:b255:814e:32bd:f35c:832c:5a09:1234	available
		ks1.local:15696	available

```
6 entries were displayed.
```

#### ONTAP 9.5 以前で外部キー管理を有効にします

1 つ以上の KMIP サーバを使用して、暗号化されたデータにアクセスする際にクラスターで使用するキーを安全に保管できます。1 つのノードに最大 4 つの KMIP サーバを接続できます。冗長性とディザスタリカバリのために、少なくとも 2 台のサーバを使用することを推奨します。

このタスクについて

ONTAP は、クラスター内のすべてのノードについて KMIP サーバの接続を設定します。

作業を開始する前に

- KMIP SSL クライアント証明書とサーバ証明書をインストールしておく必要があります。
- このタスクを実行するには、クラスタ管理者である必要があります。
- 外部キー管理ツールを設定する前に、MetroCluster 環境を設定する必要があります。
- MetroCluster 環境では、両方のクラスターに KMIP SSL 証明書をインストールする必要があります。

手順

1. クラスターノードのキー管理ツールの接続を設定します。

```
security key-manager setup
```

キー管理ツールのセットアップが開始されます。



MetroCluster 環境では、このコマンドを両方のクラスターで実行する必要があります。

2. 各プロンプトで適切な応答を入力します。

### 3. KMIP サーバを追加します。

```
security key-manager add -address key_management_server_ipaddress
```



MetroCluster 環境では、このコマンドを両方のクラスタで実行する必要があります。

### 4. 冗長性を確保するために KMIP サーバをもう 1 つ追加します。

```
security key-manager add -address key_management_server_ipaddress
```



MetroCluster 環境では、このコマンドを両方のクラスタで実行する必要があります。

### 5. 設定したすべての KMIP サーバが接続されていることを確認します。

```
security key-manager show -status
```

コマンド構文全体については、マニュアルページを参照してください。

```
cluster1::> security key-manager show -status
```

Node	Port	Registered Key Manager	Status
-----	----	-----	-----
cluster1-01	5696	20.1.1.1	available
cluster1-01	5696	20.1.1.2	available
cluster1-02	5696	20.1.1.1	available
cluster1-02	5696	20.1.1.2	available

### 6. 必要に応じて、プレーンテキストボリュームを暗号化ボリュームに変換します。

```
volume encryption conversion start
```

ボリュームを変換する前に、外部キー管理ツールの設定をすべて完了しておく必要があります。MetroCluster環境では、両方のサイトに外部キー管理ツールを設定する必要があります。

クラスタ構成の外部キーサーバを構成

ONTAP 9.11.1以降では、SVM上のクラスタ化された外部キー管理サーバへの接続を設定できます。クラスタ化されたキーサーバを使用すると、SVMのプライマリキーサーバとセカンダリキーサーバを指定できます。キーを登録すると、ONTAP は、処理が正常に完了するまで、プライマリキーサーバへのアクセスを順次試行する前に、キーの重複を防

止します。

外部キーサーバは、NSE、NVE、NAE、およびSEDのキーに使用できます。SVMでは、最大4つのプライマリ外部KMIPサーバをサポートできます。各プライマリサーバは、最大3つのセカンダリキーサーバをサポートできます。

作業を開始する前に

- "SVMでKMIPキー管理が有効になっている必要があります。"。
- このプロセスでサポートされるのは、KMIPを使用するキーサーバのみです。サポートされているキーサーバの一覧については、を参照してください ["NetApp Interoperability Matrix Tool で確認できます"](#)。
- クラスタ内のすべてのノードでONTAP 9.11.1以降が実行されている必要があります。
- サーバの順序は、で引数をリストします `-secondary-key-servers` パラメータには、外部キー管理 (KMIP) サーバのアクセス順序が反映されます。

クラスタ化されたキーサーバを作成します

設定手順 は、プライマリキーサーバを設定したかどうかによって異なります。

#### SVMにプライマリキーサーバとセカンダリキーサーバを追加する

1. クラスタでキー管理が有効になっていないことを確認します。  
`security key-manager external show -vserver svm_name`  
SVMですでに最大4つのプライマリキーサーバが有効になっている場合は、新しいプライマリキーサーバを追加する前に既存のプライマリキーサーバの1つを削除する必要があります。
2. プライマリキー管理ツールを有効にします。  
`security key-manager external enable -vserver svm_name -key-servers  
server_ip -client-cert client_cert_name -server-ca-certs  
server_ca_cert_names`
3. プライマリキーサーバを変更してセカンダリキーサーバを追加します。。 `-secondary-key-servers` パラメータには、最大3つのキーサーバをカンマで区切って指定できます。  
`security key-manager external modify-server -vserver svm_name -key-servers  
primary_key_server -secondary-key-servers list_of_key_servers`

#### 既存のプライマリキーサーバにセカンダリキーサーバを追加する

1. プライマリキーサーバを変更してセカンダリキーサーバを追加します。。 `-secondary-key-servers` パラメータには、最大3つのキーサーバをカンマで区切って指定できます。  
`security key-manager external modify-server -vserver svm_name -key-servers  
primary_key_server -secondary-key-servers list_of_key_servers`  
セカンダリキーサーバの詳細については、を参照してください [\[mod-secondary\]](#)。

クラスタ化されたキーサーバを変更

外部キーサーバクラスタの変更では、特定のキーサーバのステータス（プライマリまたはセカンダリ）を変更したり、セカンダリキーサーバを追加および削除したり、セカンダリキーサーバのアクセス順序を変更したりできます。



## プライマリキーサーバとセカンダリキーサーバの変換

プライマリキーサーバをセカンダリキーサーバに変換するには、まずを使用してSVMからプライマリキーサーバを削除する必要があります `security key-manager external remove-servers` コマンドを実行します

セカンダリキーサーバをプライマリキーサーバに変換するには、まず既存のプライマリキーサーバからセカンダリキーサーバを削除する必要があります。を参照してください [\[mod-secondary\]](#)。既存のキーの削除中にセカンダリキーサーバをプライマリサーバに変換する場合、削除および変換を実行する前に新しいサーバを追加しようとする、キーが重複する可能性があります。

セカンダリキーサーバを変更します。

セカンダリキーサーバの管理はで行います `-secondary-key-servers` のパラメータ `security key-manager external modify-server` コマンドを実行します。 `-secondary-key-servers` パラメータにはカンマで区切ったリストを指定できます。リスト内で指定されたセカンダリキーサーバの順序によって、セカンダリキーサーバのアクセスシーケンスが決まります。アクセス順序は、コマンドを実行して変更できます `security key-manager external modify-server` セカンダリキーサーバを別の順序で入力します。

セカンダリキーサーバを削除するには、を実行します `-secondary-key-servers` 引数には、削除するキーサーバを省略して保持するキーサーバを指定する必要があります。すべてのセカンダリキーサーバを削除するには、引数を使用します - 「なし」を意味します。

追加情報 の場合は、を参照してください `security key-manager external` ページのを参照してください ["ONTAP コマンドリファレンス"](#)。

### ONTAP 9.6 以降で認証キーを作成します

を使用できます `security key-manager key create` コマンドを使用してノードの認証キーを作成し、設定したKMIPサーバに格納します。

このタスクについて

セキュリティの設定によりデータ認証と FIPS 140-2 認証に異なるキーを使用する必要がある場合は、それぞれの認証用のキーを作成する必要があります。そうでない場合は、FIPSへの準拠にデータアクセスと同じ認証キーを使用できます。

ONTAP では、クラスタ内のすべてのノードに対して認証キーが作成されます。

- このコマンドは、オンボードキーマネージャが有効になっている場合はサポートされません。ただし、オンボードキーマネージャを有効にすると、2つの認証キーが自動的に作成されます。キーを表示するには、次のコマンドを使用します。

```
security key-manager key query -key-type NSE-AK
```

- 設定済みのキー管理サーバにすでに 128 個を超える認証キーが格納されている場合は警告が表示されます。
- を使用できます `security key-manager key delete` 使用されていないキーを削除するコマンド。。 `security key-manager key delete` 指定したキーがONTAP で現在使用されている場合、コマンドは失敗します。(このコマンドを使用するには 'admin より大きい特権が必要です)





MetroCluster 環境でキーを削除する前に、キーがパートナークラスタで使用されていないことを確認する必要があります。パートナークラスタで次のコマンドを使用して、キーが使用されていないことを確認できます。

- ° `storage encryption disk show -data-key-id key-id`
- ° `storage encryption disk show -fips-key-id key-id`

作業を開始する前に

このタスクを実行するには、クラスタ管理者である必要があります。

手順

1. クラスタノードの認証キーを作成します。

```
security key-manager key create -key-tag passphrase_label -prompt-for-key  
true|false
```



設定 `prompt-for-key=true` 暗号化されたドライブを認証するときに、クラスタ管理者に使用するパスフレーズの入力を求めるプロンプトが表示されます。設定しない場合は、32 バイトのパスフレーズが自動的に生成されます。° `security key-manager key create` コマンドは、に置き換わるものです `security key-manager create-key` コマンドを実行しますコマンド構文全体については、マニュアルページを参照してください。

次の例は、の認証キーを作成します `cluster1` では、32 バイトのパスフレーズが自動的に生成されます。

```
cluster1::> security key-manager key create  
Key ID:  
000000000000000000002000000000001006268333f870860128fbe17d393e5083b00000000  
00000000
```

2. 認証キーが作成されたことを確認します。

```
security key-manager key query -node node
```



° `security key-manager key query` コマンドは、に置き換わるものです `security key-manager query key` コマンドを実行しますコマンド構文全体については、マニュアルページを参照してください。出力に表示されるキー ID は、認証キーを参照するために使用される識別子です。実際の認証キーまたはデータ暗号化キーではありません。

次の例は、の認証キーが作成されたことを確認します `cluster1` :

```
cluster1::> security key-manager key query
      Vserver: cluster1
      Key Manager: external
      Node: node1
```

Key Tag	Key Type	Restored
node1	NSE-AK	yes
Key ID: 000000000000000000002000000000001000c11b3863f78c2273343d7ec5a67762e00000000 00000000		
node1	NSE-AK	yes
Key ID: 000000000000000000002000000000001006f4e2513353a674305872a4c9f3bf79700000000 00000000		

```
      Vserver: cluster1
      Key Manager: external
      Node: node2
```

Key Tag	Key Type	Restored
node2	NSE-AK	yes
Key ID: 000000000000000000002000000000001000c11b3863f78c2273343d7ec5a67762e00000000 00000000		
node2	NSE-AK	yes
Key ID: 000000000000000000002000000000001006f4e2513353a674305872a4c9f3bf79700000000 00000000		

#### ONTAP 9.5 以前で認証キーを作成します

使用できます security key-manager create-key コマンドを使用してノードの認証キーを作成し、設定したKMIPサーバに格納します。

このタスクについて

セキュリティの設定によりデータ認証と FIPS 140-2 認証に異なるキーを使用する必要がある場合は、それぞれの認証用のキーを作成する必要があります。そうでない場合は、FIPS 準拠の認証キーをデータアクセスにも使用できます。

ONTAP では、クラスタ内のすべてのノードに対して認証キーが作成されます。

- このコマンドは、オンボードキー管理が有効な場合はサポートされません。
- 設定済みのキー管理サーバにすでに 128 個を超える認証キーが格納されている場合は警告が表示されま

す。

キー管理サーバソフトウェアを使用して未使用のキーを削除し、もう一度コマンドを実行できます。

作業を開始する前に

このタスクを実行するには、クラスタ管理者である必要があります。

手順

1. クラスタノードの認証キーを作成します。

```
security key-manager create-key
```

コマンド構文全体については、コマンドのマニュアルページを参照してください。



出力に表示されるキー ID は、認証キーを参照するために使用される識別子です。実際の認証キーまたはデータ暗号化キーではありません。

次の例は、の認証キーを作成します cluster1：

```
cluster1::> security key-manager create-key
(security key-manager create-key)
Verifying requirements...

Node: cluster1-01
Creating authentication key...
Authentication key creation successful.
Key ID: F1CB30AFF1CB30B0010100000000000A68B167F92DD54196297159B5968923C

Node: cluster1-01
Key manager restore operation initialized.
Successfully restored key information.

Node: cluster1-02
Key manager restore operation initialized.
Successfully restored key information.
```

2. 認証キーが作成されたことを確認します。

```
security key-manager query
```

コマンド構文全体については、マニュアルページを参照してください。

次の例は、の認証キーが作成されたことを確認します cluster1：

```
cluster1::> security key-manager query

(security key-manager query)

      Node: cluster1-01
    Key Manager: 20.1.1.1
  Server Status: available

Key Tag          Key Type  Restored
-----
cluster1-01      NSE-AK    yes
    Key ID:
F1CB30AFF1CB30B00101000000000000A68B167F92DD54196297159B5968923C

      Node: cluster1-02
    Key Manager: 20.1.1.1
  Server Status: available

Key Tag          Key Type  Restored
-----
cluster1-02      NSE-AK    yes
    Key ID:
F1CB30AFF1CB30B00101000000000000A68B167F92DD54196297159B5968923C
```

**FIPS** ドライブまたは **SED** にデータ認証キーを割り当てる（外部キー管理）

を使用できます `storage encryption disk modify` コマンドを使用してFIPSドライブまたはSEDにデータ認証キーを割り当てることができます。このキーは、クラスタノードでドライブ上の暗号化されたデータをロックまたはロック解除する際に使用します。

このタスクについて

自己暗号化ドライブの認証キー ID がデフォルト以外の値に設定されている場合にのみ、不正アクセスから保護されます。Manufacturer Secure ID（MSID；メーカーのセキュアID）のキーIDが0x0になり、SASドライブの標準のデフォルト値になります。NVMeドライブの場合、標準のデフォルト値はnullキーで、空のキーIDとして表されます。キーIDを自己暗号化ドライブに割り当てると、認証キーIDがデフォルト以外の値に変更されます。

この手順はシステムの停止を伴いません。

作業を開始する前に

このタスクを実行するには、クラスタ管理者である必要があります。

手順

1. FIPS ドライブまたは SED にデータ認証キーを割り当てます。

```
storage encryption disk modify -disk disk_ID -data-key-id key_ID
```

コマンド構文全体については、コマンドのマニュアルページを参照してください。



を使用できます `security key-manager query -key-type NSE-AK` キーIDを表示するコマンド。

```
cluster1::> storage encryption disk modify -disk 0.10.* -data-key-id
F1CB30AFF1CB30B00101000000000000A68B167F92DD54196297159B5968923C
```

```
Info: Starting modify on 14 disks.
      View the status of the operation by using the
      storage encryption disk show-status command.
```

## 2. 認証キーが割り当てられたことを確認します。

```
storage encryption disk show
```

コマンド構文全体については、マニュアルページを参照してください。

```
cluster1::> storage encryption disk show
Disk      Mode Data Key ID
-----
-----
0.0.0     data
F1CB30AFF1CB30B0010100000000000A68B167F92DD54196297159B5968923C
0.0.1     data
F1CB30AFF1CB30B0010100000000000A68B167F92DD54196297159B5968923C
[...]
```

## オンボードキー管理を設定

**ONTAP 9.6** 以降ではオンボードキー管理を有効にしてください

オンボードキーマネージャを使用して、クラスタノードを FIPS ドライブまたは SED に対して認証できます。オンボードキーマネージャは組み込みのツールで、データと同じストレージシステムからノードに認証キーを提供します。オンボードキーマネージャは FIPS-140-2 レベル 1 に準拠しています。

オンボードキーマネージャを使用して、暗号化されたデータにアクセスする際にクラスタで使用するキーを安全に保管できます。オンボードキーマネージャは、暗号化されたボリュームや自己暗号化ディスクにアクセスする各クラスタで有効にする必要があります。

### このタスクについて

を実行する必要があります `security key-manager onboard enable` コマンドはクラスタにノードを追

加するたびに実行します。MetroCluster 構成では、を実行する必要があります security key-manager onboard enable を実行してから、を実行します security key-manager onboard sync リモートクラスタで、それぞれで同じパスフレーズを使用します。

デフォルトでは、ノードのリポート時にキー管理ツールのパスフレーズを入力する必要はありません。MetroCluster 以外では、を使用できます cc-mode-enabled=yes リポート後にユーザにパスフレーズの入力を求めるオプション。

オンボードキーマネージャがCCモードで有効になっている場合 (cc-mode-enabled=yes) では、システムの動作は次のように変更されます。

- Common Criteria モードで動作している場合、クラスタパスフレーズの試行に連続して失敗したかどうか監視されます。

NetApp Storage Encryption (NSE) が有効になっている場合に、ブート時に正しいクラスタパスフレーズを入力しないと、システムはドライブを認証できず、自動的にリポートされます。これを修正するには、ブートプロンプトで正しいクラスタパスフレーズを入力する必要があります。ブート後、パラメータとしてクラスタパスフレーズを必要とするコマンドに対して、最大 5 回連続してクラスタパスフレーズを 24 時間以内に入力することができます。制限に達した場合（たとえば、クラスタのパスフレーズを 5 回連続して正しく入力できなかった場合など）は、24 時間のタイムアウトが経過するまで待つか、ノードをリポートして制限をリセットする必要があります。

- システムイメージの更新では、NetApp RSA-3072 コード署名証明書と SHA-384 コード署名ダイジェストを使用して、通常の NetApp RSA-2048 コード署名証明書および SHA-256 コード署名ダイジェストではなく、イメージの整合性をチェックします。

upgrade コマンドは、さまざまなデジタル署名をチェックして、イメージの内容が変更されていないか、壊れていないかを確認します。検証に成功した場合は、イメージの更新プロセスが次の手順に進みます。成功しなかった場合は、イメージの更新が失敗します。システムの更新については 'cluster image マニュアル・ページを参照してください

オンボードキーマネージャは、揮発性メモリにキーを格納します。揮発性メモリの内容は、システムのリポート時または停止時にクリアされます。通常の動作条件下では、システムが停止すると 30 秒以内に揮発性メモリの内容がクリアされます。

作業を開始する前に

- NSE で外部キー管理 (KMIP) サーバを使用している場合は、外部キー管理ツールのデータベースを削除しておく必要があります。

#### "外部キー管理からオンボードキー管理への移行"

- このタスクを実行するには、クラスタ管理者である必要があります。
- オンボードキーマネージャを設定する前に、MetroCluster 環境を設定する必要があります。

手順

1. キー管理ツールの setup コマンドを開始します。

```
security key-manager onboard enable -cc-mode-enabled yes|no
```



設定 `cc-mode-enabled=yes` リブート後にユーザにキー管理ツールのパスフレーズの入力を求める場合。。 - `cc-mode-enabled` オプションはMetroCluster 構成ではサポートされません。。 `security key-manager onboard enable` コマンドは、に置き換わるものです `security key-manager setup` コマンドを実行します

次の例では、リブートのたびにパスフレーズの入力を求めずに、`cluster1` でキー管理ツールの `setup` コマンドを開始します。

```
cluster1::> security key-manager onboard enable
```

```
Enter the cluster-wide passphrase for onboard key management in Vserver
"cluster1":> <32..256 ASCII characters long text>
Reenter the cluster-wide passphrase: <32..256 ASCII characters long
text>
```

2. パスフレーズのプロンプトで 32 ～ 256 文字のパスフレーズを入力します。または、64 ～ 256 文字のパスフレーズを「`cc-mode]`」に入力します。



指定された "cc-mode" パスフレーズが 64 文字未満の場合、キー管理ツールのセットアップ操作によってパスフレーズのプロンプトが再表示されるまでに 5 秒の遅延が発生します。

3. パスフレーズの確認のプロンプトでパスフレーズをもう一度入力します。
4. 認証キーが作成されたことを確認します。

```
security key-manager key query -node node
```



。 `security key-manager key query` コマンドは、に置き換わるものです `security key-manager query key` コマンドを実行しますコマンド構文全体については、マニュアルページを参照してください。

次の例は、の認証キーが作成されたことを確認します `cluster1` :

```
cluster1::> security key-manager key query
      Vserver: cluster1
      Key Manager: onboard
      Node: node1
```

Key Tag	Key Type	Restored
-----	-----	-----
node1	NSE-AK	yes
Key ID:		
000000000000000000002000000000001000c11b3863f78c2273343d7ec5a67762e0000000000000000		
node1	NSE-AK	yes
Key ID:		
000000000000000000002000000000001006f4e2513353a674305872a4c9f3bf7970000000000000000		

```
      Vserver: cluster1
      Key Manager: onboard
      Node: node2
```

Key Tag	Key Type	Restored
-----	-----	-----
node1	NSE-AK	yes
Key ID:		
000000000000000000002000000000001000c11b3863f78c2273343d7ec5a67762e0000000000000000		
node2	NSE-AK	yes
Key ID:		
000000000000000000002000000000001006f4e2513353a674305872a4c9f3bf7970000000000000000		

完了後

あとで使用できるように、ストレージシステムの外部の安全な場所にパスフレーズをコピーしておきます。

キー管理情報は、クラスタの Replicated Database（RDB；複製データベース）にすべて自動的にバックアップされます。災害時に備えて、情報を手動でもバックアップしておく必要があります。

#### ONTAP 9.5 以前でオンボードキー管理を有効にします

オンボードキーマネージャを使用して、クラスタノードを FIPS ドライブまたは SED に対して認証できます。オンボードキーマネージャは組み込みのツールで、データと同じストレージシステムからノードに認証キーを提供します。オンボードキーマネージャは FIPS-140-2 レベル 1 に準拠しています。

オンボードキーマネージャを使用して、暗号化されたデータにアクセスする際にクラスタで使用するキーを安



全に保管できます。オンボードキーマネージャは、暗号化されたボリュームや自己暗号化ディスクにアクセスする各クラスタで有効にする必要があります。

このタスクについて

を実行する必要があります `security key-manager setup` コマンドはクラスタにノードを追加するたびに実行します。

MetroCluster 構成を使用する場合は、次のガイドラインを確認してください。

- ONTAP 9.5では、を実行する必要があります `security key-manager setup` ローカルクラスタおよび `security key-manager setup -sync-metrocluster-config yes` リモートクラスタで、それぞれで同じパスフレーズを使用します。
- ONTAP 9.5より前のバージョンでは、を実行する必要があります `security key-manager setup` ローカルクラスタで、約20秒待ってからを実行します `security key-manager setup` リモートクラスタで、それぞれで同じパスフレーズを使用します。

デフォルトでは、ノードのリブート時にキー管理ツールのパスフレーズを入力する必要はありません。ONTAP 9.4以降では、`-enable-cc-mode yes` リブート後にユーザにパスフレーズの入力を求めるオプション。

NVEの場合は、を設定します `-enable-cc-mode yes` を使用して作成したボリューム ``volume create`` および `volume move start` コマンドは自動的に暗号化されます。の場合 `volume create`` を指定する必要はありません ``-encrypt true``。の場合 `volume move start`` を指定する必要はありません ``-encrypt-destination true``。



パスフレーズの試行に失敗した場合は、ノードを再起動する必要があります。

作業を開始する前に

- NSE で外部キー管理（KMIP）サーバを使用している場合は、外部キー管理ツールのデータベースを削除しておく必要があります。

#### "外部キー管理からオンボードキー管理への移行"

- このタスクを実行するには、クラスタ管理者である必要があります。
- オンボードキーマネージャを設定する前に、MetroCluster 環境を設定する必要があります。

手順

1. キー管理ツールのセットアップを開始します。

```
security key-manager setup -enable-cc-mode yes|no
```



ONTAP 9.4以降では、`-enable-cc-mode yes` リブート後にユーザにキー管理ツールのパスフレーズの入力を求めるオプション。NVEの場合は、を設定します `-enable-cc-mode yes`` を使用して作成したボリューム ``volume create`` および `volume move start` コマンドは自動的に暗号化されます。

次の例では、リブートのたびにパスフレーズの入力を求めずに、`cluster1` でキー管理ツールをセットアップします。



完了後

キー管理情報は、クラスタの Replicated Database（RDB；複製データベース）にすべて自動的にバックアップされます。

オンボードキーマネージャのパスフレーズを設定するときは、災害時に備えて、ストレージシステムの外部の安全な場所にも手動で情報をバックアップしておく必要があります。を参照してください ["オンボードキー管理情報を手動でバックアップ"](#)。

**FIPS** ドライブまたは **SED** にデータ認証キーを割り当てる（オンボードキー管理）

を使用できます `storage encryption disk modify` コマンドを使用して FIPS ドライブまたは SED にデータ認証キーを割り当てることができます。このキーは、クラスタノードでドライブのデータにアクセスする際に使用します。

このタスクについて

自己暗号化ドライブの認証キー ID がデフォルト以外の値に設定されている場合にのみ、不正アクセスから保護されます。Manufacturer Secure ID（MSID；メーカーのセキュア ID）のキー ID が 0x0 になり、SAS ドライブの標準のデフォルト値になります。NVMe ドライブの場合、標準のデフォルト値は null キーで、空のキー ID として表されます。キー ID を自己暗号化ドライブに割り当てると、認証キー ID がデフォルト以外の値に変更されます。

作業を開始する前に

このタスクを実行するには、クラスタ管理者である必要があります。

手順

1. FIPS ドライブまたは SED にデータ認証キーを割り当てます。

```
storage encryption disk modify -disk disk_ID -data-key-id key_ID
```

コマンド構文全体については、コマンドのマニュアルページを参照してください。



を使用できます `security key-manager key query -key-type NSE-AK` キー ID を表示するコマンド。

```
cluster1::> storage encryption disk modify -disk 0.10.* -data-key-id  
0000000000000000000020000000000010019215b9738bc7b43d4698c80246db1f4
```

```
Info: Starting modify on 14 disks.  
View the status of the operation by using the  
storage encryption disk show-status command.
```

2. 認証キーが割り当てられたことを確認します。

```
storage encryption disk show
```

コマンド構文全体については、マニュアルページを参照してください。

```
cluster1::> storage encryption disk show
Disk      Mode Data Key ID
-----
-----
0.0.0     data
00000000000000000000200000000000010019215b9738bc7b43d4698c80246db1f4
0.0.1     data
00000000000000000000200000000000010059851742AF2703FC91369B7DB47C4722
[...]
```

## FIPS ドライブに FIPS 140-2 認証キーを割り当てます

を使用できます `storage encryption disk modify` コマンドにを指定します `-fips-key-id` FIPS 140-2 認証キーを FIPS ドライブに割り当てるオプション。このキーは、ドライブに対する DoS 攻撃を防止するなど、データアクセス以外のドライブ処理に使用されます。

このタスクについて

セキュリティの設定によっては、データ認証と FIPS 140-2 認証に異なるキーを使用する必要がある場合があります。そうでない場合は、FIPS 準拠の認証キーをデータアクセスにも使用できます。

この手順 はシステムの停止を伴いません。

作業を開始する前に

ドライブファームウェアで FIPS 140-2 準拠がサポートされている必要があります。。 ["NetApp Interoperability Matrix Tool で確認できます"](#) サポートされているドライブファームウェアのバージョンに関する情報が含まれます。

手順

- 最初に、データ認証キーを割り当てておく必要があります。これは、を使用して実行できます [外部キー管理ツール](#) または [オンボードキーマネージャ](#)。コマンドを使用して、キーが割り当てられていることを確認します `storage encryption disk show`。
- SED に FIPS 140-2 認証キーを割り当てます。

```
storage encryption disk modify -disk disk_id -fips-key-id
fips_authentication_key_id
```

を使用できます `security key-manager query` キーIDを表示するコマンド。

```
cluster1::> storage encryption disk modify -disk 2.10.* -fips-key-id
6A1E21D8000000000100000000000005A1FB4EE8F62FD6D8AE6754C9019F35A
```

Info: Starting modify on 14 disks.  
View the status of the operation by using the  
storage encryption disk show-status command.

### 3. 認証キーが割り当てられたことを確認します。

```
storage encryption disk show -fips
```

コマンド構文全体については、マニュアルページを参照してください。

```
cluster1::> storage encryption disk show -fips
Disk      Mode FIPS-Compliance Key ID
-----
-----
2.10.0    full
6A1E21D8000000000100000000000005A1FB4EE8F62FD6D8AE6754C9019F35A
2.10.1    full
6A1E21D8000000000100000000000005A1FB4EE8F62FD6D8AE6754C9019F35A
[...]
```

**KMIP** サーバ接続に対して、クラスタ全体の **FIPS** 準拠モードを有効にします

を使用できます `security config modify` コマンドにを指定します `-is-fips-enabled` 転送中のデータに対してクラスタ全体のFIPS準拠モードを有効にするオプション。これにより、クラスタが **KMIP** サーバに接続する際に **FIPS** モードの **OpenSSL** が使用されるようになります。

このタスクについて

クラスタ全体の **FIPS** 準拠モードを有効にすると、自動的に **TLS1.2** と **FIPS** 認定暗号スイートのみが使用されます。クラスタ全体の **FIPS** 準拠モードは、デフォルトでは無効になっています。

クラスタ全体のセキュリティの設定を変更した場合は、変更後にクラスタノードを手動でリブートする必要があります。

作業を開始する前に

- ストレージコントローラは **FIPS** 準拠モードで設定する必要があります。
- すべての **KMIP** サーバで **TLSv1.2** がサポートされている必要がありクラスタ全体の **FIPS** 準拠モードが有効になっている場合、**KMIP** サーバへの接続を完了するために **TLSv1.2** が必要になります。

手順

1. 権限レベルを **advanced** に設定します。

```
set -privilege advanced
```

2. TLSv1.2 がサポートされていることを確認します。

```
security config show -supported-protocols
```

コマンド構文全体については、マニュアルページを参照してください。

```
cluster1::> security config show
```

	Cluster		Cluster
Security			
Interface	FIPS Mode	Supported Protocols	Supported Ciphers
Ready			Config
-----	-----	-----	-----
-----			
SSL	false	TLSv1.2, TLSv1.1, TLSv1	ALL:!LOW: !aNULL:!EXP: !eNULL
			yes

3. クラスタ全体の FIPS 準拠モードを有効にします。

```
security config modify -is-fips-enabled true -interface SSL
```

コマンド構文全体については、マニュアルページを参照してください。

4. クラスタノードを手動でリブートします。
5. クラスタ全体の FIPS 準拠モードが有効になっていることを確認します。

```
security config show
```

```
cluster1::> security config show
```

	Cluster		Cluster
Security			
Interface	FIPS Mode	Supported Protocols	Supported Ciphers
Ready			Config
-----	-----	-----	-----
-----			
SSL	true	TLSv1.2, TLSv1.1	ALL:!LOW: !aNULL:!EXP: !eNULL:!RC4
			yes

## ネットアップの暗号化を管理

ボリュームデータの暗号化を解除します

を使用できます `volume move start` ボリュームデータを移動および暗号化解除するコマンド。

作業を開始する前に

このタスクを実行するには、クラスタ管理者である必要があります。または、クラスタ管理者から権限を委譲されたSVM管理者を指定することもできます。詳細については、を参照してください ["volume move コマンドの実行権限を委譲します"](#)。

手順

1. 既存の暗号化されたボリュームを移動し、ボリュームのデータの暗号化を解除します。

```
volume move start -vserver SVM_name -volume volume_name -destination-aggregate aggregate_name -encrypt-destination false
```

コマンド構文全体については、コマンドのマニュアルページを参照してください。

次のコマンドは、という名前の既存のボリュームを移動します `vol1` デスティネーションアグリゲートに移動します `aggr3` ボリューム上のデータの暗号化を解除します。

```
cluster1::> volume move start -vserver vs1 -volume vol1 -destination -aggregate aggr3 -encrypt-destination false
```

ボリュームの暗号化キーが削除されます。ボリュームのデータの暗号化が解除されます。

2. ボリュームで暗号化が無効になっていることを確認します。

```
volume show -encryption
```

コマンド構文全体については、コマンドのマニュアルページを参照してください。

次のコマンドは、ボリュームが上にあるかどうかを表示します `cluster1` 暗号化：

```
cluster1::> volume show -encryption
```

Vserver	Volume	Aggregate	State	Encryption State
-----	-----	-----	-----	-----
vs1	vol1	aggr1	online	none

暗号化されたボリュームを移動します

を使用できます `volume move start` 暗号化されたボリュームを移動するコマンド。ボリュームを移動するアグリゲートは同じアグリゲートでも別のアグリゲートでもかまいません。

このタスクについて

デスティネーションノードまたはデスティネーションボリュームでボリューム暗号化がサポートされていない場合、移動は失敗します。

。-encrypt-destination のオプション volume move start 暗号化されたボリュームの場合、デフォルトはtrueです。デスティネーションボリュームを暗号化しないように指定すると、ボリューム上のデータの暗号化が誤って解除されることがなくなります。

作業を開始する前に

このタスクを実行するには、クラスタ管理者である必要があります。または、クラスタ管理者から権限を委譲されたSVM管理者を指定することもできます。詳細については、[を参照してください "volume move コマンドの実行権限を委譲する"](#)。

手順

1. 既存の暗号化されたボリュームを移動し、ボリュームのデータを暗号化されたままにします。

```
volume move start -vserver SVM_name -volume volume_name -destination-aggregate aggregate_name
```

コマンド構文全体については、コマンドのマニュアルページを参照してください。

次のコマンドは、という名前の既存のボリュームを移動します vol1 デスティネーションアグリゲートに移動します aggr3 ボリューム上のデータは暗号化されたままになります。

```
cluster1::> volume move start -vserver vs1 -volume vol1 -destination -aggregate aggr3
```

2. ボリュームで暗号化が有効になっていることを確認します。

```
volume show -is-encrypted true
```

コマンド構文全体については、コマンドのマニュアルページを参照してください。

次のコマンドは、の暗号化されたボリュームを表示します cluster1：

```
cluster1::> volume show -is-encrypted true
```

Vserver	Volume	Aggregate	State	Type	Size	Available	Used
-----	-----	-----	-----	----	-----	-----	-----
vs1	vol1	aggr3	online	RW	200GB	160.0GB	20%

**volume move** コマンドの実行権限を委譲します

を使用できます volume move コマンドを使用して、既存のボリュームを暗号化したり、暗号化されたボリュームを移動したり、ボリュームの暗号化を解除したりできます。クラスタ管理者はを実行できます volume move コマンド自体を実行することも、



コマンドの実行権限をSVM管理者に委譲することもできます。

このタスクについて

デフォルトでは、SVM管理者にはが割り当てられます `vsadmin` ロール。ボリュームを移動する権限は含まれません。を割り当てる必要があります `vsadmin-volume` の実行を許可するSVM管理者のロール `volume move` コマンドを実行します

ステップ

1. を実行する権限を委任します `volume move` コマンドを実行します

```
security login modify -vserver SVM_name -user-or-group-name user_or_group_name  
-application application -authmethod authentication_method -role vsadmin-  
volume
```

コマンド構文全体については、コマンドのマニュアルページを参照してください。

次のコマンドは、SVM管理者にを実行する権限を付与します `volume move` コマンドを実行します

```
cluster1::>security login modify -vserver engData -user-or-group-name  
SVM-admin -application ssh -authmethod domain -role vsadmin-volume
```

**volume encryption rekey start** コマンドを使用してボリュームの暗号化キーを変更します

セキュリティのベストプラクティスとして、ボリュームの暗号化キーを定期的に変更することが重要です。ONTAP 9.3以降では、を使用できます `volume encryption rekey start` コマンドを使用して暗号化キーを変更します。

このタスクについて

キー変更処理を開始したら、最後まで完了する必要があります。古いキーに戻ることはありません。処理中にパフォーマンス問題が発生した場合は、を実行できます `volume encryption rekey pause` 処理を一時停止するコマンド、および `volume encryption rekey resume` コマンドを実行して処理を再開します。

キー変更処理が完了するまで、ボリュームには2つのキーが存在することになります。新しい書き込みとそれに対応する読み取りでは、新しいキーが使用されます。それ以外の読み取りでは、古いキーが使用されます。



を使用することはできません `volume encryption rekey start` をクリックしてSnapLockボリュームのキーを変更します。

手順

1. 暗号化キーを変更します。

```
volume encryption rekey start -vserver SVM_name -volume volume_name
```

次の例は、の暗号化キーを変更します `vol1 SVM上vs1` :

```
cluster1::> volume encryption rekey start -vserver vs1 -volume vol1
```

2. キー変更処理のステータスを確認します。

```
volume encryption rekey show
```

コマンド構文全体については、コマンドのマニュアルページを参照してください。

次のコマンドは、キー変更処理のステータスを表示します。

```
cluster1::> volume encryption rekey show
```

Vserver	Volume	Start Time	Status
-----	-----	-----	-----
vs1	vol1	9/18/2017 17:51:41	Phase 2 of 2 is in progress.

3. キー変更処理が完了したら、ボリュームで暗号化が有効になっていることを確認します。

```
volume show -is-encrypted true
```

コマンド構文全体については、コマンドのマニュアルページを参照してください。

次のコマンドは、の暗号化されたボリュームを表示します cluster1：

```
cluster1::> volume show -is-encrypted true
```

Vserver	Volume	Aggregate	State	Type	Size	Available	Used
-----	-----	-----	-----	-----	-----	-----	-----
vs1	vol1	aggr2	online	RW	200GB	160.0GB	20%

**volume move start** コマンドを使用して、ボリュームの暗号化キーを変更します

セキュリティのベストプラクティスとして、ボリュームの暗号化キーを定期的に変更することが重要です。を使用できます volume move start コマンドを使用して暗号化キーを変更します。を使用する必要があります volume move start ONTAP 9.2以前では、ボリュームを移動するアグリゲートは同じアグリゲートでも別のアグリゲートでもかまいません。

このタスクについて

を使用することはできません volume move start をクリックしてSnapLock またはFlexGroup ボリュームのキーを変更します。

作業を開始する前に

このタスクを実行するには、クラスタ管理者である必要があります。または、クラスタ管理者から権限を委譲

されたSVM管理者を指定することもできます。詳細については、を参照してください ["volume move コマンドの実行権限を委譲する"](#)。

#### 手順

1. 既存のボリュームを移動し、暗号化キーを変更します。

```
volume move start -vserver SVM_name -volume volume_name -destination-aggregate aggregate_name -generate-destination-key true
```

コマンド構文全体については、コマンドのマニュアルページを参照してください。

次のコマンドは、という名前の既存のボリュームを移動します **vol1** デスティネーションアグリゲートに移動します **aggr2** 暗号化キーを変更します。

```
cluster1::> volume move start -vserver vs1 -volume vol1 -destination -aggregate aggr2 -generate-destination-key true
```

ボリュームの新しい暗号化キーが作成されます。ボリュームのデータは暗号化されたままです。

2. ボリュームで暗号化が有効になっていることを確認します。

```
volume show -is-encrypted true
```

コマンド構文全体については、コマンドのマニュアルページを参照してください。

次のコマンドは、の暗号化されたボリュームを表示します cluster1：

```
cluster1::> volume show -is-encrypted true
```

Vserver	Volume	Aggregate	State	Type	Size	Available	Used
-----	-----	-----	-----	-----	-----	-----	-----
vs1	vol1	aggr2	online	RW	200GB	160.0GB	20%

#### NetApp Storage Encryption の認証キーをローテーションします

NetApp Storage Encryption （NSE）を使用する場合は、認証キーをローテーションすることができます。

このタスクについて

外部キーマネージャ（KMIP）を使用している場合は、NSE 環境での認証キーのローテーションがサポートされます。



NSE 環境でのオンボードキーマネージャ（OKM）での認証キーのローテーションはサポートされていません。

#### 手順

1. を使用します `security key-manager create-key` コマンドを使用して新しい認証キーを生成します。

認証キーを変更する前に、新しい認証キーを生成する必要があります。

2. を使用します `storage encryption disk modify -disk * -data-key-id` コマンドを使用して認証キーを変更します。

暗号化されたボリュームを削除する

を使用できます `volume delete` 暗号化されたボリュームを削除するコマンド。

作業を開始する前に

- このタスクを実行するには、クラスタ管理者である必要があります。または、クラスタ管理者から権限を委譲されたSVM管理者を指定することもできます。詳細については、["volume move コマンドの実行権限を委譲する"](#)。
- ボリュームはオフラインである必要があります。

ステップ

1. 暗号化されたボリュームを削除します。

```
volume delete -vserver SVM_name -volume volume_name
```

コマンド構文全体については、コマンドのマニュアルページを参照してください。

次のコマンドは、という名前の暗号化されたボリュームを削除します `vol1` :

```
cluster1::> volume delete -vserver vs1 -volume vol1
```

入力するコマンド `yes` 削除を確認するプロンプトが表示されたら、

24 時間後にボリュームの暗号化キーが削除されます。

使用 `volume delete` を使用 `-force true` ボリュームを削除して対応する暗号化キーをただちに破棄するオプション。このコマンドには `advanced` 権限が必要です。詳細については、[のマニュアルページを参照してください](#)。

完了後

を使用できます `volume recovery-queue` コマンドを使用して、を実行したあとに保持期間内に削除されたボリュームをリカバリします `volume delete` コマンドを実行します

```
volume recovery-queue SVM_name -volume volume_name
```

["ボリュームリカバリ機能の使用法"](#)

暗号化されたボリューム上のデータをセキュアにパージします

ONTAP 9.4 以降では、セキュアパージを使用して、NVE 対応ボリューム上のデータを無停止でスクラビングできます。暗号化されたボリュームのデータをスクラビングすることで、「柱」、「ブロックが上書きされたときにデータトレースが残されている」などの物理メディアからデータをリカバリすることができなくなります。また、解約するテナントのデータを安全に削除することもできます。

セキュアパージの対象となるのは、NVE 対応ボリューム上で以前に削除されたファイルだけです。暗号化されていないボリュームはスクラビングできません。キーの提供には、オンボードキーマネージャではなく、KMIP サーバを使用する必要があります。

#### セキュアパージを使用する場合の考慮事項

- NetApp Aggregate Encryption (NAE) が有効になっているアグリゲートで作成されたボリュームでは、セキュアパージがサポートされません。
- セキュアパージの対象となるのは、NVE 対応ボリューム上で以前に削除されたファイルだけです。
- 暗号化されていないボリュームはスクラビングできません。
- キーの提供には、オンボードキーマネージャではなく、KMIP サーバを使用する必要があります。

セキュアパージの機能は、ONTAP のバージョンによって異なります。

## ONTAP 9.8以降

- セキュアパージは、MetroCluster および FlexGroup でサポートされています。
- パージするボリュームが SnapMirror 関係のソースである場合は、セキュアパージを実行するために SnapMirror 関係を解除する必要はありません。
- 再暗号化の方法は、SnapMirror データ保護を使用するボリュームと、SnapMirror データ保護（DP）を使用していないボリュームまたは SnapMirror 拡張データ保護を使用しているボリュームで異なります。
  - デフォルトでは、SnapMirror データ保護（DP）モードを使用するボリュームは、ボリューム移動の再暗号化方式を使用してデータを再暗号化します。
  - デフォルトでは、SnapMirror データ保護を使用していないボリュームや SnapMirror 拡張データ保護（XDP）モードを使用しているボリュームでは、インプレースの再暗号化方式を使用します。
  - これらのデフォルト値は、を使用して変更できます `secure purge re-encryption-method [volume-move|in-place-rekey]` コマンドを実行します
- デフォルトでは、セキュアパージ処理の実行中に、FlexVol ボリューム内のすべての Snapshot コピーが自動的に削除されます。デフォルトでは、FlexGroup の Snapshot および SnapMirror データ保護を使用するボリュームは、セキュアパージ処理の実行中に自動的に削除されません。これらのデフォルト値は、を使用して変更できます `secure purge delete-all-snapshots [true|false]` コマンドを実行します

## ONTAP 9.7以前：

- セキュアパージでは、次のものはサポートされません。
  - FlexClone
  - SnapVault
  - FabricPool
- パージするボリュームが SnapMirror 関係のソースである場合は、ボリュームをパージする前に SnapMirror 関係を解除する必要があります。

ボリューム内に使用中の Snapshot コピーがある場合は、ボリュームをパージする前にその Snapshot コピーを解放する必要があります。たとえば、FlexClone ボリュームを親ボリュームからスプリットする必要がある場合があります。

- セキュアパージ機能を呼び出すと、ボリューム移動がトリガーされ、パージされない残りのデータが新しいキーで再暗号化されます。

移動されたボリュームは現在のアグリゲートに残ります。パージされたデータをストレージメディアからリカバリできないように、古いキーは自動的に破棄されます。

**SnapMirror** 関係なしで暗号化されたボリューム上のデータをセキュアにパージします

ONTAP 9.4 以降では、NVE 対応ボリューム上で、システムを停止することなく「crub」データにセキュアパージを使用できます。

このタスクについて

削除されたファイルのデータ量によっては、セキュアパージが完了するまでに数分から数時間かかることがあります。を使用できます `volume encryption secure-purge show` コマンドを使用して処理のステータスを表示します。を使用できます `volume encryption secure-purge abort` コマンドを入力して処理を終了します。



SAN ホストでセキュアパージを実行するには、パージするファイルを含む LUN 全体を削除するか、パージするファイルに属するブロックの LUN で穴を開ける必要があります。LUN を削除できない場合や、ホストオペレーティングシステムで LUN のパンチ穴がサポートされていない場合は、セキュアパージを実行できません。

作業を開始する前に

- このタスクを実行するには、クラスタ管理者である必要があります。
- このタスクを実行するには advanced 権限が必要です。

手順

1. セキュアパージするファイルまたは LUN を削除します。
  - NAS クライアントで、セキュアパージするファイルを削除します。
  - SAN ホストで、パージするファイルに属するブロックのために、LUN から安全にパージまたはパンチ穴を開ける LUN を削除します。
2. ストレージシステムで、advanced 権限レベルに切り替えます。

```
set -privilege advanced
```

3. 安全にパージするファイルがスナップショットにある場合は、スナップショットを削除します。

```
snapshot delete -vserver SVM_name -volume volume_name -snapshot
```

4. 削除したファイルを安全にパージします。

```
volume encryption secure-purge start -vserver SVM_name -volume volume_name
```

次のコマンドは、で削除したファイルをセキュアパージします vol1 SVM上vs1：

```
cluster1::> volume encryption secure-purge start -vserver vs1 -volume vol1
```

5. セキュアパージ処理のステータスを確認します。

```
volume encryption secure-purge show
```

非同期 **SnapMirror** 関係によって暗号化されたボリューム上のデータをセキュアにパージします

ONTAP 9.8 以降では、非同期 SnapMirror 関係を持つ NVE 対応ボリュームで、システムを停止せずに「crub」データをセキュアパージできます。

作業を開始する前に

- このタスクを実行するには、クラスタ管理者である必要があります。
- このタスクを実行するには advanced 権限が必要です。

#### このタスクについて

削除されたファイルのデータ量によっては、セキュアパーズが完了するまでに数分から数時間かかることがあります。を使用できます volume encryption secure-purge show コマンドを使用して処理のステータスを表示します。を使用できます volume encryption secure-purge abort コマンドを入力して処理を終了します。



SAN ホストでセキュアパーズを実行するには、パーズするファイルを含む LUN 全体を削除するか、パーズするファイルに属するブロックの LUN で穴を開ける必要があります。LUN を削除できない場合や、ホストオペレーティングシステムで LUN のパンチ穴がサポートされていない場合は、セキュアパーズを実行できません。

#### 手順

1. ストレージシステムで、advanced権限レベルに切り替えます。

```
set -privilege advanced
```

2. セキュアパーズするファイルまたは LUN を削除します。

- NAS クライアントで、セキュアパーズするファイルを削除します。
- SAN ホストで、パーズするファイルに属するブロックのために、LUN から安全にパーズまたはパンチ穴を開ける LUN を削除します。

3. 非同期関係のデスティネーションボリュームを安全にパーズするように準備します。

```
volume encryption secure-purge start -vserver SVM_name -volume volume_name  
-prepare true
```

非同期 SnapMirror 関係の各ボリュームについて、この手順を繰り返します。

4. セキュアにパーズするファイルが Snapshot コピーにある場合は、Snapshot コピーを削除します。

```
snapshot delete -vserver SVM_name -volume volume_name -snapshot
```

5. セキュアパーズの対象となるファイルがベース Snapshot コピー内にある場合は、次の手順を実行します。

- a. 非同期 SnapMirror 関係のデスティネーションボリュームに Snapshot コピーを作成します。

```
volume snapshot create -snapshot snapshot_name -vserver SVM_name -volume  
volume_name
```

- b. SnapMirror を更新してベースの Snapshot コピーをフォワードします。

```
snapmirror update -source-snapshot snapshot_name -destination-path  
destination_path
```

非同期 SnapMirror 関係のボリュームごとにこの手順を繰り返します。



- a. ベース Snapshot コピーの数に 1 を加えた値と同じ手順 (a) および (b) を繰り返します。

たとえば、2 つのベース Snapshot コピーがある場合は、手順 (a) と (b) を 3 回繰り返します。

- b. ベースの Snapshot コピーが存在することを確認します。

[+]

```
snapshot show -vserver SVM_name -volume volume_name
```

- c. ベースの Snapshot コピーを削除します。

[+]

```
snapshot delete -vserver svm_name -volume volume_name -snapshot snapshot
```

## 6. 削除したファイルを安全にパージします。

```
volume encryption secure-purge start -vserver svm_name -volume volume_name
```

非同期 SnapMirror 関係の各ボリュームについて、この手順を繰り返します。

次のコマンドは、SVM 「vs1」上の「vol1」にある削除済みファイルを安全にパージします。

```
cluster1::> volume encryption secure-purge start -vserver vs1 -volume vol1
```

## 7. セキュアパージ処理のステータスを確認します。

```
volume encryption secure-purge show
```

同期 **SnapMirror** 関係が設定された暗号化されたボリュームのデータをスクラビングします

ONTAP 9.8以降では、セキュアパージを使用して、同期SnapMirror関係にあるNVE対応ボリュームのデータを無停止で「スクラビング」できます。

このタスクについて

削除されたファイルのデータ量によっては、セキュアパージが完了するまでに数分から数時間かかることがあります。を使用できます volume encryption secure-purge show コマンドを使用して処理のステータスを表示します。を使用できます volume encryption secure-purge abort コマンドを入力して処理を終了します。



SAN ホストでセキュアパージを実行するには、パージするファイルを含む LUN 全体を削除するか、パージするファイルに属するブロックの LUN で穴を開ける必要があります。LUN を削除できない場合や、ホストオペレーティングシステムで LUN のパンチ穴がサポートされていない場合は、セキュアパージを実行できません。

作業を開始する前に

- このタスクを実行するには、クラスタ管理者である必要があります。
- このタスクを実行するには advanced 権限が必要です。

手順

1. ストレージシステムで、advanced 権限レベルに切り替えます。

```
set -privilege advanced
```

2. セキュアパーズするファイルまたは LUN を削除します。

- NAS クライアントで、セキュアパーズするファイルを削除します。
- SAN ホストで、パーズするファイルに属するブロックのために、LUN から安全にパーズまたはパンチ穴を開ける LUN を削除します。

3. 非同期関係のデスティネーションボリュームを安全にパーズするように準備します。

```
volume encryption secure-purge start -vserver SVM_name -volume volume_name  
-prepare true
```

同期 SnapMirror 関係にある他のボリュームに対してこの手順を繰り返します。

4. セキュアにパーズするファイルが Snapshot コピーにある場合は、Snapshot コピーを削除します。

```
snapshot delete -vserver SVM_name -volume volume_name -snapshot snapshot
```

5. セキュアなパーズファイルがベースまたは共通の Snapshot コピーに含まれている場合は、SnapMirror を更新して共通の Snapshot コピーをフォワードします。

```
snapmirror update -source-snapshot snapshot_name -destination-path  
destination_path
```

共通の Snapshot コピーが 2 つあるため、このコマンドは 2 回実行する必要があります。

6. セキュアなパーズファイルがアプリケーションと整合性のある Snapshot コピーに含まれている場合は、同期 SnapMirror 関係にある両方のボリュームで Snapshot コピーを削除します。

```
snapshot delete -vserver SVM_name -volume volume_name -snapshot snapshot
```

この手順は両方のボリュームで実行します。

7. 削除したファイルを安全にパーズします。

```
volume encryption secure-purge start -vserver SVM_name -volume volume_name
```

同期 SnapMirror 関係にある各ボリュームについて、この手順を繰り返します。

次のコマンドは 'SMV "vs1 "' 上の "vol1" 上の削除されたファイルを安全にパーズします

```
cluster1::> volume encryption secure-purge start -vserver vs1 -volume  
vol1
```

8. セキュアパーズ処理のステータスを確認します。

```
volume encryption secure-purge show
```

オンボードキー管理のパスフレーズを変更します

セキュリティのベストプラクティスとして、オンボードキー管理のパスフレーズを定期的に変更することが重要です。あとでできるように、ストレージシステムの外部の安全な場所にオンボードキー管理の新しいパスフレーズをコピーしておく必要があります。

作業を開始する前に

- このタスクを実行するには、クラスタ管理者または SVM の管理者である必要があります。
- このタスクを実行するには advanced 権限が必要です。

手順

1. advanced 権限レベルに切り替えます。

```
set -privilege advanced
```

2. オンボードキー管理のパスフレーズを変更します。

ONTAP バージョン	使用するコマンド
ONTAP 9.6 以降	<code>security key-manager onboard update-passphrase</code>
ONTAP 9.5 以前	<code>security key-manager update-passphrase</code>

コマンド構文全体については、マニュアルページを参照してください。

次のONTAP 9.6のコマンドでは、のオンボードキー管理のパスフレーズを変更できます cluster1:

```
cluster1::> security key-manager onboard update-passphrase
Warning: This command will reconfigure the cluster passphrase for
onboard key management for Vserver "cluster1".
Do you want to continue? {y|n}: y
Enter current passphrase:
Enter new passphrase:
```

3. 入力するコマンド y で、オンボードキー管理のパスフレーズを変更するよう求められます。
4. 現在のパスフレーズのプロンプトで現在のパスフレーズを入力します。
5. 新しいパスフレーズのプロンプトで 32 ~ 256 文字のパスフレーズを入力します。または、64 ~ 256 文字のパスフレーズを「cc-mode」に入力します。

指定された "cc-mode" パスフレーズが 64 文字未満の場合、キー管理ツールのセットアップ操作によってパスフレーズのプロンプトが再表示されるまでに 5 秒の遅延が発生します。

6. パスフレーズの確認のプロンプトでパスフレーズをもう一度入力します。

完了後

MetroCluster 環境では、パートナークラスタでパスフレーズを更新する必要があります。

- ONTAP 9.5以前では、を実行する必要があります security key-manager update-passphrase パートナークラスタで同じパスフレーズを使用。
- ONTAP 9.6以降では、を実行するように求められます security key-manager onboard sync パートナークラスタで同じパスフレーズを使用。

あとで使用できるように、ストレージシステムの外部の安全な場所にオンボードキー管理のパスフレーズをコピーしておく必要があります。

オンボードキー管理のパスフレーズを変更するときは、キー管理情報を手動でバックアップしておく必要があります。

"オンボードキー管理情報の手動でのバックアップ"

オンボードキー管理情報を手動でバックアップ

オンボードキーマネージャのパスフレーズを設定する場合、ストレージシステムの外部の安全な場所にオンボードキー管理の情報をコピーしておく必要があります。

必要なもの

- このタスクを実行するには、クラスタ管理者である必要があります。
- このタスクを実行するには advanced 権限が必要です。

このタスクについて

キー管理情報は、クラスタの Replicated Database （ RDB ；複製データベース）にすべて自動的にバックアップされます。災害時に備えて、キー管理情報を手動でもバックアップしておく必要があります。

手順

1. advanced 権限レベルに切り替えます。

```
set -privilege advanced
```

2. クラスタのキー管理バックアップ情報を表示します。

ONTAP バージョン	使用するコマンド
ONTAP 9.6 以降	security key-manager onboard show-backup
ONTAP 9.5 以前	security key-manager backup show

コマンド構文全体については、マニュアルページを参照してください。

[+]

次の9.6のコマンドは、次のキー管理バックアップ情報を表示します： cluster1：

[+]

[illegible]



Flash Cacheモジュールを搭載したシステムでNSEを使用する場合は、NVEまたはNAEも有効にする必要があります。NSEは、Flash Cacheモジュール上のデータを暗号化しません。

ルートボリュームを暗号化した**ONTAP 9.8**以降



ONTAP 9.8以降を実行していてルートボリュームが暗号化されていない場合は、ONTAP 9.6以降の手順に従います。

ONTAP 9.8 以降を実行していて、ルートボリュームが暗号化されている場合は、ブートメニューを使用してオンボードキー管理のリカバリパスフレーズを設定する必要があります。ブートメディアの交換を行う場合も、このプロセスが必要です。

1. ノードをブートメニューでブートし、オプションを選択します (10) Set onboard key management recovery secrets。
2. 入力するコマンド `y` このオプションを使用します。
3. プロンプトで、クラスタのオンボードキー管理のパスフレーズを入力します。
4. プロンプトで、バックアップキーのデータを入力します。

ノードがブートメニューに戻ります。

5. ブートメニューからオプションを選択します (1) Normal Boot。

#### ONTAP 9.6 以降

1. キーのリストアが必要であることを確認します。+  
`security key-manager key query -node node`
2. キーを復元します。+  
`security key-manager onboard sync`

コマンド構文全体については、マニュアルページを参照してください。

ONTAP 9.6 の次のコマンドを使用して、オンボードキー階層のキーを同期します。

```
cluster1::> security key-manager onboard sync
```

```
Enter the cluster-wide passphrase for onboard key management in Vserver  
"cluster1":::    <32..256 ASCII characters long text>
```

3. パスフレーズのプロンプトで、クラスタのオンボードキー管理のパスフレーズを入力します。

#### ONTAP 9.5 以前

1. キーのリストアが必要であることを確認します。+  
`security key-manager key show`
2. ONTAP 9.8 以降を実行していて、ルート・ボリュームが暗号化されている場合は、次の手順を実行します。

ONTAP 9.6 または 9.7 を実行している場合、または ONTAP 9.8 以降を実行していて、ルートボリュームが暗号化されていない場合は、この手順を省略してください。

3. キーを復元します。+

```
security key-manager setup -node node
```

コマンド構文全体については、マニュアルページを参照してください。

4. パスフレーズのプロンプトで、クラスタのオンボードキー管理のパスフレーズを入力します。

外部キー管理の暗号化キーをリストアします

外部キー管理の暗号化キーを手動でリストアし、別のノードにプッシュすることができます。この処理は、クラスタのキーの作成時に一時的に停止していたノードを再起動する場合などに実行します。

このタスクについて

ONTAP 9.6以降では、を使用できます `security key-manager key query -node node_name` コマンドを実行して、キーのリストアが必要かどうかを確認します。

ONTAP 9.5以前では、を使用できます `security key-manager key show` コマンドを実行して、キーのリストアが必要かどうかを確認します。



Flash Cacheモジュールを搭載したシステムでNSEを使用する場合は、NVEまたはNAEも有効にする必要があります。NSEは、Flash Cacheモジュール上のデータを暗号化しません。

作業を開始する前に

このタスクを実行するには、クラスタ管理者または SVM の管理者である必要があります。

手順

1. ONTAP 9.8 以降を実行していて、ルートボリュームが暗号化されている場合は、次の手順を実行します。

ONTAP 9.7 以前を実行している場合、または ONTAP 9.8 以降を実行していて、ルートボリュームが暗号化されていない場合は、この手順を省略してください。

a. bootargを設定します。

```
[] `setenv kmip.init.ipaddr <ip-address>` []  
setenv kmip.init.netmask <netmask>  
[] `setenv kmip.init.gateway <gateway>` []  
setenv kmip.init.interface e0M  
[+]  
boot_ontap
```

b. ノードをブートメニューでブートし、オプションを選択します (11) Configure node for external key management。

c. プロンプトに従って管理証明書を入力します。

管理証明書の情報をすべて入力すると、システムがブートメニューに戻ります。

d. ブートメニューからオプションを選択します (1) Normal Boot。

## 2. キーをリストアします。

ONTAP バージョン	使用するコマンド
ONTAP 9.6 以降	<code>`security key-manager external restore -vserver SVM -node node -key-server host_name`</code>
IP_address:port -key-id key_id -key -tag key_tag`	ONTAP 9.5 以前



node デフォルトはすべてのノードです。コマンド構文全体については、マニュアルページを参照してください。このコマンドは、オンボードキー管理が有効な場合はサポートされません。

次のONTAP 9.6のコマンドは、外部キー管理の認証キーをのすべてのノードにリストアします cluster1 :

```
cluster1::> security key-manager external restore
```

## SSL 証明書を交換します

すべての SSL 証明書には有効期限があります。認証キーへのアクセスが失われないように、証明書の有効期限が切れる前に証明書を更新する必要があります。

作業を開始する前に

- クラスタ（KMIP クライアント証明書）の交換用のパブリック証明書と秘密鍵を入手しておく必要があります。
- KMIP サーバ（KMIP server-ca 証明書）の交換用のパブリック証明書を入手しておく必要があります。
- このタスクを実行するには、クラスタ管理者または SVM の管理者である必要があります。
- MetroCluster 環境では、両方のクラスタのKMIP SSL証明書を置き換える必要があります。



KMIP サーバへの交換用のクライアント証明書とサーバ証明書のインストールは、クラスタに証明書をインストールする前でもインストールしたあとでもかまいません。

## 手順

1. 新しい KMIP サーバ CA 証明書をインストールします。

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

2. 新しい KMIP クライアント証明書をインストールします。

```
security certificate install -type client -vserver <>
```

3. 新しくインストールした証明書を使用するようにキー管理ツールの設定を更新します。

```
security key-manager external modify -vserver <> -client-cert <> -server-ca
```



-certs <>

MetroCluster 環境でONTAP 9.6以降を実行している場合に、管理SVMでキー管理ツールの設定を変更するには、構成内の両方のクラスタでコマンドを実行する必要があります。



新しくインストールした証明書を使用するようにキー管理ツールの設定を更新すると、新しいクライアント証明書の公開鍵と秘密鍵が以前にインストールしたキーと異なる場合にエラーが返されます。サポート技術情報の記事を参照してください ["新しいクライアント証明書の公開鍵または秘密鍵が、既存のクライアント証明書と異なります"](#) このエラーを無視する方法については、[を参照してください](#)。

**FIPS** ドライブまたは **SED** を交換します

FIPS ドライブと SED は、通常のディスクと同じ方法で交換できます。交換用ドライブに新しいデータ認証キーを割り当ててください。FIPS ドライブの場合は、新しい FIPS 140-2 認証キーを割り当てることもできます。



HA ペアが使用している場合 ["SAS ドライブまたは NVMe ドライブの暗号化（SED、NSE、FIPS）"](#)、の手順に従ってください ["FIPS ドライブまたは SED を非保護モードに戻します"](#) システムを初期化する前の HA ペア内のすべてのドライブ（ブートオプション 4 または 9）。そうしないと、ドライブを転用した場合にデータが失われる可能性があります。

作業を開始する前に

- ドライブで使用される認証キーのキー ID を確認しておく必要があります。
- このタスクを実行するには、クラスタ管理者である必要があります。

手順

1. ディスクが障害状態としてマークされていることを確認します。

```
storage disk show -broken
```

コマンド構文全体については、マニュアルページを参照してください。

```
cluster1::> storage disk show -broken
```

```
Original Owner: cluster1-01
```

```
Checksum Compatibility: block
```

											Usable
Physical											
Disk	Outage	Reason	HA	Shelf	Bay	Chan	Pool	Type	RPM	Size	
Size											
-----	----	-----	----	----	----	----	-----	-----	-----	-----	
0.0.0	admin	failed	0b	1	0	A	Pool0	FCAL	10000	132.8GB	
133.9GB											
0.0.7	admin	removed	0b	2	6	A	Pool1	FCAL	10000	132.8GB	
134.2GB											
[...]											

2. ディスクシェルフモデルのハードウェアガイドの指示に従い、障害ディスクを取り外して、新しい FIPS ドライブまたは SED に交換します。
3. 交換した新しいディスクの所有権を割り当てます。

```
storage disk assign -disk disk_name -owner node
```

コマンド構文全体については、マニュアルページを参照してください。

```
cluster1::> storage disk assign -disk 2.1.1 -owner cluster1-01
```

4. 新しいディスクが割り当てられたことを確認します。

```
storage encryption disk show
```

コマンド構文全体については、マニュアルページを参照してください。

```
cluster1::> storage encryption disk show
Disk      Mode Data Key ID
-----
-----
0.0.0     data
F1CB30AFF1CB30B00101000000000000A68B167F92DD54196297159B5968923C
0.0.1     data
F1CB30AFF1CB30B00101000000000000A68B167F92DD54196297159B5968923C
1.10.0    data
F1CB30AFF1CB30B00101000000000000CF0EFD81EA9F6324EA97B369351C56AC
1.10.1    data
F1CB30AFF1CB30B00101000000000000CF0EFD81EA9F6324EA97B369351C56AC
2.1.1     open 0x0
[...]
```

5. FIPS ドライブまたは SED にデータ認証キーを割り当てます。

"FIPS ドライブまたは SED へのデータ認証キーの割り当て (外部キー管理) "

6. 必要に応じて、FIPS 140-2 認証キーを FIPS ドライブに割り当てます。

"FIPS ドライブに FIPS 140-2 認証キーを割り当てています"

**FIPS** ドライブまたは **SED** のデータにアクセスできない状態にします

**FIPS** ドライブまたは **SED** のデータにアクセスできない概要を確認します

FIPS ドライブまたは SED のデータに永久にアクセスできない状態にし、ドライブの未使用スペースは新しいデータに使用できるようにしておく場合は、ディスクを完全消去できます。データに永久にアクセスできない状態にし、ドライブを再利用する必要もない場合は、ディスクを破棄できます。

- ディスク完全消去

自己暗号化ドライブを完全消去すると、ディスク暗号化キーが新しいランダムな値に変更され、電源オンロックの状態が false にリセットされ、キー ID がデフォルト値の Manufacturer Secure ID ( SAS ; メーカーのセキュア ID ) 0x0 ( SAS ドライブ ) または null ( NVMe ドライブ ) に設定されます。これにより、ディスクのデータにアクセスできない状態になり、データを取得できなくなります。完全消去されたディスクは、初期化されていないスペアディスクとして再利用できます。

- ディスクの破棄

FIPS ドライブまたは SED を破棄すると、ディスク暗号化キーが不明なランダム値に設定され、ディスクが完全にロックされます。これにより、ディスクが永続的に使用できない状態になり、ディスクのデータに永久にアクセスできなくなります。

完全消去と破棄は、個々の自己暗号化ドライブまたはノードのすべての自己暗号化ドライブに対して実行でき

ます。

**FIPS** ドライブまたは **SED** を完全消去します

FIPSドライブまたはSEDのデータに永久にアクセスできない状態にして、そのドライブを新しいデータに使用する場合は、`storage encryption disk sanitize` コマンドを使用してドライブを完全消去します。

このタスクについて

自己暗号化ドライブを完全消去すると、ディスク暗号化キーが新しいランダムな値に変更され、電源オンロックの状態が `false` にリセットされ、キー ID がデフォルト値の Manufacturer Secure ID (SAS ; メーカーのセキュア ID) `0x0` (SAS ドライブ) または `null` (NVMe ドライブ) に設定されます。これにより、ディスクのデータにアクセスできない状態になり、データを取得できなくなります。完全消去されたディスクは、初期化されていないスペアディスクとして再利用できます。

作業を開始する前に

このタスクを実行するには、クラスタ管理者である必要があります。

手順

1. 保持する必要があるデータを別のディスク上のアグリゲートにすべて移行します。
2. 完全消去する FIPS ドライブまたは SED のアグリゲートを削除します。

```
storage aggregate delete -aggregate aggregate_name
```

コマンド構文全体については、マニュアルページを参照してください。

```
cluster1::> storage aggregate delete -aggregate aggr1
```

3. 完全消去する FIPS ドライブまたは SED のディスク ID を確認します。

```
storage encryption disk show -fields data-key-id,fips-key-id,owner
```

コマンド構文全体については、マニュアルページを参照してください。

```
cluster1::> storage encryption disk show
Disk      Mode Data Key ID
-----
-----
0.0.0     data
F1CB30AFF1CB30B0010100000000000A68B167F92DD54196297159B5968923C
0.0.1     data
F1CB30AFF1CB30B0010100000000000A68B167F92DD54196297159B5968923C
1.10.2    data
F1CB30AFF1CB30B0010100000000000CF0EFD81EA9F6324EA97B369351C56AC
[...]
```

4. FIPS ドライブが FIPS 準拠モードの場合は、ノードの FIPS 認証キー ID をデフォルトの MSID である 0x0 に戻します。

```
storage encryption disk modify -disk disk_id -fips-key-id 0x0
```

を使用できます security key-manager query キーIDを表示するコマンド。

```
cluster1::> storage encryption disk modify -disk 1.10.2 -fips-key-id 0x0

Info: Starting modify on 1 disk.
      View the status of the operation by using the
      storage encryption disk show-status command.
```

5. ドライブを完全消去します。

```
storage encryption disk sanitize -disk disk_id
```

このコマンドで完全消去できるのは、ホットスペアディスクと破損ディスクのみです。タイプに関係なくすべてのディスクを完全消去するには、を使用します -force-all-state オプションコマンド構文全体については、マニュアルページを参照してください。



続行する前に、確認フレーズの入力を求めるプロンプトがONTAPに表示されます。画面に表示されたフレーズを正確に入力します。

```
cluster1::> storage encryption disk sanitize -disk 1.10.2

Warning: This operation will cryptographically sanitize 1 spare or
broken self-encrypting disk on 1 node.
        To continue, enter sanitize disk: sanitize disk

Info: Starting sanitize on 1 disk.
      View the status of the operation using the
      storage encryption disk show-status command.
```

**FIPS** ドライブまたは **SED** を破棄します

FIPSドライブまたはSEDのデータに永久にアクセスできない状態にし、ドライブを再利用する必要もない場合は、を使用できます storage encryption disk destroy コマンドを使用してディスクを破棄します。

このタスクについて

FIPS ドライブまたは SED を破棄すると、ディスク暗号化キーが不明なランダム値に設定され、ドライブが完全にロックされます。これにより、ディスクが実質的に使用できない状態になり、ディスクのデータに永久にアクセスできなくなります。ただし、ディスクのラベルに印刷されている Physical Secure ID (PSID ; 物理的なセキュア ID) を使用して、ディスクを工場出荷時の設定にリセットすることはできます。詳細については、を参照してください ["認証キーが失われた場合に FIPS ドライブまたは SED を使用可能な状態に戻す"](#)



(故障) ディスク返却不要サービス (NRD Plus) を契約している場合を除き、FIPS ドライブまたは SED は破棄しないでください。ディスクを破棄すると保証が無効になります。

作業を開始する前に

このタスクを実行するには、クラスタ管理者である必要があります。

手順

1. 保持しておく必要のあるデータを別のディスク上のアグリゲートにすべて移行します。
2. 破棄する FIPS ドライブまたは SED のアグリゲートを削除します。

```
storage aggregate delete -aggregate aggregate_name
```

コマンド構文全体については、マニュアルページを参照してください。

```
cluster1::> storage aggregate delete -aggregate aggr1
```

3. 破棄する FIPS ドライブまたは SED のディスク ID を確認します。

```
storage encryption disk show
```

コマンド構文全体については、マニュアルページを参照してください。

```
cluster1::> storage encryption disk show
Disk      Mode Data Key ID
-----
-----
0.0.0     data
F1CB30AFF1CB30B0010100000000000A68B167F92DD54196297159B5968923C
0.0.1     data
F1CB30AFF1CB30B0010100000000000A68B167F92DD54196297159B5968923C
1.10.2    data
F1CB30AFF1CB30B0010100000000000CF0EFD81EA9F6324EA97B369351C56AC
[...]
```

4. ディスクを破棄します。

```
storage encryption disk destroy -disk disk_id
```

コマンド構文全体については、マニュアルページを参照してください。



続行する前に確認のフレーズを入力するように求められます。画面に表示されたフレーズを正確に入力します。

```
cluster1::> storage encryption disk destroy -disk 1.10.2
```

Warning: This operation will cryptographically destroy 1 spare or broken self-encrypting disks on 1 node.

You cannot reuse destroyed disks unless you revert them to their original state using the PSID value.

To continue, enter

destroy disk

:destroy disk

Info: Starting destroy on 1 disk.

View the status of the operation by using the "storage encryption disk show-status" command.

#### FIPSドライブまたはSEDの緊急時のシュレッドデータ

セキュリティに関する緊急事態が発生した場合は、ストレージシステムまたは KMIP サーバへの給電が遮断されていても、FIPS ドライブまたは SED へのアクセスをただちに禁止できます。

作業を開始する前に

- 使用可能な電力がない KMIP サーバを使用している場合は、KMIP サーバで簡単に破棄できる認証アイテム（スマートカードや USB ドライブなど）が設定されている必要があります。
- このタスクを実行するには、クラスタ管理者である必要があります。

ステップ

1. FIPS ドライブまたは SED のデータの緊急時のシュレディングを実行します。

状況	作業
----	----

<p>ストレージシステムに給電されており、ストレージシステムを適切な手順でオフラインにする時間があります</p>	<ol style="list-style-type: none"> <li>ストレージシステムが HA ペアとして構成されている場合は、テイクオーバーを無効にします。</li> <li>すべてのアグリゲートをオフラインにしてから削除します。</li> <li>権限レベルを advanced に設定します。 [+] set -privilege advanced</li> <li>ドライブが FIPS 準拠モードの場合は、ノードの FIPS 認証キー ID をデフォルトの MSID に戻します。 [+] storage encryption disk modify -disk * -fips-key-id 0x0</li> <li>ストレージシステムを停止します。</li> <li>メンテナンスモードでブートします。</li> <li>ディスクを完全消去するか破棄します。 <ul style="list-style-type: none"> <li>ディスクのデータにアクセスできない状態にし、ディスクを再利用できるようにするには、ディスクを完全消去します。 [+] disk encrypt sanitize -all</li> <li>ディスクのデータにアクセスできない状態にし、ディスクを保存する必要もない場合は、ディスクを破棄します。 [+] disk encrypt destroy disk_id1 disk_id2 ...</li> </ul> </li> </ol>	<p>ストレージシステムに給電されており、データをただちにシュレディングする必要があります</p>
--	---	---



<p>a. * ディスク上のデータにアクセスできない状態にし、ディスクを再利用する場合は、ディスクを完全消去します。 *</p> <p>b. ストレージシステムが HA ペアとして構成されている場合は、テイクオーバーを無効にします。</p> <p>c. 権限レベルを advanced に設定します。</p> <pre>set -privilege advanced</pre> <p>d. ドライブが FIPS 準拠モードの場合は、ノードの FIPS 認証キー ID をデフォルトの MSID に戻します。</p> <pre>storage encryption disk modify -disk * -fips-key-id 0x0</pre> <p>e. ディスクを完全消去します。</p> <pre>storage encryption disk sanitize -disk * -force-all-states true</pre>	<p>a. * ディスク上のデータにアクセスできない状態にし、ディスクを保存する必要もない場合は、ディスクを破棄してください： *</p> <p>b. ストレージシステムが HA ペアとして構成されている場合は、テイクオーバーを無効にします。</p> <p>c. 権限レベルを advanced に設定します。</p> <pre>set -privilege advanced</pre> <p>d. ディスクを破棄します。</p> <pre>storage encryption disk destroy -disk * -force-all-states true</pre>	<p>ストレージシステムがパニック状態になります。これで、システムは永続的に無効な状態になり、すべてのデータが消去されます。システムを再度使用するには、再設定する必要があります。</p>
<p>KMIP サーバに給電されているが、ストレージシステムには給電されていない</p>	<p>a. KMIPサーバにログインします。</p> <p>b. アクセスを禁止するデータを含む FIPS ドライブまたは SED に関連付けられているすべてのキーを破棄します。これにより、ストレージシステムからディスク暗号化キーにアクセスできなくなります。</p>	<p>KMIP サーバまたはストレージシステムに給電されていない</p>

コマンド構文全体については、マニュアルページを参照してください。

認証キーが失われた場合に **FIPS** ドライブまたは **SED** を使用可能な状態に戻します

FIPS ドライブまたは SED の認証キーが永久に失われ、KMIP サーバから取得できない場合、FIPS ドライブまたは SED は破損しているとみなされます。ディスクのデータにアクセスしたりリカバリしたりすることはできませんが、SED の未使用スペースをデータに再び使用できるようにすることができます。

作業を開始する前に

このタスクを実行するには、クラスタ管理者である必要があります。

このタスクについて

このプロセスは、FIPS ドライブまたは SED の認証キーが永久に失われてリカバリできないことが確実である場合にのみ使用してください。

ディスクがパーティショニングされている場合、このプロセスを開始する前にパーティショニングされていないディスクである必要があります。



ディスクのパーティショニングを解除するコマンドはdiagレベルでのみ使用でき、ネットアップサポートの指示があった場合にのみ実行してください。続行する前に、**NetApp**サポートに問い合わせることを強くお勧めします。ナレッジベースの記事も参照してください。 ["ONTAP でスペアドライブのパーティショニングを解除する方法"](#)。

手順

- 1. FIPS ドライブまたは SED を使用可能な状態に戻します。

SED の状況	実行する手順
---------	--------

FIPS 準拠モードでないか、FIPS 準拠モードでFIPS キーを使用できません

- a. 権限レベルを advanced に設定します。  
`set -privilege advanced`
- b. FIPSキーをデフォルトのメーカーセキュアIDである0x0にリセットします。  
`storage encryption disk modify -fips-key-id 0x0 -disk disk_id`
- c. 処理が成功したことを確認します。  
`storage encryption disk show-status`  
処理に失敗した場合は、このトピックのPSIDプロセスを使用してください。
- d. 破損ディスクを完全消去します。  
`storage encryption disk sanitize -disk disk_id`  
コマンドを使用して、処理が成功したことを確認します `storage encryption disk show-status` 次の手順に進む前に。
- e. 完全消去したディスクの障害状態を解除します。  
`storage disk unfail -spare true -disk disk_id`
- f. ディスクに所有者が設定されているかどうかを確認します。  
`storage disk show -disk disk_id`  
[+]  
ディスクに所有者がない場合は、所有者を割り当てます。  
`storage disk assign -owner node -disk disk_id`
  - i. 完全消去するディスクを所有するノードのノードシェルに切り替えます。  
  
`system node run -node node_name`  
  
を実行します `disk sanitize release` コマンドを実行します
- g. ノードシェルを終了します。ディスクの障害状態を再度解除します。  
`storage disk unfail -spare true -disk disk_id`
- h. ディスクがスペアとしてアグリゲートで再利用できる状態になったことを確認します。  
`storage disk show -disk disk_id`

FIPS 準拠モードであるが FIPS キーは使用できず、SED の PSID がラベルに印刷されている

- a. ディスクの PSID をディスクラベルで確認します。
- b. 権限レベルを `advanced` に設定します。  
`set -privilege advanced`
- c. ディスクを工場出荷時の設定にリセットします。  
`storage encryption disk revert-to-original-state -disk disk_id -psid disk_physical_secure_id`  
コマンドを使用して、処理が成功したことを確認します `storage encryption disk show-status` 次の手順に進む前に。
- d. ONTAP 9.8P5以前を実行している場合は、次の手順に進みます。ONTAP 9.8P6以降を実行している場合は、完全消去したディスクの障害状態を解除します。  
`storage disk unfail -disk disk_id`
- e. ディスクに所有者が設定されているかどうかを確認します。  
`storage disk show -disk disk_id`  
[+]  
ディスクに所有者がない場合は、所有者を割り当てます。  
`storage disk assign -owner node -disk disk_id`
  - i. 完全消去するディスクを所有するノードのノードシェルに切り替えます。  
  
`system node run -node node_name`  
  
を実行します `disk sanitize release` コマンドを実行します
- f. ノードシェルを終了します。ディスクの障害状態を再度解除します。  
`storage disk unfail -spare true -disk disk_id`
- g. ディスクがスペアとしてアグリゲートで再利用できる状態になったことを確認します。  
`storage disk show -disk disk_id`

コマンド構文全体については、を参照してください ["コマンドリファレンス"](#)。

**FIPS** ドライブまたは **SED** を非保護モードに戻します

FIPS ドライブまたは SED は、ノードの認証キー ID がデフォルト以外の値に設定されている場合にのみ不正アクセスから保護されます。を使用して、FIPSドライブまたはSEDを非保護モードに戻すことができます `storage encryption disk modify` キーIDをデフォルトに設定するコマンド。

HA ペアで暗号化 SAS ドライブまたは NVMe ドライブ（SED、NSE、FIPS）を使用している場合は、システムを初期化する前に、HA ペア内のすべてのドライブでこのプロセスに従う必要があります（ブートオプション 4 または 9）。そうしないと、ドライブを転用した場合にデータが失われる可能性があります。

作業を開始する前に

このタスクを実行するには、クラスタ管理者である必要があります。

## 手順

1. 権限レベルを advanced に設定します。

```
set -privilege advanced
```

2. FIPS ドライブが FIPS 準拠モードの場合は、ノードの FIPS 認証キー ID をデフォルトの MSID である 0x0 に戻します。

```
storage encryption disk modify -disk disk_id -fips-key-id 0x0
```

を使用できます security key-manager query キーIDを表示するコマンド。

```
cluster1::> storage encryption disk modify -disk 2.10.11 -fips-key-id 0x0
```

```
Info: Starting modify on 14 disks.  
View the status of the operation by using the  
storage encryption disk show-status command.
```

次のコマンドで、処理が成功したことを確認します。

```
storage encryption disk show-status
```

show -statusコマンドを繰り返して、「Disksでした」と「Disks done」の番号が同じになるようにします。

```
cluster1:: storage encryption disk show-status
```

	FIPS	Latest	Start		Execution	Disks	
Disks	Disks						
Node	Support	Request	Timestamp		Time (sec)	Begun	
Done	Successful						
-----	-----	-----	-----		-----	-----	
-----	-----						
cluster1	true	modify	1/18/2022 15:29:38		3	14	5
5							

1 entry was displayed.

3. ノードのデータ認証キー ID をデフォルトの MSID である 0x0 に戻します。

```
storage encryption disk modify -disk disk_id -data-key-id 0x0
```

の値 -data-key-id SASドライブまたはNVMeドライブを非保護モードに戻すかどうかに関係なく、0x0 に設定する必要があります。

を使用できます security key-manager query キーIDを表示するコマンド。

```
cluster1::> storage encryption disk modify -disk 2.10.11 -data-key-id 0x0
```

```
Info: Starting modify on 14 disks.  
View the status of the operation by using the  
storage encryption disk show-status command.
```

次のコマンドで、処理が成功したことを確認します。

```
storage encryption disk show-status
```

番号が同じになるまで、`show -status` コマンドを繰り返します。「disks begin」と「disks done」の数値が同じであれば、処理は完了です。

#### メンテナンスモード

ONTAP 9.7以降では、FIPSドライブのキーを保守モードから変更できます。保守モードは、前のセクションのONTAP CLI手順を使用できない場合にのみ使用してください。

#### 手順

1. ノードのFIPS認証キーIDをデフォルトのMSIDである0x0に戻します。

```
disk encrypt rekey_fips 0x0 disklist
```

2. ノードのデータ認証キー ID をデフォルトの MSID である 0x0 に戻します。

```
disk encrypt rekey 0x0 disklist
```

3. FIPS認証キーのキーが変更されたことを確認します。

```
disk encrypt show_fips
```

4. データ認証キーのキーが変更されたことを確認します。

```
disk encrypt show
```

出力には、デフォルトのMSID 0x0キーIDまたはキーサーバが保持する64文字の値が表示される可能性があります。。 `Locked?` フィールドはデータロックを表します。

Disk	FIPS Key ID	Locked?
0a.01.0	0x0	Yes

外部キー管理ツールの接続を削除します

KMIP サーバが不要になったときはノードから切断できます。たとえば、ボリューム暗

号化に移行する場合は KMIP サーバを切断できます。

このタスクについて

HA ペアのいずれかのノードから KMIP サーバを切断すると、自動的にすべてのクラスタノードからサーバが切断されます。



KMIP サーバを切断したあとも外部キー管理を引き続き使用する場合は、別の KMIP サーバから認証キーを提供できることを確認してください。

作業を開始する前に

このタスクを実行するには、クラスタ管理者または SVM の管理者である必要があります。

ステップ

1. 現在のノードから KMIP サーバを切断します。

ONTAP バージョン	使用するコマンド
ONTAP 9.6 以降	<code>`security key-manager external remove-servers -vserver SVM -key -servers host_name</code>
IP_address:port,...`	ONTAP 9.5 以前

MetroCluster 環境では、管理SVMの両方のクラスタで上記のコマンドを繰り返す必要があります。

コマンド構文全体については、マニュアルページを参照してください。

次のONTAP 9.6のコマンドは、に対する2つの外部キー管理サーバへの接続を無効にします cluster1、最初の名前 `ks1` では、デフォルトポート5696をリッスンしています。2番目のポートはIPアドレス10.0.0.20で、ポート24482をリッスンしています。

```
cluster1::> security key-manager external remove-servers -vserver  
cluster-1 -key-servers ks1,10.0.0.20:24482
```

外部キー管理サーバのプロパティを変更します

ONTAP 9.6以降では、`security key-manager external modify-server` コマンドを使用して、外部キー管理サーバのI/Oタイムアウトとユーザ名を変更します。

作業を開始する前に

- このタスクを実行するには、クラスタ管理者または SVM の管理者である必要があります。
- このタスクを実行するには advanced 権限が必要です。
- MetroCluster 環境では、管理SVMの両方のクラスタで上記の手順を繰り返す必要があります。

手順

1. ストレージシステムで、advanced 権限レベルに切り替えます。

```
set -privilege advanced
```

## 2. クラスタの外部キー管理サーバのプロパティを変更します。

```
security key-manager external modify-server -vserver admin_SVM -key-server  
host_name|IP_address:port,... -timeout 1...60 -username user_name
```



タイムアウト値は秒単位で表されます。ユーザ名を変更すると、新しいパスワードの入力を求められます。クラスタのログインプロンプトでコマンドを実行すると、`admin_SVM` デフォルトでは、現在のクラスタの管理SVMが使用されます。外部キー管理サーバのプロパティを変更するには、クラスタ管理者である必要があります。

次のコマンドは、のタイムアウト値を45秒に変更します `cluster1` デフォルトポート5696をリスンしている外部キー管理サーバ：

```
cluster1::> security key-manager external modify-server -vserver  
cluster1 -key-server ks1.local -timeout 45
```

## 3. SVM の外部キー管理サーバのプロパティを変更します（NVE のみ）。

```
security key-manager external modify-server -vserver SVM -key-server  
host_name|IP_address:port,... -timeout 1...60 -username user_name
```



タイムアウト値は秒単位で表されます。ユーザ名を変更すると、新しいパスワードの入力を求められます。SVMのログインプロンプトでコマンドを実行すると、`SVM` デフォルトは現在のSVMです。外部キー管理サーバのプロパティを変更するには、クラスタ管理者または SVM 管理者である必要があります。

のユーザ名とパスワードを変更するコマンドの例を次に示します `svm1` デフォルトポート5696をリスンしている外部キー管理サーバ：

```
svm1::> security key-manager external modify-server -vserver svm11 -key  
-server ks1.local -username svm1user  
Enter the password:  
Reenter the password:
```

## 4. 最後の手順をその他の SVM に対して繰り返します。

オンボードキー管理から外部キー管理に移行

オンボードキー管理から外部キー管理に切り替える場合は、外部キー管理を有効にする前にオンボードキー管理の設定を削除する必要があります。

作業を開始する前に

- ハードウェアベースの暗号化の場合は、すべての FIPS ドライブまたは SED のデータキーをデフォルト値にリセットする必要があります。



"FIPS ドライブまたは SED を非保護モードに戻します"

- ソフトウェアベースの暗号化では、すべてのボリュームの暗号化を解除する必要があります。

"ボリュームデータの暗号化を解除します"

- このタスクを実行するには、クラスタ管理者である必要があります。

#### ステップ

1. クラスタのオンボードキー管理の設定を削除します。

ONTAP バージョン	使用するコマンド
ONTAP 9.6 以降	<code>security key-manager onboard disable -vserver SVM</code>
ONTAP 9.5 以前	<code>security key-manager delete-key-database</code>

コマンド構文全体については、を参照してください ["ONTAP のマニュアルページ"](#)。

外部キー管理からオンボードキー管理に移行します

外部キー管理からオンボードキー管理に切り替える場合は、オンボードキー管理を有効にする前に外部キー管理の設定を削除する必要があります。

作業を開始する前に

- ハードウェアベースの暗号化の場合は、すべての FIPS ドライブまたは SED のデータキーをデフォルト値にリセットする必要があります。

"FIPS ドライブまたは SED を非保護モードに戻します"

- すべての外部キー管理ツールの接続を削除しておく必要があります。

"外部キー管理ツールの接続を削除しています"

- このタスクを実行するには、クラスタ管理者である必要があります。

#### 手順

キー管理の移行手順は、使用しているONTAPのバージョンによって異なります。

## ONTAP 9.6 以降

1. advanced 権限レベルに切り替えます。

```
set -privilege advanced
```

2. 次のコマンドを使用します。

```
security key-manager external disable -vserver admin_SVM
```



MetroCluster 環境の場合は、管理SVMの両方のクラスタでコマンドを繰り返す必要があります。

## ONTAP 9.5 以前

次のコマンドを使用します。

```
security key-manager delete-kmip-config
```

ブートプロセス時にキー管理サーバにアクセスできない場合

ブートプロセス時に NSE 用に構成されたストレージシステムが指定されたどのキー管理サーバにもアクセスできない場合、ONTAP ではストレージシステムの望ましくない動作を回避するために、特定の予防措置を取ります。

ストレージシステムが NSE 用に設定されている場合、SED のキーが変更されてロックされ、SED の電源がオンになっているときは、ストレージシステムは、キー管理サーバから必要な認証キーを取得して SED に対して自身を認証し、データにアクセスできるようにする必要があります。

ストレージシステムは、指定されたキー管理サーバへのアクセスを最大 3 時間試行します。その時間が経過してもストレージシステムがどのキー管理サーバにもアクセスできない場合は、ブートプロセスが停止して、ストレージシステムも停止します。

ストレージシステムが指定されたいずれかのキー管理サーバに正常にアクセスできた場合は、SSL 接続の確立を最大 15 分間試行します。ストレージシステムが指定されたどのキー管理サーバとも SSL 接続を確立できない場合は、ブートプロセスが停止して、ストレージシステムも停止します。

ストレージシステムがキー管理サーバへのアクセスと接続を試行している間、失敗したアクセス試行に関する詳細情報が CLI に表示されます。アクセスの試行は、Ctrl+C キーを押すことによっていつでも中断できます

SED では、セキュリティ対策として、無許可のアクセス試行回数が制限されています。試行回数が上限に達すると、既存データへのアクセスが無効になります。ストレージシステムが指定されたどのキー管理サーバにもアクセスできず、適切な認証キーを取得できない場合は、デフォルトのキーを使用した認証のみ試行できます。この場合、認証が失敗したり、パニック状態になったりします。パニック状態になった場合に自動的にリブートするように設定されているストレージシステムはブートループに入り、SED での認証が連続して失敗します。

仕様では、次のような場合にストレージシステムを停止して、認証の連続失敗回数の上限を超えたことが原因で SED が永続的にロックされても、ストレージシステムがブートループに入ったり、意図しないデータ損失が発生したりすることを回避します。ロックアウト保護の制限とタイプは、SED の仕様とタイプによって異なります。

SEDタイプ	ロックアウトされるまでの認証の連続失敗回数	安全制限に達したときのロックアウト保護タイプ
HDD	一、〇二四	永続的。適切な認証キーが再び使用可能になった場合でも、データをリカバリできません。
ファームウェアバージョンがNA00 または NA01 の X440_PHM2800MCTO 800GB NSE SSD	5.	一時的。ロックアウトが有効になるのは、ディスクの電源が再投入されるまでです。
ファームウェアバージョンがNA00またはNA01のX577_PHM2800MCTO 800GB NSE SSD	5.	一時的。ロックアウトが有効になるのは、ディスクの電源が再投入されるまでです。
ファームウェアバージョンが上記よりも高い X440_PHM2800MCTO 800GB NSE SSD	一、〇二四	永続的。適切な認証キーが再び使用可能になった場合でも、データをリカバリできません。
ファームウェアバージョンが上位のX577_PHM2800MCTO 800GB NSE SSD	一、〇二四	永続的。適切な認証キーが再び使用可能になった場合でも、データをリカバリできません。
その他すべての SSD モデル	一、〇二四	永続的。適切な認証キーが再び使用可能になった場合でも、データをリカバリできません。

すべての SED タイプでは、認証が成功すると試行回数が 0 にリセットされます。

ストレージシステムが指定されたどのキー管理サーバにもアクセスできないために停止した場合は、引き続きストレージシステムのブートを試行する前に、通信エラーの原因を特定して修正しておく必要があります。

暗号化をデフォルトで無効にする

ONTAP 9.7 以降では、ボリューム暗号化（VE）ライセンスがあり、オンボードキーマネージャまたは外部キーマネージャを使用している場合、アグリゲートとボリューム暗号化がデフォルトで有効になります。必要に応じて、暗号化をデフォルトでクラスタ全体で無効にすることができます。

作業を開始する前に

このタスクを実行するには、クラスタ管理者であるか、クラスタ管理者から権限を委譲された SVM 管理者である必要があります。

ステップ

1. ONTAP 9.7 以降のクラスタ全体で暗号化をデフォルトで無効にするには、次のコマンドを実行します。

```
options -option-name encryption.data_at_rest_encryption.disable_by_default  
-option-value on
```

# データ保護とディザスタリカバリ

## System Manager によるデータ保護

### System Manager によるデータ保護の概要

このセクションのトピックでは、ONTAP 9.7 以降のリリースの System Manager を使用してデータ保護を設定および管理する方法について説明します。

ONTAP 9.7以前のシステムでSystem Managerを使用している場合は、を参照してください ["ONTAP System Manager Classic のドキュメント"](#)

Snapshot コピー、ミラー、バックアップ、ミラーとバックアップ関係を作成および管理して、データを保護します。

SnapMirror は、地理的に離れたサイトのプライマリストレージからセカンダリストレージへのフェイルオーバー用に設計されたディザスタリカバリテクノロジーです。名前のとおり、SnapMirror はセカンダリストレージに作業データのレプリカ（ミラー）を作成します。プライマリサイトで災害が発生した場合でも、セカンダリストレージからデータを引き続き提供できます。

a\_vault\_ は、基準への準拠およびその他のガバナンス関連の目的で、ディスクツーディスクの Snapshot コピーレプリケーションを実現するように設計されています。SnapMirror 関係では、通常、ソースボリューム内の Snapshot コピーだけがデスティネーションに含まれますが、SnapVault デスティネーションはより長期間にわたって作成されたポイントインタイムの Snapshot コピーを保持します。

ONTAP 9.10.1 以降では、S3 SnapMirror を使用して S3 バケット間にデータ保護関係を作成できます。デスティネーションバケットは、ローカルまたはリモートの ONTAP システム、あるいは StorageGRID や AWS などの ONTAP 以外のシステムで使用できます。詳細については、を参照してください ["S3 SnapMirror の概要"](#)。

### カスタムのデータ保護ポリシーを作成する

既存のデフォルトの保護ポリシーがニーズに適していない場合は、System Manager でカスタムのデータ保護ポリシーを作成できます。ONTAP 9.11.1以降では、System Managerを使用して、カスタムのミラーポリシーとバックアップポリシーを作成し、古いポリシーを表示して選択できます。この機能は、ONTAP 9.8のONTAP 9.8P12以降のパッチでも使用できます。

ソースクラスタとデスティネーションクラスタの両方にカスタムの保護ポリシーを作成する。

#### 手順

1. [\* Protection] > [Local Policy Settings] をクリックします。
2. [\* 保護ポリシー \*] で、をクリックします →。
3. [\* 保護ポリシー \*] ペインで、をクリックします + Add。
4. 新しいポリシー名を入力し、ポリシーの範囲を選択します。
5. ポリシータイプを選択します。バックアップ専用ポリシーまたはミラーのみのポリシーを追加するには、\*非同期\*を選択し、\*従来のポリシータイプを使用\*をクリックします。

6. 必須フィールドに入力します。
7. [ 保存 ( Save ) ] をクリックします。
8. もう一方のクラスタで同じ手順を繰り返します。

## Snapshot コピーを設定します

Snapshot コピーポリシーを作成して、自動的に作成される Snapshot コピーの最大数と頻度を指定できます。このポリシーは、Snapshot コピーを作成するタイミング、保持するコピーの数、および Snapshot コピーに名前を付ける方法を指定します。

この手順で作成されるのは、ローカルクラスタのみです。

### 手順

1. [ 保護 ]、[ 概要 ]、[ ローカルポリシーの設定 ] の順にクリックします。
2. [\* Snapshot Policies\*]( スナップショットポリシー ) で、をクリックします → をクリックし、をクリックします + Add。
3. ポリシー名を入力し、ポリシースコープを選択して、\* Schedules \* ( スケジュール \* ) でをクリックします + Add スケジュールの詳細を入力します。

## Snapshot コピーを削除する前に再利用可能なスペースを計算します

ONTAP 9.10.1 以降の System Manager を使用して、削除する Snapshot コピーを選択し、削除前に再利用可能なスペースを計算できます。

### 手順

1. [ ストレージ ]、[ ボリューム ] の順にクリックします。
2. Snapshot コピーを削除するボリュームを選択します。
3. 「\* Snapshot copies \*」をクリックします。
4. 1 つ以上の Snapshot コピーを選択します。
5. [ 再計算可能スペースを計算 ( Calculate Reclaimable Space ) ] をクリックします。

## Snapshot コピーディレクトリへのクライアントアクセスを有効または無効にします


ONTAP 9.10.1 以降の System Manager を使用して、クライアントシステムからボリューム上の Snapshot コピーディレクトリへのアクセスを有効または無効にすることができます。アクセスを有効にすると、Snapshot コピーディレクトリがクライアントに表示されるようになります。また、Windows クライアントは、ドライブを Snapshot コピーディレクトリにマッピングして、その内容を表示およびアクセスできるようになります。

ボリュームの Snapshot コピーディレクトリへのアクセスを有効または無効にするには、ボリュームの設定を編集するか、ボリュームの共有設定を編集します。

ボリュームを編集して、**Snapshot** コピーディレクトリへのクライアントアクセスを有効または無効にします

デフォルトでは、ボリューム上の Snapshot コピーディレクトリにクライアントからアクセスできます。


手順

1. [ストレージ]、[ボリューム]の順にクリックします。
2. 表示または非表示にする Snapshot コピーディレクトリが含まれているボリュームを選択します。
3. をクリックします  をクリックし、\* Edit \* を選択します。
4. 「\* Snapshot Copies (Local) Settings \*」セクションで、「\* Show the Snapshot copies directory to clients \*」を選択または選択解除します。
5. [保存 (Save)] をクリックします。

共有を編集して、**Snapshot** コピーディレクトリへのクライアントアクセスを有効または無効にします

デフォルトでは、ボリューム上の Snapshot コピーディレクトリにクライアントからアクセスできます。

手順

1. [\* ストレージ]、[共有]の順にクリックします。
2. 表示または非表示にする Snapshot コピーディレクトリが含まれているボリュームを選択します。
3. をクリックします  をクリックし、\* Edit \* を選択します。
4. 「\* 共有プロパティ \*」セクションで、「\* クライアントによる Snapshot コピー・ディレクトリへのアクセスを許可する」を選択または選択解除します。
5. [保存 (Save)] をクリックします。

## ミラーとバックアップを準備

データをリモートクラスタにレプリケートして、データのバックアップやディザスタリカバリを目的としてデータを保護することができます。




いくつかのデフォルトの保護ポリシーが用意されています。カスタムポリシーを使用する場合は、保護ポリシーを作成しておく必要があります。



手順

1. ローカルクラスタで、\* Protection > Overview \* をクリックします。
2. 「\* クラスタ間設定 \*」を展開します。Add Network Interfaces \* をクリックして、クラスタのクラスタ間ネットワークインターフェイスを追加します。

リモートクラスタでこの手順を繰り返します。

3. リモートクラスタで、[\* Protection] > [Overview] をクリックします。をクリックします  [ クラスタピア ] セクションで、[ パスフレーズの生成 ] をクリックします。
4. 生成されたパスフレーズをコピーしてローカルクラスタに貼り付けます。
5. ローカルクラスタで、[ クラスタピア ] の下の [\* ピアクラスタ \*] をクリックし、ローカルクラスタとリモートクラスタをピアリングします。
6. 必要に応じて、Storage VM peers の下で、をクリックします  さらに \* Storage VM\* をピアリングして、Storage VM のピアリングを行います。
7. Protect Volumes] をクリックしてボリュームを保護します。LUN を保護するには、\* Storage > LUNs \* をクリックし、保護する LUN を選択して、をクリックします  Protect。

必要なデータ保護のタイプに基づいて保護ポリシーを選択します。

8. ボリュームと LUN がローカルクラスタから正常に保護されていることを確認するには、\* Storage > Volumes \* または \* Storage > LUNs \* をクリックし、ボリュームと LUN の表示を展開します。

## ONTAP でこれを行うその他の方法

実行するタスク	参照するコンテンツ
System Manager Classic （ ONTAP 9.7 以前で使用可能）	<a href="#">"ボリュームのディザスタリカバリの準備の概要"</a>
ONTAP のコマンドラインインターフェイス	<a href="#">"クラスタピア関係を作成"</a>

## ミラーとバックアップを設定します

ボリュームのミラーとバックアップを作成し、災害時にデータを保護し、アーカイブされた複数のバージョンのデータをロールバックできるようにします。ONTAP 9.11.1以降では、System Managerを使用して、事前に作成されたミラーポリシーやカスタムのミラーポリシーやバックアップポリシーを選択したり、古いポリシーを表示および選択したり、ボリュームやStorage VMを保護する際に保護ポリシーに定義された転送スケジュールを上書きしたりできます。この機能は、ONTAP 9.8のONTAP 9.8P12以降のパッチでも使用できます。




ONTAP 9.8P12以降のONTAP 9.8パッチリリースを使用しており、System Managerを使用してSnapMirrorを設定している場合、ONTAP 9.9.1またはONTAP 9.10.1リリースにアップグレードする場合は、ONTAP 9.9.1P13以降およびONTAP 9.10.1P10以降のパッチリリースを使用する必要があります。

この手順は、リモートクラスタにデータ保護ポリシーを作成します。ソースクラスタとデスティネーションクラスタは、クラスタ間ネットワークインターフェイスを使用してデータを交換します。手順は、を想定しています ["クラスタ間ネットワークインターフェイスが作成され、ボリュームを含むクラスタ間にピア関係が設定されます"](#)（ペア）。また、データ保護用に Storage VM をピアリングすることもできます。ただし、Storage VM がピア関係になく、権限が有効になっている場合、保護関係の作成時に Storage VM が自動的にピア関係に設定されます。





## 手順

1. 保護するボリュームまたは LUN を選択します。 \* Storage > Volumes \* または \* Storage > LUNs \* をクリックし、目的のボリュームまたは LUN 名をクリックします。
2. をクリックします  **Protect**。
3. デスティネーションクラスタと Storage VM を選択してください。
4. デフォルトでは非同期ポリシーが選択されます。同期ポリシーを選択するには、 \* その他のオプション \* をクリックします。
5. **[Protect]**( 保護 ) をクリックします
6. 選択したボリュームまたは LUN の \* SnapMirror (ローカルまたはリモート) \* タブをクリックして、保護が正しく設定されていることを確認します。

## 関連情報

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

## ONTAP でこれを行うその他の方法


実行するタスク	参照するコンテンツ
System Manager Classic ( ONTAP 9.7 以前で使用可能)	<a href="#">"SnapVault によるボリュームのバックアップの概要"</a>
ONTAP のコマンドラインインターフェイス	<a href="#">"レプリケーション関係を作成"</a>

## 保護関係を再同期する

災害発生後に元のソースボリュームを再び使用できるようになったら、デスティネーションボリュームからデータを再同期し、保護関係を再確立できます。

この手順は非同期関係にある元のソースボリュームのデータを置き換えるため、元のソースボリュームからデータの提供を再開して元の保護関係を再開できます。

## 手順


1. [ \* 保護 ]、[ 関係 ] の順にクリックし、再同期する切断された関係をクリックします。
2. をクリックします  次に、 \* Resync \* を選択します。
3. 「 \* Relationships 」で、再同期の進捗状況を監視します。再同期が完了すると、状態が「 Mirrored 」に変わります。

## 以前の **Snapshot** コピーからボリュームをリストアします

ボリューム内のデータが失われた場合や破損した場合、以前の Snapshot コピーからリストアすることでデータをロールバックできます。

この手順は、ソースボリューム上の現在のデータを、以前のバージョンの Snapshot コピーのデータで置き換えます。このタスクはデスティネーションクラスタで実行する必要があります。

手順

1. [ 保護 ]、[ 関係 ] の順にクリックし、ソースボリューム名をクリックします。
2. をクリックします  次に、 [ \* Restore ] を選択します。
3. ソースボリュームは、 \* Source \* でデフォルトで選択されます。ソース以外のボリュームを選択する場合は、「 \* その他のボリューム 」をクリックします。
4. 「 \* Destination \* 」で、リストアする Snapshot コピーを選択します。
5. ソースとデスティネーションが異なるクラスタにある場合は、リモートクラスタで、 \* Protection > Relationships \* をクリックしてリストアの進捗状況を監視します。

ONTAP でこれを行うその他の方法


実行するタスク	参照するコンテンツ
System Manager Classic （ ONTAP 9.7 以前で使用可能）	<a href="#">"SnapVault によるボリュームリストアの概要"</a>
ONTAP のコマンドラインインターフェイス	<a href="#">"SnapMirror デスティネーションからボリュームの内容をリストアします"</a>

Snapshot コピーからリカバリします

Snapshot コピーからリストアすることにより、ボリュームを以前の時点にリカバリできます。

この手順は、 Snapshot コピーからボリュームをリストアします。

手順


1. [ \* ストレージ ] をクリックし、ボリュームを選択します。
2. 「 \* Snapshot copies \* 」の下のをクリックします  リストアする Snapshot コピーの横にある \* Restore \* を選択します。

新しいボリュームにリストアします

ONTAP 9.8 以降では、 System Manager を使用して、デスティネーションボリューム上にバックアップされたデータを元のソース以外のボリュームにリストアできます。

別のボリュームにリストアする場合は、既存のボリュームを選択するか、新しいボリュームを作成できます。

手順

1. 適切な保護関係を選択します。 \* Protection > Relationships \* をクリックします。
2. をクリックします  をクリックし、 \* リストア \* をクリックします。
3. 「 \* ソース 」セクションで「 \* その他のボリューム 」を選択し、クラスタと Storage VM を選択します。
4. 既存のボリュームを選択するか、 \* 新しいボリュームを作成する \* を選択します。

5. 新しいボリュームを作成する場合は、ボリューム名を入力します。
6. 「\* Destination \*」セクションで、リストアするSnapshotコピーを選択します。
7. [ 保存 ( Save ) ] をクリックします。
8. 「\* Relationships \*」で、関係の「\* Transfer Status \*」を表示してリストアの進捗状況を監視します。

## 保護関係の逆再同期


ONTAP 9.8 以降では、System Manager を使用して逆再同期操作を実行し、既存の保護関係を削除して、ソースボリュームとデスティネーションボリュームの機能を切り替えることができます。次に、デスティネーションボリュームでデータを提供しながら、ソースを修理または交換し、ソースを更新して、システムの元の構成を再確立します。



System Managerでは、クラスタ内の関係との逆再同期はサポートされません。クラスタ内の関係に対する逆再同期処理は、ONTAP CLIを使用して実行できます。

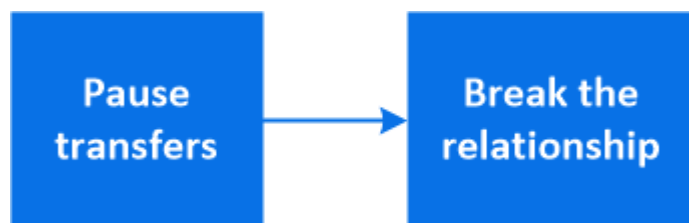
逆再同期処理を実行すると、共通の Snapshot コピーのデータよりも新しいソースボリューム上のデータはすべて削除されます。

### 手順


1. 適切な保護関係を選択します。\* Protection > Relationships \* をクリックします。
2. をクリックします  をクリックし、\* 逆再同期 \* をクリックします。
3. 「\* Relationships \*」で、関係の「\* Transfer Status \*」を表示して、逆再同期の進捗を監視します。

## SnapMirror デスティネーションからのデータの提供

ソースが使用できなくなったときにミラーデスティネーションからデータを提供するには、デスティネーションへのスケジュールされた転送を停止してから、SnapMirror 関係を解除してデスティネーションを書き込み可能にします。



### 手順

1. 保護関係を選択します。\* Protection > Relationships \* をクリックし、目的のボリューム名をクリックします。
2. をクリックします .
3. スケジュールされた転送を停止するには、\* Pause \* をクリックします。
4. 宛先を書き込み可能にします。\* Break \* をクリックします。
5. メインの \* 関係 \* ページに移動して、関係の状態が「切断」と表示されていることを確認します。

次のステップ：

無効にしたソースボリュームが再び使用可能になったら、関係を再同期して、現在のデータを元のソースボリュームにコピーする必要があります。元のソースボリュームのデータは、このプロセスで置き換えられます。

**ONTAP** でこれを行うその他の方法

実行するタスク	参照するコンテンツ
System Manager Classic （ ONTAP 9.7 以前で使用可能）	<a href="#">"ボリュームディザスタリカバリの概要"</a>
ONTAP のコマンドラインインターフェイス	<a href="#">"デスティネーションボリュームをアクティブ化"</a>

## Storage VM ディザスタリカバリを設定

System Manager を使用して、Storage VM ディザスタリカバリ（Storage VM DR）関係を作成して、Storage VM の構成を相互にレプリケートできます。プライマリサイトで災害が発生した場合に、デスティネーション Storage VM を迅速にアクティブ化できます。

デスティネーションからこの手順を作成します。ソースStorage VMでSMBを設定している場合などに新しい保護ポリシーを作成する必要がある場合は、System Managerを使用してポリシーを作成し、【保護ポリシーの追加】\*ウィンドウで[Identity preserve]\*オプションを選択します。詳細については、を参照してください ["カスタムのデータ保護ポリシーを作成する"](#)。


手順

1. デスティネーションクラスターで、\* Protection > Relationships \* をクリックします。
2. **[Relationships]** ( リレーションシップ ) で、**[Protect]** ( 保護 ) をクリックし、**[Storage VM(DR)]** を選択します。
3. 保護ポリシーを選択します。カスタムの保護ポリシーを作成した場合は、ポリシーを選択し、レプリケートするソースクラスターと Storage VM を選択します。新しい Storage VM 名を入力して、新しいデスティネーション Storage VM を作成することもできます。
4. [ 保存（ Save ） ] をクリックします。

## SVM DR デスティネーションからのデータの提供

ONTAP 9.8以降では、System Managerを使用して、災害発生後にデスティネーションStorage VMをアクティブ化できます。デスティネーションStorage VMをアクティブ化すると、SVMデスティネーションボリュームが書き込み可能になり、クライアントにデータを提供できるようになります。

手順

1. ソースクラスターにアクセスできる場合は、SVMが停止していることを確認します。\* Storage > Storage VM\*に移動し、SVMの\* State \*列を確認します。
2. ソースSVMの状態が「running」の場合は、停止します。select  「\*停止」を選択します。
3. デスティネーションクラスターで、目的の保護関係を探します。\* Protection > Relationships \*に移動します。

4. をクリックします  デスティネーション Storage VM のアクティブ化\* を選択します。

## ソース **Storage VM** を再アクティブ化


ONTAP 9.8 以降では、災害発生後に System Manager を使用してソース Storage VM を再アクティブ化できます。ソース Storage VM を再アクティブ化すると、デスティネーション Storage VM が停止し、ソースからデスティネーションへのレプリケーションが再度有効化されます。

このタスクについて

ソース Storage VM を再アクティブ化すると、System Manager によって次の処理がバックグラウンドで実行されます。

- SnapMirror resync を使用して、元のデスティネーションから元のソースへの反転 SVM DR 関係を作成します
- デスティネーション SVM を停止します
- SnapMirror 関係を更新します
- SnapMirror 関係を解除します
- 元の SVM を再起動します
- 元のソースから元のデスティネーションへの SnapMirror 再同期を実行します
- SnapMirror 関係をクリーンアップします

手順

1. 適切な保護関係を選択します。\* Protection > Relationships \* をクリックします。
2. をクリックします  をクリックし、\* Reactivate Source Storage VM \* をクリックします。
3. [\* 関係 \*] で、保護関係の [\* 転送ステータス \*] を表示して、ソースの再アクティブ化の進行状況を監視します。

## デスティネーション **Storage VM** を再同期

ONTAP 9.8 以降では、System Manager を使用して、ソース Storage VM のデータおよび設定の詳細を、解除した保護関係のデスティネーション Storage VM に再同期し、関係を再確立できます。

ONTAP 9.11.1 では、災害復旧のリハーサルを実行するときにデータウェアハウスの完全な再構築をバイパスするオプションが導入されており、本番環境に戻すまでの時間を短縮できます。

再同期処理は元の関係のデスティネーションからのみ実行できます。再同期を実行すると、ソース Storage VM のデータよりも新しいデスティネーション Storage VM のデータがすべて削除されます。

手順

1. 適切な保護関係を選択します。\* Protection > Relationships \* をクリックします。
2. 必要に応じて、[クイック再同期を実行する] を選択すると、災害復旧のリハーサル時にデータウェアハウスの完全な再構築をバイパスできます。

3. をクリックします  をクリックし、\* Resync \* をクリックします。
4. 「\* Relationships \*」で、関係の「\* Transfer Status \*」を表示して、再同期の進捗状況を監視します。

## SnapMirror を使用してデータをクラウドにバックアップ

ONTAP 9.9.1以降では、System Managerを使用して、クラウドにデータをバックアップしたり、クラウドストレージから別のボリュームにデータをリストアしたりできます。ONTAP または StorageGRID S3 をクラウドオブジェクトストアとして使用できます。


SnapMirrorクラウド機能を使用する前に、ネットアップサポートサイトからSnapMirror Cloud APIライセンスキーを要求する必要があります。"[SnapMirror Cloud APIライセンスキーを申請します](#)"。

指示に従って、ビジネスチャンスの簡単な概要を入力し、指定されたEメールアドレスにEメールを送信してAPIキーを要求します。24時間以内に応答するEメールと、APIキーの入手方法に関する詳しい説明が記載されています。

### クラウドオブジェクトストアを追加します

SnapMirror クラウドバックアップを設定する前に、StorageGRID または ONTAP S3 クラウドオブジェクトストアを追加する必要があります。

#### 手順

1. [保護]、[概要]、[クラウドオブジェクトストア\*]の順にクリックします。
2. をクリックします  Add。

### デフォルトのポリシーを使用してバックアップします

デフォルトのクラウド保護ポリシーである DailyBackup を使用して、既存のボリュームの SnapMirror Cloud バックアップを簡単に設定できます。

#### 手順

1. [保護]、[概要]の順にクリックし、[クラウドへのボリュームのバックアップ\*]を選択します。
2. 初めてクラウドにバックアップする場合は、ライセンスのフィールドに次のように SnapMirror Cloud API ライセンスキーを入力します。
3. [\* Authenticate and Continue] をクリックします。\*
4. ソースボリュームを選択
5. クラウドオブジェクトストアを選択します。
6. [保存 (Save)] をクリックします。

### カスタムクラウドバックアップポリシーを作成する

SnapMirror クラウドバックアップにデフォルトの DailyBackup クラウドポリシーを使用しない場合は、独自のポリシーを作成できます。

#### 手順

1. [保護]、[概要]、[ローカルポリシーの設定]の順にクリックし、[保護ポリシー\*]を選択します。



2. [ \* 追加 ] をクリックし、新しいポリシーの詳細を入力します。
3. [ \* ポリシータイプ \* ] セクションで、 [ クラウドにバックアップ ] を選択してクラウドポリシーを作成していることを示します。
4. [ 保存 ( Save ) ] をクリックします。

#### [ \* Volumes ] ページからバックアップを作成します

System Manager \* Volumes \* ページでは、複数のボリュームのクラウドバックアップを一度に選択して作成する場合や、カスタムの保護ポリシーを使用する場合に使用できます。

##### 手順

1. [ ストレージ ]、[ ボリューム ] の順にクリックします。
2. クラウドにバックアップするボリュームを選択し、 \* Protect \* をクリックします。
3. [ \* Protect Volume ] (ボリュームの保護) ウィンドウで、 [ \* More Options \* (その他のオプション) ] をクリックします。
4. ポリシーを選択します。


デフォルトポリシー、 DailyBackup 、または作成したカスタムクラウドポリシーを選択できます。

5. クラウドオブジェクトストアを選択します。
6. [ 保存 ( Save ) ] をクリックします。

#### クラウドからリストアします

System Manager を使用して、クラウドストレージからソースクラスタ上の別のボリュームにバックアップしたデータをリストアできます。


##### 手順

1. [ ストレージ ]、[ ボリューム ] の順にクリックします。
2. [ クラウドにバックアップ \* ] タブを選択します。
3. をクリックします  をクリックし、リストアするソースボリュームの横にある \* Restore \* を選択します。
4. 「 \* Source \* 」で Storage VM を選択し、データのリストア先となるボリュームの名前を入力します。
5. 「 \* Destination \* 」で、リストアする Snapshot コピーを選択します。
6. [ 保存 ( Save ) ] をクリックします。

#### SnapMirror クラウド関係を削除します

System Manager を使用してクラウド関係を削除できます。

##### 手順


1. [ \* ストレージ ]、[ ボリューム ] の順にクリックし、削除するボリュームを選択します。
2. をクリックします  をクリックし、 \* Delete \* を選択します。
3. クラウドオブジェクトストアエンドポイントを削除する場合は、 \* クラウドオブジェクトストアエンドポイントを削除 (オプション) \* を選択します。

4. [ 削除 ( Delete ) ] をクリックします。

## クラウドオブジェクトストアを削除する

Cloud Backup 関係に含まれていないクラウドオブジェクトストアは、System Manager を使用して削除できます。クラウドオブジェクトストアがクラウドバックアップ関係の一部である場合、そのクラウドオブジェクトストアは削除できません。

### 手順

1. [ 保護 ]、[ 概要 ]、[ クラウドオブジェクトストア \* ] の順にクリックします。
2. 削除するオブジェクトストアを選択し、 をクリックします  をクリックし、 \* Delete \* を選択します。

## Cloud Backup を使用してデータをバックアップ

ONTAP 9.9.1以降では、System Managerを使用して、Cloud Backupを使用してクラウド内のデータをバックアップできます。



Cloud Backup は、FlexVol の読み書き可能ボリュームとデータ保護 ( DP ) ボリュームをサポートしています。FlexGroup ボリュームと SnapLock ボリュームはサポートされません。

### 作業を開始する前に

BlueXPでアカウントを確立するには、次の手順を実行する必要があります。サービスアカウントには、「Account Admin」というロールを作成する必要があります。（他のサービスアカウントロールには、System Manager からの接続の確立に必要な権限がありません）。

1. "BlueXPでアカウントを作成します"。
2. "BlueXPでコネクタを作成します" 次のいずれかのクラウドプロバイダを使用：
  - Microsoft Azure
  - Amazon Web Services ( AWS )
  - Google Cloud Platform ( GCP )
  - StorageGRID ( ONTAP 9.10.1 )



ONTAP 9.10.1以降では、クラウドバックアッププロバイダとしてStorageGRID を選択できますが、BlueXPがオンプレミスに導入されている場合にのみ選択できます。BlueXPコネクタは、オンプレミスにインストールし、BlueXPソフトウェアサービス ( SaaS ) アプリケーションから利用できるようにする必要があります。

3. "BlueXPでCloud Backup Service を購読します"（適切なライセンスが必要です）。
4. "BlueXPを使用して、アクセスキーとシークレットキーを生成します"。

## クラスタをBlueXPに登録します

クラスタは、BlueXPまたはSystem Managerを使用してBlueXPに登録できます。

### 手順

1. System Manager で、「保護の概要」に移動します。



2. \* Cloud Backup Service \* で、以下の詳細を指定します。

- クライアント ID
- クライアントシークレットキー

3. [Register and Continue] を選択します。

### Cloud Backup を有効にします

クラスタをBlueXPに登録したら、クラウドバックアップを有効にして、クラウドへの最初のバックアップを開始する必要があります。

#### 手順

1. System Manager で、 \* Protection > Overview \* をクリックし、 \* Cloud Backup Service \* セクションまでスクロールします。
2. クライアント ID \* と \* クライアントシークレット \* を入力します。



ONTAP 9.10.1 以降では、クラウドの使用コストについて、「 \* クラウドの使用コストの詳細 \* 」をクリックして確認できます。

3. [ 接続して Cloud Backup Service を有効にする \*] をクリックします。
4. [\* Cloud Backup Service を有効にする \*] ページで、選択したプロバイダーに応じて次の詳細を入力します。

クラウドプロバイダ	入力するデータ
Azure	<ul style="list-style-type: none"><li>• Azure サブスクリプション ID</li><li>• 地域</li><li>• リソースグループ名（既存または新規）</li></ul>
AWS	<ul style="list-style-type: none"><li>• AWS アカウント ID</li><li>• アクセスキー</li><li>• シークレットキー</li><li>• 地域</li></ul>
Google Cloud プロジェクト（GCP）	<ul style="list-style-type: none"><li>• Google Cloud プロジェクト名</li><li>• Google Cloud Access キー</li><li>• Google Cloud Secret キー</li><li>• 地域</li></ul>
StorageGRID （ONTAP 9.10.1以降。BlueXPのオンプレミス環境のみ）	<ul style="list-style-type: none"><li>• サーバ</li><li>• SGアクセスキー</li><li>• SG シークレットキー</li></ul>

## 5. 保護ポリシー \* を選択：

- \* 既存のポリシー \*：既存のポリシーを選択します。
- \* 新しいポリシー \*：名前を指定し、転送スケジュールを設定します。



ONTAP 9.10.1 以降では、Azure と AWS のどちらでアーカイブを有効にするかを指定できます。



Azure または AWS を使用してボリュームのアーカイブを有効にした場合、アーカイブを無効にすることはできません。

Azure または AWS のアーカイブを有効にする場合は、次の情報を指定します。

- ボリュームがアーカイブされるまでの日数。
- アーカイブに保持するバックアップの数。最新のバックアップまでアーカイブするには、「0」（ゼロ）を指定します。
- AWS の場合は、アーカイブストレージクラスを選択します。


## 6. バックアップするボリュームを選択します。

## 7. [ 保存（ Save ） ] を選択します。

クラウドバックアップに使用する保護ポリシーを編集します

Cloud Backup で使用する保護ポリシーを変更できます。

### 手順

1. System Manager で、 \* Protection > Overview \* をクリックし、 \* Cloud Backup Service \* セクションまでスクロールします。
2. をクリックします  をクリックし、 \* Edit \* をクリックします。
3. 保護ポリシー \* を選択：
  - \* 既存のポリシー \*：既存のポリシーを選択します。
  - \* 新しいポリシー \*：名前を指定し、転送スケジュールを設定します。



ONTAP 9.10.1 以降では、Azure と AWS のどちらでアーカイブを有効にするかを指定できます。



Azure または AWS を使用してボリュームのアーカイブを有効にした場合、アーカイブを無効にすることはできません。

Azure または AWS のアーカイブを有効にする場合は、次の情報を指定します。

- ボリュームがアーカイブされるまでの日数。
- アーカイブに保持するバックアップの数。最新のバックアップまでアーカイブするには、「0」（ゼロ）を指定します。
- AWS の場合は、アーカイブストレージクラスを選択します。

4. [ 保存 ( Save ) ] を選択します。

クラウド上の新しいボリュームまたは **LUN** を保護します

新しいボリュームまたは LUN を作成するときは、ボリュームまたは LUN のクラウドにバックアップできる SnapMirror 保護関係を確立できます。

作業を開始する前に

- SnapMirror ライセンスが必要です。
- クラスタ間 LIF を設定する必要があります。
- NTP を設定する必要があります。
- クラスタで ONTAP 9.9.1 が実行されている必要があります。

このタスクについて

次のクラスタ構成では、クラウド上の新しいボリュームや LUN を保護することはできません。

- クラスタを MetroCluster 環境に含めることはできません。
- SVM-DR はサポートされていません。
- Cloud Backup を使用して FlexGroup をバックアップすることはできません。

手順

1. ボリュームまたは LUN をプロビジョニングするときは、System Manager の \* Protection \* ページで、\* SnapMirror を有効にする (ローカルまたはリモート) \* チェックボックスを選択します。
2. クラウドバックアップポリシータイプを選択します。
3. クラウドバックアップが有効になっていない場合は、\* Cloud Backup Service を有効にする \* を選択します。

クラウド上の既存のボリュームまたは **LUN** を保護

既存のボリュームと LUN に対して SnapMirror 保護関係を確立できます。

手順

1. 既存のボリュームまたは LUN を選択し、\* Protect \* (保護) をクリックします。
2. [\* Protect Volumes] ページで、保護ポリシーに [\* Backup using Cloud Backup Service \*] を指定します。
3. **[Protect]**( 保護 ) をクリックします
4. [\* 保護] ページで、[ SnapMirror を有効にする ( ローカルまたはリモート ) ] チェックボックスをオンにします。
5. 「 Cloud Backup Service を有効にする 」を選択します。

バックアップファイルからデータをリストアする

データのリストア、関係の更新、関係の削除などのバックアップ管理操作は、BlueXP インターフェイスを使用している場合にのみ実行できます。を参照してください ["バックアップファイルからのデータのリストア"](#) を参照してください。

# CLI を使用したクラスタと SVM のピアリング

## CLI を使用したクラスタと SVM のピアリングの概要

ソースとデスティネーションのクラスタ間およびソースとデスティネーションの Storage Virtual Machine (SVM) 間にピア関係を作成できます。SnapMirror を使用して Snapshot コピーをレプリケートするには、これらのエンティティ間にピア関係を作成しておく必要があります。

ONTAP 9.3 では、クラスタと SVM 間にピア関係を設定する方法が簡易化されています。クラスタと SVM のピアリング手順は、ONTAP 9 のすべてのバージョンで使用できます。使用している ONTAP のバージョンに適した手順を使用してください。

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

## クラスタピアリングと SVM ピアリングを準備

### ピアリングの基本

SnapMirror を使用して Snapshot コピーをレプリケートするには、ソースとデスティネーションのクラスタ間およびソースとデスティネーションの SVM 間でピア関係を作成する必要があります。ピア関係で定義されるネットワーク接続により、クラスタ間および SVM 間でデータをセキュアにやり取りすることができます。

ピア関係にあるクラスタおよび SVM は、\_intercluster 論理インターフェイス (LIF) を使用してクラスタ間ネットワーク経由で通信します。\_ クラスタ間 LIF は、「intercluster-core」ネットワークインターフェイスサービスをサポートする LIF で、通常は「default-intercluster」ネットワークインターフェイスポリシーを使用して作成されます。ピア関係にあるクラスタ内の各ノードでクラスタ間 LIF を作成する必要があります。

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

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



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

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

## クラスタピアリングの前提条件

クラスタピアリングを設定する前に、接続、ポート、IP アドレス、サブネット、ファイアウォール、とクラスタの命名要件が満たされている。



ONTAP 9.6以降では、クラスタピア暗号化によって、データレプリケーションに対してTLS 1.2 AES-256 GCM暗号化がデフォルトでサポートされます。暗号化が無効になっていてもクラスタピアリングが機能するには、デフォルトのセキュリティ暗号（「PSK-AES256-GCM-SHA384」）が必要です。

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

## 接続要件

ローカルクラスタのすべてのクラスタ間 LIF が、リモートクラスタのすべてのクラスタ間 LIF と通信できる必要があります。

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

- サブネットがクラスタ間通信で使用するポートを含むブロードキャストドメインに属している。
- サブネットには、各ノードに 1 つのインタークラスタ LIF が割り当てられる十分な数の IP アドレスが必要です。

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

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

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



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

## ポート要件

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

- 特定のリモートクラスタとの通信に使用するポートは、すべて同じ IPspace に属している必要があります。

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

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

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

- すべてのポートが接続されている。
- すべてのポートが正常な状態である必要があります。
- ポートの MTU 設定が一貫している。

#### ファイアウォールの要件



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

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

- 双方向ICMPトラフィック
- ポート11104および11105経由ですべてのクラスタ間LIFのIPアドレスへの双方向開始TCPトラフィック
- クラスタ間 LIF 間の双方向 HTTPS

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

デフォルト intercluster ファイアウォールポリシーでは、HTTPSプロトコル経由のアクセスとすべてのIPアドレス（0.0.0.0/0）からのアクセスが許可されます。ポリシーは必要に応じて変更または置き換えできます。

#### クラスタ要件

クラスタは、次の要件を満たす必要があります。

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

#### 共有ポートまたは専用ポートを使用します

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



ピア関係にある一方のクラスタではポートを共有し、もう一方のクラスタでは専用ポートを使用することができます。

#### ネットワーク帯域幅

10GbE のように高速なネットワークの場合は、データアクセスに使用されるのと同じ 10GbE ポートを使用してレプリケーションを実行するためのローカル LAN 帯域幅が十分にあると考えられます。

その場合も、LAN 側と WAN 側の使用帯域幅を比較する必要があります。WAN 側で使用可能な帯域幅が

10GbE よりも大幅に狭い場合、専用ポートを使用しなければならないことがあります。



ただし、クラスタのすべてまたは多数のノードでデータをレプリケートする場合は例外で、この場合は一般に帯域幅がノード間で分散して使用されます。

専用ポートを使用しない場合、一般にレプリケーションネットワークの最大転送単位（MTU）サイズはデータネットワークの MTU サイズと同じにします。

#### レプリケーション間隔

ピーク時を避けてレプリケーションを実施する場合は、10GbE LAN 接続がなくてもデータポートを使用できるはずです。

通常の業務時間にレプリケーションを実施する場合は、レプリケートされるデータの量と、原因がデータプロトコルと競合するために必要な帯域幅を考慮する必要があるかどうかを検討する必要があります。データプロトコル（SMB、NFS、iSCSI）によるネットワーク利用率が 50% を超える場合は、ノードのフェイルオーバーが発生してもパフォーマンスの低下を招かないよう、クラスタ間通信に専用のポートを使用します。

#### ポートの可用性

レプリケーショントラフィックがデータトラフィックの妨げになる場合は、同じノード上にある他の任意のクラスタ間対応共有ポートにクラスタ間 LIF を移行できます。

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

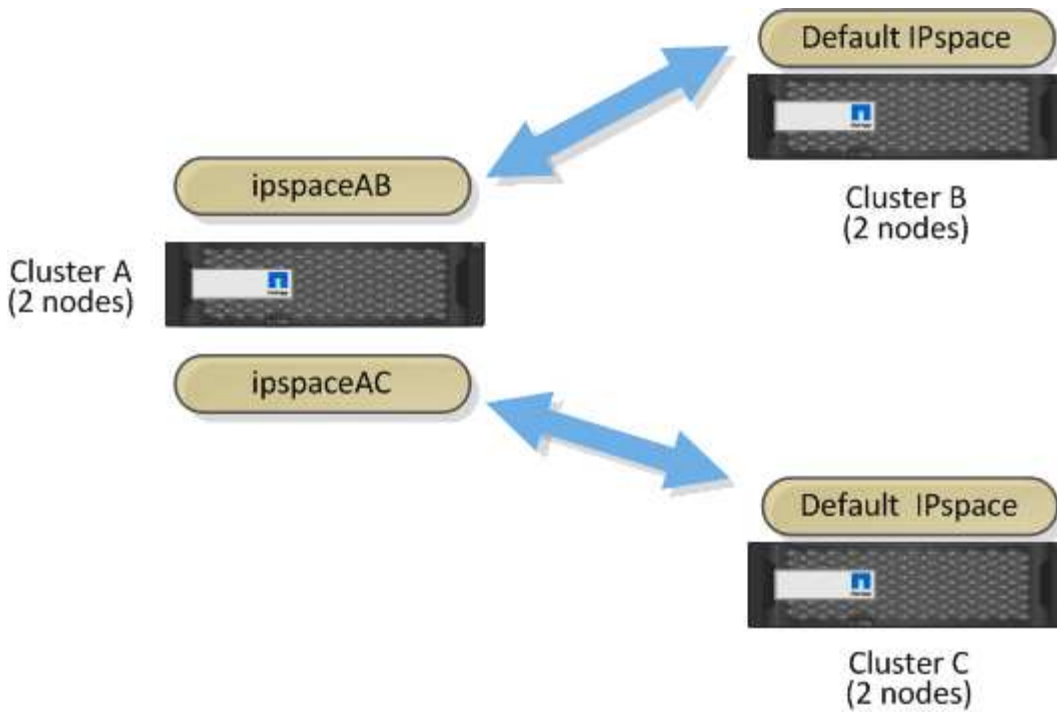
#### カスタム IPspace を使用してレプリケーショントラフィックを分離します

カスタム IPspace を使用すると、クラスタがそのピアに対して行ったやり取りを分離できます。Called `_Designated intercluster connectivity_`。この設定により、サービスプロバイダはマルチテナント環境でレプリケーショントラフィックを分離できます。

たとえば、クラスタ A とクラスタ B の間のレプリケーショントラフィックを、クラスタ A とクラスタ C の間のレプリケーショントラフィックから切り離すとしますこれを行うには、クラスタ A に IPspace を 2 つ作成します

一方の IPspace には、クラスタ B との通信に使用するクラスタ間 LIF が含まれています次の図に示すように、もう一方の IPspace には、クラスタ C との通信に使用するクラスタ間 LIF が含まれています。





カスタム IPspace の設定については、[\\_ ネットワーク管理ガイド \\_](#)を参照してください。

## クラスタ間 LIF を設定する

共有データポートにクラスタ間 LIF を設定します

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

### 手順

1. クラスタ内のポートの一覧を表示します。

```
network port show
```

コマンド構文全体については、マニュアルページを参照してください。

次の例は、のネットワークポートを示しています cluster01：



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

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

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

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

コマンド構文全体については、マニュアルページを参照してください。

次の例は、クラスタ間LIFを作成します cluster01\_icl01 および cluster01\_icl02：

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

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

### 3. クラスタ間 LIF が作成されたことを確認します。

オプション	説明
• ONTAP 9.6 以降： *	network interface show -service-policy default-intercluster
• ONTAP 9.5 以前： *	network interface show -role intercluster

コマンド構文全体については、マニュアルページを参照してください。

```
cluster01::> network interface show -service-policy default-intercluster
Logical      Status      Network      Current
Current Is
Vserver      Interface  Admin/Oper  Address/Mask      Node      Port
Home
-----
cluster01
      cluster01_icl01
              up/up      192.168.1.201/24      cluster01-01      e0c
true
      cluster01_icl02
              up/up      192.168.1.202/24      cluster01-02      e0c
true
```

### 4. クラスタ間 LIF が冗長構成になっていることを確認します。

オプション	説明
• ONTAP 9.6 以降： *	network interface show -service-policy default-intercluster -failover
• ONTAP 9.5 以前： *	network interface show -role intercluster -failover

コマンド構文全体については、マニュアルページを参照してください。

次の例は、クラスタ間LIFを示しています cluster01\_icl01 および cluster01\_icl02 をクリックします e0c ポートはにフェイルオーバーします e0d ポート：

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

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

専用ポートにクラスタ間 LIF を設定します

専用ポートにクラスタ間 LIF を設定できます。通常は、レプリケーショントラフィックに使用できる帯域幅が増加します。

手順

1. クラスタ内のポートの一覧を表示します。

```
network port show
```

コマンド構文全体については、マニュアルページを参照してください。

次の例は、のネットワークポートを示しています cluster01：

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

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

## 2. クラスタ間通信専用で使用可能なポートを特定します。

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

コマンド構文全体については、マニュアルページを参照してください。

次の例は、そのポートを示しています e0e および e0f LIFが割り当てられていません：

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

## 3. 専用ポートのフェイルオーバーグループを作成します。

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

次の例は、ポートを割り当てます e0e および e0f をフェイルオーバーグループに追加します intercluster01 システムSVM cluster01：

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

4. フェイルオーバーグループが作成されたことを確認します。

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

コマンド構文全体については、マニュアルページを参照してください。

```
cluster01::> network interface failover-groups show
Vserver      Group      Failover
-----
Targets
-----
Cluster
Cluster
cluster01-01:e0a, cluster01-01:e0b,
cluster01-02:e0a, cluster01-02:e0b
cluster01
Default
cluster01-01:e0c, cluster01-01:e0d,
cluster01-02:e0c, cluster01-02:e0d,
cluster01-01:e0e, cluster01-01:e0f
cluster01-02:e0e, cluster01-02:e0f
intercluster01
cluster01-01:e0e, cluster01-01:e0f
cluster01-02:e0e, cluster01-02:e0f
```

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

オプション	説明
• ONTAP 9.6 以降： *	network interface create -vserver system_SVM -lif LIF_name -service -policy default-intercluster -home -node node -home- port port -address port_IP -netmask netmask -failover -group failover_group

オプション	説明
<ul style="list-style-type: none"> <li>• ONTAP 9.5 以前： *</li> </ul>	<pre>network interface create -vserver system_SVM -lif LIF_name -role intercluster -home-node node -home -port port -address port_IP -netmask netmask -failover-group failover_group</pre>

コマンド構文全体については、マニュアルページを参照してください。

次の例は、クラスタ間LIFを作成します cluster01\_icl01 および cluster01\_icl02（フェイルオーバーグループ内） intercluster01：

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

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

## 6. クラスタ間 LIF が作成されたことを確認します。

オプション	説明
<ul style="list-style-type: none"> <li>• ONTAP 9.6 以降： *</li> </ul>	<pre>network interface show -service-policy default-intercluster</pre>
<ul style="list-style-type: none"> <li>• ONTAP 9.5 以前： *</li> </ul>	<pre>network interface show -role intercluster</pre>

コマンド構文全体については、マニュアルページを参照してください。

```

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

```

7. クラスタ間 LIF が冗長構成になっていることを確認します。

オプション	説明
• ONTAP 9.6 以降： *	network interface show -service-policy default-intercluster -failover
• ONTAP 9.5 以前： *	network interface show -role intercluster -failover

コマンド構文全体については、マニュアルページを参照してください。

次の例は、クラスタ間LIFを示しています cluster01\_icl01 および cluster01\_icl02 指定しますe0e ポートはにフェイルオーバーします e0f ポート：

```

cluster01::> network interface show -service-policy default-intercluster
-failover
          Logical      Home      Failover      Failover
Vserver   Interface  Node:Port      Policy      Group
-----
cluster01
          cluster01_icl01 cluster01-01:e0e  local-only
intercluster01
                                Failover Targets:  cluster01-01:e0e,
                                                cluster01-01:e0f
          cluster01_icl02 cluster01-02:e0e  local-only
intercluster01
                                Failover Targets:  cluster01-02:e0e,
                                                cluster01-02:e0f

```

カスタム IPspace にクラスタ間 LIF を設定します

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

カスタム IPspace を作成すると、その IPspace 内のシステムオブジェクトのコンテナとして機能するシステム Storage Virtual Machine (SVM) が作成されます。この SVM は、作成した IPspace 内のすべてのクラスタ間 LIF のコンテナとして使用できます。新しい SVM の名前がカスタム IPspace と同じです。

#### 手順

1. クラスタ内のポートの一覧を表示します。

```
network port show
```

コマンド構文全体については、マニュアルページを参照してください。

次の例は、のネットワークポートを示しています cluster01：

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

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

2. クラスタにカスタム IPspace を作成します。

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

次の例は、カスタムIPspaceを作成します ipspace-IC1：

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



3. クラスタ間通信専用で使用可能なポートを特定します。

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

コマンド構文全体については、マニュアルページを参照してください。

次の例は、そのポートを示しています e0e および e0f LIFが割り当てられていません：

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

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

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

一度に複数のブロードキャストドメインにポートを配置することはできません。コマンド構文全体については、マニュアルページを参照してください。

次の例は、ポートを削除します e0e および e0f デフォルトブロードキャストドメインから、次のコマンドを実行します。

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

5. デフォルトのブロードキャストドメインからポートが削除されたことを確認します。

```
network port show
```

コマンド構文全体については、マニュアルページを参照してください。

次の例は、そのポートを示しています e0e および e0f がデフォルトのブロードキャストドメインから削除されました。

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

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

## 6. カスタム IPspace にブロードキャストドメインを作成します。

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

次の例は、ブロードキャストドメインを作成します `ipspace-IC1-bd` (IPspace内) `ipspace-IC1` :

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

## 7. ブロードキャストドメインが作成されたことを確認します。

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

コマンド構文全体については、マニュアルページを参照してください。

```

cluster01::> network port broadcast-domain show
IPspace Broadcast
Name      Domain Name      MTU      Port List
-----
Cluster Cluster      9000
cluster01-01:e0a      complete
cluster01-01:e0b      complete
cluster01-02:e0a      complete
cluster01-02:e0b      complete
Default Default      1500
cluster01-01:e0c      complete
cluster01-01:e0d      complete
cluster01-01:e0f      complete
cluster01-01:e0g      complete
cluster01-02:e0c      complete
cluster01-02:e0d      complete
cluster01-02:e0f      complete
cluster01-02:e0g      complete
ipspace-IC1
    ipspace-IC1-bd
                1500
cluster01-01:e0e      complete
cluster01-01:e0f      complete
cluster01-02:e0e      complete
cluster01-02:e0f      complete

```

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

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

LIF は、ホームポートが割り当てられているブロードキャストドメインに作成されます。ブロードキャストドメインには、そのドメインと同じ名前のデフォルトのフェイルオーバーグループがあります。コマンド構文全体については、マニュアルページを参照してください。

次の例は、クラスタ間LIFを作成します cluster01\_icl01 および cluster01\_icl02 （ブロードキャストドメイン内） ipspace-IC1-bd：

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

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

9. クラスタ間 LIF が作成されたことを確認します。

オプション	説明
• ONTAP 9.6 以降： *	network interface show -service-policy default-intercluster
• ONTAP 9.5 以前： *	network interface show -role intercluster

コマンド構文全体については、マニュアルページを参照してください。

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

      Logical      Status      Network      Current
Current Is
Vserver      Interface  Admin/Oper Address/Mask      Node          Port
Home
-----
-----
ipspace-IC1
      cluster01_icl01
              up/up      192.168.1.201/24  cluster01-01  e0e
true
      cluster01_icl02
              up/up      192.168.1.202/24  cluster01-02  e0f
true
```

10. クラスタ間 LIF が冗長構成になっていることを確認します。

オプション	説明
• ONTAP 9.6 以降： *	network interface show -service-policy default-intercluster -failover
• ONTAP 9.5 以前： *	network interface show -role intercluster -failover

コマンド構文全体については、マニュアルページを参照してください。

次の例は、クラスタ間LIFを示しています cluster01\_icl01 および cluster01\_icl02 指定します e0e ポートがe0fポートにフェイルオーバーされます。

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

Vserver	Logical Interface	Home Node:Port	Failover Policy	Failover Group
-----				
ipspace-IC1				
	cluster01_icl01	cluster01-01:e0e	local-only	
intercluster01				
			Failover Targets:	cluster01-01:e0e, cluster01-01:e0f
	cluster01_icl02	cluster01-02:e0e	local-only	
intercluster01				
			Failover Targets:	cluster01-02:e0e, cluster01-02:e0f

## ピア関係を設定

### クラスタピア関係を作成

を使用できます cluster peer create コマンドを使用して、ローカルクラスタとリモートクラスタ間にピア関係を作成します。ピア関係が作成されたら、を実行できます cluster peer create リモートクラスタにアクセスしてローカルクラスタに対して認証します。

### 作業を開始する前に

- ピア関係にあるクラスタ内の各ノードでクラスタ間 LIF を作成しておく必要があります。
- クラスタで ONTAP 9.3 以降が実行されている必要があります。（クラスタで ONTAP 9.2 以前が実行されている場合は、の手順を参照してください ["このアーカイブ済みドキュメント".](#)）



### 手順

この作業は、ONTAP システムマネージャまたはONTAP CLIを使用して実行します。

## System Manager の略

1. ローカルクラスタで、\*[クラスタ]>[設定]\*をクリックします。
2. セクションで、[ネットワークインターフェイスの追加]\*をクリックし、クラスタのクラスタ間ネットワークインターフェイスを追加します。

リモートクラスタでこの手順を繰り返します。

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

## CLI の使用

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

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

両方を指定する場合は `-generate-passphrase` および `-peer-addr` にクラスタ間LIFが指定されているクラスタのみ `-peer-addr` 生成されたパスワードを使用できます。

は無視してかまいません `-ipspace` オプション（カスタムIPspaceを使用しない場合）。コマンド構文全体については、マニュアルページを参照してください。

ONTAP 9.6以降でピア関係を作成する場合に、クラスタ間ピアリング通信を暗号化しないようにするには、を使用する必要があります `-encryption-protocol-proposed none` 暗号化を無効にするオプション。

次の例は、リモートクラスタを指定せずにクラスタピア関係を作成し、SVMとのピア関係を事前承認します `vs1` および `vs2` ローカルクラスタ：

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

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

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

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

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

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

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

次の例は、リモートクラスタを指定せずにクラスタピア関係を作成し、SVM とのピア関係を事前承認します vs1 および vs2 ローカルクラスタ：

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

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

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

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

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

コマンド構文全体については、マニュアルページを参照してください。

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

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

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

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

Enter the passphrase:

Confirm the passphrase:

Clusters cluster02 and cluster01 are peered.

プロンプトが表示されたら、ピア関係のパスフレーズを入力します。

3. クラスタピア関係が作成されたことを確認します。

```
cluster peer show -instance
```



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

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

4. ピア関係にあるノードの接続状態とステータスを確認します。

```
cluster peer health show
```

```

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

```

#### ONTAP でこれを行うその他の方法

実行するタスク	参照するコンテンツ
再設計された System Manager （ ONTAP 9.7 以降で使用可能）	<a href="#">"ミラーとバックアップを準備"</a>
System Manager Classic （ ONTAP 9.7 以前で使用可能）	<a href="#">"ボリュームのディザスタリカバリの準備の概要"</a>

#### クラスタ間 **SVM** ピア関係を作成

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

#### 作業を開始する前に

- ソースクラスタとデスティネーションクラスタのピア関係が確立されている必要があります。
- クラスタで ONTAP 9.3 が実行されている必要があります。（クラスタで ONTAP 9.2 以前が実行されている場合は、の手順を参照してください ["このアーカイブ済みドキュメント"](#)。）
- リモートクラスタの SVM について、「事前承認」されたピア関係が必要です。

詳細については、を参照してください ["クラスタピア関係を作成"](#)。

#### このタスクについて

ONTAP 9.2以前では、一度に1つのSVMのピア関係のみを許可できます。つまり、`vserver peer accept` コマンドは、保留中のSVMピア関係を承認するたびに実行します。

ONTAP 9.3以降では、にSVMを一覧表示して、複数のSVMのピア関係を「事前承認」できます `-initial -allowed-vserver` オプションは、クラスタピア関係を作成するときに使用します。詳細については、を参照してください ["クラスタピア関係を作成"](#)。

#### 手順

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

```
vserver peer permission show
```

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

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

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

コマンド構文全体については、マニュアルページを参照してください。

次の例は、ローカルSVM間にピア関係を作成します `pvs1` および事前承認されたりモートSVM `vs1` :

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

3. SVM ピア関係を確認します。

```
vserver peer show
```

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

クラスタ間 **SVM** ピア関係を追加します

クラスタピア関係を設定したあとに SVM を作成する場合は、SVM のピア関係を手動で追加する必要があります。を使用できます `vserver peer create` コマンドを使用して SVM 間のピア関係を作成します。ピア関係が作成されたら、を実行できます `vserver peer accept` リモートクラスタ上でピア関係を承認します。

作業を開始する前に

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

このタスクについて

ローカルデータのバックアップ用に、同じクラスタの SVM 間にピア関係を作成できます。詳細については、を参照してください `vserver peer create` のマニュアルページ。

管理者がを使用することがあります `vserver peer reject` コマンドを使用して、提示された SVM ピア関係を拒否します。SVM 間の関係がにある場合 `rejected` 状態の場合は、新しい関係を作成する前に関係を削除する必要があります。詳細については、を参照してください `vserver peer delete` のマニュアルページ。

手順

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

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

次の例は、ローカル SVM 間にピア関係を作成します `pvs1` およびリモート SVM `vs1`

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

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

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

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

```
vserver peer show-all
```

コマンド構文全体については、マニュアルページを参照してください。

次の例は、SVM 間のピア関係を示しています `pvs1` および SVM `vs1` が開始されました：

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

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

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

```
vserver peer show
```

コマンド構文全体については、マニュアルページを参照してください。

次の例は、の保留中のピア関係を表示します cluster02 :

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

Vserver	Peer Vserver	Peer State
-----	-----	-----
vs1	pvs1	pending

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

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

コマンド構文全体については、マニュアルページを参照してください。

次の例は、ローカルSVM間のピア関係を承認します vs1 およびリモートSVM pvs1 :

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

5. SVM ピア関係を確認します。

```
vserver peer show
```

```
cluster01::> vserver peer show
```

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

## 既存のピア関係でクラスタピアリングの暗号化を有効にします

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

### このタスクについて

ピアクラスタを ONTAP 9.6 以降にアップグレードする場合、ONTAP 9.5 以前でピア関係が作成されているときは、アップグレード後にクラスタピアリングの暗号化を手動で有効にする必要があります。クラスタピアリングの暗号化を有効にするには、ピア関係の両方のクラスタで ONTAP 9.6 以降が実行されている必要があります。

### 手順

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

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

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

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

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

## 既存のピア関係からクラスタピアリングの暗号化を削除します

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

### 手順

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

- 認証を維持したまま暗号化を解除するには、次のように入力

```
cluster peer modify _source_cluster_ -auth-status-admin use-  
authentication -encryption-protocol-proposed none
```

- 暗号化と認証を解除するには、次のように入力します

```
cluster peer modify _source_cluster_ -auth-status no-authentication
```

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

- 認証を維持したまま暗号化を解除するには、次のように入力

```
cluster peer modify _destination_cluster_ -auth-status-admin use-  
authentication -encryption-protocol-proposed none
```

- 暗号化と認証を解除するには、次のように入力します

```
cluster peer modify _destination_cluster_ -auth-status no-  
authentication
```

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

## ローカル Snapshot コピーを管理します

### Manage local Snapshot copies の概要

Snapshot コピー \_ は、ボリュームの読み取り専用のポイントインタイムイメージです。イメージには Snapshot コピーが最後に作成されたあとに発生したファイルへの変更だけが記録されるため、ストレージスペースは最小限しか消費せず、パフォーマンスのオーバーヘッドもわずかです。

Snapshot コピーを使用すると、ボリュームの内容全体をリストアしたり、個々のファイルや LUN をリカバリしたりできます。Snapshot コピーはディレクトリに格納されます .snapshot ボリューム上。

ONTAP 9.3 以前では、ボリュームに格納できる Snapshot コピーは最大 255 個です。ONTAP 9.4 以降では、FlexVol ボリュームに格納できる Snapshot コピーは最大 1023 個です。



ONTAP 9.8 以降、FlexGroup ボリュームに 1023 個を含めることができます。詳細については、[を参照してください "Snapshot コピーを使用して FlexGroup ボリュームを保護する"](#)。

## カスタム Snapshot ポリシーを設定する

### カスタム Snapshot ポリシーの概要の設定

a\_snapshot\_policy\_ - Snapshot コピーの作成方法を定義します。このポリシーは、Snapshot コピーを作成するタイミング、保持するコピーの数、および Snapshot コピーに名前を付ける方法を指定します。たとえば、毎日午前12時10分に1つのSnapshotコピーを作成し、最新の2つのコピーを保持して、それらのコピーに「毎日」という名前を付けることができます。`.timestamp."`

ボリュームのデフォルトポリシーでは、次のスケジュールで Snapshot コピーが自動的に作成されます。新しいコピー用のスペースを確保するために、最も古い Snapshot コピーが削除されます。

- 最大 6 つの時間単位 Snapshot コピーが毎時 5 分に作成されます。
- 最大 2 つの日単位 Snapshot コピーが月曜日から土曜日の午前 0 時 10 分に作成されます。
- 最大 2 つの週単位 Snapshot コピーが毎週日曜日の午前 0 時 15 分に作成されます。

ボリュームの作成時に Snapshot ポリシーを指定しなかった場合は、そのボリュームを含む Storage Virtual Machine (SVM) に関連付けられている Snapshot ポリシーが継承されます。

### カスタム Snapshot ポリシーを設定するタイミング

デフォルトの Snapshot ポリシーがボリュームに適していない場合は、Snapshot コピーの頻度、保持設定、および名前を変更するカスタムポリシーを設定できます。スケジュールは、主にアクティブファイルシステムの変更率によって決まります。

使用頻度の高いファイルシステムは 1 時間ごとにデータベースのようにバックアップし、ほとんど使用されないファイルは 1 日に 1 回バックアップします。データベースであっても、通常は 1 日に 1~2 回フルバックアップを実行しますが、トランザクションログのバックアップは 1 時間ごとに行います。

その他の要因としては、組織におけるファイルの重要性、サービスレベルアグリーメント (SLA)、目標復旧時点 (RPO)、および目標復旧時間 (RTO) があります。通常は、Snapshot コピーを必要な数だけ保持してください。

### Snapshot ジョブスケジュールを作成

Snapshot ポリシーには、Snapshot コピーのジョブスケジュールが少なくとも 1 つ必要です。を使用できます `job schedule cron create` コマンドを使用してジョブスケジュールを作成します。

#### このタスクについて

デフォルトでは、ONTAP が Snapshot コピーの名前を作成する際には、ジョブスケジュール名にタイムスタンプを追加します。

日にちと曜日の両方に値を指定すると、それぞれ個別に判断されます。たとえば、dayが指定されたcronスケ



ジョブルなどです Friday 日付を指定します 13 13日の金曜日だけでなく、毎月の毎週金曜日と13日に実行されます。

## ステップ

### 1. ジョブスケジュールを作成します。

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

の場合 -month、-dayofweek`および`-hour`を指定できます `all` 毎月、曜日、および時間ごとにジョブを実行します。

ONTAP 9.10.1 以降では、ジョブスケジュールに SVM を追加できます。

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

次の例は、という名前のジョブスケジュールを作成します myweekly 土曜日の午前3時に実行されます。

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

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

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

## Snapshot ポリシーを作成します

Snapshot ポリシーは、Snapshot コピーを作成するタイミング、保持するコピーの数、および Snapshot コピーに名前を付ける方法を指定します。たとえば、毎日午前12時10分に1つのSnapshotコピーを作成し、最新の2つのコピーを保持して、「毎日」という名前を付けることができます。`timestamp."` Snapshotポリシーには最大5つのジョブスケジュールを含めることができます。

このタスクについて

デフォルトでは、ONTAP が Snapshot コピーの名前を作成する際には、ジョブスケジュール名にタイムスタンプを追加します。

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

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

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

## ステップ

### 1. Snapshot ポリシーを作成します

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

次の例は、という名前のSnapshotポリシーを作成します snap\_policy\_daily これはAで実行されます daily スケジュール：このポリシーには最大5つのSnapshotコピーが含まれ、それぞれにという名前が付付けられます daily.timestamp およびSnapMirrorラベル daily：

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

## Snapshotコピーを手動で管理する

### 手動でのSnapshotコピーの作成と削除

スケジュールされたSnapshotコピーが作成されるのを待たずに手動でSnapshotコピーを作成したり、不要になったSnapshotコピーを削除したりできます。

### Snapshotコピーを手動で作成する

System ManagerまたはONTAP CLIを使用して、Snapshotコピーを手動で作成できます。

## System Manager の略

### 手順

1. [ストレージ]>[ボリューム]に移動し、[Snapshotコピー]\*タブを選択します。
2. をクリックします **+ Add**。
3. [Snapshotコピーの追加]\*ウィンドウで、デフォルトのSnapshotコピー名をそのまま使用するか、必要に応じて編集します。
4. オプション：SnapMirrorラベルを追加します。
5. [ 追加（Add） ] をクリックします。

### CLI の使用

1. Snapshot コピーを作成

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

## Snapshotコピーを手動で削除する

System ManagerまたはONTAP CLIを使用して、Snapshotコピーを手動で削除できます。

## System Manager の略

### 手順

1. [ストレージ]>[ボリューム]に移動し、[Snapshotコピー]\*タブを選択します。
2. 削除するSnapshotコピーを探し、**:**をクリックし、\*[削除]\*を選択します。
3. ウィンドウで、[Snapshotコピーの削除]\*を選択します。
4. [ 削除（Delete） ] をクリックします。

### CLI の使用

1. Snapshotコピーを削除します。

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

## Snapshot コピーリザーブを管理します

### Snapshot コピーリザーブの概要を管理します

Snapshot コピーリザーブは、デフォルトでは 5% です。Snapshot コピー用にディスクスペースの割合を確保します。Snapshot コピーでは、Snapshot コピーリザーブを使い

切るとアクティブファイルシステムのスペースが使用されるため、必要に応じて Snapshot コピーリザーブを増やします。また、リザーブがフルになると Snapshot コピーを自動削除することもできます。

#### Snapshot コピーリザーブを増やすタイミング

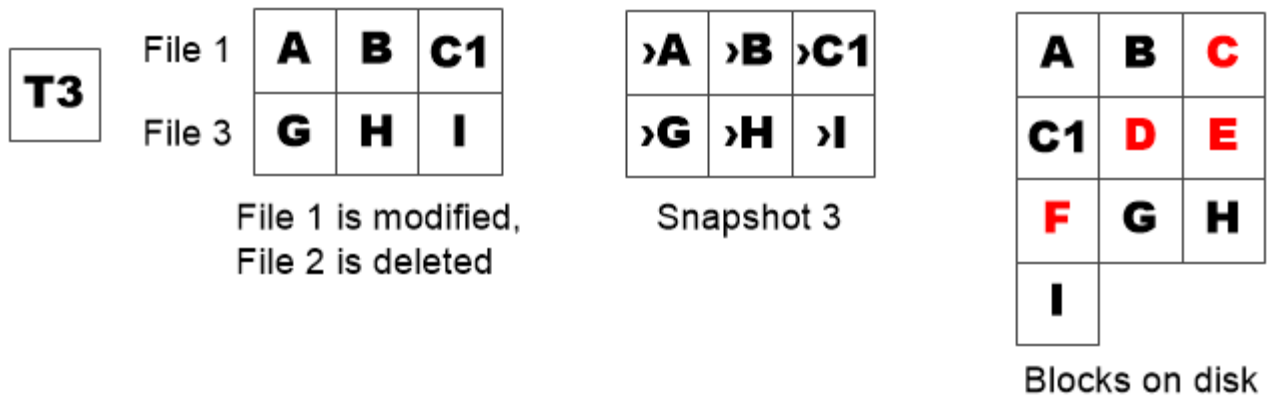
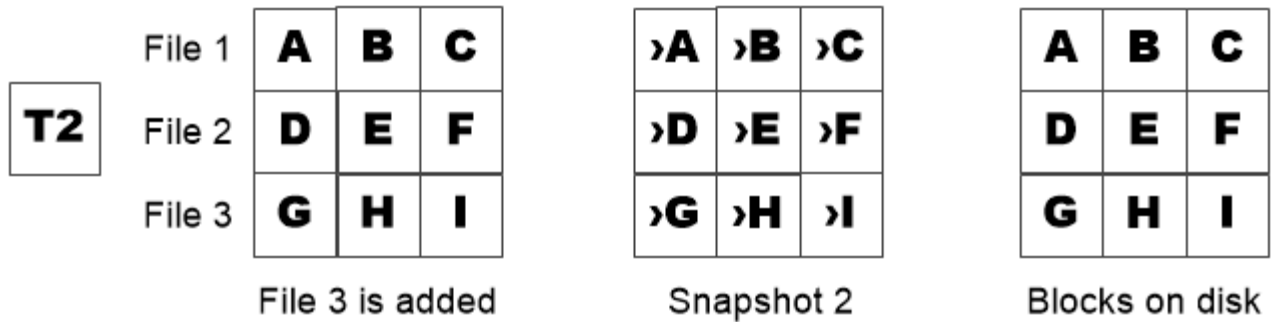
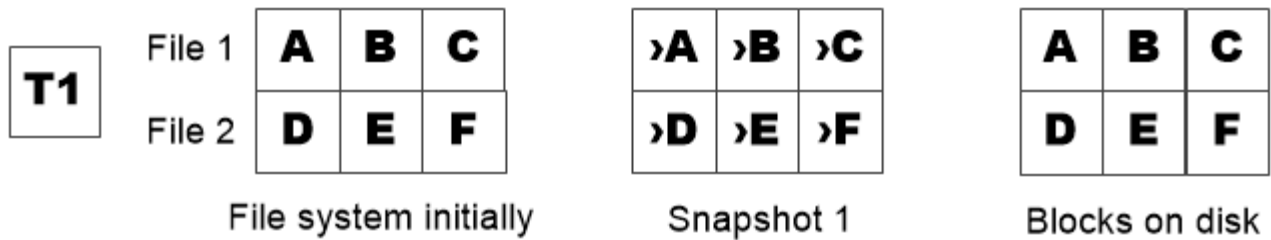
Snapshot リザーブを増やすかどうかを判断する際に重要なのは、Snapshot コピーには、前回の Snapshot コピー作成後のファイルに対する変更のみが記録されるという点です。このコピーによってディスクスペースが消費されるのは、アクティブファイルシステムのブロックが変更または削除された場合のみです。

つまり、Snapshot コピーで使用するディスクスペース容量を決定する際の重要な要素はファイルシステムの変更率です。作成する Snapshot コピーの数にかかわらず、アクティブファイルシステムが変更されていない場合、Snapshot コピーはディスクスペースを消費しません。

たとえば、データベーストランザクションログを含む FlexVol ボリュームには、変更率の増加に対応するために 20% の Snapshot コピーリザーブが用意されている場合があります。より多くの Snapshot コピーを作成して、データベースに対するより頻繁な更新をキャプチャするだけでなく、Snapshot コピーリザーブのサイズを拡張して、Snapshot コピーが消費する追加のディスクスペースを処理することができます。



Snapshot コピーは、ブロックのコピーではなくブロックへのポインタで構成されています。ポインタはブロック上の「要求」と考えることができます。ONTAP は、その Snapshot コピーが削除されるまでブロックを保持します。



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

保護対象のファイルを削除するとファイルスペースが想定よりも少なくなる可能性があります

Snapshot コピーは、ブロックを使用していたファイルを削除したあともそのブロックをポイントします。そのため、Snapshot コピーリザーブを使い切ると、期待に反した結果を引き起こす可能性があります。つまり、ファイルシステム全体を削除することで、ファイルシステムが占有するスペースよりも、使用可能なスペースが少なくなります。

次の例を考えてみましょう。ファイルを削除する前に、を実行します df コマンド出力は次のとおりです。

```

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

```

ファイルシステム全体を削除してボリュームのSnapshotコピーを作成したら、を実行します df コマンドによ

って次の出力が生成されます。

```
Filesystem      kbytes  used   avail  capacity
/vol/vol0/      3000000 2500000 500000   83%
/vol/vol0/.snapshot 1000000 3500000 0        350%
```

出力から、削除前の 0.5GB に加えて、アクティブファイルシステムで以前に使用されていた 3GB 全体が Snapshot コピーによって使用されるようになりました。

Snapshot コピーで使用するディスクスペースは Snapshot コピーリザーブを超えているため、アクティブファイル用にリザーブされたスペースに 2.5GB の「ピル」がオーバーフローします。想定していた 3GB については、ファイル用の 0.5GB の空きスペースが残ります。

### Snapshot コピーのディスク使用状況を監視します

を使用して、Snapshot コピーのディスク使用状況を監視できます `df` コマンドを実行しますコマンドは、アクティブファイルシステムおよび Snapshot コピーリザーブの空きスペースの量を表示します。

#### ステップ

1. Snapshot コピーのディスク使用状況を表示します。 `df`

次の例は、Snapshot コピーのディスク使用状況を示しています。

```
cluster1::> df
Filesystem      kbytes  used   avail  capacity
/vol/vol0/      3000000 3000000 0        100%
/vol/vol0/.snapshot 1000000 500000 500000   50%
```

### ボリュームで利用可能な Snapshot コピーリザーブを確認します

を使用して、ボリュームで使用可能な Snapshot コピーリザーブの容量を確認できます `snapshot-reserve-available` パラメータと `volume show` コマンドを実行します

#### ステップ

1. ボリュームで使用可能な Snapshot コピーリザーブを確認します。

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

コマンド構文全体については、マニュアルページを参照してください。

次の例は、の使用可能な Snapshot コピーリザーブを表示します `vol11` :

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

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

## Snapshot コピーリザーブを変更します

Snapshot コピーリザーブのサイズを拡張して、アクティブファイルシステム用にリザーブされたスペースが Snapshot コピーによって使用されないようにすることができます。Snapshot コピー用のスペースが不要になった場合は、Snapshot コピーリザーブのサイズを縮小できます。

### ステップ

1. Snapshot コピーリザーブを変更します。

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

コマンド構文全体については、マニュアルページを参照してください。

次の例は、のSnapshotコピーリザーブを設定します vol1 10%まで：

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

## Snapshot コピーを自動削除します

を使用できます volume snapshot autodelete modify Snapshotリザーブを超過したときにSnapshotコピーの自動削除を実行するコマンド。デフォルトでは、最も古い Snapshot コピーが最初に削除されます。

### このタスクについて

LUN クローンとファイルクローンは、削除する Snapshot コピーがなくなると削除されます。

### ステップ

1. Snapshot コピーを自動削除します。

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

コマンド構文全体については、マニュアルページを参照してください。

次の例は、のSnapshotコピーを自動削除します vol1 Snapshotコピーリザーブを使い切ると、次の処理が実行されます。

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

## Snapshot コピーからファイルをリストア

**NFS**または**SMB**クライアント上の**Snapshot**コピーからファイルをリストアする

NFSクライアントまたはSMBクライアントのユーザは、ストレージシステム管理者の手を借りなくとも、Snapshotコピーからファイルを直接リストアできます。

ファイルシステム内のすべてのディレクトリには、という名前のサブディレクトリが含まれています  
.snapshot NFSユーザとSMBユーザがアクセス可能。。.snapshot サブディレクトリには、ボリュームのSnapshotコピーに対応するサブディレクトリが含まれます。

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

各サブディレクトリには、Snapshot コピーが参照するファイルが含まれています。ユーザが誤ってファイルを削除または上書きした場合、Snapshot サブディレクトリから読み書き可能なディレクトリにファイルをコピーすることで、親の読み書き可能なディレクトリにファイルをリストアできます。

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

**Snapshot** コピーディレクトリへの **NFS** および **SMB** クライアントアクセスを有効または無効にします

SnapshotコピーからファイルまたはLUNをリストアするために、NFSクライアントおよびSMBクライアントがSnapshotコピーディレクトリを認識できるかどうかを確認するには、を使用してSnapshotコピーディレクトリへのアクセスを有効または無効にします  
-snapdir-access のオプション volume modify コマンドを実行します

手順



## 1. Snapshot ディレクトリのアクセスステータスを確認します。

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

例

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

## 2. Snapshot コピーのディレクトリアクセスを有効または無効にします。

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

次の例は、vol1 で Snapshot コピーのディレクトリへのアクセスを有効にします。

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

## Snapshot コピーから単一のファイルをリストアします

を使用できます volume snapshot restore-file コマンドを使用して、Snapshot コピーから単一ファイルまたはLUNをリストアします。既存のファイルを置き換えない場合は、読み書き可能な親ボリュームの別の場所にファイルをリストアできます。

このタスクについて

既存の LUN をリストアする場合は、LUN クローンが作成され、Snapshot コピーの形でバックアップされます。リストア処理中に、LUNに対する読み取りと書き込みを実行できます。

デフォルトでは、ストリームを含むファイルがリストアされます。

手順

### 1. ボリューム内の Snapshot コピーの一覧を表示します。

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

コマンド構文全体については、マニュアルページを参照してください。

次の例は、のSnapshotコピーを示しています vol1：

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

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

7 entries were displayed.

## 2. Snapshot コピーからファイルをリストアします。

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

コマンド構文全体については、マニュアルページを参照してください。

次の例は、ファイルをリストアします myfile.txt :

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

## Snapshot コピーからファイルの一部をリストアします

を使用できます volume snapshot partial-restore-file SnapshotコピーからLUN、NFSまたはSMBコンテナファイルに一定の範囲のデータをリストアするコマンド。データの開始バイトオフセットとバイト数がわかっていることが前提です。このコマンドでは、同じ LUN 内に複数のデータベースを格納するホスト上のいずれかのデータベースをリストアできます。

ONTAP 9.12.1以降では、SM-BC関係にあるボリュームで部分リストアを使用できます。

### 手順

1. ボリューム内の Snapshot コピーの一覧を表示します。

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

コマンド構文全体については、マニュアルページを参照してください。

次の例は、のSnapshotコピーを示しています vol1 :

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

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

7 entries were displayed.

## 2. Snapshot コピーからファイルの一部をリストアします。

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

開始バイトオフセットとバイト数は 4、096 の倍数でなければなりません。

次に、ファイルの最初の4、096バイトをリストアする例を示します myfile.txt：

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

## Snapshot コピーからボリュームの内容をリストアします

を使用できます volume snapshot restore コマンドを使用して、Snapshotコピーからボリュームの内容をリストアします。

このタスクについて

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

### 1. ボリューム内の Snapshot コピーの一覧を表示します。

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

次の例は、のSnapshotコピーを示しています vol1：

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

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

7 entries were displayed.

## 2. Snapshot コピーからボリュームの内容をリストアします。

```
volume snapshot restore -vserver SVM -volume volume -snapshot snapshot
```

次の例は、の内容をリストアします vol1 :

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

# SnapMirror ボリュームのレプリケーション

## 非同期 SnapMirror ディザスタリカバリの基本

SnapMirror は、地理的に離れたサイトのプライマリストレージからセカンダリストレージへのフェイルオーバー用に設計されたディザスタリカバリテクノロジーです。名前が示すように、SnapMirror はセカンダリストレージに作業データのレプリカ（\_mirror）を作成します。このデータから、プライマリサイトで災害が発生した場合にもデータの提供を継続できます。

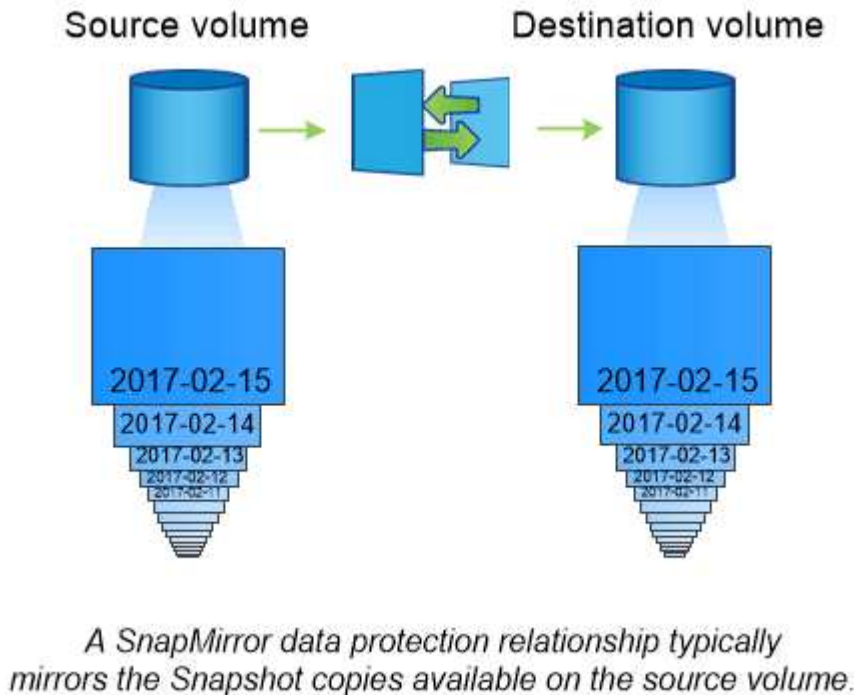
プライマリサイトから引き続きデータを提供できる場合は、必要なデータをプライマリサイトに戻すことができます。ミラーからクライアントを提供することはありません。フェイルオーバーの事例で示すように、ミラーリングされたストレージからデータを効率的に提供するには、セカンダリシステム上のコントローラがプライマリシステム上のコントローラと同じであるか、ほぼ同じである必要があります。

### データ保護関係

データのミラーリングはボリュームレベルで行われます。プライマリストレージのソースボリュームとセカンダリストレージのデスティネーションボリュームの関係は、\_data 保護関係と呼ばれます。\_ ボリュームが存在するクラスタと、ボリュームからデータを提供する SVM は \_peered になります。\_a ピア関係を設定することで、クラスタと SVM の交換が可能になります データをセキュアに保護

## "クラスタと SVM のピアリング"

次の図は、SnapMirror データ保護関係を示しています。



### データ保護関係の範囲

ボリューム間またはボリュームを所有する SVM 間で直接データ保護関係を作成できます。SVM のデータ保護関係では、SVM のすべてまたは一部の設定が NFS エクスポートおよび SMB 共有から RBAC にレプリケートされます。また、SVM が所有するボリューム内のデータもレプリケートされます。

SnapMirrorは、特殊なデータ保護アプリケーションにも使用できます。

- SVM ルートボリュームの負荷共有ミラーコピーを作成すると、ノードに障害やフェイルオーバーが発生したときに引き続きデータにアクセスできます。
- SnapLock ボリューム間のデータ保護関係：WORM ファイルをセカンダリストレージにレプリケートできます。

### "SnapLock テクノロジーを使用したアーカイブとコンプライアンス"

- ONTAP 9.13.1以降では、非同期SnapMirrorを使用して [整合グループ](#)。ONTAP 9.14.1以降では、非同期SnapMirrorを使用して、整合性グループ関係を使用してボリューム単位のSnapshotをデスティネーションクラスタにレプリケートできます。詳細については、[を参照してください 非同期SnapMirror保護を設定する](#)。

### SnapMirror データ保護関係を初期化する方法

SnapMirror を初めて起動すると、ソース・ボリュームからデスティネーション・ボリュームへの `_ベースライン転送_` が実行されます。関係の `_SnapMirror ポリシー_` は、ベースラインおよび更新の内容を定義します。

デフォルトのSnapMirrorポリシーに基づくベースライン転送 `MirrorAllSnapshots` 次の手順を実行します。

- ソースボリュームの Snapshot コピーを作成します。
- Snapshot コピーおよびコピーが参照するすべてのデータブロックをデスティネーションボリュームに転送します。
- 「アクティブ」ミラーが破損した場合に備えて、ソースボリューム上の最新ではない残りの Snapshot コピーをデスティネーションボリュームに転送します。

### **SnapMirror** データ保護関係を更新する方法

更新は、設定したスケジュールに従って非同期に行われます。保持処理によって、ソース上の Snapshot ポリシーがミラーリングされます。

をクリックします MirrorAllSnapshots ポリシーでは、SnapMirrorはソースボリュームのSnapshotコピーを作成し、そのSnapshotコピーと前回の更新後に作成されたすべてのSnapshotコピーを転送します。をクリックします snapmirror policy show コマンドを使用します MirrorAllSnapshots ポリシーでは、次の点に注意してください。

- Create Snapshot は「true」で、これを示します MirrorAllSnapshots SnapMirrorによる関係の更新時にSnapshotコピーが作成されます。
- MirrorAllSnapshots には、「sm\_created」および「all\_source\_snapshots」というルールがあります。これは、SnapMirrorが関係を更新するときに、SnapMirrorで作成されたSnapshotコピーと前回の更新以降に作成されたすべてのSnapshotコピーが転送されることを示します。

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

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

## MirrorLatest ポリシー

事前に設定されている MirrorLatest ポリシーはとまったく同じように機能します `MirrorAllSnapshots` ただし、初期化および更新の際に転送されるのは、SnapMirrorで作成されたSnapshotコピーだけです。

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

## SnapMirror Synchronous ディザスタリカバリの基本

ONTAP 9.5 以降では、16GB 以上のメモリを搭載したすべての FAS プラットフォームと AFF プラットフォーム、およびすべての ONTAP Select プラットフォームで SnapMirror Synchronous （SM-S）テクノロジーがサポートされます。SnapMirror Synchronous テクノロジーは、ノード単位のライセンスされる機能で、ボリュームレベル

の同期データレプリケーションを提供します。

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

#### 許可される**SnapMirror Synchronous**処理

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

次の表に、プラットフォームの種類とONTAP のリリース別にHAペアで実行できるSnapMirror Synchronous 処理の数を示します。

プラットフォーム	ONTAP 9.9.1より前のリリース	ONTAP 9.9.1	ONTAP 9.10.1	ONTAP 9.11.1からONTAP 9.14.1まで
AFF	80	一六〇	200	400
ASA	80	一六〇	200	400
FAS	40	80	80	80
ONTAP Select の場合	20	40	40	40

#### サポートされている機能

次の表に、SnapMirror SynchronousおよびONTAPの各リリースでサポートされる機能を示します。

フィーチャー（Feature）	最初にサポートされたリリース	追加情報
SnapMirror Synchronous 関係のプライマリボリュームに対するウィルス対策	ONTAP 9.6	
アプリケーションで作成されたSnapshotコピーのレプリケーション	ONTAP 9.7	Snapshotコピーに適切なラベルでタグ付けされている場合は、 <code>snapshot create SnapMirror Synchronous</code> は、CLIまたはONTAP APIを使用して、アプリケーションを休止すると、ユーザが作成したSnapshotコピーと外部スクリプトで作成したSnapshotコピーの両方をレプリケートします。Snapshot ポリシーを使用して作成され、スケジュール設定された Snapshot コピーはレプリケートされません。アプリケーションで作成されたSnapshot コピーのレプリケートの詳細については、ナレッジベースの記事： <a href="#">"アプリケーションで作成されたSnapshotをSnapMirror Synchronousでレプリケートする方法"</a> 。
クローンの自動削除	ONTAP 9.6	



階層化ポリシーが「なし」、「Snapshot」、または「自動」のFabricPoolアグリゲートは、SnapMirror Synchronousのソースとデスティネーションでサポートされます。	ONTAP 9.5	FabricPool アグリゲートのデスティネーションボリュームを「すべて」の階層化ポリシーに設定することはできません。
FC	ONTAP 9.5	レイテンシが10ミリ秒を超えないすべてのネットワーク
FC-NVMe	ONTAP 9.7	
ファイルクローン	ONTAP 9.7	
SnapMirror Synchronous 関係のプライマリボリュームに対する FPolicy	ONTAP 9.6	
SnapMirror Synchronous関係のプライマリボリュームに対するハードクォータとソフトクォータ	ONTAP 9.6	クォータルールはデスティネーションにレプリケートされないため、クォータデータベースはデスティネーションにレプリケートされません。
クラスタ内同期関係	ONTAP 9.14.1	高可用性は、ソースボリュームとデスティネーションボリュームが別々のHAペアに配置されている場合に提供されます。 クラスタ全体が停止すると、クラスタがリカバリされるまでボリュームにアクセスできなくなります。 クラスタ内のSnapMirror同期関係が、同時接続数の全体的な制限に影響します。 <a href="#">HAペアあたりの関係数</a> 。
iSCSI	ONTAP 9.5	
LUN クローンと NVMe ネームスペースクローン	ONTAP 9.7	
アプリケーションで作成されたSnapshotコピーによってバックアップされるLUNクローン	ONTAP 9.7	
混在プロトコルアクセス (NFS v3 とSMB)	ONTAP 9.6	
NDMP / NDMPリストア	ONTAP 9.13.1	SnapMirror SynchronousでNDMPを使用するには、ソースクラスタとデスティネーションクラスタの両方でONTAP 9.13.1以降が実行されている必要があります。詳細については、 <a href="#">を参照してください</a> <a href="#">NDMPコピーを使用してデータを転送します</a> 。
AFF / ASAプラットフォームでのみ、無停止のSnapMirror Synchronous Operations (NDO ; SnapMirror Synchronous Operations) を実行できます。	ONTAP 9.12.1	ノンストップオペレーションをサポートしているため、ダウンタイムをスケジュールせずに、一般的なメンテナンスタスクを多数実行できます。サポートされる処理には、テイクオーバーとギブバック、およびボリュームの移動があります。ただし、1つのノードが2つのクラスタのそれぞれで稼働している必要があります。
NFS v4.2	ONTAP 9.10.1	
NFS v4.3	ONTAP 9.5	

NFS v4.0	ONTAP 9.6	
NFS v4.1	ONTAP 9.6	
NVMe/FC	9.10.1	
メタデータ処理頻度の上限の削除	ONTAP 9.6	
TLS 1.2 暗号化を使用した機密データ転送時のセキュリティ	ONTAP 9.6	
単一ファイルおよび部分ファイルのリストア	ONTAP 9.13.1	
SMB 2.0以降	ONTAP 9.6	
SnapMirror Synchronous ミラー - ミラーカスケード	ONTAP 9.6	SnapMirror Synchronous 関係のデスティネーションボリュームからの関係は非同期 SnapMirror 関係である必要があります。
SVM ディザスタリカバリ	ONTAP 9.6	<p>* SnapMirror Synchronousソースは、SVMディザスタリカバリソースにすることもできます。たとえば、SnapMirror Synchronousを一方のレッグとして、SVMディザスタリカバリをもう一方のレッグとして使用するファンアウト構成などです。</p> <p>* SnapMirror Synchronousはデータ保護ソースのカスケードをサポートしていないため、SnapMirror SynchronousソースをSVMディザスタリカバリデスティネーションにすることはできません。デスティネーションクラスタでSVMディザスタリカバリのフリップ再同期を実行する前に、同期関係を解放する必要があります。</p> <p>* SVMディザスタリカバリではDPボリュームのレプリケーションがサポートされないため、SnapMirror SynchronousデスティネーションをSVMディザスタリカバリソースにすることはできません。同期ソースの逆再同期を実行すると、SVMディザスタリカバリでデスティネーションクラスタのDPボリュームが除外されます。</p>
ソースボリュームへのテープベースのリストア	ONTAP 9.13.1	
NAS のソースボリュームとデスティネーションボリュームの間のタイムスタンプパリティ	ONTAP 9.6	ONTAP 9.5 から ONTAP 9.6 にアップグレードした場合、タイムスタンプはソースボリューム内の新規および変更されたファイルについてのみレプリケートされます。ソースボリューム内の既存のファイルのタイムスタンプは同期されません。

サポートされない機能です

Synchronous SnapMirror 関係では、次の機能はサポートされません。

- 整合グループ
- DP\_Optimized （ DPO ） システム

- FlexGroup ボリューム
- FlexCache ボリューム
- グローバルスロットル
- ファンアウト構成で確立できる SnapMirror Synchronous 関係は 1 つだけで、ソースボリュームからの残りの関係はすべて非同期 SnapMirror 関係にする必要があります。
- LUNノイトウ
- MetroCluster 構成
- SAN アクセスと NVMe アクセスが混在しています  
LUN と NVMe ネームスペースは、同じボリュームまたは SVM ではサポートされません。
- SnapCenter
- SnapLock ボリューム
- 改ざん防止Snapshotコピー
- デスティネーションボリュームでのダンプおよび SMTape を使用したテープバックアップまたはリストア
- ソースボリュームのしきい値の下限（最小 QoS）
- ボリュームSnapRestore
- VVol

## 動作モード

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

### \* 同期モード \*

Syncモードでは、アプリケーションI/O処理がプライマリとセカンダリに並行して送信されます。ストレージシステム何らかの理由でセカンダリストレージへの書き込みが完了しない場合、アプリケーションはプライマリストレージへの書き込みを継続できます。エラー状態が解消されると、SnapMirror Synchronous テクノロジは自動的にセカンダリストレージを再同期し、プライマリストレージからセカンダリストレージへの同期モードでのレプリケーションを再開します。

Sync モードでは、セカンダリレプリケーションに障害問題が発生するまで RPO=0 と非常に低い RTO を実現できます。この場合、RPO と RTO は不確定になりますが、セカンダリレプリケーションが失敗し、再同期が完了するまでの時間と同じになります。

### \* StrictSync モード \*

SnapMirror Synchronous は、必要に応じて StrictSync モードで実行できます。何らかの理由でセカンダリストレージへの書き込みが完了しない場合、アプリケーション I/O が失敗し、プライマリストレージとセカンダリストレージが同一に保たれます。プライマリへのアプリケーションI/Oは、SnapMirror関係がに戻るまで再開されません InSync ステータス。プライマリストレージで障害が発生した場合は、フェイルオーバー後にセカンダリストレージでアプリケーション I/O を再開できます。データ損失は発生しません。

StrictSync モードの RPO は常にゼロで、RTO も非常に低く抑えられます。

## 関係のステータス

SnapMirror Synchronous関係のステータスは、常ににあります InSync 通常動作中のステータス。何らかの理由でSnapMirror転送に失敗した場合、デスティネーションはソースと同期されておらず、に移動できます OutofSync ステータス。

SnapMirror Synchronous関係については、関係のステータスが自動的にチェックされます InSync または OutofSync) を一定の間隔で入力します。関係のステータスがの場合 OutofSync`ONTAP は自動再同期プロセスを自動的にトリガーして、関係をに戻します `InSync ステータス。再同期が実行されるのは、ソースまたはデスティネーションでの計画外のストレージフェイルオーバーやネットワークの停止などによって転送に失敗した場合のみです。など、ユーザが開始した処理 snapmirror quiesce および snapmirror break 自動再同期はトリガーしないでください。

関係のステータスがになる場合 OutofSync StrictSyncモードのSnapMirror Synchronous関係では、プライマリボリュームに対するI/O処理がすべて停止されます。。 OutofSync SyncモードでのSnapMirror Synchronous関係の状態はプライマリへの影響を受けず、プライマリボリュームでI/O処理が許可されます。

#### 関連情報

["NetAppテクニカルレポート4733：『SnapMirror Synchronousの構成とベストプラクティス』"](#)

## StrictSync ポリシーと Sync ポリシーでサポートされるワークロードについて

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

ONTAP 9.5 では、Sync ポリシーで NFSv3 または NFSv4 ワークロードを選択する際、いくつかの重要な側面について考慮する必要があります。読み取り処理や書き込み処理のワークロードのデータ量については、Sync ポリシーでは IO ワークロードが高くてでも対応できるため考慮する必要はありません。ONTAP 9.5 では、ファイルの作成、ディレクトリの作成、ファイル権限の変更、ディレクトリ権限の変更などの処理が多いワークロード（「メタデータ比率の高いワークロード」と呼ばれます）は適さない場合があります。メタデータ比率の高いワークロードの典型的な例としては、複数のテストファイルを作成して自動化の実行後にファイルを削除する DevOps ワークロードがあります。また、コンパイル時に複数の一時ファイルを生成する並列ビルドワークロードなども含まれます。メタデータの書き込みアクティビティの比率が高いと、ミラー間の原因同期を一時的に解除して、クライアントからの読み取りや書き込みの IO が停止することがあります。

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

#### 関連情報

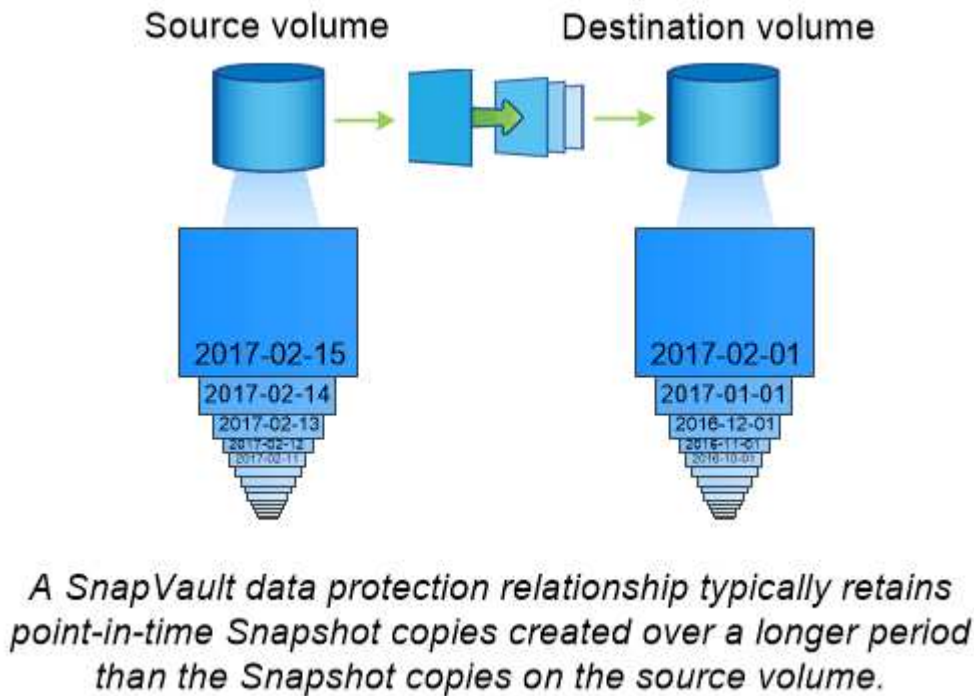
["SnapMirror Synchronous の設定およびベストプラクティス"](#)

## SnapMirror テクノロジーを使用したバックアップのアーカイブ

SnapVault 9.3 以降では、ONTAP テクノロジーの代わりに SnapMirror バックアップポリシーが使用されます。標準への準拠およびその他のガバナンス関連の目的で、ディスクツーディスクの Snapshot コピーレプリケーションに SnapMirror バックアップポリシーを使用します。SnapMirror 関係では、通常、ソースボリューム内の Snapshot コピーだけがデスティネーションに含まれますが、SnapVault デスティネーションはより長期間にわたって作成されたポイントインタイムの Snapshot コピーを保持します。

たとえば、ビジネスに関する政府会計規則に準拠するために、20年にわたってデータの月次 Snapshot コピーを保持しなければならない場合があります。SnapVault ストレージからデータを提供する必要はないため、デスティネーションシステムでは低速かつ低コストのディスクを使用できます。

次の図は、SnapMirror バックアップデータ保護関係を示しています。



#### バックアップデータ保護関係を初期化する方法

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

デフォルトのバックアップポリシーに基づくベースライン転送 XDPDefault ソースボリュームの Snapshot コピーを作成し、そのコピーおよびコピーが参照するデータブロックをデスティネーションボリュームに転送します。SnapMirror 関係とは異なり、バックアップにはベースラインに古い Snapshot コピーは含まれません。

#### バックアップデータ保護関係を更新する方法

更新は、設定したスケジュールに従って非同期に行われます。関係のポリシーで定義するルールによって、更新に含める新しい Snapshot コピーおよび保持するコピーの数が特定されます。ポリシーで定義されているラベル ("s only") は、ソース上の Snapshot ポリシーで定義されている 1 つ以上のラベルと一致する必要があります。そうしないと、レプリケーションが失敗します。

をクリックします XDPDefault ポリシー：SnapMirrorは、前回の更新後に作成されたSnapshotコピーを転送します（Snapshotコピーのラベルがポリシールールで定義されたラベルに一致する場合）。をクリックします snapmirror policy show コマンドを使用します XDPDefault ポリシーでは、次の点に注意してください。

- Create Snapshot は "false" であり、それを示します XDPDefault では、SnapMirrorによる関係の更新時にSnapshotコピーは作成されません。
- XDPDefault には、「daily」および「weekly」というルールが設定されています。SnapMirrorが関係を更新するときに、ソース上のラベルが一致するすべてのSnapshotコピーが転送されます。

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

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

## SnapMirror ユニファイドレプリケーションの基本

SnapMirror\_unified replication \_ は、同じデスティネーションボリュームでディザスタリカバリとアーカイブを設定できます。ユニファイドレプリケーションが適している場合は、必要なセカンダリストレージの量を減らし、ベースライン転送の回数を制限して、ネットワークトラフィックを減らすことができます。

### 一元化されたデータ保護関係を初期化する方法

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

デフォルトの一元化されたデータ保護ポリシーに基づくベースライン転送 MirrorAndVault ソースボリュームの Snapshot コピーを作成し、そのコピーおよびコピーが参照するデータブロックをデスティネーションボリュームに転送します。バックアップのアーカイブと同様に、一元化されたデータ保護にはベースラインの古い Snapshot コピーは含まれません。

### 一元化されたデータ保護関係を更新する方法

をクリックします MirrorAndVault SnapMirror ポリシーでは、ソースボリュームの Snapshot コピーが作成

され、そのSnapshotコピーと前回の更新後に作成されたすべてのSnapshotコピーが転送されます（Snapshotポリシーのルールで定義されたラベルに一致するラベルがある場合）。をクリックします `snapmirror policy show` コマンドを使用します MirrorAndVault ポリシーでは、次の点に注意してください。

- Create Snapshot は「true」で、これを示します MirrorAndVault SnapMirrorによる関係の更新時にSnapshotコピーが作成されます。
- MirrorAndVault には、「sm\_created」、「daily」、および「weekly」というルールが設定されています。SnapMirrorが関係を更新するときに、SnapMirrorで作成されたSnapshotコピーと、ソース上のラベルが一致するSnapshotコピーの両方が転送されることを示します。

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

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

**Unified7year ポリシー**

事前に設定されている Unified7year ポリシーはとまったく同じように機能します `MirrorAndVault` ただし、4番目のルールでは、月次Snapshotコピーを転送して7年間保持します。

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

データ破損の可能性をなくします

ユニファイドレプリケーションは、ベースライン転送の内容を、初期化時に SnapMirror で作成された Snapshot コピーに制限します。各更新で、SnapMirror はソースの Snapshot コピーをもう 1 つ作成して、その Snapshot コピーおよび Snapshot ポリシーのルールで定義されたラベルと一致するラベルを持つ新しいすべての Snapshot コピーを転送します。

最後に転送された Snapshot コピーのコピーをデスティネーションで作成することにより、更新した Snapshot コピーが破損する可能性を防ぐことができます。この「ローカル・コピー」はソース上の保持ルールに関係なく保持されるため、元は SnapMirror によって転送された Snapshot がソースで使用できなくなった場合でも、そのコピーをデスティネーションで使用できます。

ユニファイドデータレプリケーションを使用する状況

完全なミラーリングを維持するメリットと、セカンダリストレージの量を削減し、ベースライン転送の数を減らし、ネットワークトラフィックを減らすユニファイドレプリケーションのメリットをどちらかと比較する必要があります。

ユニファイドレプリケーションの妥当性を判断する際の重要な要素は、アクティブファイルシステムの変更率です。たとえば、データベーストランザクションログの時間単位 Snapshot コピーを保持するボリュームには、従来のミラーの方が適している場合があります。

**XDP は、DP を SnapMirror のデフォルトとして置き換えます**

ONTAP 9.3 以降では、SnapMirror 拡張データ保護（XDP）モードが SnapMirror データ保護（DP）モードに代わって SnapMirror のデフォルトになりました。

ONTAP 9.12.1 ONTAP 以降のリリースにアップグレードする前に、既存の DP タイプの関係を XDP に変換する必要があります。詳細については、を参照してください ["既存の DP タイプの関係を XDP に変換します"](#)。

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

- DP モードで起動する SnapMirror では、プライマリストレージとセカンダリストレージの ONTAP バージョンを同じにする必要がある、バージョンに依存するレプリケーションエンジンを使用していました。



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

- XDP モードで起動する SnapMirror では、バージョンに依存しないレプリケーションエンジンを使用していました。そのため、プライマリストレージとセカンダリストレージの ONTAP バージョンが異なってもかまいませんでした。

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

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

既存の関係には影響しません。DP タイプの既存の関係は引き続き DP タイプになります。ONTAP 9.5 以降では、データ保護モードを指定しなかった場合、および XDP モードを関係のタイプとして指定した場合、デフォルトポリシーが MirrorAndVault に変更になりました。次の表は、想定される動作を示しています。

指定するモード	タイプ	デフォルトポリシー（ポリシーを指定しない場合）
DP	XDP	MirrorAllSnapshots（SnapMirror DR）
なし	XDP	MirrorAndVault（ユニファイドレプリケーション）
XDP	XDP	MirrorAndVault（ユニファイドレプリケーション）

次の表に示すように、それぞれの状況で XDP に割り当てられるデフォルトポリシーでは、変換後も古いタイプと同等の機能が保証されます。もちろん、ユニファイドレプリケーションのポリシーなど、必要に応じて異なるポリシーを使用することもできます。

指定するモード	ポリシー	結果
DP	MirrorAllSnapshots	SnapMirror DR
XDPDefault	SnapVault	MirrorAndVault の場合
ユニファイドレプリケーション	XDP	MirrorAllSnapshots
SnapMirror DR	XDPDefault	SnapVault

変換の唯一の例外は次のとおりです。

- ONTAP 9.3 以前の SVM データ保護関係のデフォルトは引き続き DP モードです。

ONTAP 9.4 以降では、SVM データ保護関係のデフォルトが XDP モードに変更されました。

- ルートボリュームの負荷共有データ保護関係のデフォルトは引き続き DP モードです。
- ONTAP 9.4 以前の SnapLock データ保護関係のデフォルトは引き続き DP モードです。

ONTAP 9.5 以降では、SnapLock データ保護関係のデフォルトが XDP モードに変更されました。

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

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

DP を明示的に指定しない場合、このオプションは無視されます。

## デスティネーションボリュームが自動的に拡張される状況

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

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

データ保護ボリュームは、デフォルトでに設定されます `grow_shrink` オートサイズモード。使用済みスペースの量に応じてボリュームを拡張または縮小できます。データ保護ボリュームの `max-autosize` は、FlexVol の最大サイズと同じで、プラットフォームごとに異なります。例：

- FAS6240、デフォルトの DP ボリューム `max-autosize` = 70TB
- FAS8200 のデフォルトの DP ボリューム最大オートサイズは 100TB です

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

## ファンアウト構成およびカスケード構成のデータ保護

`a_fan-out_deployment` を使用すると、データ保護を複数のセカンダリシステムに拡張できます。`a_cascade_deployment` を使用して、データ保護を 3 次システムに拡張できます。

ファンアウトとカスケードのどちらの構成でも、SnapMirror DR、SnapVault、ユニファイドレプリケーションを任意に組み合わせることができます。ただし、SnapMirror Synchronous 関係（ONTAP 9.5 以降でサポート）では非同期 SnapMirror 関係を使用したファンアウト構成のみがサポートされ、カスケード構成はサポートされません。ファンアウト構成で確立できる SnapMirror Synchronous 関係は 1 つだけで、ソースボリュームからの残りの関係はすべて非同期 SnapMirror 関係にする必要があります。[SnapMirror によるビジネス継続性](#)（ONTAP 9.8 以降でサポート）では、ファンアウト構成もサポートされています。



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

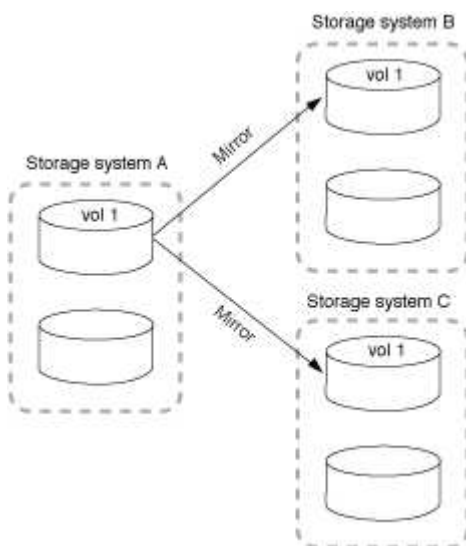


ファンアウト構成またはカスケード構成に含まれるボリュームは、再同期：SnapMirror関係のレポートが表示されることも珍しくありません。長期間のステータス「準備中」。

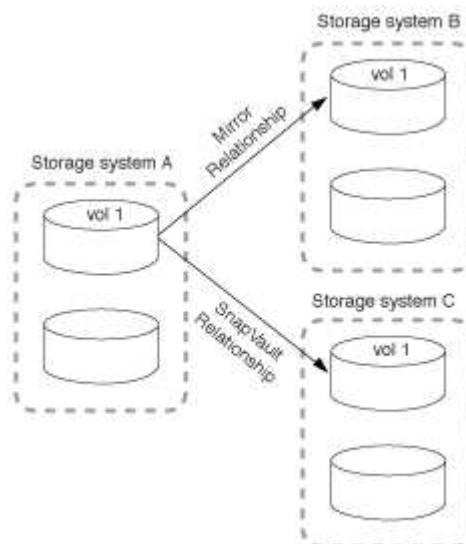
## ファンアウト構成の仕組み

SnapMirror は、`_ multiple-mirrors _` および `_ mirror -vault _ fan-out` 構成をサポートします。

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

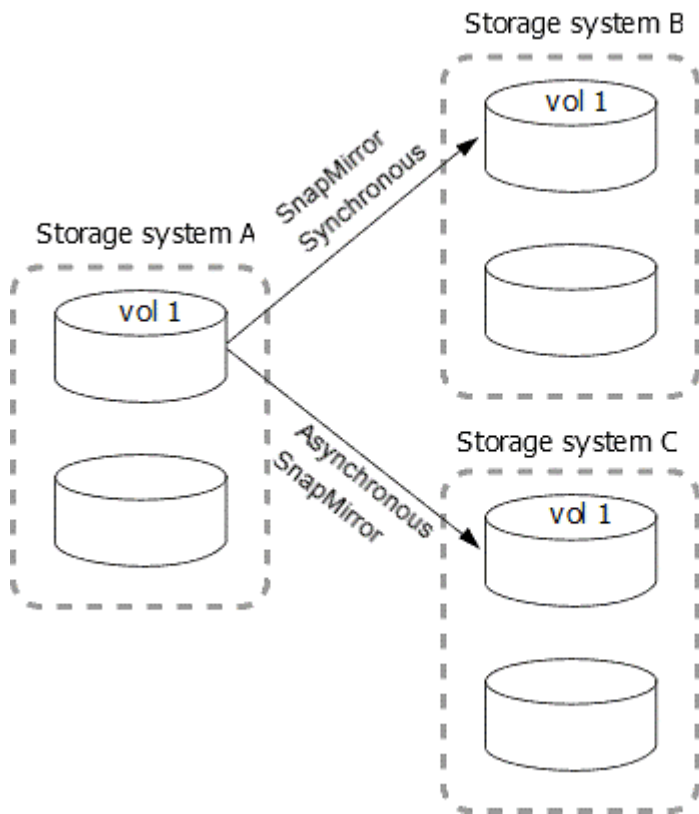


ミラー - ヴォールトファンアウト構成では、ソースボリュームからセカンダリボリュームへのミラー関係と、別のセカンダリボリュームへの SnapVault 関係が確立されます。



ONTAP 9.5 以降では、ファンアウト構成で SnapMirror Synchronous 関係を確立できます。ただし、ファンア

ウト構成で確立できる SnapMirror Synchronous 関係は 1 つだけで、ソースボリュームからの残りの関係はすべて非同期 SnapMirror 関係にする必要があります。

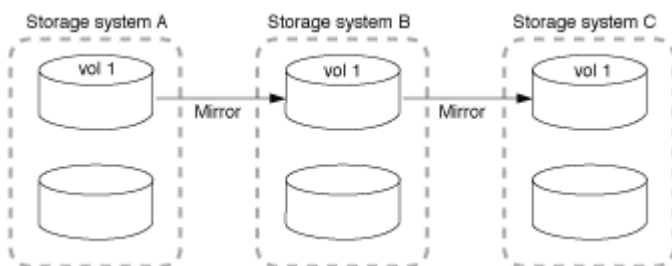


#### カスケード構成の仕組み

SnapMirror は、`_mirror -`、`_mirror - vault`、`vault - mirror`、`_vault-vault-cascade` の構成をサポートしています。

ミラー - ミラーカスケード構成の関係のチェーンでは、ソースボリュームがセカンダリボリュームにミラーリングされ、そのセカンダリボリュームが 3 番目のボリュームにミラーリングされます。セカンダリボリュームが使用できなくなった場合は、プライマリボリュームと 3 番目のボリュームの間の関係を同期できます。ベースライン転送を新たに実行する必要はありません。

ONTAP 9.6 以降では、ミラー - ミラーカスケード構成で SnapMirror Synchronous 関係がサポートされます。SnapMirror Synchronous 関係に含めることができるのは、プライマリボリュームとセカンダリボリュームだけです。セカンダリボリュームと 3 番目のボリュームの関係は非同期でなければなりません。



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



ヴォールト - ミラー、ONTAP 9.2 以降では、ヴォールト - ヴォールトカスケード構成もサポートされます。

- ヴォールト - ミラーカスケード構成の関係のチェーンでは、ソースボリュームがセカンダリボリュームに保存され、そのセカンダリボリュームが 3 番目のボリュームにミラーリングされます。
- (ONTAP 9.2 以降) ヴォールト - ヴォールトカスケード構成の関係のチェーンでは、ソースボリュームがセカンダリボリュームに保存され、そのセカンダリボリュームが 3 番目のボリュームに保存されます。

詳細はこちら

- [SM-BC を使用したファンアウト構成で保護を再開します](#)

## SnapMirror ライセンス

### SnapMirror のライセンスの概要

ONTAP 9.3 以降では、ONTAP インスタンス間のレプリケーションが簡易化されています。ONTAP 9 リリースでは、SnapMirror ライセンスでバックアップ関係とミラー関係の両方がサポートされます。SnapMirror ライセンスを使用すると、バックアップとディザスタリカバリの両方のユースケースで ONTAP レプリケーションをサポートできます。

ONTAP 9.3 より前のリリースでは、ONTAP インスタンス間の `configure_vault_relationships` には別個の SnapVault ライセンスが必要でした。この場合、DP インスタンスに保持期間の長いバックアップユースケースに対応するために、より多くの Snapshot コピーが保持される可能性がありました。また、ONTAP インスタンス間で `_mirror_relationships` を設定するには、SnapMirror ライセンスが必要でした。この場合、クラスタフェイルオーバーを可能にするディザスタリカバリのユースケースに対応するために、各 ONTAP インスタンスが同じ数の Snapshot コピー (`_mirror_image`) を保持します。ONTAP 8.x および 9.x リリースでは、SnapMirror ライセンスと SnapVault ライセンスの両方が引き続き使用され、サポートされます。

SnapVault ライセンスは引き続き機能し、ONTAP 8.x と 9.x の両方のリリースでサポートされますが、SnapVault ライセンスの代わりに SnapMirror ライセンスを使用して、ミラー構成とバックアップ構成の両方に使用できます。

ONTAP 非同期レプリケーションでは、ONTAP 9.3 以降、単一のユニファイドレプリケーションエンジンを使用して拡張データ保護モード (XDP) ポリシーを設定します。このポリシーでは、ミラーポリシー、バックアップポリシー、またはミラーバックアップポリシーに対して SnapMirror ライセンスを設定できます。ソースとデスティネーションの両方のクラスタに SnapMirror ライセンスが必要です。SnapVault ライセンスは、すでにインストールされている場合は必要ありません。SnapMirror 非同期無期限ライセンスは、新しい AFF および FAS システムにインストールされる ONTAP ONE ソフトウェアスイートに含まれています。

データ保護構成の上限は、ONTAP のバージョン、ハードウェアプラットフォーム、インストールされている

ライセンスなど、いくつかの要因で決まります。詳細については、を参照してください "[Hardware Universe](#)"。

### SnapMirror Synchronous ライセンス

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

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

SnapMirror Synchronous ライセンスは、"[ONTAP One ライセンススイート](#)"。

Premium Bundle または Flash Bundle の 2019 年 6 月より前に購入したシステムの場合、ネットアップマスターキーをダウンロードして、必要な SnapMirror Synchronous ライセンスを NetApp Support Site から入手できます。"[マスターライセンスキー](#)"。

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

### SnapMirror Cloud ライセンス

ONTAP 9.8 以降では、SnapMirror クラウドライセンスにより、ONTAP インスタンスからオブジェクトストレージエンドポイントへの Snapshot コピーの非同期レプリケーションが可能になりました。レプリケーションターゲットは、オンプレミスのオブジェクトストアと、S3 および S3 と互換性のあるパブリッククラウドのオブジェクトストレージサービスの両方を使用して設定できます。SnapMirror クラウド関係は、ONTAP システムから、事前修飾されたオブジェクトストレージターゲットへとサポートされます。

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

SnapMirror クラウド関係を作成するには、次のライセンスが必要です。

- オブジェクトストアエンドポイントに直接レプリケートするための SnapMirror ライセンスと SnapMirror Cloud ライセンスの両方。
- マルチポリシーレプリケーションワークフロー（ディスクツーディスククラウドなど）を設定する場合は、すべての ONTAP インスタンスに SnapMirror ライセンスが必要です。一方、SnapMirror クラウドライセンスが必要なのは、オブジェクトストレージエンドポイントに直接レプリケートするソースクラスタだけです。

ONTAP 9.9.1 以降では、次のことが可能になりました。"[System Manager を使用した SnapMirror Cloud レプリケーション](#)"。

SnapMirror Cloud のサードパーティ製アプリケーションの許可を受けた一覧は、ネットアップの Web サイトで公開されています。

### Data Protection Optimized ライセンス

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

DPO は ONTAP One ライセンスバンドルには含まれておらず、DPO ライセンスがシステムにインストールされ



ている場合はONTAP Oneライセンスバンドルにアップグレードできません。

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

## SnapMirror Cloudライセンスのインストール

SnapMirror Cloud関係は、認定済みの他社製バックアップアプリケーションを使用してオーケストレーションできます。ONTAP 9.9.1以降では、System Managerを使用してSnapMirror Cloudレプリケーションをオーケストレーションすることもできます。System Managerを使用してオンプレミスのONTAPをオブジェクトストレージバックアップにオーケストレーションする場合は、SnapMirrorとSnapMirror Cloudの両方の容量ライセンスが必要です。また、SnapMirror Cloud APIライセンスを要求してインストールする必要があります。

### このタスクについて

SnapMirror CloudライセンスとS3 SnapMirrorライセンスはクラスタライセンスであり、ノードライセンスではありません。そのため、ONTAP Oneライセンスバンドルには\_not\_deliveredが付属しています。これらのライセンスは、個別のONTAP One Compatibilityバンドルに含まれています。SnapMirror Cloudを有効にする場合は、このバンドルを要求する必要があります。

また、System ManagerによるオブジェクトストレージへのSnapMirror Cloudバックアップのオーケストレーションには、SnapMirror Cloud APIキーが必要です。このAPIライセンスはシングルインスタンスのクラスタ全体ライセンスであるため、クラスタ内のすべてのノードにインストールする必要はありません。

### 手順

ONTAP ONE Compatibility BundleとSnapMirror Cloud APIライセンスを要求してダウンロードし、System Managerを使用してインストールする必要があります。

1. ライセンスを付与するクラスタのクラスタUUIDを探して記録します。

クラスタ用のONTAP One Compatibilityバンドルを注文する要求を送信するには、クラスタUUIDが必要です。

2. NetApp営業チームに連絡して、ONTAP ONE互換性バンドルをリクエストしてください。
3. NetApp Support Siteに記載されている手順に従って、SnapMirror Cloud APIライセンスを要求します。

### "SnapMirror Cloud APIライセンスキーを申請します"

4. ライセンスファイルを受け取ってダウンロードしたら、System Managerを使用して、ONTAP Cloud Compatibility NLFとSnapMirror Cloud API NLFをクラスタにアップロードします。
  - a. **[Cluster] > [Settings]** の順にクリックします。
  - b. ウィンドウで、**[ライセンス]\***をクリックします。
  - c. **[ライセンス]\***ウィンドウで、 **+ Add**。
  - d. **[ \* ライセンスの追加 \* ]** ダイアログボックスで、 **[ \* 参照 ]** をクリックしてダウンロードした NLF を選択し、 **[ \* 追加 ]** をクリックしてファイルをクラスタにアップロードします。

### 関連情報

["SnapMirror を使用してデータをクラウドにバックアップ"](#)

## DPO システムの機能拡張

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

ONTAP 9.6 以降では、セカンダリシステムまたはデータ保護システムでサポートされる FlexVol の最大数が増加し、FlexVol ボリュームをノードあたり最大 2、500 個まで、フェイルオーバーモードでは最大 5、000 個まで拡張できるようになりました。FlexVolボリュームの増加は、["DP\\_Optimized \(DPO\) ライセンス"](#)。A ["SnapMirror ライセンス"](#) は、ソースノードとデスティネーションノードの両方で引き続き必要です。

ONTAP 9.4 以降では、DPO システムの次の機能が強化されています。

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

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

- ボリュームのバックグラウンド重複排除とボリューム間のバックグラウンド重複排除：DPO システムでは、ボリュームのバックグラウンド重複排除とボリューム間のバックグラウンド重複排除が有効になります。

を実行できます `storage aggregate efficiency cross-volume-dedupe start -aggregate aggregate_name -scan-old-data true` コマンドを使用して既存データを重複排除します。パフォーマンスへの影響を少なくするために、このコマンドはピーク時を避けて実行することを推奨します。

- Snapshot ブロックをドナーとして使用して削減効果を向上：アクティブなファイルシステムでは使用できないが Snapshot コピーに含まれるデータブロックをボリューム重複排除のドナーとして使用します。

Snapshot コピーに含まれるデータと照合して新しいデータを重複排除することができるため、結果として Snapshot ブロックが共有されることになります。ドナースペースが多いほど削減効果が高まり、特にボリュームに多数の Snapshot コピーがある場合に効果的です。

- コンパクション：DPO システムでは、データコンパクションはデフォルトで有効になります。

## SnapMirror ボリュームレプリケーションを管理します

### SnapMirror レプリケーションのワークフロー

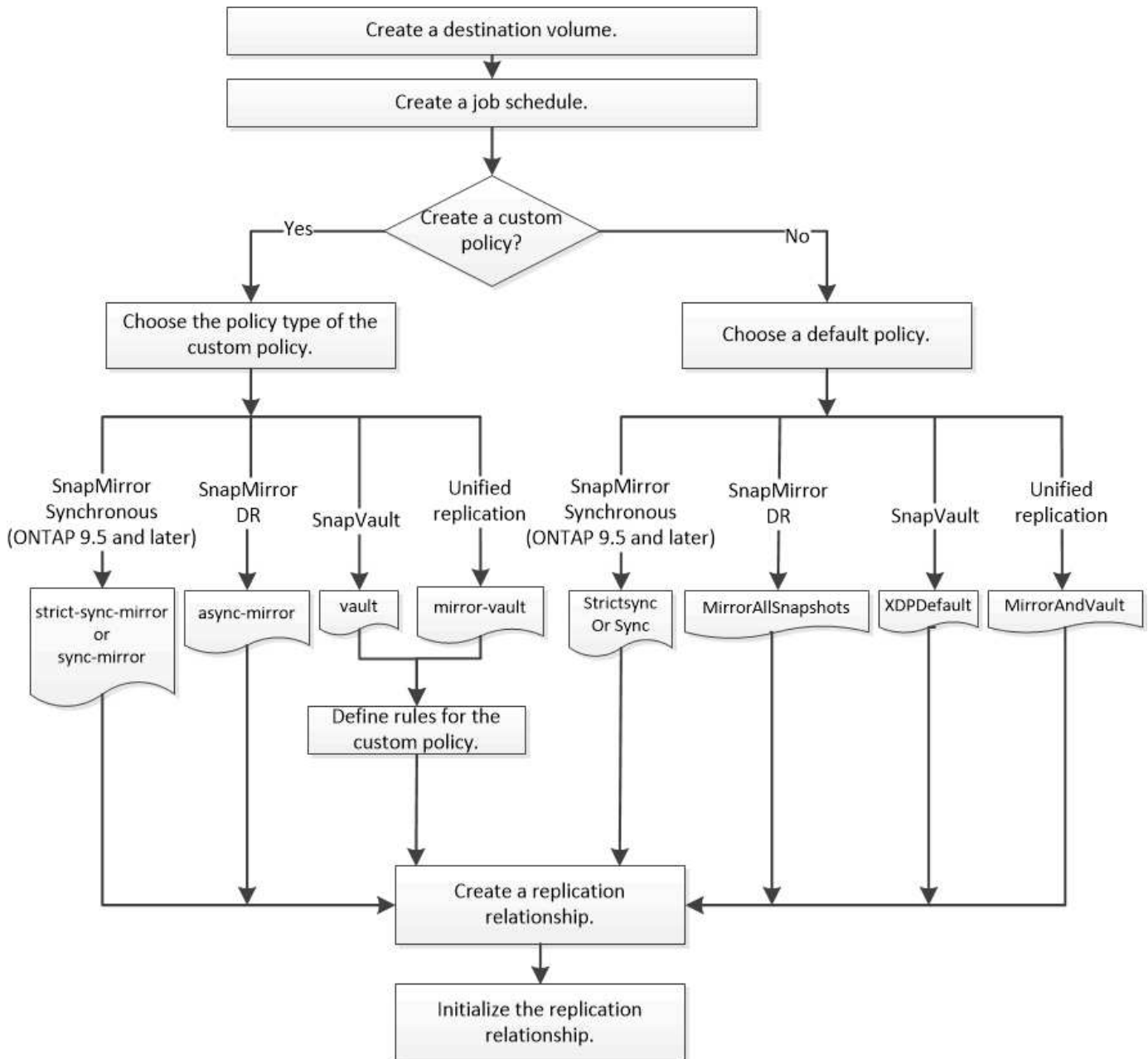
SnapMirror には、SnapMirror DR、アーカイブ（旧 SnapVault）、ユニファイドレプリケーションの 3 種類のデータ保護関係があります。各タイプの関係は、同じ基本的なワークフローに従って設定できます。

ONTAP 9.9.1の一般提供開始以降、SnapMirrorビジネス継続性（SM-BC）では、目標復旧時間ゼロ（ゼロRTO）または透過的アプリケーションフェイルオーバー（TAF）が提供され、SAN環境でビジネスクリティカルなアプリケーションを自動的にフェイルオーバーできます。SM-BCは、2つのAFFクラスタまたは2つのオールフラッシュSANアレイ（ASA）クラスタの構成でサポートされます。



SnapMirror データ保護関係のタイプごとに、ワークフローは同じです。デスティネーションボリュームの作成、ジョブスケジュールの作成、ポリシーの指定、関係の作成と初期化を行います。

ONTAP 9.3以降では、を使用できます `snapmirror protect` コマンドを使用してデータ保護関係をワンステップで設定できます。を使用する場合でも同様です `snapmirror protect` では、ワークフローの各手順を理解しておく必要があります。



レプリケーション関係をワンステップで設定します

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

## 必要なもの

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

### "クラスタと SVM のピアリング"

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

## このタスクについて

。 `snapmirror protect` コマンドは、指定したSVMに関連付けられているアグリゲートを選択します。SVM にアグリゲートが関連付けられていない場合は、クラスタ内のすべてのアグリゲートから選択されます。アグリゲートの選択は、空きスペースの量とアグリゲート上のボリュームの数に基づいて行われます。

。 `snapmirror protect` コマンドは次の手順を実行します。

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

デスティネーションボリュームの名前は、の形式になります `source_volume_name_dst`。既存の名前と競合する場合は、コマンドによってボリューム名に数字が追加されます。コマンドオプションでは、プレフィックスまたはサフィックスを指定できます。サフィックスは、システムが指定したものを置き換えます `dst` サフィックス。

ONTAP 9.3 以前では、デスティネーションボリュームに格納できる Snapshot コピーは最大 251 個です。ONTAP 9.4 以降では、デスティネーションボリュームに格納できる Snapshot コピーは最大 1019 個です。



初期化には時間がかかる場合があります。 `snapmirror protect` では、初期化が完了してからジョブが終了するまで待機しません。そのため、を使用する必要があります `snapmirror show` コマンドを使用してください `job show` 初期化がいつ完了したかを確認するコマンド。

ONTAP 9.5以降では、を使用してSnapMirror Synchronous関係を作成できます `snapmirror protect` コマンドを実行します

## ステップ

1. レプリケーション関係をワンステップで作成して初期化します。

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

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



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

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

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



必要に応じて、カスタムポリシーを使用できます。詳細については、[を参照してください "カスタムレプリケーションポリシーを作成する"](#)。

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

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

次の例は、デフォルトのを使用して、ユニファイドレプリケーション関係を作成して初期化します  
MirrorAndVault ポリシー：

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

次の例は、デフォルトのを使用して、SnapMirror Synchronous関係を作成して初期化します Sync ポリシー：

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



SnapVault ポリシーとユニファイドレプリケーションポリシーの場合は、デスティネーションで最後に転送された Snapshot コピーのコピーを作成するスケジュールを定義すると便利です。詳細については、[を参照してください "デスティネーションでローカルコピーを作成するスケジュールを定義します"](#)。

完了後

を使用します `snapmirror show` コマンドを実行して、SnapMirror関係が作成されたことを確認します。コマンド構文全体については、マニュアルページを参照してください。

## レプリケーション関係は一度に 1 つの手順で設定します

### デスティネーションボリュームを作成

を使用できます `volume create` コマンドをデスティネーションで実行し、デスティネ

ーションボリュームを作成します。デスティネーションボリュームのサイズは、ソースボリュームと同じかそれ以上である必要があります。

#### ステップ

1. デスティネーションボリュームを作成します。

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

コマンド構文全体については、マニュアルページを参照してください。

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

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

#### レプリケーションジョブスケジュールを作成

を使用できます `job schedule cron create` レプリケーションジョブスケジュールを作成するコマンド。ジョブスケジュールでは、スケジュールの割り当て先のデータ保護関係が SnapMirror によって自動的に更新されるタイミングを決定します。

#### このタスクについて

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

#### ステップ

1. ジョブスケジュールを作成します。

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

の場合 `-month`、`-dayofweek` および `-hour` を指定できます ``all`` 毎月、曜日、および時間ごとにジョブを実行します。

ONTAP 9.10.1 以降では、ジョブスケジュールに SVM を追加できます。

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



Volume SnapMirror関係にあるFlexVol でサポートされる最小スケジュール (RPO) は5分です。Volume SnapMirror関係にあるFlexGroup でサポートされる最小スケジュール (RPO) は30分です。

次の例は、という名前のジョブスケジュールを作成します my\_weekly 土曜日の午前3時に実行されます。

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

## レプリケーションポリシーをカスタマイズします

カスタムレプリケーションポリシーを作成する

関係のデフォルトポリシーが適切でない場合は、カスタムレプリケーションポリシーを作成できます。たとえば、ネットワーク転送時にデータを圧縮したり、Snapshot コピーを転送するための SnapMirror の試行回数を変更したりできます。

レプリケーション関係の作成時には、デフォルトまたはカスタムのポリシーを使用できます。カスタムアーカイブ（旧 SnapVault）またはユニファイドレプリケーションポリシーの場合は、初期化と更新の際に転送する Snapshot コピーを決定する 1 つ以上の `_rules_` を定義する必要があります。また、デスティネーションでローカル Snapshot コピーを作成するスケジュールを定義することもできます。

レプリケーションポリシーの `_policy type_of` によって、サポートされる関係のタイプが決まります。次の表は、使用可能なポリシータイプを示しています。

ポリシータイプ	関係タイプ
非同期ミラー	SnapMirror DR
バックアップ	SnapVault
ミラー - バックアップ	ユニファイドレプリケーション
strict-sync-mirror のようになります	StrictSync モードの SnapMirror Synchronous （ONTAP 9.5 以降でサポート）
SyncMirror	Sync モードの SnapMirror Synchronous （ONTAP 9.5 以降でサポート）



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

## ステップ

1. カスタムレプリケーションポリシーを作成します。

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

コマンド構文全体については、マニュアルページを参照してください。

ONTAP 9.5以降では、を使用して、SnapMirror Synchronous関係の共通のSnapshotコピースケジュールを作成するスケジュールを指定できます `-common-snapshot-schedule` パラメータデフォルトでは、SnapMirror Synchronous 関係の共通の Snapshot コピースケジュールは 1 時間です。SnapMirror Synchronous 関係の Snapshot コピースケジュールの値は、30 分から 2 時間までの範囲で指定できます。

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

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

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

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

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

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

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

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

完了後

「vault」および「`m mirror vault」ポリシータイプの場合は、初期化および更新時に転送する Snapshot コピーを決定するルールを定義する必要があります。

を使用します `snapmirror policy show` コマンドを入力して、SnapMirrorポリシーが作成されたことを確認します。コマンド構文全体については、マニュアルページを参照してください。

ポリシーのルールを定義します

ポリシータイプが「vault」または「M mirror vault」のカスタムポリシーの場合、初期化および更新時に転送する Snapshot コピーを決定するルールを少なくとも 1 つ定義する必要があります。また、ポリシータイプが「vault」または「`m mirror vault」のデフォルトポリシーのルールを定義することもできます。

このタスクについて

ポリシータイプが「vault」または「`m mirror vault」のすべてのポリシーには、レプリケートする Snapshot コピーを指定するルールが必要です。たとえば、「bi-monthly」ルールは、SnapMirror ラベルが「bi-monthly」に割り当てられた Snapshot コピーだけをレプリケートする必要があることを指定します。SnapMirror ラベルは、ソースでの Snapshot ポリシーの設定時に指定します。

各ポリシータイプは、システム定義の 1 つ以上のルールに関連付けられます。これらのルールは、ポリシータイプの指定時にポリシーに自動的に割り当てられます。次の表は、システム定義のルールを示しています。

システム定義のルール	ポリシータイプで使用されます	結果
sm_created	async-mirror、mirror-vault、Sync、StrictSync	SnapMirror で作成された Snapshot コピーが初期化および更新の際に転送されます。
all_source_snapshots を指定します	非同期ミラー	ソース上の新しい Snapshot コピーが初期化および更新の際に転送されます。
毎日	バックアップ、ミラー - ヴォールト	SnapMirror ラベルが「毎日」のソース上の新しい Snapshot コピーが初期化および更新の際に転送されます。
毎週	バックアップ、ミラー - ヴォールト	SnapMirror ラベルが「weekly」のソース上の新しい Snapshot コピーは、初期化および更新の際に転送されます。
毎月	ミラー - バックアップ	SnapMirror ラベルが「アース」の新しい Snapshot コピーがソースに転送され、初期化と更新が行われます。
APP_Consistent	Sync、StrictSync	SnapMirror ラベルが「app_consistent」の Snapshot コピーがソースからデスティネーションに同期的にレプリケートされます。ONTAP 9.7 以降でサポートされます。

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

- をクリックします MirrorAndVault ポリシーの場合は、SnapMirror ラベルが「bi-monthly」のソース Snapshot コピーを照合する「bi-monthly」というルールを作成できます。
- 「me-vault」ポリシータイプのカスタムポリシーの場合は、「bi-weekly」というルールを作成し、ソース上の Snapshot コピーと「bi-weekly」 SnapMirror ラベルを照合します。

ステップ

## 1. ポリシーのルールを定義します。

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

コマンド構文全体については、マニュアルページを参照してください。

次の例は、SnapMirrorラベルのルールを追加します bi-monthly をデフォルトに設定します MirrorAndVault ポリシー：

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

次の例は、SnapMirrorラベルのルールを追加します bi-weekly カスタムに my\_snapvault ポリシー：

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

次の例は、SnapMirrorラベルのルールを追加します app\_consistent カスタムに Sync ポリシー：

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

この SnapMirror ラベルに一致する Snapshot コピーをソースクラスタからレプリケートできます。

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

デスティネーションでローカルコピーを作成するスケジュールを定義します

SnapVault 関係とユニファイドレプリケーション関係の場合は、最後に転送された Snapshot コピーのコピーをデスティネーションで作成することによって、更新した Snapshot コピーが破損する可能性を防ぐことができます。この「ローカル・コピー」はソース上の保持ルールに関係なく保持されるため、元は SnapMirror によって転送された Snapshot がソースで使用できなくなった場合でも、そのコピーをデスティネーションで使用できます。

このタスクについて

ローカルコピーを作成するスケジュールはで指定します -schedule のオプション snapmirror policy add-rule コマンドを実行します

ステップ



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

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

コマンド構文全体については、マニュアルページを参照してください。ジョブスケジュールの作成方法の例については、を参照してください ["レプリケーションジョブスケジュールを作成します"](#)。

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

```
cluster_dst:> snapmirror policy add-rule -vserver svm1 -policy  
MirrorAndVault -snapmirror-label my_monthly -schedule my_monthly
```

次の例は、ローカルコピーを作成するスケジュールをカスタムのに追加します my\_unified ポリシー：

```
cluster_dst:> snapmirror policy add-rule -vserver svm1 -policy  
my_unified -snapmirror-label my_monthly -schedule my_monthly
```

## レプリケーション関係を作成

プライマリストレージのソースボリュームとセカンダリストレージのデスティネーションボリュームの関係は、データ保護関係と呼ばれます。\_を使用できます snapmirror create コマンドを使用して、SnapMirror DR、SnapVault、またはユニファイドレプリケーションのデータ保護関係を作成します。

### 必要なもの

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

#### "クラスタと SVM のピアリング"

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

### このタスクについて

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

- ・ DP モードで起動する SnapMirror では、プライマリストレージとセカンダリストレージの ONTAP バージョンを同じにする必要がある、バージョンに依存するレプリケーションエンジンを使用していました。

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

- ・ XDP モードで起動する SnapMirror では、バージョンに依存しないレプリケーションエンジンを使用して

いました。そのため、プライマリストレージとセカンダリストレージの ONTAP バージョンが異なってもかまいませんでした。

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

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

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

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

以下の手順の例も参照してください。

変換の唯一の例外は次のとおりです。

- SVM データ保護関係のデフォルトは引き続き DP モードです。  
  
XDPモードをデフォルトで取得するには、XDPを明示的に指定します MirrorAllSnapshots ポリシー：  
・
- 負荷共有データ保護関係のデフォルトは引き続き DP モードです。
- SnapLock データ保護関係のデフォルトは引き続き DP モードです。
- 次のクラスタ全体のオプションを設定した場合、DP を明示的に指定した場合のデフォルトは引き続き DP モードです。

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

DP を明示的に指定しない場合、このオプションは無視されます。

ONTAP 9.3 以前では、デスティネーションボリュームに格納できる Snapshot コピーは最大 251 個です。ONTAP 9.4 以降では、デスティネーションボリュームに格納できる Snapshot コピーは最大 1019 個です。

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

## ステップ

1. デスティネーションクラスタから、レプリケーション関係を作成します。

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

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

コマンド構文全体については、マニュアルページを参照してください。



。 schedule SnapMirror Synchronous関係を作成する場合は、パラメータは使用できません。

次の例は、デフォルトのを使用して、SnapMirror DR関係を作成します MirrorLatest ポリシー：

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

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

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

次の例は、デフォルトを使用して、ユニファイドレプリケーション関係を作成します MirrorAndVault ポリシー：

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

次の例は、カスタムのを使用してユニファイドレプリケーション関係を作成します my\_unified ポリシー：

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

次の例は、デフォルトを使用してSnapMirror Synchronous関係を作成します Sync ポリシー：

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

次の例は、デフォルトを使用してSnapMirror Synchronous関係を作成します StrictSync ポリシー：

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

次の例は、SnapMirror DR 関係を作成します。DPタイプは自動的にXDPに変換され、ポリシーは指定されません。デフォルトのポリシーはになります MirrorAllSnapshots ポリシー：

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

次の例は、SnapMirror DR 関係を作成します。タイプまたはポリシーが指定されていない場合、ポリシーはデフォルトでになります MirrorAllSnapshots ポリシー：

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

次の例は、SnapMirror DR 関係を作成します。ポリシーが指定されていない場合、ポリシーはデフォルトでになります XDPEndault ポリシー：

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

次の例は、事前定義されたポリシーを使用してSnapMirror Synchronous関係を作成します SnapCenterSync：

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



事前定義されたポリシー SnapCenterSync がのタイプです Sync。このポリシーは、で作成されたすべてのSnapshotコピーをレプリケートします snapmirror-label が「app\_consistent」の場合。

完了後

を使用します snapmirror show コマンドを実行して、SnapMirror関係が作成されたことを確認します。コマンド構文全体については、マニュアルページを参照してください。

## 関連情報

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

ONTAP でこれを行うその他の方法

実行するタスク	参照するコンテンツ
再設計された System Manager （ ONTAP 9.7 以降で使用可能）	<a href="#">"ミラーとバックアップを設定します"</a>
System Manager Classic （ ONTAP 9.7 以前で使用可能）	<a href="#">"SnapVault によるボリュームのバックアップの概要"</a>

## レプリケーション関係を初期化

すべての関係タイプでは、初期化の際に *baseline transfer*： ソースボリュームの Snapshot コピーが作成され、そのコピーおよびコピーが参照するすべてのデータブロックがデスティネーションボリュームに転送されます。それ以外の転送の内容はポリシーによって異なります。

### 必要なもの

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

### ["クラスタと SVM のピアリング"](#)

#### このタスクについて

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

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

#### ステップ

1. レプリケーション関係を初期化します。

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

コマンド構文全体については、マニュアルページを参照してください。



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

次の例は、ソースボリューム間の関係を初期化します volA オン svm1 デスティネーションボリュームを指定します volA\_dst オン svm\_backup：

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

例：ヴォールト - ヴォールトカスケードを設定します

レプリケーション関係を一度に 1 ステップずつ設定する方法の具体例を示します。この例で設定するヴォールト - ヴォールトカスケード構成を使用すると、「m-weekly」というラベルの付いた 251 個を超える Snapshot コピーを保持できます。

必要なもの

- ソースクラスタとデスティネーションクラスタ、および SVM のピア関係が確立されている必要があります。
- ONTAP 9.2 以降が実行されている必要があります。それより前のリリースの ONTAP では、ヴォールト - ヴォールトカスケードがサポートされていません。

このタスクについて

この例では次のことを前提としています。

- SnapMirror ラベルが「my-daily」、「my-weekly」、および「my-monthly」の Snapshot コピーをソースクラスタで設定済みである。
- セカンダリデスティネーションクラスタと 3 番目のデスティネーションクラスタに「volA」という名前のデスティネーションボリュームを設定済みである。
- セカンダリデスティネーションクラスタと 3 番目のデスティネーションクラスタに「y\_snapvault」というレプリケーションジョブスケジュールを設定しておきます。

次の例は、2 つのカスタムポリシーに基づいてレプリケーション関係を作成する方法を示しています。

- 「napvault\_secondary」ポリシーでは、7 個の日単位 Snapshot コピー、52 個の週単位 Snapshot コピー、180 個の月単位 Snapshot コピーがセカンダリデスティネーションクラスタに保持されています。
- 「napvault\_tertiary policy」は、250 個の週単位 Snapshot コピーを 3 番目のデスティネーションクラスタに保持しています。

手順

1. セカンダリデスティネーションクラスタで、「\$snapvault\_secondary」ポリシーを作成します。

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

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

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

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

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

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

```
cluster_secondary::> snapmirror policy add-rule -policy snapvault_secondary
```

```
-snapmirror-label my-monthly -keep 180 -vserver svm_secondary
```

5. セカンダリデスティネーションクラスタで、ポリシーを検証します。

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

```

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

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

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

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

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

8. 3次デスティネーションクラスタで、「'napvault\_tertiary'」ポリシーを作成します。

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

9. 3 次デスティネーションクラスタで、ポリシーの「`my-weekly`」ルールを定義します。

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

10. 3 番目のデスティネーションクラスタで、ポリシーを検証します。

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

```

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

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

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

12. 3 番目のデスティネーションクラスタで、セカンダリクラスタとの関係を初期化します。

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

既存の **DP** タイプの関係を **XDP** に変換します

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



存しない SnapMirror を活用できます。

このタスクについて

- SnapMirror では、既存の DP タイプの関係を XDP に自動的に変換しません。関係を変換するには、既存の関係を解除して削除し、新しい XDP 関係を作成して関係を再同期する必要があります。背景情報については、[を参照してください "XDP は、DP を SnapMirror のデフォルトとして置き換えます"](#)。
- 変換を計画する場合は、XDP SnapMirror 関係のバックグラウンド準備とデータウェアハウジングフェーズに時間がかかる可能性があることに注意してください。長時間にわたってステータスが「preparing」で報告されている SnapMirror 関係が表示されることは珍しくありません。



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

手順

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

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

次の例は、からの出力を示しています snapmirror show コマンドを実行します

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

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



のコピーを保持しておくと便利です `snapmirror show` 関係設定の既存の情報を追跡するためのコマンド出力。

2. ソースボリュームとデスティネーションボリュームから、両方のボリュームで共通のSnapshotコピーを作成します。

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

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

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

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

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

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

コマンド構文全体については、を参照してください ["のマニュアルページ"](#)。



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

次の例は、ソースボリューム間の関係を休止します volA オン svm1 デスティネーションボリュームを指定します volA\_dst オン svm\_backup :

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

#### 4. 既存の DP タイプの関係を解除します。

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

コマンド構文全体については、を参照してください ["のマニュアルページ"](#)。



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

次の例は、ソースボリューム間の関係を解除します volA オン svm1 デスティネーションボリュームを指定します volA\_dst オン svm\_backup :

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

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

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

次の例は、デスティネーションボリュームでSnapshotコピーの自動削除を無効にします volA\_dst :

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

#### 6. 既存の DP タイプの関係を削除します。

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

コマンド構文全体については、を参照してください ["のマニュアルページ"](#)。



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

次の例は、ソースボリューム間の関係を削除します volA オン svm1 デスティネーションボリュームを指定します volA\_dst オン svm\_backup :

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

7. ソースで元のSVMディザスタリカバリ関係を解放します。

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

次の例は、SVMディザスタリカバリ関係をリリースします。

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

8. で保持した出力を使用できます snapmirror show 次のコマンドを使用して、新しいXDPタイプの関係を作成します。

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

新しい関係では、同じソースボリュームとデスティネーションボリュームを使用する必要があります。コマンド構文全体については、マニュアルページを参照してください。



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

次の例は、ソースボリューム間のSnapMirrorディザスタリカバリ関係を作成します。 volA オン svm1 デスティネーションボリュームを指定します volA\_dst オン svm\_backup デフォルトを使用します MirrorAllSnapshots ポリシー :

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

## 9. ソースボリュームとデスティネーションボリュームを再同期します。

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

再同期時間を短縮するには、を使用します `-quick-resync` オプションですが、Storage Efficiencyによる削減効果は失われる可能性がある点に注意してください。コマンド構文全体については、マニュアルページを参照してください。 "[snapmirror resyncコマンドの実行](#)".



このコマンドはデスティネーション SVM またはデスティネーションクラスタから実行する必要があります。再同期の際にベースライン転送は不要ですが、再同期には時間がかかる場合があります。再同期はオフピークの時間帯に実行することを推奨します。

次の例は、ソースボリューム間の関係を再同期します `volA` オン `svm1` デスティネーションボリュームを指定します `volA_dst` オン `svm_backup` :

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

## 10. Snapshotコピーの自動削除を無効にした場合は、再度有効にします。

```
volume snapshot autodelete modify -vserver <SVM> -volume <volume>  
-enabled true
```

完了後

1. を使用します `snapmirror show` コマンドを実行して、SnapMirror関係が作成されたことを確認します。
2. SnapMirror XDPデスティネーションボリュームがSnapMirrorポリシーの定義に従ってSnapshotコピーの更新を開始したら、の出力を使用します。 `snapmirror list-destinations` ソースクラスタからコマンドを実行し、新しいSnapMirror XDP関係を表示します。

## SnapMirror 関係のタイプを変換します

ONTAP 9.5 以降では、SnapMirror Synchronous がサポートされます。非同期 SnapMirror 関係と SnapMirror Synchronous 関係は、ベースライン転送を実行しなくても相互に変換することができます。

このタスクについて

SnapMirror ポリシーを変更して非同期 SnapMirror 関係と SnapMirror Synchronous 関係を相互に変換することはできません

手順

- \* 非同期 SnapMirror 関係から SnapMirror Synchronous 関係への変換 \*

- a. デスティネーションクラスタから、非同期 SnapMirror 関係を削除します。

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

```
cluster2::>snapmirror delete -destination-path vs1_dr:vol1
```

- b. ソースクラスタから、共通の Snapshot コピーは削除せずに SnapMirror 関係を解放します。

```
snapmirror release -relationship-info-only true -destination-path  
dest_SVM:dest_volume
```

```
cluster1::>snapmirror release -relationship-info-only true  
-destination-path vs1_dr:vol1
```

- c. デスティネーションクラスタから、SnapMirror Synchronous 関係を作成します。

```
snapmirror create -source-path src_SVM:src_volume -destination-path  
dest_SVM:dest_volume -policy sync-mirror
```

```
cluster2::>snapmirror create -source-path vs1:vol1 -destination-path  
vs1_dr:vol1 -policy sync
```

- d. SnapMirror Synchronous 関係を再同期します。

```
snapmirror resync -destination-path dest_SVM:dest_volume
```

```
cluster2::>snapmirror resync -destination-path vs1_dr:vol1
```

• \* SnapMirror Synchronous 関係から非同期 SnapMirror 関係への変換 \*

- a. デスティネーションクラスタから、既存の SnapMirror Synchronous 関係を休止します。

```
snapmirror quiesce -destination-path dest_SVM:dest_volume
```

```
cluster2::> snapmirror quiesce -destination-path vs1_dr:vol1
```

- b. デスティネーションクラスタから、非同期 SnapMirror 関係を削除します。

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

```
cluster2::>snapmirror delete -destination-path vs1_dr:vol1
```

- c. ソースクラスタから、共通の Snapshot コピーは削除せずに SnapMirror 関係を解放します。

```
snapmirror release -relationship-info-only true -destination-path  
dest_SVM:dest_volume
```

```
cluster1::>snapmirror release -relationship-info-only true  
-destination-path vs1_dr:vol1
```

- d. デスティネーションクラスタから、非同期 SnapMirror 関係を作成します。

```
snapmirror create -source-path src_SVM:src_volume -destination-path  
dest_SVM:dest_volume -policy MirrorAllSnapshots
```

```
cluster2::>snapmirror create -source-path vs1:vol1 -destination-path  
vs1_dr:vol1 -policy sync
```

- e. SnapMirror Synchronous 関係を再同期します。

```
snapmirror resync -destination-path dest_SVM:dest_volume
```

```
cluster2::>snapmirror resync -destination-path vs1_dr:vol1
```

## SnapMirror Synchronous 関係のモードを変換します

ONTAP 9.5 以降では、SnapMirror Synchronous 関係がサポートされます。SnapMirror Synchronous 関係のモードは StrictSync と Sync の間で相互に変換できます。

このタスクについて

SnapMirror Synchronous 関係のポリシーを変更してモードを変換することはできません。

手順

1. デスティネーションクラスタから、既存の SnapMirror Synchronous 関係を休止します。

```
snapmirror quiesce -destination-path dest_SVM:dest_volume
```

```
cluster2::> snapmirror quiesce -destination-path vs1_dr:vol1
```

2. デスティネーションクラスタから、既存の SnapMirror Synchronous 関係を削除します。

```
snapmirror delete -destination-path dest_SVM:dest_volume
```

```
cluster2::> snapmirror delete -destination-path vs1_dr:vol1
```



3. ソースクラスタから、共通の Snapshot コピーは削除せずに SnapMirror 関係を解放します。

```
snapmirror release -relationship-info-only true -destination-path  
dest_SVM:dest_volume
```

```
cluster1::> snapmirror release -relationship-info-only true -destination  
-path vs1_dr:vol1
```

4. デスティネーションクラスタから、変換後のモードを指定して SnapMirror Synchronous 関係を作成します。

```
snapmirror create -source-path vs1:vol1 -destination-path dest_SVM:dest_volume  
-policy Sync|StrictSync
```

```
cluster2::> snapmirror create -source-path vs1:vol1 -destination-path  
vs1_dr:vol1 -policy Sync
```

5. デスティネーションクラスタから、SnapMirror 関係を再同期します。

```
snapmirror resync -destination-path dest_SVM:dest_volume
```

```
cluster2::> snapmirror resync -destination-path vs1_dr:vol1
```

## SnapMirror フェイルオーバーテストボリュームの作成と削除

ONTAP 9.14.1以降では、System Managerを使用してボリュームクローンを作成し、アクティブなSnapMirror関係を中断することなく、SnapMirrorフェイルオーバーとディザスタリカバリをテストできます。テストが完了したら、関連するデータをクリーンアップしてテストボリュームを削除できます。

**SnapMirror**フェイルオーバーテストボリュームを作成します。



このタスクについて

- 同期および非同期SnapMirror関係に対してフェイルオーバーテストを実行できます。
- ディザスタリカバリテストを実行するためにボリュームクローンを作成します。
- クローンボリュームは、SnapMirrorデスティネーションと同じStorage VMに作成されます。
- FlexVol関係とFlexGroup SnapMirror関係を使用できます。
- 選択した関係にテスト用のクローンがすでに存在する場合、その関係に別のクローンを作成することはできません。
- SnapLockバックアップ関係はサポートされません。

作業を開始する前に

- クラスタ管理者である必要があります。
- ソースクラスタとデスティネーションクラスタにSnapMirrorライセンスがインストールされている必要があります。


#### 手順

1. デスティネーションクラスタで、\*[保護]>[関係]\*を選択します。
2. 選択するオプション  をクリックし、\*[フェイルオーバーのテスト]\*を選択します。
3. [フェイルオーバーのテスト]ウィンドウで、\*[フェイルオーバーのテスト]\*を選択します。
4. [ストレージ]>[ボリューム]\*を選択し、テストフェイルオーバーボリュームが表示されることを確認します。
5. [ストレージ]>[共有]\*を選択します。
6.  Add メニュー"] [共有]を選択します。
7. ウィンドウで、[共有名]\*フィールドに共有の名前を入力します。
8. フィールドで[参照]を選択し、テストクローンボリュームを選択して[保存]\*を選択します。
9. ウィンドウの下部で、[保存]\*を選択します。
10. クライアントで共有を開き、テストボリュームに読み取りおよび書き込み機能があることを確認します。

フェイルオーバーデータをクリーンアップし、テストボリュームを削除する

フェイルオーバーテストが完了したら、テストボリュームに関連付けられているすべてのデータをクリーンアップして削除できます。

#### 手順

1. デスティネーションクラスタで、\*[保護]>[関係]\*を選択します。
2. 選択するオプション  をクリックし、\*[テストフェイルオーバーのクリーンアップ]\*を選択します。
3. ウィンドウで、[クリーンアップ]\*を選択します。
4. [ストレージ]>[ボリューム]\*を選択し、テストボリュームが削除されたことを確認します。

## SnapMirror DR デスティネーションボリュームからのデータの提供

デスティネーションボリュームを書き込み可能にします

デスティネーションボリュームからクライアントにデータを提供する前に、そのボリュームを書き込み可能にする必要があります。を使用できます `snapmirror quiesce` デスティネーションへのスケジュールされた転送を停止するコマンドを使用します `snapmirror abort` 実行中の転送を停止するコマンド、および `snapmirror break` デスティネーションを書き込み可能にするコマンド。

このタスクについて

この手順はデスティネーション SVM またはデスティネーションクラスタから実行する必要があります。

#### 手順

### 1. デスティネーションへのスケジュールされた転送を停止します。

```
snapmirror quiesce -source-path SVM:volume|cluster://SVM/volume, ...  
-destination-path SVM:volume|cluster://SVM/volume, ...
```

コマンド構文全体については、マニュアルページを参照してください。

次の例は、ソースボリューム間のスケジュールされた転送を停止します volA オン svm1 デスティネーションボリュームを指定します volA\_dst オン svm\_backup :

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

### 2. デスティネーションへの実行中の転送を停止します。

```
snapmirror abort -source-path SVM:volume|cluster://SVM/volume, ... -destination  
-path SVM:volume|cluster://SVM/volume, ...
```

コマンド構文全体については、マニュアルページを参照してください。



SnapMirror Synchronous 関係（ONTAP 9.5 以降でサポート）ではこの手順は必要ありません。

次の例は、ソースボリューム間の実行中の転送を停止します volA オン svm1 デスティネーションボリュームを指定します volA\_dst オン svm\_backup :

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

### 3. SnapMirror DR 関係を解除します。

```
snapmirror break -source-path SVM:volume|cluster://SVM/volume, ... -destination  
-path SVM:volume|cluster://SVM/volume, ...
```

コマンド構文全体については、マニュアルページを参照してください。

次の例は、ソースボリューム間の関係を解除します volA オン svm1 デスティネーションボリュームを指定します volA\_dst オン svm\_backup :

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

ONTAP でこれを行うその他の方法

実行するタスク	参照するコンテンツ
再設計された System Manager （ ONTAP 9.7 以降で使用可能）	<a href="#">"SnapMirror デスティネーションからのデータの提供"</a>
System Manager Classic （ ONTAP 9.7 以前で使用可能）	<a href="#">"ボリュームディザスタリカバリの概要"</a>

データアクセス用のデスティネーションボリュームを設定

デスティネーションボリュームを書き込み可能にしたあとで、データにアクセスできるようにそのボリュームを設定する必要があります。NAS クライアント、 NVMe サブシステム、および SAN ホストは、ソースボリュームが再アクティブ化されるまでの間、デスティネーションボリュームのデータにアクセスできます。

NAS 環境：

1. ソースボリュームがソース SVM でマウントされていたのと同じジャンクションパスを使用して、NAS ボリュームをネームスペースにマウントします。
2. デスティネーションボリュームのSMB共有に適切なACLを適用します。
3. デスティネーションボリュームに NFS エクスポートポリシーを割り当てます。
4. デスティネーションボリュームにクォータルールを適用します。
5. デスティネーションボリュームにクライアントをリダイレクトします。
6. NFS共有とSMB共有をクライアントに再マウントします。

SAN 環境の場合：

1. ボリューム内の LUN を適切なイニシエータグループにマッピングします。
2. iSCSI の場合、SAN ホストイニシエータから SAN LIF への iSCSI セッションを作成します。
3. SAN クライアントで、ストレージの再スキャンを実行して接続された LUN を検出します。

NVMe 環境については、を参照してください ["SAN 管理"](#)。

元のソースボリュームを再有効化

デスティネーションからデータを提供する必要がなくなった場合は、ソースボリュームとデスティネーションボリュームの間で元のデータ保護関係を再確立できます。

このタスクについて

- 以下の手順は、元のソースボリュームにあるベースラインが損なわれていないことを前提としています。ベースラインが損なわれている場合は、手順を実行する前に、データの提供元のボリュームと元のソースボリュームの間の関係を作成して初期化する必要があります。
- XDP SnapMirror 関係のバックグラウンド準備とデータウェアハウジングフェーズには時間がかかることがあります。長時間にわたってステータスが「preparing」と報告されている SnapMirror 関係が表示されることは珍しくありません。

手順

### 1. 元のデータ保護関係を反転します。

```
snapmirror resync -source-path SVM:volume -destination-path SVM:volume
```

コマンド構文全体については、マニュアルページを参照してください。



このコマンドは元のソースSVMまたは元のソースクラスタから実行する必要があります。再同期の際にベースライン転送は不要ですが、再同期には時間がかかる場合があります。再同期はオフピークの時間帯に実行することを推奨します。ソースとデスティネーションに共通の Snapshot コピーが存在しない場合、このコマンドは失敗します。使用 `snapmirror initialize` 関係を再初期化してください。

次の例は、元のソースボリューム間の関係を反転します。volA オン svm1、およびデータの提供元のボリューム、volA\_dst オン svm\_backup：

```
cluster_src::> snapmirror resync -source-path svm_backup:volA_dst  
-destination-path svm1:volA
```

### 2. 元のソースへのデータアクセスを再確立する準備ができたなら、元のデスティネーションボリュームへのアクセスを停止します。そのためには、元のデスティネーションSVMを停止します。

```
vserver stop -vserver SVM
```

コマンド構文全体については、マニュアルページを参照してください。



このコマンドは元のデスティネーションSVMまたは元のデスティネーションクラスタから実行する必要があります。このコマンドは、元のデスティネーションSVM全体へのユーザーアクセスを停止します。必要に応じて、元のデスティネーションボリュームへのアクセスを停止できます。

次の例は、元のデスティネーションSVMを停止します。

```
cluster_dst::> vserver stop svm_backup
```

### 3. 反転した関係を更新します。

```
snapmirror update -source-path SVM:volume -destination-path SVM:volume
```

コマンド構文全体については、マニュアルページを参照してください。



このコマンドは元のソースSVMまたは元のソースクラスタから実行する必要があります。

次の例は、データの提供元のボリューム間の関係を更新します。volA\_dst オン svm\_backup`および元のソースボリューム `volA オン svm1：

```
cluster_src::> snapmirror update -source-path svm_backup:volA_dst  
-destination-path svm1:volA
```

4. 元のソースSVMまたは元のソースクラスタから、反転した関係のスケジュールされた転送を停止します。

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

コマンド構文全体については、マニュアルページを参照してください。



このコマンドは元のソースSVMまたは元のソースクラスタから実行する必要があります。

次の例は、元のデスティネーションボリューム間のスケジュールされた転送を停止します。 volA\_dst オン svm\_backup`および元のソースボリューム `volA オン svm1 :

```
cluster_src::> snapmirror quiesce -source-path svm_backup:volA_dst  
-destination-path svm1:volA
```

5. 最後の更新が完了し、関係のステータスが「Quiesced」と表示されたら、元のソースSVMまたは元のソースクラスタから次のコマンドを実行して、反転した関係を解除します。

```
snapmirror break -source-path SVM:volume -destination-path SVM:volume
```

コマンド構文全体については、マニュアルページを参照してください。



このコマンドは元のソースSVMまたはソースクラスタから実行する必要があります。

次の例は、元のデスティネーションボリューム間の関係を解除します。 volA\_dst オン svm\_backup`および元のソースボリューム `volA オン svm1 :

```
cluster_scr::> snapmirror break -source-path svm_backup:volA_dst  
-destination-path svm1:volA
```

6. 元のソースSVMまたは元のソースクラスタから、反転したデータ保護関係を削除します。

```
snapmirror delete -source-path SVM:volume -destination-path SVM:volume
```

コマンド構文全体については、マニュアルページを参照してください。



このコマンドは元のソースSVMまたは元のソースクラスタから実行する必要があります。

次の例は、元のソースボリューム間の反転した関係を削除します。 volA オン svm1、およびデータの提供元のボリューム、 volA\_dst オン svm\_backup :

```
cluster_src::> snapmirror delete -source-path svm_backup:volA_dst  
-destination-path svm1:volA
```

7. 元のデスティネーションSVMまたは元のデスティネーションクラスタから反転した関係を解放します。

```
snapmirror release -source-path SVM:volume -destination-path SVM:volume
```



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

次の例は、元のデスティネーションボリューム間の反転した関係を解放します。 volA\_dst オン svm\_backup`および元のソースボリューム `volA オン svm1 :

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

8. 元のデスティネーションから元のデータ保護関係を再確立します。

```
snapmirror resync -source-path SVM:volume -destination-path SVM:volume
```

コマンド構文全体については、マニュアルページを参照してください。

次の例は、元のソースボリューム間の関係を再確立します。 volA オン svm1、および元のデスティネーションボリューム volA\_dst オン svm\_backup :

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

9. 必要に応じて、元のデスティネーションSVMを起動します。

```
vserver start -vserver SVM
```

コマンド構文全体については、マニュアルページを参照してください。

次の例は、元のデスティネーションSVMを起動します。

```
cluster_dst::> vserver start svm_backup
```

完了後

を使用します snapmirror show コマンドを実行して、SnapMirror関係が作成されたことを確認します。コマンド構文全体については、マニュアルページを参照してください。

## SnapMirror デスティネーションボリュームからファイルをリストアします

単一ファイル、**LUN**、または **NVMe** のネームスペースを **SnapMirror** デスティネーションからリストアします

単一ファイルまたは LUN、あるいは一連のファイルまたは LUN を Snapshot コピーからリストアしたり、NVMe ネームスペースを SnapMirror デスティネーションボリュームからリストアしたりできます。ONTAP 9.7 以降では、SnapMirror Synchronous デスティネーションから NVMe ネームスペースをリストアすることもできます。ファイルは元のソースボリュームにリストアするか、別のボリュームにリストアできます。

### 必要なもの

ファイルまたは LUN を SnapMirror Synchronous デスティネーション（ONTAP 9.5 以降でサポート）からリストアするには、先に関係を削除して解放しておく必要があります。

### このタスクについて

ファイルまたは LUN のリストア先のボリューム（デスティネーションボリューム）は読み書き可能なボリュームである必要があります。

- ソースボリュームとデスティネーションボリュームに共通の Snapshot コピーがある場合（通常、リストア先が元のソースボリュームである場合と同様）、SnapMirror は `_incremental restore_x` を実行します。
- それ以外の場合、SnapMirror は `_ベースラインリストア` を実行します。これにより、指定された Snapshot コピーおよびコピーが参照するすべてのデータブロックがデスティネーションボリュームに転送されます。

### 手順

1. デスティネーションボリューム内の Snapshot コピーの一覧を表示します。

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

コマンド構文全体については、マニュアルページを参照してください。

次の例は、上の Snapshot コピーを示しています `vserverB:secondary1` 目的地：



```
cluster_dst:> volume snapshot show -vserver vserverB -volume secondary1
```

Vserver	Volume	Snapshot	State	Size	Total% Used%
-----	-----	-----	-----	-----	-----
vserverB	secondary1	hourly.2013-01-25_0005	valid	224KB	0%
0%		daily.2013-01-25_0010	valid	92KB	0%
0%		hourly.2013-01-25_0105	valid	228KB	0%
0%		hourly.2013-01-25_0205	valid	236KB	0%
0%		hourly.2013-01-25_0305	valid	244KB	0%
0%		hourly.2013-01-25_0405	valid	244KB	0%
0%		hourly.2013-01-25_0505	valid	244KB	0%

7 entries were displayed.

2. 単一ファイルまたは LUN、あるいは一連のファイルまたは LUN を、 SnapMirror デスティネーションボリューム内の Snapshot コピーからリストアします。

```
snapmirror restore -source-path SVM:volume|cluster://SVM/volume, ...
-destination-path SVM:volume|cluster://SVM/volume, ... -source-snapshot snapshot
-file-list source_file_path,@destination_file_path
```

コマンド構文全体については、マニュアルページを参照してください。



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

ファイルをリストアするコマンドの例を次に示します file1 および file2 Snapshot コピーから削除します daily.2013-01-25\_0010 (元のデスティネーションボリューム内) secondary1`を元のソースボリュームのアクティブファイルシステム内の同じ場所に移動します `primary1:

```
cluster_dst:> snapmirror restore -source-path vserverB:secondary1
-destination-path vserverA:primary1 -source-snapshot daily.2013-01-
25_0010 -file-list /dir1/file1,/dir2/file2
```

```
[Job 3479] Job is queued: snapmirror restore for the relationship with
destination vserverA:primary1
```

ファイルをリストアするコマンドの例を次に示します file1 および file2 Snapshotコピーから削除します daily.2013-01-25\_0010（元のデスティネーションボリューム内） secondary1`を元のソースボリュームのアクティブファイルシステム内の別の場所に移動します `primary1。

@ マークに続くパスがデスティネーションファイルのパスで、元のソースボリュームのルートからのパスを指定しています。この例では、file1 がにリストアされます /dir1/file1.new file2はにリストアされます /dir2.new/file2 オン primary1：

```
cluster_dst:> snapmirror restore -source-path vserverB:secondary1
-destination-path vserverA:primary1 -source-snapshot daily.2013-01-
25_0010 -file-list
/dir/file1,@/dir1/file1.new,/dir2/file2,@/dir2.new/file2
```

```
[Job 3479] Job is queued: snapmirror restore for the relationship with
destination vserverA:primary1
```

ファイルをリストアするコマンドの例を次に示します file1 および file3 Snapshotコピーから削除します daily.2013-01-25\_0010（元のデスティネーションボリューム内） secondary1`を元のソースボリュームのアクティブファイルシステム内の別の場所に移動します `primary1、およびリストアを実行します file2 移動元 snap1 をアクティブファイルシステム内の同じ場所に移動します primary1。

この例では、ファイルです file1 がにリストアされます /dir1/file1.new および file3 がにリストアされます /dir3.new/file3：

```
cluster_dst:> snapmirror restore -source-path vserverB:secondary1
-destination-path vserverA:primary1 -source-snapshot daily.2013-01-
25_0010 -file-list
/dir/file1,@/dir1/file1.new,/dir2/file2,/dir3/file3,@/dir3.new/file3
```

```
[Job 3479] Job is queued: snapmirror restore for the relationship with
destination vserverA:primary1
```

## SnapMirror デスティネーションからボリュームの内容をリストアします

SnapMirror デスティネーションボリューム内の Snapshot コピーからボリューム全体の内容をリストアできます。ボリュームの内容は元のソースボリュームにリストアするか、別のボリュームにリストアできます。

このタスクについて

リストア処理のデスティネーションボリュームは次のいずれかにする必要があります。

- 読み書き可能なボリューム。このケースでは、ソースボリュームとデスティネーションボリュームに共通の Snapshot コピーがある（通常、リストア先が元のソースボリュームである）場合、SnapMirror は `_incremental restore_x` を実行します。



共通の Snapshot コピーがない場合、コマンドは失敗します。空の読み書き可能なボリュームにボリュームの内容をリストアすることはできません。

- 空のデータ保護ボリューム。このケースでは、SnapMirror は `_ベースラインリストア_` を実行します。これにより、指定された Snapshot コピーおよびコピーが参照するすべてのデータブロックがソースボリュームに転送されます。

ボリュームの内容のリストアはシステム停止を伴う処理です。リストア処理の実行中は、SnapVaultプライマリボリュームでSMBトラフィックが実行されていない必要があります。

リストア処理のデスティネーションボリュームで圧縮が有効になっていて、ソースボリュームで圧縮が有効になっていない場合は、デスティネーションボリュームで圧縮を無効にします。リストア処理の完了後に、圧縮を再度有効にする必要があります。

デスティネーションボリュームに対して定義されたクォータルールは、リストアの実行前に非アクティブ化されます。を使用できます `volume quota modify` リストア処理の完了後にクォータルールを再アクティブ化するコマンド。

#### 手順

1. デスティネーションボリューム内の Snapshot コピーの一覧を表示します。

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

コマンド構文全体については、マニュアルページを参照してください。

次の例は、上のSnapshotコピーを示しています `vserverB:secondary1` 目的地：

```
cluster_dst::> volume snapshot show -vserver vsverB -volume secondary1
```

Vserver Used%	Volume	Snapshot	State	Size	Total%
----- -----	-----	-----	-----	-----	-----
vsverB 0%	secondary1	hourly.2013-01-25_0005	valid	224KB	0%
0%		daily.2013-01-25_0010	valid	92KB	0%
0%		hourly.2013-01-25_0105	valid	228KB	0%
0%		hourly.2013-01-25_0205	valid	236KB	0%
0%		hourly.2013-01-25_0305	valid	244KB	0%
0%		hourly.2013-01-25_0405	valid	244KB	0%
0%		hourly.2013-01-25_0505	valid	244KB	0%

7 entries were displayed.

2. SnapMirror デスティネーションボリューム内の Snapshot コピーからボリュームの内容をリストアします。

```
snapmirror restore -source-path <SVM:volume>|<cluster://SVM/volume>  
-destination-path <SVM:volume>|<cluster://SVM/volume> -source-snapshot  
<snapshot>
```

コマンド構文全体については、マニュアルページを参照してください。



このコマンドは元のソースSVMまたは元のソースクラスタから実行する必要があります。

次のコマンドは、元のソースボリュームの内容をリストアします primary1 Snapshotコピーから削除します daily.2013-01-25\_0010 （元のデスティネーションボリューム内） secondary1 :

```
cluster_src::> snapmirror restore -source-path vserverB:secondary1
-destination-path vserverA:primary1 -source-snapshot daily.2013-01-
25_0010
```

Warning: All data newer than Snapshot copy daily.2013-01-25\_0010 on volume vserverA:primary1 will be deleted.

Do you want to continue? {y|n}: y

[Job 34] Job is queued: snapmirror restore from source vserverB:secondary1 for the snapshot daily.2013-01-25\_0010.

3. リストアしたボリュームを再マウントし、ボリュームを使用するすべてのアプリケーションを再起動します。

ONTAP でこれを行うその他の方法

実行するタスク	参照するコンテンツ
再設計された System Manager （ ONTAP 9.7 以降で使用可能）	<a href="#">"以前の Snapshot コピーからボリュームをリストアします"</a>
System Manager Classic （ ONTAP 9.7 以前で使用可能）	<a href="#">"SnapVault によるボリュームリストアの概要"</a>

## レプリケーション関係を手動で更新

ソースボリュームが移動されたために更新が失敗した場合は、レプリケーション関係を手動で更新しなければならないことがあります。

このタスクについて

レプリケーション関係を手動で更新するまで、SnapMirror は移動されたソースボリュームからの転送をすべて中止します。

ONTAP 9.5 以降では、SnapMirror Synchronous 関係がサポートされます。これらの関係ではソースボリュームとデスティネーションボリュームは常に同期された状態ですが、セカンダリクラスタの表示は 1 時間おきにはプライマリと同期されません。デスティネーションのポイントインタイムデータを表示する場合は、実行して手動更新を実行する必要があります snapmirror update コマンドを実行します

### ステップ

1. レプリケーション関係を手動で更新します。

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

コマンド構文全体については、マニュアルページを参照してください。



このコマンドはデスティネーション SVM またはデスティネーションクラスタから実行する必要があります。ソースとデスティネーションに共通の Snapshot コピーが存在しない場合、このコマンドは失敗します。使用 `snapmirror initialize` 関係を再初期化してください。

次の例は、ソースボリューム間の関係を更新します `volA` オン `svm1` デスティネーションボリュームを指定します `volA_dst` オン `svm_backup` :

```
cluster_src::> snapmirror update -source-path svm1:volA -destination  
-path svm_backup:volA_dst
```

## レプリケーション関係を再同期

デスティネーションボリュームを書き込み可能にしたあと、ソースボリュームとデスティネーションボリュームに共通の Snapshot コピーが存在しないために更新が失敗したあと、または関係のレプリケーションポリシーを変更した場合には、レプリケーション関係の再同期が必要です。

このタスクについて

- 再同期の際にベースライン転送は不要ですが、再同期には時間がかかる場合があります。再同期はオフピークの時間帯に実行することを推奨します。
- ファンアウト構成またはカスケード構成の一部であるボリュームの再同期には時間がかかることがあります。長時間にわたってステータスが「preparing」と報告されている SnapMirror 関係が表示されることは珍しくありません。

### ステップ

1. ソースボリュームとデスティネーションボリュームを再同期します。

```
snapmirror resync -source-path SVM:volume|cluster://SVM/volume, ... -destination  
-path SVM:volume|cluster://SVM/volume, ... -type DP|XDP -policy policy
```

コマンド構文全体については、マニュアルページを参照してください。



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

次の例は、ソースボリューム間の関係を再同期します `volA` オン `svm1` デスティネーションボリュームを指定します `volA_dst` オン `svm_backup` :

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

## ボリュームレプリケーション関係を削除します

を使用できます `snapmirror delete` および `snapmirror release` ボリュームレプリケーション関係を削除するコマンド。続いて、不要なデスティネーションボリュームを手動で削除できます。

このタスクについて

。 `snapmirror release` コマンドは、SnapMirrorで作成されたSnapshotコピーをソースから削除します。使用できます `-relationship-info-only` Snapshotコピーを保持するオプション。

手順

1. レプリケーション関係を休止します。

```
snapmirror quiesce -destination-path SVM:volume|cluster://SVM/volume
```

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

2. (オプション) デスティネーションボリュームを読み取り/書き込みボリュームにする必要がある場合は、レプリケーション関係を解除します。デスティネーションボリュームを削除する場合やボリュームの読み取り/書き込みが不要な場合は、この手順を省略できます。

```
snapmirror break -source-path SVM:volume|cluster://SVM/volume, ... -destination-path SVM:volume|cluster://SVM/volume, ...
```

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

3. レプリケーション関係を削除します。

```
snapmirror delete -source-path SVM:volume|cluster://SVM/volume, ... -destination-path SVM:volume|cluster://SVM/volume, ...
```

コマンド構文全体については、マニュアルページを参照してください。



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

次の例は、ソースボリューム間の関係を削除します `volA` オン `svm1` デスティネーションボリュームを指定します `volA_dst` オン `svm_backup` :

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

4. ソース SVM からレプリケーション関係情報をリリースします。

```
snapmirror release -source-path SVM:volume|cluster://SVM/volume, ...  
-destination-path SVM:volume|cluster://SVM/volume, ...
```

コマンド構文全体については、マニュアルページを参照してください。



このコマンドはソースクラスタまたはソース SVM から実行する必要があります。

次の例は、指定したレプリケーション関係の情報をソースSVMからリリースします svm1 :

```
cluster_src::> snapmirror release -source-path svm1:volA -destination  
-path svm_backup:volA_dst
```

## ストレージ効率の管理

SnapMirror は、ソースボリュームとデスティネーションボリュームでストレージ効率を維持します。ただし、例外が 1 つあり、デスティネーションでポストプロセスデータ圧縮が有効になっている場合、ストレージ効率は維持されません。その場合、デスティネーションではすべてのストレージ効率が失われます。この問題を修正するには、デスティネーションでポストプロセス圧縮を無効にして、関係を手動で更新し、Storage Efficiency を再度有効にする必要があります。

必要なもの

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

### "クラスタと SVM のピアリング"

- デスティネーションでポストプロセス圧縮を無効にする必要があります。

このタスクについて

を使用できます volume efficiency show コマンドを使用して、ボリュームで効率化が有効になっているかどうかを確認します。詳細については、マニュアルページを参照してください。

SnapMirror 監査ログを表示し、転送概要を特定することで、SnapMirror によるストレージ効率化が維持されているかどうかを確認できます。転送概要 が表示されている場合 `transfer\_desc=Logical Transfer` SnapMirror ではストレージ効率は維持されません。転送概要 が表示されている場合 `transfer\_desc=Logical Transfer with Storage Efficiency` SnapMirror はストレージ効率を維持します。例：

```
Fri May 22 02:13:02 CDT 2020 ScheduledUpdate[May 22 02:12:00]:cc0fbc29-  
b665-11e5-a626-00a09860c273 Operation-Uid=39fbcf48-550a-4282-a906-  
df35632c73a1 Group=none Operation-Cookie=0 action=End source=<sourcepath>  
destination=<destpath> status=Success bytes_transferred=117080571  
network_compression_ratio=1.0:1 transfer_desc=Logical Transfer - Optimized  
Directory Mode
```



## ストレージを使用した論理転送

ONTAP 9.3 以降では、Storage Efficiency を再度有効にするための手動更新が不要になりました。SnapMirror では、ポストプロセス圧縮が無効になったことを検出すると、スケジュールされた次の更新時に Storage Efficiency を自動的に再度有効にします。ソースとデスティネーションの両方で ONTAP 9.3 を実行している必要があります。

ONTAP 9.3 以降では、デスティネーションボリュームが書き込み可能になったあとで、AFF システムが Storage Efficiency の設定を FAS システムとは異なる方法で管理します。

- を使用してデスティネーションボリュームを書き込み可能にしたあと `snapmirror break` コマンドを実行した場合、ボリュームのキャッシングポリシーは自動的に「auto」（デフォルト）に設定されます。



この動作は FlexVol ボリュームにのみ該当し、FlexGroup ボリュームには適用されません。

- 再同期時に、キャッシングポリシーは自動的に「none」に設定され、重複排除およびインライン圧縮は、元の設定に関係なく自動的に無効になります。必要に応じて、設定を手動で変更する必要があります。



Storage Efficiency が有効な状態での手動更新には時間がかかる場合があります。この処理はオフピークの時間帯に実行することを推奨します。

### ステップ

1. レプリケーション関係を更新して、Storage Efficiency を再度有効にします。

```
snapmirror update -source-path SVM:volume|cluster://SVM/volume, ... -destination  
-path SVM:volume|cluster://SVM/volume, ... -enable-storage-efficiency true
```

コマンド構文全体については、マニュアルページを参照してください。



このコマンドはデスティネーション SVM またはデスティネーションクラスタから実行する必要があります。ソースとデスティネーションに共通の Snapshot コピーが存在しない場合、このコマンドは失敗します。使用 `snapmirror initialize` 関係を再初期化してください。

次の例は、ソースボリューム間の関係を更新します `volA` オン `svm1` デスティネーションボリュームを指定します `volA_dst` オン ``svm_backup`` Storage Efficiency を再度有効にします。

```
cluster_dst::> snapmirror update -source-path svm1:volA -destination  
-path svm_backup:volA_dst -enable-storage-efficiency true
```

## SnapMirror グローバルスロットルを使用します

グローバルネットワークスロットルは、ノード単位のすべての SnapMirror および SnapVault 転送で使用できます。

このタスクについて

SnapMirror グローバルスロットルは、送受信される SnapMirror 転送および SnapVault 転送で使用する帯域幅を制限します。この制限は、クラスタ内のすべてのノードで適用されます。

たとえば、送信スロットルを100Mbpsに設定した場合は、クラスタ内の各ノードで送信帯域幅が100Mbpsに設定されます。グローバルスロットルを無効にすると、すべてのノードで無効になります。

データ転送速度は多くの場合ビット / 秒 (bps) で表されますが、スロットル値はキロバイト / 秒 (KBps) で入力する必要があります。



ONTAP 9.9.1以前のリリースでは、スロットルはに影響しません volume move 転送または負荷共有ミラー転送。ONTAP 9.10.0以降では、ボリューム移動処理をスロットルするオプションを指定できます。詳細については、を参照してください ["ONTAP 9.10以降でボリューム移動のスロットルを行う方法"](#)

グローバルスロットルは、SnapMirror 転送および SnapVault 転送の関係ごとのスロットル機能と連動します。関係ごとのスロットルは、関係ごとの転送の帯域幅の合計がグローバルスロットルの値を超えるまで有効で、超えたあとはグローバルスロットルが有効になります。スロットル値 0 グローバルスロットルが無効になっていることを示します。



SnapMirror グローバルスロットルは、SnapMirror Synchronous 関係が In-Sync になっている場合は効果がありません。ただし、初期化処理や Out of Sync イベントなどの非同期転送フェーズを実行した場合は、スロットルは SnapMirror Synchronous 関係に影響しません。そのため、SnapMirror Synchronous 関係でグローバルスロットルを有効にすることは推奨されません。

#### 手順

1. グローバルスロットルを有効にします。

```
options -option-name replication.throttle.enable on|off
```

次の例は、でSnapMirrorグローバルスロットルを有効にする方法を示しています cluster\_dst :

```
cluster_dst::> options -option-name replication.throttle.enable on
```

2. デスティネーションクラスタで受信転送に使用される総帯域幅について最大値を指定します。

```
options -option-name replication.throttle.incoming.max_kbs KBps
```

推奨される最小スロットル帯域幅は 4KBps で、最大値は 2TBps です。このオプションのデフォルト値はです `unlimited` これは、使用される総帯域幅に制限がないことを意味します。

次の例は、受信転送で使用される総帯域幅について最大値を 100Mbps に設定する方法を示しています。

```
cluster_dst::> options -option-name  
replication.throttle.incoming.max_kbs 12500
```



100 Mbps = 12500 kbps

3. ソースクラスタで送信転送に使用される総帯域幅について最大値を指定します。

```
options -option-name replication.throttle.outgoing.max_kbs KBps
```

推奨される最小スロットル帯域幅は 4KBps で、最大値は 2TBps です。このオプションのデフォルト値は `unlimited` これは、使用される総帯域幅に制限がないことを意味します。パラメータ値はkbps単位です。

次の例は、送信転送で使用される総帯域幅について最大値を 100Mbps に設定する方法を示しています。

```
cluster_src::> options -option-name  
replication.throttle.outgoing.max_kbs 12500
```

## SnapMirror SVM レプリケーションを管理します

### SnapMirror SVM レプリケーションの概要

SnapMirrorを使用すると、SVM間のデータ保護関係を作成できます。このタイプのデータ保護関係では、SVM のすべてまたは一部の設定が NFS エクスポートおよび SMB 共有から RBAC にレプリケートされます。また、SVM が所有するボリューム内のデータもレプリケートされます。

サポートされている関係タイプ

レプリケート可能なのはデータ提供用SVMのみです。サポートされるデータ保護関係タイプは次のとおりです。

- SnapMirror DR : \_ 通常、デスティネーションにはソース上に現在ある Snapshot コピーだけが含まれます。

ONTAP 9.9.1以降では、mirror-vaultポリシーを使用している場合にこの動作が変更されます。ONTAP 9.9.1以降では、ソースとデスティネーションで異なるSnapshotポリシーを作成できます。デスティネーションのSnapshotコピーがソースのSnapshotコピーで上書きされることはありません。

- スケジュールされた通常の処理、更新、および再同期の実行中に、ソースからデスティネーションに上書きされることはありません
- 解除処理の実行中に削除されることはありません。
- 逆再同期処理の実行中は削除されません。  
ONTAP 9.9.1以降を使用してmirror-vaultポリシーを使用してSVMディザスタ関係を設定する場合、ポリシーは次のように動作します。
- ソースでのユーザ定義の Snapshot コピーポリシーは、デスティネーションにコピーされません。
- システム定義の Snapshot コピーポリシーはデスティネーションにコピーされません。
- ユーザおよびシステム定義の Snapshot ポリシーとのボリュームの関連付けはデスティネーションにコピーされません。

[+]

SVM :

- ONTAP 9.2 以降では、\_SnapMirror ユニファイドレプリケーション。デスティネーションに DR と長期保持の両方が設定されています。

これらの関係タイプの詳細については、を参照してください。"[SnapMirror ボリュームレプリケーションの概要](#)"。

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

ポリシータイプ	関係タイプ
非同期ミラー	SnapMirror DR
ミラー - バックアップ	ユニファイドレプリケーション

**ONTAP 9.4** では、**XDP** が **DP** に代わって **SVM** レプリケーションのデフォルトになりました

ONTAP 9.4 以降では、SVM データ保護関係のデフォルトが XDP モードに変更されました。ONTAP 9.3 以前の SVM データ保護関係のデフォルトは引き続き DP モードです。

新しいデフォルトは既存の関係には影響しません。DP タイプの既存の関係は引き続き DP タイプになります。次の表に、想定される動作を示します。

指定するモード	タイプ	デフォルトポリシー（ポリシーを指定しない場合）
DP	XDP	MirrorAllSnapshots（SnapMirror DR）
なし	XDP	MirrorAllSnapshots（SnapMirror DR）
XDP	XDP	MirrorAndVault（ユニファイドレプリケーション）

デフォルトの変更の詳細については、以下を参照してください。"[XDP は、DP を SnapMirror のデフォルトとして置き換えます](#)"。



バージョンに依存しないレプリケーションは、SVM レプリケーションではサポートされません。SVMディザスタリカバリ設定では、フェイルオーバーおよびフェイルバック処理をサポートするために、デスティネーションSVMがソースSVMクラスタと同じバージョンのONTAPを実行しているクラスタである必要があります。

"[SnapMirror 関係に対応した ONTAP バージョン](#)"

## SVM の設定のレプリケート方法

SVM レプリケーション関係の内容は、以下に示すフィールドの設定の組み合わせによって決定されます。

- `-identity-preserve true` のオプション `snapmirror create` コマンドは、SVMの設定全体をレプリケートします。
- `-identity-preserve false` オプションは、SVMのボリュームと認証と許可の設定、およびに記載されているプロトコルとネームサービスの設定のみをレプリケートします ["SVMディザスタリカバリ関係でレプリケートされる設定"](#)。
- `-discard-configs network` のオプション `snapmirror policy create` このコマンドは、ソースとデスティネーションのSVMが異なるサブネットにある場合に使用するLIFおよび関連ネットワーク設定をSVMレプリケーション対象から除外します。
- `-vserver-dr-protection unprotected` のオプション `volume modify` 指定したボリュームをSVMレプリケーション対象から除外します。

上記の点を除き、SVM レプリケーションはボリュームレプリケーションとほぼ同じです。ボリュームレプリケーションとほぼ同じワークフローを SVM レプリケーションにも使用できます。

## サポートの詳細

次の表は、SnapMirror SVM レプリケーションのサポートの詳細を示しています。

リソースまたは機能	サポートの詳細
導入タイプ	<ul style="list-style-type: none"> <li>• 単一のソースから単一のデスティネーション</li> <li>• ONTAP 9.4 以降はファンアウトファンアウトできるのは 2 つの宛先だけです。</li> </ul> <p>デフォルトでは、<code>-identity-preserve true</code> の関係はソース SVM ごとに 1 つだけ許可されます。</p>
関係タイプ	<ul style="list-style-type: none"> <li>• SnapMirrorディザスタリカバリ</li> <li>• ONTAP 9.2 以降では、SnapMirror ユニファイドレプリケーションがサポートされます</li> </ul>
レプリケーションの範囲	クラスタ間のみ。同じクラスタ内の SVM をレプリケートすることはできません。
自律的なランサムウェア防御	<ul style="list-style-type: none"> <li>• ONTAP 9.12.1以降でサポート。詳細については、<a href="#">を参照してください</a> <a href="#">"自律的なランサムウェア防御"</a></li> </ul>
整合グループの非同期サポート	ONTAP 9.14.1以降では、整合グループが存在する場合に最大32個のSVMディザスタリカバリ関係がサポートされます。 <a href="#">を参照してください</a> <a href="#">"整合グループを保護する"</a> および <a href="#">"整合グループの制限"</a> を参照してください。
FabricPool	ONTAP 9.6 以降の FabricPool では、SnapMirror SVM レプリケーションがサポートされます。

MetroCluster	<p>ONTAP 9.11.1以降では、MetroCluster構成内のSVMディザスタリカバリ関係の両側を、SVMディザスタリカバリ設定のソースとして使用できます。</p> <p>ONTAP 9.5 以降の MetroCluster 構成では、SnapMirror SVM レプリケーションがサポートされます。</p> <ul style="list-style-type: none"> <li>• ONTAP 9.10.Xより前のリリースでは、MetroCluster構成をSVMディザスタリカバリ関係のデスティネーションにすることはできません。</li> <li>• ONTAP 9.10.1以降のリリースでは、MetroCluster構成は移行目的でのみSVMディザスタリカバリ関係のデスティネーションとして使用でき、に記載されている必要なすべての要件を満たしている必要があります。"<a href="#">TR-4966：『Migrating a SVM into a MetroCluster 解決策』</a>"。</li> <li>• SVM ディザスタリカバリ関係のソースとして使用できるのは、 MetroCluster 構成内のアクティブな SVM だけです。</li> </ul> <p>スイッチオーバー前の同期元の SVM とスイッチオーバー後の同期先の SVM のどちらもソースに使用できます。</p> <ul style="list-style-type: none"> <li>• MetroCluster 構成が安定した状態のときは MetroCluster の同期先の SVM はオンラインでないため、同期先ボリュームを SVM ディザスタリカバリ関係のソースにすることはできません。</li> <li>• 同期元のSVMがSVMディザスタリカバリ関係のソースである場合は、ソースのSVMディザスタリカバリ関係の情報がMetroClusterパートナーにレプリケートされます。</li> <li>• スイッチオーバーおよびスイッチバックの処理中に、SVMディザスタリカバリデスティネーションへのレプリケーションが失敗することがあります。</li> </ul> <p>ただし、スイッチオーバーまたはスイッチバックのプロセスが完了すると、SVMディザスタリカバリの次のスケジュールされた更新は成功します。</p>
整合グループ	<p>ONTAP 9.14.1以降でサポートされます。詳細については、<a href="#">を参照してください 整合グループを保護する。</a></p>
ONTAP S3の略	<p>SVMディザスタリカバリではサポートされません。</p>

SnapMirror Synchronous	SVMディザスタリカバリではサポートされません。
バージョンに依存しません	サポート対象外
ボリューム暗号化	<ul style="list-style-type: none"> <li>• ソースで暗号化されたボリュームがデスティネーションで暗号化されます。</li> <li>• オンボードキーマネージャまたは KMIP サーバをデスティネーションで設定する必要があります。</li> <li>• 新しい暗号化キーはデスティネーションで生成されます。</li> <li>• ボリューム暗号化をサポートするノードがデスティネーションに含まれていない場合、レプリケーションは成功しますが、デスティネーションボリュームは暗号化されません。</li> </ul>

### SVMディザスタリカバリ関係でレプリケートされる設定

次の表に、の相互作用を示します `snapmirror create -identity-preserve` オプションとを使用します `snapmirror policy create -discard-configs network` オプション：

設定のレプリケート		<b>-identity-preserve true</b>		<b>-identity-preserve false</b>
		*ポリシーなし -discard -configs network SET *	*とのポリシー -discard -configs network SET *	
ネットワーク	NAS LIF	はい。	いいえ	いいえ
LIF の Kerberos 設定	はい。	いいえ	いいえ	SAN LIF
いいえ	いいえ	いいえ	ファイアウォールポリシー	はい。
はい。	いいえ	サービスポリシー	はい。	はい。
いいえ	ルート	はい。	いいえ	いいえ
ブロードキャストドメイン	いいえ	いいえ	いいえ	サブネット
いいえ	いいえ	いいえ	表示されます	いいえ

いいえ	いいえ	SMB	SMBサアハ	はい。
はい。	いいえ	ローカルグループおよびローカルユーザ	はい。	はい。
はい。	権限	はい。	はい。	はい。
シャドウコピー	はい。	はい。	はい。	BranchCache
はい。	はい。	はい。	サーバオプション	はい。
はい。	はい。	サーバセキュリティ	はい。	はい。
いいえ	ホームディレクトリ、共有	はい。	はい。	はい。
シンボリックリンク	はい。	はい。	はい。	Fpolicy ポリシー、Fsecurity ポリシー、および Fsecurity NTFS です
はい。	はい。	はい。	ネームマッピングとグループマッピング	はい。
はい。	はい。	監査情報	はい。	はい。
はい。	NFS	エクスポートポリシー	はい。	はい。
いいえ	エクスポートポリシールール	はい。	はい。	いいえ
NFS サーバ	はい。	はい。	いいえ	RBAC
セキュリティ証明書	はい。	はい。	いいえ	ログインユーザ、公開鍵、ルール、およびロールの設定
はい。	はい。	はい。	SSL	はい。
はい。	いいえ	ネームサービス	DNS および DNS ホスト	はい。
はい。	いいえ	UNIX ユーザおよび UNIX グループ	はい。	はい。



はい。	Kerberos Realm および Kerberos キーブロック	はい。	はい。	いいえ
LDAP および LDAP クライアント	はい。	はい。	いいえ	ネットグループ
はい。	はい。	いいえ	NIS	はい。
はい。	いいえ	Web および Web アクセス	はい。	はい。
いいえ	ボリューム	オブジェクト	はい。	はい。
はい。	Snapshot コピー、Snapshot ポリシー、および自動削除ポリシー	はい。	はい。	はい。
効率化ポリシー	はい。	はい。	はい。	クォータポリシーおよびクォータポリシールール
はい。	はい。	はい。	リカバリキュー	はい。
はい。	はい。	ルートボリューム	ネームスペース	はい。
はい。	はい。	ユーザデータ	いいえ	いいえ
いいえ	qtree	いいえ	いいえ	いいえ
クォータ	いいえ	いいえ	いいえ	ファイルレベルの QoS
いいえ	いいえ	いいえ	属性：ルートボリュームの状態、スペースギャランティ、サイズ、オートサイズ、およびファイル総数	いいえ
いいえ	いいえ	Storage QoS	QoS ポリシーグループ	はい。

はい。	はい。	Fibre Channel (FC ; ファイバチャネル)	いいえ	いいえ
いいえ	iSCSI	いいえ	いいえ	いいえ
LUN	オブジェクト	はい。	はい。	はい。
igroup 数	いいえ	いいえ	いいえ	ポートセット
いいえ	いいえ	いいえ	シリアル番号	いいえ
いいえ	いいえ	SNMP	v3 ユーザ	はい。

## SVMディザスタリカバリのストレージ制限

次の表に、ストレージオブジェクトごとにサポートされる推奨されるボリュームおよびSVMディザスタリカバリ関係の最大数を示します。制限はプラットフォームによって異なることが多いので注意してください。を参照してください ["Hardware Universe"](#) をクリックして、それぞれの構成の制限事項を確認してください。

ストレージオブジェクト	制限 (Limit)
SVM	300個のフレキシブルボリューム
HA ペア	フレキシブルボリューム×1、000
クラスタ	128個のSVMディザスタ関係

## SVM 設定をレプリケート

### SnapMirror SVM レプリケーションのワークフロー

SnapMirror SVM レプリケーションでは、デスティネーション SVM を作成し、レプリケーションジョブスケジュールを作成し、 SnapMirror 関係を作成して初期化します。

ニーズに最適なレプリケーションワークフローを決定する必要があります。

- ["SVM の設定全体をレプリケート"](#)
- ["SVM レプリケーション対象から LIF と関連ネットワークの設定を除外"](#)
- ["ネットワーク、ネームサービス、およびその他の設定をSVM設定から除外する"](#)

### ボリュームをデスティネーション SVM に配置する際の基準

ボリュームをソース SVM からデスティネーション SVM にレプリケートするときは、アグリゲートの選択基準を理解しておくことが重要です。

アグリゲートは次の基準に基づいて選択されます。

- ボリュームは常にルート以外のアグリゲートに配置されます。
- ルート以外のアグリゲートの中から、利用可能な空きスペースとホストしている既存のボリュームの数に基づいてアグリゲートが選択されます。

空きスペースが多く、ボリューム数が少ないアグリゲートほど優先順位が高くなります。最も優先順位が高いアグリゲートが選択されます。

- FabricPool アグリゲートのソースボリュームは、同じ階層化ポリシーを使用するデスティネーションの FabricPool アグリゲートに配置されます。
- ソース SVM のボリュームが Flash Pool アグリゲートにある場合、デスティネーション SVM に Flash Pool アグリゲートがあり、そのアグリゲートに十分な空きスペースがあれば、そのアグリゲートにボリュームが配置されます。
- 状況に応じて `-space-guarantee` レプリケートされるボリュームのオプションがに設定されている ``volume`` 空きスペースがボリュームサイズよりも大きいアグリゲートのみが考慮されます。
- ボリュームのサイズは、ソースボリュームのサイズに基づいて、レプリケーション時にデスティネーション SVM で自動的に拡張されます。

デスティネーション SVM のサイズを事前にリザーブする場合は、ボリュームのサイズを変更する必要があります。ソース SVM に基づいて、デスティネーション SVM でボリュームのサイズが自動的に縮小されることはありません。

ボリュームをアグリゲート間で移動する場合は、を使用できます `volume move` デスティネーション SVM でコマンドを実行します。

## SVM の設定全体をレプリケート

を使用できます `-identity-preserve true` のオプション `snapmirror create` SVM の設定全体をレプリケートするコマンド。

作業を開始する前に

ソースクラスタとデスティネーションクラスタ、および SVM のピア関係が確立されている必要があります。詳細については、を参照してください ["クラスタピア関係を作成"](#) および ["SVM のクラスタ間ピア関係を作成します"](#)。

コマンド構文全体については、マニュアルページを参照してください。

このタスクについて

このワークフローでは、デフォルトポリシーまたはカスタムレプリケーションポリシーをすでに使用していることを前提としています。

ONTAP 9.9.1以降では、`mirror-vault` ポリシーを使用すると、ソース SVM とデスティネーション SVM で異なる Snapshot ポリシーを作成でき、デスティネーションの Snapshot コピーがソースの Snapshot コピーで上書きされることはありません。詳細については、を参照してください ["SnapMirror SVM レプリケーションの概要"](#)。

手順

1. デスティネーション SVM を作成します。

```
vserver create -vserver SVM_name -subtype dp-destination
```

SVM 名はソースクラスタとデスティネーションクラスタの間で一意である必要があります。

次の例は、という名前のデスティネーションSVMを作成します `svm_backup` :

```
cluster_dst:> vserver create -vserver svm_backup -subtype dp-destination
```

2. デスティネーションクラスタから、を使用してSVMピア関係を作成します `vserver peer create` コマンドを実行します

詳細については、を参照してください ["SVM のクラスタ間ピア関係を作成します"](#)。

3. レプリケーションジョブスケジュールを作成

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

の場合 `-month`、`-dayofweek` および `-hour` を指定できます ``all`` 毎月、曜日、および時間ごとにジョブを実行します。



SVM SnapMirror関係にあるFlexVol ボリュームに対してサポートされる最小スケジュール (RPO) は15分です。SVM SnapMirror関係にあるFlexGroup ボリュームに対してサポートされる最小スケジュール (RPO) は30分です。

次の例は、という名前のジョブスケジュールを作成します `my_weekly` 土曜日の午前3時に実行されます。

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

4. デスティネーション SVM またはデスティネーションクラスタから、レプリケーション関係を作成します。

```
snapmirror create -source-path SVM_name: -destination-path SVM_name: -type  
DP|XDP -schedule schedule -policy policy -identity-preserve true
```



で、SVM名のあとにコロン (:) を入力する必要があります `-source-path` および `-destination-path` オプション (Options)

次の例は、デフォルトのを使用して、SnapMirror DR関係を作成します `MirrorAllSnapshots` ポリシー :

```
cluster_dst:> snapmirror create -source-path svm1: -destination-path  
svm_backup: -type XDP -schedule my_daily -policy MirrorAllSnapshots  
-identity-preserve true
```

次の例は、デフォルトを使用して、ユニファイドレプリケーション関係を作成します MirrorAndVault ポリシー：

```
cluster_dst:> snapmirror create -source-path svm1: -destination-path  
svm_backup: -type XDP -schedule my_daily -policy MirrorAndVault  
-identity-preserve true
```

ポリシータイプがのカスタムポリシーを作成しているとします `async-mirror` 次の例は、SnapMirror DR関係を作成します。

```
cluster_dst:> snapmirror create -source-path svm1: -destination-path  
svm_backup: -type XDP -schedule my_daily -policy my_mirrored -identity  
-preserve true
```

ポリシータイプがのカスタムポリシーを作成しているとします `mirror-vault` 次の例は、ユニファイドレプリケーション関係を作成します。

```
cluster_dst:> snapmirror create -source-path svm1: -destination-path  
svm_backup: -type XDP -schedule my_daily -policy my_unified -identity  
-preserve true
```

## 5. デスティネーション SVM を停止します。

```
vserver stop
```

*SVM name*

次の例は、dvs1 という名前のデスティネーション SVM を停止します。

```
cluster_dst:> vserver stop -vserver dvs1
```

## 6. デスティネーション SVM またはデスティネーションクラスタから、SVM レプリケーション関係を初期化します： +

```
snapmirror initialize -source-path SVM_name: -destination-path SVM_name:
```

次の例は、ソースSVM間の関係を初期化します。 svm1 `およびデスティネーションSVM `svm\_backup`：

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

**SVM** レプリケーション対象から **LIF** と関連ネットワークの設定を除外

ソースとデスティネーションのSVMが異なるサブネットにある場合は、を使用できます `-discard-configs network` のオプション `snapmirror policy create LIF`と関連ネットワーク設定をSVMレプリケーション対象から除外するコマンド。

必要なもの

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

詳細については、を参照してください ["クラスタピア関係を作成"](#) および ["SVM のクラスタ間ピア関係を作成します"](#)。

このタスクについて

。 `-identity-preserve` のオプション `snapmirror create` コマンドはに設定する必要があります `true` SVMレプリケーション関係の作成時。

コマンド構文全体については、マニュアルページを参照してください。

手順

1. デスティネーション SVM を作成します。

```
vserver create -vserver SVM -subtype dp-destination
```

SVM 名はソースクラスタとデスティネーションクラスタの間で一意である必要があります。

次の例は、という名前のデスティネーションSVMを作成します `svm_backup` :

```
cluster_dst:> vserver create -vserver svm_backup -subtype dp-destination
```

2. デスティネーションクラスタから、を使用してSVMピア関係を作成します `vserver peer create` コマンドを実行します

詳細については、を参照してください ["SVM のクラスタ間ピア関係を作成します"](#)。

3. ジョブスケジュールを作成します。

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

の場合 `-month`、`-dayofweek` および `-hour` を指定できます ``all`` 毎月、曜日、および時間ごとにジョブを実行します。



SVM SnapMirror関係にあるFlexVol ボリュームに対してサポートされる最小スケジュール (RPO) は15分です。SVM SnapMirror関係にあるFlexGroup ボリュームに対してサポートされる最小スケジュール (RPO) は30分です。

次の例は、という名前のジョブスケジュールを作成します `my_weekly` 土曜日の午前3時に実行されます。

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

#### 4. カスタムレプリケーションポリシーを作成します。

```
snapmirror policy create -vserver SVM -policy policy -type async-
mirror|vault|mirror-vault -comment comment -tries transfer_tries -transfer
-priority low|normal -is-network-compression-enabled true|false -discard
-configs network
```

コマンド構文全体については、マニュアルページを参照してください。

次の例は、LIF を除外する SnapMirror DR 用のカスタムレプリケーションポリシーを作成します。

```
cluster_dst::> snapmirror policy create -vserver svm1 -policy
DR_exclude_LIFs -type async-mirror -discard-configs network
```

次の例は、LIF を除外するユニファイドレプリケーション用のカスタムレプリケーションポリシーを作成します。

```
cluster_dst::> snapmirror policy create -vserver svm1 -policy
unified_exclude_LIFs -type mirror-vault -discard-configs network
```

#### 5. デスティネーション SVM またはデスティネーションクラスタから次のコマンドを実行して、レプリケーション関係を作成します。

```
snapmirror create -source-path SVM: -destination-path SVM: -type DP|XDP
-schedule schedule -policy policy -identity-preserve true|false
```



で、SVM名のあとにコロン（:）を入力する必要があります -source-path および -destination-path オプション（Options）以下の例を参照してください。

次の例は、LIF を除外する SnapMirror DR 関係を作成します。

```
cluster_dst::> snapmirror create -source-path svm1: -destination-path
svm_backup: -type XDP -schedule my_daily -policy DR_exclude_LIFs
-identity-preserve true
```

次の例は、LIF を除外する SnapMirror ユニファイドレプリケーション関係を作成します。

```
cluster_dst::> snapmirror create -source-path svm1: -destination-path  
svm_backup: -type XDP -schedule my_daily -policy unified_exclude_LIFs  
-identity-preserve true
```

## 6. デスティネーション SVM を停止します。

```
vserver stop
```

*SVM name*

次の例は、dvs1 という名前のデスティネーション SVM を停止します。

```
cluster_dst::> vserver stop -vserver dvs1
```

## 7. デスティネーション SVM またはデスティネーションクラスタから、レプリケーション関係を初期化します。

```
snapmirror initialize -source-path SVM: -destination-path SVM:
```

コマンド構文全体については、マニュアルページを参照してください。

次の例は、ソース間の関係を初期化します。svm1 目的地、svm\_backup:

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

完了後

災害発生時のデータアクセス用に、デスティネーション SVM でネットワークとプロトコルを設定する必要があります。

ネットワーク、ネームサービス、およびその他の設定を **SVM** レプリケーション対象から除外します

を使用できます `-identity-preserve false` のオプション `snapmirror create` SVM のボリュームとセキュリティ設定のみをレプリケートするコマンド。一部のプロトコルとネームサービスの設定も保持されます。

このタスクについて

保持されているプロトコルおよびネームサービスの設定のリストについては、を参照してください ["SVM DR 関係でレプリケートされる設定"](#)。

コマンド構文全体については、マニュアルページを参照してください。

作業を開始する前に

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



詳細については、を参照してください ["クラスタピア関係を作成"](#) および ["SVM のクラスタ間ピア関係を作成します"](#)。

#### 手順

1. デスティネーション SVM を作成します。

```
vserver create -vserver SVM -subtype dp-destination
```

SVM 名はソースクラスタとデスティネーションクラスタの間で一意である必要があります。

次の例は、という名前のデスティネーションSVMを作成します svm\_backup :

```
cluster_dst:> vserver create -vserver svm_backup -subtype dp-destination
```

2. デスティネーションクラスタから、を使用してSVMピア関係を作成します vserver peer create コマンドを実行します

詳細については、を参照してください ["SVM のクラスタ間ピア関係を作成します"](#)。

3. レプリケーションジョブスケジュールを作成

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

の場合 -month、-dayofweek`および`-hour`を指定できます `all` 毎月、曜日、および時間ごとにジョブを実行します。



SVM SnapMirror関係にあるFlexVol ボリュームに対してサポートされる最小スケジュール (RPO) は15分です。SVM SnapMirror関係にあるFlexGroup ボリュームに対してサポートされる最小スケジュール (RPO) は30分です。

次の例は、という名前のジョブスケジュールを作成します my\_weekly 土曜日の午前3時に実行されます。

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

4. ネットワーク、ネームサービス、およびその他の設定を除外するレプリケーション関係を作成します。

```
snapmirror create -source-path SVM: -destination-path SVM: -type DP|XDP  
-schedule schedule -policy policy -identity-preserve false
```



で、SVM名のあとにコロン (:) を入力する必要があります -source-path および -destination-path オプション (Options) 以下の例を参照してください。このコマンドはデスティネーション SVM またはデスティネーションクラスタから実行する必要があります。

次の例は、デフォルトのを使用して、SnapMirror DR関係を作成します MirrorAllSnapshots ポリシー

：この関係では、ネットワーク、ネームサービス、およびその他の設定が SVM レプリケーションから除外されます。

```
cluster_dst:> snapmirror create -source-path svm1: -destination-path  
svm_backup: -type XDP -schedule my_daily -policy MirrorAllSnapshots  
-identity-preserve false
```

次の例は、デフォルトを使用して、ユニファイドレプリケーション関係を作成します MirrorAndVault ポリシー：この関係では、ネットワーク、ネームサービス、およびその他の設定が除外されます。

```
cluster_dst:> snapmirror create svm1: -destination-path svm_backup:  
-type XDP -schedule my_daily -policy MirrorAndVault -identity-preserve  
false
```

ポリシータイプがのカスタムポリシーを作成しているとします `async-mirror` 次の例は、SnapMirror DR 関係を作成します。この関係では、ネットワーク、ネームサービス、およびその他の設定が SVM レプリケーションから除外されます。

```
cluster_dst:> snapmirror create -source-path svm1: -destination-path  
svm_backup: -type XDP -schedule my_daily -policy my_mirrored -identity  
-preserve false
```

ポリシータイプがのカスタムポリシーを作成しているとします `mirror-vault` 次の例は、ユニファイドレプリケーション関係を作成します。この関係では、ネットワーク、ネームサービス、およびその他の設定が SVM レプリケーションから除外されます。

```
cluster_dst:> snapmirror create -source-path svm1: -destination-path  
svm_backup: -type XDP -schedule my_daily -policy my_unified -identity  
-preserve false
```

## 5. デスティネーション SVM を停止します。

```
vserver stop
```

*SVM name*

次の例は、dvs1 という名前のデスティネーション SVM を停止します。

```
destination_cluster:> vserver stop -vserver dvs1
```

## 6. SMB を使用する場合は、SMB サーバも設定する必要があります。

を参照してください ["SMB のみ：SMB サーバの作成"](#)。

7. デスティネーション SVM またはデスティネーションクラスタから、SVM レプリケーション関係を初期化します。

```
snapmirror initialize -source-path SVM_name: -destination-path SVM_name:
```

完了後

災害発生時のデータアクセス用に、デスティネーション SVM でネットワークとプロトコルを設定する必要があります。

#### SVM DR 関係に使用するアグリゲートを指定する

ディザスタリカバリSVMを作成すると、を使用できます `aggr-list` オプションを指定します `vserver modify` SVM DRデスティネーションボリュームのホストに使用するアグリゲートを制限するコマンド。

ステップ

1. デスティネーション SVM を作成します。

```
vserver create -vserver SVM -subtype dp-destination
```

2. ディザスタリカバリ SVM の `aggr-list` を変更して、ディザスタリカバリ SVM のボリュームをホストする際に使用するアグリゲートを制限します。

```
cluster_dest::> vserver modify -vserver SVM -aggr-list <comma-separated-list>
```

#### SMBのみ：SMBサーバを作成する

ソースSVMでSMB構成が使用されていて、をに選択した場合 `identity-preserve` 終了：`false`では、デスティネーションSVM用のSMBサーバを作成する必要があります。SnapMirror 関係の初期化の際、共有などの一部の SMB 構成では SMB サーバが必要です。

手順

1. を使用して、デスティネーションSVMを起動します `vserver start` コマンドを実行します

```
destination_cluster::> vserver start -vserver dvs1
[Job 30] Job succeeded: DONE
```

2. デスティネーションSVMがにあることを確認します `running` 状態およびサブタイプはです `dp-destination` を使用します `vserver show` コマンドを実行します

```
destination_cluster::> vserver show
```

Vserver	Type	Subtype	Admin State	Operational State	Root Volume
Aggregate					
-----					
dvs1	data	dp-destination	running	running	-

3. を使用してLIFを作成します network interface create コマンドを実行します

```
destination_cluster::>network interface create -vserver dvs1 -lif NAS1  
-role data -data-protocol cifs -home-node destination_cluster-01 -home  
-port a0a-101 -address 192.0.2.128 -netmask 255.255.255.128
```

4. を使用してルートを作成します network route create コマンドを実行します

```
destination_cluster::>network route create -vserver dvs1 -destination  
0.0.0.0/0  
-gateway 192.0.2.1
```

### "Network Management の略"

5. を使用してDNSを設定します vserver services dns create コマンドを実行します

```
destination_cluster::>vserver services dns create -domains  
mydomain.example.com -vserver  
dvs1 -name-servers 192.0.2.128 -state enabled
```

6. を使用して、優先ドメインコントローラを追加します vserver cifs domain preferred-dc add コマンドを実行します

```
destination_cluster::>vserver cifs domain preferred-dc add -vserver dvs1  
-preferred-dc  
192.0.2.128 -domain mydomain.example.com
```

7. を使用してSMBサーバを作成します vserver cifs create コマンドを実行します

```
destination_cluster::>vserver cifs create -vserver dvs1 -domain  
mydomain.example.com  
-cifs-server CIFS1
```

8. を使用して、デスティネーションSVMを停止します `vserver stop` コマンドを実行します

```
destination_cluster::> vserver stop -vserver dvs1  
[Job 46] Job succeeded: DONE
```

## SVM レプリケーション対象からボリュームを除外

デフォルトでは、ソース SVM のすべての RW データボリュームがレプリケートされます。保護する必要がないボリュームがソースSVMにある場合は、を使用します `-vserver-dr-protection unprotected` のオプション `volume modify` SVMレプリケーション対象からボリュームを除外するコマンド。

### 手順

1. SVM レプリケーション対象からボリュームを除外します。

```
volume modify -vserver SVM -volume volume -vserver-dr-protection unprotected
```

コマンド構文全体については、マニュアルページを参照してください。

次の例は、ボリュームを除外します `volA_src` SVMレプリケーションから：

```
cluster_src::> volume modify -vserver SVM1 -volume volA_src -vserver-dr  
-protection unprotected
```

除外したボリュームをあとで SVM レプリケーション対象に含めるには、次のコマンドを実行します。

```
volume modify -vserver SVM -volume volume -vserver-dr-protection protected
```

ボリュームの例を次に示します `volA_src` SVMレプリケーションで、次の処理を行います。

```
cluster_src::> volume modify -vserver SVM1 -volume volA_src -vserver-dr  
-protection protected
```

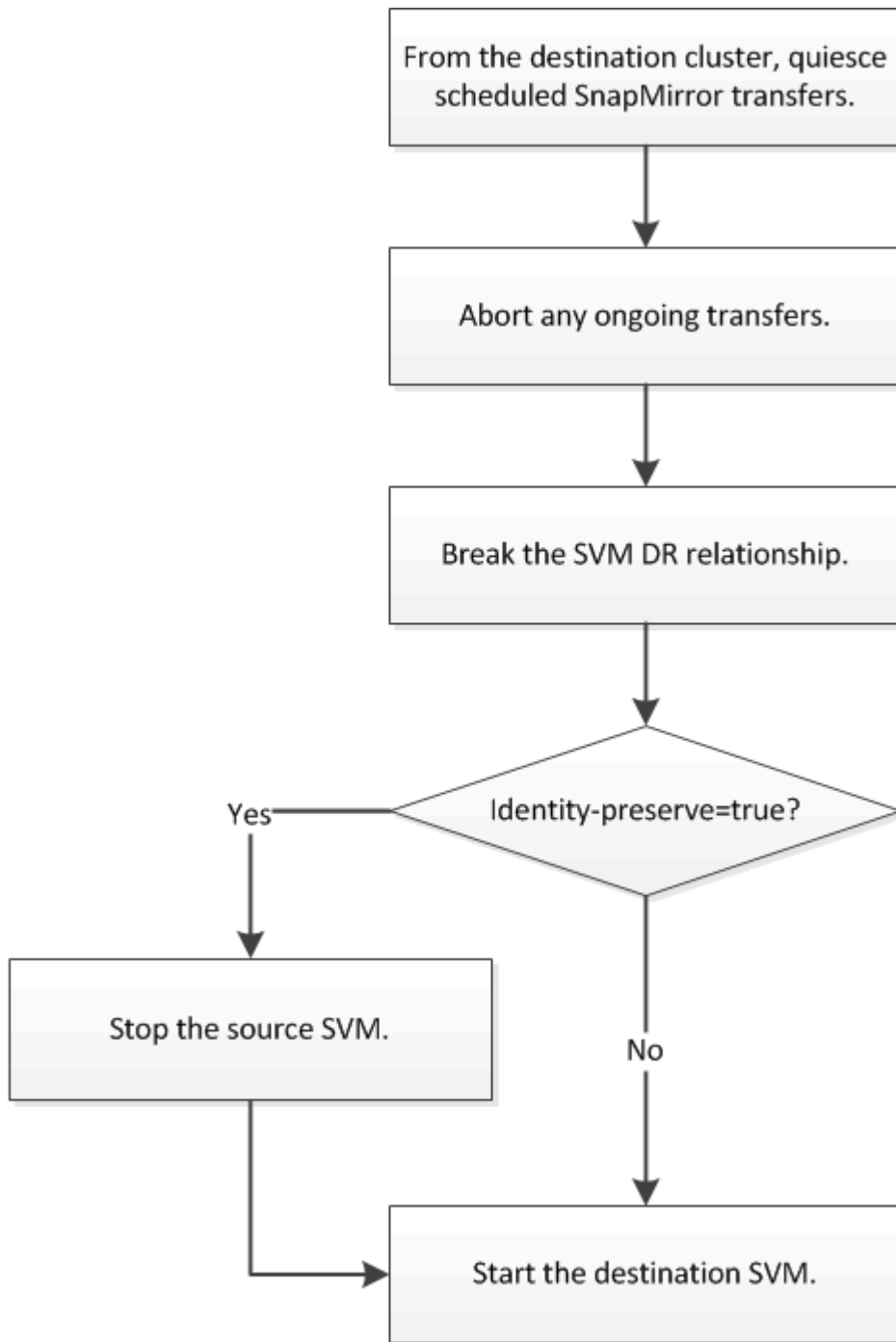
2. の説明に従って、SVM レプリケーション関係を作成して初期化します **"SVM の設定全体のレプリケート"**。

## SVM DR デスティネーションからのデータの提供

### SVM ディザスタリカバリのワークフロー

災害からリカバリしてデスティネーション SVM からデータを提供するには、デスティネーション SVM をアクティブ化する必要があります。デスティネーション SVM のアクティブ化では、スケジュールされた SnapMirror 転送の停止、実行中の SnapMirror 転送の中止、レプリケーション関係の解除、ソース SVM の停止、デスティネーション SVM

の起動が実行されます。



**SVM** デスティネーションボリュームを書き込み可能にします

クライアントにデータを提供する前に、SVM デスティネーションボリュームを書き込み可能にする必要があります。手順は、1つの例外を除いて、ボリュームレプリケーション用の手順とほとんど同じです。設定した場合 `-identity-preserve true` SVMレプリケーション関係を作成したら、デスティネーションSVMをアクティブ化する前にソースSVMを停止する必要があります。

このタスクについて

コマンド構文全体については、マニュアルページを参照してください。



ディザスタリカバリのシナリオでは、ソース SVM とそのデータにアクセスできなくなり、前回の再同期後の更新が無効または破損している可能性があるため、ソース SVM からディザスタリカバリのデスティネーション SVM への SnapMirror 更新を実行できません。

#### 手順

1. デスティネーション SVM またはデスティネーションクラスタから、デスティネーションへのスケジュールされた転送を停止します。

```
snapmirror quiesce -source-path SVM: -destination-path SVM:
```



で、SVM名のあとにコロン（:）を入力する必要があります -source-path および -destination-path オプション（Options）以下の例を参照してください。

次の例は、ソースSVM間のスケジュールされた転送を停止します svm1 およびデスティネーションSVM svm\_backup :

```
cluster_dst::> snapmirror quiesce -source-path svm1: -destination-path  
svm_backup:
```

2. デスティネーション SVM またはデスティネーションクラスタから、デスティネーションへの実行中の転送を停止します。

```
snapmirror abort -source-path SVM: -destination-path SVM:
```



で、SVM名のあとにコロン（:）を入力する必要があります -source-path および -destination-path オプション（Options）以下の例を参照してください。

次の例は、ソースSVM間の実行中の転送を停止します svm1 およびデスティネーションSVM svm\_backup :

```
cluster_dst::> snapmirror abort -source-path svm1: -destination-path  
svm_backup:
```

3. デスティネーション SVM またはデスティネーションクラスタから、レプリケーション関係を解除します。

```
snapmirror break -source-path SVM: -destination-path SVM:
```



で、SVM名のあとにコロン（:）を入力する必要があります -source-path および -destination-path オプション（Options）以下の例を参照してください。

次の例は、ソースSVM間の関係を解除します svm1 およびデスティネーションSVM svm\_backup :

```
cluster_dst:> snapmirror break -source-path svm1: -destination-path  
svm_backup:
```

4. 設定した場合 `-identity-preserve true` SVMレプリケーション関係を作成したら、ソースSVMを停止します。

```
vserver stop -vserver SVM
```

次の例は、ソースSVMを停止します `svm1` :

```
cluster_src:> vserver stop svm1
```

5. デスティネーション SVM を起動します。

```
vserver start -vserver SVM
```

次の例は、デスティネーションSVMを起動します `svm_backup` :

```
cluster_dst:> vserver start svm_backup
```

完了後

の説明に従って、データアクセス用の SVM デスティネーションボリュームを設定します "[データアクセス用のデスティネーションボリュームを設定](#)"。

## ソース **SVM** を再アクティブ化する

ソース **SVM** の再アクティブ化ワークフロー

災害発生後もソース SVM が残っている場合は、そのソース SVM を再アクティブ化し、SVM ディザスタリカバリ関係を再作成して保護できます。





元のソース **SVM** を再アクティブ化する

デスティネーションからデータを提供する必要がなくなった場合は、ソース SVM とデスティネーション SVM 間で元のデータ保護関係を再確立できます。手順は、1 つの例外を除いて、ボリュームレプリケーション用の手順とほとんど同じです。ソース SVM を再アクティブ化するには、デスティネーション SVM を停止する必要があります。

作業を開始する前に

デスティネーションボリュームからデータを提供している間にそのサイズを拡張した場合は、ソースボリュームを再アクティブ化する前に、元のソースボリュームを十分拡張できるように max-autosize を手動で増やす必要があります。

"デスティネーションボリュームが自動的に拡張される状況"

このタスクについて

ONTAP 9.11.1以降では、を使用して、ディザスタリカバリのリハーサル中の再同期時間を短縮できます -quick-resync true のオプション snapmirror resync SVM DR関係の逆再同期を実行する際のコマンド。迅速な再同期により、Data Warehouseの再構築およびリストア処理をバイパスすることで、本番環境に戻るまでの時間を短縮できます。



クイック再同期では、デスティネーションボリュームのストレージ効率は維持されません。クイック再同期を有効にすると、デスティネーションボリュームで使用されるボリュームスペースが増加する可能性があります。

この手順は、元のソースボリュームにあるベースラインが損なわれていないことを前提としています。ベースラインが損なわれている場合は、手順を実行する前に、データの提供元のボリュームと元のソースボリュームの関係を作成して初期化する必要があります。

コマンドの完全なコマンド構文については、マニュアルページを参照してください。

#### 手順

1. 元のソース SVM または元のソースクラスタから、元の SVM DR 関係と同じ設定、ポリシー、および ID 保持設定を使用して、リバース SVM DR 関係を作成します。

```
snapmirror create -source-path SVM: -destination-path SVM:
```



で、SVM名のあとにコロン（:）を入力する必要があります -source-path および -destination-path オプション（Options）以下の例を参照してください。

次の例は、データの提供元であるSVM間の関係を作成します。 svm\_backup` および元のソースSVM `svm1` :

```
cluster_src::> snapmirror create -source-path svm_backup: -destination  
-path svm1:
```

2. 元のソース SVM または元のソースクラスタから次のコマンドを実行して、データ保護関係を反転します。

```
snapmirror resync -source-path SVM: -destination-path SVM:
```



で、SVM名のあとにコロン（:）を入力する必要があります -source-path および -destination-path オプション（Options）以下の例を参照してください。

再同期の際にベースライン転送は不要ですが、再同期には時間がかかる場合があります。再同期はオフピークの時間帯に実行することを推奨します。



ソースとデスティネーションに共通の Snapshot コピーが存在しない場合、このコマンドは失敗します。使用 snapmirror initialize をクリックして関係を再初期化してください。

次の例は、元のソースSVM間の関係を反転します。 svm1` およびデータの提供元のSVM `svm\_backup` :

```
cluster_src::> snapmirror resync -source-path svm_backup: -destination  
-path svm1:
```

quick-resyncオプションの使用例：

```
cluster_src::> snapmirror resync -source-path svm_backup: -destination  
-path svm1: -quick-resync true
```

3. 元のソース SVM へのデータアクセスを再確立する準備ができれば、元のデスティネーション SVM を停止して、元のデスティネーション SVM に現在接続されているクライアントをすべて切断します。

```
vserver stop -vserver SVM
```

次の例は、現在データを提供している元のデスティネーション SVM を停止します。

```
cluster_dst::> vserver stop svm_backup
```

4. を使用して、元のデスティネーションSVMの状態がstoppedであることを確認します vserver show コマンドを実行します

```
cluster_dst::> vserver show
```

Vserver	Type	Subtype	Admin State	Operational State	Root Volume
Aggregate					
-----	-----	-----	-----	-----	-----
svm_backup	data	default	stopped	stopped	rv
aggr1					

5. 元のソース SVM または元のソースクラスタから次のコマンドを実行して、反転した関係の最終更新を実行し、元のデスティネーション SVM から元のソース SVM にすべての変更を転送します。

```
snapmirror update -source-path SVM: -destination-path SVM:
```



で、SVM名のあとにコロン（:）を入力する必要があります -source-path および -destination-path オプション（Options）以下の例を参照してください。

次の例は、データの提供元である元のデスティネーションSVMの間の関係を更新します,svm\_backup`および元のソースSVM `svm1`:

```
cluster_src::> snapmirror update -source-path svm_backup: -destination-path svm1:
```

6. 元のソース SVM または元のソースクラスタから次のコマンドを実行して、反転した関係のスケジュールされた転送を停止します。

```
snapmirror quiesce -source-path SVM: -destination-path SVM:
```



で、SVM名のあとにコロン（:）を入力する必要があります -source-path および -destination-path オプション（Options）以下の例を参照してください。

次の例は、データの提供元のSVM間のスケジュールされた転送を停止します。 svm\_backup`および元のSVM `svm1`:

```
cluster_src::> snapmirror quiesce -source-path svm_backup: -destination  
-path svm1:
```

7. 最後の更新が完了し、関係のステータスが「Quiesced」と表示されたら、元のソース SVM または元のソースクラスタから次のコマンドを実行して、反転した関係を解除します。

```
snapmirror break -source-path SVM: -destination-path SVM:
```



で、SVM名のあとにコロンの(:)を入力する必要があります -source-path および -destination-path オプション (Options) 以下の例を参照してください。

次の例は、データの提供元であった元のデスティネーションSVM間の関係を解除します。svm\_backup` および元のソースSVM `svm1:

```
cluster_src::> snapmirror break -source-path svm_backup: -destination  
-path svm1:
```

8. 元のソース SVM が以前に停止されていた場合は、元のソースクラスタから元のソース SVM を起動します。

```
vserver start -vserver SVM
```

次の例は、元のソース SVM を起動します。

```
cluster_src::> vserver start svm1
```

9. 元のデスティネーション SVM または元のデスティネーションクラスタから、元のデータ保護関係を再確立します。

```
snapmirror resync -source-path SVM: -destination-path SVM:
```



で、SVM名のあとにコロンの(:)を入力する必要があります -source-path および -destination-path オプション (Options) 以下の例を参照してください。

次の例は、元のソースSVM間の関係を再確立します。svm1`および元のデスティネーションSVM `svm\_backup:

```
cluster_dst::> snapmirror resync -source-path svm1: -destination-path  
svm_backup:
```

10. 元のソース SVM または元のソースクラスタから次のコマンドを実行して、反転したデータ保護関係を削除します。

```
snapmirror delete -source-path SVM: -destination-path SVM:
```



で、SVM名のあとにコロン（:）を入力する必要があります -source-path および -destination-path オプション（Options）以下の例を参照してください。

次の例は、元のデスティネーションSVM間の反転した関係を削除します。 svm\_backup`および元のソースSVM `svm1`:

```
cluster_src::> snapmirror delete -source-path svm_backup: -destination
-path svm1:
```

11. 元のデスティネーション SVM または元のデスティネーションクラスタから、反転したデータ保護関係を解放します。

```
snapmirror release -source-path SVM: -destination-path SVM:
```



で、SVM名のあとにコロン（:）を入力する必要があります -source-path および -destination-path オプション（Options）以下の例を参照してください。

次の例は、元のデスティネーションSVM svm\_backupと元のソースSVMの間の反転した関係をリリースします。 svm1

```
cluster_dst::> snapmirror release -source-path svm_backup: -destination
-path svm1:
```

完了後

を使用します snapmirror show コマンドを実行して、SnapMirror関係が作成されたことを確認します。コマンド構文全体については、マニュアルページを参照してください。

元のソース **SVM** を再アクティブ化する（**FlexGroup** ボリュームのみ）

デスティネーションからデータを提供する必要がなくなった場合は、ソース SVM とデスティネーション SVM 間で元のデータ保護関係を再確立できます。FlexGroup ボリュームを使用しているときに元のソース SVM を再アクティブ化するには、元の SVM DR 関係を削除して元の関係を解放してから、関係を反転するなど、いくつかの追加手順を実行する必要があります。また、スケジュールされた転送を停止する前に、反転した関係を解放し、元の関係を再作成する必要があります。

手順

1. 元のデスティネーション SVM または元のデスティネーションクラスタから、元の SVM DR 関係を削除します。

```
snapmirror delete -source-path SVM: -destination-path SVM:
```



で、SVM名のあとにコロン（:）を入力する必要があります -source-path および -destination-path オプション（Options）以下の例を参照してください。

次の例は、元のソースSVM svm1と元のデスティネーションSVMの間の元の関係を削除します。

svm\_backup :

```
cluster_dst::> snapmirror delete -source-path svm1: -destination-path  
svm_backup:
```

2. 元のソース SVM または元のソースクラスタから、Snapshot コピーはそのまま保持したまま元の関係を解放します。

```
snapmirror release -source-path SVM: -destination-path SVM: -relationship-info  
-only true
```



で、SVM名のあとにコロン（:）を入力する必要があります -source-path および -destination-path オプション（Options）以下の例を参照してください。

次の例は、元のソースSVM svm1と元のデスティネーションSVMの間の元の関係をリリースします。

svm\_backup。

```
cluster_src::> snapmirror release -source-path svm1: -destination-path  
svm_backup: -relationship-info-only true
```

3. 元のソース SVM または元のソースクラスタから、元の SVM DR 関係と同じ設定、ポリシー、および ID 保持設定を使用して、リバース SVM DR 関係を作成します。

```
snapmirror create -source-path SVM: -destination-path SVM:
```



で、SVM名のあとにコロン（:）を入力する必要があります -source-path および -destination-path オプション（Options）以下の例を参照してください。

次の例は、データの提供元であるSVM間の関係を作成します。 svm\_backup` および元のソースSVM `svm1 :

```
cluster_src::> snapmirror create -source-path svm_backup: -destination  
-path svm1:
```

4. 元のソース SVM または元のソースクラスタから次のコマンドを実行して、データ保護関係を反転します。

```
snapmirror resync -source-path SVM: -destination-path SVM:
```



で、SVM名のあとにコロン（:）を入力する必要があります -source-path および -destination-path オプション（Options）以下の例を参照してください。

再同期の際にベースライン転送は不要ですが、再同期には時間がかかる場合があります。再同期はオフピークの時間帯に実行することを推奨します。



ソースとデスティネーションに共通の Snapshot コピーが存在しない場合、このコマンドは失敗します。使用 `snapmirror initialize` をクリックして関係を再初期化してください。

次の例は、元のソースSVM間の関係を反転します。 `svm1`` およびデータの提供元のSVM ``svm_backup`` :

```
cluster_src::> snapmirror resync -source-path svm_backup: -destination
-path svm1:
```

5. 元のソース SVM へのデータアクセスを再確立する準備ができたなら、元のデスティネーション SVM を停止して、元のデスティネーション SVM に現在接続されているクライアントをすべて切断します。

```
vserver stop -vserver SVM
```

次の例は、現在データを提供している元のデスティネーション SVM を停止します。

```
cluster_dst::> vserver stop svm_backup
```

6. を使用して、元のデスティネーションSVMの状態がstoppedであることを確認します `vserver show` コマンドを実行します

```
cluster_dst::> vserver show
```

Vserver	Type	Subtype	Admin State	Operational State	Root Volume
Aggregate					
-----	-----	-----	-----	-----	-----
svm_backup	data	default	stopped	stopped	rv
aggr1					

7. 元のソース SVM または元のソースクラスタから次のコマンドを実行して、反転した関係の最終更新を実行し、元のデスティネーション SVM から元のソース SVM にすべての変更を転送します。

```
snapmirror update -source-path SVM: -destination-path SVM:
```



で、SVM名のあとにコロン（:）を入力する必要があります `-source-path` および `-destination-path` オプション（Options）以下の例を参照してください。

次の例は、データの提供元である元のデスティネーションSVMの間の関係を更新します, `svm_backup`` および元のソースSVM ``svm1`` :

```
cluster_src::> snapmirror update -source-path svm_backup: -destination
-path svm1:
```

8. 元のソース SVM または元のソースクラスタから次のコマンドを実行して、反転した関係のスケジュールされた転送を停止します。

```
snapmirror quiesce -source-path SVM: -destination-path SVM:
```



で、SVM名のあとにコロン（:）を入力する必要があります -source-path および -destination-path オプション（Options）以下の例を参照してください。

次の例は、データの提供元のSVM間のスケジュールされた転送を停止します。svm\_backup`および元のSVM `svm1`:

```
cluster_src::> snapmirror quiesce -source-path svm_backup: -destination  
-path svm1:
```

9. 最後の更新が完了し、関係のステータスが「Quiesced」と表示されたら、元のソース SVM または元のソースクラスタから次のコマンドを実行して、反転した関係を解除します。

```
snapmirror break -source-path SVM: -destination-path SVM:
```



で、SVM名のあとにコロン（:）を入力する必要があります -source-path および -destination-path オプション（Options）以下の例を参照してください。

次の例は、データの提供元であった元のデスティネーションSVM間の関係を解除します。svm\_backup`および元のソースSVM `svm1`:

```
cluster_src::> snapmirror break -source-path svm_backup: -destination  
-path svm1:
```

10. 元のソース SVM が以前に停止されていた場合は、元のソースクラスタから元のソース SVM を起動します。

```
vserver start -vserver SVM
```

次の例は、元のソース SVM を起動します。

```
cluster_src::> vserver start svm1
```

11. 元のソース SVM または元のソースクラスタから、反転した SVM DR 関係を削除します。

```
snapmirror delete -source-path SVM: -destination-path SVM:
```



で、SVM名のあとにコロン（:）を入力する必要があります -source-path および -destination-path オプション（Options）以下の例を参照してください。

次の例は、元のデスティネーションSVM svm\_backupと元のソースSVMの間の反転した関係を削除しま



す。 svm1 :

```
cluster_src::> snapmirror delete -source-path svm_backup: -destination  
-path svm1:
```

12. 元のデスティネーション SVM または元のデスティネーションクラスタから、反転した関係を解放し、Snapshot コピーはそのままにします。

```
snapmirror release -source-path SVM: -destination-path SVM: -relationship-info  
-only true
```



で、SVM名のあとにコロン（:）を入力する必要があります -source-path および -destination-path オプション（Options）以下の例を参照してください。

次の例は、元のデスティネーション SVM svm\_backup と元のソース SVM svm1 の間の反転した関係を解放します。

```
cluster_dst::> snapmirror release -source-path svm_backup: -destination  
-path svm1: -relationship-info-only true
```

13. 元のデスティネーション SVM または元のデスティネーションクラスタから、元の関係を再作成します。元の SVM DR 関係と同じ設定、ポリシー、および identity-preserve 設定を使用します。

```
snapmirror create -source-path SVM: -destination-path SVM:
```



で、SVM名のあとにコロン（:）を入力する必要があります -source-path および -destination-path オプション（Options）以下の例を参照してください。

次の例は、元のソースSVM間の関係を作成します。 svm1` および元のデスティネーションSVM `svm\_backup :

```
cluster_dst::> snapmirror create -source-path svm1: -destination-path  
svm_backup:
```

14. 元のデスティネーション SVM または元のデスティネーションクラスタから、元のデータ保護関係を再確立します。

```
snapmirror resync -source-path SVM: -destination-path SVM:
```



で、SVM名のあとにコロン（:）を入力する必要があります -source-path および -destination-path オプション（Options）以下の例を参照してください。

次の例は、元のソースSVM間の関係を再確立します。 svm1` および元のデスティネーションSVM `svm\_backup :

```
cluster_dst:> snapmirror resync -source-path svm1: -destination-path  
svm_backup:
```

ボリュームのレプリケーション関係を **SVM** のレプリケーション関係に変換します

ソース上の各ボリューム（ルートボリュームを除く）がレプリケートされている場合は、ボリューム間のレプリケーション関係を、そのボリュームを所有する Storage Virtual Machine（SVM）間のレプリケーション関係に変換できます。また、ソースの各ボリューム（ルートボリュームを含む）の名前は、デスティネーションのボリュームと同じになります。

このタスクについて

を使用します `volume rename` SnapMirror関係がアイドル状態のときにコマンドを実行し、必要に応じてデスティネーションボリュームの名前を変更します。

手順

1. デスティネーション SVM またはデスティネーションクラスタから次のコマンドを実行して、ソースとデスティネーションのボリュームを再同期します。

```
snapmirror resync -source-path SVM:volume -destination-path SVM:volume -type  
DP|XDP -policy policy
```

コマンド構文全体については、マニュアルページを参照してください。



再同期の際にベースライン転送は不要ですが、再同期には時間がかかる場合があります。再同期はオフピークの時間帯に実行することを推奨します。

次の例は、ソースボリューム間の関係を再同期します `volA` オン `svm1` デスティネーションボリュームを指定します `volA` オン `svm_backup` :

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

2. の説明に従って、ソースとデスティネーションの SVM 間に SVM レプリケーション関係を作成します "[SVM 設定のレプリケート](#)"。

を使用する必要があります `-identity-preserve true` のオプション `snapmirror create` コマンドを使用してレプリケーション関係を作成します。

3. デスティネーション SVM を停止します。

```
vserver stop -vserver SVM
```

コマンド構文全体については、マニュアルページを参照してください。

次の例は、デスティネーションSVMを停止します `svm_backup` :

```
cluster_dst:> vserver stop svm_backup
```

4. デスティネーション SVM またはデスティネーションクラスタから次のコマンドを実行して、ソースとデスティネーションの SVM を再同期します。

```
snapmirror resync -source-path SVM: -destination-path SVM: -type DP|XDP  
-policy policy
```

コマンド構文全体については、マニュアルページを参照してください。



で、SVM名のあとにコロン（:）を入力する必要があります -source-path および -destination-path オプション（Options）以下の例を参照してください。

再同期の際にベースライン転送は不要ですが、再同期には時間がかかる場合があります。再同期はオフピークの時間帯に実行することを推奨します。

次の例は、ソースSVM間の関係を再同期します svm1 およびデスティネーションSVM svm\_backup :

```
cluster_dst:> snapmirror resync -source-path svm1: -destination-path  
svm_backup:
```

## SVM レプリケーション関係を削除します

を使用できます snapmirror delete および snapmirror release SVMレプリケーション関係を削除するコマンド。続いて、不要なデスティネーションボリュームを手動で削除できます。

このタスクについて

。 snapmirror release コマンドは、SnapMirrorで作成されたSnapshotコピーをソースから削除します。を使用できます -relationship-info-only Snapshotコピーを保持するオプション。

コマンドの完全なコマンド構文については、マニュアルページを参照してください。

手順

1. デスティネーション SVM またはデスティネーションクラスタから次のコマンドを実行して、レプリケーション関係を解除します。

```
snapmirror break -source-path SVM: -destination-path SVM:
```



で、SVM名のあとにコロン（:）を入力する必要があります -source-path および -destination-path オプション（Options）以下の例を参照してください。

次の例は、ソースSVM間の関係を解除します svm1 およびデスティネーションSVM svm\_backup :

```
cluster_dst:> snapmirror break -source-path svm1: -destination-path  
svm_backup:
```

2. デスティネーション SVM またはデスティネーションクラスタから次のコマンドを実行して、レプリケーション関係を削除します。

```
snapmirror delete -source-path SVM: -destination-path SVM:
```



で、SVM名のあとにコロン（:）を入力する必要があります -source-path および -destination-path オプション（Options）以下の例を参照してください。

次の例は、ソースSVM間の関係を削除します svm1 およびデスティネーションSVM svm\_backup :

```
cluster_dst:> snapmirror delete -source-path svm1: -destination-path  
svm_backup:
```

3. ソースクラスタまたはソース SVM から次のコマンドを実行して、ソース SVM からレプリケーション関係情報をリリースします。

```
snapmirror release -source-path SVM: -destination-path SVM:
```



で、SVM名のあとにコロン（:）を入力する必要があります -source-path および -destination-path オプション（Options）以下の例を参照してください。

次の例は、指定したレプリケーション関係の情報をソースSVMからリリースします svm1 :

```
cluster_src:> snapmirror release -source-path svm1: -destination-path  
svm_backup:
```

## SnapMirror ルートボリュームのレプリケーションを管理します

### SnapMirror ルートボリュームのレプリケーションの概要を管理します

NAS 環境内のすべての SVM には一意のネームスペースがあります。オペレーティングシステムと関連情報を含む svm\_root ボリュームは、ネームスペース階層へのエントリポイントです。ノードに障害やフェイルオーバーが発生したときに引き続きクライアントからデータにアクセスできるようにするには、SVM ルートボリュームの負荷共有ミラーコピーを作成する必要があります。

SVM ルートボリュームの負荷共有ミラーの主な目的は負荷共有ではなく、ディザスタリカバリにあります。

- ルートボリュームが一時的に使用できなくなった場合は、負荷共有ミラーによって、ルートボリュームのデータへの読み取り専用アクセスが自動的に提供されます。

- ルートボリュームが完全に使用できなくなった場合は、いずれかの負荷共有ボリュームを昇格させて、ルートボリュームのデータへの書き込みアクセスを提供できます。

## 負荷共有ミラー関係を作成して初期化

クラスタ内の NAS データを提供する各 SVM ルートボリュームについて、負荷共有ミラー（LSM）を作成する必要があります。複数の HA ペアで構成されるクラスタでは、次の場合にも引き続きネームスペースにアクセスできるように、SVM ルートボリュームの負荷共有ミラーを検討する必要があります。

HA ペアの両方のノードで障害が発生した場合。負荷共有ミラーは、単一の HA ペアで構成されるクラスタには適していません。

### このタスクについて

同じノードで LSM を作成した場合は、ノードが使用できなくなると単一点障害が発生します。クライアントから引き続きデータにアクセスできるようにするためのコピーをもう 1 つ作成する必要はありません。ただし、ルートボリュームを含むノード以外のノードや別の HA ペアに LSM を作成しても、停止してもデータにアクセスできます。

たとえば、4 ノードクラスタの 3 つのノードにルートボリュームがある場合、次のようになります。

- HA 1 のノード 1 のルートボリュームについて、HA 2 のノード 1 または HA 2 のノード 2 に LSM を作成します。
- HA 1 のノード 2 のルートボリュームについて、HA 2 のノード 1 または HA 2 のノード 2 に LSM を作成します。
- HA 2 のノード 1 のルートボリュームについて、HA 1 のノード 1 または HA 1 のノード 2 に LSM を作成します。

### 手順

1. LSM のデスティネーションボリュームを作成します。

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

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

デスティネーションボリュームのサイズは、ルートボリュームと同じかそれ以上である必要があります。

ルートボリュームとデスティネーションボリュームの名前にサフィックス（など）を付けることを推奨します `_root` および `_ml`。

コマンド構文全体については、マニュアルページを参照してください。

次の例は、ルートボリューム用の負荷共有ミラーボリュームを作成します `svm1_root` インチ `cluster_src`：

```
cluster_src:> volume create -vserver svm1 -volume svm1_m1 -aggregate  
aggr_1 -size 1gb -state online -type DP
```

## 2. "レプリケーションジョブスケジュールの作成"。

3. SVM ルートボリュームと LSM のデスティネーションボリュームの間に負荷共有ミラー関係を作成します。

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

```
snapmirror create -source-path <SVM:volume> -destination-path  
<SVM:volume> -type LS -schedule <schedule>
```

コマンド構文全体については、マニュアルページを参照してください。

次の例は、ルートボリューム間に負荷共有ミラー関係を作成します svm1\_root および負荷共有ミラーボリューム svm1\_m1：

```
cluster_src::> snapmirror create -source-path svm1:svm1_root  
-destination-path svm1:svm1_m1 -type LS -schedule hourly
```

負荷共有ミラーのtype属性がから変更されます DP 終了：LS。

4. 負荷共有ミラーを初期化します。

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

```
snapmirror initialize-ls-set -source-path <SVM:volume>
```

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

コマンド構文全体については、マニュアルページを参照してください。

次の例は、ルートボリュームの負荷共有ミラーを初期化します svm1\_root：

```
cluster_src::> snapmirror initialize-ls-set -source-path svm1:svm1_root
```

## 負荷共有ミラー関係を更新

負荷共有ミラー（LSM）関係は、SVM内のボリュームのマウントまたはアンマウント後、およびの実行中にSVMルートボリュームの自動更新されます volume create junction-pathオプションを含む処理。LSM 関係を更新する必要がある場合は、スケジュー

ールされた次回の更新前に LSM 関係を更新できます。

負荷共有ミラー関係は、次の場合に自動的に更新されます。

- 今こそ、スケジュールされた更新を実行するときです
- マウントまたはアンマウント処理は、SVM ルートボリューム内のボリュームに対して実行されます
- A volume create を含むコマンドが実行されます junction-path オプション

#### ステップ

1. 負荷共有ミラー関係を手動で更新します。

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

```
snapmirror update-ls-set -source-path <SVM:volume>
```

次の例は、ルートボリュームの負荷共有ミラー関係を更新します svm1\_root :

```
cluster_src::> snapmirror update-ls-set -source-path svm1:svm1_root
```

## 負荷共有ミラーを昇格

ルートボリュームが完全に使用できなくなった場合は、負荷共有ミラー（LSM）ボリュームを昇格して、ルートボリュームのデータへの書き込みアクセスを提供できます。

#### 必要なもの

このタスクを実行するには、advanced 権限レベルのコマンドを使用する必要があります。

#### 手順

1. advanced 権限レベルに切り替えます。

```
set -privilege advanced
```

2. LSM ボリュームを昇格します。

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

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

コマンド構文全体については、マニュアルページを参照してください。

次の例は、ボリュームを昇格します svm1\_m2 新しいSVMルートボリュームとして、次の手順を実行します。

```
cluster_src::*> snapmirror promote -destination-path svm1:svm1_m2

Warning: Promote will delete the offline read-write volume
cluster_src://svm1/svm1_root and replace it with
cluster_src://svm1/svm1_m2. Because the volume is offline,
it is not possible to determine whether this promote will
affect other relationships associated with this source.
Do you want to continue? {y|n}: y
```

入力するコマンド `y`。ONTAP によって LSM ボリュームが読み取り / 書き込み可能になり、アクセス可能な場合は元のルートボリュームが削除されます。



最後の更新が最近行われていない場合は、昇格されたルートボリュームに元のルートボリュームのデータがすべて含まれているとは限りません。

3. admin 権限レベルに戻ります。

```
set -privilege admin
```

4. ルートボリュームに使用した命名規則に従って、昇格されたボリュームの名前を変更します。

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

```
volume rename -vserver <SVM> -volume <volume> -newname <new_name>
```

次の例は、昇格されたボリュームの名前を変更します `svm1_m2` 名前は `svm1_root` :

```
cluster_src::> volume rename -vserver svm11 -volume svm1_m2 -newname
svm1_root
```

5. の手順3~4の説明に従って、名前を変更したルートボリュームを保護します ["負荷共有ミラー関係を作成して初期化しています"](#)。

## SnapMirror の技術的な詳細

パス名のパターンマッチングを使用します

パターンマッチングを使用すると、でソースパスとデスティネーションパスを指定できます `snapmirror` コマンド



`snapmirror` コマンドでは、次の形式の完全修飾パス名を使用します。  
`vserver:volume`。SVM  
名を入力せずにパス名を省略できます。この操作を実行すると、が表示されます `snapmirror`  
コマンドは、ユーザのローカルSVMコンテキストを前提としています。

SVMの名前が「vserver1」、ボリュームの名前が「vol1」とすると、完全修飾パス名はになります  
vserver1:vol1。

パス名にアスタリスク（\*）をワイルドカードとして使用すると、一致する完全修飾パス名を選択できます。  
次の表に、ワイルドカードを使用して特定範囲のボリュームを選択する例を示します。

*	すべてのパスに一致します。
vs*	SVM名の先頭がであるすべてのSVMおよびボリュームが一致します vs。
:*src	ボリューム名にを含むすべてのSVMが一致します src テキスト。
:vol	ボリューム名の先頭がであるすべてのSVMが一致し ます vol。

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

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

拡張クエリを使用して、多数の **SnapMirror** 関係进行操作できます

拡張クエリを使用すると、複数の SnapMirror 関係に対して SnapMirror 処理を一度に実行できます。たとえば、初期化されていない SnapMirror 関係が複数ある場合に、それらの関係を 1 つのコマンドで初期化できます。

このタスクについて

拡張クエリは、次の SnapMirror 処理に適用できます。

- 初期化されていません
- 休止されていた関係を再開
- 解除した関係を再同期して
- アイドル状態の関係を更新中です
- 関係のデータ転送を中止しています

#### ステップ

1. 多数の関係に対して SnapMirror 処理を実行します。

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

次のコマンドは、内の SnapMirror 関係を初期化します Uninitialized 都道府県：

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

## ミラー - ヴォールト構成で共通の **Snapshot** コピーを作成する

使用できます `snapmirror snapshot-owner create` ミラー-ヴォールト構成のセカンダリにラベル付きの Snapshot コピーを保持するコマンド。これにより、バックアップ関係の更新用の共通の Snapshot コピーが確保されます。

このタスクについて

ミラー - ヴォールトファンアウト構成またはカスケード構成を組み合わせる場合は、ソースボリュームとデスティネーションボリュームに共通の Snapshot コピーが存在しなければ更新が失敗するという点を考慮する必要があります。

SnapMirror は、更新を実行する前に必ずソースボリュームの Snapshot コピーを作成するため、ミラー - ヴォールトファンアウト構成またはカスケード構成ではミラー関係の問題を使用することはありません。

ただし、バックアップ関係の更新時にソースボリュームの Snapshot コピーが SnapMirror によって作成されないため、SnapMirror はバックアップ関係の問題になる場合があります。を使用する必要があります

`snapmirror snapshot-owner create` バックアップ関係のソースとデスティネーションの両方に共通の Snapshot コピーを少なくとも1つ確保する必要があります。

#### 手順

1. ソースボリュームで、保持するラベル付きの Snapshot コピーに所有者を割り当てます。

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

次の例は、を割り当てます ApplicationA の所有者として snap1 Snapshot コピー：

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

2. の説明に従って、ミラー関係を更新します **"レプリケーション関係を手動で更新する"**。

または、ミラー関係のスケジュールされた更新が行われるまで待つこともできます。

3. ラベル付きの Snapshot コピーをヴォールトデスティネーションに転送します。

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

コマンド構文全体については、マニュアルページを参照してください。

次の例は、を転送します **snap1 Snapshot コピー**

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

ヴォールト関係の更新時にラベル付きの Snapshot コピーが保持されます。

4. ソースボリュームで、ラベル付きの Snapshot コピーから所有者を削除します。

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

次の例は、を削除します ApplicationA の所有者として snap1 Snapshot コピー：

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

## SnapMirror 関係に対応した ONTAP バージョン

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

### ユニファイドレプリケーション関係

「xdmp」タイプの SnapMirror 関係では、オンプレミスまたは Cloud Volumes ONTAP リリースを使用します。

# ONTAP 9.9.9..0以降：



- ONTAP 9.x.0リリースはクラウドのみのリリースであり、Cloud Volumes ONTAPシステムをサポートします。リリースバージョンのあとにアスタリスク（\*）が表示されている場合、クラウドのみのリリースです。
- ONTAP 9.x.1リリースは一般リリースであり、オンプレミスシステムとCloud Volumes ONTAPシステムの両方をサポートします。



双方向の互換性があります。

- ONTAP バージョン9.3以降との相互運用性\*

ONTAP バージョン...	ONTAP の以前のバージョンとの相互運用性...																	
	9.14 .1	9.14 .0 *	9.13 .1	9.13 .0 *	9.12 .1:	9.12 .0 *	9.11 .1	9.11 .0*	9.10 .1	9.10 .0 *	9.9. 1	9.9.. 0 *	9.8	9.7	9.6	9.5	9.4	9.3
9.14 .1	*はい*	*はい*	*はい*	*はい*	*はい*	*はい*	*はい*	*はい*	*はい*	*はい*	*はい*	*はい*	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ
9.14 .0 *	*はい*	*はい*	*はい*	いいえ	*はい*	いいえ	*はい*	いいえ	*はい*	いいえ	*はい*	いいえ	*はい*	いいえ	いいえ	いいえ	いいえ	いいえ
9.13 .1	*はい*	*はい*	*はい*	*はい*	*はい*	*はい*	*はい*	*はい*	*はい*	*はい*	*はい*	*はい*	*はい*	いいえ	いいえ	いいえ	いいえ	いいえ
9.13 .0 *	*はい*	いいえ	*はい*	*はい*	*はい*	いいえ	*はい*	いいえ	*はい*	いいえ	*はい*	いいえ	*はい*	いいえ	いいえ	いいえ	いいえ	いいえ
9.12 .1:	*はい*	*はい*	*はい*	*はい*	*はい*	*はい*	*はい*	*はい*	*はい*	*はい*	*はい*	*はい*	*はい*	*はい*	いいえ	いいえ	いいえ	いいえ
9.12 .0 *	*はい*	いいえ	*はい*	いいえ	*はい*	*はい*	*はい*	いいえ	*はい*	いいえ	*はい*	いいえ	*はい*	*はい*	いいえ	いいえ	いいえ	いいえ
9.11 .1	*はい*	*はい*	*はい*	*はい*	*はい*	*はい*	*はい*	*はい*	*はい*	*はい*	*はい*	*はい*	*はい*	*はい*	*はい*	いいえ	いいえ	いいえ
9.11 .0*	*はい*	いいえ	*はい*	いいえ	*はい*	いいえ	*はい*	*はい*	*はい*	いいえ	*はい*	いいえ	*はい*	*はい*	*はい*	いいえ	いいえ	いいえ
9.10 .1	*はい*	*はい*	*はい*	*はい*	*はい*	*はい*	*はい*	*はい*	*はい*	*はい*	*はい*	*はい*	*はい*	*はい*	*はい*	*はい*	いいえ	いいえ
9.10 .0 *	*はい*	いいえ	*はい*	いいえ	*はい*	いいえ	*はい*	いいえ	*はい*	*はい*	*はい*	いいえ	*はい*	*はい*	*はい*	*はい*	いいえ	いいえ
9.9. 1	*はい*	*はい*	*はい*	*はい*	*はい*	*はい*	*はい*	*はい*	*はい*	*はい*	*はい*	*はい*	*はい*	*はい*	*はい*	*はい*	いいえ	いいえ
9.9.. 0 *	*はい*	いいえ	*はい*	いいえ	*はい*	いいえ	*はい*	いいえ	*はい*	いいえ	*はい*	*はい*	*はい*	*はい*	*はい*	*はい*	いいえ	いいえ

9.8	いいえ	*はい*	*はい*	*はい*	*はい*	*はい*	*はい*	*はい*	*はい*	*はい*	*はい*	*はい*	*はい*	*はい*	*はい*	*はい*	いいえ	*はい*
9.7	いいえ	いいえ	いいえ	いいえ	*はい*	*はい*	*はい*	*はい*	*はい*	*はい*	*はい*	*はい*	*はい*	*はい*	*はい*	*はい*	いいえ	*はい*
9.6	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ	*はい*	*はい*	*はい*	*はい*	*はい*	*はい*	*はい*	*はい*	*はい*	*はい*	いいえ	*はい*
9.5	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ	*はい*	*はい*	*はい*	*はい*	*はい*	*はい*	*はい*	*はい*	*はい*	*はい*
9.4	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ	*はい*	*はい*	*はい*
9.3	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ	*はい*	*はい*	*はい*	*はい*	*はい*	*はい*

## SnapMirror Synchronous 関係



ONTAP クラウドインスタンスではSnapMirror Synchronousはサポートされません。

ONTAP バージョン...	ONTAP の以前のバージョンとの相互運用性...									
	9.14.1	9.13.1	9.12.1:	9.11.1	9.10.1	9.9.1	9.8	9.7	9.6	9.5
9.14.1	*はい*	*はい*	*はい*	*はい*	*はい*	*はい*	*はい*	いいえ	いいえ	いいえ
9.13.1	*はい*	*はい*	*はい*	*はい*	*はい*	*はい*	*はい*	*はい*	いいえ	いいえ
9.12.1:	*はい*	*はい*	*はい*	*はい*	*はい*	*はい*	*はい*	*はい*	いいえ	いいえ
9.11.1	*はい*	*はい*	*はい*	*はい*	*はい*	*はい*	いいえ	いいえ	いいえ	いいえ
9.10.1	*はい*	*はい*	*はい*	*はい*	*はい*	*はい*	*はい*	いいえ	いいえ	いいえ
9.9.1	*はい*	*はい*	*はい*	*はい*	*はい*	*はい*	*はい*	*はい*	いいえ	いいえ
9.8	*はい*	*はい*	*はい*	いいえ	*はい*	*はい*	*はい*	*はい*	*はい*	いいえ
9.7	いいえ	*はい*	*はい*	いいえ	いいえ	*はい*	*はい*	*はい*	*はい*	*はい*
9.6	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ	*はい*	*はい*	*はい*	*はい*
9.5	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ	*はい*	*はい*	*はい*

## SnapMirror SVMディザスタリカバリ関係

- SVMディザスタリカバリのデータとSVM保護の場合：

SVMディザスタリカバリは、同じバージョンのONTAPを実行するクラスタ間でのみサポートされます。バージョンに依存しないレプリケーションは**SVM**レプリケーションではサポートされません。

- SVM移行のためのSVMディザスタリカバリの場合：

- ソース上のONTAPの以前のバージョンから、デスティネーション上のONTAPの同じバージョンまたはそれ以降のバージョンへのレプリケーションが単一方向でサポートされます。

- ターゲットクラスタのONTAPのバージョンが、次の表に示すように、オンプレミスのメジャーバージョンが2つ以上ないか、クラウドのメジャーバージョンが2つ以上ないようにする必要があります。

◦ 長期的なデータ保護のユースケースでは、レプリケーションはサポートされません。

リリースバージョンのあとにアスタリスク (\*) が表示されている場合、クラウドのみのリリースです。

サポートを確認するには、左側の表の列でソースバージョンを確認し、一番上の行でデスティネーションバージョンを確認します（類似バージョンの場合はDR/Migration、新しいバージョンの場合はMigrationのみ）。

ソース	デスティネーション																	
	9.3	9.4	9.5	9.6	9.7	9.8	9.9..0 *	9.9.1	9.10.0 *	9.10.1	9.11.0*	9.11.1	9.12.0 *	9.12.1:	9.13.0 *	9.13.1.	9.14.0 *	9.14.1
9.3	DR / 移行	データ移行	データ移行	データ移行	データ移行													
9.4		DR / 移行	データ移行	データ移行	データ移行	データ移行												
9.5			DR / 移行	データ移行	データ移行	データ移行	データ移行											
9.6				DR / 移行	データ移行	データ移行	データ移行	データ移行										
9.7					DR / 移行	データ移行	データ移行	データ移行	データ移行									
9.8						DR / 移行	データ移行	データ移行	データ移行	データ移行								
9.9..0 *							DR / 移行	データ移行	データ移行	データ移行	データ移行							
9.9.1								DR / 移行	データ移行	データ移行	データ移行	データ移行						
9.10.0 *									DR / 移行	データ移行	データ移行	データ移行	データ移行					
9.10.1										DR / 移行	データ移行	データ移行	データ移行	データ移行				
9.11.0*											DR / 移行	データ移行	データ移行	データ移行	データ移行			

9.11 .1												DR / 移行	デー タ移 行	デー タ移 行	デー タ移 行	デー タ移 行		
9.12 .0 *												DR / 移行	デー タ移 行	デー タ移 行	デー タ移 行	デー タ移 行		
9.12 .1:													DR / 移行	デー タ移 行	デー タ移 行	デー タ移 行	デー タ移 行	
9.13 .0 *														DR / 移行	デー タ移 行	デー タ移 行	デー タ移 行	
9.13 .1.															DR / 移行	デー タ移 行	デー タ移 行	
9.14 .0 *																DR / 移行	デー タ移 行	
9.14 .1																		DR / 移行

## SnapMirrorディザスタリカバリ関係

タイプが「\D」でポリシータイプが「async」の SnapMirror 関係の場合：



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



次の表で、左側の列はソースボリュームの ONTAP のバージョン、上部の行はデスティネーションボリュームで利用できる ONTAP のバージョンを示しています。

ソース	デスティネーション											
	9.11.1	9.10.1	9.9.1	9.8	9.7	9.6	9.5	9.4	9.3	9.2.	9.1	9
9.11.1	はい。	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ
9.10.1	はい。	はい。	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ
9.9.1	はい。	はい。	はい。	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ
9.8	いいえ	はい。	はい。	はい。	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ
9.7	いいえ	いいえ	はい。	はい。	はい。	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ
9.6	いいえ	いいえ	いいえ	はい。	はい。	はい。	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ
9.5	いいえ	いいえ	いいえ	いいえ	はい。	はい。	はい。	いいえ	いいえ	いいえ	いいえ	いいえ
9.4	いいえ	いいえ	いいえ	いいえ	いいえ	はい。	はい。	はい。	いいえ	いいえ	いいえ	いいえ
9.3	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ	はい。	はい。	はい。	いいえ	いいえ	いいえ

9.2.	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ	はい。	はい。	はい。	いいえ	いいえ
9.1	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ	はい。	はい。	はい。	いいえ
9	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ	はい。	はい。	はい。



双方向の互換性はありません。

## SnapMirror の制限事項

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

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



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

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



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

## SnapLock テクノロジーを使用したアーカイブとコンプライアンス

### SnapLock とは

SnapLock は、規制やガバナンスに準拠するために WORM ストレージを使用して変更不可能な状態でファイルを保管する組織向けの、ハイパフォーマンスなコンプライアンス解決策です。

SnapLock を使用すると、SEC 17a-4、HIPAA、FINRA、CFTC、GDPR などの規制に準拠するために、データの削除、変更、または名前変更を防止できます。SnapLock を使用すると、特定の保持期間または無期限に、ファイルを保存して消去および書き込み不可能な状態にコミットできる特別な目的のボリュームを作成できます。SnapLock では、CIFS や NFS などの標準オープンファイルプロトコルを使用して、ファイルレベルでこのようなデータ保持を実行できます。SnapLock でサポートされるオープンファイルプロトコルは、NFS（バージョン 2、3、4）と CIFS（SMB 1.0、2.0、および 3.0）です。

SnapLock を使用して、ファイルと Snapshot コピーを WORM ストレージにコミットし、WORM 方式で保護されたデータの保持期間を設定します。SnapLock WORM ストレージでは、ネットアップの Snapshot テクノロ



ジを使用し、SnapMirrorレプリケーションとSnapVault バックアップをベーステクノロジーとして活用することで、データをバックアップリカバリで保護できます。  
WORMストレージの詳細：["NetApp SnapLock - TR-4526を使用して準拠したWORMストレージを実現します"](#)。

アプリケーションを使用して、NFS または CIFS 経由でファイルを WORM にコミットするか、SnapLock の自動コミット機能を使用してファイルを自動的にコミットすることができます。追記可能 WORM ファイルを使用すると、ログ情報のように段階的に書き込まれるデータを保持できます。詳細については、[を参照してください](#) ["ボリュームアペンドモードを使用して追記可能 WORM ファイルを作成します"](#)。

SnapLock でサポートされるデータ保護方法は、ほとんどのコンプライアンス要件に対応します。

- SnapLock for SnapVault を使用して、セカンダリストレージ上の Snapshot コピーを WORM 方式で保護できます。[を参照してください](#) ["Snapshot コピーを WORM 状態にコミット"](#)。
- SnapMirror を使用すると、ディザスタリカバリ目的で地理的に離れた別の場所に WORM ファイルをレプリケートできます。[を参照してください](#) ["WORM ファイルをミラーリングします"](#)。

SnapLock は、NetApp ONTAP のライセンスベースの機能です。1 つのライセンスで、SEC Rule 17a-4 などの社外規定に準拠するための厳格なコンプライアンスモードと、社内規定に準拠してデジタル資産を保護するためのより緩やかなエンタープライズモードで SnapLock を使用できます。SnapLock ライセンスは、["ONTAP One"](#) ソフトウェアスイート。

SnapLock は、すべてのAFF およびFAS システム、およびONTAP Select でサポートされています。SnapLock は、ソフトウェアのみの解決策ではなく、ハードウェアとソフトウェアを統合した解決策です。この違いは、ハードウェアとソフトウェアを統合した解決策が必要なSEC 17a-4などの厳しいWORM規制に重要です。詳細については、[を参照してください](#) ["SEC通訳：ブローカー電子保管-ディーラー記録"](#)。

## SnapLock でできること

SnapLock を設定したら、次の作業を実行できます。

- ["ファイルを WORM 状態にコミット"](#)
- ["セカンダリストレージのSnapshotコピーをWORM状態にコミットします"](#)
- ["ディザスタリカバリ用にWORMファイルをミラーリング"](#)
- ["リーガルホールドを使用して訴訟の際にWORMファイルを保持する"](#)
- ["privileged delete機能を使用してWORMファイルを削除します"](#)
- ["ファイルの保持期間を設定します"](#)
- ["SnapLock ボリュームを移動"](#)
- ["Snapshotコピーをロックしてランサムウェア攻撃から保護する"](#)
- ["監査ログでSnapLock の使用状況を確認します"](#)
- ["SnapLock APIを使用する"](#)

## SnapLock 準拠モードとエンタープライズモード

SnapLock の Compliance モードと Enterprise モードの主な違いは、WORM ファイルの保護レベルです。

SnapLock モード	保護レベル	保持中のWORMファイル削除
--------------	-------	----------------

Complianceモオト	ファイルレベルで指定します	削除できません
Enterpriseモード	をクリックします	監査された「privileged delete」手順を使用して、コンプライアンス管理者が削除できます

保持期間が経過したあとに不要となったファイルはすべて削除する必要があります。一度 WORM 状態にコミットされたファイルは、Compliance モードであるか Enterprise モードであるかに関係なく、保持期間が経過したあとも変更することはできません。

WORM ファイルは保持期間中も保持期間後も移動できません。WORM ファイルはコピーできますが、コピーしたファイルは WORM 状態にはなりません。

次の表に、SnapLock のComplianceモードとEnterpriseモードでサポートされる機能の違いを示します。

機能	SnapLock コンプライアンス	SnapLock エンタープライズ
privileged deleteを使用してファイルを有効化および削除します	いいえ	はい。
ディスクを再初期化する	いいえ	はい。
保持期間中にSnapLock のアグリゲートとボリュームを削除	いいえ	はい。ただし、SnapLock 監査ログボリュームは例外です
アグリゲートまたはボリュームの名前を変更します	いいえ	はい。
ネットアップ以外のディスクを使用する	いいえ	はい（。あり <a href="#">"FlexArray 仮想化"</a> ）
監査ログにはSnapLock ボリュームを使用します	はい。	はい、ONTAP 9.5 以降で使用できます

## SnapLock でサポートされる機能とサポートされない機能

次の表に、SnapLock Complianceモード、SnapLock Enterpriseモード、またはその両方でサポートされる機能を示します。

フィーチャー（Feature）	SnapLock Complianceでサポートされます	SnapLock Enterpriseでサポートされます
整合グループ	いいえ	いいえ
暗号化されたボリューム	はい（ONTAP 9.2以降）。の詳細を確認してください <a href="#">暗号化とSnapLock</a> 。	はい（ONTAP 9.2以降）。の詳細を確認してください <a href="#">暗号化とSnapLock</a> 。

SnapLock アグリゲートのFabricPool	いいえ	はい、ONTAP 9.8以降です。の詳細を確認してください <a href="#">SnapLock Enterpriseアグリゲート上のFabricPool</a> 。
Flash Pool アグリゲート	はい、ONTAP 9.1以降でサポートされています。	はい、ONTAP 9.1以降でサポートされています。
FlexClone	SnapLock ボリュームはクローニングできますが、SnapLock ボリューム上のファイルはクローニングできません。	SnapLock ボリュームはクローニングできますが、SnapLock ボリューム上のファイルはクローニングできません。
FlexGroup ボリューム	はい。ONTAP 9.11.1以降で使用してください。の詳細を確認してください <a href="#">[flexgroup]</a> 。	はい。ONTAP 9.11.1以降で使用してください。の詳細を確認してください <a href="#">[flexgroup]</a> 。
LUN	いいえの詳細を確認してください <a href="#">LUNのサポート</a> SnapLockを使用。	いいえの詳細を確認してください <a href="#">LUNのサポート</a> SnapLockを使用。
MetroCluster 構成	はい。ONTAP 9.3以降。の詳細を確認してください <a href="#">MetroCluster のサポート</a> 。	はい。ONTAP 9.3以降。の詳細を確認してください <a href="#">MetroCluster のサポート</a> 。
マルチ管理者認証 (MAV)	はい。ONTAP 9.13.1以降でサポートされています。の詳細を確認してください <a href="#">MAVサポート</a> 。	はい。ONTAP 9.13.1以降でサポートされています。の詳細を確認してください <a href="#">MAVサポート</a> 。
SAN	いいえ	いいえ
単一ファイルの SnapRestore	いいえ	はい。
SnapMirror によるビジネス継続性	いいえ	いいえ
SnapRestore	いいえ	はい。
SMTape の場合	いいえ	いいえ
SnapMirror Synchronous	いいえ	いいえ
SSD	はい、ONTAP 9.1以降でサポートされています。	はい、ONTAP 9.1以降でサポートされています。

Storage Efficiency機能	はい。ONTAP 9.9.1以降でサポートされています。の詳細を確認してください <a href="#">Storage Efficiencyのサポート</a> 。	はい。ONTAP 9.9.1以降でサポートされています。の詳細を確認してください <a href="#">Storage Efficiencyのサポート</a> 。
----------------------	--	--

## SnapLock Enterprise アグリゲート上のFabricPool

ONTAP 9.8以降のFabricPoolは、SnapLock エンタープライズアグリゲートでサポートされています。ただし、クラウド管理者がそのデータを削除できるため、アカウントチームは、パブリッククラウドまたはプライベートクラウドに階層化されたFabricPool のデータはSnapLock で保護されなくなったことを理解していることを示すProduct Variance Requestを開く必要があります。



FabricPool からパブリッククラウドまたはプライベートクラウドに階層化されたデータは、クラウド管理者が削除できるため、SnapLock で保護されなくなります。

## FlexGroup ボリューム

SnapLock はONTAP 9.11.1以降でFlexGroup ボリュームをサポートしていますが、次の機能はサポートされません。

- リーガルホールド
- イベントベースの保持
- SnapLock for SnapVault （ONTAP 9.12.1以降でサポート）

また、次の動作についても理解しておく必要があります。

- FlexGroup のボリュームコンプライアンスクロック（VCC）は、ルートコンスティチュエントのVCCによって決まります。すべての非ルートコンスティチュエントのVCCはルートのVCCと密接に同期されます。
- SnapLock の設定プロパティは、FlexGroup 全体にのみ設定されます。デフォルトの保持期間や自動コミット期間など、個々のコンスティチュエントごとに異なる設定プロパティを指定することはできません。

## LUNのサポート

SnapLockでは、SnapLock以外のボリュームで作成されたSnapshotコピーをSnapLockバックアップ関係の一部として保護するためにSnapLockに転送する場合にのみ、LUNがサポートされます。読み取り/書き込みSnapLockボリュームではLUNはサポートされません。ただし、Snapshotコピーの改ざんは、SnapMirrorのソースボリュームと、LUNを含むデスティネーションボリュームの両方でサポートされます。

## MetroCluster のサポート

MetroCluster 構成でのSnapLock のサポートは、SnapLock ComplianceモードとSnapLock Enterpriseモードで異なります。

### SnapLock コンプライアンス

- ONTAP 9.3以降では、ミラーされていないMetroCluster アグリゲートでSnapLock Complianceがサポートされます。
- ONTAP 9.3以降では、ミラーされたアグリゲートでSnapLock Complianceがサポートされます。ただし、SnapLock 監査ログボリュームのホストにアグリゲートが使用される場合のみです。

- MetroCluster を使用して、プライマリサイトとセカンダリサイトにSVM固有のSnapLock 設定をレプリケートできます。

### SnapLock エンタープライズ

- ONTAP 9以降では、SnapLock エンタープライズアグリゲートがサポートされます。
- ONTAP 9.3以降では、privileged deleteを使用したSnapLock Enterpriseアグリゲートがサポートされます。
- SVM固有のSnapLock 設定は、MetroCluster を使用して両方のサイトにレプリケートできます。

### MetroCluster 構成とコンプライアンスクロック

MetroCluster 構成では、Volume Compliance Clock（VCC；ボリュームコンプライアンスクロック）と System Compliance Clock（SCC；システムコンプライアンスクロック）の2つのコンプライアンスクロックメカニズムが使用されます。VCC と SCC はすべての SnapLock 構成で使用できます。ノードに新しいボリュームを作成すると、ボリュームの VCC はそのノードの現在の SCC の値に初期化されます。ボリューム作成後のボリュームとファイルの保持期限の追跡には、常に VCC が使用されます。

ボリュームを別のサイトにレプリケートすると、ボリュームの VCC も一緒にレプリケートされます。ボリュームのスイッチオーバーが発生した場合、サイト A からサイト B へのスイッチオーバーなどで、サイト B の VCC は引き続き更新されますが、サイト A がオフラインになるとサイト A の SCC が停止します。

サイト A がオンラインに戻り、ボリュームのスイッチバックが実行されると、サイト A の SCC のクロックが再開されますが、ボリュームの VCC は引き続き更新されます。VCC は継続的に更新されるため、スイッチオーバーやスイッチバックの処理に関係なくファイルの保持期限は SCC に依存せず、期限が延びることはありません。

### Multi-Admin Verification (MAV) のサポート

ONTAP 9.13.1以降では、クラスタ管理者がクラスタでマルチ管理者検証を明示的に有効にして、一部のSnapLock処理を実行する前にクォーラムの承認が必要になるようにすることができます。MAVが有効な場合は、default-retention-time、minimum-retention-time、maximum-retention-time、volume-append-mode、自動コミット期間、privileged-deleteなどのSnapLockボリュームプロパティでクォーラムの承認が必要になります。の詳細を確認してください ["MAV"](#)。

### ストレージ効率

ONTAP 9.9.1以降SnapLock では、SnapLock およびアグリゲートに対して、データコンパクション、ボリューム間重複排除、適応圧縮などのStorage Efficiency機能がサポートされます。Storage Efficiencyの詳細については、を参照してください ["CLI による論理ストレージ管理の概要"](#)。

### 暗号化

ONTAP は、ストレージメディアの転用、返却、置き忘れ、盗難に際して保存データが読み取られることがないようにソフトウェアベースとハードウェアベースの暗号化テクノロジーを提供します。

- 免責事項：\* 認証キーが紛失した場合や、認証に失敗した回数が指定した制限を超えたためにドライブが永続的にロックされた場合、自己暗号化ドライブまたはボリューム上の SnapLock で保護された WORM ファイルを取得できるかどうかは、ネットアップでは保証できません。認証エラーへの対策はお客様の責任で行ってください。



ONTAP 9.2 以降では、SnapLock アグリゲートで暗号化されたボリュームがサポートされます。

## 7-Mode からの移行

7-Mode Transition Toolのコピーベースの移行（CBT）機能を使用して、SnapLock ボリュームを7-ModeからONTAP に移行できます。デスティネーションボリュームの SnapLock モードである Compliance または Enterprise とソースボリュームの SnapLock モードが一致している必要があります。コピーフリーの移行（CFT）は SnapLock ボリュームの移行には使用できません。

## SnapLock を設定します

### SnapLock を設定します

SnapLockを使用する前に、次のようなさまざまなタスクを実行してSnapLockを設定する必要があります。"[SnapLockライセンスをインストールする](#)" SnapLockボリュームを含むアグリゲートをホストする各ノードについて、"[コンプライアンスクロック](#)"、ONTAP 9.10.1より前のリリースのONTAPを実行するクラスタ用にSnapLockアグリゲートを作成します。"[SnapLockボリュームの作成とマウント](#)"など。

### コンプライアンスクロックを初期化します

SnapLockでは、`_volumeコンプライアンスクロック_`を使用して、改ざんによるWORM ファイルの保持期間の変更を防止します。最初に、SnapLockアグリゲートをホストする各ノードで`_system ComplianceClock_`を初期化する必要があります。

ONTAP 9.14.1以降では、Snapshotコピーロックが有効になっているSnapLockボリュームがない場合やボリュームがない場合に、システムコンプライアンスクロックを初期化または再初期化できます。再初期化機能を使用すると、システム管理者は、システムコンプライアンスクロックが誤って初期化されたり、システムのクロックドリフトが修正されたりした場合に、システムコンプライアンスクロックをリセットできます。ONTAP 9.13.1以前のリリースでは、一度ノードでコンプライアンスクロックを初期化すると、再度初期化することはできません。

### 作業を開始する前に

コンプライアンスクロックを再初期化する手順は、次のとおりです。

- クラスタ内のすべてのノードが正常な状態である必要があります。
- すべてのボリュームがオンラインである必要があります。
- どのボリュームもリカバリキューに含めることができません。
- SnapLockボリュームが存在できません。
- Snapshotコピーロックが有効になっているボリュームは存在できません。

コンプライアンスクロックを初期化するための一般的な要件：

- このタスクを実行するには、クラスタ管理者である必要があります。
- "[ノードにSnapLockライセンスがインストールされている必要があります。](#)"。

### このタスクについて

システムのコンプライアンスクロックの時間は`_volumeコンプライアンスクロック_`に継承され、ボリューム上のWORMファイルの保持期間はボリューム側で制御されます。ボリュームコンプライアンスクロックは、



新しいSnapLockを作成すると自動的に初期化されます。



システムコンプライアンスクロックの初期設定は、現在のハードウェアシステムクロックに基づいています。そのため、各ノードでシステムコンプライアンスクロックを初期化する前に、システム時間とタイムゾーンが正しいことを確認する必要があります。ノードでシステムコンプライアンスクロックを初期化すると、ロックが有効なSnapLockボリュームまたはボリュームが存在する場合、再度初期化することはできません。

## 手順

ONTAP CLIを使用してコンプライアンスクロックを初期化できます。ONTAP 9.12.1以降では、System Managerを使用してコンプライアンスクロックを初期化できます。

### System Manager の略

1. [Cluster]>[Overview]に移動します。
2. [ノード]セクションで、[Initialize SnapLock Compliance Clock\*]をクリックします。
3. コンプライアンスクロック\*列を表示してコンプライアンスクロックが初期化されたことを確認するには、[クラスタ]>[概要]>[ノード]\*セクションで[表示/非表示]をクリックし、[SnapLockコンプライアンスクロック]\*を選択します。

### CLI の使用

1. システムコンプライアンスクロックを初期化します。

```
snaplock compliance-clock initialize -node node_name
```

次のコマンドは、システムコンプライアンスクロックをオンに初期化します。 node1 :

```
cluster1::> snaplock compliance-clock initialize -node node1
```

2. プロンプトが表示されたら、システムクロックが正しいこと、およびコンプライアンスクロックを初期化することを確認します。

```
Warning: You are about to initialize the secure ComplianceClock of
the node "node1" to the current value of the node's system clock.
This procedure can be performed only once on a given node, so you
should ensure that the system time is set correctly before
proceeding.
```

```
The current node's system clock is: Mon Apr 25 06:04:10 GMT 2016
```

```
Do you want to continue? (y|n): y
```

3. SnapLock アグリゲートをホストする各ノードについて、この手順を繰り返します。

NTPが設定されたシステムでコンプライアンスクロックの再同期を有効にする

サーバが設定されている場合は、SnapLockコンプライアンスクロック時間同期機能を有効にできます。

必要なもの

- この機能は、advanced 権限レベルでのみ使用できます。
- このタスクを実行するには、クラスタ管理者である必要があります。
- "ノードにSnapLockライセンスがインストールされている必要があります。"。
- この機能は、Cloud Volumes ONTAP、ONTAP Select、および vsim プラットフォームでのみ使用できます。

このタスクについて

SnapLockセキュアクロックデーモンがしきい値を超えたスキューを検出すると、ONTAPはシステム時間を使用してシステムクロックとボリュームコンプライアンスクロックの両方をリセットします。スキューのしきい値は 24 時間に設定されています。つまり、スキューが1日以上経過した場合にのみ、システムコンプライアンスクロックがシステムクロックに同期されます。

SnapLockセキュアクロックデーモンはスキューを検出し、コンプライアンスクロックをシステム時間に変更します。コンプライアンスクロックはシステム時間がNTP時間と同期されている場合にのみシステム時間と同期されるため、コンプライアンスクロックを強制的にシステム時間に変更しようとすると失敗します。

手順

1. サーバが設定されている場合は、SnapLockコンプライアンスクロック時間同期機能を有効にします。

```
snaplock compliance-clock ntp
```

次のコマンドは、システムコンプライアンスクロック時間同期機能を有効にします。

```
cluster1::*> snaplock compliance-clock ntp modify -is-sync-enabled true
```

2. プロンプトが表示されたら、設定した NTP サーバが信頼できることと、通信チャネルがセキュアであることを確認して機能を有効にします。
3. 機能が有効になっていることを確認します。

```
snaplock compliance-clock ntp show
```

次のコマンドは、システムコンプライアンスクロック時間同期機能が有効になっていることを確認します。

```
cluster1::*> snaplock compliance-clock ntp show  
  
Enable clock sync to NTP system time: true
```

**SnapLock** アグリゲートを作成する

ボリュームを使用します -snaplock-type ComplianceまたはEnterprise SnapLock ボ



リユームのタイプを指定するオプション。ONTAP 9.10.1 よりも前のリリースでは、別の SnapLock アグリゲートを作成する必要があります。ONTAP 9.10.1 以降では、SnapLock ボリユームと非 SnapLock ボリユームを同じアグリゲート上に配置できるため、ONTAP 9.10.1 を使用している場合に別の SnapLock アグリゲートを作成する必要がなくなりました。

作業を開始する前に

- このタスクを実行するには、クラスタ管理者である必要があります。
- SnapLock ["ライセンスをインストールする必要があります"](#) をクリックします。このライセンスは、["ONTAP One"](#)。
- ["ノードのコンプライアンスクロックを初期化する必要があります"](#)。
- ディスクを「root」、「data1」、および「data2」としてパーティショニングした場合、スペアディスクが利用可能であることを確認する必要があります。

アップグレード時の考慮事項

ONTAP 9.10.1 にアップグレードすると、既存の SnapLock アグリゲートおよび非 SnapLock アグリゲートが SnapLock ボリユームと非 SnapLock ボリユームの両方の存在をサポートするようにアップグレードされますが、既存の SnapLock ボリユームの属性は自動的に更新されません。たとえば、データコンパクション、ボリユーム間重複排除、およびボリユーム間バックグラウンド重複排除のフィールドは変更されません。既存のアグリゲートに作成された新しい SnapLock ボリユームのデフォルト値は SnapLock 以外のボリユームと同じで、新しいボリユームおよびアグリゲートのデフォルト値はプラットフォームごとに異なります。

リバートに関する考慮事項

9.10.1 より前のバージョンの ONTAP にリバートする必要がある場合は、すべての SnapLock Compliance ボリユーム、SnapLock Enterprise ボリユーム、および SnapLock ボリユームをそれぞれ独自の SnapLock アグリゲートに移動する必要があります。

このタスクについて

- FlexArray LUN に対して Compliance アグリゲートを作成することはできませんが、FlexArray Compliance アグリゲートは SnapLock LUN でサポートされます。
- SyncMirror オプションを使用して Compliance アグリゲートを作成することはできません。
- ミラーされた Compliance アグリゲートを MetroCluster 構成に作成できるのは、アグリゲートを SnapLock 監査ログボリユームのホストとして使用する場合だけです。



MetroCluster 構成では、ミラーされたアグリゲートとミラーされていないアグリゲートで SnapLock Enterprise がサポートされます。SnapLock Compliance は、ミラーされていないアグリゲートでのみサポートされます。

手順

1. SnapLock アグリゲートを作成します。

```
storage aggregate create -aggregate <aggregate_name> -node <node_name>
-diskcount <number_of_disks> -snaplock-type <compliance|enterprise>
```

すべてのオプションの一覧については、コマンドのマニュアルページを参照してください。

次のコマンドは、SnapLock を作成します Compliance という名前のアグリゲート aggr1 3本のディスクをオンにします node1 :

```
cluster1::> storage aggregate create -aggregate aggr1 -node node1
-diskcount 3 -snaplock-type compliance
```

## SnapLock ボリュームを作成してマウント

WORM 状態にコミットするファイルまたは Snapshot コピーに対しては、SnapLock ボリュームを作成する必要があります。ONTAP 9.10.1 以降では、アグリゲートの種類に関係なく、作成するすべてのボリュームがデフォルトで SnapLock 以外のボリュームとして作成されます。を使用する必要があります -snaplock-type SnapLock タイプとして Compliance または Enterprise を指定して SnapLock ボリュームを明示的に作成するオプション。デフォルトでは、SnapLock タイプはに設定されています non-snaplock。

作業を開始する前に

- SnapLock アグリゲートがオンラインになっている必要があります。
- お勧めします ["SnapLock ライセンスがインストールされていることの確認"](#)。ノードに SnapLock ライセンスがインストールされていない場合は、次の手順を実行する必要があります。 ["をインストールします"](#) それは...このライセンスは、 ["ONTAP One"](#)。ONTAP One よりも前のリリースでは、SnapLock ライセンスは Security and Compliance Bundle に含まれていました。Security and Compliance Bundle の提供は終了しましたが、引き続き有効です。現在は必須ではありませんが、既存のお客様は ["ONTAP One へのアップグレード"](#)。
- ["ノードのコンプライアンスクロックを初期化する必要があります"](#)。

このタスクについて

適切な SnapLock 権限を使用すれば、いつでも Enterprise ボリュームの削除や名前変更を行うことができます。Compliance ボリュームの削除は保持期間が終了するまでは実行できません。Compliance ボリュームの名前は一切変更できません。

SnapLock ボリュームはクローニングできますが、SnapLock ボリューム上のファイルはクローニングできません。クローンボリュームの SnapLock タイプは親ボリュームと同じになります。



SnapLock ボリュームでは LUN はサポートされません。SnapLock では、SnapLock 以外のボリュームで作成された Snapshot コピーを SnapLock バックアップ関係の一部として保護するために SnapLock に転送する場合にのみ、LUN がサポートされます。読み取り/書き込み SnapLock ボリュームでは LUN はサポートされません。ただし、Snapshot コピーの改ざんは、SnapMirror のソースボリュームと、LUN を含むデスティネーションボリュームの両方でサポートされます。

この作業は、ONTAP システムマネージャまたは ONTAP CLI を使用して実行します。

## System Manager の略

ONTAP 9.12.1以降では、System Managerを使用してSnapLock ボリュームを作成できます。

### 手順

1. [\*Storage]>[Volumes]に移動し、[\*Add]をクリックします。
2. [ボリュームの追加\*]ウィンドウで、[その他のオプション]をクリックします。
3. ボリュームの名前とサイズなど、新しいボリューム情報を入力します。
4. 「\* SnapLock を有効にする\*」を選択し、SnapLock タイプとして「Compliance」または「Enterprise」を選択します。
5. [ファイルの自動コミット\*]セクションで、[変更済み]を選択し、ファイルが自動的にコミットされるまでに変更されないようにする時間を入力します。最小値は 5 分、最大値は 10 年です。
6. [\*データ保持期間]セクションで、最小保持期間と最大保持期間を選択します。
7. デフォルトの保持期間を選択します。
8. [保存 (Save) ] をクリックします。
9. [\* Volumes]ページで新しいボリュームを選択し、SnapLock 設定を確認します。

### CLI の使用

1. SnapLock ボリュームを作成します。

```
volume create -vserver <SVM_name> -volume <volume_name> -aggregate  
<aggregate_name> -snaplock-type <compliance|enterprise>
```

すべてのオプションの一覧については、コマンドのマニュアルページを参照してください。次のオプションは、SnapLock ボリュームに対しては使用できません。-nvfail、-atime-update、-is-autobalance-eligible、-space-mgmt-try-first`および `vmalign。

次のコマンドは、SnapLock を作成します Compliance という名前のボリューム vol1 オン aggr1 オン vs1：

```
cluster1::> volume create -vserver vs1 -volume vol1 -aggregate aggr1  
-snaplock-type compliance
```

## SnapLock ボリュームをマウント

NAS クライアントからアクセスできるように、SnapLock ボリュームを SVM ネームスペースのジャンクションパスにマウントすることができます。

### 必要なもの

SnapLock ボリュームはオンラインである必要があります。

### このタスクについて

- SnapLock ボリュームは SVM のルートにしかマウントできません。
- 通常のボリュームを SnapLock ボリュームにマウントすることはできません。

## 手順

1. SnapLock ボリュームをマウントします。

```
volume mount -vserver SVM_name -volume volume_name -junction-path path
```

すべてのオプションの一覧については、コマンドのマニュアルページを参照してください。

次のコマンドは、という名前の SnapLock ボリュームをマウントします vol1 ジャンクションパスに移動します /sales を参照してください vs1 ネームスペース：

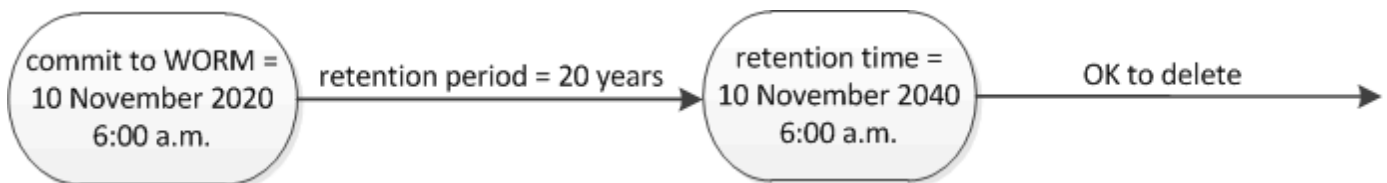
```
cluster1::> volume mount -vserver vs1 -volume vol1 -junction-path /sales
```

## 保持期限を設定

保持期限の設定については、ファイルに対して明示的に設定する方法と、ボリュームのデフォルトの保持期間から自動的に設定する方法があります。保持期限を明示的に設定しないかぎり、SnapLock はデフォルトの保持期間を使用して保持期限を計算します。イベント発生後のファイル保持期間を設定することもできます。

### 保持期間と保持期限の概要

WORM ファイルの *retention period* は、WORM 状態にコミットされたファイルを保持する必要がある期間を指定します。WORM ファイルの *\_retention time\_* は、その時点までファイルを保持する必要がなくなった時間です。たとえば、ファイルが 2020 年 11 月 10 日の午前 6 時に WORM 状態にコミットされた場合、ファイルの保持期間が 20 年であれば、保持期限は 2040 年 11 月 10 日の午前 6 時になります



ONTAP 9.10.1 以降では、最大 10 月 26 日、3058 日、保持期間を 100 年に設定できます。保持期限を延長すると、古いポリシーが自動的に変換されます。ONTAP 9.9.1 以前のリリースでは、デフォルトの保持期間を無期限に設定した場合を除き、サポートされる最大保持期間は 2071 年 1 月 19 日 (GMT) です。

### レプリケーションに関する重要な考慮事項

2071年1月19日 (GMT) よりもあとの保持期限を使用して SnapLock ソースボリュームとの SnapMirror 関係を確立する場合、デスティネーションクラスタで ONTAP 9.10.1 以降が実行されている必要があります。実行されていないと SnapMirror 転送が失敗します。

### リバートに関する重要な考慮事項

ONTAP では、保持期間が「January 19、2071 8:44:07 AM」よりもあとのファイルがある場合、ONTAP 9.10.1 から以前の ONTAP バージョンにクラスタをリバートすることはできません。

## 保持期間について

SnapLock Compliance または Enterprise ボリュームには、次の 4 つの保持期間があります。

- 最小保持期間 (min) を使用します。デフォルトは0です
- 最大保持期間 (max) 、デフォルトは30年です
- デフォルトの保持期間。デフォルトはと同じです min ONTAP 9.10.1以降では、ComplianceモードとEnterpriseモードの両方に対応しています。ONTAP 9.10.1 より前の ONTAP リリースでは、デフォルトの保持期間はモードによって異なります。
  - コンプライアンスモードの場合、デフォルトはと同じです max。
  - エンタープライズモードの場合、デフォルトはと同じです min。
- 指定されていない保持期間。

ONTAP 9.8以降では、ボリューム内のファイルの保持期間をに設定できます `unspecified` をクリックすると、絶対的な保持期限を設定するまでファイルが保持されます。新しい絶対保持時間が前に設定した絶対保持時間よりもあとであれば、絶対保持時間を指定せずに絶対保持に戻してもかまいません。

ONTAP 9.12.1以降、保持期間がに設定されたWORMファイル unspecified は、SnapLock ボリュームに対して設定された最小保持期間に保持期間が設定されていることが保証されます。ファイルの保持期間をから変更したとき unspecified 絶対保持期限には、ファイルにすでに設定されている最小保持期限よりも新しい保持期限を指定する必要があります。

したがって、Compliance モードのファイルを WORM 状態にコミットする前に保持期限を明示的に設定していない場合、デフォルトを変更していなければファイルは 30 年間保持されます。同様に、Enterprise モードのファイルを WORM 状態にコミットする前に保持期限を明示的に設定していない場合、デフォルトを変更していなければファイルは 0 年、つまり実質的には保持されません。

## デフォルトの保持期間を設定


を使用できます volume snaplock modify コマンドを使用して、SnapLock ボリューム上のファイルのデフォルトの保持期間を設定します。

## 必要なもの

SnapLock ボリュームはオンラインである必要があります。

## このタスクについて

次の表に、デフォルトの保持期間に指定できる値を示します。

- 
- デフォルトの保持期間は、最小保持期間以上、最大保持期間以下にする必要があります。

価値	単位	注：
0 ~ 65535	秒	
0 ~ 24	時間	
0 ~ 365	日	

価値	単位	注：
0 ~ 12	月	
0 ~ 100	年	ONTAP 9.10.1以降でサポートされます。以前のONTAP リリースの場合、値は0 ~ 70です。
最大	-	最大保持期間を使用します。
最小	-	最小保持期間を使用します。
制限なし	-	ファイルを無期限に保持します。
未指定	-	絶対保持期間が設定されるまでファイルを保持します。

最大保持期間と最小保持期間の値と範囲は、を除き同じです max および `min` は適用されません。このタスクの詳細については、を参照してください ["保持期限の概要を設定"](#)。

を使用できます volume snaplock show コマンドを使用してボリュームの保持期間設定を表示します。詳細については、コマンドのマニュアルページを参照してください。



ファイルが WORM 状態にコミットされたあとは、保持期間を延長することはできますが短縮することはできません。

## 手順

1. SnapLock ボリューム上のファイルにデフォルトの保持期間を設定します。

```
volume snaplock modify -vserver SVM_name -volume volume_name -default
-retention-period default_retention_period -minimum-retention-period
min_retention_period -maximum-retention-period max_retention_period
```

すべてのオプションの一覧については、コマンドのマニュアルページを参照してください。



次の例は、最小保持期間と最大保持期間が過去に変更されていないことを前提としています。

次のコマンドは、Compliance ボリュームまたは Enterprise ボリュームのデフォルトの保持期間を 20 日に設定します。

```
cluster1::> volume snaplock modify -vserver vs1 -volume vol1 -default
-retention-period 20days
```

次のコマンドは、Compliance ボリュームのデフォルトの保持期間を 70 年に設定します。

```
cluster1::> volume snaplock modify -vserver vs1 -volume vol1 -maximum  
-retention-period 70years
```

次のコマンドは、Enterprise ボリュームのデフォルトの保持期間を 10 年に設定します。

```
cluster1::> volume snaplock modify -vserver vs1 -volume vol1 -default  
-retention-period max -maximum-retention-period 10years
```

次のコマンドは、Enterprise ボリュームのデフォルトの保持期間を 10 日に設定します。

```
cluster1::> volume snaplock modify -vserver vs1 -volume vol1 -minimum  
-retention-period 10days  
cluster1::> volume snaplock modify -vserver vs1 -volume vol1 -default  
-retention-period min
```

次のコマンドは、Compliance ボリュームのデフォルトの保持期間を無期限に設定します。

```
cluster1::> volume snaplock modify -vserver vs1 -volume vol1 -default  
-retention-period infinite -maximum-retention-period infinite
```

#### ファイルの保持期限の明示的な設定

ファイルに対して保持期限を明示的に設定するには、最終アクセス時刻を変更します。最終アクセス時刻は、NFS または CIFS で適切なコマンドやプログラムを使用して変更できます。

#### このタスクについて

ファイルが WORM 状態にコミットされたあとは、保持期限を延長することはできますが短縮することはできません。保持期限はに格納されます atime ファイルのフィールド。



ファイルの保持期限をに明示的に設定することはできません infinite。この値は、デフォルトの保持期間を使用して保持期限を計算する場合にのみ使用できます。

#### 手順

1. 適切なコマンドまたはプログラムを使用して、保持期限を設定するファイルの最終アクセス日時を変更します。

UNIX シェルで、次のコマンドを使用して、保持期限を 2020 年 11 月 21 日の午前 6 時に設定しますという名前のファイルで作成します document.txt :

```
touch -a -t 202011210600 document.txt
```





Windows では、任意の適切なコマンドまたはプログラムを使用して最終アクセス時刻を変更できます。

イベント後のファイル保持期間を設定します

ONTAP 9.3以降では、SnapLock のイベントベースの保持（EBR）機能を使用して、イベントの発生後にファイルを保持する期間を定義できます。

必要なもの

- このタスクを実行するには、SnapLock 管理者である必要があります。

["SnapLock 管理者アカウントを作成します"](#)

- セキュアな接続（SSH、コンソール、または ZAPI）でログインする必要があります。

このタスクについて

イベント保持ポリシーは、イベント発生後のファイルの保持期間を定義します。このポリシーは、単一のファイルに適用することも、ディレクトリ内のすべてのファイルに適用することもできます。

- WORM ファイル以外のファイルの場合、ポリシーで定義された保持期間にわたって WORM 状態にコミットされます。
- WORM ファイルまたは追記可能 WORM ファイルの場合、保持期間がポリシーで定義された保持期間まで延長されます。

Compliance モードまたは Enterprise モードのボリュームを使用できます。



EBR ポリシーは、リーガルホールド中のファイルには適用できません。

高度な使用方法については、を参照してください ["NetApp SnapLock を使用して WORM ストレージに準拠"](#)。

#### EBR を使用して既存の WORM ファイルの保持期間を延長する

EBR は、既存の WORM ファイルの保持期間を延長する場合に便利です。たとえば、会社の方針として、従業員が源泉徴収の選択を変更した場合に、変更後 3 年間は従業員の W-4 レコードを変更不可能な状態で保管することが考えられます。別の会社の方針では、従業員が退職してから W-4 レコードを 5 年間保持する必要があります。

この場合は、保持期間を 5 年間に設定した EBR ポリシーを作成しておきます。従業員が退職した後（「イベント」）、EBR ポリシーを従業員の W-4 レコードに適用すると、保持期間が延長されます。これは、保持期間を手動で延長するよりも通常は簡単であり、関連するファイルが大量にある場合に特に便利です。

手順

1. EBR ポリシーを作成します。

```
snaplock event-retention policy create -vserver SVM_name -name policy_name  
-retention-period retention_period
```

次のコマンドは、EBRポリシーを作成します employee\_exit オン vs1 保持期間が10年の場合：



```
cluster1::>snaplock event-retention policy create -vserver vs1 -name  
employee_exit -retention-period 10years
```

2. EBR ポリシーを適用します。

```
snaplock event-retention apply -vserver SVM_name -name policy_name -volume  
volume_name -path path_name
```

次のコマンドはEBRポリシーを適用します employee\_exit オン vs1 ディレクトリ内のすべてのファイルに移動します d1 :

```
cluster1::>snaplock event-retention apply -vserver vs1 -name  
employee_exit -volume vol1 -path /d1
```

監査ログを作成します

ONTAP 9.9.1以前を使用している場合は、まずSnapLockアグリゲートを作成してから、privileged deleteまたはSnapLockボリュームの移動を実行する前にSnapLockで保護された監査ログを作成する必要があります。監査ログには、SnapLock 管理者アカウントの作成と削除、ログボリュームに対する変更、privileged delete が有効になっているかどうか、privileged delete 処理、および SnapLock ボリューム移動処理に関する情報が記録されます。

ONTAP 9.10.1以降では、SnapLockアグリゲートの作成は廃止されました。snaplock-typeオプションを使用して、"[SnapLockボリュームの明示的な作成](#)" SnapLockタイプとしてComplianceまたはEnterpriseを指定します。

作業を開始する前に

ONTAP 9.9.1以前を使用している場合は、クラスタ管理者でSnapLockアグリゲートを作成する必要があります。

このタスクについて

監査ログは、ログファイルの保持期間が経過するまで削除できません。保持期間が経過したあとも監査ログを変更することはできません。これは、SnapLock ComplianceモードとEnterpriseモードの両方に当てはまります。



ONTAP 9.4 以前では、監査ログに SnapLock Enterprise ボリュームを使用することはできません。SnapLock Compliance ボリュームを使用する必要があります。ONTAP 9.5 以降では、監査ログに SnapLock Enterprise ボリュームまたは SnapLock Compliance ボリュームのいずれかを使用できます。いずれの場合も、監査ログボリュームはジャンクションパスにマウントする必要があります /snaplock\_audit\_log。他のボリュームはこのジャンクションパスを使用できません。

SnapLock 監査ログにはあります /snaplock\_log 監査ログボリュームのルートの下サブディレクトリにあるディレクトリ privdel\_log (privileged delete処理) および system\_log (その他すべて)。監査ログのファイル名には最初に記録された処理のタイムスタンプが含まれているため、処理が実行されたおおよその時間から簡単にレコードを検索できます。

- 使用できます `snaplock log file show` コマンドを使用して、監査ログボリューム上のログファイルを表示します。
- 使用できます `snaplock log file archive` コマンドを使用して現在のログファイルをアーカイブし、新しいログファイルを作成します。これは、監査ログ情報を別のファイルに記録する必要がある場合に便利です。

詳細については、コマンドのマニュアルページを参照してください。



データ保護ボリュームは、SnapLock 監査ログボリュームとしては使用できません。

#### 手順

1. SnapLock アグリゲートを作成する。

[SnapLock アグリゲートを作成する](#)

2. 監査ログを設定する SVM に SnapLock ボリュームを作成します。

[SnapLock ボリュームを作成します](#)

3. SVM に監査ログを設定します。

```
snaplock log create -vserver SVM_name -volume snaplock_volume_name -max-log
-size size -retention-period default_retention_period
```



監査ログファイルのデフォルトの最小保持期間は 6 カ月です。該当するファイルの保持期間が監査ログの保持期間よりも長い場合は、そのファイルの保持期間が継承されます。したがって、`privileged delete` を使用して削除されたファイルの保持期間が 10 カ月で、監査ログの保持期間が 8 カ月の場合、ログの保持期間は 10 カ月に延長されます。保持期限およびデフォルトの保持期間の詳細については、[を参照してください "保持期限を設定"](#)。

次のコマンドは、を設定します SVM1 SnapLock ボリュームを使用した監査ログに使用します logVol。監査ログの最大サイズは 20GB、保持期間は 8 カ月です。

```
SVM1::> snaplock log create -vserver SVM1 -volume logVol -max-log-size
20GB -retention-period 8months
```

4. 監査ログを設定したSVMで、ジャンクションパスにSnapLock ボリュームをマウントします  
/snaplock\_audit\_log。

[SnapLock ボリュームをマウント](#)

#### SnapLock 設定を確認します

使用できます `volume file fingerprint start` および `volume file fingerprint dump` ファイルタイプ（通常、WORM、追記可能WORM）、ボリュームの有効期限など、ファイルとボリュームに関する重要な情報を表示するコマンド。

#### 手順

## 1. ファイルフィンガープリントを生成します。

**volume file fingerprint start -vserver *SVM\_name* -file *file\_path***

```
svm1::> volume file fingerprint start -vserver svm1 -file
/vol/slc/vol/f1
File fingerprint operation is queued. Run "volume file fingerprint show
-session-id 16842791" to view the fingerprint session status.
```

コマンドは、への入力として使用できるセッションIDを生成します volume file fingerprint dump  
コマンドを実行します



を使用できます volume file fingerprint show フィンガープリント処理の進捗状況を監視するためのセッションIDを指定したコマンド。フィンガープリントを表示する前に、処理が完了していることを確認してください。

## 2. ファイルのフィンガープリントを表示します。

**volume file fingerprint dump -session-id *session\_ID***

```
svm1::> volume file fingerprint dump -session-id 33619976
Vserver:svm1
Session-ID:33619976
Volume:slc_vol
Path:/vol/slc_vol/f1
Data
Fingerprint:MOFJVevxNSJm3C/4Bn5oEEYH51CrudOzZYK4r5Cfy1g=Metadata

Fingerprint:8iMjqJXiNcggXT5XuRhLiEwIrJEihDmwS0hrexnjgmc=Fingerprint
Algorithm:SHA256
Fingerprint Scope:data-and-metadata
Fingerprint Start Time:1460612586
Formatted Fingerprint Start Time:Thu Apr 14 05:43:06 GMT 2016
Fingerprint Version:3
**SnapLock License:available**
Vserver UUID:acf7ae64-00d6-11e6-a027-0050569c55ae
Volume MSID:2152884007
Volume DSID:1028
Hostname:my_host
Filer ID:5f18eda2-00b0-11e6-914e-6fb45e537b8d
Volume Containing Aggregate:slc_aggr1
Aggregate ID:c84634aa-c757-4b98-8f07-eeef32565f67
**SnapLock System ComplianceClock:1460610635
Formatted SnapLock System ComplianceClock:Thu Apr 14 05:10:35
GMT 2016
Volume SnapLock Type:compliance
```

```
Volume ComplianceClock:1460610635
Formatted Volume ComplianceClock:Thu Apr 14 05:10:35 GMT 2016
Volume Expiry Date:1465880998**
  Is Volume Expiry Date Wraparound:false
Formatted Volume Expiry Date:Tue Jun 14 05:09:58 GMT 2016
Filesystem ID:1028
File ID:96
File Type:worm
File Size:1048576
Creation Time:1460612515
Formatted Creation Time:Thu Apr 14 05:41:55 GMT 2016
Modification Time:1460612515
Formatted Modification Time:Thu Apr 14 05:41:55 GMT 2016
Changed Time:1460610598
Is Changed Time Wraparound:false
Formatted Changed Time:Thu Apr 14 05:09:58 GMT 2016
Retention Time:1465880998
Is Retention Time Wraparound:false
Formatted Retention Time:Tue Jun 14 05:09:58 GMT 2016
Access Time:-
Formatted Access Time:-
Owner ID:0
Group ID:0
Owner SID:-
Fingerprint End Time:1460612586
Formatted Fingerprint End Time:Thu Apr 14 05:43:06 GMT 2016
```

## WORMファイルを管理します

### WORMファイルを管理します

WORMファイルは、次の方法で管理できます。

- "ファイルを **WORM** 状態にコミット"
- "SnapshotコピーをバックアップデスティネーションのWORM状態にコミットします"
- "ディザスタリカバリ用にWORMファイルをミラーリング"
- "訴訟に備えてWORMファイルを保持"
- "WORMファイルを削除します"

ファイルを **WORM** 状態にコミット

手動で、または自動コミットによって、ファイルをWORM状態（Write Once、Read Many）にコミットできます。追記可能WORMファイルを作成することもできます。

## ファイルを手動で **WORM** 状態にコミット

ファイルを手動で WORM 状態にコミットするには、ファイルを読み取り専用にします。ファイルの読み書き属性は、NFS または CIFS で適切なコマンドやプログラムを使用して読み取り専用に変更できます。ファイルへの書き込みをアプリケーションで確実に終了してファイルが先にコミットされないようにする場合や、ボリューム数が多いために自動コミットスキャナで拡張の問題が発生している場合は、ファイルを手動でコミットすることを選択できます。

### 必要なもの

- コミットするファイルが SnapLock ボリュームに格納されている必要があります。
- ファイルが書き込み可能である必要があります。

### このタスクについて

ボリュームComplianceClock時間がに書き込まれます `ctime` コマンドまたはプログラムが実行されたときのファイルのフィールド。ComplianceClock 時間に基づいて、ファイルが保持期限に達する時点が特定されず。

### 手順

1. 適切なコマンドまたはプログラムを使用して、ファイルの読み書き属性を読み取り専用に変更します。

UNIXシェルで、次のコマンドを使用してという名前のファイルを作成します `document.txt` 読み取り専用：

```
chmod -w document.txt
```

Windowsシェルで、次のコマンドを使用してという名前のファイルを作成します `document.txt` 読み取り専用：

```
attrib +r document.txt
```

## ファイルを自動的に**WORM**状態にコミット

SnapLock の自動コミット機能を使用して、ファイルを WORM 状態に自動的にコミットできます。自動コミット期間中にファイルに変更がなかった場合、自動コミット機能によってSnapLockボリューム上でファイルがWORM状態にコミットされる期間。自動コミット機能はデフォルトでは無効になっています。

### 必要なもの

- 自動コミットするファイルが SnapLock ボリュームに格納されている必要があります。
- SnapLock ボリュームはオンラインである必要があります。
- SnapLock ボリュームが読み書き可能ボリュームである必要があります。



SnapLock の自動コミット機能は、ボリューム内のすべてのファイルをスキャンし、自動コミットの要件を満たすファイルをコミットします。ファイルが自動コミットできる状態になってから、SnapLock の自動コミットスキャナによって実際にコミットされるまでに、時間が空くことがあります。ただし、ファイルは自動コミットの対象になった時点からファイルシステムによる削除や変更から保護されます。

このタスクについて

`_autocommit_period_` は、ファイルが自動コミットされるまでに、ファイルに変更がないようにする期間を指定します。この期間が経過する前にファイルが変更された場合、自動コミット期間はもう一度最初からカウントされます。

自動コミット期間に指定できる値は次のとおりです。

価値	単位	注：
なし	-	デフォルト。
5-5256000	分	-
1-87600	時間	-
1~3650	日	-
1 ~ 120	月	-
1 ~ 10	年	-



最小値は 5 分、最大値は 10 年です。

手順

1. SnapLock ボリュームのファイルを WORM 状態に自動コミットします。

```
volume snaplock modify -vserver SVM_name -volume volume_name -autocommit  
-period autocommit_period
```

すべてのオプションの一覧については、コマンドのマニュアルページを参照してください。

次のコマンドは、ボリューム上のファイルを自動コミットします `vol1 SVM vs1` ので、ファイルに変更が 5 時間続いた場合は次のようになります。

```
cluster1::>volume snaplock modify -vserver vs1 -volume vol1 -autocommit  
-period 5hours
```

## 追記可能 **WORM** ファイルを作成します

追記可能 WORM ファイルには、ログエントリのように段階的に書き込まれるデータが格納されます。追記可能 WORM ファイルは、適切なコマンドやプログラムを使用して作成するか、SnapLock のボリュームアペンドモード機能を使用してデフォルトで作成できます。

### コマンドまたはプログラムを使用して、追記可能 **WORM** ファイルを作成します

追記可能 WORM ファイルは、NFS または CIFS で適切なコマンドやプログラムを使用して作成できます。追記可能 WORM ファイルには、ログエントリのように段階的に書き込まれるデータが格納されます。データは 256KB のチャンク単位でファイルに追加されます。チャンクが書き込まれるたびに、前のチャンクが WORM 方式で保護されます。このファイルは保持期間が経過するまで削除できません。

### 必要なもの

追記可能 WORM ファイルは SnapLock ボリュームに格納する必要があります。

### このタスクについて

データは、アクティブな 256KB のチャンクに順番に書き込まれる必要はありません。ファイルの  $n \times 256\text{KB} + 1$  バイトにデータが書き込まれると、1 つ前の 256KB セグメントが WORM 方式で保護されます。

### 手順

1. 適切なコマンドまたはプログラムを使用して、必要な保持期限を指定した空のファイルを作成します。

UNIX シェルで、次のコマンドを使用して、保持期限を 2020 年 11 月 21 日の午前 6 時に設定しますという名前のゼロ長ファイルの場合 `document.txt` :

```
touch -a -t 202011210600 document.txt
```

2. 適切なコマンドまたはプログラムを使用して、ファイルの読み書き属性を読み取り専用に変更します。

UNIX シェルで、次のコマンドを使用してという名前のファイルを作成します `document.txt` 読み取り専用 :

```
chmod 444 document.txt
```

3. 適切なコマンドまたはプログラムを使用して、ファイルの読み書き属性を書き込み可能に戻します。



ファイルにデータがないため、この手順はコンプライアンスリスクとはみなされません。

UNIX シェルで、次のコマンドを使用してという名前のファイルを作成します `document.txt` 書き込み可能 :

```
chmod 777 document.txt
```

4. 適切なコマンドまたはプログラムを使用して、ファイルへのデータの書き込みを開始します。

UNIXシェルで、次のコマンドを使用してにデータを書き込みます `document.txt` :

```
echo test data >> document.txt
```



ファイルにデータを追加する必要がなくなったら、ファイル権限を読み取り専用に戻してください。

ボリュームアPENDモードを使用して追記可能 **WORM** ファイルを作成します

ONTAP 9.3 以降では、SnapLock のボリュームアPENDモード（VAM）機能を使用して、追記可能 WORM ファイルをデフォルトで作成できます。追記可能 WORM ファイルには、ログエントリのように段階的に書き込まれるデータが格納されます。データは 256KB のチャンク単位でファイルに追加されます。チャンクが書き込まれるたびに、前のチャンクが WORM 方式で保護されます。このファイルは保持期間が経過するまで削除できません。

必要なもの

- 追記可能 WORM ファイルは SnapLock ボリュームに格納する必要があります。
- SnapLock ボリュームは、アンマウントされていて、Snapshot コピーやユーザが作成したファイルが含まれていない必要があります。

このタスクについて

データは、アクティブな 256KB のチャンクに順番に書き込まれる必要はありません。ファイルの  $n * 256KB + 1$  バイトにデータが書き込まれると、1 つ前の 256KB セグメントが WORM 方式で保護されます。

ボリュームに自動コミット期間を指定している場合、追記可能 WORM ファイルに変更がなかった期間が自動コミット期間を超えると、そのファイルは WORM 状態にコミットされます。



VAM は SnapLock 監査ログボリュームではサポートされません。

手順

1. VAMを有効にします。

```
volume snaplock modify -vserver SVM_name -volume volume_name -is-volume-append  
-mode-enabled true|false
```

すべてのオプションの一覧については、コマンドのマニュアルページを参照してください。

次のコマンドは、ボリュームでVAMを有効にします `vol1` SVM数`vs1` :

```
cluster1::>volume snaplock modify -vserver vs1 -volume vol1 -is-volume  
-append-mode-enabled true
```

2. 適切なコマンドまたはプログラムを使用して、書き込み権限を持つファイルを作成します。

ファイルはデフォルトで追記可能 WORM ファイルになります。



**Snapshot**コピーをバックアップデスティネーションの**WORM**状態にコミットします

SnapLock for SnapVault を使用して、セカンダリストレージ上の Snapshot コピーを WORM 方式で保護できます。SnapLockの基本タスクはすべてSnapVaultデスティネーションで実行します。デスティネーションボリュームは自動的に読み取り専用でマウントされるため、Snapshot コピーを WORM 状態に明示的にコミットする必要はありません。したがって、SnapMirror ポリシーを使用してデスティネーションボリュームにスケジューリングされた Snapshot コピーを作成することはできません。

作業を開始する前に

- ソースクラスタで ONTAP 8.2.2 以降が実行されている必要があります。
- ソースアグリゲートとデスティネーションアグリゲートはどちらも 64 ビットである必要があります。
- ソースボリュームを SnapLock ボリュームにすることはできません。
- ピア SVM を含むピアクラスタにソースボリュームとデスティネーションボリュームを作成する必要があります。

詳細については、を参照してください ["クラスタピアリング"](#)。

- ボリュームの自動拡張が無効になっている場合は、デスティネーションボリュームに、ソースボリュームで使用されているスペースよりも少なくとも 5% 多い空きスペースが必要です。

このタスクについて

ソースボリュームで使用するストレージは、ネットアップのストレージでもネットアップ以外のストレージでもかまいません。ネットアップ以外のストレージの場合は、FlexArray 仮想化を使用する必要があります。



WORM 状態にコミットされた Snapshot コピーの名前は変更できません。

SnapLock ボリュームはクローニングできますが、SnapLock ボリューム上のファイルはクローニングできません。



SnapLockボリュームではLUNはサポートされません。SnapLockでは、SnapLock以外のボリュームで作成されたSnapshotコピーをSnapLockバックアップ関係の一部として保護するためにSnapLockに転送する場合にのみ、LUNがサポートされます。読み取り/書き込みSnapLockボリュームではLUNはサポートされません。ただし、Snapshotコピーの改ざんは、SnapMirrorのソースボリュームと、LUNを含むデスティネーションボリュームの両方でサポートされます。

ONTAP 9.14.1以降では、SnapMirror関係のSnapMirrorポリシーに特定のSnapMirrorラベルの保持期間を指定できます。これにより、ソースボリュームからデスティネーションボリュームにレプリケートされたSnapshotコピーが、ルールで指定された保持期間に保持されます。保持期間を指定しない場合は、デスティネーションボリュームのデフォルトの保持期間が使用されます。

ONTAP 9.13.1以降では、ロックされたSnapshotコピーをSnapLockバックアップ関係のデスティネーションSnapLockボリュームに瞬時にリストアできます。これには、`snaplock-type` オプションを「non-snaplock」に設定し、ボリュームクローン作成処理の実行時に「parent-snapshot」としてSnapshotコピーを指定します。の詳細を確認してください ["SnapLock タイプのFlexCloneボリュームを作成します"](#)。

MetroCluster 構成の場合は、次の点に注意してください。

- SnapVault 関係は、同期元の SVM 間でのみ作成できます。同期元の SVM と同期先の SVM の間では作成できません。
- 同期元の SVM のボリュームからデータ提供用の SVM への SnapVault 関係を作成できます。
- データ提供用の SVM のボリュームから同期元の SVM の DP ボリュームへの SnapVault 関係を作成できます。

次の図は、SnapLockバックアップ関係を初期化するための手順を示しています。

#### 手順

1. デスティネーションクラスタを特定します。
2. デスティネーションクラスタで、["SnapLockライセンスをインストールする"](#)、["コンプライアンスクロックの初期化"](#) また、9.10.1より前のONTAPリリースを使用している場合は、["SnapLockアグリゲートを作成する"](#)。
3. デスティネーションクラスタで、タイプがのSnapLock デスティネーションボリュームを作成します DP ソースボリュームと同じかそれ以上のサイズが指定されています。

```
volume create -vserver SVM_name -volume volume_name -aggregate aggregate_name
-snaplock-type compliance|enterprise -type DP -size size
```



ONTAP 9.10.1 以降では、SnapLock ボリュームと非 SnapLock ボリュームを同じアグリゲート上に配置できるため、ONTAP 9.10.1 を使用している場合に別の SnapLock アグリゲートを作成する必要がなくなりました。ComplianceまたはEnterprise SnapLock のボリュームタイプを指定するには、volume-snaplock-typeオプションを使用します。ONTAP 9.10.1 より前のONTAP リリースでは、SnapLock モードのComplianceモードまたはEnterpriseモードがアグリゲートから継承されます。バージョンに依存しないデスティネーションボリュームはサポートされません。デスティネーションボリュームの言語設定とソースボリュームの言語設定が一致している必要があります。

次のコマンドは、2GBのSnapLock を作成します Compliance という名前のボリューム dstvolB インチ SVM2 アグリゲート node01\_aggr :

```
cluster2::> volume create -vserver SVM2 -volume dstvolB -aggregate
node01_aggr -snaplock-type compliance -type DP -size 2GB
```

4. デスティネーションクラスタで、デフォルトの保持期間を設定します。手順については、[を参照してください デフォルトの保持期間を設定](#)。



バックアップデスティネーションである SnapLock には、デフォルトの保持期間が割り当てられます。この期間の値は、SnapLock Enterprise ボリュームの場合は最初に 0 年以上、SnapLock Compliance ボリュームの場合は 30 年以下に設定されます。各 NetApp Snapshot コピーは、最初にこのデフォルトの保持期間でコミットされます。保持期間は、必要に応じてあとから延長できます。詳細については、[を参照してください 保持期限の設定の概要を確認します](#)。

5. [新しいレプリケーション関係を作成](#) SnapLock 以外のソースと、手順 3 で作成した新しい SnapLock デスティネーションの間。

この例は、デスティネーションSnapLock ボリュームとの新しいSnapMirror関係を作成します dstvolB ポリシーを使用します XDPDefault dailyおよびweeklyのラベルが付いたSnapshotコピーを毎時スケジュールに基づいてバックアップするには、

```
cluster2::> snapmirror create -source-path SVM1:srcvolA -destination  
-path SVM2:dstvolB -vserver SVM2 -policy XDPDefault -schedule hourly
```



カスタムレプリケーションポリシーを作成する または カスタムスケジュール 使用可能なデフォルト設定が適切でない場合。

6. デスティネーション SVM で、手順 5 で作成した SnapVault 関係を初期化します。

**snapmirror initialize -destination-path destination\_path**

次のコマンドは、ソースボリューム間の関係を初期化します srcvolA オン SVM1 デスティネーションボリュームを指定します dstvolB オン SVM2：

```
cluster2::> snapmirror initialize -destination-path SVM2:dstvolB
```

7. 関係が初期化され、アイドル状態になったら、を使用します snapshot show デスティネーションでコマンドを実行して、レプリケートされたSnapshotコピーに適用されているSnapLock の有効期限を確認します。

次の例は、ボリューム上のSnapshotコピーを表示します dstvolB SnapMirrorラベルとSnapLock の有効期限が設定されているデータセンターを次に示します。

```
cluster2::> snapshot show -vserver SVM2 -volume dstvolB -fields  
snapmirror-label, snaplock-expiry-time
```

## 関連情報

["クラスタと SVM のピアリング"](#)

["SnapVault を使用したボリュームのバックアップ"](#)

ディザスタリカバリ用に**WORM**ファイルをミラーリング

SnapMirror を使用すると、ディザスタリカバリなどの目的で、地理的に離れた別の場所に WORM ファイルをレプリケートできます。ソースボリュームとデスティネーションボリュームの両方が SnapLock 用に設定されていて、両方のボリュームの SnapLock モードが Compliance または Enterprise である必要があります。ボリュームとファイルの主要な SnapLock プロパティがすべてレプリケートされます。

## 前提条件

ピア SVM を含むピアクラスタにソースボリュームとデスティネーションボリュームを作成する必要があります。詳細については、を参照してください ["クラスタと SVM のピアリング"](#)。

## このタスクについて

- ONTAP 9.5 以降では、WORM ファイルのレプリケーションに DP（データ保護）タイプの関係ではなく XDP（拡張データ保護）タイプの SnapMirror 関係を使用できます。XDP モードは ONTAP のバージョンに依存せず、同じブロックに格納されたファイルを区別できるため、レプリケートされた Compliance モードのボリュームの再同期が大幅に簡単になります。既存の DP タイプの関係を XDP タイプの関係に変換する方法については、を参照してください ["データ保護"](#)。
- Compliance モードのボリュームで DP タイプの SnapMirror 関係を再同期する場合、再同期によってデータが失われると SnapLock で判断されると処理は失敗します。再同期処理が失敗した場合は、を使用できます `volume clone create` デスティネーションボリュームのクローンを作成するコマンド。その後、ソースボリュームをクローンと再同期できます。
- SnapLock 対応ボリューム間の XDP タイプの SnapMirror 関係では、関係解除後にデスティネーションのデータがソースから変化していても再同期がサポートされます。

再同期時に共通の Snapshot に基づいてソースとデスティネーションの間でデータの相違が検出されると、この相違をキャプチャするためにデスティネーションで新しい Snapshot が作成されます。新しい Snapshot と共通の Snapshot の両方が次の期間ロックされます。

- デスティネーションのボリューム有効期限
- ボリューム有効期限が過ぎているか設定されていない場合、Snapshot は 30 日間ロックされます
- デスティネーションにリーガルホールドが設定されている場合、実際のボリューム有効期限はマスクされ、「無期限」と表示されますが、Snapshot は実際のボリューム有効期限までロックされます。

デスティネーションボリュームの有効期限がソースよりもあとの場合、デスティネーションの有効期限が維持され、再同期後にソースボリュームの有効期限で上書きされることはありません。

デスティネーションにソースと異なるリーガルホールドが設定されている場合は、再同期を実行できません。再同期を試行する前に、ソースとデスティネーションに同じリーガルホールドを設定するか、またはデスティネーションのリーガルホールドをすべて解除する必要があります。

変更されたデータをキャプチャするためにデスティネーションボリュームで作成され、ロックされた Snapshot コピーは、の CLI を使用してソースにコピーできます `snapmirror update -s snapshot` コマンドを実行します コピーした Snapshot はソースでもロックされたままです。


- SVM データ保護関係はサポートされません。
- 負荷共有データ保護関係はサポートされません。

次の図は、SnapMirror 関係を初期化するための手順を示しています。

## System Manager の略

ONTAP 9.12.1以降では、System Managerを使用してWORMファイルのSnapMirrorレプリケーションを設定できます。

### 手順

1. [ストレージ]>[ボリューム]に移動します。
2. 表示/非表示\*をクリックし、SnapLock タイプ\*を選択して、\*ボリューム\*ウィンドウに列を表示します。
3. SnapLock ボリュームを見つけます。
4. をクリックします  をクリックし、\* Protect \*を選択します。
5. デスティネーションクラスタとデスティネーションStorage VMを選択してください。
6. [\* その他のオプション\*] をクリックします。
7. [Show legacy policies\*]を選択し、[DPDefault (legacy)]を選択します。
8. 「接続先設定の詳細」セクションで「転送スケジュールの上書き」を選択し、「\*時間単位」を選択します。
9. [保存 (Save) ] をクリックします。
10. ソースボリューム名の左側にある矢印をクリックしてボリュームの詳細を展開し、ページの右側でリモートSnapMirror保護の詳細を確認します。
11. リモートクラスタで、「保護関係」に移動します。
12. 関係を探し、デスティネーションボリューム名をクリックして関係の詳細を確認します。
13. デスティネーションボリュームのSnapLock タイプおよびその他のSnapLock 情報を確認します。

### CLI の使用

1. デスティネーションクラスタを特定します。
2. デスティネーションクラスタで、["SnapLockライセンスをインストールする"](#)、["コンプライアンスロックの初期化"](#)また、9.10.1より前のONTAPリリースを使用している場合は、["SnapLockアグリゲートを作成する"](#)。
3. デスティネーションクラスタで、タイプがのSnapLock デスティネーションボリュームを作成します  
DP ソースボリュームと同じかそれ以上のサイズが指定されている必要があります。

```
volume create -vserver SVM_name -volume volume_name -aggregate  
aggregate_name -snaplock-type compliance|enterprise -type DP -size size
```



ONTAP 9.10.1 以降では、SnapLock ボリュームと非 SnapLock ボリュームを同じアグリゲート上に配置できるため、ONTAP 9.10.1 を使用している場合に別の SnapLock アグリゲートを作成する必要がなくなりました。ComplianceまたはEnterprise SnapLock のボリュームタイプを指定するには、volume-snaplock-type オプションを使用します。ONTAP 9.10.1より前のONTAP リリースでは、SnapLock モード（ComplianceモードまたはEnterpriseモード）がアグリゲートから継承されます。バージョンに依存しないデスティネーションボリュームはサポートされません。デスティネーションボリュームの言語設定とソースボリュームの言語設定が一致している必要があります。

次のコマンドは、2GBのSnapLock を作成します Compliance という名前のボリューム dstvolB インチ SVM2 アグリゲート node01\_aggr :

```
cluster2::> volume create -vserver SVM2 -volume dstvolB -aggregate  
node01_aggr -snaplock-type compliance -type DP -size 2GB
```

4. デスティネーション SVM で、SnapMirror ポリシーを作成します。

```
snapmirror policy create -vserver SVM_name -policy policy_name
```

次のコマンドは、SVM全体のポリシーを作成します SVM1-mirror :

```
SVM2::> snapmirror policy create -vserver SVM2 -policy SVM1-mirror
```

5. デスティネーション SVM で、SnapMirror スケジュールを作成します。

```
job schedule cron create -name schedule_name -dayofweek day_of_week -hour  
hour -minute minute
```

次のコマンドは、という名前のSnapMirrorスケジュールを作成します weekendcron :

```
SVM2::> job schedule cron create -name weekendcron -dayofweek  
"Saturday, Sunday" -hour 3 -minute 0
```

6. デスティネーション SVM で、SnapMirror 関係を作成します。

```
snapmirror create -source-path source_path -destination-path  
destination_path -type XDP|DP -policy policy_name -schedule schedule_name
```

次のコマンドでは、ソースボリューム間にSnapMirror関係を作成します srcvolA オン SVM1 デスティネーションボリュームを指定します dstvolB オン SVM2`をクリックし、ポリシーを割り当てます `SVM1-mirror スケジュールも weekendcron :

```
SVM2::> snapmirror create -source-path SVM1:srcvolA -destination  
-path SVM2:dstvolB -type XDP -policy SVM1-mirror -schedule  
weekendcron
```



XDP タイプは ONTAP 9.5 以降で使用できます。ONTAP 9.4 以前では DP タイプを使用する必要があります。

7. デスティネーション SVM で、SnapMirror 関係を初期化します。

```
snapmirror initialize -destination-path destination_path
```

初期化プロセスでは、デスティネーションボリュームへの `_ベースライン転送_` が実行されま



す。SnapMirror はソースボリュームの Snapshot コピーを作成して、そのコピーおよびコピーが参照するすべてのデータブロックをデスティネーションボリュームに転送します。また、ソースボリューム上の他の Snapshot コピーもすべてデスティネーションボリュームに転送します。

次のコマンドは、ソースボリューム間の関係を初期化します srcvolA オン SVM1 デスティネーションボリュームを指定します dstvolB オン SVM2 :

```
SVM2::> snapmirror initialize -destination-path SVM2:dstvolB
```

## 関連情報

["クラスタと SVM のピアリング"](#)

["ボリュームのディザスタリカバリの準備"](#)

["データ保護"](#)

リーガルホールドを使用して訴訟の際に**WORM**ファイルを保持する

ONTAP 9.3以降では、`_Legal Hold_feature`を使用して、ComplianceモードのWORMファイルを訴訟の期間にわたって保持できます。

## 必要なもの

- このタスクを実行するには、SnapLock 管理者である必要があります。

["SnapLock 管理者アカウントを作成します"](#)

- セキュアな接続（SSH、コンソール、または ZAPI）でログインする必要があります。

## このタスクについて

リーガルホールド中のファイルは、保持期間の制限がない WORM ファイルのように機能します。リーガルホールドの期間をいつ終了するかは、お客様の責任で指定してください。

リーガルホールドとして保存できるファイル数は、ボリュームの使用可能なスペースによって異なります。

## 手順

- リーガルホールドを開始します。

```
snaplock legal-hold begin -litigation-name litigation_name -volume volume_name -path path_name
```

次のコマンドは、のすべてのファイルに対してリーガルホールドを開始します vol1 :

```
cluster1::>snaplock legal-hold begin -litigation-name litigation1 -volume vol1 -path /
```

- リーガルホールドを終了します。

```
snaplock legal-hold end -litigation-name litigation_name -volume volume_name
-path path_name
```

次のコマンドは、のすべてのファイルのリーガルホールドを終了します vol1：

```
cluster1::>snaplock legal-hold end -litigation-name litigation1 -volume
vol1 -path /
```

## WORMファイルの削除の概要

privileged delete機能を使用して、保持期間中にEnterpriseモードのWORMファイルを削除できます。

この機能を使用する前に、SnapLock 管理者アカウントを作成し、そのアカウントを使用して機能を有効にする必要があります。

### SnapLock 管理者アカウントを作成します

privileged delete を実行するには、SnapLock 管理者の権限が必要です。これらの権限は vsadmin-snaplock ロールで定義されています。このロールが割り当てられていない場合は、クラスタ管理者に依頼して、SnapLock 管理者ロールを持つ SVM 管理者アカウントを作成してもらいます。

### 必要なもの

- このタスクを実行するには、クラスタ管理者である必要があります。
- セキュアな接続（SSH、コンソール、または ZAPI）でログインする必要があります。

### 手順

1. SnapLock 管理者ロールを持つ SVM 管理者アカウントを作成します。

```
security login create -vserver SVM_name -user-or-group-name user_or_group_name
-application application -authmethod authentication_method -role role -comment
comment
```

次のコマンドは、SVM管理者アカウントを有効にします SnapLockAdmin を使用します vsadmin-snaplock アクセスするロール SVM1 パスワードの使用：

```
cluster1::> security login create -vserver SVM1 -user-or-group-name
SnapLockAdmin -application ssh -authmethod password -role vsadmin-
snaplock
```

### privileged delete 機能を有効にします

privileged delete 機能は、削除する WORM ファイルが格納されている Enterprise ボリュームに対して明示的に有効にする必要があります。

### このタスクについて



の値 `-privileged-delete` オプションでは、privileged deleteを有効にするかどうかを指定指定できる値は `enabled`、`disabled` および `permanently-disabled`。



`permanently-disabled` は、終了状態です。ボリュームで状態をに設定したあとにprivileged deleteを有効にすることはできません `permanently-disabled`。

## 手順

1. SnapLock Enterprise ボリュームに対して privileged delete を有効にします。

```
volume snaplock modify -vserver SVM_name -volume volume_name -privileged  
-delete disabled|enabled|permanently-disabled
```

次のコマンドは、Enterpriseボリュームに対してprivileged delete機能を有効にします dataVol オン SVM1  
:

```
SVM1::> volume snaplock modify -vserver SVM1 -volume dataVol -privileged  
-delete enabled
```

## EnterpriseモードのWORMファイルを削除します

privileged delete 機能を使用して、保持期間中に Enterprise モードの WORM ファイルを削除できます。

### 必要なもの

- このタスクを実行するには、SnapLock 管理者である必要があります。
- Enterprise ボリュームで、SnapLock 監査ログを作成し、privileged delete 機能を有効にしておく必要があります。

### このタスクについて

privileged delete 処理を使用して、期限切れの WORM ファイルを削除することはできません。を使用できます volume file retention show コマンドを使用して、削除するWORMファイルの保持期限を表示します。詳細については、コマンドのマニュアルページを参照してください。

### ステップ

1. Enterprise ボリュームの WORM ファイルを削除します。

```
volume file privileged-delete -vserver SVM_name -file file_path
```

次のコマンドは、ファイルを削除します /vol/dataVol/f1 指定しますSVM1 :

```
SVM1::> volume file privileged-delete -file /vol/dataVol/f1
```

## SnapLock ボリュームを移動

ONTAP 9.8 以降では、SnapLock ボリュームを同じタイプのデスティネーションアグリゲート（Enterprise から Enterprise へ、または Compliance to Compliance）に移動できます。SnapLock を移動するには、SnapLock セキュリティロールが割り当てられている必要があります。

### SnapLock セキュリティ管理者アカウントを作成します

SnapLock の移動を実行するには、SnapLock セキュリティ管理者の権限が必要です。この権限は、ONTAP 9.8 で導入された `_SnapLock_` ロールで付与されます。このロールが割り当てられていない場合は、クラスタ管理者に、この SnapLock セキュリティロールを持つ SnapLock セキュリティユーザの作成を依頼してください。

#### 必要なもの

- このタスクを実行するには、クラスタ管理者である必要があります。
- セキュアな接続（SSH、コンソール、または ZAPI）でログインする必要があります。

#### このタスクについて

SnapLock ロールは、データ SVM に関連付けられる `vsadmin-snaplock` ロールとは異なり、管理 SVM に関連付けられています。

#### ステップ

1. SnapLock 管理者ロールを持つ SVM 管理者アカウントを作成します。

```
security login create -vserver SVM_name -user-or-group-name user_or_group_name  
-application application -authmethod authentication_method -role role -comment  
comment
```

次のコマンドは、SVM管理者アカウントを有効にします SnapLockAdmin を使用します snaplock 管理SVMにアクセスするためのロール cluster1 パスワードの使用：

```
cluster1::> security login create -vserver cluster1 -user-or-group-name  
SnapLockAdmin -application ssh -authmethod password -role snaplock
```

## SnapLock ボリュームを移動

使用できます `volume move` SnapLock ボリュームをデスティネーションアグリゲートに移動するコマンド。

#### 必要なもの

- SnapLock ボリュームの移動を実行する前に、SnapLock で保護された監査ログを作成しておく必要があります。

"監査ログを作成します"。

- ONTAP 9.10.1 より前のバージョンの ONTAP を使用している場合は、デスティネーションアグリゲートの SnapLock タイプが、Compliance から Compliance へ、または Enterprise から Enterprise への移動対

象の SnapLock ボリュームと同じである必要があります。ONTAP 9.10.1 以降ではこの制限が解除され、Compliance SnapLock と Enterprise の両方のボリューム、および SnapLock 以外のボリュームをアグリゲートに含めることができます。

- SnapLock セキュリティロールを持つユーザである必要があります。

#### 手順

1. セキュアな接続を使用して、ONTAP クラスタ管理 LIF にログインします。

```
ssh snaplock_user@cluster_mgmt_ip
```

2. SnapLock ボリュームを移動します。

```
volume move start -vserver SVM_name -volume SnapLock_volume_name -destination  
-aggregate destination_aggregate_name
```

3. ボリューム移動処理のステータスを確認します。

```
volume move show -volume SnapLock_volume_name -vserver SVM_name -fields  
volume,phase,vserver
```

## Snapshotコピーをロックしてランサムウェア攻撃から保護する

ONTAP 9.12.1以降では、SnapLock以外のボリューム上のSnapshotコピーをロックして、ランサムウェア攻撃から保護できます。Snapshotコピーをロックすることで、誤って削除したり、悪意を持って削除したりすることがなくなります。

SnapLock コンプライアンスクロック機能を使用すると、指定した期間Snapshotコピーをロックして、有効期限に達するまでSnapshotコピーを削除できないようにすることができます。Snapshotコピーをロックすると、改ざんを防止し、ランサムウェアの脅威から保護します。ロックされたSnapshotコピーを使用すると、ボリュームがランサムウェア攻撃によって危険にさらされた場合にデータをリカバリできます。

ONTAP 9.14.1以降では、Snapshotコピーロックによって、SnapLockヴォールトデスティネーションおよびSnapLock以外のSnapMirrorデスティネーションボリュームでのSnapshotコピーの長期保持がサポートされます。Snapshotコピーロックを有効にするには、Snapshotコピーに関連付けられたSnapMirrorポリシールールを使用して保持期間を設定します。 [既存のポリシーラベル](#)。このルールは、ボリュームに設定されているデフォルトの保持期間よりも優先されます。SnapMirrorラベルに保持期間が関連付けられていない場合は、ボリュームのデフォルトの保持期間が使用されます。

#### 改ざん防止機能を備えたSnapshotコピーの要件と考慮事項

- ONTAP CLIを使用している場合は、クラスタ内のすべてのノードでONTAP 9.12.1以降が実行されている必要があります。System Managerを使用している場合は、すべてのノードでONTAP 9.13.1以降が実行されている必要があります。
- ["SnapLockライセンスがクラスタにインストールされている必要があります。"](#)。このライセンスは、["ONTAP One"](#)。
- ["クラスタのコンプライアンスクロックを初期化する必要があります。"](#)。
- ボリュームでSnapshotロックが有効になっている場合、クラスタをONTAP 9.12.1以降のバージョンのONTAP にアップグレードできます。ただし、ロックされたすべてのSnapshotコピーが有効期限に達して削除され、Snapshotコピーのロックが無効になるまで、以前のバージョンのONTAP にはリバートできません。

- Snapshotがロックされている場合、ボリューム有効期限はSnapshotコピーの有効期限に設定されます。複数のSnapshotコピーがロックされている場合、ボリュームの有効期限には、すべてのSnapshotコピーの中で最も長い有効期限が反映されます。
- ロックされたSnapshotコピーの保持期間はSnapshotコピーの保持数よりも優先されます。つまり、ロックされたSnapshotコピーの保持期間が期限切れになっていない場合、保持数の制限は考慮されません。
- SnapMirror関係では、mirror-vaultポリシールールに保持期間を設定できます。デスティネーションボリュームでSnapshotコピーロックが有効になっている場合は、デスティネーションにレプリケートされるSnapshotコピーに保持期間が適用されます。保持期間は保持数よりも優先されます。たとえば、保持数を超えた場合でも、保持期限を過ぎていないSnapshotコピーは保持されます。
- SnapLock以外のボリューム上のSnapshotコピーの名前は変更できます。SnapMirror関係のプライマリボリュームでのSnapshotの名前変更処理は、ポリシーがMirrorAllSnapshotsの場合にのみセカンダリボリュームに反映されます。他のタイプのポリシーでは、名前を変更したSnapshotコピーは更新時に反映されません。
- ONTAP CLIを使用している場合は、を使用してロックされたSnapshotコピーをリストアできます `volume snapshot restore` ロックされたSnapshotコピーが最新のものである場合のみ、コマンドを実行できます。リストア対象のSnapshotコピーよりもあとに期限切れ前のSnapshotコピーがあると、Snapshotコピーのリストア処理は失敗します。

#### タンパープルーフSnapshotコピーでサポートされる機能

- FlexGroup ボリューム

FlexGroup ボリュームでは、Snapshotコピーのロックがサポートされます。Snapshotロックは、ルートコンスティチュエントSnapshotコピーでのみ発生します。FlexGroup ボリュームを削除できるのは、ルートコンスティチュエントの有効期限を過ぎた場合のみです。

- FlexVol からFlexGroup への変換

ロックされたSnapshotコピーがあるFlexVol をFlexGroup ボリュームに変換できます。変換後もSnapshotコピーはロックされたままです。

- ボリュームクローンとファイルクローン

ロックされたSnapshotコピーからボリュームのクローンとファイルのクローンを作成できます。

#### サポートされない機能です

現在、タンパープルーフSnapshotコピーでは、次の機能はサポートされていません。

- Cloud Volumes ONTAP
- 整合グループ
- FabricPool
- FlexCache ボリューム
- SMTapeの場合
- SnapMirror のビジネス継続性（SM-BC）
- を使用したSnapMirrorポリシールール `-schedule` パラメータ
- SnapMirror Synchronous
- SVMデータの移動（ソースクラスタからデスティネーションクラスタにSVMを移行または再配置する場合

に使用)

ボリュームの作成時に**Snapshot**コピーのロックを有効にします

ONTAP 9.12.1以降では、新しいボリュームを作成する場合、またはを使用して既存のボリュームを変更する場合に、Snapshotコピーロックを有効にできます `-snapshot-locking-enabled` オプションを指定します `volume create` および `volume modify` コマンドを使用します。ONTAP 9.13.1以降では、System Managerを使用してSnapshotコピーロックを有効にできます。

#### System Manager の略

1. [ストレージ]>[ボリューム]に移動し、[追加]\*を選択します。
2. ウィンドウで、[その他のオプション]\*を選択します。
3. ボリューム名、サイズ、エクスポートポリシー、および共有名を入力します。
4. [Enable Snapshot locking]\*を選択します。SnapLockライセンスがインストールされていない場合、この選択は表示されません。
5. SnapLockコンプライアンスクロックがまだ有効になっていない場合は、\*[Initialize Compliance Clock]\*を選択します。
6. 変更を保存します。
7. ウィンドウで、更新したボリュームを選択し、[概要]\*を選択します。
8. SnapLock Snapshotコピーのロック\*が「有効」\*と表示されていることを確認します。

#### CLI の使用

1. 新しいボリュームを作成し、Snapshotコピーロックを有効にするには、次のコマンドを入力します。

```
volume create -vserver vs1 -volume vol1 -snapshot-locking-enabled true
```


次のコマンドは、vol1という名前の新しいボリュームでSnapshotコピーロックを有効にします。

```
> volume create -volume vol1 -aggregate aggr1 -size 100m -snapshot-locking-enabled true
Warning: Snapshot copy locking is being enabled on volume "vol1" in Vserver "vs1". It cannot be disabled until all locked Snapshot copies are past their expiry time. A volume with unexpired locked Snapshot copies cannot be deleted.
Do you want to continue: {yes|no}: y
[Job 32] Job succeeded: Successful
```

既存のボリュームで**Snapshot**コピーロックを有効にします

ONTAP 9.12.1以降では、ONTAP CLIを使用して、既存のボリュームでSnapshotコピーロックを有効にできます。ONTAP 9.13.1以降では、System Managerを使用して既存のボリュームに対してSnapshotコピーロックを有効にすることができます。

## System Manager の略

1. [ストレージ]>[ボリューム]に移動します。
2. 選択するオプション  編集>ボリューム\*を選択します。
3. ウィンドウで、**[Snapshotコピー（ローカル）設定]**セクションを探し、**[Snapshotロックの有効化]\***を選択します。

SnapLockライセンスがインストールされていない場合、この選択は表示されません。

4. SnapLockコンプライアンスクロックがまだ有効になっていない場合は、\*[Initialize Compliance Clock]\*を選択します。
5. 変更を保存します。
6. ウィンドウで、更新したボリュームを選択し、[概要]\*を選択します。
7. SnapLock Snapshotコピーのロック\*が「有効」\*と表示されていることを確認します。

## CLI の使用

1. 既存のボリュームを変更してSnapshotコピーのロックを有効にするには、次のコマンドを入力します。

```
volume modify -vserver vservice_name -volume volume_name -snapshot-locking
-enabled true
```

ロックされた**Snapshot**コピーポリシーを作成し、保持を適用します

ONTAP 9.12.1以降では、Snapshotコピーポリシーを作成してSnapshotコピーの保持期間を適用し、そのポリシーをボリュームに適用して、指定した期間Snapshotコピーをロックできます。保持期間を手動で設定して、Snapshotコピーをロックすることもできます。ONTAP 9.13.1以降では、System Managerを使用してSnapshotコピーロックポリシーを作成し、ボリュームに適用できます。

**Snapshot**コピーのロックポリシーを作成します

## System Manager の略

1. [ストレージ]>[Storage VM]\*に移動し、Storage VMを選択します。
2. [設定]\*を選択します。
3. [Snapshot Policies]\*に移動し、を選択します →。
4. [ Snapshotポリシーの追加]\*ウィンドウで、ポリシー名を入力します。
5. 選択するオプション **+ Add**。
6. スケジュール名、保持するSnapshotコピーの最大数、SnapLock の保持期間など、Snapshotコピースケジュールの詳細を指定します。
7. [Snapshot保持期間]列にSnapLock 、Snapshotコピーを保持する時間数、日数、月数、または年数を入力します。たとえば、保持期間が5日間のSnapshotコピーポリシーでは、Snapshotコピーが作成されてから5日間はロックされ、その間は削除できません。サポートされる保持期間は次のとおりです。
  - 年：0～100
  - 月：0～1200
  - 日数：0～36500
  - 時間：0～24
8. 変更を保存します。

## CLI の使用

1. Snapshotコピーポリシーを作成するには、次のコマンドを入力します。

```
volume snapshot policy create -policy policy_name -enabled true -schedule1  
schedule1_name -count1 maximum_Snapshot_copies -retention-period1  
_retention_period
```


次のコマンドは、Snapshotコピーロックポリシーを作成します。

```
cluster1> volume snapshot policy create -policy policy_name -enabled  
true -schedule1 hourly -count1 24 -retention-period1 "1 days"
```

アクティブな保持期間にあるSnapshotコピーは置き換えられません。つまり、期限切れになっていないロックされたSnapshotコピーがある場合、保持数は反映されません。

ボリュームにロックポリシーを適用します

### System Manager の略

1. [ストレージ]>[ボリューム]に移動します。
2. 選択するオプション  編集>ボリューム\*を選択します。
3. ウィンドウで、[Snapshotコピーのスケジュール設定]\*を選択します。
4. リストからSnapshotコピーロックポリシーを選択します。
5. Snapshotコピーのロックがまだ有効になっていない場合は、\*[Snapshotロックを有効にする]\*を選択します。
6. 変更を保存します。

### CLI の使用

1. 既存のボリュームにSnapshotコピーロックポリシーを適用するには、次のコマンドを入力します。

```
volume modify -volume volume_name -vserver vservers_name -snapshot-policy policy_name
```

手動での**Snapshot**コピーの作成時に保持期間を適用

Snapshotコピーの保持期間は、Snapshotコピーを手動で作成するときに適用できます。ボリュームでSnapshotコピーロックが有効になっている必要があります。有効になっていない場合、保持期間の設定は無視されます。



## System Manager の略

1. [ストレージ]>[ボリューム]\*に移動し、ボリュームを選択します。
2. ボリュームの詳細ページで、\*[Snapshotコピー]\*タブを選択します。
3. 選択するオプション **+ Add**。
4. Snapshotコピー名とSnapLockの有効期限を入力します。カレンダーを選択して、保持期限の日付と時刻を選択できます。
5. 変更を保存します。
6. [ボリューム]>[Snapshotコピー]ページで、[表示/非表示]\*を選択し、[ SnapLock 有効期限]を選択して[ SnapLock 有効期限]\*列を表示し、保持期限が設定されていることを確認します。

## CLI の使用

1. Snapshotコピーを手動で作成し、ロック保持期間を適用するには、次のコマンドを入力します。

```
volume snapshot create -volume volume_name -snapshot snapshot_copy_name  
-snaplock-expiry-time expiration_date_time
```

次のコマンドでは、新しいSnapshotコピーを作成して保持期間を設定します。

```
cluster1> volume snapshot create -vserver vs1 -volume vol1 -snapshot  
snap1 -snaplock-expiry-time "11/10/2022 09:00:00"
```

既存の**Snapshot**コピーに保持期間を適用します

## System Manager の略

1. [ストレージ]>[ボリューム]\*に移動し、ボリュームを選択します。
2. ボリュームの詳細ページで、\*[Snapshotコピー]\*タブを選択します。
3. Snapshotコピーを選択し、を選択します。 をクリックし、\*[Modify SnapLock Expiration Time]\*を選択します。カレンダーを選択して、保持期限の日付と時刻を選択できます。
4. 変更を保存します。
5. [ボリューム]>[Snapshotコピー]ページで、[表示/非表示]\*を選択し、[ SnapLock 有効期限]を選択して[ SnapLock 有効期限]\*列を表示し、保持期限が設定されていることを確認します。

## CLI の使用

1. 既存のSnapshotコピーに保持期間を手動で適用するには、次のコマンドを入力します。

```
volume snapshot modify-snaplock-expiry-time -volume volume_name -snapshot snapshot_copy_name -expiry-time expiration_date_time
```

次の例は、既存のSnapshotコピーに保持期間を適用します。

```
cluster1> volume snapshot modify-snaplock-expiry-time -volume vol1  
-snapshot snap2 -expiry-time "11/10/2022 09:00:00"
```

既存のポリシーを変更して長期保持を適用する

ONTAP 9.14.1以降では、Snapshotコピーの長期保持を設定するルールを追加して、既存のSnapMirrorポリシーを変更できます。このルールは、SnapLockヴォールトデスティネーションおよびSnapLock以外のSnapMirrorデスティネーションボリュームでのデフォルトのボリューム保持期間を上書きするために使用されます。

1. 既存のSnapMirrorポリシーにルールを追加します。

```
snapmirror policy add-rule -vserver <SVM name> -policy <policy name>  
-snapmirror-label <label name> -keep <number of Snapshot copies> -retention  
-period [<integer> days|months|years]
```

次の例は、「LockVault」という既存のポリシーに6カ月の保持期間を適用するルールを作成します。

```
snapmirror policy add-rule -vserver vs1 -policy lockvault -snapmirror  
-label test1 -keep 10 -retention-period "6 months"
```

## SnapLock API

Zephyr API を使用して、SnapLock 機能をスクリプトやワークフローオートメーションと統合することができます。API は、HTTP、HTTPS、および Windows DCE / RPC を介した XML メッセージングを使用します。詳細については、を参照してください

"ONTAP 自動化に関するドキュメント"。

**file-fingerprint - 中止**

ファイルフィンガープリント処理を中止します。

**file-fingerprint -dump** を実行します

ファイルフィンガープリント情報を表示します。

**file-fingerprint -get-iter**

ファイルフィンガープリント処理のステータスを表示します。

**file-fingerprint -start** の算出

ファイルフィンガープリントを生成します。

**snaplock-archive-vserver-log**

アクティブな監査ログファイルをアーカイブします。

**snaplock-create -vserver -log**

SVM の監査ログ設定を作成します。

**snaplock-delete -vserver -log**

SVM の監査ログ設定を削除します。

**snaplock-file-privileged-delete-delete**

privileged delete 処理を実行します。

**snaplock-get-file-retention**

ファイルの保持期間を取得します。

**snaplock-get-node-compliance-clock** では

ノードの ComplianceClock の日付と時刻を取得します。

**snaplock-get-vserver -active-log-file-iter**

アクティブなログファイルのステータスを表示します。

**snaplock-get-vserver -log-iter**

監査ログ設定を表示します。

### **snaplock-modify -vserver -log**

SVM の監査ログ設定を変更します。

### **snaplock-set-file-retention**

ファイルの保持期限を設定します。

### **snaplock-set-node-compliance-clock** のいずれかです

ノードの ComplianceClock の日付と時刻を設定します。

### **snaplock-volume-set-privileged-delete**

SnapLock Enterprise ボリュームで privileged-delete オプションを設定します。

### **volume-get-snaplock-attrs**

SnapLock ボリュームの属性を取得します。

### **volume-set-snaplock-attrs**

SnapLock ボリュームの属性を設定します。

## **整合グループ**

### **整合グループの概要**

整合グループは、1つのユニットとして管理されるボリュームの集まりです。ONTAPでは、整合グループを使用することで、複数のボリュームにまたがるアプリケーションワークロードの管理が容易になり、保護が保証されます。

整合グループを使用すると、ストレージ管理を簡易化できます。20個のLUNにまたがる重要なデータベースがあるとします。LUNを個別に管理することも、LUNを単一のデータセットとして扱い、単一の整合グループに編成することもできます。

整合グループを使用すると、アプリケーションワークロードの管理が容易になり、ローカルとリモートの保護ポリシーを簡単に設定できます。また、一連のボリュームについて、ある時点におけるcrash-consistentまたはアプリケーションと整合性のあるSnapshotコピーを同時に作成できます。整合性グループのSnapshotコピーを使用すると、アプリケーションワークロード全体をリストアできます。

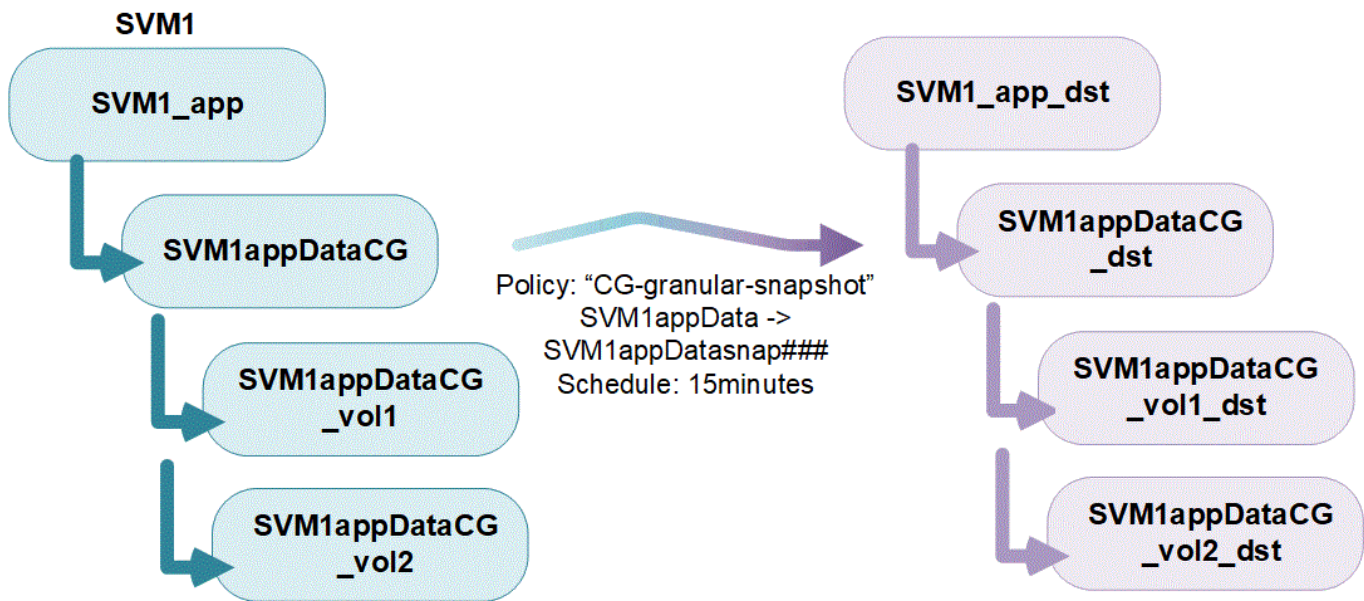
### **整合グループの詳細**

整合グループは、プロトコル（NAS、SAN、NVMe）に関係なく任意のFlexVolをサポートし、ONTAP REST APIまたは\* Storage > Consistency Groups \*メニュー項目でSystem Managerから管理できます。ONTAP 9.14.1以降では、ONTAP CLIを使用して整合グループを管理できます。

整合グループは、個々のエンティティ（ボリュームの集まり）として作成することも、他の整合グループで構成される階層関係として作成することもできます。個々のボリュームには、ボリューム単位で独自のSnapshotポリシーを設定できます。また、整合グループ全体のSnapshotポリシーを作成することもできます。整合グループには、SnapMirror Business Continuity（SM-BC）関係と共有のSM-BCポリシーを1つだけ含

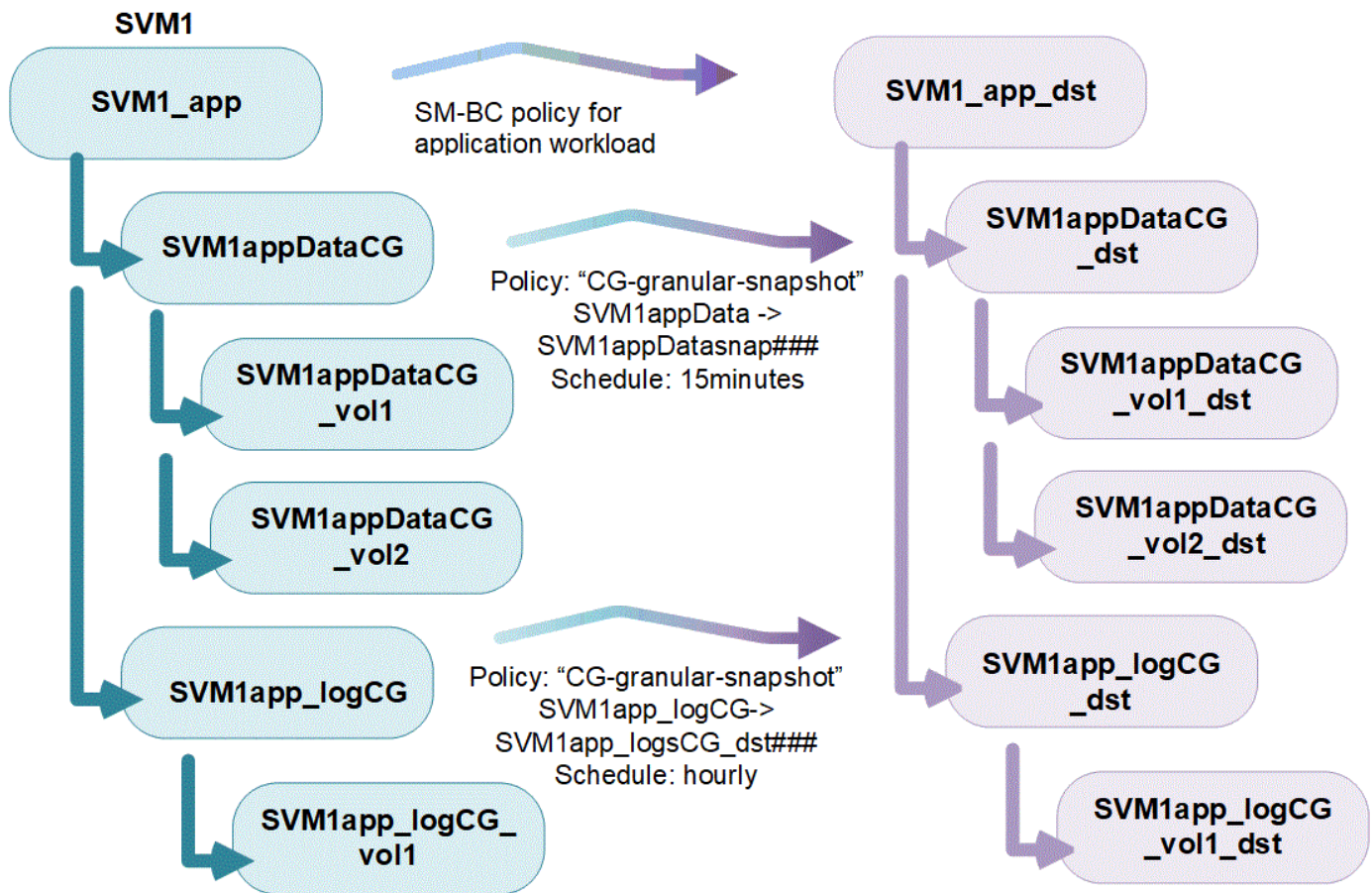
めることができます。このポリシーを使用して整合グループ全体をリカバリできます。

次の図は、個々の整合グループを使用する方法を示しています。でホストされているアプリケーションのデータ SVM1 2つのボリュームにまたがっている： vol1 および vol2。整合グループのSnapshotポリシーは、データのSnapshotコピーを15分ごとにキャプチャします。



アプリケーションワークロードが大きいほど、複数の整合グループが必要になる場合がありますこのような場合は、階層型整合グループを作成して、1つの整合グループが親整合グループの子コンポーネントになります。親整合グループには、最大5つの子整合グループを含めることができます。個々の整合グループと同様に、リモートの SM-BC 保護ポリシーを整合グループの設定全体（親と子）に適用して、アプリケーションワークロードをリカバリすることができます。

次の例では、アプリケーションがでホストされています SVM1。管理者が親整合グループを作成し、SVM1\_app`を使用します。このグループには次の2つの子整合グループ `SVM1appDataCG データおよび SVM1app\_logCG をクリックします。子整合グループには、それぞれ独自のSnapshotポリシーがあります。SVMナインボリュームノSnapshotコピー SVM1appDataCG 15分ごとに服用してください。のSnapshot SVM1app\_logCG 1時間ごとに作成されます。親整合グループ SVM1\_app データを複製し、災害発生時にサービスを継続できるようにするSM-BCポリシーが用意されています。



ONTAP 9.12.1以降では、整合グループがサポートされます [クローニング](#) 整合性のメンバーを変更するには、[ボリュームを追加または削除する](#) System ManagerとONTAP REST APIの両方で使用できます。ONTAP 9.12.1以降では、ONTAP REST APIで次の機能もサポートされます。

- 新しいNFSまたはSMBボリュームまたはNVMeネームスペースで整合グループを作成する。
- 新規または既存のNFS / SMBボリュームまたはNVMeネームスペースを既存の整合グループに追加する。

ONTAP REST APIの詳細については、[を参照してください "ONTAP REST APIのリファレンスドキュメント"](#)。

### 整合グループを監視する

ONTAP 9.13.1以降では、整合グループで容量とパフォーマンスをリアルタイムと履歴で監視し、アプリケーションや個々の整合グループのパフォーマンスに関する分析情報を提供します。

監視データは5分ごとに更新され、最長1年間保持されます。次の指標を追跡できます。

- パフォーマンス：IOPS、レイテンシ、スループット
- 容量：サイズ、使用済み論理容量、使用可能

監視データは、System Managerの整合グループメニューの[\***Overview**]タブで表示するか、REST APIで要求することで表示できます。ONTAP 9.14.1以降では、CLIを使用して整合グループの指標を表示できます。  
consistency-group metrics show コマンドを実行します





ONTAP 9.13.1では、REST APIを使用してのみ過去の指標を取得できます。ONTAP 9.14.1以降では、System Managerでも履歴指標を使用できます。

整合グループを保護します

コンシステンシ・グループは次の機能を使用

- Snapshot ポリシー
- [SnapMirror のビジネス継続性 \(SM-BC\)](#)
- [\[mcc\]](#) (ONTAP 9.11.1以降)
- [非同期SnapMirror](#) (ONTAP 9.13.1以降)
- ["SVM ディザスタリカバリ"](#) (ONTAP 9.14.1以降)

整合性グループを作成しても、保護は自動的に有効になりません。ローカルとリモートの保護ポリシーは、整合グループの作成時または作成後に設定できます。

コンシステンシグループに保護を設定するには、[を参照してください "整合グループを保護する"](#)。

リモート保護を利用するには、の要件を満たす必要があります [SnapMirror によるビジネス継続性の導入](#)。



NAS アクセス用にマウントされたボリュームでは、SM-BC 関係を確立できません。

## MetroCluster 構成の整合グループ

ONTAP 9.11.1以降では、MetroCluster 構成内のクラスタに新しいボリュームを含む整合グループをプロビジョニングできます。ミラーアグリゲートにプロビジョニングされています。

プロビジョニングが完了したら、整合グループに関連付けられているボリュームを、ミラーされたアグリゲートとミラーされていないアグリゲートの間で移動できます。したがって、整合グループに関連付けられたボリュームは、ミラーされたアグリゲート、ミラーされていないアグリゲート、またはその両方に配置できます。整合性グループに関連付けられているボリュームを含むミラーアグリゲートを変更して、ミラーされない状態にすることができます。同様に、整合グループに関連付けられたボリュームを含むミラーされていないアグリゲートを変更することで、ミラーリングを有効にすることができます

ミラーされたアグリゲートに配置された整合グループに関連付けられているボリュームとSnapshotコピーがリモートサイト（サイトB）にレプリケートされます。サイトBのボリュームの内容によって整合グループの書き込み順序が保証されるため、災害発生時にサイトBからリカバリできます。ONTAP 9.11.1以降を実行しているクラスタでは、REST APIおよびSystem Managerを使用して整合グループのSnapshotコピーにアクセスできます。ONTAP 9.14.1以降では、ONTAP CLIを使用してSnapshotコピーにアクセスすることもできます。

整合グループに関連付けられている一部またはすべてのボリュームがミラーされていないアグリゲートに配置されていて、現在アクセスできない場合、整合グループに対するGET処理またはDELETE処理は、ローカルボリュームまたはホストアグリゲートがオフラインかのように動作します。

## レプリケーション用のコンシステンシグループの設定

サイトBでONTAP 9.10.1以前が実行されている場合、ミラーされたアグリゲートにある整合グループに関連付けられているボリュームだけがサイトBにレプリケートされます整合グループの設定は、両方のサイトでONTAP 9.11.1以降が実行されている場合にのみサイトBにレプリケートされます。サイトBをONTAP 9.11.1にアップグレードしたあと、サイトAの整合グループのデータのうち、関連付けられているすべてのボリュー

ムがミラーされたアグリゲートに配置されているものはサイトBにレプリケートされます



ストレージのパフォーマンスと可用性を最適化するために、ミラーアグリゲートでは少なくとも20%の空きスペースを確保することを推奨します。ミラーされていないアグリゲートでは10%が推奨されますが、追加の10%のスペースはファイルシステムで増分変更に対応するために使用できます。増分変更を行うと、ONTAPのcopy-on-write Snapshotベースのアーキテクチャにより、ミラーされたアグリゲートのスペース使用率が向上します。これらのベストプラクティスに従わないと、パフォーマンスに悪影響を及ぼす可能性があります。

## アップグレード時の考慮事項

ONTAP 9.8および9.9.1でSM-BCで作成した整合グループは、ONTAP 9.10.1以降へのアップグレード時に、System Managerの\*[ストレージ]>[整合グループ]\*またはONTAP REST APIで自動的にアップグレードされて管理できるようになります。ONTAP 9.8または9.9.1からのアップグレードの詳細については、を参照してください ["SM-BC アップグレードおよびリバートに関する考慮事項"](#)。

REST APIで作成された整合グループSnapshotコピーは、System Managerの整合グループインターフェイスおよび整合グループREST APIエンドポイントを使用して管理できます。ONTAP 9.14.1以降では、ONTAP CLIでも整合グループSnapshotを管理できます。



ontapiコマンドで作成されたSnapshotコピー `cg-start` および `cg-commit` は整合グループのSnapshotとして認識されるため、ONTAP REST APIでは、System Managerの整合グループインターフェイスまたは整合グループエンドポイントから管理することはできません。ONTAP 9.14.1以降では、非同期SnapMirrorポリシーを使用している場合、これらのSnapshotコピーをデスティネーションボリュームにミラーリングできます。詳細については、を参照してください [非同期SnapMirror保護を設定する](#)。

## リリースごとにサポートされる機能

	ONTAP 9.14.1	ONTAP 9.13.1	ONTAP 9.12.1	ONTAP 9.11.1	ONTAP 9.10.1
階層整合グループ	✓	✓	✓	✓	✓
Snapshotコピーによるローカル保護	✓	✓	✓	✓	✓
SnapMirror によるビジネス継続性	✓	✓	✓	✓	✓
MetroCluster のサポート	✓	✓	✓	✓	
2フェーズコミット (REST APIのみ)	✓	✓	✓	✓	
アプリケーションタグとコンポーネントタグ	✓	✓	✓		
整合グループをクローニングします	✓	✓	✓		
ボリュームを追加および削除します	✓	✓	✓		
新しいNASボリュームでCGを作成します	✓	✓	REST APIのみ		
新しいNVMeネームスペースを使用してCGを作成します	✓	✓	REST APIのみ		
子整合グループ間でボリュームを移動します	✓	✓			



	ONTAP 9.14.1	ONTAP 9.13.1	ONTAP 9.12.1	ONTAP 9.11.1	ONTAP 9.10.1
コンシステンシグループジオメトリを変更します	✓	✓			
監視	✓	✓			
非同期SnapMirror（単一の整合グループのみ）	✓	✓			
SVMディザスタリカバリ（単一の整合グループのみ）	✓				
CLIのサポート	✓				

## 整合グループに関する詳細情報



## 詳細情報

- ["ONTAP 自動化に関するドキュメント"](#)
- [SnapMirror によるビジネス継続性](#)
- [非同期 SnapMirror ディザスタリカバリの基本](#)
- ["MetroCluster のドキュメント"](#)

## 整合グループの制限

整合グループを計画および管理するときは、クラスタと親または子の両方の整合グループの範囲でオブジェクトの制限を考慮してください。

## テキヨウセイケン

次の表に、整合グループの制限を示します。SnapMirrorビジネス継続性（SM-BC）を使用する整合グループには別々の制限が適用されます。詳細については、を参照してください ["SM-BC の制限および制限事項"](#)。

制限（Limit）	適用範囲	最小（Minimum）	最大
整合グループの数	クラスタ	0	クラスタの最大ボリューム数と同じ
親整合グループの数	クラスタ	0	クラスタの最大ボリューム数と同じ
個々の整合グループと親整合グループの数	クラスタ	0	クラスタの最大ボリューム数と同じ
整合グループ内のボリュームの数	単一の整合グループ	1巻	全80巻
親整合グループの子内のボリュームの数	親整合グループ	1巻	全80巻
子整合性グループ内のボリュームの数	子整合グループ	1巻	全80巻
親整合グループ内の子整合グループの数	親整合グループ	1個の整合グループ	5つの整合グループ
整合性グループが存在するSVMディザスタリカバリ関係の数（ONTAP 9.14.1以降で使用可能）	クラスタ	0	32だ

### 強制されていない制限

整合グループでサポートされる最小Snapshotコピースケジュールは30分です。これは次の値に基づいています：["FlexGroupニツイテノテスト"](#)（整合グループと同じSnapshotインフラを共有）。

### 単一の整合グループを設定する

整合グループは、既存のボリューム、または新しいLUNまたはボリュームを使用して作成できます（ONTAPのバージョンによって異なります）。ボリュームまたはLUNを関連付けることができる整合グループは一度に1つだけです。

#### このタスクについて

- ONTAP 9.10.1~9.11.1では、整合グループのメンバーボリュームを作成後に変更することはできません。

ONTAP 9.12.1以降では、整合グループのメンバーボリュームを変更できます。このプロセスの詳細については、を参照してください [整合グループを変更する](#)。

### 新しいLUNまたはボリュームを含む整合グループを作成します

ONTAP 9.10.1~9.12.1では、新しいLUNを使用して整合グループを作成できます。ONTAP 9.13.1以降では、新しいNVMeネームスペースまたは新しいNASボリュームで整合グループを作成することもできます。（これ

は、ONTAP 9.12.1以降のONTAP REST APIでもサポートされています）。

## System Manager の略

### 手順

1. Storage > Consistency groups \* を選択します。
2. [+ Add]\*を選択し、ストレージオブジェクトのプロトコルを選択します。

ONTAP 9.10.1~9.12.1では、新しいストレージオブジェクトの唯一のオプションは新しい**LUN**を使用するです。ONTAP 9.13.1以降では、System Managerで新しいNVMeネームスペースと新しいNASボリュームを使用した整合グループの作成がサポートされます。

3. 整合グループに名前を付けます。ボリュームまたはLUNの数と各ボリュームまたはLUNの容量を指定します。
  - a. アプリケーションタイプ: ONTAP 9.12.1以降を使用している場合は、アプリケーションタイプを選択します。値を選択しない場合'デフォルトではコンシステンシ・グループには **Other** のタイプが割り当てられます一貫性のタグ付けの詳細については、を参照してください [アプリケーションタグとコンポーネントタグ](#)。リモート保護ポリシーを使用して整合グループを作成する場合は、\* other \*を使用する必要があります。
  - b. **[New LUNs]**の場合：ホストオペレーティングシステムとLUN形式を選択します。ホストイニシエータの情報を入力します。
  - c. **[New NAS volumes]**の場合：SVMのNAS構成に基づいて、適切なエクスポートオプション（NFSまたはSMB/CIFS）を選択します。
  - d. **[New NVMe Namespaces]**の場合：ホストオペレーティングシステムとNVMeサブシステムを選択します。
4. 保護ポリシーを設定したり、子コンシステンシグループを追加したり、アクセス権限を追加したりするには、\*[その他のオプション]\*を選択します。
5. [ 保存（ Save ） ] を選択します。
6. 整合グループが作成されたことを確認するために、ジョブの完了後に表示されるメインの整合グループメニューに戻ります。保護ポリシーを設定した場合は、該当するポリシーの下に緑色の盾が表示されたときに、そのポリシーが適用されていることがわかります（[Look under the appropriate policy]、[remote or local]）。

### CLI の使用

ONTAP 9.14.1以降では、ONTAP CLIを使用して、新しいボリュームを含む新しい整合グループを作成できます。パラメータは、ボリュームがSAN、NVMe、NFSのいずれであるかによって異なります。

#### NFSボリュームを含む整合グループを作成する

1. 整合グループを作成します。

```
consistency-group create -vserver SVM_name -consistency-group consistency-group-name -volume volume-prefix -volume-count number -size size -export-policy policy_name
```

#### SANボリュームを含むコンシステンシグループの作成

1. 整合グループを作成します。

```
consistency-group create -vserver SVM_name -consistency-group consistency-group-name -lun lun_name -size size -lun-count number -igroup igroup_name
```

### NVMeネームスペースを含む整合性グループを作成する

1. 整合グループを作成します。

```
consistency-group create -vserver SVM_name -consistency-group  
consistency_group_name -namespace namespace_name -volume-count number  
-namespace-count number -size size -subsystem subsystem_name
```

完了したら

1. を使用して整合グループが作成されたことを確認します。 `consistency-group show` コマンドを実行します

既存のボリュームを含む整合グループを作成します

既存のボリュームを使用して整合グループを作成することができます。

## System Manager の略

### 手順

1. Storage > Consistency groups \* を選択します。
2. 「+追加」を選択し、既存のボリュームを使用する\*を選択します。
3. 整合グループに名前を付けて Storage VM を選択します。
  - a. アプリケーションタイプ: ONTAP 9.12.1以降を使用している場合は、アプリケーションタイプを選択します。値を選択しない場合'デフォルトではコンシステンシ・グループには **Other** のタイプが割り当てられます一貫性のタグ付けの詳細については、を参照してください [アプリケーションタグとコンポーネントタグ](#)。整合グループにSM-BC関係がある場合は、\* other \*を使用する必要があります。
4. 対象に含める既存のボリュームを選択します。選択できるのは、整合グループにまだ含まれていないボリュームのみです。



既存のボリュームを含む整合グループを作成する場合、整合グループではFlexVol ボリュームがサポートされます。非同期 SnapMirror 関係または同期 SnapMirror 関係が設定されたボリュームは整合グループに追加できますが、整合グループには対応していません。整合グループでは、S3バケットやSVMDR関係を使用するStorage VMはサポートされません。

5. [ 保存 ( Save ) ] を選択します。
6. 整合グループが作成されたことを確認するために、ONTAP ジョブの完了時に表示されるメインの整合グループメニューに戻ります。保護ポリシーを選択した場合は、メニューから整合グループを選択して、ポリシーが適切に設定されていることを確認します。保護ポリシーを設定した場合は、該当するポリシーの下に緑色の盾が表示されたときに、そのポリシーが適用されていることがわかります ([Look under the appropriate policy], [remote or local]) 。

### CLI の使用

ONTAP 9.14.1以降では、ONTAP CLIを使用して、既存のボリュームを含む整合グループを作成できます。

### 手順

1. 問題 `consistency-group create` コマンドを実行します。 `-volumes` パラメータには、ボリューム名をカンマで区切って指定できます。

```
consistency-group create -vserver SVM_name -consistency-group consistency-group-name -volume volumes
```

2. を使用して整合グループを表示する `consistency-group show` コマンドを実行します

### 次のステップ

- [整合グループを保護する](#)
- [整合グループを変更する](#)
- [整合グループをクローニングする](#)

## 階層型整合グループを設定します

階層整合グループを使用すると、複数のボリュームにまたがる大規模なワークロードを管理できます。作成した親整合グループは、子整合グループの傘として機能します。

階層型整合グループには、最大 5 つの個別の整合グループを含むことができる親があります。階層型整合グループでは、整合グループまたは個々のボリュームで異なるローカル Snapshot ポリシーをサポートできます。リモート保護ポリシーを使用する場合は、階層整合グループ全体（親と子）に適用されます。

ONTAP 9.13.1以降では、次の操作を実行できます。 [コンシステンシグループの形状を変更します](#) および [子整合グループ間でボリュームを移動します](#)。

整合グループのオブジェクト制限については、を参照してください [整合性グループのオブジェクトの制限](#)。

新しい**LUN**またはボリュームを含む階層整合グループを作成します

階層型整合グループを作成する場合は、新しいLUNを追加できます。ONTAP 9.13.1以降では、新しいNVMe ネームスペースとNASボリュームも使用できます。

## System Manager の略

### 手順

1. Storage > Consistency groups \* を選択します。
2. [+ Add]\*を選択し、ストレージオブジェクトのプロトコルを選択します。

ONTAP 9.10.1~9.12.1では、新しいストレージオブジェクトの唯一のオプションは新しい**LUN**を使用するです。ONTAP 9.13.1以降では、System Managerで新しいNVMeネームスペースと新しいNASボリュームを使用した整合グループの作成がサポートされます。

3. 整合グループに名前を付けます。ボリュームまたはLUNの数と各ボリュームまたはLUNの容量を指定します。
  - a. アプリケーションタイプ: ONTAP 9.12.1以降を使用している場合は、アプリケーションタイプを選択します。値を選択しない場合'デフォルトではコンシステンシ・グループには **Other** のタイプが割り当てられます一貫性のタグ付けの詳細については、を参照してください [アプリケーションタグとコンポーネントタグ](#)。リモート保護ポリシーを使用する場合は、\*[その他]\*を選択する必要があります。
4. ホストオペレーティングシステムと LUN 形式を選択します。ホストイニシエータの情報を入力します。
  - a. **[New LUNs]**の場合：ホストオペレーティングシステムとLUN形式を選択します。ホストイニシエータの情報を入力します。
  - b. **[New NAS volumes]**の場合：SVMのNAS構成に基づいて、適切なエクスポートオプション（NFSまたはSMB/CIFS）を選択します。
  - c. **[New NVMe Namespaces]**の場合：ホストオペレーティングシステムとNVMeサブシステムを選択します。
5. 子整合グループを追加するには、**[その他のオプション]\***を選択し、+子整合グループを追加\*を選択します。
6. パフォーマンスレベル、LUNまたはボリュームの数、およびLUNまたはボリュームあたりの容量を選択します。使用しているプロトコルに基づいて、適切なエクスポート設定またはオペレーティングシステム情報を指定します。
7. 必要に応じて、ローカルSnapshotポリシーを選択し、アクセス権限を設定します。
8. 最大 5 つの子整合グループに対して、を繰り返します。
9. [ 保存（ Save ） ] を選択します。
10. 整合グループが作成されたことを確認するために、ONTAP ジョブの完了時に表示されるメインの整合グループメニューに戻ります。保護ポリシーを設定する場合は、該当するポリシーの下で、リモートまたはローカルを確認します。緑の盾の横にチェックマークが表示されます。

### CLI の使用

ONTAP 9.14.1以降では、CLIを使用して新しい階層整合グループを作成できます。

### ステップ

1. を使用して新しい整合グループを作成します。 `consistency-group create` コマンドを実行します

。 `volume-count` パラメータは、各子整合性グループ内のボリューム数を設定します。最大5つの子整合グループからなる親整合グループを作成できます。



```
consistency-group create -vserver SVM_name -consistency-group  
consistency_group_name -parent-consistency-group  
parent_consistency_group_name -cg-count number_of_child_consistency_groups  
-volume volume_prefix -volume-count number -size size -export-policy  
policy_name -storage-service extreme
```

既存のボリュームを含む階層型整合グループを作成します

既存のボリュームを階層型整合グループにまとめることができます。

## System Manager の略

### 手順

1. Storage > Consistency groups \* を選択します。
2. 「+追加」を選択し、既存のボリュームを使用する\*を選択します。
3. Storage VM を選択してください。
4. 対象に含める既存のボリュームを選択します。選択できるのは、整合グループにまだ含まれていないボリュームのみです。
5. 子コンシステンシグループを追加するには、\* + 子コンシステンシグループの追加 \* を選択します。必要な整合グループを作成します。このグループには自動的に名前が付けられます。
  - a. コンポーネントタイプ: ONTAP 9.12.1以降を使用している場合は、「データ」、「ログ」、または「その他」のコンポーネントタイプを選択します。値を選択しない場合、デフォルトではコンシステンシ・グループには **Other** のタイプが割り当てられます。一貫性のタグ付けの詳細については、を参照してください [アプリケーションタグとコンポーネントタグ](#)。リモート保護ポリシーを使用する場合は、\* other \*を使用する必要があります。
6. 各整合グループに既存のボリュームを割り当てます。
7. 必要に応じて、ローカルSnapshotポリシーを選択します。
8. 最大 5 つの子整合グループに対して、を繰り返します。
9. [ 保存 ( Save ) ] を選択します。
10. 整合グループが作成されたことを確認するために、ONTAP ジョブの完了時に表示されるメインの整合グループメニューに戻ります。保護ポリシーを選択した場合は、メニューから整合グループを選択して適切に設定されていることを確認します。適切なポリシータイプの下に、緑の盾の横にチェックマークが表示されます。

### CLI の使用

ONTAP 9.14.1以降では、CLIを使用して階層整合グループを作成できます。

### 手順

1. 新しい親整合グループをプロビジョニングし、新しい子整合グループにボリュームを割り当てます。

```
consistency-group create -vserver svm_name -consistency-group  
child_consistency_group_name -parent-consistency-group  
parent_consistency_group_name -volumes volume_names
```

2. 入力するコマンド y をクリックして、新しい親整合グループと子整合グループを作成するかどうかを確認します。

### 次のステップ

- [整合グループのジオメトリを変更します](#)
- [整合グループを変更する](#)
- [整合グループを保護する](#)

## 整合グループを保護します

整合グループを使用すると、複数のボリュームにまたがる SAN、NAS、NVMe のアプリケーションに対して、ローカルとリモートで簡単に保護することができます。

整合性グループを作成しても、保護は自動的に有効になりません。保護ポリシーは、コンシステンシグループの作成時または作成後に設定できます。次のコマンドを使用して整合グループを保護できます。

- ローカルSnapshotコピー
- SnapMirror のビジネス継続性（SM-BC）
- [MetroCluster（9.11.1以降）](#)
- 非同期SnapMirror（9.13.1以降）
- 非同期SVMディザスタリカバリ（9.14.1以降）

ネストされた整合グループを使用する場合は、親整合グループと子整合グループに異なる保護ポリシーを設定できます。

ONTAP 9.11.1以降では、整合グループで [2フェーズの整合グループSnapshotの作成](#)。2フェーズSnapshot処理では事前チェックが実行され、Snapshotコピーが正常にキャプチャされたことが確認されます。

リカバリは、整合グループ全体、階層構成内の単一の整合グループ、または整合グループ内の個々のボリュームに対して実行できます。リカバリを実行するには、リカバリ元の整合グループを選択し、Snapshotコピーのタイプを選択して、リストア元となるSnapshotコピーを特定します。このプロセスの詳細については、[を参照してください "以前の Snapshot コピーからボリュームをリストアします"](#)。

### ローカルSnapshotポリシーを設定する


ローカルSnapshot保護ポリシーを設定すると、整合性グループのすべてのボリュームに適用するポリシーを作成できます。

#### このタスクについて

整合グループでサポートされる最小Snapshotコピースケジュールは30分です。これは次の値に基づいています：["FlexGroupニツイテノテスト"](#)（整合グループと同じSnapshotインフラを共有）。

## System Manager の略

### 手順

1. Storage > Consistency groups \* を選択します。
2. コンシステンシ・グループ・メニューから '作成したコンシステンシ・グループ'を選択します
3. コンシステンシ・グループの概要ページの右上にある \* 編集 \* を選択します
4. スケジュール Snapshot コピー（ローカル）\* の横のボックスをオンにします。
5. Snapshot ポリシーを選択します。新しいカスタムポリシーを設定する手順については、を参照してください ["カスタムのデータ保護ポリシーを作成する"](#)。
6. [ 保存（ Save ） ] を選択します。
7. 整合性グループの概要メニューに戻ります。左の列の\* Snapshot copies（ローカル）\*で、ステータスは横にprotectedと表示されます 。

### CLI の使用

ONTAP 9.14.1以降では、CLIを使用して整合グループの保護ポリシーを変更できます。

### ステップ

1. 保護ポリシーを設定または変更するには、次のコマンドを実行します問題。

子整合性の保護ポリシーを変更する場合は、`-parent-consistency-group parent_consistency_group_name` パラメータ

```
consistency-group modify -vserver svm_name -consistency-group  
consistency_group_name -snapshot-policy policy_name
```

## オンデマンドのSnapshotコピーを作成する

通常のスケジュールされたポリシー以外で整合グループのSnapshotコピーを作成する必要がある場合は、オンデマンドでSnapshotコピーを作成できます。

## System Manager の略

### 手順

1. >[整合グループ]\*に移動します。
2. オンデマンドSnapshotコピーを作成する整合性グループを選択します。
3. タブに切り替えて、+追加\*を選択します。
4. 名前\*とSnapMirrorラベル\*を指定してください。[整合性]のドロップダウンメニューで、[アプリケーション整合性]\*または[クラッシュ整合性]\*を選択します。
5. [保存 ( Save ) ]を選択します。

### CLI の使用

ONTAP 9.14.1以降では、CLIを使用して整合グループのオンデマンドSnapshotコピーを作成できます。

### ステップ

1. Snapshotコピーを作成します。

デフォルトのSnapshotタイプはcrash-consistentです。Snapshotタイプは、オプションの `-type` パラメータ

```
consistency-group snapshot create -vserver svm_name -consistency-group  
consistency_group_name -snapshot snapshot_name
```

## 2フェーズ・コンシステンシ・グループ・スナップショットの作成

ONTAP 9.11.1以降では、整合グループ（CG）Snapshot作成の2フェーズコミットがサポートされます。この2フェーズでは、Snapshotコピーをコミットする前に事前確認が実行されます。この機能は、ONTAP REST APIでのみ使用できます。

二段階的なCG Snapshot作成はSnapshot作成にのみ使用でき、整合グループのプロビジョニングや整合グループのリストアには使用できません。

2フェーズのCG Snapshotでは、Snapshotの作成プロセスが2つのフェーズに分割されます。

1. 最初のフェーズでは、事前確認が実行され、Snapshotの作成がトリガーされます。最初のフェーズには、Snapshotコピーが正常にコミットされるまでの時間を指定するタイムアウトパラメータが含まれています。
2. フェーズ1の要求が正常に完了した場合は、最初のフェーズから指定した間隔で第2フェーズを呼び出し、適切なエンドポイントにSnapshotコピーをコミットできます。

### 作業を開始する前に

- 2フェーズCG Snapshot作成を使用するには、クラスタ内のすべてのノードでONTAP 9.11.1以降が実行されている必要があります。
- 1つの整合グループインスタンスでサポートされる整合グループのSnapshot処理のアクティブな呼び出しは、1フェーズか2フェーズかに関係なく、一度に1回だけです。別の処理の実行中にSnapshot処理を開始しようとするとエラーになります。
- Snapshotの作成を実行するときに、オプションで5~120秒のタイムアウト値を設定できます。タイムアウト

ト値を指定しない場合、処理はデフォルトの7秒でタイムアウトします。APIで、タイムアウト値を `action_timeout` パラメータCLIでは、 `-timeout` フラグ。

#### 手順

REST APIまたはONTAP 9.14.1以降のONTAP CLIを使用して、2フェーズSnapshotを作成できます。この処理はSystem Managerではサポートされていません。



APIを使用してSnapshotの作成を呼び出す場合は、APIを使用してSnapshotコピーをコミットする必要があります。CLIを使用してSnapshotの作成を呼び出す場合は、CLIを使用してSnapshotコピーをコミットする必要があります。混在方式はサポートされていません。

## CLI の使用

ONTAP 9.14.1以降では、CLIを使用して2フェーズSnapshotコピーを作成できます。

### 手順

1. Snapshotを開始します。

```
consistency-group snapshot start -vserver svm_name -consistency-group  
consistency_group_name -snapshot snapshot_name [-timeout time_in_seconds  
-write-fence {true|false}]
```

2. Snapshotが作成されたことを確認します。

```
consistency-group snapshot show
```

3. Snapshotをコミットします。

```
consistency-group snapshot commit svm_name -consistency-group  
consistency_group_name -snapshot snapshot_name
```

## API

1. Snapshotの作成を呼び出します。を使用して、コンシステンシグループエンドポイントにPOST要求を送信します `action=start` パラメータ

```
curl -k -X POST 'https://<IP_address>/application/consistency-  
groups/<cg-uuid>/snapshots?action=start&action_timeout=7' -H  
"accept: application/hal+json" -H "content-type: application/json"  
-d '  
{  
  "name": "<snapshot_name>",  
  "consistency_type": "crash",  
  "comment": "<comment>",  
  "snapmirror_label": "<SnapMirror_label>"  
}'
```

2. POST要求が成功すると、出力にSnapshot UUIDが表示されます。指定したUUIDを使用して、PATCH要求を送信してSnapshotコピーをコミットします。

```
curl -k -X PATCH 'https://<IP_address>/application/consistency-groups/<cg_uuid>/snapshots/<snapshot_id>?action=commit' -H "accept: application/hal+json" -H "content-type: application/json"
```

For more information about the ONTAP REST API, see [link:https://docs.netapp.com/us-en/ontap-automation/reference/api\\_reference.html](https://docs.netapp.com/us-en/ontap-automation/reference/api_reference.html) [API reference^] or the [link:https://devnet.netapp.com/restapi.php](https://devnet.netapp.com/restapi.php) [ONTAP REST API page^] at the NetApp Developer Network for a complete list of API endpoints.

## コンシステンシグループにリモート保護を設定します

整合グループは、SM-BCおよびONTAP 9.13.1以降の非同期SnapMirrorを使用したリモート保護を提供します。

### SM-BCで保護を設定します

SM-BCを使用すると、整合グループに作成された整合グループのSnapshotコピーがデスティネーションにコピーされるようにすることができます。SM-BCの詳細、またはCLIを使用したSM-BCの設定方法については、[を参照してください](#)。 [ビジネス継続性の保護を構成します](#)。

#### 作業を開始する前に

- NAS アクセス用にマウントされたボリュームでは、SM-BC 関係を確立できません。
- ソースクラスタとデスティネーションクラスタのポリシーラベルが一致している必要があります。
- 事前定義されたSnapMirrorラベルが設定されたルールを追加しないかぎり、SM-BCはデフォルトでSnapshotコピーをレプリケートしません AutomatedFailOver ポリシーとSnapshotコピーは、同じラベルで作成されます。

このプロセスの詳細については、[を参照してください](#) ["SM-BCによる保護"](#)。

- [カスケード構成](#) SM-BCではサポートされません。
- ONTAP 9.13.1以降では、システムを停止することなく [整合グループにボリュームを追加します](#) アクティブなSM-BC関係を使用している場合。整合性グループにその他の変更を加える場合は、SM-BC関係を解除し、整合性グループを変更してから関係を再確立して再同期する必要があります。




CLIを使用してSM-BCを設定するには、[を参照してください](#)。 [SM-BCによる保護](#)。

### System Managerでの手順

1. が完了していることを確認します ["SM-BCを使用するための前提条件"](#)。
2. Storage > Consistency groups \* を選択します。
3. コンシステンシ・グループ・メニューから '作成したコンシステンシ・グループ'を選択します
4. 概要ページの右上で、[\* その他 \*]、[\* 保護 \*]の順に選択します。
5. ソース側の情報はSystem Managerで自動的に入力されます。デスティネーションに適したクラスタとStorage VM を選択します。保護ポリシーを選択します。「関係の初期化」がオンになっていることを確



認めます。

6. [ 保存 ( Save ) ] を選択します。
7. 整合グループを初期化して同期する必要があります。[整合グループ]\*メニューに戻って、同期が正常に完了したことを確認します。SnapMirror (リモート) \*ステータスが表示されます Protected の横 。

#### 非同期SnapMirror保護を設定する

ONTAP 9.13.1以降では、単一の整合グループに非同期SnapMirror保護を設定できます。ONTAP 9.14.1以降では、非同期SnapMirrorを使用して、整合性グループ関係を使用して、ボリューム単位のSnapshotコピーをデスティネーションクラスタにレプリケートできます。

#### このタスクについて

ボリューム単位のSnapshotコピーをレプリケートするには、ONTAP 9.14.1以降を実行している必要があります。MirrorAndVaultポリシーとVaultポリシーの場合は、ボリューム単位のSnapshotポリシーのSnapMirrorラベルが整合性グループのSnapMirrorポリシールールと一致している必要があります。ボリューム単位のSnapshotは、整合グループのSnapMirrorポリシーのkeepの値に従います。keepは、整合グループのSnapshotとは別に計算されます。たとえば、デスティネーションに2つのSnapshotコピーを保持するポリシーがある場合、ボリューム単位のSnapshotコピーを2つと整合グループのSnapshotコピーを2つ作成できます。

ボリューム単位のSnapshotコピーとSnapMirror関係を再同期する場合は、ボリューム単位のSnapshotコピーを -preserve フラグ。整合グループのSnapshotコピーよりも新しい、ボリューム単位のSnapshotコピーが保持されます。整合性グループSnapshotコピーがない場合、再同期処理でボリューム単位のSnapshotコピーを転送することはできません。

#### 作業を開始する前に

- 非同期SnapMirror保護は、単一の整合グループに対してのみ使用できます。階層型整合グループではサポートされません。階層整合グループを単一の整合グループに変換するには、[を参照してください 整合グループのアーキテクチャを変更](#)。
- ソースクラスタとデスティネーションクラスタのポリシーラベルが一致している必要があります。
- システムを停止することはありません [整合グループにボリュームを追加します](#) アクティブな非同期SnapMirror関係を使用しています。整合性グループにその他の変更を加える場合は、SnapMirror関係を解除し、整合性グループを変更してから関係を再確立して再同期する必要があります。
- 複数のボリュームに対して非同期SnapMirror保護関係を設定している場合は、既存のSnapshotコピーを保持しながら、それらのボリュームを整合グループに変換できます。ボリュームを正常に変換するには：
  - ボリュームの共通のSnapshotコピーがある必要があります。
  - 既存のSnapMirror関係を解除する必要があります。 [ボリュームを単一の整合グループに追加します](#) をクリックし、次のワークフローを使用して関係を再同期します。


#### 手順

1. デスティネーションクラスタで、\*[ストレージ]>[整合グループ]\*を選択します。
2. コンシステンシ・グループ・メニューから '作成したコンシステンシ・グループ'を選択します
3. 概要ページの右上で、[\* その他 \*]、[\* 保護 \*]の順に選択します。
4. ソース側の情報はSystem Managerで自動的に入力されます。デスティネーションに適したクラスタとStorage VMを選択します。保護ポリシーを選択します。「関係の初期化」がオンになっていることを確認します。

非同期ポリシーを選択するときは、転送スケジュールを上書きするオプションがあります。



非同期SnapMirrorを使用した整合グループでサポートされる最小スケジュール（目標復旧時点（RPO）は30分です。

5. [ 保存（ Save ） ] を選択します。
6. 整合グループを初期化して同期する必要があります。[整合グループ]\*メニューに戻って、同期が正常に完了したことを確認します。SnapMirror（リモート）\*ステータスが表示されます Protected の横 。

#### SVMディザスタリカバリの設定

ONTAP 9.14.1以降 [SVM ディザスタリカバリ](#) 整合グループがサポートされるため、整合グループの情報をソースクラスタからデスティネーションクラスタにミラーリングできます。

すでに整合グループが含まれているSVMでSVMディザスタリカバリを有効にする場合は、次のSVM設定ワークフローに従って [System Manager の略](#) または [ONTAP CLI](#)。

アクティブで正常な状態のSVMディザスタリカバリ関係が確立されたSVMに整合性グループを追加する場合は、デスティネーションクラスタからSVMディザスタリカバリ関係を更新する必要があります。詳細については、[を参照してください レプリケーション関係を手動で更新](#)。関係は、整合グループを拡張するたびに更新する必要があります。

#### 制限

- SVMディザスタリカバリでは、階層型整合グループはサポートされません。
- SVMディザスタリカバリでは、非同期SnapMirrorで保護された整合グループはサポートされません。SVMディザスタリカバリを設定する前に、SnapMirror関係を解除する必要があります。
- 両方のクラスタでONTAP 9.14.1以降が実行されている必要があります。
- 整合グループを含むSVMディザスタリカバリ構成では、ファンアウト関係はサポートされません。
- その他の制限については、[整合グループの制限](#)。

#### 関係を可視化します

System Managerの\*[保護]>[関係]\*メニューにLUNマップが表示されます。ソース関係を選択すると、ソース関係が System Manager に表示され、視覚的に確認できます。ボリュームを選択すると、これらの関係をより深く掘り下げて、含まれる LUN およびイニシエータグループの関係のリストを確認できます。この情報は、個々のボリュームビューからExcelブックとしてダウンロードできます。ダウンロード処理はバックグラウンドで実行されます。

#### 関連情報

- ["整合グループをクローニングする"](#)
- ["Snapshot コピーを設定します"](#)
- ["カスタムのデータ保護ポリシーを作成する"](#)
- ["Snapshot コピーからリカバリします"](#)
- ["以前の Snapshot コピーからボリュームをリストアします"](#)
- ["SM-BCの概要"](#)

- ["ONTAP 自動化に関するドキュメント"](#)
- [非同期 SnapMirror ディザスタリカバリの基本](#)

## 整合性グループ内のメンバーボリュームを変更します

ONTAP 9.12.1以降では、ボリュームを削除するかボリュームを追加（整合グループを拡張）して整合グループを変更できます。ONTAP 9.13.1以降では、子整合グループが共通の親を共有している場合は、子整合グループ間でボリュームを移動できます。

### 整合グループにボリュームを追加します

ONTAP 9.12.1以降では、システムを停止することなく整合グループにボリュームを追加できます。

#### このタスクについて

- 別の整合グループに関連付けられているボリュームは追加できません。
- 整合グループは、NAS、SAN、NVMeの各プロトコルをサポートします。
- 調整が全体の範囲内であれば、整合グループに一度に最大16個のボリュームを追加できます [整合グループの制限](#)。
- ONTAP 9.13.1以降では、アクティブなSnapMirrorビジネス継続性（SM-BC）または非同期SnapMirror保護ポリシーを使用して、整合グループに無停止でボリュームを追加できます。
- SM-BCで保護されている整合グループにボリュームを追加すると、新しいボリュームにミラーリングと保護が設定されるまで、SM-BC関係のステータスは「拡張中」に変わります。このプロセスの完了前にプライマリクラスタで災害が発生すると、整合グループはフェイルオーバー処理の一環として元の構成に戻ります。
- ONTAP 9.12.1以前では、SM-BC関係の整合性グループにボリュームを追加できません。最初にSM-BC関係を解除し、整合グループを変更してから、SM-BCを使用した保護をリストアする必要があります。
- ONTAP 9.12.1以降では、ONTAP REST APIで `_new_` または既存のボリュームを整合グループに追加できます。ONTAP REST APIの詳細については、[を参照してください "ONTAP REST APIのリファレンスドキュメント"](#)。

ONTAP 9.13.1以降では、この機能がSystem Managerでサポートされます。

- 整合グループを拡張する場合、変更前にキャプチャされた整合グループのSnapshotコピーは部分的なものとみなされます。このSnapshotコピーに基づくリストア処理には、Snapshotのポイントインタイムの整合グループが反映されます。
- ONTAP 9.10.1から9.11.1を使用している場合は、整合グループを変更できません。ONTAP 9.10.1または9.11.1で整合グループの設定を変更するには、整合グループを削除してから、対象に含めるボリュームを含む新しい整合グループを作成する必要があります。
- ONTAP 9.14.1以降では、非同期SnapMirrorを使用している場合に、ボリューム単位のSnapshotをデスティネーションクラスタにレプリケートできます。非同期SnapMirrorを使用して整合グループを拡張する場合、ボリューム単位のSnapshotは、SnapMirrorポリシーがMirrorAllまたはMirrorAndVaultの場合に整合グループを拡張したあとにのみレプリケートされます。ベースライン整合グループSnapshotよりも新しいボリューム単位のSnapshotのみがレプリケートされます。
- SVMディザスタリカバリ関係（ONTAP 9.14.1以降でサポート）の整合性グループにボリュームを追加する場合は、整合性グループを拡張したあとに、デスティネーションクラスタからSVMディザスタリカバリ関係を更新する必要があります。詳細については、[を参照してください。レプリケーション関係を手動で](#)

更新。

**System Manager の略**

ONTAP 9.12.1以降では、この処理をSystem Managerで実行できます。

1. Storage > Consistency groups \* を選択します。
2. 変更する整合グループを選択します。
3. 1つの整合グループを変更する場合は、\* Volumes メニューの上部で More を選択し、Expand \*を選択してボリュームを追加します。

子整合グループを変更する場合は、変更する親整合グループを特定します。[>]ボタンを選択して、子コンシステンシグループを表示し、を選択します。 をクリックします。このメニューから、\* Expand \*を選択します。

4. 整合グループに追加するボリュームを最大16個選択します。
5. [ 保存 ( Save ) ] を選択します。処理が完了したら、整合グループの\*[ボリューム]\*メニューで新たに追加されたボリュームを確認します。

**CLI の使用**

ONTAP 9.14.1以降では、ONTAP CLIを使用して整合グループにボリュームを追加できます。

**既存のボリュームを追加**

1. 問題次のコマンドを実行します。。 -volumes パラメータには、カンマで区切ったボリュームのリストを指定できます。



次のもののみを含める： -parent-consistency-group パラメータは、整合性グループが階層関係にある場合に指定します。

```
consistency-group volume add -vserver svm_name -consistency-group
consistency_group_name -parent-consistency-group parent_consistency_group
-volume volumes
```

**新しいボリュームの追加**

新しいボリュームを追加する手順は、使用するプロトコルによって異なります。



次のもののみを含める： -parent-consistency-group パラメータは、整合性グループが階層関係にある場合に指定します。

- 新しいボリュームをエクスポートせずに追加するには：

```
consistency-group volume create -vserver SVM_name -consistency-group
child_consistency_group -parent-consistency-group existingParentCg -volume
volume_name -size size
```

- 新しいNFSボリュームを追加するには：

```
consistency-group volume create -vserver SVM_name -consistency-group
consistency_group_name -volume volume-prefix -volume-count number -size
```

```
size -export-policy policy_name
```

- 新しいSANボリュームを追加するには：

```
consistency-group volume create -vserver SVM_name -consistency-group  
consistency-group-name -lun lun_name -size size -lun-count number -igroup  
igroup_name
```

- 新しいNVMeネームスペースを追加するには：

```
consistency-group volume create -vserver SVM_name -consistency-group  
consistency_group_name -namespace namespace_name -volume-count number  
-namespace-count number -size size -subsystem subsystem_name
```

整合グループからボリュームを削除します

整合性グループから削除したボリュームは削除されません。クラスタ内でアクティブなままです。

このタスクについて

- SM-BCまたはSVMディザスタリカバリ関係の整合性グループからボリュームを削除することはできません。最初にSM-BC関係を解除して整合性グループを変更してから、関係を再確立する必要があります。
- 削除処理後に整合グループ内にボリュームがない場合は、整合グループが削除されます。
- ボリュームを整合グループから削除すると、整合グループの既存のSnapshotはそのまま残りますが、無効とみなされます。既存のSnapshotを使用して整合グループの内容をリストアすることはできません。ボリューム単位のSnapshotは有効なままです。
- クラスタからボリュームを削除すると、そのボリュームは整合グループから自動的に削除されます。
- ONTAP 9.10.1または9.11.1で整合グループの設定を変更するには、整合グループを削除してから、必要なメンバーボリュームを含む新しい整合グループを作成する必要があります。
- クラスタからボリュームを削除すると、そのボリュームは整合グループから自動的に削除されます。

## System Manager の略

ONTAP 9.12.1以降では、この処理をSystem Managerで実行できます。

### 手順

1. Storage > Consistency groups \* を選択します。
2. 変更する単一または子の整合グループを選択します。
3. 整合グループから削除する個々のボリュームの横にあるチェックボックスをオンにします。
4. 「」「整合グループからボリュームを削除する」を選択します。
5. ボリュームを削除原因すると整合グループのすべてのSnapshotコピーが無効になることを確認し、「\*削除」を選択してください。

### CLI の使用

ONTAP 9.14.1以降では、CLIを使用して整合グループからボリュームを削除できます。

### ステップ

1. ボリュームを削除します。。 -volumes パラメータには、カンマで区切ったボリュームのリストを指定できます。

次のもののみを含める： -parent-consistency-group パラメータは、整合性グループが階層関係にある場合に指定します。

```
consistency-group volume remove -vserver SVM_name -consistency-group  
consistency_group_name -parent-consistency-group  
parent_consistency_group_name -volume volumes
```

## 整合グループ間でボリュームを移動します

ONTAP 9.13.1以降では、親を共有する子整合グループ間でボリュームを移動できます。

### このタスクについて

- ボリュームは、同じ親整合グループにネストされた整合グループ間でのみ移動できます。
- 既存の整合性グループSnapshotは無効になり、整合性グループSnapshotとしてアクセスできなくなります。個々のボリュームSnapshotは有効なままです。
- 親整合性グループのSnapshotコピーは引き続き有効です。
- 子整合グループからすべてのボリュームを移動すると、その整合グループは削除されます。
- 整合グループに対する変更は、に従う必要があります [整合グループの制限](#)。



## System Manager の略

ONTAP 9.12.1以降では、この処理をSystem Managerで実行できます。

### 手順

1. Storage > Consistency groups \* を選択します。
2. 移動するボリュームを含む親整合性グループを選択します。子コンシステンシグループを検索し、[\* ボリューム]メニューを展開します。移動するボリュームを選択します。
3. 移動を選択します。
4. ボリュームを新しい整合グループと既存のグループのどちらに移動するかを選択します。
  - a. 既存のコンシステンシグループに移動するには、既存の子コンシステンシグループを選択し、ドロップダウンメニューからコンシステンシグループの名前を選択します。
  - b. 新しいコンシステンシグループに移動するには、[\*新しい子コンシステンシグループ]を選択します。新しい子整合グループの名前を入力し、コンポーネントタイプを選択します。
5. 移動を選択します。

### CLI の使用

ONTAP 9.14.1以降では、ONTAP CLIを使用して整合グループ間でボリュームを移動できます。

#### 新しい子整合性グループにボリュームを移動する

1. 次のコマンドは、指定したボリュームを含む新しい子整合グループを作成します。

新しい整合グループを作成するときに、新しいSnapshot、QoS、階層化ポリシーを指定できます。

```
consistency-group volume reassign -vserver SVM_name -consistency-group  
source_child_consistency_group -parent-consistency-group  
parent_consistency_group -volume volumes -new-consistency-group  
consistency_group_name [-snapshot-policy policy -qos-policy policy -tiering  
-policy policy]
```

#### 既存の子整合性グループにボリュームを移動する

1. ボリュームを再割り当てします。。 -volumes パラメータには、ボリューム名をカンマで区切って指定できます。

```
consistency-group volume reassign -vserver SVM_name -consistency-group  
source_child_consistency_group -parent-consistency-group  
parent_consistency_group -volume volumes -to-consistency-group  
target_consistency_group
```

### 関連情報

- [整合グループの制限](#)
- [整合グループをクローニングする](#)



## コンシステンシグループジオメトリを変更します

ONTAP 9.13.1以降では、整合グループのジオメトリを変更できます。整合グループのジオメトリを変更すると、進行中のIO処理を中断することなく、子整合グループまたは親整合グループの構成を変更できます。

整合性グループのジオメトリを変更すると、既存のSnapshotコピーに影響します。



リモート保護ポリシーが設定されている整合グループのジオメトリは変更できません。最初に保護関係を解除し、ジオメトリを変更してから、リモート保護をリストアする必要があります。

## 新しい子整合グループを追加します

ONTAP 9.13.1以降では、既存の親整合グループに新しい子整合グループを追加できます。

作業を開始する前に

- 親整合グループには、最大5つの子整合グループを含めることができます。を参照してください [整合グループの制限](#) 他の制限のために。
- 1つの整合グループに子整合グループを追加することはできません。最初に実行する必要があります [\[ステートアップ\]](#) 整合グループを追加すると、子整合グループを追加できます。
- 拡張処理の前にキャプチャされた整合グループの既存のSnapshotコピーは、部分的なコピーとみなされます。このSnapshotコピーに基づくリストア処理には、Snapshotコピーのポイントインタイムの整合グループが反映されます。

### System Manager の略

ONTAP 9.13.1以降では、この処理をSystem Managerで実行できます。

1. Storage > Consistency groups \* を選択します。
2. 子整合グループを追加する親整合グループを選択します。
3. 親コンシステンシグループの名前の横にある[詳細\*]を選択してから、[新しい子コンシステンシグループの追加\*]を選択します。
4. 整合グループの名前を入力します。
5. 新しいボリュームと既存のボリュームのどちらを追加するかを選択します。
  - a. 既存のボリュームを追加する場合は、既存のボリュームを選択し、ドロップダウンメニューからボリュームを選択します。
  - b. 新しいボリュームを追加する場合は、[\*New volumes]を選択し、ボリュームの数とサイズを指定します。
6. 追加を選択します。

### CLI の使用

ONTAP 9.14.1以降では、ONTAP CLIを使用して子整合グループを追加できます。

新しいボリュームを含む子整合性グループを追加する

1. 新しい整合グループを作成します。整合グループの名前、ボリュームのプレフィックス、ボリューム数、ボリュームサイズ、ストレージサービス、 およびエクスポートポリシー名：

```
consistency-group create -vserver SVM_name -consistency-group  
consistency_group -parent-consistency-group parent_consistency_group  
-volume-prefix prefix -volume-count number -size size -storage-service  
service -export-policy policy_name
```

既存のボリュームを含む子整合性グループを追加する

1. 新しい整合グループを作成します。。 volumes パラメータには、ボリューム名をカンマで区切って指定できます。

```
consistency-group create -vserver SVM_name -consistency-group  
new_consistency_group -parent-consistency-group parent_consistency_group  
-volumes volume
```

子整合グループの接続を解除します

ONTAP 9.13.1以降では、子整合グループを親から削除して個別の整合グループに変換することができます。

作業を開始する前に

- 子整合グループの接続を解除すると、親整合グループのSnapshotが無効になり、アクセスできなくなります。ボリューム単位のSnapshotは引き続き有効です。

- 個々の整合グループの既存のSnapshotコピーは引き続き有効です。
- 接続を解除する子整合グループと同じ名前の既存の整合グループが1つある場合、この処理は失敗します。この状況が発生した場合は、整合グループの接続を解除するときに整合グループの名前を変更する必要があります。

## 例 24. 手順

### System Manager の略

ONTAP 9.13.1以降では、この処理をSystem Managerで実行できます。

1. Storage > Consistency groups \* を選択します。
2. 接続を解除する子を含む親整合性グループを選択します。
3. 分離する子コンシステンシグループの横にある[詳細\*]を選択してから、[親からの分離\*]を選択します。
4. 必要に応じて、整合グループの名前を変更し、アプリケーションタイプを選択します。
5. 切り離しを選択します。

### CLI の使用

ONTAP 9.14.1以降では、ONTAP CLIを使用して子整合グループの接続を解除できます。

1. 整合グループの接続を解除します。必要に応じて、接続解除された整合グループの名前を `-new -name` パラメータ

```
consistency-group detach -vserver SVM_name -consistency-group
child_consistency_group -parent-consistency-group parent_consistency_group
[-new-name new_name]
```

## 親整合グループの下に既存の単一の整合グループを移動する

ONTAP 9.13.1以降では、既存の単一の整合グループを子整合グループに変換できます。移動処理中に、既存の親整合グループの下に整合グループを移動するか、新しい親整合グループを作成できます。

### 作業を開始する前に

- 親整合グループには子が4つ以下である必要があります。親整合グループには、最大5つの子整合グループを含めることができます。を参照してください [整合グループの制限](#) 他の制限のために。
- この処理の前にキャプチャされた `_parent_consistency` グループの既存のSnapshotコピーは部分的なコピーとみなされます。これらのSnapshotコピーの1つに基づくリストア処理には、Snapshotコピーのポイントインタイムの整合グループが反映されます。
- 単一の整合グループの既存の整合グループSnapshotは有効なままです。

## 例 25. 手順

### System Manager の略

ONTAP 9.13.1以降では、この処理をSystem Managerで実行できます。

1. Storage > Consistency groups \* を選択します。
2. 変換する整合グループを選択します。
3. **[More\*]**を選択してから、**[Move under different consistency group]\*\***を選択します。
4. 必要に応じて、整合グループの新しい名前を入力し、コンポーネントタイプを選択します。デフォルトでは、コンポーネントタイプはOtherになります。
5. 既存の親整合グループに移行するか、新しい親整合グループを作成するかを選択します。
  - a. 既存の親コンシステンシグループに移行するには、既存のコンシステンシグループを選択し、ドロップダウンメニューからコンシステンシグループを選択します。
  - b. 新しい親コンシステンシグループを作成するには、**[\*新しいコンシステンシグループ]**を選択し、新しいコンシステンシグループの名前を指定します。
6. 移動を選択します。

### CLI の使用

ONTAP 9.14.1以降では、ONTAP CLIを使用して、親整合グループの下に1つの整合グループを移動できます。

新しい親整合グループの下に整合グループを移動する

1. 新しい親整合グループを作成します。。 -consistency-groups パラメータを指定すると、既存の整合グループが新しい親に移行されます。

```
consistency-group attach -vserver svm_name -consistency-group  
parent_consistency_group -consistency-groups child_consistency_group
```

既存の整合グループの下に整合グループを移動する

1. 整合グループを移動します。

```
consistency-group add -vserver SVM_name -consistency-group  
consistency_group -parent-consistency-group parent_consistency_group
```

### 子コンシステンシグループをプロモートします

ONTAP 9.13.1以降では、単一の整合グループを親整合グループに昇格できます。単一の整合グループを親に昇格すると、元の単一の整合グループ内のすべてのボリュームを継承する新しい子整合グループも作成されます。

作業を開始する前に

- 子整合グループを親整合グループに変換する場合は、最初に実行する必要があります **[detach]** その後、子整合グループはこの手順に従います。
- 整合グループの既存のSnapshotコピーは、整合グループを昇格したあとも有効なままです。

## 例 26. 手順

### System Manager の略

ONTAP 9.13.1以降では、この処理をSystem Managerで実行できます。

1. Storage > Consistency groups \* を選択します。
2. 昇格する整合性グループを選択します。
3. **More**を選択してから、**Promote to parent consistency group** を選択します。
4. 名前を入力し、子コンシステンシグループのコンポーネントタイプを選択します。
5. プロモートを選択します。

### CLI の使用

ONTAP 9.14.1以降では、ONTAP CLIを使用して、親整合グループの下に1つの整合グループを移動できます。

1. 整合グループを昇格します。このコマンドは、1つの親整合グループと1つの子整合グループを作成します。

```
consistency-group promote -vserver SVM_name -consistency-group  
existing_consistency_group -new-name new_child_consistency_group
```

### 親を単一の整合グループに降格します

ONTAP 9.13.1以降では、親整合グループを1つの整合グループに降格できます。親を降格すると、整合グループの階層がフラット化され、関連付けられている子整合グループがすべて削除されます。整合グループ内のすべてのボリュームは、新しい単一の整合グループに残ります。

### 作業を開始する前に

- 親整合グループの既存のSnapshotコピーは、単一整合グループに降格したあとも有効なままです。その親の関連付けられている子整合グループの既存のSnapshotコピーは無効になりますが、グループ内の個々のボリュームSnapshotはボリューム単位Snapshotとして引き続きアクセスできます。

## 例 27. 手順

### System Manager の略

ONTAP 9.13.1以降では、この処理をSystem Managerで実行できます。

1. Storage > Consistency groups \* を選択します。
2. 降格する親整合性グループを選択します。
3. **More**を選択してから **Demote to single consistency group** を選択します。
4. 関連付けられているすべての子整合グループが削除され、そのボリュームが新しい単一の整合グループの下に移動されることを示す警告が表示されます。降格を選択して、影響を理解していることを確認します。

### CLI の使用

ONTAP 9.14.1以降では、ONTAP CLIを使用して整合グループを降格できます。

1. 整合グループを降格します。オプションの `-new-name` 整合グループの名前を変更するためのパラメータ。

```
consistency-group demote -vserver SVM_name -consistency-group  
parent_consistency_group [-new-name new_consistency_group_name]
```

## アプリケーションタグとコンポーネントタグの変更

ONTAP 9.12.1以降では、コンシステンシグループでコンポーネントとアプリケーションのタギングがサポートされます。アプリケーションとコンポーネントのタグは管理ツールであり、整合グループ内のさまざまなワークロードをフィルタリングして識別できます。

このタスクについて

整合グループには、次の2種類のタグがあります。

- アプリケーションタグ:個々のコンシステンシグループと親コンシステンシグループに適用されます。アプリケーションタグは、MongoDB、Oracle、SQL Serverなどのワークロードにラベルを付けます。整合グループのデフォルトのアプリケーションタグはOtherです。
- コンポーネントタグ:階層整合グループの子には、アプリケーションタグではなくコンポーネントタグがあります。コンポーネントタグのオプションは、「data」、「logs」、または「other」です。デフォルト値はOtherです。

タグは、整合グループの作成時、または整合グループの作成後に適用できます。



整合グループにSM-BC関係がある場合は、アプリケーションタグまたはコンポーネントタグに\*other\*を使用する必要があります。

### 手順

ONTAP 9.12.1以降では、System Managerを使用してアプリケーションタグとコンポーネントタグを変更できます。ONTAP 9.14.1以降では、ONTAP CLIを使用してアプリケーションタグとコンポーネントタグを変更で

きます。

### System Manager の略

1. Storage > Consistency groups \* を選択します。
2. タグを変更する整合性グループを選択します。を選択します の横にある\*[編集]\*をクリックします。
3. ドロップダウンメニューで、適切なアプリケーションまたはコンポーネントタグを選択します。
4. [ 保存 ( Save ) ] を選択します。

### CLI の使用

ONTAP 9.14.1以降では、ONTAP CLIを使用して、既存の整合グループのアプリケーションタグまたはコンポーネントタグを変更できます。

#### アプリケーションタグの変更

1. アプリケーションタグは、限られた数のプリセット文字列を受け入れます。受け入れられた文字列のリストを確認するには、次のコマンドを実行します。  

```
consistency-group modify -vserver svm_name -consistency-group consistency_group -application-type ?
```
2. 出力から適切な文字列を選択し、整合グループを変更します。  

```
consistency-group modify -vserver svm_name -consistency-group consistency_group -application-type application_type
```

#### 構成要素タグを修正します

1. 構成要素タイプを修正します。コンポーネントタイプには、データ、ログ、またはその他があります。SM-BCを使用する場合は、「other」である必要があります。  

```
consistency-group modify -vserver svm -consistency-group child_consistency_group -parent-consistency-group parent_consistency_group -application-component-type [data|logs|other]
```

## 整合グループをクローニングする

ONTAP 9.12.1以降では、整合グループをクローニングして整合グループとその内容のコピーを作成できます。整合グループをクローニングすると、整合グループ構成のコピーと、アプリケーションタイプなどのメタデータが作成され、すべてのボリュームとその内容（ファイル、ディレクトリ、LUN、NVMeネームスペースなど）が作成されます。

#### このタスクについて

整合グループをクローニングするときは、現在の設定を使用して整合グループのクローンを作成できますが、ボリュームの内容は既存の整合グループSnapshotに基づいて作成することもできます。

整合グループのクローニングは、整合グループ全体に対してのみサポートされます。階層型関係では、個々の子整合グループをクローニングできません。クローニングできるのは、完全な整合グループ設定のみです。

整合グループをクローニングする場合、次のコンポーネントはクローニングされません。

- igroup数

- LUN マップ
- NVMe サブシステム
- NVMeネームスペースサブシステムマップ

作業を開始する前に

- 共有名を指定しない場合、整合グループをクローニングすると、クローニングされたボリューム用のSMB共有はONTAPによって作成されません。\*ジャンクションパスを指定しないと、クローン整合グループはマウントされません。
- 整合グループの現在のコンスチチュエントボリュームが反映されていないSnapshotに基づいて整合グループをクローニングしようとする、処理は失敗します。
- 整合グループのクローンを作成したら、適切なマッピング処理を実行する必要があります。

を参照してください [igroup を複数の LUN にマッピングします](#) または [NVMe ネームスペースをサブシステムにマッピングする](#) を参照してください。

- 整合グループのクローニングは、SnapMirrorビジネス継続性関係内の整合グループや、関連付けられているDPボリュームではサポートされません。



## System Manager の略

### 手順

1. Storage > Consistency groups \* を選択します。
2. [\* Consistency Group]メニューから'クローンを作成するコンシステンシ・グループ'を選択します
3. コンシステンシ・グループの概要ページの右上にある\*クローン\*を選択します
4. クローニングされた新しい整合グループの名前を入力するか、デフォルトの名前をそのまま使用します。
  - a. を有効にするかどうかを選択します **"\* シンプロビジョニング \***。
  - b. ソースから整合グループの関連付けを解除し、そのクローン整合グループに追加のディスクスペースを割り当てる場合は、**"\* Split Clone \***を選択します。
5. 現在の状態で整合グループをクローニングするには、**\*新しいSnapshotコピーを追加\***を選択します。

Snapshotに基づいて整合グループをクローニングするには、「既存の**Snapshot**コピーを使用する」を選択します。このオプションを選択すると、新しいサブメニューが開きます。クローニング処理のベースとして使用するSnapshotを選択します。

6. **"\* Clone \***」を選択します。
7. **"\* Consistency Group \***」メニューに戻り、整合グループのクローンが作成されたことを確認します。

### CLI の使用

ONTAP 9.14.1以降では、CLIを使用して整合グループをクローニングできます。

#### 整合グループをクローニングする

1. `consistency-group clone create` コマンドは、現在のポイントインタイムステータスで整合グループをクローニングします。Snapshotをベースにクローン処理を実行するには、`-source -snapshot` パラメータ

```
consistency-group clone create -vserver svm_name -consistency-group
clone_name -source-consistency-group consistency_group_name [-source-
snapshot snapshot_name]
```

### 次のステップ

- [igroup を複数の LUN にマッピングします](#)
- [NVMe ネームスペースをサブシステムにマッピングする](#)

## 整合グループを削除する

整合グループが不要になった場合は、その整合グループを削除できます。

### このタスクについて


- 整合グループを削除すると、整合グループのインスタンスが削除され、コンスティチュエントボリュームまたはLUNには影響しません。整合グループを削除しても各ボリュームの Snapshot は削除されませんが、整合グループ Snapshot としてアクセスできなくなります。ただし、Snapshotは通常のボリューム単

位のSnapshotとして引き続き管理できます。

- 整合グループ内のボリュームがすべて削除されると、ONTAPは整合グループを自動的に削除します。
- 親整合グループを削除すると、関連付けられている子整合グループがすべて削除されます。
- 9.10.1から9.12.0の間のバージョンのONTAPを使用している場合、ボリューム自体が削除された場合にのみ整合グループからボリュームを削除できます。この場合、ボリュームは整合グループから自動的に削除されます。ONTAP 9.12.1以降では、整合グループを削除せずに整合グループからボリュームを削除できます。このプロセスの詳細については、[を参照してください 整合グループを変更する](#)。

## 例 28. 手順

### System Manager の略

1. Storage > Consistency groups \* を選択します。
2. 削除する整合グループを選択します。
3. 整合グループの名前の横にあるを選択します  次に\*[削除]\*をクリックします。

### CLI の使用

ONTAP 9.14.1以降では、CLIを使用して整合グループを削除できます。

整合グループを削除する

1. 整合グループを削除します。

```
consistency-group delete -vserver svm_name -consistency-group  
consistency_group_name
```

## SnapMirror によるビジネス継続性

### SnapMirror のビジネス継続性機能の概要

SnapMirrorビジネス継続性（SM-BC）はSnapMirrorアクティブ同期とも呼ばれ、サイト全体に障害が発生してもビジネスサービスの運用を継続できるため、アプリケーションをセカンダリコピーを使用して透過的にフェイルオーバーできます。SM-BCでフェイルオーバーをトリガーするために、手動操作や追加のスクリプト作成は必要ありません。

SM-BCはONTAP 9.8以降で使用できます。SM-BCは、AFFクラスタまたはオールフラッシュSANアレイ（ASA）クラスタでサポートされます。プライマリクラスタとセカンダリクラスタにはAFFまたはASAを使用できます。SM-BCは、iSCSI LUN または FCP LUN を使用してアプリケーションを保護します。

### 利点

SM-BCには次のようなメリットがあります。

- ビジネスクリティカルなアプリケーションの継続的可用性
- 重要なアプリケーションをプライマリサイトとセカンダリサイトから交互にホストする機能
- 整合グループを使用したアプリケーション管理の簡易化により、従属書き込み順序の整合性を実現

- 各アプリケーションのフェイルオーバーをテストする機能
- アプリケーションの可用性に影響を与えることなく、ミラークローンを瞬時に作成できます
- ONTAP 9.11.1以降では、SM-BCでサポートされます。 [単一ファイルのSnapRestore](#)。
- ONTAP 9.14.1以降では、SM-BCでWindowsフェイルオーバークラスタリングと ["SCSI 3の永続的予約"](#)、高可用性の向上。

## ユースケース

アプリケーションを導入してRTO（Recovery Time Object）をゼロに

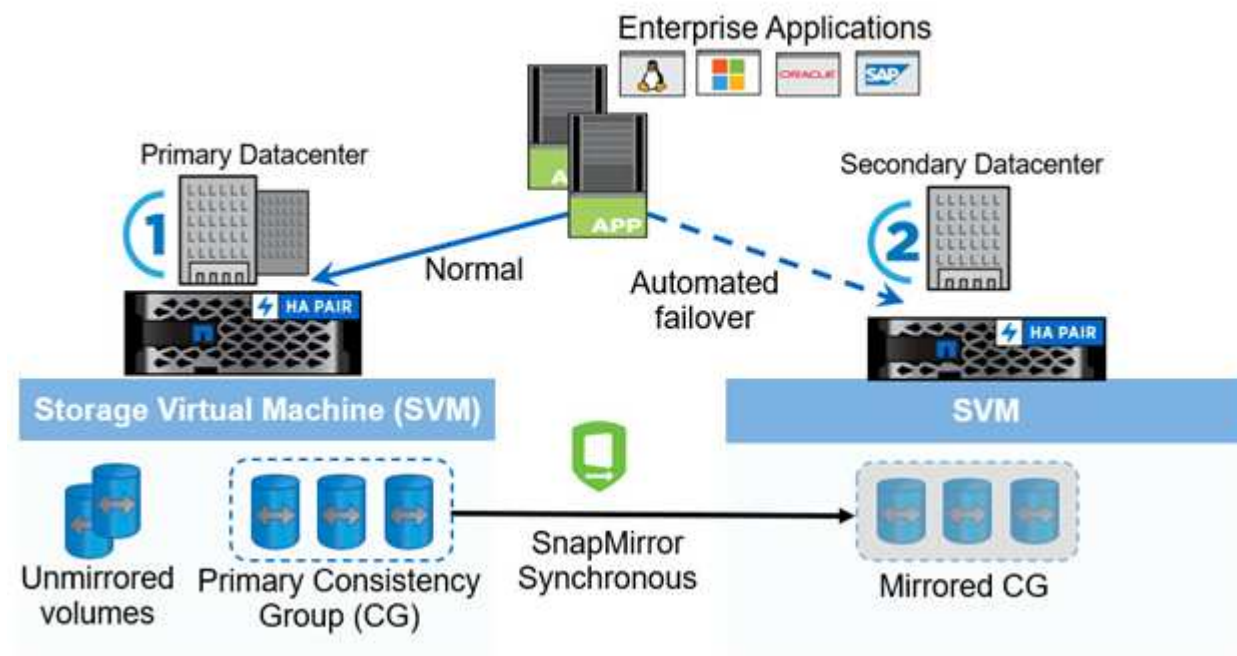
SM-BC環境では、プライマリクラスタとセカンダリクラスタを使用します。プライマリクラスタ内のLUN 1LP)は鏡を持っています (L1s) セカンダリ上。両方のLUNが同じシリアルIDを共有し、読み取り/書き込みLUNとしてホストに報告されます。ただし、読み取りおよび書き込み処理はプライマリLUNに対してのみ実行されます。1LP。ミラーへのすべての書き込み L1S プロキシによって提供されます。

## 災害シナリオ

SM-BCを使用すると、地理的に分散したサイト間で、アプリケーションの複数のボリュームを同期的にレプリケートできます。プライマリが停止した場合に自動的にセカンダリコピーにフェイルオーバーできるため、ティア1アプリケーションのビジネス継続性が実現します。

## アーキテクチャ

次の図に、 SnapMirror のビジネス継続性機能の概要を示します。



セクション1の図では、プライマリデータセンターのSVMにアプリケーションを導入しています。プライマリ整合グループに追加されたボリュームはSM-BCで保護され、セカンダリデータセンターのセカンダリ整合グループにミラーリングされます。システムが停止した場合、プライマリ整合性グループ内のボリュームはミラー整合性グループにフェイルオーバーされます。ミラー整合性グループに含まれていないボリュームは、フェイルオーバーの際に使用できません。

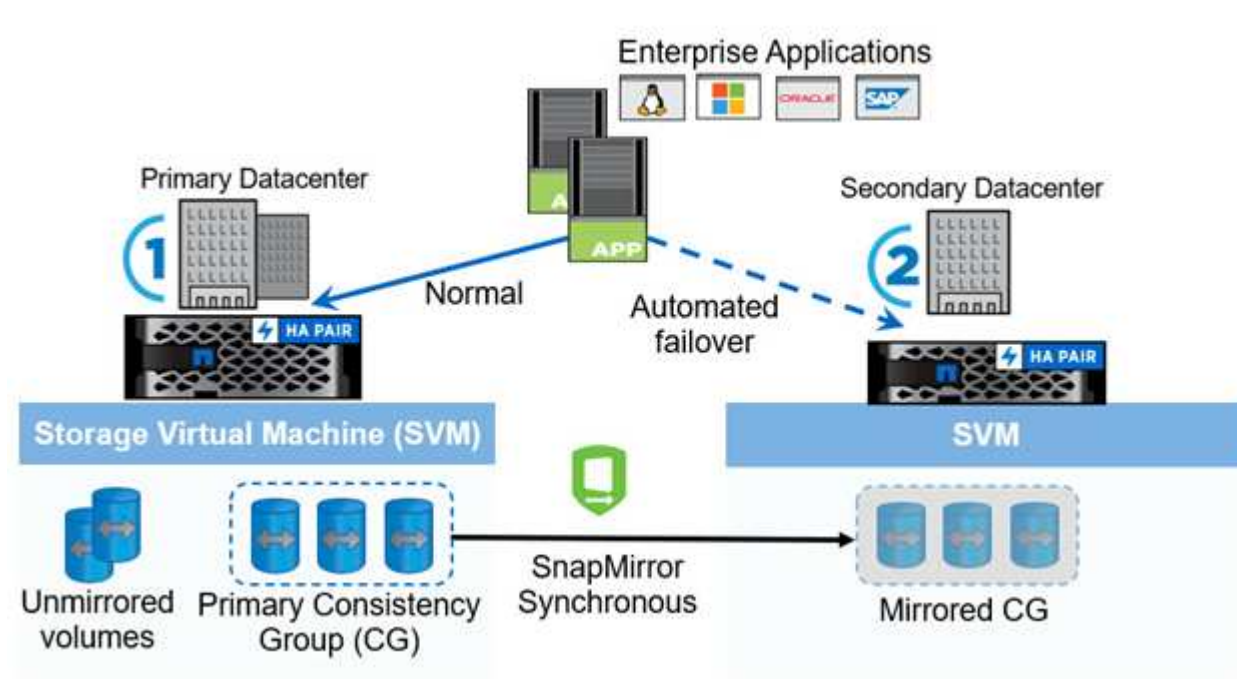
- "TR-4878 : 『SnapMirror Business Continuity』 "

## 主な概念

SnapMirrorビジネス継続性（SM-BC）は、整合グループやONTAPメディエーターなどの機能を使用して、災害が発生した場合でもデータを確実にレプリケートして提供します。SM-BCの導入を計画する際は、SM-BCとそのアーキテクチャの重要な概念を理解しておくことが重要です。

### アーキテクチャ

次の図に、SM-BC環境の概要を示します。



次の図は、プライマリデータセンターのStorage VM（SVM）でホストされているエンタープライズアプリケーションを示しています。SVMには5つのボリュームがあり、そのうちの3つは整合グループに属しています。整合グループ内の3つのボリュームがセカンダリデータセンターにミラーリングされます。通常、すべての書き込み処理はプライマリデータセンターに対して実行されます。つまり、このデータセンターがI/O処理のソースとして機能し、セカンダリデータセンターがデスティネーションとして機能します。

プライマリデータセンターで災害が発生した場合、ONTAPメディエーターはセカンダリデータセンターをプライマリとして動作させ、すべてのI/O処理を実行します。整合性グループでミラーされたボリュームのみが提供されます。SVM上の他の2つのボリュームに関する処理は、すべて災害の影響を受けます。

### 基本概念

以下の用語を理解しておくと、SM-BCを導入する際に役立ちます。

#### 整合グループ

整合グループはボリュームまたはLUNの集まりで、ビジネス継続性のために保護する必要があるアプリケーション

ョンワークロードに対して書き込み順序の整合性を保証します。整合グループを使用すると、このデータセットのすべてのボリュームが休止され、同じポイントインタイムにスナップされるため、そのデータセットのボリューム間でデータ整合性のあるリストアポイントが確立されます。

SM-BCでは、レプリケーションとデータ保護用のプライマリ整合グループとセカンダリ整合グループを作成します。システムが停止した場合は、セカンダリ整合グループがデータを提供します。

整合グループの詳細については、を参照してください。 ["整合グループの概要"](#)。

#### 構成要素

SM-BC関係で保護される整合性グループに属する個々のボリュームまたはLUN。

#### ONTAP メディエーター

ONTAPメディエーターは、2つのONTAPクラスタを監視し、プライマリストレージシステムに障害が発生した場合にフェイルオーバーをオーケストレーションします。ONTAPメディエーターを使用すると、アプリケーションがセカンダリストレージシステムのリソースに自動的に再接続されます。

ONTAPメディエーターの健全性情報を使用して、クラスタ間LIFの障害とサイト障害を区別できます。サイトが停止すると、ONTAPメディエーターは健全性情報をオンデマンドでピアクラスタに渡し、ピアクラスタのフェイルオーバーを促進します。

の詳細については、を参照してください ["ONTAP メディエーター"](#)。

#### 計画的フェイルオーバー

SM-BC 関係のコピーのロールを変更するための手動操作。プライマリサイトがセカンダリになり、セカンダリがプライマリになります。

#### 自動計画外フェイルオーバー (AUFO)

ミラーコピーへのフェイルオーバーを実行する自動処理。プライマリコピーが使用できないことをメディエーターから検出するには、処理の支援が必要です。

#### Out of Sync (OOS)

アプリケーションI/Oがセカンダリ・ストレージ・システムにレプリケートされていない場合は'**out of sync**'と報告されます非同期ステータスは、セカンダリボリュームがプライマリ（ソース）と同期されておらず、SnapMirrorレプリケーションが実行されていないことを示します。

ミラーの状態が`Snapmirrored`は、サポートされていない処理が原因で転送が失敗したことを示しています。

#### RPOはゼロです

RPOはRecovery Point Objective（目標復旧時点）の略で、所定の期間に許容可能とみなされるデータ損失量です。RPOがゼロの場合は、データ損失が許容されないことを意味します。

#### RTOゼロ

RTOはRecovery Time Objective（目標復旧時間）の略で、システム停止、障害、またはその他のデータ損失イベントが発生したあとに、アプリケーションが通常の運用に戻るのに許容できるとみなされる時間です。RTOゼロは、許容されるダウンタイムがないことを意味します。

## 計画

## 前提条件

SnapMirrorビジネス継続性の導入を計画する際には、ハードウェア、ソフトウェア、およびシステムのさまざまな構成要件を満たしていることを確認します。

### ハードウェア

- 2 ノードの HA クラスタのみがサポートされます
- 両方のクラスタが、AFF（AFF Cシリーズを含む）またはASA（混在しない）のいずれかである必要があります。

### ソフトウェア

- ONTAP 9.8以降
- ONTAP メディエーター 1.2 以降
- 次のいずれかを実行している ONTAP メディエーター用の Linux サーバまたは仮想マシン

ONTAP メディエーターのバージョン	サポートされている Linux バージョン
1.7	<ul style="list-style-type: none"><li>• Red Hat Enterprise Linux : 8.5、8.6、8.7、8.8、8.9、9.0、9.1、9.2、9.3</li><li>• Rocky Linux 8および9</li></ul>
1.6	<ul style="list-style-type: none"><li>• Red Hat Enterprise Linux : 8.4、8.5、8.6、8.7、8.8、9.0、9.1、9.2</li><li>• Rocky Linux 8および9</li></ul>
1.5	<ul style="list-style-type: none"><li>• Red Hat Enterprise Linux : 7.6、7.7、7.8、7.9、8.1、8.2、8.3、8.4、8.5</li><li>• CentOS : 7.6、7.7、7.8、7.9</li></ul>
1.4	<ul style="list-style-type: none"><li>• Red Hat Enterprise Linux : 7.6、7.7、7.8、7.9、8.1、8.2、8.3、8.4、8.5</li><li>• CentOS : 7.6、7.7、7.8、7.9</li></ul>
1.3	<ul style="list-style-type: none"><li>• Red Hat Enterprise Linux : 7.6、7.7、7.8、7.9、8.1、8.2、8.3</li><li>• CentOS : 7.6、7.7、7.8、7.9</li></ul>
1/2	<ul style="list-style-type: none"><li>• Red Hat Enterprise Linux : 7.6、7.7、7.8、8.1</li><li>• CentOS : 7.6、7.7、7.8</li></ul>

### ライセンス

- SnapMirror 同期（SM-S）ライセンスが両方のクラスタに適用されている必要があります



- 両方のクラスタに SnapMirror ライセンスが適用されている必要があります



ONTAPストレージシステムを2019年6月より前に購入した場合は、を参照してください。  
"NetApp ONTAP のマスターライセンスキー" 必要な SM-S ライセンスを取得します。

SnapMirror同期およびSnapMirrorのライセンスは、に含まれています。"ONTAP One"。

#### ネットワーク環境

- クラスタ間レイテンシのラウンドトリップ時間（RTT）は10ミリ秒未満にする必要があります。
- SCSI-3永続的予約は、SM-BCでサポートされていません\*\*。

#### サポートされているプロトコル

- サポートされるプロトコルはSANプロトコルのみです（NFS / SMBはサポートされません）。
- Fibre ChannelプロトコルとiSCSIプロトコルのみがサポートされます。
- デフォルト IPspace は、クラスタピア関係を確立するために SM-BC で必要です。カスタム IPspace はサポートされません。

#### NTFS セキュリティ形式です

NTFSセキュリティ形式は、SM-BCボリュームでは\*サポートされません。

#### ONTAP メディエーター

- ONTAPメディエーターは外部でプロビジョニングし、透過的なアプリケーションフェイルオーバーのためにONTAPに接続します。
- 完全に機能し、自動計画外フェイルオーバーを有効にするためには、外部 ONTAP メディエーターをプロビジョニングして ONTAP クラスタを設定する必要があります。
- ONTAPメディエーターは、2つのONTAPクラスタとは別の第3の障害ドメインにインストールする必要があります。
- ONTAPメディエーターをインストールするときは、自己署名証明書を信頼できる主要なCAによって署名された有効な証明書に置き換える必要があります。
- ONTAP メディエーターの詳細については、を参照してください ["ONTAP メディエーターサービスをインストールする準備をします"](#)。

#### 読み書き可能なデスティネーションボリューム

- SM-BC 関係は、読み書き可能なデスティネーションボリュームではサポートされません。読み書き可能ボリュームを使用するには、ボリュームレベルの SnapMirror 関係を作成してから関係を削除して、読み書き可能ボリュームを DP ボリュームに変換する必要があります。詳細については、を参照してください ["既存の関係を SM-BC 関係に変換します"](#)

#### LUN および大容量ボリューム

大規模なLUNと大規模なボリューム（100TBを超えるボリューム）がサポートされるかどうかは、使用しているONTAPのバージョンとプラットフォームによって異なります。

### ONTAP 9.12.1P2以降

- ONTAP 9.12.1 P2以降では、ASAおよびAFF（Cシリーズを含む）で大容量LUNと100TBを超える大容量ボリュームがサポートされます。



ONTAPリリース9.12.1P2以降では、プライマリクラスタとセカンダリクラスタの両方がオールフラッシュSANアレイまたはオールフラッシュアレイで、両方にONTAP 9.12.1 P2以降がインストールされていることを確認する必要があります。セカンダリクラスタでONTAP 9.12.1P2より前のバージョンが実行されている場合やアレイタイプがプライマリクラスタと異なる場合、プライマリボリュームが100TBを超えると同期関係が同期されなくなることがあります。

### ONTAP 9.8-9.12.1P1

- ONTAP 9.8~9.12.1 P1（P1を含む）のONTAPリリースでは、100TBを超える大容量LUNと大容量ボリュームがオールフラッシュSANアレイでのみサポートされます。



ONTAP 9.8~9.12.1 P2のONTAPリリースでは、プライマリクラスタとセカンダリクラスタの両方がオールフラッシュSANアレイで、両方にONTAP 9.8以降がインストールされていることを確認する必要があります。セカンダリクラスタでONTAP 9.8より前のバージョンが実行されている場合やオールフラッシュSANアレイでない場合、プライマリボリュームが100TBを超えると同期関係が同期されなくなることがあります。

#### 詳細情報

- ["Hardware Universe"](#)
- ["ONTAP メディエーターの概要"](#)

#### サポートされている構成と機能

SnapMirrorビジネス継続性は、ONTAPの多数のオペレーティングシステムやその他の機能と互換性があります。詳細と推奨される構成について説明します。

#### サポートされている構成

SM-BCは、次のような多数のオペレーティングシステムでサポートされています。

- AIX（ONTAP 9.11.1以降）
- HP-UX（ONTAP 9.10.1以降）
- Solaris 11.4（ONTAP 9.10.1以降）

#### AIX の場合

ONTAP 9.11.1以降では、SM-BCでAIXがサポートされます。AIX構成では、プライマリクラスタが「アクティブ」クラスタになります。

AIX構成では、フェイルオーバー時にシステムが停止します。フェイルオーバーが発生するたびに、ホストで再スキャンを実行してI/O処理を再開する必要があります。



SM-BCでAIXホストを設定する方法については、ナレッジベースの記事を参照してください "[SnapMirrorのビジネス継続性を実現するためのAIXホストの構成方法（SM-BC）](#)"。

## HP-UX

ONTAP 9.10.1 以降では、HP-UX 用の SM-BC がサポートされています。

### HP-UXでの制限事項

分離されたマスタークラスタでの自動計画外フェイルオーバー（AUFO）イベントは、プライマリクラスタとセカンダリクラスタの間の接続が失われ、プライマリクラスタとメディアーターの間の接続も失われた場合に、二重イベントの障害が原因で発生することがあります。これは、他の AUFO イベントとは異なり、まれなイベントとみなされます。

- このシナリオでは、HP-UXホストでI/Oが再開されるまでに120秒以上かかることがあります。実行中のアプリケーションによっては、I/O の中断やエラーメッセージが発生しない場合があります。
- 修正するには、中断許容時間が120秒未満のHP-UXホストでアプリケーションを再起動する必要があります。

### Solarisホスト設定の推奨事項

ONTAP 9.10.1 以降、SM-BC は Solaris 11.4 をサポートします。

SM-BC環境で計画外サイトフェイルオーバースイッチオーバーが発生した場合にSolarisクライアントアプリケーションが無停止で実行されるようにするには、Solaris OSのデフォルト設定を変更します。推奨設定でSolarisを構成するには、ナレッジベースの記事を参照してください。"[Solaris ホストでは、SnapMirror Business Continuity（SM-BC）構成での推奨設定がサポートされます](#)"。

### Windowsフェイルオーバークラスタリング

ONTAP 9.14.1以降では、SM-BCでWindowsフェイルオーバークラスタリングがサポートされます。詳細については、を参照してください "[TR-4878：『SnapMirror Business Continuity』](#)"。

### ONTAPとの統合

SM-BCでは、ONTAPの次の機能をサポートしています。

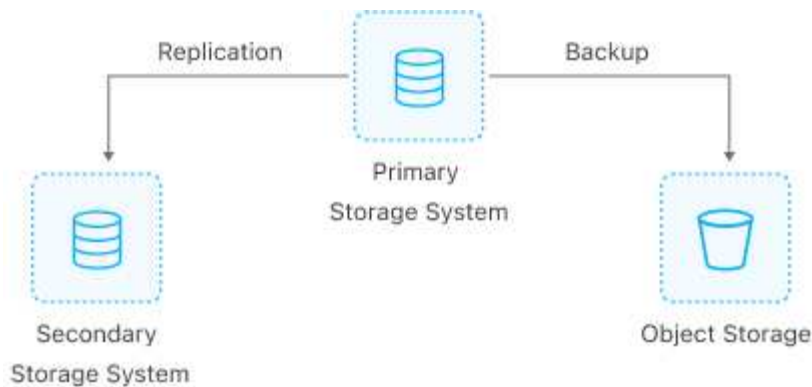
- ファンアウト構成
- NDMPコピー（ONTAP 9.13.1以降）
- 部分的なファイルのリストア（ONTAP 9.12.1以降）

### FabricPool

SM-BCでは、FabricPool アグリゲートのソースボリュームとデスティネーションボリュームの階層化ポリシーが「なし」、「Snapshot」、または「自動」に設定されています。SM-S SM-BCでは、階層化ポリシーを「すべて」に設定したFabricPool アグリゲートはサポートされません。

### ファンアウト構成

インA [ファンアウト構成](#)ソースボリュームは、SM-BCデスティネーションエンドポイントおよび1つ以上の非同期SnapMirror関係にミラーリングできます。



SM-BC はサポートしています [ファンアウト構成](#) を使用 MirrorAllSnapshots ポリシーおよび（ONTAP 9.11.1以降） MirrorAndVault ポリシー：のSM-BCでは、ファンアウト構成がサポートされません XDPDefault ポリシー：

ファンアウト構成のSM-BCデスティネーションでフェイルオーバーが発生した場合は、手動で [ファンアウト構成で保護を再開します](#)。

### NDMPリストア

ONTAP 9.13.1以降では、NDMPを使用してSM-BCでデータをコピーおよびリストアできます。NDMPを使用すると、保護を一時停止することなくデータをSM-BCソースに移動してリストアを完了できます。これは、ファンアウト構成で特に便利です。

このプロセスの詳細については、を参照してください [NDMPコピーを使用してデータを転送します](#)。

ファイルの一部をリストアします

ONTAP 9.12.1以降では、SM-BCボリュームで部分的なLUNリストアがサポートされます。このプロセスの詳細については、を参照してください ["Snapshot コピーからファイルの一部をリストアします"](#)。

### SnapMirrorビジネス継続性のオブジェクト制限

SnapMirrorビジネス継続性を使用および管理する場合は、次の制限事項に注意してください。

クラスタ内の整合グループ

SM-BCを使用するクラスタの整合グループの制限は、関係に基づいて計算され、使用するONTAP のバージョンによって異なります。制限はプラットフォームに依存しません。

ONTAPバージョン	関係の最大数
ONTAP 9.8~9.9.1	5.
ONTAP 9.10.1	20
ONTAP 9.11.1以降	50です

整合性グループあたりのボリューム数

SM-BCを使用する場合、整合グループあたりの最大ボリューム数はプラットフォームに依存しません。

ONTAPバージョン	整合性グループ関係でサポートされる最大ボリューム数
ONTAP 9.8~9.9.1	12
ONTAP 9.10.1 以降	16

#### 個のボリューム

SM-BCのボリューム制限は、関係の数ではなく、エンドポイントの数に基づいて計算されます。12個のボリュームで構成される整合グループは、プライマリクラスタとセカンダリクラスタの両方のエンドポイントを12個提供します。エンドポイントの総数は、SM-BC 関係と SnapMirror Synchronous 関係のどちらも関係します。

プラットフォームあたりの最大エンドポイント数を次の表に示します。

...いいえ	プラットフォーム	SM-BC の HA あたりのエンドポイント数			HA ごとの全体的な同期エンドポイントと SM-BC エンドポイント		
		ONTAP 9.8~9.9.1	ONTAP 9.10.1	ONTAP 9.11.1以降	ONTAP 9.8~9.9.1	ONTAP 9.10.1	ONTAP 9.11.1以降
1.	AFF	60ドルだ	200	400	80	200	400
2.	ASA	60ドルだ	200	400	80	200	400

#### SAN オブジェクトの制限

SANオブジェクトの制限を次の表に示します。これらの制限は、プラットフォームに関係なく適用されます。

SM-BC関係のオブジェクト	カウント
ボリュームあたりの LUN 数	256
ノードあたりの LUN マップ数	<ul style="list-style-type: none"> <li>• 4096 (ONTAP 9.10以降)</li> <li>• 2048 (ONTAP 9.9.1以前)</li> </ul>
クラスタあたりの LUN マップ数	<ul style="list-style-type: none"> <li>• 8192 (ONTAP 9.10以降)</li> <li>• 4096 (ONTAP 9.9.1以前)</li> </ul>
SVMあたりのLIF数 (少なくとも1つのボリュームがSM-BC関係にある場合)	256
ノードごとにクラスタ間 LIF を設定します	4.
クラスタごとにインタークラスタ LIF を設定します	8

#### 関連情報

- ["Hardware Universe"](#)
- ["整合グループの制限"](#)

## インストールとセットアップ

### SnapMirrorビジネス継続性を実現するためのONTAPメディエーターとクラスタの設定

SnapMirrorビジネス継続性（SM-BC）は、フェイルオーバー時にデータの可用性を確保するためにピアクラスタを利用します。ONTAPメディエーターは、ビジネス継続性を確保するための重要なリソースであり、各クラスタの健全性を監視します。SM-BCを設定するには、まずONTAPメディエーターをインストールし、プライマリクラスタとセカンダリクラスタが適切に設定されていることを確認する必要があります。

ONTAPメディエーターをインストールしてクラスタを設定したら、次の手順を実行する必要があります。[\[initialize-the-ontap-mediator\]](#) SM-BCで使用するONTAPメディエーター。次の手順に従ってください。 [SM-BCの整合性グループを作成、初期化、マッピングする](#)

#### ONTAP メディエーター

ONTAP メディエーターは、SM-BC 関係にある ONTAP クラスタのフォーラムを確立します。障害が検出された場合に自動フェイルオーバーを調整し、プライマリとして機能するクラスタを特定して、正しいデスティネーションとの間でデータが提供されるようにします。

#### ONTAP メディエーターの前提条件

- ONTAP メディエーターには独自の前提条件があります。メディエーターをインストールするには、あらかじめこれらの前提条件を満たしている必要があります。

詳細については、を参照してください ["ONTAP メディエーターサービスをインストールする準備をします"](#)。

- ONTAP メディエーターは、デフォルトでは TCP ポート 31784 を使用してサービスを提供します。ONTAP クラスタとメディエーターの間でポート 31784 が開いて使用可能であることを確認する必要があります。

#### ONTAPメディエーターをインストールしてクラスタ構成を確認

次の各手順を実行します。手順ごとに、特定の設定が実行されたことを確認する必要があります。各手順のあとに記載されたリンクを使用して、必要に応じて詳細を確認します。

#### 手順

1. ソースクラスタとデスティネーションクラスタが正しく設定されていることを確認するために、ONTAP メディエーターサービスをインストールします。

#### [ONTAP メディエーターサービスのインストールまたはアップグレードを準備します](#)

2. クラスタ間にクラスタピア関係が存在することを確認します。



デフォルト IPspace は、クラスタピア関係を確立するために SM-BC で必要です。カスタムIPspaceはサポートされません。

#### [ピア関係を設定](#)

3. 各クラスタに Storage VM が作成されていることを確認します。

### SVM を作成する

4. 各クラスタの Storage VM 間にピア関係が存在することを確認します。

### SVM ピア関係を作成

5. LUN に対応するボリュームが存在することを確認します。

### ボリュームを作成します

6. クラスタ内の各ノードに少なくとも 1 つの SAN LIF が作成されていることを確認します。

### "クラスタ SAN 環境での LIF に関する注意事項"

### "LIF を作成する"

7. 必要なLUNが作成され、igroupにマッピングされていることを確認します。igroupは、アプリケーションホストのイニシエータにLUNをマッピングするために使用されます。

### LUN を作成して igroup をマッピングします

8. アプリケーションホストを再スキャンして新しい LUN を検出します。

### SM-BCのONTAPメディアエーターを初期化する

ONTAPメディアエーターをインストールしてクラスタ構成を確認したら、クラスタの監視用にONTAPメディアエーターを初期化する必要があります。ONTAPメディアエーターは、System ManagerまたはONTAP CLIを使用して初期化できます。

## System Manager の略

System Managerでは、自動フェイルオーバー用にONTAPメディエーターサーバを設定できます。自己署名 SSL および CA をサードパーティによる検証済み SSL 証明書および CA に置き換えていない場合は、CA に置き換えることもできます。

### 手順

1. [\* Protection] > [Overview] > [Mediator] > [Configure] \* に移動します。
2. [追加]\*を選択し、次のONTAPメディエーターサーバ情報を入力します。
  - IPv4 アドレス
  - ユーザ名
  - パスワード
  - 証明書

## CLI の使用

ONTAPメディエーターは、ONTAP CLIを使用してプライマリクラスタまたはセカンダリクラスタから初期化できます。問題 を実行すると mediator add コマンド一方のクラスタでは、もう一方のクラスタにONTAPメディエーターが自動的に追加されます。

### 手順

1. いずれかのクラスタでメディエーターを初期化します。

```
snapmirror mediator add -mediator-address IP_Address -peer-cluster  
cluster_name -username user_name
```

◦ 例 \*

```
cluster1::> snapmirror mediator add -mediator-address 192.168.10.1  
-peer-cluster cluster2 -username mediatoradmin  
Notice: Enter the mediator password.  
  
Enter the password: *****  
Enter the password again: *****
```

2. メディエーター設定のステータスを確認します。

```
snapmirror mediator show
```

Mediator Address	Peer Cluster	Connection Status	Quorum Status
192.168.10.1	cluster-2	connected	true

Quorum Status SnapMirror整合性グループ関係がメディエーターと同期されているかどうかを示します。ステータスは true 同期が成功したことを示します

## SnapMirrorビジネス継続性による保護

SnapMirrorビジネス継続性を使用した保護を設定するには、ONTAPソースクラスタでLUNを選択して整合グループに追加します。

作業を開始する前に

- を用意しておく必要があります ["SnapMirror Synchronous ライセンス"](#)。
- クラスタ管理者または Storage VM 管理者である必要があります。
- 整合性グループ内のコンスチチュエントボリュームは、すべて1つのStorage VM（SVM）に含まれている必要があります。
  - LUN は異なるボリュームに配置できます。
- ソースとデスティネーションのクラスタを同じにすることはできません。
- ASAクラスタとASA以外のクラスタの間でSM-BC整合性グループ関係を確立することはできません。
- デフォルト IPspace は、クラスタピア関係を確立するために SM-BC で必要です。カスタム IPspace はサポートされません。
- 整合グループの名前は一意である必要があります。
- セカンダリ（デスティネーション）クラスタ上のボリュームのタイプはDPである必要があります。
- プライマリとセカンダリのSVMでピア関係が確立されている必要があります。

手順

ONTAP CLIまたはSystem Managerを使用して整合グループを設定できます。

ONTAP 9.10.1以降では、ONTAPに追加の管理ユーティリティを提供する整合グループエンドポイントと整合グループメニューがSystem Managerに用意されています。ONTAP 9.10.1以降を使用している場合は、[こちら](#)を参照してください。 ["整合グループの設定"](#) そうすると ["保護の設定"](#) をクリックしてSM-BC関係を作成してください。

## System Manager の略

1. プライマリクラスタで、\*[保護]>[概要]>[ビジネス継続性のための保護]>[LUNの保護]\*に移動します。
2. 保護するLUNを選択し、保護グループに追加します。
3. デスティネーションクラスタと SVM を選択
4. \* 初期化関係 \* がデフォルトで選択されています。[ 保存 ( Save ) ] をクリックして保護を開始します。
5. [Dashboard] > [Performance] に移動して、LUN の IOPS アクティビティを確認します。
6. デスティネーションクラスタで、System Manager を使用して、ビジネス継続性関係の保護が同期されていることを確認します。 \* Protection > Relationships \*。

## CLI の使用

1. デスティネーションクラスタから整合性グループ関係を作成

```
'デスティネーション： :> snapmirror create -source-path _source-path_-destination-path_-destination-path_-cg-item-mappings _volume-paths _policy _policy-name_
```

を使用して最大12個のコンスチチュエントボリュームをマッピングできます。 cg-item-mappings のパラメータ snapmirror create コマンドを実行します

次の例では、2つの整合グループを作成します。 cg\_src\_ on the source with `vol1 および vol2 ミラーされたデスティネーション整合グループ cg\_dst。

```
destination::> snapmirror create -source-path vs1_src:/cg/cg_src  
-destination-path vs1_dst:/cg/cg_dst -cg-item-mappings  
vol_src1:@vol_dst1,vol_src2:@vol_dst2 -policy AutomatedFailOver
```

2. デスティネーションクラスタから、整合性グループを初期化します。

```
destination::>snapmirror initialize -destination-path destination-  
consistency-group
```

3. 初期化処理が正常に完了したことを確認します。ステータスがになっている必要があります InSync。

```
snapmirror show
```

4. 各クラスタにigroupを作成して、アプリケーションホストのイニシエータにLUNをマッピングします。

```
lun igroup create -igroup name -protocol fcp|iscsi -ostype os -initiator  
initiator_name
```

5. 各クラスタで、LUNをigroupにマッピングします。

```
lun map -path path_name -igroup igroup_name
```

6. LUNマッピングが次のコマンドで正常に完了したことを確認： lun map コマンドを実行しますその後、アプリケーションホストで新しいLUNを検出できます。



## SM-BCの管理とデータの保護

共通の **Snapshot** コピーを作成します。

定期的なSnapshotコピー処理のほかに、共通のSnapshotコピーを手動で作成することもできます。 **"Snapshot コピー"** プライマリSnapMirror整合性グループ内のボリュームとセカンダリSnapMirror整合性グループ内のボリューム間。

このタスクについて

- ONTAP 9.8 では、スケジュールされている Snapshot 作成間隔は 1 時間です。

ONTAP 9.9.1以降では、この間隔は12時間です。

作業を開始する前に

- SnapMirror グループ関係が同期されている必要があります。

手順

1. 共通の Snapshot コピーを作成します。

```
destination::>snapmirror update -destination-path vs1_dst:/cg/cg_dst
```

2. 更新の進捗を監視します。

```
destination::>snapmirror show -fields -newest-snapshot
```

計画的フェイルオーバーを実行

計画的フェイルオーバーでは、プライマリクラスタからセカンダリクラスタがテイクオーバーされるように、プライマリクラスタとセカンダリクラスタのロールを切り替えます。フェイルオーバー中は、通常はセカンダリクラスタがクライアントの処理を中断せずにローカルで入出力要求を処理します。

計画的フェイルオーバーを実行して、ディザスタリカバリ構成の健全性をテストしたり、プライマリクラスタでメンテナンスを実行したりすることができます。

このタスクについて

計画的フェイルオーバーは、セカンダリクラスタの管理者が開始します。この処理を実行するには、セカンダリクラスタがプライマリからテイクオーバーするように、プライマリとセカンダリのロールを切り替える必要があります。新しいプライマリクラスタは、クライアントの処理を中断することなく、ローカルで入出力要求の処理を開始できます。

作業を開始する前に

- SM-BC関係が同期されている必要があります。
- ノンストップオペレーションの実行中は、計画的フェイルオーバーを開始できません。ノンストップオペレーションには、ボリュームの移動、アグリゲートの再配置、ストレージフェイルオーバーなどがあります。
- ONTAPメディアエーターが設定され、接続され、クォーラムを構成している必要があります。

計画的フェイルオーバーは、ONTAP CLIまたはSystem Managerを使用して実行できます。

#### System Manager の略

1. System Managerで、[\*Protection]>[Overview]>[Relationships]の順に選択します。
2. フェイルオーバーするSM-BC関係を特定します。名前の横にある ... 関係の名前の横にある[\*Failover]を選択します。
3. フェイルオーバーのステータスを監視するには、`snapmirror failover show` ONTAP CLIを使用します。

#### CLI の使用

1. デスティネーションクラスタから、フェイルオーバー処理を開始します。

```
destination::>snapmirror failover start -destination-path  
vs1_dst:/cg/cg_dst
```

2. フェイルオーバーの進捗を監視します。

```
destination::>snapmirror failover show
```

3. フェイルオーバー処理が完了したら、デスティネーションから同期 SnapMirror 保護関係のステータスを監視できます。

```
destination::>snapmirror show
```

#### 自動計画外フェイルオーバー処理からのリカバリ

自動計画外フェイルオーバー（AUFO）処理は、プライマリクラスタが停止しているか分離されている場合に実行されます。ONTAPメディアエーターは、フェイルオーバーの発生を検出し、セカンダリクラスタへの自動計画外フェイルオーバーを実行します。セカンダリクラスタがプライマリに変換され、クライアントへのサービス提供が開始されます。この処理は、ONTAP メディアエーターからのみ実行します。




自動計画外フェイルオーバーの実行後は、I/O パスが失われないようにホスト LUN I/O パスを再スキャンすることが重要です。

#### 計画外フェイルオーバー後の保護関係の再確立

保護関係は、System ManagerまたはONTAP CLIを使用して再確立できます。

## System Manager の略

### 手順

1. [\*Protection] > [Relationships] に移動し、関係の状態が [InSync ( InSync ) ] になるまで待ちます。
2. 元のソースクラスタで処理を再開するには、をクリックします  をクリックし、 \* Failover \* を選択します。

### CLI の使用

自動計画外フェイルオーバーのステータスは、 `snapmirror failover show` コマンドを実行します

例：

```
ClusterB::> snapmirror failover show -instance
Start Time: 9/23/2020 22:03:29
      Source Path: vs1:/cg/scg3
Destination Path: vs3:/cg/dcg3
Failover Status: completed
      Error Reason:
      End Time: 9/23/2020 22:03:30
Primary Data Cluster: cluster-2
Last Progress Update: -
      Failover Type: unplanned
Error Reason codes: -
```

を参照してください ["EMS参照"](#) をクリックして、イベントメッセージおよび対処方法について確認してください。

フェイルオーバー後にファンアウト構成で保護を再開する

SM-BC関係のセカンダリクラスタでフェイルオーバーが発生すると、非同期SnapMirrorデスティネーションは正常な状態でなくなります。非同期SnapMirrorエンドポイントとの関係を削除して再作成し、保護を手動でリストアする必要があります。

### 手順

1. フェイルオーバーが正常に完了したことを確認します。  
`snapmirror failover show`
2. 非同期SnapMirrorエンドポイントで、ファンアウトエンドポイントを削除します。  
`snapmirror delete -destination-path destination_path`
3. 3番目のサイトで、新しいSM-BCプライマリボリュームと非同期ファンアウトデスティネーションボリュームの間に非同期SnapMirror関係を作成します。  
`snapmirror create -source-path source_path -destination-path destination_path -policy MirrorAllSnapshots -schedule schedule`
4. 関係を再同期します。  
`snapmirror resync -destination-path destination_path`

5. 関係のステータスと健全性を確認します。

```
snapmirror show
```

### SnapMirrorビジネス継続性処理の監視

次のSnapMirrorビジネス継続性（SM-BC）処理を監視して、SM-BC構成の健全性を確保できます。

- ONTAP メディエーター
- 計画的フェイルオーバー処理
- 自動計画外フェイルオーバー処理
- SM-BC の可用性

#### ONTAP メディエーター

通常運用時は、ONTAPメディエーターの状態は「connected」になります。それ以外の状態の場合は、エラー状態を示している可能性があります。を確認します ["Event Management System（EMS；イベント管理システム）メッセージ"](#) エラーと適切な対処方法を特定します。

#### 計画的フェイルオーバー処理

を使用して、計画的フェイルオーバー処理のステータスと進捗状況を監視できます `snapmirror failover show` コマンドを実行します例：

```
ClusterB::> snapmirror failover start -destination-path vs1:/cg/dcg1
```

フェイルオーバー処理が完了したら、新しいデスティネーションクラスタから同期 SnapMirror 保護のステータスを監視できます。例：

```
ClusterA::> snapmirror show
```

を参照してください ["EMS参照"](#) をクリックしてイベントメッセージと対処方法を確認してください。

#### 自動計画外フェイルオーバー処理

自動計画外フェイルオーバーの実行中は、を使用して処理のステータスを監視できます `snapmirror failover show` コマンドを実行します

```
ClusterB::> snapmirror failover show -instance
Start Time: 9/23/2020 22:03:29
    Source Path: vs1:/cg/scg3
    Destination Path: vs3:/cg/dcg3
    Failover Status: completed
    Error Reason:
        End Time: 9/23/2020 22:03:30
Primary Data Cluster: cluster-2
Last Progress Update: -
    Failover Type: unplanned
Error Reason codes: -
```

を参照してください ["EMS参照"](#) をクリックして、イベントメッセージおよび対処方法について確認してください。

#### **SM-BC** の可用性

SM-BC 関係の可用性は、プライマリクラスタまたはセカンダリクラスタ、あるいはその両方で一連のコマンドを使用して確認できます。

使用するコマンドには、があります `snapmirror mediator show` プライマリクラスタとセカンダリクラスタの両方でコマンドを実行し、接続とクォーラムステータスを確認します `snapmirror show` コマンド、および `volume show` コマンドを実行します例：

```

SMBC_A::*> snapmirror mediator show
Mediator Address Peer Cluster      Connection Status Quorum Status
-----
10.236.172.86    SMBC_B      connected      true

SMBC_B::*> snapmirror mediator show
Mediator Address Peer Cluster      Connection Status Quorum Status
-----
10.236.172.86    SMBC_A      connected      true

SMBC_B::*> snapmirror show -expand

Progress
Source          Destination Mirror Relationship Total
Last
Path            Type Path            State Status          Progress Healthy
Updated
-----
-----
vs0:/cg/cg1 XDP vs1:/cg/cg1_dp Snapmirrored InSync -          true -
vs0:vol1     XDP vs1:vol1_dp   Snapmirrored InSync -          true -
2 entries were displayed.

SMBC_A::*> volume show -fields is-smbc-master,smbc-consensus,is-smbc-
failover-capable -volume vol1
vserver volume is-smbc-master is-smbc-failover-capable smbc-consensus
-----
vs0      vol1      true          false          Consensus

SMBC_B::*> volume show -fields is-smbc-master,smbc-consensus,is-smbc-
failover-capable -volume vol1_dp
vserver volume is-smbc-master is-smbc-failover-capable smbc-consensus
-----
vs1      vol1_dp false          true          No-consensus

```

## 整合性グループへのボリュームの追加または削除

アプリケーションワークロードの要件が変化した場合は、ビジネス継続性を確保するために、整合グループに対してボリュームの追加や削除が必要になることがあります。アクティブなSM-BC関係のボリュームを追加および削除するプロセスは、使用しているONTAPのバージョンによって異なります。

ほとんどの場合、停止を伴うプロセスです。このプロセスでは、SnapMirror関係を解除し、整合グループを変更してから保護を再開する必要があります。ONTAP 9.13.1以降では、アクティブなSM-BC関係を持つ整合グループにボリュームを追加する処理は無停止で実行されます。

#### このタスクについて

- ONTAP 9.8~9.9.1では、ONTAP CLIを使用して整合グループにボリュームを追加または削除できます。
- ONTAP 9.10.1 以降では、を管理することを推奨します ["整合グループ"](#) System Manager または ONTAP REST API を使用

ボリュームを追加または削除して整合グループの構成を変更する場合は、最初に元の関係を削除してから、新しい構成で整合グループを作成し直す必要があります。

- ONTAP 9.13.1以降では、ソースまたはデスティネーションからアクティブなSM-BC関係を持つ整合性グループに無停止でボリュームを追加できます。

ボリュームの削除はシステム停止を伴う処理です。ボリュームの削除を続行する前に、SnapMirror関係を解除する必要があります。

## ONTAP 9.8-9.13.0

作業を開始する前に

- 整合グループが内にある間に変更を開始できません。 InSync 状態。
- デスティネーションボリュームのタイプは DP でなければなりません。
- 整合性グループを拡張するために追加する新しいボリュームには、ソースボリュームとデスティネーションボリュームの間に共通の Snapshot コピーのペアが必要です。

手順

2つのボリュームマッピングで示されている例は次のとおりです。 vol\_src1 ↔ vol\_dst1 および vol\_src2 ↔ vol\_dst2、エンドポイント間の整合性グループ関係 vs1\_src:/cg/cg\_src および vs1\_dst:/cg/cg\_dst。

1. ソースクラスタとデスティネーションクラスタで、コマンドを使用して、ソースクラスタとデスティネーションクラスタの間に共通のSnapshotがあることを確認します。 snapshot show -vserver svm\_name -volume volume\_name -snapshot snapmirror

```
source::>snapshot show -vserver vs1_src -volume vol_src3 -snapshot snapmirror*
```

```
destination::>snapshot show -vserver vs1_dst -volume vol_dst3 -snapshot snapmirror*
```

2. 共通の Snapshot コピーが存在しない場合は、FlexVol の SnapMirror 関係を作成して初期化します。

```
destination::>snapmirror initialize -source-path vs1_src:vol_src3 -destination-path vs1_dst:vol_dst3
```

3. 整合性グループ関係を削除します。

```
destination::>snapmirror delete -destination-path vs1_dst:vol_dst3
```

4. ソース SnapMirror 関係を解放し、共通の Snapshot コピーを保持します。

```
source::>snapmirror release -relationship-info-only true -destination-path vs1_dst:vol_dst3
```

5. LUN のマッピングを解除し、既存の整合グループ関係を削除します。

```
destination::>lun mapping delete -vserver vs1_dst -path <lun_path> -igroup <igroup_name>
```



デスティネーション LUN はマッピング解除されますが、プライマリコピー上の LUN はホスト I/O を処理し続けます

```
destination::>snapmirror delete -destination-path vs1_dst:/cg/cg_dst
```

```
source::>snapmirror release -destination-path vs1_dst:/cg/cg_dst -relationship-info-only true
```



6. **ONTAP 9.10.1～9.13.0**を使用している場合は'ソースのコンシステンシ・グループを正しいコンポジションで削除して再作成しますの手順に従います [整合グループを削除する](#) 次に [単一の整合グループを設定する](#)。ONTAP 9.10.1以降では、System ManagerまたはONTAP REST APIで削除および作成の処理を実行する必要があります。CLI手順 はありません。

◦ ONTAP 9.8、9.0、または9.9.8.1を使用している場合は、次の手順に進みます。 \*\*

7. 新しい構成を使用して新しい整合グループをデスティネーションに作成します。

```
destination::>snapmirror create -source-path vs1_src:/cg/cg_src  
-destination-path vs1_dst:/cg/cg_dst -cg-item-mappings vol_src1:@vol_dst1,  
vol_src2:@vol_dst2, vol_src3:@vol_dst3
```

8. ゼロ RTO 整合グループ関係を再同期し、同期されていることを確認します。

```
destination::>snapmirror resync -destination-path vs1_dst:/cg/cg_dst
```

9. 手順 5 でマッピング解除した LUN を再マッピングします。

```
destination::> lun map -vserver vs1_dst -path lun_path -igroup igroup_name
```


10. ホスト LUN の I/O パスを再スキャンして、LUN へのすべてのパスをリストアします。

#### ONTAP 9.13.1以降

ONTAP 9.13.1以降では、アクティブなSM-BC関係を持つ整合性グループに無停止でボリュームを追加できます。SM-BCでは、ソースとデスティネーションの両方からボリュームを追加できます。

ソース整合性グループからのボリュームの追加の詳細については、を参照してください [整合グループを変更する](#)。

デスティネーションクラスタからボリュームを追加

1. デスティネーションクラスタで、**Protection> Relationships**を選択します。
2. ボリュームを追加するSM-BC関係を探します。選択するオプション  次に、展開。
3. 整合性グループにボリュームを追加するボリューム関係を選択します
4. [\*展開]を選択します。

既存の関係を **SM-BC** 関係に変換します

ソースクラスタとデスティネーションクラスタの間に既存の同期SnapMirror関係がある場合は、SM-BC関係に変換できます。これにより、ミラーボリュームを整合グループに関連付けることができ、マルチボリュームワークロード全体でRPOをゼロにすることができます。また、SM-BC関係を確立する前に特定の時点にリバートする必要がある場合は、既存のSnapMirror Snapshotを保持できます。

作業を開始する前に

- プライマリクラスタとセカンダリクラスタの間にRPOゼロの同期SnapMirror関係が存在している必要があります。
- RTOゼロのSnapMirror関係を作成するには、デスティネーションボリューム上のすべてのLUNのマッピン

グを解除する必要があります。

- SM-BC がサポートするのは SAN プロトコルだけです（NFS / CIFS はサポートしません）。NAS アクセス用に整合性グループのコンスティチュエントがマウントされていないことを確認します。

このタスクについて

- プライマリクラスタとセカンダリクラスタのクラスタ管理者およびSVM管理者である必要があります。
- SnapMirror ポリシーを変更して、ゼロ RPO をゼロ RTO 同期に変換することはできません。
- を実行する前に、LUNのマッピングが解除されていることを確認する必要があります snapmirror create コマンドを実行します

セカンダリボリュームの既存のLUNがマッピングされており、AutomatedFailover ポリシーが設定され、snapmirror create エラーが発生します。

手順

1. セカンダリクラスタから、既存の関係に対してSnapMirror更新を実行します。

```
destination:>snapmirror update -destination-path vs1_dst:vol1
```

2. SnapMirror の更新が正常に完了したことを確認します。

```
destination:>snapmirror show
```

3. RPO ゼロの各同期関係を休止します。

```
destination:>snapmirror quiesce -destination-path vs1_dst:vol1
```

```
destination:>snapmirror quiesce -destination-path vs1_dst:vol2
```

4. RPO ゼロの同期関係をそれぞれ削除します。

```
destination:>snapmirror delete -destination-path vs1_dst:vol1
```

```
destination:>snapmirror delete -destination-path vs1_dst:vol2
```

5. ソース SnapMirror 関係を解放しますが、共通の Snapshot コピーが保持されます。

```
source:>snapmirror release -relationship-info-only true -destination-path vs1_dst:vol1
```

```
source:>snapmirror release -relationship-info-only true -destination-path vs1_dst:vol2
```

6. グループゼロの RTO Synchronous SnapMirror 関係を作成します。

```
destination:> snapmirror create -source-path vs1_src:/cg/cg_src -destination-path vs1_dst:/cg/cg_dst -cg-item-mappings vol1:@vol1,vol2:@vol2 -policy AutomatedFailover
```

7. 整合グループを再同期します。

```
destination::> snapmirror resync -destination-path vs1_dst:/cg/cg_dst
```

8. ホスト LUN の I/O パスを再スキャンして、LUN へのすべてのパスをリストアします。

## SM-BCを使用したONTAPのアップグレードとリバート

ONTAP 9.8以降では、SnapMirrorビジネス継続性（SM-BC）がサポートされます。ONTAPクラスタのアップグレードとリバートは、アップグレードまたはリバートするONTAPのバージョンによってはSM-BC関係に影響します。

### SM-BCを使用したONTAPのアップグレード

SM-BCを使用するには、ソースクラスタとデスティネーションクラスタのすべてのノードでONTAP 9.8以降が実行されている必要があります。

アクティブなSM-BC関係を含むONTAPをアップグレードする場合は、[自動無停止アップグレード（ANDU）](#)。ANDUを使用すると、アップグレードプロセス中にSM-BC関係が同期されて正常な状態に保たれます。

SM-BC環境でONTAPのアップグレードを準備するための設定手順はありません。ただし、アップグレードの前後に次の点を確認することを推奨します。

- SM-BC関係が同期されています。
- SnapMirrorに関連するエラーはイベントログに記録されません。
- 両方のクラスタでMediatorがオンラインで正常に動作していることを確認します。
- LUNを保護するために、すべてのホストがすべてのパスを正しく認識できる。



クラスタをONTAP 9.8または9.9.1からONTAP 9.10.1以降にアップグレードすると、ONTAPは新しい [整合グループ](#) System Managerを使用して設定できるSM-BC関係のソースクラスタとデスティネーションクラスタの両方。



。snapmirror quiesce および snapmirror resume コマンドはSM-BCではサポートされていません。

### ONTAP 9.10.1からONTAP 9.9.1にリバート

関係を 9.10.1 から 9.9.1 にリバートするには、SM-BC 関係を削除してから、9.10.1 整合グループのインスタンスを削除する必要があります。アクティブなSM-BC関係がある整合性グループは削除できません。9.9.1以前のバージョンで別のスマートコンテナまたはエンタープライズアプリケーションに関連付けられていた9.10.1にアップグレードされたFlexVolボリュームは、リバート時に関連付けられなくなります。整合グループを削除しても、コンスティチュエントボリュームやボリュームの詳細なSnapshotは削除されません。を参照してください ["整合グループを削除する"](#) を参照してください。ONTAP 9.10.1以降でのこのタスクの詳細については、を参照してください。

### ONTAP 9.8からONTAP 9.7にリバート



SM-BC は、ONTAP 9.7 と ONTAP 9.8 の混在クラスタではサポートされません。

ONTAP 9.8 から ONTAP 9.7 にリバートする場合は、次の点に注意してください。

- クラスタがSM-BCデスティネーションをホストしている場合、関係を解除して削除するまで、ONTAP 9.7 にリバートすることはできません。
- クラスタがSM-BCソースをホストしている場合、関係を解放するまでONTAP 9.7にリバートすることはできません。
- ONTAP 9.7 にリバートする前に、ユーザが作成したカスタムの SM-BC SnapMirror ポリシーをすべて削除する必要があります。

これらの要件を満たすには、**"SM-BC 設定を削除します"**。

#### 手順

1. SM-BC 関係にあるいずれかのクラスタからリバートチェックを実行します。

```
cluster::*> system node revert-to -version 9.7 -check-only
```

#### 例

```
cluster::*> system node revert-to -version 9.7 -check-only
Error: command failed: The revert check phase failed. The following
issues must be resolved before revert can be completed. Bring the data
LIFs down on running vservers. Command to list the running vservers:
vserver show -admin-state running Command to list the data LIFs that are
up: network interface show -role data -status-admin up Command to bring
all data LIFs down: network interface modify {-role data} -status-admin
down
Disable snapshot policies.
    Command to list snapshot policies: "snapshot policy show".
    Command to disable snapshot policies: "snapshot policy modify
-vserver
    * -enabled false"

    Break off the initialized online data-protection (DP) volumes and
delete
    Uninitialized online data-protection (DP) volumes present on the
local
    node.
    Command to list all online data-protection volumes on the local
node:
    volume show -type DP -state online -node <local-node-name>
    Before breaking off the initialized online data-protection volumes,
quiesce and abort transfers on associated SnapMirror relationships
and
    wait for the Relationship Status to be Quiesced.
    Command to quiesce a SnapMirror relationship: snapmirror quiesce
    Command to abort transfers on a SnapMirror relationship: snapmirror
abort
    Command to see if the Relationship Status of a SnapMirror
```

```

relationship
  is Quiesced: snapmirror show
  Command to break off a data-protection volume: snapmirror break
  Command to break off a data-protection volume which is the
destination
  of a SnapMirror relationship with a policy of type "vault":
snapmirror
  break -delete-snapshots
  Uninitialized data-protection volumes are reported by the
"snapmirror
  break" command when applied on a DP volume.
  Command to delete volume: volume delete

Delete current version snapshots in advanced privilege level.
  Command to list snapshots: "snapshot show -fs-version 9.8"
  Command to delete snapshots: "snapshot prepare-for-revert -node
<nodename>"

Delete all user-created policies of the type active-strict-sync-
mirror
and active-sync-mirror.
The command to see all active-strict-sync-mirror and active-sync-
mirror
type policies is:
  snapmirror policy show -type
  active-strict-sync-mirror,active-sync-mirror
The command to delete a policy is :
  snapmirror policy delete -vserver <SVM-name> -policy <policy-name>

```

クラスタのリバートの詳細については、を参照してください ["ONTAP をリバートする"](#)。

## SM-BC 設定を削除します

RTOゼロの同期SnapMirror保護が不要になった場合は、SM-BC関係を削除できます。

このタスクについて

- SM-BC 関係を削除する前に、デスティネーションクラスタ内のすべての LUN のマッピングを解除する必要があります。
- LUN のマッピングが解除されてホストが再スキャンされると、SCSI ターゲットは LUN のインベントリが変更されたことをホストに通知します。RTO ゼロのセカンダリボリュームにある既存の LUN は、ゼロの RTO 関係が削除されたあとに新しい ID が反映されるように変更されます。ホストは、セカンダリボリューム LUN を、ソースボリューム LUN とは関係のない新しい LUN として検出します。
- 関係を削除しても、セカンダリボリュームは DP ボリュームのままです。問題を実行できます。  
snapmirror break 読み取り/書き込みに変換するコマンド。
- フェイルオーバー状態でない関係は削除できません。

## 手順

1. セカンダリクラスタから、ソースエンドポイントとデスティネーションエンドポイントの間のSM-BC整合性グループ関係を削除します。

```
destination::>snapmirror delete -destination-path vs1_dst:/cg/cg_dst
```

2. プライマリクラスタで、整合性グループ関係と関係に対して作成されたSnapshotコピーを解放します。

```
source::>snapmirror release -destination-path vs1_dst:/cg/cg_dst
```

3. ホストの再スキャンを実行して LUN インベントリを更新する。
4. ONTAP 9.10.1 以降では、SnapMirror 関係を削除しても整合グループは削除されません。整合グループを削除する場合は、System Manager または ONTAP REST API を使用する必要があります。を参照してください [整合グループを削除する](#) を参照してください。

**ONTAP** メディエーターを削除します。

ONTAP クラスタからONTAP メディエーターの既存の設定を削除する場合は、を使用します snapmirror mediator remove コマンドを実行します

## 手順

1. ONTAP メディエーターを削除します。

```
snapmirror mediator remove -mediator-address 12.345.678.90 -peer-cluster  
cluster_xyz
```

## トラブルシューティングを行う

**SnapMirror** の削除処理がテイクオーバー状態のときに失敗します

問題：

ONTAP 9.9.1がクラスタにインストールされている場合は、を実行します snapmirror delete SM-BC整合性グループ関係がテイクオーバー状態の場合、コマンドが失敗します。

```
C2_cluster::> snapmirror delete vs1:/cg/dd  
  
Error: command failed: RPC: Couldn't make connection
```

## 解決策

SM-BC 関係にあるノードがテイクオーバー状態の場合は、「-force」オプションを true に設定して SnapMirror の削除およびリリース処理を実行します。

```
C2_cluster::> snapmirror delete vs1:/cg/dd -force true

Warning: The relationship between source "vs0:/cg/ss" and destination
        "vs1:/cg/dd" will be deleted, however the items of the
destination
        Consistency Group might not be made writable, deletable, or
modifiable
        after the operation. Manual recovery might be required.
Do you want to continue? {y|n}: y
Operation succeeded: snapmirror delete for the relationship with
destination "vs1:/cg/dd".
```

## SnapMirror 関係の作成および整合グループの初期化に失敗しました

問題：

SnapMirror 関係の作成と整合グループの初期化が失敗する。

解決策：


クラスタあたりの整合グループの制限を超えないようにしてください。SM-BCの整合グループの制限はプラットフォームに依存せず、ONTAP のバージョンによって異なります。を参照してください ["その他の制約事項および制限事項"](#) ONTAP のバージョンによる制限事項については、を参照してください。

エラー：

整合性グループの初期化が停止した場合は、ONTAP REST API、System Manager、またはコマンドを使用して、整合性グループの初期化のステータスを確認します `sn show -expand`。

解決策：

整合グループの初期化に失敗した場合は、SM-BC 関係を削除し、整合グループを削除してから、関係を再作成して初期化してください。このワークフローは、使用する ONTAP のバージョンによって異なります。

ONTAP 9.8 - 9.9.1 を使用している場合	ONTAP 9.10.1以降を使用している場合
<ol style="list-style-type: none"> <li>1. <a href="#">"SM-BC 設定を削除します"</a></li> <li>2. <a href="#">"整合グループ関係を作成する"</a></li> <li>3. <a href="#">"整合グループ関係を初期化します"</a></li> </ol>	<ol style="list-style-type: none"> <li>1. [* Protection] &gt; [Relationships] で、コンシステンシグループの SM-BC 関係を探します。選択するオプション  をクリックし、* Delete * をクリックして SM-BC 関係を削除します。</li> <li>2. <a href="#">"整合グループを削除します"</a></li> <li>3. <a href="#">"整合グループを設定します"</a></li> </ol>

## 計画的フェイルオーバーに失敗しました

問題：

を実行したあとに `snapmirror failover start` コマンドを入力し、の出力を表示します `snapmirror failover show` 無停止操作が実行中であることを示すメッセージが表示されます。

```
Cluster1::> snapmirror failover show
Source Destination Error
Path Path Type Status start-time end-time Reason
-----
vs1:/cg/cg vs0:/cg/cg planned failed 10/1/2020 10/1/2020 SnapMirror
Failover cannot start because a volume move is running. Retry the command
once volume move has finished.
08:35:04
08:35:04
```

原因：

ボリューム移動、アグリゲートの再配置、ストレージフェイルオーバーなどの無停止操作の実行中は、計画的フェイルオーバーを開始できません。

解決策：

ノンストップオペレーションが完了するのを待ってから、フェイルオーバー処理をもう一度実行してください。

**ONTAP**メディアエーターに到達できないか、メディアエーターのクォーラムステータスが**false**になっている

問題：

を実行したあとに `snapmirror failover start` コマンドを入力し、の出力を表示します `snapmirror failover show` **Mediator**が設定されていないことを示すメッセージが表示されます。

を参照してください ["ONTAP メディアエーターを初期化します"](#)。

```
Cluster1::> snapmirror failover show
Source Destination Error
Path Path Type Status start-time end-time Reason
-----
vs0:/cg/cg vs1:/cg/cg planned failed 10/1/2020 10/1/2020 SnapMirror
failover cannot start because the source-side precheck failed. reason:
Mediator not configured.
05:50:42 05:50:43
```

原因：

メディアエーターが設定されていないか、ネットワーク接続に問題があります。

解決策：

**ONTAP**メディアエーターが設定されていない場合は、SM-BC関係を確立する前に**ONTAP**メディアエーターを設定する必要があります。ネットワーク接続の問題を修正 `snapmirror mediator show` コマンドを使用して、ソースサイトとデスティネーションサイトの両方でメディアエーターが接続されていること、およびクォーラムステータスが **true** であることを確認します。詳細については、[を参照してください ONTAPメディアエーターの設定](#)。



```
cluster::> snapmirror mediator show
```

Mediator	Address	Peer	Cluster	Connection	Status	Quorum	Status
10.234.10.143		cluster2		connected		true	

サイト B で自動計画外フェイルオーバーがトリガーされない

問題：

サイト A で障害が発生しても、サイト B で計画外フェイルオーバーはトリガーされません

原因 #1の候補：

ONTAPメディアエーターが設定されていません。これが原因かどうかを確認するには、問題 を実行します snapmirror mediator show コマンドをサイトBのクラスタで実行します。

```
Cluster2::*> snapmirror mediator show
```

This table is currently empty.

この例は、サイトBでONTAPメディアエーターが設定されていないことを示しています。

解決策：

両方のクラスタにONTAPメディアエーターが設定されていて、ステータスが「connected」で、クォーラムがTrueに設定されていることを確認します。

可能な原因 #2：

SnapMirror 整合グループが同期されていません。これが原因かどうかを確認するには、イベントログを表示して、サイト A で障害が発生したときに整合グループが同期されているかどうかを確認します。

```
cluster::*> event log show -event *out.of.sync*
```

Time	Node	Severity	Event
10/1/2020 23:26:12	sti42-vsimg-ucs511w	ERROR	sms.status.out.of.sync: Source volume "vs0:zrto_cg_556844_511u_RW1" and destination volume "vs1:zrto_cg_556881_511w_DP1" with relationship UUID "55ab7942-03e5-11eb- ba5a-005056a7dc14" is in "out-of-sync" status due to the following reason: "Transfer failed."

解決策：

サイト B で強制フェイルオーバーを実行するには、次の手順を実行します

1. この整合グループに属するすべての LUN のマッピングをサイト B から解除します

2. を使用して、SnapMirror整合性グループ関係を削除します `force` オプション
3. を入力します `snapmirror break` 整合性グループのコンスティチュエントボリュームに対してコマンドを実行し、ボリュームをDPからR/Wに変換してサイトBからのI/Oを可能にします
4. サイトAのノードをブートして、サイトBからサイトAへのRTO関係をゼロにします
5. を使用して整合グループを解放します `relationship-info-only` サイトAで共通のSnapshotコピーを保持し、整合グループに属するLUNのマッピングを解除します。
6. Sync ポリシーまたは非同期ポリシーを使用してボリュームレベルの関係を設定し、サイトAのボリュームをR/WからDPに変換します。
7. 問題 `snapmirror resync` 関係を同期します。
8. サイトAのSyncポリシーを使用して、SnapMirror関係を削除します
9. を使用して、Syncポリシーが設定されたSnapMirror関係を解放します `relationship-info-only true` サイトB
10. サイトBからサイトAへの整合グループ関係を作成します
11. サイトAから整合グループの再同期を実行し、整合グループが同期されていることを確認します。
12. ホストLUNのI/Oパスを再スキャンして、LUNへのすべてのパスをリストアします。

サイトBとメディアエーター間のリンクが停止し、サイトAが停止する

ONTAPメディアエーターの接続を確認するには、`snapmirror mediator show` コマンドを実行します。接続ステータスが到達不能で、サイトBがサイトAに到達できない場合は、次のような出力が表示されます。解決策の手順に従って、接続をリストアします

```

cluster::*> snapmirror mediator show
Mediator Address Peer Cluster      Connection Status Quorum Status
-----
10.237.86.17      C1_cluster      unreachable      true
SnapMirror consistency group relationship status is out of sync.

C2_cluster::*> snapmirror show -expand
Source          Destination Mirror Relationship Total
Last
Path            Type Path            State Status Progress Healthy
Updated
-----
vs0:/cg/src_cg_1 XDP vs1:/cg/dst_cg_1 Snapmirrored OutOfSync - false -
vs0:zrto_cg_655724_188a_RW1 XDP vs1:zrto_cg_655755_188c_DP1 Snapmirrored
OutOfSync - false -
vs0:zrto_cg_655733_188a_RW2 XDP vs1:zrto_cg_655762_188c_DP2 Snapmirrored
OutOfSync - false -
vs0:zrto_cg_655739_188b_RW1 XDP vs1:zrto_cg_655768_188d_DP1 Snapmirrored
OutOfSync - false -
vs0:zrto_cg_655748_188b_RW2 XDP vs1:zrto_cg_655776_188d_DP2 Snapmirrored
OutOfSync - false -
5 entries were displayed.

Site B cluster is unable to reach Site A.
C2_cluster::*> cluster peer show
Peer Cluster Name      Cluster Serial Number Availability
Authentication
-----
C1_cluster              1-80-000011              Unavailable      ok

```

## 解決策

フェイルオーバーを強制的に実行してサイト B からの I/O を有効にし、サイト B からサイト A への RTO 関係をゼロにします。サイト B で強制フェイルオーバーを実行するには、次の手順を実行します。

1. この整合グループに属するすべての LUN のマッピングをサイト B から解除します。
2. force オプションを使用して、SnapMirror 整合グループ関係を削除します。
3. snapmirror break コマンドを入力します。(snapmirror break -destination\_path svm:\_volume\_) を使用して、ボリュームを DP から RW に変換し、サイト B からの I/O を可能にします。

整合グループ内の関係ごとに、snapmirror break コマンドを問題する必要があります。たとえば、整合グループにボリュームが3つある場合は、ボリュームごとにコマンドを問題します。

4. サイト A のノードをブートして、サイト B からサイト A への RTO 関係をゼロにします。

5. サイト A で `relationship-info-only` を指定して整合グループを解放して共通の Snapshot コピーを保持し、整合グループに属する LUN のマッピングを解除します。
6. Sync ポリシーまたは非同期ポリシーを使用してボリュームレベルの関係を設定し、サイト A のボリュームを RW から DP に変換します。
7. 問題 `snapmirror resync` コマンドを使用して関係を同期します。
8. サイト A の Sync ポリシーが設定された SnapMirror 関係を削除します
9. サイト B で `relationship-info-only true` を使用して、Sync ポリシーが設定された SnapMirror 関係を解放します
10. サイトBとサイトAの間に整合性グループ関係を作成します。
11. ソースクラスタから、整合グループを再同期します。整合性グループの状態がin syncになっていることを確認します。
12. ホストのLUN I/Oパスを再スキャンして、LUNへのすべてのパスをリストアします。

サイトAとメディエーター間のリンクが停止してサイトBが停止

SM-BCを使用している場合、ONTAPメディエーターまたはピアクラスタ間の接続が失われる可能性があります。問題を診断するには、SM-BC関係のさまざまな部分の接続、可用性、および合意ステータスを確認し、接続を強制的に再開します。

確認事項	CLIコマンド	インジケータ
サイトAのメディエーター	<code>snapmirror mediator show</code>	接続ステータスはになります unreachable
サイトBへの接続	<code>cluster peer show</code>	可用性はになります unavailable
SM-BCボリュームのコンセンサステータス	<code>volume show volume_name -fields smbc-consensus</code>	。 sm-bc consensus フィールドにはと表示されます Awaiting-consensus

この問題 の診断と解決に関する追加情報 については、サポート技術情報アートを参照してください ["SM-BCを使用している場合、サイトAとメディエーターが停止し、サイトBが停止した場合のリンク"](#)。

フェンシングがデスティネーションボリュームに設定されている場合、**SM-BC** の **SnapMirror** 削除処理が失敗します

問題：

デスティネーションボリュームのいずれかにリダイレクトフェンスが設定されていると、SnapMirror の削除処理に失敗します。

解決策

次の操作を実行して、リダイレクションを再試行し、宛先ボリュームからフェンスを削除します。

- SnapMirror が再同期された
- SnapMirror の更新

プライマリが停止しているときにボリューム移動処理が停止します

問題：

ボリューム移動処理は、プライマリサイトが SM-BC 関係で停止した場合に、カットオーバー保留状態になります。

プライマリサイトが停止すると、セカンダリサイトで自動計画外フェイルオーバー（AUFO）が実行されます。AUFO がトリガーされたときにボリューム移動処理が進行中の場合、ボリューム移動が停止します。

解決策：

停止したボリューム移動インスタンスを中止して、ボリューム移動処理を再開します。

**Snapshot** コピーを削除できない場合、**SnapMirror** のリリースは失敗します

問題：

Snapshot コピーを削除できない場合、SnapMirror のリリース処理は失敗します。

解決策：

Snapshot コピーには一時タグが含まれています。を使用します `snapshot delete` コマンドにを指定します `-ignore-owners` 一時的なSnapshotコピーを削除するオプション。

```
snapshot delete -volume <volume_name> -snapshot <snapshot_name> -ignore-owners  
true -force true
```

を再試行します `snapmirror release` コマンドを実行します

ボリューム移動の参照 **Snapshot** コピーが最も新しいと表示されます

問題：

整合性グループボリュームでボリューム移動処理を実行したあと、ボリューム移動の参照 Snapshot コピーが SnapMirror 関係の最も新しいボリュームとして表示されることがあります。

最新の Snapshot コピーを表示するには、次のコマンドを使用します。

```
snapmirror show -fields newest-snapshot status -expand
```

解決策：

を手動で実行します `snapmirror resync` または、ボリューム移動処理の完了後に次の自動再同期処理が実行されるまで待ちます。

## MetroCluster および SnapMirror のビジネス継続性用のメディアエーターサービス

### ONTAP メディアエーターの概要

ONTAP メディアエーターは、ONTAP の機能に次のような機能を提供します。

- HAメタデータ用のフェンシングされた永続的なストアを提供します。
- コントローラの稼働を維持するためのpingプロキシとして機能します。
- クォーラムの決定に役立つ同期ノード健全性クエリ機能を提供します。

ONTAP メディエーターは、さらに2つのsystemctlサービスを提供します。

- **ontap\_mediator.service**

ONAP関係を管理するためのREST APIサーバを管理します。

- **mediator-scst.service**

iSCSIモジュール（SCST）の起動とシャットダウンを制御します。

システム管理者に提供されるツール

システム管理者に提供されるツール：

- **/usr/local/bin/mediator\_change\_password**

現在のAPIユーザ名とパスワードを指定したときに、新しいAPIパスワードを設定します。

- **/usr/local/bin/mediator\_change\_user**

現在のAPIユーザ名とパスワードを指定した場合に、新しいAPIユーザ名を設定します。

- **/usr/local/bin/mediator\_generate\_support\_bundle**

ネットアップカスタマーサポートとの通信に必要なすべてのサポート情報を含むローカルのtgzファイルを生成します。これには、アプリケーション構成、ログ、および一部のシステム情報が含まれます。バンドルはローカルディスク上で生成され、必要に応じて手動で転送できます。保存場所：  
：/opt/netapp/data/support bundles/

- **/usr/local/bin/uninstall\_ontap\_mediator**

ONTAP メディエーターパッケージとSCSTカーネルモジュールを削除します。これには、すべての設定、ログ、およびメールボックスデータが含まれます。

- **/usr/local/bin/mediator\_unlock\_user**

認証の再試行の上限に達した場合、APIユーザアカウントのロックアウトが解除されます。この機能は、ブルートフォースパスワードの派生を防止するために使用されます。ユーザに正しいユーザ名とパスワードの入力を求めるプロンプトが表示されます。

- **/usr/local/bin/mediator\_add\_user**

（サポートのみ）インストール時にAPIユーザを追加する場合に使用します。

## 特記事項

ONTAP メディエーターは、SCSTを使用してiSCSIを提供します（を参照） <http://scst.sourceforge.net/index.html>）。このパッケージは、インストール時にカーネル専用コンパイルされるカーネルモジュールです。カーネルを更新する場合は、SCSTの再インストールが必要になることがあります。または、ONTAP メディエーターをアンインストールしてから再インストールし、ONTAP 関係を再設定します。



サーバOSカーネルの更新は、ONTAP のメンテナンス時間に合わせて行う必要があります。

## ONTAP メディエーターの最新情報

各リリースでは、ONTAP メディエーターの機能が新たに拡張されています。最新情報をご紹介します。

### 拡張機能

ONTAP メディエーターのバージョン	拡張機能
1.7	<ul style="list-style-type: none"><li>• RHEL 8.5、8.6、8.7、8.8、8.9のサポート 9.0、9.1、9.2、9.3</li><li>• Rocky Linux 8および9のサポート</li></ul>
1.6	<ul style="list-style-type: none"><li>• Python 3.9のアップデート。</li><li>• RHEL 8.4-8.8、9.0-9.2、Rocky Linux 8および9のサポート。</li><li>• RHEL 7.x / CentOSのすべてのリリースのサポートを廃止しました。</li></ul>
1.5	<ul style="list-style-type: none"><li>• 大規模なSMBCシステムの速度を最適化します。</li><li>• インストーラに暗号化コード署名が追加されました。</li><li>• RHEL 7.x / CentOS 7.xの廃止に関する警告が追加されました</li></ul>
1.4	<ul style="list-style-type: none"><li>• RHEL 8.4および8.5のサポート。</li><li>• SCSTバージョン3.6.0が含まれています。</li><li>• UEFIベースのファームウェアのセキュアブート（SB）のサポートが追加されました。</li></ul>
1.3	<ul style="list-style-type: none"><li>• RHEL / CentOS 8.2および8.3のサポート</li><li>• SCSTバージョン3.5.0が含まれています。</li></ul>
1/2	<ul style="list-style-type: none"><li>• HTTPSメールボックスのサポート。</li><li>• ONTAP 9.8以降のMCC-IP AUSOおよびSM-BC ZRTOで使します。</li><li>• SCSTバージョン3.4.0が含まれています。</li></ul>

1.1	<ul style="list-style-type: none"> <li>• RHEL / CentOS 7.6、7.7、8.0、8.1のサポート。</li> <li>• Perlの依存関係が解消されます。</li> <li>• SCSTバージョン3.4.0が含まれています。</li> </ul>
1.0	<ul style="list-style-type: none"> <li>• iSCSIメールボックスのサポート。</li> <li>• ONTAP 9.7以降MCC-IP AUSOで使します。</li> <li>• RHEL / CentOS 7.6のサポート。</li> </ul>

## OSサポートマトリックス

ONTAP × ディエー ター用 のOS	1.7	1.6	1.5	1.4	1.3	1/2	1.1	1.0
7.6	廃止され た	廃止され た	はい。	はい。	はい。	はい。	はい。	○ (RHEL のみ)
7.7	廃止され た	廃止され た	はい。	はい。	はい。	はい。	いいえ	いいえ
7、8	廃止され た	廃止され た	はい。	はい。	はい。	はい。	いいえ	いいえ
7.9	廃止され た	廃止され た	はい。	はい。	はい。	黙示的	いいえ	いいえ
RHEL 8.0	廃止され た	廃止され た	はい。	はい。	はい。	はい。	はい。	いいえ
RHEL 8.1	廃止され た	廃止され た	はい。	はい。	はい。	はい。	いいえ	いいえ
RHEL 8.2	廃止され た	廃止され た	はい。	はい。	はい。	いいえ	いいえ	いいえ
RHEL 8.3	廃止され た	廃止され た	はい。	はい。	はい。	いいえ	いいえ	いいえ
RHEL 8.4	廃止され た	はい。	はい。	はい。	いいえ	いいえ	いいえ	いいえ
RHEL 8.5	はい。	はい。	はい。	はい。	いいえ	いいえ	いいえ	いいえ
RHEL 8.6	はい。	はい。	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ



RHEL 8.7	はい。	はい。	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ
RHEL 8.8	はい。	はい。	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ
RHEL 9.0	はい。	はい。	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ
RHEL 9.1	はい。	はい。	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ
RHEL 9.2	はい。	はい。	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ
RHEL 9.3	はい。	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ
CentOS 8 およびSTREA M	いいえ	いいえ	いいえ	いいえ	いいえ	N/A	N/A	N/A
Rocky Linux 8	はい。	はい。	N/A	N/A	N/A	N/A	N/A	N/A
Rocky Linux 9	はい。	はい。	N/A	N/A	N/A	N/A	N/A	N/A

- ・特に指定がないかぎり、「OS」とはRedHatとCentOSの両方のリリースを指します。
- ・「いいえ」は、OSとONTAP メディエーターに互換性がないことを示します。
- ・CentOS 8は再分岐のため全てのリリースで削除された。CentOS Streamは本番用のターゲットOSとしては適切ではないと考えられていた。サポートは予定されていません。
- ・ONTAP Mediator 1.5は、RHEL 7.xブランチオペレーティングシステムで最後にサポートされたリリースです。
- ・ONTAP Mediator 1.6では、Rocky Linux 8および9のサポートが追加されています。

#### 解決済みの問題

変更日	IDを変更します	説明
2023年1月10日	6567145	<p>次の変更が行われました。</p> <ul style="list-style-type: none"> <li>・ONTAP Mediatorで、RHEL 9.6、8.7、9.0、9.1のオペレーティングシステムが追加されました。</li> <li>・新たにサポートされたオペレーティングシステムの問題のブロックを解除するために、新しいSCSTバージョン3.7.0が追加されました。</li> <li>・Rocky Linuxのサポートを追加：Rocky 8および9。</li> </ul>

2023年1月24日	6621319です	ONTAP メディエーターのインストール用に事前にインストール可能なSCSTライブラリ。
2023年2月27日	6623764	mediator-scstサービスの再起動時に常にscst_diskカーネルモジュールをロードするように変更しました。これらの変更により、サービスは常に標準ロジックを使用して新しいiSCSIターゲットを作成できるようになります。
2023年2月28日	6625194	ONTAP メディエーターのインストーラに、次の新しいオプションが追加されました。 <code>--skip-yum-dependencies</code>
2023年3月24日	6652840	ONTAP メディエーターのインストーラを更新し、SCSTのインストールを再インストールまたは修復できるようにしました。
2023年3月27日	6655179	複雑なパスワードを使用したサポートバンドル収集がトリガーされたときに発生する解析問題 が修正されました。
2023年3月28日	6656739	SCST比較ロジックが変更され、ONTAP Mediatorのアップグレード時に正しいバージョンがインストールされるようになりました。

## インストールまたはアップグレード

**ONTAP** メディエーターサービスのインストールまたはアップグレードを準備します

ONTAPメディエーターサービスをインストールするには、すべての前提条件を満たしていることを確認し、インストールパッケージを読み込んでホストでインストーラを実行する必要があります。この手順は、既存の環境のインストールまたはアップグレードに使用します。

このタスクについて

- ONTAP 9.7以降では、任意のバージョンのONTAP メディエーターを使用してMetroCluster IP構成を監視できます。
- ONTAP 9.8以降では、任意のバージョンのONTAP メディエーターを使用してSM-BC関係を監視できます。

作業を開始する前に

次の前提条件を満たしている必要があります。

ONTAP メディエーターのバージョン	サポートされている Linux バージョン
1.7	<ul style="list-style-type: none"> <li>• Red Hat Enterprise Linux : 8.5、8.6、8.7、8.8、8.9、9.0、9.1、9.2、9.3</li> <li>• Rocky Linux 8および9</li> </ul>

1.6	<ul style="list-style-type: none"> <li>• Red Hat Enterprise Linux : 8.4、8.5、8.6、8.7、8.8、9.0、9.1、9.2</li> <li>• Rocky Linux 8および9</li> </ul>
1.5	<ul style="list-style-type: none"> <li>• Red Hat Enterprise Linux : 7.6、7.7、7.8、7.9、8.1、8.2、8.3、8.4、8.5</li> <li>• CentOS : 7.6、7.7、7.8、7.9</li> </ul>
1.4	<ul style="list-style-type: none"> <li>• Red Hat Enterprise Linux : 7.6、7.7、7.8、7.9、8.1、8.2、8.3、8.4、8.5</li> <li>• CentOS : 7.6、7.7、7.8、7.9</li> </ul>
1.3	<ul style="list-style-type: none"> <li>• Red Hat Enterprise Linux : 7.6、7.7、7.8、7.9、8.1、8.2、8.3</li> <li>• CentOS : 7.6、7.7、7.8、7.9</li> </ul>
1/2	<ul style="list-style-type: none"> <li>• Red Hat Enterprise Linux : 7.6、7.7、7.8、8.1</li> <li>• CentOS : 7.6、7.7、7.8</li> </ul>



カーネルのバージョンがオペレーティングシステムのバージョンと一致している必要があります。

- 64 ビットの物理インストールまたは仮想マシン
- 8GB の RAM
- 1 GBのディスクスペース（アプリケーションのインストール、サーバログ、およびデータベースに使用）
- ユーザ：ルートアクセス

カーネル以外のライブラリパッケージは安全に更新できますが、ONTAP メディエーターアプリケーション内で有効にするにはリブートが必要になる場合があります。再起動が必要な場合は、サービスウィンドウを使用することをお勧めします。

をインストールした場合 `yum-utils` パッケージの場合は、を使用できません `needs-restarting` コマンドを実行します

カーネルコアは、ONTAP メディエーターのバージョンマトリックスでサポートされているバージョンに更新することができます。再起動は必須であるため、サービスウィンドウが必要です。

リブートの前にSCSTカーネルモジュールをアンインストールし、リブート後に再インストールする必要があります。



特定のONTAP メディエーターリリースでは、サポートされているOSリリース以降のカーネルへのアップグレードはサポートされていません。(これは、テストしたSCSTモジュールがコンパイルされないことを示している可能性があります)。

## UEFIセキュアブートが有効になっている場合のセキュリティキーの登録

UEFIセキュアブートが有効になっている場合、ONTAPメディアエーターをインストールするには、ONTAPメディアエーターサービスを開始する前にセキュリティキーを登録する必要があります。システムがUEFI対応で、セキュアブートがオンになっているかどうかを確認するには、次の手順に従います。

### 手順

1. mokutilがインストールされていない場合は、次のコマンドを実行します。

```
yum install mokutil
```

2. システムでUEFIセキュアブートが有効になっているかどうかを確認するには、次のコマンドを実行します。

```
mokutil --sb-state
```

結果は、このシステムでUEFIセキュアブートが有効になっているかどうかを示します。



ONTAPメディアエーター1.2.0以前のバージョンでは、このモードはサポートされていません。

## UEFIセキュアブートを無効にする

ONTAPメディアエーターをインストールする前に、UEFIセキュアブートを無効にすることもできます。

### 手順

1. 物理マシンのBIOS設定で、「UEFIセキュアブート」オプションを無効にします。
2. VMのVMware設定で、vSphere 6.xの場合は[Safe Start]オプション、vSphere 7.xの場合は[Secure Boot]オプションを無効にします。

ホストオペレーティングシステムをアップグレードしてから、**ONTAP** メディアエーターをアップグレードします

ONTAP メディアエーター用のホストOSを新しいバージョンにアップグレードするには、最初にONTAP メディアエーターをアンインストールする必要があります。

### 作業を開始する前に

Red Hat Enterprise LinuxまたはRocky Linuxとその関連リポジトリをシステムにインストールする際のベストプラクティスを次に示します。別の方法でインストールまたは設定されたシステムでは、追加の手順が必要になる

- Red Hatのベストプラクティスに従ってRed Hat Enterprise LinuxまたはRocky Linuxをインストールする必要があります。CentOS 8.xバージョンはサポートされないため、互換性があるバージョンのCentOS 8.xは推奨されません。
- Red Hat Enterprise LinuxまたはRocky LinuxへのONTAPメディアエーターサービスのインストール中にインストールプログラムが必要なすべてのソフトウェアにアクセスしてインストールできるように、システムには適切なリポジトリへのアクセスが必要です。
- yum インストーラで Red Hat Enterprise Linux リポジトリから依存するソフトウェアを検索するには、Red Hat Enterprise Linux のインストール中またはインストール後に有効な Red Hat サブスクリプションを使用してシステムを登録しておく必要があります。

Red Hat Subscription Manager については、Red Hat のドキュメントを参照してください。

- 次のポートをメディアエーター用に空けておく必要があります。
  - 31784
  - 3260
- サードパーティ製ファイアウォールを使用している場合は、を参照してください ["ONTAP メディアエーターのファイアウォール要件"](#)
- Linuxホストがインターネットにアクセスできない場所にある場合は、必要なパッケージがローカルリポジトリにあることを確認する必要があります。

Linux環境でLink Aggregation Control Protocol (LACP) を使用している場合は、カーネルを正しく設定し、を確認する必要があります `sysctl net.ipv4.conf.all.arp_ignore` は「2」に設定されています。

## 必要なもの

ONTAP メディアエーターサービスに必要なパッケージは次のとおりです。

すべての RHEL または CentOS バージョン	RHEL 8.x/Rocky Linux 8用の追加パッケージ	RHEL 9.x/Rocky Linux 9用の追加パッケージ
<ul style="list-style-type: none"><li>• openssl</li><li>• openssl-devel</li><li>• kernel-devel-\$(uname -r)</li><li>• GCC</li><li>• メーカー</li><li>• libselinux-utils</li><li>• パッチ</li><li>• Bzip2.</li><li>• Perl - データダンパー</li><li>• PERLA-ExtUtils-MakeMaker</li><li>• efibootmgr</li><li>• モクティル</li></ul>	<ul style="list-style-type: none"><li>• python3-pip の略</li><li>• elfutils-libelf-devel</li><li>• policycoreutils -python-utils</li><li>• RedHat LSB コアです</li><li>• ピートン39</li><li>• Python39 -デベル</li></ul>	<ul style="list-style-type: none"><li>• python3-pip の略</li><li>• elfutils-libelf-devel</li><li>• policycoreutils -python-utils</li><li>• ピートン3</li><li>• Python3 -デベル</li></ul>

メディアエーターのインストールパッケージは自己解凍形式の圧縮 tar ファイルで、次のものが含まれます。

- サポートされているリリースのリポジトリから取得できないすべての依存関係を含む RPM ファイル。
- インストールスクリプト。

有効なSSL証明書を使用することを推奨します。

## このタスクについて

leapp-upgradeツールを使用してONTAP メディアエーター用のホストOSを新しいメジャーバージョン（7.xから8.xなど）にアップグレードする場合は、次の手順を実行します。 ONTAP メディアエーターは、システムに

登録されているリポジトリにインストールされているRPMの新しいバージョンを検出しようとするため、アンインストールする必要があります。

**rpm**ファイルは**ONTAP** メディエーターのインストーラの一部としてインストールされているため、その検索に含まれます。ただし、その**rpm**ファイルはインストーラの一部として展開され、登録されたリポジトリからダウンロードされなかったため、アップグレードが見つかりません。この場合、**leapp-upgrade**ツールはパッケージをアンインストールします。

サポートケースの優先順位付けに使用されるログファイルを保持するには、OSのアップグレード前にファイルをバックアップし、ONTAP メディエーターパッケージの再インストール後にリストアする必要があります。ONTAP メディエーターを再インストールするため、接続されているONTAP クラスタは新規インストール後に再接続する必要があります。



次の手順を順番に実行する必要があります。ONTAP メディエーターを再インストールしたらすぐに、**ontap\_mediator**サービスを停止してログファイルを交換し、サービスを再起動する必要があります。これにより、ログが失われなくなります。

## 手順

### 1. ログファイルをバックアップします。

```
[rootmediator-host ~]# tar -czf ontap_mediator_file_backup.tgz -C
/opt/netapp/lib/ontap_mediator ./log
./ontap_mediator/server_config/ontap_mediator.user_config.yaml
[rootmediator-host ~]# tar -tf ontap_mediator_file_backup.tgz
./log/
./log/ontap_mediator.log
./log/scstadmin.log
./log/ontap_mediator_stdout.log
./log/ontap_mediator_requests.log
./log/install_20230419134611.log
./log/scst.log
./log/ontap_mediator_syslog.log
./ontap_mediator/server_config/ontap_mediator.user_config.yaml
[rootmediator-host ~]#
```

### 2. leapp-upgradeツールを使用してアップグレードを実行します。

```
[rootmediator-host ~]# leapp preupgrade --target 8.4
..<snip upgrade checks>..
..<fix issues found>..
[rootmediator-host ~]# leapp upgrade --target 8.4
..<snip upgrade>..
[rootmediator-host ~]# cat /etc/os-release | head -2
NAME="Red Hat Enterprise Linux"
VERSION="8.4 (Ootpa)"
[rootmediator-host ~]#
```

### 3. ONTAP メディエーターを再インストールします。



ログファイルが失われないように、ONTAP メディエーターを再インストールした直後に残りの手順を実行します。

```
[rootmediator-host ~]# ontap-mediator-1.6.0/ontap-mediator-1.6.0

ONTAP Mediator: Self Extracting Installer

..<snip installation>..
[rootmediator-host ~]#
```

### 4. ontap\_mediatorサービスを停止します。

```
[rootmediator-host ~]# systemctl stop ontap_mediator
[rootmediator-host ~]#
```

### 5. ログファイルを置き換えます。

```
[rootmediator-host ~]# tar -xf ontap_mediator_log_backup.tgz -C
/opt/netapp/lib/ontap_mediator
[rootmediator-host ~]#
```

### 6. ontap\_mediatorサービスを開始します。

```
[rootmediator-host ~]# systemctl start ontap_mediator
[rootmediator-host ~]#
```

### 7. アップグレードしたONTAP メディエーターにすべてのONTAP クラスタを再接続します

```

siteA::> metrocluster configuration-settings mediator show
Mediator IP      Port      Node      Configuration
Connection
Status      Status
-----
-----
172.31.40.122
31784      siteA-node2      true      false
           siteA-node1      true      false
           siteB-node2      true      false
           siteB-node2      true      false

siteA::> metrocluster configuration-settings mediator remove
Removing the mediator and disabling Automatic Unplanned Switchover.
It may take a few minutes to complete.
Please enter the username for the mediator: mediatoradmin
Please enter the password for the mediator:
Confirm the mediator password:
Automatic Unplanned Switchover is disabled for all nodes...
Removing mediator mailboxes...
Successfully removed the mediator.

siteA::> metrocluster configuration-settings mediator add -mediator
-address 172.31.40.122
Adding the mediator and enabling Automatic Unplanned Switchover. It
may take a few minutes to complete.
Please enter the username for the mediator: mediatoradmin
Please enter the password for the mediator:
Confirm the mediator password:
Successfully added the mediator.

siteA::> metrocluster configuration-settings mediator show
Mediator IP      Port      Node      Configuration
Connection
Status      Status
-----
-----
172.31.40.122
31784      siteA-node2      true      true
           siteA-node1      true      true
           siteB-node2      true      true
           siteB-node2      true      true

siteA::>

```



SnapMirrorビジネス継続性を実現するために、/opt/netappディレクトリ以外にTLS証明書をインストールした場合は再インストールする必要はありません。生成されたデフォルトの自己署名証明書を使用していた場合、またはカスタム証明書を/opt/netappディレクトリに配置していた場合は、その証明書をバックアップおよびリストアする必要があります。

```
peer1::> snapmirror mediator show
Mediator Address Peer Cluster      Connection Status Quorum Status
-----
172.31.49.237    peer2              unreachable      true

peer1::> snapmirror mediator remove -mediator-address 172.31.49.237
-peer-cluster peer2

Info: [Job 39] 'mediator remove' job queued

peer1::> job show -id 39

Job ID Name                      Owning
Vserver      Node                      State
-----
39      mediator remove      peer1      peer1-node1      Success
Description: Removing entry in mediator

peer1::> security certificate show -common-name ONTAPMediatorCA
Vserver      Serial Number      Certificate Name
Type
-----
-----
peer1
4A790360081F41145E14C5D7CE721DC6C210007F
ONTAPMediatorCA

server-ca
Certificate Authority: ONTAP Mediator CA
Expiration Date: Mon Apr 17 10:27:54 2073

peer1::> security certificate delete -common-name ONTAPMediatorCA *
1 entry was deleted.

peer1::> security certificate install -type server-ca -vserver
peer1

Please enter Certificate: Press <Enter> when done
..<snip ONTAP Mediator CA public key>..

You should keep a copy of the CA-signed digital certificate for
```

future reference.

The installed certificate's CA and serial number for reference:

CA: ONTAP Mediator CA

serial: 44786524464C5113D5EC966779D3002135EA4254

The certificate's generated name for reference: ONTAPMediatorCA

```
peer2::> security certificate delete -common-name ONTAPMediatorCA *  
1 entry was deleted.
```

```
peer2::> security certificate install -type server-ca -vserver peer2
```

Please enter Certificate: Press <Enter> when done  
..  
..<snip ONTAP Mediator CA public key>..

You should keep a copy of the CA-signed digital certificate for future reference.

The installed certificate's CA and serial number for reference:

CA: ONTAP Mediator CA

serial: 44786524464C5113D5EC966779D3002135EA4254

The certificate's generated name for reference: ONTAPMediatorCA

```
peer1::> snapmirror mediator add -mediator-address 172.31.49.237  
-peer-cluster peer2 -username mediatoradmin
```

Notice: Enter the mediator password.

Enter the password:

Enter the password again:

Info: [Job: 43] 'mediator add' job queued

```
peer1::> job show -id 43
```

Job ID	Name	Owning Vserver	Node	State
43	mediator add	peer1	peer1-node2	Success
Description: Creating a mediator entry				

```
peer1::> snapmirror mediator show
```

Mediator Address	Peer Cluster	Connection Status	Quorum Status
172.31.49.237	peer2	connected	true

```
peer1::>
```

リポジトリへのアクセスを有効にします

インストールプロセス中にONTAP メディエーターが必要なパッケージにアクセスできるように、リポジトリへのアクセスを有効にする必要があります

手順

1. 次の表に示すように、アクセスする必要があるリポジトリを決定します。

オペレーティングシステム	リポジトリへのアクセスを指定する必要があります ...
RHEL 7.x	<ul style="list-style-type: none"><li>• rhel-7-server-optional-rpms のいずれかです</li></ul>
RHEL 8.x の場合	<ul style="list-style-type: none"><li>• RHEL-8-For x86_64-baseos-RPMs</li><li>• RHEL-8-For x86_64-AppStream-RPMs</li></ul>
RHEL 9.x	<ul style="list-style-type: none"><li>• rhel-9-for-x86_64-baseos-rpms</li><li>• RHEL-9-FOR-x86_64-AppStream-RPM</li></ul>
CentOS 7.x	<ul style="list-style-type: none"><li>• C7.6.1810 - ベースリポジトリ</li></ul>
Rocky Linux 8	<ul style="list-style-type: none"><li>• AppStreamの略</li><li>• ベースオス</li></ul>
Rocky Linux 9	<ul style="list-style-type: none"><li>• AppStreamの略</li><li>• ベースオス</li></ul>

2. インストールプロセス中にONTAP メディエーターが必要なパッケージにアクセスできるように、上記のリポジトリへのアクセスを有効にするには、次のいずれかの手順を実行します。

オペレーティングシステムが\* RHEL 7.x \*の場合は、次の手順 を使用してリポジトリへのアクセスを有効にします。

### 手順

1. 必要なリポジトリに登録します。

```
subscription-manager repos --enable rhel-7-server-optional-rpms
```

次の例は、このコマンドの実行例を示しています。

```
[root@localhost ~]# subscription-manager repos --enable rhel-7-  
server-optional-rpms  
Repository 'rhel-7-server-optional-rpms' is enabled for this system.
```

2. を実行します yum repolist コマンドを実行します

次の例は、このコマンドの実行例を示しています。rhel-7-server-optional-rpms リポジトリがリストに表示されている必要があります。

```
[root@localhost ~]# yum repolist  
Loaded plugins: product-id, search-disabled-repos, subscription-  
manager  
rhel-7-server-optional-rpms | 3.2 kB  00:00:00  
rhel-7-server-rpms | 3.5 kB  00:00:00  
(1/3): rhel-7-server-optional-rpms/7Server/x86_64/group  
| 26 kB  00:00:00  
(2/3): rhel-7-server-optional-rpms/7Server/x86_64/updateinfo  
| 2.5 MB  00:00:00  
(3/3): rhel-7-server-optional-rpms/7Server/x86_64/primary_db  
| 8.3 MB  00:00:01  
repo id                                repo name  
status  
rhel-7-server-optional-rpms/7Server/x86_64  Red Hat Enterprise  
Linux 7 Server - Optional (RPMs)  19,447  
rhel-7-server-rpms/7Server/x86_64          Red Hat Enterprise  
Linux 7 Server (RPMs)                26,758  
repolist: 46,205  
[root@localhost ~]#
```

オペレーティングシステムが\* RHEL 8.x \*の場合は、次の手順を使用してリポジトリへのアクセスを有効にします。

手順

1. 必要なリポジトリに登録します。

```
subscription-manager repos --enable rhel-8-for-x86_64-baseos-rpms
```

```
subscription-manager repos --enable rhel-8-for-x86_64-appstream-rpms
```

次の例は、このコマンドの実行例を示しています。

```
[root@localhost ~]# subscription-manager repos --enable rhel-8-for-x86_64-baseos-rpms
Repository 'rhel-8-for-x86_64-baseos-rpms' is enabled for this system.
[root@localhost ~]# subscription-manager repos --enable rhel-8-for-x86_64-appstream-rpms
Repository 'rhel-8-for-x86_64-appstream-rpms' is enabled for this system.
```

2. を実行します `yum repolist` コマンドを実行します

新しくサブスクライブしたリポジトリがリストに表示されます。

オペレーティングシステムが\* RHEL 9.x \*の場合は、次の手順 を使用してリポジトリへのアクセスを有効にします。

手順

1. 必要なリポジトリに登録します。

```
subscription-manager repos --enable rhel-9-for-x86_64-baseos-rpms
```

```
subscription-manager repos --enable rhel-9-for-x86_64-appstream-rpms
```

次の例は、このコマンドの実行例を示しています。

```
[root@localhost ~]# subscription-manager repos --enable rhel-9-for-x86_64-baseos-rpms
Repository 'rhel-9-for-x86_64-baseos-rpms' is enabled for this system.
[root@localhost ~]# subscription-manager repos --enable rhel-9-for-x86_64-appstream-rpms
Repository 'rhel-9-for-x86_64-appstream-rpms' is enabled for this system.
```

2. を実行します `yum repolist` コマンドを実行します

新しくサブスクライブしたリポジトリがリストに表示されます。

オペレーティングシステムが\* CentOS 7.x \*の場合、次の手順 を使用してリポジトリへのアクセスを有効にします。



以下の例はCentOS 7.6のリポジトリを示していますが、他のバージョンのCentOSでは機能しない可能性があります。使用しているCentOSのバージョンにはベースリポジトリを使用してください。

#### 手順

1. C7.6.1810 ベースリポジトリを追加します。C7.6.1810 - Baseヴォールトリポジトリには、ONTAPメディアーターに必要な"kernel-devel"パッケージが含まれています。
2. 次の行を /etc/yum.repos\_d/Center-Vault.repo に追加します。

```
[C7.6.1810-base]
name=CentOS-7.6.1810 - Base
baseurl=http://vault.centos.org/7.6.1810/os/$basearch/
gpgcheck=1
gpgkey=file:///etc/pki/rpm-gpg/RPM-GPG-KEY-CentOS-7
enabled=1
```

3. を実行します yum repolist コマンドを実行します

次の例は、このコマンドの実行例を示しています。CentOS-7.6.1810 ベースリポジトリがリストに表示されます。

```
Loaded plugins: fastestmirror
Loading mirror speeds from cached hostfile
* base: distro.ibiblio.org
* extras: distro.ibiblio.org
* updates: ewr.edge.kernel.org
C7.6.1810-base | 3.6 kB 00:00:00
(1/2): C7.6.1810-base/x86_64/group_gz | 166 kB 00:00:00
(2/2): C7.6.1810-base/x86_64/primary_db | 6.0 MB 00:00:04
repo id repo name status
C7.6.1810-base/x86_64 CentOS-7.6.1810 - Base 10,019
base/7/x86_64 CentOS-7 - Base 10,097
extras/7/x86_64 CentOS-7 - Extras 307
updates/7/x86_64 CentOS-7 - Updates 1,010
repolist: 21,433
[root@localhost ~]#
```

この手順は、オペレーティング・システムが\* Rocky Linux 8\*または\* Rocky Linux 9\*の場合に使用して、リポジトリへのアクセスを有効にします。

### 手順

1. 必要なリポジトリにサブスクライブします。

```
dnf config-manager --set-enabled baseos
```

```
dnf config-manager --set-enabled appstream
```

2. を実行します clean 操作：

```
dnf clean all
```

3. リポジトリのリストを確認します。

```
dnf repolist
```

```
[root@localhost ~]# dnf config-manager --set-enabled baseos
[root@localhost ~]# dnf config-manager --set-enabled appstream
[root@localhost ~]# dnf clean all
[root@localhost ~]# dnf repolist
repo id                                repo name
appstream                             Rocky Linux 8 - AppStream
baseos                                 Rocky Linux 8 - BaseOS
[root@localhost ~]#
```

```
[root@localhost ~]# dnf config-manager --set-enabled baseos
[root@localhost ~]# dnf config-manager --set-enabled appstream
[root@localhost ~]# dnf clean all
[root@localhost ~]# dnf repolist
repo id                                repo name
appstream                             Rocky Linux 9 - AppStream
baseos                                 Rocky Linux 9 - BaseOS
[root@localhost ~]#
```

メディエーターのインストールパッケージをダウンロードします

インストールプロセスの一環として、Mediatorのインストールパッケージをダウンロードします。

### 手順



1. ONTAP メディエーターのページからメディエーターのインストールパッケージをダウンロードします。

["ONTAP メディエーターのダウンロードページ"](#)

2. メディエーターのインストールパッケージが現在の作業ディレクトリにあることを確認します。

```
ls
```

```
[root@mediator-host ~]#ls
ontap-mediator-1.7.0.tgz
```



ONTAP メディエーターのバージョン1.4以前の場合、インストーラの名前はになります  
ontap-mediator。

インターネットにアクセスできない場所にいる場合は、インストーラが必要なパッケージにアクセスできることを確認する必要があります。

3. 必要に応じて、メディエーターのインストールパッケージをダウンロードディレクトリから Linux メディエーターホストのインストールディレクトリに移動します。
4. インストーラパッケージを解凍します。

```
tar xvfz ontap-mediator-1.7.0.tgz
```

```
[root@scs000099753 ~]# tar xvfz ontap-mediator-1.7.0.tgz
ontap-mediator-1.7.0/
ontap-mediator-1.7.0/ONTAP-Mediator-production.pub
ontap-mediator-1.7.0/tsa-prod-chain-ONTAP-Mediator.pem
ontap-mediator-1.7.0/tsa-prod-ONTAP-Mediator.pem
ontap-mediator-1.7.0/csc-prod-ONTAP-Mediator.pem
ontap-mediator-1.7.0/csc-prod-chain-ONTAP-Mediator.pem
ontap-mediator-1.7.0/ontap-mediator-1.7.0
ontap-mediator-1.7.0/ontap-mediator-1.7.0.sig.tsr
ontap-mediator-1.7.0/ontap-mediator-1.7.0.tsr
ontap-mediator-1.7.0/ontap-mediator-1.7.0.sig
```

## ONTAP メディエーターコードの署名を確認します

メディエーターのインストールパッケージをインストールする前に、ONTAP メディエーターコードの署名を確認する必要があります。

作業を開始する前に

メディエーターコードの署名を検証するには、システムが次の要件を満たしている必要があります。

- 基本的な検証のためのOpenSSLバージョン1.0.2～3.0

- Time Stamping Authority (TSA) 操作のOpenSSLバージョン1.1.0以降
- OCSP検証のためのパブリックインターネットアクセス

ダウンロードパッケージには次のファイルが含まれています。

ファイル。	説明
ONTAP-Mediator-development.pub	署名の検証に使用する公開鍵
csc-prod-chain-ONTAP-Mediator.pem	パブリック証明書CAの信頼チェーン
csc-prod-ONTAP-Mediator.pem	キーの生成に使用する証明書
ontap-mediator-1.7.0	バージョン1.7.0の製品インストール実行可能ファイル
ontap-mediator-1.7.0.sig	SHA-256はハッシュ化され、CSC-prodキーを使用してRSA署名されます（インストーラの署名）
ontap-mediator-1.7.0.sig.tsr	OCSCPがインストーラの署名に使用する失効要求
tsa-prod-ONTAP-Mediator.pem	TSRのパブリック証明書
tsa-prod-chain-ONTAP-Mediator.pem	TSRのパブリック証明書CAチェーン

## 手順

1. 失効チェックをオンにします csc-prod-ONTAP-Mediator.pem Online Certificate Status Protocol (OCSP) を使用します。
  - a. 開発者証明書ではURIが指定されていない可能性があるため、証明書の登録に使用するOCSP URLを検索します。

```
openssl x509 -noout -ocsp_uri -in csc-prod-chain-ONTAP-Mediator.pem
```

- b. 証明書のOCSP要求を生成します。

```
openssl ocsp -issuer csc-prod-chain-ONTAP-Mediator.pem -CAfile csc-prod-chain-ONTAP-Mediator.pem -cert csc-prod-ONTAP-Mediator.pem -reqout req.der
```

- c. OCSP Managerに接続してOCSP要求を送信します。

```
openssl ocsp -issuer csc-prod-chain-ONTAP-Mediator.pem -CAfile csc-prod-chain-ONTAP-Mediator.pem -cert csc-prod-ONTAP-Mediator.pem -url ${ocsp_uri} -resp_text -respout resp.der -verify_other csc-prod-chain-ONTAP-Mediator.pem
```

## 2. CSCの信頼チェーンと、ローカルホストに対する有効期限を確認します。

```
openssl verify
```



。openssl パスのバージョンは有効である必要があります cert.pem（自己署名ではありません）。

```
openssl verify -untrusted csc-prod-chain-ONTAP-Mediator.pem -CApath ${OPENSSLDIR} csc-prod-ONTAP-Mediator.pem # Failure action: The Code-Signature-Check certificate has expired or is invalid. Download a newer version of the ONTAP Mediator.  
openssl verify -untrusted tsa-prod-chain-ONTAP-Mediator.pem -CApath ${OPENSSLDIR} tsa-prod-ONTAP-Mediator.pem # Failure action: The Time-Stamp certificate has expired or is invalid. Download a newer version of the ONTAP Mediator.
```

## 3. を確認します ontap-mediator-1.6.0.sig.tsr および ontap-mediator-1.7.0.tsr 関連する証明書を使用しているファイル：

```
openssl ts -verify
```



.tsr ファイルには、インストーラとコード署名に関連付けられたタイムスタンプ応答が含まれます。タイムスタンプにTSAからの有効な署名があり、入力ファイルが変更されていないことが確認されます。  
検証はマシン上でローカルに実行されます。TSAサーバへのアクセスは不要です。

```
openssl ts -verify -data ontap-mediator-1.7.0.sig -in ontap-mediator-1.7.0.sig.tsr -CAfile tsa-prod-chain-ONTAP-Mediator.pem -untrusted tsa-prod-ONTAP-Mediator.pem  
openssl ts -verify -data ontap-mediator-1.7.0 -in ontap-mediator-1.7.0.tsr -CAfile tsa-prod-chain-ONTAP-Mediator.pem -untrusted tsa-prod-ONTAP-Mediator.pem
```

## 4. キーに対して署名を確認します。

```
openssl -dgst -verify
```

```
openssl dgst -sha256 -verify ONTAP-Mediator-production.pub -signature  
ontap-mediator-1.7.0.sig ontap-mediator-1.7.0
```

## ONTAP メディエーターコードの署名の確認（コンソール出力）の例

```
[root@scspa2695423001 ontap-mediator-1.7.0]# pwd
/root/ontap-mediator-1.7.0
[root@scspa2695423001 ontap-mediator-1.7.0]# ls -l
total 63660
-r--r--r-- 1 root root      8582 Feb 19 15:02 csc-prod-chain-ONTAP-
Mediator.pem
-r--r--r-- 1 root root      2373 Feb 19 15:02 csc-prod-ONTAP-
Mediator.pem
-r-xr-xr-- 1 root root 65132818 Feb 20 15:17 ontap-mediator-1.7.0
-rw-r--r-- 1 root root      384 Feb 20 15:17 ontap-mediator-1.7.0.sig
-rw-r--r-- 1 root root      5437 Feb 20 15:17 ontap-mediator-
1.7.0.sig.tsr
-rw-r--r-- 1 root root      5436 Feb 20 15:17 ontap-mediator-1.7.0.tsr
-r--r--r-- 1 root root      625 Feb 19 15:02 ONTAP-Mediator-
production.pub
-r--r--r-- 1 root root      3323 Feb 19 15:02 tsa-prod-chain-ONTAP-
Mediator.pem
-r--r--r-- 1 root root      1740 Feb 19 15:02 tsa-prod-ONTAP-
Mediator.pem
[root@scspa2695423001 ontap-mediator-1.7.0]#
[root@scspa2695423001 ontap-mediator-1.7.0]#
/root/verify_ontap_mediator_signatures.sh
++ openssl version -d
++ cut -d '"' -f2
+ OPENSSLDIR=/etc/pki/tls
+ openssl version
OpenSSL 1.1.1k  FIPS 25 Mar 2021
++ openssl x509 -noout -ocsp_uri -in csc-prod-chain-ONTAP-Mediator.pem
+ ocsp_uri=http://ocsp.entrust.net
+ echo http://ocsp.entrust.net
http://ocsp.entrust.net
+ openssl ocsp -issuer csc-prod-chain-ONTAP-Mediator.pem -CAfile csc-
prod-chain-ONTAP-Mediator.pem -cert csc-prod-ONTAP-Mediator.pem -reqout
req.der
+ openssl ocsp -issuer csc-prod-chain-ONTAP-Mediator.pem -CAfile csc-
prod-chain-ONTAP-Mediator.pem -cert csc-prod-ONTAP-Mediator.pem -url
http://ocsp.entrust.net -resp_text -respout resp.der -verify_other csc-
prod-chain-ONTAP-Mediator.pem
OCSP Response Data:
  OCSF Response Status: successful (0x0)
  Response Type: Basic OCSP Response
  Version: 1 (0x0)
  Responder Id: C = US, O = "Entrust, Inc.", CN = Entrust Extended
```

Validation Code Signing CA - EVCS2

Produced At: Feb 28 05:01:00 2023 GMT

Responses:

Certificate ID:

Hash Algorithm: sha1

Issuer Name Hash: 69FA640329AB84E27220FE0927647B8194B91F2A

Issuer Key Hash: CE894F8251AA15A28462CA312361D261F8FE78

Serial Number: 511A542B57522AEB7295A640DC6200E5

Cert Status: good

This Update: Feb 28 05:00:00 2023 GMT

Next Update: Mar 4 04:59:59 2023 GMT

Signature Algorithm: sha512WithRSAEncryption

3c:1d:49:b0:93:62:37:3e:c7:38:e3:9f:9f:62:82:73:ed:f4:  
ea:00:6b:f1:01:cd:79:57:92:f1:9d:5d:85:9b:60:59:f8:6c:  
e6:f4:50:51:f3:4c:8a:51:dd:50:68:16:8f:20:24:7e:39:b0:  
44:94:8d:b0:61:da:b9:08:36:74:2d:44:55:62:fb:92:be:4a:  
e7:6c:8c:49:dd:0c:fd:d8:ce:20:08:0d:0f:5a:29:a3:19:03:  
9f:d3:df:41:f4:89:0f:73:18:3f:ac:bb:a7:a3:96:7d:c5:70:  
4c:57:cd:17:17:c6:8a:60:d1:37:c9:2d:81:07:2a:d7:a6:02:  
ee:ce:88:16:22:db:e3:43:64:1e:9b:0d:4d:31:66:fa:ab:a5:  
52:99:94:4a:4a:d0:52:c5:34:f5:18:c7:15:5b:ce:74:c2:fc:  
61:ea:55:aa:f1:2f:82:a3:6a:95:8d:7e:2b:38:49:4f:bf:b1:  
68:7b:1b:24:8b:1f:4d:c5:77:f0:71:af:9c:34:c8:7a:82:50:  
09:a2:19:6e:c6:30:4f:da:a2:79:08:f9:d0:ff:85:d9:2a:84:  
cf:0c:aa:75:8f:72:c9:a7:a2:83:e8:8b:cf:ed:0c:69:75:b6:  
2a:7b:6b:58:99:01:d8:34:ad:e1:89:25:27:1b:fa:d9:6d:32:  
97:3a:0b:0a:8e:a3:9e:e3:f4:e0:d6:1a:c9:b5:14:8c:3e:54:  
3b:37:17:1a:93:44:84:8b:4a:87:97:1e:76:43:3e:d3:ec:8b:  
7e:56:4a:3f:01:31:c0:e5:58:fb:50:ce:6f:b1:e7:35:f9:b7:  
a3:ef:6b:3b:21:95:37:a6:5b:8f:f0:15:18:36:65:89:a1:9c:  
9b:69:00:b4:b1:65:6a:bc:11:2d:d4:9b:b4:97:cc:cb:7a:0c:  
16:11:c1:75:58:7e:13:ab:56:3c:3f:93:5b:95:24:c6:54:52:  
1f:86:a9:16:ce:d9:ea:8b:3a:f3:4f:c4:8f:ad:de:e8:3e:3c:  
d2:51:51:ad:33:7f:d8:c5:33:24:26:f1:2d:9d:0e:9f:55:d0:  
68:bf:af:bd:68:4a:40:08:bc:92:a0:62:54:7d:16:7b:36:29:  
15:b1:cd:58:8e:fb:4a:f2:3e:94:8b:fe:56:95:cc:24:32:af:  
5f:71:99:18:ed:0c:64:94:f7:54:48:87:48:d0:6d:b3:42:04:  
96:03:73:a2:8e:8a:6a:b2:af:ee:56:19:a1:c6:35:12:59:ad:  
19:6a:fe:e0:f1:27:cc:96:4e:f0:4f:fb:6a:bd:ce:05:2c:aa:  
79:7c:df:02:5c:ca:53:7d:60:12:88:7c:ce:15:c7:d4:02:27:  
c1:ab:cf:71:30:1e:14:ba

WARNING: no nonce in response

Response verify OK

csc-prod-ONTAP-Mediator.pem: good

This Update: Feb 28 05:00:00 2023 GMT

```

Next Update: Mar  4 04:59:59 2023 GMT
+ openssl verify -untrusted csc-prod-chain-ONTAP-Mediator.pem -CApath
/etc/pki/tls csc-prod-ONTAP-Mediator.pem
csc-prod-ONTAP-Mediator.pem: OK
+ openssl verify -untrusted tsa-prod-chain-ONTAP-Mediator.pem -CApath
/etc/pki/tls tsa-prod-ONTAP-Mediator.pem
tsa-prod-ONTAP-Mediator.pem: OK
+ openssl ts -verify -data ontap-mediator-1.7.0.sig -in ontap-mediator-
1.7.0.sig.tsr -CAfile tsa-prod-chain-ONTAP-Mediator.pem -untrusted tsa-
prod-ONTAP-Mediator.pem
Using configuration from /etc/pki/tls/openssl.cnf
Verification: OK
+ openssl ts -verify -data ontap-mediator-1.7.0 -in ontap-mediator-
1.7.0.tsr -CAfile tsa-prod-chain-ONTAP-Mediator.pem -untrusted tsa-
prod-ONTAP-Mediator.pem
Using configuration from /etc/pki/tls/openssl.cnf
Verification: OK
+ openssl dgst -sha256 -verify ONTAP-Mediator-production.pub -signature
ontap-mediator-1.7.0.sig ontap-mediator-1.7.0
Verified OK
[root@scspa2695423001 ontap-mediator-1.7.0]#

```

## ONTAP メディエーターのインストールパッケージをインストールします

ONTAP メディエーターサービスをインストールするには、インストールパッケージを取得してホストでインストーラを実行する必要があります。

### 手順

1. インストーラを実行し、必要に応じてプロンプトに回答します。

```
./ontap-mediator-1.7.0/ontap-mediator-1.7.0 -y
```

```
[root@scs000099753 ~]# ./ontap-mediator-1.5.0/ontap-mediator-1.7.0 -y
```

インストールプロセスが開始され、必要なアカウントの作成と必要なパッケージのインストールが行われます。以前のバージョンのメディエーターがホストにインストールされている場合は、アップグレードを確認するプロンプトが表示されます。

2. ONTAP メディエーター1.4以降では、セキュアブートメカニズムはUEFIシステムで有効になっています。セキュアブートが有効になっている場合は、インストール後に追加の手順を実行してセキュリティキーを登録する必要があります。

- README ファイルの指示に従って SCST カーネルモジュールに署名します。

```
/opt/netapp/lib/ontap_mediator/ontap_mediator/SCST_mod_keys/README.module-
signing
```

- 必要なキーを探します。

```
/opt/netapp/lib/ontap_mediator/ontap_mediator/SCST_mod_keys
```



インストール後は、READMEファイルとキーの場所もシステム出力に含まれています。



## ONTAP Mediator 1.6のインストール例（コンソール出力）

```
[root@scs000099753 ~]# ./ontap-mediator-1.6.0/ontap-mediator-1.6.0 -y
ONTAP Mediator: Self Extracting Installer

+ Extracting the ONTAP Mediator installation/upgrade archive
+ Performing the ONTAP Mediator run-time code signature check
  Using openssl from the path: /usr/bin/openssl configured for
  CApath:/etc/pki/tls

+ Unpacking the ONTAP Mediator installer
ONTAP Mediator requires two user accounts. One for the service
(netapp), and one for use by ONTAP to the mediator API (mediatoradmin).
Using default account names: netapp + mediatoradmin

Enter ONTAP Mediator user account (mediatoradmin) password:

Re-Enter ONTAP Mediator user account (mediatoradmin) password:

+ Checking if SELinux is in enforcing mode

+ Checking for default Linux firewall
success
success
success

#####
Preparing for installation of ONTAP Mediator packages.

+ Installing required packages.

Last metadata expiration check: 0:25:24 ago on Fri 21 Oct 2022 04:00:13
PM EDT.
Package openssl-1:1.1.1k-4.el8.x86_64 is already installed.
Package gcc-8.4.1-1.el8.x86_64 is already installed.
Package python36-3.6.8-2.module+el8.1.0+3334+5cb623d7.x86_64 is already
installed.
Package libselinux-utils-2.9-5.el8.x86_64 is already installed.
Package perl-Data-Dumper-2.167-399.el8.x86_64 is already installed.
Package efibootmgr-16-1.el8.x86_64 is already installed.
Package mokutil-1:0.3.0-11.el8.x86_64 is already installed.
```

Package python3-pip-9.0.3-19.el8.noarch is already installed.  
 Package polycoreutils-python-utils-2.9-14.el8.noarch is already installed.  
 Dependencies resolved.

```

=====
=====
=====
Package                                Architecture
Version                                Repository
Size
=====
=====
=====
Installing:
  bzip2                                x86_64
1.0.6-26.el8                            rhel-8-for-
x86_64-baseos-rpms                      60 k
  elfutils-libelf-devel                 x86_64
0.186-1.el8                            rhel-8-for-
x86_64-baseos-rpms                      60 k
  kernel-devel                         x86_64
4.18.0-348.el8                          rhel-8-for-
x86_64-baseos-rpms                      20 M
  make                                 x86_64
1:4.2.1-11.el8                          rhel-8-for-
x86_64-baseos-rpms                      498 k
  openssl-devel                        x86_64
1:1.1.1k-7.el8_6                       rhel-8-for-
x86_64-baseos-rpms                      2.3 M
  patch                                x86_64
2.7.6-11.el8                            rhel-8-for-
x86_64-baseos-rpms                      138 k
  perl-ExtUtils-MakeMaker               noarch
1:7.34-1.el8                            rhel-8-for-
x86_64-appstream-rpms                   301 k
  python36-devel                       x86_64
3.6.8-38.module+el8.5.0+12207+5c5719bc rhel-8-for-
x86_64-appstream-rpms                   17 k
  redhat-lsb-core                      x86_64
4.1-47.el8                              rhel-8-for-
x86_64-appstream-rpms                   45 k
Upgrading:
  cpp                                 x86_64
8.5.0-10.1.el8_6                       rhel-8-for-
x86_64-appstream-rpms                   10 M
  elfutils-libelf                     x86_64

```

0.186-1.el8			rhel-8-for-
x86_64-baseos-rpms	229 k		
elfutils-libs		x86_64	
0.186-1.el8			rhel-8-for-
x86_64-baseos-rpms	295 k		
gcc		x86_64	
8.5.0-10.1.el8_6			rhel-8-for-
x86_64-appstream-rpms	23 M		
libgcc		x86_64	
8.5.0-10.1.el8_6			rhel-8-for-
x86_64-baseos-rpms	80 k		
libgomp		x86_64	
8.5.0-10.1.el8_6			rhel-8-for-
x86_64-baseos-rpms	207 k		
libsemanage		x86_64	
2.9-8.el8			rhel-8-for-
x86_64-baseos-rpms	168 k		
mokutil		x86_64	
1:0.3.0-11.el8_6.1			rhel-8-for-
x86_64-baseos-rpms	46 k		
openssl		x86_64	
1:1.1.1k-7.el8_6			rhel-8-for-
x86_64-baseos-rpms	709 k		
openssl-libs		x86_64	
1:1.1.1k-7.el8_6			rhel-8-for-
x86_64-baseos-rpms	1.5 M		
platform-python-pip		noarch	
9.0.3-22.el8			rhel-8-for-
x86_64-baseos-rpms	1.6 M		
policycoreutils		x86_64	
2.9-19.el8			rhel-8-for-
x86_64-baseos-rpms	374 k		
policycoreutils-python-utils		noarch	
2.9-19.el8			rhel-8-for-
x86_64-baseos-rpms	253 k		
python3-libsemanage		x86_64	
2.9-8.el8			rhel-8-for-
x86_64-baseos-rpms	128 k		
python3-pip		noarch	
9.0.3-22.el8			rhel-8-for-
x86_64-appstream-rpms	20 k		
python3-policycoreutils		noarch	
2.9-19.el8			rhel-8-for-
x86_64-baseos-rpms	2.2 M		
python36		x86_64	
3.6.8-38.module+el8.5.0+12207+5c5719bc			rhel-8-for-

```

x86_64-appstream-rpms                    19 k
Installing dependencies:
  annobin                                x86_64
10.29-3.el8                               rhel-8-for-
x86_64-appstream-rpms                    117 k
  at                                    x86_64
3.1.20-11.el8                             rhel-8-for-
x86_64-baseos-rpms                       81 k
  bc                                    x86_64
1.07.1-5.el8                             rhel-8-for-
x86_64-baseos-rpms                      129 k
  cups-client                          x86_64
1:2.2.6-38.el8                           rhel-8-for-
x86_64-appstream-rpms                   169 k
  dwz                                  x86_64
0.12-10.el8                              rhel-8-for-
x86_64-appstream-rpms                   109 k
  ed                                    x86_64
1.14.2-4.el8                             rhel-8-for-
x86_64-baseos-rpms                      82 k
  efi-srpm-macros                      noarch
3-3.el8                                  rhel-8-for-
x86_64-appstream-rpms                   22 k
  esmtplib                             x86_64
1.2-15.el8                               EPEL-8
57 k
  glibc-srpm-macros                    noarch
1.4.2-7.el8                             rhel-8-for-
x86_64-appstream-rpms                   9.4 k
  go-srpm-macros                       noarch
2-17.el8                                 rhel-8-for-
x86_64-appstream-rpms                   13 k
  keyutils-libs-devel                  x86_64
1.5.10-6.el8                             rhel-8-for-
x86_64-baseos-rpms                      48 k
  krb5-devel                           x86_64
1.18.2-14.el8                           rhel-8-for-
x86_64-baseos-rpms                     560 k
  libcom_err-devel                     x86_64
1.45.6-2.el8                             rhel-8-for-
x86_64-baseos-rpms                      38 k
  libesmtplib                          x86_64
1.0.6-18.el8                             EPEL-8
70 k
  libkadm5                             x86_64
1.18.2-14.el8                           rhel-8-for-

```

x86_64-baseos-rpms	187 k		
libblockfile		x86_64	
1.14-1.el8			rhel-8-for-
x86_64-appstream-rpms	32 k		
libselinux-devel		x86_64	
2.9-5.el8			rhel-8-for-
x86_64-baseos-rpms	200 k		
libsepol-devel		x86_64	
2.9-3.el8			rhel-8-for-
x86_64-baseos-rpms	87 k		
libverto-devel		x86_64	
0.3.0-5.el8			rhel-8-for-
x86_64-baseos-rpms	18 k		
m4		x86_64	
1.4.18-7.el8			rhel-8-for-
x86_64-baseos-rpms	223 k		
mailx		x86_64	
12.5-29.el8			rhel-8-for-
x86_64-baseos-rpms	257 k		
ncurses-compat-libs		x86_64	
6.1-9.20180224.el8			rhel-8-for-
x86_64-baseos-rpms	328 k		
ocaml-srpm-macros		noarch	
5-4.el8			rhel-8-for-
x86_64-appstream-rpms	9.5 k		
openblas-srpm-macros		noarch	
2-2.el8			rhel-8-for-
x86_64-appstream-rpms	8.0 k		
pcre2-devel		x86_64	
10.32-2.el8			rhel-8-for-
x86_64-baseos-rpms	605 k		
pcre2-utf16		x86_64	
10.32-2.el8			rhel-8-for-
x86_64-baseos-rpms	229 k		
pcre2-utf32		x86_64	
10.32-2.el8			rhel-8-for-
x86_64-baseos-rpms	220 k		
perl-CPAN-Meta-YAML		noarch	
0.018-397.el8			rhel-8-for-
x86_64-appstream-rpms	34 k		
perl-ExtUtils-Command		noarch	
1:7.34-1.el8			rhel-8-for-
x86_64-appstream-rpms	19 k		
perl-ExtUtils-Install		noarch	
2.14-4.el8			rhel-8-for-
x86_64-appstream-rpms	46 k		

perl-ExtUtils-Manifest		noarch	
1.70-395.el8			rhel-8-for-
x86_64-appstream-rpms	37 k		
perl-ExtUtils-ParseXS		noarch	
1:3.35-2.el8			rhel-8-for-
x86_64-appstream-rpms	83 k		
perl-JSON-PP		noarch	
1:2.97.001-3.el8			rhel-8-for-
x86_64-appstream-rpms	68 k		
perl-Math-BigInt		noarch	
1:1.9998.11-7.el8			rhel-8-for-
x86_64-baseos-rpms	196 k		
perl-Math-Complex		noarch	
1.59-421.el8			rhel-8-for-
x86_64-baseos-rpms	109 k		
perl-Test-Harness		noarch	
1:3.42-1.el8			rhel-8-for-
x86_64-appstream-rpms	279 k		
perl-devel		x86_64	
4:5.26.3-419.el8_4.1			rhel-8-for-
x86_64-appstream-rpms	599 k		
perl-srpm-macros		noarch	
1-25.el8			rhel-8-for-
x86_64-appstream-rpms	11 k		
perl-version		x86_64	
6:0.99.24-1.el8			rhel-8-for-
x86_64-appstream-rpms	67 k		
platform-python-devel		x86_64	
3.6.8-41.el8			rhel-8-for-
x86_64-appstream-rpms	249 k		
python-rpm-macros		noarch	
3-41.el8			rhel-8-for-
x86_64-appstream-rpms	15 k		
python-srpm-macros		noarch	
3-41.el8			rhel-8-for-
x86_64-appstream-rpms	15 k		
python3-pyparsing		noarch	
2.1.10-7.el8			rhel-8-for-
x86_64-baseos-rpms	142 k		
python3-rpm-generators		noarch	
5-7.el8			rhel-8-for-
x86_64-appstream-rpms	25 k		
python3-rpm-macros		noarch	
3-41.el8			rhel-8-for-
x86_64-appstream-rpms	14 k		
qt5-srpm-macros		noarch	

5.15.2-1.el8			rhel-8-for-
x86_64-appstream-rpms	11 k		
redhat-lsb-submod-security		x86_64	
4.1-47.el8			rhel-8-for-
x86_64-appstream-rpms	22 k		
redhat-rpm-config		noarch	
125-1.el8			rhel-8-for-
x86_64-appstream-rpms	87 k		
rust-srpm-macros		noarch	
5-2.el8			rhel-8-for-
x86_64-appstream-rpms	9.3 k		
spax		x86_64	
1.5.3-13.el8			rhel-8-for-
x86_64-baseos-rpms	217 k		
systemtap-sdt-devel		x86_64	
4.6-4.el8			rhel-8-for-
x86_64-appstream-rpms	86 k		
time		x86_64	
1.9-3.el8			rhel-8-for-
x86_64-baseos-rpms	54 k		
unzip		x86_64	
6.0-46.el8			rhel-8-for-
x86_64-baseos-rpms	196 k		
util-linux-user		x86_64	
2.32.1-28.el8			rhel-8-for-
x86_64-baseos-rpms	100 k		
zip		x86_64	
3.0-23.el8			rhel-8-for-
x86_64-baseos-rpms	270 k		
zlib-devel		x86_64	
1.2.11-17.el8			rhel-8-for-
x86_64-baseos-rpms	58 k		
Installing weak dependencies:			
perl-CPAN-Meta		noarch	
2.150010-396.el8			rhel-8-for-
x86_64-appstream-rpms	191 k		
perl-CPAN-Meta-Requirements		noarch	
2.140-396.el8			rhel-8-for-
x86_64-appstream-rpms	37 k		
perl-Encode-Locale		noarch	
1.05-10.module+el8.3.0+6498+9eecfe51			rhel-8-for-
x86_64-appstream-rpms	22 k		
perl-Time-HiRes		x86_64	
4:1.9758-2.el8			rhel-8-for-
x86_64-appstream-rpms	61 k		

## Transaction Summary

=====  
=====

Install 69 Packages

Upgrade 17 Packages

Total download size: 72 M

Is this ok [y/N]: y

Downloading Packages:

(1/86): perl-ExtUtils-Install-2.14-4.el8.noarch.rpm

735 kB/s | 46 kB 00:00

(2/86): libesmtp-1.0.6-18.el8.x86\_64.rpm

1.0 MB/s | 70 kB 00:00

(3/86): esmtp-1.2-15.el8.x86\_64.rpm

747 kB/s | 57 kB 00:00

(4/86): rust-srpm-macros-5-2.el8.noarch.rpm

308 kB/s | 9.3 kB 00:00

(5/86): perl-ExtUtils-Manifest-1.70-395.el8.noarch.rpm

781 kB/s | 37 kB 00:00

(6/86): perl-CPAN-Meta-2.150010-396.el8.noarch.rpm

2.7 MB/s | 191 kB 00:00

(7/86): ocaml-srpm-macros-5-4.el8.noarch.rpm

214 kB/s | 9.5 kB 00:00

(8/86): perl-JSON-PP-2.97.001-3.el8.noarch.rpm

1.2 MB/s | 68 kB 00:00

(9/86): perl-ExtUtils-MakeMaker-7.34-1.el8.noarch.rpm

5.8 MB/s | 301 kB 00:00

(10/86): ghc-srpm-macros-1.4.2-7.el8.noarch.rpm

317 kB/s | 9.4 kB 00:00

(11/86): perl-Test-Harness-3.42-1.el8.noarch.rpm

4.5 MB/s | 279 kB 00:00

(12/86): perl-ExtUtils-Command-7.34-1.el8.noarch.rpm

520 kB/s | 19 kB 00:00

...

15 MB/s | 1.5 MB 00:00

-----  
-----  
-----  
Total

35 MB/s | 72 MB 00:02

Running transaction check

Transaction check succeeded.

Running transaction test



```

Transaction test succeeded.
Running transaction
  Preparing      :
1/1
  Running scriptlet: openssl-libs-1:1.1.1k-7.el8_6.x86_64
1/1
  Upgrading       : openssl-libs-1:1.1.1k-7.el8_6.x86_64
1/103
  Running scriptlet: openssl-libs-1:1.1.1k-7.el8_6.x86_64
1/103
  Upgrading       : libgcc-8.5.0-10.1.el8_6.x86_64
2/103
  Running scriptlet: libgcc-8.5.0-10.1.el8_6.x86_64
2/103
  Upgrading       : elfutils-libelf-0.186-1.el8.x86_64
3/103
  Installing      : perl-version-6:0.99.24-1.el8.x86_64
4/103
  Installing      : perl-CPAN-Meta-Requirements-2.140-396.el8.noarch
5/103
  Upgrading       : libsemanage-2.9-8.el8.x86_64
6/103
  Installing      : zlib-devel-1.2.11-17.el8.x86_64
7/103
  Installing      : python-srpm-macros-3-41.el8.noarch
8/103
  Installing      : python-rpm-macros-3-41.el8.noarch
9/103
  Installing      : python3-rpm-macros-3-41.el8.noarch
10/103
  Installing      : perl-Time-HiRes-4:1.9758-2.el8.x86_64
11/103
  Installing      : perl-ExtUtils-ParseXS-1:3.35-2.el8.noarch
12/103
  Installing      : perl-Test-Harness-1:3.42-1.el8.noarch
13/103
  Upgrading       : python3-libsemanage-2.9-8.el8.x86_64
14/103
  Upgrading       : polycoreutils-2.9-19.el8.x86_64
15/103
  Running scriptlet: polycoreutils-2.9-19.el8.x86_64
15/103
  Upgrading       : python3-polycoreutils-2.9-19.el8.noarch
16/103
  Installing      : dwz-0.12-10.el8.x86_64
17/103

```

```
Installing      : ncurses-compat-libs-6.1-9.20180224.el8.x86_64
18/103
Installing      : libesmtplib-1.0.6-18.el8.x86_64
19/103
Installing      : mailx-12.5-29.el8.x86_64
20/103
Installing      : libkadm5-1.18.2-14.el8.x86_64
21/103
Upgrading       : libgomp-8.5.0-10.1.el8_6.x86_64
22/103
Running scriptlet: libgomp-8.5.0-10.1.el8_6.x86_64
22/103
Upgrading       : platform-python-pip-9.0.3-22.el8.noarch
23/103
Upgrading       : python3-pip-9.0.3-22.el8.noarch
24/103
Upgrading       : python36-3.6.8-
38.module+el8.5.0+12207+5c5719bc.x86_64
25/103
Running scriptlet: python36-3.6.8-
38.module+el8.5.0+12207+5c5719bc.x86_64
25/103
Upgrading       : cpp-8.5.0-10.1.el8_6.x86_64
26/103
Running scriptlet: cpp-8.5.0-10.1.el8_6.x86_64
26/103
Upgrading       : gcc-8.5.0-10.1.el8_6.x86_64
27/103
Running scriptlet: gcc-8.5.0-10.1.el8_6.x86_64
27/103
Installing      : annobin-10.29-3.el8.x86_64
28/103
Installing      : unzip-6.0-46.el8.x86_64
29/103
Installing      : zip-3.0-23.el8.x86_64
30/103
Installing      : perl-Math-Complex-1.59-421.el8.noarch
31/103
Installing      : perl-Math-BigInt-1:1.9998.11-7.el8.noarch
32/103
Installing      : perl-JSON-PP-1:2.97.001-3.el8.noarch
33/103
Installing      : make-1:4.2.1-11.el8.x86_64
34/103
Running scriptlet: make-1:4.2.1-11.el8.x86_64
34/103
```

```
Installing      : libcom_err-devel-1.45.6-2.el8.x86_64
35/103
Installing      : util-linux-user-2.32.1-28.el8.x86_64
36/103
Installing      : libsepol-devel-2.9-3.el8.x86_64
37/103
Installing      : pcre2-utf32-10.32-2.el8.x86_64
38/103
Installing      : pcre2-utf16-10.32-2.el8.x86_64
39/103
Installing      : pcre2-devel-10.32-2.el8.x86_64
40/103
Installing      : libselinux-devel-2.9-5.el8.x86_64
41/103
Installing      : patch-2.7.6-11.el8.x86_64
42/103
Installing      : python3-pyparsing-2.1.10-7.el8.noarch
43/103
Installing      : systemtap-sdt-devel-4.6-4.el8.x86_64
44/103
Installing      : spax-1.5.3-13.el8.x86_64
45/103
Running scriptlet: spax-1.5.3-13.el8.x86_64
45/103
Installing      : m4-1.4.18-7.el8.x86_64
46/103
Running scriptlet: m4-1.4.18-7.el8.x86_64
46/103
Installing      : libverto-devel-0.3.0-5.el8.x86_64
47/103
Installing      : bc-1.07.1-5.el8.x86_64
48/103
Running scriptlet: bc-1.07.1-5.el8.x86_64
48/103
Installing      : at-3.1.20-11.el8.x86_64
49/103
Running scriptlet: at-3.1.20-11.el8.x86_64
49/103
Installing      : keyutils-libs-devel-1.5.10-6.el8.x86_64
50/103
Installing      : krb5-devel-1.18.2-14.el8.x86_64
51/103
Installing      : time-1.9-3.el8.x86_64
52/103
Running scriptlet: time-1.9-3.el8.x86_64
52/103
```

```

Upgrading      : polycoreutils-python-utils-2.9-19.el8.noarch
80/103
Installing     : elfutils-libelf-devel-0.186-1.el8.x86_64
81/103
Upgrading      : elfutils-libs-0.186-1.el8.x86_64
82/103
Upgrading      : mokutil-1:0.3.0-11.el8_6.1.x86_64
83/103
Upgrading      : openssl-1:1.1.1k-7.el8_6.x86_64
84/103
Installing     : kernel-devel-4.18.0-348.el8.x86_64
85/103
Running scriptlet: kernel-devel-4.18.0-348.el8.x86_64

...

85/103
Installing     : bzip2-1.0.6-26.el8.x86_64
86/103
Cleanup        : polycoreutils-python-utils-2.9-14.el8.noarch
87/103
Cleanup        : python3-polycoreutils-2.9-14.el8.noarch
88/103
Cleanup        : python36-3.6.8-
2.module+el8.1.0+3334+5cb623d7.x86_64
89/103
Running scriptlet: python36-3.6.8-
2.module+el8.1.0+3334+5cb623d7.x86_64
89/103
Cleanup        : elfutils-libs-0.185-1.el8.x86_64
90/103
Cleanup        : openssl-1:1.1.1k-4.el8.x86_64
91/103
Cleanup        : python3-libsemanage-2.9-6.el8.x86_64
92/103
Running scriptlet: gcc-8.4.1-1.el8.x86_64
93/103
Cleanup        : gcc-8.4.1-1.el8.x86_64
93/103
Running scriptlet: polycoreutils-2.9-14.el8.x86_64
94/103
Cleanup        : polycoreutils-2.9-14.el8.x86_64
94/103
Cleanup        : mokutil-1:0.3.0-11.el8.x86_64
95/103

```

```

Cleanup      : python3-pip-9.0.3-19.el8.noarch
96/103
Cleanup      : platform-python-pip-9.0.3-19.el8.noarch
97/103
Cleanup      : openssl-libs-1:1.1.1k-4.el8.x86_64
98/103
Running scriptlet: openssl-libs-1:1.1.1k-4.el8.x86_64
98/103
Cleanup      : libsemanage-2.9-6.el8.x86_64
99/103
Running scriptlet: cpp-8.4.1-1.el8.x86_64
100/103
Cleanup      : cpp-8.4.1-1.el8.x86_64
100/103
Cleanup      : libgcc-8.5.0-3.el8.x86_64
101/103
Running scriptlet: libgcc-8.5.0-3.el8.x86_64
101/103
Running scriptlet: libgomp-8.4.1-1.el8.x86_64
102/103
Cleanup      : libgomp-8.4.1-1.el8.x86_64
102/103
Running scriptlet: libgomp-8.4.1-1.el8.x86_64
102/103
Cleanup      : elfutils-libelf-0.185-1.el8.x86_64
103/103
Running scriptlet: elfutils-libelf-0.185-1.el8.x86_64
103/103
Verifying    : esmtp-1.2-15.el8.x86_64
1/103
Verifying    : libesmtp-1.0.6-18.el8.x86_64

...

Upgraded:
  cpp-8.5.0-10.1.el8_6.x86_64                                elfutils-
libelf-0.186-1.el8.x86_64      elfutils-libs-0.186-1.el8.x86_64
gcc-8.5.0-10.1.el8_6.x86_64
  libgcc-8.5.0-10.1.el8_6.x86_64                                libgomp-
8.5.0-10.1.el8_6.x86_64      libsemanage-2.9-8.el8.x86_64
mokutil-1:0.3.0-11.el8_6.1.x86_64
  openssl-1:1.1.1k-7.el8_6.x86_64                                openssl-
libs-1:1.1.1k-7.el8_6.x86_64      platform-python-pip-9.0.3-22.el8.noarch
policycoreutils-2.9-19.el8.x86_64
  policycoreutils-python-utils-2.9-19.el8.noarch                python3-
libsemanage-2.9-8.el8.x86_64      python3-pip-9.0.3-22.el8.noarch

```

```

python3-policycoreutils-2.9-19.el8.noarch
python36-3.6.8-38.module+el8.5.0+12207+5c5719bc.x86_64
Installed:
annobin-10.29-3.el8.x86_64                                     at-
3.1.20-11.el8.x86_64                                           bc-1.07.1-5.el8.x86_64
bzip2-1.0.6-26.el8.x86_64
cups-client-1:2.2.6-38.el8.x86_64                             dwz-0.12-
10.el8.x86_64
ed-1.14.2-4.el8.x86_64
efi-srpm-macros-3-3.el8.noarch                                 elfutils-libelf-
devel-0.186-1.el8.x86_64
esmtplib-1.2-15.el8.x86_64
ghc-srpm-macros-1.4.2-7.el8.noarch                             go-srpm-macros-2-
17.el8.noarch
kernel-devel-4.18.0-348.el8.x86_64
keyutils-libs-devel-1.5.10-6.el8.x86_64                     krb5-devel-1.18.2-
14.el8.x86_64
libcom_err-devel-1.45.6-2.el8.x86_64
libesmtplib-1.0.6-18.el8.x86_64                             libkadm5-1.18.2-
14.el8.x86_64
libblockfile-1.14-1.el8.x86_64
libselinux-devel-2.9-5.el8.x86_64                             libsepol-devel-2.9-
3.el8.x86_64
libverto-devel-0.3.0-5.el8.x86_64                             m4-
1.4.18-7.el8.x86_64                                           mailx-12.5-
29.el8.x86_64
make-1:4.2.1-11.el8.x86_64
ncurses-compat-libs-6.1-9.20180224.el8.x86_64               ocaml-srpm-macros-
5-4.el8.noarch
openblas-srpm-macros-2-2.el8.noarch
openssl-devel-1:1.1.1k-7.el8_6.x86_64                       patch-2.7.6-
11.el8.x86_64
pcre2-devel-10.32-2.el8.x86_64
pcre2-utf16-10.32-2.el8.x86_64                               pcre2-utf32-10.32-
2.el8.x86_64
perl-CPAN-Meta-2.150010-396.el8.noarch
perl-CPAN-Meta-Requirements-2.140-396.el8.noarch             perl-CPAN-Meta-
YAML-0.018-397.el8.noarch
perl-Encode-Locale-1.05-10.module+el8.3.0+6498+9eecfe51.noarch
perl-ExtUtils-Command-1:7.34-1.el8.noarch                     perl-ExtUtils-
Install-2.14-4.el8.noarch
perl-ExtUtils-MakeMaker-1:7.34-1.el8.noarch
perl-ExtUtils-Manifest-1.70-395.el8.noarch                   perl-ExtUtils-
ParseXS-1:3.35-2.el8.noarch
perl-JSON-PP-1:2.97.001-3.el8.noarch
perl-Math-BigInt-1:1.9998.11-7.el8.noarch                    perl-Math-Complex-

```

```

1.59-421.el8.noarch
perl-Test-Harness-1:3.42-1.el8.noarch
perl-Time-HiRes-4:1.9758-2.el8.x86_64 perl-devel-
4:5.26.3-419.el8_4.1.x86_64
perl-srpm-macros-1-25.el8.noarch
perl-version-6:0.99.24-1.el8.x86_64 platform-python-
devel-3.6.8-41.el8.x86_64
python-rpm-macros-3-41.el8.noarch
python-srpm-macros-3-41.el8.noarch python3-pyparsing-
2.1.10-7.el8.noarch
python3-rpm-generators-5-7.el8.noarch
python3-rpm-macros-3-41.el8.noarch python36-devel-
3.6.8-38.module+el8.5.0+12207+5c5719bc.x86_64
qt5-srpm-macros-5.15.2-1.el8.noarch
redhat-lsb-core-4.1-47.el8.x86_64 redhat-lsb-submod-
security-4.1-47.el8.x86_64
redhat-rpm-config-125-1.el8.noarch
rust-srpm-macros-5-2.el8.noarch spax-1.5.3-
13.el8.x86_64
systemtap-sdt-devel-4.6-4.el8.x86_64
time-1.9-3.el8.x86_64 unzip-6.0-
46.el8.x86_64
util-linux-user-2.32.1-28.el8.x86_64
zip-3.0-23.el8.x86_64 zlib-devel-1.2.11-
17.el8.x86_64

```

Complete!

OS package installations finished

+ Installing ONTAP Mediator. (Log: /tmp/ontap\_mediator.JixKGP/ontap-mediator-1.6.0/ontap-mediator-1.6.0/install\_20221021155929.log)

This step will take several minutes. Use the log file to view progress.

Sudoer config verified

ONTAP Mediator rsyslog and logging rotation enabled

+ Install successful. (Moving log to /opt/netapp/lib/ontap\_mediator/log/install\_20221021155929.log)

+ WARNING: This system supports UEFI

Secure Boot (SB) is currently disabled on this system.

If SB is enabled in the future, SCST will not work unless the following action is taken:

Using the keys in

/opt/netapp/lib/ontap\_mediator/ontap\_mediator/SCST\_mod\_keys follow instructions in

/opt/netapp/lib/ontap\_mediator/ontap\_mediator/SCST\_mod\_keys/README.module-signing

to sign the SCST kernel module. Note that reboot will be

needed.

SCST will not start automatically when Secure Boot is enabled and not configured properly.

+ Note: ONTAP Mediator uses a kernel module compiled specifically for the current

OS. Using 'yum update' to upgrade the kernel might cause service interruption.

For more information, see /opt/netapp/lib/ontap\_mediator/README

```
[root@scs000099753 ~]# cat /etc/redhat-release
```

```
Red Hat Enterprise Linux release 8.5 (Ootpa)
```

```
[root@scs000099753 ~]#
```

インストールを確認します。

ONTAP メディエーターをインストールしたら、ONTAP メディエーターサービスが実行されていることを確認する必要があります。

手順

1. ONTAP メディエーターサービスのステータスを表示します。

- a. `systemctl status ontap_mediator`

```
[root@scspr1915530002 ~]# systemctl status ontap_mediator
```

```
ontap_mediator.service - ONTAP Mediator
Loaded: loaded (/etc/systemd/system/ontap_mediator.service; enabled;
vendor preset: disabled)
Active: active (running) since Mon 2022-04-18 10:41:49 EDT; 1 weeks 0
days ago
Process: 286710 ExecStop=/bin/kill -s INT $MAINPID (code=exited,
status=0/SUCCESS)
Main PID: 286712 (uwsgi)
Status: "uWSGI is ready"
Tasks: 3 (limit: 49473)
Memory: 139.2M
CGroup: /system.slice/ontap_mediator.service
├─286712 /opt/netapp/lib/ontap_mediator/pyenv/bin/uwsgi --ini
/opt/netapp/lib/ontap_mediator/uwsgi/ontap_mediator.ini
├─286716 /opt/netapp/lib/ontap_mediator/pyenv/bin/uwsgi --ini
/opt/netapp/lib/ontap_mediator/uwsgi/ontap_mediator.ini
└─286717 /opt/netapp/lib/ontap_mediator/pyenv/bin/uwsgi --ini
/opt/netapp/lib/ontap_mediator/uwsgi/ontap_mediator.ini

[root@scspr1915530002 ~]#
```



b. `systemctl status mediator-scst`

```
[root@scspr1915530002 ~]# systemctl status mediator-scst
Loaded: loaded (/etc/systemd/system/mediator-scst.service;
enabled; vendor preset: disabled)
Active: active (running) since Mon 2022-04-18 10:41:47 EDT; 1
weeks 0 days ago
Process: 286595 ExecStart=/etc/init.d/scst start (code=exited,
status=0/SUCCESS)
Main PID: 286662 (iscsi-scstd)
Tasks: 1 (limit: 49473)
Memory: 1.2M
CGroup: /system.slice/mediator-scst.service
└─286662 /usr/local/sbin/iscsi-scstd

[root@scspr1915530002 ~]#
```

2. ONTAP メディエーターサービスで使用されているポートを確認します。

`netstat`

```
[root@scspr1905507001 ~]# netstat -anlt | grep -E '3260|31784'

tcp        0      0 0.0.0.0:31784      0.0.0.0:*        LISTEN
tcp        0      0 0.0.0.0:3260      0.0.0.0:*        LISTEN
tcp6       0      0 :::3260           :::*             LISTEN
```

## インストール後の設定

ONTAP メディエーターサービスをインストールして実行したら、メディエーターの機能を使用するには、ONTAP ストレージシステムで追加の設定タスクを実行する必要があります。

- MetroCluster IP 構成で ONTAP メディエーターサービスを使用する場合は、を参照してください ["MetroCluster IP 構成での ONTAP メディエーターサービスの設定"](#)。
- SnapMirror のビジネス継続性機能を使用する手順については、を参照して ["ONTAP メディエーターサービスをインストールし、ONTAP クラスタの設定を確認します"](#)。

## ONTAP メディエーターのセキュリティポリシーを設定します

ONTAP メディエーターサーバでは、いくつかの設定可能なセキュリティ設定がサポートされます。すべての設定のデフォルト値は、`low_space_threshold_mib`：10読み取り専用ファイルで提供されます。

/opt/netapp/lib/ontap\_mediator/server\_config/ontap\_mediator.user\_config.yaml

に配置されているすべての値 ontap\_mediator.user\_config.yaml デフォルト値は上書きされ、ONTAP メディエーターのすべてのアップグレードで維持されます。

を変更した後 `ontap\_mediator.user\_config.yaml` ONTAP メディエーターサービスを再起動します。

```
systemctl restart ontap_mediator
```

ONTAP メディエーターの属性を変更します。

次の属性を設定できます。



その他のデフォルト値 ontap\_mediator.config.yaml 変更しないでください。

- デフォルトの自己署名証明書の代わりにサードパーティの**SSL**証明書をインストールするための設定

```
cert_path:
'/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_mediator_server.crt'
key_path:
'/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_mediator_server.key'
ca_cert_path:
'/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ca.crt'
ca_key_path:
'/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ca.key'
ca_serial_path:
'/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ca.srl'
cert_valid_days: '1095' # Used to set the expiration
on client certs to 3 years
x509_passin_pwd: 'pass:ontap' # passphrase for the signed
client cert
```

- ブルートフォースパスワード推測攻撃に対する保護を提供する設定

この機能を有効にするには、の値を設定します window\_seconds および retry\_limit

例

- 5分間の猶予期間を設けて推測し、失敗回数をゼロにリセットします。

```
authentication_lock_window_seconds: 300
```

- 期間内に5つの障害が発生した場合は、アカウントをロックします。

```
authentication_retry_limit: 5
```

- 各試行を拒否する前に発生する遅延を設定することで、ブルートフォースパスワード推測攻撃の影響を軽減し、攻撃の速度を低下させます。

```
authentication_failure_delay_seconds: 5
```

```
authentication_failure_delay_seconds: 0    # seconds (float) to delay
failed auth attempts prior to response, 0 = no delay
authentication_lock_window_seconds: null   # seconds (int) since the
oldest failure before resetting the retry counter, null = no window
authentication_retry_limit: null           # number of retries to
allow before locking API access, null = unlimited
```

- \* ONTAP メディエーターAPIユーザーアカウントのパスワードの複雑さのルールを制御するフィールド\*

```
password_min_length: 8

password_max_length: 64

password_uppercase_chars: 0    # min. uppercase characters
password_lowercase_chars: 1    # min. lowercase character
password_special_chars: 1      # min. non-letter, non-digit
password_nonletter_chars: 2    # min. non-letter characters (digits,
specials, anything)
```

- で必要な空き容量を制御する設定 **/opt/netapp/lib/ontap\_mediator** ディスク。

スペースが設定されたしきい値を下回ると、サービスは警告イベントを問題 します。

```
low_space_threshold_mib: 10
```

- \* RESERVE\_LOG\_SPACEを制御する設定。\*

ONTAPメディエーターサーバのデフォルトのインストールでは、ログ用に独立したディスクスペースが作成されます。Mediatorのロギングに明示的に使用される、合計700MBのディスクスペースを含む新しい固定サイズのファイルがインストーラによって作成されます。

この機能を無効にしてデフォルトのディスク容量を使用するには、次の手順に従います。

- a. 次のファイルでRESERVE\_LOG\_SPACEの値を「1」から「0」に変更します。

```
/opt/netapp/lib/ontap_mediator/tools/mediator_env
```

b. Mediatorを再起動します。

- i. `cat /opt/netapp/lib/ontap_mediator/tools/mediator_env | grep "RESERVE_LOG_SPACE"`

```
RESERVE_LOG_SPACE=0
```

- ii. `systemctl restart ontap_mediator`

この機能を再度有効にするには、値を「0」から「1」に変更してMediatorを再起動します。



ディスクスペースを切り替えても、既存のログは消去されません。以前のログはすべてバックアップされ、Mediatorの切り替えと再起動のあとに現在のディスクスペースに移動されます。

## ONTAP メディエーターサービスを管理します

ONTAP メディエーターサービスをインストールしたあと、必要に応じてユーザ名またはパスワードを変更できます。ONTAPメディエーターサービスをアンインストールすることもできます。

ユーザ名を変更します

これらのタスクについて

これらのタスクは、ONTAP メディエーターサービスがインストールされた Linux ホストで実行します。

このコマンドを実行できない場合は、次の例のように完全パスを使用してコマンドを実行する必要があります。

```
/usr/local/bin/mediator_username
```

手順

次のいずれかを実行してユーザ名を変更します。

- 次の例に示すように、コマンド `mediator_change_user` を実行してプロンプトに応答します。

```
[root@mediator-host ~]# mediator_change_user
Modify the Mediator API username by entering the following values:
  Mediator API User Name: mediatoradmin
                        Password:
New Mediator API User Name: mediator
The account username has been modified successfully.
[root@mediator-host ~]#
```

- 次のコマンドを実行します。

```
MEDIATOR_USERNAME=mediator MEDIATOR_PASSWORD=mediator2
MEDIATOR_NEW_USERNAME=mediatoradmin mediator_change_user
```

```
[root@mediator-host ~]# MEDIATOR_USERNAME= mediator
MEDIATOR_PASSWORD='mediator2' MEDIATOR_NEW_USERNAME= mediatoradmin
mediator_change_user
The account username has been modified successfully.
[root@mediator-host ~]#
```

## パスワードを変更します

このタスクについて

このタスクは、ONTAP メディエーターサービスがインストールされた Linux ホストで実行します。

このコマンドを実行できない場合は、次の例のように完全パスを使用してコマンドを実行する必要があります。

```
/usr/local/bin/mediator_change_password
```

手順

次のいずれかを実行してパスワードを変更します。

- を実行します mediator\_change\_password コマンドを実行し、次の例に示すようにプロンプトに応答します。

```
[root@mediator-host ~]# mediator_change_password
Change the Mediator API password by entering the following values:
  Mediator API User Name: mediatoradmin
    Old Password:
    New Password:
    Confirm Password:
The password has been updated successfully.
[root@mediator-host ~]#
```

- 次のコマンドを実行します。

```
MEDIATOR_USERNAME= mediatoradmin MEDIATOR_PASSWORD=mediator1
MEDIATOR_NEW_PASSWORD=mediator2 mediator_change_password
```

この例では、パスワードが「mediator1」から「mediator2」に変更されています。

```
[root@mediator-host ~]# MEDIATOR_USERNAME=mediatoradmin  
MEDIATOR_PASSWORD=mediator1 MEDIATOR_NEW_PASSWORD=mediator2  
mediator_change_password  
The password has been updated successfully.  
[root@mediator-host ~]#
```

## ONTAP メディエーターサービスを停止します

ONTAP メディエーターサービスを停止するには、次の手順を実行します。

### 手順

1. ONTAP メディエーターを停止します。

```
systemctl stop ontap_mediator
```

2. SCSTを停止します。

```
systemctl stop mediator-scst
```

3. ONTAP メディエーターとSCSTを無効にします。

```
systemctl disable ontap_mediator mediator-scst
```

## ONTAP メディエーターサービスを再度有効にします

ONTAP メディエーターサービスを再度有効にするには、次の手順を実行します。

### 手順

1. ONTAP メディエーターとSCSTを有効にします。

```
systemctl enable ontap_mediator mediator-scst
```

2. SCSTを起動します。

```
systemctl start mediator-scst
```

3. ONTAP Mediatorを起動します。

```
systemctl start ontap_mediator
```

## ONTAP メディエーターが正常であることを確認します

ONTAP メディエーターをインストールしたら、ONTAP メディエーターサービスが実行されていることを確認する必要があります。

### 手順

1. ONTAP メディエーターサービスのステータスを表示します。

a. `systemctl status ontap_mediator`

```
[root@scspr1915530002 ~]# systemctl status ontap_mediator

ontap_mediator.service - ONTAP Mediator
Loaded: loaded (/etc/systemd/system/ontap_mediator.service; enabled;
vendor preset: disabled)
Active: active (running) since Mon 2022-04-18 10:41:49 EDT; 1 weeks 0
days ago
Process: 286710 ExecStop=/bin/kill -s INT $MAINPID (code=exited,
status=0/SUCCESS)
Main PID: 286712 (uwsgi)
Status: "uWSGI is ready"
Tasks: 3 (limit: 49473)
Memory: 139.2M
CGroup: /system.slice/ontap_mediator.service
├─286712 /opt/netapp/lib/ontap_mediator/pyenv/bin/uwsgi --ini
/opt/netapp/lib/ontap_mediator/uwsgi/ontap_mediator.ini
├─286716 /opt/netapp/lib/ontap_mediator/pyenv/bin/uwsgi --ini
/opt/netapp/lib/ontap_mediator/uwsgi/ontap_mediator.ini
└─286717 /opt/netapp/lib/ontap_mediator/pyenv/bin/uwsgi --ini
/opt/netapp/lib/ontap_mediator/uwsgi/ontap_mediator.ini

[root@scspr1915530002 ~]#
```

b. `systemctl status mediator-scst`

```
[root@scspr1915530002 ~]# systemctl status mediator-scst

Loaded: loaded (/etc/systemd/system/mediator-scst.service;
enabled; vendor preset: disabled)
Active: active (running) since Mon 2022-04-18 10:41:47 EDT; 1
weeks 0 days ago
Process: 286595 ExecStart=/etc/init.d/scst start (code=exited,
status=0/SUCCESS)
Main PID: 286662 (iscsi-scstd)
Tasks: 1 (limit: 49473)
Memory: 1.2M
CGroup: /system.slice/mediator-scst.service
└─286662 /usr/local/sbin/iscsi-scstd

[root@scspr1915530002 ~]#
```

2. ONTAP メディエーターサービスで使用されているポートを確認します。

netstat

```
[root@scspr1905507001 ~]# netstat -anlt | grep -E '3260|31784'
```

```
tcp    0    0 0.0.0.0:31784    0.0.0.0:*        LISTEN
tcp    0    0 0.0.0.0:3260    0.0.0.0:*        LISTEN
tcp6   0    0 :::3260         :::*             LISTEN
```

ホストのメンテナンスを実行するには、**SCST**を手動でアンインストールします

SCSTをアンインストールするには、インストールされているONTAP メディエーターのバージョンに使用するSCST tarバンドルが必要です。

#### 手順

1. 次の表に示すように、適切なSCSTバンドルをダウンロードして解凍します。

バージョン	使用するtarバンドル
ONTAPメディエーター1.7	scst-3.7.0.tar.bz2
ONTAPメディエーター1.6	scst-3.7.0.tar.bz2
ONTAPメディエーター1.5	scst-3.6.0.tar.bz2
ONTAPメディエーター1.4	scst-3.6.0.tar.bz2
ONTAP Mediator 1.3.	scst-3.5.0.tar.bz2
ONTAP メディエーター1.1	scst-3.4.0.tar.bz2
ONTAP Mediator 1.0の略	scst-3.3.0.tar.bz2

2. 「scst」ディレクトリにある次のコマンドを問題 します。

- a. `systemctl stop mediator-scst`
- b. `make scstadm_uninstall`
- c. `make iscsi_uninstall`
- d. `make usr_uninstall`
- e. `make scst_uninstall`
- f. `depmod`



ホストのメンテナンスを実行するには、**SCST**を手動でインストールしてください

SCSTを手動でインストールするには、インストールされているONTAP メディエーターのバージョンに使用するSCST tarバンドルが必要です（を参照 [上の表](#)）。

1. 「scst」ディレクトリにある次のコマンドを実行します。

- a. `make 2release`
- b. `make scst_install`
- c. `make usr_install`
- d. `make iscsi_install`
- e. `make scstadm_install`
- f. `depmod`
- g. `cp scst/src/certs/scst_module_key.der /opt/netapp/lib/ontap_mediator/ontap_mediator/SCST_mod_keys/.`
- h. `cp scst/src/certs/scst_module_key.der /opt/netapp/lib/ontap_mediator/ontap_mediator/SCST_mod_keys/.`
- i. `patch /etc/init.d/scst < /opt/netapp/lib/ontap_mediator/systemd/scst.patch`

2. (オプション) セキュアブートが有効になっている場合は、リブートする前に、次の手順を実行します。

a. 「scst\_vdisk」、 「scst」、 および 「iscsi\_scst」 モジュールの各ファイル名を確認します。

```
[root@localhost ~]# modinfo -n scst_vdisk
[root@localhost ~]# modinfo -n scst
[root@localhost ~]# modinfo -n iscsi_scst
```

b. カーネルのリリースを確認します。

```
[root@localhost ~]# uname -r
```

c. 各ファイルにカーネルで署名します。

```
[root@localhost ~]# /usr/src/kernels/<KERNEL-RELEASE>/scripts/sign-file \
sha256 \
/opt/netapp/lib/ontap_mediator/ontap_mediator/SCST_mod_keys/scst_module_key.priv \
/opt/netapp/lib/ontap_mediator/ontap_mediator/SCST_mod_keys/scst_module_key.der \
_module-filename_
```

d. UEFIファームウェアで正しいキーをインストールします。

UEFIキーのインストール手順は、次の場所にあります。

```
/opt/netapp/lib/ontap_mediator/ontap_mediator/SCST_mod_keys/README.module-  
signing
```

生成されたUEFIキーは次の場所にあります。

```
/opt/netapp/lib/ontap_mediator/ontap_mediator/SCST_mod_keys/scst_module_key.de  
r
```

### 3. リブートを実行します。

```
reboot
```

## ONTAP メディエーターサービスをアンインストールします

作業を開始する前に

必要に応じて、ONTAP メディエーターサービスを削除できます。メディエーターサービスを削除するには、事前にメディエーターを ONTAP から切断する必要があります。

このタスクについて

このタスクは、ONTAP メディエーターサービスがインストールされた Linux ホストで実行します。

このコマンドを実行できない場合は、次の例のように完全パスを使用してコマンドを実行する必要があります。

```
/usr/local/bin/uninstall_ontap_mediator
```

### ステップ

#### 1. ONTAP メディエーターサービスをアンインストールします

```
uninstall_ontap_mediator
```

```
[root@mediator-host ~]# uninstall_ontap_mediator  
  
ONTAP Mediator: Self Extracting Uninstaller  
  
+ Removing ONTAP Mediator. (Log:  
/tmp/ontap_mediator.GmRGdA/uninstall_ontap_mediator/remove.log)  
+ Remove successful.  
[root@mediator-host ~]#
```

## 一時的な自己署名証明書の再生成

このタスクについて

- このタスクは、ONTAPメディエーターサービスがインストールされているLinuxホストで実行します。
- このタスクは、ONTAPメディエーターのインストール後にホストのホスト名またはIPアドレスが変更され

たために、生成された自己署名証明書が廃止された場合にのみ実行できます。

- 一時的な自己署名証明書を信頼できるサードパーティ証明書に置き換えたあと、このタスクを使用して証明書を再生成します。自己署名証明書がないと、原因この手順は失敗します。

## ステップ

現在のホストの新しい一時的な自己署名証明書を再生成するには、次の手順を実行します。

1. ONTAPメディエーターを再起動します。

```
./make_self_signed_certs.sh overwrite
```

```
[root@xyz000123456 ~]# cd
/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config
[root@xyz000123456 server_config]# ./make_self_signed_certs.sh overwrite

Adding Subject Alternative Names to the self-signed server certificate
#
# OpenSSL example configuration file.
Generating self-signed certificates
Generating RSA private key, 4096 bit long modulus (2 primes)
.....
.....
.....++++
.....++++
e is 65537 (0x010001)
Generating a RSA private key
.....++++
.....
.....+++
+
writing new private key to 'ontap_mediator_server.key'
-----
Signature ok
subject=C = US, ST = California, L = San Jose, O = "NetApp, Inc.", OU =
ONTAP Core Software, CN = ONTAP Mediator, emailAddress =
support@netapp.com
Getting CA Private Key
```

## ONTAP メディエーター用のOSホストを維持します

最適なパフォーマンスを得るには、ONTAP メディエーター用のホストOSを定期的に保守する必要があります。

ホストをリブートします

クラスタが正常な状態になったらホストをリブートします。ONTAP メディエーターがオフラインの間は、クラスタが障害に適切に対応できなくなるリスクがあります。再起動が必要な場合は、サービスウィンドウを使用することをお勧めします。

ONTAP メディエーターはリブート中に自動的に再開され、ONTAP クラスタで以前に設定した関係が再入力されます。

## ホストパッケージの更新

ライブラリやyumパッケージ（カーネルを除く）は安全に更新できますが、有効にするには再起動が必要になる場合があります。再起動が必要な場合は、サービスウィンドウを使用することをお勧めします。

をインストールした場合 yum-utils パッケージでは、を使用します needs-restarting パッケージの変更によりリブートが必要かどうかを検出するコマンド。

実行中のプロセスにはすぐには反映されないため、ONTAP メディエーターの依存関係が更新された場合はリブートする必要があります。

## ホストOSのマイナーカーネルアップグレード

SCSTは、使用しているカーネル用にコンパイルされている必要があります。OSを更新するには、メンテナンス時間が必要です。

### 手順

ホストOSカーネルをアップグレードするには、次の手順を実行します。

1. ONTAP メディエーターを停止します
2. SCSTパッケージをアンインストールします。（SCSTにはアップグレードメカニズムはありません）。
3. OSをアップグレードし、再起動します。
4. SCSTパッケージを再インストールします。
5. ONTAP メディエーターサービスを再度有効にします。

## ホストがホスト名またはIPに変更

### このタスクについて

- このタスクは、ONTAPメディエーターサービスがインストールされているLinuxホストで実行します。
- このタスクは、ONTAPメディエーターのインストール後にホストのホスト名またはIPアドレスが変更されたために、生成された自己署名証明書が廃止された場合にのみ実行できます。
- 一時的な自己署名証明書を信頼できるサードパーティ証明書に置き換えたあと、このタスクを使用して証明書を再生成します。自己署名証明書がないと、原因この手順は失敗します。

### ステップ

現在のホストの新しい一時的な自己署名証明書を再生成するには、次の手順を実行します。

1. ONTAPメディエーターを再起動します。

```
./make_self_signed_certs.sh overwrite
```

```
[root@xyz000123456 ~]# cd
/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config
[root@xyz000123456 server_config]# ./make_self_signed_certs.sh overwrite

Adding Subject Alternative Names to the self-signed server certificate
#
# OpenSSL example configuration file.
Generating self-signed certificates
Generating RSA private key, 4096 bit long modulus (2 primes)
.....
.....
.....++++
.....++++
e is 65537 (0x010001)
Generating a RSA private key
.....++++
.....
.....++++
+
writing new private key to 'ontap_mediator_server.key'
-----
Signature ok
subject=C = US, ST = California, L = San Jose, O = "NetApp, Inc.", OU =
ONTAP Core Software, CN = ONTAP Mediator, emailAddress =
support@netapp.com
Getting CA Private Key

[root@xyz000123456 server_config]# systemctl restart ontap_mediator
```

## System Manager を使用して MetroCluster サイトを管理する

### System Manager を使用した MetroCluster サイトの管理の概要

ONTAP 9.8 以降では、MetroCluster セットアップを管理するためのシンプルなインターフェイスとして System Manager を使用できます。

MetroCluster 構成では、2 つのクラスタ間でデータを相互にミラーリングできるため、一方のクラスタが停止してもデータは失われません。

通常、組織は 2 つの異なる地域にクラスタをセットアップします。各ロケーションの管理者がクラスタを設定し、設定します。次に、一方の管理者が、データを共有できるように、クラスタ間にピア関係を設定します。

組織は、ONTAP メディエーターを 3 番目の場所にインストールすることもできます。ONTAP メディエーターサービスは、各クラスタのステータスを監視します。一方のクラスタがパートナークラスタと通信できないことを検出すると、エラーがクラスタシステムまたはネットワーク接続に問題があるかどうかを監視対象に照会します。

ネットワーク接続に問題がある場合は、システム管理者がトラブルシューティング方法を実行してエラーを修正し、再接続します。パートナークラスタが停止すると、もう一方のクラスタがスイッチオーバープロセスを開始して両方のクラスタのデータ I/O を制御します。

また、スイッチオーバーを実行して、計画的メンテナンスのために一方のクラスタシステムを停止することもできます。メンテナンスを実行してスイッチバック処理を実行するクラスタを起動するまで、両方のクラスタのすべてのデータ I/O 処理がパートナークラスタによって処理されます。

管理できる処理は次のとおりです。

- ["IP MetroCluster サイトをセットアップする"](#)
- ["IP MetroCluster ピアリングをセットアップする"](#)
- ["IP MetroCluster サイトを設定します"](#)
- ["IP MetroCluster のスイッチオーバーとスイッチバックを実行"](#)
- ["IP MetroCluster 設定に関する問題のトラブルシューティングを行う"](#)
- ["MetroCluster クラスタの ONTAP をアップグレードします"](#)

## IP MetroCluster サイトをセットアップする

ONTAP 9.8 以降では、System Manager を使用して MetroCluster サイトの IP 設定を行うことができます。

MetroCluster サイトは 2 つのクラスタで構成されます。通常、クラスタは地理的に離れた場所に配置されます。

を開始する前に

- に従って、システムの設置とケーブル接続が完了している必要があります ["インストールおよびセットアップガイド"](#) システムに同梱されていたものです。
- クラスタ内通信用に、各クラスタの各ノードにクラスタネットワークインターフェイスを設定する必要があります。

ノード管理 IP アドレスを割り当て

### Windows システム

Windows コンピュータは、コントローラと同じサブネットに接続する必要があります。これにより、システムにノード管理 IP アドレスが自動的に割り当てられます。

手順

1. Windows システムで、\* Network \* ドライブを開いてノードを検出します。
2. ノードをダブルクリックしてクラスタセットアップウィザードを起動します。

## その他のシステム

クラスタ内のいずれかのノードにノード管理 IP アドレスを設定する必要があります。このノード管理 IP アドレスを使用して、クラスタセットアップウィザードを起動できます。

を参照してください ["第 1 ノードへのクラスタの作成"](#) ノード管理 IP アドレスの割り当てについては、を参照してください。

## クラスタを初期化して設定

クラスタを初期化するには、クラスタの管理パスワードを設定し、クラスタ管理ネットワークとノード管理ネットワークをセットアップします。DNS サーバなどのサービスを設定してホスト名を解決したり、NTP サーバを設定して時間を同期したりすることもできます。

### 手順

1. Web ブラウザで、設定したノード管理 IP アドレスを入力します。 "<a href="https://node-management-IP" class="bare">https://node-management-IP"</a>

System Manager は、クラスタ内の残りのノードを自動的に検出します。

2. Initialize Storage System\*（ストレージシステムの初期化）ウィンドウで、次の手順を実行します。
  - a. クラスタ管理ネットワーク設定データを入力します。
  - b. すべてのノードのノード管理 IP アドレスを入力してください。
  - c. ドメインネームサーバ（DNS）の詳細を指定します。
  - d. [\* その他 \*（\* Other \*）] セクションで、[ タイムサービス（NTP）を使用（Use time service（NTP）\* ] というラベルの付いたチェックボックスを選択してタイムサーバを追加します。

Submit \* をクリックすると、クラスタが作成および構成されるまで待機します。その後、検証プロセスが実行されます。

### 次の手順

両方のクラスタのセットアップ、初期化、設定が完了したら、次の手順を実行します。

- ["IP MetroCluster ピアリングをセットアップする"](#)

新しいクラスタのビデオで **ONTAP** を設定



## IP MetroCluster ピアリングをセットアップする

ONTAP 9.8 以降では、MetroCluster 処理の IP 設定を System Manager で管理できます。2 つのクラスタをセットアップしたら、それらのクラスタ間にピア関係を設定します。

を開始する前に

2 つのクラスタをセットアップするために、次の手順を完了しておく必要があります。

- ["IP MetroCluster サイトをセットアップする"](#)

このプロセスの特定の手順は、各クラスタの地理的サイトにある異なるシステム管理者によって実行されます。このプロセスを説明するために、クラスタの名前は「サイト A クラスタ」および「サイト B クラスタ」です。

サイト **A** からピアリングプロセスを実行しています

このプロセスは、サイト A のシステム管理者が実行します

手順

1. サイト A のクラスタにログインします。
2. System Manager で、左側のナビゲーション列から「\* Dashboard \*」を選択してクラスタの概要を表示します。

ダッシュボードには、このクラスタ（サイト A）の詳細が表示されます。「\* MetroCluster \*」セクションの左側には、サイト A のクラスタが表示されています。

3. [Attach Partner Cluster] をクリックします。



4. サイト A のクラスタ内のノードがサイト B のクラスタ内のノードと通信できるようにするネットワークインターフェイスの詳細を入力します。
5. [保存して続行] をクリックします。
6. [\* パートナークラスタの接続\*] ウィンドウで、[パスフレーズがありません\*] を選択してパスフレーズを生成します。
7. 生成されたパスフレーズをコピーし、サイト B のシステム管理者と共有します
8. [閉じる (Close)] を選択します。

サイト B からピアリングプロセスを実行しています

このプロセスは、サイト B のシステム管理者が実行します

手順

1. サイト B のクラスタにログインします。
2. System Manager で、\* Dashboard \* を選択してクラスタの概要を表示します。

ダッシュボードには、このクラスタ（サイト B）の詳細が表示されます。MetroCluster セクションでは、左側にサイト B のクラスタが表示されます。

3. [Attach Partner Cluster] をクリックしてピアリングプロセスを開始します。
4. サイト B のクラスタ内のノードがサイト A のクラスタ内のノードと通信できるようにするネットワークインターフェイスの詳細を入力します。
5. [保存して続行] をクリックします。
6. [\* パートナークラスタの接続\*（\* Attach Partner Cluster\*）] ウィンドウで、[パスフレーズ\* があります（\* I have a passphrase\*）] を選択します。これにより、サイト A のシステム管理者から受け取ったパスフレーズを入力できます
7. ピア\* を選択してピアリングプロセスを完了します。

次の手順

ピアリングプロセスが完了したら、クラスタを設定します。を参照してください ["IP MetroCluster サイトを設定します"](#)。

## IP MetroCluster サイトを設定します

ONTAP 9.8 以降では、MetroCluster 処理の IP 設定を System Manager で管理できます。2 つのクラスタをセットアップしてピアリングしたら、各クラスタを構成します。

を開始する前に

次の作業を完了しておきます。

- ["IP MetroCluster サイトをセットアップする"](#)
- ["IP MetroCluster ピアリングをセットアップする"](#)

## クラスタ間の接続を設定します

### 手順

1. いずれかのサイトで System Manager にログインし、\* Dashboard \* を選択します。

「\* MetroCluster \*」セクションの図は、MetroCluster サイト用にセットアップしてピアリングした 2 つのクラスタを示しています。作業中のクラスタ（ローカルクラスタ）が左側に表示されます。

2. MetroCluster の設定 \* をクリックします。このウィンドウでは、次のタスクを実行できます。
  - a. MetroCluster 構成の各クラスタのノードが表示されます。ドロップダウンリストを使用して、ローカルクラスタのどのノードをディザスタリカバリパートナーとするかを選択し、リモートクラスタのどのノードを使用するかを決定します。
  - b. ONTAP メディエーターサービスを設定する場合は、チェックボックスをクリックします。を参照してください [ONTAP メディエーターサービスを設定します](#)。
  - c. 両方のクラスタに暗号化を有効にするライセンスがある場合は、\* Encryption \* セクションが表示されます。

暗号化を有効にするには、パスフレーズを入力します。

- d. 共有レイヤ 3 ネットワークで MetroCluster を設定する場合は、このチェックボックスをオンにします。



ノードに接続する HA パートナーノードとネットワークスイッチで、同じ構成を使用する必要があります。

3. 保存 \* をクリックして、MetroCluster サイトを設定します。

ダッシュボード \* の \* MetroCluster \* セクションでは、2 つのクラスタ間のリンクにチェックマークが表示され、正常な接続を示しています。

## ONTAP メディエーターサービスを設定します

ONTAP メディエーターサービスは、通常、クラスタのどちらかの場所とは別の地理的な場所にインストールします。クラスタがサービスと定期的に通信して、稼働中であることを示します。MetroCluster 構成のどちらかのクラスタで、パートナークラスタとの通信が停止していることが検出されると、ONTAP メディエーターがチェックされてパートナークラスタ自体が停止しているかどうか判断されます。

### を開始する前に

MetroCluster サイトの両方のクラスタが起動し、ピア関係にある必要があります。

### 手順

1. ONTAP 9.8 の System Manager で、\* Cluster > Settings \* を選択します。
2. [\* Mediator\*] セクションで、をクリックします .
3. Configure Mediator\*（メディエーターの設定）ウィンドウで、\* Add+\*（追加 +）をクリックします。
4. ONTAP メディエーターの設定の詳細を入力します。

System ManagerでONTAPメディエーターを設定する際には、次の情報を入力できます。

- メディエーターのIPアドレス。
- ユーザ名。
- パスワード。

## System Managerを使用したメディエーターの管理




System Managerを使用して、メディエーターを管理するタスクを実行できます。

これらのタスクについて

ONTAP 9.8以降では、System ManagerをMetroClusterセットアップの4ノードIP構成（3番目の場所にインストールされたONTAPメディエーターを含む）を管理するためのシンプルなインターフェイスとして使用できます。

ONTAP 9.14.1以降では、System Managerを使用して、MetroClusterサイトの8ノードIP構成に対してもこれらの処理を実行できます。System Managerでは8ノードシステムをセットアップまたは拡張することはできませんが、8ノードIP MetroClusterシステムがすでにセットアップされている場合はこれらの処理を実行できます。

Mediatorを管理するには、次のタスクを実行します。

このタスクを実行します。	対処方法
Mediatorサービスの設定	<p>の手順を実行します <a href="#">"ONTAP メディエーターサービスを設定します"</a>。</p>
Mediator-Assisted Automatic Switchover（MAUSO；メディエーターアシスト自動スイッチオーバー）の有効化または無効化	<ol style="list-style-type: none"> <li>1. System Manager で、 * ダッシュボード * をクリックします。</li> <li>2. MetroClusterセクションまでスクロールします。</li> <li>3. をクリックします  をクリックしますMetroCluster。</li> <li>4. または[無効化]*を選択します。</li> <li>5. 管理者のユーザ名とパスワードを入力し、【有効化】*または[無効化]*をクリックします。</li> </ol> <div>  <p>Mediatorが到達可能で、両方のサイトが「通常」モードになっていれば、Mediatorを有効または無効にできます。MetroClusterシステムが正常な状態であれば、MAUSOが有効または無効になっていてもメディエーターにアクセスできます。</p> </div>
MetroCluster構成からメディエーターを削除する	<ol style="list-style-type: none"> <li>1. System Manager で、 * ダッシュボード * をクリックします。</li> <li>2. MetroClusterセクションまでスクロールします。</li> <li>3. をクリックします  をクリックしますMetroCluster。</li> <li>4. [メディエーターの削除]*を選択します。</li> <li>5. 管理者のユーザ名とパスワードを入力し、*[削除]*をクリックします。</li> </ol>

Mediatorの健全性を確認する	の手順を実行します "IP MetroCluster 設定に関する問題のトラブルシューティングを行う"。
スイッチオーバーとスイッチバックの実行	の手順を実行します "IP MetroCluster のスイッチオーバーとスイッチバックを実行"。

## IP MetroCluster のスイッチオーバーとスイッチバックを実行

1 つの IP MetroCluster サイトからもう一方のサイトに制御を切り替えることで、問題のメンテナンスやリカバリを実施できます。



スイッチオーバーとスイッチバックの手順は、IP MetroCluster 構成でのみサポートされます。

### スイッチオーバーとスイッチバックの概要

スイッチオーバーは次の 2 つのケースで発生します。

#### • \* 計画的スイッチオーバー \*

このスイッチオーバーは、System Manager を使用してシステム管理者が開始します。計画的スイッチオーバーでは、ローカルクラスタのシステム管理者が制御を切り替えて、リモートクラスタのデータサービスをローカルクラスタで処理できるようにします。その後、リモートクラスタのシステム管理者が、リモートクラスタのメンテナンスを実行できます。

#### • \* 計画外スイッチオーバー \*

場合によっては、MetroCluster クラスタが停止したり、クラスタ間の接続が停止したりすると、実行中のクラスタがダウンしたクラスタのデータ処理を処理するように、ONTAP によってスイッチオーバー手順が自動的に開始されます。

一方のクラスタのステータスを ONTAP が特定できない場合は、動作しているサイトのシステム管理者がスイッチオーバー手順を開始し、もう一方のサイトのデータ処理責任を引き継ぎます。

どのタイプのスイッチオーバー手順の場合も、\_switchback プロセスを使用してデータサービス機能がクラスタに返されます。

ONTAP 9.7 および 9.8 では、異なるスイッチオーバープロセスとスイッチバックプロセスを実行します。

- [ONTAP 9.7 の System Manager を使用して、スイッチオーバーとスイッチバックを行います](#)
- [ONTAP 9.8 の System Manager を使用して、スイッチオーバーとスイッチバックを実行します](#)

### ONTAP 9.7 の System Manager を使用して、スイッチオーバーとスイッチバックを行います

#### 手順

1. ONTAP 9.7 で System Manager にログインします。
2. [\[クラシックバージョンに戻る\]](#) をクリックします。
3. [\[\\* Configuration\] > \[\\* MetroCluster \\*\]](#) をクリックします。


System Manager はネゴシエートスイッチオーバーが可能かどうかを検証します。

4. 検証プロセスが完了したら、次のいずれかの手順を実行します。
  - a. 検証が失敗し、サイト B が稼働している場合は、エラーが発生しています。たとえば、サブシステムに問題がある場合や、NVRAM ミラーリングが同期されていない場合があります。
    - i. エラーの原因となっている問題を修正し、[\* 閉じる \*] をクリックして、手順 2 からもう一度開始します。
    - ii. サイト B のノードを停止し、\* 閉じる \* をクリックして、の手順を実行します **"計画外スイッチオーバーの実行"**。
  - b. 検証が失敗し、サイト B が停止している場合は、接続に問題がある可能性が高くなります。サイト B が本当に停止していることを確認し、の手順を実行します **"計画外スイッチオーバーの実行"**。
5. [サイト B からサイト A\* へのスイッチオーバー] をクリックして、スイッチオーバープロセスを開始します。
6. [\* 新しい体験に切り替える \*] をクリックします。

## ONTAP 9.8 の System Manager を使用して、スイッチオーバーとスイッチバックを実行します

### 計画的スイッチオーバーを実行（ONTAP 9.8）

#### 手順

1. ONTAP 9.8でSystem Managerにログインします。
2. 「\* ダッシュボード \*」を選択します。「\* MetroCluster \*」セクションには、2つのクラスタが接続されています。
3. ローカルクラスタ（左側）で、をクリックします  をクリックし、\*リモートデータサービスをローカルサイトにスイッチオーバー\*を選択します。

スイッチオーバー要求の検証が完了すると、リモートサイトからローカルサイトに制御が転送され、両方のクラスタに対してデータサービス要求が実行されます。

リモートクラスタはリブートしますが、ストレージコンポーネントはアクティブではないため、クラスタはデータ要求を処理しません。これで、計画的なメンテナンスが可能になりました。



スイッチバックを実行するまでは、リモートクラスタをデータサービスに使用しないでください。


### 計画外スイッチオーバーの実行（ONTAP 9.8）

計画外スイッチオーバーは、ONTAP によって自動的に開始される場合があります。スイッチバックが必要かどうかを ONTAP が判断できない場合は、実行中の MetroCluster サイトのシステム管理者が次の手順でスイッチオーバーを開始します。

#### 手順

1. ONTAP 9.8でSystem Managerにログインします。
2. 「\* ダッシュボード \*」を選択します。

「\* MetroCluster \*」セクションでは、2つのクラスタ間の接続に「X」が表示され、接続を検出できません。接続またはクラスタが停止しています。

- ローカルクラスタ（左側）で、をクリックします  をクリックし、\*リモートデータサービスをローカルサイトにスイッチオーバー\*を選択します。

スイッチオーバーがエラーで失敗した場合は、エラーメッセージの「View details」リンクをクリックして、計画外スイッチオーバーを確認します。

スイッチオーバー要求の検証が完了すると、リモートサイトからローカルサイトに制御が転送され、両方のクラスタに対してデータサービス要求が実行されます。

クラスタをオンラインに戻す前に、クラスタを修復する必要があります。



リモートクラスタを再びオンラインにしたあとは、スイッチバックを実行するまでデータサービスに使用しないでください。

#### スイッチバックの実行（ONTAP 9.8）

を開始する前に

リモートクラスタが計画的なメンテナンスのために停止したか災害が原因で停止したかに関係なく、稼働中でスイッチバック待ちになっている必要があります。

手順

- ローカルクラスタで、ONTAP 9.8 から System Manager にログインします。
- 「\* ダッシュボード \*」を選択します。

「\* MetroCluster \*」セクションには、2 つのクラスタが表示されます。

- ローカルクラスタ（左側）で、をクリックします  をクリックし、\* Take back control\* を選択します。

データは、両方のクラスタ間でデータが同期およびミラーリングされるように、最初に \_ 修復 \_ されます。

- データの修復が完了したら、をクリックします  をクリックし、\* Initiate switchback \* を選択します。

スイッチバックが完了すると、両方のクラスタがアクティブになり、データ要求を処理します。また、データをミラーリングしてクラスタ間で同期しています。

## MetroCluster IP のアドレス、ネットマスク、およびゲートウェイを変更します

ONTAP 9.10.1 以降では、MetroCluster インターフェイスの IP アドレス、マスク、およびゲートウェイのプロパティを変更できます。パラメータは任意に組み合わせて更新できます。

これらのプロパティを更新する必要がある場合があります。たとえば、IP アドレスが重複して検出された場合や、ルータの設定変更によってレイヤ 3 ネットワークでゲートウェイを変更する必要がある場合などです。一度に変更できるインターフェイスは 1 つだけです。他のインターフェイスが更新されて接続が再確立されるまで、そのインターフェイス上のトラフィックは中断されます。



各ポートで変更を行う必要があります。同様に、ネットワークスイッチも構成を更新する必要があります。たとえば、ゲートウェイが更新されている場合は、HA ペアの両方のノードが同じであるため変更することを推奨します。さらに、それらのノードに接続されたスイッチでも、ゲートウェイを更新する必要があります。

## ステップ

各ノードおよびインターフェイスの IP アドレス、ネットマスク、およびゲートウェイを更新します。

## IP MetroCluster 設定に関する問題のトラブルシューティングを行う

ONTAP 9.8 以降では、System Manager によって IP MetroCluster 構成の健全性が監視されるため、発生する可能性のある問題を特定して修正できます。

### MetroCluster ヘルスチェックの概要

System Manager は、IP MetroCluster 構成の健全性を定期的にチェックします。ダッシュボードで MetroCluster セクションを表示すると、通常は「MetroCluster systems are healthy」というメッセージが表示されます。

ただし、問題が発生すると、メッセージにイベント数が表示されます。そのメッセージをクリックすると、次のコンポーネントの健全性チェックの結果を確認できます。

- ノード
- Network Interface の略
- ティア（ストレージ）
- クラスタ
- 接続
- ボリューム
- Configuration Replication（設定レプリケーション）

[ステータス\*] 列は問題のあるコンポーネントを示し、[詳細\*] 列は問題の解決方法を示します。

### MetroCluster のトラブルシューティング

#### 手順

1. System Manager で、\* Dashboard \* を選択します。
2. 「\* MetroCluster \*」セクションで、メッセージを確認します。
  - a. MetroCluster 構成が正常であることを示すメッセージが表示され、クラスタと ONTAP メディエーターの間の接続が正常である（チェックマーク付きで表示）場合は、修正する問題はありません。
  - b. メッセージにイベント数がリストされている場合、または接続がダウンした（「X」で表示）場合は、次の手順に進みます。
3. イベント数を示すメッセージをクリックします。

MetroCluster 正常性レポートが表示されます。



4. レポートに表示される問題のトラブルシューティングを、 **Details** 列の推奨事項を使用して行います。
5. すべての問題を修正したら、 **\* MetroCluster の正常性を確認 \*** をクリックします。



MetroCluster ヘルスチェックでは大量のリソースが使用されるため、チェックを実行する前にすべてのトラブルシューティングタスクを実行することをお勧めします。

MetroCluster の健全性チェックがバックグラウンドで実行されます。他のタスクは、終了するまで待つことができます。

## テープバックアップによるデータ保護

### FlexVol ボリュームのテープバックアップの概要

ONTAP は、Network Data Management Protocol (NDMP ; ネットワークデータ管理プロトコル) を使用したテープバックアップおよびリストアをサポートしています。NDMP を使用すると、ストレージシステム内のデータを直接テープにバックアップできるため、ネットワーク帯域幅を効率的に使用できます。ONTAP では、テープバックアップ用のダンプエンジンと SMTape エンジンの両方がサポートされます。

NDMP 準拠のバックアップアプリケーションを使用して、ダンプまたは SMTape バックアップ / リストアを実行できます。NDMP バージョン 4 のみがサポートされます。

#### ダンプによるテープバックアップ

ダンプとは、Snapshot コピーベースのバックアップで、ファイルシステムのデータをテープにバックアップします。ONTAP ダンプエンジンは、ファイル、ディレクトリ、および該当する Access Control List (ACL ; アクセス制御リスト) 情報をテープにバックアップします。バックアップ対象には、ボリューム全体、qtree 全体、またはボリューム全体でも qtree 全体でもないサブツリーを指定できます。ダンプでサポートされるのは、ベースラインバックアップ、差分バックアップ、および増分バックアップです。

#### SMTape によるテープバックアップ

SMTape は、ONTAP の Snapshot コピーベースのディザスタリカバリ解決策であり、データのブロックをテープにバックアップします。SMTape を使用すると、テープへのボリュームのバックアップを実行できます。ただし、バックアップを qtree レベルまたはサブツリーレベルで実行することはできません。SMTape でサポートされるのは、ベースラインバックアップ、差分バックアップ、および増分バックアップです。

ONTAP 9.13.1以降では、SMTapeを使用したテープバックアップがサポートされます [SnapMirror によるビジネス継続性](#)。

#### テープバックアップおよびリストアのワークフロー

NDMP 対応のバックアップアプリケーションを使用して、テープバックアップおよびリストア処理を実行できます。

#### このタスクについて

テープバックアップおよびリストアワークフローでは、テープバックアップおよびリストア処理の実行に関連するタスクの概要を示します。バックアップおよびリストア処理の実行の詳細については、バックアップアプ



リケーションのマニュアルを参照してください。

## 手順

1. NDMP でサポートされているテープトポロジを選択して、テープライブラリの構成をセットアップします。
2. ストレージシステムで NDMP サービスを有効にします。

NDMP サービスはノードレベルまたは Storage Virtual Machine (SVM) レベルで有効にすることができます。これは、テープバックアップおよびリストア処理を実行するために選択する NDMP モードによって異なります。

3. NDMP オプションを使用して、ストレージシステムで NDMP を管理します。

NDMP オプションはノードレベルまたは SVM レベルで使用できます。これは、テープバックアップおよびリストア処理を実行するために選択する NDMP モードによって異なります。

NDMP オプションは、を使用してノードレベルで変更できます `system services ndmp modify` コマンドを実行し、を使用してSVMレベルで実行します `vserver services ndmp modify` コマンドを実行しますこれらのコマンドの詳細については、マニュアルページを参照してください。

4. NDMP 対応のバックアップアプリケーションを使用して、テープバックアップまたはリストア処理を実行します。

ONTAP では、テープバックアップおよびリストア用のダンプエンジンと SMTape エンジンの両方がサポートされます。

バックアップアプリケーション（\_データ管理アプリケーション\_ または \_DMA\_ と呼ばれる）を使用してバックアップまたはリストア操作を実行する方法の詳細については、バックアップアプリケーションのマニュアルを参照してください。

## 関連情報

[一般的な NDMP テープバックアップトポロジ](#)

[FlexVol ボリュームのダンプエンジンの概要](#)

## テープバックアップエンジンの選択のユースケース

ONTAP では、SMTape とダンプの 2 つのバックアップエンジンがサポートされます。SMTape バックアップエンジンとダンプバックアップエンジンのユースケースについて理解しておく、テープバックアップおよびリストア処理を実行するバックアップエンジンを選択する際に役立ちます。

ダンプは次の場合に使用できます。

- ファイルおよびディレクトリの Direct Access Recovery (DAR)
- 特定のパスの一部のサブディレクトリまたはファイルのバックアップ
- バックアップ中に特定のファイルおよびディレクトリを除外する
- 長期間にわたるバックアップの保持

SM Tape は、次の場合に使用できます。

- ディザスタリカバリ解決策
- リストア処理時にバックアップしたデータの重複排除による削減効果および重複排除設定の保持
- 大容量ボリュームのバックアップ

## テープドライブを管理します

### テープドライブの管理の概要

テープバックアップまたはリストア処理を実行する前に、テープライブラリの接続とテープドライブの情報を確認できます。未認定テープドライブを使用するには、そのドライブを認定テープドライブにエミュレートする必要があります。また、既存のエイリアスを確認するだけでなく、テープエイリアスを割り当てたり、削除したりすることもできます。

データをテープにバックアップする場合、データはテープファイルに格納されます。各テープファイルはファイルマークで区切られ、名前はありません。テープファイルはテープ上の位置で指定します。テープファイルへの書き込みには、テープデバイスを使用します。テープファイルを読み取るには、そのテープファイルへの書き込み時と圧縮形式が同じデバイスを指定する必要があります。

テープドライブ、メディアチェンジャ、およびテープドライブの処理を管理するコマンドです

クラスタ内のテープドライブとメディアチェンジャに関する情報を表示するコマンド、テープドライブをオンラインまたはオフラインにするコマンド、テープドライブのカートリッジ位置を変更するコマンド、テープドライブのエイリアス名を設定およびクリアするコマンド、およびテープドライブをリセットするコマンドが用意されています。また、テープドライブの統計を表示およびリセットすることもできます。

状況	使用するコマンド
テープドライブをオンラインにします	<code>storage tape online</code>
テープドライブまたはメディアチェンジャのエイリアス名を消去します	<code>storage tape alias clear</code>
テープドライブのテープのトレース処理を有効または無効にします	<code>storage tape trace</code>
テープドライブのカートリッジ位置を変更します	<code>storage tape position</code>
テープドライブをリセットします	<div><code>storage tape reset</code><div>このコマンドは、advanced 権限レベルでのみ使用できます。</div></div>

状況	使用するコマンド
テープドライブまたはメディアチェンジャのエイリアス名を設定します	<code>storage tape alias set</code>
テープドライブをオフラインにします	<code>storage tape offline</code>
すべてのテープドライブとメディアチェンジャに関する情報を表示します	<code>storage tape show</code>
クラスタに接続されているテープドライブに関する情報を表示します	<ul style="list-style-type: none"> <li>• <code>storage tape show-tape-drive</code></li> <li>• <code>system node hardware tape drive show</code></li> </ul>
クラスタに接続されているメディアチェンジャに関する情報を表示します	<code>storage tape show-media-changer</code>
クラスタに接続されているテープドライブに関するエラー情報を表示します	<code>storage tape show-errors</code>
クラスタ内の各ノードに接続されており、ONTAP で認定およびサポートされているすべてのテープドライブを表示します	<code>storage tape show-supported-status</code>
クラスタ内の各ノードに接続されているすべてのテープドライブとメディアチェンジャのエイリアスを表示します	<code>storage tape alias show</code>
テープドライブの統計値をゼロにリセットします	<code>storage stats tape zero tape_name</code>  このコマンドはノードシェルで使用する必要があります。
ONTAP でサポートされているテープドライブを表示します	<code>storage show tape supported [-v]</code>  このコマンドはノードシェルで使用する必要があります。を使用できます <code>-v</code> 各テープドライブの詳細を表示するオプション。
テープのパフォーマンスを把握し、使用パターンを確認するには、テープデバイスの統計を表示します	<code>storage stats tape tape_name</code>  このコマンドはノードシェルで使用する必要があります。

これらのコマンドの詳細については、マニュアルページを参照してください。

## 未認定テープドライブを使用する

未認定テープドライブで認定テープドライブをエミュレートできる場合は、ストレージシステムでその未認定テープドライブを使用できます。認定テープドライブとして扱われます。未認定テープドライブを使用するには、そのドライブで認定テープドライブのエミュレートが可能かどうかを最初に確認する必要があります。

### このタスクについて

未認定テープドライブはストレージシステムに接続されているドライブですが、ONTAP ではサポートまたは認識されません。

### 手順

1. を使用して、ストレージシステムに接続されている未認定テープドライブを表示します storage tape show-supported-status コマンドを実行します

次のコマンドは、ストレージシステムに接続されているテープドライブおよび各テープドライブのサポートと認定のステータスを表示します。また、未認定テープドライブも表示されます。

tape\_drive\_vendor name は、ストレージシステムに接続されていますが、ONTAP でサポートされていない未認定テープドライブです。

```
cluster1::> storage tape show-supported-status -node Node1
```

Node: Node1	Is	
Tape Drive	Supported	Support Status
-----	-----	-----
"tape_drive_vendor_name"	false	Nonqualified tape drive
Hewlett-Packard C1533A	true	Qualified
Hewlett-Packard C1553A	true	Qualified
Hewlett-Packard Ultrium 1	true	Qualified
Sony SDX-300C	true	Qualified
Sony SDX-500C	true	Qualified
StorageTek T9840C	true	Dynamically Qualified
StorageTek T9840D	true	Dynamically Qualified
Tandberg LTO-2 HH	true	Dynamically Qualified

2. 認定テープドライブをエミュレートします。

"ネットアップのダウンロード：テープデバイスの構成ファイル"

### 関連情報

[認定テープドライブとは](#)

テープエイリアスを割り当てます

テープドライブやメディアチェンジャにテープエイリアスを割り当てて、デバイスを簡

単に識別することができます。エイリアスを割り当てることによって、バックアップデバイスの論理名と、テープドライブやメディアチェンジャに永続的に割り当てられた名前を関連付けることができます。

#### 手順

1. を使用して、テープドライブまたはメディアチェンジャにエイリアスを割り当てます `storage tape alias set` コマンドを実行します

このコマンドの詳細については、マニュアルページを参照してください。

を使用して、テープドライブに関するシリアル番号 (SN) 情報を表示できます `system node hardware tape drive show` コマンド、およびを使用したテープライブラリについて `system node hardware tape library show` コマンド

次のコマンドは、ノード `cluster1-01` に接続されているシリアル番号 `SN[123456]L4` のテープドライブにエイリアス名を設定します。

```
cluster-01::> storage tape alias set -node cluster-01 -name st3
-mapping SN[123456]L4
```

次のコマンドは、ノード `cluster1-01` に接続されているシリアル番号 `SN[65432]` のメディアチェンジャにエイリアス名を設定します。

```
cluster-01::> storage tape alias set -node cluster-01 -name mc1
-mapping SN[65432]
```

#### 関連情報

[テープのエイリアス設定とは](#)

[テープエイリアスを削除しています](#)

テープエイリアスを削除します

を使用してエイリアスを削除できます `storage tape alias clear` テープドライブまたはメディアチェンジャで永続的なエイリアスが不要になった場合のコマンド。

#### 手順

1. を使用して、テープドライブまたはメディアチェンジャからエイリアスを削除します `storage tape alias clear` コマンドを実行します

このコマンドの詳細については、マニュアルページを参照してください。

次のコマンドでは、エイリアスのクリア処理の範囲をに指定して、すべてのテープドライブのエイリアスを削除します `tape` :

```
cluster-01::>storage tape alias clear -node cluster-01 -clear-scope tape
```

完了後

NDMP を使用してテープバックアップまたはリストア処理を実行する場合は、テープドライブまたはメディアチェンジャからエイリアスを削除したあとで、そのテープドライブまたはメディアチェンジャに新しいエイリアス名を割り当てて、テープデバイスに引き続きアクセスできるようにする必要があります。

関連情報

[テープのエイリアス設定とは](#)

[テープエイリアスを割り当てます](#)

テープ予約機能の有効化または無効化

を使用して、ONTAP によるテープデバイスの予約の管理方法を制御できます

tape.reservations オプションデフォルトでは、テープ予約機能は無効になっています。

このタスクについて

テープ予約オプションを有効にすると、テープドライブ、メディアチェンジャ、ブリッジ、またはライブラリが適切に機能しない場合に原因の問題が発生する可能性があります。テープコマンドを実行した際に、他のストレージシステムがデバイスを使用していないにもかかわらず、デバイスが予約されているというメッセージが表示される場合には、このオプションを無効にしてください

手順

1. SCSI 予約 / リリースメカニズムまたは SCSI 永続的予約機能を使用してテープ予約を無効にするには、クラッシュシェルで次のコマンドを入力します。

```
options -option-name tape.reservations -option-value {scsi | persistent | off}
```

scsi SCSI予約/リリースメカニズムを選択します。

persistent SCSI永続的予約を選択します。

off テープ予約を無効にします。

関連情報

[テープ予約機能とは](#)

テープライブラリの接続を確認するコマンド

ストレージシステムとそのストレージシステムに接続されているテープライブラリの構成との間の接続パスに関する情報を表示できます。この情報は、テープライブラリの構成への接続パスを確認する場合や、接続パスに関連する問題のトラブルシューティングを行う場合に使用します。

テープライブラリに関する次の詳細情報を表示して、新しいテープライブラリを追加または作成したあとや、

テープライブラリへのシングルパスアクセスまたはマルチパスアクセスで障害が発生したパスをリストアしたあとに、テープライブラリの接続を確認できます。この情報は、パス関連のエラーのトラブルシューティングを行う場合や、テープライブラリへのアクセスが失敗した場合にも使用できます。

- テープライブラリの接続先のノードを指定します
- デバイス ID
- NDMPパス
- テープライブラリの名前
- ターゲットポートとイニシエータポートの ID
- 各ターゲットポートまたは FC イニシエータポートのテープライブラリへのシングルパスアクセスまたはマルチパスアクセス
- パス関連のデータ整合性の詳細（「パスエラー」や「パス品質」など）
- LUN グループと LUN 数

状況	使用するコマンド
クラスタ内のテープライブラリに関する情報を表示します	<code>system node hardware tape library show</code>
テープライブラリのパス情報を表示します	<code>storage tape library path show</code>
各イニシエータポートのテープライブラリのパス情報を表示します	<code>storage tape library path show-by-initiator</code>
ストレージのテープライブラリとクラスタの間の接続情報を表示します	<code>storage tape library config show</code>

これらのコマンドの詳細については、マニュアルページを参照してください。

## テープ・ドライブについて

### 認定テープドライブの概要

ストレージシステムで正常に動作することがテストによって確認された認定テープドライブを使用する必要があります。テープのエイリアス設定に従って、さらにテープ予約機能も有効にすると、一度に 1 つのストレージシステムだけがテープドライブにアクセスできるよう制御できます。

認定テープドライブとは、ストレージシステムで正常に動作することがテストによって確認されたテープドライブです。テープ構成ファイルを使用すると、既存の ONTAP リリース用にテープドライブを認定できます。

### テープ構成ファイルの形式

テープ構成ファイルの形式は、テープドライブのベンダー ID、製品 ID、圧縮形式の詳細などのフィールドで構成されます。このファイルには、テープ・ドライブの自動ロー

ド機能を有効にし、テープ・ドライブのコマンド・タイムアウト値を変更するオプションのフィールドも含まれています。

次の表に、テープ構成ファイルの形式を示します。

項目	サイズ	説明
vendor_id 文字列	最大 8 バイト	によって報告されるベンダーID SCSI Inquiry コマンドを実行します
`product_id` 文字列	最大16バイト	によって報告される製品ID SCSI Inquiry コマンドを実行します
id_match_size (数値)		テープドライブの識別に使用される製品 ID のバイト数を指定します。このバイト数は、Inquiry コマンドで表示される製品 ID の最初の文字から数えます。
vendor_pretty 文字列	最大16バイト	このパラメータを使用する場合は、コマンドによって表示される文字列を指定します。`storage tape show -device-names` 以外の場合は、INQ_VENDOR_ID と表示されます。
`product_pretty` 文字列	最大16バイト	このパラメータを使用する場合は、コマンドによって表示される文字列を指定します。`storage tape show -device-names` 以外の場合は、INQ_PRODUCT_ID が表示されます。



。 vendor\_pretty および product\_pretty フィールドはオプションですが、いずれかのフィールドに値が設定されている場合は、もう一方のフィールドにも値が設定されている必要があります。

次の表では、などのさまざまな圧縮形式の概要、密度コード、および圧縮アルゴリズムについて説明します  
l、m、h および `a` :

項目	サイズ	説明
`l`	m	h



項目	サイズ	説明
a}_description=(string)`	最大24バイト	ノードシェルコマンドに対して出力される文字列。sysconfig -t、特定の密度設定の特性を説明します。
`{	m	h
a}_density=(hex codes)`		l、m、h、またはaの密度コードに対応する SCSI モードのページブロック記述子で設定される密度コード
`{	m	h
a}_algorithm=(hex codes)`		密度コードと目的の密度特性に対応する SCSI 圧縮モードページで設定される圧縮アルゴリズム。

次の表に、テープ構成ファイル内のオプションフィールドを示します。

フィールド	説明
autoload=(Boolean yes/no)	このフィールドには設定されます yes テープドライブに自動ロード機能が搭載されている場合、つまりテープカートリッジを挿入すると、を実行しなくてもテープドライブの準備が完了します SCSI load (スタート/ストップユニット) コマンドこのフィールドのデフォルトはです no。
cmd_timeout_0x	<p>個々のタイムアウト値。このフィールドは、テープドライブのデフォルトのタイムアウト値とは異なるタイムアウト値を指定する場合にのみ使用します。サンプルファイルには、テープドライブのデフォルトの SCSI コマンドタイムアウト値の一覧が記載されています。タイムアウト値は、分 (m)、秒 (s)、またはミリ秒 (ms) で指定できます。</p> <div>  <p>このフィールドは変更しないでください。</p> </div>

テープ構成ファイルは、NetApp Support Siteからダウンロードして確認できます。

テープ構成ファイルの形式の例

HP LTO5 ULTRIUM テープドライブのテープ構成ファイルの記述形式は次のとおりです。

```
vendor_id="HP"
```

```
product_id="Ultrium 5-SCSI"

id_match_size= 9

vendor_pretty="Hewlett-Packard"

product_pretty="LTO-5"

l_description="LTO-3 (ro) / 4 4 / 800GB "

l_density= 0x00

l_algorithm= 0x00

m_description="LTO-3 (ro) / 4 8 / 1600GB CMP "

m_density= 0x00

m_algorithm= 0x01

h_description="LTO-5 1600GB"

h_density= 0x58

h_algorithm= 0x00

a_description="LTO-5 3200GB CMP"

a_density= 0x58

a_algorithm= 0x01

autoload="はい"
```

## 関連情報

["ネットアップのツール：テープデバイス構成ファイル"](#)

## ストレージシステムによる新しいテープドライブの動的な認定方法

ストレージシステムは、テープドライブのベンダー ID と製品 ID をテープ認定テーブル内の情報と照合することによって、テープドライブを動的に認定します。

テープドライブをストレージシステムに接続すると、テープ検出で取得したベンダー ID と製品 ID が内部テープ認定テーブル内の情報と一致しているかどうかを確認されます。一致する情報が見つかり、そのテープドライブが認定ドライブとしてマークされ、ストレージシステムからそのテープドライブにアクセスできるようになります。一致する情報が見つからなかった場合、そのテープドライブは未認定のままになり、ストレージシステムからアクセスすることはできません。

## テープデバイスの概要

テープデバイスとは、テープドライブを表したものです。テープドライブの巻き戻し形式および圧縮機能の特定の組み合わせです。

テープデバイスは、巻き戻し形式と圧縮機能の組み合わせごとに 1 つ作成されます。したがって、1 つのテープドライブまたはテープライブラリに複数のテープデバイスが関連付けられる可能性があります。テープの移動、書き込み、または読み取りを行うには、テープデバイスを指定する必要があります。

ストレージシステムにテープドライブまたはテープライブラリを取り付けると、ONTAP により、そのテープドライブまたはテープライブラリに関連付けられたテープデバイスが作成されます。

ONTAP は、テープドライブとテープライブラリを検出し、論理番号とテープデバイスを割り当てます。ONTAP は、インターフェイスポートに接続されている場合、ファイバチャネル、SAS、パラレル SCSI テープドライブおよびライブラリを検出します。ONTAP では、インターフェイスを有効にすると、これらのドライブが検出されます。

#### テープデバイス名の形式

各テープデバイスには、定義された形式で表示される名前が関連付けられています。この形式には、デバイスの種類、巻き戻し形式、エイリアス、および圧縮形式に関する情報が含まれています。

テープデバイス名の形式は次のとおりです。

```
rewind_type st alias_number compression_type
```

`rewind_type` は、巻き戻し形式です。

次に、巻き戻し形式のさまざまな値を示します。

- `* R *`

ONTAP は、テープファイルの書き込み終了後に、テープを巻き戻します。

- `* nr *`

ONTAP は、テープファイルの書き込み終了後に、テープを巻き戻しません。同じテープに複数のテープファイルを書き込む場合には、この巻き戻し形式を指定する必要があります。

- `* ur *`

アンロード / リロード巻き戻し形式です。この巻き戻し形式を使用すると、テープファイルの終わりに達したときにテープライブラリによってテープが取り出され、次のテープがある場合は、そのテープが装填されます。

この巻き戻し形式は、次の場合にのみ使用してください。

- このデバイスに関連付けられているテープドライブが、テープライブラリに収容されているか、ライブラリモードのメディアチェンジャに収容されている場合
- このデバイスに関連付けられているテープドライブがストレージシステムに接続されている場合

- 。このテープドライブに対して定義されているライブラリテープシーケンス内に、実行中の処理に対応する十分な数のテープがある場合



ノーリwindデバイスを使用してテープに書き込みを行った場合、そのテープを読み取る前にテープを巻き戻す必要があります。

st は、テープドライブの標準的な指定です。

alias\_number は、ONTAP がテープドライブに割り当てるエイリアスです。ONTAP ONTAP は、新しいテープドライブを検出すると、そのテープドライブにエイリアスを割り当てます。

compression\_type は、テープ上のデータ密度と圧縮形式を表すドライブ固有のコードです。

次に、のさまざまな値について説明します compression\_type :

- \* a \*

最高密度の圧縮

- \* H \*

高い圧縮率

- \* M \*

中密度の圧縮

- \* L \*

低密度の圧縮

例

nrst0a は、テープドライブ0上のノーリwindデバイスで、最高の圧縮を使用していることを示しています。

テープデバイスの一覧の例

次に、 HP Ultrium 2-SCSI に関連付けられたテープデバイスの一覧の例を示します。

```

Tape drive (fc202_6:2.126L1)  HP      Ultrium 2-SCSI
rst0l - rewind device,          format is: HP (200GB)
nrst0l - no rewind device,      format is: HP (200GB)
urst0l - unload/reload device,  format is: HP (200GB)
rst0m - rewind device,          format is: HP (200GB)
nrst0m - no rewind device,      format is: HP (200GB)
urst0m - unload/reload device,  format is: HP (200GB)
rst0h - rewind device,          format is: HP (200GB)
nrst0h - no rewind device,      format is: HP (200GB)
urst0h - unload/reload device,  format is: HP (200GB)
rst0a - rewind device,          format is: HP (400GB w/comp)
nrst0a - no rewind device,      format is: HP (400GB w/comp)
urst0a - unload/reload device,  format is: HP (400GB w/comp)

```

上記の例で使用されている略語の意味は、次のとおりです。

- GB - ギガバイト。テープの容量を示します。
- w/comp - 圧縮あり。圧縮時のテープ容量を示します。

同時に接続可能なテープデバイスの数

ONTAP では、ファイバチャネル、SCSI、または SAS の接続を任意に組み合わせた環境において、各ストレージシステムにつき（ノードあたり）最大 64 個のテープドライブの同時接続、16 台のメディアチェンジャ、および 16 台のブリッジまたはルータデバイスをサポートします。

テープドライブまたはメディアチェンジャには、物理テープライブラリまたは仮想テープライブラリ内のデバイスやスタンドアロンデバイスを使用できます。



ストレージシステムは 64 個のテープドライブの接続を検出できますが、同時に実行できるバックアップおよびリストアセッションの最大数はバックアップエンジンのスケーラビリティ制限によって異なります。

## 関連情報

[ダンプバックアップおよびリストアセッションのスケーラビリティ制限](#)

## テープのエイリアス設定

### テープのエイリアス設定の概要

エイリアス設定を行うと、デバイスの識別が簡単になります。エイリアス設定では、テープまたはメディアチェンジャの Physical Path Name（PPN；物理パス名）または Serial Number（SN；シリアル番号）を、永続的で変更可能なエイリアス名にバインドします。

次の表では、テープのエイリアス設定によって、テープドライブ（またはテープライブラリやメディアチェン

ジャ) に常に単一のエイリアス名が関連付けられるようにする方法を示します。

シナリオ ( <b>Scenario</b> )	エイリアスの再割り当て
システムが再起動したとき	テープドライブには、以前のエイリアスが自動的に再割り当てされます。
テープデバイスを別のポートに移動したとき	エイリアスは、新しいアドレスを指すように調整できます。
複数のシステムで特定のテープデバイスを使用する場合	すべてのシステムでエイリアスを同じに設定できます。



Data ONTAP 8.1.x から Data ONTAP 8.2.x にアップグレードする場合は、Data ONTAP 8.2.x のテープエイリアス機能によって、既存のテープエイリアス名が変更されます。このような場合は、バックアップアプリケーションでテープエイリアス名の更新が必要になることがあります。

テープエイリアスを割り当てることによって、バックアップデバイスの論理名 ( st0 、 mc1 など) と、ポート、テープドライブ、またはメディアチェンジャに永続的に割り当てられた名前を関連付けることができます。



st0 と st00 は異なる論理名です。



論理名とシリアル番号は、デバイスへのアクセスにのみ使用されます。アクセスされたデバイスは、物理パス名を使用してすべてのエラーメッセージを返します。

エイリアス設定に使用できる名前には、物理パス名とシリアル番号の 2 種類があります。

物理パス名とは

PPN は、ONTAP がテープドライブおよびテープライブラリに割り当てる数値アドレスです。PPN は、テープドライブおよびテープライブラリが、ストレージシステム上のどの SCSI-2 / 3 アダプタまたはスイッチ (特定の場所) に接続されているかに基づいて割り当てられます。PPN は、「電気的カル名」とも呼ばれます。

直接接続されたデバイスの PPN は、次の形式になります。host\_adapter。device\_id\_lun



LUN の値は、テープやメディアチェンジャの LUN の値が 0 以外の場合 (LUN の値が 0 の場合) にのみ表示されます lun PPN の一部は表示されません。

たとえば、PPN が 8.6 となっている場合、ホストアダプタ番号が 8、デバイス ID が 6、論理ユニット番号 (LUN) が 0 であることを示します。

SAS テープデバイスも直接接続されたデバイスです。たとえば、PPN が 5c.4 となっている場合、ストレージシステムでは、SAS HBA がスロット 5 で接続されており、SAS テープが SAS HBA のポート C に接続されており、デバイス ID が 4 であることを示します。

ファイバチャネルスイッチ接続デバイスのPPNは、次の形式になります。 switch:port\_id.  
device\_id\_lun

たとえば、PPN が MY\_SWITCH : 5.3L2 となっている場合、スイッチ MY\_SWITCH のポート 5 にテープドライブが接続されており、そのテープドライブのデバイス ID が 3、LUN が 2 であることを示します。

LUN はドライブで決定されます。ファイバチャネル、SCSI テープドライブ / ライブラリ、およびディスクには PPN が使用されます。

テープドライブおよびライブラリの PPN が変更されるのは、スイッチ名を変更した場合、テープドライブまたはライブラリを移動したり再設定したりした場合のみです。リブート後も PPN は変更されません。たとえば、MY\_SWITCH : 5.3L2 という名前のテープドライブを取り外して、デバイス ID および LUN が同じである新しいテープドライブをスイッチ MY\_SWITCH のポート 5 に接続した場合、引き続き、MY\_SWITCH : 5.3L2 という名前を使用して新しいテープドライブにアクセスできます。

シリアル番号とは

シリアル番号（SN）は、テープドライブやメディアチェンジャに割り当てられる一意の識別子です。ONTAP では、WWN ではなく SN に基づいてエイリアスが生成されます。

SN はテープドライブやメディアチェンジャに割り当てられる一意の識別子なので、テープドライブやメディアチェンジャに接続するパスが複数あってもエイリアスは変わりません。これにより、ストレージシステムでは、テープライブラリの構成で同じテープドライブまたはメディアチェンジャを追跡できます。

テープドライブまたはメディアチェンジャの接続先のファイバチャネルスイッチの名前を変更しても、テープドライブまたはメディアチェンジャの SN は変わりません。ただし、テープライブラリでは、既存のテープドライブを新しいものに交換すると、ONTAP によって新しいエイリアスが生成されます。これは、テープドライブの SN が変わるためです。また、既存のテープドライブをテープライブラリ内の新しいスロットに移動するか、テープドライブの LUN を再マッピングすると、そのテープドライブ用の新しいエイリアスが ONTAP によって生成されます。



新しく生成されたエイリアスを使用してバックアップアプリケーションを更新する必要があります。

テープデバイスのSNは、次の形式を使用します。 SN[xxxxxxxxxxx]L[X]

x は英数字とLですx は、テープデバイスのLUNです。LUNが0の場合はLx 文字列の一部は表示されません。

各 SN は最大 32 文字で構成されます。SN の形式では大文字と小文字は区別されません。

マルチパステープアクセスを設定する際の考慮事項

ストレージシステムからテープライブラリのテープドライブにアクセスするパスを 2 つ設定できます。いずれかのパスで障害が発生した場合、そのパスをすぐに修復しなくても、他のパスを使用してテープドライブにアクセスできます。これにより、テープ処理を再開できます。

ストレージシステムからのマルチパステープアクセスを設定する際には、次の点を考慮する必要があります。

- LUN マッピングをサポートするテープライブラリでは、LUN グループへのマルチパスアクセスのため

に、各パスで対称になるように LUN マッピングを行う必要があります。

テープドライブとメディアチェンジャは、テープライブラリ内の LUN グループ（同じイニシエータのパスセットを共有する LUN のセット）に割り当てられます。複数のすべてのパスにおけるバックアップおよびリストア処理で、LUN グループのすべてのテープドライブが使用可能である必要があります。

- ストレージシステムからテープライブラリのテープドライブにアクセスするパスを最大 2 つ設定できます。
- マルチパステープアクセスでは負荷分散がサポートされます。デフォルトでは、ロードバランシングは無効になっています。

次の例では、ストレージシステムは、2 つのイニシエータパス 0b および 0d を介して LUN グループ 0 にアクセスします。これらの両方のパスで、LUN グループの LUN 番号、0、LUN 数 5 は同じです。ストレージシステムは、1 つのイニシエータパス 3d のみを使用して LUN グループ 1 にアクセスします。

```
STSW-3070-2_cluster::> storage tape library config show
```

Node	LUN Group	LUN Count	Library Name	Library
Target Port	Initiator			
STSW-3070-2_cluster-01	0	5	IBM 3573-TL_1	
510a09800000412d	0b			
0d				
	1	2	IBM 3573-TL_2	
50050763124b4d6f	3d			

3 entries were displayed

詳細については、マニュアルページを参照してください。

ストレージシステムにテープドライブとライブラリを追加する方法

テープドライブとライブラリをストレージシステムに動的に追加できます（ストレージシステムをオフラインにする必要はありません）。

新しいメディアチェンジャを追加すると、ストレージシステムによって、追加したメディアチェンジャが検出されて構成に追加されます。メディアチェンジャがすでにエイリアス情報内に定義されている場合、新しい論理名は作成されません。定義されていない場合は、ストレージシステムによってそのメディアチェンジャのエイリアスが新しく作成されます。

テープライブラリの構成では、ターゲットポートの LUN 0 にテープドライブまたはメディアチェンジャを設定して、そのターゲットポート上のすべてのメディアチェンジャとテープドライブを ONTAP が検出できるようにする必要があります。



## テープ予約機能とは

テープドライブ、メディアチェンジャ、ブリッジ、テープライブラリなどは共有可能であるため、複数のストレージシステムからアクセスできます。テープ予約機能を利用すると、すべてのテープドライブ、メディアチェンジャ、ブリッジ、およびテープライブラリで、SCSI 予約 / リリースメカニズムまたは SCSI 永続的予約機能のいずれかを有効にして、一度に 1 つのストレージシステムだけがデバイスにアクセスするよう制御できます。



スイッチが含まれているかどうかにかかわらず、ライブラリ内のデバイスを共有するすべてのシステムで同じ予約方法を使用する必要があります。

SCSI 予約 / リリースメカニズムによるデバイス予約は、通常の状態では適切に機能します。ただし、インターフェイスエラーからのリカバリ処理中に予約内容が消失することがあります。この場合、予約済みの所有者以外のイニシエータがデバイスにアクセスできます。

SCSI 永続的予約機能による予約は、ループリセットやターゲットリセットなどのエラーリカバリメカニズムには影響されません。ただし、すべてのデバイスに、SCSI 永続的予約機能が正しく実装されているとは限りません。

## ndmpcopy を使用してデータを転送します

**ndmpcopy** の概要を使用してデータを転送します

。 **ndmpcopy** ノードシェルコマンドは、NDMP v4をサポートするストレージシステム間でデータを転送します。フルデータ転送と増分データ転送の両方を実行できます。ボリューム、**qtree**、ディレクトリの全体または一部や、個々のファイルを転送できます。

このタスクについて

ONTAP 8.x 以前のリリースでは、増分転送は最大 2 つのレベル（1 つのフルバックアップと最大 2 つの増分バックアップ）に制限されます。


ONTAP 9.0 以降のリリースでは、増分転送の最大レベルは 9（1 つのフルバックアップと最大 9 つの増分バックアップ）に制限されています。

走れ **ndmpcopy** ソースストレージシステムとデスティネーションストレージシステム、またはデータ転送のソースでもデスティネーションでもないストレージシステムのノードシェルコマンドライン。を実行することもできます **ndmpcopy** データ転送のソースとデスティネーションの両方に対応する単一のストレージシステム。

では、ソースストレージシステムとデスティネーションストレージシステムのIPv4アドレスまたはIPv6アドレスを使用できます **ndmpcopy** コマンドを実行しますパスの形式はです `/vserver_name/volume_name \[path\]`。

手順

1. ソースストレージシステムとデスティネーションストレージシステムで、NDMP サービスを有効にします。

ソースまたはデスティネーションでデータ転送を実行するモード	使用するコマンド
SVM を対象とした NDMP モード	<pre>vserver services ndmp on</pre> <div>  <p>管理SVMでのNDMP認証の場合、ユーザアカウントはです admin ユーザ ロールはです admin または backup。データSVMでは、ユーザ アカウントはです vsadmin ユーザ ロールはです vsadmin または vsadmin-backup ロール。</p> </div>
ノードを対象とした NDMP モード	<pre>system services ndmp on</pre>

2. を使用して、ストレージシステム内またはストレージシステム間でデータを転送します ndmpcopy 次のコマンドをノードシェルで実行します。

```
::> system node run -node <node_name> < ndmpcopy [options]
source_IP:source_path destination_IP:destination_path [-mcs {inet|inet6}] [-mcd {inet|inet6}] [-md {inet|inet6}]
```



ndmpcopy では、DNS 名はサポートされません。ソースとデスティネーションの IP アドレスを指定する必要があります。ソースまたはデスティネーションの IP アドレスでは、ループバックアドレス（127.0.0.1）はサポートされません。

- °。 ndmpcopy コマンドは、次のように制御接続のアドレスモードを決定します。
  - 制御接続用のアドレスモードは、指定された IP アドレスに対応します。
  - を使用してこれらのルールを上書きできます -mcs および -mcd オプション（Options）
- ° ソースまたはデスティネーションが ONTAP システムの場合は、NDMP モード（ノードを対象とした NDMP モードまたは SVM を対象とした NDMP モード）に応じて、ターゲットボリュームへのアクセスを許可する IP アドレスを使用します。
- ° source\_path および destination\_path は、ボリューム、qtree、ディレクトリ、またはファイルの詳細レベルまでの絶対パス名です。
- ° -mcs ソースストレージシステムへの制御接続で優先されるアドレス指定モードを指定します。

inet IPv4アドレスモードおよびを示します inet6 IPv6アドレスモードを示します。

- ° -mcd デスティネーションストレージシステムへの制御接続で優先的に使用するアドレス指定モードを指定します。

inet IPv4アドレスモードおよびを示します inet6 IPv6アドレスモードを示します。

- ° -md ソースストレージシステムとデスティネーションストレージシステム間のデータ転送で優先されるアドレス指定モードを指定します。

inet IPv4アドレスモードおよびを示します inet6 IPv6アドレスモードを示します。

を使用しない場合 `-md` のオプションを選択します `ndmpcopy` コマンドを実行する場合、データ接続のアドレッシングモードは次のように決定されます。

- 制御接続用に指定されたいずれかのアドレスが IPv6 アドレスの場合、データ接続用のアドレスモードは IPv6 になります。
- 制御接続用に指定された両方のアドレスが IPv4 アドレスの場合は、が表示されます `ndmpcopy` コマンドは、最初にデータ接続に対して IPv6 アドレスモードを試行します。

IPv6 アドレスモードで失敗した場合は、IPv4 アドレスモードを使用します。



IPv6 アドレスを指定する場合は、角かっこで囲む必要があります。

このコマンド例では、ソースパスからデータを移行します (`source_path`) を宛先パスに移動します (`destination_path`)。

```
> ndmpcopy -sa admin:<ndmp_password> -da admin:<ndmp_password>
  -st md5 -dt md5 192.0.2.129:/<src_svm>/<src_vol>
192.0.2.131:/<dst_svm>/<dst_vol>
```

+

次に、制御接続とデータ接続で IPv6 アドレスモードを使用するように明示的に設定するコマンドの例を示します。

```
> ndmpcopy -sa admin:<ndmp_password> -da admin:<ndmp_password> -st md5
-dt md5 -mcs inet6 -mcd inet6 -md
  inet6 [2001:0db8:1:1:209:6bff:feae:6d67]:/<src_svm>/<src_vol>
[2001:0ec9:1:1:200:7cgg:gfdg:7e78]:/<dst_svm>/<dst_vol>
```

## ndmpcopy コマンドのオプション

で利用できるオプションについて理解しておく必要があります `ndmpcopy` データを正常に転送するためのノードシェルコマンド。

次の表に、使用可能なオプションを示します。詳細については、を参照してください `ndmpcopy` ノードシェルから使用可能なマニュアルページ。

オプション	説明
-sa username : [password]	<p>ソースストレージシステムに接続するための、ソース側の認証のユーザ名とパスワードを設定します。これは必須オプションです。</p> <p>管理者権限を持たないユーザは、そのユーザに対応する、システムによって生成された NDMP 固有のパスワードを指定する必要があります。システムによって生成されたパスワードは、admin ユーザと admin 以外のユーザの両方に必須です。</p>
-da username : [password]	<p>デスティネーションストレージシステムに接続するための、デスティネーション側の認証のユーザ名とパスワードを設定します。これは必須オプションです。</p>
-st {md5	text}
このオプションは、ソースストレージシステムに接続するときに使用する、ソース側の認証タイプを設定します。これは必須オプションであるため、ユーザはどちらかを指定する必要があります text または md5 オプション	-dt {md5
text}	<p>デスティネーションストレージシステムに接続するときに使用する、デスティネーション側の認証タイプを設定します。</p>
-l	<p>このオプションは、転送に使用するダンプレベルを、指定したレベルの値に設定します。有効な値はです 0、1、へ 9、ここで 0 完全転送とを示します 1 終了： 9 増分転送を指定します。デフォルトはです 0。</p>
-d	<p>ndmpcopy デバッグログメッセージの生成が有効になります。ndmpcopyデバッグログファイルはにあります /mroot/etc/log ルートボリューム：ndmpcopy デバッグログファイルの名前はにあります ndmpcopy.yyyymmdd の形式で入力し</p>
-f	<p>このオプションは強制モードを有効にします。このモードでは、でシステムファイルを上書きできます /etc 7-Modeボリュームのルートにあるディレクトリ。</p>
-h	ヘルプメッセージが出力されます。

オプション	説明
-p	<p>ソース側とデスティネーション側の認証用のパスワードを入力するよう求められます。このパスワードは、に指定したパスワードよりも優先されます <code>-sa</code> および <code>-da</code> オプション（Options）</p> <div>  <p>このオプションは、対話型コンソールでコマンドを実行する場合にのみ使用できます。</p> </div>
-exclude	<p>データ転送用に指定するパスから、指定されたファイルまたはディレクトリを除外します。ディレクトリ名またはファイル名をカンマで区切ったリスト（など）を値として指定できます <code>.pst</code> または <code>.txt</code>。</p>

## FlexVol ボリューム用の NDMP

### FlexVol ボリュームの NDMP について

Network Data Management Protocol（NDMP；ネットワークデータ管理プロトコル）は、ストレージシステムやテープライブラリなど、プライマリストレージデバイスとセカンダリストレージデバイスとの間で、バックアップやリカバリなどのデータ転送を制御するための標準化されたプロトコルです。

ストレージシステム上で NDMP のサポートを有効にすると、バックアップまたはリカバリ操作に使用する NDMP 対応のネットワーク接続型バックアップアプリケーション（Data Management Applications\_or\_DMA\_とも呼ばれる）、データサーバ、およびテープサーバとの通信をストレージシステムが実行できるようになります。すべてのネットワーク通信は、TCP/IP または TCP/IPv6 ネットワーク経由で行われます。NDMP は、テープドライブとメディアチェンジャの低レベルの制御も行います。

ノードを対象とした NDMP モードと Storage Virtual Machine（SVM）を対象とした NDMP モードのどちらでもテープによるバックアップとリストア処理を実行できます。

NDMP を使用する際の考慮事項、環境変数のリスト、およびサポートされている NDMP テープバックアップトポロジを把握しておく必要があります。拡張 DAR 機能を有効または無効にすることもできます。ONTAP でストレージシステムへの NDMP アクセス認証にサポートされている認証方式は、プレーンテキストとチャレンジの 2 つです。

### 関連情報

[ONTAP でサポートされる環境変数](#)

### NDMP の動作モードについて

テープバックアップおよびリストア処理をノードレベルまたは Storage Virtual Machine（SVM）レベルで実行することができます。これらの処理を SVM レベルで正常に実行するには、SVM で NDMP サービスを有効にする必要があります。

Data ONTAP 8.2 から Data ONTAP 8.3 にアップグレードする場合は、8.2 で使用していた NDMP の動作モードがアップグレード後も維持されます。

Data ONTAP 8.2 以降で新しいクラスタをインストールする場合は、デフォルトで SVM を対象とした NDMP モードになります。ノードを対象とした NDMP モードでテープバックアップおよびリストア処理を実行するには、ノードを対象とした NDMP モードを明示的に有効にする必要があります。

#### 関連情報

[ノードを対象とした NDMP モードの管理用コマンド](#)

[FlexVol ボリュームのノードを対象とした NDMP モードの管理](#)

[FlexVol ボリュームの SVM を対象とした NDMP モードの管理](#)

ノードを対象とした **NDMP** モードとは

ノードを対象とした NDMP モードでは、テープバックアップおよびリストア処理をノードレベルで実行できます。Data ONTAP 8.2 で使用される NDMP の動作モードは、8.2 から 8.3 へのアップグレード後も維持されます。

ノードを対象とした NDMP モードでは、ボリュームを所有するノードでテープバックアップおよびリストア処理を実行できます。これらの処理を実行するには、ボリュームまたはテープデバイスを所有するノードでホストされている LIF で NDMP 制御接続を確立する必要があります。



このモードは廃止予定で、今後のメジャーリリースで削除される予定です。

#### 関連情報

[FlexVol ボリュームのノードを対象とした NDMP モードの管理](#)

**SVM** を対象とした **NDMP** モードとは

NDMP サービスが Storage Virtual Machine (SVM) で有効になっている場合、テープバックアップおよびリストア処理を SVM レベルで正常に実行できます。バックアップアプリケーションで CAB 拡張がサポートされている場合は、クラスタの SVM の異なるノード間でホストされているすべてのボリュームをバックアップおよびリストアできます。

NDMP 制御接続は、さまざまなタイプの LIF で確立できます。SVM を対象とした NDMP モードでは、このような LIF はデータ SVM または管理 SVM に属しています。LIF で接続を確立できるのは、その LIF を所有する SVM で NDMP サービスが有効になっている場合だけです。

データ LIF はデータ SVM に属しています。クラスタ間 LIF、ノード管理 LIF、およびクラスタ管理 LIF は管理 SVM に属しています。

SVM を対象とした NDMP モードでは、バックアップおよびリストア処理に使用できるボリュームとテープデバイスは、NDMP 制御接続が確立される LIF タイプおよび CAB 拡張のステータスによって異なります。バックアップアプリケーションで CAB 拡張がサポートされており、ボリュームとテープデバイスが同じアフィニティを共有している場合は、3 ウェイバックアップまたはリストア処理の代わりにローカルバックアップまたはリストア処理をバックアップアプリケーションで実行できます。

## NDMP 使用時の考慮事項

ストレージシステム上で NDMP サービスを開始する際の考慮事項について説明します。

- 接続されたテープドライブを使用して各ノードでサポートされるバックアップとリストアの同時実行数は、合計で最大 16 個です。
- NDMP サービスでは、NDMP バックアップアプリケーションからの要求に応じてファイル履歴データを生成できます。

バックアップアプリケーションは、ファイル履歴を使用して、選択したデータのサブセットだけをバックアップイメージから最適にリカバリします。ファイル履歴の生成と処理は、ストレージシステムとバックアップアプリケーションの両方で時間がかかり、CPU が占有されることがあります。



SMTape では、ファイル履歴はサポートされていません。

バックアップ・イメージ全体がリカバリされる災害復旧用にデータ保護が設定されている場合は 'ファイル履歴の生成を無効にして' バックアップ時間を短縮できます。NDMP のファイル履歴の生成を無効にできるかどうかについては、バックアップアプリケーションのマニュアルを参照してください。

- すべての LIF タイプでは、NDMP のファイアウォールポリシーがデフォルトで有効になっています。
- ノードを対象とした NDMP モードで FlexVol をバックアップするには、バックアップアプリケーションを使用して、ボリュームを所有するノードでバックアップを開始する必要があります。

ただし、ノードルートボリュームをバックアップすることはできません。

- ファイアウォールポリシーで許可されている場合は、任意の LIF から NDMP バックアップを実行できます。

データ LIF を使用する場合は、フェイルオーバーに設定されていない LIF を選択する必要があります。NDMP 処理中にデータ LIF がフェイルオーバーすると、NDMP 処理は失敗するため、再実行する必要があります。

- ノードを対象とした NDMP モードおよび Storage Virtual Machine (SVM) を対象とした NDMP モードで CAB 拡張がサポートされていない場合、NDMP データ接続では、NDMP 制御接続と同じ LIF を使用します。
- LIF の移行中は、進行中のバックアップおよびリストア処理が中断されます。

LIF の移行が完了したら、バックアップとリストアの処理を開始する必要があります。

- NDMP バックアップパスの形式は、です `/vserver_name/volume_name/path_name`。

`path_name` はオプションで、ディレクトリ、ファイル、または Snapshot コピーのパスを指定します。

- ダンプエンジンを使用して SnapMirror デスティネーションをテープにバックアップする場合は、ボリューム内のデータだけがバックアップされます。

ただし、SMTape を使用して SnapMirror デスティネーションをテープにバックアップする場合は、メタ



データもバックアップされます。SnapMirror 関係および関連するメタデータはテープにバックアップされません。そのため、リストア時には、そのボリュームのデータだけがリストアされますが、関連する SnapMirror 関係はリストアされません。

## 関連情報

### Cluster Aware Backup 拡張の動作

#### "ONTAP の概念"

#### "システム管理"

## 環境変数

### 環境変数の概要

環境変数は、NDMP 対応のバックアップアプリケーションとストレージシステムの間でバックアップまたはリストア処理に関する情報をやり取りするために使用されます。

たとえば、ユーザがバックアップアプリケーションのバックアップを指定した場合などです  
/vserver1/vol1/dir1`では、バックアップアプリケーションによってFILESYSYSTEM環境変数がに設定されます ` /vserver1/vol1/dir1。同様に、レベル 1 バックアップを実行するよう指定した場合、バックアップアプリケーションによって LEVEL 環境変数が 1 に設定されます。



通常、環境変数の設定と確認についてバックアップ管理者の対応は不要で、バックアップアプリケーションによって自動的に設定されます。

バックアップ管理者が環境変数を指定することはまれですが、機能またはパフォーマンスの問題を特定または回避するために、バックアップアプリケーションによって設定された環境変数の値を変更したい場合があります。たとえば、パフォーマンスや機能の問題が、バックアップアプリケーションによるファイル履歴情報の処理に起因しているかどうかを調べる場合、管理者はファイル履歴の生成を一時的に無効にすることがあります。

多くのバックアップアプリケーションでは、環境変数を上書きまたは変更したり、追加の環境変数を指定したりできます。詳細については、バックアップアプリケーションのマニュアルを参照してください。

### ONTAP でサポートされる環境変数

環境変数は、NDMP 対応のバックアップアプリケーションとストレージシステムの間でバックアップまたはリストア処理に関する情報をやり取りするために使用されます。ONTAP でサポートされる環境変数には、デフォルト値が関連付けられています。ただし、これらのデフォルト値は手動で変更できます。

バックアップアプリケーションによって設定された値を手動で変更すると、アプリケーションが想定外の動作をする可能性があります。これは、バックアップアプリケーションで想定されているバックアップまたはリストアとは異なる処理が行われるためです。ただし、変更を適切に行うと、問題の特定や回避に役立つ場合があります。

次の表は、動作がダンプと SMTape で共通であり、ダンプと SMTape でのみサポートされる環境変数を示しています。また、ONTAP でサポートされる環境変数が使用された場合の動作の説明も記載されています。





ほとんどの場合、値を持つ変数、Y 同意します T および N 同意します F。

#### ダンプと **SM**Tape 用にサポートされる環境変数

環境変数	有効な値：	デフォルト	説明
デバッグ	Y または N	N	デバッグ情報を出力するように指定します。
ファイルシステム	string	none	バックアップされるデータのルートのパス名を指定します。
NDMP_VERSION	return_only	none	<p>NDMP_VERSION 変数は変更しないでください。NDMP_VERSION 変数はバックアップ処理によって作成され、NDMP のバージョンを返します。</p> <p>ONTAP は、内部使用のため、および情報としてバックアップアプリケーションに渡すために、バックアップ時に NDMP_VERSION 変数を設定します。NDMP セッションの NDMP バージョンは、この変数では設定されません。</p>
pathname_separator	return_value	none	<p>パス名の区切り文字を指定します。</p> <p>この文字は、バックアップ対象のファイルシステムによって異なります。ONTAP の場合、文字 “/” はこの変数に割り当てられます。NDMP サーバでは、この変数を設定してからテープバックアップ処理を開始します。</p>
を入力します	dump または smtape	dump	テープバックアップおよびリストア処理の実行がサポートされているバックアップのタイプを指定します。

環境変数	有効な値：	デフォルト	説明
詳細	Y または N	N	テープバックアップまたはリストア処理の実行中のログメッセージの数を増やします。

#### ダンプ用にサポートされる環境変数

環境変数	有効な値：	デフォルト	説明
acl_start	return_only	none	<p>ACL_START 変数は、バックアップ処理によって作成され、直接アクセス リストアまたは再開可能 NDMP バックアップ処理で使用されるオフセット値を示します。</p> <p>オフセット値は、ダンプ ファイル内で ACL データ（Pass V）が始まるバイトオフセットであり、バックアップ終了時に返されます。直接アクセス リストア処理でバックアップデータを正しくリストアするには、開始時に ACL_START 値がリストア処理に渡されなければなりません。NDMP 再開可能バックアップ処理では、ACL_START 値を使用して、バックアップストリームで再開できない部分の開始位置をバックアップアプリケーションに伝えます。</p>

環境変数	有効な値：	デフォルト	説明
BASE_DATE	0、-1`または `DUMP_DATE 値	-1	<p>増分バックアップの開始日を指定します。</p> <p>に設定すると -1`BASE_DATEインクリメンタル指定子は無効になっています。に設定すると `0 レベル0バックアップでは、増分バックアップが有効になります。最初のバックアップ後、前回の増分バックアップの DUMP_DATE 変数の値が BASE_DATE 変数に代入されます。</p> <p>これらの変数は、LEVEL または UPDATE に基づく増分バックアップに代わるものです。</p>
直接	Y または N	N	<p>リストアの際に、テーブル全体をスキャンするのではなく、ファイルデータがある場所まで直接早送りするように指定します。</p> <p>直接アクセスリカバリを使用するには、バックアップアプリケーションが位置情報を提供する必要があります。この変数に設定されている場合 `Y` では、バックアップアプリケーションによって、ファイル名またはディレクトリ名と位置情報が指定されます。</p>
dmp_name	string	none	<p>複数サブツリーバックアップの名前を指定します。</p> <p>この変数は、複数サブツリーバックアップに必須です。</p>

環境変数	有効な値：	デフォルト	説明
DUMP_DATE	return_value	none	<p>この変数を直接変更することはありません。BASE_DATE変数が以外の値に設定されている場合、バックアップによって作成されます -1。</p> <p>DUMP_DATE 変数は、ダンプソフトウェアによって計算された 32 ビットの時刻値の前に 32 ビットのレベル値を付けることによって生成されます。レベルは、BASE_DATE 変数に最後に渡されたレベル値から増分されます。作成された値は、次回の増分バックアップの BASE_DATE 値として使用されます。</p>

環境変数	有効な値：	デフォルト	説明
ENHANCED_DAR_ENABLED 環境	Y または N	N	<p>拡張 DAR 機能が有効になっているかどうかを示します。拡張 DAR 機能では、ディレクトリ DAR および NT ストリームを含むファイルの DAR をサポートします。パフォーマンスが向上します。</p> <p>リストア時に拡張 DAR 機能を使用できるのは、次の条件が満たされている場合のみです。</p> <ul style="list-style-type: none"> <li>• ONTAP で拡張 DAR がサポートされている。</li> <li>• バックアップ時にファイル履歴が有効である（HIST=Y）。</li> <li>• 。 ndmpd.offset_map.enable オプションはに設定されています on。</li> <li>• ENHANCED_DAR_ENABLED変数がに設定されている Y リストア中。</li> </ul>

環境変数	有効な値：	デフォルト	説明
除外する	pattern_string	none	<p>データのバックアップ時に除外するファイルまたはディレクトリを指定します。</p> <p>除外リストは、ファイル名またはディレクトリ名をカンマで区切ったリストです。ファイルまたはディレクトリの名前がリスト内の名前の 1 つに一致した場合、バックアップから除外されます。</p> <p>除外リストで名前を指定する際に適用されるルールは次のとおりです。</p> <ul style="list-style-type: none"> <li>• 正確なファイル名またはディレクトリ名を使用する必要があります。</li> <li>• ワイルドカード文字であるアスタリスク（*）は、文字列の最初または最後の文字にする必要があります。</li> </ul> <p>使用できるアスタリスクの数は文字列ごとに 2 つです。</p> <ul style="list-style-type: none"> <li>• ファイル名またはディレクトリ名のカンマの前にバックスラッシュを付ける必要があります。</li> <li>• 除外リストに含めることができる名前は 32 個までです。</li> </ul>

環境変数	有効な値：	デフォルト	説明
抽出（Extract）	Y、N または E	N	<p>バックアップデータセットのサブツリーをリストアするように指定します。</p> <p>バックアップアプリケーションでは、抽出するサブツリーの名前を指定します。指定されたファイルが、内容がバックアップされたディレクトリに一致する場合、ディレクトリは再帰的に抽出されます。</p> <p>DARを使用せずにリストア時にファイル、ディレクトリ、またはqtreeの名前を変更するには、EXTRACT環境変数に設定する必要があります E。</p>
extract_acl	Y または N	Y	<p>リストア処理でバックアップファイルのACL がリストアされるように指定します。</p> <p>デフォルトでは、DAR（DIRECT=Y）を除いて、データをリストアするときにACL がリストアされます。</p>

環境変数	有効な値：	デフォルト	説明
[-force]	Y または N	N	<p>デスティネーションボリュームで使用可能なボリュームスペースと inode をリストア処理で確認する必要があるかどうかを指定します。</p> <p>この変数をに設定します Y デスティネーションパスで使用可能なボリュームスペースとinodeの確認がリストア処理でスキップされます。</p> <p>デスティネーションボリュームのボリュームスペースまたは inode が不足している場合は、デスティネーションボリュームで使用可能なボリュームスペースと inode で許容される量のデータがリストア処理によってリカバリされます。ボリュームスペースと inode を使用できない場合は、リストア処理が停止します。</p>



環境変数	有効な値：	デフォルト	説明
霧	Y または N	N	<p>ファイル履歴情報をバックアップアプリケーションに送信するように指定します。</p> <p>ほとんどの市販のバックアップアプリケーションでは、HIST変数がに設定されています Y。バックアップ処理の速度を上げる場合や、ファイル履歴の収集に関する問題のトラブルシューティングを行う場合は、この変数をに設定します N。</p> <div>  <p>HIST変数をに設定しないでください Y バックアップアプリケーションがファイル履歴をサポートしていない場合。</p> </div>

環境変数	有効な値：	デフォルト	説明
IGNORE_CTime	Y または N	N	<p>前回の増分バックアップ以降に変更されたのが ctime 値だけである場合は、ファイルを増分バックアップしないことを指定します。</p> <p>ウィルススキャンソフトウェアなどの一部のアプリケーションは、ファイルやファイル属性が変更されていなくても、inode 内のファイルの ctime 値を変更します。その結果、変更されていないファイルが増分バックアップによってバックアップされることがあります。。 IGNORE_CTIME 変数を指定する必要があるのは、ctime値が変更されたために増分バックアップに許容できない時間またはスペースが使用されている場合だけです。</p> <div><div></div><div><p>。 NDMP dump コマンドセット IGNORE_CTIME 終了 : false デフォルトではに設定します true 次のデータが失われる可能性があります。</p><p>1. 状況</p><p>IGNOR E_CTI ME ボリュームレベルの増分でtrueに設定されます `ndmpcopy` を実行すると、</p></div></div>

環境変数	有効な値：	デフォルト	説明
IGNORE_qtrees	Y または N	N	リスト処理でバックアップ qtree から qtree 情報をリストアしないことを指定します。
「レベル」	0-31	0	バックアップレベルを指定します。  レベル 0 では、データセット全体がコピーされます。0 より大きい値で指定された増分バックアップレベルでは、前回の増分バックアップ以降に新規作成または変更されたすべてのファイルがコピーされます。たとえば、レベル 1 では、レベル 0 バックアップ以降に新規または変更されたファイルがバックアップされ、レベル 2 ではレベル 1 バックアップ以降に新規または変更されたファイルがバックアップされます。
リスト	Y または N	N	データを実際にはリストアせずに、バックアップファイル名と inode 番号を一覧表示します。
リスト qtree	Y または N	N	データを実際にはリストアせずに、バックアップ qtree を一覧表示します。

IGNORE\_C  
TIME ポリ  
ュームレベ  
ルでfalseに  
設定する必  
要がありま  
す NDMP  
dumps ま  
たは  
ndmpcopy  
。

環境変数	有効な値：	デフォルト	説明
multi_subtree_names	string	none	<p>バックアップが複数のサブツリーであることを指定します。</p> <p>複数のサブツリーは、改行で区切られた null で終わるサブツリー名のリストの文字列で指定されます。サブツリーは、共通のルートディレクトリを基準とした相対パス名で指定されます。このパス名は、リストの最後の要素として指定する必要があります。</p> <p>この変数を使用する場合は、DMP_NAME 変数も使用する必要があります。</p>
NDMP_Unicode_FH	Y または N	N	<p>ファイルの NFS 名のほかに Unicode 名もファイル履歴情報に含めるように指定します。</p> <p>このオプションは、ほとんどのバックアップアプリケーションでは使用されないため、バックアップアプリケーションがこれらの追加のファイル名を受け取るように設計されている場合以外は設定しないでください。HIST 変数も設定する必要があります。</p>
no_ACLS	Y または N	N	<p>データのバックアップ時に ACL をコピーしないように指定します。</p>

環境変数	有効な値：	デフォルト	説明
NON_QUOTA_TREE	Y または N	N	<p>データのバックアップ時に qtree 内のファイルおよびディレクトリを無視するように指定します。</p> <p>に設定すると `Y` では、FILESYSTEM変数で指定されたデータセット内のqtreeの項目はバックアップされません。この変数は、FILESYSTEM変数でボリューム全体が指定された場合のみ有効になります。NON_QUOTA_TREE変数は、レベル 0 バックアップでのみ機能し、MULTI_SUBTREE_NAMES 変数が指定された場合は機能しません。</p> <div>  <p>NON_QUOTA_TREE をに設定した場合、バックアップから除外するように指定したファイルまたはディレクトリは除外されません Y 同時に。</p> </div>
NOWRITE	Y または N	N	<p>リストア処理でデータをディスクに書き込まないように指定します。</p> <p>この変数はデバッグに使用されます。</p>

環境変数	有効な値：	デフォルト	説明
再帰的	Y または N	Y	<p>DAR リストア中にディレクトリエントリが拡張されるように指定します。</p> <p>DIRECTおよびENHANCED_DAR_ENABLED環境変数を有効にする（に設定する）必要があります Y）も参照してください。再帰変数が無効になっている場合（に設定） N`テープからリストアされるのは、元のソースパスにあるすべてのディレクトリに対する権限とACLだけで、ディレクトリの内容はリストアされません。再帰変数がに設定されている場合 `N または、recover_full_paths変数がに設定されている `Y`リカバリパスは元のパスで終了する必要があります。</p> <div><p>RECURSIVE 変数が無効で、複数のリカバリパスがある場合には、すべてのリカバリパスを最長のリカバリパス内に含める必要があります。それ以外の場合は、エラーメッセージが表示されます。</p></div> <p>たとえば、次の例は、すべてのリカバリパスが内にあるため、有効なリカバリパスです</p> <pre>foo/dir1/deepdir/myfile :  /foo  /foo/dir</pre>

環境変数	有効な値：	デフォルト	説明
RECOVER_FULL_paths	Y または N	N	<p>フルリカバリパスの権限および ACL が、DAR のあとでリストアされるように指定します。</p> <p>DIRECTおよび ENHANCED_DAR_ENABLED を有効にする（に設定する）必要があります Y）も参照してください。recover_full_paths がに設定されている場合 `Y` リカバリパスは元のパスで終了する必要があります。デステーションボリュームにすでにディレクトリが存在する場合は、権限および ACL はテープからリストアされません。</p>
更新	Y または N	Y	レベルベースの増分バックアップを有効にするために、メタデータ情報を更新します。

#### SMTape 用にサポートされる環境変数

環境変数	有効な値：	デフォルト	説明
BASE_DATE	DUMP_DATE	-1	<p>増分バックアップの開始日を指定します。</p> <div><p>``BASE_DATE``は、参照Snapshot識別子の文字列表現です。を使用する``BASE_DATE``文字列を指定すると、SMTapeによって参照Snapshotコピーが検索されます。</p></div> <div><p>``BASE_DATE``は、ベースラインバックアップには必要ありません。増分バックアップの場合は、の値``DUMP_DATE``前回のベースラインバックアップまたは増分バックアップの変数が割り当てられます</p><p>``BASE_DATE``変数 (Variable)：</p></div> <p>バックアップアプリケーションによって割り当てられます DUMP_DATE 前回のSMTapeのベースラインバックアップまたは増分バックアップの値。</p>



環境変数	有効な値：	デフォルト	説明
DUMP_DATE	return_value	none	<p>SMTape バックアップの終了時、DUMP_DATE には、そのバックアップに使用される Snapshot コピーを識別する文字列識別子が含まれています。この Snapshot コピーを、次の増分バックアップの参照 Snapshot コピーとして使用できます。</p> <p>結果の DUMP_DATE の値が、次の増分バックアップの BASE_DATE 値として使用されます。</p>
smtape_backup_set_ID	string	none	<p>ベースラインバックアップに関連付けられた増分バックアップのシーケンスを識別します。</p> <p>バックアップセット ID は、ベースラインバックアップで生成される 128 ビットの一意的 ID です。バックアップアプリケーションは、この ID を入力として割り当てます</p> <p>SMTAPE_BACKUP_SET_ID 増分バックアップ中の変数。</p>
smtape snapshot_name	ボリューム内にある有効な Snapshot コピー	Invalid	<p>SMTAPE_SNAPSHOT_NAME 変数を Snapshot コピーに設定すると、その Snapshot コピーと古い Snapshot コピーがテープにバックアップされます。</p> <p>増分バックアップの場合は、この変数によって増分 Snapshot コピーが指定されます。BASE_DATE 変数はベースライン Snapshot コピーを指定します。</p>

環境変数	有効な値：	デフォルト	説明
smtape delete _snapshot	Y または N	N	SMTAPE_DELETE_SNAPSHOT変数をに設定すると、SMTapeで自動的に作成されるSnapshotコピー `Y` バックアップ処理が完了すると、SMTapeによってこのSnapshotコピーが削除されます。ただし、バックアップアプリケーションで作成されたSnapshot コピーは削除されません。
smtape break _mirror	Y または N	N	SMTAPE_BREAK_MIRROR変数がに設定されている場合 Y、タイプのボリューム DP がに変更されます RW リストアが成功したあとのボリューム。

## 一般的な **NDMP** テープバックアップトポロジ

NDMP は、バックアップアプリケーションと、データ（ファイルシステム）サービスおよびテープサービスを提供するストレージシステムまたはその他の NDMP サーバとの間で、複数のトポロジおよび構成をサポートします。

### ストレージシステムからローカルテープへの移動

最も単純な構成では、バックアップアプリケーションが、ストレージシステムのデータをストレージシステムに接続されたテープサブシステムにバックアップします。NDMP 制御接続はネットワーク境界を越えて機能します。ストレージシステム内で使用される、データサービスとテープサービス間の NDMP データ接続は、NDMP ローカル構成と呼ばれます。

### ストレージシステムから別のストレージシステムのテープ

バックアップアプリケーションは、あるストレージシステムのデータを、別のストレージシステムに接続されたテープライブラリ（1 つ以上のテープドライブを備えたメディアチェンジャ）にもバックアップできます。この場合、データサービスとテープサービス間の NDMP データ接続は、TCP または TCP / IPv6 ネットワーク接続によって提供されます。これを、NDMP 3 ウェイストレージシステム間構成と呼びます。

### ストレージシステムからネットワーク接続テープライブラリ

NDMP 対応のテープライブラリでは、別の種類の 3 ウェイ構成も使用できます。この場合は、テープライブラリが TCP / IP ネットワークに直接接続され、内部の NDMP サーバを通じてバックアップアプリケーションおよびストレージシステムと通信します。

### ストレージシステムからデータサーバさらにテープへ、またはデータサーバからストレージシステムさらにテープへ

NDMP ではストレージシステムからデータサーバ、およびデータサーバからストレージシステムへの 3 ウェ

イ構成もサポートされていますが、これらの構成はあまり幅広く導入されていません。ストレージシステムからサーバへの構成では、ストレージシステムのデータを、バックアップアプリケーションホストまたは別のデータサーバシステムに接続されたテープライブラリにバックアップできます。サーバからストレージシステムへの構成では、サーバのデータをストレージシステムに接続されたテープライブラリにバックアップできます。

サポートされている **NDMP** の認証方式

NDMP の接続要求を許可する認証方式を指定できます。ONTAP では、ストレージシステムへの NDMP アクセスについて、プレーンテキストおよびチャレンジの 2 種類の認証方式をサポートしています。

ノードを対象とした NDMP モードでは、チャレンジとプレーンテキストの両方がデフォルトで有効になっています。ただし、チャレンジを無効にすることはできません。プレーンテキストは有効または無効にすることができます。プレーンテキスト認証方式では、ログインパスワードがクリアテキストで送信されます。

Storage Virtual Machine (SVM) を対象とした NDMP モードでは、デフォルトの認証方式はチャレンジです。ノードを対象とした NDMP モードとは異なり、このモードでは、プレーンテキストとチャレンジの両方の認証方式を有効または無効にすることができます。

関連情報

[ノードを対象とした NDMP モードでのユーザ認証](#)

[SVM を対象とした NDMP モードでのユーザ認証](#)

**ONTAP** でサポートされる **NDMP** の拡張機能

NDMP v4 は、NDMP v4 プロトコルの中核部分を変更することなく、NDMP v4 プロトコルの機能拡張を可能にするメカニズムを備えています。ONTAP でサポートされる NDMP v4 の拡張機能を確認しておく必要があります。

ONTAP でサポートされる NDMP v4 の拡張機能は次のとおりです。

- ・ クラスタ対応バックアップ (CAB)



この拡張機能は、SVM を対象とした NDMP モードでのみサポートされます。

- ・ IPv6 のサポートのための Connection Address Extension (CAE)
- ・ 拡張クラス 0x2050

この拡張機能は、再開可能なバックアップ処理と Snapshot Management Extension をサポートします。



。NDMP\_SNAP\_RECOVER Snapshot Management Extensionsの一部であるメッセージは、リカバリ処理を開始し、リカバリされたデータをローカルSnapshotコピーからローカルファイルシステムの場所に転送するために使用されます。ONTAP では、このメッセージをボリュームと通常のファイルのリカバリのみに使用できます。

。NDMP\_SNAP\_DIR\_LIST メッセージを使用すると、ボリュームのSnapshotコピーを参照できます。参照処理の実行中にノンストップオペレーションが行われた場合、バックアップアプリケーションで参照処理を再開する必要があります。

## ONTAP でサポートされるダンプ用の NDMP Restartable Backup Extension

NDMP の Restartable Backup Extension (RBE) 機能を使用すると、障害発生前のデータストリームの既知のチェックポイントからバックアップを再開できます。

拡張 DAR 機能とは

拡張 DAR 機能は、ディレクトリ DAR、ファイルの DAR、および NT ストリームに使用できます。デフォルトでは、拡張 DAR 機能が有効になっています。

拡張 DAR 機能を有効にすると、オフセットマップを作成してテープに書き込む必要があるため、バックアップのパフォーマンスに影響を及ぼす可能性があります。ノードを対象とした NDMP モードと Storage Virtual Machine (SVM) を対象とした NDMP モードの両方で拡張 DAR を有効または無効にすることができます。

### NDMP セッションのスケーラビリティ制限

システムメモリ容量が異なるストレージシステムで同時に確立できる NDMP セッションの最大数に注意する必要があります。この最大数は、ストレージシステムのシステムメモリによって異なります。

次の表に、NDMP サーバの制限を示します。「ダンプバックアップおよびリストアセッションの計算性の制限」に記載されている制限は、ダンプおよびリストアセッションの制限です。

#### ダンプバックアップおよびリストアセッションのスケーラビリティ制限

ストレージシステムのシステムメモリ	NDMP セッションの最大数
16GB 未満	8
16GB 以上、24GB 未満	20
24GB 以上	36

を使用して、ストレージシステムのシステムメモリを取得できます `sysconfig -a` コマンド（ノードシェルから使用可能）。このコマンドの使用の詳細については、マニュアルページを参照してください。

## FlexGroup ボリュームの NDMP について

ONTAP 9.7 以降では、FlexGroup ボリュームで NDMP がサポートされます。

ONTAP 9.7 以降では、FlexVol ボリュームと FlexGroup ボリュームの間のデータ転送で `ndmpcopy` コマンドがサポートされます。

ONTAP 9.7 から以前のバージョンにリバートした場合、以前の転送の差分転送情報は保持されないため、リバート後にベースラインコピーを実行する必要があります。

ONTAP 9.8 以降では、FlexGroup ボリュームで次の NDMP 機能がサポートされます。

- 拡張クラス 0x2050 の NDMP\_SNAP\_RECOVER メッセージは、FlexGroup ボリューム内の個々のファイ

ルのリカバリに使用できます。

- FlexGroup ボリュームでは、NDMP の Restartable Backup Extension (RBE) がサポートされます。
- 環境変数 EXCLUDE および MULTI\_SUBTREE\_NAMES は、FlexGroup ボリュームでサポートされます。

## SnapLock を備えた NDMP について

規制対象データの複数のコピーを作成すると、冗長なリカバリシナリオが実現します。また、NDMP ダンプおよびリストアを使用すると、ソースファイルの Write Once Read Many (WORM) 特性を SnapLock ボリュームに保持できます。

SnapLock ボリューム内のファイルの WORM 属性は、データのバックアップ、リストア、およびコピー時に保持されますが、WORM 属性が適用されるのは SnapLock ボリュームへのリストア時のみです。SnapLock から SnapLock 以外のボリュームにバックアップをリストアした場合、WORM 属性は維持されますが無視され、ONTAP で強制されません。

## FlexVol ボリュームのノードを対象とした NDMP モードを管理します

ノードを対象とした **FlexVol** モードの管理の概要

NDMP オプションとコマンドを使用して、ノードレベルで NDMP を管理できます。NDMP オプションは、を使用して変更できます `options` コマンドを実行します。テープバックアップおよびリストア処理を実行するには、NDMP 固有のクレデンシャルを使用してストレージシステムにアクセスする必要があります。

詳細については、を参照してください `options` コマンドについては、マニュアルページを参照してください。

関連情報

[ノードを対象とした NDMP モードの管理用コマンド](#)

[ノードを対象とした NDMP モードとは](#)

ノードを対象とした **NDMP** モードの管理用コマンド

を使用できます `system services ndmp` ノードレベルで NDMP を管理するためのコマンド。これらのコマンドの一部は非推奨となっており、今後のメジャーリリースで削除される予定です。

次の NDMP コマンドは、advanced 権限レベルでのみ使用できます。

- `system services ndmp service terminate`
- `system services ndmp service start`
- `system services ndmp service stop`
- `system services ndmp log start`
- `system services ndmp log stop`

状況	使用するコマンド
NDMP サービスを有効にします	<code>system services ndmp on*</code>
NDMP サービスを無効にします	<code>system services ndmp off*</code>
NDMP設定を表示する	<code>system services ndmp show*</code>
NDMPの設定を変更する	<code>system services ndmp modify*</code>
デフォルトの NDMP バージョンを表示する	<code>system services ndmp version*</code>
NDMP サービス設定を表示します	<code>system services ndmp service show</code>
NDMP サービス設定を変更します	<code>system services ndmp service modify</code>
すべての NDMP セッションを表示する	<code>system services ndmp status</code>
すべての NDMP セッションに関する詳細情報を表示する	<code>system services ndmp probe</code>
指定された NDMP セッションを終了します	<code>system services ndmp kill</code>
すべての NDMP セッションを終了します	<code>system services ndmp kill-all</code>
NDMP パスワードを変更します	<code>system services ndmp password*</code>
ノードを対象とした NDMP モードを有効にします	<code>system services ndmp node-scope-mode on*</code>
ノードを対象とした NDMP モードを無効にします	<code>system services ndmp node-scope-mode off*</code>
ノードを対象とした NDMP モードのステータスを表示する	<code>system services ndmp node-scope-mode status*</code>
すべての NDMP セッションを強制的に終了します	<code>system services ndmp service terminate</code>
NDMP サービスデーモンを開始します	<code>system services ndmp service start</code>
NDMP サービスデーモンを停止します	<code>system services ndmp service stop</code>
指定した NDMP セッションのロギングを開始します	<code>system services ndmp log start*</code>

状況	使用するコマンド
指定した NDMP セッションのロギングを停止します	<code>system services ndmp log stop*</code>

- これらのコマンドは非推奨となっており、今後のメジャーリリースで削除される予定です。

これらのコマンドの詳細については、のマニュアルページを参照してください `system services ndmp` コマンド

ノードを対象とした **NDMP** モードでのユーザ認証

ノードを対象とした NDMP モードでは、テープによるバックアップとリストア処理を行うために、NDMP 固有のクレデンシャルを使用してストレージシステムにアクセスする必要があります。

デフォルトのユーザ ID は「root」です。ノードで NDMP を使用する前に、NDMP ユーザに関連付けられたデフォルトの NDMP パスワードを変更しておく必要があります。デフォルトの NDMP ユーザ ID を変更することもできます。

関連情報

[ノードを対象とした NDMP モードの管理用コマンド](#)

## FlexVol ボリュームの **SVM** を対象とした **NDMP** モードを管理します

**FlexVol** ボリュームの **SVM** を対象とした **NDMP** モードの概要を管理します

NDMP オプションとコマンドを使用して、SVM 単位で NDMP を管理できます。NDMP オプションは、を使用して変更できます `vserver services ndmp modify` コマンドを実行します SVM を対象とした NDMP モードでは、ユーザ認証がロールベースアクセス制御メカニズムに統合されます。

許可するプロトコルまたは許可しないプロトコルのリストに NDMP を追加するには、を使用します `vserver modify` コマンドを実行します デフォルトでは、NDMP は許可するプロトコルのリストに含まれています。許可しないプロトコルのリストに NDMP が追加されると、NDMP セッションを確立できません。

を使用して、NDMP データ接続を確立する LIF タイプを制御できます `-preferred-interface-role` オプション NDMP データ接続の確立時には、このオプションで指定した LIF タイプに属する IP アドレスが NDMP によって選択されます。IP アドレスがどの LIF タイプにも属していない場合は、NDMP データ接続を確立できません。詳細については、を参照してください `-preferred-interface-role` オプションについては、マニュアルページを参照してください。

詳細については、を参照してください `vserver services ndmp modify` コマンドについては、マニュアルページを参照してください。

関連情報

[SVM を対象とした NDMP モードを管理するためのコマンド](#)

[Cluster Aware Backup 拡張の動作](#)

"ONTAP の概念"

SVM を対象とした NDMP モードとは

"システム管理"

SVM を対象とした NDMP モードを管理するためのコマンド

を使用できます `vserver services ndmp` 各Storage Virtual Machine（SVM、旧Vserver）上でNDMPを管理するためのコマンド。

状況	使用するコマンド
NDMP サービスを有効にします	<div><div></div><div><code>vserver services ndmp on</code>  クラスタ内のすべてのノードで NDMP サービスを常に有効にする必要があります。を使用して、ノードでNDMPサービスを有効にできます <code>system services ndmp on</code> コマンドを実行しますデフォルトでは、NDMP サービスはノードで常に有効になっています。</div></div>
NDMP サービスを無効にします	<code>vserver services ndmp off</code>
NDMP設定を表示する	<code>vserver services ndmp show</code>
NDMPの設定を変更する	<code>vserver services ndmp modify</code>
デフォルトの NDMP バージョンを表示する	<code>vserver services ndmp version</code>
すべての NDMP セッションを表示する	<code>vserver services ndmp status</code>
すべての NDMP セッションに関する詳細情報を表示する	<code>vserver services ndmp probe</code>
指定された NDMP セッションを終了します	<code>vserver services ndmp kill</code>
すべての NDMP セッションを終了します	<code>vserver services ndmp kill-all</code>
NDMP パスワードを生成します	<code>vserver services ndmp generate-password</code>



状況	使用するコマンド
NDMP の拡張機能のステータスを表示します	<pre>vserver services ndmp extensions show</pre> <p>このコマンドは、advanced 権限レベルで使用できません。</p>
NDMP の拡張機能のステータスを変更（有効または無効に）します	<pre>vserver services ndmp extensions modify</pre> <p>このコマンドは、advanced 権限レベルで使用できません。</p>
指定した NDMP セッションのロギングを開始します	<pre>vserver services ndmp log start</pre> <p>このコマンドは、advanced 権限レベルで使用できません。</p>
指定した NDMP セッションのロギングを停止します	<pre>vserver services ndmp log stop</pre> <p>このコマンドは、advanced 権限レベルで使用できません。</p>

これらのコマンドの詳細については、のマニュアルページを参照してください `vserver services ndmp` コマンド

## Cluster Aware Backup 拡張の動作

Cluster Aware Backup（CAB）拡張は、NDMP v4 プロトコルの拡張です。この拡張を使用すると、NDMP サーバで、ボリュームを所有するノードでデータ接続を確立できます。また、ボリュームとテープデバイスがクラスタ内の同じノードに配置されているかどうかをバックアップアプリケーションで判断できます。

ボリュームを所有するノードを NDMP サーバで特定し、そのノードでデータ接続を確立できるようにするには、バックアップアプリケーションで CAB 拡張がサポートされている必要があります。CAB 拡張を使用する場合、バックアップアプリケーションでは、データ接続を確立する前に、バックアップまたはリストア対象のボリュームについて NDMP サーバに通知する必要があります。これにより、NDMP サーバはボリュームをホストするノードを決定して、データ接続を適切に確立できます。

バックアップアプリケーションで CAB 拡張がサポートされている場合は、ボリュームとテープデバイスに関するアフィニティ情報が NDMP サーバから提供されます。ボリュームとテープデバイスがクラスタ内の同じノードに配置されている場合、バックアップアプリケーションではこのアフィニティ情報を使用して、3 ウェイバックアップの代わりにローカルバックアップを実行できます。

異なる LIF タイプでのバックアップおよびリストアに使用できるボリュームとテープデバイス

クラスタ内のどのタイプの LIF でも NDMP 制御接続を確立するようにバックアップアプリケーションを設定できます。Storage Virtual Machine（SVM）を対象とした NDMP モードでは、このような LIF タイプと CAB 拡張のステータスに応じて、バックアップおよびリストア処理に使用できるボリュームとテープデバイスを決定できます。

次の表に、NDMP 制御接続の LIF タイプおよび CAB 拡張のステータスに応じて使用できるボリュームとテープデバイスを示します。

**CAB 拡張がバックアップアプリケーションでサポートされていない場合に使用できるボリュームとテープデバイス**

NDMP 制御接続の LIF タイプ	バックアップまたはリストアに使用できるボリューム	バックアップまたはリストアに使用できるテープデバイス
ノード管理 LIF	ノードでホストされるすべてのボリューム	ノード管理 LIF をホストしているノードに接続されているテープデバイス
データ LIF	データ LIF をホストするノードでホストされる SVM に属するボリュームのみ	なし
クラスタ管理 LIF	クラスタ管理 LIF をホストするノードでホストされるすべてのボリューム	なし
クラスタ間 LIF	クラスタ間 LIF をホストするノードでホストされるすべてのボリューム	インタークラスタ LIF をホストしているノードに接続されているテープデバイス

**CAB 拡張がバックアップアプリケーションでサポートされている場合に使用できるボリュームとテープデバイス**

NDMP 制御接続の LIF タイプ	バックアップまたはリストアに使用できるボリューム	バックアップまたはリストアに使用できるテープデバイス
ノード管理 LIF	ノードでホストされるすべてのボリューム	ノード管理 LIF をホストしているノードに接続されているテープデバイス
データ LIF	データ LIF をホストする SVM に属するすべてのボリューム	なし
クラスタ管理 LIF	クラスタ内のすべてのボリューム	クラスタ内のすべてのテープデバイス
クラスタ間 LIF	クラスタ内のすべてのボリューム	クラスタ内のすべてのテープデバイス

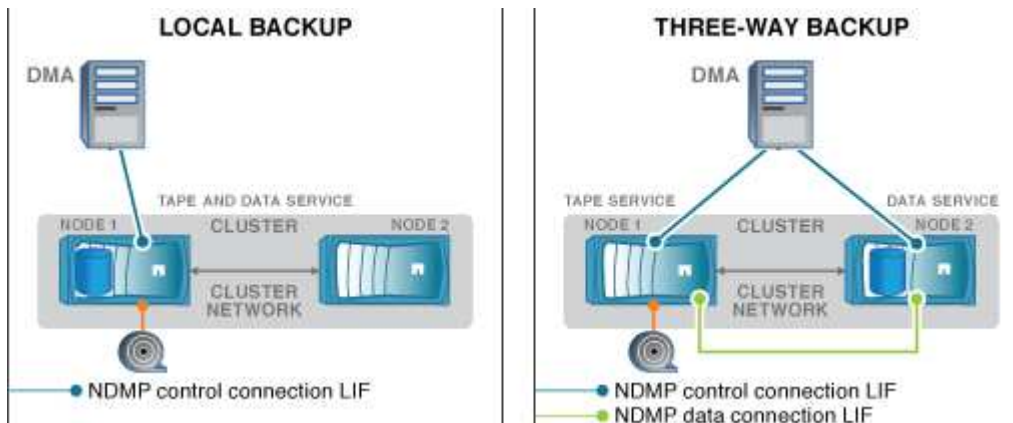
アフィニティ情報とは

CAB 対応のバックアップアプリケーションを使用すると、ボリュームとテープデバイスに関する一意の場所情報が NDMP サーバから提供されます。ボリュームとテープデバイスが同じアフィニティを共有している場合、バックアップアプリケーションではこのアフィニティ情報を使用して、3 ウェイバックアップの代わりにローカルバックアップを

実行できます。

ノード管理 LIF、クラスタ管理 LIF で NDMP 制御接続が確立されている場合は、またはクラスタ間 LIF の場合、バックアップアプリケーションではアフィニティ情報を使用してボリュームとテープデバイスが同じノードに配置されているかどうかを判断し、ローカルまたは 3 ウェイバックアップ/リストア処理を実行できます。データ LIF で NDMP 制御接続が確立されると、バックアップアプリケーションは常に 3 ウェイバックアップを実行します。

#### ローカル NDMP バックアップと 3 ウェイ NDMP バックアップ



DMA（バックアップアプリケーション）は、ボリュームとテープデバイスに関するアフィニティ情報を使用して、クラスタ内のノード 1 にあるボリュームとテープデバイスでローカル NDMP バックアップを実行します。ボリュームがノード 1 からノード 2 に移動すると、ボリュームとテープデバイスに関するアフィニティ情報が変更されます。したがって、後続のバックアップについては、DMA は 3 ウェイ NDMP バックアップ処理を実行します。これにより、ボリュームの移動先のノードに関係なく、ボリュームのバックアップポリシーが維持されます。

#### 関連情報

##### [Cluster Aware Backup 拡張の動作](#)

NDMP サーバは、**SVM** を対象としたモードでセキュアな制御接続をサポートします

セキュアソケット（SSL/TLS）を通信メカニズムとして使用することで、Data Management Application（DMA；データ管理アプリケーション）と NDMP サーバの間でセキュアな制御接続を確立できます。この SSL 通信は、サーバ証明書に基づいて行われます。NDMP サーバはポート 30000（IANA が「ndmps」サービス用に割り当てているポート）でリスンします。

このポートでクライアントから接続を確立すると、標準の SSL ハンドシェイクが開始され、サーバからクライアントに証明書が提示されます。クライアントが証明書を受け入れると、SSL ハンドシェイクが完了します。このプロセスが完了すると、クライアントとサーバの間のすべての通信が暗号化されます。NDMP プロトコルのワークフローは、それまでとまったく同じです。セキュアな NDMP 接続で必要になるのは、サーバ側の証明書の認証のみです。DMA は、セキュアな NDMP サービスまたは標準の NDMP サービスのいずれかに接続して接続を確立できます。

デフォルトでは、セキュアな NDMP サービスは Storage Virtual Machine（SVM）に対しては無効になっています。を使用して、特定の SVM でセキュアな NDMP サービスを有効または無効にできます `vserver services ndmp modify -vserver vserver -is-secure-control-connection-enabled [true|false]` コマンドを実行します

## NDMP データ接続タイプ

Storage Virtual Machine（SVM）を対象とした NDMP モードでは、サポートされる NDMP データ接続タイプは、NDMP 制御接続の LIF タイプおよび CAB 拡張のステータスによって異なります。この NDMP データ接続タイプは、ローカルまたは 3 ウェイ NDMP バックアップ / リストア処理を実行できるかどうかを示します。

TCP または TCP / IPv6 ネットワーク経由で 3 ウェイ NDMP バックアップまたはリストア処理を実行できます。次の表に、NDMP 制御接続の LIF タイプおよび CAB 拡張のステータスに基づく NDMP データ接続タイプを示します。

CAB 拡張がバックアップアプリケーションでサポートされている場合は、**NDMP データ接続タイプ**

NDMP 制御接続の LIF タイプ	NDMP データ接続タイプ
ノード管理 LIF	ローカル、TCP、TCP / IPv6
データ LIF	TCP、TCP/IPv6
クラスタ管理 LIF	ローカル、TCP、TCP / IPv6
クラスタ間 LIF	ローカル、TCP、TCP / IPv6

CAB 拡張がバックアップアプリケーションでサポートされていない場合の **NDMP データ接続タイプ**

NDMP 制御接続の LIF タイプ	NDMP データ接続タイプ
ノード管理 LIF	ローカル、TCP、TCP / IPv6
データ LIF	TCP、TCP/IPv6
クラスタ管理 LIF	TCP、TCP/IPv6
クラスタ間 LIF	ローカル、TCP、TCP / IPv6

## 関連情報

[Cluster Aware Backup 拡張の動作](#)

["Network Management の略"](#)

## SVM を対象とした NDMP モードでのユーザ認証

Storage Virtual Machine（SVM）を対象とした NDMP モードでは、NDMP ユーザ認証がロールベースアクセス制御と統合されます。SVM のコンテキストでは、NDMP ユーザには「vsadmin」または「vsadmin-backup」のいずれかのロールが必要です。クラスタのコンテキストでは 'admin' または backup のいずれかのロールが NDMP ユーザー

## に割り当てられている必要があります

これらの事前定義されたロール以外に ' カスタム・ロールに関連づけられたユーザー・アカウントを NDMP 認証に使用することもできます。ただし ' カスタム・ロールのコマンド・ディレクトリには `vserver services ndmp` フォルダがあり ' フォルダのアクセス・レベルが `none` でない場合に限られます。このモードでは、指定されたユーザアカウント用の NDMP パスワードを生成する必要があります。このパスワードは、ロールベースアクセス制御を使用して作成されます。admin ロールまたは backup ロールのクラスターユーザは、ノード管理 LIF、クラスター管理 LIF、またはインタークラスター LIF にアクセスできます。vsadmin-backup ロールまたは vsadmin ロールのユーザは、対象の SVM のデータ LIF にのみアクセスできます。そのため、ユーザのロールによって、バックアップおよびリストア処理に使用できるボリュームとテープデバイスが異なります。

このモードでは、NIS ユーザと LDAP ユーザのユーザ認証もサポートされます。そのため、NIS ユーザと LDAP ユーザは、共通のユーザ ID とパスワードを使用して複数の SVM にアクセスできます。ただし、NDMP 認証では Active Directory ユーザがサポートされません。

このモードでは、ユーザ・アカウントは SSH アプリケーションと「ユーザ・パスワード」認証方式に関連付けられている必要があります。

### 関連情報

[SVM を対象とした NDMP モードを管理するためのコマンド](#)

["システム管理"](#)

["ONTAP の概念"](#)

### NDMP ユーザ用の NDMP 固有のパスワードを生成します

Storage Virtual Machine (SVM) を対象とした NDMP モードでは、特定のユーザ ID 用のパスワードを生成する必要があります。NDMP ユーザ用の実際のログインパスワードに基づいてパスワードが生成されます。実際のログインパスワードが変更された場合は、NDMP 固有のパスワードを再度生成する必要があります。

### 手順

1. を使用します `vserver services ndmp generate-password` NDMP固有のパスワードを生成するコマンド。

このパスワードは、パスワード入力を必要とする現在または将来のすべての NDMP 処理で使用できます。



Storage Virtual Machine (SVM、旧 Vserver) のコンテキストから、その SVM にのみ属しているユーザ用の NDMP パスワードを生成できます。

次の例は、user1 という ID を持つユーザ用の NDMP 固有のパスワードを生成する方法を示しています。

```
cluster1::vserver services ndmp> generate-password -vserver vs1 -user  
user1
```

Vserver: vs1

User: user1

Password: jWZiNt57huPOoD8d

2. 通常のストレージシステムアカウントのパスワードを変更した場合は、この手順を繰り返して、新しい NDMP 固有のパスワードを取得してください。

**MetroCluster** 構成でディザスタリカバリ時にテープバックアップおよびリストア処理が受ける影響

MetroCluster 構成では、ディザスタリカバリ時にテープバックアップおよびリストア処理を同時に実行できます。ディザスタリカバリ時にこれらの処理が受ける影響について理解しておく必要があります。

ディザスタリカバリ関係にある SVM のボリュームでテープバックアップおよびリストア処理が実行される場合は、スイッチオーバーとスイッチバックのあとに増分テープバックアップおよびリストア処理を引き続き実行できます。

## FlexVol ボリュームのダンプエンジンについて

**FlexVol** ボリュームのダンプエンジンについて

ダンプは、ONTAP が提供する Snapshot コピーベースのバックアップおよびリカバリの解決策です。Snapshot コピーからテープデバイスにファイルとディレクトリをバックアップして、バックアップしたデータをストレージシステムにリストアする際に役立ちます。

ダンプバックアップを使用して、ディレクトリ、ファイル、および関連するセキュリティ設定などのファイルシステムデータをテープデバイスにバックアップできます。バックアップ対象には、ボリューム全体、qtree 全体、またはボリューム全体でも qtree 全体でもないサブツリーを指定できます。

NDMP 準拠のバックアップアプリケーションを使用して、ダンプバックアップやダンプリストアを実行できます。

ダンプバックアップを実行する際は、バックアップに使用する Snapshot コピーを指定できます。バックアップする Snapshot コピーを指定しない場合は、ダンプエンジンによってバックアップの Snapshot コピーが作成されます。バックアップ処理が完了すると、ダンプエンジンはその Snapshot コピーを削除します。

ダンプエンジンを使用して、テープへのレベル 0 バックアップ、増分バックアップ、または差分バックアップを実行できます。



Data ONTAP 8.3 よりも前のリリースにリポートした場合は、ベースラインバックアップ処理を実行してから増分バックアップ処理を実行する必要があります。

関連情報

"アップグレード、リバート、ダウングレード"

ダンプバックアップの動作

ダンプバックアップは、定義済みのプロセスに基づいて、ディスクからテープにファイルシステムのデータを書き込みます。バックアップ対象には、ボリューム、 qtree 、またはボリューム全体でも qtree 全体でもないサブツリーを指定できます。


次の表に、ダンプパスで指定されたオブジェクトについて、 ONTAP が実行するバックアッププロセスを示します。

段階	アクション
1.	フルボリュームバックアップまたはフル qtree バックアップ以外の場合、 ONTAP はディレクトリをたどってバックアップ対象のファイルを特定します。ボリューム全体または qtree 全体をバックアップする場合は、 ONTAP によってステージ 2 のプロセスが実行されます。
2.	フルボリュームバックアップまたはフル qtree バックアップの場合、 ONTAP はボリュームまたは qtree 内のバックアップ対象のディレクトリを特定します。
3.	ONTAP は、ディレクトリをテープに書き込みます。
4.	ONTAP はファイルをテープに書き込みます。
5.	ONTAP は、 ACL 情報（該当する場合）をテープに書き込みます。

ダンプバックアップは、バックアップを実行するためにデータの Snapshot コピーを使用します。したがって、バックアップを開始する前にボリュームをオフラインにする必要はありません。

ダンプバックアップでは、作成した各Snapshotコピーにという名前を付けます snapshot\_for\_backup.n、ここで n は0から始まる整数です。ダンプバックアップにより Snapshot コピーが作成されるたびに、この整数値は 1 ずつ加算されます。ストレージシステムがリブートされると、この整数値は 0 にリセットされます。バックアップ処理が完了すると、ダンプエンジンはその Snapshot コピーを削除します。

ONTAP で複数のダンプバックアップを同時に実行すると、ダンプエンジンにより複数の Snapshot コピーが作成されます。たとえば、ONTAP で2つのダンプバックアップを同時に実行すると、データのバックアップ元のボリューム内には次のSnapshotコピーが作成されます。 snapshot\_for\_backup.0 および snapshot\_for\_backup.1。



Snapshot コピーからバックアップする場合は、ダンプエンジンによって新たに Snapshot コピーが作成されることはありません。

ダンプエンジンでバックアップされるデータの種類

ダンプエンジンを使用すると、データをテープにバックアップして災害やコントローラの停止から保護できます。ダンプエンジンでは、ファイル、ディレクトリ、 qtree 、ボ



リユーム全体などのデータオブジェクトだけでなく、各ファイルに関するさまざまな種類の情報もバックアップできます。ダンプエンジンでバックアップできるデータの種類の考慮すべき制限を理解しておく、ディザスタリカバリのアプローチを計画する際に役立ちます。

ダンプエンジンでは、ファイルのデータをバックアップするだけでなく、必要に応じて、各ファイルに関する次の情報もバックアップできます。

- UNIX GID、所有者の UID、およびファイルのアクセス権
- UNIX のアクセス時間、作成時間、および変更時間
- ファイルタイプ
- ファイルサイズ
- DOS 名、DOS 属性、および作成時間
- 1、024 個の Access Control Entry（ACE；アクセス制御エントリ）を含む ACL
- qtree 情報
- ジャンクションパス

ジャンクションパスはシンボリックリンクとしてバックアップされます。

- LUN クローンおよび LUN クローン

LUN オブジェクト全体をバックアップできますが、LUN オブジェクト内の個別のファイルをバックアップすることはできません。同様に、LUN オブジェクト全体をリストアできますが、LUN オブジェクト内の個別のファイルをリストアすることはできません。



ダンプエンジンでバックアップした LUN クローンは、独立した LUN になります。

- VM-aligned ファイル

Data ONTAP 8.1.2 より前のリリースでは、VM-aligned ファイルのバックアップはサポートされていません。



Snapshot でバックアップされた LUN クローンを Data ONTAP 7-Mode から ONTAP に移行した場合、一貫性のない LUN になります。ダンプエンジンでは、一貫性のない LUN はバックアップされません。

データをボリュームにリストアする場合は、リストア対象の LUN でクライアント I/O が制限されます。LUN に関するこの制限が解除されるのは、ダンプリストア処理が完了した場合のみです。同様に、SnapMirror による単一ファイルまたは LUN のリストア処理中は、リストア対象のファイルと LUN でクライアント I/O が制限されます。この制限が解除されるのは、単一ファイル / LUN のリストア処理が完了した場合のみです。ダンプリストアまたは SnapMirror による単一ファイルまたは LUN のリストア処理を実行中のボリュームでダンプバックアップが実行される場合は、クライアント I/O が制限されているファイルまたは LUN がバックアップに含まれません。クライアント I/O の制限が解除されると、これらのファイルまたは LUN は後続のバックアップ処理に含まれます。





Data ONTAP 8.3 で実行されているテープにバックアップした LUN は、8.3 以降のリリースにのみリストアできます。8.3 より前のリリースにはリストアできません。以前のリリースに LUN をリストアする場合、その LUN はファイルとしてリストアされます。

SnapVault セカンダリボリュームまたは Volume SnapMirror デスティネーションをテープにバックアップする場合は、ボリュームのデータだけがバックアップされます。関連付けられているメタデータはバックアップされません。したがって、ボリュームをリストアしようとすると、そのボリュームのデータだけがリストアされます。Volume SnapMirror 関係に関する情報はバックアップで使えないため、リストアされません。

Windows NT のアクセス権しかないファイルをダンプし、UNIX 形式の qtree またはボリュームにリストアした場合、リストアされたファイルには、その qtree またはボリュームに対する UNIX のデフォルトのアクセス権が付与されます。

UNIX のアクセス権しかないファイルをダンプし、NTFS 形式の qtree またはボリュームにリストアした場合、リストアされたファイルには、その qtree またはボリュームに対する Windows のデフォルトのアクセス権が付与されます。

それ以外の場合は、ダンプとリストア後もアクセス権は維持

VM-aligned ファイルおよびをバックアップできます `vm-align-sector` オプション VM-aligned ファイルの詳細については、を参照してください ["論理ストレージ管理"](#)。

漸増チェーンとは

漸増チェーンとは、同じパスに対する一連の増分バックアップです。任意の時点で任意のレベルのバックアップを指定できるため、バックアップとリストアを効率的に実行するには、漸増チェーンについて理解しておく必要があります。31 レベルの増分バックアップ処理を実行できます。

漸増チェーンには次の 2 種類があります。

- 連続的漸増チェーンは、レベル 0 から始まり、1 ずつ増えていく連続した増分バックアップです。
- 非連続的漸増チェーンは、増分バックアップの各回でレベルがスキップされていたり、連続していないもの（0、2、3、1 など）です。4、またはそれ以上の一般的な 0、1、1、1 または 0、1、2、1、2。

増分バックアップでは、よりレベルが低い最新のバックアップがベースとして使用されます。たとえば、0、2、3、1、4 という一連のバックアップレベルには、「0、2、3」と「0、1、4」の 2 つの漸増チェーンがあります。次の表に、増分バックアップのベースを示します。

バックアップ順序	増分レベル	漸増チェーン	ベース（ <b>Base</b> ）	バックアップされるファイル
1.	0	両方	ストレージ・システム上のファイル	バックアップパスのすべてのファイル
2.	2.	0、2、3	レベル 0 バックアップ	レベル 0 バックアップ以降に作成されたバックアップパスのファイル

バックアップ順序	増分レベル	漸増チェーン	ベース（ <b>Base</b> ）	バックアップされるファイル
3.	3.	0、2、3	レベル 2 バックアップ	レベル 2 バックアップ以降に作成されたバックアップパスのファイル
4.	1.	0.1.4	レベル 0 バックアップです。レベル 1 バックアップよりも下位の最新レベルです	レベル 0 バックアップ以降に作成されたバックアップ・パス内のファイル（レベル 2 およびレベル 3 バックアップ内のファイルを含む）
5.	4.	0.1.4	レベル 1 バックアップは下位レベルであり、レベル 0、レベル 2、またはレベル 3 バックアップよりも新しいため、レベル 1 バックアップです	レベル 1 バックアップ以降に作成されたファイル

ブロック化因数とは

テープブロックは 1、024 バイトのデータから構成されています。テープバックアップまたはリストア中には、各読み取り / 書き込み処理で転送するテープブロックの数を指定できます。この数を「ブロック化因数」と呼びます。

4~256 のブロック化因数を使用できます。バックアップのリストア先のシステムがバックアップ元と異なる場合は、バックアップで使用したブロック化因数がリストア先のシステムでサポートされている必要があります。たとえば、ブロック化因数を 128 としてバックアップをリストアする場合、リストア先のシステムでは、ブロック化因数として 128 をサポートしている必要があります。

NDMP バックアップでは、ブロック化因数は `MOVER_RECORD_SIZE` によって決定されます。ONTAP は、`MOVER_RECORD_SIZE` の最大値として、256KB をサポートしています。

ダンプバックアップを再開するタイミング

テープ書き込みエラー、停電、ユーザによる誤った操作、ストレージシステム内部の不整合など、内外のさまざまなエラーが原因で、ダンプバックアップが完了しないことがあります。これらのいずれかの理由でバックアップに失敗した場合に、バックアップを再開できます。

ストレージシステム上のトラフィックが大量に発生する時間を避けるため、またはテープドライブなどのストレージシステム上の限られたリソース間の競合を回避するために、バックアップを中断して再開することができます。より緊急性の高いリストア（またはバックアップ）で同じテープドライブが必要な場合は、長いバックアップを中断してあとで再開できます。再開可能なバックアップはリブート後も維持されます。中止された

テープへのバックアップは、次の条件に該当する場合にのみ再開できます。

- 中止されたバックアップがフェーズ 4 である
- dump コマンドでロックされた関連する Snapshot コピーがすべて使用可能である。
- ファイル履歴が有効になっている必要があります。

このようなダンプ処理が中止され、再開可能な状態のままになると、関連付けられている Snapshot コピーがロックされます。これらの Snapshot コピーは、バックアップ・コンテキストが削除されるまで解放されません。を使用して、バックアップコンテキストのリストを表示できます `vserver services ndmp restartable backup show` コマンドを実行します

```
cluster::> vserver services ndmpd restartable-backup show
Vserver      Context Identifier      Is Cleanup Pending?
-----
vserver1 330e6739-0179-11e6-a299-005056bb4bc9 false
vserver1 481025c1-0179-11e6-a299-005056bb4bc9 false
vserver2 5cf10132-0179-11e6-a299-005056bb4bc9 false
3 entries were displayed.

cluster::> vserver services ndmpd restartable-backup show -vserver
vserver1 -context-id 330e6739-0179-11e6-a299-005056bb4bc9

Vserver: vserver1
Context Identifier: 330e6739-0179-11e6-a299-005056bb4bc9
Volume Name: /vserver1/vol1
Is Cleanup Pending?: false
Backup Engine Type: dump
Is Snapshot Copy Auto-created?: true
Dump Path: /vol/vol1
Incremental Backup Level ID: 0
Dump Name: /vserver1/vol1
Context Last Updated Time: 1460624875
Has Offset Map?: true
Offset Verify: true
Is Context Restartable?: true
Is Context Busy?: false
Restart Pass: 4
Status of Backup: 2
Snapshot Copy Name: snapshot_for_backup.1
State of the Context: 7

cluster::>"
```

## ダンプリストアの動作

ダンプリストアは、定義済みのプロセスに基づいてテープからディスクにファイルシステムのデータを書き込みます。

次の表に、ダンプリストアの動作を示します。

段階	アクション
1.	ONTAP により、テープから抽出する必要があるファイルがカタログ化されます。
2.	ONTAP は、ディレクトリと空のファイルを作成します。
3.	ONTAP は、テープからファイルを読み取り、ディスクに書き込み、ACL などのアクセス権を設定します。
4.	指定したファイルがテープからすべて複製されるまで、ONTAP はステージ 2 と 3 を繰り返します。

## ダンプエンジンでリストアされるデータの種類

災害が発生したりコントローラが停止した場合、ダンプエンジンでは、単一ファイルからファイル属性やディレクトリ全体まで、バックアップしたすべてのデータをさまざまな方法でリカバリできます。ダンプエンジンでリストアできるデータの種類と使用するリカバリ方法を理解しておく、ダウンタイムを最小限に抑えるのに役立ちます。

マッピングされたオンラインの LUN にデータをリストアできます。ただし、リストア処理が完了するまで、ホストアプリケーションはこの LUN にアクセスできません。リストア処理が完了したら、LUN データのホストキャッシュをフラッシュして、リストアされたデータとの一貫性を確保する必要があります。

ダンプエンジンでは、次のデータをリカバリできます。

- ファイルおよびディレクトリの内容
- UNIX ファイルアクセス権
- ACL

UNIX ファイルアクセス権だけを持つファイルを NTFS の qtree またはボリュームにリストアした場合、そのファイルには Windows NT ACL が含まれません。対象のファイルについて Windows NT ACL を作成しないかぎり、ストレージシステムではこのファイルに対して UNIX ファイルアクセス権だけを使用します。



Data ONTAP 8.2 を実行するストレージシステムから、Data ONTAP 8.1.x 以前を実行するストレージシステムに ACE の最大数が 1、024 より小さい ACL をリストアした場合、デフォルトの ACL がリストアされます。

- qtree 情報

qtree 情報は、qtree がボリュームのルートにリストアされる場合にのみ使用されます。などの下位のデ

ィレクトリにqtreeをリストアする場合、qtree情報は使用されません /vs1/vol1/subdir/lowerdir、qtreeではなくなります。

- その他のすべてのファイルおよびディレクトリ属性
- Windows NT ストリーム
- LUN
  - LUN としての機能を維持するには、LUN をボリュームレベルまたは qtree レベルでリストアする必要があります。

ディレクトリにリストアすると、有効なメタデータが含まれないため、ファイルとしてリストアされます。

- 7-Mode LUN は、ONTAP ボリュームで LUN としてリストアされます。
- 7-Mode ボリュームは、ONTAP ボリュームにリストアできます。
- デスティネーションボリュームにリストアされた VM-aligned ファイルは、デスティネーションボリュームの VM-align のプロパティを継承します。
- リストア処理のデスティネーションボリュームに、強制ロックまたは助言ロックが設定されたファイルが含まれていることがあります。

そのようなデスティネーションボリュームへのリストア処理を実行する場合、ダンプエンジンはそれらのロックを無視します。

#### データをリストアする際の考慮事項

バックアップされたデータを元のパスまたは別の場所にリストアできます。バックアップされたデータを別の場所にリストアする場合は、リストア先を準備しておく必要があります。

データを元のパスまたは別の場所にリストアするには、次の情報を入手しておく必要があります。また、次の要件を満たす必要があります。

- リストアのレベル
- データのリストア先のパス
- バックアップ時に使用されたブロック化因数
- 増分リストアを実行する場合は、すべてのテープがバックアップチェーンに含まれている必要があります
- リストア元のテープと互換性がある、使用可能なテープドライブ

データを別の場所にリストアするには、次の処理を実行する必要があります。

- ボリュームをリストアする場合は、新しいボリュームを作成する必要があります。
- qtree またはディレクトリをリストアする場合は、リストアするファイルと名前が同一と思われるファイルについて、名前を変更するか場所を移動します。



ONTAP 9 では、qtree 名で Unicode 形式がサポートされます。以前のリリースの ONTAP では、この形式はサポートされていません。ONTAP 9でUnicode名を持つqtreeをを使用して以前のリリースのONTAP にコピーした場合 ndmcopy コマンドまたはテープのバックアップイメージからのリストアによって、qtreeはUnicode形式のqtreeではなく、通常のディレクトリとしてリストアされます。



リストアされたファイルの名前が既存のファイルと同じである場合、既存のファイルはリストアされたファイルで上書きされます。ただし、ディレクトリは上書きされません。

DARを使用せずにリストア時にファイル、ディレクトリ、またはqtreeの名前を変更するには、EXTRACT環境変数をに設定する必要があります E。

デスティネーションストレージシステムに必要なスペース

リストア先のストレージシステムには、リストアするデータのサイズに約 100MB を加えたサイズのスペースが必要です。



リストア処理の開始時には、デスティネーションボリュームで使用可能なボリュームスペースと inode が確認されます。FORCE環境変数をに設定します Y デスティネーションパスで使用可能なボリュームスペースとinodeのチェックがリストア処理でスキップされます。デスティネーションボリュームのボリュームスペースまたは inode が不足している場合は、デスティネーションボリュームで使用可能なボリュームスペースと inode で許容される量のデータがリストア処理によってリカバリされます。ボリュームスペースと inode を使用できなくなると、リストア処理が停止します。

ダンプバックアップおよびリストアセッションのスケーラビリティ制限

システムメモリ容量が異なるストレージシステムで同時に実行できるダンプバックアップおよびリストアセッションの最大数に注意する必要があります。この最大数は、ストレージシステムのシステムメモリによって異なります。

次の表に、ダンプまたはリストアエンジンの制限を示します。「NDMP セッションのスケーラビリティ制限」に記載されている制限は、NDMP サーバの制限であり、エンジンの制限よりも高くなります。

ストレージシステムのシステムメモリ	ダンプバックアップおよびリストアセッションの総数
16GB 未満	4.
16GB 以上、24GB 未満	16
24GB 以上	32だ



を使用する場合 ndmcopy ストレージシステム内のデータをコピーするコマンドでは、ダンプバックアップ用とダンプリストア用の2つのNDMPセッションが確立されます。

を使用して、ストレージシステムのシステムメモリを取得できます sysconfig -a コマンド（ノードシェルから使用可能）。このコマンドの使用の詳細については、マニュアルページを参照してください。

**Data ONTAP 7-Mode と ONTAP** 間でのテープバックアップおよびリストアがサポートされます

7-Mode または ONTAP を実行しているストレージシステムからバックアップしたデータを、7-Mode または ONTAP を実行しているストレージシステムにリストアできます。

Data ONTAP 7-Mode と ONTAP 間では、次のテープバックアップおよびリストア処理がサポートされています。

- ONTAP を実行しているストレージシステムに接続されているテープドライブへの 7-Mode ボリュームのバックアップ
- 7-Mode システムに接続されているテープドライブへの ONTAP ボリュームのバックアップ
- ONTAP を実行しているストレージシステムに接続されているテープドライブからの 7-Mode ボリュームのバックアップデータのリストア
- 7-Mode システムに接続されているテープドライブからの ONTAP ボリュームのバックアップデータのリストア
- ONTAP ボリュームへの 7-Mode ボリュームのリストア



- A 7-Mode LUN is restored as a LUN on an ONTAP volume.
- You should retain the ONTAP LUN identifiers when restoring a 7-Mode LUN to an existing ONTAP LUN.

- ONTAP ボリュームの 7-Mode ボリュームへのリストア



ONTAP LUN は、7-Mode ボリューム上の通常のファイルとしてリストアされます。

再開可能なコンテキストを削除します

コンテキストを再開せずにバックアップを開始する場合は、コンテキストを削除できます。

このタスクについて

を使用して、再開可能なコンテキストを削除できます `vserver services ndmp restartable-backup delete` コマンドを実行します。SVM名とコンテキストIDを指定します。

手順

1. 再開可能なコンテキストを削除します。

```
vserver services ndmp restartable-backup delete -vserver vserver-name -context -id context_identifier。
```

```

cluster::> vservice ndmp restartable-backup show
Vserver      Context Identifier      Is Cleanup Pending?
-----
vserver1     330e6739-0179-11e6-a299-005056bb4bc9 false
vserver1     481025c1-0179-11e6-a299-005056bb4bc9 false
vserver2     5cf10132-0179-11e6-a299-005056bb4bc9 false
3 entries were displayed.

cluster::>
cluster::> vservice ndmp restartable-backup delete -vserver
vserver1 -context-id 481025c1-0179-11e6-a299-005056bb4bc9

cluster::> vservice ndmp restartable-backup show
Vserver      Context Identifier      Is Cleanup Pending?
-----
vserver1     330e6739-0179-11e6-a299-005056bb4bc9 false
vserver2     5cf10132-0179-11e6-a299-005056bb4bc9 false
3 entries were displayed.

cluster::>"

```

## SnapVault セカンダリボリュームでのダンプの動作

SnapVault セカンダリボリュームでミラーリングされたデータに対してテープバックアップ処理を実行できます。バックアップできるのは、SnapVault セカンダリボリュームでテープにミラーリングされたデータのみです。SnapVault 関係のメタデータはバックアップできません。

データ保護ミラー関係を解除したとき (snapmirror break) または、SnapMirrorの再同期が発生した場合は、必ずベースラインバックアップを実行する必要があります。

## ダンプとストレージフェイルオーバーおよび ARL 処理との連携

ダンプバックアップまたはリストア処理を実行するには、これらの処理とストレージフェイルオーバー（テイクオーバーとギブバック）または Aggregate Relocation（ARL；アグリゲートの再配置）処理との連携について理解しておく必要があります。。

-override-vetoes オプションは、ストレージフェイルオーバーまたはARL処理時のダンプエンジンの動作を指定します。

ダンプバックアップまたはリストア処理の実行中および -override-vetoes オプションはに設定されています false` ユーザが開始したストレージフェイルオーバーまたはARL処理が停止した場合。ただし、の場合`-override-vetoes オプションはに設定されています`true`をクリックすると、ストレージフェイルオーバーまたはARL処理が継続され、ダンプバックアップまたはリストア処理が中止されます。ストレージフェイルオーバーまたはARL処理がストレージシステムによって自動的に開始されると、アクティブなダンプバックアップまたはリストア処理が常に中止されます。ストレージフェイルオーバーまたはARL処理が完了しても、ダンプバックアップおよびリストア処理を再開することはできません。



## CAB 拡張がサポートされている場合のダンプ処理

バックアップアプリケーションで CAB 拡張がサポートされている場合は、ストレージフェイルオーバーまたは ARL 処理のあとにバックアップポリシーを再設定しなくても、増分ダンプバックアップおよびリストア処理を引き続き実行できます。

## CAB 拡張がサポートされていない場合のダンプ処理

バックアップアプリケーションで CAB 拡張がサポートされていない場合は、バックアップポリシーで設定された LIF を、デスティネーションアグリゲートをホストするノードに移行すれば、増分ダンプバックアップおよびリストア処理を引き続き実行できます。それ以外の場合は、ストレージフェイルオーバーおよび ARL 処理のあとにベースラインバックアップを実行してから増分バックアップ処理を実行する必要があります。



ストレージフェイルオーバー処理の場合は、バックアップポリシーで設定された LIF をパートナーノードに移行する必要があります。

## 関連情報

["ONTAP の概念"](#)

["高可用性"](#)

## ダンプとボリューム移動との連携

テープバックアップおよびリストア処理とボリューム移動は、ストレージシステムが最終的なカットオーバーフェーズを試行するまで並行して実行できます。最終フェーズのあとは、移動するボリュームで新しいテープバックアップおよびリストア処理を実行することはできません。ただし、現在の処理は完了するまで引き続き実行されます。

次の表に、ボリューム移動処理後のテープバックアップおよびリストア処理の動作を示します。

テープバックアップおよびリストア処理を実行する場合のモード	作業
Storage Virtual Machine (SVM) を対象とした NDMP モード (CAB 拡張がバックアップアプリケーションでサポートされている場合)	バックアップポリシーを再設定しなくても、読み取り / 書き込みボリュームおよび読み取り専用ボリュームで増分テープバックアップおよびリストア処理を引き続き実行できます。
SVM を対象とした NDMP モード (CAB 拡張がバックアップアプリケーションでサポートされていない場合)	バックアップポリシーで設定された LIF を、デスティネーションアグリゲートをホストするノードに移行する場合は、読み取り / 書き込みボリュームおよび読み取り専用ボリュームで増分テープバックアップおよびリストア処理を引き続き実行できます。それ以外の場合は、ボリューム移動後にベースラインバックアップを実行してから増分バックアップ処理を実行する必要があります。



ボリュームを移動する場合に、デスティネーションノード上の別の SVM に属しているボリュームの名前が移動対象のボリュームの名前と同じであると、移動対象のボリュームの増分バックアップ処理を実行できません。

### FlexVol ボリュームがフルの状態でのダンプの動作

増分ダンプバックアップ処理を実行する前に、FlexVol ボリュームに十分な空きスペースを確保する必要があります。

処理に失敗した場合は、サイズを拡張するか Snapshot コピーを削除して、FlexVol の空きスペースを増やす必要があります。次に、増分バックアップ処理を再度実行します。

### ボリュームのアクセスタイプが変更された場合のダンプの動作

SnapMirror デスティネーションボリュームまたは SnapVault セカンダリボリュームの状態が読み取り / 書き込みから読み取り専用、または読み取り専用から読み取り / 書き込みに変わるときは、ベースラインテープバックアップまたはリストア処理を実行する必要があります。

SnapMirror デスティネーションボリュームと SnapVault セカンダリボリュームは読み取り専用ボリュームです。それらのボリュームでテープバックアップおよびリストア処理を実行する場合は、ボリュームの状態が読み取り専用から読み取り / 書き込み、または読み取り / 書き込みから読み取り専用に変わるたびに、ベースラインバックアップまたはリストア処理を実行する必要があります。

### ダンプと SnapMirror による単一ファイルまたは LUN のリストアとの連携

SnapMirror テクノロジによる単一ファイルまたは LUN のリストア先のボリュームでダンプバックアップまたはリストア処理を実行するには、ダンプ処理と単一ファイルまたは LUN のリストア処理との連携について理解しておく必要があります。

SnapMirror による単一ファイルまたは LUN のリストア処理中は、リストア対象のファイルまたは LUN でクライアント I/O が制限されます。単一ファイル / LUN のリストア処理が終了すると、ファイルまたは LUN における I/O の制限が解除されます。単一ファイルまたは LUN のリストア先のボリュームでダンプバックアップが実行される場合は、クライアント I/O が制限されているファイルまたは LUN がダンプバックアップに含まれません。後続のバックアップ処理では、I/O の制限が解除されたあとに、このファイルまたは LUN がテープにバックアップされます。

ダンプリストアと SnapMirror による単一ファイルまたは LUN のリストア処理を同じボリュームで同時に実行することはできません。

### MetroCluster 構成でダンプバックアップおよびリストア処理が受ける影響

MetroCluster 構成でダンプバックアップおよびリストア処理を実行するには、スイッチオーバー処理またはスイッチバック処理の実行時にダンプ処理が受ける影響について理解しておく必要があります。

ダンプバックアップまたはリストア処理のあとにスイッチオーバーが行われる場合

クラスタ 1 とクラスタ 2 の 2 つのクラスタがあるとします。クラスタ 1 でダンプバックアップまたはリストア処理を実行しているときに、クラスタ 1 からクラスタ 2 へのスイッチオーバーが開始されると、次のような結果になります。

- の値の場合 `override-vetoes` オプションはです `false` をクリックすると、スイッチオーバーが中止され、バックアップまたはリストア処理が継続されます。
- オプションの値がの場合 `true` をクリックすると、ダンプバックアップまたはリストア処理が中止され、スイッチオーバーが継続されます。

ダンプバックアップまたはリストア処理のあとにスイッチバックが行われる場合

クラスタ 1 からクラスタ 2 へのスイッチオーバーが実行され、クラスタ 2 でダンプバックアップまたはリストア処理が開始されます。クラスタ 2 にあるボリュームがダンプ処理によってバックアップまたはリストアされます。この時点で、クラスタ 2 からクラスタ 1 へのスイッチバックが開始されると、次のような結果になります。

- の値の場合 `override-vetoes` オプションはです `false` をクリックすると、スイッチバックがキャンセルされ、バックアップまたはリストア処理が継続されます。
- オプションの値がの場合 `true` をクリックすると、バックアップまたはリストア処理が中止され、スイッチバックが継続されます。

スイッチオーバーまたはスイッチバックの実行中にダンプバックアップまたはリストア処理が開始された場合

クラスタ 1 からクラスタ 2 へのスイッチオーバーの実行中に、クラスタ 1 でダンプバックアップまたはリストア処理が開始されると、そのバックアップまたはリストア処理は失敗し、スイッチオーバーが継続されます。

クラスタ 2 からクラスタ 1 へのスイッチバックの実行中に、クラスタ 2 でダンプバックアップまたはリストア処理が開始されると、そのバックアップまたはリストア処理は失敗し、スイッチバックが継続されます。

## FlexVol 用の SMTape エンジンについて

### FlexVol 用の SMTape エンジンについて

SMTape は、データのブロックをテープにバックアップする、ONTAP のディザスタリカバリ解決策です。SMTape を使用すると、テープへのボリュームのバックアップを実行できます。ただし、バックアップを `qtree` レベルまたはサブツリーレベルで実行することはできません。SMTape でサポートされるのは、ベースラインバックアップ、差分バックアップ、および増分バックアップです。SMTape の場合、ライセンスは必要ありません。

NDMP 準拠のバックアップアプリケーションを使用して、SMTape バックアップおよびリストア処理を実行できます。Storage Virtual Machine (SVM) を対象とした NDMP モードでのみバックアップおよびリストア処理を実行する SMTape を選択できます。



SMTape バックアップまたはリストアセッションを実行中のリポートプロセスはサポートされていません。セッションが終了するまで待機するか、NDMP セッションを中止する必要があります。

SMTape を使用すると、255 個の Snapshot コピーをバックアップできます。以降のベースラインバックアップ、増分バックアップ、または差分バックアップでは、バックアップされた古い Snapshot コピーを削除する必要があります。

ベースラインリストアを実行する前に、データのリストア先のボリュームのタイプが必要があります DP また、このボリュームは制限状態である必要があります。リストアが成功すると、このボリュームは自動的にオンラインになります。このボリュームでは、バックアップの実行順序に従って以降の増分リストアまたは差分リストアを実行できます。

**SMTape** バックアップ時に **Snapshot** コピーを使用します

SMTape のベースラインバックアップおよび増分バックアップの際の Snapshot コピーの使用方法を理解しておく必要があります。また、SMTape を使用してバックアップを実行する場合の考慮事項もいくつかあります。

#### ベースラインバックアップ

ベースラインバックアップを実行する際は、テープにバックアップする Snapshot コピーの名前を指定できます。Snapshot コピーを指定しない場合は、ボリュームのアクセスタイプ（読み取り / 書き込みまたは読み取り専用）に応じて、Snapshot コピーが自動的に作成されるか、または既存の Snapshot コピーが使用されます。バックアップする Snapshot コピーを指定すると、指定した Snapshot コピーよりも古いすべての Snapshot コピーもテープにバックアップされます。

バックアップする Snapshot コピーを指定しない場合、次のような処理が行われます。

- 読み取り / 書き込みボリュームの場合は、Snapshot コピーが自動的に作成されます。

新たに作成された Snapshot コピーとすべての古い Snapshot コピーがテープにバックアップされます。

- 読み取り専用ボリュームの場合は、最新の Snapshot コピーを含むすべての Snapshot コピーがテープにバックアップされます。

バックアップの開始後に作成された新しい Snapshot コピーはバックアップされません。

#### 差分バックアップ

SMTape の増分または差分バックアップ処理では、NDMP 準拠のバックアップアプリケーションによって Snapshot コピーが作成および管理されます。

増分バックアップ処理を実行する場合は、Snapshot コピーを必ず指定する必要があります。増分バックアップ処理を成功させるには、以前のバックアップ処理（ベースラインまたは増分）でバックアップされた Snapshot コピーが、バックアップの実行元のボリュームに格納されている必要があります。バックアップされたこの Snapshot コピーを確実に使用するには、バックアップポリシーの設定時に、このボリュームに割り当てられている Snapshot ポリシーを考慮する必要があります。

**SnapMirror** デスティネーションでの **SMTape** バックアップに関する考慮事項

- レプリケーション用のデスティネーションボリュームには、データ保護ミラー関係によって一時的な Snapshot コピーが作成されます。

これらの Snapshot コピーを SMTape バックアップに使用しないでください。

- データ保護ミラー関係が確立されたデスティネーションボリュームで SMTape バックアップ処理が実行されているときに、同じボリュームで SnapMirror 更新が発生する場合は、SMTape でバックアップされる Snapshot コピーをソースボリュームで削除しないでください。

バックアップ処理中に、SMTape はデスティネーションボリューム上の Snapshot コピーをロックします。対応する Snapshot コピーがソースボリュームで削除されると、後続の SnapMirror 更新処理は失敗します。

- 増分バックアップでは、これらの Snapshot コピーを使用しないでください。

## SMTape の機能

Snapshot コピーのバックアップ、増分バックアップと差分バックアップ、リストアしたボリュームでの重複排除と圧縮機能の保持、テープシーディングなどの SMTape 機能を使用すると、テープのバックアップ処理とリストア処理を最適化できます。

SMTape には次の機能があります。

- ディザスタリカバリ解決策を提供します
- 増分バックアップと差分バックアップをイネーブルにします
- Snapshot コピーをバックアップします
- 重複排除ボリュームのバックアップとリストアを有効にして、リストアしたボリュームで重複排除機能を維持します
- 圧縮ボリュームをバックアップして、リストアしたボリュームで圧縮機能を維持します
- テープシーディングを有効にします

SMTape では、4~256KB の範囲で、4KB の倍数単位でブロック化因数をサポートします。



データをリストアできるのは、ONTAP の 2 つあとのメジャーリリースで作成したボリュームまでです。

## SMTape でサポートされない機能

SMTape では、再開可能なバックアップとバックアップファイルの検証はサポートされていません。

## SMTape バックアップおよびリストアセッションのスケーラビリティ制限

NDMP または CLI を使用した SMTape バックアップおよびリストア処理（テープシーディング）の実行中は、システムメモリ容量が異なるストレージシステムで同時に実行できる SMTape バックアップおよびリストアセッションの最大数に注意する必要があります。この最大数は、ストレージシステムのシステムメモリによって異なります。



SMTape バックアップおよびリストアセッションのスケーラビリティ制限は、NDMP セッションの制限やダンプセッションの制限とは異なります。

ストレージシステムのシステムメモリ	<b>SM Tape</b> バックアップおよびリストアセッションの総数
16GB 未満	6.
16GB 以上、24GB 未満	16
24GB 以上	32だ

を使用して、ストレージシステムのシステムメモリを取得できます `sysconfig -a` コマンド（ノードシェルから使用可能）。このコマンドの使用の詳細については、マニュアルページを参照してください。

## 関連情報

[NDMP セッションのスケーラビリティ制限](#)

[ダンプバックアップおよびリストアセッションのスケーラビリティ制限](#)

## テープシーディングとは

テープシーディングは、データ保護ミラー関係が確立されたデスティネーション FlexVol ボリュームの初期化に役立つ SM Tape 機能です。

テープシーディングを使用すると、ソースシステムとデスティネーションシステムの間で、低帯域幅接続を介してデータ保護ミラー関係を確立できます。

ソースからデスティネーションへの Snapshot コピーの増分ミラーリングは、低帯域幅接続上でも可能です。ただし、低帯域幅接続上では、基礎となる Snapshot コピーの最初のミラーリングに時間がかかります。このような場合、テープへのソースボリュームの SM Tape バックアップを実行し、テープを使用して最初のベース Snapshot コピーをデスティネーションに転送することができます。その後、低帯域幅接続を使用して、デスティネーションシステムへの SnapMirror の差分更新を設定できます。

## 関連情報

["ONTAP の概念"](#)

## SM Tape とストレージフェイルオーバーおよび ARL 処理との連携

SM Tape バックアップまたはリストア処理を実行するには、これらの処理とストレージフェイルオーバー（テイクオーバーとギブバック）または Aggregate Relocation（ARL；アグリゲートの再配置）処理との連携について理解しておく必要があります。。

`-override-vetoes` オプションは、ストレージフェイルオーバーまたは ARL 処理時の SM Tape エンジンの動作を指定します。

SM Tape バックアップまたはリストア処理の実行中、および `-override-vetoes` オプションはに設定されています `false` ユーザが開始したストレージフェイルオーバーまたは ARL 処理が停止し、バックアップまたはリストア処理が完了した場合。バックアップアプリケーションで CAB 拡張がサポートされている場合は、バックアップポリシーを再設定しなくても、増分 SM Tape バックアップおよびリストア処理を引き続き実行できます。ただし、の場合 `-override-vetoes` オプションはに設定されています `true` その後、ストレージフェイルオーバーまたは ARL 処理が続行され、SM Tape バックアップまたはリストア処理が中止されます。



## **SMTape とボリューム移動との連携**

SMTape バックアップ処理とボリューム移動処理は、ストレージシステムが最終カットオーバーフェーズを試行するまで並行して実行できます。最終フェーズのあとは、移動するボリュームで新しい SMTape バックアップ処理を実行することはできません。ただし、現在の処理は完了するまで引き続き実行されます。

ボリューム移動処理では、ボリュームのカットオーバーフェーズを開始する前に、同じボリュームでアクティブな SMTape バックアップ処理を確認します。アクティブな SMTape バックアップ処理がある場合、ボリューム移動処理はカットオーバー保留状態になり、SMTape バックアップ処理を完了できます。これらのバックアップ処理が完了したら、ボリューム移動処理を手動で再開する必要があります。

バックアップアプリケーションで CAB 拡張がサポートされている場合は、バックアップポリシーを再設定しなくても、読み取り / 書き込みボリュームおよび読み取り専用ボリュームで増分テープバックアップおよびリストア処理を引き続き実行できます。

ベースラインリストア処理とボリューム移動処理を同時に実行することはできません。ただし、増分リストアはボリューム移動処理と並行して実行できます。このリストアの動作は、ボリューム移動処理時の SMTape バックアップ処理と同様です。

## **SMTape とボリュームリホスト処理との連携**

ボリュームでボリュームリホスト処理を実行中のときは、SMTape 処理を開始できません。ボリュームリホスト処理に関係するボリュームでは、SMTape セッションを開始しないでください。

ボリュームリホスト処理の実行中は、SMTape バックアップまたはリストアが失敗します。SMTape バックアップまたはリストアの実行中は、ボリュームリホスト処理が失敗し、該当するエラーメッセージが表示されます。この状況では、NDMP ベースと CLI ベースの両方のバックアップまたはリストア処理が環境ベースになります。

## **ADB による NDMP バックアップポリシーへの影響**

Automatic Data Balancer（ADB；自動データバランサ）が有効な場合、ADB はアグリゲートの使用状況の統計を分析し、設定されている使用率の上限のしきい値を超えたアグリゲートを特定します。

バランサは、しきい値を超えたアグリゲートを特定すると、クラスタ内の別のノードにあるアグリゲートに移動できるボリュームを特定してそのボリュームの移動を試みます。この状況は、このボリュームに設定されているバックアップポリシーに影響します。Data Management Application（DMA；データ管理アプリケーション）が CAB に対応していない場合、バックアップポリシーを再設定してベースラインバックアップ処理を実行する必要があるためです。



DMA が CAB に対応しており、特定のインターフェイスを使用してバックアップポリシーが設定されている場合は、ADB に影響しません。

## MetroCluster 構成で SMTape バックアップおよびリストア処理が受ける影響

MetroCluster 構成で SMTape バックアップおよびリストア処理を実行するには、スイッチオーバー処理またはスイッチバック処理の実行時に SMTape 処理が受ける影響について理解しておく必要があります。

### SMTape バックアップまたはリストア処理のあとにスイッチオーバーが行われる場合

クラスタ 1 とクラスタ 2 の 2 つのクラスタがあるとします。クラスタ 1 で SMTape バックアップまたはリストア処理を実行しているときに、クラスタ 1 からクラスタ 2 へのスイッチオーバーが開始されると、次のような結果になります。

- の値の場合 `-override-vetoes` オプションはです `false` その後、スイッチオーバープロセスが中止され、バックアップまたはリストア処理が続行されます。
- オプションの値がの場合 `true` その後、SMTape バックアップまたはリストア処理が中止され、スイッチオーバープロセスが続行されます。

### SMTape バックアップまたはリストア処理のあとにスイッチバックが行われる場合

クラスタ 1 からクラスタ 2 へのスイッチオーバーが実行され、クラスタ 2 で SMTape バックアップまたはリストア処理が開始されます。クラスタ 2 にあるボリュームが SMTape 処理によってバックアップまたはリストアされます。この時点で、クラスタ 2 からクラスタ 1 へのスイッチバックが開始されると、次のような結果になります。

- の値の場合 `-override-vetoes` オプションはです `false` をクリックすると、スイッチバックプロセスが中止され、バックアップまたはリストア処理が続行されます。
- オプションの値がの場合 `true` をクリックすると、バックアップまたはリストア処理が中止され、スイッチバックプロセスが続行されます。

### スイッチオーバーまたはスイッチバックの実行中に SMTape バックアップまたはリストア処理が開始された場合

クラスタ 1 からクラスタ 2 へのスイッチオーバープロセスの実行中に、クラスタ 1 で SMTape バックアップまたはリストア処理が開始されると、そのバックアップまたはリストア処理は失敗し、スイッチオーバーが続行されます。

クラスタ 2 からクラスタ 1 へのスイッチバックプロセスの実行中に、クラスタ 2 で SMTape バックアップまたはリストア処理が開始されると、そのバックアップまたはリストア処理は失敗し、スイッチバックが続行されます。

## FlexVol ボリュームのテープバックアップおよびリストア処理を監視する

### FlexVol ボリュームのテープバックアップおよびリストア処理の概要を監視する

イベントログファイルを表示して、テープバックアップおよびリストア処理を監視できます。ONTAP は、発生したバックアップおよびリストアの重大なイベントとその時刻を、という名前のログファイルに自動的に記録します backup コントローラの



/etc/log/ ディレクトリ。デフォルトでは、イベントロギングはに設定されています on。

イベントログファイルを表示する理由には、次のものがあります。

- 夜間バックアップが成功したかどうかを確認しています
- バックアップ処理に関する統計の収集
- 過去のイベントログファイルの情報を使用した、バックアップおよびリストア処理に関する問題の診断

イベントログファイルは、週に 1 回ローテーションされます。。 /etc/log/backup ファイルの名前がに変更されました /etc/log/backup.0、 /etc/log/backup.0 ファイルの名前がに変更されました /etc/log/backup.1`など。ログファイルは最大6週間保存されるため、最大7つのメッセージファイルを保持できます (/etc/log/backup.[0-5]`そして電流 /etc/log/backup ファイル)。

イベントログファイルにアクセスします

では、テープバックアップおよびリストア処理用のイベントログファイルにアクセスできます /etc/log/ を使用してディレクトリを作成します `rdfile` コマンドを実行します。これらのイベントログファイルを表示して、テープバックアップおよびリストア処理を監視できます。

このタスクについて

へのアクセスを持つアクセス制御ロールなど、追加の設定を使用する `spi` で設定されたWebサービスまたはユーザアカウント `http` アクセス方法：Webブラウザを使用してこれらのログファイルにアクセスすることもできます。

手順

1. ノードシェルにアクセスするには、次のコマンドを入力します。

```
node run -node node_name
```

`node_name` はノードの名前です。

2. テープバックアップおよびリストア処理用のイベントログファイルにアクセスするには、次のコマンドを入力します。

```
rdfile /etc/log/backup
```

関連情報

["システム管理"](#)

["ONTAP の概念"](#)

ダンプイベントログメッセージおよびリストアイベントログメッセージの形式

ダンプイベントログメッセージおよびリストアイベントログメッセージの形式の概要

バックアップログファイルには、ダンプイベントやリストアイベントが発生するたびに

メッセージが書き込まれます。

ダンプイベントログメッセージおよびリストアイイベントログメッセージの形式は次のとおりです。

```
type timestamp identifier event (event_info)
```

次に、イベントログメッセージ形式のフィールドについて説明します。

- 各ログ・メッセージは、次の表に示すいずれかのタイプ・インジケータで始まります。

を入力します	説明
ログ	ロギングイベント
DMP	ダンプイベント
RST	リストアイイベント

- timestamp イベントの日時が表示されます。
- identifier ダンプイベントのフィールドには、ダンプパスとダンプの一意的IDが含まれます。  
identifier リストアイイベントのフィールドでは、リストア先のパス名のみが一意的識別子として使用されます。ロギング関連のイベントメッセージには、は含まれません identifier フィールド。

ロギングイベントとは

log で始まるメッセージの event フィールドは、ロギングの開始または終了を示します。

次の表に示すいずれかのイベントが含まれています。

イベント	説明
Start_Logging	ロギングの開始、またはディセーブル化後にロギングが再びオンになったことを示します。
Stop_Logging	ロギングがオフになっていることを示します。

ダンプイベントとは

ダンプイベントの event フィールドでは、イベント形式のあとのかっこ内にイベント固有の情報が示されます。

次の表に、ダンプ処理に関して記録されるイベント、その説明、および関連するイベント情報を示します。

イベント	説明	イベント情報
開始	NDMP ダンプが開始された	ダンプレベルおよびダンプのタイプ

イベント	説明	イベント情報
終了	ダンプが正常に完了しました	処理されたデータの量
中止	処理がキャンセルされました	処理されたデータの量
オプション（Options）	指定されたオプションが一覧表示されます	NDMP オプションを含む、すべてのオプションとその関連値
tape_open	読み取り / 書き込みに対してテープが開いています	新しいテープデバイスの名前
tape_close です	読み取り / 書き込みでテープを閉じます	テープデバイスの名前
フェーズ変更	ダンプの新しい処理フェーズの開始	新しいフェーズの名前
エラー	ダンプ処理における予期せぬイベントの発生	エラーメッセージです
スナップショット	Snapshot コピーが作成されるか、または検出される	Snapshot コピーの名前と時刻
base_dump	内部メタファイルにベースダンプエントリが見つかりました	ベースダンプのレベルと時刻（増分ダンプの場合のみ）

リストイベントとは

リストイベントの event フィールドでは、イベント形式のあとのかっこ内にイベント固有の情報が示されます。

次の表に、リストア処理に関して記録されるイベント、その説明、および関連するイベント情報を示します。

イベント	説明	イベント情報
開始	NDMP リストアが開始されます	リストアレベルおよびリストアタイプ
終了	リストアが正常に完了しました	処理されたファイルの数とデータの量
中止	処理がキャンセルされました	処理されたファイルの数とデータの量

イベント	説明	イベント情報
オプション（Options）	指定されたオプションが一覧表示されます	NDMP オプションを含む、すべてのオプションとその関連値
tape_open	読み取り / 書き込みに対してテープが開いています	新しいテープデバイスの名前
tape_close です	読み取り / 書き込みでテープを閉じます	テープデバイスの名前
フェーズ変更	リストアの新しい処理フェーズの開始中です	新しいフェーズの名前
エラー	リストア処理で予期しないイベントが発生しました	エラーメッセージです

イベントロギングの有効化または無効化

イベントロギングのオンとオフを切り替えることができます。

手順

1. イベントロギングを有効または無効にするには、クラスタシェルで次のコマンドを入力します。

```
options -option_name backup.log.enable -option-value {on | off}
```

on イベントロギングをオンにします。

off イベントロギングをオフにします。



イベントロギングはデフォルトでオンになっています。

## FlexVol ボリュームのテープバックアップおよびリストアに関するエラーメッセージ

バックアップおよびリストアに関するエラーメッセージ

リソース制限：使用可能なスレッドがありません

• \* メッセージ \*

```
Resource limitation: no available thread
```

• \* 原因 \*

ローカルテープ I/O スレッドのアクティブな最大数が現在使用中です。ローカルテープドライブは最大 16 本までアクティブにすることができます。

• \* 是正措置 \*

一部のテープジョブが完了するまで待ってから、新しいバックアップジョブまたはリストアジョブを開始します。

テープ予約が優先されました

- \* メッセージ \*

Tape reservation preempted

- \* 原因 \*

テープドライブが別の処理で使用されているか、テープがすでに閉じられています。

- \* 是正措置 \*

テープドライブが別の処理で使用されていないこと、および DMA アプリケーションによってジョブが中断されていないことを確認してから、再試行します。

メディアを初期化できませんでした

- \* メッセージ \*

Could not initialize media

- \* 原因 \*

このエラーは、次のいずれかの原因で発生することがあります。

- バックアップに使用するテープドライブが破損しています。
- テープに完全なバックアップが含まれていないか、テープが破損しています。
- ローカルテープ I/O スレッドのアクティブな最大数が現在使用中です。

ローカルテープドライブは最大 16 本までアクティブにすることができます。

- \* 是正措置 \*

- テープドライブが破損している場合は、有効なテープドライブを使用して処理を再試行します。
- テープに完全なバックアップが含まれていないか、テープが破損している場合は、リストア処理を実行できません。
- テープリソースを使用できない場合は、いくつかのバックアップジョブまたはリストアジョブが完了するのを待ってから、処理を再試行します。

実行中のダンプまたはリストアの最大許容数（セッション制限の最大数）

- \* メッセージ \*

Maximum number of allowed dumps or restores (*maximum session limit*) in progress

- \* 原因 \*

最大数のバックアップジョブまたはリストアジョブがすでに実行中です。

- \* 是正措置 \*

現在実行中のジョブがいくつか完了してから、処理を再試行します。

テープ書き込み時のメディアエラーです

- \* メッセージ \*

Media error on tape write

- \* 原因 \*

バックアップに使用するテープが破損しています。

- \* 是正措置 \*

テープを取り替えて、バックアップジョブを再試行します。

テープの書き込みに失敗しました

- \* メッセージ \*

Tape write failed

- \* 原因 \*

バックアップに使用するテープが破損しています。

- \* 是正措置 \*

テープを取り替えて、バックアップジョブを再試行します。

テープへの書き込みに失敗しました - 新しいテープでメディアエラーが発生しました

- \* メッセージ \*

Tape write failed - new tape encountered media error

- \* 原因 \*

バックアップに使用するテープが破損しています。

- \* 是正措置 \*

テープを取り替えて、バックアップを再試行します。

テープへの書き込みに失敗しました - 新しいテープが破損しているか '書き込み保護' されている

- \* メッセージ \*

Tape write failed - new tape is broken or write protected

- \* 原因 \*

バックアップに使用するテープが破損しているか、テープに書き込み保護が設定されています。

- \* 是正措置 \*

テープを取り替えて、バックアップを再試行します。

テープの書き込みに失敗しました - 新しいテープはすでにメディアの末尾にあります

- \* メッセージ \*

Tape write failed - new tape is already at the end of media

- \* 原因 \*

テープにバックアップを完了できるだけの十分なスペースがありません。

- \* 是正措置 \*

テープを取り替えて、バックアップを再試行します。

テープ書き込みエラー

- \* メッセージ \*

Tape write error - The previous tape had less than the required minimum capacity, size MB, for this tape operation, The operation should be restarted from the beginning

- \* 原因 \*

テープ容量が不足していてバックアップデータを格納できません。

- \* 是正措置 \*

より大きな容量のテープを使用して、バックアップジョブを再試行します。

テープ読み取り時のメディアエラーです

- \* メッセージ \*

Media error on tape read

- \* 原因 \*

データのリストア元のテープが破損しており、テープに完全なバックアップデータが含まれていない可能性があります。

- \* 是正措置 \*

テープに完全なバックアップが含まれていることがわかっている場合は、リストア処理を再試行します。テープに完全なバックアップが含まれていない場合は、リストア処理を実行できません。

テープ読み取りエラーです

- \* メッセージ \*

Tape read error

- \* 原因 \*

テープドライブが破損しているか、テープに完全なバックアップが含まれていません。

- \* 是正措置 \*

テープドライブが破損している場合は、別のテープドライブを使用します。テープに完全なバックアップが含まれていないと、データをリストアできません。

テープの終わりにはすでにある

- \* メッセージ \*

Already at the end of tape

- \* 原因 \*

テープにデータが含まれていないか、テープを巻き戻す必要があります。

- \* 是正措置 \*

テープにデータが含まれていない場合は、バックアップを含むテープを使用して、リストアジョブを再試行します。テープにデータが含まれている場合は、テープを巻き戻してリストアジョブを再試行します

テープレコードサイズが小さすぎます。サイズを大きくしてみてください。

- \* メッセージ \*

Tape record size is too small. Try a larger size.

- \* 原因 \*

バックアップ時に使用されたブロック化因数より小さいブロック化因数がリストア処理に指定されました。

- \* 是正措置 \*

バックアップ時に指定したのと同じブロック化因数を使用します。



テープレコードサイズは、**block\_size2**ではなく、**block\_size1** する必要があります

- \* メッセージ \*

Tape record size should be block\_size1 and not block\_size2

- \* 原因 \*

ローカルリストアに指定されたブロック化因数が正しくありません。

- \* 是正措置 \*

を使用してリストアジョブを再試行します block\_size1 をブロック化因数として指定します。

テープレコードサイズは **4KB** から **256KB** の範囲で指定する必要があります

- \* メッセージ \*

Tape record size must be in the range between 4KB and 256KB

- \* 原因 \*

バックアップまたはリストア処理に指定されたブロック化因数が、許容範囲内に収まっていません。

- \* 是正措置 \*

ブロック化因数を、4~256KB の範囲で指定します。

## NDMP に関するエラーメッセージです

### ネットワーク通信エラー

- \* メッセージ \*

Network communication error

- \* 原因 \*

NDMP 3 ウェイ接続でのリモートテープとの通信に失敗しました。

- \* 是正措置 \*

リモートムーバーへのネットワーク接続を確認します。

### 読み取りソケットからのメッセージ: **ERROR\_STRING**

- \* メッセージ \*

Message from Read Socket: error\_string

- \* 原因 \*

NDMP 3 ウェイ接続でのリモートテープからのリストア通信でエラーが発生しています。

- \* 是正措置 \*

リモートムーバーへのネットワーク接続を確認します。

#### Write Dirnet からのメッセージ: **ERROR\_STRING**

- \* メッセージ \*

Message from Write Dirnet: error\_string

- \* 原因 \*

NDMP 3 ウェイ接続でのリモートテープとのバックアップ通信でエラーが発生しています。

- \* 是正措置 \*

リモートムーバーへのネットワーク接続を確認します。

リードソケットが **EOF** を受信しました

- \* メッセージ \*

Read Socket received EOF

- \* 原因 \*

NDMP 3 ウェイ接続でリモートテープとの通信が試行されましたが、ファイルの終わりを示すマークに達しました。ブロックサイズが大きいバックアップイメージから 3 ウェイリストアを試行している可能性があります。

- \* 是正措置 \*

正しいブロックサイズを指定して、リストア処理を再試行します。

#### ndmpd のバージョン番号が無効です: **version\_number**

- \* メッセージ \*

ndmpd invalid version number: version\_number

- \* 原因 \*

指定した NDMP バージョンがストレージシステムでサポートされていません。

- \* 是正措置 \*

NDMP バージョン 4 を指定します。

ndmpd セッション **session\_ID** がアクティブではありません

• \* メッセージ \*

```
ndmpd session session_ID not active
```

• \* 原因 \*

NDMP セッションが存在しない可能性があります。

• \* 是正措置 \*

を使用します `ndmpd status` コマンドを使用して、アクティブなNDMPセッションを表示します。

ボリューム **volume\_name** の **vol ref** を取得できませんでした

• \* メッセージ \*

```
Could not obtain vol ref for Volume vol_name
```

• \* 原因 \*

ボリュームが他の処理で使用されている可能性があるため、ボリューム参照を取得できませんでした。

• \* 是正措置 \*

あとで処理を再試行します。

データ接続タイプ「**NDMP4\_ADDR\_TCP**」 | 「**NDMP4\_ADDR\_TCP\_IPv6**」は、「**IPv6**」 | 「**IPv4**」コントロール接続ではサポートされていません

• \* メッセージ \*

```
Data connection type ["NDMP4_ADDR_TCP"|"NDMP4_ADDR_TCP_IPv6"] not supported  
for ["IPv6"|"IPv4"] control connections
```

• \* 原因 \*

ノードを対象とした NDMP モードでは、確立された NDMP データ接続のネットワークアドレスのタイプ（IPv4 または IPv6）が NDMP 制御接続と同じである必要があります。

• \* 是正措置 \*

バックアップアプリケーションのベンダーにお問い合わせください。

**Data Listen** : **CAB** データ接続の準備前提条件エラー

• \* メッセージ \*

```
DATA LISTEN: CAB data connection prepare precondition error
```

• \* 原因 \*

バックアップアプリケーションが CAB 拡張を使用して NDMP サーバとネゴシエートし、NDMP\_CAB\_DATA\_CONN\_PREPARE メッセージと NDMP\_DATA\_LISTEN メッセージ間で、指定された NDMP データ接続のアドレスタイプの不一致を検出した場合は、NDMP データのリスンが失敗します。

- \* 是正措置 \*

バックアップアプリケーションのベンダーにお問い合わせください。

#### Data connect : CAB データ接続準備前提条件エラー

- \* メッセージ \*

DATA CONNECT: CAB data connection prepare precondition error

- \* 原因 \*

バックアップアプリケーションが CAB 拡張を使用して NDMP サーバとネゴシエートし、NDMP\_CAB\_DATA\_CONN\_PREPARE メッセージと NDMP\_DATA\_CONNECT メッセージ間で、指定された NDMP データ接続のアドレスタイプの不一致を検出した場合は、NDMP データ接続が失敗します。

- \* 是正措置 \*

バックアップアプリケーションのベンダーにお問い合わせください。

#### エラー : show failed : cannot get password for user '<username>'

- \* メッセージ \*

Error: show failed: Cannot get password for user '<username>'

- \* 原因 \*

NDMP のユーザアカウント設定が完了していません

- \* 是正措置 \*

ユーザアカウントが SSH アクセス方法に関連付けられていて、認証方法がユーザパスワードであることを確認します。

#### ダンプに関するエラーメッセージ

デスティネーションボリュームは読み取り専用です

- \* メッセージ \*

Destination volume is read-only

- \* 原因 \*

リストア処理の試行対象のパスが読み取り専用です。

- \* 是正措置 \*

データを別の場所にリストアしてみてください。

デスティネーション **qtree** は読み取り専用です

- \* メッセージ \*

```
Destination qtree is read-only
```

- \* 原因 \*

リストアの試行対象の **qtree** が読み取り専用です。

- \* 是正措置 \*

データを別の場所にリストアしてみてください。

ボリュームでダンプが一時的に無効になっています。再試行して

- \* メッセージ \*

```
Dumps temporarily disabled on volume, try again
```

- \* 原因 \*

NDMPダンプバックアップは、の一部であるSnapMirrorデスティネーションボリュームで試行されます  
`snapmirror break` または `snapmirror resync` 操作。

- \* 是正措置 \*

を待ちます `snapmirror break` または `snapmirror resync` 終了してダンプ処理を実行する処理。



SnapMirror デスティネーションボリュームの状態が読み取り / 書き込みから読み取り専用、または読み取り専用から読み取り / 書き込みに変わったときは、必ずベースラインバックアップを実行する必要があります。

**NFS** ラベルが認識されません

- \* メッセージ \*

```
Error: Aborting: dump encountered NFS security labels in the file system
```

- \* 原因 \*

NFSv4 4.2 が有効な場合、ONTAP 9.9.1 以降では NFS セキュリティラベルがサポートされます。ただし、NFS セキュリティラベルは現在ダンプエンジンで認識されていません。ファイル、ディレクトリ、またはダンプ形式の特殊ファイルに NFS セキュリティラベルがあると、ダンプは失敗します。

- \* 是正措置 \*

NFS セキュリティラベルが設定されているファイルやディレクトリがないことを確認します。

ファイルは作成されませんでした

• \* メッセージ \*

No files were created

• \* 原因 \*

拡張 DAR 機能を有効にしないで、ディレクトリ DAR が試行されました。

• \* 是正措置 \*

拡張 DAR 機能を有効にしてから、DAR を再試行します。

ファイル <ファイル名> のリストアに失敗しました

• \* メッセージ \*

Restore of the file file name failed

• \* 原因 \*

デスティネーションボリューム上の LUN と同じ名前のファイルの Direct Access Recovery (DAR) が実行された場合、その DAR は失敗します。

• \* 是正措置 \*

ファイルの DAR を再試行します。

src inode <inode 番号> ...一時的に切り捨てが失敗しました

• \* メッセージ \*

Truncation failed for src inode <inode number>. Error <error number>. Skipping inode.

• \* 原因 \*

ファイルのリストア時に、ファイルの inode が削除されます。

• \* 是正措置 \*

ボリューム上のリストア処理が完了するまで待機してから、そのボリュームを使用します。

ダンプに必要な **Snapshot** をロックできません

• \* メッセージ \*

Unable to lock a snapshot needed by dump

- \* 原因 \*

バックアップに指定された Snapshot コピーが使用できません。

- \* 是正措置 \*

別の Snapshot コピーを指定してバックアップを再試行します。

を使用します `snap list` コマンドを実行して、使用可能なSnapshotコピーのリストを確認します。

ビットマップファイルが見つかりません

- \* メッセージ \*

```
Unable to locate bitmap files
```

- \* 原因 \*

バックアップ処理に必要なビットマップファイルが削除されている可能性があります。この場合、バックアップを再開できません。

- \* 是正措置 \*

バックアップを再度実行します。

ボリュームが一時的な状態にあります

- \* メッセージ \*

```
Volume is temporarily in a transitional state
```

- \* 原因 \*

バックアップ対象のボリュームが一時的にマウント解除された状態になっています。

- \* 是正措置 \*

しばらく待ってから、もう一度バックアップを実行してください。

## **SM Tape** に関するエラーメッセージ

順序どおりにならないチャンク

- \* メッセージ \*

```
Chunks out of order
```

- \* 原因 \*

バックアップテープが正しい順序でリストアされていません。

- \* 是正措置 \*

リストア処理を再試行し、正しい順序でテープを装填します。

チャンクフォーマットはサポートされていません

- \* メッセージ \*

Chunk format not supported

- \* 原因 \*

SM Tape にバックアップイメージが含まれていません。

- \* 是正措置 \*

SM Tape にバックアップイメージが含まれていない場合は、SM Tape バックアップを含むテープを使用して処理を再試行します。

メモリの割り当てに失敗しました

- \* メッセージ \*

Failed to allocate memory

- \* 原因 \*

システムのメモリが不足しています。

- \* 是正措置 \*

システムがあまりビジー状態でないときに、ジョブを再試行します。

データバッファを取得できませんでした

- \* メッセージ \*

Failed to get data buffer

- \* 原因 \*

ストレージシステムのバッファが不足しています。

- \* 是正措置 \*

ストレージシステムの処理がいくつか完了するのを待ってから、ジョブを再試行します。

**Snapshot** が見つかりませんでした

- \* メッセージ \*



Failed to find snapshot

- \* 原因 \*

バックアップに指定された Snapshot コピーが使用できません。

- \* 是正措置 \*

指定した Snapshot コピーが使用可能かどうかを確認してください。表示されない場合は、正しい Snapshot コピーを使用して再試行します。

#### **Snapshot** を作成できませんでした

- \* メッセージ \*

Failed to create snapshot

- \* 原因 \*

ボリュームにはすでに許容最大数の Snapshot コピーが含まれています。

- \* 是正措置 \*

いくつかの Snapshot コピーを削除してから、バックアップ処理を再試行します。

#### **Snapshot** をロックできませんでした

- \* メッセージ \*

Failed to lock snapshot

- \* 原因 \*

Snapshot コピーが使用中であるか、削除されています。

- \* 是正措置 \*

Snapshot コピーを別の処理で使用中の場合は、その処理が完了するのを待ってからバックアップを再試行します。Snapshot コピーが削除されている場合は、バックアップを実行できません。

#### **Snapshot** を削除できませんでした

- \* メッセージ \*

Failed to delete snapshot

- \* 原因 \*

自動 Snapshot コピーは他の処理で使用中のため、削除できませんでした。

- \* 是正措置 \*

を使用します `snap` コマンドを使用して Snapshot コピーのステータスを確認します。Snapshot コピーが不要である場合は、手動で削除します。

最新の **Snapshot** を取得できませんでした

- \* メッセージ \*

```
Failed to get latest snapshot
```

- \* 原因 \*

ボリュームが SnapMirror によって初期化されているために、最新の Snapshot コピーが存在しない可能性があります。

- \* 是正措置 \*

初期化が完了してから再試行してください。

新しいテープをロードできませんでした

- \* メッセージ \*

```
Failed to load new tape
```

- \* 原因 \*

テープドライブまたはメディアのエラーです。

- \* 是正措置 \*

テープを取り替えて、処理を再試行します。

テープの初期化に失敗しました

- \* メッセージ \*

```
Failed to initialize tape
```

- \* 原因 \*

このエラーメッセージは、次のいずれかの理由で表示されることがあります。

- SMTape にバックアップイメージが含まれていません。
- 指定したテープブロック化因数が正しくありません。
- テープが破損しています。
- リストア用の正しいテープが装填されていません。

- \* 是正措置 \*

- SMTape にバックアップイメージが含まれていない場合は、SMTape バックアップを含むテープを使用して処理を再試行します。

- ブロック化因数が正しくない場合は、正しいブロック化因数を指定して処理を再試行します。
- テープが破損している場合は、リストア処理を実行できません。
- 間違ったテープが装填されている場合は、正しいテープを使用して処理を再試行します。

リストアストリームを初期化できませんでした

• \* メッセージ \*

```
Failed to initialize restore stream
```

• \* 原因 \*

このエラーメッセージは、次のいずれかの理由で表示されることがあります。

- SMTape にバックアップイメージが含まれていません。
- 指定したテープブロック化因数が正しくありません。
- テープが破損しています。
- リストア用の正しいテープが装填されていません。

• \* 是正措置 \*

- SMTape にバックアップイメージが含まれていない場合は、SMTape バックアップを含むテープを使用して処理を再試行します。
- ブロック化因数が正しくない場合は、正しいブロック化因数を指定して処理を再試行します。
- テープが破損している場合は、リストア処理を実行できません。
- 間違ったテープが装填されている場合は、正しいテープを使用して処理を再試行します。

バックアップイメージを読み取れませんでした

• \* メッセージ \*

```
Failed to read backup image
```

• \* 原因 \*

テープが破損しています。

• \* 是正措置 \*

テープが破損している場合は、リストア処理を実行できません。

イメージヘッダーがないか、破損しています

• \* メッセージ \*

```
Image header missing or corrupted
```

• \* 原因 \*

テープに有効な SMTape バックアップが含まれていません。

- \* 是正措置 \*

有効なバックアップが含まれているテープを使用して再試行します。

内部アサーションです

- \* メッセージ \*

Internal assertion

- \* 原因 \*

SMTape 内部エラーがあります。

- \* 是正措置 \*

エラーを報告し、を送信します etc/log/backup テクニカルサポートにファイルを送信します。

バックアップイメージのマジック番号が無効です

- \* メッセージ \*

Invalid backup image magic number

- \* 原因 \*

SMTape にバックアップイメージが含まれていません。

- \* 是正措置 \*

SMTape にバックアップイメージが含まれていない場合は、SMTape バックアップを含むテープを使用して処理を再試行します。

バックアップイメージのチェックサムが無効です

- \* メッセージ \*

Invalid backup image checksum

- \* 原因 \*

テープが破損しています。

- \* 是正措置 \*

テープが破損している場合は、リストア処理を実行できません。

無効な入力テープです

- \* メッセージ \*

Invalid input tape

- \* 原因 \*

バックアップイメージのシグネチャがテープヘッダーで無効です。テープ内のデータが破損しているか、テープに有効なバックアップイメージが含まれていません。

- \* 是正措置 \*

有効なバックアップイメージを指定して、リストアジョブを再試行します。

ボリュームパスが無効です

- \* メッセージ \*

Invalid volume path

- \* 原因 \*

バックアップ処理またはリストア処理に指定されたボリュームが見つかりません。

- \* 是正措置 \*

有効なボリュームパスとボリューム名を指定してジョブを再試行します。

バックアップセット ID が一致しません

- \* メッセージ \*

Mismatch in backup set ID

- \* 原因 \*

テープの変更時に装填されたテープが、バックアップセットに含まれるテープではありません。

- \* 是正措置 \*

正しいテープを装填して、ジョブを再試行します。

バックアップタイムスタンプが一致しません

- \* メッセージ \*

Mismatch in backup time stamp

- \* 原因 \*

テープの変更時に装填されたテープが、バックアップセットに含まれるテープではありません。

- \* 是正措置 \*

を使用します `smtape restore -h` コマンドを使用して、テープのヘッダー情報を確認します。

シャットダウンが原因でジョブが中止されました

- \* メッセージ \*

`Job aborted due to shutdown`

- \* 原因 \*

ストレージシステムをリブートしています。

- \* 是正措置 \*

ストレージシステムのリブート後にジョブを再試行します。

**Snapshot** の自動削除が原因でジョブが中止されました

- \* メッセージ \*

`Job aborted due to Snapshot autodelete`

- \* 原因 \*

ボリュームに十分なスペースがないため、Snapshot コピーの自動削除を実行できません。

- \* 是正措置 \*

ボリューム内のスペースを解放して、ジョブを再試行します。

テープは現在他の処理で使用されています

- \* メッセージ \*

`Tape is currently in use by other operations`

- \* 原因 \*

テープドライブが別のジョブで使用中です。

- \* 是正措置 \*

現在アクティブなジョブが完了してから、バックアップを再試行します。

テープの順序が切れています

- \* メッセージ \*

`Tapes out of order`

- \* 原因 \*

リストア処理に使用する一連のテープの最初のテープに、イメージヘッダーがありません。

- \* 是正措置 \*

イメージヘッダーの付いたテープを装填して、ジョブを再試行します。

転送に失敗しました ( **MetroCluster** 処理が原因で中止されました)

- \* メッセージ \*

Transfer failed (Aborted due to MetroCluster operation)

- \* 原因 \*

スイッチオーバー処理またはスイッチバック処理が原因で、SMTape 処理が中止されます。

- \* 是正措置 \*

スイッチオーバー処理またはスイッチバック処理が終了したあとに SMTape 処理を実行します。

転送に失敗しました ( **ARL** で中止)

- \* メッセージ \*

Transfer failed (ARL initiated abort)

- \* 原因 \*

SMTape 処理の実行中にアグリゲートの再配置を開始すると、SMTape 処理が中止されます。

- \* 是正措置 \*

アグリゲートの再配置処理が終了したあとに SMTape 処理を実行します。

転送に失敗しました ( **CFO** が中止を開始)

- \* メッセージ \*

Transfer failed (CFO initiated abort)

- \* 原因 \*

CFO アグリゲートのストレージフェイルオーバー (テイクオーバーとギブバック) 処理が原因で、SMTape 処理が中止されます。

- \* 是正措置 \*

CFO アグリゲートのストレージフェイルオーバーが終了したあとに SMTape 処理を実行します。

転送に失敗（**SFO** によって中止が開始されました）

- \* メッセージ \*

Transfer failed (SFO initiated abort)

- \* 原因 \*

ストレージフェイルオーバー（テイクオーバーとギブバック）処理が原因で、SMTape 処理が中止されます。

- \* 是正措置 \*

ストレージフェイルオーバー（テイクオーバーとギブバック）処理が終了したあとに SMTape 処理を実行します。

移行の基盤となるアグリゲート

- \* メッセージ \*

Underlying aggregate under migration

- \* 原因 \*

移行（ストレージフェイルオーバーまたはアグリゲートの再配置）を実行中のアグリゲートで SMTape 処理が開始されると、その SMTape 処理は失敗します。

- \* 是正措置 \*

アグリゲートの移行が終了したあとに SMTape 処理を実行します。

ボリュームは現在移動中です

- \* メッセージ \*

Volume is currently under migration

- \* 原因 \*

ボリューム移行と SMTape バックアップは同時に実行できません。

- \* 是正措置 \*

ボリューム移行が完了してから、バックアップジョブを再試行します。

ボリュームはオフラインです

- \* メッセージ \*

Volume offline

- \* 原因 \*



バックアップ対象のボリュームがオフラインです。

- \* 是正措置 \*

ボリュームをオンラインに戻し、バックアップを再試行します。

ボリュームが制限されていません

- \* メッセージ \*

Volume not restricted

- \* 原因 \*

データのリストア先のデスティネーションボリュームが制限されていません。

- \* 是正措置 \*

ボリュームを制限して、リストア処理を再試行します。

## NDMP構成

### NDMP構成の概要

サードパーティ製バックアップアプリケーションを使用してデータをテープに直接バックアップするには、Network Data Management Protocol（NDMP；ネットワークデータ管理プロトコル）を使用するように ONTAP 9 クラスタを簡単に設定します。

バックアップアプリケーションがCluster Aware Backup（CAB）をサポートしている場合は、SVMを対象としたNDMPまたはノードを対象としたNDMPを設定できます。

- SVMを対象としたNDMPをクラスタ（管理SVM）レベルでは、クラスタの複数のノードでホストされているすべてのボリュームをバックアップできます。可能であれば、SVMを対象としたNDMPを推奨します。
- ノードを対象としたNDMPを使用すると、そのノードでホストされているすべてのボリュームをバックアップできます。

バックアップアプリケーションがCABをサポートしていない場合は、ノードを対象としたNDMPを使用する必要があります。

SVMを対象としたNDMPとノードを対象としたNDMPは相互に排他的であり、同じクラスタでは設定できません。



ノードを対象としたNDMPは、ONTAP 9で廃止されました。

の詳細を確認してください "[クラスタ対応バックアップ（CAB）](#)"。

NDMPを設定する前に、次の点を確認します。

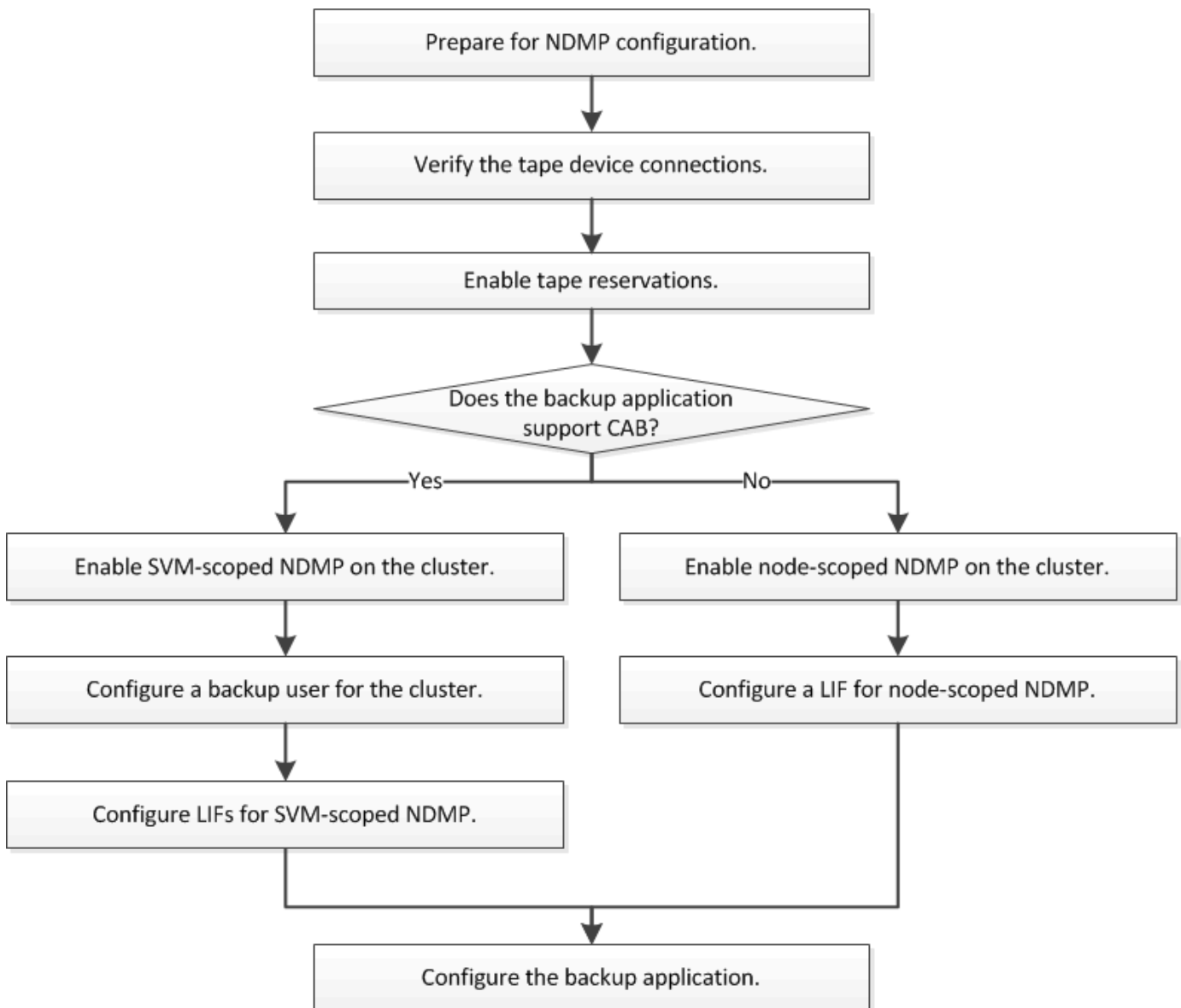
- サードパーティ製バックアップアプリケーション（データ管理アプリケーションまたは DMA と呼ばれ

る) がある。

- クラスタ管理者である。
- テープデバイスとオプションのメディアサーバがインストールされている。
- テープデバイスがクラスタに直接接続ではなく Fibre Channel (FC ; ファイバチャネル) スイッチを介して接続されている。
- 少なくとも 1 つのテープデバイスの Logical Unit Number (LUN ; 論理ユニット番号) が 0 である。

## NDMP の設定ワークフロー

NDMP を使用したテープバックアップのセットアップでは、NDMP 構成の準備、テープデバイスの接続の確認、テープ予約の有効化、SVM またはノードレベルでの NDMP の設定、クラスタでの NDMP の有効化、バックアップユーザの設定、LIF の設定、バックアップアプリケーションの設定を行います。



## NDMP 構成を準備

Network Data Management Protocol (NDMP ; ネットワークデータ管理プロトコル) を使用したテープバックアップアクセスを設定する前に、計画した構成がサポートされていることを確認し、各ノードにテープドライブが認定ドライブとして表示されていることを確認し、すべてのノードにクラスタ間 LIF があることを確認する必要があります。また、バックアップアプリケーションが Cluster Aware Backup (CAB) 拡張をサポートしているかどうかを確認します。

### 手順

1. ONTAP のサポートについては、バックアップアプリケーションプロバイダの互換性マトリックスを参照してください (ネットアップでは、ONTAP または NDMP を使用したサードパーティ製バックアップアプリケーションのサポートは対象外です)。

次のネットアップコンポーネントに互換性があることを確認する必要があります。

- クラスタで実行されている ONTAP 9 のバージョン。
- バックアップアプリケーションのベンダーとバージョン。Veritas NetBackup 8.2 や Commvault など。
- テープデバイスの詳細情報には、テープドライブのメーカー、モデル、インターフェイスなどが含まれます。たとえば、IBM Ultrium 8 や HPE StoreEver Ultrium 30750 LTO-8 などです。
- クラスタ内のノードのプラットフォーム。FAS8700 や A400 など。



バックアップアプリケーションの旧バージョンの ONTAP 互換性サポートマトリックスは、で確認できます ["NetApp Interoperability Matrix Tool で確認できます"](#)。

2. 各ノードの組み込みのテープ構成ファイルにテープドライブが認定ドライブとしてリストされていることを確認します。

- a. コマンドラインインターフェイスで、を使用して組み込みのテープ構成ファイルを表示します  
storage tape show-supported-status コマンドを実行します

```
cluster1::> storage tape show-supported-status

Node: cluster1-1

Tape Drives                                Is Supported   Support Status
-----
Certance Ultrium 2                         true          Dynamically Qualified
Certance Ultrium 3                         true          Dynamically Qualified
Digital DLT2000                           true          Qualified
```

- b. テープドライブを出力に表示された認定ドライブのリストと比較します。



出力に表示されるテープデバイスの名前は、デバイスラベルまたは Interoperability Matrix に表示された名前と多少異なる場合があります。たとえば、Digital DLT2000 は DLT2k と表示されることもあります。このような小さな名前の違いは無視してかまいません。

- c. デバイスが Interoperability Matrix で認定されているにもかかわらず、出力に認定デバイスとしてリストされない場合は、NetApp Support Siteの手順に従って、デバイスの更新された構成ファイルをダウンロードしてインストールします。

#### "ネットアップのダウンロード：テープデバイスの構成ファイル"

ノードの出荷後にテープデバイスが認定された場合、認定デバイスが組み込みのテープ構成ファイルにリストされていないことがあります。

3. クラスタ内のすべてのノードにクラスタ間 LIF があることを確認します。
  - a. を使用して、ノードのクラスタ間LIFを表示します `network interface show -role intercluster` コマンドを実行します

```
cluster1::> network interface show -role intercluster
```

	Logical	Status	Network	Current
Current Is				
Vserver	Interface	Admin/Oper	Address/Mask	Node
Port	Home			
-----	-----	-----	-----	-----
-----	-----			
cluster1	IC1	up/up	192.0.2.65/24	cluster1-1
e0a	true			

- b. クラスタ間LIFがいずれのノードにも存在しない場合は、を使用してクラスタ間LIFを作成します `network interface create` コマンドを実行します

```
cluster1::> network interface create -vserver cluster1 -lif IC2 -role
intercluster
-home-node cluster1-2 -home-port e0b -address 192.0.2.68 -netmask
255.255.255.0
-status-admin up -failover-policy local-only -firewall-policy
intercluster
```

```
cluster1::> network interface show -role intercluster
```

	Logical	Status	Network	Current
Current Is				
Vserver	Interface	Admin/Oper	Address/Mask	Node
Port	Home			
-----	-----	-----	-----	-----
-----	-----	-----	-----	-----
cluster1	IC1	up/up	192.0.2.65/24	cluster1-1
e0a	true			
cluster1	IC2	up/up	192.0.2.68/24	cluster1-2
e0b	true			

#### "Network Management の略"

4. バックアップアプリケーションに付属のドキュメントを参照して、バックアップアプリケーションが Cluster Aware Backup （ CAB ） をサポートしているかどうかを確認します。

CAB のサポートは、実行できるバックアップの種類に影響する重要な要素です。

### テープデバイスの接続を確認します

すべてのドライブとメディアチェンジャが ONTAP でデバイスとして認識されていることを確認する必要があります。

#### 手順

1. を使用して、すべてのドライブとメディアチェンジャに関する情報を表示します storage tape show コマンドを実行します

```
cluster1::> storage tape show
```

```
Node: cluster1-01
```

Device ID	Device Type	Description
-----------	-------------	-------------

Status
--------

-----	-----	-----
-------	-------	-------

sw4:10.11	tape drive	HP LTO-3
-----------	------------	----------

normal
--------

0b.125L1	media changer	HP MSL G3 Series
----------	---------------	------------------

normal
--------

0d.4	tape drive	IBM LTO 5 ULT3580
------	------------	-------------------

normal
--------

0d.4L1	media changer	IBM 3573-TL
--------	---------------	-------------

normal
--------

```
...
```

2. テープドライブが表示されない場合は、問題のトラブルシューティングを行います。
3. メディアチェンジャが表示されない場合は、を使用してメディアチェンジャに関する情報を表示します  
storage tape show-media-changer コマンドを実行し、問題のトラブルシューティングを行います。

```
cluster1::> storage tape show-media-changer
```

```
Media Changer: sw4:10.11L1
```

```
Description: PX70-TL
```

```
WWNN: 2:00a:000e11:10b919
```

```
WWPN: 2:00b:000e11:10b919
```

```
Serial Number: 00FRU7800000_LL1
```

```
Errors: -
```

```
Paths:
```

Node	Initiator	Alias	Device State
------	-----------	-------	--------------

Status
--------

-----	-----	-----	-----
-------	-------	-------	-------

cluster1-01	2b	mc0	in-use
-------------	----	-----	--------

normal
--------

```
...
```

## テープ予約を有効にします

NDMP バックアップ処理のために、バックアップアプリケーションで使用するテープドライブが予約されていることを確認する必要があります。

このタスクについて

予約の設定はバックアップアプリケーションによって異なります。これらの設定は、バックアップアプリケーションおよび同じドライブを使用するノードまたはサーバと一致する必要があります。正しい予約設定については、バックアップアプリケーションのベンダーのドキュメントを参照してください。

手順

1. を使用して予約を有効にします `options -option-name tape.reservations -option-value persistent` コマンドを実行します

次のコマンドは、で予約を有効にします `persistent` 値：

```
cluster1::> options -option-name tape.reservations -option-value
persistent
2 entries were modified.
```

2. を使用して、すべてのノードで予約が有効になっていることを確認します `options tape.reservations` コマンドを入力し、出力を確認します。

```
cluster1::> options tape.reservations

cluster1-1
    tape.reservations                persistent

cluster1-2
    tape.reservations                persistent
2 entries were displayed.
```

## SVM を対象とした NDMP を設定

クラスタで **SVM** を対象とした **NDMP** を有効化

DMAがCluster Aware Backup (CAB) 拡張をサポートしている場合は、SVMを対象としたNDMPを有効にし、クラスタ（管理SVM）でNDMPサービスを有効にし、データ接続と制御接続に使用するLIFを設定することで、クラスタの各ノードでホストされているすべてのボリュームをバックアップできます。

必要なもの

DMA で CAB 拡張がサポートされている必要があります。

このタスクについて

ノードを対象とした NDMP モードをオフにすると、クラスタで SVM を対象とした NDMP モードが有効になります。

#### 手順

1. SVMを対象としたNDMPモードを有効にします。

```
cluster1::> system services ndmp node-scope-mode off
```

SVMを対象としたNDMPモードが有効になっています。

2. 管理SVMでNDMPサービスを有効にします。

```
cluster1::> vservice services ndmp on -vservice cluster1
```

認証タイプはに設定されます challenge デフォルトでは、プレーンテキスト認証は無効になっています。



セキュアな通信のために、プレーンテキスト認証は無効にしておく必要があります。

3. NDMPサービスが有効になっていることを確認します。

```
cluster1::> vservice services ndmp show
```

Vserver	Enabled	Authentication type
cluster1	true	challenge
vs1	false	challenge

#### NDMP認証のバックアップユーザを有効にします

バックアップアプリケーションからSVMを対象としたNDMPを認証するには、十分な権限を持つ管理ユーザとNDMPパスワードが必要です。

#### このタスクについて

バックアップ管理ユーザ用のNDMPパスワードを生成する必要があります。バックアップ管理者ユーザは、クラスタレベルまたはSVMレベルで有効にすることができます。必要に応じて、新しいユーザを作成することもできます。デフォルトでは、次のロールを持つユーザがNDMPバックアップに対して認証できます。

- クラスタ全体： admin または backup
- 個々のSVM： vsadmin または vsadmin-backup

NISユーザまたはLDAPユーザを使用する場合は、それぞれのサーバ上にそのユーザが存在している必要があります。Active Directory ユーザは使用できません。



## 手順

1. 現在の管理者ユーザと権限を表示します。

```
security login show
```

2. 必要に応じて、を使用して新しいNDMPバックアップユーザを作成します security login create コマンドおよびクラスタ全体または個々のSVMの権限に該当するロール。

には、ローカルバックアップユーザの名前、またはNISまたはLDAPユーザの名前を指定できます -user -or-group-name パラメータ

次に、バックアップユーザを作成するコマンドを示します backup\_admin1 を使用 backup クラスタ全体での役割：

```
cluster1::> security login create -user-or-group-name backup_admin1  
-application ssh -authmethod password -role backup
```

次に、バックアップユーザを作成するコマンドを示します vsbackup\_admin1 を使用 vsadmin-backup 個々のSVMのロール：

```
cluster1::> security login create -user-or-group-name vsbackup_admin1  
-application ssh -authmethod password -role vsadmin-backup
```

新しいユーザのパスワードを入力し、確認のためにもう一度入力します。

3. を使用して管理SVMのパスワードを生成します vsserver services ndmp generate password コマンドを実行します

生成されたパスワードは、バックアップアプリケーションによる NDMP 接続の認証で必要になります。

```
cluster1::> vsserver services ndmp generate-password -vsserver cluster1  
-user backup_admin1
```

```
Vserver: cluster1  
User: backup_admin1  
Password: qG5CqQHYxw7tE57g
```

## LIFs を設定します

データとテープのリソース間のデータ接続、および管理 SVM とバックアップアプリケーションの間の制御接続の確立に使用される LIF を特定する必要があります。LIF を特定したら、それらの LIF に対してファイアウォールポリシーとフェイルオーバーポリシーが設定されていることを確認し、優先インターフェイスロールを指定する必要があります。

ONTAP 9.10.1以降では、ファイアウォールポリシーは廃止され、完全にLIFのサービスポリシーに置き換えられました。詳細については、を参照してください ["ONTAP 9.6 以降の LIF とサービスポリシー"](#)。

手順

1. を使用して、クラスタ間LIF、クラスタ管理LIF、およびノード管理LIFを特定します network interface show コマンドにを指定します -role パラメータ

次のコマンドは、クラスタ間 LIF を表示します。

```
cluster1::> network interface show -role intercluster
```

	Logical	Status	Network	Current
Current Is				
Vserver	Interface	Admin/Oper	Address/Mask	Node
Port	Home			
-----	-----	-----	-----	
cluster1	IC1	up/up	192.0.2.65/24	cluster1-1
e0a	true			
cluster1	IC2	up/up	192.0.2.68/24	cluster1-2
e0b	true			

次のコマンドは、クラスタ管理 LIF を表示します。

```
cluster1::> network interface show -role cluster-mgmt
```

	Logical	Status	Network	Current
Current Is				
Vserver	Interface	Admin/Oper	Address/Mask	Node
Port	Home			
-----	-----	-----	-----	
cluster1	cluster_mgmt	up/up	192.0.2.60/24	cluster1-2
e0M	true			

次のコマンドは、ノード管理 LIF を表示します。

```
cluster1::> network interface show -role node-mgmt
```

	Logical	Status	Network	Current
Current Is				
Vserver	Interface	Admin/Oper	Address/Mask	Node
Port	Home			
-----	-----	-----	-----	-----
-----	-----			
cluster1	cluster1-1_mgmt1	up/up	192.0.2.69/24	cluster1-1
e0M	true			
	cluster1-2_mgmt1	up/up	192.0.2.70/24	cluster1-2
e0M	true			

2. クラスタ間 LIF、クラスタ管理（cluster-mgmt）LIF、およびノード管理（node-mgmt）LIF で NDMP に対してファイアウォールポリシーが有効になっていることを確認します。

- a. を使用して、NDMPに対してファイアウォールポリシーが有効になっていることを確認します  
system services firewall policy show コマンドを実行します

次のコマンドは、クラスタ管理 LIF のファイアウォールポリシーを表示します。

```
cluster1::> system services firewall policy show -policy cluster
```

Vserver	Policy	Service	Allowed
-----	-----	-----	-----
cluster	cluster	dns	0.0.0.0/0
		http	0.0.0.0/0
		https	0.0.0.0/0
		** ndmp	0.0.0.0/0**
		ndmps	0.0.0.0/0
		ntp	0.0.0.0/0
		rsh	0.0.0.0/0
		snmp	0.0.0.0/0
		ssh	0.0.0.0/0
		telnet	0.0.0.0/0

10 entries were displayed.

次のコマンドは、クラスタ間 LIF のファイアウォールポリシーを表示します。

```
cluster1::> system services firewall policy show -policy intercluster
```

Vserver	Policy	Service	Allowed
cluster1	intercluster	dns	-
		http	-
		https	-
		**ndmp	0.0.0.0/0, ::/0**
		ndmps	-
		ntp	-
		rsh	-
		ssh	-
		telnet	-

9 entries were displayed.

次のコマンドは、ノード管理 LIF のファイアウォールポリシーを表示します。

```
cluster1::> system services firewall policy show -policy mgmt
```

Vserver	Policy	Service	Allowed
cluster1-1	mgmt	dns	0.0.0.0/0, ::/0
		http	0.0.0.0/0, ::/0
		https	0.0.0.0/0, ::/0
		**ndmp	0.0.0.0/0, ::/0**
		ndmps	0.0.0.0/0, ::/0
		ntp	0.0.0.0/0, ::/0
		rsh	-
		snmp	0.0.0.0/0, ::/0
		ssh	0.0.0.0/0, ::/0
		telnet	-

10 entries were displayed.

- b. ファイアウォールポリシーが有効になっていない場合は、を使用してファイアウォールポリシーを有効にします system services firewall policy modify コマンドにを指定します -service パラメータ

次のコマンドは、クラスタ間 LIF のファイアウォールポリシーを有効にします。

```
cluster1::> system services firewall policy modify -vserver cluster1  
-policy intercluster -service ndmp 0.0.0.0/0
```

3. すべての LIF のフェイルオーバーポリシーが適切に設定されていることを確認します。

- a. クラスタ管理LIFのフェイルオーバーポリシーがに設定されていることを確認します broadcast-domain-wide`をクリックし、クラスタ間LIFとノード管理LIFのポリシーがに設定されます`local-only`を使用します network interface show -failover コマンドを実行します

次のコマンドは、クラスタ管理 LIF、クラスタ間 LIF、およびノード管理 LIF のフェイルオーバーポリシーを表示します。

```
cluster1::> network interface show -failover
```

Failover Vserver Group	Logical Interface	Home Node:Port	Failover Policy
cluster cluster	cluster1_clus1	cluster1-1:e0a	local-only
Failover Targets: .....			
**cluster1 Default**	cluster_mgmt	cluster1-1:e0m	broadcast-domain-wide
Failover Targets: .....			
**IC1 Default**		cluster1-1:e0a	local-only
Failover Targets: .....			
**IC2 Default**		cluster1-1:e0b	local-only
Failover Targets: .....			
**cluster1-1 Default**	cluster1-1_mgmt1	cluster1-1:e0m	local-only
Failover Targets: .....			
**cluster1-2 Default**	cluster1-2_mgmt1	cluster1-2:e0m	local-only
Failover Targets: .....			

- a. フェイルオーバーポリシーが適切に設定されていない場合は、を使用してフェイルオーバーポリシーを変更します network interface modify コマンドにを指定します -failover-policy パラメータ

```
cluster1::> network interface modify -vserver cluster1 -lif IC1
-failover-policy local-only
```

4. を使用して、データ接続に必要なLIFを指定します `vserver services ndmp modify` コマンドにを指定します `preferred-interface-role` パラメータ

```
cluster1::> vserver services ndmp modify -vserver cluster1 -preferred
-interface-role intercluster,cluster-mgmt,node-mgmt
```

5. を使用して、クラスタに優先インターフェイスロールが設定されていることを確認します `vserver services ndmp show` コマンドを実行します

```
cluster1::> vserver services ndmp show -vserver cluster1

Vserver: cluster1
NDMP Version: 4
.....
.....
Preferred Interface Role: intercluster, cluster-mgmt, node-
mgmt
```

## ノードを対象とした **NDMP** を設定

クラスタでノードを対象とした **NDMP** を有効にします

単一のノードでホストされているボリュームをバックアップするには、ノードを対象としたNDMPを有効にし、NDMPサービスを有効にし、データ接続と制御接続に使用するLIFを設定します。これは、クラスタのすべてのノードに対して実行できます。



ノードを対象としたNDMPは、ONTAP 9で廃止されました。

このタスクについて

ノードスコープモードでNDMPを使用する場合、認証はノード単位で設定する必要があります。詳細については、[を参照してください "サポート技術情報の記事「ノードスコープモードでNDMP認証を構成する方法」"](#)。

手順

1. ノードを対象としたNDMPモードを有効にします。

```
cluster1::> system services ndmp node-scope-mode on
```

NDMP node-scope-modeが有効になっている。

2. クラスタ内のすべてのノードでNDMPサービスを有効にします。

ワイルドカード「\*」を使用すると、すべてのノードで NDMP サービスが同時に有効になります。

バックアップアプリケーションによる NDMP 接続の認証でパスワードを指定する必要があります。

```
cluster1::> system services ndmp on -node *
```

```
Please enter password:
Confirm password:
2 entries were modified.
```

3. を無効にします -clear-text NDMPパスワードのセキュアな通信のためのオプション：

ワイルドカード"\*"を使用します\*" disables the -clear-text オプションをすべてのノードで同時に選択できます。

```
cluster1::> system services ndmp modify -node * -clear-text false
```

4. NDMPサービスとが有効になっていることを確認します -clear-text オプションが無効になっています。

```
cluster1::> system services ndmp show
```

Node	Enabled	Clear text	User Id
cluster1-1	true	false	root
cluster1-2	true	false	root

2 entries were displayed.

## LIF を設定

ノードとバックアップアプリケーションの間のデータ接続と制御接続の確立に使用される LIF を特定する必要があります。LIF を特定したら、その LIF に対してファイアウォールポリシーとフェイルオーバーポリシーが設定されていることを確認する必要があります。



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

1. を使用して、ノードでホストされているクラスタ間LIFを特定します network interface show コマンドにを指定します -role パラメータ

```
cluster1::> network interface show -role intercluster
```

	Logical	Status	Network	Current	
Current Is					
Vserver	Interface	Admin/Oper	Address/Mask	Node	Port
Home					
-----	-----	-----	-----	-----	
-----	-----				
cluster1	IC1	up/up	192.0.2.65/24	cluster1-1	e0a
true					
cluster1	IC2	up/up	192.0.2.68/24	cluster1-2	e0b
true					

2. クラスタ間 LIF で NDMP に対してファイアウォールポリシーが有効になっていることを確認します。

- a. を使用して、NDMPに対してファイアウォールポリシーが有効になっていることを確認します system services firewall policy show コマンドを実行します

次のコマンドは、クラスタ間 LIF のファイアウォールポリシーを表示します。

```
cluster1::> system services firewall policy show -policy intercluster
```

Vserver	Policy	Service	Allowed
-----	-----	-----	-----
cluster1	intercluster	dns	-
		http	-
		https	-
		**ndmp	0.0.0.0/0, ::/0**
		ndmps	-
		ntp	-
		rsh	-
		ssh	-
		telnet	-

9 entries were displayed.

- b. ファイアウォールポリシーが有効になっていない場合は、を使用してファイアウォールポリシーを有効にします system services firewall policy modify コマンドにを指定します -service パラメータ

次のコマンドは、クラスタ間 LIF のファイアウォールポリシーを有効にします。



```
cluster1::> system services firewall policy modify -vserver cluster1
-policy intercluster -service ndmp 0.0.0.0/0
```

3. クラスタ間 LIF のフェイルオーバーポリシーが適切に設定されていることを確認します。

- a. クラスタ間LIFのフェイルオーバーポリシーがに設定されていることを確認します local-only を使用します network interface show -failover コマンドを実行します

```
cluster1::> network interface show -failover
```

Vserver	Logical Interface	Home Node:Port	Failover Policy	Failover Group
cluster1	**IC1	cluster1-1:e0a	local-only	
Default**				
			Failover Targets:	
			.....	
	**IC2	cluster1-2:e0b	local-only	
Default**				
			Failover Targets:	
			.....	
cluster1-1	cluster1-1_mgmt1	cluster1-1:e0m	local-only	Default
			Failover Targets:	
			.....	

- b. フェイルオーバーポリシーが適切に設定されていない場合は、を使用してフェイルオーバーポリシーを変更します network interface modify コマンドにを指定します -failover-policy パラメータ

```
cluster1::> network interface modify -vserver cluster1 -lif IC1
-failover-policy local-only
```

## バックアップアプリケーションを設定

クラスタで NDMP アクセスを設定したら、クラスタ構成から情報を収集し、バックアップアプリケーションで残りのバックアッププロセスを設定する必要があります。

### 手順

1. ONTAP で前に設定した次の情報を収集します。
  - バックアップアプリケーションで NDMP 接続を作成するために必要なユーザ名とパスワード
  - バックアップアプリケーションからクラスタに接続するために必要なクラスタ間 LIF の IP アドレス
2. ONTAP で、を使用して、ONTAP が各デバイスに割り当てたエイリアスを表示します storage tape alias show コマンドを実行します

エイリアスを確認しておく、バックアップアプリケーションの設定で役立つことがよくあります。

```
cluster1::> storage tape show -alias
```

```
Device ID: 2a.0
Device Type: tape drive
Description: Hewlett-Packard LTO-5
```

Node	Alias	Mapping
-----	-----	-----
stsw-3220-4a-4b-02	st2	SN[HU19497WVR]
...		

3. バックアップアプリケーションで、バックアップアプリケーションのドキュメントに従って残りのバックアッププロセスを設定します。

完了後

ボリューム移動や LIF 移行などのデータ移動イベントが発生した場合に備えて、中断されたバックアップ処理を再初期化できるように準備しておく必要があります。

## NetApp Element ソフトウェアと ONTAP 間のレプリケーション

### NetApp Element ソフトウェアと ONTAP 間のレプリケーションの概要

SnapMirror を使用して Element ボリュームの Snapshot コピーを ONTAP デスティネーションにレプリケートすることで、Element システムのビジネス継続性を確保できます。これにより、Element サイトで災害が発生した場合でも、ONTAP システムからクライアントに引き続きデータを提供し、サービスのリストア後に Element システムを再アクティブ化することができます。

ONTAP 9.4 以降では、ONTAP ノードで作成した LUN の Snapshot コピーを Element システムにレプリケートして戻すことができます。これは、Element サイトの停止中に LUN を作成した場合や、LUN を使用して ONTAP から Element ソフトウェアにデータを移行する場合に便利です。

以下の場合には、Element から ONTAP へのバックアップを使用する必要があります。

- すべての選択肢について検討するのではなく、ベストプラクティスに従う。
- System Manager や自動スクリプトツールではなく、ONTAP コマンドラインインターフェイス（CLI）を使用する必要がある。
- iSCSI を使用してクライアントにデータを提供している。

構成または概念の詳細な情報が必要な場合は、次のドキュメントを参照してください。

- Element の設定

- SnapMirror の概念と設定

## "データ保護の概要"

### Element と ONTAP 間のレプリケーションについて

ONTAP 9.3 以降では、SnapMirror を使用して Element ボリュームの Snapshot コピーを ONTAP デスティネーションにレプリケートできます。これにより、Element サイトで災害が発生した場合でも、ONTAP システムからクライアントに引き続きデータを提供し、サービスのリストア後に Element ソースボリュームを再アクティブ化することができます。

ONTAP 9.4 以降では、ONTAP ノードで作成した LUN の Snapshot コピーを Element システムにレプリケートして戻すことができます。これは、Element サイトの停止中に LUN を作成した場合や、LUN を使用して ONTAP から Element ソフトウェアにデータを移行する場合に便利です。

#### データ保護関係のタイプ

SnapMirror には 2 種類のデータ保護関係があります。どちらのタイプでも、SnapMirror は関係を初期化または更新する前に Element ソースボリュームの Snapshot コピーを作成します。

- a\_disaster recovery (DR ; ディザスタリカバリ) \_data 保護関係では、SnapMirror で作成された Snapshot コピーのみがデスティネーションボリュームに格納されます。この Snapshot コピーから、プライマリサイトで災害が発生した場合にデータの提供を継続できます。
- 長期保持のデータ保護関係では、Element ソフトウェアで作成されたポイントインタイムの Snapshot コピーと SnapMirror で作成された Snapshot コピーがデスティネーションボリュームに格納されます。たとえば、20 年にわたって毎月の Snapshot コピーを保持することができます。

#### デフォルトポリシー

SnapMirror を初めて起動すると、ソース・ボリュームからデスティネーション・ボリュームへの \_ベースライン転送\_ が実行されます。SnapMirror ポリシー \_ は、ベースラインおよび更新の内容を定義します。

データ保護関係を作成するときに、デフォルトまたはカスタムのポリシーを使用できます。ポリシータイプは、対象となる Snapshot コピーおよび保持するコピー数を決定します。

次の表は、デフォルトのポリシーを示しています。を使用します MirrorLatest 従来のDR関係を作成するポリシー。を使用します MirrorAndVault または Unified7year ユニファイドレプリケーション関係を作成するためのポリシー。同じデスティネーションボリュームにDRと長期保持を設定します。

ポリシー	ポリシータイプ	動作を更新します
MirrorLatest	非同期ミラー	SnapMirror で作成された Snapshot コピーが転送されます。
MirrorAndVault の場合	ミラー - バックアップ	SnapMirror で作成された Snapshot コピーと、前回の更新後に作成された Snapshot コピーの SnapMirror ラベルが「毎日」または「毎週」の場合はそれよりも古い Snapshot コピーが転送されます。

ユニファイド7年	ミラー - バックアップ	SnapMirror で作成された Snapshot コピーと、前回の更新後に作成された Snapshot コピーのうち SnapMirror ラベルが「毎日」、「毎週」、または「毎月」の Snapshot コピーが転送されます。
----------	--------------	---



SnapMirror ポリシーの詳細な背景情報と使用するポリシーのガイダンスについては、を参照してください "[データ保護](#)"。

## SnapMirror ラベルの概要

ポリシータイプが「`m mirror -vault`」のすべてのポリシーには、レプリケートする Snapshot コピーを指定するルールが必要です。たとえば、「毎日」というルールは、「毎日」という SnapMirror ラベルが割り当てられた Snapshot コピーだけを複製する必要があることを示します。SnapMirror ラベルは、Element Snapshot コピーの設定時に割り当てます。

## Element ソースクラスタから ONTAP デスティネーションクラスタへのレプリケーション

SnapMirror を使用して、Element ボリュームの Snapshot コピーを ONTAP デスティネーションシステムにレプリケートできます。これにより、Element サイトで災害が発生した場合でも、ONTAP システムからクライアントに引き続きデータを提供し、サービスのリストア後に Element ソースボリュームを再アクティブ化することができます。

Element ボリュームは ONTAP LUN とほぼ同じです。SnapMirror は、Element ソフトウェアと ONTAP の間のデータ保護関係の初期化時に、Element ボリュームの名前を使用して LUN を作成します。Element から ONTAP へのレプリケーションの要件を満たす既存の LUN がある場合は、その LUN にデータがレプリケートされます。

レプリケーションルールは次のとおりです。

- ONTAP ボリュームに格納できるのは、1 つの Element ボリュームのデータのみです。
- 1 つの ONTAP から複数の Element ボリュームにデータをレプリケートすることはできません。

## ONTAP ソースクラスタから Element デスティネーションクラスタへのレプリケーション

ONTAP 9.4 以降では、ONTAP システムで作成した LUN の Snapshot コピーを Element ボリュームにレプリケートして戻すことができます。

- Element ソースと ONTAP デスティネーションの間にすでに SnapMirror 関係がある場合は、デスティネーションからデータを提供している間に作成された LUN はソースが再アクティブ化されたときに自動的にレプリケートされます。
- SnapMirror 関係がない場合は、ONTAP ソースクラスタと Element デスティネーションクラスタの間に SnapMirror 関係を作成して初期化する必要があります。

レプリケーションルールは次のとおりです。

- レプリケーション関係には「`async`」タイプのポリシーが必要です。  
「ミラー - ヴォールト」タイプのポリシーはサポートされていません。
- iSCSI LUN のみがサポートされます。

- ONTAP ボリュームから Element ボリュームに複数の LUN をレプリケートすることはできません。
- ONTAP ボリュームから複数の Element ボリュームに LUN をレプリケートすることはできません。

#### 前提条件

Element と ONTAP の間にデータ保護関係を設定するには、次の作業を完了しておく必要があります。

- Element クラスタで NetApp Element ソフトウェアバージョン 10.1 以降が実行されている必要があります。
- ONTAP クラスタで ONTAP 9.3 以降が実行されている必要があります。
- ONTAP クラスタで SnapMirror のライセンスが有効になっている必要があります。
- Element クラスタと ONTAP クラスタに、予想されるデータ転送を処理できる十分な容量のボリュームを設定しておく必要があります。
- 「me-vault」ポリシータイプを使用している場合は、Element Snapshot コピーをレプリケートするように SnapMirror ラベルが設定されている必要があります。



このタスクは、Element ソフトウェアの Web UI でのみ実行できます。詳細については、[を参照してください "NetApp Element ソフトウェアのドキュメント"](#)

- ポート 5010 を使用できることを確認しておく必要があります。
- デスティネーションボリュームの移動が必要となることが予想される場合は、ソースとデスティネーションの間にフルメッシュ接続が確立されていることを確認しておく必要があります。Element ソースクラスタ上のすべてのノードが、ONTAP デスティネーションクラスタ上のすべてのノードと通信できる必要があります。

#### サポートの詳細

次の表に、Element から ONTAP へのバックアップのサポートの詳細を示します。

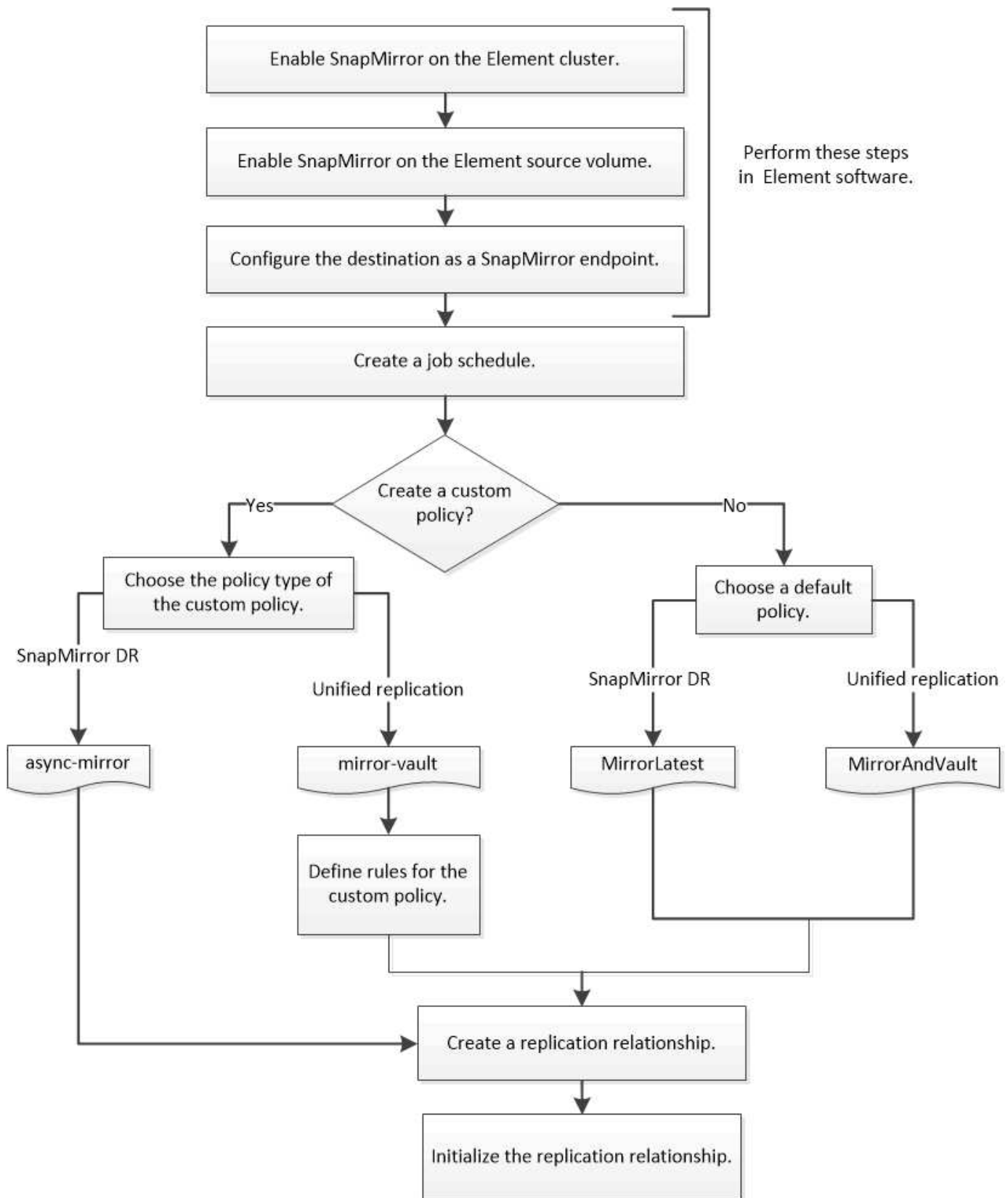
リソースまたは機能	サポートの詳細
-----------	---------

SnapMirror	<ul style="list-style-type: none"> <li>• SnapMirror のリストア機能はサポートされません。</li> <li>• 。 MirrorAllSnapshots および XDPDefault ポリシーはサポートされません。</li> <li>• 「 vault 」 ポリシータイプはサポートされていません。</li> <li>• システム定義のルール 「 all_source_snapshots 」 はサポートされていません。</li> <li>• 「 mirror vault 」 ポリシータイプは、 Element ソフトウェアから ONTAP へのレプリケーションでのみサポートされます。 ONTAP から Element ソフトウェアへのレプリケーションには 「 async 」 を使用します。</li> <li>• 。 -schedule および -prefix のオプション snapmirror policy add-rule はサポートされていません。</li> <li>• 。 -preserve および -quick-resync のオプション snapmirror resync はサポートされていません。</li> <li>• ストレージ効率は維持されません。</li> <li>• ファンアウト構成およびカスケード構成のデータ保護はサポートされません。</li> </ul>
ONTAP	<ul style="list-style-type: none"> <li>• ONTAP Select は、 ONTAP 9.4 および Element 10.3 以降でサポートされます。</li> <li>• Cloud Volumes ONTAP は、 ONTAP 9.5 および Element 11.0 以降でサポートされます。</li> </ul>
要素（ Element ）	<ul style="list-style-type: none"> <li>• ボリュームサイズの上限は 8TiB です。</li> <li>• ボリュームのブロックサイズは 512 バイトにする必要があります。 4K バイトのブロックサイズはサポートされません。</li> <li>• ボリュームサイズは 1MiB の倍数にする必要があります。</li> <li>• ボリューム属性は維持されません。</li> <li>• レプリケートされる Snapshot コピーの最大数は 30 です。</li> </ul>
ネットワーク	<ul style="list-style-type: none"> <li>• 転送ごとに 1 つの TCP 接続を使用できます。</li> <li>• Element ノードは IP アドレスとして指定する必要があります。 DNS ホスト名検索はサポートされません。</li> <li>• IPspace はサポートされません。</li> </ul>
SnapLock	SnapLock ボリュームはサポートされません。
FlexGroup	FlexGroup ボリュームはサポートされません。
SVM DR	SVM DR 構成の ONTAP はサポートされません。
MetroCluster	MetroCluster 構成の ONTAP はサポートされません。

## Element と ONTAP 間のレプリケーションのワークフロー

データを Element から ONTAP にレプリケートするか ONTAP から Element にレプリケートするかに関係を設定し、ジョブスケジュールを設定してポリシーを指定し、関係を作成して初期化する必要があります。デフォルトまたはカスタムのポリシーを使用できます。

このワークフローは、に記載された前提条件のタスクを完了していることを前提としています [前提条件](#)。SnapMirror ポリシーの詳細な背景情報と使用するポリシーのガイダンスについては、を参照してください "[データ保護](#)"。



## Element ソフトウェアで SnapMirror を有効化



## Element クラスタで SnapMirror を有効化

レプリケーション関係を作成する前に、Element クラスタで SnapMirror を有効にする必要があります。このタスクは、Element ソフトウェアの Web UI でのみ実行できます。

作業を開始する前に

- Element クラスタで NetApp Element ソフトウェアバージョン 10.1 以降が実行されている必要があります。
- SnapMirror は、NetApp ONTAP ボリュームで使用される Element クラスタに対してのみ有効にすることができます。

このタスクについて

Element システムの SnapMirror はデフォルトでは無効になっています。SnapMirror は、新規インストール時やアップグレード時に自動的に有効になることはありません。



一度有効にした SnapMirror を無効にすることはできません。SnapMirror 機能を無効にしてデフォルト設定に戻すには、クラスタを工場出荷時のイメージに戻す必要があります。

手順

1. [\* クラスタ\*]、[\* 設定\*] の順にクリックします。
2. クラスタ用の SnapMirror 設定を探します。
3. Enable SnapMirror \* をクリックします。

## Element ソースボリュームで SnapMirror を有効化

レプリケーション関係を作成する前に、Element ソースボリュームで SnapMirror を有効にする必要があります。このタスクは、Element ソフトウェアの Web UI でのみ実行できます。


作業を開始する前に

- Element クラスタで SnapMirror を有効にしておく必要があります。
- ボリュームのブロックサイズは 512 バイトにする必要があります。
- ボリュームが Element リモートレプリケーションに参加していない必要があります。
- ボリュームのアクセスタイプは「レプリケーションターゲット」にしないでください。

このタスクについて

以下の手順は、ボリュームがすでに存在することを前提としています。SnapMirror は、ボリュームを作成またはクローニングするときに有効にすることもできます。

手順

1. [\* Management] > [\* Volumes] を選択します。
2. を選択します  ボタンをクリックします。
3. ドロップダウンメニューで、\* Edit \* を選択します。

4. ボリュームの編集 \* ダイアログで、 \* SnapMirror を有効にする \* を選択します。
5. 「変更を保存」を選択します。

## SnapMirror エンドポイントを作成します

レプリケーション関係を作成する前に、 SnapMirror エンドポイントを作成する必要があります。このタスクは、 Element ソフトウェアの Web UI でのみ実行できます。

作業を開始する前に

Element クラスタで SnapMirror を有効にしておく必要があります。

手順

1. [ \* データ保護 \* > \* SnapMirror エンドポイント \* ] をクリックします。
2. [ エンドポイントの作成 \* ] をクリックします。
3. Create a New Endpoint \* ダイアログで、 ONTAP クラスタ管理 IP アドレスを入力します。
4. ONTAP クラスタ管理者のユーザ ID とパスワードを入力します。
5. [ エンドポイントの作成 \* ] をクリックします。

## レプリケーション関係を設定

レプリケーションジョブスケジュールを作成

データを Element から ONTAP にレプリケートするか ONTAP から Element にレプリケートするかに関係を設定し、ジョブスケジュールを設定してポリシーを指定し、関係を作成して初期化する必要があります。デフォルトまたはカスタムのポリシーを使用できます。

を使用できます `job schedule cron create` レプリケーションジョブスケジュールを作成するコマンド。ジョブスケジュールでは、スケジュールの割り当て先のデータ保護関係が SnapMirror によって自動的に更新されるタイミングを決定します。

このタスクについて

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

ステップ

1. ジョブスケジュールを作成します。

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

の場合 `-month`、`-dayofweek` および `-hour` を指定できます ``all`` 毎月、曜日、および時間ごとにジョブを実行します。

ONTAP 9.10.1 以降では、ジョブスケジュールに SVM を追加できます。

```
job schedule cron create -name job_name -vserver Vserver_name -month month
```

```
-dayofweek day_of_week -day day_of_month -hour hour -minute minute
```

次の例は、という名前のジョブスケジュールを作成します my\_weekly 土曜日の午前3時に実行されます。

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

レプリケーションポリシーをカスタマイズします

カスタムレプリケーションポリシーを作成する

レプリケーション関係の作成時には、デフォルトまたはカスタムのポリシーを使用できます。カスタムのユニファイドレプリケーションポリシーの場合は、初期化と更新の際に転送する Snapshot コピーを決定する 1 つ以上の *rules* を定義する必要があります。

関係のデフォルトポリシーが適切でない場合は、カスタムレプリケーションポリシーを作成できます。たとえば、ネットワーク転送時にデータを圧縮したり、Snapshot コピーを転送するための SnapMirror の試行回数を変更したりできます。

このタスクについて

レプリケーションポリシーの *\_policy type\_of* によって、サポートされる関係のタイプが決まります。次の表は、使用可能なポリシータイプを示しています。

ポリシータイプ	関係タイプ
非同期ミラー	SnapMirror DR
ミラー - バックアップ	ユニファイドレプリケーション

ステップ

1. カスタムレプリケーションポリシーを作成します。

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

コマンド構文全体については、マニュアルページを参照してください。

ONTAP 9.5以降では、を使用して、SnapMirror Synchronous関係の共通のSnapshotコピースケジュールを作成するスケジュールを指定できます *-common-snapshot-schedule* パラメータデフォルトでは、SnapMirror Synchronous 関係の共通の Snapshot コピースケジュールは 1 時間です。SnapMirror Synchronous 関係の Snapshot コピースケジュールの値は、30 分から 2 時間までの範囲で指定できます。

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

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

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

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

完了後

「me-vault」ポリシータイプの場合は、初期化および更新時に転送する Snapshot コピーを決定するルールを定義する必要があります。

を使用します `snapmirror policy show` コマンドを入力して、SnapMirrorポリシーが作成されたことを確認します。コマンド構文全体については、マニュアルページを参照してください。

ポリシーのルールを定義します

ポリシータイプが「`m mirror -vault`」のカスタムポリシーの場合、初期化および更新時に転送する Snapshot コピーを決定するルールを少なくとも 1 つ定義する必要があります。また、ポリシータイプが「ミラー - ヴォールト」のデフォルトポリシーのルールを定義することもできます。

このタスクについて

ポリシータイプが「`m mirror -vault`」のすべてのポリシーには、レプリケートする Snapshot コピーを指定するルールが必要です。たとえば、「`bi-monthly`」ルールは、SnapMirror ラベルが「`bi-monthly`」に割り当てられた Snapshot コピーだけをレプリケートする必要があることを指定します。SnapMirror ラベルは、Element Snapshot コピーの設定時に割り当てます。

各ポリシータイプは、システム定義の 1 つ以上のルールに関連付けられます。これらのルールは、ポリシータイプの指定時にポリシーに自動的に割り当てられます。次の表は、システム定義のルールを示しています。

システム定義のルール	ポリシータイプで使用されます	結果
sm_created	async-mirror 、 mirror-vault のいずれかです	SnapMirror で作成された Snapshot コピーが初期化および更新の際に転送されます。
毎日	ミラー - バックアップ	SnapMirror ラベルが「毎日」のソース上の新しい Snapshot コピーが初期化および更新の際に転送されます。

毎週	ミラー - バックアップ	SnapMirror ラベルが「weekly」のソース上の新しい Snapshot コピーは、初期化および更新の際に転送されます。
毎月	ミラー - バックアップ	SnapMirror ラベルが「アース」の新しい Snapshot コピーがソースに転送され、初期化と更新が行われます。

デフォルトポリシーまたはカスタムポリシーに対して、必要に応じて追加のルールを指定できます。例：

- をクリックします MirrorAndVault ポリシーの場合は、SnapMirrorラベルが「bi-monthly」のソースSnapshotコピーを照合する「bi-monthly」というルールを作成できます。
- 「me-vault」ポリシータイプのカスタムポリシーの場合は、「bi-weekly」というルールを作成し、ソース上の Snapshot コピーと「bi-weekly」 SnapMirror ラベルを照合します。

## ステップ

1. ポリシーのルールを定義します。

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

コマンド構文全体については、マニュアルページを参照してください。

次の例は、SnapMirrorラベルのルールを追加します bi-monthly をデフォルトに設定します MirrorAndVault ポリシー：

```
cluster_dst::> snapmirror policy add-rule -vserver svm1 -policy
MirrorAndVault -snapmirror-label bi-monthly -keep 6
```

次の例は、SnapMirrorラベルのルールを追加します bi-weekly カスタムに my\_snapvault ポリシー：

```
cluster_dst::> snapmirror policy add-rule -vserver svm1 -policy
my_snapvault -snapmirror-label bi-weekly -keep 26
```

次の例は、SnapMirrorラベルのルールを追加します app\_consistent カスタムに Sync ポリシー：

```
cluster_dst::> snapmirror policy add-rule -vserver svm1 -policy Sync
-snapmirror-label app_consistent -keep 1
```

この SnapMirror ラベルに一致する Snapshot コピーをソースクラスタからレプリケートできます。

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

## レプリケーション関係を作成

**Element** ソースから **ONTAP** デスティネーションへの関係を作成します

プライマリストレージのソースボリュームとセカンダリストレージのデスティネーションボリュームの関係は、「a\_data 保護関係」と呼ばれます。を使用できます `snapmirror create` コマンドを使用して、ElementソースからONTAP デスティネーション、またはONTAP ソースからElementデスティネーションへのデータ保護関係を作成します。

SnapMirror を使用して、Element ボリュームの Snapshot コピーを ONTAP デスティネーションシステムにレプリケートできます。これにより、Element サイトで災害が発生した場合でも、ONTAP システムからクライアントに引き続きデータを提供し、サービスのリストア後に Element ソースボリュームを再アクティブ化することができます。

作業を開始する前に

- レプリケートするボリュームを含む Element ノードから ONTAP にアクセスできるようにしておく必要があります。
- Element ボリュームの SnapMirror レプリケーションを有効にしておく必要があります。
- 「me-vault」ポリシータイプを使用している場合は、Element Snapshot コピーをレプリケートするように SnapMirror ラベルが設定されている必要があります。



このタスクは、Element ソフトウェアの Web UI でのみ実行できます。詳細については、[を参照してください "Element のドキュメント"](#)。

このタスクについて

Elementソースパスはの形式で指定する必要があります `hostip:/lun/name`` ここで、「LUN」は実際の文字列「LUN」およびです `name` は、Elementボリュームの名前です。

Element ボリュームは ONTAP LUN とほぼ同じです。SnapMirror は、Element ソフトウェアと ONTAP の間のデータ保護関係の初期化時に、Element ボリュームの名前を使用して LUN を作成します。Element ソフトウェアから ONTAP へのレプリケーションの要件を満たす既存の LUN がある場合は、その LUN にデータがレプリケートされます。

レプリケーションルールは次のとおりです。

- ONTAP ボリュームに格納できるのは、1 つの Element ボリュームのデータのみです。
- 1 つの ONTAP から複数の Element ボリュームにデータをレプリケートすることはできません。

ONTAP 9.3 以前では、デスティネーションボリュームに格納できる Snapshot コピーは最大 251 個です。ONTAP 9.4 以降では、デスティネーションボリュームに格納できる Snapshot コピーは最大 1019 個です。

## ステップ

1. デスティネーションクラスタから、Element ソースから ONTAP デスティネーションへのレプリケーション関係を作成します。

```
snapmirror create -source-path hostip:/lun/name -destination-path SVM:volume  
|cluster://SVM/volume -type XDP -schedule schedule -policy policy
```

コマンド構文全体については、マニュアルページを参照してください。

次の例は、デフォルトのを使用して、SnapMirror DR関係を作成します MirrorLatest ポリシー：

```
cluster_dst:> snapmirror create -source-path 10.0.0.11:/lun/0005  
-destination-path svm_backup:volA_dst -type XDP -schedule my_daily  
-policy MirrorLatest
```

次の例は、デフォルトを使用して、ユニファイドレプリケーション関係を作成します MirrorAndVault ポリシー：

```
cluster_dst:> snapmirror create -source-path 10.0.0.11:/lun/0005  
-destination-path svm_backup:volA_dst -type XDP -schedule my_daily  
-policy MirrorAndVault
```

次の例は、を使用してユニファイドレプリケーション関係を作成します Unified7year ポリシー：

```
cluster_dst:> snapmirror create -source-path 10.0.0.11:/lun/0005  
-destination-path svm_backup:volA_dst -type XDP -schedule my_daily  
-policy Unified7year
```

次の例は、カスタムのを使用してユニファイドレプリケーション関係を作成します my\_unified ポリシー：

```
cluster_dst:> snapmirror create -source-path 10.0.0.11:/lun/0005  
-destination-path svm_backup:volA_dst -type XDP -schedule my_daily  
-policy my_unified
```

## 完了後

を使用します `snapmirror show` コマンドを実行して、SnapMirror関係が作成されたことを確認します。コマンド構文全体については、マニュアルページを参照してください。

**ONTAP** ソースから **Element** デスティネーションへの関係を作成します

ONTAP 9.4 以降では、SnapMirror を使用して、ONTAP ソースで作成した LUN の Snapshot コピーを Element デスティネーションにレプリケートできます。LUN を使用

して ONTAP から Element ソフトウェアにデータを移行することができます。

作業を開始する前に

- Element デスティネーションノードから ONTAP にアクセスできるようにしておく必要があります。
- Element ボリュームの SnapMirror レプリケーションを有効にしておく必要があります。

このタスクについて

Elementのデスティネーションパスはの形式で指定する必要があります `hostip:/lun/name`` ここで、「LUN」は実際の文字列「LUN」およびです `name` は、Elementボリュームの名前です。

レプリケーションルールは次のとおりです。

- レプリケーション関係には「async」タイプのポリシーが必要です。

デフォルトまたはカスタムのポリシーを使用できます。

- iSCSI LUN のみがサポートされます。
- ONTAP ボリュームから Element ボリュームに複数の LUN をレプリケートすることはできません。
- ONTAP ボリュームから複数の Element ボリュームに LUN をレプリケートすることはできません。

ステップ

1. ONTAP ソースから Element デスティネーションへのレプリケーション関係を作成します。

```
snapmirror create -source-path SVM:volume|cluster://SVM/volume -destination-path hostip:/lun/name -type XDP -schedule schedule -policy policy
```

コマンド構文全体については、マニュアルページを参照してください。

次の例は、デフォルトのを使用して、SnapMirror DR関係を作成します MirrorLatest ポリシー：

```
cluster_dst:> snapmirror create -source-path svm_1:volA_dst -destination-path 10.0.0.11:/lun/0005 -type XDP -schedule my_daily -policy MirrorLatest
```

次の例は、カスタムのを使用してSnapMirror DR関係を作成します my\_mirror ポリシー：

```
cluster_dst:> snapmirror create -source-path svm_1:volA_dst -destination-path 10.0.0.11:/lun/0005 -type XDP -schedule my_daily -policy my_mirror
```

完了後

を使用します `snapmirror show` コマンドを実行して、SnapMirror関係が作成されたことを確認します。コマンド構文全体については、マニュアルページを参照してください。



## レプリケーション関係を初期化

すべての関係タイプでは、初期化の際に *baseline transfer*：ソースボリュームの Snapshot コピーが作成され、そのコピーおよびコピーが参照するすべてのデータブロックがデスティネーションボリュームに転送されます。

作業を開始する前に

- レプリケートするボリュームを含む Element ノードから ONTAP にアクセスできるようにしておく必要があります。
- Element ボリュームの SnapMirror レプリケーションを有効にしておく必要があります。
- 「me-vault」ポリシータイプを使用している場合は、Element Snapshot コピーをレプリケートするように SnapMirror ラベルが設定されている必要があります。

このタスクについて

Elementソースパスはの形式で指定する必要があります *hostip:/lun/name*。ここで、「LUN」は実際の文字列「LUN」およびです、*name* は、Elementボリュームの名前です。

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

ONTAP ソースから Element デスティネーションへの関係の初期化に何らかの理由で失敗した場合は、問題（無効な LUN 名など）を修正したあとも初期化が失敗します。回避策は次のとおりです。



1. 関係を削除します。
2. Element デスティネーションボリュームを削除します。
3. 新しい Element デスティネーションボリュームを作成
4. ONTAP ソースから Element デスティネーションボリュームへの新しい関係を作成して初期化します。

## ステップ

1. レプリケーション関係を初期化します。

```
snapmirror initialize -source-path hostip:/lun/name -destination-path  
SVM:volume|cluster://SVM/volume
```

コマンド構文全体については、マニュアルページを参照してください。

次の例は、ソースボリューム間の関係を初期化します 0005（IPアドレス10.0.0.11、デスティネーションボリューム volA\_dst オン svm\_backup）:

```
cluster_dst::> snapmirror initialize -source-path 10.0.0.11:/lun/0005  
-destination-path svm_backup:volA_dst
```

## SnapMirror DR デスティネーションボリュームからのデータの提供

デスティネーションボリュームを書き込み可能にします

災害によって SnapMirror DR 関係のプライマリサイトが機能しなくなった場合は、システム停止を最小限に抑えてデスティネーションボリュームからデータを提供できます。プライマリサイトでサービスが復旧したら、ソースボリュームを再アクティブ化できます。

デスティネーションボリュームからクライアントにデータを提供する前に、そのボリュームを書き込み可能にする必要があります。を使用できます `snapmirror quiesce` デスティネーションへのスケジュールされた転送を停止するコマンドを使用します `snapmirror abort` 実行中の転送を停止するコマンド、および `snapmirror break` デスティネーションを書き込み可能にするコマンド。

このタスクについて

Elementソースパスはの形式で指定する必要があります `hostip:/lun/name`` ここで、「LUN」は実際の文字列「LUN」およびです `name` は、Elementボリュームの名前です。

手順

1. デスティネーションへのスケジュールされた転送を停止します。

```
snapmirror quiesce -source-path hostip:/lun/name -destination-path SVM:volume  
|cluster://SVM/volume
```

コマンド構文全体については、マニュアルページを参照してください。

次の例は、ソースボリューム間のスケジュールされた転送を停止します 0005（IPアドレス10.0.0.11、デスティネーションボリューム volA\_dst オン svm\_backup）:

```
cluster_dst:> snapmirror quiesce -source-path 10.0.0.11:/lun/0005  
-destination-path svm_backup:volA_dst
```

2. デスティネーションへの実行中の転送を停止します。

```
snapmirror abort -source-path hostip:/lun/name -destination-path SVM:volume  
|cluster://SVM/volume
```

コマンド構文全体については、マニュアルページを参照してください。

次の例は、ソースボリューム間の実行中の転送を停止します 0005（IPアドレス10.0.0.11、デスティネーションボリューム volA\_dst オン svm\_backup）:

```
cluster_dst:> snapmirror abort -source-path 10.0.0.11:/lun/0005  
-destination-path svm_backup:volA_dst
```

3. SnapMirror DR 関係を解除します。

```
snapmirror break -source-path hostip:/lun/name -destination-path SVM:volume  
|cluster://SVM/volume
```

コマンド構文全体については、マニュアルページを参照してください。

次の例は、ソースボリューム間の関係を解除します 0005（IPアドレス10.0.0.11、デスティネーションボリューム volA\_dst オン svm\_backup デスティネーションボリュームを指定します volA\_dst オン svm\_backup）:

```
cluster_dst::> snapmirror break -source-path 10.0.0.11:/lun/0005  
-destination-path svm_backup:volA_dst
```

## データアクセス用のデスティネーションボリュームを設定

デスティネーションボリュームを書き込み可能にしたあとで、データにアクセスできるようにそのボリュームを設定する必要があります。SAN ホストは、ソースボリュームが再アクティブ化されるまでの間、デスティネーションボリュームのデータにアクセスできません。

1. Element LUN を適切なイニシエータグループにマッピングします。
2. SAN ホストイニシエータから SAN LIF への iSCSI セッションを作成します。
3. SAN クライアントで、ストレージの再スキャンを実行して接続された LUN を検出します。

## 元のソースボリュームを再有効化

デスティネーションからデータを提供する必要がなくなった場合は、ソースボリュームとデスティネーションボリュームの間で元のデータ保護関係を再確立できます。

### このタスクについて

以下の手順は、元のソースボリュームにあるベースラインが損なわれていないことを前提としています。ベースラインが損なわれている場合は、手順を実行する前に、データの提供元のボリュームと元のソースボリュームの間の関係を作成して初期化する必要があります。

Elementソースパスはの形式で指定する必要があります `hostip:/lun/name`。ここで、「LUN」は実際の文字列「LUN」およびです、`name` は、Elementボリュームの名前です。

ONTAP 9.4 以降では、ONTAP デスティネーションからデータを提供している間に作成された LUN の Snapshot コピーは Element ソースが再アクティブ化されたときに自動的にレプリケートされます。

レプリケーションルールは次のとおりです。

- iSCSI LUN のみがサポートされます。
- ONTAP ボリュームから Element ボリュームに複数の LUN をレプリケートすることはできません。
- ONTAP ボリュームから複数の Element ボリュームに LUN をレプリケートすることはできません。

## 手順

### 1. 元のデータ保護関係を削除します。

```
snapmirror delete -source-path SVM:volume|cluster://SVM/volume -destination  
-path hostip:/lun/name -policy policy
```

コマンド構文全体については、マニュアルページを参照してください。

次の例は、元のソースボリューム間の関係を削除します。0005 IPアドレス10.0.0.11、およびデータの提供元のボリューム volA\_dst オン svm\_backup:

```
cluster_dst:> snapmirror delete -source-path 10.0.0.11:/lun/0005  
-policy MirrorLatest -destination-path svm_backup:volA_dst
```

### 2. 元のデータ保護関係を反転します。

```
snapmirror resync -source-path SVM:volume|cluster://SVM/volume -destination  
-path hostip:/lun/name -policy policy
```

コマンド構文全体については、マニュアルページを参照してください。

再同期の際にベースライン転送は不要ですが、再同期には時間がかかる場合があります。再同期はオフピークの時間帯に実行することを推奨します。

次の例は、元のソースボリューム間の関係を反転します。0005 IPアドレス10.0.0.11、およびデータの提供元のボリューム volA\_dst オン svm\_backup:

```
cluster_dst:> snapmirror resync -source-path svm_backup:volA_dst  
-destination-path 10.0.0.11:/lun/0005 -policy MirrorLatest
```

### 3. 反転した関係を更新します。

```
snapmirror update -source-path SVM:volume|cluster://SVM/volume -destination  
-path hostip:/lun/name
```

コマンド構文全体については、マニュアルページを参照してください。



ソースとデスティネーションに共通の Snapshot コピーが存在しない場合、このコマンドは失敗します。使用 `snapmirror initialize` 関係を再初期化してください。

次の例は、データの提供元のボリューム間の関係を更新します。volA\_dst オン svm\_backup`および元のソースボリューム `0005 IPアドレス10.0.0.11の場合:

```
cluster_dst:> snapmirror update -source-path svm_backup:volA_dst  
-destination-path 10.0.0.11:/lun/0005
```

### 4. 反転した関係のスケジュールされた転送を停止します。

```
snapmirror quiesce -source-path SVM:volume|cluster://SVM/volume -destination  
-path hostip:/lun/name
```

コマンド構文全体については、マニュアルページを参照してください。

次の例は、データの提供元のボリューム間のスケジュールされた転送を停止します。volA\_dst オン svm\_backup`および元のソースボリューム `0005 IPアドレス10.0.0.11の場合：

```
cluster_dst::> snapmirror quiesce -source-path svm_backup:volA_dst  
-destination-path 10.0.0.11:/lun/0005
```

#### 5. 反転した関係の実行中の転送を停止します。

```
snapmirror abort -source-path SVM:volume|cluster://SVM/volume -destination  
-path hostip:/lun/name
```

コマンド構文全体については、マニュアルページを参照してください。

次の例は、データの提供元のボリューム間の実行中の転送を停止します。volA\_dst オン svm\_backup`および元のソースボリューム `0005 IPアドレス10.0.0.11の場合：

```
cluster_dst::> snapmirror abort -source-path svm_backup:volA_dst  
-destination-path 10.0.0.11:/lun/0005
```

#### 6. 反転した関係を解除します。

```
snapmirror break -source-path SVM:volume|cluster://SVM/volume -destination  
-path hostip:/lun/name
```

コマンド構文全体については、マニュアルページを参照してください。

次の例は、データの提供元のボリューム間の関係を解除します。volA\_dst オン svm\_backup`および元のソースボリューム `0005 IPアドレス10.0.0.11の場合：

```
cluster_dst::> snapmirror break -source-path svm_backup:volA_dst  
-destination-path 10.0.0.11:/lun/0005
```

#### 7. 反転したデータ保護関係を削除します。

```
snapmirror delete -source-path SVM:volume|cluster://SVM/volume -destination  
-path hostip:/lun/name -policy policy
```

コマンド構文全体については、マニュアルページを参照してください。

次の例は、元のソースボリューム間の反転した関係を削除します。0005 IPアドレス10.0.0.11、およびデータの提供元のボリューム volA\_dst オン svm\_backup：

```
cluster_src::> snapmirror delete -source-path svm_backup:volA_dst  
-destination-path 10.0.0.11:/lun/0005 -policy MirrorLatest
```

## 8. 元のデータ保護関係を再確立します。

```
snapmirror resync -source-path hostip:/lun/name -destination-path  
SVM:volume|cluster://SVM/volume
```

コマンド構文全体については、マニュアルページを参照してください。

次の例は、元のソースボリューム間の関係を再確立します。 0005 IPアドレス10.0.0.11、元のデスティネーションボリューム volA\_dst オン svm\_backup：

```
cluster_dst::> snapmirror resync -source-path 10.0.0.11:/lun/0005  
-destination-path svm_backup:volA_dst
```

完了後

を使用します `snapmirror show` コマンドを実行して、SnapMirror関係が作成されたことを確認します。コマンド構文全体については、マニュアルページを参照してください。

## レプリケーション関係を手動で更新

ネットワークエラーによって更新が失敗した場合は、レプリケーション関係を手動で更新しなければならないことがあります。

このタスクについて

Elementソースパスはの形式で指定する必要があります `hostip:/lun/name`。ここで、「LUN」は実際の文字列「LUN」 およびです `name` は、Elementボリュームの名前です。

手順

### 1. レプリケーション関係を手動で更新します。

```
snapmirror update -source-path hostip:/lun/name -destination-path SVM:volume  
|cluster://SVM/volume
```

コマンド構文全体については、マニュアルページを参照してください。



ソースとデスティネーションに共通の Snapshot コピーが存在しない場合、このコマンドは失敗します。使用 `snapmirror initialize` 関係を再初期化してください。

次の例は、ソースボリューム間の関係を更新します 0005 （IPアドレス10.0.0.11、デスティネーションボリューム volA\_dst オン svm\_backup）：

```
cluster_src::> snapmirror update -source-path 10.0.0.11:/lun/0005  
-destination-path svm_backup:volA_dst
```

## レプリケーション関係を再同期

デスティネーションボリュームを書き込み可能にしたあと、ソースボリュームとデスティネーションボリュームに共通の Snapshot コピーが存在しないために更新が失敗したあと、または関係のレプリケーションポリシーを変更した場合には、レプリケーション関係の再同期が必要です。

このタスクについて

再同期の際にベースライン転送は不要ですが、再同期には時間がかかる場合があります。再同期はオフピークの時間帯に実行することを推奨します。

Elementソースパスはの形式で指定する必要があります `hostip:/lun/name` ここで、「LUN」は実際の文字列「LUN」 およびです `name` は、Elementボリュームの名前です。

### ステップ

1. ソースボリュームとデスティネーションボリュームを再同期します。

```
snapmirror resync -source-path hostip:/lun/name -destination-path SVM:volume  
|cluster://SVM/volume -type XDP -policy policy
```

コマンド構文全体については、マニュアルページを参照してください。

次の例は、ソースボリューム間の関係を再同期します 0005（IPアドレス10.0.0.11、デスティネーションボリューム volA\_dst オン svm\_backup）:

```
cluster_dst::> snapmirror resync -source-path 10.0.0.11:/lun/0005  
-policy MirrorLatest -destination-path svm_backup:volA_dst
```

# イベント、パフォーマンス、健全性の監視

## System Managerを使用してクラスタパフォーマンスを監視する

### System Manager を使用してクラスタパフォーマンスを監視する

このセクションのトピックでは、ONTAP 9.7 以降のリリースで System Manager を使用してクラスタの健全性とパフォーマンスを管理する方法を説明します。

System Manager ダッシュボードでシステムに関する情報を表示することで、クラスタパフォーマンスを監視できます。ダッシュボードには、重要なアラートと通知に関する情報、ストレージ階層とボリュームの効率性と容量、クラスタで使用できるノード、HA ペアのノードのステータス、最もアクティブなアプリケーションとオブジェクト、およびクラスタまたはノードのパフォーマンス指標。

ダッシュボードでは、次の情報を確認できます。

- **\* Health \*** : クラスタの健全性はどの程度ですか？
- **\* 容量 \*** : クラスタで利用可能な容量
- **\* パフォーマンス \*** : レイテンシ、IOPS、スループットを基準に、クラスタのパフォーマンスはどの程度向上していますか？
- **\* ネットワーク \*** : ポート、インターフェイス、Storage VM などのホストとストレージオブジェクトを使用してネットワークをどのように構成しますか？

健全性と容量の概要で、をクリックできます → 追加情報を表示してタスクを実行します。

パフォーマンスの概要では、時間、日、週、月、または年に基づく指標を表示できます。

ネットワークの概要では、ネットワーク内の各オブジェクトの数（「8 NVMe/FC ポート」など）が表示されます。番号をクリックすると、各ネットワークオブジェクトの詳細を確認できます。

### クラスタダッシュボードにパフォーマンスを表示します

ダッシュボードを使用すると、追加または移動するワークロードについて、十分な情報に基づいて意思決定を下すことができます。また、ピーク使用時間を確認して、潜在的な変更を計画することもできます。

パフォーマンスの値は 3 秒ごとに更新され、パフォーマンスグラフは 15 秒ごとに更新されます。

#### 手順

1. [**\* ダッシュボード \***] をクリックします。
2. [**\* パフォーマンス \***] で、間隔を選択します。

### ホットボリュームやその他のオブジェクトを特定します

アクセス頻度の高いボリューム（ホットボリューム）とデータ（ホットオブジェクト）



を特定して、クラスタのパフォーマンスを向上させます。



ONTAP 9.10.1以降では、ファイルシステム分析のアクティビティ追跡機能を使用してボリューム内のホットオブジェクトを監視できます。

#### 手順

1. [ストレージ]、[ボリューム]の順にクリックします。
2. IOPS、レイテンシ、およびスループットの列をフィルタリングして、アクセス頻度の高いボリュームとデータを表示します。

## QoS を変更する

ONTAP 9.8以降では、ストレージのプロビジョニング時に **サービス品質 (QoS)** はデフォルトで有効になっています。QoS を無効にするか、プロビジョニングプロセスでカスタムの QoS ポリシーを選択できます。ストレージのプロビジョニングが完了したあとに QoS を変更することもできます。

#### 手順

1. System Managerで、[ストレージ]\*を選択し、[ボリューム]\*を選択します。
2. QoSを変更するボリュームの横にあるを選択します。次に\*[編集]\*をクリックします。

## リスクを監視

ONTAP 9.10.0 以降では、System Manager を使用して、Active IQ デジタルアドバイザーから報告されたリスクを監視できます。ONTAP 9.10.1 以降の System Manager を使用してリスクを確認することもできます。

NetApp Active IQ Digital Advisor は、リスクを軽減し、ストレージ環境のパフォーマンスと効率を向上させる機会を報告します。System Manager を使用すると、Active IQ によって報告されるリスクを把握し、ストレージの管理や可用性の向上、セキュリティの向上、ストレージパフォーマンスの向上に役立つ実用的な情報を受け取ることができます。

### Active IQ アカウントへのリンク

Active IQ からリスクに関する情報を受け取るには、まず System Manager から Active IQ アカウントにリンクします。

#### 手順

1. System Manager で、\* Cluster > Settings \* の順にクリックします。
2. [Active IQ Registration](登録\*)で[\*Register](登録\*)をクリックします
3. Active IQ のクレデンシャルを入力します。
4. クレデンシャルの認証が完了したら、「\* 確認」をクリックして Active IQ と System Manager \* をリンクします。

リスクの数を表示します

ONTAP 9.10.0 以降では、System Manager のダッシュボードから Active IQ で報告されたリスクの数を確認できます。

作業を開始する前に

System Manager から Active IQ アカウントへの接続を確立する必要があります。を参照してください [Active IQ アカウントへのリンク](#)。

手順

1. System Manager で、\* ダッシュボード \* をクリックします。
2. \* Health \* セクションで、報告されたリスクの数を確認します。



リスクの数を示すメッセージをクリックすると、各リスクの詳細情報を確認できます。を参照してください [リスクの詳細を表示します](#)。

リスクの詳細を表示します

ONTAP 9.10.0 以降では、Active IQ で報告されるリスクが影響領域別に分類される方法を System Manager で確認できます。報告された各リスク、システムへの潜在的な影響、対処方法に関する詳細情報も確認できます。

作業を開始する前に

System Manager から Active IQ アカウントへの接続を確立する必要があります。を参照してください [Active IQ アカウントへのリンク](#)。

手順

1. [\* イベント ] > [ すべてのイベント \* ] をクリックします。
2. 概要 \* セクションの \* Active IQ 提案 \* で、各インパクトエリアカテゴリのリスク数を表示します。リスクカテゴリは次のとおりです。
  - パフォーマンスと効率性
  - 可用性と保護
  - 容量
  - 設定
  - セキュリティ
3. Active IQ Suggestions \* (リスク提案 \*) タブをクリックして、以下を含む各リスクに関する情報を表示します。
  - システムへの影響のレベル
  - リスクのカテゴリ
  - 影響を受けるノード
  - 必要な軽減のタイプ
  - 対処方法

## リスクを承認

ONTAP 9.10.1 以降のシステムでは、System Manager を使用して開いているリスクを確認することができます。

### 手順

1. System Manager で、の手順を実行してリスクのリストを表示します [リスクの詳細を表示します](#)。
2. 承認する未完了リスクのリスク名をクリックします。
3. 次のフィールドに情報を入力します。
  - リマインダ（日付）
  - 理由
  - コメント
4. [\* Acknowledge（確認）] をクリックし



リスクを承認したあと、変更が Active IQ の提案リストに反映されるまでに数分かかります。

## リスクの承認を取り消します

ONTAP 9.10.1 以降の System Manager を使用して、以前に確認されたリスクの承認を取り消すことができます。

### 手順

1. System Manager で、の手順を実行してリスクのリストを表示します [リスクの詳細を表示します](#)。
2. 承認を取り消すリスクの名前をクリックします。
3. 次のフィールドに情報を入力します。
  - 理由
  - コメント
4. [承認の取り消し\*] をクリックします。



リスクを承認しないと、Active IQ の提案リストに変更が反映されるまでに数分かかります。

## System Managerの分析情報

ONTAP 9.11.1以降では、システムのパフォーマンスとセキュリティの最適化に役立つ\_insights\_がSystem Managerに表示されます。



インサイトの表示、カスタマイズ、応答については、"[システムの最適化に役立つ分析情報を取得できます](#)"

## 容量に関する分析

System Managerでは、システムの容量の状況に応じて次の情報を表示できます。

インサイト	重大度	条件	の修正
ローカル階層のスペースが不足しています	リスクを修正	1つ以上のローカル階層の使用率が95%を超えており、急速に拡張しています。既存のワークロードを拡張できない場合や、極端な場合には、既存のワークロードのスペースが不足して失敗することがあります。	<p>推奨される修正：次のいずれかのオプションを実行します。</p> <ul style="list-style-type: none"> <li>• ボリュームリカバリキューをクリアします。</li> <li>• シックプロビジョニングされたボリュームでシンプロビジョニングを有効にして、トラップされたストレージを解放します。</li> <li>• 別のローカル階層にボリュームを移動します。</li> <li>• 不要なSnapshotコピーを削除します。</li> <li>• ボリューム内の不要なディレクトリまたはファイルを削除します。</li> <li>• FabricPoolを有効にして、データをクラウドに階層化します。</li> </ul>
アプリケーションにスペースが不足している	要注意	95%を超えていますが、自動拡張が有効になっていません。	<p>推奨：現在の容量の150%まで自動拡張を有効にします。</p> <p>その他のオプション：</p> <ul style="list-style-type: none"> <li>• Snapshotコピーを削除してスペースを再生します。</li> <li>• ボリュームのサイズを変更します。</li> <li>• ディレクトリまたはファイルを削除します。</li> </ul>
FlexGroupボリュームの容量が不均衡になっています	ストレージの最適化	1つ以上のFlexGroupのコンスティチュエントボリュームのサイズが時間の経過とともに不均衡になっており、使用容量が不均衡になっています。コンスティチュエントボリュームがフルになると、書き込みエラーが発生する可能性があります。	<p>推奨：FlexGroupボリュームをリバランシングします。</p>

Storage VMの容量が不足しています	ストレージの最適化	1つ以上のStorage VMが最大容量に近づいています。 Storage VMが最大容量に達しても、新規または既存のボリュームに追加のスペースをプロビジョニングすることはできません。	推奨：可能であれば、Storage VMの最大容量を増やします。
-----------------------	-----------	---	----------------------------------

## セキュリティに関する分析情報

データやシステムのセキュリティを危険にさらす可能性がある状況に対して、System Managerでは次の分析情報を表示できます。

インサイト	重大度	条件	の修正
ボリュームは引き続きランサムウェア対策学習モード	要注意	1つ以上のボリュームが90日間Anti-Ransomware Learningモードになっています。	推奨：これらのボリュームに対して、ランサムウェア対策のアクティブモードを有効にします。
ボリュームでSnapshotコピーの自動削除が有効になる	要注意	Snapshotの自動削除が1つ以上のボリュームで有効になっています。	推奨：Snapshotコピーの自動削除を無効にします。そうしないと、ランサムウェア攻撃が発生した場合に、これらのボリュームのデータリカバリが不可能になる可能性があります。
ボリュームにSnapshotポリシーがありません	要注意	1つ以上のボリュームに適切なSnapshotポリシーが関連付けられていません。	推奨：Snapshotポリシーが割り当てられていないボリュームにSnapshotポリシーを適用します。そうしないと、ランサムウェア攻撃が発生した場合に、これらのボリュームのデータリカバリが不可能になる可能性があります。
ネイティブFPolicyが設定されていない	ベストプラクティス	ネイティブFPolicyが1つ以上のNAS Storage VMに設定されていません。	推奨：重要：拡張機能をブロックすると、予期しない結果になる可能性があります。9.11.1以降では、Storage VMに対してネイティブのFPolicyを有効にすることができます。これにより、ランサムウェア攻撃に使用されたことがわかっている3,000を超えるファイル拡張子がブロックされます。 <a href="#">"ネイティブFPolicyの設定"</a> NAS Storage VMを使用して、環境内のボリュームへの書き込みを許可または許可しないファイル拡張子を制御します。

Telnetが有効	ベストプラクティス	セキュアなリモートアクセスには、Secure Shell (SSH) を使用する必要があります。	推奨：Telnetを無効にし、SSHを使用してセキュアなリモートアクセスを実現します。
設定されているNTPサーバが少なすぎます	ベストプラクティス	NTP用に設定されているサーバの数が3未満です。	推奨：少なくとも3台のNTPサーバをクラスタに関連付けます。 そうしないと、クラスタ時間の同期で問題が発生する可能性があります。
Remote Shell (RSH；リモートシェル) が有効	ベストプラクティス	セキュアなリモートアクセスには、Secure Shell (SSH) を使用する必要があります。	推奨：RSHを無効にし、SSHを使用してセキュアなリモートアクセスを実現します。
ログインバナーが設定されていません	ベストプラクティス	クラスタ、Storage VM、またはその両方に対してログインメッセージが設定されることはありません。	推奨：クラスタとStorage VMのログインバナーを設定し、使用を有効にします。
AutoSupportがセキュアでないプロトコルを使用している	ベストプラクティス	AutoSupportはHTTPS経由で通信するように設定されていません。	推奨：テクニカルサポートにAutoSupportメッセージを送信するためのデフォルトの転送プロトコルとしてHTTPSを使用することを強く推奨します。
デフォルトの管理ユーザがロックされていません	ベストプラクティス	デフォルトの管理アカウント (adminまたはdiag) を使用してログインしているユーザはならず、これらのアカウントはロックされていません。	推奨：使用されていないデフォルトの管理アカウントをロックします。
Secure Shell (SSH) でセキュアでない暗号を使用	ベストプラクティス	現在の設定では、セキュアでないCBC暗号を使用しています。	推奨：訪問者との安全な通信を保護するために、Webサーバー上で安全な暗号のみを許可する必要があります。 名前に「cbc」を含む暗号（「ais128-cbc」、「aes192-cbc」、「aes256-cbc」、「3DES-cbc」など）を削除します。
FIPS 140-2へのグローバルな準拠が無効になっている	ベストプラクティス	クラスタでFIPS 140-2へのグローバル準拠が無効になっています。	推奨：セキュリティ上の理由から、ONTAPが外部のクライアントまたはサーバクライアントと安全に通信できるように、グローバルFIPS 140-2準拠の暗号化を有効にする必要があります。

ボリュームがランサムウェア攻撃で監視されていない	要注意	Anti-ransomwareが1つ以上のボリュームで無効になっています。	推奨：ボリュームでランサムウェア対策を有効にします。そうしないと、ボリュームが脅威にさらされているときや攻撃を受けているときに気付かない可能性があります。
Storage VMはランサムウェア対策用に設定されていない	ベストプラクティス	ランサムウェア対策用に設定されていないStorage VMがあります。	推奨：Storage VMでランサムウェア対策を有効にします。そうしないと、Storage VMが脅威にさらされているときや攻撃を受けているときに気付かない可能性があります。

## 構成に関する分析情報

システム構成に関する懸念事項について、System Managerでは次の情報を表示できます。

インサイト	重大度	条件	の修正
通知用のクラスタが設定されていません	ベストプラクティス	Eメール、Webhook、またはSNMPトラップホストが、クラスタの問題に関する通知を受信できるように設定されていません。	推奨：クラスタの通知を設定します。
クラスタに自動更新が設定されていません。	ベストプラクティス	最新のディスク認定パッケージ、ディスクファームウェア、シェルフファームウェア、およびSP / BMCファームウェアファイルが利用可能な場合に自動更新を受信するようにクラスタが設定されていません。	推奨：この機能を有効にします。
クラスタファームウェアが最新ではありません	ベストプラクティス	お使いのシステムには、パフォーマンス向上のためにクラスタを保護するための改善策、セキュリティパッチ、または新機能が含まれている可能性のあるファームウェアに対する最新の更新がありません。	推奨：ONTAPファームウェアをアップデートします。

## システムの最適化に役立つ分析情報を取得できます

System Managerでは、システムの最適化に役立つ分析情報を確認できます。

このタスクについて

ONTAP 9.11.0 以降では、システムの容量とセキュリティコンプライアンスの最適化に役立つ分析情報を System Manager で表示できます。

ONTAP 9.11.1以降では、システムの容量、セキュリティコンプライアンス、構成を最適化するための追加の分析情報を確認できます。



拡張機能をブロックすると、予期しない結果になる可能性があります。ONTAP 9.11.1以降では、System Managerを使用してStorage VMのネイティブFPolicyを有効にできます。推奨されるSystem Manager Insightメッセージが表示される場合があります。"[ネイティブFPolicyの設定](#)" (Storage VMの場合)。

FPolicyネイティブモードでは、特定のファイル拡張子を許可または禁止できます。System Managerでは、過去にランサムウェア攻撃で使用されたファイル拡張子が3,000を超えることを推奨しています。これらの拡張子の一部は、環境内の正規のファイルによって使用されている可能性があり、ブロックすると、予期しない問題が発生する可能性があります。

したがって、環境のニーズに合わせて拡張子のリストを変更することを強くお勧めします。を参照してください "[System Managerを使用してポリシーを再作成するためにSystem Managerで作成されたネイティブFPolicyの設定からファイル拡張子を削除する方法](#)"。

ネイティブFPolicyの詳細については、を参照してください。 "[FPolicy の設定タイプ](#)"。

これらの分析情報は、ベストプラクティスに基づいて 1 ページに表示され、システムを最適化するための緊急の操作を開始できます。各インサイトの詳細については、"[System Managerの分析情報](#)"。

### 最適化のインサイトを表示



#### 手順

1. System Manager で、左側のナビゲーション列の \* Insights \* をクリックします。

[\* Insights (インサイト) ] ページには、インサイトのグループが表示されます 各インサイトグループには、1 つ以上のインサイトが含まれる場合があります。次のグループが表示されます。

- 注意が必要です
- リスクを修正
- ストレージを最適化

2. (オプション) ページの右上隅にある以下のボタンをクリックして、表示されるインサイトをフィルタリングします。

-  セキュリティ関連の分析情報を表示します。
-  容量に関する分析情報が表示されます。
-





設定に関する分析情報を表示します。

。



すべてのインサイトを表示します。

## 分析情報に対応してシステムを最適化

System Manager では、分析情報を無視したり、さまざまな方法で問題を解決したり、プロセスを開始して問題を修正したりすることで、対応できます。

### 手順

1. System Manager で、左側のナビゲーション列の \* Insights \* をクリックします。
2. Insight にカーソルを合わせると、次の操作を実行するためのボタンが表示されます。
  - \* Dismiss \* : ビューからインサイトを削除します。洞察を「アン・却下」するには、[\[customize-settings-insights\]](#)を参照してください。
  - \* Explore \* : 洞察に言及されている問題を解決するさまざまな方法を見つけます。このボタンは、複数の修復方法がある場合にのみ表示されます。
  - \* 修正 \* : インサイトで説明されている問題を修正するプロセスを開始します。修正の適用に必要なアクションを実行するかどうかを確認するメッセージが表示されます。




これらの処理の一部は System Manager の他のページから開始できますが、\* Insights \* ページではこの 1 ページから実行できるため、日常業務を合理化できます。

## インサイトの設定をカスタマイズします

System Manager で通知を受け取るインサイトをカスタマイズできます。


### 手順

1. System Manager で、左側のナビゲーション列の \* Insights \* をクリックします。
2. ページの右上にある  をクリックし、\* 設定 \* を選択します。
3. [\* 設定 \*] ページで、通知を受けるインサイトの横にチェックボックスがあることを確認します。以前にインサイトを却下したことがある場合は、チェックボックスをオンにすることで「アン却下」できます。
4. [ 保存 ( Save ) ] をクリックします。

## インサイトをPDFファイルとしてエクスポートします

適用可能なすべてのインサイトをPDFファイルとしてエクスポートできます。

### 手順

1. System Manager で、左側のナビゲーション列の \* Insights \* をクリックします。
2. ページの右上にある  をクリックし、\* エクスポート \* を選択します。

## ネイティブFPolicyの設定

ONTAP 9.11.1以降では、ネイティブのFPolicyの実装を推奨するSystem Manager Insight

を受け取った場合は、そのInsightをStorage VMおよびボリュームに設定できます。

作業を開始する前に

System Manager Insightsにアクセスすると、\*[ベストプラクティスの適用]\*で、ネイティブのFPolicyが設定されていないことを示すメッセージが表示されることがあります。

FPolicy設定タイプの詳細については、を参照してください。 ["FPolicy の設定タイプ"](#)。

手順

1. System Manager で、左側のナビゲーション列の \* Insights \* をクリックします。
2. で、[ネイティブFPolicyは設定されていません]\*を探します。
3. アクションを実行する前に、次のメッセージをお読みください。



拡張機能をブロックすると、予期しない結果になる可能性があります。 ONTAP 9.11.1以降では、System Managerを使用してStorage VMのネイティブFPolicyを有効にできます。 FPolicyネイティブモードでは、特定のファイル拡張子を許可または禁止できます。 System Managerでは、過去にランサムウェア攻撃で使用されたファイル拡張子が3,000を超えることを推奨しています。 これらの拡張子の一部は、環境内の正規のファイルによって使用されている可能性があり、ブロックすると、予期しない問題が発生する可能性があります。

したがって、環境のニーズに合わせて拡張子のリストを変更することを強くお勧めします。 を参照してください ["System Managerを使用してポリシーを再作成するためにSystem Managerで作成されたネイティブFPolicyの設定からファイル拡張子を削除する方法"](#)。

4. [修正]\*をクリックします。
5. ネイティブFPolicyを適用するStorage VMを選択します。
6. 各Storage VMについて、ネイティブFPolicyを受け取るボリュームを選択します。
7. [Configure] をクリックします。

## CLIを使用してクラスタパフォーマンスを監視および管理します

### パフォーマンスの監視と管理の概要

基本的なパフォーマンスの監視と管理のタスクを設定し、一般的なパフォーマンスの問題を特定して解決することができます。

次の想定条件に該当する場合は、以下の手順に従ってクラスタのパフォーマンスを監視および管理してください。

- すべての選択肢について検討するのではなく、ベストプラクティスに従う。
- ONTAP コマンドラインインターフェイスに加え、Active IQ Unified Manager（旧 OnCommand Unified Manager）を使用して、システムのステータスとアラートを表示し、クラスタのパフォーマンスを監視し、根本原因分析を実施する。
- ストレージサービス品質（QoS）の設定に ONTAP コマンドラインインターフェイスを使用している。

QoS は、System Manager、NSLM、WFA、VSC（VMware プラグイン）、および API でも設定で

きます。

- Linux または Windows ベースのインストールではなく、仮想アプライアンスを使用して Unified Manager をインストールする。
- DHCP ではなく静的な設定を使用してソフトウェアをインストールする。
- ONTAP コマンドには、advanced 権限レベルでアクセスできます。
- 「admin」ロールを持つクラスタ管理者である。

#### 関連情報

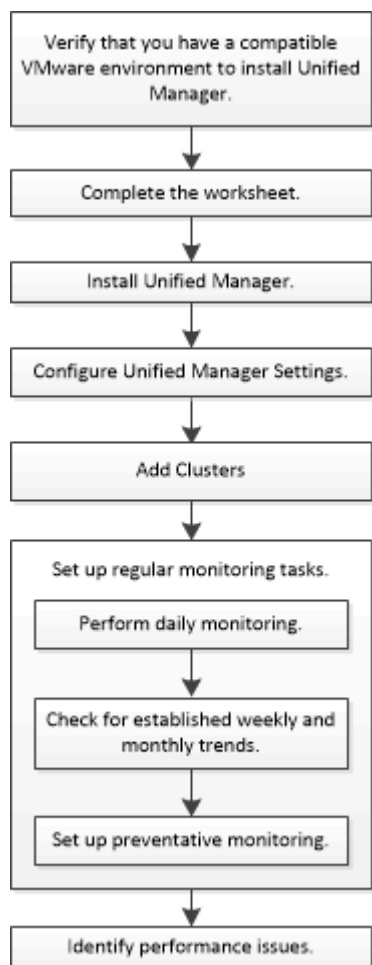
上記の想定条件に該当しない場合は、次の資料を参照してください。

- ["Active IQ Unified Manager 9.8 のインストール"](#)
- ["システム管理"](#)

## パフォーマンスを監視

### パフォーマンスの監視とメンテナンスのワークフローの概要

クラスタパフォーマンスの監視と保守では、Active IQ Unified Managerソフトウェアをインストールし、基本的な監視タスクを設定し、パフォーマンスの問題を特定して、必要に応じて調整を行います。



VMware 環境がサポートされていることを確認します

Active IQ Unified Manager を正しくインストールするには、VMware環境が要件を満たしていることを確認する必要があります。

手順

- 1. VMware インフラが Unified Manager のインストールに必要なサイジング要件を満たしていることを確認します。
- 2. にアクセスします ["互換性マトリックス"](#) 次のコンポーネントについて、サポートされている組み合わせであることを確認します。
  - ONTAPバージョン
  - ESXi オペレーティングシステムのバージョン
  - VMware vCenter Server のバージョン
  - VMware Tools のバージョン
  - ブラウザのタイプとバージョン



。 ["互換性マトリックス"](#) に、 Unified Manager でサポートされる構成を示します。

- 3. 選択した構成の構成名をクリックします。

その構成の詳細が [ 構成の詳細 ] ウィンドウに表示されます。

- 4. 次のタブの情報を確認します。

- 注：

お使いの構成に固有の重要なアラートおよび情報が表示されます。
- ポリシーとガイドライン

すべての構成に関する一般的なガイドラインが表示されます。

Active IQ Unified Manager ワークシート

Active IQ Unified Manager のインストール、設定、および接続に進む前に、環境に関する特定の情報を確認しておく必要があります。この情報はワークシートに記録できます。

Unified Manager のインストール情報

ソフトウェアが導入されている仮想マシン	あなたの価値
ESXi サーバの IP アドレス	
ホストの完全修飾ドメイン名	

ホストの IP アドレス	
ネットワークマスク	
ゲートウェイの IP アドレス	
プライマリ DNS アドレス	
セカンダリ DNS アドレス	
検索ドメイン	
メンテナンスユーザのユーザ名	
メンテナンスユーザのパスワード	


#### Unified Manager の設定情報

設定	あなたの価値
メンテナンスユーザの E メールアドレス	
NTPサーバ	
SMTP サーバのホスト名または IP アドレス	
SMTPユーザ名	
SMTPパスワード	
SMTP のデフォルトポート	25 （デフォルト値）
アラート通知の送信元 E メールアドレス	
LDAP のバインド識別名	
LDAP のバインドパスワード	
Active Directory の管理者名	
Active Directory のパスワード	

認証サーバのベース識別名	
認証サーバのホスト名または IP アドレス	

## クラスタ情報

Unified Manager で各クラスタについて次の情報を確認します。

クラスタ 1 / N	あなたの価値
ホスト名またはクラスタ管理 IP アドレス	
ONTAP 管理者のユーザ名  管理者には「admin」ロールが割り当てられている必要があります。	
ONTAP 管理者のパスワード	
プロトコル（HTTP または HTTPS）	

## 関連情報

["管理者認証と RBAC"](#)

## Active IQ Unified Manager をインストールします

Active IQ Unified Manager をダウンロードして導入

ソフトウェアをインストールするには、仮想アプライアンス（VA）インストールファイルをダウンロードし、VMware vSphere Client を使用して VMware ESXi サーバに導入する必要があります。VA は OVA ファイルとして提供されます。

## 手順

1. NetApp Support Siteソフトウェアのダウンロード \* ページにアクセスし、Active IQ Unified Manager を探します。

<https://mysupport.netapp.com/products/index.html>

2. [Select Platform\*（プラットフォームの選択）] ドロップダウンメニューで [\* VMware vSphere\*（VMware vSphere \*）] を選択し、[\* Go!\*（実行）] をクリックします
3. 「OVA」ファイルを、VMware vSphere Clientからアクセス可能なローカルまたはネットワーク上の場所に保存します。
4. VMware vSphere Client で、\* File \* > \* Deploy OVF Template \* をクリックします。
5. 「OVA」ファイルを探し、ウィザードを使用してESXiサーバに仮想アプライアンスを導入します。

ウィザードの \* Properties \* タブを使用して、静的な構成情報を入力できます。

6. VM の電源をオンにします。
7. 最初の起動プロセスを表示するには、\* Console \* タブをクリックします。
8. プロンプトに従って、VM に VMware Tools をインストールします。
9. タイムゾーンを設定します。
10. メンテナンスユーザの名前とパスワードを入力します。
11. VM コンソールに表示された URL にアクセスします。

**Active IQ Unified Manager** の初期設定を行います

Web UI への初回アクセス時に Active IQ Unified Manager の初期セットアップダイアログボックスが表示されます。このダイアログボックスでは、いくつかの初期設定を行ったり、クラスタを追加したりできます。

手順

1. AutoSupport のデフォルトの有効設定をそのまま使用します。
2. NTP サーバの詳細、メンテナンスユーザの E メールアドレス、SMTP サーバのホスト名、およびその他の SMTP オプションを入力し、\* Save \* をクリックします。

完了後

初期セットアップが完了すると、クラスタデータソースページが表示され、クラスタの詳細を確認できます。

監視対象のクラスタを指定します

クラスタを監視対象に含め、クラスタの検出ステータスを確認したり、クラスタのパフォーマンスを監視したりするには、クラスタを Active IQ Unified Manager サーバに追加する必要があります。

必要なもの

- 次の情報が必要です。
    - ホスト名またはクラスタ管理 IP アドレス
- ホスト名は、Unified Manager がクラスタへの接続に使用する完全修飾ドメイン名（FQDN）または短縮名です。このホスト名は、クラスタ管理 IP アドレスに解決される必要があります。
- クラスタ管理 IP アドレスは、管理用 Storage Virtual Machine（SVM）のクラスタ管理 LIF である必要があります。ノード管理 LIF を使用すると処理に失敗します。
- ONTAP 管理者のユーザ名とパスワード
  - クラスタおよびクラスタのポート番号で設定できるプロトコルのタイプ（HTTP または HTTPS）
- アプリケーション管理者またはストレージ管理者のロールが必要です。
  - ONTAP 管理者に ONTAPI と SSH の管理者ロールが必要です。
  - Unified Manager の FQDN を使用して、ONTAP に ping を実行できる必要があります。

これは、ONTAP コマンドを使用して確認できます `ping -node node_name -destination Unified_Manager_FQDN`。

## このタスクについて

MetroCluster 構成では、ローカルクラスタとリモートクラスタの両方を追加し、クラスタを正しく設定する必要があります。

### 手順

1. [ \* Configuration \* > \* Cluster Data Sources \* ] をクリックします。
2. [ クラスタ ] ページで、[ \* 追加 ] をクリックします。
3. Add Cluster \* (クラスタの追加) ダイアログボックスで、クラスタのホスト名または IP アドレス (IPv4 または IPv6)、ユーザ名、パスワード、通信プロトコル、ポート番号など、必要な値を指定します。

デフォルトでは HTTPS プロトコルが選択されています。

クラスタ管理 IP アドレスは、IPv6 から IPv4 または IPv4 から IPv6 に変更できます。次の監視サイクルが完了すると、クラスタグリッドとクラスタ設定ページに新しい IP アドレスが反映されます。

4. [ 追加 (Add) ] をクリックします。
5. HTTPS を選択した場合は、次の手順を実行します。
  - a. [ \* Authorize Host \* (ホストの認証) ] ダイアログボックスで、[ \* View Certificate \* (証明書の表示) ] をクリックしてクラスタに関する証明書情報を表示します。
  - b. 「 \* はい \* 」をクリックします。

Unified Manager で証明書がチェックされるのはクラスタを最初に追加したときだけです。ONTAP に対する API 呼び出しごとに確認されるわけではありません。

証明書の期限が切れているクラスタは追加できません。SSL 証明書を更新してから、クラスタを追加する必要があります。

6. \* オプション \* : クラスタ検出ステータスを表示します。
  - a. クラスタセットアップ \* ページでクラスタ検出ステータスを確認します。

デフォルトの監視間隔である約 15 分後に、Unified Manager データベースにクラスタが追加されます。

## 基本的な監視タスクを設定

### 日々の監視を実行します

監視を毎日実行することで、注意が必要なパフォーマンスの問題にすぐに対処することができます。

### 手順

1. Active IQ Unified Manager UI から \* Event Inventory \* ページに移動して、現在のイベントと廃止状態のイベントをすべて表示します。
2. [表示]\*オプションで、を選択します Active Performance Events 必要なアクションを決定します。



パフォーマンスの傾向を特定すると、ボリュームレイテンシを分析して、クラスタの使用率が高すぎる / 低すぎる状況を特定するのに役立ちます。同様の手順に従って、CPU やネットワークなど、システムのその他のボトルネックについても特定できます。

#### 手順

1. 使用率が高すぎるか低すぎる疑いがあるボリュームを探します。
2. [ボリュームの詳細] タブで、[\*30 d] をクリックして履歴データを表示します。
3. [データのブレイクダウンの条件] ドロップダウンメニューで、[Latency] を選択し、[Submit] をクリックします。
4. クラスタコンポーネント比較グラフで「\* Aggregate」を選択解除し、クラスタのレイテンシをボリュームレイテンシグラフと比較します。
5. アグリゲートを選択し、クラスタコンポーネント比較チャート内の他のすべてのコンポーネントの選択を解除して、アグリゲートのレイテンシをボリュームレイテンシチャートと比較します。
6. 読み取り / 書き込みレイテンシのグラフをボリュームレイテンシのグラフと比較します。
7. クライアントアプリケーションの負荷が原因でワークロードの競合が発生していないかどうかを確認し、必要に応じてワークロードのバランスを調整
8. アグリゲートの使用率が高すぎて競合を引き起こしていないかどうかを確認し、必要に応じてワークロードのバランスを調整

パフォーマンスしきい値を使用してイベント通知を生成

イベントは、事前に定義された状況が発生したとき、またはパフォーマンスカウンタの値がしきい値を超えたときに、Active IQ Unified Manager で自動的に生成される通知です。イベントによって、監視しているクラスタ内のパフォーマンスの問題を特定できます。特定の重大度タイプのイベントが発生したときに自動的に E メール通知を送信するアラートを設定できます。

パフォーマンスしきい値を設定

重大なパフォーマンスの問題を監視するために、パフォーマンスしきい値を設定することができます。ユーザ定義のしきい値の場合、定義されたしきい値に近づいたとき、またはしきい値を超えたときに、警告または重大イベントの通知がトリガーされます。

#### 手順

1. 警告イベントと重大イベントのしきい値を作成します。
  - a. [\* Configuration \* > \* Performance Thresholds \*] を選択します。
  - b. [作成 (Create)] をクリックします。
  - c. オブジェクトタイプを選択し、ポリシーの名前と概要を指定します。
  - d. オブジェクトカウンタの条件を選択し、警告イベントと重大イベントの制限値を指定します。
  - e. イベントを送信するために制限値に違反する必要がある期間を選択し、[保存] をクリックします。
2. しきい値ポリシーをストレージオブジェクトに割り当てます。

- a. 以前に選択したクラスタオブジェクトタイプのインベントリページに移動し、View オプションから \* Performance \* を選択します。
- b. しきい値ポリシーを割り当てるオブジェクトを選択し、\* しきい値ポリシーの割り当て \* をクリックします。
- c. 前の手順で作成したポリシーを選択し、\* ポリシーの割り当て \* をクリックします。

#### 例

重大なパフォーマンスの問題を特定するためにユーザ定義のしきい値を設定することができます。たとえば、ボリュームのレイテンシが20ミリ秒を超えるとMicrosoft Exchange Serverがクラッシュすることがわかっている場合は、警告しきい値を12ミリ秒、重大しきい値を15ミリ秒のように設定できます。このしきい値の設定を使用して、ボリュームのレイテンシが制限を超えたときに通知を受け取ることができます。

	Warning	Critical
Object Counter Condition*	Average Latency ms/op	ms/op
	12	15

アラートを追加します

特定のイベントが生成されたときに通知するようにアラートを設定できます。アラートは、単一のリソース、リソースのグループ、または特定の重大度タイプのイベントについて設定することができます。通知を受け取る頻度を指定したり、アラートにスクリプトを関連付けたりできます。

#### 必要なもの

- イベント生成時に Active IQ Unified Manager サーバからユーザに通知を送信できるように、通知に使用するユーザの E メールアドレス、SMTP サーバ、SNMP トラップホストなどを設定しておく必要があります。
- アラートをトリガーするリソースとイベント、および通知するユーザのユーザ名または E メールアドレスを確認しておく必要があります。
- イベントに基づいてスクリプトを実行する場合は、Scripts ページを使用して Unified Manager にスクリプトを追加しておく必要があります。
- アプリケーション管理者またはストレージ管理者のロールが必要です。

#### このタスクについて

アラートは、ここで説明するように、Alert Setup ページからアラートを作成するだけでなく、イベントを受信した後に Event Details ページから直接作成できます。

#### 手順

1. 左側のナビゲーションペインで、\* Storage Management \* > \* Alert Setup \* をクリックします。
2. [\* Alert Setup\*] ページで、[\* Add] をクリックします。
3. [\* アラートの追加 \*] ダイアログボックスで、[\* 名前 \*] をクリックし、アラートの名前と概要を入力します。
4. [\* リソース] をクリックし、アラートに含めるリソースまたはアラートから除外するリソースを選択します。

[\* 次を含む名前 (\* Name Contains) ] フィールドでテキスト文字列を指定してフィルタを設定し、リソースのグループを選択できます。指定したテキスト文字列に基づいて、フィルタルールに一致するリソース

スのみが使用可能なリソースのリストに表示されます。指定するテキスト文字列では、大文字と小文字が区別されます。

あるリソースが対象に含めるルールと除外するルールの両方に該当する場合は、除外するルールが優先され、除外されたリソースに関連するイベントについてはアラートが生成されません。

5. [\*Events] をクリックし、アラートをトリガーするイベント名またはイベントの重大度タイプに基づいてイベントを選択します。



複数のイベントを選択するには、Ctrl キーを押しながら選択します。

6. [\*Actions] をクリックし、通知するユーザを選択し、通知頻度を選択し、SNMP トラップをトラップレシーバに送信するかどうかを選択し、アラートが生成されたときに実行するスクリプトを割り当てます。



ユーザに対して指定されている E メールアドレスを変更し、アラートを再び開いて編集しようとする、変更した E メールアドレスが以前に選択したユーザにマッピングされていないため、名前フィールドは空白になります。また、選択したユーザの E メールアドレスを Users ページで変更した場合、変更後の E メールアドレスは反映されません。

SNMP トラップを使用してユーザに通知することもできます。

7. [保存 (Save)] をクリックします。

#### アラートの追加例

この例は、次の要件を満たすアラートを作成する方法を示しています。

- アラート名： HealthTest
- リソース：名前に「abc」が含まれるすべてのボリュームを対象に含め、名前に「xyz」が含まれるすべてのボリュームを対象から除外する
- イベント：健全性に関するすべての重大なイベントを含みます
- アクション：「[sample@domain.com](mailto:sample@domain.com)」、「Test」スクリプトが含まれ、15 分ごとにユーザに通知する必要があります

[Add Alert] ダイアログボックスで、次の手順を実行します。

1. [名前] をクリックし、と入力します HealthTest [アラート名] フィールドに入力します。
2. [\* リソース] をクリックし、[含める] タブで、ドロップダウン・リストから [\* ボリューム] を選択します。
  - a. 入力するコマンド abc [名前に次の文字を含む]\* フィールドに、名前に「abc」を含むボリュームを表示します。
  - b. 「\* +」を選択します [\[All Volumes whose name contains 'abc'\]](#) + \* を使用可能なリソース領域から選択したリソース領域に移動します。
  - c. [除外する] をクリックし、と入力します xyz [名前に\*が含まれています] フィールドで、[\*追加] をクリックします。
3. [\* イベント] をクリックし、[イベントの重要度] フィールドから [クリティカル \*] を選択します。
4. [Matching Events] 領域から [\*All Critical Events] を選択し、[Selected Events] 領域に移動します。

5. [アクション]をクリックし、と入力します sample@domain.com [これらのユーザーにアラートを送信]フィールドに入力します。
6. 15 分ごとにユーザに通知するには、「\* 15 分ごとに通知する」を選択します。

指定した期間、受信者に繰り返し通知を送信するようにアラートを設定できます。アラートに対してイベント通知をアクティブにする時間を決める必要があります。

7. 実行するスクリプトの選択メニューで、\* テスト \* スクリプトを選択します。
8. [保存 ( Save ) ]をクリックします。

#### アラートを設定

アラートについて、アラートをトリガーする Active IQ Unified Manager のイベント、アラートを受け取る E メール受信者、およびアラートの頻度を指定することができます。

#### 必要なもの

アプリケーション管理者のロールが必要です。

#### このタスクについて

次のタイプのパフォーマンスイベントについて、固有のアラートを設定できます。

- 重大イベント：ユーザ定義のしきい値に違反したときにトリガーされます
- 警告イベント：ユーザ定義のしきい値、システム定義のしきい値、または動的なしきい値に違反したときにトリガーされます

デフォルトでは、すべての新しいイベントについて、Unified Manager の管理者ユーザに E メールアラートが送信されます。他のユーザに E メールアラートを送信する場合は、それらのユーザの E メールアドレスを追加します。



特定のタイプのイベントに関するアラートの送信を無効にするには、そのイベントカテゴリですべてのチェックボックスをオフにする必要があります。この処理を実行しても、イベントがユーザインターフェイスに表示されるのを停止することはありません。

#### 手順

1. 左側のナビゲーションペインで、\* Storage Management \* > \* Alert Setup \* を選択します。

[Alert Setup] ページが表示されます。

2. [\* 追加 ] をクリックし、各イベントタイプに適切な設定を行います。

E メールアラートを複数のユーザに送信する場合は、各 E メールアドレスをカンマで区切って入力します。

3. [保存 ( Save ) ]をクリックします。

#### Active IQ Unified Manager のパフォーマンスの問題を特定する

パフォーマンスイベントが発生した場合は、Active IQ Unified Manager で問題のソースを特定し、他のツールを使用して修正することができます。イベントの発生を知らせる

E メールを受信したり、日々の監視中にイベントに気付いたりすることがあります。

#### 手順

1. E メール通知に記載されたリンクをクリックし、パフォーマンスイベントが発生しているストレージオブジェクトに直接移動します。

状況	作業
イベントの E メール通知を受信する	リンクをクリックしてイベントの詳細ページに直接移動します。
Event Inventory ページの分析中にイベントに注目してください	イベントを選択してイベントの詳細ページに直接移動します。

2. システム定義のしきい値を超えたイベントの場合は、画面に提示される対処方法に従って問題をトラブルシューティングします。
3. ユーザ定義のしきい値を超えたイベントの場合は、イベントを分析して対処が必要かどうかを判断します。
4. 問題が解決しない場合は、次の設定を確認します。
  - ストレージシステムのプロトコル設定
  - イーサネットスイッチまたはファブリックスイッチのネットワーク設定
  - ストレージシステムのネットワーク設定
  - ストレージシステムのディスクレイアウトとアグリゲートの指標を表示します
5. 問題が解除されない場合は、テクニカルサポートにお問い合わせください。

### Active IQ デジタルアドバイザーを使用して、システムのパフォーマンスを確認します

ネットアップにAutoSupport テレメトリを送信するONTAP システムについては、広範なパフォーマンスデータと容量データを表示できます。Active IQ には、System Manager に表示されるよりも長時間にわたるシステムパフォーマンスが表示されます。

CPU 利用率、レイテンシ、IOPS、プロトコル別の IOPS、およびネットワークスループットのグラフを表示できます。このデータは .csv 形式でダウンロードして、他のツールで分析することもできます。

Active IQ では、このパフォーマンスデータに加えて、ワークロード別のストレージ効率を表示して、そのワークロードタイプの想定される削減率と比較することができます。容量の傾向を確認して、特定の期間に追加する必要があるストレージの推定量を確認できます。



- Storage Efficiency は、メインダッシュボードの左側にあるお客様、クラスタ、ノードの各レベルで利用できます。
- パフォーマンスは、メインダッシュボードの左側のクラスタレベルとノードレベルで利用できます。

#### 関連情報

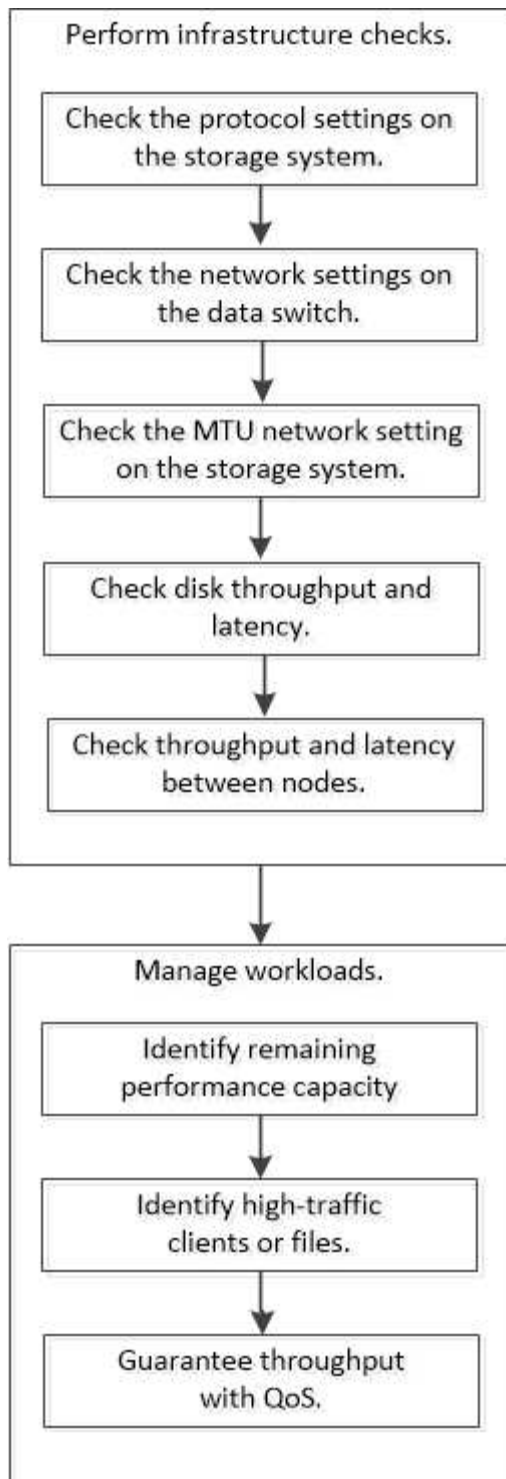
- ["Active IQ デジタルアドバイザーのドキュメント"](#)

- ["Active IQ デジタルアドバイザービデオ再生リスト"](#)
- ["Active IQ Web ポータル"](#)

## パフォーマンスの問題を管理

### パフォーマンス管理ワークフロー

パフォーマンス問題を特定したら、インフラに関するいくつかの基本的な診断チェックを実施して明らかな構成エラーを排除できます。このチェックで問題が見つからなければ、ワークロード管理の問題について調べることができます。



基本的なインフラチェックを実施

ストレージシステムのプロトコル設定を確認してください

**NFS** の **TCP** 最大転送サイズを確認します

NFS の場合、読み取りと書き込みの TCP 最大転送サイズがパフォーマンス問題の原因になっていないかどうかを確認することができます。このサイズが原因でパフォーマンスが低下している可能性がある場合は、サイズを大きくして対処できます。

#### 必要なもの

- このタスクを実行するには、クラスタ管理者の権限が必要です。
- このタスクを実行するには、advanced 権限レベルのコマンドを使用する必要があります。

#### 手順

1. advanced 権限レベルに切り替えます。

```
set -privilege advanced
```

2. TCP 最大転送サイズを確認します。

```
vserver nfs show -vserver vserver_name -instance
```

3. TCP 最大転送サイズが小さすぎる場合は、サイズを大きくします。

```
vserver nfs modify -vserver vserver_name -tcp-max-xfer-size integer
```

4. admin 権限レベルに戻ります。

```
set -privilege admin
```

#### 例

次の例は、のTCP最大転送サイズを変更します SVM1 1048576まで：

```
cluster1::*> vserver nfs modify -vserver SVM1 -tcp-max-xfer-size 1048576
```

#### iSCSI の TCP 読み取り / 書き込みサイズを確認します

iSCSI の場合、TCP 読み取り / 書き込みサイズを確認して、サイズ設定がパフォーマンス問題を作成中であるかどうかを判断できます。サイズが問題のソースである場合は、サイズを変更して対処できます。

#### 必要なもの

このタスクを実行するには、advanced 権限レベルのコマンドが必要です。

#### 手順

1. advanced 権限レベルに切り替えます。

```
set -privilege advanced
```

2. TCP ウィンドウサイズの設定を確認します。

```
vserver iscsi show -vserv,er vserver_name -instance
```

3. TCP ウィンドウサイズの設定を変更します。

```
vserver iscsi modify -vserver vserver_name -tcp-window-size integer
```



#### 4. admin 権限に戻ります。

```
set -privilege admin
```

#### 例

次の例は、のTCPウィンドウサイズを変更します svm1 131、400バイトまで：

```
cluster1::*> vserver iscsi modify -vserver vs1 -tcp-window-size 131400
```

#### CIFS 多重化設定を確認します

低速な CIFS ネットワークが原因でパフォーマンス問題が発生する場合は、多重化設定を変更して対処することができます。

#### 手順

1. CIFS 多重化設定を確認します。

```
vserver cifs options show -vserver -vserver_name -instance
```

2. CIFS 多重化設定を変更します。

```
vserver cifs options modify -vserver -vserver_name -max-mpx integer
```

#### 例

次に、の最大多重化カウントを変更する例を示します svm1 255まで：

```
cluster1::> vserver cifs options modify -vserver SVM1 -max-mpx 255
```

#### FC アダプタのポート速度を確認します

パフォーマンスを最適化するには、アダプタのターゲットポートの速度を接続先デバイスの速度と同じにします。ポートに自動ネゴシエーションが設定されている場合、ギブバックやテイクオーバーなどの中断後の再接続に時間がかかる可能性があります。

#### 必要なもの

このアダプタをホームポートとして使用しているすべての LIF をオフラインにする必要があります。

#### 手順

1. アダプタをオフラインにします。

```
network fcp adapter modify -node nodename -adapter adapter -state down
```

2. ポートアダプタの最大速度を確認します。

```
fcp adapter show -instance
```

3. 必要に応じてポート速度を変更します。

```
network fcp adapter modify -node nodename -adapter adapter -speed  
{1|2|4|8|10|16|auto}
```

4. アダプタをオンラインにします。

```
network fcp adapter modify -node nodename -adapter adapter -state up
```

5. アダプタのすべての LIF をオンラインにします。

```
network interface modify -vserver * -lif * { -home-node node1 -home-port e0c }  
-status-admin up
```

#### 例

次の例は、アダプタのポート速度を変更します 0d オン node1 2 Gbpsまで：

```
cluster1::> network fcp adapter modify -node node1 -adapter 0d -speed 2
```

データスイッチのネットワーク設定を確認します

クライアント、サーバ、ストレージシステム（ネットワークエンドポイント）で MTU 設定を同じにする必要がありますが、パフォーマンスに影響しないように、NIC やスイッチなどの中間ネットワークデバイスを最大 MTU 値に設定する必要があります。

パフォーマンスを最大限に高めるには、ネットワーク内のすべてのコンポーネントでジャンボフレームを転送できる必要があります（9、000 バイトの IP、9022 バイトのイーサネットを含む）。データスイッチは 9022 バイト以上に設定する必要がありますが、ほとんどのスイッチでは 9216 という一般的な値があります。

#### 手順

データスイッチの場合は、MTU サイズが 9022 以上に設定されていることを確認します。

詳細については、スイッチベンダーのマニュアルを参照してください。

ストレージシステムの **MTU** ネットワーク設定を確認

ストレージシステムのネットワーク設定がクライアントや他のネットワークエンドポイントと同じでない場合は、設定を変更することができます。管理ネットワークの MTU 設定は 1500 に設定されていますが、データネットワークの MTU サイズは 9000 にしてください。

#### このタスクについて

管理トラフィックを処理する e0M ポートを除き、ブロードキャストドメイン内のすべてのポートの MTU サイズが同じです。ポートがブロードキャストドメインの一部である場合は、を使用します broadcast-domain modify コマンドを使用して、変更したブロードキャストドメイン内のすべてのポートの MTU を変更します。

NIC やデータスイッチなどの中間ネットワークデバイスの MTU サイズは、ネットワークエンドポイントよりも大きく設定できます。詳細については、を参照してください ["データスイッチのネットワーク設定を確認します"](#)。

#### 手順

1. ストレージシステムの MTU ポート設定を確認します。

```
network port show -instance
```

2. ポートで使用されているブロードキャストドメインのMTUを変更します。

```
network port broadcast-domain modify -ipspace ipspace -broadcast-domain  
broadcast_domain -mtu new_mtu
```

#### 例

次の例では、MTUポート設定を9000に変更します。

```
network port broadcast-domain modify -ipspace Cluster -broadcast-domain  
Cluster -mtu 9000
```

ディスクのスループットとレイテンシを確認

ディスクのスループットとレイテンシの指標を確認すると、クラスタノードのトラブルシューティングに役立ちます。

このタスクについて

このタスクを実行するには、advanced 権限レベルのコマンドが必要です。

#### 手順

1. advanced 権限レベルに切り替えます。

```
set -privilege advanced
```

2. ディスクのスループットとレイテンシの指標を確認します。

```
statistics disk show -sort-key latency
```

#### 例

次の例は、に対する各ユーザの読み取り/書き込み処理の合計を表示します node2 オン cluster1 :

```
::*> statistics disk show -sort-key latency
cluster1 : 8/24/2015 12:44:15
```

Disk	Node	Busy (%)	Total Ops	Read Ops	Write Ops	Read (Bps)	Write (Bps)	*Latency (us)
1.10.20	node2	4	5	3	2	95232	367616	23806
1.10.8	node2	4	5	3	2	138240	386048	22113
1.10.6	node2	3	4	2	2	48128	371712	19113
1.10.19	node2	4	6	3	2	102400	443392	19106
1.10.11	node2	4	4	2	2	122880	408576	17713

ノード間のスループットとレイテンシを確認

を使用できます `network test-path` コマンドを使用してネットワークのボトルネックを特定したり、ノード間のネットワークパスを事前に確認したりできます。このコマンドは、クラスタ間のノード間でもクラスタ内のノード間でも実行できます。

必要なもの

- このタスクを実行するには、クラスタ管理者である必要があります。
- このタスクを実行するには、`advanced` 権限レベルのコマンドが必要です。
- クラスタ間のパスの場合、ソースクラスタとデスティネーションクラスタがピアリングされている必要があります。

このタスクについて

ノード間のネットワークパフォーマンスが、パス構成に対して期待される値にならない場合があります。たとえば、ソースクラスタとデスティネーションクラスタの間のリンクが 10GbE の場合でも、SnapMirror レプリケーション処理による大量のデータ転送では 1Gbps の伝送速度が観察されることがあります。

を使用できます `network test-path` ノード間のスループットとレイテンシを測定するコマンド。このコマンドは、クラスタ間のノード間でもクラスタ内のノード間でも実行できます。



このテストはネットワークパスが一杯になるまでデータを投入するため、システムがビジーでなく、ノード間のネットワークトラフィックが集中していないときに実行してください。テストは 10 秒後にタイムアウトします。このコマンドは、ONTAP 9 のノード間でのみ実行できます。

。 `session-type` オプションは、ネットワークパスで実行する処理のタイプを指定します。たとえば、リモートデスティネーションへの SnapMirror レプリケーションの場合は「`AsyncMirrorRemote`」と指定します。タイプによって、テストで使用するデータの量が決まります。次の表に、セッションタイプを示します。

セッションタイプ ( Session Type )	説明
---------------------------	----

AsyncMirrorLocal です	SnapMirrorによって同じクラスタ内のノード間で使用される設定
AsyncMirrorRemote	異なるクラスタのノード間のSnapMirrorで使用される設定（デフォルトタイプ）
RemoteDataTransfer	ONTAP が同じクラスタ内のノード間のリモートデータアクセスに使用する設定（たとえば、別のノードのボリュームに格納されたファイルを取得するためのノードへのNFS要求）

## 手順

1. advanced 権限レベルに切り替えます。

```
set -privilege advanced
```

2. ノード間のスループットとレイテンシを測定します。

```
network test-path -source-node source_nodename |local -destination-cluster destination_clustername -destination-node destination_nodename -session-type Default|AsyncMirrorLocal|AsyncMirrorRemote|SyncMirrorRemote|RemoteDataTransfer
```

ソースノードはローカルクラスタにある必要があります。デスティネーションノードはローカルクラスタまたはピアクラスタに含めることができます。の値は「local」です -source-node コマンドを実行するノードを指定します。

次のコマンドは、間のSnapMirrorタイプのレプリケーション処理のスループットとレイテンシを測定します node1 ローカルクラスタおよび node3 オン cluster2：

```
cluster1::> network test-path -source-node node1 -destination-cluster cluster2 -destination-node node3 -session-type AsyncMirrorRemote
Test Duration:      10.88 secs
Send Throughput:    18.23 MB/sec
Receive Throughput: 18.23 MB/sec
MB sent:            198.31
MB received:        198.31
Avg latency in ms:  2301.47
Min latency in ms:  61.14
Max latency in ms:  3056.86
```

3. admin 権限に戻ります。

```
set -privilege admin
```

## 完了後

パス構成に対して期待される値を得られない場合は、ノードのパフォーマンス統計の確認、ツールを使用した

ネットワークの問題の切り分け、スイッチ設定の確認などを行います。

## ワークロードの管理

残りのパフォーマンス容量を特定します

パフォーマンス容量（*headroom*）は、リソースのワークロードのパフォーマンスにレイテンシの影響を受ける前にノードまたはアグリゲートに配置できる作業量を測定します。クラスタで利用可能なパフォーマンス容量を知っておくと、ワークロードのプロビジョニングと分散に役立ちます。

必要なもの

このタスクを実行するには、advanced 権限レベルのコマンドが必要です。

このタスクについて

には次の値を使用できます `-object` ヘッドルームの統計を収集および表示するオプション：

- CPUの場合は、`resource_headroom_cpu`。
- アグリゲートの場合 `resource_headroom_aggr`。

この作業は、System Manager および Active IQ Unified Manager を使用して実行することもできます。

手順

1. advanced 権限レベルに切り替えます。

```
set -privilege advanced
```

2. リアルタイムのヘッドルーム統計の収集を開始します。

```
statistics start -object resource_headroom_cpu|aggr
```

コマンド構文全体については、マニュアルページを参照してください。

3. リアルタイムのヘッドルーム統計情報を表示します。

```
statistics show -object resource_headroom_cpu|aggr
```

コマンド構文全体については、マニュアルページを参照してください。

4. admin 権限に戻ります。

```
set -privilege admin
```

例

次の例は、クラスタノードの 1 時間あたりの平均ヘッドルーム統計を表示します。

ノードの使用可能なパフォーマンス容量は、を引いて計算できます `current_utilization` からカウンタを開きます `optimal_point_utilization` カウンタ。この例では、の利用率 CPU\_sti2520-213 IS-14%（72%~86%）は、CPUの過去1時間の平均利用率が高すぎることを示しています。

指定することもできました `ewma_daily`、`ewma_weekly` または `ewma_monthly` 同じ情報をより長期間にわたって平均化することができます。

```
sti2520-2131454963690::*> statistics show -object resource_headroom_cpu
-raw -counter ewma_hourly
(statistics show)
```

```
Object: resource_headroom_cpu
Instance: CPU_sti2520-213
Start-time: 2/9/2016 16:06:27
End-time: 2/9/2016 16:06:27
Scope: sti2520-213
```

Counter	Value
ewma_hourly	-
current_ops	4376
current_latency	37719
current_utilization	86
optimal_point_ops	2573
optimal_point_latency	3589
optimal_point_utilization	72
optimal_point_confidence_factor	1

```
Object: resource_headroom_cpu
Instance: CPU_sti2520-214
Start-time: 2/9/2016 16:06:27
End-time: 2/9/2016 16:06:27
Scope: sti2520-214
```

Counter	Value
ewma_hourly	-
current_ops	0
current_latency	0
current_utilization	0
optimal_point_ops	0
optimal_point_latency	0
optimal_point_utilization	71
optimal_point_confidence_factor	1

2 entries were displayed.

トラフィックの多いクライアントやファイルを特定

ONTAP の Active Objects テクノロジを使用すると、クラスタのトラフィック量を著しく

増大させているクライアントやファイルを特定することができます。このような「上位」のクライアントやファイルを特定したら、クラスタワークロードをリバランシングするか、別の手順に従って問題を解決できます。

#### 必要なもの

このタスクを実行するには、クラスタ管理者である必要があります。

#### 手順

1. クラスタに最もアクセスする上位のクライアントを表示します。

```
statistics top client show -node node_name -sort-key sort_column -interval  
seconds_between_updates -iterations iterations -max number_of_instances
```

コマンド構文全体については、マニュアルページを参照してください。

次のコマンドは、アクセス頻度の高い上位のクライアントを表示します cluster1：

```
cluster1::> statistics top client show
```

cluster1 : 3/23/2016 17:59:10

Client	Vserver	Node	Protocol	*Total Ops
172.17.180.170	vs4	siderop1-vs4	nfs	668
172.17.180.169	vs3	siderop1-vs3	nfs	337
172.17.180.171	vs3	siderop1-vs3	nfs	142
172.17.180.170	vs3	siderop1-vs3	nfs	137
172.17.180.123	vs3	siderop1-vs3	nfs	137
172.17.180.171	vs4	siderop1-vs4	nfs	95
172.17.180.169	vs4	siderop1-vs4	nfs	92
172.17.180.123	vs4	siderop1-vs4	nfs	92
172.17.180.153	vs3	siderop1-vs3	nfs	0

2. クラスタで最も多くアクセスされる上位のファイルを表示します。

```
statistics top file show -node node_name -sort-key sort_column -interval  
seconds_between_updates -iterations iterations -max number_of_instances
```

コマンド構文全体については、マニュアルページを参照してください。

次のコマンドは、でアクセスされる上位のファイルを表示します cluster1：



```
cluster1::> statistics top file show
```

```
cluster1 : 3/23/2016 17:59:10
```

```

                                *Total
      File Volume Vserver      Node      Ops
-----
/vol/vol1/vm170-read.dat    vol1      vs4 siderop1-vsim4      22
/vol/vol1/vm69-write.dat    vol1      vs3 siderop1-vsim3       6
  /vol/vol2/vm171.dat        vol2      vs3 siderop1-vsim3       2
/vol/vol2/vm169.dat         vol2      vs3 siderop1-vsim3       2
  /vol/vol2/p123.dat         vol2      vs4 siderop1-vsim4       2
  /vol/vol2/p123.dat         vol2      vs3 siderop1-vsim3       2
/vol/vol1/vm171.dat         vol1      vs4 siderop1-vsim4       2
/vol/vol1/vm169.dat         vol1      vs4 siderop1-vsim4       2
/vol/vol1/vm169.dat         vol1      vs4 siderop1-vsim3       2
  /vol/vol1/p123.dat         vol1      vs4 siderop1-vsim4       2
```

**QoS** でスループットを保証

**QoS** の概要を使用してスループットを保証

ストレージサービス品質（QoS）を使用して、重要なワークロードのパフォーマンスが競合するワークロードの影響を受けて低下しないようにすることができます。競合するワークロードに Throughput Ceil<sub>天</sub> を設定して、システムリソースへの影響を制限したり、重要なワークロードに Throughput Floor<sub>下</sub> を設定したりすることで、競合するワークロードによる要求に関係なく最小のスループットターゲットを満たすことができます。同じワークロードに対して上限と下限を設定することもできます。

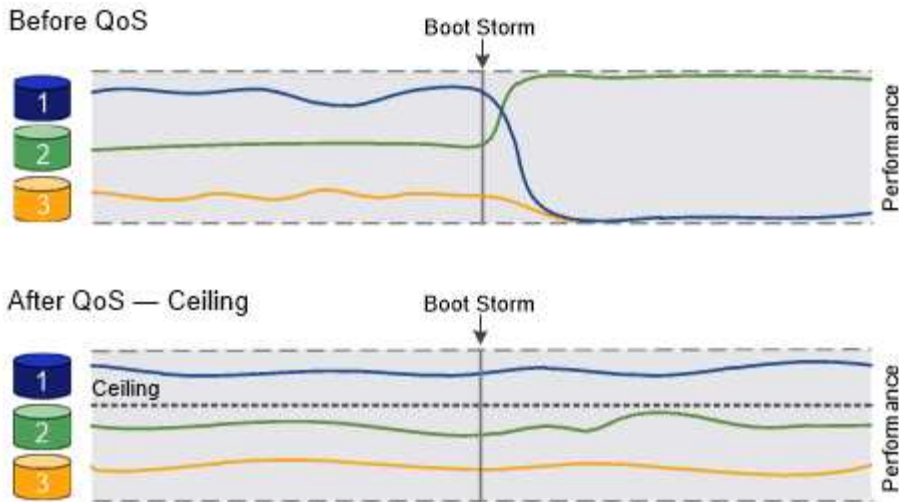
スループットの上限（最大 **QoS**）について

スループットの上限は、ワークロードのスループットを最大 IOPS / MBps、または IOPS / MBps に制限します。次の図では、ワークロード 2 がワークロード 1 および 3 の Bully にならないようにスループットの上限が設定されています。

a\_policy group<sub>下</sub> は、1 つ以上のワークロードに対するスループットの上限を定義します。ワークロードとは、a\_storage オブジェクト：\_a ボリューム、ファイル、qtree、または LUN、あるいは SVM 内のすべてのボリューム、ファイル、qtree、または LUN の I/O 処理のことです。上限はポリシーグループの作成時に指定できるほか、ワークロードをしばらく監視したあとで指定することもできます。



ワークロードのスループットは、特にスループットが急激に変化した場合、指定された上限を 10% までは超過することができます。バースト時には、上限を 50% まで超過することができます。バーストは、トークンが 150% まで累積した場合に単一ノードで発生します



### スループットの下限（最小 QoS）について

スループットの下限は、ワークロードのスループットが最小IOPS、最小MBps、またはIOPSとMBpsを下回らないことを保証します。次の図では、ワークロード 1 とワークロード 3 のスループットの下限により、ワークロード 2 からの要求に関係なく、最小スループットが確保されています。



これらの例からわかるように、スループットの上限はスループットを直接調整するのに対し、スループットの下限は下限が設定されたワークロードを優先することでスループットを間接的に調整します。

下限はポリシーグループの作成時に指定できるほか、ワークロードをしばらく監視したあとで指定することもできます。

ONTAP 9.13.1以降では、を使用してSVMスコープでスループットの下限を設定できます [\[adaptive-qos-templates\]](#)。ONTAP 9.13.1より前のリリースでは、スループットの下限を定義するポリシーグループはSVMに適用できません。

ONTAP 9.7 より前のリリースでは、使用可能なパフォーマンス容量が十分にある場合にスループットの下限が保証されます。



ONTAP 9.7 以降では、使用可能なパフォーマンス容量が不足している場合でもスループットの下限を保証できます。この新しいフロアビヘイビアをフロア v2 と呼びます。この保証を満たすために、v2 のフロアを使用すると、スループットの下限や下限の設定を超える作業を行わなくても、ワークロードのレイテンシが高くなる可能性があります。QoS とアダプティブ QoS の両方をサポートするフロア v2 環境。

ONTAP 9.7P6以降では、下限v2の新しい動作を有効または無効にするオプションを使用できます。などの重要な処理の実行中は、ワークロードが指定された下限を下回ることがあります volume move trigger-cutover。利用可能な容量が十分にあり、重要な処理が実行されていない場合でも、ワークロードのスループットは指定された下限を 5% まで下回ることができます。オーバプロビジョニングされたフロアやパフォーマンス容量がないワークロードがある場合、指定された下限を下回ることがあります。



### 共有および非共有の **QoS** ポリシーグループについて

ONTAP 9.4 以降では、`_non-shared_QoS` ポリシーグループを使用して、定義されたスループットの上限または下限の環境を各メンバーのワークロードごとに指定できます。`_shared_policy` グループの動作は 'ポリシー' タイプによって異なります

- スループットの上限については、共有ポリシーグループに割り当てられたワークロードの合計スループットが指定した上限以下でなければなりません。
- スループットの下限については、共有ポリシーグループを適用できるのは単一のワークロードのみです。

### アダプティブ **QoS** について

通常、ストレージオブジェクトに割り当てたポリシーグループの値は固定値です。ストレージオブジェクトのサイズが変わったときは、値を手動で変更する必要があります。たとえば、ボリュームの使用スペースが増えた場合、通常は指定されているスループットの上限も増やす必要があります。

アダプティブ QoS \_ワークロードのサイズの変更に合わせてポリシーグループの値が自動的に調整され、TB または GB あたりの IOPS が一定に維持されます。これは、何百何千という数のワークロードを管理する大規模な環境では大きなメリットです。

アダプティブ QoS は、主にスループットの上限の調整に使用しますが、下限の管理（ワークロードサイズが増えた場合）に使用することもできます。ワークロードのサイズは、ストレージオブジェクトに割り当てられたスペースまたはストレージオブジェクトで使用されているスペースのいずれかで表されます。



ONTAP 9.5 以降では、使用済みスペースをスループットの下限に使用できます。ONTAP 9.4 以前では使用できません。

- 割り当て済みスペースのポリシーでは、ストレージオブジェクトの公称サイズを基準に IOPS と TB / GB の比率が維持されます。比率が 100 IOPS/GB の場合、150GB のボリュームのスループットの上限はボリュームのサイズが変更されないかぎり 15、000 IOPS です。ボリュームのサイズが 300GB に変更されると、アダプティブ QoS によってスループットの上限が 30、000 IOPS に調整されます。
- `a_used space-policy`（デフォルト）は、ストレージ効率化前に格納されている実際のデータの量に基づいて、IOPS/TB|GB の比率を維持します。比率が 100 IOPS/GB の場合、100GB のデータが格納された 150GB のボリュームのスループットの上限は 10、000 IOPS です。使用済みスペースの量が変わると、アダプティブ QoS によって比率が一定になるようにスループットの上限が調整されます。

ONTAP 9.5 以降では、アプリケーションに I/O ブロックサイズを指定することで、スループット制限を IOPS と MBps の両方で指定できます。MBps の制限は、ブロックサイズに IOPS 制限を掛けて計算されます。たとえば、32K の I/O ブロックサイズで IOPS の制限が 6144 IOPS/TB の場合、MBps の制限は 192MBps になります。

以下は、スループットの上限と下限の両方に対して想定される動作です。

- アダプティブ QoS ポリシーグループにワークロードを割り当てると、上限または下限がただちに更新されます。
- アダプティブ QoS ポリシーグループに含まれるワークロードのサイズを変更すると、上限または下限が約 5 分で更新されます。

更新が実行されるためにはスループットが少なくとも 10 IOPS 増加する必要があります。

アダプティブ QoS ポリシーグループは常に非共有です。定義されているスループットの上限または下限の環境各メンバーワークロードを個別に定義します。

ONTAP 9.6以降では、SSDを使用するONTAP Select Premiumでスループットの下限がサポートされます。

アダプティブポリシーグループテンプレート

ONTAP 9.13.1以降では、アダプティブQoSテンプレートをSVMに設定できます。アダプティブポリシーグループテンプレートを使用すると、SVM内のすべてのボリュームにスループットの下限と上限を設定できます。

アダプティブポリシーグループテンプレートは、SVMの作成後にのみ設定できます。を使用します `vserver modify` コマンドにを指定します `-qos-adaptive-policy-group-template` ポリシーを設定するパラメータ。

アダプティブポリシーグループテンプレートを設定すると、ポリシーの設定後に作成または移行されたボリュームには自動的にポリシーが継承されます。ポリシーテンプレートを割り当てても、SVM上の既存のボリュームには影響しません。SVMでポリシーを無効にすると、以降SVMに移行または作成されたボリュームにポリシーは適用されません。アダプティブポリシーグループテンプレートを無効にしても、ポリシーテンプレートが保持されるため、そのポリシーテンプレートを継承したボリュームには影響しません。

詳細については、を参照してください [アダプティブポリシーグループテンプレートを設定します](#)。

一般的なサポート

次の表に、スループットの上限、スループットの下限、およびアダプティブ QoS のサポート状況を示します。

リソースまたは機能	スループットの上限	スループットの下限	スループットの下限 v2	アダプティブ QoS
ONTAP 9 バージョン	すべて	9.2以降	9.7以降	9.3以降

リソースまたは機能	スループットの上限	スループットの下限	スループットの下限 v2	アダプティブ QoS
プラットフォーム	すべて	<ul style="list-style-type: none"> <li>• AFF</li> <li>• C190 *</li> <li>• ONTAP Select プレミアム SSD *</li> </ul>	<ul style="list-style-type: none"> <li>• AFF</li> <li>• C190</li> <li>• SSD を使用する ONTAP Select Premium</li> </ul>	すべて
プロトコル	すべて	すべて	すべて	すべて
FabricPool	はい。	階層化ポリシーが「none」に設定され、ブロックがクラウドにない場合は「Yes」です。	階層化ポリシーが「none」に設定され、ブロックがクラウドにない場合は「Yes」です。	いいえ
SnapMirror Synchronous	はい。	いいえ	いいえ	はい。

C190とONTAP Selectのサポートは、ONTAP 9.6リリースから開始されました。

#### スループットの上限がサポートされるワークロード

次の表に、スループットの上限がサポートされるワークロードを ONTAP 9 のバージョン別に示します。ルートボリューム、負荷共有ミラー、およびデータ保護ミラーはサポートされません。

ワークロード - 上限	ONTAP 9.0	ONTAP 9.1	ONTAP 9.2	ONTAP 9.3	ONTAP 9.4~9.7	ONTAP 9.8以降
ボリューム	はい。	はい。	はい。	はい。	はい。	はい。
ファイル。	はい。	はい。	はい。	はい。	はい。	はい。
LUN	はい。	はい。	はい。	はい。	はい。	はい。
SVM	はい。	はい。	はい。	はい。	はい。	はい。
FlexGroup ボリューム	いいえ	いいえ	いいえ	はい。	はい。	はい。
qtree *	いいえ	いいえ	いいえ	いいえ	いいえ	はい。

ワークロード - 上限	ONTAP 9.0	ONTAP 9.1	ONTAP 9.2	ONTAP 9.3	ONTAP 9.4~9.7	ONTAP 9.8以降
ポリシーグループごとに複数のワークロードが割り当てられます	はい。	はい。	はい。	はい。	はい。	はい。
非共有のポリシーグループ	いいえ	いいえ	いいえ	いいえ	はい。	はい。

ONTAP 9.8以降では、NFSが有効なFlexVolおよびFlexGroupのqtreeでNFSアクセスがサポートされます。ONTAP 9.9.1以降では、SMBが有効なFlexVol およびFlexGroup ボリュームのqtreeでもSMBアクセスがサポートされます。

#### スループットの下限がサポートされるワークロード

次の表に、スループットの下限がサポートされるワークロードを ONTAP 9 のバージョン別に示します。ルートボリューム、負荷共有ミラー、およびデータ保護ミラーはサポートされません。

ワークロード - 下限	ONTAP 9.2	ONTAP 9.3	ONTAP 9.4~9.7	ONTAP 9.8-9.13.0	ONTAP 9.13.1以降
ボリューム	はい。	はい。	はい。	はい。	はい。
ファイル。	いいえ	はい。	はい。	はい。	はい。
LUN	はい。	はい。	はい。	はい。	はい。
SVM	いいえ	いいえ	いいえ	いいえ	はい。
FlexGroup ボリューム	いいえ	いいえ	はい。	はい。	はい。
qtree *	いいえ	いいえ	いいえ	はい。	はい。
ポリシーグループごとに複数のワークロードが割り当てられます	いいえ	いいえ	はい。	はい。	はい。
非共有のポリシーグループ	いいえ	いいえ	はい。	はい。	はい。

※ ONTAP 9.8以降では、NFSが有効なFlexVol およびFlexGroup のqtreeでNFSアクセスがサポートされます。ONTAP 9.9.1以降では、SMBが有効なFlexVol およびFlexGroup ボリュームのqtreeでもSMBアクセスがサポートされます。

#### アダプティブ QoS がサポートされるワークロード

次の表に、アダプティブ QoS がサポートされるワークロードを ONTAP 9 のバージョン別に示します。ルートボリューム、負荷共有ミラー、およびデータ保護ミラーはサポートされません。

ワークロード - アダプティブ QoS	ONTAP 9.3	ONTAP 9.4-9.13.0	ONTAP 9.13.1以降
ボリューム	はい。	はい。	はい。
ファイル。	いいえ	はい。	はい。
LUN	いいえ	はい。	はい。
SVM	いいえ	いいえ	はい。
FlexGroup ボリューム	いいえ	はい。	はい。
ポリシーグループごとに 複数のワークロードが割 り当てられます	はい。	はい。	はい。
非共有のポリシーグルー プ	はい。	はい。	はい。

## ワークロードとポリシーグループの最大数

次の表に、ワークロードとポリシーグループの最大数を ONTAP 9 のバージョン別に示します。

ワークロードのサポート	ONTAP 9.3以前	ONTAP 9.4以降
クラスタあたりの最大ワークロード	12、000	4万だ
ノードあたりの最大ワークロード	12、000	4万だ
ポリシーグループの最大数	12、000	12、000

スループットの下限 **v2** を有効または無効にします

AFF のスループットの下限 v2 を有効または無効にすることができます。デフォルトは **enabled** です。フロア v2 を有効にした場合、他のワークロードのレイテンシが高くなってもコントローラを多用した場合はスループットの下限を満たすことができます。QoS とアダプティブ QoS の両方をサポートするフロア v2 環境。

## 手順

1. advanced 権限レベルに切り替えます。

```
set -privilege advanced
```

2. 次のいずれかのコマンドを入力します。

状況	使用するコマンド
フロア v2 を無効にします	<code>qos settings throughput-floors-v2 -enable false</code>

状況	使用するコマンド
フロア v2 を有効にします	<code>qos settings throughput-floors-v2 -enable true</code>



MetroCluster クラスタでスループットの下限 v2 を無効にするには、を実行する必要があります

```
qos settings throughput-floors-v2 -enable false
```

コマンドは、ソースとデスティネーションの両方のクラスタで実行します。

```
cluster1::*> qos settings throughput-floors-v2 -enable false
```

## ストレージ QoS のワークフロー

QoS で管理するワークロードのパフォーマンス要件がすでにわかっている場合は、ポリシーグループを作成するときにスループットの制限を指定できます。それ以外の場合は、ワークロードを監視したうえで指定することができます。

### QoS を使用してスループットの上限を設定する

使用できます `max-throughput` ストレージオブジェクトのワークロードのスループットの上限（最大QoS）を定義するポリシーグループのフィールド。ポリシーグループは、ストレージオブジェクトを作成または変更するときに適用できます。

#### 必要なもの

- ポリシーグループを作成するには、クラスタ管理者である必要があります。
- ポリシーグループを SVM に適用するには、クラスタ管理者である必要があります。

#### このタスクについて

- ONTAP 9.4 以降では、`_non-shared_QoS` ポリシーグループを使用して、定義されたスループットの上限環境を各メンバーのワークロードごとに指定できます。ポリシーグループが `_shared` : ポリシーグループに割り当てられているワークロードの合計スループットが指定した上限を超えることはできません。

設定 `-is-shared=false` をクリックします `qos policy-group create` 非共有ポリシーグループを指定するコマンド。

- スループットの上限は、IOPS、MB/ 秒、またはその両方で指定できます IOPS と MB/ 秒の両方を指定した場合、先に上限に達した方が適用されます。



同じワークロードに対して上限と下限を設定する場合、スループット制限は IOPS 単位でのみ指定できます。

- QoS 制限の対象となるストレージオブジェクトは、ポリシーグループが属している SVM に含める必要が



あります。同じ SVM に複数のポリシーグループを作成することができます。

- 下位のオブジェクトまたは子オブジェクトがポリシーグループに属している場合は、そのストレージオブジェクトをポリシーグループに割り当てることはできません。
- ストレージオブジェクトのタイプごとに同じ QoS グループポリシーを適用することを推奨します。

## 手順

### 1. ポリシーグループを作成する。

```
qos policy-group create -policy-group policy_group -vserver SVM -max-throughput number_of_iops|Mb/S|iops,Mb/S -is-shared true|false
```

コマンド構文全体については、マニュアルページを参照してください。を使用できます `qos policy-group modify` コマンドを使用してスループットの上限を調整します。

次のコマンドは、共有ポリシーグループを作成します `pg-vs1` 最大スループットが5,000 IOPSの場合：

```
cluster1::> qos policy-group create -policy-group pg-vs1 -vserver vs1 -max-throughput 5000iops -is-shared true
```

次のコマンドは、非共有ポリシーグループを作成します `pg-vs3` 最大スループットが100 IOPS、400KB/秒の場合：

```
cluster1::> qos policy-group create -policy-group pg-vs3 -vserver vs3 -max-throughput 100iops,400KB/s -is-shared false
```

次のコマンドは、非共有ポリシーグループを作成します `pg-vs4` スループット制限なし：

```
cluster1::> qos policy-group create -policy-group pg-vs4 -vserver vs4 -is-shared false
```

### 2. ポリシーグループを SVM、ファイル、ボリューム、または LUN に適用します。

```
storage_object create -vserver SVM -qos-policy-group policy_group
```

コマンド構文全体については、マニュアルページを参照してください。を使用できます `storage_object modify` ストレージオブジェクトに別のポリシーグループを適用するコマンド。

次のコマンドは、ポリシーグループを適用します `pg-vs1` SVMに移動します `vs1`：

```
cluster1::> vsserver create -vserver vs1 -qos-policy-group pg-vs1
```

次のコマンドは、ポリシーグループを適用します `pg-app` ボリュームに移動します `app1` および `app2`：

```
cluster1::> volume create -vserver vs2 -volume app1 -aggregate aggr1
-qos-policy-group pg-app
```

```
cluster1::> volume create -vserver vs2 -volume app2 -aggregate aggr1
-qos-policy-group pg-app
```

### 3. ポリシーグループのパフォーマンスを監視します。

```
qos statistics performance show
```

コマンド構文全体については、マニュアルページを参照してください。



パフォーマンスはクラスタから監視します。ホスト上のツールを使用してパフォーマンスを監視しないでください。

次のコマンドは、ポリシーグループのパフォーマンスを表示します。

```
cluster1::> qos statistics performance show
```

Policy Group	IOPS	Throughput	Latency
-total-	12316	47.76MB/s	1264.00us
pg_vs1	5008	19.56MB/s	2.45ms
_System-Best-Effort	62	13.36KB/s	4.13ms
_System-Background	30	0KB/s	0ms

### 4. ワークロードのパフォーマンスを監視します。

```
qos statistics workload performance show
```

コマンド構文全体については、マニュアルページを参照してください。



パフォーマンスはクラスタから監視します。ホスト上のツールを使用してパフォーマンスを監視しないでください。

次のコマンドは、ワークロードのパフォーマンスを表示します。

```
cluster1::> qos statistics workload performance show
```

Workload	ID	IOPS	Throughput	Latency
-total-	-	12320	47.84MB/s	1215.00us
app1-wid7967	7967	7219	28.20MB/s	319.00us
vs1-wid12279	12279	5026	19.63MB/s	2.52ms
_USERSPACE_APPS	14	55	10.92KB/s	236.00us
_Scan_Backgro..	5688	20	0KB/s	0ms



を使用できます `qos statistics workload latency show` コマンドを使用してQoS ワークロードの詳細なレイテンシ統計を表示します。

**QoS** を使用してスループットの下限を設定します

を使用できます `min-throughput` ストレージオブジェクトのワークロードのスループットの下限（最小QoS）を定義するポリシーグループのフィールド。ポリシーグループは、ストレージオブジェクトを作成または変更するときに適用できます。ONTAP 9.8 以降では、スループットの下限を IOPS または MBps で指定できるようになりました。

作業を開始する前に

- ONTAP 9.2 以降が実行されている必要があります。スループットの下限は ONTAP 9.2 以降で使用できます。
- ポリシーグループを作成するには、クラスタ管理者である必要があります。
- ONTAP 9.13.1以降では、を使用してSVMレベルでスループットの下限を適用できます [アダプティブポリシーグループテンプレート](#)。QoSポリシーグループを含むSVMにアダプティブポリシーグループテンプレートを設定することはできません。

このタスクについて

- ONTAP 9.4 以降では、`_non-shared_qos` ポリシーグループを使用して、定義したスループットの下限を各メンバーワークロードに個別に適用するように指定できます。スループットの下限が定義されたポリシーグループを複数のワークロードに適用できるのは、この場合だけです。

設定 `-is-shared=false` をクリックします `qos policy-group create` 共有されていないポリシーグループを指定するコマンド。

- ノードまたはアグリゲートに十分なパフォーマンス容量（ヘッドルーム）がない場合は、ワークロードのスループットが指定された下限を下回ることがあります。
- QoS 制限の対象となるストレージオブジェクトは、ポリシーグループが属している SVM に含める必要があります。同じ SVM に複数のポリシーグループを作成することができます。
- ストレージオブジェクトのタイプごとに同じ QoS グループポリシーを適用することを推奨します。
- スループットの下限を定義するポリシーグループは、SVM には適用できません。

手順

1. の説明に従って、ノードまたはアグリゲートに十分なパフォーマンス容量があることを確認します ["残りのパフォーマンス容量を特定しています"](#)。

## 2. ポリシーグループを作成する。

```
qos policy-group create -policy group policy_group -vserver SVM -min  
-throughput qos_target -is-shared true|false
```

コマンド構文全体については、ONTAP リリースのマニュアルページを参照してください。を使用できます `qos policy-group modify` スループットの下限を調整するコマンド。

次のコマンドは、共有ポリシーグループを作成します `pg-vs2` 最小スループットが1、000 IOPSの場合：

```
cluster1::> qos policy-group create -policy group pg-vs2 -vserver vs2  
-min-throughput 1000iops -is-shared true
```

次のコマンドは、非共有ポリシーグループを作成します `pg-vs4` スループット制限なし：

```
cluster1::> qos policy-group create -policy group pg-vs4 -vserver vs4  
-is-shared false
```

## 3. ポリシーグループをボリュームまたは LUN に適用します。

```
storage_object create -vserver SVM -qos-policy-group policy_group
```

コマンド構文全体については、マニュアルページを参照してください。を使用できます `_storage_object_modify` ストレージオブジェクトに別のポリシーグループを適用するコマンド。

次のコマンドは、ポリシーグループを適用します `pg-app2` ボリュームに移動します `app2`：

```
cluster1::> volume create -vserver vs2 -volume app2 -aggregate aggr1  
-qos-policy-group pg-app2
```

## 4. ポリシーグループのパフォーマンスを監視します。

```
qos statistics performance show
```

コマンド構文全体については、マニュアルページを参照してください。



パフォーマンスはクラスタから監視します。ホスト上のツールを使用してパフォーマンスを監視しないでください。

次のコマンドは、ポリシーグループのパフォーマンスを表示します。

```
cluster1::> qos statistics performance show
```

Policy Group	IOPS	Throughput	Latency
-total-	12316	47.76MB/s	1264.00us
pg_app2	7216	28.19MB/s	420.00us
_System-Best-Effort	62	13.36KB/s	4.13ms
_System-Background	30	0KB/s	0ms

## 5. ワークロードのパフォーマンスを監視します。

```
qos statistics workload performance show
```

コマンド構文全体については、マニュアルページを参照してください。



パフォーマンスはクラスタから監視します。ホスト上のツールを使用してパフォーマンスを監視しないでください。

次のコマンドは、ワークロードのパフォーマンスを表示します。

```
cluster1::> qos statistics workload performance show
```

Workload	ID	IOPS	Throughput	Latency
-total-	-	12320	47.84MB/s	1215.00us
app2-wid7967	7967	7219	28.20MB/s	319.00us
vs1-wid12279	12279	5026	19.63MB/s	2.52ms
_USERSPACE_APPS	14	55	10.92KB/s	236.00us
_Scan_Backgro...	5688	20	0KB/s	0ms



を使用できます `qos statistics workload latency show` コマンドを使用してQoS ワークロードの詳細なレイテンシ統計を表示します。

## アダプティブ QoS ポリシーグループを使用する

アダプティブ QoS ポリシーグループを使用すると、ボリュームサイズの変更に合わせてスループットの上限や下限を自動的に調整し、TB または GB あたりの IOPS を一定に保つことができます。これは、何百何千という数のワークロードを管理する大規模な環境では大きなメリットです。

作業を開始する前に

- ONTAP 9.3以降が実行されている必要があります。アダプティブ QoS ポリシーグループは ONTAP 9.3 以降で使用できます。
- ポリシーグループを作成するには、クラスタ管理者である必要があります。

このタスクについて

ストレージオブジェクトは、アダプティブまたは非アダプティブどちらかのポリシーグループのメンバーにすることができますが、両方のメンバーにすることはできません。SVM はストレージオブジェクトとポリシーで同じである必要があります。ストレージオブジェクトはオンラインである必要があります。

アダプティブ QoS ポリシーグループは常に非共有です。定義されているスループットの上限または下限の環境各メンバーワークロードを個別に定義します。

ストレージオブジェクトサイズに対するスループット制限の比率は、以下に示すフィールドの組み合わせによって決まります。

- `expected-iops` は、割り当て済み (TB / GB) あたりの最小想定IOPSです。



``expected-iops`` は、AFF プラットフォームでのみ保証されます。  
``expected-iops`` FabricPool については、階層化ポリシーが「none」に設定されていて、ブロックがクラウドにない場合にのみ保証されます。  
``expected-iops`` は、SnapMirror Synchronous 関係にないボリュームに対して保証されます。

- `peak-iops` は、割り当て済みまたは使用済み (TB / GB) あたりの最大IOPSです。
- `expected-iops-allocation` `expected-iops`に割り当てスペース (デフォルト) と使用スペースのどちらを使用するかを示します。



`expected-iops-allocation` ONTAP 9.5以降で使用できます。ONTAP 9.4 以前ではサポートされません。

- `peak-iops-allocation` に割り当てスペースと使用済みスペース (デフォルト) のどちらを使用するかを示します `peak-iops`。
- `absolute-min-iops` は、絶対最小IOPSです。このフィールドは非常に小さいストレージオブジェクトで使用します。両方を上書きします `peak-iops` および / または `expected-iops` かつ `absolute-min-iops` が計算されたよりも大きい `expected-iops`。

たとえば、を設定した場合です `expected-iops` を1,000 IOPS/TBに設定し、ボリュームサイズが1GB未満である場合は、を計算します `expected-iops` 分数IOPになります。計算された `peak-iops` さらに小さな割合になりますこれを回避するには、を設定します `absolute-min-iops` 現実的な値に。

- `block-size` アプリケーションI/Oブロックサイズを指定します。デフォルトは32Kです。有効な値は、8K、16K、32K、64K、ANY です。ANY は、ブロックサイズが適用されないことを意味します。

次の表に示す 3 種類のアダプティブ QoS ポリシーグループがデフォルトで用意されています。これらのポリシーグループはボリュームに直接適用することができます。

デフォルトのポリシーグループ	想定 IOPS/TB	最大 IOPS/TB	絶対最小 IOPS
extreme	6,144	一二、二八八	1000
performance	2、048	四、〇九六	500ドル

value	128	512	七五
-------	-----	-----	----

下位のオブジェクトまたは子オブジェクトがポリシーグループに属している場合は、そのストレージオブジェクトをポリシーグループに割り当てることはできません。次の表に、制限事項を示します。

割り当て内容	以下のオブジェクトはポリシーグループに割り当てできない
SVM をポリシーグループに割り当てます	SVM に含まれているストレージオブジェクトのポリシーグループへの割り当て
ボリューム：ポリシーグループに割り当てます	そのボリュームを含む SVM または子 LUN
LUN	その LUN を含むボリュームまたは SVM
ファイルをポリシーグループに追加します	そのファイルを含むボリュームまたは SVM

## 手順

### 1. アダプティブ QoS ポリシーグループを作成します。

```
qos adaptive-policy-group create -policy group policy_group -vserver SVM
-expected-iops number_of_iops/TB|GB -peak-iops number_of_iops/TB|GB -expected
-iops-allocation-space|used-space -peak-iops-allocation allocated-space|used-
space -absolute-min-iops number_of_iops -block-size 8K|16K|32K|64K|ANY
```

コマンド構文全体については、マニュアルページを参照してください。



-expected-iops-allocation および -block-size ONTAP 9.5以降で使用できます。ONTAP 9.4 以前ではこれらのオプションがサポートされません。

次のコマンドは、アダプティブQoSポリシーグループを作成します `adpg-app1` を使用 `-expected-iops` TBあたり300 IOPS/TBに設定 `-peak-iops` TBあたり1、000 IOPSに設定 `-peak-iops-allocation` をに設定します `used-space`` および ``-absolute-min-iops` 50 IOPSに設定：

```
cluster1::> qos adaptive-policy-group create -policy group adpg-app1
-vserver vs2 -expected-iops 300iops/tb -peak-iops 1000iops/TB -peak-iops
-allocation used-space -absolute-min-iops 50iops
```

### 2. アダプティブ QoS ポリシーグループをボリュームに適用します。

```
volume create -vserver SVM -volume volume -aggregate aggregate -size number_of
TB|GB -qos-adaptive-policy-group policy_group
```

コマンド構文全体については、マニュアルページを参照してください。

次のコマンドは、アダプティブQoSポリシーグループを適用します `adpg-app1` ボリュームに移動します

app1 :

```
cluster1::> volume create -vserver vs1 -volume app1 -aggregate aggr1  
-size 2TB -qos-adaptive-policy-group adpg-app1
```

次のコマンドは、デフォルトのアダプティブQoSポリシーグループを適用します `extreme` 新しいボリュームに移動します `app4` および既存のボリュームに追加します `app5`。ポリシーグループの環境 ボリュームに対して定義されたスループットの上限 `app4` および `app5` 個別：

```
cluster1::> volume create -vserver vs4 -volume app4 -aggregate aggr4  
-size 2TB -qos-adaptive-policy-group extreme
```

```
cluster1::> volume modify -vserver vs5 -volume app5 -qos-adaptive-policy  
-group extreme
```

アダプティブポリシーグループテンプレートを設定します

ONTAP 9.13.1以降では、アダプティブポリシーグループテンプレートを使用して、SVMレベルでスループットの下限と上限を適用できます。

このタスクについて

- アダプティブポリシーグループテンプレートはデフォルトポリシーです `apg1`。ポリシーはいつでも変更できます。CLIまたはONTAP REST APIでのみ設定でき、既存のSVMにのみ適用できます。
- アダプティブポリシーグループテンプレートは、ポリシーの設定後にSVMで作成またはSVMに移行されるボリュームにのみ影響します。SVM上の既存のボリュームのステータスは維持されます。

アダプティブポリシーグループテンプレートを無効にした場合、SVM上のボリュームの既存のポリシーは保持されます。無効化の影響を受けるのは、あとでSVMに作成または移行されたボリュームだけです。

- QoSポリシーグループを含むSVMにアダプティブポリシーグループテンプレートを設定することはできません。
- アダプティブポリシーグループテンプレートは、AFF プラットフォーム向けに設計されています。アダプティブポリシーグループテンプレートは他のプラットフォームでも設定できますが、ポリシーによって最小スループットが適用されない場合があります。同様に、FabricPool アグリゲートまたは最小スループットをサポートしないアグリゲート内のSVMにアダプティブポリシーグループテンプレートを追加することもできますが、スループットの下限は適用されません。
- SVMがMetroCluster 構成またはSnapMirror関係に含まれている場合は、ミラーされたSVMにアダプティブポリシーグループテンプレートが適用されます。

手順

1. SVMを変更してアダプティブポリシーグループテンプレートを適用します。  
`vserver modify -qos-adaptive-policy-group-template apg1`
2. ポリシーが設定されたことを確認します。



## Unified Manager を使用してクラスタパフォーマンスを監視する

Active IQ Unified Manager を使用すると、可用性を最大限に高め、ネットアップの AFF および FAS ストレージインフラの制御を維持できるため、拡張性、サポート性、パフォーマンス、セキュリティを向上させることができます。

Active IQ Unified Manager はシステムヘルスを継続的に監視し、アラートを送信するため、お客様の組織は IT スタッフのリソースを解放できます。1 つのダッシュボードでストレージのステータスを瞬時に確認し、推奨される対処方法を通じて問題に迅速に対処できます。

ストレージのプロアクティブな管理や問題の迅速な解決に役立つ通知を検出、監視、受信できるため、データ管理が簡易化されます。ペタバイト規模のデータを単一のダッシュボードから監視して大規模なデータを管理できるため、管理効率が向上します。

Active IQ Unified Manager を使用すると、変動するビジネスニーズに対応し、パフォーマンスデータと高度な分析を使用してパフォーマンスを最適化できます。レポート機能を使用すると、標準レポートにアクセスしたり、ビジネス固有のニーズに合わせてカスタムの運用レポートを作成したりできます。

関連リンク：

- ["Active IQ Unified Managerの詳細はこちら"](#)
- ["Active IQ Unified Manager for VMwareの利用を開始する"](#)
- ["Active IQ Unified Manager for Linuxの使用を開始する"](#)
- ["Active IQ Unified Manager for Windowsの使用を開始する"](#)

## Cloud Insights を使用してクラスタパフォーマンスを監視する

NetApp Cloud Insights は、インフラ全体を可視化する監視ツールです。Cloud Insights を使用すると、パブリッククラウドやプライベートデータセンターなど、すべてのリソースの監視、トラブルシューティング、最適化を行うことができます。

### Cloud Insights には 2 つのエディションがあります

Cloud Insights 基本エディションは、ネットアップデータファブリック資産の監視と最適化を目的に設計されています。HCI を含むネットアップのすべてのリソースと、環境内の All Flash FAS（AFF）間の接続を無償で分析します。

Cloud Insights Standard エディションは、ネットアップデータファブリックに対応したインフラコンポーネントだけでなく、マルチベンダー / マルチクラウド環境にも焦点を当てています。豊富な機能により、100 を超えるサービスとリソースのサポートにアクセスできます。

今日の世界では、オンプレミスのデータセンターから複数のパブリッククラウドにリソースを活用しているため、アプリケーション自体からストレージレイのバックエンドディスクまで、完全なイメージを把握することが重要です。さらに、アプリケーションの監視（Kafka、MongoDB、Nginx など）もサポートされているため、最適な利用率レベルと完全なリスクバッファで運用するために必要な情報と知識を得ることができます。

す。

どちらのエディション（ Basic および Standard ）も NetApp Active IQ Unified Manager と統合できます。Active IQ Unified Managerを使用しているお客様は、Cloud Insightsユーザインターフェイス内で参加情報を確認できます。Active IQ Unified Managerに投稿された通知は見落とされず、Cloud Insightsのイベントに関連付けることができます。つまり、両方の世界を最大限に活用できます。

## すべてのリソースの監視、トラブルシューティング、最適化を行います

Cloud Insights を使用すると、問題の解決にかかる時間を大幅に短縮し、エンドユーザへの影響を防ぐことができます。また、クラウドインフラのコスト削減にも役立ちます。 実用的な情報でデータを保護することで、内部の脅威にさらされる危険性が軽減されます。

Cloud Insights を使用すると、パブリッククラウドからデータセンターまで、ハイブリッドインフラ全体を 1 箇所で可視化できます。 必要に応じてカスタマイズできる関連ダッシュボードを瞬時に作成できます。また、組織のニーズに合わせて、ターゲットを絞ったアラートや条件付きアラートを作成することもできます。

高度な異常検出機能により、問題が発生する前にプロアクティブに解決できます。 リソースの競合と低下を自動的に確認して、影響を受けたワークロードを迅速にリストアできます。 スタック内のさまざまなコンポーネント間の関係を自動的に構築することで、トラブルシューティングがより迅速になります。

使用されていないリソースや放置されたリソースを環境全体で特定することで、インフラの規模を適正化し、支出全体を最適化する機会を見つけ出すことができます。

Cloud Insights は、システムトポロジを可視化し、Kubernetes アーキテクチャを把握します。Kubernetes クラスタの健全性を監視できます。問題が発生しているノードを監視し、問題が発生したときにズームインすることができます。

Cloud Insights は、高度な機械学習と異常検出機能により、悪意のあるユーザや侵害されたユーザによる組織データの不正利用を防止し、内部の脅威に関する実用的な情報を提供します。

Cloud Insights は Kubernetes 指標を可視化することで、ポッド、ノード、クラスタ間の関係を完全に把握できるようになります。クラスタまたは作業ポッドの正常性、および現在処理中の負荷を評価できます。これにより、K8S クラスタのコマンドを実行し、展開の健全性とコストの両方を制御できます。

### 関連リンク

- ["Cloud Insightsの詳細はこちら"](#)
- ["Cloud Insightsの使用を開始する"](#)

## 監査ロギング

### ONTAP での監査ログの実装方法

監査ログに記録された管理アクティビティは標準の AutoSupport レポートに、特定のログアクティビティは EMS メッセージに含まれています。監査ログを指定の場所に転送したり、CLI や Web ブラウザを使用して監査ログファイルを表示することもできます。

ONTAP 9.11.1以降では、System Managerを使用して監査ログの内容を表示できます。

ONTAP 9.12.1以降では、ONTAPで監査ログの改ざんアラートが提供されます。ONTAPは、audit.log ファイルの改ざんをチェックするために毎日のバックグラウンドジョブを実行し、変更または改ざんされたログファイルが見つかったらEMSアラートを送信します。

ONTAP では、クラスタで実行された管理アクティビティについて、発行された要求、要求を発行したユーザ、ユーザのアクセス方法、要求が発行された時間などの情報が記録されます。

管理アクティビティには次のタイプがあります。

- set要求。通常は表示以外のコマンドや操作が該当します
  - これらの要求は、を実行したときに発行されます create、modify`または `delete たとえば、コマンドです。
  - set 要求はデフォルトで記録されます。
- get要求。情報を取得して管理インターフェイスに表示します
  - これらの要求は、を実行したときに発行されます show たとえば、コマンドです。
  - GET要求はデフォルトでは記録されませんが、ONTAP CLIから送信されるGET要求を制御できます ( -cliget) 、ONTAP APIから (-ontapiget) 、またはREST APIから (-httpget) がファイルに記録されます。

ONTAP は、の管理アクティビティを記録します /mroot/etc/log/mlog/audit.log ノードのファイル。CLI コマンドの 3 つのシェル（クラスタシェル、ノードシェル、および非対話型システムシェル）からのコマンドに加え、API コマンドがここに記録されます（対話型システムシェルのコマンドは記録されません）。監査ログには、クラスタ内のすべてのノードの時刻が同期しているかどうかを示すタイムスタンプが含まれています。

◦ audit.log ファイルは、AutoSupport ツールによって指定された受信者に送信されます。また、Splunk や syslog サーバなど、指定した外部の送信先にコンテンツを安全に転送することもできます。

◦ audit.log ファイルは1日単位でローテーションされます。また、サイズが 100MB に達したときにもローテーションが実行されます。以前の 48 個のコピーは保持されます（最大合計 49 個のファイル）。監査ファイルが 1 日単位のローテーションを実行するときは、EMS メッセージは生成されません。監査ファイルのサイズが上限を超えたためにローテーションが実行された場合は、EMS メッセージが生成されます。

## ONTAP 9 における監査ログの変更点

ONTAP 9以降では、を参照してください command-history.log ファイルはに置き換えられます audit.log`および `mgwd.log ファイルに監査情報が含まれなくなりました。ONTAP 9 にアップグレードする場合は、これらの従来のファイルとその中身を参照するスクリプトやツールを見直す必要があります。

ONTAP 9へのアップグレード後、既存 command-history.log ファイルは保持されます。これらは新規として回転（削除）されます audit.log ファイルはローテーションされます（作成されます）。

をチェックするツールとスクリプト command-history.log からのソフトリンクがあるため、ファイルは引き続き機能する場合があります command-history.log 終了： audit.log は、アップグレード時に作成されます。ただし、をチェックするツールとスクリプト mgwd.log ファイルに監査情報が含まれなくなったため、ファイルは失敗します。

また、ONTAP 9 以降の監査ログでは、以下のエントリは有用な情報とはみなされず、原因の不要なログアク

ティビティでもあるため、記録されなくなりました。

- ONTAP によって実行される内部コマンド（username=root のコマンド）
- コマンドのエイリアス（元のコマンドとは別に）

ONTAP 9 以降では、TCP プロトコルと TLS プロトコルを使用して監査ログを外部の宛先に安全に送信できます。

## 監査ログの内容を表示します

クラスタの内容を表示できます `/mroot/etc/log/mlog/audit.log` ONTAP CLI、System Manager、またはWebブラウザを使用して実行します。

クラスタのログファイルには、次のエントリが含まれます。

### 時間

ログエントリのタイムスタンプ。

### アプリケーション

クラスタへの接続に使用するアプリケーション。指定可能な値の例はです `internal`, `console`, `ssh`, `http`, `ontapi`, `snmp`, `rsh`, `telnet`, および `service-processor`。

### ユーザ

リモートユーザのユーザ名。

### 状態

監査要求の現在の状態 `success`, `pending`, または `error`。

### メッセージ

コマンドのステータスに関するエラーまたは追加情報 を含むオプションのフィールド。

### セッションID

要求を受信したセッションID。各SSH\_SESSION\_ISにはセッションIDが割り当てられ、各HTTP、ONTAPI、またはSNMP\_REQUESTには一意のセッションIDが割り当てられます。

### Storage VM

ユーザの接続に使用するSVM。

### 適用範囲

表示されます `svm` 要求がデータStorage VM上にある場合。それ以外の場合はと表示されます `cluster`。

### コマンドID

CLIセッションで受信した各コマンドのID。これにより、要求と応答を関連付けることができます。ZAPI、HTTP、SNMPの各要求にはコマンドIDはありません。

クラスタのログエントリは、ONTAP CLIから、Webブラウザから、ONTAP 9.11.1以降のSystem Managerから表示できます。

### System Manager の略

- インベントリを表示するには、[\* Events & Jobs]>[Audit Logs]を選択します。[+] 各列には、カテゴリのフィルタ、並べ替え、検索、表示、およびインベントリを制御できます。インベントリの詳細は、Excelブックとしてダウンロードできます。
- フィルタを設定するには、右上の\*[Filter]\*ボタンをクリックし、目的のフィールドを選択します。[+] セッションIDリンクをクリックして、障害が発生したセッションで実行されたすべてのコマンドを表示することもできます。

### CLI の使用

クラスタ内の複数のノードからマージされた監査エントリを表示するには、+と入力します

```
security audit log show [parameters]
```

を使用できます security audit log show 個々のノードの監査エントリを表示するコマンド、またはクラスタ内の複数のノードの監査エントリをマージするコマンド。の内容を表示することもできます /mroot/etc/log/mlog Webブラウザを使用して、単一のノード上のディレクトリを作成します。詳細については、のマニュアルページを参照してください。

### Web ブラウザ


の内容を表示できます /mroot/etc/log/mlog Webブラウザを使用して、単一のノード上のディレクトリを作成します。"[Webブラウザを使用してノードのログファイル、コアダンプファイル、MIBファイルにアクセスする方法について説明します](#)"。

## 監査GET要求の設定を管理します

set要求はデフォルトで記録されますが、get要求は記録されません。ただし、ONTAP HTMLから送信されるGET要求を制御することはできます (-httpget)、ONTAP CLI (-cliget)、またはONTAP APIからアクセスできます (-ontapiget) がファイルに記録されます。

監査ログ設定は、ONTAP CLIから、ONTAP 9.11.1以降の監査ログ設定は、System Managerから変更できます。

### System Manager の略

1. [\* Events & Jobs]>[Audit Logs]を選択します。
2. をクリックします  右上にあるをクリックし、追加または削除する要求を選択します。

### CLI の使用

- デフォルトのset要求に加えて、ONTAP CLIまたはAPIからのget要求を監査ログ (audit.logファイル) に記録するように指定するには、+と入力します

```
security audit modify [-cliget {on|off}][{-httpget {on|off}}][{-ontapiget {on|off}}]
```
- 現在の設定を表示するには、+と入力します

```
security audit show
```

詳細については、マニュアルページを参照してください。

## 監査ログの送信先を管理します

監査ログは最大で10箇所に転送できます。たとえば、Splunk や syslog サーバにログを転送し、監視や分析、バックアップなどの目的で使用できます。

このタスクについて

転送を設定するには、転送されたログに使用するsyslogまたはSplunkホストのIPアドレス、ポート番号、転送プロトコル、syslog機能を指定する必要があります。"[syslogファシリティについて説明します](#)"。

次のいずれかの送信値を選択できます。

### UDP暗号化なし

セキュリティなしのユーザデータグラムプロトコル（デフォルト）

### TCP暗号化なし

セキュリティなしのTransmission Control Protocol

### TCP暗号化

Transport Layer Security（TLS）を使用したTransmission Control Protocol

[TCP暗号化プロトコル]が選択されている場合は、[VERIFY SERVER]オプションを使用できます。

監査ログは、ONTAP CLIから転送できます。ONTAP 9.11.1以降は、System Managerから転送できます。

## System Manager の略

- 監査ログの送信先を表示するには、\* Cluster > Settings の順に選択します。[+] ログデスティネーションの数は、[通知管理]タイル\*に表示されます。をクリックします ⓘ 詳細を表示します。
- 監査ログの送信先を追加、変更、または削除するには、[Events & Jobs]>[Audit Logs]を選択し、画面右上の[\*Manage Audit Destinations]をクリックします。[+] をクリックします + Add またはをクリックします ⓘ エントリを編集または削除するには、\* Host Address \*列に入力します。

## CLI の使用

1. 監査ログの転送先ごとに、デスティネーション IP アドレスまたはホスト名、およびセキュリティオプションを指定します。

```
cluster1::> cluster log-forwarding create -destination
192.168.123.96
-port 514 -facility user

cluster1::> cluster log-forwarding create -destination
192.168.123.98
-port 514 -protocol tcp-encrypted -facility user
```

- 状況に応じて cluster log-forwarding create コマンドが接続を確認するためにデスティネーションホストにpingを実行できない場合、エラーが表示されてコマンドが失敗します。推奨されませんが、を使用してください -force パラメータを指定すると、接続の検証が省略されます。
  - を設定した場合 -verify-server パラメータの値 true`では、ログの転送先のIDは、証明書を検証することによって検証されます。この値はに設定できます `true を選択した場合のみ tcp-encrypted の値 -protocol フィールド。
2. を使用して、宛先レコードが正しいことを確認します cluster log-forwarding show コマンドを実行します

```
cluster1::> cluster log-forwarding show
```

Destination Host	Port	Protocol	Verify Server	Syslog Facility
192.168.123.96	514	udp-unencrypted	false	user
192.168.123.98	514	tcp-encrypted	true	user

2 entries were displayed.

詳細については、マニュアルページを参照してください。

# AutoSupport

## System Manager を使用して AutoSupport 設定を管理します

System Managerを使用して、AutoSupportアカウントの設定を管理できます。

次の手順を実行できます。

### AutoSupport 設定を表示します

System Manager を使用して、AutoSupport アカウントの設定を表示できます。

#### 手順

1. System Manager で、\* Cluster > Settings \* の順にクリックします。

「\* AutoSupport \*」セクションには、次の情報が表示されます。

- ステータス
- 転送プロトコル
- プロキシサーバ
- 送信元 E メールアドレス


2. AutoSupport セクションで、をクリックし、[その他のオプション]\*を選択します。

AutoSupport 接続と E メール設定については、追加情報が表示されます。また、メッセージの転送履歴も表示されます。

### AutoSupport データを生成して送信します

System Manager では、AutoSupport メッセージの生成を開始して、データを収集するクラスターノードを選択できます。


#### 手順

1. System Managerで、\* Cluster > Settings \*の順に選択します。
2. AutoSupport セクションで、をクリックし、[生成して送信]\*を選択します。
3. 件名を入力します。
4. [データの収集元]\*のチェックボックスをオンにして、データの収集元のノードを指定します。

### AutoSupport への接続をテストします

System Manager からテストメッセージを送信して、AutoSupport への接続を確認できます。

#### 手順

1. System Manager で、\* Cluster > Settings \* の順にクリックします。
2. AutoSupport セクションで、をクリックし、[Test Connectivity]\*を選択します。
3. メッセージの件名を入力します。



## AutoSupport を有効または無効にします



AutoSupportは、可能性のある構成上の問題をプロアクティブに特定し、サポートケースを迅速に解決するなど、NetAppのお客様に実証済みのビジネスメリットを提供します。新しいシステムでは、AutoSupportはデフォルトで有効になっています。必要に応じて、System Managerを使用して、ストレージシステムのヘルスを監視して通知メッセージを送信するAutoSupportの機能を無効にすることができます。AutoSupport を無効にしたあとで再度有効にすることができます。

### このタスクについて

AutoSupportを無効にする前に、NetAppコールホームシステムをオフにすると、次の利点が失われることに注意してください。

- **ヘルスマonitoring:** AutoSupportはストレージシステムのヘルスを監視し、テクニカルサポートおよび社内のサポート部門に通知を送信します。
- **自動化:** AutoSupportはサポートケースのレポートを自動化します。ほとんどのサポートケースは、お客様が問題に気付く前に自動的にオープンされます。
- **迅速な解決:** AutoSupportデータを送信するシステムでは、AutoSupportデータを送信しないシステムと比較して、サポートケースが半分の時間で解決されます。
- **アップグレードの高速化:** AutoSupportは、System Managerのバージョンアップグレード、アドオン、更新、ファームウェア更新の自動化など、お客様のセルフサービスワークフローを強化します。
- **その他の機能:** 他のツールの特定の機能（BlueXPの一部のワークフローなど）は、AutoSupportが有効な場合にのみ機能します。

### 手順

1. [\* Cluster]>[Settings]（設定）\*を選択します。
2. AutoSupport セクションで、をクリックし、[無効化]\*を選択します。
3. AutoSupportを再度有効にする場合は、\* AutoSupport セクションで をクリックし、[有効化]\*を選択します。

## サポートケースの生成を抑制します


ONTAP 9.10.1 以降の場合、System Manager から AutoSupport に要求を送信して、サポートケースの生成を抑制することができます。

### このタスクについて

サポートケースの生成を抑制するには、抑制を実行するノードと時間数を指定します。

システムのメンテナンス中に AutoSupport で自動ケースを作成しない場合は、サポートケースを抑制することが特に役立ちます。


### 手順

1. [\* Cluster]>[Settings]（設定）\*を選択します。
2. AutoSupport セクションで、をクリックし、[Suppress Support Case Generation]\*を選択します。
3. 抑制を実行する時間数を入力します。
4. 抑制を実行するノードを選択します。

## サポートケースの生成を再開

ONTAP 9.10.1 以降では、System Manager を使用してサポートケースが抑制されていれば AutoSupport から生成を再開できます。



### 手順

1. [\* Cluster]>[Settings] (設定) \*を選択します。
2. AutoSupport セクションで、 をクリックし、[Resume Support Case Generation]\*を選択します。
3. 生成を再開するノードを選択します。

## AutoSupport の設定を編集します

System Manager を使用して、AutoSupport アカウントの接続や E メールを設定を変更することができます。

### 手順

1. [\* Cluster]>[Settings] (設定) \*を選択します。
2. AutoSupport セクションで、 をクリックし、[その他のオプション]\*を選択します。
3. [接続]セクションまたは[電子メール]セクションで、 Edit をクリックして、いずれかのセクションの設定を変更します。

## CLI を使用して AutoSupport を管理します

### Manage AutoSupport の概要

AutoSupport は、システムヘルスをプロアクティブに監視し、ネットアップテクニカルサポート、社内のサポート部門、およびサポートパートナーにメッセージを自動的に送信します。テクニカルサポートへの AutoSupport メッセージの送信はデフォルトで有効になりますが、メッセージを社内のサポート部門に送信する場合は、適切なオプションを設定し、有効なメールホストを指定する必要があります。

AutoSupport 管理を実行できるのはクラスタ管理者だけです。Storage Virtual Machine (SVM) 管理者には AutoSupport へのアクセス権はありません。

AutoSupport は、ストレージシステムの初回設定時にデフォルトで有効になります。AutoSupport は、AutoSupport が有効になってから 24 時間後にテクニカルサポートへのメッセージ送信を開始します。この間隔を 24 時間よりも短くするには、システムをアップグレードまたはリポートするか、AutoSupport 設定を変更するか、システムの時間を 24 時間以外の時間に変更します。



AutoSupport はいつでも無効にできますが、常に有効にしておく必要があります。AutoSupport を有効にしておくと、ストレージ・システムに問題が発生したときに、迅速に原因を判断し解決できます。デフォルトでは、AutoSupport を無効にした場合でも、AutoSupport の情報が収集されてローカルに格納されます。

AutoSupport の詳細については、NetApp Support Siteを参照してください。

### 関連情報

- ["ネットアップサポート"](#)

- ["ONTAP コマンドの詳細については、AutoSupport の CLI を参照してください"](#)

## AutoSupport と Active IQ Digital Advisor を使用します

ONTAP の AutoSupport コンポーネントはテレメトリを収集し、分析用に送信します。Active IQ デジタルアドバイザーは AutoSupport からデータを分析し、プロアクティブなサポートと最適化を提供します。Active IQ は、人工知能を使用して潜在的な問題を特定し、ビジネスに影響が及ぶ前に解決を支援します。

Active IQ では、クラウドベースのポータルとモバイルアプリを通じて、実用的な予測分析とプロアクティブなサポートを提供することで、グローバルハイブリッドクラウド全体でデータインフラを最適化できます。SupportEdge との契約が締結されているネットアップのすべてのお客様は、Active IQ が提供するデータ主体の分析情報と推奨事項を利用できます（機能は製品やサポートレベルによって異なります）。

Active IQ でできることは次のとおりです。

- アップグレードを計画する。Active IQ では、ONTAP の新しいバージョンにアップグレードすることで解決可能な問題が環境内で特定されます。また、アップグレードを計画する際に役立つ Upgrade Advisor コンポーネントも用意されています。
- システムの健全性を表示します。Active IQ ダッシュボードで、健全性に関する問題が報告されるため、これらの問題の解決に役立ちます。システム容量を監視して、ストレージスペースが不足しないようにします。システムのサポートケースを表示します。
- パフォーマンスを管理Active IQ には、System Manager に表示されるよりも長時間にわたるシステムパフォーマンスが表示されます。パフォーマンスに影響を与えている構成やシステムの問題を特定します。
- 効率性の最大化Storage Efficiency 指標を表示し、より多くのデータをより少ないスペースに格納する方法を特定します。
- インベントリと構成を表示します。Active IQ は、インベントリおよびソフトウェアとハードウェアの構成に関するすべての情報を表示します。サービス契約がいつ期限切れになるかを確認し、サービス契約を更新してサポートを継続するかを確認します。

## 関連情報

["ネットアップのマニュアル：Active IQ Digital Advisor"](#)

["Active IQ を起動します"](#)

["SupportEdge サービス"](#)

## AutoSupport メッセージが送信されるタイミングおよび場所

AutoSupport は、メッセージの種類に応じた宛先にメッセージを送信します。AutoSupport がメッセージを送信するタイミングと場所を知ると、E メールで受信するメッセージまたは Active IQ（旧 My AutoSupport）Web サイトに表示されるメッセージを把握するのに役立ちます。

特に指定がないかぎり、次の表に示す設定はのパラメータです `system node autosupport modify` コマンドを実行します

## イベントトリガー型メッセージ

修正措置を必要とするシステムでイベントが発生した場合には、AutoSupport からイベントトリガー型メッセージが自動的に送信されます。

メッセージが送信されたとき	メッセージの送信先
AutoSupport は、EMS のトリガーイベントに応答します	で指定されたアドレス <code>-to</code> および <code>-noteto</code> 。（送信されるのはサービスに影響する重要なイベントのみ）。  で指定されたアドレス <code>-partner-address</code>  テクニカルサポート（該当する場合 <code>-support</code> がに設定されます <code>enable</code>

## スケジュールされたメッセージ

AutoSupport は、定期的に複数のメッセージを自動的に送信します。

メッセージが送信されたとき	メッセージの送信先
毎日（デフォルトでは、午前 12 時からチェックする必要がありますログメッセージとして送信される）	で指定されたアドレス <code>-partner-address</code>  テクニカルサポート（該当する場合 <code>-support</code> がに設定されます <code>enable</code>
毎日（デフォルトでは、午前 12 時からチェックする必要がありますパフォーマンスメッセージとして送信されます） <code>-perf</code> パラメータはに設定されます <code>true</code>	<code>partner-address</code> で指定されているアドレス  テクニカルサポート（該当する場合 <code>-support</code> がに設定されます <code>enable</code>
毎週（デフォルトでは、日曜日の午前 0 時から午前 1 時までの間に送信されます）	で指定されたアドレス <code>-partner-address</code>  テクニカルサポート（該当する場合 <code>-support</code> がに設定されます <code>enable</code>

## 手動でトリガーされるメッセージ

AutoSupport メッセージは、手動で送信または再送信できます。

メッセージが送信されたとき	メッセージの送信先
<p>を使用して、手動でメッセージを送信します <code>system node autosupport invoke</code> コマンドを実行します</p>	<p>を使用してURIを指定した場合 <code>-uri</code> のパラメータを指定します <code>system node autosupport invoke</code> コマンドを実行すると、メッセージがそのURIに送信されます。</p> <p>状況 <code>-uri</code> を省略すると、で指定したアドレスにメッセージが送信されます <code>-to</code> および <code>-partner-address</code>。このメッセージは、の場合はテクニカルサポートにも送信されます <code>-support</code> がに設定されます <code>enable</code>。</p>
<p>を使用して、手動でメッセージを送信します <code>system node autosupport invoke-core-upload</code> コマンドを実行します</p>	<p>を使用してURIを指定した場合 <code>-uri</code> のパラメータを指定します <code>system node autosupport invoke-core-upload</code> コマンドを実行すると、メッセージがそのURIに送信され、コアダンプファイルがそのURIにアップロードされます。</p> <p>状況 <code>-uri</code> では省略されています <code>system node autosupport invoke-core-upload</code> コマンドを実行すると、メッセージがテクニカルサポートに送信され、コアダンプファイルがテクニカルサポートサイトにアップロードされます。</p> <p>どちらのシナリオでもそれが必要です <code>-support</code> がに設定されます <code>enable</code> および <code>-transport</code> がに設定されます <code>https</code> または <code>http</code>。</p> <p>コアダンプファイルのサイズが大きいため、メッセージはで指定されたアドレスに送信されません <code>-to</code> および <code>-partner-addresses</code> パラメータ</p>

メッセージが送信されたとき	メッセージの送信先
<p>を使用して、手動でメッセージを送信します <code>system node autosupport invoke-performance-archive</code> コマンドを実行します</p>	<p>を使用してURIを指定した場合 <code>-uri</code> のパラメータを指定します <code>system node autosupport invoke-performance-archive</code> コマンドを実行すると、メッセージがそのURIに送信され、パフォーマンスアーカイブファイルがそのURIにアップロードされます。</p> <p>状況 <code>-uri</code> では省略されています <code>`system node autosupport invoke-performance-archive`</code> メッセージがテクニカルサポートに送信され、パフォーマンスアーカイブファイルがテクニカルサポートサイトにアップロードされます。</p> <p>どちらのシナリオでもそれが必要です <code>-support</code> がに設定されます <code>enable</code> および <code>-transport</code> がに設定されます <code>https</code> または <code>http</code>。</p> <p>パフォーマンスアーカイブファイルはサイズが大きいため、で指定したアドレスにメッセージが送信されません <code>-to</code> および <code>-partner-addresses</code> パラメータ</p>
<p>を使用して手動で過去のメッセージを再送信した <code>system node autosupport history retransmit</code> コマンドを実行します</p>	<p>で指定したURIだけに送信されます <code>-uri</code> のパラメータ <code>system node autosupport history retransmit</code> コマンドを実行します</p>

テクニカルサポートによってトリガーされるメッセージです

テクニカルサポートは、AutoSupport OnDemand 機能を使用して、AutoSupport からのメッセージを要求できます。

メッセージが送信されたとき	メッセージの送信先
<p>AutoSupport が新しい AutoSupport メッセージを生成するという送信指示を取得したとき</p>	<p>で指定されたアドレス <code>-partner-address</code></p> <p>テクニカルサポート（該当する場合 <code>-support</code> がに設定されます <code>enable</code> および <code>-transport</code> がに設定されます <code>https</code></p>
<p>過去の AutoSupport メッセージを再送信するという送信指示を AutoSupport が受け取ったとき</p>	<p>テクニカルサポート（該当する場合 <code>-support</code> がに設定されます <code>enable</code> および <code>-transport</code> がに設定されます <code>https</code></p>
<p>コアダンプファイルまたはパフォーマンスアーカイブファイルをアップロードする新しい AutoSupport メッセージを生成するという送信指示を AutoSupport が受け取ったとき</p>	<p>テクニカルサポート（該当する場合 <code>-support</code> がに設定されます <code>enable</code> および <code>-transport</code> がに設定されます <code>https</code>。テクニカルサポートサイトにコアダンプファイルまたはパフォーマンスアーカイブファイルがアップロードされます。</p>

## AutoSupport でイベントトリガー型メッセージが作成されて送信される仕組み

AutoSupport では、トリガーイベントの処理時にイベントトリガー型 AutoSupport メッセージが作成されます。イベントトリガー型 AutoSupport メッセージは、対応処置が必要な問題を受信者に通知します。問題に関連する情報だけが含まれています。含めるコンテンツと、メッセージの受信者をカスタマイズできます。

AutoSupport では、次のプロセスを使用してイベントトリガー型 AutoSupport メッセージを作成し、送信します。

1. EMS がトリガーイベントを処理すると、EMS は AutoSupport に要求を送信します。

トリガーイベントは、AutoSupport のデスティネーションとで始まる名前を含むEMSイベントです `callhome.` プレフィックス。

2. AutoSupport により、イベントトリガー型 AutoSupport メッセージが作成されます。

AutoSupport は、トリガーに関連付けられたサブシステムから基本的な情報とトラブルシューティング情報を収集し、トリガーイベントに関連する情報のみが含まれたメッセージを作成します。

各トリガーには一連のデフォルトのサブシステムが関連付けられています。ただし、を使用して、追加のサブシステムをトリガーに関連付けることもできます `system node autosupport trigger modify` コマンドを実行します

3. AutoSupport は、で定義された受信者にイベントトリガー型AutoSupport メッセージを送信します `system node autosupport modify` コマンドにを指定します `-to`、`-noteto`、`-partner` `-address`` および ``-support` パラメータ

を使用して、特定のトリガーに対するAutoSupport メッセージの配信を有効または無効にできます `system node autosupport trigger modify` コマンドにを指定します `-to` および `-noteto` パラメータ

### 特定のイベントについて送信されるデータの例

。 `storage shelf PSU failed` EMS イベントによって、必須、ログファイル、ストレージ、RAID、HA、プラットフォームサブシステム、ネットワークサブシステム、および必須サブシステム、ログファイル、およびストレージサブシステムからのトラブルシューティングデータ。

将来の対応として送信されるAutoSupport メッセージにNFSに関するデータを含めることを決定します `storage shelf PSU failed` イベント：のNFSのトラブルシューティングレベルのデータを有効にするには、次のコマンドを入力します `callhome.shlf.ps.fault` イベント：

```
cluster1::\>
system node autosupport trigger modify -node node1 -autosupport
-message shlf.ps.fault -troubleshooting-additional nfs
```

を参照してください `callhome.` プレフィックスはからドロップされます `callhome.shlf.ps.fault` を使用する場合のイベント `system node autosupport trigger` (CLIのAutoSupport イベントおよびEMSイベントで参照されている場合)。

## AutoSupport メッセージの種類とその内容

AutoSupport メッセージには、サポートされているサブシステムに関するステータス情報が含まれていAutoSupport メッセージの内容を把握しておく、Eメールで受信したメッセージまたは Active IQ（旧 My AutoSupport）Web サイトに表示されたメッセージを解釈したり、応答したりするときに役立ちます。

メッセージのタイプ	メッセージに含まれるデータのタイプ
イベントトリガー型	イベントが発生した特定のサブシステムに関するコンテキスト依存データが含まれるファイル
毎日	ログファイル
パフォーマンス	過去 24 時間以内にサンプリングされたパフォーマンスデータ
毎週	設定データおよびステータスデータ
によってトリガーされます <code>system node autosupport invoke</code> コマンドを実行します	<p>で指定した値によって異なります <code>-type</code> パラメータ：</p> <ul style="list-style-type: none"><li>• <code>test</code> いくつかの基本データを含むユーザトリガー型メッセージを送信します。</li></ul> <p>また、を使用して、テクニカルサポートからの自動応答Eメールが指定したEメールアドレス宛てに送信されます <code>-to</code> オプション。AutoSupport メッセージが受信されていることを確認できます。</p> <ul style="list-style-type: none"><li>• <code>performance</code> パフォーマンスデータを送信します。</li><li>• <code>all</code> 各サブシステムのトラブルシューティングデータを含む、週次メッセージと同様の一連のデータを含むユーザトリガー型メッセージを送信します。</li></ul> <p>通常、テクニカルサポートからはこのメッセージが要求されます。</p>
によってトリガーされます <code>system node autosupport invoke-core-upload</code> コマンドを実行します	ノードのコアダンプファイル
によってトリガーされます <code>system node autosupport invoke-performance-archive</code> コマンドを実行します	指定された期間のパフォーマンスアーカイブファイル



メッセージのタイプ	メッセージに含まれるデータのタイプ
AutoSupport OnDemand によってトリガーされます	<p>AutoSupport OnDemand では、新しいメッセージまたは過去のメッセージを要求できます。</p> <ul style="list-style-type: none"> <li>• 新しいメッセージは、AutoSupport 収集のタイプに応じてにすることができます <code>test</code>、<code>all</code> または <code>performance</code>。</li> <li>• 過去のメッセージは、再送信されるメッセージの種類によって異なります。</li> </ul> <p>AutoSupport OnDemand では、NetApp Support Site に次のファイルをアップロードする新しいメッセージを要求できます "<a href="https://mysupport.netapp.com">mysupport.netapp.com</a>" :</p> <ul style="list-style-type: none"> <li>• コアダンプ</li> <li>• パフォーマンスアーカイブ</li> </ul>

## AutoSupport サブシステムとは

各サブシステムは、AutoSupport がメッセージに使用する基本情報およびトラブルシューティング情報を提供します。各サブシステムはトリガーイベントとも関連付けられており、AutoSupport はトリガーイベントに関連する情報のみをサブシステムから収集できます。

AutoSupport は、状況に応じたコンテンツを収集します。を使用して、サブシステムおよびトリガーイベントに関する情報を表示できます `system node autosupport trigger show` コマンドを実行します

## AutoSupport のサイズ割当量と時間割当量

AutoSupport は、サブシステム別に情報を収集し、各サブシステムのコンテンツにサイズ割当量と時間割当量を適用します。ストレージシステムが拡張すると、AutoSupport の割当量によって AutoSupport のペイロードが制御され、拡張性の高い AutoSupport データの配信が可能になります。

サブシステムのコンテンツがサイズ割当量または時間割当量を超えた場合、AutoSupport は情報の収集を停止し、AutoSupport のコンテンツを切り捨てます。コンテンツを切り捨てるのが容易ではない場合（バイナリファイルなど）、AutoSupport はそのコンテンツを除外します。

デフォルトのサイズ割当量と時間割当量の変更は、ネットアップサポートから指示があった場合にのみ行うようにしてください。を使用して、サブシステムのデフォルトのサイズ割当量と時間割当量を確認することもできます `autosupport manifest show` コマンドを実行します

## イベントトリガー型 AutoSupport メッセージで送信されるファイル

イベントトリガー型 AutoSupport メッセージには、AutoSupport でメッセージが生成される原因となったイベントに関連付けられたサブシステムからの基本情報とトラブルシューティング情報のみが含まれています。特定のデータは、ネットアップサポートおよ

びサポートパートナーによる問題のトラブルシューティングに役立ちます。

AutoSupport では、イベントトリガー型 AutoSupport メッセージの内容の制御に次の基準を使用します。

- 含まれているサブシステム

データは、ログファイルなどの共通サブシステムや、RAID などの特定のサブシステムといったサブシステムにグループ化されます。各イベントは、特定のサブシステムのデータのみを含むメッセージをトリガーします。

- 含まれている各サブシステムの詳細レベル

含まれている各サブシステムのデータは、基本レベルまたはトラブルシューティングレベルで提供されます。

を使用して、考えられるすべてのイベントを表示し、各イベントに関するメッセージにどのサブシステムが含まれているかを確認できます `system node autosupport trigger show` コマンドに `-instance` パラメータ

各イベントにデフォルトで含まれるサブシステムのほかに、を使用して基本レベルまたはトラブルシューティングレベルでサブシステムを追加できます `system node autosupport trigger modify` コマンドを実行します

**AutoSupport** メッセージで送信されるログファイルです

AutoSupport メッセージには、ネットアップのテクニカルサポート担当者が最近のシステムアクティビティを確認できる、複数の主要ログファイルを含めることができます。

ログファイルサブシステムが有効になっている場合は、すべてのタイプの AutoSupport メッセージに次のログファイルが含まれる可能性があります。

ログファイル	ファイルから含まれているデータの量
<ul style="list-style-type: none"><li>• からのログファイル <code>/mroot/etc/log/mlog/</code> ディレクトリ</li><li>• MESSAGES ログファイル</li></ul>	最後の AutoSupport メッセージ以降にログに追加された、指定最大数までの新しい行のみこれにより、AutoSupport メッセージに、一意に関連性のあるデータが重複しないようになります。  (パートナーからのログファイルは例外です。パートナーについては、最大許容データが含まれます)。
<ul style="list-style-type: none"><li>• からのログファイル <code>/mroot/etc/log/shelflog/</code> ディレクトリ</li><li>• からのログファイル <code>/mroot/etc/log/acp/</code> ディレクトリ</li><li>• Event Management System (EMS ; イベント管理システム) ログデータ</li></ul>	指定された最大数までの最新のデータ行。

AutoSupport メッセージの内容は、ONTAP のリリースによって変わる場合があります。

週単位の **AutoSupport** メッセージで送信されるファイル

週単位の AutoSupport メッセージには、追加の設定およびステータスが含まれ、時間の経過に伴うシステム内の変更の追跡に役立ちます。

週単位の AutoSupport メッセージでは、次の情報が送信されます。

- 各サブシステムに関する基本情報
- 選択したの内容 /mroot/etc ディレクトリファイル
- ログファイル
- システム情報を表示するコマンドの出力
- レプリケートされたデータベース（RDB）情報、サービス統計情報などの追加情報

**AutoSupport OnDemand** がテクニカルサポートから送信指示を取得する仕組み

AutoSupport OnDemand はテクニカルサポートと定期的に通信し、AutoSupport メッセージの送信、再送信、拒否に関する配信指示を取得するとともに、NetApp Support Site に大容量ファイルをアップロードします。AutoSupport OnDemand を使用すると、週単位の AutoSupport ジョブの実行を待たずに AutoSupport メッセージをオンデマンドで送信できます。

AutoSupport OnDemand は、次のコンポーネントで構成されています。

- 各ノードで稼働する AutoSupport OnDemand クライアント
- テクニカルサポートで稼働する AutoSupport OnDemand サービス

AutoSupport OnDemand クライアントは、AutoSupport OnDemand サービスを定期的にポーリングし、テクニカルサポートから送信指示を取得します。たとえば、テクニカルサポートは、AutoSupport OnDemand サービスを使用して、新しい AutoSupport メッセージを生成するよう要求できます。AutoSupport OnDemand クライアントは、AutoSupport OnDemand サービスをポーリングして、配信指示を取得し、要求に応じて新しい AutoSupport メッセージをオンデマンドで送信します。

AutoSupport OnDemand は、デフォルトで有効になっています。ただし、AutoSupport OnDemand がテクニカルサポートとの通信を継続するかどうかは、いくつかの AutoSupport 設定によって決まります。次の要件を満たしている場合、AutoSupport OnDemand はテクニカルサポートと自動的に通信を行います。

- AutoSupport が有効になっている
- AutoSupport は、テクニカルサポートにメッセージを送信するように設定されています。
- AutoSupport は、HTTPS 転送プロトコルを使用するように設定されています。

AutoSupport OnDemand クライアントは、AutoSupport メッセージの送信先と同じ場所のテクニカルサポートに HTTPS 要求を送信します。AutoSupport OnDemand クライアントは、着信接続は受け入れません。

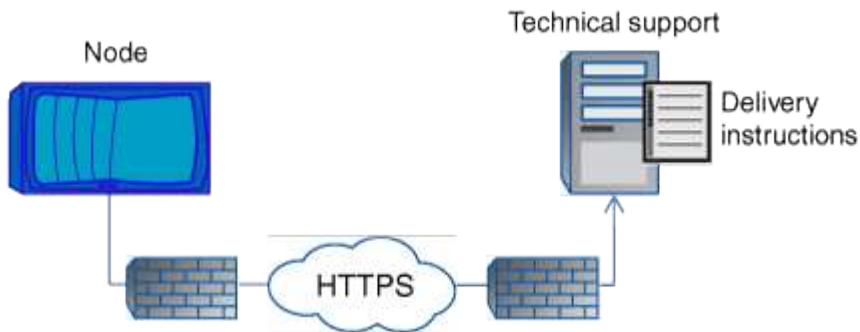


AutoSupport OnDemand は、「AutoSupport」ユーザーアカウントを使用してテクニカルサポートと通信します。ONTAP では、このアカウントを削除することはできません。

AutoSupport OnDemand を無効にし、AutoSupport は有効なままにする場合は、次のコマンドを使用しま

す。link : <https://docs.netapp.com/us-en/ontap-cli-9121/system-node-autosupport-modify.html#parameters>[system node autosupport modify -ondemand-state disable]。

次の図は、AutoSupport OnDemand がテクニカルサポートに HTTPS 要求を送信して送信指示を取得する方法を示しています。



配信指示には、AutoSupport が行う処理として、次のようなものがあります。

- 新しい AutoSupport メッセージの生成

テクニカルサポートからは、問題の優先度を選別できるように、新たな AutoSupport メッセージが要求されることが

- コアダンプファイルまたはパフォーマンスアーカイブファイルを NetApp Support Site にアップロードする新しい AutoSupport メッセージの生成

問題の優先度を選別できるように、テクニカルサポートからコアダンプファイルまたはパフォーマンスアーカイブファイルを要求されることがあります。

- 以前に生成した AutoSupport メッセージの再送信

この要求は、配信エラーが原因でメッセージが受信されなかった場合に自動的に行われます。

- 特定のトリガーイベントに対する AutoSupport メッセージ配信を無効にします。

テクニカルサポートは、使用されていないデータの配信を無効にすることがあります。

## E メールで送信される **AutoSupport** メッセージの構造

AutoSupport メッセージを E メールで送信すると、メッセージには標準的な件名、簡単な本文、およびデータが含まれた 7z ファイル形式の大きな添付ファイルが含まれます。



プライベートデータを非表示にするように AutoSupport が設定されている場合は、ヘッダー、件名、本文、添付ファイル内のホスト名などの特定の情報が省略されるか、マスクされます。

### 件名

AutoSupport メカニズムによって送信されたメッセージの件名行には、通知の理由を特定するテキスト文字列が含まれています。件名行の形式は次のとおりです。

HA グループ通知の送信元 \_ システム \_ 名前 \_ ( \_ メッセージ \_ ) \_ 重大度 \_

- *System\_Name* は、AutoSupport の設定に応じてホスト名またはシステム ID です

ボディ ( **Body** )

AutoSupport メッセージの本文には、次の情報が含まれます。

- メッセージの日付とタイムスタンプ
- メッセージを生成したノード上の ONTAP のバージョン
- メッセージを生成したノードのシステム ID、シリアル番号、およびホスト名
- AutoSupport シーケンス番号
- SNMP の連絡先名と場所 (指定されている場合)
- HA パートナーノードのシステム ID とホスト名

添付ファイル

AutoSupport メッセージの重要な情報は、という名前の 7z ファイルに圧縮されたファイルに含まれています  
`body.7z` メッセージに添付されています。

添付ファイルに含まれるファイルは、AutoSupport メッセージのタイプに固有です。

### AutoSupport の重大度のタイプ

AutoSupport メッセージには、各メッセージの目的を示す重大度のタイプが設定されます。たとえば、緊急の問題にすぐに対処する場合や、情報提供のみを目的とした場合などです。

メッセージには次のいずれかの重大度が設定されます。

- \* 警告 \* : アラートメッセージは、何らかの処置を行わないと、より高いレベルのイベントが発生する可能性があることを示します。

アラートメッセージに対しては、24 時間以内に対処を行う必要があります。

- \* 緊急 \* : システム停止が発生すると、緊急メッセージが表示されます。

緊急メッセージに対しては、すぐに対処する必要があります。

- \* エラー \* : エラー状態は、無視した場合に発生する可能性がある問題を示します。
- \* 通知 \* : 通常の状態だが重要な状態。
- \* 情報 \* : 情報メッセージは、問題に関する詳細情報を提供しますが、これは無視してかまいません。
- \* デバッグ \* : デバッグレベルのメッセージには、実行する必要がある手順が記載されています。

社内のサポート部門が AutoSupport メッセージを E メールで受信する場合、重大度は E メールメッセージの件名に表示されます。

**AutoSupport** を使用するための要件

セキュリティを最適化し、AutoSupportの最新の機能をすべてサポートするには、AutoSupportメッセージの配信にHTTPSとTLSv1.2またはセキュアSMTPを使用する必要があります。他のプロトコルで配信されたAutoSupportメッセージは拒否されます。

サポートされているプロトコル

これらのプロトコルはいずれも、名前が解決されるアドレスファミリーに応じて IPv4 または IPv6 で実行されます。

プロトコルとポート	説明
ポート 443 で HTTPS を使用します	<p>これがデフォルトのプロトコルです。できるだけこのプロトコルを使用することを推奨します。</p> <p>このプロトコルでは、AutoSupport OnDemand と大容量ファイルのアップロードがサポートされます。</p> <p>検証を無効にしないかぎり、リモートサーバからの証明書がルート証明書に照らして検証されます。</p> <p>配信にはHTTPS PUT要求が使用されます。PUT では、要求の転送中にエラーが発生した場合に、停止した場所から要求が再開されます。要求を受信したサーバがPUTをサポートしていない場合は、HTTPS POST要求が使用されます。</p>
ポート 80 の HTTP	<p>このプロトコルは SMTP よりも推奨されます。</p> <p>このプロトコルでは、大容量ファイルのアップロードがサポートされますが、AutoSupport OnDemand はサポートされません。</p> <p>配信にはHTTPS PUT要求が使用されます。PUT では、要求の転送中にエラーが発生した場合に、停止した場所から要求が再開されます。要求を受信したサーバがPUTをサポートしていない場合は、HTTPS POST要求が使用されます。</p>

プロトコルとポート	説明
SMTP : ポート 25 または別のポート	<p>このプロトコルは、ネットワーク接続でHTTPSが許可されていない場合にのみ使用してください。</p> <p>デフォルトのポート値は 25 ですが、別のポートを使用するように AutoSupport を設定できます。</p> <p>SMTP を使用する場合は、次の制限事項に注意してください。</p> <ul style="list-style-type: none"> <li>• AutoSupport OnDemand と大容量ファイルのアップロードはサポートされません。</li> <li>• データは暗号化されません。</li> </ul> <p>SMTP ではデータがクリアテキストで送信されるため、AutoSupport メッセージ内のテキストの傍受や読み取りが容易になります。</p> <ul style="list-style-type: none"> <li>• メッセージの長さや行の長さの制限が生じることがあります。</li> </ul>

AutoSupport に社内のサポート部門またはサポートパートナーの E メールアドレスを指定した場合、それらのメッセージは常に SMTP で送信されます。

たとえば、推奨されるプロトコルを使用してテクニカルサポートにメッセージを送信し、同時に社内のサポート部門にもメッセージを送信する場合は、それぞれ HTTPS と SMTP を使用して転送されます。

AutoSupport では、プロトコルごとに最大ファイルサイズが制限されます。HTTP および HTTPS 転送のデフォルト設定は 25MB です。SMTP 転送のデフォルト設定は 5MB です。AutoSupport メッセージのサイズが設定された上限を超えると、AutoSupport はできるだけ多くのメッセージを配信します。最大サイズは、AutoSupport の設定を変更することで編集できます。を参照してください `system node autosupport modify` のマニュアルページを参照してください。



コアダンプファイルやパフォーマンスアーカイブファイルを NetApp Support Site や指定の URI にアップロードする AutoSupport メッセージを生成して送信すると、HTTPS プロトコルと HTTP プロトコルの最大ファイルサイズの上限は自動的に無視されます。自動オーバーライドは、を使用してファイルをアップロードする場合にのみ適用されます `system node autosupport invoke-core-upload` または `system node autosupport invoke-performance-archive` コマンド

#### 設定要件

ネットワーク構成によっては、HTTPS プロトコルでプロキシ URL の追加設定が必要になる場合があります。テクニカルサポートへの AutoSupport メッセージの送信に HTTPS を使用し、プロキシを使用している場合は、そのプロキシの URL を指定する必要があります。プロキシがデフォルトのポート（3128）以外のポートを使用する場合は、そのプロキシのポートを指定できます。プロキシ認証のユーザ名とパスワードを指定することもできます。

SMTP を使用して社内のサポート部門やテクニカルサポートに AutoSupport メッセージを送信する場合は、外部のメールサーバを設定する必要があります。ストレージシステムはメールサーバとしては機能しないた



め、メール送信用に外部のメールサーバが別途必要になります。このメールサーバを SMTP ポート（25）または別のポートを監視するホストにして、8ビットの Multipurpose Internet Mail Extensions（MIME）エンコーディングを送受信するように設定する必要があります。メール・ホストの例としては 'sendmail プログラムなどの SMTP サーバを実行する UNIX ホストと 'Microsoft Exchange サーバを実行する Windows サーバがありますメールホストは1つでも複数でもかまいません。

## AutoSupport をセットアップする

テクニカルサポートまたは社内のサポート部門に AutoSupport 情報を送信するかどうかおよびその方法を管理し、その設定が正しいことをテストできます。

このタスクについて

ONTAP 9.5 以降のリリースでは、クラスタのすべてのノードで AutoSupport を有効にし、その設定を同時に変更できます。新しいノードがクラスタに追加されると、そのノードは AutoSupport クラスタ設定を自動的に継承します。各ノードの設定を個別に更新する必要はありません。



ONTAP 9.5以降では、の対象となります `system node autosupport modify` コマンドはクラスタ全体に適用されます。AutoSupport 設定がクラスタ内のすべてのノードで変更されます。これには、が含まれます `-node` オプションが指定されています。このオプションは無視されますが、CLI の下位互換性を維持するために保持されています。

ONTAP 9.4以前のリリースでは、の対象となります `system node autosupport modify` コマンドはノードに固有です。クラスタ内の各ノードで AutoSupport 設定を変更する必要があります。

デフォルトでは、各ノードで AutoSupport が有効になっており、HTTPS 転送プロトコルを使用してテクニカルサポートにメッセージを送信できます。

セキュリティを最適化し、AutoSupportの最新の機能をすべてサポートするには、AutoSupportメッセージの配信にHTTPSとTLSv1.2またはセキュアSMTPを使用する必要があります。

手順

1. AutoSupport が有効になっていることを確認します。

```
system node autosupport modify -state enable
```

2. テクニカルサポートに AutoSupport メッセージを送信するには、次のコマンドを使用します。

```
system node autosupport modify -support enable
```

AutoSupport を AutoSupport OnDemand と連携できるようにする場合、またはコアダンプファイルやパフォーマンスアーカイブファイルなどの大容量ファイルをテクニカルサポートまたは指定の URL にアップロードする場合は、このオプションを有効にする必要があります。

3. テクニカルサポートが AutoSupport メッセージを受信できるようになっている場合は、メッセージに使用する転送プロトコルを指定します。

次のオプションから選択できます。



状況	次に、の次のパラメータを設定します <code>system node autosupport modify</code> コマンド...
デフォルトの HTTPS プロトコルを使用します	a. 設定 <code>-transport</code> 終了: <code>https</code> 。 b. プロキシを使用する場合は、を設定します <code>-proxy-url</code> にプロキシのURLを入力します。 この設定では、AutoSupport OnDemand との通信および大容量ファイルのアップロードがサポートされます。
SMTP を使用する	設定 <code>-transport</code> 終了: <code>smtp</code> 。  この設定では、AutoSupport OnDemand や大容量ファイルのアップロードはサポートされません。

4. 社内のサポート部門またはサポートパートナーに AutoSupport メッセージを送信するには、次の操作を実行します。

- a. 組織内の受信者を特定するには、の次のパラメータを設定します `system node autosupport modify` コマンドを実行します

設定するパラメータ	パラメータの値
<code>-to</code>	重要な AutoSupport メッセージを受け取る社内サポート部門の、カンマで区切った 5 つまでの個別 E メールアドレスまたは配信リスト
<code>-noteto</code>	重要な AutoSupport メッセージの携帯電話やその他のモバイルデバイス用の短縮版を受け取る社内サポート部門の、カンマで区切った 5 つまでの個別 E メールアドレスまたは配信リスト
<code>-partner-address</code>	すべての AutoSupport メッセージを受け取るサポートパートナー部門の、カンマで区切った 5 つまでの個別 E メールアドレスまたは配信リスト

- b. を使用して送信先をリストし、アドレスが正しく設定されていることを確認します `system node autosupport destinations show` コマンドを実行します

5. メッセージを社内のサポート部門に送信するか、テクニカルサポートへのメッセージにSMTP転送を選択した場合は、の次のパラメータを設定してSMTPを設定します `system node autosupport modify` コマンドを実行します

- 設定 `-mail-hosts` をカンマで区切って1つ以上のメールホストに転送します。

最大 5 つのを設定できます。

メールホスト名のあとにコロンとポート番号を指定することで、各メールホストのポート値を設定できます。次に例を示します。`mymailhost.example.com:5678`では、5678はメールホストのポートです。

- 設定 `-from` AutoSupport メッセージを送信するEメールアドレスに送信します。

6. DNS を設定します。

7. 特定の設定を変更する場合は、必要に応じてコマンドオプションを追加します。

実行する処理	次に、の次のパラメータを設定します <code>system node autosupport modify</code> コマンド...
メッセージ内の機密データを削除、マスキング、またはエンコードすることによって、プライベートデータを非表示にします	設定 <code>-remove-private-data</code> 終了: <code>true</code> 。から変更した場合 <code>false</code> 終了: <code>'true'</code> をクリックすると、すべてのAutoSupport 履歴とすべての関連ファイルが削除されます。
定期的な AutoSupport メッセージでのパフォーマンスデータの送信を停止します	設定 <code>-perf</code> 終了: <code>false</code> 。

8. を使用して設定全体を確認します `system node autosupport show` コマンドにを指定します `-node` パラメータ

9. を使用してAutoSupport の動作を確認します `system node autosupport check show` コマンドを実行します

問題が報告された場合は、を使用してください `system node autosupport check show-details` コマンドを使用して詳細情報を表示します。

10. AutoSupport メッセージが送受信されていることをテストします。

- を使用します `system node autosupport invoke` コマンドにを指定します `-type` パラメータをに設定します `test`。

```
cluster1::> system node autosupport invoke -type test -node node1
```

- ネットアップが AutoSupport メッセージを受信していることを確認します。

`system node AutoSupport history show -node local` コマンドを実行します

最新の発信AutoSupport メッセージのステータスは、最終的にに変わります `sent-successful` すべての適切なプロトコルの宛先に対して。

- 必要に応じて、AutoSupportメッセージが社内のサポート部門またはサポートパートナーに送信されていることを確認します。そのためには、用に設定したアドレスのEメールを確認します `-to`、`-noteto` または `-partner-address` のパラメータ `system node autosupport modify` コマンドを実行します

コアダンプファイルをアップロードする

コアダンプファイルが保存されると、イベントメッセージが生成されます。AutoSupport サービスが有効であり、ネットアップサポートにメッセージを送信するように設定されている場合は、AutoSupport メッセージが送信され、自動応答メールが返信されます。

## 必要なもの

- 次の設定を使用して AutoSupport をセットアップしておく必要があります。
  - ノードで AutoSupport が有効になっている。
  - AutoSupport は、テクニカルサポートにメッセージを送信するように設定されています。
  - HTTP または HTTPS 転送プロトコルを使用するように AutoSupport が設定されている。

コアダンプファイルなどの大容量ファイルを含むメッセージを送信する場合、SMTP 転送プロトコルはサポートされません。

## このタスクについて

を使用して、HTTPS経由のAutoSupport サービスを通じてコアダンプファイルをアップロードすることもできます `system node autosupport invoke-core-upload` コマンド（ネットアップサポートから要求された場合）。

## "ネットアップにファイルをアップロードする方法"

### 手順

1. を使用して、ノードのコアダンプファイルを表示します `system node coredump show` コマンドを実行します

次の例では、ローカルノードのコアダンプファイルが表示されます。

```
cluster1::> system node coredump show -node local
Node:Type Core Name Saved Panic Time
-----
node:kernel
core.4073000068.2013-09-11.15_05_01.nz true 9/11/2013 15:05:01
```

2. を使用して、AutoSupport メッセージを生成し、コアダンプファイルをアップロードします `system node autosupport invoke-core-upload` コマンドを実行します

次の例では、AutoSupport メッセージが生成されてデフォルトの場所（テクニカルサポート）に送信されます。コアダンプファイルは、NetApp Support Siteであるデフォルトの場所にアップロードされます。

```
cluster1::> system node autosupport invoke-core-upload -core-filename
core.4073000068.2013-09-11.15_05_01.nz -node local
```

次の例では、AutoSupport メッセージが生成され、URI に指定した場所に送信されます。コアダンプファイルはその URI にアップロードされます。

```
cluster1::> system node autosupport invoke-core-upload -uri
https://files.company.com -core-filename
core.4073000068.2013-09-11.15_05_01.nz -node local
```

パフォーマンスアーカイブファイルをアップロードします

パフォーマンスアーカイブを含む AutoSupport メッセージを生成して送信できます。デフォルトでは、AutoSupport メッセージはネットアップテクニカルサポートに送信され、パフォーマンスアーカイブはNetApp Support Siteにアップロードされます。メッセージの送信先とアップロード先には別の場所を指定できます。

必要なもの

- 次の設定を使用して AutoSupport をセットアップしておく必要があります。
  - ノードで AutoSupport が有効になっている。
  - AutoSupport は、テクニカルサポートにメッセージを送信するように設定されています。
  - HTTP または HTTPS 転送プロトコルを使用するように AutoSupport が設定されている。

パフォーマンスアーカイブファイルなどの大容量ファイルを含むメッセージの送信では、SMTP 転送プロトコルはサポートされません。

このタスクについて

アップロードするパフォーマンスアーカイブデータの開始日を指定する必要があります。ほとんどのストレージシステムでは、パフォーマンスアーカイブが 2 週間保存されるため、2 週間前までの開始日を指定できます。たとえば、今日が 1 月 15 日の場合は、1 月 2 日の開始日を指定できます。

ステップ

1. を使用して、AutoSupport メッセージを生成し、パフォーマンスアーカイブファイルをアップロードします system node autosupport invoke-performance-archive コマンドを実行します

次の例では、2015 年 1 月 12 日から 4 時間分のパフォーマンスアーカイブファイルが AutoSupport メッセージに追加され、NetApp Support Siteのデフォルトの場所にアップロードされます。

```
cluster1::> system node autosupport invoke-performance-archive -node
local -start-date 1/12/2015 13:42:09 -duration 4h
```

次の例では、2015 年 1 月 12 日から 4 時間分のパフォーマンスアーカイブファイルが AutoSupport メッセージに追加され、URI で指定した場所にアップロードされます。

```
cluster1::> system node autosupport invoke-performance-archive -node
local -start-date 1/12/2015 13:42:09 -duration 4h -uri
https://files.company.com
```

## AutoSupport メッセージの説明を取得する

受信したAutoSupport メッセージの説明は、ONTAP のSyslog Translatorを使用して参照できます。

### 手順

1. にアクセスします ["Syslog Translator"](#)。
2. [リリース]フィールドに、使用しているONTAP のバージョンを入力します。検索文字列フィールドに「callhome」と入力します。[\*平行移動 (Translate) ]を選択し
3. Syslog Translatorには、入力したメッセージ文字列に一致するすべてのイベントがアルファベット順に表示されます。

## AutoSupport を管理するためのコマンド

を使用します `system node autosupport` AutoSupport の設定を変更または表示したり、以前のAutoSupport メッセージに関する情報を表示したり、AutoSupport メッセージを送信、再送信、またはキャンセルしたりするコマンド。

### AutoSupport を設定します

状況	使用するコマンド
AutoSupport メッセージを送信するかどうかを制御します	<code>system node autosupport modify</code> を使用 <code>-state</code> パラメータ
AutoSupport メッセージをテクニカルサポートに送信するかどうかを制御します	<code>system node autosupport modify</code> を使用 <code>-support</code> パラメータ
AutoSupport をセットアップするか、AutoSupport の設定を変更します	<code>system node autosupport modify</code>
個々のトリガーイベントについて、AutoSupport メッセージを社内のサポート部門に送信するかどうかを指定する。また、各トリガーイベントで送信されるメッセージに含める追加のサブシステムレポートを指定する	<code>system node autosupport trigger modify</code>

### AutoSupport の設定に関する情報を表示します


状況	使用するコマンド
AutoSupport の設定を表示します	<code>system node autosupport show</code> を使用 <code>-node</code> パラメータ
AutoSupport メッセージを受信するすべてのアドレスと URL の概要を表示します	<code>system node autosupport destinations</code> <code>show</code>


状況	使用するコマンド
個々のトリガーイベントについて社内のサポート部門に送信される AutoSupport メッセージを表示します	<code>system node autosupport trigger show</code>
AutoSupport の設定およびさまざまな宛先への配信のステータスを表示します	<code>system node autosupport check show</code>
AutoSupport の設定およびさまざまな宛先への配信の詳細なステータスを表示します	<code>system node autosupport check show-details</code>

過去の **AutoSupport** メッセージに関する情報を表示する

状況	使用するコマンド
1 つ以上の最新の 50 件の AutoSupport メッセージに関する情報を表示する	<code>system node autosupport history show</code>
テクニカルサポートサイトまたは指定の URI にコアダンプファイルまたはパフォーマンスアーカイブファイルをアップロードするために生成された最新の AutoSupport メッセージに関する情報を表示します	<code>system node autosupport history show-upload-details</code>
AutoSupport メッセージ内の情報を表示します。メッセージ用に収集された各ファイルの名前とサイズのほか、エラーがある場合はその情報も表示されます	<code>system node autosupport manifest show</code>

**AutoSupport** メッセージを送信、再送信、またはキャンセルします

状況	使用するコマンド
<p>ローカルに保存されている AutoSupport メッセージを、AutoSupport シーケンス番号で識別して再転送します</p> <div>  <p>AutoSupport メッセージを再送信し、サポート部門がすでにそのメッセージを受信している場合、サポートシステムは重複するケースを作成しません。一方、サポート部門がそのメッセージを受信しなかった場合、AutoSupport システムはメッセージを分析し、必要に応じてケースを作成します。</p> </div>	<code>system node autosupport history retransmit</code>

状況	使用するコマンド
テストなどの目的で、AutoSupport メッセージを生成して送信します	<pre>system node autosupport invoke</pre> <div>  <p>を使用します <code>-force</code> AutoSupport が無効な場合でもメッセージを送信するためのパラメータ。を使用します <code>-uri</code> 設定されている宛先ではなく、指定した宛先にメッセージを送信するためのパラメータ。</p> </div>
AutoSupport メッセージをキャンセルします	<pre>system node autosupport history cancel</pre>

## 関連情報

["ONTAP 9コマンド"](#)

## AutoSupport マニフェストに含まれる情報

AutoSupport マニフェストでは、各 AutoSupport メッセージについて収集されるファイルの詳細が表示されます。AutoSupport マニフェストには、AutoSupport が必要なファイルを収集できない場合の収集エラーに関する情報も含まれています。

AutoSupport マニフェストには次の情報が含まれています。

- AutoSupport メッセージのシーケンス番号
- AutoSupport メッセージに含まれている AutoSupport ファイル
- 各ファイルのサイズ（バイト単位）
- AutoSupport マニフェストによる収集のステータス
- 概要が 1 つ以上のファイルの収集に失敗した場合は、エラー AutoSupport

を使用して AutoSupport マニフェストを表示できます `system node autosupport manifest show` コマンドを実行します

AutoSupport マニフェストは、すべての Active IQ メッセージに含まれ、XML 形式で表示されます。つまり、一般的な XML ビューアを使用してメッセージを読んだり、AutoSupport（旧 My AutoSupport）ポータルを使用して表示したりできます。

## スケジュールされたメンテナンス時間中の **AutoSupport** ケースの抑制

AutoSupport ケースの抑制を使用すると、スケジュールされたメンテナンス時間中にトリガーされる AutoSupport メッセージによって不要なケースが作成されるのを阻止できます。

AutoSupport ケースを抑制するには、特別な形式のテキスト文字列を使用して AutoSupport メッセージを手動で呼び出す必要があります。 `MAINT=xh`。 `x` には、メンテナンス時間の長さを時間単位で指定します。

## 関連情報

## "スケジュールされたメンテナンス時間中にケースの自動作成を停止する方法"

メッセージを受信しない場合は、**AutoSupport** のトラブルシューティングを行います

システムから AutoSupport メッセージが送信されない場合は、AutoSupport がメッセージを生成できないためであるか、配信できないためであるかを判別できます。

### 手順

1. を使用して、メッセージの配信ステータスを確認します `system node autosupport history show` コマンドを実行します
2. ステータスを読みます。

このステータスです	はい
初期化中です	収集プロセスが開始しています。この状態が一時的なものであれば問題はありません。ただし、この状態が解消されない場合は、問題が存在します。
コレクション - 失敗しました	AutoSupport は、スプールディレクトリに AutoSupport コンテンツを作成できません。AutoSupport が収集しようとしている内容を表示するには、を入力します <code>system node autosupport history show -detail</code> コマンドを実行します
収集を実行中です	AutoSupport は AutoSupport コンテンツを収集しています。AutoSupport が収集している情報を表示するには、を入力します <code>system node autosupport manifest show</code> コマンドを実行します
キューに登録され	AutoSupport メッセージは配信のためにキューに登録されますが、まだ配信されていません。
送信中です	AutoSupport は現在メッセージを配信しています。
Sent - 成功しました	AutoSupport がメッセージを正常に配信しました。AutoSupport がメッセージを配信した場所を確認するには、を入力します <code>system node autosupport history show -delivery</code> コマンドを実行します
無視します	AutoSupport にメッセージの送信先がありません。配信の詳細を表示するには、を入力します <code>system node autosupport history show -delivery</code> コマンドを実行します
再キューイングされました	AutoSupport はメッセージの配信を試みましたが、失敗しました。その結果、AutoSupport は別の試行のためにメッセージを配信キューに戻しました。エラーを表示するには、を入力します <code>system node autosupport history show</code> コマンドを実行します
トランсмисシヨン - 不合格	AutoSupport は、指定された回数メッセージの配信に失敗し、メッセージ配信の試行を停止しました。エラーを表示するには、を入力します <code>system node autosupport history show</code> コマンドを実行します



このステータスです	はい
OnDemand - 無視されます	AutoSupport メッセージは正常に処理されましたが、 AutoSupport OnDemand サービスによって無視されました。

3. 次のいずれかを実行します。

をクリックします	手順
initializing または collection-failed	AutoSupport でメッセージを生成できないため、ネットアップサポートにお問い合わせください。次のナレッジベース記事に言及してください。  "AutoSupport の配信に失敗しました：ステータスが「初期化中にエラーが発生しました"
ignore、re-queued、または transmission failed のいずれかです	AutoSupport はメッセージを配信できないため、SMTP、HTTP、または HTTPS のデスティネーションが正しく設定されていることを確認します。

## HTTP または HTTPS を使用した AutoSupport メッセージ配信のトラブルシューティング

HTTP または HTTPS を使用していて、想定される AutoSupport メッセージが送信されない場合や自動更新機能が動作しない場合は、いくつかの設定を確認することで問題を解決できます。

必要なもの

基本的なネットワーク接続と DNS ルックアップについて、以下の点を確認しておきます。

- ノード管理 LIF の動作ステータスおよび管理ステータスが up になっている。
- 同じサブネット上の機能しているホストに、（ノード上の LIF ではなく）クラスタ管理 LIF から ping を実行できる。
- サブネットの外部の機能しているホストに、クラスタ管理 LIF から ping を実行できる。
- サブネットの外部の機能しているホストに、（IP アドレスではなく）ホストの名前を使用してクラスタ管理 LIF から ping を実行できる。

このタスクについて

以下の手順は、AutoSupport でメッセージを生成できているが、HTTP または HTTPS 経由でメッセージを配信できていないと判断した場合に実行します。

エラーが発生したり、この手順の手順を完了できない場合は、問題を特定し、対処してから次の手順に進んでください。

手順

1. AutoSupport サブシステムの詳細なステータスを表示します。

```
system node autosupport check show-details
```

たとえば、テストメッセージを送信して AutoSupport デスティネーションへの接続を検証したり、AutoSupport の設定で発生する可能性のあるエラーのリストを指定したりします。

2. ノード管理 LIF のステータスを確認します。

```
network interface show -home-node local -role node-mgmt -fields  
vserver,lif,status-oper,status-admin,address,role
```

。 status-oper および status-admin フィールドは「up」を返す必要があります。

3. あとで使用できるように、SVM 名、LIF 名、および LIF の IP アドレスを書き留めておきます。

4. DNS が有効になっていて正しく設定されていることを確認します

```
vserver services name-service dns show
```

5. AutoSupport メッセージからエラーが返された場合は、対処します。

```
system node autosupport history show -node * -fields node,seq-  
num,destination,last-update,status,error
```

返されたエラーのトラブルシューティングについては、を参照してください ["ONTAP AutoSupport \(Transport HTTPSおよびHTTP\) 解決ガイド"](#)。

6. クラスタが必要なサーバとインターネットの両方に正常にアクセスできることを確認します。

a. `network traceroute -lif node-management_LIF -destination DNS server`

b. `network traceroute -lif node_management_LIF -destination support.netapp.com`



住所 support.netapp.com それ自体はpingやtracerouteに応答しませんが、ホップ単位の情報は重要です。

c. `system node autosupport show -fields proxy-url`

d. `network traceroute -node node_management_LIF -destination proxy_url`

これらのルートのいずれかが機能していない場合は、ほとんどのサードパーティ製ネットワーククライアントで検出された「traceroute」または「tracert」ユーティリティを使用して、クラスタと同じサブネット上の機能しているホストから同じルートを試してください。これにより、問題がネットワーク構成とクラスタ構成のどちらに含まれているかを判断できます。

7. AutoSupport 転送プロトコルに HTTPS を使用する場合は、HTTPS トラフィックがネットワークから送信可能であることを確認します。

a. クラスタ管理 LIF と同じサブネットに Web クライアントを設定します。

プロキシサーバ、ユーザ名、パスワード、ポートを含む、すべての設定パラメータの値が AutoSupport の設定と同じであることを確認します。

b. にアクセスします `https://support.netapp.com` Webクライアントを使用します。

アクセスが成功します。成功しない場合は、HTTPS トラフィックと DNS トラフィックを許可するようにすべてのファイアウォールが設定されていること、およびプロキシサーバが正しく設定されてい

ることを確認します。support.netapp.comの静的な名前解決の設定の詳細については、サポート技術情報の記事を参照してください ["ONTAP for support.netapp.com? でホストエントリを追加する方法を説明します"](#)

8. ONTAP 9.10.1 以降では、自動更新機能を有効にした場合、次の URL への HTTPS 接続が確立されていることを確認してください。

- <https://support-sg-emea.netapp.com>
- <https://support-sg-naeast.netapp.com>
- <https://support-sg-nawest.netapp.com>

## SMTP を使用した AutoSupport メッセージ配信のトラブルシューティング

システムが SMTP 経由で AutoSupport メッセージを配信できない場合は、いくつかの設定を確認することで問題を解決できます。

### 必要なもの

基本的なネットワーク接続と DNS ルックアップについて、以下の点を確認しておきます。

- ノード管理 LIF の動作ステータスおよび管理ステータスが up になっている。
- 同じサブネット上の機能しているホストに、（ノード上の LIF ではなく）クラスタ管理 LIF から ping を実行できる。
- サブネットの外部の機能しているホストに、クラスタ管理 LIF から ping を実行できる。
- サブネットの外部の機能しているホストに、（IP アドレスではなく）ホストの名前を使用してクラスタ管理 LIF から ping を実行できる。

### このタスクについて

以下の手順は、AutoSupport でメッセージを生成できているが、SMTP 経由でメッセージを配信できていないと判断した場合に実行します。

エラーが発生したり、この手順の手順を完了できない場合は、問題を特定し、対処してから次の手順に進んでください。

特に指定がないかぎり、すべてのコマンドを ONTAP の CLI に入力します。

### 手順

1. ノード管理 LIF のステータスを確認します。

```
network interface show -home-node local -role node-mgmt -fields  
vservers,lif,status-oper,status-admin,address,role
```

- status-oper および status-admin フィールドが返される必要があります up。

2. あとで使用できるように、SVM 名、LIF 名、および LIF の IP アドレスを書き留めておきます。

3. DNS が有効になっていて正しく設定されていることを確認します

```
vservers services name-service dns show
```

4. AutoSupport で使用するように設定されているすべてのサーバを表示します。

```
system node autosupport show -fields mail-hosts
```

表示されたすべてのサーバ名を記録します。

5. 前の手順で表示された各サーバについて、およびを参照してください `support.netapp.com` ノードからサーバまたはURLにアクセスできることを確認します。

```
network traceroute -node local -destination server_name
```

これらのルートのいずれかが機能していない場合は、ほとんどのサードパーティ製ネットワーククライアントで検出された「traceroute」または「tracert」ユーティリティを使用して、クラスタと同じサブネット上の機能しているホストから同じルートを試してください。これにより、問題がネットワーク構成とクラスタ構成のどちらに含まれているかを判断できます。

6. メールホストとして指定したホストにログインし、このホストが SMTP 要求を処理できることを確認します。

```
netstat -aAn|grep 25
```

25 は、リスナーのSMTPポート番号です。

次のようなメッセージが表示されます。

```
ff64878c tcp          0          0 *.25      *.*      LISTEN.
```

7. 他のホストで、メールホストの SMTP ポートを使用した Telnet セッションを開始します。

```
telnet mailhost 25
```

次のようなメッセージが表示されます。

```
220 filer.yourco.com Sendmail 4.1/SMI-4.1 ready at Thu, 30 Nov 2014
10:49:04 PST
```

8. Telnet のプロンプトで、メールホストからメッセージをリレーできることを確認します。

```
HELO domain_name
```

```
MAIL FROM: your_email_address
```

```
RCPT TO: autosupport@netapp.com
```

domain\_name は、ネットワークのドメイン名です。

リレーが拒否されたというエラーが返された場合は、メールホストでリレーが有効になっていません。システム管理者に問い合わせてください。

9. Telnet のプロンプトで、テストメッセージを送信します。

DATA

SUBJECT: TESTING  
THIS IS A TEST

.



行の最後のピリオド (.) を単独で入力してください。このピリオドは、メッセージが完了したことをメールホストに示します。

エラーが返された場合は、メールホストが正しく設定されていません。システム管理者に問い合わせてください。

10. ONTAP のコマンドラインインターフェイスから、アクセス可能な信頼できる E メールアドレスに AutoSupport テストメッセージを送信します。

```
system node autosupport invoke -node local -type test
```

11. テストのシーケンス番号を確認します。

```
system node autosupport history show -node local -destination smtp
```

タイムスタンプに基づいて、シーケンス番号を探します。おそらく、最新の試みです。

12. テストメッセージに関するエラーを表示します。

```
system node autosupport history show -node local -seq-num seq_num -fields error
```

表示されたエラーは、です Login denied、SMTPサーバがクラスタ管理LIFからの送信要求を受け入れていません。転送プロトコルを HTTPS に変更しない場合は、サイトのネットワーク管理者に連絡して、この問題に対応するように SMTP ゲートウェイを設定してください。

このテストが成功しても mailto : [autosupport@netapp.com](mailto:autosupport@netapp.com) に同じメッセージが送信されない場合は、すべての SMTP メールホストで SMTP リレーが有効になっていることを確認するか、転送プロトコルとして HTTPS を使用してください。

ローカルで管理されている E メールアカウントへのメッセージの送信も失敗する場合は、次の両方の条件に該当する添付ファイルを転送するように SMTP サーバが設定されていることを確認してください。

- サフィックスが「7z」
- MIME タイプが「application/x-7x-compressed」。

#### AutoSupport サブシステムのトラブルシューティングを行います

。system node check show コマンドを使用すると、AutoSupport の設定と配信に関連する問題の検証とトラブルシューティングを行うことができます。

#### ステップ

1. 次のコマンドを使用して、AutoSupport サブシステムのステータスを表示します。

使用するコマンド	作業
<b>system node autosupport check show</b>	AutoSupport HTTP または HTTPS デスティネーション、AutoSupport SMTP デスティネーション、AutoSupport OnDemand サーバ、AutoSupport 設定など、AutoSupport サブシステムの全体的なステータスを表示します
<b>system node autosupport check show-details</b>	エラーの詳細な説明や対処方法など、AutoSupport サブシステムの詳細なステータスを表示する

## 健全性の監視

### システムの健全性の概要を監視

ヘルスマニタは、クラスタ内の特定のクリティカルな状態をプロアクティブに監視し、障害やリスクが検出された場合にアラートを生成します。アクティブなアラートがある場合、クラスタのヘルスステータスはデグレードと報告されます。アラートには、デグレードしたシステムヘルスへの対応に必要な情報が含まれています。

ステータスがデグレードになっている場合は、考えられる原因や推奨されるリカバリアクションなど、問題の詳細を表示できます。問題を解決すると、システムヘルスステータスは自動的に OK に戻ります。

システムヘルスステータスには、複数の異なるヘルスマニタの結果が反映されます。1つのヘルスマニタのステータスがデグレードになると、システムヘルス全体のステータスがデグレードになります。

クラスタ内のシステムヘルスの監視におけるクラスタスイッチのサポート状況 ONTAP については、Hardware Universe を参照してください。

#### "Hardware Universe でサポートされるスイッチ"

Cluster Switch Health Monitor (CSHM) AutoSupport メッセージの原因とアラートの解決方法に関する詳細については、技術情報アーティクルを参照してください。

#### "AutoSupport メッセージ：ヘルスマニタプロセス CSHM"

### ヘルスマニタの仕組み

個々のヘルスマニタには、特定の条件に該当する場合にアラートをトリガーする一連のポリシーがあります。ヘルスマニタの仕組みを理解しておく、問題に対応し、将来のアラートを制御するのに役立ちます。

ヘルスマニタは、次のコンポーネントで構成されています。

- 特定のサブシステム用のヘルスマニタ。各ヘルスマニタには独自のヘルスステータスがあります

たとえば、ストレージサブシステムにはノード接続ヘルスマニタがあります。

- 個々のヘルスマニタのヘルスステータスを統合したシステム全体のヘルスマニタ

1つのサブシステムのステータスがデグレードになると、システム全体のステータスがデグレードになります。サブシステムにアラートがない場合、システム全体のステータスは OK です。

各ヘルスマニタは、次の主要な要素で構成されています。

- ヘルスマニタが発生させる可能性があるアラート

各アラートには、アラートの重大度や原因の可能性などの詳細が定義されています。

- 各アラートをいつトリガーするかを特定するヘルスポリシー

各ヘルスポリシーには、アラートをトリガーする正確な条件または変更であるルール式があります。

ヘルスマニタは、サブシステム内のリソースの条件または状態の変化を継続的に監視し、検証します。条件または状態の変化がヘルスポリシーのルール式に一致すると、ヘルスマニタはアラートを生成します。アラートにより、サブシステムのヘルスステータスおよびシステム全体のヘルスステータスがデグレードします。

## システムヘルスアラートへの対応方法

システムヘルスアラートが発生した場合は、確認して詳細を確認し、原因となった状態を修復して、再発を防止できます。

ヘルスマニタからアラートが発せられた場合、次のいずれかの方法で対応できます。

- 影響を受けるリソース、アラートの重大度、原因の可能性、考えられる影響、対処方法など、アラートに関する情報を入手する
- アラートが発せられた時間、すでに誰かが承認しているかどうかなど、アラートに関する詳細情報を入手する
- 特定のシェルフやディスクなど、影響を受けるリソースまたはサブシステムの状態に関するヘルス関連の情報を取得する
- アラートを承認して、問題に対応中のユーザがいることを示し、自分自身を「承認者」と指定します。
- ケーブル接続を修正して接続の問題を解決するなど、アラートで指定された対処方法を実施することで、問題を解決する
- アラートが自動的に解除されない場合は、そのアラートを削除します。
- サブシステムのヘルスの状態に影響しないようにアラートを抑制する

問題を把握した場合は、抑制が役に立ちます。アラートを抑制すると、そのアラートは引き続き発生する可能性があります。抑制されたアラートが発生すると、サブシステムのヘルスは「ok-with-suppressed」と表示されます。

## システムヘルスアラートのカスタマイズ

ヘルスマニタが生成するアラートは、アラートをいつトリガーするかを定義するシステムヘルスポリシーを有効または無効にすることによって制御できます。これにより、環境に合わせてヘルス監視システムをカスタマイズできます。

ポリシーの名前は、生成されたアラートの詳細情報を表示するか、特定のヘルスマニタ、ノード、またはアラート ID のポリシー定義を表示することによって確認できます。

ヘルスポリシーの無効化と、アラートの抑制は違います。アラートを抑制した場合はサブシステムのヘルステータスには影響しませんが、アラートは発生します。

ポリシーを無効にした場合に、そのポリシールール式に定義されている条件または状態によるアラートがトリガーされなくなります。

#### 無効にするアラートの例

たとえば、役に立たないアラートが発生するとします。を使用します `system health alert show -instance` コマンドを使用してアラートのポリシーIDを取得します。ポリシーIDはで使用する `system health policy definition show` コマンドを使用してポリシーに関する情報を表示します。ポリシーのルール式およびその他の情報を確認したら、ポリシーを無効にすることにします。を使用します `system health policy definition modify` コマンドを使用してポリシーを無効にします。

### ヘルスアラートによる **AutoSupport** メッセージおよびイベントのトリガー方法

システムヘルスアラートは Event Management System （EMS ；イベント管理システム）の AutoSupport メッセージとイベントをトリガーし、ヘルス監視システムを直接使用することに加え、AutoSupport メッセージと EMS を使用してシステムのヘルスを監視できます。

アラートから 5 分以内に AutoSupport メッセージが送信されます。AutoSupport メッセージには、前の AutoSupport メッセージ以降に生成されたすべてのアラートが含まれます。ただし、同じリソースで前週に原因と同じであると考えられるアラートは除きます。

一部のアラートでは AutoSupport メッセージがトリガーされません。ヘルスポリシーで AutoSupport メッセージの送信が無効になっている場合は、アラートが発生しても AutoSupport メッセージがトリガーされません。たとえば、問題の発生時に AutoSupport ですでにメッセージが生成されているという理由で、ヘルスポリシーによってデフォルトで AutoSupport メッセージを無効にすることができます。を使用し、AutoSupport メッセージをトリガーしないようにポリシーを設定できます `system health policy definition modify` コマンドを実行します

を使用して、前の週に送信されたアラートトリガー型AutoSupport メッセージのすべてのリストを表示できます `system health autosupport trigger history show` コマンドを実行します

アラートは EMS へのイベントの生成もトリガーします。イベントは、アラートが作成されるたび、およびアラートがクリアされるたびに生成されます。

### 使用可能なクラスタヘルスマニタ

ヘルスマニタは複数あり、それぞれがクラスタの異なる部分を監視します。ヘルスマニタは、イベント検出、アラート送信、およびクリアされたイベントの削除を行い、ONTAP システム内で発生したエラーからのリカバリに役立ちます。



ヘルスマニタ名（識別子）	サブシステム名（識別子）	目的
クラスタスイッチ（cluster-switch）	スイッチ（Switch-Health）	<p>温度、利用率、インターフェイスの設定、冗長性（クラスタネットワークスイッチのみ）、ファンおよび電源の動作に関して、クラスタネットワークスイッチと管理ネットワークスイッチを監視します。クラスタスイッチヘルスマニタは SNMP でスイッチと通信します。デフォルトの設定は SNMPv2c です。</p> <div>  <p>ONTAP 9.2 以降では、最後のポーリング期間以降のクラスタスイッチのリポートをこのモニタで検出して報告できるようになりました。</p> </div>
MetroCluster ファブリック	スイッチ	MetroCluster 構成のバックエンドファブリックトポロジを監視して、間違ったケーブル接続およびゾーニングなどの設定ミスや、ISL の障害を検出します。
MetroCluster の健全性	インターコネクト、RAID、ストレージ	FC-VI アダプタ、FC イニシエータアダプタ、取り残されたアグリゲートやディスク、およびクラスタ間ポートを監視します
ノード接続（node-connect）	CIFS のノンストップオペレーション（CIFS-NDO）	SMB 接続を監視して、Hyper-V アプリケーションへのノンストップオペレーションを実現します。
ストレージ（SAS-connect）	ノードレベルでシェルフ、ディスク、およびアダプタを監視して、適切なパスと接続を維持します。	システム
該当なし	他のヘルスマニタからの情報を集約します。	システム接続（system-connect）

## システムヘルスアラートを自動的に受信する

を使用して、システムヘルスアラートを手動で表示できます `system health alert show` コマンドを実行しますただし、ヘルスマニタがアラートを生成したときに通知を自動的に受信するには、特定の Event Management System（EMS；イベント管理システム）メッセージに登録する必要があります。

## このタスクについて

次の手順は、すべての `hm.alert.raised` メッセージ、およびすべての `hm.alert.cleared` メッセージに対する通知のセットアップ方法を示しています。

すべての `hm.alert.raised` メッセージおよび `hm.alert.cleared` メッセージには SNMP トラップが含まれています。SNMP トラップの名前は `HealthMonitorAlertRaised` および `HealthMonitorAlertCleared`。SNMP トラップについては、[\\_ ネットワーク管理ガイド \\_](#) を参照してください。

## 手順

1. 使用します `event destination create` コマンドを使用して、EMSメッセージの送信先を定義します。

```
cluster1::> event destination create -name health_alerts -mail  
admin@example.com
```

2. 使用します `event route add-destinations` コマンドを使用してをルーティングします `hm.alert.raised` メッセージおよび `hm.alert.cleared` 宛先へのメッセージ。

```
cluster1::> event route add-destinations -messagename hm.alert*  
-destinations health_alerts
```

## 関連情報

["Network Management の略"](#)

## デグレードしたシステムヘルスに対応する

システムのヘルスステータスがデグレードした場合は、アラートを表示して考えられる原因および対処方法について一読し、デグレードしたサブシステムに関する情報を表示して、問題を解決できます。抑制されたアラートも表示されるため、変更して承認済みかどうかを確認できます。

## このタスクについて

AutoSupport メッセージやEMSイベントを表示するか、を使用すると、アラートが生成されたことを確認できます `system health` コマンド

## 手順

1. 使用します `system health alert show` コマンドを使用して、システムヘルスを侵害しているアラートを表示します。
2. アラートに示された原因の考えられる影響、考えられる影響、および対処方法を一読し、問題を解決できるか、または詳細情報が必要かを判断します。
3. 詳細情報が必要な場合は、`system health alert show -instance` アラートで使用可能な追加情報 を表示するコマンド。
4. 使用します `system health alert modify` コマンドにを指定します `-acknowledge` パラメータを

指定して、特定のアラートに対して作業中であることを示します。

5. の説明に従って、問題を解決するための対処方法を実行します Corrective Actions フィールドに入力します。

対処方法にはシステムのリブートが含まれている場合があります。

問題が解決すると、アラートは自動的にクリアされます。サブシステムに他のアラートがない場合は、サブシステムのヘルスがに変わります OK。すべてのサブシステムのヘルスがOKの場合は、システム全体のヘルスステータスがに変わります OK。

6. を使用します `system health status show` コマンドを入力して、システムヘルスステータスがであることを確認します OK。

システムのヘルスステータスがでない場合 OK、この手順 を繰り返します。

## デグレードしたシステムヘルスへの対応の例

ノードへの 2 つのパスが不足しているシェルフが原因でデグレードしたシステムヘルスの特定の例を使用して、アラートに対応するときに CLI に表示される内容を確認します。

ONTAP を起動したあと、システムヘルスを確認すると、ステータスがデグレードしていることがわかります。

```
cluster1::>system health status show
Status
-----
degraded
```

アラートを表示して、問題箇所を見つけ、シェルフ 2 にノード 1 へのパスが 2 つないことを確認します。

```
cluster1::>system health alert show
      Node: node1
      Resource: Shelf ID 2
      Severity: Major
      Indication Time: Mon Nov 10 16:48:12 2013
      Probable Cause: Disk shelf 2 does not have two paths to controller
                      node1.
      Possible Effect: Access to disk shelf 2 via controller node1 will be
                      lost with a single hardware component failure (e.g.
                      cable, HBA, or IOM failure).
      Corrective Actions: 1. Halt controller node1 and all controllers attached
                          to disk shelf 2.
                        2. Connect disk shelf 2 to controller node1 via two
                          paths following the rules in the Universal SAS and ACP Cabling Guide.
                        3. Reboot the halted controllers.
                        4. Contact support personnel if the alert persists.
```

アラートの詳細を表示して、アラート ID などの詳細情報を取得します。

```

cluster1::>system health alert show -monitor node-connect -alert-id
DualPathToDiskShelf_Alert -instance
    Node: node1
    Monitor: node-connect
    Alert ID: DualPathToDiskShelf_Alert
    Alerting Resource: 50:05:0c:c1:02:00:0f:02
    Subsystem: SAS-connect
    Indication Time: Mon Mar 21 10:26:38 2011
    Perceived Severity: Major
    Probable Cause: Connection_establishment_error
    Description: Disk shelf 2 does not have two paths to controller
node1.
    Corrective Actions: 1. Halt controller node1 and all controllers
attached to disk shelf 2.
                        2. Connect disk shelf 2 to controller node1 via
two paths following the rules in the Universal SAS and ACP Cabling Guide.
                        3. Reboot the halted controllers.
                        4. Contact support personnel if the alert
persists.
    Possible Effect: Access to disk shelf 2 via controller node1 will
be lost with a single
    hardware component failure (e.g. cable, HBA, or IOM failure).
    Acknowledge: false
    Suppress: false
    Policy: DualPathToDiskShelf_Policy
    Acknowledger: -
    Suppressor: -
    Additional Information: Shelf uuid: 50:05:0c:c1:02:00:0f:02
                        Shelf id: 2
                        Shelf Name: 4d.shelf2
                        Number of Paths: 1
                        Number of Disks: 6
                        Adapter connected to IOMA:
                        Adapter connected to IOMB: 4d
    Alerting Resource Name: Shelf ID 2

```

アラートを確認して対応中であることを示します。

```

cluster1::>system health alert modify -node node1 -alert-id
DualPathToDiskShelf_Alert -acknowledge true

```

シェルフ 2 とノード 1 との間のケーブルを修正してから、システムをリブートします。次に、システムヘルスを再度確認し、ステータスがになっていることを確認します OK:

```
cluster1::>system health status show
Status
-----
OK
```

## クラスタと管理ネットワークスイッチの検出を設定します

クラスタスイッチヘルスマニタは、Cisco Discovery Protocol（CDP）を使用して、クラスタと管理ネットワークスイッチの検出を自動的に試みます。ヘルスマニタがスイッチを自動的に検出できない場合、または CDP を自動検出に使用することを望まない場合は、ヘルスマニタを設定する必要があります。

### このタスクについて

。system cluster-switch show コマンドは、ヘルスマニタが検出したスイッチをリスト表示します。想定していたスイッチがこのリストに表示されない場合、ヘルスマニタは自動的にスイッチを検出できません。

### 手順

1. CDPを自動検出に使用する場合は、次の手順を実行します。
  - a. スイッチで Cisco Discovery Protocol（CDP）が有効になっていることを確認します。

手順については、スイッチのマニュアルを参照してください。

- b. クラスタ内の各ノードで次のコマンドを実行し、CDP が有効か無効かを確認します。

```
run -node node_name -command options cdpd.enable
```

CDP が有効になっている場合は、手順 d に進みます CDP が無効になっている場合は、手順 c に進みます

- c. 次のコマンドを実行して CDP を有効にします。

```
run -node node_name -command options cdpd.enable on
```

5 分待ってから次の手順に進みます。

- a. を使用します system cluster-switch show コマンドを使用して、ONTAP がスイッチを自動的に検出できるようになったかどうかを確認します。
2. ヘルスマニタがスイッチを自動的に検出できない場合は、を使用します system cluster-switch create スイッチの検出を設定するコマンドは次のとおりです。

```
cluster1::> system cluster-switch create -device switch1 -address
192.0.2.250 -snmp-version SNMPv2c -community cshml! -model NX5020 -type
cluster-network
```

5分待ってから次の手順に進みます。

3. 使用します `system cluster-switch show` コマンドを使用して、情報を追加したスイッチをONTAPが検出できることを確認します。

完了後

ヘルスマニタがスイッチを監視できることを確認します。

## クラスタと管理ネットワークスイッチの監視を確認

クラスタスイッチヘルスマニタは検出されたスイッチの監視を自動的に試みますが、スイッチが正しく設定されていないと監視が自動的に行われなかったことがあります。ヘルスマニタが使用中のスイッチを監視するように適切に設定されていることを確認してください。

手順

1. クラスタスイッチヘルスマニタによって検出されたスイッチを特定するには、次のコマンドを入力します。

### ONTAP 9.8以降

```
system switch ethernet show
```

### ONTAP 9.7以前

```
system cluster-switch show
```

状況に応じて Model 列に値が表示されます OTHER の場合、ONTAP はスイッチを監視できません。ONTAP は、値をに設定します `OTHER` 自動検出されたスイッチがヘルスマニタでサポートされていない場合。



コマンド出力にスイッチが表示されない場合は、そのスイッチの検出を設定する必要があります。

2. NetApp Support Siteで、サポートされている最新のスイッチソフトウェアとリファレンス構成ファイル（RCF）にアップグレードします。

### "ネットアップサポートのダウンロードページ"

スイッチの RCF 内のコミュニティストリングは、使用するヘルスマニタが構成されているコミュニティストリングと一致する必要があります。デフォルトでは、ヘルスマニタはコミュニティストリングを使用します cshml1!。



現時点では、ヘルスマニタはSNMPv2のみをサポートしています。

クラスタが監視するスイッチの情報を変更する必要がある場合は、次のコマンドを使用して、ヘルスマニタが使用するコミュニティストリングを変更できます。

**ONTAP 9.8以降**

```
system switch ethernet modify
```

**ONTAP 9.7以前**

```
system cluster-switch modify
```

3. スイッチの管理ポートが管理ネットワークに接続されていることを確認します。

この接続は、SNMP クエリを実行するために必要です。

## システムの健全性を監視するためのコマンドです

を使用できます `system health` システムリソースの健全性に関する情報を表示し、アラートに対応し、以降のアラートを設定するためのコマンド。CLI コマンドを使用すると、ヘルスマニタの設定に関する詳細情報を表示できます。詳細については、各コマンドのマニュアルページを参照してください。

### システムヘルスのステータスを表示します

状況	使用するコマンド
個々のヘルスマニタの全体的なステータスを反映した、システムのヘルスステータスを表示する	<code>system health status show</code>
ヘルス監視が可能なサブシステムのヘルスステータスを表示する	<code>system health subsystem show</code>

### ノード接続のステータスを表示します

状況	使用するコマンド
ノードからストレージシェルフへの接続に関する詳細を表示します。これには、ポート情報、HBA ポート速度、I/O スループット、1 秒あたりの I/O 処理数などの情報が含まれます	<code>storage shelf show -connectivity</code>  を使用します <code>-instance</code> 各シェルフに関する詳細情報を表示するためのパラメータ。
使用可能なスペース、シェルフとベイの番号、所有ノード名など、ドライブとアレイ LUN に関する情報を表示します	<code>storage disk show</code>  を使用します <code>-instance</code> 各ドライブに関する詳細情報を表示するためのパラメータ。
ポートのタイプ、速度、ステータスなど、ストレージシェルフポートに関する詳細情報を表示します	<code>storage port show</code>  を使用します <code>-instance</code> 各アダプタに関する詳細情報を表示するためのパラメータ。



クラスタ、ストレージ、および管理ネットワークスイッチの検出を管理します

状況	使用するコマンド (ONTAP 9.8以降)	使用するコマンド (ONTAP 9.7以前)
クラスタが監視するスイッチを表示します	<code>system switch ethernet show</code>	<code>system cluster-switch show</code>
削除したスイッチ（コマンド出力の Reason 列に表示）を含む、クラスタが現在監視しているスイッチ、およびクラスタや管理ネットワークスイッチへのネットワークアクセスに必要な設定情報を表示します。  このコマンドは、advanced 権限レベルで使用できます。	<code>system switch ethernet show-all</code>	<code>system cluster-switch show-all</code>
未検出のスイッチの検出を設定します	<code>system switch ethernet create</code>	<code>system cluster-switch create</code>
クラスタが監視するスイッチに関する情報（デバイス名、IP アドレス、SNMP バージョン、コミュニティストリングなど）を変更する	<code>system switch ethernet modify</code>	<code>system cluster-switch modify</code>
スイッチの監視を無効にします	<code>system switch ethernet modify -disable-monitoring</code>	<code>system cluster-switch modify -disable-monitoring</code>
スイッチの検出と監視を無効にし、スイッチの設定情報を削除します	<code>system switch ethernet delete</code>	<code>system cluster-switch delete</code>
データベースに格納されているスイッチ設定情報を完全に削除する（これにより、スイッチの自動検出が再度有効になる）	<code>system switch ethernet delete -force</code>	<code>system cluster-switch delete -force</code>
AutoSupport メッセージで送信するには、自動ロギングを有効にします。	<code>system switch ethernet log</code>	<code>system cluster-switch log</code>



生成されたアラートに対応する


状況	使用するコマンド
アラートがトリガーされたリソースやノード、アラートの重大度や原因など、生成されたアラートに関する情報を表示する	<code>system health alert show</code>
生成された各アラートの情報を表示する	<code>system health alert show -instance</code>
アラートに対して作業中であることを示します	<code>system health alert modify</code>
アラートを確認します	<code>system health alert modify -acknowledge</code>
サブシステムのヘルスステータスに影響しないように、以降のアラートを抑制する	<code>system health alert modify -suppress</code>
自動的に消去されなかったアラートを削除します	<code>system health alert delete</code>
あるアラートで AutoSupport メッセージがトリガーされたかどうかを確認するためなど、過去 1 週間にアラートによってトリガーされた AutoSupport メッセージに関する情報を表示する	<code>system health autosupport trigger history show</code>

#### 以後のアラートを設定

状況	使用するコマンド
リソースの状態に応じて特定のアラートを発行するかどうかを制御するポリシーを有効または無効にします	<code>system health policy definition modify</code>

#### ヘルスモニタの設定に関する情報を表示します

状況	使用するコマンド
ヘルスモニタについて、ノード、名前、サブシステム、ステータスなどの情報を表示する	<code>system health config show</code> <div>  <p>を使用します <code>-instance</code> 各ヘルスモニタに関する詳細情報を表示するためのパラメータ。</p> </div>
ヘルスモニタで生成される可能性があるアラートの情報を表示する	<code>system health alert definition show</code> <div>  <p>を使用します <code>-instance</code> 各アラート定義に関する詳細情報を表示するためのパラメータ。</p> </div>

状況	使用するコマンド
アラートが発行されるタイミングを決定する、ヘルスマニタのポリシーに関する情報を表示する	<pre>system health policy definition show</pre> <div>  <p>を使用します <code>-instance</code> 各ポリシーに関する詳細情報を表示するためのパラメータ。ポリシーのステータス（有効または無効）、ヘルスマニタ、アラートなどによってアラートのリストをフィルタリングするには、その他のパラメータを使用します。</p> </div>

## 環境情報を表示します

センサーを使用すると、システムの環境コンポーネントを監視できます。環境センサーについて表示できる情報には、タイプ、名前、状態、値、しきい値警告などがあります。

### ステップ

1. 環境センサーに関する情報を表示するには、を使用します `system node environment sensors show` コマンドを実行します

## File System Analytics の略

### File System Analytics の概要

ONTAP 9.8で初めてFSA（ファイルシステム分析）が導入され、ONTAP FlexGroup またはFlexVol ボリューム内のファイル使用状況やストレージ容量の傾向をリアルタイムで可視化できるようになりました。この標準搭載の機能により、外部ツールが不要になり、ストレージの利用状況や、ビジネスニーズに合わせてストレージを最適化できるかどうかに関する重要な分析情報を得ることができます。

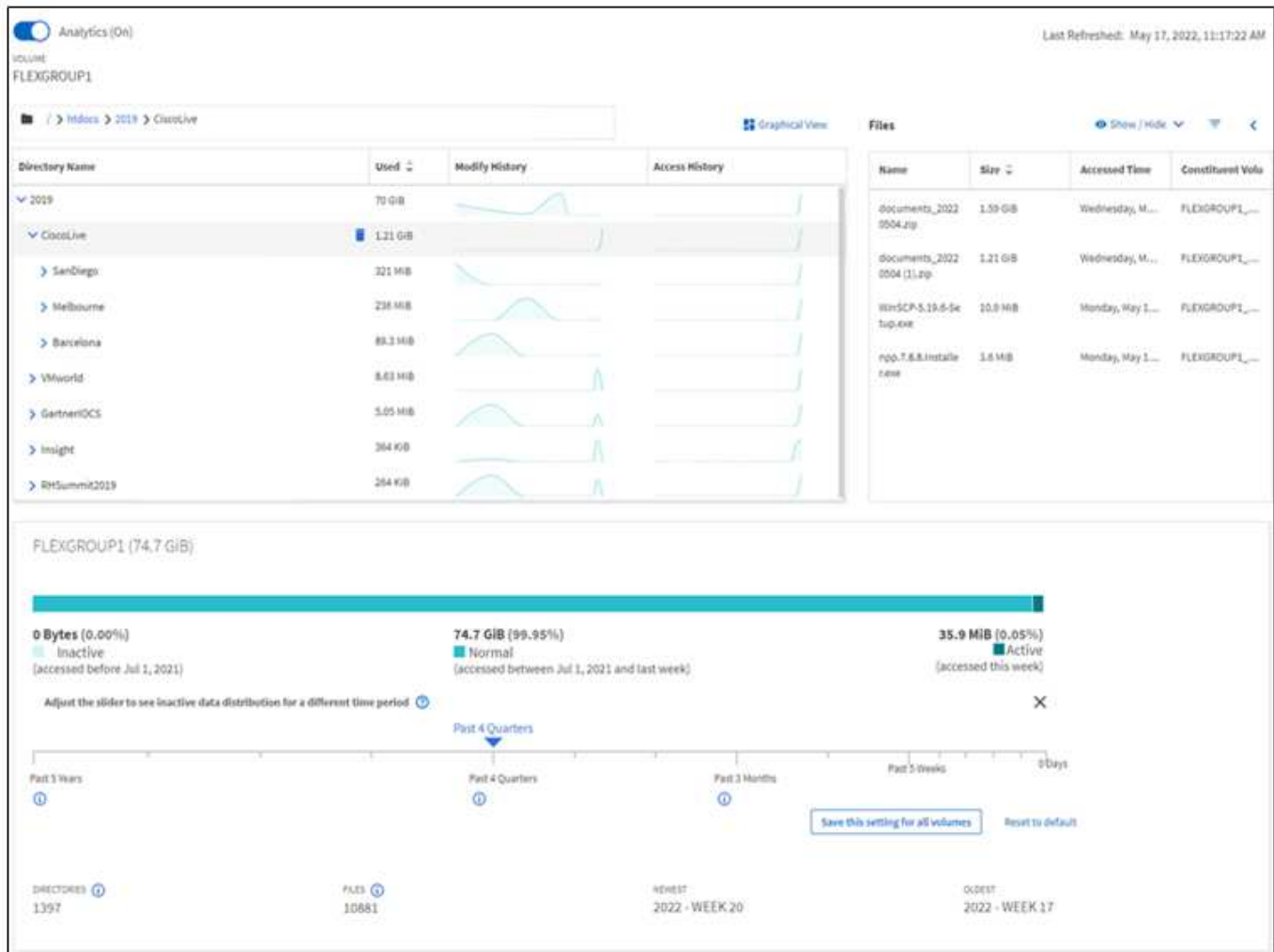
FSAを使用すると、NAS内のボリュームのファイルシステム階層のすべてのレベルが可視化されます。たとえば、Storage VM（SVM）、ボリューム、ディレクトリ、ファイルの各レベルで使用状況と容量を分析できます。FSAを使用して回答 に関する次のような質問をすることができます

- ストレージがいっぱいになっているのは何ですか？また、別のストレージに移動できる大きなファイルはありますか？
- 最もアクティブなボリューム、ディレクトリ、およびファイルはどれですか？ストレージのパフォーマンスはユーザのニーズに合わせて最適化されていますか？
- 先月に追加されたデータの量
- 最もアクティブなストレージユーザと最もアクティブでないストレージユーザのどちらを探していますか？
- プライマリストレージには、どのくらいの非アクティブデータまたは休止データがありますか？そのデータを低コストのコールド階層に移動できますか。

- 計画したサービス品質の変更は、重要で頻繁にアクセスされるファイルへのアクセスに悪影響を及ぼしますか？

ファイルシステム分析は、ONTAP システムマネージャに統合されています。System Managerには次の機能があります。

- リアルタイムで可視化できるため、効果的なデータ管理と運用が可能です
- リアルタイムのデータ収集と集約
- サブディレクトリとファイルのサイズと数、および関連付けられているパフォーマンスプロファイル
- 変更履歴およびアクセス履歴のファイル経過時間ヒストグラム



サポートされているボリュームタイプ

ファイルシステム分析は、FlexCache キャッシュと SnapMirror デスティネーションボリュームを除き、アクティブな NAS データがあるボリュームで可視化を実現するように設計されています。

ファイルシステム分析機能の可用性

ONTAPの各リリースでは、ファイルシステム分析の範囲が拡張されます。

	ONTAP 9.14.1	ONTAP 9.13.1	ONTAP 9.12.1	ONTAP 9.11.1	ONTAP 9.10.1	ONTAP 9.9.1	ONTAP 9.8
System Manager での表示	✓	✓	✓	✓	✓	✓	✓
容量分析	✓	✓	✓	✓	✓	✓	✓
アクセス頻度の低いデータの情 報	✓	✓	✓	✓	✓	✓	✓
Data ONTAP 7-Modeから移行 されたボリュームのサポート	✓	✓	✓	✓	✓	✓	
System Managerで非アクティ ブ期間をカスタマイズできます	✓	✓	✓	✓	✓	✓	
ボリュームレベルのアクティビ ティトラッキング	✓	✓	✓	✓	✓		
アクティビティトラッキングデ ータをCSVにダウンロードしま す	✓	✓	✓	✓	✓		
SVMレベルのアクティビティ追 跡	✓	✓	✓	✓			
タイムライン	✓	✓	✓	✓			
使用状況分析	✓	✓	✓				
オプションを選択して、ファイ ルシステム分析をデフォルトで 有効にします	✓	✓					
初期化スキャン進行状況モニタ	✓						

ファイルシステム分析の詳細をご覧ください

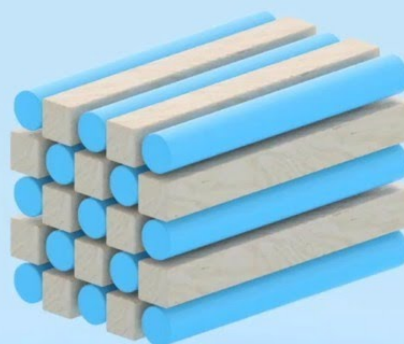
# ONTAP File System Analytics



Daniel Tennant  
Director of Software Engineering  
December 13, 2020



© 2020 NetApp, Inc. All rights reserved. — NETAPP CONFIDENTIAL —



詳細はこちら

- "TR-4687 : 『 Best Practices guidelines for ONTAP File System Analytics 』 "
- "ナレッジベース：NetApp ONTAP ファイルシステム分析をオンにしたあとにレイテンシが大きく変動する、または変動する"

## File System Analytics を有効にします

容量分析などの使用状況データを収集して表示するには、ボリュームでファイルシステム分析を有効にする必要があります。

このタスクについて

- ONTAP 9.8以降では、新規または既存のボリュームでファイルシステム分析を有効にできます。システムをONTAP 9.8以降にアップグレードする場合は、ファイルシステム分析を有効にする前に、すべてのアップグレードプロセスが完了していることを確認してください。
- ボリュームのサイズと内容によっては、ONTAP がボリューム内の既存データを処理する間、分析を有効にするのに時間がかかることがあります。完了すると、System Manager に進捗状況が表示され、分析データが表示されます。初期化の進捗状況に関する詳細情報が必要な場合は、ONTAP CLIコマンドを使用します `volume analytics show`。

ONTAP 9.14.1以降のONTAPでは、スキヤンの進行状況に影響するスロットルイベントに関する通知に加えて、初期化スキヤンの進行状況を追跡できます。

初期化スキヤンに関するその他の考慮事項については、を参照してください [スキヤンに関する考慮事項](#)。

手順

ONTAP システムマネージャまたはCLIを使用して、ファイルシステム分析を有効にできます。

## System Manager の略

ONTAP 9.8 および 9.9.1 では	ONTAP 9.10.1 以降でサポートされます
<ol style="list-style-type: none"><li>1. 「* Storage」 &gt; 「Volumes」を選択します。</li><li>2. 目的のボリュームを選択し、* エクスプローラ * を選択します。</li><li>3. 「* 分析を有効にする *」または「* 分析を無効にする *」を選択します。</li></ol>	<ol style="list-style-type: none"><li>1. 「* Storage」 &gt; 「Volumes」を選択します。</li><li>2. 目的のボリュームを選択します。個別のボリューム・メニューから、* ファイル・システム &gt; エクスプローラ * を選択します。</li><li>3. 「* 分析を有効にする *」または「* 分析を無効にする *」を選択します。</li></ol>

### CLI の使用

CLI を使用してファイルシステム分析を有効にします

1. 次のコマンドを実行します。

```
volume analytics on -vserver svm_name -volume volume_name [-foreground {true|false}]
```

デフォルトでは、このコマンドはフォアグラウンドで実行されます。ONTAP は進捗状況を表示し、完了すると分析データを表示します。より正確な情報が必要な場合は、を使用してコマンドをバックグラウンドで実行できます `-foreground false` オプションを選択し、を使用します `volume analytics show` CLIに初期化の進行状況を表示するコマンド。

2. ファイルシステム分析を有効にしたら、System ManagerまたはONTAP REST APIを使用して分析データを表示します。


ファイルシステム分析のデフォルト設定を変更します

ONTAP 9.13.1以降では、SVMまたはクラスタの設定を変更して、新しいボリュームに対してデフォルトでファイルシステム分析を有効にすることができます。

## System Manager の略

System Managerを使用している場合は、Storage VMまたはクラスタの設定を変更して、ボリューム作成時に容量分析とアクティビティ追跡をデフォルトで有効にすることができます。設定の変更後に作成された環境ボリュームのみがデフォルトで有効になり、既存のボリュームは有効になりません。

クラスタのファイルシステム分析の設定を変更します

1. System Managerで、\*[クラスタ設定]に移動します。
2. クラスタ設定で、[ファイルシステム設定]タブを確認します。設定を変更するには、 をクリックします。
3. [\*Activity Tracking]フィールドに、アクティビティ追跡をデフォルトで有効にするSVMの名前を入力します。このフィールドを空白のままにすると、すべてのSVMでアクティビティ追跡が無効のままになります。

新しいStorage VMでアクティビティ追跡をデフォルトで無効にするには、[Enable on new Storage VMs]ボックスをオフにします。

4. [\*Analytics]フィールドに、容量分析をデフォルトで有効にするStorage VMの名前を入力します。このフィールドを空白のままにすると、すべてのSVMで容量分析が無効のままになります。

新しいStorage VMに対して容量分析をデフォルトで無効にするには、[Enable on new Storage VMs]ボックスをオフにします。

5. 保存を選択します。

SVMのファイルシステム分析設定を変更します

1. 変更するSVMを選択し、**Storage VM**設定を選択します。
2. [\* File System Analytics]カードで、トグルを使用して、Storage VM上のすべての新しいボリュームに対してアクティビティ追跡と容量分析を有効または無効にします。

## CLI の使用

ONTAP CLIを使用して、新しいボリュームでファイルシステム分析をデフォルトで有効にするようにStorage VMを設定できます。

SVMでファイルシステム分析をデフォルトで有効にします

1. SVMを変更して、新しく作成したすべてのボリュームで容量分析とアクティビティ追跡をデフォルトで有効にします。

```
vserver modify -vserver svm_name -auto-enable-activity-tracking true -auto-enable-analytics true
```

## ファイルシステムのアクティビティを表示します

File System Analytics (FSA) を有効にすると、選択したボリュームのルートディレクトリの内容を各サブツリーで使用されているスペースでソートして表示できます。

ファイルシステムを参照したり、ディレクトリ内の各オブジェクトに関する詳細情報を表示したりするには、任意のファイルシステムオブジェクトを選択します。ディレクトリの情報をグラフィカルに表示することもできます。時間の経過とともに、各サブツリーの履歴データが表示されます。ディレクトリ数が 3000 を超える



場合、使用済みスペースはソートされません。

## エクスプローラ（ Explorer ）

File System Analytics \* Explorer \* 画面は、次の 3 つの領域で構成されています。

- ディレクトリとサブディレクトリのツリービュー。名前、サイズ、変更履歴、アクセス履歴を示す展開可能なリスト。
- ファイル。ディレクトリリストで選択したオブジェクトの名前、サイズ、アクセス日時を表示します。
- ディレクトリリストで選択したオブジェクトのアクティブデータと非アクティブデータの比較。

ONTAP 9.9.1以降では、レポート対象の範囲をカスタマイズできます。デフォルト値は 1 年です。これらのカスタマイズ内容に基づいて、ボリュームの移動や階層化ポリシーの変更などの対応を実行できます。

デフォルトでは、アクセス時間が表示されます。ただし、CLIから（を設定して）ボリュームのデフォルトを変更した場合は `-atime-update` オプションをに設定します `false` を使用 `volume modify` コマンド）を入力した場合は、最終変更時刻のみが表示されます。例：

- ツリービューには、\* アクセス履歴 \* は表示されません。
- ファイルビューが変更されます。
- 変更後の時刻に基づいてアクティブ/非アクティブデータビューが表示されます (`mtime`) 。

これらの表示を使用して、次のことを確認できます。

- ファイルシステムの場所が最も多くのスペースを消費している
- ディレクトリおよびサブディレクトリ内のファイル数やサブディレクトリ数など、ディレクトリツリーに関する詳細情報
- 古いデータを含むファイルシステムの場所（スクラッチ、一時、ログツリーなど）

FSA の出力を解釈するときは、次の点に留意してください。

- データの使用場所と使用時期は、処理されるデータ量ではなく、FSA によって示されます。たとえば、最近アクセスされたファイルや変更されたファイルによる大量のスペース消費は、必ずしもシステムの処理負荷が高いことを示すわけではありません。
- [ ボリュームエクスプローラ \* ] タブで FSA のスペース消費を計算する方法は、他のツールとは異なる場合があります。特に、ボリュームで Storage Efficiency 機能が有効になっている場合、ボリューム概要 \* で報告される消費量と大きく異なる可能性があります。これは、\* ボリュームエクスプローラ \* タブには効率化による削減効果がないためです。
- ディレクトリ表示のスペースに制限があるため、*List View* で 8 レベルを超えるディレクトリ階層を表示することはできません。8 レベルを超えるディレクトリを詳細に表示するには、*Graphical View* に切り替え、目的のディレクトリを見つけて、*List View* に切り替える必要があります。これにより、ディスプレイに画面スペースが追加されます。

## 手順

1. 選択したボリュームのルートディレクトリの内容を表示します。

ONTAP 9.8 および 9.9.1 では	ONTAP 9.10.1 以降でサポートされます
[* ストレージ]、[ ボリューム ] の順にクリックし、目的のボリュームを選択して、[* エクスプローラ *] をクリックします。	[* Storage] > [Volumes] を選択し、目的のボリュームを選択します。個別のボリューム・メニューから、* ファイル・システム > エクスプローラ * を選択します。

## アクティビティトラッキングを有効にします

ONTAP 9.10.1以降のファイルシステム分析にはアクティビティ追跡機能が含まれています。この機能を使用すると、ホットオブジェクトを特定してデータをCSVファイルとしてダウンロードできます。ONTAP 9.11.1以降では、アクティビティトラッキングがSVMスコープに拡張されています。また、ONTAP 9.11.1以降、System Managerではアクティビティ追跡のタイムラインが表示され、最大5分間のアクティビティ追跡データを確認できます。

アクティビティ追跡では、次の4つのカテゴリでモニタリングが可能です。

- ディレクトリ
- ファイル
- クライアント
- ユーザ

監視対象のカテゴリごとに、読み取り IOPS、書き込み IOPS、読み取りスループット、書き込みスループットが表示されます。アクティビティトラッキングに関するクエリーは、過去5秒間にシステムに表示されたホットスポットに関連する10～15秒ごとに更新されます。

アクティビティ追跡情報は概算値であり、データの正確性は受信 I/O トラフィックの分散に依存します。

System Managerでボリュームレベルでアクティビティ追跡を表示している場合は、展開されたボリュームのメニューだけがアクティブに更新されます。ボリュームのビューが縮小されている場合、ボリュームの表示が展開されるまで表示は更新されません。更新を停止するには、\* 更新を一時停止 \* ボタンを使用します。アクティビティデータはCSV形式でダウンロードでき、選択したボリュームについて収集されたすべてのポイントインタイムデータが表示されます。

タイムライン機能を使用できるONTAP 9.11.1以降では、ボリュームまたはSVM上のホットスポットアクティビティの記録を保持し、約5秒ごとに継続的に更新し、過去5分間のデータを保持できます。タイムラインデータは、ページの表示領域にあるフィールドに対してのみ保持されます。追跡カテゴリを折りたたむかスクロールしてタイムラインが表示されないようにすると、タイムラインはデータの収集を停止します。デフォルトでは、タイムラインは無効になっており、[アクティビティ]タブから移動すると自動的に無効になります。

## 1つのボリュームのアクティビティトラッキングを有効にします

アクティビティ追跡は、ONTAP System ManagerまたはCLIを使用して有効にできます。

### このタスクについて

ONTAP REST API または System Manager で RBAC を使用する場合は、アクティビティ追跡へのアクセスを管理するためのカスタムロールを作成する必要があります。を参照してください [ロールベースアクセス制御](#) をクリックしてください。

## System Manager の略

### 手順

1. Storage > Volumes (ストレージ) を選択します。目的のボリュームを選択します。個々のボリュームメニューから、ファイルシステムを選択し、アクティビティタブを選択します。
2. 上位のディレクトリ、ファイル、クライアント、およびユーザに関する個々のレポートを表示するには、\* Activity Tracking \* をオンにします。
3. 更新を行わずにデータをより詳細に分析するには、\* 更新を一時停止 \* を選択します。データをダウンロードして、レポートの CSV レコードを取得することもできます。

## CLI の使用

### 手順

1. アクティビティトラッキングを有効にする：

```
volume activity-tracking on -vserver svm_name -volume volume_name
```

2. 次のコマンドを使用して、ボリュームのアクティビティ追跡の状態がオンまたはオフになっているかどうかを確認します。

```
volume activity-tracking show -vserver svm_name -volume volume_name -state
```

3. 有効にしたら、ONTAP システムマネージャまたは ONTAP REST API を使用してアクティビティ追跡データを表示します。

## 複数のボリュームのアクティビティ追跡を有効にします

System Manager または CLI を使用して、複数のボリュームのアクティビティ追跡を有効にすることができます。

### このタスクについて

ONTAP REST API または System Manager で RBAC を使用する場合は、アクティビティ追跡へのアクセスを管理するためのカスタムロールを作成する必要があります。を参照してください [ロールベースアクセス制御](#) をクリックしてください。

## System Manager の略

特定のボリュームに対して有効にします

1. Storage > Volumes（ストレージ）を選択します。目的のボリュームを選択します。個々のボリュームメニューから、ファイルシステムを選択し、アクティビティタブを選択します。
2. アクティビティトラッキングを有効にするボリュームを選択します。ボリュームリストの上部で、その他のオプション\*ボタンを選択します。[\*アクティビティトラッキングを有効にする]を選択します。
3. SVMレベルでアクティビティの追跡を表示するには、表示するSVMを\* Storage > Volumes \*から選択します。[ファイルシステム]タブに移動して[アクティビティ]を選択すると、アクティビティ追跡が有効になっているボリュームのデータが表示されます。

すべてのボリュームで有効にします

1. Storage > Volumes（ストレージ）を選択します。メニューからSVMを選択します。
2. 「\* File System」タブに移動し、「More \*」タブを選択して、SVM内のすべてのボリュームでアクティビティの追跡を有効にします。

## CLI の使用

ONTAP 9.13.1以降では、ONTAP CLIを使用して複数のボリュームのアクティビティ追跡を有効にすることができます。

手順

1. アクティビティトラッキングを有効にする：

```
volume activity-tracking on -vserver svm_name -volume [*|!volume_names]
```

使用 \* 指定したStorage VM上のすべてのボリュームに対してアクティビティ追跡を有効にします。

使用 ! 続けてボリューム名を指定し、指定したボリュームを除くSVM上のすべてのボリュームに対してアクティビティ追跡を有効にします。

2. 処理が成功したことを確認します。

```
volume show -fields activity-tracking-state
```

3. 有効にしたら、ONTAP システムマネージャまたは ONTAP REST API を使用してアクティビティ追跡データを表示します。

## 使用状況分析を実現

ONTAP 9.12.1以降では、使用状況分析を有効にして、ボリューム内のどのディレクトリが最もスペースを使用しているかを確認できます。ボリューム内のディレクトリの総数、またはボリューム内のファイルの総数を表示できます。Reportingは、最もスペースを使用する25個のディレクトリに制限されます。

大規模ディレクトリの分析は15分ごとに更新されます。ページ上部の[Last refreshed]のタイムスタンプを確認すると、最新の更新を監視できます。[ダウンロード]ボタンをクリックして、Excelブックにデータをダウンロードすることもできます。ダウンロード処理はバックグラウンドで実行され、選択したボリュームについて最

新の情報が表示されます。結果が表示されずにスキャンが戻った場合は、ボリュームがオンラインであることを確認します。SnapRestore などのイベントが発生すると、原因 ファイルシステム分析は大きなディレクトリのリストを再構築します。

#### 手順

1. Storage > Volumes (ストレージ) を選択します。目的のボリュームを選択します。
2. 個別のボリューム・メニューから、ファイル・システム\*を選択します。次に、Usage \*タブを選択します。
3. 使用状況の分析を有効にするには、\* Analytics \*スイッチを切り替えます。
4. System Managerでは、最大サイズのディレクトリを降順に示す棒グラフが表示されます。



ONTAP では、上位ディレクトリのリストの収集中に、部分データが表示されたり、まったくデータが表示されないことがあります。スキャンの進行状況は、スキャン中に表示される[Usage]タブで確認できます。

特定のディレクトリに関する詳細な情報を得るには、次の手順を実行します。 [ファイルシステム上のアクティビティを表示する](#)。

## 分析に基づいて修正措置を講じる

ONTAP 9.9.1以降では、ファイルシステム分析画面から、現在のデータと期待される結果に基づいて直接対処できます。

### ディレクトリとファイルを削除します

エクスプローラの表示で、削除するディレクトリまたは個々のファイルを選択できます。低レイテンシの高速ディレクトリ削除機能により、ディレクトリが削除されます。（高速ディレクトリ削除は、分析を有効にしない ONTAP 9.9.1 以降でも使用できます）。

#### 手順

1. [\* ストレージ]、[ボリューム] の順にクリックし、[\* エクスプローラ \*] をクリックします。

ファイルまたはフォルダにカーソルを合わせると、削除するオプションが表示されます。一度に削除できるオブジェクトは 1 つだけです。



ディレクトリとファイルを削除しても、新しいストレージ容量の値はすぐには表示されません。

ストレージ階層にメディアコストを割り当てて、使用頻度の低いデータストレージのコストを比較します

メディアコストは、ストレージコストの評価に基づいて割り当てた値であり、GB あたりの通貨を選択したものとして表されます。設定すると、System Manager は割り当てられているメディアコストを使用して、ボリュームを移動するときの推定削減量を計算します。

設定したメディアコストは永続的ではなく、1 つのブラウザセッションにのみ設定できます。

#### 手順

1. [ストレージ]>[階層]をクリックし、ローカル階層（アグリゲート）のタイルで[メディアコストの設定]\*を

クリックします。

アクティブな階層と非アクティブな階層を選択して、比較を有効にしてください。

## 2. 通貨タイプと金額を入力します。


メディアコストを入力または変更すると、すべてのメディアタイプで変更が行われます。

### ボリュームを移動してストレージコストを削減

分析画面やメディアコストの比較に基づいて、ローカル階層内の低コストのストレージにボリュームを移動できます。

一度に 1 つのボリュームのみを比較および移動できます。

#### 手順

1. メディアコストの表示を有効にしたら、[\* ストレージ > 階層 \*] をクリックし、[\* ボリューム \*] をクリックします。
2. ボリュームのデスティネーションオプションを比較するには、をクリックします  ボリュームの場合は、\* 移動 \* をクリックします。
3. [Select Destination Local Tier]（宛先ローカル階層の選択）画面で、推定コスト差異を表示する宛先階層を選択します。
4. オプションを比較したら、目的の階層を選択し、\* 移動 \* をクリックします。

### ファイルシステム分析を使用したロールベースアクセス制御

ONTAP 9.12.1以降では、ONTAP に、という名前の事前定義されたロールベースアクセス制御（RBAC）ロールが含まれています admin-no-fsa。 admin-no-fsa ロールは管理者レベルの権限を付与しますが、に関連する処理は実行できません files ONTAP CLI、REST API、およびSystem Managerのエンドポイント（ファイルシステム分析など）

詳細については、を参照してください admin-no-fsa ロール。を参照してください [クラスタ管理者の事前定義されたロール](#)。

ONTAP 9.12.1よりも前のバージョンのONTAP を使用している場合は、ファイルシステム分析へのアクセスを制御する専用のロールを作成する必要があります。ONTAP 9.12.1よりも前のバージョンのONTAP では、ONTAP CLIまたはONTAP REST APIを使用してRBAC権限を設定する必要があります。

## System Manager の略

ONTAP 9.12.1以降では、System Managerを使用してファイルシステム分析用のRBAC権限を設定できます。

### 手順

1. [\* Cluster]>[Settings]（設定）を選択します。[\*セキュリティ]で、[ユーザーと役割]に移動し、を選択します →。
2. [役割（ Roles） ]でを選択します [+ Add](#)。
3. ロールの名前を指定します。Role Attributesで、適切なを指定してユーザロールのアクセスまたは制限を設定します ["APIエンドポイント"](#)。File System Analyticsアクセスまたは制限を設定するためのプライマリパスとセカンダリパスについては、次の表を参照してください。

制限	プライマリパス	セカンダリパス
ボリュームのアクティビティ追跡	/api/storage/volumes	<ul style="list-style-type: none"><li>• /:uuid/top-metrics/directories</li><li>• /:uuid/top-metrics/files</li><li>• /:uuid/top-metrics/clients</li><li>• /:uuid/top-metrics/users</li></ul>
SVMのアクティビティ追跡	/api/svm/svms	<ul style="list-style-type: none"><li>• /:uuid/top-metrics/directories</li><li>• /:uuid/top-metrics/files</li><li>• /:uuid/top-metrics/clients</li><li>• /:uuid/top-metrics/users</li></ul>
すべてのファイルシステム分析処理	/api/storage/volumes	/:uuid/files

を使用できます /\*/ エンドポイントのすべてのボリュームまたはSVMにポリシーを設定する場合は、UUIDの代わりにUUIDが設定されます。

各エンドポイントのアクセス権限を選択します。

4. [ 保存（ Save ） ]を選択します。
5. ユーザにロールを割り当てる手順については、を参照してください [管理者アクセスの制御](#)。

### CLI の使用

ONTAP 9.12.1よりも前のバージョンのONTAP を使用している場合は、ONTAP CLIを使用してカスタム

ロールを作成します。

#### 手順

1. すべての機能にアクセスできるようにデフォルトのロールを作成します。

この作業は 'ロールがアクティビティの追跡のみに限定されるようにするために' 制限的なロールを作成する前に実行する必要があります

```
security login role create -cmddirname DEFAULT -access all -role storageAdmin
```

2. 制限付きロールを作成します。

```
security login role create -cmddirname "volume file show-disk-usage" -access none -role storageAdmin
```

3. ロールに SVM の Web サービスへのアクセスを許可します。

- rest (REST API呼び出しの場合)
- security パスワード保護のため
- sysmgr System Managerへのアクセスに使用します

```
vserver services web access create -vserver svm-name -name_ -name rest -role storageAdmin
```

```
vserver services web access create -vserver svm-name -name security -role storageAdmin
```

```
vserver services web access create -vserver svm-name -name sysmgr -role storageAdmin
```

4. ユーザを作成します。

ユーザに適用するアプリケーションごとに個別の create コマンドを問題 に設定する必要があります。同じユーザで create を複数回呼び出すと、すべてのアプリケーションがそのユーザに適用されるだけで、毎回新しいユーザが作成されることはありません。。 http アプリケーションタイプのパラメータは、ONTAP REST APIおよびSystem Managerに適用されます。

```
security login create -user-or-group-name storageUser -authentication -method password -application http -role storageAdmin
```

5. 新しいユーザクレデンシャルを使用して、System Managerにログインするか、ONTAP REST APIを使用してファイルシステム分析データにアクセスできるようになりました。

#### 詳細情報

- [クラスタ管理者の事前定義されたロール](#)
- [System Managerで管理者アクセスを制御します](#)
- ["RBACロールとONTAP REST APIの詳細については、こちらをご覧ください"](#)



## ファイルシステム分析に関する考慮事項

ファイルシステム分析の実装に伴う使用の制限とパフォーマンスへの潜在的な影響について理解しておく必要があります。

### SVMで保護されている関係

保護関係にある SVM を含むボリュームでファイルシステム分析を有効にしている場合、分析データはデステーション SVM にレプリケートされません。リカバリ処理でソース SVM を再同期する必要がある場合は、リカバリ後に目的のボリュームの分析を手動で再度有効にする必要があります。

### パフォーマンスに関する考慮事項

場合によっては、File System Analyticsを有効にすると、メタデータの初回収集時のパフォーマンスに悪影響を及ぼすことがあります。この状況は、通常、使用率が最大のシステムで発生します。このようなシステムでは、分析を有効にしないように、ONTAP System Managerのパフォーマンス監視ツールを使用できます。

レイテンシが著しく増加している場合は、ナレッジベースの記事を参照してください ["NetApp ONTAP ファイルシステム分析を有効にしたあとにレイテンシが増減する"](#)。

### スキャンに関する考慮事項

容量分析を有効にすると、ONTAPは容量分析の初期化スキャンを実行します。スキャンは、容量分析が有効になっているボリューム内のすべてのファイルのメタデータにアクセスします。スキャン中にファイルデータは読み取られません。ONTAP 9.14.1以降では、REST API、System Managerの[\* **Explorer**]タブ、または `volume analytics show` CLIコマンド。スロットルイベントが発生した場合は、ONTAPから通知が送信されます。

スキャンが完了すると、ファイルシステムの変更に応じてファイルシステム分析がリアルタイムで継続的に更新されます。スキャンを再度実行する必要はありません。

スキャンに必要な時間は、ボリューム上のディレクトリとファイルの数に比例します。スキャンではメタデータが収集されるため、ファイルサイズはスキャン時間に影響しません。

初期化スキャンの詳細については、を参照してください ["TR-4867 : 『Best Practice Guidelines for File System Analytics』"](#)。

### ベストプラクティス

アグリゲートを共有していないボリュームでスキャンを開始する必要があります。現在どのアグリゲートがどのボリュームをホストしているかは、コマンドを使用して確認できます。

```
volume show -volume comma-separated-list_of_volumes -fields aggr-list
```

スキャンの実行中も、ボリュームは引き続きクライアントトラフィックを処理します。クライアントトラフィックが低いと予想される期間にスキャンを開始することをお勧めします。

クライアントトラフィックが増加すると、システムリソースが消費され、原因 スキャンにかかる時間が長くなります。

ONTAP 9.12.1以降では、System ManagerおよびONTAP CLIでデータ収集を一時停止できます。

- ONTAP CLIを使用する場合は、次の手順を実行します。
  - 次のコマンドを使用してデータ収集を一時停止できます。 `volume analytics initialization pause -vserver svm_name -volume volume_name`
  - クライアントトラフィックの速度が低下したら、次のコマンドを使用してデータ収集を再開できます。 `volume analytics initialization resume -vserver svm_name -volume volume_name`
- System Managerを使用している場合は、ボリュームメニューの\*ビューで[データ収集の一時停止]および[データ収集の再開]\*ボタンを使用してスキャンを管理します。

## EMSノセツテイ

### EMS設定の概要

早急な対応が必要なシステムの問題をすぐに通知するように、イベント管理システム（EMS）の重要なイベント通知をEメールアドレス、syslogサーバ、簡易管理ネットワークプロトコル（SNMP）トラップホスト、またはWebhookアプリケーションに直接送信するようにONTAP 9を設定できます。

重要なイベント通知はデフォルトでは有効になっていないため、Eメールアドレス、syslogサーバ、SNMPトラップホスト、またはWebhookアプリケーションのいずれかに通知を送信するようにEMSを設定する必要があります。

のリリース固有のバージョンを確認します ["ONTAP 9 EMSリファレンス"](#)。

EMSイベントのマッピングで廃止されたONTAP コマンドセット（イベントの送信先、イベントルートなど）を使用している場合は、マッピングを更新することを推奨します。 ["廃止されたONTAP コマンドからEMSマッピングを更新する方法について説明します"](#)。

### System Manager で EMS イベントの通知とフィルタを設定します

System Manager を使用して、早急な対応を要するシステムの問題を通知するために、Event Management System （EMS；イベント管理システム）でのイベント通知の配信方法を設定できます。

ONTAPバージョン	System Manager で実行できる作業
ONTAP 9.12.1以降	リモートsyslogサーバにイベントを送信するときに、Transport Layer Security（TLS）プロトコルを指定します。
ONTAP 9.10.1 以降	SNMPトラップホストに加え、Eメールアドレス、syslogサーバ、Webフックアプリケーションを設定します。
ONTAP 9.7 から 9.10.0	SNMPトラップホストのみを設定する。ONTAP CLI を使用して他のEMS デスティネーションを設定できます。を参照してください <a href="#">"EMS設定の概要"</a> 。

次の手順を実行できます。

- [\[add-ems-destination\]](#)
- [\[create-ems-filter\]](#)
- [\[edit-ems-destination\]](#)
- [\[edit-ems-filter\]](#)
- [\[delete-ems-destination\]](#)
- [\[delete-ems-filter\]](#)

関連情報

- ["ONTAP EMSリファレンス"](#)
- ["CLI を使用して、イベント通知を受信する SNMP トラップホストを設定します"](#)

**EMS** イベント通知の送信先を追加します

System Manager を使用して、EMS メッセージの送信先を指定できます。

ONTAP 9.12.1以降では、EMSイベントをTransport Layer Security（TLS）プロトコル経由でリモートsyslogサーバの指定ポートに送信できます。詳細については、[を参照してください event notification destination create](#) のマニュアルページ。

手順

1. **[Cluster] > [Settings]** の順にクリックします。
2. **[\*Notifications Management]** セクションで、[を](#)クリックします [:](#)をクリックし、**\* イベントの送信先の表示 \*** をクリックします。
3. **[\* 通知管理 ]** ページで、**[ イベントの送信先 \*]** タブを選択します。
4. [を](#)クリックします **+ Add**。
5. 名前、EMS デスティネーションタイプ、およびフィルタを指定します。



必要に応じて、新しいフィルタを追加できます。[新しいイベントフィルタの追加 \*] をクリックします。

6. 選択した EMS デスティネーションのタイプに応じて、次の情報を指定します。



構成する	指定または選択 ...
SNMP トラップホスト	<ul style="list-style-type: none"><li>• トラップホスト名</li></ul>
E メール  ( 9.10.1 以降)	<ul style="list-style-type: none"><li>• 送信先 E メールアドレス</li><li>• メールサーバ</li><li>• 送信元 E メールアドレス</li></ul>


syslog サーバ  ( 9.10.1 以降)	<ul style="list-style-type: none"> <li>• サーバのホスト名または IP アドレス</li> <li>• Syslogポート (9.12.1以降)</li> <li>• Syslog転送 (9.12.1以降)</li> </ul> <p>TCP Encrypted を選択すると、<b>Transport Layer Security (TLS)</b> プロトコルが有効になります。<b>syslog</b>ポート*に値を入力しない場合は、「Syslog transport *」の選択に基づいてデフォルトが使用されます。</p>
ウェブフック  ( 9.10.1 以降)	<ul style="list-style-type: none"> <li>• webhook URL</li> <li>• クライアント認証 (クライアント証明書を指定する場合はこのオプションを選択します)</li> </ul>

### 新しい **EMS** イベント通知フィルタを作成します

ONTAP 9.10.1 以降の System Manager を使用して、EMS 通知の処理ルールを指定する、カスタマイズされた新しいフィルタを定義できます。

#### 手順



1. **[Cluster] > [Settings]** の順にクリックします。
2. **[Notifications Management]** セクションで、をクリックします  をクリックし、[イベントの送信先の表示]\*をクリックします。
3. [\* 通知管理 \*] ページで、[\* イベント・フィルタ \*] タブを選択します。
4. をクリックします  **Add**。
5. 名前を指定し、既存のイベントフィルタからルールをコピーするか、新しいルールを追加するかを選択します。
6. 選択した手順に応じて、次の手順を実行します。

選択した場合	次に、次の手順を実行します。
<ul style="list-style-type: none"> <li>• 既存のイベントフィルタからルールをコピー *</li> </ul>	<ol style="list-style-type: none"> <li>1. 既存のイベントフィルタを選択します。</li> <li>2. 既存のルールを変更します。</li> <li>3. 必要に応じて、をクリックして他のルールを追加します  <b>Add</b>。</li> </ol>
<ul style="list-style-type: none"> <li>• 新しいルールを追加 *</li> </ul>	新しいルールごとに、タイプ、名前パターン、重大度、および SNMP トラップのタイプを指定します。

### **EMS** イベント通知の送信先を編集します

ONTAP 9.10.1 以降では、System Manager を使用してイベント通知の送信先情報を変更できます。

#### 手順

1. **[Cluster] > [Settings]** の順にクリックします。
2. **[\*Notifications Management]** セクションで、をクリックします  をクリックし、\* イベントの送信先の表示 \* をクリックします。
3. **[Notifications Management]** ページで、**[\*Events Destinations]** タブを選択します。
4. イベントの送信先の名前の横にあるをクリックします  をクリックし、\* 編集 \* をクリックします。
5. イベントの送信先情報を変更し、\* 保存 \* をクリックします。



### EMS イベント通知フィルタを編集します

ONTAP 9.10.1 以降の System Manager を使用して、カスタマイズしたフィルタを変更して、イベント通知の処理方法を変更できるようになりました。



システム定義のフィルタは変更できません。

#### 手順

1. **[Cluster] > [Settings]** の順にクリックします。
2. **[Notifications Management]** セクションで、をクリックします  をクリックし、[イベントの送信先の表示]\*をクリックします。
3. **[\* 通知管理 \*]** ページで、**[\* イベント・フィルタ \*]** タブを選択します。
4. イベントフィルタの名前の横にあるをクリックします  をクリックし、\* 編集 \* をクリックします。
5. イベントフィルタの情報を変更し、[ 保存 ( Save ) ] をクリックします。



### EMS イベント通知の送信先を削除します

ONTAP 9.10.1 以降の場合、 System Manager を使用して EMS イベント通知の送信先を削除できます。



SNMP 送信先は削除できません。

#### 手順

1. **[Cluster] > [Settings]** の順にクリックします。
2. **[Notifications Management]** セクションで、をクリックします  をクリックし、[イベントの送信先の表示]\*をクリックします。
3. **[\* 通知管理 ]** ページで、**[ イベントの送信先 \*]** タブを選択します。
4. イベントの送信先の名前の横にあるをクリックします  をクリックし、\*[削除]\*をクリックします。

### EMS イベント通知フィルタを削除します



ONTAP 9.10.1 以降の System Manager を使用して、カスタマイズしたフィルタを削除できるようになりました。



システム定義のフィルタは削除できません。

#### 手順

1. **[Cluster] > [Settings]** の順にクリックします。

2. **[Notifications Management]** セクションで、をクリックします  をクリックし、[イベントの送信先の表示]\*をクリックします。
3. [\* 通知管理 \*] ページで、[\* イベント・フィルタ \*] タブを選択します。
4. イベントフィルタの名前の横にあるをクリックします  をクリックし、\* 削除 \* をクリックします。

## CLI を使用して EMS イベント通知を設定します

### EMSの設定ワークフロー

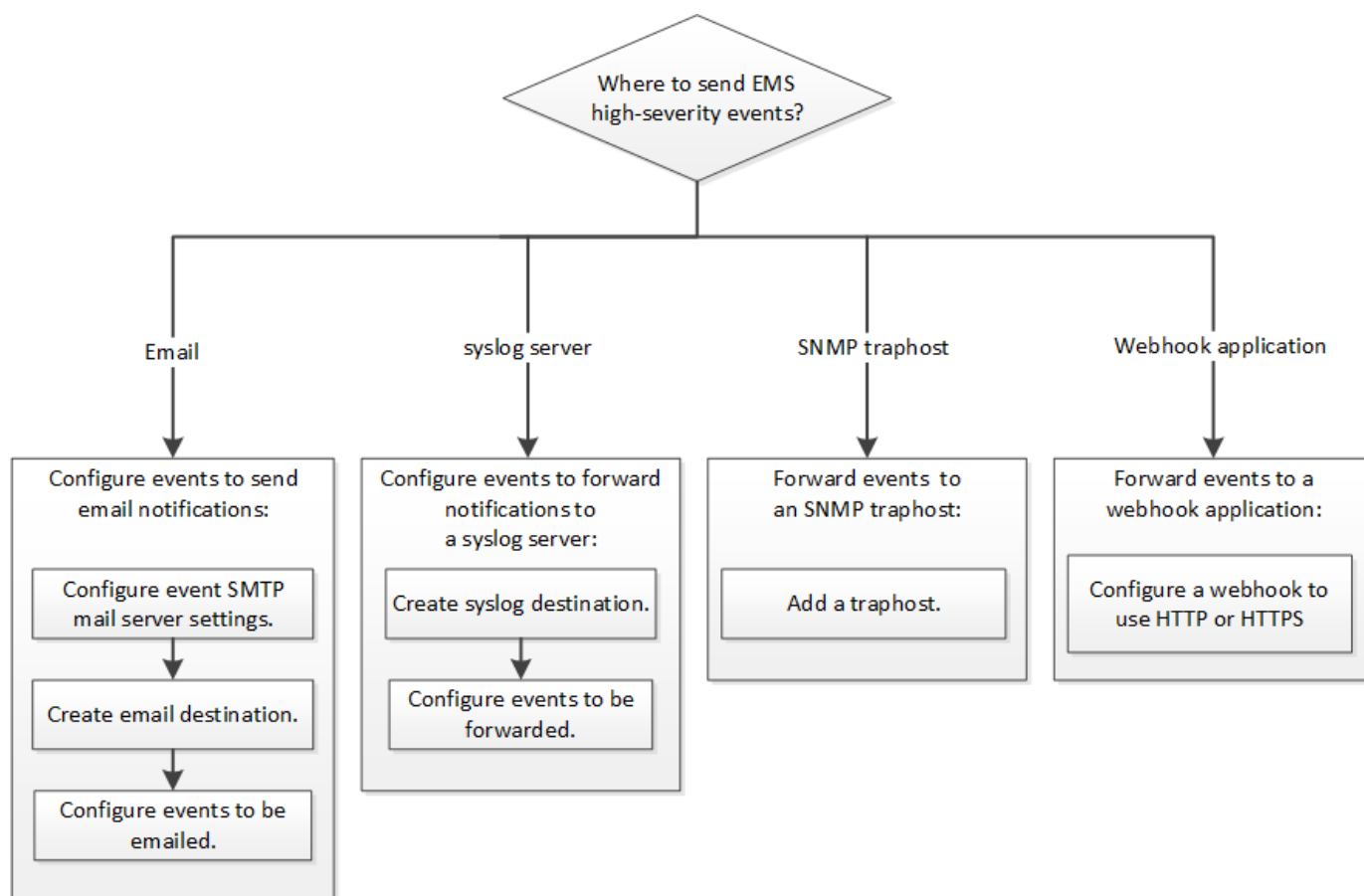
重要なEMSイベント通知は、Eメールで送信されるか、syslogサーバに転送されるか、SNMPトラップホストに転送されるか、またはWebフックアプリケーションに転送されるように設定する必要があります。これにより、適切な修正措置を講じてシステムの停止を回避できます。

このタスクについて

サーバやアプリケーションなどの他のシステムで記録されたイベントを集約するためにすでに syslog サーバを使用している場合は、ストレージシステムの重要なイベントの通知にもその syslog サーバを使用すると簡単です。

syslog サーバがまだない場合は、重要なイベントの通知に E メールを使用すると便利です。

イベント通知をすでに SNMP トラップホストに転送している場合は、そのトラップホストで重要なイベントについても監視できます。



選択肢

- ・ イベント通知を送信するように EMS を設定します。

状況	参照先
EMS の重要なイベント通知を E メールアドレスに送信します	<a href="#">重要な EMS イベントの通知を E メールで送信するように設定します</a>
EMS の重要なイベント通知を syslog サーバに転送します	<a href="#">重要な EMS イベントの通知を syslog サーバに転送するように設定します</a>
EMS のイベント通知を SNMP トラップホストに転送する	<a href="#">SNMP トラップホストでイベント通知を受信するように設定します</a>
EMSでイベント通知をwebhookアプリケーションに転送する場合	<a href="#">重要なEMSイベントについて、通知をWebフックアプリケーションに転送するように設定します</a>

重要な **EMS** イベントの通知を **E** メールで送信するように設定します

重要なイベントの通知を E メールで受信するには、重要なアクティビティを示すイベントに関する E メールメッセージを送信するように EMS を設定する必要があります。

必要なもの

クラスタで E メールアドレスを解決するように DNS が設定されている必要があります。

このタスクについて

このタスクは、クラスタの実行中であれば、ONTAP コマンドラインでコマンドを入力していつでも実行できます。

手順

1. イベント用の SMTP メールサーバを設定します。

```
event config modify -mail-server mailhost.your_domain -mail-from cluster_admin@your_domain
```

2. イベントの通知に使用する E メール送信先を作成します。

```
event notification destination create -name storage-admins -email your_email@your_domain
```

3. 重要なイベントの通知を E メールで送信するように設定します。

```
event notification create -filter-name important-events -destinations storage-admins
```

重要な **EMS** イベントの通知を **syslog** サーバに転送するための設定

重大なイベントの通知を syslog サーバに記録するには、重要なアクティビティを示すイベントに関する通知を転送するように EMS を設定する必要があります。

必要なもの

クラスタで syslog サーバ名を解決するように DNS が設定されている必要があります。

このタスクについて

イベント通知用の syslog サーバがまだない場合は、先に syslog サーバを作成する必要があります。他のシステムのイベントを記録するためにすでに syslog サーバを使用している場合は、重要なイベントの通知にも同じ syslog サーバを使用できます。

このタスクは、クラスタの実行中であれば、ONTAP CLIでコマンドを入力していつでも実行できます。

ONTAP 9.12.1以降では、EMSイベントをTransport Layer Security (TLS) プロトコル経由でリモートsyslogサーバの指定ポートに送信できます。次の2つの新しいパラメータを使用できます。

### **tcp-encrypted**

いつ tcp-encrypted にを指定します syslog-transport`ONTAP は、デスティネーションホストの証明書を検証することで、そのホストのIDを検証します。デフォルト値はです `udp-unencrypted。

### **syslog-port**

デフォルト値 syslog-port パラメータは、の設定によって異なります syslog-transport パラメータ状況 syslog-transport がに設定されます tcp-encrypted、 syslog-port のデフォルト値は6514です。

詳細については、を参照してください event notification destination create のマニュアルページ。

手順

1. 重要なイベントの転送先の syslog サーバを作成します。

```
event notification destination create -name syslog-ems -syslog syslog-server-address -syslog-transport {udp-unencrypted|tcp-unencrypted|tcp-encrypted}
```

ONTAP 9.12.1以降では、に次の値を指定できます syslog-transport :

- ° udp-unencrypted -セキュリティなしのユーザデータグラムプロトコル
- ° tcp-unencrypted -セキュリティなしのTransmission Control Protocol
- ° tcp-encrypted - Transport Layer Security (TLS) を使用したTransmission Control Protocol

デフォルトのプロトコルはです udp-unencrypted`。

2. 重要なイベントについて、 syslog サーバに通知を転送するように設定します。

```
event notification create -filter-name important-events -destinations syslog-ems
```



**SNMP** トラップホストでイベント通知を受信するように設定します

SNMP トラップホストでイベント通知を受信するには、トラップホストを設定する必要があります。

必要なもの

- ・ クラスタで SNMP トラップと SNMP トラップが有効になっている必要があります。



SNMP トラップと SNMP トラップはデフォルトで有効になっています。

- ・ クラスタでトラップホスト名を解決するように DNS が設定されている必要があります。

このタスクについて

イベント通知（SNMP トラップ）を受信するように設定した SNMP トラップホストがまだない場合は、SNMP トラップホストを追加する必要があります。

このタスクは、クラスタの実行中であれば、ONTAP コマンドラインでコマンドを入力していつでも実行できます。

ステップ

1. イベント通知を受信するように設定された SNMP トラップホストがまだない場合は、次のいずれかを追加します。

```
system snmp traphost add -peer-address snmp_traphost_name
```

SNMP でデフォルトでサポートされるすべてのイベント通知が SNMP トラップホストに転送されます。

重要な**EMS**イベントについて、通知を**Web**フックアプリケーションに転送するように設定します

重要なイベント通知をwebhookアプリケーションに転送するようにONTAP を設定できます。必要な設定手順は、選択したセキュリティのレベルによって異なります。

**EMS**イベント転送を設定するための準備をします

イベント通知をWebフックアプリケーションに転送するようにONTAP を設定する前に、いくつかの概念と要件を考慮する必要があります。

**Webhook**アプリケーション

ONTAP イベント通知を受信できるWebフックアプリケーションが必要です。webhookは、実行するリモートアプリケーションまたはサーバの機能を拡張するユーザ定義のコールバックルーチンです。webhookは、宛先URLにHTTP要求を送信することによって、クライアント（この場合はONTAP）によって呼び出されるか、アクティブになります。具体的には、ONTAP は、webhookアプリケーションをホストするサーバにHTTP POST要求を送信し、イベント通知の詳細をXML形式で送信します。

セキュリティオプション

Transport Layer Security（TLS）プロトコルの使用方法に応じて、いくつかのセキュリティオプションがあります。選択するオプションによって、必要なONTAP 設定が決まります。



TLSは、インターネットで広く使用されている暗号化プロトコルです。1つ以上の公開鍵証明書を使用して、プライバシー、データの整合性、および認証を実現します。証明書は、信頼された認証局によって発行されます。

## HTTP

HTTPを使用してイベント通知を転送できます。この設定では、接続はセキュアではありません。ONTAP クライアントおよびWebフックアプリケーションのIDは検証されません。さらに、ネットワークトラフィックは暗号化も保護もされません。を参照してください ["HTTPを使用するようにwebhookの宛先を設定します"](#) をクリックして設定の詳細を確認します

## HTTPS

セキュリティを強化するために、webhookルーチンをホストするサーバーに証明書をインストールできます。HTTPSプロトコルは、ONTAP によって、WebフックアプリケーションサーバのIDおよびネットワークトラフィックのプライバシーと整合性を確保するために、両当事者によって使用されます。を参照してください ["HTTPSを使用するようにWebhookの宛先を設定する"](#) をクリックして設定の詳細を確認します

### HTTPSを相互認証で使用

Webブック要求を発行するONTAP システムにクライアント証明書をインストールすると、HTTPSセキュリティをさらに強化できます。ONTAP がWebフックアプリケーションサーバのIDを検証し、ネットワークトラフィックを保護することに加えて、webhookアプリケーションはONTAP クライアントのIDを確認します。この双方向ピア認証は、Mutual TLSと呼ばれています。を参照してください ["相互認証でHTTPSを使用するようにwebhookの宛先を設定します"](#) をクリックして設定の詳細を確認します

### 関連情報

- ["Transport Layer Security \(TLS\) プロトコルバージョン1.3"](#)

### HTTPを使用するようにwebhookの宛先を設定します

HTTPを使用してイベント通知をWebフックアプリケーションに転送するようにONTAP を設定できます。これは最も安全性の低いオプションですが、設定が最も簡単です。

### 手順

1. 新しい保存先を作成します restapi-ems イベントを受信するには：

```
event notification destination create -name restapi-ems -rest-api-url  
http://<webhook-application>
```

上記のコマンドでは、デスティネーションに\* HTTP \*スキームを使用する必要があります。

2. をリンクする通知を作成します important-events でフィルタリングします restapi-ems 目的地：

```
event notification create -filter-name important-events -destinations restapi-  
ems
```

### HTTPSを使用するようにWebhookの宛先を設定する

HTTPSを使用してイベント通知をWebhookアプリケーションに転送するようにONTAP を設定できます。ONTAP は、サーバ証明書を使用して、WebフックアプリケーションのIDを確認し、ネットワークトラフィックを保護します。

作業を開始する前に

- webhookアプリケーションサーバの秘密鍵と証明書を生成します
- ルート証明書をONTAP にインストールできるようにします

#### 手順

1. webhookアプリケーションをホストしているサーバに、適切なサーバ秘密鍵と証明書をインストールします。具体的な設定手順は、サーバによって異なります。
2. サーバのルート証明書をONTAP にインストールします。

```
security certificate install -type server-ca
```

このコマンドでは証明書を要求します。

3. を作成します restapi-ems イベントの受信先：

```
event notification destination create -name restapi-ems -rest-api-url
https://<webhook-application>
```

上記のコマンドでは、デスティネーションに\* HTTPS \*スキームを使用する必要があります。

4. をリンクする通知を作成します important-events 新しいでフィルタリングします restapi-ems 目的地：

```
event notification create -filter-name important-events -destinations restapi-
ems
```

相互認証でHTTPSを使用するようにwebhookの宛先を設定します

相互認証を使用したHTTPSを使用してイベント通知をWebhookアプリケーションに転送するようにONTAPを設定できます。この構成では、2つの証明書があります。ONTAP は、サーバ証明書を使用して、WebフックアプリケーションのIDを確認し、ネットワークトラフィックを保護します。また、webhookをホストするアプリケーションは、クライアント証明書を使用してONTAP クライアントのIDを確認します。

作業を開始する前に

ONTAP を設定する前に、次の作業を実行する必要があります。

- webhookアプリケーションサーバの秘密鍵と証明書を生成します
- ルート証明書をONTAP にインストールできるようにします
- ONTAP クライアントの秘密鍵と証明書を生成します

#### 手順

1. タスクの最初の2つの手順を実行します "HTTPSを使用するようにWebhookの宛先を設定する" ONTAP がサーバの識別情報を確認できるようにサーバ証明書をインストールする。
2. 適切なルート証明書と中間証明書をwebhookアプリケーションにインストールして、クライアント証明書を検証します。
3. ONTAP にクライアント証明書をインストールします。

```
security certificate install -type client
```

秘密鍵と証明書を入力するよう求められます。

#### 4. を作成します restapi-ems イベントの受信先：

```
event notification destination create -name restapi-ems -rest-api-url  
https://<webhook-application> -certificate-authority <issuer of the client  
certificate> -certificate-serial <serial of the client certificate>
```

上記のコマンドでは、デスティネーションに\* HTTPS \*スキームを使用する必要があります。

#### 5. をリンクする通知を作成します important-events 新しいでフィルタリングします restapi-ems 目的地：

```
event notification create -filter-name important-events -destinations restapi-  
ems
```

## 廃止された **EMS** イベントマッピングを更新します

### EMS イベントのマッピングモデル

ONTAP 9.0 よりも前のバージョンでは、EMS イベントはイベント名のパターンマッチングに基づいてイベントデスティネーションにのみマッピングできました。ONTAP コマンドセット (event destination、event route) は、最新バージョンのONTAP でも引き続きこのモデルを使用できますが、ONTAP 9.0以降では廃止されています。

ONTAP 9.0以降ではONTAP、拡張性に優れたイベントフィルタモデルを使用して、を使用して複数のフィールドに対してパターンマッチングを実行することを推奨します event filter、event notification` および `event notification destination コマンドセット。

廃止されたコマンドを使用してEMSマッピングが設定されている場合は、を使用するようにマッピングを更新する必要があります event filter、event notification` および `event notification destination コマンドセット。

イベントの送信先には、次の 2 種類があります。

#### 1. \* システムで生成される送信先 \* ：システムで生成される 5 つのイベントの送信先があります（デフォルトで作成）。

- allevents
- asup
- criticals
- pager
- traphost

システムで生成される宛先の一部は、特別な目的に使用されます。たとえば、ASUP デスティネーションは、callhome.\* イベントを ONTAP の AutoSupport モジュールにルーティングして AutoSupport メッセージを生成します。

#### 2. ユーザが作成した送信先：を使用して手動で作成します event destination create コマンドを実行

します

```
cluster-1::event*> destination show
```

Name	Mail Dest.	SNMP Dest.	Syslog Dest.	Hide
------	------------	------------	--------------	------

Params

-----

-----

allevents	-	-	-	
-----------	---	---	---	--

false

asup	-	-	-	
------	---	---	---	--

false

criticals	-	-	-	
-----------	---	---	---	--

false

pager	-	-	-	
-------	---	---	---	--

false

traphost	-	-	-	
----------	---	---	---	--

false

5 entries were displayed.

+

```
cluster-1::event*> destination create -name test -mail test@xyz.com
```

This command is deprecated. Use the "event filter", "event notification destination" and "event notification" commands, instead.

+

```
cluster-1::event*> destination show
```

+

Hide

Name	Mail Dest.	SNMP Dest.	Syslog Dest.	Hide
------	------------	------------	--------------	------

Params

-----

-----

allevents	-	-	-	
-----------	---	---	---	--

false

asup	-	-	-	
------	---	---	---	--

false

criticals	-	-	-	
-----------	---	---	---	--

false

pager	-	-	-	
-------	---	---	---	--

false

test	test@xyz.com	-	-	
------	--------------	---	---	--

false

traphost	-	-	-	
----------	---	---	---	--

false

6 entries were displayed.

廃止されたモデルでは、EMSイベントはを使用して個別にデスティネーションにマッピングされます event route add-destinations コマンドを実行します

```
cluster-1::event*> route add-destinations -message-name raid.aggr.*
-destinations test
This command is deprecated. Use the "event filter", "event notification
destination" and "event notification" commands, instead.
4 entries were acted on.

cluster-1::event*> route show -message-name raid.aggr.*
```

Time	Severity	Destinations	Freq	Threshd
raid.aggr.autoGrow.abort	NOTICE	test	0	0
raid.aggr.autoGrow.success	NOTICE	test	0	0
raid.aggr.lock.conflict	INFORMATIONAL	test	0	0
raid.aggr.log.CP.count	DEBUG	test	0	0

4 entries were displayed.

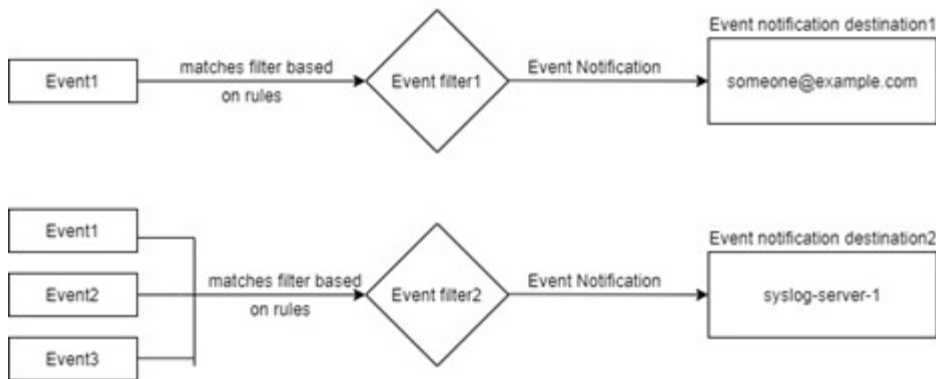
拡張性に優れた新しい EMS イベント通知メカニズムは、イベントフィルタとイベント通知の送信先に基づいています。新しいイベント通知メカニズムの詳細については、次の技術情報アートを参照してください。

- ["ONTAP 9 のイベント管理システムの概要"](#)

Legacy routing based model



Event notification based model



廃止された **ONTAP** コマンドから **EMS** イベントマッピングを更新します

廃止されたONTAP コマンドセットを使用してEMSイベントマッピングが設定されている場合 (event destination、event route`を使用するには、この手順 に従ってマッピングを更新する必要があります `event filter、event notification`および `event notification destination コマンドセット。

#### 手順

1. を使用して、システム内のすべてのイベントの送信先を一覧表示します event destination show コマンドを実行します

```
cluster-1::event*> destination show
```

Hide

Name	Mail Dest.	SNMP Dest.	Syslog Dest.
------	------------	------------	--------------

Params

allevents	-	-	-
false			
asup	-	-	-
false			
criticals	-	-	-
false			
pager	-	-	-
false			
test	test@xyz.com	-	-
false			
traphost	-	-	-
false			

6 entries were displayed.

2. 各送信先について、を使用してマッピングされているイベントを一覧表示します event route show -destinations <destination name> コマンドを実行します

```
cluster-1::event*> route show -destinations test
```

Time	Message	Severity	Destinations	Threshd	Freq
raid.aggr.autoGrow.abort	NOTICE	test	0	0	
raid.aggr.autoGrow.success	NOTICE	test	0	0	
raid.aggr.lock.conflict	INFORMATIONAL	test	0	0	
raid.aggr.log.CP.count	DEBUG	test	0	0	

4 entries were displayed.

3. 対応するを作成します event filter これには、これらすべてのイベントのサブセットが含まれます。たとえば、のみを含める場合などです raid.aggr.\* イベントの場合は、にワイルドカードを使用します message-name フィルタ作成時のパラメータ。単一のイベントに対するフィルタを作成することもできます。



最大 50 個のイベントフィルタを作成できます。



```
cluster-1::event*> filter create -filter-name test_events

cluster-1::event*> filter rule add -filter-name test_events -type
include -message-name raid.aggr.*

cluster-1::event*> filter show -filter-name test_events
Filter Name Rule      Rule      Message Name      SNMP Trap Type
Severity
      Position Type
-----
test_events
      1      include  raid.aggr.*      *      *
      2      exclude  *      *      *
2 entries were displayed.
```

4. を作成します event notification destination をクリックします event destination エンドポイント (SMTP、SNMP、syslogなど)

```
cluster-1::event*> notification destination create -name dest1 -email
test@xyz.com

cluster-1::event*> notification destination show
Name      Type      Destination
-----
dest1      email      test@xyz.com (via "localhost" from
"admin@localhost", configured in "event config")
snmp-traphost  snmp      - (from "system snmp traphost")
2 entries were displayed.
```

5. イベントフィルタをイベント通知の送信先にマッピングして、イベント通知を作成します。

```
cluster-1::event*> notification create -filter-name asup_events
-destinations dest1

cluster-1::event*> notification show
ID  Filter Name      Destinations
----
1   default-trap-events  snmp-traphost
2   asup_events         dest1
2 entries were displayed.
```

6. それぞれについて、手順1～5を繰り返します event destination が搭載されています event route

マッピング：



SNMPの送信先にルーティングされたイベントは、にマッピングする必要があります  
snmp-traphost イベント通知の送信先。SNMP トラップホストの送信先では、システム  
で設定された SNMP トラップホストを使用します。

```
cluster-1::event*> system snmp traphost add 10.234.166.135

cluster-1::event*> system snmp traphost show
      scspr2410142014.gdl.englab.netapp.com
(scspr2410142014.gdl.englab.netapp.com) <10.234.166.135>      Community:
public

cluster-1::event*> notification destination show -name snmp-traphost

      Destination Name: snmp-traphost
      Type of Destination: snmp
      Destination: 10.234.166.135 (from "system snmp
traphost")
      Server CA Certificates Present?: -
      Client Certificate Issuing CA: -
      Client Certificate Serial Number: -
      Client Certificate Valid?: -
```

# ONTAP コマンドリファレンス

ONTAP のメジャーリリースごとに、よく使用されるCLIコマンド（ONTAP のマニュアルページまたはマニュアルページ）が\_コマンドリファレンス\_にバンドルされています。これらのコマンドリファレンスでは、各ONTAP リリースでのCLIコマンドの使用方法について説明します。マニュアルページは、を使用してONTAP コマンドラインからも参照できます `man` コマンドを実行します

## サポートされているバージョンのONTAP のコマンドリファレンス

- ["ONTAP 9.14.1"](#)
- ["ONTAP 9.13.1"](#)
- ["ONTAP 9.12.1"](#)
- ["ONTAP 9.11.1"](#)
- ["ONTAP 9.10.1"](#)
- ["ONTAP 9.9.1"](#)
- ["ONTAP 9.8"](#)
- ["ONTAP 9.7"](#)
- ["ONTAP 9.6"](#)
- ["ONTAP 9.5"](#)
- ["ONTAP 9.3"](#)

## 限定サポートバージョンのONTAP のコマンドリファレンス (PDFのみ)

- ["ONTAP 9.4"](#)
- ["ONTAP 9.2"](#)
- ["ONTAP 9.1"](#)
- ["ONTAP 9.0"](#)

## CLI比較ツール

を使用すると、ONTAP リリース間でのコマンドラインインターフェイス（CLI）コマンドの変更点を確認できます ["CLI比較ツール"](#) をクリックしますNetApp Support Site。

詳細はこちら

- [ONTAP のコマンドラインインターフェイスを使用してください](#)
- [CLI コマンドディレクトリの移動方法](#)

# 法的通知

著作権に関する声明、商標、特許などにアクセスできます。

## 著作権

["https://www.netapp.com/company/legal/copyright/"](https://www.netapp.com/company/legal/copyright/)

## 商標

NetApp、NetApp のロゴ、および NetApp の商標ページに記載されているマークは、NetApp, Inc. の商標です。その他の会社名および製品名は、それぞれの所有者の商標である場合があります。

["https://www.netapp.com/company/legal/trademarks/"](https://www.netapp.com/company/legal/trademarks/)

## 特許

ネットアップが所有する特許の最新リストは、次のサイトで入手できます。

<https://www.netapp.com/pdf.html?item=/media/11887-patentspage.pdf>

## プライバシーポリシー

["https://www.netapp.com/company/legal/privacy-policy/"](https://www.netapp.com/company/legal/privacy-policy/)

## オープンソース

通知ファイルには、ネットアップソフトウェアで使用するサードパーティの著作権およびライセンスに関する情報が記載されています。

## ONTAP

["ONTAP 9.14.1に関する注意事項"](#)

["ONTAP 9.14.0に関する注意事項"](#)

["ONTAP 9.13.1に関する注意事項"](#)

["ONTAP 9.12.1に関する注意事項"](#)

["ONTAP 9.12.0の注意事項"](#)

["ONTAP 9.11.1の通知です"](#)

["ONTAP 9.10.1 での通知"](#)

["ONTAP 9.10.0に関する注意事項"](#)

["ONTAP 9.9.1 に関する注意事項"](#)

["ONTAP 9.8 に関する注意事項"](#)

["ONTAP 9.7 の場合の注意事項"](#)

["ONTAP 9.6に関する注意事項"](#)

["ONTAP 9.5 では次の点に注意"](#)

["ONTAP 9.4 の注意事項"](#)

["ONTAP 9.3 での注意"](#)

["ONTAP 9.2に関する注意事項"](#)

"ONTAP 9.1に関する注意事項"

## **MCC IPのONTAP メディエーター**

"9.9.1 MCC IPのONTAP メディエーターについての通知"

"9.8 MCC IPのONTAP メディエーターに関する通知"

"9.7 MCC IPのONTAP メディエーターについて注意が必要です"

## 著作権に関する情報

Copyright © 2024 NetApp, Inc. All Rights Reserved. Printed in the U.S. このドキュメントは著作権によって保護されています。著作権所有者の書面による事前承諾がある場合を除き、画像媒体、電子媒体、および写真複写、記録媒体、テープ媒体、電子検索システムへの組み込みを含む機械媒体など、いかなる形式および方法による複製も禁止します。

ネットアップの著作物から派生したソフトウェアは、次に示す使用許諾条項および免責条項の対象となります。

このソフトウェアは、ネットアップによって「現状のまま」提供されています。ネットアップは明示的な保証、または商品性および特定目的に対する適合性の暗示的保証を含み、かつこれに限定されないいかなる暗示的な保証も行いません。ネットアップは、代替品または代替サービスの調達、使用不能、データ損失、利益損失、業務中断を含み、かつこれに限定されない、このソフトウェアの使用により生じたすべての直接的損害、間接的損害、偶発的損害、特別損害、懲罰的損害、必然的損害の発生に対して、損失の発生の可能性が通知されていたとしても、その発生理由、根拠とする責任論、契約の有無、厳格責任、不法行為（過失またはそうでない場合を含む）にかかわらず、一切の責任を負いません。

ネットアップは、ここに記載されているすべての製品に対する変更を随時、予告なく行う権利を保有します。ネットアップによる明示的な書面による合意がある場合を除き、ここに記載されている製品の使用により生じる責任および義務に対して、ネットアップは責任を負いません。この製品の使用または購入は、ネットアップの特許権、商標権、または他の知的所有権に基づくライセンスの供与とはみなされません。

このマニュアルに記載されている製品は、1つ以上の米国特許、その他の国の特許、および出願中の特許によって保護されている場合があります。

権利の制限について：政府による使用、複製、開示は、DFARS 252.227-7013（2014年2月）およびFAR 5252.227-19（2007年12月）のRights in Technical Data -Noncommercial Items（技術データ - 非商用品目に関する諸権利）条項の(b)(3)項、に規定された制限が適用されます。

本書に含まれるデータは商用製品および / または商用サービス（FAR 2.101の定義に基づく）に関係し、データの所有権はNetApp, Inc.にあります。本契約に基づき提供されるすべてのネットアップの技術データおよびコンピュータ ソフトウェアは、商用目的であり、私費のみで開発されたものです。米国政府は本データに対し、非独占的かつ移転およびサブライセンス不可で、全世界を対象とする取り消し不能の制限付き使用权を有し、本データの提供の根拠となった米国政府契約に関連し、当該契約の裏付けとする場合にのみ本データを使用できます。前述の場合を除き、NetApp, Inc.の書面による許可を事前に得ることなく、本データを使用、開示、転載、改変するほか、上演または展示することはできません。国防総省にかかる米国政府のデータ使用权については、DFARS 252.227-7015(b)項（2014年2月）で定められた権利のみが認められます。

## 商標に関する情報

NetApp、NetAppのロゴ、<http://www.netapp.com/TM>に記載されているマークは、NetApp, Inc.の商標です。その他の会社名と製品名は、それを所有する各社の商標である場合があります。